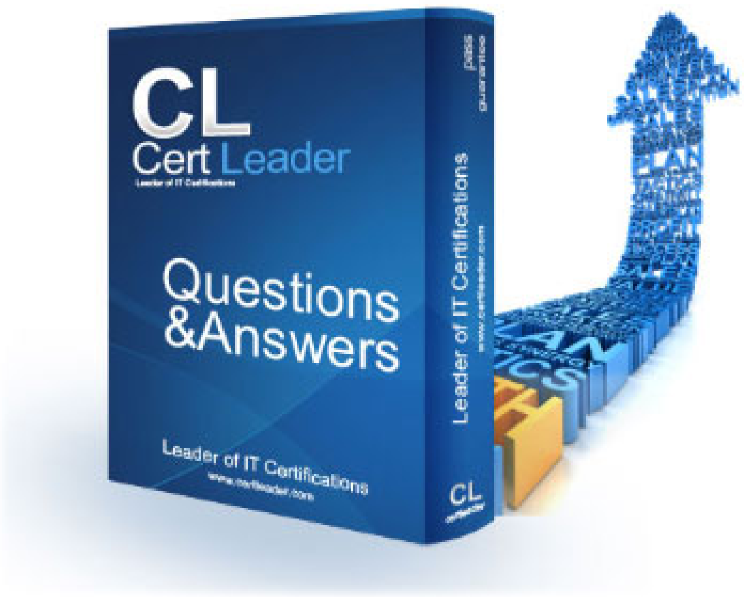
2V0-41.23 Dumps

VMware NSX 4.x Professional

https://www.certleader.com/2V0-41.23-dumps.html



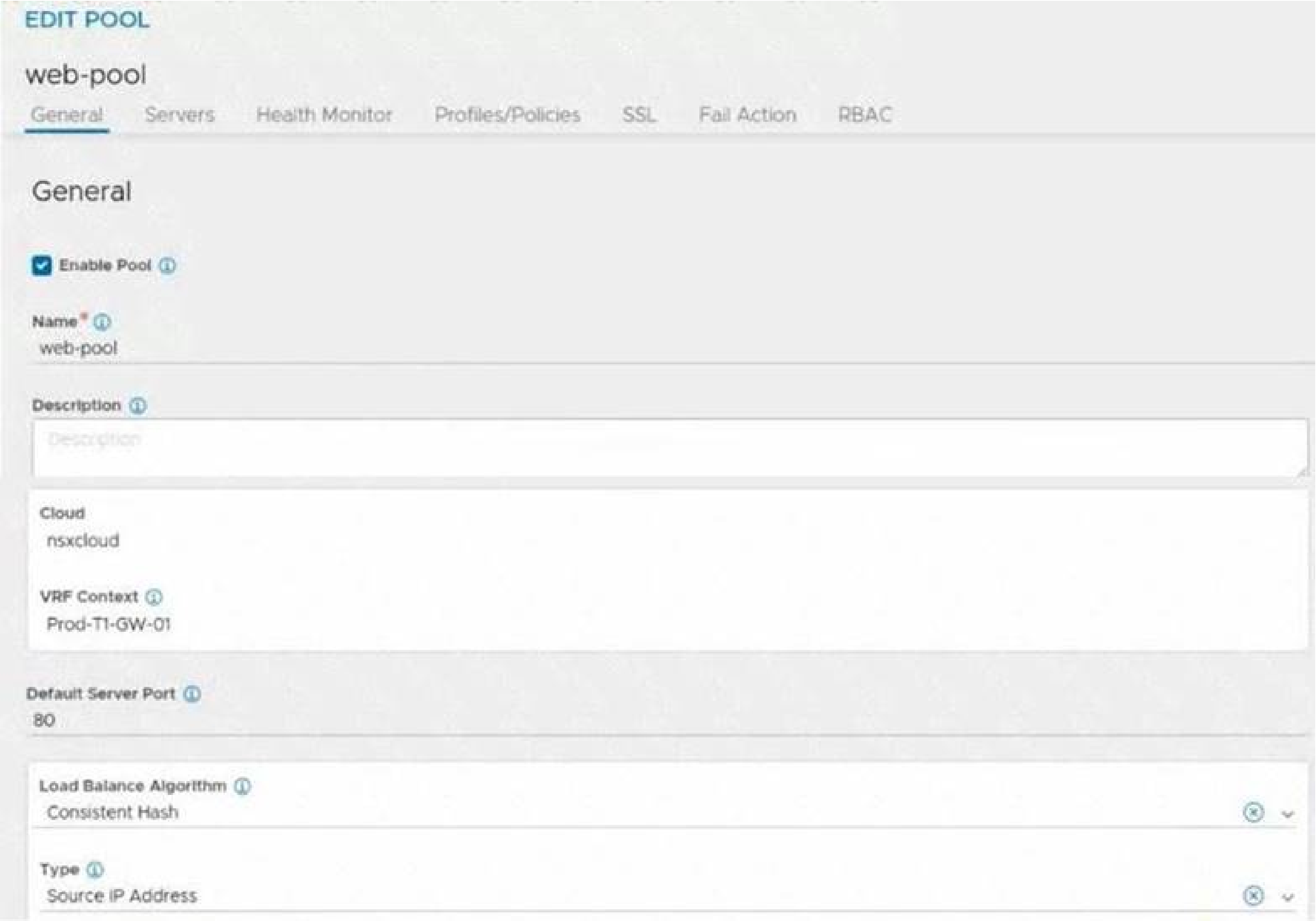
NEW QUESTION 1
An NSX administrator is troubleshooting a connectivity issue with virtual machines running on an FSXi transport node. Which feature in the NSX Ul shows the mapping between the virtual NIC and the host's physical adapter?

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.



web-pool

General

☑ Enable Pool

Name* web-pool

Description

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
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 4
Which field in a Tier-1 Gateway Firewall would be used to allow access for a collection of trustworthy web sites?

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

Answer: D

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

NEW QUESTION 5
A company security policy requires all users to log Into applications using a centralized authentication system. Which two authentication, authorization, and accounting (AAA) systems are available when Integrating NSX with VMware Identity Manager? (Choose two.)

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

Answer: CD

Explanation:
NSX supports two types of authentication, authorization, and accounting (AAA) systems when integrating with VMware Identity Manager: RSA SecurID and LDAP and OpenLDAP based on Active Directory (AD). RSA SecurID is a two-factor authentication system that uses a token-based approach to verify the identity of users. LDAP and OpenLDAP based on AD are directory services that store and manage user information and credentials. Both systems can be used to provide centralized authentication for users who want to access applications in an NSX environment .
https://blogs.vmware.com/networkvirtualization/2017/11/remote-user-authentication-and-rbac-with-nsx-t.html

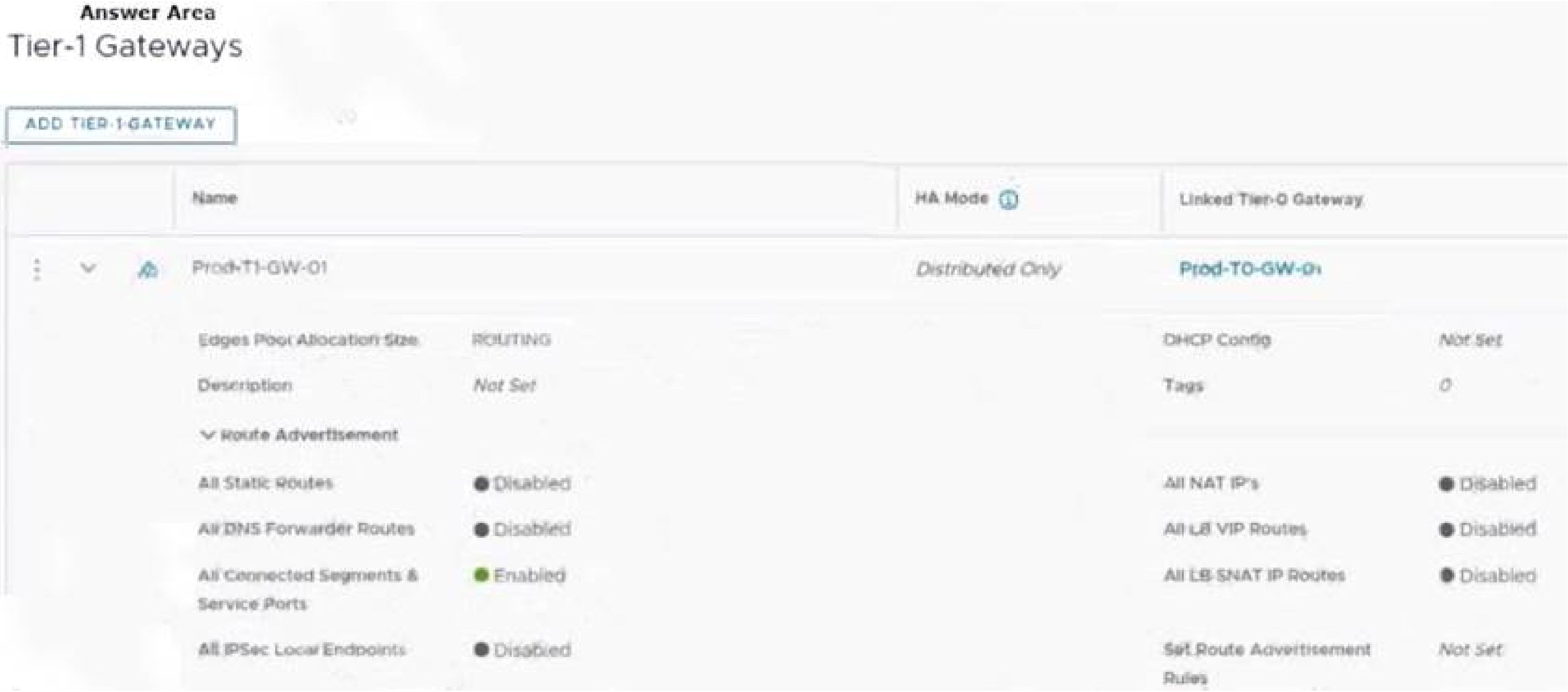
NEW QUESTION 6
In an NSX environment, an administrator is observing low throughput and congestion between the Tier-O Gateway and the upstream physical routers.
Which two actions could address low throughput and congestion? (Choose two.)

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 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 7
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.



Answer Area

Tier-1 Gateways

ADD TIER-1-GATEWAY

Name	HA Mode	Linked Tier-0 Gateway
Prod-T1-GW-01	*Distributed Only*	Prod-TO-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*

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The correct answer is to enable the option All LB VIP Routes on the Tier-1 gateway route advertisement settings. This option allows the Tier-1 gateway to advertise the NSX Advanced Load Balancer LB VIP routes to the Tier-0 gateway and other peer routers, so that the end users can reach the production website by using the VIP address1. The other options are not relevant for this scenario.
To mark the correct answer by clicking on the image, you can click on the toggle switch next to All LB VIP Routes to turn it on. The switch should change from gray to blue, indicating that the option is enabled. See the image below for reference:

NEW QUESTION 8
When configuring OSPF on a Tler-0 Gateway, which three of the following must match in order to establish a neighbor relationship with an upstream router? (Choose three.)

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

Answer: BCF

Explanation:
ccording to the VMware NSX Documentation, these are the three parameters that must match in order to establish an OSPF neighbor relationship with an upstream router on a tier-0 gateway:

> MTU of the Uplink: The maximum transmission unit (MTU) of the uplink interface must match the MTU of the upstream router interface. Otherwise, OSPF packets may be fragmented or dropped, causing neighbor adjacency issues.

> Subnet mask: The subnet mask of the uplink interface must match the subnet mask of the upstream router interface. Otherwise, OSPF packets may not reach the correct destination or be rejected by the upstream router.

> Area ID: The area ID of the uplink interface must match the area ID of the upstream router interface.
Otherwise, OSPF packets may be ignored or discarded by the upstream router.

NEW QUESTION 9
Which two choices are use cases for Distributed Intrusion Detection? (Choose two.)

A. Use agentless antivirus with Guest Introspection.
B. Quarantine workloads based on vulnerabilities.
C. Identify risk and reputation of accessed websites.
D. Gain Insight about micro-segmentation traffic flows.
E. Identify security vulnerabilities in the workloads.

Answer: BE

Explanation:
According to the VMware NSX Documentation, these are two of the use cases for Distributed Intrusion Detection, which is a feature of NSX Network Detection and Response:

> Quarantine workloads based on vulnerabilities: You can use Distributed Intrusion Detection to detect vulnerabilities in your workloads and apply quarantine

actions to isolate them from the network until they are remediated.

- Identify security vulnerabilities in the workloads: You can use Distributed Intrusion Detection to scan your workloads for known vulnerabilities and generate reports that show the severity, impact, and remediation steps for each vulnerability.

NEW QUESTION 10
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 10
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 14
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

Answer: BE

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

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

NEW QUESTION 16
Which command Is used to test management connectivity from a transport node to NSX Manager?

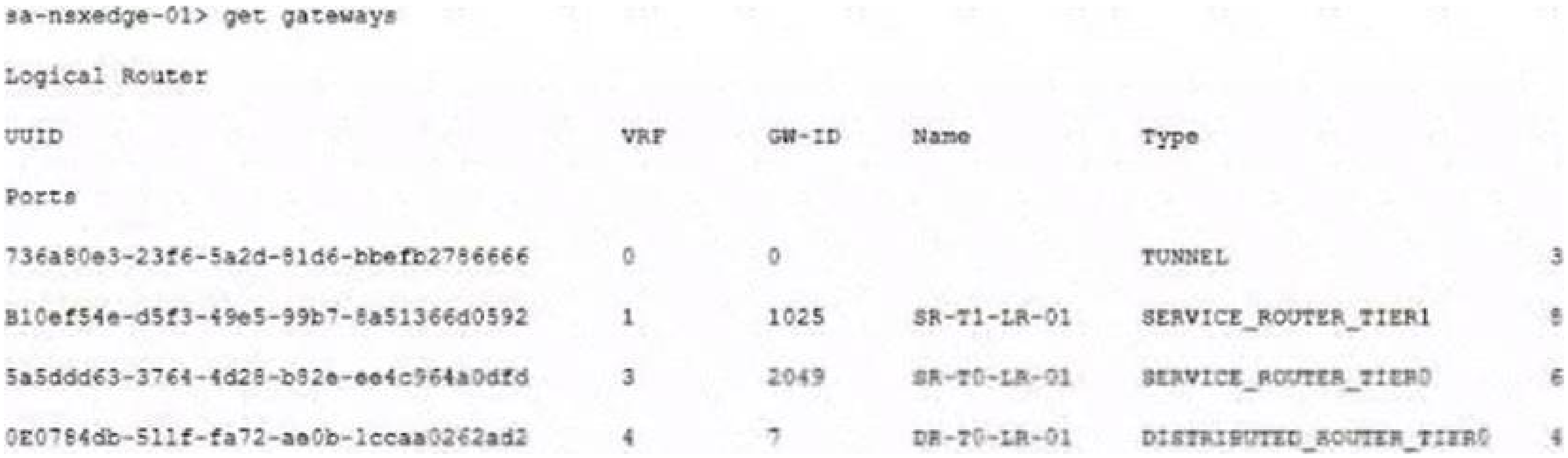
A. esxcli network ip connection list | grep 1234 esxcli network ip connection list | grep 1234
B. esxcli network connection list | grep 1235 esxcli network connection list | grep 1234
C. esxcli network ip connection list | grep 1235 esxcli network ip connection list | grep 1235
D. esxcli network connection list | grep 1234 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 21

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-nsxedge-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-b82e-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-nexedge-01(tier1_sr> get bgp neighbor
D. sa-nexedge-01(tier0_sr> get bgp neighbor
E. sa-nexedge-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-doma
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 26

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 30

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 32

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 firs 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 33
NSX improves the security of today's modern workloads by preventing lateral movement, which feature of NSX can be used to achieve this?

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

Answer: A

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

NEW QUESTION 35
An NSX administrator is creating a Tier-1 Gateway configured In Active-Standby High Availability Mode. In the event of node failure, the failover policy should not allow the original tailed node to become the Active node upon recovery.
Which failover policy meets this requirement?

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

Answer: A

Explanation:
According to the VMware NSX Documentation, a non-preemptive failover policy means that the original failed node will not become the active node upon recovery, unless the current active node fails again. This policy can help avoid unnecessary failovers and ensure stability.
The other options are either incorrect or not available for this configuration. Preemptive is the opposite of non-preemptive, meaning that the original failed node will become the active node upon recovery, if it has a higher priority than the current active node. Enable Preemptive and Disable Preemptive are not valid options for the failover policy, as the failover policy is a drop-down menu that only has two choices: Preemptive and Non-Preemptive.

NEW QUESTION 37
An administrator has a requirement to have consistent policy configuration and enforcement across NSX instances.
What feature of NSX fulfills this requirement?

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

Answer: B

Explanation:
Federation is a feature of NSX that allows the administrator to manage multiple NSX instances with a single pane of glass view, create gateways and segments that span one or more locations, and configure and enforce firewall rules consistently across locations1. Federation provides centralized policy management for security and networking services for all locations and pushes it down to NSX Local Managers at the respective sites for enforcement1. Federation also enables disaster recovery and workload mobility scenarios by providing consistent network and security policies across different sites1. References: 1: NSX Federation - VMware Docs(https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-D5B6DC79-6733-44

NEW QUESTION 42
Which two logical router components span across all transport nodes? (Choose two.)

A. SFRVICE_ROUTER_TJER0
B. TIERO_DISTRI BUTE D_ ROUTER
C. DISTRIBUTED_R0UTER_TIER1
D. DISTRIBUTED_ROUTER_TIER0
E. SERVICE_ROUTER_TIERl

Answer: CD

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

NEW QUESTION 46
An NSX administrator wants to create a Tler-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 48
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 ate 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 50
How is the RouterLink port created between a Tier-1 Gateway and Tler-0 Gateway?

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

Answer: D

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

NEW QUESTION 52
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 57
Which two statements describe the characteristics of an Edge Cluster in NSX? (Choose two.)

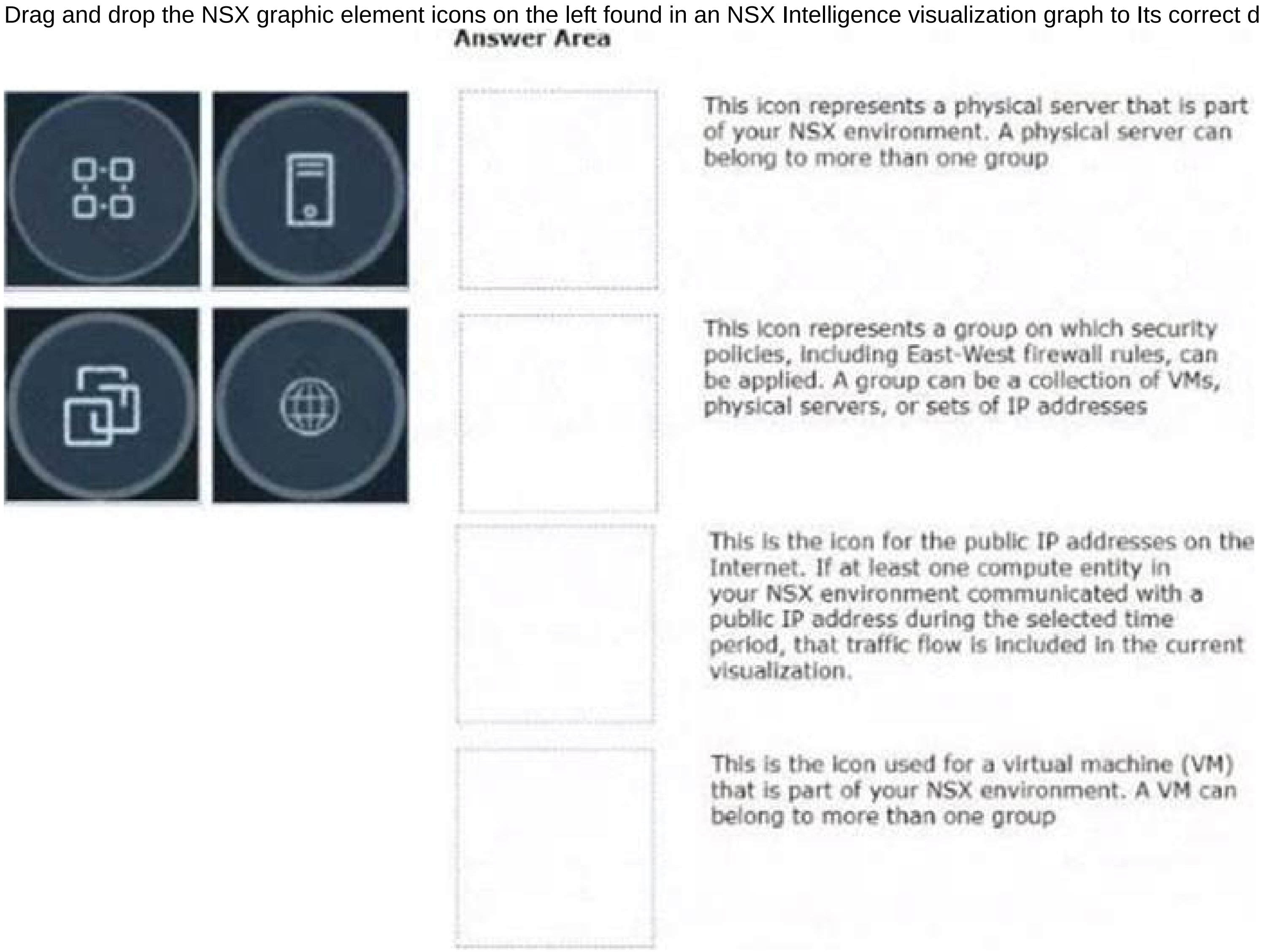
A. Can have a maximum of 8 edge nodes
B. Can have a maximum of 10 edge nodes
C. Must have only active-active edge nodes
D. Can contain multiple types of edge nodes (VM or bare metal)
E. Must contain only one type of edge nodes (VM or bare metal)

Answer: AE

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

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

NEW QUESTION 62
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.



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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://docs.vmware.com/en/VMware-NSX-Intelligence/4.0/user-guide/GUID-DC78552B-2CC4-410D-A6C9-3

NEW QUESTION 67
......