vSphere Virtual Machine Administration

ESXi 6.0

vCenter Server 6.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001472-02

vmware®

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

Copyright © 2009–2015 VMware, Inc. All rights reserved. Copyright and trademark information.

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

Contents

About vSphere Virtual Machine Administration 7

Updated Information 9

1 Introduction to VMware vSphere Virtual Machines 11
- What Is a Virtual Machine? 11
- Virtual Machines and the Virtual Infrastructure 12
- Virtual Machine Lifecycle 13
- Virtual Machine Components 13
- Virtual Machine Hardware Available to vSphere Virtual Machines 13
- Virtual Machine Options and Resources 15
- vSphere Web Client 16
- VMware Tools 17
- Where to Go From Here 17

2 Deploying Virtual Machines 19
- About Provisioning Virtual Machines 19
- Create a Virtual Machine Without a Template or Clone 20
- Deploy a Virtual Machine from a Template 26
- Clone a Virtual Machine 32
- Clone a Virtual Machine to a Template in the vSphere Web Client 37
- Clone a Template to a Template in the vSphere Web Client 41
- Convert a Template to a Virtual Machine 45
- Customizing Guest Operating Systems 47

3 Deploying OVF Templates 63
- OVF File Format and OVF Templates 63
- Deploy an OVF Template in the vSphere Web Client 64
- Browse VMware Virtual Appliance Marketplace 67
- Export an OVF Template 68

4 Using Content Libraries 71
- Create a Library 72
- Synchronize a Subscribed Library 74
- Edit the Settings of a Local Library 74
- Edit the Settings of a Subscribed Library 75
- Delete a Content Library 75
- Hierarchical Inheritance of Permissions for Content Libraries 76
- Sample User Role for Working with Content Libraries 78
- Populating Libraries with Content 78
- Working with Items in a Library 81

Creating Virtual Machines and vApps from Templates in a Content Library 84

5 Installing the Microsoft Sysprep Tool 87
Install the Microsoft Sysprep Tool from a Microsoft Web Site 87
Install the Microsoft Sysprep Tool from the Windows Operating System CD 88

6 Configuring Virtual Machine Hardware 89
Virtual Machine Compatibility 89
Virtual CPU Configuration 95
Virtual Memory Configuration 102
Network Virtual Machine Configuration 104
Parallel and Serial Port Configuration 108
Virtual Disk Configuration 115
SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility 126
Other Virtual Machine Device Configuration 131
Reduce Memory Overhead for Virtual machines with 3D graphics Option 140
USB Configuration from an ESXi Host to a Virtual Machine 140
USB Configuration from a Client Computer to a Virtual Machine 147
Add a Shared Smart Card Reader to Virtual Machines 152

7 Configuring Virtual Machine Options 155
Virtual Machine Option Overview 155
Change the Virtual Machine Name 156
View the Virtual Machine Configuration and Working File Location 157
Change the Configured Guest Operating System 157
Configuring User Mappings on Guest Operating Systems 157
Change the Virtual Machine Console Options for Remote Users 159
Configure the Virtual Machine Power States 159
Configure Virtual Machines to Automatically Upgrade VMware Tools 160
Manage Power Management Settings for a Virtual Machine 161
Delay the Boot Sequence 162
Disable Virtual Machine Acceleration 162
Enable Virtual Machine Logging 162
Configure Virtual Machine Debugging and Statistics 163
Change the Swap File Location 163
Edit Configuration File Parameters 164
Configure Fibre Channel NPIV Settings 164

8 Managing Multi-Tiered Applications with vSphere vApp 167
Create a vApp 168
Create a Virtual Machine, Resource Pool, or Child vApp Inside a vApp 169
Add Virtual Machine or Child vApp to a vApp 169
Edit vApp Settings 169
Clone a vApp 174
Perform vApp Power Operations 175
Edit vApp Notes 176
Add a Network Protocol Profile 176
Virtual Machine vApp Options 180

9 Monitoring Solutions with the vCenter Solutions Manager 185
Viewing Solutions 185
Monitoring Agents 186

10 Managing Virtual Machines 187
Edit Virtual Machine Startup and Shutdown Settings 187
Install the Client Integration Plug-In 189
Open a Virtual Machine Console 189
Install the VMware Remote Console Application 190
Using the VMware Remote Console Application 190
Adding and Removing Virtual Machines 191
Change the Template Name 192
Deleting Templates 193
Using Snapshots To Manage Virtual Machines 194

11 VMware Tools Components, Configuration Options, and Security Requirements 205
Components of VMware Tools 205
Repairing, Changing, and Uninstalling VMware Tools Components 209
Security Considerations for Configuring VMware Tools 211
Using vmwtool to Configure VMware Tools in a NetWare Virtual Machine 214
Using the VMware Tools Configuration Utility 215

12 Upgrading Virtual Machines 227
Upgrading VMware Tools 228
Installing VMware Tools 229
Planning Downtime for Virtual Machines 231
Downtime for Upgrading Virtual Machines 231
Manually Install or Upgrade VMware Tools in a Windows Virtual Machine 232
Automate VMware Tools Installation for Multiple Windows Virtual Machines 234
Manually Install or Upgrade VMware Tools in a Linux Virtual Machine 238
Operating System Specific Packages for Linux Guest Operating Systems 240
Manually Install or Upgrade VMware Tools in a Mac OS X Virtual Machine 241
Manually Install or Upgrade VMware Tools in a Solaris Virtual Machine 241
Manually Install or Upgrade VMware Tools in a NetWare Virtual Machine 243
Manually Install or Upgrade VMware Tools in a FreeBSD Virtual Machine 245
Upgrade VMware Tools 246
Perform an Automatic Upgrade of VMware Tools 247
Upgrade the Compatibility for Virtual Machines 248
Schedule a Compatibility Upgrade for Virtual Machines 249

13 Required Privileges for Common Tasks 251

Index 255

About vSphere Virtual Machine Administration

vSphere Virtual Machine Administration describes how to create, configure, and manage virtual machines in the VMware vSphere® environment.

In addition, this information provides introductions to the tasks that you can do within the system as well as cross-references to the information that describes the tasks.

This information focuses on managing virtual machines in the VMware vSphere Web Client and includes the following information.

- Creating and deploying virtual machines, templates, and clones
- Deploying OVF templates
- Configuring virtual machine hardware and options
- Managing multitiered applications with VMware vSphere vApp
- Monitoring solutions with the vCenter Solution Manager
- Managing virtual machines, including using snapshots
- Configuring and installing VMware tools
- Upgrading virtual machines

vSphere Virtual Machine Administration covers VMware ESXi™ and VMware vCenter Server™.

Intended Audience

This information is written for experienced Windows or Linux system administrators who are familiar with virtualization.

Updated Information

This *vSphere Virtual Machine Administration* documentation is updated with each release of the product or when necessary.

This table provides the update history of the *vSphere Virtual Machine Administration* documentation.

Revision	Description
EN-001472-02	Added information in "Upgrading VMware Tools," on page 228 that upgrading VMware Tools on a Windows guest operating system also installs the WDDM graphics drivers.
EN-001472-01	■ Added a new procedure about how to customize the guest operating system of an existing virtual machine. See "Apply a Customization Specification to a Virtual Machine," on page 54. ■ Updated procedures for installing VMware Tools depending on the operating system. See "Installing VMware Tools," on page 229.
EN-001472-00	Initial release.

Introduction to VMware vSphere Virtual Machines 1

Before you start creating and managing virtual machines, you benefit from some background information, for example, the virtual machine lifecycle, components, and VMware Tools.

This chapter includes the following topics:

- "What Is a Virtual Machine?," on page 11
- "Virtual Machines and the Virtual Infrastructure," on page 12
- "Virtual Machine Lifecycle," on page 13
- "Virtual Machine Components," on page 13
- "Virtual Machine Hardware Available to vSphere Virtual Machines," on page 13
- "Virtual Machine Options and Resources," on page 15
- "vSphere Web Client," on page 16
- "VMware Tools," on page 17
- "Where to Go From Here," on page 17

What Is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. The virtual machine consists of a set of specification and configuration files and is backed by the physical resources of a host. Every virtual machine has virtual devices that provide the same functionality as physical hardware are more portable, more secure, and easier to manage.

A virtual machine consists of several files that are stored on a storage device. The key files are the configuration file, virtual disk file, NVRAM setting file, and log file. You configure virtual machine settings through the vSphere Web Client, one of the vSphere command-line interfaces (PowerCLI, vCLI) or the vSphere Web Services SDK.

Caution Do not change, move, or delete virtual machine files without instructions from a VMware Technical Support representative.

Table 1-1. Virtual Machine Files

File	Usage	Description
`.vmx`	*vmname*`.vmx`	Virtual machine configuration file
`.vmxf`	*vmname*`.vmxf`	Additional virtual machine configuration files
`.vmdk`	*vmname*`.vmdk`	Virtual disk characteristics
`-flat.vmdk`	*vmname*`-flat.vmdk`	Virtual machine data disk

Table 1-1. Virtual Machine Files (Continued)

File	Usage	Description
`.nvram`	*`vmname`*`.nvram` or `nvram`	Virtual machine BIOS or EFI configuration
`.vmsd`	*`vmname`*`.vmsd`	Virtual machine snapshots
`.vmsn`	*`vmname`*`.vmsn`	Virtual machine snapshot data file
`.vswp`	*`vmname`*`.vswp`	Virtual machine swap file
`.vmss`	*`vmname`*`.vmss`	Virtual machine suspend file
`.log`	`vmware.log`	Current virtual machine log file
`–#.log`	`vmware–#.log` (where # is a number starting with 1)	Old virtual machine log files

Virtual Machines and the Virtual Infrastructure

The infrastructure that supports virtual machines consists of at least two software layers, virtualization and management. In vSphere, ESXi provides the virtualization capabilities that aggregate and present the host hardware to virtual machines as a normalized set of resources. Virtual machines can run on ESXi hosts that vCenter Server manages.

vCenter Server lets you pool and manage the resources of multiple hosts and lets you effectively monitor and manage your physical and virtual infrastructure. You can manage resources for virtual machines, provision virtual machines, schedule tasks, collect statistics logs, create templates, and more. vCenter Server also provides vSphere vMotion ™, vSphere Storage vMotion, vSphere Distributed Resource Scheduler (DRS), vSphere High Availability (HA), and vSphere Fault Tolerance. These services enable efficient and automated resource management and high availability for virtual machines.

The VMware vSphere Web Client is the interface to vCenter Server, ESXi hosts, and virtual machines. With the vSphere Web Client, you can connect remotely to vCenter Server. The vSphere Web Client is the primary interface for managing all aspects of the vSphere environment. It also provides console access to virtual machines.

NOTE For information about running virtual machines on an isolated ESXi host, see the *vSphere Single Host Management* documentation.

The vSphere Web Client presents the organizational hierarchy of managed objects in inventory views. Inventories are the hierarchal structure used by vCenter Server or the host to organize managed objects. This hierarchy includes the monitored objects in vCenter Server.

In the vCenter Server hierarchy, a data center is the primary container of ESXi hosts, folders, clusters, resource pools, vSphere vApps, virtual machines, and so on.

Datastores are virtual representations of underlying physical storage resources in the data center. A datastore is the storage location (for example, a physical disk or LUN on a RAID, or a SAN) for virtual machine files. Datastores hide the idiosyncrasies of the underlying physical storage and present a uniform model for the storage resources required by virtual machines.

For some resources, options, or hardware to be available to virtual machines, the host must have the appropriate vSphere license. Licensing in vSphere is applicable to ESXi hosts, vCenter Server, and solutions. Licensing can be based on different criteria, depending on the specifics of each product. For details about vSphere licensing, see the *vCenter Server and Host Management* documentation.

Virtual Machine Lifecycle

You create and deploy virtual machines into your datacenter in a several ways. You can create a single virtual machine and install a guest operating system and VMware Tools on it. You can clone or create a template from an existing virtual machine, or deploy OVF templates.

The vSphere Web Client New Virtual Machine wizard and Virtual Machine Properties editor let you add, configure, or remove most of the virtual machine's hardware, options, and resources. You monitor CPU, memory, disk, network, and storage metrics using the performance charts in the vSphere Web Client. Snapshots let you capture the state of the virtual machine, including the virtual machine memory, settings, and virtual disks. You can roll back to the previous virtual machine state when needed.

With vSphere vApps, you can manage multitiered applications. You use vSphere Update Manager to perform orchestrated upgrades to upgrade the virtual hardware and VMware Tools of virtual machines in the inventory at the same time.

When a virtual machine is no longer needed, you can remove it from the inventory without deleting it from the datastore, or you can delete the virtual machine and all its files.

Virtual Machine Components

Virtual machines typically have an operating system, VMware Tools, and virtual resources and hardware that you manage in much the same way as you would manage a physical computer.

You install a guest operating system on a virtual machine the same way as you install an operating system on a physical computer. You must have a CD/DVD-ROM or ISO image containing the installation files from an operating system vendor.

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. With VMware Tools, you have more control over the virtual machine interface.

In the vSphere Web Client, you assign each virtual machine to a compatible ESXi host version, cluster, or datacenter by applying a compatibility setting. The compatibility setting determines which ESXi host versions the virtual machine can run on and the hardware features available to the virtual machine.

The hardware devices listed in the Virtual Machine Properties editor complete the virtual machine. Not all devices are configurable. Some hardware devices are part of the virtual motherboard and appear in the expanded device list of the Virtual Machine Properties editor, but you cannot modify or remove them. For a list of hardware devices and their functions, see "Virtual Machine Hardware Available to vSphere Virtual Machines," on page 13.

Access to a virtual machine is controlled by the vSphere administrator.

Virtual Machine Hardware Available to vSphere Virtual Machines

VMware provides devices, resources, profiles, and vServices that you can configure or add to your virtual machine.

Virtual Machine Hardware

Not all hardware devices are available to every virtual machine. The host that the virtual machine runs on and the guest operating system must support devices that you add or configurations that you make. To verify support for a device in your environment, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility or the *Guest Operating System Installation Guide* at http://partnerweb.vmware.com/GOSIG/home.html.

In some cases, the host might not have the required vSphere license for a resource or device. Licensing in vSphere is applicable to ESXi hosts, vCenter Server, and solutions and can be based on different criteria, depending on the specifics of each product. For information about vSphere licensing, see the *vCenter Server and Host Management* documentation.

The PCI and SIO virtual hardware devices are part of the virtual motherboard, but cannot be configured or removed.

Table 1-2. Virtual Machine Hardware and Descriptions

Hardware Device	Description
CPU	You can configure a virtual machine that runs on an ESXi host to have one or more virtual processors. A virtual machine cannot have more virtual CPUs than the actual number of logical CPUs on the host. You can change the number of CPUs allocated to a virtual machine and configure advanced CPU features, such as the CPU Identification Mask and hyperthreaded core sharing.
Chipset	The motherboard uses VMware proprietary devices based on the following chips: ■ Intel 440BX AGPset 82443BX Host Bridge/Controller ■ Intel 82371AB (PIIX4) PCI ISA IDE Xcelerator ■ National Semiconductor PC87338 ACPI 1.0 and PC98/99 Compliant SuperI/O ■ Intel 82093AA I/O Advanced Programmable Interrupt Controller
DVD/CD-ROM Drive	Installed by default when you create a new vSphere virtual machine. You can configure DVD/CD-ROM devices to connect to client devices, host devices, or datastore ISO files. You can add, remove, or configure DVD/CD-ROM devices.
Floppy Drive	Installed by default when you create a new vSphere virtual machine. You can connect to a floppy drive located on the ESXi host, a floppy (`.flp`) image, or the floppy drive on your local system. You can add, remove, or configure floppy devices.
Hard Disk	Stores the virtual machine's operating system, program files, and other data associated with its activities. A virtual disk is a large physical file, or a set of files, that can be copied, moved, archived, and backed up as easily as any other file.
IDE 0, IDE 1	By default, two Integrated Drive Electronics (IDE) interfaces are presented to the virtual machine. The IDE interface (controller) is a standard way for storage devices (Floppy drives, hard drives and CD-ROM drives) to connect to the virtual machine.
Keyboard	Mirrors the keyboard that is connected to the virtual machine console when you first connect to the console.
Memory	The virtual hardware memory size determines how much memory applications that are running inside the virtual machine have available to them. A virtual machine cannot benefit from more memory resources than its configured virtual hardware memory size.
Network Adapter	ESXi networking features provide communication between virtual machines on the same host, between virtual machines on different hosts, and between other virtual and physical machines. When you configure a virtual machine, you can add network adapters (NICs) and specify the adapter type.
Parallel port	Interface for connecting peripherals to the virtual machine. The virtual parallel port can connect to a file. You can add, remove, or configure virtual parallel ports.
PCI controller	Bus on the virtual machine motherboard that communicates with components such as hard disks and other devices. One PCI controller is presented to the virtual machine. You cannot configure or remove this device.

Table 1-2. Virtual Machine Hardware and Descriptions (Continued)

Hardware Device	Description
PCI Device	You can add up to 16 PCI vSphere DirectPath devices to a virtual machine. The devices must be reserved for PCI passthrough on the host on which the virtual machine runs. Snapshots are not supported with DirectPath I/O passthrough devices.
Pointing device	Mirrors the pointing device that is connected to the virtual machine console when you first connect to the console.
Serial Port	Interface for connecting peripherals to the virtual machine. The virtual serial port can connect to a physical serial port, to a file on the host computer, or over the network. You can also use it to establish a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. You can configure a virtual machine with up to 32 serial ports. You can add, remove, or configure virtual serial ports.
SATA controller	Provides access to virtual disks and DVD/CD-ROM devices. The SATA virtual controller appears to a virtual machine as an AHCI SATA Controller.
SCSI controller	Provides access to virtual disks. The SCSI virtual controller appears to a virtual machine as different types of controllers, including LSI Logic Parallel, LSI Logic SAS, and VMware Paravirtual. You can change the SCSI controller type, allocate bus sharing for a virtual machine, or add a paravirtualized SCSI controller.
SCSI device	By default, a SCSI device interface is available to the virtual machine. The SCSI interface is a typical way to connect storage devices (floppy drives, hard drives, and DVD/CD-ROMs) to a virtual machine. You can add, remove, or configure SCSI devices.
SIO controller	Provides serial and parallel ports, floppy devices, and performs system management activities. One SIO controller is available to the virtual machine. You cannot configure or remove this device.
USB controller	The USB hardware chip that provides USB function to the USB ports that it manages. The virtual USB Controller is the software virtualization of the USB host controller function in the virtual machine.
USB device	You can add multiple USB devices, such as security dongles and mass storage devices, to a virtual machine. The USB devices can be connected to an ESXi host or a client computer.
VMCI	Virtual Machine Communication Interface device. Provides a high-speed communication channel between a virtual machine and the hypervisor. You cannot add or remove VMCI devices.

Virtual Machine Options and Resources

Each virtual device performs the same function for the virtual machine as hardware on a physical computer does.

A virtual machine might be running in any of several locations, such as ESXi hosts, datacenters, clusters, or resource pools. Many of the options and resources that you configure have dependencies on and relationships with these objects.

Every virtual machine has CPU, memory, and disk resources. CPU virtualization emphasizes performance and runs directly on the processor whenever possible. The underlying physical resources are used whenever possible. The virtualization layer runs instructions only as needed to make virtual machines operate as if they were running directly on a physical machine.

All recent operating systems provide support for virtual memory, allowing software to use more memory than the machine physically has. Similarly, the ESXi hypervisor provides support for overcommitting virtual machine memory, where the amount of guest memory configured for all virtual machines might be larger than the amount of the host's physical memory.

You can add virtual disks and add more space to existing disks, even when the virtual machine is running. You can also change the device node and allocate shares of disk bandwidth to the virtual machine.

VMware virtual machines have the following options:

General Options View or modify the virtual machine name, and check the location of the configuration file and the working location of the virtual machine.

VMware Tools Manage the power controls for the virtual machine and run VMware Tools scripts. You can also upgrade VMware Tools during power cycling and synchronize guest time with the host.

Advanced Options Disable acceleration and enable logging, configure debugging and statistics, and change the swap file location. You can also change the latency sensitivity and add configuration parameters.

Power Management Manage guest power options. Suspend the virtual machine or leave the virtual machine powered on when you put the guest operating system into standby.

CPUID Mask Hide or expose the `NX/XD` flag. Hiding the `NX/XD` flag increases vMotion compatibility between hosts.

Memory/CPU Hotplug Enable or disable CPU and memory hotplug. You can add Memory or CPU resources to a virtual machine while the virtual machine is running. You can disable Memory or CPU hotplug to avoid adding memory or CPUs while the virtual machine is running. Memory hotplug is supported on all 64 bit operating systems, but to use the added memory, the guest operating system must also support this feature. See the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Boot Options Set the boot delay when powering on virtual machines or to force BIOS setup and configure failed boot recovery.

Fibre Channel NPIV Control virtual machine access to LUNs on a per-virtual machine basis. N-port ID virtualization (NPIV) provides the ability to share a single physical Fibre Channel HBA port among multiple virtual ports, each with unique identifiers.

vApp Options Enable or disable vApp functionality. When you select the checkbox, you can view and edit vApp properties, vApp Deployment options, and vApp Authoring options. For example, you can configure an IP allocation policy or a network protocol profile for the vApp. A vApp option that is specified at the level of a virtual machine overrides the settings specified at the level of the vApp.

vSphere Web Client

All administrative functions are available through the vSphere Web Client.

The vSphere Web Client is a cross platform application that can connect only to vCenter Server. It has a full range of administrative functionality and an extensible plug-in-based architecture. Typical users are virtual infrastructure administrators, help desk, network operations center operators, and virtual machine owners.

Users can use the vSphere Web Client to access vCenter Server through a Web browser. The vSphere Web Client uses the VMware API to mediate the communication between the browser and the vCenter Server.

VMware Tools

VMware Tools improves the performance and management of the virtual machine.

VMware Tools is a suite of utilities that you install in the operating system of a virtual machine. VMware Tools enhances the performance of a virtual machine and makes possible many of the ease-of-use features in VMware products. For example, the following features are just some of the features that are available only if VMware Tools is installed:

- Significantly faster graphics performance and Windows Aero on operating systems that support Aero
- The Unity feature, which enables an application in a virtual machine to appear on the host desktop like any other application window
- Shared folders between host and guest file systems
- Copying and pasting text, graphics, and files between the virtual machine and the host or client desktop
- Improved mouse performance
- Synchronization of the clock in the virtual machine with the clock on the host or client desktop
- Scripting that helps automate guest operating system operations
- Runs pre-freeze and post-thaw quiescing scripts
- Enables capturing quiesced snapshots of guest operating systems
- Periodically collects network, disk, and memory usage information from the guest operating system and sends it to ESXi hosts.
- Sends a heartbeat to each virtual machine every second and collects guest heartbeat information from guest operating systems. VMware HA uses the heartbeat information to determine virtual machine availability.
- Transports the OVF environment to guest operating systems using the guest OS environment variable *guestinfo.ovfEnv* that contains the XML document.

Although the guest operating system can run without VMware Tools, many VMware features are not available until you install VMware Tools. For example, if you do not have VMware Tools installed in your virtual machine, you cannot get heartbeat information from guest operating systems or cannot use the shutdown or restart options from the toolbar. You can only use the power options and you have to shut down your guest operating systems from each virtual machine console. You cannot use VMware Tools for connecting and disconnecting virtual devices, and shrinking virtual disks.

VMware highly recommends that you always run the latest version of VMware Tools. You can configure your virtual machines to automatically check for and apply VMware Tools upgrades each time you power on your virtual machines. For information about enabling automatic upgrade of VMware Tools on your virtual machines, see the "Configure Virtual Machines to Automatically Upgrade VMware Tools," on page 160 topic.

The installation procedure varies, depending on the operating system. For information about installing or upgrading VMware Tools on your guest operating systems, see the *Upgrading Virtual Machines* chapter. For general instructions about installing VMware Tools, see the VMware Knowledge base article at http://kb.vmware.com/kb/1014294.

Where to Go From Here

You must create, provision, and deploy your virtual machines before you can manage them.

To begin provisioning virtual machines, determine whether to create a single virtual machine and install an operating system and VMware tools, work with templates and clones, or deploy virtual machines, virtual appliances, or vApps stored in Open Virtual Machine Format (OVF).

After you provision and deploy virtual machines into the vSphere infrastructure, you can configure and manage them. You can configure existing virtual machines by modifying or adding hardware or install or upgrade VMware Tools. You might need to manage multitiered applications with VMware vApps or change virtual machine startup and shutdown settings, use virtual machine snapshots, work with virtual disks, or add, remove, or delete virtual machines from the inventory.

Deploying Virtual Machines 2

To deploy virtual machines in the vCenter Server inventory, you can deploy from a template, create a virtual machine, or clone an existing virtual machine.

This chapter includes the following topics:

- "About Provisioning Virtual Machines," on page 19
- "Create a Virtual Machine Without a Template or Clone," on page 20
- "Deploy a Virtual Machine from a Template," on page 26
- "Clone a Virtual Machine," on page 32
- "Clone a Virtual Machine to a Template in the vSphere Web Client," on page 37
- "Clone a Template to a Template in the vSphere Web Client," on page 41
- "Convert a Template to a Virtual Machine," on page 45
- "Customizing Guest Operating Systems," on page 47

About Provisioning Virtual Machines

VMware provides several methods to provision vSphere virtual machines. The optimal method for your environment depends on factors such as the size and type of your infrastructure and the goals that you want to achieve.

Create a single virtual machine if no other virtual machines in your environment have the requirements you are looking for, such as a particular operating system or hardware configuration. For example, you might need a virtual machine that is configured only for testing purposes. You can also create a single virtual machine and install an operating system on it, and then use that virtual machine as a template from which to clone other virtual machines. See "Create a Virtual Machine Without a Template or Clone," on page 20.

Deploy and export virtual machines, virtual appliances, and vApps stored in Open Virtual Machine Format (OVF) to use a preconfigured virtual machine. A virtual appliance is a virtual machine that typically has an operating system and other software installed. You can deploy virtual machines from local file systems, such as local disks (for example, C:), removable media (for example, CDs or USB keychain drives), and shared network drives. See Chapter 3, "Deploying OVF Templates," on page 63.

Create a template to deploy multiple virtual machines from. A template is a master copy of a virtual machine that you can use to create and provision virtual machines. Use templates to save time. If you have a virtual machine that you will clone frequently, make that virtual machine a template. See "Deploy a Virtual Machine from a Template," on page 26.

Cloning a virtual machine can save time if you are deploying many similar virtual machines. You can create, configure, and install software on a single virtual machine. You can clone it multiple times, rather than creating and configuring each virtual machine individually. See "Clone a Virtual Machine," on page 32.

Cloning a virtual machine to a template preserves a master copy of the virtual machine so that you can create additional templates. For example, you can create one template, modify the original virtual machine by installing additional software in the guest operating system, and create another template. See Clone a Virtual Machine to a Template in the vSphere Web Client.

Create a Virtual Machine Without a Template or Clone

You can create a single virtual machine if no other virtual machines in your environment have the requirements you are looking for, such as a particular operating system or hardware configuration. When you create a virtual machine without a template or clone, you can configure the virtual hardware, including processors, hard disks, and memory.

During the creation process a default disk is configured for the virtual machine. You can remove this disk and add a new hard disk, select an existing disk, or add an RDM disk on the Customize hardware page of the wizard.

Prerequisites

Verify that you have the following privileges:

- **Virtual machine.Inventory.Create new** on the destination folder or datacenter.
- **Virtual machine.Configuration.Add new disk** on the destination folder or datacenter, if you are adding a new disk.
- **Virtual machine.Configuration.Add existing disk** on the destination folder or datacenter, if you are adding an existing disk.
- **Virtual machine.Configuration.Raw device** on the destination folder or datacenter, if you are using a RDM or SCSI pass-through device.
- **Virtual machine.Configuration.Host USB device** on the destination folder or datacenter, if you are attaching a virtual USB device backed by a host USB device.
- **Virtual machine.Configuration.Advanced** on the destination folder or datacenter, if you are configuring advanced virtual machine settings.
- **Virtual machine.Configuration.Swapfile placement** on the destination folder or datacenter, if you are configuring swapfile placement.
- **Virtual machine.Configuration.Disk change tracking** on the destination folder or datacenter, if you are enabling change tracking on the virtual machine's disks.
- **Resource.Assign virtual machine to resource pool** on the destination host, cluster, or resource pool.
- **Datastore.Allocate space** on the destination datastore or datastore folder.
- **Network.Assign network** on the network that the virtual machine will be assigned to.

To verify the privileges assigned to your role, see the Required Privileges for Common Tasks topic in the *vSphere Security* documentation.

Procedure

1 Start the New Virtual Machine Creation Process on page 21

   If you need a single virtual machine with a particular operating system and hardware configuration, you create a new virtual machine. You can open the New Virtual Machine wizard from any object in the inventory that is a valid parent object of a virtual machine.

2 Select the Virtual Machine Name and Folder on page 22

When you create a virtual machine, you provide a unique name for it. The unique name distinguishes it from existing virtual machines in the virtual machine folder or datacenter. The name can contain up to 80 characters. You can select a datacenter or folder location for the virtual machine, depending on your organizational needs.

3 Select a Resource on page 22

When you deploy a virtual machine, you select the host, cluster, vApp, or resource pool for the virtual machine to run in. The virtual machine will have access to the resources of the selected object.

4 Select a Datastore on page 22

Select the datastore or datastore cluster in which to store the virtual machine configuration files and all of the virtual disks. Each datastore might have a different size, speed, availability, and other properties. The available datastores are accessible from the destination resource that you selected.

5 Select the Virtual Machine Compatibility on page 23

You can accept the default ESXi host version for this virtual machine or select a different version, depending on the hosts in your environment.

6 Select a Guest Operating System on page 23

The guest operating system that you select affects the supported devices and number of virtual CPUs available for the virtual machine. The New Virtual Machine wizard does not install the guest operating system. The wizard uses this information to select appropriate default values, such as the amount of memory needed.

7 Customize Virtual Machine Hardware on page 24

Before you deploy a new virtual machine, you have the option to configure the virtual hardware. When you create a virtual machine, the virtual disk is selected by default. You can use the **New device** drop-down menu on the Customize Hardware page to add a new hard disk, select an existing disk, or add an RDM disk.

8 Finish Virtual Machine Creation on page 24

Before you deploy the virtual machine, you can review the virtual machine settings.

9 Installing a Guest Operating System on page 24

A virtual machine is not complete until you install the guest operating system and VMware Tools. Installing a guest operating system in your virtual machine is essentially the same as installing it in a physical computer.

Start the New Virtual Machine Creation Process

If you need a single virtual machine with a particular operating system and hardware configuration, you create a new virtual machine. You can open the New Virtual Machine wizard from any object in the inventory that is a valid parent object of a virtual machine.

Procedure

1 Right-click any inventory object that is a valid parent object of a virtual machine, such as a datacenter, folder, cluster, resource pool, or host, and select **New Virtual Machine**.

2 Select **Create a new virtual machine** and click **Next**.

Select the Virtual Machine Name and Folder

When you create a virtual machine, you provide a unique name for it. The unique name distinguishes it from existing virtual machines in the virtual machine folder or datacenter. The name can contain up to 80 characters. You can select a datacenter or folder location for the virtual machine, depending on your organizational needs.

Folders provide a way to store virtual machines for different groups in an organization, and you can set permissions on them. For a flatter hierarchy, you can put all virtual machines and templates in a datacenter and organize them a different way.

The virtual machine name determines the name of the virtual machine files and folder on the disk. For example, if you name the virtual machine win8, the virtual machine files are named win8.vmx, win8.vmdk, win8.nvram, and so on. If you change the virtual machine name, the names of the files on the datastore do not change.

Procedure

1 Type a name for the virtual machine.

2 Select or search for the datacenter or folder in which to deploy the virtual machine.

3 Click **Next**.

Select a Resource

When you deploy a virtual machine, you select the host, cluster, vApp, or resource pool for the virtual machine to run in. The virtual machine will have access to the resources of the selected object.

For example, a virtual machine has access to the memory and CPU resources of the host on which it resides. If you select a cluster for the virtual machine, and the administrator has configured the cluster to take advantage of HA and DRS, the virtual machine will have a greater level of availability.

Procedure

1 Search or browse for the host, cluster, vApp, or resource pool for the virtual machine.

   If deploying the virtual machine to the selected location might cause compatibility problems, the problems appear at the bottom of the window.

2 Click **Next**.

Select a Datastore

Select the datastore or datastore cluster in which to store the virtual machine configuration files and all of the virtual disks. Each datastore might have a different size, speed, availability, and other properties. The available datastores are accessible from the destination resource that you selected.

On the Customize hardware page, you can configure the storage. For example, you can add a new hard disk, apply a Virtual machine storage policy, or place the configuration and disk files on separate storage devices.

The amount of free space in the datastore is always changing. Ensure that you leave sufficient space for virtual machine creation and other virtual machine operations, such as growth of sparse files, snapshots, and so on. To review space utilization for the datastore by file type, see the *vSphere Monitoring and Performance* documentation.

Procedure

◆ Select the datastore location where you want to store the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore and click **Next**.
Store all virtual machine files in the same datastore cluster.	a Select a datastore cluster. b (Optional) If you do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the datastore cluster. c Click **Next**.

Select the Virtual Machine Compatibility

You can accept the default ESXi host version for this virtual machine or select a different version, depending on the hosts in your environment.

The default compatibility for this virtual machine is determined by the host on which the virtual machine is created or by the default compatibility settings on the host, cluster, or datacenter. You can select a different compatibility from the default.

Only host versions that are in your environment appear in the **Compatible with** drop-down menu. For information about choices and compatibility strategies, see "Virtual Machine Compatibility," on page 89.

Procedure

◆ Select the compatibility from the drop-down menu and click **Next**.

Select a Guest Operating System

The guest operating system that you select affects the supported devices and number of virtual CPUs available for the virtual machine. The New Virtual Machine wizard does not install the guest operating system. The wizard uses this information to select appropriate default values, such as the amount of memory needed.

For details, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

When you select a guest operating system, BIOS or Extensible Firmware Interface (EFI) is selected by default, depending on the firmware supported by the operating system. Mac OS X Server guest operating systems support only EFI. If the operating system supports BIOS and EFI, you can change the default from the **Options** tab of the Virtual Machine Properties editor after you create the virtual machine and before you install the guest operating system. If you select EFI, you cannot boot an operating system that supports only BIOS, and the reverse.

Important Do not change the firmware after the guest operating system is installed. The guest operating system installer partitions the disk in a particular format, depending on which firmware the installer was booted from. If you change the firmware, you will not be able to boot the guest.

The Mac OS X Server must run on Apple hardware. You cannot power on a Mac OS X Server if it is running on other hardware.

Procedure

1 Select the guest operating system family from the **Guest OS Family** drop-down menu.

2 Select a guest operating system version from the **Guest OS Version** drop-down menu.

3 If you selected **Other** as the guest operating system family, and **Other (32-bit)** or **Other (64-bit)** for the version, type a name for the operating system in the text box.

4 Click **Next**.

Customize Virtual Machine Hardware

Before you deploy a new virtual machine, you have the option to configure the virtual hardware. When you create a virtual machine, the virtual disk is selected by default. You can use the **New device** drop-down menu on the Customize Hardware page to add a new hard disk, select an existing disk, or add an RDM disk.

For information about virtual disk configuration, including instructions for adding different types of disks, see "Add a Hard Disk to a Virtual Machine," on page 118.

For help configuring other virtual machine hardware, see Chapter 6, "Configuring Virtual Machine Hardware," on page 89.

Procedure

1 (Optional) To add a new virtual hardware device, select the device from the **New device** drop-down menu and click **Add**.

2 (Optional) Expand any device to view and configure the device settings.

3 To remove a device, move your cursor over the device and click the **Remove** icon.

   This icon appears only for virtual hardware that you can safely remove.

4 Click **Next**.

Finish Virtual Machine Creation

Before you deploy the virtual machine, you can review the virtual machine settings.

Procedure

1 Review the virtual machine settings and make changes by clicking **Back** to go back to the relevant page.

2 Click **Finish**.

The virtual machine appears in the vSphere Web Client inventory.

Installing a Guest Operating System

A virtual machine is not complete until you install the guest operating system and VMware Tools. Installing a guest operating system in your virtual machine is essentially the same as installing it in a physical computer.

The basic steps for a typical operating system are described in this section. See the *Guest Operating System Installation Guide* at http://partnerweb.vmware.com/GOSIG/home.html.

Using PXE with Virtual Machines

You can start a virtual machine from a network device and remotely install a guest operating system using a Preboot Execution Environment (PXE). You do not need the operating system installation media. When you turn on the virtual machine, the virtual machine detects the PXE server.

PXE booting is supported for Guest Operating Systems that are listed in the VMware Guest Operating System Compatibility list and whose operating system vendor supports PXE booting of the operating system.

The virtual machine must meet the following requirements:

- Have a virtual disk without operating system software and with enough free disk space to store the intended system software.

- Have a network adapter connected to the network where the PXE server resides.

For details about guest operating system installation, see the *Guest Operating System Installation Guide* at http://partnerweb.vmware.com/GOSIG/home.html.

Install a Guest Operating System from Media

You can install a guest operating system from a CD-ROM or from an ISO image. Installing from an ISO image is typically faster and more convenient than a CD-ROM installation.

If the virtual machine's boot sequence progresses too quickly for you to open a console to the virtual machine and enter BIOS or EFI setup, you might need to delay the boot order. See "Delay the Boot Sequence," on page 162.

Prerequisites

- Verify that the installation ISO image is present on a VMFS datastore or network file system (NFS) volume accessible to the ESXi host.
- Verify that you have the installation instructions that the operating system vendor provides.

Procedure

1. Log in to the vCenter Server system or host on which the virtual machine resides.
2. Select an installation method.

Option	Action
CD-ROM	Insert the installation CD-ROM for your guest operating system into the CD-ROM drive of your ESXi host.
ISO image	a Right-click the virtual machine and select **Edit Settings**. The virtual machine Edit Settings dialog box opens. If the **Virtual Hardware** tab is not preselected, select it. b Select **Datastore ISO File** from the CD/DVD drop-down menu, and browse for the ISO image for your guest operating system.

3. Right-click the virtual machine and select **Power On**.

   A green right arrow appears next to the virtual machine icon in the inventory list.
4. Follow the installation instructions that the operating system vendor provides.

What to do next

Install VMware Tools. VMware highly recommends running the latest version of VMware Tools on your guest operating systems. Although the guest operating system can run without VMware Tools, you lose important functionality and convenience without them. See Chapter 12, "Upgrading Virtual Machines," on page 227 for instructions on installing and upgrading VMware Tools.

Upload ISO Image Installation Media for a Guest Operating System

You can upload an ISO image file to a datastore from your local computer. You can do this when a virtual machine, host, or cluster does not have access to a datastore or to a shared datastore that has the guest operating system installation media that you require.

Prerequisites

- Verify that the Client Integration Plug-In is installed. See "Install the Client Integration Plug-In," on page 189. The installation process requires you to close any open browsers.
- Required privileges:
  - **Datastore.Browse datastore** on the datastore.

- **Datastore.Low level file operations** on the datastore.

Procedure

1 In the inventory, click **Datastores** and on the **Objects** tab, select the datastore to which you will upload the file.

2 Click the **Navigate to the datastore file browser** icon ( ).

3 (Optional) Click the **Create a new folder** icon.

4 Select the folder that you created or select an existing folder, and click the **Upload a File** icon ( ).

5 If the Client Integration Access Control dialog box appears, click **Allow** to allow the plug-in to access your operating system and proceed with the file upload.

6 On the local computer, find the file and upload it.

ISO upload times vary, depending on file size and network upload speed.

7 Refresh the datastore file browser to see the uploaded file in the list.

What to do next

After you upload the ISO image installation media, you can configure the virtual machine CD-ROM drive to access the file.

Deploy a Virtual Machine from a Template

Deploying a virtual machine from a template creates a virtual machine that is a copy of the template. The new virtual machine has the virtual hardware, installed software, and other properties that are configured for the template.

Prerequisites

You must have the following privileges to deploy a virtual machine from a template:

- **Virtual machine .Inventory.Create from existing** on the datacenter or virtual machine folder.
- **Virtual machine.Configuration.Add new disk** on the datacenter or virtual machine folder. Required only if you customize the original hardware by adding a new virtual disk.
- **Virtual machine.Provisioning.Deploy template** on the source template.
- **Resource.Assign virtual machine to resource pool** on the destination host, cluster, or resource pool.
- **Datastore.Allocate space** on the destination datastore.
- **Network.Assign network** on the network to which the virtual machine will be assigned. Required only if you customize the original hardware by adding a new network card.
- **Virtual machine.Provisioning.Customize** on the template or template folder if you are customizing the guest operating system.
- **Virtual machine.Provisioning.Read customization specifications** on the root vCenter Server if you are customizing the guest operating system.

Procedure

1 Start the Deploy a Virtual Machine from a Template Task on page 27

To save time, you can create a virtual machine that is a copy of a configured template. You can open the New Virtual Machine wizard from any object in the inventory that is a valid parent object of a virtual machine, or directly from the template. The wizard provides several options for creating and deploying virtual machines and templates.

2 Select a Template on page 28

After you select the template from which to deploy the virtual machine, you can optionally select to customize the guest operating system and the virtual machine hardware. You can also select to turn on the virtual machine when you complete the creation procedure. You can change the properties of the guest operating system, such as the computer name, and network and license settings, which helps prevent conflicts that can result if virtual machines with identical settings are deployed. You can add a CD device such as an ISO file to install the guest operating system, or reconfigure the virtual machines' hardware, such as storage or networking, before you deploy the virtual machine.

3 Select the Virtual Machine Name and Folder on page 28

When you create a virtual machine, you provide a unique name for it. The unique name distinguishes it from existing virtual machines in the virtual machine folder or datacenter. The name can contain up to 80 characters. You can select a datacenter or folder location for the virtual machine, depending on your organizational needs.

4 Select a Resource on page 29

When you deploy a virtual machine, you select the host, cluster, vApp, or resource pool for the virtual machine to run in. The virtual machine will have access to the resources of the selected object.

5 Select a Datastore on page 29

Select the datastore or datastore cluster in which to store the virtual machine configuration files and all of the virtual disks. Each datastore might have a different size, speed, availability, and other properties. The available datastores are accessible from the destination resource that you selected. You can select a format for the virtual machine's disks and assign a storage policy.

6 Select Clone Options on page 30

You can optionally select to customize the guest operating system, customize the virtual machine's hardware, and turn on the virtual machine when you complete the creation procedure. You can customize the guest operating system to change properties, such as the computer name, and network and license settings, which helps prevent conflicts that can result if you deploy virtual machines with identical settings. You can add a CD device such as an ISO file to install the guest operating system or you can reconfigure the virtual machine storage or networking, before you deploy the virtual machine.

7 Customize the Guest Operating System on page 30

When you customize a guest operating system, you can prevent conflicts that might result if you deploy virtual machines with identical settings, such as duplicate computer names. You can change the computer name, network settings, and license settings. You can customize guest operating systems when you clone a virtual machine or deploy a virtual machine from a template.

8 Customize Virtual Machine Hardware on page 31

Before you deploy a new virtual machine, you have the option to configure the virtual hardware. When you create a virtual machine, the virtual disk is selected by default. You can use the **New device** drop-down menu on the Customize Hardware page to add a new hard disk, select an existing disk, or add an RDM disk.

9 Finish Virtual Machine Creation on page 31

Before you deploy the virtual machine, you can review the virtual machine settings.

Start the Deploy a Virtual Machine from a Template Task

To save time, you can create a virtual machine that is a copy of a configured template. You can open the New Virtual Machine wizard from any object in the inventory that is a valid parent object of a virtual machine, or directly from the template. The wizard provides several options for creating and deploying virtual machines and templates.

If you open the wizard from a template, the Select a creation type page does not appear.

Procedure

◆ Select to deploy a virtual machine from a template.

Option	Description
Open the New Virtual Machine wizard from any object in the inventory	a Right-click any inventory object that is a valid parent object of a virtual machine, such as a datacenter, folder, cluster, resource pool, or host, and select **New Virtual Machine**. b Select **Deploy from template** and click **Next**. The Select a name and folder page opens.
Open the Deploy From Template wizard from a template	Right-click the template and select **Deploy VM from this Template**. The Select a name and folder page opens.

Select a Template

After you select the template from which to deploy the virtual machine, you can optionally select to customize the guest operating system and the virtual machine hardware. You can also select to turn on the virtual machine when you complete the creation procedure. You can change the properties of the guest operating system, such as the computer name, and network and license settings, which helps prevent conflicts that can result if virtual machines with identical settings are deployed. You can add a CD device such as an ISO file to install the guest operating system, or reconfigure the virtual machines' hardware, such as storage or networking, before you deploy the virtual machine.

This page appears only if you opened the New Virtual Machine wizard from a inventory object that is not a template.

Note If you start the deploy operation from a template, you select the customization and power options on a later page in the wizard.

Procedure

1 Search for or browse to the template.

2 (Optional) Select **Customize the operating system** to customize the guest operating system of the virtual machine.

3 (Optional) Select **Customize this virtual machine's hardware** to configure the virtual machine's hardware before deployment.

4 (Optional) Select **Power On Virtual Machine after creation** to power on the virtual machine after creation is complete.

5 Click **Next**.

Select the Virtual Machine Name and Folder

When you create a virtual machine, you provide a unique name for it. The unique name distinguishes it from existing virtual machines in the virtual machine folder or datacenter. The name can contain up to 80 characters. You can select a datacenter or folder location for the virtual machine, depending on your organizational needs.

Folders provide a way to store virtual machines for different groups in an organization, and you can set permissions on them. For a flatter hierarchy, you can put all virtual machines and templates in a datacenter and organize them a different way.

The virtual machine name determines the name of the virtual machine files and folder on the disk. For example, if you name the virtual machine win8, the virtual machine files are named win8.vmx, win8.vmdk, win8.nvram, and so on. If you change the virtual machine name, the names of the files on the datastore do not change.

Procedure

1 Type a name for the virtual machine.

2 Select or search for the datacenter or folder in which to deploy the virtual machine.

3 Click **Next**.

Select a Resource

When you deploy a virtual machine, you select the host, cluster, vApp, or resource pool for the virtual machine to run in. The virtual machine will have access to the resources of the selected object.

For example, a virtual machine has access to the memory and CPU resources of the host on which it resides. If you select a cluster for the virtual machine, and the administrator has configured the cluster to take advantage of HA and DRS, the virtual machine will have a greater level of availability.

Procedure

1 Search or browse for the host, cluster, vApp, or resource pool for the virtual machine.

   If deploying the virtual machine to the selected location might cause compatibility problems, the problems appear at the bottom of the window.

2 Click **Next**.

Select a Datastore

Select the datastore or datastore cluster in which to store the virtual machine configuration files and all of the virtual disks. Each datastore might have a different size, speed, availability, and other properties. The available datastores are accessible from the destination resource that you selected. You can select a format for the virtual machine's disks and assign a storage policy.

The amount of free space in the datastore is always changing. Ensure that you leave sufficient space for virtual machine creation and other virtual machine operations, such as growth of sparse files, snapshots, and so on. To review space utilization for the datastore by file type, see the *vSphere Monitoring and Performance* documentation.

Thin provisioning lets you create sparse files with blocks that are allocated upon first access, which allows the datastore to be over-provisioned. The sparse files can continue growing and fill the datastore. If the datastore runs out of disk space while the virtual machine is running, it can cause the virtual machine to stop functioning.

Procedure

1 Select the format for the virtual machine's disks.

Option	Action
Same format as source	Use the same format as the source virtual machine.
Thick Provision Lazy Zeroed	Create a virtual disk in a default thick format. Space required for the virtual disk is allocated during creation. Any data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine.
Thick Provision Eager Zeroed	Create a thick disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out during creation. It might take longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can grow to the maximum capacity allocated to it.

2 (Optional) Select a storage policy from the **VM Storage Policy** drop-down menu.

Storage policies specify storage requirements for applications that run on the virtual machine.

3 Select a datastore location for the virtual disk.

Option	Action
Store the virtual disk and virtual machine configuration files in the same location on a datastore.	Select **Store with the virtual machine** from the **Location** drop-down menu.
Store the disk in a separate datastore location.	Select **Browse** from the **Location** drop-down menu, and select a datastore for the disk.
Store all virtual machine files in the same datastore cluster.	a Select **Browse** from the Location drop-down menu and select a datastore cluster for the disk. b (Optional) If you do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the datastore cluster.

4 Click **Next**.

Select Clone Options

You can optionally select to customize the guest operating system, customize the virtual machine's hardware, and turn on the virtual machine when you complete the creation procedure. You can customize the guest operating system to change properties, such as the computer name, and network and license settings, which helps prevent conflicts that can result if you deploy virtual machines with identical settings. You can add a CD device such as an ISO file to install the guest operating system or you can reconfigure the virtual machine storage or networking, before you deploy the virtual machine.

NOTE If you opened the wizard from an object other than a virtual machine or template, the Select Clone Options page does not appear. These options are available on a different page of the wizard.

Procedure

1 Select **Customize the Operating System**.

2 Select **Customize this virtual machine's hardware**.

3 Select **Power on virtual machine after creation**.

4 Click **Next**.

Customize the Guest Operating System

When you customize a guest operating system, you can prevent conflicts that might result if you deploy virtual machines with identical settings, such as duplicate computer names. You can change the computer name, network settings, and license settings. You can customize guest operating systems when you clone a virtual machine or deploy a virtual machine from a template.

Prerequisites

To access customization options for Windows guest operating systems, Microsoft Sysprep tools must be installed on the vCenter Server system. The Sysprep Tool is built into the Windows Vista and Windows 2008 and later operating systems. For details about this and other customization requirements, see "Guest Operating System Customization Requirements," on page 47.

Procedure

1 Apply a customization specification to the virtual machine.

Option	Description
Select an existing specification	Select a customization specification from the list.
Create a specification	Click the **Create a new specification** icon, and complete the steps in the wizard.
Create a specification from an existing specification	a Select a customization specification from the list. b Click the **Create a spec from an existing spec** icon, and complete the steps in the wizard.

2 Click **Next**.

Customize Virtual Machine Hardware

Before you deploy a new virtual machine, you have the option to configure the virtual hardware. When you create a virtual machine, the virtual disk is selected by default. You can use the **New device** drop-down menu on the Customize Hardware page to add a new hard disk, select an existing disk, or add an RDM disk.

For information about virtual disk configuration, including instructions for adding different types of disks, see "Add a Hard Disk to a Virtual Machine," on page 118.

For help configuring other virtual machine hardware, see Chapter 6, "Configuring Virtual Machine Hardware," on page 89.

Procedure

1 (Optional) To add a new virtual hardware device, select the device from the **New device** drop-down menu and click **Add**.

2 (Optional) Expand any device to view and configure the device settings.

3 To remove a device, move your cursor over the device and click the **Remove** icon.

This icon appears only for virtual hardware that you can safely remove.

4 Click **Next**.

Finish Virtual Machine Creation

Before you deploy the virtual machine, you can review the virtual machine settings.

Procedure

1 Review the virtual machine settings and make changes by clicking **Back** to go back to the relevant page.

2 Click **Finish**.

The virtual machine appears in the vSphere Web Client inventory.

Clone a Virtual Machine

Cloning a virtual machine creates a virtual machine that is a copy of the original. The new virtual machine is configured with the same virtual hardware, installed software, and other properties that were configured for the original virtual machine.

NOTE When heavily loaded applications, such as load generators, are running in the guest operating system during a clone operation, the virtual machine quiesce operation can fail and VMware Tools might be denied CPU resources and time out. It is recommended that you quiesce the virtual machines running lower I/O disk operation.

Prerequisites

If a load generator is running in the virtual machine, stop it before you perform the clone operation.

You must have the following privileges to clone a virtual machine:

- **Virtual machine.Provisioning.Clone virtual machine** on the virtual machine you are cloning.
- **Virtual machine .Inventory.Create from existing** on the datacenter or virtual machine folder.
- **Virtual machine.Configuration.Add new disk** on the datacenter or virtual machine folder.
- **Resource.Assign virtual machine to resource pool** on the destination host, cluster, or resource pool.
- **Datastore.Allocate space** on the destination datastore or datastore folder.
- **Network.Assign network** on the network to which the virtual machine will be assigned.
- **Virtual machine.Provisioning.Customize** on the virtual machine or virtual machine folder if you are customizing the guest operating system.
- **Virtual machine.Provisioning.Read customization specifications** on the root vCenter Server if you are customizing the guest operating system.

Procedure

1 Start the Clone an Existing Virtual Machine Task on page 33

   To make an original copy of a virtual machine, you can clone an existing virtual machine. You can open the New Virtual Machine wizard from any object in the inventory that is a valid parent object of a virtual machine. You can also open the wizard directly from the virtual machine that you are going to clone.

2 Select a Virtual Machine to Clone on page 34

   You select a virtual machine to clone, and you can optionally select to customize the guest operating system and the virtual machine hardware. You can also select to turn on the virtual machine when you complete the creation procedure. You can change the properties of the guest operating system, such as the computer name, and network and license settings, which helps prevent conflicts that can result if virtual machines with identical settings are deployed. You can add a CD device such as an ISO file to install the guest operating system, or reconfigure the virtual machines' hardware, such as storage or networking, before you deploy the virtual machine.

3 Select the Virtual Machine Name and Folder on page 34

   When you create a virtual machine, you provide a unique name for it. The unique name distinguishes it from existing virtual machines in the virtual machine folder or datacenter. The name can contain up to 80 characters. You can select a datacenter or folder location for the virtual machine, depending on your organizational needs.

4 Select a Resource on page 35

When you deploy a virtual machine, you select the host, cluster, vApp, or resource pool for the virtual machine to run in. The virtual machine will have access to the resources of the selected object.

5 Select a Datastore on page 35

Select the datastore or datastore cluster in which to store the virtual machine configuration files and all of the virtual disks. Each datastore might have a different size, speed, availability, and other properties. The available datastores are accessible from the destination resource that you selected. You can select a format for the virtual machine's disks and assign a storage policy.

6 Select Clone Options on page 36

You can optionally select to customize the guest operating system, customize the virtual machine's hardware, and turn on the virtual machine when you complete the creation procedure. You can customize the guest operating system to change properties, such as the computer name, and network and license settings, which helps prevent conflicts that can result if you deploy virtual machines with identical settings. You can add a CD device such as an ISO file to install the guest operating system or you can reconfigure the virtual machine storage or networking, before you deploy the virtual machine.

7 Customize the Guest Operating System on page 36

When you customize a guest operating system, you can prevent conflicts that might result if you deploy virtual machines with identical settings, such as duplicate computer names. You can change the computer name, network settings, and license settings. You can customize guest operating systems when you clone a virtual machine or deploy a virtual machine from a template.

8 Customize Virtual Machine Hardware on page 37

Before you deploy a new virtual machine, you have the option to configure the virtual hardware. When you create a virtual machine, the virtual disk is selected by default. You can use the **New device** drop-down menu on the Customize Hardware page to add a new hard disk, select an existing disk, or add an RDM disk.

9 Finish Virtual Machine Creation on page 37

Before you deploy the virtual machine, you can review the virtual machine settings.

Start the Clone an Existing Virtual Machine Task

To make an original copy of a virtual machine, you can clone an existing virtual machine. You can open the New Virtual Machine wizard from any object in the inventory that is a valid parent object of a virtual machine. You can also open the wizard directly from the virtual machine that you are going to clone.

If you open the wizard from a virtual machine, the Select a creation type page does not appear.

Procedure

◆ Select to clone a virtual machine.

Option	Description
Open the New Virtual Machine wizard from any object in the inventory	a Right-click any inventory object that is a valid parent object of a virtual machine, such as a datacenter, folder, cluster, resource pool, or host, and select **New Virtual Machine**. b Select **Clone an existing virtual machine** and click **Next**. The Select a virtual machine page opens.
Open the Clone Existing Virtual Machine wizard from a template	Right-click the virtual machine and select **Clone to Virtual Machine**. The Select a name and folder page opens.

Select a Virtual Machine to Clone

You select a virtual machine to clone, and you can optionally select to customize the guest operating system and the virtual machine hardware. You can also select to turn on the virtual machine when you complete the creation procedure. You can change the properties of the guest operating system, such as the computer name, and network and license settings, which helps prevent conflicts that can result if virtual machines with identical settings are deployed. You can add a CD device such as an ISO file to install the guest operating system, or reconfigure the virtual machines' hardware, such as storage or networking, before you deploy the virtual machine.

This page appears only if you opened the New Virtual Machine wizard from a inventory object that is not a template.

NOTE If you start the deploy operation from a template, you select the customization and power options on a later page in the wizard.

Procedure

1 Search for or browse to the virtual machine, and select it.

2 (Optional) Select **Customize the operating system** to customize the guest operating system of the virtual machine.

3 (Optional) Select **Customize this virtual machine's hardware** to configure the virtual machine's hardware before deployment.

4 (Optional) Select **Power On Virtual Machine after creation** to power on the virtual machine after creation is complete.

5 Click **Next**.

Select the Virtual Machine Name and Folder

When you create a virtual machine, you provide a unique name for it. The unique name distinguishes it from existing virtual machines in the virtual machine folder or datacenter. The name can contain up to 80 characters. You can select a datacenter or folder location for the virtual machine, depending on your organizational needs.

Folders provide a way to store virtual machines for different groups in an organization, and you can set permissions on them. For a flatter hierarchy, you can put all virtual machines and templates in a datacenter and organize them a different way.

The virtual machine name determines the name of the virtual machine files and folder on the disk. For example, if you name the virtual machine win8, the virtual machine files are named win8.vmx, win8.vmdk, win8.nvram, and so on. If you change the virtual machine name, the names of the files on the datastore do not change.

Procedure

1 Type a name for the virtual machine.

2 Select or search for the datacenter or folder in which to deploy the virtual machine.

3 Click **Next**.

Select a Resource

When you deploy a virtual machine, you select the host, cluster, vApp, or resource pool for the virtual machine to run in. The virtual machine will have access to the resources of the selected object.

For example, a virtual machine has access to the memory and CPU resources of the host on which it resides. If you select a cluster for the virtual machine, and the administrator has configured the cluster to take advantage of HA and DRS, the virtual machine will have a greater level of availability.

Procedure

1 Search or browse for the host, cluster, vApp, or resource pool for the virtual machine.

   If deploying the virtual machine to the selected location might cause compatibility problems, the problems appear at the bottom of the window.

2 Click **Next**.

Select a Datastore

Select the datastore or datastore cluster in which to store the virtual machine configuration files and all of the virtual disks. Each datastore might have a different size, speed, availability, and other properties. The available datastores are accessible from the destination resource that you selected. You can select a format for the virtual machine's disks and assign a storage policy.

The amount of free space in the datastore is always changing. Ensure that you leave sufficient space for virtual machine creation and other virtual machine operations, such as growth of sparse files, snapshots, and so on. To review space utilization for the datastore by file type, see the *vSphere Monitoring and Performance* documentation.

Thin provisioning lets you create sparse files with blocks that are allocated upon first access, which allows the datastore to be over-provisioned. The sparse files can continue growing and fill the datastore. If the datastore runs out of disk space while the virtual machine is running, it can cause the virtual machine to stop functioning.

Procedure

1 Select the format for the virtual machine's disks.

Option	Action
Same format as source	Use the same format as the source virtual machine.
Thick Provision Lazy Zeroed	Create a virtual disk in a default thick format. Space required for the virtual disk is allocated during creation. Any data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine.
Thick Provision Eager Zeroed	Create a thick disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out during creation. It might take longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can grow to the maximum capacity allocated to it.

2 (Optional) Select a storage policy from the **VM Storage Policy** drop-down menu.

   Storage policies specify storage requirements for applications that run on the virtual machine.

3 Select a datastore location for the virtual disk.

Option	Action
Store the virtual disk and virtual machine configuration files in the same location on a datastore.	Select **Store with the virtual machine** from the **Location** drop-down menu.
Store the disk in a separate datastore location.	Select **Browse** from the **Location** drop-down menu, and select a datastore for the disk.
Store all virtual machine files in the same datastore cluster.	a Select **Browse** from the Location drop-down menu and select a datastore cluster for the disk. b (Optional) If you do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the datastore cluster.

4 Click **Next**.

Select Clone Options

You can optionally select to customize the guest operating system, customize the virtual machine's hardware, and turn on the virtual machine when you complete the creation procedure. You can customize the guest operating system to change properties, such as the computer name, and network and license settings, which helps prevent conflicts that can result if you deploy virtual machines with identical settings. You can add a CD device such as an ISO file to install the guest operating system or you can reconfigure the virtual machine storage or networking, before you deploy the virtual machine.

NOTE If you opened the wizard from an object other than a virtual machine or template, the Select Clone Options page does not appear. These options are available on a different page of the wizard.

Procedure

1 Select **Customize the Operating System**.

2 Select **Customize this virtual machine's hardware**.

3 Select **Power on virtual machine after creation**.

4 Click **Next**.

Customize the Guest Operating System

When you customize a guest operating system, you can prevent conflicts that might result if you deploy virtual machines with identical settings, such as duplicate computer names. You can change the computer name, network settings, and license settings. You can customize guest operating systems when you clone a virtual machine or deploy a virtual machine from a template.

Prerequisites

To access customization options for Windows guest operating systems, Microsoft Sysprep tools must be installed on the vCenter Server system. The Sysprep Tool is built into the Windows Vista and Windows 2008 and later operating systems. For details about this and other customization requirements, see "Guest Operating System Customization Requirements," on page 47.

Procedure

1 Apply a customization specification to the virtual machine.

Option	Description
Select an existing specification	Select a customization specification from the list.
Create a specification	Click the **Create a new specification** icon, and complete the steps in the wizard.
Create a specification from an existing specification	a Select a customization specification from the list. b Click the **Create a spec from an existing spec** icon, and complete the steps in the wizard.

2 Click **Next**.

Customize Virtual Machine Hardware

Before you deploy a new virtual machine, you have the option to configure the virtual hardware. When you create a virtual machine, the virtual disk is selected by default. You can use the **New device** drop-down menu on the Customize Hardware page to add a new hard disk, select an existing disk, or add an RDM disk.

For information about virtual disk configuration, including instructions for adding different types of disks, see "Add a Hard Disk to a Virtual Machine," on page 118.

For help configuring other virtual machine hardware, see Chapter 6, "Configuring Virtual Machine Hardware," on page 89.

Procedure

1 (Optional) To add a new virtual hardware device, select the device from the **New device** drop-down menu and click **Add**.

2 (Optional) Expand any device to view and configure the device settings.

3 To remove a device, move your cursor over the device and click the **Remove** icon.

This icon appears only for virtual hardware that you can safely remove.

4 Click **Next**.

Finish Virtual Machine Creation

Before you deploy the virtual machine, you can review the virtual machine settings.

Procedure

1 Review the virtual machine settings and make changes by clicking **Back** to go back to the relevant page.

2 Click **Finish**.

The virtual machine appears in the vSphere Web Client inventory.

Clone a Virtual Machine to a Template in the vSphere Web Client

After you create a virtual machine, you can clone it to a template. Templates are master copies of virtual machines that let you create ready-for-use virtual machines. You can make changes to the template, such as installing additional software in the guest operating system, while preserving the original virtual machine.

You cannot modify templates after you create them. To alter an existing template, you must convert it to a virtual machine, make the required changes, and convert the virtual machine back to a template. To preserve the original state of a template, clone the template to a template.

Prerequisites

If a load generator is running in the virtual machine, stop it before you perform the clone operation.

Verify that you have the following privileges:

- **Virtual machine.Provisioning.Create template from virtual machine** on the source virtual machine.
- **Virtual machine .Inventory.Create from existing** on virtual machine folder where the template is created.
- **Resource.Assign virtual machine to resource pool** on the destination host, cluster, or resource pool.
- **Datastore.Allocate space** on all datastores where the template is created.

Procedure

1 Start the Clone a Virtual Machine to a Template Task on page 38

   To make a master copy of a virtual machine, you can clone the virtual machine to a template. You can open the New Virtual Machine wizard from any object in the inventory that is a valid parent object of a virtual machine, or directly from the template. The wizard provides several options for creating and deploying virtual machines and templates.

2 Select a Virtual Machine to Clone to a Template on page 39

   To clone a virtual machine to a template, you must select an existing virtual machine to clone. You cannot modify a template after you create it. To change the template, you must convert it back to a virtual machine.

3 Select a Name and Location for the Template on page 39

   When you deploy a template to the vCenter Server inventory, you provide a unique name for it. The unique name distinguishes it from existing templates in the virtual machine folder or datacenter. The name can contain up to 80 characters. You can select a datacenter or folder location for the template, depending on your organizational needs.

4 Select a Resource for a Virtual Machine Template on page 40

   When you deploy a virtual machine template, select a host or cluster resource for the template. The template must be registered with an ESXi host. The host handles all requests for the template and must be running when you create a virtual machine from the template.

5 Select a Datastore for the Virtual Machine Template on page 40

   Each virtual machine or virtual machine template requires a folder or directory for its virtual disks and files. When you create a virtual machine or template to deploy to the vCenter Server inventory, select a datastore or datastore cluster for the virtual machine's configuration and other files and all of the virtual disks. Each datastore can have a different size, speed, availability, and other properties.

6 Finish Virtual Machine Template Creation on page 41

   Before you deploy the template, you can review the template settings.

Start the Clone a Virtual Machine to a Template Task

To make a master copy of a virtual machine, you can clone the virtual machine to a template. You can open the New Virtual Machine wizard from any object in the inventory that is a valid parent object of a virtual machine, or directly from the template. The wizard provides several options for creating and deploying virtual machines and templates.

If you open the wizard from a template, the Select a creation type page does not appear.

Procedure

◆ Select an option to clone a virtual machine to a template.

Option	Description
Open the New Virtual Machine wizard from any object in the inventory	a Right-click any inventory object that is a valid parent object of a virtual machine, such as a datacenter, folder, cluster, resource pool, or host, and select **New Virtual Machine**. b Select **Clone Virtual Machine to Template** and click **Next**. The Select a name and folder page opens.
Open the Clone Virtual Machine to Template wizard from a template	Right-click the virtual machine and select **All vCenter Actions > Template > Clone to Template** . The Select a name and folder page opens.

Select a Virtual Machine to Clone to a Template

To clone a virtual machine to a template, you must select an existing virtual machine to clone. You cannot modify a template after you create it. To change the template, you must convert it back to a virtual machine.

This page appears only if you opened the New Virtual Machine wizard from an inventory object other than a virtual machine, such as a host or cluster. If you opened the wizard from a virtual machine, this page does not appear.

Procedure

1 Browse or search for the virtual machine and select it.

2 Click **Next**.

Select a Name and Location for the Template

When you deploy a template to the vCenter Server inventory, you provide a unique name for it. The unique name distinguishes it from existing templates in the virtual machine folder or datacenter. The name can contain up to 80 characters. You can select a datacenter or folder location for the template, depending on your organizational needs.

Folders provide a way to store virtual machines and templates for different groups in an organization and you can set permissions on them. If you prefer a flatter hierarchy, you can put all virtual machines and templates in a datacenter and organize them a different way.

The template name determines the name of the files and folder on the disk. For example, if you name the template win8tmp, the template files are named win8tmp.vmdk, win8tmp.nvram, and so on. If you change the template name, the names of the files on the datastore do not change.

Procedure

1 Type a name for the template.

2 Select or search for the datacenter or folder in which to deploy the template.

3 Click **Next**.

Select a Resource for a Virtual Machine Template

When you deploy a virtual machine template, select a host or cluster resource for the template. The template must be registered with an ESXi host. The host handles all requests for the template and must be running when you create a virtual machine from the template.

Procedure

1 Search or browse for the host or cluster and select it.

Any Compatibility problems appear at the bottom of the window.

2 Click **Next**.

Select a Datastore for the Virtual Machine Template

Each virtual machine or virtual machine template requires a folder or directory for its virtual disks and files. When you create a virtual machine or template to deploy to the vCenter Server inventory, select a datastore or datastore cluster for the virtual machine's configuration and other files and all of the virtual disks. Each datastore can have a different size, speed, availability, and other properties.

The amount of free space in the datastore is always changing. Ensure that you leave sufficient space for virtual machine creation and other virtual machine operations, such as growth of sparse files, snapshots, and so on. To review space utilization for the datastore by file type, see the *vSphere Monitoring and Performance* documentation.

Thin provisioning lets you create sparse files with blocks that are allocated upon first access, which allows the datastore to be over-provisioned. The sparse files can continue growing and fill the datastore. If the datastore runs out of disk space while the virtual machine is running, it can cause the virtual machine to stop functioning.

Procedure

1 Select the format for the virtual machine's disks.

Option	Action
Same format as source	Use the same format as the source virtual machine.
Thick Provision Lazy Zeroed	Create a virtual disk in a default thick format. Space required for the virtual disk is allocated during creation. Any data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine.
Thick Provision Eager Zeroed	Create a thick disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out during creation. It might take longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can grow to the maximum capacity allocated to it.

2 (Optional) Select a storage policy from the **VM Storage Policy** drop-down menu.

Storage policies specify storage requirements for applications that run on the virtual machine.

3 Select a datastore location for the virtual disk.

Option	Action
Store the virtual disk and virtual machine configuration files in the same location on a datastore.	Select **Store with the virtual machine** from the **Location** drop-down menu.
Store the disk in a separate datastore location.	Select **Browse** from the **Location** drop-down menu, and select a datastore for the disk.
Store all virtual machine files in the same datastore cluster.	a Select **Browse** from the Location drop-down menu and select a datastore cluster for the disk. b (Optional) If you do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the datastore cluster.

4 Click **Next**.

Finish Virtual Machine Template Creation

Before you deploy the template, you can review the template settings.

Procedure

1 Review the template settings and make any necessary changes by clicking **Back** to go back to the relevant page.

2 Click **Finish**.

The progress of the clone task appears in the Recent Tasks pane. When the task completes, the template appears in the inventory.

Clone a Template to a Template in the vSphere Web Client

After you create a template, you can clone it to a template. Templates are master copies of virtual machines that let you create ready-for-use virtual machines. You can make changes to the template, such as installing additional software in the guest operating system, while preserving the state of the original template.

Prerequisites

Verify that you have the following privileges:

- **Virtual machine.Provisioning.Clone template** on the source template.
- **Virtual machine .Inventory.Create from existing** on the folder where the template is created.
- **Datastore.Allocate space** on all datastores where the template is created.

Procedure

1 Start the Clone a Template to a Template Task on page 42

To make changes to a template and preserve the state of the original template, you clone the template to a template.

2 Select a Template to Clone in the vSphere Web Client on page 42

If you started the New Virtual Machine wizard from an inventory object other than a template, you select a template to clone.

3 Select a Name and Location for the Template on page 43

When you deploy a template to the vCenter Server inventory, you provide a unique name for it. The unique name distinguishes it from existing templates in the virtual machine folder or datacenter. The name can contain up to 80 characters. You can select a datacenter or folder location for the template, depending on your organizational needs.

4 Select a Resource for a Virtual Machine Template on page 43

When you deploy a virtual machine template, select a host or cluster resource for the template. The template must be registered with an ESXi host. The host handles all requests for the template and must be running when you create a virtual machine from the template.

5 Select a Datastore for the Virtual Machine Template on page 43

Each virtual machine or virtual machine template requires a folder or directory for its virtual disks and files. When you create a virtual machine or template to deploy to the vCenter Server inventory, select a datastore or datastore cluster for the virtual machine's configuration and other files and all of the virtual disks. Each datastore can have a different size, speed, availability, and other properties.

6 Finish Virtual Machine Template Creation on page 44

Before you deploy the template, you can review the template settings.

Start the Clone a Template to a Template Task

To make changes to a template and preserve the state of the original template, you clone the template to a template.

You can open the New Virtual Machine wizard from any object in the inventory that is a valid parent object of a virtual machine, or directly from the template. The wizard provides several options for creating and deploying virtual machines and templates.

If you open the wizard from a template, the Select a creation type page does not appear.

Procedure

◆ Select to clone a template to a template.

Option	Description
Open the New Virtual Machine wizard from any object in the inventory	a Right-click any inventory object that is a valid parent object of a virtual machine, such as a datacenter, folder, cluster, resource pool, or host, and select **New Virtual Machine**. b Select **Clone Template to Template** and click **Next**. The Select a name and folder page opens.
Open the Clone Template to Template wizard from a template	a Search or browse for a template. b Right-click the template and select **Clone**. The Select a name and folder page opens.

Select a Template to Clone in the vSphere Web Client

If you started the New Virtual Machine wizard from an inventory object other than a template, you select a template to clone.

This page appears only if you opened the wizard from a nontemplate inventory object, such as a host or cluster. If you opened the Convert Template to Virtual Machine wizard from a template, this page does not appear.

Procedure

1 Accept the default template, the template from which you opened the **New Virtual Machine** wizard, or select a different template.

2 Click **Next**.

Select a Name and Location for the Template

When you deploy a template to the vCenter Server inventory, you provide a unique name for it. The unique name distinguishes it from existing templates in the virtual machine folder or datacenter. The name can contain up to 80 characters. You can select a datacenter or folder location for the template, depending on your organizational needs.

Folders provide a way to store virtual machines and templates for different groups in an organization and you can set permissions on them. If you prefer a flatter hierarchy, you can put all virtual machines and templates in a datacenter and organize them a different way.

The template name determines the name of the files and folder on the disk. For example, if you name the template win8tmp, the template files are named win8tmp.vmdk, win8tmp.nvram, and so on. If you change the template name, the names of the files on the datastore do not change.

Procedure

1 Type a name for the template.

2 Select or search for the datacenter or folder in which to deploy the template.

3 Click **Next**.

Select a Resource for a Virtual Machine Template

When you deploy a virtual machine template, select a host or cluster resource for the template. The template must be registered with an ESXi host. The host handles all requests for the template and must be running when you create a virtual machine from the template.

Procedure

1 Search or browse for the host or cluster and select it.

   Any Compatibility problems appear at the bottom of the window.

2 Click **Next**.

Select a Datastore for the Virtual Machine Template

Each virtual machine or virtual machine template requires a folder or directory for its virtual disks and files. When you create a virtual machine or template to deploy to the vCenter Server inventory, select a datastore or datastore cluster for the virtual machine's configuration and other files and all of the virtual disks. Each datastore can have a different size, speed, availability, and other properties.

The amount of free space in the datastore is always changing. Ensure that you leave sufficient space for virtual machine creation and other virtual machine operations, such as growth of sparse files, snapshots, and so on. To review space utilization for the datastore by file type, see the *vSphere Monitoring and Performance* documentation.

Thin provisioning lets you create sparse files with blocks that are allocated upon first access, which allows the datastore to be over-provisioned. The sparse files can continue growing and fill the datastore. If the datastore runs out of disk space while the virtual machine is running, it can cause the virtual machine to stop functioning.

Procedure

1 Select the format for the virtual machine's disks.

Option	Action
Same format as source	Use the same format as the source virtual machine.
Thick Provision Lazy Zeroed	Create a virtual disk in a default thick format. Space required for the virtual disk is allocated during creation. Any data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine.
Thick Provision Eager Zeroed	Create a thick disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out during creation. It might take longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can grow to the maximum capacity allocated to it.

2 (Optional) Select a storage policy from the **VM Storage Policy** drop-down menu.

Storage policies specify storage requirements for applications that run on the virtual machine.

3 Select a datastore location for the virtual disk.

Option	Action
Store the virtual disk and virtual machine configuration files in the same location on a datastore.	Select **Store with the virtual machine** from the **Location** drop-down menu.
Store the disk in a separate datastore location.	Select **Browse** from the **Location** drop-down menu, and select a datastore for the disk.
Store all virtual machine files in the same datastore cluster.	a Select **Browse** from the Location drop-down menu and select a datastore cluster for the disk. b (Optional) If you do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the datastore cluster.

4 Click **Next**.

Finish Virtual Machine Template Creation

Before you deploy the template, you can review the template settings.

Procedure

1 Review the template settings and make any necessary changes by clicking **Back** to go back to the relevant page.

2 Click **Finish**.

The progress of the clone task appears in the Recent Tasks pane. When the task completes, the template appears in the inventory.

Convert a Template to a Virtual Machine

Converting a template to a virtual machine changes the template. This action does not make a copy. You convert a template to a virtual machine to edit the template. You might also convert a template to a virtual machine if you do not need to preserve it as a master image for deploying virtual machines.

Prerequisites

Verity that you have the following privileges:

- **Virtual machine.Provisioning.Mark as virtual machine** on the source template.
- **Resource.Assign virtual machine to resource pool** on the resource pool where the virtual machine will run.

Procedure

1 Start the Convert a Template to a Virtual Machine Task on page 45

   To reconfigure a template with new or updated hardware or applications, you must convert the template to a virtual machine and clone the virtual machine back to a template. In some cases, you might convert a template to a virtual machine because you no longer need the template.

2 Select a Template from Which to Deploy the Virtual Machine on page 46

   On the Select a template page of the wizard, you select a template to deploy from the list.

3 Select a Resource on page 46

   When you deploy a virtual machine, you select the host, cluster, vApp, or resource pool for the virtual machine to run in. The virtual machine will have access to the resources of the selected object.

4 Finish Virtual Machine Creation on page 46

   Before you deploy the virtual machine, you can review the virtual machine settings.

Start the Convert a Template to a Virtual Machine Task

To reconfigure a template with new or updated hardware or applications, you must convert the template to a virtual machine and clone the virtual machine back to a template. In some cases, you might convert a template to a virtual machine because you no longer need the template.

You can open the New Virtual Machine wizard from any object in the inventory that is a valid parent object of a virtual machine, or directly from the template. The wizard provides several options for creating and deploying virtual machines and templates.

If you open the wizard from a template, the Select a creation type page does not appear.

This task provides steps to convert a template to a virtual machine. To clone a virtual machine back to a template, see Clone a Virtual Machine to a Template in the vSphere Web Client.

Procedure

◆ Select how to convert a template to a virtual machine.

Option	Description
Open the New Virtual Machine wizard from any object in the inventory	a Right-click any inventory object that is a valid parent object of a virtual machine, such as a datacenter, folder, cluster, resource pool, or host, and select **New Virtual Machine**. b Select **Convert template to virtual machine** and click **Next**. The Select a resource page opens.
Open the Convert Template to Virtual Machine wizard from a template	a Search or browse for a template. b Right-click the template and select **Convert to Virtual Machine**. The Select a resource page opens.

Select a Template from Which to Deploy the Virtual Machine

On the Select a template page of the wizard, you select a template to deploy from the list.

This page appears only if you opened the New Virtual Machine wizard from a nontemplate inventory object, such as a host or cluster. If you opened the Convert Template to Virtual Machine wizard from a template, this page does not appear.

Procedure

1 Browse or search to locate a template.

2 Select the template.

3 Click **Next**.

Select a Resource

When you deploy a virtual machine, you select the host, cluster, vApp, or resource pool for the virtual machine to run in. The virtual machine will have access to the resources of the selected object.

For example, a virtual machine has access to the memory and CPU resources of the host on which it resides. If you select a cluster for the virtual machine, and the administrator has configured the cluster to take advantage of HA and DRS, the virtual machine will have a greater level of availability.

Procedure

1 Search or browse for the host, cluster, vApp, or resource pool for the virtual machine.

   If deploying the virtual machine to the selected location might cause compatibility problems, the problems appear at the bottom of the window.

2 Click **Next**.

Finish Virtual Machine Creation

Before you deploy the virtual machine, you can review the virtual machine settings.

Procedure

1 Review the virtual machine settings and make changes by clicking **Back** to go back to the relevant page.

2 Click **Finish**.

The virtual machine appears in the vSphere Web Client inventory.

Customizing Guest Operating Systems

When you clone a virtual machine or deploy a virtual machine from a template, you can customize the guest operating system of the virtual machine to change properties such as the computer name, network settings, and license settings.

Customizing guest operating systems can help prevent conflicts that can result if virtual machines with identical settings are deployed, such as conflicts due to duplicate computer names.

You can specify the customization settings by launching the Guest Customization wizard during the cloning or deployment process. Alternatively, you can create customization specifications, which are customization settings stored in the vCenter Server database. During the cloning or deployment process, you can select a customization specification to apply to the new virtual machine.

Use the Customization Specification Manager to manage customization specifications you create with the Guest Customization wizard.

Guest Operating System Customization Requirements

To customize the guest operating system, you must configure the virtual machine and guest to meet VMware Tools and virtual disk requirements. Other requirements apply, depending on the guest operating system type.

VMware Tools Requirements

The latest version of VMware Tools must be installed on the virtual machine or template to customize the guest operating system during cloning or deployment. For information about VMware Tools support matrix, see the *VMware Product Interoperability Matrixes* at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Virtual Disk Requirements

The guest operating system being customized must be installed on a disk attached as SCSI node 0:0 in the virtual machine configuration.

Windows Requirements

Customization of Windows guest operating systems requires the following conditions:

- Microsoft Sysprep tools must be installed on the vCenter Server system. See Chapter 5, "Installing the Microsoft Sysprep Tool," on page 87.
- The ESXi host that the virtual machine is running on must be 3.5 or later.

Guest operating system customization is supported on multiple Windows operating systems.

Linux Requirements

Customization of Linux guest operating systems requires that Perl is installed in the Linux guest operating system.

Guest operating system customization is supported on multiple Linux distributions.

Verifying Customization Support for a Guest Operating System

To verify customization support for Windows operating systems or Linux distributions and compatible ESXi hosts, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility. You can use this online tool to search for the guest operating system and ESXi version. After the tool generates your list, click the guest operating system to see whether guest customization is supported.

Create a vCenter Server Application to Generate Computer Names and IP Addresses

As an alternative to entering computer names and IP addresses for virtual NICs when you customize guest operating systems, you can create a custom application and configure it so that vCenter Server can generate the names and addresses.

The application can be an arbitrary executable binary or script file appropriate for the corresponding operating system in which vCenter Server is running. After you configure an application and make it available to vCenter Server, each time you initiate a guest operating system customization for a virtual machine, vCenter Server executes the application.

The application must comply with the reference XML file in the VMware knowledge base article at http://kb.vmware.com/kb/2007557.

Prerequisites

Verify that Perl is installed on vCenter Server.

Procedure

1 Create the application and save it on the vCenter Server system's local disk.

2 Select a vCenter Server instance in the inventory.

3 Click the **Manage** tab, click **Settings**, and click **Advanced Settings**.

4 Click **Edit** and enter the configuration parameters for the script.

   a In the **Key** text box, type **`config.guestcust.name-ip-generator.arg1`**.

   b In the **Value** text box, type **`c:\sample-generate-name-ip.pl`** and click **Add**.

   c In the **Key** text box, type **`config.guestcust.name-ip-generator.arg2`**.

   d In the **Value** text box, type the path to the script file on the vCenter Server system and click **Add**. For example, type **`c:\sample-generate-name-ip.pl`**.

   e In the **Key** text box, type **`config.guestcust.name-ip-generator.program`**.

   f In the **Value** text box, type **`c:\perl\bin\perl.exe`** and click **Add**.

5 Click **OK**.

You can select the option to use an application to generate computer names or IP addresses during guest operating system customization.

Customize Windows During Cloning or Deployment

You can customize Windows guest operating systems for the virtual machine when you deploy a new virtual machine from a template or clone an existing virtual machine. Customizing the guest helps prevent conflicts that can result if virtual machines with identical settings are deployed, such as duplicate computer names.

You can prevent Windows from assigning new virtual machines or templates with the same Security IDs (SIDs) as the original virtual machine. Duplicate SIDs do not cause problems when the computers are part of a domain and only domain user accounts are used. However, if the computers are part of a Workgroup or local user accounts are used, duplicate SIDs can compromise file access controls. For more information, see the documentation for your Microsoft Windows operating system.

Important The default administrator password is not preserved for Windows Server 2008 after customization. During customization, the Windows Sysprep utility deletes and recreates the administrator account on Windows Server 2008. You must reset the administrator password when the virtual machine starts the first time after customization.

Prerequisites

Verify that all requirements for customization are met. See "Guest Operating System Customization Requirements," on page 47.

To perform this procedure, start the Guest Customization wizard when you clone a virtual machine or deploy one from a template.

Procedure

1 On the Select clone options page of the Clone Existing Virtual Machine wizard, select **Customize the operating system** and click **Next**.

2 Type the virtual machine owner's name and organization and click **Next**.

3 Enter the guest operating system's computer name.

The operating system uses this name to identify itself on the network. On Linux systems, it is called the host name.

Option	Action
Enter a name	a Type a name. The name can contain alphanumeric characters and the hyphen (-) character. It cannot contain periods (.) or blank spaces and cannot be made up of digits only. Names are not case-sensitive. b (Optional) To ensure that the name is unique, select **Append a numeric value to ensure uniqueness**. This action appends a hyphen followed by a numeric value to the virtual machine name. The name is truncated if it exceeds 63 characters when combined with the numeric value.
Use the virtual machine name	The computer name that vCenter Server creates is identical to the name of the virtual machine on which the guest operating system is running. If the name exceeds 63 characters, it is truncated.
Enter a name in the Clone/Deploy wizard	The vSphere Web Client prompts you to enter a name after the cloning or deployment is complete.
Generate a name using the custom application configured with vCenter Server	Enter a parameter that can be passed to the custom application.

4 Provide licensing information for the Windows operating system and click **Next**.

Option	Action
For non-server operating systems	Type the Windows product key for the new guest operating system.
For server operating systems	a Type the Windows product key for the new guest operating system. b Select **Include Server License Information**. c Select either **Per seat** or **Per server**. d If you selected **Per server**, enter the maximum number of simultaneous connections for the server to accept.

5 Configure the administrator password for the virtual machine and click **Next**.

a Type a password for the administrator account and confirm the password by typing it again.

NOTE You can change the administrator password only if the administrator password on the source Windows virtual machine is blank. If the source Windows virtual machine or template already has a password, the administrator password does not change.

b (Optional) To log users into the guest operating system as Administrator, select the check box, and select the number of times to log in automatically.

6 Select the time zone for the virtual machine and click **Next**.

7 (Optional) On the Run Once page, specify commands to run the first time a user logs into the guest operating system and click **Next**.

See the Microsoft Sysprep documentation for information about `RunOnce` commands.

8 Select the type of network settings to apply to the guest operating system.

Option	Action
Typical settings	Select **Typical settings** and click **Next**. vCenter Server configures all network interfaces from a DHCP server using default settings.
Custom settings	a Select **Custom settings** and click **Next**. b For each network interface in the virtual machine, click the ellipsis button (**...**) . c Enter IP address and other network settings and click **OK**. d When all network interfaces are configured, click **Next**.

9 To specify IPv4 related settings, select **IPv4** and enter IP address and other network settings.

10 Select **IPv6** to configure the virtual machine to use IPv6 network.

Note that the virtual machine can retain the IP address allocated from the network as well as IPv6 addresses. Microsoft supports IPv6 for Windows Server 2003, Windows XP with Service Pack 1 (SP1) or later, and Windows CE .NET 4.1 or later. However, these operating systems have limited IPv6 support for built-in applications, system services, and are not recommended for IPv6 deployment.

a Select **Prompt user for an address when the specification is used**. Selecting this option prompts you to enter either IPv4 or IPv6 address.

b Select **Use the following IPv6 addresses** to choose an IPv6 address from the list.

- Click the **pencil** icon to enter additional IPv6 addresses. You can specify the full address or shorten it by using zero compression and zero suppression. You should specify at least one IPv6 address. You can edit an existing address, but should not duplicate existing IPv6 addresses.
- Enter subnet mask prefix. The prefix length should be between 1 to 128 where the default value is 64. Gateway is enabled by default, except when you choose **Do not use IPv6**.

11 Select **DNS** and specify DNS server address and click **OK**.

12 Select **WINS** and specify primary and secondary WINS information.

13 Select how the virtual machine will participate in the network and click **Next**.

Option	Action
Workgroup	Type a workgroup name. For example, `MSHOME`.
Windows Server Domain	a Type the domain name. b Type the user name and password for a user account that has permission to add a computer to the specified domain.

14 Select Generate New Security ID (SID) and click **Next**.

A Windows Security ID (SID) is used in some Windows operating systems to uniquely identify systems and users. If you do not select this option, the new virtual machine has the same SID as the virtual machine or template from which it was cloned or deployed.

15 Save the customized options as an `.xml` file.

a Select **Save this customization specification for later use**.

b Specify the filename for the specification and click **Next**.

16 Click **Finish** to save your changes.

You return to the Deploy Template or to the Clone Virtual Machine wizard. The customization is finished after you complete the Deploy Template or the Clone Virtual Machine wizard.

When the new virtual machine starts for the first time, the guest operating system runs finalization scripts to complete the customization process. The virtual machine might restart several times during this process.

If the guest operating system pauses when the new virtual machine starts, it might be waiting for you to correct errors, such as an incorrect product key or an invalid user name. Open the virtual machine's console to determine whether the system is waiting for information.

What to do next

After you deploy and customize versions of Windows XP or Windows 2003 that are not volume licensed, you might need to reactivate your operating system on the new virtual machine.

If the new virtual machine encounters customization errors while it is starting, the errors are logged to `%WINDIR%\temp\vmware-imc`. To view the error log file, click the Windows **Start** button and select **Programs > Administrative Tools > Event Viewer**.

Customize Linux During Cloning or Deployment

In the process of deploying a new virtual machine from a template or cloning an existing virtual machine, you can customize Linux guest operating systems for the virtual machine.

Prerequisites

Ensure that all requirements for customization are met. See "Guest Operating System Customization Requirements," on page 47.

To perform this procedure, start the Customization wizard when you clone a virtual machine or deploy one from a template.

Procedure

1 On the Select clone options page of the Clone Existing Virtual Machine wizard, select **Customize the operating system** and click **Next**.

2 Enter the guest operating system's computer name.

The operating system uses this name to identify itself on the network. On Linux systems, it is called the host name.

Option	Action
Enter a name	a Type a name. The name can contain alphanumeric characters and the hyphen (-) character. It cannot contain periods (.) or blank spaces and cannot be made up of digits only. Names are not case-sensitive. b (Optional) To ensure that the name is unique, select **Append a numeric value to ensure uniqueness**. This action appends a hyphen followed by a numeric value to the virtual machine name. The name is truncated if it exceeds 63 characters when combined with the numeric value.
Use the virtual machine name	The computer name that vCenter Server creates is identical to the name of the virtual machine on which the guest operating system is running. If the name exceeds 63 characters, it is truncated.
Enter a name in the Clone/Deploy wizard	The vSphere Web Client prompts you to enter a name after the cloning or deployment is complete.
Generate a name using the custom application configured with vCenter Server	Enter a parameter that can be passed to the custom application.

3 Enter the **Domain Name** for the computer and click **Next**.

4 Select the time zone for the virtual machine and click **Next**.

5 Select the type of network settings to apply to the guest operating system.

Option	Action
Typical settings	Select **Typical settings** and click **Next**. vCenter Server configures all network interfaces from a DHCP server using default settings.
Custom settings	a Select **Custom settings** and click **Next**. b For each network interface in the virtual machine, click the ellipsis button (**...**) . c Enter IP address and other network settings and click **OK**. d When all network interfaces are configured, click **Next**.

6 To specify IPv4 related settings, select **IPv4** and enter IP address and other network settings.

7 To specify IPv6 related settings, select **IPv6** to configure the virtual machine to use IPv6 network.

Note that the virtual machine can retain the IP address allocated from the network as well as IPv6 addresses.

a Select **Prompt user for an address when the specification is used**. Selecting this option prompt you to enter IPv6 address.

b Select **Use the following IPv6 addresses** to choose an IPv6 address from the list.

- Click the **pencil** icon to enter additional IPv6 addresses. You can specify the full address or shorten it by using zero compression and zero suppression. You should specify at least one IPv6 address. You can edit an existing address, but should not duplicate existing IPv6 addresses.
- Enter subnet mask prefix. The prefix length should be between 1 to 128 where the default value is 64. Gateway is enabled by default, except when you choose **Do not use IPv6**.

8 Enter DNS and domain settings information. The **Primary DNS**, **Secondary DNS**, and **Tertiary DNS** fields accept both IPv4 and IPv6 addresses.

9 Save the customized options as an `.xml` file.

a Select **Save this customization specification for later use**.

b Specify the filename for the specification and click **Next**.

10 Click **Finish** to save your changes.

You return to the Deploy Template or to the Clone Virtual Machine wizard. The customization is finished after you complete the Deploy Template or the Clone Virtual Machine wizard.

When the new virtual machine starts for the first time, the guest operating system runs finalization scripts to complete the customization process. The virtual machine might restart several times during this process.

If the guest operating system pauses when the new virtual machine starts, it might be waiting for you to correct errors, such as an incorrect product key or an invalid user name. Open the virtual machine's console to determine whether the system is waiting for information.

What to do next

If the new virtual machine encounters customization errors while it is starting, the errors are reported using the guest's system logging mechanism. View the errors by opening `/var/log/vmware-imc/toolsDeployPkg.log`.

Apply a Customization Specification to a Virtual Machine

You can add guest OS specification to an existing virtual machine. When you customize a guest operating system, you can prevent conflicts that might result if you deploy virtual machines with identical settings, such as duplicate computer names. You can change the computer name, network settings, and license settings.

When you clone an existing virtual machine, or deploy a virtual machine from a VM template in a folder, you can customize the guest operating system of the resulting virtual machine during the clone or the deployment tasks.

When you deploy a virtual machine from a template in a content library, you can customize the guest operating system only after the deployment task is complete.

Prerequisites

Power off the virtual machine.

Procedure

1 Right-click a virtual machine in the vSphere inventory, and select **Guest OS > Customize Guest OS**.

The Customize Guest OS wizard opens.

2 Apply a customization specification to the virtual machine.

Option	Description
Select an existing specification	Select a customization specification from the list.
Create a specification	Click the **Create a new specification** icon, and complete the steps in the wizard.
Create a specification from an existing specification	a Select a customization specification from the list. b Click the **Create a new specification from existing one** icon, and complete the steps in the wizard.

3 Click **Finish**.

What to do next

Power on the virtual machine.

Creating and Managing Customization Specifications

You can create and manage customization specifications for Windows and Linux guest operating systems. Customization specifications are XML files that contain guest operating system settings for virtual machines. When you apply a specification to the guest operating system during virtual machine cloning or deployment, you prevent conflicts that might result if you deploy virtual machines with identical settings, such as duplicate computer names.

vCenter Server saves the customized configuration parameters in the vCenter Server database. If the customization settings are saved, the administrator and domain administrator passwords are stored in encrypted format in the database. Because the certificate used to encrypt the passwords is unique to each vCenter Server system, if you reinstall vCenter Server or attach a new instance of the server to the database, the encrypted passwords become invalid. You must reenter the passwords before you can use them.

Create a Customization Specification for Linux

Use the Guest Customization wizard to save guest operating system settings in a specification that you can apply when cloning virtual machines or deploying from templates.

Prerequisites

Ensure that all requirements for customization are met. See "Guest Operating System Customization Requirements," on page 47.

Procedure

1 From the vSphere Web Client Home inventory page, select **Rules and Profiles > Customization Specification Manager**.

2 Click the **Create a New specification** icon.

3 Select **Linux** from the **Target VM Operating System** drop-down menu, and enter a name and description for the specification.

4 Enter the guest operating system's computer name.

The operating system uses this name to identify itself on the network. On Linux systems, it is called the host name.

Option	Action
Enter a name	a Type a name. The name can contain alphanumeric characters and the hyphen (-) character. It cannot contain periods (.) or blank spaces and cannot be made up of digits only. Names are not case-sensitive. b (Optional) To ensure that the name is unique, select **Append a numeric value to ensure uniqueness**. This action appends a hyphen followed by a numeric value to the virtual machine name. The name is truncated if it exceeds 63 characters when combined with the numeric value.
Use the virtual machine name	The computer name that vCenter Server creates is identical to the name of the virtual machine on which the guest operating system is running. If the name exceeds 63 characters, it is truncated.
Enter a name in the Clone/Deploy wizard	The vSphere Web Client prompts you to enter a name after the cloning or deployment is complete.
Generate a name using the custom application configured with vCenter Server	Enter a parameter that can be passed to the custom application.

5 Enter the **Domain Name** for the computer and click **Next**.

6 Select the time zone for the virtual machine and click **Next**.

7 Select the type of network settings to apply to the guest operating system.

Option	Action
Standard settings	Select **Use standard network settings** and click **Next**. vCenter Server configures all network interfaces from a DHCP server using default settings.
Custom settings	a Select **Manually select custom settings**. b For each network interface in the virtual machine, click the **pencil** icon.

8 To specify IPv4 related settings, select **IPv4** and enter IP address and other network settings.

9 To specify IPv6 related settings, select **IPv6** to configure the virtual machine to use IPv6 network.

   a Select **Prompt user for an address when the specification is used**. Selecting this option prompts you to enter IPv6 address.

   b Select **Use the following IPv6 addresses** to choose an IPv6 address from the list.

      - Click the **pencil** icon to enter additional IPv6 addresses. You can specify the full address or shorten it by using zero compression and zero suppression. You should specify at least one IPv6 address. You can edit an existing address, but should not duplicate existing IPv6 addresses.

      - Enter subnet mask prefix. The prefix length should be between 1 to 128 where the default value is 64. Gateway is enabled by default, except when you choose **Do not use IPv6**.

10 Enter DNS and domain settings information. The **Primary DNS**, **Secondary DNS**, and **Tertiary DNS** fields accept both IPv4 and IPv6 addresses.

11 Click **Finish** to save your changes.

The customization specification that you created is listed in the Customization Specification Manager. You can use the specification to customize virtual machine guest operating systems.

Create a Customization Specification for Windows

Use the Guest Customization wizard to save Windows guest operating system settings in a specification that you can apply when cloning virtual machines or deploying from templates.

NOTE The default administrator password is not preserved for Windows Server 2008 after customization. During customization, the Windows Sysprep utility deletes and recreates the administrator account on Windows Server 2008. You must reset the administrator password when the virtual machine starts the first time after customization.

Prerequisites

Ensure that all requirements for customization are met. See "Guest Operating System Customization Requirements," on page 47.

Procedure

1 From the vSphere Web Client Home inventory page, select **Rules and Profiles > Customization Specification Manager**.

2 Click the **Create a new specification** icon to open the New VM Guest Customization Spec wizard.

3 Select Windows from the **Target VM Operating System** drop-down menu, and enter a name and optional description for the specification and click **Next**.

4 On the Set Registration Information page, type the virtual machine owner's name and organization and click **Next**.

5 Enter the guest operating system's computer name.

The operating system uses this name to identify itself on the network. On Linux systems, it is called the host name.

Option	Action
Enter a name	a Type a name. The name can contain alphanumeric characters and the hyphen (-) character. It cannot contain periods (.) or blank spaces and cannot be made up of digits only. Names are not case-sensitive. b (Optional) To ensure that the name is unique, select **Append a numeric value to ensure uniqueness**. This action appends a hyphen followed by a numeric value to the virtual machine name. The name is truncated if it exceeds 63 characters when combined with the numeric value.
Use the virtual machine name	The computer name that vCenter Server creates is identical to the name of the virtual machine on which the guest operating system is running. If the name exceeds 63 characters, it is truncated.
Enter a name in the Clone/Deploy wizard	The vSphere Web Client prompts you to enter a name after the cloning or deployment is complete.
Generate a name using the custom application configured with vCenter Server	Enter a parameter that can be passed to the custom application.

6 Provide licensing information for the Windows operating system and click **Next**.

Option	Action
For nonserver operating systems	Type the Windows product key for the new guest operating system.
For server operating systems	a Type the Windows product key for the new guest operating system. b Select **Include Server License Information**. c Select either **Per seat** or **Per server**. d If you select **Per server**, enter the maximum number of simultaneous connections for the server to accept.

7 Configure the administrator password for the virtual machine and click **Next**.

a Type a password for the administrator account and confirm the password by typing it again.

Note You can change the administrator password only if the administrator password on the source Windows virtual machine is blank. If the source Windows virtual machine or template already has a password, the administrator password does not change.

b (Optional) To log users into the guest operating system as Administrator, select the check box, and select the number of times to log in automatically.

8 Select the time zone for the virtual machine and click **Next**.

9 (Optional) On the Run Once page, specify commands to run the first time a user logs into the guest operating system and click **Next**.

See the Microsoft Sysprep documentation for information about `RunOnce` commands.

10 Select the type of network settings to apply to the guest operating system.

Option	Action
Standard settings	Select **Use standard network settings** and click **Next**. vCenter Server configures all network interfaces from a DHCP server using default settings.
Custom settings	a Select **Manually select custom settings**. b For each network interface in the virtual machine, click the **pencil** icon.

11 To specify IPv4 related settings, select **IPv4** and enter IP address and other network settings.

12 To specify IPv6 related settings, select **IPv6** to configure the virtual machine to use IPv6 network.

   a Select **Prompt user for an address when the specification is used**. Selecting this option prompts you to enter IPv6 address.

   b Select **Use the following IPv6 addresses** to choose an IPv6 address from the list.

      - Click the **pencil** icon to enter additional IPv6 addresses. You can specify the full address or shorten it by using zero compression and zero suppression. You should specify at least one IPv6 address. You can edit an existing address, but should not duplicate existing IPv6 addresses.

      - Enter subnet mask prefix. The prefix length should be between 1 to 128 where the default value is 64. Gateway is enabled by default, except when you select **Do not use IPv6**.

13 Select **DNS** and specify DNS server address and click **OK**.

14 Select **WINS** and specify primary and secondary WINS information.

15 Select how the virtual machine will participate in the network and click **Next**.

Option	Action
Workgroup	Type a workgroup name. For example, `MSHOME`.
Windows Server Domain	a Type the domain name. b Type the user name and password for a user account that has permission to add a computer to the specified domain.

16 (Optional) Select Generate New Security ID (SID) and click **Next**.

   A Windows Security ID (SID) is used in some Windows operating systems to uniquely identify systems and users. If you do not select this option, the new virtual machine has the same SID as the virtual machine or template from which it was cloned or deployed.

   Duplicate SIDs do not cause problems when the computers are part of a domain and only domain user accounts are used. However, if the computers are part of a Workgroup or local user accounts are used, duplicate SIDs can compromise file access controls. For more information, see the documentation for your Microsoft Windows operating system.

17 Click **Finish** to save your changes.

The customization specification that you created is listed in the Customization Specification Manager. You can use the specification to customize virtual machine guest operating systems.

Create a Customization Specification for Windows Using a Custom Sysprep Answer File in the vSphere Web Client

A custom sysprep answer file is a file that stores a number of customization settings such as computer name, licensing information, and workgroup or domain settings. You can supply a custom sysprep answer file as an alternative to specifying many of the settings in the Guest Customization wizard.

Windows Server 2003, and Windows XP use a text file called `sysprep.inf`. Windows Server 2008, Windows Vista, and Windows 7 use an XML file called `sysprep.xml`. You can create these files using a text editor, or use the Microsoft Setup Manager utility to generate them. For more information about how to create a custom sysprep answer file, see the documentation for the relevant operating system.

You can prevent Windows from assigning new virtual machines or templates with the same Security IDs (SIDs) as the original virtual machine. Duplicate SIDs do not cause problems when the computers are part of a domain and only domain user accounts are used. However, if the computers are part of a Workgroup or local user accounts are used, duplicate SIDs can compromise file access controls. For more information, see the documentation for your Microsoft Windows operating system.

Prerequisites

Ensure that all requirements for customization are met. See "Guest Operating System Customization Requirements," on page 47.

Procedure

1 From the vSphere Web Client Home inventory page, select **Rules and Profiles > Customization Specification Manager**.

2 Click the **Create New Specification** icon.

3 In the Guest Customization wizard, select Windows from the **Target Virtual Machine OS** menu.

4 (Optional) Select **Use Custom Sysprep Answer File**.

5 Under Customization Specification Information, enter a name for the specification and an optional description and click **Next**.

6 Select the option to import or create a sysprep answer file and click **Next**.

Option	Description
Import a Sysprep answer file	Click **Browse** and browse to the file.
Create a Sysprep answer file	Type the contents of the file in the text box.

7 Select the type of network settings to apply to the guest operating system.

Option	Action
Typical settings	Select **Typical settings** and click **Next**. vCenter Server configures all network interfaces from a DHCP server using default settings.
Custom settings	a Select **Custom settings** and click **Next**. b For each network interface in the virtual machine, click the ellipsis button (**...**) . c Enter IP address and other network settings and click **OK**. d When all network interfaces are configured, click **Next**.

8 To specify IPv4 related settings, select **IPv4** and enter IP address and other network settings.

9 To specify IPv6 related settings, select **IPv6** to configure the virtual machine to use IPv6 network.

   a Select **Prompt user for an address when the specification is used**. Selecting this option prompts you to enter IPv4 or IPv6 address.

   b Select **Use the following IPv6 addresses** to choose an IPv6 address from the list.

      - Click the **pencil** icon to enter additional IPv6 addresses. You can specify the full address or shorten it by using zero compression and zero suppression. You should specify at least one IPv6 address. You can edit an existing address, but should not duplicate existing IPv6 addresses.

      - Enter subnet mask prefix. The prefix length should be between 1 to 128 where the default value is 64. Gateway is enabled by default, except when you choose Do not use IPv6.

10 Select **DNS** and specify DNS server address and **OK**.

11 Select **WINS** and specify primary and secondary WINS information.

12 Select Generate New Security ID (SID) and click **Next**.

   A Windows Security ID (SID) is used in some Windows operating systems to uniquely identify systems and users. If you do not select this option, the new virtual machine has the same SID as the virtual machine or template from which it was cloned or deployed.

13 Click **Finish** to save your changes.

The customization specification that you created is listed in the Customization Specification Manager. You can use the specification to customize virtual machine guest operating systems.

Edit a Customization Specification

You can edit existing specifications using the Customization Specification Manager.

Prerequisites

You must have at least one customization specification.

Procedure

1 From the vSphere Web Client Home inventory page, select **Rules and Profiles > Customization Specification Manager**.

2 Right-click a specification and select **Edit**.

3 Proceed through the Guest Customization wizard to change specification settings.

Remove a Customization Specification in the vSphere Web Client

You can remove customization specifications from the Customization Specification Manager.

Prerequisites

You must have at least one customization specification.

Procedure

1 From the vSphere Web Client Home inventory page, select **Rules and Profiles > Customization Specification Manager**.

2 Right-click a specification and select **Remove**.

3 In the confirmation dialog box, select **Yes**.

The specification is deleted from the disk.

Copy a Customization Specification in the vSphere Web Client

If you need a customization specification that is only slightly different from an existing specification, you can use the Customization Specification Manager to create a copy of the existing specification and modify it. For example, you might need to change the IP address or the administrator password.

Prerequisites

You must have at least one customization specification.

Procedure

1 From the vSphere Web Client Home inventory page, select **Rules and Profiles > Customization Specification Manager**.

2 Right-click a specification and select **Duplicate**.

A new specification is created. If the specification does not appear in the Name column, refresh the vSphere Web Client.

Export a Customization Specification in the vSphere Web Client

You can export customization specifications and save them as `.xml` files. To apply an exported specification to a virtual machine, import the .xml file using the Customization Specification Manager.

Prerequisites

You must have at least one customization specification.

Procedure

1 From the vSphere Web Client Home inventory page, select **Rules and Profiles > Customization Specification Manager**.

2 Right-click a specification and select **Export**.

3 Select a location for the file and click **Save**.

The specification is saved as an `.xml` file to the location you specified.

Import a Customization Specification

You can import an existing specification using the Customization Specification Manager, and use the specification to customize the guest operating system of a virtual machine.

Prerequisites

Before you begin, you must have at least one customization specification saved as an xml file located on a file system accessible from the vSphere Web Client.

Procedure

1 From the vSphere Web Client Home inventory page, select **Rules and Profiles > Customization Specification Manager**.

2 Click the **Import specification from a file** icon.

3 From the Open dialog, browse to the `.xml` to import and click **Open**.

The imported specification is added to the list of customization specifications.

Deploying OVF Templates 3

You can export virtual machines, virtual appliances, and vApps in Open Virtual Machine Format (OVF). You can then deploy the OVF template in the same environment or in a different environment.

This chapter includes the following topics:

- "OVF File Format and OVF Templates," on page 63
- "Deploy an OVF Template in the vSphere Web Client," on page 64
- "Browse VMware Virtual Appliance Marketplace," on page 67
- "Export an OVF Template," on page 68

OVF File Format and OVF Templates

OVF is a file format that supports exchange of virtual appliances across products and platforms.

The OVF format offers the following advantages:

- OVF files are compressed, allowing for faster downloads.
- The vSphere Web Client validates an OVF file before importing it, and ensures that it is compatible with the intended destination server. If the appliance is incompatible with the selected host, it cannot be imported and an error message appears.
- OVF can encapsulate multi-tiered applications and more than one virtual machine.

Exporting OVF templates allows you to create virtual appliances that can be imported by other users. You can use the export function to distribute pre-installed software as a virtual appliance, or to distributing template virtual machines to users. You can make the OVF file available to users who cannot access your vCenter Server inventory.

Deploying an OVF template allows you to add pre-configured virtual machines or vApps to your vCenter Server or ESXi inventory. Deploying an OVF template is similar to deploying a virtual machine from a template. However, you can deploy an OVF template from any local file system accessible from the vSphere Web Client, or from a remote Web server. The local file systems can include local disks (such as C:), removable media (such as CDs or USB keychain drives), and shared network drives.

Deploy an OVF Template in the vSphere Web Client

You can deploy an OVF template from a local file system accessible to the vSphere Web Client, or from a URL.

Prerequisites

Install the Client Integration plug-in before you deploy an OVF template. This plug-in enables OVF deployment from your local filesystem. See "Install the Client Integration Plug-In," on page 189.

NOTE Depending on the security settings of your browser, you might have to explicitly approve the plug-in when you use it the first time.

Procedure

1 Select any inventory object that is a valid parent object of a virtual machine, such as a datacenter, folder, cluster, resource pool, or host.

2 Select **Actions > All vCenter Actions > Deploy OVF Template**.

Select the OVF Source Location

Specify the location where the source of OVF template resides.

Procedure

1 Specify the source location.

Option	Action
URL	Type a URL to an OVF template located on the Internet. Supported URL sources are HTTP and FTP. Example: `http://vmware.com/VMTN/appliance.ovf`.
Local file	Click Browse and select an OVF or OVA template from the local file system.

2 Click **Next**.

Review the OVF Details

The OVF template details display available information about the file.

Procedure

1 Review the OVF template details and

Option	Description
Product	Product name, as specified in the OVF template file.
Version	Version, if the version is specified in the OVF template file.
Vendor	Version, if the vendor is specified in the OVF template file.
Publisher	Publisher of the OVF template, if a certificate included in the OVF template file specifies a publisher.
Download size	Size of the OVF file.
Size on disk	Size on disk after you deploy the OVF template.
Description	Description, as provided by the distributor of the OVF template.

2 Click **Next**.

Accept the OVF License Agreements

This page appears only if license agreements are packaged with the OVF template.

Procedure

- Agree to accept the terms of the end user license agreements, and click **Next**.

Select OVF Name and Location

When you deploy an OVF template, you provide a unique name for the virtual machine or vApp. The name can contain up to 80 characters. You can select a datacenter or folder location for the virtual machine.

Procedure

1. (Optional) Specify the name that the virtual machine or vApp will have when it is deployed at the target location.

   The name must be unique within each vCenter Server virtual machine folder.
2. Select or search for a datacenter or folder for the virtual machine or vApp.
3. Click **Next**.

Select OVF Deployment Configuration

The deployment configuration typically controls the memory settings, number of CPUs and reservations, and application-level configuration parameters.

This page appears only if the OVF template contains deployment options.

Procedure

- Select the deployment configuration from the drop-down menu and click **Next**.

Select a Resource for the OVF Template

When you deploy an OVF template, you select the host, cluster, or resource pool. The virtual machine or vApp will have access to the resources of the selected object.

For example, a virtual appliance has access to the memory and CPU resources of the host on which it resides.

If you start the wizard from a resource such as a host, this wizard screen does not appear. But if you start the wizard from a container such as a datacenter of folder, the wizard screen appears.

Procedure

1. Search or browse for the host, cluster, vApp, or resource pool on which you want to deploy the OVF template.

   If deploying the OVF template to the selected location might cause compatibility problems, the problems appear at the bottom of the window.
2. Click **Next**.

Select Storage for OVF Template

Select the location to store the files for the deployed template.

Procedure

1 Select the disk format to store the virtual machine virtual disks.

Format	Description
Thick Provisioned Lazy Zeroed	Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine.
Thick Provision Eager Zeroed	A type of thick virtual disk that supports clustering features such as Fault tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format the data remaining on the physical device is zeroed out when the virtual disk is created. it might take much longer to create disks in this format than to create other types o disks.
Thin Provision	Use this format to save storage space. For the thin disk, you provision as much datastore space as the disk would require based on the value that you enter for the disk size. However, the thin disk starts small and at first, uses only as much datastore space as the disk needs for its initial operations.

2 (Optional) Select a VM Storage Policy.

   This option is available only if storage policies are enabled on the destination resource.

3 Select a datastore to store the deployed OVF template.

   The configuration file and virtual disk files are stored on the datastore. Select a datastore large enough to accommodate the virtual machine or vApp and all associated virtual disk files.

4 (Optional) Disable Storage DRS if you do not want to use it for this virtual machine or vApp.

5 Click **Next**.

Configure Networks for OVF Template

Set up and configure the networks the deployed OVF templates use.

The Setup networks wizard screen allows you to map source networks to target networks, and to specify settings for those networks.

For each network, you can perform the mapping and optional customizations explained in the procedure.

Procedure

1 Select a Source network in the table and map it to a Destination network.

   The Source column lists all networks that are defined in the OVF template. The Destination column allows you to select a target network.

2 If the OVF template is set up to allow network customization, you can select the IP protocol, the IP allocation, or both.

Option	Description
Static - Manual	You will be prompted to enter the IP addresses in the Appliance Properties page.
Transient - IP Pool	IP addresses are allocated from a specified range when the appliance is powered on. The IP addresses are released when the appliance is powered off. If you select this option, and no IP pool exists, a Network Protocol Profile that contains an IP pool is automatically created and associated with the destination networks.
DHCP	A DHCP server is used to allocate the IP addresses. Select this option only if a DHCP server is available in your environment.
Static - IP Pool	IP addresses are automatically allocated from the managed IP network range of vCenter Server at power-on, and remain allocated at power-off. If you select this option, and no IP pool exists, a Network Protocol Profile that contains an IP pool is automatically created and associated with the destination networks.

3 Specify network protocol information.

This option appears only if the OVF template that you deploy contains network properties. The network protocol settings might be for the DNS servers, gateway, netmask, or subnet. You can type IP addresses that match the chosen IP protocol (IPv4 or IPv6). For DNS servers, you can type a comma-separated list of addresses.

4 Click **Next**.

Customize the OVF Template

Customize the deployment properties of the template.

Procedure

1 Customize the deployment properties.

All required properties must have a valid value before you can continue.

2 Click **Next**.

Configure vService Dependency

Select a binding service for the template's vService dependency.

This page appears if the appliance you are deploying has one or more vService dependency.

Procedure

1 Select a binding service provider.

2 Click **Next**.

Browse VMware Virtual Appliance Marketplace

The Virtual Appliance Marketplace contains a variety of virtual appliances packaged in OVF format that you can download and deploy in your vSphere environment.

Procedure

1 Go to the Virtual Appliance Marketplace, which is part of the VMware Solution Exchange.

2 Search the Marketplace to find a prepackaged application. download it.

3 Log in and download the appliance.

4 Deploy the appliance in your vSphere environment.

Export an OVF Template

An OVF template captures the state of a virtual machine or vApp into a self-contained package. The disk files are stored in a compressed, sparse format.

Required privilege: **vApp.Export**

Prerequisites

Power off the virtual machine or vApp.

Procedure

1 From the **Actions** menu in the vSphere Web Client, navigate to a virtual machine or vApp and select **Export OVF Template** .

2 In the **Name** field, type the name of the template.

For example, type **`MyVm`**.

NOTE When you export an OVF template with a name that contains asterisk (*) characters, those characters turn into underscore (_) characters.

---

3 Click **Choose** to browse to the folder location where you want to save the template.

4 Click **Overwrite existing files** to overwrite files with the same name in that folder.

5 In the **Format** field, determine how you want to store the files.

- Select **Folder of files (OVF)** to store the OVF template as a set of files (`.ovf`, `.vmdk`, and `.mf`). Use this format if you plan to publish the OVF files on a Web server or image library. You can import the package, for example into the vSphere Web Client by specifying the URL to the OVF file.
- Select **Single file (OVA)** to package the OVF template into a single `.ova` file. Use this format if the OVF template will be downloaded from a Web site or moved around using a USB key.

6 (Optional) In the **Annotation** field, type a description.

7 Select the **Enable advanced options** checkbox if you want to include BIOS UUID, MAC address, or extra configuration information in the exported template.

These options limit portability.

8 Click **OK**.

Example: Folder Locations for OVF and OVA Files

If you type **`OvfLib`** for a new OVF folder, the following files might be created:

- `C:\OvfLib\MyVm\MyVm.ovf`
- `C:\OvfLib\MyVm.mf`
- `C:\OvfLib\MyVm-disk1.vmdk`

If you type **`C:\NewFolder\OvfLib`** for a new OVF folder, the following files might be created:

- `C:\NewFolder\OvfLib\MyVm\MyVm.ovf`
- `C:\NewFolder\OvfLib\MyVm.mf`

- `C:\NewFolder\OvfLib\MyVm-disk1.vmdk`

If you choose to export into the OVA format, and type **`MyVm`**, the file `C:\MyVm.ova` is created.

Using Content Libraries 4

Content libraries are container objects for VM templates, vApp templates, and other types of files. vSphere administrators can use the templates in the library to deploy virtual machines and vApps in the vSphere inventory. Sharing templates and files across multiple vCenter Server instances in same or different locations brings out consistency, compliance, efficiency, and automation in deploying workloads at scale.

You create and manage a content library from a single vCenter Server instance, and you can share the library to other vCenter Server instances that belong to the same vCenter Single-Sign On domain. Users from vCenter Server systems that do not belong to the vCenter Single-Sign On domain of the vCenter Server instance that manages the published library, cannot subscribe to it.

Each VM template, vApp template, or another type of file in a library is a library item. An item can contain a single file or multiple files. In the case of VM and vApp templates, each item contains multiple files. For example, because an OVF template is a set of multiple files, when you upload an OVF template to the library, you actually upload all the files associated with the template (`.ovf`, `.vmdk`, and `.mf`), but in the vSphere Web Client you see listing only of the `.ovf` file in the content library.

You can create two types of libraries: local or subscribed library.

Local Libraries

You use a local library to store items in a single vCenter Server instance. You can publish the local library so that users from other vCenter Server systems can subscribe to it. When you publish a content library externally, you can configure a password for authentication.

VM templates and vApps templates are stored as OVF file formats in the content library. You can also upload other file types, such as ISO images, text files, and so on, in a content library.

Subscribed Libraries

You subscribe to a published library by creating a subscribed library. The subscribed library can be created in the same vCenter Server instance where the published library is, or in a different vCenter Server system. When creating a subscribed library you have the option to download all the contents of the published library immediately after the subscribed library is created, or to download only metadata for the items from the published library. If you download only metadata for the items in a subscribed library, you save storage space. A subscribed library, which is set with the option to download all the content of the published library immediately, automatically synchronize with the published library on regular intervals to ensure the contents are up-to-date. You have to manually synchronize a subscribed library, which is set with the option to download contents from the published library only when needed.

If you use a subscribed library, you can only utilize the content, but cannot contribute with content. Only the administrator of the published library manages the templates and files.

Table 4-1. Source Objects to Which You Can Subscribe By Creating a Subscribed Library in The vSphere Web Client .

Source Object	Create a subscribed library in the vSphere Web Client by using the option to Download all library content immediately	Create a subscribed library in the vSphere Web Client by using the option to Download library content only when needed
A library running in a vCenter Server 6.0 instance.	Supported	Supported
A catalog running in a vCloud Director 5.5 instance.	Supported	Not supported
A third-party library.	Supported for third-party libraries that require authentication, if the username of the third-party library is **vcsp**. If the username of the source third-party library is different than **vcsp**, you can subscribe to it by using VMware vCloud Suite API.	Supported for third-party libraries that require authentication, if the username of the third-party library is **vcsp**. If the username of the source third-party library is different than **vcsp**, you can subscribe to it by using VMware vCloud Suite API.

Libraries store content on a file system or a datastore. To ensure optimal performance, use file systems for libraries that are published, and use datastores for local and subscribed libraries.

This chapter includes the following topics:

- "Create a Library," on page 72
- "Synchronize a Subscribed Library," on page 74
- "Edit the Settings of a Local Library," on page 74
- "Edit the Settings of a Subscribed Library," on page 75
- "Delete a Content Library," on page 75
- "Hierarchical Inheritance of Permissions for Content Libraries," on page 76
- "Sample User Role for Working with Content Libraries," on page 78
- "Populating Libraries with Content," on page 78
- "Working with Items in a Library," on page 81
- "Creating Virtual Machines and vApps from Templates in a Content Library," on page 84

Create a Library

You can create a content library in the vSphere Web Client, and populate it with templates, which you can use to deploy virtual machines or vApps in your virtual environment.

Prerequisites

Required privileges: **Content library. Create local library** or **Content library. Create subscribed library** on the vCenter Server instance where you want to create the library.

Procedure

1. In the vSphere Web Client navigator, select **vCenter Inventory Lists > Content Libraries**.
2. Click the **Objects** tab.
3. Click the **Create a New Library** icon ( ).
4. Enter a name for the content library, and in the **Notes** text box, enter a description for the library, and click **Next**.

5 Select the type of content library you want to create.

Option	Description
Local content library	Creates a content library that is accessible only in the vCenter Server instance where you create it. To make the contents of the library available for other users, publish the library. If you want users to use a password when accessing the library, enable authentication for the library, and enter a password.
Subscribed content library	Creates a content library, which is subscribed to a published content library. You can only sync the subscribed library with the published library to see up-to-date content, but you cannot add or remove content from the subscribed library. Only an administrator of the published library can add, modify, and remove contents from the published library. Provide the following settings to subscribe to a library: a In the **Subscription URL** text box, enter the URL address of the published library. b If authentication is enabled on the published library, enter the publisher password. c Select a download method for the contents of the subscribed library. ■ If you want to download a local copy of all the templates and files in the published library immediately after subscribing to it, select **Download all library content immediately**. ■ If you want to save storage space, select **Download library content only when needed**. You download only the metadata for the templates and files in the published library. When you need to use a particular template, synchronize the item to download a full copy. d When prompted, accept the SSL certificate thumbprint. The SSL certificate thumbprint is stored on your system until you delete the subscribed content library from the inventory.

6 Click **Next**.

7 Enter the path to a storage location where to keep the contents of this library.

Option	Description
Enter a local file system path or an NFS URL	Enter the path to the local file system of the Windows machine where vCenter Server runs, or enter a path to an NFS storage if you are using vCenter Server Appliance. If you use a vCenter Server instance that runs on a Windows system, you can store your templates on the local storage or the mapped shared storage on the Windows machine. If you use vCenter Server Appliance, you can store your templates on an NFS storage that is mounted to the appliance. After the operation to create a new library is complete, the vCenter Server Appliance automatically mounts the shared storage to the host OS.
Select a datastore	Select a datastore from your vSphere inventory.

8 Review the information on the Ready to Complete page, and click **Finish**.

Synchronize a Subscribed Library

To ensure that your subscribed library displays the latest content of the published library, you can manually initiate a synchronization task.

You can also have subscribed libraries automatically synchronize with the content of the published library. To enable automatic synchronization of the subscribed library, select the option to **Enable automatic synchronization with the external library** in the subscribed library settings. Take into account that the automatic synchronization requires a lot of storage space, because you download full copies of all the items in the published library.

Prerequisites

Required privilege: **Content library. Sync subscribed library** on the library.

Procedure

1 In the vSphere Web Client navigator, select **vCenter Inventory Lists > Content Libraries**.

2 Right-click a subscribed library from the list and select **Synchronize Library**.

A new task for synchronizing the subscribed library appears in the Recent Tasks pane. After the task is complete, you can see the updated list with library items in the **Related Objects** tab under **Templates** and **Other Types**.

Edit the Settings of a Local Library

You can change the settings of a content library.

As an administrator of a content library, you can publish a local library from your vCenter Server instance to share its contents across multiple vCenter Server systems. From the Edit Setting dialog box, you can obtain the URL of your library and send it to other users to subscribe. If the library is already published, you can change its password for authentication. Users who are subscribed to your library must update the password to keep access to the published library.

Prerequisites

Required privileges: **Content library. Update library** and **Content library. Update local library** on the library.

Procedure

1 In the vSphere Web Client navigator, select **vCenter Inventory Lists > Content Libraries**.

2 Right-click a content library and select **Edit Settings**.

3 Edit the settings for the library.

Type of Content Library	Action
Content library that is local	You can publish a local library to share its contents with other users. a Select the **Publish this library externally** check box. b Select whether to set a password for authentication to the library. If you password protect the library, you must provide both the URL and the password to users who want to subscribe to your library.
Content library that is published	You can change the following settings of a library that is published: ■ You can unpublish the library by deselecting the **Publish this library externally** check box. Users who are currently subscribed to this library can no longer use the library contents. ■ You can enable or disable authentication for the library, and change the password for authentication. ■ You can copy the subscription URL to your library and send it to other users to subscribe.

4 Click **OK**.

Edit the Settings of a Subscribed Library

You can edit the settings of a subscribed library to optimize storage space and network bandwidth by switching between the options to download content from the published library. You might also need to update the password for authentication to the library if the administrator of the published library changes the password.

Prerequisites

Required privileges: **Content library. Update subscribed library** and **Content library. Probe subscription information** on the subscribed library.

Procedure

1 In the vSphere Web Client navigator, select **vCenter Inventory Lists > Content Libraries**.

2 Right-click a subscribed library and select **Edit Settings**.

3 Edit the settings of the subscribed library.

- Enable or disable the automatic synchronization with the published library.
- Update the password for authentication to the published library.
- Select a download method. You can either download all library content immediately or download library content only when needed.

  If you switch from the option to download content only when needed to the option to immediately download all library content, after confirming the dialog a synchronization task starts and content starts to download. The number and size of items in the published library determine the amount of time and network bandwidth that the task requires.

4 Click **OK**.

Delete a Content Library

You can delete a content library that you no longer want to use.

Prerequisites

Required privilege: **Content library. Delete subscribed library** or **Content library. Delete local library** on the type of library you want to delete.

Procedure

1 In the vSphere Web Client navigator, select **vCenter Inventory Lists > Content Libraries**.

2 Right-click a content library from the list and select **Delete**.

3 In the Delete library confirmation dialog box, click **Yes**.

The content library and all its contents are deleted.

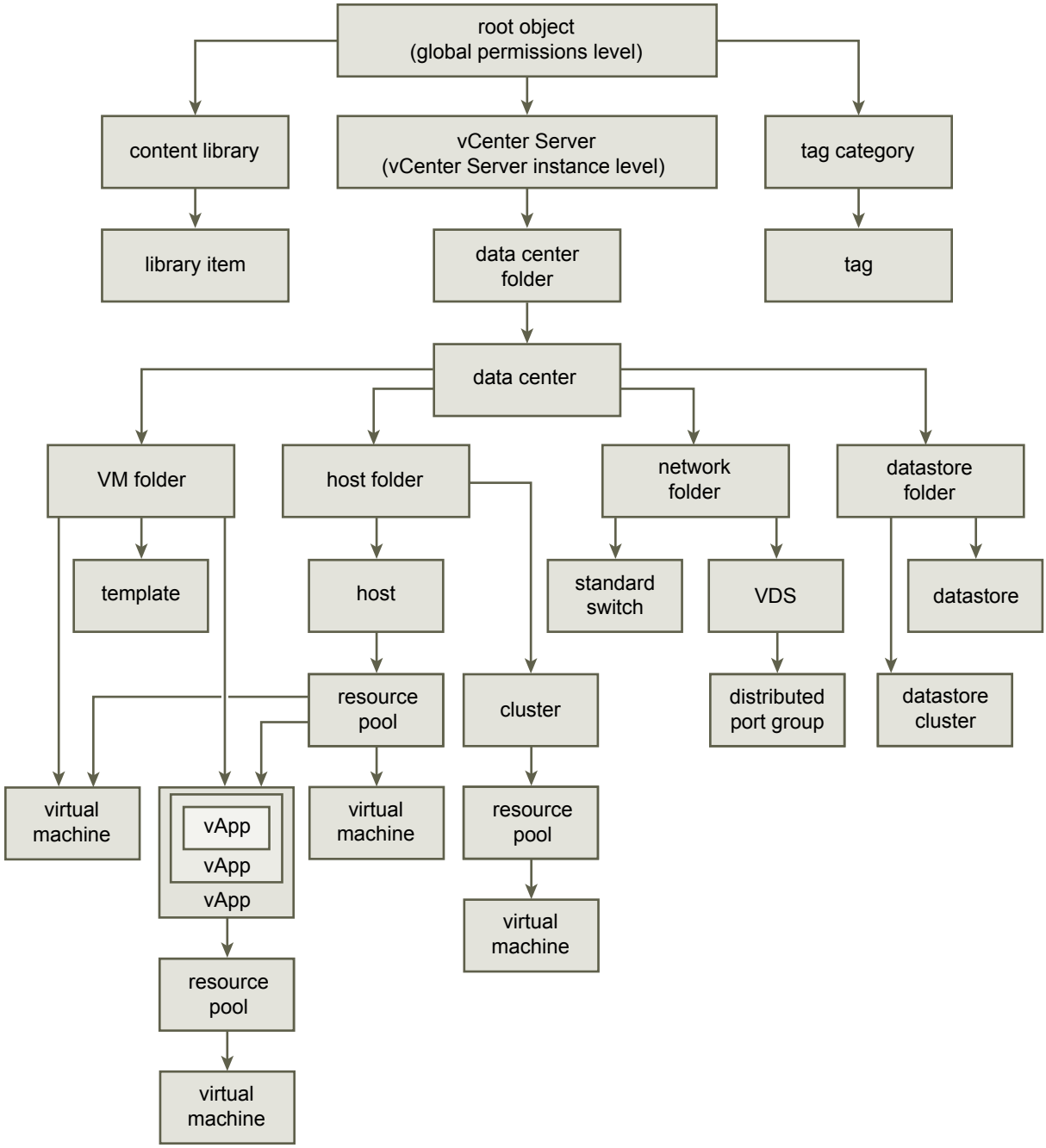
Hierarchical Inheritance of Permissions for Content Libraries

vSphere objects inherit permissions from a parent object in the hierarchy. Content libraries work in the context of a single vCenter Server instance. However, content libraries are not direct children of a vCenter Server system from an inventory perspective.

The direct parent for content libraries is the global root. This means that if you set a permission at a vCenter Server level and propagate it to the children objects, the permission applies to data centers, folders, clusters, hosts, virtual machines, and so on, but does not apply to the content libraries that you see and operate with in this vCenter Server instance. To assign a permission on a content library, an Administrator must grant the permission to the user as a global permission. Global permissions support assigning privileges across solutions from a global root object.

The figure illustrates the inventory hierarchy and the paths by which permissions can propagate.

Figure 4-1. vSphere Inventory Hierarchy



To let a user manage a content library and its items, an Administrator can assign the Content Library Administrator role to that user as a global permission. The Content Library Administrator role is a sample role in the vSphere Web Client.

Users who are Administrators can also manage libraries and their contents. If a user is an Administrator at a vCenter Server level, they have sufficient privileges to manage the libraries that belong to this vCenter Server instance, but cannot see the libraries unless they have a Read-Only role as a global permission.

For example, a user has an Administrator role that is defined at a vCenter Server level. When the Administrator navigates to Content Libraries in the object navigator, he sees 0 libraries despite there are existing libraries in the vSphere inventory of that vCenter Server instance. To see the libraries, the Administrator needs a Read-Only role assigned as a global permission.

Administrators whose role is defined as a global permissions can see and manage the libraries in all vCenter Server instances that belong to the global root.

Because content libraries and their children items inherit permissions only from the global root object, when you navigate to a library or a library item and click **Manage** tab, you can see there is no **Permissions** tab. An Administrator cannot assign individual permissions on different libraries or different items within a library.

Sample User Role for Working with Content Libraries

vSphere Web Client provides a sample role that lets you be an administrator of content libraries. You can modify the role or use it as an example to create custom roles for specific tasks you want to allow other users to perform.

Content Library Administrator

Content Library Administrator role is a predefined role that gives a user privileges to monitor and manage a library and its contents.

A user who has this role can perform the following tasks:

- Create, edit, and delete local or subscribed libraries.
- Synchronize a subscribed library and synchronize items in a subscribed library.
- View the item types supported by the library.
- Configure the global settings for the library.
- Import items to a library.
- Export library items.

Populating Libraries with Content

You can populate a content library with OVF templates that you can use to provision new virtual machines. You can also add other files to a content library such as ISO images, scripts, and text files.

There are multiple ways to populate a library with items.

- Importing Items to a Content Library on page 79

  You can import items such as VM templates and vApps to a content library from your local machine or from a Web server, and use them to create virtual machines and vApps. You can also import ISO images, certificates, and other files, which you want to keep in the library and share with other users across multiple vCenter Server systems.

- Clone a vApp to a Template in Content Library on page 80

  You can clone existing vApps to vApp templates in a content library. You can use the vApp templates later to provision new vApps on a cluster or a host in your vSphere inventory. The vApp is exported to a content library in the OVF format.

- Clone a Virtual Machine or a VM Template to a Template in Content Library on page 80

  You can clone existing virtual machines or VM templates to templates in the content library, and use them later to provision virtual machines on a cluster or a host.

- Clone Library Items from One Library to Another Library on page 81

  You can clone a template from one content library to another in the same vCenter Server instance. The cloned template is an exact copy of the original template.

Importing Items to a Content Library

You can import items such as VM templates and vApps to a content library from your local machine or from a Web server, and use them to create virtual machines and vApps. You can also import ISO images, certificates, and other files, which you want to keep in the library and share with other users across multiple vCenter Server systems.

Import Items to a Library from a URL

You can add an item that resides on a Web server to a content library.

Prerequisites

Required privilege: **Content library. Add library item** and **Content library. Update files** on the library.

Procedure

1 In the vSphere Web Client navigator, select **vCenter Inventory Lists > Content Libraries**.

2 Right-click a content library and select **Import Item**.

The Import Library Item dialog box opens.

3 Under Source section, select the option to import an item from a URL, and enter the path to a Web-server where the item is.

4 Under Destination section, enter a name and a description for the item, and click **OK**.

In the Recent Tasks pane you see two tasks, one about creating a new item in the library, and the second about uploading the contents of the item to the library. After the task is complete, the item appears on the **Related Objects** tab under **Templates** or **Other Types**.

Import Items to a Library from a Local File on Your System

You can add items to a content library by importing files from your local system. You can import an OVF package to use as a template for deploying virtual machines and vApps. You can also import other types of files, such as scripts, ISO files, and so on, that you want to use in your vCenter Server instance, or you want to share across multiple vCenter Server systems.

Prerequisites

- Verify you have the vCenter Client Integration Plug-in installed on the system. See "Install the Client Integration Plug-In," on page 189.
- Required privilege: **Content library. Add library item** and **Content library. Update files** on the library.

Procedure

1 In the vSphere Web Client navigator, select **vCenter Inventory Lists > Content Libraries**.

2 Right-click a content library and select **Import Item**.

The Import Library Item dialog box opens.

3 Under Source section, select the option to import an item from a local file, and click **Browse** to navigate to the file that you want to import from your local system.

You can use the**Files of Type** drop-down menu to filter files in your local system.

4 Under Destination section, enter a name and description for the item, and click **OK**.

In the Recent Tasks pane you see two tasks, one about creating a new item in the library, and the second about uploading the contents of the item to the library. After the task is complete, the item appears on the **Related Objects** tab under **Templates** or **Other Types**.

Clone a vApp to a Template in Content Library

You can clone existing vApps to vApp templates in a content library. You can use the vApp templates later to provision new vApps on a cluster or a host in your vSphere inventory. The vApp is exported to a content library in the OVF format.

Procedure

1 In the vSphere Web Client navigator, click **vCenter Inventory Lists > vApps**.

2 Right-click a vApp and select **Clone > Clone to Template in Library**

3 Type a name and description for the template.

4 From the list of available libraries, select the content library to which you want to add the template.

5 (Optional) Include or exclude vApp related configurations in the template you are cloning.

   You can select to preserve the MAC-addresses on the network adapters and include extra configuration.

6 Click **OK**.

A new task for exporting an OVF package appears in the Recent Tasks pane. After the task is complete, the vApp template appears on the **Templates** tab under **Related Objects** tab for the content library.

What to do next

Use the template to provision vApps on a host or a cluster in your vSphere inventory. See "Create New vApp on a Host or a Cluster from a Template in a Content Library," on page 84

Clone a Virtual Machine or a VM Template to a Template in Content Library

You can clone existing virtual machines or VM templates to templates in the content library, and use them later to provision virtual machines on a cluster or a host.

Templates are master copies of virtual machines that let you create ready-for-use virtual machines. You can make changes to the template, such as installing additional software in the guest operating system, while preserving the state of the original template. For more information, see "VM Templates and vApp Templates in Content Libraries," on page 82

Procedure

1 In the vSphere Web Client, navigate to the object you want to clone, and start the cloning task.

Option	Action
Clone a virtual machine to a template in a library	a Select **vCenter Inventory Lists > Virtual Machines**. b Right-click a virtual machine and select **Clone > Clone to Template in Library**.
Clone a VM Template to a template in a library	a Select **vCenter Inventory Lists > VM Templates in Folders**. b Right-click a VM Template and select **Clone to Library**.

   The Clone to Template in Library dialog box opens.

2 Enter a name and description for the template.

3 From the list with content libraries, select the library in which you want to add the template.

4 (Optional) Select configuration data that you want to include in the template.

   You can select to preserve the MAC-addresses on the network adapters and include extra configuration.

5 Click **OK**.

A new task for exporting an OVF package appears in the Recent Tasks pane. After the task is complete, the template appears in the **Templates** tab of the **Related Objects** tab for the content library.

What to do next

Use the template to create virtual machines on hosts or clusters in the vSphere inventory.

Clone Library Items from One Library to Another Library

You can clone a template from one content library to another in the same vCenter Server instance. The cloned template is an exact copy of the original template.

When cloning a template between libraries, in the clone wizard you can select the source library to also be a destination library.

A subscribed library can be the source of an item you want to clone, but you cannot clone items to a subscribed library. The subscribed libraries are filtered out from the list with destination libraries in the Clone Library Item dialog box. When the source library of an item you want to clone is a subscribed library with the setting to download items only when needed, the item is first downloaded to the source subscribed library and then cloned to the destination library.

Procedure

1 In the vSphere Web Client navigator, select **vCenter Inventory Lists > Content Libraries**.

2 Select a content library and click the **Related Objects** tab.

3 Right-click a library item and select **Clone Item**.

4 (Optional) Change the name and notes for the item you clone.

5 From the list of content libraries, select the library in which you want to clone the template.

   You can select the destination library to be the same as the source library if you want to have identical copy of the template in the same library.

6 Click **OK**.

A new task for cloning the template appears in the Recent Tasks pane. After the task is complete, a clone of the template appears on the **Templates** tab under the **Related objects** tab of the destination content library.

What to do next

Deploy a virtual machine from template on a host or a cluster in your vSphere inventory.

Working with Items in a Library

You can perform various tasks with the items in a content library. You can synchronize an item from a subscribed library to download all its contents and use the item to deploy a virtual machine for example. You can delete items you no longer need to use, and so on.

Each VM template, vApp template, or another type of file in a library is a library item. An item can contain a single file or multiple files. In the case of VM and vApp templates, each item contains multiple files. For example, because an OVF template is a set of multiple files, when you upload an OVF template to the library, you actually upload all the files associated with the template (`.ovf`, `.vmdk`, and `.mf`), but in the vSphere Web Client you see listing only of the `.ovf` file in the content library.

VM Templates and vApp Templates in Content Libraries

In a content library you can store VM and vApp templates. You can use the VM and vApp templates to deploy virtual machines and vApps in the vSphere inventory.

A VM template is a template of a virtual machine. The VM templates that exist in a VM template folder differentiate from the VM templates that exist in a content library. A VM template that resides in a content library is in OVF format and if you export it to your local system it is saved as an `.ovf` file. The VM templates that exist in a VM template folder are not in OVF format but if you clone them to content library, the resulting template is in an OVF format.

A vApp template is a template of a vApp, which can contain multiple virtual machines or multiple vApps. A vApp template that resides in a content library is in OVF format, and if you export the template to your local system it is saved as an `.ovf` file. vApp templates are inventory objects that exist only in content libraries.

You can use VM templates and vApp templates to deploy virtual machines and vApps to a destination object such as a host or a cluster.

Synchronize a Library Item in a Subscribed Library

To update or download the content of a library item you can synchronize it.

When creating the subscribed library, if you selected the option to download library content only when needed, only metadata for the library contents is downloaded to the associated storage. When you need to use the item, you synchronize it to download its content to your local storage. When you no longer need the item, to free space on your storage you can delete the content of the item. You continue to see the item in your subscribed library, but it no longer takes up space on your storage because only the items metadata remains on the storage.

Prerequisites

- Required privilege: **Content library. Sync library item** on the library item.

Procedure

1. In the vSphere Web Client navigator, select **vCenter Inventory Lists > Content Libraries**.
2. Select a subscribed library from the list, and click the **Related Objects** tab.
3. Synchronize the item you need to use.
   - On the **Templates** tab, right-click a VM or a vApp template, and select **Synchronize Item**.
   - On the **Other Types** tab, right-click an item, and select **Synchronize Item**.

After synchronization completes, the item content and metadata are downloaded to the backing storage of the subscribed library, and in the **Related Objects** tab the value for the item in the Stored Content Locally column changes to Yes.

Export Item from a Content Library to Your Local Computer

You might need to export an item from a content library to your local system.

Prerequisites

- Required privilege: **Content library. Download files** on the library.
- Verify you have the Client Integration Plug-in installed on the system.

Procedure

1 In the vSphere Web Client navigator, select **vCenter Inventory Lists > Content Libraries**.

2 Select a content library and click the **Related Objects** tab.

3 Select the type of file you want to export.

- From the **Templates** tab, right-click a template from the library, and select **Export Item**.
- From the **Other Types** tab, right-click a file from the library that is not a template, and select **Export Item**.

The Export Library Item dialog box opens.

4 Browse to a destination folder where you want to save the item, and click **OK**.

A folder with the same name as the item is created in the destination folder on your local computer to store the item contents.

Delete the Contents of a Library Item

If a subscribed library is created with the option to download library content only when needed, only metadata for the library items is stored in the associated with the library storage. For example, when you want to use a VM template to deploy a virtual machine, you have to synchronize the item so the entire content is downloaded to the associated storage. After you are done using the template, you can delete the item contents to free space on the storage. The template remains visible in the subscribed library because the metadata for it remains on the storage that is associated with the library. This also applies for vApp templates, and other file that exist in the subscribed library.

Prerequisites

Required privilege: **Content library. Evict library item**

Procedure

1 In the vSphere Web Client navigator, select **vCenter Inventory Lists > Content Libraries**.

2 Select a subscribed library from the list, and click the **Related Objects** tab.

3 On the **Related Objects** tab, right-click an item from the list, and select **Delete Item Content**.

The content of the item is deleted to free space on the storage. Only the item metadata remains on the storage.

Delete Library Item

You can delete an item you no longer need to use.

Prerequisites

Required privilege: **Content library. Delete library item** on the library item.

Procedure

1 In the vSphere Web Client navigator, select **vCenter Inventory Lists > Content Libraries**.

2 Select a subscribed library from the list, and click the **Related Objects** tab.

3 Right-click an item from the **Templates** or **Other Types** lists in the **Related Objects** tab, and select **Delete**.

4 In the dialog box, confirm that you want to delete the item.

The content and the metadata of the library item are deleted.

Creating Virtual Machines and vApps from Templates in a Content Library

From VM or from vApp templates stored in a content library, you can deploy virtual machines and vApps on hosts or clusters in your vSphere inventory.

The library can be a local library to the vCenter Server instance where you want to deploy the VM or the vApp template, or can be a subscribed library to that vCenter Server instance.

The use of templates brings about consistency, compliance, and efficiency when deploying virtual machines and vApps in your vCenter Server instance.

Deploy Virtual Machine on a Host or a Cluster from a VM Template in the Content Library

You can use a VM template from a content library to deploy a virtual machine to a host or a cluster in your vSphere inventory.

Procedure

1 In the vSphere Web Client navigator, select **vCenter Inventory Lists > Content Libraries**.

2 Select a content library, click the **Related Objects** tab, and click **Templates**.

3 Right-click a VM Template and select **New VM from This Template**.

The New Virtual Machine from Content Library into Host or Cluster wizard opens.

4 Enter a name, select a location for the virtual machine, and click **Next**.

5 On the Select a resource page, select a host, a cluster, a resource pool, or a vApp where to deploy the VM template.

6 On the Review details page, verify the template details and click **Next**.

7 On the Select Storage page, select the location to store the files of the VM template, and click **Next**.

8 Select a network for each network adapter in the template, and click **Next**.

9 Review the page and click **Finish**.

A new task for creating the virtual machine appears in the Recent Tasks pane. After the task is complete, the new virtual machine is created on the selected resource.

What to do next

Customize the guest operating system of the virtual machine. For more information, see "Apply a Customization Specification to a Virtual Machine," on page 54.

Create New vApp on a Host or a Cluster from a Template in a Content Library

You can use a vApp template from a content library to create new vApp on a host or a cluster in your vSphere inventory.

Procedure

1 In the vSphere Web Client navigator, select **vCenter Inventory Lists > Content Libraries**.

2 Select a content library, click the **Related Objects** tab, and click **Templates**.

3 Right-click a vApp template and select **New vApp from This Template**.

The New vApp from Content Library into Host or Cluster wizard opens.

4 Enter a name and select a location for the vApp, and click **Next**.

5 On the Select a resource page, select a host, a cluster, a resource pool, or a vApp to deploy the vApp to.

6 On the Review details page, verify the template details and click **Next**.

7 Select disk format and a storage resource for the vApp.

8 On the Customize template page, you can customize the deployment properties for the vApp.

9 On the Ready to Complete page, review the configurations you made for the vApp, and click **Finish**.

A new task for creating the vApp appears in the Recent Tasks pane. After the task is complete, the new vApp is created.

Installing the Microsoft Sysprep Tool 5

Install the Microsoft Sysprep tool so that you can customize Windows guest operating systems when you clone virtual machines.

The guest operating system customization feature in vCenter Server uses the functions of the Sysprep tool. Verify that your vCenter Server meets the following requirements before you customize your virtual machine's Windows guest operating systems:

- Install the Microsoft Sysprep tool. Microsoft includes the system tool set on the installation CD-ROM discs for Windows 2000, Windows XP, and Windows 2003. The Sysprep tool is built into the Windows Vista and Windows 2008 operating systems.
- The correct versions of the Sysprep tool is installed for each guest operating system that you want to customize.
- The password for the local administrator account on the virtual machines is set to blank ("").

NOTE Customization operations will fail if the correct version of the Sysprep tool is not found.

This chapter includes the following topics:

- "Install the Microsoft Sysprep Tool from a Microsoft Web Site," on page 87
- "Install the Microsoft Sysprep Tool from the Windows Operating System CD," on page 88

Install the Microsoft Sysprep Tool from a Microsoft Web Site

You can download and install the Microsoft Sysprep tool from the Microsoft Web site.

Prerequisites

Verify that you download the correct version for the guest operating system to customize. Microsoft has a different version of Sysprep for each release and service pack of Windows. You must use the version of Sysprep specific to the operating system that you are deploying.

The vCenter Server installer creates a Sysprep directory in *`ALLUSERSPROFILE`*. The *`ALLUSERSPROFILE`* location is usually `\Documents And Settings\All Users\`. The `vpxd.cfg` file is also in this location. On Windows 2008, the file location is `C:\ProgramData\VMware\VMware VirtualCenter\sysprep\`.

Procedure

1 Download the Sysprep files from the Microsoft Download Center and save them to your local system.

2 Open and expand the `.cab` file.

The contents of the `.cab` file vary, depending on the operating system.

3 Extract the files to the appropriate directory for your guest operating system.

   The following Sysprep support directories are created during the vCenter Server installation:

```
C:\ALLUSERSPROFILE\Application Data\Vmware\VMware VirtualCenter\sysprep
...\1.1\
...\2k\
...\xp\
...\svr2003\
...\xp-64\
...\svr2003-64\
```

4 Select the subdirectory that corresponds to your operating system.

5 Click **OK** to expand the files.

What to do next

Customize a new virtual machine with a supported Windows guest operating system when you clone an existing virtual machine.

Install the Microsoft Sysprep Tool from the Windows Operating System CD

You can install the Microsoft Sysprep tool from a CD.

The vCenter Server installer creates a Sysprep directory in *ALLUSERSPROFILE*. The *ALLUSERSPROFILE* location is usually `\Documents and Settings\All Users\`. The `vpxd.cfg` file is also in this location. On Windows 2008, the file location is `C:\ProgramData\VMware\VMware VirtualCenter\sysprep\`.

Procedure

1 Insert the Windows operating system CD into the CD-ROM drive, often the `D:` drive.

2 Locate the `DEPLOY.CAB` file in the `\Support\Tools` directory on the CD.

3 Open and expand the `DEPLOY.CAB` file.

   The contents of the `.cab` file vary, depending on the operating system.

4 Extract the files to the directory appropriate for your guest operating system.

   The following Sysprep support directories are created during the vCenter Server installation:

```
C:\ALLUSERSPROFILE\Application Data\Vmware\VMware VirtualCenter\sysprep
...\1.1\
...\2k\
...\xp\
...\svr2003\
...\xp-64\
...\svr2003-64\
```

5 Select the subdirectory that corresponds to your operating system.

6 Click **OK** to expand the files.

7 Repeat this procedure to extract Sysprep files for each of the Windows guest operating systems that you plan to customize using vCenter Server.

What to do next

Customize a new virtual machine with a supported Windows guest operating system when you clone an existing virtual machine.

Configuring Virtual Machine Hardware

6

You can add or configure most virtual machine properties during the virtual machine creation process or after you create the virtual machine and install the guest operating system.

You configure the virtual machine hardware and can change nearly every characteristic that you selected when you created the virtual machine. You can view the existing hardware configuration and add or remove hardware. You can configure CPUs, CPU hyperthreading resources, memory, and disks.

Not all hardware devices are available to every virtual machine. The host that the virtual machine runs on and the guest operating system must support devices that you add or configurations that you make.

This chapter includes the following topics:

- "Virtual Machine Compatibility," on page 89
- "Virtual CPU Configuration," on page 95
- "Virtual Memory Configuration," on page 102
- "Network Virtual Machine Configuration," on page 104
- "Parallel and Serial Port Configuration," on page 108
- "Virtual Disk Configuration," on page 115
- "SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility," on page 126
- "Other Virtual Machine Device Configuration," on page 131
- "Reduce Memory Overhead for Virtual machines with 3D graphics Option," on page 140
- "USB Configuration from an ESXi Host to a Virtual Machine," on page 140
- "USB Configuration from a Client Computer to a Virtual Machine," on page 147
- "Add a Shared Smart Card Reader to Virtual Machines," on page 152

Virtual Machine Compatibility

When you create a virtual machine or upgrade an existing virtual machine, you use the virtual machine compatibility setting to select the ESXi host versions that the virtual machine can run on.

The compatibility setting determines the virtual hardware available to the virtual machine, which corresponds to the physical hardware available on the host. Virtual hardware includes BIOS and EFI, available virtual PCI slots, maximum number of CPUs, maximum memory configuration, and other characteristics. New virtual hardware capabilities are typically released once a year with major or minor releases of vSphere.

Each virtual machine compatibility level supports at least five major or minor vSphere releases. For example, a virtual machine with ESXi 3.5 and later compatibility can run on ESXi 3.5, ESXi 4.0, ESXi 4.1, ESXi 5.0, ESXi 5.1, ESXi 5.5, and ESXi 6.0.

Table 6-1. Virtual Machine Compatibility Options

Compatibility	Description
ESXi 6.0 and later	This virtual machine (hardware version 11) is compatible with ESXi 6.0.
ESXi 5.5 and later	This virtual machine (hardware version 10) is compatible with ESXi 5.5 and 6.0.
ESXi 5.1 and later	This virtual machine (hardware version 9) is compatible with ESXi 5.1, ESXi 5.5, and ESXi 6.0.
ESXi 5.0 and later	This virtual machine (hardware version 8) is compatible with ESXi 5.0, ESXi 5.1, ESXi 5.5, and ESXi 6.0.
ESX/ESXi 4.0 and later	This virtual machine (hardware version 7) is compatible with ESX/ ESXi 4.0, ESX/ ESXi 4.1, ESXi 5.0, ESXi 5.1, ESXi 5.5, and ESXi 6.0.
ESX/ESXi 3.5 and later	This virtual machine (hardware version 4) is compatible with ESX/ESXi 3.5, ESX/ ESXi 4.0, ESX/ ESXi 4.1, ESXi 5.1, ESXi 5.5, and ESXi 6.0. It is also compatible with VMware Server 1.0 and later. ESXi 5.0 does not allow creation of virtual machines with ESX/ESXi 3.5 and later compatibility, but you can run such virtual machines if they were created on a host with different compatibility.
ESX Server 2.x and later	This virtual machine (hardware version 3) is compatible with ESX Server 2.x, ESX/ESXi 3.5, ESX/ESXi 4.x, and ESXi 5.0. You cannot create, edit, turn on, clone, or migrate virtual machines with ESX Server 2.x compatibility. You can only register or upgrade them.

The compatibility setting that appears in the **Compatible with** drop-down menu is the default for the virtual machine that you are creating. The following factors determine the default virtual machine compatibility:

- The ESXi host version on which the virtual machine is created.
- The inventory object that the default virtual machine compatibility is set on, including a host, cluster, or datacenter.

You can accept the default compatibility or select a different setting. It is not always necessary to select the latest ESXi host version. Selecting an earlier version can provide greater flexibility and is useful in the following situations:

- To standardize testing and deployment in your virtual environment.
- If you do not need the capabilities of the latest host version.
- To maintain compatibility with older hosts.

When you create a virtual machine, consider the environment that the virtual machine will run in and weigh the benefits of different compatibility strategies. Consider your options for these scenarios, which demonstrate the flexibility inherent with each virtual machine compatibility selection.

Objects in Environment	Compatibility	Results
Cluster with ESXi 5.1, ESXi 5.5, and ESXi 6.0 hosts	ESXi 5.1 and later	Preserves the ability of the virtual machine to run on other hosts in the cluster, such as ESXi 5.0. You might not have access to the latest virtual hardware features.
Cluster with ESXi 5.1, ESXi 5.5, and ESXi 6.0 hosts	ESXi 5.5 and later	Gives you access to virtual hardware features that are not available with ESXi 5.1. ■ You cannot migrate this virtual machine to an ESXi 5.1 host. ■ This virtual machine does not have all the capabilities available to virtual machines that run on ESXi 6.0, for example, you cannot configure a virtual machine to use 128 virtual CPUs.
Cluster with ESXi 5.1, ESXi 5.5, and ESXi 6.0 hosts	ESXi 6.0 and later	Provides access to the latest virtual hardware features, but but cannot run on ESXi 5.1 or ESXi 5.5.

Set the Default Compatibility for Virtual Machine Creation

You can set the default compatibility for virtual machine creation on the host, cluster, or data center. These options ensure that when virtual machines are added to an existing vSphere environment, they will be compatible with the host versions that reside there.

The following conditions apply:

- To set the default compatibility on the cluster, the cluster must contain hosts that are connected and not in maintenance mode.
- A default compatibility setting on the host overrides a default cluster or datacenter setting.
- A default compatibility setting on the cluster overrides a default datacenter setting.

Prerequisites

Required privileges:

- On the host or cluster: **Host.Inventory.Modify cluster**
- On the datacenter: **Datacenter.Reconfigure datacenter**

Procedure

◆ Select a host, cluster, or data center in the inventory.

Option	Action
Host	a Click the **Manage** tab, and click **Settings**. b In the Virtual Machines section, select **Default VM Compatibility** and click **Edit**. c Select the compatibility from the drop-down menu and click **OK**. NOTE You can set the compatibility only on hosts that are not part of a cluster.
Cluster	a Click the **Manage** tab and click **Settings**. b In the Configuration section, select **General** and click the **Edit** button next to **Default VM Compatibility**. c Select the compatibility from the drop-down menu and click **OK**. When you change the compatibility for a cluster, the compatibility for all hosts in the cluster changes as well.
Datacenter	a Right-click the datacenter and select **Edit Default VM Compatibility**. b Select the compatibility from the drop-down menu and click **OK**.

When you create a virtual machine on one of these objects, the default compatibility setting is used.

Schedule a Compatibility Upgrade for a Single Virtual Machine

The compatibility level determines the virtual hardware available to a virtual machine, which corresponds to the physical hardware available on the host machine. You can upgrade the compatibility to make the virtual machine compatible with the latest version of the host.

To schedule an upgrade for multiple virtual machines, see "Schedule a Compatibility Upgrade for Virtual Machines," on page 249.

Prerequisites

- Create a backup or snapshot of the virtual machines.
- Upgrade to the latest version of VMware Tools. On Microsoft Windows virtual machines, if you upgrade the compatibility level before you upgrade VMware Tools, the virtual machine might lose its network settings.
- Verify that all `.vmdk` files are available to the ESX/ESXi host on a VMFS-3, VMFS-5, or NFS datastore.
- Verify that the virtual machine is stored on VMFS-3, VMFS-5 or NFS datastores.

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **Upgrade** and select **Schedule VM Compatibility Upgrade.**
3. Select the compatibility from the drop-down menu.

   The virtual machine compatibility is upgraded the next time you restart the virtual machine.
4. (Optional) To upgrade the compatibility when you do regularly scheduled guest maintenance, select **Only upgrade after normal guest OS shutdown**.

The virtual machine compatibility is upgraded and the new version appears on the virtual machine Summary tab.

Determine the Default Virtual Machine Compatibility Setting in the vSphere Web Client

The compatibility setting for a virtual machine provides information about the hosts, clusters, or data center that the virtual machine is compatible with.

The virtual machine **Summary** tab displays the compatibility for the virtual machine. You can set and view the default compatibility that is used for virtual machine creation at the host, cluster, or datacenter level.

Procedure

◆ Select an inventory object and display the virtual machine compatibility.

Option	Action
Virtual machine	Select a virtual machine and click **All vCenter Actions > Compatibility**. You can select **Upgrade VM Compatibility** or **Schedule VM Compatibility Upgrade**.
Host, Cluster, Datacenter	Right-click the object and select **All vCenter Actions > Edit Default VM Compatibility**. If a host is in a cluster, it has the virtual machine compatibility set on the cluster, and the menu item is grayed out.

Hardware Features Available with Virtual Machine Compatibility Settings

The virtual machine compatibility setting determines the virtual hardware available to the virtual machine, which corresponds to the physical hardware available on the host. You can review and compare the hardware available for different compatibility levels to help you determine whether to upgrade the virtual machines in your environment.

Table 6-2. Supported Features for Virtual Machine Compatibility

Feature	ESXi 6.0 and later	ESXi 5.5 and later	ESXi 5.1 and later	ESXi 5.0 and later	ESX/ESXi 4.x and later	ESX/ESXi 3.5 and later
Hardware version	11	10	9	8	7	4
Maximum memory (GB)	4080	1011	1011	1011	255	64
Maximum number of logical processors	128	64	64	32	8	4
Maximum number of cores (virtual CPUs) per socket	128	64	64	32	8	1
Maximum SCSI adapters	4	4	4	4	4	4
Bus Logic adapters	Y	Y	Y	Y	Y	Y
LSI Logic adapters	Y	Y	Y	Y	Y	Y
LSI Logic SAS adapters	Y	Y	Y	Y	Y	N
VMware Paravirtual controllers	Y	Y	Y	Y	Y	N
SATA controllers	4	4	N	N	N	N
Virtual SCSI disk	Y	Y	Y	Y	Y	Y
SCSI passthrough	Y	Y	Y	Y	Y	Y
SCSI hot plug support	Y	Y	Y	Y	Y	Y
IDE nodes	Y	Y	Y	Y	Y	Y
Virtual IDE disk	Y	Y	Y	Y	Y	N
Virtual IDE CD-ROMs	Y	Y	Y	Y	Y	Y
IDE hot plug support	N	N	N	N	N	N

Table 6-2. Supported Features for Virtual Machine Compatibility (Continued)

Feature	ESXi 6.0 and later	ESXi 5.5 and later	ESXi 5.1 and later	ESXi 5.0 and later	ESX/ESXi 4.x and later	ESX/ESXi 3.5 and later
Maximum NICs	10	10	10	10	10	4
PCNet32	Y	Y	Y	Y	Y	Y
VMXNet	Y	Y	Y	Y	Y	Y
VMXNet2	Y	Y	Y	Y	Y	Y
VMXNet3	Y	Y	Y	Y	Y	N
E1000	Y	Y	Y	Y	Y	Y
E1000e	Y	Y	Y	Y	N	N
USB 1.x and 2.0	Y	Y	Y	Y	Y	N
USB 3.0	Y	Y	Y	Y	N	N
Maximum video memory (MB)	2 GB	512	512	128	128	128
SVGA displays	10	10	10	10	10	1
SVGA 3D hardware acceleration	Y	Y	Y	Y	N	N
VMCI	Y	Y	Y	Y	Y	N
PCI passthrough	16	6	6	6	6	0
PCI Hot plug support	Y	Y	Y	Y	Y	N
Nested HV support	Y	Y	Y	N	N	N
vPMC support	Y	Y	Y	N	N	N
Serial ports	32	4	4	4	4	4
Parallel ports	3	3	3	3	3	3
Floppy devices	2	2	2	2	2	2

Virtual CPU Configuration

You can add, change, or configure CPU resources to improve virtual machine performance. You can set most of the CPU parameters when you create virtual machines or after the guest operating system is installed. Some actions require that you power off the virtual machine before you change the settings.

VMware uses the following terminology. Understanding these terms can help you plan your CPU resource allocation strategy.

CPU	The CPU or processor is the portion of a computer system that carries out the instructions of a computer program and is the primary element carrying out the computer's functions. CPUs contain cores.
CPU Socket	A physical connector on a computer motherboard that accepts a single physical CPU. Many motherboards can have multiple sockets that can in turn accept multicore processors (CPUs). The vSphere Web Client computes the total number of virtual sockets from the number of cores and the cores per socket that you select.
Core	Comprises a unit containing an L1 cache and functional units needed to run programs. Cores can independently run programs or threads. One or more cores can exist on a single CPU.
Corelet	An AMD processor corelet is architecturally equivalent to a logical processor. Certain future AMD processors will comprise a number of compute units, where each compute unit has a number of corelets. Unlike a traditional processor core, a corelet lacks a complete set of private, dedicated execution resources and shares some execution resources with other corelets such as an L1 instruction cache or a floating-point execution unit. AMD refers to corelets as cores, but because these are unlike traditional cores, VMware uses the nomenclature of corelets to make resource sharing more apparent.
Thread	Some cores can run independent streams of instructions simultaneously. In existing implementations, cores can run one or two software threads at one time by multiplexing the functional units of the core between the software threads, as necessary. Such cores are called dual or multithreaded.
Resource sharing	Shares specify the relative priority or importance of a virtual machine or resource pool. If a virtual machine has twice as many shares of a resource as another virtual machine, it is entitled to consume twice as much of that resource when these two virtual machines are competing for resources.
Resource allocation	You can change CPU resource allocation settings, such as shares, reservation, and limit, when available resource capacity does not meet demands. For example, if at year end, the workload on accounting increases, you can increase the accounting resource pool reserve.
vSphere Virtual Symmetric Multiprocessing (Virtual SMP)	Feature that enables a single virtual machine to have multiple processors.

Virtual CPU Limitations

The maximum number of virtual CPUs that you can assign to a virtual machine depends on the number of logical CPUs on the host, the host license, and the type of guest operating system that is installed on the virtual machine.

Be aware of the following limitations:

- A virtual machine cannot have more virtual CPUs than the number of logical cores on the host. The number of logical cores is equal to the number of physical cores if hyperthreading is disabled or two times that number if hyperthreading is enabled.
- Not every guest operating system supports Virtual SMP, and guest operating systems that support this functionality might support fewer processors than are available on the host. For information about Virtual SMP support, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.
- Hyperthreaded hosts might affect virtual machine performance, depending on the workload. The best practice is to test your workload to determine whether to enable or disable hyperthreading on your hosts.

Configuring Multicore Virtual CPUs

VMware multicore virtual CPU support lets you control the number of cores per virtual socket in a virtual machine. This capability lets operating systems with socket restrictions use more of the host CPU's cores, which increases overall performance.

Important When you configure your virtual machine for multicore virtual CPU settings, you must ensure that your configuration complies with the requirements of the guest operating system EULA.

Using multicore virtual CPUs can be useful when you run operating systems or applications that can take advantage of only a limited number of CPU sockets.

You can configure a virtual machine that runs on an ESXi host 6.0 and later to have up to 128 virtual CPUs. A virtual machine cannot have more virtual CPUs than the actual number of logical CPUs on the host. The number of logical CPUs means the number of physical processor cores or two times that number if hyperthreading is enabled. For example, if a host has 128 logical CPUs, you can configure the virtual machine for 128 virtual CPUs.

You configure how the virtual CPUs are assigned in terms of cores and cores per socket. Determine how many CPU cores you want in the virtual machine, then select the number of cores you want in each socket, depending on whether you want a single core CPU, dual-core CPU, tri-core CPU, and so on. Your selection determines the number of sockets that the virtual machine has.

For more information about multicore CPUs, see the *vSphere Resource Management* documentation.

Change CPU Hot Plug Settings

By default, you cannot add CPU resources to a virtual machine when the virtual machine is turned on. The CPU hot plug option lets you add CPU resources to a running virtual machine.

The following conditions apply:

- For best results, use virtual machines that are compatible with ESXi 5.0 or later.
- Hot-adding multicore virtual CPUs is supported only with virtual machines that are compatible with ESXi 5.0 or later.
- Not all guest operating systems support CPU hot add. You can disable these settings if the guest is not supported.

- To use the CPU hot plug feature with virtual machines that are compatible with ESXi 4.x and later, set the **Number of cores per socket** to 1.
- Adding CPU resources to a running virtual machine with CPU hot plug enabled disconnects and reconnects all USB passthrough devices that are connected to that virtual machine.

Prerequisites

Required privileges: **Virtual Machine.Configuration.Settings**

Verify that the virtual machine is running and is configured as follows.

- Latest version of VMware Tools installed.
- Guest operating system that supports CPU hot plug.
- Virtual machine compatibility is ESX/ESXi 4.x or later.
- Virtual machine is turned off.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand **CPU**, and select **Enable CPU Hot Add**.

3 Click **OK**.

You can now add CPUs even if the virtual machine is turned on.

Change the Number of Virtual CPUs

You can configure a virtual machine that runs on an ESXi host 6.0 and later to have up to 128 virtual CPUs. You can change the number of virtual CPUs while your virtual machine is powered off. If virtual CPU hotplug is enabled, you can increase the number of virtual CPUs while the virtual machine is running.

Virtual CPU hot add is supported for virtual machines with multicore CPU support and ESXi 5.0 and later compatibility. When the virtual machine is turned on, and CPU hot add is enabled, you can hot add virtual CPUs to the running virtual machine. You can add only multiples of the number of cores per socket.

Important When you configure your virtual machine for multicore virtual CPU settings, you must ensure that your configuration complies with the requirements of the guest operating system EULA.

Prerequisites

- If CPU hot add is not enabled, turn off the virtual machine before adding CPUs.
- To hot add multicore CPUs, verify that the virtual machine compatibility is ESXi 5.0 and later.
- Required privilege: **Virtual Machine.Configuration.Change CPU Count** on the virtual machine

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 Expand CPU, and select the number of cores from the **CPU** drop-down menu.

3 Select the number of cores per socket from the **Cores Per Socket** drop-down menu.

4 Click **OK**.

Allocate CPU Resources

To manage workload demands, you can change the amount of CPU resources allocated to a virtual machine by using the shares, reservations, and limits settings.

A virtual machine has the following user-defined settings that affect its CPU resource allocation.

Limit Places a limit on the consumption of CPU time for a virtual machine. This value is expressed in MHz or GHz.

Reservation Specifies the guaranteed minimum allocation for a virtual machine. The reservation is expressed in MHz or GHz.

Shares Each virtual machine is granted a number of CPU shares. The more shares a virtual machine has, the more often it gets a time slice of a CPU when there is no CPU idle time. Shares represent a relative metric for allocating CPU capacity.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand **CPU**, and allocate the CPU capacity for the virtual machine.

Option	Description
Reservation	Guaranteed CPU allocation for this virtual machine.
Limit	Upper limit for this virtual machine's CPU allocation. Select **Unlimited** to specify no upper limit.
Shares	CPU shares for this virtual machine in relation to the parent's total. Sibling virtual machines share resources according to their relative share values bounded by the reservation and limit. Select **Low**, **Normal**, or **High**, which specify share values respectively in a 1:2:4 ratio. Select **Custom** to give each virtual machine a specific number of shares, which express a proportional weight.

3 Click **OK**.

Configure Hyperthreaded Core Sharing

To increase performance, you can select how the virtual CPUs of a virtual machine share physical cores on a hyperthreaded system.

Hyperthreading technology allows a single physical processor to behave like two logical processors. The hyperthreaded core sharing option provides detailed control over whether to schedule a virtual machine to share a physical processor core. The processor can run two independent applications at the same time. Although hyperthreading does not double the performance of a system, it can increase performance by better utilizing idle resources.

ESXi generally manages processor scheduling well, even when hyperthreading is enabled. These settings are useful only for fine-tuning critical virtual machines.

Prerequisites

- The hyperthreaded core sharing option must be enabled in your system's BIOS settings. See the *vSphere Resource Management* documentation.
- Turn off the virtual machine.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand **CPU**, and select a sharing mode from the **HT Sharing** drop-down menu.

Option	Description
Any (default)	The virtual CPUs of this virtual machine can share cores with other virtual CPUs of this or other virtual machines.
None	The virtual CPUs of this virtual machine have exclusive use of a processor core whenever they are scheduled to it. The other hyperthread of the core is halted while this virtual machine is using the core.
Internal	On a virtual machine with exactly two virtual processors, the two virtual processors are allowed to share one physical core (at the discretion of the host scheduler), but this virtual machine never shares a core with any other virtual machine. If this virtual machine has any other number of processors other than two, this setting is the same as the None setting.

3 Click **OK**.

Configure Processor Scheduling Affinity

The **Scheduling Affinity** option gives you detailed control over how virtual machine CPUs are distributed across the host's physical cores. The option supports hyperthreading if hyperthreading is enabled. ESXi generally manages processor scheduling well, even when hyperthreading is enabled. These settings are useful only for fine-tuning critical virtual machines.

Using CPU affinity, you can assign a virtual machine to a specific processor. This assignment allows you to restrict the assignment of virtual machines to a specific available processor in multiprocessor systems.

This setting does not appear for virtual machines in a DRS cluster or when the host has only one processor core and no hyperthreading.

For potential issues with CPU affinity, see the *vSphere Resource Management* documentation.

Prerequisites

- Verify that the virtual machine is turned off.
- Verify that the virtual machine does not reside in a DRS cluster.
- Verify that the host has more than one physical processor core.
- Privileges: **Virtual machine.Configuration.Change resource**

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand **CPU**, and enter a comma-separated list of hyphenated processor ranges in the **Scheduling Affinity** text box.

For example, "0,4-7" would indicate affinity with CPUs 0,4,5,6, and 7. Selecting all processors is identical to selecting no affinity. You must provide at least as many processor affinities as you have virtual CPUs.

3 Click **OK**.

Change CPU Identification Mask Settings in the vSphere Web Client

CPU identification (CPU ID) masks control the CPU features visible to the virtual machine's guest operating system. Masking or hiding CPU features can make a virtual machine widely available to ESXi hosts for migration. vCenter Server compares the CPU features available to a virtual machine with the CPU features of the destination host to determine whether to allow or disallow migration with vMotion.

For example, masking the AMD No eXecute (NX) and the Intel eXecute Disable (XD) bits prevents the virtual machine from using these features, but provides compatibility that allows you to migrate virtual machines to ESXi hosts that do not include this capability. When the NX/XD bit is visible to the guest operating system, the virtual machine can use this feature, but you can migrate the virtual machine only to hosts on which the feature is enabled.

Caution Changing the CPU compatibility masks can result in an unsupported configuration. Do not manually change the CPU compatibility masks unless instructed to do so by VMware Support or a VMware Knowledge base article.

Prerequisites

Turn off the virtual machine.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand **CPU**, and in the **CPUID Mask** drop-down menu, select an `NX/XD` option.

Option	Description
Hide the `NX/XD` flag from guest	Increases vMotion compatibility. Hiding the `NX/XD` flag increases vMotion compatibility between hosts, but might disable certain CPU security features.
Expose the `NX/XD` flag to guest	Keeps all CPU security features enabled.
Keep current Advanced setting values for the `NX/XD` flag	Uses the `NX/XD` flag settings specified in the CPU Identification Mask dialog box. Enabled only when current settings specify something other than what is specified in the other `NX/XD` flag options, for example, if the `NX/XD` flag bit setting varies with processor brand.

3 Click **OK**.

Expose VMware Hardware Assisted Virtualization

You can expose full CPU virtualization to the guest operating system so that applications that require hardware virtualization can run on virtual machines without binary translation or paravirtualization.

Prerequisites

- Verify that the virtual machine compatibility is ESXi 5.1 and later.
- Intel Nehalem Generation (Xeon Core i7) or later processors or AMD Opteron Generation 3 (Greyhound) or later processors.
- Verify that Intel VT-x or AMD-V is enabled in the BIOS so that hardware assisted virtualization is possible.
- Required Privileges: **Virtual machine.Configuration.Settings** set on the vCenter Server system.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand **CPU**, and select **Expose hardware-assisted virtualization to guest OS**.

3 Click **OK**.

The **Manage** tab refreshes, and the Nested Hypervisor CPU option shows **Enabled.**

Enable Virtual CPU Performance Counters

You can use performance tuning tools in the guest operating system for software profiling. You can identify and improve processor performance problems. This capability is useful for software developers who optimize or debug software that runs in the virtual machine.

The following conditions apply:

- If virtual CPU performance counters are enabled, you can migrate the virtual machine only to hosts that have compatible CPU performance counters.
- If an ESXi host's BIOS uses a performance counter or if Fault Tolerance is enabled, some virtual performance counters might not be available for the virtual machine to use.

NOTE If a virtual machine resides on an ESXi host in an EVC cluster, CPU counters are not supported for virtual machine creation or editing. You must disable CPU performance counters.

For a list of virtualized Model-Specific Registers (MSRs), see the VMware knowledge base article at http://kb.vmware.com/kb/2030221.

Prerequisites

- Verify that the virtual machine compatibility is ESXi 5.1 and later.
- Verify that the virtual machine is turned off.
- Verify that Intel Nehalem Generation (Xeon Core i7) or later processors or AMD Opteron Generation 3 ("Greyhound") or later processors are installed.
- Verify that Intel VT-x or AMD-V is enabled in the BIOS so that hardware-assisted virtualization is possible.
- Required Privileges: **Virtual machine.Configuration.Settings** is set on the vCenter Server system.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand **CPU** and enable virtualized CPU performance counters.

3 Click **OK**.

Change CPU/MMU Virtualization Settings

ESXi can determine whether a virtual machine should use hardware support for virtualization. ESXi makes this determination based on the processor type and the virtual machine. Overriding the automatic selection can provide better performance for some use cases.

You can use software MMU when your virtual machine runs heavy workloads, such as, Translation Lookaside Buffers (TLBs) intensive workloads that has significant impact on the overall system performance. However, software MMU has a higher overhead memory requirement than hardware MMU. Hence, in order to support software MMU, the maximum overhead supported for virtual machine limit in the VMkernel needs to be increased. You can configure your virtual machine with up to 128 CPUs, if your virtual machine host has ESXi 6.0 and later compatibility (hardware version 11).

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand **CPU**, and select an instruction set from the **CPU/MMU Virtualization** drop-down menu.

3 Click **OK**.

Virtual Memory Configuration

You can add, change, or configure virtual machine memory resources or options to enhance virtual machine performance. You can set most of the memory parameters during virtual machine creation or after the guest operating system is installed. Some actions require that you power off the virtual machine before changing the settings.

The memory resource settings for a virtual machine determine how much of the host's memory is allocated to the virtual machine. The virtual hardware memory size determines how much memory is available to applications that run in the virtual machine. A virtual machine cannot benefit from more memory resources than its configured virtual hardware memory size. ESXi hosts limit the memory resource use to the maximum amount useful for the virtual machine, so that you can accept the default of Unlimited memory resources.

Change the Memory Configuration

You can reconfigure the amount of memory allocated to a virtual machine to enhance performance.

Minimum memory size is 4MB for virtual machines that use BIOS firmware. Virtual machines that use EFI firmware require at least 96MB of RAM or they cannot power on.

Maximum memory size for a virtual machine depends on the host's physical memory and the virtual machine's compatibility setting.

If the virtual machine memory is greater than the host memory size, swapping occurs, which can have a severe effect on virtual machine performance. The maximum for best performance represents the threshold above which the host’s physical memory is insufficient to run the virtual machine at full speed. This value fluctuates as conditions on the host change, for example, as virtual machines are powered on or off.

The memory size must be a multiple of 4MB.

Table 6-3. Maximum Virtual Machine Memory

Introduced in Host Version	Virtual Machine Compatibility	Maximum Memory Size
ESXi 6.0	ESXi 6.0 and later	4080GB
ESXi 5.5	ESXi 5.5 and later	1011GB
ESXi 5.1	ESXi 5.1 and later	1011GB
ESXi 5.0	ESXi 5.0 and later	1011GB
ESX/ESXi 4.x	ESX/ESXi 4.0 and later	255GB
ESX/ESXi 3.x	ESX/ESXi 3.5 and later	65532MB

The ESXi host version indicates when support began for the increased memory size. For example, the memory size of a virtual machine with ESX/ESXi 3.5 and later compatibility running on ESXi 5.0 is restricted to 65,532MB.

Prerequisites

Verify that you have the **Virtual machine.Configuration.Memory** privilege on the virtual machine.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand Memory.

3 In the **RAM** text box, type the amount of RAM to assign to the virtual machine or select one of the suggested values from the drop-down menu.

4 Select whether the memory is specified in MB or GB.

5 Click **OK**.

Allocate Memory Resources

You can change the amount of memory resources allocated to a virtual machine by using the shares, reservations, and limits settings. The host determines the appropriate amount of physical RAM to allocate to virtual machines based on these settings. You can assign a high or low shares value to a virtual machine, depending on its load and status.

The following user-defined settings affect the memory resource allocation of a virtual machine.

Limit Places a limit on the consumption of memory for a virtual machine. This value is expressed in megabytes.

Reservation Specifies the guaranteed minimum allocation for a virtual machine. The reservation is expressed in megabytes. If the reservation cannot be met, the virtual machine will not turn on.

Shares Each virtual machine is granted a number of memory shares. The more shares a virtual machine has, the greater share of host memory it receives. Shares represent a relative metric for allocating memory capacity. For more information about share values, see the *vSphere Resource Management* documentation.

You cannot assign a reservation to a virtual machine that is larger than its configured memory. If you give a virtual machine a large reservation and reduce its configured memory size, the reservation is reduced to match the new configured memory size.

Prerequisites

Verify that the virtual machine is turned off.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand Memory, and allocate the memory capacity for the virtual machine.

Option	Description
Reservation	Guaranteed memory allocation for this virtual machine.
Limit	Upper limit for this virtual machine's memory allocation. Select **Unlimited** to specify no upper limit.
Shares	The values **Low**, **Normal**, **High**, and **Custom** are compared to the sum of all shares of all virtual machines on the server.

3 Click **OK**.

Change Memory Hot Add Settings

Memory hot add lets you add memory resources for a virtual machine while that virtual machine is turned on.

Enabling memory hot add produces some extra memory overhead on the ESXi host for the virtual machine.

Prerequisites

- Power off the virtual machine.
- Ensure that the virtual machine has a guest operating system that supports memory hot add functionality.
- Ensure that the virtual machine compatibility is ESXi 4.x and later.
- Ensure that VMware Tools is installed.

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **Memory**, and select **Enable** to enable adding memory to the virtual machine while it is turned on.
3. Click **OK**.

Network Virtual Machine Configuration

ESXi networking features provide communication between virtual machines on the same host, between virtual machines on different hosts, and between other virtual and physical machines. The networking features also allow management of ESXi hosts and provide communication between VMkernel services (NFS, iSCSI, or vSphere vMotion) and the physical network. When you configure networking for a virtual machine, you select or change an adapter type, a network connection, and whether to connect the network when the virtual machine powers on.

Network Adapter Types

When you configure a virtual machine, you can add network adapters (NICs) and specify the adapter type.

The type of network adapters that are available depend on the following factors:

- The virtual machine compatibility, which depends on the host that created or most recently updated it.
- Whether the virtual machine compatibility has been updated to the latest version for the current host.
- The guest operating system.

The following NIC types are supported:

E1000E	Emulated version of the Intel 82574 Gigabit Ethernet NIC. E1000E is the default adapter for Windows 8 and Windows Server 2012.
E1000	Emulated version of the Intel 82545EM Gigabit Ethernet NIC, with drivers available in most newer guest operating systems, including Windows XP and later and Linux versions 2.4.19 and later.
Flexible	Identifies itself as a Vlance adapter when a virtual machine boots, but initializes itself and functions as either a Vlance or a VMXNET adapter, depending on which driver initializes it. With VMware Tools installed, the VMXNET driver changes the Vlance adapter to the higher performance VMXNET adapter.

Vlance

Emulated version of the AMD 79C970 PCnet32 LANCE NIC, an older 10 Mbps NIC with drivers available in 32-bit legacy guest operating systems. A virtual machine configured with this network adapter can use its network immediately.

VMXNET

Optimized for performance in a virtual machine and has no physical counterpart. Because operating system vendors do not provide built-in drivers for this card, you must install VMware Tools to have a driver for the VMXNET network adapter available.

VMXNET 2 (Enhanced)

Based on the VMXNET adapter but provides high-performance features commonly used on modern networks, such as jumbo frames and hardware offloads. VMXNET 2 (Enhanced) is available only for some guest operating systems on ESX/ESXi 3.5 and later.

VMXNET 3

A paravirtualized NIC designed for performance. VMXNET 3 offers all the features available in VMXNET 2 and adds several new features, such as multiqueue support (also known as Receive Side Scaling in Windows), IPv6 offloads, and MSI/MSI-X interrupt delivery. VMXNET 3 is not related to VMXNET or VMXNET 2.

SR-IOV passthrough

Representation of a virtual function (VF) on a physical NIC with SR-IOV support. The virtual machine and the physical adapter exchange data without using the VMkernel as an intermediary. This adapter type is suitable for virtual machines where latency might cause failure or that require more CPU resources.

SR-IOV passthrough is available in ESXi 5.5 and later for guest operating systems Red Hat Enterprise Linux 6 and later, and Windows Server 2008 R2 with SP2. An operating system release might contain a default VF driver for certain NICs, while for others you must download and install it from a location provided by the vendor of the NIC or of the host.

For information about assigning an SR-IOV passthrough network adapter to a virtual machine, see the *vSphere Networking* documentation.

For network adapter compatibility considerations, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Network Adapters and Legacy Virtual Machines

Legacy virtual machines are virtual machines that are supported by the product in use, but are not current for that product. The default network adapter types for all legacy virtual machines depend on the adapters available and compatible to the guest operating system and the version of virtual hardware on which the virtual machine was created.

If you do not upgrade a virtual machine to correspond with an upgrade to a newer version of an ESXi host, your adapter settings remain unchanged. If you upgrade your virtual machine to take advantage of newer virtual hardware, your default adapter settings will likely change to be compatible with the guest operating system and upgraded host hardware.

To verify the network adapters that are available to your supported guest operating system for a particular version of vSphere ESXi, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Change the Virtual Machine Network Adapter Configuration

To change the way the virtual machine communicates with the host or other virtual machines over the network, you can change the power-on connection setting, the MAC address, and the network connection for the virtual network adapter configuration for a virtual machine.

For information about configuring the networking for virtual machine network adapters, see the *vSphere Networking* documentation.

Prerequisites

Required privilege: **Network.Assign network** on a network if you are changing the network the virtual machine connects to.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand Network adapter, and select the port group to connect to from the drop-down menu.

   The menu lists all standard and distributed port groups that are available for virtual machine use on the host.

   If you want to provision bandwidth to the network adapter from a reserved quota by using vSphere Network I/O Control version 3, select a port group that is associated with the network resource pool that provides the quota.

   If the virtual machine runs on a Cisco UCS server, the drop-down menu also shows the port profiles that are available on the Cisco UCS Virtual Machine Fabric Extender (VM-FEX) distributed switch.

3 (Optional) Change the **Status** settings.

Option	Description
Connected	Select or deselect this option while the virtual machine is running to connect or disconnect the virtual network adapter. This check box is not available when the virtual machine is turned off.
Connect at power on	Select this option for the virtual network adapter to connect to the network when the virtual machine turns on. If you do not check this option, you must manually connect the adapter in order for the virtual machine to access the network.

4 Select the network adapter type to use from the **Adapter Type** drop-down menu.

5 (Optional) Select how to assign the **MAC address** from the drop-down menu.

   - Select **Automatic** to automatically assign a MAC address.
   - Select **Manual** to manually enter the MAC address that you want.

6 If the network adapter is connected to a distributed port group of a distributed switch that has vSphere Network I/O Control version 3 enabled, allocate bandwidth to the adapter.

   NOTE You cannot allocate bandwidth to **SR-IOV passthrough** network adapters.

   a From the **Shares** drop-down menu, set the relative priority of the traffic from this virtual machine as shares from the capacity of the connected physical adapter.

   b In the **Reservation** text box, reserve a minimum bandwidth that must be available to the VM network adapter when the virtual machine is powered on.

   c In the **Limit** text box, set a limit on the bandwidth that the VM network adapter can consume.

7 If the virtual machine is connected to a port profile on a Cisco UCS Virtual Machine Fabric Extender (VM-FEX) distributed switch, to enable vSphere DirectPath I/O with vMotion, under DirectPath I/O click **Enable**.

8 Click **OK**.

Add a Network Adapter to a Virtual Machine

You can add a network adapter (NIC) to a virtual machine to connect to a network, to enhance communications, or to replace an older adapter. When you add a NIC to a virtual machine, you select the adapter type, network connection, whether the device should connect when the virtual machine is turned on, and the bandwidth allocation.

For information about configuring the networking for virtual machine network adapters, see the *vSphere Networking* documentation

Prerequisites

Required privilege: **Network.Assign network** on a network.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 From the **New device** drop-down menu, select **Network** and click **Add**.

The new network adapter appears at the bottom of the device list.

3 (Optional) Expand **New Network**, and change the **Status** settings.

Option	Description
Connected	Select this option while the virtual machine is running to connect or disconnect the virtual network adapter. This check box is not available when the virtual machine is turned off.
Connect at power on	Select this option for the virtual network adapter to connect to the network when the virtual machine turns on. If you do not check this option, you must manually connect the adapter for the virtual machine to access the network.

4 Select the network adapter type to use from the **Adapter Type** drop-down menu.

5 (Optional) Select how to assign the **MAC address** from the drop-down menu.

- Select **Automatic** to automatically assign a MAC address.
- Select **Manual** to manually enter the MAC address that you want.

6 From the drop-down menu next to the New Network label, select the standard or distributed port group to connect to.

The menu lists all standard and distributed port groups that are available for virtual machine use on the host.

If you want to provision bandwidth to the network adapter from a reserved quota by using vSphere Network I/O Control version 3, select a port group that is associated with the network resource pool that provides the quota.

If the virtual machine runs on a Cisco UCS server, the drop-down menu also shows the port profiles that are available on the Cisco UCS Virtual Machine Fabric Extender (VM-FEX) distributed switch.

7 If the network adapter is connected to a distributed port group of a distributed switch that has vSphere Network I/O Control version 3 enabled, allocate bandwidth to the adapter.

NOTE You cannot allocate bandwidth to **SR-IOV passthrough** network adapters.

a From the **Shares** drop-down menu, set the relative priority of the traffic from this virtual machine as shares from the capacity of the connected physical adapter.

b In the **Reservation** text box, reserve a minimum bandwidth that must be available to the VM network adapter when the virtual machine is powered on.

c In the **Limit** text box, set a limit on the bandwidth that the VM network adapter can consume.

8 If the virtual machine is connected to a port profile on a Cisco UCS Virtual Machine Fabric Extender (VM-FEX) distributed switch, to enable vSphere DirectPath I/O with vMotion, under DirectPath I/O click **Enable**.

9 Click **OK**.

Parallel and Serial Port Configuration

Parallel and serial ports are interfaces for connecting peripherals to the virtual machine. The virtual serial port can connect to a physical serial port or to a file on the host computer. You can also use it to establish a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. You can add parallel and serial ports and change the serial port configuration.

Using Serial Ports with vSphere Virtual Machines

You can set up virtual serial port connections for vSphere virtual machines in several ways. The connection method that you select depends on the task that you need to accomplish.

You can set up virtual serial ports to send data in the following ways.

Physical serial port on the host	Sets the virtual machine to use a physical serial port on the host computer. This method lets you use an external modem or a hand-held device in a virtual machine.
Output to file	Sends output from the virtual serial port to a file on the host computer. This method lets you capture the data that a program running in the virtual machine sends to the virtual serial port.
Connect to a named pipe	Sets a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. With this method, two virtual machines or a virtual machine and a process on the host can communicate as if they were physical machines connected by a serial cable. For example, use this option for remote debugging of a virtual machine.
Connect over the network	Enables a serial connection to and from a virtual machine's serial port over the network. The Virtual Serial Port Concentrator (vSPC) aggregates traffic from multiple serial ports onto one management console. vSPC behavior is similar to physical serial port concentrators. Using a vSPC also allows network connections to a virtual machine's serial ports to migrate seamlessly when you use vMotion to migrate the virtual machine. For requirements and steps to configure the Avocent ACS v6000 virtual serial port concentrator, see http://kb.vmware.com/kb/1022303.

Server and Client Connections for Named Pipe and Network Serial Ports

You can select a client or server connection for serial ports. Your selection determines whether the system waits for a connection or initiates it. Typically, to control a virtual machine over a serial port, you select a server connection. This selection lets you control the connections, which is useful if you connect to the virtual machine only occasionally. To use a serial port for logging, select a client connection. This selection lets the virtual machine connect to the logging server when the virtual machine starts and to disconnect when it stops.

Supported Serial Ports

When you use a physical serial port for serial port passthrough from an ESXi host to a virtual machine, serial ports that are integrated into the motherboard are supported. A virtual machine can use up to 32 serial ports.

Unsupported Serial Ports

When you use a physical serial port for serial port passthrough from an ESXi host to a virtual machine, the serial ports connected through USB are not supported for serial port passthrough. They might be supported by USB passthrough from an ESXi host to a virtual machine. See "USB Configuration from an ESXi Host to a Virtual Machine," on page 140.

In addition, you cannot use Migration with VMotion when you use a physical serial port for serial passthrough.

Adding a Firewall Rule Set for Serial Port Network Connections

If you add or configure a serial port that is backed by a remote network connection, ESXi firewall settings can prevent transmissions.

Before you connect network-backed virtual serial ports, you must add one of the following firewall rule sets to prevent the firewall from blocking communication:

- **VM serial port connected to vSPC**. Use to connect the serial port output through a network with the **Use virtual serial port concentrator** option enabled to allow only outgoing communication from the host.
- **VM serial port connected over network**. Use to connect the serial port output through a network without the virtual serial port concentrator.

Important Do not change the allowed IP list for either rule set. Updates to the IP list can affect other network services that might be blocked by the firewall.

For details about allowing access to an ESXi service through the firewall, see the *vSphere Security* documentation.

Configure Virtual Machine Communication Interface Firewall

You can configure the virtual machine Communication Interface firewall (VMCI) to restrict virtual machines accessing the hypervisor based services and VMCI based services.

You can restrict VMCI usage to a subset of VMCI-based services on each virtual machine. For example, you can allow certain virtual machines to access VMCI services and deny access to others for security reasons.

Currently, VMCI devices support guest to host communication. A virtual machine can communicate with VMCI services through the following means:

- ESXi hypervisor
- Services installed on the host operating system in the form of a vmkernel module

- Applications installed by a verified vSphere Installation Bundle

Change the Serial Port Configuration

You can connect the virtual serial port to a physical serial port or to a file on the host computer. You can also use a host-side named pipe to set up a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. In addition, you can use a port or vSPC URI to connect a serial port over the network. You can add up to 32 serial ports to a virtual machine.

Virtual machines can be in a powered-on state during configuration.

Prerequisites

- Check that you know the correct media types for the port to access, vSPC connections, and any conditions that might apply. See "Using Serial Ports with vSphere Virtual Machines," on page 108.
- To connect a serial port over a network, add a Firewall rule set. See "Adding a Firewall Rule Set for Serial Port Network Connections," on page 109.
- To use authentication parameters with network serial port connections, see "Authentication Parameters for Virtual Serial Port Network Connections," on page 111.
- Required privileges:
  - **Virtual machine.Configuration.Modify device settings** on the virtual machine.
  - **Virtual machine.Interaction.Device connection** on the virtual machine to change the device connection status.

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **Serial port**, and select a connection type.

Option	Action
Use physical serial port	Select this option to have the virtual machine use a physical serial port on the host computer. Select the serial port from the drop-down menu.
Use output file	Select this option to send output from the virtual serial port to a file on the host computer. Browse to select an output file to connect the serial port to.
Use named pipe	Select this option to set a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. a Type a name for the pipe in the **Pipe Name** field. b Select the **Near end** and **Far end** of the pipe from the drop-down menus.
Connect over the network	Select **Use network** to connect through a remote network. a Select the network backing. ■ Select **Server** to have the virtual machine monitor incoming connections from other hosts. ■ Select **Client** to have the virtual machine initiate a connection to another host. b Enter a **Port URI**. The URI is the remote end of the serial port to which the virtual machine's serial port should connect. c If vSPC is used as an intermediate step to access all virtual machines through a single IP address, select **Use Virtual Serial Port Concentrator** and enter the vSPC URI location.
Printer	Select **Printer** to connect to a remote printer.

3 (Optional) Select **Yield on CPU poll**.

   Select this option only for guest operating systems that use serial ports in polled mode. This option prevents the guest from consuming excessive CPUs.

4 Select **Connect at power on** to connect the serial port when the virtual machine powers on.

5 Click **OK**.

Example: Establishing Serial Port Network Connections to a Client or Server Without Authentication Parameters

If you do not use vSPC and you configure your virtual machine with a serial port connected as a server with a `telnet://:12345` URI, you can connect to your virtual machine's serial port from your Linux or Windows operating system.

```
telnet yourESXiServerIPAddress 12345
```

Similarly, if you run the Telnet Server on your Linux system on port 23 (`telnet://yourLinuxBox:23`), you configure the virtual machine as a client URI.

```
telnet://yourLinuxBox:23
```

The virtual machine initiates the connection to your Linux system on port 23.

Authentication Parameters for Virtual Serial Port Network Connections

When you establish serial port connections over the network, you can use authentication parameters to secure the network. These parameters can support an encrypted connection with a remote system using SSL over Telnet or Telnets, or an encrypted connection with a concentrator using SSL over Telnet or Telnets.

URI Forms

If you do not use virtual serial port network connection (vSPC) and you configure your virtual machine with a serial port connected as a server with a `telnet://:12345` URI, you can connect to your virtual machine's serial port from your Linux or Windows operating system. You use one of the following formats:

- Telnet over TCP.

  ```
  telnet://host:port
  ```

  The virtual machine and remote system can negotiate and use SSL if the remote system supports the Telnet authentication option. If not, the connection uses unencrypted text (plain text).

- Telnets over SSL over TCP.

  ```
  telnets://host:port
  ```

  SSL negotiation begins immediately, and you cannot use the Telnet authentication option.

Authentication Parameters

For an encrypted connection, the URI includes a set of authentication parameters. Enter the parameters as key words or key/value pairs. You can enter authentication parameters for secure Telnet (`telnets`), or for Telnet (`telnet`) as shown in the following syntax:

```
telnet://host:port #key[=value] [&key[=value] ...]
```

The first parameter must have a number sign (#) prefix. Additional parameters must have an ampersand (&) prefix. The following parameters are supported.

`thumbprint=value`	Specifies a certificate thumbprint against which the peer certificate thumbprint is compared. When you specify a thumbprint, certificate verification is enabled.
`peerName=value`	Specifies the peer name that is used to validate the peer certificate. When you specify a peer name, certificate verification is enabled.
`verify`	Forces certificate verification. The virtual machine will verify that the peer certificate subject matches the specified peerName and that it was signed by a certificate authority known to the ESXi host. Verification is enabled if you specify a thumbprint or peerName
`cipherList=value`	Specifies a list of SSL ciphers. The ciphers are specified as a list separated by colons, spaces, or commas.

Example: Establishing Serial Port Network Connections to a Client or Server

Simple Server Connection

To connect to a virtual machine's serial port from a Linux or Windows operating system if you do not use vSPC, configure the virtual machine with a serial port connected as a server with a `telnet://:12345` URI. To access a virtual serial port from a client, use `telnet yourESXiServerIPAddress 12345`.

Secure Server Connection

To enforce an encrypted connection to the virtual machine's serial port from a Linux operating system, you can configure Telnet to enforce encryption by configuring the virtual machine with a serial port connected as a server with a `telnet://:12345#verify` URI.

To access a virtual serial port from a client, use `telnet-ssl yourESXServerName 12345`. This connection will fail if the Telnet program you are using does not support SSL encryption.

Simple Client Connection

If you are running a Telnet server on your system and you want the virtual machine to automatically connect to it, you can configure the virtual machine as a client using `telnet://yourLinuxBox:23`.

The Virtual machine keeps initiating the Telnet connection to port 23 on *yourLinuxBox*.

Secure Client Connection

Additional URI options allow you to enforce a specific server certificate and restrict the ciphers being used. Virtual machines with a serial port configured as a client with `telnet://ipOfYourLinuxBox:23#cipherList=DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA&peerName=myLinuxBoxName.withDomain` will connect to *ipOfYourLinuxBox* only if the system supports one of two listed ciphers, and if it presents a trusted certificate issued to *myLinuxBoxName.withDomain*. Replace `.withDomain` with the full domain name, for example, `example.org`.

Add a Serial Port to a Virtual Machine

You can connect the virtual serial port to a physical serial port or to a file on the host computer. You can also use a host-side named pipe to set up a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. In addition, you can use a port or vSPC URI to connect a serial port over the network. A virtual machine can use up to 32 serial ports.

Prerequisites

- Verify that the virtual machine is powered off.
- Check that you known the correct media types for the port to access, vSPC connections, and any conditions that might apply. See "Using Serial Ports with vSphere Virtual Machines," on page 108.
- To connect a serial port over a network, add a Firewall rule set. See "Adding a Firewall Rule Set for Serial Port Network Connections," on page 109.
- To use authentication parameter with network serial port connections, see "Authentication Parameters for Virtual Serial Port Network Connections," on page 111.
- Required privilege: **Virtual Machine .Configuration.Add or Remove Device**

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, select **Serial Port** from the **New device** drop-down menu, and click **Add**.

   The serial port appears at the bottom of the virtual device list.
3. Expand **New Serial Port**.
4. On the **Virtual Hardware** tab, expand **Serial port**, and select a connection type.

Option	Action
Use physical serial port	Select this option to have the virtual machine use a physical serial port on the host computer. Select the serial port from the drop-down menu.
Use output file	Select this option to send output from the virtual serial port to a file on the host computer. Browse to select an output file to connect the serial port to.
Use named pipe	Select this option to set a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. a Type a name for the pipe in the **Pipe Name** field. b Select the **Near end** and **Far end** of the pipe from the drop-down menus.
Connect over the network	Select **Use network** to connect through a remote network. a Select the network backing. ■ Select **Server** to have the virtual machine monitor incoming connections from other hosts. ■ Select **Client** to have the virtual machine initiate a connection to another host. b Enter a **Port URI**. The URI is the remote end of the serial port to which the virtual machine's serial port should connect. c If vSPC is used as an intermediate step to access all virtual machines through a single IP address, select **Use Virtual Serial Port Concentrator** and enter the vSPC URI location.
Printer	Select **Printer** to connect to a remote printer.

5 (Optional) Select **Yield on poll**.

   Select this option only for guest operating systems that use serial ports in polled mode. This option prevents the guest from consuming excessive CPUs.

6 Select **Connect at power on** to connect the serial port when the virtual machine powers on.

7 Click **OK**.

Example: Establishing Serial Port Network Connections to a Client or Server Without Authentication Parameters

If you do not use vSPC and you configure your virtual machine with a serial port connected as a server with a `telnet://:12345` URI, you can connect to your virtual machine's serial port from your Linux or Windows operating system.

```
telnet yourESXiServerIPAddress 12345
```

Similarly, if you run the Telnet Server on your Linux system on port 23 (`telnet://yourLinuxBox:23`), you configure the virtual machine as a client URI.

```
telnet://yourLinuxBox:23
```

The virtual machine initiates the connection to your Linux system on port 23.

Change the Parallel Port Configuration

You can change the output file for peripheral device output and schedule the parallel port to connect when the virtual machine powers on.

NOTE If you are changing the parallel port on a virtual machine that runs on an ESXi 4.1 or earlier host, you can send output to a physical parallel port on the host or to an output file on the host. This option is not available with ESXi 5.0 and later.

Prerequisites

Verify that you have the following privileges:

- **Virtual machine.Configuration.Modify device settings** on the virtual machine.
- **Virtual machine.Interaction.Device connection** on the virtual machine to change the device connection status.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand **Parallel port**.

3 For virtual machines running on ESXi 4.1 and earlier hosts, select the type of media for the parallel port to access.

4 Click **Browse** to navigate to the file location.

5 Type a name for the file in the **Save As** text box and click **OK**.

   The file path appears in the **Connection** text box.

6 Select whether to connect the device whenever you power on the virtual machine.

   You can change this setting when the virtual machine is either powered on or powered off.

7 Click **OK**.

Add a Parallel Port to a Virtual Machine

To connect peripheral devices to virtual machines, such as printers or scanners, you can use a parallel port. You send the output of such devices to a file on the host computer.

NOTE If you are adding a parallel port to a virtual machine that runs on an ESXi 4.1 or earlier host, you can also select to send output to a physical parallel port on the host. This option is not available with ESXi 5.0 and later host versions.

Prerequisites

- Verify that the virtual machine is turned off. You cannot add or remove parallel ports if the virtual machine is turned on.
- Verify that you have the **Virtual machine.Configuration.Add or remove device** privilege on the virtual machine.

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, select **Parallel Port** from the **New device** drop-down menu, and click **Add**.

   The parallel port appears at the bottom of the virtual device list.
3. Expand **New Parallel port**, and click **Browse** to locate a folder to create the file in.
4. Type a name for the file in the **Save As** text box and click **OK**.

   The file path appears in the **Connection** text box.
5. (Optional) Select **Connect At Power On** to connect the device when the virtual machine powers on.
6. Click **OK**.

Output from the attached peripheral device is read to the newly created file.

Virtual Disk Configuration

You can add large-capacity virtual disks to virtual machines and add more space to existing disks, even when the virtual machine is running. You can set most of the virtual disk parameters during virtual machine creation or after you install the guest operating system.

You can store virtual machine data in a new virtual disk, an existing virtual disk, or a mapped SAN LUN. A virtual disk, which appears as a single hard disk to the guest operating system, is composed of one or more files on the host file system. You can copy or move virtual disks on the same hosts or between hosts.

For virtual machines running on an ESXi host, you can store the virtual machine data directly on a SAN LUN instead of storing it in a virtual disk file. This ability is useful if you are running applications in your virtual machines that must detect the physical characteristics of the storage device. Additionally, mapping a SAN LUN allows you to use existing SAN commands to manage storage for the disk.

To accelerate virtual machine performance, you can configure virtual machines to use vSphere Flash Read Cache™. For details about Flash Read Cache behavior, see the *vSphere Storage* documentation.

When you map a LUN to a VMFS volume, vCenter Server or the ESXi host creates a raw device mapping (RDM) file that points to the raw LUN. Encapsulating disk information in a file allows vCenter Server or the ESXi host to lock the LUN so that only one virtual machine can write to it. This file has a `.vmdk` extension, but the file contains only disk information that describes the mapping to the LUN on the ESXi system. The actual data is stored on the LUN. You cannot deploy a virtual machine from a template and store its data on a LUN. You can store only its data in a virtual disk file.

The amount of free space in the datastore is always changing. Ensure that you leave sufficient space for virtual machine creation and other virtual machine operations, such as growth of sparse files, snapshots, and so on. To review space utilization for the datastore by file type, see the *vSphere Monitoring and Performance* documentation.

Thin provisioning lets you create sparse files with blocks that are allocated upon first access, which allows the datastore to be over-provisioned. The sparse files can continue growing and fill the datastore. If the datastore runs out of disk space while the virtual machine is running, it can cause the virtual machine to stop functioning.

About Virtual Disk Provisioning Policies

When you perform certain virtual machine management operations, such as creating a virtual disk, cloning a virtual machine to a template, or migrating a virtual machine, you can specify a provisioning policy for the virtual disk file.

NFS datastores with Hardware Acceleration and VMFS datastores support the following disk provisioning policies. On NFS datastores that do not support Hardware Acceleration, only thin format is available.

You can use Storage vMotion or cross-host Storage vMotion to transform virtual disks from one format to another.

Thick Provision Lazy Zeroed

Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine. Virtual machines do not read stale data from the physical device.

Thick Provision Eager Zeroed

A type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take longer to create virtual disks in this format than to create other types of disks.

Thin Provision

Use this format to save storage space. For the thin disk, you provision as much datastore space as the disk would require based on the value that you enter for the virtual disk size. However, the thin disk starts small and at first, uses only as much datastore space as the disk needs for its initial operations. If the thin disk needs more space later, it can grow to its maximum capacity and occupy the entire datastore space provisioned to it.

Thin provisioning is the fastest method to create a virtual disk because it creates a disk with just the header information. It does not allocate or zero out storage blocks. Storage blocks are allocated and zeroed out when they are first accessed.

NOTE If a virtual disk supports clustering solutions such as Fault Tolerance, do not make the disk thin.

You can manually inflate the thin disk, so that it occupies the entire provisioned space. If physical storage space is exhausted and the thin provisioned disk cannot grow, the virtual machine becomes unusable.

Large Capacity Virtual Disk Conditions and Limitations

Virtual machines with large capacity virtual hard disks, or disks greater than 2TB, must meet resource and configuration requirements for optimal virtual machine performance.

The maximum value for large capacity hard disks is 62TB. When you add or configure virtual disks, always leave a small amount of overhead. Some virtual machine tasks can quickly consume large amounts of disk space, which can prevent successful completion of the task if the maximum disk space is assigned to the disk. Such events might include taking snapshots or using linked clones. These operations cannot finish when the maximum amount of disk space is allocated. Also, operations such as snapshot quiesce, cloning, Storage vMotion, or vMotion in environments without shared storage, can take significantly longer to finish.

Virtual machines with large capacity disks have the following conditions and limitations:

- The guest operating system must support large capacity virtual hard disks.
- You can move or clone disks that are greater than 2TB to ESXi 5.5 or later hosts or to clusters that have such hosts available.
- The datastore format must be VMFS5 or later or an NFS volume on a Network Attached Storage (NAS) server.
- Virtual Flash Read Cache supports a maximum hard disk size of 16TBs.
- VMFS3 volumes are not supported. You cannot move disks greater than 2TB from a VMFS5 datastore to a VMFS3 datastore.
- You cannot hot-extend virtual SATA disks, or any virtual disk if the capacity after extension is equal to or greater than 2TB.
- Fault Tolerance is not supported.
- Virtual SAN is not supported.
- BusLogic Parallel controllers are not supported.

Change the Virtual Disk Configuration

If you run out of disk space, you can increase the size of the disk. You can change the virtual device node and the persistence mode for virtual disk configuration for a virtual machine.

Prerequisites

Verify that you have the following privileges:

- **Virtual machine.Configuration.Modify device settings** on the virtual machine.
- **Virtual machine.Configuration.Extend virtual disk** on the virtual machine.
- **Datastore.Allocate space** on the datastore.

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **Hard disk** to view the disk options.
3. (Optional) To change the size of the disk, type a new value in the **Provisioned Size** text box and select the units from the drop-down menu.

4 (Optional) To change the way that disks are affected by snapshots, select a disk mode option.

Option	Description
Dependent	Dependent disks are included in snapshots.
Independent - Persistent	Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk.
Independent - Nonpersistent	Changes to disks in nonpersistent mode are discarded when you turn off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you turn off or reset the virtual machine.

5 Click **OK**.

Add a Hard Disk to a Virtual Machine

When you create a virtual machine, a default virtual hard disk is added. You can add another hard disk if you run out of disk space, if you want to add a boot disk, or for other file management purposes. When you add a hard disk to a virtual machine, you can create a virtual disk, add an existing virtual disk, or add a mapped SAN LUN.

You can add a virtual hard disk to a virtual machine before or after you add a SCSI or SATA storage controller. The new disk is assigned to the first available virtual device node on the default controller, for example (0:1). Only device nodes for the default controller are available unless you add additional controllers.

The following ways to add disks can help you plan your disk configuration. These approaches show how you can optimize controller and virtual device nodes for different disks. For storage controller limitations, maximums, and virtual device node behavior, see "SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility," on page 126.

Add an existing hard disk that is configured as a boot disk during virtual machine creation.

To ensure that the virtual machine can boot, remove the existing disk before you add the boot disk. After you add a new hard disk to the virtual machine, you might need to go into the BIOS setup to ensure that the disk you were using to boot the virtual machine is still selected as the boot disk. You can avoid this problem by not mixing adapter types, and by using device node 0 on the first adapter as the boot disk.

Keep the default boot disk and add a new disk during virtual machine creation.

The new disk is assigned to the next available virtual device node, for example (0:1) You can add a new controller and assign the disk to a virtual device node on that controller, for example (1:0) or (1:1).

Add multiple hard disks to an existing virtual machine.

If you add multiple hard disks to a virtual machine, you can assign them to several SCSI or SATA controllers to improve performance. The controller must be available before you can select a virtual device node. For example, if you add controllers 1, 2, and 3, and add four hard disks, you might assign the fourth disk to virtual device node (3:1).

- Add a New Hard Disk to a Virtual Machine on page 119

  You can add a virtual hard disk to an existing virtual machine, or you can add a hard disk when you customize the virtual machine hardware during the virtual machine creation process. For example, you might need to provide additional disk space for an existing virtual machine with a heavy work load. During virtual machine creation, you might want to add a hard disk that is preconfigured as a boot disk.

- Add an Existing Hard Disk to a Virtual Machine on page 121

  You can add an existing virtual hard disk to a virtual machine when you customize the virtual machine hardware during the virtual machine creation process or after the virtual machine is created. For example, you might want to add an existing hard disk that is preconfigured as a boot disk.

- Add an RDM Disk to a Virtual Machine on page 122

  You can use a raw device mapping (RDM) to store virtual machine data directly on a SAN LUN, instead of storing it in a virtual disk file. You can add an RDM disk to an existing virtual machine, or you can add the disk when you customize the virtual machine hardware during the virtual machine creation process.

Add a New Hard Disk to a Virtual Machine

You can add a virtual hard disk to an existing virtual machine, or you can add a hard disk when you customize the virtual machine hardware during the virtual machine creation process. For example, you might need to provide additional disk space for an existing virtual machine with a heavy work load. During virtual machine creation, you might want to add a hard disk that is preconfigured as a boot disk.

During virtual machine creation, a hard disk and a SCSI or SATA controller are added to the virtual machine by default, based on the guest operating system that you select. If this disk does not meet your needs, you can remove it and add a new hard disk at the end of the creation process.

If you add multiple hard disks to a virtual machine, you can assign them to several controllers to improve performance. For controller and bus node behavior, see "SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility," on page 126.

Prerequisites

- Ensure that you are familiar with configuration options and caveats for adding virtual hard disks. See "Virtual Disk Configuration," on page 115.
- Before you add disks greater than 2TB to a virtual machine, see "Large Capacity Virtual Disk Conditions and Limitations," on page 117.
- Verify that you have the **Virtual machine.Configuration.Add new disk** privilege on the destination folder or datastore.

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. (Optional) To delete the existing hard disk, move your cursor over the disk and click the **Remove** icon.

   The disk is removed from the virtual machine. If other virtual machines share the disk, the disk files are not deleted.
3. On the **Virtual Hardware** tab, select **New Hard Disk** from the **New device** drop-down menu and click **Add**.

   The hard disk appears in the Virtual Hardware devices list.
4. Expand **New hard disk**.
5. (Optional) Type a value for the hard disk and select the units from the drop-down menu.

6 Select the datastore location where you want to store the virtual machine files.

Option	Action
Store all virtual machine files in the same location on a datastore.	a (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the **VM storage policy** drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy. b Select a datastore and click **Next**.
Store all virtual machine files in the same datastore cluster.	a (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the **VM storage policy** drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage profile. b Select a datastore cluster. c (Optional) If you do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the datastore cluster. d Click **Next**.
Store virtual machine configuration files and disks in separate locations.	a Click **Advanced**. b For the virtual machine configuration file and for each virtual disk, click **Browse** and select a datastore or datastore cluster. c (Optional) Apply a virtual machine storage policy from the **VM storage profile** drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy. d (Optional) If you selected a datastore cluster and do not want to use Storage DRS with this virtual machine, select **Disable Storage DRS for this virtual machine** and select a datastore within the datastore cluster. e Click **Next**.

7 Select the format for the virtual machine's disks and click **Next**.

Option	Action
Thick Provision Lazy Zeroed	Create a virtual disk in a default thick format. Space required for the virtual disk is allocated during creation. Any data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine.
Thick Provision Eager Zeroed	Create a thick disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out during creation. It might take much longer to create disks in this format than to create other types of disks.
Thin Provision	Use the thin provisioned format. At first, a thin provisioned disk uses only as much datastore space as the disk initially needs. If the thin disk needs more space later, it can grow to the maximum capacity allocated to it.

8 In the **Shares** drop-down menu, select a value for the shares to allocate to the virtual disk.

Shares is a value that represents the relative metric for controlling disk bandwidth. The values Low, Normal, High, and Custom are compared to the sum of all shares of all virtual machines on the host.

9 If you selected **Custom**, type a number of shares in the text box.

10 In the **Limit - IOPs** box, enter the upper limit of storage resources to allocate to the virtual machine, or select **Unlimited**.

This value is the upper limit of I/O operations per second allocated to the virtual disk.

11 Accept the default or select a different virtual device node.

In most cases, you can accept the default device node. For a hard disk, a nondefault device node is useful to control the boot order or to have different SCSI controller types. For example, you might want to boot from an LSI Logic controller and share a data disk with another virtual machine that is using a Buslogic controller with bus sharing turned on.

12 (Optional) Select a disk mode and click **OK**.

Option	Description
Dependent	Dependent disks are included in snapshots.
Independent - Persistent	Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk.
Independent - Nonpersistent	Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset.

Add an Existing Hard Disk to a Virtual Machine

You can add an existing virtual hard disk to a virtual machine when you customize the virtual machine hardware during the virtual machine creation process or after the virtual machine is created. For example, you might want to add an existing hard disk that is preconfigured as a boot disk.

During virtual machine creation, a hard disk and a SCSI or SATA controller are added to the virtual machine by default, based on the guest operating system that you select. If this disk does not meet your needs, you can remove it and add an existing hard disk at the end of the creation process.

Prerequisites

- Make sure that you are familiar with controller and virtual device node behavior for different virtual hard disk configurations. See "Add a Hard Disk to a Virtual Machine," on page 118.
- Before you add disks greater than 2TB to a virtual machine, see "Large Capacity Virtual Disk Conditions and Limitations," on page 117.
- Verify that you have the **Virtual machine.Configuration.Add existing disk** privilege on the destination folder or datastore.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 (Optional) To delete the existing hard disk, move your cursor over the disk and click the **Remove** icon.

The disk is removed from the virtual machine. If other virtual machines share the disk, the disk files are not deleted.

3 On the **Virtual Hardware** tab, select **Existing Hard Disk** from the **New device** drop-down menu and click **Add**.

4 In the Datastores column, expand a datastore, select a virtual machine folder, and select the disk to add.

The disk file appears in the Contents column. The **File Type** drop-down menu shows the compatibility file types for this disk.

5 Click **OK**.

What to do next

- (Optional) Change the virtual disk configuration. See "Change the Virtual Disk Configuration," on page 117.
- (Optional) Use disk shares to prioritize virtual machine access to this disk. See "Use Disk Shares to Prioritize Virtual Machines," on page 123.

Add an RDM Disk to a Virtual Machine

You can use a raw device mapping (RDM) to store virtual machine data directly on a SAN LUN, instead of storing it in a virtual disk file. You can add an RDM disk to an existing virtual machine, or you can add the disk when you customize the virtual machine hardware during the virtual machine creation process.

When you give a virtual machine direct access to an RDM disk, you create a mapping file that resides on a VMFS datastore and points to the LUN. Although the mapping file has the same `.vmdk` extension as a regular virtual disk file, the mapping file contains only mapping information. The virtual disk data is stored directly on the LUN.

During virtual machine creation, a hard disk and a SCSI or SATA controller are added to the virtual machine by default, based on the guest operating system that you select. If this disk does not meet your needs, you can remove it and add an RDM disk at the end of the creation process.

Prerequisites

- Ensure that you are familiar with SCSI controller and virtual device node behavior for different virtual hard disk configurations. See "Add a Hard Disk to a Virtual Machine," on page 118.
- Before you add disks greater than 2TB to a virtual machine, see "Large Capacity Virtual Disk Conditions and Limitations," on page 117.
- Required privilege: **Virtual machine.Configuration.Raw device**

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. (Optional) To delete the existing hard disk, move your cursor over the disk and click the **Remove** icon.

   The disk is removed from the virtual machine. If other virtual machines share the disk, the disk files are not deleted.
3. On the **Virtual Hardware** tab, select **RDM Disk** from the **New device** drop-down menu and click **Add**.
4. Select the target LUN for the raw device mapping and click **OK**.

   The disk appears in the virtual device list.
5. Select the location for the mapping file.
   - To store the mapping file with the virtual machine configuration file, select **Store with the virtual machine**.
   - To select a location for the mapping file, select **Browse** and select the datastore location for the disk.

6 Select a compatibility mode.

Option	Description
Physical	Allows the guest operating system to access the hardware directly. Physical compatibility is useful if you are using SAN-aware applications on the virtual machine. However, a virtual machine with a physical compatibility RDM cannot be cloned, made into a template, or migrated if the migration involves copying the disk.
Virtual	Allows the RDM to behave as if it were a virtual disk, so that you can use such features as taking snapshots, cloning, and so on. When you clone the disk or make a template out of it, the contents of the LUN are copied into a `.vmdk` virtual disk file. When you migrate a virtual compatibility mode RDM, you can migrate the mapping file or copy the contents of the LUN into a virtual disk.

7 Accept the default or select a different virtual device node.

In most cases, you can accept the default device node. For a hard disk, a nondefault device node is useful to control the boot order or to have different SCSI controller types. For example, you might want to boot from an LSI Logic controller and share a data disk with another virtual machine using a BusLogic controller with bus sharing turned on.

8 (Optional) If you selected virtual compatibility mode, select a disk mode to change the way that disks are affected by snapshots.

Disk modes are not available for RDM disks using physical compatibility mode.

Option	Description
Dependent	Dependent disks are included in snapshots.
Independent - Persistent	Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk.
Independent - Nonpersistent	Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset.

9 Click **OK**.

Use Disk Shares to Prioritize Virtual Machines

You can change the disk resources for a virtual machine. If multiple virtual machines access the same VMFS datastore and the same logical unit number (LUN), use disk shares to prioritize the disk accesses from the virtual machines. Disk shares distinguish high-priority from low-priority virtual machines.

You can allocate the host disk's I/O bandwidth to the virtual hard disks of a virtual machine. Disk I/O is a host-centric resource so you cannot pool it across a cluster.

Shares is a value that represents the relative metric for controlling disk bandwidth to all virtual machines. The values are compared to the sum of all shares of all virtual machines on the server.

Disk shares are relevant only within a given host. The shares assigned to virtual machines on one host have no effect on virtual machines on other hosts.

You can select an IOP limit, which sets an upper bound for storage resources that are allocated to a virtual machine. IOPs are the number of I/O operations per second.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand **Hard disk** to view the disk options.

3 In the **Shares** drop-down menu, select a value for the shares to allocate to the virtual machine.

4 If you selected **Custom**, enter a number of shares in the text box.

5 In the **Limit - IOPs** box, enter the upper limit of storage resources to allocate to the virtual machine, or select **Unlimited**.

6 Click **OK**.

Configure Flash Read Cache for a Virtual Machine

You can configure Flash Read Cache for a virtual machine compatible with ESXi 5.5 or later.

Enabling Flash Read Cache lets you specify block size and cache size reservation.

Block size is the minimum number of contiguous bytes that can be stored in the cache. This block size can be larger than the nominal disk block size of 512 bytes, between 4KB and 1024KB. If a guest operating system writes a single 512 byte disk block, the surrounding cache block size bytes will be cached. Do not confuse cache block size with disk block size.

Reservation is a reservation size for cache blocks. There is a minimum number of 256 cache blocks. If the cache block size is 1MB, then the minimum cache size is 256MB. If the cache block size is 4K, then the minimum cache size is 1MB.

For more information about sizing guidelines, search for the *Performance of vSphere Flash Read Cache in VMware vSphere* white paper on the VMware web site.

Prerequisites

- Set up virtual flash resource.
- Verify that the virtual machine is compatible with ESXi 5.5 or later.

Procedure

1 To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.

2 Click the **Related Objects** tab and click **Virtual Machines**.

3 Right-click the virtual machine and select **Edit Settings**.

4 On the **Virtual Hardware** tab, expand **Hard disk** to view the disk options.

5 To enable Flash Read Cache for the virtual machine, enter a value in the **Virtual Flash Read Cache** text box.

6 Click **Advanced** to specify the following parameters.

Option	Description
Reservation	Select a cache size reservation.
Block Size	Select a block size.

7 Click **OK**.

Converting Virtual Disks from Thin to Thick

You can determine whether a virtual disk is in the thin provision format and if required, convert it to the thick provision format.

For more information on thin provisioning and available disk formats, see the *vSphere Storage* documentation.

Determine the Disk Format of a Virtual Machine in the vSphere Web Client

You can determine whether your virtual disk is in thick or thin format.

If you have thin provisioned disks, you can change them to thick by selecting **Flat pre-initialized** disk provisioning. You change thick provisioned disks to thin by selecting **Allocate and commit space on demand**.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand **Hard disk**.

   The disk type is displayed in the **Disk Provisioning** field.

3 Click **OK**.

What to do next

If your virtual disk is in the thin format, you can inflate it to its full size using the vSphere Web Client.

Convert a Virtual Disk from Thin to Thick in the vSphere Web Client

When the disk space is exhausted and a thin-provisioned disk cannot expand, the virtual machine cannot boot. If you created a virtual disk in the thin provision format, you can convert it to the thick provision format.

The thin provisioned disk starts small and at first, uses just as much storage space as it needs for its initial operations. After you convert the disk, it grows to its full capacity and occupies the entire datastore space provisioned to it during the disk's creation.

Procedure

1 Locate the virtual machine.

   a Select a datacenter, folder, cluster, resource pool, host, or vApp.

   b Click the **Related Objects** tab and click **Virtual Machines**.

2 Double-click the virtual machine, click the **Related Objects** tab and click **Datastores**.

   The datastore that stores the virtual machine files is listed.

3 Click the datastore link to open the datastore management panel.

4 Click the **Manage** tab and click **Files**.

5 Open the virtual machine folder and browse to the virtual disk file that you want to convert.

   The file has the `.vmdk` extension.

6 Right-click the virtual disk file and select **Inflate**.

The inflated virtual disk occupies the entire datastore space originally provisioned to it.

SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility

To access virtual disks, CD/DVD-ROM, and SCSI devices, a virtual machine uses storage controllers, which are added by default when you create the virtual machine. You can add additional controllers or change the controller type after virtual machine creation. You can make these changes while you are in the creation wizard. If you know about node behavior, controller limitations, and compatibility of different types of controllers before you change or add a controller, you can avoid potential boot problems.

How Storage Controller Technology Works

Storage controllers appear to a virtual machine as different types of SCSI controllers, including BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS, and VMware Paravirtual SCSI. AHCI SATA controllers are also available.

When you create a virtual machine, the default controller is optimized for best performance. The controller type depends on the guest operating system, the device type, and in some cases, the virtual machine's compatibility. For example, when you create virtual machines with Apple Mac OS X guests and ESXi 5.5 and later compatibility, the default controller type for both the hard disk and the CD/DVD drive is SATA. When you create virtual machines with Windows Vista and later guests, a SCSI controller is the default for the hard disk and a SATA controller is the default for the CD/DVD drive.

Each virtual machine can have a maximum of four SCSI controllers and four SATA controllers. The default SCSI or SATA controller is 0. When you create a virtual machine, the default hard disk is assigned to the default controller 0 at bus node (0:0).

When you add storage controllers, they are numbered sequentially 1, 2, and 3. If you add a hard disk, SCSI, or CD/DVD-ROM device to a virtual machine after virtual machine creation, the device is assigned to the first available virtual device node on the default controller, for example (0:1).

If you add a SCSI controller, you can reassign an existing or new hard disk or device to that controller. For example, you can assign the device to (1:*z*), where 1 is SCSI controller 1 and *z* is a virtual device node from 0 to 15. For SCSI controllers, *z* cannot be 7. By default, the virtual SCSI controller is assigned to virtual device node (*z*:7), so that device node is unavailable for hard disks or other devices.

If you add a SATA controller, you can reassign an existing or new hard disk or device to that controller. For example, you can assign the device to (1:*z*), where 1 is SATA controller 1 and *z* is a virtual device node from 0 to 29. For SATA controllers, you can use device nodes 0 through 29, including 0:7.

Storage Controller Limitations

Storage controllers have the following requirements and limitations:

- LSI Logic SAS and VMware Paravirtual SCSI are available for virtual machines with ESXi 4.x and later compatibility.
- AHCI SATA is available only for virtual machines with ESXi 5.5 and later compatibility.
- BusLogic Parallel controllers do not support virtual machines with disks larger than 2TB.

Caution Changing the controller type after the guest operating system is installed will make the disk and any other devices connected to the adapter inaccessible. Before you change the controller type or add a new controller, make sure that the guest operating system installation media contains the necessary drivers. On Windows guest operating systems, the driver must be installed and configured as the boot driver.

Storage Controller Compatibility

Adding different types of storage controllers to virtual machines that use BIOS firmware can cause operating system boot problems. In the following cases, the virtual machine might fail to boot correctly and you might have to enter the BIOS setup and select the correct boot device:

- If the virtual machine boots from LSI Logic SAS or VMware Paravirtual SCSI, and you add a disk that uses BusLogic, LSI Logic, or AHCI SATA controllers.
- If the virtual machine boots from AHCI SATA, and you add BusLogic Parallel or LSI Logic controllers.

Adding additional disks to virtual machines that use EFI firmware does not cause boot problems.

Table 6-4. VMware Storage Controller Compatibility

	Added Controller					
Existing Controller	**BusLogic Parallel**	**LSI Logic**	**LSI Logic SAS**	**VMware Paravirtual SCSI**	**AHCI SATA**	**IDE**
BusLogic Parallel	Yes	Yes	Yes	Yes	Yes	Yes
LSI Logic	Yes	Yes	Yes	Yes	Yes	Yes
LSI Logic SAS	Requires BIOS setup	Requires BIOS setup	Usually Works	Usually Works	Requires BIOS setup	Yes
VMware Paravirtual SCSI	Requires BIOS setup	Requires BIOS setup	Usually Works	Usually Works	Requires BIOS setup	Yes
AHCI SATA	Requires BIOS setup	Requires BIOS setup	Yes	Yes	Yes	Yes
IDE	Yes	Yes	Yes	Yes	Yes	N/A

Add a SATA Controller

If a virtual machine has multiple hard disks or CD/DVD-ROM devices, you can add up to three additional SATA controllers to assign the devices to. When you spread the devices among several controllers, you can improve performance and avoid data traffic congestion. You can also add additional controllers if you exceed the thirty-device limit for a single controller.

You can boot virtual machines from SATA controllers and use them for large-capacity virtual hard disks.

Not all guest operating systems support AHCI SATA controllers. Typically, when you create virtual machines with ESXi 5.5 and later compatibility and Mac OS X guest operating systems, a SATA controller is added by default for the virtual hard disk and CD/DVD-ROM devices. Most guest operating systems, including Windows Vista and later have a default SATA controller for CD/DVD-ROM devices. To verify support, see the *VMware Compatibility Guides* at http://www.vmware.com/resources/compatibility.

Prerequisites

- Verify that the virtual machine compatibility is ESXi 5.5 and later.
- Verify that you are familiar with storage controller behavior and limitations. See "SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility," on page 126.
- Verify that you have the **Virtual machine.Configuration.Add or remove device** privilege on the virtual machine.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 Click the **Virtual Hardware** tab, and select **SATA Controller** from the **New device** drop-down menu.

3 Click **Add**.

The controller appears in the Virtual Hardware devices list.

4 Click **OK**.

What to do next

You can add a hard disk or CD/DVD drive to the virtual machine and assign it to the new controller.

Add a SCSI Controller in the vSphere Web Client

Many virtual machines have a SCSI controller by default, depending on the guest operating system. If you have a heavily loaded virtual machine with multiple hard disks, you can add up to three additional SCSI controllers to assign the disks to. When you spread the disks among several controllers, you can improve performance and avoid data traffic congestion. You can also add additional controllers if you exceed the 15-device limit for a single controller.

Prerequisites

- Verify that you have the **Virtual machine.Configuration.Add or remove device** privilege on the virtual machine.
- Verify that you are familiar with storage controller behavior and limitations. See "SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility," on page 126.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, select **SCSI Controller** from the **New device** drop-down menu and click **Add**.

The controller appears in the Virtual Hardware devices list.

3 On the **Virtual Hardware** tab, expand **New SCSI Controller**, and select the type of sharing in the **SCSI Bus Sharing** drop-down menu.

Option	Description
None	Virtual disks cannot be shared by other virtual machines.
Virtual	Virtual disks can be shared by virtual machines on the same ESXi host. Select **Thick provision eager zeroed** when you create the disk.
Physical	Virtual disks can be shared by virtual machines on any ESXi host. Select **Thick provision eager zeroed** when you create the disk.

4 Select the controller type from the drop-down menu.

Do not select a BusLogic Parallel controller for virtual machines with disks larger than 2TB. This controller does not support large capacity hard disks.

5 Click **OK**.

What to do next

You can add a hard disk or other SCSI device to the virtual machine and assign it to the new SCSI controller.

Change the SCSI Bus Sharing Configuration in the vSphere Web Client

You can set the type of SCSI bus sharing for a virtual machine and indicate whether the SCSI bus is shared. Depending on the type of sharing, virtual machines can access the same virtual disk simultaneously if the virtual machines reside on the same ESXi host or on a different host.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand **SCSI controller**, and select the type of sharing in the **SCSI Bus Sharing** drop-down menu.

Option	Description
None	Virtual disks cannot be shared by other virtual machines.
Virtual	Virtual disks can be shared by virtual machines on the same ESXi host.
Physical	Virtual disks can be shared by virtual machines on any ESXi host.

For virtual or physical bus sharing, select **Thick provision eager zeroed** when you create the disk.

3 Click **OK**.

Change the SCSI Controller Type in the vSphere Web Client

You configure virtual SCSI controllers on your virtual machines to attach virtual disks and RDMs to.

The choice of SCSI controller does not affect whether your virtual disk is an IDE or SCSI disk. The IDE adapter is always ATAPI. The default for your guest operating system is already selected.

CAUTION Changing the SCSI controller type might result in a virtual machine boot failure.

Prerequisites

- Verify that you are familiar with the limitations and conditions for configuring SCSI controllers. See "SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility," on page 126.
- Verify that you have the **Virtual machine.Configuration.Modify device settings** privilege on the virtual machine.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand **SCSI controller**, and select a SCSI controller type from the **Change Type** drop-down menu.

The vSphere Web Client displays information about what will happen if you change the controller type. If you have selected a controller type that is not recommended for the virtual machine's guest operating system, a warning is displayed.

3 Select whether to change the controller type.

- Click **Change Type** to change the controller type.
- Click **Don't change** to cancel the change and keep the original controller type.

Do not select a BusLogic Parallel controller for virtual machines with disks larger than 2TB. This controller does not support large capacity hard disks.

4 Click **OK**.

About VMware Paravirtual SCSI Controllers

VMware Paravirtual SCSI controllers are high performance storage controllers that can result in greater throughput and lower CPU use. These controllers are best suited for high performance storage environments.

VMware Paravirtual SCSI controllers are available for virtual machines with ESXi 4.x and later compatibility. Disks on such controllers might not experience optimal performance gains if they have snapshots or if memory on the ESXi host is over committed. This behavior does not mitigate the overall performance gain of using VMware Paravirtual SCSI controllers as compared to other SCSI controller options.

If you have virtual machines with VMware Paravirtual SCSI controllers, those virtual machines cannot be part of an MSCS cluster.

For platform support for VMware Paravirtual SCSI controllers, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Add a Paravirtualized SCSI Adapter in the vSphere Web Client

You can add a VMware Paravirtual SCSI high performance storage controller to a virtual machine to provide greater throughput and lower CPU use.

VMware Paravirtual SCSI controllers are best suited for environments, especially SAN environments, running I/O-intensive applications.

For information about SCSI controller maximums and virtual device assignments, see "SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility," on page 126.

Prerequisites

- Verify that the virtual machine has a guest operating system with VMware Tools installed.
- Verify that the virtual machine compatibility is ESXi 4.x and later.
- Ensure that you are familiar with VMware Paravirtual SCSI limitations. See "About VMware Paravirtual SCSI Controllers," on page 130.
- To access boot disk devices attached to a VMware Paravirtual SCSI controller, verify that the virtual machine has a Windows 2003 or Windows 2008 guest operating system.
- In some operating systems, before you change the controller type, create a virtual machine with an LSI Logic controller, install VMware Tools, and then change to paravirtual mode.

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, select **SCSI Controller** from the **New device** drop-down menu and click **Add**.

   The controller appears at the bottom of the Virtual Hardware device list.
3. Expand SCSI controller and select **VMware Paravirtual** from the **Change Type** drop-down menu.
4. Click **OK**.

Other Virtual Machine Device Configuration

In addition to configuring virtual machine CPU and Memory and adding a hard disk and virtual NICs, you can also add and configure virtual hardware, such as DVD/CD-ROM drives, floppy drives, and SCSI devices. Not all devices are available to add and configure. For example, you cannot add a video card, but you can configure available video cards and PCI devices.

Change the CD/DVD Drive Configuration in the vSphere Web Client

You can configure DVD or CD devices to connect to client devices, host devices, or Datastore ISO files.

- Configure a Datastore ISO File for the CD/DVD Drive in the vSphere Web Client on page 131

  To install a guest operating system and its applications on a new virtual machine, you can connect the CD/DVD device to an ISO file that is stored on a datastore accessible to the host.

- Configure a Host Device Type for the CD/DVD Drive in the vSphere Web Client on page 132

  You can configure the virtual machine's CD/DVD drive to connect to a physical CD or DVD device on the host so that you can install a guest operating system, VMware Tools, or other applications.

- Configure a Client Device Type for the CD/DVD Drive in the vSphere Web Client on page 132

  To install a guest operating system and its applications or other media on a virtual machine, you can connect the CD/DVD device to a physical DVD or CD device on the system from which you access the vSphere Web Client

Configure a Datastore ISO File for the CD/DVD Drive in the vSphere Web Client

To install a guest operating system and its applications on a new virtual machine, you can connect the CD/DVD device to an ISO file that is stored on a datastore accessible to the host.

If an ISO image is not available on a local or shared datastore, upload the file to a datastore from your local system by using the datastore file browser. See "Upload ISO Image Installation Media for a Guest Operating System," on page 25.

To avoid performance issues and possible conflicts between virtual machines that might try to simultaneously access the ISO image, unmount and disconnect the ISO file when the installation finishes.

Prerequisites

Verify that you have the following privileges:

- **Virtual machine.Interaction.Configure CD media** on the virtual machine.
- **Datastore.Browse datastore** on the datastore to which you upload the installation media ISO image.
- **Datastore.Low level file operations** on the datastore to which you upload the installation media ISO image.

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Expand **CD/DVD drive**, and select **Datastore ISO File** from the drop-down menu.
3. Browse to select the file and click **OK**.
4. In the **Virtual Device Node** drop-down menu, select the node that the drive uses in the virtual machine.
5. (Optional) Select **Connect At Power On** to connect the device when the virtual machine powers on.
6. Click **OK**.

7 Turn on the virtual machine.

8 Click **Edit** and select **Connected** next to the datastore ISO file to connect the device.

9 Click **OK**.

Configure a Host Device Type for the CD/DVD Drive in the vSphere Web Client

You can configure the virtual machine's CD/DVD drive to connect to a physical CD or DVD device on the host so that you can install a guest operating system, VMware Tools, or other applications.

When you create a virtual machine, a controller is added by default and the CD/DVD drive is attached to that controller. The controller and driver type depend on the guest operating system. Typically, virtual machines with newer guest operating systems have a SATA controller and CD/DVD drive. Other guests use an IDE controller and CD/DVD drive.

If you connect to media that does not require you to turn off the virtual machine, you can select the media to connect to from the CD/DVD drive connection icon on the virtual machine **Summary** tab.

When you add a CD/DVD drive that is backed by a USB CD/DVD drive on the host, you must add the drive as a SCSI device. Hot adding and removing SCSI devices is not supported.

Prerequisites

- Verify that the virtual machine is turned off.
- Verify that the host is turned off before you add USB CD/DVD devices.
- You cannot use vMotion to migrate virtual machines that have CD drives that are backed by the physical CD drive on the host. Disconnect these devices before you migrate the virtual machine.
- Verify that you have the **Virtual machine.Interaction.Configure CD media** privilege on the virtual machine.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand **CD/DVD** and select **Host Device** from the drop-down menu.

3 (Optional) Select **Connect At Power On** to connect the device when the virtual machine powers on.

4 If more than one type of CD/DVD media is available on the host, select the media.

5 In the **Virtual Device Node** drop-down menu, select the node the drive uses in the virtual machine.

   The first available node is selected by default. You do not typically need to change the default.

6 Click **OK**.

7 Turn the virtual machine on and click the **Summary** tab.

The connected CD/DVD device appears in the VM Hardware list.

Configure a Client Device Type for the CD/DVD Drive in the vSphere Web Client

To install a guest operating system and its applications or other media on a virtual machine, you can connect the CD/DVD device to a physical DVD or CD device on the system from which you access the vSphere Web Client

By default, passthrough IDE mode is used for remote client device access. You can write or burn a remote CD only through passthrough mode access.

Prerequisites

- Verify that the virtual machine is turned on.

- Verify that the Client Integration Plug-In is installed.

Procedure

1 Right-click a virtual machine in the inventory and click the **Summary** tab.

2 In the VM Hardware pane, click the **CD/DVD drive** connection icon, select an available drive to connect to, and browse for the CD/DVD media.

   An Access Control dialog box opens. Click **allow** to proceed. To change your selection, click the connection icon, select **Disconnect**, and select a different option.

Add a CD or DVD Drive to a Virtual Machine in the vSphere Web Client

You can use a physical drive on a client or host or you can use an ISO image to add a CD/DVD drive to a virtual machine. CD/DVD drives are necessary for installing a guest operating system and VMware Tools.

The following conditions exist:

- If you add a CD/DVD drive that is backed by a USB CD/DVD drive on the host, you must add the drive as a SCSI device. Hot adding and removing SCSI devices is not supported.
- You must disconnect virtual machines that have CD drives that are backed by the physical CD drive on the host, before you migrate the virtual machine.
- You access the host CD-ROM device through emulation mode. Passthrough mode is not functional for local host CD-ROM access. You can write or burn a remote CD only through passthrough mode access, but in emulation mode you can only read a CD-ROM from a host CD-ROM device.

Prerequisites

- Verify that the virtual machine is turned off.
- To connect to a client device, verify that Client Integration Plug-in is installed.
- If an ISO image file is not available on a local or shared datastore, upload an ISO image to a datastore from your local system by using the datastore file browser. See "Upload ISO Image Installation Media for a Guest Operating System," on page 25.
- Verify that you have the **Virtual machine.Configuration.Add or remove device** privilege on the virtual machine.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 From the **New device** drop-down menu, select **CD/DVD Drive** and click **Add** .

   The new drive appears at the bottom of the Virtual Hardware list.

3 Expand **New CD/DVD Drive** and select the device type.

Option	Action
Client Device	a Select to connect the CD/DVD device to a physical DVD or CD device on the system from which you access the vSphere Web Client. b From the **Device Mode** drop-down menu, select **Passthrough IDE**.
Host Device	a Select to connect the CD/DVD device to a physical DVD or CD device on the host. b From the **CD/DVD Media** drop-down menu, select the media to connect to . c From the **Device Mode** drop-down menu, select **Emulate IDE**.
Datastore ISO File	a Select to connect the CD/DVD device to an ISO file that is stored on a datastore accessible to the host. b Browse to the file containing the ISO image to connect to and click **OK**.

When you turn on the virtual machine, you select the media to connect to from the **VM Hardware** panel on the virtual machine **Summary** tab.

4 (Optional) Select **Connect At Power On** to connect the device when the virtual machine turns on.

5 (Optional) To change the device node from the default, select a new mode from the **Virtual Device Node** drop-down menu.

6 Click **OK**.

What to do next

Turn on the virtual machine, select the media to connect to, and install the guest operating system or other applications.

Change the Floppy Drive Configuration in the vSphere Web Client

You can configure a virtual floppy drive device to connect to a client device or to an existing or new floppy image.

ESXi does not support floppy drives that are backed by a physical floppy drive on the host.

NOTE You cannot use vMotion to migrate virtual machines that have floppy drives backed by a physical floppy drive on ESX 3.5, 4. 0, and 4.x hosts that vCenter Server 5.0 manages. You must disconnect these devices before you migrate the virtual machine.

Prerequisites

Verify that you have the **Virtual machine.Interaction.Configure floppy media** privilege on the virtual machine.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand **Floppy drive**.

3 Select the device type to use for this virtual device.

Option	Action
Client Device	Select this option to connect the floppy device to a physical floppy device or a .flp floppy image on the system from which you access the vSphere Web Client.
Use existing floppy image	a Select this option to connect the virtual device to an existing floppy image on a datastore accessible to the host. b Click **Browse** and select the floppy image.
Create new floppy image	a Select this option to create a floppy image on a datastore accessible to the host. b Click **Browse** and browse to the location for the floppy image. c Enter a name for the floppy image and click **OK**.

4 (Optional) Select or deselect the **Connected** check box to connect or disconnect the device.

5 (Optional) Select **Connect At Power On** to connect the device when the virtual machine powers on.

6 Click **OK**.

Add a Floppy Drive to a Virtual Machine in the vSphere Web Client

Use a physical floppy drive or a floppy image to add a floppy drive to a virtual machine.

ESXi does not support floppy drives that are backed by a physical floppy drive on the host.

Note You cannot use vMotion to migrate virtual machines that have floppy drives backed by a physical floppy drive on ESX 3.5, 4. 0, and 4.x hosts that vCenter Server 5.0 manages. You must disconnect these devices before you migrate the virtual machine.

Prerequisites

Verify that you have the **Virtual machine.Configuration.Add or remove device** privilege on the virtual machine.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, select **Floppy Drive** from the **New device** drop-down menu, and click **Add**.

3 Expand **New Floppy drive** and select the device type to use for this virtual device.

Option	Description
Client Device	Select this option to connect the floppy device to a physical floppy device or a .flp floppy image on the system from which you access the vSphere Web Client.
Use existing floppy image	a Select this option to connect the virtual device to an existing floppy image on a datastore accessible to the host. b Click **Browse** and select the floppy image.
Create new floppy image	a Select this option to create a floppy image on a datastore accessible to the host. b Click **Browse** and browse to the location for the floppy image. c Enter a name for the floppy image and click **OK**.

4 (Optional) Select or deselect the **Connected** check box to connect or disconnect the device.

5 (Optional) Select **Connect At Power On** to connect the device when the virtual machine powers on.

6 Click **OK**.

Change the SCSI Device Configuration in the vSphere Web Client

You can change the physical device and configure the virtual device node. This is useful if you no longer need an existing device and want to connect to another device.

To prevent data congestion, you can assign a SCSI device to a SCSI controller and virtual device node other than the default. The new device is assigned to the first available virtual device node on the default SCSI controller, for example (0:1). Only device nodes for the default SCSI controller are available unless you add additional controllers.

For SCSI controller and virtual device node behavior, see "SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility," on page 126.

Prerequisites

- Power off the virtual machine.
- Required privilege: **Virtual machine.Configuration.Raw device**

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand **SCSI device**.

3 From the **Connection** drop-down menu, select the physical SCSI device to connect to.

4 (Optional) From the **Virtual Device Node** drop-down menu, select the virtual device node.

5 Click **OK**.

Add a SCSI Device to a Virtual Machine in the vSphere Web Client

To use peripheral SCSI devices, such as printers or storage devices, you must add the device to the virtual machine. When you add a SCSI device to a virtual machine, you select the physical device to connect to and the virtual device node.

The SCSI device is assigned to the first available virtual device node on the default SCSI controller, for example (0:1). To avoid data congestion, you can add another SCSI controller and assign the SCSI device to a virtual device node on that controller. Only device nodes for the default SCSI controller are available unless you add additional controllers. If the virtual machine does not have a SCSI controller, a controller is added when you add the SCSI device.

For SCSI controller and virtual device node assignments and behavior, see "SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility," on page 126.

Prerequisites

Required privileges: **Virtual machine.Configuration.Raw device**

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, select **SCSI Device** from the **New device** drop-down menu and click **Add**.

The SCSI device appears in the Virtual Hardware devices list.

3 Expand **New SCSI device** to change the device options.

4 (Optional) From the **Virtual Device Node** drop-down menu, select the virtual device node.

5 Click **OK**.

The virtual machine can access the device.

Add a PCI Device in the vSphere Web Client

vSphere DirectPath I/O allows a guest operating system on a virtual machine to directly access physical PCI and PCIe devices connected to a host. This action gives you direct access to devices such as high-performance graphics or sound cards. You can connect each virtual machine to up to six PCI devices.

You configure PCI devices on the host to make them available for passthrough to a virtual machine. See the *vSphere Networking* documentation. However, PCI passthroughs should not be enabled for ESXi hosts that are configured to boot from USB devices.

When PCI vSphere DirectPath I/O devices are available to a virtual machine, you cannot suspend, migrate with vMotion, or take or restore Snapshots of such virtual machines.

Prerequisites

- To use DirectPath, verify that the host has Intel Virtualization Technology for Directed I/O (VT-d) or AMD I/O Virtualization Technology (IOMMU) enabled in the BIOS.
- Verify that the PCI devices are connected to the host and marked as available for passthrough. However, if your ESXi host is configured to boot from a USB device, you should disable the USB controller for passthrough. VMware does not support USB controller passthrough for ESXi hosts that boot from USB devices or SD cards connected through USB channels. For more information, see http://kb.vmware.com/kb/2068645.
- Verify that the virtual machine is compatible with ESXi 4.x and later.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, select **PCI Device** from the **New Device** drop-down menu, and click **Add**.

3 Expand **New PCI device** and select the passthrough device to connect to the virtual machine from the drop-down list and click **Next**.

4 Click **OK**.

Configuring 3D Graphics

When you create or edit a virtual machine, you can configure 3D graphics to take advantage of Windows AERO, CAD, Google Earth, and other 3D design, modeling, and multimedia applications. Before you enable 3D graphics, become familiar with the available options and requirements.

You can enable 3D on virtual machines that have Windows desktop or Linux guest operating systems. Not all guests support 3D graphics. To verify 3D support for a guest operating system, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Prerequisites

VMware supports AMD and NVIDIA graphics cards. See the vendor Web site for supported cards. To use the graphics card or GPU hardware, download the appropriate VMware graphics driver from the vendor Web site.

- Go to the NVIDIA Web site for information about the VMware graphics driver for your NVIDIA graphics card.
- Go to the AMD Web site for information about the VMware graphics driver for your AMD graphics card.

Linux distributions must have a 3.2 or later kernel. If 3D is not available on a Linux guest, verify that the driver is available in the Linux kernel. If it is not available, upgrade to a more recent Linux distribution. The location of the kernel depends on whether the distribution is based on `deb` or `rpm`.

Table 6-5. Linux Driver Location

VMware Linux Guest Kernel Drivers	Debian Format	RPM Format
`vmwgfx.ko`	`dpkg -S vmwgfx.ko`	`rpm -qf vmwgfx.ko`
`vmwgfx_dri.so`	`dpkg -S vmwgfx_dri`	`rpm -qf vmwgfx_dri`
`vmware_drv.so`	`dpkg -S vmware_drv`	`rpm -qf vmware_drv`
`libxatracker.so.1`	`dpkg -S libxatracker`	`rpm -qf libxatracker`

3D Rendering Options

You can select the 3D rendering options for each virtual machine to be Hardware, Software, or Automatic.

Table 6-6. 3D Rendering Options

Rendering Option	Description
Hardware	The virtual machine must have access to a physical GPU. If the GPU is not available, the virtual machine cannot power on.
Software	The virtual machine's virtual device uses a software renderer and will not attempt to use a GPU, even if one if present.
Automatic	The default setting. The virtual device selects whether to use a physical GPU or software-based rendering. If a GPU is available on the system and has the resources required by the virtual machine, the virtual machine uses the GPU. Otherwise software rendering is used.

How Enabling 3D Graphics Affects the Virtual Machine

You can use vMotion to migrate virtual machines that have 3D graphics enabled. If the 3D Renderer is set to Automatic, virtual machines use either the GPU on the destination host or a software renderer, depending on GPU availability. To migrate virtual machines with the 3D Renderer set to Hardware, the destination host must have a GPU.

You can set a group of virtual machines to use only Hardware rendering. For example, if you have virtual machines that run CAD applications or have other complex engineering capabilities, you might require that those virtual machines have persistent high-quality 3D capability present. When you migrate such virtual machines, the destination host must also have GPU capability. If the host does not have GPU, the migration cannot proceed. To migrate such virtual machines, you must turn them off and change the renderer setting to Automatic.

Configure 3D Graphics and Video Cards

When you enable 3D graphics, you can select a hardware or software graphics renderer and optimize the graphics memory allocated to the virtual machine. You can increase the number of displays in multi-monitor configurations and change the video card settings to meet your graphics requirements.

The default setting for total video RAM is adequate for minimal desktop resolution. For more complex situations, you can change the default memory. Typically, 3D applications require a video memory of 64–512MB.

Fault Tolerance and HA are not supported for virtual machines that have 3D graphics enabled.

Prerequisites

- Verify that the virtual machine is powered off.
- Verify that the virtual machine compatibility is ESXi 5.0 and later.
- To enable 3D graphics in virtual machines with Windows 8 guest operating systems, the virtual machine compatibility must be ESXi 5.1 or later.
- To use a Hardware 3D renderer, ensure that graphics hardware is available. See "Configuring 3D Graphics," on page 137.
- If you update the virtual machine compatibility from ESXi 5.1 and later to ESXi 5.5 and later, reinstall VMware Tools to get the latest SVGA virtual graphics driver and Windows Display Driver Model driver.
- Verify that you have the **Virtual machine.Configuration.Modify device settings** privilege on the virtual machine.

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the **Virtual Hardware** tab, expand **Video Card**.
3. Select custom or automatic settings for your displays from the drop-down menu.

Option	Description
Auto-detect settings	Applies common video settings to the guest operating system.
Specify custom settings	Lets you select the number of displays and the total video memory.

4. Select the number of displays from the drop-down menu.

   You can set the number of displays and extend the screen across them.
5. Enter the required video memory.
6. (Optional) Click **Video Memory Calculator** to calculate the required video memory based on the maximum number of displays and resolution that the guest operating system must support, and click **OK**.
7. (Optional) Click **Enable 3D support**.

   This check box is active only for guest operating systems on which VMware supports 3D.
8. (Optional) Select a 3D Renderer.

Option	Description
Automatic	Selects the appropriate option (software or hardware) for this virtual machine.
Software	Uses normal CPU processing for 3D calculations.
Hardware	Requires graphics hardware (GPU) for faster 3D calculations. NOTE The virtual machine will not power on if graphics hardware is not available.

9. Click **OK**.

Sufficient memory allocation is set for this virtual machine's graphics.

Reduce Memory Overhead for Virtual machines with 3D graphics Option

Virtual machines with the 3D graphics option enabled can have higher memory consumption than other virtual machines. You can reduce the memory overhead by editing the configuration file (`.vmx` file) of your virtual machines and disabling certain memory related settings. Reducing the memory overhead of virtual machines can help you increase the number of virtual machines per host.

Prerequisites

Verify that your virtual machines are using hardware version 10 or later.

Procedure

1 Shut down the virtual machine on which the 3D graphics option is enabled.

2 Disable the **Accelerate 3D Graphics** option.

3 Upgrade you ESXi host to use the features available in hardware version 10 or later.

4 Set the maximum size of your display to the size you need.

5 Locate the configuration file (`.vmx`) of your virtual machine.

6 Open the virtual machine configuration file in a text editor and add the line, `vga.vgaOnly=TRUE`.

   This option removes all graphics and SVGA functionality from your SVGA device, but does not remove the settings that allow BIOS to enter VGA mode.

7 Save the changes and exit the text editor.

8 Power on your virtual machine and check the display console.

9 Verify the memory reservation settings in the `vmware.log` file.

USB Configuration from an ESXi Host to a Virtual Machine

You can add multiple USB devices to a virtual machine when the physical devices are connected to an ESXi host. USB passthrough technology supports adding USB devices, such as security dongles and mass storage devices to virtual machines that reside on the host to which the devices are connected.

How USB Device Passthrough Technology Works

When you attach a USB device to a physical host, the device is available only to virtual machines that reside on that host. The device cannot connect to virtual machines that reside on another host in the datacenter.

A USB device is available to only one virtual machine at a time. When a device is connected to a powered-on virtual machine, it is not available to connect to other virtual machines that run on the host. When you remove the active connection of a USB device from a virtual machine, it becomes available to connect to other virtual machines that run on the host.

Connecting a USB passthrough device to a virtual machine that runs on the ESXi host to which the device is physically attached requires an arbitrator, a controller, and a physical USB device or device hub.

USB Arbitrator

Manages connection requests and routes USB device traffic. The arbitrator is installed and enabled by default on ESXi hosts. It scans the host for USB devices and manages device connection among virtual machines that reside on the host. It routes device traffic to the correct virtual machine instance for delivery to the guest operating system. The arbitrator monitors the USB device and prevents other virtual machines from using it until you release it from the virtual machine it is connected to.

USB Controller

The USB hardware chip that provides USB function to the USB ports that it manages. The virtual USB Controller is the software virtualization of the USB host controller function in the virtual machine.

USB controller hardware and modules that support USB 3.0, 2.0, and USB 1.1 devices must exist on the host. Eight virtual USB controllers are available to each virtual machine. A controller must be present before you can add USB devices to the virtual computer.

The USB arbitrator can monitor a maximum of 15 USB controllers. Devices connected to controllers numbered 16 or greater are not available to the virtual machine.

USB Devices

You can add up to 20 USB devices to a virtual machine. This is the maximum number of devices supported for simultaneous connection to one virtual machine. The maximum number of USB devices supported on a single ESXi host for simultaneous connection to one or more virtual machines is also 20. For a list of supported USB devices, see the VMware knowledge base article at http://kb.vmware.com/kb/1021345. You can add USB 3.0 devices to Mac OSX guest operating system for VMware Fusion.

USB Autoconnect Feature

When you add a USB device connection from an ESXi host to a virtual machine, the autoconnect feature is enabled for the device connection. It is not disabled until you remove the device connection from the virtual machine.

With autoconnect enabled, the device connection re-establishes in the following cases:

- The virtual machine is cycling through power operations, such as Power Off/Power On, Reset, Pause/Resume.
- The device is unplugged from the host then plugged back in to the same USB port.
- The device is power cycled but has not changed its physical connection path.
- The device is mutating identity during usage.
- A new virtual USB device is added

The USB passthrough autoconnect feature identifies the device by using the USB path of the device on the host. It uses the physical topology and port location, rather than the device identity. This feature can seem confusing if you expect the autoconnect feature to match the connection target by device ID.

If the same device is plugged back in to the host through a different USB port, it cannot re-establish connection with the virtual machine. If you unplug the device from the host and plug in a different device to the same USB path, the new device appears and is connected to the virtual machine by the autoconnect feature that the previous device connection enabled.

Autoconnect is useful in cases where devices mutate during usage. For example, for iPhones and other such devices, the device VID:PID changes during software or firmware upgrades. The upgrade process disconnects and reconnects the devices to the USB port.

The USB port is speed-specific. The autoconnect feature assumes that devices do not transition from USB 1.1 (low-full speed) to USB 2.0 (high speed) or the reverse. You cannot interchange USB 2.0 high-speed devices with USB 1.1 devices. For example, you might connect a USB 2.0 high-speed device to a port and connect that device to the virtual machine. If you unplug the device from the host and plug a USB 1.1 device into the same port, the device does not connect to the virtual machine.

For a list of supported USB devices for passthrough from an ESXi host to a virtual machine, see the VMware knowledge base article at http://kb.vmware.com/kb/1021345.

vSphere Features Available with USB Passthrough

Migrations with vMotion and DRS are supported with USB device passthrough from an ESXi host to a virtual machine.

Table 6-7. vSphere Features Available for USB Passthrough from an ESXi Host to a Virtual Machine

Feature	Supported with USB Device Passthrough
vSphere Distributed Power Management (DPM)	No
vSphere Distributed Resource Scheduler (DRS)	Yes
vSphere Fault Tolerance	No
vSphere vMotion	Yes

For details about migration with vMotion, see "Configuring USB Devices for vMotion," on page 142.

If a host with connected USB devices resides in a DRS cluster with DPM enabled, you must disable DPM for that host. Otherwise DPM might turn off the host with the device, which disconnects the device from the virtual machine.

Configuring USB Devices for vMotion

With USB passthrough from a host to a virtual machine, you can migrate a virtual machine to another ESXi host in the same datacenter and maintain the USB passthrough device connections to the original host.

If a virtual machine has USB devices attached that pass through to an ESXi host, you can migrate that virtual machine with the devices attached.

For a successful migration, review the following conditions:

- You must configure all USB passthrough devices connected to a virtual machine for vMotion. If one or more devices is not configured for vMotion, the migration cannot proceed. For troubleshooting details, see the *vSphere Troubleshooting* documentation.
- When you migrate a virtual machine with attached USB devices away from the host to which the devices are connected, the devices remain connected to the virtual machine. However, if you suspend or power off the virtual machine, the USB devices are disconnected and cannot reconnect when the virtual machine is resumed. The device connections can be restored only if you move the virtual machine back to the host to which the devices are attached.
- If you resume a suspended virtual machine that has a Linux guest operating system, the resume process might mount the USB devices at a different location on the file system.
- If a host with attached USB devices resides in a DRS cluster with distributed power management (DPM) enabled, disable DPM for that host. Otherwise DPM might turn off the host with the attached device. This action disconnects the device from the virtual machine because the virtual machine migrated to another host.

- Remote USB devices require that the hosts be able to communicate over the management network following migration with vMotion, so the source and destination management network IP address families must match. You cannot migrate a virtual machine from a host that is registered to vCenter Server with an IPv4 address to a host that is registered with an IPv6 address.

Avoiding Data Loss with USB Devices

When a virtual machine connects to a physical UBS device on an ESXi host, virtual machine functions can affect USB device behavior and connections.

- Before you hot add memory, CPU, or PCI devices, you must remove any USB devices. Hot adding these resources disconnects USB devices, which might result in data loss.
- Before you suspend a virtual machine, make sure that a data transfer is not in progress. During the suspend or resume process, USB devices behave as if they have been disconnected, then reconnected. For information about suspend and resume behavior after migration with vMotion, see "Configuring USB Devices for vMotion," on page 142.
- Before you change the state of the arbitrator, make sure that USB devices residing on the host are not attached to a virtual machine. If USB devices become unavailable to a virtual machine, a host administrator might have disabled the arbitrator. When an administrator stops or disconnects the arbitrator for troubleshooting or other purposes, USB devices attached to that host become unavailable to the virtual machine. If a data transfer is taking place at this time, you might lose the data. To reestablish the arbitrator, you must restart the host.

Connecting USB Devices to an ESXi Host

You can connect and chain multiple USB hubs and devices to an ESXi host. Careful planning and knowledge of hub behavior and limitations can help ensure that your devices work optimally.

USB physical bus topology defines how USB devices connect to the host. Support for USB device passthrough to a virtual machine is available if the physical bus topology of the device on the host does not exceed tier seven. The first tier is the USB host controller and root hub. The last tier is the target USB device. You can cascade up to five tiers of external or internal hubs between the root hub and the target USB device. An internal USB hub attached to the root hub or built into a compound device counts as one tier.

The quality of the physical cables, hubs, devices, and power conditions can affect USB device performance. To ensure the best results, keep the host USB bus topology as simple as possible for the target USB device, and use caution when you deploy new hubs and cables into the topology. The following conditions can affect USB behavior:

- Communication delay between the host and virtual machine increases as the number of cascading hubs increases.
- Connecting or chaining multiple external USB hubs increases device enumeration and response time, which can make the power support to the connected USB devices uncertain.
- Chaining hubs together also increases the chance of port and hub error, which can cause the device to lose connection to a virtual machine.
- Certain hubs can cause USB device connections to be unreliable, so use care when you add a new hub to an existing setup. Connecting certain USB devices directly to the host rather than to a hub or extension cable might resolve their connection or performance issues.

NOTE To prevent additional problems, be aware of the physical constraints of long-term deployment in a machine room environment. Small devices are easily damaged by being stepped on or knocked loose.

In some cases, you must hard reset the device and hub to restore the device to a working state.

For a list of supported USB devices for passthrough from an ESXi host to a virtual machine, see the VMware knowledge base article at http://kb.vmware.com/kb/1021345.

USB Compound Devices

For compound devices, the virtualization process filters out the USB hub so that it is not visible to the virtual machine. The remaining USB devices in the compound appear to the virtual machine as separate devices. You can add each device to the same virtual machine or to different virtual machines if they run on the same host.

For example, the Aladdin HASP HL Drive USB dongle package contains three devices (0529:0001 HASP dongle, 13fe:1a00 Hub, 13fe:1d00 Kingston Drive). The virtualization process filters out the USB hub. The remaining Aladdin HASP HL Drive USB dongle devices (one Aladdin HASP dongle and one Kingston Drive) appear to the virtual machine as individual devices. You must add each device separately to make it accessible to the virtual machine.

Add USB Devices to an ESXi Host

You can connect multiple USB devices to ESXi hosts so that virtual machines that run on the hosts can access the devices. The number of devices that you can connect depends on several factors, such as how the devices and hubs chain together and the device type.

Each ESXi host has several USB ports. The number of ports on each host depends on the physical setup of the host. When you calculate the depth of hub chaining, remember that on a typical server the front ports connect to an internal hub.

The USB arbitrator can monitor a maximum of 15 USB controllers. If your system includes controllers that exceed the 15 controller limit and you connect USB devices to them, the devices are not available to the virtual machine.

The host treats USB CD/DVD-ROM devices as SCSI devices. Hot adding and removing these devices is not supported.

Prerequisites

- If a host has attached USB devices and resides in a DRS cluster with DPM enabled, disable DPM for that host. See the *vSphere Resource Management* documentation for instructions about overriding the default DPM setting for an individual host.
- Verify that you know the virtual machine requirements for USB devices. See "Connecting USB Devices to an ESXi Host," on page 143.
- Verify that the ESXi host is powered off before you add USB CD/DVD-ROM devices.
- Verify that the current version of your ESXi host is 6.0 or later for adding eight virtual xHCI controller to the ESXi host.

Procedure

◆ To add a USB device to an ESXi host, connect the device to an available port or hub.

The USB device appears in the virtual machine Add Hardware wizard device list.

What to do next

You can now add the device to the virtual machine.

Add a USB Controller to a Virtual Machine

USB controllers are available to add to virtual machines to support USB passthrough from an ESXi host or from a client computer to a virtual machine.

You can add one virtual xHCI controller, one virtual EHCI controller, and one virtual UHCI controller per virtual machine. With Hardware Version 11, the supported number of root hub ports per xHCI controller is eight (four logical USB 3.0 ports and four logical USB 2.0 ports).

The conditions for adding a controller vary, depending on the device version, the type of passthrough (host or client computer), and the guest operating system.

Table 6-8. USB Controller Support

Controller type	Supported USB Device Version	Supported for Passthrough from ESXi Host to VM	Supported for Passthrough from Client Computer to VM
EHCI+UHCI	2.0 and 1.1	Yes	Yes
xHCI	3.0, 2.0, and 1.1	Yes (USB 3.0, 2.0, and 1.1 devices only)	Yes (Linux, Windows 8 and later, and Windows Server 2012 and later guests)

For Mac OS X systems, the EHCI+UHCI controller is enabled by default and is required for USB mouse and keyboard access.

For virtual machines with Linux guests, you can add one or both controllers, but 3.0 superspeed devices are not supported for passthrough from an ESXi host to a virtual machine. You cannot add two controllers of the same type.

For USB passthrough from an ESXi host to a virtual machine, the USB arbitrator can monitor a maximum of 15 USB controllers. If your system includes controllers that exceed the 15 controller limit and you connect USB devices to them, the devices are not available to the virtual machine.

Prerequisites

- ESXi hosts must have USB controller hardware and modules that support USB 3.0, 2.0, and 1.1 devices present.
- Client computers must have USB controller hardware and modules that support USB 3.0, 2.0, and 1.1 devices present.
- To use the xHCI controller on a Linux guest, ensure that the Linux kernel version is 2.6.35 or later.
- Verify that the virtual machine is powered on.
- Required Privilege (ESXi host passthrough): **Virtual Machine.Configuration.Add or Remove Device**

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the Virtual Hardware tab, select **USB Controller** from the **New device** drop-down menu, and click **Add** .

   The new USB controller appears at the bottom of the Virtual Hardware device list.
3. Expand **New USB Controller** to change the USB controller type.

   If compatibility errors appear, fix them before you can add the controller.
4. Click **OK**.

What to do next

Add one or more USB devices to the virtual machine.

Add USB Devices from an ESXi Host to a Virtual Machine

You can add one or more USB passthrough devices from an ESXi host to a virtual machine if the physical devices are connected to the host on which the virtual machine runs.

If a USB device is connected to another virtual machine, you cannot add it until that machine releases it.

NOTE If you have the Apple Frontpanel Controller device in your environment, you can safely add it to a virtual machine. However, this device has no documented function and no known use. ESXi hosts do not use it and do not provide Xserver functionality for USB passthrough.

Prerequisites

- Verify that the virtual machine is compatible with ESX/ESXi 4.0 and later.
- Verify that a USB controller is present. See "Add a USB Controller to a Virtual Machine," on page 144.
- To use vMotion to migrate a virtual machine with multiple USB devices, enable all attached USB devices for vMotion. You cannot migrate individual USB devices. For vMotion limitations, see "Configuring USB Devices for vMotion," on page 142.
- When you add a CD/DVD-ROM drive that is backed by a USB CD/DVD drive on the host, add the drive as a SCSI device. Hot adding and removing SCSI devices is not supported.
- Verify that you know the virtual machine requirements for USB devices. See "USB Configuration from an ESXi Host to a Virtual Machine," on page 140.
- Required privileges: **Virtual Machine.Configuration.HostUSBDevice**

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. On the Virtual Hardware tab, select **Host USB Device** from the **New device** drop-down menu, and click **Add**.

   The new USB device appears at the bottom of the Virtual Hardware device list.
3. Expand **New USB Device**, and select the device to add.

   You can add multiple USB devices, but only one device at a time.
4. If you do not plan to migrate a virtual machine with USB devices attached, deselect the **Support vMotion** option.

   This action reduces migration complexity, which results in better performance and stability.
5. Click **OK**.

Remove USB Devices That Are Connected Through an ESXi Host

When you remove USB devices from a virtual machine, devices that use passthrough technology from a host to the virtual machine revert to the host. The devices become available to other virtual machines that run on that host.

Prerequisites

- Verify that the devices are not in use.

- To minimize the risk of data loss, follow the instructions to safely unmount or eject hardware for your operating system. Safely removing hardware allows accumulated data to be transmitted to a file. Windows operating systems typically include a Remove Hardware icon located in the System Tray. Linux operating systems use the **`umount`** command.

  NOTE You might need to use the `sync` command instead of or in addition to the `umount` command, for example, after you issue a `dd` command on Linux or other UNIX operating systems.

Procedure

1. Unmount or eject the USB device from the guest operating system.
2. Right-click a virtual machine in the inventory and select **Edit Settings**.
3. To remove the device, move your cursor over the device and click the **Remove** icon.
4. Click **OK** to save your changes.

Remove USB Devices from an ESXi Host

You can remove USB devices from the host if you must shut down the host for maintenance or if you do not want those devices to be available to virtual machines that run on the host. When you detach a USB device from the host, the device disconnects from the virtual machine.

CAUTION If data transfer is taking place when you remove USB devices from a host, you can lose data.

Prerequisites

Verify that the USB devices are not in use.

Procedure

- Follow the device manufacturers instructions to safely remove the device.

  When you remove the device from the host, it is no longer available to the virtual machines that run on the host.

USB Configuration from a Client Computer to a Virtual Machine

You can add multiple USB devices to a virtual machine when the physical devices connect to a client computer on which the vSphere Web Client is running. The vSphere Web Client must be logged in to an instance of vCenter Server that manages the ESXi host where the virtual machines reside. USB passthrough technology supports adding multiple USB devices, such as security dongles, mass storage devices, and smartcard readers to virtual machines.

How USB Device Passthrough Technology Works

The USB controller is the USB hardware chip that provides USB function to the USB ports that it manages. USB controller hardware and modules that support USB 3.0, 2.0, and USB 1.1 devices must exist in the virtual machine. Two USB controllers are available for each virtual machine. The controllers support multiple USB 3.0, 2.0, and 1.1 devices. The controller must be present before you can add USB devices to the virtual machine.

You can add up to 20 USB devices to a virtual machine. This is the maximum number of devices supported for simultaneous connection to one virtual machine.

NOTE If you connect to a USB device on a Mac OS X client computer, you can add only one device to the virtual machine at a time.

You can add multiple devices to a virtual machine, but only one at a time. The virtual machine retains its connection to the device while in S1 standby. USB device connections are preserved when you migrate virtual machines to another host in the datacenter.

A USB device is available to only one powered-on virtual machine at a time. When a virtual machine connects to a device, that device is no longer available to other virtual machines or to the client computer. When you disconnect the device from the virtual machine or shut the virtual machine down, the device returns to the client computer and becomes available to other virtual machines that the client computer manages.

For example, when you connect a USB mass storage device to a virtual machine, it is removed from the client computer and does not appear as a drive with a removable device. When you disconnect the device from the virtual machine, it reconnects to the client computer's operating system and is listed as a removable device.

USB 3.0 Device Limitations

USB 3.0 devices have the following requirements and limitations:

- The virtual machine that you connect the USB 3.0 device to must be configured with an xHCI controller and have a Windows 8 or later, Windows Server 2012 and later, or a Linux guest operating system with a 2.6.35 or later kernel.
- USB 3.0 devices are available only for passthrough from a client computer to a virtual machine. They are not available for passthrough from an ESXi host to a virtual machine.

Avoiding Data Loss

Before you connect a device to a virtual machine, make sure the device is not in use on the client computer.

If the vSphere Web Client disconnects from the vCenter Server or host, or if you restart or shut down the client computer, the device connection breaks. It is best to have a dedicated client computer for USB device use or to reserve USB devices connected to a client computer for short-term use, such as updating software or adding patches to virtual machines. To maintain USB device connections to a virtual machine for an extended time, use USB passthrough from an ESXi host to the virtual machine.

Connecting USB Devices to a Client Computer

You can connect and chain any multiple low, full, and high- or super-speed USB hubs and devices to a client computer. Careful planning and knowledge of hub behavior and limitations can help ensure that your devices work optimally.

USB physical bus topology defines how USB devices connect to the client computer. Support for USB device passthrough to a virtual machine is available if the physical bus topology of the device on the client computer does not exceed tier seven. The first tier is the USB host controller and root hub. The last tier is the target USB device. You can cascade up to five tiers of external or internal hubs between the root hub and the target USB device. An internal USB hub attached to the root hub or built into a compound device counts as one tier.

The quality of the physical cables, hubs, devices, and power conditions can affect USB device performance. To ensure the best results, keep the client computer USB bus topology as simple as possible for the target USB device, and use caution when you deploy new hubs and cables into the topology. The following conditions can affect USB behavior:

- Connecting or chaining multiple external USB hubs increases device enumeration and response time, which can make the power support to the connected USB devices uncertain.
- Chaining hubs together increases the chance of port and hub error, which can cause the device to lose connection to a virtual machine.

- Certain hubs can cause USB device connections to be unreliable, so use care when you add a new hub to an existing setup. Connecting certain USB devices directly to the client computer rather than to a hub or extension cable might resolve their connection or performance issues. In some cases, you must remove and reattach the device and hub to restore the device to a working state.

USB Compound Devices

For compound devices, the virtualization process filters out the USB hub so that it is not visible to the virtual machine. The remaining USB devices in the compound appear to the virtual machine as separate devices. You can add each device to the same virtual machine or to different virtual machines if they run on the same host.

For example, the Aladdin HASP HL Drive USB dongle package contains three devices (0529:0001 HASP dongle, 13fe:1a00 Hub, 13fe:1d00 Kingston Drive). The virtualization process filters out the USB hub. The remaining Aladdin HASP HL Drive USB dongle devices (one Aladdin HASP dongle and one Kingston Drive) appear to the virtual machine as individual devices. You must add each device separately to make it accessible to the virtual machine.

Connect USB Devices to a Client Computer

You can connect multiple USB devices to a client computer so that virtual machines can access the devices. The number of devices that you can add depends on several factors, such as how the devices and hubs chain together and the device type.

The number of ports on each client computer depends on the physical setup of the client. When you calculate the depth of hub chaining, remember that on a typical server the front ports connect to an internal hub.

The USB arbitrator can monitor a maximum of 15 USB controllers. If your system includes controllers that exceed the 15 controller limit and you connect USB devices to them, the devices are not available to the virtual machine.

Prerequisites

Verify that you know the requirements for configuring USB devices from a remote computer to a virtual machine.

Procedure

◆ To add a USB device to a client computer, connect the device to an available port or hub.

The USB device appears in the virtual machine toolbar menu.

What to do next

You can now add the USB device to the virtual machine.

Add a USB Controller to a Virtual Machine

USB controllers are available to add to virtual machines to support USB passthrough from an ESXi host or from a client computer to a virtual machine.

You can add one virtual xHCI controller, one virtual EHCI controller, and one virtual UHCI controller per virtual machine. With Hardware Version 11, the supported number of root hub ports per xHCI controller is eight (four logical USB 3.0 ports and four logical USB 2.0 ports).

The conditions for adding a controller vary, depending on the device version, the type of passthrough (host or client computer), and the guest operating system.

Table 6-9. USB Controller Support

Controller type	Supported USB Device Version	Supported for Passthrough from ESXi Host to VM	Supported for Passthrough from Client Computer to VM
EHCI+UHCI	2.0 and 1.1	Yes	Yes
xHCI	3.0, 2.0, and 1.1	Yes (USB 3.0, 2.0, and 1.1 devices only)	Yes (Linux, Windows 8 and later, and Windows Server 2012 and later guests)

For Mac OS X systems, the EHCI+UHCI controller is enabled by default and is required for USB mouse and keyboard access.

For virtual machines with Linux guests, you can add one or both controllers, but 3.0 superspeed devices are not supported for passthrough from an ESXi host to a virtual machine. You cannot add two controllers of the same type.

For USB passthrough from an ESXi host to a virtual machine, the USB arbitrator can monitor a maximum of 15 USB controllers. If your system includes controllers that exceed the 15 controller limit and you connect USB devices to them, the devices are not available to the virtual machine.

Prerequisites

- ESXi hosts must have USB controller hardware and modules that support USB 3.0, 2.0, and 1.1 devices present.
- Client computers must have USB controller hardware and modules that support USB 3.0, 2.0, and 1.1 devices present.
- To use the xHCI controller on a Linux guest, ensure that the Linux kernel version is 2.6.35 or later.
- Verify that the virtual machine is powered on.
- Required Privilege (ESXi host passthrough): **Virtual Machine.Configuration.Add or Remove Device**

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the Virtual Hardware tab, select **USB Controller** from the **New device** drop-down menu, and click **Add** .

   The new USB controller appears at the bottom of the Virtual Hardware device list.

3 Expand **New USB Controller** to change the USB controller type.

   If compatibility errors appear, fix them before you can add the controller.

4 Click **OK**.

What to do next

Add one or more USB devices to the virtual machine.

Add USB Devices From a Client Computer to a Virtual Machine in the vSphere Web Client

You can add one or more USB passthrough devices from a client computer to a virtual machine on the virtual machine **Summary** page in the vSphere Web Client. The devices must be connected to a client computer that connects to the ESXi host on which the virtual machine resides.

NOTE If you connect to a USB device on a Mac OS X client computer, you can add only one device to the virtual machine at a time.

The devices maintain their virtual machine connections in S1 standby, if the vSphere Web Client is running and connected. After you add the USB device to the virtual machine, an information message appears on the client computer stating that the device is disconnected. The device remains disconnected from the client computer until the virtual machine releases it.

FT is not supported with USB passthrough from a client computer to a virtual machine.

Prerequisites

- Verify that the Client Integration Plug-in is installed.
- Verify that a USB Controller is present.
- Verify that the vSphere Web Client has access to the ESXi host on which the virtual machines are running.
- Required Privilege: **Virtual machine.Configuration.Add or remove device**

Procedure

1. Navigate to a datacenter, folder, cluster, resource pool, host, or vApp, and click the **Related Options** tab and click **Virtual Machines**.
2. Select a virtual machine, click it again, and click the **Summary** tab.
3. Click the USB icon to the right of **USB Devices** under **VM Hardware** and select an available device from the drop-down menu.

   A **Connecting** label and a spinner appear, which indicates that a connection is in progress. When the device has successfully connected and the Summary tab refreshes, the device is connected and the device name appears next to USB Devices.

Remove USB Devices That Are Connected Through a Client Computer in the vSphere Web Client

You can remove USB devices from a virtual machine if the devices are no longer needed. When you disconnect a USB device from a virtual machine, the device is released from the virtual machine and is given back to the client computer, which starts using it.

Prerequisites

- To minimize the risk of data loss, follow the instructions to safely unmount or eject hardware for your operating system. Safely removing hardware allows accumulated data to be transmitted to a file. Windows operating systems typically include a Remove Hardware icon located in the System Tray. Linux operating systems use the `umount` command.

  NOTE You might need to use the `sync` command instead of or in addition to the `umount` command, for example after you run a `dd` command on Linux or other UNIX operating systems.

- Required Privilege: **Virtual machine.Configuration.Add or remove device**

Procedure

1. Unmount or eject the USB device from the guest operating system.
2. On the virtual machine **Summary** tab, click the disconnect icon on the right side of the USB device entry.
3. Select a device to disconnect from the drop-down menu.

   A **Disconnecting** label and a spinner appear, indicating that a disconnection is in progress. When the device is disconnected, after a slight delay, the **Summary** tab refreshes and the device is removed from the virtual machine configuration.

The device reconnects to the client computer and is available to add to another virtual machine. In some cases, Windows Explorer detects the device and opens a dialog box on the client computer. You can close this dialog box.

Remove a USB Controller from a Virtual Machine in the vSphere Web Client

You can remove a USB controller from the virtual machine if you do not want to connect to USB devices.

Prerequisites

- Verify that all USB devices are disconnected from the virtual machine.
- Required Privilege: **Virtual Machine.Configuration.Add or Remove Device**

Procedure

1. Navigate to a datacenter, folder, cluster, resource pool, host, or vApp, and click the **Related Options** tab and click **Virtual Machines**.
2. Select a virtual machine, click it again, and click the **Summary** tab.
3. Select **Virtual Hardware** and expand the **USB controller** menu.
4. Click **Remove**.
5. Click **OK** to save your changes and close the dialog box.

The controller is no longer connected to the virtual machine, but remains available to add at a later time.

Remove USB Devices from a Client Computer

You can remove USB devices from a client computer if you do not want those devices to be available to virtual machines.

When you detach a USB device from the remote client, the device disconnects from the virtual machine. Ensure that data transfer is not taking place before you remove the device.

Prerequisites

Verify that the devices are not in use.

Procedure

- To minimize the risk of data loss, follow the instructions to safely unmount or eject hardware for your operating system. Safely removing hardware allows accumulated data to be transmitted to a file. Windows operating systems typically include a Remove Hardware icon located in the System Tray. Linux operating systems use the **`umount`** command.

  You might need to use the `sync` command instead of or in addition to the `umount` command, for example after you issue a `dd` command on Linux or other UNIX operating systems.

  When you remove the device from the client computer, it is no longer available to virtual machines.

Add a Shared Smart Card Reader to Virtual Machines

You can configure multiple virtual machines to use a virtual shared smart card reader for smart card authentication. The smart card reader must be connected to a client computer on which the vSphere Web Client runs. All smart card readers are treated as USB devices.

A license is required for the shared smart card feature. See *vCenter Server and Host Management*.

When you log out of Windows XP guest operating systems, to log back in, you must remove the smart card from the smart card reader and re-add it. You can also disconnect the shared smart card reader and reconnect it.

If the vSphere Web Client disconnects from the vCenter Server or host, or if the client computer is restarted or shut down, the smart card connection breaks. For this reason, it is best to have a dedicated client computer for smart card use.

To connect a USB smart card reader that is not shared, see "USB Configuration from a Client Computer to a Virtual Machine," on page 147.

Prerequisites

- Verify that the smart card reader is connected to the client computer.
- Verify that the virtual machine is powered on.
- Verify that a USB controller is present.
- Required Privilege: **Virtual machine.Configuration.Add or remove device**

Procedure

1. Navigate to a datacenter, folder, cluster, resource pool, host, or vApp, and click the **Related Options** tab and click **Virtual Machines**.
2. Select a virtual machine, click it again, and click the **Summary** tab.
3. Click the USB icon on the right side of **USB Devices** under **VM Hardware**, and select an available shared smart card reader from the drop down menu.

   Select a device that appears as **Shared** ***the model name of your smart card reader*** followed by a number.

   A **Connecting** label and a spinner appear showing that a connection is in progress. When the device has successfully connected and the Summary tab refreshes, the device is connected and the device name appears next to **USB Devices**.

You can now use smart card authentication to log in to virtual machines in the vSphere Web Client inventory.

Configuring Virtual Machine Options 7

You can set or change virtual machine options to run VMware Tools scripts, control user access to the remote console, configure startup behavior, and more. The virtual machine options define a range of virtual machine properties, such as the virtual machine name and the virtual machine behavior with the guest operating system and VMware Tools.

This chapter includes the following topics:

- "Virtual Machine Option Overview," on page 155
- "Change the Virtual Machine Name," on page 156
- "View the Virtual Machine Configuration and Working File Location," on page 157
- "Change the Configured Guest Operating System," on page 157
- "Configuring User Mappings on Guest Operating Systems," on page 157
- "Change the Virtual Machine Console Options for Remote Users," on page 159
- "Configure the Virtual Machine Power States," on page 159
- "Configure Virtual Machines to Automatically Upgrade VMware Tools," on page 160
- "Manage Power Management Settings for a Virtual Machine," on page 161
- "Delay the Boot Sequence," on page 162
- "Disable Virtual Machine Acceleration," on page 162
- "Enable Virtual Machine Logging," on page 162
- "Configure Virtual Machine Debugging and Statistics," on page 163
- "Change the Swap File Location," on page 163
- "Edit Configuration File Parameters," on page 164
- "Configure Fibre Channel NPIV Settings," on page 164

Virtual Machine Option Overview

You can view or change virtual machine settings from the vSphere Web Client. Not all options are available to every virtual machine and some options rarely need to change from their defaults.

The host that the virtual machine runs on and the guest operating system must support any configurations that you make.

When you select **Edit Settings** from a virtual machine right-button menu and click **VM Options**, you can select one of the following options.

Table 7-1. Virtual Machine Options

Options	Description
General Options	Virtual machine name and location of the virtual machine configuration file and virtual machine working location. View or change the type and version of the guest operating system.
VMware Remote Console Options	Locking behavior and settings for simultaneous connections,
VMware Tools	Power Controls behavior, VMware Tools scripts, automatic upgrades, and time synchronization between the guest and host.
Power Management	Virtual machine Suspend behavior and wake on LAN.
Boot Options	Virtual machine boot options. Add a delay before booting, force entry into the BIOS or EFI setup screen, or set reboot options.
Advanced	Advanced virtual machine options. See the table below.
Fibre Channel NPIV	Virtual node and port World Wide Names (WWNs).

When you select **Edit Settings** from a virtual machine right-button menu, click **VM Options**, and click **Advanced**, you can select one of the following options.

Table 7-2. Advanced Virtual Machine Options

Advanced Options	Description
Settings	Specify acceleration and logging settings.
Debugging and statistic	Specify the level of debugging information that is being collected.
Swap file location	Specify the swap file location.
Configuration Parameters	View, modify, or add configuration parameters.
Latency Sensitivity	Set a value for latency sensitivity.

Change the Virtual Machine Name

If you move a virtual machine to a different datastore folder or move the virtual machine to a host that has an existing virtual machine of the same name, you can change the virtual machine's name to keep it unique. When you change the name of a virtual machine, you change the name used to identify the virtual machine in the vCenter Server inventory. This action does not change the name used as the computer name by the guest operating system.

The virtual machine name also determines the name of the virtual machine files and folder on the disk. For example, if you name the virtual machine win8, the virtual machine files are named win8.vmx, win8.vmdk, win8.nvram, and so on. If you change the virtual machine name, the names of the files on the datastore do not change.

Note Migration with Storage vMotion changes the virtual machine file names on the destination datastore to match the inventory name of the virtual machine. The migration renames all virtual disk, configuration, snapshot, and .nvram files. If the new names exceed the maximum filename length, the migration does not succeed.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 Click the **VM Options** tab and expand **General Options**.

3 Delete the existing name and type a new name for the virtual machine in the **VM Name** text box.

4 Click **OK**.

View the Virtual Machine Configuration and Working File Location

You can view the location of the virtual machine configuration and working files. You can use this information when you configure backup systems.

Prerequisites

Verify that the virtual machine is powered off.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 Click **VM Options** tab and expand **General Options**.

The path to the location of the virtual machine configuration file appears in the **VM Config File** text box. The path to the virtual machine working location appears in the **VM Working Location** text box.

Change the Configured Guest Operating System

When you change the guest operating system type in the virtual machine settings, you change the setting for the guest operating system in the virtual machine's configuration file. To change the guest operating system itself, you must install the new operating system in the virtual machine.

You might change the guest operating system, for example, if you are upgrading the guest operating system installed in the virtual machine.

When you set the guest operating system type for a new virtual machine, vCenter Server chooses configuration defaults based on the guest type. Changing the guest operating system type after the virtual machine is created does not retroactively change those settings. It affects the recommendations and setting ranges offered after the change.

Prerequisites

Power off the virtual machine.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 Click the **VM Options** tab and expand **General Options**.

3 Select the guest operating system family from the **Guest OS** drop-down menu.

4 Select the guest operating system version.

5 If you select **Other** for the guest operating system family and **Other (32-bit)** or **Other (64-bit)** for the version, type a name for the operating system in the text box.

6 Click **OK**.

Configuring User Mappings on Guest Operating Systems

As a vSphere administrator, you can enable guest OS access on certain SSO accounts.

Enabling SSO accounts to login to guest OS provides users with additional capabilities to perform administrative tasks on guest virtual machines, such as, installing or upgrading the VMware Tools or configuring apps.

Functionality to allow vSphere administrators to configure a guest operating system to use vgauth authentication. The vSphere administrator will need to know the guest administrator password for the enrollment process.

In order to enroll SSO users to guest user account, you should enroll SSO users to accounts in guest operating systems. The enrollment process will map a vSphere user to a particular account in the guest through the use of SSO certificates. Subsequent guest management requests can then use a SSO SAML token to log into the guest

You should configure VMs to accept X.509 certificates so that vSphere administrators in your data center can use SAM tokens issued by single sign-on service to access guest OSs.

View Existing SSO User Mappings

You can view the existing guest user mappings for guest operating systems on the selected virtual machine. You need to authenticate your credentials to view guest mappings.

Procedure

1 Select the virtual machine where you want to view the list of user mappings.

2 Click **Manage** > **Settings** > **Guest User Mappings**.

3 Specify your user name and password.

4 Click **OK**.

The existing in-guest user mappings are displayed.

Add SSO users to Guest Operating Systems

You can map a new SSO user to a guest user account by creating a new user map. Mapping can be established for any type of SSO users, such as solution as well as regular users.

Prerequisites

Power on the virtual machine.

Procedure

1 In the View Guest User Mappings window, click **Add new user mappings**.

2 Select the SSO user from the list that you want to map.

3 Specify a guest OS user name.

4 Click **OK**.

The SSO user is mapped to a guest user account. A new guest user account is added to the list of Guest User Mappings.

Remove SSO Users from Guest Operating Systems

You can remove an existing SSO account from guest user mappings.

Prerequisites

Power on your virtual machine.

Procedure

1 In the View Guest User Mappings window, select the SSO user from the list that you want to remove.

2 Click remove user mappings.

3 Click **Yes** to confirm.

The mapping between the selected SSO user account and guest OS account has been removed.

Change the Virtual Machine Console Options for Remote Users

To control access to the virtual machine, you can limit the number of simultaneous connections to a virtual machine and lock the guest operating system when the last remote user disconnects from the virtual machine console.

Prerequisites

- Verify that VMware Tools is installed and running.
- To use the **Guest OS lock** option, verify that you have a Windows XP or later guest operating system.

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Click the **VM Options** tab, and expand **VMware Remote Console Options**.
3. (Optional) Select **Guest OS lock** to lock the guest operating system when the last remote user disconnects.
4. (Optional) Select **Maximum number of sessions** to limit the number of simultaneous connections to this virtual machine, and enter a number.
5. Click **OK**.

Configure the Virtual Machine Power States

Changing virtual machine power states is useful when you do maintenance on the host. You can use the system default settings for the virtual machine power controls, or you can configure the controls to interact with the guest operating system. For example, you can configure the **Power off** control to power off the virtual machine or shut down the guest operating system.

You can modify many virtual machine configurations while the virtual machine is running, but you might need to change the virtual machine power state for some configurations.

You cannot configure A **Power on ( )** action. This action powers on a virtual machine when a virtual machine is stopped, or resumes the virtual machine and runs a script when it is suspended and VMware Tools is installed and available. If VMware Tools is not installed, it resumes the virtual machine and does not run a script.

Prerequisites

- Verify that you have privileges to perform the intended power operation on the virtual machine.
- To set optional power functions, install VMware Tools in the virtual machine.
- Power off the virtual machine before editing the VMware Tools options.

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Click the **VM Options** tab and expand **VMware Tools**.

3 Select an option for the virtual machine **Power Off** ( ) control from the drop-down menu.

Option	Description
Shut Down Guest	Uses VMware Tools to initiate an orderly system shut down of the virtual machine. Soft power operations are possible only if the tools are installed in the guest operating system.
Power Off	Immediately stops the virtual machine. A Power Off action shuts down the guest operating system or powers off the virtual machine. A message indicates that the guest operating system might not shut down properly. Use this power off option only when necessary.
Default	Follows system settings. The current value of the system settings appears in parentheses.

4 Select an option for the **Suspend (** **)** control from the drop-down menu.

Option	Description
Suspend	Pauses all virtual machine activity. When VMware Tools is installed and available, a suspend action runs a script and suspends the virtual machine. If VMware Tools is not installed, a Suspend action suspends the virtual machine without running a script.
System Default	Follows system settings. The current value of the system setting appears in parentheses.

5 Select an option for the **Reset (** **)** control from the drop-down menu.

Option	Description
Restart Guest	Uses VMware Tools to initiate an orderly restart. Soft power operations are possible only if the tools are installed in the guest operating system.
Reset	Shuts down and restarts the guest operating system without powering off the virtual machine. If VMWare Tools is not installed, a Reset action resets the virtual machine.
System Default	Follows system settings. The current value of the system setting appears in parentheses.

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

Configure Virtual Machines to Automatically Upgrade VMware Tools

You can configure virtual machines to automatically update VMware Tools before you start the virtual machines. This action helps to eliminate unnecessary shut downs by taking advantage of other updates or activities that require you to restart the virtual machine.

NOTE Automatic VMware Tools upgrade is supported for virtual machines running Windows and Linux guest operating systems.

Procedure

1 Right-click the virtual machine and click **Edit Settings**.

2 Click the **Options** tab and select **VMware Tools**.

3 Select **Check and upgrade Tools during power cycling** in the **Advanced** pane.

4 Click **OK** to save your changes and close the dialog box.

5 Click the **Options** tab and select **VMware Tools**.

6 Select **Check and upgrade Tools during power cycling** in the **Advanced** pane.

7 Click **OK** to save your changes and close the dialog box.

8 Select **Check and upgrade Tools during power cycling** in the **Advanced** pane.

9 Click **OK** to save your changes and close the dialog box.

The next time the virtual machine is powered on, it checks the ESX/ESXi host for a newer version of VMware Tools. If one is available, it is installed and the guest operating system is restarted (if required).

Manage Power Management Settings for a Virtual Machine

You can set the power options so that a virtual machine is suspended or remains powered on if the guest operating system is placed on standby. Some desktop-based guests, such as Windows 7, have standby enabled by default, so that the guest goes into standby after a predetermined time.

The following conditions apply:

- **Power Management** options are not available on every guest operating system.
- **Wake on LAN** supports only Windows guest operating systems and is not available on Vlance NICs or when a Flexible NIC is operating in Vlance mode. That is, the current VMware Tools are not installed on the guest operating system.
- **Wake on LAN** can resume virtual machines that are in an S1 sleep state only. It cannot resume suspended, hibernated, or powered off virtual machines.
- NICs that support **Wake on LAN** include Flexible (VMware Tools required), vmxnet, Enhanced vmxnet, and vmxnet 3.

NOTE To avoid having the guest operating system go into standby mode unintentionally, verify the settings before you deploy the virtual machine.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 Click the **VM Options** tab and expand **Power Management**.

3 Select a power option.

Option	Description
Suspend the virtual machine	Stops all processes, which saves resources, and copies the contents of the virtual machine's memory to the virtual machine's `.vmss` file. Writing the memory to the `.vmss` file is useful if you need to copy the file to help with a troubleshooting scenario.
Put the guest operating system in standby mode and leave the virtual machine powered on	All processes stop running, but virtual devices remain connected.

4 (Optional) Select **Wake on LAN for virtual machine traffic on** and select the virtual NICs to trigger this action.

Unsupported NICs might be listed, but are unavailable to connect.

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

Delay the Boot Sequence

Delaying the boot operation is useful when you change BIOS or EFI settings such as the boot order. For example, you can change the BIOS or EFI settings to force a virtual machine to boot from a CD-ROM.

Prerequisites

- Verify that vSphere Web Client is logged in to a vCenter Server.
- Verify that you have access to at least one virtual machine in the inventory.
- Verify that you have privileges to edit boot options for the virtual machine.

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Click **VM Options** tab and expand **Boot Options**.
3. Select the time in milliseconds to delay the boot operation.
4. (Optional) Select whether to force entry into the BIOS or EFI setup screen the next time the virtual machine boots.
5. (Optional) Select whether to try to reboot after a boot failure.
6. Click **OK**.

Disable Virtual Machine Acceleration

You might find that when you install or run software in a virtual machine, the virtual machine appears to stop responding. The problem occurs early in the program's execution. You can get past the problem by temporarily disabling acceleration in the virtual machine.

This setting slows down virtual machine performance, so use it only for getting past the problem with running the program. After the program stops encountering problems, deselect **Disable acceleration**. You might be able to run the program with acceleration.

You can enable and disable acceleration when the virtual machine is running.

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Click the **VM Options** tab and expand **Advanced**.
3. Click **VM Options** and expand **Advanced**.
4. Select **Disable acceleration**.
5. Click **OK**.

You should be able to install or run the software successfully.

Enable Virtual Machine Logging

You can enable logging to collect log files to help troubleshoot problems with your virtual machine.

ESXi hosts store virtual machine log files in the same directory as the virtual machine's configuration files. By default, the log file name is `vmware.log`. Archived log files are stored as `vmware-`*`n`*`.log`, where *n* is a number in sequential order beginning with 1.

Prerequisites

Required privilege: **Virtual machine.Configuration.Settings**

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 Click the **VM Options** tab and expand **Advanced**.

3 In the Settings row, select **Enable logging** and click **OK**.

You can view and compare log files in the same storage location as the virtual machine configuration files.

Configure Virtual Machine Debugging and Statistics

You can run a virtual machine so that it collects additional debugging information that is helpful to VMware technical support in resolving issues.

Prerequisites

Power off the virtual machine.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 Click the **VM Options** tab and expand **Advanced**.

3 Select a debugging and statistics option from the drop-down menu.

- **Run normally**
- **Record Debugging Information**
- **Record Statistics**
- **Record Statistics and Debugging Information**

The number of debugging and statistics options available depends on the host software type and version. On some hosts, some options are not available.

4 Click **OK**.

Change the Swap File Location

When a virtual machine is powered on, the system creates a VMkernel swap file to serve as a backing store for the virtual machine's RAM contents. You can accept the default swap file location or save the file to a different location. By default, the swap file is stored in the same location as the virtual machine's configuration file.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 Click the **VM Options** tab and expand **Advanced**.

3 Select a swap file location option.

Option	Description
Default	Stores the virtual machine swap file at the default location defined by the host or cluster swap file settings.
Always store with the virtual machine	Stores the virtual machine swap file in the same folder as the virtual machine configuration file.
Store in the host's swapfile datastore	If the host or cluster settings define a location for the swap file, this location is used. Otherwise, the swap file is stored with the virtual machine.

4 Click **OK**.

Edit Configuration File Parameters

You can change or add virtual machine configuration parameters when instructed by a VMware technical support representative, or if you see VMware documentation that instructs you to add or change a parameter to fix a problem with your system.

Important Changing or adding parameters when a system does not have problems might lead to decreased system performance and instability.

The following conditions apply:

- To change a parameter, you change the existing value for the keyword/value pair. For example, if you start with the keyword/value pair, keyword/value, and change it to keyword/value2, the result is keyword=value2.
- You cannot delete a configuration parameter entry.

Caution You must assign a value to configuration parameter keywords. If you do not assign a value, the keyword can return a value of 0, false, or disable, which can result in a virtual machine that cannot power on.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 Click the **VM Options** tab and expand **Advanced**.

3 Click **Edit Configuration**.

4 (Optional) To add a parameter, click **Add Row** and type a name and value for the parameter.

5 (Optional) To change a parameter, type a new value in the **Value** text box for that parameter.

6 Click **OK**.

Configure Fibre Channel NPIV Settings

N-port ID virtualization (NPIV) provides the ability to share a single physical Fibre Channel HBA port among multiple virtual ports, each with unique identifiers. This capability lets you control virtual machine access to LUNs on a per-virtual machine basis.

Each virtual port is identified by a pair of world wide names (WWNs): a world wide port name (WWPN) and a world wide node name (WWNN). These WWNs are assigned by vCenter Server.

For detailed information on how to configure NPIV for a virtual machine, see *vSphere Storage*.

NPIV support is subject to the following limitations:

- NPIV must be enabled on the SAN switch. Contact the switch vendor for information about enabling NPIV on their devices.
- NPIV is supported only for virtual machines with RDM disks. Virtual machines with regular virtual disks continue to use the WWNs of the host's physical HBAs.
- The physical HBAs on the ESXi host must have access to a LUN using its WWNs in order for any virtual machines on that host to have access to that LUN using their NPIV WWNs. Ensure that access is provided to both the host and the virtual machines.
- The physical HBAs on the ESXi host must support NPIV. If the physical HBAs do not support NPIV, the virtual machines running on that host will fall back to using the WWNs of the host's physical HBAs for LUN access.

- Each virtual machine can have up to 4 virtual ports. NPIV-enabled virtual machines are assigned exactly 4 NPIV-related WWNs, which are used to communicate with physical HBAs through virtual ports. Therefore, virtual machines can utilize up to 4 physical HBAs for NPIV purposes.

Prerequisites

- To edit the virtual machine's WWNs, power off the virtual machine.
- Verify that the virtual machine has a datastore containing a LUN that is available to the host.

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Click **VM Options** tab and expand **Fibre Channel NPIV**.
3. (Optional) Select the **Temporarily Disable NPIV for this virtual machine** check box.
4. Select an option for assigning WWNs.
   - To leave WWNs unchanged, select **Leave unchanged**.
   - To have vCenter Server or the ESXi host generate new WWNs, select **Generate New WWNs**.
   - To remove the current WWN assignments, select **Remove WWN assignment**.
5. Click **OK**.

Managing Multi-Tiered Applications with vSphere vApp

8

A vSphere vApp allows packaging of multiple interoperating virtual machines and software applications that you can manage as a unit and distribute in OVF format.

A vApp can contain one or more virtual machines, but any operation carried out on the vApp, such as clone or power off, affects all virtual machines in the vApp container,

From the vSphere Web Client, you can access the vApp summary page with the current status of the vApp, and you can manage the vApp.

NOTE Because the vApp metadata resides in the vCenter Server database, a vApp can be distributed across multiple ESXi hosts. This information can be lost if the vCenter Server database is cleared or if a standalone ESXi host that contains a vApp is removed from vCenter Server. Back up your vApps to an OVF package to avoid losing metadata.

vApp metadata for virtual machines within a vApp do not follow the snapshots semantics for virtual machine configuration. vApp properties that are deleted, modified, or defined after a snapshot is taken remain intact (deleted, modified, or defined) after the virtual machine reverts to that snapshot or any prior snapshots.

You can use VMware Studio to automate the creation of ready-to-deploy vApps with pre-populated application software and operating systems. VMware Studio adds a network agent to the guest so that vApps bootstrap with minimal effort. Configuration parameters that are specified for vApps appear as OVF properties in the vCenter Server deployment wizard. For information about VMware Studio and for download, see the VMware Studio developer page on the VMware Web site.

This chapter includes the following topics:

- "Create a vApp," on page 168
- "Create a Virtual Machine, Resource Pool, or Child vApp Inside a vApp," on page 169
- "Add Virtual Machine or Child vApp to a vApp," on page 169
- "Edit vApp Settings," on page 169
- "Clone a vApp," on page 174
- "Perform vApp Power Operations," on page 175
- "Edit vApp Notes," on page 176
- "Add a Network Protocol Profile," on page 176
- "Virtual Machine vApp Options," on page 180

Create a vApp

A vApp allows you to perform resource management and certain other management activities such as power operations for multiple virtual machines at the same time. You can think of the vApp as the container for the virtual machines, and you can perform the operations on the container.

When you create a vApp, you can add it to a folder, standalone host, resource pool, cluster enabled for DRS, or another vApp.

Prerequisites

Verify that one of those objects is available in your datacenter.

- A standalone host that is running ESX 4.0 or greater.
- A cluster that is enabled for DRS.

Procedure

1. Navigate to an object that supports vApp creation and select the Create New vApp icon ( ).
2. Select **Create a new vApp** and click **Next**.
3. In the **vApp Name** text box, type a name for the vApp.
4. Select the location or resource and click **Next**.
   - If you start the action from a folder or vApp, you are prompted for a host, cluster, or resource pool.
   - If you start the action from a resource pool, host, or cluster, you are prompted for a folder or data center.
5. In the Deployment section, click CPU resources to allocate CPU resources to this vApp.

Option	Description
Shares	CPU shares for this vApp with respect to the parent's total. Sibling vApps share resources according to their relative share values bounded by the reservation and limit. Select **Low**, **Normal**, or **High**, which specify share values respectively in a 1:2:4 ratio. Select **Custom** to give each vApp a specific number of shares, which express a proportional weight.
Reservation	Guaranteed CPU allocation for this vApp.
Reservation Type	Select the **Expandable** check box to make the reservation expandable. When the vApp is powered on, if the combined reservations of its virtual machines are larger than the reservation of the vApp, the vApp can use resources from its parent or ancestors.
Limit	Upper limit for this vApp's CPU allocation. Select **Unlimited** to specify no upper limit.

6. In the Deployment section, click Memory resources to allocate memory resources to this vApp.

Option	Description
Shares	Memory shares for this vApp with respect to the parent's total. Sibling vApps share resources according to their relative share values bounded by the reservation and limit. Select **Low**, **Normal**, or **High**, which specify share values respectively in a 1:2:4 ratio. Select **Custom** to give each vApp a specific number of shares, which express a proportional weight.
Reservation	Guaranteed memory allocation for this vApp.

Option	Description
Reservation Type	Select the **Expandable** check box to make the reservation expandable. When the vApp is powered on, if the combined reservations of its virtual machines are larger than the reservation of the vApp, the vApp can use resources from its parent or ancestors.
Limit	Upper limit for this vApp's memory allocation. Select **Unlimited** to specify no upper limit.

7 Click **Next**.

8 Review the vApp settings and click **Finish**.

Create a Virtual Machine, Resource Pool, or Child vApp Inside a vApp

You can create a virtual machine, resource pool, or child vApp within a vApp.

Procedure

1 Navigate to the vApp in which you want to create the object.

2 Right-click the vApp and select **All vCenter Actions**.

3 Select an action from the submenu.

You can create a virtual machine, a resource pool, or a child vApp. You can also deploy an OVF template to add the corresponding virtual machine or vApp to the selected vApp.

The new object appears as part of the vApp in the vApp inventory.

Add Virtual Machine or Child vApp to a vApp

You can add an object, such as a virtual machine or another vApp, to an existing vApp.

An existing virtual machine or another vApp that is not already contained inside the vApp can be moved into the currently selected vApp.

Procedure

1 Display the object in the inventory.

2 Click and drag the object to the target object.

If the move is not permitted, red x icon appears, and the object is not moved.

3 Release the mouse button.

Edit vApp Settings

You can edit and configure several vApp settings, including startup order, resources, and custom properties.

Procedure

1 Configure vApp Properties on page 170

If you define a property in the Authoring section of the Edit vApp Settings dialog, you can assign a value to that property when you edit the vApp settings the next time. If you deployed the vApp from an OVF, and properties were predefined in that OVF, you might be able to edit those properties as well.

2 Configure vApp CPU and Memory Resources on page 171

You can configure the CPU and memory resource allocation for the vApp.

3 View Unrecognized OVF Sections on page 172

If your vApp is based on an OVF file that was not created in the vSphere Web Client, it might include some configuration information that is not recognized by vCenter Server. You can view the information in the Edit vApp Settings dialog.

4 Configure vApp IP Allocation Policy on page 172

If your vApp is set up to allow it, and if you have the required privileges, you can edit how IP addresses are allocated for the vApp.

5 Configure vApp Startup and Shutdown Options on page 173

You can change the order in which virtual machines and nested vApps within a vApp start up and shut down. You can also specify delays and actions performed at startup and shutdown.

6 Configure vApp Product Properties on page 173

You can configure product and vendor information for a vApp.

7 View vApp License Agreement on page 174

You can view the license agreement for the vApp that you are editing.

Procedure

◆ Navigate to a vApp and click **Edit vApp Settings**.

Expand the areas of the vApp configuration that you want to edit.

Area	Description
Application Properties	Displays non-editable product informaion such as name, vendor, and version, and allows specifying values for vApp custom properties.
Deployment	Allows you to specify CPU and memory resources and configure IP allocation. The available allocation schemes and protocols depend on the vApp configuration. You can modify the configuration in the Authoring section.
Authoring	Allows you to specify the vApp product information and controls the configurable options that are available in the Deployment and Application Properties sections. You can modify the supported IP allocation schemes and protocols, set the VM start order, and add or reconfigure custom properties.

Configure vApp Properties

If you define a property in the Authoring section of the Edit vApp Settings dialog, you can assign a value to that property when you edit the vApp settings the next time. If you deployed the vApp from an OVF, and properties were predefined in that OVF, you might be able to edit those properties as well.

In the **Application properties** section you can view product information and assign values to custom properties.

- View information that was specified in the **Authoring** section's **Product** field of the current vApp or in the OVF package from which the vApp was deployed, you can view that information in the **Application properties** section.
- Assign values to a custom property that was defined in the **Authoring** section's **Properties** field of the current vApp or in an OVF from which the vApp was deployed, you can assign values to those properties.

Section 9.5 of the OVF 1.1 specification explains which product metadata can be contained in an OVF.vCenter Server supports those metadata.

Prerequisites

Required privilege: **vApp.vApp application configuration** on the vApp.

Procedure

1 Navigate to a vApp in the inventory and click **Edit vApp Settings**.

2 If application properties are predefined for your vApp, click the **Application Properties** triangle to expand the vApp properties.

3 Edit the vApp properties.

4 Click **OK**.

Configure vApp CPU and Memory Resources

You can configure the CPU and memory resource allocation for the vApp.

Reservations on vApps and all their child resource pools, child vApps, and child virtual machines count against the parent resources only if those objects are powered on.

Prerequisites

Required privilege: **vApp.vApp resource configuration** on the vApp.

Procedure

1 Navigate to a vApp in the inventory and click **Edit vApp Settings**.

2 In the Deployment section, click CPU resources to allocate CPU resources to this vApp.

Option	Description
Shares	CPU shares for this vApp with respect to the parent's total. Sibling vApps share resources according to their relative share values bounded by the reservation and limit. Select **Low**, **Normal**, or **High**, which specify share values respectively in a 1:2:4 ratio. Select **Custom** to give each vApp a specific number of shares, which express a proportional weight.
Reservation	Guaranteed CPU allocation for this vApp.
Reservation Type	Select the **Expandable** check box to make the reservation expandable. When the vApp is powered on, if the combined reservations of its virtual machines are larger than the reservation of the vApp, the vApp can use resources from its parent or ancestors.
Limit	Upper limit for this vApp's CPU allocation. Select **Unlimited** to specify no upper limit.

3 In the Deployment section, click Memory resources to allocate memory resources to this vApp.

Option	Description
Shares	Memory shares for this vApp with respect to the parent's total. Sibling vApps share resources according to their relative share values bounded by the reservation and limit. Select **Low**, **Normal**, or **High**, which specify share values respectively in a 1:2:4 ratio. Select **Custom** to give each vApp a specific number of shares, which express a proportional weight.
Reservation	Guaranteed memory allocation for this vApp.
Reservation Type	Select the **Expandable** check box to make the reservation expandable. When the vApp is powered on, if the combined reservations of its virtual machines are larger than the reservation of the vApp, the vApp can use resources from its parent or ancestors.
Limit	Upper limit for this vApp's memory allocation. Select **Unlimited** to specify no upper limit.

4 Click **OK**.

View Unrecognized OVF Sections

If your vApp is based on an OVF file that was not created in the vSphere Web Client, it might include some configuration information that is not recognized by vCenter Server. You can view the information in the Edit vApp Settings dialog.

Procedure

1 Navigate to a vApp in the inventory and click **Edit vApp Settings**.

2 Click **Unrecognized OVF Sections** in the Deployment section.

3 Click **OK**.

Configure vApp IP Allocation Policy

If your vApp is set up to allow it, and if you have the required privileges, you can edit how IP addresses are allocated for the vApp.

By default, you cannot edit the IP application policy in the Deployment section when you create a vApp in the vSphere Web Client. Change the **IP allocation scheme** to the protocol of your choice before you configure the IP allocation policy. If deployed an OVF template to create the vApp, IP allocation policy might be editable.

Prerequisites

Required privilege: **vApp.vApp instance configuration**

Procedure

1 Navigate to a vApp in the inventory and click **Edit vApp Settings**.

2 Click the **IP Allocation** triangle to expand the IP allocation options.

3 Select an IP allocation option.

Option	Description
Static - Manual	IP addresses are manually configured. No automatic allocation is performed.
Transient - IP Pool	IP addresses are automatically allocated using IP pools from a specified range when the vApp is powered on. The IP addresses are released when the appliance is powered off.
DHCP	A DHCP server is used to allocate the IP addresses. The addresses assigned by the DHCP server are visible in the OVF environments of virtual machines started in the vApp.
Static - IP Pool	IP addresses are automatically allocated from the managed IP network range of vCenter Server at power-on, and remain allocated at power-off.

Static - IP Pool and Transient - IP Pool have in common that IP allocation is done through the range managed by the vSphere platform as specified by the IP pool range in a network protocol profile. The difference is that for a static IP Pool, the IP addresses are allocated at first power-on and remain allocated, while for a transient IP Pool, the IP addresses are allocated when needed, typically at power-on, but released during power-off.

4 Click **OK**.

Configure vApp Startup and Shutdown Options

You can change the order in which virtual machines and nested vApps within a vApp start up and shut down. You can also specify delays and actions performed at startup and shutdown.

Prerequisites

Required privilege: **vApp.vApp application configuration** on the vApp.

Procedure

1 Navigate to a vApp in the inventory and click **Edit vApp Settings**.

2 Click the **Start Order** triangle to expand the start order options.

3 Select a virtual machine and click the up or down arrow to move the virtual machine in the startup order; the reverse order is used for shutdown.

   Virtual machines and vApps in the same group are started before the objects in the next group.

4 (Optional) For each virtual machine, select the startup action for the virtual machine.

   The default is **Power On**. Select **None** to power on the virtual machine manually.

5 (Optional) Specify when the startup action is to happen

   - Enter a time delay in seconds for the startup action.
   - Select **VMware Tools are ready** to perform the startup action when VMware Tools has started.

6 (Optional) For each virtual machine, select the shutdown action for the virtual machine.

   The default is **Power Off**. You can also select Guest Shutdown to shut down the guest and leave the virtual machine running, **Suspend**, or **None**.

7 (Optional) Enter a time delay in seconds for the shutdown action.

8 Click **OK**.

Configure vApp Product Properties

You can configure product and vendor information for a vApp.

Prerequisites

Required privilege: **vApp.vApp application configuration** on the vApp.

Procedure

1 Navigate to a vApp in the inventory and click **Edit vApp Settings**.

2 In the Authoring section, click the **Product** triangle to expand the product options.

3 Set and configure the settings that appear on the summary page of the virtual machine.

vApp Setting	Description
Product Name	Product Name.
Version	vApp version.
Full Version	Full version of the vApp.
Product URL	If you enter a product URL, a user can click the product name on the virtual machine summary page and go to the product's web page.

vApp Setting	Description
Vendor URL	If you enter a vendor URL, a user can click the vendor name on the virtual machine summary page and go to the vendor's web page.
Application URL	The vApp Summary page you can view in the vSphere Client includes a Status pane that includes information about vApp status, for example **Running** or **Stopped**. If you enter a valid application URL, the virtual machine Status pane displays **Available** instead of Running. The **Available** text is also a link to the application URL.

if you configure the virtual machine to use the property called *webserver_ip* and the virtual machine has a web server at the address represented by the property, you can enter `http://${webserver_ip}/` as the **Application URL**.

4 (Optional) Click **View** to test the **Product URL** and **Vendor URL**.

5 Click **OK**.

View vApp License Agreement

You can view the license agreement for the vApp that you are editing.

NOTE This option is available only if the vApp was imported from an OVF that includes a license agreement.

Prerequisites

Required privilege: **vApp.vApp application configuration** on the vApp.

Procedure

1 On the Summary page of the vApp, click **Edit Settings**.

2 Click **View License Agreement** in the Options list.

3 Click **OK**.

Clone a vApp

Cloning a vApp is similar to cloning a virtual machine. When you clone a vApp, you clone all virtual machines and vApps in the vApp.

Prerequisites

When you clone a vApp, you can add the clone to a folder, standalone host, resource pool, cluster enabled for DRS, or another vApp.

Verify that one of those objects is available in your datacenter.

- A standalone host that is running ESX 3.0 or greater.
- A cluster enabled for DRS is selected.

Procedure

1 Navigate to a DRS-enabled cluster and click the **Create a new vApp** icon ( ).

2 Select **Clone an existing vApp**.

3 Expand the inventory, select an existing vApp to clone, and click **Next**.

4 Select a valid host, vApp, or resource pool in which to run the vApp, and click **Next**

5 In the **vApp Name** text box, type a name for the vApp.

6 Select the datacenter or folder in which to deploy the vApp and click **Next**.

7 Select the virtual disk format and the target datastore and click **Next**.

8 Select the network for the cloned vApp and click **Next**.

9 Review the vApp settings and click **Finish**.

Perform vApp Power Operations

One of the advantages of a vApp is that you can perform power operations on all virtual machines it contains at the same time.

Power on a vApp

You can power on a vApp to power on all its virtual machines and child vApps. Virtual machines are powered on according to the startup order configuration.

When powering on a vApp within a DRS cluster in manual mode, no DRS recommendations are generated for virtual machine placements. The power-on operation performs as if DRS is run in a semiautomatic or automatic mode for the initial placements of the virtual machines. This does not affect vMotion recommendations. Recommendations for individual powering on and powering off of virtual machines are also generated for vApps that are running.

Prerequisites

Required privilege: **vApp.Power On** on the vApp.

Procedure

1 Navigate to the vApp you want to power on.

2 Right-click the vApp and select **Power On**.

If a delay is set in the startup settings of a virtual machine in the vApp, the vApp waits for the set length of time before powering on that virtual machine.

In the **Summary** tab, the **Status** indicates when the vApp has started and is available.

Power Off a vApp

You can power off a vApp to power off all its virtual machines and child vApps. Virtual machines are powered off in reverse startup order.

Prerequisites

Required privilege: **vApp.Power Off** on the vApp.

Procedure

1 Navigate to the vApp you want to power off.

2 Right-click the vApp and select **Power Off**.

If a delay is set in the shutdown settings of a virtual machine in the vApp, the vApp waits for the set length of time before powering off that virtual machine.

Suspend a vApp

You can suspend a vApp to suspend all its virtual machines and child vApps. Virtual machines are suspended in the reverse order of the specified startup order.

All virtual machines are suspended regardless of the Suspend behavior you specified in the Power Management VM Option for the virtual machine.

Prerequisites

Required privilege: **vApp.Suspend** on the vApp.

Procedure

1 Navigate to the vApp you want to suspend.

2 Right-click the vApp and select **Suspend**.

Resume a vApp

You can resume a vApp to resume all its virtual machines and child vApps. Virtual machines are resumed according to their startup order configuration.

Procedure

1 Navigate to the vApp you want to resume.

2 Right-click the virtual machine and select **Power On**.

Edit vApp Notes

You can add or edit notes for a particular vApp.

Procedure

1 Select the vApp in the inventory.

2 Select **All Actions > Edit Notes**.

3 Type your comments in the Edit Notes window.

4 Click **OK**.

Your comments appear in the Summary tab for the vApp.

Add a Network Protocol Profile

A network protocol profile contains a pool of IPv4 and IPv6 addresses. vCenter Server assigns those resources to vApps or to virtual machines with vApp functionality that are connected to port groups associated with the profile.

Network protocol profiles also contain settings for the IP subnet, DNS, and HTTP proxy server.

Note If you move a vApp or a virtual machine that retrieves its network settings from a protocol profile to another data center, to power on the vApp or virtual machine you must assign a protocol profile to the connected port group on the destination data center.

Procedure

1 Select the Network Protocol Profile Name and Network on page 177

Name the network protocol profile and select the network that should use it.

2 Specify Network Protocol Profile IPv4 Configuration on page 177

   A network protocol profile contains a pool of IPv4 and IPv6 addresses for use by vApps. When you create a network protocol profile, you set up its IPv4 configuration.

3 Specify Network Protocol Profile IPv6 Configuration on page 178

   A network protocol profile contains a pool of IPv4 and IPv6 addresses for use by vApps. When you create a network protocol profile, you set up its IPv6 configuration.

4 Specify Network Protocol Profile DNS and Other Configuration on page 178

   When you create a network protocol profile, you can specify the DNS domain, DNS search path, a host prefix, and HTTP proxy.

5 Complete the Network Protocol Profile Creation on page 179

6 Associate a Port Group with a Network Protocol Profile on page 179

   To apply the range of IP addresses from a network protocol profile to a virtual machine that is a part of a vApp or has vApp functionality enabled, associate the profile with a port group that controls the networking of the virtual machine.

7 Configure a Virtual Machine or vApp to Use a Network Protocol Profile on page 179

   After you associate a protocol profile to a port group of a standard switch or a distributed switch, enable the usage of profile on a virtual machine that is connected to the port group and is associated with a vApp or has the vApp options enabled.

Procedure

1 Navigate to a data center that is associated with the vApp and click the **Manage** tab.

2 Click **Network Protocol Profiles**

   Existing network protocol profiles are listed.

3 Click the Add icon (+) to add a new network protocol profile.

Select the Network Protocol Profile Name and Network

Name the network protocol profile and select the network that should use it.

Procedure

1 Type the name of the network protocol profile.

2 Select the networks that use this network protocol profile.

   A network can be associated with one network protocol profile at a time.

3 Click **Next**.

Specify Network Protocol Profile IPv4 Configuration

A network protocol profile contains a pool of IPv4 and IPv6 addresses for use by vApps. When you create a network protocol profile, you set up its IPv4 configuration.

You can configure network protocol profile ranges for IPv4, IPv6, or both. vCenter Server uses these ranges to dynamically allocate IP addresses to virtual machines when a vApp is set up to use transient IP allocation.

Procedure

1 Enter the **IP Subnet** and **Gateway** in their respective fields.

2 Select **DHCP Present** to indicate that the DHCP server is available on this network.

3 Enter the DNS server information.

   Specify the servers by IP addresses separated by a comma, semicolon, or space.

4 Select the **Enable IP Pool** check box to specify an IP pool range.

5 If you enable IP Pools, enter a comma-separated list of host address ranges in the **IP pool range** field.

   A range consists of an IP address, a pound sign (#), and a number indicating the length of the range.

   The gateway and the ranges must be within the subnet. The ranges that you enter in the **IP pool range** field cannot include the gateway address.

   For example, `10.20.60.4#10, 10.20.61.0#2` indicates that the IPv4 addresses can range from 10.20.60.4 to 10.20.60.13 and 10.20.61.0 to 10.20.61.1.

6 Click **Next**.

Specify Network Protocol Profile IPv6 Configuration

A network protocol profile contains a pool of IPv4 and IPv6 addresses for use by vApps. When you create a network protocol profile, you set up its IPv6 configuration.

You can configure network protocol profile ranges for IPv4, IPv6, or both.vCenter Server uses these ranges to dynamically allocate IP addresses to virtual machines when a vApp is set up to use transient IP allocation.

Procedure

1 Enter the **IP Subnet** and **Gateway** in their respective fields.

2 Select **DHCP Present** to indicate that the DHCP server is available on this network.

3 Enter the DNS server information.

   Specify the servers by IP addresses separated by a comma, semicolon, or space.

4 Select the **Enable IP Pool** check box to specify an IP pool range.

5 If you enable IP Pools, enter a comma-separated list of host address ranges in the **IP pool range** field.

   A range consists of an IP address, a pound sign (#), and a number indicating the length of the range. For example. assume that you specify the following IP pool range:

   fe80:0:0:0:2bff:fe59:5a:2b#10,fe80:0:0:0:2bff:fe59:5f:b1#2

   Then the addresses are in this range:

   fe80:0:0:0:2bff:fe59:5a:2b - fe80:0:0:0:2bff:fe59:5a:34

   and

   fe80:0:0:0:2bff:fe59:5f:b1 - fe80:0:0:0:2bff:fe59:5f:b2

   The gateway and the ranges must be within the subnet. The ranges that you enter in the **IP pool range** field cannot include the gateway address.

6 Click **Next**.

Specify Network Protocol Profile DNS and Other Configuration

When you create a network protocol profile, you can specify the DNS domain, DNS search path, a host prefix, and HTTP proxy.

Procedure

1 Enter the DNS domain.

2 Enter the host prefix.

3 Enter the DNS search path.

   The search paths are specified as a list of DNS domains separated by commas, semi-colons, or spaces.

4 Enter the server name and port number for the proxy server.

   The server name can optionally include a colon and a port number.

   For example, `web-proxy:3912` is a valid proxy server.

5 Click **Next**.

Complete the Network Protocol Profile Creation

Procedure

- Review the settings and click **Finish** to complete adding the network protocol profile.

Associate a Port Group with a Network Protocol Profile

To apply the range of IP addresses from a network protocol profile to a virtual machine that is a part of a vApp or has vApp functionality enabled, associate the profile with a port group that controls the networking of the virtual machine.

You can associate a port group of a standard switch or a distributed port group of a distributed switch with a network protocol profile by using the settings of the group.

Procedure

1 Navigate to a distributed port group of a vSphere Distributed Switch or to a port group of a vSphere Standard Switch in the Networking view of the vSphere Web Client.

   The port groups of standard switches are under the data center. The vSphere Web Client displays distributed port groups under the parent distributed switch object.

2 On the **Manage** tab, click **Network Protocol Profiles**.

3 Click **Associate a network protocol profile with the selected network**.

4 On the Set association type page of the Associate Network Protocol Profile wizard, select **Use an existing network protocol profile** and click **Next**.

   If the existing network protocol profiles do not contain settings suitable for the vApp virtual machines in the port group, you must create a new profile.

5 Select the network protocol profile and click **Next**.

6 Examine the association and settings of the network protocol profile, and click **Finish**.

Configure a Virtual Machine or vApp to Use a Network Protocol Profile

After you associate a protocol profile to a port group of a standard switch or a distributed switch, enable the usage of profile on a virtual machine that is connected to the port group and is associated with a vApp or has the vApp options enabled.

Prerequisites

Verify that the virtual machine is connected to a port group that is associated with the network protocol profile.

Procedure

1 In the vSphere Web Client, navigate to the virtual machine or the vApp.

2 Open the settings of the vApp or the **vApp Options** tab of the virtual machine.
   - Right-click a vApp and select **Edit settings**.
   - Right-click a virtual machine, select **Edit settings**, and in the Edit Settings dialog box, click the **vApp Options** tab.
3 Click **Enable vApp options**.
4 Under Authoring, expand **IP allocation** and set the IP allocation scheme to **OVF environment**.
5 Under Deployment, expand **IP allocation** and set **IP allocation** to **Transient - IP Pool** or **Static - IP Pool**.

   Both the **Static - IP Pool** and **Transient - IP Pool** options allocate an IP address from the range in the network protocol profile that is associated with the port group. If you select **Static - IP Pool**, the IP address is assigned the first time the virtual machine or vApp is powered on and the address persists across restarts. If you select **Transient - IP Pool**, an IP address is assigned every time the virtual machine or vApp is powered on.
6 Click **OK**.

When the virtual machine is powered on, the adapters connected to the port group receive IP addresses from the range in the protocol profile. When the virtual machine is powered off, the IP addresses are released.

Virtual Machine vApp Options

When you edit the settings for a virtual machine, you can enable vApp options. When vApp options are enabled, you can configure OVF properties, use the OVF environment, and specify IP allocation and product information for the virtual machine.

Enable Virtual Machine vApp Options

You can configure vApp options in a virtual machine. Those options are saved when you export the virtual machine as an OVF template, and used when the OVF is deployed.

If you enable vApp options and export a virtual machine to OVF, the virtual machine receives an OVF Environment XML descriptor at boot time. The OVF descriptor might include values for custom properties including network configuration and IP addresses.

The OVF environment can be transported to the guest in two ways:

- As a CD-ROM that contains the XML document. The CD-ROM is mounted on the CD-ROM drive.
- Through VMware Tools. The guest OS environment variable *guestinfo.ovfEnv* contains the XML document.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.
2 Click the vApp Options tab.
3 Select **Enable vApp options**.
4 Click **OK**.

Edit Application Properties and OVF Deployment Options for a Virtual Machine

If a virtual machine is a deployed OVF, you can view application properties and OVF Deployment options that are defined in the OVF. Deployment options include unrecognized OVF section and the IP allocation policy

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 Click the vApp Options tab.

3 If the OVF template included editable application properties, make changes if necessary.

4 If the OFV template includes information that vCenter Server cannot process, you can view that information under Unrecognized OVF Sections.

5 If the OVF template included editable IP allocation options, make changes if necessary.

Option	Description
Static - Manual	IP addresses are manually configured. No automatic allocation is performed.
Transient - IP Pool	IP addresses are automatically allocated using IP pools from a specified range when the vApp is powered on. The IP addresses are released when the appliance is powered off.
DHCP	A DHCP server is used to allocate the IP addresses. The addresses assigned by the DHCP server are visible in the OVF environments of virtual machines started in the vApp.
Static - IP Pool	IP addresses are automatically allocated from the managed IP network range of vCenter Server at power-on, and remain allocated at power-off.

Static - IP Pool and Transient - IP Pool have in common that IP allocation is done through the range managed by the vSphere platform as specified by the IP pool range in a network protocol profile. The difference is that for a static IP Pool, the IP addresses are allocated at first power-on and remain allocated, while for a transient IP Pool, the IP addresses are allocated when needed, typically at power-on, but released during power-off.

Edit OVF Authoring Options for a Virtual Machine

You can use the OVF Authoring options that are included in a virtual machine's vApp options to specify custom information that is included when you export the virtual machine as an OVF template.

vApp properties are a central concept of vApp deployment and self configuration; they can turn a general OVF package into a running vApp instance with a custom configuration.

The set of properties associated to a running vApp is determined by the OVF package from which the vApp was deployed.

- When an OVF package is created the author adds the set of properties necessary for the vApp to function in an unknown environment. This could for instance be properties containing network configuration, a property containing the email address of the system administrator or a property containing the number of expected users of the vApp.
- Some property values are entered by the user when the vApp is deployed, while other property values are configured by vCenter Server when the vApp is powered on. How this is handled depends on the property type and vCenter Server configuration.

When vCenter Server powers on a vApp, it creates an XML document that contains all properties and their values. This document is made available to each virtual machine in the vApp, and allows the virtual machines to apply the properties to their own environment.

1 Edit vApp Product Information for a Virtual Machine on page 182

   If you want to export a virtual machine as an OVF, you can prespecify product properties. Those properties become available when you deploy the OVF as a virtual machine.

2 Manage vApp Custom Properties for a Virtual Machine on page 183

   You can manage and define custom properties that are stored in the OVF template when you export a virtual machine or vApp and are used by vCenter Server when you deploy the OVF template. OVF templates support static properties, which are often configured by the user, and dynamic properties, which are always set by vCenter Server.

3 Edit vApp IP Allocation Policy for a Virtual Machine on page 183

   You can edit the IP allocation policy through the Virtual Machine Properties dialog box.

4 Edit OVF Settings for a Virtual Machine on page 184

   A virtual machine's OVF settings allow you to customize the OVF environment, OVF transport, and boot behavior after OVF deployment. You can edit and configure settings that affect the OVF environment in the Virtual Machine Properties dialog box.

Edit vApp Product Information for a Virtual Machine

If you want to export a virtual machine as an OVF, you can prespecify product properties. Those properties become available when you deploy the OVF as a virtual machine.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 Click the vApp Options tab.

3 In the Authoring section select **Product**.

4 Set and configure the settings that appear on the summary page of the virtual machine.

vApp Setting	Description
Product Name	Product Name.
Version	vApp version.
Full Version	Full version of the vApp.
Product URL	If you enter a product URL, a user can click the product name on the virtual machine summary page and go to the product's web page.
Vendor URL	If you enter a vendor URL, a user can click the vendor name on the virtual machine summary page and go to the vendor's web page.
Application URL	The vApp Summary page you can view in the vSphere Client includes a Status pane that includes information about vApp status, for example **Running** or **Stopped**. If you enter a valid application URL, the virtual machine Status pane displays **Available** instead of Running. The **Available** text is also a link to the application URL.

   if you configure the virtual machine to use the property called *webserver_ip* and the virtual machine has a web server at the address represented by the property, you can enter **`http://${webserver_ip}/`** as the **Application URL**.

5 Click **OK**.

Manage vApp Custom Properties for a Virtual Machine

You can manage and define custom properties that are stored in the OVF template when you export a virtual machine or vApp and are used by vCenter Server when you deploy the OVF template. OVF templates support static properties, which are often configured by the user, and dynamic properties, which are always set by vCenter Server.

Perform these tasks to customize your virtual machine or vApp with properties:

1 Define the OVF properties, for example a DNS address or gateway, in the virtual machine or vApp.

2 If you or planning to export to OVF:

   a Set up the OVF environment transport to carry the settings into the virtual machine. See "Edit OVF Settings for a Virtual Machine," on page 184.

   b Write some glue code to access and apply the information to the virtual machine.

See the VMware vApp Developer blog topic *Self-Configuration and the OVF Environment* for a discussion, sample code, and a video.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 Click the vApp Options tab.

3 In the Authoring section, click **Properties**.

   You can select and edit or delete an existing property, or create a new custom property.

4 To create a property, click **New**.

5 Specify property fields.

6 Click **OK**.

Edit vApp IP Allocation Policy for a Virtual Machine

You can edit the IP allocation policy through the Virtual Machine Properties dialog box.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 Click the vApp Options tab.

3 In the Authoring section, select **IP allocation**.

   The information you specify will be used if you export the virtual machine to OVF and deploy the OVF.

4 Select a network configuration scheme.

Option	Description
OVF environment	Determined by the environment in which you deploy the OVF template.
DHCP	The IP addresses are allocated using DHCP when the virtual machine is powered on.

5 Choose the IP protocol that this vApp supports: IPv4, IPv6, or both.

6 Click **OK**.

Edit OVF Settings for a Virtual Machine

A virtual machine's OVF settings allow you to customize the OVF environment, OVF transport, and boot behavior after OVF deployment. You can edit and configure settings that affect the OVF environment in the Virtual Machine Properties dialog box.

Prerequisites

vApp options must be enabled in order to access these options.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 Click the vApp Options tab.

3 In the Authoring section, click **OVF Settings**.

4 View and specify the settings.

Option	Description
OVF environment	Click **View** to display the OVF environment settings in XML format. The settings are not available when the virtual machine is powered off.
OVF environment transport	■ If you select ISO image, an ISO image that contains the OVF template information is mounted in the CD-ROM drive. ■ If you select VMware Tools, the VMware Tools `guestInfo.ovfEnv` variable is initialized with the OVF environment document.
Installation boot	If you click Enable, the virtual machine is reboots after OVF deployment completes. You can select the amount of time before the virtual machine starts the reboot operation.

5 Click **OK**.

Monitoring Solutions with the vCenter Solutions Manager 9

In the vSphere Web Client, you can view an inventory of installed solutions, view detailed information about the solutions, and monitor the solution health status. A solution is an extension of vCenter Server that adds new functions to a vCenter Server instance.

VMware products that integrate with vCenter Server are also considered solutions. For example, vSphere ESX Agent Manager is a solution provided by VMware to let you manage host agents that add new capabilities to ESX/ESXi hosts.

You can install a solution to add functionality from third-party technologies to the standard functions of vCenter Server. Solutions typically are delivered as OVF packages. You can install and deploy solutions from the vSphere Web Client. You can integrate solutions into the vCenter Solutions Manager, which provides a view in the vSphere Web Client that lists all solutions.

If a virtual machine or vApp is running a solution, a custom icon represents it in the inventory of the vSphere Web Client. Each solution registers a unique icon to identify that the virtual machine or vApp is being managed by that solution. The icons show the power states (powered on, paused, or powered off). The solutions display more than one type of icon if they manage more than one type of virtual machine or vApp.

When you power on or power off a virtual machine or vApp, you are notified that you are performing this operation on an entity that is managed by the Solutions Manager. When you attempt an operation on a virtual machine or a vApp that is managed by a solution, an informational warning message appears.

For more information, see the *Developing and Deploying vSphere Solutions, vServices, and ESX Agents* documentation.

This chapter includes the following topics:

- "Viewing Solutions," on page 185
- "Monitoring Agents," on page 186

Viewing Solutions

You can deploy, monitor, and interact with solutions that are installed in a vCenter Server instance with the vCenter Solutions Manager. The Solutions Manager displays information about the health of a solution.

You can navigate to the Solutions Manager from the home page of the vSphere Client. The Solutions Manager view displays information about the solution:

- Solution name
- Solution health
- vService providers

Procedure

1 Click the Solutions Manager icon from vSphere Client home.

2 Navigate through the tabs in the Solutions Manager.

- **Summary** tab. Lists the number of installed solutions and a brief health overview for each of the solutions.
- **Solutions** tab. Lists each managed solution.
- **Health** tab. Provides the health status of the vCenter services. It also shows alerts or warnings for each of the services.

3 In the Solutions Manager inventory, click one of the solutions.

- **Summary** tab. Lists information about the solution, including a link to the product and vendor Web sites, a link to launch the management UI in a separate window, and a link to the virtual machine or vApp running this solution.

  Selecting the vendor Web site link takes you to the Summary page of the virtual machine or vApp. A link under "Managed by" returns you to the solution.
- **Virtual Machines** tab. Lists all the virtual machines belonging to the solution
- **vServices Providers** tab.
- **Management** tab or any other tabs the solution specified.

Monitoring Agents

The vCenter Solutions Manager displays the vSphere ESX Agent Manager agents that you use to deploy and manage related agents on ESX/ESXi hosts.

You can use the Solutions Manager to keep track of whether the agents of a solution are working as expected. Outstanding issues are reflected by the solution's ESX Agent Manager status and a list of issues.

When the status of a solution changes, the Solutions Manager updates the ESX Agent Manager summary status and state. Administrators use this status to track whether the goal state is reached.

The agent health status is indicated by a specific color.

Table 9-1. ESX Agent Manager health status

Status	Description
Red	The solution must intervene for the ESX Agent Manager to proceed. For example, if a virtual machine agent is powered off manually on a compute resource and the ESX Agent Manager does not attempt to power on the agent. The ESX Agent Manager reports this action to the solution, and the solution alerts the administrator to power on the agent.
Yellow	The ESX Agent Manager is actively working to reach a goal state. The goal state can be enabled, disabled, or uninstalled. For example, when a solution is registered, its status is yellow until the ESX Agent Manager deploys the solutions agents to all the specified compute resources. A solution does not need to intervene when the ESX Agent Manager reports its ESX Agent Manager health status as yellow.
Green	A solution and all its agents have reached the goal state.

Managing Virtual Machines 10

You can manage individual virtual machines or a group of virtual machines that belongs to a host or cluster.

You can install the Client Integration Plug-in to access the virtual machine's console. From the console, you can change the guest operating system settings, use applications, browse the file system, monitor system performance, and so on. Use snapshots to capture the state of the virtual machine at the time you take the snapshot.

To migrate virtual machines using cold or hot migration, including vMotion, vMotion in environments without shared storage, and Storage vMotion, see the *vCenter Server and Host Management* documentation.

This chapter includes the following topics:

- "Edit Virtual Machine Startup and Shutdown Settings," on page 187
- "Install the Client Integration Plug-In," on page 189
- "Open a Virtual Machine Console," on page 189
- "Install the VMware Remote Console Application," on page 190
- "Using the VMware Remote Console Application," on page 190
- "Adding and Removing Virtual Machines," on page 191
- "Change the Template Name," on page 192
- "Deleting Templates," on page 193
- "Using Snapshots To Manage Virtual Machines," on page 194

Edit Virtual Machine Startup and Shutdown Settings

You can configure virtual machines running on an ESXi host to start up and shut down with the host. You can also set the default timing and startup order for selected virtual machines. This ability allows the operating system to save data when the host enters maintenance mode or is being powered off for another reason.

The Virtual Machine Startup and Shutdown (automatic startup) feature is disabled for all virtual machines residing on hosts that are in a vSphere HA cluster. Automatic startup is not supported with vSphere HA.

Note You can also create a scheduled task to change the power settings of a virtual machine. Information about scheduling tasks is included in *vCenter Server and Host Management*.

Procedure

1 In the vSphere Web Client, navigate to the host where the virtual machine is located.

2 Select **Manage > Settings**.

3 Under Virtual Machines, select **VM Startup/Shutdown** and click **Edit**.

The Edit VM Startup and Shutdown dialog box opens.

4 Select **Allow virtual machines to start and stop automatically with the system**.

5 (Optional) In the Default VM Settings pane, configure the default startup and shutdown behavior for all virtual machines on the host.

Option	Action
Startup Delay	Set the delay for starting the operating system after the virtual machine powers on. This delay allows time for VMware Tools or the booting system to run scripts. Note that the setting will be not be applied to the first virtual machine in your list, but to subsequent virtual machines.
Continue immediately if VMware Tools starts	Select this check box to have the operating system start immediately after VMware Tools starts without waiting for the delay to pass.
Shutdown Delay	Set the delay between shutting down each virtual machine. The shutdown delay applies only if the virtual machine does not shut down before the delay period elapses. If the virtual machine shuts down before the delay time is reached, the next virtual machine starts shutting down.
Shutdown Action	Select a shutdown option from the drop-down menu. ■ Power Off ■ Suspend ■ Guest Shutdown

6 (Optional) In the Per-VM Overrides pane, configure the startup order and behavior for individual virtual machines.

The settings that you configure for individual virtual machines override the default settings for these machines.

a To change the startup order of virtual machines, select one from the Manual Startup category and use the up arrow to move it up to Automatic Startup or Any Order.

For virtual machines in the Automatic Startup category, you can use the up and down arrows to change their startup order. During shutdown, the virtual machines shut down in the opposite order.

b Click **Startup Behavior**, select **Custom**, and configure the startup delay for the operating system to allow VMware Tools and other services to start first.

c Click **VMware Tools**, and select whether the operating system startup should wait for the delay to pass when VMware Tools is already installed on the virtual machine.

The **Continue immediate if the VMware Tools start** option enables the operating system to start without waiting for the delay to pass. The **Do not continue if VMware Tools is installed** option enables the operating system startup to wait for the delay to pass.

d Click **Shutdown Behavior**, select **Custom**, and configure the shutdown action and delay.

7 Click **OK** to close the dialog box and save your settings.

Install the Client Integration Plug-In

The Client Integration Plug-in provides access to a virtual machine's console in the vSphere Web Client, and provides access to other vSphere infrastructure features. The Client Integration Plug-in also lets you log in to the vSphere Web Client by using Windows session credentials.

You use the Client Integration Plug-in to deploy OVF or OVA templates and transfer files with the datastore browser. You can also use the Client Integration Plug-in to connect virtual devices that reside on a client computer to a virtual machine.

Install the Client Integration Plug-in only once to enable all the functionality the plug-in delivers. You must close the Web browser before installing the plug-in.

If you install the Client Integration Plug-in from an Internet Explorer browser, you must first disable Protected Mode and enable pop-up windows on your Web browser. Internet Explorer identifies the Client Integration Plug-in as being on the Internet instead of on the local intranet. In such cases, the plug-in is not installed correctly because Protected Mode is enabled for the Internet.

For information about supported browsers and operating systems, see the *vSphere Installation and Setup* documentation.

Watch the video "Installing the Client Integration Plug-In" for information about the Client Integration Plug-In:

Installing the Client Integration Plug-In (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_client_plug_in)

Prerequisites

If you use Microsoft Internet Explorer, disable Protected Mode.

Procedure

1 In the vSphere Web Client, navigate to a link to download the Client Integration Plug-in.

Option	Description
vSphere Web Client login page	a Open a Web browser and type the URL for the vSphere Web Client. b At the bottom of the vSphere Web Client login page, click **Download Client Integration Plug-in**. NOTE If the Client Integration Plug-In is already installed on your system, you will not see the link to download the plug-in. If you uninstall the Client Integration Plug-In, the link to download it will display on the vSphere Web Client login page.
OVF deployment wizard	a Select a host in the inventory and select **Actions > All vCenter Actions > Deploy OVF Template**. b Click **Download Client Integration Plug-in**.

2 If the browser blocks the installation either by issuing certificate errors or by running a pop-up blocker, follow the Help instructions for your browser to resolve the problem.

Open a Virtual Machine Console

With the vSphere Web Client, you can access a virtual machine's desktop by launching a console to the virtual machine. From the console, you can perform activities in the virtual machine such as install operating system, configure operating system settings, run applications, monitor performance, and so on.

The Client Integration Plug-in and VMRC stand-alone application helps you connect virtual devices to the virtual machine and view the console in full screen mode.

Prerequisites

- If you use Microsoft Internet Explorer, verify that the Client Integration Plug-in is installed.

  For more information, see "Install the Client Integration Plug-In," on page 189.
- Verify that the virtual machine has a guest operating system and that VMware Tools is installed.
- Verify that the virtual machine is powered on.

Procedure

1. Select a datacenter, folder, cluster, resource pool, host, or vApp and click the **Related Objects** tab.
2. Click **Virtual Machines** and select a virtual machine.
3. Click the **Summary** tab and click **Launch console**.

   The virtual machine console opens in a new tab of the Web browser.
4. Click anywhere inside the console window to start using your mouse, keyboard, and other input devices in the console.
5. (Optional) Click **Send Ctrl-Alt-Delete** to send the Ctrl+Alt+Delete keystroke combination to the guest operating system.
6. (Optional) Press Ctrl+Alt to release the cursor from the console window and work outside the console window.

   This keystroke combination is only available if the Client Integration Plug-in is installed for your Web browser.
7. (Optional) Click **Full Screen** to view the console in full screen mode.

   This button is only available if the Client Integration Plug-in is installed for your Web browser.
8. (Optional) Press Ctrl+Alt+Enter to enter or exit full screen mode.

   This keystroke combination is only available if the Client Integration Plug-in is installed for your Web browser.

Install the VMware Remote Console Application

The VMware Remote Console (VMRC) is a stand-alone console application for Windows that enables you to connect to client devices and launch virtual machine consoles on remote hosts.

Procedure

1. In the vSphere Web Client, navigate to a virtual machine console in the inventory.
2. Click the **Summary** tab, and click **Download VMRC** link.
3. Download the VMRC installer from the VMware Web site at www.vmware.com/go/download-vmrc.

Using the VMware Remote Console Application

You can use the stand-alone VMRC to connect to client devices.

With VMRC, you can access the mouse and keyboard connected to remote virtual machines. For performing any administrative tasks, make sure you log in to the VMRC as an administrator.

Prerequisites

Verify that the VMRC is installed on your local system. You can download the VMRC installer for Windows from the VMware Web site at www.vmware.com/go/download-vmrc.

Procedure

1 In the vSphere Web Client, navigate to a virtual machine console in the inventory.

2 Click the **Summary** tab, and click **Open with VMRC** link.

3 Select the **VMware Remote Console** application from the list.

4 Click **OK**.

The VMRC opens as a stand-alone application for the selected virtual machine. You can also launch more than one console to access several remote virtual machines at the same time.

Adding and Removing Virtual Machines

You add virtual machines to the vCenter Server inventory through their managed hosts. You can remove virtual machines from vCenter Server, from their managed host's storage, or from both.

Adding Existing Virtual Machines to vCenter Server

When you add a host to vCenter Server, it discovers all the virtual machines on that managed host and adds them to the vCenter Server inventory.

If a managed host is disconnected, the already discovered virtual machines continue to be listed in the inventory.

If a managed host is disconnected and reconnected, any changes to the virtual machines on that managed host are identified, and the vSphere Web Client updates the list of virtual machines. For example, if node3 is removed and node4 is added, the new list of virtual machines adds node4 and shows node3 as orphaned.

Remove Virtual Machines from vCenter Server

When you remove a virtual machine from the inventory, you unregister it from the host and vCenter Server, but you do not delete it from the datastore. Virtual machine files remain at the same storage location and you can re-registered the virtual machine by using the datastore browser at a later time. This capability is useful if you need to unregister a virtual machine to edit the virtual machine's configuration file. The ability to remove a virtual machine and maintain its files is useful when you have reached the maximum number of virtual machines that your license or hardware allows.

Prerequisites

Verify that the virtual machine is turned off.

Procedure

1 Right-click the virtual machine, and select **All vCenter Actions > Remove From Inventory**.

2 To confirm that you want to remove the virtual machine from the inventory, click **OK**.

vCenter Server removes references to the virtual machine and no longer tracks its condition.

Remove Virtual Machines from the Datastore

If you no longer need a virtual machine and want to free up space on the datastore, you can remove the virtual machine from vCenter Server and delete all virtual machine files from the datastore, including the configuration file and virtual disk files.

Prerequisites

- Power off the virtual machine.
- Ensure that another virtual machine is not sharing the disk. If two virtual machines are sharing the same disk, the disk files are not deleted.

Procedure

1 Right-click the virtual machine and select **All vCenter Actions > Delete from Disk**.

2 Click **OK**.

vCenter Server deletes the virtual machine from its datastore. Disks that are shared with other virtual machines are not deleted.

Register a Virtual Machine with vCenter Server

If you removed a virtual machine from vCenter Server but did not remove it from the managed host's datastore, you can return it to the vCenter Server inventory by registering it with the vCenter Server.

Procedure

1 In the vSphere Web Client inventory, right-click the datastore on which the virtual machine configuration file is stored and select **All vCenter Actions > Register VM**.

2 Browse to and select the virtual machine configuration (`.vmx`) file and click **OK**.

3 Use the existing virtual machine name or type a new name, and select a datacenter or folder location for the virtual machine.

4 Click **Next**.

5 Select a host or cluster on which to run the new virtual machine.

Option	Action
Run the virtual machine on a standalone host.	Select the host and click **Next**.
Run the virtual machine in a cluster with DRS automatic placement.	Select the cluster and click **Next**.
Run the virtual machine in a cluster without DRS automatic placement.	a Select the cluster and click **Next**. b Select a host within the cluster and click **Next**.

6 Select a resource pool in which to run the virtual machine and click **Next**.

7 Review your selections and click **Finish**.

The virtual machine is added to the vCenter Server inventory.

Change the Template Name

If you move a template to another host or datacenter folder, you can change the template name to make it unique in that folder.

Procedure

1 Right-click the template and select **Rename**.

2 Enter a new name and click **OK**.

Deleting Templates

You can delete a template by removing it from the inventory or deleting the template from the disk. If you remove the template from the inventory, it remains on the disk and can be reregistered with vCenter Server to restore it to the inventory.

Remove Templates from the Inventory

If a template has become outdated and you no longer use it in your environment, you can remove it from the inventory. Removing a template unregisters it from the vCenter Server inventory, but it is not removed from the datastore. The template remains at the same storage location, and you can use the datastore browser to re-registered the template at a later time. You can later decide to update the template rather than create one.

Procedure

1 Right-click the template and select **All vCenter Actions > Remove from Inventory**.

2 Click **Yes** to confirm removing the template from the vCenter Server database.

The template is unregistered from the vCenter Server inventory.

Delete a Template from the Disk

If you no longer need a template or need to free up disk space, you can remove it from the disk. Templates that you delete are permanently removed from the system.

You cannot recover a template that you delete from the disk.

Procedure

1 Right-click the template and select **All vCenter Actions > Delete from Disk**.

2 Click **Yes** to confirm removing the template from the datastore.

Reregister Templates

Templates can become unregistered from vCenter Server if they are removed from the inventory or if the hosts with which they are associated are removed from vCenter Server and then readded.

Procedure

1 Browse to or search for the datastore that contains the template.

2 Click the **Manage** tab and click **Files**.

3 Browse to locate the template and click it to display the template files.

The hard disk and configuration and other files appear in the Name column.

4 Click the template to display the template files.

5 Locate and right-click the `.vmtx` file and select **Register VM**.

The Register Virtual Machine wizard appears.

6 Maintain the original template name or enter a new name in the **Name** text box.

7 Select a location for the template and click **Next**.

8 Select a host or cluster on which to store the template and click **Next**.

9 Review your selections and click **Finish**.

10 To verify that the template is reregistered, check the host or cluster inventory.

Inventory	Description
Host	Browse to the host. Click the **Related Objects** tab, and click **VM Templates**.
Cluster	Browse to the cluster. In the inventory view, select **VM Templates** to display the list of templates.

The template is registered to the host. Click the **Related Objects** tab, and click VM Templates to view the template. You can view the template from the host's **Related Objects** tab by clicking **VM Templates** .

Using Snapshots To Manage Virtual Machines

Snapshots preserve the state and data of a virtual machine at the time you take the snapshot. Snapshots are useful when you must revert repeatedly to the same virtual machine state, but you do not want to create multiple virtual machines.

You can take multiple snapshots of a virtual machine to create restoration positions in a linear process. With multiple snapshots, you can save many positions to accommodate many kinds of work processes. Snapshots operate on individual virtual machines. Taking snapshots of multiple virtual machines, for example, taking snapshots for all members of a team, requires that you take a separate snapshot of each team member's virtual machine.

Snapshots are useful as a short term solution for testing software with unknown or potentially harmful effects. For example, you can use a snapshot as a restoration point during a linear or iterative process, such as installing update packages, or during a branching process, such as installing different versions of a program. Using snapshots ensures that each installation begins from an identical baseline.

With snapshots, you can preserve a baseline before diverging a virtual machine in the snapshot tree.

The Snapshot Manager in the vSphere Web Client provide several operations for creating and managing virtual machine snapshots and snapshot trees. These operations let you create snapshots, restore any snapshot in the snapshot hierarchy, delete snapshots, and more. You can create extensive snapshot trees that you can use to save the virtual machine state at any specific time and restore the virtual machine state later. Each branch in a snapshot tree can have up to 32 snapshots.

A snapshot preserves the following information:

- Virtual machine settings. The virtual machine directory, which includes disks that were added or changed after you took the snapshot.
- Power state. The virtual machine can be powered on, powered off, or suspended.
- Disk state. State of all the virtual machine's virtual disks.
- (Optional) Memory state. The contents of the virtual machine's memory.

The Snapshot Hierarchy

The Snapshot Manager presents the snapshot hierarchy as a tree with one or more branches. The relationship between snapshots is like that of a parent to a child. In the linear process, each snapshot has one parent snapshot and one child snapshot, except for the last snapshot, which has no child snapshots. Each parent snapshot can have more than one child. You can revert to the current parent snapshot or restore any parent or child snapshot in the snapshot tree and create more snapshots from that snapshot. Each time you restore a snapshot and take another snapshot, a branch, or child snapshot, is created.

Parent Snapshots

The first virtual machine snapshot that you create is the base parent snapshot. The parent snapshot is the most recently saved version of the current state of the virtual machine. Taking a snapshot creates a delta disk file for each disk attached to the virtual machine and optionally, a memory file. The delta disk files and memory file are stored with the base .vmdk file. The parent snapshot is always the snapshot that appears immediately above the You are here icon in the Snapshot Manager. If you revert or restore a snapshot, that snapshot becomes the parent of the You are here current state.

NOTE The parent snapshot is not always the snapshot that you took most recently.

Child Snapshots

A snapshot that is taken of the same virtual machine after the parent snapshot. Each child constitutes delta files for each attached virtual disk, and optionally a memory file that points from the present state of the virtual disk (You are here). Each child snapshot's delta files merge with each previous child snapshot until reaching the parent disks. A child disk can later be a parent disk for future child disks.

The relationship of parent and child snapshots can change if you have multiple branches in the snapshot tree. A parent snapshot can have more than one child. Many snapshots have no children.

IMPORTANT Do not manually manipulate individual child disks or any of the snapshot configuration files because doing so can compromise the snapshot tree and result in data loss. This restriction includes disk resizing and making modifications to the base parent disk using `vmkfstools`.

Snapshot Behavior

Taking a snapshot preserves the disk state at a specific time by creating a series of delta disks for each attached virtual disk or virtual RDM and optionally preserves the memory and power state by creating a memory file. Taking a snapshot creates a snapshot object in the Snapshot Manager that represents the virtual machine state and settings.

Each snapshot creates an additional delta `.vmdk` disk file. When you take a snapshot, the snapshot mechanism prevents the guest operating system from writing to the base `.vmdk` file and instead directs all writes to the delta disk file. The delta disk represents the difference between the current state of the virtual disk and the state that existed at the time that you took the previous snapshot. If more than one snapshot exists, delta disks can represent the difference between each snapshot. Delta disk files can expand quickly and become as large as the entire virtual disk if the guest operating system writes to every block of the virtual disk.

Snapshot Files

When you take a snapshot, you capture the state of the virtual machine settings and the virtual disk. If you are taking a memory snapshot, you also capture the memory state of the virtual machine. These states are saved to files that reside with the virtual machine's base files.

Snapshot Files

A snapshot consists of files that are stored on a supported storage device. A Take Snapshot operation creates `.vmdk`, `–delta.vmdk`, `.vmsd`, and `.vmsn` files. By default, the first and all delta disks are stored with the base `.vmdk` file. The `.vmsd` and `.vmsn` files are stored in the virtual machine directory.

Delta disk files

A `.vmdk` file to which the guest operating system can write. The delta disk represents the difference between the current state of the virtual disk and the state that existed at the time that the previous snapshot was taken. When you take a snapshot, the state of the virtual disk is preserved, which prevents the guest operating system from writing to it, and a delta or child disk is created.

A delta disk has two files, including a descriptor file that is small and contains information about the virtual disk, such as geometry and child-parent relationship information, and a corresponding file that contains the raw data.

The files that make up the delta disk are referred to as child disks or redo logs. A child disk is a sparse disk. Sparse disks use the copy-on-write mechanism, in which the virtual disk contains no data in places, until copied there by a write operation. This optimization saves storage space. A grain is the unit of measure in which the sparse disk uses the copy-on-write mechanism. Each grain is a block of sectors that contain virtual disk data. The default size is 128 sectors or 64KB.

Flat file

A `–flat.vmdk` file that is one of two files that comprises the base disk. The flat disk contains the raw data for the base disk. This file does not appear as a separate file in the Datastore Browser.

Database file

A `.vmsd` file that contains the virtual machine's snapshot information and is the primary source of information for the Snapshot Manager. This file contains line entries, which define the relationships between snapshots and between child disks for each snapshot.

Memory file

A `.vmsn` file that includes the active state of the virtual machine. Capturing the memory state of the virtual machine lets you revert to a turned on virtual machine state. With nonmemory snapshots, you can only revert to a turned off virtual machine state. Memory snapshots take longer to create than nonmemory snapshots. The time the ESX host takes to write the memory onto the disk is relative to the amount of memory the virtual machine is configured to use.

A **Take Snapshot** operation creates `.vmdk`, `–delta.vmdk`, `vmsd`, and `vmsn` files.

File	Description
vmname–number.vmdk and *vmname–number*–delta.vmdk	Snapshot file that represents the difference between the current state of the virtual disk and the state that existed at the time the previous snapshot was taken. The filename uses the following syntax, S1vm–000001.vmdk where S1vm is the name of the virtual machine and the six-digit number, 000001, is based on the files that already exist in the directory. The number does not consider the number of disks that are attached to the virtual machine.
vmname.vmsd	Database of the virtual machine's snapshot information and the primary source of information for the Snapshot Manager.
vmname.Snapshot*number*.vmsn	Memory state of the virtual machine at the time you take the snapshot. The file name uses the following syntax, S1vm.snapshot1.vmsn, where S1vm is the virtual machine name, and snapshot1 is the first snapshot. **Note** A .vmsn file is created each time you take a snapshot, regardless of the memory selection. A .vmsn file without memory is much smaller than one with memory.

Snapshot Limitations

Snapshots can affect virtual machine performance and do not support some disk types or virtual machines configured with bus sharing. Snapshots are useful as short-term solutions for capturing point-in-time virtual machine states and are not appropriate for long-term virtual machine backups.

- VMware does not support snapshots of raw disks, RDM physical mode disks, or guest operating systems that use an iSCSI initiator in the guest.
- Virtual machines with independent disks must be powered off before you take a snapshot. Snapshots of powered-on or suspended virtual machines with independent disks are not supported.
- Snapshots are not supported with PCI vSphere Direct Path I/O devices.
- VMware does not support snapshots of virtual machines configured for bus sharing. If you require bus sharing, consider running backup software in your guest operating system as an alternative solution. If your virtual machine currently has snapshots that prevent you from configuring bus sharing, delete (consolidate) the snapshots.
- Snapshots provide a point-in-time image of the disk that backup solutions can use, but Snapshots are not meant to be a robust method of backup and recovery. If the files containing a virtual machine are lost, its snapshot files are also lost. Also, large numbers of snapshots are difficult to manage, consume large amounts of disk space, and are not protected in the case of hardware failure.
- Snapshots can negatively affect the performance of a virtual machine. Performance degradation is based on how long the snapshot or snapshot tree is in place, the depth of the tree, and how much the virtual machine and its guest operating system have changed from the time you took the snapshot. Also, you might see a delay in the amount of time it takes the virtual machine to power-on. Do not run production virtual machines from snapshots on a permanent basis.
- If a virtual machine has virtual hard disks larger than 2TBs, snapshot operations can take significantly longer to finish.

Managing Snapshots

You can review all snapshots for the active virtual machine and act on them by using the Snapshot Manager.

After you take a snapshot, you can use the **Revert to Latest Snapshot** command from the virtual machine's right-click menu to restore that snapshot at any time. If you have a series of snapshots, you can use the **Revert to** command in the Snapshot Manager to restore any parent or child snapshot. Subsequent child snapshots that you take from the restored snapshot create a branch in the snapshot tree. You can delete a snapshot from the tree in the Snapshot Manager.

The Snapshot Manager window contains the following areas: Snapshot tree, Details region, command buttons, Navigation region, and a **You are here** icon.

Snapshot tree
Displays all snapshots for the virtual machine.

You are here icon
Represents the current and active state of the virtual machine. The **You are here** icon is always selected and visible when you open the Snapshot Manager.

You can select the **You are here** state to see how much space the node is using. **Revert to**, **Delete**, and **Delete all** are disabled for the **You are here** state.

Revert to, Delete, and Delete All
Snapshot options.

Details
Shows the snapshot name and description, the date you created the snapshot, and the disk space. The Console shows the power state of the virtual machine when a snapshot was taken. The Name, Description, and Created text boxes are blank if you do not select a snapshot.

Navigation
Contains buttons for navigating out of the dialog box.

- **Close** the Snapshot Manager.
- The question mark icon opens the help system.

Taking Snapshots of a Virtual Machine

You can take one or more snapshots of a virtual machine to capture the settings state, disk state, and memory state at different specific times. When you take a snapshot, you can also quiesce the virtual machine files and exclude the virtual machine disks from snapshots.

When you take a snapshot, other activity that is occurring in the virtual machine might affect the snapshot process when you revert to that snapshot. The best time to take a snapshot from a storage perspective, is when you are not incurring a large I/O load. The best time to take a snapshot from a service perspective is when no applications in the virtual machine are communicating with other computers. The potential for problems is greatest if the virtual machine is communicating with another computer, especially in a production environment. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file and 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. Depending on the task that you are performing, you can create a memory snapshot or you can quiesce the file system in the virtual machine.

Memory Snapshots
The default selection for taking snapshots. When you capture the virtual machine's memory state, the snapshot retains the live state of the virtual machine. Memory snapshots create a snapshot at a precise time, for example, to upgrade software that is still working. If you take a memory snapshot and the upgrade does not complete as expected, or the software does not meet your expectations, you can revert the virtual machine to its previous state.

When you capture the memory state, the virtual machine's files do not require quiescing. If you do not capture the memory state, the snapshot does not save the live state of the virtual machine and the disks are crash consistent unless you quiesce them.

Quiesced Snapshots

When you quiesce a virtual machine, VMware Tools quiesces the file system of the virtual machine. A quiesce operation ensures that a snapshot disk represents a consistent state of the guest file systems. Quiesced snapshots are appropriate for automated or periodic backups. For example, if you are unaware of the virtual machine's activity, but want several recent backups to revert to, you can quiesce the files.

If the virtual machine is powered off or VMware Tools is not available, the `Quiesce` parameter is not available. You cannot quiesce virtual machines that have large capacity disks.

Important Do not use snapshots as your only backup solution or as a long-term backup solution.

Change Disk Mode to Exclude Virtual Disks from Snapshots

You can set a virtual disk to independent mode to exclude the disk from any snapshots taken of its virtual machine.

Prerequisites

Power off the virtual machine and delete any existing snapshots before you change the disk mode. Deleting a snapshot involves committing the existing data on the snapshot disk to the parent disk.

Required privileges:

- **Virtual machine.Snapshot management.Remove Snapshot**
- **Virtual machine.Configuration.Modify device settings**

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

2 On the **Virtual Hardware** tab, expand **Hard disk**, and select an independent disk mode option.

Option	Description
Independent - Persistent	Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk.
Independent - Nonpersistent	Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset.

3 Click **OK**.

Taking a Snapshot

Snapshots capture the entire state of the virtual machine at the time you take the snapshot. You can take a snapshot when a virtual machine is powered on, powered off, or suspended. If you are suspending a virtual machine, wait until the suspend operation finishes before you take a snapshot.

When you create a memory snapshot, the snapshot captures the state of the virtual machine's memory and the virtual machine power settings. When you capture the virtual machine's memory state, the snapshot operation takes longer to complete. You might also see a momentary lapse in response over the network.

When you quiesce a virtual machine, VMware Tools quiesces the file system in the virtual machine. The quiesce operation pauses or alters the state of running processes on the virtual machine, especially processes that might modify information stored on the disk during a restore operation.

Application-consistent quiescing is not supported for virtual machines with IDE or SATA disks.

NOTE Do not use VMware snapshots to backup Dynamic Disks. If you take a snapshot of a Dynamic Disk (Microsoft specific file system), you will not be able to revert to the snapshot. Snapshot technology does not have visibility into dynamic disks and cannot preserve the quiesce state of the disk files.

Prerequisites

- If you are taking a memory snapshot of a virtual machine that has multiple disks in different disk modes, verify that the virtual machine is powered off. 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.
- To capture the memory state of the virtual machine, verify that the virtual machine is powered on.
- To quiesce the virtual machine files, verify that the virtual machine is powered on and that VMware Tools is installed.
- Verify that you have the **Virtual machine.Snapshot management. Create snapshot** privilege on the virtual machine.

Procedure

1. Right-click the virtual machine the inventory and select **Take Snapshot**.
   a. To locate a virtual machine, select a datacenter, folder, cluster, resource pool, host, or vApp.
   b. Click the **Related Objects** tab and click **Virtual Machines**.
2. Type a name for the snapshot.
3. (Optional) Type a description for the snapshot.
4. (Optional) Select the **Snapshot the virtual machine’s memory** check box to capture the memory of the virtual machine.
5. (Optional) Deselect **Snapshot the virtual machine's memory** and select the **Quiesce guest file system (Needs VMware Tools installed)** check box to pause running processes on the guest operating system so that file system contents are in a known consistent state when you take the snapshot.

   Quiesce the virtual machine files only when the virtual machine is powered on and you do not want to capture the virtual machine's memory.
6. Click **OK**.

Restoring Snapshots

To return a virtual machine to its original state, or to return to another snapshot in the snapshot hierarchy, you can restore a snapshot.

When you restore a snapshot, you return the virtual machine's memory, settings, and the state of the virtual machine disks to the state they were in at the time you took the snapshot. If you want the virtual machine to be suspended, powered on, or powered off when you start it, make sure that it is in the correct state when you take the snapshot.

You can restore snapshots in the following ways:

Revert to Latest Snapshot Restores the parent snapshot, one level up in the hierarchy from the **You are Here** position. **Revert to Latest Snapshot** activates the parent snapshot of the current state of the virtual machine.

Revert To Lets you restore any snapshot in the snapshot tree and makes that snapshot the parent snapshot of the current state of the virtual machine. Subsequent snapshots from this point create a new branch of the snapshot tree.

Restoring snapshots has the following effects:

- The current disk and memory states are discarded, and the virtual machine reverts to the disk and memory states of the parent snapshot.
- Existing snapshots are not removed. You can restore those snapshots at any time.
- If the snapshot includes the memory state, the virtual machine will be in the same power state as when you created the snapshot.

Table 10-1. Virtual Machine Power State After Restoring a Snapshot

Virtual Machine State When Parent Snapshot Is Taken	Virtual Machine State After Restoration
Powered on (includes memory)	Reverts to the parent snapshot, and the virtual machine is powered on and running.
Powered on (does not include memory)	Reverts to the parent snapshot and the virtual machine is powered off.
Powered off (does not include memory)	Reverts to the parent snapshot and the virtual machine is powered off.

Virtual machines running certain kinds of workloads can take several minutes to resume responsiveness after reverting from a snapshot.

NOTE vApp metadata for virtual machines in vApps does not follow the snapshot semantics for virtual machine configuration. vApp properties that are deleted, modified, or defined after a snapshot is taken remain intact (deleted, modified, or defined) after the virtual machine reverts to that snapshot or any previous snapshots.

Revert to the Latest Snapshot

When you revert to the latest snapshot, you immediately restore the parent snapshot of the virtual machine.

When you revert to a snapshot, disks that you added or changed after the snapshot was taken are reverted to the snapshot point. For example, when you take a snapshot of a virtual machine, add a disk, and revert the snapshot, the added disk is removed.

Independent disks are also removed when you revert to a snapshot that was taken before the disk was added. If the latest snapshot includes an independent disk, its contents do not change when you revert to that snapshot.

Prerequisites

Verify that you have the **Virtual machine.Snapshot management.Revert to snapshot** privilege on the virtual machine.

Procedure

1 Right-click a virtual machine in the inventory, and select **Revert to Latest Snapshot**.

2 When prompted, click **Yes**.

The virtual machine power and data states are returned to the states they were in at the time you took the parent snapshot. If the parent snapshot is a memory snapshot, the virtual machine is restored to an on power state.

Revert to a Snapshot

Revert to a snapshot to restore the virtual machine to the state of that snapshot.

Prerequisites

Verify that you have the **Virtual machine.Snapshot management.Revert to snapshot** privilege on the virtual machine.

Procedure

1 Right-click the virtual machine and select **Manage Snapshots**.

2 In the Snapshot Manager, click a snapshot to select it.

3 Click **Revert to** to restore the virtual machine to the snapshot.

   The **Revert to** command lets you restore the state of any snapshot.

4 Click **Yes** in the confirmation dialog box.

5 Click **Close** to exit the Snapshot Manager.

Deleting Snapshots

Deleting a snapshot removes the snapshot from the Snapshot Manager. The snapshot files are consolidated and written to the parent snapshot disk and merge with the virtual machine base disk.

Deleting a snapshot leaves the current state of the virtual machine or any other snapshot untouched. Deleting a snapshot consolidates the changes between snapshots and previous disk states and writes to the parent disk all data from the delta disk that contains the information about the deleted snapshot. When you delete the base parent snapshot, all changes merge with the base virtual machine disk.

Deleting snapshots involves large amounts of disk reads and writes, which can reduce virtual machine performance until consolidation is complete. Consolidating snapshots removes redundant disks, which improves virtual machine performance and saves storage space. The time it takes to delete snapshots and consolidate the snapshot files depends on the volume of data that the guest operating system wrote to the virtual disks after you took the last snapshot. The required time is proportional to the amount of data the virtual machine is writing during consolidation if the virtual machine is powered on.

If disk consolidation fails when you delete a snapshot or delete all snapshots and you notice a degradation in virtual machine performance, you can view a list of virtual machines to determine if any files require consolidation, and if so, run a separate consolidation operation. For information about locating and viewing the consolidation state of multiple virtual machines and running a separate consolidation operation, see "Consolidate Snapshots," on page 203.

Delete

Use the **Delete** option to remove a single parent or child snapshot from the snapshot tree. **Delete** writes disk changes between the snapshot and the previous delta disk state to the parent snapshot.

You can also use the **Delete** option to remove a corrupt snapshot and its files from an abandoned branch of the snapshot tree without merging them with the parent snapshot.

Delete All

Use the **Delete All** option to delete all snapshots from the Snapshot Manager. **Delete all** consolidates and writes changes between snapshots and previous delta disk states to the base parent disk and merges them with the base virtual machine disk.

To prevent snapshot files from merging with the parent snapshot, for example in cases of failed updates or installations, first use the **Go to** command to restore to a previous snapshot. This action invalidates the snapshot delta disks and deletes the memory file. You can then use the **Delete** option to remove the snapshot and any associated files.

Delete a Snapshot in the vSphere Web Client

You can use the Snapshot Manager to delete a single snapshot or all snapshots in a snapshot tree.

Use care when you delete snapshots. You cannot restore a deleted snapshot. For example, you might want to install several browsers, a, b, and c, and capture the virtual machine state after you install each browser. The first, or base snapshot, captures the virtual machine with browser a and the second snapshot captures browser b. If you restore the base snapshot that includes browser a and take a third snapshot to capture browser c and delete the snapshot that contains browser b, you cannot return to the virtual machine state that includes browser b.

Prerequisites

- Ensure that you are familiar with the Delete and Delete all actions and how they might affect virtual machine performance. See "Deleting Snapshots," on page 202.
- Required Privilege: **Virtual machine.Snapshot management.Remove Snapshot** on the virtual machine.

Procedure

1. Right-click the virtual machine and select **Manage Snapshots**.
   a. To locate a virtual machine, select a datacenter, folder, cluster, resource pool, host, or vApp.
   b. Click the **Related Objects** tab and click **Virtual Machines**.
2. In the Snapshot Manager, click a snapshot to select it.
3. Select whether to delete a single snapshot or all snapshots.

Option	Description
Delete	Consolidates the snapshot data to the parent snapshot and removes the selected snapshot from the Snapshot Manager and virtual machine.
Delete All	Consolidates all of the immediate snapshots before the You are here current state to the base parent disk and removes all existing snapshots from the Snapshot Manager and virtual machine.

4. Click **Yes** in the confirmation dialog box.
5. Click **Close** to exit the Snapshot Manager.

Consolidate Snapshots

The presence of redundant delta disks can adversely affect virtual machine performance. You can combine such disks without violating a data dependency. After consolidation, redundant disks are removed, which improves virtual machine performance and saves storage space.

Snapshot consolidation is useful when snapshot disks fail to compress after a **Delete** or **Delete all** operation. This might happen, for example, if you delete a snapshot but its associated disk does not commit back to the base disk.

The Needs Consolidation column in the vSphere Web Client shows the virtual machines to consolidate.

Prerequisites

Required privilege: **Virtual machine.Snapshot management.Remove Snapshot**

Procedure

1 Show the Needs Consolidation column.

   a Select a vCenter Server instance, a host, or a cluster and click the **Manage** tab and click **Virtual Machines**.

   b Right-click the menu bar for any virtual machine column and select **Show/Hide Columns > Needs Consolidation**.

   A Yes status indicates that the snapshot files for the virtual machine should be consolidated, and that the virtual machine's **Tasks and Events** tab shows a configuration problem. A No status indicates that the files are OK.

2 To consolidate the files, right-click the virtual machine and select **All vCenter Actions > Consolidate**.

3 Check the Needs Consolidation column to verify that the task succeeded.

   If the task succeeded, a No value appears in the Needs Consolidation column.

4 If the task failed, check the event log for failed conditions, such as running out of disk space.

5 Correct the error, and retry the consolidation task.

   The configuration problem is resolved, and the Needs Consolidation value is No.

VMware Tools Components, Configuration Options, and Security Requirements

11

VMware Tools provides drivers and services that enhance the performance of virtual machines and make possible many of the ease-of-use features in vSphere. When VMware Tools is installed, you can configure many of these utilities and change their characteristics. In addition, to harden a virtual machine and reduce security risks as much as possible, disable the VMware Tools features that might be vulnerable to security threats.

You can use one of the following methods to configure VMware Tools.

- The command-line configuration utility in the guest operating system. You can modify VMware Tools settings, shrink virtual disks, and connect and disconnect virtual devices.
- Custom scripts.
- For NetWare virtual machines, you use the system console to configure virtual machine options.
- Menu commands and dialog boxes.

For more information about using VMware Tools, see the following documents:

- Instructions about installing and upgrading VMware Tools in vSphere, see Chapter 12, "Upgrading Virtual Machines," on page 227.
- Information about VMware Tools in hosts that are provisioned with vSphere Auto Deploy, see VMware Knowledge Base article http://kb.vmware.com/kb/2004018.
- Information about installing and configuring VMware Tools in other VMware products, see the documentation for your product.

This chapter includes the following topics:

- "Components of VMware Tools," on page 205
- "Repairing, Changing, and Uninstalling VMware Tools Components," on page 209
- "Security Considerations for Configuring VMware Tools," on page 211
- "Using vmwtool to Configure VMware Tools in a NetWare Virtual Machine," on page 214
- "Using the VMware Tools Configuration Utility," on page 215

Components of VMware Tools

VMware Tools is a suite of utilities that enhances the performance of a virtual machine. Although a guest operating system can run without VMware Tools, but you should always run the latest version of VMware Tools on your guest operating systems to access the latest VMware Tools features and updates that are not available until you install the suite.

VMware Tools Service

The VMware Tools service starts when the guest operating system starts. The service passes information between host and guest operating systems.

This program, which runs in the background, is called `vmtoolsd.exe` in Windows guest operating systems, `vmware-tools-daemon` in Mac OS X guest operating systems, and `vmtoolsd` in Linux, FreeBSD, and Solaris guest operating systems. The VMware Tools service performs the following tasks:

- Passes messages from the host to the guest operating system.
- Provides support for customization of guest operating systems as a part of the vCenter Server and other VMware products.
- Provides support for guest operating system-bound calls created with the VMware VIX API, except in Mac OS X guest operating systems.
- Runs scripts that help automate guest operating system operations. The scripts run when the power state of the virtual machine changes.
- Synchronizes the time in the guest operating system with the time on the host.
- In Windows guest operating systems, allows the pointer to move freely between the guest and the vSphere Web Client.

  On Linux guest operating systems that run Xorg 1.8 and later, this functionality is available as a standard feature.
- In Windows and Mac OS X guest operating systems, fits the screen display resolution of the guest to the screen resolution of the vSphere Web Client, if running in full screen mode. If running in windowed mode, fits the screen resolution of the guest to the size of the window on the client or host.
- In Windows and Linux guest operating systems, helps create the quiesced snapshots used by certain backup applications.
- In Windows, Linux, Solaris, and FreeBSD guest operating systems, runs custom power-on script in the virtual machine when you shut down or restart the guest operating system.
- Is one of the processes that sends a heartbeat to the VMware product to indicate that the guest operating system is running. When the virtual machine runs under ESXi or vCenter Server, a gauge for this heartbeat appears in the management interface.
- Provides support for guest operating on Windows and Linux created using the VMware VIX API, except in Mac OS X guest operating systems. For information VIX API, see the *vSphere API Reference* documentation.

VMware Tools Device Drivers

Device drivers optimize mouse operations and improve sound, graphics, and networking performance. If you do a custom VMware Tools installation or reinstallation, you can choose which drivers to install.

Which drivers are installed when you install VMware Tools also depends on the guest operating system and the VMware product. For detailed information about the features or functionality that these drivers enable, including configuration requirements, best practices, and performance, see the documentation for your VMware product. The following device drivers can be included with VMware Tools.

SVGA driver
: This virtual driver enables 32-bit displays, high display resolution, and significantly faster graphics performance. When you install VMware Tools, a virtual SVGA driver replaces the default VGA driver, which allows for only 640 X 480 resolution and 16-color graphics.

On Windows guest operating systems whose operating system is Windows Vista or later, the VMware SVGA 3D (Microsoft - WDDM) driver is installed. This driver provides the same base functionality as the SVGA driver, and it adds Windows Aero support.

SCSI driver

A VMware Paravirtual SCSI driver is included for use with paravirtual SCSI devices. Drivers for other storage adapters are either bundled with the operating system, or they are available from third-party vendors.

For example, Windows Server 2008 defaults to LSI Logic SAS, which provides the best performance for that operating system. In this case, the LSI Logic SAS driver provided by the operating system is used.

Paravirtual SCSI driver

This driver for VMware Paravirtual SCSI adapters enhances the performance of some virtualized applications.

VMXNet NIC drivers

The `vmxnet` and `vmxnet3` networking drivers improve network performance. Which driver is used depends on how you configure device settings for the virtual machine. Search the VMware Knowledge Base for information on which guest operating systems support these drivers.

When you install VMware Tools, a VMXNet NIC driver replaces the default `vlance` driver.

Mouse driver

The virtual mouse driver improves mouse performance. This driver is required if you use some third-party tools such as Microsoft Terminal Services.

Audio driver

This sound driver is required for all 64-bit Windows guest operating systems and 32-bit Windows Server 2003, Windows Server 2008, and Windows Vista guest operating systems.

Guest Introspection

If you use vSphere and vShield, you can now perform a custom VMware Tools installation to install the Guest Introspection Thin Agent component. Guest Introspection uses the hypervisor to perform antivirus scans without a bulky agent. This strategy avoids resource bottlenecks and optimizes memory use. For more information, see the *vShield Quick Start Guide*.

Memory control driver

This driver is required for memory ballooning and is recommended if you use VMware vSphere. Excluding this driver hinders the memory management capabilities of the virtual machine in a vSphere deployment.

Modules and drivers that support making automatic backups of virtual machines

If the guest operating system is Windows Vista, Windows Server 2003, or other newer Windows operating systems, a Volume Shadow Copy Services (VSS) module is installed. For other, older Windows operating systems, the Filesystem Sync driver is installed. These modules allow external third-party backup software that is integrated with vSphere to create application-consistent snapshots. During the snapshotting process, certain processes are paused and virtual machine disks are quiesced.

VMCI and VMCI Sockets drivers

The Virtual Machine Communication Interface driver allows fast and efficient communication between virtual machines and the hosts they run on. Developers can write client-server applications to the VMCI Sock (`vsock`) interface to make use of the VMCI virtual device.

VMware drivers for Linux

The drivers for Linux are automatically installed during your operating system installation, eliminating the need to separately install drivers after OS installation. VMware actively maintains the source code for VMware paravirtual drivers and kernel modules, and any Linux distributions creating new OS releases will automatically include the latest VMware drivers.

VMware does not recommend deleting or replacing existing inbox drivers for Linux that are distributed by your OS vendors. Deleting or replacing these drivers could cause conflict with future updates to the drivers. Contact your OS vendor or OS community for availability of specific updates to drivers.

See http://kb.vmware.com/kb/2073804 for information about availability, maintenance, and support policy for inbox drivers for Linux.

VMware User Process

With the VMware user process, you can use such features as copy and paste, drag and drop with VMware products that support these features.

In Linux, Solaris, and FreeBSD guest operating systems, VMware Tools uses the VMware User process executable file that implements fit-guest-to-window and Unity mode features.

The user process process starts automatically when you log in to a Windows guest operating system or, on Linux, when you start a Desktop Environment session, but you can also start it manually.

The program file for this process is called `vmtoolsd.exe` on Windows guest operating systems and `vmusr` on Linux, Solaris, and FreeBSD guest operating systems. This process supports the following tasks:

- Allows you to copy and paste text between guest operating system and the vSphere Web Client or the Workstation, Fusion, or Player host operating system. For virtual machines that are used with Workstation or Fusion, you can copy and paste files between the host operating system and Windows, Linux, Solaris, and FreeBSD guest operating systems.
- Allows you to copy and paste text between guest operating system and the vSphere Web Client.
- On Linux, Solaris, and FreeBSD guest operating systems, grabs and releases the pointer when the SVGA driver is not installed.
- On Linux, Solaris, and FreeBSD guest operating systems, fits the screen display resolution of the guest to the screen resolution of the vSphere Web Client or the Workstation, Fusion, or Player host operating system, if running in full screen mode. If running in windowed mode, fits the screen resolution of the guest to the size of the window on the client or host.
- On Linux, Solaris, and FreeBSD guest operating systems, fits the screen display resolution of the guest to the screen resolution of the vSphere Web Client, if running in full screen mode. If running in windowed mode, fits the screen resolution of the guest to the size of the window on the client or host.
- For virtual machines used with Workstation or Fusion, allows you to drag files between the host operating system and Windows, Linux, Solaris, and FreeBSD guest operating systems.
- For VMware products that support the Unity feature, allows you to open an application window in a Windows or Linux guest operating system, enter Unity mode, and have that window appear on your Workstation, Fusion, or Player host desktop like any other host application window.

Repairing, Changing, and Uninstalling VMware Tools Components

Usually when you upgrade VMware Tools, the modules are upgraded and new features are added. If some features do not work correctly after an upgrade, you must change or repair modules. On operating systems other than Windows and Linux, you must manually start the VMware User process after an upgrade.

Repair or Change Modules in Windows Virtual Machines

If you have problems with enhanced graphics display or mouse actions or with features that depend on VMware Tools, you might need to repair or modify installed modules.

Occasionally, some new modules are not installed during a VMware Tools upgrade. You can manually install new modules by modifying installed modules.

IMPORTANT Do not use the guest operating system's **Add/Remove Programs** item in the Windows Control Panel to repair or modify VMware Tools.

Prerequisites

- Power on the virtual machine.
- Log in to the guest operating system.

Procedure

1 Mount the VMware Tools virtual disc on the guest operating system.

VMware Product	Action
vSphere Client	**Inventory > Virtual Machine > Guest > Install/Upgrade VMware**
vSphere Web Client	Right-click the virtual machine and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**.
Fusion	**Virtual Machine > Install (or Upgrade) VMware Tools**
Workstation	**VM > Install (or Upgrade) VMware Tools**
Player	**Player > Manage > Install (or Upgrade) VMware Tools**

2 Mount the VMware Tools virtual disc on the guest operating system.

VMware Product	Action
vSphere Client	**Inventory > Virtual Machine > Guest > Install/Upgrade VMware Tools**
vSphere Web Client	Right-click the virtual machine and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**. a To locate a virtual machine, select a datacenter, folder, cluster, resource pool, host, or vApp. b Click the **Related Objects** tab and click **Virtual Machines**.

3 If you are performing an upgrade or reinstallation, in the Install/Upgrade VMware Tools dialog box, select **Interactive Tools Installation** or **Interactive Tools Upgrade** and click **OK**.

The process starts by mounting the VMware Tools virtual disc on the guest operating system.

4 If autorun is not enabled for the CD-ROM drive, to manually launch the VMware Tools installation wizard, click **Start > Run** and enter `D:\setup.exe`, where `D:` is your first virtual CD-ROM drive.

5 On the Welcome page of the wizard, click **Next**.

6 Specify whether to repair or modify the modules.

- Click **Repair** to repair the files, registry settings, and so on of components that are already installed.
- Click **Modify** to specify which modules are installed.

7 Follow the on-screen instructions.

What to do next

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

Uninstall VMware Tools

If the upgrade process of VMware Tools is incomplete, you can uninstall and then reinstall the VMware Tools.

In a vSphere and open-vm-tools deployment, if you decide to use packages specific to Linux operating systems to manage VMware Tools, and if you already used vSphere to install VMware Tools, you must uninstall the existing VMware Tools. For more information about Linux OSPs for VMware Tools, see "Operating System Specific Packages for Linux Guest Operating Systems," on page 240.

Prerequisites

- Power on the virtual machine.
- Log in to the guest operating system.

Procedure

◆ Select a method to uninstall VMware Tools.

Operating System	Action
Windows 7, 8, 8.1	In the guest operating system, select **Programs > Uninstall a program**.
Windows Vista and Windows Server 2008	In the guest operating system, select **Programs and Features > Uninstall a program**.
Windows XP and earlier	In the guest operating system, select **Add/Remove Programs**.
Linux, Solaris, FreeBSD, NetWare	Log in as root and enter **`vmware-uninstall-tools.pl`** in a terminal window.
Mac OS X Server	Use the **Uninstall VMware Tools** application, found in `/Library/Application Support/VMware Tools`.

What to do next

Reinstall VMware Tools.

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

VMware Tools in Linux, Solaris, and FreeBSD guest operating systems uses the VMware User process executable file. This program implements the fit-guest-to-window feature and Unity mode, among other features.

Normally, this process starts after you configure VMware Tools, log out of the desktop environment, and log back in. The `vmware-user` program is located in the directory in which you selected to install binary programs, which defaults to `/usr/bin`. The startup script that you need to modify depends on your system. You must start the process manually in the following environments:

- If you run an X session without a session manager. For example, if you use `startx` to start a desktop session and do not use `xdm`, `kdm`, or `gdm`.
- If you are using an older version of GNOME without `gdm` or `xdm`.

- If you are using a session manager or environment that does not support the Desktop Application Autostart Specification, available from http://standards.freedesktop.org.
- If you upgrade VMware Tools.

Procedure

◆ Start the VMware User process.

Option	Action
Start the VMware User process when you start an X session.	Add `vmware-user` to the appropriate X startup script, such as the `.xsession` or `.xinitrc` file.
Start the process after a VMware Tools software upgrade, or if certain features are not working.	Open a terminal window and type the **`vmware-user`** command.

Security Considerations for Configuring VMware Tools

Some VMware Tools settings might expose security risks. For example, VMware Tools enables you to connect virtual devices such as serial and parallel ports to virtual machines. A connected device could be a potential channel of attack. To harden a virtual machine and reduce security risks as much as possible, disable the VMware Tools features that might be vulnerable to security threats.

For complete information about securely deploying VMware vSphere in a production environment, including security recommendations for hosts, virtual machines, management components, and a networking infrastructure, see the *vSphere Hardening Guide*. VMware Tools settings relate only to the virtual machine aspect of a deployment.

Virtual machines are encapsulated in a small number of files. One of the important files is the configuration file (`.vmx` file). This file governs the performance of the virtual hardware and other settings. You can use several methods to see and modify the configuration settings:

- Open the `.vmx` file directly in a text editor.
- Use the vSphere Web Client to edit virtual machine settings. In the vSphere Web Client, editing these configuration parameters is an advanced option in the virtual machine Edit Settings dialog box.
- Use the vSphere Client to edit virtual machine settings. In the vSphere Client, editing these configuration parameters is an advanced option in the virtual machine Edit Settings dialog box.
- Use a vSphere API-based tool, such as Power CLI, to view and modify `.vmx` parameters.

After you edit a setting, the change does not take effect until you restart the virtual machine.

Review the following list of potential security threats and the corresponding VMware Tools parameters to set in the virtual machine's `.vmx` file. The defaults for many of these parameters are already set to protect virtual machines from these threats.

Threats Associated with Unprivileged User Accounts

Disk shrinking feature

Shrinking a virtual disk reclaims unused disk space. Users and processes without root or administrator privileges can invoke this procedure. Because the disk-shrinking process can take considerable time to complete, invoking the disk-shrinking procedure repeatedly can cause a denial of service. The virtual disk is unavailable during the shrinking process. Use the following `.vmx` settings to disable disk shrinking:

```
isolation.tools.diskWiper.disable = "TRUE"
isolation.tools.diskShrink.disable = "TRUE"
```

Copy and paste feature

By default, the ability to copy and paste text, graphics, and files is disabled, as is the ability to drag and drop files. When this feature is enabled, you can copy and paste rich text and, depending on the VMware product, graphics and files from your clipboard to the guest operating system in a virtual machine. That is, as soon as the console window of a virtual machine gains focus, nonprivileged users and processes running in the virtual machine can access the clipboard on the computer where the console window is running. To avoid risks associated with this feature, retain the following `.vmx` settings, which disable copying and pasting:

```
isolation.tools.copy.disable = "TRUE"
isolation.tools.paste.disable = "TRUE"
```

Threats Associated with Virtual Devices

Connecting and modifying devices

By default, the ability to connect and disconnect devices is disabled. When this feature is enabled, users and processes without root or administrator privileges can connect devices such as network adapters and CD-ROM drives, and they can modify device settings. That is, a user can connect a disconnected CD-ROM drive and access sensitive information on the media left in the drive. A user can also disconnect a network adapter to isolate the virtual machine from its network, which is a denial of service. To avoid risks associated with this feature, retain the following `.vmx` settings, which disable the ability to connect and disconnect devices or to modify device settings:

```
isolation.device.connectable.disable = "TRUE"
isolation.device.edit.disable = "TRUE"
```

Threats Associated with Virtual Machine Information Flow

Configuring virtual machine log number

Depending on your log settings, new log files might be created each time the old file is larger than 100KB. Uncontrolled logging can lead to denial of service if the datastore runs out of disk space. VMware recommends saving 10 log files. By default, the maximum size for log files is 100KB, and you cannot change that value at the virtual machine level. Use the following `.vmx` setting to set number of log files:

```
vmx.log.keepOld = "10"
```

You can limit the number of log files for all virtual machines on a host by editing the `/etc/vmware/config` file. If the `vmx.log.keepOld` property is not defined in the file, you can add it. For example, to keep ten log files for each virtual machine, add the following to `/etc/vmware/config`:

```
vmx.log.keepOld = "10"
```

You can also use a PowerCLI script to change this property on all the virtual machines on a host.

A more extreme strategy is to disable logging altogether for the virtual machine. Disabling logging makes troubleshooting challenging and support difficult. Do not consider disabling logging unless the log file rotation approach proves insufficient. Use the following `.vmx` setting to disable logging altogether:

```
logging = "FALSE"
```

VMX file size

By default the configuration file is limited to a size of 1MB because uncontrolled size for the file can lead to a denial of service if the datastore runs out of disk space. Informational messages are sometimes sent from the virtual machine to the `.vmx` file. These setinfo messages define virtual machine characteristics or identifiers by writing name-value pairs to the file. You might need to increase the size of the file if large amounts of custom information must be stored in the file. The property name is `tools.setInfo.sizeLimit`, and you specify the value in kilobytes. Retain the following `.vmx` setting:

```
tools.setInfo.sizeLimit = "1048576"
```

Sending performance counters into PerfMon

You can integrate virtual machine performance counters for CPU and memory into PerfMon for Linux and Microsoft Windows guest operating systems. This feature makes detailed information about the physical host available to the guest operating system. An adversary could potentially use this information to inform further attacks on the host. By default this feature is disabled. Retain the following `.vmx` setting to prevent host information from being sent to the virtual machine:

```
tools.guestlib.enableHostInfo = "FALSE"
```

This setting blocks some but not all metrics. If you set this property to FALSE, the following metrics are blocked:

- GUESTLIB_HOST_CPU_NUM_CORES
- GUESTLIB_HOST_CPU_USED_MS
- GUESTLIB_HOST_MEM_SWAPPED_MB
- GUESTLIB_HOST_MEM_SHARED_MB
- GUESTLIB_HOST_MEM_USED_MB
- GUESTLIB_HOST_MEM_PHYS_MB
- GUESTLIB_HOST_MEM_PHYS_FREE_MB
- GUESTLIB_HOST_MEM_KERN_OVHD_MB
- GUESTLIB_HOST_MEM_MAPPED_MB

- GUESTLIB_HOST_MEM_UNMAPPED_MB

Features not exposed in vSphere that could cause vulnerabilities

Because VMware virtual machines run in many VMware products in addition to vSphere, some virtual machine parameters do not apply in a vSphere environment. Although these features do not appear in vSphere user interfaces, disabling them reduces the number of vectors through which a guest operating system could access a host. Use the following `.vmx` setting to disable these features:

```
isolation.tools.unity.push.update.disable = "TRUE"
isolation.tools.ghi.launchmenu.change = "TRUE"
isolation.tools.ghi.autologon.disable = "TRUE"
isolation.tools.hgfsServerSet.disable = "TRUE"
isolation.tools.memSchedFakeSampleStats.disable = "TRUE"
isolation.tools.getCreds.disable = "TRUE"
```

Using vmwtool to Configure VMware Tools in a NetWare Virtual Machine

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

Although you cannot use the VMware Tools configuration utility in a NetWare virtual machine, you can use the `vmwtool` command to achieve some of the same functionality. This command has the following syntax:

`vmwtool` *`command`*

Table 11-1. vmwtool Commands

vmwtool Command	Description
`help`	Displays a summary of VMware Tools commands and options in a NetWare guest operating system.
`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. By default, floppy drive is not connected when the virtual machine powers on.
`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.

Table 11-1. vmwtool Commands (Continued)

vmwtool Command	Description
`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 guest operating systems. 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.

Using the VMware Tools Configuration Utility

The VMware Tools configuration utility is a command-line interface that you can use in the guest operating system to modify VMware Tools settings, shrink virtual disks, and connect and disconnect virtual devices.

The VMware Tools configuration utility provides a command-line interface for functionality that was previously available only in the VMware Tools control panel. The name of this program depends on the guest operating system.

Table 11-2. VMware Tools Configuration Utilities for Guest Operating Systems

Guest Operating System	Utility
Windows	`VMwareToolboxCmd.exe`
Mac OS X	`vmware-tools-cli` Because the VMware Tools installer does not modify any PATH environment variables on Mac OS X operating systems, you must type `./` before the command.
Linux, FreeBSD, Solaris	`vmware-toolbox-cmd`

Use the utility's `help` command to display complete usage information and syntax.

The VMware Tools configuration utility is included in the following VMware products:

- VMware vSphere 4.1 and later
- VMware Workstation 7.0 and later
- VMware Fusion 3.0 and later
- VMware Player 3.0 and later
- VMware ACE 2.6 and later

Configure Time Synchronization Between Guest and Host Operating Systems

When you turn on periodic time synchronization, VMware Tools sets the time of the guest operating system to be the same as the time of the host.

After time synchronization occurs, VMware Tools checks once every minute to determine whether the clocks on the guest and host operating systems still match. If not, the clock on the guest operating system is synchronized to match the clock on the host.

If the clock on the guest operating system falls behind the clock on the host, VMware Tools moves the clock on the guest forward to match the clock on the host. If the clock on the guest operating system is ahead of the clock on the host, VMware Tools causes the clock on the guest to run more slowly until the clocks are synchronized.

Native time synchronization software, such as Network Time Protocol (NTP) for Linux and the Mac OS X, or Microsoft Windows Time Service (Win32Time) for Windows, is typically more accurate than VMware Tools periodic time synchronization and is therefore preferred.

IMPORTANT Use only one form of periodic time synchronization in your guests. If you are using native time synchronization software, turn off VMware Tools periodic time synchronization.

Regardless of whether you turn on VMware Tools periodic time synchronization, time synchronization occurs after certain operations:

- When the VMware Tools daemon is started, such as during a reboot or power on operation
- When resuming a virtual machine from a suspend operation
- After reverting to a snapshot
- After shrinking a disk

When the operating system starts or reboots, and when you first turn on periodic time synchronization, synchronization can be either forward or backward in time. For other events, synchronization is forward in time.

To disable time synchronization completely, you must edit the configuration file (`.vmx` file) of the virtual machine and set several synchronization properties to FALSE.

Prerequisites

- Disable other periodic time synchronization mechanisms. For example, some guests might have NTP or Win32Time clock synchronization turned on by default.
- If you plan to script the commands used in this procedure and need to know what the exit codes are, see "Exit Codes for the VMware Tools Configuration Utility," on page 225.

NOTE Mac OS X guests use NTP and do not become out of sync with the host. For Mac OS X guests, you do not need to turn on VMware Tools time synchronization.

Procedure

1 Open a command prompt or terminal in the guest operating system.

2 Change to the VMware Tools installation directory.

Operating System	Default Path
Windows	`C:\Program Files\VMware\VMware Tools`
Linux and Solaris	`/usr/sbin`
FreeBSD	`/usr/local/sbin`
Mac OS X	`/Library/Application Support/VMware Tools`

3 Type the command to determine whether time synchronization is enabled.

```
utility-name timesync status
```

For *utility-name* use the guest-specific program name.

Operating System	Program Name
Windows	`VMwareToolboxCmd.exe`
Linux, Solaris, and FreeBSD	`vmware-toolbox-cmd`

4 Type the command to enable or disable periodic time synchronization.

```
utility-name timesync subcommand
```

For *subcommand*, use `enable` or `disable`.

The VMware Tools service enables or disables periodic time synchronization, as you specified. Disabling periodic time synchronization does not disable all VMware Tools time synchronization.

What to do next

If you need to keep a fictitious time in a virtual machine, so that the clock in the guest operating system is never synchronized with that on the host, disable time synchronization completely.

Disable Time Synchronization Completely

A virtual machine occasionally synchronizes time with the host even if you do not turn on periodic time synchronization. To completely disable time synchronization, you must set some properties in the virtual machine configuration file.

Prerequisites

Power off the virtual machine.

Procedure

1 Open the configuration (`.vmx`) file of the virtual machine with a text editor.

2 Add lines for the time synchronization properties and set the properties to FALSE.

```
tools.syncTime = "FALSE"
time.synchronize.continue = "FALSE"
time.synchronize.restore = "FALSE"
time.synchronize.resume.disk = "FALSE"
time.synchronize.shrink = "FALSE"
time.synchronize.tools.startup = "FALSE"
```

3 Save and close the file.

What to do next

Power on the virtual machine.

Connect or Disconnect a Virtual Device

You can connect and disconnect removable devices such as floppy drives, DVD/CD-ROM drives, ISO images, USB devices, sound adapters, and network adapters.

IMPORTANT Some restrictions exist for connecting devices:

- Some devices cannot be shared between the host and guest operating systems or between two guest operating systems. For example, only one virtual machine or the host can access the floppy drive at any one time.
- The controls for connecting and disconnecting devices might not be available, depending on whether your system administrator has enabled them.

You can run the configuration utility to connect and disconnect virtual devices. For security reasons, this ability is disabled by default. To connect or disconnect devices, you must first change the settings in the configuration file.

Prerequisites

If you plan to script commands to connect or disconnect a virtual device, and need to know what the exit codes are, see "Exit Codes for the VMware Tools Configuration Utility," on page 225.

Procedure

1 Configure the virtual machine to allow connecting and disconnecting devices.

   a Open the configuration (`.vmx`) file of the virtual machine with a text editor.

   b If the following properties are not listed in the file, add them and set them to FALSE.

```
isolation.device.connectable.disable = "FALSE"
isolation.device.edit.disable = "FALSE"
```

   c Save and close the file.

2 Open a command prompt or terminal in the guest operating system.

3 Change to the VMware Tools installation directory.

Operating System	Default Path
Windows	`C:\Program Files\VMware\VMware Tools`
Linux and Solaris	`/usr/sbin`
FreeBSD	`/usr/local/sbin`
Mac OS X	`/Library/Application Support/VMware Tools`

4 Type ***utility-name* device list** to list available devices.

   For *utility-name*, use the guest-specific program name.

Operating System	Utility Name
Windows	`VMwareToolboxCmd.exe`
Linux, Solaris, and FreeBSD	`vmware-toolbox-cmd`
Mac OS X	`vmware-tools-cli`

5 (Optional) Type the command to determine whether a device is connected.

   utility-name* device status *device-name

   For *device-name*, use one of the names displayed when you used the `list` subcommand.

6 Type the command to connect or disconnect the device.

```
utility-name device device-name subcommand
```

Option	Action
device-name	Use one of the names displayed when you used the `list` subcommand.
subcommand	Use `enable` or `disable`.

The device is connected or disconnected, as you specified.

Shrink a Virtual Disk

Shrinking a virtual disk reclaims unused space in the virtual disk and reduces the amount of space that the virtual disk occupies on the host.

Shrinking disks is not allowed under the following circumstances:

- The virtual machine is hosted on an ESX/ESXi host. ESX/ESXi can shrink the size of a virtual disk only when a virtual machine is exported. The space occupied by the virtual disk on the server, however, does not change.
- The virtual machine has a Mac OS X guest operating system.
- You preallocated all the disk space to the virtual disk when you created it.
- The virtual machine contains a snapshot.

  The exception is if the virtual machine is used in VMware Fusion 4 and has a Windows guest operating system. In this case, you can use the **Clean Up Virtual Machine** feature in Fusion to shrink disks.
- The virtual machine is a linked clone or the parent of a linked clone.
- The virtual disk is an independent disk in nonpersistent mode.
- The file system is a journaling file system, such as an `ext4`, `xfs`, or `jfs` file system.

Shrinking a disk is a two-step process. In the preparation step, VMware Tools reclaims all unused portions of disk partitions, such as deleted files, and prepares them for shrinking. This phase takes place in the guest operating system. During this phase, you can still interact with the virtual machine.

In the shrink step, 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. The shrink step takes place outside the virtual machine and takes considerable time, depending on the size of the disk. The virtual machine stops responding while VMware Tools shrinks the disks.

Newer versions of some VMware products might include a button or menu item that performs the same function as the shrink-disk command. For example, Workstation includes a **Compact** menu item that you can use when the virtual machine is powered off. VMware Fusion 4 includes a **Clean Up Virtual Machine** button that can shrink disks even if you have snapshots.

Under some conditions, the ability to use a shrink-disk command might be considered a security risk. To configure a setting that disables the ability to shrink disk, see "Threats Associated with Unprivileged User Accounts," on page 212.

Prerequisites

- On Linux, Solaris, and FreeBSD guest operating systems, log in as root. 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.
- On Windows guests, log in as an administrator.

- Verify that the host has free disk space equal to the size of the virtual disk that you plan to shrink.

Procedure

1 Open a command prompt or terminal in the guest operating system.

2 Change to the VMware Tools installation directory.

Operating System	Default Path
Windows	`C:\Program Files\VMware\VMware Tools`
Linux and Solaris	`/usr/sbin`
FreeBSD	`/usr/local/sbin`
Mac OS X	`/Library/Application Support/VMware Tools`

3 Type the command to list available mount points.

```
utility-name disk list
```

For *utility-name* use the guest-specific program name.

Operating System	Utility Name
Windows	`VMwareToolboxCmd.exe`
Linux, Solaris, and FreeBSD	`vmware-toolbox-cmd`

4 Type the command to shrink the disk at a specified mount point.

```
utility-name disk shrink mount-point
```

For *mount-point*, use one of the mount points displayed when you used the `list` subcommand.

Using Custom VMware Tools Scripts

You can associate custom scripts with power operations.

When VMware Tools is installed, 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. For example, when you power off a virtual machine, by default the `poweroff-vm-default` script runs.

Use Custom VMware Tools Scripts in Windows Guests

On Windows guest operating systems, you can write scripts to automate guest operating system operations when you change the power state of a virtual machine.

For Windows guest operating systems, you can write new scripts or modify default scripts, save them with new names, and configure VMware Tools to use your custom script instead of the default script.

The VMware Tools service, or daemon (`vmtoolsd`), runs scripts. Because `vmtoolsd` runs as root on Linux, Mac, Solaris, and FreeBSD, and as System on Windows, the scripts run in a separate session from the session of the logged-in user. The VMware Tools daemon does not detect desktop sessions, which means that it cannot display graphical applications. Do not attempt to use custom scripts to display graphical applications.

Important You cannot run scripts on Windows NT, Me, Windows 98, and Windows 95 guest operating systems.

Prerequisites

- Familiarize yourself with the default VMware Tools scripts. See "Default VMware Tools Scripts," on page 222.

- If you plan to script commands and need to know what the exit codes are, see "Exit Codes for the VMware Tools Configuration Utility," on page 225.

Procedure

1 Write a new script or modify default scripts and save them as `.bat` files with new names.

The default scripts for power-on and power-off operations are placeholders only. These scripts are located in the `Program Files\VMware\VMware Tools` directory.

The scripts for suspend and resume operations contain a line that releases or renews the IP address for the virtual machine. You must add this line first when you write custom scripts for these operations.

Default Script	Required IP Address Line
`suspend`	`@%SYSTEMROOT%\system32\ipconfig /release`
`resume`	`@%SYSTEMROOT%\system32\ipconfig /renew`

2 Open a command prompt in the guest operating system.

3 Change directories to the VMware Tools installation directory.

The default installation directory is `C:\Program Files\VMware\VMware Tools`.

4 Type the command to enable the script.

```
VMwareToolboxCmd.exe script script-name enable
```

5 Type the command to use the custom script that you created.

```
VMwareToolboxCmd.exe script script-name set script-path
```

For *script-path*, use the full path to the file, such as, `C:\Temp\poweron-my-vm.bat`.

6 Type the command to verify that the custom script that you specified is now being used.

```
VMwareToolboxCmd.exe script script-name current
```

The VMware Tools service runs the script whenever the specified power operation occurs.

Use Custom Scripts in Operating Systems Other Than Windows

On Linux, Mac OS X, Solaris, and FreeBSD guest operating systems, you can write scripts to automate guest operating system operations when you change the power state of a virtual machine.

For Linux, Mac OS X, Solaris, and FreeBSD guests, you can write scripts and place them in a certain directory, and then VMware Tools runs your scripts in addition to the default scripts. For power-on and resume operations, the default scripts run before the custom scripts. For suspend and power-off, the default scripts run after the custom scripts. This way, VMware Tools stops services only after the custom scripts finish their work and, conversely, restores the same services before the custom scripts attempt to use the services.

The VMware Tools service, or daemon (`vmtoolsd`), runs scripts. Because `vmtoolsd` runs as root on Linux, Mac, Solaris, and FreeBSD, and as System on Windows, the scripts run in a separate session from the session of the logged-in user. The VMware Tools daemon does not detect desktop sessions, which means that it cannot display graphical applications. Do not attempt to use custom scripts to display graphical applications.

Prerequisites

- Familiarize yourself with the default VMware Tools scripts. See "Default VMware Tools Scripts," on page 222.
- On Linux, Mac OS X, Solaris, and FreeBSD guest operating systems, to test, edit, or disable the running of a script, log in as root.

- On Linux, Mac OS X, Solaris, and FreeBSD guest operating systems, to edit a script, make sure `xterm` and `vi` are installed in the guest operating system and are in your PATH, or specify which editor to use by setting the EDITOR environment variable.
- If you plan to script commands and need to know what the exit codes are, see "Exit Codes for the VMware Tools Configuration Utility," on page 225.

Procedure

1 Log in to the guest operating system as root.

2 Write the custom scripts and place them in the correct directory, as instructed by the comments in the default script files for each power operation.

Guest Operating System	Directory
Linux, Solaris, FreeBSD	`/etc/vmware-tools`
Mac OS X	`/Library/Application Support/VMware Tools`

Do not make changes to the default scripts.

The VMware Tools service runs the script whenever the specified power operation occurs.

Default VMware Tools Scripts

VMware Tools includes one or more default scripts for each power state. The default script behavior depends in part on the guest operating system.

Microsoft Windows Guest Operating Systems

On most Microsoft Windows guest operating systems, the default script that runs when you suspend a virtual machine releases the IP address of the virtual machine. The default script that runs when you resume a virtual machine renews the IP address of the virtual machine. This behavior affects only virtual machines configured to use DHCP.

On Windows guest operating systems, the default scripts are located in the `Program Files\VMware\VMware Tools` folder.

Important You cannot run scripts on Windows NT, Me, Windows 98, and Windows 95 guest operating systems.

Linux, Mac OS X, Solaris, and Free BSD Guest Operating Systems

On most Linux, Mac OS X, Solaris, and FreeBSD guest operating systems, the default script that runs when you suspend a virtual machine stops networking for the virtual machine. The default script that runs when you resume a virtual machine starts networking for the virtual machine.

On Linux, Solaris, and FreeBSD guest operating systems, the default scripts are located in the `/etc/vmware-tools` directory. On Mac OS X operating systems the default scripts are located in the `/Library/Application Support/VMware Tools` directory.

You cannot run scripts on NetWare guest operating systems.

Table 11-3. Default VMware Tools Scripts

Script Name	Description
`poweroff-vm-default`	Runs when the virtual machine is being powered off or reset. Has no effect on networking for the virtual machine.
`poweron-vm-default`	Runs when the virtual machine is being powered on rather than resumed. Also runs after virtual machine restarts. Has no effect on networking for the virtual machine.
`resume-vm-default`	Runs when the virtual machine is resumed after it was suspended. On Windows guest operating systems, if the virtual machine is configured to use DHCP, this script renews the IP address of the virtual machine. On Linux, Mac OS X, Solaris, and FreeBSD guest operating systems, this script starts networking for the virtual machine.
`suspend-vm-default`	Runs when the virtual machine is being suspended. On Windows guest operating systems, if the virtual machine is configured to use DHCP, this script releases the IP address of the virtual machine. On Linux, Mac OS X, Solaris, and FreeBSD , this script stops networking for the virtual machine.

For information about how to configure power operations, see the documentation for the VMware product you are using.

Disable a VMware Tools Script

Default scripts for suspending and resuming a virtual machine are written to work together. If you disable the script for one of these actions, you must also disable the script for the other action.

Important You cannot run scripts on Windows NT, Me, Windows 98, and Windows 95 guest operating systems.

Prerequisites

On Linux, Solaris, and FreeBSD guest operating systems, to test, edit, or disable the running of a script, log in as root.

Procedure

1 Open a command prompt or terminal in the guest operating system.

2 Change to the VMware Tools installation directory.

Operating System	Default Path
Windows	`C:\Program Files\VMware\VMware Tools`
Linux and Solaris	`/usr/sbin`
FreeBSD	`/usr/local/sbin`
Mac OS X	`/Library/Application Support/VMware Tools`

3 Type the command to disable the script.

```
utility-name script script-name disable
```

Option	Action
***utility-name* (On Windows)**	Use `VMwareToolboxCmd.exe`.
***utility-name* (On Linux, Solaris, and FreeBSD)**	Use `vmware-toolbox-cmd`.
script-name	Use `power`, `resume`, `suspend`, or `shutdown`.

4 (Optional) If you disabled the script for suspending a virtual machine, repeat this procedure.

5 (Optional) If you disabled the script for resuming a virtual machine, also disable the script for suspending the virtual machine.

Retrieve Status Information About the Virtual Machine

You can display information about host time and CPU speed. For virtual machines hosted in a vSphere environment, you can display additional information about memory and CPU reservations and limits.

Prerequisites

- Determine what status information to display. See "Subcommands for the stat Command," on page 225.
- If you plan to script commands and need to know what the exit codes are, see "Exit Codes for the VMware Tools Configuration Utility," on page 225.

Procedure

1 Open a command prompt or terminal in the guest operating system.

2 Change to the VMware Tools installation directory.

Operating System	Default Path
Windows	`C:\Program Files\VMware\VMware Tools`
Linux and Solaris	`/usr/sbin`
FreeBSD	`/usr/local/sbin`
Mac OS X	`/Library/Application Support/VMware Tools`

3 Type the command to display the status information.

```
utility-name stat subcommand
```

Option	Action
***utility-name* (On Windows)**	Use `VMwareToolboxCmd.exe`.
***utility-name* (On Linux, Solaris, and FreeBSD)**	Use `vmware-toolbox-cmd`.
***utility-name* (On Mac OS X)**	Use `vmware-tools-cli`.
subcommand	Use `hosttime` or `speed`, or, if applicable, one of the subcommands available for virtual machines hosted in a vSphere environment.

Subcommands for the stat Command

You can use the `vmware-toolbox-cmd help stat` command to display information such as host time and CPU speed. Additional subcommands are available for virtual machines in a vSphere environment.

Table 11-4. Subcommands for the stat Command

Subcommand Name	Description
`hosttime`	Displays the date and time on the host.
`speed`	Displays the CPU speed, in MHz.
`balloon`	Displays the amount of memory that is currently reclaimed from the virtual machine through ballooning, in megabytes.
`swap`	Displays the current amount of memory swapped out to the virtual machine's swap file, in megabytes.
`memlimit`	Displays memory limit information, in megabytes.
`memres`	Displays memory reservation information, in megabytes.
`cpures`	Displays CPU reservation information, in MHz.
`cpulimit`	Displays CPU limit information, in MHz.
`sessionid`	Displays the current session ID.

Table 11-5. Subcommands for the stat Command

Subcommand Name	Description
`hosttime`	Displays the date and time on the host.
`speed`	Displays the CPU speed, in MHz.

Exit Codes for the VMware Tools Configuration Utility

You can use exit codes to integrate the VMware Tools configuration utility commands with a scripting tool.

Table 11-6. Exit Codes

Code Number	Applicable Command	Description
0	All commands	The command was successful.
1	All commands	Always indicates that an error occurred. For the `shrink` command, 1 indicates that although shrinking is enabled, the shrink command cannot be carried out.
64	All commands	The command-line argument is not valid.
66	`script`	The file name does not exist.
69	`device` and `stat`	For the `device` command, 69 indicates that the specified device does not exist. Use the `list` subcommand to display valid names of devices. For the `stat` command, 69 indicates that the program could not communicate with the host (EX_UNAVAILABLE).
75	`stat`	The host does not support the query, perhaps because the host is not an ESX/ESXi host (EX_TEMPFAIL).
77	All commands	Permission errors.

Upgrading Virtual Machines 12

After you perform an ESX/ESXi upgrade, you can upgrade all of the virtual machines that reside on the host to take advantage of new features.

To determine whether your virtual machines are compatible with the new version of ESXi, see "Virtual Machine Compatibility," on page 89. For a list of hardware features available to virtual machines with each ESXi compatibility setting, see "Hardware Features Available with Virtual Machine Compatibility Settings," on page 93.

The first step in upgrading virtual machines is to upgrade VMware Tools. If the virtual machines do not have VMware Tools installed, you can use the VMware Tools upgrade procedure to install VMware Tools. After you install or upgrade VMware Tools, upgrade the virtual machine compatibility.

NOTE Do not use `vmware-vmupgrade.exe` to upgrade virtual machines.

VMware offers the following tools for upgrading virtual machines:

vSphere Web Client Requires you to perform the virtual machine upgrade one step at a time, but does not require vSphere Update Manager.

vSphere Update Manager Automates the process of upgrading and patching virtual machines, ensuring that the steps occur in the correct order. You can use Update Manager to directly upgrade virtual machine hardware, VMware Tools, and virtual appliances. You can also patch and update third-party software running on the virtual machines and virtual appliances. See the *Installing and Administering VMware vSphere Update Manager* documentation.

This chapter includes the following topics:

- "Upgrading VMware Tools," on page 228
- "Installing VMware Tools," on page 229
- "Planning Downtime for Virtual Machines," on page 231
- "Downtime for Upgrading Virtual Machines," on page 231
- "Manually Install or Upgrade VMware Tools in a Windows Virtual Machine," on page 232
- "Automate VMware Tools Installation for Multiple Windows Virtual Machines," on page 234
- "Manually Install or Upgrade VMware Tools in a Linux Virtual Machine," on page 238
- "Operating System Specific Packages for Linux Guest Operating Systems," on page 240
- "Manually Install or Upgrade VMware Tools in a Mac OS X Virtual Machine," on page 241
- "Manually Install or Upgrade VMware Tools in a Solaris Virtual Machine," on page 241

- "Manually Install or Upgrade VMware Tools in a NetWare Virtual Machine," on page 243
- "Manually Install or Upgrade VMware Tools in a FreeBSD Virtual Machine," on page 245
- "Upgrade VMware Tools," on page 246
- "Perform an Automatic Upgrade of VMware Tools," on page 247
- "Upgrade the Compatibility for Virtual Machines," on page 248
- "Schedule a Compatibility Upgrade for Virtual Machines," on page 249

Upgrading VMware Tools

You can upgrade VMware Tools manually, or you can configure virtual machines to check for and install newer versions of VMware Tools.

The guest operating system checks the version of VMware Tools when you power on a virtual machine. In the vSphere Web Client, the status bar of your virtual machine displays a message when a new version is available. The displayed version also is the version of the ESXi the VMware Tools is bundled with.

In Windows virtual machines, you can set VMware Tools to notify you when an upgrade is available. If this notification option is enabled, the VMware Tools icon in the Windows taskbar includes a yellow caution icon when a VMware Tools upgrade is available.

To install a VMware Tools upgrade, you can use the same procedure that you used for installing VMware Tools the first time. Upgrading VMware Tools means installing a new version.

For Windows and Linux guest operating systems, you can configure the virtual machine to automatically upgrade VMware Tools. Although the version check is performed when you power on the virtual machine, on Windows guest operating systems, the automatic upgrade occurs when you power off or restart the virtual machine. The status bar displays the message `Installing VMware Tools ...` when an upgrade is in progress.

Important After you upgrade VMware Tools on Linux guest operating systems, new network modules are available but are not used until you either restart the guest operating system or stop networking, unload and reload the VMware networking kernel modules, and restart networking. This behavior means that even if VMware Tools is set to automatically upgrade, you must restart or reload network modules to make new features available.

This strategy avoids network interruptions and allows you to install VMware Tools over SSH.

Upgrading VMware Tools on Windows guest operation systems automatically installs the WDDM graphics drivers. The WDDM graphics driver makes the sleep mode available in guest OS power settings to adjust the sleep options. For example, you can use the sleep mode setting **Change when the computer sleeps** to configure your guest OS to automatically go to sleep mode after a certain time or prevent your guest OS from automatically switching to sleep mode after being idle for some time.

For vSphere virtual machines, you can use one of the following processes to upgrade multiple virtual machines at the same time.

You can use one of the following processes to upgrade multiple virtual machines at the same time.

- Log in to vCenter Server, select a host or cluster, and on the **Virtual Machines** tab specify the virtual machines on which to perform a VMware Tools upgrade.
- Use Update Manager to perform an orchestrated upgrade of virtual machines at the folder or datacenter level.

Some features in a particular release of a VMware product might depend on installing or upgrading to the version of VMware Tools included in that release. Upgrading to the latest version of VMware Tools is not always necessary, however, VMware highly recommends that you upgrade to the most updated version of the VMware Tools. Newer versions of VMware Tools are compatible with several ESXi host versions. To avoid unnecessary upgrades, evaluate whether the added features and capabilities are necessary for your environment. See "Hardware Features Available with Virtual Machine Compatibility Settings," on page 93. However, VMware highly recommends installing and using the latest version of VMware Tools.

Some features in a particular release of a VMware product might depend on installing or upgrading to the version of VMware Tools included in that release. Upgrading to the latest version of VMware Tools is not always necessary. Newer versions of VMware Tools are compatible with several host versions. To avoid unnecessary upgrades, evaluate whether the added features and capabilities are necessary for your environment.

Table 12-1. Virtual Machine Compatibility Options

Compatibility	Description
ESXi 6.0 and later	This virtual machine (hardware version 11) is compatible with ESXi 6.0 and later.
ESXi 5.5 and later	This virtual machine (hardware version 10) is compatible with ESXi 5.5 and later.
ESXi 5.1 and later	This virtual machine (hardware version 9) is compatible with ESXi 5.1 and later.
ESXi 5.0 and later	This virtual machine (hardware version 8) is compatible with ESXi 5.0 and 5.1.
ESX/ESXi 4.x and later	This virtual machine (hardware version 7) is compatible with ESX/ ESXi 4.x, ESXi 5.0, and ESXi 5.1.
ESX/ESXi 3.5 and later	This virtual machine (hardware version 4) is compatible with ESX/ESX 3.5. ESX/ESX 4.x, and ESXi 5.1. It is also compatible with VMware Server 1.0 and later. You cannot create a virtual machine with ESX/ESXi 3.5 compatibility on ESXi 5.0.

For more information, see the documentation for your specific VMware product.

Installing VMware Tools

Although your guest operating systems can run without VMware Tools, many VMware features are not available until you install VMware Tool. When you install VMware Tools, the utilities in the tools suite enhances the performance of your virtual machine's guest operating system and improves the management of your virtual machines.

The installers for VMware Tools are ISO image files. An ISO image file looks like a CD-ROM to your guest operating system. Each type of guest operating system, including Windows, Linux, Solaris, FreeBSD, and NetWare, has an ISO image file. When you select the command to install or upgrade VMware Tools, the virtual machine's first virtual CD-ROM disk drive temporarily connects to the VMware Tools ISO file for your guest operating system.

If you are using VMware Fusion, Player, or Workstation, you can use the Windows Easy Install or Linux Easy Install feature to install VMware Tools as soon as the operating system is finished installing.

If you are using VMware Fusion, Player, or Workstation, the most recent versions of the ISO files are stored on a VMware Web site. When you select the command to install or upgrade VMware Tools, the VMware product determines whether it has downloaded the most recent version of the ISO file for the specific operating system. If the latest version was not downloaded or if no VMware Tools ISO file for that operating system was ever downloaded, you are prompted to download the file.

- For information about installing or upgrading VMware Tools in Windows virtual machines, see "Manually Install or Upgrade VMware Tools in a Windows Virtual Machine," on page 232 and "Automate VMware Tools Installation for Multiple Windows Virtual Machines," on page 234.
- For information about installing or upgrading VMware Tools in Linux virtual machines, see "Manually Install or Upgrade VMware Tools in a Linux Virtual Machine," on page 238.

- For information about installing or upgrading VMware Tools in Mac OS X virtual machines, see "Manually Install or Upgrade VMware Tools in a Mac OS X Virtual Machine," on page 241.
- For information about installing or upgrading VMware Tools in Solaris virtual machines, see "Manually Install or Upgrade VMware Tools in a Solaris Virtual Machine," on page 241.
- For information about installing or upgrading VMware Tools in NetWare virtual machines, see "Manually Install or Upgrade VMware Tools in a NetWare Virtual Machine," on page 243.
- For information about installing or upgrading VMware Tools in FreeBSD virtual machines, see "Manually Install or Upgrade VMware Tools in a FreeBSD Virtual Machine," on page 245.

Using Open Virtual Machine Tools

Open Virtual Machine Tools is the open source implementation of the open-vm-tools suite, which includes virtualization utilities to improve the function and management of virtual machines on VMware hypervisors.

The open-vm-tools suite is bundled with Linux operating systems and is installed as a part of the OS installation, eliminating the need to separately install the suite on guest OSs. All leading Linux vendors support the open-vm-tools suite on vSphere, Workstation, and Fusion, and bundle them with their product releases, which VMware must certify before you can use them safely. For information about OS compatibility check for the open-vm-tools suite, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.

Bundling open-vm-tools with Linux OS releases reduces virtual machine downtime because all updates to the open-vm-tools suite and the VMware drivers are included with the OS maintenance patches and updates. You do not have to maintain separate maintenance cycles for open-vm-tools suite updates.

In a few cases, the integration of the open-vm-tools suite with OS releases might slightly vary when the suite is bundled with OSs on installation CDs or DVDs and is installed by default when you install your guest operating systems. In other cases, the open-vm-tools suite is not installed by default, unless specifically selected during installation.

Use the OS package manager for installing OSs from open source communities. Follow the installation instructions provided by your OS vendor for your specific release or check the partner Web site at http://partnerweb.vmware.com/GOSIG/home.html.

VMware fully supports Open VM Tools that are developed in collaboration with OS vendors and open source communities and does not recommend removing open-vm-tools that are redistributed by your OS vendors.

NOTE If you use open-vm-tools or OS specific package (OSP) for packaging and distribution of VMware Tools, the VMware Tools status displays as Guest Managed on the virtual machine **Summary** tab. The status Guest Managed means that you cannot use the vCenter Server for managing OSP and Open VM Tools software updates. Instead, manage the installation and update for Open VM Tools and OSP from within each guest operating system and expect to get updates on Open VM Tools in synch with the guest OS and virtual appliances updates and patches.

Open VM Tools Packages

For better managing guest operating systems, the open-vm-tools suite includes the following packages:

- The core open-vm-tools package contains the core open-vm-tools user space utilities, application programs, and libraries, including `vmtoolsd` to help effectively manage communication between your host and guest OSs. This package includes features as, synchronizing guest OS clocks with the virtualization platform, transferring files between hosts and guests, sending heartbeat information from guest OSs to the virtualization infrastructure to support vSphere High Availability (HA), publishing resource utilization and networking information of the guest OSs to the virtualization platform, and so on.

- The `open-vm-tools-desktop` package is optional and includes additional user space programs and libraries to improve the interactive functionality of desktop operations of your virtual machines. The package enables you to resize a guest display to match with its host console window or the VMware Remote Console Window for vSphere. The package also allows you to copy and paste between host and guest OSs as well as to drag and drop between guests and a host for the VMware Workstation and VMware Fusion products.
- The `open-vm-tools-devel` package contains libraries and additional documentation for developing `vmtoolsd` plug-ins and applications.
- The `open-vm-tools-debuginfo` package contains the source code for open-vm-tools and binary files. For the latest copy of the Open VM Tools source code, see the Sourceforge Web site at http://open-vm-tools.sourceforge.net. You can also the obtain a copy of the source code from the GitHub web site at https://github.com/vmware/open-vm-tools.

For information about the open-vm-tools support policy and availability, see the VMware knowledge base article at http://kb.vmware.com/kb/2073803.

Planning Downtime for Virtual Machines

Plan downtime for each virtual machine during the upgrade process. Typically, this downtime occurs during the virtual machine upgrade and the VMware Tools upgrade. Depending on your upgrade plan, some virtual machine downtime might be required during the ESX upgrade.

If an ESX/ESXi host is not managed by vCenter Server, you cannot use vMotion to move virtual machines. The virtual machines must have some downtime when the ESX/ESXi host reboots after upgrade.

You might not have to shut down more than a single virtual machine at any given time. You can stagger virtual machine downtimes to accommodate a schedule convenient to you and your customers.

For example:

- If your virtual machine users are located in diverse time zones, you can prepare by migrating virtual machines to specific hosts to serve a given time zone. This way you can arrange host upgrades so that virtual machine downtime occurs transparently outside business hours for that time zone.
- If your virtual machine users operate around the clock, you can delay downtime for their virtual machines to normally scheduled maintenance periods. You do not need to upgrade any stage within a certain time period. You can take as long as needed at any stage.

Downtime for Upgrading Virtual Machines

When you upgrade virtual machines, the required downtime depends on the guest operating system and the type of upgrade you are performing.

When you upgrade VMware Tools, expect the following downtime:

- No downtime is required for vCenter Server.
- No downtime is required for ESXi hosts.
- For Windows guest operating systems, you must restart the virtual machines at the end of the upgrade procedure, or later, for the upgrade take effect. You must always restart the virtual machine after you upgrade VMware Tools and after you upgrade the virtual machine compatibility.
- For Linux guest operating systems, you must restart the virtual machine to load the new versions of the VMXNET, VMXNET3, and PVSCSI drivers. You can also manually reload the drivers. To verify that the drivers are configured in the Linux kernel and that the virtual hardware is available, see Knowledge Base article, http://kb.vmware.com/kb/2050364. Note that manual restart is not required for the Linux guest operating system using kernel version 3.10.

- For BSD, NetWare, Solaris, and Mac OS X guest operating systems, no restart is required at the end of the procedure.

During the virtual machine compatibility upgrade, you must shut down the virtual machine for all guest operating systems.

Table 12-2. Virtual Machine Downtime by Guest Operating System

Guest Operating System	Upgrade VMware Tools	Upgrade Virtual Machine Compatibility
Microsoft Windows	Downtime to restart the guest operating system.	Downtime to shut down and power on the virtual machine.
Linux	Downtime to restart the guest operating system is required to load drivers.	Downtime to shut down and power on the virtual machine.
NetWare	No downtime.	Downtime to shut down and power on the virtual machine.
Solaris	No downtime.	Downtime to shut down and power on the virtual machine.
FreeBSD	No downtime.	Downtime to shut down and power on the virtual machine.
Mac OS X	No downtime.	Downtime to shut down and power on the virtual machine.

Manually Install or Upgrade VMware Tools in a Windows Virtual Machine

All supported Windows guest operating systems support VMware Tools.

Before you upgrade VMware Tools, consider the environment that the virtual machine runs in and weigh the benefits of different upgrade strategies. For example, you can install the latest version of VMware Tools to enhance the performance of the virtual machine's guest operating system and improve virtual machine management, or you can continue using the existing version to provide more flexibility and avoid downtime in your environment.

For Windows 2000 and later, VMware Tools installs a virtual machine upgrade helper tool. This tool restores the network configuration if you upgrade from ESX/ESXi 3.5 and later compatibility (hardware version 4) to ESX/ESXi 4.0 and later compatibility (hardware version 7).

Prerequisites

- Power on the virtual machine.
- Verify that the guest operating system is running.
- To determine whether you have the latest version of VMware Tools, look on the **Summary** tab for the virtual machine.
- For vSphere virtual machines, determine whether you have the latest version of VMware Tools. In the vSphere Client inventory, select the virtual machine and click the **Summary** tab.
- For VMware Player, Fusion, and Workstation virtual machines, if you connected the virtual machine’s virtual CD/DVD drive to an ISO image file when you installed the operating system, change the setting so that the virtual CD/DVD drive is configured to autodetect a physical drive.

  The autodetect setting enables the virtual machine's first virtual CD/DVD drive to detect and connect to the VMware Tools ISO file for a VMware Tools installation. This ISO file looks like a physical CD to your guest operating system. Use the virtual machine settings editor to set the CD/DVD drive to autodetect a physical drive.

- Log in as an administrator unless you are using an older Windows operating system. Any user can install VMware Tools in a Windows 95, Windows 98, or Windows ME guest operating system. For operating systems newer than these, you must log in as an administrator.
- If you use vSphere and plan to install the Guest Introspection Thin Agent driver, see the system requirements listed in the *vShield Quick Start Guide*. The vShield component is not installed by default. You must perform a custom installation and include that component.
- If you plan to install the Guest Introspection Thin Agent driver, see the system requirements listed in the *vShield Quick Start Guide*. The vShield component is not installed by default. You must perform a custom installation and include that component.

Procedure

1 Mount the VMware Tools virtual disc on the guest operating system.

VMware Product	Action
vSphere Client	**Inventory > Virtual Machine > Guest > Install/Upgrade VMware**
vSphere Web Client	Right-click the virtual machine and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**.
Fusion	**Virtual Machine > Install (or Upgrade) VMware Tools**
Workstation	**VM > Install (or Upgrade) VMware Tools**
Player	**Player > Manage > Install (or Upgrade) VMware Tools**

2 If you are using vCenter Server and are performing an upgrade or reinstallation, in the Install/Upgrade VMware Tools dialog box, select **Interactive Tools Installation** or **Interactive Tools Upgrade** and click **OK**.

The process starts by mounting the VMware Tools virtual disc on the guest operating system.

3 Mount the VMware Tools virtual disc on the guest operating system.

VMware Product	Action
vSphere Client	**Inventory > Virtual Machine > Guest > Install/Upgrade VMware Tools**
vSphere Web Client	Right-click the virtual machine and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**. a To locate a virtual machine, select a datacenter, folder, cluster, resource pool, host, or vApp. b Click the **Related Objects** tab and click **Virtual Machines**.

4 If you are performing an upgrade or reinstallation, in the Install/Upgrade VMware Tools dialog box, select **Interactive Tools Installation** or **Interactive Tools Upgrade** and click **OK**.

The process starts by mounting the VMware Tools virtual disc on the guest operating system.

5 If you are installing VMware Tools for the first time, click **OK** on the Install VMware Tools information page.

If autorun is enabled for the CD-ROM drive in the guest operating system, the VMware Tools installation wizard starts.

6 If autorun is not enabled, to manually launch the wizard, click **Start > Run** and enter `D:\setup.exe`, where `D:` is your first virtual CD-ROM drive. Use `D:\setup64.exe` for 64-bit Windows guest operating system.

7 Follow the on-screen instructions.

   To install nondefault components or remove certain components, such as the Guest Introspection Thin Agent driver, select the **Custom** setup.

   If you use vSphere, to install nondefault components, such as the Guest Introspection Thin Agent driver, select the **Custom** setup.

8 If the New Hardware wizard appears, follow the prompts and accept the defaults.

9 If you are installing a beta or RC version of VMware Tools and you see a warning that a package or driver is not signed, click **Install Anyway** to complete the installation.

10 When prompted, reboot the virtual machine.

The **VMware Tools** label on the **Summary** tab changes to **OK**.

If you are using vCenter Server, the **VMware Tools** label on the **Summary** tab changes to **OK**.

What to do next

If you upgraded VMware Tools as part of a larger, system-wide upgrade, next determine whether to upgrade the virtual machines in your environment. To review and compare the hardware available for different compatibility levels, see "Hardware Features Available with Virtual Machine Compatibility Settings," on page 93.

If you upgraded VMware Tools as part of a vSphere upgrade, next determine whether to upgrade the virtual machines in your environment. To review and compare the hardware available for different compatibility levels, see the *vSphere Virtual Machine Administration* documentation.

Automate VMware Tools Installation for Multiple Windows Virtual Machines

If you are installing VMware Tools in multiple virtual machines with Windows guest operating systems, you can automate its installation and specify options for the components to include or exclude.

Prerequisites

- Power on the virtual machine.
- Log in to the guest operating system as an administrator.
- If you plan to use the `setup.exe` command at the command line to run the VMware Tools installation, edit the virtual machine settings to connect the virtual CD/DVD drive to the VMware Tools ISO image.
- If you plan to use the `setup.exe` command at the command line to run the VMware Tools installation, edit the virtual machine settings to connect the virtual CD/DVD drive to the VMware Tools ISO image. In VMware Workstation and Player, the `windows.iso` file is on the host in the directory where you installed Workstation or Player.
- If you plan to use MSI arguments to specify options regarding the silent installation, go to the Windows Installer page on the MSDN Web site to familiarize yourself with the syntax. You can use these arguments with the `setup.exe` command or place them in the vCenter Server dialog box for automatic installations and upgrades.
- To prevent some VMware Tools components from being installed, familiarize yourself with the VMware Tools component names so that you can specify which components to exclude. See "Names of VMware Tools Components Used in Silent Installations," on page 236.
- If you are installing VMware Tools from a beta or release candidate of a VMware product, suppress prompts about unsigned drivers. See "Suppress Prompts About Unsigned Drivers on Windows Operating Systems Before Vista," on page 235 and "Add VMware as a Trusted Publisher to Suppress Driver Prompts," on page 235.

Procedure

1 In the vSphere Web Client inventory, select the host, cluster, or datacenter and click the **Virtual Machines** tab.

2 Select the virtual machines, right-click and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**.

3 Provide the installation or upgrade configuration information.

Suppress Prompts About Unsigned Drivers on Windows Operating Systems Before Vista

If you are installing a beta or RC version of VMware Tools in a Windows Server 2003 or earlier guest operating system, you can use a computer properties setting to suppress prompts that interfere with automatic installation of VMware Tools.

The version of VMware Tools included in a beta or release candidate version of a VMware product usually has some drivers that are signed only by VMware. If you are installing one of these versions in many virtual machines that run Windows Server 2003 or earlier guest operating systems, or if you plan to install VMware Tools from the command line, you can suppress prompts about unsigned drivers. If you do not suppress the prompts, during a VMware Tools installation, a message box appears several times and requires you to click **Continue Anyway** to complete the installation.

Prerequisites

- Power on the virtual machine.
- Log in to the guest operating system as an administrator.

Procedure

1 In the Windows Server 2003 or earlier guest operating system, in the **Start** menu, right-click **My Computer** and select **Properties**.

2 In the System Properties dialog box, click the **Hardware** tab and click **Driver Signing**.

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

When you run the VMware Tools installer, no prompts appear in the guest operating system.

What to do next

Install VMware Tools.

Add VMware as a Trusted Publisher to Suppress Driver Prompts

If you are installing a beta or RC version of VMware Tools in a Windows Vista or later guest operating system, you can add a VMware certificate to suppress prompts that interfere with automatic installation of VMware Tools.

The version of VMware Tools included in a beta or release candidate version of a VMware product usually has some drivers that are signed only by VMware. If you are installing one of these versions in many virtual machines that run Windows Vista or later guest operating systems, or if you plan to install VMware Tools from the command line, add a VMware security certificate to the trusted publishers group. If you do not add the VMware certificate, during a VMware Tools installation, a message box appears several times and prompts you to install device software from VMware.

Prerequisites

- Power on the virtual machine.
- Log in to the guest operating system as an administrator.

- Obtain a copy of the `certmgr.exe` application and copy it to the guest operating system on which you plan to install VMware Tools. The `certmgr.exe` application is included in the Windows SDK

Procedure

1 Use the certificate export wizard to create a VMware certificate file.

   a Locate a signed VMware file, such as a VMware `.exe` or `.sys` file.

   b Right-click the file and select **Properties**.

   c Click the **Digital Signatures** tab and select **View Certificate**.

   d Click the **Details** tab and click **Copy to File**.

   e Follow the prompts and name the exported certificate `vmware.cer`.

2 Copy the exported VMware certificate to the guest operating system on which you plan to install VMware Tools.

3 In the guest operating system, run the `certmgr.exe` command to add the VMware certificate to the trusted publishers group.

```
certmgr.exe –add vmware.cer –c –s –r localMachine TrustedPublisher
```

When you run the VMware Tools installer, no prompts appear in the guest operating system.

What to do next

Install VMware Tools.

Names of VMware Tools Components Used in Silent Installations

In Windows virtual machines, when running an automatic installation or running an installation of VMware Tools using the command line, you can specify which VMware Tools components to install.

Because VMware Tools contains so many components, if you do not want to install particular components, you specify which ones to exclude rather than which ones to include. The syntax is `ADDLOCAL=ALL REMOVE=`*`component`*. The valid values for VMware Tools components are listed in the following table.

Component names are case-sensitive. Not all components are installed on all operating systems.

Table 12-3. VMware Tools Component Values

Valid Component Values	Description	
`Drivers`	**`Audio`**	Audio driver for 64-bit operating systems and Windows Vista and later systems.
	`BootCamp`	Driver for Mac BootCamp support.
	`LSI`	PCI Fusion-MPT Miniport driver for Windows XP systems.
	`MemCtl`	VMware memory control driver. Use this driver if you plan to use this virtual machine in a vSphere environment. Excluding this feature hinders the memory management capabilities of the virtual machine running in a vSphere environment.
	`Mouse`	VMware mouse driver. Excluding this feature decreases mouse performance in your virtual machine.
	`PVSCSI`	Driver for VMware Paravirtual SCSI adapters, which enhance the performance of some virtualized applications.
	`SVGA`	VMware SVGA driver. Excluding this feature limits the display capabilities of your virtual machine.
	`Sync`	Filesystem Sync driver, which enables backup applications to create application-consistent snapshots. This driver ensures that no I/O is written during snapshot creation. This driver is used if the guest operating system is earlier than Windows Server 2003. For newer operating systems, the VSS driver is used instead.
	`VMCI`	Virtual Machine Communication Interface driver. This driver allows virtual machines to communicate with the hosts they run on without using the network. Developers can write client-server applications to the VMCI Sock (`vsock`) interface to make use of the VMCI virtual device.
	`Hgfs`	VMware shared folders driver. Use this driver if you plan to use this virtual machine with VMware Workstation, Player, or Fusion. Excluding this feature prevents you from sharing a folder between your virtual machine and the host system.
	`VMXNet`	VMware VMXnet networking driver.
	`VMXNet3`	Next-generation VMware VMXnet networking driver for virtual machines that use virtual hardware version 7 and higher. For more information, see the VMware Knowledge Base article 1001805. Virtual hardware version 7 corresponds to ESX/ESXi 4.x compatibility.
	`VShield`	Driver for the Guest Introspection Thin Agent component. Install this component if you use vSphere and Guest Introspection. By default, this component is not installed.
	`VSS`	Driver for creating automatic backups. This driver is used if the guest operating system is Windows Vista, Windows Server 2003, or other newer operating system. For older operating systems and in Linux operating system, the Filesystem Sync driver is used instead.
`Toolbox`	**`Unity`**	Component to support the Unity feature, which allows you to open an application window in a virtual machine, enter Unity mode, and have that window appear on your host desktop like any other host application window.
	`Perfmon`	Driver for WMI performance logging.

Important One way to determine the component values to use is to run the interactive VMware Tools installer with full logging turned on, select the components that you want installed, and then search the log files for the ADDLOCAL and REMOVE properties. The log files show the names used by the program. The following command runs the interactive installer with full logging turned on:

```
Setup.exe /s /v"/qn /l*v ""%TEMP%\vmmsi.log"""
```

Manually Install or Upgrade VMware Tools in a Linux Virtual Machine

For Linux virtual machines, you manually install or upgrade VMware Tools by using the command line.

This procedure describes how to use the VMware Tools tar installer to install or upgrade VMware Tools. For virtual machines in a vSphere environment, you can alternatively use VMware Tools operating system specific packages (OSPs) and open-vm-tools to install and upgrade VMware Tools. With OSPs open-vm-tools, you can use the native update mechanisms of your operating system to download, install, and manage VMware Tools. For more information, see "Operating System Specific Packages for Linux Guest Operating Systems," on page 240.

Prerequisites

- Power on the virtual machine.
- Verify that the guest operating system is running.
- Because the VMware Tools installer is written in Perl, verify that Perl is installed in the guest operating system.
- To determine whether you have the latest version of VMware Tools, look on the **Summary** tab for the virtual machine.
- For vSphere virtual machines, determine whether you have the latest version of VMware Tools. In the vSphere Client inventory, select the virtual machine and click the **Summary** tab.

Procedure

1 Mount the VMware Tools virtual disc on the guest operating system.

VMware Product	Action
vSphere Client	**Inventory > Virtual Machine > Guest > Install/Upgrade VMware**
vSphere Web Client	Right-click the virtual machine and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**.
Fusion	**Virtual Machine > Install (or Upgrade) VMware Tools**
Workstation	**VM > Install (or Upgrade) VMware Tools**
Player	**Player > Manage > Install (or Upgrade) VMware Tools**

2 Mount the VMware Tools virtual disc on the guest operating system.

VMware Product	Action
vSphere Client	**Inventory > Virtual Machine > Guest > Install/Upgrade VMware Tools**
vSphere Web Client	Right-click the virtual machine and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**. a To locate a virtual machine, select a datacenter, folder, cluster, resource pool, host, or vApp. b Click the **Related Objects** tab and click **Virtual Machines**.

3 If you are performing an upgrade or reinstallation, in the Install/Upgrade VMware Tools dialog box, select **Interactive Tools Installation** or **Interactive Tools Upgrade** and click **OK**.

The process starts by mounting the VMware Tools virtual disc on the guest operating system.

4 In the virtual machine, log in to the guest operating system as root and open a terminal window.

5 Run the `mount` command with no arguments to determine whether your Linux distribution automatically mounted the VMware Tools virtual CD-ROM image.

   If the CD-ROM device is mounted, the CD-ROM device and its mount point are listed as something like this:

   ```
   /dev/cdrom on /mnt/cdrom type iso9660 (ro,nosuid,nodev)
   ```

6 If the VMware Tools virtual CD-ROM image is not mounted, mount the CD-ROM drive.

   a If a mount point directory does not already exist, create it.

      ```
      mkdir /mnt/cdrom
      ```

      Some Linux distributions use different mount point names. For example, on some distributions the mount point is `/media/VMware Tools` rather than `/mnt/cdrom`. Modify the command to reflect the conventions that your distribution uses.

   b Mount the CD-ROM drive.

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

      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 that your distribution uses.

7 Change to a working directory, for example, `/tmp`.

   ```
   cd /tmp
   ```

8 Delete any previous `vmware-tools-distrib` directory before you install VMware Tools.

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

9 List the contents of the mount point directory and note the filename of the VMware Tools tar installer.

   ```
   ls mount-point
   ```

10 Uncompress the installer.

   ```
   tar zxpf /mnt/cdrom/VMwareTools-x.x.x-yyyy.tar.gz
   ```

   The value *x.x.x* is the product version number, and *yyyy* is the build number of the product release.

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

11 If necessary, unmount the CD-ROM image.

   ```
   umount /dev/cdrom
   ```

   If your Linux distribution automatically mounted the CD-ROM, you do not need to unmount the image.

12 Run the installer and configure VMware Tools.

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

   Usually, the `vmware-config-tools.pl` configuration file runs after the installer file finishes running.

13 Follow the prompts to accept the default values, if appropriate for your configuration.

14 Follow the instructions at the end of the script.

   Depending on the features you use, these instructions can include restarting the X session, restarting networking, logging in again, and starting the VMware User process. You can alternatively reboot the guest operating system to accomplish all these tasks.

The **VMware Tools** label on the **Summary** tab changes to **OK**.

If you are using vCenter Server, the **VMware Tools** label on the **Summary** tab changes to **OK**.

What to do next

If you upgraded VMware Tools as part of a larger, system-wide upgrade, next determine whether to upgrade the virtual machines in your environment. To review and compare the hardware available for different compatibility levels, see "Hardware Features Available with Virtual Machine Compatibility Settings," on page 93.

If you upgraded VMware Tools as part of a vSphere upgrade, next determine whether to upgrade the virtual machines in your environment. To review and compare the hardware available for different compatibility levels, see the *vSphere Virtual Machine Administration* documentation.

Operating System Specific Packages for Linux Guest Operating Systems

For vSphere deployments, VMware provides operating system specific packages (OSPs) as a packaging and distribution mechanism for VMware Tools. These VMware Tools OSPs are packaged using native package formats and standards such as `rpm` and `deb`.

Note If you already have open-vm-tools installed, it is recommended that you do not create OSPs for Linux distributions. For information about compatibility support for guest operating system, see the *VMware Compatibility Guide*.

Using OSPs provides the following benefits:

- You can use the native update mechanisms of the guest operating system to download, install, and manage VMware Tools.
- You can upgrade to the latest version of VMware Tools without having to upgrade to the latest version of vSphere.
- Because VMware Tools OSPs follow the best practices and standards of the specific Linux operating system, OSPs use standard mechanisms for determining dependencies among packages. These mechanisms allow you to audit the packages on virtual machines with or without graphics components.
- You can use standard operating system tools to examine OSPs during VMware Tools installation. This process allows you to easily determine which components to install and to verify the validity of the packaging.

Important Use OSPs if you want to use native update mechanisms, rather than vCenter Server, to manage updates for VMware Tools. If you use an OSP, the VMware Tools status is Guest Managed on the virtual machine **Summary** tab. The status Guest Managed means that you cannot use the vCenter Server to manage VMware Tools and you cannot use vSphere Update Manager to upgrade VMware Tools.

For more information, go to the VMware Operating System Specific Packages Web site, at http://www.vmware.com/download/packages.html.

Manually Install or Upgrade VMware Tools in a Mac OS X Virtual Machine

For Mac OS X Server virtual machines you install or upgrade VMware Tools using an installer assistant.

If you use VMware Fusion or ESXi on a computer with an Apple label, you can create Mac OS X Server (10.5 or later) virtual machines and install VMware Tools.

Prerequisites

- Power on the virtual machine.
- Verify that the guest operating system is running.

Procedure

1 Select the menu command to mount and open the VMware Tools virtual disc on the guest operating system.

VMware Product	Menu Command
vSphere Client	**Inventory > Virtual Machine > Guest > Install/Upgrade VMware Tools** and select **Interactive Tools Installation** or **Interactive Tools Upgrade**
vSphere Web Client	Right-click the virtual machine in the vCenter inventory and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**
Fusion	**Virtual Machine > Install (or Upgrade) VMware Tools**

2 Mount the VMware Tools virtual disc on the guest operating system.

VMware Product	Action
vSphere Client	**Inventory > Virtual Machine > Guest > Install/Upgrade VMware Tools**
vSphere Web Client	Right-click the virtual machine and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**. a To locate a virtual machine, select a datacenter, folder, cluster, resource pool, host, or vApp. b Click the **Related Objects** tab and click **Virtual Machines**.

3 If you are performing an upgrade or reinstallation, in the Install/Upgrade VMware Tools dialog box, select **Interactive Tools Installation** or **Interactive Tools Upgrade** and click **OK**.

The process starts by mounting the VMware Tools virtual disc on the guest operating system.

4 Open **Install VMware Tools** on the VMware Tools virtual disc, follow the prompts in the installer assistant, and click **OK**.

The virtual machine restarts to have VMware Tools take effect.

Manually Install or Upgrade VMware Tools in a Solaris Virtual Machine

For Solaris virtual machines, you manually install or upgrade VMware Tools by using the command line.

Before you upgrade VMware Tools, consider the environment that the virtual machine runs in and weigh the benefits of different upgrade strategies. For example, you can install the latest version of VMware Tools to enhance the performance of the virtual machine's guest operating system and improve virtual machine management, or you can continue using the existing version to provide more flexibility and avoid downtime in your environment.

Prerequisites

- Power on the virtual machine.
- Verify that the guest operating system is running.
- Because the VMware Tools installer is written in Perl, verify that Perl is installed in the guest operating system.
- To determine whether you have the latest version of VMware Tools, look on the **Summary** tab for the virtual machine.
- For vSphere virtual machines, determine whether you have the latest version of VMware Tools. In the vSphere Client inventory, select the virtual machine and click the **Summary** tab.

Procedure

1 Mount the VMware Tools virtual disc on the guest operating system.

VMware Product	Action
vSphere Client	**Inventory > Virtual Machine > Guest > Install/Upgrade VMware**
vSphere Web Client	Right-click the virtual machine and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**.
Fusion	**Virtual Machine > Install (or Upgrade) VMware Tools**
Workstation	**VM > Install (or Upgrade) VMware Tools**
Player	**Player > Manage > Install (or Upgrade) VMware Tools**

2 Mount the VMware Tools virtual disc on the guest operating system.

VMware Product	Action
vSphere Client	**Inventory > Virtual Machine > Guest > Install/Upgrade VMware Tools**
vSphere Web Client	Right-click the virtual machine and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**. a To locate a virtual machine, select a datacenter, folder, cluster, resource pool, host, or vApp. b Click the **Related Objects** tab and click **Virtual Machines**.

3 If you are performing an upgrade or reinstallation, in the Install/Upgrade VMware Tools dialog box, select **Interactive Tools Installation** or **Interactive Tools Upgrade** and click **OK**.

The process starts by mounting the VMware Tools virtual disc on the guest operating system.

4 In the virtual machine, log in to the guest operating system as root and open a terminal window.

5 If the Solaris volume manager does not mount the CD-ROM under `/cdrom/vmwaretools`, restart the volume manager.

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

6 Change to a working directory, for example, `/tmp`.

```
cd /tmp
```

7 Extract VMware Tools.

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

8 Run the installer and configure VMware Tools.

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

Usually, the `vmware-config-tools.pl` configuration file runs after the installer file finishes running.

9 Follow the prompts to accept the default values, if appropriate for your configuration.

10 Follow the instructions at the end of the script.

Depending on the features you use, these instructions can include restarting the X session, restarting networking, logging in again, and starting the VMware User process. You can alternatively reboot the guest operating system to accomplish all these tasks.

The **VMware Tools** label on the **Summary** tab changes to **OK**.

If you are using vCenter Server, the **VMware Tools** label on the **Summary** tab changes to **OK**.

What to do next

If you upgraded VMware Tools as part of a larger, system-wide upgrade, next determine whether to upgrade the virtual machines in your environment. To review and compare the hardware available for different compatibility levels, see "Hardware Features Available with Virtual Machine Compatibility Settings," on page 93.

If you upgraded VMware Tools as part of a vSphere upgrade, next determine whether to upgrade the virtual machines in your environment. To review and compare the hardware available for different compatibility levels, see the *vSphere Virtual Machine Administration* documentation.

Manually Install or Upgrade VMware Tools in a NetWare Virtual Machine

For NetWare virtual machines, you manually install or upgrade VMware Tools by using the command line.

Before you upgrade VMware Tools, consider the environment that the virtual machine runs in and weigh the benefits of different upgrade strategies. For example, you can install the latest version of VMware Tools to enhance the performance of the virtual machine's guest operating system and improve virtual machine management, or you can continue using the existing version to provide more flexibility and avoid downtime in your environment.

Prerequisites

- Power on the virtual machine.
- Verify that the guest operating system is running.
- Because the VMware Tools installer is written in Perl, verify that Perl is installed in the guest operating system.
- To determine whether you have the latest version of VMware Tools, look on the **Summary** tab for the virtual machine.
- For vSphere virtual machines, determine whether you have the latest version of VMware Tools. In the vSphere Client inventory, select the virtual machine and click the **Summary** tab.

Procedure

1 Mount the VMware Tools virtual disc on the guest operating system.

VMware Product	Action
vSphere Client	**Inventory > Virtual Machine > Guest > Install/Upgrade VMware**
vSphere Web Client	Right-click the virtual machine and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**.
Fusion	**Virtual Machine > Install (or Upgrade) VMware Tools**
Workstation	**VM > Install (or Upgrade) VMware Tools**
Player	**Player > Manage > Install (or Upgrade) VMware Tools**

2 Mount the VMware Tools virtual disc on the guest operating system.

VMware Product	Action
vSphere Client	**Inventory > Virtual Machine > Guest > Install/Upgrade VMware Tools**
vSphere Web Client	Right-click the virtual machine and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**. a To locate a virtual machine, select a datacenter, folder, cluster, resource pool, host, or vApp. b Click the **Related Objects** tab and click **Virtual Machines**.

3 If you are performing an upgrade or reinstallation, in the Install/Upgrade VMware Tools dialog box, select **Interactive Tools Installation** or **Interactive Tools Upgrade** and click **OK**.

The process starts by mounting the VMware Tools virtual disc on the guest operating system.

4 Load the CD-ROM driver so that the virtual CD-ROM device mounts the ISO image as a volume.

Operating System	Command
NetWare 6.5	`LOAD CDDVD`
NetWare 6.0 or NetWare 5.1	`LOAD CD9660.NSS`
NetWare 4.2 (not available in vSphere)	`load cdrom`

When the installation finishes, the message `VMware Tools for NetWare are now running` appears in the Logger Screen for NetWare 6.5 and NetWare 6.0 guest operating systems and in the Console Screen for NetWare 4.2 and 5.1 operating systems.

5 For NetWare 4.2 guest operating systems, restart the guest operating system.

a In the system console, shut down the system.

```
down
```

b In the system console, restart the guest operating system.

```
restart server
```

6 If the VMware Tools virtual disc (`netware.iso`) is attached to the virtual machine, right-click the CD-ROM icon in the status bar of the console window and select **Disconnect** to disconnect it.

What to do next

If you upgraded VMware Tools as part of a larger, system-wide upgrade, next determine whether to upgrade the virtual machines in your environment. To review and compare the hardware available for different compatibility levels, see "Hardware Features Available with Virtual Machine Compatibility Settings," on page 93.

If you upgraded VMware Tools as part of a vSphere upgrade, next determine whether to upgrade the virtual machines in your environment. To review and compare the hardware available for different compatibility levels, see the *vSphere Virtual Machine Administration* documentation.

Manually Install or Upgrade VMware Tools in a FreeBSD Virtual Machine

For FreeBSD virtual machines, you manually install or upgrade VMware Tools by using the command line.

Before you upgrade VMware Tools, consider the environment that the virtual machine runs in and weigh the benefits of different upgrade strategies. For example, you can install the latest version of VMware Tools to enhance the performance of the virtual machine's guest operating system and improve virtual machine management, or you can continue using the existing version to provide more flexibility and avoid downtime in your environment.

Prerequisites

- Power on the virtual machine.
- Verify that the guest operating system is running.
- Because the VMware Tools installer is written in Perl, verify that Perl is installed in the guest operating system.
- To determine whether you have the latest version of VMware Tools, look on the **Summary** tab for the virtual machine.
- For vSphere virtual machines, determine whether you have the latest version of VMware Tools. In the vSphere Client inventory, select the virtual machine and click the **Summary** tab.

Procedure

1 Mount the VMware Tools virtual disc on the guest operating system.

VMware Product	Action
vSphere Client	**Inventory > Virtual Machine > Guest > Install/Upgrade VMware**
vSphere Web Client	Right-click the virtual machine and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**.
Fusion	**Virtual Machine > Install (or Upgrade) VMware Tools**
Workstation	**VM > Install (or Upgrade) VMware Tools**
Player	**Player > Manage > Install (or Upgrade) VMware Tools**

2 Mount the VMware Tools virtual disc on the guest operating system.

VMware Product	Action
vSphere Client	**Inventory > Virtual Machine > Guest > Install/Upgrade VMware Tools**
vSphere Web Client	Right-click the virtual machine and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**. a To locate a virtual machine, select a datacenter, folder, cluster, resource pool, host, or vApp. b Click the **Related Objects** tab and click **Virtual Machines**.

3 If you are performing an upgrade or reinstallation, in the Install/Upgrade VMware Tools dialog box, select **Interactive Tools Installation** or **Interactive Tools Upgrade** and click **OK**.

The process starts by mounting the VMware Tools virtual disc on the guest operating system.

4 In the virtual machine, log in to the guest operating system as root and open a terminal window.

5 If the distribution does not automatically mount CD-ROMs, mount the VMware Tools virtual CD-ROM image.

   For example, type **`mount /cdrom`**.

6 Change to a working directory, for example, `/tmp`.

```
cd /tmp
```

7 Untar the VMware Tools tar file.

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

8 If the distribution does not use automounting, unmount the VMware Tools virtual CD-ROM image.

```
umount /cdrom
```

9 Run the installer and configure VMware Tools.

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

   Usually, the `vmware-config-tools.pl` configuration file runs after the installer file finishes running.

10 Follow the prompts to accept the default values, if appropriate for your configuration.

11 Follow the instructions at the end of the script.

   Depending on the features you use, these instructions can include restarting the X session, restarting networking, logging in again, and starting the VMware User process. You can alternatively reboot the guest operating system to accomplish all these tasks.

The **VMware Tools** label on the **Summary** tab changes to **OK**.

If you are using vCenter Server, the **VMware Tools** label on the **Summary** tab changes to **OK**.

What to do next

If you upgraded VMware Tools as part of a larger, system-wide upgrade, next determine whether to upgrade the virtual machines in your environment. To review and compare the hardware available for different compatibility levels, see "Hardware Features Available with Virtual Machine Compatibility Settings," on page 93.

If you upgraded VMware Tools as part of a vSphere upgrade, next determine whether to upgrade the virtual machines in your environment. To review and compare the hardware available for different compatibility levels, see the *vSphere Virtual Machine Administration* documentation.

Upgrade VMware Tools

You can upgrade VMware Tools in one or more virtual machines by using the vSphere Web Client.

Procedure

1 Start the vSphere Web Client and log in to the vCenter Server.

2 Select the virtual machines.

   a Select a datacenter, folder, cluster, resource pool, or host.

   b Click the **Related Objects** tab, and click **Virtual Machines**.

3 Power on the virtual machines to upgrade.

4 Right-click your selections.

5 Select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools** and click **OK**.

6 Select **Interactive Upgrade** or **Automatic Upgrade** and click **Upgrade**.

7 If you chose the interactive upgrade for a virtual machine with a Linux guest operating system, reboot the operating system by running the `reboot` command from a command-line prompt so that you can use the new network modules.

VMware Tools are upgraded.

Perform an Automatic Upgrade of VMware Tools

When you start an automatic upgrade of VMware Tools, you do not need to perform any operations in the guest operating system that is running on the virtual machine. The automatic upgrade uninstalls the previous version of VMware Tools, installs the latest version that is available for your ESXi host.

Automatic VMware Tools upgrade is supported only for virtual machines with Windows or Linux guest operating systems.

Prerequisites

The following requirements are for each virtual machine in the upgrade:

- Power on the virtual machine.
- Verify that the guest operating system is running.
- To determine whether you have the latest version of VMware Tools, look on the **Summary** tab for the virtual machine.

Procedure

1 Select **Automatic Tools Upgrade**.

2 (Optional) In the **Advanced Options** text box, enter advanced options for the guest operating system.

Option	Action
Microsoft Windows Guest Operating Systems	Enter **`/s /v "/qn" /l "`*`Microsoft_Windows_location`*`\`*`filename`*`.log"`** to perform a silent upgrade of VMware Tools and create a log file in the specified location on the guest operating system.
Linux Guest Operating Systems	■ Enter **`--default`** to perform the default behavior. Perform a silent upgrade of VMware Tools. Install tools `bin`, `lib` and `doc` files in the default `/usr` directory. ■ Enter **`--prefix=`***`binary_location`*`,`*`lib_location`*`,`*`doc_location`* to perform a silent upgrade of VMware Tools and install the binary, library, and document files in the specified locations.

3 Click **OK.**

The **VMware Tools** label on the **Summary** tab changes to **OK**.

Important After you upgrade VMware Tools on Linux guest operating systems, new network modules are available but are not used until you either restart the guest operating system or stop networking, unload and reload the VMware networking kernel modules, and restart networking. This behavior means that even if VMware Tools is set to automatically upgrade, you must restart or reload network modules to make new features available.

This strategy avoids network interruptions and allows you to install VMware Tools over SSH.

Upgrading VMware Tools on Windows guest operation systems automatically installs the WDDM graphics drivers. The WDDM graphics driver makes the sleep mode available in guest OS power settings to adjust the sleep options. For example, you can use the sleep mode setting **Change when the computer sleeps** to configure your guest OS to automatically go to sleep mode after a certain time or prevent your guest OS from automatically switching to sleep mode after being idle for some time.

What to do next

Upgrade the virtual machine compatibility.

Upgrade the Compatibility for Virtual Machines

The virtual machine compatibility determines the virtual hardware available to the virtual machine, which corresponds to the physical hardware available on the host machine. You can upgrade the compatibility level to make a virtual machine compatible with the latest version of ESXi running on the host.

This procedure upgrades one or more virtual machines to the latest supported virtual hardware version immediately. To schedule an upgrade for the next virtual machine reboot, and choose from all supported virtual hardware upgrade versions, see "Schedule a Compatibility Upgrade for Virtual Machines," on page 249.

For information about virtual machine hardware versions and compatibility, see "Virtual Machine Compatibility," on page 89.

Prerequisites

- Create a backup or snapshot of the virtual machines. See "Using Snapshots To Manage Virtual Machines," on page 194.
- Upgrade VMware Tools. On Microsoft Windows virtual machines, if you upgrade the compatibility before you upgrade VMware Tools, the virtual machine might automatically lose its network settings.
- Verify that all `.vmdk` files are available to the ESX/ESXi host on a VMFS3, VMFS5, or NFS datastore.
- Verify that the virtual machines are stored on VMFS3, VMFS5 or NFS datastores.
- Verify that the compatibility settings for the virtual machines are not the latest supported version.
- Determine the ESXi versions that you want the virtual machines to be compatible with. See "Virtual Machine Compatibility," on page 89.

Procedure

1. Log in to the vCenter Server from the vSphere Web Client.
2. Select the virtual machines.
   a. Select a datacenter, folder, cluster, resource pool, or host.
   b. Click the **Related Objects** tab, and click **Virtual Machines**.
3. Power off the selected virtual machines.
4. Select **Actions > All vCenter Actions > Compatibility > Upgrade VM Compatibility**.

5 Click **Yes** to confirm the upgrade.

6 Select the ESXi versions for the virtual machines to be compatible with.

7 Click **OK**.

The selected virtual machines are upgraded to the corresponding hardware version for the Compatibility setting that you chose, and the new hardware version is updated in the Summary tab of the virtual machine.

What to do next

Power on the virtual machines.

Schedule a Compatibility Upgrade for Virtual Machines

The virtual machine compatibility determines the virtual hardware available to the virtual machine, which corresponds to the physical hardware available on the host. You can schedule a compatibility upgrade to make a virtual machine compatible with newer versions of ESXi.

Use this procedure to schedule an upgrade of one or more virtual machines at the next reboot of the virtual machine, and choose from all supported compatibility level upgrades. To upgrade virtual machines immediately to the latest supported compatibility, see "Upgrade the Compatibility for Virtual Machines," on page 248.

For information about virtual machine hardware versions and compatibility, see "Virtual Machine Compatibility," on page 89.

Prerequisites

- Create a backup or snapshot of the virtual machines. See "Using Snapshots To Manage Virtual Machines," on page 194.
- Upgrade to the latest version of VMware Tools. If you upgrade the compatibility before you upgrade VMware Tools, the virtual machine might lose its network settings.
- Verify that all `.vmdk` files are available to the ESX/ESXi host on a VMFS3, VMFS5, or NFS datastore.
- Verify that the virtual machines are stored on VMFS3, VMFS5 or NFS datastores.
- Verify that the compatibility settings for the virtual machines are not the latest supported version.
- Determine the ESXi versions that you want the virtual machines to be compatible with. See "Virtual Machine Compatibility," on page 89.

Procedure

1 Log in to the vCenter Server from the vSphere Web Client.

2 Select the virtual machines.

   a Select a datacenter, folder, cluster, resource pool, or host.

   b Click the **Related Objects** tab and click **Virtual Machines**.

3 Power off the selected virtual machines.

4 Select **Actions > All vCenter Actions > Compatibility > Schedule VM Compatibility Upgrade**.

5 Click **Yes** to confirm the upgrade.

6 Select the ESXi versions for the virtual machines to be compatible with.

7 (Optional) Select **Only upgrade after normal guest OS shutdown**.

   This prevents the scheduled upgrade from occurring unless the guest operating system of the virtual machine is shut down or restarted normally.

Each of the selected virtual machines is upgraded to the compatibility that you chose at the next reboot of the virtual machine, and the Compatibility setting is updated in the Summary tab of the virtual machine.

Required Privileges for Common Tasks

13

Many tasks require permissions on more than one object in the inventory. You can review the privileges that are required to perform the tasks and, where applicable, the appropriate sample roles.

The table below lists common tasks that require more than one privilege. You can add permissions to inventory objects by pairing a user with one of the predefined roles, or you can create custom roles with the set of privileges that you expect to use multiple times.

If the task that you want to perform is not in this table, the following rules can help you determine where you must assign permissions to allow particular operations:

- Any operation that consumes storage space, such as creating a virtual disk or taking a snapshot, requires the **Datastore.Allocate Space** privilege on the target datastore, as well as the privilege to perform the operation itself.
- Moving an object in the inventory hierarchy requires appropriate privileges on the object itself, the source parent object (such as a folder or cluster), and the destination parent object.
- Each host and cluster has its own implicit resource pool that contains all the resources of that host or cluster. Deploying a virtual machine directly to a host or cluster requires the **Resource.Assign Virtual Machine to Resource Pool** privilege.

Table 13-1. Required Privileges for Common Tasks

Task	Required Privileges	Applicable Role
Create a virtual machine	On the destination folder or data center: ■ **Virtual machine.Inventory.Create new** ■ **Virtual machine.Configuration.Add new disk** (if creating a new virtual disk) ■ **Virtual machine.Configuration.Add existing disk** (if using an existing virtual disk) ■ **Virtual machine.Configuration.Raw device** (if using an RDM or SCSI pass-through device)	Administrator
	On the destination host, cluster, or resource pool: **Resource.Assign virtual machine to resource pool**	Resource pool administrator or Administrator
	On the destination datastore or folder containing a datastore: **Datastore.Allocate space**	Datastore Consumer or Administrator
	On the network that the virtual machine will be assigned to: **Network.Assign network**	Network Consumer or Administrator

Table 13-1. Required Privileges for Common Tasks (Continued)

Task	Required Privileges	Applicable Role
Deploy a virtual machine from a template	On the destination folder or data center: ■ **Virtual machine .Inventory.Create from existing** ■ **Virtual machine.Configuration.Add new disk**	Administrator
	On a template or folder of templates: **Virtual machine.Provisioning.Deploy template**	Administrator
	On the destination host, cluster or resource pool: **Resource.Assign virtual machine to resource pool**	Administrator
	On the destination datastore or folder of datastores: **Datastore.Allocate space**	Datastore Consumer or Administrator
	On the network that the virtual machine will be assigned to: **Network.Assign network**	Network Consumer or Administrator
Take a virtual machine snapshot	On the virtual machine or a folder of virtual machines: **Virtual machine.Snapshot management. Create snapshot**	Virtual Machine Power User or Administrator
	On the destination datastore or folder of datastores: **Datastore.Allocate space**	Datastore Consumer or Administrator
Move a virtual machine into a resource pool	On the virtual machine or folder of virtual machines: ■ **Resource.Assign virtual machine to resource pool** ■ **Virtual machine.Inventory.Move**	Administrator
	On the destination resource pool: **Resource.Assign virtual machine to resource pool**	Administrator
Install a guest operating system on a virtual machine	On the virtual machine or folder of virtual machines: ■ **Virtual machine.Interaction.Answer question** ■ **Virtual machine.Interaction.Console interaction** ■ **Virtual machine.Interaction.Device connection** ■ **Virtual machine.Interaction.Power Off** ■ **Virtual machine.Interaction.Power On** ■ **Virtual machine.Interaction.Reset** ■ **Virtual machine.Interaction.Configure CD media** (if installing from a CD) ■ **Virtual machine.Interaction.Configure floppy media** (if installing from a floppy disk) ■ **Virtual machine.Interaction.VMware Tools install**	Virtual Machine Power User or Administrator
	On a datastore containing the installation media ISO image: **Datastore.Browse datastore** (if installing from an ISO image on a datastore) On the datastore to which you upload the installation media ISO image: ■ **Datastore.Browse datastore** ■ **Datastore.Low level file operations**	Virtual Machine Power User or Administrator
Migrate a virtual machine with vMotion	On the virtual machine or folder of virtual machines: ■ **Resource.Migrate powered on virtual machine** ■ **Resource.Assign Virtual Machine to Resource Pool** (if destination is a different resource pool from the source)	Resource Pool Administrator or Administrator
	On the destination host, cluster, or resource pool (if different from the source): **Resource.Assign virtual machine to resource pool**	Resource Pool Administrator or Administrator

Table 13-1. Required Privileges for Common Tasks (Continued)

Task	Required Privileges	Applicable Role
Cold migrate (relocate) a virtual machine	On the virtual machine or folder of virtual machines: ■ **Resource.Migrate powered off virtual machine** ■ **Resource.Assign virtual machine to resource pool** (if destination is a different resource pool from the source)	Resource Pool Administrator or Administrator
	On the destination host, cluster, or resource pool (if different from the source): **Resource.Assign virtual machine to resource pool**	Resource Pool Administrator or Administrator
	On the destination datastore (if different from the source): **Datastore.Allocate space**	Datastore Consumer or Administrator
Migrate a virtual machine with Storage vMotion	On the virtual machine or folder of virtual machines: **Resource.Migrate powered on virtual machine**	Resource Pool Administrator or Administrator
	On the destination datastore: **Datastore.Allocate space**	Datastore Consumer or Administrator
Move a host into a cluster	On the host: **Host.Inventory.Add host to cluster**	Administrator
	On the destination cluster: **Host.Inventory.Add host to cluster**	Administrator

Index

Numerics

3D graphics
- drivers for **137**
- enabling **138**
- rendering options **137**
- requirements **137**
- selecting renderer **138**
- vendors **137**

A

acceleration, disabling **162**
adapters, *See* storage controllers
add Guest OS specification **54**
Add SSO Users **158**
adding
- floppy drives **135**
- network adapters **107**
- PCI devices **137**
- SATA controllers **127**
- SCSI controllers **128**
- SCSI devices **136**
- USB devices to client computers **149**

agent manager **186**
AHCI SATA controller, *See* storage controllers
AMD override mask **100**
apply Guest OS specification to a virtual machine **54**
audio adapters, connecting **218**
audio drivers, virtual **206**
Authoring options, OVF **181**
autoconnect feature, for USB passthrough **141**
automatic VMware Tools upgrade **247**

B

backup applications, drivers for **206**
boot sequence, delaying **162**

C

CD drives
- adding **133**
- client devices **132**
- host devices **132**

CD-ROM drives, connecting **218**
Client Integration Plug-in, installing **189**
clock, synchronization between host and guest operating systems **214, 215, 217**
clone
- virtual machine to template in content library **80**
- VM template to template in content library **80**

cloning
- datastore considerations **40, 43**
- existing virtual machines **30, 36**
- templates to templates **41**
- virtual machines **19, 32, 33**
- virtual machines to templates **37, 38**

compatibility
- and hardware features **93**
- schedule upgrade for single virtual machine **92**
- schedule upgrade for virtual machines **249**
- setting virtual machine default **91**
- upgrading virtual machine **92**
- upgrading virtual machines **248**
- virtual machines **23, 89**

compatibility, virtual machine **92**
computer names, generating with a script **48**
configuration files, virtual machines **157, 164**
configuration parameters, virtual machines **164**
configuration utility for VMware Tools **215**
configure Flash Read Cache **124**
configuring
- floppy drives **134**
- parallel ports **114**
- SCSI devices **136**
- serial ports **110**
- video cards **138**
- VM network adapters **106**
- VM NICs **106**

Configuring Guest User Mappings Guest User Mappings **157**
connecting virtual devices **211, 218**
consoles, viewing virtual machine **189**
consolidation **12**
content library
- administrator **78**
- clone items between libraries **81**
- clone objects **78**
- clone templates between libraries **81**
- clone vApp to vApp template **80**
- cloning library items between libraries **81**
- create vApp on a cluster **84**

create vApp on a host **84**
create virtual machine from VM template **84**
create virtual machine on a cluster **84**
create virtual machine on a host **84**
creating vApps **84**
creating VMs **84**
delete **75**
deploy virtual machine **84**
description **71**
edit settings **74**
export item **82**
how to use **71**
import file **79**
import items **79**
import OVF **79**
import item **78**
import item from local file on your system **79**
import item from URL **79**
import item from Web server **79**
overview **71**
permissions **76**
URL **74**
user roles **78**
users **78**
controllers, *See* storage controllers
converting
in smaller IT environments **19**
physical systems **19**
templates to virtual machines **45**
copy and paste, of files and text **208, 211**
CPU performance counters, enabling **101**
CPU configuration, virtual machines **97**
CPU statistics **224, 225**
CPUs
advanced settings **98**
configuring **97**
defined **95**
disabling security **100**
enabling CPU/MMU Virtualization **101**
enabling hardware assisted virtualization **100**
enabling virtual performance counters **101**
hot plug **96**
hyperthreaded core sharing **98**
identification mask **100**
limitations **96**
limits **98**
parameters **95**
performance with hyperthreaded hosts **96**
reservation **98**
resources **98**
scheduling affinity **99**
shares **98**
create
content library **72**
vApp from vApp template in a library to a host or a cluster **84**
vApp from a vApp template in library **84**
virtual machine from VM template in library **84**
virtual machine from content library to a host or a cluster **84**
creating
datastore considerations **22**
vApps **168**
virtual machines **20**
custom sysprep answer file **59**
custom VMware Tools scripts **220, 221**
customization
changing specifications **60**
copying specifications **61**
creating Linux specifications **55**
creating Windows specification **59**
creating Windows specifications **56**
exporting specifications **61**
guest operating system requirements **47**
importing specifications **61**
Linux **47**
Windows **47**
customization specifications **54**

D

data centers **12**
datastores
ISO file **131**
leaving sufficient disk space **22, 29, 35, 40, 43**
roll in data center **12**
selecting **22, 29, 35, 40, 43**
selecting storage policy **29, 35, 40, 43**
sparse file behavior **29, 35, 40, 43**
thin provisioning considerations **29, 35, 40, 43**
uploading ISO image files **25**
debugging mode, for virtual machine **163**
default compatibility, setting for virtual machines **91**
delaying, boot sequence **162**
deleting
snapshots **203**
templates **193**
deploy, virtual machine from VM template in a library **84**
deploying
datastore considerations **29, 35**
OVF templates **63, 64**
virtual machines from templates **30, 36**
device drivers, virtual **206**
device command **214, 218**
disabling, acceleration **162**

disconnecting virtual devices **211, 218**
disk command **219**
disk formats
  thick provisioned **116**
  thin provisioned **116**
  virtual machines **125**
disks
  format **125**
  limits **123**
  shares **123**
  See also virtual disks
downtime
  during compatibility upgrade **231**
  during VMware Tools upgrade **231**
drag and drop, of files and text **208, 211**
drivers, VMware Tools **206**
DVD drives
  adding **133**
  client devices **132**
  connecting **218**
  host devices **132**

E

edit settings, subscribed library **75**
editing, vApp properties **169, 170**
ESX Agent Manager **186**
ESXi, managing single host **12**
exit codes **225**
exporting
  OVF templates **63, 68**
  virtual machines **68**

F

Fibre Channel NPIV settings **164**
Filesystem Sync drivers **206**
Flash Read Cache **115**
floppy drives
  adding **135**
  configuring **134**
  connecting **218**
FreeBSD guest operating system, VMware Tools installation or upgrade (tar installer) **245**

G

graphics, *See* 3D graphics
guest customization
  changing specifications **60**
  copying specifications **61**
  creating Linux specifications **55**
  creating Windows specifications **56, 59**
  exporting specifications **61**
  importing specifications **61**
  Linux customization during cloning or deployment **52**
  removing specifications **60**
  requirements **47**
  scripts **48**
  specifications **54**
  Windows customization during cloning or deployment **49**
guest operating systems
  configuring **157**
  customization requirements **47**
  customizing **30, 36**
  installing **24, 25**
  selecting **23**
Guest User Mappings **158**

H

hard disks
  adding **118, 119**
  adding boot disk **118**
  adding SCSI controllers for **118**
  adding to a virtual machine **121**
  SCSI device node options **118**
hardware, virtual machine **13, 89**
hardware devices
  SATA controllers **127**
  SCSI controllers **128**
hardware assisted virtualization, enabling **100**
hgfs.sys kernel module **206**
host devices
  CD drives **132**
  DVD drives **132**
host time **224**
hosts, viable for migration **100**
hot add enablement **96, 104**
hyperthreaded core sharing **98**

I

image files, ISO **131**
importing items to a library **79**
install, VMware Tools **17, 227**
installation media, uploading **25**
installing
  Client Integration Plug-in **189**
  guest operating systems from media **25**
  guest operating systems over PXE **24**
  Microsoft Sysprep tool **87**
  Virtual Machine Remote Console Plug-in **190**
installing VMware Tools
  FreeBSD (tar installer) **245**
  Linux (tar installer) **238**
  Mac OS X **241**
  Microsoft Windows **232**
  NetWare (tar installer) **243**

process overview **229**
silently on Windows guest operating systems **234**
Solaris (tar installer) **241**
inventory folders **12**
IP allocation, vApp **183**
IP address configuration **177, 178**
IP addresses, generating with a script **48**
ISO images, connecting **218**
ISO image files, uploading to datastore **25**
isolation.device.connectable.disable property **211**
isolation.device.edit.disable property **211**
isolation.tools.copy.disable property **211**
isolation.tools.diskShrink.disable property **211**
isolation.tools.diskWiper.disable property **211**
isolation.tools.paste.disable property **211**

L

legacy virtual machines, NICs **105**
library
add content **78**
administrator **78**
clone items between libraries **81**
clone templates between libraries **81**
clone vApp to vApp template **80**
cloning library items between libraries **81**
create **72**
create virtual machine from VM template **84**
create vApp on a cluster **84**
create vApp on a host **84**
create virtual machine on a cluster **84**
create virtual machine on a host **84**
deploy vApp on a cluster **84**
deploy vApp on a host **84**
deploy virtual machine **84**
edit settings **74**
export item **82**
import files **78**
import items **79**
import OVF **79**
import item from local file on your system **79**
import item from URL **79**
import item from Web server **79**
items **81**
methods to add content **78**
permissions **76**
populate with contents **78**
synchronize **74**
upload file **79**
URL **74**
user roles **78**
users **78**
library item
delete **83**
delete content **83**
delete the content of an item **83**
synchronize **82**
library items **81**
licensing, for resources, options, and hardware **12**
Linux
customizing during cloning or deployment **52**
guest operating system customization **47**
requirements for customization **47**
Linux operating system specific packages for VMware Tools **210, 240**
Linux guest, VMware Tools installation or upgrade (tar installer) **238**
logging, enabling **162**
logging property **211**
LSI Logic adapters, virtual **206**
LUNs **115**

M

Mac OS X guest operating system, VMware Tools installation or upgrade **241**
mask values **100**
memory, hot adding **104**
memory resources, allocating **103**
memory control drivers, virtual **206**
memory statistics **224, 225**
Microsoft Sysprep tool
installing **87**
installing from CD **88**
installing from Web **87**
Microsoft Windows guest operating system, VMware Tools installation or upgrade **232**
migration
cold **187**
cross-host Storage vMotion **116**
hot **187**
storage **116**
migration with vMotion, conditions for USB passthrough **142**
modifying VMware Tools modules **209**
mouse drivers, virtual **206**
multicore CPUs **96**

N

name-ip-generator **48**
names, virtual machines **156**
NetWare guest operating system, VMware Tools installation or upgrade (tar installer) **243**

NetWare, Novell **214**
network drivers, virtual **206**
network adapters
  adding **107**
  connecting **218**
  supported types **104**
network association settings **177**
network protocol profile
  associating with a port group **179**
  configuring vApp **179**
  configuring virtual machine **179**
networks, IP address configuration **177, 178**
NIC, *See* network adapters
NICs
  adding **107**
  legacy virtual machines **105**
NX flag **100**

O

Open Virtual Machine Format, *See also* OVF
Open Virtual Machine Tools suite **230**
Open Virtual Machine Tools **230**
operating system specific packages for VMware Tools in Linux virtual machines **210, 240**
operating systems, guest **24**
options
  vApps **180**
  virtual machine **155**
OSPs for installing VMWare Tools in Linux virtual machines **210, 240**
OVA, selecting, *See also* OVF
OVF
  browsing virtual appliance marketplace **67**
    deploying
      accept license agreements **65**
      configure networks **66**
      configure vService dependency **67**
      customize template **67**
      deployment configuration **65**
      review details **64**
      select resource **65**
      select source **64**
      select storage **66**
      specify name and location **65**
  deploying templates **63**
  exporting templates **63, 68**
  folder location for files **68**
  settings **184**
OVF Authoring options **181**

P

parallel ports
  adding **115**
  configuring **114**
paravirtual SCSI drivers **206**
paravirtualized SCSI adapters **130**
PCI devices, adding **137**
ports
  adding parallel **115**
  parallel **108**
  serial **108**
power off
  vApps **175**
  virtual machines **159**
power on
  vApps **175**
  virtual machines **159**
power states, virtual machine **159**
poweroff-vm-default script **222**
poweron-vm-default script **222**
preboot execution environment **24**
preface **7**
privileges, required
  for cloning virtual machines to templates **37**
  for cloning templates to templates **41**
  for cloning virtual machines **32**
  for common tasks **251**
  for converting templates to virtual machines **45**
  for creating virtual machines **20**
  for deploying virtual machines from templates **26**
processes, VMware user **208**
provisioning, virtual machines **17**
PXE **24**

Q

quiet mode for installing VMware Tools on Windows guests **234**

R

raw device mappings **115, 122**
RDMs, adding to a virtual machine **122**
Reduce Memory overhead **140**
registering, virtual machines **192**
removable devices **214, 218**
Remove SSO Users **158**
repairing VMware Tools installations **209, 210**
required privileges
  for cloning templates to templates **41**
  for cloning virtual machines to templates **37**
  for converting templates to virtual machines **45**
  for adding SCSI controllers **128**

for changing SCSI controller type **129**
for cloning virtual machines **32**
for common tasks **251**
for creating virtual machines **20**
for deploying virtual machines from templates **26**
resetting virtual machines **159**
resource pools, selecting **22, 29, 35, 46**
resources, virtual machine **13**
resources, virtual machine **15**
restart settings, for virtual machines **159**
resume
vApps **176**
virtual machines **159**
resume-vm-default script **222**

S

SAN LUNs **115**
SATA controllers
adding **127**
default behavior **126**
guest operating system support **127**
maximum number of **126**
node assignment **126**
See also storage controllers
scheduling affinity **99**
script command **220, 221**
scripts, VMware Tools **220–222**
SCSI, bus sharing **129**
SCSI controllers
adding **126, 128**
and virtual device nodes **126**
changing type **129**
default virtual hard disk assignments **126**
maximum number of **126**
types **126**
SCSI drivers, virtual **206**
SCSI adapters, paravirtualized **130**
SCSI devices
adding **136**
configuring **136**
security-related configuration settings **211**
selecting
datastores **22, 29, 35, 40, 43**
templates **28**
serial ports
adding **113**
adding Firewall rule set **109**
authentication parameters **111**
conditions for network connections **109**
conditions for physical connections **108**
configuring **110**
connection types **108**
URI for network connection **111**
service, VMware Tools **206**
services, VMware Tools **17, 227**
session ID **224**
shared folders, kernel module for **206**
shrinking a virtual disk **211, 214, 219**
shutdown, settings for virtual machines **159**
shutdown, settings, for virtual machines **187**
single host management **12**
smart card reader
adding to virtual machines **152**
shared **152**
snapshot, delta disks **196**
snapshots
about **194**
avoiding use as virtual machine backups **197**
behavior **194**
bus-sharing limitation **197**
child **194**
consolidating **203**
copy-on-write **196**
Delete all option **202**
Delete option **202**
deleting **202, 203**
delta disks **194**
files **196**
for virtual machines with large capacity disks **197**
hierarchy **194**
limitations **197**
manage **197**
memory **198**
memory files **196**
parent **194**
performance impact of **197**
quiescing **199**
quiescing virtual machine files **198**
restoring **200**
reverting to **200–202**
Snapshot Manager **197**
sparse disks **196**
taking **198, 199**
unsupported disk types **197**
virtual machine activity **198**
Solaris guest operating system, VMware Tools installation or upgrade (tar installer) **241**
solutions, monitor **185**
solutions,viewing **185**
sound adapters, connecting **218**
standby settings, for virtual machines **159**
startup settings, for virtual machines **187**

stat command **224, 225**
statistics, virtual machines **163**
status information, retrieving **224**
storage **115**
storage controllers
  adding SATA **127**
  adding SCSI **128**
  AHCI SATA **126**
  and snapshots **126**
  BusLogic Parallel **126**
  changing type **129**
  compatibility **126**
  IDE **126**
  limitations for VMware Paravirtual SCSI **130**
  limitations of **126**
  LSI Logic SAS **126**
  maximum number of **126**
  required privileges for changing type **129**
  SCSI **126**
  VMware Paravirtual SCSI **126, 130**
Storage vMotion, file name behavior **156**
subscribed library
  create **72**
  edit settings **75**
  synchronize **74**
subscribed library item, synchronize **82**
suspend-vm-default script **222**
suspending
  vApps **176**
  virtual machines **159**
SVGA drivers, virtual **206**
swap files, virtual machines **163**
synchronize an item in a library **82**
Sysprep tool
  installing **87**
  installing from CD **88**
  installing from Web **87**
Sysprep Answer Files
  custom **59**
  sysprep.inf **59**
  sysprep.xml **59**

T

taking, snapshots **199**
tar installer **238**
templates
  cloning to templates **42**
  converting to virtual machines **45, 46**
  creating **19**
  customizing guest operating systems **30, 36**
  deleting **193**
  deploying from **26**
  deploying virtual machines **27**
  finishing creation **41, 44**
  OVF **68**
  providing name and location **39, 43**
  removing from inventory **193**
  renaming **192**
  returning to inventory **193**
  returning to vCenter Server **192**
  selecting **28**
  selecting resource for **40, 43**
  selecting template to clone **42**
  unregistering **193**
thin provisioned disks **124**
time synchronization **214, 215, 217**
timesync command **215**
tools.guestlib.enableHostInfo property **211**
tools.setInfo.sizeLimit property **211**

U

uninstalling VMware Tools **210**
Unity feature **208**
unsigned drivers, in beta versions of VMware Tools **235**
updated information **9**
upgrade, VMware Tools **17, 227**
upgrade VMware Tools, automatic **247**
upgrading
  stage 4 **17**
  VMware Tools **160**
upgrading VMware Tools
  FreeBSD (tar installer) **245**
  Linux (tar installer) **238**
  Mac OS X **241**
  Microsoft Windows **232**
  NetWare (tar installer) **243**
  process overview **228**
  Solaris (tar installer) **241**
uploading files to datastore **25**
USB passthrough
  arbitrator for **140**
  autoconnect feature **141**
  avoiding data loss **143, 147**
  configuring from a client computer to a VM **147**
  configuring from a host to a virtual machine **140**
  controllers for **140, 147**
  devices, *See also* USB devices
  DRS requirements **142**
  features supported with **142**
USB controllers
  adding to virtual machine **144, 149**
  removing from virtual machine **152**

USB devices
adding from client computer to VM in the vSphere Web Client **150**
adding to client computers **149**
adding to hosts **144**
cascading hubs **143**
compound **143**
configuring for vMotion **142**
connecting **218**
connecting to a client computer **148**
device limits for Mac OS X guests **147**
ejecting from guest OS **146**
removing client computer device from VM **151**
removing from host **147**
removing from remote client **152**
removing host device from virtual machine **146**
setting up on host **143**
USB passthrough devices **146**
user process, VMware **208**
using, Virtual Machine Remote Console **190**
using library items **81**
utilities, VMware Tools **17, 227**

V

vApp
clone to template in library **80**
custom properties **183**
deploy from vApp template in a library **84**
IP allocation **183**
network protocol profile **179**
vApp options, advanced **182**
vApp power operations **175**
vApp properties **181**
vApp templates in content libraries **82**
vApps
adding objects to **169**
cloning **174**
configuring IPv4 **177**
configuring IPv6 **178**
configuring networks **172**
creating **168**
creating objects inside **169**
editing annotations **176**
editing properties **169, 170**
editing resources **171**
managing **167**
options **180**
power off settings **175**
power on settings **175**
product properties **173**
resuming **176**
selecting network associations **177**
shutdown options **173**
startup options **173**
suspending **176**
viewing license agreement **174**
viewing OVF Sections **172**
vCenter Server **12**
vCenter Solutions Manager **185**
video cards, configuring **138**
virtual devices
adding USB controller **144, 149**
CPU limitations **96**
See also virtual hardware
virtual disks
configuration **117**
configuring **115**
disk mode **199**
formats **116**
greater than 2TB **117**
high capacity **117**
limitations for high capacity **117**
requirements for high capacity **117**
requirements for guest operating system customization **47**
shrinking **211, 214, 219**
sparse **115**
thick format **124**
thin provisioning **115**
thin format **124**
virtual hard disks, adding **118, 119**
virtual hardware
adding USB devices **150**
CPU hyperthreading **98**
CPU advanced settings **99**
CPU/MMU enablement **101**
hot add enablement **96**
licenses for **12**
multicore CPUs **96**
parallel ports **115**
serial ports **113**
upgrading **227**
video cards **138**
virtual hardware upgrade, downtime **231**
virtual infrastructure **12**
virtual machine
clone to VM template in library **80**
customization specification **54**
Guest OS **54**
network protocol profile **179**
virtual machine compatibility
determining on host, cluster, or datacenter **92**
determining on virtual machine **92**
hardware features available with **93**

selecting for virtual machine creation **89**
setting default **89**
upgrading **89**
virtual machine console
installing **189, 190**
using **190**
virtual machine hardware
virtual disks **117**
See also virtual machines compatibility
virtual machine options **155**
Virtual Machine Communication Interface firewall **109**
virtual machine configuration file (.vmx file) **211**
virtual machine files **11**
virtual machine options overview **155**
Virtual Machine Remote Console
installing **190**
using **190**
virtual machine resources **13**
virtual machine templates
finishing creation **41, 44**
renaming **192**
selecting template to clone **42**
virtual machines
add existing **191**
adding **191**
adding hard disks **118, 119, 121**
adding raw device mappings **122**
boot sequence **162**
CD drives **132**
changing name of **156**
cloning **19, 32–34**
cloning existing **30, 36**
cloning to template **38, 39**
compatibility **23, 89, 92, 93**
components **13**
configuration files **157, 164**
configuration parameters **164**
configuring **89**
configuring 3D graphics **138**
configuring devices **131**
configuring guest operating systems **157**
console options **159**
CPU configuration **97**
CPU resources **95**
creating **19–21**
creating and deploying **13**
creating templates **19**
customizing hardware **24, 31, 37**
debugging information **163**
defined **11**
deploy and export **19**
deploying **19**
deploying from templates **26, 27, 46**
disk formats **125**
downtime during upgrade **231**
DVD drives **132**
enabling logging **162**
exporting **68**
features **93**
files **11**
finishing creation **24, 31, 37, 46**
floppy drives **134**
guest operating system **24**
hardware **13, 89**
hardware version, *See* virtual machines,compatibility
hardware versions **13**
hot add enablement **104**
introduction to **11**
lifecycle **13**
managing **187**
memory **102**
memory resources **103**
names **156**
naming **22, 28, 34**
network adapters **107**
network configuration **104**
options and resources **15**
parallel ports **114**
performance with hyperthreaded hosts **96**
power management settings **161**
power states **159**
privileges required for cloning **32**
provisioning **17, 19**
registering **192**
remove from the datastore **191**
remove from vCenter Server **191**
removing **191**
returning to vCenter Server **192**
schedule compatibility upgrade **249**
selecting **34, 39**
selecting folders **22, 28, 34**
selecting guest operating systems **23**
serial ports **110**
setting default compatibility **91**
shutdown settings **187**
snapshots **194**
startup settings **187**
statistics **163**
swap files **163**
upgrading compatibility **248**
upgrading Compatibility **92**

viewing consoles **189**
working file location **157**
See also templates, clones
See also virtual hardware
virtual memory
allocation **102**
configuring **102**
Virtual Serial Port Concentrator **108, 113**
VM NICs, configuring **106**
VM template, clone to VM template in library **80**
VM network adapters, configuring **106**
VM templates in content libraries **82**
VMCI drivers **206, 211**
vmci0.unrestricted property **211**
VMFS volume **115**
vmhgfs kernel module **206**
vMotion
compatibility **100**
limitations for USB passthrough **142**
Storage vMotion file name behavior **156**
without shared storage **187**
vmtoolsd **206**
VMware Tools
components of **205**
configuration utility **215**
configuring **205**
defined **13**
install and upgrade **17, 227**
installing and configuring **25**
requirement for customization **47**
security considerations **211**
upgrading **160**
VMware Compatibility Guide, accessing **47**
VMware Paravirtual SCSI controllers **130**
VMware Tools installation
automated install on Windows guests **234, 236**
FreeBSD (tar installer) **245**
Linux (tar installer) **238**
Mac OS X **241**
Microsoft Windows **232**
NetWare (tar installer) **243**
process **229**
repairing **209**
silent install on Windows guests **234, 236**
Solaris (tar installer) **241**
troubleshooting **209**
unsigned drivers **235**
VMware Tools scripts
custom **220, 221**
default **222**
disabling **223**
VMware Tools upgrade
downtime **231**
FreeBSD (tar installer) **245**
Linux (tar installer) **238**
Mac OS X **241**
Microsoft Windows **232**
NetWare (tar installer) **243**
process **228**
Solaris (tar installer) **241**
troubleshooting **209**
VMware Tools service **206**
VMware Tools upgrade, automatic **247**
VMware Tools,upgrading by using the vSphere Web Client **246**
VMware user process **208**
vmware-toolbox-cmd utility for Linux, Solaris, and FreeBSD guest operating systems **215**
vmware-tools-cli utility for Mac OS X guest operating systems with Fusion **215**
vmware-user, starting manually **210**
VMwareToolboxCmd.exe utility for Windows guest operating systems **215**
vmwtool command **214**
vmx.log.keepOld property **211**
vmxnet networking drivers **206**
Volume Shadow Copy Services drivers **206**
vSPC **108, 113**

W

web access, vSphere Web Client **16**
Windows
customizing during cloning or deployment **49**
guest operating system customization **47**
requirements for customization **47**
working with library items **81**