



VMware

Exam Questions 2V0-41.23

VMware NSX 4.x Professional

NEW QUESTION 1

An NSX administrator is troubleshooting a connectivity issue with virtual machines running on an FSXi 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

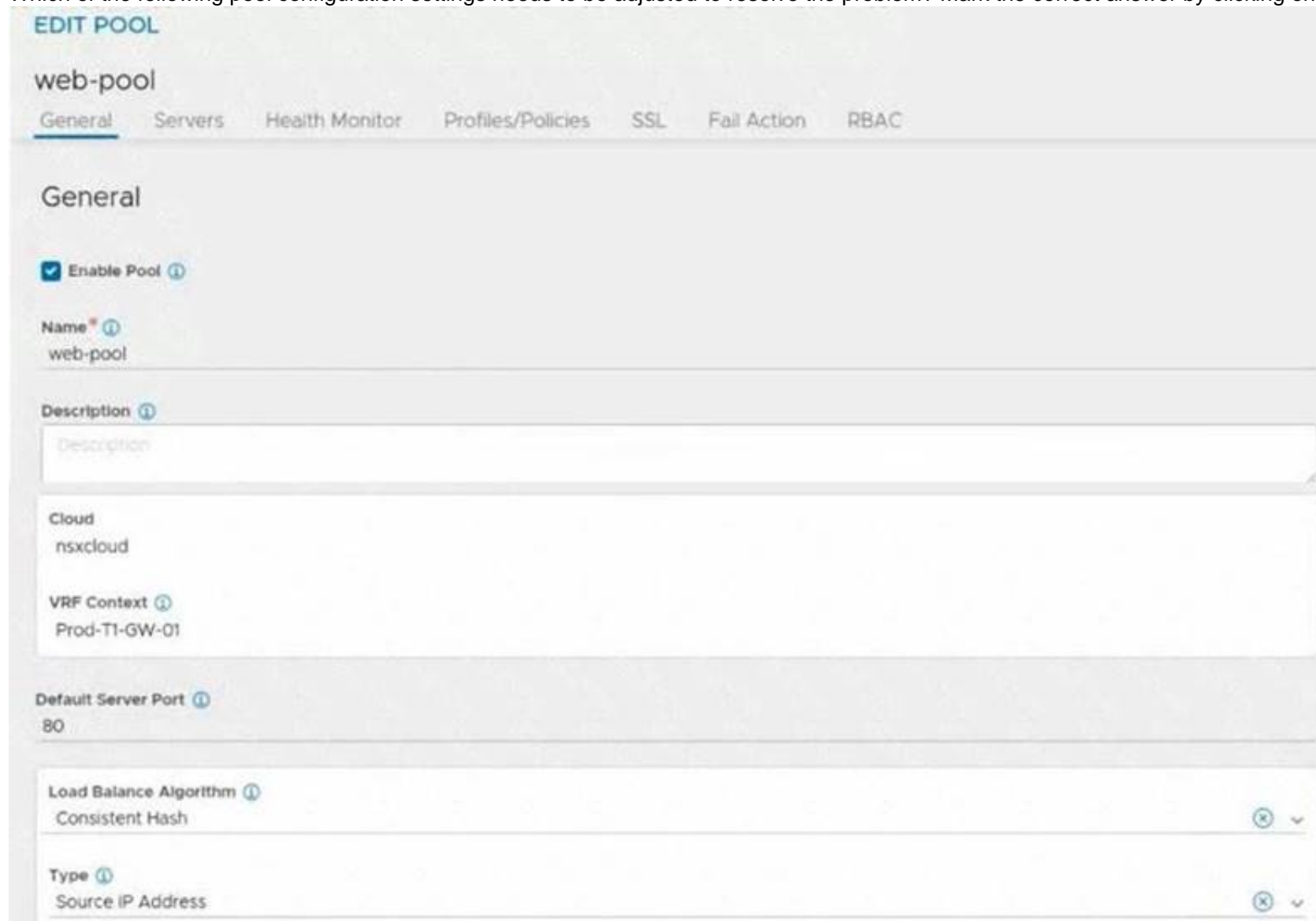
Explanation:

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 2

Refer to the exhibit.

An administrator configured NSX Advanced Load Balancer to redistribute the traffic between the web servers. However, requests are sent to only one server. Which of the following pool configuration settings needs to be adjusted to resolve the problem? Mark the correct answer by clicking on the image.



The screenshot shows the 'EDIT POOL' configuration page for a pool named 'web-pool'. The 'General' tab is selected. The configuration includes:

- Enable Pool:** Checked.
- Name:** web-pool.
- Description:** (Empty text field).
- Cloud:** nsxcloud.
- VRF Context:** Prod-T1-GW-01.
- Default Server Port:** 80.
- Load Balance Algorithm:** Consistent Hash.
- Type:** Source IP Address.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Load Balancing Algorithm

NEW QUESTION 3

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-88>

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 Execu 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 permissions¹. 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 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-B757CAED>

NEW QUESTION 6

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 Tler-0 and Tler-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 gateways¹. NSX Edge also leverages the DPDK accelerated performance library to optimize the performance of IPSec VPN².

NEW QUESTION 7

Which TraceFlow traffic type should an NSX administrator use tor 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 documentation¹, 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 on². 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 parameters¹. The traceflow will show the path of the packet across the network and any observations or errors along the way³. 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 simultaneously². Multicast traffic is used for applications such as video streaming, online gaming and group communication⁴. To perform a traceflow with multicast traffic, the NSX administrator needs to specify the source IP address and the destination multicast IP address¹. Broadcast traffic is the traffic type that is used to send a packet from one source to all devices on the same subnet². 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

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-F179-42](https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-443B6B0D-F179-42NSX-Edge-VM-System-Requirements-VMware) NSX 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 9

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

- A. Route & SSL based VPNs
- B. Route-based VPN
- C. Policy & Route based VPNs
- D. SSL-based VPN

Answer: B

Explanation:

Route-based VPN is a VPN type that uses Virtual Tunnel interfaces (VTI) to establish IPsec tunnels between an NSX Edge node and remote sites². A VTI is a logical interface that is assigned an IP address and is associated with a physical or virtual interface. The VTI acts as an end point of the IPsec tunnel and routes traffic between the NSX Edge node and the remote site². Route & SSL based VPNs, Policy & Route based VPNs, and SSL-based VPN are not VPN types that use VTI. References: Virtual Private Network (VPN)

NEW QUESTION 10

How does the Traceflow tool identify issues in a network?

- A. Compares the management plane configuration states containing control plane traffic and error reporting from transport node agents.
- B. Compares intended network state in the control plane with Tunnel End Point (TEP) keepalives in the data plane.
- 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.

Answer: D

Explanation:

The Traceflow tool identifies issues in a network by injecting synthetic traffic into the data plane and observing the results in the control plane. This allows the tool to identify any issues in the network and provide a detailed report on the problem. You can use the Traceflow tool to test connectivity between any two endpoints in your NSX-T Data Center environment.

NEW QUESTION 10

A company is deploying NSX micro-segmentation in their vSphere environment to secure a simple application composed of web, app, and database tiers. The naming convention will be:

- WKS-WEB-SRV-XXX
- WKY-APP-SRR-XXX
- WKI-DB-SRR-XXX

What is the optimal way to group them to enforce security policies from NSX?

- A. Use Edge as a firewall between tiers.
- B. Do a service insertion to accomplish the task.

- C. Group all by means of tags membership.
- D. Create an Ethernet based security policy.

Answer: C

Explanation:

The answer is C. Group all by means of tags membership.

Tags are metadata that can be applied to physical servers, virtual machines, logical ports, and logical segments in NSX. Tags can be used for dynamic security group membership, which allows for granular and flexible enforcement of security policies based on various criteria¹

In the scenario, the company is deploying NSX micro-segmentation to secure a simple application composed of web, app, and database tiers. The naming convention will be:

- WKS-WEB-SRV-XXX
- WKY-APP-SRR-XXX
- WKI-DB-SRR-XXX

The optimal way to group them to enforce security policies from NSX is to use tags membership. For example, the company can create three tags: Web, App, and DB, and assign them to the corresponding VMs based on their names. Then, the company can create three security groups: Web-SG, App-SG, and DB-SG, and use the tags as the membership criteria. Finally, the company can create and apply security policies to the security groups based on the desired rules and actions² Using tags membership has several advantages over the other options:

- It is more scalable and dynamic than using Edge as a firewall between tiers. Edge firewall is a centralized solution that can create bottlenecks and performance issues when handling large amounts of traffic³
- It is more simple and efficient than doing a service insertion to accomplish the task. Service insertion is a feature that allows for integrating third-party services with NSX, such as antivirus or intrusion prevention systems. Service insertion is not necessary for basic micro-segmentation and can introduce additional complexity and overhead.
- It is more flexible and granular than creating an Ethernet based security policy. Ethernet based security policy is a type of policy that uses MAC addresses as the source or destination criteria. Ethernet based security policy is limited by the scope of layer 2 domains and does not support logical constructs such as segments or groups.

To learn more about tags membership and how to use it for micro-segmentation in NSX, you can refer to the following resources:

- VMware NSX Documentation: Security Tag 1
- VMware NSX Micro-segmentation Day 1: Chapter 4 - Security Policy Design 2
- VMware NSX 4.x Professional: Security Groups
- VMware NSX 4.x Professional: Security Policies

NEW QUESTION 11

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 13

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 18

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

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

Answer: C

Explanation:

The insertion point for East-West network introspection is the Guest VM vNIC. Network introspection is a service insertion feature that allows third-party network services to be integrated with NSX. Network introspection enables traffic redirection from the Guest VM vNIC to a service virtual machine (SVM) that runs the partner service. The SVM can then inspect, monitor, or modify the traffic before sending it back to the original destination¹. The other options are incorrect because they are not the insertion points for East-West network introspection. The Tier-0 router is used for North-South routing and network services. The partner SVM is the service virtual machine that runs the partner service, not the insertion point. The host physical NIC is not involved in network introspection. References: Network Introspection Settings

NEW QUESTION 21

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

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

Answer: B

Explanation:

The MAC table on an ESXi host is used to determine the location of a particular workload for a frame-forwarding decision. The MAC table maps the MAC addresses of the workloads to their corresponding tunnel endpoint (TEP) IP addresses. The TEP IP address identifies the ESXi host where the workload resides. The MAC table is populated by learning the source MAC addresses of the incoming frames from the workloads. The MAC table is also synchronized with other ESXi hosts in the same transport zone by using the NSX Controller.
<https://nsx.techzone.vmware.com/resource/nsx-reference-design-guide>

NEW QUESTION 24

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 29

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 30

Which command is used to test management connectivity from a transport node to NSX Manager?

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

Answer: A

Explanation:

The NSX Manager management plane communicates with the transport nodes by using APH Server over NSX-RPC/TCP through port 1234. CCP communicates with the transport nodes by using APH Server over NSX-RPC/TCP through port 1235.

NEW QUESTION 31

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 (file 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-9931-4719-8F>

NEW QUESTION 36

A customer has a network where BGP has been enabled and the BGP neighbor is configured on the Tier-0 Gateway. An NSX administrator used the get gateways command to retrieve this Information:

```
sa-nxedge-01> get gateways
```

Logical Router					
UUID	VRF	GW-ID	Name	Type	
Ports					
736a80e3-23f6-5a2d-81d6-bbefb2786666	0	0		TUNNEL	3
B10ef54e-d5f3-49e5-99b7-8a51366d0592	1	1025	SR-T1-LR-01	SERVICE_ROUTER_TIER1	8
5a5ddd63-3764-4d28-b92e-ee4c964a0dfd	3	2049	SR-T0-LR-01	SERVICE_ROUTER_TIER0	6
0E0784db-511f-fa72-ae0b-1ccaa0262ad2	4	7	DR-T0-LR-01	DISTRIBUTED_ROUTER_TIER0	4

Which two commands must be executed to check BGP neighbor status? (Choose two.)

- A. vrf 1
- B. vrf 4
- C. sa-nxedge-01(tier1_sr> get bgp neighbor
- D. sa-nxedge-01(tier0_sr> get bgp neighbor
- E. sa-nxedge-01(tier1_dr> get bgp neighbor
- F. vrf 3

Answer: DF

Explanation:

BGP will be configured on the T0 SR. Connect to the VRF for the T0 SR and run get bgp neighbor once connected to it.

<https://docs.vmware.com/en/VMware-Validated-Design/5.1/sddc-deployment-of-vmware-nsx-t-workload-domain>

For the BGP configuration on NSX-T, the Tier-0 Service Router (SR) is typically where BGP is configured. To check the BGP neighbor status:

Connect to the VRF for the T0 SR, which is VRF 3 based on the provided output. Run the command to get BGP neighbor status once connected to it.

NEW QUESTION 39

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

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

Answer: ABD

Explanation:

* A. Can be used as an Exterior Gateway Protocol. This is correct. BGP is a protocol that can be used to exchange routing information between different autonomous systems (AS). An AS is a network or a group of networks under a single administrative control. BGP can be used as an Exterior Gateway Protocol (EGP) to connect an AS to other ASes on the internet or other external networks¹

* B. It supports a 4-byte autonomous system number. This is correct. BGP supports both 2-byte and 4-byte AS numbers. A 2-byte AS number can range from 1 to 65535, while a 4-byte AS number can range from 65536 to 4294967295. NSX supports both 2-byte and 4-byte AS numbers for BGP configuration on a Tier-0 Gateway²

* C. The network is divided into areas that are logical groups. This is incorrect. This statement describes OSPF, not BGP. OSPF is another routing protocol that operates within a single AS and divides the network into areas to reduce routing overhead and improve scalability. BGP does not use the concept of areas, but rather uses attributes, policies, and filters to control the routing decisions and traffic flow³

* D. FIGRP Is disabled by default. This is correct. FIGRP stands for Fast Interior Gateway Routing Protocol, which is an enhanced version of IGRP, an obsolete routing protocol developed by Cisco. FIGRP is not supported by NSX and is disabled by default on a Tier-0 Gateway.

* E. BGP is enabled by default. This is incorrect. BGP is not enabled by default on a Tier-0 Gateway. To enable BGP, you need to configure the local AS number and the BGP neighbors on the Tier-0 Gateway using the NSX Manager UI or API.

To learn more about BGP configuration on a Tier-0 Gateway in NSX, you can refer to the following resources:

- VMware NSX Documentation: Configure BGP 1
- VMware NSX 4.x Professional: BGP Configuration
- VMware NSX 4.x Professional: BGP Troubleshooting

NEW QUESTION 44

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 46

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

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

Answer: BE

Explanation:

According to the VMware NSX Documentation¹, Packet Capture and Traceflow are two built-in VMware tools that can help identify the cause of packet loss on VLAN segments.

Packet Capture allows you to capture packets on a specific interface or segment and analyze them using tools such as Wireshark or tcpdump. Packet Capture can help you diagnose network issues such as misconfigured MTU, incorrect VLAN tags, or firewall drops.

Traceflow allows you to inject synthetic packets into the network and trace their path from source to destination. Traceflow can help you verify connectivity, routing, and firewall rules between virtual machines or segments. Traceflow can also show you where packets are dropped or modified along the way.

NEW QUESTION 50

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 53

Match the NSX Intelligence recommendations with their correct purpose.

Recommendations:	Purposes:
security policy recommendations	Are service objects that were used by applications in the VMs or physical servers that an administrator had specified, but the services are not yet defined in the NSX inventory.
security group recommendations	Are VMs or physical servers whose traffic flows were analyzed for the time period and the boundary an administrator had specified.
service recommendations	Are East-West distributed firewall (DFW) security policies in the application category.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- Security policy recommendations: Are East-West distributed firewall (DFW) security policies in the application category¹².
- Security group recommendations: Are VMs or physical servers whose traffic flows were analyzed for the time period and the boundary you had specified¹².
- Service recommendations: Are service objects that were used by applications in the VMs or physical servers that you had specified, but the services are not yet defined in the NSX inventory¹².

NEW QUESTION 55

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

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

Answer: C

Explanation:

The sequence of commands that could be used to check the BGP connection status between the Tier-O Gateway and the upstream physical router on NSX Edge node is get gateways, vrf <number>, get bgp neighbor. These commands can be executed on the NSX Edge node CLI after logging in as admin⁶. The first command, get gateways, displays the list of logical routers (gateways) configured on the Edge node, along with their IDs and VRF numbers⁷. The second command, vrf <number>, switches to the VRF context of the desired Tier-O Gateway, where <number> is the VRF number obtained from the previous command⁷. The third command, get bgp neighbor, displays the BGP neighbor summary for the selected VRF, including the neighbor IP address, AS number, state, uptime, and prefixes received⁸. The other options are incorrect because they either use invalid or incomplete commands or do not switch to the correct VRF context. References: NSX-T Command-Line Interface Reference, NSX Edge Node CLI Commands, Troubleshooting BGP on NSX-T Edge Nodes

NEW QUESTION 60

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

- A. Reinstalling the NSX VIBs on the ESXi host.
- B. Restarting the NTPservice on the ESXi host.
- C. Changing the lime zone on the ESXi host.
- D. Reconfiguring the ESXI host with a local NTP server.

Answer: B

Explanation:

According to the web search results, error code 1001 is related to a time synchronization issue between the ESXi host and the NSX Manager. This can cause problems when configuring a time-based firewall rule, which requires the ESXi host and the NSX Manager to have the same time zone and NTP server settings . To resolve this error, you need to restart the NTP service on the ESXi host to synchronize the time with the NSX Manager. You can use the following command to restart the NTP service on the ESXi host:

```
/etc/init.d/ntpd restart
```

The other options are not valid solutions for this error. Reinstalling the NSX VIBs on the ESXi host will not fix the time synchronization issue. Changing the time zone on the ESXi host may cause more discrepancies with the NSX Manager. Reconfiguring the ESXi host with a local NTP server may not be compatible with the NSX Manager's NTP server.

NEW QUESTION 61

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 64

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 65

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 66

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 69

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 71

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

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

Answer: ABEG

Explanation:

<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-26C44DE8-1854-4B06-B6DA-A2FD426>

NEW QUESTION 72

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 76

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 77

An NSX administrator is using ping to check connectivity between VM1 running on ESXi1 to VM2 running on ESXi2. The ping tests fails. 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. esxcli network diag ping -I vmk00 -H <destination IP address>
- B. vmkping ++netstack=geneve -d -s 1572 <destination IP address>
- C. esxcli network diag ping -H <destination IP address>
- D. vmkping ++netstack=vxlan -d -s 1572 <destination IP address>

Answer: B

Explanation:

The command vmkping ++netstack=geneve -d -s 1572 <destination IP address> is used to check the VMware kernel ports for tunnel end point communication. This command uses the geneve netstack, which is the default netstack for NSX-T. The -d option sets the DF (Don't Fragment) bit in the IP header, which prevents the packet from being fragmented by intermediate routers. The -s 1572 option sets the packet size to 1572 bytes, which is the maximum payload size for a geneve encapsulated packet with an MTU of 1600 bytes.

The <destination IP address> is the IP address of the remote ESXi host or VM. References: : VMware NS Data Center Installation Guide, page 19. : VMware Knowledge Base: Testing MTU with the vmkping command (1003728). : VMware NSX-T Data Center Administration Guide, page 102.

NEW QUESTION 81

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 83

An administrator needs to download the support bundle for NSX Manager. Where does the administrator download the log bundle from?

- A. System > Utilities > Tools
- B. System > Support Bundle
- C. System > Settings > Support Bundle
- D. System > Settings

Answer: B

Explanation:

According to the VMware NSX Documentation, this is where you can download the support bundle for NSX Manager from the NSX UI:

➤ System > Support Bundle: This option allows you to download a support bundle that contains logs, configuration files, and diagnostic information from your NSX Manager node and cluster. You can use this option to troubleshoot issues or provide information to VMware support.

<https://docs.vmware.com/en/VMware-vSphere/7.0/vmware-vsphere-with-tanzu/GUID-794C691E-B950-4838-9> <https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-73D9AF0D-4000-4EF2-AC66-6572AD1>

NEW QUESTION 88

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

Answer: A

Explanation:

According to the VMware NSX 4.x Professional documents and tutorials, BFD is a failover detection protocol that provides fast and reliable detection of link failures between two routing devices. BFD can be used with ECMP routing to monitor the health of the ECMP paths and trigger a route change in case of a failure¹². BFD is supported by both BGP and OSPF routing protocols in NSX-T3. BFD can also be configured with different timers to achieve different detection times³.

NEW QUESTION 89

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 94

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 95

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

- A. Set cli-timeout
- B. Get auth-policy minimum-password-length
- C. Set hardening- policy
- D. Set auth-policy

Answer: D

Explanation:

According to the VMware NSX Documentation⁴, the set auth-policy command is used to change the authentication policy settings for local users, such as password length, lockout period, and maximum authentication failures. The other commands are either used to view the authentication policy settings (B), change the CLI session timeout (A), or change the hardening policy settings ©.

NEW QUESTION 100

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 102

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

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

Answer: A

Explanation:

The RouterLink port is automatically created when a Tier-1 Gateway is connected with a Tier-0 Gateway from the NSX UI¹. The RouterLink port is a logical interface that is assigned an IP address and is associated with a physical or virtual interface. The RouterLink port acts as an end point of the IPSec tunnel and routes traffic between the Tier-1 Gateway and the Tier-0 Gateway². The other options are incorrect because they involve manual creation of logical switches or segments, which are not required for RouterLink port

creation. References: Configure NSX for Virtual Networking from vSphere Client, Virtual Private Networ (VPN)

NEW QUESTION 104

Which two tools are used for centralized logging in VMware NSX? (Choose two.)

- A. VMware Aria Operations
- B. Syslog Server
- C. VMware Aria Automation
- D. VMware Aria Operations for Logs
- E. VMware Aria Operations for Networks

Answer: BD

Explanation:

Two tools that are used for centralized logging in VMware NSX are Syslog Server and VMware Aria Operations for Logs. Syslog Server is a standard protocol for

sending log messages from various network devices to a centralized server¹. VMware NSX supports syslog for long term retention of logs and all NSX components can send syslog messages to a configured syslog server². VMware Aria Operations for Logs is a VMware product that provides intelligent log analytics for NSX³. It provides monitoring and troubleshooting capabilities and customizable dashboards for network virtualization, flow analysis, and alerts³. The other options are incorrect because they are not tools for centralized logging in VMware NSX. VMware Aria Operations is a VMware product that provides operations management and automation for NSX⁴, but it is not the same as VMware Aria Operations for Logs. VMware Aria Automation is a VMware product that provides automation and orchestration for NSX⁵, but it is not related to logging. VMware Aria Operations for Networks is not a valid product name. References: Syslog, NSX Logging and System Events, VMware vRealize Lo Insight for NSX, VMware vRealize Operations Management Pack for NSX, VMware vRealize Automation

NEW QUESTION 109

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 112

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

Answer: C

Explanation:

An overlay segment is a logical construct that provides Layer 2 connectivity between virtual machines that are attached to it. An overlay segment can span multiple hosts and can be extended across different subnets or locations using Geneve encapsulation³. Therefore, two virtual machines on the same overlay segment belong to the same Layer 2 broadcast domain, which means they can communicate with each other using their MAC addresses without requiring any routing. The other options are incorrect because they involve Layer 3 or higher network boundaries, which require routing or tunneling to connect different segments. References: VMware NSX Documentation

NEW QUESTION 116

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 121

Which CLI command does an NSX administrator run on the NSX Manager to generate support bundle logs if the NSX UI is inaccessible?

- A. set support-bundle file vcpnv.tgz
- B. esxcli system syslog config logger set - -id=nsxmanager
- C. vm-support
- D. get support-bundle file vcpnv.tgz

Answer: D

Explanation:

To generate the support bundle logs on the NSX Manager via API, the NSX administrator needs to use the POST method with the URL https://nsxmgr_ip/api/1.0/appliance-management/techsupportlogs/NSX, where nsxmgr_ip is the IP address of the NSX Manager¹. This will create a tech support bundle file with a name like vcpnv.tgz. To download the generated tech support bundle file via CLI, the NSX administrator needs to use the get support-bundle file vcpnv.tgz command on the NSX Manager¹. The other commands are incorrect because they either do not generate or download the support bundle logs, or they are not related to the NSX Manager.

NEW QUESTION 126

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

Answer: C

Explanation:

The minimum MTU size for the UPLINK profile is 1700 bytes. This is because the UPLINK profile is used to configure the physical NICs that connect to the NSX-T overlay network. The overlay network uses geneve encapsulation, which adds an overhead of 54 bytes to the original packet. Therefore, to support a standard MTU of 1500 bytes for the inner packet, the outer packet must have an MTU of at least 1554 bytes. However, VMware recommends adding an extra buffer of 146 bytes to account for possible additional headers or VLAN tags. Therefore, the minimum MTU size for the UPLINK profile is 1700 bytes (1554 + 146). References: : VMware NSX-T Data Center Installation Guide, page 23. : VMware NSX-T Data Center Administration Guide, page 102. : VMware NSX-T Data Center Installation Guide, page 24.

NEW QUESTION 128

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 129

.....

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](#)