VMware

Exam Questions 2V0-41.24

VMware NSX 4.X Professional V2

NEW QUESTION 1
Which of the following settings must be configured in an NSX environment before enabling stateful active-active SNAT?

A. Tier-1 gateway in active-standby mode
B. A Punting Traffic Group for the NSX Edge uplinks
C. An Interface Group for the NSX Edge uplinks
D. Tier-1 gateway in distributed only mode

Answer: B

Explanation:
In an NSX environment, a Punting Traffic Group for the NSX Edge uplinks must be configured before enabling stateful active-active Source NAT (SNAT). This configuration ensures that traffic is appropriately handled and forwarded between the NSX Edge nodes in an active-active setup, allowing stateful connections to be maintained across multiple Edge nodes.

NEW QUESTION 2
Where does an administrator configure the VLANs used in VRF Lite? (Choose two.)

A. uplink interface of the VRF gateway
B. uplink interface of the default Tier-0 gateway
C. uplink trunk segment
D. segment connected to the Tier-1 gateway

Answer: AD

Explanation:
The VLANs used in VRF Lite are configured on the uplink interface of the VRF gateway, which enables traffic segmentation and routing within the VRF context. The uplink trunk segment is where multiple VLANs can be configured and tagged, allowing them to be used by the VRF Lite setup for routing and segmentation across the network.

NEW QUESTION 3
When configuring OSPF on Tier-0 Gateway, which three of the following must match in order to establish a neighbor relationship with an upstream router? (Choose three.)

A. Area ID
B. MTU of the Uplink C Naming convention
C. Address of the neighbor
D. Subnet mask
E. Protocol and Port

Answer: ABE

Explanation:
Area ID: Both routers must belong to the same OSPF area for a neighbor relationship to form.
MTU of the Uplink: Mismatched MTU settings can prevent the OSPF adjacency from forming, as OSPF packets may be dropped if they exceed the MTU size.
Subnet mask: Both routers must have the same subnet mask on the interface where OSPF is configured to establish a neighbor relationship.

NEW QUESTION 4
Which command on ESXi is used to verify the Local Control Plane connectivity with Central Control Plane?

A. esxcli network ip connection list | grep netcpa
B. esxcli network ip connection list | grep ccpd
C. esxcli network ip connection list | grep 1234
D. esxcli network ip connection list | grep 1235

Answer: A

Explanation:
The netcpa process is responsible for Local Control Plane (LCP) connectivity with the Central Control Plane (CCP) in NSX. Using the command esxcli network ip connection list | grep netcpa, administrators can verify the connectivity status between the LCP on the ESXi host and the CCP, ensuring proper communication for NSX operations.

NEW QUESTION 5
Which troubleshooting step will resolve an error with code 1001 during the configuration of a time-based firewall rule?

A. Restarting the NTPservice on the ESXi host.
B. Reconfiguring the ESXi host with a local NTP server.
C. Re-installing the NSX VIBs on the ESXi host.
D. Changing the time zone on the ESXi host.

Answer: A

Explanation:
An error with code 1001 during the configuration of a time-based firewall rule often indicates a time synchronization issue. Restarting the NTP service on the ESXi host can resolve this issue by ensuring that the host??s time is synchronized correctly, which is essential for time-based rules to function accurately.

NEW QUESTION 6
An NSX administrator wants to create a Tier-0 Gateway to support equal cost multi-path (ECMP) routing.
Which failover detection protocol must be used to meet this requirement?

A. Host Standby Router Protocol (HSRP)
B. Beacon Probing (BP)
C. Virtual Router Redundancy Protocol (VRRP)
D. Bidirectional Forwarding Detection (BFD)

Answer: D

Explanation:
To support Equal-Cost Multi-Path (ECMP) routing in an NSX environment, Bidirectional Forwarding Detection (BFD) must be used for failover detection. BFD is a rapid failure detection protocol that works with ECMP to provide fast failure detection between routers. It helps in detecting link failures more quickly than traditional protocols, ensuring that traffic is routed through available paths as quickly as possible.

NEW QUESTION 7
An NSX administrator would like to create an L2 segment with the following requirements:
• L2 domain should not exist on the physical switches.
• East/West communication must be maximized as much as possible. Which type of segment must the administrator choose?

A. VLAN
B. Overlay
C. Bridge
D. Hybrid

Answer: B

Explanation:
An overlay segment is a layer 2 broadcast domain that is implemented as a logical construct in the NSX-T Data Center software. Overlay segments do not require any configuration on the physical switches, and they allow for optimal east/west communication between workloads on different ESXi hosts. Overlay segments use the Geneve protocol to encapsulate and decapsulate traffic between the hosts. Overlay segments are created and managed by the NSX Manager.
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID- 316E5027-E588-455C-88AD-A7DA930A4F0B.html

NEW QUESTION 8
Which CLI command on NSX Manager and NSX Edge is used to change NTP settings?

A. set timezone
B. set ntp-server
C. get timezone
D. get time-server

Answer: B

Explanation:
The set ntp-server command is used on NSX Manager and NSX Edge to configure the NTP (Network Time Protocol) settings. This command allows administrators to specify the NTP server, ensuring that the NSX components synchronize their time accurately with the designated time server.

NEW QUESTION 9
Which two built-in VMware tools will help identify the cause of packet loss on VLAN Segments? (Choose two.)
Which two built-in VMware tools will help identify the cause of packet loss on VLAN Segments? (Choose two.)

A. Flow Monitoring
B. Traceflow
C. Live Flow
D. Packet Capture
E. Activity Monitoring

Answer: BD

Explanation:
Traceflow: This tool helps in troubleshooting network issues by injecting synthetic packets into the network and observing their path. It allows administrators to trace the packet flow across various network segments, making it easier to identify points of packet loss. Packet Capture: This tool enables detailed inspection of traffic by capturing packets at specific points in the network. It allows administrators to analyze packet headers and payloads to determine if packet loss is occurring and to identify possible causes.

NEW QUESTION 10
What is the VMware recommended way to deploy a virtual NSX Edge Node?

A. Through the NSX Ul
B. Through automated or interactive mode using an ISO
C. Through the vSphere Web Client
D. Through the OVF command line tool

Answer: B

Explanation:
VMware recommends deploying a virtual NSX Edge Node using an ISO in either automated or interactive mode. This method provides flexibility and ensures that

the NSX Edge node is deployed properly with all the necessary configurations. Using an ISO allows for a more streamlined and controlled deployment process, especially in larger environments.

NEW QUESTION 10
Which two statements describe the characteristics of an Edge Cluster in NSX? (Choose two.)

A. Must have only active-active edge nodes
B. Can contain multiple types of edge nodes (VM or bare metal)
C. Must contain only one type of edge nodes (VM or bare metal)
D. Can have a maximum of 10 edge nodes
E. Can have a maximum of 8 edge nodes

Answer: BE

Explanation:
An NSX Edge Cluster can contain a mix of edge node types, meaning it can have both virtual machine (VM) and bare-metal edge nodes within the same cluster.
An NSX Edge Cluster supports a maximum of 8 edge nodes, allowing for scalability while adhering to the NSX design limitations for edge clusters.

NEW QUESTION 12
Which NSX CLI command is used to change the authentication policy for local users?

A. set hardening-policy
B. get auth-policy minimum-password-length
C. set cli-timeout
D. set auth-policy

Answer: D

Explanation:
The set auth-policy command in the NSX CLI is used to configure the authentication policy for local users. This command allows administrators to adjust settings related to password policies, lockout policies, and other authentication-related parameters for local user accounts on NSX Manager.

NEW QUESTION 14
Which table on an ESXi host is used to determine the location of a particular workload for a frame-forwarding decision?

A. Routing Table
B. ARP Table
C. TEP Table
D. MAC Table

Answer: D

Explanation:
The MAC Table on an ESXi host is used to determine the location of a particular workload for frame-forwarding decisions. This table maps MAC addresses to specific interfaces, enabling the ESXi host to forward frames to the correct destination based on the MAC address of the workload. This is crucial for efficient Layer 2 forwarding decisions within the host.

NEW QUESTION 18
Where is the insertion point for East-West network introspection?

A. Tier-0 router
B. Guest VM vNIC
C. Partner SVM
D. Host Physical NIC

Answer: B

Explanation:
The insertion point for East-West network introspection in NSX is at the Guest VM vNIC (virtual Network Interface Card). By inspecting traffic at the vNIC level, NSX can monitor and apply security policies to traffic between virtual machines (East-West traffic) within the same network segment or data center, providing detailed security controls for VM-to-VM communication.

NEW QUESTION 20
What are three NSX Manager roles? (Choose three.)

A. master
B. manager
C. controller
D. cloud
E. policy
F. zookeeper

Answer: ACF

Explanation:
master: The master role in NSX Manager is responsible for managing and coordinating the other NSX Manager nodes in the cluster.
policy: The policy role handles the policy-driven API and configuration, allowing administrators to define and manage network and security policies.

controller: The controller role in NSX Manager manages control plane functions and handles routing, switching, and other network state information required for NSX operations.

NEW QUESTION 22
The security administrator turns on logging for a firewall rule. Where is the log stored on an ESXi transport node?

A. /var/log/messages.log
B. /var/log/vmware/nsx/firewall.log
C. /var/log/fw.log
D. /var/log/dfwpktlogs.log

Answer: D

Explanation:
When logging is enabled for a firewall rule in NSX, the logs are stored on the ESXi transport node in the /var/log/vmware/nsx/firewall.log file. This file contains information about firewall rule hits and is useful for monitoring and troubleshooting firewall activity on the transport node.

NEW QUESTION 25
An administrator wants to validate the BGP connection status between the Tier-0 Gateway and the upstream physical router.
What sequence of commands could be used to check this status on NSX Edge node?

A. - enable <LR-D>- get vrf <ID>- show bgp neighbor
B. - get gateways- vrf <number>- get bgp neighbor
C. - set vrf <ID>- show logical-routers- show <LR-D> bgp
D. - show logical-routers- get vrf- show ip route bgp

Answer: A

Explanation:
To validate the BGP connection status between the Tier-0 Gateway and the upstream physical router on an NSX Edge node, the correct sequence involves enabling the specific logical router (Tier-0 Gateway), checking the VRF (Virtual Routing and Forwarding) context, and then using the show bgp neighbor command to view the BGP session status. enable <LR-D>: This command enables the logical router interface (Tier-0 Gateway) to access its configuration.
get vrf <ID>: This command checks the specific VRF (used for routing separation) to see the associated routing table.
show bgp neighbor: This command displays the status of the BGP connection, including details about the neighbor relationships and their state.

NEW QUESTION 30
An administrator is configuring service insertion for Network Introspection. Which two places can the Network Introspection be configured? (Choose two.)

A. Edge Node
B. Host pNIC
C. Tier-0 gateway
D. Tier-1 gateway
E. Partner SVM

Answer: DE

Explanation:
Tier-1 gateway: Network introspection services can be configured at the Tier-1 gateway level to inspect and control East-West traffic between workloads.
Partner SVM (Service Virtual Machine): Network introspection is often implemented through integration with a Partner SVM, which is a virtual machine provided by a third-party security partner to perform deep packet inspection and other security functions.

NEW QUESTION 35
Which VPN type must be configured before enabling an L2VPN?

A. Policy-based IPSec VPN
B. Port-based IPSec VPN
C. SSL-based IPSec VPN
D. Route-based IPSec VPN

Answer: D

Explanation:
Before enabling an L2VPN (Layer 2 VPN) in NSX, a Route-based IPSec VPN must be configured. Route-based VPNs create a secure tunnel over which Layer 2 traffic can be extended, allowing for the creation of L2VPN connections. This setup is required to establish the underlying secure connectivity that L2VPN relies on for traffic between sites.

NEW QUESTION 37
What should an NSX administrator check to verify that VMware Identity Manager integration is successful?

A. From the NSX Ul the status of the VMv/are Identity Manager Integration must be Enabled'
B. From the NSX CLI the status of the VMware Identity Manager Integration must be Configured'
C. From VMware Identity Manager the status of the remote access application must be green
D. From the NSX Ul the URI in the address bar must have locaMalstf part of it.

Answer: B

Explanation:

To verify that VMware Identity Manager integration is successful with NSX, the administrator should check the NSX UI for the integration status. If it is configured correctly, the status should be marked as "Enabled," indicating that the integration is active and functioning.

NEW QUESTION 41
Which three of the following describe the Border Gateway Routing Protocol (BGP) configuration on a Tier-0 Gateway? (Choose three.)

A. It supports a 4-byte autonomous system number.
B. Can be used as an Exterior Gateway Protocol.
C. The network is divided into areas that are logical groups.
D. EIGRP is disabled by default.
E. BGP is enabled by default.

Answer: ABE

Explanation:
It supports a 4-byte autonomous system number: BGP on a Tier-0 Gateway supports 4-byte AS (Autonomous System) numbers, which are necessary for larger routing domains. Can be used as an Exterior Gateway Protocol: BGP is commonly used as an Exterior Gateway Protocol to establish routing between different autonomous systems (AS).
BGP is enabled by default: On a Tier-0 Gateway, BGP is typically enabled by default, allowing administrators to configure it for external routing.

NEW QUESTION 45
Which three selections are capabilities of Network Topology? (Choose three.)

A. Display how the different NSX components are interconnected.
B. Display the VMs connected to Segments.
C. Display how the Physical components are interconnected.
D. Display the uplinks configured on the Tier-1 Gateways.
E. Display the uplinks configured on the Tier-0 Gateways.

Answer: ABC

Explanation:
Display how the different NSX components are interconnected.
Network Topology in NSX provides a visual representation of how different NSX components (like Edge nodes, Logical Routers, and other NSX components) are interconnected.
Display the VMs connected to Segments.
It also allows you to see which VMs are connected to specific segments (logical switches). Display how the Physical components are interconnected.
The Network Topology view includes information about how physical network components are connected, providing a comprehensive overview of both the virtual and physical networking infrastructure.

NEW QUESTION 47
What are two supported host switch modes? (Choose two.)

A. Overlay Datapath
B. Secure Datapath
C. Standard Datapath
D. Enhanced Datapath
E. DPDK Datapath

Answer: CD

Explanation:
Standard Datapath: This is the traditional mode used by the NSX host switch. It is typically used in environments where performance requirements are standard and no special acceleration techniques are needed.
Enhanced Datapath: This mode is designed to improve performance and provide better scalability, especially for environments with higher traffic loads or more demanding applications. It can provide better performance in certain scenarios by improving packet processing efficiency.

NEW QUESTION 49
In an NSX environment, an administrator is observing low throughput and congestion between the Tier-0 Gateway and the upstream physical routers.
Which two actions could address low throughput and congestion? (Choose two.)

A. Configure ECMP on the Tier-0 gateway.
B. Configure a Tier-1 gateway and connect it directly to the physical routers.
C. Deploy Large size Edge node/s.
D. Configure NAT on the Tier-0 gateway.
E. Add an additional vNIC to the NSX Edge node.

Answer: AC

Explanation:
Configure ECMP on the Tier-0 gateway: ECMP (Equal-Cost Multi-Path) allows multiple paths for traffic between the Tier-0 Gateway and the upstream physical routers, effectively distributing the traffic load and improving throughput. By enabling ECMP, you can reduce congestion and increase bandwidth utilization, thus addressing performance issues. Deploy Large size Edge node/s: Deploying larger Edge nodes can provide more resources (CPU, memory, and network interfaces) to handle higher throughput and reduce congestion. This is especially important if the existing Edge node is overwhelmed by the amount of traffic.

NEW QUESTION 53
As part of an organization??s IT security compliance requirement, NSX Manager must be configured for 2FA (two-factor authentication).
What should an NSX administrator have ready before the integration can be configured?

A. Active Directory LDAP integration with ADFS
B. VMware Identity Manager with NSX added as a Web Application
C. VMware Identity Manager with an OAuth Client added
D. Active Directory LDAP integration with OAuth Client added

Answer: B

Explanation:
To enable two-factor authentication (2FA) for NSX Manager, VMware Identity Manager must be configured and integrated with NSX. The NSX Manager should be added as a web application in VMware Identity Manager, which will allow 2FA to be applied during the authentication process. VMware Identity Manager supports 2FA methods, including integration with external identity providers, and it can manage access to NSX with additional security layers.

NEW QUESTION 57
What are four NSX built-in role-based access control (RBAC) roles? (Choose four.)

A. None
B. Read
C. Auditor
D. Full Access
E. Network Admin
F. Enterprise Admin
G. Operator

Answer: ABCD

Explanation:
None: No permissions are granted, restricting the user??s access entirely.
Read: Grants read-only access, allowing the user to view configurations and settings without making changes.
Auditor: Similar to Read, but typically includes access to audit logs and more detailed viewing permissions for compliance purposes.
Full Access: Grants complete control over all NSX configurations and settings, allowing unrestricted access.

NEW QUESTION 60
An administrator has deployed 10 Edge Transport Nodes in their NSX Environment, but has forgotten to specify an NTP server during the deployment.
What is the efficient way to add an NTP server to all 10 Edge Transport Nodes?

A. Use a Node Profile
B. Use Transport Node Profile
C. Use the CLI on each Edge Node
D. Use a PowerCLI script

Answer: B

Explanation:
Using a Transport Node Profile allows the administrator to apply configuration changes, such as specifying an NTP server, across multiple Edge Transport Nodes efficiently. This method is scalable and avoids the need for manual configuration on each individual node. Once the Transport Node Profile is updated, the configuration can be pushed to all associated nodes.

NEW QUESTION 61
Which three NSX Edge components are used for North-South Malware Prevention? (Choose three.)

A. Thin Agent
B. RAPID
C. Security Hub
D. IDS/IPS
E. Security Analyzer
F. Reputation Service

Answer: BCD

Explanation:
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-69DF70C2-1769-4858- 97E7-B757CAED08F0.html#:~:text=On%20the%20north%2Dsouth%20traffic,Guest%20Introspe ction%20(GI)%20platform.
The main components on the edge node for north-south malware prevention perform the following functions:
• IDS/IPS engine: Extracts files and relays events and data to the security hub
North-south malware prevention uses the file extraction features of the IDS/IPS engine that runs on NSX Edge for north-south traffic.
• Security hub: Collects file events, obtains verdicts for known files, sends files for local and cloud-based analysis, and sends information to the security analyzer
• RAPID: Provides local analysis of the file
• ASDS Cache: Caches reputation and verdicts of known files

NEW QUESTION 64
Which three data collection sources are used by NSX Network Detection and Response to create correlations/Intrusion campaigns? (Choose three.)

A. Files and anti-malware (lie events from the NSX Edge nodes and the Security Analyzer
B. East-West anti-malware events from the ESXi hosts
C. Distributed Firewall flow data from the ESXi hosts
D. IDS/IPS events from the ESXi hosts and NSX Edge nodes
E. Suspicious Traffic Detection events from NSX Intelligence

Answer: ADE

Explanation:
The correct answers are A. Files and anti-malware (file) events from the NSX Edge nodes and the Security Analyzer, D. IDS/IPS events from the ESXi hosts and NSX Edge nodes, and E. Suspicious Traffic Detection events from NSX Intelligence. According to the VMware NSX Documentation3, these are the three data collection sources that are used by NSX Network Detection and Response to create correlations/intrusion campaigns.
The other options are incorrect or not supported by NSX Network Detection and Response. East-West anti-malware events from the ESXi hosts are not collected by NSX
Network Detection and Response3. Distributed Firewall flow data from the ESXi hosts are not used for correlation/intrusion campaigns by NSX Network Detection and Response3. https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID- 14BBE50D-9931-4719-8FA7-884539C0D277.html

NEW QUESTION 68
An NSX administrator is using ping to check connectivity between VM1 running on ESXi1 to VM2 running on ESXi2. The ping tests fail. The administrator knows the maximum transmission unit size on the physical switch is 1600.
Which command does the administrator use to check the VMware kernel ports for tunnel end point communication?

A. vmkping ++netstack=geneve -d -s 1572 <destination IP address>
B. vmkping ++netstack=vxlan -d -s 1572 <destination IP address>
C. esxcli network diag ping –H <destination IP address>
D. esxcli network diag ping -I vmk0 -H <destination IP address>

Answer: A

Explanation:
The vmkping ++netstack=geneve -d -s 1572 <destination IP address> command is used to check connectivity for VMware kernel ports specifically for Geneve tunnel endpoints (TEPs). The -s 1572 option sets the packet size to test within the 1600 MTU limit, accounting for the Geneve encapsulation overhead. The -d option enables the "Don't Fragment" bit, ensuring the packet isn??t fragmented along the path, which is essential for verifying MTU consistency across the network.

NEW QUESTION 72
Which field in a Tier-1 Gateway Firewall would be used to allow access for a collection of trustworthy web sites?

A. Source
B. Profiles -> Context Profiles
C. Destination
D. Profiles -> L7 Access Profile

Answer: D

Explanation:
The field in a Tier-1 Gateway Firewall that would be used to allow access for a collection of trustworthy web sites is Profiles -> L7 Access Profile. This field allows the user to create a Layer 7 access profile that defines a list of allowed or blocked URLs based on categories, reputation, or custom entries1. The user can then apply the L7 access profile to a firewall rule to control the traffic based on the URL filtering criteria1. The other options are incorrect because they are not related to URL filtering. The Source field specifies the source IP address or group of the firewall rule1. The Destination field specifies the destination IP address or group of the firewall rule1. The Profiles -> Context Profiles field allows the user to create a context profile that defines a list of application signatures or attributes that can be used to identify and classify network traffic1. References: Gateway Firewall

NEW QUESTION 77
A customer is preparing to deploy a VMware Kubernetes solution in an NSX environment. What is the minimum MTU size for the UPLINK profile?

A. 1700
B. 1500
C. 1550
D. 1650

Answer: A

Explanation:
For a VMware Kubernetes deployment in an NSX environment, the minimum recommended MTU size for the UPLINK profile is 1700. This allows sufficient space for the additional overhead introduced by encapsulation protocols, such as Geneve, used in NSX- T Data Center, ensuring optimal performance and avoiding fragmentation.

NEW QUESTION 82
Which statement is true about an alarm in a Suppressed state?

A. An alarm can be suppressed for a specific duration in hours.
B. An alarm can be suppressed for a specific duration in seconds.
C. An alarm can be suppressed for a specific duration in days.
D. An alarm can be suppressed for a specific duration in minutes

Answer: A

Explanation:
In NSX and VMware environments, an alarm in a suppressed state can typically be set to remain suppressed for a specific duration measured in hours. This allows administrators to temporarily ignore the alarm for a set period while working on a resolution without continuous alerts.

NEW QUESTION 83

Which two statements are correct about East-West Malware Prevention? (Choose two.)

A. A SVM is deployed on every ESXi host.
B. NSX Application Platform must have Internet access.
C. An agent must be installed on every ESXi host.
D. An agent must be installed on every NSX Edge node.
E. NSX Edge nodes must have Internet access.

Answer: AB

Explanation:
Reference: https://docs.vmware.com/en/VMware-NSX-T-Data- Center/3.2/administration/GUID-0A8BF7D8-9C2E-48A5-8219-17C00F1EC13A.html
https://www.wwt.com/blog/primer-series-napp-malware-prevention

NEW QUESTION 86
Which command is used to display the network configuration of the Tunnel Endpoint (TEP) IP on a bare metal transport node?

A. debug
B. tcpdump
C. tcpconfig
D. ifconfig

Answer: D

Explanation:
The ifconfig command is used to display the network configuration of interfaces, including the Tunnel Endpoint (TEP) IP on a bare metal transport node. This command provides details about IP addresses, subnet masks, and other network settings for each interface on the node.

NEW QUESTION 89
An administrator has been tasked with implementing the SSL certificates for the NSX Manager Cluster VIP.
Which is the correct way to implement this change?

A. Send an API call to https://<nsx-mgr>/api/vl/cluster/api- certificate?action=set_cluster_certificate&certificate_id=<certificate_id>
B. Send an API call to https://<nsx- mgr>/api/vl/node/services/http?action=apply_certificate&certificate_id=<certificate_id>
C. SSH as admin into the NSX manager with the cluster VIP IP and run nsxcli cluster certificate node install <certificate_id>
D. SSH as admin into the NSX manager with the cluster VIP IP and run nsxcli cluster certificate vip install <certificate_id>

Answer: D

Explanation:
To implement SSL certificates for the NSX Manager Cluster VIP, the correct method is to SSH into the NSX Manager (using the Cluster VIP IP) and run the nsxcli cluster certificate vip install <certificate_id> command. This command installs the SSL certificate for the VIP, ensuring that the cluster's SSL certificate is properly configured for secure communications.

NEW QUESTION 90
Which two logical router components span across all transport nodes? (Choose two.)

A. SERVICE_ROUTER_TIER0
B. TIER0_DISTRIBUTED_ROUTER
C. DISTRIBUTED_ROUTER_TIER0
D. DISTRIBUTED_ROUTER_TIER1
E. SERVICE_ROUTER_TIER1

Answer: BD

Explanation:
TIER0_DISTRIBUTED_ROUTER: The Tier-0 Distributed Router spans all transport nodes, providing distributed routing capabilities across the NSX environment at the Tier-0 level. DISTRIBUTED_ROUTER_TIER1: Similarly, the Tier-1 Distributed Router spans all transport nodes, enabling distributed routing at the Tier-1 level, which allows routing functions to occur closer to the workload VMs across the transport nodes.

NEW QUESTION 93
When running nsxcli on an ESXi host, which command will show the Replication mode?

A. get logical-switch <Local-Switch-UUID> status
B. get logical-switch <Logical-Switch-UUID>
C. get logical-switches
D. get logical-switch status

Answer: C

Explanation:
https://vdc-download.vmware.com/vmwb-repository/dcr-public/c3fd9cef-6b2b-4772-93be-3fe60ce064a1/1f67b9e1-b111-4de7-9ea1-39931d28f560/NSX-T%20Command-Line%20Interface%20Reference.html#get%20logical- switch%20%3Clogical-switch-id%3E

NEW QUESTION 94
When a stateful service is enabled for the first time on a Tier-0 Gateway, what happens on the NSX Edge node?

A. DR is instantiated and automatically connected with SR.
B. SR is instantiated and automatically connected with DR.
C. SR and DR doesn??t need to be connected to provide any stateful services.
D. SR and DR is instantiated but requires manual connection.

Answer: B

Explanation:
When a stateful service (such as NAT or firewall) is enabled for the first time on a Tier-0 Gateway, the Service Router (SR) is instantiated on the NSX Edge node and automatically connected with the Distributed Router (DR). This connection enables the Tier-0 Gateway to handle stateful services by routing traffic through the SR, which manages stateful packet processing, while the DR provides distributed routing functionality.

NEW QUESTION 98
Which two of the following are used to configure Distributed Firewall on VDS? (Choose two.)

A. vSphere API
B. NSX API
C. NSX CU
D. vCenter API
E. NSX UI

Answer: BE

Explanation:
According to the VMware NSX Documentation, these are two of the ways that you can use to configure Distributed Firewall on VDS:
? NSX API: This is a RESTful API that allows you to programmatically configure and
manage Distributed Firewall on VDS using HTTP methods and JSON payloads. You can use tools such as Postman or curl to send API requests to the NSX Manager node.
? NSX UI: This is a graphical user interface that allows you to configure and manage Distributed Firewall on VDS using menus, tabs, buttons, and forms. You can access the NSX UI by logging in to the NSX Manager node using a web browser.
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-0DEF9F18-608D- 4B5C-9175-5514750E901B.html

NEW QUESTION 101
What must be configured on Transport Nodes for encapsulation and decapsulation of Geneve protocol?

A. TEP
B. STT
C. VXLAN
D. UDP

Answer: A

Explanation:
TEP (Tunnel Endpoint): TEPs (Tunnel Endpoints) are configured on transport nodes to handle the encapsulation and decapsulation of the Geneve protocol. TEPs are responsible for creating the overlay network by encapsulating traffic in the Geneve protocol when it moves between transport nodes and decapsulating it upon arrival.

NEW QUESTION 102
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

2V0-41.24 Practice Exam Features:

* 2V0-41.24 Questions and Answers Updated Frequently

* 2V0-41.24 Practice Questions Verified by Expert Senior Certified Staff

* 2V0-41.24 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 2V0-41.24 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 2V0-41.24 Practice Test Here