

# vSphere Virtual Machine Administration

Update 2

Modified on 12 AUG 2020

VMware vSphere 5.5

VMware ESXi 5.5

vCenter Server 5.5

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

<https://docs.vmware.com/>

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2009-2020 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

About vSphere Virtual Machine Administration 11

Updated Information 12

## 1 Introduction to VMware vSphere Virtual Machines 14

Virtual Machine Files 14

Virtual Machines and the Virtual Infrastructure 15

Virtual Machine Lifecycle 16

Virtual Machine Components 17

Virtual Machine Hardware Available to vSphere Virtual Machines 17

Virtual Machine Options and Resources 19

vSphere Web Client 21

VMware Tools 21

Where to Go From Here 22

## 2 Deploying Virtual Machines in the vSphere Web Client 23

About Provisioning Virtual Machines 23

Create a Virtual Machine Without a Template or Clone in the vSphere Web Client 24

Start the New Virtual Machine Creation Process 26

Select the Virtual Machine Name and Folder 26

Select a Resource 27

Select a Datastore 27

Select the Virtual Machine Compatibility 28

Select a Guest Operating System 28

Customize Virtual Machine Hardware in the vSphere Web Client 29

Finish Virtual Machine Creation 29

Installing a Guest Operating System 29

Deploy a Virtual Machine from a Template in the vSphere Web Client 32

Start the Deploy a Virtual Machine from a Template Task 33

Select a Template 34

Select the Virtual Machine Name and Folder 35

Select a Resource 35

Select a Datastore 35

Select Clone Options 37

Customize the Guest Operating System 37

Customize Virtual Machine Hardware in the vSphere Web Client 38

Finish Virtual Machine Creation 38

Clone a Virtual Machine in the vSphere Web Client 38

Start the Clone an Existing Virtual Machine Task	40
Select the Virtual Machine Name and Folder	41
Select a Resource	42
Select a Datastore	42
Select Clone Options	44
Customize the Guest Operating System	44
Customize Virtual Machine Hardware in the vSphere Web Client	45
Finish Virtual Machine Creation	45
Clone a Virtual Machine to a Template in the vSphere Web Client	45
Start the Clone a Virtual Machine to a Template Task	47
Select a Virtual Machine to Clone to a Template	47
Select a Name and Location for the Template	48
Select a Resource for a Virtual Machine Template	48
Select a Datastore for the Virtual Machine Template	48
Finish Virtual Machine Template Creation	49
Clone a Template to a Template in the vSphere Web Client	50
Start the Clone a Template to a Template Task	51
Select a Template to Clone in the vSphere Web Client	51
Select a Name and Location for the Template	52
Select a Resource for a Virtual Machine Template	52
Select a Datastore for the Virtual Machine Template	52
Finish Virtual Machine Template Creation	54
Convert a Template to a Virtual Machine in the vSphere Web Client	54
Start the Convert a Template to a Virtual Machine Task	55
Select a Template from Which to Deploy the Virtual Machine	55
Select a Resource	56
Finish Virtual Machine Creation	56
Customizing Guest Operating Systems in the vSphere Web Client	56
Guest Operating System Customization Requirements	57
Create a vCenter Server Application to Generate Computer Names and IP Addresses in the vSphere Web Client	57
Customize Windows During Cloning or Deployment in the vSphere Web Client	58
Customize Linux During Cloning or Deployment in the vSphere Web Client	61
Creating and Managing Customization Specifications in the vSphere Web Client	63

### 3 Deploying OVF Templates 71

OVF File Format and OVF Templates	71
Deploy an OVF Template in the vSphere Web Client	72
Select the OVF Source Location	72
Review the OVF Details	72
Accept the OVF License Agreements	73
Select OVF Name and Location	73

Select OVF Deployment Configuration	73
Select a Resource for the OVF Template	73
Select Storage for OVF Template	74
Configure Networks for OVF Template	75
Customize the OVF Template	75
Configure vService Dependency	76
Browse VMware Virtual Appliance Marketplace	76
Export an OVF Template	76

## 4 Installing the Microsoft Sysprep Tool 78

Install the Microsoft Sysprep Tool from a Microsoft Web Site	78
Install the Microsoft Sysprep Tool from the Windows Operating System CD	79
Install the Microsoft Sysprep Tool for VMware vCenter Server Appliance	80

## 5 Configuring Virtual Machine Hardware in the vSphere Web Client 82

Virtual Machine Compatibility	82
Set the Default Compatibility for Virtual Machine Creation in the vSphere Web Client	84
Schedule a Compatibility Upgrade for a Single Virtual Machine	85
Determine the Default Virtual Machine Compatibility Setting in the vSphere Web Client	86
Hardware Features Available with Virtual Machine Compatibility Settings	86
Virtual CPU Configuration	88
Virtual CPU Limitations	89
Configuring Multicore Virtual CPUs	90
Change CPU Hot Plug Settings in the vSphere Web Client	90
Change the Number of Virtual CPUs	91
Allocate CPU Resources in vSphere Web Client	92
Configure Hyperthreaded Core Sharing in the vSphere Web Client	93
Configure Processor Scheduling Affinity in the vSphere Web Client	93
Change CPU Identification Mask Settings in the vSphere Web Client	94
Expose VMware Hardware Assisted Virtualization in the vSphere Web Client	95
Enable Virtual CPU Performance Counters in the vSphere Web Client	95
Change CPU/MMU Virtualization Settings in the vSphere Web Client	96
Virtual Memory Configuration	97
Change the Memory Configuration in the vSphere Web Client	97
Allocate Memory Resources in the vSphere Web Client	98
Change Memory Hot Add Settings in the vSphere Web Client	99
Network Virtual Machine Configuration	99
Network Adapter Types	100
Network Adapters and Legacy Virtual Machines	101
Change the Virtual Network Adapter (NIC) Configuration in the vSphere Web Client	101
Add a Network Adapter to a Virtual Machine in the vSphere Web Client	102

Parallel and Serial Port Configuration	103
Using Serial Ports with vSphere Virtual Machines	103
Adding a Firewall Rule Set for Serial Port Network Connections	104
Change the Serial Port Configuration in the vSphere Web Client	105
Authentication Parameters for Virtual Serial Port Network Connections	107
Add a Serial Port to a Virtual Machine in the vSphere Web Client	108
Change the Parallel Port Configuration in the vSphere Web Client	110
Add a Parallel Port to a Virtual Machine in the vSphere Web Client	111
Virtual Disk Configuration	112
About Virtual Disk Provisioning Policies	113
Large Capacity Virtual Disk Conditions and Limitations	114
Change the Virtual Disk Configuration in the vSphere Web Client	114
Add a Hard Disk to a Virtual Machine in the vSphere Web Client	115
Use Disk Shares to Prioritize Virtual Machines in the vSphere Web Client	122
Configure Flash Read Cache for a Virtual Machine	123
Converting Virtual Disks from Thin to Thick in the vSphere Web Client	124
SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility	125
Add a SATA Controller	127
Add a SCSI Controller in the vSphere Web Client	128
Change the SCSI Bus Sharing Configuration in the vSphere Web Client	129
Change the SCSI Controller Type in the vSphere Web Client	129
About VMware Paravirtual SCSI Controllers	130
Add a Paravirtualized SCSI Adapter in the vSphere Web Client	130
Other Virtual Machine Device Configuration	131
Change the CD/DVD Drive Configuration in the vSphere Web Client	131
Add a CD or DVD Drive to a Virtual Machine in the vSphere Web Client	134
Change the Floppy Drive Configuration in the vSphere Web Client	135
Add a Floppy Drive to a Virtual Machine in the vSphere Web Client	136
Change the SCSI Device Configuration in the vSphere Web Client	137
Add a SCSI Device to a Virtual Machine in the vSphere Web Client	138
Add a PCI Device in the vSphere Web Client	138
Configuring 3D Graphics	139
USB Configuration from an ESXi Host to a Virtual Machine	142
USB Autoconnect Feature	143
vSphere Features Available with USB Passthrough	144
Configuring USB Devices for vMotion	144
Avoiding Data Loss with USB Devices	145
Connecting USB Devices to an ESXi Host	145
Connect USB Devices to an ESXi Host	147
Add a USB Controller to a Virtual Machine in the vSphere Web Client	147
Add USB Devices from an ESXi Host to a Virtual Machine in the vSphere Web Client	149

Remove USB Devices That Are Connected Through an ESXi Host	150
Remove USB Devices from an ESXi Host	150
USB Configuration from a Client Computer to a Virtual Machine in the vSphere Web Client	151
Connecting USB Devices to a Client Computer	152
Connect USB Devices to a Client Computer	153
Add a USB Controller to a Virtual Machine in the vSphere Web Client	153
Add USB Devices From a Client Computer to a Virtual Machine in the vSphere Web Client	155
Remove USB Devices That Are Connected Through a Client Computer in the vSphere Web Client	155
Remove a USB Controller from a Virtual Machine in the vSphere Web Client	156
Remove USB Devices from a Client Computer	157
Add a Shared Smart Card Reader to Virtual Machines in the vSphere Web Client	157

## 6 Configuring Virtual Machine Options in the vSphere Web Client 159

Virtual Machine Option Overview	159
Change the Virtual Machine Name in the vSphere Web Client	160
View the Virtual Machine Configuration and Working File Location in the vSphere Web Client	161
Change the Configured Guest Operating System in the vSphere Web Client	161
Change the Virtual Machine Console Options for Remote Users in the vSphere Web Client	162
Configure the Virtual Machine Power States in the vSphere Web Client	163
Configure Virtual Machines to Automatically Upgrade VMware Tools in the vSphere Web Client	164
Manage Power Management Settings for a Virtual Machine in the vSphere Web Client	165
Delay the Boot Sequence in the vSphere Web Client	166
Disable Virtual Machine Acceleration in the vSphere Web Client	166
Enable Virtual Machine Logging in the vSphere Web Client	167
Configure Virtual Machine Debugging and Statistics in the vSphere Web Client	167
Change the Swap File Location in the vSphere Web Client	168
Edit Configuration File Parameters	169
Configure Fibre Channel NPIV Settings in the vSphere Web Client	169

## 7 Managing Multi-Tiered Applications with vSphere vApp 171

Create a vApp	172
Create a Virtual Machine, Resource Pool, or Child vApp Inside a vApp	173
Add Virtual Machine or Child vApp to a vApp	173
Edit vApp Settings	174
Configure vApp Properties	175
Configure vApp CPU and Memory Resources	176
View Unrecognized OVF Sections	177
Configure vApp IP Allocation Policy	177
Configure vApp Startup and Shutdown Options	178

Configure vApp Product Properties	178
View vApp License Agreement	179
Clone a vApp	180
Perform vApp Power Operations	180
Power on a vApp	180
Power Off a vApp	181
Suspend a vApp	181
Resume a vApp	182
Edit vApp Notes	182
Add a Network Protocol Profile	182
Select the Network Protocol Profile Name and Network	183
Specify Network Protocol Profile IPv4 Configuration	183
Specify Network Protocol Profile IPv6 Configuration	184
Specify Network Protocol Profile DNS and Other Configuration	185
Complete the Network Protocol Profile Creation	185
Associate a Port Group with a Network Protocol Profile in the vSphere Web Client	185
Configure a Virtual Machine or vApp to Use a Network Protocol Profile in the vSphere Web Client	186
Virtual Machine vApp Options	187
Enable Virtual Machine vApp Options	187
Edit Application Properties and OVF Deployment Options for a Virtual Machine	188
Edit OVF Authoring Options for a Virtual Machine	188
<b>8 Monitoring Solutions with the vCenter Solutions Manager</b>	<b>193</b>
View Solutions and vServices in the vSphere Web Client	194
Monitoring Agents	194
Monitoring vServices	195
<b>9 Managing Virtual Machines</b>	<b>196</b>
Edit Virtual Machine Startup and Shutdown Settings in the vSphere Web Client	197
Install the Client Integration Plug-In	198
Using a Virtual Machine Remote Console	199
Open the HTML 5 Remote Console	199
Install the VMware Remote Console Application	200
Using the VMware Remote Console Application	201
Adding and Removing Virtual Machines	201
Adding Existing Virtual Machines to vCenter Server	201
Remove Virtual Machines from vCenter Server in the vSphere Web Client	201
Remove Virtual Machines from the Datastore in the vSphere Web Client	202
Register a Virtual Machine with the vSphere Web Client	202
Change the Template Name in the vSphere Web Client	203
Deleting Templates in the vSphere Web Client	203



Remove Templates from the Inventory in the vSphere Web Client	203
Delete a Template from the Disk in the vSphere Web Client	204
Reregister Templates in the vSphere Web Client	204
Using Snapshots To Manage Virtual Machines	205
Snapshot Files	207
Snapshot Limitations	208
Managing Snapshots	209
Taking Snapshots of a Virtual Machine	210
Restoring Snapshots	213
Deleting Snapshots	215
Consolidate Snapshots in the vSphere Web Client	217
Managing vServices in the vSphere Web Client	218
Add a vService Dependency in the vSphere Web Client	218
Remove a vService Dependency in the vSphere Web Client	219
Edit a vService Dependency in the vSphere Web Client	219
<b>10 VMware Tools Components, Configuration Options, and Security Requirements</b>	<b>220</b>
Components of VMware Tools	221
VMware Tools Service	221
VMware Tools Device Drivers	222
VMware User Process	223
Repairing, Changing, and Uninstalling VMware Tools Components	224
Repair or Change Modules in Windows Virtual Machines	224
Uninstall VMware Tools	226
Start the VMware User Process Manually If You Do Not Use a Session Manager	226
Security Considerations for Configuring VMware Tools	227
Using vmwtool to Configure VMware Tools in a NetWare Virtual Machine	231
Using the VMware Tools Configuration Utility	232
Configure Time Synchronization Between Guest and Host Operating Systems	233
Disable Time Synchronization Completely	235
Connect or Disconnect a Virtual Device	235
Shrink a Virtual Disk	237
Using Custom VMware Tools Scripts	238
Retrieve Status Information About the Virtual Machine	243
<b>11 Upgrading Virtual Machines</b>	<b>246</b>
Upgrading VMware Tools	247
Installing VMware Tools	249
Planning Downtime for Virtual Machines	250
Downtime for Upgrading Virtual Machines	250
Manually Install or Upgrade VMware Tools in a Windows Virtual Machine	251

Automate VMware Tools Installation for Multiple Windows Virtual Machines	254
Suppress Prompts About Unsigned Drivers on Windows Operating Systems Before Vista	255
Add VMware as a Trusted Publisher to Suppress Driver Prompts	256
Names of VMware Tools Components Used in Silent Installations	257
Manually Install or Upgrade VMware Tools in a Linux Virtual Machine	259
Operating System Specific Packages for Linux Guest Operating Systems	262
Manually Install or Upgrade VMware Tools in a Mac OS X Virtual Machine	263
Manually Install or Upgrade VMware Tools in a Solaris Virtual Machine	264
Manually Install or Upgrade VMware Tools in a NetWare Virtual Machine	266
Manually Install or Upgrade VMware Tools in a FreeBSD Virtual Machine	268
Upgrade VMware Tools by Using the vSphere Web Client	270
Perform an Automatic Upgrade of VMware Tools	270
Upgrade the Compatibility for Virtual Machines by Using the vSphere Web Client	272
Schedule a Compatibility Upgrade for Virtual Machines	273

## **12** Required Privileges for Common Tasks 275

# 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* document 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
12 AUG 2020	At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we are replacing some of the terminology in our content. We have updated this guide to remove instances of non-inclusive language.
16 JAN 2019	<ul style="list-style-type: none"><li>■ Added a prerequisite step in <a href="#">Change the Swap File Location in the vSphere Web Client</a>.</li><li>■ Added a reference to the MSCS documentation in <a href="#">About VMware Paravirtual SCSI Controllers</a>.</li><li>■ Updated information about virtual machine and template names in <a href="#">Select the Virtual Machine Name and Folder</a>, <a href="#">Select a Name and Location for the Template</a>, and <a href="#">Change the Virtual Machine Name in the vSphere Web Client</a>,</li></ul>
04 MAY 2018	<ul style="list-style-type: none"><li>■ Added information about the consequences of increasing the size of Eager Zeroed Thick virtual disks in <a href="#">About Virtual Disk Provisioning Policies</a> and in <a href="#">Change the Virtual Disk Configuration in the vSphere Web Client</a>, Step 3.</li><li>■ Added a note in <a href="#">Deleting Snapshots</a> explaining how deleting a single snapshot affects the virtual machine and other snapshots.</li><li>■ Added a note about the time synchronization default value in <a href="#">Configure Time Synchronization Between Guest and Host Operating Systems</a>.</li></ul>
14 FEB 2018	Changed the description of .vmsd and .vmsn files in <a href="#">Virtual Machine Files</a> .
03 OCT 2017	<ul style="list-style-type: none"><li>■ Added the power on a virtual machine task in <a href="#">Chapter 12 Required Privileges for Common Tasks</a>.</li><li>■ Added information about .hlog and .vmtx files in <a href="#">Virtual Machine Files</a>.</li><li>■ Corrected navigation instructions in the tasks in <a href="#">Add a vService Dependency in the vSphere Web Client</a>, <a href="#">Remove a vService Dependency in the vSphere Web Client</a>, and <a href="#">Edit a vService Dependency in the vSphere Web Client</a>.</li><li>■ Fixed the broken URL in <a href="#">Install the VMware Remote Console Application</a>.</li><li>■ Added information about the consequences of a virtual hardware version upgrade in <a href="#">Chapter 11 Upgrading Virtual Machines</a> and <a href="#">Upgrade the Compatibility for Virtual Machines by Using the vSphere Web Client</a>.</li></ul>
EN-001518-05	Removed the internal option from the Configure Hyperthreaded Core table. See <a href="#">Configure Hyperthreaded Core Sharing in the vSphere Web Client</a> .
EN-001518-04	<ul style="list-style-type: none"><li>■ Removed VMware Studio information from the multi-tiered application topic. See <a href="#">Chapter 7 Managing Multi-Tiered Applications with vSphere vApp</a>.</li></ul>

Revision	Description
EN-001518-03	<ul style="list-style-type: none"> <li>■ Updated information about VMware Tools component values. See <a href="#">Names of VMware Tools Components Used in Silent Installations</a>.</li> <li>■ Added a new topic about the HTML 5 Remote console to a virtual machine. See <a href="#">Open the HTML 5 Remote Console</a>.</li> <li>■ Updated information about the virtual machine remote consoles. See <a href="#">Using a Virtual Machine Remote Console</a>.</li> </ul>
EN-001518-02	<ul style="list-style-type: none"> <li>■ Updated procedures for installing VMware Tools depending on the operating system. See <a href="#">Installing VMware Tools</a>.</li> <li>■ Added information about automatic installation of the WDDM graphics drivers on Windows guest operating systems. See <a href="#">Upgrading VMware Tools</a>.</li> <li>■ Removed Datastore.Allocate space privilege from privileges required to take a virtual machine snapshot. See <a href="#">Chapter 12 Required Privileges for Common Tasks</a>.</li> <li>■ Updated information about virtual machine startup and shutdown settings. See <a href="#">Edit Virtual Machine Startup and Shutdown Settings in the vSphere Web Client</a>.</li> <li>■ Added a link to the requirements for configuring USB devices from a remote computer. See <a href="#">Connect USB Devices to a Client Computer</a>.</li> <li>■ Updated information about enabling the advanced options in the export an OVF template process. See <a href="#">Export an OVF Template</a>.</li> </ul>
EN-001518-01	<ul style="list-style-type: none"> <li>■ Corrected the KB link in <a href="#">Add a PCI Device in the vSphere Web Client</a>.</li> <li>■ Added the new topic <a href="#">Install the VMware Remote Console Application</a> that provides instructions for installing the VMware Remote Console (VMRC).</li> <li>■ Added the new topic <a href="#">Using the VMware Remote Console Application</a> that provides instructions for using the VMRC.</li> <li>■ Removed information about downloading the Client Integration Plugin (CIP) from a virtual machine console in <a href="#">Install the Client Integration Plug-In</a>.</li> </ul>
EN-001518-00	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:

- [Virtual Machine Files](#)
- [Virtual Machines and the Virtual Infrastructure](#)
- [Virtual Machine Lifecycle](#)
- [Virtual Machine Components](#)
- [Virtual Machine Hardware Available to vSphere Virtual Machines](#)
- [Virtual Machine Options and Resources](#)
- [vSphere Web Client](#)
- [VMware Tools](#)
- [Where to Go From Here](#)

## Virtual Machine Files

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	<i>vmname.vmx</i>	Virtual machine configuration file
.vmxf	<i>vmname.vmx</i> f	Additional virtual machine configuration files
.vmdk	<i>vmname.vmdk</i>	Virtual disk characteristics
-flat.vmdk	<i>vmname-flat.vmdk</i>	Virtual machine data disk
.nvram	<i>vmname.nvram</i> or <i>nvram</i>	Virtual machine BIOS or EFI configuration
.vmsd	<i>vmname.vmsd</i>	Virtual machine snapshot descriptions
.vmsn	<i>vmname.vmsn</i>	Virtual machine snapshot data file
.vswp	<i>vmname.vswp</i>	Virtual machine swap file
.vmss	<i>vmname.vmss</i>	Virtual machine suspend file
.log	<i>vmware.log</i>	Current virtual machine log file
-#.log	<i>vmware-#.log</i> (where # is a number starting with 1)	Old virtual machine log files

Additional files are created when you perform certain tasks with the virtual machine.

- A .hlog file is a log file that is used by vCenter Server to keep track of virtual machine files that must be removed after a certain operation completes.
- A .vmtx file is created when you convert a virtual machine to a template. The .vmtx file replaces the virtual machine configuration file (.vmx file).

## 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 hierarchical 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 datacenter 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 datacenter. 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](#).

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: <ul style="list-style-type: none"> <li>■ Intel 440BX AGPset 82443BX Host Bridge/Controller</li> <li>■ Intel 82371AB (PIIX4) PCI ISA IDE Xcelerator</li> <li>■ National Semiconductor PC87338 ACPI 1.0 and PC98/99 Compliant SuperI/O</li> <li>■ Intel 82093AA I/O Advanced Programmable Interrupt Controller</li> </ul>
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.
PCI Device	You can add up to six 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.

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

Hardware Device	Description
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. A virtual machine can use up to four virtual 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

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 use the shutdown or restart options from the toolbar. You can use only the power options.

## 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 in the vSphere Web Client

# 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](#)
- [Create a Virtual Machine Without a Template or Clone in the vSphere Web Client](#)
- [Deploy a Virtual Machine from a Template in the vSphere Web Client](#)
- [Clone a Virtual Machine in the vSphere Web Client](#)
- [Clone a Virtual Machine to a Template in the vSphere Web Client](#)
- [Clone a Template to a Template in the vSphere Web Client](#)
- [Convert a Template to a Virtual Machine in the vSphere Web Client](#)
- [Customizing Guest Operating Systems in the vSphere Web Client](#)

## 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 in the vSphere Web Client](#).

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](#).

Create a template to deploy multiple virtual machines from. A template is a primary 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 in the vSphere Web Client](#).

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 in the vSphere Web Client](#).

Cloning a virtual machine to a template preserves a primary 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 in the vSphere Web Client

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.

## Procedure

### 1 [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.

### 2 [Select the Virtual Machine Name and Folder](#)

When you create a virtual machine, you provide a name for it. The name must be unique within the folder where the virtual machine is located. 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](#)

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](#)

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](#)

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](#)

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 in the vSphere Web Client](#)

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

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

## 9 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.

# 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 name for it. The name must be unique within the folder where the virtual machine is located. 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 in a different way.

A folder cannot contain virtual machines with identical names.

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 Enter 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 <b>Next</b> .
Store all virtual machine files in the same datastore cluster.	<ol style="list-style-type: none"> <li>a Select a datastore cluster.</li> <li>b (Optional) If you do not want to use Storage DRS with this virtual machine, select <b>Disable Storage DRS for this virtual machine</b> and select a datastore within the datastore cluster.</li> <li>c Click <b>Next</b>.</li> </ol>

## 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](#).

### 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 in the vSphere Web Client

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 in the vSphere Web Client](#).

For help configuring other virtual machine hardware, see [Chapter 5 Configuring Virtual Machine Hardware in the vSphere Web Client](#).

### 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**.

### Results

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 in the vSphere Web Client](#).

### 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
<b>CD-ROM</b>	Insert the installation CD-ROM for your guest operating system into the CD-ROM drive of your ESXi host.
<b>ISO image</b>	<ol style="list-style-type: none"> <li>a Right-click the virtual machine and select <b>Edit Settings</b>. The virtual machine Edit Settings dialog box opens. If the <b>Virtual Hardware</b> tab is not preselected, select it.</li> <li>b Select <b>Datastore ISO File</b> from the CD/DVD drop-down menu, and browse for the ISO image for your guest operating system.</li> </ol>

- 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. Installing VMware Tools in the guest operating system is important. Although the guest operating system can run without VMware Tools, you lose important functionality and convenience without them. See [Chapter 11 Upgrading Virtual Machines](#) 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](#) . 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 in the vSphere Web Client

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](#)

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](#)

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

When you create a virtual machine, you provide a name for it. The name must be unique within the folder where the virtual machine is located. 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

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

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

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

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 in the vSphere Web Client

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

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
<b>Open the New Virtual Machine wizard from any object in the inventory</b>	<p>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 <b>New Virtual Machine</b>.</p> <p>b Select <b>Deploy from template</b> and click <b>Next</b>.</p> <p>The Select a name and folder page opens.</p>
<b>Open the Deploy From Template wizard from a template</b>	<p>Right-click the template and select <b>Deploy VM from this Template</b>.</p> <p>The Select a name and folder page opens.</p>

## 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 name for it. The name must be unique within the folder where the virtual machine is located. 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 in a different way.

A folder cannot contain virtual machines with identical names.

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 Enter 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
<b>Same format as source</b>	Use the same format as the source virtual machine.
<b>Thick Provision Lazy Zeroed</b>	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.
<b>Thick Provision Eager Zeroed</b>	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.
<b>Thin Provision</b>	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
<b>Store the virtual disk and virtual machine configuration files in the same location on a datastore.</b>	Select <b>Store with the virtual machine</b> from the <b>Location</b> drop-down menu.
<b>Store the disk in a separate datastore location.</b>	Select <b>Browse</b> from the <b>Location</b> drop-down menu, and select a datastore for the disk.
<b>Store all virtual machine files in the same datastore cluster.</b>	<ol style="list-style-type: none"> <li>a Select <b>Browse</b> from the <b>Location</b> drop-down menu and select a datastore cluster for the disk.</li> <li>b (Optional) If you do not want to use Storage DRS with this virtual machine, select <b>Disable Storage DRS for this virtual machine</b> and select a datastore within the datastore cluster.</li> </ol>

- 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](#).

### Procedure

- 1 Apply a customization specification to the virtual machine.

Option	Description
<b>Select an existing specification</b>	Select a customization specification from the list.
<b>Create a specification</b>	Click the <b>Create a new specification</b> icon, and complete the steps in the wizard.
<b>Create a specification from an existing specification</b>	<ol style="list-style-type: none"> <li>a Select a customization specification from the list.</li> <li>b Click the <b>Create a spec from an existing spec</b> icon, and complete the steps in the wizard.</li> </ol>

- 2 Click **Next**.

## Customize Virtual Machine Hardware in the vSphere Web Client

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 in the vSphere Web Client](#).

For help configuring other virtual machine hardware, see [Chapter 5 Configuring Virtual Machine Hardware in the vSphere Web Client](#).

### 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**.

### Results

The virtual machine appears in the vSphere Web Client inventory.

## Clone a Virtual Machine in the vSphere Web Client

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.

---

## 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

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

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

When you create a virtual machine, you provide a name for it. The name must be unique within the folder where the virtual machine is located. 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

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

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

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

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 in the vSphere Web Client

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

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
<b>Open the New Virtual Machine wizard from any object in the inventory</b>	<p>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 <b>New Virtual Machine</b>.</p> <p>b Select <b>Clone an existing virtual machine</b> and click <b>Next</b>.</p> <p>The Select a virtual machine page opens.</p>
<b>Open the Clone Existing Virtual Machine wizard from a virtual machine</b>	<p>Right-click the virtual machine and select <b>Clone to Virtual Machine</b>.</p> <p>The Select a name and folder page opens.</p>

## 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 name for it. The name must be unique within the folder where the virtual machine is located. 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 in a different way.

A folder cannot contain virtual machines with identical names.

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 Enter 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
<b>Same format as source</b>	Use the same format as the source virtual machine.
<b>Thick Provision Lazy Zeroed</b>	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.
<b>Thick Provision Eager Zeroed</b>	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.
<b>Thin Provision</b>	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
<b>Store the virtual disk and virtual machine configuration files in the same location on a datastore.</b>	Select <b>Store with the virtual machine</b> from the <b>Location</b> drop-down menu.
<b>Store the disk in a separate datastore location.</b>	Select <b>Browse</b> from the <b>Location</b> drop-down menu, and select a datastore for the disk.
<b>Store all virtual machine files in the same datastore cluster.</b>	<ol style="list-style-type: none"> <li>a Select <b>Browse</b> from the <b>Location</b> drop-down menu and select a datastore cluster for the disk.</li> <li>b (Optional) If you do not want to use Storage DRS with this virtual machine, select <b>Disable Storage DRS for this virtual machine</b> and select a datastore within the datastore cluster.</li> </ol>

- 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](#).

### Procedure

- 1 Apply a customization specification to the virtual machine.

Option	Description
<b>Select an existing specification</b>	Select a customization specification from the list.
<b>Create a specification</b>	Click the <b>Create a new specification</b> icon, and complete the steps in the wizard.
<b>Create a specification from an existing specification</b>	<ol style="list-style-type: none"> <li>a Select a customization specification from the list.</li> <li>b Click the <b>Create a spec from an existing spec</b> icon, and complete the steps in the wizard.</li> </ol>

- 2 Click **Next**.

## Customize Virtual Machine Hardware in the vSphere Web Client

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 in the vSphere Web Client](#).

For help configuring other virtual machine hardware, see [Chapter 5 Configuring Virtual Machine Hardware in the vSphere Web Client](#).

### 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**.

### Results

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 primary 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

To make a primary 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

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

When you deploy a template to the vCenter Server inventory, you provide a name for it. The name must be unique within the folder where the template is located. 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

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

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

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

# Start the Clone a Virtual Machine to a Template Task

To make a primary 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
<b>Open the New Virtual Machine wizard from any object in the inventory</b>	<p>a Right-click any inventory object that is a valid parent object of a virtual machine, such as a data center, folder, cluster, resource pool, or host, and select <b>New Virtual Machine</b>.</p> <p>b Select <b>Clone Virtual Machine to Template</b> and click <b>Next</b>.</p> <p>The Select a name and folder page opens.</p>
<b>Open the Clone Virtual Machine to Template wizard from a template</b>	<p>Right-click the virtual machine and select <b>All vCenter Actions &gt; Template &gt; Clone to Template</b>.</p> <p>The Select a name and folder page opens.</p>

## 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 name for it. The name must be unique within the folder where the template is located. 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.

A folder cannot contain virtual machines or templates with identical names.

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 Enter 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
<b>Same format as source</b>	Use the same format as the source virtual machine.
<b>Thick Provision Lazy Zeroed</b>	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.
<b>Thick Provision Eager Zeroed</b>	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.
<b>Thin Provision</b>	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
<b>Store the virtual disk and virtual machine configuration files in the same location on a datastore.</b>	Select <b>Store with the virtual machine</b> from the <b>Location</b> drop-down menu.
<b>Store the disk in a separate datastore location.</b>	Select <b>Browse</b> from the <b>Location</b> drop-down menu, and select a datastore for the disk.
<b>Store all virtual machine files in the same datastore cluster.</b>	<ol style="list-style-type: none"> <li>a Select <b>Browse</b> from the Location drop-down menu and select a datastore cluster for the disk.</li> <li>b (Optional) If you do not want to use Storage DRS with this virtual machine, select <b>Disable Storage DRS for this virtual machine</b> and select a datastore within the datastore cluster.</li> </ol>

- 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**.

### Results

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 primary 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](#)

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](#)

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](#)

When you deploy a template to the vCenter Server inventory, you provide a name for it. The name must be unique within the folder where the template is located. 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](#)

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

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

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
<b>Open the New Virtual Machine wizard from any object in the inventory</b>	<p>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 <b>New Virtual Machine</b>.</p> <p>b Select <b>Clone Template to Template</b> and click <b>Next</b>.</p> <p>The Select a name and folder page opens.</p>
<b>Open the Clone Template to Template wizard from a template</b>	<p>a Search or browse for a template.</p> <p>b Right-click the template and select <b>Clone</b>.</p> <p>The Select a name and folder page opens.</p>

## 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 name for it. The name must be unique within the folder where the template is located. 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.

A folder cannot contain virtual machines or templates with identical names.

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 Enter 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
<b>Same format as source</b>	Use the same format as the source virtual machine.
<b>Thick Provision Lazy Zeroed</b>	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.
<b>Thick Provision Eager Zeroed</b>	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.
<b>Thin Provision</b>	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
<b>Store the virtual disk and virtual machine configuration files in the same location on a datastore.</b>	Select <b>Store with the virtual machine</b> from the <b>Location</b> drop-down menu.
<b>Store the disk in a separate datastore location.</b>	Select <b>Browse</b> from the <b>Location</b> drop-down menu, and select a datastore for the disk.
<b>Store all virtual machine files in the same datastore cluster.</b>	<ol style="list-style-type: none"> <li>a Select <b>Browse</b> from the <b>Location</b> drop-down menu and select a datastore cluster for the disk.</li> <li>b (Optional) If you do not want to use Storage DRS with this virtual machine, select <b>Disable Storage DRS for this virtual machine</b> and select a datastore within the datastore cluster.</li> </ol>

- 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**.

### Results

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 in the vSphere Web Client

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 golden image for deploying virtual machines.

### Prerequisites

Verify 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](#)

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

#### 3 [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.

#### 4 Finish Virtual Machine Creation

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
<b>Open the New Virtual Machine wizard from any object in the inventory</b>	<p>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 <b>New Virtual Machine</b>.</p> <p>b Select <b>Convert template to virtual machine</b> and click <b>Next</b>.</p> <p>The Select a resource page opens.</p>
<b>Open the Convert Template to Virtual Machine wizard from a template</b>	<p>a Search or browse for a template.</p> <p>b Right-click the template and select <b>Convert to Virtual Machine</b>.</p> <p>The Select a resource page opens.</p>

### 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**.

### Results

The virtual machine appears in the vSphere Web Client inventory.

## Customizing Guest Operating Systems in the vSphere Web Client

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 current version of VMware Tools must be installed on the virtual machine or template to customize the guest operating system during cloning or deployment.

### 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 4 Installing the Microsoft Sysprep Tool](#).
- 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 in the vSphere Web Client

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**.

### Results

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 in the vSphere Web Client

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](#).

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.

Option	Action
<b>Enter a name</b>	<p>a Type a name.</p> <p>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.</p> <p>b (Optional) To ensure that the name is unique, select <b>Append a numeric value to ensure uniqueness</b>. This action appends a hyphen followed by a numeric value to the virtual machine name. The name is truncated if it exceeds 15 characters when combined with the numeric value.</p>
<b>Use the virtual machine name</b>	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 15 characters, it is truncated.
<b>Enter a name in the Clone/Deploy wizard</b>	The vSphere Web Client prompts you to enter a name after the cloning or deployment is complete.
<b>Generate a name using the custom application configured with vCenter Server</b>	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
<b>For non-server operating systems</b>	Type the Windows product key for the new guest operating system.
<b>For server operating systems</b>	<ul style="list-style-type: none"> <li>a Type the Windows product key for the new guest operating system.</li> <li>b Select <b>Include Server License Information</b>.</li> <li>c Select either <b>Per seat</b> or <b>Per server</b>.</li> <li>d If you selected <b>Per server</b>, enter the maximum number of simultaneous connections for the server to accept.</li> </ul>

- 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
<b>Typical settings</b>	<p>Select <b>Typical settings</b> and click <b>Next</b>.</p> <p>vCenter Server configures all network interfaces from a DHCP server using default settings.</p>
<b>Custom settings</b>	<ul style="list-style-type: none"> <li>a Select <b>Custom settings</b> and click <b>Next</b>.</li> <li>b For each network interface in the virtual machine, click the ellipsis button (...).</li> <li>c Enter IP address and other network settings and click <b>OK</b>.</li> <li>d When all network interfaces are configured, click <b>Next</b>.</li> </ul>

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

Option	Action
<b>Workgroup</b>	Type a workgroup name. For example, <b>MSHOME</b> .
<b>Windows Server Domain</b>	<ul style="list-style-type: none"> <li>a Type the domain name.</li> <li>b Type the user name and password for a user account that has permission to add a computer to the specified domain.</li> </ul>

- 10 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.

- 11 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**.

- 12 Click **Finish** to save your changes.

## Results

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 vSphere Web Client

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](#).

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
<b>Enter a name</b>	<p>a Type a name.</p> <p>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.</p> <p>b (Optional) To ensure that the name is unique, select <b>Append a numeric value to ensure uniqueness</b>. 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.</p>
<b>Use the virtual machine name</b>	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.
<b>Enter a name in the Clone/Deploy wizard</b>	The vSphere Web Client prompts you to enter a name after the cloning or deployment is complete.
<b>Generate a name using the custom application configured with vCenter Server</b>	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
<b>Typical settings</b>	<p>Select <b>Typical settings</b> and click <b>Next</b>.</p> <p>vCenter Server configures all network interfaces from a DHCP server using default settings.</p>
<b>Custom settings</b>	<p>a Select <b>Custom settings</b> and click <b>Next</b>.</p> <p>b For each network interface in the virtual machine, click the ellipsis button (...).</p> <p>c Enter IP address and other network settings and click <b>OK</b>.</p> <p>d When all network interfaces are configured, click <b>Next</b>.</p>

## 6 Enter DNS and domain settings.

## 7 Save the customized options as an .xml file.

- Select **Save this customization specification for later use**.
- Specify the filename for the specification and click **Next**.

## 8 Click **Finish** to save your changes.

## Results

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`.

# Creating and Managing Customization Specifications in the vSphere Web Client

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 in the vSphere Web Client

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](#).

### 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
<b>Enter a name</b>	<ol style="list-style-type: none"> <li>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.</li> <li>b (Optional) To ensure that the name is unique, select <b>Append a numeric value to ensure uniqueness</b>. 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.</li> </ol>
<b>Use the virtual machine name</b>	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.
<b>Enter a name in the Clone/Deploy wizard</b>	The vSphere Web Client prompts you to enter a name after the cloning or deployment is complete.
<b>Generate a name using the custom application configured with vCenter Server</b>	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
<b>Standard settings</b>	<p>Select <b>Use standard network settings</b> and click <b>Next</b>.</p> <p>vCenter Server configures all network interfaces from a DHCP server using default settings.</p>
<b>Custom settings</b>	<ol style="list-style-type: none"> <li>a Select <b>Manually select custom settings</b>.</li> <li>b For each network interface in the virtual machine, click the pencil icon.</li> <li>c Enter IP address and other network settings and click <b>OK</b>.</li> <li>d When all network interfaces are configured, click <b>Next</b>.</li> </ol>

- 8 Enter DNS and domain settings information.
- 9 Click **Finish** to save your changes.

## Results

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 in the vSphere Web Client

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](#).

### 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
<b>Enter a name</b>	<ol style="list-style-type: none"> <li>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.</li> <li>b (Optional) To ensure that the name is unique, select <b>Append a numeric value to ensure uniqueness</b>. 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.</li> </ol>
<b>Use the virtual machine name</b>	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.

Option	Action
<b>Enter a name in the Clone/Deploy wizard</b>	The vSphere Web Client prompts you to enter a name after the cloning or deployment is complete.
<b>Generate a name using the custom application configured with vCenter Server</b>	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
<b>For nonserver operating systems</b>	Type the Windows product key for the new guest operating system.
<b>For server operating systems</b>	<ul style="list-style-type: none"> <li>a Type the Windows product key for the new guest operating system.</li> <li>b Select <b>Include Server License Information</b>.</li> <li>c Select either <b>Per seat</b> or <b>Per server</b>.</li> <li>d If you select <b>Per server</b>, enter the maximum number of simultaneous connections for the server to accept.</li> </ul>

- 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
<b>Standard settings</b>	<p>Select <b>Use standard network settings</b> and click <b>Next</b>.</p> <p>vCenter Server configures all network interfaces from a DHCP server using default settings.</p>
<b>Custom settings</b>	<ul style="list-style-type: none"> <li>a Select <b>Manually select custom settings</b>.</li> <li>b For each network interface in the virtual machine, click the pencil icon.</li> <li>c Enter IP address and other network settings and click <b>OK</b>.</li> <li>d When all network interfaces are configured, click <b>Next</b>.</li> </ul>

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

Option	Action
<b>Workgroup</b>	Type a workgroup name. For example, <b>MSHOME</b> .
<b>Windows Server Domain</b>	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.

- 12** (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.

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

## Results

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](#).

## 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 <b>Browse</b> 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 <b>Typical settings</b> and click <b>Next</b> . vCenter Server configures all network interfaces from a DHCP server using default settings.
Custom settings	<ol style="list-style-type: none"> <li>a Select <b>Custom settings</b> and click <b>Next</b>.</li> <li>b For each network interface in the virtual machine, click the ellipsis button (...).</li> <li>c Enter IP address and other network settings and click <b>OK</b>.</li> <li>d When all network interfaces are configured, click <b>Next</b>.</li> </ol>

- 8 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.

- 9 Click **Finish** to save your changes.

## Results

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 in the vSphere Web Client

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**.

### Results

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**.

## Results

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**.

### Results

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

## Import a Customization Specification in the vSphere Web Client

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**.

### Results

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](#)
- [Deploy an OVF Template in the vSphere Web Client](#)
- [Browse VMware Virtual Appliance Marketplace](#)
- [Export an OVF Template](#)

## 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](#).

**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: <b>http://vmware.com/VMTN/appliance.ovf</b> .
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.



Option	Description
<b>Publisher</b>	Publisher of the OVF template, if a certificate included in the OVF template file specifies a publisher.
<b>Download size</b>	Size of the OVF file.
<b>Size on disk</b>	Size on disk after you deploy the OVF template.
<b>Description</b>	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 or 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
<b>Thick Provisioned Lazy Zeroed</b>	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.
<b>Thick Provision Eager Zeroed</b>	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 of disks.
<b>Thin Provision</b>	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
<b>Static - Manual</b>	You will be prompted to enter the IP addresses in the Appliance Properties page.
<b>Transient - IP Pool</b>	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.
<b>DHCP</b>	A DHCP server is used to allocate the IP addresses. Select this option only if a DHCP server is available in your environment.
<b>Static - IP Pool</b>	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 additional information or configurations in the exported template. The advanced settings include information about the BIOS UUID, MAC addresses, boot order, PCI Slot numbers, and configuration settings used by other applications, such as VMware vShield.

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.

# Installing the Microsoft Sysprep Tool

## 4

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 and VMware vCenter Server Appliance uses the functions of the Sysprep tool. Verify that your vCenter Server or VMware vCenter Server Appliance system 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 ("").
- If you are using the VMware vCenter Server Application, you must have access to the VMware vCenter Server Appliance Web console.

---

**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](#)
- [Install the Microsoft Sysprep Tool from the Windows Operating System CD](#)
- [Install the Microsoft Sysprep Tool for VMware vCenter Server Appliance](#)

## 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.

## Install the Microsoft Sysprep Tool for VMware vCenter Server Appliance

After you download and install the Microsoft Sysprep tool from the Microsoft Web site, you can use the VMware vCenter Server Appliance Web console to upload the files to the appliance.

#### 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.

When you upload the files to vCenter Server Appliance, the contents of the CAB file for the Sysprep Tool version that you downloaded are saved in /etc/vmware-vpx/sysprep/*OS*. For example, /etc/vmware-vpx/sysprep/2k or /etc/vmware-vpx/sysprep/xp.

#### Procedure

- 1 Download the Sysprep files from the Microsoft Download Center and save them to your local system.
- 2 Log in to the VMware vCenter Server Appliance Web console and click the vCenter Server **Summary** tab.
- 3 In the Utilities panel, click the Sysprep Files **Upload** button.



- 4 Select a Windows platform directory, and browse to the file.
- 5 Click **Open**.

The file is uploaded to the VCenter Server Appliance.

- 6 Click **Close**.

### Results

You can customize a new virtual machine with a supported Windows guest operating system when you clone an existing virtual machine.

# Configuring Virtual Machine Hardware in the vSphere Web Client

## 5

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](#)
- [Virtual CPU Configuration](#)
- [Virtual Memory Configuration](#)
- [Network Virtual Machine Configuration](#)
- [Parallel and Serial Port Configuration](#)
- [Virtual Disk Configuration](#)
- [SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility](#)
- [Other Virtual Machine Device Configuration](#)
- [USB Configuration from an ESXi Host to a Virtual Machine](#)
- [USB Configuration from a Client Computer to a Virtual Machine in the vSphere Web Client](#)
- [Add a Shared Smart Card Reader to Virtual Machines in the vSphere Web Client](#)

## 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, and ESXi 5.5.

**Table 5-1. Virtual Machine Compatibility Options**

Compatibility	Description
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 ESXi 5.5.
ESXi 5.0 and later	This virtual machine (hardware version 8) is compatible with ESXi 5.0, ESXi 5.1, and ESXi 5.5.
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, and ESXi 5.5.
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, and ESXi 5.5. 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 5.0 and ESXi 4.x hosts	ESX/ESX 4.0 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 5.0 and ESXi 4.x hosts	ESXi 5.0 and later	Gives you access to virtual hardware features that are not available with ESXi 4.x. Can also run on ESXi 5.1 and later hosts. <ul style="list-style-type: none"> <li>■ You cannot migrate this virtual machine to an ESXi 4.x host.</li> <li>■ This virtual machine does not have all the capabilities available to virtual machines that run on ESXi 5.1, for example, you cannot use 64 virtual processors.</li> </ul>
ESXi 5.5 host	ESXi 5.5 and later	Provides access to the latest virtual hardware features, but cannot share resources with earlier hosts.

If virtual machines do not have to stay compatible with older ESX/ESXi host versions, you can upgrade them.

- To maintain virtual machine compatibility with ESX/ESXi 3.5 hosts, upgrade the virtual machine on an ESX/ESXi 3.5 host, which results in a virtual machine upgrade to version 4.
- To maintain virtual machine compatibility with ESX/ESXi 4.x hosts, upgrade the virtual machine on an ESX/ESXi 4.x host, which results in a virtual machine upgrade to version 7.

## Set the Default Compatibility for Virtual Machine Creation in the vSphere Web Client

You can set the default compatibility for virtual machine creation on the host, cluster, or datacenter. 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 datacenter in the inventory.

Option	Action
<b>Host</b>	<ol style="list-style-type: none"> <li>Click the <b>Manage</b> tab, and click <b>Settings</b>.</li> <li>In the Virtual Machines section, select <b>Default VM Compatibility</b> and click <b>Edit</b>.</li> <li>Select the compatibility from the drop-down menu and click <b>OK</b>.</li> </ol> <p><b>Note</b> You can set the compatibility only on hosts that are not part of a cluster.</p>
<b>Cluster</b>	<ol style="list-style-type: none"> <li>Click the <b>Manage</b> tab and click <b>Settings</b>.</li> <li>In the Configuration section, select <b>General</b> and click the <b>Edit</b> button next to <b>Default VM Compatibility</b>.</li> <li>Select the compatibility from the drop-down menu and click <b>OK</b>.</li> </ol> <p>When you change the compatibility for a cluster, the compatibility for all hosts in the cluster changes as well.</p>
<b>Datacenter</b>	<ol style="list-style-type: none"> <li>Right-click the datacenter and select <b>Edit Default VM Compatibility</b>.</li> <li>Select the compatibility from the drop-down menu and click <b>OK</b>.</li> </ol>

## Results

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](#).

## Prerequisites

- Create a backup or snapshot of the virtual machines.
- Upgrade 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**.

#### Results

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 datacenter 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
<b>Virtual machine</b>	Select a virtual machine and click <b>All vCenter Actions &gt; Compatibility</b> . You can select <b>Upgrade VM Compatibility</b> or <b>Schedule VM Compatibility Upgrade</b> .
<b>Host, Cluster, Datacenter</b>	Right-click the object and select <b>All vCenter Actions &gt; Edit Default VM Compatibility</b> . 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 5-2. Supported Features for Virtual Machine Compatibility**

<b>Feature</b>	<b>ESXi 5.5 and later</b>	<b>ESXi 5.1 and later</b>	<b>ESXi 5.0 and later</b>	<b>ESX/ESXi 4.x and later</b>	<b>ESX/ESXi 3.5 and later</b>
Hardware version	10	9	8	7	4
Maximum memory (MB)	1035264	1035264	1035264	261120	65532
Maximum number of logical processors	64	64	32	8	4
Maximum number of cores (virtual CPUs) per socket	64	64	32	8	1
Maximum SCSI adapters	4	4	4	4	4
Bus Logic adapters	Y	Y	Y	Y	Y
LSI Logic adapters	Y	Y	Y	Y	Y
LSI Logic SAS adapters	Y	Y	Y	Y	N
VMware Paravirtual controllers	Y	Y	Y	Y	N
SATA controllers	4	N	N	N	N
Virtual SCSI disk	Y	Y	Y	Y	Y
SCSI passthrough	Y	Y	Y	Y	Y
SCSI hot plug support	Y	Y	Y	Y	Y
IDE nodes	Y	Y	Y	Y	Y
Virtual IDE disk	Y	Y	Y	Y	N
Virtual IDE CD-ROMs	Y	Y	Y	Y	Y
IDE hot plug support	N	N	N	N	N
Maximum NICs	10	10	10	10	4
PCNet32	Y	Y	Y	Y	Y
VMXNet	Y	Y	Y	Y	Y
VMXNet2	Y	Y	Y	Y	Y
VMXNet3	Y	Y	Y	Y	N
E1000	Y	Y	Y	Y	Y
E1000e	Y	Y	Y	N	N

**Table 5-2. Supported Features for Virtual Machine Compatibility (continued)**

<b>Feature</b>	<b>ESXi 5.5 and later</b>	<b>ESXi 5.1 and later</b>	<b>ESXi 5.0 and later</b>	<b>ESX/ESXi 4.x and later</b>	<b>ESX/ESXi 3.5 and later</b>
USB 1.x and 2.0	Y	Y	Y	Y	N
USB 3.0	Y	Y	Y	N	N
Maximum video memory (KB)	524288	524288	131072	131072	131072
SVGA displays	10	10	10	10	1
SVGA 3D hardware acceleration	Y	Y	Y	N	N
VMCI	Y	Y	Y	Y	N
PCI passthrough	6	6	6	6	0
PCI Hot plug support	Y	Y	Y	Y	N
Nested HV support	Y	Y	N	N	N
vPMC support	Y	Y	N	N	N
Serial ports	4	4	4	4	4
Parallel ports	3	3	3	3	3
Floppy devices	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 during virtual machine creation or after the guest operating system is installed. Some actions require you to power off the virtual machine before changing 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 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. It 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 cores.

## 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 to have up to 64 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 is the number of physical processor cores or two times that number if hyperthreading is enabled. For example, if a host has 64 logical CPUs, you can configure the virtual machine for 64 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 in the vSphere Web Client

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.

- VMware Tools is installed (Linux guest operating systems).
- 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**.

#### Results

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 to have up to 64 virtual CPUs. You can change the number of virtual CPUs while the virtual machine is running or turned off.

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.
- If CPU hot remove is not enabled, turn off the virtual machine before removing 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 in vSphere Web Client

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
<b>Reservation</b>	Guaranteed CPU allocation for this virtual machine.
<b>Limit</b>	Upper limit for this virtual machine's CPU allocation. Select <b>Unlimited</b> to specify no upper limit.
<b>Shares</b>	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 <b>Low</b> , <b>Normal</b> , or <b>High</b> , which specify share values respectively in a 1:2:4 ratio. Select <b>Custom</b> to give each virtual machine a specific number of shares, which express a proportional weight.

### 3 Click **OK**.

## Configure Hyperthreaded Core Sharing in the vSphere Web Client

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.

---

**Note** Hyperthreaded core sharing is only supported for ESXi hosts version 5.0 and earlier.

---

### 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
<b>Any (default)</b>	The virtual CPUs of this virtual machine can share cores with other virtual CPUs of this or other virtual machines.
<b>None</b>	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.

### 3 Click **OK**.

## Configure Processor Scheduling Affinity in the vSphere Web Client

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**.

- On the **Virtual Hardware** tab, expand **CPU**, and in the **CPUID Mask** drop-down menu, select an NX/XD option.

Option	Description
<b>Hide the NX/XD flag from guest</b>	Increases vMotion compatibility. Hiding the NX/XD flag increases vMotion compatibility between hosts, but might disable certain CPU security features.
<b>Expose the NX/XD flag to guest</b>	Keeps all CPU security features enabled.
<b>Keep current Advanced setting values for the NX/XD flag</b>	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.

- Click **OK**.

## Expose VMware Hardware Assisted Virtualization in the vSphere Web Client

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

- Right-click a virtual machine in the inventory and select **Edit Settings**.
- On the **Virtual Hardware** tab, expand **CPU**, and select **Expose hardware-assisted virtualization to guest OS**.
- Click **OK**.

The **Manage** tab refreshes, and the Nested Hypervisor CPU option shows **Enabled**.

## Enable Virtual CPU Performance Counters in the vSphere Web Client

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 in the vSphere Web Client

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.

#### 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 in the vSphere Web Client

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 5-3. Maximum Virtual Machine Memory**

Introduced in Host Version	Virtual Machine Compatibility	Maximum Memory Size
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	65,532MB

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 in the vSphere Web Client

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
<b>Reservation</b>	Guaranteed memory allocation for this virtual machine.
<b>Limit</b>	Upper limit for this virtual machine's memory allocation. Select <b>Unlimited</b> to specify no upper limit.
<b>Shares</b>	The values <b>Low</b> , <b>Normal</b> , <b>High</b> , and <b>Custom</b> are compared to the sum of all shares of all virtual machines on the server.

- 3 Click **OK**.

## Change Memory Hot Add Settings in the vSphere Web Client

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:

### **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 Vlane adapter when a virtual machine boots, but initializes itself and functions as either a Vlane or a VMXNET adapter, depending on which driver initializes it. With VMware Tools installed, the VMXNET driver changes the Vlane adapter to the higher performance VMXNET adapter.

### **Vlane**

Emulated version of the AMD 79C970 PCnet32 LANCE NIC, an older 10 Mbps NIC with drivers available in most 32-bit guest operating systems except Windows Vista and later. 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 Network Adapter (NIC) Configuration in the vSphere Web Client

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.

### 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 network to connect to from the drop-down menu.

The menu lists all networks configured for virtual machine use on the host.

- 3 (Optional) Change the **Status** settings.

Option	Description
<b>Connected</b>	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.
<b>Connect at power on</b>	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 you want.
- 6 Click **OK**.

## Add a Network Adapter to a Virtual Machine in the vSphere Web Client

You can add a network adapter (NIC) to a virtual machine to bridge 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, and whether the device should connect when the virtual machine is turned on.

### 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
<b>Connected</b>	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 not turned on.
<b>Connect at power on</b>	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 **Network Connection** drop-down menu, select the network to connect to.
- The menu lists all networks configured for virtual machine use on the host.
- 7 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.

### Unsupported Serial Ports

When you use a physical serial port for serial port passthrough from an ESXi host to a virtual machine, the following serial ports are not supported.

- Serial ports present on add-on expansion cards might be supported by PCI DirectPath I/O. See [Add a PCI Device in the vSphere Web Client](#).
- 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](#).

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.

## Change the Serial Port Configuration in the vSphere Web Client

A virtual machine can use up to four virtual serial ports. 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.

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](#).
- To connect a serial port over a network, add a Firewall rule set. See [Adding a Firewall Rule Set for Serial Port Network Connections](#).
- To use authentication parameters with network serial port connections, see [Authentication Parameters for Virtual Serial Port Network Connections](#).
- 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
<b>Use physical serial port</b>	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.
<b>Use output file</b>	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.
<b>Use named pipe</b>	<p>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.</p> <ol style="list-style-type: none"> <li>Type a name for the pipe in the <b>Pipe Name</b> field.</li> <li>Select the <b>Near end</b> and <b>Far end</b> of the pipe from the drop-down menus.</li> </ol>
<b>Connect over the network</b>	<p>Select <b>Use network</b> to connect through a remote network.</p> <ol style="list-style-type: none"> <li>Select the network backing. <ul style="list-style-type: none"> <li>Select <b>Server</b> to have the virtual machine monitor incoming connections from other hosts.</li> <li>Select <b>Client</b> to have the virtual machine initiate a connection to another host.</li> </ul> </li> <li>Enter a <b>Port URI</b>. <p>The URI is the remote end of the serial port to which the virtual machine's serial port should connect.</p> </li> <li>If vSPC is used as an intermediate step to access all virtual machines through a single IP address, select <b>Use Virtual Serial Port Concentrator</b> and enter the vSPC URI location.</li> </ol>
<b>Printer</b>	Select <b>Printer</b> 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.

<b>thumbprint=value</b>	Specifies a certificate thumbprint against which the peer certificate thumbprint is compared. When you specify a thumbprint, certificate verification is enabled.
<b>peerName=value</b>	Specifies the peer name that is used to validate the peer certificate. When you specify a peer name, certificate verification is enabled.

<b>verify</b>	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
<b>cipherList=<i>value</i></b>	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 in the vSphere Web Client

A virtual machine can use up to four virtual serial ports. 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.

### Prerequisites

- Verify that the virtual machine is powered off.
- 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](#).
- To connect a serial port over a network, add a Firewall rule set. See [Adding a Firewall Rule Set for Serial Port Network Connections](#).
- To use authentication parameter with network serial port connections, see [Authentication Parameters for Virtual Serial Port Network Connections](#).
- 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
<b>Use physical serial port</b>	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.
<b>Use output file</b>	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.
<b>Use named pipe</b>	<p>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.</p> <ol style="list-style-type: none"> <li>a Type a name for the pipe in the <b>Pipe Name</b> field.</li> <li>b Select the <b>Near end</b> and <b>Far end</b> of the pipe from the drop-down menus.</li> </ol>

Option	Action
<b>Connect over the network</b>	<p>Select <b>Use network</b> to connect through a remote network.</p> <ol style="list-style-type: none"> <li>Select the network backing. <ul style="list-style-type: none"> <li>Select <b>Server</b> to have the virtual machine monitor incoming connections from other hosts.</li> <li>Select <b>Client</b> to have the virtual machine initiate a connection to another host.</li> </ul> </li> <li>Enter a <b>Port URI</b>. <p>The URI is the remote end of the serial port to which the virtual machine's serial port should connect.</p> </li> <li>If vSPC is used as an intermediate step to access all virtual machines through a single IP address, select <b>Use Virtual Serial Port Concentrator</b> and enter the vSPC URI location.</li> </ol>
<b>Printer</b>	Select <b>Printer</b> 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 in the vSphere Web Client

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 in the vSphere Web Client

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**.

## Results

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. Increasing the size of an Eager Zeroed Thick virtual disk causes a significant stun time for the virtual machine.

### 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 in the vSphere Web Client

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.

---

**Important** Extending the size of a virtual hard disk causes stun time for the virtual machine. The stun time is longer if the virtual disk is of the Eager Zeroed Thick type.

---

- 4 (Optional) To change the way that disks are affected by snapshots, select a disk mode option.

Option	Description
<b>Dependent</b>	Dependent disks are included in snapshots.
<b>Independent - Persistent</b>	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.
<b>Independent - Nonpersistent</b>	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 in the vSphere Web Client

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](#).

**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 in the vSphere Web Client](#)

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 in the vSphere Web Client](#)

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 in the vSphere Web Client](#)

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 in the vSphere Web Client**

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](#).

### Prerequisites

- Ensure that you are familiar with configuration options and caveats for adding virtual hard disks. See [Virtual Disk Configuration](#).
- Before you add disks greater than 2TB to a virtual machine, see [Large Capacity Virtual Disk Conditions and Limitations](#).
- 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
<b>Store all virtual machine files in the same location on a datastore.</b>	<p>a (Optional) Apply a virtual machine storage profile for the virtual machine home files and the virtual disks from the <b>VM Storage Profile</b> drop-down menu.</p> <p>The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage profile.</p> <p>b Select a datastore and click <b>Next</b>.</p>
<b>Store all virtual machine files in the same datastore cluster.</b>	<p>a (Optional) Apply a virtual machine storage profile for the virtual machine home files and the virtual disks from the <b>VM Storage Profile</b> drop-down menu.</p> <p>The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage profile.</p> <p>b Select a datastore cluster.</p> <p>c (Optional) If you do not want to use Storage DRS with this virtual machine, select <b>Disable Storage DRS for this virtual machine</b> and select a datastore within the datastore cluster.</p> <p>d Click <b>Next</b>.</p>
<b>Store virtual machine configuration files and disks in separate locations.</b>	<p>a Click <b>Advanced</b>.</p> <p>b For the virtual machine configuration file and for each virtual disk, click <b>Browse</b> and select a datastore or datastore cluster.</p> <p>c (Optional) Apply a virtual machine storage profile from the <b>VM Storage Profile</b> drop-down menu.</p> <p>The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage profile.</p> <p>d (Optional) If you selected a datastore cluster and do not want to use Storage DRS with this virtual machine, select <b>Disable Storage DRS for this virtual machine</b> and select a datastore within the datastore cluster.</p> <p>e Click <b>Next</b>.</p>

## 7 Select the format for the virtual machine's disks and click **Next**.

Option	Action
<b>Thick Provision Lazy Zeroed</b>	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.
<b>Thick Provision Eager Zeroed</b>	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.
<b>Thin Provision</b>	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
<b>Dependent</b>	Dependent disks are included in snapshots.
<b>Independent - Persistent</b>	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.
<b>Independent - Nonpersistent</b>	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 in the vSphere Web Client

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 in the vSphere Web Client](#).

- Before you add disks greater than 2TB to a virtual machine, see [Large Capacity Virtual Disk Conditions and Limitations](#).
- 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 in the vSphere Web Client](#).
- (Optional) Use disk shares to prioritize virtual machine access to this disk. See [Use Disk Shares to Prioritize Virtual Machines in the vSphere Web Client](#).

### Add an RDM Disk to a Virtual Machine in the vSphere Web Client

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 in the vSphere Web Client](#).
- Before you add disks greater than 2TB to a virtual machine, see [Large Capacity Virtual Disk Conditions and Limitations](#).
- 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
<b>Physical</b>	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.
<b>Virtual</b>	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
<b>Dependent</b>	Dependent disks are included in snapshots.
<b>Independent - Persistent</b>	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.
<b>Independent - Nonpersistent</b>	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 in the vSphere Web Client

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 5.5* white paper on the VMware web site.

### Prerequisites

Verify that the virtual machine is compatible with ESXi 5.5 or later.

### Procedure

- 1 To locate a virtual machine, select a datacenter, 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
<b>Reservation</b>	Select a cache size reservation.
<b>Block Size</b>	Select a block size.

- 7 Click **OK**.

## Converting Virtual Disks from Thin to Thick in the vSphere Web Client

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**.

## Results

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 5-4. VMware Storage Controller Compatibility

Existing Controller	Added 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

Table 5-4. VMware Storage Controller Compatibility (continued)

Existing Controller	Added Controller					
	BusLogic Parallel	LSI Logic	LSI Logic SAS	VMware Paravirtual SCSI	AHCI SATA	IDE
<b>VMware Paravirtual SCSI</b>	Requires BIOS setup	Requires BIOS setup	Usually Works	Usually Works	Requires BIOS setup	Yes
<b>AHCI SATA</b>	Requires BIOS setup	Requires BIOS setup	Yes	Yes	Yes	Yes
<b>IDE</b>	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](#).
- 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](#).

#### 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
<b>None</b>	Virtual disks cannot be shared by other virtual machines.
<b>Virtual</b>	Virtual disks can be shared by virtual machines on the same ESXi host. Select <b>Thick provision eager zeroed</b> when you create the disk.
<b>Physical</b>	Virtual disks can be shared by virtual machines on any ESXi host. Select <b>Thick provision eager zeroed</b> 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
<b>None</b>	Virtual disks cannot be shared by other virtual machines.
<b>Virtual</b>	Virtual disks can be shared by virtual machines on the same ESXi host.
<b>Physical</b>	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](#).
- 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 more information about configuring MSCS clusters, see the *Setup for Failover Clustering and Microsoft Cluster Service* documentation.

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](#).

### 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](#).
- 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](#)  
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](#)  
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](#)  
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](#).

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.

### Results

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](#).

- 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
<b>Client Device</b>	<ol style="list-style-type: none"> <li>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.</li> <li>b From the <b>Device Mode</b> drop-down menu, select <b>Passthrough IDE</b>.</li> </ol>
<b>Host Device</b>	<ol style="list-style-type: none"> <li>a Select to connect the CD/DVD device to a physical DVD or CD device on the host.</li> <li>b From the <b>CD/DVD Media</b> drop-down menu, select the media to connect to .</li> <li>c From the <b>Device Mode</b> drop-down menu, select <b>Emulate IDE</b>.</li> </ol>
<b>Datastore ISO File</b>	<ol style="list-style-type: none"> <li>a Select to connect the CD/DVD device to an ISO file that is stored on a datastore accessible to the host.</li> <li>b Browse to the file containing the ISO image to connect to and click <b>OK</b>.</li> </ol>

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
<b>Client Device</b>	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.
<b>Use existing floppy image</b>	<ol style="list-style-type: none"> <li>a Select this option to connect the virtual device to an existing floppy image on a datastore accessible to the host.</li> <li>b Click <b>Browse</b> and select the floppy image.</li> </ol>
<b>Create new floppy image</b>	<ol style="list-style-type: none"> <li>a Select this option to create a floppy image on a datastore accessible to the host.</li> <li>b Click <b>Browse</b> and browse to the location for the floppy image.</li> <li>c Enter a name for the floppy image and click <b>OK</b>.</li> </ol>

- 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
<b>Client Device</b>	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.
<b>Use existing floppy image</b>	<ol style="list-style-type: none"> <li>a Select this option to connect the virtual device to an existing floppy image on a datastore accessible to the host.</li> <li>b Click <b>Browse</b> and select the floppy image.</li> </ol>
<b>Create new floppy image</b>	<ol style="list-style-type: none"> <li>a Select this option to create a floppy image on a datastore accessible to the host.</li> <li>b Click <b>Browse</b> and browse to the location for the floppy image.</li> <li>c Enter a name for the floppy image and click <b>OK</b>.</li> </ol>

- 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](#).

### 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](#).

### 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**.

### Results

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>.

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 5-5. 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

You can select the 3D rendering options for each virtual machine to be Hardware, Software, or Automatic.

Table 5-6. 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 is 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.

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 in the vSphere Web Client

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](#).
- 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
<b>Auto-detect settings</b>	Applies common video settings to the guest operating system.
<b>Specify custom settings</b>	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
<b>Automatic</b>	Selects the appropriate option (software or hardware) for this virtual machine.
<b>Software</b>	Uses normal CPU processing for 3D calculations.
<b>Hardware</b>	Requires graphics hardware (GPU) for faster 3D calculations.
<b>Note</b> The virtual machine will not power on if graphics hardware is not available.	

**9** Click **OK**.**Results**

Sufficient memory allocation is set for this virtual machine's graphics.

## 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 2.0 and USB 1.1 devices must exist on the host. Two 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>.

## 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.

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 5-7. 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](#).

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 USB 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](#).
- 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.

## Connect 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](#).
- Verify that the ESXi host is powered off before you add USB CD/DVD-ROM devices.

### Procedure

- ◆ To add a USB device to an ESXi host, connect the device to an available port or hub.

### What to do next

You can now add the device to the virtual machine. See [Add USB Devices from an ESXi Host to a Virtual Machine in the vSphere Web Client](#).

## Add a USB Controller to a Virtual Machine in the vSphere Web Client

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 two USB controllers to a virtual machine. The xHCI controller, available for Linux, Windows 8 and later, and Windows Server 2012 and later guest operating systems, supports USB 3.0 superspeed, 2.0, and 1.1 devices. The EHCI+UHCI controller supports USB 2.0 and 1.1 devices.

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 5-8. 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 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 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 in the vSphere Web Client

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 in the vSphere Web Client](#).
- 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](#).
- 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](#).
- 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 in the vSphere Web Client

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. See [USB Configuration from a Client Computer to a Virtual Machine in the vSphere Web Client](#).

### Procedure

- ◆ To add a USB device to a client computer, connect the device to an available port or hub.

### Results

The USB device appears in the toolbar menu.

### What to do next

You can now add the USB device to the virtual machine. See [Add USB Devices From a Client Computer to a Virtual Machine in the vSphere Web Client](#).

## Add a USB Controller to a Virtual Machine in the vSphere Web Client

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 two USB controllers to a virtual machine. The xHCI controller, available for Linux, Windows 8 and later, and Windows Server 2012 and later guest operating systems, supports USB 3.0 superspeed, 2.0, and 1.1 devices. The EHCI+UHCI controller supports USB 2.0 and 1.1 devices.

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 5-9. 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 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 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.

### Results

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.

### Results

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 in the vSphere Web Client

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 in the vSphere Web Client](#).

### 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**.

### Results

You can now use smart card authentication to log in to virtual machines in the vSphere Web Client inventory.

# Configuring Virtual Machine Options in the vSphere Web Client

## 6

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](#)
- [Change the Virtual Machine Name in the vSphere Web Client](#)
- [View the Virtual Machine Configuration and Working File Location in the vSphere Web Client](#)
- [Change the Configured Guest Operating System in the vSphere Web Client](#)
- [Change the Virtual Machine Console Options for Remote Users in the vSphere Web Client](#)
- [Configure the Virtual Machine Power States in the vSphere Web Client](#)
- [Configure Virtual Machines to Automatically Upgrade VMware Tools in the vSphere Web Client](#)
- [Manage Power Management Settings for a Virtual Machine in the vSphere Web Client](#)
- [Delay the Boot Sequence in the vSphere Web Client](#)
- [Disable Virtual Machine Acceleration in the vSphere Web Client](#)
- [Enable Virtual Machine Logging in the vSphere Web Client](#)
- [Configure Virtual Machine Debugging and Statistics in the vSphere Web Client](#)
- [Change the Swap File Location in the vSphere Web Client](#)
- [Edit Configuration File Parameters](#)
- [Configure Fibre Channel NPIV Settings in the vSphere Web Client](#)

## 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 6-1. 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 6-2. 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 in the vSphere Web Client

A virtual machine must have a name that is unique within the folder where the virtual machine is located. If you move a virtual machine to a different datastore folder or host that has an existing virtual machine of the same name, you must 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 filenames 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 enter 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 in the vSphere Web Client

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 in the vSphere Web Client

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**.

## Change the Virtual Machine Console Options for Remote Users in the vSphere Web Client

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 in the vSphere Web Client

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
<b>Shut Down Guest</b>	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.
<b>Power Off</b>	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.
<b>Default</b>	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
<b>Suspend</b>	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.
<b>System Default</b>	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
<b>Restart Guest</b>	Uses VMware Tools to initiate an orderly restart. Soft power operations are possible only if the tools are installed in the guest operating system.
<b>Reset</b>	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.
<b>System Default</b>	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 in the vSphere Web Client

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 not supported for virtual machines with Solaris or NetWare guest operating systems.

### Prerequisites

- Verify that the virtual machines have a version of VMware Tools shipped with ESX/ESXi 3.5 or later installed.
- Verify that the virtual machines are hosted on ESX/ESXi 3.5 or later and vCenter Server 3.5 or later.
- Verify that the virtual machines are running a Linux or Windows guest OS that ESX/ESXi 3.5 or later and vCenter Server 3.5 or later support.

### 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 the **Check and upgrade VMware Tools before each power on** check box.
- 4 Click **OK** to save your changes.

## Manage Power Management Settings for a Virtual Machine in the vSphere Web Client

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
<b>Suspend the virtual machine</b>	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.
<b>Put the guest operating system in standby mode and leave the virtual machine powered on</b>	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 in the vSphere Web Client

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 in the vSphere Web Client

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**.

#### Results

You should be able to install or run the software successfully.

## Enable Virtual Machine Logging in the vSphere Web Client

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**.

#### Results

You can view and compare log files in the same storage location as the virtual machine configuration files.

## Configure Virtual Machine Debugging and Statistics in the vSphere Web Client

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 in the vSphere Web Client

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.

### 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 swap file location option.

Option	Description
<b>Default</b>	Stores the virtual machine swap file at the default location defined by the host or cluster swap file settings.
<b>Virtual machine directory</b>	Stores the virtual machine swap file in the same folder as the virtual machine configuration file.
<b>Datastore specified by host</b>	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 in the vSphere Web Client

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

# 7

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.

---

This chapter includes the following topics:

- [Create a vApp](#)
- [Create a Virtual Machine, Resource Pool, or Child vApp Inside a vApp](#)
- [Add Virtual Machine or Child vApp to a vApp](#)
- [Edit vApp Settings](#)
- [Clone a vApp](#)
- [Perform vApp Power Operations](#)
- [Edit vApp Notes](#)
- [Add a Network Protocol Profile](#)
- [Virtual Machine vApp Options](#)

## 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
<b>Shares</b>	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 <b>Low</b> , <b>Normal</b> , or <b>High</b> , which specify share values respectively in a 1:2:4 ratio. Select <b>Custom</b> to give each vApp a specific number of shares, which express a proportional weight.
<b>Reservation</b>	Guaranteed CPU allocation for this vApp.
<b>Reservation Type</b>	Select the <b>Expandable</b> 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.
<b>Limit</b>	Upper limit for this vApp's CPU allocation. Select <b>Unlimited</b> to specify no upper limit.

- 6 In the Deployment section, click Memory resources to allocate memory resources to this vApp.

Option	Description
<b>Shares</b>	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 <b>Low</b> , <b>Normal</b> , or <b>High</b> , which specify share values respectively in a 1:2:4 ratio. Select <b>Custom</b> to give each vApp a specific number of shares, which express a proportional weight.
<b>Reservation</b>	Guaranteed memory allocation for this vApp.
<b>Reservation Type</b>	Select the <b>Expandable</b> 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.
<b>Limit</b>	Upper limit for this vApp's memory allocation. Select <b>Unlimited</b> 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.

### Results

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](#)

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](#)

You can configure the CPU and memory resource allocation for the vApp.

- 3 [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.

- 4 [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.

- 5 [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.

- 6 [Configure vApp Product Properties](#)

You can configure product and vendor information for a vApp.

- 7 [View vApp License Agreement](#)

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
<b>Application Properties</b>	Displays non-editable product information such as name, vendor, and version, and allows specifying values for vApp custom properties.
<b>Deployment</b>	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.
<b>Authoring</b>	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
<b>Shares</b>	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 <b>Low</b> , <b>Normal</b> , or <b>High</b> , which specify share values respectively in a 1:2:4 ratio. Select <b>Custom</b> to give each vApp a specific number of shares, which express a proportional weight.
<b>Reservation</b>	Guaranteed CPU allocation for this vApp.
<b>Reservation Type</b>	Select the <b>Expandable</b> 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.
<b>Limit</b>	Upper limit for this vApp's CPU allocation. Select <b>Unlimited</b> to specify no upper limit.

- 3 In the Deployment section, click Memory resources to allocate memory resources to this vApp.

Option	Description
<b>Shares</b>	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 <b>Low</b> , <b>Normal</b> , or <b>High</b> , which specify share values respectively in a 1:2:4 ratio. Select <b>Custom</b> to give each vApp a specific number of shares, which express a proportional weight.
<b>Reservation</b>	Guaranteed memory allocation for this vApp.
<b>Reservation Type</b>	Select the <b>Expandable</b> 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.
<b>Limit</b>	Upper limit for this vApp's memory allocation. Select <b>Unlimited</b> 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
<b>Static - Manual</b>	IP addresses are manually configured. No automatic allocation is performed.
<b>Transient - IP Pool</b>	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.
<b>DHCP</b>	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.
<b>Static - IP Pool</b>	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
<b>Product Name</b>	Product Name.
<b>Version</b>	vApp version.
<b>Full Version</b>	Full version of the vApp.
<b>Product URL</b>	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.
<b>Vendor URL</b>	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.
<b>Application URL</b>	The vApp Summary page you can view in the vSphere Client includes a Status pane that includes information about vApp status, for example <b>Running</b> or <b>Stopped</b> . If you enter a valid application URL, the virtual machine Status pane displays <b>Available</b> instead of Running. The <b>Available</b> 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.

## Results

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**.

### Results

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 datacenter, to power on the vApp or virtual machine you must assign a protocol profile to the connected port group on the destination datacenter.

---

### Procedure

- 1 [Select the Network Protocol Profile Name and Network](#)  
Name the network protocol profile and select the network that should use it.
- 2 [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.

### 3 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.

### 4 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.

### 5 Complete the Network Protocol Profile Creation

### 6 Associate a Port Group with a Network Protocol Profile in the vSphere Web Client

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 in the vSphere Web Client

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 datacenter 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 in the vSphere Web Client

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 datacenter. 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 in the vSphere Web Client

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 Navigate to the virtual machine or the vApp in the inventory of the vSphere Web Client.
- 2 In the vSphere Web Client, 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**.

### Results

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
<b>Static - Manual</b>	IP addresses are manually configured. No automatic allocation is performed.
<b>Transient - IP Pool</b>	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.
<b>DHCP</b>	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.
<b>Static - IP Pool</b>	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.

### Procedure

#### 1 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.

#### 2 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.

#### 3 Edit vApp IP Allocation Policy for a Virtual Machine

You can edit the IP allocation policy through the Virtual Machine Properties dialog box.

#### 4 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.

## 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
<b>Product Name</b>	Product Name.
<b>Version</b>	vApp version.
<b>Full Version</b>	Full version of the vApp.
<b>Product URL</b>	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.
<b>Vendor URL</b>	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.
<b>Application URL</b>	The vApp Summary page you can view in the vSphere Client includes a Status pane that includes information about vApp status, for example <b>Running</b> or <b>Stopped</b> . If you enter a valid application URL, the virtual machine Status pane displays <b>Available</b> instead of Running. The <b>Available</b> 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](#).
  - 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
<b>OVF environment</b>	Determined by the environment in which you deploy the OVF template.
<b>DHCP</b>	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
<b>OVF environment</b>	Click <b>View</b> to display the OVF environment settings in XML format. The settings are not available when the virtual machine is powered off.
<b>OVF environment transport</b>	<ul style="list-style-type: none"><li>■ If you select ISO image, an ISO image that contains the OVF template information is mounted in the CD-ROM drive.</li><li>■ If you select VMware Tools, the VMware Tools <code>guestInfo.ovfEnv</code> variable is initialized with the OVF environment document.</li></ul>
<b>Installation boot</b>	If you click Enable, the virtual machine reboots after the 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

## 8

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. Another standard solution that vSphere provides is vService Manager.

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:

- [View Solutions and vServices in the vSphere Web Client](#)
- [Monitoring Agents](#)
- [Monitoring vServices](#)

## View Solutions and vServices in the vSphere Web Client

In the vSphere Web Client, you can view information about solutions and vService providers. A vService is a service that a solution provides to specific applications that run inside virtual machines and vApps.

### Procedure

- 1 Navigate to the vCenter Server system in the object navigator.
- 2 Double-click the vCenter Server object.
- 3 Click **Extensions**.
- 4 Select a solution.  
The **Summary** tab displays more information about the solution.
- 5 To view vService provider information, click **Monitor**, and click **vServices**.

## 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 8-1. 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.

## Monitoring vServices

A vService is a service or function that a solution provides to virtual machines and vApps. A solution can provide one or more vServices. These vServices integrate with the platform and are able to change the environment in which the vApp or virtual machine runs.

A vService is a type of service for a virtual machine and a vApp provided by a vCenter extension. Virtual machines and vApps can have dependencies on vServices. Each dependency is associated with a vService type. The vService type must be bound to a particular vCenter extension that implements that vService type. This vService type is similar to a virtual hardware device. For example, a virtual machine can have a networking device that at deployment must be connected to a particular network.

The vService Manager allows a solution to connect to operations related to OVF templates:

- Importing OVF templates. Receive a callback when OVF templates with a vService dependency of a certain type is imported.
- Exporting OVF templates. Inserts OVF sections when a virtual machine is exported.
- OVF environment generation. Inserts OVF sections into the OVF environment at the power-on instance.

The **vServices** tab in the Solution Manager provides details for each vCenter extension. This information allows you to monitor vService providers and list the virtual machines or vApps to which they are bound.

# Managing Virtual Machines

# 9

You can manage individual virtual machines or a group of virtual machines that belongs to a host or cluster. If you have vCenter Server systems in your environment that are connected with vCenter Linked Mode, you can connect to that vCenter Server system and view and manage all virtual machines that run in that system.

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 in the vSphere Web Client](#)
- [Install the Client Integration Plug-In](#)
- [Using a Virtual Machine Remote Console](#)
- [Open the HTML 5 Remote Console](#)
- [Install the VMware Remote Console Application](#)
- [Using the VMware Remote Console Application](#)
- [Adding and Removing Virtual Machines](#)
- [Change the Template Name in the vSphere Web Client](#)
- [Deleting Templates in the vSphere Web Client](#)
- [Using Snapshots To Manage Virtual Machines](#)
- [Managing vServices in the vSphere Web Client](#)

## Edit Virtual Machine Startup and Shutdown Settings in the vSphere Web Client

You can configure virtual machines running on an ESXi host to start up and shut down with the host or after a delay. You can also set the default timing and startup order for selected virtual machines. This way, the operating system has enough time 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. See *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
<b>Startup Delay</b>	After you start the ESXi host, it starts powering on the virtual machines that are configured for automatic startup. After the ESXi host powers on the first virtual machine, the host waits for the specified delay time and then powers on the next virtual machine. The virtual machines are powered on in the startup order specified in the Per-VM Overrides pane.
<b>Continue immediately if VMware Tools starts</b>	Shortens the startup delay of the virtual machine. If VMware Tools starts before the specified delay time passes, the ESXi host powers on the next virtual machine without waiting for the delay time to pass.
<b>Shutdown Delay</b>	When you power off the ESXi host, it starts powering off the virtual machines that run on it. The order in which virtual machines are powered off is the reverse of their startup order. After the ESXi host powers off the first virtual machine, the host waits for the specified shutdown delay time and then powers off the next virtual machine. The ESXi host shuts down only after all virtual machines are powered off.
<b>Shutdown Action</b>	Select a shutdown action that is applicable to the virtual machines on the host when the host shuts down. <ul style="list-style-type: none"> <li>■ Power Off</li> <li>■ Suspend</li> <li>■ Guest Shutdown</li> </ul>

- 6 (Optional) In the Per-VM Overrides pane, configure the startup order and behavior for individual virtual machines.

Use this option when you need the delay of the virtual machine to be different than the default delay for all machines. The settings that you configure for individual virtual machines override the default settings for all 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.

Use the up and down arrows to change the startup order for virtual machines in the Automatic Startup category. During shutdown, the virtual machines shut down in the reverse order.

- b Click **Startup Behavior**, select **Custom**, and configure the startup delay before the next virtual machine in the sequence is powered on.
- c Click **VMware Tools**, and select whether the ESXi host waits for the delay to pass when VMware Tools is already installed on the virtual machine.

If you select the **Continue if VMware Tools is installed** the ESXi host powers on the next virtual machine without waiting for the delay to pass. If you select the **Do not continue if VMware Tools is installed** the ESXi host waits 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](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
<b>vSphere Web Client login page</b>	<ol style="list-style-type: none"> <li>a Open a Web browser and type the URL for the vSphere Web Client.</li> <li>b At the bottom of the vSphere Web Client login page, click <b>Download Client Integration Plug-in</b>.</li> </ol>
<b>OVF deployment wizard</b>	<ol style="list-style-type: none"> <li>a Select a host in the inventory and select <b>Actions &gt; All vCenter Actions &gt; Deploy OVF Template</b>.</li> <li>b Click <b>Download Client Integration Plug-in</b>.</li> </ol>

- 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.

## Using a Virtual Machine Remote Console

With the vSphere Web Client, you can access a virtual machine's desktop by launching a remote console to the virtual machine.

From the virtual machine remote console, you can perform tasks in the virtual machine such as installing an operating system, configuring the operating system settings, running applications, monitoring performance, and so on. In the vSphere Web Client there are two different virtual machine remote consoles.

The VMware Remote Console (VMRC) standalone application for Windows that opens in a separate window. The VMware Remote Console standalone application has extended functionality that enables you to connect to client devices and launch virtual machine consoles on remote hosts.

The HTML 5 remote console opens in a browser tab. Some functions might not be available when you use the HTML 5 remote console.

## Open the HTML 5 Remote Console

With the vSphere Web Client, you can access a virtual machine's desktop by launching the HTML 5 remote console to the virtual machine. From the HTML 5 remote console, you can perform tasks in the virtual machine such as installing an operating system, configuring the operating system settings, running applications, monitoring performance, and so on.

### 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](#).
- 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 In the vSphere Web Client, navigate to a virtual machine in the inventory.
- 2 Right-click the virtual machine and select **Open Console**.  
The HTML 5 remote console opens in a new tab of the Web browser.
- 3 Click anywhere inside the console window to start using your mouse, keyboard, and other input devices in the console.
- 4 (Optional) Click **Send Ctrl-Alt-Delete** to send the Ctrl+Alt+Delete keystroke combination to the guest operating system.
- 5 (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.
- 6 (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.
- 7 (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 <http://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](http://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 in the vSphere Web Client

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-register 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**.

### Results

vCenter Server removes references to the virtual machine and no longer tracks its condition.

## Remove Virtual Machines from the Datastore in the vSphere Web Client

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**.

### Results

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 the vSphere Web Client

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 <b>Next</b> .
Run the virtual machine in a cluster with DRS automatic placement.	Select the cluster and click <b>Next</b> .
Run the virtual machine in a cluster without DRS automatic placement.	<ol style="list-style-type: none"> <li>a Select the cluster and click <b>Next</b>.</li> <li>b Select a host within the cluster and click <b>Next</b>.</li> </ol>

- 6 Select a resource pool in which to run the virtual machine and click **Next**.
- 7 Review your selections and click **Finish**.

#### Results

The virtual machine is added to the vCenter Server inventory.

## Change the Template Name in the vSphere Web Client

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 in the vSphere Web Client

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 in the vSphere Web Client

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-register 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 in the vSphere Web Client

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 in the vSphere Web Client

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
<b>Host</b>	Browse to the host. Click the <b>Related Objects</b> tab, and click <b>VM Templates</b> .
<b>Cluster</b>	Browse to the cluster. In the inventory view, select <b>VM Templates</b> to display the list of templates.

## Results

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
<code>vmname-number.vmdk</code> and <code>vmname-number-delta.vmdk</code>	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, <code>S1vm-000001.vmdk</code> where <code>S1vm</code> is the name of the virtual machine and the six-digit number, <code>000001</code> , 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.
<code>vmname.vmsd</code>	Database of the virtual machine's snapshot information and the primary source of information for the Snapshot Manager.
<code>vmname.Snapshotnumber.vmsn</code>	Memory state of the virtual machine at the time you take the snapshot. The file name uses the following syntax, <code>S1vm.snapshot1.vmsn</code> , where <code>S1vm</code> is the virtual machine name, and <code>snapshot1</code> is the first snapshot.  <b>Note</b> A <code>.vmsn</code> file is created each time you take a snapshot, regardless of the memory selection. A <code>.vmsn</code> 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 in the vSphere Web Client

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
<b>Independent - Persistent</b>	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.
<b>Independent - Nonpersistent</b>	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**.

## Take a Snapshot in the vSphere Web Client

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** If you take a snapshot of a Dynamic Disk (Microsoft specific disk type), the snapshot technology preserves the quiesce state of the file system, but does not preserve the quiesce state of the application.

---

### 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 in 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 9-1. Virtual Machine Power State After Restoring a Snapshot**

<b>Virtual Machine State When Parent Snapshot Is Taken</b>	<b>Virtual Machine State After Restoration</b>
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 in the vSphere Web Client

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**.

### Results

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 in the vSphere Web Client

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 in the vSphere Web Client](#).

### 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.

---

**Note** Deleting a single snapshot preserves the current state of the virtual machine and does not affect any other 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](#).
- 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
<b>Delete</b>	Consolidates the snapshot data to the parent snapshot and removes the selected snapshot from the Snapshot Manager and virtual machine.
<b>Delete All</b>	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 in the vSphere Web Client

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 **Related Objects** 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 > Snapshots > Consolidate**.
- 3 Check the Needs Consolidation column to verify that the task succeeded.
 

If the task succeeded, a Not Required 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 Not Required.

## Managing vServices in the vSphere Web Client

A vService dependency allows a vApp or a virtual machine to request that a vService be available on a specified platform.

A vService specifies a particular service on which vApps and virtual machines can depend.

The vService management page tab displays all the dependencies that a virtual machine or vApp has and each of their states.

### Add a vService Dependency in the vSphere Web Client

You can add a vService dependency to a virtual machine or vApp. This dependency allows a virtual machine or vApp to request that a specific vService be available.

#### Prerequisites

The virtual machine must be powered off before adding a dependency.

#### Procedure

- 1 Display the virtual machine or vApp in the inventory.
- 2 Under the **Manage** tab, click the **vServices** tab.
- 3 Click **Add**.

The **New vService Dependency** opens.

- 4 On the **Select provider type** wizard, select the provider for this dependency and click **Next**.
- 5 On the **Describe dependency** page, enter a name and description for this dependency and click **Next**.
- 6 On the **Bind dependency** page, determine whether the dependency is required and whether to bind it to the provider immediately. Click **Next**.

Required dependencies must be bound before powering on.

The **Bind to provider immediately** option requires validation of the binding. The validation result shows in the wizard pane. If the validation fails, you cannot continue. To finish creating the dependency, you must choose to bind the dependency to the provider later.

- 7 On the **Ready to complete** page, review the options and click **Finish** to create the dependency.

#### Results

The new dependency is added to the list of dependencies.

## Remove a vService Dependency in the vSphere Web Client

You can remove a vService dependency from a virtual machine or vApp.

### Procedure

- 1 Display the virtual machine or vApp in the inventory.
- 2 Click the **Manage** tab and click **vServices**.
- 3 Select the dependency and click **Remove**.

### Results

The dependency is removed from the list.

## Edit a vService Dependency in the vSphere Web Client

You can edit a vService dependency name, description, and requirement.

### Procedure

- 1 Display the virtual machine or vApp in the inventory.
- 2 Click the **Manage** tab and click **vServices**.
- 3 Select a dependency and click **Edit**.
- 4 In the **Dependency Properties** dialog box, edit the dependency name and description.
- 5 Select or deselect the check box to change the required status of the dependency.

The required check box is disabled if the virtual machine or vApp is running.

- 6 Select a provider for the dependency.

When you select a provider, the description is entered containing the provider description. The validation box displays the results of the validation. If validation fails, the **OK** button is disabled until another provider or no provider is selected.

- 7 Click **OK**.

# VMware Tools Components, Configuration Options, and Security Requirements

# 10

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, you can set parameters to protect virtual machines against security risks that VMware Tools settings might expose.

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 11 Upgrading Virtual Machines](#).
- 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](#)
- [Repairing, Changing, and Uninstalling VMware Tools Components](#)
- [Security Considerations for Configuring VMware Tools](#)
- [Using vmwtool to Configure VMware Tools in a NetWare Virtual Machine](#)
- [Using the VMware Tools Configuration Utility](#)

## 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, many VMware features are not available until you install VMware Tools.

### 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, 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, except in Mac OS X guest operating systems.
- 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 guest operating systems, allows the pointer to move freely between the guest and the Workstation, Fusion, or Player host operating system.

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. This functionality is performed by the VMware Tools service container (`vmtoolsd`).
- In Windows and Mac OS X guest operating systems, fits the screen display resolution of the guest to the screen resolution of the Workstation, Fusion, or Player host, 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. This functionality is performed by the VMware Tools service container (`vmtoolsd`).
- In Windows guest operating systems, helps create the quiesced snapshots used by certain backup applications.

- In Linux, Solaris, and FreeBSD guest operating systems, runs commands 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 system-bound calls created with the VMware VIX API, except in Mac OS X guest operating systems.

## VMware Tools Device Drivers

Device drivers smooth mouse operations, make VMware features such as folder sharing available, 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

Included with VMware Tools is the VMware Paravirtual SCSI driver 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 is for VMware Paravirtual SCSI adapters, which enhance 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 User Process**

With the VMware user process, you can use such features as copy and paste, drag and drop, and Unity with VMware products that support these features.

This 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. On Windows guests, however, if you do not perform a custom upgrade, new modules might not be added. If some features do not work correctly after an upgrade, you must change or repair modules. On operating systems other than Windows, 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 Right-click the virtual machine in the inventory and select **All vCenter Actions > Guest OS > Install/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
vSphere Web Client	Right-click the virtual machine and select <b>All vCenter Actions &gt; Guest OS &gt; Install/Upgrade VMware Tools</b> .
Fusion	Virtual Machine > Install (or Upgrade) VMware Tools
Workstation	VM > Install (or Upgrade) VMware Tools
Player	Player > Manage > Install (or Upgrade) VMware Tools

- 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

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

In a vSphere 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](#).

### 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	In the guest operating system, select <b>Programs &gt; Uninstall a program</b> .
Windows Vista and Windows Server 2008	In the guest operating system, select <b>Programs and Features &gt; Uninstall a program</b> .
Windows XP and earlier	In the guest operating system, select <b>Add/Remove Programs</b> .
Linux	On a Linux guest operating system that has VMware Tools installed by using an RPM installer, enter <b>rpm -e VMwareTools</b> in a terminal window.
Linux, Solaris, FreeBSD, NetWare	Log in as root and enter <b>vmware-uninstall-tools.pl</b> in a terminal window.
Mac OS X Server	Use the <b>Uninstall VMware Tools</b> application, found in <b>/Library/Application Support/VMware Tools</b> .

### 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
<b>Start the VMware User process when you start an X session.</b>	Add <code>vmware-user</code> to the appropriate X startup script, such as the <code>.xsession</code> or <code>.xinitrc</code> file.
<b>Start the process after a VMware Tools software upgrade, or if certain features are not working.</b>	Open a terminal window and type the <code>vmware-user</code> 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"
```

### Virtual Machine Communication Interface (VMCI) for ESXi 5.0 and Earlier

This setting applies to ESXi 5.0 and earlier virtual machines. It does not apply to ESXi 5.1 and later virtual machines.

If VMCI is not restricted, a virtual machine can detect and be detected by all others with the same option enabled within the same host. Custom-built software that uses this interface might have unexpected vulnerabilities that lead to an exploit. Also, a virtual machine could detect how many other virtual machines are within the same ESX/ESXi system by registering the virtual machine. This information could be used for a malicious objective. The virtual machine can be exposed to others within the system as long as at least one program is connected to the VMCI socket interface. Use the following `.vmx` setting to restrict VMCI:

```
vmci0.unrestricted = "FALSE"
```

## 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 `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 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 10-1. 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 [ <i>partition</i> ]	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 [ <i>device_name</i> ]	Disables the specified device or devices in the virtual machine. If no device is specified, all removable devices in the virtual machine are disabled.

Table 10-1. vmwtool Commands (continued)

vmwtool Command	Description
enabledevice [ <i>device_name</i> ]	Enables the specified device or devices in the virtual machine. If no device is specified, all removable devices in the virtual machine are enabled.
synctime [on off]	Lets you turn on or off synchronization of time in the guest operating system with time on the host operating system. By default, time synchronization is turned off.  Use this command without any options to view the current time synchronization status.
idle [on off]	Lets you turn the CPU idler on or off. By default, the idler is turned on. The CPU idler program is included in VMware Tools for NetWare 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 10-2. 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 <code>./</code> 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 vSphere 4.1 and later.

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.

---

**Note** Time synchronization with the host is disabled by default.

---

### 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](#).

**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.

## Results

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](#).

## 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
<b><i>device-name</i></b>	Use one of the names displayed when you used the <b>list</b> subcommand.
<b><i>subcommand</i></b>	Use <b>enable</b> or <b>disable</b> .

## Results

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](#).

### 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 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](#).
- If you plan to script commands and need to know what the exit codes are, see [Exit Codes for the VMware Tools Configuration Utility](#).

### 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
```

## Results

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 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](#).

## 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.

## Results

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 10-3. Default VMware Tools Scripts

Script Name	Description
poweroff-vm-default	<p>Runs when the virtual machine is being powered off or reset.</p> <p>Has no effect on networking for the virtual machine.</p>
poweron-vm-default	<p>Runs when the virtual machine is being powered on rather than resumed.</p> <p>Also runs after virtual machine restarts.</p> <p>Has no effect on networking for the virtual machine.</p>
resume-vm-default	<p>Runs when the virtual machine is resumed after it was suspended.</p> <p>On Windows guest operating systems, if the virtual machine is configured to use DHCP, this script renews the IP address of the virtual machine.</p> <p>On Linux, Mac OS X, Solaris, and FreeBSD guest operating systems, this script starts networking for the virtual machine.</p>
suspend-vm-default	<p>Runs when the virtual machine is being suspended.</p> <p>On Windows guest operating systems, if the virtual machine is configured to use DHCP, this script releases the IP address of the virtual machine.</p> <p>On Linux, Mac OS X, Solaris, and FreeBSD , this script stops networking for the virtual machine.</p>

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

Operating System	Default Path
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
<i>utility-name</i> (On Windows)	Use VMwareToolboxCmd.exe.
<i>utility-name</i> (On Linux, Solaris, and FreeBSD)	Use vmware-toolbox-cmd.
<i>script-name</i>	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](#).
- If you plan to script commands and need to know what the exit codes are, see [Exit Codes for the VMware Tools Configuration Utility](#).

### 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
<b><i>utility-name</i> (On Windows)</b>	Use VMwareToolboxCmd.exe.
<b><i>utility-name</i> (On Linux, Solaris, and FreeBSD)</b>	Use vmware-toolbox-cmd.
<b><i>utility-name</i> (On Mac OS X)</b>	Use vmware-tools-cli.
<b><i>subcommand</i></b>	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 stat command to display information such as host time and CPU speed. Additional subcommands are available for virtual machines in a vSphere environment.

Table 10-4. 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 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.

## 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 10-5. 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.

Table 10-5. Exit Codes (continued)

Code Number	Applicable Command	Description
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

# 11

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](#). For a list of hardware features available to virtual machines with each ESXi compatibility setting, see [Hardware Features Available with Virtual Machine Compatibility Settings](#).

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.

---

**Important** Upgrading virtual machine hardware is a heavyweight operation that might cause some applications or the operating system to stop working properly.

---

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](#)
- [Installing VMware Tools](#)

- [Planning Downtime for Virtual Machines](#)
- [Downtime for Upgrading Virtual Machines](#)
- [Manually Install or Upgrade VMware Tools in a Windows Virtual Machine](#)
- [Automate VMware Tools Installation for Multiple Windows Virtual Machines](#)
- [Manually Install or Upgrade VMware Tools in a Linux Virtual Machine](#)
- [Operating System Specific Packages for Linux Guest Operating Systems](#)
- [Manually Install or Upgrade VMware Tools in a Mac OS X Virtual Machine](#)
- [Manually Install or Upgrade VMware Tools in a Solaris Virtual Machine](#)
- [Manually Install or Upgrade VMware Tools in a NetWare Virtual Machine](#)
- [Manually Install or Upgrade VMware Tools in a FreeBSD Virtual Machine](#)
- [Upgrade VMware Tools by Using the vSphere Web Client](#)
- [Perform an Automatic Upgrade of VMware Tools](#)
- [Upgrade the Compatibility for Virtual Machines by Using the vSphere Web Client](#)
- [Schedule a Compatibility Upgrade for Virtual Machines](#)

## 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. The status bar of the virtual machine displays a message when a new version is available.

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** When 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. 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](#).

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 11-1. Virtual Machine Compatibility Options**

Compatibility	Description
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

VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine.

Although the guest operating system can run without VMware Tools, 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 use the shutdown or restart options from the toolbar. You can use only the power options.

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.

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, 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](#) and [Automate VMware Tools Installation for Multiple Windows Virtual Machines](#).
- For information about installing or upgrading VMware Tools in Linux virtual machines, see [Manually Install or Upgrade VMware Tools in a Linux Virtual Machine](#).

- 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](#).
- For information about installing or upgrading VMware Tools in Solaris virtual machines, see [Manually Install or Upgrade VMware Tools in a Solaris Virtual Machine](#).
- For information about installing or upgrading VMware Tools in NetWare virtual machines, see [Manually Install or Upgrade VMware Tools in a NetWare Virtual Machine](#).
- For information about installing or upgrading VMware Tools in FreeBSD virtual machines, see [Manually Install or Upgrade VMware Tools in a FreeBSD Virtual Machine](#).

## 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 also 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>.
- 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 11-2. 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 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	<b>Inventory &gt; Virtual Machine &gt; Guest &gt; Install/Upgrade VMware</b>
vSphere Web Client	Right-click the virtual machine and select <b>All vCenter Actions &gt; Guest OS &gt; Install/Upgrade VMware Tools</b> .
Fusion	<b>Virtual Machine &gt; Install (or Upgrade) VMware Tools</b>
Workstation	<b>VM &gt; Install (or Upgrade) VMware Tools</b>
Player	<b>Player &gt; Manage &gt; Install (or Upgrade) VMware Tools</b>

- 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 Right-click the virtual machine in the inventory and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**.

- 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.

- 7 Follow the on-screen instructions.

To install nondefault 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.

## Results

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](#).

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. 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 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](#) .
- 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](#) and [Add VMware as a Trusted Publisher to Suppress Driver Prompts](#) .

## 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.

- 4 To add MSI arguments or to exclude VMware Tools components during the installation process, add the arguments and options to the `setup.exe` command in the Advanced Options text box.
  - a Type the `setup.exe` command with any MSI arguments.

```
setup.exe /S /v "/qn msi_args"
```

To exclude some of the VMware Tools components, use the `ADDLOCAL` and `REMOVE` options.

```
setup.exe /S /v "/qn msi_args ADDLOCAL=ALL REMOVE=component"
```

For example, this command performs a silent installation and suppresses rebooting when installation is complete. This command also installs all components except the shared folders component.

```
setup.exe /S /v "/qn REBOOT=R ADDLOCAL=ALL REMOVE=Hgfs"
```

This example shows the same command, but with logging added.

```
setup.exe /S /v "/qn /l*v ""%TEMP%\vmmsi.log"" REBOOT=R ADDLOCAL=ALL REMOVE=Hgfs"
```

## 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.

### Results

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
```

## Results

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 11-3. VMware Tools Component Values

Valid Component Values	Description
Drivers	<p><b>Audio</b></p> <p>Audio driver for 64-bit operating systems and Windows Vista and later systems.</p> <p><b>BootCamp</b></p> <p>Driver for Mac BootCamp support.</p> <p><b>LSI</b></p> <p>PCI Fusion-MPT Miniport driver for Windows XP systems.</p> <p><b>MemCtl</b></p> <p>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.</p> <p><b>Mouse</b></p> <p>VMware mouse driver. Excluding this feature decreases mouse performance in your virtual machine.</p> <p><b>PVSCSI</b></p> <p>Driver for VMware Paravirtual SCSI adapters, which enhance the performance of some virtualized applications.</p> <p><b>SVGA</b></p> <p>VMware SVGA driver. Excluding this feature limits the display capabilities of your virtual machine.</p> <p><b>Sync</b></p> <p>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.</p> <p><b>VMCI</b></p> <p>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.</p> <p><b>Hgfs</b></p> <p>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.</p> <p><b>VMXNet</b></p> <p>VMware VMXnet networking driver.</p> <p><b>VMXNet3</b></p>

Table 11-3. VMware Tools Component Values (continued)

Valid Component Values	Description
	<p>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.</p> <p>Virtual hardware version 7 corresponds to ESX/ESXi 4.x compatibility.</p> <p><b>VShield</b></p> <p>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.</p> <p><b>VSS</b></p> <p>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.</p>
Toolbox	<p><b>Unity</b></p> <p>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.</p> <p><b>Perfmon</b></p> <p>Driver for WMI performance logging.</p>

**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.

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 in your environment.

**Note** 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) to install and upgrade VMware Tools. With OSPs 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](#).

### 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	<b>Inventory &gt; Virtual Machine &gt; Guest &gt; Install/Upgrade VMware</b>
vSphere Web Client	Right-click the virtual machine and select <b>All vCenter Actions &gt; Guest OS &gt; Install/Upgrade VMware Tools</b> .
Fusion	<b>Virtual Machine &gt; Install (or Upgrade) VMware Tools</b>
Workstation	<b>VM &gt; Install (or Upgrade) VMware Tools</b>
Player	<b>Player &gt; Manage &gt; Install (or Upgrade) VMware Tools</b>

- 2 Right-click the virtual machine in the inventory and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**.
- 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 xzpf /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.

## Results

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](#).

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`.

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 unmanaged on the virtual machine **Summary** tab. The status unmanaged means that you cannot use 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	<b>Inventory &gt; Virtual Machine &gt; Guest &gt; Install/Upgrade VMware Tools</b> and select <b>Interactive Tools Installation</b> or <b>Interactive Tools Upgrade</b>
vSphere Web Client	Right-click the virtual machine in the vCenter inventory and select <b>All vCenter Actions &gt; Guest OS &gt; Install/Upgrade VMware Tools</b>
Fusion	<b>Virtual Machine &gt; Install (or Upgrade) VMware Tools</b>

- 2 Right-click the virtual machine in the inventory and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**.
- 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**.

## Results

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 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	<b>Inventory &gt; Virtual Machine &gt; Guest &gt; Install/Upgrade VMware</b>
vSphere Web Client	Right-click the virtual machine and select <b>All vCenter Actions &gt; Guest OS &gt; Install/Upgrade VMware Tools</b> .
Fusion	<b>Virtual Machine &gt; Install (or Upgrade) VMware Tools</b>
Workstation	<b>VM &gt; Install (or Upgrade) VMware Tools</b>
Player	<b>Player &gt; Manage &gt; Install (or Upgrade) VMware Tools</b>

- 2 Right-click the virtual machine in the inventory and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**.

- 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.

**Results**

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](#).

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 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 <b>All vCenter Actions &gt; Guest OS &gt; Install/Upgrade VMware Tools</b> .
Fusion	Virtual Machine > Install (or Upgrade) VMware Tools
Workstation	VM > Install (or Upgrade) VMware Tools
Player	Player > Manage > Install (or Upgrade) VMware Tools

- 2 Right-click the virtual machine in the inventory and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**.

- 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](#).

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 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	<b>Inventory &gt; Virtual Machine &gt; Guest &gt; Install/Upgrade VMware</b>
vSphere Web Client	Right-click the virtual machine and select <b>All vCenter Actions &gt; Guest OS &gt; Install/Upgrade VMware Tools</b> .
Fusion	<b>Virtual Machine &gt; Install (or Upgrade) VMware Tools</b>

VMware Product	Action
Workstation	VM > Install (or Upgrade) VMware Tools
Player	Player > Manage > Install (or Upgrade) VMware Tools

- 2 Right-click the virtual machine in the inventory and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**.

- 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 xpf /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.

## Results

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](#).

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 by Using the vSphere Web Client

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.

### Results

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, and if necessary, restarts the virtual machine.

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 Right-click the virtual machine in the inventory and select **All vCenter Actions > Guest OS > Install/Upgrade VMware Tools**.
- 2 Select **Automatic Tools Upgrade**.
- 3 (Optional) In the **Advanced Options** text box, enter advanced options for the guest operating system.

Option	Action
Microsoft Windows Guest Operating Systems	Enter <code>/s /v "/qn" /l "Microsoft_Windows_location\filename.log"</code> 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	<ul style="list-style-type: none"> <li>■ Enter <code>—default</code> to perform the default behavior. Perform a silent upgrade of VMware Tools. Install tools bin, lib and doc files in the default /usr directory.</li> <li>■ Enter <code>—prefix=binary_location, lib_location, doc_location</code> to perform a silent upgrade of VMware Tools and install the binary, library, and document files in the specified locations.</li> </ul>

- 4 Click **OK**.

## Results

The **VMware Tools** label on the **Summary** tab changes to **OK**.

**Important** When 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 by Using the vSphere Web Client

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](#).

For information about virtual machine hardware versions and compatibility, see [Virtual Machine Compatibility](#).

---

**Important** Upgrading virtual machine hardware is a heavyweight operation that might cause some applications or the operating system to stop working properly. Perform a hardware version upgrade only if you need a feature that comes with the newer hardware version.

---

## Prerequisites

- Create a backup or snapshot of the virtual machines. See [Using Snapshots To Manage Virtual Machines](#).
- Upgrade VMware Tools. On Microsoft Windows virtual machines, 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](#).

## 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**.

### Results

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 by Using the vSphere Web Client](#).

For information about virtual machine hardware versions and compatibility, see [Virtual Machine Compatibility](#).

### Prerequisites

- Create a backup or snapshot of the virtual machines. See [Using Snapshots To Manage Virtual Machines](#).
- Upgrade VMware Tools. On Microsoft Windows virtual machines, 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](#).

#### 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.

#### Results

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

# 12

Many tasks require permissions on more than one object in the inventory. You can review the privileges required to perform the tasks and, where applicable, the appropriate sample roles.

The following table lists common tasks that require more than one privilege. You can use the Applicable Roles on the inventory objects to grant permission to perform these tasks, or you can create your own roles with the equivalent required privileges.

**Table 12-1. Required Privileges for Common Tasks**

Task	Required Privileges	Applicable Role
Create a virtual machine	On the destination folder or datacenter:	Administrator
	■ <b>Virtual machine.Inventory.Create new</b>	
	■ <b>Virtual machine.Configuration.Add new disk</b> (if creating a new virtual disk)	
	■ <b>Virtual machine.Configuration.Add existing disk</b> (if using an existing virtual disk)	
	■ <b>Virtual machine.Configuration.Raw device</b> (if using an RDM or SCSI pass-through device)	
	On the destination host, cluster, or resource pool:	Resource pool administrator or Administrator
	<b>Resource.Assign virtual machine to resource pool</b>	
	On the destination datastore or folder containing a datastore:	Datastore Consumer or Administrator
	<b>Datastore.Allocate space</b>	
	On the network that the virtual machine will be assigned to:	Network Consumer or Administrator
	<b>Network.Assign network</b>	
Power on a virtual machine	On the data center in which the virtual machine is deployed:	Virtual Machine Power User or Administrator
	<b>Virtual machine.Interaction.Power On</b>	
	On the virtual machine or folder of virtual machines:	
	<b>Virtual machine.Interaction.Power On</b>	
Deploy a virtual machine from a template	On the destination folder or datacenter:	Administrator
	■ <b>Virtual machine.Inventory.Create from existing</b>	
	■ <b>Virtual machine.Configuration.Add new disk</b>	

Table 12-1. Required Privileges for Common Tasks (continued)

Task	Required Privileges	Applicable Role
	On a template or folder of templates: <b>Virtual machine.Provisioning.Deploy template</b>	Administrator
	On the destination host, cluster or resource pool: <b>Resource.Assign virtual machine to resource pool</b>	Administrator
	On the destination datastore or folder of datastores: <b>Datastore.Allocate space</b>	Datastore Consumer or Administrator
	On the network that the virtual machine will be assigned to: <b>Network.Assign network</b>	Network Consumer or Administrator
Take a virtual machine snapshot	On the virtual machine or a folder of virtual machines: <b>Virtual machine.Snapshot management. Create snapshot</b>	Virtual Machine Power User or Administrator
Move a virtual machine into a resource pool	On the virtual machine or folder of virtual machines: <ul style="list-style-type: none"> <li>■ <b>Resource.Assign virtual machine to resource pool</b></li> <li>■ <b>Virtual machine.Inventory.Move</b></li> </ul>	Administrator
	On the destination resource pool: <b>Resource.Assign virtual machine to resource pool</b>	Administrator
Install a guest operating system on a virtual machine	On the virtual machine or folder of virtual machines: <ul style="list-style-type: none"> <li>■ <b>Virtual machine.Interaction.Answer question</b></li> <li>■ <b>Virtual machine.Interaction.Console interaction</b></li> <li>■ <b>Virtual machine.Interaction.Device connection</b></li> <li>■ <b>Virtual machine.Interaction.Power Off</b></li> <li>■ <b>Virtual machine.Interaction.Power On</b></li> <li>■ <b>Virtual machine.Interaction.Reset</b></li> <li>■ <b>Virtual machine.Interaction.Configure CD media</b> (if installing from a CD)</li> <li>■ <b>Virtual machine.Interaction.Configure floppy media</b> (if installing from a floppy disk)</li> <li>■ <b>Virtual machine.Interaction.VMware Tools install</b></li> </ul>	Virtual Machine Power User or Administrator
	On a datastore containing the installation media ISO image: <b>Datastore.Browse datastore</b> (if installing from an ISO image on a datastore)	Virtual Machine Power User or Administrator
	On the datastore to which you upload the installation media ISO image: <ul style="list-style-type: none"> <li>■ <b>Datastore.Browse datastore</b></li> <li>■ <b>Datastore.Low level file operations</b></li> </ul>	
Migrate a virtual machine with vMotion	On the virtual machine or folder of virtual machines: <ul style="list-style-type: none"> <li>■ <b>Resource.Migrate powered on virtual machine</b></li> <li>■ <b>Resource.Assign Virtual Machine to Resource Pool</b> (if destination is a different resource pool from the source)</li> </ul>	Resource Pool Administrator or Administrator

Table 12-1. Required Privileges for Common Tasks (continued)

Task	Required Privileges	Applicable Role
	On the destination host, cluster, or resource pool (if different from the source): <b>Resource.Assign virtual machine to resource pool</b>	Resource Pool Administrator or Administrator
Cold migrate (relocate) a virtual machine	On the virtual machine or folder of virtual machines: <ul style="list-style-type: none"> <li>■ <b>Resource.Migrate powered off virtual machine</b></li> <li>■ <b>Resource.Assign virtual machine to resource pool</b> (if destination is a different resource pool from the source)</li> </ul>	Resource Pool Administrator or Administrator
	On the destination host, cluster, or resource pool (if different from the source): <b>Resource.Assign virtual machine to resource pool</b>	Resource Pool Administrator or Administrator
	On the destination datastore (if different from the source): <b>Datastore.Allocate space</b>	Datastore Consumer or Administrator
Migrate a virtual machine with Storage vMotion	On the virtual machine or folder of virtual machines: <b>Resource.Migrate powered on virtual machine</b>	Resource Pool Administrator or Administrator
	On the destination datastore: <b>Datastore.Allocate space</b>	Datastore Consumer or Administrator
Move a host into a cluster	On the host: <b>Host.Inventory.Add host to cluster</b>	Administrator
	On the destination cluster: <b>Host.Inventory.Add host to cluster</b>	Administrator