2V0-41.23Q&As

VMware NSX 4.x Professional

Pass VMware 2V0-41.23 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/2v0-41-23.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by VMware Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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 show logical-routers show bgp

B. show logical-routers get vrf show ip route bgp

C. get gateways vrf get bgp neighbor

D. enable get vrf show bgp neighbor

Correct Answer: C

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 , get bgp neighbor. These commands can be executed on the NSX Edge node CLI after logging in as admin6. The first command, get gateways, displays the list of logical routers (gateways) configured on the Edge node, along with their IDs and VRF numbers7. The second command, vrf , switches to the VRF context of the desired Tier-O Gateway, where 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

QUESTION 2

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: ACE

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.

https://docs.vmware.com/en/VMware-NSX/4.0/administration/GUID-486C1281-C6CF-47EC-B2A2-0ECFCC4A68CE.html

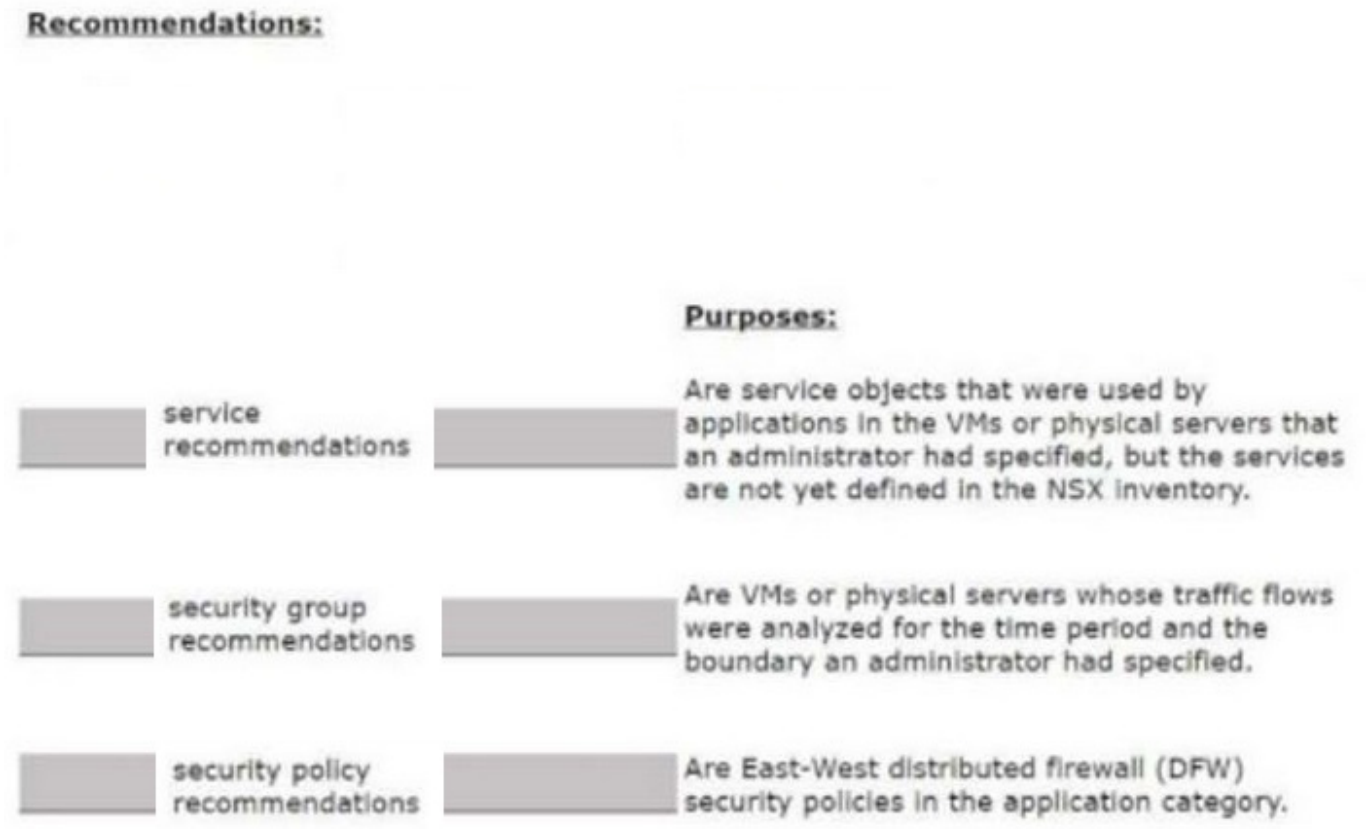
QUESTION 3

DRAG DROP

Match the NSX Intelligence recommendations with their correct purpose.

Select and Place:

Correct Answer:



Security policy recommendations: Are East-West distributed firewall (DFW) security policies in the application category12.

Security group recommendations: Are VMs or physical servers whose traffic flows were analyzed for the time period and the boundary you had specified12. Service recommendations: Are service objects that were used by applications in the

VMs or physical servers that you had specified, but the services are not yet defined in the NSX inventory12.

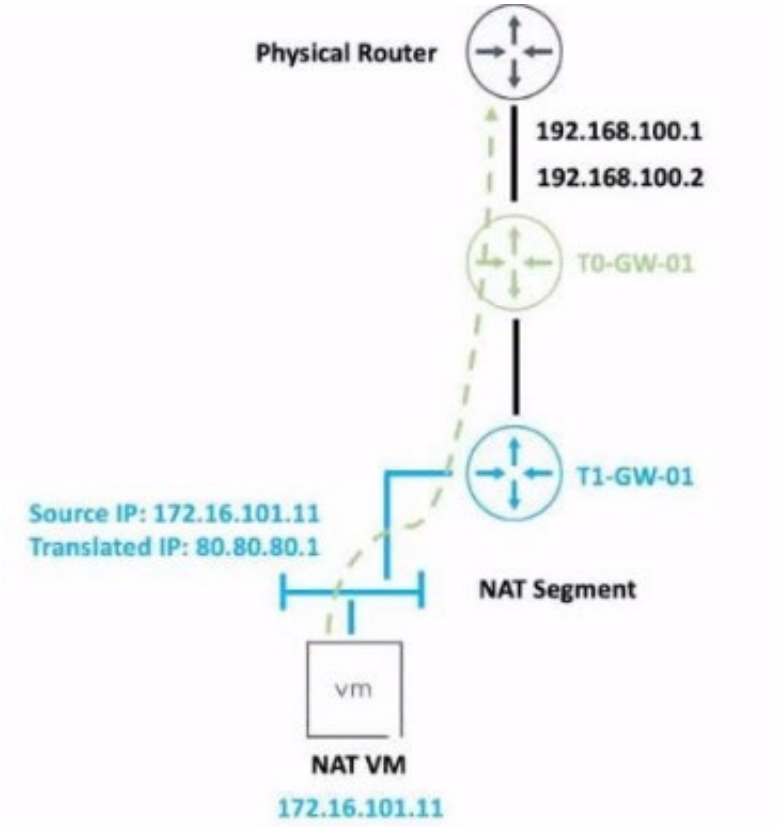
https://docs.vmware.com/en/VMware-NSX-Intelligence/4.1/user-guide/GUID-BA3B0D67-4AA8-439E-A845-4598DAD6B9D0.html

QUESTION 4

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

Correct Answer: B

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 uide, 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-A44A-DEF45AA18A92.html

QUESTION 5

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.

Correct Answer: BE

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.

QUESTION 6

Which three protocols could an NSX administrator use to transfer log messages to a remote log server? (Choose three.)

A. HTTPS

B. TCP

C. SSH

D. UDP

E. TLS

F. SSL

Correct Answer: BDE

An NSX administrator can use TCP, UDP, or TLS protocols to transfer log messages to a remote log server. These protocols are supported by NSX Manager, NSX Edge, and hypervisors for remote logging. A Log Insight log server supports all these protocols, as well as LI and LI-TLS, which are specific to Log Insight and optimize network usage. HTTPS, SSH, and SSL are not valid protocols for remote logging in NSX-T Data Center. References: : VMware NSX-T Data Center Administration Guide, page 102. : VMware Docs: Configure Remote Logging

QUESTION 7

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.

Correct Answer: DE

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.

QUESTION 8

When a stateful service is enabled for the first lime 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 Is instantiated but requites manual connection.

D. SR and DR doesn\\'t need to be connected to provide any stateful services.

Correct Answer: A

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 uide, 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 9

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.

Correct Answer: D

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 Tier0 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 10

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

```
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
```

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

Correct Answer: DF

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-domains-withmultiple-availability-zones/GUID-8BD4228A-75C6-4C60-80B4-538D4297E11A.html 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.

QUESTION 11

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

A. Controller

B. Policy

C. Proxy

D. Proton

Correct Answer: B

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. https://docs.vmware.com/en/VMware-NSX/4.0/administration/GUID-29998FC5-C1AB-40BC-B669-6E8E9937F345.html

QUESTION 12

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.

Correct Answer: ABD

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.

https://docs.vmware.com/en/VMware-NSX/4.0/administration/GUID-A75B2553-7595-40B9-A902-854941BB06FD.html

QUESTION 13

An NSX administrator is reviewing syslog and notices that Distributed Firewall Rules hit counts are not being logged.

What could cause this issue?

A. Syslog is not configured on the ESXi transport node.

B. Zero Trust Security is not enabled.

C. Syslog is not configured on the NSX Manager.

D. Distributed Firewall Rule logging is not enabled.

Correct Answer: D

https://docs.vmware.com/en/VMware-NSX/4.0/administration/GUID-D57429A1-A0A9-42BE-A299-0C3C3546ABF3.html

QUESTION 14

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

A. Network Admin

B. Enterprise Admin

C. Full Access

D. Read

E. LB Operator

F. None

G. Auditor

Correct Answer: ABEG

https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-26C44DE8-1854-4B06-B6DA-A2FD426CDF44.html

QUESTION 15

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

Correct Answer: ABDF

The four types of role-based access control (RBAC) permissions are Read, None, Full access, and Execute1. 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)