PassQueen
a.k.a dumpsqueen.com

VCE Vblock™ Systems Deployment and Implementation - Core Exam

VCE 210-010

Version Demo

Total Demo Questions: 15

Total Premium Questions: 156

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

An ESXi host connected to a Vblock System 720 storage array requires a new 2 TB LUN.

According to VCE best practice, which type of device must be created to add to the host?

A. 4 member striped meta

B. 4 member concatenated meta

C. 8 member striped meta

D. 8 member concatenated meta

ANSWER: C

Explanation:

8 member striped meta is the appropriate device for presenting a new 2 TB LUN to an ESXi host in a Vblock System 720 configuration. Vblock 720 systems use EMC Symmetrix VMAX storage, where a meta device combines multiple Symmetrix hypers into one larger host-addressable device. For a 2 TB LUN, the prescribed layout is an eight-member striped meta, producing the required capacity from eight approximately 240 GB member devices.

Striping distributes I/O across all meta members rather than directing sequential ranges of the LUN to individual members. This gives the VMware datastore or raw device mapping consistent access to the aggregate performance available from the underlying members and aligns the LUN with the validated Vblock storage-design practice. Creating the device in this format also supports predictable operational procedures for masking, presentation through the SAN, and subsequent VMware use.

VMware documents the supported use of VMFS datastores and storage devices with ESXi in its vSphere Storage documentation. Dell Technologies provides current Symmetrix VMAX product and documentation resources at Dell EMC VMAX All Flash.

QUESTION NO: 2

Which two virtual machines are deployed as part of the Advanced Management Pod (AMP)? (Choose two.)

A. VMware View Connection server

B. VMware Update Manager server

C. Cisco Adaptive Security Appliance

D. VMware vCenter server

ANSWER: B D

Explanation:

The Advanced Management Pod (AMP) provides the dedicated virtualized management environment used to operate and maintain a Vblock system. **VMware vCenter server** is deployed in the AMP because it is the central VMware management platform for administering the vSphere inventory, hosts, clusters, virtual machines, permissions, and operational tasks. The AMP separates this essential management function from the workload resources being managed.

VMware Update Manager server is also deployed as an AMP virtual machine. VMware Update Manager, subsequently incorporated into vSphere Lifecycle Manager, supports the lifecycle-management process for ESXi hosts, including baselines or desired images, remediation, and coordinated software/firmware update workflows. Locating it in the management pod makes it available to support the managed compute environment without requiring a workload VM to provide that service.

Together, these management virtual machines support the AMP's role as the platform's administration and maintenance layer. VMware's vCenter documentation describes vCenter Server as the centralized management component for vSphere environments, while lifecycle-management documentation covers host update and remediation operations: VMware vCenter Server documentation and vSphere Lifecycle Manager documentation.

QUESTION NO: 3

A customer would like to add a new production VLAN to their Vblock System with UIM/P. The VLAN was added to the UIM/P service profile, and the connected Cisco Nexus 5000. The customer is still not able to use the new VLAN with a virtual machine.

Which step must the customer complete?

A. Create a new VSAN.

B. Add the VLAN to Cisco Nexus 1000V.

C. Add the VLAN to Cisco Catalyst 3560.

D. Disable spanning tree on UCS.

ANSWER: B

Explanation:

Add the VLAN to Cisco Nexus 1000V. The VLAN must be configured throughout every relevant layer of the virtual-network path before a virtual machine can use it. Adding it to the UIM/P service profile makes the VLAN available through the UCS-side configuration, and configuring the connected Cisco Nexus 5000 provides the required physical-switch connectivity. However, when Cisco Nexus 1000V is used as the virtual switch, it also controls the port profiles and virtual Ethernet ports presented to virtual machines. The new VLAN therefore needs to be defined and permitted in the applicable Nexus 1000V port profile or VLAN configuration. Once that configuration is in place, the appropriate virtual-machine network/port group can expose the production VLAN to the guest virtual machine, with the intended VLAN tag carried across the uplinks. This is consistent with Cisco Nexus 1000V documentation, which describes creating VLANs and associating them with port profiles used by virtual machine interfaces. See the Cisco Nexus 1000V VLAN configuration guide and Cisco's Nexus 1000V product documentation for the virtual-switch VLAN and port-profile model.

QUESTION NO: 4

VCE support asks you to collect VMware diagnostic logs from an ESXi host.

Which two management tools would you use to accomplish this task? (Choose two.)

A. vSphere Client connected to ESXi host

B. VMware Update Manager (VUM) server

C. vSphere client connected to vCenter Server

D. VMware vCenter SQL database

ANSWER: A C

Explanation:

vSphere Client connected to ESXi host and **vSphere client connected to vCenter Server** can both collect an ESXi diagnostic support bundle. When the client is connected directly to an ESXi host, an administrator can use the host's management interface to export system logs and configuration information for that individual host. This produces the diagnostic data needed by support, including ESXi logs and relevant host-state information.

When the client is connected to vCenter Server, the administrator can select the affected ESXi host from inventory and invoke the log-export or support-bundle workflow centrally. Centralized collection is especially useful in a managed Vblock

environment because it provides access to hosts through the vCenter inventory and can coordinate collection without requiring the administrator to connect separately to every host. In either case, the resulting archive can be supplied to VCE or VMware support for troubleshooting. VMware documents host log collection as part of exporting diagnostic information through vSphere management interfaces; see the vSphere Monitoring and Performance documentation and the Broadcom VMware Knowledge Base.

QUESTION NO: 5

Where does a system administrator configure virtual machine affinity rules in VMware vCenter?

A. HA settings

B. DPM settings

C. virtual machine settings

D. DRS settings

ANSWER: D

Explanation:

Virtual machine affinity rules are configured in **DRS settings** for a vSphere cluster. VMware Distributed Resource Scheduler (DRS) evaluates resource availability across the hosts in the cluster and applies placement rules when initially powering on virtual machines and, depending on the cluster's automation configuration, during ongoing load balancing. Administrators create VM/Host rules to control whether specified virtual machines must run on particular hosts, should run on particular hosts, or must not run on particular hosts. They can also configure VM/VM affinity rules that keep selected virtual machines together, as well as anti-affinity rules that separate them across hosts for availability or workload-isolation purposes. In the vSphere Client, these rules are managed from the cluster configuration under DRS, typically through the VM/Host Rules area. This makes DRS the appropriate location because affinity is a cluster-level placement and scheduling policy rather than an individual virtual-machine setting. For VMware's current configuration guidance, see VMware vSphere Resource Management documentation and the VM/Host affinity rules documentation.

QUESTION NO: 6

How many parity disks are in a RAID 5 configuration?

A. 1

B. 2

C. 3

D. 4

ANSWER: A

Explanation:

RAID 5 uses distributed parity and has the equivalent of one disk's capacity allocated to parity across the RAID set. Therefore, **1** is correct. Parity is not stored permanently on one dedicated physical drive; instead, parity blocks are spread among all member disks. This distribution helps avoid concentrating parity I/O on a single disk while still allowing the array to reconstruct data if one member drive fails.

For capacity planning, a RAID 5 group containing *N* equal-sized disks provides usable capacity equivalent to *N − 1* disks, because one disk's worth of total capacity is consumed by the distributed parity information. RAID 5 is designed to tolerate a single disk failure, provided the failed disk is replaced and the array can rebuild successfully. This single-parity design distinguishes RAID 5 from dual-parity layouts, which reserve the equivalent capacity of two disks. Dell's storage documentation describes RAID 5 as using distributed parity with capacity overhead equal to one drive: Dell RAID types overview. Additional RAID-level guidance is available from NetApp RAID overview.

QUESTION NO: 7

-- Exhibit --

-- Exhibit --

Click the Exhibit button.

Vblock Systems have multiple power connector capabilities.

Which power receptacle is shown in the exhibit?

A. 30A 250V, 3 phase (NEMA L15-30P)

B. 60A 250V,3 phase (IEC 60309)

C. 60A 120V, 3 phase (IEC 60309)

D. 30A 120V, 3 phase (C8303 L6-30P)

ANSWER: A

Explanation:

The receptacle shown is identified as a 30A 250V, 3 phase (NEMA L15-30P) connection. NEMA locking-device nomenclature conveys both the electrical rating and the connector family: the L15 pattern is a locking configuration intended for three-phase, 250 V AC service, and the 30 suffix denotes a 30-ampere rating. This connector type uses a twist-lock interface, helping prevent an equipment power lead from being unintentionally disconnected in a data-center or infrastructure environment. The matching connector geometry and rating are important when planning Vblock System power because the branch-circuit capacity, voltage, phase arrangement, and plug/receptacle configuration must all align with the system's power-distribution design. NEMA's locking plug and receptacle standard defines the dimensional and configuration requirements used to distinguish these devices, including the L15 family. See NEMA's Locking Plugs and Receptacles standards information and Leviton's 30 A locking L15-30 device listing for the stated three-phase, 250 V, 30 A configuration.

QUESTION NO: 8

Which protocol is used to provide unified file storage connectivity to a Vblock System 320?

A. FCoE

B. IP

C. iSCSI

D. FC

ANSWER: B

Explanation:

IP is used to provide unified file storage connectivity because file services on the unified storage platform are delivered over Ethernet/IP networks. This enables client systems to access shared file data using file-level protocols such as NFS for UNIX/Linux environments and SMB/CIFS for Windows environments. In a Vblock System 320 design, the unified storage file component presents file shares through IP interfaces, with the network infrastructure carrying that client-to-file-service traffic. This model is what makes the storage “unified”: it can provide both block storage services and NAS file services, while file access remains based on standard IP networking. IP connectivity also allows file clients to use familiar Ethernet switching, VLAN segmentation, routing, and IP-address-based service interfaces when reaching the file storage service. Dell documentation for Vblock systems and their component support resources is available through the Dell Vblock Series support documentation. For background on Dell unified storage file protocols and IP-based NAS access, see the Dell Unity NAS capabilities documentation.

QUESTION NO: 9

Your manager asks you to configure an external Syslog on VMware ESXi hosts.

In which two ways would the Syslog be configured? (Choose two.)

A. using the vSphere client

B. using the esxcli system syslog command

C. using VMware Update Manager

D. using the VMware SQL database

ANSWER: A B

Explanation:

External Syslog forwarding on an ESXi host can be configured through the vSphere Client or from the ESXi command line with the `esxcli system syslog` command namespace. In the vSphere Client, an administrator selects the host and configures its advanced Syslog settings, including the remote logging destination, normally through the `Syslog.global.logHost` setting. This provides a central GUI-based method for setting the remote Syslog target on managed hosts.

The ESXCLI method supports the same operational need through automation or direct host administration. Administrators can use commands such as `esxcli system syslog config set` to specify the remote log host and `esxcli system syslog reload` to apply the revised configuration. This approach is particularly useful in deployment procedures, scripted configuration, and troubleshooting when vCenter Server or the graphical client is not available.

After setting the destination, the ESXi Syslog service forwards host log data to the configured remote collector, helping preserve diagnostic information and support centralized monitoring. VMware documents the ESXCLI Syslog command set in the ESXCLI Command Reference and describes host configuration through the vSphere Monitoring and Performance documentation.

QUESTION NO: 10

You are deploying a Vblock System and you are unable to log in to the vCenter server using single sign-on (SSO).

Which two steps should be verified? (Choose two.)

A. Log in credentials are correct.

B. vCenter server is licensed.

C. vCenter services are started.

D. The single sign-on server is licensed.

ANSWER: A C

Explanation:

Verify that the log-in credentials are correct and that the vCenter services are started. SSO authentication first requires a valid account name and password in the appropriate SSO identity source or vSphere domain. During initial deployment, credentials can be entered with an incorrect domain, an incorrect administrator account, or an invalid password, so confirming the exact account format and password is an essential first troubleshooting step.

The vCenter Server components that support authentication must also be running. In the vSphere versions commonly used with Vblock deployments, SSO is delivered through vCenter Server services; if the required services have not started successfully, or have stopped, users cannot complete an SSO-based login even when their credentials are valid. Checking service status and ensuring the relevant vCenter/SSO services are started restores the server-side authentication path. VMware's vSphere documentation describes vCenter Single Sign-On as the authentication service used by vSphere components, and Broadcom provides the current vSphere technical documentation portal for service and authentication administration guidance: Broadcom vSphere Technical Documentation and Broadcom VMware Knowledge Base.

QUESTION NO: 11

A SAN administrator must use the zone commit command to activate a zone set on a Cisco MDS 9148.

Which feature is enabled on the switch?

A. hardware zoning by access control lists

B. enhanced zoning

C. extended broadcast zoning

D. basic zoning

ANSWER: B

Explanation:

enhanced zoning is enabled. Cisco MDS switches support both basic and enhanced zoning modes, but enhanced zoning introduces a commit-based workflow to protect the active zoning database from conflicting or incomplete changes. In this mode, an administrator first makes zoning changes in a session-specific copy of the zoning configuration. The changes do not affect the fabric's active zoneset until the administrator explicitly issues `zone commit`. The commit operation validates and distributes the pending zoning database changes, then activates the updated configuration in a controlled manner.

This workflow is especially important in a shared Fibre Channel SAN because zoning controls which initiators and targets can communicate. Requiring an explicit commit provides transactional behavior: administrators can review a complete group of aliases, zones, and zoneset changes before publishing them to the fabric. Cisco documents enhanced zoning as the zoning mode that uses zoning sessions and requires the `zone commit` command to commit changes. For implementation details, see Cisco's MDS NX-OS Zoning Configuration Guide and the MDS NX-OS Command Reference.

QUESTION NO: 12

Which three identity values can be assigned to a Cisco UCS service profile from an identity pool? (Choose three.)

A. MAC address

B. WWPN

C. UUID

D. Datastore UUID

E. VLAN ID

ANSWER: A B C

Explanation:

A Cisco UCS service profile can receive a **MAC address** for a virtual NIC, a **WWPN** for a virtual HBA, and a **UUID** for the server identity. UCS Manager assigns these values from the applicable identity pools and applies them when the service profile is associated with a server.

This identity abstraction is a central UCS capability because the server configuration and its network and SAN identities can be applied consistently to replacement or newly associated hardware. Cisco documents identity pools and service-profile configuration in the Cisco UCS Manager configuration guides.

QUESTION NO: 13

Which port is used for communication between EMC Secure Remote Support (ESRS) and the Policy Manager?

A. 443

B. 5414

C. 8090

D. 8443

ANSWER: D

Explanation:

8443 is used for communication between EMC Secure Remote Support (ESRS) and the Policy Manager. In an ESRS deployment, the Policy Manager provides centralized policy, access-control, and configuration services for ESRS components. The ESRS implementation uses TCP port 8443 for this protected management communication, allowing the components to exchange the information needed to apply remote-support policies and maintain the trusted ESRS relationship. Network and firewall planning must therefore permit the required TCP 8443 path between the ESRS component and the Policy Manager; otherwise, policy-related connectivity and management functions cannot operate as designed. This port should be documented during deployment along with the source and destination systems, rather than being opened broadly across unrelated network segments. Dell's support documentation provides Secure Remote Services technical resources and deployment guidance, while the VCE documentation portal provides product documentation for Vblock environments: Dell Secure Remote Services documentation and Dell Technologies documentation.

QUESTION NO: 14

You are required to log in to a Cisco UCS C220 CIMC to validate the firmware.

What are two ways to launch and obtain the login prompt? (Choose two.)

A. http://ipaddress

B. http://ipaddress/cimc

C. https://hostname

D. https://ipaddress/cimc

ANSWER: A C

Explanation:

The CIMC management interface can be reached through a web browser by using the controller's configured network identity. Entering `http://ipaddress` connects to the CIMC using its assigned management IPv4 address; on supported CIMC releases, an HTTP request can be accepted and directed to the CIMC web-login service. Entering `https://hostname` is also valid when the CIMC hostname is resolvable through DNS or another name-resolution mechanism. HTTPS is the preferred operational method because it protects the administrator's authentication session with TLS while accessing server-management functions, including firmware inventory and validation. In both cases, the browser opens the CIMC authentication page, where an authorized administrator can sign in and review the installed firmware versions. Cisco CIMC documentation describes browser-based access to the controller through its configured management address and recommends secure web access for management activities. See the Cisco IMC GUI Configuration Guide and Cisco's UCS C-Series Rack Servers documentation.

QUESTION NO: 15

You have configured a remote Syslog destination on an ESXi host by using ESXCLI.

Which two actions are required to apply and validate the revised Syslog configuration? (Choose two.)

A. Run esxcli system syslog reload.

B. Run esxcli system syslog mark and verify receipt at the collector.

C. Restart VMware Update Manager.

D. Reboot the vCenter Server database.

ANSWER: A B

Explanation:

After specifying the remote logging destination, the Syslog service must be reloaded by using **esxcli system syslog reload** so that the changed configuration is applied. The configuration can then be validated by generating a test message with **esxcli system syslog mark** and confirming that the message is received by the remote Syslog collector. This validation confirms both the host configuration and the network path to the external logging service. VMware documents the ESXCLI Syslog commands in the ESXCLI Command Reference.