

Associate VMware Data Center Virtualization Exam

VMware 1V0-21-20PSE

Version Demo

Total Demo Questions: 8

Total Premium Questions: 87

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, IT Architectures, Technologies, Standards	11
Topic 2, VMware Products and Solutions	41
Topic 3, Installing, Configuring, and Setup	17
Topic 4, Performance-tuning, Optimization, and Upgrades	8
Topic 5, Troubleshooting and Repairing	10
Total	87

QUESTION NO: 1

Which two storage protocols can a virtual infrastructure operator use to create a VMFS datastore? (Choose two.)

- A. Fibre Channel
- B. NFS
- C. iSCSI
- D. CIFS
- E. SMB

ANSWER: A C

Explanation:

Fibre Channel and iSCSI are the supported protocol types in this question because both present block-storage devices, or LUNs, to an ESXi host. After ESXi detects an available block device through either a Fibre Channel SAN fabric or an iSCSI storage network, an operator can partition and format that device with the VMware Virtual Machine File System (VMFS). The resulting VMFS datastore provides a shared clustered file system that multiple ESXi hosts can access concurrently, supporting core vSphere capabilities such as storing virtual machine files and enabling vMotion where the hosts have shared access to the datastore.

Fibre Channel uses dedicated Fibre Channel adapters and SAN connectivity to expose storage LUNs. iSCSI carries SCSI block commands over IP networks, using either software iSCSI, dependent hardware iSCSI, or independent hardware iSCSI adapters. Despite their different transports, both supply the block-device access required by VMFS. VMware identifies VMFS as a datastore type created on block storage devices and documents Fibre Channel and iSCSI among the supported storage protocols for ESXi hosts. See the [vSphere Storage documentation](#) and the [VMFS technical overview](#).

QUESTION NO: 2

Which vSphere feature protects against host hardware failures by restarting virtual machines (VMs) on hosts that are running in the cluster?

- A. vSphere HA
- B. vSphere vMotion
- C. vSphere Fault Tolerance
- D. vSphere DRS

ANSWER: A

Explanation:

vSphere HA is the vSphere cluster availability feature designed to provide automated recovery after an ESXi host fails. When vSphere High Availability is enabled on a cluster, the ESXi hosts monitor one another through network heartbeats. If a host failure is detected, HA identifies the virtual machines that were running on the failed host and restarts them on other surviving hosts in the same cluster, provided sufficient resources are available. This behavior directly addresses host hardware failure protection through VM restart and is the core recovery capability described in the question.

HA also uses datastore heartbeating to improve failure detection in certain network-isolation scenarios and can monitor individual virtual machines through VMware Tools or application monitoring when configured. Although a restart involves a brief service interruption, HA substantially reduces recovery time without requiring manual intervention. Administrators configure admission control policies to reserve enough cluster capacity so that virtual machines can be restarted following a host failure. VMware documents this capability in its [vSphere Availability documentation](#) and summarizes HA as an automated restart mechanism in the [vSphere Availability overview](#).

QUESTION NO: 3

Which storage protocol is supported by vSphere?

- A. NFS
- B. FTP
- C. CIFS
- D. SMB

ANSWER: A

Explanation:

NFS is supported by vSphere as a network-based datastore protocol. An ESXi host can mount an NFS export provided by a NAS storage system and use that export as a datastore for virtual-machine files, including configuration files, virtual disks, snapshots, and related files. vSphere supports both NFS version 3 and NFS version 4.1 datastores, subject to the applicable host, storage, and configuration requirements. This lets multiple ESXi hosts access shared storage through standard IP networking, enabling core vSphere capabilities that require shared datastores, such as vMotion and High Availability configurations when properly configured. NFS access is configured in vSphere by adding an NFS datastore and specifying the server name or IP address, the exported folder, and the NFS version. VMware documents NFS alongside other supported vSphere storage types, including VMFS on Fibre Channel, iSCSI, and Fibre Channel over Ethernet devices. See the [vSphere Storage documentation for NFS datastores](#) and VMware's [vSphere storage resource overview](#) for supported storage architecture and datastore guidance.

QUESTION NO: 4

What is the purpose of the VMware Tools balloon driver?

- A. To improve a VM's memory management capabilities
- B. To provide a high-resolution display for the VM's console
- C. To improve a VM's network performance
- D. To provide fast and efficient communication between VMs

ANSWER: A

Explanation:

The VMware Tools balloon driver improves a virtual machine's memory management capabilities by allowing the ESXi host to reclaim unused guest memory when the host experiences memory pressure. The driver, installed as part of VMware Tools, "inflates" inside the guest operating system by allocating guest physical memory. This causes the guest OS to free or page out less-active memory according to its own memory-management policies. ESXi can then repurpose the reclaimed machine memory for other virtual machines, helping the host manage memory overcommitment while maintaining efficient use of available RAM.

This mechanism is important because the guest operating system has better knowledge of which memory pages are least useful than the hypervisor does. Ballooning therefore provides a cooperative method for memory reclamation between ESXi and the guest OS. It is not intended to add memory to a VM; rather, it enables controlled reclamation of idle or less-active memory for the benefit of the host's overall workload. VMware documents the balloon driver as a VMware Tools component used for memory reclamation. See [vSphere Resource Management: Understanding Memory Overcommitment](#) and [Understanding memory ballooning in VMware](#).

QUESTION NO: 5

A system administrator has to configure several virtual machines for different business units. The administrator needs to enable features that allow overcommitment of resources while adhering to the business requirements and different department performance SLAs.

Which two features should the administrator enable to achieve this goal? (Choose two.)

- A. vSphere Distributed Power Management
- B. vSphere Fault Tolerance
- C. vSphere Resource Pools
- D. vSphere High Availability
- E. vSphere Storage I/O Control

ANSWER: C E

Explanation:

vSphere Resource Pools is appropriate because it groups virtual machines according to business unit or application requirements and allocates CPU and memory through reservations, limits, and shares. A reservation can protect a minimum amount of capacity for an important department, while shares establish relative entitlement when the cluster is contended. This enables resource overcommitment without treating every workload equally: higher-priority pools retain preferential access to CPU and memory as demand rises. Resource pools can also be arranged hierarchically to reflect organizational or service-level boundaries.

vSphere Storage I/O Control complements this approach for shared datastore performance. It monitors datastore latency and, when a datastore is congested, uses configurable I/O shares to distribute available storage performance fairly among virtual machines according to their assigned priority. This makes it possible to consolidate workloads onto shared storage while preserving differentiated storage-performance treatment for workloads with separate SLAs. Together, these features apply policy-based prioritization to compute, memory, and storage I/O resources during contention, which is the essential control needed in an overcommitted virtual infrastructure. VMware documents these resource-allocation controls in the [vSphere Resource Management documentation](#) and describes storage-I/O resource management in the [vSphere Resource Management guide](#).

QUESTION NO: 6

What is the default encrypted vSphere vMotion state for virtual machines that are not encrypted?

- A. Disabled
- B. Required
- C. Opportunistic
- D. Enabled

ANSWER: C

Explanation:

Opportunistic is the default encrypted vSphere vMotion setting for a virtual machine that is not itself encrypted. With this setting, vSphere attempts to encrypt the virtual machine's migration traffic when the participating hosts support encrypted vMotion. This provides protection for the memory and state data transferred during a live migration without requiring administrators to configure encryption separately for every ordinary, unencrypted virtual machine. If encryption cannot be used because the required host capabilities are unavailable, the migration can proceed without encrypted vMotion traffic. This behavior makes Opportunistic a practical default: it uses encryption whenever the environment can provide it while retaining migration compatibility. VMware documents encrypted vMotion as a distinct setting from virtual machine encryption and describes Opportunistic as the default policy for unencrypted virtual machines. For configuration details and policy behavior, see the VMware vSphere Security documentation on [vMotion Encryption](#) and the [vSphere Security guide](#).

QUESTION NO: 7

An administrator is copying a powered-off virtual machine to another datastore by using the datastore browser.

The virtual machine has no snapshots.

Which two files contain the virtual disk definition and virtual disk data that must be copied? (Choose two.)

- A. The .vmdk descriptor file
- B. The -flat.vmdk data file
- C. The .vmx configuration file
- D. The .vmsd snapshot metadata file
- E. The .vmtx template configuration file

ANSWER: A B

Explanation:

A virtual disk normally consists of a small .vmdk descriptor file and a corresponding -flat.vmdk file that contains the virtual disk data. Both files are required for the virtual machine to access that virtual disk after it is copied.

The .vmx file contains the virtual machine configuration rather than the virtual disk data. A .vmsd file stores snapshot metadata, and a .vmtx file is associated with a virtual machine template configuration.

QUESTION NO: 8

A vSphere administrator is unable to remove an ESXi host from a

vSphere Distributed Switch (VDS).

Which two reasons could have caused this issue?

- A. The VDS is configured with ingress traffic shaping.
- B. Virtual machines network adapters on the host are connected to the switch
- C. Virtual machine network adapters are faulty.
- D. The ESXi host is connected to another VDS.
- E. The ESXi host had VMkernel adapters assigned to the switch.

ANSWER: B E

Explanation:

Removing an ESXi host from a vSphere Distributed Switch requires that the host no longer use distributed-switch resources that would lose connectivity when the association is removed. Therefore, *Virtual machines network adapters on the host are connected to the switch* is a valid cause: virtual machines running on that host can have virtual NICs attached to distributed port groups on the switch. Those virtual NICs must be migrated to an appropriate port group on another switch, or the affected virtual machines must be migrated or powered off as appropriate, before the host can be removed safely.

The ESXi host had VMkernel adapters assigned to the switch is also a valid cause. VMkernel adapters provide essential host services, such as management traffic, vMotion, vSAN, IP storage, Fault Tolerance logging, and provisioning traffic. Before removing the host from the distributed switch, an administrator must migrate each VMkernel adapter and its associated physical uplinks to a suitable standard switch or another distributed switch. This preserves the host's required network paths and prevents management or service disruption. VMware documents these host networking migration and distributed-switch management requirements in the [vSphere Networking documentation](#) and the [vSphere Distributed Switch configuration documentation](#).