

VMware.2V0-41.23.vSep-2023.by.Tzen.51q

Number: 2V0-41.23

Passing Score: 800.0

Time Limit: 120.0

File Version: 3.0

Exam Code: 2V0-41.23

Exam Name: VMware NSX 4.x Professional

Exam A

QUESTION 1

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

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

Correct Answer: C, E

Section:

Explanation:

According to the VMware NSX Documentation, these are two of the characteristics of NAT64, which is a feature that allows IPv6-only workloads to communicate with IPv4-only servers:

NAT64 requires the Tier-1 gateway to be configured in active-active mode: You need to configure the tier-1 gateway in active-active mode to enable NAT64, as this mode supports stateless NAT operations. NAT64 is not supported on tier-1 gateways in active-standby mode, as this mode supports stateful NAT operations.

NAT64 is supported on Tier-1 gateways only: You can only configure NAT64 on tier-1 gateways, as they provide local services for segments. NAT64 is not supported on tier-0 gateways, as they provide global services for routing and connectivity.

QUESTION 2

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

Correct Answer: B

Section:

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.

QUESTION 3

Which two BGP configuration parameters can be configured in the VRF Lite gateways? (Choose two.)

- A. Graceful Restart
- B. BGP Neighbors
- C. Local AS
- D. Route Distribution
- E. Route Aggregation

Correct Answer: B, D

Section:

Explanation:

According to the VMware NSX Documentation¹, you can configure BGP neighbors for VRF-Lite by specifying the neighbor IP address, remote AS number, source IP address, and route filter. You can also configure route distribution for VRF-Lite by selecting the route redistribution sources and the route map to apply.

QUESTION 4

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

Correct Answer: D

Section:

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.

QUESTION 5

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

Correct Answer: A, D, E

Section:

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.

QUESTION 6

DRAG DROP

Sort the rule processing steps of the Distributed Firewall. Order responses from left to right.

Select and Place:

If the packet matches source, destination, service, profile and applied to fields, apply the action defined.

If the rule table action is allow, create an entry in the connection table and forward the packet.

Packet arrives at dvfilter connection table, if matching entry in the table, process the packet.

If the rule table action is reject or deny, take that action.

If connection table has no match, compare the packet to the rule table.

Correct Answer:

Packet arrives at dvfilter connection table, if matching entry in the table, process the packet.

If connection table has no match, compare the packet to the rule table.

If the packet matches source, destination, service, profile and applied to fields, apply the action defined.

If the rule table action is allow, create an entry in the connection table and forward the packet.

If the rule table action is reject or deny, take that action.

Section:

Explanation:

QUESTION 7

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

Correct Answer: D

Section:

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.

QUESTION 8

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

Correct Answer: A, D

Section:

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 .

QUESTION 9

HOTSPOT

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.

Hot Area:

EDIT POOL

web-pool

GeneralServersHealth MonitorProfiles/PoliciesSSLFail ActionRBAC

General

☒ Enable Pool ⓘ

Name ⓘ
web-pool

Description ⓘ
Description

Cloud
nsxcloud

VRF Context ⓘ
Prod-T1-GW-01

Default Server Port ⓘ
80

Load Balance Algorithm ⓘ
Consistent Hash ⓘ

Type ⓘ
Source IP Address ⓘ

Answer Area:

EDIT POOL

web-pool

General Servers Health Monitor Profiles/Policies SSL Fail Action RBAC

General

☒ Enable Pool ⓘ

Name ⓘ
web-pool

Description ⓘ
Description

Cloud
nsxcloud

VRF Context ⓘ
Prod-T1-GW-01

Default Server Port ⓘ
80

Load Balance Algorithm ⓘ
Consistent Hash ⓘ

Type ⓘ
Source IP Address ⓘ

Section:

Explanation:

QUESTION 10

An administrator has been tasked with Implementing the SSL certificates for the NSX Manager Cluster VIP. Which Is the correct way to implement this change?

A)

SSH as admin into the NSX manager with the cluster VIP IP and run `nsxcli cluster certificate node install <certificate_id>`

B)

SSH as admin into the NSX manager with the cluster VIP IP and run `nsxcli cluster certificate vip install <certificate_id>`

C)

Send an API call to `https://<nsx-mgr>/api/v1/cluster/api-certificate?action=set_cluster_certificates&certificate_id=<certificate_id>`

D)

Send an API call to `https://<nsx-mgr>/api/v1/node/services/http?action=apply_certificates&certificate_id=<certificate_id>`

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

Correct Answer: B

Section:

Explanation:

SSH as admin into the NSX manager with the cluster VIP and run `nsxcli cluster certificate vip install certificate_id=<certificate_id>`

Send an API call to `https://<nsx_mgr_vip>/api/2.0/services/trustmanagement/cluster_certificate/install?cluster_certificate_id=<certificate_id>`

These steps are consistent with the VMware NSX Documentation, which states that you need to install the SSL certificate for the cluster VIP on both the NSX Manager node and the cluster using the `nsxcli` command and the API call respectively.

QUESTION 11

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`

Correct Answer: D

Section:

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.

QUESTION 12

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

- A. segment connected to the Tier-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

Correct Answer: B, D

Section:

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.

QUESTION 13

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.

Correct Answer: A, B, D

Section:

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.

QUESTION 14

Which two are requirements for FQDN Analysis? (Choose two.)

- A. A layer 7 gateway firewall rule must be configured on the Tier-1 gateway uplink.
- B. ESXi control panel requires access to the Internet to download category and reputation definitions.
- C. The NSX Manager requires access to the Internet to download category and reputation definitions.
- D. The NSX Edge nodes require access to the Internet to download category and reputation definitions.
- E. A layer 7 gateway firewall rule must be configured on the Tier-0 gateway uplink.

Correct Answer: C, E

Section:

Explanation:

According to the VMware NSX Documentation, these are two of the requirements for FQDN Analysis, which is a feature that allows you to monitor and control the traffic based on the fully qualified domain names (FQDNs) of the websites that your workloads access:

The NSX Manager requires access to the Internet to download category and reputation definitions: The NSX Manager periodically downloads the latest category and reputation definitions from a cloud service provider and distributes them to the NSX Edge nodes. These definitions are used to classify and score the FQDNs based on their content and risk level.

A layer 7 gateway firewall rule must be configured on the Tier-0 gateway uplink: You need to configure a layer 7 gateway firewall rule on the tier-0 gateway uplink interface that matches the traffic that you want to analyze based on FQDNs. You also need to enable FQDN Analysis on the firewall rule and select the categories and reputations that you want to allow or deny.

QUESTION 15

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

Correct Answer: B

Section:

Explanation:

According to the VMware NSX Documentation, Partner SVM is a valid insertion point for north-south network introspection. Network introspection is a feature that allows you to insert third-party network services into the data path of your traffic. Partner SVM stands for Partner Service Virtual Machine and is a virtual appliance that runs on an NSX Edge node and provides network services from a partner solution.

QUESTION 16

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

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

Correct Answer: C

Section:

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.

QUESTION 17

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

Correct Answer: A

Section:

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.

QUESTION 18

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-vmknics -l
- E. esxcfg-vmsvc/get.network

Correct Answer: A, B

Section:

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

QUESTION 19

Which two of the following will be used for Ingress traffic on the Edge node supporting a Single Tier topology? (Choose two.)

- A. Downlink Interface for the Tier-0 OR
- B. Downlink Interface for the Tier-1 DR
- C. Inter-Tier Interface on the Tier-0 gateway
- D. Tier-0 Uplink Interface H Tier-1 SR Router Port

Correct Answer: C, D

Section:

Explanation:

Single Tier topology is a simplified NSX design that uses only one logical router (Tier-1) for both north-south and east-west traffic. The Tier-1 logical router has two components: a Distributed Router (DR) and a Services Router (SR). The DR performs distributed routing across all transport nodes, while the SR provides centralized services such as NAT, DHCP, VPN, etc. The SR is hosted on an Edge node that also hosts a Tier-0 gateway. The Tier-0 gateway is used for connecting to the physical network and providing dynamic routing protocols such as BGP or OSPF.

Ingress traffic on the Edge node supporting a Single Tier topology will use two interfaces: an Inter-Tier Interface on the Tier-0 gateway and a Tier-1 SR Router Port. The Inter-Tier Interface is a logical port that connects the Tier-0 gateway to the Tier-1 gateway. This interface enables routing between the two gateways and carries all the routing protocols and traffic. The Tier-1 SR Router Port is a logical port that connects the Tier-1 SR to the Tier-1 DR. This interface enables routing between the centralized and distributed components of the Tier-1 logical router.

QUESTION 20

Which Is the only supported mode In NSX Global Manager when using Federation?

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

Correct Answer: B

Section:

Explanation:

NSX Global Manager is a feature of NSX that allows managing multiple NSX domains across different sites or clouds from a single pane of glass. NSX Global Manager supports Federation, which is a capability that enables synchronizing configuration and policy across multiple NSX domains. Federation has many benefits such as simplifying operations, improving resiliency, and enabling disaster recovery.

The only supported mode in NSX Global Manager when using Federation is Policy mode. Policy mode means that NSX Global Manager acts as a policy manager that defines and distributes global policies to local NSX managers in different domains. Policy mode also allows local NSX managers to have their own local policies that can override or merge with global policies.

QUESTION 21

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

- A. VXIAN

- B. UDP
- C. STT
- D. TEP

Correct Answer: D

Section:

Explanation:

According to the VMware NSX Documentation, TEP stands for Tunnel End Point and is a logical interface that must be configured on transport nodes for encapsulation and decapsulation of Geneve protocol. Geneve is a tunneling protocol that encapsulates the original packet with an outer header that contains metadata such as the virtual network identifier (VNI) and the transport node IP address. TEPs are responsible for adding and removing the Geneve header as the packet traverses the overlay network.

QUESTION 22

An NSX administrator is treating a NAT rule on a Tier-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

Correct Answer: B, E

Section:

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.

QUESTION 23

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

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

Correct Answer: A, C, F

Section:

Explanation:

According to the VMware NSX Documentation, these are three of the security features that are dependent on the NSX Application Platform:

NSX Firewall: This feature provides distributed firewalling and micro-segmentation capabilities for network and application security. It allows you to create and enforce granular firewall rules based on various criteria such as identity, context, or tags.

NSX Distributed IDS/IPS: This feature provides distributed intrusion detection and prevention capabilities for network and application security. It allows you to detect and block malicious traffic based on signatures, behaviors, or anomalies.

NSX Network Detection and Response: This feature provides advanced threat detection and response capabilities for network and application security. It includes features such as Distributed Intrusion Detection and Prevention (IDS/IPS), Web Reputation Analysis, File and Process Analysis, and NSX Advanced Threat Prevention.

QUESTION 24

Which NSX feature can be leveraged to achieve consistent policy configuration and simplicity across sites?

- A. VRF Lite
- B. Ethernet VPN
- C. NSX MTML5 UI
- D. NSX Federation

Correct Answer: D

Section:

Explanation:

According to the VMware NSX Documentation, this is the NSX feature that can be leveraged to achieve consistent policy configuration and simplicity across sites:

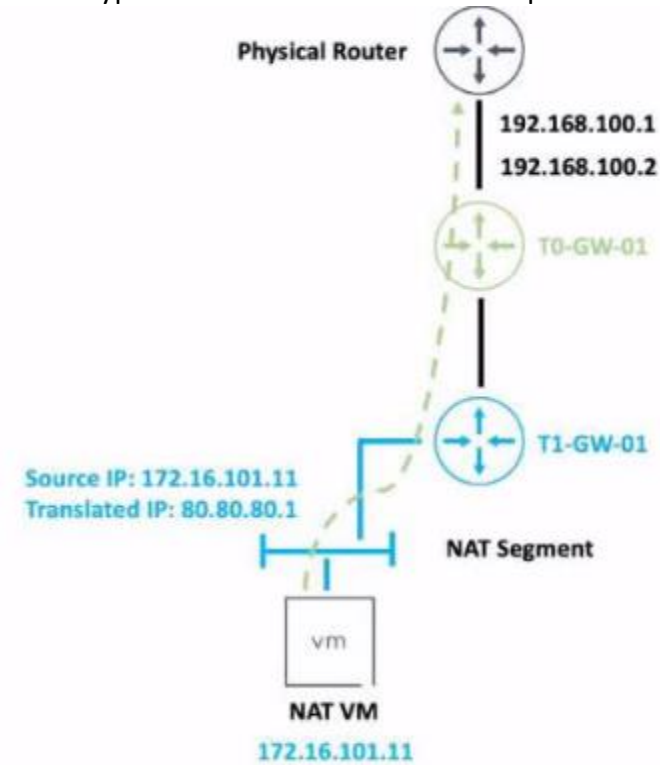
NSX Federation: This feature allows you to create and manage a global network infrastructure that spans across multiple sites using a single pane of glass. You can use this feature to synchronize policies, segments, gateways, firewalls, VPNs, load balancers, and other network services across sites.

QUESTION 25

Refer to the exhibit.

An administrator would like to change the private IP address of the NAT VM 172.16.101.11 to a public address of 80.80.80.1 as the packets leave the NAT-Segment network.

Which type of NAT solution should be implemented to achieve this?



- A. DNAT

- B. SNAT
- C. Reflexive NAT
- D. NAT64

Correct Answer: B

Section:

Explanation:

SNAT stands for Source Network Address Translation. It is a type of NAT that translates the source IP address of outgoing packets from a private address to a public address. SNAT is used to allow hosts in a private network to access the internet or other public networks¹

In the exhibit, the administrator wants to change the private IP address of the NAT VM 172.16.101.11 to a public address of 80.80.80.1 as the packets leave the NAT-Segment network. This is an example of SNAT, as the source IP address is modified before the packets are sent to an external network.

According to the VMware NSX 4.x Professional Exam Guide, SNAT is one of the topics covered in the exam objectives²

To learn more about SNAT and how to configure it in VMware NSX, you can refer to the following resources:

VMware NSX Documentation: NAT³

VMware NSX 4.x Professional: NAT Configuration⁴

VMware NSX 4.x Professional: NAT Troubleshooting⁵

QUESTION 26

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

Correct Answer: C, D

Section:

Explanation:

The answer is C and D.

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.

QUESTION 27

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 don't need to be connected to provide any stateful services.

Correct Answer: A

Section:

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

QUESTION 28

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.

Correct Answer: C

Section:

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

QUESTION 29

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

Correct Answer: C, D

Section:

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.

QUESTION 30

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. FIGRP is disabled by default.
- E. BGP is enabled by default.

Correct Answer: A, B, D

Section:

Explanation:

The answer is A, B, and D.

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

QUESTION 31

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

Correct Answer: B, D, F

Section:

Explanation:

The answer is B, D, and F.

B) RAPID. This is correct. RAPID stands for Real-time Anti-malware Protection with Intelligent Detection. It is a component of the NSX Edge node that provides malware prevention for the north-south traffic. RAPID extracts files from the network traffic and analyzes them for malicious behavior using hash-based detection, local analysis, and cloud analysis techniques¹

D) IDS/IPS. This is correct. IDS/IPS stands for Intrusion Detection and Prevention System. It is a component of the NSX Edge node that provides intrusion detection and prevention for the north-south traffic. IDS/IPS monitors the network traffic and compares it against a known set of signatures that specify patterns for different types of network intrusions. IDS/IPS can generate alerts or block the traffic based on the matching signatures and the configured actions²

F) Reputation Service. This is correct. Reputation Service is a component of the NSX Edge node that provides reputation-based filtering for the north-south traffic. Reputation Service uses a cloud-based database of known malicious IP addresses and domains to block or allow the traffic based on the reputation score of the source or destination. Reputation Service can also integrate with third-party reputation providers to enhance the security coverage³

A) Thin Agent. This is incorrect. Thin Agent is not a component of the NSX Edge node, but rather a component of the NSX Guest Introspection platform that runs on the virtual machine endpoints in the distributed east-west traffic. Thin Agent enables communication between the virtual machines and the NSX Manager, and facilitates malware prevention and intrusion detection on the host level.

C) Security Hub. This is incorrect. Security Hub is not a component of the NSX Edge node, but rather a component of the VMware Cloud Services platform that provides a unified view of security posture across multiple cloud environments. Security Hub integrates with NSX Advanced Threat Prevention to collect and display security events, alerts, and recommendations from NSX IDS/IPS and NSX Malware Prevention features.

E) Security Analyzer. This is incorrect. Security Analyzer is not a real product name or component name related to NSX Edge or NSX Advanced Threat Prevention. It is a fictional name that does not exist in the VMware portfolio.

To learn more about NSX Edge components for North-South Malware Prevention, you can refer to the following resources:

VMware NSX Documentation: Overview of NSX IDS/IPS and NSX Malware Prevention 2

VMware NSX Documentation: Configure North-South Malware Prevention 1

VMware NSX Documentation: Configure North-South Intrusion Detection and Prevention

QUESTION 32

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.

Correct Answer: B, E

Section:

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.

QUESTION 33

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

Correct Answer: D

Section:

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 .

QUESTION 34

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

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

Correct Answer: D

Section:

Explanation:

The answer is D. An alarm can be suppressed for a specific duration in hours.

According to the VMware NSX documentation, an alarm can be in one of the following states: Open, Acknowledged, Suppressed, or Resolved¹²

An alarm in a Suppressed state means that the status reporting for this alarm has been disabled by the user for a user-specified duration¹²

When a user moves an alarm into a Suppressed state, they are prompted to specify the duration in hours. After the specified duration passes, the alarm state reverts to Open. However, if the system determines the condition has been corrected, the alarm state changes to Resolved¹³

To learn more about how to manage alarm states in NSX, you can refer to the following resources:

VMware NSX Documentation: Managing Alarm States ¹

VMware NSX Documentation: View Alarm Information ²

VMware NSX Intelligence Documentation: Manage NSX Intelligence Alarm States ³

QUESTION 35

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.

Correct Answer: D

Section:

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.

QUESTION 36

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

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

Correct Answer: D, E, F

Section:

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.

QUESTION 37

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

Correct Answer: C, E

Section:

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

QUESTION 38

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.

Correct Answer: B, C

Section:

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.

QUESTION 39

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

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

Correct Answer: C, D

Section:

Explanation:

<https://docs.vmware.com/en/VMware-Validated-Design/5.0.1/com.vmware.vvd.sddc-nsxt-design.doc/GUID-74141ABD-C9AF-4A92-8338-092CD67EB56E.html>

QUESTION 40

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)

Correct Answer: A

Section:

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.

QUESTION 41

HOTSPOT

Refer to the exhibit.

An administrator configured NSX Advanced Load Balancer to load balance the production web server traffic, but the end users are unable to access the production website by using the VIP address. Which of the following Tier-1 gateway route advertisement settings needs to be enabled to resolve the problem? Mark the correct answer by clicking on the image.

Hot Area:

Answer Area

Tier-1 Gateways

ADD TIER-1 GATEWAY

	Name	HA Mode ⓘ	Linked Tier-0 Gateway	
⋮	Prod-T1-GW-01	Distributed Only	Prod-T0-GW-01	
	Edges Pool Allocation Size	ROUTING	DHCP Config	Not Set
	Description	Not Set	Tags	0
	Route Advertisement			
	All Static Routes	● Disabled	All NAT IP's	● Disabled
	All DNS Forwarder Routes	● Disabled	All LB VIP Routes	● Disabled
	All Connected Segments & Service Ports	● Enabled	All LB SNAT IP Routes	● Disabled
	All IPsec Local Endpoints	● Disabled	Set Route Advertisement Rules	Not Set

Answer Area:

Answer Area

Tier-1 Gateways

ADD TIER-1 GATEWAY

	Name	HA Mode ⓘ	Linked Tier-0 Gateway
⋮	Prod-T1-GW-01	Distributed Only	Prod-T0-GW-01
	Edges Pool Allocation Size	ROUTING	DHCP Config
	Description	Not Set	Tags
	<div>Route Advertisement</div> <div> <div>All Static Routes</div> <div>● Disabled</div> </div> <div> <div>All DNS Forwarder Routes</div> <div>● Disabled</div> </div> <div> <div>All Connected Segments & Service Ports</div> <div>● Enabled</div> </div> <div> <div>All IPsec Local Endpoints</div> <div>● Disabled</div> </div>		<div>All NAT IP's</div> <div>● Disabled</div> <div>All LB VIP Routes</div> <div>● Disabled</div> <div>All LB SNAT IP Routes</div> <div>● Disabled</div> <div>Set Route Advertisement Rules</div> <div>Not Set</div>

Section:

Explanation:

QUESTION 42

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

Correct Answer: B

Section:

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.

QUESTION 43

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

Correct Answer: B

Section:

Explanation:

According to the VMware Knowledge Base article¹, 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.

QUESTION 44

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

Correct Answer: B, E

Section:

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.

QUESTION 45

What should an NSX administrator check to verify that VMware Identity Manager Integration is successful?

- A. From VMware Identity Manager the status of the remote access application must be green.
- B. From the NSX UI the status of the VMware Identity Manager Integration must be 'Enabled'.
- C. From the NSX CLI the status of the VMware Identity Manager Integration must be 'Configured'.
- D. From the NSX UI the URI in the address bar must have 'locaNfatse' part of it.

Correct Answer: B

Section:

Explanation:

From the NSX UI the status of the VMware Identity Manager Integration must be "Enabled". According to the VMware NSX Documentation¹, after configuring VMware Identity Manager integration, you can validate the functionality by checking the status of the integration in the NSX UI. The status should be "Enabled" if the integration is successful. The other options are either incorrect or not relevant.

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

Correct Answer: D

Section:

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.

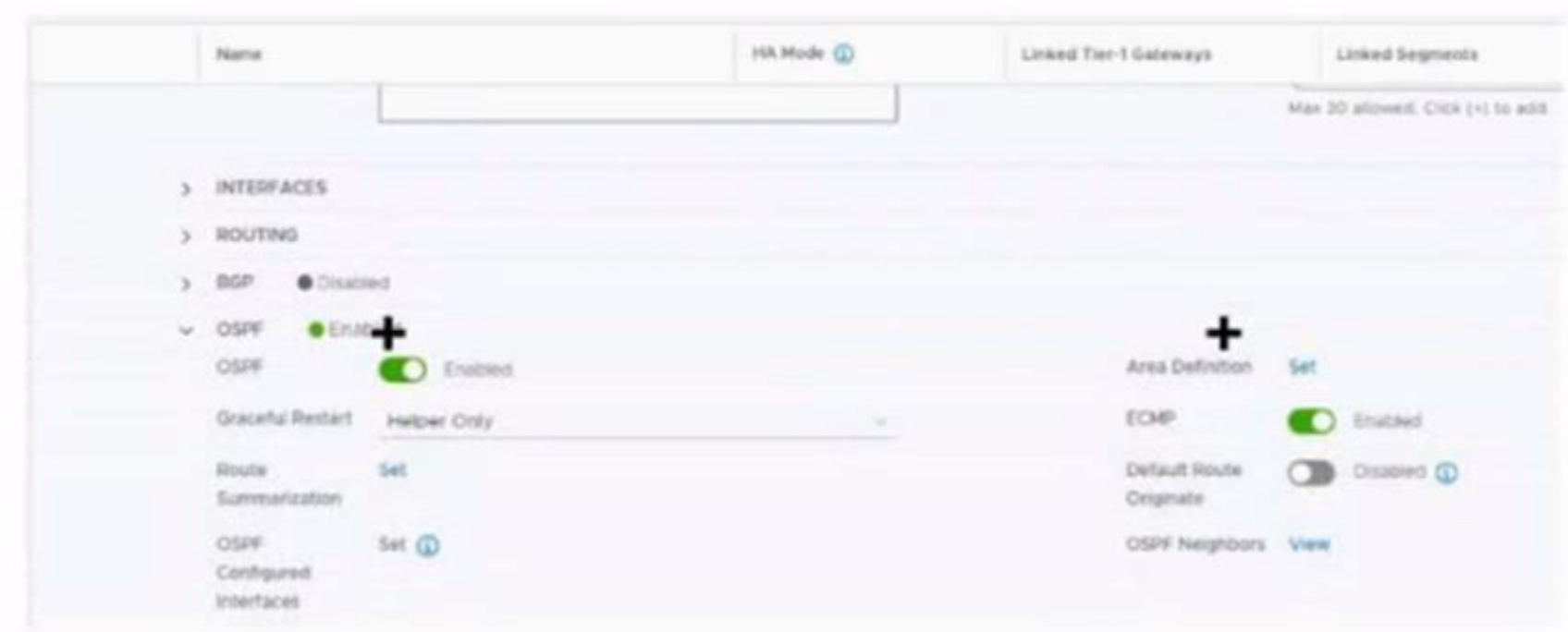
QUESTION 47

HOTSPOT

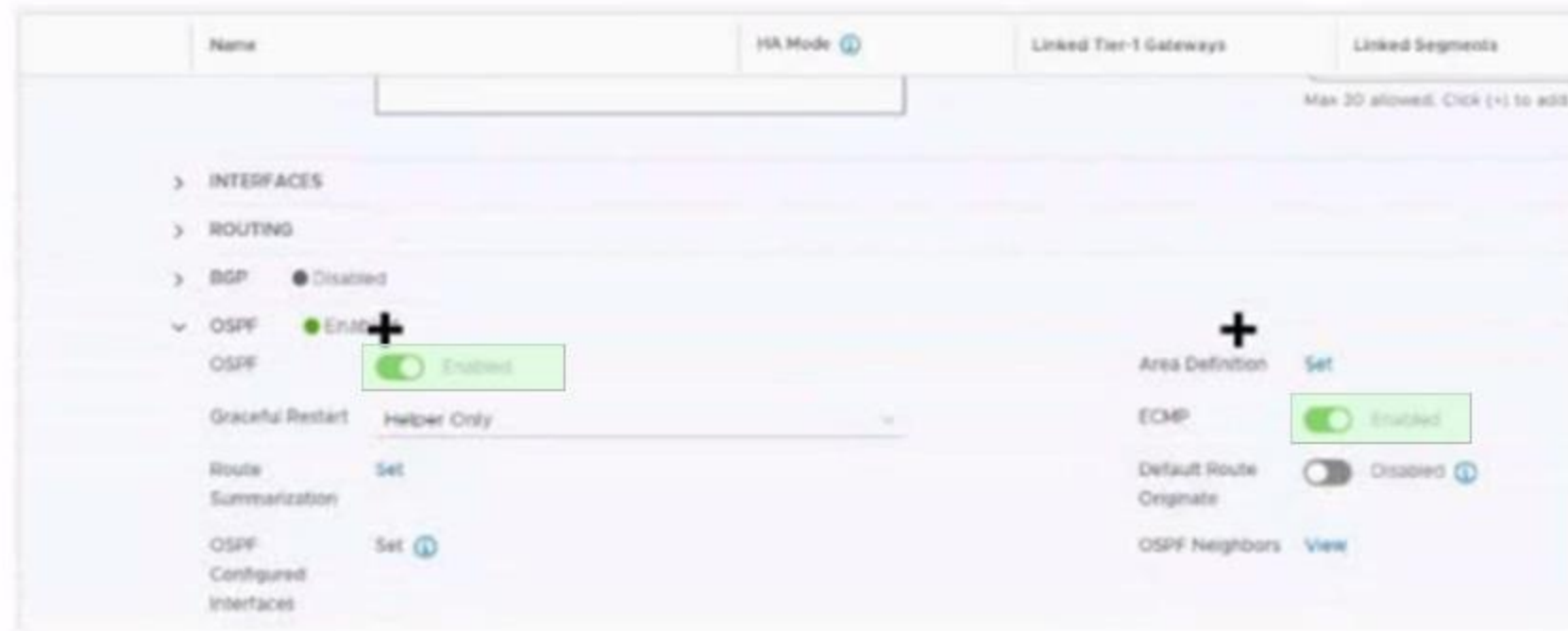
Refer to the exhibit.

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

Hot Area:



Answer Area:



Section:

Explanation:

QUESTION 48

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

Correct Answer: A, C, E

Section:

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.

QUESTION 49

Where in the NSX UI would an administrator set the time attribute for a time-based Gateway Firewall rule?

- A. The option to set time-based rule is a clock icon in the rule.
- B. The option to set time based rule is a field in the rule itself.
- C. There is no option in the NSX UI. It must be done via command line interface.

D. The option to set time-based rule is a clock icon in the policy.

Correct Answer: D

Section:

Explanation:

According to the VMware documentation¹, the clock icon appears on the firewall policy section that you want to have a time window. By clicking the clock icon, you can create or select a time window that applies to all the rules in that policy section. The other options are incorrect because they either do not exist or are not related to the time-based rule feature. There is no option to set a time-based rule in the rule itself, as it is a policy-level setting. There is also an option to set a time-based rule in the NSX UI, so it does not require using the command line interface.

QUESTION 50

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

Correct Answer: A

Section:

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.

QUESTION 51

DRAG DROP

Refer to the exhibits.

Drag and drop the NSX graphic element icons on the left found in an NSX Intelligence visualization graph to its correct description on the right.

Select and Place:



Answer Area



This icon represents a physical server that is part of your NSX environment. A physical server can belong to more than one group



This icon represents a group on which security policies, including East-West firewall rules, can be applied. A group can be a collection of VMs, physical servers, or sets of IP addresses

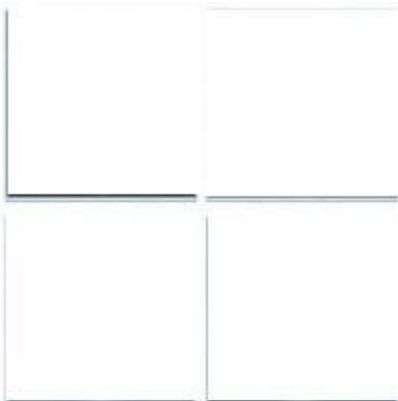


This is the icon for the public IP addresses on the Internet. If at least one compute entity in your NSX environment communicated with a public IP address during the selected time period, that traffic flow is included in the current visualization.



This is the icon used for a virtual machine (VM) that is part of your NSX environment. A VM can belong to more than one group

Correct Answer:



Answer Area



This icon represents a physical server that is part of your NSX environment. A physical server can belong to more than one group



This icon represents a group on which security policies, including East-West firewall rules, can be applied. A group can be a collection of VMs, physical servers, or sets of IP addresses



This is the icon for the public IP addresses on the Internet. If at least one compute entity in your NSX environment communicated with a public IP address during the selected time period, that traffic flow is included in the current visualization.



This is the icon used for a virtual machine (VM) that is part of your NSX environment. A VM can belong to more than one group

Section:

Explanation: