Download VMware 2V0-13.25 Exam Dumps Free

Shared by Brock on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which statement defines the purpose of Technical Requirements?

Options:

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

Answer:

D

Explanation:

According to the VMware Cloud Foundation 9.0.1 Design Framework, Technical Requirements describe how the business and functional goals are to be implemented through technology, configuration, and design mechanisms. The document defines:

''Technical requirements determine how a solution's business and functional objectives are achieved using technical means such as architecture components, configurations, and integrations.''

These are distinct from business requirements, which define what must be achieved, and constraints, which limit design options. Technical requirements translate abstract needs (for example, availability, scalability, performance) into actionable design implementations (such as anti-affinity rules, distributed switches, NSX federation, or vSAN stretched clusters).

By following VMware's VCF Design Methodology, architects use technical requirements to shape logical and physical architectures, ensuring that all solution components meet the identified business outcomes and compliance standards.

Reference (VMware Cloud Foundation documents):

VMware Cloud Foundation 9.0.1 Design and Architecture Guide --- Requirements Classification and Technical Requirements Definition (pp. 58--61).

VMware Cloud Foundation 9.0.2 Design Framework --- Business, Functional, and Technical Requirement Mapping to Design Decisions.

Question 2

Question Type: MultipleChoice

A large financial institution is designing a VMware Cloud Foundation (VCF) solution. During the initial discovery meetings, the customer detailed the following requirements:

* Management of the physical network environment is handled by an outsourced team.

* The VMware Administration team cannot re-configure the physical network.

* All hosts must use Link Aggregation.

* The storage environment is disaggregated.

* NFS will be used as principal storage.

The customer provided the bill-of-materials for the physical servers being purchased. Each server will have four 25 GbE physical NICs: two connected to the network fabric for Management, vMotion, and virtual machine traffic; and two connected to the storage fabric hosting the NFS server.

How does the information provided impact the overall design?

Options:

A- Link Aggregation cannot be used in the Workload Domain.
B- NIC teaming for Virtual Standard Switch (vSS) must be configured.
C- Multiple Link Aggregation Groups are not supported.
D- Link Aggregation cannot be used in the Management Domain.

Answer:

D

Explanation:

VCF networking guidance emphasizes independent uplinks and notes that while LACP is supported, it is not recommended and introduces additional operational considerations. Specifically: ''Link aggregation to the host is supported but not recommended---the default switch-independent load-based teaming (LBT) provides benefits similar to those of LACP without added configuration complexity.'' It further states: ''Use of LACP... requires specific LACP configuration and switch setup... Not all vSphere features are supported with LACP... [and is] API only.'' The design recommendation is: ''Ensure each connection between the fabric switch and

host operates as an independent uplink.''

Given the customer constraint that the VMware Administration team cannot re-configure the physical network, the prerequisite physical switch port-channel configuration for LACP cannot be performed. During bring-up and life-cycle operations, the Management Domain must follow VCF's standardized, automated patterns and therefore cannot rely on fabric changes the team cannot make. As a result, LAG cannot be used in the Management Domain, and the design must adopt independent uplinks (LBT) for management, vMotion, and VM traffic while using NFS as principal storage per the NFS Storage Model.

Reference (VMware Cloud Foundation documents):

* VCF 9.0.1 Design -- Network Link Aggregation: support, ''not recommended,'' API-only, and independent uplink recommendation.

* VCF 9.0.1 Design -- Link Aggregation Design Recommendations (independent uplinks).

* VCF 9.0.1 Design -- NFS Storage Model (principal NFS usage context).

Question 3

Question Type: MultipleChoice

An architect is tasked to plan for an upgrade of an existing vSphere-only deployment utilizing vSAN to VMware Cloud Foundation (VCF).

Which three new infrastructure components are required for the upgrade? (Select three.)

Options:

A- NSX
B- SDDC Manager
C- VCF Identity Broker
D- VCF Operations
E- vSphere Supervisor

Answer:

A, B, E

Explanation:

Upgrading a vSphere + vSAN environment to a full VMware Cloud Foundation deployment

requires introducing the components that make up the integrated software-defined data center (SDDC):

A . NSX -- Provides network virtualization, overlay segments, distributed firewalling, and routing required in VCF.

B . SDDC Manager -- The core management and lifecycle automation tool of VCF, responsible for bring-up, patching, and upgrades.

E . vSphere Supervisor -- Required to enable VMware Tanzu Kubernetes Grid (TKG) and modern application deployment in VCF environments.

Why not the others?

C . VCF Identity Broker -- Provides federated authentication but is not mandatory for initial upgrade. It is optional depending on identity requirements.

D . VCF Operations -- This is VMware Aria Operations (for monitoring/analytics). While strongly recommended, it is not required to upgrade from vSphere/vSAN to VCF.

VMware Cloud Foundation 9.0 Architecture Guide -- Required Components for Bring-Up and Upgrade from vSphere + vSAN

VMware Cloud Foundation Planning and Preparation Guide

Question 4

Question Type: MultipleChoice

A company is deploying a new VMware Cloud Foundation (VCF) environment to support their growing infrastructure requirements.

The company is planning to scale their environment over time by adding more workload domains as new applications and departments are onboarded.

The company requires that the architecture must be highly scalable and flexible, able to accommodate both current and future demands. They also require a seamless transition when adding new workload domains.

Which design decisions should the architect make to meet the stated scalability requirements and facilitate the future growth?

Options:

A- Use a single workload domain for all departments and increase the size of the vSphere clusters

as the demand grows.
B- Use multiple workload domains for each department and ensure that each workload domain is independently scaled.
C- Use a single workload domain and rely on storage and network scaling to accommodate future growth.
D- Use multiple workload domains for each department but combine them into a single vSphere cluster to reduce complexity.

Answer:

B

Explanation:

VMware Cloud Foundation scales using workload domains (WLDs). Each WLD provides its own vCenter Server, NSX Manager, and lifecycle independence through SDDC Manager.

By using multiple WLDs for each department, the architecture supports independent scaling, policy separation, and lifecycle management.

Option A or C restricts flexibility as all tenants would share a single WLD, leading to lifecycle constraints and ''noisy neighbor'' issues.

Option D contradicts best practices: multiple departments should not share a single cluster inside a WLD when separation and lifecycle flexibility are required.

This design ensures seamless addition of new workload domains as departments and applications grow.

Question 5

Question Type: MultipleChoice

An architect is tasked with designing a new VMware Cloud Foundation (VCF) solution. During workshops with the customer, the following requirements were captured:

* REQ01: The solution must provide a self-service catalog.

* REQ02: The solution must support the segregation of the Development and Production resources (networks, virtual machines, users).

When documenting the design decisions, which statement should the architect include in order to help meet these requirements?

Options:

A- VCF Automation does not support the use of multiple Active Directory domains.
B- Separate workload domains must be configured to provide segregation between the Development and Production environments.
C- VCF Automation will be configured with separate service catalog instances for Development and Production.
D- VCF Automation will be configured with separate organizations for Development and Production.

Answer:

D

Explanation:

In the VMware Cloud Foundation 9.0.4 Architecture and Design Guide, VCF Automation supports multi-tenancy through the creation of separate organizations, each with its own catalog, users, and identity source. The document under ''Organizations in VCF Automation'' explains:

''Organizations in VCF Automation are created by the provider administrator in the Provider Management Portal. Each organization has its own identity source and resource allocations. The organization administrator can then configure its own self-service catalog and governance policies.''

By configuring separate organizations for Development and Production, the architect ensures logical segregation of resources, catalogs, and permissions. Each organization can manage its own projects, namespaces, and service catalogs independently, meeting both the self-service and segregation requirements.

This design aligns with VMware's provider--tenant model, where each tenant (organization) operates autonomously while still being managed under a common provider infrastructure.

Reference (VMware Cloud Foundation documents):

VMware Cloud Foundation 9.0.4 Design Guide --- ''Organizations in VCF Automation: All Apps and VM Apps Organizations.''

VMware Cloud Foundation 9.0.4 --- ''Self-Service Catalog in VCF Automation.''

Question 6

Question Type: MultipleChoice

Which four component areas are provided by a VMware Kubernetes Service (VKS) cluster?

Options:

A- Identity federation, persistent logging, firewall services, and monitoring.
B- Authentication, external storage, virtual machine networking, and DNS services.
C- Authorization, backup services, VLAN segmentation, and DHCP.
D- Authentication and authorization, storage integration, pod networking, and load balancing.

Answer:

D

Explanation:

The VMware Cloud Foundation 9.0.4 Documentation explicitly defines the four key component areas provided by a VKS cluster:

''The components that run in a VKS cluster span four areas: Authentication and authorization, storage integration, pod networking, and load balancing.''

These components are implemented as follows:

Authentication webhook: validates user access tokens.

Container Storage Interface (CSI): integrates with VMware Cloud Native Storage (CNS).

Container Network Interface (CNI): provides pod-level networking (Antrea or Calico).

Cloud Provider Implementation: enables Kubernetes LoadBalancer service creation.

This holistic integration ensures secure, scalable, and production-grade operation of Kubernetes workloads within vSphere Supervisor.

Reference (VMware Cloud Foundation documents):

VMware Cloud Foundation 9.0.4 Architecture Guide --- ''VKS Cluster Components.'' (pp. 5637--5639)

VMware Cloud Foundation 9.0.4 Workload Management Overview --- ''VKS Functional Architecture and Services.''

Question 7

Question Type: MultipleChoice

An architect has made an assumption that existing support staff are adequately skilled to operate the proposed infrastructure design.

The risk associated with this assumption would be that existing support staff are inadequately skilled to operate the proposed infrastructure design. How would the architect mitigate the risk?

Options:

A- Hire additional support staff with the same skillsets to add more support capacity.
B- Allocate the necessary time and budget to train existing support staff on the necessary skills required to operate.
C- Complete a skills assessment of the existing support staff to identify the skill gap.
D- Engage a third-party company to deploy and configure the proposed solution.

Answer:

B

Explanation:

The correct mitigation for a skills-based risk is to bridge the gap through training and upskilling. Providing time and budget for training ensures that existing staff can competently support the solution and aligns with long-term sustainability of the environment.

Option A does not address the skills gap, just adds capacity. Option C is a risk identification tool, not a mitigation step. Option D outsources the issue, which contradicts the goal of internal capability development.

VMware Cloud Foundation Architecture and Design Guide -- Risk Identification and Mitigation Strategies

==========

Question 8

Question Type: MultipleChoice

An architect is designing a VMware Cloud Foundation (VCF)-based solution. The company policy

mandates that all VCF patches and upgrades must be tested in a development environment before applying to production.

Which VCF construct design decision would comply with this mandate?

Options:

A- Deploy two VCF vSphere Clusters within a VCF Domain.
B- Deploy two VCF Instances within a VCF Fleet.
C- Deploy two VCF Domains within a VCF Instance.
D- Deploy two VCF Fleets within a VCF Private Cloud.

Answer:

B

Explanation:

Deploying two VCF Instances allows isolation between environments. One instance can serve as development/test and the other as production.

This separation enables patch/upgrade validation without impacting production. VCF architecture supports managing multiple VCF instances in a Fleet for centralized visibility and policy enforcement.

VMware explicitly recommends separating environments for lifecycle testing in environments with strict change control policies.

Question 9

Question Type: MultipleChoice

Requirement: NSX VPC Full Services Model for single tenant, preventing BGP advertisements from being dropped due to loop detection.

Which element should be considered in the physical network design?

Options:

A- Adjust the default BGP timers.
B- Use a unique, private BGP AS number for each Tier-0 gateway.

C- Use iBGP as the routing protocol between the Tier-0 gateway and the physical network.
D- Configure edge datapath interface to transport only TEP traffic.

Answer:

B

Explanation:

BGP loop prevention relies on unique AS numbers. If the same AS is reused, routes may be dropped. In NSX VPC designs, assigning a unique private AS per Tier-0 gateway ensures clean routing without triggering loop detection.

A: Timer adjustment affects convergence, not loop detection.

C: iBGP with physical routers is non-standard and doesn't solve the loop issue.

D: TEP traffic is unrelated to BGP routing loops.