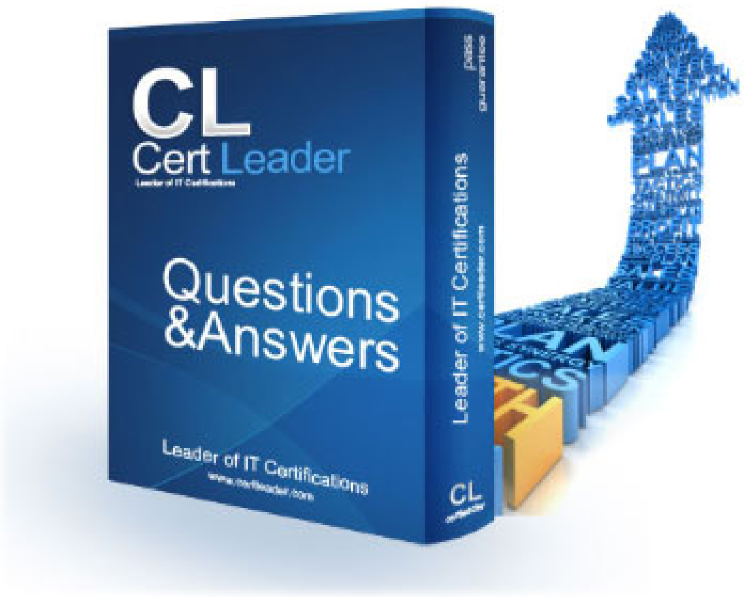
2V0-41.23 Dumps

VMware NSX 4.x Professional

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



NEW QUESTION 1
Which two of the following will be used for Ingress traffic on the Edge node supporting a Single Tier topology? (Choose two.)

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

Answer: BC

Explanation:
The two interfaces that will be used for ingress traffic on the Edge node supporting a Single Tier topology are:

- B. Tier-0 Uplink interface
- C. Downlink Interface for the Tier-0 DR

The Tier-0 Uplink interface is the interface that connects the Tier-0 gateway to the external network. It is used to receive traffic from the physical router or switch that is the next hop for the Tier-0 gateway. The Tier-0 Uplink interface can be configured with a static IP address or use BGP to exchange routes with the external network.

The Downlink Interface for the Tier-0 DR is the interface that connects the Tier-0 gateway to the workload segments. It is used to receive traffic from the VMs or containers that are attached to the segments. The Downlink Interface for the Tier-0 DR is a logical interface (LIF) that is distributed across all transport nodes that host the segments. The Downlink Interface for the Tier-0 DR has an IP address that acts as the default gateway for the VMs or containers on the segments.

NEW QUESTION 2
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 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
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.

Answer: B

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.

NEW QUESTION 5
Which of the following settings must be configured in an NSX environment before enabling stateful active-active SNAT?

A. Tier-1 gateway in active-standby mode
B. Tier-1 gateway in distributed only mode
C. An Interface Group for the NSX Edge uplinks
D. A Punting Traffic Group for the NSX Edge uplinks

Answer: C

Explanation:
To enable stateful active-active SNAT on a Tier-0 or Tier-1 gateway, you must configure an Interface Group for the NSX Edge uplinks. An Interface Group is a logical grouping of NSX Edge interfaces that belong to the same failure domain. A failure domain is a set of NSX Edge nodes that share the same physical network infrastructure and are subject to the same network failures. By configuring an Interface Group, you can ensure that the stateful services are distributed across different failure domains and can recover from network failures1

NEW QUESTION 6
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

Answer: D

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.

NEW QUESTION 7
Which two statements are true about IDS Signatures? (Choose two.)

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

Answer: BE

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

NEW QUESTION 8
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 9
When configuring OSPF on a TIer-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

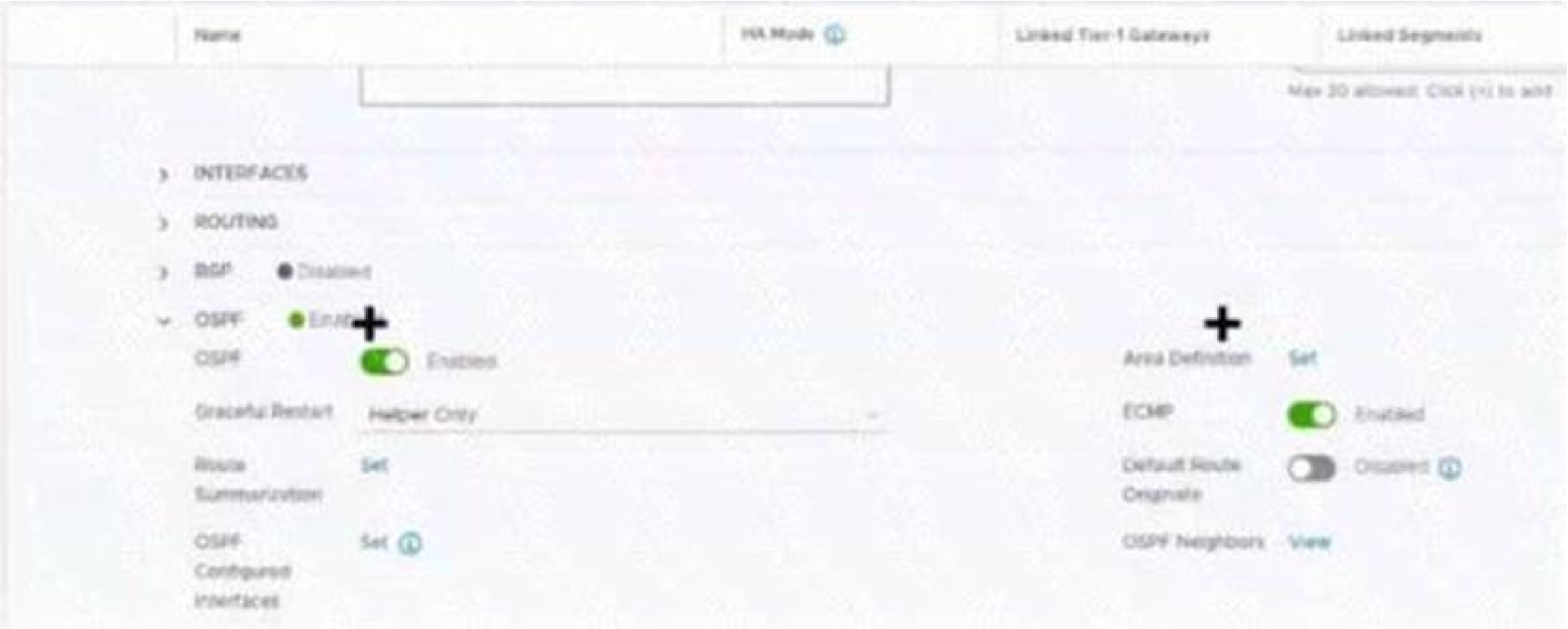
Answer: BCF

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 10
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.



OSPF: Enabled
Graceful Restart: Helper Only
Route Summarization: Set
OSPF Configured Interfaces: Set
Area Definition: Set
ECMP: Enabled
Default Route Originate: Disabled
OSPF Neighbors: View

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 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 14
Which command is used to display the network configuration of the Tunnel Endpoint (TEP) IP on a bare metal transport node?

A. tepconfig
B. ifconfig
C. tcpdump
D. debug

Answer: B

Explanation:
The command ifconfig is used to display the network configuration of the Tunnel Endpoint (TEP) IP on a ba metal transport node2. The TEP IP is assigned to a network interface on the bare metal server that is used for overlay traffic. The ifconfig command can show the IP address, netmask, broadcast address, and other information of the network interface. For example, the following command shows the network configuration
of the TEP IP on a bare metal transport node with interface name ens192:
ifconfig ens192
The output of the command would look something like this:
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 10.10.10.10 netmask 255.255.255.1 broadcast 10.10.10.255 inet6 fe80::250:56ff:fe9a:1b8c prefixlen 64 scopeid 0x20<link> ether 00:50:56:9a:1b:8c txqueuelen 1000 (Ethernet) RX packets 123456 bytes 123456789 (123.4 MB) RX errors 0
dropped 0 overruns 0 frame 0 TX packets 234567 bytes 234567890 (234.5 MB) TX errors 0 dropped 0
overruns 0 carrier 0 collisions 0
The TEP IP in this example is 10.10.10.10. References:

- IBM Cloud Docs

NEW QUESTION 17
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 20
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 21
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 U
D. It must be done via command line interface.
E. The option to set time-based rule is a clock Icon in the policy.

Answer: D

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.
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-8572496E-A60E-48C3-A016-4A081AC8

NEW QUESTION 23
Where does an administrator configure the VLANs used In VRF Lite? (Choose two.)

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

Answer: BD

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

➢ Uplink trunk segment: This is a segment that connects a tier-0 gateway to a physical network using multiple VLAN tags. You need to configure the VLAN IDs for each VRF on this segment.

➢ Uplink interface of the VRF gateway: This is an interface that connects a VRF gateway to an uplink trunk segment using a specific VLAN tag. You need to configure the VLAN ID for each VRF on this interface.

NEW QUESTION 24
An NSX administrator Is treating a NAT rule on a Tler-0 Gateway configured In active-standby high availability mode. Which two NAT rule types are supported for this configuration? (Choose two.)

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

Answer: BE

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

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

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

NEW QUESTION 29
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

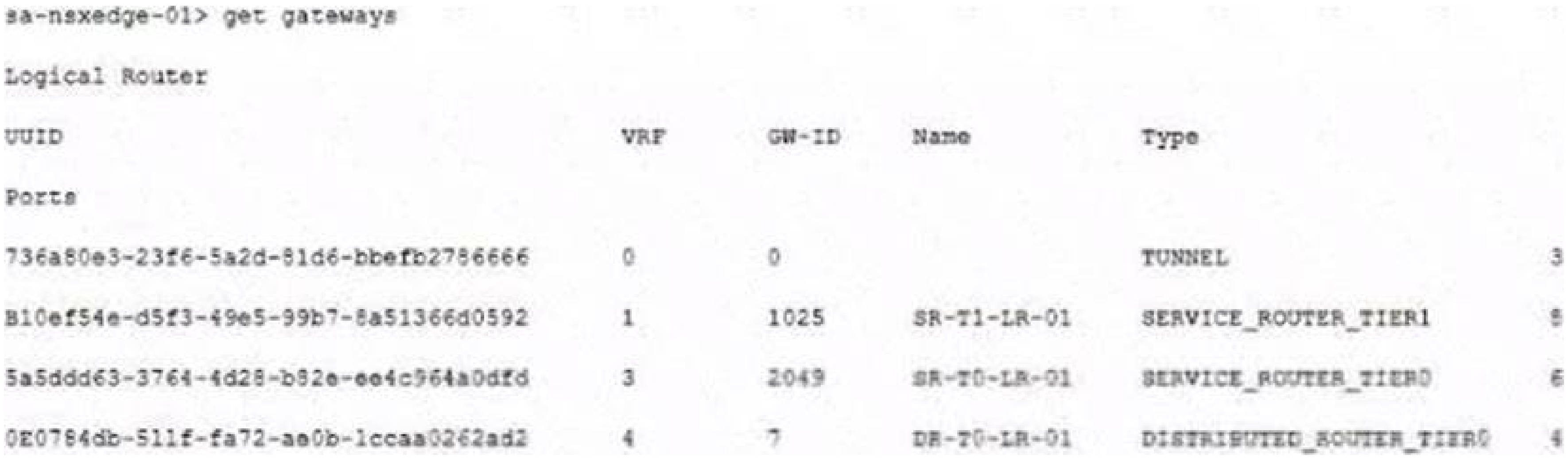
NEW QUESTION 31
Which command Is used to test management connectivity from a transport node to NSX Manager?

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 34
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 35
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 40
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 42
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.

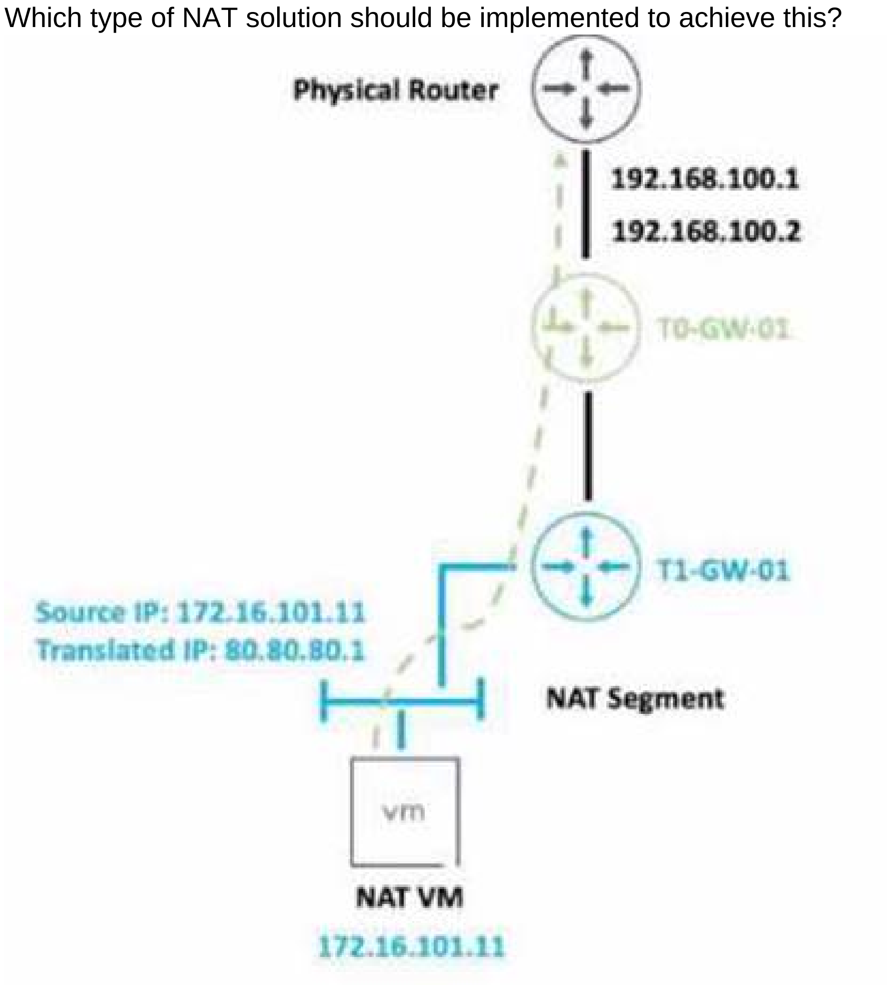
Answer: B

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 46
Refer to the exhibit.
An administrator would like to change the private IP address of the NAT VM I72.l6.101.il 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

Answer: B

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: NAT 3

➢ VMware NSX 4.x Professional: NAT Configuration 4

➢ VMware NSX 4.x Professional: NAT Troubleshooting 5
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-7AD2C384-4303-4D6C-A

NEW QUESTION 47
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

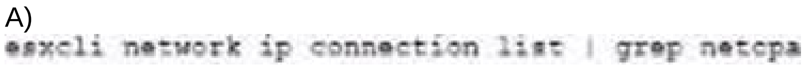
NEW QUESTION 51
NSX improves the security of today's modern workloads by preventing lateral movement, which feature of NSX can be used to achieve this?

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

Answer: A

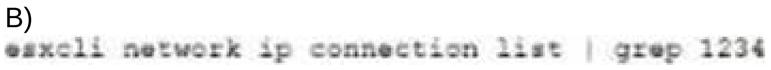
Explanation:
According to the web search results, network segmentation is a feature of NSX that improves the security of today’s modern workloads by preventing lateral movement. Lateral movement is a technique used by attackers to move from one compromised system to another within a network, exploiting 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 55
Which command on ESXI is used to verify the Local Control Plane connectivity with Central Control Plane?
A)



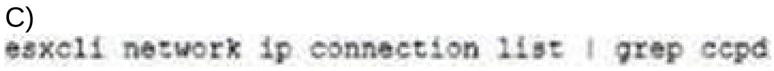
```
esxcli network ip connection list | grep netcpa
```

B)



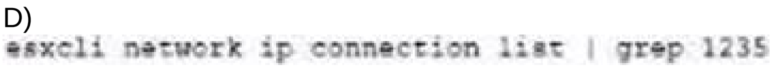
```
esxcli network ip connection list | grep 1234
```

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 58
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 61
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 62
Which Is the only supported mode In NSX Global Manager when using Federation?

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

Answer: B

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.

NEW QUESTION 63
What needs to be configured on a Tler-0 Gateway lo make NSX Edge Services available to a VM on a VLAN-backed logical switch?

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

Answer: B

Explanation:
To make NSX Edge Services available to a VM on a VLAN-backed logical switch, you need to configure
a VLAN Uplink on the Tier-0 Gateway. A VLAN Uplink is a logical interface that connects the Tier-0 Gateway to the physical network and provides external connectivity for the NSX Edge Services1. A VLAN Uplink can be configured on the NSX Manager UI by selecting Networking > Tier-0 Gateways > Interfaces > Set > Add Interface1.
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-D641380B-4C8E-4C8A-AF64-4261A266

NEW QUESTION 64
An NSX administrator has deployed a single NSX Manager node and will be adding two additional nodes to form a 3-node NSX Management Cluster for a production environment. The administrator will deploy these two additional nodes and Cluster VIP using the NSX UI.
What two are the prerequisites for this configuration? (Choose two.)

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

Answer: DE

Explanation:
According to the VMware NSX Documentation, these are the prerequisites for adding nodes to an NSX Management Cluster using the NSX UI:

- All nodes must be in the same subnet and have IP connectivity with each other.
- A compute manager must be configured and associated with the NSX Manager node.
- The NSX Manager node must have a valid license.
- The NSX Manager node must have a valid certificate.

NEW QUESTION 69

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 vmk0O -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 VMwar 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 71
What are three NSX Manager roles? (Choose three.)

A. master
B. cloud
C. zookeepet
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 76
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 79
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 81
Which CLI command would an administrator use to allow syslog on an ESXi transport node when using the esxcli utility?

A. esxcli network firewall ruleset set -r syslog -e true
B. esxcli network firewall ruleset -e syslog

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

Answer: A

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

NEW QUESTION 84
Which of the following exist only on TIer-1 Gateway firewall configurations and not on Tier-0?

A. Applied To
B. Actions
C. Profiles
D. Sources

Answer: A

Explanation:
According to the VMware NSX Documentation, Applied To is a feature that exists only on tier-1 gateway firewall configurations and not on tier-0. Applied To allows you to specify which logical router ports or segments are affected by a firewall rule. This can help reduce the scope and improve the performance of firewall rules. By default, gateway firewall rules are applied to all the available uplinks and service interfaces on a selected gateway. For URL filtering, Applied To can only be Tier-1 gateways.
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-DE6FE8CB-017E-41C8-8

NEW QUESTION 86
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 91
When running nsxcli on an ESXi host, which command will show the Replication mode?

A. get logical-switch <Local-Switch-UUID> status
B. get logical-switch <Logical-Switch-UUID>
C. get logical-switches
D. get logical-switch status

Answer: B

NEW QUESTION 94
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 98

......