Free Questions for 2V0-41.23 by braindumpscollection

Shared by Perez on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which NSX feature can be leveraged to achieve consistent policy configuration and simplicity across sites?

Options:

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.

Question 2

Question Type: MultipleChoice

Which three security features are dependent on the NSX Application Platform? (Choose three.)

Options:

A- NSX Firewall

B- NSX TLS Inspection

C- NSX Distributed IDS/IPS

D- NSX Intelligence

E- NSX Malware Prevention

F- NSX Network Detection and Response

Answer:

A, C, F

Explanation:

According to the VMware NSX Documentation, these are three of the security features that are dependent on the NSX Application Platform:

NSX Firewall: This feature provides distributed firewalling and micro-segmentation capabilities for network and application security. It allows you to create and enforce granular firewall rules based on various criteria such as identity, context, or tags.

NSX Distributed IDS/IPS: This feature provides distributed intrusion detection and prevention capabilities for network and application security. It allows you to detect and block malicious traffic based on signatures, behaviors, or anomalies.

NSX Network Detection and Response: This feature provides advanced threat detection and response capabilities for network and application security. It includes features such as Distributed Intrusion Detection and Prevention (IDS/IPS), Web Reputation Analysis, File and Process Analysis, and NSX Advanced Threat Prevention.

Question 3

Question Type: MultipleChoice

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.)

Options:

A- Reflexive NAT

B- Destination NAT

C- 1:1 NAT

D- Port NAT

E- Source NAT

Answer:

B, E

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.

Question 4

Question Type: MultipleChoice

What must be configured on Transport Nodes for encapsulation and decapsulation of Geneve protocol?

Options:

A- VXIAN

B- UDP

C- STT

D- TEP

Answer:

D

Explanation:

According to the VMware NSX Documentation, TEP stands for Tunnel End Point and is a logical interface that must be configured on transport nodes for encapsulation and decapsulation of Geneve protocol. Geneve is a tunneling protocol that encapsulates the original packet with an outer header that contains metadata such as the virtual network identifier (VNI) and the transport node IP address. TEPs are responsible for adding and removing the Geneve header as the packet traverses the overlay network.

Question 5

Question Type: MultipleChoice

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

Options:

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.

Question 6

Question Type: **MultipleChoice**

An administrator has deployed 10 Edge Transport Nodes in their NSX Environment, but has forgotten to specify an NTP server during the deployment.

What is the efficient way to add an NTP server to all 10 Edge Transport Nodes?

Options:

A- Use Transport Node Profile

B- Use the CU on each Edge Node

C- Use a Node Profile

D- Use a PowerCU script

Answer:

C

Explanation:

A node profile is a configuration template that can be applied to multiple NSX Edge nodes or transport nodes at once.A node profile can include settings such as NTP server, DNS server, syslog server, and so on1.By using a node profile, an administrator can efficiently configure or update the network settings of multiple NSX Edge nodes or transport nodes in a single operation2. The other options are incorrect because they are either not efficient or not supported. Using the CLI on each Edge node would require manual and repetitive commands for each node, which is not efficient.Using a Transport Node Profile would not work, because a Transport Node Profile is used to configure the NSX-T Data Center components on a transport node, such as the transport zone, the N-VDS, and the uplink profiles3. Using a PowerCLI script might work, but it would require writing and testing a custom script, which is not as efficient as using a built-in feature like a node profile.

Question 7

Question Type: MultipleChoice

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?

Options:

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.

Question 8

Question Type: MultipleChoice

Which two are requirements for FQDN Analysis? (Choose two.)

Options:

A- A layer 7 gateway firewall rule must be configured on the Tfer-1 gateway uplink.

B- ESXI control panel requires access to the Internet to download category and reputation definitions.

C- The NSX Manager requires access to the Internet to download category and reputation definitions.

D- The NSX Edge nodes require access to the Internet to download category and reputation definitions.

E- A layer 7 gateway firewall rule must be configured on the Tier-0 gateway uplink.

Answer:

C, E

Explanation:

According to the VMware NSX Documentation, these are two of the requirements for FQDN Analysis, which is a feature that allows you to monitor and control the traffic based on the fully qualified domain names (FQDNs) of the websites that your workloads access:

The NSX Manager requires access to the Internet to download category and reputation definitions: The NSX Manager periodically downloads the latest category and reputation definitions from a cloud service provider and distributes them to the NSX Edge nodes. These definitions are used to classify and score the FQDNs based on their content and risk level.

A layer 7 gateway firewall rule must be configured on the Tier-0 gateway uplink: You need to configure a layer 7 gateway firewall rule on the tier-0 gateway uplink interface that matches the traffic that you want to analyze based on FQDNs. You also need to enable FQDN Analysis on the firewall rule and select the categories and reputations that you want to allow or deny.

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

20%
DISCOUNT