Vendor: VMware

Exam Code: 2V0-41.23

Exam Name: VMware NSX 4.x Professional

Version: DEMO

QUESTION 1
Which three of the following describe the Border Gateway Routing Protocol (BGP) configuration on a Tier-0 Gateway? (Choose three.)

A. It supports a 4-byte autonomous system number.
B. The network is divided into areas that are logical groups.
C. Can be used as an Exterior Gateway Protocol.
D. BGP is enabled by default.
E. EIGRP is disabled by default.

Answer: ACE
Explanation:
A. It supports a 4-byte autonomous system number. - BGP supports both 2-byte and 4-byte autonomous system numbers, but 4-byte autonomous system numbers are more common.
C. Can be used as an Exterior Gateway Protocol. - BGP is an Exterior Gateway Protocol (EGP), which means that it can be used to exchange routing information between different autonomous systems.
E. EIGRP is disabled by default. - EIGRP (Enhanced Interior Gateway Routing Protocol) is an Interior Gateway Protocol (IGP), which means that it is used to exchange routing information within an autonomous system. EIGRP is disabled by default on Tier-0 Gateways in NSX.

QUESTION 2
Which is an advantages of a L2 VPN in an NSX 4.x environment?

A. Enables Multi-Cloud solutions
B. Enables VM mobility with re-IP
C. Achieve better performance
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 3
Which NSX feature can be leveraged to achieve consistent policy configuration and simplicity across sites?

A. NSX HTML5 UI
B. Ethernet VPN
C. VRF Lite
D. NSX Federation

Answer: D
Explanation:
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 4
Which two choices are use cases for Distributed Intrusion Detection? (Choose two.)

A. Identify risk and reputation of accessed websites.
B. Quarantine workloads based on vulnerabilities.
C. Gain insight about micro-segmentation traffic flows.
D. Identify security vulnerabilities in the workloads.
E. Use agentless antivirus with Guest Introspection.

Answer: BD
Explanation:
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 5
Which command is used to set the NSX Manager's logging-level to debug mode for troubleshooting?

A. set service manager logging-level debug
B. set service nsx-manager logging-level debug
C. set service nsx-manager log-level debug
D. set service manager log-level debug

Answer: A
Explanation:
The CLI command to set the log level of the NSX Manager to debug mode is set service manager logging-level debug. This command can be used when the NSX UI is inaccessible or when troubleshooting issues with the NSX Manager. The other commands are incorrect because they either use a wrong syntax or a wrong service name. The NSX Manager service name is manager, not nsx-manager. The log level parameter is logging-level, not log-level.

QUESTION 6
What are two valid BGP Attributes that can be used to influence the route path traffic will take? (Choose two.)

A. AS-Path Prepend
B. Cost
C. BFD
D. MED

Answer: AD
Explanation:
AS-Path Prepend: This attribute allows you to prepend one or more AS numbers to the AS path of a route, making it appear longer and less preferable to other BGP routers. You can use this attribute to manipulate the inbound traffic from your BGP peers by advertising a longer AS path for some routes and a shorter AS path for others .

MED: This attribute stands for Multi-Exit Discriminator and allows you to specify a preference value for a route among multiple exit points from an AS. You can use this attribute to manipulate the outbound traffic to your BGP peers by advertising a lower MED value for some routes and a higher MED value for others .

QUESTION 7
What must be configured on Transport Nodes for encapsulation and decapsulation of Geneve protocol?

A. STT
B. TEP
C. UDP
D. VXLAN

Answer: B
Explanation:
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 8
An NSX administrator would like to export syslog events that capture messages related to NSX host preparation events.
Which message ID (msgid) should be used in the syslog export configuration command as a filter?

A. MONITORING
B. GROUPING
C. FABRIC
D. SYSTEM

Answer: C
Explanation:
The FABRIC message ID (msgld) captures messages related to NSX host preparation events, such as installation, upgrade, or uninstallation of NSX components on ESXi hosts. The syslog export configuration command for NSX host preparation events would look something like this:

set service syslog export FABRIC

The other options are either incorrect or not relevant for NSX host preparation events. MONITORING captures messages related to NSX monitoring features, such as alarms and system events. SYSTEM captures messages related to NSX system events, such as login, logout, or configuration changes. GROUPING captures messages related to NSX grouping objects, such as security groups, security tags, or IP sets.

QUESTION 9
An NSX administrator wants to create a Tier-0 Gateway to support equal cost multi-path (ECMP) routing.
Which failover detection protocol must be used to meet this requirement?

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

Answer: B
Explanation:
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 failure. BFD is supported by both BGP and OSPF routing protocols in NSX-T. BFD can also be configured with different timers to achieve different detection times.

QUESTION 10
A company is deploying NSX micro-segmentation in their vSphere environment to secure a simple application composed of web, app, and database tiers.
The naming convention will be:

```
WKS-WEB-SRV-XXX
WKY-APP-SRR-XXX
WKI-DB-SRR-XXX
```

What is the optimal way to group them to enforce security policies from NSX?

A. Use Edge as a firewall between tiers.
B. Group all by means of tags membership.
C. Create an Ethernet based security policy.
D. Do a service insertion to accomplish the task.

Answer: B
Explanation:
This can be done by creating tags for each tier, such as WKS-WEB-SRV, WKY-APP-SRR, and WKI-DB-SRR, and then applying those tags to the corresponding virtual machines.
Once the virtual machines have been tagged, you can create security policies that target the tags. For example, you could create a policy that allows traffic from the WKS-WEB-SRV tag to the WKY-APP-SRR tag, but blocks traffic from the WKY-APP-SRR tag to the WKI-DB-SRR tag.
This approach is scalable and flexible, and it allows you to easily enforce security policies across multiple applications.

QUESTION 11
An NSX administrator is creating a NAT rule on a Tier-0 Gateway configured in active-standby high availability mode.
Which two NAT rule types are supported for this configuration? (Choose two.)

A. Destination NAT
B. Reflexive NAT
C. Port NAT
D. Source NAT
E. 1:1 NAT

Answer: AD
Explanation:

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 12
Which choice is a valid insertion point for North-South network introspection?

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

Answer: A
Explanation:
North-South network introspection is the process of inspecting traffic flowing between the NSX environment and the external network. This can be done using a variety of security tools, such as firewalls, intrusion detection systems, and data loss prevention systems.
The Tier-0 gateway is the ideal place to insert North-South network introspection tools because it is the single point of entry and exit for all traffic between the NSX environment and the external network. This allows the security tools to inspect all traffic, regardless of which Tier-1 gateway or segment the traffic is flowing to or from.

QUESTION 13
Where in the NSX UI would an administrator set the time attribute for a time-based Gateway Firewall rule?

A. There is no option in the NSX UI. It must be done via command line interface.
B. The option to set time-based rule is a clock icon in the policy.
C. The option to set time-based rule is a field in the rule itself.
D. The option to set time-based rule is a clock icon in the rule.

Answer: B
Explanation:
The clock icon appears on the firewall policy section that you want to have a time window. By clicking the clock icon, you can create or select a time window that applies to all the rules in that policy section. The other options are incorrect because they either do not exist or are not related to the time-based rule feature. There is no option to set a time-based rule in the rule itself, as it is a policy-level setting. There is also an option to set a time-based rule in the NSX UI, so it does not require using the command line interface.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**