Managing Virtual Machines in VMware Cloud on AWS

5 September 2018
VMware Cloud on AWS

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

Contents

About Managing Virtual Machines in VMware Cloud on AWS

The *Managing Virtual Machines in VMware Cloud on AWS* documentation explains how to deploy, configure, and customize virtual machines in a VMware Cloud on AWS data center.

You learn about deploying a VM from scratch, or by cloning existing templates, configuring virtual machine hardware, and customizing virtual machine behavior. The documentation also explains how to use content libraries, and how to secure and upgrade your VMs.

Table 1. ***Managing Virtual Machines in VMware Cloud on AWS*** **Highlights**

Topics	Content Highlights
Introduction to vSphere Virtual Machines	■ Overview of VM lifecycle and components. ■ List of VM files and what they're used for. ■ Overview of VM hardware and other options.
Deploying Virtual Machines Deploying OVF and OVA Templates	Step-by-step instructions for creating VMs. You have many options, including: ■ Deploying a VM from scratch. ■ Cloning existing VMs or templates ■ Deploying an OVF or OVA template ■ Deploying a VM from an OVF or OVA
Using Content Libraries	Content libraries allow you to store VM templates and use them to deploy new VMs. With hybrid linked mode, you will be able to share VM templates between an on-prem environment and VMware Cloud on AWS.
Configuring Virtual Machine Hardware	Detailed information about the options for configuring different hardware options, such as CPU, memory, and devices. You can modify existing virtual devices or add new devices - but the options in VMware Cloud on AWS are different from the options in an on-premises environment.

Table 1. *Managing Virtual Machines in VMware Cloud on AWS* Highlights (Continued)

Topics	Content Highlights
Configuring Virtual Machine Options	Explains how VM options and how to change them. ■ Power Management settings ■ UEFI secure boot for virtual machines ■ VM Boot options ■ Advance options such as logging, debugging, and latency sensitivity
Customizing Virtual Machines	Instructions for performing post-deployment customization tasks, including: ■ Options for installing a guest OS ■ Customizing the guest OS with a customization spec ■ Using a virtual machine console ■ Using snapshots ■ Upgrading VMware Tools or the Hardware Compatibility setting.

Intended Audience

This information is intended for anyone who wants to use VMware Cloud on AWS to create, configure, and manage an SDDC. The information is written for administrators who have a basic understanding of configuring and managing vSphere in an on-premises environment and are familiar with virtualization concepts. In-depth knowledge of Amazon Web Services is not required.

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

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`	*`vmname`*`.vmx`	Virtual machine configuration file
`.vmxf`	*`vmname`*`.vmxf`	Additional virtual machine configuration files

Table 1-1. Virtual Machine Files (Continued)

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

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.

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.

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 *Managing the VMware Cloud on AWS Data Center* 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.

Table 1-2. Virtual Machine Hardware and Descriptions

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

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

Hardware Device	Description
Pointing device	Mirrors the pointing device that is connected to the virtual machine console when you first connect to the console.
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 physical USB devices must be connected to your client computer.
VMCI	Virtual Machine Communication Interface device. Provides a high-speed communication channel between a virtual machine and the hypervisor. You cannot add or remove VMCI devices.
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 and Resources

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

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

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

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

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

VMware virtual machines have the following options:

General Options	View or modify the virtual machine name, and check the location of the configuration file and the working location of the virtual machine.
VMware Tools	Manage the power controls for the virtual machine and run VMware Tools scripts. You can also upgrade VMware Tools during power cycling and synchronize guest time with the host.
Advanced Options	Disable acceleration and enable logging, configure debugging and statistics, and change the swap file location. You can also change the latency sensitivity and add configuration parameters.
Power Management	Manage guest power options. Suspend the virtual machine or leave the virtual machine powered on when you put the guest operating system into standby.
CPUID Mask	Hide or expose the `NX/XD` flag. Hiding the `NX/XD` flag increases vMotion compatibility between hosts.
Memory/CPU Hotplug	Enable or disable CPU and memory hotplug. You can add Memory or CPU resources to a virtual machine while the virtual machine is running. You can disable Memory or CPU hotplug to avoid adding memory or CPUs while the virtual machine is running. Memory hotplug is supported on all 64 bit operating systems, but to use the added memory, the guest operating system must also support this feature. See the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility.
Boot Options	Set the boot delay when powering on virtual machines or to force BIOS setup and configure failed boot recovery.

Fibre Channel NPIV	Control virtual machine access to LUNs on a per-virtual machine basis. N-port ID virtualization (NPIV) provides the ability to share a single physical Fibre Channel HBA port among multiple virtual ports, each with unique identifiers.
vApp Options	Enable or disable vApp functionality. When you select the checkbox, you can view and edit vApp properties, vApp Deployment options, and vApp Authoring options. For example, you can configure an IP allocation policy or a network protocol profile for the vApp. A vApp option that is specified at the level of a virtual machine overrides the settings specified at the level of the vApp.

vSphere Web Client

All administrative functions are available through the vSphere Web Client.

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

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

Where to Go From Here

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

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

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

Deploying Virtual Machines 2

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 VMware Cloud on AWS.

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 VMware Cloud on AWS.

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 VMware Cloud on AWS.

This chapter includes the following topics:

- Clone a Template to a Template
- 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

On VMware Cloud on AWS, you can create VMs from the following objects:

- Workloads folder and subfolders
- Compute-ResourcePool and child resource pools

Procedure

1. From the vSphere Client VMs and Templates view, right click a valid parent object of a VM, such as the **Workloads** folder, 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.

   On VMware Cloud on AWS, select the Workloads folder or one of its subfolder.
4. On the Select a compute resource page, select the Compute-ResourcePool or one of its child resource pools and click **Next**.

   If creating the virtual machine at the selected location causes compatibility problems, an alarm appears in the **Compatibility** pane.
5. On the Select storage page, select the **WorkloadDatastore**.

   You can optionally change the VM Storage Policy, or change it later.
6. On the Select compatibility page, select the virtual machine compatibility with ESXi host versions and click **Next**.

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 in VMware Cloud on AWS

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.

Procedure

1 Open a wizard to start the cloning a virtual machine procedure:

Option	Description
Open the New Virtual Machine wizard from an object in the inventory	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 **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 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 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 a different way.

3 On the Select a compute resource page, select Compute-ResourcePool or a child resource pool.

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 template configuration files and all of the virtual disks and click **Next**.

   a Choose the type of storage for the template by selecting the **Standard**, the **PMem**, or the **Hybrid** radio button.

   If you choose the **Hybrid** mode, all Pmem virtual disks will remain stored on a Pmem database. Non-Pmem disks are affected by your choice of a VM storage policy and datastore or datastore cluster.

   b (Optional) From the **VM Storage Policy** drop-down menu, select a virtual machine storage policy or leave the default.

   c Select a datastore or a datastore cluster.

   d (Optional) Select the **Disable Storage DRS for this virtual machine** check box if you do not want to use storage DRS with the virtual machine.

   e (Optional) Select the **Configure per disk** option if you need a separate datastore or a datastor cluster for the template configuration file and for each virtual disk.

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 in VMware Cloud on AWS

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.

Procedure

1 Start the **Deploy From Template** wizard.

Option	Description
Start the Deploy From Template wizard from an object in the inventory	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 **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.
Start 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.

   In VMware Cloud on AWS, select WorkloadFolder or one of its subfolders.

3 On the Select a compute resource page, select the Compute-ResourcePool or one of its child resource pools and click **Next**.

   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**.

   a Choose the type of storage for the virtual machine by selecting the **Standard**, the **PMem**, or the **Hybrid** radio button.

      If you choose the **Hybrid** mode, all PMem virtual disks will remain stored on a PMem database. Non-PMem disks are affected by your choice of a VM storage policy and datastore or datastore cluster.

   b (Optional) From the **VM Storage Policy** drop-down menu, select a virtual machine storage policy or leave the default one.

   c Select a datastore or a datastore cluster.

   d (Optional) Select the **Disable Storage DRS for this virtual machine** check box if you do not want to use storage DRS with the virtual machine.

   e (Optional) Turn on the **Configure per disk** option to select a separate datastore or a datastor cluster for the virtual machine configuration file and for its virtual disks.

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 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.

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**.

Clone an Existing Virtual Machine in VMware Cloud on AWS

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.

Procedure

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

Option	Description
Open the Clone Existing Virtual Machine wizard from a object in the inventory	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 **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 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 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 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 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**.

   a Choose the type of storage for the template by selecting the **Standard**, the **PMem**, or the **Hybrid** radio button.

      If you choose the **Hybrid** mode, all PMem virtual disks will remain stored on a PMem database. Non-PMem disks are affected by your choice of a VM storage policy and datastore or datastore cluster.

   b (Optional) From the **VM Storage Policy** drop-down menu, select a virtual machine storage policy or leave the default one.

   c Select a datastore or a datastore cluster.

   d (Optional) Select the **Disable Storage DRS for this virtual machine** check box if you do not want to use storage DRS with the virtual machine.

   e (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.

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 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 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	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 click **Next**.

a (Optional) Under the **Virtual Hardware** tab, click **ADD NEW DEVICE** and select a virtual hardware device to add.

b (Optional) Expand any of the listed devices to view its configuration settings and make changes.

c (Optional) Move the pointer over a device and click the **Remove** icon to remove a device from the virtual machine configuration.

You confirm the deletion of the selected device when you finish the cloning task.

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

The new virtual machine appears in the inventory.

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.

Procedure

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

Option	Description
Open the Clone Template to Template wizard from an object in the inventory	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.

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	a Choose the type of storage for the template by selecting the **Standard**, the **PMem**, or the **Hybrid** radio button. If you select the **Standard** mode, all virtual disks will be stored on a standard datastore. If you select the **PMem** mode, all virtual disks will be stored on the host-local PMem datastore. Configuration files cannot be stored ona 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 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. For more information about persistent memory and PMem storage, see the *vSphere Resource Management* guide. 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. c (Optional) From the **VM Storage Policy** drop-down menu, select a virtual machine storage policy or leave the default one. 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. 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. **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.
Clone a virtual machine that does not have vPMem hard disks	a Select the disk format for the virtual machine virtual disks. **Same format as source** uses the same disk format as the source virtual machine. 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. **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.

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.

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.

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	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.

This chapter includes the following topics:

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 From the vSphere Client VMs and Templates view, right click a valid parent object of a VM, such as the **Workloads** folder, and select **New virtual machine**.

2 Select **Deploy OVF Template**.

The **Deploy OVF Template** wizard opens.

3 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/VMTN/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.

4 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.

5 On the **Select a compute resource** page, select a resource where to run the deployed VM template, and click **Next**.

6 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.

7 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 of 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://kb.vmware.com/kb/52370.

8 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.

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 VM from an OVF Template in a Content Library

You can deploy a virtual machine from an OVF template in a local or subscribed content library.

Prerequisites

You must have a Content Library containing the OVF template you want to use.

- For more information on creating content libraries, see Create a Library.
- For more information on importing content into a content library, see Add Items to a Content Library in *Managing Virtual Machines in VMware Cloud on AWS*.

Procedure

1. From the vSphere Client VMs and Templates view, right click a valid parent object of a VM, such as the **Workloads** folder, and select **New virtual machine**.
2. Select **Deploy from template** and click **Next**.
3. Select the template to deploy.
4. Proceed through the New Virtual Machine wizard, using the following settings.
   a. For the VM folder, select **Workloads**, **Templates**, or another folder that you have write permissions on.
   b. For the compute resource, select **Compute-ResourcePool**.
   c. For the datastore, select **workloadDatastore**.
5. On the Select networks page, enter an IP address in the **IP address** field.

   The **IP Allocation Settings** on this page show only the Static IP option, even if the logical network you have selected uses DHCP. You must enter something into the **IP address** field to proceed in the wizard. If DHCP is enabled, the VM deploys with DHCP.
6. Review the VM settings and click **Finish**.

Deploy a VM from a Client OVF or OVA Template

You can deploy a VM from an OVF or OVA template on your client machine.

For more information on deploying OVF or OVA templates, see Deploying OVF and OVA Templates.

Prerequisites

Have an OVF or OVA template on your client machine.

Procedure

1. From the vSphere Client VMs and Templates view, right click the **Workloads** folder and select **Deploy OVF Template**.
2. Select **Local file**, click **Choose files**, and browse to the OVF or OVA template.

3 Proceed through the Deploy OVF Template wizard, using the following settings.

   a For the VM folder, select **Workloads**, **Templates**, or another folder that you have write permissions on.

   b For the compute resource, select **Compute-ResourcePool**.

   c For the datastore, select **workloadDatastore**.

4 On the **Select networks** page, enter an IP address in the **IP address** field.

   The **IP Allocation Settings** field is populated based on the OVF descriptor file. If the imported OVF specifies only DHCP, **IP Allocation Settings** shows only DHCP. If the OVF specifies both static IP and DHCP, **IP Allocation Settings** shows both.

Use ovftool to Deploy a VM from a Client OVF or OVA Template

You can use `ovftool` deploy a VM from an OVF or OVA template on your client machine or transfer a VM from your on-premises vSphere environment to your VMware Cloud on AWS SDDC.

VMware OVF Tool (`ovftool`) is a flexible command-line utility that you can use to migrate virtual machines between an on-premises installation and an SDDC. For more information about `ovftool`, see the OVF Tool User's Guide

Prerequisites

- You must have the CloudAdmin role to run this command.
- Configure a management VPN.
- Configure additional firewall rules for the management gateway that allow traffic on port 443 from your on-premises vSphere environment to the vCenter Server and ESXi hosts in your SDDC.

Table 3-1. Firewall Rules Required by ovftool

Name	Action	Source	Destination	Service	Ports
On-Premises to SDDC vCenter	Allow	CIDR block of on-premises data center	vCenter	HTTPS (TCP 443)	443
On-Premises to SDDC ESXi	Allow	CIDR block of on-premises data center	ESXi	HTTPS (TCP 443)	443

Procedure

- Construct an `ovftool` command line that specifies `Workloads` as the `vmFolder` and the Compute-ResourcePool.

  See Example: Use ovftool to Deploy a VM from an OVA Template.

Example: Use ovftool to Deploy a VM from an OVA Template

This example `ovftool` command deploys the OVA template in `\tmp\Example.ova` from the local host to the SDDC vCenter with FQDN *SDDC-FQDN*. The locator path (`vi`) argument specifies the required target resource pool name, .../Compute-ResourcePool.

```
ovftool --acceptAllEulas --name=Example-to-SDDC \
--datastore=WorkloadDatastore --net:Non=sddc-cgw-network-1
--vmFolder=Workloads \tmp\Example.ova \
'vi://cloudadmin@vmc.local:passwd@SDDC-FQDN/SDDC-Datacenter/host/Cluster-1/Resources/Compute-
ResourcePool/'
```

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.

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 and 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

4

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.

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:

- 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.

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	A local content library is accessible only in the vCenter Server instance where you create it by default. 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	Creates a content library that subscribes to published content library. Use this option to take advantage of already existing content libraries. 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. Provide the following information to subscribe to a library: a In the **Subscription URL** text box, enter the URL address of the published library. b If authentication is enabled on the published library, select **Enable authentication** and enter the publisher password. c Select a download method for the contents of the subscribed library. ■ If you want to download a local copy of all the 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. If you need to use an item, synchronize the item or the entire library to download its content. d If prompted, accept the SSL certificate thumbprint. The SSL certificate thumbprint is stored on your system until you delete the subscribed content library from the inventory.

4 Select the WorkloadDatastore and click **Next**.

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.

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 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 or Delete 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.

Procedure

1 In the vSphere Client, select **Menu > Content Libraries**.

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

Task	Action
Edit local content library that is unpublished	You can publish a local library to share its contents with other users. a Select the **Publish this library externally** check box to publish the local library and share its contents with other users. b Click the **Copy Link** button to obtain the URL of your library and distribute it. c (Optional) Select **Enable user authenticcation for access to this content library** to set a password for the library. If you password protect the library, you must provide both the URL and the password to users who want to subscribe to your library. d Click **OK**.
Edit local content library that is published	You can change the following settings of a local library that is published. ■ 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. 1 Click **Change Password**. 2 Enter the current password and the new password. Confirm the new password. 3 Click **OK**.
Edit subscribed content library	You can change the following settings of a subscribed library: ■ Enable or disable the automatic synchronization with the published library. ■ Update the password for authentication to the published library. ■ Select a download method. You can either download all library content immediately or download library content only when needed. If you switch from the option to download content only when needed to the option to 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.

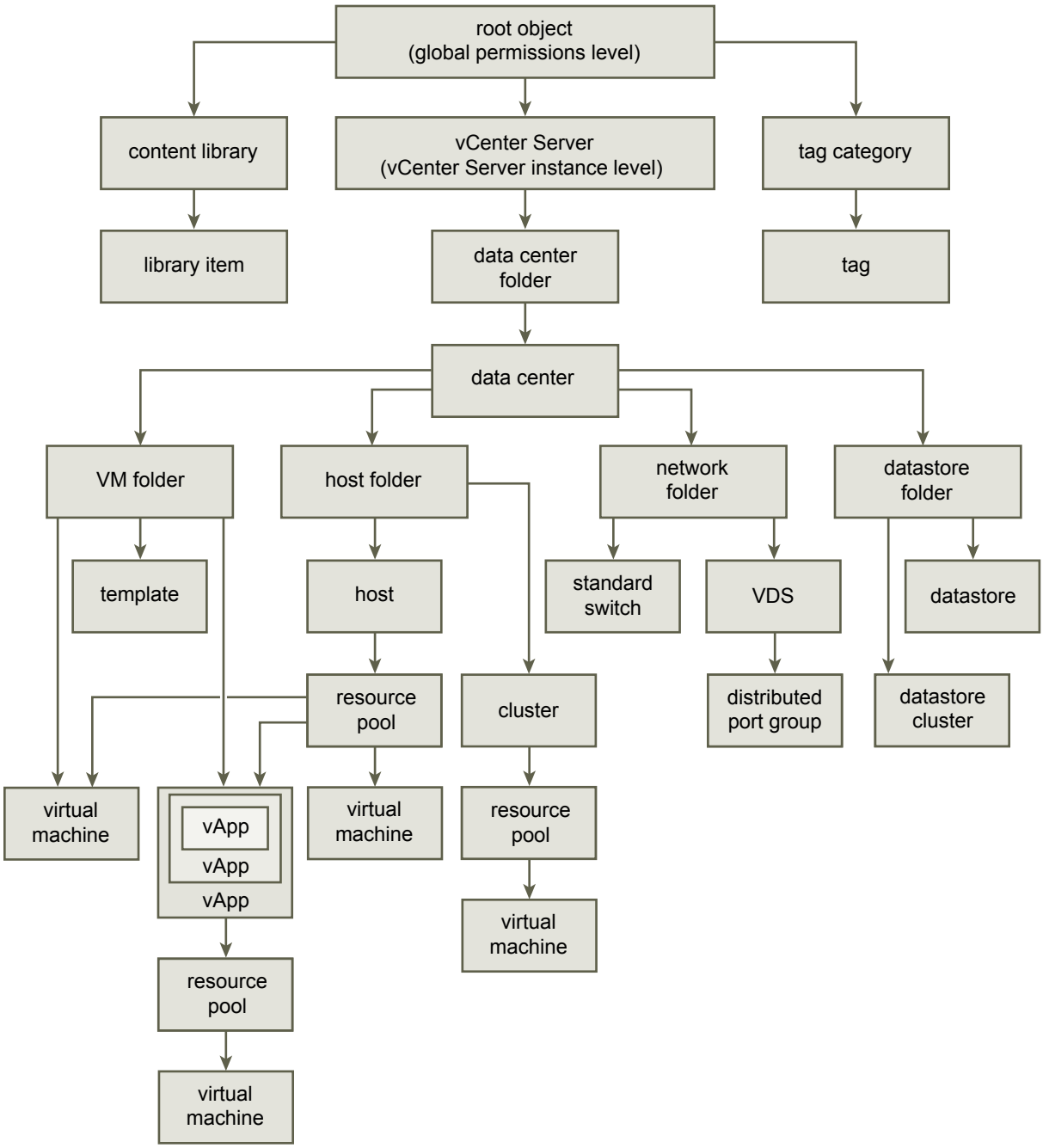
Hierarchical Inheritance of Permissions for Content Libraries

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 permission 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.

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.

- Import Items to a Content Library

  You can add items to a content library by importing files from your local machine or from a Web server. You can import OVF and OVA templates and other types of files, such as ISO images, certificates, and so on. You can keep the items in the library and share them with other users across multiple vCenter Server instances. You can also use the templates in the content library to deploy new virtual machines and vApps.

- 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 Virtual Machine Template to a Template in a Content Library

  You can add new templates to a content library by cloning virtual machines or virtual machine templates from your vCenter Server inventory to templates in the content library. You can use the content library items later to provision virtual machines on a cluster or a host. You can also update an existing template in the content library by clone a virtual machine or virtual machine template from the vCenter Server 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.

Import Items to a Content Library

You can add items to a content library by importing files from your local machine or from a Web server. You can import OVF and OVA templates and other types of files, such as ISO images, certificates, and so on. You can keep the items in the library and share them with other users across multiple vCenter Server instances. You can also use the templates in the content library to deploy new virtual machines and vApps.

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 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 the Web server where the item is. **Note** You can import either an `.ovf` or `.ova` file. The resulting content library item is of the OVF Template type.
Import from a Local 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** You can import either an `.ovf` or `.ova` file. When you import an OVF template, first select the OVF descriptor file (`.ovf`). Next, you are prompted to select the other files in the OVF template, for example the `.vmdk` file. The resulting content library item is of the OVF Template type.

vCenter Server reads and validates the manifest and certificate files in the OVF package during importing. A warning is displayed in the **Import Library Item** wizard, if certificate issues exist, for example if vCenter Server detects an expired certificate.

Note vCenter Server does not read signed content, if the OVF package is imported from an `.ovf` file from your local machine.

4 In the Destination section, enter a name and a description for the item.

5 Click **Import**.

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 Client navigator, click **Menu > VMs and Templates**.

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 Virtual Machine Template to a Template in a Content Library

You can add new templates to a content library by cloning virtual machines or virtual machine templates from your vCenter Server inventory to templates in the content library. You can use the content library items later to provision virtual machines on a cluster or a host. You can also update an existing template in the content library by clone a virtual machine or virtual machine template from the vCenter Server inventory.

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 Navigate to the virtual machine or template that you want to clone.

2 Select your task.

Option	Description
Clone a virtual machine	a Right-click the virtual machine and select **Clone > Clone as Template in Library**. The **Clone Virtual Machine To Template** wizard opens. b On the Basic information page, enter a name and description for the template, select the template type, and select an inventory folder for the template. You can create an OVF Template or VM Template in the content library. c On the Location page, select a local content library in which you want to add the template. d On the Select a compute resource page, select the compute resource for the template. e On the Select storage page, select the storage for the template disk and configuration files. f On the Review page, review the details and click **Finish** to complete the cloning task.
Clone a virtual machine template	a Right-click the virtual machine template and select **Clone to Library**. The **Clone to Template in Library** dialog box opens. b Select the **Clone as** option. You can create a new template or you can choose an existing template to update. c From the content libraries list, select the library in which you want to add the template. d Enter a name and description for the template. e 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. f click **OK**.

A new task for cloning appears in the Recent Tasks pane. After the task is complete, the template appears in the **Templates** tab for the content library. You can view the type of template in the Type column.

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	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	a Choose the type of storage for the template by selecting the **Standard**, the **PMem**, or the **Hybrid** radio button. If you select the **Standard** mode, all virtual disks will be stored on a standard datastore. 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. 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. For more information about persistent memory and PMem storage, see the *vSphere Resource Management* guide. b (Optional) From the **VM Storage Policy** drop-down menu, select a virtual machine storage policy or leave the default one. c Select a datastore or a datastore cluster. 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. 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. **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.
Deploy a virtual machine from a template that does not have vPMem hard disks	a Select the disk format for the virtual machine virtual disks. **Same format as source** uses the same disk format as the source virtual machine. 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. **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.

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 a Content Library

In the vSphere Client, you can use a content library item of the VM Template type to deploy a virtual machine to a host or cluster in your vSphere environment.

Procedure

1 In the vSphere Client, select **Menu > Content Libraries**.

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

The **Deploy From Vm template** wizard opens.

3 On the **Select a name and folder** page, enter a name and select a location for the virtual machine.

4 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.

5 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	a Choose the type of storage for the template by selecting the **Standard**, the **PMem**, or the **Hybrid** radio button. If you select the **Standard** mode, all virtual disks will be stored on a standard datastore. 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. 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. For more information about persistent memory and PMem storage, see the *vSphere Resource Management* guide. b (Optional) From the **VM Storage Policy** drop-down menu, select a virtual machine storage policy or leave the default one. c Select a datastore or a datastore cluster. 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. 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. **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.
Deploy a virtual machine from a template that does not have vPMem hard disks	a Select the disk format for the virtual machine virtual disks. **Same format as source** uses the same disk format as the source virtual machine. 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. **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.

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.

6 On the Select deploy 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.

7 (Optional) On the Customize guest OS page, select a customization specification to apply 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.

8 (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.

9 On the Ready to complete page, review the information 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 an object to deploy the vApp to and click **Next**.

   In VMware Cloud on AWS, that might be a Workload folder or resource pool.
6. On the Review details page, verify the template details and click **Next**.
7. On the Select storage page, select disk format and a storage resource for the vApp.
8. On the Select networks page, select a destination network for each source network.
9. On the Ready to Complete page, review the configurations you made for the vApp, and click **Finish**.

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

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. You can use the content library to store and manage templates of virtual machines and vApps. 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.

Content libraries support two types of templates, the OVF Template type and the VM Template type.

In a content library, you can store and manage virtual machine templates as OVF templates or VM templates. vApps are always converted to OVF templates in the content library.

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 into a template.

You can create a VM template as either a vCenter Server inventory object, or a content library item. In previous releases of vSphere, you could manage VM templates only through the vCenter Server inventory list. When you cloned a virtual machine or a VM template to a content library template, the resulting content library item was in an OVF format. Local content libraries in vSphere now support both OVF templates and VM templates. You choose the type of template when you clone the virtual machine into the content library.

vApp Templates in Content Libraries

A vApp template is a template of a vApp, which can contain multiple virtual machines or multiple vApps. A vApp template can be either a vCenter Server inventory object or a library item. A vApp template that resides in a content library is always in the 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.

The VM Template as a Content Library Item

In VMware Cloud on AWS, content libraries support both OVF and VM templates. You can choose to save and manage a virtual machine or a VM template from the vCenter Server inventory as a content library item of either the OVF format or the VM template type.

VM Template or OVF Template: Template Properties

See the table below for a detailed list of the differences between the VM template and the OVF template types.

Table 4-2. VM Templates and OVF Templates Properties

Property	VM Templates in Content Library	OVF Templates in Content Library
Datastore	VM templates are stored on the datastore that is defined in the configuration specifications of the source virtual machines.	OVF templates are stored on the datastore that is associated with the content library.
Footprint	Configurable.	Compressed or Thin.
Host/Datastore Maintenance Mode	When the host becomes inaccessible, VM templates are automatically migrated to another host. When the datastore becomes inaccessible, you must convert the VM template to a virtual machine and manually migrate the virtual machine to another datastore.	When either the host or the datastore becomes inaccessible, you must manually migrate the OVF templates to another host or datastore.
Associated with a Host	Yes.	No.
SDRS	Supported.	Not supported.
Cross-vendor Compatibility	Not supported.	Supported.
Software License Agreement	Not supported.	Supported.

Note You can convert a VM template into an OVF template. However, the snapshots and some extra configuration settings of the source virtual machine are lost. The virtual machine disks are consolidated and the virtual disks hierarchy is lost.

VM Template or OVF Template: Deployment Options

You can use both VM templates and OVF templates to deploy new virtual machines. However, there are differences between the two types of templates in regards to the available deployment options.

Table 4-3. Deployment Options with VM Templates and OVF Templates

Deployment Option	VM Templates in Content Library	OVF Templates in Content Library
Guest OS Customization	Supported. Encryption is also supported.	Supported, but except for encryption.
Hardware Customization	Supported.	Not supported.

VM Templates in Content Library vs. VM Templates in the vCenter Server Inventory

When you create a VM template library item, this item is backed by an identical VM template in the vCenter Server inventory. The content library item and the corresponding inventory object are related in the following way.

- If you convert the VM template in the vCenter Server inventory to a virtual machine, the corresponding VM template library item is also deleted.
- If you delete the VM template in the vCenter Server inventory, the corresponding VM template library item is also deleted.

- If you delete the VM template library item, the associated VM template in the vCenter Server inventory is also deleted.

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.

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 Select a subscribed library from the list.

3 Synchronize the item you need to use.

- On the **Templates** tab, right-click a VM or a vApp template, and select **Synchronize Item**.
- On the **Other Types** tab, right-click an item, and select **Synchronize Item**.

After synchronization completes, the item content and metadata are downloaded to the backing storage of the subscribed library, and 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.

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 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.

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.

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	In the vSphere Client, you can only delete the selected item. ■ 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	In the vSphere Web Client, you can delete the contents of an item or delete the item altogether. To delete the contents of an item, do the following. ■ 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**. To delete an item, do the following. ■ 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 guest operating system must support devices that you add or configurations that you make.

This chapter includes the following topics:

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

Objects in Environment	Compatibility	Results
Cluster with ESXi 6.0, ESXi 6.5, and ESXi 6.7 hosts	ESXi 6.5 and later	Gives you access to virtual hardware features that are not available with ESXi 6.0. ■ 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	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.

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	■ Change the default compatibility setting of a virtual machine. ■ Right-click a virtual machine and click **Compatibility > Upgrade VM Compatibility**. ■ Right-click a virtual machine and click **Compatibility > Schedule VM Compatibility Upgrade**.

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
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

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
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 Controller s	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
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

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
PCNet 32	Y	Y	Y	Y	Y	Y	Y	Y
VMXNet	Y	Y	Y	Y	Y	Y	Y	Y
VMXNet2	Y	Y	Y	Y	Y	Y	Y	Y
VMXNet3	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
PCI passthrough	16	16	16	6	6	6	6	0

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 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 Virtual Machine CPU Settings

After you create a VM, you can change its CPU settings. You can change the resource allocation, cores per socket, and CPUID Mask. You can also enable hardware virtualization and performance counters.

Prerequisites

Additional Prerequisites depend on the type of change that you want to make.

Table 5-3. Prerequisites for CPU Changes

Change	Prerequisite
CPU Hot Plug	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.
CPUID Mask	Turn off the virtual machine.

Table 5-3. Prerequisites for CPU Changes (Continued)

Change	Prerequisite
Hardware virtualization	■ Verify that the virtual machine compatibility is ESXi 5.1 and later. ■ Verify that Intel VT-x or AMD-V is enabled in the BIOS so that hardware assisted virtualization is possible.
Performance Counters	■ Verify that the virtual machine compatibility is ESXi 5.1 and later. ■ Verify that the virtual machine is turned off. ■ Verify that Intel VT-x or AMD-V is enabled in the BIOS so that hardware-assisted virtualization is possible.

Procedure

1 In the vSphere Client, right-click the VM and choose **Edit Settings**.

2 Select **Virtual Hardware** and open **CPU**.

3 (Optional) If you want to make changes to CPU while the virtual machine is running, select **Enable CPU Hot Add**.

4 Make changes to the following settings and click **OK**.

Option	Description
Cores per Socket	Number of cores per socket
CPU Hot Plug	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. ■ 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.
Reservation, Limit, Shares	A virtual machine has the following user-defined settings that affect its CPU resource allocation. ■ **Limit**:Upper limit for this VM's CPU allocation. Select **Unlimited** to specify no upper limit. ■ **Reservation**: Guaranteed CPU allocation for this VM ■ **Shares**:CPU shares for this VM 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 in a 1:2:4 ratio. Select **Custom** to give each VM a specific number of shares, which express a proportional weight. See the *vSphere Resource Management* documentation for details.

Option	Description
CPUID Mask	You cannot change the default in a VMware Cloud on AWS environment.
Hardware virtualization	Select **Expose hardware-assisted virtualization to guest OS** to 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.
Performance Counters	Select **Enable virtualized CPU performance counters** to 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. **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
CPU/MM Virtualization	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 host has ESXi 6.0 and later compatibility (hardware version 11). **Note** To take advantage of all features that virtual hardware version 13 provides, use the default hardware MMU setting.

Change the Virtual Machine Memory Settings

You can change the virtual machine memory configuration to improve virtual machine performance across your data center. You can set most of the memory parameters during virtual machine creation or after the guest operating system is installed. Most changes require that you power off the virtual machine first.

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 5-4. 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

- Power off the virtual machine.
- Verify that VMware Tools is installed.

Procedure

1. Right-click a virtual machine in the inventory and select **Edit Settings**.
2. Make changes to the following settings and click **OK**.

Option	Description
RAM	In the **RAM** text box, type the amount of RAM to assign to the virtual machine or select one of the suggested values from the drop-down menu.
Reservation, Limit, Shares	A virtual machine has the following user-defined settings that affect its memory resource allocation. ■ **Limit**: Upper limit for this VM's memory allocation. Select **Unlimited** to specify no upper limit. ■ **Reservation**: Guaranteed memory allocation for this VM ■ **Shares**: Memory shares for this VM 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 in a 1:2:4 ratio. Select **Custom** to give each VM a specific number of shares, which express a proportional weight. See the *vSphere Resource Management* documentation for details.

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 Vlance adapter when a virtual machine boots, but initializes itself and functions as either a Vlance or a VMXNET adapter, depending on which driver initializes it. With VMware Tools installed, the VMXNET driver changes the Vlance adapter to the higher performance VMXNET adapter.
Vlance	Emulated version of the AMD 79C970 PCnet32 LANCE NIC, an older 10 Mbps NIC with drivers available in 32-bit legacy guest operating systems. A virtual machine configured with this network adapter can use its network immediately.
VMXNET	Optimized for performance in a virtual machine and has no physical counterpart. Because operating system vendors do not provide built-in drivers for this card, you must install VMware Tools to have a driver for the VMXNET network adapter available.

VMXNET 2 (Enhanced)	Based on the VMXNET adapter but provides high-performance features commonly used on modern networks, such as jumbo frames and hardware offloads. VMXNET 2 (Enhanced) is available only for some guest operating systems on ESX/ESXi 3.5 and later.
VMXNET 3	A paravirtualized NIC designed for performance. VMXNET 3 offers all the features available in VMXNET 2 and adds several new features, such as multiqueue support (also known as Receive Side Scaling in Windows), IPv6 offloads, and MSI/MSI-X interrupt delivery. VMXNET 3 is not related to VMXNET or VMXNET 2.
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.

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.

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.

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 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.

5 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

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	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 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.

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**.

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.

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.

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 *vSphere Storage* 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 *vSphere Storage* documentation. You cannot change this setting in a VMware Cloud on AWS environment.
Sharing	Specifies sharing information. You cannot change this setting in a VMware Cloud on AWS environment.
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. In a VMware Cloud on AWS environment, disk mode is always dependent, which means that dependent disks are included in snapshots.
Virtual Device Node	Displays the virtual device node.

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 Storage Controllers.

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 Storage Controllers.

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.

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	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.

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	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.

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	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**.

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	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**.

SCSI Storage Controllers

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.

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.

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	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.

   If you are using VMware Cloud on AWS, you cannot further customize the SCSI controller.

3. 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.

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.

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.

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**.
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. a In the **Select File** dialog box, browse to the file containing the ISO image to connect to. b 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 a In the **Choose an ISO image to mount**, select the ISO image to connect to. b 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.

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.

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.

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 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.

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

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.

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.

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.

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).
- 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

- 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 Option Overview

You can view or change virtual machine settings from the vSphere Client. Not all options are available to every virtual machine. For many virtual machines, the default is the optimal setting.

The host that the virtual machine runs on and the guest operating system must support any configurations that you make.

When you select **Edit Settings** from a virtual machine right-button menu and click **VM Options**, you can select one of the following options.

Table 6-1. Virtual Machine Options

Options	Description
General Options	Include useful information: ■ Virtual machine name ■ Virtual machine configuration file location ■ Virtual machine working location ■ Operating system. This information is currently read only. To rename a VM, select **Edit Settings > Rename**. 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.
VMware Remote Console Options	Locking behavior and settings for simultaneous connections.
Power Management	Virtual machine Suspend behavior and wake on LAN.
VMware Tools	Power Controls behavior, VMware Tools scripts, automatic upgrades, and time synchronization between the guest and host.
Boot Options	Virtual machine boot options. Add a delay before booting, force entry into the BIOS or EFI setup screen, or set reboot options.
Advanced	Advanced virtual machine options, including the following: ■ Acceleration and logging settings. ■ Debugging and statistics ■ Swap file location ■ Configuration parameters ■ Latency sensitivity
Fibre Channel NPIV	Virtual node and port World Wide Names (WWNs).

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.

Power Management options are not available on every guest operating system.

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	In the Standby response section, select the standby response of the virtual machine. ■ 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	a In the Standby response section, select the standby response of the virtual machine. ■ 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. b (Optional) Select **Wake on LAN for virtual machine traffic on** and select the virtual NICs to trigger this action. Unsupported NICs might be listed, but are unavailable to connect.

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.

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.

Change VM Boot Options

For each VM, you can change the boot options. You can delay the boot, force entry into the BIOS or EFI screen, or set up the VM to retry after a boot failure.

Procedure

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

2 Click **VM Options** expand **Boot Options**, and make your selection:

Option	Description
Boot Delay	Select the time in milliseconds to delay the boot operation.
Force BIOS setup	Select whether to force entry into the BIOS or EFI setup screen the next time the virtual machine boots.
Failed Boot Recovery	Select to have the VM try a reboot after boot failure. You can set a reboot time.

3 Click **OK**.

Set Advanced Virtual Machine Options

Advanced options supporting changes to logging, hardware acceleration, and swap file location. Change the default settings only if you are sure that makes sense.

Prerequisites

Power off your VM before you change advanced options.

Procedure

1 In the vSphere Client, right-click the VM and choose **Edit Settings**.

2 Select **VM Options**, make changes, and click **OK**.

Option	Description
Disable 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**.
Enable logging	VMware stores 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. Logging is enabled by default.

Option	Description
Debugging and Statistics	Select a non-default option to have the VM collect additional debugging information. You usually change this option when requested by VMware Technical Support in resolving issues.
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. In VMware Cloud on AWS it usually does not make sense to change this option.
Latency sensitivity	Change to **High** for special cases.

Customizing Virtual Machines 7

You can customize your virtual machines to have a different startup behavior, create snapshots, and remove and reregister virtual machines. You can also create and apply a Virtual Machine Customization Spec.

This chapter includes the following topics:

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.

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	a Right-click the virtual machine and select **Edit Settings**. The virtual machine Edit Settings dialog box opens. If the **Virtual Hardware** tab is not preselected, select it. b Select **Datastore ISO File** from the CD/DVD drop-down menu, and browse for the ISO image for your guest operating system.
ISO image from a Content Library	a Right-click the virtual machine and select **Edit Settings**. The virtual machine Edit Settings dialog box opens. If the **Virtual Hardware** tab is not preselected, select it. b Select **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 GUID-EE77B0A9-F8FF-4785-BEAD-B6F04EE04492#GUID-EE77B0A9-F8FF-4785-BEAD-B6F04EE04492 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.

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	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.

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

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 it 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

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	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-imc`. To view the error log file, click the Windows **Start** button and select **Programs > Administrative Tools > Event Viewer**.

Customize Linux During Cloning or Deployment in the vSphere Web Client

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

Prerequisites

Ensure that all requirements for customization are met. See Guest Operating System Customization Requirements.

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	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.

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 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.

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	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	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.

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

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	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	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	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	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 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.

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 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.

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. ■ **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.

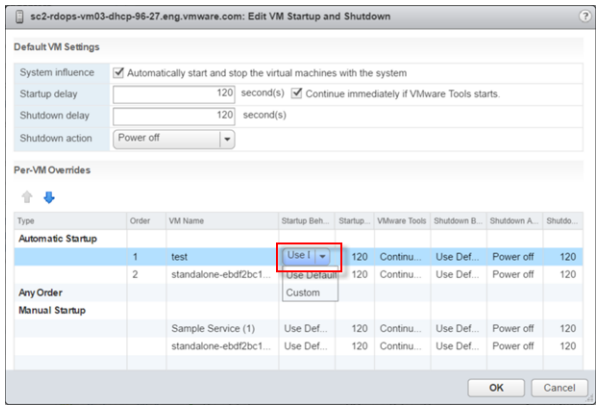
a To change the startup order of virtual machines, select a virtual machine from the Manual Startup category and use the up arrow to move it up to the Automatic Startup or Any Order categories.

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 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. ■ **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 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 resource pool in which to run the virtual machine and click **Next**.

5 Review your selections and click **Finish**.

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**.

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
vmname–number`.vmdk` and *vmname–number*`–delta.vmdk`	Snapshot file that represents the difference between the current state of the virtual disk and the state that existed at the time the previous snapshot was taken. The filename uses the following syntax, `S1vm–000001.vmdk` where `S1vm` is the name of the virtual machine and the six-digit number, `000001`, is based on the files that already exist in the directory. The number does not consider the number of disks that are attached to the virtual machine.
vmname`.vmsd`	Database of the virtual machine's snapshot information and the primary source of information for the Snapshot Manager.
vmname`.Snapshot`*number*`.vmsn`	Memory state of the virtual machine at the time you take the snapshot. The filename uses the following syntax, `S1vm.snapshot1.vmsn`, where `S1vm` is the virtual machine name, and `snapshot1` is the first snapshot. **Note** A `.vmsn` file is created each time you take a snapshot, regardless of the memory selection. A `.vmsn` file without memory is much smaller than one with memory.

Snapshot Limitations

Snapshots can affect virtual machine performance and do not support some disk types or virtual machines configured with bus sharing. Snapshots are useful as short-term solutions for capturing point-in-time virtual machine states and are not appropriate for long-term virtual machine backups.

- VMware does not support snapshots of raw disks, RDM physical mode disks, or guest operating systems that use an iSCSI initiator in the guest.
- Virtual machines with independent disks must be powered off before you take a snapshot. Snapshots of powered-on or suspended virtual machines with independent disks are not supported.
- Snapshots are not supported with PCI vSphere Direct Path I/O devices.
- VMware does not support snapshots of virtual machines configured for bus sharing. If you require bus sharing, consider running backup software in your guest operating system as an alternative solution. If your virtual machine currently has snapshots that prevent you from configuring bus sharing, delete (consolidate) the snapshots.

- Snapshots provide a point-in-time image of the disk that backup solutions can use, but Snapshots are not meant to be a robust method of backup and recovery. If the files containing a virtual machine are lost, its snapshot files are also lost. Also, large numbers of snapshots are difficult to manage, consume large amounts of disk space, and are not protected in the case of hardware failure.
- Snapshots can negatively affect the performance of a virtual machine. Performance degradation is based on how long the snapshot or snapshot tree is in place, the depth of the tree, and how much the virtual machine and its guest operating system have changed from the time you took the snapshot. Also, you might see a delay in the amount of time it takes the virtual machine to power-on. Do not run production virtual machines from snapshots on a permanent basis.
- If a virtual machine has virtual hard disks larger than 2TBs, snapshot operations can take significantly longer to finish.

Managing Snapshots

You can review all snapshots for the active virtual machine and act on them by using the Snapshot Manager.

After you take a snapshot, you can use the **Revert to Latest Snapshot** command from the virtual machine's right-click menu to restore that snapshot at any time. If you have a series of snapshots, you can use the **Revert to** command in the **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 7-1. 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 7-2. 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.

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	a Right-click the virtual machine and select **Manage Snapshots**. b Navigate to a snapshot in the snapshot tree and click the **Revert To** button. c 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. **Note** Deleting a single snapshot preserves the current state of the virtual machine and does not affect any other snapshot. You can also use the **Delete** option to remove a corrupt snapshot and its files from an abandoned branch of the snapshot tree without merging them with the parent snapshot.
Delete All	Use the **Delete All** option to delete all snapshots from the Snapshot Manager. **Delete all** consolidates and writes 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.

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.

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.

Compatibility and Requirements

The Per-VM EVC feature has the following requirements.

Compatibility	Requirement
Host Compatibility	SDDC version 1.3 or later
vCenter Server Compatibility	SDDC version 1.3 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 collocate 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.

To migrate virtual machines with disks larger than 2 TB, the source and destination ESXi hosts must be version 6.0 and later.

Virtual Machine Conditions and Limitations for vMotion

To migrate virtual machines with vMotion, the virtual machine must meet certain network, disk, CPU, USB, and other device requirements.

The following virtual machine conditions and limitations apply when you use vMotion:

- 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.
- Using 1 GbE network adapters for the vMotion network might result in migration failure, if you migrate virtual machines with large vGPU profiles. Use 10 GbE network adapters for the vMotion network.
- If virtual CPU performance counters are enabled, you can migrate virtual machines only to hosts that have compatible CPU performance counters.
- You can migrate virtual machines that have 3D graphics enabled. If the 3D Renderer is set to Automatic, virtual machines use the graphics renderer that is present on the destination host. The renderer can be the host CPU or a GPU graphics card. To migrate virtual machines with the 3D Renderer set to Hardware, the destination host must have a GPU graphics card.
- You can migrate virtual machines with USB devices that are connected to a physical USB device on the host. You must enable the devices for vMotion.

- You cannot use migration with vMotion to migrate a virtual machine that uses a virtual device backed by a device that is not accessible on the destination host. For example, you cannot migrate a virtual machine with a CD drive backed by the physical CD drive on the source host. Disconnect these devices before you migrate the virtual machine.
- You cannot use migration with vMotion to migrate a virtual machine that uses a virtual device backed by a device on the client computer. Disconnect these devices before you migrate the virtual machine.
- You can migrate virtual machines that use Flash Read Cache if the destination host also provides Flash Read Cache. During the migration, you can select whether to migrate the virtual machine cache or drop it, for example, when the cache size is large.

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

-
- 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.	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.	a Click **Configure per disk**. **Note** You can use the **Configure per disk** option to dowgrade 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. **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

-
- 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.	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.	a Click **Advanced**. **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. **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 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.

- 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

-
-
- 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.

Option	Action
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.	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.	a Click **Configure per disk**. **Note** You can use the **Configure per disk** option to dowgrade 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. **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

-
- 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.	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.	a Click **Advanced**. **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. **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 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

- 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.	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.	a Click **Configure per disk**. **Note** You can use the **Configure per disk** option to dowgrade 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. **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

- 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.	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.	a Click **Advanced**. **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. **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.

Securing Virtual Machines

8

To secure your VMs, keep the guest operating systems patched and protect your environment just as you protect your physical machine. Consider disabling unnecessary functionality, minimize the use of the VM console, and follow other best practices.

Protect the guest operating system

To protect your guest operating system, make sure that it uses the most recent patches and, if appropriate, anti-spyware and anti-malware applications. See the documentation from your guest operating system vendor and, potentially, other information available in books or on the Internet for that operating system.

Disable unnecessary functionality

Check that unnecessary functionality is disabled to minimize potential points of attack. Many of the features that are used infrequently are disabled by default. Remove unnecessary hardware and disable certain features such as host-guest filesystem (HGFS) or copy and paste between the VM and a remote console.

See Disable Unnecessary Functions Inside Virtual Machines.

Use templates and scripted management

VM templates enable you to set up the operating system so that it meets your requirements, and to create other VMs with the same settings.

If you want to change VM settings after initial deployment, consider using scripts, for example, PowerCLI. This documentation explains how to perform tasks using the GUI. Consider using scripts instead of the GUI to keep your environment consistent. In large environments, you can group VMs into folders to optimize scripting.

For information on templates, see Use Templates to Deploy Virtual Machines and the *vSphere Virtual Machine Administration*. For information on PowerCLI, see the VMware PowerCLI documentation.

Minimize use of the virtual machine console	The virtual machine console provides the same function for a VM that a monitor on a physical server provides. Users with access to a virtual machine console have access to VM power management and to removable device connectivity controls. As a result, virtual machine console access might allow a malicious attack on a VM.
Consider UEFI secure boot	Starting with vSphere 6.5, you can configure your VM to use UEFI boot. If the operating system supports secure UEFI boot, you can select that option for your VMs for additional security. See Enable or Disable UEFI Secure Boot for a Virtual Machine.

This chapter includes the following topics:

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.

Virtual Machine Security Best Practices

Following virtual machine security best practices helps ensure the integrity of your vSphere deployment.

General Virtual Machine Protection

A virtual machine is, in most respects, the equivalent of a physical server. Employ the same security measures in virtual machines that you do for physical systems.

Follow these best practices to protect your virtual machine:

Patches and other protection	Keep all security measures up-to-date, including applying appropriate patches. It is especially important to keep track of updates for dormant virtual machines that are powered off, because it can be easy to overlook them. For example, ensure that anti-virus software, anti-spy ware, intrusion detection, and other protection are enabled for every virtual machine in your virtual infrastructure. You should also ensure that you have enough space for the virtual machine logs.
Anti-virus scans	Because each virtual machine hosts a standard operating system, you must protect it from viruses by installing anti-virus software. Depending on how you are using the virtual machine, you might also want to install a software firewall. Stagger the schedule for virus scans, particularly in deployments with a large number of virtual machines. Performance of systems in your environment degrades significantly if you scan all virtual machines simultaneously. Because software firewalls and antivirus software can be virtualization-intensive, you can balance the need for these two security measures against virtual machine performance, especially if you are confident that your virtual machines are in a fully trusted environment.

Use Templates to Deploy Virtual Machines

When you manually install guest operating systems and applications on a virtual machine, you introduce a risk of misconfiguration. By using a template to capture a hardened base operating system image with no applications installed, you can ensure that all virtual machines are created with a known baseline level of security.

You can use templates that can contain a hardened, patched, and properly configured operating system to create other, application-specific templates, or you can use the application template to deploy virtual machines.

Procedure

- Provide templates for virtual machine creation that contain hardened, patched, and properly configured operating system deployments.

  If possible, deploy applications in templates as well. Ensure that the applications do not depend on information specific to the virtual machine to be deployed.

What to do next

For more information about templates, see Chapter 2 Deploying Virtual Machines.

Minimize Use of the Virtual Machine Console

The virtual machine console provides the same function for a virtual machine that a monitor provides on a physical server. Users with access to the virtual machine console have access to virtual machine power management and removable device connectivity controls. Console access might therefore allow a malicious attack on a virtual machine.

Procedure

1. Use native remote management services, such as terminal services and SSH, to interact with virtual machines.

   Grant access to the virtual machine console only when necessary.

2. Limit the connections to the console.

   For example, in a highly secure environment, limit the connection to one. In some environments, you can increase the limit if several concurrent connections are necessary to accomplish normal tasks.

Prevent Virtual Machines from Taking Over Resources

When one virtual machine consumes so much of the host resources that other virtual machines on the host cannot perform their intended functions, a Denial of Service (DoS) might occur. To prevent a virtual machine from causing a DoS, use host resource management features such as setting Shares and using resource pools.

By default, all virtual machines on an ESXi host share resources equally. You can use Shares and resource pools to prevent a denial of service attack that causes one virtual machine to consume so much of the host's resources that other virtual machines on the same host cannot perform their intended functions.

Do not use Limits unless you fully understand the impact.

Procedure

1. Provision each virtual machine with just enough resources (CPU and memory) to function properly.
2. Use Shares to guarantee resources to critical virtual machines.
3. Group virtual machines with similar requirements into resource pools.
4. In each resource pool, leave Shares set to the default to ensure that each virtual machine in the pool receives approximately the same resource priority.

   With this setting, a single virtual machine cannot use more than other virtual machines in the resource pool.

What to do next

See the *vSphere Resource Management* documentation for information about shares and limits.

Disable Unnecessary Functions Inside Virtual Machines

Any service that is running in a virtual machine provides the potential for attack. By disabling system components that are not necessary to support the application or service that is running on the system, you reduce the potential.

Virtual machines do not usually require as many services or functions as physical servers. When you virtualize a system, evaluate whether a particular service or function is necessary.

Procedure

- Disable unused services in the operating system.

  For example, if the system runs a file server, turn off any Web services.
- Disconnect unused physical devices, such as CD/DVD drives, floppy drives, and USB adapters.
- Disable unused functionality, such as unused display features, or VMware Shared Folders, which enables sharing of host files to the virtual machine (Host Guest File System).
- Turn off screen savers.
- Do not run the X Window system on top of Linux, BSD, or Solaris guest operating systems unless it is necessary.