VMware 2V0-21.23 Exam Questions

Total Questions: 170+
Demo Questions: 30
Version: Updated for 2025

Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

For Access to the full set of Updated Questions – Visit: 2v0-21.23 Exam Dumps by Cert Empire

Question: 1

An administrator is working with VMware Support and is asked to provide log bundles for the ESXi hosts in an environment. Which three options does the administrator have? (Choose three.)

A: Generate a combined log bundle for all ESXi hosts using the vCenter Management Interface.

B: Generate a separate log bundle for each ESXi host using the vSphere Host Client.

C: Generate a combined log bundle for all ESXi hosts using the vSphere Client.

D: Generate a separate log bundle for each ESXi host using the vSphere Client.

E: Generate a separate log bundle for each ESXi host using the vCenter Management Interface.

F: Generate a combined log bundle for all ESXi hosts using the vSphere Host Client.

Correct Answer:

B, C, D

Explanation:

An administrator has three primary UI-based methods to gather ESXi host log bundles.

1. vSphere Client (Multiple Hosts): By connecting to vCenter Server with the vSphere Client, the administrator can select a parent object (like a cluster) or multiple ESXi hosts and use the "Export System Logs" wizard. This generates a single downloadable package containing the log bundles for all selected hosts.

2. vSphere Client (Single Host): The same "Export System Logs" wizard in the vSphere Client can be used on a single ESXi host object to generate a log bundle for only that host.

3. vSphere Host Client: By connecting directly to an individual ESXi host's IP address or FQDN, the administrator can use the vSphere Host Client to generate a support bundle for that specific host. This process must be repeated for each host.

Why Incorrect Options are Wrong:

F: The vSphere Host Client connects to a single ESXi host and has no awareness of other hosts; therefore, it cannot generate a combined log bundle for multiple hosts.

References:

1. VMware vSphere 8.0 Documentation, vCenter Server and Host Management, "Export Log Files".

This section details the procedure for exporting logs using the vSphere Client: "You can select vCenter Server systems and ESXi hosts and export log files for them... The wizard collects the selected log files and saves them in a .zip file that you can download." This supports options C and D.

2. VMware vSphere 8.0 Documentation, vCenter Server and Host Management, "Log In to the VMware Host Client".

This section describes accessing the individual host client. The subsequent monitoring and log generation features within the Host Client are documented, confirming its use for generating a single host's log bundle. This supports option B.

3. VMware vSphere 8.0 Documentation, vCenter Server Configuration, "Log In to the vCenter Server Management Interface".

This document outlines the functions of the VAMI, which include monitoring health, managing backups, and configuring networking for the vCenter appliance. It makes no mention of managing or collecting logs from ESXi hosts, confirming options A and E are incorrect.

Question: 2

An administrator is tasked with configuring remote direct memory access (RDMA) over Converged Ethernet v2 (RoCE v2). Which two types of adapters must the administrator configure? (Choose two.)

A: Paravirtual RDMA adapter

B: RDMA network adapter

C: Software iSCSi adapter

D: Fibre Channel over Ethernet (FCoE) adapter

E: Software NVMe over RDMA storage adapter

Correct Answer:

B, E

Explanation:

To configure and utilize RDMA over Converged Ethernet v2 (RoCE v2) in a vSphere environment, an administrator must configure components at both the physical and logical layers on the ESXi host.

First, a physical RDMA network adapter (B) that supports RoCE v2 must be installed and configured. This involves setting up the associated VMkernel networking to enable the RDMA protocol stack.

Second, to use this RDMA fabric for a primary use case like high-performance storage, the administrator must add and configure a Software NVMe over RDMA storage adapter (E). This logical adapter allows the ESXi host to discover and connect to NVMe-oF storage targets using the RoCE v2 transport.

Why Incorrect Options are Wrong:

A: Paravirtual RDMA adapter: This is a virtual device added to a specific virtual machine for VM-to-VM communication, not a fundamental host-level adapter for general RoCE v2 setup.

C: Software iSCSI adapter: This adapter is used for the iSCSI storage protocol. While iSCSI can use RDMA (iSER), this is not the adapter type for NVMe over RDMA.

D: Fibre Channel over Ethernet (FCoE) adapter: This adapter is for the FCoE storage protocol and is unrelated to RDMA or RoCE v2.

References:

1. VMware vSphere Documentation (vSphere 8.0), vSphere Storage, "Configuring NVMe over RDMA (RoCE v2)": This official guide explicitly outlines the required steps. It states, "To use the NVMe over RDMA storage, you must configure the RDMA network adapters on your ESXi host." It then continues, "After you configure the physical RDMA adapters, you add a corresponding software NVMe over RDMA adapter on your ESXi host." This directly supports the selection of both the RDMA network adapter (B) and the Software NVMe over RDMA storage adapter (E).

2. VMware vSphere Documentation (vSphere 8.0), vSphere Networking, "RDMA on an ESXi Host": This document details the prerequisites for using RDMA, starting with the physical hardware. It mentions, "Your ESXi host must have an RDMA-capable network adapter installed." This confirms the necessity of the RDMA network adapter (B) as the foundational component.

Question: 3

Which two datastore types store the components of a virtual machine as a set of objects? (Choose two.)

A: VMware Virtual Machine File System (VMFS)

B: VMware vSAN

C: Network File System (NFS) 3

D: vSphere Virtual Volumes (vVols)

E: Network File System (NFS) 4.1

Correct Answer:

B, D

Explanation:

VMware vSAN and vSphere Virtual Volumes (vVols) are object-based storage technologies. vSAN is a software-defined storage solution that treats each component of a virtual machine (e.g., VM home, VMDK, snapshot) as a discrete object. These objects are then distributed across the vSAN cluster according to their storage policies.

Similarly, the vVols framework enables storage arrays to manage VM components as individual objects called virtual volumes. Instead of managing large LUNs or file shares, the storage array is aware of and manages each virtual disk and its derivatives as a separate entity. This contrasts with traditional file-based datastores like VMFS and NFS.

Why Incorrect Options are Wrong:

A: VMware Virtual Machine File System (VMFS): VMFS is a high-performance clustered file system. It stores virtual machines as a collection of files within a directory structure on a block-based LUN.

C: Network File System (NFS) 3: NFS is a file-sharing protocol. When used as a vSphere datastore, it stores VM components as files on a network-attached share.

E: Network File System (NFS) 4.1: Like NFS 3, NFS 4.1 is a file-based protocol and stores VM components as files, not as native storage objects.

References:

1. VMware vSphere Documentation, vSAN Planning and Deployment Guide 8.0, "Understanding the vSAN Object-Based Storage": "vSAN stores and manages data in the form of flexible data containers called objects... When you provision a virtual machine on a vSAN datastore, vSAN creates a set of objects for each virtual machine. For example, a virtual machine home namespace, a VMDK, a snapshot... are individual objects."

2. VMware vSphere Documentation, vSphere Storage 8.0, "Working with vSphere Virtual Volumes": "vSphere Virtual Volumes is an integration and management framework that virtualizes SAN and NAS arrays... With Virtual Volumes, an individual virtual machine and its disks, rather than a LUN, become a unit of storage management... A virtual volume is an object that is exported by a storage array and that corresponds to a VM file, such as a VMDK or a snapshot."

3. VMware vSphere Documentation, vSphere Storage 8.0, "VMFS Datastores": "vSphere VMFS is a special high-performance file system format that is optimized for storing virtual machines." This section describes its nature as a file system, not an object store.

Question: 4

An administrator has a host profile named Standard-Config. The administrator wants to change the other host profiles to use only the storage configuration settings that are defined in the Standard-Config host profile. What should the administrator do to make this change?

A: Export host customizations and import them to the other host profiles.

B: Copy the storage settings from Standard-Config to all other host profiles.

C: Duplicate the Standard-Config host profile and only modify the storage configuration settings.

D: Export the Standard-Config host profile and attach it to tile other hosts.

Correct Answer:

B

Explanation:

The vSphere Client provides a specific function to copy settings from one host profile to another. An administrator can select a source profile (Standard-Config) and one or more destination profiles. The interface then allows the administrator to select specific configuration categories, such as "Storage configuration," to copy. This action updates the destination profiles with only the selected settings from the source, precisely matching the requirement to apply only the storage configuration without altering other settings in the destination profiles.

Why Incorrect Options are Wrong:

A: Host customizations are host-specific values (e.g., IP addresses) applied to a profile, not the profile's configuration settings themselves. This action would not copy settings between profiles.

C: Duplicating creates a new, separate host profile. It does not update any other existing host profiles as required by the scenario.

D: Attaching the Standard-Config profile to other hosts would replace their entire configuration, not just update the storage settings within their existing, different profiles.

References:

1. VMware vSphere Documentation, "Copy Settings from a Host Profile to Another Host Profile": This official guide details the procedure. It states, "You can copy settings from a

host profile to one or more other host profiles. You can copy all settings or a subset of the settings from the source profile." The steps involve right-clicking the destination profile, selecting "Copy Settings from Profile," choosing the source profile, and then selecting the specific settings (e.g., Storage configuration) to be copied.

Source: VMware vSphere Product Documentation, vSphere Host Profiles. (Accessed for vSphere 8, but the feature is consistent across relevant versions for the 2V0-21.23 exam).

2. VMware vSphere Documentation, "Using Host Profiles to Manage ESXi Host Configuration": This document explains the core concepts of Host Profiles. It implicitly differentiates between applying a whole profile and managing its sub-profile settings. The "Copy Settings" feature is a key part of managing these sub-profiles across multiple different host profiles.

Source: VMware vSphere Product Documentation, vSphere Host Profiles.

Question: 5

A company has two sites: Site A and Site The administrator would like to manage the VMware vCenter inventories in both sites from a single vSphere Client session. Which vCenter feature must be configured?

A: VMware Certificate Authority

B: VMware Site Recovery Manager

C: vCenter Single Sign-On

D: Enhanced Linked Mode

Correct Answer:

D

Explanation:

Enhanced Linked Mode (ELM) is the specific vCenter Server feature designed to connect multiple vCenter Server instances. When configured, an administrator can log in to any of the linked vCenter Servers and view, search, and manage the inventories (e.g., virtual machines, hosts, datastores) of all connected vCenter Servers from a single vSphere Client session. This provides a unified management experience across different sites or pods, which directly fulfills the requirement stated in the question. While vCenter Single Sign-On is a prerequisite for ELM, it is ELM that provides the inventory linking capability.

Why Incorrect Options are Wrong:

A: VMware Certificate Authority: This component is responsible for issuing and managing security certificates for vSphere components; it does not link vCenter inventories for unified management.

B: VMware Site Recovery Manager: This is a disaster recovery solution used to orchestrate the failover of virtual machines between sites, not for consolidating daily management into a single interface.

C: vCenter Single Sign-On: This feature provides centralized authentication for the vSphere environment but does not, by itself, link the inventories of multiple vCenter Servers for a single-pane-of-glass view.

References:

1. VMware vSphere Product Documentation, "vCenter Server and Host Management" Guide for vSphere 8.0. In the section "vCenter Enhanced Linked Mode," it states: "vCenter Enhanced Linked Mode allows you to log in to any single instance of vCenter Server and view and manage the inventories of all the vCenter Server systems in the group." (This concept is consistent across recent vSphere versions relevant to the exam).

2. VMware vSphere Product Documentation, "vSphere Authentication" Guide for vSphere 8.0. The section on "vCenter Single Sign-On and vCenter Enhanced Linked Mode" clarifies the relationship: "To join vCenter Server systems in Enhanced Linked Mode, you connect them to the same vCenter Single Sign-On domain." This shows SSO is a prerequisite, not the feature that provides the linked view.

3. VMware vSphere Product Documentation, "vSphere Security" Guide for vSphere 8.0. The chapter on "vSphere Certificate Management" describes the role of the VMware Certificate Authority (VMCA) in managing certificates, which is distinct from inventory management.

Question: 6

During the staging of a patch on a vCenter Server Appliance, an error was encountered and the process stopped. An administrator resolved the root cause and is ready to continue with the staging of the patch. From the vCenter Management Interface, which action should the administrator take to continue the process from the point at which the error occurred?

A: Use the Stage and Install option to resume the staging.

B: Use the Resume option to resume the staging.

C: Use the Unstage option to restart the staging.

D: Use the Stage Only option to restart the staging.

Correct Answer:

B

Explanation:

When staging a patch for a vCenter Server Appliance (VCSA) through the vCenter Management Interface (VAMI), if the process is interrupted by an error, the system is designed to allow for continuation. After the administrator resolves the underlying issue (e.g., network connectivity, disk space), the VAMI presents a Resume option. This specific action is designed to continue the staging process from the point of failure, preventing the need to download and stage the entire patch from the beginning.

Why Incorrect Options are Wrong:

A: Use the Stage and Install option to resume the staging. This option initiates a new, complete workflow to both stage and then immediately install the patch, not resume a failed staging operation.

C: Use the Unstage option to restart the staging. This action would remove any partially downloaded patch files, forcing the administrator to start the entire staging process over from scratch.

D: Use the Stage Only option to restart the staging. This option is used to initiate a new staging process. It would restart the download from the beginning, not resume it.

References:

1. VMware vSphere Documentation: vCenter Server and Host Management Guide for vSphere 8.0, section "Patch or Update a vCenter Server Appliance".

The guide states: "If the staging process fails, find the cause of the failure, resolve the issue, and click Resume to continue the staging of the patch." This directly confirms that "Resume" is the correct action to continue from the point of error. (This procedure is consistent across recent vSphere versions relevant to the exam).

2. VMware vSphere Documentation: vSphere Upgrade Guide for vSphere 7.0, section "Stage Patches to the vCenter Server Appliance".

This document also describes the patching workflow via the VAMI and explicitly mentions the "Resume" functionality in case of a staging failure: "If staging fails, you must resolve the problem that caused the failure, and click Resume to continue staging."

Question: 7

An administrator needs to consolidate a number of physical servers by migrating the workloads to a software-defined data center solution. Which VMware solution should the administrator recommend?

A: VMware Horizon

B: VMware vSAN

C: VMware vSphere

D: VMware NSX

Correct Answer:

C

Explanation:

The core requirement is to consolidate physical servers by migrating their workloads. This process is known as server virtualization. VMware vSphere is the foundational server virtualization platform that enables this by allowing multiple virtual machines (VMs) to run on a single physical host. It includes the ESXi hypervisor and vCenter Server for management, forming the essential compute pillar of a software-defined data center (SDDC). The primary use case for vSphere is to abstract server resources to achieve consolidation, increased utilization, and simplified management of workloads.

Why Incorrect Options are Wrong:

A: VMware Horizon: This is a solution for virtual desktop infrastructure (VDI) and application delivery, not for consolidating general-purpose server workloads.

B: VMware vSAN: This is a software-defined storage (SDS) solution that provides the storage pillar of an SDDC, but it does not perform the compute virtualization needed for server consolidation.

D: VMware NSX: This is a network virtualization and security platform. It provides the networking pillar of an SDDC but is not used for migrating and running server workloads.

References:

1. VMware vSphere Documentation: "VMware vSphere is the industry-leading server virtualization software and the heart of a modern SDDC... It enables users to run, manage,

connect, and secure their applications in a common operating environment..." This establishes vSphere as the core compute and management platform for virtualization.

Source: VMware, "What is vSphere?", VMware vSphere Product Page. (Accessed via official VMware product documentation).

2. VMware SDDC Architecture Overview: The Software-Defined Data Center (SDDC) architecture is built upon three key pillars: compute, storage, and network virtualization. VMware vSphere provides the compute virtualization layer. "vSphere abstracts, aggregates, and allocates the physical compute resources..."

Source: VMware, "VMware SDDC Architecture," VMware Cloud Foundation Documentation.

3. VMware Server Consolidation Guide: "Server consolidation is a common practice for organizations that want to make better use of their server resources. With VMware vSphere, you can consolidate applications onto fewer servers..." This directly links the action (server consolidation) to the specific product (vSphere).

Source: VMware, "Server Consolidation and Containment with VMware vSphere," Official VMware White Paper.

Question: 8

An administrator is tasked with applying updates to a vSphere cluster running vSAN using vSphere Lifecycle Manager. Downtime to the ESXi hosts must be minimal while the work is completed. The administrator has already completed the following steps and no errors have been returned: Downloaded all applicable software and created a new image. Attached the new image to the cluster and run a compliance check against the image for the cluster. Ran a remediation pre-check for the cluster. Which two series of steps should the administrator perform to start the remediation of the cluster using the new image? (Choose two.)

A: 1. Use the Remediate option in vSphere Lifecycle Manager to remediate all of the ESXi hosts in the cluster in parallel. 2. Allow vSphere Lifecycle Manager to automatically control maintenance mode on the ESXi hosts.

B: 1. Place each of the ESXi hosts into maintenance mode manually. 2. Use the Stage option in vSphere Lifecycle Manager to stage the required software on all ESXi hosts one at a time.

C: 1. Leave all ESXi hosts in the cluster operational. 2. Use the Stage All option in vSphere Lifecycle Manager to stage the required software onto all ESXi hosts one at a time.

D: 1. Leave all ESXi hosts in the cluster operational. 2. Use the Stage All option in vSphere Lifecycle Manager to stage the required software onto all ESXi hosts in the cluster in parallel.

E: 1. Use the Remediate option in vSphere Lifecycle Manager to remediate all of the ESXi hosts in the cluster in sequence.
2. Allow vSphere Lifecycle Manager to automatically control maintenance mode on the ESXi hosts.

Correct Answer:

D, E

Explanation:

To update a vSAN cluster using vSphere Lifecycle Manager (vLCM) with minimal downtime, a two-phase approach is recommended after the initial pre-checks.

First, the administrator should stage the image. Staging downloads the necessary software components to the ESXi hosts without requiring maintenance mode. This can be done for all hosts in parallel while they remain operational, which significantly reduces the time each host will later spend in maintenance mode (Option D).

Second, the administrator initiates the remediation. For a vSAN cluster, vLCM enforces a sequential remediation process, updating only one host at a time to ensure data availability and adherence to storage policies. During this process, vLCM automatically manages placing each host into and out of maintenance mode (Option E).

Why Incorrect Options are Wrong:

A: Remediating a vSAN cluster in parallel is not supported as it would violate vSAN availability requirements by taking multiple hosts (and their data components) offline simultaneously.

B: Manually placing hosts into maintenance mode is inefficient and unnecessary, as vLCM automates this task. Staging one at a time is also less efficient than parallel staging.

C: Staging software to hosts one at a time is less efficient than the parallel staging operation, which can be performed safely while hosts are operational.

References:

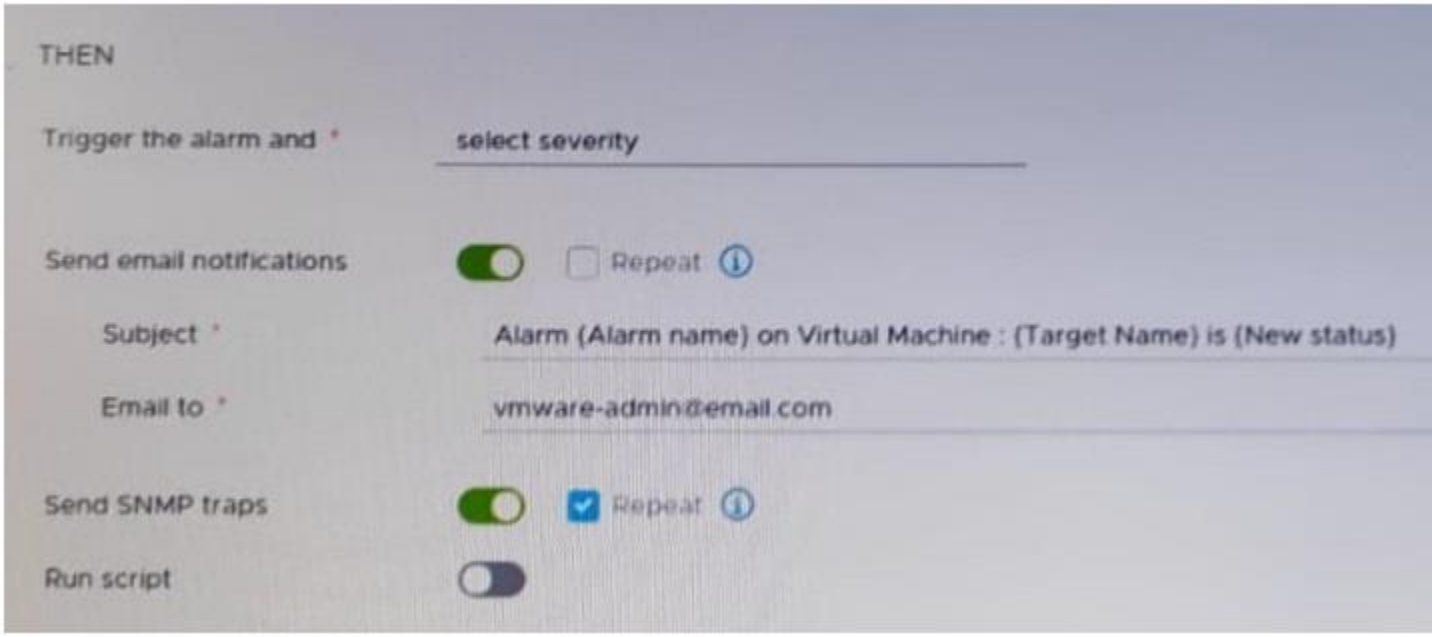
1. VMware vSphere 8.0 Documentation, "Stage Patches and Extensions to ESXi Hosts": "Staging the software on the hosts before remediation helps you save time during the remediation itself... You can stage the updates, patches, or extensions to multiple ESXi hosts in parallel." This supports the procedure in Option D.

2. VMware vSphere 8.0 Documentation, "Remediating a vSAN Cluster": "vSphere Lifecycle Manager remediates the hosts in a vSAN cluster sequentially, even if you configure it to remediate hosts in parallel. This is to ensure vSAN data availability." This directly supports the sequential remediation described in Option E and invalidates Option A.

3. VMware vSphere 8.0 Documentation, "Remediate the Hosts in a Cluster Against a Single Image": The procedure outlines that during the remediation wizard, vLCM handles the maintenance mode migration tasks automatically. "vSphere Lifecycle Manager migrates the powered on virtual machines from the host and puts the host in maintenance mode." This supports the second part of Option E.

Question: 9

Refer to the exhibit.



After updating a predefined alarm on VMware vCenter, an administrator enables email notifications as shown in the attached alarm; however, notifications are NOT being sent. Where must the mail server settings be configured by the administrator to resolve this issue?

A: In the ESXi host system config

B: In the alarm rule definition

C: In the vCenter settings in the vSphere Client

D: In the vCenter Management Interface

Correct Answer:

C

Explanation:

For vCenter Server to send email notifications for alarms, it must be configured with the details of an SMTP mail server. This is a global setting for the vCenter Server instance, not for individual alarms or hosts. The administrator configures these settings by navigating to the vCenter Server object within the vSphere Client, selecting the 'Configure' tab, and then editing the 'General' settings to provide the mail server (SMTP server) and mail sender

information. The alarm action shown in the exhibit will only succeed after this fundamental configuration is completed.

Why Incorrect Options are Wrong:

A: ESXi host configuration is separate from vCenter Server's application-level services. Mail settings for vCenter alarms are not configured on individual hosts.

B: The alarm rule definition specifies the action to send an email, but it does not define the SMTP server vCenter uses to send it.

D: The vCenter Management Interface (VAMI) is used for appliance-level management (e.g., backups, updates, networking), not for configuring application services like mail notifications.

References:

1. VMware vSphere 7.0 Documentation, vCenter Server and Host Management, section "vCenter Server Configuration", subsection "Configure Mail Sender Settings for vCenter Server". This guide details the procedure: "In the vSphere Client, navigate to the vCenter Server instance. ... Select Configure. Under Settings, select General. ... In the Mail section, enter the SMTP server information and a sender account."

2. VMware vSphere 8.0 Documentation, vCenter Server and Host Management, section "Configure Mail Sender Settings". The procedure remains consistent: "You can configure the mail server that vCenter Server uses to send email notifications for alarms... In the vSphere Client, navigate to the vCenter Server instance... Select Configure > Settings > General... Click Edit... Select Mail."

Question: 10

A vSphere cluster has the following configuration: Virtual machines (VMs) are running Production and Test workloads vSphere Distributed Resource Scheduler (DRS) is enabled There are no resource pools in the cluster Performance monitoring data shows that the Production workload VMs are not receiving their fully allocated memory when the vSphere cluster is fully utilized. A combination of which two steps could the administrator perform to ensure that the Production VMs are always guaranteed the full allocation of memory? (Choose two.)

A: Assign a custom memory share value to the resource pool containing the Production VMs.

B: Assign a memory reservation value to the resource pool containing the Production VMs.

C: Create a parent resource pool for the Production VMs.

D: Create a sibling resource pool for each of the Production and Test VMs.

E: Create a child resource pool for the Test VMs.

Correct Answer:

B, D

Explanation:

To resolve memory contention and provide a guarantee for Production virtual machines (VMs), the administrator must first logically separate the Production and Test workloads. Creating sibling resource pools—one for Production and one for Test—achieves this separation, allowing distinct resource policies to be applied to each group.

Subsequently, to ensure the Production VMs receive their full memory allocation even under load, a memory reservation must be configured on the Production resource pool. A reservation is a guaranteed lower bound on the amount of physical memory that the host reserves for the VMs within that pool, effectively preventing the Test workload from impacting the Production workload's memory availability.

Why Incorrect Options are Wrong:

A: Shares define relative priority during resource contention but do not provide a minimum guarantee, which is required by the scenario.

C: Creating only a parent pool for Production is an incomplete action; it does not separate the Test workload for effective management.

E: This suggests an improper hierarchy. Production and Test workloads are distinct service tiers and should be managed as peers (siblings), not in a parent-child relationship.

References:

1. VMware vSphere 8.0 Documentation, vSphere Resource Management, "Resource Allocation Settings" section.

Page 10: "A reservation specifies the guaranteed minimum allocation for a virtual machine... The server allows you to power on a virtual machine only if there are enough unreserved resources to satisfy the reservation of the virtual machine." This supports the use of a reservation (Option B) for a guarantee.

Page 10: "Shares specify the relative importance of a virtual machine (or resource pool)... Shares are relevant only when virtual machines or resource pools compete for resources." This clarifies why shares (Option A) do not provide a guarantee.

2. VMware vSphere 8.0 Documentation, vSphere Resource Management, "Managing Resource Pools" section.

Page 37: Discusses creating a resource pool hierarchy to "Separate resources for different departments or for a service tier (for example, a gold, silver, and bronze service tier)." This supports the practice of creating separate, sibling pools for different workload types like Production and Test (Option D).

Question: 11

An administrator is adding a new ESXi host to an existing vSphere cluster. When selecting the cluster, the administrator is unable to use the Cluster Quickstart workflow to add and configure the additional host. What could be the root cause of this issue?

A: The administrator has previously dismissed the Cluster Quickstart workflow.

B: The administrator must manually add the host to the cluster before using the Cluster Quickstart workflow.

C: The administrator has not been assigned the required permissions to use the Cluster Quickstart workflow.

D: The administrator must enable the Cluster Quickstart workflow option in VMware vCenter.

Correct Answer:

A

Explanation:

The Cluster Quickstart workflow is presented as a card on the cluster's Summary tab. This interface element can be dismissed by an administrator. If dismissed, the workflow will no longer be visible on the Summary tab, making it inaccessible from its primary location. To use the workflow again, the administrator must explicitly re-enable it. This is a common and direct cause for an administrator being unable to find and use the Cluster Quickstart workflow for an existing cluster.

Why Incorrect Options are Wrong:

B: The purpose of the Cluster Quickstart workflow is specifically to add and configure new hosts. Adding the host manually beforehand is contrary to the workflow's design.

C: While correct permissions are required to execute the workflow, dismissing it removes the UI entry point entirely, which is a more fundamental reason for being "unable to use" it.

D: The visibility of the Cluster Quickstart workflow is managed on a per-cluster basis, not through a global setting in VMware vCenter.

References:

1. VMware vSphere Documentation (vSphere 8.0), "vSphere Resource Management", Using the Cluster Quickstart Workflow.

This official guide states, "If you previously dismissed the Cluster Quickstart workflow, you can re-enable it from the cluster's Configure tab under Configuration > Quickstart." This directly confirms that dismissing the workflow makes it unavailable from the main view, supporting answer A.

2. VMware vSphere Documentation (vSphere 8.0), "vSphere Resource Management", Prerequisites for Using the Cluster Quickstart Workflow.

This section lists the required privileges (e.g., Host.Inventory.Add host to cluster), confirming that permissions are necessary (relevant to option C), but the issue described in A (a dismissed UI) is a more direct cause for the workflow being unavailable to start.

Question: 12

An administrator creates a virtual machine that contains the latest company-approved software, tools and security updates. Company policy requires that only full clones are allowed for server workloads. A combination of which two tasks should the administrator complete to prepare for the deployment of this virtual machine for multiple users? (Choose two.)

A: Set appropriate permissions on the virtual machine.

B: Create a virtual machine customization specification.

C: Upgrade the virtual hardware.

D: Convert the virtual machine to a template.

E: Take a snapshot of the virtual machine.

Correct Answer:

B, D

Explanation:

To prepare a master virtual machine for repeatable, scalable deployment, the standard VMware vSphere practice is to first convert the configured VM into a template. A template is a master copy used to create new VMs, and it cannot be powered on or modified, which protects its integrity.

Second, to ensure each deployed clone is unique on the network, a customization specification is created. This specification automates the application of unique settings like computer name, IP address, and Windows Security ID (SID) to each new VM during the cloning process. This combination allows for the rapid deployment of multiple, unique, and ready-to-use servers.

Why Incorrect Options are Wrong:

A: Setting permissions is an access control task, not a core step in preparing the master image's configuration for deployment.

C: Upgrading virtual hardware is a maintenance task and is not required for deployment unless the hardware version is out of date, which is not specified.

E: While cloning from a snapshot is possible, a template is the purpose-built, non-editable object for managing a master image for deployment.

References:

1. VMware vSphere 8.0 Documentation, vCenter Server and Host Management, "Clone a Virtual Machine to a Template". This section states, "You can clone a virtual machine to a template to create a master copy of the virtual machine that you can use to create and provision other virtual machines."

2. VMware vSphere 8.0 Documentation, vCenter Server and Host Management, "Managing Customization Specifications". This section explains, "You can save guest operating system customization settings in a customization specification... When you clone a virtual machine or deploy a virtual machine from a template, you can apply the customization specification to the new virtual machine."

3. VMware vSphere 8.0 Documentation, vCenter Server and Host Management, "Deploy a Virtual Machine from a Template". Step 9 of the procedure explicitly details the "Customize the operating system" page in the deployment wizard, where an administrator applies a pre-existing customization specification.

Question: 13

An administrator wants to create virtual machine (VM) templates and store them in a content library. The administrator would like to use the content library to manage different versions of these templates so that reverting to an earlier version is an option. How should the administrator create these templates?

A: Select a VM in the vCenter inventory. Clone the VM to the content library as a VM template type.

B: Select a VM template in the vCenter inventory. Clone the template to the content library.

C: Export a VM in the vCenter inventory to an OVF template. Import the OVF template into the content library.

D: Convert a VM to a template in the vCenter inventory. Clone the template to the content library.

Correct Answer:

A

Explanation:

To leverage the versioning capabilities of a vSphere Content Library, an administrator must create a VM template item. The most direct and efficient method to do this is by cloning an existing virtual machine directly into the content library as a VM template. This action creates the initial version of the template. Subsequently, the administrator can use the check-out and check-in operations to modify the template and create new versions, with the option to revert to any previous version. This workflow is specifically designed for VM templates (VMTX format) within the content library.

Why Incorrect Options are Wrong:

B: While cloning an existing vCenter template is possible, the question implies creating new templates, for which a configured VM (as in option A) is the most common and logical source.

C: Exporting to OVF and importing creates an OVF template. The check-in/check-out versioning workflow is designed for the native VM template type, not OVF/OVA items.

D: Converting a VM to a template in the vCenter inventory before cloning is an unnecessary extra step that makes the source VM unusable. Cloning directly from the VM is more efficient.

References:

1. VMware vSphere Documentation - vSphere Virtual Machine Administration (vSphere 8.0)

Topic: Create a VM Template in a Content Library

Content: "You can create a VM template in a content library by cloning a virtual machine or a VM template." This supports that cloning a VM is a primary method.

Reference: VMware vSphere 8.0 Documentation, "vSphere Virtual Machine Administration," Chapter: "Working with Content Libraries," Section: "Create a VM Template in a Content Library."

2. VMware vSphere Documentation - vSphere Virtual Machine Administration (vSphere 8.0)

Topic: Version Control of a VM Template

Content: "You can use the check-in and check-out operations to maintain a linear version history for a VM template in a content library... When you check in a VM to the template, you create a new version of the template." This confirms the versioning mechanism is tied to the check-in/check-out process for VM templates.

Reference: VMware vSphere 8.0 Documentation, "vSphere Virtual Machine Administration," Chapter: "Working with Content Libraries," Section: "Version Control of a VM Template."

3. VMware vSphere Documentation - vSphere Virtual Machine Administration (vSphere 8.0)

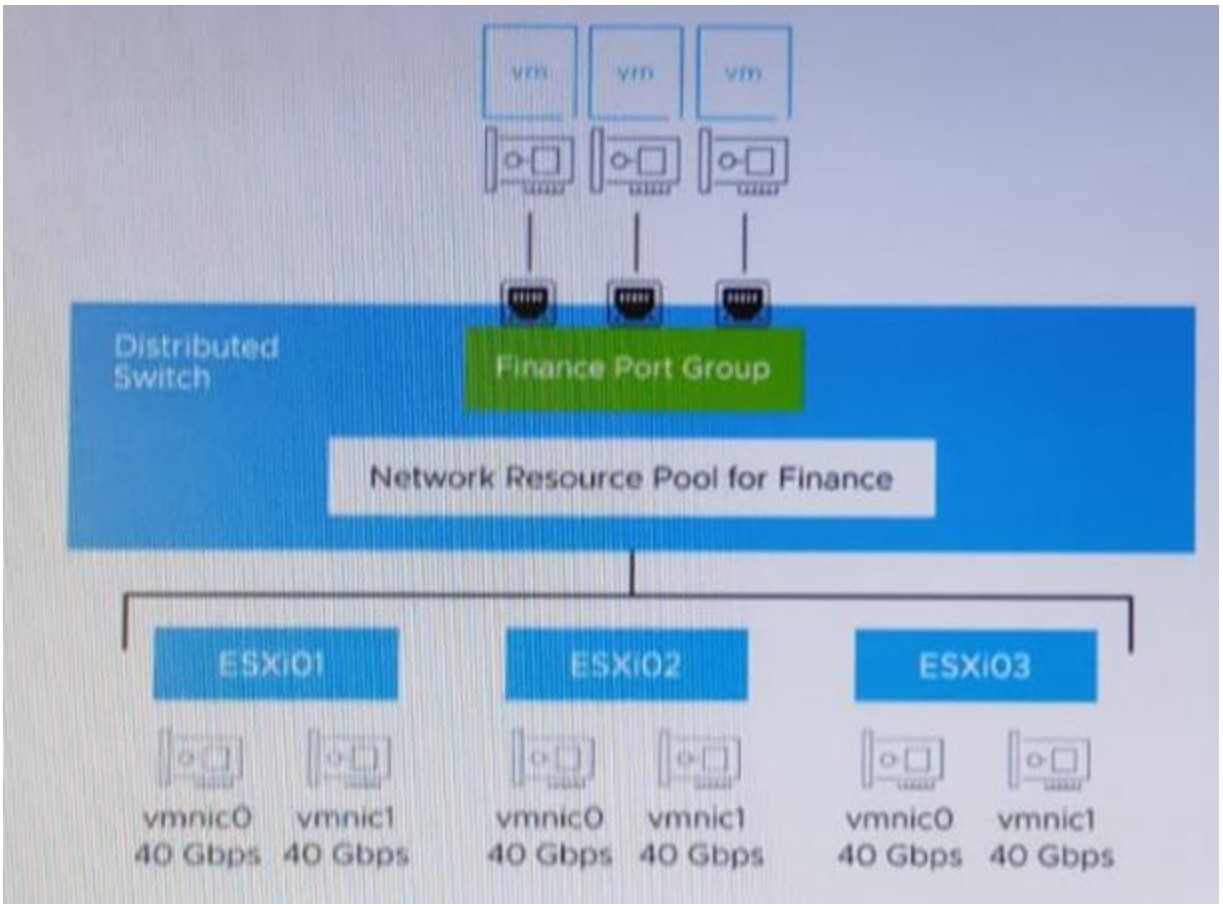
Topic: Clone a Virtual Machine to a Template in a Content Library

Content: The documentation provides a step-by-step procedure that starts with selecting a virtual machine in the inventory and using the "Clone to Template in Library" wizard. This directly matches the description in option A.

Reference: VMware vSphere 8.0 Documentation, "vSphere Virtual Machine Administration," Chapter: "Working with Content Libraries," Section: "Clone a Virtual Machine to a Template in a Content Library."

Question: 14

Refer to the exhibit.



An administrator set up the following configuration: * The distributed switch has three ESXi hosts, and each host has two 40 Gbps NICs. * The amount of bandwidth reserved for virtual machine (VM) traffic is 6 Gbps. The administrator wants to guarantee that VMs in the Finance distributed port group can access 50 percent of the available reserved bandwidth for VM traffic. k Given this scenario, what should the size (in Gbps) of the Finance network resource pool be?

A: 18

B: 80

C: 36

D: 120

Correct Answer:

A

Explanation:

The size of a Network Resource Pool on a vSphere Distributed Switch (vDS) is the aggregate of the per-host bandwidth reservations for that pool across all hosts connected to the vDS.

According to official VMware documentation, a Network I/O Control (NIOC) reservation for a system traffic type is the minimum bandwidth guaranteed on a single physical adapter.

1. Per-Host Reserved Bandwidth for VM Traffic: Each host has two 40 Gbps NICs. The reservation for VM traffic is 6 Gbps per NITherefore, the total reserved bandwidth for VM traffic on each host is 2 NICs 6 Gbps/NIC = 12 Gbps.

2. Per-Host Reservation for Finance Pool: The Finance port group requires 50% of the available reserved bandwidth for VM traffic on each host. This is 50% of 12 Gbps = 6 Gbps per host.

3. Total Finance Network Resource Pool Size: The total size is the per-host reservation multiplied by the number of hosts: 6 Gbps/host 3 hosts = 18 Gbps.

Why Incorrect Options are Wrong:

B: 80: This is the total physical network capacity of a single host (2 x 40 Gbps), not the size of the reserved resource pool.

C: 36: This represents the total reserved bandwidth for all VM traffic across all three hosts (12 Gbps/host 3 hosts), not the 50% portion allocated to the Finance pool.

D: 120: This is half of the total physical bandwidth across all three hosts (240 Gbps / 2) and is not based on the specified reservation values.

References:

1. VMware vSphere 7 Networking Guide (EN-002690-01)

Page 101, Section "Network I/O Control in a vSphere Distributed Switch": States, "The bandwidth reservation for a certain traffic type is the minimum bandwidth that is guaranteed to the traffic type on a single physical adapter." This confirms that the 6 Gbps reservation applies to each NIC.

Page 103, Section "Network Resource Pools on a vSphere Distributed Switch": Explains, "The reservation that you set on a network resource pool is aggregated across all physical adapters on the hosts that are connected to the distributed switch." This supports calculating the per-host total before aggregating.

Page 103, Section "Network Resource Pools on a vSphere Distributed Switch": Provides an example confirming the aggregation logic: "For example, if you set a reservation of 1 Gbps

for a network resource pool and the distributed switch has 3 connected hosts, the virtual machines that are members of the pool can consume in total 3 Gbps of reserved bandwidth." This validates the final calculation step (6 Gbps/host 3 hosts).

Question: 15

An administrator creates a new corporate virtual machine (VM) template every month to include all of the latest patches. The administrator needs to ensure that the new VM template is synchronized from the primary data center site (London) to two secondary data center sites (Tokyo and New York). The administrator is aware that datastore space is limited within the secondary data center sites. The administrator needs to ensure that the VM template is available in the secondary sites the first time a new virtual machine is requested. Which four steps should the administrator take to meet these requirements? (Choose four.)

A: Create a new published content library at the primary site.

B: Add the virtual machine template to the subscribed content library.

C: Create a new published content library in each secondary site.

D: Create a new subscribed content library in each secondary site.

E: Configure the subscribed content library to download content when needed.

F: Configure each subscribed content library to download content immediately.

G. **G:** Add the virtual machine template to the published content library.

Correct Answer:

A, D, E, G

Explanation:

This scenario requires a multi-site content distribution solution that is conscious of storage space at the destination sites. The vSphere Content Library feature is designed for this purpose.

1. A published content library must be created at the primary site (London) to act as the central source for the VM template.

2. The VM template must then be added (cloned) to this newly created published library.

3. At each secondary site (Tokyo, New York), a subscribed content library is created, pointing to the published library in London.

4. To address the limited datastore space and on-demand availability, the subscribed libraries must be configured to download content only when needed. This setting downloads only the item metadata initially, and the full template files are transferred only when a deployment is initiated.

Why Incorrect Options are Wrong:

B: Content is added to a published library to be distributed, not directly to a subscribed library, which only consumes content.

C: The secondary sites are consumers (subscribers) of the content, not publishers. Creating published libraries there would not synchronize the template from the primary site.

F: Downloading content immediately would consume significant datastore space at the secondary sites, violating a key requirement of the scenario.

References:

1. VMware vSphere Documentation, "Creating a Content Library". This guide outlines the process of creating both published and subscribed libraries. It states, "You can create a local or a published content library... You can also create a subscribed library that synchronizes with a published library." This supports options A and D.

2. VMware vSphere Documentation, "Subscribing to a Published Library". This section details the configuration options for a subscribed library, including the download settings. It explains, "Select the Download all library content only when needed option to save storage space. With this option, only the metadata for the items in the published library is downloaded. The content of the items is downloaded only when you use the items." This directly supports option E and refutes option F.

3. VMware vSphere Documentation, "Clone a Virtual Machine to a Template in a Content Library". This document describes the process of adding a VM template to a library. The action is performed on the source vCenter Server where the published library exists. This supports option G.

Question: 16

An administrator needs to update a VMware vCenter instance to a newer minor release version. Due to restrictions within the environment, the vCenter instance does not have access to the Internet As a first step, the administrator downloads the required update on another machine. What are the next steps the administrator must perform to complete the update? A Place the update ISO file in a Virtual Machine File System (VMFS) datastore. ' Use the vSphere Client to select the update ISO file as the source for the update.

A: Place the update ISO file in a Virtual Machine File System (VMFS) datastore. Use the vSphere Client to select the update ISO file as the source for the update

B: Mount the ISO update file to the CD-ROM drive of the vCenter instance Use the vCenter Management Interface to select the CD-ROM as the source for the update

C: Place the ISO update file in a folder accessible to the vCenter instance over HTTPS. Use the vCenter Management Interface to select the update file as the source for the update

D: Place the ZIP update file in a folder accessible to the vCenter instance over HTTPS Use the vSphere Client to select the update file as the source for the update.

Correct Answer:

B

Explanation:

The standard, officially documented procedure for patching a vCenter Server Appliance (VCSA) that is offline involves using the downloaded patch ISO file. The administrator must first mount this ISO file to the virtual CD/DVD drive of the VCSA virtual machine. After mounting the ISO, the update process is managed through the vCenter Management Interface (VAMI), which is accessible via a web browser at https://:5480. Within the VAMI, the administrator navigates to the 'Update' section and selects the option to check for updates from the CD-ROM, which then allows the patch to be staged and installed.

Why Incorrect Options are Wrong:

A: The vSphere Client is not used to initiate the vCenter update process; this is done through the vCenter Management Interface (VAMI).

C: While a custom repository can be used, the standard method for a downloaded ISO is mounting it to the CD-ROM, not serving the ISO file itself over HTTPS.

D: The update patch is distributed as an ISO file, not a ZIP file, and the update is managed via the VAMI, not the vSphere Client.

References:

1. VMware vSphere 8.0 Documentation, vCenter Server and Host Management, Chapter: "Patching and Upgrading vCenter Server", Section: "Patch a vCenter Server Appliance by Using the Appliance Management Interface".

This official guide explicitly states the procedure: "You can patch a vCenter Server appliance by using an ISO image that you download from the VMware Web site and mount to the CD/DVD drive of the vCenter Server appliance... In the appliance management interface, navigate to Update... From the Check Updates drop-down menu, select Check CD ROM."

2. VMware vSphere 7.0 Documentation, vCenter Server and Host Management, Chapter: "Patching and Upgrading vCenter Server", Section: "Patch a vCenter Server Appliance by Using the Appliance Management Interface".

This documentation for the previous major version confirms the same procedure, demonstrating its consistency. The steps outlined are to mount the ISO to the VCSA's CD/DVD drive and then use the VAMI to check the CD-ROM for the update.

Question: 17

An administrator has been notified that a number of hosts are not compliant with the company policy for time synchronization. The relevant portion of the policy states: * All physical servers must synchronize time with an external time source that is accurate to the microsecond. Which step should the administrator take to ensure compliance with the policy?

A: Ensure that each vCenter Server Appliance is configured to use a Network Time Protocol (NTP) source.

B: Ensure that each ESXi host is configured to use a Precision Time Protocol (PTP) source.

C: Ensure that each ESXi host is configured to use a Network Time Protocol (NTP) source.

D: Ensure that each vCenter Server Appliance is configured to use a Precision Time Protocol (PTP) source.

Correct Answer:

B

Explanation:

The company policy mandates time synchronization for physical servers (ESXi hosts) with microsecond-level accuracy. The Precision Time Protocol (PTP), defined by IEEE 1588, is specifically designed for high-precision clock synchronization, capable of achieving microsecond or even sub-microsecond accuracy. In contrast, the Network Time Protocol (NTP) typically provides accuracy in the millisecond range. Therefore, to comply with the stringent accuracy requirement, the administrator must configure the ESXi hosts to use a PTP source. Configuring vCenter or using NTP on the hosts would not satisfy the policy's requirements.

Why Incorrect Options are Wrong:

A: This targets the vCenter Server, not the physical servers (ESXi hosts) as required, and NTP lacks the necessary microsecond precision.

C: While this correctly targets the ESXi hosts, NTP does not provide the required microsecond-level accuracy specified in the policy.

D: This targets the vCenter Server, which is not the physical server specified in the policy, even though PTP provides the correct level of accuracy.

References:

1. VMware vSphere 8.0 Documentation, vCenter Server and Host Management, "Timekeeping in a VMware vSphere Environment".

Section: "Precision Time Protocol"

Content: "Precision Time Protocol (PTP), also known as IEEE 1588, is a time service that allows for a very high degree of accuracy for time synchronization. While NTP can provide millisecond-level accuracy, PTP can provide microsecond-level accuracy." This directly contrasts the accuracy of PTP and NTP, supporting the choice of PTP for the microsecond requirement.

2. VMware vSphere 8.0 Documentation, ESXi Host Management, "Configuring Time Synchronization for an ESXi Host".

Section: "Configure Precision Time Protocol on an ESXi Host"

Content: This section provides the procedural steps for enabling and configuring PTP on an ESXi host, confirming that this is a valid administrative action to achieve compliance.

3. IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, IEEE Std 1588-2019 (Revision of IEEE Std 1588-2008).

Section: 1 (Overview), Clause 1.1 (Scope)

Content: The standard's scope describes a protocol to enable precise synchronization of clocks in measurement and control systems implemented with packet networks, typically to sub-microsecond accuracy. This establishes PTP as the industry standard for high-precision timekeeping. (DOI: 10.1109/IEEESTD.2020.9120376)

Question: 18

An administrator is performing maintenance activities and discovers that a Virtual Machine File System (VMFS) datastore has a lot more used capacity than expected. The datastore contains 10 virtual machines (VMs) and, when the administrator reviews the contents of the associated datastore, discovers that five virtual machines have a snapshot file (-delta.vmdk files) that has not been modified in over 12 months. The administrator checks the Snapshot Manager within the vSphere Client and confirms that there are no snapshots visible.

Which task should the administrator complete on the virtual machines to free up datastore space?

A: Consolidate the snapshots for each VM.

B: Inflate the disk files for each VM.

C: Delete all snapshots for each VM.

D: Storage vMotion each VM to another datastore.

Correct Answer:

A

Explanation:

The scenario describes a condition where snapshot delta disks (-delta.vmdk) exist on the datastore, but are not registered in the vSphere Client's Snapshot Manager. This indicates an inconsistency or orphaned snapshot state. The correct vSphere feature to resolve this issue is Consolidation. The consolidation process merges the data from the snapshot delta disks into the parent disk and then removes the now-redundant delta files. This action directly addresses the problem of orphaned delta files and achieves the goal of freeing up datastore space.

Why Incorrect Options are Wrong:

Inflate the disk files for each VM: Inflating a disk converts it from thin to thick provisioned, which would increase, not decrease, the amount of space used on the datastore.

Delete all snapshots for each VM: This option is not available because the question explicitly states that "there are no snapshots visible" in the Snapshot Manager UI.

Storage vMotion each VM to another datastore: While a Storage vMotion does consolidate a VM's disks as part of the migration, it is an indirect method. Consolidation is the specific, direct, and intended task for this problem.

References:

1. VMware vSphere Documentation (vSphere 8.0), vSphere Virtual Machine Administration, "Consolidate Snapshots" section.

Quote/Paraphrase: "The Consolidate command is useful when snapshot disks fail to commit after a Delete or Delete all operation... The presence of redundant delta disks can adversely affect virtual machine performance and consume storage space. You can combine such disks and remove redundant data by using the consolidation feature." This directly describes the solution for the problem presented.

2. VMware Knowledge Base Article 2003638, "Consolidating snapshots in vSphere".

Quote/Paraphrase: "The snapshot consolidation feature was introduced in vSphere 5.0 and is used for situations when snapshot disks exist on the datastore but are not visible in the Snapshot Manager... The Needs Consolidation column in the vSphere Client reports the consolidation status of the virtual machines." This KB article confirms that consolidation is the designated feature for the exact scenario in the question.

Question: 19

An administrator is attempting to configure Storage I/O Control (SIOC) on five datastores within a vSphere environment. The administrator is being asked to determine why SIOC configuration completed successfully on only four of the datastores. What are two possible reasons why the configuration was not successful? (Choose two.)

A: The datastore contains Raw Device Mappings (RDMs).

B: SAS disks are used for the datastore.

C: The datastore has multiple extents.

D: The datastore is using ISCSI.

E: The administrator is using NFS storage.

Correct Answer:

A, C

Explanation:

Storage I/O Control (SIOC) is a vSphere feature that provides I/O prioritization for virtual machines running on a shared datastore. For SIOC to be enabled and function correctly, certain datastore requirements must be met. According to official VMware vSphere documentation, two explicit limitations are that SIOC is not supported on datastores that span multiple extents and it does not support Raw Device Mapping (RDM) files. Therefore, if an administrator attempts to enable SIOC on a datastore that either contains RDMs or is composed of multiple extents, the configuration will not be successful.

Why Incorrect Options are Wrong:

B: The underlying disk type, such as SAS, SATA, or SSD, is irrelevant to SIOC functionality. SIOC operates at a higher level.

D: iSCSI is a standard block storage protocol fully supported by vSphere and compatible with SIOC.

E: NFS datastores (v3 with VAAI support and v4.1) are supported for SIOUsing NFS is not, by itself, a reason for configuration failure.

References:

1. VMware vSphere 8.0 Documentation, vSphere Storage Guide, "Storage I/O Control Requirements and Limitations".

This section explicitly states: "Storage I/O Control is not supported on datastores with multiple extents." This directly supports option C.

The same section also lists: "Storage I/O Control does not support Raw Device Mapping (RDM) files." This directly supports option A.

2. VMware vSphere 7.0 Documentation, vSphere Resource Management Guide, "Storage I/O Control Requirements".

This document provides the same limitations for vSphere 7.0, confirming that SIOC is not supported on datastores with multiple extents or on datastores containing RDMs. This corroborates the correctness of options A and C.

Question: 20

An administrator has mapped three vSphere zones to three vSphere clusters. Which two statements are true for this vSphere with Tanzu zonal Supervisor enablement? (Choose two.)

A: One Supervisor will be created in a specific zone.

B: One Supervisor will be created across all zones.

C: Three Supervisors will be created in Linked Mode.

D: Individual vSphere Namespaces will be placed into a specific zone.

E: Individual vSphere Namespaces will be spread across all zones.

Correct Answer:

B, D

Explanation:

When vSphere with Tanzu is enabled with a zonal architecture, a single Supervisor is created. This Supervisor's control plane spans across all the underlying vSphere clusters that are mapped to the zones, providing high availability. This single, distributed Supervisor manages the resources of all three clusters as a unified entity.

When an administrator creates a vSphere Namespace on this zonal Supervisor, they must associate the namespace with one specific zone. Consequently, all Kubernetes workloads, including Tanzu Kubernetes Grid clusters deployed within that namespace, are placed on the resources of the vSphere cluster corresponding to that designated zone.

Why Incorrect Options are Wrong:

A: The Supervisor is not created in a specific zone; its control plane is distributed across all configured zones for high availability.

C: A single Supervisor is created that spans multiple clusters, not three separate Supervisors. vCenter Linked Mode is an unrelated concept.

E: A vSphere Namespace is explicitly bound to a single zone, not spread across all available zones.

References:

1. VMware vSphere 8.0 Documentation, vSphere with Tanzu Configuration and Management, "Deploying a Supervisor with vSphere Zones".

This source states, "A Supervisor that is deployed on vSphere Zones is a single Supervisor that spans across all vSphere clusters that are backing up the zones." This directly supports option B.

2. VMware vSphere 8.0 Documentation, vSphere with Tanzu Configuration and Management, "Create a vSphere Namespace on a Zonal Supervisor".

This section details the process and explicitly states, "When you create a vSphere Namespace on a Supervisor that is deployed with vSphere Zones, you must associate the namespace with one of the zones." This directly supports option D and refutes option E.

Question: 21

An administrator is investigating reports of users experiencing difficulties logging into a VMware vCenter instance using LDAP accounts. Which service should the administrator check as part of troubleshooting?

A: vSphere Authentication Proxy Service

B: Lookup Service

C: Identity Management Service

D: VMware Authentication Framework Daemon

Correct Answer:

C

Explanation:

Authentication of external directory users (Active Directory or generic LDAP) in vCenter Single Sign-On is handled by the VMware Identity Management Service (process vmware-sts-idmd). If this service is stopped or unhealthy, SSO cannot query the configured LDAP identity source, resulting in log-in failures for LDAP accounts. Therefore, checking the Identity Management Service status is the first troubleshooting step.

Why Incorrect Options are Wrong:

vSphere Authentication Proxy Service – joins ESXi hosts to AD without storing credentials; unrelated to user log-ins to vCenter.

Lookup Service – only registers and discovers vCenter/PSC services; does not perform directory authentication.

VMware Authentication Framework Daemon – manages certificates and trusted roots for SSO; it does not query LDAP identity sources.

References:

1. VMware KB 2109887 “Description of vCenter Server 6.x services,” Table – “VMware Identity Management Service (vmware-sts-idmd): provides AD/LDAP identity bridging for Single Sign-On” (para 6).

2. VMware vSphere 7.0 Documentation, “Authentication and Identity” Guide, 3.2 “Single Sign-On Components – Identity Management Service handles identity source (LDAP/AD) authentication.”

3. VMware Ports and Protocols vSphere 8.0, Identity Management Service entry (ports 389/636) – shows service role interacting with LDAP directories.

Question: 22

An administrator is looking to deploy a new VMware vCenter instance. The current environment consists of 75 hosts and is expected to grow up to 100 hosts over the next three years. Which deployment size should the administrator select?

A: Medium

B: Tiny

C: Large

D: Small

Correct Answer:

D

Explanation:

The selection of a vCenter Server deployment size is determined by the scale of the inventory it will manage, specifically the number of ESXi hosts and virtual machines. The administrator must plan for future growth. The environment is expected to grow to 100 hosts. According to official VMware documentation, the "Small" deployment size is specifically designed to support an environment of up to 100 hosts and 1,000 virtual machines. This option precisely matches the maximum expected scale of the environment, ensuring sufficient capacity without over-provisioning resources.

Why Incorrect Options are Wrong:

A: Medium: This size supports up to 400 hosts. It is oversized for the stated requirement of 100 hosts, leading to unnecessary resource consumption.

B: Tiny: This size supports only up to 10 hosts, which is insufficient for both the current (75) and future (100) host count.

C: Large: This size supports up to 1,000 hosts. It is significantly oversized for the requirement, resulting in a highly inefficient use of resources.

References:

1. VMware vSphere 8.0 Documentation, vCenter Server Installation and Setup, "Hardware Requirements for the vCenter Server Appliance". The official documentation provides a table detailing the resource requirements and inventory size for each deployment option. The "Small" deployment is listed as supporting "Up to 100 Hosts, Up to 1,000 VMs".

Source: VMware. (2023). Hardware Requirements for the vCenter Server Appliance. vSphere 8.0 Documentation. https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-vcenter-installation/GUID-4752FB86-A365-4872-B42A-6FA84A2AF293.html

2. VMware vSphere 7.0 Documentation, vCenter Server Installation and Setup, "Hardware Requirements for the vCenter Server Appliance". The sizing guidelines for vSphere 7.0 are consistent for this scenario. The "Small" deployment size is specified for "Up to 100 Hosts, Up to 1000 VMs".

Source: VMware. (2022). Hardware Requirements for the vCenter Server Appliance. vSphere 7.0 Documentation. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vcenter.install.doc/GUID-4752FB86-A365-4872-B42A-6FA84A2AF293.html

Question: 23

An administrator is creating a content library to manage VM templates and ISO images. The administrator wants to password-protect the images and templates and share them with a remote site. Which two tasks must the administration perform when creating the content library? (Choose two.)

A: Publish the local content library.

B: Enable the security policy.

C: Create a subscribed content library.

D: Select an NFS datastore.

E: Enable authentication.

Correct Answer:

A, E

Explanation:

To share a content library with a remote site, the administrator must first create a local library and then publish it. Publishing makes the library's contents available via a URL for other vCenter Server instances to subscribe to. To meet the requirement of password-protecting the images and templates, the administrator must enable authentication for the published library. This requires setting a password that subscribers at the remote site must provide to access the content, thus securing the shared templates and images.

Why Incorrect Options are Wrong:

B: Enable the security policy. This is too generic. The specific action to password-protect a published library is to "enable authentication," not a general "security policy."

C: Create a subscribed content library. A subscribed library is created at the remote site to consume the content, not at the source site where the content is being created and shared from.

D: Select an NFS datastore. The type of datastore (NFS, VMFS, vSAN) used to back the content library is irrelevant to the requirements of publishing, sharing, or password protection.

References:

1. VMware vSphere 8.0 Documentation, vCenter Server and Host Management, "Create a Content Library".

Section: "Create a Content Library" > Step 5

Content: "To share the content of a local library with other vCenter Server instances, you must publish the library. ... When you publish a local library, you can set a password to protect the content." This directly supports that publishing (A) and enabling authentication for password protection (E) are the necessary steps.

2. VMware vSphere 8.0 Documentation, vCenter Server and Host Management, "Content Library Privileges".

Section: "Content Library Privileges" Table

Content: The privileges listed, such as Content library > Add library item and Content library > Publish library, distinguish between local management and the specific action of publishing for sharing. The requirement to "Enable authentication" is a sub-option within the publishing workflow.

Question: 24

An administrator is responsible for the management of a VMware vCenter instance that is currently experiencing performance issues. The administrator quickly identifies that the CPU and memory utilization of vCenter is consistently over 80%. Upon further analysis, it seems that the vpxd process is contributing significantly to the performance issue. A combination of which four steps should the administrator take to resolve the performance issues and ensure that a similar issue can be rectified without requiring downtime to vCenter moving forward? (Choose four.)

A: Gracefully shut down vCenter using the vSphere Client.

B: Enable CPU Hot Add on the vCenter virtual machine.

C: Power on the vCenter Server Appliance using the vSphere Host Client.

D: Enable CPU and Memory Hot Add on the vCenter virtual machine.

E: Add additional CPU and memory to the vCenter Server Appliance.

F: Power on the vCenter Server Appliance using the vSphere Client.

G. **G:** Enable Memory Not Add on the vCenter virtual machine.

Correct Answer:

A, C, D, E

Explanation:

The scenario requires resolving a current vCenter performance issue caused by insufficient resources and preventing future downtime for similar adjustments. This necessitates a maintenance window.

The correct procedure is:

1. Gracefully shut down vCenter (A): To modify settings like Hot Add or add resources (if Hot Add is not already enabled), the virtual machine must be powered off. A graceful shutdown is the proper method.

2. Enable CPU and Memory Hot Add (D): This addresses the requirement to allow future resource additions without downtime. This setting can only be changed when the VM is powered off.

3. Add additional CPU and memory (E): This step directly resolves the current performance bottleneck caused by high utilization.

4. Power on vCenter using the vSphere Host Client (C): Since the vCenter Server is offline, the vSphere Client is unavailable. The administrator must connect directly to the ESXi host running the vCenter VM using the vSphere Host Client to power it back on.

Why Incorrect Options are Wrong:

B: Enable CPU Hot Add on the vCenter virtual machine. This option is incomplete. To address both CPU and memory constraints in the future, both should be enabled, as covered in option D.

F: Power on the vCenter Server Appliance using the vSphere Client. This is not possible. The vSphere Client connects to the vCenter Server, which is offline. The VM must be powered on from the underlying ESXi host.

G: Enable Memory Not Add on the vCenter virtual machine. This option contains a typo ("Not" instead of "Hot") and is incomplete. Option D correctly includes enabling Hot Add for both CPU and memory.

References:

1. Enable CPU and Memory Hot Add: The official VMware vSphere documentation states that enabling vCPU Hot Add and Memory Hot-Plug must be done while the virtual machine is powered off.

Source: VMware vSphere 8.0 Documentation, "vSphere Virtual Machine Administration," Chapter: "Virtual Machine Hardware and Resource Configuration," Section: "Enable or Disable vCPU Hot-Add for a Virtual Machine" and "Configure Virtual Memory Hot-Add Settings."

2. Adding Resources to a VM: The procedure for increasing CPU or memory for a virtual machine is performed by editing its settings. This action requires the VM to be powered off unless Hot Add is already enabled.

Source: VMware vSphere 8.0 Documentation, "vSphere Virtual Machine Administration," Chapter: "Virtual Machine Hardware and Resource Configuration," Section: "Change the Number of Virtual CPUs" and "Change the Memory Size of a Virtual Machine."

3. Managing vCenter when it is down: If vCenter Server is unavailable, management of the vCenter Server Appliance (VCSA) virtual machine itself must be performed by connecting directly to the ESXi host on which it runs.

Source: VMware vSphere 8.0 Documentation, "vCenter Server Installation and Setup," Chapter: "vCenter Server and Platform Services Controller Deployment," Section: "Troubleshooting a vCenter Server Deployment." This section implicitly relies on the administrator's ability to manage the VCSA VM via the host client when vCenter services are down.

Question: 25

When configuring vCenter High Availability (HA), which two statements are true regarding the active, passive, and witness nodes? (Choose two.)

A: Network latency must be less than 10 milliseconds.

B: They must have a supported Wide Area Network (WAN).

C: They must have a minimum of a 10 Gbps network adapter.

D: They must have a minimum of a 1 Gbps network adapter.

E: Network latency must be more than 10 milliseconds.

Correct Answer:

A, D

Explanation:

For a vCenter High Availability (HA) cluster to function correctly, specific network requirements must be met for the private network connecting the Active, Passive, and Witness nodes. The round-trip time (RTT) latency on this network must be less than 10 milliseconds to ensure timely state replication and failover decisions. Additionally, the underlying ESXi hosts that run the vCenter HA nodes must meet minimum hardware specifications, which include having at least a 1 Gigabit per second (Gbps) network adapter. While a 10 Gbps adapter is recommended for better performance, 1 Gbps is the minimum supported speed.

Why Incorrect Options are Wrong:

B: The requirement is based on network latency, not the network type (e.g., LAN or WAN). A WAN connection could be used only if it meets the strict

C: A 10 Gbps network adapter is recommended for optimal performance, but it is not the minimum requirement. The minimum supported speed is 1 Gbps.

E: Network latency greater than 10 milliseconds would cause replication timeouts and potential split-brain scenarios, preventing vCenter HA from functioning reliably.

References:

1. VMware vSphere 8.0 Documentation, "vCenter Server and Host Management", Prerequisites for vCenter HA: "The vCenter HA network latency between the Active, Passive, and Witness nodes must be less than 10 ms."

Source: VMware vSphere 8.0 Documentation, "vCenter Server and Host Management", Chapter: vCenter High Availability, Section: Prerequisites for vCenter HA.

2. VMware vSphere 8.0 Documentation, "ESXi Installation and Setup", Hardware Requirements for ESXi Hosts: "One or more Gigabit or faster Ethernet controllers."

Source: VMware vSphere 8.0 Documentation, "ESXi Installation and Setup", Chapter: ESXi Requirements, Section: Hardware Requirements for ESXi Hosts. (This establishes the minimum network speed for the physical hosts where the vCenter HA nodes are deployed).

Question: 26

An administrator is deploying a new all flash vSAN cluster based on the vSAN Original Storage Architecture (OSA). What is the minimum supported network throughput in Gb/s for each host?

A: 50

B: 10

C: 25

D: 1

Correct Answer:

B

Explanation:

For a vSAN Original Storage Architecture (OSA) all-flash cluster, the minimum supported network throughput for each host is 10 Gb/s. This requirement ensures sufficient bandwidth to handle the high I/O operations, resynchronization traffic, and metadata communication inherent in all-flash configurations. While higher speeds like 25 Gb/s or 50 Gb/s are recommended for optimal performance, especially in demanding environments, 10 Gb/s is the baseline supported configuration for production workloads. Using a lower bandwidth network would create a performance bottleneck and is not supported for all-flash deployments.

Why Incorrect Options are Wrong:

References:

1. VMware. (2023). VMware vSAN 8.0 U2 Planning and Deployment. Page 17. "For all-flash configurations, a dedicated or shared 10 GbE network is required. For better performance, use a 25 GbE or faster network."

2. VMware. (2023). VMware vSAN Design Guide. Version 8.0. Page 31, Section 4.1 "Network Physical Layer". "For all-flash clusters, 10GbE is the minimum, but 25GbE or higher is recommended to prevent the network from becoming a bottleneck."

Question: 27

An administrator enables Secure Boot on an ESXi host. On booting the ESXi host, the following error message appears: Fatal error: 39 (Secure Boot Failed) What is the cause of this issue?

A: The kernel hos been tampered with.

B: The Trusted Platform Module chip has failed.

C: The administrator attempted to boot with a bootloader that is unsigned or has been tampered with.

D: A package (VIB or driver) has been tampered with.

Correct Answer:

D

Explanation:

The error message "Fatal error: 39 (Secure Boot Failed)" is a specific indicator from the ESXi boot process. When UEFI Secure Boot is enabled, the ESXi kernel performs a signature verification of all installed packages, known as vSphere Installation Bundles (VIBs), before loading them. This error occurs when the kernel detects a VIB that is either unsigned, has been tampered with, or is signed by a party that is not trusted by the system's secure boot policy. The boot process is intentionally halted to prevent potentially compromised code from executing, thus maintaining the integrity of the hypervisor.

Why Incorrect Options are Wrong:

A: While a tampered kernel would cause a Secure Boot failure, it is verified by the bootloader earlier in the process and would typically result in a different failure signature.

B: A Trusted Platform Module (TPM) failure relates to host attestation and measured boot, not the signature verification chain that produces this specific "Fatal error: 39".

C: A tampered or unsigned bootloader would be rejected by the UEFI firmware itself, preventing the ESXi kernel from even starting to load and thus not generating this specific error message.

References:

1. VMware vSphere 8.0 Documentation, vSphere Security, "Securing ESXi Hosts", "Troubleshooting Secure Boot for ESXi Hosts".

Reference Detail: This official guide explicitly states: "If you see the message Fatal error: 39 (Secure Boot Failed) on the ESXi host console, a VIB that is not signed by a trusted party is installed on the host. You can see which VIB is causing the problem in the /var/log/boot.gz log file." This directly links the error code to a VIB issue.

Question: 28

To keep virtual machines (VMs) up and running at all times in a vSphere cluster, an administrator would like VMs to be migrated automatically when the host hardware health status becomes degraded. Which cluster feature can be used to meet this requirement?

A: Predictive DRS

B: Proactive HA

C: vSphere HA Orchestrated Restart

D: vSphere Fault Tolerance

Correct Answer:

B

Explanation:

Proactive High Availability (HA) is a vSphere cluster feature designed specifically to address the scenario of hardware degradation. It integrates with hardware vendor monitoring systems to receive health status updates about components like fans, power supplies, or memory modules. When a provider marks a component as degraded, Proactive HA can automatically place the host into a quarantine or maintenance mode. It then uses vMotion to migrate the virtual machines (VMs) to healthy hosts in the cluster before the component fails completely, thus preventing potential VM downtime and meeting the administrator's requirement.

Why Incorrect Options are Wrong:

A: Predictive DRS: This feature uses analytics from VMware Aria Operations (formerly vRealize Operations) to predict future resource bottlenecks and moves VMs to prevent performance contention, not to react to hardware health degradation.

C: vSphere HA Orchestrated Restart: This is a reactive feature that controls the power-on sequence and priority of VMs after a host has already failed and vSphere HA is restarting them on other hosts.

D: vSphere Fault Tolerance: This provides continuous availability for individual, critical VMs by maintaining a live shadow copy on another host for instantaneous failover, but it does not migrate all VMs from a degraded host.

References:

1. VMware vSphere Documentation, "vSphere Availability," vSphere 8.0, Proactive HA.

"Proactive HA responds to events such as a power supply or fan failure on a host. VMware vCenter Server connects to hardware vendor monitoring services... When a hardware component fails, the vendor monitoring service sends a health alarm to vCenter Server. In response to the alarm, Proactive HA determines which hosts are at risk and migrates the virtual machines from those hosts to healthy hosts."

2. VMware vSphere Documentation, "vSphere Resource Management," vSphere 8.0, Predictive DRS.

"Predictive DRS is integrated with VMware vRealize Operations. vRealize Operations collects data from vSphere and learns the behavior of your workloads... Based on the predicted utilization, Predictive DRS can make migration recommendations to avoid resource contention."

3. VMware vSphere Documentation, "vSphere Availability," vSphere 8.0, VM and Application Monitoring.

This section details the reactive nature of vSphere HA, including restart priorities for VMs after a host failure, which is the context for Orchestrated Restart. It states, "vSphere HA uses VM Restart Priority to determine the order in which virtual machines are restarted."

Question: 29

An administrator wants to allow a DevOps engineer the ability to delete Tanzu Kubernetes Grid (TKG) cluster objects in a vSphere Namespace. Which role would provide the minimum required permissions to perform this operation?

A: Administrator

B: Can View

C: Owner

D: Can Edit

Correct Answer:

C

Explanation:

In vSphere with Tanzu, permissions are managed at the vSphere Namespace level using three primary roles: Owner, Can Edit, and Can View. The Owner role provides full control over all objects within the namespace, which includes the ability to create, manage, and delete Tanzu Kubernetes Grid (TKG) clusters. The Can Edit role allows a user to manage workloads within the namespace but does not grant the permission to delete the cluster object itself. Since the requirement is to delete TKG cluster objects, the Owner role is the minimum predefined role that provides this capability.

Why Incorrect Options are Wrong:

A: Administrator: This is a vCenter Server global role, not a namespace-specific role. It grants excessive permissions beyond the scope of the namespace, violating the principle of least privilege.

B: Can View: This role provides read-only access to the namespace and its objects, which does not permit any deletions.

D: Can Edit: This role allows for the creation and modification of workloads (like pods and services) but lacks the permission to delete foundational objects like the TKG cluster.

References:

1. VMware vSphere Documentation, "Managing User Permissions for vSphere Namespaces": This official document details the permissions associated with each role for a

vSphere Namespace. It specifies that the Owner role has full control, the Can Edit role is for managing workloads, and the Can View role is for read-only access.

Reference: VMware vSphere Product Documentation > vSphere with Tanzu Configuration and Management > "Managing User Permissions for vSphere Namespaces".

2. VMware vSphere Documentation, "vSphere with Tanzu Concepts": This guide explains the object hierarchy and security model, clarifying that permissions for TKG clusters are inherited from and controlled by the containing vSphere Namespace roles.

Reference: VMware vSphere Product Documentation > vSphere with Tanzu Concepts > "vSphere with Tanzu Security" section.

Question: 30

A group of new virtual machines have been deployed using thin-provisioned disks due to the limited storage space available in an environment. The storage team has expressed concern about extensive use of this type of provisioning. An administrator is tasked with creating a custom alarm to notify the storage team when thin provisioning reaches a certain capacity threshold. Where must the administrator define this alarm?

A: Datastore

B: Data center

C: Datastore cluster

D: Virtual machine

Correct Answer:

A

Explanation:

The alarm's purpose is to monitor storage capacity consumed by thin-provisioned disks. This is a characteristic and metric of the storage container itself, which is the datastore. In the vSphere Client, custom alarms are defined on specific inventory objects. To monitor datastore space utilization, the administrator must select the datastore object as the target for the alarm definition. The alarm trigger can then be configured using datastore-specific metrics, such as "Datastore Disk Usage on Thin-provisioned LUNs" or "Datastore usage on disk," to alert when a specified percentage threshold is crossed.

Why Incorrect Options are Wrong:

B: Data center: This is an organizational container. While an alarm can be defined here and propagated, it is not the specific object type whose capacity is being monitored.

C: Datastore cluster: This is a collection of datastores. While you can set aggregate usage alarms here, the most direct and fundamental object for monitoring individual storage capacity is the datastore.

D: Virtual machine: This is a consumer of storage, not the storage resource itself. The alarm's focus is on the datastore's capacity, which affects all VMs residing on it.

References:

1. VMware vSphere 8.0 Documentation, "Monitoring vSphere", section: "Create or Edit an Alarm Definition". This guide details the process of creating an alarm, which begins by selecting a specific inventory object, such as a datastore, on which to define the alarm.

2. VMware vSphere 8.0 Documentation, "Monitoring vSphere", section: "Alarm Triggers". This section lists the available event and condition triggers for different object types. For a datastore, triggers such as "Datastore usage on disk" are available, confirming that capacity-based alarms are defined at the datastore level.

3. VMware vSphere 8.0 Documentation, "vSphere Storage", section: "Monitoring Datastore Space Usage". This section explicitly states, "You can monitor space usage for all datastores in your data center. vCenter Server provides a default alarm that is triggered when a datastore usage exceeds the specified percentage." This reinforces that datastore usage monitoring and alarms are functions applied directly to datastore objects.