PassQueen
a.k.a dumpsqueen.com

VMware Cloud Provider Specialist

VMware 5V0-32.21

Version Demo

Total Demo Questions: 7

Total Premium Questions: 73

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, VMware Cloud Provider Platform Architecture and Technologies	22
Topic 2, VMware Cloud Provider Platform Installation, Configuration and Setup	19
Topic 3, VMware Cloud Provider Platform Management and Operations	32
Total	73

QUESTION NO: 1

Which VMware Cloud Director construct provides the logical security and administrative boundary for a tenant?

A. Organization

B. Provider VDC

C. Catalog

D. Network Pool

ANSWER: A

Explanation:

Organization is correct. An organization represents a tenant boundary in VMware Cloud Director. It contains the tenant users, roles, catalogs, organization virtual data centers, policies, and other tenant-scoped resources that are assigned to that customer. Organization administrators manage users and authorized resources within their own organization without being granted access to resources that belong to other organizations.

A Provider VDC supplies underlying provider compute and storage capacity, while an Organization VDC is an allocation of that capacity to a particular organization. A catalog is a repository of reusable content and is not the primary tenancy boundary. See the VMware Cloud Director documentation.

QUESTION NO: 2

Which two steps are mandatory before upgrading VMware Cloud Director appliances from 10.1 to 10.2? (Choose two.)

A. Take a snapshot of the entire VCD appliances cluster.

B. Take a snapshot of the primary VCD appliance.

C. Take a snapshot of the standby VCD appliance.

D. Change the database failover from Manual to Automatic.

E. Change the database failover from Automatic to Manual.

ANSWER: A E

Explanation:

Before beginning an upgrade of a VMware Cloud Director appliance deployment, administrators must take a snapshot of the entire VCD appliances cluster. The snapshot provides a coordinated recovery point for every appliance participating in the deployment, including the appliance hosting the active Cloud Director service and, where deployed, the standby appliance. VMware's appliance-upgrade guidance requires preserving this rollback capability before making the version change, because the upgrade alters appliance software and Cloud Director components.

Administrators must also change the database failover from Automatic to Manual before the upgrade. In an appliance deployment using the embedded PostgreSQL high-availability configuration, manual failover prevents an unintended database role transition while appliances are being rebooted, upgraded, or temporarily unavailable. This keeps the database topology under administrator control for the duration of the maintenance activity. After the upgrade has completed successfully and the environment has been validated, the configured failover behavior can be restored in accordance with the provider's operational policy. These prerequisite actions are part of the documented appliance upgrade workflow for VMware Cloud Director 10.2. See the VMware Cloud Director 10.2 Installation, Configuration, and Upgrade Guide and the VMware Cloud Director 10.2 documentation.

QUESTION NO: 3

A service provider is using vRealize Operations Tenant App for chargeback of tenant-used resources.

Which action should the system administrator take to update the price for a CPU and memory consumption?

A. Change the sizing policy in the VMware Cloud Director provider portal.

B. Change the pricing policy in the Tenant App UI.

C. Change the pricing metadata in the concerned Organization VDC in the VMware Cloud Provider portal.

D. Change the report definition in the vRealize Operations Manager.

ANSWER: A

Explanation:

Change the sizing policy in the VMware Cloud Director provider portal. In a VMware Cloud Director environment integrated with vRealize Operations Tenant App for Chargeback and Metering, chargeback pricing for virtual-machine compute consumption is obtained from the relevant VMware Cloud Director sizing policy. The provider administrator manages the sizing policy centrally and updates its chargeback-related pricing values for CPU and memory. Tenant App then uses those policy values when it calculates and presents tenant resource costs, ensuring that the chargeback rate corresponds to the VM's assigned sizing policy and is applied consistently across the provider environment. This approach also lets a provider maintain separate rates for different service tiers by associating the appropriate sizing policies with workloads or organization VDC offerings. The documented Tenant App chargeback workflow identifies VMware Cloud Director sizing-policy configuration as the location for configuring CPU and memory prices used by the application. For implementation context, review VMware's vRealize Operations Tenant App for Chargeback and Metering white paper and the VMware Cloud Director product documentation.

QUESTION NO: 4

Which three allocation models can be selected when creating an Organization VDC? (Choose three.)

A. Allocation Pool

B. Pay-As-You-Go

C. Reservation Pool

D. Network Pool

E. Storage Policy

F. vSphere Resource Pool

ANSWER: A B C

Explanation:

Allocation Pool, **Pay-As-You-Go**, and **Reservation Pool** are Organization VDC allocation models. Allocation Pool allocates a defined pool of CPU and memory to the Organization VDC and applies configured allocation guarantees. Pay-As-You-Go allocates resources as individual virtual machines are deployed and powered on. Reservation Pool reserves the configured Organization VDC compute capacity from the backing Provider VDC.

Network Pool provides backing resources for tenant network creation, while a storage policy defines characteristics and placement for virtual-machine disks. A resource pool is a vSphere construct used as compute backing for provider resources. See the VMware Cloud Director documentation.

QUESTION NO: 5

An administrator is configuring and managing multisite deployments.

Which Association Member Status is an invalid status?

A. Inactive

B. Asymmetric

C. Active

D. Unreachable

ANSWER: A

Explanation:

Inactive is the invalid Association Member Status. In a VMware Cloud Director multisite association, the member-status value represents the current relationship and communication state between the local Cloud Director instance and an associated remote instance. VMware Cloud Director identifies association members using the supported states *Active*, *Unreachable*, and *Asymmetric*. An active member is participating normally in the association. The status can instead reflect a communication condition or an inconsistency in the association configuration, which VMware reports through its defined status values. *Inactive* is not part of the Association Member Status vocabulary exposed by VMware Cloud Director for multisite associations, so it cannot be a valid status returned for an association member. Administrators should use the association-member status information when validating multisite connectivity and configuration consistency before relying on cross-site capabilities such as organization migration or shared multisite administration. VMware documents these status values in the multisite-management material for Cloud Director service providers. See the VMware Cloud Director Service Provider Admin Guide and the VMware Cloud Director Service Provider Portal Guide.

QUESTION NO: 6

A customer requires VM encryption.

Which action must be taken to provide this feature?

A. Upgrade the vCenter Server to at least version 7.0.

B. Encrypt the VM directly from vCenter Server, as it is transparent to VMware Cloud Director.

C. In the vCenter Server, add a KMS > enable encryption policy > in VMware Cloud Director, add policy to Provide VDC > add policy to Organization VDC.

D. Add a KMS to VMware Cloud Director > create encryption policy > add policy to Organization VDC.

ANSWER: C

Explanation:

VM encryption in VMware Cloud Director is enabled through the underlying vCenter Server and its configured external Key Management Server (KMS). The provider must first register a KMS with vCenter Server so that vSphere can obtain and manage the encryption keys required for encrypted virtual machines and disks. The provider then enables VM encryption in a vSphere storage policy. VMware Cloud Director discovers and consumes the applicable vSphere storage policy as a storage policy for a Provider VDC. Finally, assigning that policy to an Organization VDC makes the encryption-capable policy available to tenant users, who can select it when deploying or reconfiguring workloads. This workflow ensures that encryption remains controlled by the provider's vSphere and KMS infrastructure while being exposed to tenants through VMware Cloud Director's policy-based allocation model. The KMS must be reachable and operational whenever key operations are needed, and the configured storage policy is the essential bridge between the vSphere encryption capability and the Organization VDC. See the vSphere Virtual Machine Encryption documentation and the VMware Cloud Director Service Provider Administration documentation.

QUESTION NO: 7

The system administrator has to configure transfer server storage during the deployment of a VMware Cloud Director appliance.

What are two purposes of this storage? (Choose two.)

A. For VMware Cloud Director appliance database backups

B. As temporary storage for vApp and media uploads and downloads

C. Used when upgrading a vSphere datastore to a newer VMFS version

D. For network traffic when Cross-VDC Networking is enabled

E. Used during Storage vMotion based migration of virtual machines

ANSWER: A B

Explanation:

Transfer server storage is used both for VMware Cloud Director operational data transfers and for appliance database backups. The transfer server provides the staging area required when users upload or download vApp templates, media files, and other catalog content. Rather than transferring these objects directly between a client and their final cloud storage location, VMware Cloud Director uses the transfer storage as an intermediate location while processing the request. This storage must therefore be sized to accommodate expected concurrent uploads, downloads, and catalog-item operations.

The VMware Cloud Director appliance also uses this storage location for backups of its embedded PostgreSQL database. Maintaining database backup data on the transfer server storage gives administrators a defined appliance-level location from which database backups can be retained, copied, and managed as part of recovery procedures. Because both catalog-transfer activity and database backup operations depend on this location, it should be reliable, appropriately sized, and included in the provider's backup and capacity-planning approach. VMware documents transfer storage configuration as part of appliance deployment and identifies its use for transfers and database backup files. See the VMware Cloud Director appliance deployment guidance and the VMware Cloud Director appliance configuration documentation.