



Free Questions for 2V0-41.23 by certscare

Shared by Carter on 04-10-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

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

Answer:

C, D

Explanation:

Single Tier topology is a simplified NSX design that uses only one logical router (Tier-1) for both north-south and east-west traffic. The Tier-1 logical router has two components: a Distributed Router (DR) and a Services Router (SR). The DR performs distributed routing

across all transport nodes, while the SR provides centralized services such as NAT, DHCP, VPN, etc. The SR is hosted on an Edge node that also hosts a Tier-0 gateway. The Tier-0 gateway is used for connecting to the physical network and providing dynamic routing protocols such as BGP or OSPF.

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

Question 2

Question Type: MultipleChoice

Which two CLI commands could be used to see if vmnic link status is down? (Choose two.)

Options:

A- esxcfg-nics -1

B- excli network nic list

C- esxcli network vswitch dvs vmware list

D- esxcfg-vmknics -l

E- esxcfg-vmknics/get.network

Answer:

A, B

Explanation:

esxcfg-nics -l and esxcli network nic list are two CLI commands that can be used to see the vmnic link status on an ESXi host. Both commands display information such as the vmnic name, driver, link state, speed, and duplex mode. The link state can be either Up or Down, indicating whether the vmnic is connected or not. For example, the output of esxcfg-nics -l can look like this:

Name	PCI	Driver	Link	Speed	Duplex	MAC Address	MTU	Description
------	-----	--------	------	-------	--------	-------------	-----	-------------

vmnic0	0000:02:00.0	igbn	Up	1000Mbps	Full	00:50:56:01:2a:3b	1500	Intel Corporation I350 Gigabit Network Connection
--------	--------------	------	----	----------	------	-------------------	------	---

vmnic1	0000:02:00.1	igbn	Down	0Mbps	Half	00:50:56:01:2a:3c	1500	Intel Corporation I350 Gigabit Network Connection
--------	--------------	------	------	-------	------	-------------------	------	---

Question 3

Question Type: MultipleChoice

Which VPN type must be configured before enabling a L2VPN?

Options:

- A- Route-based IPsec VPN
- B- Policy based IPsec VPN
- C- SSL-based IPsec VPN
- D- Port-based IPsec VPN

Answer:

A

Explanation:

According to the VMware NSX Documentation, this VPN type must be configured before enabling a L2VPN. L2VPN stands for Layer 2 VPN and is a feature that allows you to extend your layer 2 network across different sites using an IPsec tunnel. Route-based IPsec VPN is a VPN type that uses logical router ports to establish IPsec tunnels between sites.

Question 4

Question Type: MultipleChoice

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

Options:

A- tcpdump

B- debug

C- pktcap-uw

D- set capture

Answer:

C

Explanation:

According to the VMware Knowledge Base, this CLI command is used for packet capture on the ESXi node. pktcap-uw stands for Packet Capture User World and is a tool that allows you to capture packets from various points in the network stack of an ESXi host. You can use this tool to troubleshoot network issues or analyze traffic flows.

The other options are either incorrect or not available for this task. tcpdump is not a valid CLI command for packet capture on the ESXi node, as it is a tool that runs on Linux systems, not on ESXi hosts. debug is not a valid CLI command for packet capture on the ESXi node, as it is a generic term that describes the process of finding and fixing errors, not a specific tool or command. set capture is not a valid CLI command for packet capture on the ESXi node, as it does not exist in the ESXi CLI.

Question 5

Question Type: MultipleChoice

Which choice is a valid insertion point for North-South network introspection?

Options:

- A- Guest VM vNIC
- B- Partner SVM
- C- Tier-0 gateway
- D- Host Physical NIC

Answer:

B

Explanation:

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

Question 6

Question Type: MultipleChoice

Which CLI command shows syslog on NSX Manager?

Options:

A- get log-file auth.lag

B- /var/log/syslog/syslog.log

C- show log manager follow

D- get log-file syslog

Answer:

D

Explanation:

According to the VMware NSX CLI Reference Guide, this CLI command shows the syslog messages on the NSX Manager node. You can use this command to view the system logs for troubleshooting or monitoring purposes.

The other options are either incorrect or not available for this task. `get log-file auth.log` is a CLI command that shows the authentication logs on the NSX Manager node, not the syslog messages. `/var/log/syslog/syslog.log` is not a CLI command, but a file path that may contain syslog messages on some Linux systems, but not on the NSX Manager node. `show log manager follow` is not a valid CLI command, as there is no `show log` command or `manager` option in the NSX CLI.

Question 7

Question Type: MultipleChoice

Which is an advantages of a L2 VPN In an NSX 4.x environment?

Options:

- A- Enables Multi-Cloud solutions
- B- Achieve better performance
- C- Enables VM mobility with re-IP
- D- Use the same broadcast domain

Answer:

D

Explanation:

L2 VPN is a feature of NSX that allows extending Layer 2 networks across different sites or clouds over an IPsec tunnel. L2 VPN has an advantage of enabling VM mobility with re-IP, which means that VMs can be moved from one site to another without changing their IP addresses or network configurations. This is possible because L2 VPN allows both sites to use the same broadcast domain, which means that they share the same subnet and VLAN .

Question 8

Question Type: MultipleChoice

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.)

Options:

- A- RADIUS 2.0
- B- Keycloak Enterprise
- C- RSA SecurID
- D- LDAP and OpenLDAP based on Active Directory (AD)
- E- SecureDAP

Answer:

C, D

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 .

To Get Premium Files for 2V0-41.23 Visit

<https://www.p2pexams.com/products/2v0-41.23>

For More Free Questions Visit

<https://www.p2pexams.com/vmware/pdf/2v0-41.23>

