Section 7
Administrative and Operational Tasks

Objective 7.1
Identify how to create and manage VM snapshots

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.

Take a Snapshot of a Virtual Machine

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 revert 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 (a 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 In the vSphere Client, navigate to a virtual machine and click the Snapshots tab.

2 Click Take Snapshot.

The Take snapshot dialog box opens.

3 Enter a name for the snapshot.

4 (Optional) Enter a description for the snapshot.

5 (Optional) To capture the memory of the virtual machine, select the Snapshot the virtual machine's memory check box.

6 (Optional) To pause running processes on the guest operating system so that file system contents are in a known consistent state when you take a snapshot, select the Quiesce guest file system (requires VMware Tools) check box.

You can quiesce the virtual machine files only when the virtual machine is powered on and the Snapshot the virtual machine's memory check box is deselected.

7 Click Create.

Revert a Virtual Machine Snapshot

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 revert 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 revert any snapshot in the snapshot tree and make 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 revert those snapshots at any time.
- If the snapshot includes the memory state, the virtual machine will be in the same power state as when you created the snapshot.

Table 9-1. Virtual Machine Power State After Restoring a Snapshot

Virtual Machine State When Parent Snapshot Is Taken	Virtual Machine State After Restoration
Powered on (includes memory)	Reverts to the parent snapshot, and the virtual machine is powered on and running.
Powered on (does not include memory)	Reverts to the parent snapshot and the virtual machine is powered off.
Powered off (does not include memory)	Reverts to the parent snapshot and the virtual machine is powered off.

When you revert to a snapshot, disks that you added or changed after the snapshot was taken are reverted to the snapshot point. For example, when you take a snapshot of a virtual machine, add a disk, and revert the snapshot, the added disk is removed.

Independent disks are also removed when you revert to a snapshot that was taken before the disk was added. If the latest snapshot includes an independent disk, its contents do not change when you revert to that snapshot.

Prerequisites

Verify that you have the Virtual machine.Snapshot management.Revert to snapshot privilege on the virtual machine.

Procedure

- To revert a snapshot, navigate to a virtual machine in the vSphere Client inventory and click the Snapshots tab.
- Navigate to a snapshot in the snapshot tree, click Revert, and click the Revert button.

Delete a Snapshot

Deleting a snapshot permanently removes the snapshot from the snapshot tree. The snapshot files are consolidated and written to the parent snapshot disk and merge with the virtual machine base disk. You can 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. Then it 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 must be read and written to a disk. This process can reduce the virtual machine performance until the consolidation is complete. Consolidating snapshots removes redundant disks, which improves the virtual machine performance and saves storage space. The time 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. If the virtual machine is powered on, the required time is proportional to the amount of data the virtual machine is writing during consolidation.

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. This option 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 tree. The Delete all option consolidates and writes the changes that occur between snapshots and the previous delta disk states to the base parent disk. It then 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 Revert button to revert 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 revert 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 revert 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

- Familiarize yourself with the delete and delete all actions and how they affect virtual machine performance.
- Required Privilege: Virtual machine.Snapshot management.Remove Snapshot on the virtual machine.

Procedure

- To delete snapshots from a snapshot tree, navigate to a virtual machine in the vSphere Web Client inventory and click the Snapshots tab.

Option	Action
Delete a single snapshot	a Navigate to and select a snapshot in the snapshots tree. b Click Delete and click the Delete button. The snapshot data is consolidated to the parent snapshot and the selected snapshot is removed from the snapshot tree.
Delete all snapshots	a Click Delete All and click the Delete all button. All immediate snapshots before the You are here current state are consolidated to the base parent disk. All existing snapshots are removed from the snapshot tree and the virtual machine.

Consolidate Snapshots

The presence of redundant delta disks can adversely affect the virtual machine performance. You can combine such disks without violating a data dependency. After consolidation, redundant disks are removed, which improves the virtual machine performance and saves storage space.

Snapshot consolidation is useful when snapshot disks fail to compress after a Revert, 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.

Prerequisites

Required privilege: Virtual machine.Snapshot management.Remove Snapshot

Procedure

1 Navigate to a virtual machine in the vSphere Web Client inventory and click the Snapshots tab.

2 Perform the necessary snapshot operations.

If the virtual machine snapshot files must be consolidated, the Consolidation is required message appears.

3 Click the Consolidate button.

The Consolidate dialog box appears.

4 Click OK.

5 To verify that the consolidation is successful, check the Needs Consolidation column.

a Navigate to an inventory object that contains a list of virtual machines, for example a vCenter Server instance, a host, or a cluster.

b Click the VMs tab and click Virtual Machines.

c Click the arrow icon next to any column name.

d Select Show/Hide Columns > Needs Consolidation.

A `Yes` status indicates that the snapshot files for the virtual machine must be consolidated. A `Not Required` status indicates that the files are consolidated.

vSphere Virtual Machine Administration Update 1 - VMware vSphere 7.0, page 259

Managing Snapshots

You can view and manage all snapshots for an active virtual machine. You can review the snapshots information, revert to the latest snapshot, change the name and description, or delete a snapshot.

You can manage the snapshots when you select a virtual machine in the vSphere Client inventory and click the Snapshots tab.

The snapshot tree displays all snapshots of the virtual machine and the power state of the virtual machine when a snapshot was taken. The detailed information region contains the snapshot name and description, time of creation, and the disk space. You can also see whether you took a snapshot of the virtual machine memory and if you quiesced the guest file system.

The You are here pin represents the current and active state of the virtual machine and it is always visible.

vSphere Virtual Machine Administration Update 1 - VMware vSphere 7.0, page 259

Objective 7.2
Identify how to manage VM templates and clones.

Managing VM Templates

In vSphere 7.0, you can manage VM templates in an efficient and flexible manner. You can edit the contents of the VM templates by checking them out, making the necessary changes, and checking them in.

You can track history of changes over time by using the vertical timeline view. The vertical timeline view provides you with detailed information about the different VM template versions, the updates that privileged users have made, and when the last change was made. By using the vertical timeline, you can revert VM templates back to their previous state or delete the previous version of a VM template.

In addition, you can deploy a virtual machine from the latest version of the VM template without any disruptions while it is checked out for update. You can update the virtual machine and check it back in into the same VM template.

Templates in Content Libraries

Templates are primary 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.

A VM template can be managed by vCenter Server or by a content library.

In previous releases of vSphere, you can 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. Starting with vSphere 6.7 Update 1, local content libraries support both OVF templates and VM templates. You choose the type of template when you clone the virtual machine into the content library.

OVF Templates in Content Libraries

In a content library, an OVF template is either a template of a virtual machine, or a template of a vApp. When you clone a virtual machine into a template in a content library, you choose whether to create an OVF template or a VM template. However, if you clone a vApp into a template in a content library, the resulting content library item is always an OVF template. 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

You can choose to save and manage a virtual machine from the vCenter Server inventory as a content library item of either the OVF Template or the VM Template type. Each VM Template library item is backed by a corresponding VM template in the vCenter Server inventory.

VM Templates in the Content Library and VM Templates in the vCenter Server Inventory

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

- 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 rename the VM template in the vCenter Server, the corresponding VM template library item is also renamed.
- If you rename the VM template library item the associated VM template in the vCenter Server inventory is also renamed.
- 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.

VM Templates and OVF Templates in the Content Library

You can use both VM templates and OVF templates to deploy new virtual machines in your vSphere environment. However, the two types of templates have different properties and support different deployment options.

See the following table for a detailed list of the differences between VM templates and OVF templates in a content library.

Table 4-2. VM Templates and OVF Templates Properties

Property	VM Templates in Content Library	OVF Templates in Content Library
Datastore	VM templates can be stored on any datastore that you have privileges to. Note VM templates cannot be stored in a library that uses NFS or SMB storage.	OVF templates can only be stored on the datastore that is associated with the content library.
Footprint	The default one.	Compressed or Thin.
Host/Datastore Maintenance Mode	When the host becomes inaccessible, VM templates are automatically migrated to another host.	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.
Storage DRS	Supported.	Not supported.
Cross-vendor Compatibility	Not supported.	Supported.
Software License Agreement	Not supported.	Supported.
Encryption	Supported. You can create encrypted VM templates.	Not supported. While OVF templates cannot be encrypted themselves, you can still deploy an encrypted virtual machine from an OVF template.
Deployment Options	During the deployment of a VM template, hardware customization and guest OS customization are both supported.	During the deployment of an OVF template, only guest OS customization is supported. Hardware customization is not supported.

The supported operations on a content library template are different depending on the template type. You can edit the settings for both OVF and VM templates. However, you can update, export, and clone a template only if it is an OVF template.

Check Out a Virtual Machine from a Template

In the vSphere Client, you can edit the VM templates and monitor the changes that have been made by other privileged users. You can perform the checkout operation to update a virtual machine from the VM template. During this process, the VM template is not available for checkout from other users, but they can deploy a virtual machine from the VM template without any disruptions.

When you check out a VM template, you cannot convert the virtual machine to a template or migrate the virtual machine to a different vCenter Server inventory.

Prerequisites

Verify that you have the following privileges:

- Content library.Check out a template
- Resource.Assign virtual machine to resource pool

- Datastore.Allocate space
- Virtual machine.Inventory.Create from existing
- Virtual machine.Configuration.Set annotation
- If you want to power on the checked out virtual machine, verify that you have the Virtual machine.Interaction.Power On privilege.

Procedure

1 To check out a VM template

Option	Action
From a content library	a Navigate to Menu > Content Libraries. b To open a local library, click its name. c On the Templates tab, select a VM template and click the Check out VM from this template button.
From the vSphere Client inventory	a Navigate to Menu > VMs and Templates and click the VM template. b Click the Versioning tab and in the vertical timeline view, click Check out VM from this template.

The Check out VM from VM Template dialog box opens.

2 On the Name and location page, enter a virtual machine name, select the virtual machine location, and click Next.

3 On the Select compute resource page, select the compute resource for the checked out virtual machine and click Next.

4 On the Review page, review the configuration.

5 Choose whether to power on the virtual machine after checkout by selecting the Power on VM after checkout check box.

6 Click Finish.

Results

The checked out virtual machine appears in the selected location marked with a blue circle icon. You can perform the necessary configuration changes.

What to do next

After you complete the virtual machine updates, you can check in the virtual machine back to the template.

Check In a Virtual Machine to a Template

After you check out a virtual machine from a template and update the virtual machine, you must check the virtual machine back into the VM template. When you check in the virtual machine to a template, you create a new version of the VM template containing the updated state of the virtual machine.

When you check in the virtual machine to the VM template, you allow the deployment of the last changes that you make to the virtual machine.

Prerequisites

Verify that the virtual machine is powered off or suspended. You cannot check in a powered on virtual machine to a VM template.

Required privileges:

- Content library.Check in a template

Procedure

1 To check in a virtual machine to a template:

Option	Action
From a content library	a Navigate to Menu > Content Libraries. b To open a content library, click its name. c On the Templates tab, select a VM template and click Check in VM to template.
From the vSphere Client inventory	a Navigate to Menu > VMs and Templates and click the VM template. b Click the Versioning tab and in the vertical timeline view, click Check in VM to template.

The Check in VM dialog box opens.

2 To describe the change, enter a comment in Check in notes .

3 Click Check in.

Results

The updated version of the VM template appears in the vertical timeline. You can see the check-in comment, the name of the user who made the changes, and the date of the change.

Discard a Checked Out Virtual Machine

If you check out a VM template and make no updates to the virtual machine or perform an update that you do not want to keep, you can discard the checked out virtual machine. Each time you check in the virtual machine back to the template, you create a new version of the VM template. You can discard the checked out virtual machine to avoid creating new versions or to prevent other users from using a faulty version.

Prerequisites

Required privileges:

- Virtual machine.Inventory.Delete

Procedure

1 To discard a checked out virtual machine:

Option	Action
From a content library	a Navigate to Menu > Content Libraries. b To open a local library, click its name. c On the Templates tab, select a VM template. d From the vertical timeline, click the horizontal ellipsis icon () that appears in the checked out VM template box and select Discard Checked Out VM.
From the vSphere Client inventory	a Navigate to Menu > VMs and Templates and click the VM template. b Click the Versioning tab in the vertical timeline. c Click the horizontal ellipsis icon () that appears in the checked out VM template box, and select Discard Checked Out VM.

2 The Discard Checked Out VM dialog box opens.

3 To delete the checked out virtual machine and discard all changes, click Discard.

Results

You deleted the virtual machine from the inventory and discarded all changes.

Revert to a Previous Version of a Template

If the latest VM template contains changes that you no longer want to keep or you made a mistake during your last checkin, you can revert the VM template to the previous version.

Prerequisites

Required privileges:

- Content library.Check in a template

Procedure

1 To revert to a previous version of a template:

Option	Action
From a content library	a Navigate to Menu > Content Libraries. b To open a local library, click its name. c On the Templates tab, select a VM template.
From the vSphere Client inventory	a Navigate to Menu > VMs and Templates and click the VM template. b Click the Versioning tab.

2 From the vertical timeline, navigate to the previous state of the VM template, click the horizontal ellipsis icon (), and select Revert to This Version.

The Revert to Version dialog box opens.

3 Enter a reason for the revert operation and click Revert.

Results

The VM template that you revert to becomes the current VM template.

Delete a Previous Version of a VM Template

Delete a previous version of a VM template if you no longer want to allow the use of the template. Deleting a VM template removes the template and its content from the inventory.

Prerequisites

Required privileges:

- Content Library.Delete library item

Procedure

1 To delete a previous version of a template:

Option	Action
From a content library	a Navigate to Menu > Content Libraries. b To open a local library, click its name.

	c	On the Templates tab, select a VM template.
From the vSphere Client inventory	a	Navigate to Menu > VMs and Templates and click the VM template.
	b	Click the Versioning tab.

2 From the vertical timeline, navigate to the previous state of the VM template, click the horizontal ellipsis icon (), and select Delete Version.

The Confirm Delete dialog box opens.

3 To delete permanently the VM template and its contents, click Yes.

vSphere Virtual Machine Administration Update 1 - VMware vSphere 7.0, page 78

Objective 7.3
Identify the considerations when provisioning a VM.

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.

vSphere Virtual Machine Administration Update 1 - VMware vSphere 7.0, page 10

Objective 7.4
Identify the options that can be performed on different inventory objects.

vSphere Managed Inventory Objects

In vSphere, the inventory is a collection of virtual and physical objects on which you can place permissions, monitor tasks and events, and set alarms. You can group most inventory objects by using folders to more easily manage them.

All inventory objects, with the exception of hosts, can be renamed to represent their purposes. For example, they can be named after company departments or locations or functions.

Note Managed object names cannot exceed 214 bytes (UTF-8 encoded).
vCenter Server monitors and manages the following inventory objects:

vCenter Server monitors and manages the following inventory objects:

Data Centers

Unlike folders, which are used to organize specific object types, a data center is an aggregation of all the different types of objects used to work in virtual infrastructure.

Within each data center, there are four separate hierarchies.

- Virtual machines (and templates)

- Hosts (and clusters)
- Networks
- Datastores

Clusters

A collection of ESXi hosts and associated virtual machines intended to work together as a unit. When you add a host to a cluster, the host's resources become part of the cluster's resources. vCenter Server manages the resources of all hosts in a cluster as one unit.

Datastores

A virtual representation of physical storage resources in the data center. A datastore is the storage location for virtual machine files. In an on-premises SDDC, these physical storage resources can come from the local SCSI disk of the ESXi host, the Fibre Channel SAN disk arrays, the iSCSI SAN disk arrays, or Network Attached Storage (NAS) arrays. For both on-premises and cloud SDDCs, vSAN datastores hide the idiosyncrasies of the underlying physical storage and present a uniform model for the storage resources required by virtual machines.

Folders

Folders allow you to group objects of the same type so you can easily manage them. For example, you can use folders to set permissions across objects, to set alarms across objects, and to organize objects in a meaningful way.

A folder can contain other folders, or a group of objects of the same type: data centers, clusters, datastores, networks, virtual machines, templates, or hosts. For example, one folder can contain hosts and a folder containing hosts, but it cannot contain hosts and a folder containing virtual machines.

Hosts

The physical computer on which ESXi is installed. All virtual machines run on hosts or clusters.

Networks

A set of virtual network interface cards (virtual NICs), distributed switches or vSphere Distributed Switches, and port groups or distributed port groups that connect virtual machines to each other or to the physical network outside of the virtual data center. You can monitor networks and set permissions and alarms on port groups and distributed port groups.

Resource pools

Resource pools are used to compartmentalize the CPU and memory resources of a host or cluster. Virtual machines run in, and draw their resources from, resource pools. You can create multiple resource pools as direct children of a standalone host or cluster and then delegate control over each resource pool to other individuals or organizations.

You can monitor resources and set alarms on them.

Templates

A template is a primary copy of a virtual machine that can be used to create and provision new virtual machines. Templates can have a guest operating system and application software installed. They can be customized during deployment to ensure that the new virtual machine has a unique name and network settings.

Virtual machines

A virtualized computer environment in which a guest operating system and associated application software can run. Multiple virtual machines can operate on the same managed host machine concurrently.

vApps

vSphere vApp is a format for packaging and managing applications. A vApp can contain multiple virtual machines.

vCenter Server and Host Management Update 1 - VMware vSphere 7.0, page 19

Tasks for Organizing Your Inventory

Populating and organizing your inventory involves the following activities:

- Creating data centers.
- Adding hosts to the data centers.
- Organizing inventory objects in folders.
- Setting up networking by using vSphere Standard Switches or vSphere Distributed Switches. To use services such as vMotion, TCP/IP storage, VMware vSAN™, and Fault Tolerance, set up VMkernel networking for these services. For more information, see *vSphere Networking*.
- Configuring storage systems and creating datastore inventory objects to provide logical containers for storage devices in your inventory. See *vSphere Storage*.
- Creating clusters to consolidate the resources of multiple hosts and virtual machines. You can enable vSphere HA and vSphere DRS for increased availability and more flexible resource management. See *vSphere Availability* for information about configuring vSphere HA, and *vSphere Resource Management* for information about configuring vSphere DRS.
- Creating resource pools to provide logical abstraction and flexible management of the resources in vSphere. Resource pools can be grouped into hierarchies and used to hierarchically partition available CPU and memory resources. See *vSphere Resource Management* for details.

This chapter includes the following topics:

- Create a Data Center
- Create a Folder
- Add a Host to a Folder or a Data Center
- Creating and Configuring Clusters
- Extend a Cluster

Create a Data Center

A virtual data center is a container for all the inventory objects required to complete a fully functional environment for operating virtual machines. You can create multiple data centers to organize groups of environments to meet different user needs. For example, you can create a data center for each organizational unit in your enterprise or create some data centers for high-performance environments and other data centers for less demanding environments.

Prerequisites

Required privileges:

- Datacenter.Create datacenter

Procedure

1 In the vSphere Client home page, navigate to Home > Hosts and Clusters.

2 Right-click the vCenter Server object and select New Datacenter.

3 (Optional) Enter a name for the data center and click OK.

What to do next

Add hosts, clusters, resource pools, vApps, networking, datastores, and virtual machines to the data center.

Create a Folder

You can use folders to group objects of the same type for easier management. For example, you can apply a common set of permissions to the folder and these permissions apply to all objects grouped in the folder.

A folder can contain other folders, or a group of objects of the same type. For example, one folder can contain both virtual machines and another folder that contains virtual machines, but it cannot contain both hosts and a folder that contains virtual machines.

Procedure

1 In the vSphere Client, select either a data center or another folder as a parent object for the folder that you want to create.

2 Right-click the parent object and click New Folder.

   - If the parent object is a folder, the new folder is of the same type as the parent folder - it can contain only objects of the same type that the parent folder contains.

   - If the parent object is a data center, you can create one of four types of folders: Host and Cluster folders, Network folders, Storage folders, and VM and Template folders.

3 Enter a name for the folder and click OK.

What to do next

Move objects into the folder by right-clicking the object and selecting Move To. Select the folder as the destination. You can also move an object by dragging it to the destination folder.

Add a Host to a Folder or a Data Center

You can add hosts under a data center object, a folder object, or a cluster object. If a host contains virtual machines, those virtual machines are added under the host in the inventory.

Prerequisites

- Verify that a data center or a folder exists in the inventory.

- Obtain the user name and password of the root user account for the host.

- Verify that hosts behind a firewall are able to communicate with the vCenter Server system and all other hosts through port 902 or another custom-configured port.

- Verify that all NFS mounts on the host are active.

- Verify that you have the proper privileges. Different sets of privileges apply when you add multiple hosts to a cluster and a single host to a cluster or a data center. For more information, see Required Privileges for Common Tasks in the *vSphere Security* documentation.
- If you want to add a host with more than 512 LUNs and 2,048 paths to the vCenter Server inventory, verify that the vCenter Server instance is suitable for a large or an x-large environment.

Procedure

1 In the vSphere Client, navigate to a data center or folder within a data center.
2 Right-click the data center or folder and select Add Host.
3 Enter the IP address or the name of the host and click Next.
4 Enter administrator credentials and click Next.
5 Review the host summary and click Next.
6 License the host through one of the following methods.
   - Assign an already existing license.
   - Assign a new license.
     a Click Create New Licenses. The Add Host wizard minimizes in Work in Progress and the New Licenses wizard appears.
     b Enter or copy and paste the new license key from My VMware and click Next.
     c Enter a new name for the license and click Next.
     d Review the new license and click Finish.
7 In the Add Host wizard, click Next.
8 (Optional) Select a lockdown mode option to disable the remote access for the administrator account after vCenter Server takes control of this host and click Next.
9 (Optional) If you add the host to a data center or a folder, select a location for the virtual machines that reside on the host and click Next.
10 Review the summary and click Finish.

Results

A new task for adding the host appears in the Recent Tasks pane. It might take a few minutes for the task to complete.

Creating and Configuring Clusters

A cluster is a group of hosts. When a host is added to a cluster, the resources of the host become part of the resources of the cluster. The cluster manages the resources of all hosts that it contains.

Starting with vSphere 6.7, you can create and configure a cluster that is hyper-converged. The hyper-converged infrastructure collapses compute, storage, and networking on a single software layer that runs on industry standard x86 servers.

You can create and configure a cluster by using the simplified Quickstart workflow in the vSphere Client. On the Cluster quickstart page, there are three cards for configuring your new cluster.

Table 6-1. The cards initiating wizards for renaming and configuring a new cluster

Cluster Quickstart Workflow	Description
1. Cluster basics	You can edit the cluster name and enable or disable cluster services. The card lists the services you enabled.
2. Add hosts	You can add new ESXi hosts. After the hosts are added, the card shows the total number of the hosts present in the cluster and health check validation for those hosts.
3.Configure cluster	You can configure network settings for vMotion traffic, review and customize cluster services. After the cluster is configured, the card provides details on configuration mismatch and reports cluster health results through the vSAN Health service.

The Skip Quickstart button prompts you to continue configuring the cluster and its hosts manually. To confirm exiting the simplified configuration workflow, click Continue. After you dismiss the Cluster quickstart workflow, you cannot restore it for the current cluster.

You must create clusters if you plan to enable vSphere High Availability (HA), vSphere Distributed Resource Scheduler (DRS), and the VMware vSAN features.

Starting with vSphere 7.0, you can create a cluster that you manage with a single image. By using vSphere Lifecycle Manager images, you can easily update and upgrade the software and firmware on the hosts in the cluster. For more information about using images to manage ESXi hosts and clusters, see the *Managing Host and Cluster Lifecycle* documentation.

Starting with vSphere 7.0 Update 1, vSphere Cluster Services (vCLS) is enabled by default and runs in all vSphere clusters. vCLS ensures that if vCenter Server becomes unavailable, cluster services remain available to maintain the resources and health of the workloads that run in the clusters. For more information about vCLS, see vSphere Cluster Services (vCLS).

Create a Cluster

You create a new and empty cluster object by using the Quickstart workflow in the vSphere Client.

Starting with vSphere 7.0, the clusters that you create can use vSphere Lifecycle Manager images for host updates and upgrades.

A vSphere Lifecycle Manager image is a combination of vSphere software, driver software, and desired firmware with regard to the underlying host hardware. The image that a cluster uses defines the full software set that you want to run on the ESXi hosts in the cluster: the ESXi version, additional VMware-provided software, and vendor software, such as firmware and drivers.

The image that you define during cluster creation is not immediately applied to the hosts. If you do not set up an image for the cluster, the cluster uses baselines and baseline groups. For more information about using images and baselines to manage hosts in clusters, see the *Managing Host and Cluster Lifecycle* documentation.

Prerequisites

- Verify that a data center, or a folder within a data center, exists in the inventory.
- Verify that hosts have the same ESXi version and patch level.
- Obtain the user name and password of the root user account for the host.
- Verify that hosts do not have a manual vSAN configuration or a manual networking configuration.
- To create a cluster that you manage with a single image, review the requirements and limitations information in the *Managing Host and Cluster Lifecycle* documentation and verify that you have an ESXi image available in the vSphere Lifecycle Manager depot.

Required privileges:

- Host.Inventory.Create cluster

Procedure

1 In the vSphere Client home page, navigate to Home > Hosts and Clusters.

2 Select a data center.

3 Right-click the data center and select New Cluster.

4 Enter a name for the cluster.

5 Select DRS, vSphere HA, or vSAN cluster features.

Option	Description
To use DRS with this cluster	a Slide the switch to the right to enable the DRS service. b (Optional) Click the info icon on the left to see the Default Settings for the DRS service. The default values are: • Automation Level: Fully Automated Migration • Threshold: 3
To use vSphere HA with this cluster	a Slide the switch to the right to enable the vSphere HA service. b (Optional) Click the info icon on the left to see the Default Settings for the vSphere HA service. You are present with the following default values: Host Monitoring: Enabled Admission Control: Enabled VM Monitoring: Disabled
To use vSAN with this cluster	• Slide the switch to the right to enable the vSAN service. For more information on vSAN, see Creating a vSAN Cluster in the vSAN Planning and Deployment documentation.

You can override the default values later on in the workflow.

6 (Optional) To create a cluster that you manage by a single image, select the Manage all hosts in the cluster with a single image check box.

Verify you have an ESXi Version 7.0 or later in the vSphere Lifecycle Manager repository.

a Select an ESXi Version from the drop-down menu.

b (Optional) Select a Vendor Addon and a Vendor Addon version from the drop-down menu.

You can edit the image specification later from the Updates tab.

If you do not set up an image for the cluster, you must manage the cluster by using baselines and baseline groups. You can switch from using baselines to using images at a later time.

7 Click OK.

The cluster appears in the vCenter Server inventory. The Quickstart service appears under the Configure tab.

8 (Optional) To rename your cluster and to enable or disable cluster services, click Edit in the Cluster basics card.

Results

You have created an empty cluster in the vCenter Server inventory.

What to do next

Add hosts to the cluster.

Add a Host to a Cluster

You can add new and existing ESXi hosts to the vCenter Server inventory.

You can also add hosts to a DRS cluster. For more information, see *vSphere Resource Management*.

When you add the first three hosts to the cluster, vSphere Cluster Services (vCLS) agent virtual machines are added by default to the cluster. A quorum of up to three vCLS agent virual machines are required to run in a cluster, one agent virtual machine per host. For more information about vCLS, see vSphere Cluster Services (vCLS).

Prerequisites

- Verify that hosts have the same ESXi version and patch level.
- Obtain the user name and password of the root user account for the host.
- Verify that hosts do not have a manual vSAN configuration or a manual networking configuration.
- Verify that you have the proper privileges. Different sets of privileges apply when you add multiple hosts to a cluster and a single host to a cluster or a data center. For more information, see Required Privileges for Common Tasks in the *vSphere Security* documentation.
- To add a host to a cluster that you manage with a single image, review the requirements andlimitations information in the *Managing Host and Cluster Lifecycle* documentation.

Procedure

1 In the vSphere Client, navigate to a cluster within a data center.

2 On the Configure tab, select Configuration > Quickstart.

3 Click Add in the Add hosts card.

4 On the Add hosts page, under the New hosts tab, add hosts that are not part of the vCenter Server inventory by populating the IP Address and credentials text boxes for those hosts.

5 (Optional) Select the `Use the same credentials for all hosts` option to reuse the credentials for all added hosts.

6 On the Add hosts page, click the Existing hosts tab, and add hosts that are managed by the vCenter Server and are in the same data center as your cluster.

7 Click Next.

The Host summary page lists all hosts that will be added to the cluster and related warnings.

Note If a host cannot be validated automatically by the system, you are prompted to manually validate its certificate and accept its thumbprint in the Security Alert pop-up.

8 On the Host summary page, review the details of the added hosts and click Next.

9 On the Ready to complete page, review the IP addresses or FQDN of the added hosts and click Finish.

Review the number of added hosts and the health check validation, performed by the vSAN Health service, in the Add hosts card.

10 (Optional) Click Re-validate to retrigger the validation of the hosts.

Note If an error occurs, it is visible in the Recent Tasks tab only.

Results

All hosts are placed in maintenance mode and added to your cluster. You can manually exit the maintenance mode.

What to do next

Configure your cluster default settings through the Quickstart workflow.

Configure a Cluster

To configure the host networking settings on your host and to customize the cluster settings, start the Configure cluster wizard, part of the Cluster quickstart workflow.

Procedure

1 In the vSphere Client, navigate to a cluster.

2 On the Configure tab, select Configuration > Quickstart.

The Cluster quickstart page appears.

Note To configure your cluster host networking and services manually by referring to different parts of the vSphere software, click the Skip quickstart button. If you dismiss the Cluster quickstart workflow, you cannot restore it, and you have to configure manually any hosts that you add to this cluster in the future.

3 In the Configure hosts card, select Configure.

4 On the Distributed switches page, configure the cluster networking.

Alternatively, you can select the `Configure networking settings later` check box to configure the default settings only for the cluster services and to hide all options that are related to host networking.

Caution After you select the `Configure networking settings later` check box, and complete the Configure cluster workflow, you cannot perform the networking configuration in the future by using the Configure cluster wizard.

a Specify the number of distributed switches to create from the drop-down menu.

Note You can select up to three distributed switches.

The selected distributed switches are configured as part of this workflow and all hosts in the cluster connect to them.

b Enter a unique name for each of the distributed switches you are about to create.

c (Optional) Click Use Existing to select an existing compatible distributed switch and an existing compatible distributed port group.

d To set up the vMotion network, select a distributed switch from the drop-down menu and assign a new default port group to it.

e In the Physical adapters section, for each physical network adapter (NIC), select the distributed switch name from the drop-down menu.

The new distributed switch must be assigned to at least one physical adapter.

Note If you are using an existing distributed switch, the physical adapter selection must match the current mapping of the distributed switch. Any variation results in an error.

This mapping of physical NICs to the distributed switches is applied to all hosts in this cluster.

f Click Next.

If you enabled the vSphere DRS feature during cluster creation, the vMotion traffic page appears.

g (Optional) Select the Use VLAN check box and enter an ID for the vMotion distributed port group.

h (Optional) Select a protocol type from the drop-down menu.

i (Optional) Populate the text boxes for each host in the cluster depending on the IP address type you need for setting up the networking.

If the IP address type is set to DHCP, these text boxes are dimmed.

5 Click Next.

The Advanced options page appears.

6 (Optional) If you have enabled the vSphere HA feature during cluster creation, use the options in the High Availability section to enable or disable host failure monitoring, virtual machine monitoring, and admission control.

If you enable admission control, you can specify the failover capacity by number of hosts.

7 (Optional) If you enabled the vSphere DRS feature during cluster creation, the Distributed Resource Scheduler section is visible.

a Set the Automation level to `Fully Automated`, `Partially Automated` or `Manual`.

b Select one of the five migration settings from the Migration threshold drop-down menu.

8 In the Host Options section, set the Lockdown mode to `Strict`, `Normal` or `Disabled`, and enter an NTP server address.

The settings are applied across all hosts in this cluster.

9 (Optional) In the Enhanced vMotion Capability section, enable EVC and select the CPU model from the EVC mode drop-down menu.

10 Click Next.

The Ready to complete page appears.

11 Review the settings and select Finish.

The card closes, and the progress of the operation appears in the Recent Tasks tab.

Results

You have created a fully configured cluster in the vCenter Server inventory.

What to do next

Expand your cluster by using the Add hosts card.

Extend a Cluster

You extend a configured cluster by adding hosts to it with the Cluster quickstart workflow in the vSphere Client.

After you configure your cluster, you can scale it out by adding more hosts. Then, you specify the network configuration for the new hosts in the cluster. During the initial configuration of the cluster, if you postponed configuring the host networking, no configuration, as for the existing hosts, is applied to the newly added hosts.

Extend a Cluster Without Host Networking Configuration

You extend a cluster by adding hosts to that cluster. If you previously configured the cluster without setting up the host networking, the configuration of the existing hosts in the cluster is applied to the new hosts.

Prerequisites

- Verify that you have an existing cluster and hosts added to it.
- During the initial cluster configuration, select the `Configure networking settings later` check box. For more information, see Configure a Cluster.
- Verify that hosts have the same ESXi version and patch level.
- Obtain the user name and password of the root user account for the host.
- To add a host to a cluster that you manage with a single image, review the requirements and limitations information in the *Managing Host and Cluster Lifecycle* documentation.

Procedure

1 In the vSphere Client home page, navigate to Home > Hosts and Clusters and select a configured cluster.

2 Right-click the cluster and select Add Hosts.

  The Add hosts wizard appears.

3 From the Add hosts wizard, add new and existing hosts from the vCenter Server inventory and review the Host summary.

4 On the Ready to complete page, click Finish.

  The Extend Cluster Guide page appears.

5 In the Configure hosts card, select Configure.

  A pop-up window appears. It informs you that the configuration for the hosts that exist in the cluster is applied to the newly added hosts.

6 Select Continue.

Results

After successful validation, your newly added hosts are configured as the existing hosts in your cluster, and the Configure button in the Configure hosts card becomes inactive. You can only click Re-validate to verify the cluster configuration.

What to do next

Configure the host networking manually and add more hosts to the cluster.

Extend a Cluster with Host Networking Configuration

You extend a hyper-converged cluster by adding hosts and configuring their networking to match the cluster configuration.

Prerequisites

- Verify that you have an existing cluster and hosts added to it.
- In the initial cluster configuration, you configured the host networking.
- Verify that hosts have the same ESXi version and patch level.
- Obtain the user name and password of the root user account for the host.
- Verify that hosts do not have a manual vSAN configuration or a manual networking configuration.
- To add a host to a cluster that you manage with a single image, review the requirements and limitations information in the *Managing Host and Cluster Lifecycle* documentation.

Procedure

1 In the vSphere Client home page, navigate to Home > Hosts and Clusters and select a configured cluster.

2 Right-click the cluster and select Add Hosts.

The Add hosts wizard appears.

3 From the Add hosts wizard, add new and existing hosts from the vCenter Server inventory, review the Host summary and click Finish on the Ready to complete page.

The Extend Cluster Guide page appears.

4 From the Add hosts wizard, add new and existing hosts from the vCenter Server inventory and review the Host summary.

5 On the Ready to complete page, click Finish.

The Extend Cluster Guide page appears.

6 In the Configure hosts card, select Configure.

7 (Optional) If the vSphere DRS feature is enabled on the cluster, configure the networking options in the vMotion traffic page.

a (Optional) Select a protocol type from the drop-down menu.

b (Optional) Populate the text boxes for each host in the cluster depending on the IP address type you need for setting up the networking.

If the IP address type is set to DHCP, these text boxes are dimmed.

8 Click Next.

The Ready to complete page appears.

9 Review the settings and select Finish.

The card closes, and the progress of the operation appears in the Recent Tasks tab.

Results

After successful validation, your newly added hosts are configured as the existing hosts in your cluster and the Configure button in the Configure hosts card becomes inactive. You can only click Re-validate to verify the cluster configuration.

What to do next

Add more hosts to the cluster.

vCenter Server and Host Management Update 1 - VMware vSphere 7.0, page 39

Objective 7.6
Identify the concepts of role-based user management

Using Roles to Assign Privileges

A role is a predefined set of privileges. Privileges define rights to perform actions and read properties. For example, the Virtual Machine Administrator role allows a user to read and change virtual machine attributes.

When you assign permissions, you pair a user or group with a role and associate that pairing with an inventory object. A single user or group can have different roles for different objects in the inventory.

For example, assume that you have two resource pools in your inventory, Pool A and Pool B. You can assign group Sales the Virtual Machine User role on Pool A, and the Read Only role on Pool B. With these assignments, the users in group Sales can turn on virtual machines in Pool A, but can only view virtual machines in Pool B.

vCenter Server provides system roles and sample roles by default.

System roles

System roles are permanent. You cannot edit the privileges associated with these roles.

Sample roles

VMware provides sample roles for certain frequently performed combination of tasks. You can clone, modify, or remove these roles.

Note To avoid losing the predefined settings in a sample role, clone the role first and make modifications to the clone. You cannot reset the sample to its default settings.

Users can schedule tasks only if they have a role that includes privileges to perform that task at the time the task is created.

Note Changes to roles and privileges take effect immediately, even if the users involved are logged in. The exception is searches, where changes take effect after the user has logged out and logged back in.

Custom Roles in vCenter Server and ESXi

You can create custom roles for vCenter Server and all objects that it manages, or for individual hosts.

vCenter Server Custom Roles (Recommended)

Create custom roles by using the role-editing facilities in the vSphere Client to create privilege sets that match your needs.

ESXi Custom Roles

You can create custom roles for individual hosts by using a CLI or the VMware Host Client. See the *vSphere Single Host Management - VMware Host Client* documentation. Custom host roles are not accessible from vCenter Server.

If you manage ESXi hosts through vCenter Server, do not maintain custom roles in both the host and vCenter Server. Define roles at the vCenter Server level.

When you manage a host using vCenter Server, the permissions associated with that host are created through vCenter Server and stored on vCenter Server. If you connect directly to a host, only the roles that are created directly on the host are available.

Note When you add a custom role and do not assign any privileges to it, the role is created as a Read Only role with three system-defined privileges: System.Anonymous, System.View, and System.Read.

Create a Custom Role

You can create vCenter Server custom roles to suit the access control needs of your environment. You can create a role or clone an existing role.

You can create or edit a role on a vCenter Server system that is part of the same vCenter Single Sign-On domain as other vCenter Server systems. The VMware Directory Service (vmdir) propagates the role changes that you make to all other vCenter Server systems in the group. Assignments of roles to specific users and objects are not shared across vCenter Server systems.

Prerequisites

Verify that you are logged in as a user with Administrator privileges.

Procedure

1. Log in to the vCenter Server by using the vSphere Client.
2. Select Administration and click Roles in the Access Control area.
3. Create the role:

Option	Description
To create a role	Click the Create role action icon.
To create the role by cloning	Select a role, and click the Clone role action icon.

   See vCenter Server System Roles for more information.

4. Select and deselect privileges for the role.

   See Chapter 14 Defined Privileges for more information.

   Note When creating a cloned role, you cannot change privileges. To change privileges, select the cloned role after it is created and click the Edit role action icon.

5. Enter a name for the new role.
6. Click Finish.

What to do next

You can now create permissions by selecting an object and assigning the role to a user or group for that object.

vCenter Server System Roles

A role is a predefined set of privileges. When you add permissions to an object, you pair a user or group with a role. vCenter Server includes several system roles, which you cannot change.

vCenter Server provides a few default roles. You cannot change the privileges associated with the default roles. The default roles are organized as a hierarchy. Each role inherits the privileges of the previous role. For example, the Administrator role inherits the privileges of the Read Only role.

The vCenter Server role hierarchy also includes several sample roles. You can clone a sample role to create a similar role.

If you create a role, it does not inherit privileges from any of the system roles.

Administrator Role

Users with the Administrator role for an object are allowed to view and perform all actions on the object. This role also includes all privileges of the Read Only role. If you have the Administrator role on an object, you can assign privileges to individual users and groups.

If you are acting in the Administrator role in vCenter Server, you can assign privileges to users and groups in the default vCenter Single Sign-On identity source. See the *vSphere Authentication* documentation for supported identity services.

By default, the administrator@vsphere.local user has the Administrator role on both vCenter Single Sign-On and vCenter Server after installation. That user can then associate other users with the Administrator role on vCenter Server.

Read Only Role

Users with the Read Only role for an object are allowed to view the state of the object and details about the object. For example, users with this role can view virtual machine, host, and resource pool attributes, but cannot view the remote console for a host. All actions through the menus and toolbars are disallowed.

No Access Role

Users with the No Access role for an object cannot view or change the object in any way. New users and groups are assigned this role by default. You can change the role on an object-by-object basis.

The administrator of the vCenter Single Sign-On domain, administrator@vsphere.local by default, the root user, and vpxuser are assigned the Administrator role by default. Other users are assigned the No Access role by default.

No Cryptography Administrator Role

Users with the No cryptography administrator role for an object have the same privileges as users with the Administrator role, except for Cryptographic operations privileges. This role allows administrators to designate other administrators that cannot encrypt or decrypt virtual machines or access encrypted data, but that can perform all other administrative tasks.

Trusted Infrastructure Administrator Role

Users with the Trusted Infrastructure administrator role are allowed to perform VMware® vSphere Trust Authority™ operations on some objects. Membership in the TrustedAdmins group is required for full vSphere Trust Authority capabilities.

No Trusted Infrastructure Administrator Role

> Users with the No Trusted Infrastructure administrator role have the same privileges as users with the Administrator role, except for vSphere Trust Authority privileges. This role allows administrators to designate other administrators that cannot enable or manage vSphere Trust Authority features, but that can perform other administrative tasks.

Best practice is to create a user at the root level and assign the Administrator role to that user. After creating a named user with Administrator privileges, you can remove the root user from any permissions or change its role to No Access.

Best Practices for Roles and Permissions

Follow best practices for roles and permissions to maximize the security and manageability of your vCenter Server environment.

Follow these best practices when configuring roles and permissions in your vCenter Server environment:

- Where possible, assign a role to a group rather than individual users.
- Grant permissions only on the objects where they are needed, and assign privileges only to users or groups that must have them. Use the minimum number of permissions to make it easier to understand and manage your permissions structure.
- If you assign a restrictive role to a group, check that the group does not contain the Administrator user or other users with administrative privileges. Otherwise, you might unintentionally restrict administrators' privileges in the parts of the inventory hierarchy where you have assigned that group the restrictive role.
- Use folders to group objects. For example, to grant modify permission on one set of hosts and view permission on another set of hosts, place each set of hosts in a folder.
- Use caution when adding a permission to the root vCenter Server objects. Users with privileges at the root level have access to global data on vCenter Server, such as roles, custom attributes, vCenter Server settings.
- Consider enabling propagation when you assign permissions to an object. Propagation ensures that new objects in the object hierarchy inherit permissions. For example, you can assign a permission to a virtual machine folder and enable propagation to ensure that the permission applies to all VMs in the folder.
- Use the No Access role to mask specific areas of the hierarchy. The No Access role restricts access for the users or groups with that role.
- Changes to licenses propagate to all linked vCenter Server systems in the same vCenter Single Sign-On domain.
- License propagation happens even if the user does not have privileges on all vCenter Server systems.

Required Privileges for Common Tasks

Many tasks require permissions on multiple objects in the inventory. If the user who attempts to perform the task only has privileges on one object, the task cannot complete successfully.

The following table lists common tasks that require more than one privilege. You can add permissions to inventory objects by pairing a user with one of the predefined roles or with multiple privileges. If you expect that you assign a set of privileges multiple times, create custom roles.

If the task that you want to perform is not in this table, the following rules explain where you must assign permissions to allow particular operations:

- Any operation that consumes storage space requires the Datastore.Allocate Space privilege on the target datastore, and the privilege to perform the operation itself. You must have these privileges, for example, when creating a virtual disk or taking a snapshot.
- Moving an object in the inventory hierarchy requires appropriate privileges on the object itself, the source parent object (such as a folder or cluster), and the destination parent object.
- Each host and cluster has its own implicit resource pool that contains all the resources of that host or cluster. Deploying a virtual machine directly to a host or cluster requires the Resource.Assign Virtual Machine to Resource Pool privilege.

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

into a resource pool	• Resource.Assign virtual machine to resource pool • Virtual machine.Inventory.Move	
	On the destination resource pool: Resource.Assign virtual machine to resource pool	Administrator
Install a guest operating system on a virtual machine	On the virtual machine or folder of virtual machines: • Virtual machine.Interaction.Answer question • Virtual machine.Interaction.Console interaction • Virtual machine.Interaction.Device connection • Virtual machine.Interaction.Power Off • Virtual machine.Interaction.Power On • Virtual machine.Interaction.Reset • Virtual machine .Interaction.Configure CD media (if installing from a CD) • Virtual machine .Interaction.Configure floppy media (if installing from a floppy disk) • Virtual machine.Interaction.VMware Tools install	Virtual Machine Power User or Administrator
	On a datastore that contains the installation media ISO image: Datastore.Browse datastore (if installing from an ISO image on a datastore) On the datastore to which you upload the installation media ISO image: • Datastore.Browse datastore • Datastore.Low level file operations	Virtual Machine Power User or Administrator
Migrate a virtual machine with vMotion	On the virtual machine or folder of virtual machines: • Resource.Migrate powered on virtual machine • Resource.Assign Virtual Machine to Resource Pool (if destination is a different resource pool from the source)	Resource Pool Administrator or Administrator
	On the destination host, cluster, or resource pool (if different from the source): Resource.Assign virtual machine to resource pool	Resource Pool Administrator or Administrator
Cold migrate (relocate) a virtual machine	On the virtual machine or folder of virtual machines: • Resource.Migrate powered off virtual machine • Resource.Assign virtual machine to resource pool (if destination is a different resource pool from the source)	Resource Pool Administrator or Administrator
	On the destination host, cluster, or resource pool (if different from the source): Resource.Assign virtual machine to resource pool	Resource Pool Administrator or Administrator
	On the destination datastore (if different from the source): Datastore.Allocate space	Datastore Consumer or Administrator
Migrate a virtual machine with Storage vMotion	On the virtual machine or folder of virtual machines: Resource.Migrate powered on virtual machine	Resource Pool Administrator or Administrator
	On the destination datastore: Datastore.Allocate space	Datastore Consumer or Administrator
Move a host into a cluster	On the host:	Administrator

	Host.Inventory.Add host to cluster	
	On the destination cluster: • Host.Inventory.Add host to cluster • Host.Inventory.Modify cluster	Administrator
Add a single host to a data center by using the vSphere Client, or add a single host to a cluster by using PowerCLI or API (leveraging the addHost API)	On the host: Host.Inventory.Add host to cluster	Administrator
	On the cluster: • Host.Inventory.Modify cluster • Host.Inventory.Add host to cluster	Administrator
	On the data center: Host.Inventory.Add standalone host	Administrator
Add multiple hosts to a cluster	On the cluster: • Host.Inventory.Modify cluster • Host.Inventory.Add host to cluster	Administrator
	On the parent data center of the cluster (with propagate): • Host.Inventory.Add standalone host • Host.Inventory.Move host • Host.Inventory.Modify cluster • Host.Configuration.Maintenance	Administrator
Encrypt a virtual machine	Encryption tasks are possible only in environments that include vCenter Server. In addition, the ESXi host must have encryption mode enabled for most encryption tasks. The user who performs the task must have the appropriate privileges. A set of Cryptographic Operations privileges allows fine-grained control. See Prerequisites and Required Privileges for Encryption Tasks.	Administrator

vSphere Security Update 1 - VMware vSphere 7.0, page 42

Objective 7.5
Identify virtual networking issues that impact vSphere

Networking Best Practices

Consider these best practices when you configure your network.

- To ensure a stable connection between vCenter Server, ESXi, and other products and services, do not set connection limits and timeouts between the products. Setting limits and timeouts can affect the packet flow and cause services interruption.
- Isolate from one another the networks for host management, vSphere vMotion, vSphere FT, and so on, to improve security and performance.
- Dedicate a separate physical NIC to a group of virtual machines, or use Network I/O Control and traffic shaping to guarantee bandwidth to the virtual machines. This separation also enables distributing a portion of the total networking workload across multiple CPUs. The isolated virtual machines can then better handle application traffic, for example, from a vSphere Client.

- To physically separate network services and to dedicate a particular set of NICs to a specific network service, create a vSphere Standard Switch or vSphere Distributed Switch for each service. If this is not possible, separate network services on a single switch by attaching them to port groups with different VLAN IDs. In either case, verify with your network administrator that the networks or VLANs you choose are isolated from the rest of your environment and that no routers connect them.

- Keep the vSphere vMotion connection on a separate network. When migration with vMotion occurs, the contents of the guest operating system's memory is transmitted over the network. You can do this either by using VLANs to segment a single physical network or by using separate physical networks (the latter is preferable).

  For migration across IP subnets and for using separate pools of buffer and sockets, place traffic for vMotion on the vMotion TCP/IP stack, and traffic for migration of powered-off virtual machines and cloning on the Provisioning TCP/IP stack. See VMkernel Networking Layer.

- You can add and remove network adapters from a standard or distributed switch without affecting the virtual machines or the network service that is running behind that switch. If you remove all the running hardware, the virtual machines can still communicate among themselves. If you leave one network adapter intact, all the virtual machines can still connect with the physical network.

- To protect your most sensitive virtual machines, deploy firewalls in virtual machines that route between virtual networks with uplinks to physical networks and pure virtual networks with no uplinks.

- For best performance, use VMXNET 3 virtual machine NICs.

- Physical network adapters connected to the same vSphere Standard Switch or vSphere Distributed Switch should also be connected to the same physical network.

- Configure the same MTU on all VMkernel network adapters in a vSphere Distributed Switch. If several VMkernel network adapters, configured with different MTUs, are connected to vSphere distributed switches, you might experience network connectivity problems.

vSphere Networking Update 1 - VMware vSphere 7.0, page 259

Objective 7.7
Identify virtual storage issues that impact vSphere

Best Practices for Fibre Channel Storage

When using ESXi with Fibre Channel SAN, follow recommendations to avoid performance problems.

The vSphere Client offers extensive facilities for collecting performance information. The information is graphically displayed and frequently updated.

You can also use the `resxtop` or `esxtop` command-line utilities. The utilities provide a detailed look at how ESXi uses resources. For more information, see the *vSphere Resource Management* documentation.

Check with your storage representative if your storage system supports Storage API - Array Integration hardware acceleration features. If it does, refer to your vendor documentation to enable hardware acceleration support on the storage system side. For more information, see Chapter 24 Storage Hardware Acceleration.

This chapter includes the following topics:

- Preventing Fibre Channel SAN Problems

- Disable Automatic ESXi Host Registration
- Optimizing Fibre Channel SAN Storage Performance

Preventing Fibre Channel SAN Problems

When you use ESXi with a Fibre Channel SAN, follow specific guidelines to avoid SAN problems.

To prevent problems with your SAN configuration, observe these tips:

- Place only one VMFS datastore on each LUN.
- Do not change the path policy the system sets for you unless you understand the implications of making such a change.
- Document everything. Include information about zoning, access control, storage, switch, server and FC HBA configuration, software and firmware versions, and storage cable plan.
- Plan for failure:
  - Make several copies of your topology maps. For each element, consider what happens to your SAN if the element fails.
  - Verify different links, switches, HBAs, and other elements to ensure that you did not miss a critical failure point in your design.
- Ensure that the Fibre Channel HBAs are installed in the correct slots in the host, based on slot and bus speed. Balance PCI bus load among the available buses in the server.
- Become familiar with the various monitor points in your storage network, at all visibility points, including host's performance charts, FC switch statistics, and storage performance statistics.
- Be cautious when changing IDs of the LUNs that have VMFS datastores being used by your ESXi host. If you change the ID, the datastore becomes inactive and its virtual machines fail. Resignature the datastore to make it active again. See Managing Duplicate VMFS Datastores.

  After you change the ID of the LUN, rescan the storage to reset the ID on your host. For information on using the rescan, see Storage Rescan Operations.

Disable Automatic ESXi Host Registration

Certain storage arrays require that ESXi hosts register with the arrays. ESXi performs automatic host registration by sending the host's name and IP address to the array. If you prefer to perform manual registration using storage management software, disable the ESXi auto-registration feature.

Procedure

1 In the vSphere Client, navigate to the ESXi host.

2 Click the Configure tab.

3 Under System, click Advanced System Settings.

4 Under Advanced System Settings, select the Disk.EnableNaviReg parameter and click the Edit icon.

5 Change the value to 0.

Results

This operation disables the automatic host registration that is enabled by default.

Optimizing Fibre Channel SAN Storage Performance

Several factors contribute to optimizing a typical SAN environment.

If the environment is properly configured, the SAN fabric components (particularly the SAN switches) are only minor contributors because of their low latencies relative to servers and storage arrays. Make sure that the paths through the switch fabric are not saturated, that is, that the switch fabric is running at the highest throughput.

Storage Array Performance

Storage array performance is one of the major factors contributing to the performance of the entire SAN environment.

If you encounter any problems with storage array performance, consult your storage array vendor documentation for any relevant information.

To improve the array performance in the vSphere environment, follow these general guidelines:

- When assigning LUNs, remember that several hosts might access the LUN, and that several virtual machines can run on each host. One LUN used by a host can service I/O from many different applications running on different operating systems. Because of this diverse workload, the RAID group containing the ESXi LUNs typically does not include LUNs used by other servers that are not running ESXi.
- Make sure that the read/write caching is available.
- SAN storage arrays require continual redesign and tuning to ensure that I/O is load-balanced across all storage array paths. To meet this requirement, distribute the paths to the LUNs among all the SPs to provide optimal load-balancing. Close monitoring indicates when it is necessary to rebalance the LUN distribution.

  Tuning statically balanced storage arrays is a matter of monitoring the specific performance statistics, such as I/O operations per second, blocks per second, and response time. Distributing the LUN workload to spread the workload across all the SPs is also important.

  Note Dynamic load-balancing is not currently supported with ESXi.

Server Performance with Fibre Channel

You must consider several factors to ensure optimal server performance.

Each server application must have access to its designated storage with the following conditions:

- High I/O rate (number of I/O operations per second)
- High throughput (megabytes per second)
- Minimal latency (response times)

Because each application has different requirements, you can meet these goals by selecting an appropriate RAID group on the storage array.

To achieve performance goals, follow these guidelines:

- Place each LUN on a RAID group that provides the necessary performance levels. Monitor the activities and resource use of other LUNs in the assigned RAID group. A high-performance RAID group that has too many applications doing I/O to it might not meet performance goals required by an application running on the ESXi host.
- Ensure that each host has enough HBAs to increase throughput for the applications on the host for the peak period. I/O spread across multiple HBAs provides faster throughput and less latency for each application.
- To provide redundancy for a potential HBA failure, make sure that the host is connected to a dual redundant fabric.
- When allocating LUNs or RAID groups for ESXi systems, remember that multiple operating systems use and share that resource. The LUN performance required by the ESXi host might be much higher than when you use regular physical machines. For example, if you expect to run four I/O intensive applications, allocate four times the performance capacity for the ESXi LUNs.
- When you use multiple ESXi systems in with vCenter Server, the performance requirements for the storage subsystem increase correspondingly.
- The number of outstanding I/Os needed by applications running on the ESXi system must match the number of I/Os the HBA and storage array can handle.

vSphere Storage Update 1 - VMware vSphere 7.0, page 71

Best Practices for iSCSI Storage

When using ESXi with the iSCSI SAN, follow recommendations that VMware offers to avoid problems.

Check with your storage representative if your storage system supports Storage API - Array Integration hardware acceleration features. If it does, refer to your vendor documentation to enable hardware acceleration support on the storage system side. For more information, see Chapter 24 Storage Hardware Acceleration.

This chapter includes the following topics:

- Preventing iSCSI SAN Problems
- Optimizing iSCSI SAN Storage Performance
- Checking Ethernet Switch Statistics

Preventing iSCSI SAN Problems

When using ESXi with a SAN, you must follow specific guidelines to avoid SAN problems.

Observe the following tips:

- Place only one VMFS datastore on each LUN.
- Do not change the path policy the system sets for you unless you understand the implications of making such a change.
- Document everything. Include information about configuration, access control, storage, switch, server and iSCSI HBA configuration, software and firmware versions, and storage cable plan.
- Plan for failure:

    - Make several copies of your topology maps. For each element, consider what happens to your SAN if the element fails.
    - Cross off different links, switches, HBAs, and other elements to ensure that you did not miss a critical failure point in your design.
- Ensure that the iSCSI HBAs are installed in the correct slots in the ESXi host, based on slot and bus speed. Balance PCI bus load among the available buses in the server.
- Become familiar with the various monitor points in your storage network, at all visibility points, including ESXi performance charts, Ethernet switch statistics, and storage performance statistics.
- Change LUN IDs only when VMFS datastores deployed on the LUNs have no running virtual machines. If you change the ID, virtual machines running on the VMFS datastore might fail.

  After you change the ID of the LUN, you must rescan your storage to reset the ID on your host. For information on using the rescan, see Storage Rescan Operations.
- If you change the default iSCSI name of your iSCSI adapter, make sure that the name you enter is worldwide unique and properly formatted. To avoid storage access problems, never assign the same iSCSI name to different adapters, even on different hosts.

Optimizing iSCSI SAN Storage Performance

Several factors contribute to optimizing a typical SAN environment.

If the network environment is properly configured, the iSCSI components provide adequate throughput and low enough latency for iSCSI initiators and targets. If the network is congested and links, switches or routers are saturated, iSCSI performance suffers and might not be adequate for ESXi environments.

Storage System Performance

Storage system performance is one of the major factors contributing to the performance of the entire iSCSI environment.

If issues occur with storage system performance, consult your storage system vendor's documentation for any relevant information.

When you assign LUNs, remember that you can access each shared LUN through a number of hosts, and that a number of virtual machines can run on each host. One LUN used by the ESXi host can service I/O from many different applications running on different operating systems. Because of this diverse workload, the RAID group that contains the ESXi LUNs should not include LUNs that other hosts use that are not running ESXi for I/O intensive applications.

Enable read caching and write caching.

Load balancing is the process of spreading server I/O requests across all available SPs and their associated host server paths. The goal is to optimize performance in terms of throughput (I/O per second, megabytes per second, or response times).

SAN storage systems require continual redesign and tuning to ensure that I/O is load balanced across all storage system paths. To meet this requirement, distribute the paths to the LUNs among all the SPs to provide optimal load balancing. Close monitoring indicates when it is necessary to manually rebalance the LUN distribution.

Tuning statically balanced storage systems is a matter of monitoring the specific performance statistics (such as I/O operations per second, blocks per second, and response time) and distributing the LUN workload to spread the workload across all the SPs.

Server Performance with iSCSI

To ensure optimal ESXi host performance, consider several factors.

Each server application must have access to its designated storage with the following conditions:

- High I/O rate (number of I/O operations per second)
- High throughput (megabytes per second)
- Minimal latency (response times)

Because each application has different requirements, you can meet these goals by selecting an appropriate RAID group on the storage system.

To achieve performance goals, follow these guidelines:

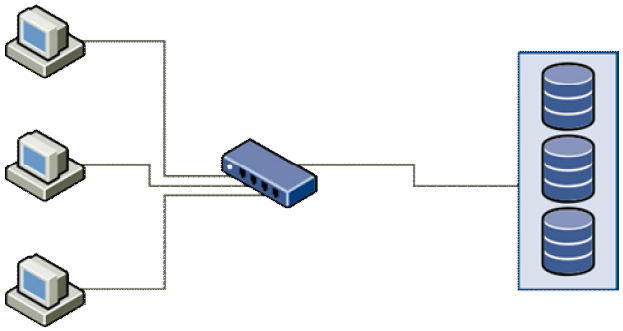
- Place each LUN on a RAID group that provides the necessary performance levels. Monitor the activities and resource use of other LUNS in the assigned RAID group. A high-performance RAID group that has too many applications doing I/O to it might not meet performance goals required by an application running on the ESXi host.
- To achieve maximum throughput for all the applications on the host during the peak period, install enough network adapters or iSCSI hardware adapters. I/O spread across multiple ports provides faster throughput and less latency for each application.
- To provide redundancy for software iSCSI, make sure that the initiator is connected to all network adapters used for iSCSI connectivity.
- When allocating LUNs or RAID groups for ESXi systems, remember that multiple operating systems use and share that resource. The LUN performance required by the ESXi host might be much higher than when you use regular physical machines. For example, if you expect to run four I/O intensive applications, allocate four times the performance capacity for the ESXi LUNs.
- When you use multiple ESXi systems with vCenter Server, the storage performance requirements increase.
- The number of outstanding I/Os needed by applications running on an ESXi system must match the number of I/Os the SAN can handle.

Network Performance

A typical SAN consists of a collection of computers connected to a collection of storage systems through a network of switches. Several computers often access the same storage.

The following graphic shows several computer systems connected to a storage system through an Ethernet switch. In this configuration, each system is connected through a single Ethernet link to the switch. The switch is connected to the storage system through a single Ethernet link.

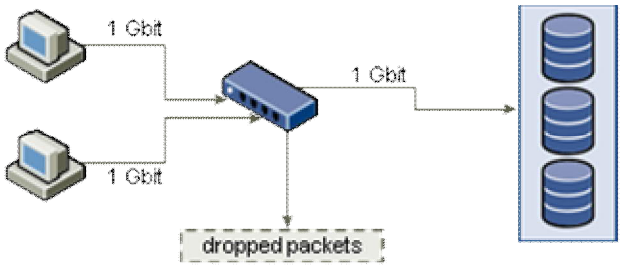
Figure 13-1. Single Ethernet Link Connection to Storage



When systems read data from storage, the storage responds with sending enough data to fill the link between the storage systems and the Ethernet switch. It is unlikely that any single system or virtual machine gets full use of the network speed. However, this situation can be expected when many systems share one storage device.

When writing data to storage, multiple systems or virtual machines might attempt to fill their links. As a result, the switch between the systems and the storage system might drop network packets. The data drop might occur because the switch has more traffic to send to the storage system than a single link can carry. The amount of data the switch can transmit is limited by the speed of the link between it and the storage system.

Figure 13-2. Dropped Packets



Recovering from dropped network packets results in large performance degradation. In addition to time spent determining that data was dropped, the retransmission uses network bandwidth that can otherwise be used for current transactions.

iSCSI traffic is carried on the network by the Transmission Control Protocol (TCP). TCP is a reliable transmission protocol that ensures that dropped packets are retried and eventually reach their destination. TCP is designed to recover from dropped packets and retransmits them quickly and seamlessly. However, when the switch discards packets with any regularity, network throughput suffers. The network becomes congested with requests to resend data and with the resent packets. Less data is transferred than in a network without congestion.

Most Ethernet switches can buffer, or store, data. This technique gives every device attempting to send data an equal chance to get to the destination. The ability to buffer some transmissions, combined with many systems limiting the number of outstanding commands, reduces transmissions to small bursts. The bursts from several systems can be sent to a storage system in turn.

If the transactions are large and multiple servers are sending data through a single switch port, an ability to buffer can be exceeded. In this case, the switch drops the data it cannot send, and the storage system must request a retransmission of the dropped packet. For example, if an Ethernet switch can buffer 32 KB, but the server sends 256 KB to the storage device, some of the data is dropped.

Most managed switches provide information on dropped packets, similar to the following:

```
*: interface is up
IHQ: pkts in input hold queue       IQD: pkts dropped from input queue
OHQ: pkts in output hold queue      OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec)            RXPS: rx rate (pkts/sec
TXBS: tx rate (bits/sec)            TXPS: tx rate (pkts/sec
TRTL: throttle count
```

Table 13-1. Sample Switch Information

Interface	IHQ	IQD	OHQ	OQD	RXBS	RXPS	TXBS	TXPS	TRTL
* GigabitEthernet0/1	3	9922	0	0	476303000	62273	477840000	63677	0

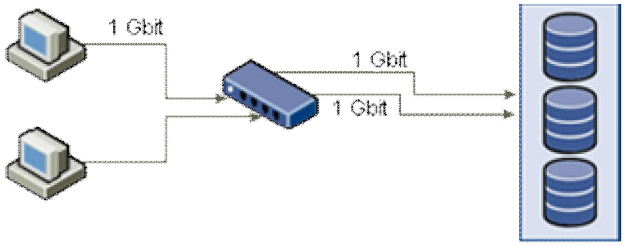
In this example from a Cisco switch, the bandwidth used is 476303000 bits/second, which is less than half of wire speed. The port is buffering incoming packets, but has dropped several packets. The final line of this interface summary indicates that this port has already dropped almost 10,000 inbound packets in the IQD column.

Configuration changes to avoid this problem involve making sure several input Ethernet links are not funneled into one output link, resulting in an oversubscribed link. When several links transmitting near capacity are switched to a smaller number of links, oversubscription becomes possible.

Generally, applications or systems that write much data to storage must avoid sharing Ethernet links to a storage device. These types of applications perform best with multiple connections to storage devices.

Multiple Connections from Switch to Storage shows multiple connections from the switch to the storage.

Figure 13-3. Multiple Connections from Switch to Storage



Using VLANs or VPNs does not provide a suitable solution to the problem of link oversubscription in shared configurations. VLANs and other virtual partitioning of a network provide a way of logically designing a network. However, they do not change the physical capabilities of links and trunks between switches. When storage traffic and other network traffic share physical connections, oversubscription and lost packets might become possible. The same is true of VLANs that share interswitch trunks. Performance design for a SAN must consider the physical limitations of the network, not logical allocations.

Checking Ethernet Switch Statistics

Many Ethernet switches provide different methods for monitoring switch health.

Switches that have ports operating near maximum throughput much of the time do not provide optimum performance. If you have ports in your iSCSI SAN running near the maximum, reduce the load. If the port is connected to an ESXi system or iSCSI storage, you can reduce the load by using manual load balancing.

If the port is connected between multiple switches or routers, consider installing additional links between these components to handle more load. Ethernet switches also commonly provide information about transmission errors, queued packets, and dropped Ethernet packets. If the switch regularly reports any of these conditions on ports being used for iSCSI traffic, performance of the iSCSI SAN will be poor.

vSphere Storage Update 1 - VMware vSphere 7.0, page 127

Best Practices for Working with vVols

Observe the following recommendations when you use vVols with ESXi and vCenter Server.

- Guidelines and Limitations when Using vVols

  For the best experience with vVols functionality, you must follow specific guidelines.

- Best Practices for Storage Container Provisioning

  Follow these best practices when provisioning storage containers on the vVols array side.

- Best Practices for vVols Performance

  To ensure optimal vVols performance results, follow these recommendations.

Guidelines and Limitations when Using vVols

For the best experience with vVols functionality, you must follow specific guidelines.

vVols supports the following capabilities, features, and VMware products:

- With vVols, you can use advanced storage services that include replication, encryption, deduplication, and compression on individual virtual disks. Contact your storage vendor for information about services they support with vVols.

- vVols functionality supports backup software that uses vSphere APIs - Data Protection. Virtual volumes are modeled on virtual disks. Backup products that use vSphere APIs - Data Protection are as fully supported on virtual volumes as they are on VMDK files on a LUN. Snapshots that the backup software creates using vSphere APIs - Data Protection look as non-vVols snapshots to vSphere and the backup software.

  Note vVols does not support SAN transport mode. vSphere APIs - Data Protection automatically selects an alternative data transfer method.

  For more information about integration with the vSphere Storage APIs - Data Protection, consult your backup software vendor.

- vVols supports such vSphere features as vSphere vMotion, Storage vMotion, snapshots, linked clones, and DRS.

- You can use clustering products, such as Oracle Real Application Clusters, with vVols. To use these products, you activate the multiwrite setting for a virtual disk stored on the vVols datastore.

For more details, see the knowledge base article at http://kb.vmware.com/kb/2112039. For a list of features and products that vVols functionality supports, see *VMware Product Interoperability Matrixes*.

vVols Limitations

Improve your experience with vVols by knowing the following limitations:

- Because the vVols environment requires vCenter Server, you cannot use vVols with a standalone host.

- vVols functionality does not support RDMs.

- A vVols storage container cannot span multiple physical arrays. Some vendors present multiple physical arrays as a single array. In such cases, you still technically use one logical array.

- Host profiles that contain vVols datastores are vCenter Server specific. After you extract this type of host profile, you can attach it only to hosts and clusters managed by the same vCenter Server as the reference host.

Best Practices for Storage Container Provisioning

Follow these best practices when provisioning storage containers on the vVols array side.

Creating Containers Based on Your Limits

Because storage containers apply logical limits when grouping virtual volumes, the container must match the boundaries that you want to apply.

Examples might include a container created for a tenant in a multitenant deployment, or a container for a department in an enterprise deployment.

- Organizations or departments, for example, Human Resources and Finance
- Groups or projects, for example, Team A and Red Team
- Customers

Putting All Storage Capabilities in a Single Container

Storage containers are individual datastores. A single storage container can export multiple storage capability profiles. As a result, virtual machines with diverse needs and different storage policy settings can be a part of the same storage container.

Changing storage profiles must be an array-side operation, not a storage migration to another container.

Avoiding Over-Provisioning Your Storage Containers

When you provision a storage container, the space limits that you apply as part of the container configuration are only logical limits. Do not provision the container larger than necessary for the anticipated use. If you later increase the size of the container, you do not need to reformat or repartition it.

Using Storage-Specific Management UI to Provision Protocol Endpoints

Every storage container needs protocol endpoints (PEs) that are accessible to ESXi hosts.

When you use block storage, the PE represents a proxy LUN defined by a T10-based LUN WWN. For NFS storage, the PE is a mount point, such as an IP address or DNS name, and a share name.

Typically, configuration of PEs is array-specific. When you configure PEs, you might need to associate them with specific storage processors, or with certain hosts. To avoid errors when creating PEs, do not configure them manually. Instead, when possible, use storage-specific management tools.

No Assignment of IDs Above Disk.MaxLUN to Protocol Endpoint LUNs

By default, an ESXi host can access LUN IDs that are within the range of 0 to 1023. If the ID of the protocol endpoint LUN that you configure is 1024 or greater, the host might ignore the PE.

If your environment uses LUN IDs that are greater than 1023, change the number of scanned LUNs through the `Disk.MaxLUN` parameter. See Change the Number of Scanned Storage Devices.

Best Practices for vVols Performance

To ensure optimal vVols performance results, follow these recommendations.

Using Different VM Storage Policies for Individual Virtual Volume Components

By default, all components of a virtual machine in the vVols environment get a single VM storage policy. However, different components might have different performance characteristics, for example, a database virtual disk and a corresponding log virtual disk. Depending on performance requirements, you can assign different VM storage policies to individual virtual disks and to the VM home file, or config-vVol.

When you use the vSphere Client, you cannot change the VM storage policy assignment for swap-vVol, memory-vVol, or snapshot-vVol.

See Create a VM Storage Policy for vVols.

Getting a Host Profile with vVols

The best way to get a host profile with vVols is to configure a reference host and extract its profile. If you manually edit an existing host profile in the vSphere Client and attach the edited profile to a new host, you might trigger compliance errors. Other unpredictable problems might occur. For more details, see the VMware Knowledge Base article 2146394.

Monitoring I/O Load on Individual Protocol Endpoint

- All virtual volume I/O goes through protocol endpoints (PEs). Arrays select protocol endpoints from several PEs that are accessible to an ESXi host. Arrays can do load balancing and change the binding path that connects the virtual volume and the PE. See Binding and Unbinding Virtual Volumes to Protocol Endpoints.
- On block storage, ESXi gives a large queue depth to I/O because of a potentially high number of virtual volumes. The `Scsi.ScsiVVolPESNRO` parameter controls the number of I/O that can be queued for PEs. You can configure the parameter on the Advanced System Settings page of the vSphere Client.

Monitoring Array Limitations

A single VM might occupy multiple virtual volumes. See Virtual Volume Objects.

Suppose that your VM has two virtual disks, and you take two snapshots with memory. Your VM might occupy up to 10 vVols objects: a config-vVol, a swap-vVol, two data-vVols, four snapshot-vVols, and two memory snapshot-vVols.

Ensuring that Storage Provider Is Available

To access vVols storage, your ESXi host requires a storage provider (VASA provider). To ensure that the storage provider is always available, follow these guidelines:

- Do not migrate a storage provider VM to vVols storage.
- Back up your storage provider VM.
- When appropriate, use vSphere HA or Site Recovery Manager to protect the storage provider VM.

vSphere Storage Update 1 - VMware vSphere 7.0, page 323

Objective 7.8
Identify the purpose of monitoring alarms, tasks and events

Events

Events are records of user actions or system actions that occur on objects in vCenter Server or on a host. Actions that might be recorded as events include, but are not limited to, the following examples:

- A license key expires
- A virtual machine is powered on
- A user logs in to a virtual machine
- A host connection is lost

Event data includes details about the event such as who generated it, when it occurred, and what type of event it is.

The types of events are:

Table 5-1. Event Types

Event Type	Description
Error	Indicates that a fatal problem has occurred in the system and terminates the process or operation.
Warning	Indicates that there is a potential risk to the system which needs to be fixed. This event does not terminate the process or operation.
Information	Describes that the user or system operation is completed successfully.
Audit	Provides important audit log data which is crucial for the security framework. The audit log data includes information about what is the action, who did it, when it occurred, and the IP address of the user. You can learn more about this in the vSphere Security guide.

Alarms

Alarms are notifications that are activated in response to an event, a set of conditions, or the state of an inventory object. An alarm definition consists of the following elements in the vSphere Client:

- Name and description - Provides an identifying label and description.
- Targets - Defines the type of object that is monitored.
- Alarm Rules - Defines the event, condition, or state that triggers the alarm and defines the notification severity. It also defines operations that occur in response to triggered alarms.
- Last modified - The last modified date and time of the defined alarm.

Alarms have the following severity levels:

- Normal – green
- Warning – yellow
- Alert – red

Alarm definitions are associated with the object selected in the inventory. An alarm monitors the type of inventory objects specified in its definition.

For example, you might want to monitor the CPU usage of all virtual machines in a specific host cluster. You can select the cluster in the inventory, and add a virtual machine alarm to it. When enabled, that alarm monitors all virtual machines running in the cluster and triggers when any one of them meets the criteria defined in the alarm. To monitor a specific virtual machine in the cluster, but not others, select that virtual machine in the inventory and add an alarm to it. To apply the same alarms to a group of objects, place those objects in a folder and define the alarm on the folder.

Note You can enable, disable, and modify alarms only from the object in which the alarm is defined. For example, if you defined an alarm in a cluster to monitor virtual machines, you can only enable, disable, or modify that alarm through the cluster. You cannot change the alarm at the individual virtual machine level.

vSphere Monitoring and Performance Update 1 – Vmware vSphere 7.0, page 130

Objective 7.9
Identify how to monitor vSphere Cluster and SDRS Cluster

Monitoring vSphere Cluster Services

You can monitor the resources consumed by vCLS VMs and their health status.

vCLS VMs are not displayed in the inventory tree in the Hosts and Clusters tab. vCLS VMs from all clusters within a data center are placed inside a separate VMs and templates folder named vCLS. This folder and the vCLS VMs are visible only in the VMs and Templates tab of the vSphere Client. These VMs are identified by a different icon than regular workload VMs. You can view information about the purpose of the vCLS VMs in the Summary tab of the vCLS VMs.

You can monitor the resources consumed by vCLS VMs in the Monitor tab.

Table 11-3. vCLS VM Resource Allocation

Property	Size
VMDK size	245 MB (thin disk)
Memory	128 MB
CPU	1 vCPU
Hard disk	2 GB
Storage on datastore	480 MB (thin disk)

Note Each vCLS VM has 100MHz and 100MB capacity reserved in the cluster. Depending on the number of vCLS VMs running in the cluster, a max of 400 MHz and 400 MB of capacity can be reserved for these VMs.

You can monitor the health status of vCLS in the Cluster Services portlet displayed in the Summary tab of the cluster.

Table 11-4. Health status of vCLS

Status	Color Coding	Summary
Healthy	Green	If there is at least one vCLS VM running, the status remains healthy, regardless of the number of hosts in the cluster.

Degraded	Yellow	If there is no vCLS VM running for less than 3 minutes (180 seconds), the status is degraded.
Unhealthy	Red	If there is no vCLS VM running for 3 minutes or more, the status is unhealthy in a DRS enabled cluster.

vSphere Resource Management Update 1 – Vmware vSphere 7.0, page 78

Objective 7.10
Identify how to perform and monitor vMotion, Storage vMotion, and Cold migrations

Migrating Virtual Machines

You can move virtual machines from one compute resource or storage location to another by using cold or hot 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.

Moving a virtual machine from one inventory folder to another folder or resource pool in the same data center is not a form of migration. Unlike migration, cloning a virtual machine or copying its virtual disks and configuration file are procedures that create a new virtual machine. Cloning and copying a virtual machine are also not forms of migration.

By using migration, you can change the compute resource that the virtual machine runs on. For example, you can move a virtual machine from one host to another host or cluster.

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

Depending on the power state of the virtual machine that you migrate, migration can be cold or hot.

Cold Migration

Moving 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 virtual switch to another, and from one data center to another. You can perform cold migration manually or you can schedule a task.

Hot Migration

Moving a powered on virtual machine to a new host. Optionally, you can also move the virtual machine disks or folder to a different datastore. Hot migration is also called live migration or vMotion. With vMotion, you migrate the virtual machine without any interruption in its availability.

Depending on the virtual machine resource type, you can perform three types of migration.

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 can move the virtual machine to another compute resource by using cold or hot migration. If you change the compute resource of a powered on virtual machine, you use vMotion.

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 of a virtual machine by using cold or hot migration. If you move a powered on virtual machine and its storage to a new datastore, you use Storage vMotion.

Change both compute resource and storage

Moving a virtual machine to another host and at the same time moving its disk or virtual machine folder to another datastore. You can change the host and datastore simultaneously by using cold or hot migration.

In vSphere 6.0 and later, you can move virtual machines between vSphere sites by using migration between the following 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. By using 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. 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.

Migrate to another data center

Moving a virtual machine to a different data center. You can change the data center of a virtual machine by using cold or hot migration. 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 a virtual machine to a vCenter Server instance that is connected to the source vCenter Server instance through vCenter Enhanced Linked Mode.

You can also move virtual machines between vCenter Server instances that are located across a long distance from each other.

This chapter includes the following topics:

- Cold Migration
- Migration with vMotion
- Migration with Storage vMotion
- CPU Compatibility and EVC
- Migrate a Powered Off or Suspended Virtual Machine
- Migrate a Virtual Machine to a New Compute Resource
- Migrate a Virtual Machine to a New Compute Resource and Storage
- Migrate a Virtual Machine to New Storage
- Place vMotion Traffic on the vMotion TCP/IP Stack of an ESXi Host
- Place Traffic for Cold Migration, Cloning, and Snapshots on the Provisioning TCP/IP Stack
- Limits on Simultaneous Migrations
- About Migration Compatibility Checks

Cold Migration

Cold migration is the migration of powered off or suspended virtual machines between hosts across clusters, data centers, and vCenter Server instances. By using cold migration, you can also move associated disks from one datastore to another.

You can use cold migration to have the target host checked against fewer requirements than when you use vMotion. For example, if you use cold migration when a virtual machine contains a complex application setup, the compatibility checks during vMotion might prevent the virtual machine from moving to another host.

You must power off or suspend the virtual machines before you begin the cold migration process. Migrating a suspended virtual machine is considered a cold migration because although the virtual machine is powered on, it is not running.

You cannot implement a cold migration across different subnets.

CPU Compatibility Check During Cold Migration

If you attempt to migrate a powered off virtual machine that is configured with a 64-bit operating system to a host that does not support 64-bit operating systems, vCenter Server generates a warning. Otherwise, CPU compatibility checks do not apply when you migrate powered off virtual machines with cold migration.

When you migrate a suspended virtual machine, the new host for the virtual machine must meet CPU compatibility requirements. This requirement allows the virtual machine to resume execution on the new host.

Operations During Cold Migration

A cold migration consists of the following operations:

1. If you select the option to move to a different datastore, the configuration files, including the NVRAM file (BIOS settings), log files, and the suspend file, are moved from the source host to the destination host's associated storage area. You can choose to move the virtual machine's disks as well.
2. The virtual machine is registered with the new host.
3. After the migration is completed, the old version of the virtual machine is deleted from the source host and datastore if you selected the option to move to a different datastore.

Network Traffic for Cold Migration

By default, data for VM cold migration, cloning, and snapshots is transferred through the management network. This traffic is called provisioning traffic. It is not encrypted but uses run-length encoding of data.

On a host, you can dedicate a separate VMkernel network adapter to the provisioning traffic, for example, to isolate this traffic on another VLAN. On a host, you can assign no more than one VMkernel adapter for provisioning traffic. For information about enabling provisioning traffic on a separate VMkernel adapter, see the *vSphere Networking* documentation.

If you plan to transfer high volumes of virtual machine data that the management network cannot accommodate, redirect the cold migration traffic on a host to the TCP/IP stack that is dedicated to cold migration and cloning of powered off virtual machines. You can also redirect if you want to isolate cold migration traffic in a subnet different from the management network, for example, for migration over a long distance. See Place Traffic for Cold Migration, Cloning, and Snapshots on the Provisioning TCP/IP Stack.

Migration with vMotion

If you must take a host offline for maintenance, you can move the virtual machine to another host. Migration with vMotion™ allows virtual machine processes to continue working throughout a migration.

When you migrate a virtual machine with vMotion, the new host for the virtual machine must meet compatibility requirements so that the migration can proceed.

vMotion Migration Types

With vMotion, you can change the compute resource on which a virtual machine is running. You also can change both the compute resource and the storage of the virtual machine.

When you migrate virtual machines with vMotion and choose to change only the host, the entire state of the virtual machine is moved to the new host. The associated virtual disk remains in the same location on storage that must be shared between the two hosts.

When you choose to change both the host and the datastore, the virtual machine state is moved to a new host and the virtual disk is moved to another datastore. vMotion migration to another host and datastore is possible in vSphere environments without shared storage.

After the virtual machine state is migrated to the alternate host, the virtual machine runs on the new host. Migrations with vMotion are transparent to the running virtual machine.

When you choose to change both the compute resource and the storage, you can use vMotion to migrate virtual machines across vCenter Server instances, data centers, and subnets.

Transferred State Information

The state information includes the current memory content and all the information that defines and identifies the virtual machine. The memory content includes transaction data and the bits of the operating system and applications that are in the memory. The defining and identification information stored in the state includes all the data that maps to the virtual machine hardware elements. This information includes BIOS, devices, CPU, MAC addresses for the Ethernet cards, chipset states, registers, and so forth.

Stages in vMotion

Migration with vMotion occurs in three stages:

1 When the migration with vMotion is requested, vCenter Server verifies that the existing virtual machine is in a stable state with its current host.

2 The virtual machine state information (memory, registers, and network connections) is copied to the target host.

3 The virtual machine resumes its activities on the new host.

If errors occur during migration, the virtual machine reverts to its original state and location.

Host Configuration for vMotion

Before using vMotion, you must configure your hosts correctly.

Ensure that you have correctly configured your hosts.

- Each host must be correctly licensed for vMotion.
- Each host must meet shared storage requirements for vMotion.
- Each host must meet the networking requirements for vMotion.

> Important The ESXi firewall in ESXi 6.5 and later does not allow per-network filtering of vMotion traffic. Therefore, you must apply rules on your external firewall to ensure that no incoming connections can be made to the vMotion socket on TCP port 8000.

vMotion Across Long Distances

You can perform reliable migrations between hosts and sites that are separated by high network round-trip latency times. vMotion across long distances is enabled when the appropriate license is installed. No user configuration is necessary.

For long-distance migration, verify the network latency between the hosts and your license.

- The round-trip time between the hosts must be up to 150 milliseconds.
- Your license must cover vMotion across long distances.
- You must place the traffic related to transfer of virtual machine files to the destination host on the provisioning TCP/IP stack. See Place Traffic for Cold Migration, Cloning, and Snapshots on the Provisioning TCP/IP Stack.

vMotion Shared Storage Requirements

Configure hosts for vMotion with shared storage to ensure that virtual machines are accessible to both source and target hosts.

During a migration with vMotion, the migrating virtual machine must be on storage accessible to both the source and target hosts. Ensure that the hosts configured for vMotion use shared storage. Shared storage can be on a Fibre Channel storage area network (SAN), or can be implemented using iSCSI and NAS.

If you use vMotion to migrate virtual machines with raw device mapping (RDM) files, make sure to maintain consistent LUN IDs for RDMs across all participating hosts.

See the *vSphere Storage* documentation for information on SANs and RDMs.

vSphere vMotion Networking Requirements

Migration with vMotion requires correctly configured network interfaces on source and target hosts.

Configure each host with at least one network interface for vMotion traffic. To ensure secure data transfer, the vMotion network must be a secure network, accessible only to trusted parties. Additional bandwidth significantly improves vMotion performance. When you migrate a virtual machine with vMotion without using shared storage, the contents of the virtual disk is transferred over the network as well.

vSphere 6.5 and later allow the network traffic with vMotion to be encrypted. Encrypted vMotion depends on host configuration, or on compatibility between the source and destination hosts.

Requirements for Concurrent vMotion Migrations

You must ensure that the vMotion network has at least 250 Mbps of dedicated bandwidth per concurrent vMotion session. Greater bandwidth lets migrations complete more quickly. Gains in throughput resulting from WAN optimization techniques do not count towards the 250-Mbps limit.

To determine the maximum number of concurrent vMotion operations possible, see Limits on Simultaneous Migrations. These limits vary with a host's link speed to the vMotion network.

Round-Trip Time for Long-Distance vMotion Migration

If you have the proper license applied to your environment, you can perform reliable migrations between hosts that are separated by high network round-trip latency times. The

maximum supported network round-trip time for vMotion migrations is 150 milliseconds. This round-trip time lets you migrate virtual machines to another geographical location at a longer distance.

Multiple-NIC vMotion

You can configure multiple NICs for vMotion by adding two or more NICs to the required standard or distributed switch. For details, see Knowledge Base article KB 2007467.

Network Configuration

Configure the virtual networks on vMotion enabled hosts as follows:

- On each host, configure a VMkernel port group for vMotion.

  To have the vMotion traffic routed across IP subnets, enable the vMotion TCP/IP stack on the host. See Place vMotion Traffic on the vMotion TCP/IP Stack of an ESXi Host.

- If you are using standard switches for networking, ensure that the network labels used for the virtual machine port groups are consistent across hosts. During a migration with vMotion, vCenter Server assigns virtual machines to port groups based on matching network labels.

Note By default, you cannot use vMotion to migrate a virtual machine that is attached to a standard switch with no physical uplinks configured, even if the destination host also has a no-uplink standard switch with the same label.

To override the default behavior, set the `config.migrate.test.CompatibleNetworks.VMOnVirtualIntranet` advanced settings of vCenter Server to `false`. The change takes effect immediately. For details about the setting, see Knowledge Base article KB 1003832. For information about configuring advanced settings of vCenter Server, see *vCenter Server Configuration*.

For information about configuring the vMotion network resources, see Networking Best Practices for vSphere vMotion.

For more information about vMotion networking requirements, see Knowledge Base article KB 59232.

Networking Best Practices for vSphere vMotion

Consider certain best practices for configuring the network resources for vMotion on an ESXi host.

- Provide the required bandwidth in one of the following ways:

Physical Adapter Configuration	Best Practices
Dedicate at least one adapter for vMotion.	Use at least one 1 GbE adapter for workloads that have a small number of memory operations. Use at least one 10 GbE adapter if you migrate workloads that have many memory operations. • If only two Ethernet adapters are available, configure them for security and availability.For best security, dedicate one adapter to vMotion, and use VLANs to divide the virtual machine and management traffic on the other adapter. • For best availability, combine both adapters into a team, and use VLANs to divide traffic into networks: one or more for virtual machine traffic and one for vMotion
Direct vMotion traffic to one or more physical NICs that have high-bandwidth capacity and are shared between other types of traffic as well	• To distribute and allocate more bandwidth to vMotion traffic across several physical NICs, use multiple-NIC vMotion. • On a vSphere Distributed Switch 5.1 and later, use vSphere Network I/O Control shares to guarantee bandwidth to outgoing vMotion traffic. Defining shares also prevents from contention as a result from excessive vMotion or other traffic.

	• To avoid saturation of the physical NIC link as a result of intense incoming vMotion traffic, use traffic shaping in egress direction on the vMotion port group on the destination host. By using traffic shaping you can limit the average and peak bandwidth available to vMotion traffic, and reserve resources for other traffic types.

- Provision at least one additional physical NIC as a failover NIC.
- Use jumbo frames for best vMotion performance.

  Ensure that jumbo frames are enabled on all network devices that are on the vMotion path including physical NICs, physical switches, and virtual switches.
- Place vMotion traffic on the vMotion TCP/IP stack for migration across IP subnets that have a dedicated default gateway that is different from the gateway on the management network. See Place vMotion Traffic on the vMotion TCP/IP Stack of an ESXi Host.

For information about configuring networking on an ESXi host, see the *vSphere Networking* documentation.

Encrypted vSphere vMotion

vSphere vMotion always uses encryption when migrating encrypted virtual machines. For virtual machines that are not encrypted, you can select one of the encrypted vSphere vMotion options.

Encrypted vSphere vMotion secures confidentiality, integrity, and authenticity of data that is transferred with vSphere vMotion. vSphere supports encrypted vMotion of unencrypted and encrypted virtual machines across vCenter Server instances.

What Is Encrypted

For encrypted disks, the data is transmitted encrypted. For disks that are not encrypted, Storage vMotion encryption is not supported.

For virtual machines that are encrypted, migration with vSphere vMotion always uses encrypted vSphere vMotion. You cannot turn off encrypted vSphere vMotion for encrypted virtual machines.

Encrypted vSphere vMotion States

For virtual machines that are not encrypted, you can set encrypted vSphere vMotion to one of the following states. The default is Opportunistic.

Disabled

Do not use encrypted vSphere vMotion.

Opportunistic

Use encrypted vSphere vMotion if source and destination hosts support it. Only ESXi versions 6.5 and later use encrypted vSphere vMotion.

Required

Allow only encrypted vSphere vMotion. If the source or destination host does not support encrypted vSphere vMotion, migration with vSphere vMotion is not allowed.

When you encrypt a virtual machine, the virtual machine keeps a record of the current encrypted vSphere vMotion setting. If you later disable encryption for the virtual machine, the encrypted vMotion setting remains at Required until you change the setting explicitly. You can change the settings using Edit Settings.

Note Currently, you must use the vSphere APIs to migrate or clone encrypted virtual machines across vCenter Server instances. See *vSphere Web Services SDK Programming Guide* and *vSphere Web Services API Reference*.

Migrating or Cloning Encrypted Virtual Machines Across vCenter Server Instances

vSphere vMotion supports migrating and cloning encrypted virtual machines across vCenter Server instances.

When migrating or cloning encrypted virtual machines across vCenter Server instances, the source and destination vCenter Server instances must be configured to share the Key Management Server cluster that was used to encrypt the virtual machine. In addition, the KMS cluster name must be the same on both the source and destination vCenter Server instances. The destination vCenter Server ensures the destination ESXi host has encryption mode enabled, ensuring the host is cryptographically "safe."

The following privileges are required when using vSphere vMotion to migrate or clone an encrypted virtual machine across vCenter Server instances.

- Migrating: Cryptographic operations.Migrate on the virtual machine
- Cloning: Cryptographic operations.Clone on the virtual machine

Also, the destination vCenter Server must have the Cryptographic operations.EncryptNew privilege. If the destination ESXi host is not in "safe" mode, the Cryptographic operations.RegisterHost privilege must also be on the destination vCenter Server.

Certain tasks are not allowed when migrating encrypted virtual machines across vCenter Server instances.

- You cannot change the VM Storage Policy.
- You cannot perform a key change.

vSphere Trust Authority and Encrypted vMotion

vSphere Trust Authority supports vSphere vMotion in migrating and cloning encrypted virtual machines across vCenter Server instances with the following requirements.

- The vSphere Trust Authority service must be configured for the destination host and the destination host must be attested.
- Encryption cannot change on migration. For example, an unencrypted disk cannot be encrypted while the virtual machine is migrated to the new storage.
- You can migrate a standard encrypted virtual machine onto a Trusted Host. The KMS cluster name must be the same on both the source and destination vCenter Server instances.
- You cannot migrate a vSphere Trust Authority encrypted virtual machine onto a non-Trusted Host.

Enable or Disable Encrypted vMotion

You can enable encrypted vMotion during virtual machine creation. You can later change the encrypted vMotion state from the virtual machine settings. You can change the encrypted vMotion state only for virtual machines that are not encrypted.

For more information about virtual machine encryption, see Encrypted vSphere vMotion.

Prerequisites

Encrypted vMotion is supported only in vSphere 6.5 and later.

Procedure

1 Right-click the virtual machine and select Edit Settings.

2 Select VM Options.

3 Click Encryption, and select an option from the Encrypted VMotion drop-down menu.

Disabled

Do not use encrypted vMotion.

Opportunistic

Use encrypted vMotion if source and destination hosts support it. Only ESXi hosts of version 6.5 and later use encrypted vMotion.

Required

Allow only encrypted vMotion. If the source or destination host does not support encrypted vMotion, migration with vMotion fails.

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.
- Starting with vSphere 6.7 Update 1 and later, vSphere vMotion supports virtual machines with vGPU.
- vSphere DRS supports initial placement of vGPU virtual machines running vSphere 6.7 Update 1 or later without load balancing support.
- 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.

Using vMotion to Migrate vGPU Virtual Machines

You can use vMotion to perform a live migration of NVIDIA vGPU-powered virtual machines without causing data loss.

In vSphere 6.7 Update 1 and vSphere 6.7 Update 2, when you migrate vGPU virtual machines with vMotion and vMotion stun time exceeds 100 seconds, the migration process might fail for vGPU profiles with 24 GB frame buffer size or larger. To avoid the vMotion timeout, upgrade to vSphere 6.7 Update 3 or later.

During the stun time, you are unable to access the VM, desktop, or application. Once the migration is completed, access to the VM resumes and all applications continue from their previous state. For information on frame buffer size in vGPU profiles, refer to the NVIDIA Virtual GPU documentation.

The expected VM stun times (the time when the VM is inaccessible to users during vMotion) are listed in the following table. These stun times were tested over a 10Gb network with NVIDIA Tesla V100 PCIe 32 GB GPUs :

Table 12-1. Expected Stun Times for vMotion of vGPU VMs

Used vGPU Frame Buffer (GB)	VM Stun Time (sec)
1	1.95
2	3.18
4	5.74
8	11.05
16	21.32
32	38.83

Note The configured vGPU profile represents an upper bound to the used vGPU frame buffer. In many VDI/Graphics use cases, the amount of vGPU frame buffer memory used by the VM at any given time is below the assigned vGPU memory in the profile. Treat these times as worst case stun times for cases when the entire assigned vGPU memory is being used at the time of the migration. For example, a V100-32Q vGPU profile allocates 32 GB of vGPU frame buffer to the VM, but the VM can use any amount between 0-32 GB of frame buffer during the migration. As a result, the stun time can end up being between less than 1 second to 38.83 seconds.

DRS supports initial placement of vGPU VMs running vSphere 6.7 Update 1 and later without load balancing support.

VMware vSphere vMotion is supported only with and between compatible NVIDIA GPU device models and NVIDIA GRID host driver versions as defined and supported by NVIDIA. For compatibility information, refer to the NVIDIA Virtual GPU User Guide.

To check compatibility between NVIDIA vGPU host drivers, vSphere, and Horizon, refer to the VMware Compatibility Matrix.

Swap File Location Compatibility

Virtual machine swap file location affects vMotion compatibility in different ways depending on the version of ESXi running on the virtual machine's host.

You can configure ESXi 6.5 or later hosts to store virtual machine swap files with the virtual machine configuration file, or on a local swap file datastore specified for that host.

The location of the virtual machine swap file affects vMotion compatibility as follows:

- For migrations between hosts running ESXi 6.5 and later, vMotion and migrations of suspended and powered-off virtual machines are allowed.

- During a migration with vMotion, if the swap file location on the destination host differs from the swap file location on the source host, the swap file is copied to the new location. This activity can result in slower migrations with vMotion. If the destination host cannot access the specified swap file location, it stores the swap file with the virtual machine configuration file.

See the *vSphere Resource Management* documentation for information about configuring swap file policies.

Migration with vMotion in Environments Without Shared Storage

You can use vMotion to migrate virtual machines to a different compute resource and storage simultaneously. Unlike Storage vMotion, which requires a single host to have access to both the source and destination datastore, you can migrate virtual machines across storage accessibility boundaries.

vMotion does not require environments with shared storage. This is useful for performing cross-cluster migrations, when the target cluster machines might not have access to the storage of the source cluster. Processes that are working on the virtual machine continue to run during the migration with vMotion.

You can use vMotion to migrate virtual machines across vCenter Server instances.

You can place the virtual machine and all its disks in a single location or select separate locations for the virtual machine configuration file and each virtual disk. In addition, you can change virtual disks from thick-provisioned to thin-provisioned or from thin-provisioned to thick-provisioned. For virtual compatibility mode RDMs, you can migrate the mapping file or convert from RDM to VMDK.

vMotion without shared storage is useful for virtual infrastructure administration tasks similar to vMotion with shared storage or Storage vMotion tasks.

- Host maintenance. You can move virtual machines from a host to allow maintenance of the host.

- Storage maintenance and reconfiguration. You can move virtual machines from a storage device to allow maintenance or reconfiguration of the storage device without virtual machine downtime.

- Storage load redistribution. You can manually redistribute virtual machines or virtual disks to different storage volumes to balance capacity or improve performance.

Requirements and Limitations for vMotion Without Shared Storage

A virtual machine and its host must meet resource and configuration requirements for the virtual machine files and disks to be migrated with vMotion in the absence of shared storage.

vMotion in an environment without shared storage is subject to the following requirements and limitations:

- The hosts must be licensed for vMotion.

- The hosts must be running ESXi 5.1 or later.

- The hosts must meet the networking requirement for vMotion. See vSphere vMotion Networking Requirements.

- The virtual machines must be properly configured for vMotion. See Virtual Machine Conditions and Limitations for vMotion

- Virtual machine disks must be in persistent mode or be raw device mappings (RDMs). See Storage vMotion Requirements and Limitations.
- The destination host must have access to the destination storage.
- When you move a virtual machine with RDMs and do not convert those RDMs to VMDKs, the destination host must have access to the RDM LUNs.
- Consider the limits for simultaneous migrations when you perform a vMotion migration without shared storage. This type of vMotion counts against the limits for both vMotion and Storage vMotion, so it consumes both a network resource and 16 datastore resources. See Limits on Simultaneous Migrations.

Migration Between vCenter Server Systems

vSphere 6.0 or later lets you migrate virtual machines between vCenter Server instances.

Migration of virtual machines across vCenter Server systems is helpful in certain VM provisioning cases.

- Balance workloads across clusters and vCenter Server instances.
- Elastically expand or shrink capacity across resources in different vCenter Server instances in the same site or in another geographical area .
- Move virtual machines between environments that have different purposes, for example, from a development to production.
- Move virtual machines to meet different Service Level Agreements (SLAs) regarding storage space, performance, and so on.

Note During the migration of a virtual machine to another vCenter Server system, the performance data that has been collected about the virtual machine is lost.

- Requirements for Migration Between vCenter Server Instances
- You can use migration across vCenter Server instances if your system meets certain requirements.
- Network Compatibility Checks During vMotion Between vCenter Server Instances
- Migration of VMs between vCenter Server instances moves VMs to new networks. The migration process performs checks to verify that the source and destination networks are similar.
- MAC Address Management During Migration Between vCenter Server Systems
- When you move a virtual machine between vCenter Server instances, the environment specifically handles MAC address migration to avoid address duplication and loss of data in the network.

Requirements for Migration Between vCenter Server Instances

You can use migration across vCenter Server instances if your system meets certain requirements.

The following list sums the requirements that your system must meet so that you can use migration across vCenter Server instances:

- The source and destination vCenter Server instances and ESXi hosts must be 6.0 or later.

- The cross vCenter Server and long-distance vMotion features require an Enterprise Plus license. For more information, see http://www.vmware.com/uk/products/vsphere/compare.html.

- Both vCenter Server instances must be time-synchronized with each other for correct vCenter Single Sign-On token verification.

- For migration of compute resources only, both vCenter Server instances must be connected to the shared virtual machine storage.

- When using the vSphere Client, both vCenter Server instances must be in Enhanced Linked Mode and must be in the same vCenter Single Sign-On domain. Enhanced Link Mode lets the source vCenter Server authenticate to the destination vCenter Server.

  For information about installing vCenter Server in Enhanced Linked Mode, see the *vCenter Server Installation and Setup* documentation.

  If the vCenter Server instances exist in separate vCenter Single Sign-On domains, you can use vSphere APIs/SDK to migrate virtual machines. For more information, see the VirtualMachineRelocateSpec data object in the *VMware vSphere API Reference*.

Network Compatibility Checks During vMotion Between vCenter Server Instances

Migration of VMs between vCenter Server instances moves VMs to new networks. The migration process performs checks to verify that the source and destination networks are similar.

vCenter Server performs network compatibility checks to prevent the following configuration problems:

- MAC address compatibility on the destination host

- vMotion from a distributed switch to a standard switch

- vMotion between distributed switches of different versions

- vMotion to an internal network, for example, a network without a physical NIC

- vMotion to a distributed switch that is not working properly

vCenter Server does not perform checks for and notify you about the following problems:

- If the source and destination distributed switches are not in the same broadcast domain, virtual machines lose network connectivity after migration.

- If the source and destination distributed switches do not have the same services configured, virtual machines might lose network connectivity after migration.

MAC Address Management During Migration Between vCenter Server Systems

When you move a virtual machine between vCenter Server instances, the environment specifically handles MAC address migration to avoid address duplication and loss of data in the network.

In an environment with multiple vCenter Server instances, when a virtual machine is migrated, its MAC addresses are transferred to the target vCenter Server. The source vCenter Server adds the MAC addresses to a denylist so that it does not assign them to newly created virtual machines.

To reclaim unused MAC addresses from the denylist, contact VMware Technical Support for assistance.

Migration with Storage vMotion

With Storage vMotion, you can migrate a virtual machine and its disk files from one datastore to another while the virtual machine is running. With Storage vMotion, you can move virtual machines off of arrays for maintenance or to upgrade. You also have the flexibility to optimize disks for performance, or to transform disk types, which you can use to reclaim space.

You can choose to place the virtual machine and all its disks in a single location, or you can select separate locations for the virtual machine configuration file and each virtual disk. The virtual machine does not change execution host during a migration with Storage vMotion.

During a migration with Storage vMotion, you can change the disk provisioning type.

Migration with Storage vMotion changes virtual machine files on the destination datastore to match the inventory name of the virtual machine. The migration renames all virtual disk, configuration, snapshot, and `.nvram` files. If the new names exceed the maximum filename length, the migration does not succeed.

Storage vMotion has several uses in administering virtual infrastructure, including the following examples of use.

- Storage maintenance and reconfiguration. You can use Storage vMotion to move virtual machines off a storage device to allow maintenance or reconfiguration of the storage device without virtual machine downtime.
- Redistributing storage load. You can use Storage vMotion to redistribute virtual machines or virtual disks to different storage volumes to balance capacity or improve performance.

Storage vMotion Requirements and Limitations

A virtual machine and its host must meet resource and configuration requirements for the virtual machine disks to be migrated with Storage vMotion.

Storage vMotion is subject to the following requirements and limitations:

- Virtual machine disks must be in persistent mode or be raw device mappings (RDMs). For virtual compatibility mode RDMs, you can migrate the mapping file or convert to thick-provisioned or thin-provisioned disks during migration if the destination is not an NFS datastore. If you convert the mapping file, a new virtual disk is created and the contents of the mapped LUN are copied to this disk. For physical compatibility mode RDMs, you can migrate the mapping file only.
- Migration of virtual machines during VMware Tools installation is not supported.
- Because VMFS3 datastores do not support large capacity virtual disks, you cannot move virtual disks greater than 2 TB from a VMFS5 datastore to a VMFS3 datastore.
- The host on which the virtual machine is running must have a license that includes Storage vMotion.
- ESXi 4.0 and later hosts do not require vMotion configuration to perform migration with Storage vMotion.
- The host on which the virtual machine is running must have access to both the source and target datastores.
- For limits on the number of simultaneous migrations with vMotion and Storage vMotion, see Limits on Simultaneous Migrations.

vCenter Server and Host Management Update 1 - VMware vSphere 7.0, page 103

Migrate a Powered Off or Suspended Virtual Machine

You can use cold migration to move a virtual machine and its associated disks from one datastore to another. The virtual machines are not required to be on shared storage.

Prerequisites

- Make sure that you are familiar with the requirements for cold migration. See Cold Migration.
- 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.

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.

---

1 If you change the storage of the virtual machine, enter the required details in the Select Storage page.

   a 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.

Selecting the type of storage is possible only if PMem or Hybrid storage types are available in the data center.

b Select the format for the virtual machine 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.

c 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.

d 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 from the list and click Next.
Store all virtual machine files in the same Storage DRS cluster.	1 Select a Storage DRS cluster. 2 (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. 3 Click Next.
Store virtual machine configuration files and disks in separate locations.	1 Click Configure per disk. Note You can use the Configure per disk option to downgrade from or upgrade to PMem storage. 2 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.
	3	(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.
	4	Click Next.

6 If you change the compute resource of the virtual machine, select destination networks for the virtual machine migration.

You can migrate a virtual machine network to another distributed switch in the same or to another data center or vCenter Server

Option	Action	
Select a destination network for all VM network adapters connected to a valid source network.	a	Click the arrow in the Destination Network column and select Browse.
	b	Select a destination network and click OK.
	c	Click Next.
Select a new destination network for each VM network adapter connected to a valid source network.	a	Click Advanced.
	b	Click the arrow in the Destination Network column and select Browse.
	c	Select a destination network and click OK.
	d	Click Next.

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

Results

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.

vCenter Server and Host Management Update 1 - VMware vSphere 7.0, page 129

Objective 7.11
Given a vSphere environment, identify how to use performance charts to monitor the environment

Performance Chart Types

Performance metrics are displayed in different types of charts, depending on the metric type and object.

Table 1-1. Performance Chart Types

Chart Type	Description
Line chart	Displays metrics for a single inventory object. The data for each performance counter is plotted on a separate line in the chart. For example, a network chart for a host can contain two lines: one showing the number of packets received, and one showing the number of packets transmitted.
Bar chart	Displays storage metrics for datastores in a selected data center. Each datastore is represented as a bar in the chart. Each bar displays metrics based on the file type: virtual disks, snapshots, swap files, and other files.
Pie chart	Displays storage metrics for a single object, based on the file types, or virtual machines. For example, a pie chart for a datastore can display the amount of storage space occupied by the virtual machines taking up the largest space.

Stacked chart	Displays metrics for the child objects that have the highest statistical values. All other objects are aggregated, and the sum value is displayed with the term Other. For example, a host's stacked CPU usage chart displays CPU usage metrics for the 10 virtual machines on the host that are consuming the most CPU. The Other amount contains the total CPU usage of the remaining virtual machines. The metrics for the host itself are displayed in separate line charts. Stacked charts are useful in comparing the resource allocation and usage across multiple hosts or virtual machines. By default, the 10 child objects with the highest data counter values are displayed.

vSphere Monitoring and Performance Update 1 – Vmware vSphere 7.0, page 10

View Performance Charts

The vCenter Server statistics settings, the type of object selected, and the features that are enabled on the selected object determine the amount of information displayed in charts. Charts are organized into views. You can select a view to see related data together on one screen. You can also specify the time range, or data collection interval. The duration extends from the selected time range to the present time.

Overview charts display multiple data sets in one panel to evaluate different resource statistics, display thumbnail charts for child objects. It also displays charts for a parent and a child object. Advanced charts display more information than overview charts, are configurable, and can be printed or exported. You can export data in the PNG, JPEG, or CSV formats. See #unique_10.

Procedure

1 Select a valid inventory object in the vSphere Client.

   Overview and advanced performance charts are available for datacenter, cluster, host, resource pool, vApp, and virtual machine objects. Overview charts are also available for datastores and datastore clusters. Performance charts are not available for network objects.

2 Click the Monitor tab, and click Performance.

3 Select a view.

   Available views depend on the type of object. For views that might contain many charts in a large environment, the vSphere Client displays the charts distributed on multiple pages. You can use the arrow buttons to navigate between pages.

4 Select a predefined or custom time range.

Performance Charts Options Available Under the View Menu

The performance chart options that you can access under the View menu vary depending on the type of inventory object you select.

For example, the Virtual Machines view is available when you view host performance charts only if there are virtual machines on the selected host. Likewise, the Fault Tolerance view for virtual machine performance charts is available only when that feature is enabled for the selected virtual machine.

Table 1-6. Performance Chart Views by Inventory Object

Object	View List Items
Data center	• Storage - space utilization charts for datastores in the data center, including space by file type and storage space used by each datastore in the data center. • Clusters - thumbnail CPU and memory charts for each cluster, and stacked

	charts for total CPU and memory usage in the data center. This view is the default.

Datastore and datastore cluster	• Space - space utilization charts for the datastore:space utilization by file type
	  • space utilization by virtual machine
	  • space usage
	• Performance - performance charts for the datastore or datastore cluster and for virtual machine disks on the resource.
	Note The Performance view for datastores is only available when all hosts that are connected to the datastores are ESX/ESXi 4.1 or greater. The Performance view for datastore clusters is only available when the Storage DRS is enabled.

Cluster	• Home - CPU and memory charts for the cluster. • Resource Pools & Virtual Machines - thumbnail charts for resource pools and virtual machines, and stacked charts for total CPU and memory usage in the cluster. • Hosts - thumbnail charts for each host in the cluster, and stacked charts for total CPU, memory, disk usage, and network usage.
Host	• Home - CPU, memory, disk, and network charts for the host. • Virtual Machines - thumbnail charts for virtual machines, and stacked charts for total CPU usage and total memory usage on the host.
Resource Pool and vApps	• Home - CPU and memory charts for the resource pool. • Resource Pools & Virtual Machines - thumbnail charts for resource pools, and virtual machines and stacked charts for CPU and memory usage in the resource pool or vApp.
Virtual Machine	• Storage - space utilization charts for the virtual machine: space by file type, space by datastore, and total gigabytes. • Fault Tolerance - CPU and memory charts that display comparative metrics for the fault-tolerant primary and secondary virtual machines. • Home - CPU, memory, network, host (thumbnail charts), and disk usage charts for the virtual machine.

vSphere Monitoring and Performance Update 1 – Vmware vSphere 7.0, page 17

Objective 7.12
Identify the purpose for VMware Tools.

Introduction to VMware Tools

VMware Tools is a set of services and modules that enable several features in VMware products for better management of, and seamless user interactions with, guests operating systems.

- For example, VMware Tools has the ability to:
- Pass messages from the host operating system to the guest operating system.
- Customize guest operating systems as a part of the vCenter Server and other VMware products.
- Run scripts that help automate guest operating system operations. The scripts run when the power state of the virtual machine changes.
- Synchronize the time in the guest operating system with the time on the host operating system

VMware Tools Lifecycle Management provides a simplified and scalable approach for installation and upgrade of VMware Tools. It includes a number of feature enhancements,

driver-related enhancements, and support for new guest operating systems. Run the latest version of VMware Tools or use open-vm-tools distributed with the Linux OS distribution. Although a guest operating system can run without VMware Tools, always run the latest version of VMware Tools in your guest operating systems to access the latest features and updates. You can configure your virtual machine to automatically check for and apply VMware Tools upgrades each time you power on your virtual machines. For information about enabling automatic upgrade of VMware Tools on your virtual machines, see *vSphere Virtual Machine Administration Guide*

This chapter includes the following topics:

- VMware Tools Services
- VMware Tools Lifecycle Management
- VMware Tools Device Drivers
- VMware User Process
- Using Open VM Tools
- Operating System Specific Packages for Linux Guest Operating Systems

VMware Tools User Guide – Vmware Tools 11.1.0, page 7