



VMware VCP-VCf Architect 2V0-13.24 Practice Questions

Shared by Barton on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

A customer has stated the following requirements for Aria Automation within their VCF implementation:

- * Users must have access to specific resources based on their company organization
- * Developers must only be able to provision to the Development environment
- * Production workloads can be placed on DMZ or Production clusters

What two design decisions must be implemented to satisfy these requirements? (Choose two.)

Options:

- A- Separate cloud zones will be configured for Development and Production.
- B- Users' access to resources will be controlled by project membership.
- C- Users' access to resources will be controlled by tenant membership.
- D- Separate tenants will be configured for Development and Production.

Answer:

A, B

Explanation:

Aria Automation in VCF 5.2 uses cloud zones and projects for resource control. Option A, 'Separate cloud zones for Development and Production,' restricts provisioning to specific clusters (Development, Production/DMZ), meeting the second and third requirements. Option B, 'Project membership,' assigns users to projects tied to specific zones and roles, satisfying organization-based access and developer restrictions. Option C (tenant membership) is for multi-tenancy, unnecessary here within one VCF instance. Option D (separate tenants) overcomplicates isolation beyond needs. A and B leverage Aria Automation's native capabilities effectively.

Question 2

Question Type: MultipleChoice

The following requirements were identified in an architecture workshop for a virtual

infrastructure design project.

REQ001: All virtual machines must meet the Recovery Time Objective (RTO) of twenty-four hours or less in a disaster recovery (DR) scenario.

Which two test cases will verify these requirements?

Options:

- A- Simulate or trigger an outage of the primary datacenter. All virtual machines must be restored within four hours or less.
- B- Simulate or trigger an outage of the primary datacenter. All virtual machines must be restored within twenty-four hours or less.
- C- Simulate or trigger an outage of the primary datacenter. All virtual machines must not lose more than twenty-four hours of data prior to the outage.
- D- Simulate or trigger an outage of the primary datacenter. All virtual machines must not lose more than four hours of data prior to the outage.

Answer:

B, C

Explanation:

RTO measures time to restore VMs after a DR event (24 hours here). Option B directly tests this: restoration within 24 hours meets the requirement. Option C tests data loss (RPO-like), but in DR context, ensuring no more than 24 hours of data loss complements RTO by verifying the recovery process's effectiveness, a common validation in VCF with tools like Site Recovery Manager (SRM). Option A (4 hours) is stricter than required, and D (4-hour data loss) tests RPO, not RTO. B and C align with VCF DR testing best practices.

Question 3

Question Type: MultipleChoice

A company plans to expand its existing VMware Cloud Foundation (VCF) environment for a new application. The current VCF environment includes a Management Domain and two separate VI Workload Domains with different hardware profiles. The new application has the following requirements:

The application will use significantly more memory than current workloads.

The application will have a limited number of licenses to run on hosts.

Additional VCF and hardware costs have been approved for the application.

The application will contain confidential customer information that requires isolation from other workloads.

What design recommendation should the architect document?

Options:

- A- Implement a new Workload Domain with hardware supporting the memory requirements of the new application.
- B- Deploy a new consolidated VCF instance and deploy the new application into it.
- C- Purchase sufficient matching hardware to meet the new application's memory requirements and expand an existing cluster to accommodate the new application. Use host affinity rules to manage the new licensing.
- D- Order enough identical hardware for the Management Domain to meet the new application requirements and design a new Workload Domain for the application.

Answer:

A

Explanation:

In VMware Cloud Foundation (VCF) 5.2, expanding an existing environment for a new application involves balancing resource needs, licensing, cost, and security. The requirements---high memory, limited licenses, approved budget, and isolation---guide the design. Let's evaluate:

Option A: Implement a new Workload Domain with hardware supporting the memory requirements of the new application

This is correct. A new VI Workload Domain (minimum 3-4 hosts, depending on vSAN HA) can be tailored to the application's high memory needs with new hardware. Isolation is achieved by dedicating the domain to the application, separating it from existing workloads (e.g., via NSX segmentation). Limited licenses can be managed by sizing the domain to match the license count (e.g., 4 hosts if licensed for 4), and the approved budget supports this. This aligns with VCF's Standard architecture for workload separation and scalability.

Option B: Deploy a new consolidated VCF instance and deploy the new application into it

This is incorrect. A consolidated VCF instance runs management and workloads on a single cluster (4-8 hosts), mixing the new application with management components. This violates the isolation requirement for confidential data, as management and application workloads share infrastructure. It also overcomplicates licensing and memory allocation, and a new instance exceeds the intent of "expanding" the existing environment.

Option C: Purchase sufficient matching hardware to meet the new application's memory requirements and expand an existing cluster to accommodate the new application. Use host

affinity rules to manage the new licensing

This is incorrect. Expanding an existing VI Workload Domain cluster with matching hardware (to maintain vSAN compatibility) could meet memory needs, and DRS affinity rules could pin the application to licensed hosts. However, mixing the new application with existing workloads in the same domain compromises isolation for confidential data. NSX segmentation helps, but a shared cluster increases risk, making this less secure than a dedicated domain.

Option D: Order enough identical hardware for the Management Domain to meet the new application requirements and design a new Workload Domain for the application

This is incorrect. Upgrading the Management Domain (minimum 4 hosts) with high-memory hardware for the application is illogical---management domains host SDDC Manager, vCenter, etc., not user workloads. A new Workload Domain is feasible, but tying it to Management Domain hardware mismatches the VCF architecture (Management and VI domains have distinct roles). This misinterprets the requirement and wastes resources.

Conclusion:

The architect should recommend A: Implement a new Workload Domain with hardware supporting the memory requirements of the new application. This meets all requirements---memory, licensing (via domain sizing), budget (approved costs), and isolation (dedicated domain)---within VCF 5.2's Standard architecture.

VMware Cloud Foundation 5.2 Architecture and Deployment Guide (Section: Workload Domain Design)

VMware Cloud Foundation 5.2 Planning and Preparation Guide (Section: Isolation and Sizing)

Question 4

Question Type: MultipleChoice

An architect is designing a VMware Cloud Foundation (VCF)-based Private Cloud solution. During the requirements gathering workshop with customer stakeholders, the following information was captured:

The solution must be capable of deploying 50 concurrent workloads.

The solution must ensure that once submitted, each service does not take longer than 6 hours to provision.

When creating the design documentation, which design quality should be used to classify the stated requirements?

Options:

- A- Availability
- B- Recoverability
- C- Performance
- D- Manageability

Answer:

C

Explanation:

In VMware Cloud Foundation (VCF) 5.2, design qualities (or non-functional requirements) categorize how the solution meets its objectives. The requirements---"deploying 50 concurrent workloads" and "provisioning each service within 6 hours"---must be classified under a quality that reflects their intent. Let's evaluate each option:

Option A: Availability

Availability ensures the solution is accessible and operational when needed (e.g., uptime percentage). While deploying workloads and provisioning services assume availability, the requirements focus on speed and capacity (50 concurrent workloads, 6-hour limit), not uptime or fault tolerance. This quality doesn't directly address the stated needs, making it incorrect.

Option B: Recoverability

Recoverability addresses the ability to restore services after a failure (e.g., disaster recovery). The requirements don't mention failure scenarios, backups, or restoration---they focus on provisioning speed and concurrency during normal operation. Recoverability is unrelated to these operational metrics, so this is incorrect.

Option C: Performance

This is the correct answer. Performance measures how well the solution executes tasks, including speed, throughput, and capacity. In VCF 5.2:

"Deploying 50 concurrent workloads" is a throughput requirement, ensuring the system can handle multiple deployments simultaneously.

"Each service does not take longer than 6 hours to provision" is a latency or response time requirement, setting a performance boundary.

Both align with the performance quality, which governs resource efficiency and user experience in provisioning workflows (e.g., via SDDC Manager or Aria Automation). This classification fits VMware's design framework.

Option D: Manageability

Manageability focuses on ease of administration, monitoring, and maintenance (e.g., automation, UI simplicity). While provisioning workloads involves management, the

requirements emphasize how fast and how many---performance metrics---not the ease of managing the process. Manageability might apply to tools enabling this, but it's not the primary quality here.

Conclusion:

The design quality to classify these requirements is Performance (Option C). It directly reflects the solution's ability to handle 50 concurrent workloads and provision services within 6 hours, aligning with VCF 5.2's focus on operational efficiency.

VMware Cloud Foundation 5.2 Planning and Preparation Guide (Section: Design Qualities)

VMware Cloud Foundation 5.2 Architecture and Deployment Guide (Section: Performance Considerations)

Question 5

Question Type: MultipleChoice

Which statement defines the purpose of Technical Requirements?

Options:

- A- Technical requirements define which goals and objectives can be achieved.
- B- Technical requirements define what goals and objectives need to be achieved.
- C- Technical requirements define which audience needs to be involved.
- D- Technical requirements define how the goals and objectives can be achieved.

Answer:

D

Explanation:

In VMware's design methodology, as outlined in the VMware Cloud Foundation 5.2 Architectural Guide, requirements are categorized into Business Requirements (high-level organizational goals) and Technical Requirements (specific system capabilities or constraints to achieve those goals). Technical Requirements bridge the gap between what the business wants and how the solution delivers it. Let's evaluate each option:

Option A: Technical requirements define which goals and objectives can be achieved

This suggests Technical Requirements determine feasibility, which aligns more with a scoping

or assessment phase, not their purpose. VMware documentation positions Technical Requirements as implementation-focused, not evaluative.

Option B: Technical requirements define what goals and objectives need to be achieved

This describes Business Requirements, which outline "what" the organization aims to accomplish (e.g., reduce costs, improve uptime). Technical Requirements specify "how" these are realized, making this incorrect.

Option C: Technical requirements define which audience needs to be involved

Audience involvement relates to stakeholder identification, not Technical Requirements. The VCF 5.2 Design Guide ties Technical Requirements to system functionality, not personnel.

Option D: Technical requirements define how the goals and objectives can be achieved

This is correct. Technical Requirements detail the system's capabilities, constraints, and configurations (e.g., "support 10,000 users," "use AES-256 encryption") to meet business goals. The VCF 5.2 Architectural Guide defines them as the "how"---specific, measurable criteria enabling the solution's implementation.

Conclusion:

Option D accurately reflects the purpose of Technical Requirements in VCF 5.2, focusing on the means to achieve business objectives.

VMware Cloud Foundation 5.2 Architectural Guide (docs.vmware.com): Section on Requirements Classification.

VMware Cloud Foundation 5.2 Design Guide (docs.vmware.com): Business vs. Technical Requirements.

Question 6

Question Type: MultipleChoice

During a requirements gathering workshop, several Business and Technical requirements were captured from the customer. Which requirement will be classified as a Business Requirement?

Options:

- A- Reduce processing time for service requests by 30%.
- B- The system must support 10,000 concurrent users.
- C- Data must be encrypted using AES-256 encryption.
- D- The application must be compatible with Windows, macOS, and Linux operating systems.

Answer:

A

Explanation:

In VMware's design methodology (aligned with VCF 5.2), requirements are categorized as Business Requirements (goals tied to organizational outcomes, often non-technical) or Technical Requirements (specific system capabilities or constraints). Let's classify each option:

Option A: Reduce processing time for service requests by 30%

This is a Business Requirement. It focuses on a business outcome---improving service request efficiency by a measurable percentage---without specifying **how** the system achieves it. The VMware Cloud Foundation 5.2 Architectural Guide classifies such high-level, outcome-driven goals as business requirements, as they reflect the customer's operational or strategic priorities rather than technical implementation details.

Option B: The system must support 10,000 concurrent users

This is a Technical Requirement. It specifies a measurable system capability (supporting 10,000 concurrent users), directly tied to performance and capacity. VMware documentation treats such quantifiable system behaviors as technical, focusing on "what" the system must do functionally.

Option C: Data must be encrypted using AES-256 encryption

This is a Technical Requirement. It mandates a specific technical implementation (AES-256 encryption) for security, a non-functional attribute. The VCF 5.2 Design Guide categorizes encryption standards as technical constraints or requirements, not business goals.

Option D: The application must be compatible with Windows, macOS, and Linux operating systems

This is a Technical Requirement. It defines a functional capability---cross-platform compatibility---specifying technical details about the system's operation. VMware classifies such compatibility needs as technical, per the design methodology.

Conclusion:

Option A is the Business Requirement, as it aligns with a business goal (efficiency improvement) rather than a technical specification.

VMware Cloud Foundation 5.2 Architectural Guide (docs.vmware.com): Section on Requirements Gathering and Classification.

VMware Cloud Foundation 5.2 Design Guide (docs.vmware.com): Business vs. Technical Requirements.

Question 7

Question Type: MultipleChoice

An architect is designing a new VCF solution to meet the following requirements:

The solution must be deployed across two availability zones.

The physical hosts must be installed in a single rack per availability zone.

Workloads running in the cluster must be able to run on hosts in either availability zone.

The architect has decided that to meet these requirements, the solution will be deployed using the Single Instance - Multiple Availability Zones VCF Topology. When considering the design for the network, what should the architect include in the logical design to meet these requirements?

Options:

- A- A physical network fabric in a leaf-spine configuration with dual Cisco switches within each availability zone.
- B- A highly available gateway that supports the failure of an entire availability zone.
- C- A 25-GbE port on each Top of Rack (ToR) switch connected to the ESXi host uplinks.
- D- A single NSX Overlay Transport Zone for all clusters to carry the traffic between the ESXi hosts.

Answer:

D

Explanation:

The VCF 5.2 design uses a Single Instance - Multiple Availability Zones topology (e.g., stretched cluster), requiring centralized management across two AZs, hosts in one rack per AZ, and workload mobility across AZs. The logical design focuses on high-level networking architecture, not physical details. Let's evaluate:

Option A: A physical network fabric in a leaf-spine configuration with dual Cisco switches within each availability zone

A leaf-spine fabric enhances physical network scalability and redundancy, aligning with rack-based deployments. However, it's a physical design detail (switch topology), not a logical networking decision, per the VCF 5.2 Design Guide.

Option B: A highly available gateway that supports the failure of an entire availability zone

A gateway (e.g., NSX Edge Tier-0) with AZ failover supports North-South traffic resilience.

While valuable, it doesn't directly enable workload mobility across AZs (East-West traffic), which is the core requirement. The VCF 5.2 Networking Guide treats gateways as supplementary, not foundational for stretched clusters.

Option C: A 25-GbE port on each Top of Rack (ToR) switch connected to the ESXi host uplinks

Specifying 25-GbE ports is a physical network detail (bandwidth, cabling), not a logical design element. The VCF 5.2 Design Guide relegates port speeds to physical implementation, not logical architecture.

Option D: A single NSX Overlay Transport Zone for all clusters to carry the traffic between the ESXi hosts

In a stretched cluster topology, a single NSX Overlay Transport Zone enables VM mobility across AZs via overlay networks (e.g., Geneve). It ensures workloads can run on hosts in either AZ by providing a unified L2/L3 connectivity layer, managed by NSX. The VCF 5.2 Architectural Guide mandates a single Overlay TZ for stretched deployments to support vMotion and workload distribution, directly meeting the requirement.

Conclusion:

Option D is the logical design decision, enabling workload mobility across AZs in a stretched VCF topology via NSX overlay networking.

VMware Cloud Foundation 5.2 Architectural Guide (docs.vmware.com): Multi-AZ Topology and NSX Overlay.

VMware Cloud Foundation 5.2 Networking Guide (docs.vmware.com): Transport Zones in Stretched Clusters.

VMware Cloud Foundation 5.2 Design Guide (docs.vmware.com): Logical vs. Physical Design.

Question 8

Question Type: MultipleChoice

An architect is working with a service provider to design a VMware Cloud Foundation (VCF) solution that is required to host workloads for multiple tenants. The following requirements were gathered:

Each tenant requires full access to their own vCenter.

Each tenant will utilize and manage their own identity provider for access.

A total of 28 tenants are expected to be onboarded.

Each tenant will have their own independent VCF lifecycle maintenance schedule.

Which VCF architecture option will meet these requirements?

Options:

- A- A single VCF instance consolidated architecture model with 28 tenant clusters
- B- A single VCF instance standard architecture model and 28 isolated SSO domains
- C- Two VCF instances consolidated architecture model with 14 tenant clusters each
- D- Two VCF instances with standard architecture model and 14 isolated SSO domains each

Answer:

C

Explanation:

To determine the appropriate VMware Cloud Foundation (VCF) architecture for this scenario, we need to evaluate each option against the provided requirements and the capabilities of VCF 5.2 as outlined in official documentation.

Requirement Analysis:

Each tenant requires full access to their own vCenter: This implies that each tenant needs a dedicated vCenter Server instance for managing their workloads, ensuring isolation and administrative control.

Each tenant will utilize and manage their own identity provider: This requires separate Single Sign-On (SSO) domains or identity sources per tenant, as tenants must integrate their own identity providers (e.g., Active Directory, LDAP) independently.

A total of 28 tenants: The solution must scale to support 28 isolated environments.

Independent VCF lifecycle maintenance schedule: Each tenant's environment must support its own lifecycle management (e.g., upgrades, patches) without impacting others, implying separate VCF instances or fully isolated workload domains.

VCF Architecture Models Overview (Based on VCF 5.2 Documentation):

Standard Architecture Model: A single VCF instance with one vCenter Server managing all workload domains under a single SSO domain. Additional workload domains share the same vCenter and SSO infrastructure.

Consolidated Architecture Model: A single VCF instance where the management domain and workload domains are managed by one vCenter Server, but workload domains can be isolated at the cluster level.

Multiple VCF Instances: Separate VCF deployments, each with its own management domain, vCenter Server, and SSO domain, enabling full isolation and independent lifecycle management.

Option Analysis:

A . A single VCF instance consolidated architecture model with 28 tenant clusters:

In a consolidated architecture, a single vCenter Server manages the management domain and all workload clusters. While 28 tenant clusters could be created, all would share the same vCenter and SSO domain. This violates the requirements for each tenant having their own vCenter and managing their own identity provider, as a single SSO domain cannot support 28 independent identity providers. Additionally, lifecycle management would be tied to the single VCF instance, conflicting with the independent maintenance schedule requirement. This option does not meet the requirements.

B . A single VCF instance standard architecture model and 28 isolated SSO domains:

In a standard architecture, a single VCF instance includes one vCenter Server and one SSO domain for all workload domains. While workload domains can be created for isolation, VMware Cloud Foundation 5.2 does not support multiple isolated SSO domains within a single vCenter instance. The vSphere SSO architecture allows only one SSO domain per vCenter Server. Even with creative configurations (e.g., identity federation), managing 28 independent identity providers within one SSO domain is impractical and unsupported. Furthermore, all workload domains share the same lifecycle schedule under one VCF instance, failing the independent maintenance requirement. This option is not viable.

C . Two VCF instances consolidated architecture model with 14 tenant clusters each:

With two VCF instances, each instance has its own management domain, vCenter Server, and SSO domain. Each instance operates in a consolidated architecture, where tenant clusters (workload domains) are managed by the instance's vCenter. However, the key here is that each VCF instance can be fully isolated from the other, allowing:

Each tenant cluster to be assigned a dedicated vCenter (via separate workload domains or vSphere clusters with permissions).

Independent SSO domains per instance, with tenant-specific identity providers configured through federation or external identity sources.

Independent lifecycle management, as each VCF instance can be upgraded or patched separately.

Splitting 28 tenants into 14 per instance is feasible, as VCF 5.2 supports up to 25 workload domains per instance (per the VCF Design Guide), and tenant isolation can be achieved at the cluster level with proper permissions and NSX segmentation. This option meets all requirements.

D . Two VCF instances with standard architecture model and 14 isolated SSO domains each:

In a standard architecture, each VCF instance has one vCenter Server and one SSO domain. While having two instances provides lifecycle independence, the mention of "14 isolated SSO domains each" is misleading and unsupported. A single vCenter Server (and thus a single VCF instance) supports only one SSO domain. It's possible this intends to mean 14 tenants with isolated identity configurations, but this would still conflict with the single-SSO limitation per instance. Even with two instances, achieving 14 isolated SSO domains per instance is not architecturally possible in VCF 5.2. This option fails the identity provider and vCenter requirements.

Conclusion:

Option C (Two VCF instances consolidated architecture model with 14 tenant clusters each) is the only architecture that satisfies all requirements. It provides tenant isolation via separate clusters, supports dedicated vCenter access through permissions or additional vCenter deployments, allows independent identity providers via SSO federation, scales to 28 tenants across two instances, and ensures independent lifecycle management.

VMware Cloud Foundation 5.2 Design Guide (Section: Architecture Models)

VMware Cloud Foundation 5.2 Planning and Preparation Workbook (Section: Multi-Tenancy Considerations)

VMware Cloud Foundation 5.2 Administration Guide (Section: Lifecycle Management)

VMware vSphere 8.0 Update 3 Documentation (Section: SSO and Identity Federation)



To Get Premium Files for 2V0-13.24 Visit

<https://www.p2pexams.com/products/2v0-13.24>

For More Free Questions Visit

<https://www.p2pexams.com/vmware/pdf/2v0-13.24>

20%
DISCOUNT

P2P
exams