DUMPSBOSS.

Associate VMware Data Center Virtualization

VMware 1V0-21.20

Version Demo

Total Demo Questions: 12

Total Premium Questions: 123

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, IT Architectures, Technologies, Standards	13
Topic 2, VMware Products and Solutions	45
Topic 3, Installing, Configuring, and Setup	17
Topic 4, Performance-tuning, Optimization, and Upgrades	11
Topic 5, Troubleshooting and Repairing	11
Topic 6, Administrative and Operational Tasks	26
Total	123

QUESTION NO: 1

An administrator has observed an alert message in the vSphere UI related to a host's storage sensor hardware. Where should the administrator look for more information related to this alert?

A. Menu > Lifecycle Manager > Baselines

B. Host > Monitor > Skyline Health

C. Host > Monitor > Hardware Health > Storage Sensors

D. Host > Monitor > Hardware Health > System Event Log

ANSWER: C

Explanation:

Host > Monitor > Hardware Health > Storage Sensors is the appropriate location because the alert specifically concerns hardware storage sensors on an ESXi host. The Hardware Health view presents sensor data reported by the host hardware and its management controller, allowing an administrator to inspect the health state and details associated with storage-related components. Selecting Storage Sensors narrows the displayed information to the relevant sensor category, such as storage-controller, disk, enclosure, or other vendor-exposed storage hardware conditions. This lets the administrator correlate the vSphere alert with the underlying sensor status and determine whether the condition requires hardware investigation or remediation. VMware documents that host hardware health information is accessed from the host monitoring views and is populated from the hardware monitoring interfaces available to ESXi. The vSphere monitoring documentation is available from Broadcom TechDocs: vSphere Monitoring and Performance. Additional VMware guidance on viewing and troubleshooting host hardware sensor health is available through Broadcom Knowledge Base.

QUESTION NO: 2

Which VMware feature would an administrator configure to migrate

VMs using vSphere vMotion between ESXi hosts with different

underlying CPU Architectures?

A. Enhanced vMotion Compatibility

B. VSphere HA

C. VMware Fault Tolerance

D. vSphere Storage DRS

ANSWER: A

Explanation:

Enhanced vMotion Compatibility is the feature used to enable vMotion between ESXi hosts whose CPUs have different generations or feature sets, provided the processors are compatible with an available EVC baseline. EVC establishes a common CPU feature baseline for every host in a cluster by masking newer CPU instructions that are not present on older compatible hosts. As a result, a virtual machine sees a consistent virtual CPU feature set regardless of the host on which it runs. This consistency is essential because vMotion transfers a running virtual machine without changing the CPU capabilities exposed to its guest operating system. An administrator configures EVC at the cluster level and selects the appropriate vendor-specific baseline, such as an Intel or AMD baseline supported by all hosts to be included. Hosts must still use CPUs from the same vendor family; EVC does not make Intel and AMD processors mutually compatible. VMware also documents that EVC can be enabled before hosts are added to a cluster, or an appropriate baseline can be chosen when existing hosts and workloads meet the requirements. See Broadcom's Enhanced vMotion Compatibility processor compatibility guidance and the vSphere Resource Management documentation.

QUESTION NO: 3

Which two vSphere features help address an organization's business availability challenges? (Choose two.)

A. vSphere Fault Tolerance

B. vSphere Pod Service

C. vSphere DPM

D. vSphere Trust Authority

E. vSphere High Availability

ANSWER: A E

Explanation:

vSphere Fault Tolerance and vSphere High Availability directly address business availability by helping workloads remain available when ESXi host failures occur. vSphere High Availability monitors hosts in a cluster and, following a host failure, automatically restarts the affected virtual machines on other available hosts. This provides automated recovery and reduces the duration of service interruption without requiring manual intervention. vSphere Fault Tolerance provides a higher level of protection for selected virtual machines by maintaining a live secondary copy on another host. If the host running the primary virtual machine fails, the secondary instance takes over without interruption or data loss for the protected workload. Together, these capabilities support availability requirements with different recovery objectives: automated restart through vSphere High Availability and continuous availability through vSphere Fault Tolerance. VMware describes these availability capabilities in the vSphere Availability documentation at vSphere Availability and its overview of vSphere Fault Tolerance.

QUESTION NO: 4

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 and **vSphere Storage I/O Control** provide the controls needed to safely share and overcommit infrastructure resources while maintaining business-unit priorities. Resource pools create logical groupings of virtual machines and allow the administrator to allocate CPU and memory through reservations, limits, and shares. Shares establish relative priority when demand exceeds available capacity, while reservations can protect a minimum amount of CPU or memory for workloads that have a defined service-level requirement. This lets separate departments consume a common cluster without giving every virtual machine an equal claim on constrained compute resources.

Storage I/O Control extends this priority-based approach to shared datastore performance. It uses storage shares to prioritize the I/O access of virtual machines when a datastore experiences contention. Administrators can therefore assign higher relative importance to workloads with stricter storage-performance requirements and lower importance to less critical departmental workloads. Together, these features address resource contention at both compute and storage layers, enabling consolidation and resource overcommitment while applying differentiated service levels. VMware documents resource-pool allocation settings in the vSphere Resource Management documentation and describes datastore I/O prioritization in its Storage I/O Control documentation.

QUESTION NO: 5

Which two security policy settings are available on a vSphere Standard Switch port group? (Choose two.)

A. MAC Address Changes

B. Forged Transmits

C. Storage I/O Control

D. CPU reservation

E. Datastore heartbeating

ANSWER: A B

Explanation:

MAC Address Changes and **Forged Transmits** are security policy settings available on a vSphere Standard Switch port group. MAC Address Changes controls whether ESXi accepts traffic when a guest operating system changes the MAC address of its virtual network adapter. Forged Transmits controls whether ESXi allows outbound frames with a source MAC address that differs from the MAC address assigned to the virtual adapter. These settings, along with Promiscuous Mode, can be configured to Accept or Reject. See the vSphere Networking documentation.

QUESTION NO: 6

Which piece of information does vSphere DRS consider when

making decisions about which host to place a virtual machine?

A. Network bandwidth on the host

B. Disk usage by the virtual machine

C. Storage bandwidth on the host

D. Network usage by the virtual machine

ANSWER: A

Explanation:

Network bandwidth on the host is correct because Distributed Resource Scheduler evaluates host resource availability when making virtual-machine placement and balancing decisions. In addition to its core CPU and memory resource analysis, DRS can account for the available network capacity of an ESXi host so that a placement decision does not unnecessarily concentrate network demand on a host with constrained bandwidth. This host-level information helps DRS select a destination that can support the virtual machine's operational requirements while maintaining balanced resource utilization across the cluster. The purpose is not merely to find a host with sufficient compute capacity, but to make an informed cluster-wide placement decision using relevant host resource information. This is particularly important in environments where workloads generate meaningful network traffic, such as application tiers communicating with databases, storage traffic using IP-based protocols, or virtual machines serving large numbers of clients. vSphere DRS continuously monitors cluster resource conditions and can recommend or perform migrations according to the configured automation level. For VMware's overview of DRS capabilities, see VMware vSphere Distributed Resource Scheduler. Additional vSphere resource-management documentation is available from the vSphere 7 Documentation.

QUESTION NO: 7

Which two guest operating systems are supported when a virtual

machine must be deployed?

A. iOS

B. Microsoft Windows

C. Android

D. MacOS

E. T/TOS (tandem Transactional OS)

ANSWER: B D

Explanation:

Microsoft Windows is a supported guest operating-system family for vSphere virtual machines. When creating a VM, the selected guest OS family and version establish appropriate default virtual hardware and compatibility settings, and Windows releases are represented in VMware's supported guest OS compatibility information.

MacOS is also supported as a vSphere guest operating system, subject to Apple's licensing terms and VMware's platform requirements. In particular, macOS virtual machines must run on Apple-branded hardware; administrators should also select the applicable macOS version and confirm that the target ESXi/vSphere release supports it. VMware's compatibility information is authoritative for verifying support for a specific guest OS release, virtual hardware version, and ESXi version before deployment. See the VMware Compatibility Guide for supported guest OS combinations and Apple's macOS Software License Agreement for the Apple-branded-hardware virtualization condition.

QUESTION NO: 8

An administrator notices a virtual machine named vm01 is missing

from the inventory, but the configuration files can be located.

Which file should the administrator click on to register the VM?

A. vm01.vmdk

B. vm01.vmsd

C. vm01.vmx

D. vm01.nvram

ANSWER: C

Explanation:

vm01.vmx is the correct file to select because it is the virtual machine's primary configuration file. The .vmx file contains the settings that define the virtual machine, including its virtual hardware configuration, guest operating system type, memory and CPU allocation, virtual network adapters, and references to the VM's virtual disks. When a VM is missing from vCenter Server or an ESXi host inventory but its files remain accessible on a datastore, an administrator can browse the datastore, locate the VM's .vmx file, and use the registration action to add that existing VM back into inventory. Registration does not recreate the VM or copy its files; it restores the inventory record by reading the configuration stored in the .vmx file. After registration, the VM can be managed normally and, if its referenced files are intact and accessible, powered on. VMware's vSphere documentation describes registering a virtual machine by browsing datastore files and selecting the VM configuration (.vmx) file. See the vSphere documentation on registering virtual machines and VMware's knowledge base guidance for registering an existing virtual machine.

QUESTION NO: 9

A vSphere cluster running a virtual machine with VMware HA and

DRS enabled in fully automated mode is experiencing a catastrophic host

failure.

Which action can the administrator expect DRS to take?

A. It will move the VM to a host on a different cluster with enough resources after the HA rstart.

B. It will pro-actively move the virtual machine to a different host.

C. It will move the VM to a host in the same cluster with enough resources after the HA restart.

D. It will pro-actively move the virtual machine to a different cluster.

ANSWER: C

Explanation:

It will move the VM to a host in the same cluster with enough resources after the HA restart. When a host suffers a catastrophic failure, VMware HA detects the failure and restarts the affected virtual machines on surviving hosts in the configured HA cluster. Because DRS is enabled, it can participate in selecting an appropriate placement that satisfies the virtual machine's resource requirements and applicable cluster constraints. After the VM is restarted, DRS in fully automated mode continues to evaluate cluster load and may automatically perform vMotion migrations within that cluster to maintain resource balance. The key point is that HA provides restart availability following the host failure, while DRS supplies resource-aware placement and ongoing load balancing for hosts that are members of the same DRS cluster. VMware documents the HA restart process and its integration with DRS placement in the vSphere Availability documentation. DRS automation and its automated migration behavior are described in the vSphere Resource Management documentation.

QUESTION NO: 10

Which vSphere component centralizes automated patch and version management for clusters. ESXi. drivers and firmware. Virtual Hardware, and VMware Tools?

A. vSphere DRS

B. VMware Cloud Foundation

C. Content Library

D. vSphere Lifecycle Manager

ANSWER: D

Explanation:

vSphere Lifecycle Manager is the vSphere component that provides centralized lifecycle and image management for ESXi hosts and clusters. It can use a desired-state cluster image to define and apply a validated software specification, including the ESXi version, vendor add-ons, and firmware and driver add-ons supplied through supported hardware integrations. Lifecycle Manager assesses cluster compliance against that desired image and orchestrates remediation while using vSphere capabilities such as maintenance mode and, where available, DRS to minimize workload disruption. It also manages VMware Tools upgrades and virtual machine hardware compatibility upgrades through lifecycle management baselines or related upgrade workflows. This centralized approach enables administrators to standardize software versions across hosts, check for drift, and safely bring clusters into compliance rather than manually patching hosts one at a time. VMware documents vSphere Lifecycle Manager as the service for managing ESXi images, baselines, and cluster remediation in the vSphere Lifecycle Manager documentation. For the cluster-image model and the included ESXi, vendor add-on, firmware, and driver components, see the Using vSphere Lifecycle Manager Images guide.

QUESTION NO: 11

Which two physical resources are abstracted by the hypervisor and presented to virtual machines? (Choose two.)

A. CPU

B. Libraries

C. Application

D. Desktop

E. Memory

ANSWER: A E

Explanation:

CPU and **Memory** are physical host resources that the VMware hypervisor abstracts and exposes to each virtual machine as virtual hardware. A virtual machine is configured with one or more virtual processors and a specified amount of virtual memory, while the hypervisor schedules and manages access to the underlying host processors and physical RAM. This abstraction lets multiple virtual machines run independently on the same ESXi host while maintaining the impression that each guest operating system has its own dedicated compute and memory resources. VMware resource-management controls, such as shares, reservations, and limits, govern how processor time and physical memory are allocated when contention occurs. The virtual machine therefore consumes virtual CPU and virtual memory resources rather than interacting directly with a particular physical processor or memory module. This hardware abstraction is a foundational characteristic of server virtualization and enables workload consolidation, isolation, and flexible allocation of host capacity. VMware's vSphere documentation describes CPU and memory as core resources managed for virtual machines and explains how ESXi presents virtual hardware to guests. See the vSphere Resource Management documentation and the vSphere Virtual Machine Administration documentation.

QUESTION NO: 12

Which two block storage protocols are supported on vSphere?

A. Fibre Channel (FC)

B. SMB

C. iSCSI

D. NFSv3

ANSWER: A C

Explanation:

Fibre Channel (FC) and iSCSI are supported block-storage connectivity protocols for vSphere. Both present block devices, known as LUNs, to ESXi hosts, where they can be used as VMFS datastores. With Fibre Channel, ESXi accesses LUNs through Fibre Channel host bus adapters and a Fibre Channel storage fabric. This is a traditional storage-area-network implementation designed for dedicated, high-performance storage connectivity. iSCSI carries SCSI block commands over standard TCP/IP networking, enabling ESXi hosts to access storage LUNs across Ethernet networks. ESXi supports iSCSI through either software iSCSI adapters or supported hardware iSCSI adapters. After the host discovers and claims the presented LUNs, vSphere can format eligible devices with VMFS and make that datastore available for virtual-machine files. VMware's storage documentation identifies Fibre Channel and iSCSI among the supported block-storage protocols and explains the ESXi storage-adapter model used to access these devices. See the vSphere Storage documentation on storage types and the vSphere documentation on iSCSI storage.