

VMware 2V0-13.24 Practice Guide - 2V0-13.24 Test Discount Voucher



BONUS!!! Download part of Test4Cram 2V0-13.24 dumps for free: <https://drive.google.com/open?id=16TEg5RGBrvgL2abp6ClabWn81Jw1luHl>

In this hustling society, our 2V0-13.24 study guide is highly beneficial existence which can not only help you master effective knowledge but pass the 2V0-13.24 exam effectively. They have a prominent role to improve your soft-power of personal capacity and boost your confidence of conquering the exam with efficiency. As there are all keypoints in the 2V0-13.24 Practice Engine, it is easy to master and it also helps avoid a waste of time for selecting main content.

VMware 2V0-13.24 Exam Syllabus Topics:

Topic	Details
Topic 1	IT Architectures, Technologies, Standards: This section of the exam measures the skills of enterprise architects and solution architects and focuses on the fundamentals of IT architectures, technologies, and standards. It covers differentiating between business and technical requirements, understanding conceptual models, and logical and physical designs, and recognizing the distinctions between requirements, assumptions, constraints, and risks. Also included are availability, manageability, performance, recoverability, and security (AMPRS), developing risk mitigation strategies, documenting design decisions, and creating design validation strategies.
Topic 2	VMware by Broadcom Solution: This section of the exam measures the skills of cloud architects and infrastructure engineers and focuses on understanding the architecture of VMware by Broadcom solution. Candidates should be able to differentiate between various VMware Cloud Foundation architecture options based on different scenarios.

Topic 3	Plan and Design the VMware by Broadcom Solution: This section of the exam measures the skills of VMware administrators. It involves gathering and analyzing business objectives and requirements to create a conceptual model. Additionally, it covers the creation of VMware Cloud Foundation logical and physical designs. This includes prerequisites and design decisions related to Network Infrastructure, VCF Management Domain, VCF Workload Domain, VCF Edge Cluster, VCF Cloud Automation, and VCF Cloud Operations. Designs should consider availability within and across availability zones, manageability (Lifecycle Management, Scalability, Capacity Management), performance, recoverability (BCDR strategies), and security for VCF Management Components and Workloads. Workload mobility, consumption, and monitoring strategies are also addressed in this section.
Topic 4	Troubleshoot and Optimize the VMware by Broadcom Solution: This section has NO TESTABLE OBJECTIVES in this version of the exam.
Topic 5	Install, Configure, and Administrate the VMware by Broadcom Solution: This section has NO TESTABLE OBJECTIVES in this version of the exam.

>> VMware 2V0-13.24 Practice Guide <<

Latest VMware Cloud Foundation 5.2 Architect free dumps & 2V0-13.24 passleader braindumps

If you are still in colleges, it is a good chance to learn the knowledge of the 2V0-13.24 study engine because you have much time. At present, many office workers are keen on learning our 2V0-13.24 guide materials even if they are busy with their work. So you should never give up yourself as long as there has chances. In short, what you have learned on our 2V0-13.24 study engine will benefit your career development.

VMware Cloud Foundation 5.2 Architect Sample Questions (Q49-Q54):

NEW QUESTION # 49

When selecting a VMware Cloud Foundation architecture, which factor is most important when deciding between a single-site or multi-site deployment?

Response:

- A. Budget constraints
- B. Compliance and regulatory requirements
- C. Required scalability and high availability
- D. Type of workload being deployed

Answer: C

NEW QUESTION # 50

The following requirements were identified in an architecture workshop for a VMware Cloud Foundation (VCF) design project using vSAN as the primary storage solution:

REQ001: The application must maintain a minimum of 1,000 transactions per second (TPS) during business hours, excluding disaster recovery (DR) scenarios.

REQ002: Automatic DRS and HA must be utilized.

REQ003: Planned maintenance must be performed outside of business hours.

While monitoring the TPS of the application, which of the following is NOT a valid test case to validate these requirements?

- A. Trigger a vCenter upgrade workflow.
- B. Trigger a vSAN disk group cache drive failure.
- C. Trigger a vSphere High Availability (HA) failover activity.
- D. Trigger fully automatic DRS vMotion activity.

Answer: A

Explanation:

The test case must validate all three requirements: maintaining 1,000 TPS during business hours (REQ001), using automatic DRS and HA (REQ002), and ensuring maintenance occurs outside business hours (REQ003, implying minimal disruption during business hours). Let's assess each:

Option A: Trigger a vSphere High Availability (HA) failover activityHA failover (e.g., host failure) tests automatic VM restarts (REQ002) and ensures TPS (REQ001) remains at 1,000 during business hours under failure conditions (excluding DR, as this is intra-site). The VCF 5.2 Administration Guide recommends HA testing to validate availability, making this valid.

Option B: Trigger a vSAN disk group cache drive failureA cache drive failure in vSAN tests data resilience and HA's ability to restart VMs if needed (REQ002), while monitoring TPS (REQ001) during business hours. The vSAN Administration Guide supports this as a standard test for vSAN performance and recovery, aligning with the requirements.

Option C: Trigger fully automatic DRS vMotion activityFully automatic DRS triggers vMotion to balance loads (REQ002), testing TPS (REQ001) during business hours without disruption. While not maintenance, it validates DRS automation's impact on performance, per the vSphere Resource Management Guide, making it a valid test.

Option D: Trigger a vCenter upgrade workflowA vCenter upgrade is a planned maintenance activity (REQ003) that should occur outside business hours. Performing it during business hours to monitor TPS contradicts REQ003 and isn't a typical test for DRS/HA (REQ002) or application performance (REQ001), as it affects management, not workloads directly. The VCF 5.2 Administration Guide treats upgrades as separate from runtime validation.

Conclusion: Option D is not a valid test case, as it violates REQ003 and doesn't directly validate REQ001 or REQ002 in a runtime context. References:

VMware Cloud Foundation 5.2 Administration Guide(docs.vmware.com): HA and vSAN Testing.

vSphere Resource Management Guide(docs.vmware.com): DRS Automation Testing.

vSAN Administration Guide(docs.vmware.com): Disk Failure Scenarios.

NEW QUESTION # 51

A VMware Cloud Foundation multi-AZ (Availability Zone) design mandates that:

All availability zones must operate independently of each other.

The availability SLA must adhere to no less than 99.9%.

What would be the three design decisions that would help satisfy those requirements? (Choose three.)

- A. Configure a non-routable separate recovery VLAN for the infrastructure management components within each AZ
- B. Choose two close proximity AZ(s) and configure a stretched management workload domain
- C. Make sure all configuration backups are replicated between the selected AZ(s)
- D. Make sure the recovery VLAN for the infrastructure management components has access to both AZ(s)
- E. Configure array-based replication between the selected AZ(s) for the management domain
- F. Choose two distant AZ(s) and consider each AZ the DR for the other

Answer: A,C,E

Explanation:

This scenario involves a VCF multi-AZ design where AZs must operate independently (no shared dependencies) and achieve a 99.9% availability SLA (allowing ~8.76 hours of downtime annually). The design decisions must ensure resilience, fault isolation, and recovery capabilities across AZs.

Requirement Analysis:

Independent AZ operation: Each AZ must function standalone, with no single point of failure or dependency across AZs.

99.9% availability: The design must minimize downtime through redundancy, replication, and recovery mechanisms.

Option Analysis:

A: Configure array-based replication between the selected AZ(s) for the management domain: Array-based replication (e.g., vSphere Replication or SAN replication) for the management domain (vCenter, NSX Manager, SDDC Manager) ensures that critical management VMs are duplicated across AZs. If one AZ fails, the other can take over with minimal downtime, supporting independent operation and high availability. The VCF 5.2 Design Guide recommends replication for multi-AZ deployments to meet SLAs, as it provides a recovery point objective (RPO) near zero. This option enhances availability and is correct.

B: Make sure all configuration backups are replicated between the selected AZ(s): Replicating configuration backups (e.g., SDDC Manager backups, NSX configurations) ensures that each AZ has access to recovery data. If an AZ's management components fail, the other AZ can restore operations independently using its local backup copy. This supports the independence requirement and reduces downtime (contributing to 99.9% SLA) by enabling quick recovery. The VCF Administration Guide emphasizes backup replication for multi-AZ resilience, making this option correct.

C: Make sure the recovery VLAN for the infrastructure management components has access to both AZ(s): A recovery VLAN spanning both AZs implies a shared network dependency. If this VLAN fails (e.g., due to a network outage), both AZs could be impacted, violating the independence requirement. Multi-AZ designs in VCF favor isolated networks per AZ to avoid cross-AZ single points of failure. The VCF Design Guide advises against shared VLANs for critical components in independent AZ setups.

This option undermines the requirements and is incorrect.

D: Choose two distant AZ(s) and consider each AZ the DR for the other: Distant AZs (e.g., separate data centers) with mutual DR (disaster recovery) roles enhance geographic fault tolerance. However, "operate independently" in VCF typically means each AZ can run workloads standalone, not that one is a passive DR site. Distant AZs introduce latency, complicating synchronous replication needed for 99.9% availability, and may rely on shared management, conflicting with independence. The VCF Multi-AZ Guide focuses on active-active AZs, not DR-centric designs, making this less suitable.

E: Choose two close proximity AZ(s) and configure a stretched management workload domain: A stretched management domain (e.g., using vSAN stretched cluster) spans AZs with synchronous replication, ensuring high availability. However, this creates a dependency: both AZs share the same vCenter and management stack, so a failure (e.g., vCenter outage) could affect both, violating independence. The VCF 5.2 Design Guide notes stretched clusters are for single logical domains, not independent AZs. This option contradicts the requirement and is incorrect.

F: Configure a non-routable separate recovery VLAN for the infrastructure management components within each AZ: A non-routable, AZ-specific recovery VLAN isolates management recovery traffic (e.g., for vMotion, backups) within each AZ. This ensures that each AZ's management components operate independently, with no cross-AZ network reliance. If one AZ's network fails, the other remains unaffected, supporting the SLA through fault isolation. The VCF Multi-AZ Design Guide recommends separate, isolated networks per AZ for resilience, making this option correct.

Conclusion: The three design decisions are Configure array-based replication between the selected AZ(s) for the management domain (A), Make sure all configuration backups are replicated between the selected AZ(s) (B), and Configure a non-routable separate recovery VLAN for the infrastructure management components within each AZ (F). These ensure independent operation and meet the 99.9% SLA through replication and isolation.

References:

VMware Cloud Foundation 5.2 Design Guide (Section: Multi-AZ Design)

VMware Cloud Foundation 5.2 Administration Guide (Section: Backup and Recovery) VMware Cloud Foundation Multi-AZ Deployment Guide (Section: Networking) VMware vSphere 8.0 Update 3 Documentation (Section: vSAN Stretched Clusters)

NEW QUESTION # 52

As a VMware Cloud Foundation architect, you are provided with the following requirements:

All administrative access to the cloud management components must be trusted.

All cloud management components' communications must be encrypted.

Enhancement of lifecycle management should always be considered.

Which design decision fulfills the requirements?

- A. Write an Aria Orchestrator Workflow to change the ESXi hosts' certificates in bulk.
- B. Write a PowerCLI script to run on all virtual appliances and force a redirection on port 443.
- C. Integrate the SDDC Manager with the vCenter Server in VMCA mode.
- **D. Integrate the SDDC Manager with a supported 3rd-party certificate authority (CA).**

Answer: D

Explanation:

The requirements focus on trust, encryption, and lifecycle management for a VMware Cloud Foundation (VCF) 5.2 solution. VCF leverages SDDC Manager, vCenter Server, NSX, and ESXi hosts as core management components, and their security and manageability are critical. Let's evaluate each option against the requirements:

Option A: Integrate the SDDC Manager with a supported 3rd-party certificate authority (CA) This is the correct answer. In VCF 5.2, integrating SDDC Manager with a 3rd-party CA (e.g., Microsoft CA, OpenSSL) allows it to manage and deploy trusted certificates across all management components (e.g., vCenter, NSX Manager, ESXi hosts). This ensures:

Trusted administrative access: Certificates from a trusted CA secure administrative interfaces (e.g., HTTPS access to SDDC Manager and vCenter), ensuring authenticated and verified connections.

Encrypted communications: All management component interactions (e.g., API calls, UI access) use TLS with CA-signed certificates, encrypting data in transit.

Lifecycle management enhancement: SDDC Manager automates certificate lifecycle operations (e.g., issuance, renewal, replacement), reducing manual effort and improving operational efficiency. The VMware Cloud Foundation documentation explicitly supports this integration as a best practice for security and scalability, fulfilling all three requirements comprehensively.

Option B: Integrate the SDDC Manager with the vCenter Server in VMCA mode This is incorrect. The vCenter Server's VMware Certificate Authority (VMCA) can issue certificates for vSphere components (e.g., ESXi hosts, vCenter itself), but it operates within the vSphere domain, not across the broader VCF stack.

SDDC Manager requires a higher-level CA integration to manage certificates for all components (including NSX and itself). VMCA mode doesn't extend trust to SDDC Manager or NSX Manager natively, nor does it enhance lifecycle management across the entire VCF solution—it's limited to vSphere. This option fails to fully address the requirements.

Option C: Write a PowerCLI script to run on all virtual appliances and force a redirection on port 443 This is incorrect. Forcing

redirection to port 443 (HTTPS) via a PowerCLI script might enable encrypted communication for some components, but it's a manual, ad-hoc solution that:

Doesn't ensure trusted access (no mention of certificate trust).

Doesn't integrate with a CA for certificate management.

Contradicts lifecycle enhancement, as it requires ongoing manual intervention rather than automation. This approach is not scalable or supported in VCF 5.2 for meeting security requirements.

Option D: Write an Aria Orchestrator Workflow to change the ESXi hosts' certificates in bulk. This is incorrect. While VMware Aria Orchestrator (formerly vRealize Orchestrator) can automate certificate updates for ESXi hosts, it's a partial solution that:

Only addresses ESXi hosts, not all management components (e.g., SDDC Manager, NSX).

Doesn't inherently ensure trust unless tied to a trusted CA (not specified here).

Improves lifecycle management only for ESXi certificates, not the broader VCF stack. This option lacks the holistic scope required by the question and isn't a native VCF design decision.

Conclusion: Integrating SDDC Manager with a 3rd-party CA (Option A) is the only design decision that fully satisfies all requirements. It leverages VCF 5.2's built-in certificate management capabilities to ensure trust, encryption, and lifecycle efficiency across the entire solution.

References:

VMware Cloud Foundation 5.2 Architecture and Deployment Guide (Section: Certificate Management) VMware Cloud Foundation 5.2 Planning and Preparation Guide (Section: Security Design Considerations) vSphere 7.0U3 Security Configuration Guide (integrated in VCF 5.2): Certificate Authority Integration

NEW QUESTION # 53

As part of a VMware Cloud Foundation (VCF) design, an architect is responsible for planning for the migration of existing workloads using HCX to a new VCF environment. Which two prerequisites would the architect require to complete the objective? (Choose two.)

- **A. Active Directory configured as an authentication source.**
- B. NSX Federation implemented between the VCF instances.
- **C. Service accounts for the applicable appliances.**
- D. DRS enabled within the VCF instance.
- E. Extended IP spaces for all moving workloads.

Answer: A,C

Explanation:

VMware HCX (Hybrid Cloud Extension) is a key workload migration tool in VMware Cloud Foundation (VCF) 5.2, enabling seamless movement of VMs between on-premises environments and VCF instances (or between VCF instances). To plan an HCX-based migration, the architect must ensure prerequisites are met for deployment, connectivity, and operation. Let's evaluate each option:

Option A: Extended IP spaces for all moving workloads. This is incorrect. HCX supports migrations with or without extending IP spaces. Features like HCX vMotion and Bulk Migration allow VMs to retain their IP addresses (Layer 2 extension via Network Extension), while HCX Mobility Optimized Networking (MON) can adapt IPs if needed. Extended IP space is a design choice, not a prerequisite, making this option unnecessary for completing the objective.

Option B: DRS enabled within the VCF instance. This is incorrect. VMware Distributed Resource Scheduler (DRS) optimizes VM placement and load balancing within a cluster but is not required for HCX migrations.

HCX operates independently of DRS, handling VM mobility across environments (e.g., from a source vSphere to a VCF destination). While DRS might enhance resource management post-migration, it's not a prerequisite for HCX functionality.

Option C: Service accounts for the applicable appliances. This is correct. HCX requires service accounts with appropriate permissions to interact with source and destination environments (e.g., vCenter Server, NSX).

In VCF 5.2, HCX appliances (e.g., HCX Manager, Interconnect, WAN Optimizer) need credentials to authenticate and perform operations like VM discovery, migration, and network extension. The architect must ensure these accounts are configured with sufficient privileges (e.g., read/write access in vCenter), making this a critical prerequisite.

Option D: NSX Federation implemented between the VCF instances. This is incorrect. NSX Federation is a multi-site networking construct for unified policy management across NSX deployments, but it's not required for HCX migrations. HCX leverages its own Network Extension service to stretch Layer 2 networks between sites, independent of NSX Federation. While NSX is part of VCF, Federation is an advanced feature unrelated to HCX's core migration capabilities.

Option E: Active Directory configured as an authentication source. This is correct. In VCF 5.2, HCX integrates with the VCF identity management framework, which typically uses Active Directory (AD) via vSphere SSO for authentication. Configuring AD as an authentication source ensures that HCX administrators can log in using centralized credentials, aligning with VCF's security model. This is a prerequisite for managing HCX appliances and executing migrations securely.

Conclusion: The two prerequisites required for HCX migration in VCF 5.2 are service accounts for the applicable appliances (Option

