VMware VCAP-NV Design 3V0-42.23 Practice Questions

Shared by Battle on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A Solutions Architect is working with a customer who wants to extend their traditional Telco IP/MPLS core network to an NFV cloud.

Which NSX feature can be recommended by the architect?

Options:

A- BGP
B- EVPN
C- Load Balancer
D- Distributed IDS

Answer:

B

Explanation:

EVPN for Telco and NFV Cloud Extensions (Correct Answer - B):

Ethernet VPN (EVPN) allows seamless integration between MPLS-based networks and NSX overlays.

Supports L2/L3 VPN, VLAN stretching, and multi-data center deployments.

Ideal for Telco NFV (Network Function Virtualization) clouds that require scalable, multi-tenant networking.

Incorrect Options:

(A - BGP):

BGP (Border Gateway Protocol) is used for dynamic routing, but EVPN is specifically designed for Telco MPLS integration.

(C - Load Balancer):

Load Balancers improve application availability, but do not provide Telco network extension.

(D - Distributed IDS):

IDS/IPS secures workloads, but is not relevant for NFV cloud connectivity.

VMware NSX 4.x Reference:

NSX-T EVPN and Multi-Site Network Extension Guide

Telco NFV Cloud Deployment with VMware NSX

Question 2

Question Type: MultipleChoice

What is the function of the control plane in NSX?

Options:

A- It provides the NSX APIs for automation and integration.
B- It configures the data plane within the NSX environment.
C- It handles access control within the NSX environment.
D- It forwards traffic in the NSX environment.

Answer:

B

Explanation:

1. NSX Control Plane Responsibilities

The control plane is responsible for programming and distributing network configurations to the data plane.

It ensures that forwarding decisions are precomputed and pushed to transport nodes (ESXi/KVM hosts).

It does not forward traffic itself but instructs the data plane on how to do so.

2. Why 'Configures the Data Plane' is the Correct Answer (B)

NSX Control Plane manages configuration and route distribution.

Uses Central Control Plane (CCP) to compute forwarding decisions.

Uses Local Control Plane (LCP) to communicate with Transport Nodes.

3. Why Other Options are Incorrect

(A - Provides APIs):

NSX APIs belong to the management plane, not the control plane.

(C - Handles Access Control):

Security policies are enforced in the data plane, not the control plane.

(D - Forwards Traffic):

The data plane is responsible for forwarding packets, not the control plane.

4. NSX Control Plane Design Considerations

Ensure NSX Managers (which include the control plane) are deployed in a 3-node cluster for high availability.

BGP and OSPF routes should be dynamically distributed to transport nodes via the control plane.

Monitor NSX Manager performance to ensure routing convergence times are optimal.

VMware NSX 4.x Reference:

NSX-T Control Plane Architecture and Best Practices

NSX-T Routing and Forwarding Table Optimization

Question 3

Question Type: MultipleChoice

A global logistics company is planning to expand its operations to multiple locations across continents. Their existing on-premises network is unable to scale to meet the demands of the growing number of sites and the increasing volume of East-West traffic within their data center. The company has chosen VMware NSX as their preferred network virtualization platform, aiming to simplify network management and improve intra-data center routing.

Which of the following would be part of the optimal recommended design?

Options:

A- Deploy NSX and use Centralized Service Ports to handle East-West routing within the data center.
B- Deploy NSX with Aria Operations for Networks to handle North-South routing within the data center.
C- Deploy NSX with Tier-1 Gateways to handle East-West routing within the data center.
D- Deploy NSX with Tier-0 Gateways to handle North-South routing within the data center.

Answer:

C

Explanation:

Tier-1 Gateways for East-West Traffic (Correct Answer - C):

East-West traffic refers to communication within the data center (e.g., between workloads).

Tier-1 Gateways are optimized for East-West routing, ensuring efficient intra-data center traffic handling.

This minimizes unnecessary traffic to external routers, reducing latency and improving performance.

Incorrect Options:

(A - Centralized Service Ports for East-West Routing):

Centralized Service Ports (CSPs) are used for stateful services, not for general East-West routing.

(B - Aria Operations for Networks for North-South Routing):

Aria Operations for Networks (formerly vRealize Network Insight) is a monitoring and analytics tool, not a routing solution.

(D - Tier-0 for East-West Routing):

Tier-0 Gateways handle North-South routing (external connectivity), not East-West traffic.

VMware NSX 4.x Reference:

NSX-T Data Center Routing Design Guide

NSX-T Multi-Tier Gateway Architecture Best Practices

Question 4

Question Type: MultipleChoice

Which three VMware guidelines are recommended when designing VLANs and subnets for a single region and single availability zone? (Choose three.)

Options:

A- Use the RFC1918 IPv4 address space for these subnets and allocate one octet by region and another octet by function.
B- Use the RFC2460 IPv6 address space for these subnets and allocate one set by region and another set by function.
C- Use only /16 subnets to reduce confusion and mistakes when handling IPv4 subnetting.
D- Use only /24 subnets to reduce confusion and mistakes when handling IPv4 subnetting.
E- Use the IP address of the floating interface for Virtual Router Redundancy Protocol (VRRP) or Hot Standby Routing Protocol (HSRP) as the gateway.

Answer:

A, D, E

Explanation:

Recommended Network Design Guidelines:

(A - Use RFC1918 Addressing):

VMware NSX-T recommends using RFC1918 private address space for internal networks to avoid public address conflicts.

(D - Use /24 Subnets):

/24 subnets are preferred as they provide 256 usable IPs, simplifying management and subnetting.

(E - Floating Interface for VRRP/HSRP):

NSX Gateway HA uses VRRP (Virtual Router Redundancy Protocol) or HSRP (Hot Standby Routing Protocol) for gateway failover, ensuring redundancy.

Incorrect Options:

(B - Use IPv6 RFC2460 Addressing) IPv6 is optional in NSX, but IPv4 remains the primary addressing method.

(C - Use /16 Subnets) Using /16 subnets results in large broadcast domains and unnecessary complexity.

VMware NSX 4.x Reference:

NSX-T Network Design Best Practices

NSX-T Gateway HA & VRRP Configuration Guide

Question 5

Question Type: MultipleChoice

A large multinational company is expanding its data center due to increased demand for online services.

The company is considering shifting from an NSX Edge VM design to a bare-metal NSX Edge design to accommodate new hardware acquisitions and maximize performance.

Which is a potential benefit for the company in shifting from an NSX Edge VM design to a bare-metal NSX Edge design?

Options:

A- It will maximize performance by reducing virtualization overhead.
B- It will allow for the implementation of more VLANs.
C- It will automatically distribute stateful services across Edge nodes.
D- It will eliminate the need for stateful services.

Answer:

A

Explanation:

Performance Benefits of Bare-Metal NSX Edge (Correct Answer - A):

Bare-metal NSX Edge Nodes provide higher performance by eliminating the virtualization overhead associated with Edge VMs running inside ESXi/KVM hosts.

This increases throughput and reduces latency, making it ideal for high-bandwidth applications (e.g., Load Balancing, VPN, and NAT).

Incorrect Options:

(B - More VLANs):

The number of VLANs is not limited by the NSX Edge type. VLAN scalability depends on physical network design.

(C - Automatic Stateful Service Distribution):

Stateful services (NAT, FW, LB, VPN) do not auto-distribute. Stateful HA must be manually configured.

(D - Eliminates Stateful Services):

Stateful services (e.g., NAT, Load Balancer, Firewall) are still required, regardless of Edge deployment mode.

VMware NSX 4.x Reference:

VMware NSX-T Bare-Metal Edge Deployment Guide

NSX-T Edge Node Performance Optimization

Question 6

Question Type: MultipleChoice

What is the effect of stateful services placement on NSX Edge design?

Options:

A- It has stateless services applications that cannot run with stateful applications.
B- It affects the scalability of the Edge cluster and performance of Edge nodes.
C- It reduces the need for load balancing in the Edge cluster.
D- It determines the complexity of the Edge cluster and size of Edge node.

Answer:

B

Explanation:

Impact of Stateful Services on NSX Edge Cluster (Correct Answer - B):

Stateful services (NAT, FW, LB, VPN) require additional processing power, impacting Edge node performance.

More stateful services means higher CPU and memory utilization, affecting scalability.

Edge Cluster design must balance stateful workloads to avoid performance degradation.

Incorrect Options:

(A - Stateless services cannot run with stateful applications):

Stateful and stateless services can coexist on NSX Edge, but require careful placement.

(C - Reduces the need for load balancing):

Load balancing is still needed, even if stateful services exist.

(D - Determines complexity of Edge cluster size):

While it adds complexity, the primary impact is on performance and scalability.

VMware NSX 4.x Reference:

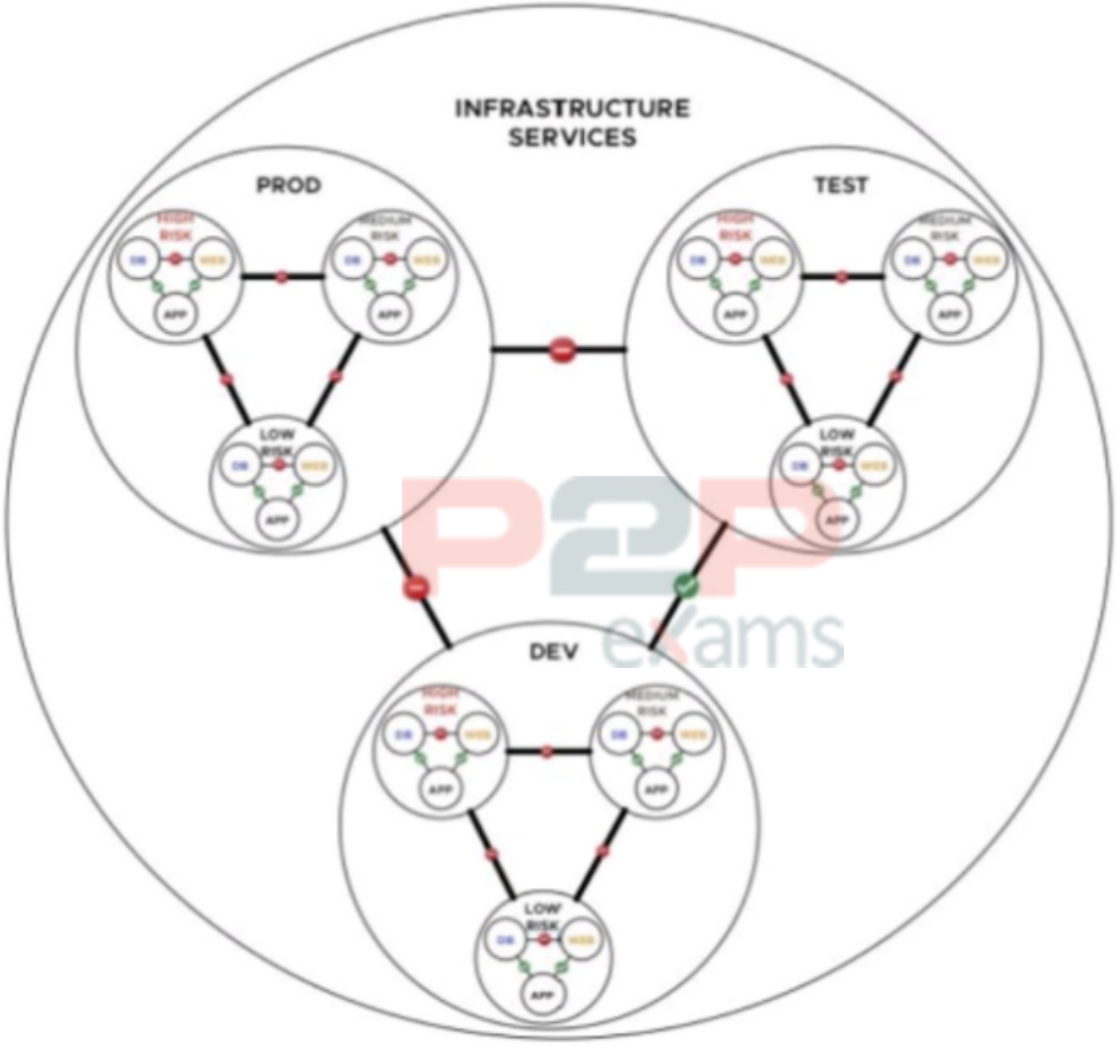
NSX-T Edge Cluster Design and Performance Best Practices

VMware NSX-T Scaling Stateful Services Guide

Question 7

Question Type: MultipleChoice

Refer to the exhibit.



A financial company is adopting micro-services with the intent of simplifying network security.

An NSX architect is proposing a NSX segmentation logical design. The architect

has created a diagram to share with the customer.

Which design choice provides less management overhead?

Options:

A- Create one firewall rule per application tier.
B- Create one security policy per level of security.
C- Create one firewall rule per level of security.
D- Create a security policy based on IP groups.

Answer:

B

Explanation:

1. Understanding the Exhibit and NSX Security Segmentation

The diagram represents NSX-T logical segmentation for a microservices-based financial company.

It categorizes workloads into three distinct risk levels:

High Risk (Red)

Medium Risk (Yellow)

Low Risk (Blue)

The objective is to enforce security policies with minimal management overhead while maintaining isolation between risk levels.

2. Why 'One Security Policy Per Level of Security' is the Best Choice (B)

Grouping workloads based on security levels (High, Medium, Low) simplifies firewall rule management.

By defining a single security policy per level of security, it reduces the need to create multiple firewall rules for each microservice individually.

Advantages of this approach:

Scalability: New workloads can inherit existing security policies without manual rule creation.

Simplification: Instead of hundreds of firewall rules, a few policies handle traffic isolation effectively.

Automation-Friendly: Security policies can be applied dynamically using NSX-T security groups.

3. Why Other Options are Incorrect

(A - Create One Firewall Rule Per Application Tier)

High overhead and complexity: Each application has its own rule, making it harder to scale as the number of applications grows.

Requires continuous manual rule creation, increasing administrative burden.

Better suited for small, static environments but not scalable for microservices.

(C - Create One Firewall Rule Per Level of Security)

Firewall rules alone do not provide granular segmentation.

A single firewall rule is insufficient to define security controls across multiple application tiers.

Security policies provide a more structured approach, including Layer 7-based controls and dynamic membership.

(D - Create a Security Policy Based on IP Groups)

IP-based security policies are outdated and not scalable in a dynamic microservices environment.

NSX-T supports workload-based security policies instead of traditional IP-based segmentation.

Microservices often use dynamic IP addresses, making IP-based groups ineffective for security enforcement.

4. NSX Security Best Practices for Microservices-Based Designs

Use NSX Distributed Firewall (DFW) for Micro-Segmentation

Apply security at the workload (vNIC) level to prevent lateral movement of threats.

Enforce Zero Trust security model by restricting traffic between risk zones.

Group Workloads by Security Posture Instead of Static IPs

Leverage dynamic security groups (tags, VM attributes) instead of static IPs.

Assign security rules based on business logic (e.g., production vs. development, PCI-compliant workloads).

Use Security Policies Instead of Individual Firewall Rules

Policies provide abstraction, reducing the number of firewall rules.

Easier to manage and apply to multiple workloads dynamically.

Monitor and Automate Security Policies Using NSX Intelligence

Continuously analyze workload communication patterns using VMware Aria Operations for Networks (formerly vRealize Network Insight).

Automate rule updates based on detected traffic flows.

Question 8

Question Type: MultipleChoice

A rapidly growing e-commerce company, with a global customer base, is seeking to enhance their current network infrastructure to ensure a seamless and secure user experience. They have opted for VMware NSX to leverage software-defined networking (SDN) capabilities, and are particularly interested in employing NSX Edge to maximize their network performance.

A solutions architect is tasked with designing an effective and efficient solution using NSX Edge that meets the customer's requirements. The design should incorporate North-South routing to handle traffic to and from the internet.

To meet the company's requirements, what optimal solution should the solutions architect recommend, utilizing NSX Edge?

Options:

A- Deploy a single NSX Edge node for North-South routing services.
B- Deploy a single NSX Edge node and use a separate physical router for East-West routing.
C- Deploy multiple NSX Edge nodes and configure a Tier-0 Gateway in Active-Standby mode for North-South routing services.
D- Deploy multiple NSX Edge nodes and configure a Tier-0 Gateway in Active-Active mode for North-South routing services.

Answer:

D

Explanation:

1. Importance of NSX Edge for North-South Traffic

NSX Edge nodes provide routing, NAT, firewall, and load balancing services for North-South traffic (external connectivity).

Active-Active Tier-0 Gateway provides maximum performance and resiliency for high traffic volume.

2. Why Active-Active Tier-0 with Multiple Edge Nodes is the Best Choice (D)

Supports Equal-Cost Multi-Path (ECMP) routing, distributing North-South traffic across multiple paths.

Provides better scalability and performance than Active-Standby mode.

Ideal for high-volume applications like e-commerce sites that require low-latency, high-throughput connections.

3. Why Other Options are Incorrect

(A - Single NSX Edge Node):

Single Edge Nodes introduce a single point of failure.

(B - Using a Physical Router for East-West Routing):

NSX handles East-West traffic internally using Distributed Routing.

(C - Active-Standby Tier-0 Gateway):

Active-Standby mode does not provide load balancing across multiple nodes.

4. NSX Edge and Tier-0 Gateway Design Considerations

Ensure sufficient bandwidth allocation for North-South traffic.

Use BGP or OSPF for dynamic route advertisement.

Configure ECMP for efficient multi-path forwarding.

VMware NSX 4.x Reference:

NSX-T Edge Node Scaling and Performance Best Practices

Tier-0 Gateway Active-Active vs. Active-Standby Deployment Guide

Question 9

Question Type: MultipleChoice

A Solutions Architect is helping an organization with the multi-location design of an NSX solution.

This information was gathered during a design workshop:

No Jumbo Frames allowed on the WAN

Simple DR solution with no fabric nor vCenter requirements

GDPR requirements (Management Plane distributed in each location)

What should the architect recommend be configured in the NSX environment?

Options:

A- NSX Federation
B- NSX Multisite
C- Tier-0 Gateway Active/Active
D- IPSec VPN between the sites

Answer:

B

Explanation:

NSX Multisite for Compliance & Distributed Management (Correct Answer - B):

NSX Multisite supports deployments without requiring centralized management (NSX Federation).

Since GDPR requires data locality, separate NSX Managers per site help comply with data protection laws.

No Jumbo Frames requirement indicates transport overlays are not required, making Multisite a better fit than NSX Federation.

Incorrect Options:

(A - NSX Federation):

Federation requires Global Manager, which is not needed for a simple DR solution.

(C - Active/Active Tier-0 Gateway):

Active/Active Tier-0 is a routing decision, not a multi-location design strategy.

(D - IPSec VPN):

IPSec VPN is not sufficient for multi-site management.

VMware NSX 4.x Reference:

NSX Multisite vs. Federation Architecture Guide

GDPR Compliance with NSX Multisite Best Practices

Question 10

Question Type: MultipleChoice

A financial institution is looking to improve their existing virtual environment with a focus on increasing security to protect sensitive dat

a. The firm has a single data center and is concerned about lateral movement of threats within the network. They are particularly interested in utilizing VMware NSX to implement segmentation and adopt a Zero Trust security model.

Which of the following would be part of the optimal recommended design, utilizing a firewall?

Options:

A- Implement NSX with Gateway Firewall with each application deployed on its own Overlay Network.
B- Implement NSX with a Distributed Firewall with each application deployed on its own Overlay Network.
C- Implement NSX with Gateway Firewall with the use of VLAN-backed virtual standard switch for network segmentation.
D- Implement NSX with a Distributed Firewall with the use of VLAN-backed virtual standard switch for network segmentation.

Answer:

B

Explanation:

NSX Distributed Firewall for Zero Trust Security (Correct Answer - B):

NSX Distributed Firewall (DFW) provides micro-segmentation at the vNIC level to enforce Zero Trust policies.

Each application runs on its own NSX Overlay Network, preventing lateral movement of threats.

Application-specific segmentation ensures granular control and compliance with regulatory standards (PCI-DSS, GDPR).

Incorrect Options:

(A - Gateway Firewall on Overlay Networks):

The Gateway Firewall controls North-South traffic, but DFW is required for East-West security.

(C & D - VLAN-Backed Networks Instead of Overlays):

VLANs are limited in scalability compared to overlay networks, reducing segmentation flexibility.

VMware NSX 4.x Reference:

NSX-T Distributed Firewall and Micro-Segmentation Guide

Zero Trust Security Model Implementation in NSX