VMware.2V0-41.24.by.Rian.43q

Number: 2V0-41.24
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: 2V0-41.24

Exam Name: VMware NSX 4.X Professional V2

Exam A

QUESTION 1
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

Correct Answer: A, D
Section:
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.

QUESTION 2
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

Correct Answer: B, D
Section:
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.

QUESTION 3
What must be configured on Transport Nodes for encapsulation and decapsulation of Geneve protocol?

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

Correct Answer: A
Section:
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.

QUESTION 4
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

Correct Answer: A
Section:
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.

QUESTION 5
Which two of the following parameters are required for deploying the NSX Application Platform? (Choose two.)

A. Interface Name
B. Upload XML File
C. Cluster Format Type
D. Interface Service Name
E. Upload Kubernetes Configuration File

Correct Answer: B, E
Section:
Explanation:
Cluster Format Type: This parameter specifies the type of cluster format that will be used for the NSX Application Platform deployment.
Upload Kubernetes Configuration File: NSX Application Platform requires a Kubernetes environment, and the configuration file for Kubernetes must be uploaded to facilitate the deployment.

QUESTION 6
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.

Correct Answer: A, B, E
Section:
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.

QUESTION 7

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

Correct Answer: B
Section:
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.

QUESTION 8
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

Correct Answer: B
Section:
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.

QUESTION 9
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.

Correct Answer: A, B, C
Section:
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.

QUESTION 10
An NSX administrator has deployed a single NSX Manager node and will be adding two additional nodes to form a 3-node NSX Management Cluster for a production environment. The administrator will deploy these two

additional nodes and Cluster VIP using the NSX UI.
What two are the prerequisites for this configuration? (Choose two.)

A. The cluster configuration must be completed using API.
B. All nodes must be in the same subnet.
C. All nodes must be in separate subnets.
D. A compute manager must be configured.
E. NSX Manager must reside on a Windows Server.

Correct Answer: B, D
Section:
Explanation:
For a 3-node NSX Manager cluster, all nodes must be within the same subnet to ensure proper communication and functionality between them.
A compute manager must be configured before adding nodes to the cluster, as it provides the necessary integration between the NSX Manager and the underlying virtualization infrastructure (such as vSphere or vCenter).

QUESTION 11
Which two commands does an NSX administrator use to check the IP address of the VMkernel port for the Geneve protocol on the ESXi transport node? (Choose two.)

A. net-dvs
B. esxcfg-nics -l
C. esxcli network ip interface ipv4 get
D. esxcfg-vmknic -l
E. esxcli network nic list

Correct Answer: C
Section:
Explanation:
The esxcli network ip interface ipv4 get command is used to display the IP address configuration of the VMkernel network interfaces, including those used for the Geneve protocol.
The esxcfg-vmknic -l command lists all VMkernel network interfaces, including their IP addresses, which can help identify the VMkernel port for the Geneve protocol.

QUESTION 12
Which two are supported by L2 VPN clients? (Choose two.)

A. NSX Autonomous Edge
B. NSX Edge
C. NSX for vSphere Edge
D. 3rd party Hardware VPN Device

Correct Answer: B, D
Section:
Explanation:
The NSX Edge supports L2 VPN (Layer 2 VPN) functionality, which allows it to connect different Layer 2 networks over an IP transport.
Third-party hardware VPN devices can also be used as L2 VPN clients, providing connectivity between different Layer 2 networks through an external device.

QUESTION 13
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

Correct Answer: B
Section:
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.

QUESTION 14
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.

Correct Answer: A
Section:
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.

QUESTION 15
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>

Correct Answer: D
Section:
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.

QUESTION 16
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

Correct Answer: A
Section:
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.

QUESTION 17
What is VMware's recommendation for the minimum MTU requirements when planning an NSX deployment?

A. MTU should be set to 1700 or greater across the data center network including inter-data center connections.

B. MTU should be set to 1500 or less only on inter-data center connections.

C. Configure Path MTU Discovery and rely on fragmentation.

D. MTU should be set to 1550 or less across the data center network including inter-data center connections.

Correct Answer: A
Section:
Explanation:
VMware recommends setting the MTU (Maximum Transmission Unit) to 1700 or greater for NSX deployments. This is to ensure that the VXLAN encapsulation, which adds overhead to the original Ethernet frame, can be accommodated without fragmentation. This MTU requirement includes the entire data center network, including inter-data center connections, to ensure consistent communication across all network components involved in the NSX deployment.

QUESTION 18
In which VPN type are the Virtual Tunnel interfaces (VTI) used?

A. SSL-based VPN

B. Route & SSL based VPNs

C. Policy & Route based VPNs

D. Route-based VPN

Correct Answer: D
Section:
Explanation:
Virtual Tunnel Interfaces (VTI) are used in route-based VPNs. In this type of VPN, the tunnel is treated like a regular interface on the router. This allows for the configuration of routing protocols and the application of routing decisions to the traffic flowing through the VPN tunnel. VTIs simplify the management of routing and make it more flexible in VPN scenarios.

QUESTION 19
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.

Correct Answer: A, C
Section:
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.

QUESTION 20
A company security policy requires all users to log into applications using a centralized authentication system.
Which two authentication, authorization, and accounting (AAA) systems are available when integrating NSX with VMware Identity Manager? (Choose two.)

A. RSA SecureID
B. SecureDAP
C. RADII 2.0
D. LDAP and OpenLDAP based on Active Directory (AD)
E. Keygen Enterprise

Correct Answer: A, D
Section:
Explanation:
RSA SecureID: RSA SecureID is a commonly used two-factor authentication (2FA) system that can integrate with VMware Identity Manager for enhanced security during authentication, making it a suitable AAA system for user authentication.
LDAP and OpenLDAP based on Active Directory (AD): VMware Identity Manager can integrate with LDAP and OpenLDAP directories, including Active Directory (AD), for centralized user authentication. This allows users to authenticate against an organization's directory service.

QUESTION 21
An NSX administrator would like to export syslog events that capture messages related to NSX host preparation events.
Which message ID (msgid) should be used in the syslog export configuration command as a filter?

A. FABRIC
B. SYSTEM
C. GROUPING
D. MONITORING

Correct Answer: A
Section:
Explanation:
In NSX, the FABRIC message ID is used to capture and export syslog events related to host preparation and other fabric-related activities. These events are important for tracking and troubleshooting the setup and configuration of NSX components across the fabric, including host preparation events.

QUESTION 22
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)

Correct Answer: D
Section:
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.

QUESTION 23
An administrator has connected two virtual machines on the same overlay segment. Ping between both virtual machines is successful.
What type of network boundary does this represent?

A. Layer 2 bridge
B. Layer 2 broadcast domain
C. Layer 2 VPN
D. Layer 3 route

Correct Answer: B
Section:
Explanation:
When two virtual machines are connected on the same overlay segment, they are part of the same Layer 2 broadcast domain. In this case, the communication between the two VMs is happening within the same broadcast domain, which means that broadcast traffic can be sent to all devices on the segment. Since the ping is successful, the two VMs can communicate directly over Layer 2 without needing routing.

QUESTION 24
What are two supported host switch modes? (Choose two.)

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

Correct Answer: C, D
Section:
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.

QUESTION 25
Which is an advantage of an L2 VPN in an NSX 4.x environment?

A. Achieve better performance

B. Use the same broadcast domain

C. Enables Multi-Cloud solutions

D. Enables VM mobility with re-IP

Correct Answer: B
Section:
Explanation:
An L2 VPN (Layer 2 VPN) in an NSX 4.x environment allows you to extend a Layer 2 network across different sites or data centers. This enables the connected environments to share the same broadcast domain, meaning that broadcast traffic can be transmitted between sites as if they were on the same local network. This is particularly useful for scenarios where you need to maintain Layer 2 connectivity across geographically dispersed locations.

QUESTION 26
Which two steps must an NSX administrator take to integrate VMware Identity Manager in NSX to support role-based access control? (Choose two.)

A. Create a SAML authentication in VMware Identity Manager using the NSX Manager FQDN.

B. Add NSX Manager as a Service Provider (SP) in VMware Identity Manager.

C. Enter the Identity Provider (IdP) metadata URL in NSX Manager.

D. Enter the service URL, Client Secret, and SSL thumbprint in NSX Manager.

E. Create an OAuth 2.0 client in VMware Identity Manager.

Correct Answer: B, C
Section:
Explanation:
Adding NSX Manager as a Service Provider (SP) in VMware Identity Manager is necessary to enable SAML-based single sign-on (SSO), which allows VMware Identity Manager to manage and authenticate users accessing NSX.
Entering the Identity Provider (IdP) metadata URL in NSX Manager is required to establish a connection between NSX and VMware Identity Manager, enabling NSX to use VMware Identity Manager as the IdP for authentication.

QUESTION 27
Which of the two following characteristics about NAT64 are true? (Choose two.)

A. NAT64 requires the Tier-1 gateway to be configured in active-active mode.

B. NAT64 is stateless and requires gateways to be deployed in active-standby mode.

C. NAT64 is supported on Tier-0 and Tier-1 gateways.

D. NAT64 is supported on Tier-1 gateways only.

E. NAT64 requires the Tier-1 gateway to be configured in active-standby mode.

Correct Answer: C, E
Section:
Explanation:
NAT64 is supported on both Tier-0 and Tier-1 gateways, allowing for IPv6-to-IPv4 address translation at different gateway levels within NSX.
NAT64 requires the Tier-1 gateway to be configured in active-standby mode, as this configuration ensures stateful translation and consistency for IPv6-to-IPv4 traffic handling.

QUESTION 28
Which VMware GUI tool is used to identify problems in a physical network?

A. VMware Aria Operations Networks

B. VMware Aria Automation

C. VMware Site Recovery Manager

D. VMware Aria Orchestrator

Correct Answer: A
Section:
Explanation:
VMware Aria Operations Networks (formerly known as vRealize Network Insight) is a tool specifically designed for network visibility and troubleshooting. It provides insights into both virtual and physical network infrastructures, making it ideal for identifying problems in a physical network.

QUESTION 29
Which three protocols could an NSX administrator use to transfer log messages to a remote log server? (Choose three.)

A. HTTPS
B. SSH
C. TCP
D. UDP
E. SSL
F. TLS

Correct Answer: C, D, F
Section:
Explanation:
Both TCP and UDP are commonly used protocols for transferring log messages in syslog configurations. TCP is preferred when reliability is needed, while UDP is used for faster, connectionless transmission.
TLS can be used to secure the log messages being sent over TCP, ensuring encrypted transmission to the remote log server.

QUESTION 30
What are three NSX Manager roles? (Choose three.)

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

Correct Answer: A, C, F
Section:
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.

QUESTION 31
When collecting support bundles through NSX Manager, which files should be excluded for potentially containing sensitive information?

A. Core Files
B. Controller Files
C. Audit Files

D. Management Files

Correct Answer: A
Section:
Explanation:
Core Files should be excluded when collecting support bundles through NSX Manager because they may contain sensitive information, such as memory dumps that could reveal sensitive data from processes at the time of an issue. Excluding core files helps ensure that potentially sensitive data is not unintentionally shared.

QUESTION 32
What can the administrator use to identify overlay segments in an NSX environment if troubleshooting is required?

A. Geneve ID
B. VMI ID
C. Segment ID
D. VLANID

Correct Answer: B
Section:
Explanation:
In an NSX environment, each overlay segment is uniquely identified by a VNI ID (Virtual Network Identifier). The VNI is used to distinguish different overlay networks within the NSX environment and is essential for troubleshooting, as it helps administrators identify specific segments where traffic is encapsulated and isolated.

QUESTION 33
How does the Traceflow tool identify issues in a network?

A. Compares intended network state in the control plane with Tunnel End Point (TEP) keepalives in the data plane.
B. Compares the management plane configuration states containing control plane traffic and error reporting from transport node agents.
C. Injects ICMP traffic into the data plane and observes the results in the control plane.
D. Injects synthetic traffic into the data plane and observes the results in the control plane.

Correct Answer: D
Section:
Explanation:
The Traceflow tool in NSX injects synthetic traffic into the data plane and monitors the traffic flow through the network, allowing administrators to observe how the traffic is handled at each hop. This approach helps identify issues such as dropped packets, routing errors, or misconfigurations by providing visibility into the path taken by the traffic and any potential disruptions.

QUESTION 34
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

Correct Answer: B
Section:
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.

QUESTION 35
Which is the only supported mode in NSX Global Manager when using Federation?

A. Proxy
B. Policy
C. Controller
D. Proton

Correct Answer: B
Section:
Explanation:
When using NSX Federation, Policy mode is the only supported mode in NSX Global Manager. This mode allows centralized management and consistent policy enforcement across multiple NSX environments, providing a unified approach to managing network and security policies in federated deployments.

QUESTION 36
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.

Correct Answer: B
Section:
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.

QUESTION 37
An NSX administrator is creating a Tier-1 Gateway configured in Active-Standby High Availability Mode. In the event of node failure, the failover policy should not allow the original failed node to become the Active node upon recovery.
Which failover policy meets this requirement?

A. Enable Preemptive
B. Non-Preemptive
C. Preemptive
D. Disable Preemptive

Correct Answer: B
Section:
Explanation:
In Non-Preemptive failover policy, once a failover occurs and a new Active node is designated, the original failed node will not automatically become the Active node upon recovery. This setting ensures that the failover does not revert to the original node after it comes back online, maintaining the stability of the network by keeping the current Active node as is.

QUESTION 38
Which CLI command is used for packet capture on the ESXi Node?

A. tcpdump
B. set capture
C. pktcap-uw
D. debug

Correct Answer: C
Section:
Explanation:
The pktcap-uw command is specifically used on ESXi hosts for packet capture. It provides a detailed packet capture utility that allows administrators to capture traffic at various points on the ESXi host, such as virtual switches, uplinks, and VMkernel interfaces, making it a powerful tool for network troubleshooting on ESXi nodes.

QUESTION 39
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

Correct Answer: A
Section:
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.

QUESTION 40
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

Correct Answer: B, E
Section:
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.

QUESTION 41
Which two CLI commands could be used to see if vmnic link status is down? (Choose two.)

A. esxcfg-nics -l
B. esxcli network nic list
C. esxcfg-vmknic -l

D. esxcfg-vmsvc/get.networks
E. esxcli network vswitch dvs vmware list

Correct Answer: A, B
Section:
Explanation:
esxcfg-nics -l: This command lists all physical NICs on the ESXi host along with their link status, allowing you to check if any vmnic link status is down.
esxcli network nic list: This command provides a list of network interfaces with their details, including link status, making it useful for verifying if the link status of a vmnic is down.

QUESTION 42
Which VMware NSX Portfolio product can be described as a distributed analysis solution that provides visibility and dynamic security policy enforcement for NSX environments?

A. NSX Manager
B. NSX Distributed IDS/IPS
C. NSX Intelligence
D. NSX Cloud

Correct Answer: C
Section:
Explanation:
NSX Intelligence is a distributed analytics solution within the VMware NSX Portfolio that provides visibility and dynamic security policy enforcement in NSX environments. It enables detailed traffic analysis, identifies security threats, and helps in the automated creation and enforcement of security policies based on observed network traffic patterns and behaviors.

QUESTION 43
An administrator has a requirement to have consistent policy configuration and enforcement across NSX instances.
What feature of NSX fulfills this requirement?

A. Multi-hvpervisor support
B. Federation
C. Load balancer
D. Policy-driven configuration

Correct Answer: B
Section:
Explanation:
NSX Federation allows consistent policy configuration and enforcement across multiple NSX instances or environments. It provides a unified framework to manage security and networking policies across different NSX deployments, enabling centralized control and consistent application of policies across multiple sites or data centers.