killexams.com

Vmware

2V0-41.23

VMware NSX 4.x Professional

ORDER FULL VERSION

Question: 9

An NSX administrator is creating a Tier-1 Gateway configured In Active-Standby High Availability Mode. In the event of node failure, the failover policy should not allow the original tailed node to become the Active node upon recovery.

Which failover policy meets this requirement?

A. Non-Preemptive
B. Preemptive
C. Enable Preemptive
D. Disable Preemptive

Answer: A

Explanation:

According to the VMware NSX Documentation, a non-preemptive failover policy means that the original failed node will not become the active node upon recovery, unless the current active node fails again. This policy can help avoid unnecessary failovers and ensure stability.

The other options are either incorrect or not available for this configuration. Preemptive is the opposite of non-preemptive, meaning that the original failed node will become the active node upon recovery, if it has a higher priority than the current active node. Enable Preemptive and Disable Preemptive are not valid options for the failover policy, as the failover policy is a drop-down menu that only has two choices: Preemptive and Non-Preemptive.

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:

```
sa-nsxedge-01> get gateways

Logical Router

UUID                                    VRF     GW-ID     Name          Type

Ports

736a80e3-23f6-5a2d-91d6-bbefb2786666    0       0                       TUNNEL                        3

B10ef54e-d5f3-49e5-99b7-8a51366d0592    1       1025      SR-T1-LR-01   SERVICE_ROUTER_TIER1          6

5a5ddd63-3764-4d28-b92e-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
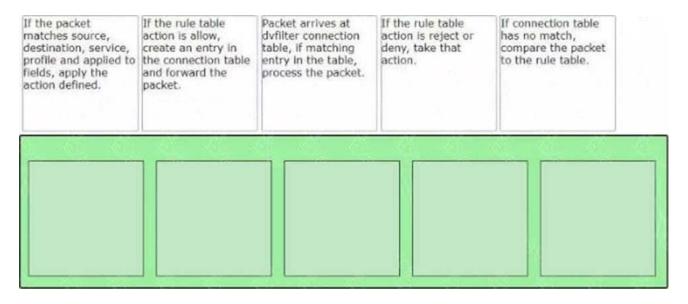F. vrf 3

Answer: B,D

Explanation:

According to the image that you sent, the BGP neighbor is configured on the tier-0 gateway with the UUID 9f8e3a7c-5f9c-4d1a-bb6f-9c7f3d6f3d63 and the VRF ID 4. Therefore, to check the BGP neighbor status, you need to enter the VRF context of 4 and execute the get bgp neighbor command on the tier-0 service router (SR) node.

The other options are either incorrect or not applicable for this scenario. vrf 1, vrf 3, and sa-nexedge-01(tier1_dr)> get bgp neighbor are not related to the BGP neighbor configuration on the tier-0 gateway. sa-nexedge-01(tier1_sr> get bgp neighbor is also not relevant, as there is no BGP neighbor configured on the tier-1 gateway.

Question: 11

Sort the rule processing steps of the Distributed Firewall. Order responses from left to right.

If the packet matches source, destination, service, profile and applied to fields, apply the action defined.	If the rule table action is allow, create an entry in the connection table and forward the packet.	Packet arrives at dvfilter connection table, if matching entry in the table, process the packet.	If the rule table action is reject or deny, take that action.	If connection table has no match, compare the packet to the rule table.

- wrong

Answer: B,D

Question: 12

Which TraceFlow traffic type should an NSX administrator use tor validating connectivity between App and DB virtual machines that reside on different segments?

A. Multicast
B. Unkrast
C. Anycast
D. Broadcast

Answer: C

Explanation:

According to the VMware NSX Documentation1, TraceFlow supports four types of traffic: Unicast, Broadcast, Multicast, and Anycast. Unicast traffic is sent to a specific destination IP address. Broadcast traffic is sent to all hosts on a network segment. Multicast traffic is sent to a group of hosts that have joined a multicast group. Anycast traffic is sent to the nearest or best destination among a group of hosts that share the same IP address.

Anycast traffic is useful for validating connectivity between virtual machines that reside on different segments, because it can test the routing and firewall rules that apply to the traffic. Anycast traffic can also help identify the optimal path for the traffic based on factors such as latency, bandwidth, and load balancing.

Question: 13

Which two logical router components span across all transport nodes? (Choose two.)

A. SFRVICE_ROUTER_TJER0
B. TIERO_DISTRI BUTE D_ ROUTER
C. D1STRIBUTED_R0UTER_TIER1
D. DISTRIBUTED_ROUTER_TIER0
E. SERVICE_ROUTER_TIERl

Answer: B,C

Explanation:

According to the VMware NSX 4.x Professional documents and tutorials, NSX-T has two logical router components, namely the Services Router (SR) and the Distributed Router (DR). As the names imply, SR is where centralized services are provisioned such as NAT, DHCP, VPN, Perimeter Firewall, Load Balancing, etc., and DR performs distributed routing across all hosts participating in a given transport zone3. The DR component is present in both Tier-0 and Tier-1 logical routers, while the SR component is only present in Tier-1 logical routers or in active-standby mode of Tier-0 logical routers4. Therefore, the logical router components that span across all transport nodes are TIER0_DISTRIBUTED_ROUTER and DISTRIBUTED_ROUTER_TIER1.

Question: 14

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

A)

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

B)

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

C)

```
esxcli network ip connection list | grep 1235
```

D)

```
esxcli network connection list | grep 1235
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

Explanation:

According to the web search results, the command that is used to test management connectivity from a transport node to NSX Manager is get managers. This command displays the status, IP address, and thumbprint of the NSX Manager that the transport node is connected to. It also shows the connection state, which can be UP or DOWN. If the connection state is DOWN, it means that there is a problem with the management connectivity.

Question: 15

Which two of the following features are supported for the Standard NSX Application Platform Deployment? (Choose two.)

A. NSX Intrusion Detection and Prevention
B. NSX Intelligence
C. NSX Network Detection and Response
D. NSX Malware Prevention Metrics
E. NSX Intrinsic Security

Answer: C,E

Explanation:

According to the VMware NSX Documentation, these are two of the features that are supported for the Standard NSX Application Platform Deployment:

- 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.

- NSX Intrinsic Security: This feature provides built-in security for applications and workloads across clouds. It includes features such as Distributed Firewall, Identity Firewall, Service Insertion, Micro-segmentation, and Policy-based Automation.

Question: 16

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

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: 17

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

A. esxcfg-nics -1
B. excli network nic list
C. esxcli network vswitch dvs wmare list
D. esxcfg-vmknic -1
E. esxcfg-vmsvc/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: 18

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.

Question: 19

An NSX administrator wants to create a Tler-0 Gateway to support equal cost multi-path (ECMP) routing.

Which failover detection protocol must be used to meet this requirement?

A. Bidirectional Forwarding Detection (BFD)
B. Virtual Router Redundancy Protocol (VRRP)
C. Beacon Probing (BP)
D. Host Standby Router Protocol (HSRP)

Answer: A

Explanation:

According to the VMware NSX 4.x Professional documents and tutorials, BFD is a failover detection protocol that provides fast and reliable detection of link failures between two routing devices. BFD can be used with ECMP routing to monitor the health of the ECMP paths and trigger a route change in case of a failure12. BFD is supported by both BGP and OSPF routing protocols in NSX-T3. BFD can also be configured with different timers to achieve different detection times3.

Question: 20

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 âEnabledâ. 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 âEnabledâ if the integration is successful. The other options are either incorrect or not relevant.

These questions are for demo purpose only. **Full version** *is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

ORDER FULL VERSION
Special Discount Coupon

Actual Exam Questions: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.

Exam Dumps: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.

Practice Tests: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.

Updated Content: Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.

Technical Support: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.