

VMware

Exam Questions 2V0-41.23

VMware NSX 4.x Professional



NEW QUESTION 1

What are two valid options when configuring the scope of a distributed firewall rule? (Choose two.)

- A. DFW
- B. Tier-1 Gateway
- C. Segment
- D. Segment Port
- E. Group

Answer: CE

Explanation:

* C. Segment. This is correct. A segment is a logical construct that represents a layer 2 broadcast domain and a layer 3 subnet in NSX. A segment can be used to group and connect virtual machines, containers, or bare metal hosts that belong to the same application or service. A segment can also be used as the scope of a distributed firewall rule, which means that the rule will apply to all the traffic that enters or exits the segment¹²

* E. Group. This is correct. A group is a logical construct that represents a collection of objects in NSX, such as segments, segment ports, virtual machines, IP addresses, MAC addresses, tags, or security policies. A group can be used to define dynamic membership criteria based on various attributes or filters. A group can also be used as the scope of a distributed firewall rule, which means that the rule will apply to all the traffic that matches the group membership criteria³²

NEW QUESTION 2

An NSX administrator is troubleshooting a connectivity issue with virtual machines running on an ESXi transport node. Which feature in the NSX UI shows the mapping between the virtual NIC and the host's physical adapter?

- A. Port Mirroring
- B. Switch Visualization
- C. Activity Monitoring
- D. IPFIX

Answer: B

Explanation:

According to the VMware NSX Documentation, Switch Visualization is a feature in the NSX UI that shows the mapping between the virtual NIC and the host's physical adapter for virtual machines running on an ESXi transport node. You can use Switch Visualization to view details such as port ID, MAC address, VLAN ID, IP address, MTU, port state, port speed, port type, and port group for each virtual NIC and physical adapter. <https://docs.vmware.com/en/VMware-NSX/4.1/installation/GUID-55E5C735-18AD-43F8-9BE5-F75D5B8C6E>

NEW QUESTION 3

Which two choices are solutions offered by the VMware NSX portfolio? (Choose two.)

- A. VMware Tanzu Kubernetes Grid
- B. VMware Tanzu Kubernetes Cluster
- C. VMware NSX Advanced Load Balancer
- D. VMware NSX Distributed IDS/IPS
- E. VMware Aria Automation

Answer: CD

Explanation:

VMware NSX is a portfolio of networking and security solutions that enables consistent policy, operations, and automation across multiple cloud environments¹ The VMware NSX portfolio includes the following solutions:

- VMware NSX Data Center: A platform for data center network virtualization and security that delivers a complete L2-L7 networking stack and overlay services for any workload¹
- VMware NSX Cloud: A service that extends consistent networking and security to public clouds such as AWS and Azure¹
- VMware NSX Advanced Load Balancer: A solution that provides load balancing, web application firewall, analytics, and monitoring for applications across any cloud¹²
- VMware NSX Distributed IDS/IPS: A feature that provides distributed intrusion detection and prevention for workloads across any cloud¹²
- VMware NSX Intelligence: A service that provides planning, observability, and intelligence for network and micro-segmentation¹
- VMware NSX Federation: A capability that enables multi-site networking and security management with consistent policy and operational state synchronization¹
- VMware NSX Service Mesh: A service that connects, secures, and monitors microservices across multiple clusters and clouds¹
- VMware NSX for Horizon: A solution that delivers secure desktops and applications across any device, location, or network¹
- VMware NSX for vSphere: A solution that provides network agility and security for vSphere environments with a built-in console in vCenter¹
- VMware NSX-T Data Center: A platform for cloud-native applications that supports containers, Kubernetes, bare metal hosts, and multi-hypervisor environments¹

VMware Tanzu Kubernetes Grid and VMware Tanzu Kubernetes Cluster are not part of the VMware NSX portfolio. They are solutions for running Kubernetes clusters on any cloud³

VMware Aria Automation is not a real product name. It is a fictional name that does not exist in the VMware portfolio.

<https://blogs.vmware.com/networkvirtualization/2020/01/nsx-hero.html/>

NEW QUESTION 4

What are the four types of role-based access control (RBAC) permissions? (Choose four.)

- A. Read
- B. None

- C. Auditor
- D. Full access
- E. Enterprise Admin
- F. Execute
- G. Network Admin

Answer: ABDF

Explanation:

The four types of role-based access control (RBAC) permissions are Read, None, Full access, and Execute. Read permission allows the user to view the configuration and status of the system. None permission denies any access to the system. Full access permission grants all permissions including Create, Read, Update, and Delete (CRUD). Execute permission includes Read and Update permissions. Auditor, Enterprise Admin, and Network Admin are not types of permissions, but types of roles that have different sets of permissions. References: NSX Features

There are four types of permissions. Included in the list are the abbreviations for the permissions that are used in the Roles and Permissions and Roles and Permissions for Manager Mode tables.

- Full access (FA) - All permissions including Create, Read, Update, and Delete
- Execute (E) - Includes Read and Update
- Read (R)
- None

NSX-T Data Center has the following built-in roles. Role names in the UI can be different in the API.

In NSX-T Data Center, if you have permission, you can clone an existing role, add a new role, edit newly created roles, or delete newly created roles.

Role-Based Access Control (vmware.com)

NEW QUESTION 5

Which two statements are true for IPSec VPN? (Choose two.)

- A. VPNs can be configured on the command line Interface on the NSX manager.
- B. IPSec VPN services can be configured at Tier-0 and Tier-1 gateways.
- C. IPSec VPNs use the DPDK accelerated performance library.
- D. Dynamic routing is supported for any IPSec mode in NSX.

Answer: BC

Explanation:

According to the VMware NSX 4.x Professional documents and tutorials, IPSec VPN secures traffic flowing between two networks connected over a public network through IPSec gateways called endpoints. NSX Edge supports a policy-based or a route-based IPSec VPN. Beginning with NSX-T Data Center 2.5, IPSec VPN services are supported on both Tier-0 and Tier-1 gateways. NSX Edge also leverages the DPDK accelerated performance library to optimize the performance of IPSec VPN.

NEW QUESTION 6

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 list of allowed or blocked URLs based on categories, reputation, or custom entries. The user can then apply the L7 access profile to a firewall rule to control the traffic based on the URL filtering criteria. 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 rule. The Destination field specifies the destination IP address or group of the firewall rule. 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 traffic. References: Gateway Firewall

NEW QUESTION 7

Which TraceFlow traffic type should an NSX administrator use for validating connectivity between App and DB virtual machines that reside on different segments?

- A. Multicast
- B. Unicast
- C. Anycast
- D. Broadcast

Answer: B

Explanation:

Unicast is the traffic type that an NSX administrator should use for validating connectivity between App and DB virtual machines that reside on different segments. According to the VMware documentation, unicast traffic is the traffic type that is used to send a packet from one source to one destination. Unicast traffic is the most common type of traffic in a network, and it is used for applications such as web browsing, email, file transfer, and so on. To perform a traceflow with unicast traffic, the NSX administrator needs to specify the source and destination IP addresses, and optionally the protocol and related parameters. The traceflow will show the path of the packet across the network and any observations or errors along the way. The other options are incorrect because they are not suitable for validating connectivity between two specific virtual machines. Multicast traffic is the traffic type that is used to send a packet from one source to multiple destinations simultaneously. Multicast traffic is used for applications such as video streaming, online gaming and group communication. To perform a traceflow with multicast traffic, the NSX administrator needs to specify the source IP address and the destination multicast IP address. Broadcast traffic is the traffic type that is used to send a packet from one source to all devices on the same subnet. Broadcast traffic is used for applications such as ARP, DHCP, and network

discovery. To perform a traceflow with broadcast traffic, the NSX administrator needs to specify the source IP address and the destination MAC address as FF:FF:FF:FF:FF:FF1. Anycast traffic is not a valid option, as it is not supported by NSX Traceflow. Anycast traffic is a traffic type that is used to send a packet from one source to the nearest or best destination among a group of devices that share the same IP address. Anycast traffic is used for applications such as DNS, CDN, and load balancing.

NEW QUESTION 8

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. RADIUS 2.0
- B. Keycloak Enterprise
- C. RSA SecurID
- D. LDAP and OpenLDAP based on Active Directory (AD)
- E. SecureDAP

Answer: CD

Explanation:

NSX supports two types of authentication, authorization, and accounting (AAA) systems when integrating with VMware Identity Manager: RSA SecurID and LDAP and OpenLDAP based on Active Directory (AD). RSA SecurID is a two-factor authentication system that uses a token-based approach to verify the identity of users. LDAP and OpenLDAP based on AD are directory services that store and manage user information and credentials. Both systems can be used to provide centralized authentication for users who want to access applications in an NSX environment.

<https://blogs.vmware.com/networkvirtualization/2017/11/remote-user-authentication-and-rbac-with-nsx-t.html>

NEW QUESTION 9

Which two of the following features are supported for the Standard NSX Application Platform Deployment? (Choose two.)

- A. NSX Intrusion Detection and Prevention
- B. NSX Intelligence
- C. NSX Network Detection and Response
- D. NSX Malware Prevention Metrics
- E. NSX Intrinsic Security

Answer: CD

Explanation:

The NSX Application Platform Deployment features are divided into three form factors: Evaluation, Standard, and Advanced. Each form factor determines which NSX features can be activated or installed on the platform¹. The Evaluation form factor supports only NSX Intelligence, which provides network visibility and analytics for NSX-T environments². The Standard form factor supports both NSX Intelligence and NSX Network Detection and Response, which provides network threat detection and response capabilities for NSX-T environments³. The Advanced form factor supports all four features: NSX Intelligence, NSX Network Detection and Response, NSX Malware Prevention, and NSX Metrics¹.

<https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/nsx-application-platform/GUID-85CD2728-8081>

NEW QUESTION 10

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

Answer: BC

Explanation:

ECMP (Equal Cost Multi-Path) is a routing protocol that increases the north and south communication bandwidth by adding an uplink to the tier-0 logical router and configure it for each Edge node in an NSX Edge cluster². The ECMP routing paths are used to load balance traffic and provide fault tolerance for failed paths². The tier-0 logical router must be in active-active mode for ECMP to be available². A maximum of eight ECMP paths are supported². Configuring ECMP on the tier-0 gateway can address low throughput and congestion by distributing the traffic among multiple paths and avoiding bottlenecks.

Deploying Large size Edge node/s can also address low throughput and congestion by providing more resources (memory, CPU, disk) for the Edge node to handle the network traffic. The NSX Edge VM system requirements vary depending on the appliance size, which affects the bandwidth, NAT/firewall, load balancer, and VPN capabilities of the Edge node¹. A Large size Edge node has 32 GB memory, 8 vCPU, 200 GB disk space, and can support 2-10 Gbps bandwidth, L2-L4 features, and L7 load balancer¹. An Extra Large size Edge node has 64 GB memory, 16 vCPU, 200 GB disk space, and can support more than 10 Gbps bandwidth, L2-L4 features, L7 load balancer, and VPN¹. Deploying a larger size Edge node can improve the performance and capacity of the tier-0 gateway.

References: 2: Understanding ECMP Routing - VMware Docs(<https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-443B6B0D-F179-42NSX-Edge-VM-System-Requirements-VMware>)

Docs(<https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/installation/GUID-22F87CA8-01A9-4F2E>)

NEW QUESTION 10

Which two statements are true about IDS Signatures? (Choose two.)

- A. Users can upload their own IDS signature definitions.
- B. An IDS signature contains data used to identify known exploits and vulnerabilities.
- C. An IDS signature contains data used to identify the creator of known exploits and vulnerabilities.
- D. IDS signatures can be High Risk, Suspicious, Low Risk and Trustworthy.
- E. An IDS signature contains a set of instructions that determine which traffic is analyzed.

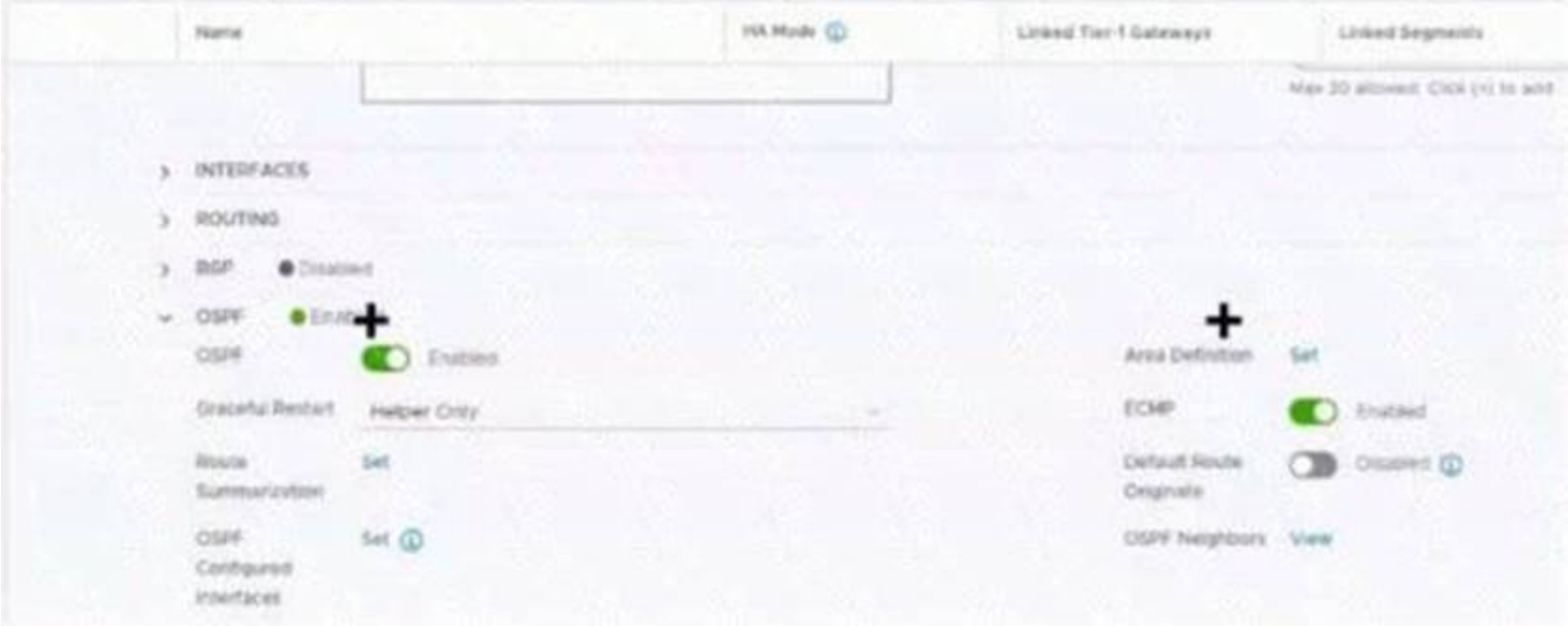
Answer: BE

Explanation:

According to the Network Bachelor article¹, an IDS signature contains data used to identify an attacker’s attempt to exploit a known vulnerability in both the operating system and applications. This implies that statement B is true. According to the VMware NSX Documentation², IDS/IPS Profiles are used to group signatures, which can then be applied to select applications and traffic. This implies that statement E is true. Statement A is false because users cannot upload their own IDS signature definitions, they have to use the ones provided by VMware or Trustwave³. Statement C is false because an IDS signature does not contain data used to identify the creator of known exploits and vulnerabilities, only the exploits and vulnerabilities themselves. Statement D is false because IDS signatures are classified into one of the following severity categories: Critical, High, Medium, Low, or Informational¹.

NEW QUESTION 15

Refer to the exhibit.
 Which two items must be configured to enable OSPF for the Tier-0 Gateway in the Image? Mark your answers by clicking twice on the image.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The correct answer is to enable the OSPF toggle and to add an Area Definition for the Tier-0 gateway in image. These two items are required to configure OSPF on the Tier-0 gateway, as explained in the web search results¹²³.
 To mark your answers by clicking twice on the image, you can double-click on the toggle switch next to OSPF to turn it on. The switch should change from gray to blue, indicating that the option is enabled. The you can double-click on the Set button next to Area Definition to add an area definition. A pop-up windo should appear where you can specify the area ID and type.
 * 1. Click the OSPF toggle to enable OSPF 2. In the Area Definition field, click Set to add an area definition <https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-5BEC626C-5312-467D-B>

NEW QUESTION 17

Which three DHCP Services are supported by NSX? (Choose three.)

- A. Gateway DHCP
- B. Port DHCP per VNF
- C. Segment DHCP
- D. VRF DHCP Server
- E. DHCP Relay

Answer: ACE

Explanation:

According to the VMware NSX Documentation¹, NSX-T Data Center supports the following types of DHCP configuration on a segment:

- Local DHCP server: This option creates a local DHCP server that has an IP address on the segment and provides dynamic IP assignment service only to the VMs that are attached to the segment.
- Gateway DHCP server: This option is attached to a tier-0 or tier-1 gateway and provides DHCP service to the networks (overlay segments) that are directly connected to the gateway and configured to use a gateway DHCP server.
- DHCP Relay: This option relays the DHCP client requests to the external DHCP servers that can be in any subnet, outside the SDDC, or in the physical network.

NEW QUESTION 21

A security administrator needs to configure a firewall rule based on the domain name of a specific application. Which field in a distributed firewall rule does the administrator configure?

- A. Profile
- B. Service
- C. Policy
- D. Source

Answer: A

Explanation:

To configure a firewall rule based on the domain name of a specific application, the administrator needs to use the Profile field in a distributed firewall rule. The Profile field allows the administrator to select a context profile that contains one or more attributes for filtering traffic. One of the attributes that can be used is Domain (FQDN) Name, which specifies the fully qualified domain name of the application. For example, if the administrator wants to filter traffic to *.office365.com, they can create a context profile with the Domain (FQDN) Name attribute set to *.office365.com and use it in the Profile field of the firewall rule.

References:

- Filtering Specific Domains (FQDN/URLs)
- FQDN Filtering

NEW QUESTION 23

Which is an advantages of a L2 VPN In an NSX 4.x environment?

- A. Enables Multi-Cloud solutions
- B. Achieve better performance
- C. Enables VM mobility with re-IP
- D. Use the same broadcast domain

Answer: D

Explanation:

L2 VPN is a feature of NSX that allows extending Layer 2 networks across different sites or clouds over an IPsec tunnel. L2 VPN has an advantage of enabling VM mobility with re-IP, which means that VMs can be moved from one site to another without changing their IP addresses or network configurations. This is possible because L2 VPN allows both sites to use the same broadcast domain, which means that they share the same subnet and VLAN .

NEW QUESTION 27

Where does an administrator configure the VLANs used In VRF Lite? (Choose two.)

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

Answer: BD

Explanation:

According to the VMware NSX Documentation, these are the two places where you need to configure the VLANs used in VRF Lite:

- Uplink trunk segment: This is a segment that connects a tier-0 gateway to a physical network using multiple VLAN tags. You need to configure the VLAN IDs for each VRF on this segment.
- Uplink interface of the VRF gateway: This is an interface that connects a VRF gateway to an uplink trunk segment using a specific VLAN tag. You need to configure the VLAN ID for each VRF on this interface.

NEW QUESTION 29

An NSX administrator Is treating a NAT rule on a Tler-0 Gateway configured In active-standby high availability mode. Which two NAT rule types are supported for this configuration? (Choose two.)

- A. Reflexive NAT
- B. Destination NAT
- C. 1:1 NAT
- D. Port NAT
- E. Source NAT

Answer: BE

Explanation:

According to the VMware NSX Documentation, these are two NAT rule types that are supported for a tier-0 gateway configured in active-standby high availability mode. NAT stands for Network Address Translation and is a feature that allows you to modify the source or destination IP address of a packet as it passes through a gateway.

- Destination NAT: This rule type allows you to change the destination IP address of a packet from an external IP address to an internal IP address. You can use this rule type to provide access to your internal servers from external networks using public IP addresses.
- Source NAT: This rule type allows you to change the source IP address of a packet from an internal IP address to an external IP address. You can use this rule type to provide access to external networks from your internal servers using public IP addresses.

NEW QUESTION 30

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-9175-5514750E9>

NEW QUESTION 33

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

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

Answer: C

Explanation:

According to the VMware Knowledge Base, this CLI command is used for packet capture on the ESXi node. pktcap-uw stands for Packet Capture User World and is a tool that allows you to capture packets from various points in the network stack of an ESXi host. You can use this tool to troubleshoot network issues or analyze traffic flows.

The other options are either incorrect or not available for this task. tcpdump is not a valid CLI command for packet capture on the ESXi node, as it is a tool that runs on Linux systems, not on ESXi hosts. debug is not a valid CLI command for packet capture on the ESXi node, as it is a generic term that describes the process of finding and fixing errors, not a specific tool or command. set capture is not a valid CLI command for packet capture on the ESXi node, as it does not exist in the ESXi CLI.

NEW QUESTION 34

Which choice is a valid insertion point for North-South network introspection?

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

Answer: C

Explanation:

A valid insertion point for North-South network introspection is Tier-0 gateway. North-South network introspection is a service insertion feature that allows third-party network services to be integrated with

NSX. North-South network introspection enables traffic redirection from the uplink of an NSX Edge node to a service chain that consists of one or more service profiles¹. The Tier-0 gateway is the logical router that connects the NSX Edge node to the physical network and provides North-South routing and network services².

<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-D5933474-34A2-4DCE-AE9B-A82FF33>

NEW QUESTION 38

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

- A. SR is instantiated and automatically connected with DR.
- B. DR is instantiated and automatically connected with SR.
- C. SR and DR are instantiated but require manual connection.
- D. SR and DR doesn't need to be connected to provide any stateful services.

Answer: A

Explanation:

The answer is A. SR is instantiated and automatically connected with DR.

SR stands for Service Router and DR stands for Distributed Router. They are components of the NSX Edge node that provide different functions¹

The SR is responsible for providing stateful services such as NAT, firewall, load balancing, VPN, and DHCP. The DR is responsible for providing distributed routing and switching between logical segments and the physical network¹

When a stateful service is enabled for the first time on a Tier-0 Gateway, the NSX Edge node automatically creates an SR instance and connects it with the existing DR instance. This allows the stateful service to be applied to the traffic that passes through the SR before reaching the DR²

According to the VMware NSX 4.x Professional Exam Guide, understanding the SR and DR components and their functions is one of the exam objectives³

To learn more about the SR and DR components and how they work on the NSX Edge node, you can refer to the following resources:

- VMware NSX Documentation: NSX Edge Components ¹
- VMware NSX 4.x Professional: NSX Edge Architecture
- VMware NSX 4.x Professional: NSX Edge Routing

NEW QUESTION 40

What are two functions of the Service Engines in NSX Advanced Load Balancer? (Choose two.)

- A. It collects real-time analytics from application traffic flows.
- B. It stores the configuration and policies related to load-balancing services.
- C. It performs application load-balancing operations.
- D. It deploys web servers to perform load-balancing operations.
- E. It provides a user interface to perform configuration and management tasks.

Answer: CE

Explanation:

The Service Engines in NSX Advanced Load Balancer are VM-based applications that handle all data plane operations by receiving and executing instructions from the Controller. The Service Engines perform the following functions:

- They perform application load-balancing operations for all client- and server-facing network interactions. They support various load-balancing algorithms, health monitors, SSL termination, and persistence profiles.
 - They provide a user interface to perform configuration and management tasks. The user interface is accessible through a web browser or a REST API. The user interface allows the user to create and modify virtual services, pools, health monitors, policies, analytics, and other load-balancing settings
- <https://docs.vmware.com/en/VMware-Telco-Cloud-Platform/3.0/vmware-telco-cloud-reference-architecture-gui>

NEW QUESTION 42

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

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

Answer: AB

Explanation:

Network Introspection is a service insertion feature that allows third-party network security services to monitor and analyze the traffic between virtual machines. Network Introspection can be configured on the host pNIC or on the partner SVM, depending on the type of service and the deployment model. The host pNIC configuration is used for services that require traffic redirection from the physical network to the service virtual machine. The partner SVM configuration is used for services that require traffic redirection from the virtual network to the service virtual machine. Network Introspection cannot be configured on the Tier-0 or Tier-1 gateways, as they are not part of the data plane where the service insertion occurs. Network Introspection also cannot be configured on the edge node, as it is a logical construct that hosts the Tier-0 and Tier-1 gateways. References: Distributed Service Insertion, NSX Securing “Anywhere” Part IV

NEW QUESTION 46

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

- A. Through the OVF command line tool
- B. Through the vSphere Web Client
- C. Through automated or Interactive mode using an ISO
- D. Through the NSXUI

Answer: D

Explanation:

Through the NSX UI. According to the VMware NSX Documentation², you can deploy NSX Edge nodes as virtual appliances through the NSX UI by clicking Add Edge Node and providing the required information. The other options are either outdated or not applicable for virtual NSX Edge nodes.

<https://docs.vmware.com/en/VMware-NSX/4.1/installation/GUID-E9A01C68-93E7-4140-B306-19CD6806199>

NEW QUESTION 47

NSX improves the security of today's modern workloads by preventing lateral movement, which feature of NSX can be used to achieve this?

- A. Network Segmentation
- B. Virtual Security Zones
- C. Edge Firewalling
- D. Dynamic Routing

Answer: A

Explanation:

According to the web search results, network segmentation is a feature of NSX that improves the security of today's modern workloads by preventing lateral movement. Lateral movement is a technique used by attackers to move from one compromised system to another within a network, exploiting vulnerabilities or credentials. Network segmentation prevents lateral movement by dividing a network into smaller segments or zones, each with its own security policies and controls. This way, if one segment is compromised, the attacker cannot access other segments or resources. NSX enables network segmentation by using micro-segmentation, which applies granular firewall rules at the virtual machine level, regardless of the physical network topology.

NEW QUESTION 49

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

Answer: BD

Explanation:

To check the IP address of the VMkernel port for the Geneve protocol on the ESXi transport node, an NSX administrator can use the following commands:

- esxcli network ip interface ipv4 get: This command displays the IPv4 configuration of all VMkernel interfaces on the host, including their IP addresses, netmasks, and gateways. The Geneve protocol uses a VMkernel interface named geneve0 by default¹

➤ esxcfg-vmknic -l: This command lists all VMkernel interfaces on the host, along with their MAC addresses, MTU, and netstack. The Geneve protocol uses a netstack named nsx-overlay by default

NEW QUESTION 52

Which CLI command shows syslog on NSX Manager?

- A. get log-file auth.lag
- B. /var/log/syslog/syslog.log
- C. show log manager follow
- D. get log-file syslog

Answer: D

Explanation:

According to the VMware NSX CLI Reference Guide, this CLI command shows the syslog messages on the NSX Manager node. You can use this command to view the system logs for troubleshooting or monitoring purposes.

The other options are either incorrect or not available for this task. get log-file auth.log is a CLI command that shows the authentication logs on the NSX Manager node, not the syslog messages. /var/log/syslog/syslog.log is not a CLI command, but a file path that may contain syslog messages on some Linux systems, but not on the NSX Manager node. show log manager follow is not a valid CLI command, as there is no show log command or manager option in the NSX CLI.

NSX Cli command get log-file <filename>

get log-file <filename> follow

Below are commonly used log files, there are many more log files

get log-file <auth.log | controller | controller-error | http.log | kern.log | manager.log | node-mgmt.log | policy.log | syslog> [follow]

use [follow] to continuing monitor Example: get log-file syslog follow get log-file syslog

NEW QUESTION 54

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 1234`
- C)
`esxcli network ip connection list | grep ccpd`
- D)
`esxcli network ip connection list | grep 1235`

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

Explanation:

According to the web search results, the command that is used to verify the Local Control Plane (LCP) connectivity with Central Control Plane (CCP) on ESXi is get control-cluster status. This command displays the status of the LCP and CCP components on the ESXi host, such as the LCP agent, CCP client, CCP server, and CCP connection. It also shows the IP address and port number of the CCP server that the LCP agent is connected to. If the LCP agent or CCP client are not running or not connected, it means that there is a problem with the LCP connectivity .

NEW QUESTION 56

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

- A. VNI ID
- B. Segment ID
- C. Geneve ID
- D. VIAN ID

Answer: A

Explanation:

According to the VMware NSX Documentation¹, a segment is mapped to a unique Geneve segment that is distributed across the ESXi hosts in a transport zone. The Geneve segment uses a virtual network identifier (VNI) as an overlay network identifier. The VNI ID can be used to identify overlay segments in an NSX environment if troubleshooting is required.

NEW QUESTION 60

Which command is used to set the NSX Manager's logging-level to debug mode for troubleshooting?

- A. Set service manager log-level debug
- B. Set service manager logging-level debug
- C. Set service nsx-manager log-level debug
- D. Set service nsx-manager logging-level debug

Answer: B

Explanation:

According to the VMware Knowledge Base article ¹, the CLI command to set the log level of the NSX Manager to debug mode is set service manager logging-level debug. This command can be used when the NSX UI is inaccessible or when troubleshooting issues with the NSX Manager¹. The other commands are incorrect

because they either use a wrong syntax or a wrong service name. The NSX Manager service name is manager, not nsx-manager2. The log level parameter is logging-level, not log-level3.
<https://kb.vmware.com/s/article/55868>

NEW QUESTION 61

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

Answer: A

Explanation:

According to the VMware NSX Documentation, a non-preemptive failover policy means that the original failed node will not become the active node upon recovery, unless the current active node fails again. This policy can help avoid unnecessary failovers and ensure stability.

The other options are either incorrect or not available for this configuration. Preemptive is the opposite of non-preemptive, meaning that the original failed node will become the active node upon recovery, if it has a higher priority than the current active node. Enable Preemptive and Disable Preemptive are not valid options for the failover policy, as the failover policy is a drop-down menu that only has two choices: Preemptive and Non-Preemptive.

NEW QUESTION 66

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

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

Answer: C

Explanation:

The log for a firewall rule on an ESXi transport node is stored in the /var/log/dfwptlogs.log file. This file contains information about the packets that match or do not match the firewall rules, such as the source and destination IP addresses, ports, protocols, actions, and rule IDs. The log file can be viewed using the esxcli network firewall get command or the vSphere Client.

<https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-D57429A1-A0A9-42BE-A>

NEW QUESTION 68

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

- A. NAT64 is stateless and requires gateways to be deployed in active-standby mode.
- B. NAT64 is supported on Tier-1 gateways only.
- C. NAT64 is supported on Tier-0 and Tier-1 gateways.
- D. NAT64 requires the Tier-1 gateway to be configured in active-standby mode.
- E. NAT64 requires the Tier-1 gateway to be configured in active-active mode.

Answer: CD

Explanation:

<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-69604E49-BC8B-4777-BFD8-B98F8D1F>

NEW QUESTION 69

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

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

Answer: AD

Explanation:

L2 VPN clients are supported by NSX for vSphere Edge and NSX Edge. NSX for vSphere Edge is a virtual appliance that provides network services such as routing, firewalling, load balancing, VPN, and NAT for NSX Data Center for vSphere environments. NSX Edge is a virtual appliance that provides network services such as routing, firewalling, load balancing, VPN, and NAT for NSX-T Data Center environments. Both NSX for vSphere Edge and NSX Edge can act as L2 VPN clients to extend layer 2 networks across multiple sites using L2 VPN service over SSL or IPSec tunnels

NEW QUESTION 74

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 Transport Node Profile
- B. Use the CU on each Edge Node
- C. Use a Node Profile
- D. Use a PowerCU script

Answer: C

Explanation:

A node profile is a configuration template that can be applied to multiple NSX Edge nodes or transport nodes at once. A node profile can include settings such as NTP server, DNS server, syslog server, and so on¹. By using a node profile, an administrator can efficiently configure or update the network settings of multiple NSX Edge nodes or transport nodes in a single operation². The other options are incorrect because they are either not efficient or not supported. Using the CLI on each Edge node would require manual and repetitive commands for each node, which is not efficient. Using a Transport Node Profile would not work, because a Transport Node Profile is used to configure the NSX-T Data Center components on a transport node, such as the transport zone, the N-VDS, and the uplink profiles³. Using a PowerCLI script might work, but it would require writing and testing a custom script, which is not as efficient as using a built-in feature like a node profile.

<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-B4AE1432-690E-480E-91C4-903C1E549>

NEW QUESTION 78

What needs to be configured on a Tier-0 Gateway to make NSX Edge Services available to a VM on a VLAN-backed logical switch?

- A. Downlink Interface
- B. VLAN Uplink
- C. Loopback Router Port
- D. Service Interface

Answer: B

Explanation:

To make NSX Edge Services available to a VM on a VLAN-backed logical switch, you need to configure a VLAN Uplink on the Tier-0 Gateway. A VLAN Uplink is a logical interface that connects the Tier-0 Gateway to the physical network and provides external connectivity for the NSX Edge Services¹. A VLAN Uplink can be configured on the NSX Manager UI by selecting Networking > Tier-0 Gateways > Interfaces > Set > Add Interface¹.

<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-D641380B-4C8E-4C8A-AF64-4261A266>

NEW QUESTION 82

Which VPN type must be configured before enabling a L2VPN?

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

Answer: A

Explanation:

According to the VMware NSX Documentation, this VPN type must be configured before enabling a L2VPN. L2VPN stands for Layer 2 VPN and is a feature that allows you to extend your layer 2 network across different sites using an IPsec tunnel. Route-based IPsec VPN is a VPN type that uses logical router ports to establish IPsec tunnels between sites.

<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-86C8D6BB-F185-46DC-828C-1E1876B8>

NEW QUESTION 85

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

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

Answer: DEF

Explanation:

According to the VMware NSX 4.x Professional documents and tutorials, an NSX Manager is a standalone appliance that hosts the API services, the management plane, control plane, and policy management. The NSX Manager has three built-in roles: policy, manager, and controller². The policy role handles the declarative configuration of the system and translates it into desired state for the manager role. The manager role receives and validates the configuration from the policy role and stores it in a distributed persistent database. The manager role also publishes the configuration to the central control plane. The controller role implements the central control plane that computes the network state based on the configuration and topology information³. The other roles (master, cloud, and zookeeper) are not valid NSX Manager roles.

NEW QUESTION 86

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

- A. SFRVICE_ROUTER_TJERO
- B. TIERO_DISTRI BUTE D_ ROUTER
- C. DISTRIBUTED_ROUTER_TIER1
- D. DISTRIBUTED_ROUTER_TIER0
- E. SERVICE_ROUTER_TIERI

Answer: CD

Explanation:

<https://docs.vmware.com/en/VMware-Validated-Design/5.0.1/com.vmware.vvd.sddc-nsxt-design.doc/GUID-74>

NEW QUESTION 90

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

- A. VMware Aria Automation
- B. VMware Aria Orchestrator
- C. VMware Site Recovery Manager
- D. VMware Aria Operations Networks

Answer: D

Explanation:

According to the web search results, VMware Aria Operations Networks (formerly vRealize Network Insight) is a network monitoring tool that can help monitor, discover and analyze networks and applications across clouds¹. It can also provide enhanced troubleshooting and visibility for physical and virtual networks². The other options are either incorrect or not relevant for identifying problems in a physical network. VMware Aria Automation is a cloud automation platform that can help automate the delivery of IT services. VMware Aria Orchestrator is a cloud orchestration tool that can help automate workflows and integrate with other systems. VMware Site Recovery Manager is a disaster recovery solution that can help protect and recover virtual machines from site failures.

NEW QUESTION 95

Which CLI command would an administrator use to allow syslog on an ESXi transport node when using the esxcli utility?

- A. esxcli network firewall ruleset set -r syslog -e true
- B. esxcli network firewall ruleset -e syslog
- C. esxcli network firewall ruleset set -r syslog -e false
- D. esxcli network firewall ruleset set -a -e false

Answer: A

Explanation:

To allow syslog on an ESXi transport node, the administrator needs to use the esxcli utility to enable the syslog ruleset in the ESXi firewall. The correct syntax for this command is esxcli network firewall ruleset set -r syslog -e true, where -r specifies the ruleset name and -e specifies whether to enable or disable it. The options are incorrect because they either use an invalid syntax, such as omitting the ruleset name or using -a instead of -r, or they disable the syslog ruleset instead of enabling it, which is the opposite of what question asks. References: [ESXi Firewall Command-Line Interface], [Configure Syslog on ESXi Hosts]

NEW QUESTION 99

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

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

Answer: ABD

Explanation:

According to the VMware NSX Documentation, these are three of the capabilities of Network Topology, which is a graphical representation of your network infrastructure in NSX:

- Display how the different NSX components are interconnected: You can use Network Topology to view how your segments, gateways, routers, firewalls, load balancers, VPNs, and other NSX components are connected and configured in your network.
- Display the uplink configured on the Tier-0 Gateways: You can use Network Topology to view the uplink interface and segment that connect your tier-0 gateways to your physical network. You can also view the VLAN ID and IP address of the uplink interface.
- Display the VMs connected to Segments: You can use Network Topology to view the VMs that are attached to your segments. You can also view the IP address and MAC address of each VM.

NEW QUESTION 100

How is the RouterLink port created between a Tier-1 Gateway and Tier-0 Gateway?

- A. Manually create a Logical Switch and connect to both Tier-1 and Tier-0 Gateways.
- B. Automatically created when Tier-1 is created.
- C. Manually create a Segment and connect to both Tier-1 and Tier-0 Gateways.
- D. Automatically created when Tier-1 is connected with Tier-0 from NSX UI.

Answer: D

Explanation:

According to the VMware NSX 4.x Professional documents and tutorials, a RouterLink port is a logical port that connects a Tier-1 gateway to a Tier-0 gateway. This port is automatically created when a Tier-1 gateway is associated with a Tier-0 gateway from the NSX UI or API. The RouterLink port enables routing between the two gateways and carries all the routing protocols and traffic. There is no need to manually create a logical switch or segment for this purpose¹.

NEW QUESTION 105

Which of the following exist only on Tier-1 Gateway firewall configurations and not on Tier-0?

- A. Applied To
- B. Actions
- C. Profiles

D. Sources

Answer: A

Explanation:

According to the VMware NSX Documentation, Applied To is a feature that exists only on tier-1 gateway firewall configurations and not on tier-0. Applied To allows you to specify which logical router ports or segments are affected by a firewall rule. This can help reduce the scope and improve the performance of firewall rules. By default, gateway firewall rules are applied to all the available uplinks and service interfaces on a selected gateway. For URL filtering, Applied To can only be Tier-1 gateways.

<https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-DE6FE8CB-017E-41C8-8>

NEW QUESTION 107

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

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

Answer: D

Explanation:

According to the VMware NSX Documentation², the FABRIC message ID (msgld) captures messages related to NSX host preparation events, such as installation, upgrade, or uninstallation of NSX components on ESXi hosts. The syslog export configuration command for NSX host preparation events would look something like this:

set service syslog export FABRIC

The other options are either incorrect or not relevant for NSX host preparation events. MONITORING captures messages related to NSX monitoring features, such as alarms and system events². SYSTEM captures messages related to NSX system events, such as login, logout, or configuration changes². GROUPING captures messages related to NSX grouping objects, such as security groups, security tags, or IP sets².

<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-CC18C0E3-D076-41AA-8B8C-133650FD>

NEW QUESTION 108

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

- A. Controller Files
- B. Management Files
- C. Core Files
- D. Audit Files

Answer: C

Explanation:

According to the VMware NSX Documentation¹, core files and audit logs can contain sensitive information and should be excluded from the support bundle unless requested by VMware technical support. Controller files and management files are not mentioned as containing sensitive information.

NEW QUESTION 111

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

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

Answer: BE

Explanation:

The host switch modes determine how the NSX network and security stack is allocated on the underlying host CPU or DPU. There are two supported host switch modes: Enhanced Datapath and Standard

Datapath¹. Enhanced Datapath mode leverages the DPU to offload the NSX datapath processing from the host CPU, while Standard Datapath mode uses the host CPU for the NSX datapath processing¹. DPDK Datapath, Overlay Datapath, and Secure Datapath are not valid host switch modes for NSX 4.x. References: NSX Features

NEW QUESTION 115

Which steps are required to activate Malware Prevention on the NSX Application Platform?

- A. Select Cloud Region and Deploy Network Detection and Response.
- B. Activate NSX Network Detection and Response and run Pre-checks.
- C. Activate NSX Network Detection and Response and Deploy Malware Prevention.
- D. Select Cloud Region and run Pre-checks.

Answer: D

Explanation:

To activate Malware Prevention on the NSX Application Platform, the steps are:

- In the NSX Manager UI, select System and in the Configuration section, select NSX Application Platform.
- Navigate to the Features section, locate the NSX Malware Prevention feature card, and click Activate or anywhere in the card.

- In the NSX Malware Prevention activation window, select one of the available cloud regions from which you can access the NSX Advanced Threat Prevention cloud service.
- Click Run Prechecks. This precheck process can take some time as the system validates that the minimum license requirement is met and that it is eligible for use with the NSX Advanced Threat Prevention cloud service. The system also validates that the selected cloud region is reachable.
- Click Activate. This step can take some time¹. Therefore, the correct answer is D. The other options are incorrect because they involve activating or deploying NSX Network Detection and Response, which is a different feature from Malware Prevention. References: Activate NSX Malware Prevention

NEW QUESTION 118

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

Answer: AB

Explanation:

esxcfg-nics -l and esxcli network nic list are two CLI commands that can be used to see the vmnic link status on an ESXi host. Both commands display information such as the vmnic name, driver, link state, speed, and duplex mode. The link state can be either Up or Down, indicating whether the vmnic is connected or not. For example, the output of esxcfg-nics -l can look like this:

Name PCI Driver Link Speed Duplex MAC Address MTU Description

vmnic0 0000:02:00.0 igbn Up 1000Mbps Full 00:50:56:01:2a:3b 1500 Intel Corporation I350 Gigabit Network Connection
vmnic1 0000:02:00.1 igbn Down 0Mbps
Half 00:50:56:01:2a:3c 1500 Intel Corporation I350 Gigabit Network Connection

NEW QUESTION 121

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

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

Answer: AE

Explanation:

Two statements that describe the characteristics of an Edge Cluster in NSX are:

- An Edge Cluster can have a maximum of 8 edge nodes². This is the upper limit for scaling out the Edge Cluster and providing high availability and load balancing for network services.
- An Edge Cluster must contain only one type of edge nodes (VM or bare metal)³. This is because different types of edge nodes have different performance and resource requirements, and mixing them in the same cluster can cause inconsistency and instability. The other options are incorrect because they do not describe the characteristics of an Edge Cluster in NSX. An Edge Cluster can have either active-active or active-standby edge nodes, depending on the configuration and services⁴. An Edge Cluster cannot contain multiple types of edge nodes, as explained above. References: Enhanced NSX Edge and Networking Services in NSX 4.0.1.1, NSX Edge Installation Requirements, NSX-T Edge Node Cluster

NEW QUESTION 122

Which three security features are dependent on the NSX Application Platform? (Choose three.)

- A. NSX Intelligence
- B. NSX Firewall
- C. NSX Network Detection and Response
- D. NSX TLS Inspection
- E. NSX Distributed IDS/IPS
- F. NSX Malware Prevention

Answer: ACF

Explanation:

<https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/nsx-application-platform/GUID-42EDE0AD-CD>

NEW QUESTION 123

What are two valid BGP Attributes that can be used to influence the route path traffic will take? (Choose two.)

- A. AS-Path Prepend
- B. BFD
- C. Cost
- D. MED

Answer: AD

Explanation:

- AS-Path Prepend: This attribute allows you to prepend one or more AS numbers to the AS path of a route, making it appear longer and less preferable to other BGP routers. You can use this attribute to manipulate the inbound traffic from your BGP peers by advertising a longer AS path for some routes and a shorter AS path for others .

➤ MED: This attribute stands for Multi-Exit Discriminator and allows you to specify a preference value for a route among multiple exit points from an AS. You can use this attribute to manipulate the outbound traffic to your BGP peers by advertising a lower MED value for some routes and a higher MED value for others .

NEW QUESTION 125

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

2V0-41.23 Practice Exam Features:

- * 2V0-41.23 Questions and Answers Updated Frequently
- * 2V0-41.23 Practice Questions Verified by Expert Senior Certified Staff
- * 2V0-41.23 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 2V0-41.23 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 2V0-41.23 Practice Test Here](#)