Section 1
Architecture and Technologies

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

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.

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

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

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.

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

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

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.

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

Objective 1.4
Identify business challenges addressed by vSphere.

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.

vSphere Availability –Vmware vSphere 7.0 Update 1, page 7

Identify the components of a vSphere environment.

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: lCIM/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.

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

Objective 1.6
Identify vSphere virtual networking components and types.

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.

vSphere Networking - VMware vSphere 7.0, page 13

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

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, using an RPC-based protocol. VMware currently implements NFS version 3 over TCP/IP. Support for NFS was introduced in ESX 3.0 in 2006	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 transport is Ethernet. VMware introduced support for hardware FCoE in vSphere 4.x and software FCoE in VMware vSphere® 5.0 in 2011.
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).	Requires a dedicated 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.

	iSCSI	NFS	Fibre Channel	FCoe
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 concurrently.

	iSCSI	NFS	FIbre ChaNNel	FCoe
Resilience	VMware PSA implements failover via its Storage Array Type Plug-in (SATP) for all supported iSCSI arrays. The preferred method to do this for software iSCSI is with iSCSI binding implemented, but it can be achieved by adding multiple targets on different subnets mapped to the iSCSI initiator.	Network adapter teaming can be configured so that if one interface fails, another can take its place. However, this relies on a network failure and might not be able to handle error conditions occurring on the NFS array/server side.	VMware PSA implements failover via its Storage Array Type Plug-in (SATP) for all supported FC arrays.	VMware PSA implements failover via its Storage Array Type Plug-in (SATP) for all supported FCoE arrays.
Error Checking	iSCSI uses TCP, which resends dropped packets.	NFS uses TCP, which resends dropped packets.	FC is implemented as a lossless network. This is achieved by throttling throughput at times of congestion, using B2B and E2E credits.	FCoE requires a lossless network. This is achieved by the implementation of a pause frame mechanism at times of congestion.
Security	iSCSI implements the Challenge Handshake Authentication Protocol (CHAP) to ensure that initiators and targets trust each other. VLANs or private networks are highly recommended, to isolate the iSCSI traffic from other traffic types.	VLANs or private networks are highly recommended, to isolate the NFS traffic from other traffic types.	Some FC switches support the concepts of a VSAN, to isolate parts of the storage infrastructure. VSANs are conceptually similar to VLANs. Zoning between hosts and FC targets also offers a degree of isolation.	Some FCoE switches support the concepts of a VSAN, to isolate parts of the storage infrastructure. Zoning between hosts and FCoE targets also offers a degree of isolation.

	iSCSI	NFS	FIbre ChaNNel	FCoe
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 offload 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

	iSCSI	NFS	FIbre ChaNNel	FCoe
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 Configuration	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 datastores or RDMs.	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 or RDMs.	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 datastores or RDMs.

	iSCSI	NFS	FIbre ChaNNeI	FCoe
Advantages	No additional hardware is necessary. Can useexisting networking hardware components and iSCSI driver from VMware, so it's inexpensiveto implement. Well-known and well-understood protocol. Quite mature at this stage. Administratorswith networkskills should be able to implement. Can be troubleshooted with generic network tools such as Wireshark.	No additional hardware is necessary. Can useexisting networking hardware components, so it's inexpensiveto implement. Well-known andwell-understood protocol. It also is very mature. Administrators with network skills should be able to implement. Can be troubleshooted with generic network toolssuchasWireshark.	Well-known and well-understood protocol. Very mature and trusted. Found in majorityof 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. Possiblesecurity 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 andattention. No PSAmultipathing. 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 stillversion3, 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 (16Gbthrottledto run at 8Gb in vSphere 5.0). Requiresdedicated 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. Requiresa 10Gb lossless network infrastructure, which canbeexpensive. 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.

Storage Protocol Comparison - White Paper, page 4

Objective 1.8
Identify the characteristics of vSphere storage technologies.

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.

vSphere Storage - VMware vSphere 7.0, page 16

Objective 1.9
Identify the purposes of different virtual machine files.

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).

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

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

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

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

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

Using Snapshots To Manage Virtual Machines

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

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

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

With snapshots, you can preserve a baseline before 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.

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

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

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 106

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 Updater 1 - VMware vSphere 7.0, page 118

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.

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.

vSphere Availability Update 1 – Vmware vSphere 7.0, page 7

Objective 1.16
Identify the functionality of VMware Distributed Resource Scheduler.

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.

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

Objective 1.17
Given a DRS score, identify the meaning.

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.

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

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

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.

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