Free Questions for 2V0-41.23 by certsdeals

Shared by Jenkins on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A customer is preparing to deploy a VMware Kubernetes solution in an NSX environment.

What is the minimum MTU size for the UPLINK profile?

Options:

A- 1500

B- 1550

C- 1700

D- 1650

Answer:

C

Explanation:

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

https://nsx.techzone.vmware.com/resource/nsx-reference-design-guide#a-31-the-nsx-virtual-switch

Question 2

Question Type: MultipleChoice

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?

Options:

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 commandvmkping ++netstack=geneve -d -s 1572 <destination IP address>is used to check the VMware kernel ports for tunnel end point communication. This command uses the geneve netstack, which is the default netstack for NSX-T. The-doption sets the DF (Don't Fragment) bit in the IP header, which prevents the packet from being fragmented by intermediate routers. The-s 1572option 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.Reference: : VMware NSX-T 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.

Question 3

Question Type: MultipleChoice

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

Options:

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

Question 4

Question Type: MultipleChoice

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?

Options:

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-88AD-A7DA930A4F0B.html

Question 5

Question Type: MultipleChoice

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

Options:

A- tepconfig

B- ifconfig

C- tcpdump

D- debug

Answer:

B

Explanation:

The commandifconfigis used to display the network configuration of the Tunnel Endpoint (TEP) IP on a bare metal transport node2. The TEP IP is assigned to a network interface on the bare metal server that is used for overlay traffic. Theifconfigcommand 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 255.255.255.0 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 is10.10.10.10.

IBM Cloud Docs

Question 6

Question Type: MultipleChoice

An architect receives a request to apply distributed firewall in a customer environment without making changes to the network and vSphere environment. The architect decides to use Distributed Firewall on VDS.

Which two of the following requirements must be met in the environment? (Choose two.)

Options:

A- vCenter 8.0 and later

B- NSX version must be 3.2 and later

C- NSX version must be 3.0 and later

D- VDS version 6.6.0 and later

Answer:

B, D

Explanation:

Distributed Firewall on VDS is a feature of NSX-T Data Center that allows users to install Distributed Security for vSphere Distributed Switch (VDS) without the need to deploy an NSX Virtual Distributed Switch (N-VDS). This feature provides NSX security capabilities such as Distributed Firewall (DFW), Distributed IDS/IPS, Identity Firewall, L7 App ID, FQDN Filtering, NSX Intelligence, and NSX Malware Prevention. To enable this feature, the following requirements must be met in the environment:

The NSX version must be3.2 and later1. This is the minimum version that supports Distributed Security for VDS.

The VDS version must be6.6.0 and later1. This is the minimum version that supports the NSX host preparation operation that activates the DFW with the default rule set to allow.

Overview of NSX IDS/IPS and NSX Malware Prevention

Question 7

Question Type: MultipleChoice

The security administrator turns on logging for a firewall rule.

Where is the log stored on an ESXi transport node?

Options:

A- /var/log/vmware/nsx/firewall.log

B- /var/log/messages.log

C- /var/log/dfwpktlogs.log

D- /var/log/fw.log

Answer:

C

Explanation:

The log for a firewall rule on an ESXi transport node is stored in the /var/log/dfwpktlogs.log file. This file contains information about the packets that match or do not match the firewall rules, such as the source and destination IP addresses, ports, protocols, actions, and rule IDs. The log file can be viewed using the esxcli network firewall get command or the vSphere Client.

https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-D57429A1-A0A9-42BE-A299-0C3C3546ABF3.html

Question 8

Question Type: MultipleChoice

What are two functions of the Service Engines in NSX Advanced Load Balancer? (Choose two.)

Options:

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:

A, C