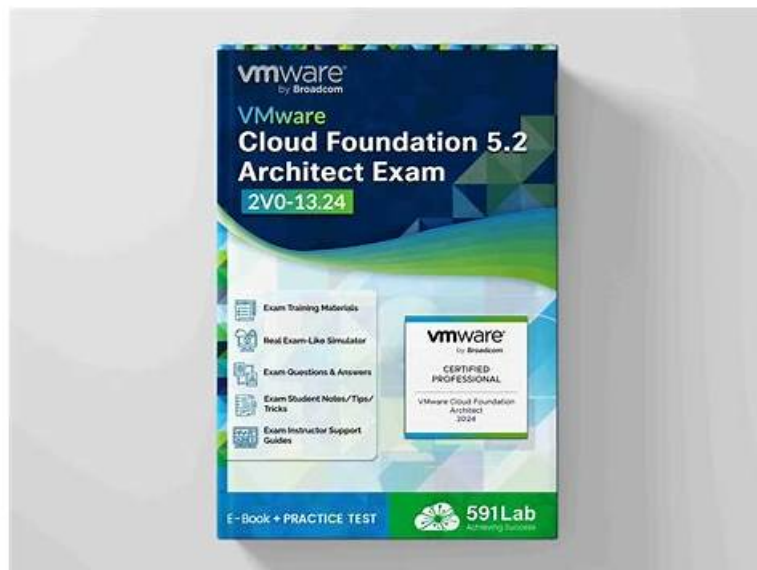


Free PDF 2025 2V0-13.24: Pass-Sure Examinations VMware Cloud Foundation 5.2 Architect Actual Questions



As you know, our 2V0-13.24 practice exam has a vast market and is well praised by customers. All you have to do is to pay a small fee on our 2V0-13.24 practice materials, and then you will have a 99% chance of passing the 2V0-13.24 exam and then embrace a good life. We are confident that your future goals will begin with this successful exam. So choosing our 2V0-13.24 Training Materials is a wise choice. Our practice materials will provide you with a platform of knowledge to help you achieve your dream. Welcome to select and purchase our 2V0-13.24 practice materials.

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	Troubleshoot and Optimize the VMware by Broadcom Solution: This section has NO TESTABLE OBJECTIVES in this version of the exam.
Topic 4	Install, Configure, and Administrate the VMware by Broadcom Solution: This section has NO TESTABLE OBJECTIVES in this version of the exam.

Topic 5	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.
---------	--

>> Examinations 2V0-13.24 Actual Questions <<

New 2V0-13.24 Study Materials | Exam 2V0-13.24 Overviews

Free demo is the benefit we give every candidate. you can download any time if you are interested in our 2V0-13.24 dumps torrent. Don't worry about the quality of our exam materials, you can tell from our free demo. If you would like to receive 2V0-13.24 dumps torrent fast, we can satisfy you too. After your payment you can receive our email including downloading link, account and password on website. You can download our complete high-quality VMware 2V0-13.24 Dumps Torrent as soon as possible if you like any time.

VMware Cloud Foundation 5.2 Architect Sample Questions (Q80-Q85):

NEW QUESTION # 80

An architect is working on higher-scale NSX Grouping and security design requirements for Management and VI Workload Domains in VMware Cloud Foundation. Which NSX Manager appliance size will be considered for use?

- A. Medium
- B. Small
- C. Extra Large
- D. Large

Answer: D

Explanation:

In VMware Cloud Foundation (VCF) 5.2, NSX Manager appliances manage networking and security (e.g., grouping, policies, firewalls) for Management and VI Workload Domains. The appliance size-Small, Medium, Large, Extra Large-determines its capacity to handle scale, such as the number of hosts, VMs, and security objects. The phrase "higher scale" implies a larger-than-minimum deployment. Let's evaluate:

NSX Manager Appliance Sizes (VCF 5.2 with NSX-T 3.2):

Small: 4 vCPUs, 16 GB RAM, 300 GB disk. Supports up to 16 hosts, basic deployments (e.g., lab environments).

Medium: 6 vCPUs, 24 GB RAM, 300 GB disk. Supports up to 64 hosts, suitable for small to medium production environments.

Large: 12 vCPUs, 48 GB RAM, 300 GB disk. Supports up to 512 hosts, 10,000 VMs, and complex security policies-standard for production VCF.

Extra Large: 24 vCPUs, 64 GB RAM, 300 GB disk. Supports over 512 hosts, massive scale (e.g., service providers, multi-VCF instances).

VCF Context:

Management Domain: Minimum 4 hosts, often 6-7 for HA, with NSX for overlay networking.

VI Workload Domains: Variable host counts, but "higher scale" suggests multiple domains or significant workload growth.

Security Design: Grouping and policies (e.g., distributed firewall rules, tags) increase NSX Manager load, especially at scale.

Evaluation:

Small: Insufficient for production VCF, limited to 16 hosts. Unsuitable for a Management Domain (4-7 hosts) plus VI Workload Domains.

Medium: Adequate for small VCF deployments (up to 64 hosts), but "higher scale" implies more hosts or complex security, exceeding its capacity.

Large: The default and recommended size for VCF 5.2 production environments. It supports up to 512 hosts, thousands of VMs, and extensive security policies, fitting a Management Domain and multiple VI Workload Domains with "higher scale" needs.

Extra Large: Overkill unless managing hundreds of hosts or multiple VCF instances, which isn't indicated here.

Conclusion: The Large NSX Manager appliance size (Option B) is appropriate for a higher-scale NSX design in VCF 5.2. It balances

capacity and performance for Management and VI Workload Domains with advanced security requirements, aligning with VMware's standard recommendation.

References:

VMware Cloud Foundation 5.2 Architecture and Deployment Guide (Section: NSX Manager Sizing) NSX-T 3.2 Installation Guide (integrated in VCF 5.2): Appliance Size Specifications VMware Cloud Foundation 5.2 Planning and Preparation Guide (Section: Security Design)

NEW QUESTION # 81

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

Answer: C

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 # 82

An architect is designing a VMware Cloud Foundation (VCF)-based private cloud solution for a customer that will include two physical locations. The customer has stated the following requirement:

All management tooling must be resilient at the component level within a single site.

When considering the design decisions for VMware Aria Suite components, what should the Architect document to meet the stated requirement?

- A. The solution will implement an external load balancer for Aria Operations Cloud Proxies.
- B. The solution will configure the VCF Workload domain in a stretched topology across two locations.
- **C. The solution will deploy three Aria Automation appliances in a clustered configuration.**
- D. The solution will deploy Aria Suite Lifecycle Manager in a high availability configuration.

Answer: C

Explanation:

The requirement specifies that management tooling must be resilient at the component level within a single site, meaning each site's management components (e.g., VMware Aria Suite) must withstand individual failures without relying on the other site. Let's evaluate each option in the context of VCF 5.2 and Aria Suite:

Option A: The solution will implement an external load balancer for Aria Operations Cloud Proxies. Aria Operations Cloud Proxies collect data for monitoring and don't inherently require an external load balancer for resiliency within a site. The VMware Aria Operations Administration Guide indicates that proxies are lightweight and typically deployed per cluster, with resiliency achieved via multiple proxies, not load balancing. This doesn't directly address component-level resiliency for the broader Aria Suite management tools.

Option B: The solution will configure the VCF Workload domain in a stretched topology across two locations. A stretched topology extends a workload domain across two sites for site-level resiliency (e.g., disaster recovery), not component-level resiliency within a single site. The VCF 5.2 Architectural Guide notes that stretched clusters rely on cross-site failover, which contradicts the requirement for single-site resilience, making this irrelevant to management tooling within one site.

Option C: The solution will deploy three Aria Automation appliances in a clustered configuration. VMware Aria Automation (formerly vRealize Automation) supports a clustered deployment with three appliances (primary, replica, and failover) to ensure high availability within a site. The VMware Aria Automation Installation Guide confirms that this configuration provides component-level resiliency by allowing the cluster to tolerate individual appliance failures without service disruption. In VCF, Aria Automation is a key management tool, and this design meets the requirement for single-site resilience.

Option D: The solution will deploy Aria Suite Lifecycle Manager in a high availability configuration. Aria Suite Lifecycle Manager (LCM) manages the lifecycle of Aria components but isn't deployed in a clustered HA configuration itself in VCF 5.2—it's a single appliance with backup/restore options. The VCF

5.2 Administration Guide notes that LCM resiliency is typically achieved via infrastructure HA (e.g., vSphere HA), not native clustering, making this less directly aligned with component-level resiliency compared to Aria Automation clustering.

Conclusion: Option C best meets the requirement by ensuring Aria Automation, a critical management tool, is resilient at the component level within a single site through clustering, aligning with VCF and Aria Suite best practices. References:

VMware Cloud Foundation 5.2 Architectural Guide (docs.vmware.com): Management Component Design.

VMware Aria Automation Installation Guide (docs.vmware.com): Clustered Configuration for HA.

VMware Aria Suite Lifecycle Administration Guide (docs.vmware.com): LCM Deployment Options.

NEW QUESTION # 83

In a conceptual model for VMware Cloud Foundation, which of the following components is typically included?

Response:

- A. Detailed configurations of the management components
- B. The exact number of ESXi hosts and storage devices
- C. The specific models of the servers to be used
- **D. Logical groupings of services such as compute, storage, and networking**

Answer: D

NEW QUESTION # 84

Answer: D

- • • • •

- [illegible]