

Professional VMware vSphere 7.x

VMware 2V0-21.20

Version Demo

Total Demo Questions: 12

Total Premium Questions: 129

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Architectures and Technologies	43
Topic 2, VMware Products and Solutions	15
Topic 3, Planning and Designing	1
Topic 4, Installing, Configuring, and Setup	21
Topic 5, Performance-tuning, Optimization, and Upgrades	15
Topic 6, Troubleshooting and Repairing	7
Topic 7, Administrative and Operational Tasks	27
Total	129

QUESTION NO: 1

When deploying a vCenter Server Appliance, which two single sign-on (SSO)-related options are presented to an administrator? (Choose two.)

- A. Create a vCenter Enhanced Linked Mode group
- B. Create a vCenter Single Sign-On domain
- C. Join an existing vCenter Single Sign-On domain
- D. Repoint to another domain
- E. Reset Single Sign-On password

ANSWER: B C

Explanation:

During Stage 2 of a vCenter Server Appliance deployment, the administrator configures the appliance's vCenter Server Single Sign-On domain relationship. The deployment workflow presents the choice to create a vCenter Single Sign-On domain, which establishes a new SSO domain and makes the newly deployed vCenter Server the first vCenter Server instance in that domain. This is the appropriate selection for an initial vCenter Server deployment or when a separate SSO administrative boundary is required.

The workflow also presents the choice to join an existing vCenter Single Sign-On domain. Joining adds the new vCenter Server to an existing SSO domain and enables it to share the domain's identity infrastructure, including the common authentication domain and associated SSO services. This is the deployment choice used when adding a vCenter Server to an established environment, including environments intended to use Enhanced Linked Mode. VMware documents these deployment paths as the SSO configuration choices during installation: [vCenter Server Appliance deployment and SSO configuration](#) and [joining or creating an SSO domain](#).

QUESTION NO: 2

An administrator wants vSphere HA to restart a virtual machine when VMware Tools heartbeats are no longer received from the guest operating system.

Which vSphere HA feature should the administrator enable? (Choose the best answer.)

- A. VM Monitoring
- B. Host Monitoring
- C. Admission Control
- D. Datastore Heartbeating

ANSWER: A

Explanation:

VM Monitoring is correct because it monitors VMware Tools heartbeats from virtual machines. When the configured monitoring sensitivity determines that a guest is no longer responding, vSphere HA can reset or restart the affected virtual machine.

Host Monitoring detects ESXi host failures, whereas VM Monitoring is intended to detect failures of an individual guest operating system or its VMware Tools heartbeat. VMware Tools must be installed and running in the virtual machine for VM Monitoring to work. See the [vSphere Availability documentation](#).

QUESTION NO: 3

An administrator configures vSphere Replication for a virtual machine and needs the shortest supported recovery point objective (RPO).

What RPO should the administrator configure? (Choose the best answer.)

- A. 5 minutes
- B. 1 minute
- C. 15 seconds
- D. 0 minutes

ANSWER: A

Explanation:

The shortest supported vSphere Replication recovery point objective is **5 minutes**. The RPO defines the maximum amount of data that can be lost following recovery of a replicated virtual machine. vSphere Replication performs asynchronous replication, so it does not provide zero data loss in the same manner as synchronous replication technologies.

Configuring a shorter RPO increases the frequency of replication operations and can increase demand on network bandwidth, source storage, and target storage. The administrator should select an RPO that meets the application recovery requirements while accounting for available infrastructure capacity. See the [vSphere Replication documentation](#).

QUESTION NO: 4

A company has a vSphere environment consisting of the following characteristics:

- A content library named 'CORP' is published at corporate headquarters on a vCenter Server named 'vcenterCorp'.
- A regional data center contains a set of hosts managed by a vCenter Server named vcenterR1.
- vcenterR1 subscribes to the CORP content library.

The administrator wants to create a new virtual machine image to use on vcenterR1. What are two possible ways the administrator can accomplish this task? (Choose two.)

- A. Configure vcenterR1 to download all library content immediately.
- B. Upload the new image to the CORP library on vcenterR1.
- C. Publish the CORP content library on vcenterR1.
- D. Upload the new image to the CORP library on vcenterCorp.
- E. Upload the new image to a local content library on vcenterR1.

ANSWER: D E

Explanation:

Uploading the new image to the CORP library on vcenterCorp is a valid method because CORP is the published source library. After the item is added to that source library, the subscribed library on vcenterR1 receives its metadata during synchronization and can make the item available for deployment at the regional vCenter Server. The subscribed library can retrieve item content on demand or according to its configured download behavior, while the source library remains the authoritative location for centrally shared images.

Uploading the new image to a local content library on vcenterR1 is also valid. A local library is managed only by its associated vCenter Server and supports storing VM templates and OVF/OVA items for direct use within that vCenter Server inventory. This provides a regional, independently managed image location when the image does not need to be distributed from corporate headquarters or shared with other subscribing sites.

VMware content libraries are designed to support both centralized distribution through published and subscribed libraries and local storage for content that is specific to one vCenter Server. For details, see the [vSphere Content Library guide](#) and the [vSphere Content Library documentation](#).

QUESTION NO: 5

An administrator must prevent users from logging directly in to an ESXi host through the ESXi Host Client or DCUI. A small group of emergency administrators must retain direct access to the host.

Which configuration should the administrator use? (Choose the best answer.)

- A. Configure Lockdown Mode and add the emergency administrators as Exception Users.
- B. Configure a Host Profile and add the emergency administrators as profile users.
- C. Enable SSH and add the emergency administrators to the DCUI.Access advanced setting.
- D. Configure the host to use the vSphere vMotion TCP/IP stack.

ANSWER: A

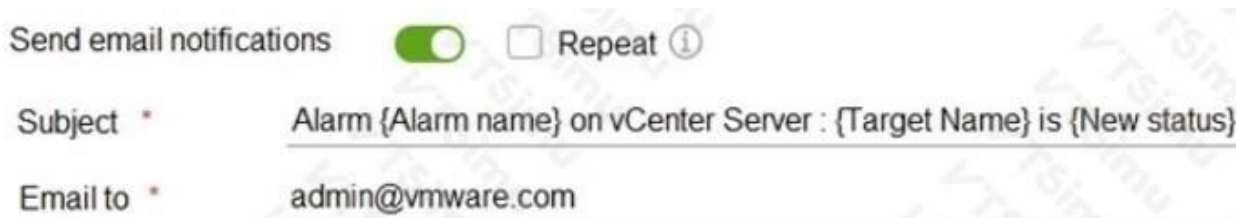
Explanation:

Configure Lockdown Mode and add the emergency administrators as Exception Users. Lockdown Mode restricts direct administrative access to an ESXi host and requires administrators to manage the host through vCenter Server. Exception Users are specifically permitted to access the host directly when Lockdown Mode is enabled, which provides a controlled break-glass access method.

The administrator should assign only required emergency accounts as Exception Users and manage routine host operations through vCenter Server. See the [vSphere Security documentation](#).

QUESTION NO: 6

Refer to the exhibit.



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 to resolve this issue? (Choose the best answer.)

- A. In vCenter Server General settings in the vSphere Client.
- B. In the alarm rule definitions
- C. In the ESXi host system config for the cluster node hosting the vCenter Server Appliance
- D. In Administration settings in the vCenter Server Management Interface

ANSWER: A

Explanation:

In **vCenter Server General settings in the vSphere Client**, is correct because alarm email actions only specify the recipient address and the event conditions that trigger notification. vCenter Server itself sends the message, so it must have a configured SMTP server and sender address before an alarm action can deliver email. In the vSphere Client, these global settings are configured from the vCenter Server's *Configure* tab under *Settings > General*, where the administrator supplies the mail server address and the sender account/address. After the SMTP details are saved, the alarm's existing "Send a notification email" action can use that centralized vCenter Server mail configuration whenever the alarm transitions into its configured state. This configuration applies to vCenter Server alarm notifications rather than being configured independently for every individual alarm or ESXi host. Ensure that the SMTP server is reachable from the vCenter Server Appliance and accepts relay from it; the specified sender address should also be permitted by the mail system. VMware's vSphere monitoring documentation describes configuring vCenter Server mail settings before using email alarm actions, and VMware's alarm documentation describes email as an alarm action managed by vCenter Server. See [Configure vCenter Server Mail Settings](#) and [vSphere Alarm Actions](#).

QUESTION NO: 7

Which two performance tools can be used to monitor virtual machines outside the guest operating system? (Choose two.)

- A. vCenter Server performance charts
- B. Task Manager
- C. top
- D. esxtop
- E. Perfmon

ANSWER: A D

Explanation:

vCenter Server performance charts and **esxtop** can monitor a virtual machine from the vSphere infrastructure layer, without installing or using a monitoring utility inside that VM's guest operating system. vCenter Server performance charts present collected performance metrics for inventory objects including virtual machines, hosts, clusters, datastores, and networks. For a virtual machine, these charts can show resource-consumption and performance data such as CPU, memory, disk, and network metrics as observed by vSphere.

esxtop is run from an ESXi host's shell or through a remote ESXi connection and provides detailed, real-time performance statistics from the hypervisor perspective. It can display per-virtual-machine CPU scheduling, memory, storage, and network data, making it particularly useful when investigating contention or latency that is visible outside the guest. Because both tools obtain their information through vCenter Server or ESXi rather than from within the VM, they satisfy the requirement to monitor virtual machines externally. VMware documents performance monitoring through vCenter Server and ESXi tools in the [vSphere Monitoring and Performance documentation](#) and describes esxtop usage in the [ESXTOP documentation](#).

QUESTION NO: 8

What can an administrator use to partition limited CPU and memory resources between two departments? (Choose the best answer.)

- A. vSphere distributed switch
- B. vSphere High Availability
- C. vCenter folders
- D. Resource pools

ANSWER: D

Explanation:

Resource pools are used to partition and manage available CPU and memory capacity among groups of virtual machines, such as separate departments. An administrator can create a resource pool for each department and assign relative CPU and memory shares, reservations, and limits. Shares establish each pool's relative priority when resource contention occurs, allowing the administrator to express that one department should receive a larger or smaller proportion of available resources. Reservations guarantee a minimum amount of CPU or memory for workloads in a pool, while limits prevent a pool from consuming more than a specified amount even if unused capacity exists elsewhere. Resource pools can also be nested, enabling allocation policies at departmental, application, and workload levels. This provides controlled resource distribution without requiring separate physical clusters for every department. VMware documents that resource pools divide available CPU and memory resources of a standalone host or a cluster into hierarchical resource groups, making them the appropriate vSphere construct for this requirement. See the [VMware vSphere Resource Management documentation](#) and the [resource pool configuration guidance](#).

QUESTION NO: 9

Which two VMware features are supported in a virtual machine using Intel Software Guard Extensions (Intel SGX) technology? (Choose two.)

- A. Fault tolerance
- B. vSphere vMotion
- C. VM encryption
- D. Virtual machine suspend and resume
- E. Storage I/O Control

ANSWER: C E

Explanation:

VM encryption and Storage I/O Control are supported for a virtual machine configured to use Intel Software Guard Extensions (Intel SGX). VM encryption protects a VM's files at rest, including its virtual disks and configuration data, through vSphere encryption and key management. This protection is complementary to Intel SGX, which provides hardware-based isolation for sensitive application code and data inside enclaves while the VM is running. Enabling SGX therefore does not preclude applying the normal vSphere VM-encryption capability to the workload.

Storage I/O Control is also supported because it is a datastore-level resource-management feature. It monitors datastore latency and can regulate the I/O share allocation of virtual machines when contention occurs. Its operation is independent of an SGX-enabled guest's enclave configuration, so an SGX workload can continue to receive controlled and prioritized datastore access according to the configured shares and limits. VMware documents the SGX virtual-machine configuration and its feature considerations in the [vSphere Client documentation](#).

QUESTION NO: 10

Which virtual disk option allows a virtual machine to consume the minimum storage capacity? (Choose the best answer.)

- A. Independent persistent
- B. Lazy-zeroed thick-provisioned
- C. Eager-zeroed thick-provisioned
- D. Thin-provisioned

ANSWER: D

Explanation:

Thin-provisioned is correct because it initially allocates only the storage space required for the virtual machine's current disk usage, rather than reserving the entire configured virtual disk capacity on the datastore. As data is written to the guest

operating system's virtual disk, the thin VMDK grows incrementally, up to its configured maximum size. This enables a virtual machine to consume the minimum capacity at deployment and can improve overall datastore utilization when multiple virtual machines have allocated disk capacity that they do not immediately use. For example, a virtual machine configured with a 100 GB virtual disk but containing only 15 GB of written data generally consumes approximately that amount of datastore space, plus VMDK metadata and any relevant overhead. Administrators must actively monitor datastore free space because thin disks can grow as workloads write additional data; datastore overcommitment can lead to capacity issues if growth is not managed. VMware documents thin provisioning as allocating blocks on demand, whereas thick disk formats reserve the full configured size when created. See the [vSphere storage provisioning documentation](#) and the [vSphere virtual disk configuration guidance](#).

QUESTION NO: 11

Which two features are only supported by VMFS6 datastores? (Choose two.)

- A. Concurrent access to shared storage
- B. On-disk locking
- C. Dynamic expansion
- D. 4K native storage devices
- E. Automatic space reclamation

ANSWER: D E

Explanation:

4K native storage devices and **Automatic space reclamation** are the VMFS6-specific capabilities in this question. VMFS6 supports datastores created on native 4 KB (4Kn) disk devices. This is important because 4Kn devices expose 4 KB logical sectors rather than emulating traditional 512-byte sectors, and VMFS6 provides the required filesystem support for using them as vSphere datastores.

VMFS6 also introduces automatic space reclamation through background UNMAP processing. When virtual-machine data is deleted or moved, ESXi can automatically issue UNMAP commands to compatible thin-provisioned storage, allowing the array to reclaim blocks that are no longer in use. This improves thin-provisioned capacity efficiency without requiring the administrator to run a manual reclamation operation. The feature depends on storage hardware that supports the relevant SCSI UNMAP capabilities, but VMFS6 provides the automatic, priority-based reclamation mechanism.

VMware documents VMFS6 support for 4Kn storage and its automatic space-reclamation behavior in the [vSphere Storage documentation](#) and describes datastore space reclamation in the [VMware space-reclamation guidance](#).

QUESTION NO: 12

Which two protocols can an administrator use as a backup location when creating a file-based backup of a vCenter Server Appliance? (Choose two.)

- A. FTP
- B. SCP
- C. SMB
- D. NFS
- E. VMFS

ANSWER: A B

Explanation:

FTP and SCP are supported protocols for file-based vCenter Server Appliance backups. The backup workflow copies the appliance configuration, inventory, and selected historical data to a remote backup location using a supported protocol. The backup can then be used to restore a new vCenter Server Appliance if the original appliance fails.

The administrator must ensure that the selected backup server is reachable, has adequate available storage, and is configured with the required credentials and permissions. See the [vCenter Server Configuration documentation](#).