Workstation User's Manual

Workstation 6.5

Workstation User’s Manual
Item: EN-000041-00

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About This Book

This manual, the *Workstation User's Manual*, provides information about installing and using VMware® Workstation 6.5. With Workstation, you can convert an existing physical PC into a VMware virtual machine or create a new virtual machine. Each virtual machine represents a complete PC, including the processor, memory, network connections and peripheral ports. Use Workstation to do the following:

- Host legacy applications and overcome platform migration issues.
- Configure and test new software or patches in an isolated environment.
- Automate tasks for software development and testing.
- Demonstrate multi-tier configurations on a single PC.

Intended Audience

This book is intended for anyone who needs to install, upgrade, or use VMware Workstation. Workstation users typically include people who do software development and testing or work with multiple operating systems or computing environments: software developers, QA engineers, trainers, salespeople who run demos, and anyone who wants to create virtual machines.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to:

docfeedback@vmware.com

Technical Support and Education Resources

The following sections describe the technical support resources available to you. To access the current versions of this book and other books, go to:

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

Online and Telephone Support

Use online support to submit technical support requests, view your product and contract information, and register your products. Go to:

http://www.vmware.com/support

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to:

http://www.vmware.com/support/phone_support.html

Support Offerings

Find out how VMware support offerings can help meet your business needs. Go to:

http://www.vmware.com/support/services

VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to:

http://www.vmware.com/services

Introduction and System Requirements

1

VMware Workstation is a desktop software that allows you to run multiple x86-compatible desktop and server operating systems simultaneously on a single PC, in fully networked, portable virtual machines—with no rebooting or hard drive partitioning required. This chapter includes the following topics:

- "Product Benefits" on page 21
- "Overview of This Manual" on page 22
- "Host System Requirements" on page 23
- "Virtual Machine Specifications" on page 29
- "Supported Guest Operating Systems" on page 32

Product Benefits

Workstation is used in the software development, quality assurance, training, sales, and IT fields.

Workstation streamlines software development and testing:

- Develop and test multiple operating systems and applications on a single PC.
- Connect virtual machines to simulate and test multitier configurations.
- Use multiple snapshots and debugging support to facilitate testing.
- Archive test environments on file servers where they can be easily restored or shared.

Workstation enhances productivity of IT professionals:

- Configure and test desktops and servers as virtual machines before deploying them to production.
- Test new multitier applications, application updates, and operating system patches on a single PC.
- Host legacy applications within virtual machines, facilitating operating system migrations and eliminating the need to port legacy applications.
- Create a virtual library of end-user configurations on a shared drive.

Workstation facilitates computer-based training and software demos:

- Package and deploy classroom material in virtual machines.
- Allow students to experiment with multiple operating systems, applications, and tools in secure, isolated virtual machines.
- Configure virtual machines to undo all changes at shutdown.
- Demo complex or multitier configurations on a single laptop.

Overview of This Manual

If you are a veteran Workstation user, see the Workstation Release Notes for a list of new features. For upgrade instructions, see "Preparing for an Upgrade" on page 46.

If you are new to Workstation, the first chapters of this manual—through Chapter 7, "Getting Started with Virtual Machines," on page 145—guide you through the key steps for installing the software and provide an introduction to using Workstation.

Later chapters provide in-depth information about the sophisticated features of Workstation. These chapters are intended for expert users.

Chapter 18, "Learning the Basics of VMware ACE," on page 365 through Chapter 22, "Installing ACE Packages," on page 447 describe how to use the ACE features included with the version of Workstation that runs on Windows hosts. VMware ACE authoring features enable you to package and deploy Pocket ACE and desktop virtual machines with encryption, restricted network access, and device control.

Host System Requirements

Like physical computers, the virtual machines running under Workstation perform better if they have faster processors and more memory.

The terms *host* and *guest* describe physical and virtual machines:

- **Host** — The physical computer on which you install the Workstation software is called the host computer, and its operating system is the host operating system.
- **Guest** — The operating system running inside a virtual machine is called a guest operating system.

For definitions of these and other special terms, see "Glossary" on page 511.

PC Hardware

- Standard x86-compatible or x86-64-compatible personal computer
- 733MHz or faster CPU minimum

  Compatible processors include the following:

  - Intel — Celeron, Pentium II, Pentium III, Pentium 4, Pentium M (including computers with Centrino mobile technology), Xeon (including "Prestonia"), Core, and Core 2 processors
  - AMD —Athlon, Athlon MP, Athlon XP, Athlon 64, Duron, Opteron, Turion 64, and Sempron
- Multiprocessor systems are supported.
- Support for 64-bit guest operating systems is available only on the following versions of these processors:
  - Revision D or later of AMD Athlon 64, Opteron, Turion 64, and Sempron
  - Intel Pentium 4, Core 2, and Xeon processors with EM64T and Intel Virtualization Technology

Memory

You need enough memory to run the host operating system, plus the memory required for each guest operating system and for applications on the host and guest. The minimum is 512MB (2GB is recommended). For memory requirements, see your guest operating system and application documentation.

As of version 6.5 of Workstation, the total amount of memory you can assign to all virtual machines running on a single host is limited only by the amount of RAM on the host. The maximum amount of memory for each virtual machine is 8GB.

Display

16-bit or 32-bit display adapter is recommended.

Disk Drives

Guest operating systems can reside on physical disk partitions or in virtual disk files.

Hard Disks

- IDE and SCSI hard drives are supported.
- VMware recommends at least 1GB free disk space for each guest operating system and the application software used with it. If you use a default setup, the actual disk space needs are approximately the same as those for installing and running the guest operating system and applications on a physical computer.
- 200MB (Linux) or 1.5GB (Windows) free disk space is required for basic installation. Delete the installer afterwards to reclaim disk space.

Optical CD-ROM/DVD-ROM Drives

- IDE and SCSI optical drives are supported.
- CD-ROM and DVD-ROM drives are supported.
- ISO disk image files are supported.

Floppy Drives

Virtual machines can connect to the host's disk drives. Floppy disk image files are also supported.

Local Area Networking

- You can use any Ethernet controller that the host operating system supports.
- Non-Ethernet networks are supported by using built-in network address translation (NAT) or using a combination of host-only networking plus routing software on the host operating system.

Host Operating System

VMware Workstation is available for Windows and Linux host operating systems. VMware ACE features are included only in the version of Workstation that runs on Windows hosts.

A Web browser is required for the Workstation Help system.

Windows Host Operating Systems

Workstation supports the following Windows 32-bit and 64-bit host operating systems.

Table 1-1. Supported Windows Host Operating Systems

Processor Type	Operating System Edition
32-bit	Windows Vista Enterprise Edition, SP1 Windows Vista Business Edition, SP1 Windows Vista Home Basic and Premium Editions, SP1 Windows Vista Ultimate Edition, SP1, SP3 Listed versions are also supported with no service pack.
	Windows Server 2003 Standard Edition with SP1 Windows Server 2003 Web Edition with SP1 Windows Server 2003 Small Business Edition with SP1 Windows Server 2003 Enterprise Edition with SP1 Windows Server 2003 R2, SP2
	Windows XP Home Edition with SP2 or later service pack Windows XP Professional with SP2 or later service pack
	Windows 2000 Server with SP4 Windows 2000 Professional with SP4 Windows 2000 Advanced Server with SP4

Table 1-1. Supported Windows Host Operating Systems (Continued)

Processor Type	Operating System Edition
64-bit	Windows Vista Enterprise Edition, SP1 Windows Vista Business Edition, SP1 Windows Vista Home Basic and Premium Editions, SP1 Windows Vista Ultimate Edition, SP1 Listed versions are also supported with no service pack.
	Windows Server 2003 x64 Edition with SP1 Windows Server 2003 x64 Edition R2 SP2
	Windows XP Professional x64 Edition with SP1 or later service pack

Linux Host Operating Systems

Workstation supports the following Linux 32-bit and 64-bit distributions and kernels for the host operating systems. Workstation might not run on systems that do not meet these requirements.

As newer Linux kernels and distributions are released, VMware modifies and tests its products for stability and reliability on those host platforms. VMware makes every effort to add support for new kernels and distributions in a timely manner, but until a kernel or distribution is added to the following list, its use with VMware products is not supported. Look for newer prebuilt modules in the Downloads area of the VMware Web site.

Table 1-2. Supported Linux Host Operating Systems

Processor Type	Operating System Edition
32-bit	Asianux Server 3
	CentOS 5.3 (experimental) CentOS 5.2 CentOS 5.1 CentOS 5.0
	Mandriva Corporate Desktop 4.0 Mandriva Corporate Server 4.0
	Oracle Enterprise Linux 5.3 (experimental) Oracle Enterprise Linux 5.2 Oracle Enterprise Linux 5.1 Oracle Enterprise Linux 5.0

Table 1-2. Supported Linux Host Operating Systems (Continued)

Processor Type	Operating System Edition
32-bit (continued)	Red Hat Enterprise Linux 5.2 WS Red Hat Enterprise Linux 5.2 AS, ES Red Hat Enterprise Linux 5.1 WS Red Hat Enterprise Linux 5.1 AS, ES Red Hat Enterprise Linux 5.0
	Red Hat Enterprise Linux 4.8 (experimental) Red Hat Enterprise Linux 4.7 Red Hat Enterprise Linux 4.6 Red Hat Enterprise Linux WS 4.5 (formerly called 4.0 Update 5) Red Hat Enterprise Linux AS 4.0, updates 1, 2, 3, 4 Red Hat Enterprise Linux ES 4.0, updates 1, 2, 3, 4 Red Hat Enterprise Linux WS 4.0, updates 1, 2, 3, 4
	SUSE Linux Enterprise Server 10 SP1 SUSE Linux Enterprise Server 9, SP1, SP2, SP3, SP4 SUSE Linux Enterprise Desktop 10, SP1, SP2 Listed versions are also supported with no service pack.
	openSUSE 10.3 (experimental) openSUSE 10.2 (formerly known as SUSE Linux 10.2)
	Ubuntu Linux 8.04 Ubuntu Linux 7.10 Ubuntu Linux 7.04 Ubuntu Linux 6.10 Ubuntu Linux 6.06
64-bit	Asianux Server 3
	CentOS 5.3 (experimental) CentOS 5.2 CentOS 5.1 CentOS 5.0
	Mandriva Corporate Desktop 4.0 Mandriva Corporate Server 4.0 **Note:** On 64-bit Mandriva hosts, some 32-bit compatibility libraries are required. Specifically, 32-bit `glibc`, `X11`, and `libXtst.so` are required.
	Oracle Enterprise Linux 5.3 (experimental) Oracle Enterprise Linux 5.2 Oracle Enterprise Linux 5.1 Oracle Enterprise Linux 5.0

Table 1-2. Supported Linux Host Operating Systems (Continued)

Processor Type	Operating System Edition
64-bit (continued)	Red Hat Enterprise Linux 5.2 WS Red Hat Enterprise Linux 5.2 AS, ES Red Hat Enterprise Linux 5.1 WS Red Hat Enterprise Linux 5.1 AS, ES Red Hat Enterprise Linux 5.0
	Red Hat Enterprise Linux 4.8 (experimental) Red Hat Enterprise Linux 4.7 Red Hat Enterprise Linux 4.6 Red Hat Enterprise Linux 4.5 (formerly called 4.0 Update 5) Red Hat Enterprise Linux AS 4.0, updates 3, 4 Red Hat Enterprise Linux ES 4.0, updates 3, 4 Red Hat Enterprise Linux WS 4.0, updates 3, 4
	Red Hat Enterprise Linux AS 3.0, stock 2.4.21, updates 2.4.21-15, 6, 7, 8 Red Hat Enterprise Linux ES 3.0, stock 2.4.21, updates 2.4.21-15, 6, 7, 8 Red Hat Enterprise Linux WS 3.0, stock 2.4.21, updates 2.4.21-15, 6, 7, 8
	SUSE Linux Enterprise Server 10, SP1 SUSE Linux Enterprise Server 9, SP1, SP2, SP3, SP4 SUSE Linux Enterprise Desktop 10, SP1, SP2 Listed versions are also supported with no service pack.
	openSUSE 10.3 openSUSE 10.2 (formerly known as SUSE Linux 10.2)
	Ubuntu Linux 8.04 Ubuntu Linux 7.10 Ubuntu Linux 7.04 Ubuntu Linux 6.10 Ubuntu Linux 6.06 **Note:** On 64-bit Ubuntu 6.x hosts, some 32-bit compatibility libraries are required. Specifically, 32-bit `glibc` and `X11` are required.

Virtual Machine Specifications

The following sections describe the devices that Workstation virtual machines support.

Processor

- Same processor as that on host computer.
- One virtual processor on a host with one or more logical processors.
- Two virtual processors (two-way virtual symmetric multiprocessing, or Virtual SMP) on a host with at least two logical processors.

  The following are considered to have two logical processors:

  - A multiprocessor host with two or more physical CPUs
  - A single-processor host with a multicore CPU
  - A single-processor host with hyperthreading enabled

  See "Use Two-Way Virtual Symmetric Multiprocessing" on page 349.

Chip Set

- Intel 440BX-based motherboard
- NS338 SIO
- 82093AA IOAPIC

BIOS

Phoenix BIOS 4.0 Release 6 with VESA BIOS

Memory

You can allocate up to 8GB of memory for a virtual machine, depending on host memory.

No maximum limit for the total available for all virtual machines.

Graphics

VGA and SVGA are supported.

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 950GB.
- CD-ROM can be a physical device or an ISO image file.

SCSI Devices

- Up to 60 devices.
- SCSI virtual disks up to 950GB.
- Hard disks can be virtual disks or physical disks.
- Generic SCSI support allows devices to be used without need for drivers in the host operating system. Works with scanners, CD-ROM, DVD-ROM, tape drives and other SCSI devices.
- LSI Logic LSI53C10xx Ultra320 SCSI I/O controller.
- Mylex (BusLogic) BT-958 compatible host bus adapter (requires add-on driver from VMware for Windows XP and Windows Server 2003).

Floppy Drives

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

Serial (COM) Ports

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

Parallel (LPT) Ports

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

USB Ports

- USB 1.1 UHCI controller, with a (transparent) virtual hub so that more than two devices can be connected.
- USB 2.0 EHCI controller that supports up to six devices. (Use the virtual machine settings editor to enable USB 2.0 support. See "Enable the USB 2.0 Controller for a Virtual Machine" on page 335.)
- Supports most devices, including USB printers, scanners, PDAs, hard disk drives, memory card readers, and digital cameras, as well as streaming devices such as webcams, speakers, and microphones.

Keyboard

104-key Windows 95/98 enhanced

Mouse and Drawing Tablets

- PS/2 mouse
- Serial tablets supported
- USB tablets supported

Ethernet Card

- Up to 10 virtual Ethernet cards.
- AMD PCnet-PCI II compatible.
- For 64-bit guests: Intel Pro/1000 MT Server Adapter compatible.

Sound

- Sound output and input.
- Emulates Creative Labs Sound Blaster AudioPCI. (Does not support MIDI input or game port controller/joysticks.)

Virtual Networking

- Support for 10 virtual Ethernet switches on Microsoft Windows host operating systems. Support for 255 virtual Ethernet switches on Linux hosts. Three switches are configured by default for bridged, host-only, and NAT networking.
- Support for most Ethernet-based protocols, including TCP/IP, NetBEUI, Microsoft Networking, Samba, Novell Netware, and Network File System.
- Built-in NAT supports client software using TCP/IP, FTP, DNS, HTTP, and Telnet, including VPN support for PPTP over NAT.

Supported Guest Operating Systems

Table 1-3 provides a simplified list of guest operating systems supported for virtual machines running in Workstation. For the most recent list, including details about specific operating system versions, service packs, and updates supported, see the *VMware Guest Operating System Installation Guide*, on the VMware Web site. The guide also provides notes on installing the most common guest operating systems.

Table 1-3. Guest Operating Systems

Processor Type	Operating System Edition
Windows 32-bit	Windows Vista Home Basic and Premium Windows Vista Business Windows Vista Enterprise Windows Vista Ultimate (Aero and 3-D effects not yet supported)
	Windows Server 2008 Standard Edition with or without Hyper-V Windows Server 2008 Datacenter Edition with or without Hyper-V Windows Server 2008 Enterprise Edition with or without Hyper-V Windows Web Server 2008 Windows Storage Server 2008 (experimental) (Aero and 3-D effects not yet supported)
	Windows Server 2003 Standard Edition Windows Server 2003 Small Business Edition Windows Server 2003 Web Edition
	Windows XP Professional Windows XP Home Edition
	Windows PE Windows RE

Table 1-3. Guest Operating Systems (Continued)

Processor Type	Operating System Edition
Windows 32-bit (continued)	Windows 2000 Professional Windows 2000 Server Windows 2000 Advanced Server
	Windows NT 4.0 Workstation with SP6 Windows NT 4.0 Server with SP6 Windows NT 4.0 Terminal Server Edition with SP6
	Windows Me
	Windows 98
	Windows 95
	Windows for Workgroups
Microsoft MS-DOS	MS-DOS
Windows 64-bit	Windows Vista Home Basic and Premium Windows Vista Business Windows Vista Enterprise Windows Vista Ultimate (Aero and 3-D effects not yet supported)
	Windows Essential Business Server 2008 Windows HPC Server 2008 Windows Server 2008 x64 Standard Ed. with or without Hyper-V Windows Server 2008 Datacenter x64 Ed. with or without Hyper-V Windows Server 2008 Enterprise x64 Ed. with or without Hyper-V Windows Web Server 2008 Windows Small Business Server 2008 Windows Storage Server 2008 (Aero and 3-D effects not yet supported)
	Windows Server 2003 x64
	Windows Server x64
	Windows XP Professional x64
	Windows PE x64 Windows RE x64

Table 1-3. Guest Operating Systems (Continued)

Processor Type	Operating System Edition
Linux 32-bit	Asianux Server
	CentOS
	Mandrake Linux Mandriva Linux Mandriva Corporate Desktop Mandriva Corporate Server
	Novell Linux Desktop
	Oracle Enterprise Linux
	Red Hat Linux
	Red Hat Enterprise Linux Red Hat Enterprise Linux Advanced Server (AS) Red Hat Enterprise Linux Enterprise Server (ES) Red Hat Enterprise Linux Workstation Red Hat Enterprise Linux Desktop with or without the Workstation Option Red Hat Enterprise Linux Advanced Platform with or without the Workstation Option
	SUSE Linux
	openSUSE Linux
	SUSE Linux Enterprise Server SUSE Linux Enterprise Desktop
	Turbolinux Server Turbolinux Enterprise Server Turbolinux Workstation Turbolinux Desktop
	Ubuntu Linux
Linux 64-bit	Asianux Server
	CentOS
	Mandriva Linux Mandriva Corporate Desktop Mandriva Corporate Server
	Oracle Enterprise Linux

Table 1-3. Guest Operating Systems (Continued)

Processor Type	Operating System Edition
Linux 64-bit (continued)	Red Hat Enterprise Linux Red Hat Enterprise Linux Advanced Server (AS) Red Hat Enterprise Linux Enterprise Server (ES) Red Hat Enterprise Linux Workstation Red Hat Enterprise Linux Desktop with or without the Workstation Option Red Hat Enterprise Linux Advanced Platform with or without the Workstation Option
	SUSE Linux
	openSUSE Linux
	SUSE Linux Enterprise Server SUSE Linux Enterprise Desktop
	Turbolinux Server
	Ubuntu Linux
Novell NetWare 32-Bit	NetWare
Novell Open Enterprise Server 32-bit	Open Enterprise Server 32-bit
FreeBSD 32-bit	FreeBSD 32-bit **Note:** If you use SCSI virtual disks larger than 2GB with FreeBSD 4.0–4.3, the guest operating system does not boot. To work around this issue, see the *VMware Guest Operating System Installation Guide*.
FreeBSD 64-bit	FreeBSD 64-bit
Sun 32-bit	Solaris x86 32-bit
	Sun Java Desktop System (JDS)
Sun 64-bit	Solaris x86 64-bit

Support for 64-Bit Guest Operating Systems

Workstation supports virtual machines with 64-bit guest operating systems, running on host machines with the following processors:

- Revision D or later of AMD Athlon 64, Opteron, Turion 64, and Sempron
- Intel Pentium 4 and Core 2 processors with EM64T and Intel Virtualization Technology

Workstation supports virtual machines with 64-bit guest operating systems only on host machines that have one of the supported 64-bit processors. When you power on a virtual machine with a 64-bit guest operating system, Workstation performs an internal check. If the host CPU is not a supported 64-bit processor, you cannot power on the virtual machine.

VMware also provides a standalone utility that you can use without Workstation to perform the same check and determine whether your CPU is supported for Workstation virtual machines with 64-bit guest operating systems. Download the 64-bit processor check utility from the downloads area of the VMware Web site.

Workstation supports virtual machines with 64-bit guest operating systems only in versions 5.5 and later. If your version of Workstation is 5.0 or earlier, upgrade to version 6.0 or later for 64-bit guest operating system support. A virtual machine created in Workstation version 5.5 with a 64-bit operating system cannot be powered on or resumed in Workstation versions 5.0 and earlier.

Installing and Upgrading VMware Workstation

2

This chapter discusses how to install Workstation on your Linux or Windows host. This chapter contains the following topics:

Installation Prerequisites

Installing VMware Workstation is usually a simple process of running a standard installation wizard.

Before you run the installation program, be sure you have the following:

- **A compatible host** – Verify that the computer and host operating system meet the system requirements for running Workstation. See "Host System Requirements" on page 23.
- **Workstation installation software** – If you have the packaged distribution of Workstation, the installation software is on the installation media in your package. If you have the electronic distribution, the installation software is in the file you downloaded.

  Workstation is available for Windows and Linux host computers. The installation files for both host platforms are included in the packaged distribution.

- **Workstation or VMware ACE serial number** – Your serial number is on the registration card in your package. If you purchased Workstation or VMware ACE online, the serial number is sent by email.

  Your serial number allows you to use Workstation only on the host operating system for which you licensed the software. For example, if you have a serial number for a Windows host, you cannot run the software on a Linux host.

  You need one license for each user.

  To use Workstation on a different host operating system, purchase a license on the VMware Web site. You can also obtain an evaluation license at no charge for a 30-day evaluation of the software. For more information, go to the VMware Web site.

  If you do not enter the Workstation serial number at installation time (an option available on a Windows host), you are prompted to enter it the first time you attempt to power on a virtual machine.

- **A guest operating system** – After Workstation is installed, you need the operating system installation CDs, DVDs, or ISO image files to set up a guest in a virtual machine.

- **(Optional) Eclipse or Microsoft Visual Studio** – To install the Eclipse or Visual Studio Integrated Virtual Debugger plug-ins included with Workstation, Eclipse or Visual Studio must be installed on the host before you run the Workstation installer. If you install one or both of these programs after you install Workstation, run the Workstation installer again and select the **Modify** option to install the plug-ins at that time.

  For more information about supported versions of Visual Studio and Eclipse, see "Supported Versions of Visual Studio" on page 486 and "Eclipse Requirements" on page 474.

Sharing a Workstation Host with Other VMware Products

You cannot have VMware Workstation installed on the same host machine with another VMware product, such as VMware Server or the VMware Virtual Machine Console. The only VMware products that can share a host machine with Workstation are the VMware VirtualCenter client software and VMware Converter. If you plan to install VMware Workstation on a host machine that already contains another VMware product, you must uninstall that product first.

After you complete the prerequisites and determine which computer you want to use for hosting Workstation, see the appropriate platform-specific installation topic.

Install Workstation on a Windows Host

Before you begin, make sure you have the items listed in "Installation Prerequisites" on page 37. Although you can enter the serial number after installation, VMware recommends entering it at installation time.

This topic describes how to use an installation wizard to install Workstation. To instead use the command-line interface to perform a silent installation on many computers, see "Install Workstation Silently" on page 40.

To install Workstation on a Windows host

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

   Log in as local administrator (that is, do not log in to the domain, unless your domain account is also a local administrator).

   Although an administrator must install Workstation, a user without administrative privileges can run the program after it is installed.

2. From the **Start** menu, choose **Run** and specify the path to either the CD/DVD drive or the downloaded installer file:

   - If you are installing from the installation media, enter **`D:\setup.exe`**, where `D:` is the drive letter for your CD/DVD drive.
   - If you are installing from a downloaded file, browse to the directory where you saved the downloaded installer file, and run the installer.

     The filename is similar to `VMware-workstation-<xxxx-xxxx>.exe`, where `<xxxx-xxxx>` is a series of numbers representing the version and build numbers.

   On Windows Vista, when the User Account Control dialog box prompts you for permission to run the installer, click **Continue**.

   If you have an earlier version of Workstation installed on your system, the installer removes that version before installing the new version. After the uninstallation is complete, you might be prompted to restart your computer before the installer can install the new version.

3. When the wizard opens and finishes computing space requirements, click **Next**.

4 On the Setup Type page, select **Typical** unless you do not want to install the applicable Workstation IDE plug-ins, or if you have Eclipse installed in a nonstandard location.

   If you have Visual Studio or Eclipse installed, the installer installs an integrated virtual debugger. If you do not want a plug-in installed, select the **Custom** setup, and select not to install that component.

   Do not attempt to install the Eclipse Virtual Debugger on 64-bit Windows hosts.

   If you select **Custom**, you can use the **Space** button to find out how much disk space is required for each component of the installation. Click **Help** for a description of what each type of icon in the list means.

5 (Optional) On the Destination Folder page (for typical setups) or the Custom Setup page (for custom setups), if you do not want Workstation installed in the directory that is shown, click **Change** and specify a different directory.

   If you specify a directory that does not exist, the installer creates it for you. You cannot install Workstation on a network drive.

6 Follow the rest of the wizard prompts.

Some installations might require that you reboot your computer. When you restart, you do not need to log in as a user with Administrator privileges.

Install Workstation Silently

If you are installing Workstation on several Windows host computers and do not want to respond to wizard prompts, you can use the silent installation feature of the Microsoft Windows Installer. This feature is convenient, for example, in a large enterprise.

Before you begin, ensure that the host computer has version 2.0 or higher of the MSI runtime engine. This version of the installer is available in versions of Windows beginning with Windows XP and is available separately from Microsoft. For additional details on using the Microsoft Windows Installer, see the Microsoft Web site.

To install Workstation silently

1 Open a command prompt and enter the following command to silently extract the administrative installation image from the VMware Workstation installer:

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

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

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

2 Enter the following command on one line to run a silent installation using `msiexec` and the administrative installation image you extracted in the previous step:

```
msiexec -i "<install_temp_path>\VMware Workstation.msi"
[INSTALLDIR="<path_to_program_directory>"] ADDLOCAL=ALL
[REMOVE=<feature_name,feature_name>] /qn
```

To install Workstation in a location other than the default, change the path that follows `INSTALLDIR=` to specify the location.

Use the optional `REMOVE=<property>` to skip installation of certain features. The `REMOVE=<property>` setting can take one or more of the values listed in Table 2-1.

Table 2-1. Values for the `REMOVE` Property

Value	Description
`Authd`	VMware authorization service, which is used to perform tasks when you are not running Workstation as an Administrator user.
`Network`	Networking components, including the virtual bridge and the host adapters for host-only networking and NAT networking. Do not remove this component if you want to use NAT or DHCP.
`DHCP`	Virtual DHCP server.
`NAT`	Virtual NAT device.

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

If you specify `REMOVE=Network`, the installer skips installation of certain networking components, including NAT and DHCP. You do not need to specify DHCP or NAT separately.

You can customize the installation further by using the format `<property>="<value>"` to add any of the installation properties listed in Table 2-2 to the command. A value of 1 means true. A value of 0 means false. If you use the serial number property, enter the serial number with hyphens (xxxxx-xxxxx-xxxxx-xxxxx).

Table 2-2. Property Values

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

Uninstall Workstation from a Windows Host

Use the Windows Control Panel to uninstall Workstation. Workstation licenses, preference settings, and virtual machines are not removed, but virtual network settings are removed.

To uninstall Workstation from a Windows host

Do one of the following:

- On Windows Vista hosts, go to **Start > Control Panel > Programs > Programs and Features > Uninstall a program** and uninstall **VMware Workstation**.
- On other Windows hosts, use the Add/Remove Programs item in the control panel and remove **VMware Workstation**.

Install Workstation on a Linux Host

Before you begin, read the following notes and make adjustments to your host system:

- Make sure you have the items listed in "Installation Prerequisites" on page 37.
- The real-time clock function must be compiled into your Linux kernel.
- 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).
- To use the Workstation Help system, you must have a Web browser installed on the host computer.

The installation topic describes an installation from the installation media included in the Workstation media kit. 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 installation media.

Install Workstation on a Linux Host Using a Bundle

The bundle-based installer lets you install the product in one step. If the GUI-based installer fails, run the installer file with the `--console` command in your terminal.

NOTE On Red Hat Enterprise Linux 5.1 hosts and possibly some other Linux distributions, the bundle-based installer launches a command-line wizard rather than a GUI wizard.

`VMware-Workstation-<xxxx-xxxx>.<architecture>.bundle` is the name of the installer file. In the name, `<xxxx-xxxx>` is a series of numbers that represent the version and build numbers, and `<architecture>` is `i386` or `.x86_64`.

To install Workstation on a Linux host using a bundle

1. Log in to your Linux host with the user name you plan to use when running Workstation.
2. In a terminal window, become root to perform the initial installation steps:

   `su`

3. If you are installing from the installation media instead of a downloaded file, mount the Workstation installation media.

4 Change directories to the directory where the installer file is located and run the installation file:

```
sh VMware-Workstation-<xxxx-xxxx>.<architecture>.bundle
```

If you are using the Workstation installation media, this file is in the `Linux` directory.

5 Accept the EULA to continue.

6 (Optional) If you are using the `--console` option or running a host that does not support the GUI installation do one of the following:

- To scroll to the end of the VIX EULA, press spacebar.
- To exit the EULA and go to the prompt **Do you agree? [yes/no]**, press q.

7 (Optional) Enter the directory path to the Integrated Virtual Debugger for Eclipse if Eclipse is installed.

8 Click **Install**.

9 Open Workstation to launch the kernel module updater to install and configure the kernel.

See "Start Workstation on a Linux Host" on page 52.

Using Command-Line Installation Options with the Bundle

You can also use command-line installation options to install Workstation on a Linux host. To use the options, you must be logged in as root. After finishing the installation process, exit from the root account.

The common command-line installation options for the bundle installer are the following:

- `--gtk` – Opens the GUI-based VMware installer, which is the default option.
- `--regular` – Shows the optional steps for installation such as the directory path for the Integrated Virtual Debugger for Eclipse. This is the default option.
- `--console` – Lets you use the terminal for installation.
- `--custom` – Shows all the directory paths for the binary files, library files, manual files, documentation files, and init script during installation.
- `--required` – Opens only the EULA and proceeds to install Workstation.
- `--ignore-errors` – Uninstalls the files and ignores configuration errors during uninstall.

Install Workstation on a Linux Host Using an RPM

The RPM-based VMware installer does not have a GUI. You must install the RPM using the command-line.

To install Workstation on a Linux host using an RPM

1. Log in to your Linux host with the user name you plan to use when running Workstation.
2. In a terminal window, use the following command to become root so you can perform the initial installation steps:

   ```
   su
   ```

3. If you are installing from the installation media instead of a downloaded file, mount the Workstation installation media.
4. Change to the `Linux` directory on the installation media.
5. Run RPM specifying the installation file:

   ```
   rpm -Uhv VMware-Workstation-<xxxx>.rpm
   ```

   `VMware-Workstation-<xxxx>.rpm` is the installation file. In place of <xxxx> the filename contains numbers that correspond to the version and build.

6. Accept the EULA to continue.
   - To scroll to the end of the VIX EULA, press spacebar.
   - To exit the EULA and go to the prompt **Do you agree? [yes/no]**, press q.

Uninstall Workstation from a Linux Host

When you uninstall Workstation, product licenses, preference settings, and virtual machines are not removed, but virtual network settings are removed.

To uninstall Workstation from a Linux host

Do one of the following:

- If you used the bundle installer, enter the following command:

  ```
  vmware-uninstall
  ```

- If you used the RPM installer, enter the following command:

  ```
  rpm -e VMware-Workstation
  ```

Preparing for an Upgrade

When you install a new version of Workstation, the previous version is uninstalled but the preferences you set, license files, and virtual machines are not removed. Although you do not delete virtual machines created with an earlier version of Workstation, VMware recommends that you make backup copies and power them off completely in preparation for the upgrade.

VMware recommends that you complete the following tasks before upgrading:

- Make sure all virtual machines are Workstation 4, 5, or 6.0.x virtual machines. Direct upgrades from a Workstation 2 or 3 virtual machine are not supported in Workstation 6.0.x and 6.5.
- If a virtual machine was created with a version of Workstation earlier than Workstation 5.5 and it has a snapshot, delete the snapshot before upgrading. See "Delete a Snapshot or a Recording" on page 198.
- For upgrades from Workstation 4, 5.x, or 6.0.x, if you bridged (mapped) virtual networks to specific physical or virtual adapters, write down the settings you used.

  Although Workstation 6.5 generally preserves network settings during the upgrade, it cannot preserve bridge settings created with Workstation 4, 5.x, or 6.0.x.
- If any virtual machines are suspended, resume them, shut down the guest operating system, and power them off.
- If any virtual machines are running in the background, start them in Workstation and power them off. See "Start a Virtual Machine That Is Running in the Background" on page 147.
- Back up the virtual machines by making backup copies of all the files in the virtual machine directories.

  This includes `.vmdk` or `.dsk` files, `.vmx` or `.cfg` files, and `.nvram` files. Depending on your upgrade path, you might not be able to run your virtual machines under both Workstation 6.5 and your previous version of Workstation.

You can now use one of the following platform-specific tasks to install Workstation:

- "Upgrade Workstation on a Windows Host" on page 47
- "Upgrade Workstation on a Linux Host" on page 50

Upgrade Workstation on a Windows Host

You can upgrade from Workstation version 4, 5, or 6.0.x to Workstation 6.5 by running the VMware Workstation 6.5 installation program.

Before you begin, make sure that you have a Workstation 6.5 serial number. Also perform the tasks described in "Preparing for an Upgrade" on page 46.

To upgrade Workstation and upgrade the host operating system to Windows Vista, see "Upgrading to a Windows Vista Host" on page 48.

To upgrade Workstation on a Windows host

1. Log in to your Microsoft Windows host as the Administrator user or as a user who is a member of the Windows Administrators group.
2. Launch the Workstation 6.5 installer from your download directory or CD/DVD drive.

   Workstation automatically uninstalls the previous version but saves all the network settings except for bridged settings used to map individual virtual networks to specific physical or virtual adapters.
3. Reboot your computer if you are prompted to do so, and log in again as the Administrator user or as a user who is a member of the Windows Administrators group.
4. Follow the installation wizard prompts to complete the installation.
5. Reboot your computer if you are prompted to do so.

   You can now log in as you normally do. You do not need to log in as an Administrator now that Workstation is installed.
6. If you used bridged settings to map virtual networks to specific physical or virtual adapters, re-create the mappings.

   Although Workstation 6.5 generally preserves network settings during the upgrade, it cannot preserve mappings created with Workstation 4, 5.x, or 6.0.x.

To use Workstation 6.5 to upgrade virtual machines, see "Change the Version of a Virtual Machine" on page 91.

Upgrading to a Windows Vista Host

This topic provides instructions for various upgrade scenarios that involve Windows Vista.

During the upgrade from Windows XP to Windows Vista, the location of virtual machines might change. The Windows Vista upgrade uses the registry to map the virtual machines to a new location by using the following paths:

- On Windows XP, the default virtual machine location before the upgrade is `C:\Documents and Settings\<user>\My Virtual Machines`.
- On Windows Vista, the default virtual machine location after the upgrade is `C:\Users\<user>\Documents\Virtual Machines`.

After the upgrade is complete, if the **Favorites** list in Workstation does not work correctly, you can remove the virtual machines from it and add them again.

Upgrade Workstation 5 on Windows XP to Workstation 6.5 on Windows Vista

As part of the upgrade, you must uninstall the Workstation 5 application, but you do not need to uninstall Workstation 5 virtual machines.

To upgrade Workstation 5 on Windows XP to Workstation 6.5 on Windows Vista

1. On the Windows XP host, use the Control Panel's **Add/Remove Programs** item to uninstall Workstation 5.x.
2. Upgrade the operating system to Windows Vista, as described in the Microsoft documentation.
3. Install Workstation 6.5.
4. (Optional) To upgrade the virtual machines, use the Change Version wizard in Workstation 6.5.

   See "Change the Version of a Virtual Machine" on page 91.

Upgrade Workstation 5 on Windows Vista to Workstation 6.5 on Windows Vista

Because Workstation 5 was only experimentally supported on Windows Vista, VMware recommends manually uninstalling Workstation 5.x before installing Workstation 6.5.

As part of the upgrade, you must uninstall the Workstation 5 application, but you do not need to uninstall Workstation 5 virtual machines.

To upgrade Workstation 5 on Windows Vista to Workstation 6.5 on Windows Vista

1. Go to **Start** > **Control Panel** > **Programs** > **Programs and Features** > **Uninstall a program**.
2. Select **VMware Workstation** and click **Uninstall**.
3. Install Workstation 6.5.

   See "Install Workstation on a Windows Host" on page 39.
4. (Optional) To upgrade the virtual machines, use the Change Version wizard in Workstation 6.5.

   See "Change the Version of a Virtual Machine" on page 91.

Upgrade Workstation 6.x on Windows XP to Workstation 6.5 on Windows Vista

Before you begin, make sure that you have Windows XP with Service Pack 2.

To upgrade Workstation 6.x from Windows XP to Windows Vista

1. Log in as the Administrator user or as a user who is a member of the Windows Administrators group.
2. Make sure that Workstation is not running and that no virtual machines are running in the background.
3. Upgrade the host operating system to Windows Vista, as described in the Microsoft documentation.
4. Run the Workstation 6.5 installer.
5. (Optional) To upgrade the virtual machines, use the Change Version wizard in Workstation 6.5.

   See "Change the Version of a Virtual Machine" on page 91.

Upgrade Workstation on a Linux Host

You can upgrade from Workstation version 4, 5, or 6.0.x to version 6.5 by running the VMware Workstation 6.5 installation program.

Before you begin, make sure that you have a Workstation 6.5 serial number. You are prompted to enter the serial number after installation is complete, the first time you start Workstation after the upgrade. Also perform the tasks described in "Preparing for an Upgrade" on page 46.

If you currently have Workstation 4, 5, or 6.0.x installed on your system, the older version will be uninstalled automatically before the latest version of Workstation is installed. Workstation 6.5 saves network settings except for bridged settings used to map individual virtual networks to specific physical or virtual adapters.

NOTE Starting with Workstation 5, Samba is no longer automatically configured during installation.

To upgrade Workstation on a Linux host

1. If your previous installation was from an RPM installer and you want to use the RPM installer for Workstation 6.5, manually uninstall the previous version of Workstation.

   To manually uninstall Workstation, see "Uninstall Workstation from a Linux Host" on page 45.

   If you manually uninstall the older version, Workstation cannot save the network settings. If you want to preserve network settings, do not manually uninstall Workstation. Instead, use the bundle installer program rather than the RPM installer.

2. Run the Workstation installer as you would for a new installation.

3. If you used bridged settings to map virtual networks to specific physical or virtual adapters, re-create the mappings.

   Although Workstation 6.5 generally preserves network settings during the upgrade, it cannot preserve mappings created with Workstation 4, 5.x, or 6.0.x.

4. (Optional) To upgrade the virtual machines, use the Change Version wizard in Workstation 6.5.

   See "Change the Version of a Virtual Machine" on page 91.

Learning Workstation Basics

3

This chapter discusses launching the Workstation program and introduces the VMware Workstation window. This chapter includes the following topics:

Start Workstation on a Windows Host

Depending on the options you selected during installation, you might have a desktop shortcut, a **Start** menu item, or both for launching Workstation.

To start Workstation on a Windows host

1 From the **Start** menu, choose **Start > Programs > VMware > VMware Workstation**.

2 If this is the first time you are launching Workstation, read and accept the end user license agreement (EULA).

Start Workstation on a Linux Host

Whether you can start Workstation from a Linux user interface depends on the Linux distribution. For example, on Red Hat Enterprise Linux 5.1, the **VMware Workstation** menu item is in the **Applications > System Tools** menu.

You can always start Workstation from the command line. Although you must become root to install Workstation, you do not have to be root to start and run Workstation.

To start Workstation on a Linux host

1. Open a terminal window.
2. Do one of the following:
   - If `/usr/bin` is in your default path, enter the following command:

     ```
     vmware &
     ```

   - If `/usr/bin` is not in your default path, enter the following command:

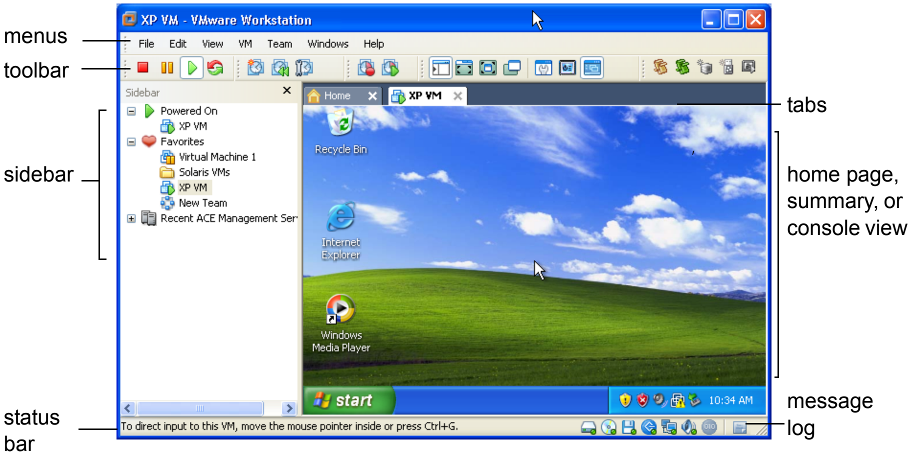
     ```
     /usr/bin/vmware &
     ```

3. Read and accept the end user license agreement (EULA).

Overview of the Workstation Window

A Workstation virtual machine is like a separate computer that runs in a window on your physical computer. However, Workstation displays more than the screen of another computer. From the Workstation window, you can access and run virtual machines and teams of virtual machines. You can also switch easily from one virtual machine to another.

Figure 3-1. VMware Workstation Window



To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

The VMware Workstation window contains the following sections:

- **Home page, summary, console, or appliance view** – Main part of the window that shows the virtual machines.
- **Tabs** – Each open virtual machine has a tab. Click a tab to make that virtual machine active. Click the **Close** button to close the tab. Depending on how you configure Workstation, the virtual machine is then either powered off or continues to run in the background.
- **Sidebar** – Bookmark your favorite virtual machines and teams of virtual machines for quick access. You can also see which virtual machines are powered on. Right-click context menus enable you to perform many operations on a selected virtual machine. An additional section of the sidebar displays ACE Management Servers.
- **Status bar** – Displays Workstation messages and an icon for each removable device. You can click or right-click an icon to disconnect it or edit its configuration.
- **Message log**— A note icon indicates whether any unread messages are present in the message log for the selected virtual machine. If the icon is dimmed, all messages were read. To open the message log, right-click the icon and choose **Open Message Log**. Alternatively, from the menu bar, choose **VM > Message Log**.

  Messages include warning information about the virtual machine, such as “Could not connect to the floppy drive.” or “No bootable device was detected.” Select an item in the message log to see a longer description of the message.

Home Page and Views

Workstation displays one of four views in the main part of the window: the home page, the summary view, the console view, or the appliance view.

Home Page

Click the **Home** tab to display the Workstation home page. Use the icons on the home page to start creating a new virtual machine or open an existing virtual machine.

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

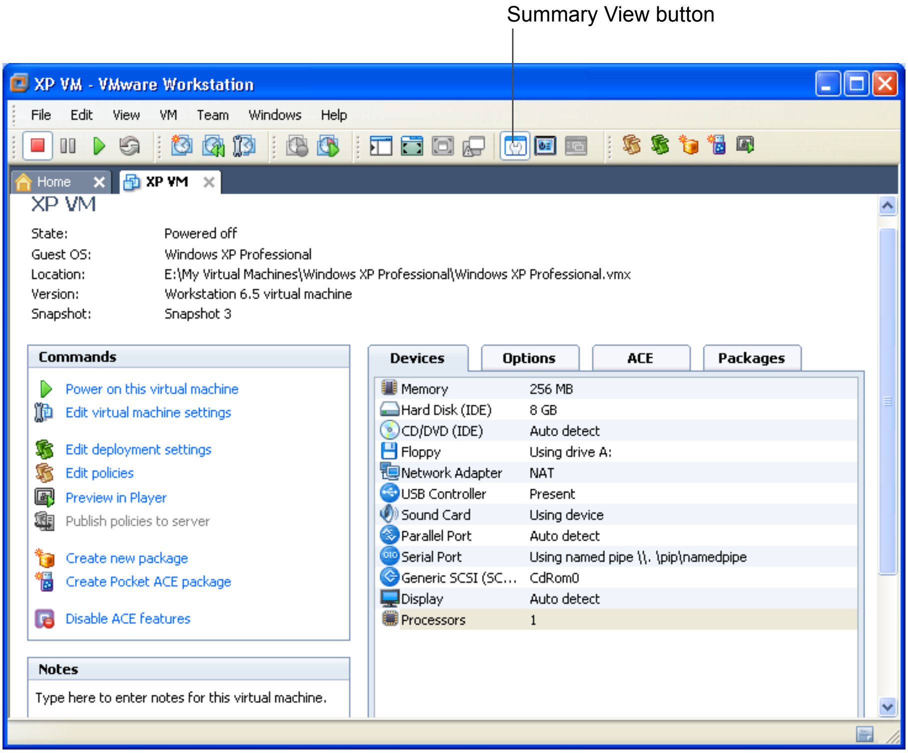
Summary View

When you select a tab for a powered-off virtual machine or team of machines, Workstation displays only a summary of the configuration information about that item. Workstation also displays a summary for a suspended virtual machine or team. Click the **Summary** button in the toolbar at any time to examine settings in the summary view.

Summary views appear only for virtual machines that are currently open. See "Starting a Virtual Machine" on page 145. The summary or console view remains visible as long as the virtual machine remains open.

Figure 3-2 shows an example of the summary view.

Figure 3-2. Summary View for a Virtual Machine on a Windows Host



Summary View button

XP VM

State:	Powered off
Guest OS:	Windows XP Professional
Location:	E:\My Virtual Machines\Windows XP Professional\Windows XP Professional.vmx
Version:	Workstation 6.5 virtual machine
Snapshot:	Snapshot 3

Commands

- Power on this virtual machine
- Edit virtual machine settings
- Edit deployment settings
- Edit policies
- Preview in Player
- Publish policies to server
- Create new package
- Create Pocket ACE package
- Disable ACE features

Notes

Type here to enter notes for this virtual machine.

Memory	256 MB
Hard Disk (IDE)	8 GB
CD/DVD (IDE)	Auto detect
Floppy	Using drive A:
Network Adapter	NAT
USB Controller	Present
Sound Card	Using device
Parallel Port	Auto detect
Serial Port	Using named pipe \\. \pip\namedpipe
Generic SCSI (SC...	CdRom0
Display	Auto detect
Processors	1

The **Commands** section gives you access to the most-often used commands from the **VM** menu. On Windows hosts, for ACE-enabled virtual machines, this includes commands for creating security policies and virtual machine packages to deploy to end users, as well as a command for previewing the ACE-enabled virtual machine in VMware Player.

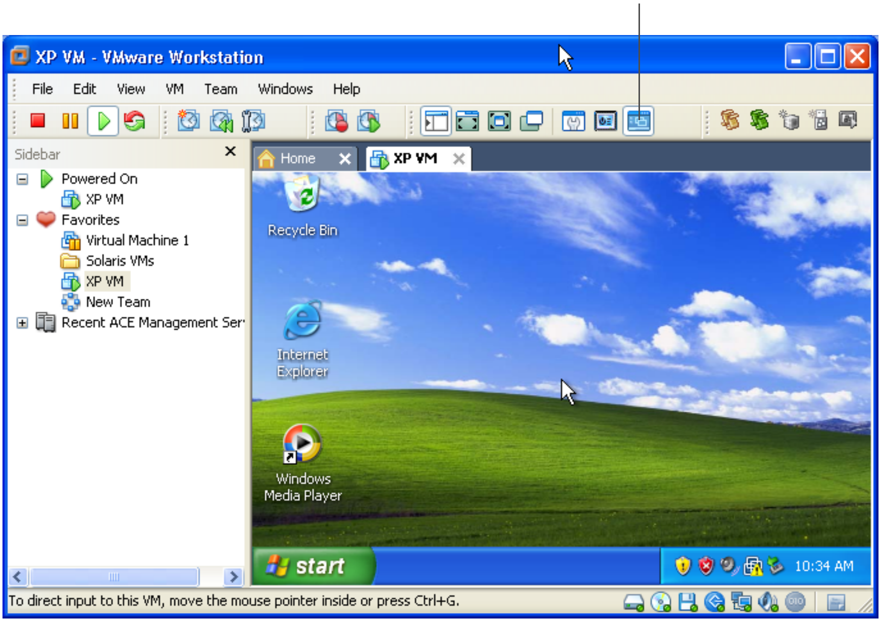
The section that includes the **Devices**, **Options**, and (sometimes) **ACE** and **Packages** tabs enables you to review configuration settings quickly. Double-click an item on the tab to display the item's configuration panel and change a setting.

Console View

The console view for an active virtual machine is like the monitor display of a physical computer.

Figure 3-3. Console View on a Windows Host

Console View button



To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

When a virtual machine is active, the name of the virtual machine or team of virtual machines appears in a tab at the top of the console. To switch from the active virtual machine or team, click the tab of another virtual machine or team. You can use the console tabs in the window mode and also in the quick switch mode.

Appliance View

If you set up the virtual machine to act as an appliance, such as a Web server with a browser-based console, you can specify that the default view is an appliance view. The appliance view gives a brief description of the type of server or appliance. It also provides a link that opens the browser on the host system and connects to the appliance's management console.

The appliance view is available only for virtual machines that you designate as appliances. See "Configure the Appliance View for a Virtual Machine" on page 170.

Displaying Multiple Virtual Machines at the Same Time

To simultaneously view more than one virtual machine when they are not all on the same team, open multiple Workstation windows and launch one or more virtual machines in each Workstation window.

Use a team of virtual machines to coordinate and use multiple virtual machines within a single console window. See "Summary and Console Views for Teams and Their Virtual Machines" on page 256.

Toolbar Buttons

The toolbar area at the top of the VMware Workstation window contains buttons you can click to power virtual machines on and off, change the Workstation display, manage snapshots, and record virtual machine activity.

Figure 3-4. Workstation Toolbars

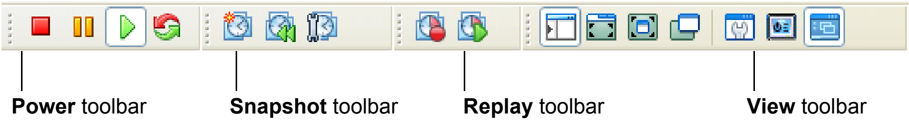
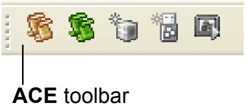


Figure 3-5. ACE Toolbar (Windows Hosts Only)



If you point to a toolbar button, a tooltip appears and displays the name of the button. To change which buttons appear, see "Customize the Toolbar on a Windows Host" on page 60 and "Customize the Toolbar on a Linux Host" on page 59.

The **Power** toolbar contains the following buttons:

- **Power Off** – Turns off the active virtual machine or team like the power button on a physical PC. You can configure Workstation for a soft power off (called shut down) or a hard power off (called power off). See "Shut Down a Virtual Machine" on page 149 or "Power Off or Close a Team" on page 255.
- **Suspend** – Stops a virtual machine or team in a manner that allows you to resume your work later. See "Using the Suspend and Resume Features" on page 187.

- **Power On** or **Resume** – Powers on a selected virtual machine or team that is powered off, or resumes a virtual machine or team that is suspended. See “Starting a Virtual Machine” on page 145, “Power On a Team” on page 259, and “Using the Suspend and Resume Features” on page 187.
- **Reset** – Resets a virtual machine or team like the reset button on a physical PC. See “Configure Power Off and Reset Options for a Virtual Machine” on page 149.

The **Snapshot** toolbar contains the following buttons:

- **Take Snapshot** – Enables you to save the state of a virtual machine in the same manner you might save a word-processing document. You can return to that state if you make a mistake by using the **Revert** button. See “Using Snapshots” on page 189.
- **Revert** – Allows you to return a virtual machine to the parent state, a state previously preserved by taking a snapshot. See “Using Snapshots” on page 189.
- **Manage Snapshots** – Opens the snapshot manager, where you can view the virtual machine’s existing snapshots, revert to a snapshot, take a new snapshot, and make a clone from a snapshot. See “Snapshot Manager Overview” on page 194.

The **View** toolbar contains the following buttons:

- **Show or Hide Sidebar** – Toggles between showing and hiding the sidebar. See “View the Sidebar” on page 60.
- **Quick Switch** – Enlarges the Workstation console to cover the entire host monitor. Console tabs enable you to switch between virtual machines and teams with a single click. See “Use Quick Switch Mode” on page 157.
- **Full Screen** – Enlarges the virtual machine display to cover the entire host monitor. The virtual machine no longer appears in a window. See “Use Full Screen Mode” on page 154.
- **Unity** – Integrates your favorite guest applications with your host’s desktop so that guest application windows look just like host application windows, but with color-coded borders. See “Using Unity Mode” on page 151.
- **Summary View** – Displays the summary view. See “Summary View” on page 54.
- **Appliance View** – Displays the appliance view. See “Appliance View” on page 56.
- **Console View** – Displays the console view. See “Console View” on page 56.

The **Replay** toolbar contains the following buttons:

- **Replay Last Recording** – Plays the last recording made for this virtual machine.
- **Record** – Begins recording the activity of this virtual machine.

  For information about the record/replay feature, see Chapter 12, "Recording and Replaying Virtual Machine Activity," on page 239.

The **ACE** toolbar, which is available on Windows hosts only, contains the following buttons:

- **Edit Policies** – Opens the policy editor.
- **Edit Deployment Settings** – Opens the deployment settings editor.
- **Create New Package** – Opens the New Package wizard.
- **Create Pocket ACE Package** – Opens the Pocket ACE Package wizard.
- **Preview in Player** – Allows you to run an ACE instance as it will run on the user's machine. Using preview mode also allows you to view the effects of changed policies as they will appear on the user's machine.

See Chapter 18, "Learning the Basics of VMware ACE," on page 365.

Customize the Toolbar on a Linux Host

You can customize the Workstation toolbar by adding, removing, and rearranging toolbar buttons. On a Linux host, all the buttons are contained in a single toolbar.

To customize the toolbar on a Linux host

1. Right-click the far-right side of the toolbar to display a **Toolbar** menu.
2. Click **Power**, **Snapshot**, **View**, or **Replay** to add or remove that toolbar.

   When a toolbar name is checked, the corresponding buttons appear in the interface.
3. In the Desktop Style part of the menu, choose the display style for toolbar buttons.

Customize the Toolbar on a Windows Host

You can customize the Workstation toolbar by adding, removing, and rearranging toolbar buttons.

To customize the toolbar on a Windows host

1. Right-click any part of the toolbar to display a **Toolbar** menu.
2. Click **Power**, **Snapshot**, **ACE**, **View**, or **Replay** to add or remove that toolbar.

   When a toolbar is checked, it appears in the interface.

   To change which buttons appear in a toolbar or the order in which they appear, display that toolbar and continue with the following steps.
3. Right-click the **Power**, **Snapshot**, **ACE**, **View**, or **Replay** toolbar to open the Customize Toolbar dialog box.

   Buttons listed under **Current Toolbar Buttons** appear in the toolbar, in the order shown in the Customize Toolbars dialog box.
4. Do any of the following:

   - To add or remove a button from the toolbar, select the button and click **Add** or **Remove**. Add a separator to display a vertical line between the buttons.
   - To change the order of the buttons, select any button under **Current Toolbar Buttons** and click **Move Up** or **Move Down**.
   - To change the order of the currently displayed buttons without opening the Customize Toolbar window, hold down the Shift key while you drag a button to a different location in the toolbar.
   - To restore the default setup, with all buttons displayed, click **Reset**.
5. Click **Close**.

View the Sidebar

The sidebar contains a list of favorites and shows which virtual machines or teams of virtual machines are currently powered on. On Windows hosts, an additional section of the sidebar displays ACE Management Servers. For more information, see the *VMware ACE Management Server Administrator's Manual*.

To view the Sidebar

Choose **View > Sidebar**.

If the sidebar was hidden, it becomes visible. If it was visible, it is hidden.

Favorites List in the Sidebar

The **Favorites** list lets you organize and access frequently used items.

The **Favorites** list provides the following benefits:

- **Fast access** – Quickly access frequently used items. With your virtual machines and teams on the **Favorites** list, you can open them without browsing the host file system. Also like browser bookmarks, **Favorites** list icons can be organized in folders, added, rearranged, or deleted.

- **Status** – Different icons indicate the status of virtual machines and teams. A **Favorites** list icon indicates whether the team or virtual machine is powered off, powered on, or suspended. A brown (rather than blue) virtual machine icon indicates that the virtual machine is a Workstation 4 virtual machine.

	Powered off Workstation 5 or 6.x virtual machine or full clone. To determine the exact version, use the summary view's **Version** field.
	Powered off virtual machine created as a linked clone of another virtual machine.
	Powered off team of virtual machines.
	Powered off Workstation 4 virtual machine.
	Powered on indicator can appear for virtual machines and teams.
	Suspended indicator can appear for virtual machines and teams.
	Unavailable indicator can appear if a virtual machine or team gets corrupted or moved from the location that was used to create the favorites item. The indicator also appears if the virtual machine is already open in VMware Player or is opened by another user.

- **Right-click commands** – Right-click on a **Favorites** icon to display a menu of commands you can use for that virtual machine or team. You can click elsewhere in the **Favorites** list (that is, not on a virtual machine or team) to display a context menu from which you can choose to create a new virtual machine, team, or folder. You can also open an existing virtual machine, team, Microsoft Virtual PC or Virtual Server virtual machine, StorageCraft, or Symantec Backup Exec System Recovery system image.

Use Folders for Organizing Favorites

You can organize favorites into folders and nest folders inside other folders.

To use folders for organizing favorites

1 Right-click **Favorites** (or any item in the **Favorites** list), and choose **New Folder**.

2 Complete the New Folder dialog box that appears.

3 (Optional) Drag and drop folders to place one inside another.

4 Drag and drop Favorites items in the desired folder.

Add Virtual Machines and Teams to the Favorites List

Virtual machines and teams are automatically added to the **Favorites** list when you complete the New Virtual Machine wizard. You can also add them manually.

To add virtual machines and teams to the Favorites list

1 Choose **File > Open** and browse to the location of the virtual machine (`.vmx` file) or team (`.vmtm` file).

2 Click **Open**.

3 Choose **File > Add to Favorites**.

Remove an Item from the Favorites List

You can remove the name of a virtual machine or team from the **Favorites** list regardless of whether the virtual machine or team is open or powered on. Removing the name does not affect the virtual machine's files or operation.

To remove an item from the Favorites list

1 Click a name in the **Favorites** list to select it.

2 Choose **File > Remove from Favorites**.

Rename an Item in the Favorites List

Renaming an item in the **Favorites** list also renames the virtual machine or team.

To rename a Favorite list entry for a virtual machine or a team

1 Right-click the **Favorites** item to rename.

2 Choose **Rename** from the context menu.

3 Type the new name for the item and press Enter.

Powered On List

This list in the sidebar enables you to find out which virtual machines or teams are currently powered on. Right-click items in the **Powered On** list to display a menu of commands you can use for that virtual machine or team.

Check for Product Updates

Workstation automatically checks for product updates every three days. If an update check fails on two consecutive attempts, you receive a notification.

NOTE Checking for product updates works only if the host computer is connected to the Internet.

To check for product updates

1 (Optional) To check for updates immediately, choose **Help > Check for Updates on the Web**.

2 To configure Workstation to periodically check for updates, choose **Edit > Preferences > Workspace**.

3 In the **Software Updates** section, select the check box called **Check for software updates** and click **OK**.

Quickly Create a Virtual Machine

The instructions in this section get you started quickly with creating a virtual machine and installing a guest operating system. After you create a virtual machine, you will find the information in the rest of this chapter easier to understand.

The instructions tell you to accept the default settings so that you can complete the New Virtual Machine wizard quickly. The purpose is to learn about Workstation. Later, when you want to create virtual machines that you actually use in your work or production environment, you can learn about all the options available. This information is provided in Chapter 4, "Creating and Upgrading a Virtual Machine," on page 77.

For simplicity, use a Windows installation CD or ISO image file for the operating system you install in the virtual machine. Most Windows operating systems fit on one CD, whereas Linux requires multiple CDs. If you want to use a Linux guest operating system, use installation media for one of the newer versions of Red Hat, SUSE Linux, or Ubuntu. The easy install feature is supported for these operating systems.

To quickly create a virtual machine

1. To use an installation CD or DVD for the operating system, rather than an ISO image file, insert the CD or DVD in the host CD-ROM drive.
2. Start VMware Workstation.

   For instructions, see "Start Workstation on a Windows Host" on page 51 or "Start Workstation on a Linux Host" on page 52.
3. Choose **File > New > Virtual Machine**.
4. On the Welcome page, select **Typical** and click **Next**.
5. On the Guest Operating system Installation page, select **Installer disc** or **Installer disc image file**, as appropriate, and click **Next**.
6. Complete the fields on the Easy Install Information page.

   Specifying a password is optional. On Windows, the password you enter here is used for an account with Administrator permissions. On Windows 2000, the password is used for the Administrator account.
7. Accept the defaults on the rest of the wizard pages.

   The virtual machine is created and its name is added to the **Favorites** list.

The console view for the virtual machine appears. Soon the boot device (such as the CD-ROM) is detected and installation of the operating system begins.

On Windows 2000 guests, if you entered a password when completing the New Virtual Machine wizard, then when the operating system starts up, it might prompt you to enter an Administrator password. Use the password that you created when completing the New Virtual Machine wizard.

After installation is finished, VMware Tools is automatically installed.

Now that you have a virtual machine with a guest operating system installed, you can refer to it as you read the rest of the topics in this chapter.

Introduction to Workstation Preferences

The Preferences dialog box appears when you choose **Edit > Preferences**. It lets you change a number of settings that apply to Workstation itself, no matter which virtual machine you are running.

The default settings for Workstation preferences are correct for most cases. Do not change settings unless you are an experienced user.

NOTE On a Linux host, you must be logged in as root to save global preference changes.

Following is a list of the tabs in the Preferences dialog box, along with cross-references to the sections of this manual that pertain to each tab:

- **Workspace** tab – Lets you configure the following settings:
  - **Location** section – Lets you change the directory in which newly created virtual machines are stored. See "Virtual Machine Location" on page 81 and "Files That Make Up a Virtual Machine" on page 93.
  - **Virtual Machines** section – Several of these options have to do with exiting Workstation while leaving some virtual machines powered on. See "Closing Virtual Machines and Exiting Workstation" on page 69. For information about enabling shared folders, see "Set Up Shared Folders" on page 178.
  - **Software Updates** section – See "Check for Product Updates" on page 63.
- **Input** tab – Lets you adjust the way the virtual machine captures control of keyboard and mouse. For example, by default the virtual machine grabs keyboard and mouse input when you click in the virtual machine window.
- **Hot Keys** tab – Lets you specify the key combination that is used with hot-key sequences for all your virtual machines. Use hot-key combinations to enter and leave full screen mode, ungrab mouse and keyboard input, and so on. See "Keyboard Shortcuts" on page 70.
- **Display** tab – Lets you adjust the manner in which the console and the host display accommodate a different guest operating system display resolution.

  Also see "Fitting the Workstation Console to the Virtual Machine Display" on page 162 and "Use Full Screen Mode" on page 154.
- **Memory** tab – For details on adjusting memory settings in Workstation, click **Help** on this tab. On Linux, you must be running Workstation as root in order to change these settings.

- **Priority** tab – For information about the snapshot settings on this tab, see "Enable or Disable Background Snapshots" on page 193. On Linux, you must be running Workstation as root in order to change this setting.

  For information about the process priority settings available on Windows hosts, click **Help** on this tab.

- **Lockout** tab – (Windows hosts only) 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 351.

- **Tools** tab – Lets you specify whether to automatically update VMware Tools on Windows and Linux guest systems when a new version becomes available. On Linux hosts, you must be running Workstation as root in order to change these settings.

  VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine. See Chapter 5, "Installing and Using VMware Tools," on page 97.

- **Devices** tab – (Windows hosts only) By default, the autorun feature mentioned on this tab is disabled. Therefore, you need to manually connect to the CD-ROM drive by using the **VM > Removable Devices** menu. See "Use Removable Devices in a Virtual Machine" on page 169.

In addition to the cross-references mentioned in this list, more information about the settings on each tab is available in the Workstation online help. Click **Help** in the Preferences dialog box.

The settings on the following tabs apply only to the user currently logged on to the host computer: **Workspace** tab, **Input** tab, **Hot Keys** tab, **Priority** tab, and **Tools** tab.

The settings on the following tabs apply no matter which virtual machine is running or which user is logged on to the host computer: **Display** tab, **Memory** tab, **Lockout** tab, and **Devices** tab.

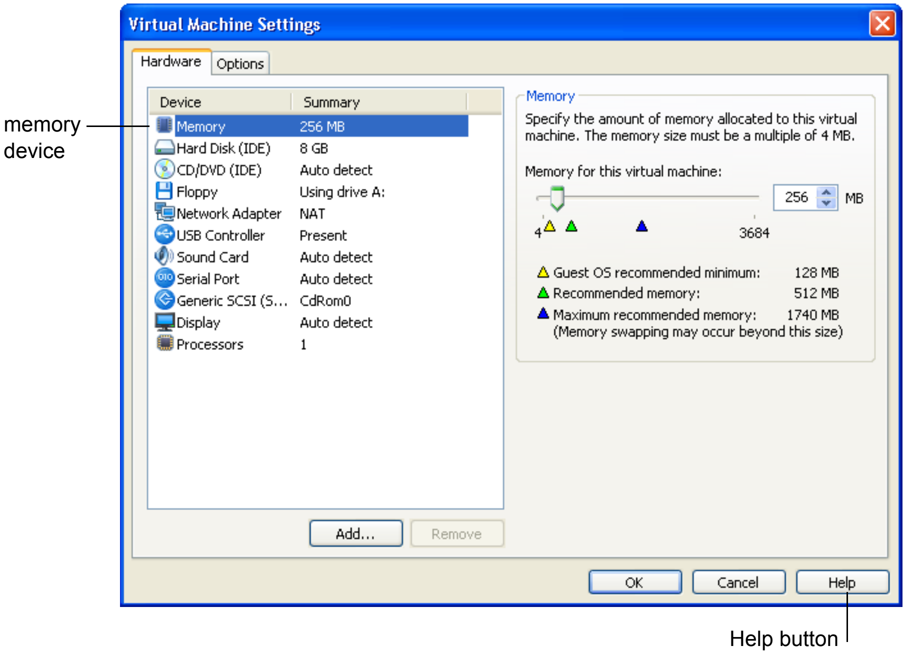
Introduction to Virtual Machine Settings

Workstation configures a new virtual machine based on the guest operating system you select in the New Virtual Machine wizard. After the virtual machine is created, you can use the virtual machine settings editor to change many configuration options set by the wizard. The virtual machine settings editor appears when you select a virtual machine and choose **VM > Settings**.

Hardware Tab

Use the **Hardware** tab to add, remove, and configure virtual devices for the selected virtual machine.

Figure 3-6. Virtual Machine Settings Hardware Tab



Device	Summary
Memory	256 MB
Hard Disk (IDE)	8 GB
CD/DVD (IDE)	Auto detect
Floppy	Using drive A:
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Serial Port	Auto detect
Generic SCSI (S...	CdRom0
Display	Auto detect
Processors	1

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 256 MB

4 ... 3684

Guest OS recommended minimum:	128 MB
Recommended memory:	512 MB
Maximum recommended memory: (Memory swapping may occur beyond this size)	1740 MB

When you select an item in the hardware list, the options that correspond to the item appear on the right side of the dialog box. For example, in Figure 3-6, memory options appear because the **Memory** item is selected.

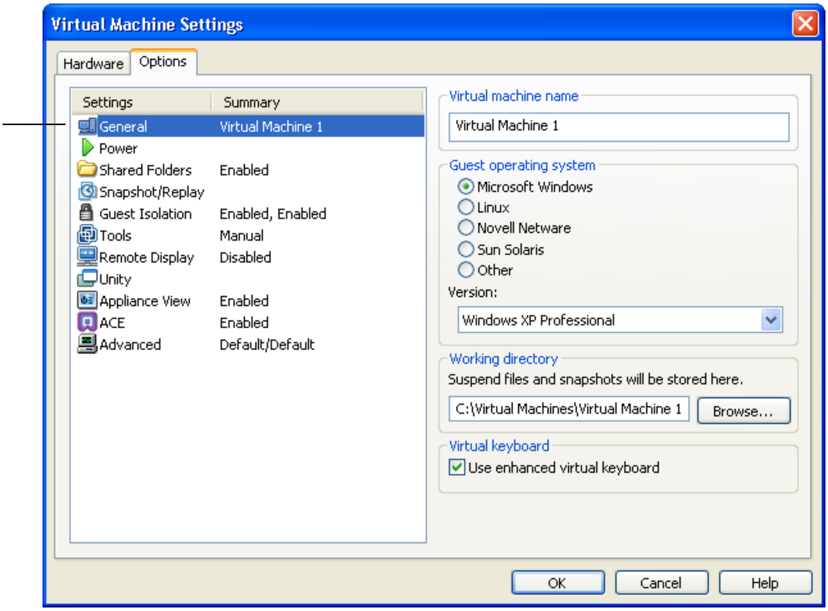
Topics and chapters related to each of the virtual devices in the **Hardware** list are provided later in this manual. To display online help for an item you select in the **Hardware** list, click **Help**.

Options Tab

The **Options** tab lets you adjust characteristics of the selected virtual machine:

- Many options control interactions between the host and the guest operating system, such as how folders can be shared, how files are transferred, and what happens to a guest operating system when you exit Workstation.
- Some options let you override similar Preferences dialog box options, which are global preferences set for all virtual machines. For example, you can use the **Advanced** option to override the process priorities set on the **Priority** tab in the Preferences dialog box.
- Some options let you change settings you might initially make when running the New Virtual Machine wizard to create a virtual machine. For example, you can use the **General** options to change the name of the virtual machine.

Figure 3-7. Virtual Machine Settings Options Tab



General options

Settings	Summary
General	Virtual Machine 1
Power	
Shared Folders	Enabled
Snapshot/Replay	
Guest Isolation	Enabled, Enabled
Tools	Manual
Remote Display	Disabled
Unity	
Appliance View	Enabled
ACE	Enabled
Advanced	Default/Default

Virtual machine name: Virtual Machine 1

Guest operating system
● Microsoft Windows
○ Linux
○ Novell Netware
○ Sun Solaris
○ Other
Version: Windows XP Professional

Working directory
Suspend files and snapshots will be stored here.
C:\Virtual Machines\Virtual Machine 1

Virtual keyboard
☑ Use enhanced virtual keyboard

The settings for the virtual machine **Options** tab are discussed later in this manual, in the task-specific topics and procedures where you would use them. To display online help for an item you select in the **Options** list, click **Help**.

Closing Virtual Machines and Exiting Workstation

When you close a virtual machine or team, and when you exit Workstation, if any virtual machines are still powered on, you are prompted to specify one of the following actions to take:

- Continue running the virtual machine in the background. If a virtual machine continues running after you exit Workstation, you can still interact with it through virtual network computing (VNC) or some other service.
- Suspend the virtual machine. The suspend operation saves the state of the virtual machine. See "Using the Suspend and Resume Features" on page 187.
- Power the virtual machine off. If you configured the power operation to do a "soft" power-off, a VMware Tools script runs in order to cleanly shut down the guest operating system before powering off. See "Configure Power Off and Reset Options for a Virtual Machine" on page 149.

To avoid receiving a prompt every time you exit Workstation or close a virtual machine or team, set a preference for virtual machines to always run in the background when you exit.

Set a Virtual Machine to Run in the Background

You can set a virtual machine that is powered on to continue running in the background when you close a virtual machine or team tab, or when you exit Workstation. You can still interact with it through VNC or another service.

By default, when virtual machines run in the background, a status icon appears in the notification area of the taskbar. Point to the icon to display a a tooltip that shows the number of virtual machines and teams that are running in the background. These are the virtual machines and teams that belong to the user who is logged in.

To set a virtual machine to run in the background

Do one of the following:

- Click **Run in Background** at the prompt when you close the virtual machine or exit Workstation.
- Set a Workstation preference:

  a From the VMware Workstation menu bar, choose **Edit > Preferences**.

  b On the **Workspace** tab, select **Keep VMs running after Workstation closes** and click **OK**.

  When you close a tab or exit Workstation, you no longer receive a prompt.

Keyboard Shortcuts

You can use keyboard shortcuts to interact with Workstation and with virtual machines. Most of the available keyboard shortcuts for Workstation are listed next to their associated commands in Workstation menus.

Hot keys, or keyboard shortcuts for interactions with virtual machines, are shown in Table 3-1. Hot-key combinations can be used to do the following:

- Switch between virtual machines
- Enter and leave full screen mode
- Ungrab input
- Send Ctrl+Alt+Del to the virtual machine only (and not to the host)
- Send commands to the virtual machine only (and not to the host)

By default, most hot-key combinations include Ctrl+Alt, but you can change this combination. See "Change the Hot-Key Combination" on page 71.

If you change the Preferences setting for the hot-key combination, substitute your new setting for Ctrl+Alt as needed in the shortcuts listed in Table 3-1. For example, if you change the hot-key combination to Ctrl+Shift+Alt, you must press Ctrl+Shift+Alt+spacebar to have Workstation not process a command.

Table 3-1. Hot-Key Combinations

Shortcut	Action
Ctrl+G	Grab input from keyboard and mouse.
Ctrl+Alt	Release the mouse cursor. If the virtual machine is in the type of full screen mode called exclusive mode, pressing Ctrl+Alt changes the virtual machine from exclusive mode to full screen mode.
Ctrl+Alt+Insert	Shuts down or (depending upon the guest operating system) logs out of the guest. This command is received solely by the virtual machine. **Note:** For this and all shortcuts that include Ctrl+Alt, changing the hot-key combination changes the sequence you need to use. For instance, if you change the hot-key combination to Ctrl+Shift+Alt, you must press Ctrl+Shift+Alt+Insert to end the guest operating system session.
Ctrl+Alt+Delete	Shuts down or (depending upon the operating system) logs out of the guest operating system. On Windows hosts, if you are not using the enhanced virtual keyboard feature, this command is received by both the host operating system and the virtual machine, even when Workstation has control of input. You can cancel the ending of the host operating system's session and return to the virtual machine to log out or shut down or perform administrative tasks.

Table 3-1. Hot-Key Combinations (Continued)

Shortcut	Action
Ctrl+Alt+spacebar	Sends any command into the virtual machine so that Workstation does not process it. Hold down Ctrl+Alt as you press and release the spacebar, and continue to hold the Ctrl+Alt keys down as you press the next key in the combination.
Ctrl+Alt+Tab	Switch among open virtual machines while mouse and keyboard input are grabbed.
Ctrl+Tab Ctrl+Shift+Tab	On Windows hosts, switch among open virtual machines while mouse and keyboard input are not grabbed. Workstation must be the active application.
Ctrl+Alt+right arrow	In full screen mode, switch to the next powered-on virtual machine.
Ctrl+Alt+left arrow	In full screen mode, switch to the previous powered-on virtual machine.

Change the Hot-Key Combination

Hot-key combinations, or shortcut keys, are key combinations you press to interact with virtual machines. For a list of actions you can invoke by using hot keys, see Table 3-1.

By default, most hot-key combinations include Ctrl+Alt, but you can change this combination. For example, you can change the setting so that all hot-key combinations use Ctrl+Shift+Alt. This is useful if you want to prevent certain key combinations (such as Ctrl+Alt+Del) from being intercepted by Workstation instead of being sent to the guest operating system.

The hot-key preferences you set in the preferences editor apply to virtual machines you access from within Workstation. These settings do not affect virtual machines or ACE instances distributed to other users.

To change the hot-key combination

1 Choose **Edit > Preferences**.

2 Click the **Hot Keys** tab.

3 Use the following information to help you choose a key combination:

   Custom key combinations involve using a combination of the Ctrl, Shift, Alt, and Windows keys. The Windows key is the key between the Ctrl and Alt keys on your keyboard. The modifiers for the custom combination are:

   - **Down** – The key must be pressed to use the hot-key sequence.
   - **Up** – The key must not be pressed to use the hot-key sequence.
   - **Either** – The key can be up or down. This modifier is useful to allow users a variety of keystrokes to leave full screen mode. For example, selecting **Either** for the Shift key means that both Ctrl+Alt+Enter and Ctrl+Shift+Alt+Enter cause Workstation to leave full screen mode.

   If you select **Either** for all of the keys (Ctrl, Alt, Shift, and Win) in the custom combination, you can use the Esc key to release the cursor.

4 Click **OK**.

Gathering Information for VMware Technical Support

When you need help from VMware technical support, VMware recommends that you create a support request. For some problems, the representative will ask you to turn on debugging, run a script to collect log files, and send the logs to VMware.

Register and Create a Support Request

Before you can report problems to the VMware support team, you must register for a VMware account.

Before you begin, locate the serial number. It is on the registration card in your package. If you purchased Workstation online, the serial number is sent by email.

To register and create a support request

1 From the Workstation menu bar, choose **Help > VMware on the Web > Register Now!**

2 Follow the instructions on the Web site.

3 To report problems, from the Workstation menu bar, choose **Help > VMware on the Web > Request Support**.

Gather Debugging Information for a Virtual Machine

Workstation provides several levels of logging to help diagnose and troubleshoot various types of problems.

You can use full debugging mode to gather the greatest amount of data, which is useful when a virtual machine freezes or powers off unexpectedly. You can use statistics mode to gather performance statistics when virtual machines run slowly. You can also increase logging without going into full debugging mode. A VMware technical support representative can tell you which level to use.

After you gather debugging information, you can send the log files to VMware technical support.

To gather debugging information for a virtual machine

1. Select the virtual machine.
2. Make sure the virtual machine is powered off or suspended.
3. Choose **VM > Settings**.
4. On the **Options** tab, select **Advanced**.
5. Select from the **Gather debugging information** drop-down menu or the **Log virtual machine progress periodically** check box, as directed by VMware technical support.

   Using full debugging mode and logging progress periodically cause a decrease in performance.
6. In the **File locations** section, note the directory path to the log file.

   To view the complete path, click in the read-only text box and use the right arrow key to scroll through the path.
7. Click **OK**.

Running the Support Script

To help diagnose a problem, the VMware support team might ask you to run a support script in order to gather information. For example, if a virtual machine exits abnormally or crashes, run the support script to collect the appropriate log files and system information.

As of Workstation 6.0.1, you can run the support script by clicking a button in the **Help > About VMware Workstation** box. You can also, as in previous releases, run the script from the command line.

Run the Support Script from the Workstation User Interface

Run this script only when requested to do so by VMware technical support.

Before you begin, create a support request. See "Register and Create a Support Request" on page 72. Increase the level of logging, as described in "Gather Debugging Information for a Virtual Machine" on page 73.

To run the support script from the Workstation user interface

1 Choose **Help > About VMware Workstation**.

2 Click **Collect Support Data**.

3 In the confirmation box that appears, confirm that you want to collect support data.

   On Windows hosts, after the script finishes running, it creates a `.zip` file and displays the path to the file.

   On Linux hosts, the script creates a compressed `.tgz` file in the user's home directory. Because the script is not run as root, the script displays messages indicating that it cannot collect some information. This is normal. If the VMware support team needs that information, a support representative will ask you to run the script from the command line as root. For instructions, see "Run the Support Script from a Linux Terminal Window" on page 75.

4 Add this data file to your support request.

Run the Support Script from a Windows Command Prompt

Run this script only when requested to do so by VMware technical support.

Before you begin, create a support request. See "Register and Create a Support Request" on page 72. Increase the level of logging, as described in "Gather Debugging Information for a Virtual Machine" on page 73.

To run the support script from a Windows command prompt

1 Open a command prompt.

2 Change to the VMware Workstation program directory:

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

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

3 Run the support script:

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

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

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

If you are reporting a problem you encountered while installing VMware Workstation, also include the installation log file.

On a Windows host, the file is `VMInst.log`. It is saved in the `Temp` folder. On a Windows 2000, Windows XP, or Windows Server 2003 host, the default location is `C:\Documents and Settings\<username>\Local Settings\Temp`.

You can use the command `cd %temp%` to locate the `Local Settings` folder, which 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**.

Run the Support Script from a Linux Terminal Window

Run this script only when requested to do so by VMware technical support.

Before you begin, create a support request. See "Register and Create a Support Request" on page 72. Increase the level of logging, as described in "Gather Debugging Information for a Virtual Machine" on page 73.

To run the support script from a Linux terminal window

1 Open a terminal window.

2 Run the support script as the user who is running the virtual machine:

```
vm-support
```

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

The script creates a compressed `.tgz` file in the user's home directory.

3 Include that output file with your support request.

If you are reporting a problem you encountered while installing Workstation, also include the installation log file.

Creating and Upgrading a Virtual Machine

4

This chapter describes how to create a virtual machine by using the New Virtual Machine wizard. It also provides general information about installing guest operating systems.

This chapter includes the following topics:

Methods of Creating Virtual Machines

Workstation gives you several options for creating virtual machines:

- Create a virtual machine from scratch.

  If you do not have any virtual machines or system images, you must use this method. Use the New Virtual Machine wizard to create a virtual machine. Next, you must install an operating system. The process is the same as installing it on a physical computer.

  The rest of this chapter describes this method of creating a virtual machine.

- Clone a virtual machine from an existing VMware virtual machine or virtual machine template.

  Clones are useful when you must deploy many identical virtual machines to a group. Cloning is preferable to copying a virtual machine because a clone's MAC address and UUID are different from the original virtual machine, to avoid network conflicts. Use the Clone Virtual Machine wizard to create a clone.

  See "Cloning a Virtual Machine" on page 203.

- On Windows hosts, convert a physical machine, virtual machine, or system image that was created by using another VMware product or a third-party product.

  This process creates a clone of the original virtual machine or system image. Use the Conversion wizard to convert a physical or virtual machine or a system image.

  See Chapter 6, "Creating a Virtual Machine from a System Image or Another Virtual Machine," on page 131.

Configuration Options for the New Virtual Machine Wizard

As you complete the New Virtual Machine wizard, you are prompted to make decisions about many aspects of the virtual machine. The topics in this section provide information about the issues involved so that you can determine which choices you want to make before running the wizard.

Easy Install Feature for Some Guest Operating Systems

The easy install features enable you to perform an unattended installation of the guest operating system after you complete the New Virtual Machine wizard. You can use this feature regardless of whether you choose a typical or a custom configuration in the wizard.

If you specify an installer disc or image (`.iso`) file and if the wizard detects an operating system that supports the easy install feature, you are prompted to supply the following information:

- For Windows guests:
  - (Optional) **Windows product key** – If you specify a product key, you are not prompted for it later, during installation of the operating system. Enter a product key unless the installation media already contains a volume license product key.
  - **Full name** – This name is used for registering the operating system. Do not use the name Administrator or Guest. If you use one of these names, you will receive an error message during installation of the operating system and be prompted to enter a different name.
  - (Optional) **Password** – On Windows operating systems other than Windows 2000, the password you enter here is used for an account with Administrator permissions. On Windows 2000, the password you enter here is used for the Administrator account.
- For Linux guests:
  - **Full name** – This name is used for registering the operating system, if registration is required. The first name is used as the host name for the virtual machine.
  - **User name** – You can use lowercase letters and numbers, with no spaces. Do not use the name root. Some operating systems set up sudo access for this user, and some require this user to use `su` to get root privileges.
  - **Password** – The password you enter here is used for both the user name you supply and the root user.

The easy install feature is available for newer Windows operating systems and several Linux operating systems. The installation media that you can use include operating system installation CDs, DVDs, and ISO images.

This feature also installs VMware Tools in the guest operating system. For more information about VMware Tools, see "Components of VMware Tools" on page 97.

If you plan to use a CD, DVD, or ISO image that contains a product key number and is already set up to perform an unattended installation, the only benefit you gain by using the easy install feature is the automatic installation of VMware Tools.

Typical Compared to Custom Configurations

The New Virtual Machine wizard prompts you to choose between doing a typical configuration and a custom configuration. If you select **Typical**, the wizard prompts you to specify or accept defaults for the following choices:

- Medium for installing the guest operating system (CD, image file, or neither)
- Guest operating system
- Virtual machine name and the location of the virtual machine files
- Size of the virtual disk and whether to split the disk into 2GB files
- Hardware customization, for advanced users

You are not prompted to specify the virtual machine version. The virtual machine version (Workstation 4, 5, 6, or 6.5) is assumed to be the one specified in the preferences editor. From the Workstation menu bar, choose **Edit > Preferences**, and see the setting for **Default hardware compatibility**.

On the last page of the wizard, you can click **Customize Hardware** to change the defaults for memory allocation, number of virtual CPUs, network connection type, and so on.

Many circumstances require you to select a custom installation. Select **Custom** if you want to do any of the following:

- Make a different version of virtual machine than what is specified in the preferences editor.
- Specify the I/O adapter type for SCSI adapters: BusLogic, LSI Logic, or LSI Logic SAS.
- Specify whether you want to create an IDE or a SCSI virtual disk, regardless of the default that is usually used for the guest operating system.
- Use a physical disk rather than a virtual disk (for expert users).
- Use an existing virtual disk rather than create a virtual disk.
- Place the virtual disk file in a location other than the virtual machine directory.
- Allocate all virtual disk space rather than allowing the disk space to gradually grow to the maximum.

Guest Operating System Selection

If you specify that the source media for installing the operating system is **Installer disc** or **Installer disc image file** and if the wizard can detect the operating system, you might not see a wizard page for selecting the operating system.

After you specify an operating system or after the wizard detects it from the installation media, Workstation uses this information to do the following:

- Select appropriate default values, such as the amount of memory to allocate.
- Name files associated with the virtual machine.
- Adjust settings for optimal performance.
- Work around special behaviors and bugs within a guest operating system.

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

For some operating systems, the operating system and VMware Tools are installed automatically after the virtual machine is created. See "Easy Install Feature for Some Guest Operating Systems" on page 78.

NOTE Workstation supports 64-bit guest operating systems only in Workstation versions 5.5 and later, and only on host machines with supported processors. For the list of processors Workstation supports for 64-bit guest operating systems, see "PC Hardware" on page 23.

Virtual Machine Location

The following examples show the default locations suggested for virtual machines:

- On Windows 2000, Windows XP, and Windows Server 2003 hosts, the default folder for a Windows XP Professional virtual machine is:

  ```
  C:\Documents and Settings\<username>\My Documents\My Virtual
  Machines\Windows XP Professional
  ```

- On Windows Vista hosts, the default folder is:

  ```
  C:\Users\<username>\Documents\Virtual Machines\Windows XP Professional
  ```

- On Linux hosts, the default location for a Windows XP Professional virtual machine is:

  ```
  <homedir>/vmware/Windows XP Professional
  ```

  The `<homedir>` value is the home directory of the user who is currently logged in.

Virtual machine performance might be slower if your virtual hard disk is on a network drive. For best performance, be sure the virtual machine's folder is on a local drive. However, if other users need to access this virtual machine, consider placing the virtual machine files in a location that is accessible to them. See "Sharing Virtual Machines with Other Users" on page 211.

NOTE If you plan to deploy the virtual machine on a USB drive, first, create the virtual machine on your local hard disk. You can then use Pocket ACE features to deploy the virtual machine.

For information about the files stored in the virtual machine folder, see "Files That Make Up a Virtual Machine" on page 93.

Virtual Hardware Compatibility Levels

This option is available for custom configurations only.

When you make a selection from the **Hardware Compatibility** list, you see a list of other VMware products and versions that are compatible with your selection. You also see a list of features that are not available for that version.

If one of the feature compatibility check boxes is available for the version you select, you can select the check box to see a list of the additional limitations.

Number of Processors

This option is available for custom configurations only. Setting the virtual machine to have two processors is supported only for host machines with at least two logical processors. (If you are creating a Workstation 4 virtual machine, you do not see this panel.)

The following are all considered to have two logical processors:

- A single-processor host with hyperthreading enabled
- A single-processor host with a dual-core CPU
- A multiprocessor host with two CPUs, regardless of whether they are dual-core or have hyperthreading enabled

Memory Allocation

This option is available for custom configurations or if you click **Customize Hardware** on the last page of the New Virtual Machine wizard.

A color-coded icon corresponds to each value. To use one of these amounts, move the slider to the corresponding icon. The high end of the range that appears is determined by the amount of memory allocated to all running virtual machines. If you allow virtual machine memory to be swapped, this value changes to reflect the amount of swapping that was specified. To change the amount of memory available to all virtual machines, use the Workstation preferences editor (**Edit > Preferences**).

Network Connection Type

This option is available for custom configurations or if you click **Customize Hardware** on the last page of the New Virtual Machine wizard. You have several options for connecting the virtual machine to the network:

- **Bridged networking** – 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**. Other computers on the network can then communicate directly with the virtual machine.

- **NAT** – 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)**. The virtual machine and the host share a single network identity that is not visible outside the network.

- **Host-only** – Host-only networking provides a network connection between the virtual machine and the host computer, using a virtual network adapter that is visible to the host operating system. With host-only networking, the virtual machine can communicate only with the host and other virtual machines in the host-only network. Use this approach to set up an isolated virtual network.

- **No connection** – You can always set up a connection after you finish creating the virtual machine.

See “Common Networking Configurations” on page 266.

SCSI Adapter Types and Disk Types

This option is available for custom configurations only. An IDE and a SCSI adapter are installed in the virtual machine. The IDE adapter is always ATAPI. For the SCSI adapter, you can choose BusLogic, LSI Logic, or LSI Logic SAS. BusLogic and LSI Logic adapters have parallel interfaces. LSI Logic SAS has a serial interface.

The default for your guest operating system is already selected. Older operating systems, such as Windows XP and Red Hat Enterprise Linux 2, default to BusLogic. Only Windows Server 2008 defaults to LSI Logic SAS.

NOTE The LSI Logic adapter has improved performance and works better with generic SCSI devices. The LSI Logic adapter is also supported by ESX Server 2.0 and higher.

Your choice of SCSI adapter does not affect your decision to make your virtual disk an IDE or SCSI disk. However, some guest operating systems, such as 32-bit Windows XP, do not include a driver for the LSI Logic or LSI Logic SAS adapter. You must download the driver from the LSI Logic Web site.

NOTE Drivers for a Mylex (BusLogic) compatible host bus adapter are not obvious on the LSI Logic Web site. Search the support area for the numeric string in the model number. For example, search for "958" for BT/KT-958 drivers.

On Linux hosts, and in the Add Hardware wizard, you can select a disk mode on the Select a Disk Type page. See "Normal and Independent Disk Modes" on page 84.

See the *VMware Guest Operating System Installation Guide* for details about the driver and the guest operating system you plan to install in this virtual machine.

Normal and Independent Disk Modes

The option to select normal or independent mode is available on Linux hosts for custom configurations only. Normal mode means you want to include disks in any snapshots you take. If you do not want data on the disk to be recorded when you take a snapshot of the virtual machine, you can configure the disk to be independent.

If you configure the disk to be independent, you can further specify whether changes you make to the disk are to persist or be discarded when you power off the virtual machine or restore it to a snapshot.

Although for Windows hosts, this configuration setting is not available in the New Virtual Machine wizard, you can exclude virtual disks from snapshots by using the virtual machine settings editor. See "Exclude a Virtual Disk from Snapshots" on page 193.

Virtual Disks and Physical Disks

This option is available for custom configurations only. If you use a typical configuration, a new virtual disk is created and used for the virtual machine. Virtual disks are the best choice for most virtual machines. They are easy to set up and can be moved to new locations on the same host computer or to different host computers.

Even for custom configurations, you usually choose the option **Create a New Virtual Disk**. In some cases you might want to choose **Use an Existing Virtual Disk**, to use a virtual disk you created previously. The wizard displays a page for you to enter the path or browse to the existing virtual disk (`.vmdk`) file.

It is possible to use a physical hard disk (a "raw" disk) or IDE disk partition in a virtual machine. Do not use a physical disk configuration unless you are an expert user. See "Using Physical Disks in a Virtual Machine" on page 227.

Disk Capacity

The wizard prompts you to set a size between 0.1GB and 950GB for a virtual disk. On Windows hosts, the Pocket ACE size calculator can help determine the disk size for an ACE instance that fits on a portable device.

Select the option **Split virtual disk into 2 GB files** if your virtual disk is stored on a file system that does not support files larger than 2GB.

For custom configurations, you are also given the option **Allocate all disk space now**. VMware recommends that you allow the disk to grow. Allocating all disk space now gives somewhat better performance, but it is a time-consuming operation that cannot be canceled. Also it requires as much physical disk space as you specify for the virtual disk. If you allocate all the disk space now, you cannot use the shrink disk feature later.

Pocket ACE Disk Size Calculator on Windows Only

The Pocket ACE feature allows you to store ACE instances on portable devices such as USB keys (flash memory drives), Apple iPod mobile digital devices, and portable hard drives. ACE users attach these portable devices to x86 host computers and run their ACE instances with VMware Player.

On the Specify Disk Capacity page of the New Virtual Machine wizard, you can use the **Pocket ACE size calculator** button to determine what number to use in the **Disk size** text box. Disk size refers only to the size of the virtual hard disk. If you plan to create Pocket ACEs, you must also consider the amount of disk space required for memory, installers, and other files related to virtual machine overhead.

Select the **Fast synchronize cache** check box to reserve space for writing changes from the Pocket ACE cache on the host. Having this space available reduces the time it takes to synchronize files with the host.

To determine what number to enter in the **Virtual hard disk size** text box of the calculator, you need to how much disk space is available on the device. Plug the USB device in to your host computer and use the My Computer item to display its properties. This number cannot be less than the amount shown for **Space required on USB device** in the calculator. If necessary reduce the number in the **Virtual hard disk size** text box until the amount of total space required is correct for the device.

Use the New Virtual Machine Wizard

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.

Many of the settings you specify in the New Virtual Machine can be changed later, if necessary. You can use the virtual machine settings editor if you need to make changes after the initial creation. (From the menu bar, choose **VM > Settings**.)

Before you begin, determine what type of media to use for installing the operating system in the virtual machine and do one of the following:

- If you plan to use an installation CD or DVD for installing the guest operating system, insert the CD or DVD in the host's CD-ROM drive.
- If you plan to use an ISO image file, make sure the file is accessible to the host.

To use the New Virtual Machine wizard

1. From the Workstation menu bar, choose **File > New > Virtual Machine**.
2. Follow the prompts.

   For more information about the fields on a wizard page, click **Help** on that page.

After the wizard creates the virtual machine, the next step is installing the guest operating system. See "Installing a Guest Operating System" on page 87.

Installing a Guest Operating System

Installation of a guest operating system can be automated or manual:

- If you specified an installer disc or image (`.iso`) file and if the wizard detected an operating system that supports the easy install feature, installation is automated. An unattended installation of the operating system and VMware Tools begins when the virtual machine is powered on.

  The installation process usually runs without requiring input from you. See "Respond to Easy Install Prompts" on page 87.

- If you did not use the easy install feature, see "Install a Guest Operating System Manually" on page 88.

Respond to Easy Install Prompts

Usually you are not prompted for input during operating system installation if the easy install feature runs. If, however, you did not enter all the easy install information in the New Virtual Machine wizard, you might be prompted for a product key, user name, or password.

Also, if the operating system installation disc or image spans multiple CDs, DVDs, or image files, you might be prompted when the installer requires the next disk.

To respond to easy install prompts

1. If you are prompted to supply a product key, user name, or password, do the following:

   a. Click in the virtual machine window to allow mouse and keyboard input to be grabbed by the virtual machine.

   b. Type in the required information.

2. If you are using CDs or DVDs and are prompted to insert the next CD or DVD, use the CD or DVD drive attached to the host.

3. If you are using image files and are prompted to insert the next disc, do the following:

   - On Windows hosts, click **Change Disk**, browse to the image file for the next CD, and click **OK**.

   - On Linux hosts, from the Workstation menu bar, choose **VM > Settings > CD/DVD**, and browse to the image file for the next CD.

Install a Guest Operating System Manually

You must install an operating system manually if you did not or were not able to use the easy install feature when completing the New Virtual Machine wizard.

Before you begin, use the following documents to determine additional requirements for the specific operating system and version you plan to install:

- See the *VMware Guest Operating System Installation Guide*, available from the VMware Web site or from the **Help** menu.
- For information about installing a Linux operating system that has a VMware VMI (Virtual Machine Interface) enabled kernel in the guest operating system, see "Use a Paravirtualized Kernel in Linux Guests" on page 89.

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

Installing a guest operating system inside a virtual machine is essentially the same as installing it on a physical computer.

NOTE Workstation supports 64-bit guest operating systems only in Workstation 5.5 and higher, and only on host machines with supported processors. For the list of processors Workstation supports for 64-bit guest operating systems, see "PC Hardware" on page 23.

To install a guest operating system manually

1. Start Workstation.
2. Do one of the following so that the virtual machine can access the installation media for the guest operating system:

   - For a CD or DVD, if necessary, configure the virtual machine to use the host's CD-ROM/DVD drive, and insert the operating system media in the drive.

     In some host configurations, the virtual machine cannot boot from the installation CD-ROM. You can work around that problem by creating an ISO image file from the installation CD-ROM. Use the virtual machine settings editor (choose **VM > Settings**) to connect the virtual machine's CD drive to the ISO image file, and power on the virtual machine.

   - For an ISO image, connect the CD-ROM drive to an ISO image file of an installation disk.

To use a PXE server to install the guest operating system over a network connection, you do not need the operating system installation media. When you power on the virtual machine, the virtual machine detects the PXE server.

3 Click the **Power On** button.

4 Follow the instructions provided by the operating system vendor.

5 If the operating system spans several CDs, follow these steps when you are prompted to insert the second CD:

a Disconnect from the current image by choosing **VM > Removable Devices > CD-ROM > Disconnect**.

b Edit the CD settings by choosing **VM > Removable Devices > CD-ROM > Edit**.

c For **Use ISO image file**, click **Browse**, and select the ISO image for the second CD.

d In the **Device Status** area, select the **Connected** check box and click **OK**.

e In the guest operating system, click **OK** or respond to the prompt so that installation can continue.

f Repeat this process for additional CDs.

After the guest operating system is installed, you can use the standard tools within the operating system to configure its settings. VMware recommends that you install VMware Tools before you activate the license for the operating system. See "Installing VMware Tools" on page 100.

Use a Paravirtualized Kernel in Linux Guests

Since 2005, VMware has been collaborating with the Linux community to develop a common paravirtualization interface. In 2006, VMware released its VMI specification as an open specification. It allows VMware virtual machines to support various paravirtualized operating systems from popular Linux distributions.

Before you begin, obtain installation media (CD or ISO image) for the operating system. Paravirtualized kernel support is available for 32-bit versions of Ubuntu 7.04, 7.10, or 8.04 and SUSE Linux Enterprise Server 10 SP2.

The 64-bit version of SUSE Linux Enterprise Server 10 SP2 already contains paravirtualization. You do not need to use a Workstation setting to enable it.

For more information about paravirtualization in general, see the following VMware Web site at:

http://www.vmware.com/interfaces/paravirtualization.html

If you have a VMware VMI (Virtual Machine Interface) enabled kernel in the guest operating system, you will see improved performance if you enable paravirtual support in the virtual machine.

To use a paravirtualized kernel in Linux guests

1. Use the New Virtual Machine wizard to create virtual machine for one of the supported 32-bit guest operating systems.
2. After you finish creating the virtual machine, enable paravirtual kernel support, as follows:

   a. Choose **VM > Settings**.

   b. On the **Hardware** tab, select **Processors**, and in the **Execution Mode** section, select the **VMware kernel paravirtualization** check box.

Upgrade a Guest Operating System

When you use the New Virtual Machine wizard to create a virtual machine, one of the settings you specify is the guest operating system type and version. Workstation chooses configuration defaults based on the guest type and version you choose.

If you upgrade a guest operating system to a newer version, also update the guest operating system version for the virtual machine.

To upgrade a guest operating system

1. Start Workstation and select the virtual machine.
2. Make sure the virtual machine is powered off.
3. Choose **VM > Settings**.
4. Click the **Options** tab.
5. On the **General** settings panel, in the **Version** field, select the version to which you plan to upgrade and click **OK**.

   The setting you specify here is written to the virtual machine's configuration file. This setting does not actually change the guest operating system itself.
6. Power on the virtual machine.
7. To upgrade the guest operating system, follow the upgrade instructions provided by the operating system vendor.

Change the Version of a Virtual Machine

If you created virtual machines with an earlier version of Workstation, you must upgrade to the latest version to use the newest features. For information about new features, see the release notes.

If you created Workstation 6.5 virtual machines and you want to deploy those virtual machines to run on a different VMware product, you might need to downgrade to a version that is compatible with that product.

Using Workstation 6.5, you can upgrade and downgrade to versions 4, 5, 6.0, and 6.5.

You can also determine which virtual hardware version to use.

Consider the following when changing the virtual hardware version of a virtual machine:

- For Workstation 5, 6, and 6.5 virtual machines, you can change the version of the original virtual machine or create a full clone, so that the original remains unaltered. For Workstation 4 virtual machines, Workstation changes the original virtual machine.
- If you upgrade a Workstation 4 or 5 virtual machine that is compatible with ESX Server to Workstation 6.x, you cannot use the Change Version wizard to later downgrade it again to an ESX-compatible virtual machine.

  On Windows hosts, however, you can use the Conversion wizard (choose **File > Import**) to perform such a downgrade.
- When you upgrade a Windows XP, Windows Server 2003, or Windows Vista virtual machine, the Microsoft product activation feature might require you to reactivate the guest operating system.

To change the version of a virtual machine

1. Make backup copies of the virtual disks (`.vmdk` files).
2. If you are upgrading from a Workstation 4 or 5 virtual machine, or downgrading to a Workstation 4 or 5 virtual machine, make a note of the NIC settings in the guest.

   Specifically, if you specified a static IP address for this virtual machine, after the upgrade, that setting might be changed to automatic assignment by DHCP.

   To check the NIC settings, use the method appropriate for your operating system. For example, on Windows XP, you can use the Control Panel's Network Connections item to find information about the TCP/IP address for the virtual machine.

3 Shut down the guest operating system and power off the virtual machine.

4 Select the virtual machine and choose **VM > Upgrade or Change Version**.

5 Follow the prompts.

When you select a hardware compatibility version, you see a list of the VMware products that are compatible with that version. If you select Workstation 4, 5, or 6.0.x you also see a list of Workstation 6.5 features that are not supported for that version.

6 Power on the virtual machine.

If you upgrade a virtual machine that contains a Windows 98 operating system to a Workstation 6.5 virtual machine, you are prompted to install a PCI-PCI bridge driver when you power on the virtual machine. Because Workstation 6.5 has 32 more PCI-PCI bridges than Workstation 6.0.x, you might need to respond to the prompt 32 or 33 times.

7 If applicable, in the guest operating system, check the NIC settings and adjust them if they changed, as described in Step 2.

8 If the virtual machine does not have the latest version of VMware Tools installed, update VMware Tools.

Even if, for example, you upgraded a Workstation 4 virtual machine to Workstation 5 rather than 6.5, be sure to update VMware Tools to the version included with Workstation 6.5. See "VMware Tools Update Process" on page 113. Do not remove the older version of VMware Tools before installing the new version.

If you are upgrading a virtual machine that runs from a physical (raw) disk, you can safely ignore the message, "Unable to upgrade <drive_name>. One of the supplied parameters is invalid." Click **OK**.

Using an Older-Version Virtual Machine Without Upgrading

You might not want to upgrade a virtual machine because you want it to remain compatible with other VMware products you are using. Following is a brief summary of VMware product version compatibility.

Version of Workstation	Compatible VMware Products
4.x	GSX Server 3.x, VMware Server 1.x and 2.0, ESX Server 2.x and 3.x, VMware Fusion 1.1 and 2.0, and ACE 1.x, 2.0, and 2.5
5.x	VMware Server 1.x and 2.0, VMware Fusion 1.1 and 2.0, ESX Server 3.x, VMware ACE 2.0 and 2.5, and VMware Player 1.x, 2.0, and 2.5
6.0.x	VMware Server 2.0, VMware Fusion 1.1 and 2.0, VMware ACE 2.0 and 2.5, and VMware Player 2.0 and 2.5
6.5	VMware Player 2.5, VMware ACE 2.5, VMware Server 2.0, and Fusion 2.0

You can run older versions of virtual machines in Workstation 6.5, but you will not have the benefits of the new features of Workstation 6.5.

For more information about compatibility between VMware products, see the *VMware Virtual Machine Mobility Planning Guide*.

If you decide not to upgrade a virtual machine, you still need to upgrade VMware Tools to the new version. Follow the instructions for your guest operating system in "VMware Tools Update Process" on page 113. Do not remove the older version of VMware Tools before installing the new version.

Files That Make Up a Virtual Machine

You might never need to know the filenames or locations for your virtual machine files. Virtual machine file management is performed by Workstation.

A virtual machine typically is stored on the host computer in a set of files, usually in a directory created by Workstation for that specific virtual machine. See "Virtual Machine Location" on page 81.

The key files are listed in Table 4-1 by extension. In these examples, `<vmname>` is the name of your virtual machine.

Table 4-1. Virtual Machine Files

Extension	File Name	Description

`.log`	`<vmname>.log`
	or
	`vmware.log`
		The log file of key Workstation activity. This file is useful in troubleshooting. This file is stored in the directory that holds the configuration (`.vmx`) file of the virtual machine.

`.nvram`	`<vmname>.nvram`
	or
	`nvram`
		The NVRAM file, which stores the state of the virtual machine's BIOS.

`.vmdk`	`<vmname>.vmdk`	VMDK files, which store the contents of the virtual machine's hard disk drive. A virtual disk is made up of one or more virtual disk (`.vmdk`) files. The virtual machine settings editor shows the name of the first file in the set. This file contains pointers to the other files in the set. (If you specify that all space should be allocated when you create the disk, these files start at the maximum size and do not grow.) Almost all of a `.vmdk` file's content is the virtual machine's data, with a small portion allotted to virtual machine overhead. If the virtual machine is connected directly to a physical disk, the `.vmdk` file stores information about the partitions the virtual machine is allowed to access. Earlier VMware products used the extension `.dsk` for virtual disk files.
	`<vmname>-s<###>.vmdk`	If you specified that the files can grow, the filenames include an `s` in the file number (for example, `Windows XP Professional-s001.vmdk`). If you specified that the virtual disk is split into 2GB chunks, the number of `.vmdk` files depends on the size of the virtual disk. As data is added to a virtual disk, the `.vmdk` files grow, to a maximum of 2GB each.
	`<vmname>-f<###>.vmdk`	If the disk space was allocated when the disk was created, the names include an `f` instead of an `s` (for example, `Windows XP Professional-f001.vmdk`).
	`<vmname>-<disk>-<###>.vmdk`	If the virtual machine has one or more snapshots, some files are redo-log files. They store changes made to a virtual disk while the virtual machine is running. The `###` indicates a unique suffix added by Workstation to avoid duplicate file names.

Table 4-1. Virtual Machine Files (Continued)

Extension	File Name	Description
.vmem	<uuid>.vmem	The virtual machine's paging file, which backs up the guest main memory on the host file system. This file exists only when the virtual machine is running or if the virtual machine fails.
	<snapshot_name_number>.vmem	Each snapshot of a virtual machine that is powered on has an associated `.vmem` file, which contains the guest's main memory, saved as part of the snapshot.
.vmsd	<vmname>.vmsd	A centralized file for storing information and metadata about snapshots.
.vmsn	<vmname>-Snapshot.vmsn	The snapshot state file, which stores the running state of a virtual machine at the time you take that snapshot.
	<vmname>-Snapshot<###>.vmsn	The file that stores the state of a snapshot.
.vmss	<vmname>.vmss	The suspended state file, which stores the state of a suspended virtual machine. Some earlier VMware products used the extension `.std` for suspended state files.
.vmtm	<vmname>.vmtm	The configuration file containing team data.
.vmx	<vmname>.vmx	The primary configuration file, which stores settings chosen in the New Virtual Machine wizard or virtual machine settings editor. If you created the virtual machine with an earlier version of Workstation on a Linux host, this file might have a `.cfg` extension.
.vmxf	<vmname>.vmxf	A supplemental configuration file for virtual machines that are in a team. This `.vmxf` file remains if a virtual machine is removed from the team.

Other files might be present in the directory. Some are present only while a virtual machine is running. See "Lock Files" on page 220.

Installing and Using VMware Tools

5

This chapter discusses how to install, update, and run VMware Tools. This chapter includes the following topics:

Components of VMware Tools

VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine. Although the guest operating system can run without VMware Tools, you lose important functionality and convenience.

VMware Tools includes the following components:

- VMware Tools service
- VMware device drivers
- VMware user process
- VMware Tools control panel

VMware Tools Service

The program file is called `VMwareService.exe` on Windows guest operating systems and `vmware-guestd` on Linux, FreeBSD, and Solaris guests.

This service starts when the guest operating system boots and performs various duties within the guest operating system:

- Passes messages from the host operating system to the guest operating system.
- Executes commands in the operating system to cleanly shut down or restart a Linux, FreeBSD, or Solaris system when you select power operations in Workstation.
- On Windows guests, allows the mouse cursor to move freely between the guest and host operating systems.
- On Windows guests, matches the guest's screen resolution to the host's screen resolution and the reverse.
- Synchronizes the time in the guest operating system with the time in the host operating system.
- Runs scripts that help automate guest operating system operations. The scripts run when the virtual machine's power state changes.

The VMware Tools service is not installed on NetWare operating systems. Instead, the `vmwtool` program is installed. It synchronizes time and allows you to turn the CPU idler on or off.

VMware Device Drivers

These device drivers include:

- SVGA display driver that provides high display resolution and significantly faster overall graphics performance.
- The `vmxnet` networking driver for some guest operating systems.
- BusLogic SCSI driver for some guest operating systems.
- VMware mouse driver.
- A kernel module for handling shared folders, called `hgfs.sys` on Windows and `vmhgfs` on Linux and Solaris.
- The Virtual Machine Communication Interface (VMCI) driver for creating client-server applications that are optimized for fast and efficient communication between virtual machines.

VMware User Process

The program file is called `VMwareUser.exe` on Windows guests and `vmware-user` on Linux, Solaris, and FreeBSD guests.

This service performs the following tasks within the guest operating system:

- Enables you to copy and paste text between the guest and host operating systems, and copy and paste files between the host operating systems and Windows, Linux, and Solaris guest operating systems.
- Enables you to drag and drop files between the host operating systems and Windows, Linux, and Solaris guest operating systems.
- Enables you to use the Unity feature with Windows and Linux guests.
- On Linux and Solaris guests, grabs and releases the mouse cursor when the SVGA driver is not installed.
- On Linux and Solaris guests, matches the guest's screen resolution to the host's.

This process starts when you begin an X11 session. To use a different mechanism to start the process, see "Start the VMware User Process Manually If You Do Not Use a Session Manager on UNIX" on page 112.

The VMware Tools user process is not installed on NetWare operating systems. Instead, the `vmwtool` program is installed. It controls the grabbing and releasing of the mouse cursor. It also allows you copy and paste text. You cannot drag and drop or copy and paste files between hosts and NetWare guest operating systems.

VMware Tools Control Panel

The VMware Tools control panel lets you modify settings, shrink virtual disks, and connect and disconnect virtual devices. See "Open the VMware Tools Control Panel" on page 117.

Installing VMware Tools

The installers for VMware Tools are installed with Workstation as ISO image files. When you choose **VM > Install VMware Tools**, Workstation temporarily connects the virtual machine's first virtual CD-ROM drive to the correct ISO image file for the guest operating system. The installation procedure varies depending on the operating system:

- "Manually Install VMware Tools in a Windows Guest Operating System" on page 100
- "Install VMware Tools on a Linux Guest Within X by Using the RPM Installer" on page 105
- "Install VMware Tools from the Command Line with the tar or RPM Installer" on page 106
- "Install VMware Tools in a Solaris Guest" on page 108
- "Install VMware Tools in a FreeBSD Guest" on page 109
- "Install VMware Tools in a NetWare Virtual Machine" on page 111

Manually Install VMware Tools in a Windows Guest Operating System

VMware Tools is supported on all Windows guest operating systems. Before you use the menu command to install VMware Tools, perform the following tasks, as necessary:

- If you are running Workstation on a Windows host and your virtual machine has only one CD-ROM drive, make sure the CD-ROM drive is configured as an IDE or SCSI CD-ROM drive. It cannot be configured as a generic SCSI device. If necessary, add an IDE or SCSI CD-ROM drive to the virtual machine. See "Adding DVD/CD-ROM and Floppy Drives to a Virtual Machine" on page 234.
- Make sure the virtual CD-ROM drive is configured to auto-detect a physical drive. This task is necessary if you connected the virtual machine's CD drive to an ISO image file when you installed the operating system. Change the connection from the ISO image to auto-detect a physical drive. (With the virtual machine powered off, choose **VM > Settings > CD/DVD > Use Physical Drive > Auto-detect**.)
- When you install VMware Tools, make sure the virtual machine is powered on.
- If the guest operating system is a Windows NT, Windows 2000, Windows XP, Windows Server 2003, or Windows Vista operating system, log in as an administrator. Any user can install VMware Tools in a Windows 95, Windows 98, or Windows Me guest operating system.

To install VMware Tools

1 On the host, from the Workstation menu bar, choose **VM > Install VMware Tools**.

If an earlier version of VMware Tools is installed, the menu item is **Update VMware Tools**.

Depending on whether autorun is enabled, one of the following occurs inside the guest operating system:

- If autorun is enabled in the guest operating system, a dialog box appears after a few seconds. It asks whether you want to install VMware Tools.
- If autorun is not enabled, the dialog box does not appear automatically. Click **Start > Run** and enter **`D:\setup\setup.exe`** where **`D:`** is your first virtual CD-ROM drive.

2 Click **Yes** to launch the InstallShield wizard.

3 Follow the on-screen instructions.

On some Windows operating systems, after the SVGA driver is installed, you are prompted to reboot to use this new driver.

4 Reboot the virtual machine if necessary.

To change the default configuration options, see “Open the VMware Tools Control Panel” on page 117.

Configure the Video Driver on Older Versions of Windows

If you are installing VMware Tools in a virtual machine that has a Windows NT, Windows Me, Windows 98, or Windows 95 operating system, you might need to configure the video driver manually. When you click **Finish** in the VMware Tools installation wizard, a message appears indicating that VMware Tools failed to install the SVGA driver.

A Notebook window, the Display Properties/Settings dialog box, and a message box appear, prompting you to reboot the machine.

To configure the video driver on older versions of Windows

1 In the message box that prompts you to reboot, click **No**.

If you click **Yes**, after the virtual machine reboots, run the VMware Tools installer again (choose **VM > Reinstall VMware Tools**). Select the **Repair** option. The **Repair** option allows the Notebook window to appear again so that the installer can access the SVGA driver.

2 Follow the instructions in the Notebook file.

The instructions are specific to each operating system. They provide steps for selecting the VMware SVGA driver, usually in the Display Properties/Settings dialog box, and installing it from the VMware Tools ISO image.

The English version of the instructions from the Notebook file are reprinted in Knowledge Base article 1001819 at the VMware Web site.

Automate the Installation of VMware Tools in a Windows Guest

If you are installing VMware Tools in a number of Windows virtual machines, you can automate its installation. This silent installation feature uses the Microsoft Windows Installer runtime engine.

Make sure the Microsoft Windows Installer runtime engine version 2.0 or higher is installed in the guest operating system.

Version 2.0 or higher is included with newer versions of Windows. If you are installing VMware Tools in older Windows guest operating systems, check the version of the `%WINDIR%\system32\msiexec.exe` file.

If the file version is not 2.0 or higher, upgrade the engine by running `instmsiw.exe` (`instmsia.exe` for Windows 95 or Windows 98 guests), which is included with the VMware Tools installer.

For more information about using the Microsoft Windows Installer, including command-line options, go to the Windows Installer page on the MSDN Web site.

To automate the installation of VMware Tools in a Windows guest

1. Make sure the virtual machine's CD-ROM drive is connected to the VMware Tools ISO image and that it is configured to connect whenever you power on the virtual machine:

   a. Select the virtual machine and choose **VM > Settings > Hardware > CD-ROM**.

   b. In the **Device status** section, select the **Connect at Power On** check box.

   c. In the **Connection** section, select **Use ISO image** and browse to the `windows.iso` file, located in the directory where you installed Workstation.

   d. Click **OK**.

2. (Optional) In the guest operating system, suppress prompts about installing unsigned drivers.

   If you are installing VMware Tools from a beta or RC (release candidate) version of Workstation, you are asked to confirm the installation of unsigned drivers. Follow these steps to suppress these confirmation prompts.

   For all Windows systems except Windows Vista:

   a. On the virtual machine's desktop or **Start** menu, right-click **My Computer** and choose **Properties**.

   b. Click the **Hardware** tab and click **Driver Signing**.

   c. In the Driver Signing Options dialog box, click **Ignore** and click **OK**.

   d. Click **OK** in the System Properties dialog box.

   For Windows Vista:

   a. On the **Start** menu, right-click **Computer** and choose **Properties**.

   b. Click **Advanced system settings > Hardware > Windows Update Driver Settings**.

   c. Click **Never check for drivers when I connect a new device** and click **OK**.

   d. Click **OK** in the System Properties dialog box.

3 Open a command prompt and use the following command to install some or all of the VMware Tools components:

```
msiexec –i "D:\VMware Tools.msi" ADDLOCAL=ALL [REMOVE=<component>] /qn
```

In this command, you can optionally use **`REMOVE=<component>`** if you do not want to install a particular component.

Valid Component Values	Description
`Toolbox`	VMware Tools control panel and its utilities. Excluding this feature prevents you from using VMware Tools in the guest operating system. VMware does not recommend excluding this feature.
`Drivers`	Includes the SVGA, mouse, BusLogic, and `vmxnet` drivers. ■ `SVGA` – VMware SVGA driver. Excluding this feature limits the display capabilities of your virtual machine. ■ `Mouse` – VMware mouse driver. Excluding this feature decreases mouse performance in your virtual machine. ■ `Buslogic` – VMware BusLogic driver. If your virtual machine is configured to use the LSI Logic driver, you might want to remove this feature. ■ `VMXNet` – VMware `VMXnet` networking driver.
`MemCtl`	VMware memory control driver. Use this driver if you plan to use this virtual machine with VMware ESX Server. Excluding this feature hinders the memory management capabilities of the virtual machine running on a VMware ESX Server system.
`Hgfs`	VMware shared folders driver. Use this driver if you plan to use this virtual machine with VMware Workstation. Excluding this feature prevents you from sharing a folder between your virtual machine and the Workstation host.

For example, to install everything but the shared folders driver, type the following on the command line:

```
msiexec –i "D:\VMware Tools.msi" ADDLOCAL=ALL REMOVE=Hgfs /qn
```

The SVGA, Mouse, BusLogic, VMXnet, and MemCtl features are children of the Drivers feature. This means that the following command skips installation of the SVGA, mouse, BusLogic, `vmxnet`, and `MemCtl` drivers:

```
msiexec –i "D:\VMware Tools.msi" ADDLOCAL=ALL REMOVE=Drivers /qn
```

To include a feature, use it with the ADDLOCAL option. To exclude a feature, use it with the REMOVE option.

Install VMware Tools on a Linux Guest Within X by Using the RPM Installer

You can use a graphical user interface to install VMware Tools in a Linux guest. For information about how to install VMware Tool from the command line, see "Install VMware Tools from the Command Line with the tar or RPM Installer" on page 106.

Before you begin, make sure the virtual machine is powered on and the guest operating system is running.

To install VMware Tools on a Linux Guest Within X by Using the RPM Installer

1 On the host, choose **VM > Install VMware Tools**.

   If an earlier version of VMware Tools is installed, the menu item is **Update VMware Tools**.

   The guest operating system mounts the VMware Tools installation virtual CD. A window manager displaying two files might appear. One file is for the RPM installer and one is for the tar installer. Alternatively, a VMware Tools CD icon might appear on the desktop.

2 Do one of the following:

   - If you see a **VMware Tools CD** icon on the desktop, double-click it, and after it opens, double-click the RPM installer in the root of the CD-ROM.
   - If you see a file manager window, double-click the RPM installer file.

   In some Linux distributions, the **VMware Tools CD** icon might fail to appear. In this case, install VMware Tools from the command line.

3 When prompted, enter the root password and click **OK**.

   The installer prepares the packages.

4 Click **Continue** when the installer presents a dialog box that shows **Completed System Preparation**.

   When the installer is done, no confirmation window or finish button appears, but VMware Tools is installed.

5 In an X terminal, as root (**su**), run the following file to configure VMware Tools:

```
vmware-config-tools.pl
```

   Respond to the questions the command-line wizard displays on the screen. Press Enter to accept the default value.

6 Exit from the root account.

```
exit
```

7 In an X terminal, to start the VMware User process, enter the following command:

```
vmware-user
```

8 To start the VMware Tools control panel, enter the following command:

```
vmware-toolbox &
```

To change the default VMware Tools configuration options, see "Open the VMware Tools Control Panel" on page 117.

Install VMware Tools from the Command Line with the tar or RPM Installer

Before you begin, make sure the virtual machine is powered on and the guest operating system is running.

To install VMware Tools from the command line with the tar or RPM installer

1 On the host, choose **VM > Install VMware Tools**.

If an earlier version of VMware Tools is installed, the menu item is **Update VMware Tools**.

2 On the guest, log in as root (**su**).

3 If necessary, mount the VMware Tools virtual CD-ROM image by entering a command similar to the following:

```
mount /dev/cdrom /mnt/cdrom
```

Some Linux distributions automatically mount CD-ROMs. If your distribution uses automounting, you can skip this step.

Some Linux distributions use different device names or organize the /dev directory differently. If your CD-ROM drive is not /dev/cdrom or if the mount point for a CD-ROM is not /mnt/cdrom, modify the command to reflect the conventions used by your distribution.

4 Change to a working directory by entering a command such as the following:

```
cd /tmp
```

5 If a previous installation exists, delete the previous `vmware-tools-distrib` directory before installing.

The location of this directory depends on where you placed it during the previous installation. Often it is placed in `/tmp/vmware-tools-distrib`.

6 Run the installer and unmount the CD-ROM image.

Depending on whether you are using the tar installer or the RPM installer, do one of the following:

- For the tar installer, at the command prompt, enter:

```
tar zxpf /mnt/cdrom/VMwareTools-<xxxx>.tar.gz
umount /dev/cdrom
```

- For the RPM installer, at the command prompt, enter:

```
rpm -Uhv /mnt/cdrom/VMwareTools-<xxxx>.i386.rpm
umount /dev/cdrom
```

The value <xxxx> is the build number of the product release.

If your Linux distribution automatically mounted the CD-ROMs, you do not need to use the `unmount` portion of the command.

If you attempt to install an RPM installation over a tar installation or the reverse, the installer detects the previous installation and must convert the installer database format before continuing.

7 Configure VMware Tools.

Depending on whether you are using the tar installer or the RPM installer, do one of the following:

- For the tar installer, enter the following commands to run the installer:

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

  Respond to the questions the command-line wizard displays on the screen. Press Enter to accept the default value. The configuration file, `vmware-config-tools.pl`, runs after the installer file finishes running.

- For the RPM installer, enter the following command to run the configuration file:

```
vmware-config-tools.pl
```

  Respond to the questions the command-line wizard displays on the screen. Press Enter to accept the default value.

8 Log out of the root account.

```
exit
```

9 (Optional) Start your graphical environment.

10 In an X terminal, to start the VMware User process, enter the following command:

```
vmware-user
```

11 (Optional) To start the VMware Tools control panel, enter the following command:

```
vmware-toolbox &
```

To change the default VMware Tools configuration options, see "Open the VMware Tools Control Panel" on page 117.

Install VMware Tools in a Solaris Guest

Before you begin, make sure the virtual machine is powered on and the guest operating system is running.

To install VMware Tools in a Solaris guest

1 On the host, choose **VM > Install VMware Tools**.

If an earlier version of VMware Tools is installed, the menu item is **Update VMware Tools**.

2 On the guest, log in as root (**su**).

3 If necessary, mount the VMware Tools virtual CD-ROM image.

Usually, the Solaris volume manager vold mounts the CD-ROM under /cdrom/vmwaretools. If the CD-ROM is not mounted, restart the volume manager using the following commands:

```
/etc/init.d/volmgt stop
/etc/init.d/volmgt start
```

4 After the CD-ROM is mounted, change to a working directory (for example, /tmp) and extract VMware Tools by entering the following commands:

```
cd /tmp
gunzip -c /cdrom/vmwaretools/vmware-solaris-tools.tar.gz | tar xf -
```

5 Run the VMware Tools tar installer:

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

Respond to the configuration prompts. Press Enter to accept the default value.

6 Log out of the root account:

```
exit
```

7 (Optional) Start your graphical environment.

8 In an X terminal, to start the VMware User process, enter the following command:

```
vmware-user
```

9 (Optional) To start the VMware Tools control panel, enter the following command:

```
vmware-toolbox &
```

To change the default VMware Tools configuration options, see "Open the VMware Tools Control Panel" on page 117.

Install VMware Tools in a FreeBSD Guest

Before you begin, make sure the virtual machine is powered on and the guest operating system is running.

To install VMware Tools in a FreeBSD guest

1 On the host, choose **VM > Install VMware Tools**.

If an earlier version of VMware Tools is installed, the menu item is **Update VMware Tools**.

2 Make sure the guest operating system is running in text mode.

You cannot install VMware Tools while X is running.

3 On the guest, log in as root (**su**).

4 If necessary, mount the VMware Tools virtual CD-ROM image by entering a command similar to the following:

```
mount /cdrom
```

Some FreeBSD distributions automatically mount CD-ROMs. If your distribution uses automounting, skip this step.

5 Change to a working directory by entering a command such as the following:

```
cd /tmp
```

6 Untar the VMware Tools tar file:

```
tar zxpf /cdrom/vmware-freebsd-tools.tar.gz
```

7 If necessary, unmount the VMware Tools virtual CD-ROM image by entering a command similar to the following:

```
umount /cdrom
```

If your distribution uses automounting, skip this step.

8 Run the VMware Tools installer:

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

9 Log out of the root account:

```
exit
```

10 (Optional) Start your graphical environment.

11 In an X terminal, to start the VMware User process, enter the following command:

```
vmware-user
```

12 (Optional) To start the VMware Tools control panel, enter the following command:

```
vmware-toolbox &
```

In minimal installations of the FreeBSD 4.5 guest operating system, sometimes VMware Tools does not start. See "Install the Missing FreeBSD Library" on page 110.

To change the default VMware Tools configuration options, see "Open the VMware Tools Control Panel" on page 117.

Install the Missing FreeBSD Library

If VMware Tools does not start after you install it, you might need to install a library that is missing because you do not have a full installation of FreeBSD 4.5.

Before you begin, make sure you have the FreeBSD 4.5 installation CD or access to the ISO image file.

To install the missing FreeBSD library

1 Reboot the guest operating system.

2 On the guest, in an X terminal, enter the following command to start the VMware Tools control panel:

```
vmware-toolbox &
```

If the following error message appears, the required library was not installed:

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

3. Insert and mount the FreeBSD 4.5 installation CD or access the ISO image file.

4. Change directories and run the installation script:

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

Install VMware Tools in a NetWare Virtual Machine

Before you begin, make sure the virtual machine is powered on and the guest operating system is running.

To install VMware Tools in a NetWare virtual machine

1. On the host, choose **VM > Install VMware Tools**.

   If an earlier version of VMware Tools is installed, the menu item is **Update VMware Tools**.

2. On the guest, load the CD-ROM driver so the CD-ROM device mounts the ISO image as a volume by doing one of the following:

   - For a NetWare 6.5 virtual machine in the system console, enter:

     ```
     LOAD CDDVD
     ```

   - For a NetWare 6.0 or NetWare 5.1 virtual machine, in the system console, enter:

     ```
     LOAD CD9660.NSS
     ```

   - For a NetWare 4.2 virtual machine, in the system console, enter:

     ```
     load cdrom
     ```

     Mount the VMware Tools CD-ROM image by entering:

     ```
     cd mount vmwtools
     ```

3. In the system console, enter one of the following:

   - For NetWare 5.1, 6.0, or 6.5:

     ```
     vmwtools:\setup.ncf
     ```

   - For NetWare 4.2:

     ```
     vmwtools:\setup
     ```

   When the installation finishes, the message `VMware Tools for NetWare are now running` appears in the Logger Screen (NetWare 6.5 and NetWare 6.0 guests) or the Console Screen (NetWare 4.2 and 5.1 guests).

4 If you have a NetWare 4.2 guest, restart the guest operating system, as follows:

   a To shut down the system, in the system console, enter:

   ```
   down
   ```

   b To restart the guest operating system, in the system console, enter:

   ```
   restart server
   ```

5 Make sure the VMware Tools virtual CD-ROM image (`netware.iso`) is not attached to the virtual machine.

   If it is attached, disconnect it. Right-click the CD-ROM icon in the status bar of the console window and choose **Disconnect**.

Start the VMware User Process Manually If You Do Not Use a Session Manager on UNIX

One of the executables used by VMware Tools in UNIX guests is `vmware-user`. This program implements the fit-guest-to-window feature and Unity mode, among other features.

Normally, `vmware-user` is started automatically after you configure VMware Tools and then log out of the desktop environment and log back in.

However, if you run an X session without a session manager (for example, by using `startx` and getting a desktop and not using `xdm`, `kdm`, or `gdm`), you must start the VMware User process manually.

You must also start `vmware-user` manually after you update to a new version of VMware Tools.

To start the VMware User process manually if you do not use a session manager

Do one of the following:

- To have `vmware-user` start when you start an X session, add `vmware-user` to the appropriate X startup script, such as the `.xsession` or `.xinitrc` file.

  The `vmware-user` program is located in the directory where you selected to install binary programs, which defaults to `/usr/bin`. The startup script that needs to be modified depends on your particular system.

- To start `vmware-user` after a VMware Tools software update or if you notice certain features are not working, open a terminal window and enter the following command:

  ```
  vmware-user
  ```

VMware Tools Update Process

Because VMware Tools installers (ISO images) are installed with Workstation, when you update to a new version of Workstation, a check is performed to determine if a new version of VMware Tools is available. When you update from a version of VMware Tools included with Workstation 4.x, 5.x, 6.0.x, or 6.x, the previous version of VMware Tools might be uninstalled.

Although you can set Workstation to check regularly for Workstation updates, the guest operating system checks for VMware Tools updates only when you power on a virtual machine. It compares its version of VMware Tools against the version that is installed on the host.

For VMware Tools updates on Linux and Windows guests, you can set the guest to update automatically or you can perform a manual update. On other guests, you must manually update.

When you update VMware Tools, any changes you made to the default scripts are overwritten. Any custom scripts you created remain untouched, but do not benefit from any underlying changes that enhance the default scripts.

How Automatic Updates Occur

On Windows and Linux guest systems, you can set VMware Tools to update itself when the virtual machine is powered on. The status bar displays the message `Installing VMware Tools . . .` when an update is in progress. After the update is complete, if you are logged in to a Windows guest, a restart prompt appears for 30 seconds. If you are not logged in, the operating system restarts without prompting.

An auto-update check is performed as part of the boot sequence when you power on a virtual machine. If the virtual machine was suspended and you resume it or restore it to a snapshot during the boot sequence before this check occurs, the automatic update occurs as planned.

If you resume the virtual machine or restore it to a snapshot after the auto-update check occurs, the automatic update does not occur.

For more information about automatic updates, see "Use Global Settings to Update VMware Tools Automatically" on page 114 and "Set Autoupdate Options for Each Virtual Machine" on page 115.

How You Are Notified to Do a Manual Update

On Windows and Linux guests, you can specify that no automatic update should occur. On other operating systems, automatic updates are not possible. In these cases, perform a manual update.

The status bar of the guest system displays a message when a new version is available. To install the update, use the same procedure that you used for installing VMware Tools the first time. On Linux guests, the VMware User process (`vmware–user`) does not restart following an update until you launch it manually or log out of your window manager and log in again.

On Windows, you can alternatively open the VMware Tools control panel (double-click the **VMware Tools** icon in the notification area of the taskbar), and on the **Options** tab, click **Update**.

Use Global Settings to Update VMware Tools Automatically

To automatically update VMware Tools for most or all Windows or Linux guests when the virtual machine starts, configure the global preference first and then configure the per-virtual-machine update option to use that global preference.

Before you begin, if you use a UNIX host, become root (**`su`**) before starting Workstation. On UNIX systems, nonroot users are not allowed to modify the preference setting for VMware Tools updates.

To use global settings to update VMware Tools automatically

1. Start Workstation.
2. Choose **Edit > Preferences** and click the **Tools** tab.
3. Select the check box on this tab and click **OK**.
4. For each of your virtual machines, do the following:
    a. Select the virtual machine.
    b. Choose **VM > Settings**.
    c. Click the **Options** tab and select **Tools**.
    d. Select **Use global settings** from **Edit > Preferences > Tools** and click **OK**.

Set Autoupdate Options for Each Virtual Machine

Use this procedure to override global settings for automatically updating VMware Tools on Linux and Windows guests. New versions of VMware Tools become available when you install a new version of Workstation on the host.

Automatic updates work for versions of VMware Tools included in Workstation 5.5 and above (build 29772 and above). Automatic updates do not work for versions of VMware Tools included in virtual machines created with VMware Server 1.x.

To set autoupdate options for each virtual machine

1. Select the Linux or Windows virtual machine.
2. Choose **VM > Settings**.
3. Click the **Options** tab and select **Tools**.
4. Select an update option and click **OK**.

   If you specify **Do nothing**, you must update VMware Tools manually. In this case, the status bar displays a message when a new version is available. To install the update, use the same procedure that you used for installing VMware Tools the first time. For the platform-specific installation instructions, see "Installing VMware Tools" on page 100.

Update VMware Tools in Older Windows Virtual Machines

When a Microsoft installer performs an update, it updates only the components that it finds already installed. It does not add new components. If you update VMware Tools in a Windows virtual machine that was created with Workstation 5.x, some new components are not installed. Specifically, the Workstation 6.x component for file sharing and dragging and dropping files is not installed.

To get the new components, you must uninstall the old version of VMware Tools and install the new version of VMware Tools.

To update VMware Tools in older Windows virtual machines

1. To uninstall the old version of VMware Tools, use the **Add/Remove Programs** item in the guest's Control Panel.
2. To install the new version of VMware Tools, see "Installing VMware Tools" on page 100.

Uninstall VMware Tools

Occasionally, an update of VMware Tools is incomplete. You can usually solve the problem by uninstalling VMware Tools and then reinstalling.

To uninstall VMware Tools

Depending on the guest operating system, do one of the following:

- On a Windows guest, use the guest operating system's **Add/Remove Programs** item to remove VMware Tools.
- On any UNIX guest, log on as root (**`su`**) and enter the following command:

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

- On a Linux guest that has VMware Tools installed by using an RPM installer, you can uninstall by using the following command:

  ```
  rpm -e VMwareTools
  ```

Repair or Change Installed Modules

If features like enhanced file sharing do not work after a VMware Tools update, you might need to change or repair installed modules. Be sure to follow these steps. Do not use the guest's **Add/Remove Programs** item in the Windows Control Panel.

To repair or change installed modules

1. In Workstation, select the virtual machine and choose **VM > Reinstall VMware Tools**.
2. On the Welcome page, click **Next** and do one of the following:
   - Click **Change** to repair or modify which components of VMware Tools are installed.
   - Click **Modify** to specify which modules are installed.

     Occasionally, some new modules are not installed during an update. You can manually install new modules by using the **Modify** option.
3. Complete the rest of the pages of the wizard.

If features still do not work, uninstall VMware Tools and reinstall.

Open the VMware Tools Control Panel

Use the VMware Tools control panel to modify VMware Tools configuration settings, shrink virtual disks, and connect and disconnect virtual devices.

Before you begin, make sure VMware Tools is installed in the guest operating system.

On Windows Vista guests, log in to the operating system as an Administrator user.

To open the VMware Tools control panel

Do one of the following:

- On Windows guests, double-click **VMware Tools** icon in the notification area of the guest's Windows taskbar.

  If you cannot find the **VMware Tools** icon in the notification area, use the guest's Windows Control Panel to display it.

- On Linux, FreeBSD, and Solaris guests, open a terminal window and enter the command:

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

- On NetWare guests, do one of the following:

  - In a NetWare 5.1 or higher guest, choose **Novell > Settings > VMware Tools for NetWare**.
  - In a NetWare 4.2 guest, use VMware Tools commands in the system console. The VMware Tools program is called `vmwtool`.

Use the Windows Control Panel to Display the Taskbar Icon

If VMware Tools is installed in a Windows guest operating system but the **VMware Tools** icon does not appear in the notification area of the Windows taskbar, you can use the Windows Control Panel to display it.

To use the Windows Control Panel to display the taskbar icon

1. Go to **Start > Control Panel**.
2. Double-click the **VMware Tools** icon.
3. On the **Options** tab, select **Show VMware Tools in the taskbar** and click **Apply**.

Options Tab Settings

The **Options** tab of the VMware Tools control panel provides the following options:

- **Time synchronization between the virtual machine and the host operating system** – Periodically (every minute) checks whether the guest operating system’s time is lagging behind the host’s. If so, the guest’s clock is moved forward to match the host’s clock. If you use this option, disable all other time synchronization mechanisms. For example, some guests might have NTP or CMOS clock synchronization turned on by default.

  Regardless of whether you enable this setting, time synchronization occurs when the VMware Tools daemon is started (such as during a reboot), when resuming from a suspend operation, and after shrinking a disk. When the operating system starts or reboots, synchronization can be either forward or backward in time. For other events, synchronization is forward in time.

  To disable time synchronization completely, see “Disable Time Synchronization by Editing the Virtual Machine Configuration File” on page 118.

- **Show VMware Tools in the taskbar** – (Windows guests only) Displays the **VMware Tools** icon in the notification area of the taskbar. The icon indicates whether VMware Tools is running and whether an update is available.

- **Notify if update is available** – (Windows guests only) Displays the **VMware Tools** icon with a yellow caution icon when an update is available.

- **Update** button – (Windows guests only) Becomes enabled when an update is available. Clicking this button has the same effect as choosing **VM > Update VMware Tools** from the Workstation menu bar.

Disable Time Synchronization by Editing the Virtual Machine Configuration File

A virtual machine occasionally synchronizes time with the host even if you use the VMware Tools control panel (**Options** tab) to disable periodic time synchronization. You can disable time synchronization completely by editing the virtual machine configuration file.

You can follow these steps to keep a fictitious time in your guest, so that the guest is never synchronized with the host.

To disable time synchronization by editing the virtual machine configuration file

1. Power off the virtual machine.
2. Open the virtual machine's configuration file (`.vmx`) in a text editor and set the following options to FALSE.

Option Name	Synchronization Occurs During the Following Event
`tools.syncTime`	Periodically (normally once per minute). Time synchronization is only forward in time.
`time.synchronize.continue`	Taking a snapshot. Time synchronization is only forward in time.
`time.synchronize.restore`	Reverting to a snapshot. Time synchronization is only forward in time.
`time.synchronize.resume.disk`	Resuming a suspended virtual machine. Time synchronization is only forward in time.
`time.synchronize.shrink`	Shrinking a virtual disk. Time synchronization is only forward in time.
`time.synchronize.tools.startup`	Booting the guest operating system. Time synchronization can be either forward or backward in time.

3. Save and close the file.

Devices Tab Settings

The **Devices** tab of the VMware Tools control panel provides options for enabling and connecting to removable devices such as floppy drives, DVD/CD-ROM drives, ISO images, USB devices, sound adapters, and network adapters.

The controls for connecting and disconnecting devices might not be available, depending on whether your system administrator enabled them.

You might not see a particular network adapter listed that should appear in the list. If this happens, edit the virtual machine settings to remove all network adapters from the list and then add them back to the list.

Besides using the VMware Tools control panel to connect or disconnect a device, you can right-click the device icon in the status bar of the virtual machine window. See "Use Removable Devices in a Virtual Machine" on page 169.

Scripts Tab Settings

From the **Scripts** tab of the VMware Tools control panel, you can edit, disable, or run scripts that help automate guest operating system operations when you change the virtual machine’s power state.

From this tab, you can also specify the location of custom scripts for the **Suspend**, **Resume**, **Power On**, **Power Off**, and **Reset** buttons.

On most guest operating systems, if VMware Tools is installed and if you configure a virtual machine’s power controls to use the guest options, one or more default scripts run on the guest whenever you change the power state of the virtual machine.

For example, if you use the virtual machine settings editor (choose **VM > Settings > Options > Power**) and set the **Power Off** control to use **Shutdown Guest**, then the `poweroff-vm-default` script runs when you click the **Power Off** button in the Workstation toolbar. This script causes the guest operating system to shut down gracefully.

Scripts can be run on most guest operating systems, but not on Windows 95, NetWare, and FreeBSD guests. See “Run or Disable a Script” on page 126.

Shared Folders Tab Information

The **Shared Folder** tab of the VMware Tools control panel tab is available only on newer Windows guests and only when shared folders are enabled. It provides information on how to access your shared folders on the host, so you can share files between the host and guest.

With a shared folder, you can share files between two virtual machines and between a virtual machine and the host operating system, even if one has a Windows operating system and the other has Linux or Solaris.

Although the **Shared Folders** tab does not appear in Linux or Solaris guests, you can share folders with Linux and Solaris guests. See “Set Up Shared Folders” on page 178.

The shared folders feature works only when the virtual machine is running under newer versions of some VMware products and only when shared folders are enabled for the virtual machine. Shared folders are not supported with Windows 95, Windows 98, Windows Me, and FreeBSD guest operating systems.

Shrink Tab Settings

The **Shrink** tab of the VMware Tools control panel provides options for reclaiming unused space in a virtual disk. If your virtual machine cannot be shrunk, this tab displays information explaining why you cannot shrink your virtual disks.

Shrinking a disk is a two-step process: a preparation step and the shrink step. In the first step, VMware Tools reclaims all unused portions of disk partitions (such as deleted files) and prepares them for shrinking. This step takes place in the guest operating system.

The shrink process is the second step, and it takes place outside the virtual machine. The VMware application reduces the size of the disk based on the disk space reclaimed during the preparation step. If the disk has empty space, this process reduces the amount of space the virtual disk occupies on the host drive. See "Shrink a Virtual Disk" on page 224.

On UNIX guests, run VMware Tools as the root user (**su**) to shrink virtual disks. If you shrink the virtual disk as a nonroot user, you cannot prepare to shrink the parts of the virtual disk that require root-level permissions.

About Tab

The **About** tab displays version (build number) and copyright information.
In Windows guests, this tab also shows the status of the VMware Tools service.

Configure VMware Tools in a NetWare Guest

In a NetWare virtual machine, using the system console, you can configure certain virtual machine options such as time synchronization, CPU idling, and device configuration with VMware Tools. The VMware Tools command-line program is called `vmwtool`.

To configure VMware Tools in a NetWare Guest

1 Open a terminal window (system console) in the NetWare guest.

2 Enter a command that uses the following format:

```
vmwtool <command>
```

`<command>` is one of the commands listed in Table 5-1.

Table 5-1. vmwtool Commands

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

Customizations to VMware Tools

Customizations include modifying or writing scripts that run when a virtual machine's power state changes, executing commands when you shut down or restart a UNIX guest, and passing commands in strings that run in startup scripts.

How VMware Tools Scripts Affect Power States

When VMware Tools is installed, if you configure a virtual machine's power controls to use the guest, or soft, power options, one or more default scripts run on the guest whenever you change the power state of the virtual machine. You change the power state by using menu commands or by clicking the **Suspend**, **Resume**, **Power On**, and **Power Off** buttons.

What the default scripts do depends in part on the guest operating system:

- On most Microsoft Windows guests, but not windows NT and Windows Me, the default script executed when you suspend a virtual machine releases the IP address of the virtual machine. The default script executed when you resume a virtual machine renews the IP address of the virtual machine (this affects only virtual machines configured to use DHCP). Scripts cannot be run on Windows 95 guests.

  In Windows guests, the default scripts are located in the `Program Files\VMware\VMware Tools` folder.

- On most UNIX guests, the default script executed when you suspend a virtual machine stops networking for the virtual machine. The default script executed when you resume a virtual machine starts networking for the virtual machine. Scripts cannot be run on NetWare and FreeBSD guests.

  On UNIX, the default scripts are located in the `/etc/vmware-tools` directory.

You can create your own scripts and use them instead of the default scripts shown in Table 5-2.

Table 5-2. Default VMware Tools Scripts

Script Name	Description
`poweroff-vm-default`	If you configured the power-off operation to shut down the guest, this script runs when the virtual machine is being powered off. If you configured the reset operation to restart the guest, this script runs when the virtual machine is being reset. This script has no effect on networking for the virtual machine.
`poweron-vm-default`	If you configured the power-on operation to start the guest, this script runs when the virtual machine is being powered on rather than resumed. If you configured the reset operation to restart the guest, this script runs after virtual machine restarts. This script has no effect on networking for the virtual machine.
`resume-vm-default`	If you configured the power-on operation to start the guest, or the reset operation to restart the guest, this script runs when the virtual machine is resumed after it was suspended. On Windows guests, if the virtual machine is configured to use DHCP, this script renews the IP address of the virtual machine. On Linux, FreeBSD, and Solaris guests, this script starts networking for the virtual machine.
`suspend-vm-default`	If you configured the suspend operation to suspend the guest, this script runs when the virtual machine is being suspended. On Windows guests, if the virtual machine is configured to use DHCP, this script releases the IP address of the virtual machine. On Linux, FreeBSD, and Solaris guests, this script stops networking for the virtual machine.

Create Scripts to Override Default VMware Tools Scripts

You can create your own scripts to override the default VMware Tools scripts that control power state changes.

Scripts are run by the VMware Tools daemon (`VMwareService.exe on` Windows and `vmware-guestd` on UNIX). Because `vmware-guestd` is run as root on UNIX and as System on Windows, the scripts are run in a separate session from the logged-in user’s session. The VMware Tools daemon has no knowledge of desktop sessions, which means that it cannot display graphical applications. Do not attempt to use custom scripts to display graphical applications.

Before creating custom scripts, make sure that the following conditions are met in the guest operating system:

- The virtual machine is using the latest version of VMware Tools.
- The VMware Tools service is running in the virtual machine.
- Depending on the operation the script performs, the virtual machine has a virtual network adapter connected. If not, the power operation fails.
- (UNIX guests only) To edit a script by using the **Edit** button on the **Scripts** tab, `xterm` and `vi` must be installed in the guest operating system and must be in your PATH. You must be a root user to edit the script.

To create scripts to override default VMware Tools scripts

1. Determine whether you want to create your custom script by making changes to the default script and saving it to a new location.

   In Windows guests, the default scripts are located in the `Program Files\VMware\VMware Tools` folder.

   On UNIX, the default scripts are located in the `/etc/vmware-tools` directory.

2. Modify the default script and save it with a different name or write a different script.

   On Windows guests, if you write a new script, create the script as a batch file. For UNIX, create the script in any executable format (such as shell or Perl scripts).

   You can also use the **Edit** button on the **Scripts** tab of the VMware Tools control panel to edit a custom script. You can also edit scripts manually using any text editor.

3. Associate each custom script with its particular power operation:

   a. On the **Scripts** tab of the VMware Tools control panel, select the appropriate script event.

   b. Select the **Use Script** check box, select **Custom script**, and use the **Browse** button to point to the script you want to use.

   c. Click **OK**.

When you reinstall VMware Tools after you update the Workstation software, any changes you made to the default scripts are overwritten. Any custom scripts you created remain untouched, but do not benefit from any underlying changes that enhance the default scripts.

Run or Disable a Script

If you are creating a custom script, run the script before associating it with a power operation.

To run or disable a script

1 On the **Scripts** tab of the VMware Tools control panel, select the appropriate script event.

2 Do one of the following:

- To disable the script, clear the **Use Script** check box and click **OK**.

  Default scripts for suspending and resuming work together. If you disable the script of one of these actions, disable the script for the other action as well.

- To run a script immediately, click **Run Now**.

  You can successfully run a script by clicking the **Run Now** button in the VMware Tools control panel, but this same script can fail when run as part of a Workstation power operation. This is because scripts run by clicking **Run Now** are run as the logged-in user and have a different working directory than when scripts are run by the VMware Tools daemon during a power operation.

Execute Commands After You Power Off or Reset a Virtual Machine

In a Linux, Solaris, or FreeBSD guest, you can use the VMware Tools service to execute specific commands when you shut down or restart the guest operating system. This is in addition to any script that you specified to run when you shut down the guest operating system.

1 Use a text editor to open the following file:

```
/etc/vmware-tools/tools.conf
```

2 Add one or both of the following commands to the file:

- **`halt-command`** `= <command>`

  `<command>` is the command to execute when you shut down the guest operating system.

- **`reboot-command`** `= <command>`

  `<command>` is the command to execute when you restart the guest operating system.

Passing a String from the Host to the Guest at Startup

To pass a string from the host to the guest at startup, you pass the string from your virtual machine's configuration file in the host to the guest operating system when you power on the virtual machine.

You can pass items like the Windows system ID (SID), a machine name, or an IP address. Inside the guest operating system startup script, you can have the service retrieve this string. The string can then be used in another script to set your virtual machine's system ID, machine name, or IP address.

Use this strategy, for example, to make copies of the same configuration file, add a different string to each (either in the configuration file itself or at the command line), and use these variations of the same configuration file to launch the same virtual disk in nonpersistent mode multiple times in a training or testing environment.

Passing a string is also useful when you want to deploy virtual machines on a network using a common configuration file while providing each machine with its own unique identity.

You can pass strings to a virtual machine's guest operating system in one of two ways: placing the string in the virtual machine's configuration file or passing the string to the guest from the command line.

Use this feature only if you have a good understanding of a scripting language (for example, Perl or NetShell) and know how to modify system startup scripts.

String in a Configuration File

Place a string in the virtual machine's configuration file (`.vmx` file) by setting the string to the `machine.id` parameter. For example, you can set this string:

```
machine.id = "Hello World."
```

Following is an example of portions of two configuration files that point to the same virtual disk. Each configuration file contains its own unique string set for the `machine.id` parameter.

`config_file_1.vmx` contains:

```
ide0:0.present = TRUE
ide0:0.fileName = "my_common_virtual_hard_drive.vmdk"
machine.id = "the_string_for_my_first_vm"
```

`config_file_2.vmx` contains:

```
ide0:0.present = TRUE
ide0:0.fileName = "my_common_virtual_hard_drive.vmdk"
machine.id = "the_string_for_my_second_vm"
```

To prevent a string from being passed from the host to the guest through the service, set the following line in your virtual machine's configuration file:

```
isolation.tools.getMachineID.disable = "TRUE"
```

String in a Startup Command

Rather than setting the `machine.id` parameter in the configuration file, you can pass the string to the guest operating system from the command line when you power on the virtual machine. Following is an example of such a startup command (entered on one line):

```
“C:\Program Files\VMware\VMware Workstation\vmware –s
              'machine.id=Hello World'
              C:\Virtual Machines\win2000\win2000.vmx”
```

Use this method to deploy virtual machines on a network using a common configuration file while providing each machine with its own unique identity.

Launch each virtual machine with the **`vmware –s`** command. Each virtual machine disk file must be copied into its own directory if it shares its filename with another virtual machine disk file.

On a Linux host, the machine ID passed on the command line takes precedence and is passed to the guest operating system if the following conditions are met:

- A virtual machine ID is specified in the virtual machine's configuration (`.vmx`) file which is used to open the virtual machine.
- You specify a machine ID on the command line.

Use a String in a Startup Script to Set a Name and IP Address

The following example uses a Windows host to illustrate how you can use the service to retrieve a string containing what becomes the virtual machine's machine name and IP address. In this example, W2K-VM is the machine name and 148.30.16.24 is the IP address.

To use a string in a startup script to set a name and IP address

1. Define the string by using one of the following methods:

   - On the host machine, add the following line to your virtual machine's configuration file (`.vmx` file):

     ```
     machine.id = "W2K-VM 148.30.16.24"
     ```

     Open the virtual machine using this configuration file.

   - Open the virtual machine from the command line by entering the following on one line:

     ```
     "C:\Program Files\VMware\VMware Workstation\vmware -s
     'machine.id=W2K-VM 148.30.16.24' C:\Virtual
     Machines\win2000\win2000.vmx"
     ```

2. Do one of the following to retrieve the string in the virtual machine:

   - In a Windows guest, enter the following command to retrieve the string:

     ```
     VMwareService --cmd machine.id.get
     ```

   - In a Linux guest, in the operating system's startup script, add the following command before the network startup section. For example:

     ```
     /usr/sbin/vmware-guestd --cmd 'machine.id.get'
     ```

     The location of `vmware-guestd` depends on the directory you specify at the time of installation.

3. Further customize this startup script so that it uses the string the service retrieved during startup to set the virtual machine's network name to W2K-VM and its IP address to 148.30.16.24.

4. Place this string in the script before the command to start the network services.

   If you're using a Windows 2000 guest operating system, for example, you can call the NetShell utility (`netsh`) and pass it the contents of the string, which uses the string accordingly. That is, it can set a new IP address for the virtual machine, if that is what was passed in the string originally.

Passing Information Between the Guest and Another Program

The VMware Tools service allows you to use VMware programmatic interfaces to manage virtual machines from your own independent programs and from existing frameworks developed by partners and third parties.

For more information about the VMware Infrastructure SDK, go to the VMware APIs and SDKs Documentation page of the VMware Web site.

Use the VMware Tools Command-Line Interface

The VMware Tools command-line interface enables you to do the following:

- Configure time synchronization in your Linux guest operating system without running X.
- Install and uninstall VMware Tools, determine the version, and so on.

To use the VMware Tools command-line interface

1 On the guest operating system, change directories to the directory that contains the VMware Tools daemon.

Depending on the operating system, the name and default location of the daemon are as follows:

- On Microsoft Windows systems, the daemon is called `VMwareService.exe` and the location is:

```
C:\Program Files\VMware\VMware Tools\VMwareService.exe
```

- On UNIX systems, the daemon is called `vmware-guestd.` The location of `vmware-guestd` depends on the directory you specify at the time of installation. The default location is:

```
/usr/sbin/vmware-guestd
```

2 To configure periodic time synchronization, use the `vmx.set_option` command.

Use the following syntax:

```
<daemon> --cmd "vmx.set_option synctime <old_val> <new_val>"
```

`<daemon>` is **`vmware-guestd`** on UNIX systems or **`VMwareService.exe`** on Windows systems.

`<old_val>` and `<new_val>` are the old and new values, respectively. Use 0 to mean FALSE and 1 to mean TRUE.

Following is an example of setting time synchronization to TRUE on a Linux guest:

```
./vmware-guestd --cmd "vmx.set_option synctime 0 1"
```

The new setting is written to the `tools.syncTime` property in the virtual machine's configuration `(.vmx)` file. Using this option is equivalent to using the time synchronization option on the **Options** tab of the VMware Tools control panel.

3 To use commands other than `--cmd`, use the `--help` command-line command.

Creating a Virtual Machine from a System Image or Another Virtual Machine

6

This chapter describes how to convert a physical machine, virtual machine, or system image to a VMware virtual machine. On Windows hosts, you can convert a virtual machine that was created by using a VMware product or a third-party product.

This chapter includes the following topics:

Conversion Process for Importing from Other Formats

On Windows hosts, Workstation 6.5 incorporates the Conversion wizard from the VMware Converter product. Using the Conversion wizard to perform a conversion to VMware virtual machines enables you to do the following:

- Avoid reinstalling operating systems and applications for system configurations you use often.
- Overcome legacy migration barriers. Certain legacy systems might be impossible to recreate through reinstallation.
- Convert a physical machine into a virtual machine.

- Use virtual machines or system images created with products from other companies such as Norton, Symantec, and StorageCraft.
- Convert virtual appliances that use open virtualization format (OVF).

Workstation provides two ways to convert a virtual machine or system image:

- Using the **File > Open** command converts and opens a virtual machine or system image quickly. Workstation uses default settings to make the conversion automatically, with no input required from you. The original Microsoft Virtual PC, Symantec Backup Exec System Recovery, StorageCraft ShadowProtect, or Acronis True Image (`.vmc`, `.spf`, `.sv2i`, or `.tib`) file is unchanged.

  For all supported file types except `.ovf` and `.ova` files, the **File > Open** command creates a linked clone when it opens the file. If you open a virtual appliance that uses `.ovf` or `.ova` files, Workstation creates a full clone.

  If you attempt to open a virtual machine or system image that is password protected, you are prompted for the password, and Workstation creates a full clone.

- Using the **File > Import or Export** command starts the Conversion wizard. It lets you specify the converted virtual machine's location, whether or not the converted virtual machine shares virtual disks with the original virtual machine or system image, and which versions of VMware products the converted virtual machine is to be compatible with.

The wizard creates a completely new VMware virtual machine based on the input virtual machine or system image. The newly migrated VMware virtual machine retains the configuration of the original virtual machine or image.

The migration process can be nondestructive, so you can continue to use the original virtual machine with Microsoft Virtual PC, or the original system image with Symantec Backup Exec System Recovery. However, to run a new VMware virtual machine on the same network as the original Virtual PC virtual machine, you must modify the network name and IP address on one of the virtual machines so the original and new virtual machines can coexist.

For Microsoft Virtual PC and Microsoft Virtual Server virtual machines, you have the option of sharing the source virtual hard disk (`.vhd`) files. This means that the VMware virtual machine can write directly to the original `.vhd` files instead of VMware virtual hard disk (`.vmdk`) files.

VMware Converter Compared to the Conversion Wizard

Workstation 6.5 incorporates the Conversion wizard from the VMware Converter product. VMware Converter is a separate downloadable application for Windows hosts that provides an easy-to-use, scalable solution for migrations of machines, both physical to virtual and virtual to virtual. In addition to the Conversion wizard, VMware Converter provides a task manager that lets you schedule migrations of many machines.

The Conversion wizard included with Workstation lets you create VMware virtual machines from a local or remote physical machine or from virtual machines and system images that were originally created by using other products than VMware products. You can also use the wizard to change a virtual machine using one VMware format to that using another. For example, you can copy a VMware Server virtual machine and use it to create an ESX virtual machine.

To use other features of VMware Converter, such as its task manager, or the ability to import more than one virtual machine at a time, download the VMware Converter.

Supported Source Machines

The VMware Conversion wizard in Workstation allows you to import the following types of physical and virtual machines:

- Physical machines
  - Windows 2000
  - Windows Server 2003 32-bit and 64-bit
  - Windows XP Professional 32-bit and 64-bit
  - Windows Vista 32-bit and 64-bit
- VMware virtual machines (`.vmx` and `.vmtn` files)
  - Workstation 4.5, 5.x, 6.0.x, and 6.5
  - VMware ACE 1.x, 2.0.x, and 2.5
  - VMware Fusion 1.x and 2.0.x
  - VMware Player 1.x and 2.x
  - ESX Server 3.x
  - ESX Server 2.5.x (if the virtual machine is managed with VirtualCenter 2.x)
  - VMware Server 1.x and 2.0 x (if the virtual machine is on the local file system)
  - VirtualCenter 2.x

- Virtual appliances

  Appliances that use open virtualization format (`.ovf` and `.ova` files) and that use VMware virtual hard disks (`.vmdk` files).

- Other virtual machines and system images

  - Acronis True Image 9 (`.tib` files)
  - StorageCraft ShadowProtect (`.spf` files)
  - Microsoft Virtual PC 7.x and higher (`.vmc` files)
  - Any version of Microsoft Virtual Server (`.vmc` files)
  - Symantec Backup Exec System Recovery (formerly LiveState Recovery) 6.5 and 7.0, LiveState Recovery 3.0 and 6.0 (`.sv2i` files)
  - Norton Ghost images 9.x and higher (`.sv2i` files)

  The operating system on the source Microsoft Virtual PC or Virtual Server virtual machine must be a Windows 2000 or later guest operating system supported by the intended VMware platform (for example, Workstation 4, 5, or 6). For a list of supported operating systems, see the *VMware Guest Operating System Installation Guide*, available from the VMware Web site.

NOTE Virtual machines from Macintosh versions of Microsoft Virtual PC are not supported.

Operating System Compatibility

To import a virtual or physical machine or a third-party image, the operating system on which Workstation is installed must be equal to or greater than the operating system on the source machine. For example, if Workstation is installed on a Windows 2000 machine, you cannot import a virtual machine from a Windows XP or Windows 2003 source machine.

Importing from Various Sources

Keep these points in mind when using the Conversion wizard.

Physical Machine Source

To import a remote machine, you are prompted to supply the computer name or IP address and the user name and password for logging in to the machine with administrative privileges. The user name must take the form `<DOMAIN>\<user_name>`.

NOTE Remote physical machines cannot be imported into an ESX-compatible format by the wizard.

Microsoft Virtual PC and Virtual Server Virtual Hard Disks

As of Workstation 6.5, a converted virtual machine can share the source Microsoft virtual hard disk (`.vhd` files). This means that the VMware virtual machine can write directly to the original `.vhd` files instead of VMware virtual hard disk (`.vmdk`) files.

If you select **Share source** the converted virtual machine consists of a VMware virtual machine configuration file (`.vmx` file) and the original `.vhd` file, which remains in its original location. VMware modifies the `.vhd` file, installing VMware-specific video drivers, device drivers for virtual network cards, and so on. The VMware -specific drivers replace the Microsoft drivers.

ShadowProtect and Backup Exec System Recovery Images

You can import ShadowProtect and Backup Exec System Recovery images, but keep the following limitations in mind:

- Dynamic disks are not supported.
- All images for the backup of a machine should be in a single folder, with no other images placed there.
- All volumes in the disk up to the active and system volumes must be backed up. For example, if a disk has four partitions, 1–4, with partition 2 as the active volume and partition 3 as the system volume, the backup must include 1 through 3.
- If it is an incremental image, up to 16 incremental backups are supported.
- For ShadowProtect, images of systems with logical drives are not supported if the logical drive is also a system or active volume.

Appliances That Use Open Virtualization Format

Open virtualization format (OVF) is a platform-neutral, secure, and portable format for packaging and distributing virtual appliances. Although OVF does not rely on a specific virtualization platform, the Conversion wizard supports only OVF appliances that use VMware virtual hard disks (`.vmdk` files).

In the Conversion wizard, you can select `.ovf` files, which are the OVF equivalent of a VMware virtual machine configuration file (`.vmx` file), or you can select `.ova` files (open virtual appliance files). An `.ova` file stores the configuration file and virtual hard disk file together, like a `.zip` file, for easy distribution.

When specifying the location of the OVF appliance, you can browse to a directory or use a URL to download the appliance from a Web server. You can also download the appliance from a secure (HTTPS) Web server.

NOTE When you use a URL, the virtual appliance is downloaded before the conversion process starts. Downloading can take 15 minutes or longer, depending on the size of the file.

The Conversion wizard always makes a full clone when it converts an OVF appliance to a virtual machine. See “Full or Linked Clones” on page 137.

Dual-Boot System Source

When you import a physical machine that is part of a dual-boot system, you can import only the default operating system to which `boot.ini` points. To import the nondefault operating system, change `boot.ini` to point to the other operating system and reboot before attempting to import. Even if `boot.ini` points to the correct operating system, occasionally, the virtual machine might not be bootable in the default operating system.

Windows NT Virtual Machine Source

If the source virtual machine is Windows NT SMP, the wizard might require files from service packs or hot fixes. The wizard shows which files it requires. You must browse to the required files. They can be on a disk, your local system, or the network.

On Windows NT machines, during the import process, a snapshot driver is downloaded to the machine. This driver handles the copying and moving of files and registry settings. The driver requires a reboot to complete its tasks. When it is finished, the driver is uninstalled.

NOTE Although Windows NT virtual machines are supported as a source, Windows NT physical machines are not supported.

ESX Virtual Machine Source

You must supply the name of the ESX server and the user name and password for logging in.

Password-Protected Virtual Machines

If the virtual machine you want to import is password protected, you must supply the password.

About Page Files and Hibernation Files

You can import all the disks for the physical or virtual machine or, to save space, you can select some of the volumes and leave out others. If you select specific volumes, you can also ignore the page and hibernation files. These files are large and, for volume-based cloning, do not provide information that you need to copy.

Supported Volume Types

Some types of source volumes, or partitions, are unsupported and are skipped during cloning. Virtual machine importing supports basic volumes and all types of dynamic volumes except RAID. Only Master Boot Record (MBR) disks are supported. GUID Partition Table (GPT) disks are not supported.

Disk Space Allocation

As is the case when you use the New Virtual Machine wizard, you must specify whether to allocate all the space at creation time or allow the files to grow. Allocating space at creation time gives you better performance but is a time-consuming process. VMware recommends that you allow the disk to grow.

Select the option **Split disk into 2GB files** if your virtual disk is stored on a file system that does not support files larger than 2GB.

Full or Linked Clones

If the source is a virtual machine, you can create a full or linked clone. On the Virtual Machines Options page of the Conversion wizard, select **Import and Convert** to create a full clone. Select **Share source and store changes separately** to create a linked clone.

NOTE For Microsoft Virtual PC and Virtual Server virtual machines, you have a third option. Instead of creating a full or linked clone, you can have the converted virtual machine use the original Microsoft virtual hard disk. This option modifies the source virtual machine. See "Microsoft Virtual PC and Virtual Server Virtual Hard Disks" on page 135.

Linked clones can be created from VMware virtual machines, Symantec Backup Exec System Recovery virtual machines (`.sv2i` files), Microsoft Virtual PC and Virtual Server virtual machines, Acronis True Image (`.tib` files), and StorageCraft files (`.spf` files). Creating a linked clone of a VMware virtual machine requires that the virtual hardware version of the destination machine not be higher than the hardware version of the source.

CAUTION For linked clones, the virtual machine created by the wizard becomes corrupted if the source is modified after the import. This is true for linked clones imported from Virtual PC and Virtual Server machines and from Symantec backup images. In the case of Virtual PC and Virtual Server source virtual machines, powering them on in Virtual PC or Virtual Server modifies them.

Supported Destinations

The Conversion wizard can create virtual machines that are compatible with the following products:

- Workstation 4.5, 5.x, 6.0.x, and 6.5
- VMware ACE 1.x, 2.0.x, and 2.5
- VMware Fusion 1.x and 2.0.x
- VMware Player 1.x and 2.x
- ESX Server 3.x (This destination is not supported if you are importing a remote physical machine.)
- ESX Server 2.5.x (This destination is supported only by importing through a VirtualCenter 2.x server that manages the 2.5.x ESX Server.)
- VMware Server 1.x and 2.0.x (if the virtual machine is on the local file system)
- VirtualCenter 2.x

NOTE Workstation 4 virtual machines are compatible with VMware GSX Server 3.0, ESX Server 2.x, and ACE 1.x.

Designating a Destination for a Virtual Machine

Keep these points in mind when using the Conversion wizard to specify a destination for a newly created virtual machine.

ESX Virtual Machine Destination

You must supply the name of the ESX server and the user name and password for logging in.

VirtualCenter Virtual Machine Destination

You must provide the following information:

- Name of the VirtualCenter server and the user name and password for logging in.
- Name of the folder in the VirtualCenter inventory where you want to store the virtual machine.
- Name of the host, cluster, or resource pool within a host or cluster from which the virtual machine is to be run. If you select a cluster in manual mode, you must also choose a specific host.
- Name of the datastore for the virtual machine's configuration files and disks. Use the advanced setting to distribute the virtual machine's disks over multiple datastores.

Network Adapters

You are prompted to choose from the available networks at the destination location. For more information about networking choices for virtual machines used with Workstation rather than ESX or Virtual Center, see "Common Networking Configurations" on page 266.

Optional Guest Operating System Customization

You can make changes to the identity of the virtual machine (such as computer name and security ID), networking information, and so on with the wizard. For virtual machines that are converted to ESX virtual machines, you can have the wizard install VMware Tools if the guest operating system is Windows 2000 or later.

You can make the following customizations:

- Computer information
  - **Computer name** – Alphanumeric name of up to 63 characters. Hyphens and underscores are allowed.
  - **Security ID (SID)** – Optionally, generate a new security ID.
  - **Sysprep file location** – If the wizard can detect the location, the wizard page displays it. Otherwise, you need to supply the location.
- Windows licensing information
  - **Product ID** – Optional.
  - **Windows Server license information** – For Microsoft Windows 2000 Server and 2003 Server only.
- Time zone
- Network information
  - **Network adapter (interfaces)** – Reset to default or make changes.
  - **DHCP** – Choose between using DHCP to obtain IP addresses or entering them manually. You can also use DHCP to obtain a DNS server address or enter it manually.
  - **DNS** – Enter DNS suffixes and customize their order to specify the order in which a virtual machine uses them to make connections.
  - **WINS** – Specify primary and secondary WINS addresses.
  - **Workgroup or domain** – For workgroups, specify the workgroup name, up to 15 characters. For domains, specify the Windows Server domain, along with the appropriate user name and password.

Conversion Impact on Settings

The VMware virtual machine created by the Conversion wizard contains an exact copy of the disk state from your source virtual machine or system image, with the exception of some hardware-dependent drivers and, sometimes, the mapped drive letters.

The following settings from the source computer remain identical:

- Operating system configuration (computer name, security ID, user accounts, profiles and preferences, and so forth)
- Applications and data files
- Each disk partition's volume serial number

Because the target and the source virtual machines or system images have the same identities (name, SID, and so on), running both on the same network can result in conflicts. If you plan to redeploy the source virtual machine or system image, do not run both the source and target images or virtual machines on the same network at the same time.

Alternatively, you can resolve the duplicate ID problem by using additional tools, such as the Windows 2000 System Preparation Tool (Sysprep). For example, if you use the Conversion to test the viability of running a Virtual PC virtual machine as a VMware virtual machine without first decommissioning the original Virtual PC machine, you need to resolve the duplicate ID problem.

Migration Issues Caused by Hardware Changes

Most migrated applications function correctly in the VMware virtual machine because their configuration and data files have the same location as the source virtual machine. However, applications might not work if they depend on specific characteristics of the underlying hardware such as the serial number or the device manufacturer.

When troubleshooting after virtual machine migration, consider the following potential hardware changes:

- The CPU model and serial numbers (if activated) can be different after the migration. They correspond to the physical computer hosting the VMware virtual machine.
- The network adapter can be different (AMD PCNet or VMXnet) with a different MAC address. Each interface's IP address must be individually reconfigured.
- The graphics card can be different (VMware SVGA card).
- The numbers of disks and partitions are the same, but each disk device can have a different model and different manufacturer strings.
- The primary disk controllers can be different from the source machine's controllers.
- Applications might not work if they depend on devices that are not available from within a virtual machine.

Open a Third-Party Virtual Machine or System Image

The **File > Open** command lets you convert a virtual appliance, system image, or virtual machine created with software from another company into a VMware virtual machine.

To open a third-party virtual machine or system image

1 From the Workstation menu bar, choose **File > Open**.

2 In the **File name** field, browse to and open the configuration (`.vmx`, `.vmc`, `.spf`, `.ovf`, `.ova`, or `.sv2i`) file for the virtual appliance, virtual machine, or system image to convert.

You can use the field **Files of type** to filter the files displayed by file extension.

3 Click **Open**.

Workstation creates a VMware virtual machine, with a VMware configuration file (`.vmx`) for the converted virtual machine or system image. The converted virtual machine links to the virtual disks of the original virtual machine or system image unless the source uses open virtualization format (`.ovf` or `.ova` files). The original Virtual PC, Symantec Backup Exec System Recovery, or StorageCraft configuration (`.vmc`, `.spf`, or `.sv2i`) file is unchanged.

If you open a virtual appliance that uses `.ovf` or `.ova` files, Workstation creates a full clone.

If you attempt to open a virtual machine or system image that is password protected, you are prompted for the password, and Workstation creates a full clone.

Import a Virtual Machine, Virtual Appliance, or System Image

The **File > Import or Export** command enables you to convert a system image or virtual machine into a VMware virtual machine.

Before you begin, review the restrictions and requirements for source and destination virtual machines. See "Supported Source Machines" on page 133 and "Supported Destinations" on page 138.

To import a virtual machine, virtual appliance, or system image

1 If you are importing a virtual machine, make sure the virtual machine is powered off.

2 Choose **File > Import or Export** to launch the VMware Conversion wizard.

3 Complete the wizard pages.

The text on the wizard pages changes, depending on the selections you make. For example, on the Source Type page, when you select a source type from the drop-down list, the text below the list changes to describe which types of virtual machines are included in that source type.

As you proceed through the wizard, the navigation pane on the left side of the wizard helps track your progress.

Whenever you start a new phase or step, a list expands to display the names of the wizard pages included in that step. When you complete an entire step, the next step expands.

To go back to a previous page, click its name in the navigation pane.

Getting Started with Virtual Machines 7

This chapter includes the following topics:

Starting a Virtual Machine

Starting a virtual machine means displaying its running console so that you can interact with it. Depending on the situation, starting a virtual machine can involve any of the following:

- To start a virtual machine from the Workstation user interface, you must open the virtual machine and power it on.

- To start a virtual machine that is running in the background when Workstation is not running, you must open its console from the taskbar on the host.

- To start a virtual machine that is available from a Web server, you must use a command-line command to begin streaming the virtual machine and then start it from the Workstation window.
- To start a virtual machine from the command line, you must use the platform-specific program and startup options. See "Startup Options for Workstation and Virtual Machines" on page 467.

Start a Virtual Machine from the Workstation User Interface

Before you begin, make sure that all of the virtual machine files are accessible to the host where Workstation is installed.

You can add the name of the virtual machine to the **Favorites** list so that you do not need to browse to the file to open the virtual machine. See "Favorites List in the Sidebar" on page 61.

To start a virtual machine from the Workstation user interface

1. Start Workstation.

   For instructions, see "Start Workstation on a Windows Host" on page 51.

2. Choose **File > Open** and browse to the configuration file (`.vmx` file) for the virtual machine.

   See "Virtual Machine Location" on page 148.

3. Choose **VM > Power** > **Power On**.

   If you ever need to enter the BIOS setup for the guest operating system, choose **VM > Power > Power On to BIOS**.

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

5. To log on to the operating system in the virtual machine, type your name and password just as you would on a physical computer.

Start a Virtual Machine That Is Running in the Background

If you do not power off a virtual machine when you exit Workstation, the virtual machine continues to run in the background. To start the virtual machine, use the power status icon on the host to open the virtual machine's console.

By default Workstation is configured to display a power status icon in the notification area of the host's taskbar even when Workstation is not running.

If this icon is not visible, before you begin, use the **Workspace** tab of the Workstation preferences editor to display it. See "Introduction to Workstation Preferences" on page 65.

To start a virtual machine that is running in the background

1. Click the power status icon in the notification area of the host's taskbar.
2. Select a virtual machine from list that appears in the tooltip.

   The list contains the virtual machines and teams that belong to the user who is logged in.

   Workstation starts and displays the console view of the virtual machine.

Start a Virtual Machine by Using VM Streaming

Beginning with Workstation 6.5, you can now stream a virtual machine from a Web server. You can start the virtual machine shortly after the download process begins.

Before you begin, determine the URL of the virtual machine and verify that the Web server on which it resides is correctly configured. See "Make Virtual Machines Available for Streaming from a Web Server" on page 214.

To start a virtual machine by using VM streaming

1. Open a command prompt or terminal window.
2. Use the platform-specific command with the URL of the virtual machine:

   - On Windows hosts, use **`vmware.exe http://`**`<path_to_vm>`**`.vmx`**.
   - On Linux hosts, use **`vmware http://`**`<path_to_vm>`**`.vmx`**.

   HTTPS is also supported.

3. When a tab for the virtual machine opens in the Workstation window, choose **VM > Power > Power On**.

   Virtual disk data is fetched on demand so that you can begin using the virtual machine before the download completes.

   The status bar indicates the progress of the download. Point to the icon on the status bar for VM streaming and a tooltip indicates whether streaming is active and provides the URL of the Web server.

4. (Optional) To save the virtual machine so that you can use it when you do not have access to the Web server, choose **VM > Save for Offline Use**.

   Using this setting also allows you to pause downloading by powering off the virtual machine before streaming is finished. You can restart later by powering on the virtual machine. It also allows you to use the **File > Open** command to open the virtual machine after you close it.

When you power off a streamed virtual machine, you are prompted to save or discard changes. If you discard changes, the directory that was created on your local machine and all the virtual machine data are deleted.

Virtual Machine Location

By default, virtual machine files are stored in the virtual machine's working directory:

- On Windows hosts, Workstation stores virtual machines in the `My Documents` folder of the user who is logged in at the time the virtual machine is created.

  On Windows Server 2003, Windows XP, and Windows 2000, the default folder is:

  ```
  C:\Documents and Settings\<username>\My Documents\My Virtual
                 Machines\<guestOSname>
  ```

  On Windows Vista, the default folder is:

  ```
  C:\Users\<username>\Virtual Machines\<guestOSname>
  ```

- On Linux hosts, Workstation stores virtual machines in:

  ```
  <homedir>/vmware/<guestOSname>
  ```

  Here <`homedir`> is the home directory of the user who is logged in at the time the virtual machine is created.

The working directory is also where Workstation stores suspended state (`.vmss`), snapshot (`.vmsn`), and redo log files. The **General** tab of the virtual machine settings editor displays the path to the working directory. See"Introduction to Virtual Machine Settings" on page 67.

Shut Down a Virtual Machine

As with physical computers, you can shut down a guest operating system before you power off the virtual machine or team.

You are not required to shut down the guest before you exit Workstation. To exit Workstation but leave the virtual machine running in the background, see "Closing Virtual Machines and Exiting Workstation" on page 69.

To shut down a virtual machine

1 In the guest system, shut down the operating system as you would if you were using a physical machine rather than a virtual machine.

For example, in Windows XP, click **Start > Shut Down**.

2 In the Workstation menu bar, choose **VM > Power Options > Power Off** to turn off the virtual machine.

If you use the **Power Off** command before you shut down the guest operating system, the virtual machine is powered off abruptly. The effect is like using the power button on a physical machine. You can, however, configure the **Power Off** button in the toolbar to shut down the operating system before powering off. See "Configure Power Off and Reset Options for a Virtual Machine" on page 149.

Configure Power Off and Reset Options for a Virtual Machine

You can configure the **Power Off** toolbar button to power off the virtual machine abruptly or to send a signal that gracefully shuts down the guest operating system.

Before you begin, make sure VMware Tools is installed in the guest operating system. To perform a graceful shutdown, the VMware Tools service component issues a **Shutdown Guest** command and runs a script to shut down gracefully.

CAUTION Powering off abruptly works the same way a power switch works on a power supply. The power is cut off with no consideration for work in progress. If a virtual machine is writing to disk when it receives a **Power Off** command, data corruption might occur.

Similarly, you can configure the **Reset** button to work the same way as a reset switch, so that it resets the virtual machine abruptly. Or you can configure the **Reset** button so that the VMware Tools service sends a restart signal to the guest operating system. It then shuts down gracefully and restarts.

Not all guest operating systems respond to a shutdown signal from the **Power Off** button, or to a restart signal from the **Reset** button. If your operating system does not respond to the signal, shut down or restart from the operating system, as you would with a physical machine.

To configure the Power Off and Reset options for a virtual machine

1. Select the virtual machine.

   The virtual machine can be powered on or off.

2. Choose **VM > Settings**.

3. Click the **Options** tab and select **Power**.

4. In the **Power Controls** section of the dialog box, set the **Power Off** button to shut down the guest gracefully or to abruptly power the virtual machine off.

   The selection you make is reflected in the tooltip you see when you point to the **Power Off** button.

5. Specify how you want the **Reset** button to work.

6. If you want to change any of the other settings and need more information, click **Help**.

   For UNIX guests, to pass X toolkit options when you power on a virtual machine, see Appendix A, "Workstation Command-Line Reference," on page 467.

Delete a Virtual Machine

You can use a Workstation command to delete a virtual machine and all of its files from the host file system.

If, instead of deleting the virtual machine altogether, you want to remove it from the **Favorites** list or from a team, see "Remove an Item from the Favorites List" on page 62 or "Remove a Virtual Machine from a Team" on page 258.

CAUTION Do not delete a virtual machine if it was used to make a linked clone virtual machine and you still want to use the linked clone. If the linked clone cannot find the virtual disk files from the parent virtual machine, the linked clone stops working.

To delete a virtual machine

1. Select the virtual machine.

2. Make sure the virtual machine is powered off.

3. Choose **VM > Delete from Disk**.

Controlling the Virtual Machine Display

You can control the way Workstation displays virtual machines and their applications. For example, you can use full screen mode to hide the host user interface altogether, or you can use Unity mode so that applications from the virtual machine appear on the host desktop and hide the rest of the virtual machine user interface.

Using Unity Mode

In virtual machines with Linux or Windows 2000 or later guest operating systems, you can switch to Unity mode to display applications directly on the host desktop.
The taskbar displays items for open applications in Unity mode just as it does for open host applications.

The virtual machine console view is hidden, and you can minimize the Workstation window.

You can use keyboard shortcuts to copy, cut, and paste text between applications on your host machine and virtual machine applications displayed in Unity mode. You can also drag and drop and copy and paste files between host and guest.

NOTE If you save a file or attempt to open a file from an application in Unity mode, the file system you see is the file system inside the virtual machine. You cannot open a file from the host operating system or save a file to the host operating system.

When a virtual machine is in Unity mode, you can access the virtual machine's **Start** menu (for Windows virtual machines) or **Applications** menu (for Linux virtual machines) by pointing to one of the following locations:

- On Windows hosts, point to the **Start** menu.
- On Linux hosts, point to the upper-left corner of the primary monitor.

For this release, the Unity feature has the following limitation: For some guest and host operating systems, if you have multiple monitors, application windows in Unity mode can appear only on the monitor that is set as the primary display. If the host and guest are Windows XP or later, the application windows can appear on additional monitors.

Set Preferences for Unity Mode

You can configure Unity mode so that you can access a virtual machine's **Start** or **Applications** menu from the host's desktop. You can also specify the border color around applications that run in Unity mode on the desktop.

Accessing a virtual machine's **Start** or **Applications** menu from the host's desktop enables you to start applications in the virtual machine that are not open in Unity mode. If you do not enable this feature, you must exit Unity mode to display the virtual machine's **Start** or **Applications** menu in the console view.

To help distinguish between the application windows that belong to various virtual machines, you can give them different colors. For example, you can set the applications for one virtual machine to have a blue border and set the applications for another virtual machine to have a yellow border.

You can also set a Workstation preference to minimize the Workstation window when you enter Unity mode.

To set preferences for Unity mode

1. Select the virtual machine.
2. Choose **VM > Settings**.
3. Click the **Options** tab and select **Unity**.
4. Complete the settings panel and click **OK**.

   Use the following information to determine which features to enable:

   - To identify the application as belonging to this virtual machine rather than the host, use the **Show borders** check box to set a window border. Use the **Show badges** check box to display a logo in the title bar.
   - To use a custom color, click the colored rectangle to access the color chooser on Linux hosts. On Windows hosts, click **Choose color**.
   - If you select the **Enable applications menu** check box, one of the following menus appears when you point to correct location on the host's desktop:
     - A **Start** menu appears on Windows guests.
     - An **Applications** menu appears on Linux guests.

     On Windows hosts, point to the **Start** menu. On Linux hosts, point to the upper-left corner of the primary monitor. The menu has the same color border as the virtual machine application windows.

5 Repeat this process for each virtual machine that you plan to use in Unity mode.

6 (Optional) To automatically minimize the Workstation window when you enter Unity mode, do the following:

   a Choose **Edit > Preferences**.

   b Click the **Display** tab.

   c Select **Minimize Workstation when entering Unity** and click **OK**.

   This Workstation preference is used for all virtual machines.

Enter and Exit Unity Mode

In Unity mode, a virtual machine's applications look like other application windows on the host, except that they have a colored window border and a VMware logo in the window's title bar.

Before you begin, make sure the virtual machine meets these requirements:

- The virtual machine must be a Workstation 6 or higher virtual machine.
- VMware Tools must be installed and running in the virtual machine's guest operating system. The version of VMware Tools must be the version included in Workstation 6.5 or higher. For instructions, see "Installing VMware Tools" on page 100.
- The guest operating system in the virtual machine must be Linux or Windows 2000 or later.
- For Linux guests and hosts, VMware recommends that you use a modern version of Metacity or KDE. Performance on Linux depends on a combination of variables such as the system, the applications that are running, and the amount of RAM.

To enter and exit Unity mode

1 In the virtual machine, open the applications to use in Unity mode.

2 From the Workstation menu bar, choose **View > Unity**.

   A check mark appears next to **Unity** in the menu.

   The virtual machine's console view in the Workstation window is hidden, and the guest's open applications appear in application windows on the host's desktop.

   You can also enter Unity mode from full screen mode.

3 To exit Unity mode, display the Workstation window and choose **View > Unity** to remove the check mark next to **Unity**, or click **Exit Unity** in the virtual machine's console view.

Access a Virtual Machine’s Start or Applications Menu in Unity Mode

If configured to do so, a virtual machine in Unity mode can display a **Start** or **Applications** menu above the host’s **Start** or **Applications** menu. This feature enables easy access to applications in the virtual machine that are not open in Unity mode.

Before you begin, verify that the virtual machine is configured to use this feature. See “Set Preferences for Unity Mode” on page 152.

To access a virtual machine’s Start or Applications menu in Unity mode

1. To enter Unity mode, power on a virtual machine, open one or more applications, and choose **View > Unity** from the Workstation menu bar.

2. To display the virtual machine’s **Start** or **Applications** menu on the host, do one of the following:

   - Point to the **Start** menu on Windows hosts or to the upper-left corner of the primary monitor on Linux hosts.

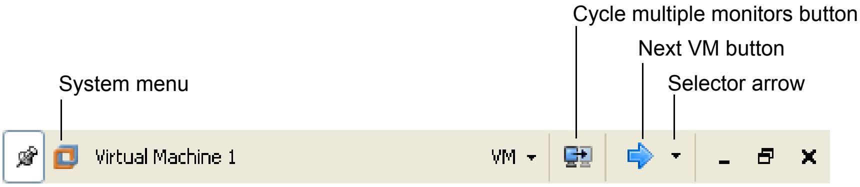
   - Press Ctrl+Shift+V.

     If you have multiple virtual machines in Unity mode, you can navigate between multiple **Start** and **Applications** menus by using standard navigation keys such as arrow keys, Tab, and Shift+Tab. You can select one by using standard keys such as Enter and the space bar.

Use Full Screen Mode

In full screen mode, the virtual machine display fills the screen, so that you cannot see the borders of the Workstation window.

Figure 7-1. Full Screen Toolbar on a Windows Host



Before you begin, make sure the guest operating system has VMware Tools installed. See “Installing VMware Tools” on page 100.

NOTE If you plan to run the virtual machine in full screen mode on a laptop computer, also set the guest to report battery information. See “Report Battery Information in the Guest” on page 157.

To use full screen mode

1. Select the virtual machine and make sure it is powered on.

2. If you have multiple monitors, move the Workstation window into the monitor to use for full screen mode.

3. Choose **View > Full Screen**.

   If you cannot enter full screen mode when the guest's display mode is smaller than the host's display mode, try adding the following line to the virtual machine's configuration (`.vmx`) file:

   ```
   mks.maxRefreshRate=1000
   ```

   For more information about the configuration file, see "Files That Make Up a Virtual Machine" on page 93.

4. (Optional) You can perform the following optional tasks:

   - To switch from full screen mode back to windowed mode, which shows the virtual machine inside a Workstation window again, press Ctrl+Alt+Enter.

   - To hide the full screen toolbar and menus while you are using full screen mode, click the push pin icon and move the pointer off of the toolbar.

     This action unpins the toolbar. The toolbar slides up to the top of the monitor and disappears. To display the toolbar again, point to the top of the screen until the toolbar appears.

     If you cannot display the full screen toolbar, see "Set Preferences for Autofit, Full Screen Mode, and Unity Mode" on page 156.

   - To switch from one powered-on virtual machine to another while in full screen mode, do one of the following:

     - To go to a specific powered-on virtual machine, click the virtual machine arrow, as shown in Figure 7-1, and select the virtual machine.

     - To go to the next virtual machine, press Ctrl+Alt+right arrow, or press Ctrl+Alt+left arrow to go to the previous virtual machine.

   - Use the **VM** menu on the toolbar to access the Workstation **VM** menu commands.

   - Use the **System** menu to switch to Unity mode or exclusive mode, or to use the autofit command to adjust screen resolution.

   - To display the virtual machine across two or more monitors in full screen mode, see "Use Multiple Monitors for One Virtual Machine" on page 159.

Set Preferences for Autofit, Full Screen Mode, and Unity Mode

You can set preferences for how the display settings of all virtual machines adjust to fit the Workstation window. These adjustments occur when you resize the Workstation window or when you change the display settings inside the guest.

You can also configure how the host and guest display settings interact when you enter full screen mode and Unity mode.

Before you begin, make sure that VMware Tools is installed in the guest operating systems in the virtual machines.

To set preferences for autofit, full screen mode, and Unity mode

1. Choose **Edit > Preferences**.
2. Click the **Display** tab.
3. Select one or more check boxes in the **Autofit** section.
4. Use the following information to help you complete the **Full Screen** section:
   - Select **Autofit guest** to change the guest's resolution settings to match the display settings of the host while you are in full screen mode.
   - Select **Stretch guest** to retain the guest's resolution settings but still have the display fill the full screen.

     This setting is useful if you need to retain a guest's low-resolution settings. For example, use this setting to play older computer games that run only at low resolutions.
   - Select **Center guest** to have both host and guest retain their own display settings while you are in full screen mode.
   - If you deselect **Show toolbar edge when unpinned**, you will not be able to display the full screen toolbar by placing your mouse cursor near the top of the screen. To display it again, use the preferences editor and select **Show toolbar edge when unpinned** again.
5. If you plan to have multiple virtual machines running, with some in Unity mode and some accessible only in the Workstation window, do not select the **Minimize Workstation when entering Unity** check box.
6. Click **OK**.

Report Battery Information in the Guest

If you run a virtual machine on a laptop in full screen mode, configure the option to report battery information in the guest. This way, you can determine when the battery is running low.

To report battery information in the guest

1. Select the virtual machine.
2. Make sure the virtual machine is powered off.
3. Choose **VM > Settings**.
4. Click the **Options** tab and select **Power**.
5. Select the **Report battery information to guest** check box and click **OK**.

Use Quick Switch Mode

In quick switch mode, the virtual machine's screen is resized to fill the screen completely, except for the space that the tabs occupy.

Before you begin, make sure the guest operating system has VMware Tools installed. See "Installing VMware Tools" on page 100.

Quick switch mode is similar to full screen mode with the addition of tabs at the top of the screen for switching from one virtual machine to another. The other difference is that you can use quick switch mode with virtual machines that are powered on or off.

To use quick switch mode

1. Select the virtual machine.
2. Choose **View > Quick Switch**.
3. (Optional) To view the Workstation menu and toolbar while using quick switch mode, point to the top of the screen.
4. (Optional) To resize a guest operating system's display so that it fills as much of the screen as possible in quick switch mode, choose **View > Fit Guest Now**.
5. To exit quick switch mode, point to the top of the screen and choose **View > Quick Switch**.

Use Exclusive Mode

You might want to use exclusive mode to run graphics-intensive applications, such as games, in full screen mode.

Before you begin, make sure the guest operating system has VMware Tools installed. See "Installing VMware Tools" on page 100.

Like full screen mode, exclusive mode causes the Workstation virtual machine display to fill the screen. Drawbacks to using exclusive mode include the following:

- The full screen toolbar is not available in exclusive mode. To configure any virtual machine settings, you need to exit exclusive mode (press Ctrl+Alt).
- Exclusive mode does not use multiple monitors.
- Exclusive mode causes the host resolution to resize, which can cause items on the host desktop to be moved.

To use exclusive mode

1. Select the virtual machine.
2. Make sure the virtual machine is powered on.
3. If you have multiple monitors, move the Workstation window onto the monitor you want to use.
4. Press Ctrl+Alt+Enter.
5. On the full screen toolbar, do one of the following:
    - On Windows hosts, click the **Workstation** icon to display the system menu and choose **Exclusive Mode**.
    - On Linux hosts, click the **View** menu on the full screen toolbar and choose **Exclusive Mode**.
6. To exit exclusive mode and return to windowed mode, press Ctrl+Alt.

Use Multiple Monitors for One Virtual Machine

If your host has a multiple-monitor display, you can configure a virtual machine to use two or more monitors.

On Windows guests, you do not need to use the Windows display properties settings to configure multiple monitors.

Before you begin, make sure the virtual machine meets these requirements:

- The virtual machine is a Workstation 6 or higher virtual machine.
- VMware Tools is installed and running in the virtual machine's guest operating system. The version of VMware Tools must be the version included in Workstation 6 or higher. For instructions, see "Installing VMware Tools" on page 100.
- The guest operating system in the virtual machine is Windows XP, Windows Vista, or Linux.
- On the host, the display settings for monitors must be set in a compatible topology. For example, the left-most monitor cannot be placed lower than any other monitor in the display topology. It does not matter if the monitors have different resolutions or orientations. When entering full screen mode, the monitor that contains the Workstation window cannot be lower than another monitor.

  Put another way: When you use the Windows display properties controls, if you select a monitor icon and begin to drag it to a new location, a tooltip displays the coordinates. If a coordinate shown for the new location of the icon is a negative number, that location will not work.

To use multiple monitors for one virtual machine

1. Choose **Edit > Preferences**.
2. Click the **Display** tab and in the **Full Screen** section, select **Autofit guest** and click **OK**.
3. Select a virtual machine.
4. Make sure the virtual machine is powered off.
5. Choose **VM > Settings**.
6. On the **Hardware** tab, select **Display**.

   If **Display** does not appear in the list on the **Hardware** tab, it probably means that the virtual machine is a Workstation 4 or 5 virtual machine. Only Workstation 6 or higher virtual machines have this feature.

7 On the settings panel for the **Display** tab, specify how to determine the number of monitors.

In most cases, select **Use host setting for monitors**. If the virtual machine is run on a host that is using one monitor, the virtual machine detects only one monitor. But if the same virtual machine is moved to a host that is using two monitors, the virtual machine detects two monitors.

The number of monitors depends on the number of monitors that the host recognizes at startup. For example, if you power on a laptop that is undocked, the host setting is one monitor, even if you later place the running laptop in a docking station that uses two monitors.

Similarly, if the host has one monitor and you suspend the virtual machine and change the host to have two monitors, when you resume the virtual machine, it is still configured to use one monitor. You must restart the virtual machine to detect the new settings.

You might want to set a specific number of monitors if, for example, you are writing an application to be displayed on multiple monitors but the host you are using has only one monitor.

8 If you set a specific number of monitors, specify a sufficient maximum resolution.

The resolution of a host monitor that you use to display the virtual machine must not exceed the **Maximum resolution** setting that you specify.

9 Power on the virtual machine and choose **View > Full Screen**.

For more information, see "Use Full Screen Mode" on page 154.

Make sure the virtual machine is completely powered on. If when you power on the virtual machine, it is set to be restored from a snapshot and if background snapshots are enabled, powering on might take longer. In this case, displaying the virtual machine to two monitors might not work correctly at first. If you see this issue, go to **Edit > Preferences > Priority** and deselect the check box called **Take and restore snapshots in the background**.

10 On the full screen toolbar, click the **Cycle Multiple Monitors** button.

This button is available only if the host has multiple monitors. This button is shown in Figure 7-1, "Full Screen Toolbar on a Windows Host," on page 154.

Clicking the **Cycle Multiple Monitors** button causes the guest operating system's desktop to extend to the additional monitor or monitors.

If the virtual machine does not appear correctly, use the system menu (on Windows hosts) or the **View** menu (on Linux hosts) and select **Autofit Guest**.

11 If you have more than two monitors, and you want the virtual machine to use them, click the **Cycle Multiple Monitors** button again.

   The order in which the monitors are used depends on the order in which the monitors were added to the host operating system.

12 To return to using only one monitor, click the **Cycle Multiple Monitors** button until the display returns to one monitor.

Use Multiple Monitors for Multiple Virtual Machines

If your host has a multiple-monitor display, you can run a different virtual machine on each monitor.

Before you begin, make sure the guest operating system has VMware Tools installed. See "Installing VMware Tools" on page 100.

To use multiple monitors for multiple virtual machines

1 To open multiple Workstation windows, choose **File > New > Window**.

   On Linux hosts, although you can have multiple Workstation windows, the windows operate in a single Workstation process, which saves memory and allows preferences and **Favorites** list items to be shared.

2 (Optional) On Linux hosts, to run separate Workstation processes in different X servers, start the second instance of Workstation with the `–W` flag.

   In a terminal window, enter the following command:

```
vmware –W &
```

3 Start one or more virtual machines in each Workstation window.

   If you have a virtual machine running in one window and you want to run that virtual machine in another Workstation window, close the virtual machine in the first window before you attempt to open it in another.

4 Drag each Workstation window to the monitor on which you want to use it.

5 To switch mouse and keyboard input from the virtual machine on the first monitor to the virtual machine on the second monitor, move the mouse pointer from one screen to the other and click inside the second monitor.

Fitting the Workstation Console to the Virtual Machine Display

The **Autofit** and **Fit** commands in the **View** menu allow you to match the Workstation console with the guest operating system display size.

With both **Autofit** commands toggled off, Workstation does not automatically match window sizes as you work. Scroll bars appear in the console when the Workstation console is smaller than the guest operating system display. A black border appears in the console when the console is larger than the guest operating system display.

The **Autofit** and **Fit** commands are described in Table 7-1.

Table 7-1. Autofit and Fit Commands

View Menu Command	Description
Autofit Window	Causes the Workstation console to maintain the size of the virtual machine's display resolution. If the guest operating system changes its resolution, the Workstation console resizes to match the new resolution.
Autofit Guest	Causes the virtual machine to resize the guest display resolution to match the size of the Workstation console.
Fit Window Now	Causes the Workstation console to match the current display size of the guest operating system.
Fit Guest Now	Causes the guest operating system display size to match the current Workstation console.

An **Autofit** command is toggled on or off each time you select it. If **Autofit Window** and **Autofit Guest** are toggled on, you can manually resize the Workstation console, but the guest operating system can also resize the Workstation console.

The **Fit Window Now** or **Fit Guest Now** command is redundant if the corresponding Autofit command is active because the console and the guest operating system display are the same size.

Display Resizing in Linux Guests

For Linux guests, the following considerations apply to display resizing:

- If you have virtual machines that were suspended under a version of VMware Tools earlier than version 5.5, display resizing does not work until the virtual machines are completely powered off and powered on again. (Rebooting the guest operating system is not sufficient.)
- Update VMware Tools to the latest version in the guest for the display resizing options to work.

- Before you can use the **Autofit Guest** and **Fit Guest Now** options, VMware Tools must be running.
- All the restrictions for resizing that the X11 Windows system imposes on physical hosts apply to guests:
  - You cannot resize to a mode that is not defined. The VMware Tools configuration script can add a large number of mode lines, but you cannot resize in 1-pixel increments as you can in Windows. VMware Tools adds modelines in 100-pixel increments. This means you cannot resize a guest larger than the largest mode defined in your X11 configuration file. If you attempt to resize larger than that mode, a black border appears and the guest stops increasing.
  - The X server always starts up in the largest resolution that is defined. You cannot avoid this restriction. The XDM/KDM/GDM login screen always appears at the largest size. But Gnome and KDE allow you to specify your preferred resolution, so that you can reduce the guest display size after you log in.

Display Resizing in Solaris Guests

For Solaris 10 guests, the following considerations apply to display resizing:

- Update VMware Tools to version 6.0 or higher in the guest for the display resizing options to work.
- Before you can use the **Autofit Guest** and **Fit Guest Now** options, VMware Tools must be running.
- Solaris 10 guests must be running an Xorg X server and JDS/Gnome.

Working with Nonstandard Resolutions

A guest operating system and its applications might react unexpectedly when the Workstation console size is not a standard VESA resolution (640×480, 800×600, 1024×768, and so on).

For example, the **Autofit Guest** and **Fit Guest Now** commands allow your guest operating system screen resolution to be set smaller than 640×480, but some installers do not run at resolutions smaller than 640×480. Programs might refuse to run. Error messages might include such phrases as “VGA Required to Install” or “You must have VGA to install.”

Use one of the following strategies to work around this problem with nonstandard resolutions:

- If your host computer’s screen resolution is high enough, you can enlarge the window and choose **Fit Guest Now**.
- If your host computer’s screen resolution does not allow you to enlarge the Workstation console sufficiently, you can manually set the guest operating system’s screen resolution to 640×480 or larger.

Configuring Video and Sound

For best color and graphics display, you must coordinate host and guest color settings. Workstation also supports games and applications that use DirectX 9 accelerated graphics, but you must perform some 3-D preparation tasks on the host and guest.

With regards to sound support, Workstation usually installs the necessary drivers, but on some of the oldest and newest guest operating systems, you must manually install a driver.

Setting Screen Color Depth

The number of screen colors available in the guest operating system depends on the screen color setting of the host operating system.

Virtual machines support:

- 16-color (VGA) mode
- 8-bit pseudocolor
- 16 bits per pixel (16 significant bits per pixel)
- 32 bits per pixel (24 significant bits per pixel)

If the host is in 15-bit color mode, the guest operating system’s color setting controls offer 15-bit mode in place of 16-bit mode.

If the host is in 24-bit color mode, the guest operating system’s color setting controls offer 24-bit mode in place of 32-bit mode.

If you run a guest operating system set for a greater number of colors than your host operating system is using, you can encounter problems. In some cases, for example, the colors in the guest are not correct. In others, the guest operating system cannot use a graphical interface.

You can try either of the following solutions:

- Increase the number of colors available on the host.
- Decrease the number of colors used in the guest.

For best performance, use the same number of colors in the guest and on the host.

Changing Screen Color Depth on the Host

If you choose to change the color settings on the host operating system, shut down all guest operating systems, power off the virtual machines, and close Workstation.

Follow standard procedures for changing the color settings on your host operating system and restart Workstation and the virtual machines.

Changing Screen Color Depth in the Guest

The approach you take to change the color settings in the guest operating system depends on the guest operating system.

Follow the process for changing screen colors in the guest operating system:

- In a Windows guest, the Display Properties control panel offers only those settings that are supported.
- In a Linux or FreeBSD guest, you must change the color depth before you start the X server, or you must restart the X server after making the changes.

Support for Direct3D Graphics

To take advantage of the 3-D capabilities of Workstation, the virtual machine must be running the version of VMware Tools included with Workstation 6.5 or higher.
For example, you do not need to upgrade a Workstation 6.0 virtual machine to Workstation 6.5, but you do need to upgrade the VMware Tools running inside it. If you move the virtual machine and want to use the 3-D capabilities, be sure you have the correct version of VMware Tools installed.

Accelerated 3-D Restrictions

Support for applications that use DirectX 9 accelerated graphics applies only to Windows XP guests, on hosts running Windows 2000, Windows XP, Windows Vista, or Linux.

This feature currently has the following restrictions:

- Workstation now offers support for DirectX games and applications with DirectX versions 9 and lower.
- Support for 3-D applications is not optimized for performance.
- OpenGL applications run in software emulation mode.
- You cannot use the record/replay feature to record a 3-D application.

Prepare a Host for Accelerated 3-D

By default, Direct3D technology is enabled for Workstation 6 and later virtual machines. You must prepare the host first, the virtual machine second, and the guest operating system last.

Before you begin, make sure the host operating system is Windows 2000, Windows XP, Windows Vista, or Linux. For Windows hosts, make sure you have a video card that supports DirectX 9 and the latest DirectX Runtime. For Linux hosts, make sure the host has a video card that can run accelerated OpenGL 2.0. If you are unsure, check with your hardware manufacturer.

To prepare a host for accelerated 3-D

1 Upgrade the host's video drivers to the latest version available:

  a ATI Graphics drivers are available from the AMD Web site.

  b NVIDIA drivers are available from the NVIDIA Web site.

2 If you are using a Windows XP host, turn up hardware acceleration in the display properties:

  a Right-click the desktop and choose **Properties > Settings > Advanced > Troubleshoot**.

  b Move the **Hardware Acceleration** slider all the way to the **Full** position.

3 If you are using Linux, test your Linux host for compatibility:

  a To verify that direct rendering is enabled, run:

```
glxinfo | grep direct
```

  b To ensure that 3-D applications work on your host, run:

```
glxgears
```

After your host is configured, configure a virtual machine for accelerated 3-D.

Prepare a Virtual Machine for Accelerated 3-D

Before you begin, make sure the guest operating system is Windows XP.

To prepare a virtual machine for accelerated 3-D

1 Select the virtual machine.

2 Make sure the virtual machine is powered off rather than suspended.

3 Choose **VM > Settings.**

4 On the **Hardware** tab, select **Display**.

5 In the **Monitors** section, if the virtual machine is set to use more than one monitor, set it to use only one monitor.

6 In the **3D Graphics** section, make sure the check box is selected and click **OK**.

Prepare the Guest Operating System for Accelerated 3-D

Before you begin, make sure the guest operating system is Windows XP and make sure the latest version of VMware Tools is installed. See "Installing VMware Tools" on page 100.

To prepare the guest operating system for accelerated 3-D

1 Power on the virtual machine.

2 Install DirectX 9.0c End User Runtime.

This download is available from Microsoft Download Center.

3 Install and run your 3-D applications.

Configuring Sound

Workstation provides a sound device compatible with the Sound Blaster AudioPCI and supports sound in Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000, Windows XP, Windows Server 2003, and Linux guest operating systems. The Workstation sound device is enabled by default.

Sound support includes pulse code modulation (PCM) output and input. For example, you can play `.wav` files, MP3 audio, and Real Media audio. MIDI output from Windows guests is supported through the Windows software synthesizer. MIDI input is not supported, and no MIDI support is available for Linux guests.

Windows 2000, Windows XP, and most recent Linux distributions automatically detect the sound device and install appropriate drivers for it.

For Windows Vista, when you install VMware Tools in a 64-bit Windows Vista guest operating system, a sound driver is installed. For 32-bit Windows Vista guests and Windows 2003 Server guests, use Windows Update to install a 32-bit driver.

Installing Sound Drivers in Windows 9x and NT Guests

Windows 95, Windows 98, Windows 98SE, and Windows NT 4.0 do not have drivers for the Sound Blaster AudioPCI adapter. To use sound in these guest operating systems, download the driver from the Creative Labs Web site and install it in the guest operating system.

Creative Labs has a number of Web sites serving various regions of the world. The adapter name varies, depending on the region, but usually includes PCI 128.

Install New Software in a Virtual Machine

Installing new software in a virtual machine is like installing it on a physical computer. Only a few additional steps are required.

To install new software in a virtual machine

1 Select the virtual machine.

2 Choose **VM > Removable Devices** and verify that the virtual machine has access to the CD-ROM drive, ISO image file, or floppy drive where the installation software is located.

For more information, see "Add DVD or CD Drives to a Virtual Machine" on page 234.

3 Choose **VM > Settings** and use the **Memory** settings panel on the **Hardware** tab to set the final memory size for the virtual machine.

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 might require you to reactivate the software. To minimize the number of significant changes, set the memory size.

4 Install VMware Tools in the guest operating system.

See "Installing VMware Tools" on page 100. Installing VMware Tools before installing the new application also minimizes the likelihood of requiring you to reactivate the software.

5 Install the new application according to the manufacturer's instructions.

Disable Acceleration If a Program Does Not Run

Occasionally, when you install or run software inside a virtual machine, Workstation appears to freeze. In many cases, you can get past the problem by temporarily disabling acceleration in the virtual machine.

If this problem occurs, it usually occurs early in the program's execution.

To disable acceleration

1 Select the virtual machine.

The virtual machine can be powered off or on.

2 Choose **VM > Settings**.

3 On the **Hardware** tab, select **Processors**.

4 In the **Execution Mode** section, select **Disable acceleration for binary translation** and click **OK**.

This setting slows down virtual machine performance. VMware recommends that you use the setting only for getting past the problem with running the program.

5 After you pass the point where the program encountered problems, repeat Step 2 through Step 4 and deselect **Disable acceleration for binary translation**.

Use Removable Devices in a Virtual Machine

You can configure a number of removable devices for use in a virtual machine, including floppy drives, DVD/CD-ROM drives, USB devices, smart card readers, and network adapters.

Some devices cannot be used by the host and guest or by multiple guests at the same time. For example, if the host is using a floppy drive, you must connect it to the virtual machine before you can use it in the virtual machine. To use it on the host again, you must disconnect it from the virtual machine.

For information about how to add or configure specific devices, see Chapter 16, "Connecting Devices," on page 313 and Chapter 11, "Using Disks and Disk Drives," on page 219.

To use removable devices in a virtual machine

1 Select the virtual machine.

2 Make sure the virtual machine is powered on.

3 Choose **VM > Removable Devices > <Device_Name>** and then **Connect**, **Disconnect**, or one of the other choices.

   If you choose **Settings**, a dialog box appears. Make the desired changes and click **OK**. If you need assistance, click **Help** to display online help.

   If the device is a USB device, you can change which icon is used to represent this device in the status bar. You can also choose not to display an icon for this device.

4 (Optional) To connect, disconnect, or change settings for a device, click or right-click the device icon in the notification area of the taskbar and choose a command from the context menu.

   Using the device icon in the virtual machine taskbar is especially useful if you run the virtual machine in full screen mode.

Configure the Appliance View for a Virtual Machine

To have a virtual machine function as an appliance, such as a Web server with a browser-based interface, set the virtual machine to display its appliance view when starting up.

Before you begin, verify that the virtual machine is a Workstation 6 or higher virtual machine. For instructions on upgrading, see "Change the Version of a Virtual Machine" on page 91.

The appliance view does the following:

- Displays a brief description of the type of server or appliance
- Provides a link that opens the browser on the host system and connects to the appliance's management console

NOTE The appliance view cannot be displayed for virtual machines that are part of a team, just as the summary view is not displayed for individual members of a team.

To configure the appliance view for a virtual machine

1 (Optional) To use a logo in the appliance view, create a PNG, GIF, or BMP image file that is no larger than 256 x 256 pixels and place it in the directory that contains the `.vmx` file for the virtual machine.

2 Select the virtual machine.

   The virtual machine can be powered on or off.

3 Choose **VM > Settings**.

4 Click the **Options** tab and select **Appliance View**.

5 Select the **Enable appliance view** check box.

6 Complete the fields on this settings panel to create the text and images that users see when the virtual machine starts up.

   Use the following information to configure the settings on this panel:

   - Only the **Name** field is required.
   - Specify the TCP/IP port number for the appliance to use to serve HTTP content.
   - If you do not select **Switch to appliance view at power on**, the console view appears instead of the appliance view. Often the console view shows only a simple display of the virtual machine's IP address and tells the user to open a browser.

7 Click **OK**.

When a user starts this virtual machine, the appliance view appears. A "powering on" message appears, followed by a link to access the appliance's management console.

Create a Screenshot of a Virtual Machine

You can capture a screenshot of a virtual machine and save it to the clipboard, to a file, or both. On Linux hosts, saving to the clipboard works only on systems running Gnome 2.12 or higher.

By default, the image is saved as a portable network graphics (`.png`) file. On Windows hosts, you can also save it as a bitmap (`.bmp`) file.

To create a screenshot of a virtual machine

1 Specify your preferences for taking screenshots:

   a From the Workstation menu bar, choose **Edit > Preferences**.

   b On the **Workspace** tab, use the **Save screenshots to** check boxes to specify whether to save the screenshot to the clipboard, a file, or both.

   c If you select **File**, specify whether to save the file to your desktop or to be prompted for the location when you take the screenshot.

   If you select **Save to desktop**, the filename is generated automatically from the virtual machine name and the time at which the screenshot is taken. The file format is `.png` file.

   On Windows hosts, if you select **Ask for location**, when you are prompted for the filename and path, you can also change the file format to bitmap.

   d Click **OK**.

2 To take the screenshot, do one of the following:

- From the Workstation menu bar, choose **VM > Capture Screen**.
- Press Ctrl+Alt+PrtScr (on Windows hosts) or Shift+Ctrl+PrtScr (on Linux hosts).

  The keyboard shortcut works regardless of whether mouse and keyboard input is currently grabbed by the virtual machine or the host.

  The key combination Ctrl+Alt+PrtScr assumes that your virtual machine is configured to ungrab keyboard and mouse input if you press Ctrl+Alt. If you configured a different shortcut for ungrabbing input, use that shortcut with the PrtScr key. See "Change the Hot-Key Combination" on page 71.

Create and Play Back a Movie of a Virtual Machine

You can capture a movie of your screen activity within a virtual machine.

Before you begin, make sure you have the VMware movie decoder. Although you can capture a movie on Linux, you need to play it back on a Windows machine. The VMware CODEC (coder-decoder) is automatically installed with Workstation on Windows hosts. A separately downloadable installer is also available to play back movies on Windows machines without Workstation. Go to the Downloads page on the VMware Web site and click the **Tools & Drivers** tab on the VMware Workstation download page.

NOTE To actually record the execution of the virtual machine instead of creating a movie, see Chapter 12, "Recording and Replaying Virtual Machine Activity," on page 239. You might want to record virtual machine execution for debugging purposes or to exactly reproduce the steps that cause a certain behavior.

To create and play back a movie of a virtual machine

1 Select the virtual machine.

2 Make sure the virtual machine is powered on.

3 Choose **VM > Capture Movie**.

4 In the Save File dialog box, enter information for your movie and click **Save**.

Use the following guidelines:

- The **Quality** setting determines the compression and therefore the file size of the resulting movie.
- If you select **Omit frames in which nothing occurs**, the movie includes only those periods when something is actually happening in the virtual machine. This reduces the file size and length of the movie.

While movie capture is active, a red circle (a virtual LED) appears in the notification area of the taskbar.

5 In the virtual machine, perform the actions to appear in the movie.

6 To stop the movie, choose **VM > Stop Movie Capture**.

If you do not want to use the menu bar or if you are using the virtual machine in full screen mode, right-click the movie capture icon and choose **Stop Movie Capture**.

Workstation saves this image as an `.avi` file on the host.

7 Play the movie back in any compatible media player.

Advanced Options for Application Developers

Application developers can use the following APIs, SDKs, and IDEs when writing and debugging applications that run in virtual machines:

- **VIX API for writing programs to automate virtual machine operations** – The API is high-level, easy to use, and practical for both script writers and application programmers. API functions allow you to register, power on or off virtual machines, and run programs in the guest operating systems. Additional language bindings are available for Perl, COM, and shell scripts (`vmrun`). For more information, see the VMware VIX API Release Notes.
- **VAssert API for inserting replay-only code to debug applications** – The experimental VAssert feature enables you to use virtual assertions as you would regular assertions in the applications you develop. VAsserts appear only when you replay a recording of using the application and so are overhead free. This API is currently available only for Windows guests. See the *VAssert Programming Guide*.

- **VProbes tool for investigating guest behavior** – You can write VProbes scripts that inspect and record activities in the guest, VMM, VMX, and virtual device state, without modifying that state. For example, VProbes can track which applications are running or indicate which processes are causing page faults. See the *VProbes Programming Reference*.
- **VMCI Sockets interface** – This feature is a sockets interface for the Virtual Machine Communication Interface, which provides a faster means of communication among applications running on the host and in virtual machines. This feature is well-suited for developers who want to write client-server applications. See the *VMCI Sockets Programming Guide*.
- **Integrated Virtual Debuggers for Visual Studio and Eclipse** – The integrated development environment (IDE) plug-ins provide a configurable interface between virtual machines and Visual Studio or Eclipse that lets you test, run, and debug programs in virtual machines. See Appendix B, "Using the Integrated Virtual Debugger for Eclipse," on page 471 and Appendix C, "Using the Integrated Virtual Debugger for Visual Studio," on page 483.

Transferring Files and Text Between the Host and Guest

8

This chapter discusses how to transfer files between the host and guest. This chapter includes the following topics:

Using Drag-and-Drop

To use the drag-and-drop feature, VMware Tools must be installed on the virtual machine. This feature requires Linux hosts and guests to run X Windows and Solaris 10 guests to run an Xorg X server and JDS/Gnome. With this feature, you can move files and directories easily between Linux and Windows hosts and Linux, Windows, and Solaris 10 guests. However, the drag-and-drop feature does not work on Windows 95 and Windows 98 guests.

You can drag-and-drop files or folders from the following locations:

- A file manager, such as Windows Explorer, on the host to a file manager in the virtual machine and the reverse.
- A file manager to an application that supports drag-and-drop.
- Applications such as zip file managers that support drag-and-drop extraction of individual files.
- One virtual machine to another.

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

Initially, the application opens using a copy of the file that is stored in your temp directory. On Windows, this is the file specified in the `%TEMP%` environment variable, and on Linux and Solaris, it is the `/tmp/VMwareDnD` directory. To protect any changes you make, choose **File > Save As** from the application's menu and save the file in a different directory.

Enable or Disable Drag-and-Drop

To prevent files from being transferred between the virtual machine and the host, disable the drag-and-drop feature. Before you begin, make sure VMware Tools is installed on the virtual machine.

To enable or disable drag-and-drop

1. Start Workstation and select the virtual machine.
2. Choose **VM > Settings**.
3. Click the **Options** tab and select **Guest Isolation**.
4. Select or deselect the **Enable drag and drop** check box and click **OK**.

Using Copy and Paste

To use the copy and paste feature, VMware Tools must be installed on the virtual machine. This feature requires Linux hosts and guests to run X Windows and Solaris 10 guests to run an Xorg X server and JDS/Gnome. Copying and pasting text and files works with Linux and Windows hosts and Linux, Windows, and Solaris 10 guests. However, this feature does not work on Windows 95, 98, and NT guests.

You can cut or copy and paste text from one virtual machine to another, but you cannot copy and paste files between virtual machines. You can cut or copy and paste text between applications in the virtual machine and the host computer or between two virtual machines. Use the normal hot keys or menu choices to cut or copy and paste.

Enable or Disable Copy and Paste

To prevent accidental copying and pasting from one environment to another, disable this feature. Before you begin, VMware Tools must be installed on the virtual machine.

To enable or disable copy and paste

1. Select the virtual machine.
2. Choose **VM > Settings**.
3. Click the **Options** tab, and select **Guest Isolation**.
4. Select or deselect the **Enable copy and paste** check box and click **OK**.

Using Shared Folders

With shared folders you can share files among virtual machines and the host computer. You choose a directory on the host or on a network directory that is accessible to the host, and you give it the name you want to use on the guest.

You can use shared folders with virtual machines running the following guest operating systems and on all supported host systems:

- Windows Server 2003
- Windows XP
- Windows 2000
- Windows NT 4.0
- Windows Vista
- Linux with a kernel version of 2.4 or higher
- Solaris x86 10
- Solaris x86 10 Update 1 and higher

Set Up Shared Folders

Shared folders provide an easy way to share files among virtual machines, and between virtual machines and the host. The directories you add as shared folders can be on the host computer or they can be network directories accessible from the host computer.

Before you begin, make sure the following prerequisites are satisfied:

- Make sure the virtual machines use a guest operating system that supports shared folders. For a list of supported guest operating systems, see "Using Shared Folders" on page 177.
- Verify that the current version of VMware Tools installed in the guest operating system. See "Installing VMware Tools" on page 100.
- Check permission settings. Access to files in the shared folder is governed by permission settings on the host computer. For example, if you are running Workstation as a user named User, the virtual machine can read and write files in the shared folder only if User has permission to read and write them. For information about how permission setting are mapped between Linux and Windows, see "Improved Handling of Permissions" on page 184.

To set up a folder for sharing between virtual machines, configure each virtual machine to use the same directory on the host system (or on the network).

To set up shared folders

1. Start Workstation and select a virtual machine.
2. Choose **VM > Settings**.
3. Click the **Options** tab and select **Shared Folders**.
4. (Optional) For easy access, select the **Map as a network drive in Windows guests** check box to map a drive to the `Shared Folders` directory.

   This directory contains all the shared folders you enable. The drive letter is selected automatically.
5. Click **Add**.

   On Windows, clicking **Add** starts the Add Shared Folder wizard. On Linux, it opens the Shared Folder Properties dialog box.

6 Use the following information to complete the wizard or Properties dialog box:

- **Name** – Name that appears inside the virtual machine.

  Characters that the guest operating system considers illegal in a share name appear differently when viewed inside the guest. For example, if you use an asterisk in a share name, you see `%002A` instead of `*` in the share name on the guest. Illegal characters are converted to their ASCII hexadecimal value.

- **Host folder** – Path on the host to the directory that you want to share.

  If you specify a directory on a network share, such as `D:\share`, Workstation always attempts to use that path. If the directory is later connected to the host on a different drive letter, the shared folder cannot be located.

- **Enabled** or **Enable this share** – Deselect this option to disable a shared folder without deleting it from the virtual machine configuration. You can enable the folder by selecting the check box next to its name in the list.

  To enable a folder at a later time select its name in the list, click **Properties**, and enable the folder in the Properties dialog box.

- **Read-only** – Select this option to prevent the virtual machine from changing the contents of the shared folder in the host file system. Access to files in the shared folder is also governed by permission settings on the host computer.

To change these properties, use the Properties dialog box. On Windows, after you select **Shared Folders** on the **Options** tab, click **Properties**.

7 (Optional) To enable shared folders for a virtual machine after a shared folder is created, on the **Shared Folders** settings panel, use the **Folder Sharing** section:

- Select **Enabled until next power off or suspend** to enable folder sharing temporarily, until you power off or suspend the virtual machine.

  If you select **Enabled until next power off or suspend** and restart the guest or use the guest operating system to shut down, shared folders are not disabled when you restart the virtual machine.

- Select **Always enabled** to enable or disable specific folders in the **Folders** section.

8 Access the enabled shared folder:

- For Windows guests, see "View Shared Folders in a Windows Guest" on page 182.
- On Linux guests, shared folders appear under `/mnt/hgfs`.
- On Solaris guests, shared folders appear under `/hgfs`.

Enabling and Disabling Shared Folders

You can enable shared folders for virtual machines created by other users, enable or disable all folder sharing for a specific virtual machine, and enable a specific shared folder for a virtual machine.

CAUTION Enabling all shared folders can pose a security risk because a shared folder might enable existing programs inside the virtual machine to access the host file system without your knowledge.

Enable Shared Folders for Virtual Machines Created By Other Users

A shared folder is disabled by default if it was not created by the user who powers on the virtual machine. This is a security precaution.

Folder sharing is also disabled by default for Workstation 4 and 5 virtual machines regardless of who created the folder.

To enable shared folders for virtual machines created by other users

1. Choose **Edit > Preferences**.
2. On the **Workspace** tab, in the **Virtual Machines** section, select **Enable all shared folders by default**.

   This setting applies to shared folders on all virtual machines that are created by other users, such as appliance developers.

You can now specify which virtual machines can share folders and which folders can be shared.

Enable or Disable Folder Sharing for Specific Virtual Machines

To reduce the security threat of enabling all shared folders, you must specify whether a specific virtual machine is allowed to share folders and then specify which folders to share.

To enable or disable folder sharing for specific virtual machines

1. Select a virtual machine.
2. Choose **VM > Settings**.
3. Click the **Options** tab and select **Shared Folders**.

4. Use the buttons in the **Folder Sharing** section to enable or disable shared folders and click **OK**.

   You can select **Enabled until next power off or suspend** only when the virtual machine is powered on. This setting enables folder sharing temporarily, until you shut down, suspend, or restart the virtual machine. You must select this option or **Always enabled** to enable or disable specific folders in the **Folders** section.

5. If the virtual machine has a Windows operating system, select whether to map a network drive.

   On Windows, if you disable shared folders, after you power on a virtual machine and attempt to select a mapped drive to the shared folder, you receive a message that the connection cannot be made.

After you enable folder sharing for a virtual machine, specify which folders can be shared.

Specify Which Folders to Share

Before you begin, make sure the virtual machine is allowed to share folders. See "Enable or Disable Folder Sharing for Specific Virtual Machines" on page 180.

To specify which folders to share

1. Select the virtual machine.
2. Choose **VM > Settings > Options > Shared Folders**.
3. In the **Folders** list for the virtual machine, select the check box next to the name of the shared folder that you want to enable.
4. (Optional) To make the shared folder read-only, select the shared folder and click **Properties,** select the read-only check box and click **OK**.

Viewing a Shared Folder

Viewing shared folders in a guest varies based on whether the guest operating system is Windows, Solaris, or Linux. You can use shared folders to share any type of files.

To determine which folders on the host are being shared with a virtual machine, choose **VM > Settings > Options > Shared Folders** to see a list of the shared folders and the directory paths to them.

CAUTION Do not open a file in a shared folder from more than one application at a time. For example, do not open the same file using an application on the host operating system and another application in the guest operating system. If one of the applications writes to the file, data corruption can occur.

View Shared Folders in a Windows Guest

In a Windows guest operating system, you can view shared folders using desktop icons.

NOTE If your guest operating system has VMware Tools from Workstation 4.0, shared folders appear as folders on a designated drive letter.

To view shared folders in a Windows guest

- Look in **My Network Places > Entire Network** (**Network Neighborhood** for a Windows NT guest, or **Network** for Windows Vista) under **VMware Shared Folders**.

  If you have trouble finding a shared folder using the desktop icon, open Windows Explorer and look in **My Network Places** (or **Network Neighborhood**).

- To view a specific shared folder, do one of the following:

  - Navigate to it on the guest system by opening **My Network Places > Entire Network > VMware Shared Folders > .host > Shared Folders > <shared_ folder_ name>**.

  - Go directly to the folder using the UNC path `\\.host\Shared Folders\<shared_folder_name>`.

View Shared Folders in a Linux or Solaris 10 Guest

For information about permission settings on the files you view, also see "Permissions and Folder Mounting for Shared Folders on Linux Guests" on page 182.

To view shared folders in a Linux or Solaris 10 guest

- On a Linux virtual machine, shared folders appear under `/mnt/hgfs`.
- On a Solaris virtual machine, shared folders appear under `/hgfs`.

Permissions and Folder Mounting for Shared Folders on Linux Guests

The version of VMware Tools included in Workstation 6.5 contains performance improvements, support for symbolic links if you use a Linux host, a new mechanism for mounting shared folders, and permissions enhancements.

Performance Improvements

Host-guest file sharing is integrated with the guest page cache. Files in shared folders are cached for reading and can be written to asynchronously. However, you do not experience the read caching benefits on files that are being actively written to from the guest.

To speed performance, use the `ttl` (time to live) option to the `mount` command. Use this option to specify the interval used by the `hgfs` (host-guest file system) driver for validating file attributes. For example, if you use the following command, attributes are validated every 3 seconds instead of every 1 second, which is the default:

```
mount –o ttl=3 –t vmhgfs .host:/<share> <mountpoint>
```

NOTE Lengthening the interval involves some risk. If a process in the host modifies a file's attributes, the guest might not get the modifications as quickly, and the file can become corrupted.

Folder Mounting

This mechanism allows you to mount one or more directories or subdirectories in a shared folder to any location in your file system in addition to the default location of `/mnt/hgfs`. You can use the `mount` program to mount all shares, one share, or a subdirectory within a share to any location in your file system. The following table provides examples.

Command	Description
`mount –t vmhgfs .host:/ /home/user1/shares`	Mounts all shares to `/home/user1/shares`
`mount –t vmhgfs .host:/foo /tmp/foo`	Mounts the share named `foo` to `/tmp/foo`
`mount –t vmhgfs .host:/foo/bar /var/lib/bar`	Mounts the subdirectory `bar` within the share `foo` to `/var/lib/bar`

When you use the `mount` program, you can use VMware-specific options in addition to the standard `mount` syntax. To see usage information for the host-guest file system options, enter this command:

```
/sbin/mount.vmhgfs –h
```

NOTE When you install VMware Tools, an entry is made to `etc/fstab` to specify the location of shared folders. You can edit this file to change or add entries.

To use `mount` in this way, you must use the virtual machine settings editor in Workstation to set up and enable a shared folder. After the share exists, you can mount the shared folder to other locations besides the default.

In previous versions of VMware Tools, when a Linux guest attempted to mount a shared folder, the `vmware-guestd` program attempted to perform the mount. If it failed, the only evidence of the failure was an empty folder.

With the new version of VMware Tools, the Tools services script loads a driver that performs the mount. If the mount fails, a message appears regarding mounting HGFS shares.

The mount can fail if shared folders are disabled or if the share does not exist. You are not prompted to re-run the VMware Tools configurator (the `vmware-config-tools.pl` file).

Improved Handling of Permissions

Many refinements have been made for Linux guests on both Linux and Windows hosts:

- If you use a Linux host and create files that you want to share with a Linux guest, the file permissions shown on the guest are exactly the same as those on the host.

  Use `fmask` and `dmask` to mask permissions bits for files and directories.

- If you use a Windows host and create files that you want to share with a Linux guest, read-only files are displayed as having read and execute permission for everyone, and other files are shown as fully writable by everyone.

- If you use a Linux guest to create files for which you want to restrict permissions, use the `mount` program with the following options in the guest: `uid`, `gid`, `fmask`, `dmask`, `ro` (read-only), and `rw` (read-write). Note that `rw` is the default.

  If you are using a Windows host or a Linux host created with a previous release of Workstation, you can change only the owner permissions. This behavior is the same as in previous releases.

Using a Mapped Drive for Windows Only

You can map a virtual disk to a host instead of using shared folders or copying data between a Windows guest and host. In this case, you can mount a virtual disk in a Windows host file system as a separate mapped drive. Using a mapped drive lets you connect to the virtual disk without going into a virtual machine.

After you map a drive to the virtual disk, you are not able to power on any virtual machine that uses that disk until you disconnect it from the host. Map only disks for Windows guests. If you map a disk from a Linux guest, when you attempt to access the disk from your host computer, you will be prompted to format the disk.

You can use Workstation to map the disk to a drive on the host, and to disconnect the drive. If you attempt to use the host's **My Computer > Tools > Disconnect Network Drive** command, you will not see the mapped drive letter in the list of network drives.

Map a Virtual Disk to a Drive on the Host

Before you begin to map a virtual disk, make sure that all virtual machines that use the disk are powered off. Also, take the following considerations into account:

- You can mount volumes formatted with FAT (12/16/32) or NTFS only. If the virtual disk has a mix of partitions (volumes) where, for example, a partition is unformatted or is formatted with a Linux operating system and another partition is formatted with a Windows operating system, you can mount the Windows partition only.
- You can mount a virtual disk that has a snapshot, but if you write to the disk, you can irreparably damage a snapshot or linked clone previously created from the virtual machine.
- You cannot mount a virtual disk if any of its `.vmdk` files are compressed or have read-only permissions. Change these attributes before mounting the virtual disk.

CAUTION VMware recommends that you leave the check box called **Open file in read-only mode** selected in the Map a Virtual Disk dialog box. This setting prevents you from accidentally writing data to a virtual disk that might be the parent of a snapshot or linked clone. Writing to such a disk might make the snapshot or clone unusable.

To map a virtual disk to a drive on the host

1. Choose **File > Map or Disconnect Virtual Disks**.
2. In the Map or Disconnect Virtual Drives dialog box, click **Map**.
3. In the dialog box, click **Browse**, navigate to a disk file (`.vmdk` file), select it, and click **Open**.

4. Select the volume to map, and select a drive letter that is not being used on your host.

5. Click **OK**.

   The drive appears in Windows Explorer on your host. From the host, you can read from or write to files on the mapped virtual disk.

6. (Optional) To view a mapped drive, choose **VM > Settings > Hardware**, select the hard disk and click **Utilities > Map**.

When you are ready to unmap the drive, see "Disconnect the Host from the Virtual Disk" on page 186.

Disconnect the Host from the Virtual Disk

To access the mapped virtual disk from a virtual machine again, you must disconnect it. You can disconnect the host from the virtual disk using two different methods.

To disconnect the host from the virtual disk

Do one of the following:

- Use the **File** menu in Workstation:

  a. Choose **File > Map or Disconnect Virtual Disks**.

  b. In the Map or Disconnect Virtual Drives dialog box, select a volume to disconnect and click **Disconnect**.

  c. If you receive an error message asking whether to forcibly disconnect, click **Yes**.

  d. Click **OK**.

- Use the **VM** menu for a selected virtual machine:

  a. Choose **VM > Settings > Hardware**.

  b. Select the hard disk and click **Utilities > Disconnect**.

You can now power on any virtual machine that uses this disk.

Preserving the State of a Virtual Machine

9

Suspending a virtual machine lets you save the current state so that you can continue work later from the same state. Taking a snapshot lets you preserve the state of the virtual machine so you can return to the same state repeatedly. This chapter includes the following topics:

Using the Suspend and Resume Features

You can use the suspend and resume features to save the current state of a virtual machine. When you resume, any applications you were running when you suspended the virtual machine are resumed in their running state, and the content is the same as when you suspended the virtual machine.

The speed of the suspend and resume operations depends on how much data changed since the virtual machine started. In general, the first suspend operation takes longer than later suspend operations.

When you resume and do additional work in the virtual machine, you cannot return to the state the virtual machine was in at the time you suspended. To preserve the state of the virtual machine so that you can return to the same state repeatedly, take a snapshot, as described in "Using Snapshots" on page 189.

Use Hard Suspend or Soft Suspend

You can configure the **Suspend** button or menu command to run a VMware Tools script in the guest operating system before doing the suspend operation. This configuration is called a soft suspend.

Before you begin, make sure VMware Tools is installed in the guest operating system. See "Installing VMware Tools" on page 100.

On Windows guests, when you do a soft suspend, a script releases the IP address if the guest operating system is using DHCP. On Linux, FreeBSD, and Solaris guests, the script stops networking for the virtual machine. When you use the **Resume** command on Windows guests, a script gets a new IP address from DHCP. On Linux, FreeBSD, and Solaris guests, networking restarts.

To use hard suspend or soft suspend

1. Select the virtual machine.
2. Choose **VM > Settings**.
3. Click the **Options** tab, and select **Power**.
4. In the **Power controls** section, specify a hard suspend (**Suspend**) or a soft suspend (**Suspend Guest**) operation.
5. Click **OK**.

Suspend or Resume a Virtual Machine

The suspend and resume features let you save the current state of your virtual machine and continue work later from the same state.

Before suspending a virtual machine, specify whether to stop networking before suspending. See "Use Hard Suspend or Soft Suspend" on page 188.

To suspend or resume a virtual machine

Do one of the following:

- To suspend a virtual machine, choose **VM > Power > Suspend**.

  If the virtual machine is running in full screen mode, which hides the toolbar, return to windowed mode by pressing the Ctrl+Alt+Enter key combination.

  When you suspend a virtual machine, a file with a `.vmss` extension is created in the working directory.

- To resume a suspended virtual machine that you suspended, select the virtual machine and choose **VM > Power > Resume**.

  When you resume the virtual machine, its state is restored from the `.vmss` file.

Using Snapshots

Taking snapshots lets you preserve the state of the virtual machine so that you can return to the same state repeatedly.

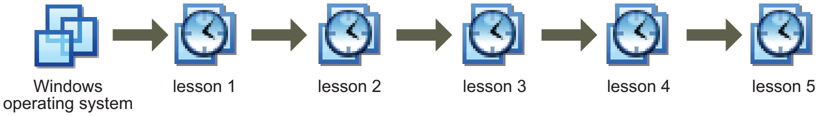
Scenarios for Using Multiple Snapshots

You can take multiple snapshots of a virtual machine.

Snapshots in a Linear Process

Taking snapshots in a linear process means taking a snapshot, continuing to use the virtual machine from that point, taking another snapshot at a later point, and so on. Each snapshot is a restoration point in a single long sequence.

Figure 9-1. Snapshots as Restoration Points in a Linear Process



Workstation supports more than 100 snapshots for each linear process.

Use snapshots in a linear process for the following situations:

- You plan to make risky changes in a virtual machine, such as by testing new software or examining a virus. Before adding new, untested code to a project, take a snapshot.

  You can always revert to a previous known working state of the project if the new code does not work as expected. If the new code causes no problems, you can take another snapshot of the virtual machine in its new state.

  NOTE You can configure a virtual machine to take a snapshot any time it is powered off, preserving a virtual audit trail as work progresses. See "Take or Revert to a Snapshot at Power Off" on page 199.

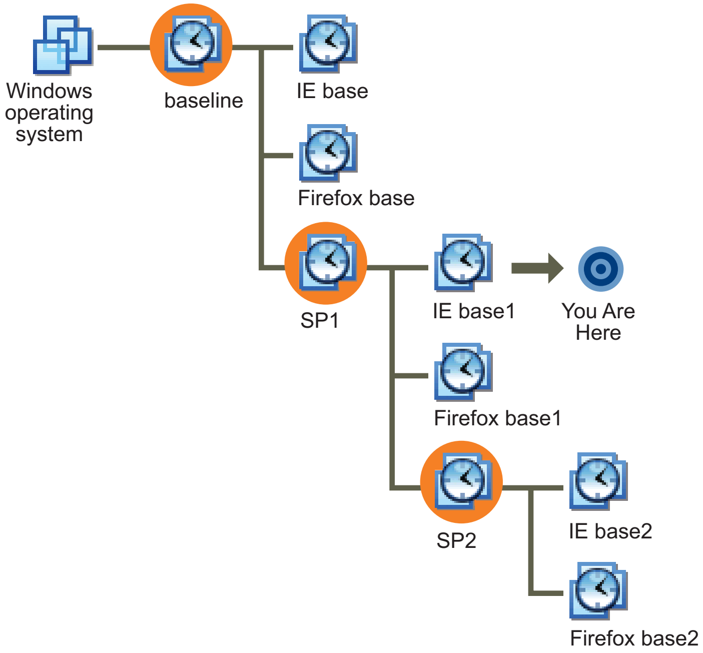
- You create a training course and want to save the state of the virtual machine in a snapshot at each lesson's starting point. You can use the snapshots to skip lengthy computer preparation time.

  You can also configure the virtual machine to revert to a snapshot any time it is powered off. Each time a new class begins a lesson, the previous student's work is discarded. See "Revert at Power Off" on page 197.

Snapshots in a Process Tree

You can save a number of sequences as branches from a single baseline, as Figure 9-2 shows. This strategy is often used in testing software. You can take a snapshot before installing different versions of a program to ensure that each installation begins from an identical baseline.

Figure 9-2. Snapshots as Restoration Points in a Process Tree



Although Workstation supports more than 100 snapshots for each branch in a process tree, keeping more than 99 might cause the guest operating system to have problems booting. Delete some snapshots or make a full clone of the virtual machine.

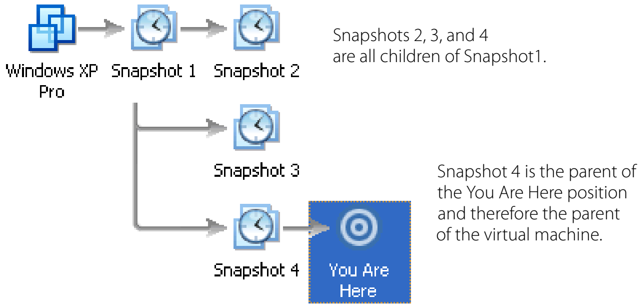
Snapshot Relationships

The relationship between snapshots is like a parent-child relationship:

- In a linear process, each snapshot has one parent and one child, except for the last snapshot, which has no children.
- In a process tree, each snapshot has one parent, but one snapshot can have more than one child. Many snapshots have no children.

The parent snapshot of a virtual machine is the snapshot on which the current state (the You Are Here position in Figure 9-3) is based. After you take a snapshot, that stored state is the parent snapshot of the virtual machine. If you revert or go to an earlier snapshot, the earlier snapshot becomes the parent snapshot of the virtual machine.

Figure 9-3. Parent-Child Relationship Between Snapshots


Windows XP Pro
Snapshot 1
Snapshot 2
Snapshot 3
Snapshot 4
You Are Here
Snapshots 2, 3, and 4 are all children of Snapshot1.
Snapshot 4 is the parent of the You Are Here position and therefore the parent of the virtual machine.

Information Captured by Snapshots

A snapshot captures the entire state of the virtual machine at the time you take the snapshot. This includes:

- **Memory state** – Contents of the virtual machine memory
- **Settings state** – Virtual machine settings
- **Disk state** – State of all the virtual disks

The state of a physical disk or independent disk is not preserved when you take a snapshot.

Snapshots operate on individual virtual machines. If you select a team of virtual machines and take a snapshot, only the state of the active virtual machine is preserved. See "Summary and Console Views for Teams and Their Virtual Machines" on page 256.

When you revert to a snapshot, you return the memory, settings, and virtual disks of the virtual machine to the state they were in when you took the snapshot. To suspend, power on, or power off the virtual machine when you launch it, be sure it is in that state when you take the snapshot.

Snapshot Conflicts

Avoid taking a snapshot when applications in the virtual machine are communicating with other computers, especially in production environments.

Suppose you take a snapshot while the virtual machine is downloading a file from a server on the network. After you take the snapshot, the virtual machine continues downloading the file, communicating its progress to the server. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails.

Or consider a case in which you take a snapshot while an application in the virtual machine is sending a transaction to a database on a separate machine. If you revert to that snapshot after the transaction starts but before it is committed, the database is likely to be confused.

Enable or Disable Background Snapshots

When you set a preference to take snapshots in the background, you can continue working while the state of the virtual machine is being preserved. A progress indicator for the background snapshot is displayed in one of the corners of the Workstation window.

Before you begin, on Linux hosts, run Workstation as the root user. Only root users are allowed to change this preference setting.

If you take another snapshot or revert to a snapshot before Workstation completes a pending snapshot operation, a progress dialog box appears. You must wait for the pending snapshot operation to finish before the next snapshot or resume operation begins.

Enabling background snapshots for a host with slow hard disks can adversely affect performance. If you experience significant performance problems when taking or restoring snapshots, disable background snapshots.

To enable or disable background snapshots

1. Choose **Edit > Preferences**.
2. Click the **Priority** tab.
3. Use the check box in the **Snapshots** section to enable or disable background snapshots.
4. Click **OK** and restart the virtual machine.

Exclude a Virtual Disk from Snapshots

In certain configurations, you might want to revert some disks to a snapshot while other disks retain all changes. For example, you might want a snapshot to preserve a disk with your operating system and applications, while always keeping the changes to a disk with your documents.

You can exclude virtual disks from a snapshot by changing the disk mode. Before you begin, power off the virtual machine and delete any existing snapshots.

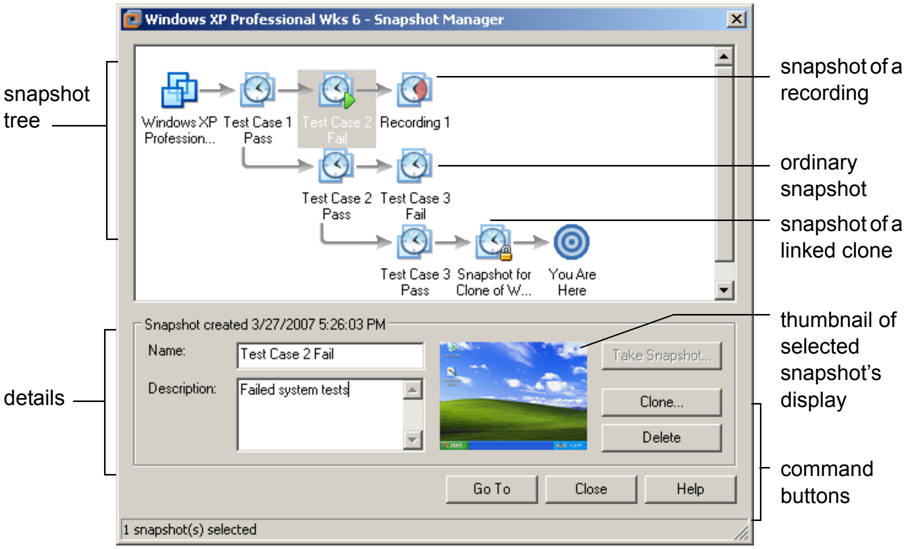
To exclude a virtual disk from snapshots

1. Select the virtual machine.
2. Choose **VM > Settings**.
3. On the **Hardware** tab, select the drive to exclude and click **Advanced**.
4. Select **Independent** and select one of the following options:
   - **Persistent** – Changes are immediately and permanently written to the disk. All changes to an independent disk in persistent mode remain, even when you revert to a snapshot.
   - **Nonpersistent** – Current changes to the disk are discarded when you power off or revert to a snapshot.

Snapshot Manager Overview

You can review all snapshots for the active virtual machine and act on them directly in the snapshot manager. Figure 9-4 illustrates the components of the snapshot manager.

Figure 9-4. Snapshot Manager on a Windows Host



Snapshot created 3/27/2007 5:26:03 PM

Name: Test Case 2 Fail

Description: Failed system tests

1 snapshot(s) selected

The snapshot tree shows all snapshots for the virtual machine and the relationship between snapshots. The **You Are Here** icon is not a snapshot. It shows the current state of the virtual machine. See "Snapshot Relationships" on page 191.

NOTE Point to a snapshot (without clicking) to display the complete name of that snapshot.

Most snapshot manager actions are available as menu commands from the **VM > Snapshot** menu. The following actions, however, are available only from the snapshot manager:

- **Renaming a snapshot** – The **Name** text box is editable. If you rename a snapshot for a cloned virtual machine, use the **Description** field for future identification.
- **Changing or adding a description** – The **Description** text box is editable.
- **Deleting a snapshot** – See "Delete a Snapshot or a Recording" on page 198.

The snapshot manager has a slightly different appearance on Linux hosts. On Linux hosts, right-click the toolbar to change the icon style. You can display icons and text, icons only, text only, and so on.

Open and Use the Snapshot Manager

Use the snapshot manager to review all snapshots for the active virtual machine and act on them directly.

To open and use the snapshot manager

1. Select the virtual machine.
2. Choose **VM > Snapshot > Snapshot Manager**.
3. Select a snapshot or recording and click the button for the desired action.

   To select more than one snapshot or recording, Ctrl+click the desired snapshots and recordings.

   If the **Take Snapshot** button is disabled, it might be because the virtual machine has multiple disks in different disk modes. For example, if you have a special purpose configuration that requires you to use an independent disk, you must power off the virtual machine before taking a snapshot.

Take a Snapshot

You can usually take a snapshot while a virtual machine is powered on, powered off, or suspended.

Following are the prerequisites for taking a snapshot:

- Any suspend operations must be complete.
- The virtual machine is not communicating with another computer. See “Snapshot Conflicts” on page 192.
- If your use of virtual machines is strongly performance oriented, the guest operating system’s drives are defragmented. See “Defragment Virtual Disks” on page 223.
- If the virtual machine has multiple disks in different disk modes, the virtual machine is powered off. For example, if a special purpose configuration requires you to use an independent disk, you must power off the virtual machine before taking a snapshot.
- If the virtual machine was created with Workstation 4 delete any existing snapshots or upgrade the virtual machine to Workstation 5 or higher. See “Change the Version of a Virtual Machine” on page 91.

To take a snapshot

1. Choose **VM > Snapshot > Take Snapshot**.
2. Enter a unique name.
3. (Optional) Enter a description.

   Use this field to record notes about the virtual machine state captured in the snapshot.
4. Click **OK**.

Rename a Snapshot or Recording

Use the snapshot manager to change the name of a snapshot or its description at any time.

To rename a snapshot or recording

1. Choose **VM > Snapshot > Snapshot Manager**.
2. Select the snapshot or recording.
3. Edit the text in the **Name** text box and click **Close**.

   If you rename a snapshot for a cloned virtual machine, use the **Description** field to specify which virtual machine was cloned.

Restore an Earlier State from a Snapshot

Restore a snapshot in Workstation by using the **Revert** and **Go to** commands.

The **Revert** command has the same effect as using the **Go to** command and selecting the parent snapshot of the virtual machine. It reverts to the parent snapshot of the current state. This state corresponds to the You Are Here position in the snapshot manager. See “Snapshot Relationships” on page 191.

The **Go to** command is not limited to the parent snapshot of the current state. You can choose any existing snapshot of the virtual machine.

To restore an earlier state from a snapshot

Do one of the following:

- To revert to the parent snapshot, choose **VM > Snapshot > Revert to Snapshot**.
- To revert to a snapshot that is not the parent, choose **VM > Snapshot** and select the snapshot name.
- To set the virtual machine to revert to the parent snapshot every time the virtual machine is powered off, see “Revert at Power Off” on page 197.

Revert at Power Off

You can set the virtual machine to revert to the parent snapshot any time it is powered off. The parent snapshot of a virtual machine is the snapshot on which the current state (the You Are Here position) is based.

To set a virtual machine to revert to a snapshot at power off

1. Select the virtual machine.
2. Choose **VM > Settings**.
3. Click the **Options** tab and select **Snapshot/Replay**.
4. In the **When powering off** section, select **Revert to snapshot**.

Delete a Snapshot or a Recording

In most cases, deleting a snapshot or recording does not affect other snapshots, recordings, or the current state of the virtual machine. Use the snapshot manager to delete a snapshot.

CAUTION If a snapshot is used to create a clone, the snapshot becomes locked. If you delete a locked snapshot, the clones created from that snapshot no longer operate.

You cannot delete a snapshot if the associated virtual machine is designated as a template for cloning. See "Enable Template Mode for a Parent Virtual Machine of Linked Clones" on page 205.

To delete a snapshot or recording

1. Choose **VM > Snapshot > Snapshot Manager**.
2. Do one of the following:
   - To delete a single snapshot or recording, select it and click **Delete**.
   - To delete a snapshot or recording and all its children, right-click it and choose **Delete Snapshot/Recording and Children**.
   - To delete all snapshots and recordings, right-click a snapshot or recording, choose **Select All**, and click **Delete**.
3. When prompted to confirm the deletion, click **OK**, and click **Close** in the snapshot manager.

Take or Revert to a Snapshot at Power Off

You can set a virtual machine to automatically revert to a snapshot or to take a new snapshot whenever you power off the virtual machine.

To take a snapshot or revert to one at power off

1. Select the virtual machine.
2. Choose **VM > Settings**.
3. Click the **Options** tab and select **Snapshot/Replay**.
4. Select an option in the **When powering off** section:
   - **Just power off** – Powers off without making any changes to snapshots.
   - **Revert to snapshot** – Reverts to the parent snapshot of the current state of the virtual machine (that is, the parent snapshot of the You Are Here position in the Snapshot Manager window).

     An instructor might use this setting to discard student answers for a computer lesson when a virtual machine is powered off at the end of class.
   - **Take a new snapshot** – Takes a snapshot of the virtual machine state after it is powered off. This is useful to preserve milestones automatically. The snapshot appears in the snapshot manager. The name of this snapshot is the date and time the virtual machine was powered off. The description is "Automatic snapshot created when powering off."
   - **Ask me** – Prompts you, every time you power off a virtual machine, choose to power off, revert, or take a snapshot.
5. Click **OK**.

Snapshots and Workstation 4 Virtual Machines

Workstation 4 virtual machines do not support multiple snapshots. For full Workstation 6 functionality, you must upgrade. See "Change the Version of a Virtual Machine" on page 91.

If a Workstation 4 virtual machine has a snapshot, you must remove the snapshot before you upgrade. Use your earlier, Workstation 4 application to remove the snapshot, and then upgrade to Workstation 6.

Cloning, Moving, and Sharing Virtual Machines 10

Cloning a virtual machine is faster and easier than copying it. This chapter provides instructions and also provides information on how to move your virtual machines from one host to another, or elsewhere on the same host, plus recommendations on how to share virtual machines with other users. This chapter includes the following topics:

The Virtual Machine's Universal Unique Identifier

To ensure all virtual machines are identified properly, each virtual machine is automatically assigned a universal unique identifier (UUID).

Use the UUID of a virtual machine for system management in the same way you use the UUID of a physical computer. The UUID is stored in the SMBIOS system information descriptor. It can be accessed by standard SMBIOS scanning software, such as SiSoftware Sandra or the IBM utility smbios2.

This UUID is generated when you initially power on the virtual machine. As long as you do not move or copy the virtual machine to another location, the UUID remains constant. To set a specific UUID, see "Specify a UUID for a Virtual Machine" on page 202.

UUID Options When You Move a Virtual Machine

When you power on a virtual machine that was moved or copied to a new location, a message appears, asking whether you moved or copied the virtual machine. If you reply that you copied the virtual machine, a new UUID is generated.

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

Set the Virtual Machine to Always Keep or Always Create a UUID

If a virtual machine is set to always keep or always create a UUID, users are not prompted when a virtual machine is moved or copied. You can set this property by editing the virtual machine's configuration file.

To set the virtual machine to always keep or always create a UUID

1 Power off the virtual machine.

2 Open the configuration (`.vmx`) file with a text editor.

3 Add the following line:

```
uuid.action = "<action>"
```

The value for `<action>` can be either **`create`**, to always generate a new UUID, or **`keep`**, to always retain the UUID.

Specify a UUID for a Virtual Machine

Although UUIDs are automatically assigned to virtual machines, you can override the generated UUID value and assign a specific UUID.

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

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

To specify a UUID for a virtual machine

1. Power off the virtual machine.
2. Open the configuration (`.vmx`) file with a text editor.
3. Search for the line that contains `uuid.bios`.

   The format of the line is `uuid.bios = "<uuid_value>"`, with quotation marks around the parameter value. Following is an example of the configuration setting:

   ```
   uuid.bios = "00 11 22 33 44 55 66 77-88 99 aa bb cc dd ee ff"
   ```
4. Replace the existing UUID value with the specific UUID value.
5. Save and close the file.
6. Power on the virtual machine.

The new UUID is used when the virtual machine boots.

Cloning a Virtual Machine

Installing a guest operating system and applications can be time consuming. With clones, you can make many copies of a virtual machine from a single installation and configuration process.

Clones are useful when you must deploy many identical virtual machines to a group. For example:

- An MIS department can clone a virtual machine for each employee, with a suite of preconfigured office applications.
- A virtual machine can be configured with a complete development environment and then cloned repeatedly as a baseline configuration for software testing.
- A teacher can clone a virtual machine for each student, with all the lessons and labs required for the term.
- With clones you can make copies of a virtual machine without browsing a host file system or worrying if you have located all the configuration files. The existing virtual machine is called the parent of the clone. When the cloning operation is complete, the clone becomes a separate virtual machine. These are the main characteristics of a clone:

- Changes made to a clone do not affect the parent virtual machine. Changes made to the parent virtual machine do not appear in a clone.
- A clone’s MAC address and UUID are different from the parent virtual machine.

Although a clone is a separate virtual machine, if the clone is a linked clone, it shares virtual disks with the parent virtual machine. See “Types of Clones” on page 204.

Types of Clones

Two types of clones are available: full and linked.

Full Clones

A full clone is a complete and independent copy of a virtual machine. It shares nothing with the parent virtual machine after the cloning operation. Ongoing operation of a full clone is entirely separate from the parent virtual machine.

Because a full clone does not share virtual disks with the parent virtual machine, full clones generally perform better than linked clones. However, full clones take longer to create than linked clones. Creating a full clone can take several minutes if the files involved are large.

The full clone duplicates only the state of the virtual machine at the instant of the cloning operation. Thus the full clone does not have access to any snapshots that might exist of the parent virtual machine.

Linked Clones

A linked clone is a copy of a virtual machine that shares virtual disks with the parent virtual machine in an ongoing manner. A linked clone is made from a snapshot of the parent. See “Scenarios for Using Multiple Snapshots” on page 189. This conserves disk space and allows multiple virtual machines to use the same software installation.

CAUTION You cannot delete the linked clone snapshot without destroying the linked clone. You can safely delete this snapshot only if you also delete the clone that depends on it.

All files available on the parent at the moment you take the snapshot continue to remain available to the linked clone. Ongoing changes to the virtual disk of the parent do not affect the linked clone, and changes to the disk of the linked clone do not affect the parent.

A linked clone must have access to the parent. Without access to the parent, you cannot use a linked clone. You can make a linked clone from a linked clone, but keep in mind that the performance of the linked clone degrades. When possible, make a linked clone of the parent virtual machine.

If you make a full clone from a linked clone, however, the full clone is an independent virtual machine that does not require access to the linked clone or its parent.

Linked clones are created swiftly, so you can easily create a unique virtual machine for each task. You can also easily share a virtual machine with other users by storing the virtual machine on your local network, where other users can quickly make a linked clone. This facilitates collaboration. For example, a support team can reproduce a bug in a virtual machine, and an engineer can quickly make a linked clone of that virtual machine to work on the bug.

Creating Clones

If you decide to create a linked clone and you want to prevent the parent virtual machine from being accidentally deleted, enable template mode before using the Clone Virtual Machine wizard.

Enable Template Mode for a Parent Virtual Machine of Linked Clones

To prevent anyone from deleting the parent virtual machine for a linked clone, designate the parent as a template. When template mode is enabled, a virtual machine cannot be deleted or added to a team, and the virtual machine’s snapshots cannot be deleted.

To enable template mode for a parent virtual machine of linked clones

1. Select the virtual machine to use as a parent of your linked clone.
2. Verify that the parent has at least one snapshot.

   Open the snapshot manager and create a snapshot if none exists. See “Snapshot Manager Overview” on page 194.
3. Choose **VM > Settings**.
4. Click the **Options** tab, and select **Advanced**.
5. In the **Settings** section, click **Enable Template mode (to be used for cloning)** and click **OK**.

Use the Clone Virtual Machine Wizard

The Clone Virtual Machine wizard guides you through the process of making a clone. You do not need to locate and manually copy the parent virtual machine files.

Before making a linked clone, defragment the guest operating system's drives on the parent virtual machine. Use the tools in the guest operating system to run a defragmentation utility. See "Defragment Virtual Disks" on page 223.

For information about preventing a linked clone's parent virtual machine from being deleted, see "Enable Template Mode for a Parent Virtual Machine of Linked Clones" on page 205.

NOTE Workstation 4 virtual machines, and virtual machines created with other VMware products that are compatible with Workstation 4, must be upgraded to at least Workstation 5 virtual machines before you can clone them. See "Change the Version of a Virtual Machine" on page 91.

To use the Clone Virtual Machine wizard

1 Select the virtual machine.

2 Make sure the virtual machine is powered off.

3 Choose **VM > Clone** to open the Clone Virtual Machine wizard.

4 On the Welcome page, click **Next**.

5 On the Clone Source page, select the state of the parent from which you want to create a clone and click **Next**.

   You can choose to create a clone from the parent's current state or from any existing snapshot of the parent. If you select the current state, Workstation creates a snapshot of the virtual machine before cloning it.

   The wizard does not allow you to clone from the current state when template mode is enabled.

6 On the Clone Type page, specify whether to create a linked clone or a full clone and click **Next**.

7 On the Name of the New Virtual Machine page, enter a name and a path for the cloned virtual machine and click **Finish**.

   A full clone can take many minutes to create, depending on the size of the virtual disk that is being duplicated.

8 Click **Done** to exit the Clone Virtual Machine wizard.

The Clone Virtual Machine wizard automatically creates a new MAC address and UUID for the clone. Other configuration information is identical to that of the parent virtual machine. For example, a machine's name and static IP address configuration are not altered by the Clone Virtual Machine wizard.

9 To prevent conflict with static IP addressing, change the clone's static IP address before the clone connects to the network.

See "Selecting IP Addresses on a Host-Only Network or NAT Configuration" on page 286.

Moving a Virtual Machine

You can take a virtual machine that was created by using Workstation and move it to a different computer or to a different location on the same computer. You can even move a virtual machine to a host with a different operating system. For example, you can move a virtual machine from a Windows host to a Linux or ESX Server host.

In general, moving a virtual machine means moving the files that make up the virtual machine. The path names for all files associated with a Workstation virtual machine are relative, meaning the path to each file is relative to the virtual machine directory. For example, if you are in the virtual machine directory, the relative path to the virtual disk file is `<machine_name>.vmdk`.

CAUTION Always make backup copies of all the files in a virtual machine's directory before you start a process like this.

Hosts with Different Hardware

The guest operating system might not work correctly if you move a virtual machine to a host with significant hardware differences, such as from a 64-bit host to a 32-bit host or from a multiprocessor host to a uniprocessor host.

Moving Between 64-Bit and 32-Bit Hosts

You can move a virtual machine from a 32-bit host to a 64-bit host but not from a 64-bit host to a 32-bit host unless the 32-bit host has a supported 64-bit processor.

NOTE Workstation supports 64-bit guest operating systems only in Workstation 5.5 and higher, and only on host machines with supported processors. When you power on a virtual machine with a 64-bit guest operating system, Workstation performs an internal check. If the host CPU is not a supported 64-bit processor, you cannot power on the virtual machine. For the list of processors Workstation supports for 64-bit guest operating systems, see "PC Hardware" on page 23.

Moving Between Multiprocessor and Uniprocessor Hosts

For all supported configurations of 32-bit and 64-bit host and guest operating systems running on multiprocessor host machines, Workstation 5.5 and higher virtual machines support two-way virtual symmetric multiprocessing (SMP). This support enables you to assign two virtual processors to a virtual machine. This is supported only for host machines with at least two logical processors. See "Use Two-Way Virtual Symmetric Multiprocessing" on page 349.

NOTE If the host is a uniprocessor machine, assigning two processors is not supported. A warning message appears. You can disregard this message and assign two processors to the virtual machine, but when you finish creating the virtual machine, you cannot power it on unless you move it to a host machine with at least two logical processors.

Open a Virtual Machine Created in ESX Server That Has More Than Two Processors

You can use Workstation 5.5 or higher, running on a multiprocessor host machine, to open a virtual machine created in VMware ESX Server that has one or more virtual processors. However, in Workstation you cannot power on or resume a virtual machine that has more than two virtual processors assigned, even if more processors were assigned when the virtual machine was created in ESX Server.

You can see this setting in the virtual machine's summary view or by using the virtual machine settings editor.

To open a virtual machine created in ESX Server that has more than two processors

1 Select the virtual machine and choose **VM > Settings > Hardware > Processors**.

2 Note that **Number of Processors** is set to **Other (x)**, where **x** is the number of processors originally assigned in ESX Server.

Workstation preserves this original configuration setting for the number of processors, even though two is the maximum number of processors supported.

3 Change this setting to two processors so that you can power on the virtual machine in Workstation.

After you commit a change to this setting, the original setting for number of processors is discarded, and no longer appears as an option in the virtual machine settings editor.

Move a Virtual Machine to a New Location or a New Host

You can move the virtual machine to a different location on the same host or to move it to a new host.

For more information about compatibility between VMware products, see the *VMware Virtual Machine Mobility Planning Guide*.

To move a virtual machine to a new location or a new host

1 Make sure that all the virtual machine files are stored in the virtual machine directory.

For example, if you configured the working directory to reside in a different location on the host, move it into the virtual machine directory and use the virtual machine settings editor (**VM > Settings > Options > General**) to point to this location.

If the virtual machine you want to move is a linked clone, see "Moving Linked Clones" on page 210.

2 Shut down the guest operating system and power off the virtual machine.

3 Copy all the files in the virtual machine directory to the new location.

To move the virtual machine's files to another host, if you do not have a network connection to the new host, use a shared network directory, burn the files onto a DVD, or use some other storage media that has enough disk space.

For more information about the files that you are moving, see "Files That Make Up a Virtual Machine" on page 93.

4 On the new host, start Workstation, choose **File > Open**, and browse to the virtual machine's configuration (`.vmx`) file in its new location.

5 (Optional) If you are moving the virtual machine to a different location on the same host, remove the virtual machine from the **Favorites** list and add it again using the new location.

6 When you are certain that the virtual machine in the new location works correctly, delete the virtual machine files from the old location, if desired.

   If the virtual machine in the new location is not working correctly, examine the virtual machine in the original location to determine if you missed copying some files. Some files might reside outside of the virtual machine directory.

   Use the virtual machine settings editor (**VM > Settings > Hardware**) to select devices and determine whether any associated files point to locations that cannot be accessed from the new location.

Workstation generates a different MAC address for the virtual network adapter when you move a virtual machine to a new host computer or to a different directory on the same host computer. A new MAC address is also generated when you rename a directory in the path to the virtual machine's configuration file. See "Maintaining and Changing the MAC Address of a Virtual Machine" on page 291.

Moving an Older Virtual Machine

If you created a virtual machine by using Workstation 2.x or 3.x, you must upgrade it to at least Workstation 4. Workstation 6.x does not support Workstation 2 or 3 virtual machines.

Moving Linked Clones

You can move a linked clone as you do an ordinary Workstation virtual machine. However, if you move a linked clone (or if you move its parent virtual machine), make sure the clone can access the parent virtual machine. Place the parent in shared directory or on a networked file server.

For example, if you put a linked clone on a laptop and the parent remains on another machine, you can use the clone only when the laptop connects to the network or drive where the parent is stored. To use a cloned virtual machine on a disconnected laptop, you must use a full clone or you must move the parent virtual machine to the laptop.

You cannot power on a linked clone if Workstation cannot locate the original virtual machine.

Sharing Virtual Machines with Other Users

If you want other users to be able to access your virtual machines, consider the following points:

- Only one user can run a virtual machine at a time. Other users can also share a virtual machine by making a linked clone of it. A linked clone is a copy that uses the same virtual disks as the parent virtual machine it was copied from. See "Cloning a Virtual Machine" on page 203.
- On Windows hosts, relocate the virtual machine files to a directory that is accessible to all appropriate users. The default location for a Windows host is not typically accessible to other users:
  - On Windows XP: `C:\Documents and Settings\<user_name>\My Documents\My Virtual Machines`
  - On Windows Vista: `C:\Users\<user_name>\Documents\Virtual Machines`

  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 a network volume.
- On Linux hosts, set permissions for the virtual machine files appropriately.

  Permissions settings are especially important for the configuration file (`.vmx`) and virtual disks (`.vmdk`). For example, if you want users to run a virtual machine but not be able to modify its configuration, do not make the configuration file writable.

Using VNC for Remote Connections to a Virtual Machine

Virtual network computing (VNC) software enables you to view and interact with one computer from any other computer or mobile device anywhere on the Internet.

VNC software is cross-platform, allowing remote control between different types of computers. For example, you can use VNC to view a Linux machine on your Windows PC. Open-source versions of VNC are freely and publicly available.

You can use Workstation to set a virtual machine to act as a VNC server, and users on other computers can install a VNC client (also called a VNC viewer) to connect to the virtual machine. After you set up a virtual machine as a VNC server, you can see a list of users who are remotely connected to the virtual machine and find out how long they have been connected.

Workstation does not need to be running when VNC connections are made. Only the virtual machine needs to be running, and it can be running in the background.

Configure a Virtual Machine as a VNC Server

You do not need to install specialized VNC software in a virtual machine to set it up as a VNC server.

To configure a virtual machine as a VNC server

1. Select the virtual machine and choose **VM > Settings**.
2. Click the **Options** tab and select **Remote Display**.
3. Click **Enable remote display**.

   After remote display is enabled and users connect to the virtual machine with a VNC client, use the **View Connected Users** button on Remote Display settings panel to see a list of the connected users.
4. (Optional) Change the port number.

   To connect to multiple virtual machines on the same host with a VNC client, specify a unique port number for each virtual machine. VMware suggests that you use a port number in the range from 5901 to 6001.

   Keep in mind that other applications use certain port numbers, and some port numbers are privileged (only the root or Administrator user can listen). For example, the VMware Management Interface uses ports 8333 and 8222. On Linux, only the root user can listen to ports up to port number 1024.
5. (Optional) Set a password for connecting to the virtual machine from a VNC client.

   The password can be up to 8 characters long. Because it is not encrypted when the VNC client sends it, do not use a password that you use for other systems.
6. Click **OK**.

After you set up a virtual machine as a VNC server, you can see a list of users who are remotely connected to the virtual machine and find out how long they have been connected. To see the list, right-click the VNC icon in the status bar and choose **Connected Users**.

Use a VNC Client to Connect to a Virtual Machine

You can install a VNC client on your host and connect to a running virtual machine.

Before you begin, determine the machine name or IP address of the host on which the virtual machine is running and, if applicable, the VNC port number and password. See "Configure a Virtual Machine as a VNC Server" on page 212.

For information about mapping the keyboard to languages other than U.S. English, see "Specify a Language Keyboard Map for VNC Clients" on page 324.

The following issues are known to occur when you connect to virtual machines with a VNC client:

- You cannot take or revert to snapshots.
- You cannot change the power state of the virtual machine. That is, you cannot power on, power off, suspend, or resume. Although you cannot power off, you can shut down the guest operating system, and shutting down might power off the virtual machine.
- You cannot copy and paste text between the host and guest operating system.
- You cannot configure the virtual machine with the virtual machine settings editor.
- Remote display does not work well if you are also using the 3-D feature. This feature is described in "Support for Direct3D Graphics" on page 165.

To use a VNC client to connect to a virtual machine

1. On a local or remote computer, start a VNC client.

   You can use any VNC client, but not a Java viewer in a browser. To download and install a VNC client, check one of the many Web sites where you can buy or get one for free.

2. Make sure the client is set for hextile encoding.

   For example, if you use RealVNC Viewer, under the **Preferred Encoding** option, select **Hextile**.

3. Set the client to use all colors.

   For example, if you use RealVNC Viewer, under the **Colour Level** option, select **Full (all available colours)**.

4 When prompted for the VNC server name, enter the name or IP address of the host computer and the port number.

   Use the format:

   ```
   <machine_name>:<port_number>
   ```

5 Enter a password if you are prompted to do so.

Make Virtual Machines Available for Streaming from a Web Server

With virtual machine (VM) streaming, virtual disk data is fetched on demand. You can power on a virtual machine soon after you begin downloading it from a Web server.

Downloading a virtual machine in a `.zip` or `.tar` file from a Web server can take a considerable amount of time, depending on the size of the virtual machine. To use VM streaming, you place the virtual machine directory on the Web server without zipping it. VMware recommends that you configure the Web server to support persistent connections (HTTP keep-alive connections).

To make virtual machines available for streaming from a Web server

1 If the virtual machine any snapshots, delete them.

   See "Delete a Snapshot or a Recording" on page 198.

2 (Optional) To improve streaming performance, use Virtual Disk Manager to compress the virtual disk files (`.vmdk` files) for a virtual machine.

   See the *Virtual Disk Manager User's Guide,* in the Virtual Disk Development Kit.

3 Depending on the type of Web server, use the following keep-alive settings:

   - For Apache HTTP Server 1.2 and higher, turn the **KeepAlive** option on, set **MaxKeepAliveRequest** to 2000 to 5000, and set **KeepAliveTimeout** to 2000 to 5000 seconds, depending on server load.

   - For Microsoft Internet Information Services (IIS) 6.0 and higher, set the connection timeout to a value above 300 seconds and load **HTTP Keep-Alives**.

4 On proxy servers, set the proxy connection to **Keep-alive**.

5 Upload the virtual machine directory to the Web server.

After a virtual machine is placed on a Web server, users can use a URL to stream it and start it with Workstation or VMware Player. See "Start a Virtual Machine by Using VM Streaming" on page 147.

Sharing Virtual Machines with VMware Player

VMware Player is a free application that opens and plays virtual machines created with other VMware products. On Windows hosts, VMware Player also opens and plays Microsoft Virtual PC and Virtual Server virtual machines and Symantec LiveState Recovery and system images.

VMware Player is included with Workstation 5.5 and higher. "Standalone" Player is also freely available for download at http://www.vmware.com/products/player/

VMware Player makes your VMware virtual machines accessible to colleagues, partners, customers, and clients who do not own other VMware products.

NOTE Use of VMware Player is subject to the VMware Player End User License terms, and no technical support is provided by VMware for VMware Player.

Start and Exit VMware Player

VMware Player is included in the Workstation distribution. When you install Workstation, the application file (`vmplayer.exe` on Windows or `vmplayer` on Linux), is stored with the rest of your Workstation program files.

To start and exit VMware Player

1 Open VMware Player, either from the graphical user interface (GUI) or from the command line:

- From the GUI, on Windows, choose **VMware Player** from the **Start > Programs > VMware** menu.

  In a Linux X session, choose **VMware Player** from the corresponding program menu, such as the **System Tools** menu.

- From the command line, open a command prompt, and enter one of the following commands:

  - On Windows, enter `<path>`**`vmplayer.exe`**

    The `<path>` value is the path on your system to the application file.

  - On Linux, enter **`vmplayer &`**

  - To stream the virtual machine, use the command with the virtual machine URL (for example, `vmplayer http://server.acme.com/myVM.vmx`).

    For more information, see "Make Virtual Machines Available for Streaming from a Web Server" on page 214.

From the Welcome page, you can:

- Browse to a virtual machine file.
- Open a recently used virtual machine.
- Download a virtual appliance from the VMTN (VMware Technology Network) Web site.

2 Open a virtual machine.

For instructions on using and configuring VMware Player, see the online help provided in VMware Player. From the VMware Player menu bar, choose **VMware Player > Help**.

3 To exit VMware Player, do one of the following:

- Shut down the guest operating system in the virtual machine.

  VMware Player closes after the guest operating system shuts down.

- In VMware Player, choose **VMware Player > Exit** (Windows) or **VMware Player > Quit** (Linux).

VMware Player either suspends or powers off the virtual machine, depending on the preference you set for exit behavior in **VMware Player > Preferences**.

When you exit VMware Player that is using a streamed virtual machine, you are prompted to save or discard changes. If you discard changes, the directory that was created on your local machine and all the virtual machine data are deleted.

Setting Up Virtual Machines for Use with VMware Player

When you create a virtual machine that you intend to distribute to other users, configure the virtual machine for maximum compatibility with all expected host systems. Because the configuration options for VMware Player are limited, users are limited in their ability to make changes in a virtual machine so that it is compatible with their host systems.

Following are recommendations to help you configure virtual machines for maximum compatibility with VMware Player and with the widest range of host machines:

- Determine which virtual devices are actually required, and do not include any that are not needed or useful for the software you are distributing with the virtual machine and VMware Player. For example, generic SCSI devices are extremely unlikely to be appropriate.
- To connect a physical device to a virtual device, use the **Auto detect** options when configuring the virtual machine. The **Auto detect** options allow the virtual machine to adapt to the user's system, and they work whether the host operating system is Windows or Linux. Users who have no physical device receive a warning message.
- To connect a CD-ROM or floppy to an image file that you ship with the virtual machine, make sure the image file is in the same directory as the virtual machine. This way, a relative path, rather than an absolute path, is used.
- For both a physical CD-ROM and an image, provide two virtual CD-ROM devices in the virtual machine. VMware Player does not provide a way in the user interface to switch a single CD-ROM device between a physical CD-ROM and an image. This also means that if you want to ship multiple images, the user cannot switch between them.
- Choose a reasonable amount of memory to allocate to the virtual machine. If the user's host machine does not have enough physical memory to support the memory allocation, VMware Player cannot power on the virtual machine.
- Install VMware Tools in the virtual machine. VMware Tools significantly improves the user's experience working with the virtual machine.
- Choose a reasonable screen resolution for the guest. A user is likely to find it easier to increase the resolution manually than to deal with a display that exceeds the user's physical screen size.

- Some host operating systems do not support CD-ROMs in non-legacy mode. To ensure that CD-ROMs work properly in virtual machines that you intend to be distributed and played on VMware Player, configure CD-ROM devices in legacy mode. See “Legacy Emulation for DVD and CD Drives” on page 235.
- Select an appropriate setting in **VM > Settings > Options > Snapshots > When powering off.** Set this option to **Just power off** or **Revert to snapshot**. VMware Player does not allow taking snapshots.

  The option **Revert to snapshot** is useful if you want to distribute a demo that resets itself to a clean state when powered off.

Using Disks and Disk Drives 11

This chapter provides information about how to configure virtual hard disk storage to best meet your needs. This chapter includes the following topics:

Virtual Machine Disk Storage

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, Workstation provides ways to undo changes to the virtual machine's hard disk.

The New Virtual Machine wizard creates a virtual machine with one disk drive. Use the virtual machine settings editor (choose **VM > Settings**) to add more disk drives to your virtual machine, to remove disk drives from your virtual machine, and to change certain settings for the existing disk drives.

Benefits of Using Virtual Disks

In most cases, it is best to configure virtual machines to use virtual hard disks rather than physical hard disks. 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.

Portability

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 Workstation on a Windows host to create virtual disks, move them to a Linux computer, and use them with Workstation for Linux, and the reverse. See "Moving a Virtual Machine" on page 207.

Disk Size and Files

Virtual disks can be as large as 950GB (IDE or SCSI). Depending on the size of the virtual disk and the host operating system, Workstation creates one or more files to hold each virtual disk. These files include information such as the operating system, program files, and data files. The virtual disk files have a `.vmdk` extension.

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

You can also configure virtual disks so that all of the disk space is allocated when the virtual disk is created. This approach provides enhanced performance and is useful if you are running performance-sensitive applications in the virtual machine.

Regardless of whether you allocate all disk space in advance, you can configure the virtual disk to use a set of files limited to 2GB per file. Use this option if you plan to move the virtual disk to a file system that does not support files larger than 2GB.

Lock Files

A running virtual machine creates lock files to prevent consistency problems on virtual disks. Without locks, multiple virtual machines might read and write to the disk, causing data corruption.

Lock files are created in subdirectories with a `.lck` suffix. The locking subdirectories reside in the same directory as the virtual machine's `.vmdk` files. A locking subdirectory and lock file are created for `.vmdk` files, `.vmx` files, and `.vmem` files.

As of the Workstation 6.0 release, a unified locking method is used on all host operating systems, so files shared between them are fully protected. For example, if one user on a Linux host tries to power on a virtual machine that is already powered on by another user with a Windows host, the lock files prevent the second user from powering on the virtual machine.

When a virtual machine powers off, it removes the locking subdirectories and their lock files. If it cannot remove these locking controls, one or more stale lock files might remain. For example, if the host machine fails before the virtual machine removes its locking controls, stale lock files remain.

When the virtual machine restarts, it scans any locking subdirectories for stale lock files and, when possible, removes them. A lock file is considered stale if both of the following conditions are true:

- The lock file was created on the same host that is now running the virtual machine.
- The process that created the lock is no longer running.

If either of these conditions is not true, a dialog box warns you that the virtual machine cannot be powered on. You can delete the locking directories and their lock files manually.

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

IDE and SCSI Disk Types

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 with a driver for the LSI Logic or BusLogic SCSI adapter available in a Workstation virtual machine. You determine which SCSI adapter to use at the time you create the virtual machine.

NOTE To use SCSI disks in a 32-bit Windows XP virtual machine, download a special SCSI driver from the Downloads page of the VMware Web site. Follow the instructions on the Web site to use the driver with a fresh installation of Windows XP.

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 or SCSI virtual disk can be stored on an IDE hard disk or a SCSI hard disk. They can also be stored on other types of fast-access storage media.

Physical Disks

In some circumstances, you might need to give your virtual machine direct access to a physical hard drive on the host computer. A physical disk directly accesses an existing local disk or partition. You can use physical disks to run one or more guest operating systems from existing disk partitions.

CAUTION Do not attempt physical disk configurations unless you are an expert user.

Although virtual disks are limited to 950GB, physical disks can be set up on both IDE and SCSI devices of up to 2TB capacity. Booting from an operating system already set up on an existing SCSI disk or partition is currently not supported.

CAUTION Running an operating system natively on the host computer and switching 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 hardware. The steps you take depend on the operating system you want to use inside the virtual machine. See the VMware technical note *Dual-Boot Computers and Virtual Machines*.

You can also create a new virtual machine that uses a physical disk. See "Using Physical Disks in a Virtual Machine" on page 227. In most cases, however, it is better to use a virtual disk. If you use a physical disk, the `.vmdk` file stores information about the physical disk or partition that the virtual machine uses.

After you configure a virtual machine to use one or more partitions on a physical disk, do not modify the partition tables by running `fdisk` or a similar utility in the guest operating system.

If you use `fdisk` or a similar utility on the host operating system to modify the partition table of the physical disk, you must re-create the virtual machine's physical disk. All files that were on the physical disk are lost when you modify the partition table.

Virtual Disk Maintenance Tasks

Defragmenting virtual disks can improve performance. Shrinking virtual disks reclaims any unused space.

Defragment Virtual Disks

Like physical disk drives, virtual disks can become fragmented. Defragmenting disks rearranges files, programs, and unused space on the virtual disk so that programs run faster and files open more quickly.

Before you begin, make sure you have adequate free working space on the host computer. If your virtual disk is contained in a single file, for example, you need free space equal to the size of the virtual disk file. Other virtual disk configurations require less free space.

Defragmenting does not reclaim unused space on a virtual disk. To reclaim unused space, shrink the disk. See "Shrink a Virtual Disk" on page 224.

To defragment a virtual disk

1. Run a disk defragmentation utility inside the guest operating system.

   For example, in a virtual machine with a Windows XP guest operating system, use the Windows XP Disk Defragmenter tool from within the virtual machine.

   Defragmenting disks can take considerable time.

2. If the virtual disk is "growable" rather than preallocated, defragment it by using the Workstation defragmentation tool:

   a. Select the virtual machine.

   b. Make sure the virtual machine is powered off.

   c. Choose **VM > Settings**.

   d. On the **Hardware** tab, select **Hard Disk**, and do one of the following:

      - On Linux hosts, click **Defragment**.

      - On Windows hosts, click **Utilities** and choose **Defragment**.

   e. When the process is finished, click **OK**.

3. Run a disk defragmentation utility on the host computer.

   Defragmenting disks can take considerable time.

Shrink a Virtual Disk

Shrinking a virtual disk reclaims unused space in the virtual disk. If a disk has empty space, this process reduces the amount of space the virtual disk occupies on the host drive.

Before you begin, make sure the following prerequisites are met:

- VMware Tools is installed in the guest operating system.
- The host has free disk space equal to the size of the virtual disk you plan to shrink.
- The disk space is not preallocated for the virtual hard disk. Use the virtual machine settings editor to view the disk information for this virtual hard disk. If the disk space was preallocated, you cannot shrink the disk.
- The virtual machine has no snapshots. If it has a snapshot, a **Snapshot** line appears in its summary view.

  To delete a snapshot, choose **VM > Snapshot > Snapshot Manager**. Select the snapshot and click the **Delete** button (on Windows) or icon (on the snapshot toolbar on Linux).
- The virtual machine is not a linked clone or the parent of a linked clone. If the virtual machine is a linked clone, a **Clone of** line appears on its summary tab. If it is the parent of a linked clone, a **Snapshot** line appears on its summary tab.
- If the virtual hard disk is an independent disk, it is in persistent mode.

  To change the mode, see "Exclude a Virtual Disk from Snapshots" on page 193 for a description of independent disks.

To shrink a virtual disk

1. Launch the VMware Tools control panel:
   - For a Windows guest, double-click the **VMware Tools** icon in the notification area of the taskbar.

     If the icon is not available, choose **Start > Settings > Control Panel**, and double-click **VMware Tools**.
   - For a Linux, Solaris, or FreeBSD guest, open a terminal window, become root, and run `vmware-toolbox`.

     If you shrink disks as a nonroot user, you cannot wipe the parts of the virtual disk that require root-level permissions.
2. In the VMware Tools control panel, click the **Shrink** tab.

   If the virtual machine does not allow shrinking, the **Shrink** tab shows the reason.

3 Select virtual disks to shrink and click **Prepare to Shrink**.

If you deselect some partitions, the whole disk still shrinks. However, those partitions are not wiped for shrinking, and the shrink process does not reduce the size of the virtual disk as much as it would with all partitions selected.

VMware Tools reclaims all unused portions of disk partitions (such as deleted files) and prepares them for shrinking. During this phase, you can still interact with the virtual machine.

VMware Tools finishes wiping the selected disk partitions, a prompt to shrink disks appears.

4 Click **Yes**.

Shrinking disks can take considerable time.

5 Click **OK**.

Adding Virtual and Physical Disks to a Virtual Machine

This section provides instructions for creating virtual disks, removing disks, adding existing disks to virtual machines, and using physical disks in a virtual machine.

You can connect other SCSI devices to a virtual machine by using the generic SCSI driver for the host operating system. See "Add a Generic SCSI Device to a Virtual Machine" on page 346.

Add a New Virtual Disk to a Virtual Machine

Virtual disks are stored as files on the host computer or on a network file server. A virtual IDE drive or SCSI drive can be stored on a physical IDE drive or SCSI drive.

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.

To add a new virtual disk to a virtual machine

1 Select the virtual machine and choose **VM > Settings**.

2 On the **Hardware** tab, click **Add** to start the Add Hardware wizard.

3 On the Hardware Type page, select **Hard Disk** and click **Next**.

4 On the Select a Disk page, select **Create a new virtual disk** and click **Next**.

5 On the Select a Disk Type page, choose **IDE** disk or **SCSI**.

See "IDE and SCSI Disk Types" on page 221.

Workstation 6.x virtual machines can use up to 4 IDE devices and up to 60 SCSI devices. Any of these devices can be a virtual or physical hard disk or DVD or CD-ROM drive.

6 (Optional) To exclude disks from snapshots, in the **Mode** section, select **Independent** for the mode and choose one of the following options:

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

See "Information Captured by Snapshots" on page 192.

7 On the Specify Disk Capacity page, set the capacity for the new virtual disk.

You can set a size between 0.1GB and 950GB for a virtual disk. See "Disk Size and Files" on page 220.

8 On the Specify Disk File page, accept the default filename and location or browse to and select a different location and click **Finish**.

The wizard creates the new virtual disk. It appears to your guest operating system as a new, blank hard disk.

9 In the virtual machine settings editor, click **OK**.

10 Use the guest operating system tools to partition and format the new drive for use.

Add an Existing Virtual Disk to a Virtual Machine

You can reconnect an existing virtual disk that was removed from a virtual machine.

Workstation 6.x virtual machines can use up to 4 IDE devices and up to 60 SCSI devices. Any of these devices can be a virtual or physical hard disk or DVD or CD-ROM drive.

To map an existing virtual disk drive to a Windows host machine, rather than adding it to a virtual machine, see "Using a Mapped Drive for Windows Only" on page 184.

To add an existing virtual disk to a virtual machine

1 Select the virtual machine.

2 Choose **VM > Settings**.

3 On the **Hardware** tab, click **Add** to start the Add Hardware wizard.

4 On the Hardware Type page, select **Hard Disk** and click **Next**.

5 On the Select a Disk page, select **Use an existing virtual disk** and click **Next**.

6 On the Select an Existing Disk page, specify the path name and filename for the existing disk file and click **Finish**.

7 In the virtual machine settings editor, click **OK**.

Remove a Virtual Disk from a Virtual Machine

Removing a virtual disk disconnects it from a virtual machine. Removing the virtual disk does not delete files from the host file system.

After you remove the disk from the virtual machine, you can map or mount it to a host and copy data from the guest to the host without powering on the virtual machine or starting Workstation.

To remove a virtual disk from a virtual machine

1 Select the virtual machine.

2 Choose **VM** > **Settings**.

3 On the **Hardware** tab, select a virtual disk and click **Remove**.

After you remove the disk from the virtual machine, you can do either of the following:

- Map the disk to the host. See "Using a Mapped Drive for Windows Only" on page 184.
- Add the disk to another virtual machine. See "Add an Existing Virtual Disk to a Virtual Machine" on page 226.

Using Physical Disks in a Virtual Machine

You can install a guest operating system directly on an unused physical disk or unused partition. However, an operating system installed in this setting probably cannot boot outside of the virtual machine, even though the data is available to the host.

CAUTION Do not use a physical disk to share files between host and guest operating systems. It is not safe to make the same partition visible to both host and guest. You can cause data corruption if you do this. To share files between host and guest operating systems, use shared folders. See "Using Shared Folders" on page 177.

For information about using an operating system that can also boot outside of the virtual machine, see the VMware's *Dual-Boot Computers and Virtual Machines* technical note.

Physical disks are an advanced feature. Do not configure them unless you are an expert user. To use a physical disk in a virtual machine, you can add the physical disk to an existing virtual machine, or create a virtual machine and specify which physical disk the virtual machine uses.

NOTE Using a physical disk rather than a virtual disk is not an appropriate option for a virtual machine you intend to distribute as an ACE instance.

Prerequisites for Using a Physical Disk

Before you run the New Virtual Machine wizard or use the virtual machine settings editor to add a physical (raw) disk, perform the following tasks:

- Because the virtual machine and guest operating system access a physical disk partition while the host continues to run its operating system, verify that the partition is not mounted by the host or in use by another virtual machine.

  Corruption is possible if you allow the virtual machine to modify a partition that is simultaneously mounted on the host operating system.

- Check the guest operating system documentation regarding the type of partition on which the operating system can be installed.

  - On Windows Vista hosts, you cannot use the system partition or the physical disk that contains it in a virtual machine.
  - DOS, Windows 95, and Windows 98 operating systems must be installed on the first primary partition.
  - Other operating systems, such as Linux, can be installed on a primary or an extended partition on any part of the drive.

- Make sure the physical partition or disk does not have data you need in the future. If it does, back up the data.

- On Windows hosts:
  - If you use a Windows host's IDE disk in a physical disk configuration, make sure it is not configured as the slave on the secondary IDE channel if the master on that channel is a CD-ROM drive.
  - If your host is running Windows 2000, Windows XP, or Windows Server 2003, do not use a dynamic disk as a physical disk in a virtual machine. Use the disk management tool to check the disk type and change a dynamic disk to a basic disk, which destroys all data. See "Change a Windows Disk Type from Dynamic to Basic" on page 229.
  - Make sure the partition you want to use is unmapped. See "Unmap a Partition That Is Mapped to a Windows NT Host" on page 230.
- On Linux hosts, set the device group membership or device ownership appropriately. See "Set Permissions on Linux Hosts" on page 231.

After you determine that the physical disk meets these prerequisites, use either of the following strategies to use the physical disk in a virtual machine:

- "Create a Virtual Machine That Uses a Physical Disk" on page 231
- "Add a Physical Disk to an Existing Virtual Machine" on page 232

Change a Windows Disk Type from Dynamic to Basic

To use a hard disk in a virtual machine whose host is running Windows 2000, Windows XP, or Windows Server 2003, the virtual machine must use a basic disk.

To change a Windows disk type from dynamic to basic

1. On the host, choose **Start > Settings > Control Panel > Administrative Tools > Computer Management > Disk Management**.

   The disk management tool opens.

2. Delete all logical volumes on the disk.

   This action destroys all data on the disk.

3. Right-click the disk icon and select **Revert to Basic Disk**.
4. Partition the disk.

Unmap a Partition That Is Mapped to a Windows NT Host

Corruption can occur if you allow the virtual machine to modify a physical disk partition that is simultaneously used as a mapped drive on the host.

To unmap a partition that is mapped to a Windows NT host

1 Choose **Start > Programs > Administrative Tools**.

2 Highlight the partition on which you plan to install the guest operating system, and choose **Tools > Assign Drive Letter**.

3 Choose **Do not assign a drive letter for the partition** and click **OK**.

Unmap a Partition That Is Mapped to a Windows Server 2003, Windows XP, or Windows 2000 Host

Corruption can occur if you allow the virtual machine to modify a physical disk partition that is simultaneously used as a mapped drive on the host.

To unmap a partition that is mapped to a Windows Server 2003, Windows XP, or Windows 2000 host

1 Choose **Start > Settings > Control Panel > Administrative Tools > Computer Management > Storage > Disk Management**.

2 Select a partition and choose **Action > All Tasks > Change Drive Letter and Paths**.

3 Click **Remove**.

Unmap a Partition That Is Mapped to a Windows Vista Host

Corruption can occur if you allow the virtual machine to modify a physical disk partition that is simultaneously used as a mapped drive on the host.

To unmap a partition that is mapped to a Windows Vista host

1 Choose **Start > Control Panel (Classic View) > Administrative Tools > Computer Management > Storage > Disk Management**.

2 Right-click a partition and choose **Change Drive Letter and Paths**.

3 Click **Remove**.

Set Permissions on Linux Hosts

If permissions are set correctly, the physical disk configuration files in Workstation guard access. This reliability provides boot managers access to configuration files and other files they might need to boot operating systems. For example, LILO needs to read `/boot` on a Linux partition to boot a non-Linux operating system that might be on another drive.

To set permissions on Linux hosts

1 Make sure the master physical disk device or devices are readable and writable by the user who runs Workstation.

- Physical devices, such as `/dev/hda` (IDE physical disk) and `/dev/sdb` (SCSI physical disk), belong to group-id `disk` on most distributions. 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. Consider all the security issues involved in this option.

2 Grant VMware Workstation users access to all `/dev/hd[abcd]` physical devices that contain operating systems or boot managers.

Create a Virtual Machine That Uses a Physical Disk

Use the New Virtual Machine wizard to create a new virtual machine that uses a physical disk rather than adding a physical disk to an existing virtual machine.

Before you begin, complete the tasks described in "Prerequisites for Using a Physical Disk" on page 228.

To create a virtual machine that uses a physical disk

1 Use the Custom setup in the New Virtual Machine wizard to create a virtual machine that uses a physical disk.

2 On the Select a Disk page of the wizard, select **Use a physical disk**, and choose to use individual partitions or the entire disk.

If you use individual partitions, only the partitions you select are accessible to the virtual machine. The other partitions might be visible to the guest operating system, but you cannot mount, access, or format them.

3 (Optional) To specify a device node for the virtual disk or exclude disks from snapshots, do the following:

   a Select the virtual machine and choose **VM > Settings**.

   b On the **Hardware** tab, select the physical disk and click **Advanced**.

   c To change the device node, select from the **Virtual device node** list.

   d To exclude disks from snapshots, select **Independent** for the mode and choose one of the following options:

   - **Persistent** – Changes are immediately and permanently written to the disk.

   - **Nonpersistent** – Changes to the disk are discarded when you power off or revert to a snapshot.

   See "Information Captured by Snapshots" on page 192.

4 Install the guest operating system on the physical disk.

For more information about supported operating systems, see the *VMware Guest Operating System Installation Guide*. This guide is available from the Workstation **Help** menu.

Add a Physical Disk to an Existing Virtual Machine

Use the virtual machine settings editor, rather than the New Virtual Machine wizard, to add a physical disk to an existing virtual machine.

Before you begin, complete the tasks described in "Prerequisites for Using a Physical Disk" on page 228.

CAUTION After you add a virtual machine disk by using one or more partitions on a physical disk, never modify the partition tables by running `fdisk` or a similar utility in the guest operating system. If you do so, you must re-create the virtual machine's physical disk.

To add a physical disk to an existing virtual machine

1 Select the virtual machine.

2 Make sure the virtual machine is powered off.

3 Choose **VM > Settings**.

4 On the **Hardware** tab, click **Add**.

5 On the Hardware Type page, select **Hard Disk** and click **Next**.

6 On the Select a Disk page, select **Use a physical disk** and click **Next**.

7 If a warning appears, click **OK**.

8 On the Select a Physical Disk page, do the following:

   a Choose the physical hard disk to use from the drop-down list.

   Workstation supports physical disks up to 2TB.

   b Select whether you want to use the entire disk or only individual partitions on the disk and click **Next**.

9 If you selected **Use individual partitions**, select the partitions you want to use in the virtual machine and click **Next**.

The virtual machine can access only the partitions you select. The guest operating system might be able to detect other partitions, but you cannot mount, access, or format them.

10 On the Specify Disk File page, accept the default filename and location or browse to a different location.

11 (Optional) To specify a device node for the virtual disk or exclude disks from snapshots, do the following:

   a On the Specify Disk File page, click **Advanced**.

   b To change the device node, select from the **Virtual device node** list.

   c To exclude disks from snapshots, select **Independent** for the mode and choose one of the following options:

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

   See "Information Captured by Snapshots" on page 192.

12 Click **Finish**.

13 Use the guest operating system's tools to format any partitions on the physical disk that are not formatted for your guest operating system.

Adding DVD/CD-ROM and Floppy Drives to a Virtual Machine

Workstation 6.x virtual machines can use up to 4 IDE devices and up to 60 SCSI devices. Any of these devices can be a virtual or physical hard disk or DVD or CD-ROM drive.

A virtual machine can read data from a DVD disc. Workstation does not support playing DVD movies in a virtual machine. You might be able to play a movie if you use a DVD player application that does not require video overlay support in the video card.

Add DVD or CD Drives to a Virtual Machine

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

You can configure the virtual DVD or CD drive as either IDE or SCSI regardless of the type of physical drive you connect it to. For example, if your host computer has an IDE CD drive, you can set up the virtual machine drive as either SCSI or IDE and connect it to the host drive. The same is true if the physical drive on the host is a SCSI drive.

To add a DVD or CD drive to a virtual machine

1. Select the virtual machine.
2. Choose **VM > Settings**.
3. On the **Hardware** tab, click **Add**.
4. On the Hardware Type page, select **DVD/CD-ROM Drive** and click **Next**.
5. Make a selection on the Select a Drive Connection page and click **Next**.
6. (Optional) If you select **Use physical drive**:

   a. Choose a drive from the drop-down list or choose **Auto detect**.

   b. To avoid connecting the CD drive when the virtual machine starts, deselect **Connect at power on**.

   c. To specify which device node the drive uses in the virtual machine, click **Advanced**.

      Select **Legacy emulation** only if you experienced problems using normal mode. See “Legacy Emulation for DVD and CD Drives” on page 235.

   d. Click **Finish**.

7 (Optional) If you select **Use ISO image**:

   a Enter the path and filename for the image file or browse to the file.

   b To avoid connecting the CD drive when the virtual machine starts, deselect **Connect at power on**.

   c To specify which device node the drive uses in the virtual machine, click **Advanced**.

   d Click **Finish**.

   The drive is set up initially so that it appears as an IDE drive to the guest operating system.

8 (Optional) To make the drive appear to the guest operating system as a SCSI drive, click the entry for that drive in the virtual machine settings editor and edit the settings in the panel on the right.

Legacy Emulation for DVD and CD Drives

In normal mode (that is, not legacy emulation mode), the guest operating system communicates directly with the CD or DVD drive. This direct communication enables you to read multisession CDs, perform digital audio extraction, view videos, and use CD and DVD writers to burn discs.

Legacy emulation mode enables you to read only from data discs in the DVD or CD drive. It does not provide the other capabilities of normal mode. Use legacy emulation mode to work around direct communication problems between a guest operating system and a DVD or CD drive.

Use the virtual machine settings editor (**VM > Settings**) to set the **Legacy emulation** option for DVD and CD drives attached to the virtual machine:

- On Windows hosts, this option is deselected by default.
- On Linux hosts with IDE drives, the default setting depends on whether the `ide-scsi` module is loaded in your kernel. The `ide-scsi` module must be loaded, or you must be using a physical SCSI drive to connect directly to the DVD or CD drive.

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

Add a Floppy Drive to a Virtual Machine

You can add up to two floppy drives to a virtual machine. 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.

To add a floppy drive to a virtual machine

1 Select the virtual machine.

2 Make sure the virtual machine is powered off.

3 Choose **VM > Settings**.

4 On the **Hardware** tab, click **Add**.

5 On the Hardware Type page, select **Floppy Drive** and click **Next**.

6 Follow the instructions to complete the wizard.

7 (Optional) If you are adding a second floppy drive to the virtual machine, enable this second floppy drive in the virtual machine BIOS, as follows:

   a Select the virtual machine and choose **VM > Power > Power On to BIOS**.

   b On the main screen, choose **Legacy Diskette B:** and use the plus (+) and minus (-) keys on the numerical keypad to select the type of floppy drive to use.

   c Press F10 to save the settings.

Connect a CD-ROM, DVD, or Floppy Drive to an Image File

You can connect an existing virtual CD-ROM, DVD, or floppy drive to an image file (ISO file) rather than the physical drive on the host. An ISO image file resembles a CD-ROM to your guest operating system and even appears as a CD-ROM in Windows Explorer.

In some host configurations, the virtual machine cannot boot from the installation CD-ROM. To avoid that problem, create an ISO image file from the installation CD-ROM.

To connect a CD-ROM, DVD, or floppy drive to an image file

1 Select the virtual machine.

2 Choose **VM > Settings**.

3 On the **Hardware** tab, select a DVD, CD-ROM, or floppy drive.

4 Do one of the following:

    - For a DVD or CD-ROM drive, select **Use ISO Image** and specify the path name and filename.
    - For a floppy drive:
        - If the file already exists, select **Use floppy Image** and specify the path name and filename.
        - To create an image file, click **Create**, browse to the directory where you plan to store the floppy image file, supply a filename, and click **Save** (on Windows hosts) or **Open** (on Linux hosts).

5 (Optional) To make the file read only, select the **Read Only** check box.

6 Click **OK**.

Using VMware Virtual Disk Manager

VMware Virtual Disk Manager is a Workstation utility that allows you to create, manage, and modify virtual disk files from the command line or in scripts.

You can enlarge a virtual disk so that its maximum capacity is larger than it was when you created it. This is useful if you need more disk space in a given virtual machine, but do not want to add another virtual disk or use ghosting software to transfer the data on a virtual disk to a larger virtual disk. You cannot do this with physical hard drives.

You can also change disk types. When you create a virtual machine, you specify how disk space is allocated, as follows:

- All space for the virtual disk is allocated in advance. This corresponds to the preallocated disk type for Virtual Disk Manager.
- Space allocated for the virtual disk begins small and grows as needed. This corresponds to the growable disk type for Virtual Disk Manager.

If you allocate all the disk space for a virtual disk but later need to reclaim some hard disk space on the host, you can convert the preallocated virtual disk into a growable disk. The new virtual disk is still large enough to contain all the data in the original virtual disk.

You can also change whether the virtual disk is stored in a single file or split into 2GB files.

These features and the ability to use scripting to automate management of virtual disks were added to Workstation in version 5.0. See the VMware technical note about using Virtual Disk Manager.

Using Dual-Boot Computers with Virtual Machines

Some users install Workstation on a dual-boot or multiple-boot computer so that they can run one or more of the existing operating systems in a virtual machine. For more information about using dual-boot computers with Workstation, see the VMware *Dual-Boot Computers and Virtual Machines* technical note.

Legacy Virtual Disks

You have several options for using Workstation 6.5 in a mixed environment with virtual machines that were created with earlier versions of Workstation or created with other VMware products.

For compatibility information, see the *VMware Virtual Machine Mobility Planning Guide*.

You can use Workstation 6.5 to power on virtual machines created with older versions of Workstation or other VMware products. However, many new features of Workstation are not available in older virtual machines. To upgrade your virtual machines to Workstation 6.5, see "Change the Version of a Virtual Machine" on page 91.

If you decide not to upgrade a virtual machine, VMware recommends that you upgrade VMware Tools to the latest version. See "VMware Tools Update Process" on page 113. Do not remove the older version of VMware Tools before installing the new version.

You can also use Workstation to create a version 4, 5, or 6.0 virtual machine. See "Use the New Virtual Machine Wizard" on page 86. Use the Custom setup in the wizard.

NOTE If you have Workstation 2 or 3 virtual machines that you want to use with Workstation 6.5, upgrade the virtual machines to at least Workstation version 4 before you attempt to power them on with Workstation 6.5.

Recording and Replaying Virtual Machine Activity 12

The record/replay feature allows you to record all of a Workstation 5, 6, or 6.5 virtual machine's activity over a period of time. This chapter includes the following topics:

Uses of the Record/Replay Feature

Unlike Workstation's movie-capture feature, the record/replay feature records all the processor instructions of the virtual machine throughout the time of the recording. This feature helps software developers and QA engineers to record a bug and attach a debugger while replaying the recording.

After you enable the record/replay feature for a virtual machine, click the **Record** button in the toolbar to start the recording and click **Stop** to end the recording. You can make multiple recordings and use the snapshot manager to name, delete, and play them. While you are making a recording you can insert markers to return to events and replay them. You can also make an execution trace file of a recording, to record events that occur during the recording.

Playing a recording is in some respects similar to going to a snapshot. When you play a recording, you discard the current state of the virtual machine and go to the recording. At any time when the recording is playing, you can click the **Go Live** button and resume interacting with the guest operating system at the state the virtual machine is in when you click **Go Live**.

NOTE Virtual machine recordings are not interchangeable between different versions of Workstation. Recordings created using earlier Workstation releases or beta releases cannot be replayed using the current version of Workstation. If you have created recordings with an earlier release, you must delete them.

Physical and Virtual Hardware Requirements

Following is a list of requirements for and limitations of this feature:

- **Host CPUs** – Record/replay support is limited to certain processors on the host. If you use the record/replay feature on a host computer that does not have an Intel P4 processor, when you enable the record/replay feature and power on the virtual machine, a message appears, informing you that recording is not supported on your processor.

  Supported processors include Intel Pentium 4, Intel Core 2 and later versions, AMD Barcelona and later versions, Next-Generation Intel Microarchitecture - Penryn/Harpertown. Other processors might operate more slowly during recording and replaying.

  NOTE If the record/replay feature is unstable on your P4 system, disable hyperthreading and logical processors in the BIOS.

  When these features are enabled in BIOS, other applications using performance counters may interfere with the virtual machine running in the record/replay mode. An example of an application using performance counters is the performance profiling tool.

  To assign two virtual processors to a virtual machine on any host machine that has at least two logical processors select **VM > Settings > Hardware > Processors** and choose the virtual processor. In the **Preferred mode** drop-down menu, choose **Automatic** or **Automatic with Replay** to let Workstation choose the execution mode based on the guest operating system and the host CPU. **Automatic with Replay** refers to the execution record/replay feature.

  For many combinations of CPU and guest operating system, you can choose **Automatic** and still use the record/replay feature. If not, an error message directs you to choose **Automatic with Replay**.

  Choosing **Automatic** or **Automatic with Replay** means that Workstation chooses one of the following:

  - **Binary translation** – Uses a mix of directly executing guest code and binary translation to run the guest. This option uses shadow page tables to map guest memory.
  - **Intel VT-x or AMD-V** – Uses hardware extensions to run and isolate guest code. This option also uses shadow page tables to map guest memory.
  - **Intel VT-x/EPT or AMD-V/RVI** – Uses hardware extensions to run and isolate guest code. This option uses hardware paging support to map guest memory.

  The choice depends on which mode provides the best performance for the selected guest operating system on the host's CPU.

- **Virtual machine version** – Only Workstation 5, 6, and 6.5 virtual machines can be recorded.
- **Supported operating systems** – You can use the record/replay feature only on 32-bit versions of the following guest operating systems:
  - Windows 2000, XP, 2003, Vista
  - Red Hat Enterprise Linux 3 and 4
  - SUSE Linux 9.3 and 10.x
  - 64-bit versions have experimental support
- **Unsupported operating systems** – If you attempt to enable the record/replay feature on an unsupported operating system, the virtual machine does not power on until you disable record/replay. In addition, SMP and paravirtualization on VMI are not supported with record/replay.
- **Unsupported virtual devices** – Avoid connecting the virtual machine to a network or disconnecting it during a recording session.

- **Disk space** – How much disk space a recording uses depends on the type of activity that occurs on the virtual machine and the duration of the recording session. By default, a screenshot is created every five seconds. Therefore, assume that you will need several megabytes of disk space for one minute of recording.

  NOTE Having a number of virtual machines with high-resolution display settings open on the screen consumes more disk space.

- **Disk mode** – You cannot use the record/replay feature if the virtual machine's virtual hard disk is set to independent mode. Recording virtual machine activity requires writing data about the disk to a continual snapshot. Use the virtual machine settings editor to change the disk mode (choose **VM > Settings > Hardware > Hard Disk > Advanced**).

Configure Record/Replay for a Virtual Machine

Make sure that the virtual machine meets the requirements listed in "Physical and Virtual Hardware Requirements" on page 240.

To configure record/replay for a virtual machine

1. Make sure the virtual machine is powered off.
2. Select the virtual machine and choose **VM > Settings.**
3. Click the **Options** tab and select **Snapshot/Replay.**
4. (Optional) On the **Replay** settings panel as a safety precaution, use the **When Recording** controls to limit how much disk space the recording can use.
   - Setting the Maximum disk space to **Unlimited** uses much more disk space than setting it to **2GB**.
   - Selecting **Save the last** sets the duration of the time to save the recording.
   - Setting **Marker frequency** to **5 min** uses much more disk space than setting it to **Never**.
5. (Optional) Select the **Enable VAssert (experimental)** check box to use VMware VAssert to debug applications.

   VAssert enables developers and support engineers to take advantage of traditional assert and logging capabilities to debug errors in replay logs. The asserts appear only during replay of a recording.
6. Click **OK**.

Record Control Dialog Box Features

On Windows, a record control dialog box appears when you click the **Record** button in the toolbar. On Linux, the record options are located in the toolbar.

- **Stop** – Stops the recording that is in progress.
- **Add Marker** – Takes a replay-specific snapshot at the current location within the recording. You can use this marker during replay to skip ahead in a recording.
- **Minimize** – On Windows and Linux hosts, the **(-)** button minimizes the record control dialog box to the lower-left side of the status bar. The minimized mode allows you to work on the virtual machine and use the controls in the status bar to either stop a recording or add a marker.
- **Maximum disk space** – Shows the maximum disk space quota allocated for the recording.
- **Saving the last** – Displays the approximate duration of time where the end of a recording is saved. For example, if you are saving the last 30 minutes of the recording, as the recording continues, only the last 30 minutes of the virtual machine activity is saved at any given time.
- **Marker Frequency** – Shows the frequency when an automatic marker is added to the recording.
- **Next auto marker** – Displays when the next automatic marker is going to be added to the recording.
- **Last marker** – Indicates when the last marker was added to the recording.

NOTE You cannot close the record control dialog box.

Replay Control Dialog Box Features

The replay control dialog box appears when you replay a recording.

Figure 12-1. Windows Replay Control Dialog Box

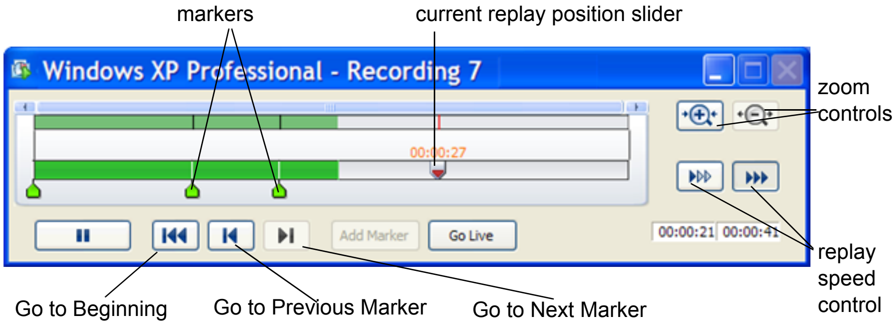
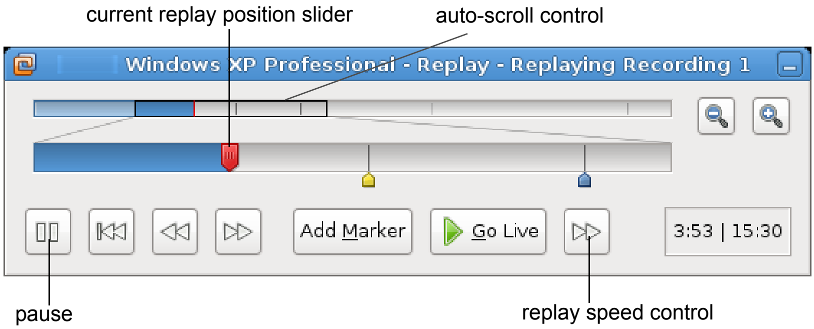


Figure 12-2. Linux Replay Control Dialog Box


current replay position slider
auto-scroll control
Windows XP Professional - Replay - Replaying Recording 1
Add Marker
Go Live
3:53 | 15:30
pause
replay speed control

The replay control dialog box contains the following buttons:

- **Play/Pause** – Plays the last recording you made for the selected virtual machine. If the virtual machine is powered off, the recording is resumed, as if it had been suspended. If you click the same button once the replay is paused. To resume replay click the button again.
- **Go Live** – Stops the replay that is in progress and reverts to the current state of the virtual machine.

- **Add Marker** – Takes a replay-specific snapshot at the current location within the recording. You can use this marker during replay to skip ahead in a recording.
- **Go to Beginning** – Returns to the beginning of the recording.
- **Go to Previous Marker** – Replays the recording to the point where the previous marker is located and pauses the playback.
- **Go to Next Marker** – Replays the recording to the point where the next marker is located and pauses the playback.
- **Current replay Position Slider** – Allows you to preview a replay. You can drag the slider to the nearest previous marker and start replaying. On Linux, the auto-scroll function of the zoomed in portion is enabled. The **Current Replay Position Slider** is a red arrow located in the progress timeline.
- **Zoom control** – Controls the zoom in and out function during replay.
- **Minimize** – The **(-)** button minimizes the dialog box to the bottom left-hand side of the status bar. The minimized mode allows you to view the recording in the virtual machine and use the controls in the status bar. The progress indicator in the status bar shows the timeline of the recording.

  NOTE You cannot close the replay control dialog box.

- **Replay speed control** – Controls the replay speed of a recording. On Windows, click the right button to increase the replay speed to the maximum. Click the left button to decrease the replay speed to normal. On Linux, click button to toggle between speeds.

  NOTE The speed of a playback depends on the host activity and workload of the guest.

Make a Recording

You cannot use record/replay to record a 3-D application. While making a recording you cannot pause or reverse it. For more information about enabling record/replay see "Configure Record/Replay for a Virtual Machine" on page 242.

Before you begin, verify the screen resolution settings. The existing screen resolution is used in the virtual machine while replaying a recording. The resolution cannot be changed during replay.

To make a recording

1 Power on the virtual machine.

2 To begin recording choose **VM > Replay > Record**.

A recording-specific snapshot is taken, and the recording dialog box indicates that recording is in progress.

If the **Record** command is unavailable, the feature might not be enabled or the hard disk might be set to independent mode.

3 To add a marker during recording, click **Add Marker** in the recording dialog box**.**

Aside from the markers you add, markers are automatically added according to the frequency you set by using the virtual machine settings editor.

4 To stop recording, click the **Stop** button in the recording dialog box or in the toolbar.

(Optional) On Windows, while making a recording you can use the minimized record control to stop a recording or add a marker.

5 Complete the dialog box that appears and click **Save**.

6 To change the name of the recording, add or change the description, or delete the recording, choose **VM > Snapshot > Snapshot Manager**.

Replay a Recording

If you change from windowed mode to full screen mode during replay, the auto-fit feature does not work.

To replay a recording

1 Select the virtual machine.

2 If it is powered on and you do not want to lose the current state of the virtual machine, take a snapshot of it.

For instructions, see "Take a Snapshot" on page 196.

3 To play the latest recording of the virtual machine choose **VM > Replay > Replay <name_of _recording>**.

On Windows, while replaying a recording you can use the controls in the minimized replay control.

4 To play an earlier recording, use the snapshot manager, as follows:

   a Choose **VM > Snapshot > Snapshot Manager**.

   b Select the recording snapshot to play and click **Replay**.

   If you stop the recording before it is finished replaying by clicking the **Go Live** button and replay the recording again, the recording starts from the beginning, not from the point where you clicked **Go Live**.

   A snapshot of a recording is shown in Figure 9-4, "Snapshot Manager on a Windows Host," on page 194.

5 In the dialog box that appears, confirm that you want to start replaying the recording.

6 To suspend the replay, click the **Pause** button in the replay control dialog box. The button toggles to a **Play** button so that you can click it again to resume playing the recording.

7 (Optional) To make a trace file of events that occurred during recording, see "Create an Execution Trace File of a Recording" on page 248.

8 (Optional) To stop replaying the recording before it finishes playing, click the **Go Live** button to stop the replay and resume interacting with the virtual machine.

Browse a Recording

The length of a recording can vary from a few minutes to several hours. When the recording is several hours long, use the position slider to access the recording at random intervals. On Windows and Linux hosts, zoom in and out of the recording by using the zoom controls. Use the zoomed in auto scroll function to browse the recording.

To browse a recording

1 Drag the slider from the current position in the recording to another specific position.

   The new slider position must have a 16 seconds interval from the previous position.

2 (Optional) In the confirmation dialog box, select the check box **Never show this again.**

   The dialog box stops reappearing every time you browse a recording.

3 Click **OK**.

   The virtual machine reverts to the nearest previous snapshot and starts replaying until it reaches the target location. During the replay, the slider remains at the same point and the remaining playback time appears in red above the slider. For more information, see Figure 12-1.When the recording reaches the slider's position, the recording is paused.

Create an Execution Trace File of a Recording

Trace files are detailed logs produced by a program that are helpful for debugging. When you make an execution trace file of a recording, you can view all the events that occurred during the recording.

To create an execution trace file of a recording

1 Open the preferences file with a text editor.

This files is located in:

- On Windows hosts, `c:\Documents and Settings\<user>\Application Data\VMware\preferences.ini`
- On Linux hosts, `~/vmware/preferences`

2 Add the following line to the preferences file:

```
pref.replay.enableTrace = "TRUE"
```

3 Start play back of a recording, as described in "Replay a Recording" on page 246.

4 In the replay dialog box, click **Trace** to start the trace file.

The play back speed of the recording slows considerably while the trace file is created.

5 To end the trace file, click **Trace** again.

Otherwise, the trace file ends when the recording finishes playing.

Maintenance Tasks for Using Recordings

Depending on the length of a recording, the number of its periodic screenshots, and the number of recordings, the disk space used for the record/replay feature can be considerable. When you create recordings, Workstation goes into full debugging mode.

Delete a Recording

Delete recordings that you do not need to free disk space.

To delete a recording

1 Select the virtual machine.

2 Choose **VM** > **Snapshot** > **Snapshot Manager**.

3 In the Snapshot Manager window, select the recording to delete.

4 Right-click and choose **Delete > Recording and Children**.

If you select a recording and click the **Delete** button, the selected recording is removed and the corresponding snapshots in the recording remain intact.

Disable Periodic Screenshots

If the recording session lasts for a long time, a significant number of screenshots are automatically created in the virtual machine directory. Even when periodic screenshots are disabled, one screenshot is taken at the end of every recording.

To disable periodic screenshots

1 Add the following line to the configuration (`.vmx`) file for the virtual machine where X denotes the interval of screenshots taken in seconds. The default value for X is 15 seconds.

```
snapshot.periodicScreenshots = "X"
```

2 To disable periodic screenshots, change the value of X to 0.

3 Save and close the configuration file.

Configuring Teams 13

This chapter describes what virtual machine teams are used for, how to create them, and how to configure them. This chapter includes the following topics:

Benefits of Using Teams

Workstation teams allow you to set up a virtual computer lab on one host computer. Use a team to power on multiple associated virtual machines with a single click.

You can use teams to do the following:

- **Virtualize multitier environments** – Start separate client, server, and database virtual machines with one click. Configure startup delay times so clients do not submit queries before the server is ready.

  Setting a startup delay between the booting of virtual machines also avoids overloading the CPU of the host.

- **Virtualize multiple-machine testing environments** – Set up a software package for QA on a virtual machine, and configure automation on other virtual machines to test the first.

- **Virtualize network performance and security –** Team virtual machines can use networking just as other virtual machines can. In addition, team members can communicate in private networks called LAN segments. Team networking lets you to do the following:

  - Isolate a team completely from the host network. A team LAN segment is undetectable and inaccessible from any other network.
  - Create a virtual DMZ or proxy server to securely bridge the team members to the outside network.
  - Allow specific network bandwidth and packet loss to each virtual machine on the team.
  - Connect all team members fully to host resources.

  You control all traffic allowed between the host network and team virtual machines.

- **Monitor multiple virtual machines –** Use thumbnail views of the virtual machine displays to review activity on team virtual machines simultaneously.

Managing Teams

Managing teams requires creating, deleting, opening, closing, and changing the names of teams.

Create a Team

Use the New Team wizard to create a team and add virtual machines.

Before creating a team, if you plan to add virtual machines to the team while completing the New Team wizard, take these actions:

- Power off any virtual machines that you want to add to the team.
- Power off any virtual machines that you want to clone if you intend to create a clone and add it to the team.

You can instead add virtual machines after you create the team, by using the **Team** menu.

NOTE Workstation 4 virtual machines cannot be added to teams.

To create a team

1. From the Workstation menu bar, choose **File > New > Team**.
2. In the New Team wizard, supply the following information:

    a. Enter a name for the team and specify the location of the virtual team files.

    By default, the team files are stored in the same directory as virtual machines. See "Virtual Machine Location" on page 81.

    b. Specify whether to add virtual machines to the team now or later.

    If you want to add virtual machines now, you have the following options:

    - **New Virtual Machine** – Launches the New Virtual Machine wizard. See "Use the New Virtual Machine Wizard" on page 86.
    - **Existing Virtual Machine** – Opens a file browser from which you can navigate the host file system to locate an existing `.vmx` file.

        When you add a virtual machine to a team it can no longer be accessed outside the team. See "Add a Virtual Machine to a Team" on page 257.
    - **New Clone of Virtual Machine** – Opens a file browser from which you can navigate the host file system to locate an existing `.vmx` file. After you select a virtual machine, Workstation launches the Clone Virtual Machine wizard. See "Creating Clones" on page 205.

    c. Specify whether to add one or more LAN segments.

    You can add LAN segments after you create the team by using the **Team** menu. If you add LAN segments while creating the team, you can change default names and bandwidth later. See "Working with Team Networks" on page 260.

After the team is created, you can add it to the **Favorites** list. Use the **Team** menu to configure the team further, or to add and remove virtual machines.

Open a Team and Add It to the Favorites List

Opening a team displays its summary tab but does not power on the virtual machines included in the team.

To open a team and add it to the Favorites list

1. From the Workstation menu bar, choose **File > Open**.
2. Browse to the location of the `.vmtm` file for the team you want.
3. Select the file and click **Open**.
4. (Optional) To add the team to the **Favorites** list, choose **File > Add to Favorites**.

   After a team is added to the **Favorites** list, you can open it by clicking it in the **Favorites** list rather than using the menu bar.

You can now power on one or more of the virtual machines in the team. See "Power On a Team" on page 259.

Rename a Team

When you create a team, the name of the directory where the team (`.vmtm`) file is stored is based on the name you originally give the team. Although you can change the name of the team, the name of this file does not change.

To rename a team

Do one of the following:

- If the team is in the **Favorites** list, right-click it and choose **Rename**. Type the new name and press Enter.
- Select the team and choose **Team > Settings > Options**. Type a new name in the **Team name** field and click **OK**.

Power Off or Close a Team

Powering off a team means shutting down all the virtual machines in the team. The virtual machines are powered off in reverse order of that shown in the startup sequence. See "Specify the Startup Sequence for a Team" on page 258.

Closing a team removes its summary tab from the Workstation window. Depending on how you set Workstation preferences, closing a team might require powering off the team.

To power off or close a team

Depending on which operation you want to perform, do one of the following:

- To power off the team, select it and choose **Team > Power > Power Off**.

  Depending on how you configured power operations, the guest operating system might be shut down before the virtual machine is powered off. See "Configure Power Off and Reset Options for a Virtual Machine" on page 149.

- To close the team, select it and choose **File > Close**.

  Depending on how Workstation preferences are set, if any of the team's virtual machines are still powered on, you might see a prompt. For information about the options shown in the prompt, see "Closing Virtual Machines and Exiting Workstation" on page 69.

Delete a Team

Before you can delete a team, you must power off all virtual machines that are members of the team. See "Power Off or Close a Team" on page 255.

When you delete a team, you can choose to delete:

- Only the team (retaining the virtual machines in the team)
- The team and the virtual machines in the team

To remove a team from the Workstation window rather than deleting it, see "Remove a Virtual Machine from a Team" on page 258.

CAUTION Deleting a team permanently removes the team files from the host file system and removes associated LAN segments from all virtual machines. Deleting the team's virtual machines along with the team removes the virtual machine files permanently.

To delete a team

1. Select the team and choose **Team > Delete from Disk**.
2. Complete the dialog box that appears:
   - To delete the team without deleting the virtual machines in it, choose **Delete**.
   - To delete the team and the virtual machines in it, choose **Delete Team and VMs**.

   When you delete a team, you also delete all team LAN segments. The virtual network adapters associated with deleted LAN segments become disconnected. Bridged, host-only, NAT, and custom configurations remain unchanged.
3. Click **OK**.

Summary and Console Views for Teams and Their Virtual Machines

Workstation displays teams in a summary view or console view:

- The summary view is available at any time. See "Summary View" on page 54.
- The console view is available only when a team is powered on. A grab bar allows you to resize the areas. This view displays a large console view of the selected virtual machine and thumbnail console views of the other virtual machines in the team. Thumbnail views show the order of the startup sequence, from left to right and top to bottom.

If the team contains many virtual machines, you might need to scroll the thumbnails to view all the virtual machines. The thumbnails are displayed in the same order as the team's startup sequence. The left-most virtual machine is the first one in the sequence.

Workstation updates thumbnails in real time, to display the actual content of the virtual machine screens. The active virtual machine is the one you select or switch to by using the **Team > Switch To** menu. It appears in the lower pane of the console. Its thumbnail is represented by the **VMware** icon.

Workstation menus and commands directly affect only the active virtual machine, and you can use the mouse and keyboard to interact directly with the active virtual machine.

In full screen mode, Workstation displays only the active virtual machine. See "Use Full Screen Mode" on page 154.

Managing the Members of a Team

Managing members of a team requires adding virtual machines to a team, removing them from a team, and setting the order in which members of a team start and stop.

Add a Virtual Machine to a Team

Before you add a virtual machine to a team, consider these issues:

- A virtual machine is not powered on when you add it to a running team. You must power on the added virtual machine manually to use it during the current session. The added virtual machine is thereafter powered on or off with the rest of the team.
- When you add a virtual machine to a team, you can no longer operate the virtual machine outside the team. Adding a virtual machine to a team therefore removes it from the **Favorites** list.

NOTE Workstation 4 virtual machines cannot be added to teams.

To add a virtual machine to a team

Select the team, choose **Team > Add**, and choose one of the following options:

- **New Virtual Machine** – Launches the New Virtual Machine wizard. See "Use the New Virtual Machine Wizard" on page 86.
- **Existing Virtual Machine** – Opens a file browser from which you can navigate the host file system to locate an existing `.vmx` file.

  When you add a virtual machine to a team it can no longer be accessed outside the team.
- **New Clone of Virtual Machine** – Opens a file browser from which you can navigate the host file system to locate an existing `.vmx` file. After you select a virtual machine, Workstation launches the Clone Virtual Machine wizard. See "Creating Clones" on page 205.

Remove a Virtual Machine from a Team

Remove a virtual machine from a team when you want to use the virtual machine independently. That is, it does not need to be started up or shut down before or after any other virtual machine. It also does not need to be in a private team network.

NOTE When you remove a virtual machine from a team, you also remove it from team LAN segments. Virtual network adapters associated with LAN segments become disconnected. Bridged, host-only, NAT, and custom configurations remain unchanged.

To remove a virtual machine from a team

1 Power off the virtual machine that you want to remove.

2 Select the team and choose **Team > Remove > <virtual machine name>**.

The selected virtual machine is removed from the team.

You might want to perform these tasks after removing the virtual machine:

- Add the virtual machine to the **Favorites** list. See "To add virtual machines and teams to the Favorites list" on page 62.
- Delete the virtual machine and erase its files from the host file system. See "Delete a Virtual Machine" on page 150.

Specify the Startup Sequence for a Team

Use a startup sequence to specify the order in which virtual machines start and stop and the delay, in seconds, between starting and stopping the next virtual machine in the sequence.

Power on and resume operations occur in the order of the sequence shown in the team settings list. Power off operations occur in reverse order. The default sequence is the order in which you added the virtual machines to the team. The default delay is 10 seconds.

Setting a startup sequence is useful, for example, if you have a virtual machine that runs an application to be tested and you want it to start before the virtual machines running an automated testing script.

Setting a delay avoids overloading the CPU when multiple virtual machines start and allows applications on a virtual machine to launch before another team virtual machine attempts to connect.

To specify a startup sequence for a team

1. Select the team and choose **Team > Settings** and click the **Virtual Machines** tab.
2. Use the up and down arrow buttons to arrange the virtual machines in the list.

   The virtual machine at the top of the list is the first in the startup sequence.
3. Select each virtual machine and specify how many seconds you want it to wait before starting the next virtual machine.

   If the virtual machine team depends on precise startup timing, experiment to determine how much time the host and guest operating environments and applications need to launch.
4. Click **OK** to save your changes.

Power Operations for Teams and Their Members

Power operations for teams are much the same as those for an individual virtual machine. However, for a team, you can also change the sequence in which the members of a team power on and off. See "Specify the Startup Sequence for a Team" on page 258.

You can also use Workstation's command-line application for team power operations. See Appendix A, "Workstation Command-Line Reference," on page 467.

Power On a Team

When you power on a team, the virtual machines in the team power on in the startup sequence specified in the team settings editor. See "Specify the Startup Sequence for a Team" on page 258.

To power on a team

Do one of the following:

- To use the Workstation GUI, select the team and choose **Team > Power > Power On**.
- To use the command line, see "Startup Options for Workstation and Virtual Machines" on page 467.

Suspend or Resume a Team

When you suspend a team, all team virtual machines are suspended simultaneously. The startup sequence determines the order in which virtual machines are resumed and how much time elapses before resuming the next team member. See "Specify the Startup Sequence for a Team" on page 258.

If you attempt to close Workstation while a team suspend or resume operation is still in progress, a warning dialog box appears.

To suspend or resume a team

1 To suspend or resume a team, select the team and choose one of the **Team > Power** options.

All team virtual machines are suspended simultaneously.

2 To see the progress of a particular team member, choose **Team > Switch To > <virtual_machine_name>**.

The time to complete the operation varies with the size of the virtual machines.

Perform Power Operations on One Team Member

Performing a power operation for one member of a team is similar to performing the operation for a virtual machine that is not part of the team, except that instead of selecting the machine from the **Favorites** list, you select it from the team's console tab.

To perform power operations on one team member

1 Select the virtual machine from the team's console tab.

2 Choose the appropriate command from the **VM > Power** menu.

Working with Team Networks

One of the advantages of teams is the ability to isolate virtual machines in private virtual networks, called LAN segments. This can be useful with multitier testing, network performance analysis, and situations where isolation and packet loss are important.

For information about other aspects of networking than LAN segments, see Chapter 14, "Configuring a Virtual Network," on page 265.

LAN Segment Requirements Regarding IP Addresses

When you add an existing virtual machine to a team, the virtual machine might be configured to expect an IP address from a DHCP server. Unlike host-only and NAT networking, LAN segments have no DHCP server provided automatically by Workstation.

Each network client must have an IP address for TCP/IP networking. Therefore you must manually configure IP addressing for team virtual machines on a LAN segment. Two choices are available:

- **DHCP** – Configure a DHCP server on your LAN segment to allocate IP addresses to your virtual machines.
- **Static IP** – Configure a fixed IP address for each virtual machine on the LAN segment.

Create a Team LAN Segment

The first step to creating a virtual network for a team is to add and name a LAN segment. You can then configure connections to this segment.

To create a team LAN segment

1. Select the team and choose **Team > Add > LAN Segment**.
2. Enter a name for the private network and click **OK**.

   You can configure the other settings in this dialog box later.

You might want to perform these tasks after creating a LAN segment:

- Configure network transmission properties for the segment. See “Configure LAN Segments” on page 262.
- Create a network adapter and connect it to the segment. See “Add or Remove Network Adapters” on page 263.

Configure LAN Segments

You can configure network transmission properties for a team LAN segment, including bandwidth settings such as connection type and speed, as well as percentage of packet loss allowed.

To configure LAN segments

1 Select the team and choose **Team > Settings**.

2 Click the **LAN Segments** tab, and complete the fields.

From this tab you can add, remove, and rename the LAN segments configured for the team.

The list in the left pane displays LAN segments associated with the team.

3 Click a name to select the LAN segment you want to configure.

The right pane displays parameters for the physical properties of the emulated LAN segment link:

- **Name** – Name of the LAN segment. To change the name, type a new name in the **Name** field.
- **Bandwidth** – Drop-down menu of bandwidths for typical network links. To change the bandwidth, choose another connection type from the drop-down menu.
- **Kbps** – Field to set a custom bandwidth, in kilobits per second. Changes here are overwritten when you make a selection from the **Bandwidth** menu. To change the bandwidth, type a number into the field.
- **Packet Loss** – Specification of the efficiency or faultiness of the link, measured in the percentage of packets lost from the total number of packets transmitted. To change the packet loss setting, type a number into the field.

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

5 (Optional) If virtual machines are currently running and you want them to adopt these configuration changes, power on, reset, or resume the virtual machines, as appropriate.

Add or Remove Network Adapters

A physical PC must have a network adapter or NIC (network interface controller), for each physical network connection. Similarly, a virtual machine must be configured with a virtual network adapter for each LAN segment it interacts with.

To connect a virtual machine to multiple LAN segments simultaneously, you must configure that virtual machine with multiple network adapters.

To add or remove network adapters

1. Power off the virtual machine that you want to add a network adapter to or remove an adapter from.
2. Select the team and choose **Team > Settings**.
3. On the **Connections** tab, select the virtual machine and do one of the following:
   - To add a network adapter, click **Add Adapter**.

     The added adapter is displayed in the **Adapters** column. By default, the adapter connects to the bridged LAN segment, but you can change the setting by clicking a check box for another segment. If the segment you want to use is not listed, create it. See "Create a Team LAN Segment" on page 261.

     NICs configured with connections through a DHCP server cannot connect to a team LAN segment.
   - To remove an adapter, select the adapter you want to remove and click **Remove Adapter**.
4. Click **OK**.

Delete a LAN Segment

Deleting a LAN segment disconnects all virtual network adapters that are configured for that LAN segment. When you remove a virtual machine from a team, you must manually configure its disconnected virtual network adapter if you want to reconnect the virtual machine to a network.

To delete a LAN segment

1. Select the team and choose **Team > Settings**.
2. Click the **LAN Segments** tab and select the LAN segment you want to delete.
3. Click **Remove** and click **OK**.

Cloning and Taking Snapshots of Team Virtual Machines

You can clone a virtual machine in a team in the same way you clone any other virtual machine. See “Creating Clones” on page 205.

When you clone a virtual machine in a team:

- The resulting clone is not part of the team.
- The clone appears on the **Favorites** list as well as in a summary window.
- If the parent virtual machine is configured for a LAN segment, the virtual network adapter for that LAN segment on the clone is disconnected. To connect to a network, you must reconfigure the virtual Ethernet adapter manually.

Snapshots operate only on virtual machines and not on the whole team. When a team is active, you can use the **Snapshot** button on the toolbar to take a snapshot of only the active virtual machine.

To preserve the state of all virtual machines on a team, power off the team, and take a snapshot of each virtual machine before you power on the team again.

Configuring a Virtual Network 14

This chapter previews the virtual networking components that VMware Workstation provides and shows how to use them with your virtual machine. This chapter includes the following topics:

Components of the Virtual Network

Workstation provides the bridged, network address translation (NAT), and host-only networking options to configure a virtual machine for virtual networking.

Virtual Switch

Like a physical switch, a virtual switch lets you connect other networking components together. Virtual switches are created as needed by Workstation, up to a total of 10 virtual switches on Windows and 255 on Linux. You can connect one or more virtual machines to a switch. By default, a few of the virtual switches are mapped to specific networks.

Table 14-1. Virtual Network Switches

Network Type	Switch Name	Reference
Bridged	VMnet0	"Bridged Networking" on page 267
NAT	VMnet8	"Network Address Translation (NAT)" on page 269
Host-only	VMnet1	"Host-Only Networking" on page 270

The other available networks are named VMnet2, VMnet3, VMnet4, and so on.

DHCP Server

The dynamic host configuration protocol (DHCP) server provides IP network addresses to virtual machines in configurations that are not bridged to an external network. For example, host-only and NAT configurations use the DHCP server.

Network Adapter

A virtual network adapter is set up for your virtual machine when you use any type of networking to create it with the New Virtual Machine wizard. It appears in the guest operating system as an AMD PCNET PCI adapter or as an Intel Pro/1000 MT Server Adapter. On Windows Vista guests, it is an Intel Pro/1000 MT Server Adapter.

Use the virtual machine settings editor to create and configure up to 10 virtual network adapters in each Workstation 6.0 and higher virtual machine. The limit is three adapters for Workstation 4 or 5 virtual machines. For more information, see "Changing a Networking Configuration" on page 275.

Common Networking Configurations

When you choose the standard networking options in the New Virtual Machine wizard or the virtual machine settings editor, the networking configurations are set up for you automatically.

If you select the Typical setup path in the New Virtual Machine wizard, the wizard sets up network address translation (NAT) for the virtual machine. Select the Custom setup path to choose any of the other common configurations: bridged networking, NAT, or host-only networking. The wizard connects the virtual machine to the appropriate virtual network.

You can set up more specialized configurations by choosing the appropriate settings in the virtual machine settings editor, in the virtual network editor (on Windows and Linux hosts), and on your host computer. On both hosts, the software needed for all networking configurations is installed when you install Workstation.

You can connect multiple virtual machines 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.

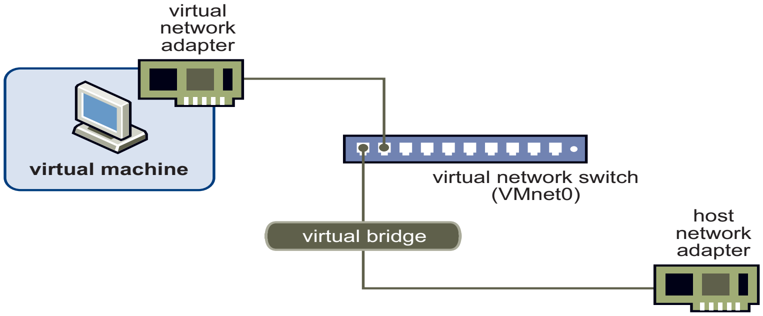
If you have set your virtual network settings on a previous version of Workstation and upgrade, your previous network settings might be fully or partially preserved. For more information, see "Preparing for an Upgrade" on page 46.

Bridged Networking

Bridged networking connects a virtual machine to a network by using the host computer's network adapter. If your host computer is on a network, this is often the easiest way to give your virtual machine access to that network. The virtual network adapter in the virtual machine connects to the physical network adapter in your host computer, allowing it to connect to the LAN the host computer uses.

Bridged networking configures your virtual machine as a unique identity on the network, separate from and unrelated to its host. It makes the virtual machine visible to other computers on the network, and they can communicate directly with the virtual machine. Bridged networking works with both wired and wireless physical host network cards.

Figure 14-1. Bridged Networking Setup



Set Up Bridged Networking

Windows and Linux hosts can use bridged networking to connect to wired and wireless networks.

To set up bridged networking

Do one of the following:

- For a new virtual machine, choose **File > New > Virtual Machine > Custom (advanced)** and select **Use bridged networking** in the New Virtual Machine wizard.
- For an existing virtual machine, choose **VM > Settings.**

  a. On the **Hardware** tab select **Network Adapter**.

  b. In the **Network connection** section select **Bridged: Connected directly to the physical network**.

  c. (Optional) Select **Replicate physical network connection state** if you use the virtual machine on a laptop or other mobile device.

     As you move from one wired or wireless network to another, the IP address is automatically renewed.

Setup Requirements for IP Addresses

If you use bridged networking, your virtual machine must 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 which networking settings you should use in the guest operating system. Generally, your guest operating system can acquire an IP address and other network details automatically from a DHCP server, or you might 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 other machines on the network can contact it as if it were a physical computer on the network.

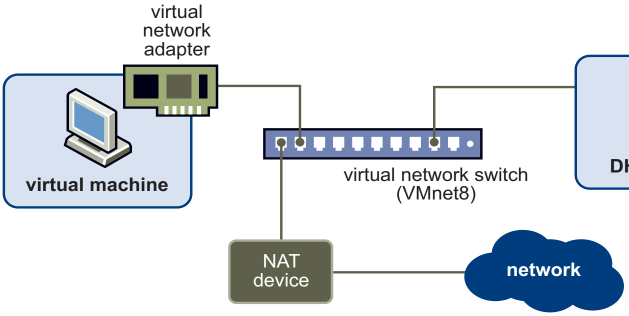
Users who boot multiple operating systems often assign the same address to all systems, because they assume that only one operating system will be running at a time.

NOTE If the host computer is set up to boot multiple operating systems and you run one or more of them in virtual machines, configure each operating system with a unique network address.

Network Address Translation (NAT)

NAT configures a virtual machine to share the IP and MAC addresses of the host. The virtual machine and the host share a single network identity that is not visible outside the network. NAT can be useful when your network administrator lets you use a single IP address or MAC address. If cannot give your virtual machine an IP address on the external network, you can use NAT to give your virtual machine access to the Internet or another TCP/IP network. NAT uses the host computer's network connection. NAT works with Ethernet, DSL, and phone modems.

Figure 14-2. NAT Setup



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. NAT also lets you to connect to a TCP/IP network by using a Token Ring adapter on the host computer.

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. This configuration protects the guest operating system from being compromised before you have a chance to install security software. For more information on NAT, see "Using NAT" on page 299.

Setting Up NAT

By default, NAT is used when you use the Typical setup to create a virtual machine in the New Virtual Machine wizard.

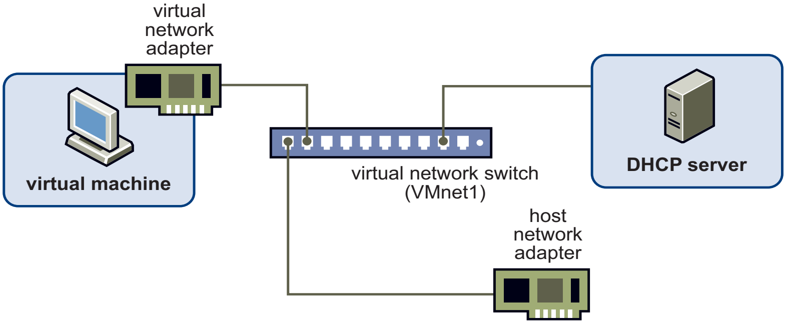
Setup Requirements for IP Addresses

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.

Host-Only Networking

Host-only networking creates a network that is completely contained within the host computer. Host-only networking provides a network connection between the virtual machine and the host computer, using a virtual network adapter that is visible to the host operating system. This approach can be useful if you need to set up an isolated virtual network. In this configuration, the virtual machine cannot connect to the Internet. For more information on host-only networking, see "Selecting IP Addresses on a Host-Only Network or NAT Configuration" on page 286.

Figure 14-3. Host-Only Networking Setup



Set Up Host-Only Networking

You can set up host-only networking while creating a virtual machine or after a virtual machine is created.

To set up host-only networking

Do one of the following:

- For a new virtual machine, choose **File > New > Virtual Machine > Custom (advanced)** and select **Use host-only networking** in the New Virtual Machine wizard.
- For an existing virtual machine, choose **VM > Settings.**
  a On the **Hardware** tab select **Network Adapter**.
  b In the **Network connection** section click **Host-only: A private network shared with the host**.

Setup Requirements for IP Addresses

If you use host-only networking, your virtual machine and the host virtual adapter are connected to a private Ethernet network. The VMware DHCP server provides addresses on this network.

Routing and Connection Sharing

If you install the proper routing or proxy software on your host computer, you can establish a connection between the host virtual network adapter and a physical network adapter on the host computer. This lets you, for example, to connect the virtual machine to a Token Ring or other non-Ethernet network.

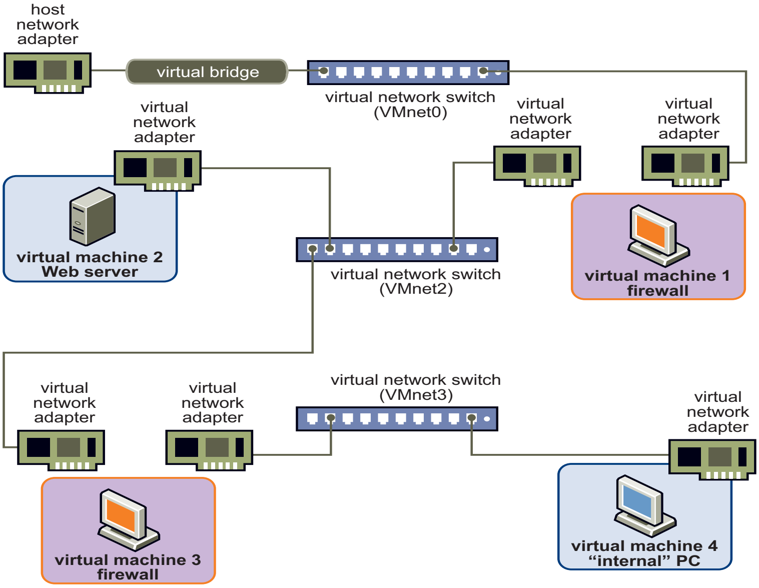
On a Windows 2000, Windows XP, or Windows Server 2003 host computer, you can use host-only networking in combination with the Internet connection sharing feature in Windows to allow a virtual machine to use the host's dial-up networking adapter or other connection to the Internet. For details on how to configure Internet connection sharing, see your Windows documentation.

Example of a Custom Networking Configuration

With the Workstation virtual networking components, you can create sophisticated virtual networks. The virtual networks can be connected to one or more external networks, or they can run entirely on the host computer. On Windows hosts, you can use the virtual network editor to access multiple network cards in your host and create multiple virtual networks.

Before you attempt to set up complex virtual networks, have a good understanding of how to configure network devices in your host and guest operating systems. Figure 14-4 shows most of the ways you can combine devices on a virtual network. Other custom configurations are described in "Advanced Virtual Networking" on page 285 and "Using NAT" on page 299. In this example, a Web server connects through a firewall to an external network. An administrator's computer connects to the Web server through a second firewall.

Figure 14-4. Custom Configuration with Two Firewalls


host network adapter
virtual bridge
virtual network switch (VMnet0)
virtual network adapter
virtual network adapter
virtual network adapter
virtual machine 2 Web server
virtual network switch (VMnet2)
virtual machine 1 firewall
virtual network adapter
virtual network adapter
virtual network switch (VMnet3)
virtual network adapter
virtual machine 3 firewall
virtual machine 4 "internal" PC

Set Up a Custom Networking Configuration

To set up the custom networking configuration, create four virtual machines and use the virtual machine settings editor to adjust the settings for their virtual network adapters. Install the appropriate guest operating systems and application software in each virtual machine and make the appropriate networking settings in each virtual machine.

To set up a custom networking configuration

1 Set up four virtual machines using the New Virtual Machine wizard:

   a Choose **File > New > Virtual Machine**.

   b Create the first virtual machine with bridged networking so that it can connect to an external network by using the host computer's network adapter.

   c Create the other three virtual machines without networking.

   Setting up virtual network adapters and installation of the operating systems are performed in Step 7.

2 Configure network settings for the first virtual machine:

   a Open the first virtual machine, but do not power it on.

   b Use the virtual machine settings editor to add a second virtual network adapter.

   See "Changing a Networking Configuration" on page 275.

   c Connect the second adapter to Custom (VMnet2).

3 Configure network settings for the second virtual machine.

   a Open a virtual machine, but do not power it on.

   b Use the virtual machine settings editor to add a virtual network adapter.

   c Connect the adapter to Custom (VMnet2).

4 Configure network settings for the third virtual machine:

   a Open virtual machine 3, but do not power it on.

   b Use the virtual machine settings editor to add a virtual network adapter.

   c Connect the adapter to Custom (VMnet2).

   d Use the virtual machine settings editor to add a second virtual network adapter.

   e Connect the second adapter to Custom (VMnet3).

5 Configure network settings for the fourth virtual machine:

   a Open virtual machine 4, but do not power it on.

   b Use the virtual machine settings editor to add a virtual network adapter.

   c Connect the adapter to Custom (VMnet3).

6 Determine the network addresses used for VMnet2 and VMnet3:

   - On Windows hosts, open a command prompt and run the following command:

     ```
     ipconfig /all
     ```

     Note the network addresses that each virtual adapter uses.

   - On Linux hosts, open a terminal and run the following command:

     ```
     ifconfig
     ```

     Note the network addresses that each virtual switch uses.

7 Power on each virtual machine in turn and install the appropriate guest operating system.

8 On a Windows and Linux hosts, to configure network addresses using the DHCP server, do the following:

   a Choose **Edit > Virtual Network Settings > DHCP**.

     On Linux, choose **Applications > System Tools > Virtual Network Configuration**, or the equivalent menu path for your version of Linux.

   b Add VMnet2 and VMnet3 to the list of virtual networks that the virtual DHCP server serves.

     For more information on changing subnets, see "Change Subnet or DHCP Settings on a Windows Host" on page 280 and "Change Subnet or DHCP Settings on a Linux Host" on page 281.

9 Configure the networking in each guest operating system:

- **Machine 1** – For the bridged network adapter in virtual machine 1, use the networking settings needed for a connection to the external network. If the virtual machine receives its IP address from a DHCP server on the external network, the default settings should work.

  For the second network adapter in virtual machine 1, manually assign an IP address in the range you are using with VMnet2.

- **Machine 2** – Assign an IP address in the range you are using with VMnet2.

- **Machine 3** – Network adapters are connected to VMnet2 and VMnet3. Assign to each adapter an IP address in the range you are using with the virtual network to which it is connected.

- **Machine 4** – Assign an IP address in the range you are using with VMnet3.

10 Install the necessary application software in each virtual machine.

Changing a Networking Configuration

You can determine the type of network a virtual machine is using, use the virtual machine settings editor to add virtual network adapters to your virtual machine, and change the configuration of existing adapters.

Find the Network Type of a Virtual Machine

Unless you set up a custom network connection, a virtual machine uses a bridged, NAT, or host-only network connection. If you use the Typical setup path in the New Virtual Machine wizard to create a virtual machine, the new virtual machine uses the NAT network type.

For more information, see "Common Networking Configurations" on page 266.

To find the network type of a virtual machine

1 Select the virtual machine.

2 Choose **VM > Settings > Hardware.**

3 Select the network adapter.

  The **Network Connection** section displays the details that lets you to change the settings.

To change the network type, see "Modify Existing Virtual Network Adapters" on page 276.

Add Virtual Network Adapters

You can add up to 10 virtual network adapters to a virtual machine.

To add virtual network adapters

1 Select the virtual machine to which you want to add the adapter.

2 Choose **VM > Settings**.

3 On the **Hardware** tab, click **Add**.

4 Select **Network Adapter** and click **Next**.

5 Select the network type to use.

6 (Optional) If you select **Custom**, choose the VMnet network to use from the drop-down menu.

Although VMnet0, VMnet1, and VMnet8 are technically available in this list, they are usually used for bridged, host-only, and NAT configurations, respectively. You must perform another procedure to make them available for use in custom configurations. Choose one of the other VMnet switches.

7 Click **Finish**.

The new adapter is added.

8 Click **OK** to save your configuration.

Modify Existing Virtual Network Adapters

Before you begin modifying the virtual network adapters, determine the network type you want to assign. See "Common Networking Configurations" on page 266.

To modify existing virtual network adapters

1 Select the virtual machine.

2 Choose **VM > Settings**.

3 On the **Hardware** tab, select the adapter to modify.

4 Select the network type to use.

5 (Optional) If you select **Custom**, choose the VMnet virtual network to use for the network from the drop-down menu.

Although VMnet0, VMnet1, and VMnet8 are technically available in this menu, they are usually used for bridged, host-only, and NAT configurations, respectively. You must perform another procedure to make them available for use in custom configurations. Choose one of the other VMnet switches.

6 Click **OK**.

7 Be sure the guest operating system is configured to use an appropriate IP address on the new network.

If the guest is using DHCP, release and renew the lease. If the IP address is set statically, be sure the guest has an address on the correct virtual network.

Configuring Bridged Networking

Windows and Linux hosts allow you to configure bridged networking. You can view and change the settings for bridged networking on your host, determine which network adapters on your host to use for bridged networking, and map specific network adapters to specific virtual networks, called VMnets.

Configure VMnet0 Automatic Bridged Networking on a Windows Host

When you configure VMnet0 bridged networking the change you make affects all the virtual machines that use bridged networking on the host.

To configure VMnet0 bridged networking on a Windows host

1 Choose **Edit > Virtual Network Settings**.

The virtual network editor appears, with the **Summary** tab active.

By default, VMnet0 is set to use automatic bridging mode and bridges to one of the active network adapters on the host computer.

2 Click the **Automatic Bridging** tab, and select the check box for **Automatically choose an available physical adapter to bridge to VMnet0**.

To place restrictions on a network adapter, see "Add or Remove a Host Network Adapter from the List of Excluded Adapters."

3 Click **OK**.

Add or Remove a Host Network Adapter from the List of Excluded Adapters

On host systems with multiple physical network adapters, the choice of which adapter Workstation uses is arbitrary. Therefore, you can place or remove restrictions on a network adapter of your choice.

To add or remove a host network adapter from the list of excluded adapters

1. Choose **Edit > Virtual Network Settings**.
2. Click the **Automatic Bridging** tab.
3. In the **Excluded adapters** section, do one of the following:
   - To remove an adapter, select the adapter and click **Remove**.
   - To add an adapter, do the following:
     - i Click **Add**.
     - ii In the Add Excluded Adapters dialog box, select the listing for the adapter to add and click **OK**.
4. Click **OK**.

Designate a Physical Network Adapter to Bridge to Custom Virtual Switches

Before you change the bridged adapter mappings, check which virtual network the physical network adapter is going to be assigned to.

CAUTION If you reassign a physical network adapter to a different virtual network, any virtual machine that is using the original network loses its network connectivity through that network. You must then change the setting for each affected virtual machine's network adapter individually.

This can be especially troublesome if your host has only one physical network adapter and you reassign it to a VMnet other than VMnet0. In this case, even though the VMnet still appears to be bridged to an automatically chosen adapter, the only adapter it can use was assigned to another VMnet.

To designate a physical network adapter to bridge to custom virtual switches

1. Choose **Edit > Virtual Network Settings**.
2. Click the **Host Virtual Network Mapping** tab.

3. Choose an adapter from the drop-down menu beside the name of the virtual switch to use.

   You can create a custom bridged network on virtual switches VMnet2 to VMnet7. On Windows, you can also use VMnet9. On Linux, you can also use vmnet10 through vmnet255.

4. Click **OK**.

Configure vmnet0 Automatic Bridged Networking on a Linux Host

By default, vmnet0 is set to use automatic bridging mode and bridges to one of the active network adapters on the host computer.

To configure vmnet0 automatic bridged networking on a Linux host

1. On the Linux host, do one of the following:

   - From the desktop,

   - Open a terminal window and enter the following command:

     ```
     /usr/bin/vmware-netcfg
     ```

2. When prompted, enter the administrator password.

3. If the table in the network editor does not display a row for vmnet0, click **Add Network** and complete the Add Virtual Network dialog box.

4. Select the vmnet0 row in the table and select **Bridged**.

5. Do one of the following:

   - To use automatic bridging, click **Automatic Settings** and complete the dialog box.

     If you select multiple check boxes, the virtual machine bridges to the first available host network adapter. If an item in the list is disabled, the adapter is not available because it is already being used to bridge to another vmnet.

   - To specify one host network adapter, use the **Bridge to** list box.

6. Click **Save**.

Setting Up a Second Automatic Bridged Network Interface

If you have two network adapters installed on your host computer, connected to two different networks, you might want your virtual machines on that host computer to bridge to both network adapters so that the virtual machines can access either or both physical networks.

When you install Workstation on a host computer with multiple network adapters, you can configure multiple bridged networks. On Windows host, to set up multiple bridged networks see "Configure VMnet0 Automatic Bridged Networking on a Windows Host" on page 277. On Linux host, to set up multiple bridged networks see "Configure vmnet0 Automatic Bridged Networking on a Linux Host" on page 279.

Changing the Subnet or DHCP Settings for a Virtual Network

On Windows and Linux hosts, you can use the virtual network editor to make changes to subnet and DHCP settings.

IP networks are divided using subnet masks. When you modify the subnet mask, Workstation automatically updates the IP address settings for other components such as DHCP, NAT, and host virtual adapter if the default settings were never changed. The specific settings that are automatically updated include DHCP lease range, DHCP server address, NAT gateway address, and host virtual adapter IP address.

However, if you changed any of these settings from its default value, Workstation does not update that setting automatically. Workstation presumes that custom settings are not to be modified. This is the case even if you later changed the setting back to the default.

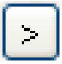
Change Subnet or DHCP Settings on a Windows Host

To change the subnet settings, configure the subnet mask. The default subnet mask is 255.255.255.0 (a Class C address). Typically, this means you should modify only the third number in the IP address—for example, x in 192.168.x.0 or 198.16.x.0. In general, do not change the subnet mask. Certain virtual network services might not work as well with a customized subnet mask.

To change subnet or DHCP settings on a Windows host

1. Choose **Edit > Virtual Network Settings**.
2. Click the **Host Virtual Network Mapping** tab.

3 Click the button on the right that corresponds to the virtual network to configure.



4 Choose **Subnet** or **DHCP**:

- In the Subnet dialog box, you can change the subnet's IP address and the subnet mask.

  The address should specify a valid network address that is suitable for use with the subnet mask.

- In the DHCP settings dialog box, you can change the range of IP addresses provided by the Workstation DHCP server on a particular virtual network.

  You can also set the duration of DHCP leases provided to clients on the virtual network.

5 Click **OK**.

Change Subnet or DHCP Settings on a Linux Host

NAT and host-only network types can have settings for subnet IP. You can use the virtual network editor to change subnet settings for a virtual network on a Linux host.

You can also use the virtual network editor to specify that a local DHCP service distributes IP addresses to virtual machines. To change DHCP settings further, edit the `dhcp.conf` file. See "Configure the DHCP Server on a Linux Host" on page 288.

To change subnet or DHCP settings on a Linux host

1 On the Linux host, do one of the following:

- From the desktop, choose **Applications > System Tools > Virtual Network Configuration**, or the equivalent menu path for your version of Linux.

- Open a terminal window and enter the following command:

  ```
  /usr/bin/vmware-netcfg
  ```

2 When prompted, enter the administrator password.

3 If the table in the network editor does not display a row for the network type you want, click **Add Network** and complete the Add Virtual Network dialog box.

  Use vmnet1 for a host-only network type, and use vmnet8 for a NAT network type.

4 Select the row in the table that corresponds to the network to edit and select **NAT** or **Host-only**, as appropriate.

5 Use the appropriate check boxes to specify whether to use a DHCP service, a host virtual adapter, or both.

6 To specify subnet IP, do one of the following:

- To automatically select an unused subnet IP, leave the **Subnet IP** text box empty.

  The next time you start the virtual network editor, the subnet IP appears in the text box.

- Type the subnet IP you want to use in the **Subnet IP** text box.

7 Click **Save.**

Configuring Host Virtual Network Adapters

When you install Workstation, two network adapters are added to the configuration of your host operating system. One lets the host to connect to the host-only network, and the other lets the host to connect to the NAT network.

The presence of virtual network adapters has a slight performance cost, because broadcast packets must go to the extra adapters. On Windows networks, browsing your network might be slower than usual. In some cases, these adapters interact with the host computer's networking configuration in undesirable ways.

Enable or Disable a Host Virtual Adapter

Before you disable a host virtual adapter determine whether you are going to use the virtual network adapter.

To enable or disable a host virtual adapter

1 Choose **Edit > Virtual Network Settings**.

2 Click the **Host Virtual Adapters** tab.

3 Select the adapter to enable or disable.

4 Click **Disable** or **Enable**.

5 Click **OK**.

Add or Remove a Host Virtual Adapter

You can add a virtual network and specify which virtual or physical adapter to associate with it.

To add or remove a host virtual adapter

1. Choose **Edit > Virtual Network Settings**.
2. Click the **Host Virtual Adapters** tab.
3. To add an adapter, do the following:
   a. Click **Add**.
   b. In the Add Network Adapter dialog box, choose the virtual network on which you want to use the adapter and click **OK**.
4. To remove an adapter, select the adapter to remove and click **Remove**.
5. Click **OK**.

Setting Up Two Separate Host-Only Networks

Set up multiple host-only networks on the same host computer in situations such as the following:

- To have two virtual machines connected to one host-only network, and other virtual machines connected to another host-only network to isolate the network traffic on each network.
- To test routing between two virtual networks.
- To test a virtual machine with multiple network interface cards, without using any physical network adapters.

On Windows and Linux hosts, the first host-only network is set up automatically when you install Workstation. To set up multiple host-only networks on Windows and Linux hosts see "Add or Remove a Host Virtual Adapter" on page 283.

On a Linux host, after the host-only networks are set up, at least four network interfaces appear: eth0, lo, vmnet1, and vmnet2. These four interfaces should have different IP addresses on separate subnets.

Advanced Virtual Networking

15

This chapter provides detailed information about networking capabilities and specialized configurations for expert users. This chapter includes the following advanced virtual networking topics:

Selecting IP Addresses on a Host-Only Network or NAT Configuration

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 network use the TCP/IP protocol suite, although other communication protocols can 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. A host virtual adapter connects the host computer 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 by using the DHCP server included with Workstation. 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 the DHCP server does not assign.

How the Subnet Number Is Assigned

When host-only networking is enabled at the time Workstation is installed, the subnet IP address for the virtual network is automatically selected as an unused private subnet IP address. A NAT configuration also uses an unused private network automatically selected when you install Workstation.

Find the Network Type Used on a Virtual Machine

Before you assign a subnet number, determine the network type used on the virtual machine.

To find the network type used on a virtual machine

Choose **Edit > Virtual Network Editor**.

On a Windows host, the **Summary** tab displays the subnet number associated with the virtual network.

Determining Whether to Use DHCP or Statically Assign Addresses

Using DHCP to assign IP addresses is simpler and more automatic than statically assigning them. Most Windows operating systems, for example, are 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 might 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.

DHCP Conventions for Assigning IP Addresses

For temporary virtual machines, use DHCP and let it allocate an IP address.

For each host-only or NAT network, the available IP addresses are allocated using the conventions shown in Table 15-1 and Table 15-2, where `<net>` is the network number assigned to your host-only or NAT network. Workstation always uses a Class C address for host-only and NAT networks.

Table 15-1. IP Address Use on a Host-Only Network

Range	Address Use	Example
`<net>`.1	Host machine	192.168.0.1
`<net>`.2–`<net>`.127	Static addresses	192.168.0.2–192.168.0.127
`<net>`.128–`<net>`.253	DHCP-assigned	192.168.0.128–192.168.0.253
`<net>`.254	DHCP server	192.168.0.254
`<net>`.255	Broadcasting	192.168.0.255

Table 15-2. IP Address Use on a NAT Network

Range	Address Use	Example
`<net>`.1	Host machine	192.168.0.1
`<net>`.2	NAT device	192.168.0.2
`<net>`.3–`<net>`.127	Static addresses	192.168.0.3–192.168.0.127
`<net>`.128–`<net>`.253	DHCP-assigned	192.168.0.128–192.168.0.253
`<net>`.254	DHCP server	192.168.0.254
`<net>`.255	Broadcasting	192.168.0.255

Configure the DHCP Server on a Windows Host

On a Windows host, use the virtual network editor to configure the DHCP server.

To configure the DHCP server on a Windows host

1. Choose **Edit > Virtual Network Editor**.
2. Click the **DHCP** tab.
3. Select the virtual network for which you want to change settings and click **Properties**.
4. In the DHCP Settings dialog box that appears, make changes and click **OK**.

Configure the DHCP Server on a Linux Host

Editing the DHCP server configuration file requires information that is best obtained directly from the DHCP server documentation. Consult the `dhcpd(8)` and `dhcpd.conf(8)`manual pages.

NOTE The edits made inside the read-only section of the DHCP configuration file are lost the next time you run the network editor.

To configure the DHCP server on a Linux host

- To configure the host-only DHCP server, edit 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`).

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, packets that virtual machines send on this network should not leak out to a physical network attached to the host. Packet leakage can occur only if a machine actively forwards packets.

If you use dial-up networking support in a virtual machine and packet forwarding is enabled, host-only network traffic might leak out through the dial-up connection.
To prevent the leakage, disable packet forwarding in your guest operating system.

If the host computer has multiple network adapters, it might be intentionally configured to use IP forwarding. If that is the case, you do not want to disable forwarding. 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.

Disable Packet Forwarding on Windows Hosts

Systems using server versions of Windows operating systems can forward IP packets that are not addressed to them. By default, these systems and Windows Vista systems have IP packet forwarding disabled. IP forwarding is not a problem on Windows 2000 Professional, Windows XP Professional, or Windows XP Home Edition hosts.

NOTE If you are running Windows 2000 Professional, install Windows 2000 administrative tools to access the server tools and disable packet forwarding.

If you find packets leaking from a host-only network on a Windows host computer, check whether forwarding was enabled on the host machine. If it is enabled, disable it.

To disable packet forwarding on Windows hosts

Do one of the following:

- Stop the Routing and Remote Access service:

  a Choose **Start > Run** and enter **`services.msc`** in the Run dialog box.

  b In the Services window that appears, disable the Routing and Remote Access service.

- Use Windows Administrative Tools to disable routing and remote access:

  a On a Windows 2000 or Windows 2003 Server host, choose **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.

  b To turn off IP forwarding, right-click the icon and disable **Routing and Remote Access**.

  A red dot appears, indicating that IP forwarding is disabled.

Install Windows 2000 Administrative Tools to Access Server Tools

Windows 2000 Administrative 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 Administrative Tools to access server tools

1 Open the `i386` folder on the applicable Windows 2000 Server disc.

2 Double-click the `adminpak.msi` file, and follow the instructions that appear in the Windows 2000 Administrative Tools Setup Wizard.

3 After Windows 2000 Administrative Tools are installed, you can access most of the server administrative tools by choosing **Start > Programs > Administrative Tools**.

Disable Packet Forwarding on Linux Hosts

If you find packets leaking from a host-only network on a Linux host computer, check whether forwarding was mistakenly enabled on the host machine. If it is enabled, disable it.

To disable packet forwarding on Linux hosts

Depending on which type of Linux system you have, use one of the following methods:

- Disable forwarding by writing a 0 (zero) to the special file `/proc/sys/net/ipv4/ip_forward`. As root (`su–`), enter the following command:

  ```
  echo "0" > /proc/sys/net/ipv4/ip_forward
  ```

- Use a configuration option that is appropriate for your Linux distribution. For example, you might use a control panel, specify a setting at the time you compile your kernel, or enter a specification when you boot your system.

  For details about the method to use with your distribution, consult your operating system documentation.

Maintaining and Changing the MAC Address of a Virtual Machine

When a virtual machine is powered on, Workstation assigns each of its virtual network adapters an Ethernet media access control (MAC) address. A MAC address is the unique address assigned to each Ethernet network device.

The software guarantees that virtual machines are assigned unique MAC addresses within a given host system. The virtual machine is assigned the same MAC address every time it is powered on if both of the following conditions are true:

- The virtual machine is not moved. That is, the path name and filename for the virtual machine's configuration file remain the same.
- No changes are made to certain settings in the configuration file.

However, Workstation cannot guarantee to automatically assign unique MAC addresses for virtual machines that run on multiple host systems.

Avoiding MAC Address Changes

To avoid changes in the MAC address automatically assigned to a virtual machine, do not move the virtual machine's configuration file. Moving it to a different host computer or even moving it to a different location on the same host computer changes the MAC address.

Also do not change certain settings in the virtual machine's configuration (`.vmx`) file. If you never edit the configuration file by hand and do not remove the virtual network adapter, these settings remain unchanged. If you do edit the configuration file by hand, do not remove or change the following options:

```
ethernet[n].generatedAddress
ethernet[n].addressType
ethernet[n].generatedAddressOffset
uuid.location
uuid.bios
ethernet[n].present
```

In these options, [n] is the number of the virtual network adapter, for example `0`.

NOTE To preserve a virtual network adapter's MAC address, you must be careful not to remove the adapter. If you remove the adapter but later re-create it, the adapter might receive a different MAC address.

Assign the Same MAC Address to Any Virtual Machine Manually

Assign the MAC address manually instead of allowing Workstation to assign it to guarantee the following:

- The same MAC address is assigned to a given virtual machine every time you power it on, even if the virtual machine is moved.
- A unique MAC address is provided for each virtual machine within a networked environment.

To assign the same MAC address to any virtual machine manually

1 Use a text editor to remove from the configuration (`.vmx`) file the three lines that begin with the following:

```
ethernet[n].generatedAddress
ethernet[n].addressType
ethernet[n].generatedAddressOffset
```

In these options, [n] is the number of the virtual network adapter, for example, 0.

On a Linux host, a virtual machine created with an earlier VMware product might have a configuration file with a `.cfg` extension.

2 Add the following line to the configuration file above the UUID lines in the file:

```
ethernet[n].address = 00:50:56:XX:YY:ZZ
```

In this line, the fourth pair of numbers, XX, must be a valid hexadecimal number between 00h and 3Fh, and YY and ZZ must be valid hexadecimal numbers between 00h and FFh. You must use the above format because Workstation virtual machines do not support arbitrary MAC addresses.

A value for XX:YY:ZZ that is unique among your hard-coded addresses avoids conflicts between the automatically assigned MAC addresses and the manually assigned addresses.

Controlling Routing Information for a Host-Only Network on Linux

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 the host-only network and propagate information on how to reach the network unless you explicitly configure them not to do so.

If either of these processes is being run only to receive routing information, the easiest solution is to run the routing configuration with a –q option so that the host-only network does not supply but only receives routing information.

If, however, routing services are running because they are to supply routing information, configure them so that they do not advertise routes to the host-only network.

The version of routed included 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.

For gated, configuration is involved. You must 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, contact VMware technical support by submitting a support request on the VMware Web site.

Potential Issues with Host-Only Networking on Linux

The following are common issues you might encounter when you are configuring a host-only network on Linux.

DHCPD on the Linux Host Does Not Work After Installing Workstation

If you were running the DHCP server dhcpd utility on your machine before you installed 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 might notice this.

In such cases, some dhcpd implementations abort if their configuration files do not include a subnet specification for the interface. This can happen even if dhcpd is not supposed to respond to messages that arrive through the interface.

The best solution is to add a line to the dhcpd configuration file in the following format:

```
subnet <net>.0 netmask 255.255.255.0 {}
```

Here <net> is the network number assigned to your host-only network—for example, 192.168.0. This line in the configuration file informs dhcpd about the host-only network and tells it explicitly not to respond to any DHCP requests arriving from it.

An alternative solution is to explicitly state the set of network interfaces for dhcpd to monitor each time you start the program. For example, if your machine has one Ethernet interface, eth0, each time you start dhcpd, list the interface on the command line:

```
dhcpd eth0
```

This prevents dhcpd from searching for all available network interfaces.

If these solutions do not work for your DHCP server program, it might be an old DHCP server. You can try upgrading to a more current version of DHCP available from the Internet Systems Consortium (ISC) Web site.

DHCP and DDNS

Use DHCP to supply IP addresses as well as other information, such as the identity of a host running a name server and the nearest router or gateway. The DHCP server in Workstation does not provide a means to dynamically establish a relationship between the IP address it assigns and a client's name (that is, to update a DNS server using dynamic domain name service (DDNS).

To use names to communicate with other virtual machines, you must either edit the DHCP configuration file for vmnet1 (`/etc/vmware/vmnet1/dhcpd/dhcpd.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 `dhcpd(8)` and `dhcpd.conf(8)`manual pages.

NOTE The edits made inside the read-only section of the DHCP configuration file are lost the next time you run the network editor.

Configuring Host-Only Virtual Machines

If you have already created two host-only interfaces (VMnet1 and VMnet2), you can set up your virtual machines for one of the following configurations:

- **Configuration 1** – The virtual machine is configured with one virtual network adapter, and that virtual adapter is connected to the default host-only interface (VMnet1). To use this configuration, see "Set Up Using Configuration 1 or 2" on page 295.
- **Configuration 2** – The virtual machine is configured with one virtual network adapter, and that virtual adapter is connected to the newly created host-only interface (VMnet2). To use this configuration, see "Set Up Using Configuration 1 or 2" on page 295.
- **Configuration 3** – The virtual machine is configured with two virtual network 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). To use this configuration, see "Set Up Using Configuration 3" on page 296.

Set Up Using Configuration 1 or 2

Use the virtual machine settings editor to connect the virtual machine to the default host-only adapter or a custom host-only adapter.

To set up using configuration 1 or 2

1. Select the virtual machine.
2. Choose **VM** > **Settings**.
3. On the **Hardware** tab, select **Network Adapter**.

4 In the **Network Connection** section, do one of the following:

- To connect to the default host-only interface (VMnet1), select **Host-only**.
- To connect to the newly created host-only interface, select **Custom**, and choose **VMnet2** from the drop-down menu on the right.

5 (Optional) If no network adapter is shown in the list of devices, add one, as described in "Add Virtual Network Adapters" on page 276.

Set Up Using Configuration 3

Make sure that there are two network devices for this virtual machine. For more information on adding virtual network adapters, see "Add Virtual Network Adapters" on page 276.

To set up using configuration 3

1 Select the virtual machine.

2 Make sure the virtual machine is powered off.

3 Choose **VM > Settings**.

4 On the **Hardware** tab, select the first **Network Adapter**.

5 In the **Network Connection** section, select **Host-only**.

This adapter is connected to the default host-only interface (VMnet1).

6 Select the second network adapter in the list, and in the **Network Connection** section, select **Custom** and choose **VMnet2** from the drop-down menu.

Complete Configuring the Virtual Network Adapters

To complete the configuration you must assign an IP address on the appropriate VMnet subnet to each virtual network adapter as you would for physical adapters on a physical computer.

To complete configuring the virtual network adapters

1 Power on the virtual machine and install your guest operating system.

In configurations 1 and 2, you see one network adapter. In configuration 3, you see two network adapters within the guest.

2 Assign IP addresses to the virtual network adapters.

3 (Optional) To see the IP address that a host-only network is using:

- On Windows hosts, open a command prompt and run the following command:

  ```
  ipconfig /all
  ```

- On Linux hosts, open a terminal and run the following command:

  ```
  ifconfig
  ```

Set Up Routing Between Two Host-Only Networks

If you are setting up a complex test network that uses virtual machines, you might want to have two independent host-only networks with a router between them.

Use one of the following methods. In both cases, you need two host-only interfaces.:

- The router software runs on the host computer.
- The router software runs on its own virtual machine.

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.

To set up routing between two host-only networks

1 Set up the connection to the first (default) host-only interface, as described in "Set Up Using Configuration 1 or 2" on page 295.

2 Set up the connection to the second (VMnet2) host-only interface, as described in "Set Up Using Configuration 1 or 2" on page 295.

3 (Optional) To run the router software on a virtual machine, set up a third virtual machine with connections to the two host only interfaces, as described in "Set Up Using Configuration 3" on page 296.

   To run the router software on your host computer, skip this step.

4 Stop the VMnet DHCP server service:

- On a Windows host, choose **Edit > Virtual Network Editor > DHCP**, select the service and click **Stop**.
- On a Linux host, open a terminal and use the following command to stop the `vmnet-dhcpd` service:

  ```
  killall -TERM vmnet-dhcpd
  ```

5 Install guest operating systems in each of the virtual machines.

6 Install the router software, either on the host computer or in the third virtual machine, depending on the approach you are using.

7 Configure networking in the first two virtual machines to use addresses on the appropriate host-only network:

- On Windows hosts, open a command prompt and run the `ipconfig /all` command to determine which IP addresses each host-only network is using.
- On Linux hosts, open a terminal and run the `ifconfig` command to determine which IP addresses each host-only network is using.

8 Assign IP addresses by doing one of the following:

- 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 in a third virtual machine, set the default router addresses in the first two virtual machines based on the addresses that the third virtual machine uses.

  In the first virtual machine's networking configuration, the default router address should be the IP address for the third virtual machine's network 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 network adapter connected to VMnet2.

You can now ping the router machine from virtual machines 1 and 2. If the router software is set up correctly, you can communicate between the first and second virtual machines.

Using Virtual Network Adapters in Promiscuous Mode on a Linux Host

Workstation does not allow the virtual network adapter to go into promiscuous mode unless the user running Workstation has permission to make that setting. This restriction follows the standard Linux practice that only the root user can put a network interface into promiscuous mode.

When you install and configure Workstation, you must run the installation as the root user. Workstation creates the vmnet devices with root ownership and root group ownership, which means that only the root user has read and write permissions to the devices.

To set the virtual machine's network adapter to promiscuous mode, you must launch Workstation as the root user because you must have read and write access to the vmnet device. For example, if you are using bridged networking, you must have access to `/dev/vmnet0`.

To grant selected other users read and write access to the vmnet device, you can create a new group, add the appropriate users to the group, and grant that group read and write access to the appropriate device. You must make these changes on the host operating system as the root user (`su –`). For example, you can enter the following commands:

```
chgrp <newgroup> /dev/vmnet0
chmod g+rw /dev/vmnet0
```

Here `<newgroup>` is the group that should be able to set vmnet0 to promiscuous mode.

For all users to be able to set the virtual network adapter (`/dev/vmnet0` in the example) to promiscuous mode, run the following command on the host operating system as the root user:

```
chmod a+rw /dev/vmnet0
```

Using NAT

NAT provides a 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 the address 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 is coming from the host machine.

The host computer has a host virtual adapter on the NAT network (identical to the host virtual adapter on the host-only network). This adapter allows the host and the virtual machines to communicate with each other for such purposes as file sharing. The NAT device never forwards traffic from the host virtual adapter.

How the NAT Device Uses the VMnet8 Virtual Switch

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 the address 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 the address 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.

DHCP on the NAT Network

To make networking configuration easy, a DHCP server is installed when you install Workstation. Virtual machines running on the network with the NAT device can send out DHCP requests to dynamically obtain their IP addresses.

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. 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 and`<net>`.2 is reserved for the NAT device. For more information, see “DHCP Conventions for Assigning IP Addresses” on page 287.

In addition to the IP address, the DHCP server on the NAT network sends out configuration information that enables the virtual machine to operate. 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 routing 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. The NAT device is a DNS proxy and forwards DNS requests from the virtual machines to a DNS server that the host knows. Responses return to the NAT device, which then forwards them to the virtual machines.

If they get their configuration information from DHCP, the virtual machines on the NAT network automatically use the NAT device as the DNS server. However, the virtual machines can be statically configured to use another DNS server.

The virtual machines in the private NAT network are not, themselves, accessible through DNS. To have the virtual machines running on the NAT network 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, a virtual machine on the NAT network can automatically use any protocol using TCP, or UDP can be used automatically by a virtual machine on the NAT network as 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 is built into the NAT device to allow FTP and ICMP echo (ping) to work 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. The virtual machine can send and receive data using TCP/IP to any machine that is accessible from the host.

Before any communication can occur, the NAT device must set up a map 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 map is created automatically. The operation is transparent to the user of the virtual machine on the NAT network. No additional work needs to be done.

Network connections that are initiated from outside the NAT network to a virtual machine on the NAT network are not transparent. When a machine on the external network attempts to initiate a connection with a virtual machine on the NAT network, it cannot reach the virtual machine because the NAT device does not forward the request.

However, you can configure port forwarding manually on the NAT device so that network traffic destined for a certain port can still be forwarded automatically to a virtual machine on the NAT network. See "Advanced NAT Configuration" on page 302.

File sharing of the type used by Windows operating systems and Samba is possible among computers on the NAT network, including virtual machines and the host computer. If you are using WINS servers on your network, a virtual machine using NAT networking can access shared files and folders on the host that the WINS server knows if those shared files and folders are in the same workgroup or domain.

Advanced NAT Configuration

You can configure NAT to make custom configuration settings for Windows and Linux.

Configure NAT on a Windows Host

Use the virtual network settings to configure NAT on a Windows host. To edit the NAT configuration file, see "Custom NAT and DHCP Configuration on a Windows Host" on page 302.

To configure NAT on a Windows host

1. Choose **Edit > Virtual Network Editor**.
2. Use the controls on the **NAT** tab to configure NAT:
   - To stop and start the virtual NAT device, click the appropriate buttons.
   - To edit NAT settings for a virtual network, choose the VMnet network from the drop-down menu and click **Edit**.
3. Click the appropriate button to set up or change port forwarding or to specify DNS servers that the virtual NAT device should use.
4. Click **OK**.

Custom NAT and DHCP Configuration on a Windows Host

If you are an advanced user on a Windows host computer, you can edit the NAT and DHCP configuration files to make custom configuration settings. If your host operating system is installed on the C drive, the configuration files for NAT and DHCP are in the following locations:

Table 15-3. NAT and DHCP File Locations

File Type	Location
NAT	`C:\Documents and Settings\All Users\Application Data\VMware\vmnetnat.conf` For more information about this file, see "Contents of the NAT Configuration File" on page 304.
DHCP	`C:\Documents and Settings\All Users\Application Data\VMware\vmnetdhcp.conf`

Use the virtual network editor (**Edit > Virtual Network Editor**) to change many key NAT and DCHP settings.

If you make manual changes to the configuration files, those changes might be lost when you use the virtual network editor. Make backup copies of the files before you change any settings in the virtual network editor. You can then copy your manual changes back into the appropriate configuration files.

Specifying Connections from Ports Below 1024

When a client machine makes a TCP or UDP connection to a server, the connection comes from a particular port on the client (the source port) and connects to a particular port on the server (the destination port). For security reasons, some servers accept connections only from source ports below 1024. You might see this configuration on machines used as NFS file servers, for example.

If a virtual machine using NAT attempts to connect to a server that requires the client to use a source port below 1024, the NAT device must forward the request from a port below 1024. You can specify this behavior in the `vmnetnat.conf` file.

This behavior is controlled by entries in sections headed `[privilegedUDP]` and `[privilegedTCP]`. You might need to add settings to or modify settings in either or both of these sections, depending on the kind of connection you need to make.

You can set two parameters, each of which appears on a separate line.

Table 15-4. Parameters to Map Virtual Machine Source and Destination Ports

Parameter	Description
`autodetect = <n>`	The autodetect setting determines whether the VMware NAT device automatically attempts to map virtual machine source ports below 1024 to NAT source ports below 1024. A setting of `1` means true. A setting of `0` means false. On a Windows host, the default is `1` (true). On a Linux host, the default is `0` (false).
`port = <n>`	The port setting specifies a destination port (where `<n>` is the port on the server that accepts the connection from the client). Whenever a virtual machine connects to the specified port on any server, the NAT device attempts to make the connection from a source port below 1024. You can include one or more port settings in the `[privilegedUDP]` or `[privilegedTCP]` section or in both sections, as required for the connections you need to make. Enter each port setting on a separate line.

Configuring NAT on a Linux Host

Use the default NAT configuration file on the host to configure the NAT device. This file is located in `/etc/vmware/vmnet8/nat/nat.conf`.

For an example of a NAT configuration file, see "Sample Linux nat.conf File" on page 309.

Contents of the NAT Configuration File

The NAT configuration file is in the following locations:

- On a Windows host:

  `C:\Documents and Settings\All Users\Application Data\VMware\vmnetnat.conf`

  If you edit this file and then use the virtual network editor (**Edit > Virtual Network Editor**) your edits might be lost.

- On a Linux host:

  `/etc/vmware/vmnet8/nat/nat.conf`

The NAT configuration file is divided into sections. Each section configures a part of the NAT device. Text surrounded by square brackets — such as [dns] — 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`. The NAT configuration file contains the following sections.

The [host] Section

The [host] section includes parameters to configure the NAT connection.

- `ip` – The IP address that the NAT device should use. It can be followed by a slash and the number of bits in the subnet.

- `netmask` – The subnet mask to use for the NAT network. DHCP addresses are allocated from this range of addresses.

- `configport` – A port that can be used to access status information about the NAT device.

- `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 this flag to `0` to turn it off.

The [udp] Section

`timeout` – Number of seconds to keep the UDP mapping for the NAT network.

The [dns] Section

The [dns] section is for Windows hosts only. Linux does not use this section.

- `policy` – Policy to use for DNS forwarding. Accepted values include:
  - `order` – Send one DNS request at a time in the 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 stops trying to respond to a DNS request.
- `autodetect` – Flag to indicate whether the NAT device should detect the DNS servers available to the host.
- `nameserver1` – IP address of a DNS server to use.
- `nameserver2` – IP address of a DNS server to use.
- `nameserver3` – IP address of a DNS server to use.

  If autodetect is on and some name servers are specified, the DNS servers specified in `nameserver1`, `nameserver2,` and `nameserver3` are added before the list of detected DNS servers.

The [netbios] Section

The [netbios] section applies to Windows hosts only. Linux does not use this section.

- `nbnsTimeout = 2` – Timeout, in seconds, for NBNS queries.
- `nbnsRetries = 3` – Number of retries for each NBNS query.
- `nbdsTimeout = 3` – Timeout, in seconds, for NBDS queries.

The [incomingtcp] Section

Use the [incomingtcp] section to configure TCP port forwarding for NAT. In this section, you can assign a port number to an IP address and port number on a virtual machine.

The following line shows the format used in this section:

```
8887 = 192.168.27.128:21
```

This example creates a map from port 8887 on the host to the IP address 192.168.27.128 and port 21. When this map is set and an external machine connects to the host at port 8887, the network packets are forwarded to port 21 (the standard port for FTP) on the virtual machine with IP address 192.168.27.128.

The [incomingudp] Section

Use the [incomingudp] section to configure UDP port forwarding for NAT. In this section, you can assign a port number to an IP address and port number on a virtual machine.

The following line shows the format used in this section. It illustrates a way to forward X server traffic from the host port 6000 to the virtual machine’s port 6001:

```
6000 = 192.168.27.128:6001
```

This example creates a map from port 6000 on the host to the IP address 192.168.27.128 and port 6001. When this map is set and an external machine connects to the host at port 6000, the network packets are forwarded to port 6001 on the virtual machine with IP address 192.168.27.128.

Considerations for Using NAT

Consider the following items when you use NAT:

- NAT causes some performance loss.

  Because NAT requires that every packet sent to and received from a virtual machine must be in the NAT network, an unavoidable performance penalty occurs.

- NAT is not perfectly transparent.

  NAT does not usually allow connections to be initiated from outside the network, although you can manually configure the NAT device to set up server connections. 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 might not work at all.

- NAT provides some firewall protection.

  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 usually cannot initiate connections to the private NAT network.

Using NAT with NetLogon

When you use NAT networking in a virtual machine with a Windows guest operating system running on a Windows host, you can use NetLogon to log in to a Windows domain from the virtual machine. You can then access file shares that the WINS server knows.

To use NetLogon, you need to know how WINS servers and Windows domain controllers work. This section explains how to set up the virtual machine to use NetLogon. The setup process is similar to the way you set up a physical computer on one LAN that is using a domain controller on another LAN.

To log in to a Windows domain outside the virtual NAT network, the virtual machine needs access to a WINS server for that domain. You can connect the virtual machine to a WINS server in the following ways:

- Connect to the WINS server that the DHCP server used on the NAT network provides, if the WINS server is already set up on the host.
- Manually enter the IP address of the WINS server to connect from the virtual machine to a WINS server not set up on the host.

Use NAT to Connect to an Existing WINS Server Set Up on the Host

To use NAT to connect, a WINS server in the same workgroup or domain must be set up on the host. This procedure applies to the Windows 2000, XP, 2003 Server, NT, Me, and 9x guest versions.

Differences for Windows Vista, are noted in the specific steps.

To use NAT to connect to an existing WINS server set up on the host

1. In the virtual machine, right-click **My Network Places** and choose **Properties**.

   For Windows Vista, open the Network and Sharing Center and click the **View Status** link for the connection that uses the desired virtual network adapter.

2. In the Network Connections window, right-click the virtual network adapter and choose **Properties**.

   For Windows Vista, in the Connection Status window, click **Properties** and click **Continue** when prompted for permission.

3. In the Properties dialog box, select **Internet Protocol (TCP/IP)** and click **Properties**.
4. In the TCP/IP Properties dialog box, click **Advanced**.
5. On the **WINS** tab, under **NetBIOS** setting, select **Use NetBIOS setting from DHCP Server**.
6. Click **OK** twice and click **Close**.

Enter the IP Address of a WINS Server Manually

Use the IP address to connect to a WINS server in the same workgroup or domain that is not already set up on the host.

To enter the IP address of a WINS server manually

1 In the virtual machine, right-click **My Network Places** and choose **Properties**.

For Windows Vista, open the Network and Sharing Center, and click the **View Status** link for the connection that uses the virtual network adapter.

2 In the Network Connections window, right-click the virtual network adapter and choose **Properties**.

For Windows Vista, in the Connection Status window, click **Properties** and click **Continue** when prompted for permission.

3 In the Properties dialog box, select **Internet Protocol (TCP/IP)** and click **Properties**.

4 In the TCP/IP Properties dialog box, click **Advanced**.

5 On the **WINS** tab, click **Add**.

6 In the TCP/IP WINS Server dialog box, enter the IP address for the WINS server in the WINS server field and click **OK**.

The IP address of the WINS server appears in the WINS addresses list on the **WINS** tab.

7 Repeat Step 5 and Step 6 for each WINS server to which you want to connect from this virtual machine.

8 Click **OK** twice and click **Close**.

Now that the virtual machine has an IP address for a WINS server, you can use NetLogon in the virtual machine to log in to a domain and access shares in that domain. However, your access is limited to shares of virtual machines that are on the same NAT network or are bridged on the same domain.

For example, if the WINS server covers a domain with a domain controller, you can access that domain controller from the virtual machine and add the virtual machine to the domain. You need to know the Administrator user ID and password for the domain controller.

Sample Linux nat.conf File

```
# Linux NAT configuration file

[host]

# NAT gateway address
ip = 192.168.237.2/24
hostMAC = 00:50:56:C0:00:08

# enable configuration; disabled by default for security reasons
#configport = 33445

# vmnet device if not specified on command line
device = vmnet8

# Allow PORT/EPRT FTP commands (they need incoming TCP stream...)
activeFTP = 1

# Allows the source to have any OUI. Turn this one if you change the OUI
# in the MAC address of your virtual machines.
#allowAnyOUI = 1

[udp]
# Timeout in seconds, 0 = no timeout, default = 60; real value might
# be up to 100% longer
timeout = 30

[dns]
# This section applies only to Windows.
#
# Policy to use for DNS forwarding. Accepted values include order,
# rotate, burst.
#
# order: send one DNS request at a time in order of the name servers
# rotate: send one DNS request at a time, rotate through the DNS servers
# burst: send to three servers and wait for the first one to respond
policy = order;

# Timeout in seconds before retrying DNS request.
timeout = 2

# Retries before giving up on DNS request
retries = 3

# Automatically detect the DNS servers (not supported in Windows NT)
autodetect = 1
```

```
# List of DNS servers to use. Up to three may be specified
#nameserver1 = 208.23.14.2
#nameserver2 = 63.93.12.3
#nameserver3 = 208.23.14.4

[netbios]
# This section applies only to Windows.

# Timeout for NBNS queries.
nbnsTimeout = 2

# Number of retries for each NBNS query.
nbnsRetries = 3

# Timeout for NBDS queries.
nbdsTimeout = 3

[incomingtcp]
# Use these with care – anyone can enter into your virtual machine through
# these...

# FTP (both active and passive FTP is always enabled)
#   ftp localhost 8887
#8887 = 192.168.27.128:21

# WEB (make sure that if you are using named webhosting, names point to
#   your host, not to guest... And if you are forwarding port other
#   than 80 make sure that your server copes with mismatched port
#   number in Host: header)
#   lynx http://localhost:8888
#8888 = 192.168.27.128:80

# SSH
#   ssh –p 8889 root@localhost
#8889 = 192.168.27.128:22

[incomingudp]
# UDP port forwarding example
    #6000 = 192.168.27.128:6001
```

Using Samba with Workstation

If you have Samba on your Linux host, you can configure Samba so that it works with Workstation.

Modify your Samba configuration so that it includes the IP subnet that the vmnet1 Workstation virtual network adapter uses. To determine which subnet vmnet1 is using, run the following command:

```
/sbin/ifconfig vmnet1
```

Make 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 match those used for logging on to the guest operating system.

Add Users to the Samba Password File

You can add user names and passwords to the Samba password file at any time from a terminal window on your Linux host computer.

To add users to the Samba password file

1 Log in to the root account:

```
su
```

2 Run the Samba password command:

```
smbpasswd -a <username>
```

Here <username> is the user name to add.

3 Follow the instructions on the screen.

4 Log out of the root account:

```
exit
```

Using a Samba Server for Bridged and Host-Only Networks

To use your Samba server for host-only and bridged networking, you must modify one parameter in the smb.conf file. You can define the interface parameter so that your Samba server serves multiple interfaces. An example of this is the following:

```
interface = eth0 vmnet1
```

This example tells the Samba server to monitor and use both the eth0 and vmnet1 interfaces, which are the interfaces that bridged and host-only networking use, respectively.

Use Samba Without Network Access

To make Samba inaccessible from your physical network interface, you must configure the configuration file.

To use Samba without network access

1 Open the configuration file:

```
/etc/samba/smb.conf
```

2 Add the following line to the configuration file and save the changes.

```
interfaces = vmnet*
```

3 Restart Samba.

16

Connecting Devices

This chapter describes how to use various devices with a virtual machine.

This chapter includes the following topics:

Using Parallel Ports

Parallel ports are used by a variety of devices, including printers, scanners, dongles, and disk drives. Although these devices can connect to the host without problems, only printers can reliably connect to virtual machines by using parallel ports.

Currently, Workstation provides only partial emulation of PS/2 hardware. Interrupts that a device connected to the physical port requests 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. Do not use parallel port storage devices in a virtual machine.

Add a Virtual Parallel Port to a Virtual Machine

If the virtual machine is configured with a parallel port, most guest operating systems detect the port at installation time and install the required drivers. Some operating systems, including Linux, Windows NT, and Windows 2000, automatically detect the ports at boot time. Others, like Windows 95 and Windows 98, do not.

To add a virtual parallel port to a virtual machine

1. Select the virtual machine.
2. Make sure the virtual machine is powered off.
3. Choose **VM > Settings**.
4. On the **Hardware** tab, click **Add**.
5. In the New Hardware wizard, select **Parallel Port** and click **Next**.
6. Specify which option to use for the parallel port:
   - If you select **Use physical parallel port**, click **Next** and choose the port from the drop-down menu.
   - If you select **Output file**, click **Next** and enter the path and filename or browse to the location of the file.
7. Under **Device status**, if you do not want the parallel port to connect at power on, deselect the check box.
8. Click **Finish**.
9. If the guest operating system is Windows 95 or Windows 98, run the guest operating system's Add New Hardware wizard to let Windows detect the new device.

   To display this wizard, choose **Start > Settings > Control Panel > Add New Hardware**.

Troubleshoot ECR Errors for Parallel Ports

When you power on the virtual machine after adding a parallel port, you might see an error message stating that the parallel port on the host does not have an Extended Control Register (ERC). If so, it is possible the hardware supports ECR but it has been disabled in the BIOS.

To troubleshoot ECR errors for parallel ports

1. Reboot the host.
2. Early in the boot process, press and hold down the Delete key to enter the host computer's BIOS configuration editor.
3. Find the parallel port field and enable Extended Capability Port (ECP) mode or a combination of modes that includes ECP.

   Most modern computers support ECP mode.

Configuring a Parallel Port on a Linux Host

For a parallel port to work properly in a guest, it must first be configured properly on the host. Most problems with parallel ports are caused by mistakes in the host configuration.

Linux kernels in the 2.4.x and 2.6.x series use a special arbitrator for access to the parallel port hardware. If the host is using the parallel port, the virtual machine cannot use it. If a virtual machine is using the parallel port, the host and any users accessing the host are denied access to the device. You must use the **VM > Removable Devices** menu to disconnect the parallel port from the virtual machine to access the device from the host.

Configure Parallel Ports for Linux 2.4.x Kernels

The 2.4.x kernels that support parallel ports use the `parport`, `parport_pc`, and `ppdev` modules. 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`. Support for user-space parallel device drivers (CONFIG_PPDEV) must also be enabled.

To configure parallel ports for Linux 2.4.x kernels

1. To determine whether the `parport`, `parport_pc`, and `ppdev` modules are installed and loaded on your system, run the `lsmod` command as the root user.

   These three modules are included in the listing of loaded modules. You can also look at the `/proc/modules` file for the list.

2. To load the proper modules, run the following command:

   ```
   insmod <modulename>
   ```

3. If none of the listed parallel port modules is loaded, use the following command:

   ```
   insmod parport_pc
   ```

   This command inserts the `parport` and `parport_pc` modules needed for a parallel port.

4. Use the following command to load the `ppdev` module:

   ```
   insmod ppdev
   ```

   If problems persist, the `lp` module might be loaded. If it is, the virtual machine cannot use the parallel port correctly.

5. If the `lp` module is loaded, run the following command as root to remove it:

   ```
   rmmod lp
   ```

6. To verify that the line referring to the `lp` module in the `/etc/modules.conf` or `/etc/conf.modules` file is removed or commented out, insert a pound sign (#) 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.

7. To ensure that the proper modules for the parallel port are loaded at boot time, add the following line to the `/etc/modules.conf` or `/etc/conf.modules` file:

   ```
   alias parport_lowlevel parport_pc
   ```

Configure Parallel Ports for Linux 2.6.x Kernels

The 2.6.x kernels that support parallel ports use the `modprobe <modulename>` and `modprobe parport_pc` modules. 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`.

To configure parallel ports for Linux 2.6.x kernels

1. To determine whether the `modprobe <modulename>` and `modprobe parport_pc` modules are installed and loaded on your system, run the `lsmod` command as the root user.

   You can also look at the `/proc/modules` file for the list.

   With 2.6.x, loading `parport_pc` does not load all modules.

2. If none of the listed parallel port modules is loaded, use the following command:

   ```
   modprobe parport_pc && modprobe ppdev
   ```

   This command inserts the modules needed for a parallel port.

   If problems persist, the `lp` module might be loaded. If it is, the virtual machine cannot use the parallel port correctly.

3. If the `lp` module is loaded, run the following command as root to remove it:

   ```
   rmmod lp
   ```

4. To verify that the line referring to the `lp` module in the `/etc/modules.conf` or `/etc/conf.modules` file is removed or commented out, insert a pound sign (#) 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.

5. To ensure that the proper modules for the parallel port are loaded at boot time, add the following line to the `/etc/modules.conf` or `/etc/conf.modules` file:

   ```
   alias parport_lowlevel parport_pc
   ```

Configure Device Permissions for Parallel Ports

Some Linux distributions by default do not grant the virtual machine access to the `lp` and `parport` devices. You must add the VMware user to the group that has permission to access these devices.

To configure device permissions for parallel ports

1. Run the following command to determine the owner and group for the device:

   ```
   ls -la /dev/parport0
   ```

   The third and fourth columns of the output show the owner and group, respectively. In most cases, the owner of the device is `root` and the associated group is `lp`.

2. To add the user to the device group, become the root user and open the `/etc/group` file with a text editor.

3. On the line starting with `lp`, which defines the `lp` group, add the Workstation user's user name.

   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.

Using Serial Ports

A Workstation virtual machine can use up to four virtual serial ports. The virtual serial ports can be configured in several ways:

- Connect a virtual serial port to a physical serial port on the host computer.
- Connect a virtual serial port to a file on the host computer.
- Make a direct connection between two virtual machines or between a virtual machine and an application running on the host computer.

For each of these choices, you can also select whether to connect the virtual serial port when you power on the virtual machine.

Add a Virtual Serial Port to a Virtual Machine

Use virtual serial ports to make devices such as modems available to virtual machines or to send debugging data from a virtual machine to the host or to another virtual machine.

You can use virtual serial ports to send data to the following:

- **Physical serial port** – Enables you to use a device such as an external modem or hand-held device in a virtual machine.
- **Output file on the host** – Captures the data that a program running in the virtual machine sends to the virtual serial port.
- **An application on the host** – Enables you to use an application on the host to capture debugging information sent from the virtual machine's serial port.
- **Another virtual machine** – Enables you to use an application in one virtual machine (the client) to capture debugging information sent from the other (the server) virtual machine's serial port.

To add a virtual serial port to a virtual machine

1. Select the virtual machine.
2. Make sure the virtual machine is powered off.
3. Choose **VM > Settings**.
4. On the **Hardware** tab, click **Add**.
5. In the Add Hardware wizard, select **Serial Port** and click **Next**.
6. On the Serial Port Type page, do one of the following:
    - For physical devices such as modems, select **Use physical serial port on the host**, click **Next,** and choose the port on the host computer that you want to use for this serial connection.
    - To capture data from an application in an output file, select **Output file**, click **Next,** and enter the path and filename or browse to the location of the file on the host.
    - To connect to a debugging application on the host or in another virtual machine, select **Output to Named Pipe** and click **Next**.

7 If you selected **Output to Named Pipe**, do one of the following:

- For a Windows host, on the Specify Named Pipe page, specify the pipe name.

  The pipe name must follow the form `\\.\pipe\<namedpipe>`. That is, it must begin with `\\.\pipe\`.

- For a Linux host, in the **Path** field, enter **`/tmp/`**`<socket>` or another UNIX socket name.

8 Also if you selected **Output to Named Pipe**, do one of the following:

- To send debugging information to an application on the host:

  i In the first drop-down menu, select **This end is the server** or **This end is the client**.

  Select **This end is the server** to start this end of the connection first.

  ii In the second drop-down menu, select **The other end is an application**.

- To send debugging information to another virtual machine:

  i In the first drop-down menu, select **This end is the server**.

  ii In the second drop-down menu, select **The other end is a virtual machine**.

9 Make sure the **Connect at power on** check box is selected if desired.

10 Click **Finish**.

11 (Optional) On the **Hardware** tab of the virtual machine settings editor, to configure this serial port to use polled mode, select **Yield CPU on poll**.

This option is of interest to developers who are using debugging tools that communicate over a serial connection. If the serial port in the guest is being used in polled mode rather than interrupt mode, you might notice performance issues. This option forces the virtual machine to yield processor time if the only task it is trying to do is poll the virtual serial port.

If you are setting up a connection between two virtual machines, you now have the first virtual machine set up as the server. Repeat this procedure for the second virtual machine, but set it up as the client by selecting **This end is the client** when configuring the named pipe.

Change the Input Speed of the Serial Connection

You can increase the speed of a serial connection over a pipe to a virtual machine.

Before you begin, 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.

In principle, the output speed, which is the speed at which the virtual machine sends data through the virtual serial port, is unlimited. In practice, the output speed depends on how fast the application at the other end of the pipe reads inbound data.

To change the input speed of the serial connection

1 Power off the virtual machine and close the Workstation window.

2 Use a text editor to add the following line to your virtual machine's configuration (.vmx) file:

```
serial<n>.pipe.charTimePercent = "<x>"
```

<n> is the number of the serial port, starting from 0. The first serial port is serial0.

The <x> value is a positive integer that specifies the time taken to transmit a character, expressed as a percentage of the default speed set for the serial port in the guest. For example, a setting of 200 forces the port to take twice as long for each character, or send data at half the default speed. A setting of 50 forces the port to take only half as long for each character, or send data at twice the default speed.

Assuming that 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.

Debugging over a Virtual Serial Port

Using virtual machines, you can debug kernel code on one system without the need for two physical computers, a modem, or a serial cable. 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 Hardware Developer Central (WHDC) Web site.

Debug an Application in a Virtual Machine from a Windows Host

In this configuration, 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`) on a Windows host.

Before you begin, on the host, make sure you have a recent version of Debugging Tools for Windows, which supports debugging over a pipe. You need version 5.0.18.0 or higher.

To debug an application in a virtual machine from a Windows host

1. Prepare the target virtual machine as described in "Add a Virtual Serial Port to a Virtual Machine" on page 319.

   Make sure you select **This end is the server** when configuring the named pipe.

2. Power on the virtual machine.

3. Choose **VM > Removable Devices** menu to make sure the serial port is connected.

   If **Serial<n>** is not reported as `\\.\pipe\<namedpipe>`, choose the virtual serial port and click **Connect**.

4. On the host, open a command prompt window and enter the following command:

```
<debugger> -k com:port=\\.\pipe\<namedpipe>,pipe
<debugger> is WinDbg or KD.
```

5. Press Enter to start debugging.

Debug an Application in a Virtual Machine from Another Virtual Machine

This configuration is useful if you use Workstation on a Linux host. In this situation, you have kernel code to debug in the target virtual machine and are running Debugging Tools for Windows (`WinDbg`) or Kernel Debugger (`KD`) in the debugger virtual machine on the same host.

Before you begin, download and install `WinDbg` or `KD` in the Windows guest that you plan to use as the debugger virtual machine.

To debug an application from another virtual machine

1. Prepare the virtual machines as described in "Add a Virtual Serial Port to a Virtual Machine" on page 319.

2. Power on both virtual machines.

3. Use the **VM > Removable Devices** menu to make sure the serial port is connected.

   If the serial port is not connected, choose the virtual serial port and click **Connect**.

4. In the debugger virtual machine, start debugging with WinDbg or KD.

Configuring Keyboard Features

You can change which key combinations you use for hot-key sequences in Workstation and which language to use for the keyboard that virtual network computing (VNC) clients use. In addition, you can configure platform-specific keyboard features for Windows and Linux hosts.

Use the Enhanced Virtual Keyboard for Windows Hosts

The enhanced virtual keyboard feature provides better handling of international keyboards and keyboards with extra keys. It also offers security improvements because it processes raw keyboard input as soon as possible, bypassing Windows keystroke processing and any malware that is not already at a lower layer. This feature is currently available for all 32-bit Windows guests except Windows Vista guests.

If you use the enhanced virtual keyboard, when you press Ctrl+Alt+Delete, the guest system only, rather than both guest and host, acts on the command.

Before you begin, if you just installed or upgraded to Workstation 6.x and have not yet restarted your computer, do so.

To use the enhanced virtual keyboard for Windows hosts

1. Select the virtual machine.
2. Make sure the virtual machine is powered off.
3. Choose **VM > Settings**.
4. Click the **Options** tab, and select **General**.
5. To enable or disable the setting, select or deselect the **Use enhanced virtual keyboard** check box and click **OK**.

Hot Keys for Virtual Machines

Hot keys let you specify the key combination that is used with hot-key sequences for virtual machines. For example, you can require that all hot-key sequences use Ctrl+Shift+Alt.

Configuring hot keys is useful to prevent certain key combinations (such as Ctrl+Alt+Del) from being intercepted by Workstation instead of being sent to the guest operating system. Use hot-key sequences to:

- Switch between virtual machines
- Enter and leave full screen mode
- Release (ungrab) input

- Send Ctrl+Alt+Del to the virtual machine only (not to the host machine)
- Send commands to the virtual machine only (not to the host machine)

The default settings for hot keys are listed in the preferences editor (choose **Edit > Preferences > Hot Keys**). Use the preferences editor to change them.

Use Ctrl+Alt in a Key Combination

Because Ctrl+Alt tells Workstation to release (ungrab) mouse and keyboard input, combinations that include Ctrl+Alt are not passed to the guest operating system. You must use the Space key if the key combination includes Ctrl+Alt.

To use Ctrl+Alt in a key combination

1. Press Ctrl+Alt+spacebar.
2. Release the spacebar without releasing Ctrl and Alt.
3. Press the third key of the key combination you want to send to the guest.

Specify a Language Keyboard Map for VNC Clients

If you set a virtual machine to act as a VNC server, you can specify which language to use for the keyboard that VNC clients use. By default, the US101 keyboard map (U.S. English) is used.

Before you begin, set the virtual machine to act as a VNC server. See “Configure a Virtual Machine as a VNC Server” on page 212.

Also, determine the location of the keymap file to use. Default keymap files are included in the Workstation installation directory:

- On Windows hosts, this directory is in `C:\Documents and Settings\All Users\Application Data\VMware\vnckeymap`.
- On Linux hosts, this directory is in `/usr/lib/vmware/vnckeymap`.

If the keymap file you want to use is in another location, determine the path to the file.

Also determine the language code. Use the following list:

- `de`: German
- `de-ch`: German (Switzerland)
- `es`: Spanish
- `fi`: Finnish
- `fr`: French
- `fr-be`: French (Belgium)

- fr–ch: French (Switzerland)
- is: Icelandic
- it: Italian
- jp: Japanses
- nl–be: Dutch (Belgium)
- no: Norwegian
- pt: Polish
- uk: UK English
- us: US English

To specify a language keyboard map for VNC clients

1. Use a text editor to open the configuration file (.vmx file) for the virtual machine and add the following lines, where <port number> is the port number to use:

   - **RemoteDisplay.vnc.enabled = "TRUE"**
   - **RemoteDisplay.vnc.port = "**<port number>**"**

2. Add one of the following properties to the configuration file, where <xx> is the code for the language to use, such as jp for Japanese:

   - To use the default keymap file included in the Workstation installation directory, set the following property:

     RemoteDisplay.vnc.keyMap = "<xx>**"**

   - To use a keyboard map file in another location, set the following property to an absolute file path:

     RemoteDisplay.vnc.keyMapFile

You can now start the virtual machine and connect to it from a VNC client. See "Use a VNC Client to Connect to a Virtual Machine" on page 213.

Keyboard Mapping on a Linux Host

Several situations might require you to set properties in a virtual machine's configuration file (`.vmx` file) to change the way a key is mapped.

Configure Keyboard Mapping for a Remote X Server

Sometimes the keyboard works correctly with a local X server but not when you run the same virtual machine with a remote X server. You need to set additional properties in the configuration (`.vmx`) file.

Before you begin, verify that the remote X server is an XFree86 server running on a PC.

If the keyboard does not work correctly on an XFree86 server running locally, report the problem to VMware technical support.

For local X servers, Workstation maps X key codes to PC scan codes to correctly identify a key. Workstation uses this key code map only for local X servers because it cannot tell whether a remote X server is running on a PC or on some other kind of computer. In this case, you can set a property to tell Workstation to use key code mapping. For a description of key code mapping, see "X Key Codes Compared to Keysyms" on page 327.

To configure keyboard mapping for a remote X server

1. Power off the virtual machine and close the Workstation window.
2. On the machine that hosts the virtual machine, add one of the following lines to the virtual machine configuration (`.vmx`) file or to `~/.vmware/config`:
   - If you use an XFree86-based server that Workstation does not recognize as an XFree86 server, use the following property:

     ```
     xkeymap.usekeycodeMap = "TRUE"
     ```

     This property tells Workstation to always use key code mapping regardless of server type.
   - If Workstation does recognize the remote server as an XFree86 server, use the following property:

     ```
     xkeymap.usekeycodeMapIfXFree86 = "TRUE"
     ```

     This property tells Workstation to use key code mapping if you are using an XFree86 server, even if it is remote.
3. Save and close the file.

Change How a Specific Key Is Mapped

If some keys on the keyboard do not work correctly in a virtual machine, you can set a property that makes a modification to the map.

Before you begin, perform the following tasks:

- Verify that the X server is an XFree86 server running on a PC. If the X server is remote, configure it to use key code mapping. See "Configure Keyboard Mapping for a Remote X Server" on page 326. For a description of key code mapping, see "X Key Codes Compared to Keysyms" on page 327.
- Determine the X key code and the corresponding v-scan code for the key. To find the X key code for a key, run `xev` or `xmodmap -pk`. Most v-scan codes are listed in "V-Scan Code Table" on page 330.

To change how a specific key is mapped

1. Power off the virtual machine and close the Workstation window.
2. On the machine that hosts the virtual machine, add the following line to the virtual machine configuration (`.vmx`) file or to `~/.vmware/config`:

   ```
   xkeymap.keycode.<code> = "<v-scan_code>"
   ```

   The `<code>` value must be a decimal number and `<v-scan_code>` must be a C-syntax hexadecimal number (for example, `0x001`).

   For example, to swap left Ctrl and Caps Lock, use the following lines:

   ```
   xkeymap.keycode.64 = "0x01d # X Caps_Lock -> VM left ctrl"
   xkeymap.keycode.37 = "0x03a # X Control_L -> VM caps lock"
   ```

3. Save and close the file.

X Key Codes Compared to Keysyms

Pressing a key on the PC keyboard generates a PC scan code based roughly on the position of the key. For example, the Z key on a German keyboard generates the same code as the Y key on an English keyboard because they are in the same position on the keyboard. Most keys have one-byte scan codes, but some keys have two-byte scan codes with prefix 0xe0.

Internally, Workstation uses a simplified version of the PC scan code that is a single nine-bit numeric value, called a v-scan code. A v-scan code is written as a three-digit hexadecimal number. The first digit is 0 or 1. For example, the Ctrl key on the left side of the keyboard has a one-byte scan code (0x1d). Its v-scan code is 0x01d. The Ctrl key scan code on the right side of the keyboard is two bytes (0xe0, 0x1d). Its v-scan code is 0x11d.

An XFree86 server on a PC has a one-to-one mapping from X key codes to PC scan codes, or v-scan codes, which is what Workstation uses. When Workstation is hosted on an XFree86 server and runs a local virtual machine, 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 languages. In other cases (not an XFree86 server or not a local server), Workstation must map keysyms to v-scan codes by using a set of keyboard-specific tables.

An X server uses a two-level encoding of keys, which includes the X key code and the keysym. 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. You can use an X application to control the mapping by using the function `XChangeKeyboardMapping()` or by the program `xmodmap`. To explore keyboard mappings, you can use the `xev` command, which shows the key codes and keysyms for keys typed into its window.

A key code corresponds roughly to a physical key, whereas 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.

Configure How Keysyms Are Mapped

When key code mapping cannot be used or is disabled, Workstation maps keysyms to v-scan codes. If a language-specific keyboard does not appear to be supported by Workstation, you might need to set a property that tells Workstation which keysym table to use.

Before you begin, perform the following tasks:

- To change the mapping of a few keys, determine the keysym name for each key that is not mapped correctly.

  The easiest way to find the keysym name for a key is to run the `xev` or `xmodmap –pk` commands. The X header file `/usr/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.

- To use a different keysym table, determine which mapping table to use.

  The tables are located in the xkeymap directory in the Workstation installation directory (usually /usr/lib/vmware). The table you must 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. For most of these, both the 101-key (or 102-key) and the 104-key (or 105-key) variants are available.

- If none of the mapping tables is completely correct, find one that works best, copy it to a new location, and change the individual keysym mappings.

Workstation determines which table to use by examining the current X keymap. However, its decision-making process can sometimes fail. In addition, each mapping is fixed and might not be completely correct for any given keyboard and X key code-to-keysym mapping. For example, a user might have swapped Ctrl and Caps Lock using xmodmap. This means the keys are swapped in the virtual machine when using a remote server (keysym mapping) but are unswapped when using a local server (key code mapping). To correct this situation, use configuration settings.

To configure how keysyms are mapped

1. Power off the virtual machine and close the Workstation window.
2. On the machine that hosts the virtual machine, add one or more of the following lines to the virtual machine configuration (.vmx) file or to ~/.vmware/config:

   - To disable X key code mapping to map keysyms rather than key codes to v-scan codes, set the following property:

     ```
     xkeymap.nokeycodeMap = "TRUE"
     ```

     For more information, see “X Key Codes Compared to Keysyms” on page 327.

   - If Workstation has a table in the xkeymap directory for your keyboard but cannot detect it, set the following property:

     ```
     xkeymap.language = "<keyboard_type>"
     ```

     The value <keyboard_type> must specify one of the tables in the xkeymap directory. However, the failure to detect the keyboard probably means the table is not completely correct for you. You might need to create a modified table and use the xkeymap.fileName property, described next.

- To use a different keysym mapping table that is not in the xkeymap directory, set the following property, where <file_path> is the path to the table:

  ```
  xkeymap.fileName = "<file_path>"
  ```

  The table must list a keysym for each key by using the following form:

  ```
  <sym> = "<v-scan_code>"
  ```

  The <sym> value is an X keysym name, and <v-scan_code> is a C-syntax hexadecimal number (for example, 0x001). Use a new line for each keysym.

  Compiling a complete keysym mapping is difficult. VMware recommends editing an existing table and making small changes.

- To change the keysym mapping of a few keys, set the following property for each key, on separate lines:

  ```
  xkeymap.keysym.<sym> = "<v-scan_code>"
  ```

  The value <sym> must be an X keysym name and <v-scan_code> is a C-syntax hexadecimal number (for example, 0x001).

  Most v-scan codes are listed in "V-Scan Code Table" on page 330. The xkeymap tables themselves are also helpful.

3 Save and close the file.

V-Scan Code Table

Table 16-1 shows the v-scan codes for the 104-key U.S. keyboard.

Table 16-1. V-Scan Codes for the 104-Key U.S. Keyboard

Symbol	Shifted Symbol	Location	V-Scan Code
Esc			0x001
1	!		0x002
2	@		0x003
3	#		0x004
4	$		0x005
5	%		0x006
6	^		0x007
7	&		0x008
8	*		0x009
9	(		0x00a

Table 16-1. V-Scan Codes for the 104-Key U.S. Keyboard (Continued)

Symbol	Shifted Symbol	Location	V-Scan Code
0	)		0x00b
-	_		0x00c
=	+		0x00d
Backspace			0x00e
Tab			0x00f
Q			0x010
W			0x011
E			0x012
R			0x013
T			0x014
Y			0x015
U			0x016
I			0x017
O			0x018
P			0x019
[	{		0x01a
]	}		0x01b
Enter			0x01c
Ctrl		left	0x01d
A			0x01e
S			0x01f
D			0x020
F			0x021
G			0x022
H			0x023
J			0x024
K			0x025
L			0x026
;			0x027

Table 16-1. V-Scan Codes for the 104-Key U.S. Keyboard (Continued)

Symbol	Shifted Symbol	Location	V-Scan Code
'			0x028
`			0x029
Shift		left	0x02a
\	|		0x02b
Z			0x02c
X			0x02d
C			0x02e
V			0x02f
B			0x030
N			0x031
M			0x032
,	<		0x033
.	>		0x034
/	?		0x035
Shift		right	0x036
*		numeric pad	0x037
Alt		left	0x038
Space bar			0x039
Caps Lock			0x03a
F1			0x03b
F2			0x03c
F3			0x03d
F4			0x03e
F5			0x03f
F6			0x040
F7			0x041
F8			0x042
F9			0x043
F10			0x044

Table 16-1. V-Scan Codes for the 104-Key U.S. Keyboard (Continued)

Symbol	Shifted Symbol	Location	V-Scan Code
Num Lock		numeric pad	0x045
Scroll Lock			0x046
Home	7	numeric pad	0x047
Up arrow	8	numeric pad	0x048
PgUp	9	numeric pad	0x049
-		numeric pad	0x04a
Left arrow	4	numeric pad	0x04b
5		numeric pad	0x04c
Right arrow	6	numeric pad	0x04d
+		numeric pad	0x04e
End	1	numeric pad	0x04f
Down arrow	2	numeric pad	0x050
PgDn	3	numeric pad	0x051
Ins	0	numeric pad	0x052
Del		numeric pad	0x053
F11			0x057
F12			0x058
Break	Pause		0x100
Enter		numeric pad	0x11c
Ctrl		right	0x11d
/		numeric pad	0x135
SysRq	Print Scrn		0x137
Alt		right	0x138
Home		function pad	0x147
Up arrow		function pad	0x148
Page Up		function pad	0x149
Left arrow		function pad	0x14b
Right arrow		function pad	0x14d
End		function pad	0x14f

Table 16-1. V-Scan Codes for the 104-Key U.S. Keyboard (Continued)

Symbol	Shifted Symbol	Location	V-Scan Code
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 key on the numeric pad. Its v-scan code is 0x054.

Keyboards outside the U.S. usually have an extra key (often < > or < > |) next to the left Shift key. The v-scan code for this key is 0x056.

Using USB Devices in a Virtual Machine

Workstation provides a two-port USB controller, so that you can connect to USB 1.1 and USB 2.0 devices:

- For USB 1.1, a UHCI controller with a virtual hub enables you to connect to more than two USB 1.1 devices.
- For USB 2.0, an EHCI controller enables you to connect to up to six USB 2.0 devices. For USB 2.0 support, your host must support USB 2.0, and you must enable USB 2.0 support in Workstation. USB 2.0 devices include high-speed or isochronous devices such as webcams, speakers, and microphones.

  USB 2.0 support is available only for Workstation 6 and higher virtual machines.

On the host, when a USB 2.0 device connects to a port, the device connects to the EHCI controller and operates in USB 2.0 mode. A USB 1.1 device is automatically connected to a UHCI controller and operates in USB 1.1 mode. In Workstation 6 and higher virtual machines, this behavior is simulated if you enabled it. See "Enable the USB 2.0 Controller for a Virtual Machine" on page 335.

Although your host operating system must support USB, you do not need to install device-specific drivers for USB devices in the host operating system to use those devices only in the virtual machine. Windows NT and Linux kernels earlier than 2.2.17 do not support USB.

VMware has tested a variety of USB devices with Workstation 6.5. If the guest operating system has appropriate drivers, you can use PDAs, printers, storage (disk) devices, scanners, MP3 players, digital cameras, and memory card readers.

USB human interface devices, such as the keyboard and mouse, can be handled though the virtual machine's USB controller. If you do not select the option to show all USB input devices as removable devices, 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.

Enable the USB 2.0 Controller for a Virtual Machine

The virtual machine's USB ports are enabled by default, although support for high-speed USB 2.0 devices is not enabled by default. Modems and certain streaming data devices, such as speakers and webcams, do not work properly unless you enable USB 2.0 support.

Before you begin, perform one of the following tasks that apply to your configuration:

- Verify that the virtual machine is a Workstation 6 or higher virtual machine.
- On Windows XP guests, verify that the latest service pack is installed to use USB 2.0.

  If you use Windows XP with no service packs, the driver for the EHCI controller cannot be loaded.
- On a Windows 2000 host with USB 2.0 support, use the Microsoft USB 2.0 driver for the USB controller.

  Third-party USB 2.0 drivers, such as those that some motherboard manufacturers provide, are not supported. See "Replace USB 2.0 Drivers on a Windows 2000 Host" on page 339.

If you do not plan to use USB devices in a virtual machine, you can use the virtual machine settings editor to disable USB 2.0 support.

To enable the USB 2.0 Controller for a virtual machine

1. Select the virtual machine.
2. Choose **VM > Settings**.
3. On the **Hardware** tab, select **USB Controller**.
4. Select the **Enable high-speed support for USB 2.0 devices** check box and click **OK**.

Add a USB Controller to a Virtual Machine

By default, a USB controller is included when you create a virtual machine. If you remove the USB controller, you can add it back.

This controller is required to use a smart card in a virtual machine regardless of whether the smart card reader is a USB device.

To add a USB controller to a virtual machine

1. Select the virtual machine.
2. Make sure the virtual machine is powered off.
3. Choose **VM > Settings**.
4. On the **Hardware** tab, click **Add** to start the Add Hardware wizard.
5. On the Hardware Type page, select **USB Controller** and click **Next**.
6. On the USB page, click **Finish**.
7. In the virtual machine settings editor, click **OK**.

You can now start the virtual machine and automatically or manually connect USB devices and smart card readers.

Connecting USB Devices

When a virtual machine is running, its window is the active window. If you plug a USB device into the host, by default, the device connects to the virtual machine instead of the host.

If you manually connect a USB device to a virtual machine (choose **VM > Removable Devices**), Workstation retains the virtual machine's connection to the affected port on the host. You can suspend or power off the virtual machine, or unplug the device. When you plug the device back in or resume the virtual machine, Workstation reconnects the device. Workstation retains the connection by writing an autoconnect entry to the virtual machine's configuration (`.vmx`) file.

If Workstation cannot reconnect to the device (for example, because you disconnect the device), the device is removed and a message is displayed, indicating that Workstation cannot connect to the device. You can connect manually to the device if it is still available.

Enable or Disable Automatic Connection of USB Devices

You can disable the autoconnect feature if you do not want USB devices to automatically connect to the virtual machine when you power it on.

To enable or disable automatic connection of USB devices

1 Select the virtual machine.

  The virtual machine can be powered on or off unless you plan to change the setting for connecting to USB mouse and keyboard devices. In this case, the virtual machine must be powered off.

2 Choose **VM > Settings**.

3 On the **Hardware** tab, select **USB Controller**.

4 To connect to human interface devices (HIDs), such as USB 1.1 and 2.0 mouse and keyboard devices, select the **Show all USB input devices** check box.

  An HID that is connected to the guest is not available to the host.

5 Select or deselect the **Automatically connect new USB devices to this virtual machine when it has focus** check box to enable or disable the setting and click **OK**.

Connect a USB Device Manually

If a device that is connected to the host does not automatically connect to a virtual machine at power on, you can connect the device manually.

Before you begin, for USB mouse, keyboard, and other input devices, you must enable showing these devices. See "Enable or Disable Automatic Connection of USB Devices" on page 337.

Also, when you are using a virtual machine, if you plug a device in to the host, the autoconnect feature usually connects the device to the virtual machine. If this action does not occur, you can connect the device manually.

To connect a USB device manually

1 Select the virtual machine.

2 Make sure the virtual machine is powered on.

3 Choose **VM > Removable Devices > <device_name>**.

Here **<device_name>** specifies the USB device that is plugged in to the host. A check mark appears next to the device's name, indicating that it is connected.

If the physical USB devices are connected to the host through a hub, the virtual machine sees only the USB devices, not the hub.

USB Driver Installation on a Windows Host

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 Windows XP and Windows Server 2003 hosts, the Microsoft Windows Found New Hardware wizard prompts you to run it. Select the default action, **Install the software automatically**. After the software is installed, the guest operating system detects the USB device and searches for a suitable driver.

Synchronize a PDA to Install a PDA Driver

When you synchronize 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 might exceed the device's connection timeout value. This causes the device to disconnect itself from the computer before the guest can synchronize with it.

To synchronize a PDA to install a PDA driver

1 Connect the USB device to the computer that hosts the virtual machine.

2 Synchronize the PDA with the host.

3 Let the guest finish installing the PDA driver.

4 Dismiss any connection error warnings.

5 Synchronize the PDA again.

This second attempt usually succeeds.

Replace USB 2.0 Drivers on a Windows 2000 Host

To use Workstation on a Windows 2000 host that has USB 2.0 ports, you must use the Microsoft USB 2.0 drivers for the USB controller in the host operating system. If your host operating system is using a third-party driver, a driver supplied by your motherboard vendor, for example, you must replace it.

To replace USB 2.0 drivers on a Windows 2000 host

1 To determine the provider of the USB driver, open the Device Manager, as follows:

   a Right-click **My Computer** and choose **Properties**.

   b Click the **Hardware** tab and click **Device Manager**.

2 Expand the listing for Universal Serial Bus controllers.

3 Right-click the listing for the controller and choose **Properties**.

4 Click the **Driver** tab.

   If the driver provider shown on the tab is Microsoft, you have the correct driver and do not need to replace it.

5 If the driver provider is not Microsoft, download and install the latest USB driver for your host operating system from the Microsoft Web site.

   Details are available in Microsoft knowledge base article 319973.

Access and Use a USB Device on a Linux Host

On Linux hosts, Workstation uses the USB device file system to connect to USB devices. If the USB device file system is not located in `/proc/bus/usb`, you must mount the USB file system to that location.

Before you begin, add a USB controller to the virtual machine if the virtual machine does not have one. See "Add a USB Controller to a Virtual Machine" on page 336.

Do not attempt to add a USB drive's device node directory (for example, `/dev/sda`) to the virtual machine as a hard disk.

To access and use a USB device on a Linux host

1 Run the following command as root:

```
mount –t usbfs none /proc/bus/usb
```

2 Connect the USB device to the host and begin using it.

How Device Control Is Shared Between Host and Guest

Only the host or the guest can have control of a USB device at any one time. Device control operates differently, depending on whether the host is a Linux or a Windows computer.

Device Control on a Windows Host

When you connect a device to a virtual machine, it is disconnected 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.

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, and connect to the device in the virtual machine again.

On Windows 2000, Windows XP, and Windows Server 2003 hosts, when you connect a USB network or storage device to a virtual machine, a message might appear on the host that says the device can be removed safely. This is normal behavior, and you can dismiss the dialog box. However, do *not* remove the device from your physical computer.

If the network or storage device does not disconnect from the host, use the appropriate system tray icon to disconnect it. On Windows 2000, the icon is called **Eject Hardware**. On Windows XP and Windows Server 2003, it is called **Safely Remove Hardware**.

Troubleshoot Device Control Issues on a Linux Host

On Linux hosts, guest operating systems can use devices that are not already in use by the host—that is, devices that are not claimed by a host operating system driver.

If the device is in use by the host and you try to choose **VM > Removable Devices** to connect it to the guest, a dialog box appears, asking whether you want to disconnect the driver on the host. Occasionally, disconnecting the device fails.

A related issue sometimes affects devices that rely on automatic connection (as PDAs often do). Occasionally, even if you successfully used autoconnection to connect the device to the virtual machine, you might experience problems with the connection to the device.

To troubleshoot device control issues on a Linux host

1. If you have problems with automatic connections, choose **VM > Removable Devices** to disconnect the device and reconnect it.
2. If the problem persists, unplug the device physically and plug it in again.
3. If a warning appears that the device is in use, disable the device in the `hotplug` configuration files in the `/etc/hotplug` directory.

   For details on editing these configuration files, see your Linux distribution's documentation.
4. If a disconnection fails, do one of the following:

   - If the driver was automatically loaded by `hotplug`, disable it in the `hotplug` configuration files in the `/etc/hotplug` directory.

     For details on editing these configuration files, see your Linux distribution's documentation.
   - To unload the device driver manually, become root (`su –`) and use the `rmmod` command.

Disconnecting USB Devices from a Virtual Machine

Before you unplug a USB device or choose **VM > Removable Devices** to disconnect it from a virtual machine, be sure it is in a safe state.

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 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 did not actually write the data to the disk, you can lose data.

Use Smart Cards with Virtual Machines

A smart card is a plastic card about the size of a credit card but embedded with a computer chip. Many government agencies and large enterprises use smart cards to authenticate users who access their computer networks. Users plug a smart card reader into their computer and insert their smart card in the reader. They are then prompted for credentials to log on.

NOTE This feature is supported experimentally in this release of Workstation 6.5.

The virtual machine considers smart card readers to be a type of USB device. You can choose **VM > Removable Devices** to access them. Virtual machines can connect to smart card readers that interface to serial ports, parallel ports, USB ports, PCMCIA slots, and PCI slots.

A smart card can be shared between virtual machines or between the host and one or more virtual machines. Sharing is enabled by default. To disable sharing, see "Disable Smart Card Sharing" on page 343.

To use a host's smart card reader in a virtual machine, make sure the following prerequisites are satisfied:

- On Windows hosts, start the service called `SCardSvr.exe` if it is not already running.
- On Linux hosts, make sure the `libpcsclite` library is installed. Most recent Linux distributions include this library. Also make sure the `pcscd` daemon is running.
- Make sure the virtual machine has a USB controller.

  A USB controller is required regardless of whether the smart card reader itself is a USB device. By default, USB controllers are included when you create a virtual machine. If you removed the USB controller, you must add it back. See "Add a USB Controller to a Virtual Machine" on page 336.

To use smart cards with virtual machines

1. Connect the smart card reader to the host machine.
2. Start the virtual machine.
3. To connect the smart card reader to a virtual machine, choose **VM > Removable Devices > Virtual** `<smart_card_reader_model>`.

   If the smart card reader is a USB smart card reader, two items appear for it in the **Removable Devices** menu. Both items use the model name of the reader, but one item name begins with **Virtual**. Always select the virtual smart card item. If for some reason that item does not work correctly, select the other item.

   On Linux hosts, if you select the wrong item and then want to select the **Virtual** smart card item, see "Switch to Using the Virtual Smart Card Reader on Linux Hosts" on page 343.

Switch to Using the Virtual Smart Card Reader on Linux Hosts

Because of the way smart card reader functionality is implemented on Linux hosts, you must exit Workstation and restart the `pcscd` daemon on the host before switching from the non-virtual smart card reader to the virtual smart card reader.

To switch to using the virtual smart card reader on Linux hosts

1. To disconnect from the non-virtual smart card reader, use the **Removable Devices** menu and select **Disconnect**.
2. Power off the virtual machine and exit Workstation.
3. Physically disconnect the smart card reader from the host.
4. Restart the `pcscd` daemon on the host.
5. Physically connect the smart card reader to the host.
6. Start Workstation, power on the virtual machine, and connect to the virtual smart card reader.

   See "Use Smart Cards with Virtual Machines" on page 341.

Disable Smart Card Sharing

By default, you can share a smart card between virtual machines or between the host and one or more virtual machines. For security reasons, or if you encounter problems when attempting to share a smart card, you might want to disable smart card sharing.

The setting that controls smart card sharing is located in the global configuration file. The global configuration file is created when you change any of the default settings in the Workstation preferences editor (**Edit > Preferences**). The file location depends on the host operating system:

- On most Windows hosts:

  ```
  C:\Documents and Settings\All Users\Application Data\VMware\VMware
  Workstation\config.ini
  ```

- On Windows Vista hosts:

  ```
  C:\Users\All Users\VMware\VMware Workstation\config.ini
  ```

- On Linux hosts:

  ```
  /etc/vmware/config
  ```

To disable smart card sharing

1. If the `config.ini` file does not yet exist on your host computer, choose **Edit > Preferences** and change at least one of the settings in the preference editor.
2. Open the `config.ini` file with a text editor and add the following line:

   ```
   usb.ccid.useSharedMode = "FALSE"
   ```

3. Save and close the file.
4. Set permissions on this file so that other users cannot change it.

Support for Generic SCSI Devices

Generic SCSI gives the guest operating system direct access to SCSI devices connected to the host, such as scanners, tape drives, and other data storage devices. Using the SCSI generic driver, Workstation allows a virtual machine to run any SCSI device that is supported by the guest operating system.

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. Try any SCSI hardware and report problems to VMware technical support.

On Windows hosts, to access host SCSI devices from within a virtual machine, you must run Workstation as a user with administrator access.

On Linux hosts, you must have read and write permissions on a given generic SCSI device 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 can create a group with access to read and write to these devices and add the appropriate users to that group.

Installing Required Adapters or Drivers for Some Windows Guests

On older Windows guest operating systems, you might need to install special host bus adapters. To use a SCSI device with 32-bit Windows XP guests, you must install a special driver that VMware provides.

Installing a SCSI Adapter on Windows 9.x and Me Guests

If you use generic SCSI devices in a Windows 95, Windows 98, or Windows Me guest operating system and are experiencing problems with the devices, download the latest Mylex (BusLogic) BT/KT-958 compatible host bus adapter from LSI Web site. To install the driver, follow the instructions on the Web site.

This driver overrides what Windows chooses as the best driver, but it corrects known problems.

Installing a SCSI Driver for 32-Bit Windows XP Guests

To use SCSI devices in a 32-bit Windows XP virtual machine, you need a special SCSI driver available from the Downloads page of the VMware Web site. To install the driver, follow the instructions on the Web site.

Install the BusLogic Driver in a Windows NT 4.0 Guest

Generic SCSI devices use the virtual Mylex (BusLogic) BT/KT-958 compatible host bus adapter provided by the virtual machine. On Windows NT 4.0, you might need to install the driver manually if it is not already installed for a virtual SCSI disk. Do so before you add a generic SCSI device.

Before you begin, have your Windows NT installation CD available.

To install the BusLogic driver in a Windows NT 4.0 guest

1. To open the SCSI Adapters control panel, choose **Start > Settings > Control Panel > SCSI Adapters**.
2. On the **Drivers** tab, click **Add**.
3. In the list of vendors on the left, select **BusLogic**.
4. In the list of drivers on the right, select **BusLogic MultiMaster PCI SCSI Host Adapters** and click **OK**.
5. Insert the Windows NT CD when you are prompted and click **OK**.
6. Reboot when you are prompted.

Avoiding Concurrent Access on Linux Hosts

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 number. For example, `/dev/sg0` 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.

Some Linux devices such as tape drives, disk drives, and CD-ROM drives already have a designated `/dev` entry (`st`, `sd`, and `sr`, respectively). When the SCSI generic driver is installed, Linux identifies these devices with corresponding `sg` entries in `/dev` in addition to their traditional entries. 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` entry and the traditional `/dev` entry at the same time. When you specify which SCSI device to use in a virtual machine, do not specify `/dev/st0` or `/dev/sr0`.

CAUTION Do not attempt to use the same generic SCSI device in both host and guest. This can cause unexpected behavior and might cause loss or corruption of data.

Add a Generic SCSI Device to a Virtual Machine

To map virtual SCSI devices on a virtual machine to physical generic SCSI devices on the host, you must add a generic SCSI device to the virtual machine.

Before you begin, make sure you have the following required permissions:

- On Windows hosts, to access host SCSI devices as generic SCSI devices, you must run Workstation as a user with administrator access.
- On Linux hosts, generic SCSI requires version 2.1.36 or higher of the SCSI Generic (`sg.o`) driver, which comes with kernel 2.2.14 and higher. Also, you must be logged on as a user who has permissions to use the device (that is, read and write permissions).

To add a generic SCSI device to a virtual machine

1. Select the virtual machine.
2. Choose **VM** > **Settings**.
3. On the **Hardware** tab, click **Add** to start the Add Hardware wizard.
4. On the Hardware Type page, select **Generic SCSI Device** and click **Next**.
5. On the Choose SCSI Device page, from the drop-down menu of SCSI devices, select the physical device to map.

   If you do not see the device you want in the list, see “Troubleshoot Problems Detecting Generic SCSI Devices” on page 347.

   On Linux hosts, if you type in the path to the SCSI device, do not enter `/dev/st0` or `/dev/sr0`.

6 Select the **Connect at power on** check box to configure automatic connection behavior and click **Finish**.

7 On the **Hardware** tab, in the **Virtual device node** section, select the SCSI device identifier to use for the drive and click **OK**.

For example, if you select SCSI 0:2, the guest operating system sees the drive as ID 2 on controller 0.

Troubleshoot Problems Detecting Generic SCSI Devices

When you use the virtual machine settings editor to add a generic SCSI device to a virtual machine, occasionally the device does not appear in the list of available SCSI devices.

Before you begin troubleshooting this problem, you might need to know the following:

- The SCSI bus number that the device uses on the host system. The SCSI bus is assigned a number by the host operating system after all IDE buses are assigned numbers. For example, if you have two IDE buses, they are numbered 0 and 1. The first SCSI bus is assigned bus number 2.

  If you cannot determine the SCSI bus number, try using a third-party tool such as `winobj` to determine this information. You can download `winobj` for free from the Windows Sysinternals Web site.

- The target ID the device uses in the virtual machine and on the host. This ID is usually set by some jumpers or switches on the device. To determine the target ID, see the owner’s manual for the device.

The root causes or reasons Workstation cannot detect a device include the following:

- A driver for that device is not installed on the host.
- A driver on the host prevents the device from being detected.
- The virtual machine uses a device for which there are no drivers available to the host operating system. In this case, add the device manually to the virtual machine’s configuration (`.vmx`) file. Adding a device in this manner is recommended for advanced users only.

To troubleshoot problems detecting generic SCSI devices

1 Find out whether the device driver for this device is installed on the host.

2 If the device driver is not installed and you want to install it, do so and see if the device appears correctly in the virtual machine settings editor.

You might not want to install the driver on the host if you want to avoid a device-in-use conflict between the host and guest.

If a driver is installed but does not appear correctly, if you cannot install the driver on the host, or if you do not want to install the driver on the host, continue with the rest of this procedure.

3 If an original SCSI device driver is already installed on the host, disable it.

Some Windows operating systems do not process the send command from the adapter if the device driver owns the device.

4 Power off the virtual machine and open the virtual machine's configuration (`.vmx`) file in a text editor.

5 Add or change the following line in the `.vmx` file, where `X` is the SCSI bus number the device uses on the host system, and *Y* is the target ID the device uses both in the virtual machine and on the host:

```
scsiZ:Y.fileName = "<deviceName>"
```

For `"<deviceName>"` use:

```
"scsiX:Y"
```

The following is an example of how to set the option. The problematic device is a CD-ROM drive, and the existing entry in the configuration file is:

```
scsi0:4.fileName = "CdRom0"
```

If the device on the host is located on bus 2 with target ID 4, change this line to:

```
scsi0:4.fileName = "scsi2:4"
```

If your problem was that the virtual machine has a SCSI adapter and generic SCSI device, but Workstation did not recognize the device when the virtual machine was powered on, you can stop at this point.

6 If the virtual machine does not contain any SCSI devices, to add a generic SCSI device to a new virtual SCSI adapter, or to use an existing SCSI device as a generic SCSI device, also add the following line in the `.vmx` file:

```
scsiZ:Y.deviceType = "scsi-passthru"
```

If you wanted to use an existing SCSI device as a generic SCSI device, you can stop at this point.

7 If the virtual machine does not contain any SCSI devices, or to add a generic SCSI device to a new virtual SCSI adapter, also add the following lines in the `.vmx` file, where *Z* is the SCSI bus number the device uses in the virtual machine:

```
scsiZ:Y.present = "true"
scsiZ.present = "true"
```

If the virtual machine settings editor still does not include this device in the list of available SCSI devices for this virtual machine, contact VMware technical support.

Use Two-Way Virtual Symmetric Multiprocessing

With Virtual SMP, you can assign two virtual processors to a virtual machine on any host machine that has at least two logical processors.

The following are all considered to have two or more logical processors:

- A multiprocessor host with two or more physical CPUs
- A single-processor host with a multicore CPU
- A single-processor host with hyperthreading enabled

NOTE On hyperthreaded uniprocessor hosts, performance of virtual machines with Virtual SMP might be below normal. Even on multiprocessor hosts, performance is affected if you overcommit by running multiple workloads that require more total CPU resources than are physically available.

Guests with more than two virtual processors are not supported in Workstation. However, you can power on and run multiple dual-processor virtual machines concurrently.

The number of virtual processors for a given virtual machine appears in the summary view of the virtual machine.

To use two-way virtual symmetric multiprocessing

Do one of the following:

- For a new virtual machine, choose the custom configuration in the New Virtual Machine wizard. On the Processor Configuration page, specify the number.
- For an existing virtual machine, choose **VM > Settings** and on the **Hardware** tab, select **Processors** and specify the number.

Use a Virtual Machine That Originally Had More Than Two Virtual Processors

You can use Workstation 6.5 or higher, running on a multiprocessor host machine, to open a virtual machine created in ESX Server that has one or more virtual processors. You cannot use Workstation, however, to power on a virtual machine that has more than two virtual processors assigned, even if more processors were assigned when the virtual machine was created in ESX Server.

You can see the number of processors in the virtual machine's summary view or by using the virtual machine settings editor. To use a virtual machine that has more than two virtual processors assigned, you must change the number of processors before powering it on.

To use a virtual machine that originally had more than two virtual processors

1 Select the virtual machine.

2 Make sure the virtual machine is powered off.

3 Choose **VM > Settings**.

4 On the **Hardware** tab, select **Processors**, and note that **Number of Processors** is set to **Other (x)**, where **x** is the number of processors originally assigned in ESX Server.

Workstation preserves this original configuration setting for the number of processors, even though two is the maximum number of processors supported.

After you commit a change to this setting, the original setting for the number of processors is discarded and no longer appears as an option in the virtual machine settings editor.

5 Change the **Number of processors** setting to **One** or **Two** and click **OK**.

Special-Purpose Configuration Options for Windows Hosts 17

You can use configuration options for tasks like restricting the operations a user can perform with a virtual machine or simplifying the user interface for inexperienced users. In a classroom, for example, you can ensure that virtual machine configurations remain consistent from one class session to the next.

This chapter includes the following topics:

Locking Out Interface Features

Administrative lockout is a global setting that affects all virtual machines for all users on a host computer. It allows you to configure settings so that only a user who knows the password can perform the following tasks:

- Create new virtual machines.
- Edit virtual machine configurations.
- Edit network settings.

Set Administrative Lockout Preferences

If no user has set administrative lockout preferences, any user can set them and set a password for access to the administrative lockout features. If administrative lockout preferences are already set, you must know the password to change the settings.

To set administrative lockout preferences

1. Choose **Edit > Preferences**.
2. Click the **Lockout** tab and enter the password if prompted.
3. Select the **Enable** check box and select the actions you want to restrict.

   If this is the first time administrative lockout options are being set, specify a password in the fields provided.
4. Click **OK.**

Removing a Forgotten Password

If you cannot remember the password and need 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 can enable the administrative lockout features and set a new password.

Restricting the User Interface

To enable the restricted user interface, a user must have sufficient privileges to edit the virtual machine's configuration file and to set file permissions. The restricted user interface affects only the specific virtual machines for which the setting is created.

The following changes occur when you enable the restricted user interface:

- The toolbar is always hidden.
- All functions on the **VM > Power** menu, **Snapshot** menu, **Replay** menu, and **Removable Devices** menu are disabled.
- No access is provided to the virtual machine settings editor (**VM > Settings**).
- The user cannot change virtual networking settings (**Edit > Virtual Network Editor**).
- The user starts the virtual machine by double-clicking the configuration (`.vmx`) file or a desktop shortcut. The user shuts down by closing the virtual machine (**File > Exit**). It is also possible to launch Workstation and open a restricted-interface virtual machine from the **Favorites** list or **File** menu.

Enable the Restricted User Interface

Although the restricted user interface provides no access to menu and toolbar controls for a snapshot, you can give users limited snapshot control. If you set up a snapshot for the restricted virtual machine and set the power-off option to **Ask Me**, the standard dialog box appears when a virtual machine shuts down and the user can choose **Just Power Off**, **Take Snapshot**, or **Revert to Snapshot**.

To enable the restricted user interface

1. Power off the virtual machine and close the VMware Workstation window.
2. Open the virtual machine's configuration file (`.vmx` file) in a text editor.
3. Add the following line anywhere in the file:

   ```
   gui.restricted = "TRUE"
   ```
4. (Optional) Set file permissions on the configuration file to give normal users of the system only read access to the file.
5. Create a shortcut to the configuration file on the desktop and give it an appropriate name.

Restrict the User Interface and Return to a Snapshot

You can combine a restricted user interface with a snapshot to ensure that users' virtual machines always start in the same state. Typically, users running a virtual machine with a restricted user interface can only power it on and off, and the virtual machine boots when powered on. When the virtual machine has a snapshot set and is configured to return to that snapshot when powered off, the user can only start and power off the virtual machine. The virtual machine always starts from the snapshot.

To restrict the user interface and return to a snapshot

1. Power on the virtual machine and be sure it is in the appropriate state.
2. Create a snapshot.

   See "Take a Snapshot" on page 196.
3. Configure the virtual machine to return to the snapshot any time it is powered off: Choose **VM > Settings > Options > Snapshot/Replay** and select **After Powering Off** and **Revert to Snapshot**.

4 With the virtual machine powered off, restrict the user interface, as follows:

   a Close the VMware Workstation window.

   b Open the virtual machine's configuration file (`.vmx` file) in a text editor.

   c Add the following line anywhere in the file.

   ```
   gui.restricted = "TRUE"
   ```

5 (Optional) Set file permissions on the configuration file to give normal users of the system read-only access to the file.

6 Create a shortcut to the configuration file on the desktop and name it.

7 Run this virtual machine by double-clicking the shortcut to the configuration file.

   The virtual machine starts at the snapshot, with the user interface restricted. Users do not have a toolbar or access to the **VM > Power** menu or the virtual machine settings editor.

8 Choose **File > Close**.

   The virtual machine powers off, and the next time a user powers it on, it returns to the snapshot.

Disable the Restricted User Interface

Disable the restricted user interface to make items in the **VM** menu available to users again.

To disable the restricted user interface

1 Power off the virtual machine and close the VMware Workstation window.

2 Open the configuration file (`.vmx`) file and do one of the following:

   - Set `gui.restricted = "FALSE"`.
   - Remove or comment out the `gui.restricted = "TRUE"` line.

3 Save the changes to the configuration file and close it.

4 Start the virtual machine by double-clicking the shortcut.

   The virtual machine starts at the snapshot, and the interface is not restricted.

Making a Virtual Machine Always Use Full Screen Switch Mode

Full screen switch mode is a runtime option for the Workstation on Windows hosts. When Workstation is running in full screen switch mode, the user has no access to the Workstation user interface. The user cannot create, reconfigure, or launch virtual machines. A system administrator performs these functions.

When Workstation is running in full screen switch mode, one or more virtual machines can be running, and you can use hot keys to switch from one to another. You can also provide hot-key access to the host operating system.

Create a Virtual Machine for Use in Full Screen Switch Mode

To create virtual machines, run Workstation in standard mode. The instructions in this section assume that you are creating the virtual machines on a separate administrative computer. You can also create the virtual machines directly on the user's computer.

To create a virtual machine for use in full screen switch mode

1 Create a virtual machine for use in full screen switch mode:

   a Choose **File > New > Virtual Machine**.

   b On the Welcome page, select the Custom configuration.

   c On the Name the Virtual Machine page, make a note of the folder in which you create the virtual machine.

   d On the Specify Disk Capacity page, specify the size for the virtual disk and select **Allocate all disk space now**.

   If you do not make this selection and the host computer's hard disk runs out of space for a growing virtual disk file, the user sees no warning message and does not know what is causing the problem in the virtual machine.

2 Select the virtual machine and choose **VM > Settings**.

3 Make all needed configuration settings before you configure the user's computer to launch Workstation when the computer starts.

4 (Optional) If you plan to run the virtual machine on a laptop computer, be sure to set the virtual machine to report the battery status.

   See "Report Battery Information in the Guest" on page 157.

5 Copy all the files in this folder to the user's computer after you finish creating and configuring the virtual machine.

Moving a Virtual Machine to a User's Computer

The easiest way to move the virtual machine to a user's computer is to use a network connection to copy all the files in the virtual machine directory to a directory on the user's computer. You can also move the directory by using a DVD or other removable media large enough to store the files.

Place each virtual machine in its own separate directory.

Configuring Hot Keys for Full Screen Switch Mode

You can specify hot-key combinations for cycling through the currently powered on virtual machines, to switch to a specific virtual machine or the host, and more.

Specify Global Configuration Settings for Full Screen Switch Mode

To use full screen switch mode, you must, set one or more properties in the Workstation global configuration file.

The global configuration file is created when you change any of the default settings in the Workstation preferences editor (**Edit > Preferences**). The file location depends on the host operating system:

- On most Windows hosts:

  ```
  C:\Documents and Settings\All Users\Application Data\VMware\VMware
  Workstation\config.ini
  ```

- On Windows Vista hosts:

  ```
  C:\Users\All Users\VMware\VMware Workstation\config.ini
  ```

To specify global configuration settings for full screen switch mode

1. If the `config.ini` file does not yet exist on your host computer, choose **Edit > Preferences** and change at least one of the settings in the preference editor.

2. Open the `config.ini` file with a text editor and add at least one of the following lines:

   - **`fullScreenSwitch.cycleHost = "TRUE"`**

     This setting causes the host operating system to be included when you use a hot key for cycling through powered on virtual machines. See "Hot Key for Cycling Through Virtual Machines and the Host Computer" on page 359.

   - **`FullScreenSwitch.hostDirectKey = "`**`<value>`**`"`**

     Use this setting to define a hot key for switching directly to the host operating system. See "Host Operating System Hot Key" on page 360.

3 (Optional) Specify other full screen switch mode settings you want to use.

To specify hot keys for switching to other virtual machines or the host computer, first, see the following sections, in the order listed:

- "Virtual Key Codes" on page 357
- "Other Entries in the Global Configuration File" on page 360

4 Save and close the file.

5 Set permissions on this file so that other users cannot change it.

6 Open the `preferences.ini` file with a text editor and add the following lines:

```
pref.fullScreen.v5 = "TRUE"
pref.autoFitFullScreen = "fitGuestToHost"
```

On most Windows hosts, this file is located in:

```
%USERPROFILE%\Application Data\VMware\preferences.ini
```

On Windows Vista hosts, this file is located in:

```
%USERPROFILE%\AppData\Roaming\VMware\preferences.ini
```

To specify a hot key for switching to a specific virtual machine, see "Virtual Machine Hot Key" on page 359.

Virtual Key Codes

The hot-key entries described in this section require you to enter a virtual key code as part of the value for an option. Virtual key codes use hexadecimal format, which is a hexadecimal number preceded by 0x. For example, to use the virtual key code of 5A as a value, type **`0x5A`**.

Microsoft provides a reference list of virtual key codes. To access this reference list, enter the keyword virtual key codes on the MSDN Web site.

The hot-key entries also include modifier keys. The modifier keys are Ctrl, Alt, Shift, and Windows keys. The Windows key is the key between the Ctrl and Alt keys. You can also use a combination of those keys. Table 17-1 lists the key codes for modifier keys.

Table 17-1. Modifier Keys for Hot-Key Entries

Modifier Key	Hexadecimal Value
No modifier	0x0
Alt	0x1
Ctrl	0x2
Shift	0x4
Win (Windows)	0x8
Ctrl+Alt	0x3
Alt+Shift	0x5
Ctrl+Shift	0x6
Ctrl+Alt+Shift	0x7
Win+Alt	0x9
Win+Ctrl	0xa
Win+Ctrl+Alt	0xb
Win+Shift	0xc
Win+Shift+Alt	0xd
Win+Shift+Ctrl	0xe
Win+Shift+Ctrl+Alt	0xf

Keep the following limitations in mind when defining cycle keys and switch keys:

- Do not use the Pause key with the Ctrl key. You can use the Pause key with other modifier keys.
- If you use the F12 key, you must use one or more modifier keys. You cannot use the F12 key alone.
- You cannot use combinations that include only the Shift, Ctrl, and Alt keys. These keys can be used only as modifiers in combination with some other key.

When listing a key plus a modifier, type the virtual key code for the key followed by a comma and type the value for the modifier key or keys. For example, the value entry for Ctrl+Shift+F1 is `0x70,0x6`.

Hot Key for Cycling Through Virtual Machines and the Host Computer

You can specify a hot key or hot-key combination for cycling through the available virtual machines on a host computer. Hot keys behave in the following manner:

- Each time you press the specified hot key, the next virtual machine appears in order. You can also include the host operating system in the cycle.
- If any particular virtual machine is not running, it is skipped.
- If only one virtual machine is running and the host operating system is not included in the cycle, pressing the hot key has no effect.

The hot key for cycling through virtual machines is defined in the global configuration file (`config.ini`). Two options control cycling:

- `FullScreenSwitch.cycleKey`

  The value of this option defines the hot key. It is specified as `<key>,<modifier>`. It has no default. For example, to use the Pause key with no modifier to cycle through virtual machines, add the following line to the `config.ini` file, or modify its value if the option is already listed:

  ```
  FullScreenSwitch.cycleKey = "0x13,0x0"
  ```

- `FullScreenSwitch.cycleHost`

  Set this option to `TRUE` to include the host operating system in the cycle. The default is `FALSE`. For example, to include the host operating system in the cycle, add the following line to the `config.ini` file, or modify its value if the option is already listed:

  ```
  FullScreenSwitch.cycleHost = "TRUE"
  ```

Hot Keys for Switching Directly to Virtual Machines and the Host Computer

You can specify a hot key or combination of hot keys for switching directly to any available virtual machine on a host computer. Each time you press the specified hot key, the screen display switches to that of the specified virtual machine. You can also specify a hot key for switching directly to the host operating system.

Virtual Machine Hot Key

You define the hot key used to switch to a virtual machine by adding a local configuration setting in the virtual machine's `.vmx` file.

Use the following format:

```
<option> = "<value>"
```

Entries in the configuration files can appear in any order. The value of this option defines the hot key. It is specified as `<key>,<modifier>`. It has no default.

For example, to use Ctrl+Shift+F1 to switch to a particular virtual machine, add the following line to that virtual machine's `.vmx` file or modify its value if the option is already listed:

```
FullScreenSwitch.directKey = "0x70,0x6"
```

If any particular virtual machine is not running, pressing the hot key for that virtual machine has no effect.

Host Operating System Hot Key

You define the hot key used to switch to the host operating system by adding a line to the global configuration file (`config.ini`). The value of this option defines the hot key. It is specified as `<key>,<modifier>`. It has no default.

For example, to use Ctrl+Shift+F9 to switch to the host operating system, add the following line to the `config.ini` file, or modify its value if the option is already listed:

```
FullScreenSwitch.hostDirectKey = "0x78,0x6"
```

Other Entries in the Global Configuration File

The global configuration file (`config.ini`) entries in Table 17-2 are optional. They enable you to control certain functions of the virtual machine that are important in work environments where virtual machines need to be isolated from each other and from the host computer.

Table 17-2. Optional Global Configuration File Entries

Option	Description	Default Setting
`Isolation.tools.copy.enable` `Isolation.tools.paste.enable`	This option determines whether data in one virtual machine or the host operating system can be copied to another virtual machine or to the host operating system.	TRUE
`Isolation.tools.paste.enable` `Isolation.tools.copy.enable`	This option determines whether data copied in one virtual machine or the host operating system can be pasted into another virtual machine or the host operating system.	TRUE
`Isolation.tools.HGFS.disable`	This option determines whether virtual machines can be configured with shared folders, for sharing files among virtual machines and with the host computer.	FALSE

Table 17-2. Optional Global Configuration File Entries (Continued)

Option	Description	Default Setting
mks.CtlAltDel.ignore	Set this property to TRUE so that dialog boxes usually generated by Microsoft Windows Secure Attention Sequence (SAS) are not displayed but are passed on to the guest if the guest has keyboard focus.	
mks.fullscreen.allScreenSaver	Set this property to TRUE to allow the host operating system to run its screen saver when it determines that the machine is idle.	
msg.autoAnswer	Set this property to TRUE to suppress any Workstation dialog boxes that otherwise appear. The default answer is selected in these dialog boxes.	

Using vmware-fullscreen to Run a Virtual Machine

Use the vmware-fullscreen command to run Workstation in full screen switch mode and to start and stop virtual machines on a user's computer. The command can pass certain information to the virtual machine when it starts.

As administrator, you must decide how to issue the command. For example, you can use a custom application or script running on the host operating system to issue one or more vmware-fullscreen commands. Or you can include the command to start a virtual machine in a shortcut in the host operating system's startup group, so the virtual machine starts when the user logs in to the host computer.

Issue the vmware-fullscreen command once for each virtual machine you want to start or stop. The syntax for this command is:

```
C:\Program Files\VMware\VMware Workstation\vmware-fullscreen.exe [-poweron
               <parameters> | -poweroff <parameters> | -exit | -switchto
               <paramters> | -query | -listvms]
```

You can type these commands at the Windows command prompt or create scripts to run multiple commands.

Table 17-3 describes the available options and parameters.

Table 17-3. Command-Line Options for the vmware-fullscreen Program

Option	Parameters	Description

`-poweron`
or
`-fullscreen`
	`"<config-file>"`	Powers on the virtual machine, where `"<config-file>"` is required and specifies the full path to the virtual machine's configuration (`.vmx`) file.
		With `-poweron`, the user sees no immediate indication when the virtual machine starts, but the user can switch to the virtual machine with its direct-switch key or with the cycle key.
		With `-fullscreen`, the virtual machine goes to full screen mode immediately instead of running invisibly until the user switches to it later.

	`-s <variable>=<value>`	(Optional) Sets the specified variable to the specified value. Any variable names and values that are valid in the configuration file can be specified on the command line with the `-s` switch.
	`-name=<alias>`	(Optional) Gives an alias to the virtual machine. You can the use that alias in `-switchto` and `-poweroff` commands.
	`-directkey=<keyspec>`	(Optional) Specifies the virtual machine's direct-switch key. If a direct-switch key is specified in the virtual machine's configuration file, the command line overrides the configuration file. The following is an example of this switch: `-directkey=0x70,0x6`

`-poweroff`	`"<config-file>"`
	or
	`<alias>`
		Powers off the specified virtual machine. To specify the virtual machine, use either the full path to the virtual machine's configuration (`.vmx`) file or the alias if you defined one by using the `-name` switch.

`-exit`		Powers off all virtual machines and exits Workstation.

Table 17-3. Command-Line Options for the vmware-fullscreen Program (Continued)

Option	Parameters	Description
`–switchto`		Depending on the parameter you use, switches to the specified virtual machine, host operating system, or next machine (virtual machine or host) in the cycling order. A virtual machine must be powered on before you can switch to it.
	`"<config-file>"`	Switches to the virtual machine, where `"<config-file>"`specifies the full path to the virtual machine's configuration (`.vmx`) file.
	`<alias>`	Switches to the virtual machine, where `<alias>` specifies the alias you defined by using the `–name` switch.
	`host`	Switches to the host operating system.
	`next –qu`	Switches to the next machine in the cycling order.
`–query`		Determines whether Workstation is running in full screen switch mode. If so, also displays the process ID and window handle.
`–listvms`		Lists all virtual machines that are currently powered on. The list is added to the `vmware–fullscreen` log file.

vmware-fullscreen Log File

The `vmware–fullscreen` program writes to a log file. This log file records errors reported by `vmware–fullscreen` itself as it starts, stops, and passes other commands to Workstation. It is separate from the `vmware.log` file, which stores information on the running virtual machines.

The name of the `vmware–fullscreen` log file is `vmware–<username>–<pid>.log`. By default, the `vmware–fullscreen` log file is in the `temp` directory for the user logged in to the host computer. This location might be specified in the TEMP environment variable. The default location is:

```
C:\Documents and Settings\<username>\Local Settings\Temp
```

The administrator can specify a different location for this log file by adding the following line to the Workstation global configuration file (`config.ini`):

```
fullScreenSwitch.log.filename="<path>"
```

VMware recommends using a full path. If you use a relative path, the location is relative to the directory that is active when the `vmware–fullscreen` command is issued for the first time after the host computer reboots.

Guest ACPI S1 Sleep

Workstation provides experimental support for guest operating system ACPI S1 sleep. Not all guest operating systems support this feature. Common guest operating system interfaces for entering standby are supported.

By default, ACPI S1 sleep is implemented in Workstation as suspend. You can use the Workstation **Resume** button to wake the guest.

With the following entry in the configuration (`.vmx`) file for a virtual machine, ACPI S1 sleep is instead implemented as power-on suspend:

```
chipset.onlineStandby = TRUE
```

The guest operating system is not fully powered down. You can awaken the virtual machine in the following ways:

- Keyboard input
- Mouse input
- Programming the CMOS external timer

This feature can be useful for test and development scenarios.

Learning the Basics of VMware ACE 18

This chapter provides an overview of how to use Workstation to create and deploy virtual machines for end users. ACE (Assured Computing Environment) features are available only in the version of Workstation that runs on Windows hosts. This chapter includes the following topics:

Benefits of Using VMware ACE

VMware ACE is a software solution that enables organizations to deploy and manage secure, platform-independent virtual machines that end users can use on their work PC, personal computer, or even a portable USB media device. End users can be either connected to or disconnected from the enterprise network.

VMware ACE enables safe access to enterprise resources from assured computing environments. These isolated PC environments run on top of existing PCs. The assured computing environment (ACE) contains an operating system, enterprise applications, and preconfigured security settings.

With virtual rights management, built-in copy protection controls, and automatic encryption, VMware ACE helps prevent theft, tampering, and unauthorized copying of applications, data, system settings, and files. Administrators can protect data and ensure compliance with IT policies, including software life-cycle management and access to data and applications.

Key Features of VMware ACE

The key features of VMware ACE include manageability, security, and usability.

Manageability

- Create standardized hardware-independent PC environments and deploy them to any PC throughout the extended enterprise.
- Control the virtual machine's life cycle, security settings, network settings, system configuration, and user interface capabilities.
- Track instances through the user interface. View and manage the activation, expiration, and other policies of instances managed with ACE Management Server.

Security

- Rules-based network access lets you identify and quarantine unauthorized or out-of-date ACE instances. Enable access to the network once the ACE instance complies with IT policies.
- Tamper-resistant computing environment protects the entire ACE instance and package, including data and system configuration, with seamless encryption.
- Copy-protected computing environment prevents users from copying enterprise information.
- Roles-based SSL communication provides a secure protocol between the ACE Management Server and client.
- Resource signing lets you specify that ACE Resource files be protected from all tampering.

Usability

- The customizable interface lets you customize the behavior and look and feel for users.
- The flexible computing environment lets users revert to a previous state within seconds and can work when connected or disconnected from the enterprise network.

VMware ACE Terminology

The following terms are used frequently in the chapters describing VMware ACE features:

- **ACE-enabled virtual machine** – A virtual machine template that the ACE administrator creates. The ACE-enabled virtual machine can be configured with various policies, devices, and deployment settings and then used as the basis for creating any number of packages to be sent to ACE users.
- **ACE instance** – The virtual machine that ACE administrators create, associate with policies, and activate on end users' computers. An ACE instance that is managed by ACE Management Server is a managed ACE instance. An ACE instance that is not managed by ACE Management Server is a standalone ACE instance.
- (Optional) **ACE Management Server** – The ACE Management Server enables you to manage ACE instances, to publish policy changes to dynamically update those instances, and to test and deploy packages more easily. ACE Management Server adds new integration with Active Directory setups and provides secure Active Directory and LDAP integration, with role-based secure SSL communication.

  For more information, see the *VMware ACE Management Server Administrator's Guide*.
- **Pocket ACE** – Enables an administrator to bundle and deploy an ACE instance onto a USB portable media device, including USB flash drives, Apple iPod mobile digital devices, and portable hard drives.

Network and Disk Space Requirements for the Administrative Workstation

As an administrator, you use Workstation to create and manage the virtual machines you distribute to end users. Following is a list of prerequisites for the machine that hosts Workstation:

- If your company already has a library of standard virtual machines, you need network access to that library from your host computer.
- If you are creating virtual machines, you need access to installers for the guest operating systems and application software that you plan to install in the virtual machines.

  You can install operating systems from CDs, DVDs, ISO image files on a local drive or on the network, or a PXE server. You can install application software from CDs, DVDs, or installers on a local drive or on the network.
- You need to provide adequate disk space for virtual machine files and package files. The files for each virtual machine can be as large as several gigabytes. The package files can also be large. The default location for the package files is the `Packages` folder inside the virtual machine's folder.
- Workstation needs a substantial amount of temporary working space when it creates a package. The total disk space required is about twice the combined sizes of all the components of the package. The New Package wizard displays information about the amount of space needed and the locations where the space is needed.
- Workstation must be installed on a Windows host.

Overview of Creating and Deploying ACE Packages

The following is an overview of the tasks you must perform to create, deploy, and manage ACE instances.

1. With Workstation on a Windows host, create or clone a virtual machine that meets the requirements of your end users.

   The procedures are the same as for any virtual machine. For the network type, VMware recommends using Network Address Translation (NAT) or bridged networking with an IP address a DHCP server provides.
2. Make sure the virtual machine is powered off, display the summary view for the virtual machine, and click **Enable ACE Features** in the **Commands** list.

   ACE-specific commands are added to the **Commands** list in the summary view, and the **VM > ACE** menu is enabled.

3 Use the **VM > Settings** menu to configure the virtual machine.

(Optional) Use the ACE Options settings panel to associate the virtual machine with an ACE Management Server. You can then use the server to activate and track instances and make changes to policies, instance customization data, and other data for each ACE instance.

Because managed ACE instances check periodically for updates, the updates are dynamic. You do not need to create and deploy new update packages. See the *VMware ACE Management Server Administrator's Guide*.

4 Install a guest operating system, VMware Tools, and other software in the virtual machine.

The procedures are the same as for any virtual machine. See the *VMware Guest Operating System Installation Guide*.

5 Set policies for the ACE instance.

Policies control such things as what network access end users have from ACE instances and what devices on their host computers they may use in the instances. See Chapter 19, "Setting and Using Policies and Customizing VMware Player," on page 373.

6 Specify deployment settings for the ACE instance.

Deployment settings control such things as encryption, package lifetime, and security IDs. See Chapter 20, "Deploying ACE Packages," on page 417.

7 Create packages to deploy to end users.

Workstation guides you through the process. See "Creating a Package" on page 431 or Chapter 21, "Pocket ACE," on page 439.

8 Distribute packages to end users.

Distribute the packages on CD, DVD, or portable media, or make them available on a network. See "Deploy Packages" on page 438 or "Deploying the ACE Package on a Portable Device" on page 443.

9. Install ACE instances on end users' machines.

   See "Installing ACE Packages" on page 447 or "Run the Pocket ACE Instance" on page 445.

   You can install multiple ACE instances on the same machine. They can be from different vendors and be governed by different policies. You can also uninstall individual ACE instances or Workstation while leaving other ACE instances installed.

10. Keep users up-to-date.

    If you need to update the guest operating system, update a program running inside the ACE instance, or change policies set for the ACE package, you can create and distribute a new package.

Package updates do not upgrade the virtual machine version. You can use a package update to provide end users with VMware ACE 2.5 policies, but the update package does not update ACE Player or the virtual machine to version 2.5.

Overview of the ACE User Interface

Use any of the following methods to access the policy editor, deployment settings editor, and packaging wizards:

- Select the ACE-enabled virtual machine and choose a command from the **VM > ACE** menu.
- In the summary view for the ACE-enabled virtual machine, click an ACE-related command in the **Commands** list.

  The **ACE** tab in the summary view lists the current settings for policies and deployment.
- Click a button in the **ACE** toolbar.
- Right-click the ACE-enabled virtual machine in the sidebar and choose an ACE-related command.

ACE Management Server has two interfaces:

- In Workstation, select an ACE Management Server in the sidebar to display the instance view.
- Use the VMware Help Desk application. Because this interface is browser-based, you can use it from machines that do not have Workstation installed.

Both interfaces offer the same basic functionality. Administrators can view and control all managed ACE instances. An advanced search function allows you to locate instances in the database quickly. You can customize the interface by adding searchable custom fields. See the *VMware ACE Management Server Administrator's Guide*.

Troubleshooting Users' Problems

End users might need help with lost passwords, expired ACE instances, or copy-protected ACE instances that they have moved to a different location.

Use one of the following methods to fix those problems:

- **Managed ACE instances** – Use ACE Management Server. See the *VMware ACE Management Server Administrator's Guide*.

- **Standalone ACE instances** – Use the `vmware-acetool` command-line program to fix those problems directly on the users' machines. See "Using the vmware-acetool Command-Line Tool" on page 461.

  You can also use the hot-fix feature to respond to these problems. See "Setting Hot-Fix Policies for Standalone ACE Instances" on page 403 and "Respond to Hot Fix Requests" on page 463.

You might find it useful to modify the configuration of an ACE instance on an end-user's computer. Administrator mode enables you to access and use the virtual machine settings editor when running the ACE instance with VMware Player on the user's computer. See "Setting Administrator Mode Policies" on page 401.

Setting and Using Policies and Customizing VMware Player

19

This chapter describes how to set policies for an ACE-enabled virtual machine and customize the VMware Player interface for end users. This chapter includes the following topics:

Benefits of Using Policies

Policies give you control over many aspects of the ACE instances you distribute to end users. For example, you can set policies for the following security purposes:

- Permit the ACE instance to be used only by certain users and groups defined in an Active Directory domain.
- Specify which network resources end users may access from the virtual machine.
- Permit users to connect and disconnect certain removable devices configured for the virtual machine.
- Set an expiration date for an ACE instance.

You set policies with the policy editor. You can change some or all of the policies for an ACE instance at any time by editing the policies and creating and distributing a new package that contains only the policies.

For ACE-enabled virtual machines that ACE Management Server manages, you can dynamically change some policies and deploy those changes to the ACE instances on users' machines.

Set Policies for ACE Instances

Policy settings offer several levels of security for daily use of ACE instances. For information about the encryption aspect of security, see "Edit Deployment Settings" on page 417.

Before you can use the policy editor on a virtual machine, you must enable ACE features for that virtual machine. See "Overview of Creating and Deploying ACE Packages" on page 368.

To set policies for ACE instances

1. Select the ACE-enabled virtual machine and choose **VM > ACE > Policies**.
2. In the policy editor, select an item in the **Policy** list.
3. Complete the settings panel for that policy and either click **OK** or select another policy to edit.

   For assistance with the fields on a settings panel, click **Help**.

Setting Access Control Policies

Activation and authentication policies control access to installed ACE packages and the instances created from those packages. The activation policy specifies who can access an installed ACE package and turn it into an ACE instance. The authentication policy specifies who can run an ACE instance.

The settings you choose for these policies determine the default settings for package and encryption policies, which protect the ACE packages and files in transit. See "Encryption Settings" on page 418.

The settings for these policies and how they are implemented vary depending on how your ACE instances are managed and (optionally) tracked. The possible management setups are:

- **Server, with Active Directory** – ACE instances are managed by an ACE Management Server, and the server is integrated with Active Directory.

  An end user must enter Active Directory user credentials each time the ACE instance is run. Only the user who activates the instance can authenticate (run) the instance. The activation step is performed whenever an ACE package is installed.

- **Server, no Active Directory** – ACE instances are managed by an ACE Management Server, and the server is not integrated with Active Directory.

  The administrator chooses whether the end user must enter a password to activate the ACE instance and run it.

- **Standalone** – ACE instances are standalone, which means they are not managed by a server.

  The administrator chooses whether the end user must enter a password to activate the ACE instance and run it.

If you use ACE Management Server, the server also verifies the following items before the instance is allowed to run:

- The revocation flag is not set and the instance is not blocked from running because of any policy errors.
- The expiration date set for the instance, if any, has not been reached. See "Setting Expiration Policies" on page 383.

Create or Edit an Access Control Policy

After you enable ACE features for a virtual machine, you can create a policy to control which end users can access an installed ACE package and turn it into an ACE instance. This policy also controls which users can power on an ACE instance.

To create or edit an access control policy

1. Select the ACE-enabled virtual machine and choose **VM > ACE > Policies**.
2. In the policy editor, select **Access Control** and complete the fields in the settings panel.
3. Click **OK**.
4. Verify that the new settings appear correctly on the **ACE** tab in the virtual machine's summary view.

   If you change an activation setting, the policy takes effect when a new instance from this package is installed and activated. You can also edit an imported keyword list.
5. (Optional) To change the authentication setting from one type to another, create a policy update package and distribute it to the user.

Activation Settings

Use activation settings to control which users can activate an ACE instance after it is installed. The activation date is used for the expiration policy.

If you use ACE Management Server with Active Directory, the controls in the **Activation** section enable you to open the Active Directory Users and Groups dialog box. The machine on which Workstation runs must be in the same domain that which ACE Management Server is configured for. User-list changes are effective at the next startup of the instance.

If you do not use Active Directory or if you are creating standalone ACE instances, the settings panel includes the following options for activation passwords or keys:

- **None** – No password or key is required. Any user can activate this instance.
- **Password** – The user must enter the password that the administrator uses to activate this ACE instance. You must provide the user with the password through email or other means.

  For standalone ACE-enabled virtual machines, you set the password during the packaging process.

- **Activation key** – This option is available if you use ACE Management Server without Active Directory integration. You specify one or more keys and the end user must enter a key that is in that list.

  Activation keys are serial numbers (free-form strings) that can be tracked as used or unused by the server. You can enter the keys or import them from a text file.

  To import keys, you need a text file that contains the list of activation tokens. Each token is one line in the file. Blank lines are ignored.

  After an ACE instance is activated using a key, that key cannot be used to activate another instance. Removing a key from the list does not affect an instance that was activated with that key.

Authentication Settings

The authentication step is performed whenever the user runs the instance, unless **Authentication** is set to **None**.

If you use ACE Management Server with Active Directory, the controls in the **Authentication** section enable you to open the Active Directory Users and Groups dialog box. The machine on which Workstation runs must be in the same domain that which ACE Management Server is configured for.

If you do not use Active Directory or if you are creating standalone ACE instances, the settings panel includes the following options for authentication control:

- **None** – No password is required. Any user can run this instance after it is activated.
- **User-specified password** – The instance does not run until the user enters the correct password. Each user must set a password during activation, the first time the instance is powered on.

  You can create password policies to control such things as the minimum number of characters, types of characters, and number of password attempts before the user is locked out for a specified amount of time.
- **Script** – A custom authentication script is run to determine who can use the instance. See “Using an Authentication Script” on page 378.

Using an Authentication Script

You can create a custom authentication script that runs on the end user's computer to determine who can use the instance.

To require that the script be signed before deployment to prevent tampering, set a resource signing policy. See "Setting Resource Signing Policies" on page 384.

For instructions on creating and deploying the script, see "Specify a Script and a Command to Run It" on page 381.

Include a Power-On and Power-Off Script in the Package

You can provide a script that runs when an ACE instance powers on that determines whether the ACE instance can be run. You can provide a script that runs when an ACE instance powers off to reset any changes made to the host from a power-on script, reset authentication settings, or perform other procedures as the instance powers off.

To require that the script be signed before deployment to prevent tampering, set a resource signing policy. See "Setting Resource Signing Policies" on page 384.

The power-on or power-off script provides a customizable way of controlling access to an ACE instance in addition to the authentication policy.

To include a power-on and power-off script in the package

1 Create the script and save it in the `ACE Resources` folder.

2 On the access control policy page, select **Script** and click **Power-on/off scripts**.

3 Select one or both check boxes for the scripts you want to run.

4 Click **Set** to specify the path to the script and enter the command to run the script.

5 If you are enabling a power-on or power-off script after you deployed packages, provide an update package or a custom package for the `ACE Resources` directory.

When the script runs on the user's system, the script prints "`TRUE`" for power on or "`FALSE`" for power off. It must also conform to standard script exit code rules. The following is an example of a power-on script:

```
# VMware Sample Script
#
#   Sample script for ACE power-on hook
#
#   Description:
#   This sample script implements a power-on hook for ACE. This can be used
#   in addition to authentication to control the circumstances under which an
#   ACE is allowed to run.
```

```
#
#   This script assumes that the username is defined in the environment
#   variable TEST_USERNAME (a ficticious environment variable used for this
#   sample) and returns TRUE if the user is allowed to run, and FALSE
#   otherwise.
#
#   Input to script:
#   None.
#
#   Returns:
#   TRUE if username is on white list.
#   FALSE if username is not on white list or is undefined.
#
#   Expected output:
#   One of the strings "TRUE" or "FALSE"
#

my @white_list = ("alan", "bob", "mary", "sonia", "chris");

my $username = $ENV{TEST_USERNAME};
if (! defined $username) {
   print "FALSE";
   exit(0);
}

my @grepNames = grep(/$username/, @white_list);
if (@grepNames == 1) {
   print "TRUE";
   exit(0);
}

print "FALSE";
exit(0);
```

Scripts can be in any language. For example, you can use a `.bat` file on Windows operating systems or `perl` or `sh` on Linux operating systems. A script provides Workstation with a command-line executable file or a script file in the `ACE Resources` directory. The guidelines a script must follow depend on which policy the script is implementing.

The script must exit with a 0 (zero) value to be considered a success. Any other output results in failure. Upon success, the `stdout` output of the script is examined. For a given policy, this should be a specific value such as TRUE or FALSE. For a power-on script, output should be TRUE or FALSE. The authentication script output is used as a password. The host to guest data script is a string in a particular format such as `guestinfo.var1="value1"\nguestinof.var2="value2"`.

Set a Recovery Key for Encrypted ACE Instances

You can specify the key to be used for access to encrypted ACE instances. This key enables you to reset the password for a deployed ACE instance.

To set a recovery key for encrypted ACE instances

1 On the access control policy page, click **Recovery key**.

2 In the Recovery Key dialog box, select **Use recovery key**.

3 Do one of the following:

- To use an existing PEM-format key pair, click **Browse for Existing Key** and navigate to the public key of the pair to use.
- To create a PEM-format key pair, click **Create New Recovery Key** and complete the dialog box that appears.

4 Click **OK** to generate the keys.

After several seconds, the newly generated public key is listed in the field on the **Recovery Key** tab. The two parts of the key are stored in the location you indicated, with the names you specified followed by the extensions `.pub` for the public key and `.priv` for the private key.

5 Record the private key password and location of the private key file so that you can supply it if you need to reset a password.

Set Activation Limit

The activation limit is the maximum number of ACE instances that can be activated from the specified ACE-enabled virtual machine. This option is available if you use ACE Management Server.

To set an activation limit

On the access control policy page, under **Activation limit**, in **Total number of activations,** choose how many instances can be activated from this ACE-enabled virtual machine.

You can use the drop-down list or type in a number.

Active Directory Password Change Proxying

You can provide additional security for your ACE instances by integrating with Active Directory.

You can specify password expiration and change requirements, set up the domain to expire passwords, and require password changes periodically. These settings are in addition to ACE access control policy settings.

In cases in which Active Directory users need to change their passwords, you can configure ACE Management Server as an Active Directory password change proxy. In this mode, ACE Management Server makes the password change request to the Active Directory domain controller on the user's behalf.

Setting Host to Guest Data Script Policies

You can provide a host to guest data script that runs when the ACE instance is powered on. It passes values to the guest. Use this policy setting to share specific host information with the guest operating system when the ACE instance is powered on.

The script, which runs on the host, should output a set of key-value pairs, which become available to the applications that are running inside the guest. The VMware Tools service provides this ability. The set of acceptable keys consists of `machine.id` and keys prefixed with `guestinfo`, such as `guestinfo.ipAddress`.

If the ACE-enabled virtual machine for this instance is configured for both Windows and Linux platforms, you can provide scripts for both Windows and Linux systems.

Changes to a script require that you deploy an update package that includes the new script.

For instructions on creating and deploying the script, see "Specify a Script and a Command to Run It" on page 381.

Specify a Script and a Command to Run It

The procedure for using authentication scripts and host-guest data scripts is identical.

Use this procedure for the following scripts:

- **Access control authentication script** – Custom authentication script that runs on the end user's computer to determine who can use the ACE instance.

  If you plan to use the script with a Pocket ACE that will run on both Windows and Linux hosts, make sure that the script outputs on both platforms are exactly the same, including characters for line endings or new lines.

- **Host-guest data script** – Script for sharing host information such as the host machine ID and IP address with applications that run on the guest.

To specify a script and a command to run it

1. Create the script and save it in the `ACE Resources` directory inside the virtual machine's directory.
2. In Workstation, select the ACE-enabled virtual machine and choose **VM > ACE > Policies**.
3. In the policy editor, do one of the following:
   - If the script is a custom authentication script, select **Access Control** and in the **Authentication** section, select **Script** and click **Set Script**.
   - If the script is for passing host information to the guest, select **Host-Guest Data Script**, select **Run a host-guest script at power on**, and click **Set**.
4. In the dialog box that appears, browse to the script file and click **Open**.

   If the deployment platform setting in the deployment settings editor is set to **Both Windows and Linux**, this dialog box contains text fields for both Windows and Linux.
5. Type the command for running the script.

   Include the script file in the command line, as well as any needed executable file for running the script and any arguments to the script.
6. (Optional) Select **Timeout** and type a timeout interval in seconds, in case the script does not run to completion.

   The user is denied access if the timeout interval elapses before the script runs to completion.
7. Click **OK**.
8. If you are enabling this script for an ACE-enabled virtual machine that you already deployed, do one of the following:
   - For standalone instances, include the script in the update package you distribute to end users.
   - For managed instances, use a policy and server update package or a custom package that includes the `ACE Resources` directory to provide end users with the script.

Setting Expiration Policies

Expiration policies are useful, for instance, if you want to prevent a contract employee from using a virtual machine past a certain date or for more than a certain number of days.

When an instance expires, the files remain on the user's computer, but the instance cannot be used. This way, the user can request an extension to the expiration date.

If you specify a date range, the instance can be powered on and run no earlier or later than the start and end dates. You can deploy ACE instances with expired date ranges.

You can also set and customize a warning message that appears each time an instance powers on as the expiration date approaches. An expiration message appears when the instance expires and the instance can no longer be powered on.

A standalone ACE instance has the same expiration policy as all instances created from the corresponding ACE package. The fixed expiration date or the fixed date range is established at activation time. Each time the user powers on the instance, the date or date range is checked. Expiration checks are also performed while the instance is running. If the expiration is reached, an expiration message appears and the instance is suspended.

With a managed ACE instance, the expiration policy works similarly as for standalone instances, but the expiration policy value can be specified for individual instances. A valid date range for an ACE-enabled virtual machine applies to each of its associated ACE instances until an instance is individually configured with its own date range. After that configuration, any changes to the ACE-enabled virtual machine's expiration policy do not affect the instance. All expiration values, both for ACE-enabled virtual machines and for all ACE instances, are dynamic. This means that after you change the value and publish the policy update to ACE Management Server, ACE instances get the new value the next time they check for policy updates.

Setting Copy Protection Policies

Copy protection policies ensure that an ACE instance runs only from the location where it was originally installed. If you copy-protect an ACE instance, its files can be moved or copied, but the instance cannot run from the new location.

For standalone ACE instances, you can specify whether copying and moving are allowed. For managed ACE instances, you can specify whether both copying and moving are allowed or whether only moving is allowed. In this case, only one copy of the ACE instance is allowed to run at a time.

If the user moves or copies a copy-protected ACE instance and tries to run it, an error message appears. It lists an alphanumeric string that the user can send to the system administrator or help desk assistant to get the copy protection changed.

For managed instances, you can also dynamically change the copy protection settings, switching the settings so that moved or copied instances will run or not run.This means that after you change the value and publish the policy update to ACE Management Server, ACE instances get the new value the next time they check for policy updates.

Every ACE instance has a copy protection identifier (CPID) that contains the path to the ACE instance on the host file system. For standard ACE instances, the CPID also contains the system's BIOS ID. For Pocket ACE instances, the CPID contains the file system ID. If copy protection is on, Workstation compares the current CPID with the stored CPID. If they do not match, the instance was moved or copied.

For standalone ACE instances, you can set the CPID by using `vmware-acetool` or by sending hot fixes (on Windows systems, if hot fixes are enabled). See "Using the vmware-acetool Command-Line Tool" on page 461 and "Respond to Hot Fix Requests" on page 463.

For managed ACE instances, the CPID is stored on the server and the administrator can update it. See the *ACE Management Server Administrator's Guide*.

Setting Resource Signing Policies

You can set the resource signing policy so that an ACE instance cannot be run if resource files, such as policy scripts or custom EULA text files, are tampered with.

A resource is considered any file in the `ACE Resources` subdirectory in the virtual machine directory on the Workstation host. Files that are put in this directory on the end user's machine are not resources in this sense and are not signature checked.

Signature checking is performed on the end user's machine at power on and then every time a script is run. You can specify whether to verify all files in the `ACE Resources` directory or just the policy scripts in that directory.

If you are creating a package that has substantial resources, such as large files or large numbers of files, signature checking might take a long time. In this case, consider verifying scripts only or not using resource signing.

NOTE If you set the encryption package setting options to **None**, any verification specified in the resource signing policy is not performed. The encryption package setting overrides the resource signing policy. See "Encryption Settings" on page 418.

Setting Network Access Policies

The network access feature uses a packet-filtering firewall to enable you to specify which machines or subnets an ACE instance or its host system may access. This means that you can, for example, configure the instance so that it is allowed to connect only to your VPN server, which then controls access to other resources.

You can also customize the network access settings to filter on the basis of network addresses, traffic direction, protocol, and ports. You can set the following types of network access restriction definitions:

- Network zones
- Network access for the ACE instance's host machine (also known as "host network access")
- Network access for your ACE instance's guest operating system (also known as "guest network access")

Network access policies can be dynamic if the ACE instance is associated with an ACE Management Server. This means that after you publish a policy update to ACE Management Server, ACE instances get the new policy the next time they check for policy updates. You can quickly lock ACE instances out of all or part of your network to help combat the spread of a worm or virus without deploying update packages. See the *VMware ACE Management Server Administrator's Guide*.

Before You Begin Setting Host Policies

Use the following guidelines as you plan network access policies:

- A host machine for ACE instances can have only one host policy file. If you try to install an ACE package with a host policy file on a machine that already has a different host policy file, installation of the new package fails.
- A host policy is in effect even when no ACE instances are running. The policy starts immediately after installation and starts working every time the host system boots.
- Any restrictions on the host's network access also restrict network access for an ACE instance that uses NAT networking, because the NAT connection is affected by all the policies you apply to the host. If you set up restricted host access by using the ACE ruleset editor and rules editor rather than the Network Access wizard, configure the ACE-enabled virtual machine's virtual NICs to use bridged networking.
- If you are setting up a managed ACE-enabled virtual machine, you must allow the host to access ACE Management Server, communicating through TCP over the appropriate port that you configure.

- Host policies do not apply to Pocket ACE instances. If you specify a restricted host policy for an ACE-enabled virtual machine and then create a Pocket ACE package with that ACE-enabled virtual machine, the package is created but the host policy is not included in the package.
- You cannot view changes to host policies in the preview mode. If you want to test the effects of such changes, you must perform a test deployment. See Chapter 20, "Deploying ACE Packages," on page 417.

Use the Network Access Wizard to Configure Network Access

VMware recommends that you use the Network Access wizard to configure basic settings and then use the zone editor and ruleset editor to fine-tune the settings if necessary. The Network Access wizard is initiated when you click **Quick Setup**.

The Network Access wizard creates or changes rules for the following zones:

- If you choose the **Desktop Configuration** option, the wizard creates a new guest access ruleset for the Everywhere zone. This ruleset restricts ACE instance access to your VPN or other specified network hosts.
- If you choose the **Laptop Configuration** option, the wizard creates a new internal zone that restricts the network address and, optionally, the domain on which the ACE instance can run. It can also create a new host access ruleset for this zone to restrict access to the internal network. For example, you can specify a proxy server. Finally, you can configure the same remote access as for the **Desktop Configuration** option.

  If you use this option and you do not modify any of the default settings that the wizard provides, the host is still allowed to communicate with DNS and DHCP servers so that the zone-detection mechanism can function properly.

To use the Network Access wizard to configure network access

1. In the policy editor, select **Network Access**.
2. Select **Restrict network access of the ACE instance and/or its host** and click **Quick Setup**.
3. Complete the wizard.

   Depending on which configuration type you choose, a new zone might be added to the Network Access settings panel, and new rulesets might appear in the **Host Network Access** and **Guest Network Access** columns in the table.
4. (Optional) To view or edit the zones or rulsets you created with the wizard, click the zone or ruleset name in the table on the Network Access settings panel.

When you use the Network Access wizard to create an internal zone, choosing the **Laptop Configuration** option enables you to specify the network address, domain, and subdomains. If you want to also configure DNS, DHCP, WINS, or gateway servers, use the zone editor. See "Guidelines for Specifying Zone Conditions" on page 387.

Guidelines for Specifying Zone Conditions

Zone conditions describe the characteristics of a network zone. Workstation examines the networks that are directly connected to network adapters on the host computer to see if a match exists for all the criteria for any adapter in any of the zone definitions.

The zone editor appears when you click a name in the Zones column of the Network Access policy page. It shows the following details about the zone:

- You can specify a zone by using up to six conditions:
  - Domain
  - Subnet
  - DNS servers
  - DHCP servers
  - Gateway servers
  - WINS servers

  For a match to occur, all specified conditions must be met.
- All zone conditions except the domain condition allow users to specify a list of addresses. The match is made if the host's address matches any of the address-list entries in a specified condition.

When the host connects to a network, a check is performed to determine whether the network matches the conditions for a zone. The checking starts with the topmost zone in the table and continues down the table until a match is made or the Everywhere Else zone is reached. When a match is made, the zone checking stops and filter rules for that zone are applied.

There are trade-offs between using shorter and longer lists of conditions. If you use a longer list, you minimize the chances of a false-positive result or a misidentification. Minimizing the chance of a false-positive result or a misidentification can be important if you are providing an ACE package to someone who connects a host computer to multiple networks at different times. If one of the other networks matches the characteristics you define in the zone definition, the host and instance access policies are applied, even if the host is not connected to your network.

In some cases, however, using a longer list might also increase the likelihood that a user could circumvent the detection mechanism. For example, such an error might be made if you switch the host to use a static IP address instead of DHCP and configure the host with only a subset of the characteristics defined for your zone, such as only network address, or network address and DNS server information.

Also consider that the addresses or names of certain servers can change over time. Such changes can also introduce detection issues.

Using a smaller set of information in a zone description, such as only the network address and the subnet mask, is safer. The disadvantage is that it increases the chance that a false positive or misidentification can occur. Such false positives are especially likely if your network is using a common netblock, such as 10/8, 172.16/12, or 192.168/16, that is also used by other networks.

Descriptions of the Zone Condition Settings

Each zone description must contain one or more of the following setting options describing the conditions of the zone:

- **Domain** – Specifies the domain name of the network, such as `mycompany.com.` Enter only one domain name. The value of **Allow subdomains of this domain** governs the interpretation of this option.
- **Allow subdomains of this domain** – Modifies the **Domain** option. It specifies whether, for the **Domain** zone condition to be met, a domain name must exactly match the domain name specified in the **Domain** box or whether a match of the domain name is made any time the string contains `<domain_name>.` For example, if this option is selected, `corp.mycompany.com` is considered a match for `mycompany.com`. If this option is not selected, `corp.mycompany.com` is not considered a match for `mycompany.com`.
- **Network address** – Specifies an IP address or subnet range that the network uses. The value of `<subnet>`, if you include a subnet range, must be the number of bits in the netmask. A network adapter matches this condition if it is using an IP address that lies within any of the specified ranges.
- **DNS servers** – Specifies one or more IP addresses or host names for DNS servers on the network. A network adapter matches this condition if it is using at least one of these servers.

  If the value of the **Match at least** option is greater than `1`, the host must be using the specified number of DNS servers on the list before a network adapter is considered to be on the defined network.

Because multiple methods exist for assigning DNS domain names to a Linux host, using just the DNS domain name to define a zone can be error prone. To define a zone for a Linux host, use criteria in addition to the DNS domain names.

- **DHCP servers** – Specifies one or more IP addresses or host names for DHCP servers on the network. A network adapter matches this condition if it is using at least one of these servers.
- **Gateway servers** – Specifies one or more IP addresses or host names for default gateways on the network. A network adapter matches this condition if it is using at least one of these gateways.
- **WINS servers** – Specifies one or more IP addresses or host names for WINS servers on the network. A network adapter matches this condition if it is using at least one of these servers. Linux hosts ignore WINS server settings during zone detection.

  If the value of the **Match at least** option is greater than 1, the host must be using the specified number of WINS servers on the list before a network adapter is considered to be on the defined network.

Add or Edit a Network Zone

Use the zone editor to configure the network address, domain, DNS, DHCP, WINS, or gateway servers that an ACE instance can use for network connections.

Before you open the zone editor, determine what criteria to use for connecting to internal and external networks. See "Guidelines for Specifying Zone Conditions" on page 387 and "Descriptions of the Zone Condition Settings" on page 388.

To add or edit a network zone

1. In the policy editor, select **Network Access** and do one of the following:
   - To add a zone, click **Add Zone** and click the **New Zone** entry that appears in the table.
   - To edit a zone, click the name of the zone in the Zones column of the table.
2. Complete the fields in the zone editor that appears and click **OK**.

Using the Ruleset Editor to Configure Host and Guest Access

Each access setting for the ACE instance's host machine and for the ACE instance's guest system is based on a set of access rules. Whenever you use the Network Access wizard, a default ruleset is used for host and guest network access. You can use the ruleset editor to change the parameters of those rules.

Network access policies are applied by filtering on the IP address, the protocol number from the IP header, the direction of traffic, and TCP and UDP port values. The filtering does not involve deep packet inspection. For DNS and DHCP access, the TCP and UDP ports on which those services traditionally reside are opened.

Note the following aspects of the filtering actions:

- If you move your services to different ports, the network access rules for those services no longer work.
- The host or instance is open to all traffic on these protocols and ports.

To understand the particulars of how traffic is being blocked or allowed for DNS, DHCP, and ICMP protocols and ports, see the rules displayed in the ruleset editor.

Add or Edit Rulesets and Rules for Network Access

The rules in the ruleset editor are listed in the order in which they are to be evaluated. When a network traffic packet arrives or is to be sent from the host or guest, it is compared with each rule in the ruleset, in order from the top down. If the following packet settings match the rule conditions, the packet is allowed or blocked according to the rule's action:

- Source address for incoming packets
- Destination address for outgoing packets, protocol, and ports

The packet is compared to each rule in order until it matches a rule or it was compared with all of the rules. When a match is made, the packet-to-rule comparison ends. The packet is not compared to subsequent rules in the ordered list. If it was compared to all rules without a match, the default rule action is applied.

To add and edit rulesets and rules for network access

1. In the policy editor, select **Network Access** and click the link in the table column that applies to the access setting to edit.

   The Zone and Access Type information just below the **Ruleset Name** text box shows the name of the zone and whether the access setting applies to host network access or to the network access for ACE instances (guest access).

2. Use the ruleset editor to change the order of rules in the set, edit rules, and specify whether the host or guest is allowed to use DNS, DHCP, or ICMP.

   By default, **DNS**, **DHCP**, and **ICMP** are included in the network access setup for both host and instance access. VMware recommends that you keep **DHCP** and **DNS** selected because they are important for zone detection.

   Whether the following settings apply to the host or to the ACE instance (guest access) depends on whether you are editing a host network access ruleset or a guest network access ruleset:

   - **DNS** – Allows the guest or host to use a DNS server to resolve IP addresses. Select this option if the DNS server is not included in any other network access setting for this host or ACE instance.
   - **DHCP** – Allows the host or guest to obtain its IP address from a DHCP server. Select this option if the DHCP server is not included in any other network access setting for the host or ACE instance.
   - **ICMP** – Enables you to use the `ping` command. For guests, `ping` enables you to check network connectivity to and from the ACE instance. For hosts, it enables you to check network connectivity with other hosts in the network and with the ACE instance.

3. (Optional) To add or edit a rule, do one of the following:

   - To change a specific rule's settings, click the row for that rule in the table in the ruleset editor and click **Edit**.
   - To add a rule, click **Add**.

4 (Optional) Use the Rule Editor dialog box to specify the type of traffic, whether to block or allow traffic from specified network locations, the protocol, and ports or port ranges.

- **Addresses** – To edit an existing host name or address, double-click that item and edit it. The wildcard setting for all IP addresses is 0.0.0.0/0.
- **Protocol** – To allow or block communication for a specific protocol, select **Custom** from the **Protocol** list. The protocol number is in the packet. If that number matches the number supplied in the **Custom** field, the packet is allowed or blocked as the rule specifies. The protocol number is used in the protocol field of IPv4 packets.

  For a list of protocol numbers, see the Internet Assigned Numbers Authority (IANA) organization's Web site. Most protocol numbers are permanently assigned.
- **Remote Ports** and **Local Ports** – If you are using either TCP or UDP and want to qualify the rule with specific port numbers for this type of traffic, type the port numbers or port-number ranges.

  The wildcard port setting is "" (double quotation marks).

  Usually you specify filtering on either local or remote ports, not both, because both specifications have to match for the rule to be applied. (DHCP represents an exception to this general rule.)

  The local port is the source port for outgoing packets and the destination port for incoming packets. Typically you specify a local port when the host or guest is being used as a server obtaining remote connections on some port.

  The remote port is the source port for incoming packets and the destination port for outgoing packets. Typically you specify a remote port when the host or guest is a client and is contacting a remote server on some port.

Change NAT Settings

You can use the NAT feature of the network access policy to specify the IP address range for the virtual network VMnet8 on the ACE instance's host system. You deploy this network properties setting with the ACE package.

CAUTION If you set this property, the setting affects all of the ACE instances and virtual machines on this instance's host system.

To change NAT settings

1. In the policy editor, select **Network Access**.
2. Click **Host Virtual Network** on the policy page.
3. In the NAT section of the dialog box, select **Assign IP addresses from this subnet**.
4. Type the subnet IP address to use, enter zero (0) as the last byte in the address, and click **OK**.
5. Create an ACE package and deploy the package.

   The NAT setting is not a dynamic policy setting. This means that simply publishing a policy update to ACE Management Server does not cause ACE instances to change NAT settings. You can change the setting for a deployed ACE instance only by changing it in the policy and then creating and deploying a new ACE package.

Configure Which Physical Network Adapter to Use

If the host is likely to have multiple network adapters, you can specify which one to use for a bridged network connection. For example, you can specify that only the wireless adapter or only a VPN is to be used.

CAUTION If you set this property, the setting affects all of the ACE instances and virtual machines on this instance's host system.

To configure which physical network adapter to use

1. In the policy editor, select **Network Access**.
2. Click **Host Virtual Network** on the policy page.
3. Select one of the radio buttons in the **Automatic Bridging** section.
4. If you select **Device name**, also enter part or all of the device name.

   For example, if device name of the local area connection is Broadcom NetXtreme 57xx Gigabit Controller #2, you might enter **`Broadcom`** or **`broadcom netxtreme`**. On Windows hosts, to determine the device name, go to the **Network Connections** item in the Control Panel.
5. Click **OK**.
6. Create an ACE package and deploy the package.

   This automatic bridging setting is a host policy, which means that you can change the setting for a deployed ACE instance only by changing it in the policy and then creating and deploying a new ACE package

Understanding the Interaction of Host and Guest Access Filters with Tunneling Protocols

Host and guest access filters can differ in their interactions with tunneling protocols.

A host network access filter sees traffic before packets are encapsulated in the tunneling protocol (for example, VPN). A guest network access filter sees traffic after the packets are encapsulated in the tunneling protocol.

Because of this guest access filter behavior, a user might be able to circumvent guest access restrictions by using tunneling protocols or proxies.

Updating a Network Access Policy

You must create and deploy a new package in order for the host policy to take effect.

If you use a managed ACE-enabled virtual machine to create packages that do not contain a host policy and later edit the ACE-enabled virtual machine's network access policy to include a host policy and publish the change, instances created from packages of that ACE-enabled virtual machine do not have a host policy applied. A warning appears on the network access policy page if you attempt to apply a host policy in this way.

You can package just the host policy in a custom package, keeping the package size small.

Setting Removable Devices Policies

Removable devices policies allow you to control whether users can connect and disconnect removable devices from their ACE instances.

A removable devices policy is applied to an ACE-enabled virtual machine and affects all users of all instances created from that ACE-enabled virtual machine.

When you select **Removable Devices** in the policy editor, all removable device types for this ACE-enabled virtual machine are displayed in a list. You can specify which devices to allow end users to access.

Setting USB Device Policies

You can set USB device policies to restrict the ACE user's access to USB devices. The policies are dynamic. This means that you can change the settings on deployed ACE instances by publishing a policy update to ACE Management Server.

Access Levels for USB Devices

You can set restrictions at various levels of specificity, and you can mix levels of restriction in a policy setting. The levels of restriction are:

- **Specific USB device** – For example, allow use of a specific type of digital camera but disallow use of iPod mobile digital devices.

  If a rule exists for a specific device, that rule overrides any rules set for device classes in which the device belongs.

  All entries in the list of specific USB devices are maintained in a device database that is included with the files for this ACE-enabled virtual machine. You can copy and share the database. It is not write-protected. The default location for the file is:

  ```
  C:\Documents and Settings\All Users\Application Data\VMware\VMware
                 Workstation\usbhistory.ini
  ```

- **Device class** – For example, allow use of human input devices (HIDs), such as mice and keyboards, but disallow use of communications devices, such as modems and cell phones.

  If no specific device rule exists for a device and more than one device class rule applies to that device, the most restrictive rule is applied. For example, a device might include both a fax function and a print function and therefore can belong to more than one class. If one rule blocks a fax device but another rule allows a print device, the combination fax and print device is blocked.

- **All USB devices** – Allow or deny access to all connected USB devices. Device class rules and specific device rules override general access rules.

Set an Access Policy for USB Devices

You might want to set a policy that prevents end users from connecting such USB devices as mass storage devices, printers, or modems to the ACE instance.

Before you use the policy editor, determine a strategy for setting the policy. If you want a restricted environment, you can plan to generally block access to all USB devices and then specify exactly which classes or specific devices to allow. See "Access Levels for USB Devices" on page 395.

To set an access policy for USB devices

1. In the policy editor, select **USB Devices**.
2. Use the **General access to all USB devices** radio buttons to specify whether to allow or block general access to USB devices.

3 To specify a USB policy by device class:

   a If the device does not appear in the **Access to specific types of USB devices** list, click **Add**, select the device in the USB Device Classes dialog box, and click **OK**.

   You can Ctrl-click and Shift-click items to select more than one class.

   b Use the **Allow** and **Block** check boxes in the **Access to specific types of USB devices** list to specify the rule for each device in the list.

4 To specify a USB policy by specific device:

   a If the device does not appear in the **Access to individual USB device models** list, click **Add**, select the device in the USB Device List dialog box, and click **OK**.

   If the device does not appear in the USB Device List dialog box, do one of the following:

   - Connect the device to the host and click **Refresh**.
   - Determine the device's vendor ID (VID) and product ID (PID) and click **Manual Add** to enter the information. This information is available from the Windows Device Manager when you connect the USB device to a Windows computer.

   b Use the **Allow** and **Block** check boxes in the **Access to individual USB device models** list to specify the rule for each device in the list.

   c (Optional) To change the information for a device, click **Remove** and add the device again with the new information.

5 Click **OK** in the policy editor.

Setting Virtual Printer Policies

VMware ACE includes a virtual printer that allows users to print to any printer available to the host computer without installing additional drivers in the virtual machine.

The virtual printer feature is available for ACE instances running with these Windows host and guest operating systems:

- Host – Windows 2000, XP, 2003, or Vista, 32-bit only
- Guest – Windows 2000, XP, 2003, Vista (32- and 64-bit), Red Hat Enterprise Linux 4 (32 bit only), Ubuntu, and SUSE

After you enable the virtual printer policy, a serial port is added to the virtual machine. This serial port appears on the **Hardware** tab of the virtual machine settings editor, with the summary **Used by Virtual Printer**. You cannot add or remove this serial port by using the virtual machine settings editor. To add or remove it, you must enable or disable the option in the virtual printer policy.

NOTE If the ACE-enabled virtual machine already has four serial ports, you cannot add another serial port for the virtual printer. To enable the virtual printer, delete an existing serial port.

After end users install the ACE instance, they can use the **VMware Player > Virtual Printers** menu command to specify which printers from the host are available to the guest. If end users on Windows hosts have problems, make sure the TP AutoConnect Service Windows service is started.

Setting Runtime Preferences Policies

You can set options on the Runtime Preferences policy page to specify which Workstation runtime attributes the user can choose.

Runtime Preferences Settings

Use the following information to decide which features to enable:

- **Always run in full screen** – VMware Player fills the full screen when it starts, hiding the host operating system. You might find this useful, for example, to avoid confusion about the differences between the host system environment and that of the ACE instance.

  Users can return to the host operating system by clicking the minimize button on the toolbar. If the mouse pointer is not available, pressing Ctrl+Alt minimizes the display.

- **Always hide the full screen toolbar** – End users cannot display the toolbar that usually appears at the top of the screen when in full screen mode.

- **Always run in appliance view** – The ACE instance opens in appliance view and the user cannot change to console view.

  To use this setting, you must also enable appliance view for the virtual machine. See "Configure the Appliance View for a Virtual Machine" on page 170. If you attempt to use this policy without enabling appliance view, an error message appears when the user attempts to start the ACE instance.

- **Allow users to modify the memory allocation** – The **Change Memory Allocation** command will appear in the **VMware Player > Troubleshoot** menu of VMware Player.
- **Reduce virtual machine memory size if needed when powering on** – The virtual machine powers on even if the amount of available memory is less than the amount configured for the virtual machine. If you do not use this feature and the required amount of memory is not available, users need to modify the memory allocation to power on the virtual machine.

Enhanced Virtual Keyboard Settings

Use the following information to decide which features to enable:

- **Require enhanced virtual keyboard for secure input** – This setting applies only to Windows hosts running Windows guests. This feature provides better handling of international keyboards and keyboards with extra keys. It also provides security improvements because it processes raw keyboard input as soon as possible, bypassing Windows keystroke processing and any malware that is not already at a lower layer.

  If an ACE instance uses this feature, when end users press Ctrl+Alt+Delete, the guest system only, rather than both guest and host, responds to the command.

  Before you create a runtime policy for this feature, turn on the enhanced keyboard filter with the virtual machine settings editor. See "Use the Enhanced Virtual Keyboard for Windows Hosts" on page 323.

  When the ACE instance is installed and the guest operating system starts for the first time, a special keyboard filter driver is installed on the host. After installation, the end user must restart the host computer. Keyboard filtering is then enabled.

- **When a suspected keylogger is detected** – Keystroke logging is a method of recording user keystrokes, including determining user passwords. VMware ACE now includes a feature that can detect (but not disable) keyloggers.

  If you select **Ask user**, end users can exit or continue using the virtual machine and only log that the keylogger was detected. If you allow end users to continue using the virtual machine when a keylogger is detected, the keylogger still records the users' keystrokes. To avoid this possibility, select **Exit**.

Exit Behavior Settings

Use the following information to decide which features to enable:

- **When closing a non-Pocket ACE instance** – If you select **User Preference**, the user has access to **Suspend** and **Power off** in the Preferences dialog box in VMware Player (**VMware Player > Preferences**). If you select one of the other choices, the end user's virtual machine is suspended or powered off when the user chooses **VMware Player > Exit** or clicks the close box in VMware Player.
- **When closing a Pocket ACE instance** – If you select **User Preference**, the user has access to **Go mobile** and **Ask to go mobile or stay connected to the computer** in the Preferences dialog box in VMware Player (**VMware Player > Preferences**).
    - **Always Go** – The virtual machine is powered off and synchronized to the host. After synchronization, the user can unplug the USB device and use it in another machine.
    - **Always Stay** – The user wants to exit VMware Player but does not want to unplug the device. The virtual machine is suspended and no synchronization occurs.
    - **Always Discard** – The user wants to exit VMware Player but does not want to synchronize. All changes are lost.
- **Allow users to manually power off or reset the virtual machine –** The **Reset** and **Power off and Exit** commands will appear in the **VMware Player > Troubleshoot** menu. If you do not select this option, the user must exit VMware Player to power off or suspend the ACE instance.

Pocket ACE Cache Settings

For performance reasons, when you use Pocket ACE, files from the USB device are cached as needed on the host. When you are finished using the Pocket ACE, you synchronize changes so that the updated files are written to the USB device.

You can disable this caching if you do not have enough disk space on the host. For example, if the virtual disk on the Pocket ACE has 8GB, you might potentially need 8 GB of disk space on the host for caching. You can also disable caching for security reasons if you do not want to create a cache on the host.

If you disable caching, the exit behavior in the **When closing a Pocket ACE instance** list changes to **Always Go** but synchronization does not occur because it is not necessary.

Setting Snapshot Policies

You can set policy options for two types of snapshots:

- **Reimage snapshots** – At installation time, a snapshot is taken after all of the required instance setup steps are complete, including, if applicable, encryption, instance customization, and domain join. The snapshot is taken before the virtual machine runs for the first time.

  NOTE Manually disable the automatic reimage snapshot by editing the ACE-enabled virtual machine's `aceMaster.dat` file. Edit the `packaging.takeReimageSnapshot` option.

  Reimage snapshots allow the ACE administrator, or the user if the administrator enables reimage snapshot options for the user, to revert the ACE instance to its known good starting state or to the known good updated reimage state.

  If you enable reimage snapshot options, commands for the options appear in the **VMware Player > Troubleshoot** menu.

  If you choose not to enable the reimage snapshot options for the user, you can replace the reimage snapshot or revert to it on the user's machine by providing administrator mode access through the Administrator Mode policy. See "Setting Administrator Mode Policies" on page 401.

- **User snapshots** – You can enable users to take a snapshot of the ACE instance either when the instance is running or immediately after powering it off. You can also enable them to delete that user snapshot.

  User snapshots enable the user to return the virtual machine to a known stable state. User snapshots can be taken, reverted to, and deleted without affecting the reimage snapshot. Only one user snapshot can be saved at a time.

  If you enable user snapshot options, commands for the options appear in the **VMware Player > Snapshot** menu.

NOTE You cannot take snapshots of a Pocket ACE instance. For more about Pocket ACEs, see Chapter 21, "Pocket ACE," on page 439.

Setting Administrator Mode Policies

You can use the administrator mode policy to set an administrative password so that you can do any of the following:

- Run the ACE instance on the user's machine and enter administrator mode to access the virtual machine settings and make changes to the instance's configuration (on Windows systems only). You can only edit the settings. You cannot add or remove virtual hardware devices.
- Run the ACE instance on the user's machine and enter administrative mode to access all the snapshot commands. See "Setting Snapshot Policies" on page 400.
- Use the `vmware-acetool` command-line program on an ACE user's system to fix a limited set of problems for standalone ACE instances.

Use Administrator Mode on an ACE Instance

Using administrator mode on an end user's virtual machine enables you to troubleshoot and access features and commands that might not be available to the end user.

To use administrator mode on an ACE instance

1 Start VMware Player on the end user's machine and choose **VMware Player > Troubleshoot > Enter Administrator Mode.**

2 Enter the password for administrator access.

3 Choose the appropriate commands as follows:

   - To edit virtual machine settings from the user's machine, choose **VMware Player > Troubleshoot > Virtual Machine Settings**. This command is available only on Windows hosts.
   - To use the user snapshot commands, choose **VMware Player > Snapshot**.
   - To use the reimage snapshot commands, choose **VMware Player > Troubleshoot > Revert to Reimage Snapshot**.
   - To use the ACE Tools, see "Using the vmware-acetool Command-Line Tool" on page 461.

4 When you finish changing virtual machine settings or using the snapshot commands, choose **VMware Player > Troubleshoot > Exit Administrator Mode**.

Setting Kiosk Mode Policies

When an ACE instance runs in kiosk mode, the user cannot access the host system at all. For example, the user cannot shut down the host machine. The virtual machine runs in full screen mode and does not display the ACE menu bar or ACE Player online help.

If an ACE instance has the kiosk mode policy turned on, by default, a message appears at startup to provide the following information:

- Warns the user that the virtual machine is about to go into kiosk mode.
- Tells the user which key combination to use to exit kiosk mode. The default is the hot-key combination for ungrabbing input from a virtual machine (often Ctrl+Alt). See “Change the Key Combination for Exiting Kiosk Mode” on page 402.
- If the policy includes an administrator password, tells the user that host access is available only if the user enters the password after pressing the key combination to exit kiosk mode.

When a user exits kiosk mode, the virtual machine is powered off or suspended, according to the runtime preference policy for exit behavior. Pocket ACE instances are powered off and synchronized. When the virtual machine is powered off, the ACE Player prompts the user to exit kiosk mode.

On Linux hosts, you must set some additional properties after installing the ACE instance. See “Prepare a Linux Host for Running in Kiosk Mode” on page 454.

For information about startup options for kiosk mode, see “Change Default Kiosk Mode Startup Behavior” on page 457 and “Use Multiple Virtual Machines in Kiosk Mode” on page 458.

Change the Key Combination for Exiting Kiosk Mode

You can use Ctrl, Alt, Shift, the Windows key, or a combination of these keys with a regular key.

To change the key combination for exiting kiosk mode

1. In the policy editor, select **Kiosk Mode**.
2. Select **Always run in kiosk mode** and select **Custom hot key to exit kiosk mode**.
3. Click in the **Type hot key here** field and press a key combination.

   For example, press Alt+X rather than typing the characters **`Alt+X`**.

Setting Hot-Fix Policies for Standalone ACE Instances

This policy enables users of standalone ACE instances to request hot fixes if they lose or forget the ACE password, try to run an expired ACE instance, or move a copy-protected ACE instance to a new location.

To address these types of problems for managed rather than standalone ACE instances, use the VMware Help Desk Web application or the instance view in Workstation. For more information, see the *ACE Management Server Administrator's Guide*.

The hot- fix request is a file that the user must submit to an administrator for action. You configure whether the user submits the file to an administrator manually or through email generated by the Hot Fix Request wizard.

For automatically generated email, the Hot Fix Request wizard on the user's computer attempts to use a MAPI email client on the host operating system. The hot-fix request file is included as an attachment to the email message. The message uses the email address and subject line that you specify.

If you choose email and the automatic submission fails, the Hot Fix Request wizard allows the user to save the hot-fix request as a file. The user must then send the file to an administrator manually.

The administrator uses Workstation to respond to hot-fix requests. See "Respond to Hot Fix Requests" on page 463.

Setting the Policy Update Frequency for Managed ACE Instances

This policy controls how often an ACE instance connects to ACE Management Server to download policy updates while it is running. It also controls how long a managed ACE instance can be used if it cannot connect to ACE Management Server.

This policy applies only to managed ACE instances. To deploy policy updates for standalone ACE instances, you must create policy update packages. Policy changes are applied when the instance is started after the update package is installed.

The settings for offline usage include text for warning and timeout messages. You can customize messages by adding text to them. You cannot edit the existing standard text except by using the controls on the panel to change the number of minutes, hours, or days shown.

Policy updates take effect while the instance is running, with the following exceptions:

- Updates to access control policies, which include user and group lists, passwords, and scripts, take effect the next time the instance is powered on.
- Updates to policy update frequency policies, if set to **Only when the ACE instance powers on**, take effect the next time the instance is powered on.

Control Which ACE Instances Run on a Host

You can set restrictions such as the following:

- Specify whether virtual machines that are not ACE instances can run on the machine. This is a host-wide policy, which requires an administrator to install the package.
- Specify that only ACE instances with a specific creator ID can run on the machine.

You can control which virtual machines and ACE instances can be run on a host by editing the `aceMaster.dat` file in the virtual machine directory.

Before you begin, if you plan to run multiple ACE instances on the end user's machine, determine which ACE-enabled virtual machine you want to use for setting host-wide policies.

To control which ACE instances run on a host

1. On the administrator machine where Workstation is installed, power off and close the ACE-enabled virtual machine.
2. Use a text editor to open the `aceMaster.dat` file for the ACE-enabled virtual machine.

   This file is located in the same directory as the configuration file (.`vmx` file) for the ACE-enabled virtual machine.
3. (Optional) To specify that non-ACE virtual machines cannot run on the host, find the `allowVMs` property and change it from `1` to `0`.
4. Find the `requiredCreatorID` property and set it to an identifier.

   For example, to set the required creator ID to `creator1`, edit the line as follows:

   ```
   requiredCreatorID = "creator1"
   ```

   You set `requiredCreatorID` once for each host. You do not need to set this property on other ACE instances that run on the same host.

   This is a host-wide policy, which requires an administrator to install the package.

5 Find the `creatorID` property and set it to the same identifier.

   For example, to set the creator ID to `creator1`, edit the line as follows:

   ```
   creatorID = "creator1"
   ```

   Only ACE instances with this creator ID can run on the same host.

   The ID string is in plain text in the `aceMaster.dat` file on the administrator's machine, but it is hidden in the policy file.

   If you publish the policy set of an ACE instance to `requiredCreator=yourPolicySetting` and install it on a host, only you (or others with access to the administrator files) know what the creator ID is. Without knowing the `requiredCreator` policy setting, you cannot create your own ACE instance that can run on the host.

6 Do one of the following:

   - If you are creating a new ACE instance, create a package for this ACE-enabled virtual machine and install it on the end user's host.
   - If you are creating an update for a standalone ACE instance, create an update package.
   - If you are creating an update for a managed ACE instance, open the virtual machine and publish the changes to ACE Management Server.

   Changes to the `allowVMs` property or the `requiredCreatorID` property represent changes to host-wide policies. Packages that include these host policies require administrator privileges to install.

7 (Optional) If you plan to run multiple ACE instances on the end user's machine, do the following:

   a Edit the `aceMaster.dat` file for the other ACE-enabled virtual machines and set the `creatorID` property to the same value that you used in Step 5.

      Set only the `creatorID` property and not the `requiredCreatorID` property for these other virtual machines.

   b Repeat Step 6.

Writing Plug-In Policy Scripts

You can write scripts to control certain policies in VMware Player. You may use any language that is supported on the user's computer.

For security reasons, scripts must be deployed as part of a package and installed by the package installer. Users cannot modify these scripts.

When scripts run, they must write the appropriate values to the StdOut file. Output to the StdOut file might be up to 4096 bytes long.

Place any scripts you want to use for a package in the ACE Resources directory in the virtual machine directory. Do not place them in a subdirectory of the ACE Resources directory. If the scripts need any additional resource files, place those files in the main ACE Resources directory. Make sure the script uses relative paths to reference those resources.

Scripts can also write messages to the StdErr file. Output to the StdErr file may be up to 4096 bytes long. Any messages generated on the StdErr file are captured in the log file on the end user's machine at the following location:

```
<UserAppData>\VMware\VMware ACE\<package_name>\Virtual
              Machines\<VM_name>\vmware.log
```

The exit code of a script indicates whether the script succeeded or failed.

Table 19-1 describes the environment variables set in the script execution environment.

Table 19-1. Environment Variables

Variable	Description
VMWARE_MASTER_ID	The ID of the ACE-enabled virtual machine (ACE master).
VMWARE_PACKAGE_ID	The ID of the package the virtual machine was instantiated from.
VMWARE_INSTANCE_ID	A Boolean value that is set to TRUE the first time the virtual machine is powered on. Otherwise, it is set to FALSE.

All scripts run each time the end user starts VMware Player or resets the virtual machine. Some might run more often. For example, an expiration script is run every 24 hours.

The sample scripts presented in "Examples of Policy Scripts" on page 407 are installed with VMware Player in the following location:

```
C:\Program Files\VMware\VMware Player\Samples
```

The topics that follow show the format for the output that your scripts must write to the StdOut file to control various policies.

Examples of Policy Scripts

Examples include an authentication script, a host to guest data script, and a power-on hook script.

Sample scripts are installed with VMware Player in the following location:

```
C:\Program Files\VMware\VMware Player\Samples
```

Example of an Authentication Script

This script example includes the basic elements required for any authentication script. The purpose of an authentication script is to do one of the following:

- If the user is to be granted access to the virtual machine, generate the data used to create the key for this user and send it as output. The data must be unique for each user. If access is granted, the exit code is 0.
- If the user is to be denied access to the virtual machine, the script exits with a non-zero exit code. This is a reference to the exit code, not the output value.

The output of the script is hashed to create a key to encrypt and decrypt virtual machine files. The first time this script is run, the output is hashed to encrypt the virtual machine. When a virtual machine is decrypted, the script must return the same value. If the script returns a different value, the virtual machine is not decrypted and the user sees an error message.

The script may return any value. To ensure best security, a value that includes only printable characters should be at least 32 bytes long. For binary data, the value should be at least 16 bytes long to ensure proper entropy. The output is sent to the `StdOut` file.

The following example is written in Perl. It is installed by Workstation as `sample_auth.pl`. Compile it with a Perl interpreter to run it.

```
#
#   VMware Sample Script
#
#   Sample script for ACE script authentication
#
#   Description:
#   This sample script looks up the user as defined in the environment
#   variable TEST_USERNAME and returns seed data that is used to make a key
#   for authenticationpurposes.
#
#   It assumes that the username is defined in the environment variable
#   TEST_USERNAME (a ficticious environment variable used for this sample)
#   and returns the seed data from a harcoded map of username to seed data.
#
```

```
#   Input to script:
#   None.
#
#   Returns:
#   0 if successful (user is correctly authenticated).
#   -1 if TEST_USERNAME is not set, or the user is unrecognized.
#
#   Expected output:
#   Seed data for creating script authentication key on stdout.
#
#   Notes:
#   If the script returns success, its output will be used to create a key.
#   Therefore, it is important that the output of this script be unique for
#   each user, and that there is enough data to make a meaningful key (at
#   least 16 bytes).
#
#

my %user_map= ( 'charlie'         => 'E1C4F612135B4D98A33B2C9BD595025D',
                'kathy'           => 'C79AFFEF773D61225751C2566858DB08',
                'beth'            => '05B169B439B26AAB2EA4F755B7E3800C',
                'ernie'           => '8CE63D4AA2068BD8AFF2D1B05F3495A5',
                'bert'            => '"172B1619B2EFBE0E4F381AA1C428F049'
                 );

my $username = $ENV{TEST_USERNAME};
if (! defined $username) {
   print "You should set the TEST_USERNAME environment variable.\n";
   exit(-1);
}


my $key_seed = $user_map{$username};
if (! defined $key_seed) {
   print "Unrecognized username.\n";
   exit(-1);
}

print $key_seed;
exit(0);
```

Example of a Host to Guest Data Script

The following example is written in Perl. It is installed by Workstation as `sample_hostdata.pl`. You need a Perl interpreter to run this script.

```
#
#   VMware Sample Script
#
#   Sample script for ACE Host-Guest Data script
#
#   Description:
#   This sample script passes information defined on the host to the guest.
#   It assumes that the machine name is defined in the environment variable
#   TEST_MACHINENAME and that the asset tag is defined in the environment
#   variable TEST_ASSETTAG. (These are fictitious variables used for this # #
   sample).
#
#   Input to script:
#   None.
#
#   Returns:
#   0 if successful.
#
#   Expected output:
#   Set of acceptable key/value pairs where the values are fetched from the
#   environment variables. These values can be retrieved from within the
#   Guest operating system using the VMware Tools.

my $machine_name = $ENV{TEST_MACHINENAME};
my $asset_tag = $ENV{TEST_ASSETTAG};
my $host_mac = $ENV{TEST_MACHINEMAC};

if (defined $machine_name) {
   print "machine.id = " . $machine_name . "\n";
}

if (defined $asset_tag) {
   print "guestinfo.assetTag = " . $asset_tag . "\n";
}

if (defined $host_mac) {
   printf "guestinfo.mac = " . $host_mac . "\n";
}

exit(0);
```

Example of a Power-On Hook Script

The following example is written in Perl. It is installed by Workstation as `sample_poweron.pl`. You need a Perl interpreter to run this script.

```
#
#   VMware Sample Script
#
#   Sample script for ACE power-on hook
#
#   Description:
#   This sample script implements a power-on hook for ACE. This can be used
#   in addition to authentication to control the circumstances under which an
#   ACE is allowed to run.
#   This script assumes that the username is defined in the environment
#   variable TEST_USERNAME (a ficticious environment variable used for this
#   sample) and returns TRUE if the user is allowed to run, and FALSE
#   otherwise.
#   Input to script:
#   None.
#
#   Returns:
#   TRUE if username is on white list.
#   FALSE if username is not on white list or is undefined.
#
#   Expected output:
#   One of the strings "TRUE" or "FALSE"
#
#

my @white_list = ("alan", "bob", "mary", "sonia", "chris");

my $username = $ENV{TEST_USERNAME};
if (! defined $username) {
   print "FALSE";
   exit(0);
}

my @grepNames = grep(/$username/, @white_list);
if (@grepNames == 1) {
   print "TRUE";
   exit(0);
}

print "FALSE";
exit(0);
```

Customizing the VMware Player Interface on Windows Hosts Only

You can customize several aspects of the VMware Player user interface for ACE instances that run on Windows hosts. You save these customizations in a text file and identify that text file, called the skin file.

Create and Specify a Skin File

A skin file contains parameter settings for customizing the VMware Player user interface. Use this file to change application icons, the text that appears in the title bar, and to change the way removable devices are presented.

This feature is available only for VMware Player running on Windows hosts.

To create and specify a skin file

1 Use a text editor to create a skin file that includes the parameters to customize.

Use one line for each parameter and use the following form:

```
<parameter> = "<value>"
```

For a list of values to use in parameters, see Table 19-2, Table 19-3, and Table 19-4.

To comment out a line in the skin file, begin the line with the pound (#) sign.

2 Save the skin file with the filename `skin.txt` in the `ACE Resources` directory in the virtual machine directory for the ACE-enabled virtual machine.

The filename must be `skin.txt`.

3 (Optional) To display application icons other than the VMware Player icon, place the new `.ico` icon files in the `ACE Resources` directory.

For icons sizes and skin file parameters, see "Customizing the VMware Player Icons" on page 412.

4 In Workstation, close the ACE-enabled virtual machine.

5 Use a text editor to open the `aceMaster.dat` file in the virtual machine directory and add the following line:

```
vmplayer.skin = "skin.txt"
```

Because the skin file is in the `ACE Resources` directory, you do not need to specify the directory path to the file.

6 Save and close the aceMaster.dat file.

7 (Optional) To determine whether the parameters are set correctly, preview the virtual machine in VMware Player.

See "Use Preview Mode to Test Policy and Deployment Settings" on page 429.

Customizing the VMware Player Icons

VMware Player has separate large and small application icons. The large icon is used in the application switching interface (visible when you press Alt+Tab). The size of the large icon is usually 32x32 pixels, but VMware Player uses whatever size is specified for icon size in the system preference. The small (16x16 pixels) icon is used in the VMware Player title bar and on the Windows taskbar button for VMware Player.

The icons used for these purposes must be in .ico file format and located in the ACE Resources subdirectory in the virtual machine directory. The applicable parameters in the skin file include the following:

```
player.iconSmall = "<filename>"
player.iconLarge = "<filename>"
```

One .ico file can contain multiple icons of different sizes. You can specify the same .ico file for player.iconSmall and player.iconLarge. VMware Player extracts the icon of the appropriate size for each use.

Customizing the Title Bar Text

You can specify what text appears in the VMware Player title bar. You can also specify the font and font size used to display the text.

The text displayed in the title bar consists of three sections: a prefix, the virtual machine name, and a suffix. The parameters listed in Table 19-2 allow you to set any prefix and suffix, or to omit the prefix, the suffix, or both. They also allow you to include or omit the virtual machine name.

If you leave the defaults for all values, the title bar displays only the virtual machine name at 32 points in the MS Shell Dlg font.

Table 19-2 describes the VMware Player title text parameters.

Table 19-2. VMware Player Title Text Parameters

Parameter	Type	Default	Controls
`player.title.prefix`	string	""	Title bar prefix
`player.title.useVMName`	Boolean	"TRUE"	Whether the virtual machine name is displayed
`player.title.suffix`	string	""	Title bar suffix
`player.title.font.face`	string	"MS Shell Dlg"	Font name (the font must be on the user's computer)
`player.title.font.size`	integer	32	Point size for the text

Customizing the Removable Device Display

Removable devices are represented in the VMware Player interface either by buttons on a toolbar or by menu items on a **Devices** menu. You can specify the type of display. You can also specify text, icon, or a combination of the two and specify custom icons.

If you use custom icons, copy the icon files to the `ACE Resources` directory in the virtual machine directory for the ACE-enabled virtual machine.

Settings you make in the skin file override any settings the user makes in the VMware Player preferences dialog box.

Use the following parameter to control whether devices are shown as toolbar items:

```
player.deviceBar.toplevel = [TRUE | FALSE]
```

Set the parameter to TRUE for a toolbar or FALSE for a menu.

Use the parameters shown in Table 19-3 to customize the display for each removable device configured in the virtual machine.

Table 19-3. Removable DevicesParameters

Parameter	Type	Default	Controls
`player.deviceBar.<deviceName>.buttonStyle`	string (`text`, `icon`, `texticon`)	`"text"`	Appearance of toolbar button or menu item
`player.deviceBar.<deviceName>.buttonText`	string	User-friendly device name	Text that appears on the toolbar button or menu item when device is connected
`player.deviceBar.<deviceName>.buttonTextDisconnected`	string (optional)	Normal button text	Text that appears on the toolbar button or menu item when device is disconnected
`player.deviceBar.<deviceName>.tooltip`	string	""	Text that appears in the tooltip when device is connected
`player.deviceBar.<deviceName>.tooltipDisconnected`	string (optional)	Normal tooltip	Text that appears in the tooltip when device is disconnected
`player.deviceBar.<deviceName>.icon`	filename	Icon representing this type of device	Custom icon file when device is connected
`player.deviceBar.<deviceName>iconDisconnected`	filename (optional)	Normal icon	Custom icon file when device is disconnected
`player.deviceBar.<deviceName>.shortcutKey`	keySpec		Shortcut key combination to switch the device between connected and disconnected (see "Shortcut Key Values" on page 415)

Following are the device names you can use for `<deviceName>` in the parameter name:

- `floppy0`, `floppy1`
- `serial0`, `serial1`, `serial2`, `serial3`
- `parallel0`, `parallel1`, `parallel2`
- `ide0:0`, `ide0:1`, `ide1:0`, `ide1:1` (IDE CD-ROM or hard drives)
- `scsi0:0` – `scsi0:7` (SCSI CD-ROM or hard drives)

Shortcut Key Values

Use virtual key codes to specify keyboard shortcuts. Virtual key codes use hexadecimal format, which is a hexadecimal number preceded by 0x. For example, to use the virtual key code of 5A as a value, type **`0x5A`**.

Microsoft provides a reference list of virtual key codes on its MSDN Web site.

You can also use the Ctrl, Alt, and Shift modifier keys, or a combination of those keys. Table 19-4 provides the shortcut key values.

Table 19-4. Shortcut Key Values

Modifier key	Value
No modifier	0x0
Alt	0x1
Ctrl	0x2
Shift	0x4
Ctrl+Alt	0x3
Alt+Shift	0x5
Ctrl+Shift	0x6
Ctrl+Alt+Shift	0x7

When you list a key plus a modifier, type the virtual key code for the key followed by a comma, followed by the value for the modifier key or keys. For example, the value entry for Ctrl+Shift+F1 is `0x70,0x6`.

Keep the following limitations in mind when defining shortcut keys:

- Do not use the Pause key with the Ctrl key.
- If you use F12, you must use one or more modifier keys. You cannot use F12 alone.
- You cannot use combinations that include only the Shift, Ctrl, and Alt keys. You can use these keys only as modifiers in combination with some other key.

Sample Skin File

```
player.title.prefix = "Our Company <<"
player.title.suffix = ">> Environment"
# player.title.useVMName = "FALSE"

# player.deviceBar.toplevel = TRUE
player.deviceBar.floppy0.buttonStyle = "icon"
player.deviceBar.floppy0.buttonText = "First Floppy Drive"
player.deviceBar.floppy0.shortcutKey = "0x30,0x7"
player.deviceBar.floppy0.icon = "custom-floppy.ico"
player.deviceBar.floppy0.tooltip = "Click to disconnect"
player.deviceBar.floppy0.tooltipDisconnected = "Click to connect"
# player.deviceBar.ethernet0.buttonStyle = "icon"
# player.deviceBar.ide1:0.buttonStyle = "icon"
# player.deviceBar.audio.buttonStyle = "icon"
```

Deploying ACE Packages 20

This chapter provides instructions for specifying deployment settings for ACE packages, creating ACE packages, and deploying packages to end users. This chapter includes the following topics:

- "Edit Deployment Settings" on page 417
- "ACE Resources Directory" on page 428
- "Review the Configuration of an ACE-Enabled Virtual Machine" on page 429
- "Use Preview Mode to Test Policy and Deployment Settings" on page 429
- "Creating a Package" on page 431
- "Perform an End-to-End Deployment Test" on page 437
- "Deploy Packages" on page 438

Edit Deployment Settings

Deployment settings enable you to configure package characteristics, such as instance customization and encryption, and then apply those settings to as many packages as you choose. Changes to deployment settings affect only packages created after the changes are made. They do not apply to existing packages.

Before you can use the deployment settings editor on a virtual machine, you must enable ACE features for that virtual machine. See "Overview of Creating and Deploying ACE Packages" on page 368.

To edit deployment settings

1. Select the ACE-enabled virtual machine and choose **VM > ACE > Deployment Settings**.
2. In the deployment settings editor, select an item in the **Setting** list.
3. Complete the settings panel for that deployment setting and click **OK** or select another setting to edit.

   For assistance with the fields on a settings panel, click **Help**.

Encryption Settings

Encryption settings are of two types:

- **Package protection** – Protects package files from being copied or altered while in transit. If you set package protection to **Encrypted**, the New Package wizard encrypts the virtual machine when a package is created.
- **Instance protection** – Protects ACE instance files from being copied or altered after installation and activation. You must specify an authentication method if you want the installer to encrypt the ACE instance.

The activation and authentication policies you choose determine which default encryption settings are applied to the package and files. See "Setting Access Control Policies" on page 375. VMware recommends these default settings for production environments. The files do not need to be encrypted when you deploy a package in a test environment.

NOTE If you set the encryption settings to **None**, any verification specified in the resource signing policy is not performed. The encryption package setting overrides the resource signing policy setting. See "Setting Resource Signing Policies" on page 384.

Package Lifetime Settings

You can specify a time period during which an ACE package is installable. If a user attempts to install a package outside of this time period, an error message appears and the package is not installed.

The administrator can change the package lifetime settings on managed packages even after package creation.

Change Package Lifetime Settings for a Managed Package

If you use the ACE Management Server, you can change the package lifetime settings or deactivate a package immediately.

Before you begin, make sure Workstation is connected to the ACE Management Server. For information about installing and setting up the server, see the *ACE Management Server Administrator's Guide*.

To change package lifetime settings for a managed package

1. Select the ACE-enabled virtual machine and choose **View > Current View > Summary**.
2. Click the **Packages** section tab.
3. Right-click the package and do one of the following:
   - To change the package lifetime settings choose **Properties > Settings**.
   - To deactivate the package immediately choose **Deactivate**.

Instance Customization on Windows Hosts Only

Instance customization applies only to ACE instances that have a Windows guest operating system installed. The instance customization process is built around the standard Microsoft Sysprep deployment tools. It provides the following benefits:

- Automates the Sysprep process (the use of the Microsoft Sysprep deployment tools). It gives you better control of some Sysprep parameters, such as computer name.
- Automates joining ACE instances to a domain from a remote site. See "Set Up a Remote Domain Join" on page 425.
- For managed ACE instances, the instance customization process on the user's machine reports the success or failure of the process to the server. The information is available in the instance view of Workstation. Besides status, the process also reports the MAC address and the new computer name.

Instance Customization Process During Packaging

If you specify instance customization deployment settings, the following events occur when you complete the New Package wizard:

1 A snapshot of the ACE-enabled virtual machine is taken and saved.

2 The ACE-enabled virtual machine is powered on, and all the required deployment tools and files, including the appropriate Microsoft Sysprep tools, are copied into the guest.

   No visible indication shows the copying process. See "Download the Microsoft Sysprep Deployment Tools" on page 421.

3 The Microsoft deployment tools run inside the guest operating system to seal the guest and prepare for deployment.

4 The guest operating system shuts down.

5 The ACE-enabled virtual machine is cloned into the package directory.

   The virtual machine files are copied into the directory, encrypted if set to do so, and divided to be put on media if set to do so.

6 The ACE-enabled virtual machine reverts to the snapshot.

7 The snapshot is deleted.

8 The installer files are copied into the package directory.

Instance Customization on the End User's Machine

On the ACE user's machine, after the installation and instance activation, the following events occur:

1 All information required for resolving placeholder variables is obtained.

2 Placeholder variables are resolved and replaced with the actual values for the ACE instance.

   See "Placeholder Values to Use in Instance Customization" on page 423.

3 The Microsoft Mini-Setup process runs unattended.

   If the Mini-Setup process fails, the ACE instance shuts down.

4 (Optional) Additional commands to execute other scripts that you specified in the instance customization deployment settings are executed.

5. (Optional) If you configured a remote domain join, the software executes the script you specified, connects the ACE instance to the VPN server, and joins the virtual machine to the domain.

   See “Set Up a Remote Domain Join” on page 425.

6. For managed instances, instance customization is reported to the server if it is successful.

Prerequisites for Using Instance Customization

Instance customization is available for both managed and standalone ACE instances.

Before you specify instance customization settings, perform the following tasks:

- Install a Windows 2000, XP Professional, Server 2003, or Vista guest operating system on an ACE-enabled virtual machine.
- Install the latest version of VMware Tools on the guest operating system. See “Installing VMware Tools” on page 100.
- Download the Microsoft Sysprep tools. See “Download the Microsoft Sysprep Deployment Tools” on page 421.
- Gather the following information:
  - The Windows product ID for the guest operating system installation.
  - If the ACE instance will be joined to a domain (whether the instance is local or remote to the domain), the user name and password for an account that has permission to add computers to the domain.
  - Remote domain join parameters if a remote ACE instance will be joined to a domain. See “Set Up a Remote Domain Join” on page 425.

Download the Microsoft Sysprep Deployment Tools

You do not need to download Microsoft Sysprep deployment tools if you have a Windows Vista operating system. They are included with the Windows Vista installation.

To download the Microsoft Sysprep deployment tools

1. Go to the Microsoft Web site and search for Sysprep deployment tools.
2. Follow the instructions on the site for downloading the Sysprep deployment tools.

   Download all versions that correspond to the guest operating systems that you plan to deploy. These tools include Sysprep deployment tools for Windows 2000, Windows 2003, and Windows XP Professional SP1 and SP2. The SP1 version works with Windows XP Professional with no service pack and Windows XP Professional SP1.
3. Unzip the files into the directory where Workstation is installed.

   The default installation directory is:

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

Specify Deployment Settings for Instance Customization

Before you begin, install all required files for customization scripts. See “Prerequisites for Using Instance Customization” on page 421.

To specify deployment settings for instance customization

1. Select the ACE-enabled virtual machine and choose **VM > ACE > Deployment Settings**.
2. Select **Instance Customization** and complete the settings panel.
3. Select **System Options** and complete the settings panel.

   Use the following information to complete the fields:

   - **System options** – You can use placeholder variables for the system name, organization name, and computer name. For details on the placeholder variables, including an example, see “Placeholder Values to Use in Instance Customization” on page 423.

     CAUTION The Mini-Setup process fails if you enter **`administrator`** in the **Name** field or the **Computer Name** field or for Windows Vista guests, if the computer name is more than 15 characters.

     If you set the `%logon_user%` placeholder in those fields and the placeholder variable resolves to `administrator`, the software automatically changes the value to a random alphanumeric string of 10 characters.
   - **Security ID** – A new SID is always generated for Windows Vista guests, regardless of the setting you choose here.

4 Select **Initialization Scripts** and type the additional commands to run scripts in the guest operating system at the end of the Mini-Setup process on the ACE user's machine.

For more information about commands, see the Microsoft deployment tools documentation.

Specify the path to the batch file without using quotation marks. Quotation marks are added automatically. For more information, see the Microsoft knowledge base article about troubleshooting `Cmdlines.text` during an unattended setup.

5 Select **Workgroup or Domain** and complete the settings panel using the following information:

- Instance customization supports only IP addresses that DHCP servers provide. Static IP addresses are not supported.

- To allow this ACE instance to join the domain from a location remote to the domain, see "Set Up a Remote Domain Join" on page 425.

6 Specify other types of deployment settings or click **OK**.

To create a package with these settings, see "Creating a Package" on page 431.

Placeholder Values to Use in Instance Customization

Use placeholder values to construct machine-specific names inside the guest operating system during the Mini-Setup process.

Following are the available placeholders:

- `%logon_user%` or `%logon_user(n)%` – The user logged in to the host machine at the time the Microsoft Mini-Setup process begins.

  You can use `%logon_user(n)%`, where <n> is the maximum number of characters obtained from the actual logged-in user when the name is resolved. Use <n> if you the user name must be resolved to no more than a certain number of characters. For example, if you specify that 3 random characters are to be added to the actual user name and you want to limit the resolved name to 15 characters, set <n> to 12. Your entry in the **Name** field in the **System Options** panel is `%logon_user(12)%%random_alpha_digit(3)%.`

  Including `(n)` in the placeholder is optional. If you use only `%logon_user%` or if you set <n> to zero (0), the placeholder resolves to the full logged-in user name.

- %host_name% or %host_name(n)% – The name of the host computer (usually used with some additional random number or name).

  You can use %host_name(n)%, where <n> is the maximum number of characters obtained from the actual computer host name when the name is resolved. Use <n> if the host name must be resolved to not more than a certain number of characters. For example, if you specify that 3 random characters are to be added to the actual host name and you want to limit the resolved name to 15 characters, set <n> to 12. Your entry in the **Computer Name** field in the **System Options** panel is %host_name(12)%%random_alpha_digit(3)%.

  Including (n) in the placeholder is optional. If you use only %host_name%, or if you set <n> to zero (that is, the placeholder resolves to the full host name.

- %random_alpha_digit(n)% – A randomly generated string of letters and numbers, where <n> is the number of characters. You must specify <n>.

- %random_alpha(n)% – A randomly generated string of letters, where <n> is the number of characters. You must specify <n>.

- %random_digit(n)% – A randomly generated string of numeric characters, where <n> is the number of characters. You must specify <n>.

For Windows Vista guests, if the computer name is more than 15 characters, the Mini-Setup process fails on the user machine.

Specify Additional License Information for Windows Server Products

To supply additional license information for Windows Server products, you can add a file named sysprep_license.txt to the ACE-enabled virtual machine directory.

To specify additional license information for Windows Server products

1 Use a text editor to create a file named sysprep_license.txt in the virtual machine directory for the ACE-enabled virtual machine.

2 Add the following line to the file:

```
AutoMode=[PerSeat | PerServer]
```

This line indicates whether the license is for one client license or for a certain number of client licenses for a server.

3 If AutoMode is set to PerServer, add the following line to the file, where <n> indicates the number of client licenses for the server:

```
AutoUsers=<n>
```

4 Save and close the file.

For more information, go to the Microsoft TechNet Web site and in the Windows Server Library, search for [LicenseFilePrintData] (Sysprep).

If this file is not found in the virtual machine directory, a default is used. `AutoMode` is set to `PerServer` with 5 client licenses.

If you supply this file, the license portion of the Mini-Setup process appears unchanged during preview. You always see `AutoMode=PerServer` and `AutoUsers=5` in the Mini-Setup user interface. The license information you supply is nevertheless set correctly by the Mini-Setup process.

Set Up a Remote Domain Join

The remote domain join feature provides an automated way to join ACE instances to a domain from a remote site.

After the ACE package is installed on the end user's machine and the ACE instance is activated and authenticated, the Microsoft Mini-Setup process runs. The script for joining the remote ACE instance to the domain executes at the end of that process, and the machine is joined to the domain.

Before you begin, perform the following tasks:

- Determine which VPN client to download. The VPN client must support a command-line interface so that a script can be used for logging in to the VPN server. You might need to contact the VPN product's technical support to find out whether the VPN client supports a command-line interface.

- Obtain a VPN account for logging in to the server. Credentials include a user name and password. Randomly generated security tokens cannot be used as passwords. For example, you cannot use an RSA security token.

- Determine the following information to use for the VPN client profile: the company's group and password information and the name of the VPN server to contact to establish a secure connection.

- Determine the name of the domain that you plan to add the ACE instance to.

- Determine the user name and password for an account that has permission to add computers to the domain.

To set up a remote domain join

1. In the guest operating system of the ACE-enabled virtual machine, install a VPN client that supports a command-line interface.

2. Use the VPN client software to configure a profile for this client.

   The profile in the VPN client contains a company's group and password information and determines which server to contact to establish a secure connection.

3. Write a `.bat` script that allows remote execution during the instance customization process.

   Following is an example of a `.bat` script for a Cisco VPN client:

   ```
   "net" start "Cisco Systems, Inc. VPN Service"
   "C:\Program Files\Cisco Systems\VPN Client\vpnclient.exe" connect
                 <profile_name> user <vpn_user_name> pwd %1 >> vpnlogs.txt
   ```

   This example consists of two lines. The command in the first line starts the Cisco VPN client's background service. The command in the second line connects to the Cisco VPN using a command-line interface. It supplies the name of the VPN profile and the credentials for logging in to the VPN server. The example uses the password placeholder variable, but you could also use a static password for the VPN account. A static password included in a script is sent in clear text.

4. Save the `.bat` file on the `C:` drive of the guest's file system.

5. In Workstation, select the ACE-enabled virtual machine and choose **VM > ACE > Deployment Settings**.

6. Select **Workgroup or Domain.**

7. In the settings panel, select **Domain** and specify an organizational unit and user name for an account that has permission to add computers to the domain.

   An example of an entry in the OU full path file is **`OU=orgunits,DC=dpt,DC=domain,DC=com`**.

   If the ACE-enabled virtual machine is managed, passwords and commands are stored on ACE Management Server.

   If the ACE-enabled virtual machine is standalone, passwords and commands are stored with the package. Be sure to use encryption for the package.

8. Select **Enable Remote Domain Join**.

9 Specify the password for logging in to the VPN server.

   You can then use the `%password%` placeholder variable in the **Command** text box to refer to this password.

10 Enter the command that executes the script.

   For example, if you name the `.bat` script `vpn.bat` and want to use the password placeholder variable, enter the following command:

   ```
   C:\vpn.bat%password%
   ```

   If you use a password placeholder variable (`%password%`) in the **Command** field, the placeholder variable is resolved and replaced with the value from the **Password** field when the script executes.

11 Click **OK**.

To create a package with these settings, see "Creating a Package" on page 431.

Custom EULA Settings

You can provide a custom end-user license agreement (EULA) that appears when an ACE instance is activated. The user must see and accept the agreement before the instance can run for the first time.

The custom EULA must be a text file located in the `ACE Resources` directory for the ACE-enabled virtual machine. The file can use the following formats:

- For Windows hosts, use a `.txt` or `.rtf` file.
- For Linux hosts, use a `.txt` file.
- If you plan to deploy the package to both Windows and Linux computers, use a `.txt` file.

To specify whether to deploy to Windows hosts, Linux hosts, or both, use the **Deployment Platform** setting in the deployment settings editor.

Deployment Platform Settings

By default, ACE packages are created for Windows hosts. Change this setting to deploy to Linux or both Linux and Windows hosts.

ACE Resources Directory

The ACE Resources directory is a subdirectory of the ACE-enabled virtual machine's directory. All files placed in this directory are copied into the ACE package so that they can be used in end users' virtual machines.

Place the following types of files in the ACE Resources directory:

- Authentication scripts

  See "Using an Authentication Script" on page 378.

- Power-on and power-off scripts

  See "Include a Power-On and Power-Off Script in the Package" on page 378.

- Other resource files that authentication, power-on, or power-off scripts call

- Device files such as ISO images or FLP images that the virtual machine is configured to point to

- The skin file, which you can create to customize the VMware Player icons, removable device icons, and title bar text used in the VMware Player user interface on Windows guests

  See "Create and Specify a Skin File" on page 411.

- Icon files for removable devices or the VMware Player application

  See "Customizing the VMware Player Icons" on page 412 and "Customizing the Removable Device Display" on page 413.

- Custom EULAs

  See "Custom EULA Settings" on page 427.

When you use the ACE Resources directory, take the following considerations into account:

- Do not place files in a subdirectory of the ACE Resources directory. If scripts or skin files reference other files, place those other files in the main ACE Resources directory. Make sure the script uses relative paths to reference those resources.

  A resource is considered any file in the ACE Resources directory. You can specify whether to verify all files in the ACE Resources directory or just the policy scripts in that directory. For more information, see "Setting Resource Signing Policies" on page 384.

- If you change a policy or package setting that requires the ACE Resources directory, you must create an update package to deploy the change to end users.

Review the Configuration of an ACE-Enabled Virtual Machine

To finish preparing your ACE-enabled virtual machine and its files for packaging, review its configuration and policies and ensure that the appropriate operating system and software are installed in it.

To review the configuration of an ACE-enabled virtual machine

1. Verify that the ACE-enabled virtual machine has the necessary operating system, application software, and VMware Tools installed.

   See "Installing VMware Tools" on page 100. For information about specific operating systems, see the *VMware Guest Operating System Installation Guide*.

2. To review configuration settings, select the ACE-enabled virtual machine and choose **View > Current View > Summary**.

3. To review virtual machine devices and virtual hardware, click the **Devices** tab in the summary view.

4. To review virtual machine configuration options, click the **Options** tab.

5. To make changes to devices or options, click **Edit virtual machine settings** in the **Commands** list.

6. To review policies and deployment settings, click the **ACE** tab.

7. To make changes to policies or deployment settings, click **Edit policies** or **Edit deployment settings** in the **Commands** list.

Use Preview Mode to Test Policy and Deployment Settings

Preview mode enables you to see the effects of changed policies without having to package and deploy them. Preview mode also enables you to see the effects of setup choices without having to create, deploy, and install a full package.

Before you begin, verify that the settings and deployment platforms you want to test are appropriate for preview mode. Because ACE features are available only in the Windows version of Workstation, you cannot use preview mode to run ACE instances created for Linux hosts. You also cannot test a host policy in preview mode. To test ACE instances that you plan to deploy on Linux hosts, or for which you want to test a host policy, see "Perform an End-to-End Deployment Test" on page 437.

You can run the ACE instance in preview mode in VMware Player and also run the ACE-enabled virtual machine in Workstation without having to shut down the preview.

NOTE You can run any ACE-enabled virtual machine directly in Workstation to be sure that the guest operating system and applications perform as expected. However, an ACE-enabled virtual machine running in Workstation does not respect any policies that restrict its functionality.

To use preview mode to test policy and deployment settings

1 Open the ACE-enabled virtual machine to test.

2 In the summary view, click **Edit policies** in the **Commands** list.

3 In the **Policy** list, select the policy to change, complete the settings panel for that policy, and click **OK**.

4 In the summary view, click the **Preview in Player** in the **Commands** list.

A package based on a linked clone is created in a new directory, `Preview Deployment`, inside the ACE-enabled virtual machine's directory. The linked clone is created from a snapshot of the virtual machine's current state. Unlike a package that is deployed to an ACE user's machine, this package is not installed.

VMware Player allows you to activate and authenticate the ACE instance (if those policies are set). If configured, instance customization is also performed. The guest operating system starts.

5 Test the policy change in the running ACE instance to ensure that it is the one you want to make.

Preview mode enables VMware Player to run interactively so that you can see any instance customization errors and make corrections as needed.

6 (Optional) To make additional changes to policies or deployment settings, shut down the virtual machine and repeat this procedure.

You can have only one preview instance per ACE-enabled virtual machine. When you click **Preview in Player** a second or subsequent time, a message asks if you want to replace the current preview instance with a new deployment or use the existing deployment.

To change only policies and not repeat the activation and instance customization steps, use the existing deployment.

7 If ACE Management Server is managing the virtual machine, click **Publish Policies to Server**.

Creating a Package

After you create an ACE-enabled virtual machine and configure policies, devices, and deployment settings, use the New Package wizard to create a package to deploy instances to users.

NOTE To create a Pocket ACE package for distribution on portable devices, use the Pocket ACE Package wizard rather than the New Package wizard. See "Create a Pocket ACE Package" on page 442.

For packages that you plan to deploy to Windows hosts, you can specify that the package is to be distributed through a network image or through DVDs or CDs. For DVD and CD distribution, the package is divided into files that fit on standard discs.

Overview of Package Creation and Validation

Depending on whether you want to deploy a new ACE instance or update an installed one, you can create any of the following types of packages:

- **Full** – Includes an installer and the additional files needed to install an ACE package and the VMware Player application that runs the ACE instance. A full package allows you to create a completely new ACE instance.

CAUTION If you replace an existing ACE instance by supplying a new full package, end users lose any data or custom settings stored in the older ACE instance.

- **Policy Update** or **Server Update** – Includes just the policy-related files.
  - For standalone ACE-enabled virtual machines, the option is **Policy Update**.
  - For managed virtual machines, it is **Server Update**.

    Among other policies, a server update package allows you to change the server that the ACE-enabled virtual machine is associated with or change an activation-only server setup to an activation and tracking setup.
- **Custom** – Allows you to choose specific items to deploy.
- **Pocket ACE** – The components for a Pocket ACE package vary slightly from those for the full package. For information about the Pocket ACE package, see "Create a Pocket ACE Package" on page 442.

The deployment settings and device settings that you already set for an ACE-enabled virtual machine allow you to create multiple packages quickly. You can use the same settings again and again.

Package validation occurs after you complete the New Package wizard. Package validation does the following:

- Checks that all files that the ACE-enabled virtual machine requires are present. Those files include:
  - Disk and snapshot files
  - Script files (if any policy is using scripts)

  NOTE Package validation does not check for device files (ISO images, FLP images, and so on). To include device files in the package, put the files in the `ACE Resources` folder for the ACE-enabled virtual machine and set the devices to point to that location.

- Checks that the ACE-enabled virtual machine can be cloned: that it is powered off, multiple snapshots are enabled, and it is not read-only.
- Checks that the latest version of VMware Tools is installed.
- If instance customization is enabled, checks that the `SysprepTools` directory for the ACE-enabled virtual machine's guest operating system is not empty.
- If the guest operating system is Windows 2000, Windows XP, or Windows 2003, checks that the folders in the `Program Files\VMware\VMware Workstation\Resources\SysprepTools` folder are not empty.

You can deploy a package over a network or on DVD or CD. If you deploy the package on discs, the first disc of the set includes the autorun files needed to start the installer automatically when the user inserts the disc in the host computer's drive.

Turn Off the VMware Tools Check for Test Deployments

If you do not have the latest version of VMware Tools installed in the guest operating system, the wizard fails to create the package. To create packages without installing the latest VMware Tools version each time—for example, if you want to perform a test deployment—you can turn off the VMware Tools check.

To turn off the VMware Tools check for test deployments

1 Close Workstation.

Use a text editor to open the `preferences.ini` file, which is located in the following directory:

```
C:\Documents and Settings\<user>\Application Data\VMware
```

2 Add the following line to the file:

```
pref.ignoreToolsPkgCheck = "TRUE"
```

Setting this line to FALSE reinstates the VMware Tools check.

3 Save and close the `preferences.ini` file.

Before you create packages that you plan to deploy in production environments, reinstate the VMware Tools check.

Prerequisites for Using the Packaging Wizards

The following prerequisites apply to the New Package wizard and the Pocket ACE Package wizard:

- Ensure that the guest operating system and the most recent version of VMware Tools are installed in the ACE-enabled virtual machine. See "Installing VMware Tools" on page 100.
- Defragment virtual disks to ensure that the package is as compact as possible. See "Defragment Virtual Disks" on page 223.
- Preview the ACE instance to verify that all settings are working correctly. See "Use Preview Mode to Test Policy and Deployment Settings" on page 429.
- Determine the passwords used for the policies and deployment settings. These can include the following:
  - **Activation password** – Access control policy is set to **Password**.
  - **Domain join credentials** – Access control policy for the ACE instance is set to **Password**, and the **Instance Customization** deployment setting for **Domain** is enabled. This password is for the user account that has permission to add computers to this domain.
  - **Remote domain join credentials and VPN credentials** – The **Instance Customization** deployment settings for **Domain** and **Enable remote domain join** are enabled. The domain password is for the user account that has permission to add computers to this domain. The password in the **Remote domain join** section is for the user account that has permission to access the VPN server.

- Verify that you have enough disk space for temporary files created during packaging. You must have twice the combined sizes of all the components of the package.

  The wizard displays information about the amount of space needed and the locations where the space is needed. If you do not have enough free space, you can move or delete files on the target drives to make room for the wizard's working files.

- Determine the type of package you want to deploy: full, update, or custom. See "Overview of Package Creation and Validation" on page 431.

- To distribute the package on DVDs or CDs, determine how much disk space is available. You can then specify the maximum file size used when the package is divided into multiple files.

To use instance customization, verify that the following prerequisites are satisfied:

- Make sure that the guest operating system is Windows XP, Windows 2000, or Windows Server 2003, or Windows Vista.

- Copy the Microsoft Sysprep Deployment Tools into the correct folder for the virtual machine. See "Download the Microsoft Sysprep Deployment Tools" on page 421.

  If these tools are not available, the packaging operation fails. The failure might not occur until well into the packaging process and might cause you to lose substantial time.

- Use preview mode to test whether instance customization runs unattended. For example, verify that a valid Windows product ID is used so that no dialog box prompts for the product ID during the Mini-Setup process.

- If you configured automatic login, use preview mode to verify that automatic login works correctly. If it fails, instance customization fails.

Use the New Package Wizard

The New Package wizard creates an executable file that contains an ACE-enabled virtual machine, its policies, deployment settings, scripts, and a copy of VMware Player. You can easily deploy and install the package on end user's machines.

Before you begin, verify that the packaging prerequisites are satisfied. See "Prerequisites for Using the Packaging Wizards" on page 433.

To use the New Package wizard

1 Open the ACE-enabled virtual machine to use as the basis for the package.

2 Make sure the virtual machine is powered off rather than suspended.

When you exit preview mode, by default VMware Player suspends the virtual machine. If necessary, use Workstation to power off the virtual machine.

3 Choose **VM > ACE > New Package**.

4 Complete the New Package wizard.

5 (Optional) If you are prompted to select a package distribution format and you select **Multiple folders for creating DVDs or CDs**, write down the disc label prefix you specify.

When you later use disc-burning software to create the discs, the name you enter for each disc must be the same as the name of the folder the wizard creates to hold that disc's contents (for example, DISC1, DISC2).

6 To begin the packaging process, click **Next** on the Package Summary page.

Package creation takes a substantial amount of time, especially for packages that include large virtual machines or instance customization settings.

During the instance customization stage, if the guest operating system does not shut down after approximately 10 minutes, the problem might be that the Sysprep tools were not in place. The operation is cancelled and an error message tells you that instance customization failed.

The Package Creation Complete page appears when the process is complete. It lists the location of the newly created package and provides a link to the package directory.

7 Depending on which distribution method you chose, do one of the following:

- If you created a single file for network distribution, copy the file to the appropriate location on a network.
- If you created one or more files for distribution on CD or DVD, use disc-burning software to create the discs. Follow these guidelines:
    - The disc label you enter in your disc-burning software for each disc must be the same as the name of the folder the wizard creates to hold that disc's contents.
    - Burn the contents of each disc onto the top level of the disc.

      The package installer expects to find only the contents of the folder, and not the folder itself, at the root level on the disc. If you burn the folder itself onto the disc, when you attempt to install the contents of the second or subsequent discs on the user's machine, the error 1309, "`Error reading from file <filename>`", appears.

View Package Properties and Add Notes

Use the Package Properties dialog box to view properties of the packages that you created. Also add or edit notes that appear in the summary view of the ACE-enabled virtual machine.

To view package properties and add notes

1 Open the ACE-enabled virtual machine.

2 Choose **View > Current View > Summary**.

3 On the **Packages** tab, double-click the package name.

4 In the Package Properties dialog box, click the tabs to view the properties.

5 Click the **Notes** tab to add or edit notes.

Existing notes might have been added when the package was created using the New Package wizard. These notes are not be seen by end users. They are visible only in the Workstation window.

Perform an End-to-End Deployment Test

Perform an end-to-end test to deploy a new ACE package rather than a package update. Also use an end-to-end test if using preview mode is not appropriate.

Because Workstation runs only on Windows hosts, you cannot use preview mode to run ACE instances as they will run on Linux hosts. You also cannot test a host policy in preview mode.

NOTE This test might take a substantial amount of time because packaging and encryption processes can be lengthy.

Before you begin, if you plan to use an ACE Management Server to manage the ACE instances, install and configure a test ACE Management Server. See the *VMware ACE Management Server Administrator's Guide*.

To perform an end-to-end deployment test

1. If you use the ACE Management Server, select the ACE-enabled virtual machine, choose **File > Connect to ACE Management Server**, and connect to the test server.
2. In the virtual machine's summary view, click **Create new package** in the **Commands** list.
3. Complete the New Package wizard.
4. Navigate to the package location and copy the package directory to a client test machine.
5. On the client test machine, run the ACE instance's `setup.exe` file and complete the pages of the installation wizard.
6. Start the ACE instance and activate it when prompted.

   Depending on how you configured the package, a **Start** menu item or a desktop shortcut or both are created on the client machine. Depending on the runtime preferences you set, the ACE instance might start in full screen mode when the host system starts.
7. Verify that the ACE instance is configured as you intended and runs as you expect.

8 If you use ACE Management Server, connect the ACE-enabled virtual machine to the production server.

   On the administrator machine, in Workstation, select the ACE-enabled virtual machine and choose **File > Connect to ACE Management Server**, and connect to the production server.

9 If you use ACE Management Server, create a new package.

   The package you created for the test refers to the server you used for testing. Instances created from that package refer to the test server.

Deploy Packages

Deploying packages means making the ACE package available to end users. You specify the distribution method when you create the package.

To deploy packages

Depending on the type of package, do one of the following:

- For a full, policy update, server update, or custom package, distribute the package on CD or DVD, or make the package available on a network.
- For a Pocket ACE package, see "Deploying the ACE Package on a Portable Device" on page 443.

Pocket ACE

21

The Pocket ACE feature enables you to store ACE instances on portable devices such as USB keys (flash memory drives), Apple iPod mobile digital devices, and portable hard drives. ACE users attach these portable devices to x86 host computers, run their ACE instances with VMware Player, and then detach the portable devices. The next time they need access to their ACE instances, they can attach the devices to the same host computers or to different computers.

Use Pocket ACE to package a daily computing environment and allow end users to take that environment—including documents, settings, applications, and VPN access—wherever they need to go.

This chapter includes the following topics:

Use Cases for Pocket ACE

Use the following scenarios to determine when to use Pocket ACE and which kinds of policies to set for various situations:

- **Providing access to employees working remotely** – Employees often use their own home computer for accessing enterprise resources remotely. Unmanaged clients can be infected by malware or spyware. In addition, there is a risk of lost data if a remote user downloads sensitive data to a personal computer. There is also the added burden of deploying and managing the software needed by remote users.

  Using Pocket ACE, IT administrators can deploy a trusted, managed, and more secure virtual desktop instance to remote users. The virtual disk of the Pocket ACE can be encrypted to minimize the risk of lost data. By setting specific network quarantine policies, administrators can strictly control traffic between the untrusted client and Pocket ACE instance, protecting the enterprise from creating a compromised host.

- **Increasing the security and mobility of mobile users** – Mobile users often access or carry sensitive data outside the enterprise using laptops or other mobile devices. The question for IT organizations is not if, but when, a mobile user's laptop will be lost or stolen, leading to the loss of sensitive or confidential data.

  Using Pocket ACE to deploy a desktop environment to mobile users, IT administrators can reduce the risk of lost data while also increasing users' mobility because Pocket ACE instance can be used with any supported x86 system. A desktop instance with an encrypted disk can be deployed to mobile users. Using ACE Management Server, a lost or stolen Pocket ACE can be disabled remotely.

- **Providing temporary access to contract workers using untrusted hosts** – Contractors and business partners often connect to the enterprise network from unknown or untrusted clients. Pocket ACE can be used to provide a standardized, trusted, and managed environment to these users while enabling safe connectivity to enterprise resources.

  For contractors, the Pocket ACE instance can be configured to be available only during the length of the contract. When the expiration date is reached, the contractor can no longer use the Pocket ACE instance.

- **Providing access to offshore outsource partners** – Typically, offshore partners manage and own the desktop systems they use. Because these resources are owned by an outside organization, they do not fall under standard IT policy. In some cases, desktop systems are purchased, imaged, and shipped to an offshore partner for accessing the enterprise. This is often a lengthy and costly process.

  With Pocket ACE, IT administrators can easily deploy a trusted, managed, and more secure virtual desktop instance to offshore partners. The virtual desktop instances can be distributed using portable media or download. Security features include the data encryption feature and the network quarantine and restriction features already mentioned.

- **Providing disaster recovery** – Using Pocket ACE, organizations can easily package desktop instances with all the necessary enterprise applications for use in the case of a disaster. These instances can be deployed to portable media devices and stored safely in a secure offsite facility. If a disaster occurs, the Pocket ACE instances can be quickly distributed and used.

- **Distributing beta or trial software** – Using Pocket ACE, ISVs can distribute software preinstalled as a virtual appliance either by download or on a portable media device. An ISV can provide a complete working environment, ensuring no compatibility issues. Custom EULAs can be created and used to ensure that a user accepts the agreement prior to using an ACE instance. In addition, an expiration period can be set that disables an ACE instance after an allotted period of time.

Portable Device Requirements

You can install ACE packages on the following types of devices:

- Flash memory drives (USB keys)
- Flash-based Apple iPod mobile digital devices
- Hard drive–based Apple iPod mobile digital devices
- Portable hard drives

For USB devices, use USB 2 high-speed devices only.

When a Pocket ACE package is deployed to a removable device, the virtual disk is preallocated to full capacity for enhanced performance. Make sure that the removable device has enough disk space to store the virtual disk’s total capacity, memory, and approximately 300MB for overhead. See “Use the New Virtual Machine Wizard” on page 86.

Policies and Deployment Settings for Pocket ACE

Some policies apply only to Pocket ACE. You can set Pocket ACE close behavior by editing the runtime preferences policy.

Close behavior determines whether the ACE instance is powered off or suspended when the user exits and whether changes are synchronized on the removable device. See "Pocket ACE Cache Settings" on page 399.

Pocket ACE ignores some policies. Although you can set host and snapshot policies and create a package that includes them, Pocket ACE instances ignore these policies. Administrators cannot revert to reimage snapshots when running a Pocket ACE in administrator mode in VMware Player.

Create a Pocket ACE Package

Before you begin, determine the following information, which is specific to Pocket ACE:

- Make sure the portable device meets the hardware and disk space requirements for Pocket ACE. See "Portable Device Requirements" on page 441.
- Determine whether you want to deploy the Pocket ACE to Windows machines, 32-bit Linux machines, 64-bit Linux machines, or some combination. Your choices affect the disk space requirements.
- Determine the password you want to use for anyone who attempts to deploy the package to a portable device.

  If you do not want to require a password, make sure the access control policy's authentication type is set to **None**. Make sure the encryption deployment setting for package protection is set to **None**.

In addition, complete the tasks listed in "Prerequisites for Using the Packaging Wizards" on page 433.

To create a Pocket ACE package

1. Open the ACE-enabled virtual machine to use as the basis for the package.
2. Make sure the virtual machine is powered off rather than suspended.

   When you exit preview mode, by default VMware Player suspends the virtual machine. If necessary, use Workstation to power off the virtual machine.
3. To create a new Pocket ACE or an update package, choose **VM > ACE > New Pocket ACE Package**.

4 Complete the wizard.

When you specify a location on the Name the Package page, choose a location on the administrator machine. Do not specify a location on the portable device. You deploy the package to the device after the package is created.

The Completing the Pocket ACE Package Wizard page appears when the process is complete.

5 (Optional) To deploy the package immediately, select **Deploy to a portable device now**.

If you do not deploy the package immediately, see "Deploying the ACE Package on a Portable Device."

Deploying the ACE Package on a Portable Device

You can deploy multiple ACE packages on a single portable device. The only limitation on the number of packages is the amount of available space on the device.

Run the `deploy.exe` file to use the GUI deployment utility. Use the `bulkDeploy.exe` program to use the command-line deployment utility. You can create a batch file that contains multiple `bulkDeploy` commands to deploy multiple ACE packages to a portable device.

The wizard automatically preallocates disk space and splits the disk into 2GB segments.

The Pocket ACE instance is reencrypted during the deployment instead of after the user's first run of the instance. For this reencryption, the policy applied is the package protection policy that was in place at the time of packaging.

Use the Graphical Utility to Deploy Pocket ACE Packages

Before you begin, make sure the removable device meets the hardware and disk space requirements. See "Portable Device Requirements" on page 441.

To use the graphical utility to deploy Pocket ACE packages

1 Navigate to the package location you specified in the New Pocket ACE Package wizard.

2 Double-click the `deploy.exe` file.

3 If the Enter Password dialog box appears, enter the deployment password.

4 Complete the VMware Pocket ACE Deploy Utility dialog box and click **Deploy**.

When you distribute the Pocket ACE, give it directly to the user and tell the user to keep the Pocket ACE secure until the user runs the ACE and changes the user password.

Use the Command-Line Utility to Deploy Pocket ACE Packages

The `bulkDeploy.exe` utility is a command-line version of the VMware Pocket ACE Deploy Utility dialog box (`deploy.exe`). Use `bulkDeploy.exe` commands in a batch file to deploy one or more Pocket ACE packages to the same or multiple target directories or removable devices.

Before you begin, make sure the removable device meets the hardware and disk space requirements. See “Portable Device Requirements” on page 441.

If you plan to deploy the Pocket ACE package to a custom folder rather than a removable drive, create the folder.

To use the command-line utility to deploy Pocket ACE packages

1 Open a command prompt and change directories to the package location you specified in the New Pocket ACE Package wizard.

For example, enter the following command:

```
cd C:\Documents and Settings\Administrator\My Documents\
Virtual Machines\ACE-Enabled Virtual Machine\Packages\Pocket ACE Package
```

2 Enter the following bulk deployment command and specify the necessary parameters:

```
bulkDeploy.exe <deployment_directory> <parameters>
```

The `<deployment_directory>` value can specify a removable drive or a custom folder.

Parameter	Usage
`-p`	Deployment password. Required when the package is password protected.
`-s`	Path to the `.vmx` file on the host. Use this parameter only if you use a `bulkDeploy.exe` file that is not located inside the same Pocket ACE package as the `.vmx` file you want to deploy.
`-q`	Parameter to turn off reporting the progress of the bulk deployment.
`-t`	Performs a speed test to determine whether the USB device and the host USB stack are fast enough for Pocket ACE. If the test is successful, 0 is returned. If it fails, a negative number is returned. This test is always done at runtime when the Pocket ACE is opened. It is done when you use the `bulkDeploy` command only if you use the `-t` parameter.

For example,

```
bulkDeploy.exe E: -p password -s C:\pocketACEPackage\VM\packagedVMX.vmx
               -q -t
```

3 (Optional) To deploy a Pocket ACE package to multiple locations, or to deploy multiple packages to the same or multiple locations, create a batch file with a `bulkDeploy.exe` command on each line.

Use quotation marks for paths that contain spaces. Following is an example of a batch file:

```
"C:\My VMs\vm_1\Packages\Pkg_1\bulkDeploy.exe" E: -p password -q -t
"C:\My VMs\vm_1\Packages\Pkg_1\bulkDeploy.exe" F: -p password -s
            "C:\My VMs\vm_2\Packages\Pkg_2\VM\Pkg_2.vmx" -q -t
"C:\My VMs\vm_1\Packages\Pkg_1\bulkDeploy.exe" F: -p password -s
            "C:\My VMs\vm_3\Packages\Pkg_3\VM\Pkg_3.vmx" -q -t
```

Run the Pocket ACE Instance

After you deploy a Pocket ACE package to a removable device, running it usually involves only plugging it in.

Before you begin, make sure that the host computer’s clock is set to the correct time. If you move a Pocket ACE from one host computer to another and the clock of the second host is earlier than the clock of the first, the Pocket ACE does not run.

When the ACE instance runs, its disk and checkpoint caches are initialized. If the Pocket ACE has a session on this host, that session continues. Otherwise a new session is started.

The checkpoint state and virtual disk are cached on the host during use and synchronized back to the portable device later. The checkpoint state and virtual disk are protected with the same encryption level used for the ACE instance on the portable device.

The Pocket ACE runs primarily from the host cache, although it occasionally reads from the parent disk on the portable device. The ACE instance does not write to the parent disk until synchronization.

To run a pocket ACE instance

1. Plug the portable device into the host computer.
2. If the host system's autorun configuration is not set to start the ACE instance automatically, do one of the following:
   - On Windows hosts, navigate to the removable device and run the Pocket ACE.

     Usually, starting the Pocket ACE manually is not necessary. The autorun program is included in the package and checks whether VMware Player is installed. If not, VMware Player is installed automatically.
   - On Linux systems, install VMware Player from the `Player` directory on the USB drive.

     For example, if the USB drive is mounted at `/media/USBFLASH`, navigate to `/media/USBFLASH/player.`
     - Install VMware Player as described in "Manually Install VMware Player on a Linux Host" on page 451.
     - Use VMware Player to open the `.vmx` file and start the ACE instance (see "Install the ACE Instance on a Single Linux Host" on page 452).

Installing ACE Packages 22

This chapter includes the following topics:

Installing an ACE Package on a Windows Host

If an end user's computer does not already have VMware ACE or VMware Player installed, the first time you install an ACE package, VMware Player is installed along with the ACE instance.

You can install ACE instances on one host at a time, or you can use the silent installation features of the Microsoft Windows Installer to quickly install an ACE instance on multiple computers.

Install an ACE Instance on a Single Windows Host

If VMware Player is not already installed on the machine, the installation program installs it before installing the virtual machine files that make up the ACE instance.

Before you begin, consider the following prerequisites:

- Make sure the host computer has enough disk space for the ACE instance.
- If this is the first installation of an ACE instance on the user's machine, a user with administrative privileges must run the installation. Only a user with administrative privileges can install and uninstall VMware Player.
- If the ACE instance includes a host policy, a user with administrative privileges must run the installation. A host policy is a host network access policy or a policy that restricts which virtual machines can run on a host. See "Setting Network Access Policies" on page 385 and "Control Which ACE Instances Run on a Host" on page 404.

  Only one set of host policies can be deployed to a particular host. If a package contains host policies and the host already contains host policies from another package, installation of the second package fails.

To install an ACE instance on a single Windows host

1. If VMware Player is not yet installed on the user's machine, log in to the host computer as the Administrator user or as a user who is a member of the Windows Administrators group.
2. Depending on whether you are installing from a CD, DVD, or network location, do one of the following:
   - For CDs and DVDs, insert the first disc.
   - For a network location, navigate to the location of the installer.
3. Find the `setup.exe` file and double-click it.
4. Follow the prompts.

Installing an ACE Package Silently on Multiple Windows Hosts

If you are installing a VMware ACE package on a number of Windows host computers, you might want to use the silent installation features of the Microsoft Windows Installer. This type of installation requires that the host computers have version 2.0 or later of the MSI runtime engine. This version of the installer is available in versions of Windows beginning with Windows XP. If the runtime engine is not installed, see "Install the MSI 2.0 Runtime Engine from an ACE Package" on page 449.

Install the MSI 2.0 Runtime Engine from an ACE Package

The installer for the MSI 2.0 runtime engine is included in the VMware ACE package as the `instmsiw.exe` file.

To install the MSI 2.0 runtime engine from an ACE package

1. On the host computer, open a command prompt.
2. Enter the following command:

```
instmsiw.exe /Q
```

For additional details on how to use the Microsoft Windows Installer, see the Microsoft Web site.

Install an ACE Instance on Multiple Hosts

You can use the Microsoft Windows Installer command-line interface to silently install an ACE instance on many computers. End users are not prompted for information during the installation process.

Before you begin, verify that the host computers have version 2.0 or later of the MSI runtime engine.

You can customize the basic package installation command to specify one or more of the following:

- Installation directory for the ACE instance
- Installation directory for VMware Player
- Installation without a desktop icon

You can also install an upgrade silently. An upgrade is always installed in the same directory or directories as the previous package.

To install the ACE instance on multiple hosts

1 On the host computer, open a command prompt.

2 Enter the following command:

```
setup.exe /s/v"/qn"
```

This command installs the package and VMware Player (if included) into the default locations and creates a shortcut for the ACE instance on the desktop. The default location for the VMware Player application is `C:\Program Files\VMware\VMware Player`.

The default location for the virtual machine files on a Windows XP system is `C:\Documents and Settings\All Users\Application Data\VMware\VMware ACE\<ACE_name>`.

3 To customize the package, enter the following command:

```
msiexec –i package.msi <installation_options>
```

Enter the command on one line. The installation options follow.

Option	Description
DESKTOP_SHORTCUTS	When set to 0, skips installation of the ACE instance shortcut on the desktop. The default is 1.
INSTALLDIR	Sets the root installation directory for the ACE instance.
PLAYER_INSTALLDIR	Sets the root installation directory for the VMware Player application.

The following example command illustrates the options and their usage:

```
msiexec –i package.msi DESKTOP_SHORTCUTS=0
INSTALLDIR="G:\packages"
PLAYER_INSTALLDIR="C:\VMware\VMware Player" /qn
```

Uninstall VMware Player or an ACE instance from a Windows Host

Uninstalling VMware Player does not uninstall the ACE instance. Only the Administrator user or a user who is a member of the Windows Administrators group can uninstall VMware Player.

Uninstalling an ACE instance does not uninstall the VMware Player application. When you remove an ACE instance, the ACE instance's data files, shortcuts, and registry entries are removed. You do not need to be an Administrator user to uninstall an ACE instance.

To uninstall VMware Player or an ACE instance from a Windows host

1. Go to **Start > Control Panel > Add or Remove Programs > Change or Remove Programs**.
2. Select the VMware Player program or the ACE instance and click **Remove**.
3. Follow the instructions in the wizard.
4. (Optional) If you used Pocket ACE on this host and want to remove the Pocket ACE cache to conserve disk space, delete the following folder:

   ```
   C:\Documents and Settings\<user>\Local Settings\Application
                 Data\VMware\Roaming VM cache\
   ```

   In this path, `<user>` represents a user-specific directory. If more than one user used Pocket ACE on the host, you must remove the directory for each user.

Installing an ACE Package on a Linux Host

If an end user's computer does not already have VMware ACE or VMware Player installed, VMware Player is automatically installed when you run the ACE package's `VMware-Player.bundle` file as root or sudo.

You can install ACE instances on one host at a time, or you can silently install an ACE instance on multiple computers.

Manually Install VMware Player on a Linux Host

Manually install VMware Player on systems where the end user does not have root access and does not already have VMware ACE or VMware Player installed.

To manually install VMware Player on a Linux host

1. In a terminal window, enter the following command to become the root user:

   ```
   su
   ```

2. Mount the ACE package, and locate the VMware Player installer in the package directory.

   Depending on whether the host is a 32-bit computer or a 64-bit computer, you see one of the following filenames:

   - `VMware-Player-i386.bundle`
   - `VMware-Player-x86_64.bundle`

3 Copy the `.bundle` file to a temporary directory on the hard drive.

For example, if you have a 64-bit computer and you want to put the file in the `/tmp` directory, enter the following command:

```
cp VMware-Player-x86_64.bundle /tmp
```

4 Enter the following command to change to the directory to which you copied the file:

```
cd /tmp
```

5 Enter the following command to run the installation program:

```
sh VMware-Player-<architecture>.bundle
```

The `<architecture>` value is either `i386`, for 32-bit systems, or `x86_64`, for 64-bit systems.

6 Follow the wizard prompts that appear.

On most Linux distributions, a GUI wizard appears. On Red Hat Enterprise Linux 5.1 and some other distributions, a command-line wizard appears. In the command-line wizard, to quickly scroll to the end of the license agreement prompt, press **q** and accept the agreement.

7 When installation is completed, enter the following command to exit from the `root` account:

```
exit
```

Install the ACE Instance on a Single Linux Host

Only the user who installs the ACE instance or a user with necessary permissions (such as root) is allowed to run that ACE instance. If VMware Player is not already installed on the machine, it is automatically installed when you run the ACE package's `VMware-Player.bundle` as root or sudo.

Before you begin, consider the following prerequisites:

- Make sure the host computer has enough disk space for the ACE instance.
- The ACE package must be accessible to the Linux user machines for installation.

- If this is the first installation of an ACE instance on the user machine, a root user must run the installation. Only a root user can install and uninstall VMware Player.
- If the ACE instance includes a host policy, a root user must run the installation. A host policy is a host network access policy or a policy that restricts which virtual machines can run on a host. See "Setting Network Access Policies" on page 385 and "Control Which ACE Instances Run on a Host" on page 404.

  Only one set of host policies can be deployed to a particular host. If a package contains host policies and the host already contains host policies from another package, installation of the second package fails.

To install an ACE instance on a single Linux host

1. Copy the `.bundle` file for the package to the host computer.
2. Open a terminal window and change to the package directory.
3. Enter the following command to run the installation program:

   ```
   sh VMware-Player-<architecture>.bundle
   ```

   The `<architecture>` value is either `i386`, for 32-bit systems, or `x86_64`, for 64-bit systems.
4. Follow the wizard prompts that appear.

   On most Linux distributions, a GUI wizard appears. On Red Hat Enterprise Linux 5.1 and some other distributions, a command-line wizard appears. In the command-line wizard, to quickly scroll to the end of the license agreement prompt, press **q** and accept the agreement.

Install an ACE Package Silently on Multiple Linux Hosts

You can silently install an ACE instance on many computers. End users are not prompted for information during the installation process.

To install the ACE instance on multiple Linux hosts

1. Copy the `.bundle` file for the package to the first host computer.
2. Open a terminal window and enter the following command:

   ```
   <path_to_package>/sh VMware-Player-<architecture>.bundle --required
   ```

   This command installs the package and VMware Player (if included) into the default locations. Only the license agreement prompt appears, if a EULA is included in the package.
3. Repeat this procedure for other hosts.

Prepare a Linux Host for Running in Kiosk Mode

On Linux hosts, if you plan to use kiosk mode to prevent users from accessing the host operating system, you must set some additional properties. If you do not prepare the host, users might be able to use keyboard shortcuts or other mechanisms to access the host when in kiosk mode.

Before you begin, create an ACE instance that uses a kiosk mode policy and install it on a Linux host. See "Setting Kiosk Mode Policies" on page 402 and "Installing an ACE Package on a Linux Host" on page 451.

The preferred window managers for running ACE instances in kiosk mode are F Virtual Window Manager (FVWM) and Metacity.

To prepare a Linux host for running in kiosk mode

1 Use a text editor to add the following lines to the host's ~/.vmware/preferences file:

```
pref.grabOnKeyPress = "TRUE"
pref.grabOnMouseClick = "TRUE"
```

2 Add the following lines to create a ServerFlags section in the /etc/X11/xorg.conf file:

```
Section "ServerFlags"
    Option  "DontZoom" "true"
    Option  "DontZap" "true"
    Option  "DontVTSwitch" "true"
EndSection
```

3 Restart the X session.

4 Manually disable all keyboard shortcuts in host's window manager.

5 If the Deskbar applet program is used in the panel on the host, remove it by right-clicking it and selecting **Remove from Panel**.

If you do not remove this applet, a user can press the keyboard combination for exiting kiosk mode and then press Alt+F3 to access the host file system.

6 To prevent the host's file browser from opening when a removable device is connected to the host, disable the applicable options in the host's system preferences and file browser preferences.

For example, open a file browser on the host and select **Edit > Preferences > Media** and deselect the **Browse media when inserted** check box. Also, from the host's **System** menu, select **Preferences > Removable Devices**, or similarly named tabs, and deselect the check boxes.

Uninstall VMware Player or an ACE Instance from a Linux Host

ACE users can uninstall only the ACE instances that they installed. Only the root user can uninstall others' ACE instances. Uninstalling an ACE instance does not uninstall the VMware Player application. When you uninstall an ACE instance, the ACE instance's data files, shortcuts, and registry entries are uninstalled.

Uninstalling VMware Player does not uninstall the ACE instance. Only the root user can uninstall VMware Player.

To uninstall VMware Player or an ACE instance from a Linux host

1 On the host computer, open a terminal window.

2 Do one or both of the following:

- To uninstall an ACE instance, enter the following command:

```
<path_to_instance_directory>./vmware-uninstall-ace.pl
```

- To uninstall VMware Player, enter the following command:

```
/usr/bin/vmware-uninstall
```

3 (Optional) If you used Pocket ACE on this host and want to remove the Pocket ACE cache to conserve disk space, delete the following directory:

```
/home/<user>/.vmware/roamcache
```

In this path, `<user>` represents a user-specific directory. If more than one user used Pocket ACE on the host, you must remove the directory for each user.

Upgrading ACE Instances to ACE 2.5

If you have ACE 2.0 instances, you can use Workstation 6.5 and ACE Management Server 2.5 to send new ACE 2.5 policies to end users.

Although new policies, such as Pock ACE cache settings and network adapter settings can be used on ACE 2.0 endpoints, the virtual machine version is not changed. To upgrade end users' virtual machine hardware version, you must create a full package and use it to replace the existing ACE instance.

When you uninstall the older ACE instance and VMware Player from the user's computer, the end user loses any data or custom settings stored in the old ACE instance. Take this consideration into account when choosing between upgrading the hardware version and continuing with the current hardware version but adding new ACE 2.5 policies.

Start and Use an ACE Instance

When you run an ACE instance, VMware Player starts and opens the instance. You start the instance in the same way that you start other applications on the host.

One exception is if the administrator configures the ACE instance to start and run in full screen mode when the host system starts. See "Setting Runtime Preferences Policies" on page 397.

Depending on how the ACE instance is configured, end users might be required to enter no password, one, or two passwords when they run the instance for the first time. The possibilities are:

- No passwords are required at the first run of the instance or on subsequent runs.
- You must enter one password at the first run, and that password is supplied to you by the administrator. On subsequent runs of the instance, no passwords are required.
- You must create a password at the first run. On subsequent runs, you must enter that password.
- You must enter an administrator-supplied password at the first run and also create a password. On subsequent runs, you must enter only the password that you created.

The administrator can also restrict how many characters or which characters can be used in passwords that end users create. See "Authentication Settings" on page 377.

To start and use an ACE instance

1. Depending on the host operating system, do one of the following:
   - On Windows hosts, use the desktop icon or the **Start** menu to start the ACE instance.
   - On Linux hosts, use the **Applications** menu or enter the following command in a terminal window:

     ```
     vmplayer <path_to__package_directory>/<name_of_ACE_vmx_file>.vmx
     ```
2. If prompted to enter or create a password, do so.
3. If the Enter Serial Number dialog box appears, do one of the following:
   - If your administrator provided a serial number, enter it.
   - If you need to purchase a license, click **Get Serial Number**.

4 Click inside the VMware Player window to begin using the guest operating system and the applications installed in the ACE instance.

  You can use the operating system and applications just as you would if they were running directly on a physical computer.

5 (Optional) To change a password that you created, choose **VMware Player** > **Change Password**.

6 (Optional) For more information about using VMware Player, choose **VMware Player** > **Help**.

Change Default Kiosk Mode Startup Behavior

If an ACE instance is configured to run in kiosk mode, the virtual machine runs in full screen mode and does not display the ACE menu bar or ACE Player online help.

Before going into kiosk mode, a dialog box appears, requiring the user to consent to entering kiosk mode. For more information, see "Setting Kiosk Mode Policies" on page 402.

You can use a command-line command to start an ACE instance in kiosk mode without displaying the usual warning message.

You can also start the ACE instance so that it is not in kiosk mode. You can then use the VMware Player menus to change preference settings or enter administrator mode if the ACE instance is configured for that mode.

To change default kiosk mode startup behavior

1 Open a command prompt on Windows hosts or a terminal window on Linux hosts.

2 To suppress the dialog box usually shown at startup, do one of the following:

- On Windows, enter the following command:

  ```
  <path>\vmplayer.exe -k "<config-file>"
  ```

  In this command, `<path>` is the path on your system to the VMware Player application file and `<config-file>` is the path to the virtual machine configuration (`.vmx`) file.

- On Linux, enter one of the following commands:

  - `vmplayer -k "<config-file>"`
  - `vmplayer --noKioskWarning "<config-file>"`

In these commands, `<config-file>` is the path to the virtual machine configuration (`.vmx`) file.

3 To start the ACE instance without entering kiosk mode, do one of the following:

- On Windows, enter the following command:

  ```
  <path>\vmplayer.exe -K "<config-file>"
  ```

  Notice the capital **K**. In this command, `<path>` is the path on your system to the VMware Player application file and `<config-file>` is the path to the virtual machine configuration (`.vmx`) file.

- On Linux, enter one of the following commands:

  - **`vmplayer -K`** `"<config-file>"`
  - **`vmplayer --forceNoKiosk`** `"<config-file>"`

In these commands, `<config-file>` is the path to the virtual machine configuration (`.vmx`) file.

4 If you use a command to start the instance without entering kiosk mode, enter the administrator password when prompted.

This procedure describes typing the command at the command line, but you can also use the command to create a batch file or a desktop shortcut. See "Using Startup Options in a Windows Shortcut" on page 469.

Use Multiple Virtual Machines in Kiosk Mode

You can start multiple ACE instances that are configured to run in kiosk mode. You can then switch between virtual machines by using a keyboard shortcut.

Before you begin, create and package multiple ACE instances that use the same administrator password for kiosk mode and the same hot-key combination for exiting kiosk mode. See "Setting Kiosk Mode Policies" on page 402.

When multiple virtual machines run in kiosk mode, end users can press the hot-key combination along with the right arrow or left arrow key to switch to the next or previous virtual machine. For example, if the hot-key combination is Ctrl+Alt, users can press Ctrl+Alt+right arrow to switch to the next virtual machine or Ctrl+Alt+left arrow to switch to the previous virtual machine.

To use multiple virtual machines in kiosk mode

1 Install the ACE instances on the host machine.

2 Use the following examples to write a batch file or script to start the virtual machines:

Windows batch file:

```
cd Program Files\VMware\VMware Player
start vmplayer.exe –k "C:\Documents and Settings\user1\My Documents\My
               Virtual Machines\ace1\ace1.vmx"
sleep 20
start vmplayer.exe –k "C:\Documents and Settings\user1\My Documents\My
               Virtual Machines\ace2\ace2.vmx"
sleep 20
start vmplayer.exe –k "C:\Documents and Settings\user1\My Documents\My
               Virtual Machines\ace3\ace3.vmx"
```

Linux script file:

```
#!/bin/bash
vmplayer –k ~/vmware–ace/ace1/ace1.vmx & sleep 20
vmplayer –k ~/vmware–ace/ace2/ace2.vmx & sleep 20
vmplayer –k ~/vmware–ace/ace3/ace3.vmx &
```

The –k flag suppresses the kiosk mode dialog box so that you do not need to click **OK** to enter kiosk mode.

3 If any virtual machines that are not set to run in kiosk mode are open or running on the host, power them off and close them.

The script cannot start and run virtual machines in kiosk mode if any non-kiosk-mode virtual machines are open.

4 Run the batch file or script to start the virtual machines in kiosk mode.

The virtual machines are started in the order listed in the batch file or script. The first virtual machine started defines the administrator password for kiosk mode and the hot-key combination for exiting kiosk mode. If a subsequent virtual machine in the list has a different password or hot-key, it does not start. If a subsequent virtual machine in the list is not configured to start in kiosk mode, it is not allowed to start.

Install an ACE Client License

An ACE client license is a device-specific license. Devices include PCs, laptops, and portable media devices such as USB flash drives (storing a Pocket ACE). The details of the licensing terms are provided in the end user license agreement (EULA) for ACE published on www.vmware.com.

A licensed device can run any number of ACE instances. The ACE client license is associated with the device it is installed on and is not restricted to a specific ACE instance.

If you purchase a volume license, you do not need to install client licenses.

To install an ACE client license

1. Obtain the ACE client license serial number from your ACE administrator.
2. Double-click the desktop shortcut for the installed ACE instance.
3. At the prompt, enter the serial number in the appropriate field and enter your name and the organization name in the dialog box.
4. Click **OK**.

Change the ACE Client License

You can use a VMware Player menu command to change or update a license.

To change the ACE Client License

1. Choose **VMware Player > Enter ACE Client License**.
2. Do one of the following:
   - Enter the serial number in the dialog box.
   - If you need to purchase a license, click **Get Serial Number**.
3. Click **OK**.

Quit VMware Player

As a best practice, quit VMware Player before you shut down the host computer.

To quit VMware Player

Choose **VMware Player > Exit** on Windows hosts or **VMware Player > Quit** on Linux hosts.

Depending on the configured exit behavior, the ACE instance is suspended or shuts down and the window closes.

Also depending on the configuration, end users might be able to change the exit behavior in the Preferences dialog box (**Player > Preferences**).

Troubleshooting Tools

VMware ACE includes some troubleshooting tools that allow administrators and help desk assistants to fix some common problems that users have with ACE instances, such as forgotten user passwords. The tools are:

- For standalone ACE instances:
  - The ACE Tools, which is a command-line tool. See "Using the vmware-acetool Command-Line Tool" on page 461.
  - The hot fix feature, which users access from buttons in dialog boxes. See "Respond to Hot Fix Requests" on page 463.
- For managed ACE instances, see the *VMware ACE Management Server Administrator's Guide*.

Using the vmware-acetool Command-Line Tool

The `vmware-acetool` command-line tool is a troubleshooting tool that enables ACE administrators to fix a limited set of problems for standalone ACE instances directly on an ACE user's system.

You can provide the following solutions with `vmware-acetool`:

- Set the user's password, so the user can run the ACE instance.
- Set copy protection, so the user can run the ACE instance in a new location.
- Set the expiration date, so the user can continue to use an ACE instance that is past its scheduled expiration date.

The configuration file (`.vmx` file) for the ACE instance must be on the ACE user's machine. That is, you cannot use `vmware-acetool` to make fixes to files associated with the instance unless the configuration file is on the same machine as those files.

You can actually use the `vmware-acetool` program to reset passwords and fix expiration dates on another machine, but you must have the .`vmx`, .`vmpl`, and `ace.dat` files from the user all set up in the same directory. The following is an example of a `vmware-acetool` command:

```
vmware-acetool <command> <ACEconfigurationfile> <parameters>
```

Table 22-1. Commands and Parameters for `vmware-acetool`

Command	Parameters	Description
`setPassword`	Path to recovery key file	Set the ACE instance's password.
`setExpirationDate`	New expiration date	Set the ACE instance's expiration date.
`allowCopy`		Allow the ACE instance to run from its current location.
`updateCurrentTime`		Update the internal policy clock of an ACE instance to the current time.
`cloneToVM`	Net clone configuration file Path to recovery key file	Clone a regular virtual machine from an ACE-enabled virtual machine.

Password Prompts

All commands prompt for the administrative tools password. See "Setting Administrator Mode Policies" on page 401.

The `setPassword` command also prompts for the recovery key password for the private recovery key file, a new ACE instance password, and confirmation of that new password. See "Set a Recovery Key for Encrypted ACE Instances" on page 380. Following is an example of the command:

```
vmware-acetool setPassword myACE.vmx recKey.priv
```

Expiration Dates

The new expiration date can be passed as one of the following:

- A number of days from the current date
- An absolute date in the format `YYYY-MM-DD`
- A start date and an end date in the format `YYYY-MM-DD YYYY-MM-DD`
- The special value `"never"`, so that the instance never expires
- The special value `"expired"`, so that the instance expires immediately

Following are examples of the command:

```
vmware-acetool setExpirationDate myACE.vmx 30
```

```
vmware-acetool setExpirationDate myACE.vmx 2007-06-16
```

```
vmware-acetool setExpirationDate myACE.vmx "never"
```

```
vmware-acetool allowCopy myACE.vmx 30
```

Respond to Hot Fix Requests

If you enable the hot fix feature for standalone ACE instances, users can easily request help to resolve the following problems:

- Lost or forgotten password
- Expired ACE instance
- Copy-protected ACE instance run from a new location

For information about enabling the hot fix feature, see "Setting Hot-Fix Policies for Standalone ACE Instances" on page 403. For information about setting a recovery key, which you must have to send a hot fix for a lost or forgotten user password, see "Set a Recovery Key for Encrypted ACE Instances" on page 380.

When the hot fix feature is enabled, if an end user sees a notification that the ACE instance is expired or copy protected, a **Request Hot Fix** button appears in the dialog box. The user clicks this button, which launches the Hot Fix Request wizard. This wizard generates a hot fix request file. The user can submit this file to the administrator as an email attachment or in some other way.

To respond to a hot fix request

1. When you receive the hot fix request file, save it to a location that you can access from the administrator machine where Workstation is installed.
2. Open the ACE-enabled virtual machine for the instance that requires the hot fix.
3. Choose **File** > **Open**.
4. Navigate to the location of the hot fix request file and click **Open**.

   A hot fix tab opens in the Workstation window. The hot fix tab displays the user's name and email address, the problem that led to the hot fix request, and any additional note the user entered.

5 Click **Approve hot fix**.

6 Enter the appropriate information in the dialog box.

7 Select one of the following methods for sending the response:

   - Click **Send hot fix** on the hot fix tab and click **OK**.
   - Send the hot fix file. It is in the same folder as the hot fix request. The file extension for the fix file is `.vmhf`.

The display on the hot fix tab shows the status of the hot fix request, approved or denied, and the date on which you took action.

The user applies the hot fix by double-clicking the hot fix file.

Troubleshooting Setup Issues

Occasionally ACE end users have problems logging in to a domain after running the **Revert to Reimage Snapshot** command. They might sometimes also have problems with domain validation and name resolution.

Login Issues After Reverting to a Reimage Snapshot

Problem: The ACE user cannot log the ACE instance back in to a domain after choosing **VMware Player > Troubleshoot > Revert to Reimage Snapshot**.

Description: The ACE instance has a Windows guest operating system installed and the machine account password for the domain is periodically renewed by default. If the password is renewed by the time the user reverts the ACE instance to the snapshot, the snapshot’s password is invalid and login fails.

Solution: To avoid this problem, ensure that the following security policy is enabled: **Refuse machine account password changes.**

You can enable this policy on the ACE-enabled virtual machine (affecting all instances created from it) or on the primary domain controller. For details about how to change the policy, see the following Microsoft articles:

- Local Security Policies – Go to the Microsoft Support site, enter the Microsoft knowledge base article ID 175468 in the search criteria, and click the first search result.
- PDC Security Policies – Go to the Microsoft TechNet Web site and enter Domain controller: Refuse machine account password changes, in the search criteria.

Issues with Domain Validation or Name Resolution

Problem: When you try to join an ACE-enabled virtual machine to a domain, domain validation or name resolution does not work.

Description: Some ACE-enabled virtual machines with certain network configurations might demonstrate these problems.

Solution: Consult the Microsoft knowledge base article. Go to the Microsoft Support Web site, enter the Microsoft knowledge base article ID 314108 in the search criteria, and click the first search result.

Issues with Domain Joins for Windows Vista Guests

Problem: An ACE instance running under a Windows Vista guest operating system cannot join the local domain and instance customization failed with the message "`NetDomainJoin function Error 1722: Could not join domain.`"

Description: ACE instances running in the Windows Vista operating system might have this problem.

Solution: Tell the user to power off the instance and power it on again to retry instance customization. The problem is intermittent and restarting might solve the problem.

Workstation Command-Line Reference

A

This appendix discusses the command-line options that are available for the `vmware` program.

For information about using the `vmware-fullscreen` command to use full screen switch mode, see "Using vmware-fullscreen to Run a Virtual Machine" on page 361.

For information about using the `vmrun` program to operate teams or virtual machines from the command line, see manual called *Using vmrun to Control Virtual Machines*.

This appendix includes the following topics:

- "Startup Options for Workstation and Virtual Machines" on page 467
- "Using Startup Options in a Windows Shortcut" on page 469

Startup Options for Workstation and Virtual Machines

Table A-1 describes options available when you run Workstation from the command line. You can type these commands in a Linux terminal window or at the Windows command prompt. You can also create scripts to run multiple commands.

The syntax for this command is:

- On a Linux host operating system:

```
/usr/bin/vmware [-n] [-x] [-X] [-m] [-t] [-q] [-s <variablename>=<value>]
                [-v]
                [/<path_to_virtual_machine>/<virtual_machine_name>.vmx]
                [X toolkit options]
```

- On a Windows host operating system:

```
C:\Program Files\VMware\VMware Workstation\vmware.exe [-B] [-n] [-x] [-X]
                [-t] [-q] [-s <variablename>=<value>] [-v]
                [<path_to_virtual_machine>\<virtual_machine_name>.vmx]
```

Table A-1. Command-Line Options for the vmware Program

Option	Description
`-n`	Opens a new Workstation window.
`-B`	(Windows hosts only) Opens a new Workstation window but hides the sidebar and toolbars. Only the tabs of open virtual machines are shown. Using this option has the same effect as clicking the **Workstation** icon in the upper-left corner of the Workstation window and choosing **Hide Controls** from the menu that appears.
`-t`	Opens a virtual machine or team in a new tab in the existing Workstation window.
`-x`	Powers on the virtual machine when Workstation starts. This is equivalent to clicking the **Power On** button in the Workstation toolbar.
`-X`	Powers on the virtual machine and switches the Workstation window to full screen mode.
`-m`	Starts the program in quick switch mode.
`-q`	Closes the virtual machine's tab when the virtual machine powers off. If no other virtual machine is open, it also exits Workstation. This option is useful when the guest operating system can power off the virtual machine.
`-s`	Sets the specified variable to the specified value. Any variable names and values that are valid in the configuration file can be specified on the command line with the `-s` switch.
`-v`	Displays the product name, version, and build number.
`<path_to_VM_or_team>`	Launches a virtual machine by using the specified virtual machine or team configuration file (`.vmx` or `.vmtm` file).

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

X toolkit options are not relevant on a Windows host.

Using Startup Options in a Windows Shortcut

The most convenient way to use the startup options is to incorporate them into the command that a Windows shortcut generates.

To create the shortcut, right-click the shortcut and click **Properties**. In the **Target** field, add any switches to use after the `vmware.exe` filename. For example, the following command launches the Windows Me virtual machine specified, powers it on, and switches to full screen mode:

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

Enclose the entire command string in quotation marks. The configuration file has a `.vmx` extension by default.

Using the Integrated Virtual Debugger for Eclipse

B

This document contains the following sections:

- "Installation Requirements for the Integrated Virtual Debugger Environment" on page 472
- "Managing Virtual Machine Launch Configurations" on page 477
- "Running and Debugging Applications in Virtual Machines" on page 480

The Integrated Virtual Debugger for Eclipse provides a configurable interface between Eclipse and virtual machines, making it easy to develop and debug applications that run in multiple operating system environments on a single PC. Debugging your applications in virtual machines enables you to reproduce and record errors while maintaining the integrity of the host machine.

You can perform typical debugging tasks such as pausing at breakpoints, stepping through code, and viewing and modifying the state of your application, all without impacting the host environment. The Integrated Virtual Debugger also enables you to:

- Manage launch configuration settings for application execution and debugging in virtual machines.
- Start an application debugging session in a virtual machine.
- Start an application in a virtual machine without debugging.
- Start a debugging session that attaches to a process already running in a virtual machine.

Using Eclipse launch configurations, you can choose a virtual machine in which to run your application and determine how the application is executed. When configured, the Integrated Virtual Debugger finds the virtual machine, powers it on if necessary, sets up the environment based on your configuration settings, and starts or attaches to the application.

To configure how an application is started in a virtual machine, you can specify:

- Name of the virtual machine (`.vmx` configuration file).
- Account credentials for guest console.
- (Optional) Path to the Java Virtual Machine (JVM) on the guest system.
- (Optional) Locations of folders to be shared between the host and the guest.
- (Optional) Actions to perform before launching an application from Eclipse, including:
  - Revert to the most recent snapshot.
  - Run specified pre-execution commands.
- (Optional) Actions to perform after an application launched from Eclipse is terminated, including:
  - Run specified post-execution commands (for example, to perform cleanup tasks).
  - Set the virtual machine state to:
    - Suspended (default)
    - Revert to the most recent snapshot
    - Powered off

Installation Requirements for the Integrated Virtual Debugger Environment

Review the requirements and recommendations in this section before following the instructions in Chapter 2, “Installing and Upgrading VMware Workstation,” on page 37 to install the Eclipse Integrated Virtual Debugger as an optional component of Workstation 6.5. This section describes the requirements for host and guest systems, Eclipse, and the Java Runtime Environment (JRE).

When you install the Integrated Virtual Debugger:

- The Integrated Virtual Debugger plug-in, `ivd.jar`, Foundry Java bindings, and the `plugin.xml` launch configuration file are placed in the `com.vmware.bfg_1.0.0` subdirectory of the Eclipse plug-in directory.
- After you restart Eclipse, the **Debug** menu includes the new launch configuration types **VMware attach to application** and **VMware execute Java application**. These launch configuration types have a **VMware** tab that enables you to configure virtual machine settings.

You can debug in multiple virtual machines simultaneously. You can also debug multiple sessions in a single virtual machine.

Host System Requirements

The Integrated Virtual Debugger can run on any supported host operating system that is running Workstation 6.5 and has Eclipse installed. Eclipse must be running on the same system as Workstation 6.5. For more information about, see "Eclipse Requirements" on page 474.

Supported Host Operating Systems

The Integrated Virtual Debugger supports the following Windows 32-bit, Linux 32-bit, and Linux 64-bit host operating systems.

Table B-1. Windows and Linux Host Operating Systems

Operating System	Edition
Windows 32-bit	Windows Vista Enterprise Edition, SP1 Windows Vista Business Edition, SP1 Windows Vista Home Basic and Premium Editions, SP1 Windows Vista Ultimate Edition, SP1, SP3 Listed versions are also supported with no service pack.
	Windows XP Home Edition with SP2 or later service pack Windows XP Professional with SP2 or later service pack
	Windows 2000 Server SP3, SP4 Windows 2000 Professional, SP3, SP4 Windows 2000 Advanced Server, SP3, SP4
Windows 64-bit	Windows XP Professional with SP1 or later service pack

Table B-1. Windows and Linux Host Operating Systems (Continued)

Operating System	Edition
Linux 32 and 64-bit	Red Hat Enterprise Linux WS 4.5 (Beta, formerly called 4.0 Update 5) Red Hat Enterprise Linux AS 4.0, updates 1, 2, 3, 4 Red Hat Enterprise Linux ES 4.0, updates 1, 2, 3, 4 Red Hat Enterprise Linux WS 4.0, updates 1, 2, 3, 4 Red Hat Linux 9.0 — stock 2.4.20-8, upgrade 2.4.20-20.9
	Ubuntu Linux 6.10 and 6.06

NOTE Windows 64-bit host operating systems are not currently supported.

Supported JRE Versions

The host system must be running a JRE meeting Java 2 Platform Standard Edition (J2SE) 5.0 or higher specifications. J2SE consists of the JRE and developer tools for compiling, debugging, and running applications written in the Java language.

NOTE Eclipse displays the error message `unable to load class` if an unsupported version of J2SE is being used on the host system.

Eclipse Requirements

You must have Eclipse 3.2 or 3.3 installed on the host. On Windows Vista hosts, you must have Eclipse 3.2.2 or 3.3 installed. Only the Java language is supported.

By default the Eclipse 3.3 launcher loads the JVM in a manner that prevents certain Java Native Interface (JNI) calls used in the VMware plugin from working on 32-bit Linux hosts. A workaround for this issue is to specify the location of the JVM binary using the `–vm` flag, for example **`/opt/eclipse/eclipse –vm /usr/bin/java,`** when launching Eclipse 3.3. For more information on the Eclipse 3.3 launcher, go to the eclipsepedia Web site and search for the **Equinox Launcher**.

NOTE You cannot have GNU Compiler for the Java programming language (GCJ)/GNU Interpreter for Java (GIJ) installed on either the host or guest operating system.

Virtual Machine Requirements

The Integrated Virtual Debugger is supported on any Workstation 6.5 virtual machine that is running a supported Windows or Linux guest operating system.

Supported Guest Operating Systems

This section provides a simplified list of guest operating systems supported for debugging in virtual machines. For the most recent list of supported guest operating systems, including detailed information about the specific operating system versions, service packs, and updates supported, see the *VMware Guest Operating System Installation Guide* on the VMware Web site. This guide also provides notes on installing the most common guest operating systems.

NOTE Operating systems that are not listed are not supported for debugging in a virtual machine.

The Integrated Virtual Debugger supports the following Windows 32-bit, Windows 64-bit, Linux 32-bit, and Linux 64-bit guest operating systems.

Table B-2. Windows and Linux Guest Operating Systems

Processor Type	Operating System Edition
Windows 32-bit	Windows Vista (all editions except Vista Home Edition, which cannot be run in a virtual machine due to Microsoft licensing restrictions.)
	Windows Server 2003 Enterprise Edition and R2
	Windows XP Professional Windows Home Edition
	Windows 2000 Professional Windows 2000 Server Windows 2000 Advanced Server
Windows 64-bit	Windows Vista x64 Edition (Aero and 3-D effects not yet supported)
	Windows Server 2003 x64 Edition
	Windows XP Professional x64

Table B-2. Windows and Linux Guest Operating Systems (Continued)

Processor Type	Operating System Edition
Linux 32 and 64-bit	Red Hat Linux 8 and 9
	Red Hat Enterprise Linux Advanced Server Enterprise Server Workstation 4 and 5
	Ubuntu Linux 6.10 and 6.06
	SUSE Linux 10 SUSE Linux Enterprise Server 10

VMware Tools Requirements

Make sure that the version of VMware Tools on the guest operating system matches the version of Workstation 6.5 (of which the Integrated Virtual Debugger is a component) on the host.

Update the Eclipse Build Settings to Use a 1.4.x JRE

You cannot have GCJ installed on the guest operating system.

The guest operating system must be running JRE 1.4.2 or higher. If you are not using JRE 5.0 on the guest, you must update the build settings in Eclipse to use a 1.4.x JRE on the guest.

To update the Eclipse build settings to use a 1.4.x JRE

1. In the Eclipse Package Explorer, right-click the topmost folder (Project item) and choose **Properties**.
2. In the left pane of the Properties page, select **Java Compiler**.
3. Select **Enable project specific settings**, and set the Java Development Kit (JDK) Compliance Compiler compliance level to `1.4`.

Installing PSAPI.DLL on Windows NT

On Windows NT, you must install the `psapi.dll` library file to retrieve process status information so that the Integrated Virtual Debugger can attach to a process. You can download `psapi.dll` from the Microsoft Developer Network.

Disabling the Firewall on Linux Guest Systems

You must disable the firewall on Linux guest operating systems. The Integrated Virtual Debugger opens an available port (searching from port 49152) for each debugging session.

Configure the Firewall on Windows Guest Systems

If you are using a 1.4.x JRE on Windows guest systems, you must disable the firewall or allow incoming connections to the JVM. If your Windows system (such as Windows XP SP2, Windows 2003, and Windows Vista) allows you to configure exceptions to the firewall, you can add the JVM to the exceptions list.

To configure the firewall on Windows guest systems

1 Choose **Start > Control Panel > Windows Firewall** and select the **Exceptions** tab.

2 Click **Add Program** and browse to the Java executable.

3 Click **OK**.

4 (Optional) On Windows Vista guests, you might have to restart the firewall after configuring it to allow incoming connections to the JVM.

Managing Virtual Machine Launch Configurations

You can manage configuration settings for each virtual machine in which you want to debug applications. Integrated Virtual Debugger launch configurations determine which virtual machine to run the application in and how the application is executed.

The launch configuration types **VMware attach to application** and **VMware execute Java application** have a **VMware** tab. The values you enter in the **VMware** tab determine virtual machine configuration settings. Once configured, you can start and attach to applications in virtual machines from the Eclipse **Debug** and **Run** menus.

Use Application Configurations to Start Applications in a Virtual Machine

This section describes how to create, duplicate, or edit a launch configuration to start an application in a virtual machine.

To use application configurations to start applications in a virtual machine

1 Choose **Run > Debug.**

The **Debug** page is displayed. You can create, manage, and run configurations from this page.

2 To create a launch configuration or edit an existing configuration, do one of the following:

- Create a configuration based on default settings by selecting **VMware execute Java application** in the left pane, and clicking the **New launch configuration** icon at the top of the pane.
- Create a configuration based on another configuration by selecting the configuration you want to duplicate under **VMware execute Java application** in the left pane, and clicking the **Duplicates the currently selected configuration** icon at the top of the pane.
- Edit an existing configuration by selecting the configuration you want to edit under **VMware execute Java application** in the left pane.

3 Perform the remaining steps in the **VMware** tab of the right pane.

4 Browse to choose a virtual machine from the drop-down menu of recently used and currently running virtual machines.

5 Enter your account credentials to access the guest console.

6 (Optional) If you want to use a JVM other than the one that is automatically selected, select an alternate JVM path.

7 (Optional) Expand the list of shared folders to add, edit, or remove folders to be shared between the host and the guest systems.

For each folder, enter the share name and the location on the host system. By default, the project folder is shared.

8 (Optional) Indicate actions to be performed before the application is launched:

- Select **Set virtual machine state to most recent snapshot** to revert to the most recent snapshot before the application is launched.
- Select **Run script** and enter one or more shell commands to be executed in the guest operating system before the application is launched. No syntax checking is performed. Either enter one command per line, or enter multiple commands on the same line using a semicolon as a separator.

9 (Optional) Indicate actions to be performed after the application has terminated:

- Select **Run script** and enter one or more shell commands to be executed in the guest operating system after the application has terminated. No syntax checking is performed. Either enter one command per line, or enter multiple commands on the same line using a semicolon as a separator.
- Select one of the **Set virtual machine state** options.

10 Click **Apply**.

If newly created, the launch configuration is added to the left pane.

Use Application Configurations to Attach to Applications Running in a Virtual Machine

This section describes how to create, duplicate, or edit a configuration that attaches to a running application in a virtual machine.

To use application configurations to attach to applications running in a virtual machine

1 Choose **Run > Debug**.

2 Do one of the following:

- Create a configuration based on default settings by selecting **VMware attach to application** in the left pane, and clicking the **New launch configuration** icon at the top of the pane.
- Create a configuration based on another configuration by selecting the configuration you want to duplicate under **VMware attach to application** in the left pane and clicking the **Duplicates the currently selected configuration** icon at the top of the pane.
- Edit an existing configuration by selecting the configuration you want to edit under **VMware attach to application** in the left pane.

3 Perform the remaining steps in the **VMware** tab of the right pane.

4 Browse or choose a virtual machine from the drop-down menu of recently used and currently running virtual machines.

5 Enter your account credentials to access the guest console.

6 Click **Apply**.

If newly created, the launch configuration is added to the left pane.

Delete a Configuration

Before you delete a configuration, make sure the virtual machine is powered off or suspended.

To remove a configuration

1 Choose **Run > Debug**.

2 In the left pane, select one or more configurations you want to delete and click the **Delete selected launch configuration(s)** icon at the top of the pane.

Running and Debugging Applications in Virtual Machines

After you create the appropriate launch configurations, the Integrated Virtual Debugger enables you to:

- Start an application debugging session in a virtual machine.
- Start an application in a virtual machine without debugging.
- Start a debugging session that attaches to a process already running in a virtual machine.

Start an Application Debugging Session in a Virtual Machine

Do not suspend a virtual machine while the Integrated Virtual Debugger is connected to an application. If you do, the Integrated Virtual Debugger disconnects from the application.

To start an application debugging session in a virtual machine

1. Begin the session in one of the following ways:

   - From the **Debug** menu, choose the configuration for the application to start debugging.

   - In the **Debug** page, select the configuration under **VMware execute Java application** in the left pane and click **Debug** in the right pane.

2. Perform debugging tasks as you would in a local debugging environment.

Start an Application in a Virtual Machine Without Debugging

You can start an application without debugging in any configured virtual machine.

To start an application in a virtual machine without debugging

Begin the session in one of the following ways:

- From the **Run** menu, choose the configuration for the application to start.

- In the **Run** page, select the configuration under **VMware execute Java application** in the left pane and click **Run** in the right pane.

Attach to an Application Running in a Virtual Machine

Do not suspend a virtual machine while the Integrated Virtual Debugger is connected to an application. If you do, the Integrated Virtual Debugger will disconnect from the application.

To attach to an application running in a virtual machine

1. In the **Debug** page, select the configuration under **VMware attach to application** in the left pane and click **Debug** in the right pane.

2. Select the process you want to attach to.

   If more than one instance of the Java application is running in the virtual machine, a dialog box appears with a list of the running instances, each identified by their process ID, port number, and arguments.

3. Perform debugging tasks as you would in a local debugging environment.

Using the Integrated Virtual Debugger for Visual Studio

C

The Integrated Virtual Debugger for Visual Studio provides a configurable extension to Visual Studio for debugging programs in virtual machines. The Integrated Virtual Debugger simplifies virtual machine management and provides new debugging features for replaying a recorded application execution. This chapter includes the following sections:

The Integrated Virtual Debugger lets you perform the following tasks:

- Manage configuration settings for application execution and debugging in virtual machines.
- Start a debugging session in a virtual machine.
- Start an application in a virtual machine without debugging.

- Start a debugging session that attaches to a process already running in a virtual machine.
- Debug a recording of a program's execution.
- Execute a program in reverse.

You can install the Integrated Virtual Debugger on most Windows host systems that are running Workstation 6.5 and have a supported version of Visual Studio installed. For more information about installation, see Chapter 2, "Installing and Upgrading VMware Workstation," on page 37.

Debugging Modes of the Integrated Virtual Debugger

The Integrated Virtual Debugger includes two different debugging modes, each supporting different features and usage scenarios. They are the remote debugging and the replay debugging modes. Only one mode can be used during a single debugging session.

Remote debugging lets you debug an application in a virtual machine. It is often necessary to debug an application in many different environments. For example, you can debug using different versions of Windows, service packs, DLLs installed, and so on. Using virtual machines for debugging purposes provides a convenient alternative to debugging on physical machines. However, managing these virtual machines and their files might be difficult. The remote debugging mode of the Integrated Virtual Debugger addresses these issues by powering virtual machines on and off, managing the application to debug, starting the application to debug in a virtual machine, and attaching to the application. The remote debugging mode makes a remote debugging session as convenient as a local debugging session. For more information, see "Using the Remote Debugging Mode" on page 485.

Replay debugging lets you record the execution of an application in a virtual machine and debug the recorded form of the application. This feature is experimental in the current release. For more information, see "Using the Replay Debugging Mode" on page 499.

Replay debugging has the following benefits over traditional debugging:

- Bugs captured in a recording are reproduced exactly during debugging. Recorded bugs can be examined in Visual Studio repeatedly, and always exhibit the same behavior. This benefit of replay debugging makes it a powerful tool for fixing bugs that cannot be reliably reproduced due to subtle variations in timing or input.
- No debugging is performed during the recording process, so debugging activities do not affect the normal execution of an application. This is useful for applications that interact with other processes or remote servers. For example, TCP connections do not time out because there is minimal delay while a recording is created.
- A feature simulating reverse execution is available in the replay debugging mode. In a traditional debugging context, you rerun an application and try to stop early enough to find the source of a bug. Reverse execution makes it easier to find the cause of a bug. For example, if your data structure is corrupted, you set a data breakpoint (that is, watchpoint) on the corrupted data and execute backward until you encounter the code that caused the corruption.

Using the Remote Debugging Mode

The remote debugging mode of the Integrated Virtual Debugger simplifies the task of debugging applications in virtual machines using the remote debugging feature of Visual Studio. When you use remote debugging using Visual Studio, you have to manually manage the virtual machine, manage the files in the virtual machine, start the application to debug in a virtual machine, and attach the Integrated Virtual Debugger to an application. Remote debugging provides the same debugging options as a standard remote debugging session using Visual Studio, however it eliminates some of the tedium of standard remote debugging.

The remote debugging mode differs from the replay debugging mode in that the remote debugging mode debugs a live execution of an application. Replay debugging mode debugs a recording of an application. For more information, see “Using the Replay Debugging Mode” on page 499.

Requirements and Recommendations for Remote Debugging

Visual Studio must be running on the same machine as Workstation.

Supported Versions of Visual Studio

Visual Studio 2005 and 2008 Professional and Team Systems editions are supported. These versions of Visual Studio allow remote debugging on Windows systems, with the exceptions of Windows NT, Windows Vista Starter Edition, and Windows XP Home editions. The Integrated Virtual Debugger uses the features of the Remote Debug Monitor (`msvsmon.exe`) to communicate with the guest operating system.

For more information on Visual Studio 2005, go to the Microsoft Developer Network Web site and search for **Visual Studio 2005 Service Pack 1 (SP1)**.

Running the Integrated Virtual Debugger on Windows Vista Starter Edition and Windows XP Home Edition is not supported. For information about issues running Visual Studio on Windows Vista Starter Edition, go to the Microsoft Developer Network Web site, enter the search keywords **Visual Studio 2005 on Windows Vista Issue List**, and search for information on **Windows Vista Starter Edition** or **Windows XP Home**.

Supported Programming Languages

Remote debugging supports C/C++ (Native and Managed), C#, and Visual Basic programming languages.

Host System Requirements

The Integrated Virtual Debugger can run on most Windows host operating systems that Workstation 6.5 supports, listed in “32-bit” on page 25 and “64-bit” on page 26.

Only Enterprise Edition SP1 and R2 of Windows Server 2003 are supported. If remote debugging is not working on a Windows Vista host, try the following:

- Manually configure the firewall to allow traffic from Visual Studio.
- Run Visual Studio with Administrator permissions.

  For more information, go to the Microsoft Developer Network Web site and search for **Visual Studio 2005 on Windows Vista Issue List**.

Guest Operating System Support

You can use the Integrated Virtual Debugger with any Windows guest operating system except the following: Windows NT, Me, 98, 95, 3.1, XP Home Edition, Vista Starter Edition, and Windows for Workgroups.

The version of VMware Tools on the guest operating system must match the version of Workstation 6.5 (which the Integrated Virtual Debugger is a component of) on the host.

Configuring the Remote Debugging Mode

You can manage remote debugging configuration settings for each virtual machine in which you can run and debug applications. Virtual machine configuration properties, set in the Integrated Virtual Debugger configuration pages, determine which virtual machine to run the application in and how the application is run.

Before configuring a virtual machine for remote debugging, complete the following configuration requirements for the guest system, Visual Studio, and Integrated Virtual Debugger.

Configuring the Guest System for Remote Debugging

Several aspects of the guest operating system must be configured to enable remote debugging.

Configure the Group Policy Settings for Windows

To verify that the group policy is set correctly, follow the same steps as for Windows XP Professional. You cannot view this policy on Windows Vista Home Premium and Vista Home Basic.

To configure the group policy settings for Windows

Do one of the following:

- To configure the group policy settings for Windows XP Professional, in the guest system:

  a Select **Control Panel > Administrative Tools > Local Security Policy > Local Policies** and select the **Security Options** page.

  b Set the **Network access: Sharing and security model for local accounts** policy to **Classic - local users authenticate as themselves**.

- To configure the network on a Windows Vista guest, the policy for the **Classic - local users authenticate as themselves** must be set to the default value.

Configuring the Firewall on Windows XP SP2 Virtual Machines

Windows XP SP2 systems have the firewall enabled by default. To debug in a virtual machine with Windows XP SP2, disable the firewall or configure it appropriately. VMware recommends disabling the firewall if you are on a safe network.

For information about using Windows XP SP2 with the firewall enabled to set up remote debugging in Visual Studio, go to the Microsoft Support Web site and enter the Microsoft knowledge base article ID **833977** in the **Search** menu.

Configuring User Accounts

To configure user accounts, log in to the guest operating system with an Administrator account. You must use the same local or domain user account on the host machine to log in to the guest operating system.

NOTE The user name, password, and domain name (if not local on both systems) must match on the host and the guest. Otherwise the Remote Debug Monitor on the guest cannot communicate with the Visual Studio on the host.

For additional information about how to set up Windows user accounts for remote debugging, go to the Microsoft Developer Network Web site, enter the search keywords **Error: Remote Debugger Service On the Target Computer Cannot Connect Back**, and click the first search result.

Communication between Visual Studio and the guest operating system is not initiated until the virtual machine is powered on and the configured user is logged in. The user runs the Remote Debug Monitor on the guest, which in turn communicates with Visual Studio on the host.

To prevent a time delay, power on the virtual machine and log in to the guest operating system before you debug in a virtual machine. You can set up automatic login to bypass the login screen when the guest is booting.

Using the Default Password Policy

Windows has a default security feature that helps protect users with blank passwords from network-based attacks. Users who do not password-protect their accounts can log in only at their physical computer console: the monitor, keyboard, and mouse that are physically connected to their computer. This restriction applies only to local user accounts, not to domain user accounts.

For information on how to disable blank password restrictions, go to the Microsoft Support Web site, enter the Microsoft knowledge base article ID **303846** in the **Search** menu, and click the first search result.

Suppressing Security Prompts on the Guest System

Running an application from a network share triggers a security prompt every time the file is accessed. You can suppress security prompts using Internet Explorer or editing your registry key.

Suppress Security Prompts on the Guest System Using Internet Explorer

VMware recommends that you turn off security prompts on the guest operating system.

To suppress security prompts on the guest system using Internet Explorer

1. In the guest Internet Explorer, choose **Tools > Internet Options > Security > Local Intranet** and click **Sites**.
2. Click **Advanced** and add a new Web site:

   ```
   file://*..host
   ```

Edit a Registry Key to Suppress Security Prompts

VMware recommends that you turn off security prompts on the guest operating system.

To edit a registry key to suppress security prompts

1. In the guest, open the registry.
2. Add a new key called`.host` under `HKCU\Software\Microsoft\Windows\CurrentVersion\InternetSettings\ZoneMap\Domains`.
3. In the `.host` key, create **DWORD Value** called `file` and set its value to `1`.

Installing the Microsoft .NET Framework to Support Managed Applications

To debug managed C++, C#, and Visual Basic applications, which use the Common Language Runtime, install the Microsoft .NET Framework version 2.0 or higher on the guest operating system.

Rename Virtual Machine Computer Names

Computer names must be unique on all virtual machines, otherwise the Integrated Virtual Debugger cannot find the appropriate virtual machine on the network.

To rename virtual machine computer names

1 On the guest system, choose **Start > Control Panel > System**.

2 Select the **Computer Name** tab.

3 Click **Change**.

4 Type a unique name and click **OK**.

Install the Remote Debug Monitor Manually on Windows 98 Guest Systems

To enable debugging in a virtual machine, the Integrated Virtual Debugger shares the host folder that contains the Remote Debug Monitor, and runs that Remote Debug Monitor on the guest. On Windows 98, you cannot run the Remote Debug Monitor (or any executable file) from a shared folder. An attempt to do so generates the following error:

```
The remote debugger is not properly installed. On a Windows ME or
Windows 98 computer, the debugger cannot be run off a file share. Run
the remote debugger setup.
```

Manually install and start the `msvsmon.exe` Remote Debug Monitor executable file on the guest operating system before you start a debugging session. The `msvsmon.exe` is included in the Visual Studio 2005 installation CD.

To install the Remote Debug Monitor manually on Windows 98 guest systems

Do one of the following:

- Create a mapping to a network share with the host where `msvsmon.exe` is located.
- Install `msvsmon.exe` from the Visual Studio 2005 installation CD.

Start the Remote Debug Monitor Without Authentication on the Default Port

Running the Remote Debug Monitor on the guest system without authentication poses a security risk for that guest system. VMware recommends to take a snapshot first and set **Revert to Parent Snapshot** to **Yes** in **Post-Debug Event** or **Pre-Debug Event** properties, as described in"Setting Configuration Properties" on page 493.

Because of the shared folder limitations, you must also:

- In Visual Studio, set **Run Command As** to **a guest path**. This property indicates how the command being executed by the debugger is run.
- In Visual Studio, leave **Shared Directories** unset, because directories cannot be shared between the host and the guest.

For more information, see "Set General Properties" on page 493.

To start the Remote Debug Monitor without authentication on the default port

1. In the guest, run the command:

   ```
   msvsmon.exe /noauth
   ```

2. Verify that you are using port `4015` by confirming that Remote Debug Monitor displays the following message:

   ```
   Msvsmon started a new server named '<guest_name>:4015'.  Authentication
                  is disabled.  Waiting for new connections.
   ```

Configuring Visual Studio

You must configure Visual Studio to enable remote debugging.

Configure the Runtime Library Setting for C++ Applications

When you debug on a remote machine or in a virtual machine, the application might not start if the runtime library setting is set to certain values. If you encounter this problem, change the C++ runtime library setting.

For additional information on C++ libraries, go to the Microsoft Developer Network Web site and search for **Visual C++ Libraries as Shared Side-by-Side Assemblies**.

To configure the runtime library setting for C++ applications

1. In Visual Studio, choose **Project > Properties**.
2. Expand **Configuration Properties > C/C++** and select **Code Generation**.
3. Set **Code Generation** to **Multi-threaded (/MT)** or **Multi-threaded Debug (/MTd)**.

Configuring the Integrated Virtual Debugger for Remote Debugging

Before you can start or debug applications in a virtual machine, create or modify virtual machine configurations and set configuration properties. The default configuration initially includes the default values for all properties that have them.

In Visual Studio, choose **VMware > Options** to manage configurations. You can create, rename, and remove configurations, and you can set and modify configuration properties for existing configurations as described in "Setting Configuration Properties" on page 493.

The configuration selected in the **Configuration** drop-down menu is the configuration being edited in the configuration pages. The configuration selected in the **Active Configuration** drop-down menu is the configuration used when you choose **VMware > Start Debugging in VM** or **VMware > Start Without Debugging in VM**.

Create Configurations

When you create a configuration, it includes all the aspects of the Integrated Virtual Debugger configuration.

To create configurations

1 Choose **VMware > Options**.

2 Click the **New** icon next to the **Configuration** drop-down menu.

3 In the New Configuration page, type a name for the new configuration.

4 Choose a configuration to copy settings from.

5 The default selection is **<Default>**, which includes the default values for all properties that have them.

6 Click **OK**.

The new configuration is created and listed as the active configuration in the **Configuration** and **Active Configuration** drop-down menus. You can start editing the configuration properties.

Setting Configuration Properties

You can edit configuration properties for a specific configuration by choosing the configuration name from the **Configuration** drop-down menu. You can also edit configuration properties for all configurations by choosing **All Configurations** from the **Configuration** drop-down menu.

Set General Properties

The default configuration initially includes the default values for all properties that have them. General properties for remote debugging include:

- The path to the virtual machine file (the `.vmx` file).
- The command that Visual Studio runs in the guest operating system.
- How the command is run: as a path on the host in a shared folder or as a path on the guest.
- The location of the Remote Debug Monitor on the host.
- The name of the Remote Debug Monitor on the guest.
- (Optional) The location of any directories shared between the host and the guest.

To set general properties

1 Choose **VMware > Options**.

2 In the left pane, click **Remote Debugging in VM** and select **General**.

3 Set **Command** to the command that the debugger in the guest system runs.

4 Click **Browse** to select a path to the executable file on the host file system.

The command directory is shared between the host and the guest.

5 Set **Run Command As** to indicate how the debug command is run: either as **a host path through a shared folder** or as **a guest path**.

When you select **a host path through a shared folder**, the folder where the command is located is shared before the debugging session is started. The command is run from the shared folder, and when the debugging session ends, the folder is no longer shared. The name of the shared folder is `\\.host\Shared Folders\.$(ProjectName)<random_number>`

When **a guest path** is selected, the command is run from the specified path on the guest.

The default is **a host path through a shared folder**.

6 Set **Remote Debug Monitor Path** to the location of the Remote Debug Monitor on the host.

The default is the Visual Studio installed path:

```
\Program Files\Microsoft Visual Studio 8\Common7\IDE\Remote Debugger\x86\
               msvsmon.exe
```

Use this default Remote Debug Monitor to debug a 32-bit process in a 32-bit virtual machine and a 32-bit process in a 64-bit virtual machine.

To debug a 64-bit process in a 64-bit virtual machine, use the 64-bit Remote Debug Monitor:

```
\Program Files\Microsoft Visual Studio 8\Common7\IDE\Remote
               Debugger\x64\msvsmon.exe
```

7 Enter the **Remote Debug Monitor Name** on the guest.

If a Remote Debug Monitor is already running on the guest, when the new connection is made between the Remote Debug Monitor on the guest and Visual Studio on the host, you are prompted to choose whether to connect to the debugger that is running or start another debugger with a different name.

8 Set **Virtual Machine** to the path to the virtual machine file (`.vmx` file).

9 (Optional) Set **Shared Folders** to a semicolon-delimited list of paired folder names in the form <`shared_name`>=<`host_folder_name`>.

Set Pre-Debug Event Properties

Pre-Debug Event properties determine which actions are performed before the debug command is run. All of these settings are optional.

To set Pre-Debug Event properties

1 Choose **VMware > Options.**

2 In the left pane, click **Remote Debugging in VM** and select **Pre-Debug Event**.

3 Set **Revert to Parent Snapshot** to **Yes** or **No**.

If set to **Yes**, the virtual machine reverts to its parent snapshot when the debugging session is started.

4 Set **Copy Files** to a semicolon-delimited list of paired file or directory names that are copied from the host to the guest machine in the form `<host_machine_file/folder>=<virtual_machine_file/folder>`.

   All specified files are copied before any pre-debugging commands are run.

5 Set **Command Line** to one or more semicolon-delimited commands that are run after files are copied and before the debugging session starts.

Set Post-Debug Event Properties

Post-Debug Event properties determine which actions are performed after the debug command ends. All of these settings are optional.

To set Post-Debug Event properties

1 Choose **VMware > Options.**

2 In the left pane, click **Remote Debugging in VM** and select **Post-Debug Event**.

3 Set **Command Line** to one or more semicolon-delimited commands that are run after the debugging session ends.

4 Set the **Termination Mode** to one of the following:

   - No operation (default)
   - Power off
   - Revert to parent
   - Suspend

Rename a Configuration

You can rename a configuration so that the new name reflects the settings of your configuration.

To rename a configuration

1 Choose **VMware > Options**.

2 Choose the configuration to rename from the **Configuration** drop-down menu and click the **Edit** icon.

3 On the Edit Configuration page, select the configuration to rename and click **Rename**.

4 Type the new name over the existing name and press Enter.

5 At the confirmation prompt click **Yes**.

6 Click **Close**.

The renamed configuration is listed as the active configuration in the **Configuration** drop-down menu. You can edit its configuration properties, as described in “Setting Configuration Properties” on page 493.

Remove a Configuration

When you no longer need a configuration, you can remove it without affecting another configuration.

To remove a configuration

1 Choose **VMware > Options**.

2 Choose the name of the configuration to delete from the **Configuration** drop-down menu and click the **Edit** icon.

3 In the Edit Configuration page, select the configuration to delete and click **Remove**.

4 At the confirmation prompt, click **Yes**.

5 Click **Close**.

Debugging Applications in Virtual Machines Using Remote Debugging

After you create the appropriate configurations for remote debugging, the Integrated Virtual Debugger lets you:

- Start a remote debugging session in a virtual machine.
- Start an application in a virtual machine without debugging.
- Start a debugging session that attaches to a process already running in a virtual machine.

Start a Remote Debugging Session in a Virtual Machine

You can debug an application in any configured virtual machine. Log in to the guest system manually before the application is started. For additional information, see "Configuring User Accounts" on page 488.

To start a remote debugging session in a virtual machine

1. Choose **VMware > Start Debugging in VM**.
2. Perform debugging tasks as you would from the **Debug > Start Debugging** Visual Studio menu.
3. (Optional) To stop the processes associated with the debugging session on the guest system and restart debugging, choose **VMware > Restart**.

Start a Session Without Debugging in a Virtual Machine

You can start an application in any configured virtual machine without debugging. When you start an application without debugging, the Integrated Virtual Debugger does not run pre-debug or post-debug operations, share additional directories, or start the Remote Debug Monitor on the guest system.

Log in to the guest system manually before you run the application. For additional information, see "Configuring User Accounts" on page 488.

To start a session without debugging in a virtual machine

Choose **VMware > Start Without Debugging in VM**.

The Integrated Virtual Debugger initiates the following:

1. Powers on the virtual machine if necessary.
2. Shares the folder with the executable file.
3. Runs the executable file.
4. Removes the shared folder when the executable file ends.
5. Starts the application in the virtual machine.

Attach the Debugger to a Process Running in a Virtual Machine

Before you attach the debugger to a process running in a virtual machine, make sure that the virtual machine is powered on.

To attach the debugger to a process running in a virtual machine

1 Choose **VMware > Attach to Process**.

2 Choose the virtual machine on which to view running processes from the **Running Virtual Machines** drop-down menu.

3 Set **Remote Debug Monitor** to the location of the Remote Debug Monitor on the host.

The default is the Visual Studio installed path:

```
\Program Files\Microsoft Visual Studio 8\Common7\IDE\Remote Debugger\x86\
               msvsmon.exe
```

Use this default Remote Debug Monitor to debug a 32-bit process in a 32-bit virtual machine and a 32-bit process in a 64-bit virtual machine.

To debug a 64-bit process in a 64-bit virtual machine, use the 64-bit Remote Debug Monitor:

```
\Program Files\Microsoft Visual Studio 8\Common7\IDE\Remote
               Debugger\x64\msvsmon.exe
```

4 Type a name for the Remote Debug Monitor on the guest.

The default name is `VMDebug`.

If a Remote Debug Monitor is already running on the guest with that name, start another one with a different name.

5 Choose the process to attach to from the list of available processes and click **Attach**.

6 (Optional) To refresh the list of running processes, click **Refresh**.

Using the Replay Debugging Mode

The replay debugging mode of the Integrated Virtual Debugger allows you to debug an application in a recording of a virtual machine execution. This mode is different from the remote debugging mode in that replay debugging requires creating a recording of an application's execution before you can debug. Recordings can be made using the Workstation user interface or from within Visual Studio, using the **Create Recording for Replay** option in the **VMware** drop-down menu. When you create a recording in Visual Studio, the Integrated Virtual Debugger starts the virtual machine, creates a recording, ensures that the application is available in the virtual machine, runs the application to completion, and stops the recording. When you create a recording in Workstation, you must perform these steps yourself. For more information on creating a recording using Workstation, see "Make a Recording" on page 245.

After a recording is created, you can debug the application running in the recording. Use the **Start Replay Recording** option in the **VMware** drop-down menu to debug the application in the recording. Like traditional debugging, in the replay debugging mode you can for example, set breakpoints, add data breakpoints, step through source statements, and examine your threads, locals, and stack frames.

Unlike traditional debugging, the application you debug using replay debugging does not interact with the user or network but appears to accept user and network input and send network output. This is because the application is exhibiting exactly the same behavior as when the recording was created. The application shows the same behavior every time it is debugged.

Replay debugging also provides a reverse execution feature. This feature is analogous to forward execution, except the application runs until it reaches the previous breakpoint, data breakpoint, or exception. Reverse execution is initiated using the **Reverse Continue** or **Reverse Run to Cursor** options from the **VMware** drop-down menu. The Integrated Virtual Debugger implements reverse execution by replaying a recording to find a specific time in the past. In certain circumstances multiple replay steps may be necessary to achieve a single reverse execution operation.

Requirements and Recommendations for Replay Debugging

Visual Studio must be running on the same machine as Workstation.

Supported Versions of Visual Studio

Visual Studio 2005 and Visual Studio 2008 are supported. For important information about running Visual Studio 2005 on Windows Vista, go to the Microsoft Developer Network Web site and search for **Visual Studio 2005 on Windows Vista Issue List**.

Supported Programming Languages

Replay debugging supports the C and Native C++ programming languages.

Host System Requirements

The Integrated Virtual Debugger can run on most Windows host operating systems that Workstation 6.5 supports, listed in "32-bit" on page 25 and "64-bit" on page 26.

Replay debugging is supported on machines using the Intel Pentium 4, Intel Core 2, Intel Penryn (stepping B0+), and AMD Barcelona (B3x) processors. For more information on the hardware requirements, see "Physical and Virtual Hardware Requirements" on page 240.

Guest Operating System Support

You can run the Integrated Virtual Debugger only on 32-bit Windows guest operating systems. Windows NT, Me, 98, 95, 3.1, and 2000 are not supported guest operating systems. A guest operating system running in the SMP mode is not supported by replay debugging.

Configuring the Replay Debugging Mode

Before using replay debugging, complete the following configuration requirements for the guest system, Visual Studio, and Integrated Virtual Debugger.

To use replay debugging you must install the latest version of the VMware Tools in the guest operating system. For more information on installing tools, see "Installing VMware Tools" on page 100. Replay debugging is enabled by default in the Workstation Virtual Machine Settings.

Configure the Guest System for Replay Debugging

You must configure the guest system so that all DLLs and files required by the application to be debugged are accessible by the guest system. The applications generated by Visual Studio using the default project settings often do not run on remote systems because the settings use non-standard DLLs. You can copy the required DLLs into the guest system or configure Visual Studio not to use the non-standard DLLs.

To configure the guest system

1 Choose **Project > Properties**.

2 Expand **Configuration Properties > C/C++** and select **Code Generation**.

3 Set **Run Time Library** to **Multi-threaded Debug (/MTd)**.

Configuring the Integrated Virtual Debugger for Replay Debugging

Before you can start or debug applications in a virtual machine, you must set configuration properties.

Set General Properties for Replay Debugging

You must set some general properties before you can use replay debugging.

To set general properties for replay debugging

1. Choose **VMware > Options**.
2. In the left pane, click **Replay Debugging in VM** and select **General**.
3. Enter the `.vmx` file of the virtual machine that has the recording in the **Virtual Machine** section.
4. (Optional) Select the name of the recording for replay.

   The names of recordings are automatically populated when a recording is created using Visual Studio.

Set Advanced Properties for Replay Debugging

The following options are available in the advanced properties:

- **Use Host DLL Search Path** – Determines how Visual Studio finds DLLs and their associated symbol files on the host system. When this option is set to Yes, the host DLL search path is used to find DLLs. When this option is set to the default No, Visual Studio assumes DLLs used by the debugged program are at the same location on the host machine as in the virtual machine. This requires you to ensure that the DLLs used by your application are in the same location on both the host machine and the virtual machine.
- **Base Snapshot for Recording** – Allows you to specify the state of the virtual machine before each recording is started. When the base snapshot for recording is not specified the recording starts from the current state of the virtual machine, powering it on if necessary.

To set advanced properties for replay debugging

1. Choose **VMware > Options**.
2. In the left pane, click **Replay Debugging in VM** and select **Advanced**.

Enable Automatic Markers

If you use reverse execution for a long recording, configure Workstation to periodically create markers. Markers are snapshots that the Integrated Virtual Debugger uses to avoid replaying the entire recording during reverse execution. Markers reduce the latency of reverse execution for long-running recordings.

To enable automatic markers

1. From the Workstation menu bar, choose **VM > Settings**.
2. Select the **Options** tab.
3. Click **Snapshot/Replay**.
4. Under the Replay section, set the **Marker Frequency** option.

Debugging Applications in Virtual Machines Using Replay Debugging

After you create the appropriate configurations for replay debugging, the Integrated Virtual Debugger lets you:

- Create a recording.
- Start a debugging session in the replay debugging mode.
- Start a reverse execution.
- Stop a reverse execution.

Create a Recording of a Program Execution Using Visual Studio

Before you can debug an application in a recording, you must create a recording of the application. Recordings can be created from within Visual Studio or manually using Workstation. For more information on creating a recording using Workstation, see "Make a Recording" on page 245.

To create a recording of a program execution using Visual Studio

1. In Visual Studio, choose **VMware > Create Recording for Replay**.
2. Log in using the same local or domain user account on the host machine to log in to the guest operating system.

   The Integrated Virtual Debugger initiates the following:

   a. Powers on the virtual machine if necessary.

   b. Shares the folder to the executable file.

   c. Creates a recording.

   d. Runs the executable file.

   e. Stops the recording when the program ends.

   f. Removes the shared folder.

   g. Starts the application in the virtual machine.

Start a Replay Debugging Session with a Recording Made by Visual Studio

Starting a replay debugging session powers on a virtual machine and starts replaying a recording. Like in traditional debugging, when a breakpoint or exception is encountered, the application is suspended. You can examine the status of the application or continue execution.

If you made the recording manually, see "Start a Replay Debugging Session with a Manual Recording" on page 505.

To start a replay debugging session with a recording made by Visual Studio

Choose **VMware > Start Replay Debugging**.

The Integrated Virtual Debugger initiates the following:

1. Replays the recording until the beginning of the debugging process.
2. Continues debugging until the recording reaches a breakpoint, exception, or end of the application.

If the end of the program is reached during replay debugging, the program execution is interrupted before exiting so that you can use reverse execution.

Using Reverse Execution

The reverse execution feature of the Integrated Virtual Debugger simulates executing the application backward until a debugging event such as a breakpoint or exception is encountered or the beginning of the application is reached.

To improve the usage of the reverse execution feature consider the following best practices:

- Reverse execution is simulated by replaying a recording to arrive at a previous point in time. This process is slow for long recordings, but markers can be used to reduce the replay time. You can manually add markers using the **Create Marker** option in the Replay Control dialog box or configure Workstation to automatically add markers. For more information on enabling markers, see "Enable Automatic Markers" on page 502.
- Disable background snapshots to reduce the time for restoring from snapshots, which is a frequent constituent of reverse execution. For more information on disabling background snapshots, see "Enable or Disable Background Snapshots" on page 193.
- Avoid executing in reverse beyond the creation of or exit from many threads. Each of these processes requires a replay step and slows down the reverse execution process.

Starting Reverse Execution

Select **Reverse Continue** from the **VMware** drop-down menu to start reverse execution. When you start reverse execution, the virtual machine powers on and off and replays the execution multiple times. A status window appears to inform you about the progress of the reverse execution. To reduce the number of replay steps, events associated with debugger strings are suppressed during reverse execution.

Stopping Reverse Execution

Select **Stop Debugging** from the **Debug** drop-down menu to stop reverse execution. Reverse execution cannot be stopped by using **Debug > Break All**, because reverse execution is simulated by replaying a recording. The state of the virtual machine at any given instance may not represent a valid point in time between when reverse execution was initiated and the previous debugging event. The only way reverse execution can be interrupted is by stopping the debugging session.

Start a Replay Debugging Session with a Manual Recording

When recordings are manually created using the record/replay feature of Workstation, you must configure the Integrated Virtual Debugger for the recording mode.

To start a replay debugging session with a manual recording

1. Choose V**Mware > Options**.
2. Under the **General** category of **Replay Debugging in VM,** complete the following:
   - a Enter the `.vmx` file of the virtual machine that has the recording in the **Virtual Machine** option.
   - b Select the name of the recording that you manually created in the **Recording to Replay** option.
3. (Optional) Define any breakpoints.
4. Choose **VMware > Start Replay Recording** to start the debugging session.

Limitations of Replay Debugging Mode

The following are the limitations of replay debugging:

- Memory, registers, and control flow cannot be changed while replay debugging.
- Reverse execution may not function properly with more than four data breakpoints.
- Individual threads cannot be suspended using the Visual Studio Freeze feature.
- Reading process memory of an application running in a virtual machine results in zeros.
- You cannot attach to a process in the replay debugging mode.
- Suspending the application you are debugging also suspends everything in the virtual machine. Your guest screen output might lag from the state observed in the Integrated Virtual Debugger.
- Debugging events associated with unloading DLLs are not delivered to Visual Studio. The Visual Studio modules window might show DLLs that are actually unloaded.

Integrated Virtual Debugger Environment

The Integrated Virtual Debugger uses an aspect of the Visual Studio environment and creates its own preference and project files.

Identify the Application for Replay Debugging

When you start a replay debugging session, the Integrated Virtual Debugger uses the current Visual Studio Startup Project in the solution to determine which executable file in the recording to debug. If your Visual Studio solution has more than one project that builds an executable file, then you must set the project you want to debug as the StartUp Project before you replay.

To identify the application for replay debugging

1. In the Visual Studio Solution Explorer window, right-click the project that you want to replay debug.
2. Select **Set As StartUp Project**.

Files Maintained by the Integrated Virtual Debugger

The Integrated Virtual Debugger creates and maintains the following files:

- A preference file, `vsid-prefs.xml`, is located in the `\Documents and Settings\<user_name>\Application Data\VMware` directory. Do not edit this file directly. It is updated when you make changes in the Integrated Virtual Debugger configuration pages.
- A file, `<project_name>.idc`, is created in the project directory for each project type that the Integrated Virtual Debugger supports.

Troubleshooting Tips

Before you start troubleshooting an error make sure that you have correctly installed and configured the Integrated Virtual Debugger.

Reporting Bugs and Viewing Log Files

Contact VMware customer support to report any bugs and send the log files that were generated.

To view the log files, choose **VMware > About VMware Virtual Debugger**. The log files contain informational and error messages about the actions of the Integrated Virtual Debugger.

- A log file, `vmware-vsid-<user_name>-<integer>.log`, is created in the `\Documents and Settings\<user_name>\Local Settings\Temp` directory.
- A log file, `vmware-vixWrapper-<user_name>-<pid>.log`, is created in the `\Documents and Settings\<user_name>\Local Settings\Temp\vmware-<user_name>` directory.

Remote Debugging Tips

You might experience the following common errors when you are debugging using the remote debugging mode.

Changing Shortcut Keys

If you change the shortcut keys for `VMDebugger` commands (choose **Tools > Options > Keyboard**), the tooltips for the **VMware** menu and toolbar do not reflect the changes until you restart Visual Studio.

Reinstalling VMware Tools If the Debugging Session Does Not Start

If the debugging session fails to start and the last message in the VMware output window (and log file) is `Waiting for VMware Tools to start`, check whether the guest system has the latest VMware Tools installed and running. If not, upgrade to the latest version of VMware Tools. See "VMware Tools Update Process" on page 113.

Exiting Visual Studio Before Powering Off a Virtual Machine

If you attempt to exit Visual Studio after starting a debugging session but before you log in or run VMware Tools on the guest, Visual Studio does not exit until the virtual machine is powered off or the user is logged in to the guest operating system.

Unloading the VMDebugger Add-in

To permanently uninstall the Integrated Virtual Debugger, run the Workstation installation program, select **Modify** on the Program Maintenance page, deselect **Visual Studio PlugIn** in the **Custom** setup, and finish the installation.

Deselecting **Start** in **Tools > Add-In Manager** does not prevent the Integrated Virtual Debugger Add-in from loading.

Clean Up After a Failure and Debug Locally

If you try to run the debugger locally after a debugging session in a virtual machine fails or stalls, you might get a Visual Studio error that indicates that the remote server cannot be found.

To clean up after a failure and debug locally

Do one of the following:

- In C++, choose **Project Property Pages > Debugging** and set the **Debugger to Launch** property to `Local Windows Debugger`.

  Set the **Command** property to either an empty string or the correct local path.

- In C# and Visual Basic, choose **Project Property Pages > Debug**.

  Make sure **Start project** is selected and **Use remote machine** is deselected.

- (Optional) You can remove any shared folders that were used to run the debug command and the Remote Debug Monitor. Shared folders are usually removed at the end of a debugging session, but they might not be removed in the following circumstances:

  - If the debugging session causes a failure.
  - If the virtual machine is powered off while the debugging session is still running.

  These shared folders are typically reused when another debugging session is started, so this cleanup is not required.

Replay Debugging Tips

You might experience the following common errors when you are debugging using the replay debugging mode.

Restarting Application to Enable Shared Folders

If starting an application to debug with replay debugging in a virtual machine fails with `A file is not found` error, wait a few minutes and restart the application. This is because the shared folders are not enabled at that moment.

Renaming a Recording

When recordings are created they are named **Recording <n>** by default. It is useful to rename recordings so that the name reflects the content and add descriptive text to each recording. For more information on renaming a recording, see "Rename a Snapshot or Recording" on page 197.

Determining Why an Application Does Not Run in the Guest System

If your application does not run in the guest system, it may be because a DLL is missing. Copy the application manually to the virtual machine and run it to get better diagnostics.

To copy the application to the guest system use any of the following methods:

- Create a shared folder that contains the application. For more information on creating a shared folder, see "Set Up Shared Folders" on page 178.
- Drag and drop the application from the host system to the guest system. For more information on dragging and dropping an application, see"Enable or Disable Drag-and-Drop" on page 176.
- Use Windows networking to share a folder on the host system containing the application and map that network drive on the guest.

Glossary

A

administrative lockout

A global setting providing password protection for Windows hosts. Administrative lockout restricts users from creating new virtual machines, editing virtual machine configurations, and changing network settings.

B

bridged networking

A type of network connection between a virtual machine and the host's physical network. With bridged networking, a virtual machine appears as an additional computer on the same physical network as the host. *See also* host-only networking.

C

clone

A duplicate of a virtual machine. *See also* full clone, linked clone.

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.

D–E

disk mode

A property of a virtual disk that defines its external behavior (how the virtualization layer treats its data) but is completely invisible to the guest operating system. Available modes include persistent mode (changes to the disk are always preserved across sessions), nonpersistent mode (changes are never preserved), and undoable mode (changes are preserved at the user's discretion).

F

Favorites list

A list in the left panel of the main Workstation window that shows the names of virtual machines that a user has added. You can use the **Favorites** list to launch a virtual machine or to connect to the virtual machine's configuration file and make changes in the virtual machine settings.

full clone

A complete copy of the original virtual machine, including all associated virtual disks. *See also* linked clone.

full screen mode

A display mode in which the virtual machine's display fills the entire screen. *See also* full screen switch mode.

full screen switch mode

A display mode in which the virtual machine's display fills the entire screen, and the user has no access to the Workstation user interface. The user cannot create, reconfigure, or launch virtual machines. A system administrator performs those functions. *See also* full screen mode.

G

Go to Snapshot

A command that allows you to restore any snapshot of the active virtual machine. *See also* Revert to Snapshot.

guest operating system

An operating system that runs inside a virtual machine. *See also* "host operating system" on page 512.

H–K

host-only networking

A type of network connection between a virtual machine and the host. With 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.

host

The physical computer on which the VMware Workstation software is installed.

host operating system

An operating system that runs on the host machine. *See also* guest operating system.

independent disk

A type of virtual disk that is not affected by snapshots. You can configure independent disks in persistent and nonpersistent modes. *See also* nonpersistent mode, persistent mode, snapshot.

L–M

LAN segment

A private virtual network that is available only to virtual machines within the same team. *See also* virtual network, team.

linked clone

A copy of the original virtual machine that must have access to the parent virtual machine's virtual disks. The linked clone stores changes to the virtual disks in a separate set of files. *See also* full clone.

lockout

See administrative lockout.

N–O

nonpersistent mode

A disk mode in which all disk writes issued by software running inside a virtual machine appear to be written to the independent disk but are in fact discarded after the virtual machine is powered off. As a result, a virtual disk or physical disk in independent-nonpersistent mode is not modified by activity in the virtual machine. *See also* disk mode, persistent mode.

P

parent

The source virtual machine from which you take a snapshot or make a clone. A full clone has no continued link to its parent, but a linked clone and a snapshot must have access to the parent's virtual disk files. If you delete the parent virtual machine, any linked clone or snapshot becomes permanently disabled. To prevent deletion, you can make the parent a template virtual machine. *See also* full clone, linked clone, snapshot.

persistent mode

A disk mode in which all disk writes issued by software running inside a virtual machine are immediately and permanently written to a virtual disk that has been configured as an independent disk. As a result, a virtual disk or physical disk in independent-persistent mode behaves like a conventional disk drive on a physical computer. *See also* disk mode, nonpersistent mode.

physical disk

A hard disk in a virtual machine that is mapped to a physical disk drive or partition on the host machine. A physical disk is also referred to as a raw disk. A virtual machine's disk can be stored as a file on the host file system or on a local hard disk. When a virtual machine is configured to use a physical disk, Workstation directly accesses the local disk or partition as a physical device (not as a file on a file system). *See also* virtual disk.

Q

quick switch mode

A display mode in which the virtual machine's display fills most of the screen. In this mode, tabs at the top of the screen allow you to switch quickly from one running virtual machine to another. *See also* full screen mode.

R

raw disk

See physical disk.

record/replay feature

This feature lets you record all of a Workstation 5 or 6.x virtual machine's activity over a period of time. Unlike Workstation's movie-capture feature, the record/replay feature lets you exactly duplicate the operations and state of the virtual machine throughout the time of the recording.

redo log

The file that stores changes made to a disk in all modes except the persistent and independent-persistent modes. For a disk in nonpersistent mode, the redo-log file is deleted when you power off or reset the virtual machine without writing any changes to the disk. You can permanently apply the changes saved in the redo log to a disk in undoable mode so that they become part of the main disk files. *See also* disk mode.

Revert to Snapshot

A command that restores the status of the active virtual machine to its immediate parent snapshot. This parent is represented in the snapshot manager by the snapshot appearing to the immediate left of the **You Are Here** icon. *See also* Go to Snapshot, snapshot manager.

S

shared folder

A folder on a host computer—or on a network drive accessible from the host—that can be used by both the host and one or more virtual machines. It provides a way of sharing files between host and guest or among virtual machines. In a Windows virtual machine, shared folders appear as folders on a drive letter. In a Linux or Solaris virtual machine, shared folders appear under a specified mount point.

snapshot

A reproduction of the virtual machine just as it was when you took the snapshot, including the virtual machine's power state (on, off, or suspended). If the virtual hard disks are not set to independent mode, a snapshot also includes the state of the data on all the virtual machine's disks. You can take a snapshot when a virtual machine is powered on, powered off, or suspended. *See also* independent disk.

snapshot manager

A control panel used to take actions on any of the snapshots and recordings associated with the selected virtual machine. *See also* record/replay feature, snapshot.

T–U

team

A group of virtual machines that are configured to operate as one object. You can power on, power off, and suspend a team with one command. You can configure a team to communicate independently of any other virtual or real network by setting up a LAN segment. *See also* LAN segment, virtual network.

Unity mode

A display mode in which a virtual machine's applications are displayed in application windows directly on the host's desktop. The virtual machine console view is hidden, and you can minimize the Workstation window. In this mode, a virtual machine's applications look just like other application windows on the host.

V–X

virtual disk

A file or set of files that appears as a physical disk drive to a guest operating system. These files can be on the host machine or on a remote file system. *See also* physical disk.

virtual hardware

The devices that make up a virtual machine. The virtual hardware includes the virtual disk, removable devices such as the DVD-ROM/CD-ROM and floppy drives, and the virtual Ethernet adapter. You configure these devices with the virtual machine settings editor. *See also* virtual machine settings editor.

virtual machine

A virtualized x86 PC environment in which a guest operating system and associated application software can run. Multiple virtual machines can operate on the same host machine concurrently.

virtual machine configuration

The specification of which virtual devices, such as disks and memory, 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. This `.vmx` file is created when you create the virtual machine. It is used to identify and run a specific virtual machine.

virtual machine settings editor

A point-and-click control panel used to view and modify a virtual machine’s settings.

virtual network

A network connecting virtual machines that does not depend on physical hardware connections. For example, you can create a virtual network between a virtual machine and a host that has no external network connections. You can also create a LAN segment for communication between virtual machines on a team. *See also* LAN segment, team.

virtual network editor

A point-and-click editor used to view and modify the networking settings for the virtual networks created by Workstation.

VMware Player

Free software that enables PC users to easily run any virtual machine on a Windows or Linux PC. VMware Player runs virtual machines created by VMware Workstation, VMware Server, or ESX Server and also supports Microsoft virtual machines and Symantec Backup Exec System Recovery disk formats.

VMware Tools

A suite of utilities and drivers that enhances the performance and functionality of your guest operating system. Key features of VMware Tools include some or all of the following, depending on your guest operating system: an SVGA driver, a mouse driver, the VMware Tools control panel and support for such features as shared folders, drag-and-drop in Windows and Linux guests, shrinking virtual disks, time synchronization with the host, VMware Tools scripts, and connecting and disconnecting devices while the virtual machine is running. *See also* shared folder.

Index