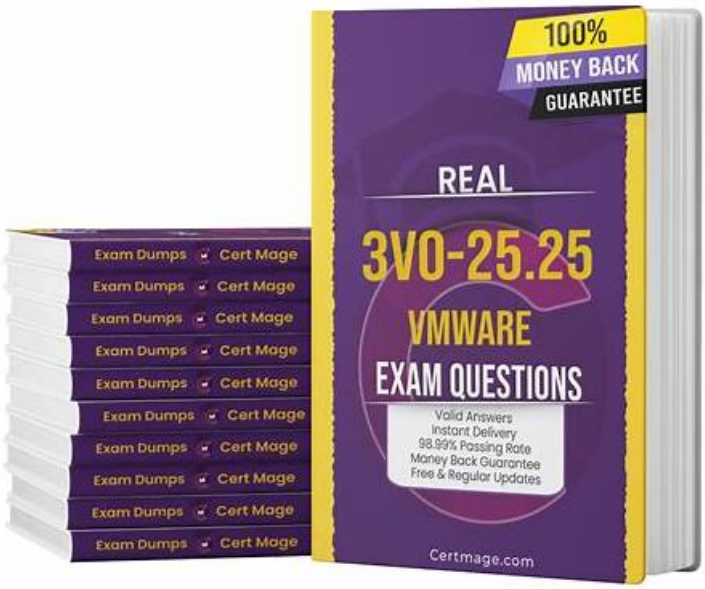
3V0-25.25 Valid Test Topics, Exam 3V0-25.25 Simulator



DOWNLOAD the newest PassReview 3V0-25.25 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1_t4mGK5esIePh8-Ha4gl1K9wv9pc4oF4

The 3V0-25.25 exam questions are the ideal and recommended study material for quick and easiest Advanced VMware Cloud Foundation 9.0 Networking (3V0-25.25) exam dumps preparation. The Advanced VMware Cloud Foundation 9.0 Networking (3V0-25.25) practice questions are designed and verified by qualified and renowned VMware Certification Exams trainers. They work closely and check all VMware 3V0-25.25 Exam Dumps step by step. They also ensure the best possible answer for all 3V0-25.25 exam questions and strive hard to maintain the top standard of Advanced VMware Cloud Foundation 9.0 Networking (3V0-25.25) exam dumps all the time.

VMware 3V0-25.25 Exam Syllabus Topics:

Topic	Details
Topic 1	• VMware Products and Solutions: This domain focuses on VMware's core offerings including vSphere for virtualization, NSX for software-defined networking, and vSAN for storage, enabling private and hybrid cloud environments.
Topic 2	• IT Architectures, Technologies, Standards: This domain covers foundational IT structural designs like client-server and microservices, implementation technologies such as containerization and APIs, and industry standards like ISO • IEC, TOGAF, and security frameworks.
Topic 3	• Install, Configure, Administrate the VMware Solution: This domain covers NSX implementation including deploying Federation, configuring components, creating Edge Clusters and gateways, managing VPC, stateful services, tenancy, integrations, and operational tasks.
Topic 4	• Troubleshoot and Optimize the VMware Solution: This domain focuses on identifying and resolving NSX issues using VCF tools, troubleshooting infrastructure and routing problems, and understanding ECMP, high availability, and packet flows.

Topic 5	• Plan and Design the VMware Solution: This domain addresses NSX design including architecture, connectivity solutions, multisite deployments, NSX Fleet considerations, and optimization decisions based on given scenarios.

>> 3V0-25.25 Valid Test Topics <<

VMware 3V0-25.25 Exam Dumps Fastest Way Of Preparation 2026

There are thousands of customers have passed their exam successfully and get the related certification. After that, all of their Advanced VMware Cloud Foundation 9.0 Networking exam torrents were purchase on our website. Our 3V0-25.25 study tool boost three versions for you to choose and they include PDF version, PC version and APP online version. Each version is suitable for different situation and equipment and you can choose the most convenient method to learn our 3V0-25.25 test torrent. For example, APP online version is printable and boosts instant access to download. You can study the Advanced VMware Cloud Foundation 9.0 Networking guide torrent at any time and any place. We provide 365-days free update and free demo available. The PC version of 3V0-25.25 Study Tool can stimulate the real exam's scenarios, is stalled on the Windows operating system and runs on the Java environment. You can use it any time to test your own exam stimulation tests scores and whether you have mastered our 3V0-25.25 test torrent or not.

VMware Advanced VMware Cloud Foundation 9.0 Networking Sample Questions (Q36-Q41):

NEW QUESTION # 36
An architect is designing a VMware Cloud Foundation (VCF) solution. The following information was gathered during the assessment phase:
* There is a critical application used by the Finance Team.
* The critical application has an availability and recoverability SLA of 99.999%.
* The critical application is sensitive to network changes.
Which two configurations should the architect include in their design? (Choose two.)

- A. Configure Tier-0 gateway for eBGP and ECMP.
- B. Install and configure hosts with 100Gbps physical NICs.
- C. Configure Tier-1 gateway for eBGP and ECMP.
- D. Configure multiple static routes on Tier-1 gateway.
- E. Enable BFD on the Tier-0 gateway.

Answer: A,E

Explanation:
Comprehensive and Detailed 250 to 350 words of Explanation From VMware Cloud Foundation (VCF) documents:
Designing for "five nines" (99.999%) availability in aVMware Cloud Foundation (VCF)environment requires a network architecture that minimizes convergence time and eliminates single points of failure. For a critical application sensitive to network changes, the connection between the virtualized SDDC and the physical network must be highly resilient and capable of near-instantaneous failover.
TheTier-0 Gatewayis the primary interface for North-South traffic. To meet high availability requirements, the Tier-0 should be configured witheBGP (External Border Gateway Protocol)to peer with physical Top- of-Rack (ToR) switches. By enablingECMP (Equal Cost Multi-Pathing), the architect allows the Tier-0 to utilize multiple active paths to the physical world simultaneously. This not only increases available bandwidth but also ensures that if one physical link or router fails, traffic is immediately redistributed across the remaining active paths without a protocol timeout.
To complement ECMP,BFD (Bidirectional Forwarding Detection)is essential. While BGP's default keepalive and hold timers are often measured in seconds (typically 60 and 180 seconds, respectively), BFD provides sub-second failure detection. In a VCF environment, BFD operates as a lightweight "heartbeat" between the Tier-0 Edge nodes and the physical ToR routers. If a path fails, BFD detects it within milliseconds and notifies BGP to pull the failed path from the routing table. This combination ofeBGP/ECMP for path redundancy andBFDfor rapid detection is the verified standard for VCF designs requiring extreme uptime and sensitivity to network disruptions.
Static routes (Option A) are unsuitable for high-availability designs as they lack dynamic failure detection.
While 100Gbps NICs (Option E) provide bandwidth, they do not inherently provide the protocol-level resilience needed to meet a 99.999% SLA.

NEW QUESTION # 37
An administrator has deployed a new VMware Cloud Foundation (VCF) management domain. To be compliant with company policy, backups must be configured to occur anytime a change is made to the NSX configuration. How can the administrator ensure that complete configuration backups are captured every time a change occurs?

- A. Create a recurring backup schedule and explicitly indicate that backups should be captured anytime the configuration changes.
- B. Configure an alarm to detect configuration changes and automatically trigger a complete configuration backup.
- C. No action is required as by default NSX will automatically perform a complete backup every time a change is made to the configuration.
- D. Configure a cron job on the NSX Manager to automatically perform an incremental backup of the NSX configuration every hour.

Answer: A

Explanation:
Comprehensive and Detailed 250 to 350 words of Explanation From VMware Cloud Foundation (VCF) documents:
InVMware Cloud Foundation (VCF), the protection of theNSX Managerconfiguration is paramount, as it contains the state of the entire software-defined network, including firewall rules, logical switches, and routing topologies. To meet strict compliance requirements for real-time or change-based protection, NSX offers specific automated backup triggers.
Within theNSX Manager UI(under System > Lifecycle > Backup & Restore), an administrator can configure the backup behavior. While a time-based schedule (e.g., daily at 2:00 AM) is common, it does not satisfy the requirement for backups "anytime a change is made." To accomplish this, the administrator must enable the
"Backup on Configuration Change"toggle within the backup scheduling configuration.
When this feature is enabled, the NSX Manager monitors its own management database (DS) for write operations. Once a configuration change is detected (such as adding a segment or modifying a DFW rule), the system initiates an automated backup process. This ensures that the backup repository always contains a near- instantaneous reflection of the current network state, minimizing data loss in the event of a cluster failure.
Option B is incorrect because this feature is not enabled by default; it requires an external SFTP/FTP server to be configured first. Option C (Cron jobs) is an unsupported manual workaround that bypasses the SDDC- native management tools. Option A is redundant as the functionality is built directly into the NSX backup engine. Consequently, the verified method for compliance is to use thenative recurring backup schedule with the "Detect Configuration Change" option enabled.

NEW QUESTION # 38
An administrator has noticed an issue in a freshly deployed VMware Cloud Foundation (VCF) environment where the BGP neighborship between the Tier-0 gateway and a physical router remains in the Idle state. Pings between the uplink IPs are successful. What is the issue?

- A. Distributed Firewall blocking traffic.
- B. Geneve tunnel down.
- C. Overlay MTU too low.
- D. Autonomous System number mismatch.

Answer: D

Explanation:
Comprehensive and Detailed 250 to 350 words of Explanation From VMware Cloud Foundation (VCF) documents:
In the context ofVMware Cloud Foundation (VCF), particularly versions 5.x and the architectural advancements inVCF 9.0, the establishment of North-South routing via theNSX Tier-0 Gatewayis a critical post-deployment or bring-up task. The Tier-0 gateway usesBorder Gateway Protocol (BGP)to peer with physical Top-of-Rack (ToR) switches to exchange reachability information for the overlay networks.
When a BGP session is reported in the"Idle"state, it indicates that the BGP Finite State Machine (FSM) is at its first stage and is not yet attempting a TCP connection, or it has encountered an error that forced it back to this state. According to VMware VCF documentation and NSX troubleshooting guides, if the administrator can successfully ping between the Tier-0 uplink IP and the physical router interface,Layer 3 reachability is confirmed. This eliminates issues related to physical cabling, VLAN tagging on the trunk ports, or basic IP interface configuration.
The primary reason a BGP session remainsIdledespite successful ICMP reachability is a configuration mismatch. Specifically, anAutonomous System (AS) number mismatchis the most frequent culprit. BGP requires that the "Remote AS" configured on the Tier-0 gateway matches the "Local AS" of the physical peer.

If the SDDC Manager automated workflow or the manual configuration in NSX Manager contains a typo in these values, the protocol handshake will fail immediately.
While aDistributed Firewall (DFW)could technically block port 179, it is not common in a "freshly deployed" environment for the default rules to block the Edge Node's control plane traffic.Geneve tunnelsand MTU issues(Option C and D) typically affect the data plane-causing packet loss for encapsulated guest VM traffic-but they do not prevent the BGP control plane (running over standard TCP) from moving beyond the Idle state. Therefore, verifying the AS numbers in the VCF Planning and Preparation Workbook against the physical switch configuration is the verified resolution path.

NEW QUESTION # 39
An administrator has observed an NSX Local Manager (LM) outage at the secondary Site. However, the NSX Global Manager (GM) in secondary Site remains operational. What happens to data plane operations and policy enforcement at the secondary site?

- A. The data plane operates normally until LM recovery and reconnection.
- B. Only local policies work; global policies cease to apply on the secondary site.
- C. All traffic is blocked until secondary site LM recovers.
- D. Secondary site must failover all workloads to Primary site.

Answer: A

Explanation:
Comprehensive and Detailed 250 to 350 words of Explanation From VMware Cloud Foundation (VCF) documents:
The architecture ofNSX Federationwithin a VCF Multi-Site design is built upon a separation of theControl Planeand theData Plane. This "decoupled" architecture ensures high availability and resiliency even when management components become unavailable.
In NSX Federation, theGlobal Manager (GM)handles the configuration of objects that span multiple locations, while theLocal Manager (LM)is responsible for pushing those configurations down to the local Transport Nodes (ESXi hosts and Edges) within its specific site. When a configuration is pushed, the Local Manager communicates with theCentral Control Plane (CCP)and subsequently theLocal Control Plane (LCP)on the hosts.
If an NSX Local Manager goes offline, the "Management Plane" for that site is lost. This means no new segments, routers, or firewall rules can be created or modified at that site. However, the existing configuration is already programmed into theData Plane(the kernels of the ESXi hosts and the DPDK process of the Edge nodes).
According to VMware's "NSX Multi-Location Design Guide," the data plane remains fully operational during a Management Plane outage. Existing VMs will continue to communicate, BGP sessions on the Edges will remain established, and Distributed Firewall (DFW) rules will continue to be enforced based on the last known good configuration state cached on the hosts. The data plane does not require constant heartbeats from the Local Manager to forward traffic. Therefore, operations continue normally "headless" until the LM is restored and can resume synchronization with the Global Manager and local hosts. Failover to a primary site (Option D) is only necessary if the actual data plane (hosts/storage) fails, not just the management components.

NEW QUESTION # 40
An administrator must provide North/South connectivity for a VPC. The fabric exposes a distributed external VLAN across all ESX hosts. But, the only BGP peer to the core is on a VLAN only accessible on the Edge Cluster. Which design is required?

- A. Deploy a Provider Tier-1 with BGP and connect the VPC Transit Gateway via route leaking.
- B. Centralized Transit Gateway on the Edge Cluster.
- C. Distributed Transit Gateway with an EVPN route reflector on the transport nodes.
- D. Use a VPC Tier-0 Gateway in active/active mode with distributed eBGP peering.

Answer: B

Explanation:
Comprehensive and Detailed 250 to 350 words of Explanation From VMware Cloud Foundation (VCF) documents:
In aVMware Cloud Foundation (VCF)environment utilizing theVirtual Private Cloud (VPC)model, North /South connectivity is managed by theTransit Gateway (TGW). The TGW acts as the bridge between the VPC-internal networks and the provider-level physical network.
The scenario presents a specific constraint: while an external VLAN exists across all hosts, the actual BGP peering point (the interface to the physical core routers) is restricted to theNSX Edge Cluster. In NSX terminology, when a gateway or service must be anchored to specific Edge Nodes to access physical network services-such as BGP peering, NAT, or stateful firewalls-it must be configured as aCentralizedcomponent.
ACentralized Transit Gateway(Option C) is instantiated on the Edge nodes. This allows the TGW to participate in the BGP session with the core routers on the VLAN that is only accessible to those Edges. The TGW then handles the routing for the VPC's internal

segments. Traffic from the ESXi transport nodes (East- West) travels via the Geneve overlay to the Edge nodes, where it is then routed North-South by the Centralized TGW using the physical BGP peer.
Option A is incorrect because "distributed eBGP peering" would require every ESXi host to have peering capabilities, which contradicts the constraint. Option B involves EVPN, which is a significantly more complex and different architecture than what is required for standard VPC North/South access. Option D is an unnecessarily complex routing design that is not the standard VCF/VPC implementation pattern. Thus, the use of a Centralized Transit Gateway on the Edge cluster is the verified design requirement to bridge the gap between the overlay VPC and the localized BGP peering point.

NEW QUESTION # 41
.....