

vSphere Virtual Machine Administration

17 APR 2018

VMware vSphere 6.7

VMware ESXi 6.7

vCenter Server 6.7



vmware®

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

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

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

docfeedback@vmware.com

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

Copyright © 2009–2018 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

About vSphere Virtual Machine Administration 6

1 Introduction to VMware vSphere Virtual Machines 7

- [Virtual Machine Files 7](#)
- [Virtual Machines and the Virtual Infrastructure 8](#)
- [Virtual Machine Lifecycle 9](#)
- [Virtual Machine Components 9](#)
- [Virtual Machine Hardware Available to vSphere Virtual Machines 11](#)
- [Virtual Machine Options 13](#)
- [vSphere Web Client 14](#)
- [Where to Go From Here 14](#)

2 Deploying Virtual Machines 16

- [Create a Virtual Machine with the New Virtual Machine Wizard 17](#)
- [Clone a Virtual Machine to a Template 20](#)
- [Clone a Virtual Machine to a Template in the vSphere Web Client 23](#)
- [Deploy a Virtual Machine from a Template 26](#)
- [Deploy a Virtual Machine from a Template in the vSphere Web Client 30](#)
- [Clone an Existing Virtual Machine 33](#)
- [Clone an Existing Virtual Machine in the vSphere Web Client 38](#)
- [Cloning a Virtual Machine with Instant Clone 42](#)
- [Clone a Template to a Template 43](#)
- [Clone a Template to a Template in the vSphere Web Client 46](#)
- [Convert a Template to a Virtual Machine 49](#)

3 Deploying OVF and OVA Templates 51

- [OVF and OVA File Formats and Templates 51](#)
- [Deploy an OVF or OVA Template 52](#)
- [Export an OVF Template 53](#)
- [Browse VMware Virtual Appliance Marketplace 54](#)

4 Using Content Libraries 55

- [Create a Library 57](#)
- [Synchronize a Subscribed Content Library 58](#)
- [Edit a Content Library 59](#)
- [Hierarchical Inheritance of Permissions for Content Libraries 61](#)
- [Content Library Administrator Role 63](#)
- [Populating Libraries with Content 63](#)

Creating Virtual Machines and vApps from Templates in a Content Library	67
Working with Items in a Library	74

5 Configuring Virtual Machine Hardware 79

Virtual Machine Compatibility	79
Virtual CPU Configuration	87
Virtual Memory Configuration	95
Virtual Disk Configuration	100
SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility	112
Virtual Machine Network Configuration	119
Other Virtual Machine Device Configuration	134
USB Configuration from an ESXi Host to a Virtual Machine	147
USB Configuration from a Client Computer to a Virtual Machine	156
Add a Shared Smart Card Reader to Virtual Machines	163
Securing Virtual Machines with Virtual Trusted Platform Module	164

6 Configuring Virtual Machine Options 167

Virtual Machine Options Overview	167
General Virtual Machine Options	168
Configuring User Mappings on Guest Operating Systems	170
VMware Remote Console Options	171
Virtual Machine Encryption	172
Virtual Machine Power Management Options	174
Configuring VMware Tools Options	176
Virtualization Based Security	178
Configuring Virtual Machine Boot Options	180
Configuring Virtual Machine Advanced Options	182
Configure Fibre Channel NPIV Settings	185

7 Managing Multi-Tiered Applications with vSphere vApp 187

Create a vApp	188
Create or Add an Object to a vApp	189
Edit vApp Settings	190
Clone a vApp	196
Perform vApp Power Operations	197
Edit vApp Notes	198
Add a Network Protocol Profile in the vSphere Web Client	198
Virtual Machine vApp Options	202

8 Monitoring Solutions with the vCenter Solutions Manager 208

View Solutions in the vSphere Web Client	208
Monitoring Agents	209

9	Managing Virtual Machines	211
	Installing a Guest Operating System	212
	Customizing Guest Operating Systems	214
	Edit Virtual Machine Startup and Shutdown Settings in the vSphere Web Client	232
	Edit Virtual Machine Startup and Shutdown Settings	234
	Install the VMware Enhanced Authentication Plug-in	236
	Using a Virtual Machine Console	237
	Answer Virtual Machine Questions	238
	Removing and Reregistering VMs and VM Templates	239
	Managing Virtual Machine Templates	240
	Using Snapshots To Manage Virtual Machines	242
	Enhanced vMotion Compatibility as a Virtual Machine Attribute	254
	Migrating Virtual Machines	257
10	Upgrading Virtual Machines	277
	Downtime for Upgrading Virtual Machines	278
	Upgrade the Compatibility of a Virtual Machine Manually	279
	Schedule a Compatibility Upgrade for Virtual Machines	280
11	Required Privileges for Common Tasks	282
12	Troubleshooting Overview	285
	Guidelines for Troubleshooting	285
	Troubleshooting with Logs	287
13	Troubleshooting Virtual Machines	289
	Troubleshooting USB Passthrough Devices	289
	Recover Orphaned Virtual Machines	290
	Virtual Machine Does Not Power On After Cloning or Deploying from Template	291

About vSphere Virtual Machine Administration

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

This guide provides introductions to the tasks that you can perform within the system and also cross-references to the documentation that describes the tasks in detail.

This information focuses on managing virtual machines 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
- 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.

vSphere Web Client and vSphere Client

Instructions in this guide reflect the vSphere Client (an HTML5-based GUI). You can also use the instructions to perform most of the tasks by using the vSphere Web Client (a Flex-based GUI).

Tasks for which the workflow differs significantly between the vSphere Client and the vSphere Web Client have duplicate procedures that provide steps according to the respective client interface. The procedures that relate to the vSphere Web Client, contain vSphere Web Client in the title.

Note In vSphere 6.7, most of the vSphere Web Client functionality is implemented in the vSphere Client. For an up-to-date list of the unsupported functionality, see [Functionality Updates for the vSphere Client](#).

Introduction to VMware vSphere Virtual Machines

1

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 but are more portable, more secure, and easier to manage.

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](#)
- [vSphere Web Client](#)
- [Where to Go From Here](#)

Virtual Machine Files

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 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.f</i>	Additional virtual machine configuration files

Table 1-1. Virtual Machine Files (Continued)

File	Usage	Description
.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 snapshots
.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 run on ESXi hosts that vCenter Server manages.

vCenter Server can pool the resources of multiple hosts and lets you effectively monitor and manage your data center 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 vSphere Client is the primary interface for managing vCenter Server, ESXi hosts, and virtual machines. The vSphere Client 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 Client presents the organizational hierarchy of managed objects in inventory views. Inventories are the hierarchal structure used by vCenter Server or the host to organize managed objects. This hierarchy includes the monitored objects in vCenter Server.

In the vCenter Server hierarchy that you see in the vSphere Client, a data center is the top-level container of ESXi hosts, folders, clusters, resource pools, vSphere vApps, virtual machines, and so on.

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

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 have many choices for creating and deploying virtual machines. 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 or OVA templates.

The vSphere Client **New Virtual Machine** wizard and the **Edit Settings** dialog 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 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. You manage these components just like the components of a physical computer.

Operating System

You install a guest operating system on a virtual machine just 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.

After installation, you are responsible for securing and patching the operating system.

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. It includes device drivers and other software that is essential for your VM. With VMware Tools, you have more control over the virtual machine interface.

Compatibility Setting

In the vSphere 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.

Hardware Devices

Each virtual hardware device performs the same function for the virtual machine as hardware on a physical computer does. 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 access the hardware devices in the **Edit Settings** dialog box. Not all devices are configurable. Some hardware devices are part of the virtual motherboard and appear in the expanded device list of the **Edit Settings** dialog box, 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](#).

In the **Edit Settings** dialog box you can also add virtual hardware devices to the virtual machine. You can use the memory or CPU hotplug options to 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>

A vSphere administrator or other privileged user can determine who can access or modify a virtual machine by setting permissions on the virtual machine. See the *vSphere Security* documentation.

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.

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"> ■ Intel 440BX AGPset 82443BX Host Bridge/Controller ■ Intel 82371AB (PIIX4) PCI ISA IDE Xcelerator ■ National Semiconductor PC87338 ACPI 1.0 and PC98/99 Compliant SuperI/O ■ Intel 82093AA I/O Advanced Programmable Interrupt Controller
DVD/CD-ROM Drive	Installed by default when you create a new vSphere virtual machine. You can configure DVD/CD-ROM devices to connect to client devices, host devices, or datastore ISO files. You can add, remove, or configure DVD/CD-ROM devices.
Floppy Drive	Installed by default when you create a new vSphere virtual machine. You can connect to a floppy drive located on the ESXi host, a floppy (.flp) image, or the floppy drive on your local system. You can add, remove, or configure floppy devices.
Hard Disk	Stores the virtual machine's operating system, program files, and other data associated with its activities. A virtual disk is a large physical file, or a set of files, that can be copied, moved, archived, and backed up as easily as any other file.
IDE 0, IDE 1	By default, two Integrated Drive Electronics (IDE) interfaces are presented to the virtual machine. The IDE interface (controller) is a standard way for storage devices (Floppy drives, hard drives and CD-ROM drives) to connect to the virtual machine.

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

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

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

Hardware Device	Description
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.
NVMe controller	NVM Express controller. NVMe is a logical device interface specification for accessing nonvolatile storage media attached through a PCI Express (PCIe) bus in real and virtual hardware.
NVDIMM controller	Provides access to the non-volatile memory resources of the host.
NVDIMM device	Non-Volatile Dual In-Line Memory Module. NVDIMM modules are memory devices that sit on an ordinary memory channel, but contain non-volatile memory. You can add up to 64 virtual NVDIMM devices to a virtual machine.
TPM device	Trusted Platform Module. When you add a virtual TPM 2.0 device to a virtual machine, the guest OS uses the device to store sensitive information, perform cryptographic tasks, or attest the integrity of the guest platform.

Virtual Machine Options

Use the available virtual machine options to fine-tune the settings and behaviour of your virtual machine and to ensure maximum performance.

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.

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.
Encryption Options	<p>Enable or disable encryption for the virtual machine if the vCenter Server instance is in a trusted relationship with a KMS server. For more information, see the <i>vSphere Security</i> documentation.</p> <p>You can also enable or disable encrypted vMotion for virtual machines that are not encrypted. You can set encrypted vMotion to the disabled, opportunistic, or required state. You can enable encrypted vMotion during virtual machine creation. Alternatively, you can change the encrypted vMotion state at a later time. For more information, see the <i>vCenter Server and Host Management</i> documentation.</p>
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.

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.
Virtualization Based Security (VBS)	Enable VBS to provide an additional level of protection to the virtual machine. VBS is available on the latest Windows OS versions. For more information, see the <i>vSphere Security</i> documentation.
Boot Options	Set the boot delay when powering on virtual machines or to force BIOS setup and configure failed boot recovery.
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.
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	Use the vSphere Web Client to 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.

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

VMware supports several methods to provision vSphere virtual machines. What works best in 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. 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 with the New Virtual Machine Wizard](#).

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 and from shared network drives. See [Chapter 3 Deploying OVF and OVA Templates](#).

Create a template and deploy multiple virtual machines from it. A template is a master copy of a virtual machine that you can use to create and provision virtual machines. Use templates to save time. If you have a virtual machine that you will clone frequently, make that virtual machine a template. See [Deploy a Virtual Machine from a Template 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 an Existing Virtual Machine in the vSphere Web Client](#).

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

This chapter includes the following topics:

- [Create a Virtual Machine with the New Virtual Machine Wizard](#)
- [Clone a Virtual Machine to a Template](#)
- [Clone a Virtual Machine to a Template in the vSphere Web Client](#)
- [Deploy a Virtual Machine from a Template](#)

- [Deploy a Virtual Machine from a Template in the vSphere Web Client](#)
- [Clone an Existing Virtual Machine](#)
- [Clone an Existing Virtual Machine in the vSphere Web Client](#)
- [Cloning a Virtual Machine with Instant Clone](#)
- [Clone a Template to a Template](#)
- [Clone a Template to a Template in the vSphere Web Client](#)
- [Convert a Template to a Virtual Machine](#)

Create a Virtual Machine with the New Virtual Machine Wizard

You can create a single virtual machine if no virtual machines in your environment meet your needs, for example of 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. You open the New Virtual Machine wizard from any object in the inventory that is a valid parent object of a virtual machine.

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 Virtual Hardware page of the wizard.

Prerequisites

Verify that you have the following privileges:

- **Virtual machine.Inventory.Create new** on the destination folder or data center.
- **Virtual machine.Configuration.Add new disk** on the destination folder or data center, if you are adding a new disk.
- **Virtual machine.Configuration.Add existing disk** on the destination folder or data center, if you are adding an existing disk.
- **Virtual machine.Configuration.Raw device** on the destination folder or data center, if you are using an RDM or SCSI pass-through device.
- **Virtual machine.Configuration.Host USB device** on the destination folder or data center, if you are attaching a virtual USB device backed by a host USB device.
- **Virtual machine.Configuration.Advanced** on the destination folder or data center, if you are configuring advanced virtual machine settings.
- **Virtual machine.Configuration.Swapfile placement** on the destination folder or data center, if you are configuring swap file placement.
- **Virtual machine.Configuration.Disk change tracking** on the destination folder or data center, if you are enabling change tracking on the virtual machine's disks.

- **Resource.Assign virtual machine to resource pool** on the destination host, cluster, or resource pool.
- **Datastore.Allocate space** on the destination datastore or datastore folder.
- **Network.Assign network** on the network that the virtual machine will be assigned to.

To verify the privileges assigned to your role, click **Menu > Administration > Roles** and select the role.

Procedure

- 1 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 **New Virtual Machine**.
- 2 On the Select a creation type page, select **Create a new virtual machine** and click **Next**.
- 3 On the Select a name and folder page, enter a unique name for the virtual machine and select a deployment location.
- 4 On the Select a compute resource page, select the host, cluster, resource pool, or vApp where the virtual machine will run and click **Next**.

If creating the virtual machine at the selected location causes compatibility problems, an alarm appears in the **Compatibility** pane.

Note If you want to create a virtual machine that uses persistent memory, choose a host or a cluster with available PMem resource.

- 5 On the Select storage page, choose the storage type, the storage policy, and a datastore or datastore cluster where to store the virtual machine files.

Option	Description
Create a virtual machine on a host that has PMem resource	a Choose the type of storage by selecting the Standard or the PMem radio button. With the PMem storage option, every virtual machine disk file is stored on the host-local PMem datastore by default. You can change the datastore at a later time. The virtual machine home location must be on a non-PMem datastore. For more information about persistent memory and PMem storage, see the <i>vSphere Resource Management</i> guide.
	b (Optional) From the VM Storage Policy drop-down menu, select a virtual machine storage policy or leave the default one.
	c (Optional) Select the Encrypt this virtual machine check box to encrypt the virtual machine.
	d Select a datastore or a datastore cluster.
	e Select the Disable Storage DRS for this virtual machine check box if you do not want to use storage DRS with the virtual machine.
Create a virtual machine on a host that does not have PMem resource	a Select a VM storage policy or leave the default one.
	b (Optional) Select the Encrypt this virtual machine check box to encrypt the virtual machine.
	c Select a datastore or a datastore cluster.

Important For information about creating an encrypted virtual machine, see *vSphere Security*.

- 6 On the Select compatibility page, select the virtual machine compatibility with ESXi host versions and click **Next**.

Note Select the latest compatibility if you want to have access to the latest hardware features.

- 7 On the Select a guest OS page, select the guest OS family and version and click **Next**.

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 **VM Options** tab of the **Edit Settings** dialog 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.

8 (Optional) Enable **Windows Virtualization Based Security**.

The **Enable Windows Virtualization Based Security** option is available for the latest Windows OS versions, for example Windows 10 and Windows Server 2016. For more information about VBS, see the *vSphere Security* documentation.

9 On the Customize hardware page, configure the virtual machine hardware and options and click **Next**.

You can leave the defaults and configure the virtual machine hardware and options later. For more information, see [Chapter 5 Configuring Virtual Machine Hardware](#) and [Chapter 6 Configuring Virtual Machine Options](#).

Important If you chose to use PMem storage for the virtual machine, its default hard disk, the new hard disks that you configure, and the NVDIMM devices that you add to the virtual machine all share the same PMem resources. So, you must adjust the size of the newly added devices in accordance with the amount of the PMem available to the host. If any part of the configuration requires attention, the wizard alerts you.

10 On the Ready to complete page, review the details and click **Finish**.

The virtual machine appears in the vSphere Client inventory.

Clone a Virtual Machine to a Template

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

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

Prerequisites

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

Verify that you have the following privileges:

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

Procedure

1 Start the **Clone Virtual Machine To Template** wizard.

Option	Description
Open the Clone Virtual Machine To Template wizard from any object in the inventory	<ul style="list-style-type: none"> a Right-click any inventory object that is a valid parent object of a virtual machine, such as a datacenter, folder, cluster, resource pool, or host, and select New Virtual Machine. b On the Select a creation type page, select Clone virtual machine to template and click Next. c On the Select a virtual machine page, select the virtual machine that you want to clone.
Open the Clone Virtual Machine To Template wizard from a template	Right-click the virtual machine and select Clone > Clone to Template .

2 On the Select a name and folder page, enter a name for the template and select a data center or a folder in which to deploy it.

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.

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.

3 On the Select a compute resource, select a host or a cluster resource for the template.

The **Compatibility** pane shows the result from the compatibility checks.

Important If the virtual machine that you clone has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, you cannot proceed with the task.

If the virtual machine that you clone does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, all the hard disks of the template will use the storage policy and datastore selected for the configuration files of the source virtual machine.

- 4 On the Select storage page, select the datastore or datastore cluster in which to store the template configuration files and all of the virtual disks. Click **Next**.

Option	Description
Clone a virtual machine that has vPMem hard disks	<p>a Choose the type of storage for the template by selecting the Standard, the PMem, or the Hybrid radio button.</p> <p>If you select the Standard mode, all virtual disks are stored on a standard datastore.</p> <p>If you select the PMem mode, all virtual disks are stored on the host-local PMem datastore. Configuration files cannot be stored on a PMem datastore and you must additionally select a regular datastore for the configuration files of the virtual machine.</p> <p>If you select the Hybrid mode, all PMem virtual disks remain stored on a PMem datastore. Non-PMem disks are affected by your choice of a VM storage policy and datastore or datastore cluster.</p> <p>For more information about persistent memory and PMem storage, see the <i>vSphere Resource Management</i> guide.</p> <p>b From the Select virtual disk format drop-down menu, select a new virtual disk format for the template or keep the same format as the source virtual machine.</p> <p>c (Optional) From the VM Storage Policy drop-down menu, select a virtual machine storage policy or leave the default one.</p> <p>d Select a datastore or a datastore cluster.</p> <p>e Select the Disable Storage DRS for this virtual machine check box if you do not want to use storage DRS with the virtual machine.</p> <p>f (Optional) Turn on the Configure per disk option to select a separate datastore or a datastor cluster for the template configuration file and for each virtual disk.</p> <p>Note You can use the Configure per disk option to convert a PMem hard disk to a regular one, but that change might cause performance problems. You can also convert a standard hard disk to a PMem hard disk.</p>
Clone a virtual machine that does not have vPMem hard disks	<p>a Select the disk format for the virtual machine virtual disks.</p> <p>Same format as source uses the same disk format as the source virtual machine.</p> <p>The Thick Provision Lazy Zeroed format 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 later, on demand, on first write from the virtual machine.</p> <p>Thick Provision Eager Zeroed is a type of thick virtual disk that supports clustering features such as Fault tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types o disks.</p>

Option	Description
	The Thin Provision format saves storage space. 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.
b	(Optional) Select a VM storage policy or leave the default one.
c	Select a datastore or a datastore cluster.
d	(Optional) Turn on the Configure per disk option to select a separate datastore or a datastore cluster for the template configuration file and for each virtual disk.
	Note You can use the Configure per disk option to convert a PMem hard disk to a regular one, but that change might cause performance problems. You can also convert a standard hard disk to a PMem hard disk.

Important You cannot change the storage policy if you clone an encrypted virtual machine. For information about cloning an encrypted virtual machine, see *vSphere Security*.

- 5 On the Ready to complete page, review the template settings and click **Finish**.

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

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

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

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

Prerequisites

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

Verify that you have the following privileges:

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

Procedure

1 Start the **Clone Virtual Machine To Template** wizard.

Option	Description
Start the Clone Virtual Machine To Template wizard from any object in the inventory	<ul style="list-style-type: none"> a Right-click any inventory object that is a valid parent object of a virtual machine, such as a datacenter, folder, cluster, resource pool, or host, and select New Virtual Machine > New Virtual Machine. b On the Select a creation type page, select Clone virtual machine to template and click Next. c On the Select a virtual machine page, select the virtual machine that you want to clone and click Next.
Start the Clone Virtual Machine To Template wizard from a template	Right-click the virtual machine and select Clone > Clone to Template .

2 On the Select a name and folder page, enter a name for the template and select a data center or a folder in which to deploy it.

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.

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.

3 On the Select a compute resource, select a host or a cluster resource for the template.

The **Compatibility** pane shows the result from the compatibility checks.

Important If the virtual machine that you clone has an NVDIMM device and uses Pmem storage, the destination host or cluster must have available PMem resource.

If the virtual machine that you clone does not have an NVDIMM device but it uses Pmem storage, the destination host or cluster must have available PMem resource. Otherwise, all the hard disk of the template will use the storage policy and datastore selected for the configuration files of the source virtual machine.

- 4 On the Select storage page, select the datastore or datastore cluster in which to store the virtual machine configuration files and all of the virtual disks. Click **Next**.

- a Select the format for the virtual machine's disks.

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

- b (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.

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

Your selection affects the storage creation process.

Option	Action
Store all virtual machine files in the same location on a datastore.	<ol style="list-style-type: none"> (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the VM storage policy drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy. Select a datastore and click Next.
Store all virtual machine files in the same datastore cluster.	<ol style="list-style-type: none"> (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the VM storage policy drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage profile. Select a datastore cluster. (Optional) If you do not want to use Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the datastore cluster. Click Next.
Store virtual machine configuration files and disks in separate locations.	<ol style="list-style-type: none"> Click Advanced. For the virtual machine configuration file and for each virtual disk, click Browse and select a datastore or datastore cluster.

Option	Action
	<p>3 Apply a virtual machine storage policy from the VM storage profile drop-down menu.</p> <p>The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy.</p> <p>4 (Optional) If you selected a datastore cluster and do not want to use Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the datastore cluster.</p> <p>5 Click Next.</p>
Store all virtual machine files in the same non-volatile memory disk	<p>1 (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the VM storage policy drop-down menu.</p> <p>2 Select a non-volatile memory disk and click Next.</p>

Important You cannot change the storage policy if you clone an encrypted virtual machine. For information about cloning an encrypted virtual machine, see *vSphere Security*.

- 5 On the Ready to complete page, review the template settings and click **Finish**.

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

Deploy a Virtual Machine from a Template

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

Prerequisites

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

- **Virtual machine .Inventory.Create from existing** on the data center or virtual machine folder.
- **Virtual machine.Configuration.Add new disk** on the data center 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 is 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 From Template** wizard.

Option	Description
Open the Deploy From Template wizard from any object in the inventory	<ol style="list-style-type: none"> 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 New Virtual Machine. b On the Select a creation type page, select Deploy from template and click Next. c On the Select a template page, select the template that you want to use.
Open the Deploy From Template wizard from a template	Right-click a template and select New VM from This Template .

- 2 On the Select a name and folder page, enter a unique name for the virtual machine and select a deployment location.
- 3 On the Select a compute resource page, select the host, cluster, resource pool, or vApp where the virtual machine will run and click **Next**.

The virtual machine will have access to the resources of the selected object.

Important If the template that you deploy has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, you cannot proceed with the task.

If the template that you deploy does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, all the hard disks of the virtual machine will use the storage policy and datastore selected for the configuration files of the source template.

If creating the virtual machine at the selected location causes compatibility problems, an alarm appears in the **Compatibility** pane.

- 4 On the Select storage page, select the datastore or datastore cluster in which to store the virtual machine configuration files and all of the virtual disks. Click **Next**.

Option	Description
Deploy a virtual machine from a template that has vPMem hard disks	<p>a Choose the type of storage for the template by selecting the Standard, the PMem, or the Hybrid radio button.</p> <p>If you select the Standard mode, all virtual disks will be stored on a standard datastore.</p> <p>If you select the PMem mode, all virtual disks will be stored on the host-local PMem datastore. Configuration files cannot be stored on a PMem datastore and you must additionally select a regular datastore for the configuration files of the virtual machine.</p> <p>If you select the Hybrid mode, all PMem virtual disks will remain stored on a PMem datastore. Non-PMem disks are affected by your choice of a VM storage policy and datastore or datastore cluster.</p> <p>For more information about persistent memory and PMem storage, see the <i>vSphere Resource Management</i> guide.</p> <p>b (Optional) From the Select virtual disk format drop-down menu, select a new virtual disk format for the template or keep the same format as the source virtual machine.</p> <p>c (Optional) From the VM Storage Policy drop-down menu, select a virtual machine storage policy or leave the default one.</p> <p>d Select a datastore or a datastore cluster.</p> <p>e Select the Disable Storage DRS for this virtual machine check box if you do not want to use storage DRS with the virtual machine.</p> <p>f (Optional) Turn on the Configure per disk option to select a separate datastore or a datastore cluster for the template configuration file and for each virtual disk.</p> <p>Note You can use the Configure per disk option to convert a PMem hard disk to a regular one, but that change might cause performance problems. You can also convert a standard hard disk to a PMem hard disk.</p>
Deploy a virtual machine from a template that does not have vPMem hard disks	<p>a Select the disk format for the virtual machine virtual disks.</p> <p>Same format as source uses the same disk format as the source virtual machine.</p> <p>The Thick Provision Lazy Zeroed format 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 later, on demand, on first write from the virtual machine.</p> <p>Thick Provision Eager Zeroed is 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.</p>

Option	Description
	<p>The Thin Provision format saves storage space. 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.</p> <p>b (Optional) Select a VM storage policy or leave the default one.</p> <p>c Select a datastore or a datastore cluster.</p> <p>d (Optional) Turn on the Configure per disk option to select a separate datastore or a datastor cluster for the template configuration file and for each virtual disk.</p> <p>Note You can use the Configure per disk option to convert a PMem hard disk to a regular one, but that change might cause performance problems. You can also convert a standard hard disk to a PMem hard disk.</p>

- 5 On the Select clone options, select additional customization options for the new virtual machine.

You can choose to customize the guest operating system or the virtual machine hardware. You can also choose to power on the virtual machine after its creation.

- 6 (Optional) On the Customize guest OS page, apply a customization specification to the virtual machine.

Customizing the guest OS prevents from conflicts that might occur if you deploy virtual machines with identical settings, such as duplicate computer names.

Note 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](#).

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

- 7 (Optional) On the Customize hardware page, configure the virtual machine hardware and options and click **Next**.

You can leave the defaults and configure the virtual machine hardware and options later. For more information, see [Chapter 5 Configuring Virtual Machine Hardware](#) and [Chapter 6 Configuring Virtual Machine Options](#)

Important If you chose to use PMem storage for the virtual machine, its default hard disk, the new hard disks that you configure, and the NVDIMM devices that you add to the virtual machine all share the same PMem resources. So, you must adjust the size of the newly added devices in accordance with the amount of the PMem available to the host. If any part of the configuration requires attention, the wizard alerts you.

- 8 On the Ready to complete page, review the information and click **Finish**.

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 data center or virtual machine folder.
- **Virtual machine.Configuration.Add new disk** on the data center 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 is 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 From Template** wizard.

Option	Description
Open the Deploy From Template wizard from any object in the inventory	<ol style="list-style-type: none"> 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 New Virtual Machine > New Virtual Machine. b On the Select a creation type page, select Deploy from template and click Next. c On the Select a template page, select the template that you want to use. d (Optional) Select the Customize the operating system check box to customize the guest operating system of the virtual machine. e (Optional) Select the Customize this virtual machine's hardware check box to customize the virtual hardware of the virtual machine. f (Optional) Select the Power On Virtual Machine after creation check box to power on the virtual machine after creation.
Open the Deploy From Template wizard from a template	Right-click a template and select New VM from This Template .

- 2 On the Select a name and folder page, enter a unique name for the virtual machine and select a deployment location.
- 3 On the Select a compute resource page, select the host, cluster, resource pool, or vApp where the virtual machine will run and click **Next**.

The virtual machine will have access to the resources of the selected object.

Important If the template that you deploy has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, you cannot proceed with the task.

If the template that you deploy does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, all the hard disks of the virtual machine will use the storage policy and datastore selected for the configuration files of the source template.

If creating the virtual machine at the selected location causes compatibility problems, an alarm appears in the **Compatibility** pane.

4 On the Select storage page, configure the datastore.

- a Select the format for the virtual machine's disks.

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

- b (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.

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

Your selection affects the storage creation process.

Option	Action
Store all virtual machine files in the same location on a datastore.	<ol style="list-style-type: none"> (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the VM storage policy drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy. Select a datastore and click Next.
Store all virtual machine files in the same datastore cluster.	<ol style="list-style-type: none"> (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the VM storage policy drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage profile. Select a datastore cluster. (Optional) If you do not want to use Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the datastore cluster. Click Next.
Store virtual machine configuration files and disks in separate locations.	<ol style="list-style-type: none"> Click Advanced. For the virtual machine configuration file and for each virtual disk, click Browse and select a datastore or datastore cluster.

Option	Action
	<ol style="list-style-type: none"> 3 Apply a virtual machine storage policy from the VM storage profile drop-down menu. <p>The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy.</p> <ol style="list-style-type: none"> 4 (Optional) If you selected a datastore cluster and do not want to use Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the datastore cluster. 5 Click Next.
Store all virtual machine files in the same non-volatile memory disk	<ol style="list-style-type: none"> 1 (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the VM storage policy drop-down menu. 2 Select a non-volatile memory disk and click Next.

- 5 (Optional) On the Customize hardware page, configure the virtual machine hardware, virtual machine options, and Storage DRS rules, and click **Next**.

Customizing the guest OS prevents from conflicts that might occur if you deploy virtual machines with identical settings, such as duplicate computer names.

Note 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](#).

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

- 6 On the Ready to complete page, review the information and click **Finish**.

Clone an Existing Virtual Machine

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

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

Prerequisites

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

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

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

Procedure

- 1 Start the **Clone Existing Virtual Machine** wizard.

Option	Description
Open the Clone Existing Virtual Machine wizard from any object in the inventory	<ol style="list-style-type: none"> 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 New Virtual Machine. b On the Select a creation type page, select Clone an existing virtual machine and click Next. c On the Select a virtual machine page, select the virtual machine that you want to clone.
Open the Clone Existing Virtual Machine wizard from a virtual machine	Right-click a virtual machine and select Clone > Clone to Virtual Machine .

- 2 On the Select a name and folder page, enter a unique name for the new virtual machine and select a deployment location.

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.

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 in a different way.

- 3 On the Select a compute resource page, select the host, cluster, resource pool, or vApp where the virtual machine will run and click **Next**.

The **Compatibility** pane shows the result from the compatibility checks.

Important If the virtual machine that you clone has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, you cannot proceed with the task.

If the virtual machine that you clone does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, all the hard disk of the destination virtual machine will use the storage policy and datastore selected for the configuration files of the source virtual machine.

- 4 On the Select storage page, select the datastore or datastore cluster in which to store the template configuration files and all of the virtual disks. Click **Next**.

Option	Description
Clone a virtual machine that has vPMem hard disks	<p>a Choose the type of storage for the template by selecting the Standard, the PMem, or the Hybrid radio button.</p> <p>If you select the Standard mode, all virtual disks will be stored on a standard datastore.</p> <p>If you select the PMem mode, all virtual disks will be stored on the host-local PMem datastore. Configuration files cannot be stored on a PMem datastore and you must additionally select a regular datastore for the configuration files of the virtual machine.</p> <p>If you select the Hybrid mode, all PMem virtual disks will remain stored on a PMem datastore. Non-PMem disks are affected by your choice of a VM storage policy and datastore or datastore cluster.</p> <p>For more information about persistent memory and PMem storage, see the <i>vSphere Resource Management</i> guide.</p> <p>b (Optional) From the Select virtual disk format drop-down menu, select a new virtual disk format for the template or keep the same format as the source virtual machine.</p> <p>c (Optional) From the VM Storage Policy drop-down menu, select a virtual machine storage policy or leave the default one.</p> <p>d Select a datastore or a datastore cluster.</p> <p>e Select the Disable Storage DRS for this virtual machine check box if you do not want to use storage DRS with the virtual machine.</p> <p>f (Optional) Turn on the Configure per disk option to select a separate datastore or a datastore cluster for the template configuration file and for each virtual disk.</p> <p>Note You can use the Configure per disk option to convert a PMem hard disk to a regular one, but that change might cause performance problems. You can also convert a standard hard disk to a PMem hard disk.</p>
Clone a virtual machine that does not have vPMem hard disks	<p>a Select the disk format for the virtual machine virtual disks.</p> <p>Same format as source uses the same disk format as the source virtual machine.</p> <p>The Thick Provision Lazy Zeroed format 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 later, on demand, on first write from the virtual machine.</p> <p>Thick Provision Eager Zeroed is 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.</p>

Option	Description
	<p>The Thin Provision format saves storage space. 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.</p> <ul style="list-style-type: none"> b (Optional) Select a VM storage policy or leave the default one. c Select a datastore or a datastore cluster. d (Optional) Turn on the Configure per disk option to select a separate datastore or a datastor cluster for the template configuration file and for each virtual disk. <p>Note You can use the Configure per disk option to convert a PMem hard disk to a regular one, but that change might cause performance problems. You can also convert a standard hard disk to a PMem hard disk.</p>

Important You cannot change the storage policy if you clone an encrypted virtual machine. For information about cloning an encrypted virtual machine, see *vSphere Security*.

- 5 On the Select clone options, select additional customization options for the new virtual machine.

You can choose to customize the guest operating system or the virtual machine hardware. You can also choose to power on the virtual machine after its creation.

- 6 (Optional) On the Customize guest OS page, apply a customization specification to the virtual machine.

Customizing the guest OS prevents from conflicts that might occur if you deploy virtual machines with identical settings, such as duplicate computer names.

Note 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](#).

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

- 7 (Optional) On the Customize hardware page, configure the virtual machine hardware and options and click **Next**.

You can leave the defaults and configure the virtual machine hardware and options later. For more information, see [Chapter 5 Configuring Virtual Machine Hardware](#) and [Chapter 6 Configuring Virtual Machine Options](#)

Important If you chose to use PMem storage for the virtual machine, its default hard disk, the new hard disks that you configure, and the NVDIMM devices that you add to the virtual machine all share the same PMem resources. So, you must adjust the size of the newly added devices in accordance with the amount of the PMem available to the host. If any part of the configuration requires attention, the wizard alerts you.

- 8 On the Ready to complete page, review the virtual machine settings and click **Finish**.

The new virtual machine appears in the inventory.

Clone an Existing 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. It is recommended that you quiesce the virtual machines running lower I/O disk operation.

Prerequisites

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

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

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

- **Virtual machine .Provisioning.Read customization specifications** on the root vCenter Server if you are customizing the guest operating system.

Procedure

- 1 Open the **Clone Existing Virtual Machine** wizard.

Option	Description
Open the Clone Existing Virtual Machine wizard from any object in the inventory	<ol style="list-style-type: none"> 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 New Virtual Machine. b On the Select a creation type page, select Clone an existing virtual machine and click Next. c On the Select a virtual machine page, select the virtual machine that you want to clone.
Open the Clone Existing Virtual Machine wizard from a virtual machine	Right-click a virtual machine and select Clone > Clone to Virtual Machine .

- 2 On the Select a name and folder page, enter a unique name for the new virtual machine and select a deployment location.

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.

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 in a different way.

- 3 On the Select a compute resource page, select the host, cluster, resource pool, or vApp where the virtual machine will run and click **Next**.

The **Compatibility** pane shows the result from the compatibility checks.

Important If the virtual machine that you clone has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, you cannot proceed with the task.

If the virtual machine that you clone does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, all the hard disk of the destination virtual machine will use the storage policy and datastore selected for the configuration files of the source virtual machine.

- 4 On the Select storage page, select the datastore or datastore cluster in which to store the virtual machine configuration files and all of the virtual disks.
- a Select the format for the virtual machine's disks.

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

- b (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.
- c Select the datastore location where you want to store the virtual machine files.
- Your selection affects the storage creation process.

Option	Action
Store all virtual machine files in the same location on a datastore.	<ol style="list-style-type: none"> (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the VM storage policy drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy. Select a datastore and click Next.
Store all virtual machine files in the same datastore cluster.	<ol style="list-style-type: none"> (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the VM storage policy drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage profile. Select a datastore cluster. (Optional) If you do not want to use Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the datastore cluster. Click Next.
Store virtual machine configuration files and disks in separate locations.	<ol style="list-style-type: none"> Click Advanced. For the virtual machine configuration file and for each virtual disk, click Browse and select a datastore or datastore cluster.

Option	Action
	<ol style="list-style-type: none"> 3 Apply a virtual machine storage policy from the VM storage profile drop-down menu. <p>The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy.</p> <ol style="list-style-type: none"> 4 (Optional) If you selected a datastore cluster and do not want to use Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the datastore cluster. 5 Click Next.
Store all virtual machine files in the same non-volatile memory disk	<ol style="list-style-type: none"> 1 (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the VM storage policy drop-down menu. 2 Select a non-volatile memory disk and click Next.

Important You cannot change the storage policy if you clone an encrypted virtual machine. For information about cloning an encrypted virtual machine, see *vSphere Security*.

- 5 On the Select clone options, select additional customization options for the new virtual machine.

You can choose to customize the guest operating system or the virtual machine hardware. You can also choose to power on the virtual machine after its creation.

- 6 (Optional) On the Customize guest OS page, apply a customization specification to the virtual machine.

Customizing the guest OS prevents from conflicts that might occur if you deploy virtual machines with identical settings, such as duplicate computer names.

Note 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](#).

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

- 7 (Optional) On the Customize hardware page, configure the virtual machine hardware and options and click **Next**.

You can leave the defaults and configure the virtual machine hardware and options later. For more information, see [Chapter 5 Configuring Virtual Machine Hardware](#) and [Chapter 6 Configuring Virtual Machine Options](#)

Important If you chose to use PMem storage for the virtual machine, its default hard disk, the new hard disks that you configure, and the NVDIMM devices that you add to the virtual machine all share the same PMem resources. So, you must adjust the size of the newly added devices in accordance with the amount of the PMem available to the host. If any part of the configuration requires attention, the wizard alerts you.

- 8 On the Ready to complete page, review the virtual machine settings and click **Finish**.

The new virtual machine appears in the inventory.

Cloning a Virtual Machine with Instant Clone

You can use the Instant Clone technology to create powered on virtual machines from the running state of another powered on virtual machine. The result of an Instant Clone operation is a new virtual machine that is identical to the source virtual machine. With Instant Clone you can create new virtual machines from a controlled point in time. Instant cloning is very convenient for large scale application deployments because it ensures memory efficiency and allows for creating numerous virtual machines on a single host.

The result of an Instant Clone operation is a virtual machine that is called a destination virtual machine. The processor state, virtual device state, memory state, and disk state of the destination virtual machine are identical to those of the source virtual machine. To avoid network conflicts, you can customize the virtual hardware of the destination virtual machine during an Instant Clone operation. For example, you can customize the MAC addresses of the virtual NICs or the serial and parallel port configurations of the destination virtual machine. vSphere 6.7 does not support customization of the guest OS of the destination virtual machine. For information about manual guest OS customization, see the *vSphere Web Services SDK Programming Guide*.

During an Instant Clone operation, the source virtual machine is stunned for a short period of time, less than 1 second. While the source virtual machine is stunned, a new writable delta disk is generated for each virtual disk and a checkpoint is taken and transferred to the destination virtual machine. The destination virtual machine then powers on by using the source's checkpoint. After the destination virtual machine is fully powered on, the source virtual machine also resumes running.

Instant Cloned virtual machines are fully independent vCenter Server inventory objects. You can manage Instant Cloned virtual machines like regular virtual machines without any restrictions.

In vSphere 6.7, you can Instant Clone a virtual machine only through the API calls.

For more information about Instant Clone, see the *vSphere Web Services SDK Programming Guide*.

Clone a Template to a Template

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

Prerequisites

Verify that you have the following privileges:

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

Procedure

- 1 Start the **Clone Template to Template** wizard.

Option	Description
Open the Clone Template to Template wizard from an object in the inventory	<ol style="list-style-type: none"> a Right-click any inventory object that is a valid parent object of a virtual machine and select New Virtual Machine. b Select Clone Template to Template and click Next. c On the Select a template to clone page, browse to the template that you want to clone or accept the default one.
Open the Clone Template to Template wizard from a template	Right-click a template and select Clone to Template .

- 2 On the **Select a name and folder** page, enter a unique name for the template and select the data center or folder in which to deploy it. Click **Next**.

The template name determines the name of the files and folder on the disk. For example, if you name the template win10tmp, the template files are named win10tmp.vmdk, win10tmp.nvram, and so on. If you change the template name, the names of the files on the datastore do not change.

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 in a different way.

- 3 On the **Select a compute resource** page, select a host or cluster resource for the template.

The **Compatibility** pane shows the result from the compatibility checks.

Note 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.

Important If the template that you clone has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, you cannot proceed with the task.

If the template that you clone does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, all the hard disks of the template will use the storage policy and datastore selected for the configuration files of the source template.

- 4 On the **Select storage** page, select the datastore or datastore cluster in which to store the virtual machine configuration files and all of the virtual disks. Click **Next**.

Option	Description
Clone a virtual machine that has vPMem hard disks	<p>a Choose the type of storage for the template by selecting the Standard, the PMem, or the Hybrid radio button.</p> <p>If you select the Standard mode, all virtual disks will be stored on a standard datastore.</p> <p>If you select the PMem mode, all virtual disks will be stored on the host-local PMem datastore. Configuration files cannot be stored on a PMem datastore and you must additionally select a regular datastore for the configuration files of the virtual machine.</p> <p>If you select the Hybrid mode, all PMem virtual disks will remain stored on a PMem datastore. Non-PMem disks are affected by your choice of a VM storage policy and datastore or datastore cluster.</p> <p>For more information about persistent memory and PMem storage, see the <i>vSphere Resource Management</i> guide.</p> <p>b (Optional) From the Select virtual disk format drop-down menu, select a new virtual disk format for the template or keep the same format as the source virtual machine.</p> <p>c (Optional) From the VM Storage Policy drop-down menu, select a virtual machine storage policy or leave the default one.</p> <p>d Select a datastore or a datastore cluster.</p> <p>e Select the Disable Storage DRS for this virtual machine check box if you do not want to use storage DRS with the virtual machine.</p> <p>f (Optional) Turn on the Configure per disk option to select a separate datastore or a datastore cluster for the template configuration file and for each virtual disk.</p> <p>Note You can use the Configure per disk option to convert a PMem hard disk to a regular one, but that change might cause performance issues. You can also convert a standard hard disk to a PMem hard disk.</p>
Clone a virtual machine that does not have vPMem hard disks	<p>a Select the disk format for the virtual machine virtual disks.</p> <p>Same format as source uses the same disk format as the source virtual machine.</p> <p>The Thick Provision Lazy Zeroed format 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 later, on demand, on first write from the virtual machine.</p> <p>Thick Provision Eager Zeroed is 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.</p>

Option	Description
	The Thin Provision format saves storage space. 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.
b	(Optional) Select a VM storage policy or leave the default one.
c	Select a datastore or a datastore cluster.
d	(Optional) Turn on the Configure per disk option to select a separate datastore or a datastore cluster for the template configuration file and for each virtual disk.
	Note You can use the Configure per disk option to convert a PMem hard disk to a regular one, but that change might cause performance issues. You can also convert a standard hard disk to a PMem hard disk.

Important You cannot change the storage policy if you clone an encrypted virtual machine. For information about cloning an encrypted virtual machine, see *vSphere Security*.

- 5 On the Ready to complete page, review the template settings and click **Finish**.

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

Clone a Template to a Template in the vSphere Web Client

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

Prerequisites

Verify that you have the following privileges:

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

Procedure

- 1 Start the **Clone Template to Template** wizard.

Option	Description
Open the Clone Template to Template wizard from any object in the inventory	<ol style="list-style-type: none"> 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 New Virtual Machine. b Select Clone Template to Template and click Next. c On the Select a template to clone page, browse to the template that you want to clone or accept the default one.
Open the Clone Template to Template wizard from a template	Right-click a template and select Clone to Template .

- 2 On the Select a name and folder page, enter a unique name for the template and select the data center or folder in which to deploy it. Click **Next**.

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.

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 in a different way.

- 3 On the Select a compute resource page, select a host or cluster resource for the template.

The **Compatibility** pane shows the result from the compatibility checks.

Note 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.

Important If the template that you clone has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, you cannot proceed with the task.

If the template that you clone does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, all the hard disks of the template will use the storage policy and datastore selected for the configuration files of the source template.

- 4 On the Select storage page, select the datastore or datastore cluster in which to store the virtual machine configuration files and all of the virtual disks. Click **Next**.

- a Select the format for the virtual machine's disks.

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

- b (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.

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

Your selection affects the storage creation process.

Option	Action
Store all virtual machine files in the same location on a datastore.	<ol style="list-style-type: none"> (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the VM storage policy drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy. Select a datastore and click Next.
Store all virtual machine files in the same datastore cluster.	<ol style="list-style-type: none"> (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the VM storage policy drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage profile. Select a datastore cluster. (Optional) If you do not want to use Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the datastore cluster. Click Next.
Store virtual machine configuration files and disks in separate locations.	<ol style="list-style-type: none"> Click Advanced. For the virtual machine configuration file and for each virtual disk, click Browse and select a datastore or datastore cluster.

Option	Action
	<p>3 Apply a virtual machine storage policy from the VM storage profile drop-down menu.</p> <p>The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy.</p> <p>4 (Optional) If you selected a datastore cluster and do not want to use Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the datastore cluster.</p> <p>5 Click Next.</p>
Store all virtual machine files in the same non-volatile memory disk	<p>1 (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the VM storage policy drop-down menu.</p> <p>2 Select a non-volatile memory disk and click Next.</p>

Important You cannot change the storage policy if you clone an encrypted virtual machine. For information about cloning an encrypted virtual machine, see *vSphere Security*.

- 5 On the Ready to complete page, review the template settings and click **Finish**.

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

Convert a Template to a Virtual Machine

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

Prerequisites

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 Template to Virtual Machine** wizard.

Option	Description
Open the Convert Template to Virtual Machine wizard from an object in the inventory	<ol style="list-style-type: none"> a Right-click any inventory object that is a valid parent object of a virtual machine and select New Virtual Machine. b On the Select a creation type page, select Convert template to virtual machine and click Next. c On the Select a template page of the wizard, select a template to deploy from the list.
Open the Convert Template to Virtual Machine wizard from a template	Right-click the template and select Convert to Virtual Machine .

- 2 On the **Select a compute resource** page, select the host, cluster, vApp, or resource pool for the virtual machine to run in. Click **Next**.

Important If the template that you convert has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, you cannot proceed with the task.

If the template that you convert does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, all the hard disks of the virtual machine will use the storage policy and datastore selected for the configuration files of the source template.

The **Compatibility** pane shows the result from the compatibility checks.

- 3 On the **Ready to complete** page, review the settings and click **Finish**.

The virtual machine appears in the inventory.

Deploying OVF and OVA Templates

3

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

Note In vSphere 6.5 and later, you cannot export OVA templates, OVF templates is the only option.

In previous versions of vSphere, you needed to install the Client Integration Plug-in to deploy and export OVF or OVA templates. vSphere 6.5 no longer requires that you install the Client Integration Plug-in to export OVF templates or to deploy OVF and OVA templates.

This chapter includes the following topics:

- [OVF and OVA File Formats and Templates](#)
- [Deploy an OVF or OVA Template](#)
- [Export an OVF Template](#)
- [Browse VMware Virtual Appliance Marketplace](#)

OVF and OVA File Formats and Templates

OVF is a file format that supports exchange of virtual appliances across products and platforms. OVA is a single-file distribution of the same file package.

The OVF and OVA formats offer the following advantages:

- OVF and OVA files are compressed, allowing for faster downloads.
- The vSphere Client validates an OVF or OVA 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 and OVA can encapsulate multi-tiered applications and more than one virtual machine.

Exporting OVF or OVA 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 or OVA file available to users who cannot access your vCenter Server inventory.

Deploying an OVF or OVA template allows you to add pre-configured virtual machines or vApps to your vCenter Server or ESXi inventory. Deploying an OVF or OVA template is similar to deploying a virtual machine from a template. However, you can deploy an OVF or OVA template from any local file system accessible from the vSphere 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 or OVA Template

You can deploy an OVF or OVA template from a local file system or from a URL.

Procedure

- 1 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 **Deploy OVF Template**.

The **Deploy OVF Template** wizard opens.

- 2 On the **Select an OVF template** page, specify the location of the source OVF or OVA template and click **Next**.

Option	Action
URL	Type a URL to an OVF or OVA template located on the Internet. Supported URL sources are HTTP and HTTPS. Example: http://vmware.com/MTN/appliance.ovf .
Local file	Click Browse and select all the files associated with an OVF template or OVA file. This includes files such as .ovf, .vmdk, etc. If you do not select all the required files, a warning message displays.

- 3 On the **Select a name and folder** page, enter a unique name for the virtual machine or vAPP, select a deployment location, and click **Next**.

The default name for the virtual machine is the same as the name of the selected OVF or OVA template. If you change the default name, choose a name that is unique within each vCenter Server virtual machine folder.

The default deployment location for the virtual machine is the inventory object where you started the wizard.

- 4 On the **Select a compute resource** page, select a resource where to run the deployed VM template, and click **Next**.
- 5 On the **Review details** page, verify the OVF or OVA template details and click **Next**.

Option	Description
Publisher	Publisher of the OVF or OVA template, if a certificate included in the OVF or OVA template file specifies a publisher.
Download size	Size of the OVF or OVA file.
Size on disk	Size on disk after you deploy the OVF or OVA template.

- 6 On the **Select storage** page, define where and how to store the files for the deployed OVF or OVA template.

- a Select the disk format for the virtual machine virtual disks.

Format	Description
Thick Provision Lazy Zeroed	Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out later, on demand, on first write from the virtual machine.
Thick Provision Eager Zeroed	A type of thick virtual disk that supports clustering features such as Fault tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types o disks.
Thin Provision	Use this format to save storage space. For the thin disk, you provision as much datastore space as the disk requires 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.

- b Select a VM Storage Policy.

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

- c (Optional) Enable the **Show datastores from Storage DRS clusters** check box to choose individual datastores from Storage DRS clusters for the initial placement of the virtual machine.
- d Select a datastore to store the deployed OVF or OVA 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.

Note If you want to use the API calls to deploy an OVF template that contains vPMem hard disks and that has been exported from a content library, consult <https://ikb.vmware.com/s/article/52370>.

- 7 On the **Select networks** page, select a source network and map it to a destination network. Click **Next**.

The Source Network column lists all networks that are defined in the OVF or OVA template.

- 8 On the **Ready to complete** page, review the page and click **Finish**.

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

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.

Prerequisites

Power off the virtual machine or vApp.

Required privilege: **vApp.Export**

Procedure

- 1 Navigate to a virtual machine or vApp and select **Template > 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 (Optional) In the **Annotation** field, type a description.
- 4 Select the **Enable advanced options** check box 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. These options limit portability.

- 5 Click **OK** and respond to the prompts to save each file associated with the template (.ovf, .vmdk, .mf).

Note If you are using the Internet Explorer browser to export an OVF template, new tabs open in the browser for each file of the OVF template. For each new tab, you are prompted to accept a security certificate. Accept each security certificate, before saving each file.

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.
- 3 Log in and download the appliance.
- 4 Deploy the appliance in your vSphere environment.

Using Content Libraries

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

A content library stores and manages the different types of content as library items. A single library item can contain one file or multiple files. For example, the OVF template is a set of files (.ovf, .vmdk, .mf). When you upload an OVF template to the library, you upload the entire set of files, but in the UI you only see one library item of the OVF template type.

Content libraries support only OVF templates. As a result, VM and Vapp templates are converted to OVF files when you upload the to a content library.

You create and manage a content library from a single vCenter Server instance, but you can share the library items with other vCenter Server instances if HTTP(S) traffic is allowed between them.

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

Local Libraries

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

Subscribed Libraries

You subscribe to a published library by creating a subscribed library. You can create the subscribed library in the same vCenter Server instance where the published library is, or in a different vCenter Server system. In the **Create Library** wizard you have the option to download all the contents of the published library immediately after the subscribed library is created, or to download only metadata for the items from the published library and to later download the full content of only the items you intend to use.

To ensure the contents of a subscribed library are up-to-date, the subscribed library automatically synchronizes to the source published library on regular intervals. You can also manually synchronize subscribed libraries.

You can use the option to download content from the source published library immediately or only when needed to manage your storage space.

- When you synchronize a subscribed library that is set with the option to download all the contents of the published library immediately, the process synchronizes both the item metadata and the item contents. During synchronisation, the library items that are new for the subscribed library are fully downloaded to the storage location of the subscribed library.
- When you synchronize a subscribed library that is set with the option to download contents only when needed, the process synchronizes only the metadata for the library items from the published library, and does not download the contents of the items. This saves storage space. If you need to use a library item you need to synchronize that item. After you are done using the item, you can delete the item contents to free space on the storage. For subscribed libraries that are set with the option to download contents only when needed, synchronizing the subscribed library downloads only the metadata of all the items in the source published library, while synchronizing a library item downloads the full content of that item to your storage.

You can take advantage of optimized transfer speed for synchronization between a published and a subscribed library under certain circumstances.

- If a published and a subscribed library belong to vCenter Server systems that are in the same vCenter Single Sign-On domain, and both libraries use datastores as backing storage, transfer speed for synchronization is faster. The transfer speed optimization is made possible if the libraries can store their contents to datastores managed by ESXi hosts that are directly connected to each other. Therefore, the synchronization between the libraries is handled by a direct ESXi host to ESXi host transfer.
- If the datastores have VMware vSphere Storage APIs - Array Integration (VAAI) enabled, the library content synchronization between the published and the subscribed library is further optimized. In this case, the contents are synchronized by a direct datastore to datastore transfer.

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

Table 4-1. Source Objects to Which You Can Subscribe by Creating a Subscribed Library in the vSphere Client .

Source Object	Download library content immediately	Download library content when needed
A library running in a vCenter Server 6.x instance.	Supported	Supported
A catalog running in a vCloud Director 5.5 and later instance.	Supported	Not supported
A third-party library.	Supported for third-party libraries that require authentication, if the username of the third-party library is vcsp . If the username of the source third-party library is different than vcsp , you can subscribe to it by using VMware vCloud Suite API.	Supported for third-party libraries that require authentication, if the username of the third-party library is vcsp . If the username of the source third-party library is different than vcsp , you can subscribe to it by using VMware vCloud Suite API.

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

This chapter includes the following topics:

- [Create a Library](#)
- [Synchronize a Subscribed Content Library](#)
- [Edit a Content Library](#)
- [Hierarchical Inheritance of Permissions for Content Libraries](#)
- [Content Library Administrator Role](#)
- [Populating Libraries with Content](#)
- [Creating Virtual Machines and vApps from Templates in a Content Library](#)
- [Working with Items in a Library](#)

Create a Library

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

Prerequisites

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

Procedure

- 1 Open the **New Content Library** wizard.

Client	Steps
vSphere Client	a Select Menu > Content Libraries .
	b Click the Create a new content library icon (+).
vSphere Web Client	a Select Home > Content Libraries .
	b On the Objects tab, click the Create a new content library icon.

- 2 On the Name and location page, enter a name and select a vCenter Server instance for the content library. Click **Next**.

- 3 On the Configure content library page, select the type of content library that you want to create and click **Next**.

Option	Description
Local content library	<p>A local content library is accessible only in the vCenter Server instance where you create it by default.</p> <ul style="list-style-type: none"> a Select Publish externally to make the content of the library available to other vCenter Server instances. b (Optional) Select Optimize for syncing over HTTP to optimize synchronization. c (Optional) Select Enable authentication and set a password if you want to require a password for accessing the content library.
Subscribed content library	<p>Creates a content library that subscribes to published content library. Use this option to take advantage of already existing content libraries.</p> <p>You can sync the subscribed library with the published library to see up-to-date content, but you cannot add or remove content from the subscribed library. Only an administrator of the published library can add, modify, and remove contents from the published library.</p> <p>Provide the following information to subscribe to a library:</p> <ul style="list-style-type: none"> a In the Subscription URL text box, enter the URL address of the published library. b If authentication is enabled on the published library, select Enable authentication and enter the publisher password. c Select a download method for the contents of the subscribed library. <ul style="list-style-type: none"> ■ If you want to download a local copy of all the items in the published library immediately after subscribing to it, select immediately. ■ If you want to save storage space, select when needed. You download only the metadata for the items in the published library. <p>If you need to use an item, synchronize the item or the entire library to download its content.</p> d If prompted, accept the SSL certificate thumbprint. <p>The SSL certificate thumbprint is stored on your system until you delete the subscribed content library from the inventory.</p>

- 4 On the Add storage page, select a storage location for the content library contents and click **Next**.

Client	Steps
vSphere Client	Select a datastore.
vSphere Web Client	Select a datastore, or enter the path to a remote storage location where to keep the contents of the library.

- 5 On the Ready to Complete page, review the details and click **Finish**.

Synchronize a Subscribed Content Library

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

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

Prerequisites

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

Procedure

- 1 Navigate to the **Content Libraries** list.

Client	Steps
vSphere Client	Select Menu > Content Libraries .
vSphere Web Client	<ol style="list-style-type: none"> a Select Home > Content Libraries. b Click the Objects tab.

- 2 Right-click a subscribed library and select **Synchronize**.

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

Edit a Content Library

From the vSphere Client, you can edit the settings of a local content library or a subscribed library, and you can delete a library.

You can publish a local library from your vCenter Server instance to share its contents across multiple vCenter Server systems. From the Edit Setting dialog box, you can obtain the URL of your library and send it to other users to subscribe.

If a library is already published, you can change its password for authentication. Users who are subscribed to your library must update the password to keep access to the published library.

Prerequisites

The privileges you need depend on the task you want to perform.

Task	Privilege
Edit Local Content Library Settings	Content library.Update library and Content library.Update local library on the library.
Edit Subscribed Content Library Settings	Content library.Update subscribed library and Content library.Probe subscription information on the subscribed library.
Delete Content Library	Content library.Delete subscribed library or Content library.Delete local library on the type of library you want to delete.

Procedure

- 1 Navigate to the **Content Libraries** list.

Client	Steps
vSphere Client	Select Menu > Content Libraries .
vSphere Web Client	<ol style="list-style-type: none"> a Select Home > Content Libraries. b Click the Objects tab.

- 2 Right-click a content library and select the action that you want to perform.

Client	Task
vSphere Client	<p>You can perform the following actions with a content library.</p> <ul style="list-style-type: none"> ■ Select Edit notes to edit the content library description. ■ Select Rename to change the name of the content library. ■ Select Tags > Assign Tag to assign a tag to the content library. <p>For more information about tags and tag categories, see the <i>vCenter Server and Host Management</i> guide.</p> <ul style="list-style-type: none"> ■ Select Tags > Remove Tag to remove a tag from the content library. <p>For more information about tags and tag categories, see the <i>vCenter Server and Host Management</i> guide.</p> <ul style="list-style-type: none"> ■ Select Delete to delete the content library. ■ Select Edit settings to make changes to a content library. <p>The changes that you can make depend on the type of content library that you edit. Consult the table below to learn about the different options.</p>
vSphere Web Client	<p>You can perform the following actions with a content library.</p> <ul style="list-style-type: none"> ■ Select Edit notes to edit the content library description. ■ Select Rename to change the name of the content library. ■ Select Delete to delete the content library. ■ Select Edit settings to make changes to a content library. <p>The changes that you can make depend on the type of content library that you edit. Consult the table below to learn about the different options.</p>

- 3 If you want to edit the settings of a content library, right-click the content library and click **Edit Settings**.

Task	Action
Edit local content library that is unpublished	<p>You can publish a local library to share its contents with other users.</p> <ol style="list-style-type: none"> Select the Publish this library externally check box to publish the local library and share its contents with other users. Click the Copy Link button to obtain the URL of your library and distribute it. (Optional) Select Enable user authentication for access to this content library to set a password for the library. <p>If you password protect the library, you must provide both the URL and the password to users who want to subscribe to your library.</p> <ol style="list-style-type: none"> Click OK.
Edit local content library that is published	<p>You can change the following settings of a local library that is published.</p> <ul style="list-style-type: none"> ■ You can copy the subscription URL to your library and send it to other users to subscribe. ■ You can unpublish the library by deselecting the Publish this library externally check box. Users who are currently subscribed to this library can no longer use the library contents. ■ You can enable or disable authentication for the library. ■ In the vSphere Web Client, you can change the password for authentication if the library is published and password-protected. <ol style="list-style-type: none"> Click Change Password. Enter the current password and the new password. Confirm the new password. Click OK.
Edit subscribed content library	<p>You can change the following settings of a subscribed library:</p> <ul style="list-style-type: none"> ■ Enable or disable the automatic synchronization with the published library. ■ Update the password for authentication to the published library. ■ Select a download method. You can either download all library content immediately or download library content only when needed. <p>If you switch from the option to download content only when needed to the option to download all library content immediately, a synchronization task starts and content starts downloading. The number and size of items in the published library determine the amount of time and network bandwidth that the task requires.</p>

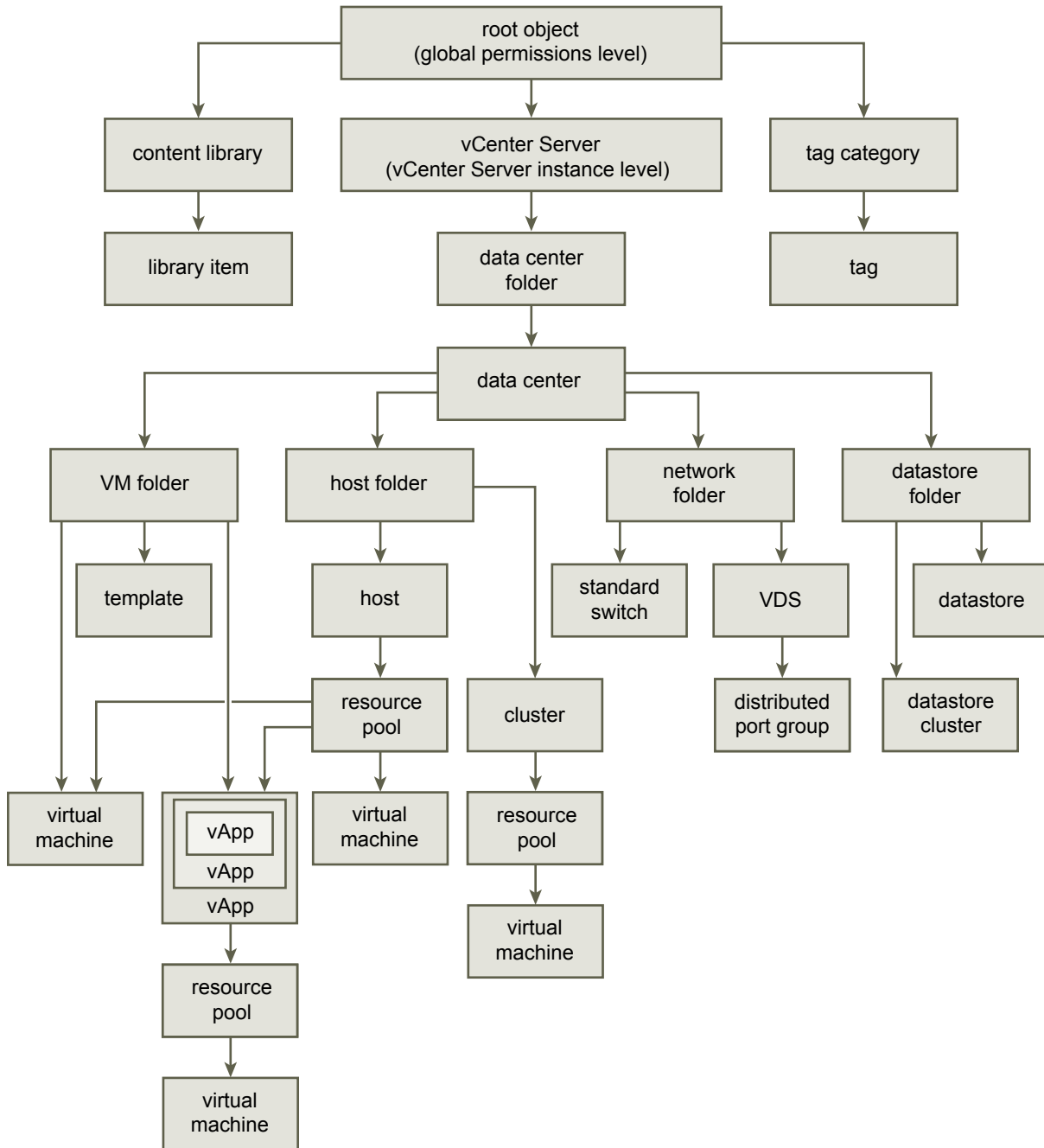
Hierarchical Inheritance of Permissions for Content Libraries

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

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

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

Figure 4-1. vSphere Inventory Hierarchy



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

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

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

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

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

Content Library Administrator Role

vCenter Server provides a sample role that allows you to give users or groups privileges to manage selected content libraries.

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

You can modify the role or use it as an example to create custom roles for specific tasks you want to allow other users to perform.

If a user has this role on a library, that user can perform the following tasks on that library.

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

Populating Libraries with Content

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

There are multiple ways to populate a library with items.

■ [Add Items to a Content Library](#)

You can import items such as VM templates and vApps to a content library from your local machine or from a Web server, and use them to create virtual machines and vApps. You can also import ISO images, certificates, and other files that you want to keep in the library and share with other users across multiple vCenter Server instances. You can add an item that resides on a Web server to a content library, or you can add items to a content library by importing files from your local file system.

■ [Clone a vApp to a Template in Content Library in the vSphere Web Client](#)

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

■ [Clone a Virtual Machine or a VM Template to a Template in a Content Library](#)

You can clone virtual machines or VM templates from your vCenter Server inventory to templates in the content library and use them later to provision virtual machines on a cluster or a host. You can also clone a virtual machine or VM template to update an existing template in the library.

■ [Clone Library Items from One Library to Another Library](#)

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

Add Items to a Content Library

You can import items such as VM templates and vApps to a content library from your local machine or from a Web server, and use them to create virtual machines and vApps. You can also import ISO images, certificates, and other files that you want to keep in the library and share with other users across multiple vCenter Server instances. You can add an item that resides on a Web server to a content library, or you can add items to a content library by importing files from your local file system.

You can import an OVF package to use as a template for deploying virtual machines and vApps. You can also import other types of files, such as scripts or ISO files, that you want to use in your vCenter Server instance, or you want to share across multiple vCenter Server systems.

Prerequisites

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

Procedure

- 1 Navigate to the **Content Libraries** list.

Client	Steps
vSphere Client	Select Menu > Content Libraries .
vSphere Web Client	<ol style="list-style-type: none"> a Select Home > Content Libraries. b Click the Objects tab.

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

The **Import Library Item** dialog box opens.

- 3 In the Source section, choose the source of the item.

Option	Description
Import from a URL	Enter the path to a Web-server where the item is.
Import from File	Click Browse to navigate to the file that you want to import from your local system. You can use the drop-down menu to filter files in your local system.
	Note When you import an OVF template, first select the OVF descriptor file (.ovf). Next, you are prompted to select the other reference files in the OVF template. Reference files might include files such as .vmdk and .mf.

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

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

Clone a vApp to a Template in Content Library in the vSphere Web Client

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

Procedure

- 1 In the vSphere Web Client navigator, click **vCenter Inventory Lists > vApps**.
- 2 Right-click a vApp and select **Clone > Clone to Template in Library**.

The **Clone to Template in Content Library** dialog box opens.

- 3 Select the **New template** radio button.
- 4 From the list of available libraries, select the content library to which you want to add the template.
- 5 Type a name and description for the template.
- 6 (Optional) Include or exclude vApp-related configurations in the template that you clone, and click **OK**.

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

A new task for cloning to OVF package appears in the Recent Tasks pane. After the task is complete, the vApp template appears on the **Templates** tab for the content library.

What to do next

Use the template to provision vApps on a host or a cluster in your vSphere inventory. See [Create New vApp From a Template in a Content Library in the vSphere Web Client](#).

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

You can clone virtual machines or VM templates from your vCenter Server inventory to templates in the content library and use them later to provision virtual machines on a cluster or a host. You can also clone a virtual machine or VM template to update an existing template in the library.

Templates are master copies of virtual machines that you can use to create virtual machines that are ready for use. You can make changes to the template, such as installing additional software in the guest operating system, while preserving the state of the original template. For more information, see [Templates in Content Libraries](#).

Procedure

- 1 In the vSphere Client, navigate to the virtual machine or template that you want to clone.
- 2 Start the cloning task.
 - Right-click a virtual machine and select **Clone > Clone to Template in Library**.
 - Right-click a VM template, and select **Clone to Library**.
- 3 Select the **Clone as** option.

Option	Description
New template	a Select New template .
	b Select the content library where to add the template.
Update existing template	a Select Update existing template .
	b Select the template to update.

- 4 From the content libraries list, select the library in which you want to add the template.
- 5 Enter a name and description for the template.
- 6 (Optional) Select the configuration data that you want to include in the template.
 You can select to preserve the MAC-addresses on the network adapters and include extra configuration.
- 7 Click **OK**.

A new task for cloning to OVF package appears in the Recent Tasks pane. After the task is complete, the template appears in the **Templates** tab for the content library.

What to do next

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

Clone Library Items from One Library to Another Library

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

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

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

Procedure

- 1 Navigate to the **Content Libraries** list.

Client	Steps
vSphere Client	Select Menu > Content Libraries .
vSphere Web Client	<ol style="list-style-type: none"> a Select Home > Content Libraries. b Click the Objects tab.

- 2 Click a content library and click the **Templates** tab.

- 3 Right-click a template and select **Clone Item**.

The **Clone Library Item** dialog box opens.

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

- 5 From the list of content libraries, select the library in which you want to clone the template and click **OK**.

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

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

What to do next

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

Creating Virtual Machines and vApps from Templates in a Content Library

You can deploy virtual machines and vApps from VMs or from vApp templates that are stored in a content library.

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

The use of templates results in consistency, compliance, and efficiency when you deploy virtual machines and vApps in your data center.

Deploy VM to a Host or a Cluster from VM Template in the vSphere Client

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

Procedure

- 1 In the vSphere Client, select **Menu > Content Libraries**.
- 2 Select a content library and click the **Templates** tab.
- 3 Right-click a VM Template and select **New VM from This Template**.

The **New Virtual Machine from Content Library** wizard opens.

- 4 On the **Select a name and folder** page, enter a name and select a location for the virtual machine.
- 5 On the **Select a compute resource** page, select a host, a cluster, a resource pool, or a vApp where to run the deployed VM template, and click **Next**.

Important If the template that you deploy has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, you cannot proceed with the task.

If the template that you deploy does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, all the hard disks of the virtual machine will use the storage policy and datastore selected for the configuration files of the source template.

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

- 7 On the Select storage page, select the datastore or datastore cluster in which to store the virtual machine configuration files and all of the virtual disks. Click **Next**.

Option	Description
Deploy a virtual machine from a template that has vPMem hard disks	<p>a Choose the type of storage for the template by selecting the Standard, the PMem, or the Hybrid radio button.</p> <p>If you select the Standard mode, all virtual disks will be stored on a standard datastore.</p> <p>If you select the PMem mode, all virtual disks will be stored on the host-local PMem datastore. Configuration files cannot be stored on a PMem datastore and you must additionally select a regular datastore for the configuration files of the virtual machine.</p> <p>If you select the Hybrid mode, all PMem virtual disks will remain stored on a PMem datastore. Non-PMem disks are affected by your choice of a VM storage policy and datastore or datastore cluster.</p> <p>For more information about persistent memory and PMem storage, see the <i>vSphere Resource Management</i> guide.</p> <p>b (Optional) From the VM Storage Policy drop-down menu, select a virtual machine storage policy or leave the default one.</p> <p>c Select a datastore or a datastore cluster.</p> <p>d Select the Disable Storage DRS for this virtual machine check box if you do not want to use storage DRS with the virtual machine.</p> <p>e (Optional) Turn on the Configure per disk option to select a separate datastore or a datastore cluster for the template configuration file and for each virtual disk.</p> <hr/> <p>Note You can use the Configure per disk option to convert a PMem hard disk to a regular one, but that change might cause performance problems. You can also convert a standard hard disk to a PMem hard disk.</p>
Deploy a virtual machine from a template that does not have vPMem hard disks	<p>a Select the disk format for the virtual machine virtual disks.</p> <p>Same format as source uses the same disk format as the source virtual machine.</p> <p>The Thick Provision Lazy Zeroed format 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 later, on demand, on first write from the virtual machine.</p> <p>Thick Provision Eager Zeroed is 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.</p>

Option	Description
	The Thin Provision format saves storage space. 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.
b	(Optional) Select a VM storage policy or leave the default one.
c	Select a datastore or a datastore cluster.
d	(Optional) Turn on the Configure per disk option to select a separate datastore or a datastore cluster for the template configuration file and for each virtual disk.
Note You can use the Configure per disk option to convert a PMem hard disk to a regular one, but that change might cause performance problems. You can also convert a standard hard disk to a PMem hard disk.	

Note If you want to use the API calls to deploy an OVF template that contains vPMem hard disks and that has been exported from a content library, consult <https://ikb.vmware.com/s/article/52370>.

- 8 On the Select networks page, select a network for each network adapter in the template and click **Next**.
- 9 On the Ready to complete page, review the page and click **Finish**.

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

Deploy a Virtual Machine From a VM Template in the Content Library in the vSphere Web Client

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

Procedure

- 1 Select **Home > Content Libraries**.
- 2 Select a content library and click the **Templates** tab.
- 3 Right-click a VM Template and select **New VM from This Template**.
The **New Virtual Machine from Content Library** wizard opens.
- 4 On the Select name and location page, enter a name and select a location for the virtual machine.
- 5 (Optional) To apply a customization specification to your virtual machine, select the **Customize the operating system** check-box and click **Next**.
- 6 On the Customize Guest OS page, select a customization specification or create a new one, and click **Next**.
- 7 On the Select a resource page, select a host, a cluster, a resource pool, or a vApp where to run the deployed VM template, and click **Next**.

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

9 On the Select storage page, configure the datastore.

- a Select the format for the virtual machine's disks.

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

- b (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.

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

Your selection affects the storage creation process.

Option	Action
Store all virtual machine files in the same location on a datastore.	<ol style="list-style-type: none"> (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the VM storage policy drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy. Select a datastore and click Next.
Store all virtual machine files in the same datastore cluster.	<ol style="list-style-type: none"> (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the VM storage policy drop-down menu. The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage profile. Select a datastore cluster. (Optional) If you do not want to use Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the datastore cluster. Click Next.
Store virtual machine configuration files and disks in separate locations.	<ol style="list-style-type: none"> Click Advanced. For the virtual machine configuration file and for each virtual disk, click Browse and select a datastore or datastore cluster.

Option	Action
	<p>3 Apply a virtual machine storage policy from the VM storage profile drop-down menu.</p> <p>The list shows which datastores are compatible and which are incompatible with the selected virtual machine storage policy.</p> <p>4 (Optional) If you selected a datastore cluster and do not want to use Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the datastore cluster.</p> <p>5 Click Next.</p>
Store all virtual machine files in the same non-volatile memory disk	<p>1 (Optional) Apply a virtual machine storage policy for the virtual machine home files and the virtual disks from the VM storage policy drop-down menu.</p> <p>2 Select a non-volatile memory disk and click Next.</p>

10 On the Select networks page, select a network for each network adapter in the template and click **Next**.

11 On the Ready to complete page, review the page and click **Finish**.

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

Create New vApp From a Template in a Content Library in the vSphere Web Client

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

Procedure

- 1 In the vSphere Web Client, select **Home > Content Libraries** and click the **Objects** tab.
- 2 Select a content library, and click the **Templates** tab.
- 3 Right-click a vApp template and select **New vApp from This Template**.
- 4 On the Select name and location page, enter a name and select a location for the vApp, and click **Next**.
- 5 On the Select a resource page, select a host, a cluster, a resource pool, or a vApp to deploy the vApp to.
- 6 On the Select a resource page, select an object to deploy the vApp to and click **Next**.
- 7 On the Review details page, verify the template details and click **Next**.
- 8 On the Select storage page, select disk format and a storage resource for the vApp.
- 9 On the Select networks page, select a destination network for each source network.
- 10 On the Ready to Complete page, review the configurations you made for the vApp, and click **Finish**.

A new task for creating the vApp appears in the Recent Tasks pane. After the task is complete, the new vApp is created.

Working with Items in a Library

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

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

Templates in Content Libraries

Templates are master copies of virtual machines that you can use to deploy virtual machines that are customized and ready for use. Templates promote consistency throughout your vSphere environment. Content libraries support only OVF templates. As a result, VM and vApp templates are converted to OVF files when you upload them to a content library. You can use the templates to deploy virtual machines and vApps in the vSphere inventory.

VM Templates in Content Libraries

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

vApp Templates in Content Libraries

A vApp template is a template of a vApp, which can contain multiple virtual machines or multiple vApps. vApp templates are inventory objects that exist only in content libraries. A vApp template that resides in a content library is in OVF format. Because the OVF format is actually a set of files, if you export the template, all the files in the OVF template library item (.ovf, .vmdk, .mf) are saved to your local system.

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

Synchronize a Library Item in a Subscribed Library

To update or download the content of a library item in a subscribed library, you can synchronize the library item.

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

Prerequisites

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

Procedure

- Navigate to the **Content Libraries** list.

Client	Steps
vSphere Client	Select Menu > Content Libraries .
vSphere Web Client	<ol style="list-style-type: none"> Select Home > Content Libraries. Click the Objects tab.

- Select a subscribed library from the list.
- Synchronize the item you need to use.
 - On the **Templates** tab, right-click a VM or a vApp template, and select **Synchronize Item**.
 - On the **Other Types** tab, right-click an item, and select **Synchronize Item**.

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

Export an Item from a Content Library to Your Local Computer

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

Prerequisites

Required privilege: **Content library.Download files** on the library.

Procedure

- Navigate to the **Content Libraries** list.

Client	Steps
vSphere Client	Select Menu > Content Libraries .
vSphere Web Client	<ol style="list-style-type: none"> Select Home > Content Libraries. Click the Objects tab.

- Select a content library.

- 3 Select the type of file you want to export.
 - From the **Templates** tab, right-click a template from the library, and select **Export Item**.
 - From the **Other Types** tab, right-click a file from the library that is not a template, and select **Export Item**.
- 4 In the **Export Library Item** dialog box click **OK**.
- 5 If you are exporting an OVF template, you are prompted to save each file associated with the template to the browser download location (for example, .vmdk and .mf files)

Note If you are using the Internet Explorer browser to export an OVF template, new tabs open in the browser for each file of the OVF template. For each new tab, you are prompted to accept a security certificate. Accept each security certificate, before saving each file.

Update a Content Library Item in the vSphere Web Client

Managing and keeping your virtual environment up-to-date might require you to update the content of a library item. For example, you can directly update a VM template when you want to add a patch to it, instead of deleting the existing template and creating a new one.

Prerequisites

Verify that you have the Content Library Administrator role.

Procedure

- 1 In the vSphere Web Client, select **Home > Content Libraries** and choose a content library.
- 2 Click a content library and select the file that you want to update.
 - From the **Templates** tab, right-click a template from the library, and select **Update Item**.
 - From the **Other Types** tab, right-click a file from the library that is not a template, and select **Update Item**.

The **Update Library Item** dialog box opens.

- 3 In the Contents section, select a file to overwrite the item in your library with.

Option	Description
URL	Enter the URL to a web server where the item is stored .
Browse	Navigate to an item that is stored on your local system.

- 4 (Optional) In the Details section, change the name of the item, the description of the item, or both. Click **OK**.

The content of the item is updated. In the **Summary** tab of the item, you can view the time of the last update of the item.

Delete Content Library Items or Item Contents

If you use a subscribed library, and you synchronize it, you can later delete the library from storage but keep the metadata. You can also delete a library item such as a template completely.

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

Prerequisites

Required privileges depend on the task you want to perform.

Task	Required Privileges
Delete the contents of a library item	Content library.Evict library item
Delete a library item	Content library.Delete library item

Procedure

- 1 Navigate to the **Content Libraries** list.

Client	Steps
vSphere Client	Select Menu > Content Libraries .
vSphere Web Client	a Select Home > Content Libraries . b Click the Objects tab.

- 2 Click a content library, select the type of item, and select the task you want to perform with the item.

Client	Description
vSphere Client	<p>In the vSphere Client, you can only delete the selected item.</p> <ul style="list-style-type: none">■ From the Templates tab, right-click a template from the library, and select Delete .■ From the Other Types tab, right-click a file from the library that is not a template, and select Delete .
vSphere Web Client	<p>In the vSphere Web Client, you can delete the contents of an item or delete the item altogether.</p> <p>To delete the contents of an item, do the following.</p> <ul style="list-style-type: none">■ From the Templates tab, right-click a template from the library, and select Delete Item Content.■ From the Other Types tab, right-click a file from the library that is not a template, and select Delete Item Content. <p>To delete an item, do the following.</p> <ul style="list-style-type: none">■ From the Templates tab, right-click a template from the library, and select Delete .■ From the Other Types tab, right-click a file from the library that is not a template, and select Delete .

Configuring Virtual Machine Hardware

5

You can add or configure most virtual machine hardware settings during virtual machine creation or configure those settings after you create the virtual machine and install the guest operating system.

When you configure the virtual machine hardware, you can view the existing hardware configuration and add or remove hardware. You can change nearly every setting that was selected during virtual machine creation.

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](#)
- [Virtual Disk Configuration](#)
- [SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility](#)
- [Virtual Machine Network Configuration](#)
- [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](#)
- [Add a Shared Smart Card Reader to Virtual Machines](#)
- [Securing Virtual Machines with Virtual Trusted Platform Module](#)

Virtual Machine Compatibility

When you create a virtual machine or upgrade an existing virtual machine, you use the virtual machine compatibility setting to select the ESXi host versions that the virtual machine can run on.

The compatibility setting determines the virtual hardware available to the virtual machine, which corresponds to the physical hardware available on the host. Virtual hardware includes BIOS and EFI, available virtual PCI slots, maximum number of CPUs, maximum memory configuration, and other characteristics. New virtual hardware capabilities are typically released once a year with major or minor releases of vSphere.

Each virtual machine compatibility level supports at least five major or minor vSphere releases. For example, a virtual machine with ESXi 3.5 and later compatibility can run on ESXi 3.5, ESXi 4.0, ESXi 4.1, ESXi 5.0, ESXi 5.1, ESXi 5.5, ESXi 6.0, ESXi 6.5, and ESXi 6.7.

Table 5-1. Virtual Machine Compatibility Options

Compatibility	Description
ESXi 6.7 and later	This virtual machine (hardware version 14) is compatible with ESXi 6.7.
ESXi 6.5 and later	This virtual machine (hardware version 13) is compatible with ESXi 6.5 and ESXi 6.7.
ESXi 6.0 and later	This virtual machine (hardware version 11) is compatible with ESXi 6.0, ESXi 6.5, and ESXi 6.7.
ESXi 5.5 and later	This virtual machine (hardware version 10) is compatible with ESXi 5.5, ESXi 6.0, ESXi 6.5, and ESXi 6.7.
ESXi 5.1 and later	This virtual machine (hardware version 9) is compatible with ESXi 5.1, ESXi 5.5, ESXi 6.0, ESXi 6.5, and ESXi 6.7.
ESXi 5.0 and later	This virtual machine (hardware version 8) is compatible with ESXi 5.0, ESXi 5.1, ESXi 5.5, ESXi 6.0, ESXi 6.5, and ESXi 6.7.
ESX/ESXi 4.0 and later	This virtual machine (hardware version 7) is compatible with ESX/ ESXi 4.0, ESX/ ESXi 4.1, ESXi 5.0, ESXi 5.1, ESXi 5.5, ESXi 6.0, ESXi 6.5, and ESXi 6.7.
ESX/ESXi 3.5 and later	This virtual machine (hardware version 4) is compatible with ESX/ESXi 3.5, ESX/ ESXi 4.0, ESX/ ESXi 4.1, ESXi 5.1, ESXi 5.5, ESXi 6.0, ESXi 6.5, and ESXi 6.7. 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.

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 6.0, ESXi 6.5, and ESXi 6.7 hosts	ESXi 6.5 and later	<p>Gives you access to virtual hardware features that are not available with ESXi 6.0.</p> <ul style="list-style-type: none"> ■ You cannot migrate this virtual machine to an ESXi 6.0 host. ■ This virtual machine does not have all the capabilities available to virtual machines that run on ESXi 6.7 hosts.
Cluster with ESXi 6.0, ESXi 6.5, and ESXi 6.7 hosts	ESXi 6.7 and later	<p>This provides access to the latest virtual hardware features and ensures best performance. However, a virtual machine with such compatibility cannot run on ESXi 6.0 or ESXi 6.5.</p>

Set the Default Compatibility for Virtual Machine Creation

You can set the default compatibility for virtual machine creation on the host, cluster, or data center. These options ensure that when virtual machines are added to an existing vSphere environment, they are 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 data center setting.
- A default compatibility setting on the cluster overrides a default data center setting.

Prerequisites

Required privileges:

- On the host or cluster: **Host.Inventory.Modify cluster**
- On the data center: **Datacenter.Reconfigure datacenter**

Procedure

- ◆ Select a host, cluster, or data center in the inventory.

Option	Action
Host	<ol style="list-style-type: none"> Click the Configure tab, and under Virtual Machines, select Default VM Compatibility. Click Edit. The Edit Default VM Compatibility dialog box opens. From the Compatible with drop-down menu, select the compatibility and click OK. <p>Note You can set the compatibility only on hosts that are not part of a cluster.</p>
Cluster	<ol style="list-style-type: none"> Click the Configure tab, and under Configuration, select General. In the Default VM Compatibility section, click Edit. From the Compatible with drop-down menu, select the compatibility and click OK. <p>When you change the compatibility for a cluster, the compatibility for all hosts in the cluster changes as well.</p>
Data Center	<ol style="list-style-type: none"> Right-click the data center and select Edit Default VM Compatibility. From the Compatible with drop-down menu, select the compatibility and click OK. <p>Important You can set a default compatibility setting on a data center only in the vSphere Web Client.</p>

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 to the latest version of VMware Tools. On Microsoft Windows virtual machines, if you upgrade the compatibility level before you upgrade VMware Tools, the virtual machine might lose its network settings.
- Verify that all .vmdk files are available to the ESX/ESXi host on a VMFS5, or NFS datastore.
- Verify that the virtual machine is stored on VMFS5 or NFS datastores.

Procedure

- 1 Right-click a virtual machine and select **Compatibility > Schedule VM Compatibility Upgrade**.
- 2 In the **Schedule VM Compatibility Upgrade** dialog box, confirm that you want to schedule a compatibility upgrade by clicking **Yes**.
- 3 From the **Compatible with** drop-down menu, select the compatibility to upgrade to.
The virtual machine compatibility is upgraded the next time you restart the virtual machine.
- 4 (Optional) To upgrade the compatibility when you do regularly scheduled guest maintenance, select **Only upgrade after normal guest OS shutdown**.

The virtual machine compatibility is upgraded and the new version appears on the virtual machine Summary tab.

Change the Default Virtual Machine Compatibility Setting

The virtual machine compatibility determines the virtual hardware available to the virtual machine. You can schedule a compatibility upgrade to make a virtual machine compatible with newer versions of ESXi.

Prerequisites

- Create a backup or snapshot of the virtual machines. See [Using Snapshots To Manage Virtual Machines](#).
- Upgrade to the latest version of VMware Tools. If you upgrade the compatibility before you upgrade VMware Tools, the virtual machine might lose its network settings.
- Verify that all .vmdk files are available to the 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 (Optional) To determine the compatibility setting of a virtual machine, select the virtual machine in the inventory and click the **Summary** tab.

2 Change the default virtual machine compatibility setting.

Client	Tasks
vSphere Client	<ul style="list-style-type: none"> Change the default compatibility setting of a virtual machine. <ul style="list-style-type: none"> Right-click a virtual machine and click Compatibility > Upgrade VM Compatibility. Right-click a virtual machine and click Compatibility > Schedule VM Compatibility Upgrade. Change the default compatibility setting of a host or a cluster. See Set the Default Compatibility for Virtual Machine Creation.
vSphere Web Client	<ul style="list-style-type: none"> Change the default compatibility setting of a virtual machine. <ul style="list-style-type: none"> Right-click a virtual machine and click Compatibility > Upgrade VM Compatibility. Right-click a virtual machine and click Compatibility > Schedule VM Compatibility Upgrade. Change the default compatibility setting of a host, cluster, or data center. <ul style="list-style-type: none"> Right-click the object and select Edit Default VM Compatibility. <p>Note If a host is in a cluster, it has the virtual machine compatibility set on the cluster level, and the menu item is grayed out.</p>

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

Feature	ESXi 6.7 and later	ESXi 6.5 and later	ESXi 6.0 and later	ESXi 5.5 and later	ESXi 5.1 and later	ESXi 5.0 and later	ESX/ESXi 4.x and later	ESX/ESXi 3.5 and later
Hardware version	14	13	11	10	9	8	7	4
Maximum memory (GB)	6128	6128	4080	1011	1011	1011	255	64
Maximum number of logical processors	128	128	128	64	64	32	8	4

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

Feature	ESXi 6.7 and later	ESXi 6.5 and later	ESXi 6.0 and later	ESXi 5.5 and later	ESXi 5.1 and later	ESXi 5.0 and later	ESX/ESXi 4.x and later	ESX/ESXi 3.5 and later
Maximum number of cores (virtual CPUs) per socket	128	128	128	64	64	32	8	1
Maximum SCSI adapters	4	4	4	4	4	4	4	4
Bus Logic adapters	Y	Y	Y	Y	Y	Y	Y	Y
LSI Logic adapters	Y	Y	Y	Y	Y	Y	Y	Y
LSI Logic SAS adapters	Y	Y	Y	Y	Y	Y	Y	N
VMware Paravirtual controllers	Y	Y	Y	Y	Y	Y	Y	N
SATA controllers	4	4	4	4	N	N	N	N
NVMe Controllers	4	4	N	N	N	N	N	N
Virtual SCSI disk	Y	Y	Y	Y	Y	Y	Y	Y
SCSI passthrough	Y	Y	Y	Y	Y	Y	Y	Y
SCSI hot plug support	Y	Y	Y	Y	Y	Y	Y	Y
IDE nodes	Y	Y	Y	Y	Y	Y	Y	Y

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

Feature	ESXi 6.7 and later	ESXi 6.5 and later	ESXi 6.0 and later	ESXi 5.5 and later	ESXi 5.1 and later	ESXi 5.0 and later	ESX/ESXi 4.x and later	ESX/ESXi 3.5 and later
Virtual IDE disk	Y	Y	Y	Y	Y	Y	Y	N
Virtual IDE CD-ROMs	Y	Y	Y	Y	Y	Y	Y	Y
IDE hot plug support	N	N	N	N	N	N	N	N
Maximum NICs	10	10	10	10	10	10	10	4
PCNet32	Y	Y	Y	Y	Y	Y	Y	Y
VMXNet	Y	Y	Y	Y	Y	Y	Y	Y
VMXNet 2	Y	Y	Y	Y	Y	Y	Y	Y
VMXNet 3	Y	Y	Y	Y	Y	Y	Y	N
E1000	Y	Y	Y	Y	Y	Y	Y	Y
E1000e	Y	Y	Y	Y	Y	Y	N	N
USB 1.x and 2.0	Y	Y	Y	Y	Y	Y	Y	N
USB 3.0	Y	Y	Y	Y	Y	Y	N	N
Maximum video memory (MB)	128	128	128	512	512	128	128	128
Maximum graphics memory (GB)	2	2	2	N	N	N	N	N
SVGA displays	10	10	10	10	10	10	10	1
SVGA 3D hardware acceleration	Y	Y	Y	Y	Y	Y	N	N
VMCI	Y	Y	Y	Y	Y	Y	Y	N

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

Feature	ESXi 6.7 and later	ESXi 6.5 and later	ESXi 6.0 and later	ESXi 5.5 and later	ESXi 5.1 and later	ESXi 5.0 and later	ESX/ESXi 4.x and later	ESX/ESXi 3.5 and later
PCI passthrough	16	16	16	6	6	6	6	0
PCI Hot plug support	Y	Y	Y	Y	Y	Y	Y	N
Nested HV support	Y	Y	Y	Y	Y	N	N	N
vPMC support	Y	Y	Y	Y	Y	N	N	N
Serial ports	32	32	32	4	4	4	4	4
Parallel ports	3	3	3	3	3	3	3	3
Floppy devices	2	2	2	2	2	2	2	2
Virtual RDMA	Y	Y	N	N	N	N	N	N
NVDIMM controller	1	N	N	N	N	N	N	N
NVDIMM device	64	N	N	N	N	N	N	N
Virtual I/O MMU	Y	N	N	N	N	N	N	N
Virtual TPM	Y	N	N	N	N	N	N	N
Microsoft VBS	Y	N	N	N	N	N	N	N

Virtual CPU Configuration

You can add, change, or configure CPU resources to improve virtual machine performance. You can set most of the CPU parameters when you create virtual machines or after the guest operating system is installed. Some actions require that you power off the virtual machine before you change the settings.

VMware uses the following terminology. Understanding these terms can help you plan your strategy for CPU resource allocation.

CPU	The CPU, or processor, is the component of a computer system that performs the tasks required for computer applications to run. The CPU is the primary element that performs the computer functions. CPUs contain cores.
CPU Socket	A CPU socket is a physical connector on a computer motherboard that connects to a single physical CPU. Some motherboards have multiple sockets and can connect multiple multicore processors (CPUs).
Core	A core contains a unit containing an L1 cache and functional units needed to run applications. Cores can independently run applications or threads. One or more cores can exist on a single CPU.
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 the 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)	Virtual SMP or vSphere Virtual Symmetric Multiprocessing is a feature that enables a single virtual machine to have multiple processors.

Virtual CPU Limitations

The maximum number of virtual CPUs that you can assign to a virtual machine is 128. The number of virtual CPUs depends on the number of logical CPUs on the host, and the type of guest operating system that is installed on the virtual machine.

Be aware of the following limitations:

- A virtual machine cannot have more virtual CPUs than the number of logical cores on the host. The number of logical cores is equal to the number of physical cores if hyperthreading is disabled or two times that number if hyperthreading is enabled.
- Not every guest operating system supports Virtual SMP, and guest operating systems that support this functionality might support fewer processors than are available on the host. For information about Virtual SMP support, see the *VMware Compatibility Guide* at <http://www.vmware.com/resources/compatibility>.

- Hyperthreaded hosts might affect virtual machine performance, depending on the workload. The best practice is to test your workload to determine whether to enable or disable hyperthreading on your hosts.

Configuring Multicore Virtual CPUs

VMware multicore virtual CPU support lets you control the number of cores per virtual socket in a virtual machine. This capability lets operating systems with socket restrictions use more of the host CPU's cores, which increases overall performance.

Important When you configure your virtual machine for multicore virtual CPU settings, you must ensure that your configuration complies with the requirements of the guest operating system EULA.

Using multicore virtual CPUs can be useful when you run operating systems or applications that can take advantage of only a limited number of CPU sockets.

You can configure a virtual machine that runs on an ESXi host 6.0 and later to have up to 128 virtual CPUs. A virtual machine cannot have more virtual CPUs than the actual number of logical CPUs on the host. The number of logical CPUs means the number of physical processor cores or two times that number if hyperthreading is enabled. For example, if a host has 128 logical CPUs, you can configure the virtual machine for 128 virtual CPUs.

You configure how the virtual CPUs are assigned in terms of cores and cores per socket. Determine how many CPU cores you want in the virtual machine, then select the number of cores you want in each socket, depending on whether you want a single core CPU, dual-core CPU, tri-core CPU, and so on. Your selection determines the number of sockets that the virtual machine has.

For more information about multicore CPUs, see the *vSphere Resource Management* documentation.

Change CPU Hot Plug Settings

By default, you cannot add CPU resources to a virtual machine when the virtual machine is turned on. The CPU hot plug option lets you add CPU resources to a running virtual machine.

The following conditions apply:

- For best results, use virtual machines that are compatible with ESXi 5.0 or later.
- Hot-adding multicore virtual CPUs is supported only with virtual machines that are compatible with ESXi 5.0 or later.
- Not all guest operating systems support CPU hot add. You can disable these settings if the guest is not supported.
- To use the CPU hot plug feature with virtual machines that are compatible with ESXi 4.x and later, set the **Number of cores per socket** to 1.
- Adding CPU resources to a running virtual machine with CPU hot plug enabled disconnects and reconnects all USB passthrough devices that are connected to that virtual machine.

Prerequisites

Required privileges: **Virtual Machine.Configuration.Settings**

Verify that the virtual machine is running and is configured as follows.

- Latest version of VMware Tools installed.
- Guest operating system that supports CPU hot plug.
- Virtual machine compatibility is ESX/ESXi 4.x or later.
- Virtual machine is turned off.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, expand **CPU**, and select **Enable CPU Hot Add**.
- 3 Click **OK**.

You can now add CPUs even if the virtual machine is turned on.

Change the Number of Virtual CPUs

You can configure a virtual machine that runs on an ESXi host 6.5 and later to have up to 128 CPUs. You can change the number of virtual CPUs while your virtual machine is powered off. If virtual CPU hotplug is enabled, you can increase the number of virtual CPUs while the virtual machine is running.

Virtual CPU hot add is supported for virtual machines with multicore CPU support and ESXi 5.0 and later compatibility. When the virtual machine is turned on, and CPU hot add is enabled, you can hot add virtual CPUs to the running virtual machine. You can add only multiples of the number of cores per socket.

Important When you configure your virtual machine for multicore virtual CPU settings, you must ensure that your configuration complies with the requirements of the guest operating system EULA.

Prerequisites

- If CPU hot add is not enabled, turn off the virtual machine before adding virtual CPUs.
- To hot add multicore CPUs, verify that the virtual machine is compatible with ESXi 5.0 and later.
- Verify that you have the **Virtual Machine.Configuration.Change CPU Count** privilege.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, expand **CPU**.
- 3 From the **CPU** drop-down menu, select the number of cores.
- 4 From the **Cores Per Socket** drop-down menu, select the number of cores per socket and click **OK**.

Allocate CPU Resources

To manage workload demands, you can change the amount of CPU resources allocated to a virtual machine by using the shares, reservations, and limits settings.

A virtual machine has the following user-defined settings that affect its CPU resource allocation.

Limit	Places a limit on the consumption of CPU time for a virtual machine. This value is expressed in MHz or GHz.
Reservation	Specifies the guaranteed minimum allocation for a virtual machine. The reservation is expressed in MHz or GHz.
Shares	Each virtual machine is granted a number of CPU shares. The more shares a virtual machine has, the more often it gets a time slice of a CPU when there is no CPU idle time. Shares represent a relative metric for allocating CPU capacity.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, expand **CPU**, and allocate the CPU capacity for the virtual machine.

Option	Description
Reservation	Guaranteed CPU allocation for this virtual machine.
Limit	Upper limit for this virtual machine's CPU allocation. Select Unlimited to specify no upper limit.
Shares	CPU shares for this virtual machine in relation to the parent's total. Sibling virtual machines share resources according to their relative share values bounded by the reservation and limit. Select Low , Normal , or High , which specify share values respectively in a 1:2:4 ratio. Select Custom to give each virtual machine a specific number of shares, which express a proportional weight.

- 3 Click **OK**.

Change CPU Identification Mask Settings

CPU identification (CPU ID) masks control the CPU features visible to the virtual machine's guest operating system. Masking or hiding CPU features can make a virtual machine widely available to ESXi hosts for migration. vCenter Server compares the CPU features available to a virtual machine with the CPU features of the destination host to determine whether to allow or disallow migration with vMotion.

For example, masking the AMD No eXecute (NX) and the Intel eXecute Disable (XD) bits prevents the virtual machine from using these features, but provides compatibility that allows you to migrate virtual machines to ESXi hosts that do not include this capability. When the NX/XD bit is visible to the guest operating system, the virtual machine can use this feature, but you can migrate the virtual machine only to hosts on which the feature is enabled.

Caution Changing the CPU compatibility masks can result in an unsupported configuration. Do not manually change the CPU compatibility masks unless instructed to do so by VMware Support or a VMware Knowledge base article.

Prerequisites

Turn off the virtual machine.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, expand **CPU** and select an NX/XD option from the **CPUID Mask** drop-down menu.

Option	Description
Hide the NX/XD flag from guest	Increases vMotion compatibility. Hiding the NX/XD flag increases vMotion compatibility between hosts, but might disable certain CPU security features.
Expose the NX/XD flag to guest	Keeps all CPU security features enabled.
Keep current Advanced setting values for the NX/XD flag	Uses the NX/XD flag settings specified in the CPU Identification Mask dialog box. Enabled only when current settings specify something other than what is specified in the other NX/XD flag options, for example, if the NX/XD flag bit setting varies with processor brand.

- 3 Click **OK**.

Expose VMware Hardware Assisted Virtualization

You can expose full CPU virtualization to the guest operating system so that applications that require hardware virtualization can run on virtual machines without binary translation or paravirtualization.

Prerequisites

- Verify that the virtual machine compatibility is ESXi 5.1 and later.
- Intel Nehalem Generation (Xeon Core i7) or later processors or AMD Opteron Generation 3 (Greyhound) or later processors.
- Verify that Intel VT-x or AMD-V is enabled in the BIOS so that hardware assisted virtualization is possible.
- Required Privileges: **Virtual machine.Configuration.Settings** set on the vCenter Server system.

Procedure

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

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

Enable Virtual CPU Performance Counters

You can use performance tuning tools in the guest operating system for software profiling. You can identify and improve processor performance problems. This capability is useful for software developers who optimize or debug software that runs in the virtual machine.

The following conditions apply:

- If virtual CPU performance counters are enabled, you can migrate the virtual machine only to hosts that have compatible CPU performance counters.
- If an ESXi host's BIOS uses a performance counter or if Fault Tolerance is enabled, some virtual performance counters might not be available for the virtual machine to use.

Note If a virtual machine resides on an ESXi host in an EVC cluster, CPU counters are not supported for virtual machine creation or editing. You must disable CPU performance counters.

For a list of virtualized Model-Specific Registers (MSRs), see the VMware knowledge base article at <http://kb.vmware.com/kb/2030221>.

Prerequisites

- Verify that the virtual machine compatibility is ESXi 5.1 and later.
- Verify that the virtual machine is turned off.
- Verify that Intel Nehalem Generation (Xeon Core i7) or later processors or AMD Opteron Generation 3 ("Greyhound") or later processors are installed.
- Verify that Intel VT-x or AMD-V is enabled in the BIOS so that hardware-assisted virtualization is possible.
- Required Privileges: **Virtual machine.Configuration.Settings** is set on the vCenter Server system.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, expand **CPU** and select the **Enable virtualized CPU performance counters** check-box.
- 3 Click **OK**.

Configure Processor Scheduling Affinity

The **Scheduling Affinity** option gives you detailed control over how virtual machine CPUs are distributed across the host's physical cores. The option supports hyperthreading if hyperthreading is enabled. ESXi generally manages processor scheduling well, even when hyperthreading is enabled. These settings are useful only for fine-tuning critical virtual machines.

Using CPU affinity, you can assign a virtual machine to a specific processor. This assignment allows you to restrict the assignment of virtual machines to a specific available processor in multiprocessor systems.

This setting does not appear for virtual machines in a DRS cluster or when the host has only one processor core and no hyperthreading.

For potential issues with CPU affinity, see the *vSphere Resource Management* documentation.

Prerequisites

- Verify that the virtual machine is turned off.
- Verify that the virtual machine does not reside in a DRS cluster.
- Verify that the host has more than one physical processor core.
- Privileges: **Virtual machine.Configuration.Change resource**

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, expand **CPU**, and enter a comma-separated list of hyphenated processor ranges in the **Scheduling Affinity** text box.

For example, "0,4-7" would indicate affinity with CPUs 0,4,5,6, and 7. Selecting all processors is identical to selecting no affinity. You must provide at least as many processor affinities as you have virtual CPUs.

- 3 Click **OK**.

Change CPU/MMU Virtualization Settings

ESXi can determine whether a virtual machine needs hardware support for virtualization. ESXi makes this determination based on the processor type and the virtual machine. Overriding the automatic selection can provide better performance for some use cases.

You can use software MMU when your virtual machine runs heavy workloads, such as Translation Lookaside Buffers (TLBs) intensive workloads that have significant impact on the overall system performance. However, software MMU has a higher overhead memory requirement than hardware MMU. So, to support software MMU, the maximum overhead supported for virtual machine limit in the VMkernel needs to be increased. You can configure your virtual machine with up to 128 CPUs if your virtual machine has ESXi 6.0 and later compatibility (hardware version 11).

Important Modern x86 processors can fully support virtualized workloads without software assistance. So, the CPU/MMU Virtualization setting has been deprecated in ESXi 6.7.

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.

Note To take advantage of all features that virtual hardware version 13 provides, use the default hardware MMU setting.

You cannot change the CPU/MMU Virtualization setting of virtual machines with ESXi 6.7 and later compatibility.

- 3 Click **OK**.

Virtual Memory Configuration

You can add, change, or configure virtual machine memory resources or options to enhance virtual machine performance. You can set most of the memory parameters during virtual machine creation or after the guest operating system is installed. Some actions require that you power off the virtual machine before changing the settings.

The memory resource settings for a virtual machine determine how much of the host's memory is allocated to the virtual machine. The virtual hardware memory size determines how much memory is available to applications that run in the virtual machine. A virtual machine cannot benefit from more memory resources than its configured virtual hardware memory size. ESXi hosts limit the memory resource use to the maximum amount useful for the virtual machine, so that you can accept the default of Unlimited memory resources.

Change the Memory Configuration

You can reconfigure the amount of memory allocated to a virtual machine to enhance performance.

Minimum memory size is 4MB for virtual machines that use BIOS firmware. Virtual machines that use EFI firmware require at least 96MB of RAM or they cannot power on.

Maximum memory size for a virtual machine depends on the host's physical memory and the virtual machine's compatibility setting.

If the virtual machine memory is greater than the host memory size, swapping occurs, which can have a severe effect on virtual machine performance. The maximum for best performance represents the threshold above which the host's physical memory is insufficient to run the virtual machine at full speed. This value fluctuates as conditions on the host change, for example, as virtual machines are powered on or off.

The memory size must be a multiple of 4MB.

Table 5-3. Maximum Virtual Machine Memory

Introduced in Host Version	Virtual Machine Compatibility	Maximum Memory Size
ESXi 6.7	ESXi 6.7 and later	6128GB
ESXi 6.5	ESXi 6.5 and later	6128GB
ESXi 6.0	ESXi 6.0 and later	4080GB
ESXi 5.5	ESXi 5.5 and later	1011GB
ESXi 5.1	ESXi 5.1 and later	1011GB
ESXi 5.0	ESXi 5.0 and later	1011GB
ESX/ESXi 4.x	ESX/ESXi 4.0 and later	255GB
ESX/ESXi 3.x	ESX/ESXi 3.5 and later	65532MB

The ESXi host version indicates when support began for the increased memory size. For example, the memory size of a virtual machine with ESX/ESXi 3.5 and later compatibility running on ESXi 5.0 is restricted to 65,532MB.

Prerequisites

Verify that you have the **Virtual machine.Configuration.Memory** privilege on the virtual machine.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, expand **Memory** and change the memory configuration.
 - a In the **Memory** 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.
 - b Select whether the memory is specified in MB or GB.
- 3 Click **OK**.

Allocate Memory Resources

You can change the amount of memory resources allocated to a virtual machine by using the shares, reservations, and limits settings. The host determines the appropriate amount of physical RAM to allocate to virtual machines based on these settings. You can assign a high or low shares value to a virtual machine, depending on its load and status.

The following user-defined settings affect the memory resource allocation of a virtual machine.

Limit	Places a limit on the consumption of memory for a virtual machine. This value is expressed in megabytes.
Reservation	Specifies the guaranteed minimum allocation for a virtual machine. The reservation is expressed in megabytes. If the reservation cannot be met, the virtual machine will not turn on.
Shares	Each virtual machine is granted a number of memory shares. The more shares a virtual machine has, the greater share of host memory it receives. Shares represent a relative metric for allocating memory capacity. For more information about share values, see the <i>vSphere Resource Management</i> documentation.

You cannot assign a reservation to a virtual machine that is larger than its configured memory. If you give a virtual machine a large reservation and reduce its configured memory size, the reservation is reduced to match the new configured memory size.

Prerequisites

Verify that the virtual machine is turned off.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, expand Memory, and allocate the memory capacity for the virtual machine.

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

- 3 Click **OK**.

Change Memory Hot Add Settings

Memory hot add lets you add memory resources for a virtual machine while that virtual machine is turned on.

Enabling memory hot add produces some memory overhead on the ESXi host for the virtual machine.

Prerequisites

- Power off the virtual machine.
- Verify that the virtual machine has a guest operating system that supports memory hot add functionality.

- Verify that the virtual machine compatibility is ESXi 4.x and later.
- Verify 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**.

Managing Persistent Memory

ESXi 6.7 provides support for the latest computer memory technology, which is called non-volatile memory (NVM) or persistent memory (PMem). PMem combines the high data transfer rate of volatile computer memory with the persistence and resiliency of traditional storage. PMem devices have low access latency and can retain stored data through reboots or power outages.

Modes of Consumption of the Persistent Memory Resources of the Host

When you add a physical PMem device to a host, ESXi detects the PMem resource and exposes it as a host-local PMem datastore to the virtual machines that run on the host. Depending on the guest OS, virtual machines can have direct access to the PMem resources or access and consume them through a regular SCSI device.

Each host can have only one local PMem datastore that pools and represents all PMem resources of the host.

Persistent memory combines the properties of both memory and storage. So, virtual machines can consume the PMem resources of the ESXi host as memory (through virtual NVDIMM devices) or as storage (through virtual PMem hard disks).

The host-local PMem datastore stores all direct-accessed NVDIMM devices and virtual PMem hard disks.

Virtual PMem (vPMem)

In this mode, if the guest operating system is PMem-aware, the virtual machine can have direct access to the physical PMem resources of the host and use them as standard, byte-addressable memory.

Virtual machines use virtual non-volatile dual in-line memory modules (NVDIMMs) for direct access to PMem. The NVDIMM is a memory device that sits on an ordinary memory channel, but contains non-volatile memory. In vSphere 6.7, the virtual NVDIMM is a new type of device that represents the physical PMem regions of the host. A single virtual machine can have up to 64 virtual NVDIMM devices. Each NVDIMM device is stored on the host-local PMem datastore.

Note To add an NVDIMM device to a virtual machine, the virtual machine must be of hardware version 14 and the guest OS must support persistent memory. If the guest OS is not PMem-aware, you can still use PMem, but you cannot add an NVDIMM device to the virtual machine.

Virtual PMem Disks (vPMemDisk)

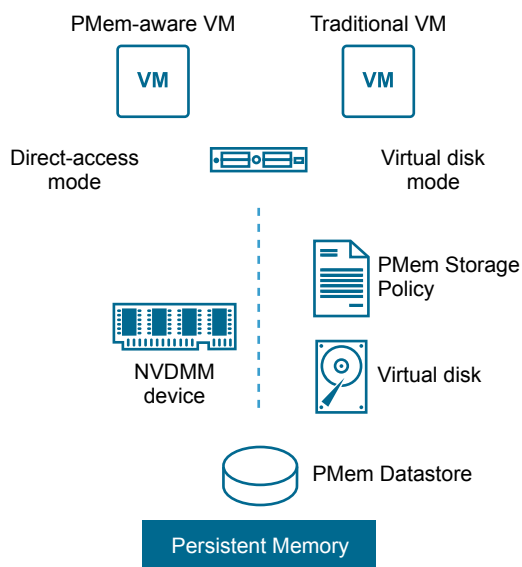
In this mode, the virtual machine does not have direct access to the PMem resources of the host.

You must add a virtual PMem hard disk to the virtual machine. A virtual PMem hard disk is a traditional SCSI disk to which the PMem Storage Policy is applied. The policy automatically places the hard disk on the host-local PMem datastore.

In this mode of usage, there are no requirements for the hardware version of the virtual machine and the guest OS.

Note If the guest OS is not PMem-aware, virtual machines can use PMem only through vPMemDisks.

The following graphic illustrates how the persistent memory components interact.



For information about how to configure and manage VMs with NVDIMMs or virtual persistent memory disks, see the *vSphere Resource Management* documentation.

Add an NVDIMM Device to a Virtual Machine

Add a virtual NVDIMM device to a virtual machine to enable it to use non-volatile, or persistent, computer memory. Non-volatile memory (NVM), or persistent memory (PMem), combines the high data transfer rates of the volatile memory with the persistence and resiliency of traditional storage. The virtual NVDIMM device is a virtual NVM device that can retain stored data through reboots or power source failures.

Virtual machines consume the PMem resource of the host in two ways, through a virtual non-volatile dual in-line memory module (NVDIMM) or through a virtual persistent memory disk. When you add an NVDIMM module to a virtual machine, the virtual machine gains direct access to a PMem region of computer memory.

For more information, see the *vSphere Resource Management* guide.

Prerequisites

- Verify that the guest OS of the virtual machine supports PMem.

- Verify that the virtual hardware version is 14 or higher.
- Verify that you have the **Datastore.Allocate space** privilege on the virtual machine.
- Verify that the host or the cluster on which the virtual machine resides has available PMem resources.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, add a new NVDIMM device. click **Add a new device** and select **NVDIMM** from the drop-down menu.

Client	Steps
vSphere Client	Click the Add New Device button and select NVDIMM from the drop-down menu.
vSphere Web Client	<ol style="list-style-type: none"> a Select NVDIMM from the New device drop-down menu at the bottom of the wizard. b Click Add.

The NVDIMM device appears in the Virtual Hardware devices list together with the virtual NVDIMM controller. Each virtual machine can have a maximum of one virtual NVDIMM controller and each NVDIMM controller can have up to 64 virtual NVDIMM devices.

Note You can change the size of the NVDIMM device at a later time. The virtual machine must be powered off.

- 3 In the **New NVDIMM** text box, enter the size of the NVDIMM device and select the units from the drop-down menu.

Note If the virtual machine uses PMem storage, the hard disks that are stored on a PMem datastore and the NVDIMM devices that you add to the virtual machine all share the same PMem resources. So, you must adjust the size of the newly added devices in accordance with the amount of the PMem available to the host. If any part of the configuration requires attention, the wizard alerts you.

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 appears as a single hard disk to the guest operating system. The virtual disk 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 virtual machine data directly on a SAN LUN instead of using a virtual disk file. This option is useful if in your virtual machines you run applications that must detect the physical characteristics of the storage device. Mapping a SAN LUN also 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 its data only 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, you can specify a provisioning policy for the virtual disk file. The operations include creating a virtual disk, cloning a virtual machine to a template, or migrating a virtual machine.

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 later 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.

Large Capacity Virtual Disk Conditions and Limitations

Virtual machines with large capacity virtual hard disks, or disks greater than 2 TB, must meet resource and configuration requirements for optimal virtual machine performance.

The maximum value for large capacity hard disks is 62 TB. 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 2 TB to ESXi 6.0 or later hosts or to clusters that have such hosts available.
- The datastore format must be one of the following:
 - VMFS5 or later
 - An NFS volume on a Network Attached Storage (NAS) server
 - vSAN
- Virtual Flash Read Cache supports a maximum hard disk size of 16 TB.
- Fault Tolerance is not supported.
- BusLogic Parallel controllers are not supported.

Change the Virtual Disk Configuration

If you run out of disk space, you can increase the size of the disk. You can change the virtual device node and the persistence mode for virtual disk configuration for a virtual machine.

Prerequisites

Verify that you have the following privileges:

- **Virtual machine.Configuration.Modify device settings** on the virtual machine.
- **Virtual machine.Configuration.Extend virtual disk** on the virtual machine.
- **Datastore.Allocate space** on the datastore.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, expand **Hard disk** to view or change the disk settings, and click **OK**.

Option	Description
Maximum Size	Shows the maximum size of this hard disk on this VM. Note 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.
VM storage policy	Select one of the available storage policies. See the <i>vSphere Storage</i> documentation for details. Note You cannot change the VM storage policy of an existing PMem hard disk. You also cannot change the storage policy of an existing non-PMem disk to Host-local PMem Default Storage Policy.
Type	Shows the storage type. You cannot change this setting for an existing hard disk. You choose the storage type of a hard disk when you add the hard disk to the virtual machine. For more information about storage types and available disk formats, see the <i>vSphere Storage</i> documentation.
Sharing	Specifies sharing information.

Option	Description
Disk File	Lists disk files on the datastore.
Shares	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.
Limit - IOPs	Allows you to customize IOPs. This value is the upper limit of I/O operations per second allocated to the virtual disk.
Virtual flash read cache	Determines the block size and cache size reservation. See Configure Flash Read Cache for a Virtual Machine for details.
Disk mode	Disk mode determines how a virtual disk is affected by snapshots. You have the following options: <ul style="list-style-type: none"> ■ Dependent: Dependent disks are included in snapshots. ■ Independent - Persistent: Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to disk. ■ Independent - Nonpersistent: Changes to disks in nonpersistent mode are discarded when you turn off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you turn off or reset the virtual machine.
Virtual Device Node	Displays the virtual device node.

Use Disk Shares to Prioritize Virtual Machines

You can change the disk resources for a virtual machine. If multiple virtual machines access the same VMFS datastore and the same logical unit number (LUN), use disk shares to prioritize the disk accesses from the virtual machines. Disk shares distinguish high-priority from low-priority virtual machines.

You can allocate the host disk's I/O bandwidth to the virtual hard disks of a virtual machine. Disk I/O is a host-centric resource so you cannot pool it across a cluster.

Shares is a value that represents the relative metric for controlling disk bandwidth to all virtual machines. The values are compared to the sum of all shares of all virtual machines on the server.

Disk shares are relevant only within a given host. The shares assigned to virtual machines on one host have no effect on virtual machines on other hosts.

You can select an IOP limit, which sets an upper bound for storage resources that are allocated to a virtual machine. IOPs are the number of I/O operations per second.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, expand **Hard disk** to view the disk options.
- 3 From the **Shares** drop-down menu, select a value for the shares to allocate to the virtual machine. Alternatively, you can select **Custom** and you can enter a number of shares in the text box manually.
- 4 In the **Limit - IOPs** box, enter the upper limit of storage resources to allocate to the virtual machine, or select **Unlimited**.

- 5 Click **OK**.

Configure Flash Read Cache for a Virtual Machine

You can configure a Flash Read Cache for your virtual machine. When you enable Flash Read Cache, you can specify the 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 4 KB and 1024 KB. If a guest operating system writes a single 512-byte disk block, the surrounding cache block size bytes are cached. Do not confuse the cache block size with the 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 1 MB, then the minimum cache size is 256 MB. If the cache block size is 4 K, then the minimum cache size is 1 MB.

For more information about sizing guidelines, search for the *Performance of vSphere Flash Read Cache in VMware vSphere* white paper on the VMware website.

Prerequisites

Set up a virtual flash resource on your client computer.

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 menu items.
- 3 Enter a value in the **Virtual Flash Read Cache** text box.
- 4 (Optional) Select a block size and a cache size reservation.

Client	Steps
vSphere Client	You cannot specify block size and cache size reservation in the vSphere Client.
vSphere Web Client	<ol style="list-style-type: none"> a Next to the Virtual flash read cache text box, click Advanced. The Virtual Flash Read Cache Settings dialog box opens. b Click Enable virtual Flash Read Cache. c In the Reservation text box, enter the cache size reservation, and select the units from the drop-down menu. d From the Block Size drop-down menu, select the block size. e Click OK.

- 5 Click **OK**.

Determine the Virtual Disk Format and Convert a Virtual Disk from the Thin Provision Format to a Thick Provision Format

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.

For more information about thin provisioning and available disk formats, see the *vSphere Storage* documentation.

Procedure

- 1 Verify that the disk format of a virtual hard disk is Thin Provision.
 - a Right-click a virtual machine and click **Edit Settings**.
 - b On the **Virtual Hardware** tab, expand **Hard disk** and check the Type field.
 - c Click **Cancel** to exit the wizard.
- 2 Click the **Datastores** tab, and click a datastore from the list to open the datastore management panel.

The datastore that stores the virtual machine files is listed.
- 3 Click the **Files** tab, and open the virtual machine folder.
- 4 Browse to the virtual disk file that you want to convert.

The file has the .vmdk extension.
- 5 Convert the virtual disk to a thick provision format.

Client	Steps
vSphere Client	Click the virtual disk file and click the Inflate icon.
vSphere Web Client	Right-click the virtual disk file and select Inflate .

The inflated virtual disk occupies the entire datastore space originally provisioned to it.

Add a Hard Disk to a Virtual Machine

When you create a virtual machine, a default virtual hard disk is added. You can add another hard disk if you run out of disk space, if you want to add a boot disk, or for other file management purposes. When you add a hard disk to a virtual machine, you can create a virtual disk, add an existing virtual disk, or add a mapped SAN LUN.

You can add a virtual hard disk to a virtual machine before or after you add a SCSI or SATA storage controller. The new disk is assigned to the first available virtual device node on the default controller, for example (0:1). Only device nodes for the default controller are available unless you add additional controllers.

The following ways to add disks can help you plan your disk configuration. These approaches show how you can optimize controller and virtual device nodes for different disks. For storage controller limitations, maximums, and virtual device node behavior, see [SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility](#).

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](#)

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](#)

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](#)

You can use a raw device mapping (RDM) to store virtual machine data directly on a SAN LUN, instead of storing it in a virtual disk file. You can add an RDM disk to an existing virtual machine, or you can add the disk when you customize the virtual machine hardware during the virtual machine creation process.

Add a New Hard Disk to a Virtual Machine

You can add a virtual hard disk to an existing virtual machine, or you can add a hard disk when you customize the virtual machine hardware during the virtual machine creation process. For example, you might need to provide additional disk space for an existing virtual machine with a heavy work load. During virtual machine creation, you might want to add a hard disk that is preconfigured as a boot disk.

During virtual machine creation, a hard disk and a SCSI or SATA controller are added to the virtual machine by default, based on the guest operating system that you select. If this disk does not meet your needs, you can remove it and add a new hard disk at the end of the creation process.

If you add multiple hard disks to a virtual machine, you can assign them to several controllers to improve performance. For controller and bus node behavior, see [SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility](#).

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 On the **Virtual Hardware** tab, add a new hard disk to the virtual machine.

Client	Steps
vSphere Client	Click the Add New Device button and select Hard Disk from the drop-down menu.
vSphere Web Client	<ol style="list-style-type: none"> a Select New Hard Disk from the New device drop-down menu at the bottom of the wizard. b Click Add.

The hard disk appears in the Virtual Hardware devices list.

Note If the host where the virtual machine resides has available PMem resources, you can place the new hard drive on the host-local PMem datastore.

- 3 Expand **New hard disk** and customize the settings of the new hard disk.
 - a Enter a size for the hard disk and select the unit from the drop-down menu.
 - b From the **VM storage policy**, select a storage policy or leave the default one.
 - c From the **Location** drop-down menu, select the datastore location where you want to store virtual machine files.

- d From the **Disk Provisioning** drop-down menu, select the format for the hard disk.

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

- e From the **Shares** drop-down menu, select a value for the shares to allocate to the virtual disk. Alternatively, you can select **Custom** and enter a value in the text box.

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.

- f From the **Limit - IOPs** drop-down menu, customize 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.

- g From the **Disk Mode** drop-down menu, select a disk mode.

Option	Description
Dependent	Dependent disks are included in snapshots.
Independent - Persistent	Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk.
Independent - Nonpersistent	Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset.

- h From the **Virtual Device Node**, select a virtual device node or leave the default one.

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.

Add an Existing Hard Disk to a Virtual Machine

You can add an existing virtual hard disk to a virtual machine when you customize the virtual machine hardware during the virtual machine creation process or after the virtual machine is created. For example, you might want to add an existing hard disk that is preconfigured as a boot disk.

During virtual machine creation, a hard disk and a SCSI or SATA controller are added to the virtual machine by default, based on the guest operating system that you select. If this disk does not meet your needs, you can remove it and add an existing hard disk at the end of the creation process.

Prerequisites

- Make sure that you are familiar with controller and virtual device node behavior for different virtual hard disk configurations. See [Add a Hard Disk to a Virtual Machine](#).
- 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, add an existing hard disk.

Client	Steps
vSphere Client	Click the Add New Device button and select Existing Hard Disk from the drop-down menu.
vSphere Web Client	<ol style="list-style-type: none"> a Select Existing Hard Disk from the New device drop-down menu at the bottom of the wizard. b Click Add.

The **Select File** dialog box opens.

- 4 In the **Select File**, expand a datastore, select a virtual machine folder, and select the disk to add. Click **OK**.

The disk file appears in the **Contents** column. The **File Type** drop-down menu shows the compatibility file types for this disk.

- 5 (Optional) Expand **New Hard disk** and make further customizations for the hard disk. .
- 6 Click **OK**.

Add an RDM Disk to a Virtual Machine

You can use a raw device mapping (RDM) to store virtual machine data directly on a SAN LUN, instead of storing it in a virtual disk file. You can add an RDM disk to an existing virtual machine, or you can add the disk when you customize the virtual machine hardware during the virtual machine creation process.

When you give a virtual machine direct access to an RDM disk, you create a mapping file that resides on a VMFS datastore and points to the LUN. Although the mapping file has the same `.vmdk` extension as a regular virtual disk file, the mapping file contains only mapping information. The virtual disk data is stored directly on the LUN.

During virtual machine creation, a hard disk and a SCSI or SATA controller are added to the virtual machine by default, based on the guest operating system that you select. If this disk does not meet your needs, you can remove it and add an RDM disk at the end of the creation process.

Prerequisites

- Ensure that you are familiar with SCSI controller and virtual device node behavior for different virtual hard disk configurations. See [Add a Hard Disk to a Virtual Machine](#).
- 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 On the **Virtual Hardware** tab, add a new RDM disk. select **RDM Disk** from the **New device** drop-down menu and click **Add**.

Client	Steps
vSphere Client	Click the Add New Device button and select RDM Disk from the drop-down menu.
vSphere Web Client	<ol style="list-style-type: none"> a Select RDM Disk from the New device drop-down menu at the bottom of the wizard. b Click Add.

The **Select Target LUN** dialog box opens.

- 3 In the **Select Target LUN** dialog box, select the target LUN for the raw device mapping and click **OK**.
The disk appears in the virtual device list.
- 4 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.

5 Select a compatibility mode.

Option	Description
Physical	Allows the guest operating system to access the hardware directly. Physical compatibility is useful if you are using SAN-aware applications on the virtual machine. However, a virtual machine with a physical compatibility RDM cannot be cloned, made into a template, or migrated if the migration involves copying the disk.
Virtual	Allows the RDM to behave as if it were a virtual disk, so that you can use such features as taking snapshots, cloning, and so on. When you clone the disk or make a template out of it, the contents of the LUN are copied into a .vmdk virtual disk file. When you migrate a virtual compatibility mode RDM, you can migrate the mapping file or copy the contents of the LUN into a virtual disk.

6 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.

7 (Optional) If you selected virtual compatibility mode, select a disk mode to change the way that disks are affected by snapshots.

Disk modes are not available for RDM disks using physical compatibility mode.

Option	Description
Dependent	Dependent disks are included in snapshots.
Independent - Persistent	Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk.
Independent - Nonpersistent	Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset.

8 Click **OK**.

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, and NVMe 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 sometimes, 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.

In high performance storage environments you can benefit from using VMware Paravirtual SCSI controllers. The VMware Paravirtual SCSI controller ensures greater throughput and lower CPU use, which boosts performance as compared to the other SCSI controller options. For platform support for VMware Paravirtual SCSI controllers, see the *VMware Compatibility Guide* at <http://www.vmware.com/resources/compatibility>.

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.

Alternatively, each virtual machine can have a maximum of four NVMe controllers. You can reassign an existing or new hard disk or device to that controller. For example, you can assign the hard disk to (x:z), where x is NVMe controller and z is a virtual device node. x has values from 0 to 3, and z has values from 0 to 14.

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.
- Virtual machines with VMware Paravirtual SCSI controllers cannot be part of an MSCS cluster.

- AHCI SATA is available only for virtual machines with ESXi 5.5 and later compatibility.
- NVMe is available only for virtual machines with ESXi 6.5 and later compatibility.
- BusLogic Parallel controllers do not support virtual machines with disks larger than 2TB.
- Disks on VMware Paravirtual SCSI controllers might not experience optimal performance gains if they have snapshots or if the host's memory is overcommitted.

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	NVME
BusLogic Parallel	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LSI Logic	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LSI Logic SAS	Requires BIOS setup	Requires BIOS setup	Usually Works	Usually Works	Requires BIOS setup	Yes	Usually Works
VMware Paravirtual SCSI	Requires BIOS setup	Requires BIOS setup	Usually Works	Usually Works	Requires BIOS setup	Yes	Usually Works
AHCI SATA	Requires BIOS setup	Requires BIOS setup	Yes	Yes	Yes	Yes	Yes
IDE	Yes	Yes	Yes	Yes	Yes	N/A	Yes
NVME	Requires BIOS setup	Requires BIOS setup	Usually Works	Usually Works	Requires BIOS setup	Yes	Usually Works

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 On the **Virtual Hardware** tab, add a SATA controller.

Client	Steps
vSphere Client	Click the Add New Device button and select SATA Controller from the drop-down menu.
vSphere Web Client	<ol style="list-style-type: none"> a Select SATA Controller from the New device drop-down menu at the bottom of the wizard. b Click Add.

The controller appears in the Virtual Hardware devices list.

- 3 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 to a Virtual Machine

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.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, add a new SCSI controller.

Client	Steps
vSphere Client	Click the Add New Device button and select SCSI Controller from the drop-down menu.
vSphere Web Client	<ol style="list-style-type: none"> a Select SCSI Controller from the New device drop-down menu at the bottom of the wizard. b Click Add.

The controller appears in the Virtual Hardware devices list.

- 3 From the **Change Type** drop-down menu, select the 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 On the **Virtual Hardware** tab, expand **New SCSI Controller**, and select the type of sharing in the **SCSI Bus Sharing** drop-down menu.

Option	Description
None	Virtual disks cannot be shared by other virtual machines.
Virtual	Virtual disks can be shared by virtual machines on the same ESXi host. Select Thick provision eager zeroed when you create the disk.
Physical	Virtual disks can be shared by virtual machines on any ESXi host. Select Thick provision eager zeroed when you create the disk.

- 5 Click **OK**.

What to do next

You can now add a hard disk or other SCSI device to the virtual machine and assign it to the new SCSI controller.

Add a Paravirtualized SCSI Adapter

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 the VMware Paravirtual SCSI controller type.
- 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, add a paravirtualized SCSI adapter.

Client	Steps
vSphere Client	<ol style="list-style-type: none"> a Click the Add New Device button and select SCSI Controller from the drop-down menu. b Expand New SCSI controller and from the Change Type drop-down menu, select VMware Paravirtual.
vSphere Web Client	<ol style="list-style-type: none"> a Select SCSI Controller from the New device drop-down menu at the bottom of the wizard. b Click Add. c Expand New SCSI controller and from the Change Type drop-down menu, select VMware Paravirtual. d Click the Change Type button.

The controller appears at the bottom of the Virtual Hardware device list.

- 3 Click **OK**.

Add an NVMe Controller

If a virtual machine has multiple hard disks, you can add up to four virtual NVMe controllers to which to assign the disks. Using a NVMe controller significantly reduces the software overhead for processing guest OS I/O, as compared to AHCI SATA or SCSI controllers.

NVMe controllers perform best with virtual disks on an all-flash disk array, local NVMe SSD, and PMem storage.

Prerequisites

- Verify that the virtual machine has a guest operating system that supports NVMe.
- Verify that the virtual machine compatibility is ESXi 6.5 or later.
- Verify that you are familiar with storage controller behaviour and limitations. See [SCSI and SATA Storage Controller Conditions, Limitations, and Compatibility](#).
- Verify that you have the **Virtual machine.Configuration.Add new disk** 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, add an NVMe controller.

Client	Steps
vSphere Client	Click the Add New Device button and select NVMe Controller from the drop-down menu.
vSphere Web Client	<ol style="list-style-type: none"> a Select NVMe Controller from the New device drop-down menu at the bottom of the wizard. b Click Add.

The controller appears in the Virtual Hardware devices list.

- 3 Click **OK**.

What to do next

You can add a hard disk to the virtual machine and assign it to the NVMe controller.

Change the SCSI Controller Configuration

You can specify the SCSI controller type and you can set the type of SCSI bus sharing for a virtual machine.

The choice of a SCSI controller type 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.

The choice of a SCSI bus sharing option determines whether virtual machines on different hosts can access the same virtual disk.

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.

Client	Steps
vSphere Client	The vSphere 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.
vSphere Web Client	<p>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.</p> <p>You must confirm or discard the change.</p> <ul style="list-style-type: none"> ▪ Click the Change Type button to change the controller type. ▪ Click the Don't change button to cancel the change and keep the original controller type.

Caution Changing the SCSI controller type might result in a virtual machine boot failure.

The vSphere Client displays information about what happens if you change the SCSI controller type. If you select a controller type that is not recommended for the virtual machine's guest operating system, a warning is displayed.

Do not select a BusLogic Parallel controller for virtual machines with disks larger than 2TB. This controller does not support large capacity hard disks.

- 3 On the **Virtual Hardware** tab, expand **SCSI controller**, and select the type of sharing in the **SCSI Bus Sharing** drop-down menu.

Option	Description
None	Virtual disks cannot be shared by other virtual machines.
Virtual	Virtual disks can be shared by virtual machines on the same ESXi host.
Physical	Virtual disks can be shared by virtual machines on any ESXi host.

For virtual or physical bus sharing, select **Thick provision eager zeroed** when you create the disk.

- 4 Click **OK**.

Virtual Machine Network Configuration

vSphere 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 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 Basics

When you configure a virtual machine, you can add network adapters (NICs) and specify the adapter type.

Network Adapter Types

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.

Supported NICs currently differ between an on-premises environment and VMware Cloud on AWS. The following NIC types are supported in an on-premises deployment:

E1000E	Emulated version of the Intel 82574 Gigabit Ethernet NIC. E1000E is the default adapter for Windows 8 and Windows Server 2012.
E1000	Emulated version of the Intel 82545EM Gigabit Ethernet NIC, with drivers available in most newer guest operating systems, including Windows XP and later and Linux versions 2.4.19 and later.
Flexible	Identifies itself as a Vlan adapter when a virtual machine boots, but initializes itself and functions as either a Vlan or a VMXNET adapter, depending on which driver initializes it. With VMware Tools installed, the VMXNET driver changes the Vlan adapter to the higher performance VMXNET adapter.
Vlan	Emulated version of the AMD 79C970 PCnet32 LANCE NIC, an older 10 Mbps NIC with drivers available in 32-bit legacy guest operating systems. A virtual machine configured with this network adapter can use its network immediately.
VMXNET	Optimized for performance in a virtual machine and has no physical counterpart. Because operating system vendors do not provide built-in drivers for this card, you must install VMware Tools to have a driver for the VMXNET network adapter available.
VMXNET 2 (Enhanced)	Based on the VMXNET adapter but provides high-performance features commonly used on modern networks, such as jumbo frames and hardware offloads. VMXNET 2 (Enhanced) is available only for some guest operating systems on ESX/ESXi 3.5 and later.

VMXNET 3

A paravirtualized NIC designed for performance. VMXNET 3 offers all the features available in VMXNET 2 and adds several new features, such as multiqueue support (also known as Receive Side Scaling in Windows), IPv6 offloads, and MSI/MSI-X interrupt delivery. VMXNET 3 is not related to VMXNET or VMXNET 2.

PVRDMA

A paravirtualized NIC that supports remote direct memory access (RDMA) between virtual machines through the OFED verbs API. All virtual machines must have a PVRDMA device and should be connected to a distributed switch. PVRDMA supports VMware vSphere vMotion and snapshot technology. It is available in virtual machines with hardware version 13 and guest operating system Linux kernel 4.6 and later.

For information about assigning an PVRDMA network adapter to a virtual machine, see the *vSphere Networking* documentation.

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 6.0 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>.

Legacy Network Adapters and ESXi Virtual Hardware Versions

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 use a virtual hardware version, 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>.

Network Adapters and Legacy Virtual Machines

Legacy virtual machines are virtual machines that are supported by the product in use, but are not current for that product. The default network adapter types for all legacy virtual machines depend on the adapters available and compatible to the guest operating system and the version of virtual hardware on which the virtual machine was created.

If you do not upgrade a virtual machine to correspond with an upgrade to a newer version of an ESXi host, your adapter settings remain unchanged. If you upgrade your virtual machine to take advantage of newer virtual hardware, your default adapter settings will likely change to be compatible with the guest operating system and upgraded host hardware.

To verify the network adapters that are available to your supported guest operating system for a particular version of vSphere ESXi, see the *VMware Compatibility Guide* at <http://www.vmware.com/resources/compatibility>.

Change the Virtual Machine Network Adapter Configuration

You can change the virtual machine network configuration, including its power-on behavior and resource allocation.

For details about configuring the networking for virtual machine network adapters, see the *vSphere Networking* documentation.

Prerequisites

Required privilege: **Network.Assign network** on a network if you are changing the network the virtual machine connects to.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, expand **Network adapter**, and select the port group to connect to from the drop-down menu.

The menu lists all standard and distributed port groups that are available for virtual machine use on the host.

If you want to provision bandwidth to the network adapter from a reserved quota by using vSphere Network I/O Control version 3, select a port group that is associated with the network resource pool that provides the quota.

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

Option	Description
Connected	Select or deselect this option while the virtual machine is running to connect or disconnect the virtual network adapter. This check box is not available when the virtual machine is turned off.
Connect at power on	Select this option for the virtual network adapter to connect to the network when the virtual machine turns on. If you do not check this option, you must manually connect the adapter in order for the virtual machine to access the network.

4 Select the network adapter type to use from the **Adapter Type** drop-down menu.

5 (Optional) Select how to assign the **MAC address** from the drop-down menu.

- Select **Automatic** to assign a MAC address automatically.
- Select **Manual** to enter manually the MAC address that you want.

6 If the network adapter is connected to a distributed port group of a distributed switch that has vSphere Network I/O Control version 3 enabled, allocate bandwidth to the adapter.

Note You cannot allocate bandwidth to **SR-IOV passthrough** network adapters.

- a From the **Shares** drop-down menu, set the relative priority of the traffic from this virtual machine as shares from the capacity of the connected physical adapter.
- b In the **Reservation** text box, reserve a minimum bandwidth that must be available to the VM network adapter when the virtual machine is powered on.
- c In the **Limit** text box, set a limit on the bandwidth that the VM network adapter can consume.

7 Click **OK**.

Add a Network Adapter to a Virtual Machine

You can add a network adapter (NIC) to a virtual machine to connect to a network, to enhance communications, or to replace an older adapter. When you add a NIC to a virtual machine, you select the adapter type, network connection, whether the device should connect when the virtual machine is turned on, and the bandwidth allocation.

For details about configuring the networking for virtual machine network adapters, see the *vSphere Networking* documentation

Prerequisites

Required privilege: **Network.Assign network** on a network.

Procedure

1 Right-click a virtual machine in the inventory and select **Edit Settings**.

- 2 On the **Virtual Hardware** tab, add a new network adapter.

Client	Steps
vSphere Client	Click the Add New Device button and select Network Adapter from the drop-down menu.
vSphere Web Client	<ol style="list-style-type: none"> a Select Network from the New device drop-down menu at the bottom of the wizard. b Click Add.

The new network adapter appears at the bottom of the device list.

- 3 Expand **New Network** and select the standard or distributed port group to connect to.

The menu lists all standard and distributed port groups that are available for virtual machine use on the host.

If you want to provision bandwidth to the network adapter from a reserved quota by using vSphere Network I/O Control version 3, select a port group that is associated with the network resource pool that provides the quota.

- 4 (Optional) Review and optionally change the **Status** settings.

Option	Description
Connected	Select this option while the virtual machine is running to connect or disconnect the virtual network adapter. This check box is not available when the virtual machine is turned off.
Connect at power on	Select this option for the virtual network adapter to connect to the network when the virtual machine turns on. If you do not check this option, you must manually connect the adapter for the virtual machine to access the network.

- 5 Select the network adapter type to use from the **Adapter Type** drop-down menu.
- 6 Disable DirectPath I/O if that seems appropriate in your environment.

DirectPath I/O allows virtual machine access to physical PCI functions on platforms with an I/O Memory Management Unit. Some features become unavailable with DirectPath I/O enabled, others become available. See the *vSphere Networking* documentation for details.
- 7 If the network adapter is connected to a distributed port group of a distributed switch that has vSphere Network I/O Control version 3 enabled, allocate bandwidth to the adapter.

Note You cannot allocate bandwidth to **SR-IOV passthrough** network adapters.

- a From the **Shares** drop-down menu, set the relative priority of the traffic from this virtual machine as shares from the capacity of the connected physical adapter.
- b In the **Reservation** text box, reserve a minimum bandwidth that must be available to the VM network adapter when the virtual machine is powered on.
- c In the **Limit** text box, set a limit on the bandwidth that the VM network adapter can consume.

8 (Optional) Select how to assign the **MAC address** from the drop-down menu.

- Select **Automatic** to assign a MAC address automatically.
- Select **Manual** to enter manually the MAC address that you want.

9 Click **OK**.

Parallel and Serial Port Configuration

Parallel and serial ports are interfaces for connecting peripherals to the virtual machine. The virtual serial port can connect to a physical serial port or to a file on the host computer. You can also use it to establish a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. You can add parallel and serial ports and change the parallel and serial port configuration. Hardware version 11 and later versions allow you to configure virtual machines in such a way that serial and parallel ports are absent from the virtual chipset altogether.

Using Serial Ports with vSphere Virtual Machines

You can set up virtual serial port connections for vSphere virtual machines in several ways. The connection method that you select depends on the task that you need to accomplish.

You can set up virtual serial ports to send data in the following ways.

Physical serial port on the host	Sets the virtual machine to use a physical serial port on the host computer. This method lets you use an external modem or a hand-held device in a virtual machine.
Output to file	Sends output from the virtual serial port to a file on the host computer. This method lets you capture the data that a program running in the virtual machine sends to the virtual serial port.
Connect to a named pipe	Sets a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. With this method, two virtual machines or a virtual machine and a process on the host can communicate as if they were physical machines connected by a serial cable. For example, use this option for remote debugging of a virtual machine.
Connect over the network	Enables a serial connection to and from a virtual machine's serial port over the network. The Virtual Serial Port Concentrator (vSPC) aggregates traffic from multiple serial ports onto one management console. vSPC behavior is similar to physical serial port concentrators. Using a vSPC also allows network connections to a virtual machine's serial ports to migrate seamlessly when you use vMotion to migrate the virtual machine. For requirements and steps to configure the Avocent ACS v6000 virtual serial port concentrator, see http://kb.vmware.com/kb/1022303 .

Server and Client Connections for Named Pipe and Network Serial Ports

You can select a client or server connection for serial ports. Your selection determines whether the system waits for a connection or initiates it. Typically, to control a virtual machine over a serial port, you select a server connection. This selection lets you control the connections, which is useful if you connect to the virtual machine only occasionally. To use a serial port for logging, select a client connection. This selection lets the virtual machine connect to the logging server when the virtual machine starts and to disconnect when it stops.

Supported Serial Ports

When you use a physical serial port for serial port passthrough from an ESXi host to a virtual machine, serial ports that are integrated into the motherboard are supported. A virtual machine can use up to 32 serial ports.

Unsupported Serial Ports

When you use a physical serial port for serial port passthrough from an ESXi host to a virtual machine, the serial ports connected through USB are not supported for serial port passthrough. They might be supported by USB passthrough from an ESXi host to a virtual machine. See [USB Configuration from an ESXi Host to a Virtual Machine](#).

In addition, you cannot use Migration with VMotion when you use a physical serial port for serial passthrough.

Adding a Firewall Rule Set for Serial Port Network Connections

If you add or configure a serial port that is backed by a remote network connection, ESXi firewall settings can prevent transmissions.

Before you connect network-backed virtual serial ports, you must add one of the following firewall rule sets to prevent the firewall from blocking communication:

- **VM serial port connected to vSPC.** Use to connect the serial port output through a network with the **Use virtual serial port concentrator** option enabled to allow only outgoing communication from the host.
- **VM serial port connected over network.** Use to connect the serial port output through a network without the virtual serial port concentrator.

Important Do not change the allowed IP list for either rule set. Updates to the IP list can affect other network services that might be blocked by the firewall.

For details about allowing access to an ESXi service through the firewall, see the *vSphere Security* documentation.

Configure Virtual Machine Communication Interface Firewall

You can configure the virtual machine Communication Interface firewall (VMCI) to restrict virtual machines accessing the hypervisor-based services and VMCI-based services.

You can restrict VMCI usage to a subset of VMCI-based services on each virtual machine. For example, you can allow certain virtual machines to access VMCI services and deny access to others for security reasons.

Currently, VMCI devices support guest to host communication. A virtual machine can communicate with VMCI services through the following means:

- ESXi hypervisor
- Services installed on the host operating system in the form of a vmkernel module
- Applications installed by a verified vSphere Installation Bundle

Change the Serial Port Configuration in the vSphere Web Client

You can connect the virtual serial port to a physical serial port or to a file on the host computer. You can also use a host-side named pipe to set up a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. In addition, you can use a port or vSPC URI to connect a serial port over the network. You can add up to 32 serial ports to a virtual machine.

Virtual machines can be in a powered-on state during configuration.

Prerequisites

- Check that you know the correct media types for the port to access, vSPC connections, and any conditions that might apply. See [Using Serial Ports with vSphere Virtual Machines](#).
- 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
Use physical serial port	Select this option to have the virtual machine use a physical serial port on the host computer. Select the serial port from the drop-down menu.
Use output file	Select this option to send output from the virtual serial port to a file on the host computer. Browse to select an output file to connect the serial port to.

Option	Action
Use named pipe	<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"> Type a name for the pipe in the Pipe Name field. Select the Near end and Far end of the pipe from the drop-down menus.
Use Network	<p>Select Use network to connect through a remote network.</p> <ol style="list-style-type: none"> Select the network backing. <ul style="list-style-type: none"> Select Server to have the virtual machine monitor incoming connections from other hosts. Select Client to have the virtual machine initiate a connection to another host. Enter a Port URI. <p>The URI is the remote end of the serial port to which the virtual machine's serial port should connect.</p> If vSPC is used as an intermediate step to access all virtual machines through a single IP address, select Use Virtual Serial Port Concentrator and enter the vSPC URI location.
Printer	Select Printer to connect to a remote printer.

3 (Optional) Select **Yield CPU 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.

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.

```
telnet://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 (`telnet`), or for Telnet (`telnet`) as shown in the following syntax:

```
telnet://host:port #key[=value] [&key[=value] ...]
```

The first parameter must have a number sign (#) prefix. Additional parameters must have an ampersand (&) prefix. The following parameters are supported.

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

verify	Forces certificate verification. The virtual machine will verify that the peer certificate subject matches the specified peerName and that it was signed by a certificate authority known to the ESXi host. Verification is enabled if you specify a thumbprint or peerName
cipherList=value	Specifies a list of SSL ciphers. The ciphers are specified as a list separated by colons, spaces, or commas.

Example: Establishing Serial Port Network Connections to a Client or Server

Simple Server Connection	To connect to a virtual machine's serial port from a Linux or Windows operating system if you do not use vSPC, configure the virtual machine with a serial port connected as a server with a <code>telnet://:12345</code> URI. To access a virtual serial port from a client, use <code>telnet yourESXiServerIPAddress 12345</code> .
Secure Server Connection	<p>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 <code>telnet://:12345#verify</code> URI.</p> <p>To access a virtual serial port from a client, use <code>telnet-ssl yourESXServerName 12345</code>. This connection will fail if the Telnet program you are using does not support SSL encryption.</p>
Simple Client Connection	<p>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 <code>telnet://yourLinuxBox:23</code>.</p> <p>The Virtual machine keeps initiating the Telnet connection to port 23 on <i>yourLinuxBox</i>.</p>
Secure Client Connection	<p>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 <code>telnet://ipOfYourLinuxBox:23#cipherList=DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA&peerName=myLinuxBoxName.withDomain</code> will connect to <i>ipOfYourLinuxBox</i> only if the system supports one of two listed ciphers, and if it presents a trusted certificate issued to <i>myLinuxBoxName.withDomain</i>. Replace <i>.withDomain</i> with the full domain name, for example, <code>example.org</code>.</p>

Add a Serial Port to a Virtual Machine in the vSphere Web Client

You can connect the virtual serial port to a physical serial port or to a file on the host computer. You can also use a host-side named pipe to set up a direct connection between two virtual machines or a connection between a virtual machine and an application on the host computer. In addition, you can use a port or vSPC URI to connect a serial port over the network. A virtual machine can use up to 32 serial ports.

Important With virtual hardware version 11 and later, if you configure a virtual machine without serial ports, they are entirely removed from the virtual chipset and they are not visible to the virtual machine OS.

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 Select a connection type.

Option	Action
Use physical serial port	Select this option to have the virtual machine use a physical serial port on the host computer. Select the serial port from the drop-down menu.
Use output file	Select this option to send output from the virtual serial port to a file on the host computer. Browse to select an output file to connect the serial port to.

Option	Action
Use named pipe	<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"> Type a name for the pipe in the Pipe Name field. Select the Near end and Far end of the pipe from the drop-down menus.
Use Network	<p>Select Use network to connect through a remote network.</p> <ol style="list-style-type: none"> Select the network backing. <ul style="list-style-type: none"> Select Server to have the virtual machine monitor incoming connections from other hosts. Select Client to have the virtual machine initiate a connection to another host. Enter a Port URI. <p>The URI is the remote end of the serial port to which the virtual machine's serial port should connect.</p> If vSPC is used as an intermediate step to access all virtual machines through a single IP address, select Use Virtual Serial Port Concentrator and enter the vSPC URI location.

5 (Optional) Select **Yield CPU on poll**.

Select this option only for guest operating systems that use serial ports in polled mode. This option prevents the guest from consuming excessive CPUs.

6 Select **Connect at power on** to connect the serial port when the virtual machine powers on.

7 Click **OK**.

Example: Establishing Serial Port Network Connections to a Client or Server Without Authentication Parameters

If you do not use vSPC and you configure your virtual machine with a serial port connected as a server with a `telnet://:12345` URI, you can connect to your virtual machine's serial port from your Linux or Windows operating system.

```
telnet yourESXiServerIPAddress 12345
```

Similarly, if you run the Telnet Server on your Linux system on port 23 (`telnet://yourLinuxBox:23`), you configure the virtual machine as a client URI.

```
telnet://yourLinuxBox:23
```

The virtual machine initiates the connection to your Linux system on port 23.

Change the Parallel Port Configuration

You can change the output file for peripheral device output and schedule the parallel port to connect when the virtual machine powers on.

Note If you are changing the parallel port on a virtual machine that runs on an ESXi 4.1 or earlier host, you can send output to a physical parallel port on the host or to an output file on the host. This option is not available with ESXi 5.0 and later.

Prerequisites

Verify that you have the following privileges:

- **Virtual machine.Configuration.Modify device settings** on the virtual machine.
- **Virtual machine .Interaction .Device connection** on the virtual machine to change the device connection status.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, expand **Parallel port**.
- 3 For virtual machines running on ESXi 4.1 and earlier hosts, select the type of media for the parallel port to access.
- 4 Click **Browse** to navigate to the file location.
- 5 Type a name for the file in the **Save As** text box and click **OK**.
The file path appears in the **Connection** text box.
- 6 Select whether to connect the device whenever you power on the virtual machine.
You can change this setting when the virtual machine is either powered on or powered off.
- 7 Click **OK**.

Add a Parallel Port to a Virtual Machine 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.

Important With virtual hardware version 11 and later, if you configure a virtual machine without parallel ports, they are entirely removed from the virtual chipset and they are not visible to the guest OS.

Prerequisites

- Verify that the virtual machine is turned off. You cannot add or remove parallel ports if the virtual machine is turned on.
- Verify that you have the **Virtual machine.Configuration.Add or remove device** privilege on the virtual machine.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, select **Parallel Port** from the **New device** drop-down menu, and click **Add**.

The parallel port appears at the bottom of the virtual device list.

- 3 Expand **New Parallel port**, and click **Browse** to locate a folder to create the file in.
- 4 Type a name for the file in the **Save As** text box and click **OK**.
The file path appears in the **Connection** text box.
- 5 (Optional) Select **Connect At Power On** to connect the device when the virtual machine powers on.
- 6 Click **OK**.

Output from the attached peripheral device is read to the newly created file.

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, Datastore ISO files, or Content Library ISO files.

- [Configure a Datastore ISO File for the CD/DVD Drive](#)
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 Content Library ISO File for the CD/DVD Drive](#)
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 in a content library.
- [Configure a Host Device Type for the CD/DVD Drive](#)
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](#)

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

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.
The **Select File** dialog box opens
- 3 Browse to select the file and click **OK**.
- 4 From 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 Power on the virtual machine and click the **Summary** tab.
- 8 Expand the **VM Hardware** panel and click the **Connected** icon next to the datastore ISO file to connect the device

Configure a Content Library ISO File for the CD/DVD Drive

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 in a content library.

Prerequisites

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 Expand **CD/DVD drive** and select **Content Library ISO File** from the drop-down menu.
The **Choose an ISO image to mount dialog** box opens.
- 3 Select the ISO file and click **OK**.
- 4 (Optional) Select **Connect At Power On** to connect the device when the virtual machine powers on.
- 5 Click **OK**.
- 6 Turn on the virtual machine and click the **Summary tab**.

What to do next

Power on the virtual machine.

Configure a Host Device Type for the CD/DVD Drive

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.
- You cannot use vMotion to migrate virtual machines that have CD drives that are backed by the physical CD drive on the host. Disconnect these devices before you migrate the virtual machine.
- Verify that you have the **Virtual machine .Interaction .Configure CD media** privilege on the virtual machine.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, expand **CD/DVD** and select **Host Device** from the drop-down menu.

- 3 (Optional) Select **Connect At Power On** to connect the device when the virtual machine powers on.
- 4 If more than one type of CD/DVD media is available on the host, select the media.
- 5 In the **Virtual Device Node** drop-down menu, select the node the drive uses in the virtual machine.
The first available node is selected by default. You do not typically need to change the default.
- 6 Click **OK**.
- 7 Turn the virtual machine on and click the **Summary** tab.

The connected CD/DVD device appears in the VM Hardware list.

Configure a Client Device Type for the CD/DVD Drive

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.

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 or Modify a Virtual Machine CD or DVD Drive

CD/DVD drives are necessary for installing a guest operating system and VMware Tools. 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.

When you turn on the virtual machine, you can then select the media to connect to from the **VM Hardware** panel on the virtual machine **Summary** tab.

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.
- 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 Select your task.

Option	Description
Add a CD/DVD drive	On the Virtual Hardware tab, click the Add New Device button and select CD/DVD Drive .
Modify CD/DVD settings	On the Virtual Hardware tab, expand CD/DVD drive and change the configuration settings.

- 3 To change CD/DVD settings, select the device type from the **CD/DVD drive** drop-down menu.

Option	Action
Client Device	Select this option to connect the CD/DVD device to a physical DVD or CD device on the system from which you access the vSphere Client. From the Device Mode drop-down menu, select Passthrough CD-ROM .
Host Device	<ol style="list-style-type: none"> Select to connect the CD/DVD device to a physical DVD or CD device on the host. From the CD/DVD Media drop-down menu, select the media to connect to . From the Device Mode drop-down menu, select Emulate CD-ROM.
Datastore ISO File	Select this option to connect the CD/DVD device to an ISO file that is stored on a datastore accessible to the host. The Select File dialog box opens. <ol style="list-style-type: none"> In the Select File dialog box, browse to the file containing the ISO image to connect to . Click OK.
Content Library ISO File	Select this option to connect the CD/DVD device to an ISO file that is stored in a content library. The Choose an ISO image to mount dialog box opens <ol style="list-style-type: none"> In the Choose an ISO image to mount, select the ISO image to connect to. Click OK.

4 (Optional) Specify additional settings for the CD/DVD drive.

Option	Description
Connect At Power On	Select this option to connect to the device when the virtual machine turns on.
Device Mode	Select Passthrough CD-ROM for a CD/DVD drive that is connected to the physical client machine. Select Emulate CD-ROM otherwise.
Virtual Device Node	Specify the location of the ISO that you are mounting. To change the device node from the default, select a new mode from the Virtual Device Node drop-down menu.

5 Turn on the virtual machine and click the **Summary** tab.

6 Expand the **VM Hardware** panel and click **Connected** next to select to.

What to do next

You can now install the guest operating system or other applications.

Change the Floppy Drive Configuration in the vSphere Web Client

You can configure a virtual floppy drive device to connect to a client device or to an existing or new floppy image.

ESXi does not support floppy drives that are backed by a physical floppy drive on the host.

Note You cannot use vMotion to migrate virtual machines that have floppy drives backed by a physical floppy drive on ESX 3.5, 4. 0, and 4.x hosts that vCenter Server 5.0 manages. You must disconnect these devices before you migrate the virtual machine.

Prerequisites

Verify that you have the **Virtual machine .Interaction .Configure floppy media** privilege on the virtual machine.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, expand **Floppy drive**.

3 Select the device type to use for this virtual device.

Option	Action
Client Device	Select this option to connect the floppy device to a physical floppy device or a .flp floppy image on the system from which you access the vSphere Web Client.
Use existing floppy image	<ol style="list-style-type: none"> Select this option to connect the virtual device to an existing floppy image on a datastore accessible to the host. Click Browse and select the floppy image.
Create new floppy image	<ol style="list-style-type: none"> Select this option to create a floppy image on a datastore accessible to the host. Click Browse and browse to the location for the floppy image. Enter a name for the floppy image and click OK.

4 (Optional) Select or deselect the **Connected** check box to connect or disconnect the device.

5 (Optional) Select **Connect At Power On** to connect the device when the virtual machine powers on.

6 Click **OK**.

Add a Floppy Drive to a Virtual Machine in the vSphere Web Client

Use a physical floppy drive or a floppy image to add a floppy drive to a virtual machine.

ESXi does not support floppy drives that are backed by a physical floppy drive on the host.

Note You cannot use vMotion to migrate virtual machines that have floppy drives backed by a physical floppy drive on ESX 3.5, 4. 0, and 4.x hosts that vCenter Server 5.0 manages. You must disconnect these devices before you migrate the virtual machine.

Important With virtual hardware version 11 and later, the floppy disk controller is absent from the virtual chipset unless a floppy drive is connected to 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**.

- Expand **New Floppy drive** and select the device type to use for this virtual device.

Option	Description
Client Device	Select this option to connect the floppy device to a physical floppy device or a .flp floppy image on the system from which you access the vSphere Web Client.
Use existing floppy image	<ol style="list-style-type: none"> Select this option to connect the virtual device to an existing floppy image on a datastore accessible to the host. Click Browse and select the floppy image.
Create new floppy image	<ol style="list-style-type: none"> Select this option to create a floppy image on a datastore accessible to the host. Click Browse and browse to the location for the floppy image. Enter a name for the floppy image and click OK.

- (Optional) Select or deselect the **Connected** check box to connect or disconnect the device.
- (Optional) Select **Connect At Power On** to connect the device when the virtual machine powers on.
- Click **OK**.

Add and Configure a SCSI Device

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. 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.

The SCSI 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. If the virtual machine does not have a SCSI controller, a controller is added when you add the SCSI device. So, to avoid data congestion, you can add another SCSI controller and assign the SCSI device to a virtual device node on that controller.

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

- Right-click a virtual machine in the inventory and select **Edit Settings**.

- On the **Virtual Hardware** tab, add a SCSI device to the virtual machine.

Client	Steps
vSphere Client	Click the Add New Device button and select SCSI Device from the drop-down menu.
vSphere Web Client	<ol style="list-style-type: none"> Select SCSI Device from the New device drop-down menu at the bottom of the wizard. Click Add.

The SCSI device appears in the Virtual Hardware devices list.

- On the **Virtual Hardware** tab, expand **SCSI Device** and configure the SCSI device or change the default configuration settings.
 - From the **Connection** drop-down menu, select the physical SCSI device to connect to.
 - (Optional) From the **Virtual Device Node** drop-down menu, select the virtual device node.
- Click **OK**.

The virtual machine can access the device.

Add a PCI Device

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. Disable the USB controller for passthrough if your ESXi host is configured to boot from a USB device, or if the active coredump partition is configured to be on a USB device or SD cards connected through USB channels. VMware does not support USB controller passthrough for ESXi hosts that boot from USB devices or SD cards connected through USB channels or if the active coredump partition is configured to be on a USB device or SD card connected through USB channels. For more information, see <http://kb.vmware.com/kb/1021345>.
- Verify that the virtual machine is compatible with ESXi 4.x and later.

Procedure

- Right-click a virtual machine in the inventory and select **Edit Settings**.

- On the **Virtual Hardware** tab, add a new PCI device.

Client	Steps
vSphere Client	Click the Add New Device button and select PCI Device from the drop-down menu.
vSphere Web Client	<ol style="list-style-type: none"> Select PCI Device from the New device drop-down menu at the bottom of the wizard. Click Add.

- Expand **New PCI device** and select the passthrough device to connect to the virtual machine from the drop-down list and click **Next**.
- Click **OK**.

Configuring 3D Graphics

When you create or edit a virtual machine, you can configure 3D graphics to take advantage of Windows AERO, CAD, Google Earth, and other 3D design, modeling, and multimedia applications. Before you enable 3D graphics, become familiar with the available options and requirements.

You can enable 3D on virtual machines that have Windows desktop or Linux guest operating systems. Not all guests support 3D graphics. To verify 3D support for a guest operating system, see the *VMware Compatibility Guide* at <http://www.vmware.com/resources/compatibility>.

Prerequisites

VMware supports AMD and NVIDIA graphics cards. See the vendor website for supported cards. To use the graphics card or GPU hardware, download the appropriate VMware graphics driver from the vendor website.

- Go to the NVIDIA website for information about the VMware graphics driver for your NVIDIA graphics card.
- Go to the AMD website 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

3D Rendering Options

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.

How Enabling 3D Graphics Affects the Virtual Machine

You can use vMotion to migrate virtual machines that have 3D graphics enabled. If the 3D Renderer is set to Automatic, virtual machines use either the GPU on the destination host or a software renderer, depending on GPU availability. To migrate virtual machines with the 3D Renderer set to Hardware, the destination host must have a GPU.

You can set a group of virtual machines to use only Hardware rendering. For example, if you have virtual machines that run CAD applications or have other complex engineering capabilities, you might require that those virtual machines have persistent high-quality 3D capability present. When you migrate such virtual machines, the destination host must also have GPU capability. If the host does not have GPU, the migration cannot proceed. To migrate such virtual machines, you must turn them off and change the renderer setting to Automatic.

Configure 3D Graphics and Video Cards

When you enable 3D graphics, you can select a hardware or software graphics renderer and optimize the graphics memory allocated to the virtual machine. You can increase the number of displays in multi-monitor configurations and change the video card settings to meet your graphics requirements.

The default setting for total video RAM is adequate for minimal desktop resolution. For more complex situations, you can change the default memory. Typically, 3D applications require a video memory of 64–512MB.

Fault Tolerance is 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
Auto-detect settings	Applies common video settings to the guest operating system.
Specify custom settings	Lets you select the number of displays and the total video memory.

- 4 Select the number of displays from the drop-down menu.
You can set the number of displays and extend the screen across them.
- 5 Enter the required video memory.
- 6 (Optional) Click **Video Memory Calculator** to calculate the required video memory based on the maximum number of displays and resolution that the guest operating system must support, and click **OK**.
- 7 (Optional) Click **Enable 3D support**.
This check box is active only for guest operating systems on which VMware supports 3D.
- 8 (Optional) Select a 3D Renderer.

Option	Description
Automatic	Selects the appropriate option (software or hardware) for this virtual machine.
Software	Uses normal CPU processing for 3D calculations.
Hardware	Requires graphics hardware (GPU) for faster 3D calculations.
Note The virtual machine will not power on if graphics hardware is not available.	

- 9 Click **OK**.

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

Reduce Memory Overhead for Virtual Machines with 3D Graphics Option

Virtual machines with the 3D graphics option enabled can have higher memory consumption than other virtual machines. You can reduce the memory overhead by editing the configuration file (.vmx file) of your virtual machines and disabling certain memory-related settings. Reducing the memory overhead of virtual machines can help you increase the number of virtual machines per host.

Prerequisites

Verify that your virtual machines are using hardware version 10 or later.

Procedure

- 1 Shut down the virtual machine on which the 3D graphics option is enabled.
- 2 Disable the **Accelerate 3D Graphics** option.
- 3 Upgrade your ESXi host to use the features available in hardware version 10 or later.
- 4 Set the maximum size of your display to the size you need.
- 5 Locate the configuration file (.vmx) of your virtual machine.
- 6 Open the virtual machine configuration file in a text editor and add the line, `svga.vgaOnly=TRUE`.

This option removes all graphics and SVGA functionality from your SVGA device, but does not remove the settings that allow BIOS to enter VGA mode.
- 7 Save the changes and exit the text editor.
- 8 Power on your virtual machine and check the display console.
- 9 Verify the memory reservation settings in the `vmware.log` file.

Add an NVIDIA GRID vGPU to a Virtual Machine

If an ESXi host has an NVIDIA GRID GPU graphics device, you can configure a virtual machine to use the NVIDIA GRID virtual GPU (vGPU) technology.

NVIDIA GRID GPU graphics devices are designed to optimize complex graphics operations and enable them to run at high performance without overloading the CPU. NVIDIA GRID vGPU provides unparalleled graphics performance, cost-effectiveness and scalability by sharing a single physical GPU among multiple virtual machines as separate vGPU-enabled passthrough devices.

Prerequisites

- Verify that an NVIDIA GRID GPU graphics device with an appropriate driver is installed on the host. See the *vSphere Upgrade* documentation.
- Verify that the virtual machine is compatible with ESXi 6.0 and later.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.

- 2 On the **Virtual Hardware** tab, add a shared PCI device to the virtual machine.

Client	Steps
vSphere Client	Click the Add New Device button and select Shared PCI Device from the drop-down menu.
vSphere Web Client	<ol style="list-style-type: none"> a Select Shared PCI Device from the New device drop-down menu at the bottom of the wizard. b Click Add.

- 3 Expand the **New PCI device**, and select the NVIDIA GRID vGPU passthrough device to which to connect your virtual machine.
- 4 Select a GPU profile.
A GPU profile represents the vGPU type.
- 5 Click **Reserve all memory**.
- 6 Click **OK**.

The virtual machine can access the device.

USB Configuration from an ESXi Host to a Virtual Machine

You can add multiple USB devices to a virtual machine when the physical devices are connected to an ESXi host. USB passthrough technology supports adding USB devices, such as security dongles and mass storage devices to virtual machines that reside on the host to which the devices are connected.

How USB Device Passthrough Technology Works

When you attach a USB device to a physical host, the device is available only to virtual machines that reside on that host. The device cannot connect to virtual machines that reside on another host in the datacenter.

A USB device is available to only one virtual machine at a time. When a device is connected to a powered-on virtual machine, it is not available to connect to other virtual machines that run on the host. When you remove the active connection of a USB device from a virtual machine, it becomes available to connect to other virtual machines that run on the host.

Connecting a USB passthrough device to a virtual machine that runs on the ESXi host to which the device is physically attached requires an arbitrator, a controller, and a physical USB device or device hub.

USB Arbitrator

Manages connection requests and routes USB device traffic. The arbitrator is installed and enabled by default on ESXi hosts. It scans the host for USB devices and manages device connection among virtual machines that reside on the host. It routes device traffic to the correct virtual machine instance for delivery to the guest operating system. The arbitrator monitors the USB device and prevents other virtual machines from using it until you release it from the virtual machine it is connected to.

USB Controller

The USB hardware chip that provides USB function to the USB ports that it manages. The virtual USB Controller is the software virtualization of the USB host controller function in the virtual machine.

USB controller hardware and modules that support USB 3.0, 2.0, and USB 1.1 devices must exist on the host. Eight virtual USB controllers are available to each virtual machine. A controller must be present before you can add USB devices to the virtual computer.

The USB arbitrator can monitor a maximum of 15 USB controllers. Devices connected to controllers numbered 16 or greater are not available to the virtual machine.

USB Devices

You can add up to 20 USB devices to a virtual machine. This is the maximum number of devices supported for simultaneous connection to one virtual machine. The maximum number of USB devices supported on a single ESXi host for simultaneous connection to one or more virtual machines is also 20. For a list of supported USB devices, see the VMware knowledge base article at <http://kb.vmware.com/kb/1021345>. You can add USB 3.0 devices to Mac OSX guest operating system for VMware Fusion.

USB 3.0 Device Requirements

Starting with vSphere 5.5 Patch 3, USB 3.0 devices are available for passthrough not only from a client computer to a virtual machine, but also from an ESXi host to a virtual machine. USB 3.0 devices still have the following virtual machine configuration requirements:

- 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 Autoconnect Feature

When you add a USB device connection from an ESXi host to a virtual machine, the autoconnect feature is enabled for the device connection. It is not disabled until you remove the device connection from the virtual machine.

With autoconnect enabled, the device connection re-establishes in the following cases:

- The virtual machine is cycling through power operations, such as Power Off/Power On, Reset, Pause/Resume.
- The device is unplugged from the host then plugged back in to the same USB port.
- The device is power cycled but has not changed its physical connection path.
- The device is mutating identity during usage.
- A new virtual USB device is added

The USB passthrough autoconnect feature identifies the device by using the USB path of the device on the host. It uses the physical topology and port location, rather than the device identity. This feature can seem confusing if you expect the autoconnect feature to match the connection target by device ID.

If the same device is plugged back in to the host through a different USB port, it cannot re-establish connection with the virtual machine. If you unplug the device from the host and plug in a different device to the same USB path, the new device appears and is connected to the virtual machine by the autoconnect feature that the previous device connection enabled.

Autoconnect is useful in cases where devices mutate during usage. For example, for iPhones and other such devices, the device VID:PID changes during software or firmware upgrades. The upgrade process disconnects and reconnects the devices to the USB port.

The USB port is speed-specific. The autoconnect feature assumes that devices do not transition from USB 1.1 (low-full speed) to USB 2.0 (high speed) or the reverse. You cannot interchange USB 2.0 high-speed devices with USB 1.1 devices. For example, you might connect a USB 2.0 high-speed device to a port and connect that device to the virtual machine. If you unplug the device from the host and plug a USB 1.1 device into the same port, the device does not connect to the virtual machine.

For a list of supported USB devices for passthrough from an ESXi host to a virtual machine, see the VMware knowledge base article at <http://kb.vmware.com/kb/1021345>.

vSphere Features Available with USB Passthrough

Migrations with vMotion and DRS are supported with USB device passthrough from an ESXi host to a virtual machine.

Table 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 [Troubleshooting USB Passthrough Devices](#) 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.

Add USB Devices to an ESXi Host

You can connect multiple USB devices to ESXi hosts so that virtual machines that run on the hosts can access the devices. The number of devices that you can connect depends on several factors, such as how the devices and hubs chain together and the device type.

Each ESXi host has several USB ports. The number of ports on each host depends on the physical setup of the host. When you calculate the depth of hub chaining, remember that on a typical server the front ports connect to an internal hub.

The USB arbitrator can monitor a maximum of 15 USB controllers. If your system includes controllers that exceed the 15 controller limit and you connect USB devices to them, the devices are not available to the virtual machine.

The host treats USB CD/DVD-ROM devices as SCSI devices. Hot adding and removing these devices is not supported.

Prerequisites

- If a host has attached USB devices and resides in a DRS cluster with DPM enabled, disable DPM for that host. See the *vSphere Resource Management* documentation for instructions about overriding the default DPM setting for an individual host.
- Verify that you know the virtual machine requirements for USB devices. See [Connecting USB Devices to an ESXi Host](#).
- Verify that the ESXi host is powered off before you add USB CD/DVD-ROM devices.
- Verify that the current version of your ESXi host is 6.0 or later for adding eight virtual xHCI controller to the ESXi host.

Procedure

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

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](#).

Add a USB Controller to a Virtual Machine

USB controllers are available to add to virtual machines to support USB passthrough from an ESXi host or from a client computer to a virtual machine.

You can add one virtual xHCI controller, one virtual EHCI controller, and one virtual UHCI controller per virtual machine. With Hardware Version 11, the supported number of root hub ports per xHCI controller is eight (four logical USB 3.0 ports and four logical USB 2.0 ports).

The conditions for adding a controller vary, depending on the device version, the type of passthrough (host or client computer), and the guest operating system.

Table 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 3.0, 2.0, and 1.1 devices only)	Yes (Linux, Windows 8 and later, and Windows Server 2012 and later guests)

For Mac OS X systems, the EHCI+UHCI controller is enabled by default and is required for USB mouse and keyboard access.

For virtual machines with Linux guests, you can add one or both controllers, but 3.0 superspeed devices are not supported for passthrough from an ESXi host to a virtual machine. You cannot add two controllers of the same type.

For USB passthrough from an ESXi host to a virtual machine, the USB arbitrator can monitor a maximum of 15 USB controllers. If your system includes controllers that exceed the 15 controller limit and you connect USB devices to them, the devices are not available to the virtual machine.

Prerequisites

- ESXi hosts must have USB controller hardware and modules that support USB 3.0, 2.0, and 1.1 devices present.
- Client computers must have USB controller hardware and modules that support USB 3.0, 2.0, and 1.1 devices present.
- To use the xHCI controller on a Linux guest, ensure that the Linux kernel version is 2.6.35 or later.
- Verify that the virtual machine is powered on.
- Required Privilege (ESXi host passthrough): **Virtual Machine.Configuration.Add or Remove Device**

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, add a USB controller.

Client	Steps
vSphere Client	Click the Add New Device button and select USB Controller from the drop-down menu.
vSphere Web Client	<ol style="list-style-type: none"> a Select USB Controller from the New device drop-down menu at the bottom of the Edit Settings wizard. b Click Add.

The controller appears in the Virtual Hardware devices list.

- 3 Expand **New USB Controller** to change the USB controller type.
If compatibility errors appear, fix them before you can add the controller.
- 4 Click **OK**.

What to do next

Add one or more USB devices to the virtual machine.

Add USB Devices from an ESXi Host to a Virtual Machine

You can add one or more USB passthrough devices from an ESXi host to a virtual machine if the physical devices are connected to the host on which the virtual machine runs.

If a USB device is connected to another virtual machine, you cannot add it until that machine releases it.

Note If you have the Apple Frontpanel Controller device in your environment, you can safely add it to a virtual machine. However, this device has no documented function and no known use. ESXi hosts do not use it and do not provide Xserver functionality for USB passthrough.

Prerequisites

- Verify that the virtual machine is compatible with ESX/ESXi 4.0 and later.
- Verify that a USB controller is present. See [Add a USB Controller to a Virtual Machine](#).
- 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, add a USB passthrough device to the virtual machine.

Client	Steps
vSphere Client	Click the Add New Device button and select Host USB Device from the drop-down menu.
vSphere Web Client	<ol style="list-style-type: none"> a Select Host USB Device from the New device drop-down menu at the bottom of the Edit Settings wizard. b 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 the pointer over the device and click the **Remove** icon.
- 4 Click **OK** to save your changes.

Remove USB Devices from an ESXi Host

You can remove USB devices from the host if you must shut down the host for maintenance or if you do not want those devices to be available to virtual machines that run on the host. When you detach a USB device from the host, the device disconnects from the virtual machine.

Caution If data transfer is taking place when you remove USB devices from a host, you can lose data.

Prerequisites

Verify that the USB devices are not in use.

Procedure

- ◆ Follow the device manufacturers instructions to safely remove the device.

When you remove the device from the host, it is no longer available to the virtual machines that run on the host.

USB Configuration from a Client Computer to a Virtual Machine

You can add multiple USB devices to a virtual machine when the physical devices connect to a client computer on which the vSphere Client is running. The vSphere 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 Requirements

Starting with vSphere 5.5 Patch 3, USB 3.0 devices are available for passthrough not only from a client computer to a virtual machine, but also from an ESXi host to a virtual machine. USB 3.0 devices still have the following virtual machine configuration requirements:

- 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.

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 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.

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.

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.

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.

Procedure

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

What to do next

You can now add the USB device to the virtual machine.

Add a USB Controller to a Virtual Machine

USB controllers are available to add to virtual machines to support USB passthrough from an ESXi host or from a client computer to a virtual machine.

You can add one virtual xHCI controller, one virtual EHCI controller, and one virtual UHCI controller per virtual machine. With Hardware Version 11, the supported number of root hub ports per xHCI controller is eight (four logical USB 3.0 ports and four logical USB 2.0 ports).

The conditions for adding a controller vary, depending on the device version, the type of passthrough (host or client computer), and the guest operating system.

Table 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 3.0, 2.0, and 1.1 devices only)	Yes (Linux, Windows 8 and later, and Windows Server 2012 and later guests)

For Mac OS X systems, the EHCI+UHCI controller is enabled by default and is required for USB mouse and keyboard access.

For virtual machines with Linux guests, you can add one or both controllers, but 3.0 superspeed devices are not supported for passthrough from an ESXi host to a virtual machine. You cannot add two controllers of the same type.

For USB passthrough from an ESXi host to a virtual machine, the USB arbitrator can monitor a maximum of 15 USB controllers. If your system includes controllers that exceed the 15 controller limit and you connect USB devices to them, the devices are not available to the virtual machine.

Prerequisites

- ESXi hosts must have USB controller hardware and modules that support USB 3.0, 2.0, and 1.1 devices present.
- Client computers must have USB controller hardware and modules that support USB 3.0, 2.0, and 1.1 devices present.
- To use the xHCI controller on a Linux guest, ensure that the Linux kernel version is 2.6.35 or later.
- Verify that the virtual machine is powered on.
- Required Privilege (ESXi host passthrough): **Virtual Machine.Configuration.Add or Remove Device**

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, add a USB controller.

Client	Steps
vSphere Client	Click the Add New Device button and select USB Controller from the drop-down menu.
vSphere Web Client	<ol style="list-style-type: none"> a Select USB Controller from the New device drop-down menu at the bottom of the Edit Settings wizard. b Click Add.

The controller appears in the Virtual Hardware devices 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

You can add one or more USB passthrough devices from a client computer to a virtual machine in the vSphere 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 Client is running and connected. After you add the USB device to the virtual machine, a message on the client computer states that the device is disconnected. The device remains disconnected from the client computer until you disconnect it from the virtual machine.

Fault Tolerance is not supported with USB passthrough from a client computer to a virtual machine.

Prerequisites

- Verify that a USB device is connected to the client computer.
- Verify that the virtual machine is powered on.
- Verify that a USB controller is present.
- Verify that the vSphere 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 In the vSphere Client, navigate to a virtual machine.
- 2 Launch the VMware Remote Console application.

Note You cannot connect a USB device to a virtual machine if you use the HTML5 console in the vSphere Client.

- 3 In the VMware Remote Console toolbar, click **VMRC > Removable Devices** and find the USB device.
- 4 Click **Connect (Disconnect from menu)**.

The USB device is connected to the virtual machine.

Remove USB Devices That Are Connected Through a Client Computer

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

- Verify that the virtual machine is powered on.
- To minimize the risk of data loss, follow the instructions to safely unmount or eject hardware for your operating system. Safely removing hardware allows accumulated data to be transmitted to a file. Windows operating systems typically include a Remove Hardware icon located in the System Tray. Linux operating systems use the **umount** command.

Note You might need to use the sync command instead of or in addition to the umount command, for example after you run a dd command on Linux or other UNIX operating systems.

- Required Privilege: **Virtual machine.Configuration.Add or remove device**

Procedure

- 1 Unmount or eject the USB device from the guest operating system.
- 2 On the virtual machine **Summary** tab, click the disconnect icon on the right side of the USB device entry.
- 3 Select a device to disconnect from the drop-down menu.

A **Disconnecting** label and a spinner appear, indicating that a disconnection is in progress. When the device is disconnected, after a slight delay, the **Summary** tab refreshes and the device is removed from the virtual machine configuration.

The device reconnects to the client computer and is available to add to another virtual machine. In some cases, Windows Explorer detects the device and opens a dialog box on the client computer. You can close this dialog box.

Remove a USB Controller from a Virtual Machine

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, click the **VMs** tab and click **Virtual Machines**.
- 2 Right-click a virtual machine and click **Edit Settings**.
- 3 On the **Virtual Hardware** tab, move the pointer over the USB controller and click the **Remove** icon.
- 4 Click **OK** to confirm the deletion and close the dialog box.

The controller is no longer connected to the virtual machine, but remains available to add at a later time.

Add a Shared Smart Card Reader to Virtual Machines

You can configure multiple virtual machines to use a virtual shared smart card reader for smart card authentication. The smart card reader must be connected to a client computer on which the vSphere 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 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](#).

Prerequisites

- Verify that the smart card reader is connected to the client computer.
- Verify that the virtual machine is powered on.
- Verify that a USB controller is present.
- Required Privilege: **Virtual machine.Configuration.Add or remove device**

Procedure

- 1 Navigate to a datacenter, folder, cluster, resource pool, host, or vApp, and click the **Related Options** tab and click **Virtual Machines**.
- 2 Select a virtual machine, click it again, and click the **Summary** tab.
- 3 Click the USB icon on the right side of **USB Devices** under **VM Hardware**, and select an available shared smart card reader from the drop down menu.

Select a device that appears as **Shared the model name of your smart card reader** followed by a number.

A **Connecting** label and a spinner appear showing that a connection is in progress. When the device has successfully connected and the Summary tab refreshes, the device is connected and the device name appears next to **USB Devices**.

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

Securing Virtual Machines with Virtual Trusted Platform Module

The Virtual Trusted Platform Module (vTPM) feature lets you add a TPM 2.0 virtual cryptoprocessor to a virtual machine.

Virtual Trusted Platform Module Overview

vTPMs perform cryptographic coprocessor capabilities in software. When added to a virtual machine, a vTPM enables the guest operating system to create and store keys that are private. These keys are not exposed to the guest operating system itself. Therefore, the virtual machine attack surface is reduced. Usually, compromising the guest operating system compromises its secrets, but enabling a vTPM greatly reduces this risk. These keys can be used only by the guest operating system for encryption or signing. With an attached vTPM, a third party can remotely attest to (validate) the identity of the firmware and the guest operating system.

You can add a vTPM to either a new virtual machine or an existing virtual machine. A vTPM depends on virtual machine encryption to secure vital TPM data. When you configure a vTPM, VM encryption automatically encrypts the virtual machine files but not the disks. You can choose to add encryption explicitly for the virtual machine and its disks.

You can also back up a virtual machine enabled with a vTPM. The backup must include all virtual machine data, including the *.nvram file. If your backup does not include the *.nvram file, you cannot restore a virtual machine with a vTPM. Also, because the VM home files of a vTPM-enabled virtual machine are encrypted, ensure that the encryption keys are available at the time of a restore.

A vTPM does not require a physical Trusted Platform Module (TPM) 2.0 chip to be present on the ESXi host. However, if you want to perform host attestation, an external entity, such as a TPM 2.0 physical chip, is required. For more details, see the *vSphere Security* documentation.

Note By default, no storage policy is associated with a virtual machine that has been enabled with a vTPM. Only the virtual machine files (VM Home) are encrypted. If you prefer, you can choose to add encryption explicitly for the virtual machine and its disks, but the virtual machine files would have already been encrypted.

Requirements for vTPM

To use a vTPM, your vSphere environment must meet these requirements:

- Virtual machine requirements:
 - EFI firmware
 - Hardware version 14
- Component requirements:
 - vCenter Server 6.7.

- Virtual machine encryption (to encrypt the virtual machine home files).
- Key Management Server (KMS) configured for vCenter Server (virtual machine encryption depends on KMS). For more details, see the *vSphere Security* documentation.
- Guest OS support:
 - Windows Server 2016 (64 bit)
 - Windows 10 (64 bit)

Differences Between a Hardware TPM and a Virtual TPM

You use a hardware Trusted Platform Module (TPM) as a cryptographic coprocessor to provide secure storage of credentials or keys. A vTPM performs the same functions as a TPM, but it performs cryptographic coprocessor capabilities in software. A vTPM uses the `.nvram` file, which is encrypted using virtual machine encryption, as its secure storage.

A hardware TPM includes a preloaded key called the Endorsement Key (EK). The EK has a private and public key. The EK provides the TPM with a unique identity. For a vTPM, this key is provided either by the VMware Certificate Authority (VMCA) or by a third-party Certificate Authority (CA). Once the vTPM uses a key, it is typically not changed because doing so invalidates sensitive information stored in the vTPM. The vTPM does not contact the CA at any time.

Enable Virtual Trusted Platform Module for an Existing Virtual Machine

You can add a Virtual Trusted Platform Module (vTPM) to an existing virtual machine to provide enhanced security to the guest operating system. You must set up the KMS before you can add a vTPM.

You can enable a vTPM for virtual machines running on vSphere 6.7 and later. The VMware virtual TPM is compatible with TPM 2.0, and creates a TPM-enabled virtual chip for use by the virtual machine and the guest OS it hosts.

Prerequisites

- Ensure your vSphere environment is configured for virtual machine encryption. See the *vSphere Security* documentation.
- The guest OS you use must be either Windows Server 2016 (64 bit) or Windows 10 (64 bit).
- Verify that the virtual machine is turned off.
- The ESXi hosts running in your environment must be ESXi 6.7 or later.
- The virtual machine must use EFI firmware.

Procedure

- 1 Connect to vCenter Server by using the vSphere Client.
- 2 Right-click the virtual machine in the inventory that you want to modify and select **Edit Settings**.
- 3 In the **Edit Settings** dialog box, click **Add New Device** and select **Trusted Platform Module**.

4 Click **OK**.

The virtual machine **Summary** tab now includes Virtual Trusted Platform Module in the **VM Hardware** pane.

Remove Virtual Trusted Platform Module from a Virtual Machine

You can remove Virtual Trusted Platform Module (vTPM) security from a virtual machine.

Removing vTPM causes all encrypted information on the virtual machine to become unrecoverable. In addition, removing a vTPM initiates an immediate reboot of the virtual machine. Before removing a vTPM from a virtual machine, disable any applications in the Guest OS, such as BitLocker, that use vTPM. Failure to do so can cause the virtual machine to not boot.

Procedure

- 1 Connect to vCenter Server by using the vSphere Client.
- 2 Right-click the virtual machine in the inventory that you want to modify and select **Edit Settings**.
- 3 In the **Edit Settings** dialog box, locate the Trusted Platform Module entry in the **Virtual Hardware** tab.
- 4 Move your cursor over the device and click the **Remove** icon.

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

- 5 Click **Delete** to confirm you want to remove the device.

The vTPM device is marked for removal.

- 6 Click **OK**.

Verify that the Virtual Trusted Platform Module entry no longer appears in the virtual machine **Summary** tab in the **VM Hardware** pane.

Configuring Virtual Machine Options

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 Options Overview](#)
- [General Virtual Machine Options](#)
- [Configuring User Mappings on Guest Operating Systems](#)
- [VMware Remote Console Options](#)
- [Virtual Machine Encryption](#)
- [Virtual Machine Power Management Options](#)
- [Configuring VMware Tools Options](#)
- [Virtualization Based Security](#)
- [Configuring Virtual Machine Boot Options](#)
- [Configuring Virtual Machine Advanced Options](#)
- [Configure Fibre Channel NPIV Settings](#)

Virtual Machine Options Overview

You can view or change virtual machine settings from the vSphere 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.

You can view and change virtual machine settings on the **VM Options** tab of the **Edit Settings** wizard.

You can select one of the following options.

Table 6-1. Virtual Machine Options in the vSphere Client and the vSphere Web Client

Options	Description
General Options	<p>In this section, you can view or change the following settings.</p> <ul style="list-style-type: none"> Virtual machine name Virtual machine configuration file location Virtual machine working location Guest operating system and OS version <p>Currently, you can only edit the virtual machine name. The information about the other settings is currently read only.</p> <p>To change the operating system for a VM, you have to reinstall the OS - or consider deploying a new VM with your operating system of choice.</p>
VMware Remote Console Options	In this section, you can change the locking behavior of a virtual machine and the settings for simultaneous connections.
Encryption	In this section, you can change the encryption settings of a virtual machine.
Power Management	In this section, you can change virtual machine suspend behavior.
VMware Tools	In this section, you can change the behavior of VMware Tools scripts. You can also customize the automatic VMware Tools upgrades and the time synchronization between the guest and host.
Virtualization Based Security	<p>Enable or disable VBS for the virtual machine.</p> <p>Note This option is only available in the vSphere Client.</p>
Boot Options	In this section, you can change the virtual machine boot options. For example, add a delay before booting, force entry into the BIOS or EFI setup screen, or set reboot options.
Advanced	<p>In this section, you can change the following advanced virtual machine options.</p> <ul style="list-style-type: none"> Acceleration and logging settings Debugging and statistics Swap file location Latency sensitivity
Fibre Channel NPIV	In this section, you can change the virtual node and port World Wide Names (WWNs).

General Virtual Machine Options

View or change general virtual machine settings, such as the name and location of the virtual machine, configuration file location, and operating system.

Change the Virtual Machine Name

If you move a virtual machine to a different datastore folder or move the virtual machine to a host that has an existing virtual machine of the same name, you can change the virtual machine's name to keep it unique. When you change the name of a virtual machine, you change the name used to identify the virtual machine in the vCenter Server inventory. This action does not change the name used as the computer name by the guest operating system.

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

Note Migration with Storage vMotion changes the virtual machine file names on the destination datastore to match the inventory name of the virtual machine. The migration renames all virtual disk, configuration, snapshot, and .nvram files. If the new names exceed the maximum filename length, the migration does not succeed.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 Click the **VM Options** tab and expand **General Options**.
- 3 Delete the existing name and type a new name for the virtual machine in the **VM Name** text box.
- 4 Click **OK**.

View the Virtual Machine Configuration and Working File Location

You can view the location of the virtual machine configuration and working files. You can use this information when you configure backup systems.

Prerequisites

Verify that the virtual machine is powered off.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 Click **VM Options** tab and expand **General Options**.

The path to the location of the virtual machine configuration file appears in the **VM Config File** text box. The path to the virtual machine working location appears in the **VM Working Location** text box.

Change the Configured Guest Operating System

When you change the guest operating system type in the virtual machine settings, you change the setting for the guest operating system in the virtual machine's configuration file. To change the guest operating system itself, you must install the new operating system in the virtual machine.

You might change the guest operating system, for example, if you are upgrading the guest operating system installed in the virtual machine.

When you set the guest operating system type for a new virtual machine, vCenter Server chooses configuration defaults based on the guest type. Changing the guest operating system type after the virtual machine is created does not retroactively change those settings. It affects the recommendations and setting ranges offered after the change.

Prerequisites

Power off the virtual machine.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 Click the **VM Options** tab and expand **General Options**.
- 3 From the **Guest OS** drop-down menu, select the guest operating system family.
- 4 From the **Guest OS Version** drop-down menu, 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, in the vSphere Web Client you are prompted to type a name for the operating system in the text box.
- 6 Click **OK**.

Configuring User Mappings on Guest Operating Systems

As a vSphere administrator, you can enable guest OS access on certain SSO accounts.

Enabling SSO accounts to log in to a guest OS provides users with additional capabilities to perform administrative tasks on guest virtual machines, such as installing or upgrading the VMware Tools or configuring apps.

Functionality to allow vSphere administrators to configure a guest operating system to use VGAAuth authentication. The vSphere administrator must know the guest administrator password for the enrollment process.

To enroll SSO users to a guest user account, you must enroll SSO users to accounts in guest operating systems. The enrollment process maps a vSphere user to a particular account in the guest by using SSO certificates. Subsequent guest management requests use an SSO SAML token to log in to the guest.

You must configure VMs to accept X.509 certificates. X.509 certificates allow the vSphere administrators in your data center to use SAM tokens issued by single sign-on service to access guest OSs.

View Existing SSO User Mappings

You can view the existing guest user mappings for guest operating systems on the selected virtual machine. You need to authenticate your credentials to view guest mappings.

Procedure

- 1 Select the virtual machine where you want to view the list of user mappings.
- 2 Click **Configure > Settings > Guest User Mappings**.
- 3 Specify your user name and password.
- 4 Click **OK**.

The existing in-guest user mappings are displayed.

Add SSO users to Guest Operating Systems

You can map a new SSO user to a guest user account by creating a new user map. Mapping can be established for any type of SSO users, such as solution as well as regular users.

Prerequisites

Power on the virtual machine.

Procedure

- 1 In the View Guest User Mappings window, click **Add new user mappings**.
- 2 Select the SSO user from the list that you want to map.
- 3 Specify a guest OS user name.
- 4 Click **OK**.

The SSO user is mapped to a guest user account. A new guest user account is added to the list of Guest User Mappings.

Remove SSO Users from Guest Operating Systems

You can remove an existing SSO account from guest user mappings.

Prerequisites

Power on your virtual machine.

Procedure

- 1 In the View Guest User Mappings window, select the SSO user from the list that you want to remove.
- 2 Click remove user mappings.
- 3 Click **Yes** to confirm.

The mapping between the selected SSO user account and guest OS account has been removed.

VMware Remote Console Options

Change the VMware Remote Console options to control the access to the virtual machine .

Change the Virtual Machine Console Options for Remote Users

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 the **Guest OS lock** check box to lock the guest operating system when the last remote user disconnects.
- 4 (Optional) Select **Maximum number of sessions** check box to limit the number of simultaneous connections to this virtual machine, and enter a number.
- 5 Click **OK**.

Virtual Machine Encryption

Starting with vSphere 6.5, you can take advantage of virtual machine encryption. Encryption protects not only your virtual machine but also virtual machine disks and other files. You set up a trusted connection between vCenter Server and a key management server (KMS). vCenter Server can then retrieve keys from the KMS as needed.

For detailed information about virtual machine encryption, see the *vSphere Security* documentation.

Encrypt an Existing Virtual Machine or Virtual Disk

You can encrypt an existing virtual machine or virtual disk by changing its storage policy. You can encrypt virtual disks only for encrypted virtual machines.

This task describes how to encrypt an existing virtual machine or virtual disk using either the vSphere Client (HTML5-based client) or the vSphere Web Client.

Prerequisites

- Establish a trusted connection with the KMS and select a default KMS.
- Create an encryption storage policy, or use the bundled sample, VM Encryption Policy.
- Ensure that the virtual machine is powered off.
- Verify that you have the required privileges:
 - **Cryptographic operations.Encrypt new**
 - If the host encryption mode is not Enabled, you also need **Cryptographic operations.Register host**.

Procedure

- 1 Connect to vCenter Server by using either the vSphere Client (HTML5-based client) or the vSphere Web Client.

- 2 Right-click the virtual machine that you want to change and select **VM Policies > Edit VM Storage Policies**.

You can set the storage policy for the virtual machine files, represented by VM home, and the storage policy for virtual disks.

- 3 Select the storage policy.

- vSphere Client (HTML5-based client):
 - To encrypt the VM and its hard disks, select an encryption storage policy and click **OK**.
 - To encrypt the VM but not the virtual disks, toggle on **Configure per disk**, select the encryption storage policy for VM Home and other storage policies for the virtual disks, and click **OK**.
- vSphere Web Client:
 - To encrypt the VM and its hard disks, select an encryption storage policy and click **Apply to all**.
 - To encrypt the VM but not the virtual disks, select the encryption storage policy for VM Home and other storage policies for the virtual disks, and click **Apply**.

You cannot encrypt the virtual disk of an unencrypted VM.

- 4 If you prefer, you can encrypt the virtual machine, or both virtual machine and disks, from the **Edit Settings** menu in the vSphere Client.
 - a Right-click the virtual machine and select **Edit Settings**.
 - b Select the **VM Options** tab, and open **Encryption**. Choose an encryption policy. If you deselect all disks, only the VM home is encrypted.
 - c Click **OK**.

Decrypt an Encrypted Virtual Machine or Virtual Disk

You can decrypt a virtual machine, its disks, or both, by changing the storage policy.

This task describes how to decrypt an encrypted virtual machine using either the vSphere Client (HTML5-based client) or the vSphere Web Client.

All encrypted virtual machines require encrypted vMotion. During virtual machine decryption, the Encrypted vMotion setting remains. To change this setting so that Encrypted vMotion is no longer used, change the setting explicitly.

This task explains how to perform decryption using storage policies. For virtual disks, you can also perform decryption using the **Edit Settings** menu.

Prerequisites

- The virtual machine must be encrypted.
- The virtual machine must be powered off or in maintenance mode.
- Required privileges: **Cryptographic operations.Decrypt**

Procedure

- 1 Connect to vCenter Server by using either the vSphere Client (HTML5-based client) or the vSphere Web Client.
- 2 Right-click the virtual machine that you want to change and select **VM Policies > Edit VM Storage Policies**.

You can set the storage policy for the virtual machine files, represented by VM home, and the storage policy for virtual disks.

- 3 Select a storage policy.
 - vSphere Client (HTML5-based client):
 - To decrypt the VM and its hard disks, toggle off **Configure per disk**, select a storage policy from the drop-down menu, and click **OK**.
 - To decrypt a virtual disk but not the virtual machine, toggle on **Configure per disk**, select the encryption storage policy for VM Home and other storage policies for the virtual disks, and click **OK**.
 - vSphere Web Client:
 - To decrypt the virtual machine and its hard disks, select a storage policy from the drop-down menu, click **Apply to all**, and click **OK**.
 - To decrypt a virtual disk but not the virtual machine, select a storage policy for the virtual disk from the drop-down menu in the table. Do not change the policy for VM Home. Click **OK**.

You cannot decrypt the virtual machine and leave the disk encrypted.

- 4 If you prefer, you can use the vSphere Client (HTML5-based client) to decrypt the virtual machine and disks from the **Edit Settings** menu.
 - a Right-click the virtual machine and select **Edit Settings**.
 - b Select the **VM Options** tab and expand **Encryption**.
 - c To decrypt the VM and its hard disks, choose **None** from the **Encrypt VM** drop-down menu.
 - d To decrypt a virtual disk but not the virtual machine, deselect the disk.
 - e Click **OK**.
- 5 (Optional) You can change the Encrypted vMotion setting.
 - a Right-click the virtual machine and click **Edit Settings**.
 - b Click **VM Options**, and open **Encryption**.
 - c Set the **Encrypted vMotion** value.

Virtual Machine Power Management Options

Configure virtual machine Power management options to define how the virtual machine responds when the guest OS is placed on standby.

Manage Power Management Settings for a Virtual Machine

If the guest operating system is placed on standby, the VM can either remain powered on or be suspended. You can use the Power Management settings to control this behavior. 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 Vlan NICs or when a Flexible NIC is operating in Vlan 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 **VM Options** and expand **Power Management**.

3 Customize the power management settings for the virtual machine.

Client	Steps
vSphere Client	<p>In the Standby response section, select the standby response of the virtual machine.</p> <ul style="list-style-type: none"> ■ The Suspend the virtual machine option 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. ■ The Put the guest operating system in standby mode and leave the virtual machine powered on option stops all processes, but leaves the virtual devices connected to the virtual machine.
vSphere Web Client	<p>a In the Standby response section, select the standby response of the virtual machine.</p> <ul style="list-style-type: none"> ■ The Suspend the virtual machine option 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. ■ The Put the guest operating system in standby mode and leave the virtual machine powered on option stops all processes, but leaves the virtual devices connected to the virtual machine. <p>b (Optional) Select Wake on LAN for virtual machine traffic on and select the virtual NICs to trigger this action.</p> <p>Unsupported NICs might be listed, but are unavailable to connect.</p>
Option	Description
Suspend the virtual machine	Stops all processes, which saves resources, and copies the contents of the virtual machine's memory to the virtual machine's .vmss file. Writing the memory to the .vmss file is useful if you need to copy the file to help with a troubleshooting scenario.
Put the guest operating system in standby mode and leave the virtual machine powered on	All processes stop running, but virtual devices remain connected.

4 Click **OK** to save your changes.


Configuring VMware Tools Options

Configure the VMware Tools options to define the power operations for the virtual machine, synchronize the virtual machine's time with the host, and decide when to run VMware Tools Scripts.

Configure the Virtual Machine Power States

Changing virtual machine power states is useful when you do maintenance on the host. You can use the system default settings for the virtual machine power controls, or you can configure the controls to interact with the guest operating system. For example, you can configure the **Power off** control to power off the virtual machine or shut down the guest operating system.

You can modify many virtual machine configurations while the virtual machine is running, but you might need to change the virtual machine power state for some configurations.

You cannot configure a **Power on** () action. This action powers on a virtual machine when a virtual machine is stopped, or resumes the virtual machine and runs a script when it is suspended and VMware Tools is installed and available. If VMware Tools is not installed, it resumes the virtual machine and does not run a script.

Prerequisites

- Verify that you have privileges to perform the intended power operation on the virtual machine.
- To set optional power functions, install VMware Tools in the virtual machine.
- Power off the virtual machine before editing the VMware Tools options.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 Click the **VM Options** tab and expand **VMware Tools**.
- 3 Select an option for the virtual machine **Power Off** () control from the drop-down menu.

Option	Description
Shut Down Guest	Uses VMware Tools to initiate an orderly system shut down of the virtual machine. Soft power operations are possible only if the tools are installed in the guest operating system.
Power Off	Immediately stops the virtual machine. A Power Off action shuts down the guest operating system or powers off the virtual machine. A message indicates that the guest operating system might not shut down properly. Use this power off option only when necessary.
Default (Shut Down Guest)	Follows system settings. The current value of the system settings appears in parentheses.

- 4 Select an option for the **Suspend** () control from the drop-down menu.

Option	Description
Suspend	Pauses all virtual machine activity. When VMware Tools is installed and available, a suspend action runs a script and suspends the virtual machine. If VMware Tools is not installed, a Suspend action suspends the virtual machine without running a script.
Default (Suspended)	Follows system settings. The current value of the system setting appears in parentheses.

- 5 Select an option for the **Reset**  control from the drop-down menu.

Option	Description
Restart Guest	Uses VMware Tools to initiate an orderly restart. Soft power operations are possible only if the tools are installed in the guest operating system.
Reset	Shuts down and restarts the guest operating system without powering off the virtual machine. If VMWare Tools is not installed, a Reset action resets the virtual machine.
Default (Restart Guest)	Follows system settings. The current value of the system setting appears in parentheses.

- 6 Click **OK** to save your changes.

Virtualization Based Security

Microsoft VBS, a feature of Windows 10 and Windows Server 2016 operating systems, uses hardware and software virtualization to enhance system security by creating an isolated, hypervisor-restricted, specialized subsystem. Starting with vSphere 6.7, you can enable Microsoft virtualization-based security (VBS) on supported Windows guest operating systems.

For more detailed information about VBS, see the *vSphere Security* documentation.

Enable Virtualization-based Security on an Existing Virtual Machine

You can enable Microsoft virtualization-based security (VBS) on existing virtual machines for supported Windows guest operating systems.

Enabling VBS is a process that involves first enabling VBS in the virtual machine then enabling VBS in the guest OS.

Note New virtual machines configured for Windows 10 and Windows Server 2016 on hardware versions less than version 14 are created using Legacy BIOS by default. If you change the virtual machine's firmware type from Legacy BIOS to UEFI, you must reinstall the guest operating system.

Prerequisites

Intel hosts are recommended. See the *vSphere Security* documentation for information about acceptable CPUs and VBS best practices.

The virtual machine must have been created using hardware version 14 or later, UEFI firmware, and one of the following supported guest operating systems:

- Windows 10 (64 bit)
- Windows Server 2016 (64 bit)

Procedure

- 1 In the vSphere Client, browse to the virtual machine.

- 2 Right-click the virtual machine and select **Edit Settings**.
- 3 Click the **VM Options** tab.
- 4 Check the **Enable** check box for Virtualization Based Security.
- 5 Click **OK**.

Confirm that the virtual machine's **Summary** tab displays "VBS true" in the Guest OS description.

What to do next

See [Enable Virtualization-based Security on the Guest Operating System](#).

Enable Virtualization-based Security on the Guest Operating System

You can enable Microsoft virtualization-based security (VBS) for supported Windows guest operating systems.

You enable VBS from within the Windows Guest OS. Windows configures and enforces VBS through a Group Policy Object (GPO). The GPO gives you the ability to turn off and on the various services, such as Secure Boot, Device Guard, and Credential Guard, that VBS offers. Certain Windows versions also require you to perform the additional step of enabling the Hyper-V platform.

See Microsoft's documentation about deploying Device Guard to enable virtualization-based security for details.

Prerequisites

- Ensure that virtualization-based security has been enabled on the virtual machine.

Procedure

- 1 In Microsoft Windows, edit the group policy to turn on VBS and choose other VBS-related security options.
- 2 (Optional) For Microsoft Windows versions less than Redstone 4, in the Windows Features control panel, enable the Hyper-V platform.
- 3 Reboot the guest operating system.

Disable Virtualization-based Security

If you no longer use virtualization-based security (VBS) with a virtual machine, you can disable VBS. When you disable VBS for the virtual machine, the Windows VBS options remain unchanged but might induce performance issues. Before disabling VBS on the virtual machine, disable VBS options within Windows.

Prerequisites

Ensure that the virtual machine is powered off.

Procedure

- 1 In the vSphere Client, browse to the VBS-enabled virtual machine.
See [Identify VBS-Enabled Virtual Machines](#) for help in locating VBS-enabled virtual machines.
- 2 Right-click the virtual machine and select **Edit Settings**.
- 3 Click **VM Options**.
- 4 Deselect the **Enable** check box for Virtualization Based Security.
A message reminds you to disable VBS in the guest OS.
- 5 Click **OK**.
- 6 Verify that the virtual machine's **Summary** tab no longer displays "VBS true" in the Guest OS description.

Identify VBS-Enabled Virtual Machines

You can identify which of your virtual machines have VBS enabled, for reporting and compliance purposes.

Procedure

- 1 Connect to vCenter Server by using the vSphere Client.
- 2 Select a vCenter Server instance, a data center, or a host in the inventory.
- 3 Click the **VMs** tab and click **Virtual Machines**.
- 4 In the list of virtual machines, click the down arrow in a column header to show/hide columns, and select the **VBS** check box.
The **VBS** column appears.
- 5 Scan for Present in the **VBS** column.

Configuring Virtual Machine Boot Options

Edit Boot Options to enable or disable UEFI Secure Boot and configure the boot behavior of the virtual machine.

Enable or Disable UEFI Secure Boot for a Virtual Machine

UEFI Secure Boot is a security standard that helps ensure that your PC boots using only software that is trusted by the PC manufacturer. For certain virtual machine hardware versions and operating systems, you can enable secure boot just as you can for a physical machine.

In an operating system that supports UEFI secure boot, each piece of boot software is signed, including the bootloader, the operating system kernel, and operating system drivers. The virtual machine's default configuration includes several code signing certificates.

- A Microsoft certificate that is used only for booting Windows.

- A Microsoft certificate that is used for third-party code that is signed by Microsoft, such as Linux bootloaders.
- A VMware certificate that is used only for booting ESXi inside a virtual machine.

The virtual machine's default configuration includes one certificate for authenticating requests to modify the secure boot configuration, including the secure boot revocation list, from inside the virtual machine, which is a Microsoft KEK (Key Exchange Key) certificate.

In almost all cases, it is not necessary to replace the existing certificates. If you do want to replace the certificates, see the VMware Knowledge Base system.

VMware Tools version 10.1 or later is required for virtual machines that use UEFI secure boot. You can upgrade those virtual machines to a later version of VMware Tools when it becomes available.

For Linux virtual machines, VMware Host-Guest Filesystem is not supported in secure boot mode. Remove VMware Host-Guest Filesystem from VMware Tools before you enable secure boot.

Note If you turn on secure boot for a virtual machine, you can load only signed drivers into that virtual machine.

Prerequisites

You can enable secure boot only if all prerequisites are met. If prerequisites are not met, the check box is not visible in the vSphere Client.

- Verify that the virtual machine operating system and firmware support UEFI boot.
 - EFI firmware
 - Virtual hardware version 13 or later.
 - Operating system that supports UEFI secure boot.

Note You cannot upgrade a virtual machine that uses BIOS boot to a virtual machine that uses UEFI boot. If you upgrade a virtual machine that already uses UEFI boot to an operating system that supports UEFI secure boot, you can enable secure boot for that virtual machine.

- Turn off the virtual machine. If the virtual machine is running, the check box is dimmed.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 Click the **VM Options** tab, and expand **Boot Options**.
- 3 Under **Boot Options**, ensure that firmware is set to **EFI**.
- 4 Select your task. Select the **Secure Boot** check box to enable secure boot. and click **OK**.
 - Select the **Secure Boot** check box to enable secure boot.
 - Deselect the **Secure Boot** check box to disable secure boot.

When the virtual machine boots, only components with valid signatures are allowed. The boot process stops with an error if it encounters a component with a missing or invalid signature.

Delay the Boot Sequence

Delaying the boot operation is useful when you change BIOS or EFI settings such as the boot order. For example, you can change the BIOS or EFI settings to force a virtual machine to boot from a CD-ROM.

Prerequisites

- Verify that vSphere 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 In the Boot Delay section, select the time in milliseconds to delay the boot operation.
- 4 (Optional) In the Force EFI setup section, select whether to force entry into the BIOS or EFI setup screen the next time the virtual machine boots.
- 5 (Optional) In the Failed Boot Recovery section, select whether the virtual machine should reboot after a boot failure and enter the time in seconds.
- 6 Click **OK**.

Configuring Virtual Machine Advanced Options

You can edit the Advanced virtual machines settings when you need to solve issues caused by an application or when you need log files and debugging information for troubleshooting purposes. You can also add or change configuration parameters and change the latency sensitivity of a virtual machine.

Disable Virtual Machine Acceleration

When you install or run software in a virtual machine, the virtual machine appears to stop responding. The problem occurs early when you run an application. You can resolve the issue by temporarily disabling acceleration in the virtual machine.

The **Disable acceleration** option slows down virtual machine performance, so use it only to solve the issue caused by running the application. After the application stops encountering problems, deselect **Disable acceleration**. You might be able to run the application 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 Select **Disable acceleration**.

4 Click **OK**.

You can install or run the software successfully.

Enable Virtual Machine Logging

You can enable logging to collect log files to help troubleshoot problems with your virtual machine.

ESXi hosts store virtual machine log files in the same directory as the virtual machine's configuration files. By default, the log file name is `vmware.log`. Archived log files are stored as `vmware-n.log`, where *n* is a number in sequential order beginning with 1.

Prerequisites

Required privilege: **Virtual machine.Configuration.Settings**

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 Click the **VM Options** tab and expand **Advanced**.
- 3 In the Settings row, select **Enable logging** and click **OK**.

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

Configure Virtual Machine Debugging and Statistics

You can run a virtual machine so that it collects additional debugging information that is helpful to VMware technical support in resolving issues.

Prerequisites

Power off the virtual machine.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 Click the **VM Options** tab and expand **Advanced**.
- 3 Select a debugging and statistics option from the drop-down menu.
 - **Run normally**
 - **Record Debugging Information**
 - **Record Statistics**
 - **Record Statistics and Debugging Information**

The number of debugging and statistics options available depends on the host software type and version. On some hosts, some options are not available.

- 4 Click **OK**.

Change the Swap File Location

When a virtual machine is powered on, the system creates a VMkernel swap file to serve as a backing store for the virtual machine's RAM contents. You can accept the default swap file location or save the file to a different location. By default, the swap file is stored in the same location as the virtual machine's configuration file.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 Click the **VM Options** tab and expand **Advanced**.
- 3 Select a swap file location option.

Option	Description
Default	Stores the virtual machine swap file at the default location defined by the host or cluster swap file settings.
Always store with the virtual machine	Stores the virtual machine swap file in the same folder as the virtual machine configuration file.
Store in the host's swapfile datastore	If the host or cluster settings define a location for the swap file, this location is used. Otherwise, the swap file is stored with the virtual machine.

- 4 Click **OK**.

Edit Configuration File Parameters

You can change or add virtual machine configuration parameters when instructed by a VMware technical support representative, or if you see VMware documentation that instructs you to add or change a parameter to fix a problem with your system.

Important Changing or adding parameters when a system does not have problems might lead to decreased system performance and instability.

The following conditions apply:

- To change a parameter, you change the existing value for the keyword/value pair. For example, if you start with the keyword/value pair, keyword/value, and change it to keyword/value2, the result is keyword=value2.
- You cannot delete a configuration parameter entry.

Caution You must assign a value to configuration parameter keywords. If you do not assign a value, the keyword can return a value of 0, false, or disable, which can result in a virtual machine that cannot power on.

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.

- 2 Click the **VM Options** tab and expand **Advanced**.
- 3 Click **Edit Configuration**.
- 4 (Optional) To add a parameter, click **Add Row** and type a name and value for the parameter.
- 5 (Optional) To change a parameter, type a new value in the **Value** text box for that parameter.
- 6 Click **OK**.

Configure Fibre Channel NPIV Settings

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

Each virtual port is identified by a pair of world wide names (WWNs) that vCenter Server assigns. The pair consists of a world wide port name (WWPN) and a world wide node name (WWNN).

For detailed information on how to configure NPIV for a virtual machine, see the *vSphere Storage* documentation.

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 through their WWNs in order for the 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 on that host start using the WWNs of the 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 use 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 the **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 and the vSphere 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 or Add an Object to a vApp](#)
- [Edit vApp Settings](#)
- [Clone a vApp](#)
- [Perform vApp Power Operations](#)
- [Edit vApp Notes](#)
- [Add a Network Protocol Profile in the vSphere Web Client](#)
- [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 Start the **New vApp** wizard.

Client	Step
vSphere Client	Right-click an object that supports vApp creation and click New vApp .
vSphere Web Client	Right-click an object that supports vApp creation and click New vApp > New vApp ( .

- 2 On the Select creation type page, select **Create a new vApp** and click **Next**.
- 3 On the Select a name and location page, type a name for the vApp, select a location for the vApp, and click **Next**.
 - If you start the creation process from a folder or vApp, you are prompted for a host, cluster, or resource pool.
 - If you start the creation process from a resource pool, host, or cluster, you are prompted for a folder or data center.
- 4 Allocate CPU resources to the vApp.
 - In the vSphere Client, click the **Resources** tab and expand **CPU**.
 - In the vSphere Web Client, expand **CPU resources** under **Deployment**.

Option	Description
Shares	CPU shares for this vApp with respect to the parent's total. Sibling vApps share resources according to their relative share values bounded by the reservation and limit. Select Low , Normal , or High , which specify share values respectively in a 1:2:4 ratio. Select Custom to give each vApp a specific number of shares, which express a proportional weight.
Reservation	Guaranteed CPU allocation for this vApp.

Option	Description
Reservation Type	Select the Expandable check box to make the reservation expandable. When the vApp is powered on, if the combined reservations of its virtual machines are larger than the reservation of the vApp, the vApp can use resources from its parent or ancestors.
Limit	Upper limit for this vApp's CPU allocation. Select Unlimited to specify no upper limit.

5 Allocate memory resources to the vApp.

- In the vSphere Client, click the **Resources** tab and expand **Memory**.
- In the vSphere Web Client, expand **Memory resources** under **Deployment**.

Option	Description
Shares	Memory shares for this vApp with respect to the parent's total. Sibling vApps share resources according to their relative share values bounded by the reservation and limit. Select Low , Normal , or High , which specify share values respectively in a 1:2:4 ratio. Select Custom to give each vApp a specific number of shares, which express a proportional weight.
Reservation	Guaranteed memory allocation for this vApp.
Reservation Type	Select the Expandable check box to make the reservation expandable. When the vApp is powered on, if the combined reservations of its virtual machines are larger than the reservation of the vApp, the vApp can use resources from its parent or ancestors.
Limit	Upper limit for this vApp's memory allocation. Select Unlimited to specify no upper limit.

6 On the Ready to complete page, review the vApp settings and click **Finish**.

Create or Add an Object to a vApp

You can create a virtual machine, resource pool, or child vApp within a vApp. You can also add an existing object from the inventory, such as virtual machine or another vApp, to the vApp.

Procedure

- ◆ Select your task.
 - ◆ Create an object inside an existing vApp.

Client	Steps
vSphere Client	<p>Right-click a vApp in the inventory and from the Actions submenu, select a task.</p> <ul style="list-style-type: none"> ■ Click New Virtual Machine to create a new virtual machine within the vApp. ■ Click New Resource Pool to create a new resource pool within the vApp. ■ Click Deploy OVF Template to deploy an OVF template and add the corresponding virtual machine to the selected vApp.
vSphere Web Client	<p>Right-click a vApp in the inventory and from the Actions submenu, select a task.</p> <ul style="list-style-type: none"> ■ Click New Virtual Machine to create a new virtual machine within the vApp. ■ Click New vApp to create a child vApp within the vApp. ■ Click New Resource Pool to create a new resource pool within the vApp. ■ Click OVF Template > Deploy OVF Template to deploy an OVF template and add the corresponding virtual machine to the selected vApp.

- ◆ Add an existing object to a vApp.
 - a Navigate to an object in the inventory.
 - b Click and drag the object to the destination vApp.
 - c Release the mouse button.

If the move is not permitted, the object is not added to the vApp.

The new object appears as part of the vApp in the vApp inventory.

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 box, 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 in the vSphere Web Client](#)

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 in the vSphere Web Client](#)

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

- ◆ Right-click a vApp in the inventory and click **Edit Settings**.

Client	Description
vSphere Client	<p>In the vSphere Client, you can change the following settings.</p> <ul style="list-style-type: none"> ■ On the Resources tab, you can edit CPU and memory settings, such as shares, reservation, and limit. ■ On the Start Order tab, you can set and edit the start order of the virtual machines. ■ On the IP Allocation tab, you can specify IP protocol and choose an IP allocation scheme. ■ On the Details tab, you can view product information, such as name, vendor, product URL, and vendor URL.
vSphere Web Client	<p>In the vSphere Web Client, you can change the following settings.</p> <ul style="list-style-type: none"> ■ The Application properties section displays non-editable product information, such as name, vendor, and version, and allows specifying values for vApp custom properties. ■ In the Deployment section, you can specify CPU and memory resources, and you can also configure IP allocation. The available allocation schemes and protocols depend on the vApp configuration. You can modify the configuration in the Authoring section. ■ In the Authoring section, you can specify the vApp product information and you can change 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 box, 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.

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 Right-click a vApp in the inventory and click **Edit 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 Right-click a vApp in the inventory and click **Edit Settings**.

2 Allocate CPU resources to the vApp.

- In the vSphere Client, click the **Resources** tab and expand **CPU**.
- In the vSphere Web Client, expand **CPU resources** under **Deployment**.

Option	Description
Shares	CPU shares for this vApp with respect to the parent's total. Sibling vApps share resources according to their relative share values bounded by the reservation and limit. Select Low , Normal , or High , which specify share values respectively in a 1:2:4 ratio. Select Custom to give each vApp a specific number of shares, which express a proportional weight.
Reservation	Guaranteed CPU allocation for this vApp.
Reservation Type	Select the Expandable check box to make the reservation expandable. When the vApp is powered on, if the combined reservations of its virtual machines are larger than the reservation of the vApp, the vApp can use resources from its parent or ancestors.
Limit	Upper limit for this vApp's CPU allocation. Select Unlimited to specify no upper limit.

3 Allocate memory resources to the vApp.

- In the vSphere Client, click the **Resources** tab and expand **Memory**.
- In the vSphere Web Client, expand **Memory resources** under **Deployment**.

Option	Description
Shares	Memory shares for this vApp with respect to the parent's total. Sibling vApps share resources according to their relative share values bounded by the reservation and limit. Select Low , Normal , or High , which specify share values respectively in a 1:2:4 ratio. Select Custom to give each vApp a specific number of shares, which express a proportional weight.
Reservation	Guaranteed memory allocation for this vApp.
Reservation Type	Select the Expandable check box to make the reservation expandable. When the vApp is powered on, if the combined reservations of its virtual machines are larger than the reservation of the vApp, the vApp can use resources from its parent or ancestors.
Limit	Upper limit for this vApp's memory allocation. Select Unlimited to specify no upper limit.

4 Click **OK**.

View Unrecognized OVF Sections in the vSphere Web Client

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 Right-click a vApp in the inventory and click **Edit 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 Right-click a vApp in the inventory and click **Edit Settings**.
- 2 Select an IP allocation scheme.
 - In the vSphere Client, click the **IP Allocation** tab of the **Edit vApp** wizard.
 - In the vSphere Web Client, expand **IP allocation** under **Deployment**.

Option	Description
Static - Manual	IP addresses are manually configured. No automatic allocation is performed.
Transient - IP Pool	IP addresses are automatically allocated using IP pools from a specified range when the vApp is powered on. The IP addresses are released when the appliance is powered off.
DHCP	A DHCP server is used to allocate the IP addresses. The addresses assigned by the DHCP server are visible in the OVF environments of virtual machines started in the vApp.
Static - IP Pool	IP addresses are automatically allocated from the managed IP network range of vCenter Server at power-on, and remain allocated at power-off.

Static - IP Pool and Transient - IP Pool have in common that IP allocation is done through the range managed by the vSphere platform as specified by the IP pool range in a network protocol profile. The difference is that for a static IP Pool, the IP addresses are allocated at first power-on and remain allocated, while for a transient IP Pool, the IP addresses are allocated when needed, typically at power-on, but released during power-off.

- 3 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 Right-click a vApp in the inventory and click **Edit Settings**.
- 2 Configure the start order for the virtual machines.
 - In the vSphere Client, click the **Start Order** tab.
 - In the vSphere Web Client, expand **Start order** under **Authoring**.
- 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 in the vSphere Web Client

You can configure product and vendor information for a vApp.

Prerequisites

Required privilege: **vApp.vApp application configuration** on the vApp.

Procedure

- 1 Right-click a vApp in the inventory and click **Edit Settings**.
- 2 In the Authoring section, click the **Product** triangle to expand the product options.
- 3 Set and configure the settings that appear on the summary page of the virtual machine.

vApp Setting	Description
Product Name	Product Name.
Version	vApp version.

vApp Setting	Description
Full Version	Full version of the vApp.
Product URL	If you enter a product URL, a user can click the product name on the virtual machine summary page and go to the product's web page.
Vendor URL	If you enter a vendor URL, a user can click the vendor name on the virtual machine summary page and go to the vendor's web page.
Application URL	From the vSphere Web Client and the vSphere Client, you can access the vApp summary page. The Summary page includes a Status pane that includes information about vApp status, for example Running or Stopped . If you enter a valid application URL, the virtual machine Status pane displays Available instead of Running . The Available text is also a link to the application URL.

If you configure the virtual machine to use the property called *webserver_ip* and the virtual machine has a web server at the address represented by the property, you can enter **http://{webserver_ip}/** as the **Application URL**.

- 4 (Optional) Click **View** to test the **Product URL** and **Vendor URL**.
- 5 Click **OK**.

View vApp License Agreement

You can view the license agreement for the vApp that you are editing.

Note This option is available only if the vApp was imported from an OVF that includes a license agreement.

Prerequisites

Required privilege: **vApp.vApp application configuration** on the vApp.

Procedure

- 1 On the Summary page of the vApp, click **Edit Settings**.
- 2 Click **View License Agreement** in the Options list.
- 3 Click **OK**.

Clone a vApp

Cloning a vApp is similar to cloning a virtual machine. When you clone a vApp, you clone all virtual machines and vApps in the vApp.

Prerequisites


When you clone a vApp, you can add the clone to a folder, standalone host, resource pool, cluster enabled for DRS, or another vApp.

Verify that one of those objects is available in your datacenter.

- A standalone host that is running ESX 3.0 or greater.

- A cluster enabled for DRS is selected.

Procedure

- 1 Navigate to a DRS-enabled cluster, right-click the cluster and click **New vApp > New vApp** (.
- 2 On the Select a creation type page, select **Clone an existing vApp**.
- 3 On the Select source vApp page, select an existing vApp to clone, and click **Next**.
- 4 On the Select destination page, select a valid host, vApp, or resource pool in which to run the vApp, and click **Next**.
- 5 On the Select a name and location page, type a name for the vApp, select location, and click **Next**.
- 6 On the Select storage page, select the virtual disk format and the target datastore and click **Next**.
- 7 On the Resource allocation page, allocate CPU and memory resources for the vApp and click **Next**.
- 8 On the Ready to complete page, 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.

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

Prerequisites depend on the task that you want to perform.

Task	Required Privileges
Power on a vApp	vApp.Power On on the vApp.
Power off a vApp	vApp.Power Off on the vApp.
Suspend a vApp.	vApp.Suspend

Procedure

- 1 Navigate to a vApp in the inventory.

2 Select one of the power operation options.

Task	Action
Power on	<p>Right-click the vApp and select Power > Power On .</p> <p>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.</p> <p>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.</p>
Power off	<p>Right-click the vApp and select Power > Power Off</p> <p>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.</p> <p>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.</p>
Suspend	<p>Right-click the vApp and select Power > Suspend.</p> <p>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.</p>
Resume	<p>Right-click a vApp that is powered off or suspended and select Power On.</p> <p>Virtual machines are resumed according to their startup order configuration.</p>

In the **Summary** tab, the **Status** indicates the vApp status.

Edit vApp Notes

You can add or edit notes for a particular vApp.

Procedure

- 1 Right-click a vApp in the inventory and select **Edit Notes**.
- 2 Type your comments in the **Edit Notes** window.
- 3 Click **OK**.

Your comments appear in the Summary tab for the vApp.

Add a Network Protocol Profile in the vSphere Web Client

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.

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.

Network protocol profiles also contain settings for the IP subnet, DNS, and HTTP proxy server.

Note If you move a vApp or a virtual machine that retrieves its network settings from a protocol profile to another data center, to power on the vApp or virtual machine you must assign a protocol profile to the connected port group on the destination data center.

Procedure

1 Associate a Port Group with a Network Protocol Profile

To apply the range of IP addresses from a network protocol profile to a virtual machine that is a part of a vApp or has vApp functionality enabled, associate the profile with a port group that controls the networking of the virtual machine.

2 Configure a Virtual Machine or vApp to Use a Network Protocol Profile

After you associate a protocol profile to a port group of a standard switch or a distributed switch, enable the usage of profile on a virtual machine that is connected to the port group and is associated with a vApp or has the vApp options enabled.

Procedure

1 Navigate to a data center that is associated with the vApp and click the **Configure** tab.

2 Click **Network Protocol Profiles**

Existing network protocol profiles are listed.

3 Click the Add icon (+) to add a new network protocol profile.

The **Add Network Protocol Profile** wizard opens.

4 On the Select name and network page, type the name of the network protocol profile and select the networks that use this profile. Click **Next**.

A network can be associated with one network protocol profile at a time.

5 On the Configure IPv4 page, specify the relevant IPv4 configuration.

- a In the **Subnet** and the **Gateway** fields, enter the IP subnet and gateway.
- b Select the **DHCP Present** check box to indicate that the DHCP server is available on this network.
- c In the **DNS server addresses**, enter the DNS server information.
- d Select the **Enable IP Pool** check box to specify an IP pool range.

- e 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, **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.

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.

- f Click **Next**.

6 On the Configure IPv6 page, specify the relevant IPv6 configuration.

- a In the **Subnet** and the **Gateway** fields, enter the IP subnet and gateway.
- b Select the **DHCP Present** check box to indicate that the DHCP server is available on this network.
- c In the **DNS server addresses**, enter the DNS server information.
- d Select the **Enable IP Pool** check box to specify an IP pool range.
- e 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.

- f Click **Next**.

7 On the Set other network configurations page, specify additional network configurations.

- a Enter the DNS domain.
- b Enter the host prefix.
- c Enter the DNS search path.

The search paths are specified as a list of DNS domains separated by commas, semi-colons, or spaces.

- d 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.

- e Click **Next**.

- 8 On the ready to complete page, review the settings and click **Finish**.

What to do next

You can now associate a port group with a network protocol profile. For more details, see [Associate a Port Group with a Network Protocol Profile](#).

Associate a Port Group with a Network Protocol Profile

To apply the range of IP addresses from a network protocol profile to a virtual machine that is a part of a vApp or has vApp functionality enabled, associate the profile with a port group that controls the networking of the virtual machine.

You can associate a port group of a standard switch or a distributed port group of a distributed switch with a network protocol profile by using the settings of the group.

Procedure

- 1 Navigate to a distributed port group of a vSphere Distributed Switch or to a port group of a vSphere Standard Switch in the Networking view of the vSphere Web Client.

The port groups of standard switches are under the data center. The vSphere Web Client displays distributed port groups under the parent distributed switch object.

- 2 On the **Configure** tab, expand **More** and click **Network Protocol Profiles**.
- 3 Click **Associate a network protocol profile with the selected network** button in the upper right corner.
- 4 On the Set association type page of the **Associate Network Protocol Profile** wizard, select **Use an existing network protocol profile** and click **Next**.

If the existing network protocol profiles do not contain settings suitable for the vApp virtual machines in the port group, you must create a new profile.

- 5 Select the network protocol profile and click **Next**.
- 6 Examine the association and settings of the network protocol profile, and click **Finish**.

Configure a Virtual Machine or vApp to Use a Network Protocol Profile

After you associate a protocol profile to a port group of a standard switch or a distributed switch, enable the usage of profile on a virtual machine that is connected to the port group and is associated with a vApp or has the vApp options enabled.

Prerequisites

Verify that the virtual machine is connected to a port group that is associated with the network protocol profile.

Procedure

- 1 Navigate to the virtual machine or the vApp.
- 2 Open the settings of the vApp or the **vApp Options** tab of the virtual machine.
 - Right-click a vApp and select **Edit settings**.
 - Right-click a virtual machine, select **Edit settings**, and in the Edit Settings dialog box, click the **vApp Options** tab.
- 3 Click **Enable vApp options**.
- 4 Under Authoring, expand **IP allocation** and set the IP allocation scheme to **OVF environment**.
- 5 Under Deployment, expand **IP allocation** and set **IP allocation** to **Transient - IP Pool** or **Static - IP Pool**.

Both the **Static - IP Pool** and **Transient - IP Pool** options allocate an IP address from the range in the network protocol profile that is associated with the port group. If you select **Static - IP Pool**, the IP address is assigned the first time the virtual machine or vApp is powered. The assigned IP 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.

Important If the virtual machine is connected to a distributed switch and has the vApp option enabled, you cannot select any of the following **Dynamic property** options: IP address, Subnet, Netmask, Gateway, Domain name, HTTP Proxy, Host prefix, DNS servers, DNS search path, Network name.

- 6 Click **OK**.

When the virtual machine is powered on, the adapters connected to the port group receive IP addresses from the range in the protocol profile. When the virtual machine is powered off, the IP addresses are released.

Virtual Machine vApp Options

When you edit the settings for a virtual machine, you can enable vApp options. When vApp options are enabled, you can configure OVF properties, use the OVF environment, and specify IP allocation and product information for the virtual machine.

Enable Virtual Machine vApp Options in the vSphere Web Client

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 in the vSphere Web Client

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 Click the **Enable vApp options** check box.
- 4 If the OVF template included editable application properties, make changes if necessary.
- 5 If the OFV template includes information that vCenter Server cannot process, you can view that information under Unrecognized OVF Sections.
- 6 If the OVF template included editable IP allocation options, make changes if necessary.

Option	Description
Static - Manual	IP addresses are manually configured. No automatic allocation is performed.
Transient - IP Pool	IP addresses are automatically allocated using IP pools from a specified range when the vApp is powered on. The IP addresses are released when the appliance is powered off.

Option	Description
DHCP	A DHCP server is used to allocate the IP addresses. The addresses assigned by the DHCP server are visible in the OVF environments of virtual machines started in the vApp.
Static - IP Pool	IP addresses are automatically allocated from the managed IP network range of vCenter Server at power-on, and remain allocated at power-off.

Static - IP Pool and Transient - IP Pool have in common that IP allocation is done through the range managed by the vSphere platform as specified by the IP pool range in a network protocol profile. The difference is that for a static IP Pool, the IP addresses are allocated at first power-on and remain allocated, while for a transient IP Pool, the IP addresses are allocated when needed, typically at power-on, but released during power-off.

Edit OVF Authoring Options for a Virtual Machine

You can use the OVF Authoring options that are included in a virtual machine's vApp options to specify custom information that is included when you export the virtual machine as an OVF template.

vApp properties are a central concept of vApp deployment and self configuration; they can turn a general OVF package into a running vApp instance with a custom configuration.

The set of properties associated to a running vApp is determined by the OVF package from which the vApp was deployed.

- When an OVF package is created the author adds the set of properties necessary for the vApp to function in an unknown environment. This could for instance be properties containing network configuration, a property containing the email address of the system administrator or a property containing the number of expected users of the vApp.
- Some property values are entered by the user when the vApp is deployed, while other property values are configured by vCenter Server when the vApp is powered on. How this is handled depends on the property type and vCenter Server configuration.

When vCenter Server powers on a vApp, it creates an XML document that contains all properties and their values. This document is made available to each virtual machine in the vApp, and allows the virtual machines to apply the properties to their own environment.

1 [Edit vApp Product Information for a Virtual Machine in the vSphere Web Client](#)

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 in the vSphere Web Client](#)

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 in the vSphere Web Client](#)

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

4 Edit OVF Settings for a Virtual Machine in the vSphere Web Client

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 in the vSphere Web Client

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 Click the **Enable vApp options** check box.
- 4 In the Authoring section select **Product**.
- 5 Set and configure the settings that appear on the summary page of the virtual machine.

vApp Setting	Description
Product Name	Product Name.
Version	vApp version.
Full Version	Full version of the vApp.
Product URL	If you enter a product URL, a user can click the product name on the virtual machine summary page and go to the product's web page.
Vendor URL	If you enter a vendor URL, a user can click the vendor name on the virtual machine summary page and go to the vendor's web page.
Application URL	From the vSphere Web Client and the vSphere Client, you can access the vApp summary page. The Summary page includes a Status pane that includes information about vApp status, for example Running or Stopped . If you enter a valid application URL, the virtual machine Status pane displays Available instead of Running. The Available text is also a link to the application URL.

If you configure the virtual machine to use the property called *webserver_ip* and the virtual machine has a web server at the address represented by the property, you can enter **http://\${webserver_ip}/** as the **Application URL**.

- 6 Click **OK**.

Manage vApp Custom Properties for a Virtual Machine in the vSphere Web Client

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 are 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 in the vSphere Web Client](#).
 - 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 Click the **Enable vApp options** check box.
- 4 In the Authoring section, click **Properties**.

You can select and edit or delete an existing property, or create a new custom property.

- 5 To create a property, click **New**.
- 6 Specify property fields.
- 7 Click **OK**.

Edit vApp IP Allocation Policy for a Virtual Machine in the vSphere Web Client

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 Select **Enable vApp options**.
- 4 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.

- 5 Select a network configuration scheme.

Option	Description
OVF environment	Determined by the environment in which you deploy the OVF template.
DHCP	The IP addresses are allocated using DHCP when the virtual machine is powered on.

- 6 Choose the IP protocol that this vApp supports: IPv4, IPv6, or both.

- 7 Click **OK**.

Edit OVF Settings for a Virtual Machine in the vSphere Web Client

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 Select **Enable vApp options**.
- 4 In the Authoring section, click **OVF Settings**.
- 5 View and specify the settings.

Option	Description
OVF environment	Click View to display the OVF environment settings in XML format. The settings are not available when the virtual machine is powered off.
OVF environment transport	<ul style="list-style-type: none">■ If you select ISO image, an ISO image that contains the OVF template information is mounted in the CD-ROM drive.■ If you select VMware Tools, the VMware Tools <code>guestInfo.ovfEnv</code> variable is initialized with the OVF environment document.
Installation boot	If you click Enable, the virtual machine is reboots after OVF deployment completes. You can select the amount of time before the virtual machine starts the reboot operation.

- 6 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.

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 in the vSphere Web Client](#)
- [Monitoring Agents](#)

View Solutions in the vSphere Web Client

You can deploy, monitor, and interact with solutions that are installed in a vCenter Server instance with the vCenter Solutions Manager. The Solutions Manager displays information about the health of a solution.

You can navigate to the Solutions Manager from the home page of the vSphere Web Client. The Solutions Manager view displays information about the solution, such as the solution name, the vendor name and the version of the product.

Procedure

- 1 From the vSphere Web Client home page, navigate to the Solutions Manager by selecting **Administration > Solutions > vCenter Server Extensions**.
- 2 Double-click a solution.
- 3 In the Solutions Manager inventory, navigate through the tabs to view information about a solution..
 - **Summary** tab. Lists information about the solution, such as the product name, a short description, and a link to the vendor Web sites.

Selecting the vendor Web site link takes you to the Summary page of the virtual machine or vApp. A link under "Managed by" returns you to the solution.
 - **VMs** tab. Lists all the virtual machines belonging to the solution.
 - **Monitor** tab. Shows tasks and events related with the solution.

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.

Managing Virtual Machines

You can manage individual virtual machines or a group of virtual machines that belongs to a host or cluster.

From the virtual machine's 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:

- [Installing a Guest Operating System](#)
- [Customizing Guest Operating Systems](#)
- [Edit Virtual Machine Startup and Shutdown Settings in the vSphere Web Client](#)
- [Edit Virtual Machine Startup and Shutdown Settings](#)
- [Install the VMware Enhanced Authentication Plug-in](#)
- [Using a Virtual Machine Console](#)
- [Answer Virtual Machine Questions](#)
- [Removing and Reregistering VMs and VM Templates](#)
- [Managing Virtual Machine Templates](#)
- [Using Snapshots To Manage Virtual Machines](#)
- [Enhanced vMotion Compatibility as a Virtual Machine Attribute](#)
- [Migrating Virtual Machines](#)

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](#).

Prerequisites

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

Alternatively, verify that an ISO image is present in a content library.

- Verify that you have the installation instructions that the operating system vendor provides.

Procedure

- 1 Log in to the vCenter Server system or host on which the virtual machine resides.

2 Select an installation method.

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

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

A green right arrow appears next to the virtual machine icon in the inventory list.

4 Follow the installation instructions that the operating system vendor provides.

What to do next

Install VMware Tools. VMware highly recommends running the latest version of VMware Tools on your guest operating systems. Although the guest operating system can run without VMware Tools, you lose important functionality and convenience without them. See [Chapter 10 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

Required privileges:

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

Procedure

- 1 In the inventory, click **Storage** and select the datastore from the inventory to which you will upload the file.
- 2 (Optional) On the **Files** tab, click the **New Folder** icon to create a new folder.
- 3 Select an existing folder or the folder that you created, and click the **Upload Files** icon.

- 4 On the local computer, find the file and upload it.
ISO upload times vary, depending on file size and network upload speed.
- 5 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.

Customizing Guest Operating Systems

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

Customizing guest operating systems helps prevent conflicts that occur if virtual machines with identical settings are deployed, for example conflicts due to duplicate computer names. You can apply customization as part of virtual machine deployment or later.

- During the cloning or deployment process, you can specify customization settings, your you can select an existing customization spec.
- You can create a customization spec explicitly from the **Policies and Profiles** UI and apply it to a VM.

Guest Operating System Customization Requirements

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

VMware Tools Requirements

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

Virtual Disk Requirements

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

Windows Requirements

Customization of Windows guest operating systems requires the virtual machine to be running on an ESXi host running version 3.5 or later.

Linux Requirements

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

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

Instead of entering computer names and IP addresses for virtual NICs when you customize guest operating systems, you can create a custom application and configure it in such a way that vCenter Server generates 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, every time you initiate a guest operating system customization for a virtual machine, vCenter Server runs 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 **Configure** tab, click **Settings**, and click **Advanced Settings**.
- 4 Click **Edit** and enter the configuration parameters for the script.
 - a In the **Key** text box, type `config.guestcust.name-ip-generator.arg1`.
 - b In the **Value** text box, type `c:\sample-generate-name-ip.pl` and click **Add**.
 - c In the **Key** text box, type `config.guestcust.name-ip-generator.arg2`.
 - d In the **Value** text box, type the path to the script file on the vCenter Server system and click **Add**. For example, type `c:\sample-generate-name-ip.pl`.
 - e In the **Key** text box, type `config.guestcust.name-ip-generator.program`.
 - f In the **Value** text box, type `c:\perl\bin\perl.exe` and click **Add**.

5 Click **OK**.

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

Customize Windows During Cloning or Deployment 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](#).
- start the **Guest Customization** wizard when you clone a virtual machine or deploy one from a template.

Procedure

- 1 Start the **New VM Guest Customization Spec** wizard from the **Clone Existing Virtual Machine** wizard or the **Deploy From Template** wizard.
 - a Follow the prompts until you reach the Select clone options page.
 - b On the Select clone options page, select the **Customize the operating system** check box and click **Next**.
 - c On the Customize guest OS page, click the **Create a new specification** icon (.
- 2 On the Specify Properties page, enter a customization specification name and, optionally, a description.
- 3 On the Set Registration Information page, type the name and the organization of the virtual machine owner and click **Next**.

- 4 On the Computer Name page, enter a computer name for the guest operating system.

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

Option	Action
Enter a name	<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 the Append a numeric value check box. 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>
Use the virtual machine name	The computer name that vCenter Server creates is identical to the name of the virtual machine on which the guest operating system is running. If the name exceeds 63 characters, it is truncated.
Enter a name in the Clone/Deploy wizard	You are prompted to enter a name after the cloning or deployment is complete.
Generate a name using the custom application configured with vCenter Server	Enter a parameter that can be passed to the custom application.

- 5 On the Enter Windows License page, provide licensing information for the Windows operating system and click **Next**.

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

- 6 On the Administrator password page, 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) Select the **Automatically logon as Administrator** check box to log users in to the guest operating system as Administrator, and select the number of times to log in automatically.

- 7 On the Time Zone page, select the time zone for the virtual machine and click **Next**.

- 8 (Optional) On the Commands to run once page, specify commands to run the first time a user logs in to the guest operating system and click **Next**.

See the Microsoft Sysprep documentation for information about RunOnce commands.

- 9 On the Network page, select the type of network settings to apply to the guest operating system.

Option	Description
Use standard network settings for the guest operating system, including enabling DHCP on all network interfaces	vCenter Server configures all network interfaces from a DHCP server using default settings.
Manually select custom settings	You can specify the IP address and other network settings for each network interface in the virtual machine.

- 10 If you chose to manually configure network settings, select a NIC from the list and edit its network settings.
 - a Click the **Edit the selected adapter** icon (✎).

The **Edit Network** wizard opens.
 - b Click **IPv4** to specify IPv4-related settings.
 - Select **Use DHCP to obtain an IP address automatically** if you want to use DHCP.
 - Select **Prompt the user for an address when the specification is used** if you want vCenter Server to prompt you to enter an IP address. You can enter either an IPv4 or an IPv6 address.
 - Select **Use the following IP address** to enter the IPv4 address setting manually.

- c Click **IPv6** to configure the virtual machine to use IPv6 network.
 - Select **Do not use IPv6** if you do not want to use IPv6.
 - Select the **Use DHCP to obtain an IP address automatically** option if you want to use DHCP.
 - Select **Prompt the user for an address when the specification is used** if you want vCenter Server to prompt you to enter an IP address. You can enter either an IPv4 or an IPv6 address.
 - Select **Use the following IPv6 addresses** to choose an IPv6 address from the list. You can also add IPv6 addresses manually.
 - Click the **Add** icon to enter additional IPv6 addresses.
 - In the TCP/IP Address dialog box, specify the full IP address and the subnet mask prefix.

You can shorten the IP address by using zero compression and zero suppression. You must specify at least one IPv6 address.

The prefix length must be between 1 to 128, and the default value is 64.

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

Note Gateway is enabled by default, except when you select the **Do not use IPv6** option.

- d Click **DNS** to specify a DNS server address.
 - e Click **WINS** to specify primary and secondary WINS information.
 - f Click **OK** to save the configuration settings and exit the **Edit Network** wizard
- 11 On the Workgroup or domain page, select how the virtual machine will participate in the network and click **Next**.

Option	Action
Workgroup	Type a workgroup name. For example, MSHOME .
Windows Server Domain	<ul style="list-style-type: none"> 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 On the Set Operating System Options page, select **Generate New Security ID (SID)** and click **Next**.

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

- 13 On the Ready to complete page, review the details and click **Finish** to save your changes and return to the **Clone Existing Virtual Machine** wizard or the **Deploy From Template** wizard.

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 certain Windows operating systems 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-vmc. 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](#).

Procedure

- 1 Start the **New VM Guest Customization Spec** wizard from the **Clone Existing Virtual Machine** wizard or the **Deploy From Template** wizard.
 - a Follow the prompts until you reach the Select clone options page.
 - b On the Select clone options page, select the **Customize the operating system** check box and click **Next**.
 - c On the Customize guest OS page, click the **Create a new specification** icon (). Alternatively, you can select a customization specification from the list and click the **Create a new specification from existing one** icon (.

- 2 On the Computer Name page, enter a computer name for the guest operating system.

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

Option	Action
Enter a name	<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 the Append a numeric value check box. 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>
Use the virtual machine name	The computer name that vCenter Server creates is identical to the name of the virtual machine on which the guest operating system is running. If the name exceeds 63 characters, it is truncated.
Enter a name in the Clone/Deploy wizard	You are prompted to enter a name after the cloning or deployment is complete.
Generate a name using the custom application configured with vCenter Server	Enter a parameter that can be passed to the custom application.

- 3 Enter the **Domain Name** for the computer and click **Next**.
- 4 On the Time Zone page, select the time zone for the virtual machine and click **Next**.
- 5 On the Network page, select the type of network settings to apply to the guest operating system.

Option	Description
Use standard network settings for the guest operating system, including enabling DHCP on all network interfaces	vCenter Server configures all network interfaces from a DHCP server using default settings.
Manually select custom settings	You can specify the IP address and other network settings for each network interface in the virtual machine.

- 6 If you chose to manually configure network settings, select a NIC from the list and edit its network settings.

- a Click the **Edit the selected adapter** icon (✎).

The **Edit Network** wizard opens.

- b Click **IPv4** to specify IPv4-related settings.

- Select **Use DHCP to obtain an IP address automatically** if you want to use DHCP.
- Select **Prompt the user for an address when the specification is used** if you want vCenter Serve to prompt you to enter an IP address. You can enter either an IPv4 or an IPv6 address.
- Select **Use the following IP address** to enter the IPv4 address setting manually.

- c Click **IPv6** to configure the virtual machine to use IPv6 network.

- Select **Do not use IPv6** if you do not want to use IPv6.
- Select the **Use DHCP to obtain an IP address automatically** option if you want to use DHCP.
- Select **Prompt the user for an address when the specification is used** if you want vCenter Serve to prompt you to enter an IP address. You can enter either an IPv4 or an IPv6 address.
- Select **Use the following IPv6 addresses** to choose an IPv6 address from the list. You can also add IPv6 addresses manually.
 - Click the **Add** icon to enter additional IPv6 addresses.
 - In the TCP/IP Address dialog box, specify the full IP address and the subnet mask prefix.

You can shorten the IP address by using zero compression and zero suppression. You must specify at least one IPv6 address.

The prefix length must be between 1 to 128, and the default value is 64.

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

Note Gateway is enabled by default, except when you select the **Do not use IPv6** option.

- d Click **DNS** to specify a DNS server address.
- e Click **WINS** to specify primary and secondary WINS information.
- f Click **OK** to save the configuration settings and exit the **Edit Network** wizard.

- 7 On the Enter DNS and Domain Settings page, enter the DNS and domain information.

The **Primary DNS**, **Secondary DNS**, and **Tertiary DNS** fields accept both IPv4 and IPv6 addresses.

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

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

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

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

What to do next

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

Apply a Customization Specification to a Virtual Machine

You can apply a customization spec to an existing virtual machine. Using customization specs helps prevent conflicts that can result if you deploy virtual machines with identical settings, such as duplicate computer names.

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

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

Prerequisites

- Verify the guest operating system is installed.
- Verify that VMware Tools is installed and running.
- Power off the virtual machine.

Procedure

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

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

3 Click **Finish**.

Creating and Managing Customization Specifications

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

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

Create a Customization Specification for Linux

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

Prerequisites

Ensure that all requirements for customization are met. See [Guest Operating System Customization Requirements](#).

Procedure

- 1 Select **Menu > Policies and Profiles**, and under Policies and Profiles, click **VM Customization Specifications**.

- 2 Click the **Create a new specification** icon.

The **New VM Guest Customization Spec** wizard opens.

- 3 On the Name and target OS page, enter a name and description for the customization specification and select **Linux** as a target guest OS. Click **Next**.

- 4 On the Computer Name page, enter a computer name for the guest operating system.

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

Option	Action
Enter a name	<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 the Append a numeric value check box. 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>
Use the virtual machine name	The computer name that vCenter Server creates is identical to the name of the virtual machine on which the guest operating system is running. If the name exceeds 63 characters, it is truncated.
Enter a name in the Clone/Deploy wizard	You are prompted to enter a name after the cloning or deployment is complete.
Generate a name using the custom application configured with vCenter Server	Enter a parameter that can be passed to the custom application.

- 5 Enter the **Domain Name** for the computer and click **Next**.
- 6 On the Time Zone page, select the time zone for the virtual machine and click **Next**.
- 7 On the Network page, select the type of network settings to apply to the guest operating system.

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

The **Edit Network** dialog box opens.

- 8 Click **IPv4** and specify IPv4-related settings and subnet and gateway details.
- Select **Use DHCP to obtain an IP address automatically** if you want to use DHCP.
 - Select **Prompt the user for an address when the specification is used** if you want vCenter Serve to prompt you to enter an IP address. You can enter either an IPv4 or an IPv6 address.
 - Select **Use custom settings** to enter the IPv4 address setting manually.
- 9 Click **IPv6** to configure the virtual machine to use IPv6 network.
- Select **Do not use IPv6** if you do not want to use IPv6.
 - Select the **Use DHCP to obtain an IP address automatically** option if you want to use DHCP.

- Select **Prompt the user for an address when the specification is used** if you want vCenter Serve to prompt you to enter an IP address. You can enter either an IPv4 or an IPv6 address.
- Select **Use the following IPv6 addresses** to choose an IPv6 address from the list. You can also add IPv6 addresses manually.

Gateway is enabled by default, except when you choose **Do not use IPv6**

- 10 On the DNS settings page, enter DNS and domain settings information. The **Primary DNS**, **Secondary DNS**, and **Tertiary DNS** fields accept both IPv4 and IPv6 addresses.
- 11 On the Ready to complete page, review the details and click **Finish** to save your changes.

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

Create a Customization Specification for Windows

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

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

Prerequisites

Ensure that all requirements for customization are met. See [Guest Operating System Customization Requirements](#).

Procedure

- 1 Select **Menu > Policies and Profiles**, and under Policies and Profiles, click **VM Customization Specifications**.

- 2 Click the **Create a new specification** icon.

The **New VM Guest Customization Spec** wizard opens.

- 3 On the Name and target OS page, enter a name and description for the customization specification and select **Windows** as a target guest OS.
- 4 (Optional) Select the **Generate a new security identity (SID)** option 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.

- 5 On the Registration information page, type the virtual machine owner's name and organization and click **Next**.
- 6 On the Computer Name page, enter a computer name for the guest operating system.

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

Option	Action
Enter a name	<ol style="list-style-type: none"> a Type a name. The name can contain alphanumeric characters and the hyphen (-) character. It cannot contain periods (.) or blank spaces and cannot be made up of digits only. Names are not case-sensitive. b (Optional) To ensure that the name is unique, select the Append a numeric value check box. This action appends a hyphen followed by a numeric value to the virtual machine name. The name is truncated if it exceeds 63 characters when combined with the numeric value.
Use the virtual machine name	The computer name that vCenter Server creates is identical to the name of the virtual machine on which the guest operating system is running. If the name exceeds 63 characters, it is truncated.
Enter a name in the Clone/Deploy wizard	You are prompted to enter a name after the cloning or deployment is complete.
Generate a name using the custom application configured with vCenter Server	Enter a parameter that can be passed to the custom application.

- 7 On the Windows license page, provide licensing information for the Windows operating system and click **Next**.

Option	Action
For nonserver operating systems	Type the Windows product key for the new guest operating system.
For server operating systems	<ol style="list-style-type: none"> a Type the Windows product key for the new guest operating system. b Select Include Server License Information. c Select either Per seat or Per server. d If you select Per server, enter the maximum number of simultaneous connections for the server to accept.

- 8 On the Administrator password page, 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) Select the **Automatically logon as Administrator** check box to log users in to the guest operating system as Administrator, and select the number of times to log in automatically.

- 9 On the Time Zone page, select the time zone for the virtual machine and click **Next**.
- 10 (Optional) On the Commands to run once page, specify commands to run the first time a user logs in to the guest operating system and click **Next**.

See the Microsoft Sysprep documentation for information about RunOnce commands.

- 11 On the Network page, select the type of network settings to apply to the guest operating system.

Option	Action
Standard settings	Select Use standard network settings and click Next . vCenter Server configures all network interfaces from a DHCP server using default settings.
Custom settings	<ol style="list-style-type: none"> a Select Manually select custom settings. b For each network interface in the virtual machine, click Edit.

The **Edit Network** dialog box opens.

- 12 Click **IPv4** and specify IPv4-related settings and subnet and gateway details.
 - Select **Use DHCP to obtain an IP address automatically** if you want to use DHCP.
 - Select **Prompt the user for an address when the specification is used** if you want vCenter Serve to prompt you to enter an IP address. You can enter either an IPv4 or an IPv6 address.
 - Select **Use custom settings** to enter the IPv4 address setting manually.
- 13 Click **IPv6** to configure the virtual machine to use IPv6 network.
 - Select **Do not use IPv6** if you do not want to use IPv6.
 - Select the **Use DHCP to obtain an IP address automatically** option if you want to use DHCP.
 - Select **Prompt the user for an address when the specification is used** if you want vCenter Serve to prompt you to enter an IP address. You can enter either an IPv4 or an IPv6 address.
 - Select **Use the following IPv6 addresses** to choose an IPv6 address from the list. You can also add IPv6 addresses manually.

Gateway is enabled by default, except when you choose **Do not use IPv6**

- 14 Click **DNS** and specify DNS server address details.
- 15 Click **WINS** and specify primary and secondary WINS information.
- 16 On the Workgroup or domain page, select how the virtual machine will participate in the network and click **Next**.

Option	Action
Workgroup	Type a workgroup name. For example, MSHOME .
Windows Server Domain	<ol style="list-style-type: none"> 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.

- 17 On the Ready to complete page, review the details and click **Finish** to save your changes.

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

Create a Customization Specification for Windows Using a Custom Sysprep Answer File

A custom sysprep answer file is a file that stores various 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 Select **Menu > Policies and Profiles**, and under Policies and Profiles, click **VM Customization Specifications**.

- 2 Click the **Create a new specification** icon.

The **New VM Guest Customization Spec** wizard opens.

- 3 On the Name and target OS page, enter a name and description for the customization specification and select **Windows** as a target guest OS.

- 4 (Optional) Select the **Generate a new security identity (SID)** option.

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.

- 5 Select **Use Custom Sysprep Answer File** and click **Next**.

- 6 On the Custom sysprep file, select the option to import or create a sysprep answer file and click **Next**.

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

- 7 On the Network page, select the type of network settings to apply to the guest operating system.

Option	Description
Use standard network settings for the guest operating system, including enabling DHCP on all network interfaces	vCenter Server configures all network interfaces from a DHCP server using default settings.
Manually select custom settings	You can specify the IP address and other network settings for each network interface in the virtual machine.

- 8 If you chose to manually configure network settings, select a NIC from the list and click **Edit** to edit its network settings.

- a In the **Edit Network** dialog box, click **IPv4** to specify IPv4-related settings.
 - Select **Use DHCP to obtain an IP address automatically** if you want to use DHCP.
 - Select **Prompt the user for an address when the specification is used** if you want vCenter Server to prompt you to enter an IP address. You can enter either an IPv4 or an IPv6 address.
 - Select **Use the following IP address** to enter the IPv4 address setting manually.
- b Click **IPv6** to configure the virtual machine to use IPv6 network.
 - Select **Do not use IPv6** if you do not want to use IPv6.
 - Select the **Use DHCP to obtain an IP address automatically** option if you want to use DHCP.
 - Select **Prompt the user for an address when the specification is used** if you want vCenter Server to prompt you to enter an IP address. You can enter either an IPv4 or an IPv6 address.
 - Select **Use the following IPv6 addresses** to choose an IPv6 address from the list. You can also add IPv6 addresses manually.

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

Note Gateway is enabled by default, except when you select the **Do not use IPv6** option.

- c Click **DNS** to specify a DNS server address.

- d Click **WINS** to specify primary and secondary WINS information.
 - e Click **OK** to save the configuration settings and exit the **Edit Network** wizard.
 - f Click **Next**.
- 9 On the Ready to complete page, review the details and click **Finish** to save your changes.

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

Manage Customization Specifications

You can edit, duplicate, export, or delete existing specifications.

Procedure

- 1 In the vSphere Client, select **Menu > Policies and Profiles** and click **VM Customization Specifications**.
- 2 Select a customization specification and select your task.

Option	Description
Edit customization spec	You can make changes to the customization spec, such as changing the networking configuration. Click Edit and make the necessary changes.
Duplicate customization spec	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.
Export customization spec	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 Import button.
Delete specification spec	You can remove customization specifications to free up storage.

Import a Customization Specification

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

Prerequisites

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

Procedure

- 1 In the vSphere Client, select **Menu > Policies and Profiles** and click **VM Customization Specifications**.
- 2 Click the **Import specification from a file** icon.
- 3 Browse to the .xml file to import, specify a name and optional description, and click **OK**.

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

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 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) setting 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 for 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 and click the **Configure** tab.

- 2 Under **Virtual Machines**, select **VM Startup/Shutdown** and click **Edit**.

The **Edit VM Startup/Shutdown Configuration** dialog box opens.

- 3 Select **Automatically start and stop the virtual machines with the system**.
- 4 (Optional) In the Default VM Settings pane, configure the default startup and shutdown behavior for all virtual machines on the host.

Setting	Description
Startup Delay	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.
Continue immediately if VMware Tools starts	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.

Setting	Description
Shutdown delay	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.
Shutdown action	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"> ■ Guest Shutdown ■ Power Off ■ Suspend ■ None

- 5 (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 from the default delay for all machines. The settings that you configure for individual virtual machines override the default settings for all machines.

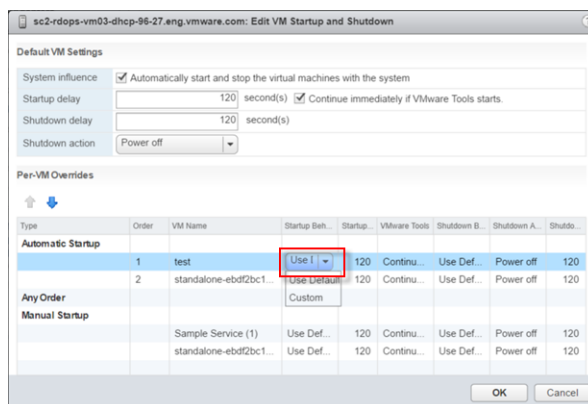
- a To change the startup order of virtual machines, select a virtual machine from the Manual Startup category and use the up arrow to move it up to the Automatic Startup or Any Order categories.

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

- b To change the start up behavior of a virtual machine, select a virtual machine and click the default option in the Startup Behavior column.

The default option is **Use Defaults**.

A drop-down menu appears.



- c Select **Custom** and configure the startup delay by clicking the default value (**120**) in the Startup Delay(s) column.

- d For the selected virtual machine, click the default option in the VMware Tools column. Define whether the ESXi host waits for the delay to pass when VMware Tools is already installed on the virtual machine.

If you select **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 **Do not continue if VMware Tools is installed**, the ESXi host waits for the delay to pass.

- e For the selected virtual machine, click the default option in the Shutdown Behavior column.

The default is **Use Defaults**.

- f From the drop-down menu, select **Custom** and configure the Shutdown Action and the Shutdown Delay(s) by clicking the default options in the those columns.

The default shutdown action is **Power off** and the default shutdown delay is **120**.

- 6 Click **OK**.

Edit Virtual Machine Startup and Shutdown Settings

You can configure virtual machines running on an ESXi host to start up and shut down with the host or after a delay. You can also set the default timing and startup order for 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) setting 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 for a virtual machine. See *vCenter Server and Host Management*.

Procedure

- 1 In the vSphere Client, navigate to the host where the virtual machine is located and click the **Configure** tab.
- 2 Under **Virtual Machines**, select **VM Startup/Shutdown** and click **Edit**.
The **Edit VM Startup/Shutdown Configuration** dialog box opens.
- 3 Select **Automatically start and stop the virtual machines with the system**.

- 4 (Optional) In the Default VM Settings pane, configure the default startup and shutdown behavior for all virtual machines on the host.

Setting	Description
Startup Delay	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.
Continue immediately if VMware Tools starts	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.
Shutdown delay	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.
Shutdown action	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"> ■ Guest Shutdown ■ Power Off ■ Suspend ■ None

- 5 (Optional) You can also 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 from the default delay for all machines. The settings that you configure for individual virtual machines override the default settings for all machines.

- a To configure the startup order of virtual machines, select a virtual machine from the Manual Startup category and use the up arrow to move it up to the Automatic category.

Use the up and down arrows to change the startup order for virtual machines in the Automatic and Manual categories. During shutdown, the virtual machines shut down in the reverse order.
- b To configure the startup and shutdown behavior of virtual machines, select a virtual machine and click the **Edit** icon.
- c In the **Virtual Machine Startup/Shutdown settings** dialog box, configure the startup behavior of the virtual machine.

You can decide to use the default startup delay or you can specify a new one. If you select **Continue if VMware Tools starts**, the ESXi host powers on the next virtual machine without waiting for the delay to pass.

- d In the **Virtual Machine Startup/Shutdown settings** dialog box, configure the shutdown behavior of the virtual machine.

You can decide to use the default shutdown delay or you can specify a new one.

- e Click **OK**.

- 6 Click **OK**.

Install the VMware Enhanced Authentication Plug-in

The VMware Enhanced Authentication Plug-in provides Integrated Windows Authentication and Windows-based smart card functionality.

In the vSphere 6.5 release, the VMware Enhanced Authentication Plug-in replaced the Client Integration Plug-in from vSphere 6.0 releases and earlier. The Enhanced Authentication Plug-in provides Integrated Windows Authentication and Windows-based smart card functionality. These are the only two features carried over from the previous Client Integration Plug-in. The Enhanced Authentication Plug-in can function seamlessly if you already have the Client Integration Plug-in installed on your system from vSphere 6.0 or earlier. There are no conflicts if both plug-ins are installed.

Install the plug-in only once to enable all the functionality the plug-in delivers.

If you install the 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 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 *vCenter Server Installation and Setup* documentation.

Prerequisites

If you use Microsoft Internet Explorer, disable Protected Mode.

Procedure

- 1 Open a Web browser and type the URL for the vSphere Client.
- 2 At the bottom of the vSphere Client login page, click **Download Enhanced Authentication Plug-in**.
- 3 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.
- 4 Save the plug-in to your computer, and run the executable.
- 5 Step through the installation wizard for both the VMware Enhanced Authentication Plug-in and the VMware Plug-in Service which are run in succession.
- 6 When the installations are complete, refresh your browser.

- 7 On the External Protocol Request dialog box, click **Launch Application** to run the Enhanced Authentication Plug-in.

The link to download the plug-in disappears from the login page.

Using a Virtual Machine Console

With the vSphere Client, you can access a virtual machine's console by displaying it in a separate Web browser, or from the VMware Remote Console (VMRC).

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. The vSphere Client offers these choices:

- Launch the Web console to display the VM console in a separate browser tab.
- Download the VMware Remote Console (VMRC) standalone application, which opens in a separate window. The VMware Remote Console standalone application enables you to connect to client devices and launch virtual machine consoles on remote hosts.

Install and Use the VMware Remote Console Application

The VMware Remote Console (VMRC) is a standalone console application. VMRC enables you to connect to client devices and open virtual machine consoles on remote hosts.

Procedure

- 1 In the vSphere Client, navigate to a virtual machine in the inventory.
- 2 Click the **Summary** tab, and click the **Launch Remote Console** link.
- 3 Click the **Download Remote Console** link.
- 4 If prompted, click **Allow** to confirm.

The VMRC opens as a standalone application for the selected virtual machine. You can also launch more than one console to access several remote virtual machines at the same time.

Launch the VMware Remote Console Application

You can use the standalone VMRC to connect to client devices.

With VMRC, you can access the mouse and keyboard connected to remote virtual machines. To perform administrative tasks, make sure that 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 <http://www.vmware.com/go/download-vmrc>.

Procedure

- 1 In the vSphere Client, navigate to a virtual machine in the inventory.

- 2 Click the **Summary** tab, and click the **Launch Remote Console** link.
- 3 Click **Allow** to confirm.

The VMRC opens as a standalone application for the selected virtual machine. You can also launch more than one console to access several remote virtual machines at the same time.

Launch the Web Console

You can access a virtual machine's desktop from the vSphere Client by launching the web console. From the web console, you can perform various tasks in the virtual machine. For example, you can install an operating system, configure the operating system settings, run applications, monitor performance, and so on.

Prerequisites

- 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 Client, navigate to a virtual machine in the inventory.
- 2 In the **Summary** tab, select **Launch Web Console**.

The console opens in a new browser tab.

- 3 Click anywhere inside the console window to start using your mouse, keyboard, and other input devices in the console.

Note For information about supported international keyboards, refer to the VMware HTML Console SDK Release Notes at <https://www.vmware.com/support/developer/html-console/html-console-21-releasenotes.html#knownissues>.

- 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 pointer from the console window and work outside the console window.
- 6 (Optional) Click **Full Screen** to view the console in full screen mode.
- 7 (Optional) Press Ctrl+Alt+Enter to enter or exit full screen mode.

Answer Virtual Machine Questions

The virtual machine questions are messages that are generated on the vCenter Server. The virtual machine questions appear whenever the virtual machine needs a user intervention to continue its operation. In most cases, the virtual machine questions appear when you power on a virtual machine .

You can answer the virtual machine questions from the vSphere Web Client. To save time and ensure the consistency of your virtual environment, you can apply the same answer to other or all virtual machines in your vCenter Server inventory that have the same pending question.

Prerequisites

Verify that the virtual machine hardware version is 11 or higher.

Procedure

- 1 In the Answer Question dialog box, click **Show virtual machines**.
- 2 Select all the virtual machines that you want to apply this answer to.
- 3 Click **OK**.

Removing and Reregistering VMs and VM Templates

You can remove VMs and VM templates from the vCenter Server inventory or delete them from disk. If you only removed the VM from the inventory, you can add it back from the datastore.

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 VMs or VM Templates from vCenter Server or from the Datastore

You can temporarily remove a VM or VM template from vCenter Server or you can permanently delete it from the datastore.

The process is the same for a VM or a VM template:

- When you remove a VM from the inventory, you unregister it from the host and vCenter Server, you do not delete it from the datastore. Virtual machine files remain at the same storage location and you can later re-register the virtual machine by using the datastore browser. This helps if you want to edit the virtual machine's configuration file. It's also useful to temporarily remove a VM when you have reached the maximum number of virtual machines that your license or hardware allows.
- If you no longer need a VM and want to free up space on the datastore, you can remove the VM from vCenter Server and delete all virtual machine files from the datastore, including the configuration file and virtual disk files.

Prerequisites

Verify that the virtual machine is turned off.

Procedure

- ◆ Log in to the vSphere Client and perform the task:

Option	Description
Temporarily remove the VM or VM template	a Right-click the virtual machine. b Select Remove From Inventory and click OK .
Permanently delete the VM or VM template	a Right-click the virtual machine. b Select Delete from Disk and click OK .

Register a VM or VM Template with vCenter Server

If you removed a VM or VM template from vCenter Server but did not delete it from disk, you can return it to the vCenter Server inventory by registering it with the vCenter Server.

Procedure

- 1 In the vSphere Client inventory, right-click the datastore on which the virtual machine configuration file is stored and select **Register VM**.
- 2 Browse to, select the virtual machine configuration (.vmx) file or the VM template configuration file (.vmtx file) and click **OK**.
- 3 Use the existing name or type a new name, select a datacenter or folder location and click **Next**.
- 4 Select a host or cluster on which to run the new virtual machine.

Option	Action
Run the virtual machine on a standalone host.	Select the host and click Next .
Run the virtual machine in a cluster with DRS automatic placement.	Select the cluster and click Next .
Run the virtual machine in a cluster without DRS automatic placement.	a Select the cluster and click Next . b Select a host within the cluster and click Next .

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

Managing Virtual Machine Templates

After you clone a virtual machine to a template, you can perform different operation with the template. You can rename the template, delete it from the vCenter Server inventory, or delete it from the disk. You can also register the template with vCenter Server.

Change the Template Name

If you move a template to another host or datacenter folder, you can change the template name to make it unique in that folder.

Procedure

- 1 Right-click the template and select **Rename**.
- 2 Enter a new name and click **OK**.

Deleting Templates

You can delete a template by removing it from the inventory or deleting the template from the disk. If you remove the template from the inventory, it remains on the disk and can be reregistered with vCenter Server to restore it to the inventory.

Remove Templates from the Inventory

If a template has become outdated and you no longer use it in your environment, you can remove it from the inventory. Removing a template unregisters it from the vCenter Server inventory, but it is not removed from the datastore. The template remains at the same storage location, and you can use the datastore browser to re-register the template at a later time. You can later decide to update the template rather than create one.

Procedure

- 1 Click the template and select **Remove from Inventory**.
- 2 Click **Yes** to confirm removing the template from the vCenter Server database.

The template is unregistered from the vCenter Server inventory.

Delete a Template from the Disk

If you no longer need a template or need to free up disk space, you can remove it from the disk. Templates that you delete are permanently removed from the system.

You cannot recover a template that you delete from the disk.

Procedure

- 1 Right-click the template and select **Delete from Disk**.
- 2 Click **Yes** to confirm removing the template from the datastore.

Reregister Templates

Templates can become unregistered from vCenter Server if they are removed from the inventory or if the hosts with which they are associated are removed from vCenter Server and then readded.

Procedure

- 1 In the vSphere Client, navigate to the datastore that contains the template.
- 2 Select the datastore and click the **Files** tab.
- 3 Locate the template folder and click it to display the template files.
- 4 Select the .vmtx file and click the **Register VM** icon.

The **Register VM Template** wizard opens.

- 5 On the Select a name and folder page, specify a name and location for the template and click **Next**.
- 6 On the Select a compute resource page, select a host or cluster on which to store the template and click **Next**.
- 7 On the Ready to complete page, review your selections and click **Finish**.
- 8 (Optional) To verify that the template is reregistered, check the host or cluster inventory.

Inventory Object	Steps
Host	Browse to the host. On the VMs tab, click VM Templates .
Cluster	On the VMs tab, click VM Templates .

The template is registered to the host. You can view the template by clicking on the host's **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. When you take a snapshot of a virtual machine, an image of the virtual machine in a given state is copied and stored. Snapshots are useful when you want to revert repeatedly to a 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 a snapshot of a VM for each member 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 making changes to a virtual machine.

Several operations for creating and managing virtual machine snapshots and snapshot trees are available in the vSphere Client. These operations enable you to create snapshots, restore any snapshot in the snapshot hierarchy, delete snapshots, and more. You can create snapshot trees where you save the virtual machine state at any specific time so that you can restore that 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 the disks added or changed after you take 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 vSphere Client presents the snapshot hierarchy as a tree with one or more branches. Snapshots in the hierarchy have parent to child relationships. In linear processes, each snapshot has one parent snapshot and one child snapshot, except for the last snapshot, which has no child snapshot. 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 (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 of a virtual machine taken after the parent snapshot. Each child snapshot contains 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.

Caution 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 by 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, the guest operating system stops writing to it, and a delta or child disk is created.

A delta disk has two files. One is a small descriptor file that contains information about the virtual disk, such as geometry and child-parent relationship information. The other one is a corresponding file that contains the raw data.

The files that make up the delta disk are called child disks or redo logs.

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 ESXi host takes to write the memory onto the disk depends on 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 filename 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. Note 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 **Manage Snapshots** dialog box 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 **Manage Snapshots** dialog box contains a snapshot tree, details region, command buttons, 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 Manage Snapshots dialog box. You can select the You are here state to see how much space the node is using. Revert to and Delete 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.

Taking Snapshots of a Virtual Machine

You can take one or more snapshots of a virtual machine to capture the settings state, disk state, and memory state at different specific times. When you take a snapshot, you can also quiesce the virtual machine files and exclude the virtual machine disks from snapshots.

When you take a snapshot, other activity that is occurring in the virtual machine might affect the snapshot process when you revert to that snapshot. The best time to take a snapshot from a storage perspective, is when you are not incurring a large I/O load. The best time to take a snapshot from a service perspective is when no applications in the virtual machine are communicating with other computers. The potential for problems is greatest if the virtual machine is communicating with another computer, especially in a production environment. For example, if you take a snapshot while the virtual machine is downloading a file from a server on the network, the virtual machine continues downloading the file and communicating its progress to the server. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails. Depending on the task that you are performing, you can create a memory snapshot or you can quiesce the file system in the virtual machine.

Memory Snapshots

The default selection for taking snapshots. When you capture the virtual machine's memory state, the snapshot retains the live state of the virtual machine. Memory snapshots create a snapshot at a precise time, for example, to upgrade software that is still working. If you take a memory snapshot and the upgrade does not complete as expected, or the software does not meet your expectations, you can revert the virtual machine to its previous state.

When you capture the memory state, the virtual machine's files do not require quiescing. If you do not capture the memory state, the snapshot does not save the live state of the virtual machine and the disks are crash consistent unless you quiesce them.

Quiesced Snapshots

When you quiesce a virtual machine, VMware Tools quiesces the file system of the virtual machine. A quiesce operation ensures that a snapshot disk represents a consistent state of the guest file systems. Quiesced snapshots are appropriate for automated or periodic backups. For example, if you are unaware of the virtual machine's activity, but want several recent backups to revert to, you can quiesce the files.

If the virtual machine is powered off or VMware Tools is not available, the Quiesce parameter is not available. You cannot quiesce virtual machines that have large capacity disks.

Important Do not use snapshots as your only backup solution or as a long-term backup solution.

Change Disk Mode to Exclude Virtual Disks from Snapshots

You can set a virtual disk to independent mode to exclude the disk from any snapshots taken of its virtual machine.

Prerequisites

Power off the virtual machine and delete any existing snapshots before you change the disk mode. Deleting a snapshot involves committing the existing data on the snapshot disk to the parent disk.

Required privileges:

- **Virtual machine .Snapshot management.Remove Snapshot**
- **Virtual machine.Configuration.Modify device settings**

Procedure

- 1 Right-click a virtual machine in the inventory and select **Edit Settings**.
- 2 On the **Virtual Hardware** tab, expand **Hard disk**, and select an independent disk mode option.

Option	Description
Independent - Persistent	Disks in persistent mode behave like conventional disks on your physical computer. All data written to a disk in persistent mode are written permanently to the disk.
Independent - Nonpersistent	Changes to disks in nonpersistent mode are discarded when you power off or reset the virtual machine. With nonpersistent mode, you can restart the virtual machine with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when you power off or reset.

- 3 Click **OK**.

Taking a Snapshot

Snapshots capture the entire state of the virtual machine at the time you take the snapshot. You can take a snapshot when a virtual machine is powered on, powered off, or suspended. If you are suspending a virtual machine, wait until the suspend operation finishes before you take a snapshot.

When you create a memory snapshot, the snapshot captures the state of the virtual machine's memory and the virtual machine power settings. When you capture the virtual machine's memory state, the snapshot operation takes longer to complete. You might also see a momentary lapse in response over the network.

When you quiesce a virtual machine, VMware Tools quiesces the file system in the virtual machine. The quiesce operation pauses or alters the state of running processes on the virtual machine, especially processes that might modify information stored on the disk during a restore operation.

Application-consistent quiescing is not supported for virtual machines with IDE or SATA disks.

Note 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 the inventory and select **Snapshots > Take Snapshot**.
The **Take Snapshot** dialog box opens.
- 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) 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

Virtual Machine State When Parent Snapshot Is Taken	Virtual Machine State After Restoration
Powered on (includes memory)	Reverts to the parent snapshot, and the virtual machine is powered on and running.
Powered on (does not include memory)	Reverts to the parent snapshot and the virtual machine is powered off.
Powered off (does not include memory)	Reverts to the parent snapshot and the virtual machine is powered off.

Virtual machines running certain kinds of workloads can take several minutes to resume responsiveness after reverting from a snapshot.

Note vApp metadata for virtual machines in vApps does not follow the snapshot semantics for virtual machine configuration. vApp properties that are deleted, modified, or defined after a snapshot is taken remain intact (deleted, modified, or defined) after the virtual machine reverts to that snapshot or any previous snapshots.

Restore VM Snapshots Using Revert

To return a virtual machine to its original state, or to return to another snapshot in the snapshot hierarchy, you can use the revert options.

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 when you took 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 9-2. Virtual Machine Power State After Restoring a Snapshot

Virtual Machine State When Parent Snapshot Is Taken	Virtual Machine State After Restoration
Powered on (includes memory)	Reverts to the parent snapshot, and the virtual machine is powered on and running.
Powered on (does not include memory)	Reverts to the parent snapshot and the virtual machine is powered off.
Powered off (does not include memory)	Reverts to the parent snapshot and the virtual machine is powered off.

Virtual machines running certain kinds of workloads can take several minutes to resume responsiveness after reverting from a snapshot.

Note vApp metadata for virtual machines in vApps does not follow the snapshot semantics for virtual machine configuration. vApp properties that are deleted, modified, or defined after a snapshot is taken remain intact (deleted, modified, or defined) after the virtual machine reverts to that snapshot or any previous snapshots.

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

- ◆ In the vSphere Client, right-click a virtual machine and make your selection. and

Task	Description
Revert to the latest snapshot	Select Revert to Latest Snapshot and click OK .
Revert to a selected snapshot	<ol style="list-style-type: none"> Right-click the virtual machine and select Manage Snapshots. Navigate to a snapshot in the snapshot tree and click the Revert To button. Click Yes to confirm.

Delete a Snapshot

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. You can use the Snapshot Manager to delete a single snapshot or all snapshots in a snapshot tree.

Deleting a snapshot does not change the virtual machine or other snapshots. Deleting a snapshot consolidates the changes between snapshots and previous disk states and writes all the data from the delta disk that contains the information about the deleted snapshot to the parent disk. When you delete the base parent snapshot, all changes merge with the base virtual machine disk.

To delete a snapshot, a large amount of information needs to be read and written to a disk. This process 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 amount of data that the guest operating system writes to the virtual disks after you take 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.

Failure of disk consolidation can reduce the performance of virtual machines. You can check whether any virtual machines require separate consolidation operations by viewing a list. For information about locating and viewing the consolidation state of multiple virtual machines and running a separate consolidation operation, see *vSphere Virtual Machine Administration*.

Delete Use the **Delete** option to remove a single parent or child snapshot from the snapshot tree. **Delete** writes disk changes that occur between the state of the snapshot and the previous disk state to the parent snapshot.

You can also use the **Delete** option to remove a corrupt snapshot and its files from an abandoned branch of the snapshot tree without merging them with the parent snapshot.

Delete All Use the **Delete All** option to delete all snapshots from the Snapshot Manager. **Delete all** consolidates and writes the changes that occur between snapshots and the 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 if, for example, an update or installation fails, first use the **Restore** 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.

Caution 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.

- 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 **VMs** tab and click **Virtual Machines**.
- 2 In the Snapshot Manager, click a snapshot to select it.
- 3 Select whether to delete a single snapshot or all snapshots.

Option	Description
Delete	Consolidates the snapshot data to the parent snapshot and removes the selected snapshot from the Snapshot Manager and virtual machine.
Delete All	Consolidates all of the immediate snapshots before the You are here current state to the base parent disk and removes all existing snapshots from the Snapshot Manager and virtual machine.

- 4 Click **Yes** in the confirmation dialog box.
- 5 Click **Close** to exit the Snapshot Manager.

Consolidate Snapshots

The presence of redundant delta disks can adversely affect virtual machine performance. You can combine such disks without violating a data dependency. After consolidation, redundant disks are removed, which improves virtual machine performance and saves storage space.

Snapshot consolidation is useful when snapshot disks fail to compress after a **Delete** or **Delete all** operation. This might happen, for example, if you delete a snapshot but its associated disk does not commit back to the base disk.

The Needs Consolidation column in the vSphere 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 **VMs** 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 **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.

Enhanced vMotion Compatibility as a Virtual Machine Attribute

Cluster-level EVC ensures CPU compatibility between hosts in a cluster, so that you can seamlessly migrate virtual machines within the EVC cluster. In vSphere 6.7, you can also enable, disable, or change the EVC mode at the virtual machine level. The per-VM EVC feature facilitates the migration of the virtual machine beyond the cluster and across vCenter Server systems and datacenters that have different processors.

The EVC mode of a virtual machine is independent from the EVC mode defined at the cluster level. The cluster-based EVC mode limits the CPU features a host exposes to virtual machines. The per-VM EVC mode determines the set of host CPU features that a virtual machine requires in order to power on and migrate.

By default, when you power on a newly created virtual machine, it inherits the feature set of its parent EVC cluster or host. However, you can change the EVC mode for each virtual machine separately. You can raise or lower the EVC mode of a virtual machine. Lowering the EVC mode increases the CPU compatibility of the virtual machine. You can also use the API calls to customize the EVC mode further.

Cluster-based EVC and Per-VM EVC

There are several differences between the way the EVC feature works at the host cluster level and at the virtual machine level.

- Unlike cluster-based EVC, you can change the per-VM EVC mode only when the virtual machine is powered off.
- With cluster-based EVC, when you migrate a virtual machine out of the EVC cluster, a power cycle resets the EVC mode that the virtual machine has. With Per-VM EVC, the EVC mode becomes an attribute of the virtual machine. A power cycle does not affect the compatibility of the virtual machine with different processors.
- When you configure EVC at the virtual machine level, the per-VM EVC mode overrides cluster-based EVC. If you do not configure per-VM EVC, when you power on the virtual machine, it inherits the EVC mode of its parent EVC cluster or host.

- If a virtual machine is in an EVC cluster and the per-VM EVC is also enabled, the EVC mode of the virtual machine cannot exceed the EVC mode of the EVC cluster in which the virtual machine runs. The baseline feature set that you configure for the virtual machine cannot contain more CPU features than the baseline feature set applied to the hosts in the EVC cluster. For example, if you configure a cluster with the Intel "Merom" Generation EVC mode, you should not configure a virtual machine with any other Intel baseline feature set. All other sets contain more CPU features than the Intel "Merom" Generation feature set and as a result of such configuration, the virtual machine fails to power on.

To learn more about cluster-based EVC, see the *vCenter Server and Host Management* guide.

Compatibility and Requirements

The Per-VM EVC feature has the following requirements.

Compatibility	Requirement
Host Compatibility	ESXi 6.7 or later.
vCenter Server Compatibility	vCenter Server 6.7 or later.
Virtual Machine Compatibility	Virtual hardware version 14 or greater.

To check EVC support for a specific processor or server model, see the *VMware Compatibility Guide* at <http://www.vmware.com/resources/compatibility/search.php>.

Change the EVC Mode of a Virtual Machine

Set the EVC mode of a virtual machine to ensure its seamless migration across clusters, vCenter Server systems, and datacenters that have different processors.

Prerequisites

The virtual machine must be powered off before you can enable, disable, or change its EVC mode.

To verify the EVC mode of virtual machines, see [Determine the EVC Mode of a Virtual Machine](#)

Procedure

- 1 In the vSphere Client, navigate to the virtual machine.

2 Under the **Configure** tab, select **VMware EVC**.

The pane shows details about the EVC mode of the virtual machine and CPUID details.

Important For newly created virtual machines, the EVC mode that shows in the **VMware EVC** pane is disabled.

For powered-off virtual machines, the **VMware EVC** pane always shows the EVC status defined at the virtual machine level.

For powered-on virtual machines with per-VM EVC enabled, the VMware EVC pane shows the EVC status defined at the virtual machine level.

For powered-on virtual machines with per-VM EVC disabled, the VMware EVC pane shows the EVC mode that the virtual machine inherits from its parent EVC cluster or host.

3 Click **Edit** and select whether to enable or disable EVC.

Option	Description
Disable EVC	The EVC feature is disabled for the virtual machine. When you power on the virtual machine, it inherits the feature set of its parent EVC cluster or host.
Enable EVC for AMD Hosts	The EVC feature is enabled for AMD hosts.
Enable EVC for Intel Hosts	The EVC feature is enabled for Intel hosts.
Custom	This option is visible only if you have customized the EVC mode of the virtual machine through the API calls.

4 If you want to enable EVC, choose a baseline CPU feature set from the **VMware EVC Mode** drop-down menu.

Important If the virtual machine is in an EVC cluster and the per-VM EVC mode exceeds the cluster-based EVC mode, the virtual machine will fail to power on. The baseline CPU feature set for the virtual machine should not contain more CPU features than the baseline CPU feature set of the cluster.

5 Click **OK**.

Determine the EVC Mode of a Virtual Machine

The EVC mode of a virtual machine determines the CPU features that a host must have in order for the virtual machine to power on and migrate. The EVC mode of a virtual machine is determined when the virtual machine is powered on. In vSphere 6.7, the EVC mode of a virtual machine is independent from the EVC mode that you configure for the cluster in which the virtual machine runs.

The EVC mode of a virtual machine is determined when the virtual machine is powered on. At power-on, the virtual machine also determines the EVC mode of the cluster in which it is running. If the EVC mode of a running virtual machine or the entire EVC cluster is raised, the virtual machine does not change its EVC mode until it is powered off and powered on again. This means that the virtual machine does not use any CPU features exposed by the new EVC mode until the virtual machine is powered off and powered on again.

For example, consider a cluster that contains hosts with Intel Xeon 45 nm Core two processors that are set to the Intel Merom Generation (Xeon Core 2) EVC mode. When you power on a virtual machine in this cluster, it runs in the Intel Merom Generation (Xeon Core 2) EVC mode. If the EVC mode of the cluster is raised to Intel Penryn Generation (Xeon 45 nm Core 2), the virtual machine remains at the lower Intel Merom Generation (Xeon Core 2) EVC mode. To use any of the features exposed by the higher cluster EVC mode, such as SSE4.1, you must power off the virtual machine and power it on again.

Procedure

- 1 In the vSphere Client, select a cluster or a host in the inventory.
- 2 Click the **VMs** tab.

A list of all virtual machines in the selected cluster or on the selected host appears.

- 3 If the EVC Mode column does not appear, click the arrow in any column title, select **Show/Hide Columns**, and select the **EVC Mode** check box.

The **EVC Mode** column shows the EVC modes of all virtual machines in the cluster or on the host.

Important The **EVC Mode** column displays the EVC mode defined at the virtual machine level. However, if you do not configure per-VM EVC for a virtual machine, the virtual machine inherits the EVC mode of its parent cluster or host. As a result, for all virtual machines that do not have per-VM EVC configured, the **EVC Mode** column displays the inherited cluster-based EVC mode.

Important If the virtual machine is running in an EVC cluster, its EVC mode is determined in the following manner.

Per-VM EVC	Cluster-level EVC	EVC Mode for the Virtual Machine
Enabled	Enabled	Enabled. The EVC Mode column displays the EVC mode of the virtual machine.
Disabled	Enabled	Enabled. The EVC Mode column displays the EVC mode of the EVC cluster.

If a virtual machine is powered off and is in an EVC cluster, the **EVC Mode** column always displays the per-VM EVC mode.

Migrating Virtual Machines

You can move virtual machines from one host or storage location to another location using hot or cold migration. For example, with vSphere vMotion you can move powered on virtual machines away from a host to perform maintenance, to balance loads, to colocate virtual machines that communicate with each other, to move virtual machines apart to minimize fault domain, to migrate to new server hardware, and so on.

You can use cold or hot migration to move virtual machines to different hosts or datastores.

Cold Migration

You can move a powered off or suspended virtual machine to a new host. Optionally, you can relocate configuration and disk files for powered off or suspended virtual machines to new storage locations. You can also use cold migration to move virtual machines from one data center to another. To perform a cold migration, you can move virtual machines manually or set up a scheduled task.

Hot Migration

You can use vMotion or Storage vMotion to move a powered on virtual machine to a different host and move its disks or folder to a different datastore. You can move the virtual machine without any interruption in availability. You can also move a virtual machine to a different host and to a different storage location at the same time. vMotion is also called live migration or hot migration.

Note Copying a virtual machine creates a new virtual machine. It is not a form of migration. Cloning a virtual machine or copying its disks and configuration file creates a new virtual machine. Cloning is not a form of migration.

You can perform several types of migration according to the virtual machine resource type.

Change compute resource only

Moving a virtual machine but not its storage to another compute resource, such as a host, cluster, resource pool, or vApp. You use vMotion to move a powered on virtual machine to another compute resource. You can move the virtual machine to another host by using cold migration or hot migration.

Change storage only

Moving a virtual machine and its storage, including virtual disks, configuration files, or a combination of these, to a new datastore on the same host. You can change the datastore using cold or hot migration. You use Storage vMotion to move a powered on virtual machine and its storage to a new datastore .

Change both compute resource and storage

Moving a virtual machine to another host and moving its disk or virtual machine folder to another datastore. You can change the host and datastore using cold or hot migration. When you move a virtual machine network between distributed switches, the network configuration and policies that are associated with the network adapters of the virtual machine are transferred to the target switch.

In vSphere 6.0 and later, you can move virtual machines between vSphere sites by using migration between these types of objects.

Migrate to another virtual switch

Moving the network of a virtual machine to a virtual switch of a different type. You can migrate virtual machines without reconfiguring the physical and virtual network. While performing cold or hot migration, you can move the virtual machine from a standard to a standard or distributed switch and from a distributed switch to another distributed switch.

Migrate to another data center

Moving virtual machines between data centers. While performing cold or hot migration, you can change the data center of a virtual machine. For networking in the target data center, you can select a dedicated port group on a distributed switch.

Migrate to another vCenter Server system

Moving virtual machines between two vCenter Server instances that are connected in Enhanced Linked Mode.

You can also move virtual machines between vCenter Server instances that are located across a long distance from each other.

For information about the requirements about vMotion across vCenter Server instances, see the *vCenter Server and Host Management* documentation.

To migrate virtual machines with disks larger than 2 TB, the source and destination ESXi hosts must be version 6.0 and later.

Migrate a Powered Off or Suspended Virtual Machine

You can use cold migration to move a virtual machine and its associated disks from one datastore to another. The virtual machines are not required to be on shared storage.

Prerequisites

- Make sure that you are familiar with the requirements for cold migration. See the *vCenter Server and Host Management* documentation.
- Required privilege: **Resource.Migrate powered off virtual machine**

Procedure

- 1 Power off or suspend the virtual machine.
- 2 Right-click the virtual machine and select **Migrate**.
 - a To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.
 - b Click the **Virtual Machines** tab.

3 Select the migration type and click **Next**.

Option	Description
Change compute resource only	Move the virtual machine to another host.
Change storage only	Move the virtual machine's configuration file and virtual disks.
Change both compute resource and storage	Move the virtual machine to another host and move its configuration file and virtual disks.
Migrate virtual machine(s) to a specific datacenter	Move the virtual machine to a virtual data center, where you can assign policies to VMs.

4 If you change the compute resource of the virtual machine, select the destination compute resource for this virtual machine migration and click **Next**.

Any compatibility problem appears in the Compatibility panel. Fix the problem, or select another host or cluster.

Possible targets include hosts and DRS clusters with any level of automation. If a cluster has no DRS enabled, select a specific host in the cluster rather than selecting the cluster.

Important If the virtual machine that you migrate has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, the compatibility check fails and you cannot proceed further with the migration.

If the virtual machine that you migrate does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resource, so that all PMem hard disks remain stored on a PMem datastore. Otherwise, all the hard disks will use the storage policy and datastore selected for the configuration files of the virtual machine.

Important Migrating a virtual machine that has an NVDIMM device or a vPMem disk to a host that does not have the proper license fails and leaves the virtual machine in an unmanageable state for 90 seconds. You can afterwards retry the migration and choose a destination host that is licensed to use PMem devices.

5 On the Select storage page, select the storage type for the virtual machine configuration files and all the hard disks.

- If you select the **Standard** mode, all virtual disks are stored on a standard datastore.
- If you select the **PMem** mode, all virtual disks are stored on the host-local PMem datastore. Configuration files cannot be stored on a PMem datastore and you must additionally select a regular datastore for the configuration files of the virtual machine.
- If you select the **Hybrid** mode, all PMem virtual disks remain stored on a PMem datastore. Non-PMem disks are affected by your choice of a VM storage policy and datastore or datastore cluster.

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

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

7 Select a virtual machine storage policy from the **VM Storage Policy** drop-down menu.

Storage policies specify storage requirements for applications that run on the virtual machine. You can also select the default policy for vSAN or Virtual Volumes datastores.

Important If the virtual machine hard disks use different storage policies, the new policy that you select only applies to non-PMem hard disks. PMem hard disks are migrated to the host-local PMem datastore of the destination host.

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

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore and click Next .
Store all virtual machine files in the same Storage DRS cluster.	<ul style="list-style-type: none"> a Select a Storage DRS cluster. b (Optional) To disable Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the Storage DRS cluster. c Click Next.
Store virtual machine configuration files and disks in separate locations.	<ul style="list-style-type: none"> a Click Configure per disk. <ul style="list-style-type: none"> Note You can use the Configure per disk option to downgrade from or upgrade to PMem storage. b For the virtual machine configuration file and for each virtual disk, select Browse, and select a datastore or Storage DRS cluster. <ul style="list-style-type: none"> Note Configuration files cannot be stored on a PMem datastore. c (Optional) If you selected a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the Storage DRS cluster. d Click Next.

- 9 Select a destination network for all VM network adapters connected to a valid source network and click **Next**.

You can click **Advanced** to select a new destination network for each VM network adapter connected to a valid source network.

You can migrate a virtual machine network to another distributed switch in the same or to another data center or vCenter Server.

- 10 On the Ready to complete page, review the details and click **Finish**.

vCenter Server moves the virtual machine to the new host or storage location.

Event messages appear in the **Events** tab. The data displayed on the **Summary** tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

Migrate a Powered-Off or Suspended Virtual Machine in the vSphere Web Client

You can use cold migration to move a virtual machine and its associated disks from one datastore to another. The virtual machines are not required to be on shared storage.

Prerequisites

- Make sure that you are familiar with the requirements for cold migration. See the *vCenter Server and Host Management* documentation.
- Required privilege: **Resource.Migrate powered off virtual machine**

Procedure

- 1 Power off or suspend the virtual machine.
- 2 Right-click the virtual machine and select **Migrate**.
 - a To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.
 - b Click the **Virtual Machines** tab.
- 3 Select the migration type and click **Next**.

Option	Description
Change compute resource only	Move the virtual machine to another host.
Change storage only	Move the virtual machine's configuration file and virtual disks.
Change both compute resource and storage	Move the virtual machine to another host and move its configuration file and virtual disks.
Migrate virtual machine(s) to a specific datacenter	Move the virtual machine to a virtual data center, where you can assign policies to VMs.

- 4 If you change the compute resource of the virtual machine, select the destination compute resource for this virtual machine migration and click **Next**.

Any compatibility problem appears in the Compatibility panel. Fix the problem, or select another host or cluster.

Possible targets include hosts and DRS clusters with any level of automation. If a cluster has no DRS enabled, select a specific host in the cluster rather than selecting the cluster.

Important If the virtual machine that you migrate has an NVDIMM device and uses PMem storage, the destination host or cluster must have available PMem resources. Otherwise, the compatibility check fails and you cannot proceed further with the migration.

If the virtual machine that you migrate does not have an NVDIMM device but it uses PMem storage, you must select a host or cluster with available PMem resources, so that all PMem hard disks remain stored on a PMem datastore. Otherwise, all the hard disks use the storage policy and datastore selected for the configuration files of the virtual machine.

Important Migrating a virtual machine that has an NVDIMM device or a vPMem disk to a host that does not have the proper license fails and leaves the virtual machine in an unmanageable state for 90 seconds. You can afterwards retry the migration and select a destination host that is licensed to use PMem devices.

- 5 Select the format for the virtual machine's disks.

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

- 6 Select a virtual machine storage policy from the **VM Storage Policy** drop-down menu.

Storage policies specify storage requirements for applications that run on the virtual machine. You can also select the default policy for vSAN or Virtual Volumes datastores.

Important If the virtual machine hard disks use different storage policies, the new policy that you select only applies to non-PMem hard disks. PMem hard disks are migrated to the host-local PMem datastore of the destination host.

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

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore and click Next .
Store all virtual machine files in the same Storage DRS cluster.	<ol style="list-style-type: none"> Select a Storage DRS cluster. (Optional) To disable Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the Storage DRS cluster. Click Next.
Store virtual machine configuration files and disks in separate locations.	<ol style="list-style-type: none"> Click Advanced. <ul style="list-style-type: none"> Note You can use the Advanced option to downgrade from or upgrade to PMem storage. For the virtual machine configuration file and for each virtual disk, select Browse, and select a datastore or Storage DRS cluster. <ul style="list-style-type: none"> Note Configuration files cannot be stored on a PMem datastore. (Optional) If you selected a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the Storage DRS cluster. Click Next.

8 Select a destination network for all VM network adapters connected to a valid source network and click **Next**.

You can click **Advanced** to select a new destination network for each VM network adapter connected to a valid source network.

You can migrate a virtual machine network to another distributed switch in the same or to another data center or vCenter Server.

9 On the Ready to complete page, review the details and click **Finish**.

vCenter Server moves the virtual machine to the new host or storage location.

Event messages appear in the **Events** tab. The data displayed on the **Summary** tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

Migrate a Virtual Machine to a New Compute Resource

You can use the **Migration** wizard to migrate a powered-on virtual machine from one compute resource to another by using vMotion. To relocate only the disks of a powered-on virtual machine, migrate the virtual machine to a new datastore by using Storage vMotion.

Prerequisites

Verify that your hosts and virtual machines meet the requirements for migration with vMotion with shared storage.

- Verify that your hosts and virtual machines meet the requirements for migration with vMotion. See the *vCenter Server and Host Management* documentation.
- Verify that the storage that contains the virtual machine disks is shared between the source and target hosts. See "vMotion Shared Storage Requirements" in the *vCenter Server and Host Management* documentation.
- For migration across vCenter Server instances, verify whether your system meets additional requirements. See "Requirements for Migration Across vCenter Servers" in the *vCenter Server and Host Management* documentation.
- Required privilege: **Resource.Migrate powered on virtual machine**

Procedure

- 1 Right-click the virtual machine and select **Migrate**.
 - a To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.
 - b Click the **Virtual Machines** tab.
- 2 Click **Change compute resource only** and click **Next**.
- 3 Select a host, cluster, resource pool, or vApp to run the virtual machine, and click **Next**.

Any compatibility problem appears in the Compatibility panel. Fix the problem, or select another host or cluster.

Possible targets include hosts and fully automated DRS clusters in the same or another vCenter Server system. If your target is a non-automated cluster, select a host within the non-automated cluster.

Important If the virtual machine that you migrate has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resources. Otherwise, the compatibility check fails and you cannot proceed further with the migration.

If the virtual machine that you migrate does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resources, so that all PMem hard disks remain stored on a PMem datastore. Otherwise, all the hard disks use the storage policy and datastore selected for the configuration files of the virtual machine.

Important Migrating a virtual machine that has an NVDIMM device or a vPMem disk to a host that does not have the proper license fails and leaves the virtual machine in an unmanageable state for 90 seconds. You can afterwards retry the migration and select a destination host that is licensed to use PMem devices.

- 4 Select a destination network for all VM network adapters connected to a valid source network and click **Next**.

You can click **Advanced** to select a new destination network for each VM network adapter connected to a valid source network.

You can migrate a virtual machine network to another distributed switch in the same or to another data center or vCenter Server.

- 5 Select the migration priority level and click **Next**.

Option	Description
Schedule vMotion with high priority	vCenter Server attempts to reserve resources on both the source and destination hosts to be shared among all concurrent migrations with vMotion. vCenter Server grants a larger share of host CPU resources. If sufficient CPU resources are not immediately available, vMotion is not initiated.
Schedule regular vMotion	vCenter Server reserves resources on both the source and destination hosts to be shared among all concurrent migration with vMotion. vCenter Server grants a smaller share of host CPU resources. If there is a lack of CPU resources, the duration of vMotion can be extended.

- 6 Review the page and click **Finish**.

vCenter Server moves the virtual machine to the new host or storage location.

Event messages appear in the **Events** tab. The data displayed on the **Summary** tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

Migrate a Virtual Machine to New Storage

Use migration with Storage vMotion to relocate the configuration file of a virtual machine and virtual disks while the virtual machine is powered on.

You can change the virtual machine host during a migration with Storage vMotion.

Prerequisites

-
- Verify that your system satisfies the requirements for Storage vMotion. See "Storage vMotion Requirements and Limitations" in the *vCenter Server and Host Management* documentation.
- Required privilege: **Resource.Migrate powered on virtual machine**

Procedure

- 1 Right-click the virtual machine and select **Migrate**.
 - a To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.
 - b Click the **Virtual Machines** tab.
- 2 Click **Change storage only** and click **Next**.

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

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

4 Select a virtual machine storage policy from the **VM Storage Policy** drop-down menu.

Storage policies specify storage requirements for applications that run on the virtual machine. You can also select the default policy for vSAN or Virtual Volumes datastores.

Important If the virtual machine hard disks use different storage policies, the new policy that you select only applies to non-PMem hard disks. PMem hard disks are migrated to the host-local PMem datastore of the destination host.

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

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore and click Next .
Store all virtual machine files in the same Storage DRS cluster.	<ul style="list-style-type: none"> a Select a Storage DRS cluster. b (Optional) To disable Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the Storage DRS cluster. c Click Next.
Store virtual machine configuration files and disks in separate locations.	<ul style="list-style-type: none"> a Click Configure per disk. <ul style="list-style-type: none"> Note You can use the Configure per disk option to downgrade from or upgrade to PMem storage. b For the virtual machine configuration file and for each virtual disk, select Browse, and select a datastore or Storage DRS cluster. <ul style="list-style-type: none"> Note Configuration files cannot be stored on a PMem datastore. c (Optional) If you selected a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the Storage DRS cluster. d Click Next.

6 On the Ready to complete page, review the details and click **Finish**.

vCenter Server moves the virtual machine to the new storage location. Names of migrated virtual machine files on the destination datastore match the inventory name of the virtual machine.

Event messages appear in the **Events** tab. The data displayed on the **Summary** tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

Migrate a Virtual Machine to New Storage in the vSphere Web Client

Use migration with Storage vMotion to relocate the configuration file of a virtual machine and virtual disks while the virtual machine is powered on.

You can change the virtual machine host during a migration with Storage vMotion.

Prerequisites

- Verify that your system satisfies the requirements for Storage vMotion. See "Storage vMotion Requirements and Limitations" in the *vCenter Server and Host Management* documentation.
- Required privilege: **Resource.Migrate powered on virtual machine**

Procedure

- 1 Right-click the virtual machine and select **Migrate**.
 - a To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.
 - b Click the **Virtual Machines** tab.
- 2 Click **Change storage only** and click **Next**.
- 3 Select the format for the virtual machine's disks.

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

- 4 Select a virtual machine storage policy from the **VM Storage Policy** drop-down menu.

Storage policies specify storage requirements for applications that run on the virtual machine. You can also select the default policy for vSAN or Virtual Volumes datastores.

Important If the virtual machine hard disks use different storage policies, the new policy that you select only applies to non-PMem hard disks. PMem hard disks are migrated to the host-local PMem datastore of the destination host.

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

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore and click Next .
Store all virtual machine files in the same Storage DRS cluster.	<ol style="list-style-type: none"> Select a Storage DRS cluster. (Optional) To disable Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the Storage DRS cluster. Click Next.
Store virtual machine configuration files and disks in separate locations.	<ol style="list-style-type: none"> Click Advanced. <ul style="list-style-type: none"> Note You can use the Advanced option to downgrade from or upgrade to PMem storage. For the virtual machine configuration file and for each virtual disk, select Browse, and select a datastore or Storage DRS cluster. <ul style="list-style-type: none"> Note Configuration files cannot be stored on a PMem datastore. (Optional) If you selected a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the Storage DRS cluster. Click Next.

- 6 On the Ready to complete page, review the details and click **Finish**.

vCenter Server moves the virtual machine to the new storage location. Names of migrated virtual machine files on the destination datastore match the inventory name of the virtual machine.

Event messages appear in the **Events** tab. The data displayed on the **Summary** tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

Migrate a Virtual Machine to a New Compute Resource and Storage

You can move a virtual machine to another compute resource and move its disks or virtual machine folder to another datastore. With vMotion, you can migrate a virtual machine and its disks and files while the virtual machine is powered on.

Simultaneous migration to a new compute resource and datastore provides greater mobility for virtual machines by eliminating the vCenter Server boundary. Virtual machine disks or content of the virtual machine folder are transferred over the vMotion network to reach the destination host and datastores.

To make disk format changes and preserve them, you must select a different datastore for the virtual machine files and disks. You cannot preserve disk format changes if you select the same datastore on which the virtual machine currently resides.

Prerequisites

- Verify that your hosts and virtual machines meet the requirements for live migration. See "Requirements and Limitations for vMotion Without Shared Storage" in the *vCenter Server and Host Management* documentation.
- For migration across vCenter Server instances, verify whether your system meets additional requirements. See "Requirements for Migration Across vCenter Servers" in the *vCenter Server and Host Management* documentation.
- Required privilege: **Resource.Migrate powered on virtual machine**

Procedure

- 1 Right-click the virtual machine and select **Migrate**.
 - a To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.
 - b Click the **Virtual Machines** tab.
- 2 Select **Change both compute resource and storage** and click **Next**.
- 3 Select a destination resource for the virtual machine, and click **Next**.

Any compatibility problems appear in the Compatibility panel. Fix the problem, or select another host or cluster.

Possible targets include hosts and fully automated DRS clusters. If your target is a non-automated cluster, select a host within the non-automated cluster.

If your environment has more than one vCenter Server instances, you can move virtual machines from one vCenter Server inventory to another.

Important If the virtual machine that you migrate has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have available PMem resource. Otherwise, the compatibility check fails and you cannot proceed further with the migration.

If the virtual machine that you migrate does not have an NVDIMM device, but it has virtual PMem hard disks, the destination host or cluster must have available PMem resource, so that all PMem hard disks remain stored on a PMem datastore. Otherwise, all the hard disks will use the storage policy and datastore selected for the configuration files of the virtual machine.

Important Migrating a virtual machine that has an NVDIMM device or a vPMem disk to a host that does not have the proper license fails and leaves the virtual machine in an unmanageable state for 90 seconds. You can afterwards retry the migration and choose a destination host that is licensed to use PMem devices.

- 4 On the Select storage page, select the storage type for the virtual machine configuration files and all the hard disks.
 - If you select the **Standard** mode, all virtual disks are stored on a standard datastore.
 - If you select the **PMem** mode, all virtual disks are stored on the host-local PMem datastore. Configuration files cannot be stored on a PMem datastore and you must additionally select a regular datastore for the configuration files of the virtual machine.
 - If you select the **Hybrid** mode, all PMem virtual disks remain stored on a PMem datastore. Non-PMem disks are affected by your choice of a VM storage policy and datastore or datastore cluster.
- 5 Select the format for the virtual machine's disks.

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

- 6 Select a virtual machine storage policy from the **VM Storage Policy** drop-down menu.

Storage policies specify storage requirements for applications that run on the virtual machine. You can also select the default policy for vSAN or Virtual Volumes datastores.

Important If the virtual machine hard disks use different storage policies, the new policy that you select only applies to non-PMem hard disks. PMem hard disks are migrated to the host-local PMem datastore of the destination host.

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

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore and click Next .
Store all virtual machine files in the same Storage DRS cluster.	<ul style="list-style-type: none"> a Select a Storage DRS cluster. b (Optional) To disable Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the Storage DRS cluster. c Click Next.
Store virtual machine configuration files and disks in separate locations.	<ul style="list-style-type: none"> a Click Configure per disk. <ul style="list-style-type: none"> Note You can use the Configure per disk option to downgrade from or upgrade to PMem storage individual hard disks. b For the virtual machine configuration file and for each virtual disk, select Browse, and select a datastore or Storage DRS cluster. <ul style="list-style-type: none"> Note Configuration files cannot be stored on a PMem datastore. c (Optional) If you selected a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the Storage DRS cluster. d Click Next.

- 8 Select a destination network for all VM network adapters connected to a valid source network and click **Next**.

You can click **Advanced** to select a new destination network for each VM network adapter connected to a valid source network.

You can migrate a virtual machine network to another distributed switch in the same or to another data center or vCenter Server.

9 Select the migration priority level and click **Next**.

Option	Description
Schedule vMotion with high priority	vCenter Server attempts to reserve resources on both the source and destination hosts to be shared among all concurrent migrations with vMotion. vCenter Server grants a larger share of host CPU resources. If sufficient CPU resources are not immediately available, vMotion is not initiated.
Schedule regular vMotion	vCenter Server reserves resources on both the source and destination hosts to be shared among all concurrent migration with vMotion. vCenter Server grants a smaller share of host CPU resources. If there is a lack of CPU resources, the duration of vMotion can be extended.

10 On the Ready to complete page, review the details and click **Finish**.

vCenter Server moves the virtual machine to the new host or storage location.

Event messages appear in the **Events** tab. The data displayed on the **Summary** tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

Migrate a Virtual Machine to a New Compute Resource and Storage in the vSphere Web Client

You can move a virtual machine to another compute resource and move its disks or virtual machine folder to another datastore. With vMotion, you can migrate a virtual machine and its disks and files while the virtual machine is powered on.

Simultaneous migration to a new compute resource and datastore provides greater mobility for virtual machines by eliminating the vCenter Server boundary. Virtual machine disks or contents of the virtual machine folder are transferred over the vMotion network to reach the destination host and datastores.

To make disk format changes and preserve them, you must select a different datastore for the virtual machine files and disks. You cannot preserve disk format changes if you select the same datastore on which the virtual machine currently resides.

Prerequisites

- Verify that your hosts and virtual machines meet the requirements for live migration. See "Requirements and Limitations for vMotion Without Shared Storage" in the *vCenter Server and Host Management* documentation.
- For migration across vCenter Server instances, verify whether your system meets additional requirements. See "Requirements for Migration Across vCenter Servers" in the *vCenter Server and Host Management* documentation.
- Required privilege: **Resource.Migrate powered on virtual machine**

Procedure

- 1 Right-click the virtual machine and select **Migrate**.
 - a To locate a virtual machine, select a data center, folder, cluster, resource pool, host, or vApp.
 - b Click the **Virtual Machines** tab.

- 2 Select **Change both compute resource and storage** and click **Next**.

- 3 Select a destination resource for the virtual machine, and click **Next**.

Any compatibility problems appear in the Compatibility panel. Fix the problem, or select another host or cluster.

Possible targets include hosts and fully automated DRS clusters. If your target is a non-automated cluster, select a host within the non-automated cluster.

If your environment has more than one vCenter Server instances, you can move virtual machines from one vCenter Server inventory to another.

Important If the virtual machine that you migrate has an NVDIMM device and uses PMem storage, the destination host or cluster must have available PMem resources. Otherwise, the compatibility check fails and you cannot proceed further with the migration.

If the virtual machine that you migrate does not have an NVDIMM device but it uses PMem storage, you must select a host or cluster with available PMem resources, so that all PMem hard disks remain stored on a PMem datastore. Otherwise, all the hard disks use the storage policy and datastore selected for the configuration files of the virtual machine.

Important Migrating a virtual machine that has an NVDIMM device or a vPMem disk to a host that does not have the proper license fails and leaves the virtual machine in an unmanageable state for 90 seconds. You can afterwards retry the migration and select a destination host that is licensed to use PMem devices.

- 4 Select the format for the virtual machine's disks.

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

- 5 Select a virtual machine storage policy from the **VM Storage Policy** drop-down menu.

Storage policies specify storage requirements for applications that run on the virtual machine. You can also select the default policy for vSAN or Virtual Volumes datastores.

Important If the virtual machine hard disks use different storage policies, the new policy that you select only applies to non-PMem hard disks. PMem hard disks are migrated to the host-local PMem datastore of the destination host.

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

Option	Action
Store all virtual machine files in the same location on a datastore.	Select a datastore and click Next .
Store all virtual machine files in the same Storage DRS cluster.	<ul style="list-style-type: none"> a Select a Storage DRS cluster. b (Optional) To disable Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the Storage DRS cluster. c Click Next.
Store virtual machine configuration files and disks in separate locations.	<ul style="list-style-type: none"> a Click Advanced. <ul style="list-style-type: none"> Note You can use the Advanced option to downgrade from or upgrade to PMem storage. b For the virtual machine configuration file and for each virtual disk, select Browse, and select a datastore or Storage DRS cluster. <ul style="list-style-type: none"> Note Configuration files cannot be stored on a PMem datastore. c (Optional) If you selected a Storage DRS cluster and do not want to use Storage DRS with this virtual machine, select Disable Storage DRS for this virtual machine and select a datastore within the Storage DRS cluster. d Click Next.

- 7 Select a destination network for all VM network adapters connected to a valid source network and click **Next**.

You can click **Advanced** to select a new destination network for each VM network adapter connected to a valid source network.

You can migrate a virtual machine network to another distributed switch in the same or to another data center or vCenter Server.

- 8 Select the migration priority level and click **Next**.

Option	Description
Schedule vMotion with high priority	vCenter Server attempts to reserve resources on both the source and destination hosts to be shared among all concurrent migrations with vMotion. vCenter Server grants a larger share of host CPU resources. If sufficient CPU resources are not immediately available, vMotion is not initiated.
Schedule regular vMotion	vCenter Server reserves resources on both the source and destination hosts to be shared among all concurrent migration with vMotion. vCenter Server grants a smaller share of host CPU resources. If there is a lack of CPU resources, the duration of vMotion can be extended.

- 9 On the Ready to complete page, review the details and click **Finish**.

vCenter Server moves the virtual machine to the new host or storage location.

Event messages appear in the **Events** tab. The data displayed on the **Summary** tab shows the status and state throughout the migration. If errors occur during migration, the virtual machines revert to their original states and locations.

Upgrading Virtual Machines

You can upgrade virtual machines to a higher level of compatibility and a higher version of VMware tools. After the upgrade, your VMs can take advantage of new hardware options and new features.

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

To determine whether your virtual machines are compatible with a new version of ESXi, see [Virtual Machine Compatibility](#).

VMware Tools Upgrade

The first step in upgrading virtual machines is to upgrade VMware Tools. Installing VMware Tools is part of the process of creating a new virtual machine. 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. For information about installing, upgrading, and configuring VMware Tools, see the *VMware Tools User Guide*.

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.

Virtual Machine Compatibility Upgrade

VMware offers the following tools for upgrading virtual machines:

vSphere Client

Requires that you perform the virtual machine upgrade one step at a time, but does not require vSphere Update Manager.

In the vSphere Client, you can upgrade virtual machines manually, or schedule upgrades.

Manual Upgrade	Use this procedure to upgrade one or more virtual machines to the latest supported virtual hardware version immediately.
Schedule VM Upgrades	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.

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.

Note Do not use `vmware-vmupgrade.exe` to upgrade virtual machines.

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

This chapter includes the following topics:

- [Downtime for Upgrading Virtual Machines](#)
- [Upgrade the Compatibility of a Virtual Machine Manually](#)
- [Schedule a Compatibility Upgrade for Virtual Machines](#)

Downtime for Upgrading Virtual Machines

During a virtual machine compatibility upgrade, you must shut down the virtual machine for all guest operating systems. For VMware Tools upgrade, downtime is not required for many Linux operating systems.

Table 10-1. 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.

Table 10-1. Virtual Machine Downtime by Guest Operating System (Continued)

Guest Operating System	Upgrade VMware Tools	Upgrade Virtual Machine Compatibility
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.

Note 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>. Manual restart is not required for the Linux guest operating system using kernel version 3.10.

Planning Downtime for Virtual Machines

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.

Upgrade the Compatibility of a Virtual Machine Manually

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 additional hardware available to the virtual machine.

Important Upgrading virtual machine hardware 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 VMs, the virtual machine might lose its network settings if you upgrade the compatibility before you upgrade VMware Tools.

- Verify that all virtual machines and their .vmdk files are stored on storage connected to the ESXi host or the client machine.
- Determine the ESXi versions that you want the virtual machines to be compatible with. See [Virtual Machine Compatibility](#).
- Check whether the guest operating systems of the virtual machines that you upgrade require a power off. For example, some Linux operating systems do not require a power-off before a virtual machine compatibility upgrade. See [Downtime for Upgrading Virtual Machines](#).

Procedure

- 1 In the vSphere Client, navigate to the virtual machine.
- 2 (Optional) Right-click the virtual machine and select **Power > Power Off**.
- 3 Select **Actions > Compatibility > Upgrade VM Compatibility**.
- 4 Click **Yes** to confirm the upgrade.
- 5 Select a compatibility and click **OK**.

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 of a Virtual Machine Manually](#).

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 to the latest version of VMware Tools. If you upgrade the compatibility before you upgrade VMware Tools, the virtual machine might lose its network settings.
- Verify that all .vmdk files are available to the ESX/ESXi host on a VMFS5 or NFS datastore.
- Verify that the virtual machines are stored on 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 **VMs** tab and click **Virtual Machines**.
- 3 Power off the selected virtual machines.
- 4 Select **Actions > Compatibility > Schedule VM Compatibility Upgrade...**
- 5 Click **Yes** to confirm the upgrade.
- 6 Select the ESXi versions for the virtual machines to be compatible with.
- 7 (Optional) Select **Only upgrade after normal guest OS shutdown**.

This prevents the scheduled upgrade from occurring unless the guest operating system of the virtual machine is shut down or restarted normally.

Each of the selected virtual machines is upgraded to the compatibility that you chose at the next reboot of the virtual machine, and the Compatibility setting is updated in the Summary tab of the virtual machine.

Required Privileges for Common Tasks

11

Many tasks require permissions on multiple objects in the inventory. If the user who attempts to perform the task only has privileges on one object, the task cannot complete successfully.

The following table lists common tasks that require more than one privilege. You can add permissions to inventory objects by pairing a user with one of the predefined roles or with multiple privileges. If you expect that you assign a set of privileges multiple times, create custom roles.

If the task that you want to perform is not in this table, the following rules explain where you must assign permissions to allow particular operations:

- Any operation that consumes storage space requires the **Datastore.Allocate Space** privilege on the target datastore, and the privilege to perform the operation itself. You must have these privileges, for example, when creating a virtual disk or taking a snapshot.
- Moving an object in the inventory hierarchy requires appropriate privileges on the object itself, the source parent object (such as a folder or cluster), and the destination parent object.
- Each host and cluster has its own implicit resource pool that contains all the resources of that host or cluster. Deploying a virtual machine directly to a host or cluster requires the **Resource.Assign Virtual Machine to Resource Pool** privilege.

Table 11-1. Required Privileges for Common Tasks

Task	Required Privileges	Applicable Role
Create a virtual machine	On the destination folder or data center:	Administrator
	■ Virtual machine.Inventory.Create new	
	■ Virtual machine.Configuration.Add new disk (if creating a new virtual disk)	
	■ Virtual machine.Configuration.Add existing disk (if using an existing virtual disk)	
	■ Virtual machine.Configuration.Raw device (if using an RDM or SCSI pass-through device)	
	On the destination host, cluster, or resource pool: Resource.Assign virtual machine to resource pool	Resource pool administrator or Administrator
	On the destination datastore or the folder that contains the datastore: Datastore.Allocate space	Datastore Consumer or Administrator

Table 11-1. Required Privileges for Common Tasks (Continued)

Task	Required Privileges	Applicable Role
	On the network that the virtual machine will be assigned to: Network.Assign network	Network Consumer or Administrator
Power on a virtual machine	On the data center in which the virtual machine is deployed: Virtual machine .Interaction .Power On On the virtual machine or folder of virtual machines: Virtual machine .Interaction .Power On	Virtual Machine Power User or Administrator
Deploy a virtual machine from a template	On the destination folder or data center: <ul style="list-style-type: none"> ■ Virtual machine .Inventory.Create from existing ■ Virtual machine.Configuration.Add new disk 	Administrator
	On a template or folder of templates: Virtual machine .Provisioning.Deploy template	Administrator
	On the destination host, cluster or resource pool: Resource.Assign virtual machine to resource pool	Administrator
	On the destination datastore or folder of datastores: Datastore.Allocate space	Datastore Consumer or Administrator
	On the network that the virtual machine will be assigned to: Network.Assign network	Network Consumer or Administrator
Take a virtual machine snapshot	On the virtual machine or a folder of virtual machines: Virtual machine .Snapshot management. Create snapshot	Virtual Machine Power User or Administrator
Move a virtual machine into a resource pool	On the virtual machine or folder of virtual machines: <ul style="list-style-type: none"> ■ Resource.Assign virtual machine to resource pool ■ Virtual machine .Inventory.Move 	Administrator
	On the destination resource pool: Resource.Assign virtual machine to resource pool	Administrator
Install a guest operating system on a virtual machine	On the virtual machine or folder of virtual machines: <ul style="list-style-type: none"> ■ Virtual machine.Interaction .Answer question ■ Virtual machine .Interaction .Console interaction ■ Virtual machine .Interaction .Device connection ■ Virtual machine .Interaction .Power Off ■ Virtual machine .Interaction .Power On ■ Virtual machine .Interaction .Reset ■ Virtual machine .Interaction .Configure CD media (if installing from a CD) ■ Virtual machine .Interaction .Configure floppy media (if installing from a floppy disk) ■ Virtual machine .Interaction .VMware Tools install 	Virtual Machine Power User or Administrator

Table 11-1. Required Privileges for Common Tasks (Continued)

Task	Required Privileges	Applicable Role
	<p>On a datastore that contains the installation media ISO image:</p> <p>Datastore.Browse datastore (if installing from an ISO image on a datastore)</p> <p>On the datastore to which you upload the installation media ISO image:</p> <ul style="list-style-type: none"> ■ Datastore.Browse datastore ■ Datastore.Low level file operations 	Virtual Machine Power User or Administrator
Migrate a virtual machine with vMotion	<p>On the virtual machine or folder of virtual machines:</p> <ul style="list-style-type: none"> ■ Resource.Migrate powered on virtual machine ■ Resource.Assign Virtual Machine to Resource Pool (if destination is a different resource pool from the source) 	Resource Pool Administrator or Administrator
	<p>On the destination host, cluster, or resource pool (if different from the source):</p> <p>Resource.Assign virtual machine to resource pool</p>	Resource Pool Administrator or Administrator
Cold migrate (relocate) a virtual machine	<p>On the virtual machine or folder of virtual machines:</p> <ul style="list-style-type: none"> ■ Resource.Migrate powered off virtual machine ■ Resource.Assign virtual machine to resource pool (if destination is a different resource pool from the source) 	Resource Pool Administrator or Administrator
	<p>On the destination host, cluster, or resource pool (if different from the source):</p> <p>Resource.Assign virtual machine to resource pool</p>	Resource Pool Administrator or Administrator
	<p>On the destination datastore (if different from the source):</p> <p>Datastore.Allocate space</p>	Datastore Consumer or Administrator
Migrate a virtual machine with Storage vMotion	<p>On the virtual machine or folder of virtual machines:</p> <p>Resource.Migrate powered on virtual machine</p>	Resource Pool Administrator or Administrator
	<p>On the destination datastore:</p> <p>Datastore.Allocate space</p>	Datastore Consumer or Administrator
Move a host into a cluster	<p>On the host:</p> <p>Host.Inventory.Add host to cluster</p>	Administrator
	<p>On the destination cluster:</p> <p>Host.Inventory.Add host to cluster</p>	Administrator
Encrypt a virtual machine	<p>Encryption tasks are possible only in environments that include vCenter Server. In addition, the ESXi host must have encryption mode enabled for most encryption tasks. The user who performs the task must have the appropriate privileges. A set of Cryptographic Operations privileges allows fine-grained control. For more information, see the <i>vSphere Security</i> documentation.</p>	Administrator

Troubleshooting Overview

vSphere Troubleshooting contains common troubleshooting scenarios and provides solutions for each of these problems. You can also find guidance here for resolving problems that have similar origins. For unique problems, consider developing and adopting a troubleshooting methodology.

The following approach for effective troubleshooting elaborates on how to gather troubleshooting information, such as identifying symptoms and defining the problem space. Troubleshooting with log files is also discussed.

This chapter includes the following topics:

- [Guidelines for Troubleshooting](#)
- [Troubleshooting with Logs](#)

Guidelines for Troubleshooting

To troubleshoot your implementation of vSphere, identify the symptoms of the problem, determine which of the components are affected, and test possible solutions.

Identifying Symptoms	A number of potential causes might lead to the under-performance or nonperformance of your implementation. The first step in efficient troubleshooting is to identify exactly what is going wrong.
Defining the Problem Space	After you have isolated the symptoms of the problem, you must define the problem space. Identify the software or hardware components that are affected and might be causing the problem and those components that are not involved.
Testing Possible Solutions	When you know what the symptoms of the problem are and which components are involved, test the solutions systematically until the problem is resolved.



Troubleshooting Basics (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere_troubleshooting)

Identifying Symptoms

Before you attempt to resolve a problem in your implementation, you must identify precisely how it is failing.

The first step in the troubleshooting process is to gather information that defines the specific symptoms of what is happening. You might ask these questions when gathering this information:

- What is the task or expected behavior that is not occurring?
- Can the affected task be divided into subtasks that you can evaluate separately?
- Is the task ending in an error? Is an error message associated with it?
- Is the task completing but in an unacceptably long time?
- Is the failure consistent or sporadic?
- What has changed recently in the software or hardware that might be related to the failure?

Defining the Problem Space

After you identify the symptoms of the problem, determine which components in your setup are affected, which components might be causing the problem, and which components are not involved.

To define the problem space in an implementation of vSphere, be aware of the components present. In addition to VMware software, consider third-party software in use and which hardware is being used with the VMware virtual hardware.

Recognizing the characteristics of the software and hardware elements and how they can impact the problem, you can explore general problems that might be causing the symptoms.

- Misconfiguration of software settings
- Failure of physical hardware
- Incompatibility of components

Break down the process and consider each piece and the likelihood of its involvement separately. For example, a case that is related to a virtual disk on local storage is probably unrelated to third-party router configuration. However, a local disk controller setting might be contributing to the problem. If a component is unrelated to the specific symptoms, you can probably eliminate it as a candidate for solution testing.

Think about what changed in the configuration recently before the problems started. Look for what is common in the problem. If several problems started at the same time, you can probably trace all the problems to the same cause.

Testing Possible Solutions

After you know the problem's symptoms and which software or hardware components are most likely involved, you can systematically test solutions until you resolve the problem.

With the information that you have gained about the symptoms and affected components, you can design tests for pinpointing and resolving the problem. These tips might make this process more effective.

- Generate ideas for as many potential solutions as you can.
- Verify that each solution determines unequivocally whether the problem is fixed. Test each potential solution but move on promptly if the fix does not resolve the problem.

- Develop and pursue a hierarchy of potential solutions based on likelihood. Systematically eliminate each potential problem from the most likely to the least likely until the symptoms disappear.
- When testing potential solutions, change only one thing at a time. If your setup works after many things are changed at once, you might not be able to discern which of those things made a difference.
- If the changes that you made for a solution do not help resolve the problem, return the implementation to its previous status. If you do not return the implementation to its previous status, new errors might be introduced.
- Find a similar implementation that is working and test it in parallel with the implementation that is not working properly. Make changes on both systems at the same time until few differences or only one difference remains between them.

Troubleshooting with Logs

You can often obtain valuable troubleshooting information by looking at the logs provided by the various services and agents that your implementation is using.

Most logs are located in `C:\ProgramData\VMware\vCenterServer\logs` for Windows deployments or `/var/log/` for Linux deployments. Common logs are available in all implementations. Other logs are unique to certain deployment options (Management Node or Platform Services Controller).

Common Logs

The following logs are common to all deployments on Windows or Linux.

Table 12-1. Common Log Directories

Log Directory	Description
applmgmt	VMware Appliance Management Service
cloudvm	Logs for allotment and distribution of resources between services
cm	VMware Component Manager
firstboot	Location where first boot logs are stored
rhttpproxy	Reverse Web Proxy
sca	VMware Service Control Agent
statsmonitor	Vmware Appliance Monitoring Service (Linux only)
vapi	VMware vAPI Endpoint
vmaffd	VMware Authentication Framework daemon
vmdird	VMware Directory Service daemon
vmon	VMware Service Lifecycle Manager

Management Node Logs

The following logs are available if a management node deployment is chosen.

Table 12-2. Management Node Log Directories

Log Directory	Description
autodeploy	VMware vSphere Auto Deploy Waiter
content-library	VMware Content Library Service
eam	VMware ESX Agent Manager
invsvc	VMware Inventory Service
mbcs	VMware Message Bus Config Service
netdump	VMware vSphere ESXi Dump Collector
perfcharts	VMware Performance Charts
vmcam	VMware vSphere Authentication Proxy
vmldird	VMware Directory Service daemon
vmsyslog collector	vSphere Syslog Collector (Windows only)
vmware-sps	VMware vSphere Profile-Driven Storage Service
vmware-vpx	VMware VirtualCenter Server
vpostgres	vFabric Postgres database service
mbcs	VMware Message Bus Config Service
vsphere-client	VMware vSphere Web Client
vcha	VMware High Availability Service (Linux only)

Platform Services Controller Logs

You can examine the following logs if a Platform Services Controller node deployment is chosen.

Table 12-3. Platform Services Controller Node Log Directories

Log Directory	Description
cis-license	VMware Licensing Service
sso	VMware Secure Token Service
vmcad	VMware Certificate Authority daemon
vmldird	VMware Directory Service

For Platform Services Controller node deployments, additional runtime logs are located at `C:\ProgramData\VMware\CIS\runtime\VMwareSTSService\logs`.

Troubleshooting Virtual Machines

13

The virtual machine troubleshooting topics provide solutions to potential problems that you might encounter when using your virtual machines.

This chapter includes the following topics:

- [Troubleshooting USB Passthrough Devices](#)
- [Recover Orphaned Virtual Machines](#)
- [Virtual Machine Does Not Power On After Cloning or Deploying from Template](#)

Troubleshooting USB Passthrough Devices

Information about feature behavior can help you troubleshoot or avoid potential problems when USB devices are connected to a virtual machine.

Error Message When You Try to Migrate Virtual Machine with USB Devices Attached

Migration with vMotion cannot proceed and issues a confusing error message when you connect multiple USB devices from an ESXi host to a virtual machine and one or more devices are not enabled for vMotion.

Problem

The Migrate Virtual Machine wizard runs a compatibility check before a migration operation begins. If unsupported USB devices are detected, the compatibility check fails and an error message similar to the following appears: Currently connected device 'USB 1' uses backing 'path:1/7/1', which is not accessible.

Cause

To successfully pass vMotion compatibility checks, you must enable all USB devices that are connected to the virtual machine from a host for vMotion. If one or more devices are not enabled for vMotion, migration will fail.

Solution

- 1 Make sure that the devices are not in the process of transferring data before removing them.

- 2 Re-add and enable vMotion for each affected USB device.

Cannot Copy Data From an ESXi Host to a USB Device That Is Connected to the Host

You can connect a USB device to an ESXi host and copy data to the device from the host. For example, you might want to gather the vm-support bundle from the host after the host loses network connectivity. To perform this task, you must stop the USB arbitrator.

Problem

If the USB arbitrator is being used for USB passthrough from an ESXi host to a virtual machine the USB device appears under `lsusb` but does not mount correctly.

Cause

This problem occurs because the nonbootable USB device is reserved for the virtual machine by default. It does not appear on the host's file system, even though `lsusb` can see the device.

Solution

- 1 Stop the `usbarbitrator` service: `/etc/init.d/usbarbitrator stop`
- 2 Physically disconnect and reconnect the USB device.
By default, the device location is `/vmfs/devices/disks/mpx.vmhbaXX:C0:T0:L0`.
- 3 After you reconnect the device, restart the `usbarbitrator` service: `/etc/init.d/usbarbitrator start`
- 4 Restart `hostd` and any running virtual machines to restore access to the passthrough devices in the virtual machine.

What to do next

Reconnect the USB devices to the virtual machine.

Recover Orphaned Virtual Machines

Virtual machines appear with (orphaned) appended to their names.

Problem

Virtual machines that reside on an ESXi host that vCenter Server manages might become orphaned in rare cases. Such virtual machines exist in the vCenter Server database, but the ESXi host no longer recognizes them.

Cause

Virtual machines can become orphaned if a host failover is unsuccessful, or when the virtual machine is unregistered directly on the host. If this situation occurs, move the orphaned virtual machine to another host in the data center on which the virtual machine files are stored.

Solution

- 1 Determine the datastore where the virtual machine configuration (.vmx) file is located.
 - a Select the virtual machine in the vSphere Web Client inventory, and click the **Datastores** tab.
The datastore or datastores where the virtual machine files are stored are displayed.
 - b If more than one datastore is displayed, select each datastore and click the file browser icon to browse for the .vmx file.
 - c Verify the location of the .vmx file.
- 2 Return to the virtual machine in the vSphere Web Client, right-click it, and select **All Virtual Infrastructure Actions > Remove from Inventory**.
- 3 Click **Yes** to confirm the removal of the virtual machine.
- 4 Reregister the virtual machine with vCenter Server.
 - a Right-click the datastore where the virtual machine file is located and select **Register VM**.
 - b Browse to the .vmx file and click **OK**.
 - c Select the location for the virtual machine and click **Next**.
 - d Select the host on which to run the virtual machine and click **Next**.
 - e Click **Finish**.

Virtual Machine Does Not Power On After Cloning or Deploying from Template

Virtual machines do not power on after you complete the clone or deploy from template workflow in the vSphere Web Client.

Problem

When you clone a virtual machine or deploy a virtual machine from a template, you might not be able to power on the virtual machine after creation.

Cause

The swap file size is not reserved when the virtual machine disks are created.

Solution

- Reduce the size of the swap file that is required for the virtual machine. You can do this by increasing the virtual machine memory reservation.
 - a Right-click the virtual machine and select **Edit Settings**.
 - b Select **Virtual Hardware** and click **Memory**.

- c Use the Reservation drop-down menu to increase the amount of memory allocated to the virtual machine.
- d Click **OK**.
- Alternatively, you can increase the amount of space available for the swap file by moving other virtual machine disks off the datastore that is being used for the swap file.
 - a Browse to the datastore in the vSphere Web Client object navigator.
 - b Select the **VMs** tab.
 - c For each virtual machine to move, right-click the virtual machine and select **Migrate**.
 - d Select **Change storage only**.
 - e Proceed through the **Migrate Virtual Machine** wizard.
- You can also increase the amount of space available for the swap file by changing the swap file location to a datastore with adequate space.
 - a Browse to the host in the vSphere Web Client object navigator.
 - b Select the **Configure** tab.
 - c Under Virtual Machines, select **Swap file location**.
 - d Click **Edit**.

Note If the host is part of a cluster that specifies that the virtual machine swap files are stored in the same directory as the virtual machine, you cannot click **Edit**. You must use the Cluster Settings dialog box to change the swap file location policy for the cluster.

- e Select **Use a specific datastore** and select a datastore from the list.
- f Click **OK**.