Valerio Passeri

VMware Certified Technical Associate (VCTA)
Unofficial Study Guide
Exam 1V0-21.20

Version 2.0

Introduction

I created this Unofficial Study Guide as a mean to achieve the required preparation for exam 1V0-21.20, in the absence (but NOT as a substitute) of an Official Guide.
I started from the VMware 1V0-21.10 Exam Preparation Guide. From the references listed in it, I extracted the study material that I consider relevant for every exam objective. Consequently, this document uses the same layout that VMware applied to the topics for exam 1V0-21.20: three sections and from 5 to 18 exam objectives for each section.

I hope that this Guide will be useful to anyone that will use it in preparing to achieve the VCTA certification. Good luck on your exam!

Also…

Whether you're reading this document to prepare yourself for the exam or to become a VMware engineer, I strongly suggest you to take a look at this:

Aleksandra Todorovska is a VCTA/VCP-DCV certified VMware engineer, as well as an authentic and genuine virtualization enthusiast. She published a revised version of this Unofficial Study Guide, which is the closest thing to a hands-on VCTA lab manual I have seen so far. If you want to practice for the VCTA exam, before taking the real test, these are the "links to go":

Aleksandra Todorovska on LinkedIn – https://www.linkedin.com/in/alexandra-todorovska
Aleksandra's Blog - https://aleksandra-todorovska.medium.com
Alexandra's VCTA Unoffical Study Guide -
https://www.dropbox.com/s/sg9k4rtwev4mdv2/Vcta%202022%20Guide.pdf?dl=0

Disclaimer

In this Study Guide, all content associated to each exam 1V0-21.20 objective is protected by copyright, and the copyright owner is VMware Inc.: any other content is intellectual property of the author of this document.

As its name suggests, this is an UNOFFICIAL Study Guide for exam 1V0-21.20. It is NOT recognized and/or endorsed as an Official Study Guide by VMware, and is NOT to be considered and/or used as such by anyone else. It is just an attempt to summarize all documentation related to exam 1V0-21.20 topics, and to collect the concepts required by each exam objective, to create a document which MUST be considered and/or used by anyone as an OPTIONAL Study Guide in addition to any other Official Study Curriculum.

Studying on this Study Guide may help in passing exam 1V0-21.20, but the use of this Study Guide DOES NOT guarantee the achieving of VCTA certification. Given this, NEITHER this Study Guide or its author can be considered responsible for any outcome of any exam 1V0-21.20 session taken by anyone who studied on this document.

As well as VMware documentation is FREE to anyone who wants access to it, this Study Guide is FREE, is NOT a commercial project, and MUST be made available to anyone WITHOUT any charge.

In addition to being an UNOFFICIAL Study Guide, this document is NOT an exhaustive preparation tool for exam 1V0-21.20. Anyone can contribute to it: each contribution is FOR FREE, does NOT imply any right to anyone, and is subject to the author's discretion. If you want to contribute, contact me at my e-mail address:

v_passeri@alice.it

Thank you.

Valerio Passeri

Section 1 - Architecture and Technologies

Section 4 - Installing, Configuring, and Setup

Section 7 - Administrative and Operational Tasks

Section 1
Architecture and Technologies

Objective 1.1 - Identify how physical resources are presented to multiple virtual machines.

Objective 1.2 - Identify how virtual resources can be shared across multiple virtual machines.

Objective 1.3 - Identify examples of type 1 and type 2 hypervisors.

Objective 1.4 - Identify business challenges addressed by vSphere.

Objective 1.5 - Identify the components of a vSphere environment.

Objective 1.6 - Identify vSphere virtual networking components and types.

Objective 1.7 - Identify the characteristics of storage access protocols for vSphere.

Objective 1.8 - Identify the characteristics of vSphere storage technologies.

Objective 1.9 - Identify the purposes of different virtual machine files.

Objective 1.10 - Identify the types of OS that can run on virtual machines.

Objective 1.11 - Identify use cases for virtual machine snapshots, cloning and templates.

Objective 1.12 - Identify the functionality of vSphere vMotion and Storage vMotion technology.

Objective 1.13 - Identify use cases for virtual machine snapshots, cloning and templates.

Objective 1.14 - Identify the characteristics of vSphere High Availability and Fault Tolerance.

Objective 1.15 - Identify use cases of High Availability and Disaster Recovery.

Objective 1.16 - Identify the functionality of VMware Distributed Resource Scheduler.

Objective 1.17 - Given a DRS score, identify the meaning.

Objective 1.18 - Identify use cases for Enhanced vMotion Compatibility (EVC).

Objective 1.1
Identify how physical resources are presented to multiple virtual machines.

vCenter Server and Host Management - VMware vSphere 7.0 Update 1, page 10

Virtualization Basics

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. The hypervisor serves as a platform for running virtual machines and allows for the consolidation of computing resources.

Each virtual machine contains its own virtual, or software-based, hardware, including a virtual CPU, memory, hard disk, and network interface card.

ESXi is the hypervisor in a vSphere environment. The hypervisor is installed on physical or virtual hardware in a virtualized data center, and acts as a platform for virtual machines. The hypervisor provides physical hardware resources dynamically to virtual machines to support the operation of the virtual machines. The hypervisor allows virtual machines to operate with a degree of independence from the underlying physical hardware. For example, a virtual machine can be moved from one physical host to another, or its virtual disks can be moved from one type of storage to another, without affecting the functioning of the virtual machine.

Because virtual machines are decoupled from the underlying physical hardware, virtualization allows you to consolidate physical computing resources such as CPUs, memory, storage, and networking into pools of resources. These resources can be dynamically and flexibly made available to virtual machines. With the vCenter Server management platform, you can increase the availability and security of your virtual infrastructure.

Objective 1.2
Identify how virtual resources can be shared across multiple virtual machines.

vSphere Resource Management Update 1 – Vmware vSphere 7.0, page 11

Resource Types

Resources include CPU, memory, power, storage, and network resources.

Note ESXi manages network bandwidth and disk resources on a per-host basis, using network traffic shaping and a proportional share mechanism, respectively.

Resource Providers

Hosts and clusters, including datastore clusters, are providers of physical resources.

For hosts, available resources are the host's hardware specification, minus the resources used by the virtualization software.

A cluster is a group of hosts. You can create a cluster using vSphere Client, and add multiple hosts to the cluster. vCenter Server manages these hosts' resources jointly: the cluster owns all of the CPU and memory of all hosts. You can enable the cluster for joint load balancing or failover. See Chapter 11 Creating a DRS Cluster for more information.

A datastore cluster is a group of datastores. Like DRS clusters, you can create a datastore cluster using the vSphere Client, and add multiple datastores to the cluster. vCenter Server manages the datastore resources jointly. You can enable Storage DRS to balance I/O load and space utilization. See Chapter 14 Creating a Datastore Cluster.

Resource Consumers

Virtual machines are resource consumers.

The default resource settings assigned during creation work well for most machines. You can later edit the virtual machine settings to allocate a share-based percentage of the total CPU, memory, and storage I/O of the resource provider or a guaranteed reservation of CPU and memory. When you power on that virtual machine, the server checks whether enough unreserved resources are available and allows power on only if there are enough resources. This process is called admission control.

A resource pool is a logical abstraction for flexible management of resources. Resource pools can be grouped into hierarchies and used to hierarchically partition available CPU and memory resources. Accordingly, resource pools can be considered both resource providers and consumers. They provide resources to child resource pools and virtual machines, but are also resource consumers because they consume their parents' resources. See Chapter 10 Managing Resource Pools.

ESXi hosts allocate each virtual machine a portion of the underlying hardware resources based on a number of factors:

- Resource limits defined by the user.
- Total available resources for the ESXi host (or the cluster).
- Number of virtual machines powered on and resource usage by those virtual machines.
- Overhead required to manage the virtualization.

Goals of Resource Management

When managing your resources, you must be aware of what your goals are.

In addition to resolving resource overcommitment, resource management can help you accomplish the following:

- Performance Isolation: Prevent virtual machines from monopolizing resources and guarantee predictable service rates.
- Efficient Usage: Exploit undercommitted resources and overcommit with graceful degradation.
- Easy Administration: Control the relative importance of virtual machines, provide flexible dynamic partitioning, and meet absolute service-level agreements.

Objective 1.3
Identify examples of type 1 and type 2 hypervisors.

https://www.vmware.com/topics/glossary/content/hypervisor

What is a hypervisor?

A hypervisor, also known as a virtual machine monitor or VMM, is software that creates and runs virtual machines (VMs). A hypervisor allows one host computer to support multiple guest VMs by virtually sharing its resources, such as memory and processing.

Why use a hypervisor?

Hypervisors make it possible to use more of a system's available resources and provide greater IT mobility since the guest VMs are independent of the host hardware. This means they can be easily moved between different servers. Because multiple virtual machines can run off of one physical server with a hypervisor, a hypervisor reduces:

- Space
- Energy
- Maintenance requirements

Types of hypervisors

There are two main hypervisor types, referred to as "Type 1" (or "bare metal") and "Type 2" (or "hosted"). A type 1 hypervisor acts like a lightweight operating system and runs directly on the host's hardware, while a type 2 hypervisor runs as a software layer on an operating system, like other computer programs.

The most commonly deployed type of hypervisor is the type 1 or bare-metal hypervisor, where virtualization software is installed directly on the hardware where the operating system is normally installed. Because bare-metal hypervisors are isolated from the attack-prone operating system, they are extremely secure. In addition, they generally perform better and more efficiently than hosted hypervisors. For these reasons, most enterprise companies choose bare-metal hypervisors for data center computing needs.

While bare-metal hypervisors run directly on the computing hardware, hosted hypervisors run on top of the operating system (OS) of the host machine. Although hosted hypervisors run within the OS, additional (and different) operating systems can be installed on top of the hypervisor. The downside of hosted hypervisors is that latency is higher than bare-metal hypervisors. This is because communication between the hardware and the hypervisor must pass through the extra layer of the OS. Hosted hypervisors are sometimes known as client hypervisors because they are most often used with end users and software testing, where higher latency is less of a concern.

Hardware acceleration technology can create and manage virtual resources faster by boosting processing speed for both bare-metal and hosted hypervisors. A type of hardware accelerator known as a virtual Dedicated Graphics Accelerator (vDGA) takes care of sending and refreshing high-end 3-D graphics. This frees up the main system for other tasks and greatly increases the display speed of images. For industries such as oil and gas exploration, where there is a need to quickly visualize complex data, this technology can be very useful.

Both types of hypervisors can run multiple virtual servers for multiple tenants on one physical machine. Public cloud service providers lease server space on the different virtual servers to different companies. One server might host several virtual servers that are all running workloads for different companies. This type of resource sharing can result in a “noisy neighbor” effect, when one of the tenants runs a large workload that interferes with the server performance for other tenants. It also poses more of a security risk than using a dedicated bare-metal server.

A bare-metal server that a single company has full control over will always provide higher performance than a virtual server that is sharing a physical server’s bandwidth, memory and processing power with other virtual servers. The hardware for bare-metal servers can also be optimized to increase performance, which is not the case with shared public servers. Businesses that need to comply with regulations that require physical separation of resources will need to use their own bare-metal servers that do not share resources with other tenants.

What is a cloud hypervisor?

As cloud computing becomes pervasive, the hypervisor has emerged as an invaluable tool for running virtual machines and driving innovation in a cloud environment. Since a hypervisor is a software layer that enables one host computer to simultaneously support multiple VMs, hypervisors are a key element of the technology that makes cloud computing possible. Hypervisors make cloud-based applications available to users across a virtual environment while still enabling IT to maintain control over a cloud environment’s infrastructure, applications and sensitive data.

Digital transformation and rising customer expectations are driving greater reliance on innovative applications. In response, many enterprises are migrating their virtual machines to the cloud. However, having to rewrite every existing application for the cloud can consume precious IT resources and lead to infrastructure silos. Fortunately, as an integral part of a virtualization platform, a hypervisor can help migrate applications to the cloud quickly. As a result, enterprises can reap the cloud’s many benefits, including reduced hardware expenditures, increased accessibility and greater scalability, for a faster return on investment.

How does a hypervisor work?

Hypervisors support the creation and management of virtual machines (VMs) by abstracting a computer’s software from its hardware. Hypervisors make virtualization possible by translating requests between the physical and virtual resources. Bare-metal hypervisors are sometimes embedded into the firmware at the same level as the motherboard basic input/output system (BIOS) to enable the operating system on a computer to access and use virtualization software.

Benefits of hypervisors

There are several benefits to using a hypervisor that hosts multiple virtual machines:

- Speed: Hypervisors allow virtual machines to be created instantly, unlike bare-metal servers. This makes it easier to provision resources as needed for dynamic workloads.
- Efficiency: Hypervisors that run several virtual machines on one physical machine’s resources also allow for more efficient utilization of one physical server. It is more cost- and energy-efficient to run several virtual machines on one physical machine than to run multiple underutilized physical machines for the same task.

- Flexibility: Bare-metal hypervisors allow operating systems and their associated applications to run on a variety of hardware types because the hypervisor separates the OS from the underlying hardware, so the software no longer relies on specific hardware devices or drivers.
- Portability: Hypervisors allow multiple operating systems to reside on the same physical server (host machine). Because the virtual machines that the hypervisor runs are independent from the physical machine, they are portable. IT teams can shift workloads and allocate networking, memory, storage and processing resources across multiple servers as needed, moving from machine to machine or platform to platform. When an application needs more processing power, the virtualization software allows it to seamlessly access additional machines.

Container vs hypervisor

Containers and hypervisors are both involved in making applications faster and more efficient, but they achieve this in different ways.

Hypervisors:

- Allow an operating system to run independently from the underlying hardware through the use of virtual machines.
- Share virtual computing, storage and memory resources.
- Can run multiple operating systems on top of one server (bare-metal hypervisor) or installed on top of one standard operating system and isolated from it (hosted hypervisor).

Containers:

- Allow applications to run independently of an operating system.
- Can run on any operating system—all they need is a container engine to run.
- Are extremely portable since in a container, an application has everything it needs to run.

Hypervisors and containers are used for different purposes. Hypervisors are used to create and run virtual machines (VMs), which each have their own complete operating systems, securely isolated from the others. In contrast to VMs, containers package up just an app and its related services. This makes them more lightweight and portable than VMs, so they are often used for fast and flexible application development and movement.

Objective 1.4
Identify business challenges addressed by vSphere.

vSphere Availability –Vmware vSphere 7.0 Update 1, page 7

Reducing Planned Downtime

Planned downtime typically accounts for over 80% of data center downtime. Hardware maintenance, server migration, and firmware updates all require downtime for physical servers. To minimize the impact of this downtime, organizations are forced to delay maintenance until inconvenient and difficult-to-schedule downtime windows.

vSphere makes it possible for organizations to dramatically reduce planned downtime. Because workloads in a vSphere environment can be dynamically moved to different physical servers without downtime or service interruption, server maintenance can be performed without requiring application and service downtime. With vSphere, organizations can:

- Eliminate downtime for common maintenance operations.
- Eliminate planned maintenance windows.
- Perform maintenance at any time without disrupting users and services.

The vSphere vMotion® and Storage vMotion functionality in vSphere makes it possible for organizations to reduce planned downtime because workloads in a VMware environment can be dynamically moved to different physical servers or to different underlying storage without service interruption. Administrators can perform faster and completely transparent maintenance operations, without being forced to schedule inconvenient maintenance windows.

Preventing Unplanned Downtime

While an ESXi host provides a robust platform for running applications, an organization must also protect itself from unplanned downtime caused from hardware or application failures. vSphere builds important capabilities into data center infrastructure that can help you prevent unplanned downtime.

These vSphere capabilities are part of virtual infrastructure and are transparent to the operating system and applications running in virtual machines. These features can be configured and utilized by all the virtual machines on a physical system, reducing the cost and complexity of providing higher availability. Key availability capabilities are built into vSphere:

- Shared storage. Eliminate single points of failure by storing virtual machine files on shared storage, such as Fibre Channel or iSCSI SAN, or NAS. The use of SAN mirroring and replication features can be used to keep updated copies of virtual disk at disaster recovery sites.
- Network interface teaming. Provide tolerance of individual network card failures.
- Storage multipathing. Tolerate storage path failures.

In addition to these capabilities, the vSphere HA and Fault Tolerance features can minimize or eliminate unplanned downtime by providing rapid recovery from outages and continuous availability, respectively.

vSphere HA Provides Rapid Recovery from Outages

vSphere HA leverages multiple ESXi hosts configured as a cluster to provide rapid recovery from outages and cost-effective high availability for applications running in virtual machines.

vSphere HA protects application availability in the following ways:

- It protects against a server failure by restarting the virtual machines on other hosts within the cluster.
- It protects against application failure by continuously monitoring a virtual machine and resetting it in the event that a failure is detected.
- It protects against datastore accessibility failures by restarting affected virtual machines on other hosts which still have access to their datastores.
- It protects virtual machines against network isolation by restarting them if their host becomes isolated on the management or vSAN network. This protection is provided even if the network has become partitioned.

Unlike other clustering solutions, vSphere HA provides the infrastructure to protect all workloads with the infrastructure:

- You do not need to install special software within the application or virtual machine. All workloads are protected by vSphere HA. After vSphere HA is configured, no actions are required to protect new virtual machines. They are automatically protected.
- You can combine vSphere HA with vSphere Distributed Resource Scheduler (DRS) to protect against failures and to provide load balancing across the hosts within a cluster.

vSphere HA has several advantages over traditional failover solutions:

Minimal setup

After a vSphere HA cluster is set up, all virtual machines in the cluster get failover support without additional configuration.

Reduced hardware cost and setup

The virtual machine acts as a portable container for the applications and it can be moved among hosts. Administrators avoid duplicate configurations on multiple machines. When you use vSphere HA, you must have sufficient resources to fail over the number of hosts you want to protect with vSphere HA. However, the VMware vCenter Server® system automatically manages resources and configures clusters.

Increased application availability

Any application running inside a virtual machine has access to increased availability. Because the virtual machine can recover from hardware failure, all applications that start at boot have increased availability without increased computing needs, even if the application is not itself a clustered application. By monitoring and responding to VMware Tools heartbeats and restarting nonresponsive virtual machines, it protects against guest operating system crashes.

DRS and vMotion integration

> If a host fails and virtual machines are restarted on other hosts, DRS can provide migration recommendations or migrate virtual machines for balanced resource allocation. If one or both of the source and destination hosts of a migration fail, vSphere HA can help recover from that failure.

vSphere Fault Tolerance Provides Continuous Availability

vSphere HA provides a base level of protection for your virtual machines by restarting virtual machines in the event of a host failure. vSphere Fault Tolerance provides a higher level of availability, allowing users to protect any virtual machine from a host failure with no loss of data, transactions, or connections.

Fault Tolerance provides continuous availability by ensuring that the states of the Primary and Secondary VMs are identical at any point in the instruction execution of the virtual machine.
If either the host running the Primary VM or the host running the Secondary VM fails, an immediate and transparent failover occurs. The functioning ESXi host seamlessly becomes the Primary VM host without losing network connections or in-progress transactions. With transparent failover, there is no data loss and network connections are maintained. After a transparent failover occurs, a new Secondary VM is respawned and redundancy is re-established. The entire process is transparent and fully automated and occurs even if vCenter Server is unavailable.

Protecting vCenter Server with vCenter High Availability

vCenter High Availability (vCenter HA) protects not only against host and hardware failures but also against vCenter Server application failures. Using automated failover from active to passive, vCenter HA supports high availability with minimal downtime.

Option	Description
Automatic	The automatic option clones the Active node to the Passive node and witness node, and configures the nodes for you. If your environment meets the following requirements, you can use this option. • The vCenter Server that becomes the Active node is managing its own ESXi host and its own virtual machine. This configuration is sometimes called a self-managed vCenter Server.
Manual	The manual option offers more flexibility. You can use this option provided that your environment meets hardware and software requirements. If you select this option, you are responsible for cloning the Active node to the Passive node and the Witness node. You must also perform some networking configuration.

Protecting vCenter Server with VMware Service Lifecycle Manager

Availability of vCenter Server is provided by VMware Service Lifecycle Manager.

If a vCenter service fails, VMware Service Lifecycle Manager restarts it. VMware Service Lifecycle Manager monitors the health of services and it takes preconfigured remediation action when it detects a failure. Service does not restart if multiple attempts to remediate fail.

Objective 1.5
Identify the components of a vSphere environment.

vCenter Server and Host Management Update 1 - VMware vSphere 7.0, page 12

vSphere Software Components

VMware vSphere is a suite of software components for virtualization. These include ESXi, vCenter Server, and other software components that fulfill several different functions in the vSphere environment.

vSphere includes the following software components:

ESXi

The hypervisor runs virtual machines. Each virtual machine has a set of configuration and disk files that together perform all the functions of a physical machine.

Through ESXi, you run the virtual machines, install operating systems, run applications, and configure the virtual machines. Configuration includes identifying the virtual machine's resources, such as storage devices.

The server provides bootstrapping, management, and other services that manage your virtual machines.

vCenter Server

A service that acts as a central administrator for VMware ESXi hosts that are connected on a network. vCenter Server directs actions on the virtual machines and the ESXi hosts.

vCenter Server is installed to run automatically on a preconfigured virtual machine. The vCenter Server service runs continuously in the background. It performs its monitoring and managing activities even when no vSphere Clients are connected and when no one is logged on to the computer where it resides. It must have network access to all the hosts it manages.

vCenter Server is deployed as a preconfigured virtual machine optimized for running vCenter Server and the vCenter Server components. You can deploy vCenter Server on ESXi hosts 6.5 or later.

All prerequisite services for running vCenter Server and the vCenter Server components are bundled in the vCenter Server installation. All vCenter Server services run as child processes of the VMware Service Library Lifecycle Manager service. See the *vCenter Server Installation and Setup* documentation for details about setting up this configuration.

vCenter Single Sign-On

A service that is part of the vCenter Server management infrastructure. The vCenter Single Sign-On authentication service makes the VMware cloud infrastructure platform more secure by allowing the various vSphere software components to communicate with each other. The vCenter Single Sign-On authentication service uses a secure token exchange mechanism instead of requiring each component to authenticate a user separately with a directory service like Active Directory.

When you install vCenter Single Sign-On, the following components are deployed.

STS (Security Token Service)

STS certificates enable a user who has logged on through vCenter Single Sign-On to authenticate to any vCenter service that vCenter Single Sign-On supports. The STS service issues Security Assertion Markup Language (SAML) tokens. These security tokens represent the identity of a user in each of the vCenter Single Sign-On identity sources.

Administration server

The administration server allows users with vCenter Single Sign-On administrator privileges to configure the vCenter Single Sign-On service and manage users and groups from the vSphere Client. Initially, only the user administrator@vsphere.local has these privileges.

vCenter Lookup Service

vCenter Lookup Service contains topology information about the vSphere infrastructure, enabling vSphere components to connect to each other securely. Unless you are using Simple Install, you are prompted for the Lookup Service URL when you install other vSphere components. For example, the Inventory Service and the vCenter Server installers ask for the Lookup Service URL and then contact the Lookup Service to find vCenter Single Sign-On. After installation, the Inventory Service and vCenter Server system are registered with the vCenter Lookup Service so other vSphere components, like the vSphere Client, can find them.

VMware Directory Service

Directory service associated with the vsphere.local domain. This service is a multi-tenanted, peer-replicating directory service that makes an LDAP directory available on port 389. In multisite mode, an update of VMware Directory Service content in one VMware Directory Service instance results in the automatic update of the VMware Directory Service instances associated with all other vCenter Single Sign-On nodes.

vCenter Server plug-ins

Applications that provide additional features and functionality to vCenter Server. Typically, plug-ins consist of a server component and a client component. After the plug-in server is installed, it is registered with vCenter Server and the plug-in client is available to the vSphere Client for download. After a plug-in is installed on the vSphere Client, it might alter the interface by adding views, tabs, toolbar buttons, or menu items related to the added functionality.

Plug-ins leverage core vCenter Server capabilities, such as authentication and permission management, but can have their own types of events, tasks, metadata, and privileges.

Some vCenter Server features are implemented as plug-ins, and can be managed using the vSphere Client Plug-in Manager. These features include vCenter Storage Monitoring, vCenter Hardware Status, and vCenter Service Status.

vCenter Server database

Persistent storage for maintaining the status of each virtual machine, host, and user managed in the vCenter Server environment. The vCenter Server database can be remote or local to the vCenter Server system.

The database is installed and configured during vCenter Server installation.

If you are accessing your ESXi host directly through the VMware Host Client, and not through a vCenter Server system and associated vSphere Client, you do not use a vCenter Server database.

tcServer

Many vCenter Server functions are implemented as web services that require the tcServer. The tcServer is installed on the vCenter Server machine as part of the vCenter Server installation.

Features that require the tcServer to be running include: ICIM/Hardware Status tab, Performance charts, WebAccess, Storage Policy-Based services, and vCenter Service status.

vCenter Server agent

On each managed host, the software that collects, communicates, and runs the actions received from vCenter Server. The vCenter Server agent is installed the first time any host is added to the vCenter Server inventory.

Host agent

On each managed host, the software that collects, communicates, and runs the actions received through the vSphere Client. It is installed as part of the ESXi installation.

Objective 1.6
Identify vSphere virtual networking components and types.

vSphere Networking Update 1 - VMware vSphere 7.0, page 13

Networking Concepts Overview

A few concepts are essential for a thorough understanding of virtual networking. If you are new to vSphere, it is helpful to review these concepts.

Physical Network

A network of physical machines that are connected so that they can send data to and receive data from each other. VMware ESXi runs on a physical machine.

Virtual Network

A network of virtual machines running on a physical machine that are connected logically to each other so that they can send data to and receive data from each other. Virtual machines can be connected to the virtual networks that you create when you add a network.

Opaque Network

An opaque network is a network created and managed by a separate entity outside of vSphere. For example, logical networks that are created and managed by VMware NSX® appear in vCenter Server as opaque networks of the type nsx.LogicalSwitch. You can choose an opaque network as the backing for a VM network adapter. To manage an opaque network, use the management tools associated with the opaque network, such as VMware NSX® Manager or the VMware NSX API management tools.

Physical Ethernet Switch

A physical ethernet switch manages network traffic between machines on the physical network. A switch has multiple ports, each of which can be connected to a single machine or another switch on the network. Each port can be configured to behave in certain ways depending on the needs of the machine connected to it. The switch learns which hosts are connected to which of its ports and uses that information to forward traffic to the correct physical machines. Switches are the core of a physical network. Multiple switches can be connected together to form larger networks.

vSphere Standard Switch

It works much like a physical Ethernet switch. It detects which virtual machines are logically connected to each of its virtual ports and uses that information to forward traffic to the correct virtual machines. A vSphere standard switch can be connected to physical switches by using physical Ethernet adapters, also referred to as uplink adapters, to join virtual networks with physical networks. This type of connection is similar to connecting physical switches together to create a larger network. Even though a vSphere standard switch works much like a physical switch, it does not have some of the advanced functionality of a physical switch.

vSphere Distributed Switch

A vSphere distributed switch acts as a single switch across all associated hosts in a data center to provide centralized provisioning, administration, and monitoring of virtual networks. You configure a vSphere distributed switch on the vCenter Server system and the configuration is propagated to all hosts that are associated with the switch. This lets virtual machines maintain consistent network configuration as they migrate across multiple hosts.

Host Proxy Switch

A hidden standard switch that resides on every host that is associated with a vSphere distributed switch. The host proxy switch replicates the networking configuration set on the vSphere distributed switch to the particular host.

Standard Port Group

Network services connect to standard switches through port groups. Port groups define how a connection is made through the switch to the network. Typically, a single standard switch is associated with one or more port groups. A port group specifies port configuration options such as bandwidth limitations and VLAN tagging policies for each member port.

Distributed Port

A port on a vSphere distributed switch that connects to a host's VMkernel or to a virtual machine's network adapter.

Distributed Port Group

A port group associated with a vSphere distributed switch that specifies port configuration options for each member port. Distributed port groups define how a connection is made through the vSphere distributed switch to the network.

NSX Distributed Port Group

A port group associated with a vSphere distributed switch that specifies port configuration options for each member port. To distinguish between vSphere distributed port groups and NSX port groups, in the vSphere Client the NSX virtual distributed switch, and its associated port group, is identified with the icon. NSX appears as an opaque network in vCenter Server, and you cannot configure NSX settings in vCenter Server. The NSX settings displayed are read only. You configure NSX distributed port groups using VMware NSX® Manager or the VMware NSX API management tools. To learn about configuring NSX, see the *NSX Data Center for vSphere* documentation.

NIC Teaming

NIC teaming occurs when multiple uplink adapters are associated with a single switch to form a team. A team can either share the load of traffic between physical and virtual networks among some or all of its members, or provide passive failover in the event of a hardware failure or a network outage.

VLAN

VLAN enable a single physical LAN segment to be further segmented so that groups of ports are isolated from one another as if they were on physically different segments. The standard is 802.1Q.

VMkernel TCP/IP Networking Layer

The VMkernel networking layer provides connectivity to hosts and handles the standard infrastructure traffic of vSphere vMotion, IP storage, Fault Tolerance, and vSAN.

IP Storage

Any form of storage that uses TCP/IP network communication as its foundation. iSCSI and NFS can be used as virtual machine datastores and for direct mounting of .ISO files, which are presented as CD-ROMs to virtual machines.

TCP Segmentation Offload

TCP Segmentation Offload, TSO, allows a TCP/IP stack to emit large frames (up to 64KB) even though the maximum transmission unit (MTU) of the interface is smaller. The network adapter then separates the large frame into MTU-sized frames and prepends an adjusted copy of the initial TCP/IP headers.

Network Services in ESXi

A virtual network provides several services to the host and virtual machines.

You can enable two types of network services in ESXi:

- Connecting virtual machines to the physical network and to each other.

- Connecting VMkernel services (such as NFS, iSCSI, or vMotion) to the physical network.

VMware ESXi Dump Collector Support

The ESXi Dump Collector sends the state of the VMkernel memory, that is, a core dump to a network server when the system encounters a critical failure.

The ESXi Dump Collector in ESXi supports both vSphere Standard and Distributed Switches. The ESXi Dump Collector can also use any active uplink adapter from the team of the port group that handles the VMkernel adapter for the collector.

Changes to the IP address for the ESXi Dump Collector interface are automatically updated if the IP addresses for the configured VMkernel adapter changes. The ESXi Dump Collector also adjusts its default gateway if the gateway configuration of the VMkernel adapter changes.

If you try to delete the VMkernel network adapter used by the ESXi Dump Collector, the operation fails and a warning message appears. To delete the VMkernel network adapter, disable dump collection and delete the adapter.

There is no authentication or encryption in the file transfer session from a crashed host to the ESXi Dump Collector. You should configure the ESXi Dump Collector on a separate VLAN when possible to isolate the ESXi core dump from regular network traffic.

For information about installing and configuring the ESXi Dump Collector, see the *vCenter Server Installation and Setup* documentation.

Objective 1.7
Identify the characteristics of storage access protocols for vSphere.

Storage Protocol Comparison White Paper - v 1 .0, page 4

Storage Protocol Comparison Table

	iSCSI	NFS	FIbre ChaNNel	FCoe
Description	iSCSI presents block devices to a VMware® ESXi™ host. Rather than accessing blocks from a local disk, I/O operations are carried out over a network using a block access protocol. In the case of iSCSI, remote blocks are accessed by encapsulating SCSI commands and data into TCP/IP packets. Support for iSCSI was introduced in VMware® ESX® 3.0 in 2006.	NFS presents file devices over a network to an ESXi host for mounting. The NFS server/array makes its local file systems available to ESXi hosts. ESXi hosts access the metadata and files on the NFS array/server, usinganRPC-based protocol. VMware currently implements NFSversion3over TCP/IP.Support for NFS was introduced in ESX 3.0in2006	Fibre Channel (FC) presents block devices similar to iSCSI. Again, I/O operations are carried out over a network, using a block access protocol. In FC, remote blocks are accessed by encapsulating SCSI commands and data into FC frames. FC is commonly deployed in the majority of mission-critical environments. It has been the only one of these four protocols supported on ESX since the beginning.	Fibre Channel over Ethernet (FCoE) also presents block devices, with I/O operations carried out over a network using a block access protocol. In this protocol, SCSI commands and data are encapsulated into Ethernet frames. FCoE has many of the same characteristics as FC, except that the transportisEthernet. VMware introduced support for hardware FCoEinvSphere4.x and software FCoE in VMware vSphere® 5.0 in2011.
Implementation Options	• Network adapter with iSCSI capabilities, using software iSCSI initiator and accessed using a VMkernel (vmknic) port. or: • Dependent hardware iSCSI initiator. or: • Independent hardware iSCSI initiator.	Standard network adapter, accessed using a VMkernel port (vmknic).	Requiresadedicated host bus adapter (HBA) (typically two, for redundancy and multipathing).	• Hardware converged network adapter (CNA). or: • Network adapter with FCoE capabilities, using software FCoE initiator.

Performance Considerations	iSCSI can run over a 1Gb or a 10Gb TCP/IP network. Multiple connections can be multiplexed into a single session, established between the initiator and target. VMware supports jumbo frames for iSCSI traffic, which can improve performance. Jumbo frames send payloads larger than 1,500. Support for jumbo frames with IP storage was introduced in ESX 4, but not on all initiators. (See VMware knowledge base articles 1007654 and 1009473.) iSCSI can introduce overhead on a host's CPU (encapsulating SCSI data into TCP/IP packets).	NFS can run over 1Gb or 10Gb TCP/IP networks. NFS also supports UDP, but the VMware implementation requires TCP. VMware supports jumbo frames for NFS traffic, which can improve performance in certain situations. Support for jumbo frames with IP storage was introduced in ESX 4. NFS can introduce overhead on a host's CPU (encapsulating file I/O into TCP/IP packets).	FC can run on 1Gb/2Gb/4Gb/8Gb and 16Gb HBAs, but 16Gb HBAs must be throttled to run at 8Gb in vSphere 5.0. Buffer-to-buffer credits and end-to- end credits throttle throughput to ensure a lossless network. This protocol typically affects a host's CPU the least, because HBAs (required for FC) handle most of the processing (encapsulation of SCSI data into FC frames).	This protocol requires 10Gb Ethernet. With FCoE, there is no IP encapsulation of the data as there is with NFS and iSCSI. This reduces some of the overhead/latency. FCoE is SCSI over Ethernet, not IP. This protocol also requires jumbo frames, because FC payloads are 2.2K in size and cannot be fragmented.
Load Balancing	VMware Pluggable Storage Architecture (PSA) provides a round-robin (RR) path selection policy (PSP) that distributes load across multiple paths to an iSCSI target. Better distribution of load with PSP_RR is achieved when multiple LUNs are accessed concurrently.	There is no load balancing per se on the current implementation of NFS, because there is only a single session. Aggregate bandwidth can be configured by creating multiple paths to the NAS array, accessing some datastores via one path and other datastores via another.	VMware Pluggable Storage Architecture (PSA) provides a round-robin (RR) path selection policy (PSP) that distributes load across multiple paths to an FC target. Better distribution of load with PSP_RR is achieved when multiple LUNs are accessed concurrently.	VMware Pluggable Storage Architecture (PSA) provides a round-robin (RR) path selection policy (PSP) that distributes load across multiple paths to an FCoE target. Better distribution of load with PSP_RR is achieved when multiple LUNs are accessed concurrenttly.

Resilience	VMware PSA implements failover via itsStorageArray Type Plug-in (SATP) forall supported iSCSI arrays. The preferredmethodto dothisforsoftware iSCSIiswith iSCSIbinding implemented, but it can beachievedby adding multiple targetson different subnets mappedto theiSCSI initiator.	Networkadapter teamingcanbe configuredsothatif one interface fails, another cantakeits place. However,this reliesona network failureandmight not beabletohandle error conditions occurring on the NFS array/server side.	VMware PSA implements failover via itsStorageArray Type Plug-in (SATP) forall supported FCarrays.	VMware PSA implements failover via itsStorageArray Type Plug-in (SATP) forall supported FCoE arrays.
Error Checking	iSCSIusesTCP,which resends dropped packets.	NFSusesTCP,which resends dropped packets.	FCisimplementedas a lossless network. Thisis achievedby throttling throughput attimesof congestion, using B2B and E2E credits.	FCoE requires a lossless network. Thisis achievedby the implementation ofa pauseframe mechanismattimes of congestion.
Security	iSCSIimplementsthe Challenge Handshake Authentication Protocol (CHAP) to ensure that initiators and targetstrust each other. VLANs orprivatenetworks are highly recommended, to isolate theiSCSI trafficfromother traffic types.	VLANs or private networksarehighly recommended, to isolate the NFS traffic fromother traffic types.	Some FC switches supporttheconcepts ofa VSAN,toisolate partsof thestorage infrastructure. VSANsare conceptually similar to VLANs. Zoning between hosts andFC targets alsooffers adegree ofisolation.	SomeFCoEswitches supporttheconcepts ofa VSAN,toisolate partsof thestorage infrastructure. Zoning between hosts and FCoE targetsalso offersa degree of isolation.
VMware vSphere Storage APIs – Array Integration (VAAI) Primitives	Although VMware vSphere® Storage APIs – Array Integration (VAAI) primitives can vary from array to array, iSCSI devices can benefit from the following full complement of block primitives: • Atomic test/set • Full copy • Block zero • Thin provisioning • UNMAP These primitives are built in to ESXi and require no additional software installed on the host.	Again, these vary from array to array. The following VAAI primitives are available on NFS devices: • Full copy (but only with cold migration—not with VMware vSphere® Storage vMotion®) • Preallocated space (WRITE_ZEROs) • Cloned offl d using native snapshots A plug-in from the storage array vendor is required for VAAI NAS.	Although VAAI primitives can vary from array to array, FC devices can benefit from the following full complement of block primitives: • Atomic test/set • Full copy • Block zero • Thin provisioning • UNMAP These primitives are built in to ESXi and require no additional software installed on the host.	Although VAAI primitives can vary from array to array, FCoE devices can benefit from the following full complement of block primitives: • Atomic test/set • Full copy • Block zero • Thin provisioning • UNMAP These primitives are built in to ESXi and require no additional software installed on the host.

ESXi Boot from SAN	Yes	No	Yes	Software FCoE – No Hardware FCoE (CNA) – Yes
RDM Support	Yes	No	Yes	Yes
Maximum Device Size	64TB	Refer to NAS array vendor or NAS server vendor for maximum supported datastore size. Theoretical size is much larger than 64TB but requires NAS vendor to support it.	64TB	64TB
Maximum Number of Devices	256	Default: 8 Maximum: 256	256	256

Protocol Direct to Virtual Machine	Yes, via in-guest iSCSI initiator.	Yes, via in-guest NFS client.	No, but FC devices can be mapped directly to the virtual machine with NPIV. This still requires prior RDM mapping to the virtual machine, and hardware must support NPIV (FC switch, HBA).	No
Storage vMotion Support	Yes	Yes	Yes	Yes
Storage DRS Support	Yes	Yes	Yes	Yes
Storage I/O Control Support	Yes, since vSphere 4.1.	Yes, since vSphere 5.0.	Yes, since vSphere 4.1.	Yes, since vSphere 4.1.

Virtualized MSCS Support	No. VMware does not support MSCS nodes built on virtual machines residing on iSCSI storage. However, the use of software iSCSI initiators within guest operating systems configured with MSCS, in any configuration supported by Microsoft, is transparent to ESXi hosts. There is no need for explicit support statements from VMware.	No. VMware does not support MSCS nodes built on virtual machines residing on NFS storage.	Yes. VMware supports MSCS nodes built on virtual machines residing on FC storage.	No. VMware does not support MSCS nodes built on virtual machines residing on FCoE storage.
Ease of Confi uration	Medium – Setting up the iSCSI initiator requires aptitude and the FDQN or IP address of the target, plus some configuration for initiator maps and LUN presentation on the array side. After the target has been discovered through a scan of the SAN, LUNs are available for	Easy – This requires only the IP or FQDN of the target, plus the mount point. Datastores appear immediately after the host has been granted access from the NFS array/server side.	Difficult – This involves zoning at the FC switch level and LUN masking at the array level after the zoning is complete. It is more complex to configure than IP storage. After the target has been discovered through a scan of the SAN, LUNs are available for datastores	Difficult – This involves zoning at the FCoE switch level and LUN masking at the array level after the zoning is complete. It is more complex to configure than IP storage. After the target has been discovered through a scan of the SAN, LUNs are available for
Advantages	No additional hardware is necessary. Can use existing networking hardware components and iSCSI driver from VMware, so it's inexpensive to implement. Well-known and well-understood protocol. Quite mature at this stage. Administrators with network skills should be able to implement. Can be troubleshooted with generic network tools such as Wireshark.	No additional hardware is necessary. Can use existing networking hardware components, so it's inexpensive to implement. Well-known and well-understood protocol. It also is very mature. Administrators with network skills should be able to implement. Can be troubleshooted with generic network tools such as Wireshark.	Well-known and well-understood protocol. Very mature and trusted. Found in majority of mission- critical environments.	Enables consolidation of storage and other traffic onto the same network via converged network adapter (CNA). Using Data Center Bridging Exchange (DCBX) protocol, FCoE has been made lossless even though it runs over Ethernet. DCBX does other things, such as enabling different traffic classes to run on the same network, but that is beyond the scope of this discussion.

Disadvantages	Inability to route with iSCSI binding implemented. Possible security issues because there is no built-in encryption, so care must be taken to isolate traffic (e.g., VLANs). Software iSCSI can cause additional CPU overhead on the ESX host. TCP can introduce latency for iSCSI.	Because there is only a single session per connection, configuring for maximum bandwidth across multiple paths requires some care and attention. No PSA multipathing. Same security concerns as with iSCSI, because everything is transferred in clear text, so care must be taken to isolate traffic (e.g., VLANs). NFS is still version 3, which does not have the multipathing or security features of NFS v4 or NFS v4.1. NFS can cause additional CPU overhead on the ESX host. TCP can introduce latency for NFS.	Still runs only at 8Gb, which is slower than other networks (16Gb throttled to run at 8Gb in vSphere 5.0). Requires dedicated HBA, FC switch, and FC-capable storage array, which makes an FC implementation somewhat more expensive. Additional management overhead (e.g., switch zoning) is required. Might prove harder to troubleshoot than other protocols.	Somewhat new and currently not quite as mature as other protocols. Requires a 10Gb lossless network infrastructure, which can be expensive. Cannot route between initiator and targets using native IP routing. Instead, it must use protocols such as FIP (FCoE Initialization Protocol). Might prove complex to troubleshoot/isolate issues, with network and storage traffic using the same pipe.

Objective 1.8
Identify the characteristics of vSphere storage technologies.

vSphere Storage - VMware vSphere 7.0, page 16

Traditional Storage Virtualization Models

Generally, storage virtualization refers to a logical abstraction of physical storage resources and capacities from virtual machines and their applications. ESXi provides host-level storage virtualization.

In vSphere environment, a traditional model is built around the following storage technologies and ESXi and vCenter Server virtualization functionalities.

Local and Networked Storage

In traditional storage environments, the ESXi storage management process starts with storage space that your storage administrator preallocates on different storage systems. ESXi supports local storage and networked storage.

See Types of Physical Storage.

Storage Area Networks

A storage area network (SAN) is a specialized high-speed network that connects computer systems, or ESXi hosts, to high-performance storage systems. ESXi can use Fibre Channel or iSCSI protocols to connect to storage systems.

See Chapter 3 Overview of Using ESXi with a SAN.

Fibre Channel

Fibre Channel (FC) is a storage protocol that the SAN uses to transfer data traffic from ESXi host servers to shared storage. The protocol packages SCSI commands into FC frames. To connect to the FC SAN, your host uses Fibre Channel host bus adapters (HBAs).

See Chapter 4 Using ESXi with Fibre Channel SAN.

Internet SCSI

Internet iSCSI (iSCSI) is a SAN transport that can use Ethernet connections between computer systems, or ESXi hosts, and high-performance storage systems. To connect to the storage systems, your hosts use hardware iSCSI adapters or software iSCSI initiators with standard network adapters.

See Chapter 10 Using ESXi with iSCSI SAN.

Storage Device or LUN

In the ESXi context, the terms device and LUN are used interchangeably. Typically, both terms mean a storage volume that is presented to the host from a block storage system and is available for formatting.

See Target and Device Representations and Chapter 14 Managing Storage Devices.

Virtual Disks

A virtual machine on an ESXi host uses a virtual disk to store its operating system, application files, and other data associated with its activities. Virtual disks are large physical files, or sets of files, that can be copied, moved, archived, and backed up as any other files. You can configure virtual machines with multiple virtual disks.
To access virtual disks, a virtual machine uses virtual SCSI controllers. These virtual controllers include BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS, and VMware Paravirtual. These controllers are the only types of SCSI controllers that a virtual machine can see and access.
Each virtual disk resides on a datastore that is deployed on physical storage. From the standpoint of the virtual machine, each virtual disk appears as if it were a SCSI drive connected to a SCSI controller. Whether the physical storage is accessed through storage or network adapters on the host is typically transparent to the VM guest operating system and applications.

VMware vSphere® VMFS

The datastores that you deploy on block storage devices use the native vSphere Virtual Machine File System (VMFS) format. It is a special high-performance file system format that is optimized for storing virtual machines.

See Understanding VMFS Datastores.

NFS

An NFS client built into ESXi uses the Network File System (NFS) protocol over TCP/IP to access an NFS volume that is located on a NAS server. The ESXi host can mount the volume and use it as an NFS datastore.

See Understanding Network File System Datastores.

Raw Device Mapping

In addition to virtual disks, vSphere offers a mechanism called raw device mapping (RDM). RDM is useful when a guest operating system inside a virtual machine requires direct access to a storage device. For information about RDMs, see Chapter 19 Raw Device Mapping.

Software-Defined Storage Models

In addition to abstracting underlying storage capacities from VMs, as traditional storage models do, software-defined storage abstracts storage capabilities.

With the software-defined storage model, a virtual machine becomes a unit of storage provisioning and can be managed through a flexible policy-based mechanism. The model involves the following vSphere technologies.

VMware vSphere® Virtual Volumes™ (vVols)

The vVols functionality changes the storage management paradigm from managing space inside datastores to managing abstract storage objects handled by storage arrays. With vVols, an individual virtual machine, not the datastore, becomes a unit of storage management. And storage hardware gains complete control over virtual disk content, layout, and management.

See Chapter 22 Working with VMware vSphere Virtual Volumes (vVols).

VMware vSAN

vSAN is a distributed layer of software that runs natively as a part of the hypervisor. vSAN aggregates local or direct-attached capacity devices of an ESXi host cluster and creates a single storage pool shared across all hosts in the vSAN cluster.

See *Administering VMware vSAN*.

Storage Policy Based Management

Storage Policy Based Management (SPBM) is a framework that provides a single control panel across various data services and storage solutions, including vSAN and vVols. Using storage policies, the framework aligns application demands of your virtual machines with capabilities provided by storage entities.

See Chapter 20 Storage Policy Based Management.

I/O Filters

I/O filters are software components that can be installed on ESXi hosts and can offer additional data services to virtual machines. Depending on implementation, the services might include replication, encryption, caching, and so on.

See Chapter 23 Filtering Virtual Machine I/O.

vSphere Storage APIs

Storage APIs is a family of APIs used by third-party hardware, software, and storage providers to develop components that enhance several vSphere features and solutions.

This Storage publication describes several Storage APIs that contribute to your storage environment. For information about other APIs from this family, including vSphere APIs - Data Protection, see the VMware website.

vSphere APIs for Storage Awareness

Also known as VASA, these APIs, either supplied by third-party vendors or offered by VMware, enable communications between vCenter Server and underlying storage. Through VASA, storage entities can inform vCenter Server about their configurations, capabilities, and storage health and events. In return, VASA can deliver VM storage requirements from vCenter Server to a storage entity and ensure that the storage layer meets the requirements.

VASA becomes essential when you work with vVols, vSAN, vSphere APIs for I/O Filtering (VAIO), and storage VM policies. See Chapter 21 Using Storage Providers.

vSphere APIs for Array Integration

These APIs, also known as VAAI, include the following components:

- Hardware Acceleration APIs. Help arrays to integrate with vSphere, so that vSphere can offload certain storage operations to the array. This integration significantly reduces CPU overhead on the host. See Chapter 24 Storage Hardware Acceleration.

- Array Thin Provisioning APIs. Help to monitor space use on thin-provisioned storage arrays to prevent out-of-space conditions, and to perform space reclamation. See ESXi and Array Thin Provisioning.

vSphere APIs for Multipathing

Known as the Pluggable Storage Architecture (PSA), these APIs allow storage partners to create and deliver multipathing and load-balancing plug-ins that are optimized for each array. Plug-ins communicate with storage arrays and determine the best path selection strategy to increase I/O performance and reliability from the ESXi host to the storage array. For more information, see Pluggable Storage Architecture and Path Management.

Objective 1.9
Identify the purposes of different virtual machine files.

vSphere Virtual Machine Administration Update 1 - VMware vSphere 7.0, page 11

Virtual Machine Files

A virtual machine consists of several files that are stored on a storage device. The key files are the configuration file, virtual disk file, NVRAM setting file, and log file. You configure virtual machine settings through the vSphere Client, ESXCLI, or the vSphere Web Services SDK.

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

Table 1-1. Virtual Machine Files

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

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

- A .hlog file is a log file that is used by vCenter Server to keep track of virtual machine files that must be removed after a certain operation completes.

- A .vmtx file is created when you convert a virtual machine to a template. The .vmtx file replaces the virtual machine configuration file (.vmx file).

Objective 1.10
Identify the types of OS that can run on virtual machines.

Guest Operating System Installation Guide - http://partnerweb.vmware.com/GOSIG/home.html

Supported Guest Operating Systems

VMware supports the following Windows, Linux, Unix, Macintosh, and other operating systems. Operating systems that are not listed are not supported.

To see which guest operating system customizations are supported for a particular version of vSphere or vCenter, see the Guest OS Customization Support Matrix.

Windows Operating Systems

- Windows
  - Windows Server 2019
  - Windows Server 2016
  - Windows 10
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows 8.1
  - Windows 8
  - Windows Server 2008 R2
  - Windows 7
  - Windows Server 2008
  - Windows Vista
  - Windows Server 2003
  - Windows XP
  - Windows 2000
  - Windows NT 4.0
  - Windows ME
  - Windows 98
  - Windows 95
  - MS-DOS 6.22 and Windows 3.1x

UNIX and Other Operating Systems

- eComStation
  - eComStation 2.x
  - eComStation 1.0

- FreeBSD
  - FreeBSD 12.x
  - FreeBSD 11.x
  - FreeBSD 10.x
  - FreeBSD 9.x
  - FreeBSD 8.x
  - FreeBSD 7.x
  - FreeBSD 6.x
  - FreeBSD 5.x
  - FreeBSD 4.x
- IBM OS/2 Warp
  - IBM OS/2 Warp 4.5.2
  - IBM OS/2 Warp 4.0
- Mac OS X Server
  - macOS 10.15
  - macOS 10.14
  - macOS 10.13
  - macOS 10.12
  - OS X 10.11
  - OS X 10.10
  - OS X 10.9
  - OS X 10.8
  - OS X 10.7
  - Mac OS X Server 10.6
  - Mac OS X Server 10.5
- Netware
  - Netware 6.5 Server
  - Netware 6.0 Server
  - Netware 5.1 Server
  - Netware 4.2 Server
- Solaris
  - Solaris 11
  - Solaris 10
  - Solaris 9
  - Solaris 8
- SCO
  - SCO OpenServer 5.0
  - SCO UnixWare 7.0

Linux Operating Systems

- Amazon Linux
    - Amazon Linux 2
- Asianux Server
    - Asianux Server 7.0
    - Asianux Server 4.0
    - Asianux Server 3.0
- CentOS
    - CentOS 8
    - CentOS 7
    - CentOS 6
    - CentOS 5
    - CentOS 4
- CoreOS
    - CoreOS
- Debian
    - Debian 10
    - Debian 9
    - Debian 8
    - Debian 7
    - Debian 6
    - Debian 5
    - Debian 4
- Fedora
    - Fedora 24 Desktop Edition
    - Fedora 23 Desktop Edition
    - Fedora 22 Desktop Edition
    - Fedora 21 Desktop Edition
    - Fedora 20 Desktop Edition
    - Fedora 19 Desktop Edition
    - Fedora 18 Desktop Edition
    - Fedora 17 Desktop Edition
    - Fedora 16 Desktop Edition
- Flatcar
    - Flatcar
- Mandrake
    - Mandrake Linux 10.x
    - Mandrake Linux 9.x
    - Mandrake Linux 8.x

- Mandriva
    - Mandriva Corporate 4
    - Mandriva Linux 2011
    - Mandriva Linux 2010
    - Mandriva Linux 2009
    - Mandriva Linux 2008
    - Mandriva Linux 2007
    - Mandriva Linux 2006
- NeoKylin
    - NeoKylin Linux Advanced Server 6
    - NeoKylin Linux Advanced Server 7
- Novell
    - Novell Linux Desktop 9
- openSUSE Linux
    - openSUSE Linux 13.x
    - openSUSE Linux 12.x
    - openSUSE Linux 11.x
    - openSUSE Linux 10.x
- Oracle Enterprise
    - Oracle Linux 8
    - Oracle Linux 7
    - Oracle Linux 6
    - Oracle Enterprise Linux 5
    - Oracle Enterprise Linux 4
- VMware Photon OS
    - VMware Photon OS
- Red Hat Enterprise Linux
    - Red Hat Enterprise Linux 8
    - Red Hat Enterprise Linux Atomic Host
    - Red Hat Enterprise Linux 7
    - Red Hat Enterprise Linux 6
    - Red Hat Enterprise Linux 5
    - Red Hat Enterprise Linux 4
    - Red Hat Enterprise Linux 3
    - Red Hat Enterprise Linux 2.1
- Red Hat Linux
    - Red Hat Linux 9.0
    - Red Hat Linux 8.0
    - Red Hat Linux 7.0
    - Red Hat Linux 6.2

- Sun Java Desktop System
  - Sun Java Desktop System 2
- SUSE Linux Enterprise
  - SUSE Linux Enterprise 15
  - SUSE Linux Enterprise 12
  - SUSE Linux Enterprise 11
  - SUSE Linux Enterprise 10
  - SUSE Linux Enterprise Server 9
  - SUSE Linux Enterprise Server 8
  - SUSE Linux Enterprise Server 7
- SUSE Linux
  - SUSE Linux 10.x
  - SUSE Linux 9.x
  - SUSE Linux 8.x
  - SUSE Linux 7.3
- Turbolinux
  - Turbolinux 11
  - Turbolinux 10
  - Turbolinux 8
  - Turbolinux 7
- Ubuntu
  - Ubuntu 20.04 LTS
  - Ubuntu 19.10
  - Ubuntu 19.04
  - Ubuntu 18.10
  - Ubuntu 18.04 LTS
  - Ubuntu 17.10
  - Ubuntu 17.04
  - Ubuntu 16.10
  - Ubuntu 16.04 LTS
  - Ubuntu 15.10
  - Ubuntu 15.04
  - Ubuntu 14.10
  - Ubuntu 14.04 LTS
  - Ubuntu 13.10
  - Ubuntu 13.04
  - Ubuntu 12.10
  - Ubuntu 12.04 LTS
  - Ubuntu 11.10
  - Ubuntu 11.04

  - Ubuntu 10.10
  - Ubuntu 10.04 LTS

Objective 1.11
Identify use cases for virtual machine snapshots, cloning and templates.

vSphere Virtual Machine Administration Update 1 - VMware vSphere 7.0, page 255

Using Snapshots To Manage Virtual Machines

Snapshots preserve the state and data of a virtual machine at the time you take the snapshot. When you take a snapshot of a virtual machine, an image of the virtual machine in a given state is copied and stored. Snapshots are useful when you want to revert repeatedly to a virtual machine state, but you do not want to create multiple virtual machines.

You can take multiple snapshots of a virtual machine to create restoration positions in a linear process. With multiple snapshots, you can save many positions to accommodate many kinds of work processes. Snapshots operate on individual virtual machines. Taking snapshots of multiple virtual machines, for example, taking a snapshot of a VM for each member of a team, requires that you take a separate snapshot of each team member's virtual machine.

Snapshots are useful as a short term solution for testing software with unknown or potentially harmful effects. For example, you can use a snapshot as a restoration point during a linear or iterative process, such as installing update packages, or during a branching process, such as installing different versions of a program. Using snapshots ensures that each installation begins from an identical baseline.

With snapshots, you can preserve a baseline before you change a virtual machine.

Several operations for creating and managing virtual machine snapshots and snapshot trees are available in the vSphere Client. These operations enable you to create snapshots, revert any snapshot in the snapshot hierarchy, delete snapshots, and more. You can create snapshot trees where you save the virtual machine state at any specific time so that you can revert that virtual machine state later. Each branch in a snapshot tree can have up to 32 snapshots.

A snapshot preserves the following information:

- Virtual machine settings. The virtual machine directory, which includes the disks added or changed after you take the snapshot.
- Power state. The virtual machine can be powered on, powered off, or suspended.
- Disk state. State of all the virtual machine's virtual disks.
- (Optional) Memory state. The contents of the virtual machine's memory.

The Snapshot Hierarchy

The vSphere Client presents the snapshot hierarchy as a tree with one or more branches. Snapshots in the hierarchy have parent to child relationships. In linear processes, each snapshot has one parent snapshot and one child snapshot, except for the last snapshot, which has no child snapshot. Each parent snapshot can have more than one child. You can revert to the current parent snapshot or to any parent or child snapshot in the snapshot tree and create more snapshots from that snapshot. Each time you revert a snapshot and take another snapshot, a branch (child snapshot) is created.

Parent Snapshots

The first virtual machine snapshot that you create is the base parent snapshot. The parent snapshot is the most recently saved version of the current state of the virtual machine. Taking a snapshot creates a delta disk file for each disk attached to the virtual machine and optionally, a memory file. The delta disk files and memory file are stored with the base .vmdk file. The parent snapshot is always the snapshot that appears immediately above the You are here icon in the Snapshot Manager. If you revert a snapshot, that snapshot becomes the parent of the You are here current state.

Note The parent snapshot is not always the snapshot that you took most recently.

Child Snapshots

A snapshot of a virtual machine taken after the parent snapshot. Each child snapshot contains delta files for each attached virtual disk, and optionally a memory file that points from the present state of the virtual disk (You are here). Each child snapshot's delta files merge with each previous child snapshot until reaching the parent disks. A child disk can later be a parent disk for future child disks.
The relationship of parent and child snapshots can change if you have multiple branches in the snapshot tree. A parent snapshot can have more than one child. Many snapshots have no children.

Caution Do not manually manipulate individual child disks or any of the snapshot configuration files because doing so can compromise the snapshot tree and result in data loss. This restriction includes disk resizing and making modifications to the base parent disk by using the vmkfstools command.

Snapshot Behavior

Taking a snapshot preserves the disk state at a specific time by creating a series of delta disks for each attached virtual disk or virtual RDM and optionally preserves the memory and power state by creating a memory file. Taking a snapshot creates a snapshot object in the Snapshot Manager that represents the virtual machine state and settings.

Each snapshot creates an additional delta .vmdk disk file. When you take a snapshot, the snapshot mechanism prevents the guest operating system from writing to the base .vmdk file and instead directs all writes to the delta disk file. The delta disk represents the difference between the current state of the virtual disk and the state that existed at the time that you took the previous snapshot. If more than one snapshot exists, delta disks can represent the difference between each snapshot. Delta disk files can expand quickly and become as large as the entire virtual disk if the guest operating system writes to every block of the virtual disk.

Snapshot Files

When you take a snapshot, you capture the state of the virtual machine settings and the virtual disk. If you are taking a memory snapshot, you also capture the memory state of the virtual machine. These states are saved to files that reside with the virtual machine's base files.

Snapshot Files

A snapshot consists of files that are stored on a supported storage device. A Take Snapshot operation creates .vmdk, -delta.vmdk, .vmsd, and .vmsn files. By default, the first and all delta disks are stored with the base .vmdk file. The .vmsd and .vmsn files are stored in the virtual machine directory.

Delta disk files

A .vmdk file to which the guest operating system can write. The delta disk represents the difference between the current state of the virtual disk and the state that existed at the time that the previous snapshot was taken. When you take a snapshot, the state of the virtual disk is preserved, the guest operating system stops writing to it, and a delta or child disk is created.

A delta disk has two files. One is a small descriptor file that contains information about the virtual disk, such as geometry and child-parent relationship information. The other one is a corresponding file that contains the raw data.

The files that make up the delta disk are called child disks or redo logs.

Flat file

A -flat.vmdk file that is one of two files that comprises the base disk. The flat disk contains the raw data for the base disk. This file does not appear as a separate file in the Datastore Browser.

Database file

A .vmsd file that contains the virtual machine's snapshot information and is the primary source of information for the Snapshot Manager. This file contains line entries, which define the relationships between snapshots and between child disks for each snapshot.

Memory file

A .vmsn file that includes the active state of the virtual machine. Capturing the memory state of the virtual machine lets you revert to a turned on virtual machine state. With nonmemory snapshots, you can only revert to a turned off virtual machine state. Memory snapshots take longer to create than nonmemory snapshots. The time the ESXi host takes to write the memory onto the disk depends on the amount of memory the virtual machine is configured to use.

A Take Snapshot operation creates .vmdk, -delta.vmdk, vmsd, and vmsn files.

Snapshot Limitations

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

- VMware does not support snapshots of raw disks, RDM physical mode disks, or guest operating systems that use an iSCSI initiator in the guest.

- Virtual machines with independent disks must be powered off before you take a snapshot. Snapshots of powered-on or suspended virtual machines with independent disks are not supported.

- Quiesced snapshots require VMware Tools installation and guest operating system support.

- Snapshots are not supported with PCI vSphere DirectPath I/O devices.

- VMware does not support snapshots of virtual machines configured for bus sharing. If you require bus sharing, consider running backup software in your guest operating system as an alternative solution. If your virtual machine currently has snapshots that prevent you from configuring bus sharing, delete (consolidate) the snapshots.

- Snapshots provide a point-in-time image of the disk that backup solutions can use, but Snapshots are not meant to be a robust method of backup and recovery. If the files containing a virtual machine are lost, its snapshot files are also lost. Also, large numbers of snapshots are difficult to manage, consume large amounts of disk space, and are not protected if there is hardware failure.

- Snapshots can negatively affect the performance of a virtual machine. Performance degradation is based on how long the snapshot or snapshot tree is in place, the depth of the tree, and how much the virtual machine and its guest operating system have changed from the time you took the snapshot. Also, you might see a delay in the amount of time it takes the virtual machine to power on. Do not run production virtual machines from snapshots on a permanent basis.

- If a virtual machine has virtual hard disks larger than 2 TB, snapshot operations can take much longer to finish.

Objective 1.12
Identify the functionality of vSphere vMotion and Storage vMotion technology.
Objective 1.13
Identify use cases for virtual machine snapshots, cloning and templates.

vCenter Server and Host Management Update 1 - VMware vSphere 7.0, page 106

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.

vCenter Server and Host Management Updater 1 - VMware vSphere 7.0, page 118

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.

Objective 1.14
Identify the characteristics of vSphere High Availability and Fault Tolerance.
Objective 1.15
Identify use cases of High Availability and Disaster Recovery.

vSphere Availability Update 1 – Vmware vSphere 7.0, page 7

Reducing Planned Downtime

Planned downtime typically accounts for over 80% of data center downtime. Hardware maintenance, server migration, and firmware updates all require downtime for physical servers. To minimize the impact of this downtime, organizations are forced to delay maintenance until inconvenient and difficult-to-schedule downtime windows.

vSphere makes it possible for organizations to dramatically reduce planned downtime. Because workloads in a vSphere environment can be dynamically moved to different physical servers without downtime or service interruption, server maintenance can be performed without requiring application and service downtime. With vSphere, organizations can:

- Eliminate downtime for common maintenance operations.
- Eliminate planned maintenance windows.
- Perform maintenance at any time without disrupting users and services.

The vSphere vMotion® and Storage vMotion functionality in vSphere makes it possible for organizations to reduce planned downtime because workloads in a VMware environment can be dynamically moved to different physical servers or to different underlying storage without service interruption. Administrators can perform faster and completely transparent maintenance operations, without being forced to schedule inconvenient maintenance windows.

Preventing Unplanned Downtime

While an ESXi host provides a robust platform for running applications, an organization must also protect itself from unplanned downtime caused from hardware or application failures. vSphere builds important capabilities into data center infrastructure that can help you prevent unplanned downtime.

These vSphere capabilities are part of virtual infrastructure and are transparent to the operating system and applications running in virtual machines. These features can be configured and utilized by all the virtual machines on a physical system, reducing the cost and complexity of providing higher availability. Key availability capabilities are built into vSphere:

- Shared storage. Eliminate single points of failure by storing virtual machine files on shared storage, such as Fibre Channel or iSCSI SAN, or NAS. The use of SAN mirroring and replication features can be used to keep updated copies of virtual disk at disaster recovery sites.
- Network interface teaming. Provide tolerance of individual network card failures.
- Storage multipathing. Tolerate storage path failures.

In addition to these capabilities, the vSphere HA and Fault Tolerance features can minimize or eliminate unplanned downtime by providing rapid recovery from outages and continuous availability, respectively.

vSphere HA Provides Rapid Recovery from Outages

vSphere HA leverages multiple ESXi hosts configured as a cluster to provide rapid recovery from outages and cost-effective high availability for applications running in virtual machines.

vSphere HA protects application availability in the following ways:

- It protects against a server failure by restarting the virtual machines on other hosts within the cluster.
- It protects against application failure by continuously monitoring a virtual machine and resetting it in the event that a failure is detected.
- It protects against datastore accessibility failures by restarting affected virtual machines on other hosts which still have access to their datastores.
- It protects virtual machines against network isolation by restarting them if their host becomes isolated on the management or vSAN network. This protection is provided even if the network has become partitioned.

Unlike other clustering solutions, vSphere HA provides the infrastructure to protect all workloads with the infrastructure:

- You do not need to install special software within the application or virtual machine. All workloads are protected by vSphere HA. After vSphere HA is configured, no actions are required to protect new virtual machines. They are automatically protected.
- You can combine vSphere HA with vSphere Distributed Resource Scheduler (DRS) to protect against failures and to provide load balancing across the hosts within a cluster.

vSphere HA has several advantages over traditional failover solutions:

Minimal setup

After a vSphere HA cluster is set up, all virtual machines in the cluster get failover support without additional configuration.

Reduced hardware cost and setup

The virtual machine acts as a portable container for the applications and it can be moved among hosts. Administrators avoid duplicate configurations on multiple machines. When you use vSphere HA, you must have sufficient resources to fail over the number of hosts you want to protect with vSphere HA. However, the VMware vCenter Server® system automatically manages resources and configures clusters.

Increased application availability

Any application running inside a virtual machine has access to increased availability. Because the virtual machine can recover from hardware failure, all applications that start at boot have increased availability without increased computing needs, even if the application is not itself a clustered application. By monitoring and responding to VMware Tools heartbeats and restarting nonresponsive virtual machines, it protects against guest operating system crashes.

DRS and vMotion integration

> If a host fails and virtual machines are restarted on other hosts, DRS can provide migration recommendations or migrate virtual machines for balanced resource allocation. If one or both of the source and destination hosts of a migration fail, vSphere HA can help recover from that failure.

vSphere Fault Tolerance Provides Continuous Availability

vSphere HA provides a base level of protection for your virtual machines by restarting virtual machines in the event of a host failure. vSphere Fault Tolerance provides a higher level of availability, allowing users to protect any virtual machine from a host failure with no loss of data, transactions, or connections.

Fault Tolerance provides continuous availability by ensuring that the states of the Primary and Secondary VMs are identical at any point in the instruction execution of the virtual machine.

If either the host running the Primary VM or the host running the Secondary VM fails, an immediate and transparent failover occurs. The functioning ESXi host seamlessly becomes the Primary VM host without losing network connections or in-progress transactions. With transparent failover, there is no data loss and network connections are maintained. After a transparent failover occurs, a new Secondary VM is respawned and redundancy is re-established. The entire process is transparent and fully automated and occurs even if vCenter Server is unavailable.

Protecting vCenter Server with vCenter High Availability

vCenter High Availability (vCenter HA) protects not only against host and hardware failures but also against vCenter Server application failures. Using automated failover from active to passive, vCenter HA supports high availability with minimal downtime.

You configure vCenter HA from the vSphere Client. The configuration wizard provides these options.

Option	Description
Automatic	The automatic option clones the Active node to the Passive node and witness node, and configures the nodes for you. If your environment meets the following requirements, you can use this option. • The vCenter Server that becomes the Active node is managing its own ESXi host and its own virtual machine. This configuration is sometimes called a self-managed vCenter Server.
Manual	The manual option offers more flexibility. You can use this option provided that your environment meets hardware and software requirements. If you select this option, you are responsible for cloning the Active node to the Passive node and the Witness node. You must also perform some networking configuration.

Protecting vCenter Server with VMware Service Lifecycle Manager

Availability of vCenter Server is provided by VMware Service Lifecycle Manager.

If a vCenter service fails, VMware Service Lifecycle Manager restarts it. VMware Service Lifecycle Manager monitors the health of services and it takes preconfigured remediation action when it detects a failure. Service does not restart if multiple attempts to remediate fail.

Objective 1.16
Identify the functionality of VMware Distributed Resource Scheduler.

Distributed Resource Scheduler - VMware vSphere
https://www.vmware.com/products/vsphere/drs-dpm.html

Distributed Resource Scheduler, Distributed Power Management

Enable VMware DRS to Manage Workloads

Group VMware ESXi hosts into resource clusters to segregate the computing needs of different business units. VMware vSphere clusters allow you to:

- Provide highly available resources to your workloads.
- Balance workloads for optimal performance.
- Scale and manage computing resources without service disruption.

Balanced Capacity

Balance computing capacity by cluster to deliver optimized performance for hosts and virtual machines. VMware vSphere Distributed Resource Scheduler (DRS) is a feature included in the vSphere Enterprise Plus. Using DRS, you can:

- Improve service levels by guaranteeing appropriate resources to virtual machines.
- Deploy new capacity to a cluster without service disruption.
- Automatically migrate virtual machines during maintenance without service disruption.
- Monitor and manage more infrastructure per system administrator.

Reduced Energy Consumption

Optimize power consumption dynamically within a vSphere cluster with VMware vSphere Distributed Power Management (DPM), which is also included in vSphere Enterprise Plus and vSphere with Operation Management Enterprise Plus editions. When demand for resources is low, DPM places hosts in standby mode and when demand is high, DPM powers on enough hosts to manage that demand and keep your services available. Dynamic power management with DPM allows you to:

- Cut power and cooling costs by as much as 20 percent during low utilization periods.
- Automate energy management in your data center more efficiently.

Technical Details

Initial Workload Placement

When you power on a virtual machine in a cluster, DRS places it on an appropriate host or generates a recommendation, depending on the automation level you choose. Automation levels, also known as migration thresholds, range from conservative to aggressive. VMware vCenter will only apply recommendations that satisfy cluster constraints such as host affinity rules or maintenance. It applies DRS recommendations that can provide even a slight improvement to the cluster's overall load balance. DRS offers five automation levels to fit your needs on a per cluster basis.

Automated Load Balancing

DRS spreads the virtual machine workloads across vSphere hosts inside a cluster and monitors available resources for you. Based on your automation level, DRS will migrate (VMware vSphere vMotion) virtual machines to other hosts within the cluster to maximize performance.

Optimized Power Consumption

Like DRS, vSphere's Distributed Power Management feature optimizes power consumption at the cluster and host level. When you enable DPM, it compares cluster- and host-level capacity to virtual machine demand, including recent historical demand, and places hosts in standby mode. If capacity demands increase, DPM powers on hosts in standby to absorb the additional workload. You can also set DPM to issue recommendations but take no actions.

Cluster Maintenance

DRS accelerates the VMware vSphere Update Manager remediation process by determining the optimum number of hosts that can enter maintenance mode simultaneously, based on current cluster conditions and demands.

Constraint Correction

DRS redistributes virtual machines across vSphere cluster hosts to comply with user-defined affinity and anti-affinity rules following host failures or during maintenance operations.

Objective 1.17
Given a DRS score, identify the meaning.

vSphere Resource Management Update 1 – Vmware vSphere 7.0, page 84

DRS Migration Threshold

The DRS migration threshold allows you to specify which recommendations are generated and then applied (when the virtual machines involved in the recommendation are in fully automated mode) or shown (if in manual mode). This threshold is a measure of how aggressive DRS is in recommending migrations to improve VM happiness.

You can move the threshold slider to use one of five settings, ranging from Conservative to Aggressive. The higher the aggressiveness setting, the more frequently DRS might recommend migrations to improve VM happiness. The Conservative setting generates only priority-one recommendations (mandatory recommendations).

After a recommendation receives a priority level, this level is compared to the migration threshold you set. If the priority level is less than or equal to the threshold setting, the recommendation is either applied (if the relevant virtual machines are in fully automated mode) or displayed to the user for confirmation (if in manual or partially automated mode.)

DRS Score

Each migration recommendation is computed using the VM happiness metric which measures execution efficiency. This metric is displayed as DRS Score in the cluster's Summary tab in the vSphere Client. DRS load balancing recommendations attempt to improve the DRS score of a VM. The Cluster DRS score is a weighted average of the VM DRS Scores of all the powered on VMs in the cluster. The Cluster DRS Score is shown in the gauge component. The color of the filled in section changes depending on the value to match the corresponding bar in the VM DRS Score histogram. The bars in the histogram show the percentage of VMs that have a DRS Score in that range. You can view the list with server-side sorting and filtering by selecting the Monitor tab of the cluster and selecting vSphere DRS, which shows a list of the VMs in the cluster sorted by their DRS score in ascending order.

Objective 1.18
Identify use cases for Enhanced vMotion Compatibility (EVC).

vCenter Server and Host Management - VMware vSphere 7.0 Update 1, page 122

About Enhanced vMotion Compatibility

You can use the Enhanced vMotion Compatibility (EVC) feature to help ensure vMotion compatibility for the hosts in a cluster. EVC ensures that all hosts in a cluster present the same CPU feature set to virtual machines, even if the actual CPUs on the hosts differ. Using EVC prevents migrations with vMotion from failing because of incompatible CPUs.

Configure EVC from the cluster settings dialog box. When you configure EVC, you configure all host processors in the cluster to present the feature set of a baseline processor. This baseline feature set is called the EVC mode. EVC uses AMD-V Extended Migration technology (for AMD hosts) and Intel FlexMigration technology (for Intel hosts) to mask processor features so that hosts can present the feature set of an earlier generation of processors. The EVC mode must be equivalent to, or a subset of, the feature set of the host with the smallest feature set in the cluster.

EVC masks only those processor features that affect vMotion compatibility. Enabling EVC does not prevent a virtual machine from taking advantage of faster processor speeds, increased numbers of CPU cores, or hardware virtualization support that might be available on newer hosts.

EVC cannot prevent virtual machines from accessing hidden CPU features in all circumstances. Applications that do not follow CPU vendor recommended methods of feature detection might behave unexpectedly in an EVC environment. VMware EVC cannot be supported with ill-behaved applications that do not follow the CPU vendor recommendations. For more information about creating well-behaved applications, search the VMware Knowledge Base for the article *Detecting and Using New Features in CPUs*.

Starting with vSphere 7.0 Update 1, you can take advantage of the EVC feature for Virtual Shared Graphics Acceleration (vSGA). vSGA allows multiple virtual machines to share GPUs installed on ESXi hosts and leverage the 3D graphics acceleration capabilities.

Section 4
Installing, Configuring, and Setup

Objective 4.1 - Identify Virtual Switch configuration options.

Objective 4.2 - Identify how to configure different types of datastores.

Objective 4.3 - Identify how to configure vSphere HA.

Objective 4.4 - Identify how to configure vSphere DRS.

Objective 4.5 - Identify how to configure EVC.

Objective 4.1
Identify Virtual Switch configuration options.

vSphere Networking Update 1 - VMware vSphere 7.0, page 23

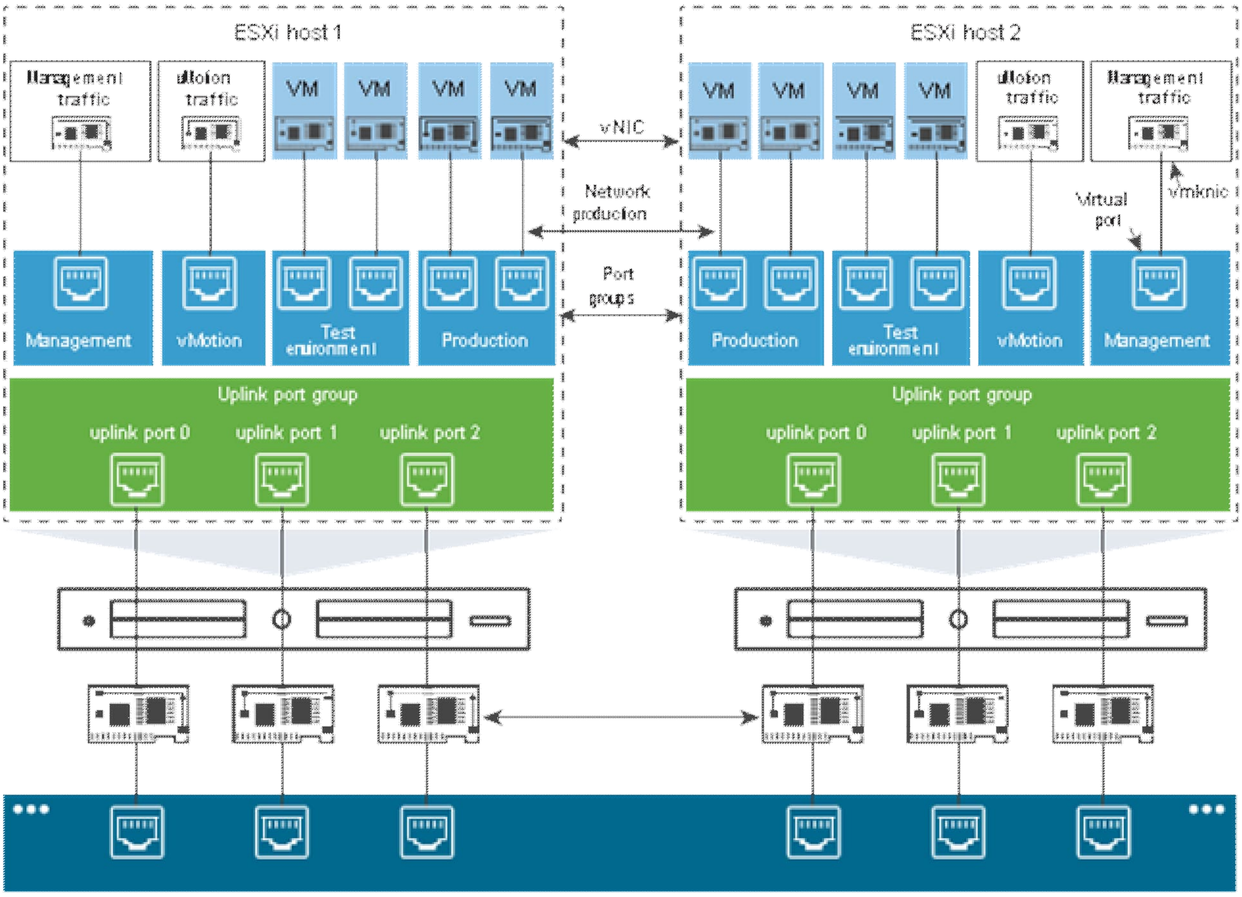
vSphere Standard Switches

You can create abstracted network devices called vSphere Standard Switches. You use standard switches to provide network connectivity to hosts and virtual machines. A standard switch can bridge traffic internally between virtual machines in the same VLAN and link to external networks.

Standard Switch Overview

To provide network connectivity to hosts and virtual machines, you connect the physical NICs of the hosts to uplink ports on the standard switch. Virtual machines have network adapters (vNICs) that you connect to port groups on the standard switch. Every port group can use one or more physical NICs to handle their network traffic. If a port group does not have a physical NIC connected to it, virtual machines on the same port group can only communicate with each other but not with the external network.

Figure 2-1. vSphere Standard Switch architecture



A vSphere Standard Switch is very similar to a physical Ethernet switch. Virtual machine network adapters and physical NICs on the host use the logical ports on the switch as each adapter uses one port. Each logical port on the standard switch is a member of a single port group. For information about maximum allowed ports and port groups, see the *Configuration Maximums* documentation.

Standard Port Groups

Each port group on a standard switch is identified by a network label, which must be unique to the current host. You can use network labels to make the networking configuration of virtual machines portable across hosts. You should give the same label to the port groups in a data center that use physical NICs connected to one broadcast domain on the physical network. Conversely, if two port groups are connected to physical NICs on different broadcast domains, the port groups should have distinct labels.

For example, you can create *Production* and *Test environment* port groups as virtual machine networks on the hosts that share the same broadcast domain on the physical network.

A VLAN ID, which restricts port group traffic to a logical Ethernet segment within the physical network, is optional. For port groups to receive the traffic that the same host sees, but from more than one VLAN, the VLAN ID must be set to VGT (VLAN 4095).

Number of Standard Ports

To ensure efficient use of host resources on ESXi hosts, the number of ports of standard switches are dynamically scaled up and down. A standard switch on such a host can expand up to the maximum number of ports supported on the host.

vSphere Networking Update 1 - VMware vSphere 7.0, page 17

vSphere Standard Switch Properties

vSphere Standard Switch settings control switch-wide defaults for ports, which can be overridden by port group settings for each standard switch. You can edit standard switch properties, such as the uplink configuration and the number of available ports.

Number of Ports on ESXi Hosts

To ensure efficient use of host resources on ESXi hosts, the ports of virtual switches are dynamically scaled up and down. A switch on such a host can expand up to the maximum number of ports supported on the host. The port limit is determined based on the maximum number of virtual machines that the host can handle.

Change the Size of the MTU on a vSphere Standard Switch

Change the size of the maximum transmission unit (MTU) on a vSphere Standard Switch to improve the networking efficiency by increasing the amount of payload data transmitted with a single packet, that is, enabling jumbo frames.

Procedure

1 In the vSphere Client, navigate to the host.

2 On the Configure tab, expand Networking and select Virtual Switches.

3 Select a standard switch from the table and click Edit settings.

4 Change the MTU (Bytes) value for the standard switch.

You can enable jumbo frames by setting an MTU value greater than 1500. You cannot set an MTU size greater than 9000 bytes.

5 Click OK.

Change the Speed of a Physical Adapter

A physical adapter can become a bottleneck for network traffic if the adapter speed does not match application requirements. You can change the connection speed and duplex of a physical adapter to transfer data in compliance with the traffic rate.

If the physical adapter supports SR-IOV, you can enable it and configure the number of virtual functions to use for virtual machine networking.

Procedure

1 In the vSphere Client, navigate to a host.

2 On the Configure tab, expand Networking and select Physical adapters.

The physical network adapters of the host appear in a table that contains details for each physical network adapter.

3 Select the physical network adapter from the list and click the Edit adapter settings icon.

4 Select speed and duplex mode of the physical network adapter from the drop-down menu.

5 Click OK.

Add and Team Physical Adapters in a vSphere Standard Switch

Assign a physical adapter to a standard switch to provide connectivity to virtual machines and VMkernel adapters on the host. You can form a team of NICs to distribute traffic load and to configure failover.

NIC teaming combines multiple network connections to increase throughput and provide redundancy should a link fail. To create a team, you associate multiple physical adapters to a single vSphere Standard Switch.

Procedure

1 In the vSphere Client, navigate to the host.

2 On the Configure tab, expand Networking and select Virtual Switches.

3 Select the standard switch you want to add a physical adapter to.

4 Click Manage Physical Adapters.

5 Add one or more available physical network adapters to the switch.

a Click Add adapters, select one or more network adapters from the list and click OK.

The selected adapters appear in the failover group list under the Assigned Adapters list.

b (Optional) Use the up and down arrows to change the position of an adapter in the failover groups.

The failover group determines the role of the adapter for exchanging data with the external network, that is, active, standby or unused. By default, the adapters are added as active to the standard switch.

6 Click OK to apply the physical adapter configuration.

View the Topology Diagram of a vSphere Standard Switch

You can examine the structure and components of a vSphere Standard Switch by using its topology diagram.

The topology diagram of a standard switch provides a visual representation of the adapters and port groups connected to the switch.
From the diagram you can edit the settings of a selected port group and of a selected adapter.

Procedure

1 In the vSphere Client, navigate to the host.

2 On the Configure tab, expand Networking and select Virtual Switches.

3 Select the standard switch from the list.

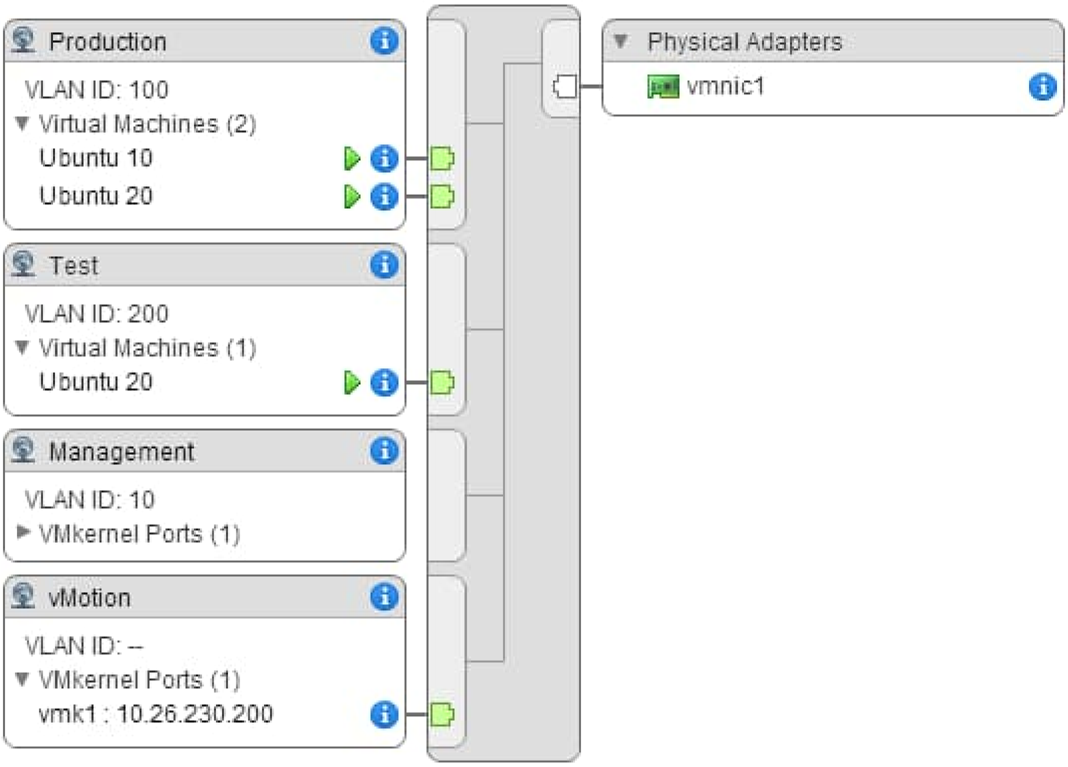
Results

The diagram appears under the list of virtual switches on the host.

Example: Diagram of a Standard Switch That Connects the VMkernel and Virtual Machines to the Network

In your virtual environment, a vSphere Standard Switch handles VMkernel adapters for vSphere vMotion and for the management network, and virtual machines grouped. You can use the central topology diagram to examine whether a virtual machine or VMkernel adapter is connected to the external network and to identify the physical adapter that carries the data.

Figure 2-2. Topology Diagram of a Standard Switch That Connects the VMkernel and Virtual Machines to the Network

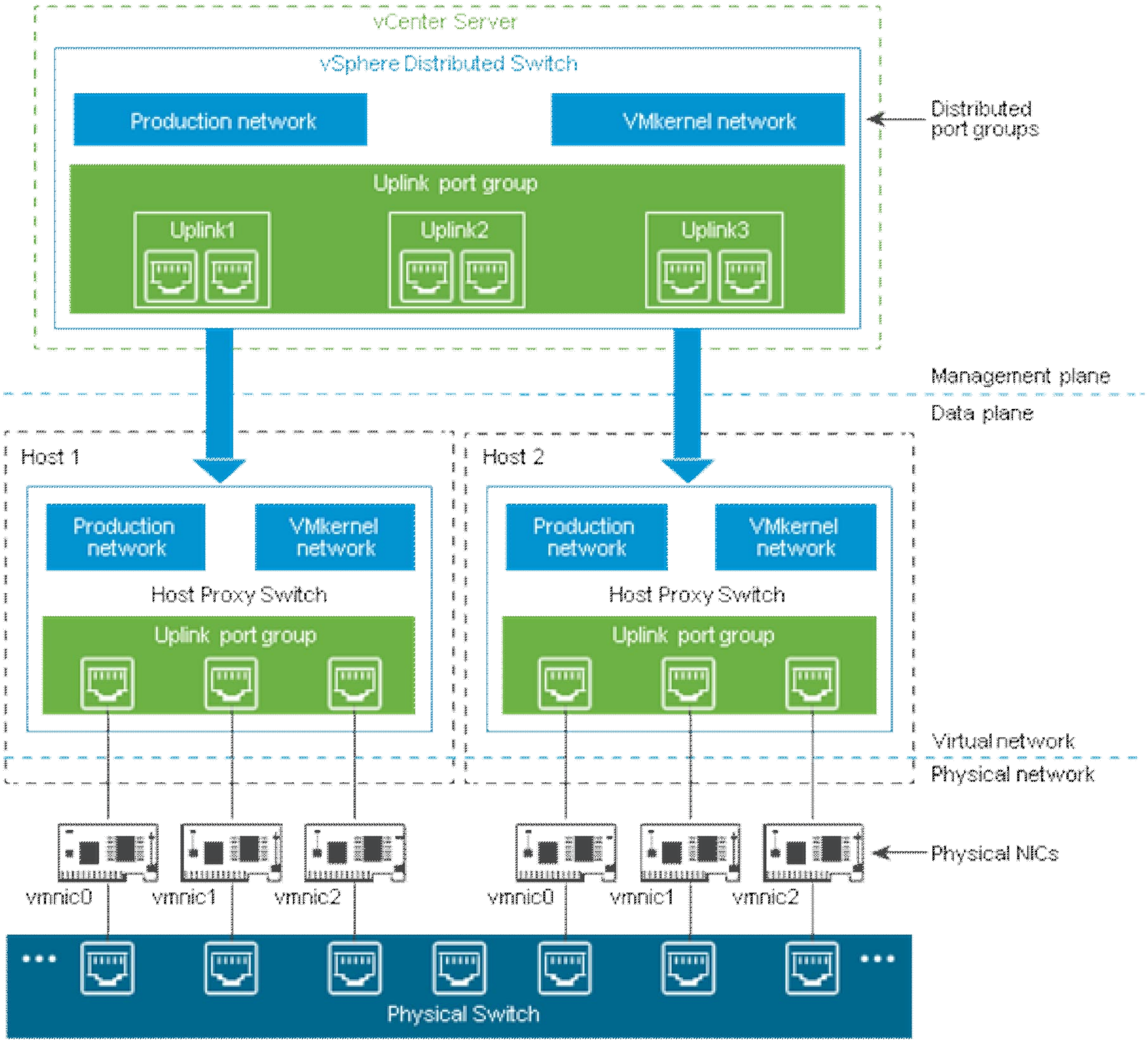


vSphere Networking Update 1 - VMware vSphere 7.0, page 27

vSphere Distributed Switch Architecture

A vSphere Distributed Switch provides centralized management and monitoring of the networking configuration of all hosts that are associated with the switch. You set up a distributed switch on a vCenter Server system, and its settings are propagated to all hosts that are associated with the switch.

Figure 3-1. vSphere Distributed Switch Architecture



A network switch in vSphere consists of two logical sections that are the data plane and the management plane. The data plane implements the packet switching, filtering, tagging, and so on. The management plane is the control structure that you use to configure the data plane functionality. A vSphere Standard Switch contains both data and management planes, and you configure and maintain each standard switch individually.

A vSphere Distributed Switch separates the data plane and the management plane. The management functionality of the distributed switch resides on the vCenter Server system that lets you administer the networking configuration of your environment on a data center level. The data plane remains locally on every host that is associated with the distributed switch. The data plane section of the distributed switch is called a host proxy switch. The networking configuration that you create on vCenter Server (the management plane) is automatically pushed down to all host proxy switches (the data plane).

The vSphere Distributed Switch introduces two abstractions that you use to create consistent networking configuration for physical NICs, virtual machines, and VMkernel services.

Uplink port group

An uplink port group or dvuplink port group is defined during the creation of the distributed switch and can have one or more uplinks. An uplink is a template that you use to configure physical connections of hosts as well as failover and load balancing policies. You map physical NICs of hosts to uplinks on the distributed switch. At the host level, each physical NIC is connected to an uplink port with a particular ID. You set failover and load balancing policies over uplinks and the policies are automatically propagated to the host proxy switches, or the data plane. In this way you can apply consistent failover and load balancing configuration for the physical NICs of all hosts that are associated with the distributed switch.

Distributed port group

Distributed port groups provide network connectivity to virtual machines and accommodate VMkernel traffic. You identify each distributed port group by using a network label, which must be unique to the current data center. You configure NIC teaming, failover, load balancing, VLAN, security, traffic shaping , and other policies on distributed port groups. The virtual ports that are connected to a distributed port group share the same properties that are configured to the distributed port group. As with uplink port groups, the configuration that you set on distributed port groups on vCenter Server (the management plane) is automatically propagated to all hosts on the distributed switch through their host proxy switches (the data plane). In this way you can configure a group of virtual machines to share the same networking configuration by associating the virtual machines to the same distributed port group.

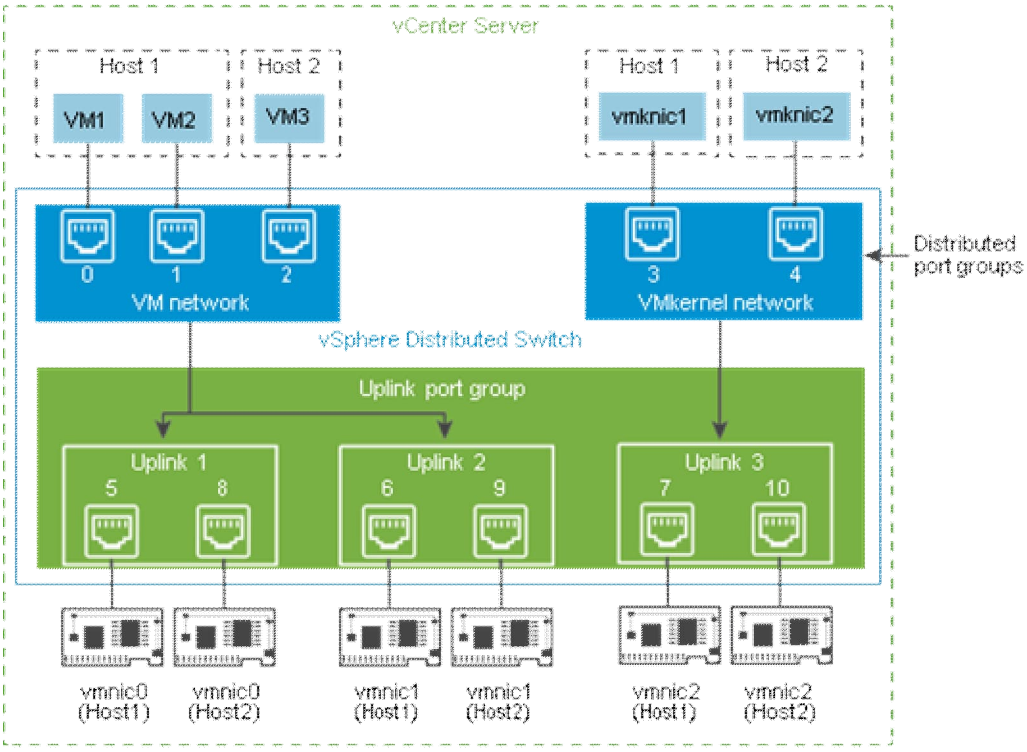
For example, suppose that you create a vSphere Distributed Switch on your data center and associate two hosts with it. You configure three uplinks to the uplink port group and connect a physical NIC from each host to an uplink. In this way, each uplink has two physical NICs from each host mapped to it, for example Uplink 1 is configured with vmnic0 from Host 1 and Host 2. Next you create the Production and the VMkernel network distributed port groups for virtual machine networking and VMkernel services. Respectively, a representation of the Production and the VMkernel network port groups is also created on Host 1 and Host 2. All policies that you set to the Production and the VMkernel network port groups are propagated to their representations on Host 1 and Host 2.

To ensure efficient use of host resources, the number of distributed ports of proxy switches is dynamically scaled up and down. A proxy switch on such a host can expand up to the maximum number of ports supported on the host. The port limit is determined based on the maximum number of virtual machines that the host can handle.

vSphere Distributed Switch Data Flow

The data flow from the virtual machines and VMkernel adapters down to the physical network depends on the NIC teaming and load balancing policies that are set to the distributed port groups. The data flow also depends on the port allocation on the distributed switch.

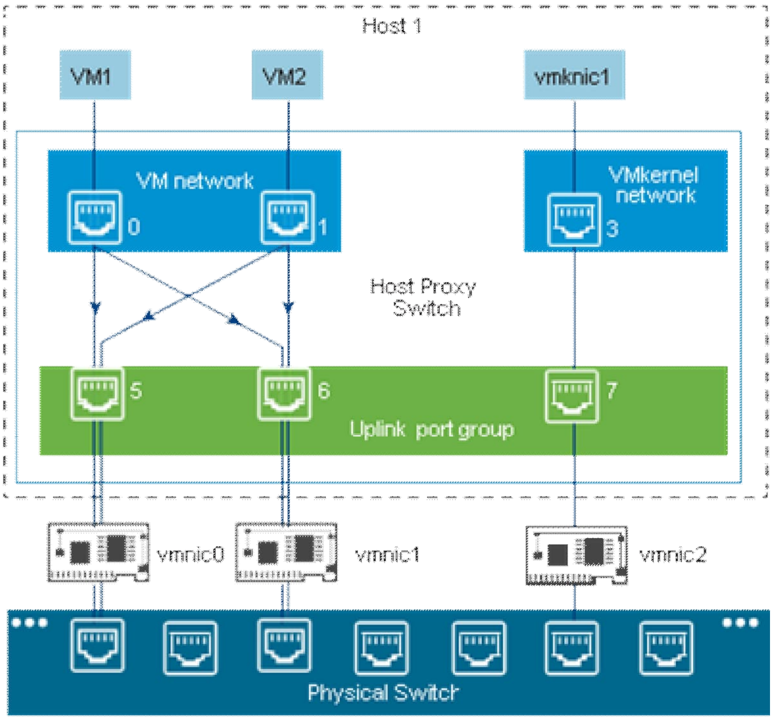
Figure 3-2. NIC Teaming and Port Allocation on a vSphere Distributed Switch



For example, suppose that you create the VM network and the VMkernel network distributed port groups, respectively with 3 and 2 distributed ports. The distributed switch allocates ports with IDs from 0 to 4 in the order that you create the distributed port groups. Next, you associate Host 1 and Host 2 with the distributed switch. The distributed switch allocates ports for every physical NIC on the hosts, as the numbering of the ports continues from 5 in the order that you add the hosts. To provide network connectivity on each host, you map vmnic0 to Uplink 1, vmnic1 to Uplink 2, and vmnic2 to Uplink 3.

To provide connectivity to virtual machines and to accommodate VMkernel traffic, you configure teaming and failover to the VM network and to the VMkernel network port groups. Uplink 1 and Uplink 2 handle the traffic for the VM network port group, and Uplink 3 handles the traffic for the VMkernel network port group.

Figure 3-3. Packet Flow on the Host Proxy Switch



On the host side, the packet flow from virtual machines and VMkernel services passes through particular ports to reach the physical network. For example, a packet sent from VM1 on Host 1 first reaches port 0 on the VM network distributed port group. Because Uplink 1 and Uplink 2 handle the traffic for the VM network port group, the packet can continue from uplink port 5 or uplink port 6 . If the packet goes through uplink port 5, it continues to vmnic0, and if the packet goes to uplink port 6, it continues to vmnic1.

vSphere Networking Update 1 - VMware vSphere 7.0, page 34

Edit General and Advanced vSphere Distributed Switch Settings

General settings for a vSphere Distributed Switch include the switch name and number of uplinks. Advanced settings for a distributed switch include Cisco Discovery Protocol and the maximum MTU for the switch.

Procedure

1 In the vSphere Client Home page, click Networking and select the distributed switch.

2 On the Configure tab, expand Settings and select Properties.

3 Click Edit.

4 Click General to edit the vSphere Distributed Switch settings.

Option	Description
Name	Enter the name for the distributed switch.
Number of uplinks	Select the number of uplink ports for the distributed switch. Click Edit uplink names to change the names of the uplinks.

Network I/O Control	Use the drop-down menu to enable or disable Network I/O control.
Description	Add or modify a description of the distributed switch settings.

5 Click Advanced to edit the vSphere Distributed Switch settings.

Option	Description
MTU (Bytes)	Maximum MTU size for the vSphere Distributed Switch. To enable jumbo frames, set a value greater than 1500 bytes.
Multicast filtering mode	• Basic. The distributed switch forwards traffic that is related to a multicast group based on a MAC address generated from the last 23 bits of the IPv4 address of the group. • IGMP/MLD snooping. The distributed switch forwards multicast traffic to virtual machines according to the IPv4 and IPv6 addresses of subscribed multicast groups by using membership messages defined by the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery protocol.
Discovery Protocol	a Select Cisco Discovery Protocol, Link Layer Discovery Protocol, or (disabled) from the Type drop-down menu. b Set Operation to Listen, Advertise, or Both. For information about Discovery Protocol, see Switch Discovery Protocol.
Administrator Contact	Enter the name and other details of the administrator for the distributed switch.

6 Click OK.

Objective 4.2
Identify how to configure different types of datastores.

vSphere Storage Update 1 - VMware vSphere 7.0, page 175

Types of Datastores

Depending on the storage you use, datastores can be of different types.
vCenter Server and ESXi support the following types of datastores.

Table 17-1. Types of Datastores

Datastore Type	Description
VMFS (version 5 and 6)	Datastores that you deploy on block storage devices use the vSphere Virtual Machine File System (VMFS) format. VMFS is a special high-performance file system format that is optimized for storing virtual machines. See Understanding VMFS Datastores.
NFS (version 3 and 4.1)	An NFS client built into ESXi uses the Network File System (NFS) protocol over TCP/IP to access a designated NFS volume. The volume is located on a NAS server. The ESXi host mounts the volume as an NFS datastore, and uses it for storage needs. ESXi supports versions 3 and 4.1 of the NFS protocol. See Understanding Network File System Datastores
vSAN	vSAN aggregates all local capacity devices available on the hosts into a single datastore shared by all hosts in the vSAN cluster. See the *Administering VMware vSAN* documentation.
vVol	vVols datastore represents a storage container in vCenter Server and vSphere Client. See Chapter 22 Working with VMware vSphere Virtual Volumes (vVols).

Depending on your storage type, some of the following tasks are available for the datastores.

- Create datastores. You can use the vSphere Client to create certain types of datastores.
- Perform administrative operations on the datastores. Several operations, such as renaming a datastore, are available for all types of datastores. Others apply to specific types of datastores.
- Organize the datastores. For example, you can group them into folders according to business practices. After you group the datastores, you can assign the same permissions and alarms on the datastores in the group at one time.
- Add the datastores to datastore clusters. A datastore cluster is a collection of datastores with shared resources and a shared management interface. When you create the datastore cluster, you can use Storage DRS to manage storage resources. For information about datastore clusters, see the *vSphere Resource Management* documentation.

Understanding VMFS Datastores

To store virtual disks, ESXi uses datastores. The datastores are logical containers that hide specifics of physical storage from virtual machines and provide a uniform model for storing the virtual machine files. The datastores that you deploy on block storage devices use the native vSphere Virtual Machine File System (VMFS) format. It is a special high-performance file system format that is optimized for storing virtual machines.

Use the vSphere Client to set up the VMFS datastore in advance on the block-based storage device that your ESXi host discovers. The VMFS datastore can be extended to span over several physical storage devices that include SAN LUNs and local storage. This feature allows you to pool storage and gives you flexibility in creating the datastore necessary for your virtual machines.

You can increase the capacity of the datastore while the virtual machines are running on the datastore. This ability lets you add new space to your VMFS datastores as your virtual machine requires it. VMFS is designed for concurrent access from multiple physical machines and enforces the appropriate access controls on the virtual machine files.

Versions of VMFS Datastores

Several versions of the VMFS file system have been released since its introduction. Currently, ESXi supports VMFS5 and VMFS6.

For all supported VMFS version, ESXi offers complete read and write support. On the supported VMFS datastores, you can create and power on virtual machines.

Table 17-2. Host Access to VMFS Versions

VMFS	ESXi
VMFS6	Read and write
VMFS5	Read and write

The following table compares major characteristics of VMFS5 and VMFS6. For additional information, see *Configuration Maximums*.

Table 17-3. Comparing VMFS5 and VMFS6

Features and Functionalities	VMFS5	VMFS6
Access for ESXi hosts version 6.5 and later	Yes	Yes
Access for ESXi hosts version 6.0 and earlier	Yes	No
Datastores per host	512	512
512n storage devices	Yes	Yes (default)
512e storage devices	Yes. Not supported on local 512e devices.	Yes (default)
4Kn storage devices	No	Yes
Automatic space reclamation	No	Yes
Manual space reclamation through the esxcli command. See Manually Reclaim Accumulated Storage Space.	Yes	Yes
Space reclamation from guest OS	Limited	Yes
GPT storage device partitioning	Yes	Yes
MBR storage device partitioning	Yes For a VMFS5 datastore that has been previously upgraded from VMFS3.	No

Storage devices greater than 2 TB for each VMFS extent	Yes	Yes
Support for virtual machines with large capacity virtual disks, or disks greater than 2 TB	Yes	Yes
Support of small files of 1 KB	Yes	Yes
Default use of ATS-only locking mechanisms on storage devices that support ATS. See VMFS Locking Mechanisms.	Yes	Yes
Block size	Standard 1 MB	Standard 1 MB
Default snapshots	VMFSsparse for virtual disks smaller than 2 TB. SEsparse for virtual disks larger than 2 TB.	SEsparse
Virtual disk emulation type	512n	512n
vMotion	Yes	Yes
Storage vMotion across different datastore types	Yes	Yes
High Availability and Fault Tolerance	Yes	Yes
DRS and Storage DRS	Yes	Yes
RDM	Yes	Yes

When you work with VMFS datastores, consider the following:

- Datastore Extents. A spanned VMFS datastore must use only homogeneous storage devices, either 512n, 512e, or 4Kn. The spanned datastore cannot extend over devices of different formats.
- Block Size. The block size on a VMFS datastore defines the maximum file size and the amount of space a file occupies. VMFS5 and VMFS6 datastores support the block size of 1 MB.
- Storage vMotion. Storage vMotion supports migration across VMFS, vSAN, and vVols datastores. vCenter Server performs compatibility checks to validate Storage vMotion across different types of datastores.
- Storage DRS. VMFS5 and VMFS6 can coexist in the same datastore cluster. However, all datastores in the cluster must use homogeneous storage devices. Do not mix devices of different formats within the same datastore cluster.
- Device Partition Formats. Any new VMFS5 or VMFS6 datastore uses GUID partition table (GPT) to format the storage device. The GPT format enables you to create datastores larger than 2 TB. If your VMFS5 datastore has been previously upgraded from VMFS3, it continues to use the master boot record (MBR) partition format, which is characteristic for VMFS3. Conversion to GPT happens only after you expand the datastore to a size larger than 2 TB.

vSphere Storage Update 1 - VMware vSphere 7.0, page 199

Creating Datastores

You use the New Datastore wizard to create your datastores. Depending on the type of your storage and storage needs, you can create a VMFS, NFS, or vVols datastore.

A vSAN datastore is automatically created when you enable vSAN. For information, see the *Administering VMware vSAN* documentation.

You can also use the New Datastore wizard to manage VMFS datastore copies.

- Create a VMFS Datastore

  VMFS datastores serve as repositories for virtual machines. You can set up VMFS datastores on any SCSI-based storage devices that the host discovers, including Fibre Channel, iSCSI, and local storage devices.

- Create an NFS Datastore

  You can use the New Datastore wizard to mount an NFS volume.

- Create a vVols Datastore

  You use the New Datastore wizard to create a vVols datastore.

Create a VMFS Datastore

VMFS datastores serve as repositories for virtual machines. You can set up VMFS datastores on any SCSI-based storage devices that the host discovers, including Fibre Channel, iSCSI, and local storage devices.

Prerequisites

1 Install and configure any adapters that your storage requires.

2 To discover newly added storage devices, perform a rescan. See Storage Rescan Operations.

3 Verify that storage devices you are planning to use for your datastores are available. See Storage Device Characteristics.

Procedure

1 In the vSphere Client object navigator, browse to a host, a cluster, or a data center.

2 From the right-click menu, select Storage > New Datastore.

3 Select VMFS as the datastore type.

4 Enter the datastore name and if necessary, select the placement location for the datastore.

The system enforces a 42 character limit for the datastore name.

5 Select the device to use for your datastore.

Important The device you select must not have any values displayed in the Snapshot Volume column. If a value is present, the device contains a copy of an existing VMFS datastore. For information on managing datastore copies, see Managing Duplicate VMFS Datastores.

6 Specify the datastore version.

Option	Description

VMFS6	Default format on all hosts that support VMFS6. The ESXi hosts of version 6.0 or earlier cannot recognize the VMFS6 datastore.
VMFS5	VMFS5 datastore supports access by the ESXi hosts of version 6.7 or earlier.

7 Define configuration details for the datastore.

Note The required minimum size for a VMFS6 datastore is 2 GB.

a Specify partition configuration.

Option	Description
Use all available partitions	Dedicates the entire disk to a single VMFS datastore. If you select this option, all file systems and data currently stored on this device are destroyed.
Use free space	Deploys a VMFS datastore in the remaining free space of the disk.

b If the space allocated for the datastore is excessive for your purposes, adjust the capacity values in the Datastore Size field.

By default, the entire free space on the storage device is allocated.

c For VMFS6, specify the block size and define space reclamation parameters. See Space Reclamation Requests from VMFS Datastores.

8 In the Ready to Complete page, review the datastore configuration information and click Finish.

Results

The datastore on the SCSI-based storage device is created. It is available to all hosts that have access to the device.

What to do next

After you create the VMFS datastore, you can perform the following tasks:

- Change the capacity of the datastore. See Increase VMFS Datastore Capacity.
- Edit space reclamation settings. See Change Space Reclamation Settings.
- Enable shared vmdk support. See Enable or Disable Support for Clustered Virtual Disks on the VMFS6 Datastore.

Create an NFS Datastore

You can use the New Datastore wizard to mount an NFS volume.

Prerequisites

- Set up NFS storage environment.

- If you plan to use Kerberos authentication with the NFS 4.1 datastore, make sure to configure the ESXi hosts for Kerberos authentication.

Procedure

1 In the vSphere Client object navigator, browse to a host, a cluster, or a data center.

2 From the right-click menu, select Storage > New Datastore.

3 Select NFS as the datastore type and specify an NFS version.

   - NFS 3
   - NFS 4.1

   Important If multiple hosts access the same datastore, you must use the same protocol on all hosts.

4 Enter the datastore parameters.

Option	Description
Datastore name	The system enforces a 42 character limit for the datastore name.
Folder	The mount point folder name
Server	The server name or IP address. You can use IPv6 or IPv4 formats. With NFS 4.1, you can add multiple IP addresses or server names if the NFS server supports trunking. The ESXi host uses these values to achieve multipathing to the NFS server mount point.

5 Select Mount NFS read only if the volume is exported as read-only by the NFS server.

6 To use Kerberos security with NFS 4.1, enable Kerberos and select an appropriate Kerberos model.

Option	Description
Use Kerberos for authentication only (krb5)	Supports identity verification
Use Kerberos for authentication and data integrity (krb5i)	In addition to identity verification, provides data integrity services. These services help to protect the NFS traffic from tampering by checking data packets for any potential modifications.

   If you do not enable Kerberos, the datastore uses the default AUTH_SYS security.

7 If you are creating a datastore at the data center or cluster level, select hosts that mount the datastore.

8 Review the configuration options and click Finish.

Create a vVols Datastore

You use the New Datastore wizard to create a vVols datastore.

Procedure

1 In the vSphere Client object navigator, browse to a host, a cluster, or a data center.

2 From the right-click menu, select Storage > New Datastore.

3 Select vVol as the datastore type.

4 Enter the datastore name and select a backing storage container from the list of storage containers.

   Make sure to use the name that does not duplicate another datastore name in your data center environment.

   If you mount the same vVols datastore to several hosts, the name of the datastore must be consistent across all hosts.

5 Select the hosts that require access to the datastore.

6 Review the configuration options and click Finish.

What to do next

After you create the vVols datastore, you can perform such datastore operations as renaming the datastore, browsing datastore files, unmounting the datastore, and so on.

You cannot add the vVols datastore to a datastore cluster.

vSphere Storage Update 1 - VMware vSphere 7.0, page 207

Administrative Operations for Datastores

After creating datastores, you can perform several administrative operations on the datastores. Certain operations, such as renaming a datastore, are available for all types of datastores. Others apply to specific types of datastores.

- Change Datastore Name

  Use the vSphere Client to change the name of an existing datastore. You can rename the datastore that has virtual machines running on it without any negative impact.

- Unmount Datastores

  When you unmount a datastore, it remains intact, but can no longer be seen from the hosts that you specify. The datastore continues to appear on other hosts, where it remains mounted.

- Mount Datastores

  You can mount a datastore you previously unmounted. You can also mount a datastore on additional hosts, so that it becomes a shared datastore.

- Remove VMFS Datastores

  You can delete any type of VMFS datastore, including copies that you have mounted without resignaturing. When you delete a datastore, it is destroyed and disappears from all hosts that have access to the datastore.

- Use Datastore Browser

  Use the datastore file browser to manage contents of your datastores. You can browse folders and files that are stored on the datastore. You can also use the browser to upload files and perform administrative tasks on your folders and files.

- Turn Off Storage Filters

  When you perform VMFS datastore management operations, vCenter Server uses default storage protection filters. The filters help you to avoid storage corruption by retrieving only the storage devices that can be used for a particular operation. Unsuitable devices are not displayed for selection. You can turn off the filters to view all devices.

Change Datastore Name

Use the vSphere Client to change the name of an existing datastore. You can rename the datastore that has virtual machines running on it without any negative impact.

Note If the host is managed by vCenter Server, you cannot rename the datastore by directly accessing the host from the VMware Host Client. You must rename the datastore from vCenter Server.

Procedure

1 In the vSphere Client, navigate to the datastore.

2 Right-click the datastore to rename, and select Rename.

3 Enter a new datastore name.

The system enforces a 42 character limit for the datastore name.

Results

The new name appears on all hosts that have access to the datastore.

Unmount Datastores

When you unmount a datastore, it remains intact, but can no longer be seen from the hosts that you specify. The datastore continues to appear on other hosts, where it remains mounted.

Do not perform any configuration operations that might result in I/O to the datastore while the unmounting is in progress.

Note Make sure that the datastore is not used by vSphere HA Heartbeating. vSphere HA Heartbeating does not prevent you from unmounting the datastore. However, if the datastore is used for heartbeating, unmounting it might cause the host to fail and restart any active virtual machine.

Prerequisites

When appropriate, before unmounting datastores, make sure that the following prerequisites are met:

- No virtual machines reside on the datastore.

- Storage DRS does not manage the datastore.
- Storage I/O Control is disabled for this datastore.

Procedure

1 In the vSphere Client, navigate to the datastore.

2 Right-click the datastore and select Unmount Datastore.

3 If the datastore is shared, select the hosts from which to unmount the datastore.

4 Confirm that you want to unmount the datastore.

Results

After you unmount a VMFS datastore from all hosts, the datastore is marked as inactive. If you unmount an NFS or a vVols datastore from all hosts, the datastore disappears from the inventory. You can mount the unmounted VMFS datastore. To mount the NFS or vVols datastore that has been removed from the inventory, use the New Datastore wizard.

What to do next

If you unmounted the VMFS datastore as a part of a storage removal procedure, you can now detach the storage device that is backing the datastore. See Detach Storage Devices.

Mount Datastores

You can mount a datastore you previously unmounted. You can also mount a datastore on additional hosts, so that it becomes a shared datastore.

A VMFS datastore that has been unmounted from all hosts remains in inventory, but is marked as inaccessible. You can use this task to mount the VMFS datastore to a specified host or multiple hosts.

If you have unmounted an NFS or a vVols datastore from all hosts, the datastore disappears from the inventory. To mount the NFS or vVols datastore that has been removed from the inventory, use the New Datastore wizard.

A datastore of any type that is unmounted from some hosts while being mounted on others, is shown as active in the inventory.

Procedure

1 In the vSphere Client, navigate to the datastore.

2 Right-click the datastore to mount and select one of the following options:

   - Mount Datastore
   - Mount Datastore on Additional Hosts

3 Whether you see one or another option depends on the type of datastore you use.

4 Select the hosts that should access the datastore and click OK.

5 To list all hosts that share the datastore, navigate to the datastore, and click the Hosts tab.

Remove VMFS Datastores

You can delete any type of VMFS datastore, including copies that you have mounted without resignaturing. When you delete a datastore, it is destroyed and disappears from all hosts that have access to the datastore.

Note The delete operation for the datastore permanently deletes all files associated with virtual machines on the datastore. Although you can delete the datastore without unmounting, it is preferable that you unmount the datastore first.

Prerequisites

- Remove or migrate all virtual machines from the datastore.
- Unmount the datastore from all hosts.
- Disable Storage DRS for the datastore.
- Disable Storage I/O Control for the datastore.
- Make sure that the datastore is not used for vSphere HA heartbeating.

Procedure

1 In the vSphere Client, navigate to the datastore.

2 Right-click the datastore to remove, and select Delete Datastore.

3 Confirm that you want to remove the datastore.

Use Datastore Browser

Use the datastore file browser to manage contents of your datastores. You can browse folders and files that are stored on the datastore. You can also use the browser to upload files and perform administrative tasks on your folders and files.

Procedure

1 Open the datastore browser.

a Display the datastore in the inventory.

b Right-click the datastore and select Browse Files.

2 Explore the contents of the datastore by navigating to existing folders and files.

3 Perform administrative tasks by using the icons and options.

Icons and Options	Descriptions
Upload Files	Upload a file to the datastore.
Upload Folder (Available only in the vSphere Client)	Upload a folder to the datastore.
Download	Download from the datastore.
New Folder	Create a folder on the datastore.
Copy to	Copy selected folders or files to a new location, either on the same datastore or on a different datastore.
Move to	Move selected folders or files to a new location, either on the same datastore or on a different datastore.
Rename to	Rename selected files.
Delete	Delete selected folders or files.
Inflate	Convert a selected thin virtual disk to thick. This option applies only to thin-provisioned disks.

Upload Files or Folders to Datastores

Use the datastore file browser to upload files to datastores on the ESXi host. If you use the vSphere Client, you can also upload folders.

In addition to their traditional use as storage for virtual machines files, datastores can serve to store data or files related to virtual machines. For example, you can upload ISO images of operating systems from a local computer to a datastore on the host. You then use these images to install guest operating systems on the new virtual machines.

Note You cannot upload files directly to the vVols datastores. You must first create a folder on the vVols datastore, and then upload the files into the folder. The created folders in vVols datastores for block storage have a limited storage capacity space of 4GB. The vVols datastore supports direct uploads of folders.

Prerequisites

Required privilege: Datastore.Browse Datastore

Procedure

1 Open the datastore browser.

   a Display the datastore in the inventory.

   b Right-click the datastore and select Browse Files.

2 (Optional) Create a folder to store the file or folder.

3 Upload the file or folder.

Option	Description
Upload a file	a Select the target folder and click Upload Files.

	b	Locate the item to upload on the local computer and click Open.
Upload a folder (available only in the vSphere Client)	a	Select the datastore or the target folder and click Upload Folders.
	b	Locate the item to upload on the local computer and click Ok.

4 Refresh the datastore file browser to see the uploaded files or folders on the list.

What to do next

You might experience problems when deploying an OVF template that you previously exported and then uploaded to a datastore. For details and a workaround, see the VMware Knowledge Base article 2117310.

Download Files from Datastores

Use the datastore file browser to download files from the datastore available on your ESXi host to your local computer.

Prerequisites

Required privilege: Datastore.Browse Datastore

Procedure

1 Open the datastore browser.

a Display the datastore in the inventory.

b Right-click the datastore and select Browse Files.

2 Navigate to the file to download and click Download.

3 Follow the prompts to save the file to your local computer.

Move or Copy Datastore Folders or Files

Use the datastore browser to move or copy folders or files to a new location, either on the same datastore or on a different datastore.

Note Virtual disk files are moved or copied without format conversion. If you move a virtual disk to a datastore that belongs to a host different from the source host, you might need to convert the virtual disk. Otherwise, you might not be able to use the disk.

You cannot copy VM files across vCenter Servers.

Prerequisites

Required privilege: Datastore.Browse Datastore

Procedure

1 Open the datastore browser.

a Display the datastore in the inventory.

b Right-click the datastore and select Browse Files.

2 Browse to an object you want to move or copy, either a folder or a file.

3 Select the object and click Move to or Copy to.

4 Specify the destination location.

5 (Optional) Select Overwrite files and folders with matching names at the destination.

6 Click OK.

Rename Datastore Files

Use the datastore browser to rename files.

Prerequisites

Required privilege: Datastore.Browse Datastore

Procedure

1 Open the datastore browser.

a Display the datastore in the inventory.

b Right-click the datastore and select Browse Files.

2 Browse to a file you want to rename.

3 Select the file and click Rename to.

4 Specify the new name and click OK.

Inflate Thin Virtual Disks

If you created a virtual disk in the thin format, you can change the format to thick.

You use the datastore browser to inflate the thin virtual disk.

Prerequisites

- Make sure that the datastore where the virtual machine resides has enough space.
- Make sure that the virtual disk is thin.
- Remove snapshots.
- Power off your virtual machine.

Procedure

1 In the vSphere Client, navigate to the folder of the virtual disk you want to inflate.

a Navigate to the virtual machine.

b Click the Datastores tab.

The datastore that stores the virtual machine files is listed.

c Right-click the datastore and select Browse Files.

The datastore browser displays contents of the datastore.

2 Expand the virtual machine folder and browse to the virtual disk file that you want to convert.

The file has the .vmdk extension and is marked with the virtual disk () icon.

3 Select the virtual disk file and click Inflate.

Note The option might not be available if the virtual disk is thick or when the virtual machine is running.

Results

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

Turn Off Storage Filters

When you perform VMFS datastore management operations, vCenter Server uses default storage protection filters. The filters help you to avoid storage corruption by retrieving only the storage devices that can be used for a particular operation. Unsuitable devices are not displayed for selection. You can turn off the filters to view all devices.

Prerequisites

Before you change the device filters, consult with the VMware support team.

Procedure

1 Browse to the vCenter Server instance.

2 Click the Configure tab.

3 Under Settings, click Advanced Settings, and click EDIT SETTINGS.

4 Specify the filter to turn off.

In the Name and Value text boxes at the bottom of the page, enter appropriate information.

Name	Value
config.vpxd.filter.vmfsFilter	False
config.vpxd.filter.rdmFilter	False
config.vpxd.filter.sameHostsAndTransportsFilter	False
config.vpxd.filter.hostRescanFilter	False Note If you turn off this filter, your hosts continue to perform a rescan each time you present a new LUN to a host or a cluster.

5 Click ADD, and click SAVE to save your changes.

You are not required to restart the vCenter Server system.

Storage Filtering

vCenter Server provides storage filters to help you avoid storage device corruption or performance degradation that might be caused by an unsupported use of storage devices. These filters are available by default.

Table 17-6. Storage Filters

Filter Name	Description
config.vpxd.filter.vmfsFilter (VMFS Filter)	Filters out storage devices, or LUNs, that are already used by a VMFS datastore on any host managed by vCenter Server. The LUNs do not show up as candidates to be formatted with another VMFS datastore or to be used as an RDM.
config.vpxd.filter.rdmFilter (RDM Filter)	Filters out LUNs that are already referenced by an RDM on any host managed by vCenter Server. The LUNs do not show up as candidates to be formatted with VMFS or to be used by a different RDM. For your virtual machines to access the same LUN, the virtual machines must share the same RDM mapping file. For information about this type of configuration, see the *vSphere Resource Management* documentation.
config.vpxd.filter.sameHostsAndTransportsFilter (Same Hosts and Transports Filter)	Filters out LUNs ineligible for use as VMFS datastore extents because of host or storage type incompatibility. Prevents you from adding the following LUNs as extents: • LUNs not exposed to all hosts that share the original VMFS datastore. • LUNs that use a storage type different from the one the original VMFS datastore uses. For example, you cannot add a Fibre Channel extent to a VMFS datastore on a local storage device.
config.vpxd.filter.hostRescanFilter (Host Rescan Filter)	Automatically rescans and updates VMFS datastores after you perform datastore management operations. The filter helps provide a consistent view of all VMFS datastores on all hosts managed by vCenter Server. Note If you present a new LUN to a host or a cluster, the hosts automatically perform a rescan no matter whether you have the Host Rescan Filter on or off.

Objective 4.3
Identify how to configure vSphere HA.

vSphere Availability Update 1 - VMware vSphere 7.0, page 11

How vSphere HA Works

vSphere HA provides high availability for virtual machines by pooling the virtual machines and the hosts they reside on into a cluster. Hosts in the cluster are monitored and in the event of a failure, the virtual machines on a failed host are restarted on alternate hosts.

When you create a vSphere HA cluster, a single host is automatically elected as the primary host. The primary host communicates with vCenter Server and monitors the state of all protected virtual machines and of the secondary hosts. Different types of host failures are possible, and the primary host must detect and appropriately deal with the failure. The primary host must distinguish between a failed host and one that is in a network partition or that has become network isolated. The primary host uses network and datastore heartbeating to determine the type of failure.

Sphere HA Clusters
(http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:vSphereHAClusters)

Primary and Secondary Hosts

When you add a host to a vSphere HA cluster, an agent is uploaded to the host and configured to communicate with other agents in the cluster. Each host in the cluster functions as a primary host or a secondary host.

When vSphere HA is enabled for a cluster, all active hosts (that are not in standby, maintenance mode or not disconnected) participate in an election to choose the cluster's primary host. The host that mounts the greatest number of datastores has an advantage in the election. Only one primary host typically exists per cluster and all other hosts are secondary hosts. If the primary host fails, is shut down or put in standby mode, or is removed from the cluster a new election is held.

The primary host in a cluster has several responsibilities:

- Monitoring the state of secondary hosts. If a secondary host fails or becomes unreachable, the primary host identifies which virtual machines must be restarted.

- Monitoring the power state of all protected virtual machines. If one virtual machine fails, the primary host ensures that it is restarted. Using a local placement engine, the primary host also determines where the restart takes place.

- Managing the lists of cluster hosts and protected virtual machines.

- Acting as the vCenter Server management interface to the cluster and reporting the cluster health state.

The secondary hosts primarily contribute to the cluster by running virtual machines locally, monitoring their runtime states, and reporting state updates to the primary host. A primary host can also run and monitor virtual machines. Both secondary hosts and primary hosts implement the VM and Application Monitoring features.

One of the functions performed by the primary host is to orchestrate restarts of protected virtual machines. A virtual machine is protected by a primary host after vCenter Server observes that the virtual machine's power state has changed from powered off to powered on in response to a user action. The primary host persists the list of protected virtual machines in the cluster's datastores. A newly elected primary host uses this information to determine which virtual machines to protect.

Note If you disconnect a host from a cluster, the virtual machines registered to that host are unprotected by vSphere HA.

Host Failure Types

The primary host of a VMware vSphere® High Availability cluster is responsible for detecting the failure of secondary hosts. Depending on the type of failure detected, the virtual machines running on the hosts might need to be failed over.

In a vSphere HA cluster, three types of host failure are detected:

- Failure. A host stops functioning.
- Isolation. A host becomes network isolated.
- Partition. A host loses network connectivity with the primary host.

The primary host monitors the liveness of the secondary hosts in the cluster. This communication happens through the exchange of network heartbeats every second. When the primary host stops receiving these heartbeats from a secondary host, it checks for host liveness before declaring the host failed. The liveness check that the primary host performs is to determine whether the secondary host is exchanging heartbeats with one of the datastores. See Datastore Heartbeating . Also, the primary host checks whether the host responds to ICMP pings sent to its management IP addresses.

If a primary host cannot communicate directly with the agent on a secondary host, the secondary host does not respond to ICMP pings. If the agent is not issuing heartbeats, it is viewed as failed. The host's virtual machines are restarted on alternate hosts. If such a secondary host is exchanging heartbeats with a datastore, the primary host assumes that the secondary host is in a network partition or is network isolated. So, the primary host continues to monitor the host and its virtual machines. See Network Partitions.

Host network isolation occurs when a host is still running, but it can no longer observe traffic from vSphere HA agents on the management network. If a host stops observing this traffic, it attempts to ping the cluster isolation addresses. If this pinging also fails, the host declares that it is isolated from the network.

The primary host monitors the virtual machines that are running on an isolated host. If the primary host observes that the VMs power off, and the primary host is responsible for the VMs, it restarts them.

Note If you ensure that the network infrastructure is sufficiently redundant and that at least one network path is always available, host network isolation is less likely to occur.

Proactive HA Failures

A Proactive HA failure occurs when a host component fails, which results in a loss of redundancy or a noncatastrophic failure. However, the functional behavior of the VMs residing on the host is not yet affected. For example, if a power supply on the host fails, but other power supplies are available, that is a Proactive HA failure.

If a Proactive HA failure occurs, you can automate the remediation action taken in the vSphere Availability section of the vSphere Client. The VMs on the affected host can be evacuated to other hosts and the host is either placed in Quarantine mode or Maintenance mode.

Note Your cluster must use vSphere DRS for the Proactive HA failure monitoring to work.

Determining Responses to Host Issues

If a host fails and its virtual machines must be restarted, you can control the order in which the virtual machines are restarted with the VM restart priority setting. You can also configure how vSphere HA responds if hosts lose management network connectivity with other hosts by using the host isolation response setting. Other factors are also considered when vSphere HA restarts a virtual machine after a failure.

The following settings apply to all virtual machines in the cluster in the case of a host failure or isolation. You can also configure exceptions for specific virtual machines. See Customize an Individual Virtual Machine.

Host Isolation Response

Host isolation response determines what happens when a host in a vSphere HA cluster loses its management network connections, but continues to run. You can use the isolation response to have vSphere HA power off virtual machines that are running on an isolated host and restart them on a non-isolated host. Host isolation responses require that Host Monitoring Status is enabled. If Host Monitoring Status is disabled, host isolation responses are also suspended. A host determines that it is isolated when it is unable to communicate with the agents running on the other hosts, and it is unable to ping its isolation addresses. The host then executes its isolation response. The responses are Power off and restart VMs or Shutdown and restart VMs. You can customize this property for individual virtual machines.

Note If a virtual machine has a restart priority setting of Disabled, no host isolation response is made.

To use the Shutdown and restart VMs setting, you must install VMware Tools in the guest operating system of the virtual machine. Shutting down the virtual machine provides the advantage of preserving its state. Shutting down is better than powering off the virtual machine, which does not flush most recent changes to disk or commit transactions. Virtual machines that are in the process of shutting down take longer to fail over while the shutdown completes. Virtual Machines that have not shut down in 300 seconds, or the time specified in the advanced option das.isolationshutdowntimeout, are powered off.

After you create a vSphere HA cluster, you can override the default cluster settings for Restart Priority and Isolation Response for specific virtual machines. Such overrides are useful for virtual machines that are used for special tasks. For example, virtual machines that provide infrastructure services like DNS or DHCP might need to be powered on before other virtual machines in the cluster.

A virtual machine "split-brain" condition can occur when a host becomes isolated or partitioned from a primary host and the primary host cannot communicate with it using heartbeat datastores. In this situation, the primary host cannot determine that the host is alive and so declares it dead. The primary host then attempts to restart the virtual machines that are running on the isolated or partitioned host. This attempt succeeds if the virtual machines remain running on the isolated/partitioned host and that host lost access to the virtual machines' datastores when it became isolated or partitioned. A split-brain condition then exists because there are two instances of the virtual machine. However, only one instance is able to read or write the virtual machine's virtual disks. VM Component Protection can be used to prevent this split-brain condition. When you enable VMCP with the aggressive setting, it monitors the datastore accessibility of powered-on virtual machines, and shuts down those that lose access to their datastores.

To recover from this situation, ESXi generates a question on the virtual machine that has lost the disk locks for when the host comes out of isolation and cannot reacquire the disk locks. vSphere HA automatically answers this question, allowing the virtual machine instance that has lost the disk locks to power off, leaving just the instance that has the disk locks.

Virtual Machine Dependencies

You can create dependencies between groups of virtual machines. To do so, you must first create the VM groups in the vSphere Client by going to the Configure tab for the cluster and selecting VM/Host Groups. Once the groups have been created, you can create restart dependency rules between the groups by browsing toVM/Host Rules and in the Type drop-down menu, select Virtual Machines to Virtual Machines. These rules can specify that certain VM groups cannot be restarted until other, specified VM groups have been Ready first.

Factors Considered for Virtual Machine Restarts

After a failure, the cluster's primary host attempts to restart affected virtual machines by identifying a host that can power them on. When choosing such a host, the primary host considers a number of factors.

File accessibility

Before a virtual machine can be started, its files must be accessible from one of the active cluster hosts that the primary can communicate with over the network

Virtual machine and host compatibility

If there are accessible hosts, the virtual machine must be compatible with at least one of them. The compatibility set for a virtual machine includes the effect of any required VM-Host affinity rules. For example, if a rule only permits a virtual machine to run on two hosts, it is considered for placement on those two hosts.

Resource reservations

Of the hosts that the virtual machine can run on, at least one must have sufficient unreserved capacity to meet the memory overhead of the virtual machine and any resource reservations. Four types of reservations are considered: CPU, Memory, vNIC, and Virtual flash. Also, sufficient network ports must be available to power on the virtual machine.

Host limits

In addition to resource reservations, a virtual machine can only be placed on a host if doing so does not violate the maximum number of allowed virtual machines or the number of in-use vCPUs.

Feature constraints

If the advanced option has been set that requires vSphere HA to enforce VM to VM anti-affinity rules, vSphere HA does not violate this rule. Also, vSphere HA does not violate any configured per host limits for fault tolerant virtual machines.
If no hosts satisfy the preceding considerations, the primary host issues an event stating that there are not enough resources for vSphere HA to start the VM and tries again when the cluster conditions have changed. For example, if the virtual machine is not accessible, the primary host tries again after a change in file accessibility.

VM and Application Monitoring

VM Monitoring restarts individual virtual machines if their VMware Tools heartbeats are not received within a set time. Similarly, Application Monitoring can restart a virtual machine if the heartbeats for an application it is running are not received. You can enable these features and configure the sensitivity with which vSphere HA monitors non-responsiveness.

When you enable VM Monitoring, the VM Monitoring service (using VMware Tools) evaluates whether each virtual machine in the cluster is running by checking for regular heartbeats and I/O activity from the VMware Tools process running inside the guest. If no heartbeats or I/O activity are received, this is most likely because the guest operating system has failed or VMware Tools is not being allocated any time to complete tasks. In such a case, the VM Monitoring service determines that the virtual machine has failed and the virtual machine is rebooted to restore service.

Occasionally, virtual machines or applications that are still functioning properly stop sending heartbeats. To avoid unnecessary resets, the VM Monitoring service also monitors a virtual machine's I/O activity. If no heartbeats are received within the failure interval, the I/O stats interval (a cluster-level attribute) is checked. The I/O stats interval determines if any disk or network activity has occurred for the virtual machine during the previous two minutes (120 seconds). If not, the virtual machine is reset. This default value (120 seconds) can be changed using the advanced option das.iostatsinterval.

To enable Application Monitoring, you must first obtain the appropriate SDK (or be using an application that supports VMware Application Monitoring) and use it to set up customized heartbeats for the applications you want to monitor. After you have done this, Application Monitoring works much the same way that VM Monitoring does. If the heartbeats for an application are not received for a specified time, its virtual machine is restarted.

You can configure the level of monitoring sensitivity. Highly sensitive monitoring results in a more rapid conclusion that a failure has occurred. While unlikely, highly sensitive monitoring might lead to falsely identifying failures when the virtual machine or application in question is actually still working, but heartbeats have not been received due to factors such as resource constraints. Low sensitivity monitoring results in longer interruptions in service between actual failures and virtual machines being reset. Select an option that is an effective compromise for your needs.

You can also specify custom values for both monitoring sensitivity and the I/O stats interval by selecting the Custom checkbox.

Table 2-1. VM Monitoring Settings

Setting	Failure Interval (seconds)	Reset Period
High	30	1 hour
Medium	60	24 hours
Low	120	7 days

After failures are detected, vSphere HA resets virtual machines. The reset ensures that services remain available. To avoid resetting virtual machines repeatedly for nontransient errors, by default, virtual machines will be reset only three times during a certain configurable time interval. After virtual machines have been reset three times, vSphere HA makes no further attempts to reset the virtual machines after subsequent failures until after the specified time has elapsed. You can configure the number of resets using the Maximum per-VM resets custom setting.

Note The reset statistics are cleared when a virtual machine is powered off then back on, or when it is migrated using vMotion to another host. This causes the guest operating system to reboot, but is not the same as a 'restart' in which the power state of the virtual machine is changed.

VM Component Protection

If VM Component Protection (VMCP) is enabled, vSphere HA can detect datastore accessibility failures and provide automated recovery for affected virtual machines.

VMCP provides protection against datastore accessibility failures that can affect a virtual machine running on a host in a vSphere HA cluster. When a datastore accessibility failure occurs, the affected host can no longer access the storage path for a specific datastore. You can determine the response that vSphere HA will make to such a failure, ranging from the creation of event alarms to virtual machine restarts on other hosts.

Note When you use the VM Component Protection feature, your ESXi hosts must be version 6.0 or higher.

Types of Failure

There are two types of datastore accessibility failure:

PDL

PDL (Permanent Device Loss) is an unrecoverable loss of accessibility that occurs when a storage device reports the datastore is no longer accessible by the host. This condition cannot be reverted without powering off virtual machines.

APD

APD (All Paths Down) represents a transient or unknown accessibility loss or any other unidentified delay in I/O processing. This type of accessibility issue is recoverable.

Configuring VMCP

VM Component Protection is configured in the vSphere Client. Go to the Configure tab and click vSphere Availability and Edit. Under Failures and Responses you can select Datastore with PDL or Datastore with APD. The storage protection levels you can choose and the virtual machine remediation actions available differ depending on the type of database accessibility failure.

PDL Failures

Under Datastore with PDL, you can select Issue events or Power off and restart VMs.

APD Failures

The response to APD events is more complex and accordingly the configuration is more fine-grained. You can select Issue events, Power off and restart VMs--conservative restart policy, or Power off and restart VMs--aggressive restart policy

Note If either the Host Monitoring or VM Restart Priority settings are disabled, VMCP cannot perform virtual machine restarts. Storage health can still be monitored and events can be issued, however.

Network Partitions

When a management network failure occurs for a vSphere HA cluster, a subset of the cluster's hosts might be unable to communicate over the management network with the other hosts. Multiple partitions can occur in a cluster.

A partitioned cluster leads to degraded virtual machine protection and cluster management functionality. Correct the partitioned cluster as soon as possible.

- Virtual machine protection. vCenter Server allows a virtual machine to be powered on, but it can be protected only if it is running in the same partition as the primary host that is responsible for it. The primary host must be communicating with vCenter Server. A primary host is responsible for a virtual machine if it has exclusively locked a system-defined file on the datastore that contains the virtual machine's configuration file.

- Cluster management. vCenter Server can communicate with the primary host, but only a subset of the secondary hosts. As a result, changes in configuration that affect vSphere HA might not take effect until after the partition is resolved. This failure could result in one of the partitions operating under the old configuration, while another uses the new settings.

Datastore Heartbeating

When the primary host in a VMware vSphere® High Availability cluster cannot communicate with a secondary host over the management network, the primary host uses datastore heartbeating to determine whether the secondary host has failed, is in a network partition, or is network isolated. If the secondary host has stopped datastore heartbeating, it is considered to have failed and its virtual machines are restarted elsewhere.

VMware vCenter Server® selects a preferred set of datastores for heartbeating. This selection is made to maximize the number of hosts that have access to a heartbeating datastore and minimize the likelihood that the datastores are backed by the same LUN or NFS server.

You can use the advanced option das.heartbeatdsperhost to change the number of heartbeat datastores selected by vCenter Server for each host. The default is two and the maximum valid value is five.

vSphere HA creates a directory at the root of each datastore that is used for both datastore heartbeating and for persisting the set of protected virtual machines. The name of the directory is .vSphere-HA. Do not delete or modify the files stored in this directory, because this can have an impact on operations. Because more than one cluster might use a datastore, subdirectories for this directory are created for each cluster. Root owns these directories and files and only root can read and write to them. The disk space used by vSphere HA depends on several factors including which VMFS version is in use and the number of hosts that use the datastore for heartbeating. With vmfs3, the maximum usage is 2GB and the typical usage is 3MB. With vmfs5, the maximum and typical usage is 3MB. vSphere HA use of the datastores adds negligible overhead and has no performance impact on other datastore operations.

vSphere HA limits the number of virtual machines that can have configuration files on a single datastore. See *Configuration Maximums* for updated limits. If you place more than this number of virtual machines on a datastore and power them on, vSphere HA protects virtual machines only up to the limit.

Note A vSAN datastore cannot be used for datastore heartbeating. Therefore, if no other shared storage is accessible to all hosts in the cluster, there can be no heartbeat datastores in use. However, if you have storage that is accessible by an alternate network path independent of the vSAN network, you can use it to set up a heartbeat datastore.

vSphere HA Security

vSphere HA is enhanced by several security features.

Select firewall ports opened

vSphere HA uses TCP and UDP port 8182 for agent-to-agent communication. The firewall ports open and close automatically to ensure they are open only when needed.

Configuration files protected using file system permissions

vSphere HA stores configuration information on the local storage or on ramdisk if there is no local datastore. These files are protected using file system permissions and they are accessible only to the root user. Hosts without local storage are only supported if they are managed by Auto Deploy.

Detailed logging

The location where vSphere HA places log files depends on the version of host.

- For ESXi 5.x hosts, vSphere HA writes to syslog only by default, so logs are placed where syslog is configured to put them. The log file names for vSphere HA are prepended with fdm, fault domain manager, which is a service of vSphere HA.

- For legacy ESXi 4.x hosts, vSphere HA writes to /var/log/vmware/fdm on local disk, as well as syslog if it is configured.

- For legacy ESX 4.x hosts, vSphere HA writes to /var/log/vmware/fdm.

Secure vSphere HA logins

vSphere HA logs onto the vSphere HA agents using a user account, vpxuser, created by vCenter Server. This account is the same account used by vCenter Server to manage the host. vCenter Server creates a random password for this account and changes the password periodically. The time period is set by the vCenter Server VirtualCenter.VimPasswordExpirationInDays setting. Users with administrative privileges on the root folder of the host can log in to the agent.

Secure communication

All communication between vCenter Server and the vSphere HA agent is done over SSL. Agent-to-agent communication also uses SSL except for election messages, which occur over UDP. Election messages are verified over SSL so that a rogue agent can prevent only the host on which the agent is running from being elected as a primary host. In this case, a configuration issue for the cluster is issued so the user is aware of the problem.

Host SSL certificate verification required

vSphere HA requires that each host have a verified SSL certificate. Each host generates a self-signed certificate when it is booted for the first time. This certificate can then be regenerated or replaced with one issued by an authority. If the certificate is replaced, vSphere HA needs to be reconfigured on the host. If a host becomes disconnected from vCenter Server after its certificate is updated and the ESXi or ESX Host agent is restarted, then vSphere HA is automatically reconfigured when the host is reconnected to vCenter Server. If the disconnection does not occur because vCenter Server host SSL certificate verification is disabled at the time, verify the new certificate and reconfigure vSphere HA on the host.

vSphere Availability Update 1 - VMware vSphere 7.0, page 34

Creating a vSphere HA Cluster

vSphere HA operates in the context of a cluster of ESXi (or legacy ESX) hosts. You must create a cluster, populate it with hosts, and configure vSphere HA settings before failover protection can be established.

When you create a vSphere HA cluster, you must configure a number of settings that determine how the feature works. Before you do this, identify your cluster's nodes. These nodes are the ESXi hosts that will provide the resources to support virtual machines and that vSphere HA will use for failover protection. You should then determine how those nodes are to be connected to one another and to the shared storage where your virtual machine data resides. After that networking architecture is in place, you can add the hosts to the cluster and finish configuring vSphere HA.

You can enable and configure vSphere HA before you add host nodes to the cluster. However, until the hosts are added, your cluster is not fully operational and some of the cluster settings are unavailable. For example, the Specify a Failover Host admission control policy is unavailable until there is a host that can be designated as the failover host.

Note The Virtual Machine Startup and Shutdown (automatic startup) feature is disabled for all virtual machines residing on hosts that are in (or moved into) a vSphere HA cluster. Automatic startup is not supported when used with vSphere HA.

vSphere HA Checklist

The vSphere HA checklist contains requirements that you must be aware of before creating and using a vSphere HA cluster.

Review this list before you set up a vSphere HA cluster. For more information, follow the appropriate cross reference.

- All hosts must be licensed for vSphere HA.
- A cluster must contain at least two hosts.
- All hosts must be configured with static IP addresses. If you are using DHCP, you must ensure that the address for each host persists across reboots.
- All hosts must have at least one management network in common. The best practice is to have at least two management networks in common. You should use the VMkernel network with the Management traffic checkbox enabled. The networks must be accessible to each other and vCenter Server and the hosts must be accessible to each other on the management networks. See Best Practices for Networking.
- To ensure that any virtual machine can run on any host in the cluster, all hosts must have access to the same virtual machine networks and datastores. Similarly, virtual machines must be located on shared, not local, storage otherwise they cannot be failed over in the case of a host failure.

  Note vSphere HA uses datastore heartbeating to distinguish between partitioned, isolated, and failed hosts. So if some datastores are more reliable in your environment, configure vSphere HA to give preference to them.
- For VM Monitoring to work, VMware tools must be installed. See VM and Application Monitoring.

- vSphere HA supports both IPv4 and IPv6. See Other vSphere HA Interoperability Issues for considerations when using IPv6.

- For VM Component Protection to work, hosts must have the All Paths Down (APD) Timeout feature enabled.

- To use VM Component Protection, clusters must contain ESXi 6.0 hosts or later.

- Only vSphere HA clusters that contain ESXi 6.0 or later hosts can be used to enable VMCP. Clusters that contain hosts from an earlier release cannot enable VMCP, and such hosts cannot be added to a VMCP-enabled cluster.

- If your cluster uses Virtual Volume datastores, when vSphere HA is enabled a configuration Virtual Volume is created on each datastore by vCenter Server. In these containers, vSphere HA stores the files it uses to protect virtual machines. vSphere HA does not function correctly if you delete these containers. Only one container is created per Virtual Volume datastore.

Create a vSphere HA Cluster in the vSphere Client

To enable your cluster for vSphere HA, you must first create an empty cluster. After you plan the resources and networking architecture of your cluster, use the vSphere Client to add hosts to the cluster and specify the cluster's vSphere HA settings.

A vSphere HA-enabled cluster is a prerequisite for vSphere Fault Tolerance.

Prerequisites

- Verify that all virtual machines and their configuration files reside on shared storage.

- Verify that the hosts are configured to access the shared storage so that you can power on the virtual machines by using different hosts in the cluster.

- Verify that hosts are configured to have access to the virtual machine network.

- Verify that you are using redundant management network connections for vSphere HA. For information about setting up network redundancy, see Best Practices for Networking.

- Verify that you have configured hosts with at least two datastores to provide redundancy for vSphere HA datastore heartbeating.

- Connect vSphere Client to vCenter Server by using an account with cluster administrator permissions.

Procedure

1 In the vSphere Client, browse to the data center where you want the cluster to reside and click New Cluster.

2 Complete the New Cluster wizard.

Do not turn on vSphere HA (or DRS).

3 Click OK to close the wizard and create an empty cluster.

4 Based on your plan for the resources and networking architecture of the cluster, use the vSphere Client to add hosts to the cluster.

5 Browse to the cluster and enable vSphere HA.

a Click the Configure tab.

b Select vSphere Availability and click Edit.

c Select vSphere HA.

6 Under Failures and Responses select Enable Host Monitoring.

With Host Monitoring enabled, hosts in the cluster can exchange network heartbeats and vSphere HA can take action when it detects failures. Host Monitoring is required for the vSphere Fault Tolerance recovery process to work properly.

7 Select a setting for VM Monitoring.

Select VM Monitoring Only to restart individual virtual machines if their heartbeats are not received within a set time. You can also select VM and Application Monitoring to enable application monitoring.

8 Click OK.

Results

You have a vSphere HA cluster, populated with hosts.

What to do next

Configure the appropriate vSphere HA settings for your cluster.

- Failures and responses
- Admission Control
- Heartbeat Datastores
- Advanced Options

See Configuring vSphere Availability Settings.

Configuring vSphere Availability Settings

When you create a vSphere HA cluster or configure an existing cluster, you must configure settings that determine how the feature works.

In the vSphere Client, you can configure following the vSphere HA settings:

Failures and responses

Provide settings here for host failure responses, host isolation, VM monitoring, and VM Component Protection.

Admission Control

Enable or disable admission control for the vSphere HA cluster and choose a policy for how it is enforced.

Heartbeat Datastores

Specify preferences for the datastores that vSphere HA uses for datastore heartbeating.

Advanced Options

Customize vSphere HA behavior by setting advanced options.

Configuring Responses to Failures

The Failure and Responses pane of the vSphere HA settings allows you to configure how your cluster should function when problems are encountered.

In this part of the vSphere Client, you can determine the specific responses the vSphere HA cluster has for host failures and isolation. You can also configure VM Component Protection (VMCP) actions when Permanent Device Loss (PDL) and All Paths Down (APD) situations occur and you can enable VM monitoring.

The following tasks are available:

Procedure

1 Respond to Host Failure

You can set specific responses to host failures that occur in your vSphere HA cluster.

2 Respond to Host Isolation

You can set specific responses to host isolation that occurs in your vSphere HA cluster.

3 Configure VMCP Responses

Configure the response that VM Component Protection (VMCP) makes when a datastore encounters a PDL or APD failure.

4 Enable VM Monitoring

You can turn on VM and Application Monitoring and also set the monitoring sensitivity for your vSphere HA cluster.

Respond to Host Failure

You can set specific responses to host failures that occur in your vSphere HA cluster.

This page is editable only if you have enabled vSphere HA.

Procedure

1 In the vSphere Client, browse to the vSphere HA cluster.

2 Click the Configure tab.

3 Select vSphere Availability and click Edit.

4 Click Failures and Responses and then expand Host Failure Response.

5 Select from the following configuration options.

Option	Description
Failure Response	If you select Disabled, this setting turns off host monitoring and VMs are not restarted when host failures occur. If Restart VMs is selected, VMs are failed over based on their restart priority when a host fails.
Default VM Restart Priority	The restart priority determines the order in which virtual machines are restarted when the host fails. Higher priority virtual machines are started first. If multiple hosts fail, all virtual machines are migrated from the first host in order of priority, then all virtual machines from the second host in order of priority, and so on.
VM Restart Priority Condition	A specific condition must be selected as well as a delay after that condition has been met, before vSphere HA is allowed to continue to the next VM restart priority.

6 Click OK.

Results

Your settings for the host failure response take effect.

Respond to Host Isolation

You can set specific responses to host isolation that occurs in your vSphere HA cluster.

This page is editable only if you have enabled vSphere HA.

Procedure

1 In the vSphere Client, browse to the vSphere HA cluster.

2 Click the Configure tab.

3 Select vSphere Availability and click Edit.

4 Click Failures and Responses and expand Response for Host Isolation.

5 To configure the host isolation response, select Disabled, Shut down and restart VMs, or Power off and restart VMs.

6 Click OK.

Results

Your setting for the host isolation response takes effect.

Configure VMCP Responses

Configure the response that VM Component Protection (VMCP) makes when a datastore encounters a PDL or APD failure.

This page is editable only if you have enabled vSphere HA.

Procedure

1 In the vSphere Client, browse to the vSphere HA cluster.

2 Click the Configure tab.

3 Select vSphere Availability and click Edit.

4 Click Failures and Responses, and expand either Datastore with PDL or Datastore with APD .

5 If you clicked Datastore with PDL, you can set the VMCP failure response for this type of issue, either Disabled, Issue Events, or Power off and restart VMs.

6 If you clicked Datastore with APD, you can set the VMCP failure response for this type of issue, either Disabled, Issue Events, Power off and restart VMs--Conservative restart policy, or Power off and restart VMs--Aggressive restart policy. You can also set Response recovery, which is the number of minutes that VMCP waits before taking action.

7 Click OK.

Results

Your settings for the VMCP failure response take effect.

Enable VM Monitoring

You can turn on VM and Application Monitoring and also set the monitoring sensitivity for your vSphere HA cluster.

This page is editable only if you have enabled vSphere HA.

Procedure

1 In the vSphere Client, browse to the vSphere HA cluster.

2 Click the Configure tab.

3 Select vSphere Availability and click Edit.

4 Click Failures and Responses and expand VM Monitoring.

5 Select VM Monitoring and Application Monitoring.

These settings turn on VMware Tools heartbeats and application heartbeats, respectively.

6 To set the heartbeat monitoring sensitivity, move the slider between Low and High or select Custom to provide custom settings.

7 Click OK.

Results

Your monitoring settings take effect.

Configure Proactive HA

You can configure how Proactive HA responds when a provider has notified its health degradation to vCenter, indicating a partial failure of that host.

This page is editable only if you have enabled vSphere DRS.

Procedure

1 In the vSphere Client, browse to the Proactive HA cluster.

2 Click the Configure tab.

3 Select vSphere Availability and click Edit.

4 Select Turn on Proactive HA.

5 Click Proactive HA Failures and Responses.

6 Select from the following configuration options.

Option	Description
Automation Level	Determine whether host quaratine or maintenance mode and VM migrations are recommendations or automatic • Manual. vCenter Server suggests migration recommendations for virtual machines. • Automated. Virtual machines are migrated to healthy hosts and degraded hosts are entered into quarantine or maintenance mode depending on the configured Proactive HA automation level.
Remediation	Determine what happens to partially degraded hosts. • Quarantine mode for all failures. Balances performance and availability, by avoiding the usage of partially degraded hosts provided that virtual machine performance is unaffected. • Quarantine mode for moderate and Maintenance mode for severe failure (Mixed). Balances performance and availability, by avoiding the usage of moderately degraded hosts provided that virtual machine performance is unaffected. Ensures that virtual machines do not run on severely failed hosts. • Maintenance mode for all failures. Ensures that virtual machines do not run on partially failed hosts. Host.Config.Quarantine and Host.Config.Maintenance privileges are required to put hosts in Quarantine mode and Maintenance mode, respectively.

To enable Proactive HA providers for this cluster, select the check boxes. Providers appear when their corresponding vSphere Client plugin has been installed and the providers monitor every host in the cluster. To view or edit the failure conditions supported by the provider, click the edit link.

7 Click OK.

Configure Admission Control

After you create a cluster, you can configure admission control to specify whether virtual machines can be started if they violate availability constraints. The cluster reserves resources so that failover can occur for all running virtual machines on the specified number of hosts.

The Admission Control page appears only if you enabled vSphere HA.

Procedure

1 In the vSphere Client, browse to the vSphere HA cluster.

2 Click the Configure tab.

3 Select vSphere Availability and click Edit.

4 Click Admission Control to display the configuration options.

5 Select a number for the Host failures cluster tolerates. This is the maximum number of host failures that the cluster can recover from or guarantees failover for.

6 Select an option for Define host failover capacity by.

Option	Description
Cluster resource percentage	Specify a percentage of the cluster's CPU and memory resources to reserve as spare capacity to support failovers.
Slot Policy (powered-on VMs)	Select a slot size policy that covers all powered on VMs or is a fixed size. You can also calculate how many VMs require multiple slots.
Dedicated failover hosts	Select hosts to use for failover actions. Failovers can still occur on other hosts in the cluster if a default failover host does not have enough resources.
Disabled	Select this option to disable admission control and allow virtual machine power ons that violate availability constraints.

7 Set the percentage for the Performance degradation VMs tolerate.

This setting determines what percentage of performance degradation the VMs in the cluster are allowed to tolerate during a failure.

8 Click OK.

Results

Your admission control settings take effect.

Configure Heartbeat Datastores

vSphere HA uses datastore heartbeating to distinguish between hosts that have failed and hosts that reside on a network partition. With datastore heartbeating, vSphere HA can monitor hosts when a management network partition occurs and continue to respond to failures.

You can specify the datastores that you want to be used for datastore heartbeating.

Procedure

1 In the vSphere Client, browse to the vSphere HA cluster.

2 Click the Configure tab.

3 Select vSphere Availability and click Edit.

4 Click Heartbeat Datastores to display the configuration options for datastore heartbeating.

5 To instruct vSphere HA about how to select the datastores and how to treat your preferences, select from the following options.

Table 2-3.

Datastore Heartbeating Options
Automatically select datastores accessible from the host
Use datastores only from the specified list
Use datastores from the specified list and complement automatically if needed

6 In the Available heartbeat datastores pane, select the datastores that you want to use for heartbeating.

The listed datastores are shared by more than one host in the vSphere HA cluster. When a datastore is selected, the lower pane displays all the hosts in the vSphere HA cluster that can access it.

7 Click OK.

Set Advanced Options

To customize vSphere HA behavior, set advanced vSphere HA options.

Prerequisites

Verify that you have cluster administrator privileges.

Note Because these options affect the functioning of vSphere HA, change them with caution.

Procedure

1 In the vSphere Client, browse to the vSphere HA cluster.

2 Click the Configure tab.

3 Select vSphere Availability and click Edit.

4 Click Advanced Options.

5 Click Add and type the name of the advanced option in the text box.

You can set the value of the option in the text box in the Value column.

6 Repeat step 5 for each new option that you want to add and click OK.

Results

The cluster uses the options that you added or modified.

What to do next

Once you have set an advanced vSphere HA option, it persists until you do one the following:

- Using the vSphere Client, reset its value to the default value.
- Manually edit or delete the option from the fdm.cfg file on all hosts in the cluster.

vSphere HA Advanced Options

You can set advanced options that affect the behavior of your vSphere HA cluster.

Table 2-4. vSphere HA Advanced Options

Option	Description
das.isolationaddress[...]	Sets the address to ping to determine if a host is isolated from the network. This address is pinged only when heartbeats are not received from any other host in the cluster. If not specified, the default gateway of the management network is used. This default gateway has to be a reliable address that is available, so that the host can determine if it is isolated from the network. You can specify multiple isolation addresses (up to 10) for the cluster: das.isolationAddressX, where X = 0-9. Typically you should specify one per management network. Specifying too many addresses makes isolation detection take too long.
das.usedefaultisolationaddress	By default, vSphere HA uses the default gateway of the console network as an isolation address. This option specifies whether or not this default is used (true|false).
das.isolationshutdowntimeout	The period of time the system waits for a virtual machine to shut down before powering it off. This only applies if the host's isolation response is Shut down VM. Default value is 300 seconds.
das.slotmeminmb	Defines the maximum bound on the memory slot size. If this option is used, the slot size is the smaller of this value or the maximum memory reservation plus memory overhead of any powered-on virtual machine in the cluster.
das.slotcpuinmhz	Defines the maximum bound on the CPU slot size. If this option is used, the slot size is the smaller of this value or the maximum CPU reservation of any powered-on virtual machine in the cluster.
das.vmmemoryminmb	Defines the default memory resource value assigned to a virtual machine if its memory reservation is not specified or zero. This is used for the Host Failures Cluster Tolerates admission control policy. If no value is specified, the default is 0 MB.
das.vmcpuminmhz	Defines the default CPU resource value assigned to a virtual machine if its CPU reservation is not specified or zero. This is used for the Host Failures Cluster Tolerates admission control policy. If no value is specified, the default is 32MHz.
das.iostatsinterval	Changes the default I/O stats interval for VM Monitoring sensitivity. The default is 120 (seconds). Can be set to any value greater than, or equal to 0. Setting to 0 disables the check. Note Values of less than 50 are not recommended since smaller values can result in vSphere HA unexpectedly resetting a virtual machine.
das.ignoreinsufficienthbdatastore	Disables configuration issues created if the host does not have sufficient heartbeat datastores for vSphere HA. Default value is false.
das.heartbeatdsperhost	Changes the number of heartbeat datastores required. Valid values can range from 2-5 and the default is 2.
das.config.fdm.isolationPolicyDelaySec	The number of seconds system waits before executing the isolation policy once it is determined that a host is isolated. The minimum value is 30. If set to a value less than 30, the delay will be 30 seconds.
das.respectvmvmantiaffinityrules	Determines if vSphere HA enforces VM-VM anti-affinity rules. The default value is "true" and

	rules are enforced even if vSphere DRS is not enabled. In this case, vSphere HA does not fail over a virtual machine if doing so violates a rule, but it issues an event reporting there are insufficient resources to perform the failover. This option can also be set to "false", whereby the rules are not enforced. See vSphere Resource Management for more information on anti-affinity rules.
das.maxresets	The maximum number of reset attempts made by VMCP. If a reset operation on a virtual machine affected by an APD situation fails, VMCP retries the reset this many times before giving up
das.maxterminates	The maximum number of retries made by VMCP for virtual machine termination.
das.terminateretryintervalsec	If VMCP fails to terminate a virtual machine, this is the number of seconds the system waits before it retries a terminate attempt
das.config.fdm.reportfailoverfailevent	When set to 1, enables generation of a detailed per-VM event when an attempt by vSphere HA to restart a virtual machine is unsuccessful. Default value is 0. In versions earlier than vSphere 6.0, this event is generated by default.
vpxd.das.completemetadataupdateintervalsec	The period of time (seconds) after a VM-Host affinity rule is set during which vSphere HA can restart a VM in a DRS-disabled cluster, overriding the rule. Default value is 300 seconds.
das.config.fdm.memReservationMB	By default vSphere HA agents run with a configured memory limit of 250 MB. A host might not allow this reservation if it runs out of reservable capacity. You can use this advanced option to lower the memory limit to avoid this issue. Only integers greater than 100, which is the minimum value, can be specified. Conversely, to prevent problems during primary agent elections in a large cluster (containing 6,000 to 8,000 VMs) you should raise this limit to 325 MB. Note Once this limit is changed, for all hosts in the cluster you must run the Reconfigure HA task. Also, when a new host is added to the cluster or an existing host is rebooted, this task should be performed on those hosts in order to update this memory setting.
das.reregisterrestartdisabledvms	When vSphere HA is disabled on a specific VM this option ensures that the VM is registered on another host after a failure. This allows you to power-on that VM without needing to re-register it manually. Note When this option is used, vSphere HA does not power on the VM, but only registers it.
das.respectvmhostsoftaffinityrules	Determines if vSphere HA restarts a respective VM on a host that belongs to the same VM-Host group. If no such host is available or if the value of this option is set to “false”, vSphere HA restarts the VM on any available host in the cluster. In vSphere 6.5, the default value is "true". This value might not be visibly defined in the advanced HA options of the cluster. If you want to disable the option, you must manually set this option as "false" in the advanced HA options for the cluster.

Note If you change the value of any of the following advanced options, you must disable and then re-enable vSphere HA before your changes take effect.

- das.isolationaddress[...]
- das.usedefaultisolationaddress
- das.isolationshutdowntimeout

Customize an Individual Virtual Machine

Each virtual machine in a vSphere HA cluster is assigned the cluster default settings for VM Restart Priority, Host Isolation Response, VM Component Protection, and VM Monitoring. You can specify specific behavior for each virtual machine by changing these defaults. If the virtual machine leaves the cluster, these settings are lost.

Procedure

1 In the vSphere Client, browse to the vSphere HA cluster.

2 Click the Configure tab.

3 Under Configuration, select VM Overrides and click Add.

4 Use the + button to select virtual machines to which to apply the overrides.

5 Click OK.

6 (Optional) You can change other settings, such as the Automation level, VM restart priority, Response for Host Isolation, VMCP settings,VM Monitoring, or VM monitoring sensitivity settings.

> Note You can view the cluster defaults for these settings by first expanding Relevant Cluster Settings and then expanding vSphere HA.

7 Click OK.

Results

The virtual machine’s behavior now differs from the cluster defaults for each setting that you changed.

Objective 4.4
Identify how to configure vSphere DRS.

vSphere Resource Management Update 1 - VMware vSphere 7.0, page 86

vSphere DRS

vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere Cluster. Starting with vSphere 7.0 Update 1, DRS depends on the availability of vCLS VMs.

Note If you try to enable DRS on a cluster where there are issues with the vCLS VMs, a warning message is displayed on the Cluster Summary page.

Note If DRS is on but there are issues with the vCLS VMs, you must resolve these issues for DRS to operate. A warning message is displayed on the Cluster Summary page.

If DRS is non-functional this does not mean that DRS is disabled. Existing DRS settings and resource pools survive across a lost vCLS VMs quorum. vCLS health turns Unhealthy only in a DRS enabled cluster when vCLS VMs are not running and the first instance of DRS is skipped because of this. vCLS health will stay Degraded on a non-DRS enabled cluster when at least one vCLS VM is not running.

vSphere Resource Management Update 1 - VMware vSphere 7.0, page 77

DRS Cluster Requirements

Hosts that are added to a DRS cluster must meet certain requirements to use cluster features successfully.

Note vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere Cluster. Starting with vSphere 7.0 Update 1, DRS depends on the availability of vCLS VMs. See vSphere Cluster Services (vCLS) for more information.

Shared Storage Requirements

A DRS cluster has certain shared storage requirements.

Ensure that the managed hosts use shared storage. Shared storage is typically on a SAN, but can also be implemented using NAS shared storage.

See the *vSphere Storage* documentation for information about other shared storage.

Shared VMFS Volume Requirements

A DRS cluster has certain shared VMFS volume requirements.

Configure all managed hosts to use shared VMFS volumes.

- Place the disks of all virtual machines on VMFS volumes that are accessible by source and destination hosts.

- Ensure the VMFS volume is sufficiently large to store all virtual disks for your virtual machines.

- Ensure all VMFS volumes on source and destination hosts use volume names, and all virtual machines use those volume names for specifying the virtual disks.

Note Virtual machine swap files also need to be on a VMFS accessible to source and destination hosts (just like .vmdk virtual disk files). This requirement does not apply if all source and destination hosts are ESX Server 3.5 or higher and using host-local swap. In that case, vMotion with swap files on unshared storage is supported. Swap files are placed on a VMFS by default, but administrators might override the file location using advanced virtual machine configuration options.

Processor Compatibility Requirements

A DRS cluster has certain processor compatibility requirements.

To avoid limiting the capabilities of DRS, you should maximize the processor compatibility of source and destination hosts in the cluster.

vMotion transfers the running architectural state of a virtual machine between underlying ESXi hosts. vMotion compatibility means that the processors of the destination host must be able to resume execution using the equivalent instructions where the processors of the source host were suspended. Processor clock speeds and cache sizes might vary, but processors must come from the same vendor class (Intel versus AMD) and the same processor family to be compatible for migration with vMotion.

Processor families are defined by the processor vendors. You can distinguish different processor versions within the same family by comparing the processors' model, stepping level, and extended features.

Sometimes, processor vendors have introduced significant architectural changes within the same processor family (such as 64-bit extensions and SSE3). VMware identifies these exceptions if it cannot guarantee successful migration with vMotion.

vCenter Server provides features that help ensure that virtual machines migrated with vMotion meet processor compatibility requirements. These features include:

- Enhanced vMotion Compatibility (EVC) – You can use EVC to help ensure vMotion compatibility for the hosts in a cluster. EVC ensures that all hosts in a cluster present the same CPU feature set to virtual machines, even if the actual CPUs on the hosts differ. This prevents migrations with vMotion from failing due to incompatible CPUs.

  Configure EVC from the Cluster Settings dialog box. The hosts in a cluster must meet certain requirements for the cluster to use EVC. For information about EVC and EVC requirements, see the *vCenter Server and Host Management* documentation.

- CPU compatibility masks – vCenter Server compares the CPU features available to a virtual machine with the CPU features of the destination host to determine whether to allow or disallow migrations with vMotion. By applying CPU compatibility masks to individual virtual machines, you can hide certain CPU features from the virtual machine and potentially prevent migrations with vMotion from failing due to incompatible CPUs.

vMotion Requirements for DRS Clusters

A DRS cluster has certain vMotion requirements.

To enable the use of DRS migration recommendations, the hosts in your cluster must be part of a vMotion network. If the hosts are not in the vMotion network, DRS can still make initial placement recommendations.

To be configured for vMotion, each host in the cluster must meet the following requirements:

- vMotion does not support raw disks or migration of applications clustered using Microsoft Cluster Service (MSCS).

- vMotion requires a private Gigabit Ethernet migration network between all of the vMotion enabled managed hosts. When vMotion is enabled on a managed host, configure a unique network identity object for the managed host and connect it to the private migration network.

Create a Cluster

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

Clusters enable the vSphere High Availability (HA) and vSphere Distributed Resource Scheduler (DRS) solutions.

Note vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere Cluster. Starting with vSphere 7.0 Update 1, DRS depends on the availability of vCLS VMs. See vSphere Cluster Services (vCLS) for more information.

Prerequisites

- Verify that you have sufficient permissions to create a cluster object.

- Verify that a data center exists in the inventory.

- If you want to use vSAN, it must be enabled before you configure vSphere HA.

Procedure

1 Browse to a data center in the vSphere Client.

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

3 Enter a name for the cluster.

4 Select DRS and vSphere HA cluster features.

Option	Description
To use DRS with this cluster	a Select the DRS Turn ON check box. b Select an automation level and a migration threshold.
To use HA with this cluster	a Select the vSphere HA Turn ON check box. b Select whether to enable host monitoring and admission control. c If admission control is enabled, specify a policy.

d Select a VM Monitoring option.

e Specify the virtual machine monitoring sensitivity.

5 Select an Enhanced vMotion Compatibility (EVC) setting.

EVC ensures that all hosts in a cluster present the same CPU feature set to virtual machines, even if the actual CPUs on the hosts differ. This prevents migrations with vMotion from failing due to incompatible CPUs.

6 Click OK.

Results

The cluster is added to the inventory.

What to do next

Add hosts and resource pools to the cluster.

Note Under the Cluster Summary page, you can see Cluster Services which displays vSphere Cluster Services health status.

Edit Cluster Settings

When you add a host to a DRS cluster, the host's resources become part of the cluster's resources. In addition to this aggregation of resources, with a DRS cluster you can support cluster-wide resource pools and enforce cluster-level resource allocation policies.

The following cluster-level resource management capabilities are also available.

Load Balancing

The distribution and usage of CPU and memory resources for all hosts and virtual machines in the cluster are continuously monitored. DRS compares these metrics to an ideal resource usage given the attributes of the cluster's resource pools and virtual machines, the current demand, and the imbalance target. DRS then provides recommendations or performs virtual
machine migrations accordingly. See Virtual Machine Migration. When you power on a virtual machine in the cluster, DRS attempts to maintain proper load balancing by either placing the virtual machine on an appropriate host or making a recommendation. See Admission Control and Initial Placement.

Power management

When the vSphere Distributed Power Management (DPM) feature is enabled, DRS compares cluster and host-level capacity to the demands of the cluster's virtual machines, including recent historical demand. DRS then recommends you place hosts in standby, or places hosts in standby power mode when sufficient excess capacity is found. DRS powers-on hosts if capacity is needed. Depending on the resulting host power state recommendations, virtual machines might need to be migrated to and from the hosts as well. See Managing Power Resources.

Affinity Rules
You can control the placement of virtual machines on hosts within a cluster, by assigning affinity rules. See Using DRS Affinity Rules.

Prerequisites

You can create a cluster without a special license, but you must have a license to enable a cluster for vSphere DRS or vSphere HA.

> Note vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere Cluster. Starting with vSphere 7.0 Update 1, DRS depends on the availability of vCLS VMs. See vSphere Cluster Services (vCLS) for more information.

Procedure

1 Browse to a cluster in the vSphere Client.

2 Click the Configure tab and click Services.

3 Under vSphere DRS click Edit.

4 Under DRS Automation, select a default automation level for DRS.

Automation Level	Action
Manual	• Initial placement: Recommended host is displayed. • Migration: Recommendation is displayed.
Partially Automated	• Initial placement: Automatic. • Migration: Recommendation is displayed.
Fully Automated	• Initial placement: Automatic. • Migration: Recommendation is run automatically.

5 Set the Migration Threshold for DRS.

6 Select the Predictive DRS check box. In addition to real-time metrics, DRS responds to forecasted metrics provided by vRealize Operations server. You must also configure Predictive DRS in a version of vRealize Operations that supports this feature

7 Select Virtual Machine Automation check box to enable individual virtual machine automation levels.

Override for individual virtual machines can be set from the VM Overrides page.

8 Under Additional Options, select a check box to enforce one of the default policies.

Option	Description
VM Distribution	For availability, distribute a more even number of virtual machines across hosts. This is secondary to DRS load balancing.
Memory Metric for Load Balancing	Load balance based on consumed memory of virtual machines rather than active memory. This setting is only recommended for clusters where host memory is not over-committed. Note This setting is no longer supported and will not be displayed in vCenter 7.0.
CPU Over-Commitment	Control CPU over-commitment in the cluster.

Scalable Shares	Enable scalable shares for the resource pools on this cluster.

9 Under Power Management, select Automation Level.

10 If DPM is enabled, set the DPM Threshold.

11 Click OK.

What to do next

Note Under the Cluster Summary page, you can see Cluster Services which displays vSphere Cluster Services health status.

You can view memory utilization for DRS in the vSphere Client. To find out more, see:

Viewing Distributed Resource Scheduler Memory Utilization (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere67_drs)

Set a Custom Automation Level for a Virtual Machine

After you create a DRS cluster, you can customize the automation level for individual virtual machines to override the cluster's default automation level.

For example, you can select Manual for specific virtual machines in a cluster with full automation, or Partially Automated for specific virtual machines in a manual cluster.

If a virtual machine is set to Disabled, vCenter Server does not migrate that virtual machine or provide migration recommendations for it.

Procedure

1 Browse to the cluster in the vSphere Client.

2 Click the Configure tab and click Services.

3 Under Services, select vSphere DRS and click Edit. Expand DRS Automation.

4 Select the Enable individual virtual machine automation levels check box.

5 To temporarily disable any individual virtual machine overrides, deselect the Enable individual virtual machine automation levels check box.

Virtual machine settings are restored when the check box is selected again.

6 To temporarily suspend all vMotion activity in a cluster, put the cluster in manual mode and deselect the Enable individual virtual machine automation levels check box.

7 Select one or more virtual machines.

8 Click the Automation Level column and select an automation level from the drop-down menu.

Option	Description

Manual	Placement and migration recommendations are displayed, but do not run until you manually apply the recommendation.
Fully Automated	Placement and migration recommendations run automatically.
Partially Automated	Initial placement is performed automatically. Migration recommendations are displayed, but do not run.
Disabled	vCenter Server does not migrate the virtual machine or provide migration recommendations for it.

9 Click OK.

Results

Note Other VMware products or features, such as vSphere vApp and vSphere Fault Tolerance, might override the automation levels of virtual machines in a DRS cluster. Refer to the product-specific documentation for details.

Disable DRS

You can turn off DRS for a cluster.

When DRS is disabled, the cluster's resource pool hierarchy and affinity rules are not reestablished when DRS is turned back on. If you disable DRS, the resource pools are removed from the cluster. To avoid losing the resource pools, save a snapshot of the resource pool tree on your local machine. You can use the snapshot to restore the resource pool when you enable DRS.

Procedure

1 Browse to the cluster in the vSphere Client.

2 Click the Configure tab and click Services.

3 Under vSphere DRS, click Edit.

4 Deselect the Turn On vSphere DRS check box.

5 Click OK to turn off DRS.

6 (Optional) Choose an option to save the resource pool.

- Click Yes to save a resource pool tree snapshot on a local machine.
- Click No to turn off DRS without saving a resource pool tree snapshot.

Results

DRS is turned off.

Note vSphere DRS is a critical feature of vSphere which is required to maintain the health of the workloads running inside vSphere Cluster. Starting with vSphere 7.0 Update 1, DRS depends on the availability of vCLS VMs. See vSphere Cluster Services (vCLS) for more information.

Restore a Resource Pool Tree

You can restore a previously saved resource pool tree snapshot.

Prerequisites

- vSphere DRS must be turned ON.
- You can restore a snapshot only on the same cluster that it was taken.
- No other resource pools are present in the cluster.

Procedure

1 Browse to the cluster in the vSphere Client.

2 Right-click on the cluster and select Restore Resource Pool Tree.

3 Click Browse, and locate the snapshot file on your local machine.

4 Click Open.

5 Click OK to restore the resource pool tree.

Objective 4.5
Identify how to configure EVC.

vSphere Virtual Machine Administration Update 1 - VMware vSphere 7.0, page 266

Enhanced vMotion Compatibility as a Virtual Machine Attribute

Enhanced vMotion Compatibility (EVC) is a cluster feature that ensures CPU compatibility between hosts in a cluster, so that you can seamlessly migrate virtual machines within the EVC cluster. You can also enable, disable, or change the EVC mode at the virtual machine level. The per-VM EVC feature facilitates the migration of the virtual machine beyond the cluster and across vCenter Server systems and data centers that have different processors.

Starting with vSphere 7.0 Update 1, you can take advantage of the EVC feature for Virtual Shared Graphics Acceleration (vSGA). vSGA allows multiple virtual machines to share GPUs installed on ESXi hosts and leverage the 3D graphics acceleration capabilities.

The EVC mode of a virtual machine is independent from the EVC mode defined at the cluster level. The cluster-based EVC mode limits the CPU features a host exposes to virtual machines. The per-VM EVC mode determines the set of host CPU features that a virtual machine requires to power on and migrate.

By default, when you power on a newly created virtual machine, it inherits the feature set of its parent EVC cluster or host. However, you can change the EVC mode for each virtual machine separately. You can raise or lower the EVC mode of a virtual machine. Lowering the EVC mode increases the CPU compatibility of the virtual machine. You can also use the API calls to customize the EVC mode further.

Cluster-Level EVC and Per-VM EVC

There are several differences between the way the EVC feature works at the host cluster level and at the virtual machine level.

- Unlike cluster-based EVC, you can change the per-VM EVC mode only when the virtual machine is powered off.

- With cluster-based EVC, when you migrate a virtual machine out of the EVC cluster, a power cycle resets the EVC mode that the virtual machine has. With Per-VM EVC, the EVC mode becomes an attribute of the virtual machine. A power cycle does not affect the compatibility of the virtual machine with different processors.

- When you configure EVC at the virtual machine level, the per-VM EVC mode overrides cluster-based EVC. If you do not configure per-VM EVC, when you power on the virtual machine, it inherits the EVC mode of its parent EVC cluster or host.

- If a virtual machine is in an EVC cluster and the per-VM EVC is also enabled, the EVC mode of the virtual machine cannot exceed the EVC mode of the EVC cluster in which the virtual machine runs. The baseline feature set that you configure for the virtual machine cannot contain more CPU features than the baseline feature set applied to the hosts in the EVC cluster. For example, if you configure a cluster with the Intel "Merom" Generation EVC mode, you should not configure a virtual machine with any other Intel baseline feature set. All other sets contain more CPU features than the Intel "Merom" Generation feature set and as a result of such configuration, the virtual machine fails to power on.

To learn more about EVC clusters, see the *vCenter Server and Host Management* guide.

Compatibility and Requirements

The per-VM EVC feature has the following requirements.

Compatibility	Requirement
Host compatibility	ESXi 6.7 or later.
vCenter Server compatibility	vCenter Server 6.7 or later.
Virtual machine compatibility	Virtual hardware version 14 or later.

To check EVC support for a specific processor or server model, see the *VMware Compatibility Guide* at http://www.vmware.com/resources/compatibility/search.php.

Configure the EVC Mode of a Virtual Machine

Per-VM EVC is disabled by default. You can enable, disable, and change the EVC mode of a virtual machine to ensure its seamless migration across clusters, vCenter Server systems, and data centers that have different processors.

To check what the EVC mode of a virtual machine is, see Determine the EVC Mode of a Virtual Machine.

Prerequisites

Power off the virtual machine

- Power off the virtual machine.

Procedure

1 Navigate to a virtual machine in the vCenter Server inventory.

2 On the Configure tab, select VMware EVC.

The pane shows details about the EVC mode of the virtual machine and CPUID details.

Important For newly created virtual machines, the EVC mode that shows in the VMware EVC pane is disabled.
For powered off virtual machines, the VMware EVC pane always shows the EVC status defined at the virtual machine level.
For powered on virtual machines with per-VM EVC enabled, the VMware EVC pane shows the EVC status defined at the virtual machine level.
For powered on virtual machines with per-VM EVC disabled, the VMware EVC pane shows the EVC mode that the virtual machine inherits from its parent EVC cluster or host.

3 Click the Edit button.

The Change EVC Mode dialog box opens.

4 In the Change EVC Mode dialog box, select whether to enable or disable EVC.

Option	Description
Disable EVC	The EVC feature is disabled for the virtual machine. When you power on the virtual machine, it inherits the feature set of its parent EVC cluster or host.
Enable EVC for AMD hosts	The EVC feature is enabled for AMD hosts.
Enable EVC for Intel hosts	The EVC feature is enabled for Intel hosts.
Custom	This option is visible only if you have customized the EVC mode of the virtual machine through the API calls.

5 (Optional) From the CPU Mode drop-down menu, select a baseline CPU feature set.

Important If the virtual machine is in an EVC cluster and the per-VM EVC mode exceeds the EVC mode for the cluster, the virtual machine fails to power on. The baseline CPU feature set for the virtual machine must not contain more CPU features than the baseline CPU feature set of the cluster.

6 (Required) From the Graphics Mode (vSGA) drop-down menu, select a baseline graphics feature set.

Note Graphics Mode (vSGA) applies only the Baseline Graphics set that includes features through Direct3D 10.1/OpenGL 3.3. The Baseline Graphics feature set is compatible with all supported features for ESXi 7.0 or earlier.

7 Click OK.

Determine the EVC Mode of a Virtual Machine

The EVC mode of a virtual machine determines the CPU and graphics features that a host must have in order for the virtual machine to migrate to that host and power on. The EVC mode of a virtual machine is independent from the EVC mode that you configure for the cluster in which the virtual machine runs.

The EVC mode of a virtual machine is determined when the virtual machine powers on. At power-on, the virtual machine also determines the EVC mode of the cluster in which it runs. If the EVC mode of a running virtual machine or the entire EVC cluster is raised, the virtual machine does not change its EVC mode until it is powered off and powered on again. This means that the virtual machine does not use any CPU features exposed by the new EVC mode until the virtual machine is powered off and powered on again.

For example, you create an EVC cluster that contains hosts with Intel processors and you set the EVC mode to Intel "Merom" Generation (Xeon Core 2). When you power on a virtual machine in this cluster, it runs in the Intel Merom Generation (Xeon Core 2) EVC mode. If you raise the EVC mode of the cluster to Intel "Penryn" Generation (Xeon 45 nm Core 2), the virtual machine retains the lower Intel "Merom" Generation (Xeon Core 2) EVC mode. To use the feature set of the higher EVC mode, such as SSE4.1, the virtual machine must be powered off and powered on again.

Procedure

1 Navigate to a cluster or a host in the vCenter Server inventory.

2 Click the VMs tab.

A list of all virtual machines in the selected cluster or on the selected host appears.

3 To verify the status of the CPU mode, check the EVC CPU Mode column.

a Click the angle icon next to any column title and select Show/Hide Columns > EVC CPU Mode.

The EVC CPU Mode column shows the CPU modes of all virtual machines in the cluster or on the host.

Important For each virtual machine, the EVC CPU Mode column displays the EVC mode defined at the virtual machine level.

However, if you do not configure per-VM EVC for a virtual machine, the virtual machine inherits the EVC mode of its parent cluster or host. As a result, for all virtual machines that do not have per-VM EVC configured, the EVC CPU Mode column displays the inherited EVC mode of the parent host or cluster.

If the virtual machine is in an EVC cluster, the EVC mode that you see in the EVC CPU Mode column is defined in the following manner.

- When the virtual machine is powered on, the EVC CPU Mode column displays either the per-VM EVC mode, or the cluster-level EVC mode.

Per-VM EVC	Cluster-Level EVC	EVC Mode for the Virtual Machine
Enabled	Enabled	Enabled. The EVC CPU Mode column displays the EVC mode of the virtual machine.
Disabled	Enabled	Enabled. The EVC CPU Mode column displays the EVC mode of the EVC cluster.

- When the virtual machine is powered off, the EVC CPU Mode column displays the per-VM EVC mode. If per-VM EVC is disabled, the EVC CPU Mode column for the virtual machine is empty.

When the virtual machine is not in an EVC cluster and per-VM EVC is not configured, the EVC mode that you see in the EVC CPU Mode column is defined in the following manner.

- When the virtual machine is powered on, the EVC CPU Mode column displays the EVC mode of the parent host.
- When the virtual machine is powered off, the EVC CPU Mode column is empty.

4 To verify the status of the graphics mode, check the EVC Graphics Mode (vSGA) column.

a Click the angle icon next to any column title and select Show/Hide Columns > EVC Graphics Mode (vSGA).

The EVC Graphics Mode (vSGA) column displays the baseline graphics features set. To view the baseline graphics, you must enable 3D graphics in the virtual machine.
For information on how to configure 3D graphics, see Configure 3D Graphics and Video Cards.

Section 7
Administrative and Operational Tasks

Objective 7.1 - Identify how to create and manage VM snapshots.

Objective 7.2 - Identify how to manage VM templates and clones.

Objective 7.3 - Identify the considerations when provisioning a VM.

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

Objective 7.5 - Identify the concepts of role-based user management.

Objective 7.6 - Identify virtual networking issues that impact vSphere.

Objective 7.7 - Identify virtual storage issues that impact vSphere.

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

Objective 7.9 - Identify how to monitor vSphere Cluster and SDRS Cluster.

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

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

Objective 7.12 - Identify the purpose for VMware Tools.

Objective 7.1
Identify how to create and manage VM snapshots.

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

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.

Objective 7.2
Identify how to manage VM templates and clones.

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

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.

Objective 7.3
Identify the considerations when provisioning a VM.

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

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.

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

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

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 39

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.

Objective 7.5
Identify the concepts of role-based user management.

vSphere Security Update 1 - VMware vSphere 7.0, page 42

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:	Administrator

	Virtual machine.Provisioning.Deploy template	
	On the destination host, cluster or resource pool: Resource.Assign virtual machine to resource pool	Administrator
	On the destination datastore or folder of datastores: Datastore.Allocate space	Datastore Consumer or Administrator
	On the network that the virtual machine will be assigned to: Network.Assign network	Network Consumer or Administrator
Take a virtual machine snapshot	On the virtual machine or a folder of virtual machines: Virtual machine.Snapshot management.Create snapshot	Virtual Machine Power User or Administrator
Move a virtual machine into a resource pool	On the virtual machine or folder of virtual machines: • Resource.Assign virtual machine to resource pool • Virtual machine.Inventory.Move	Administrator
	On the destination resource pool: Resource.Assign virtual machine to resource pool	Administrator
Install a guest operating system on a virtual machine	On the virtual machine or folder of virtual machines: • Virtual machine.Interaction.Answer question • Virtual machine.Interaction.Console interaction • Virtual machine.Interaction.Device connection • Virtual machine.Interaction.Power Off • Virtual machine.Interaction.Power On • Virtual machine.Interaction.Reset • Virtual machine .Interaction.Configure CD media (if installing from a CD) • Virtual machine .Interaction.Configure floppy media (if installing from a floppy disk) • Virtual machine.Interaction.VMware Tools install	Virtual Machine Power User or Administrator
	On a datastore 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: Host.Inventory.Add host to cluster	Administrator
	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

Objective 7.6
Identify virtual networking issues that impact vSphere.

vSphere Networking Update 1 - VMware vSphere 7.0, page 259

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.

Objective 7.7
Identify virtual storage issues that impact vSphere.

vSphere Storage Update 1 - VMware vSphere 7.0, page 71

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 127

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:

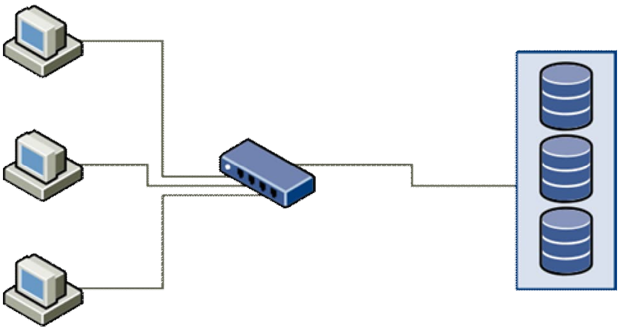
- Place each LUN on a RAID group that provides the necessary performance levels. Monitor the activities and resource use of other LUNS in the assigned RAID group. A high-performance RAID group that has too many applications doing I/O to it might not meet performance goals required by an application running 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.

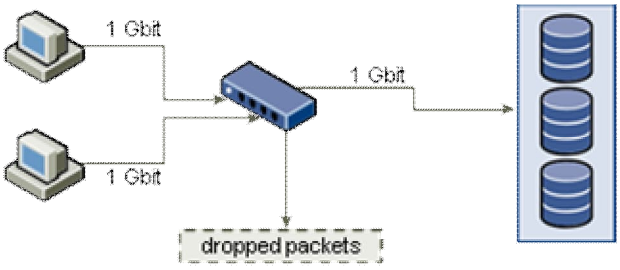
Figure 13-1. Single Ethernet Link Connection to Storage



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

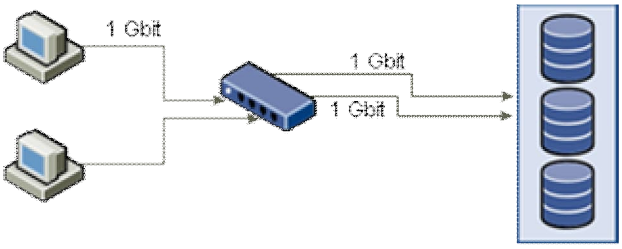
In this example from a Cisco switch, the bandwidth used is 476303000 bits/second, which is less than half of wire speed. The port is buffering incoming packets, but has dropped several packets. The final line of this interface summary indicates that this port has already dropped almost 10,000 inbound 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 323

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.

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

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

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.

Objective 7.9
Identify how to monitor vSphere Cluster and SDRS Cluster.

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

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.

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

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

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 129

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.

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

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

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.

Objective 7.12
Identify the purpose for VMware Tools.

VMware Tools User Guide – Vmware Tools 11.1.0, page 7

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