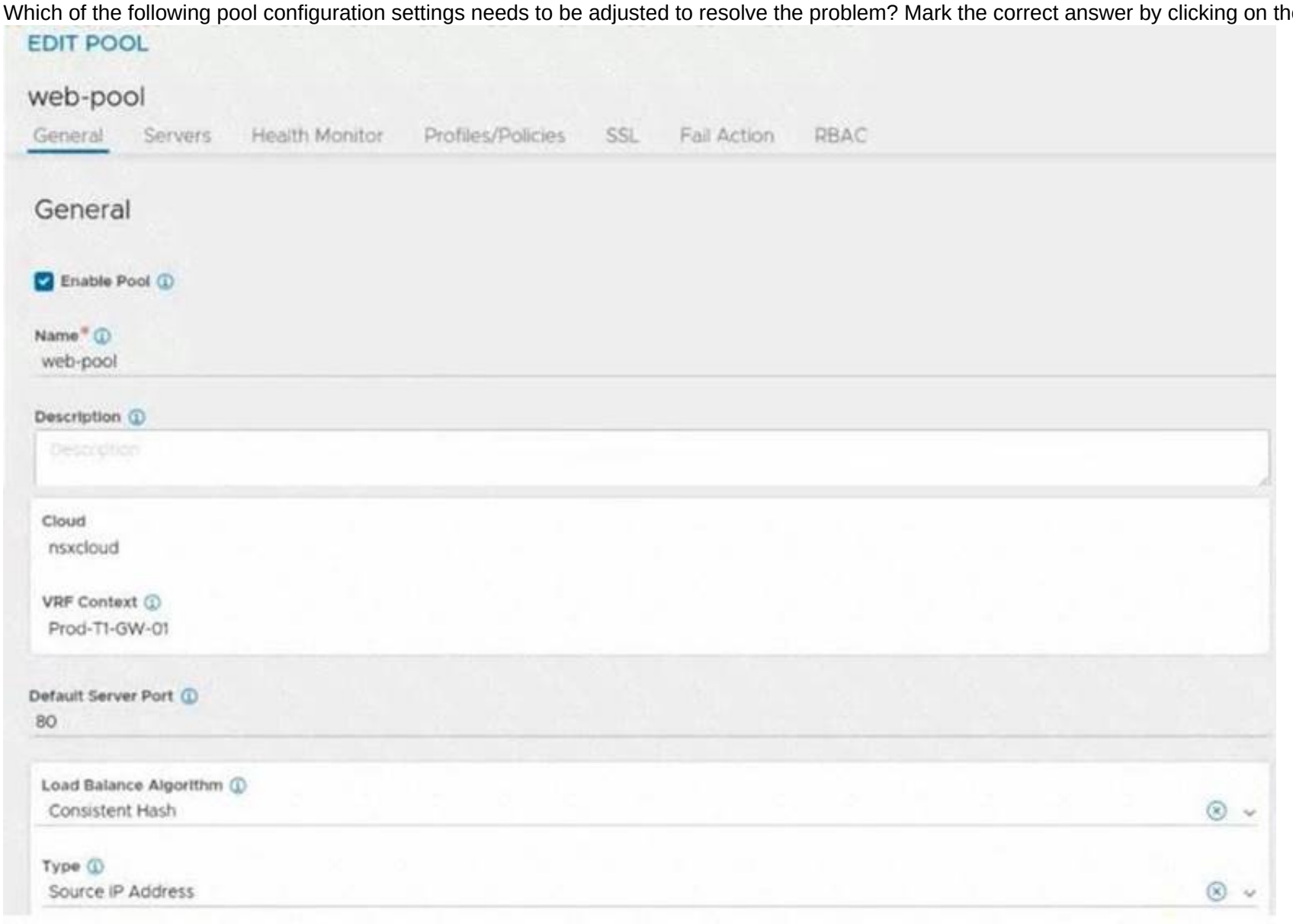
VMware

Exam Questions 2V0-41.23

VMware NSX 4.x Professional

NEW QUESTION 1
Refer to the exhibit.
An administrator configured NSX Advanced Load Balancer to redistribute the traffic between the web servers. However, requests are sent to only one server
Which of the following pool configuration settings needs to be adjusted to resolve the problem? Mark the correct answer by clicking on the image.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Load Balancing Algorithm

NEW QUESTION 2
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?

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-88

NEW QUESTION 3
What are the four types of role-based access control (RBAC) permissions? (Choose four.)

A. Read
B. None
C. Auditor
D. Full access
E. Enterprise Admin
F. Execute
G. Network Admin

Answer: ABDF

Explanation:
The four types of role-based access control (RBAC) permissions are Read, None, Full access, and Execu Read permission allows the user to view the configuration and status of the system. None permission denies any access to the system. Full access permission grants all permissions including Create, Read, Update, and Delete (CRUD). Execute permission includes Read and Update permissions1. Auditor, Enterprise Admin, and Network Admin are not types of permissions, but types of roles that have different sets of permissions. References: NSX Features
There are four types of permissions. Included in the list are the abbreviations for the permissions that are used in the Roles and Permissions and Roles and Permissions for Manager Mode tables.

- Full access (FA) - All permissions including Create, Read, Update, and Delete
- Execute (E) - Includes Read and Update
- Read (R)
- None

NSX-T Data Center has the following built-in roles. Role names in the UI can be different in the API.
In NSX-T Data Center, if you have permission, you can clone an existing role, add a new role, edit newly created roles, or delete newly created roles.
Role-Based Access Control (vmware.com)

NEW QUESTION 4
Which of the following settings must be configured in an NSX environment before enabling stateful active-active SNAT?

A. Tier-1 gateway in active-standby mode
B. Tier-1 gateway in distributed only mode
C. An Interface Group for the NSX Edge uplinks
D. A Punting Traffic Group for the NSX Edge uplinks

Answer: C

Explanation:
To enable stateful active-active SNAT on a Tier-0 or Tier-1 gateway, you must configure an Interface Group for the NSX Edge uplinks. An Interface Group is a logical grouping of NSX Edge interfaces that belong to the same failure domain. A failure domain is a set of NSX Edge nodes that share the same physical network infrastructure and are subject to the same network failures. By configuring an Interface Group, you can ensure that the stateful services are distributed across different failure domains and can recover from network failures1

NEW QUESTION 5
Which two of the following features are supported for the Standard NSX Application Platform Deployment? (Choose two.)

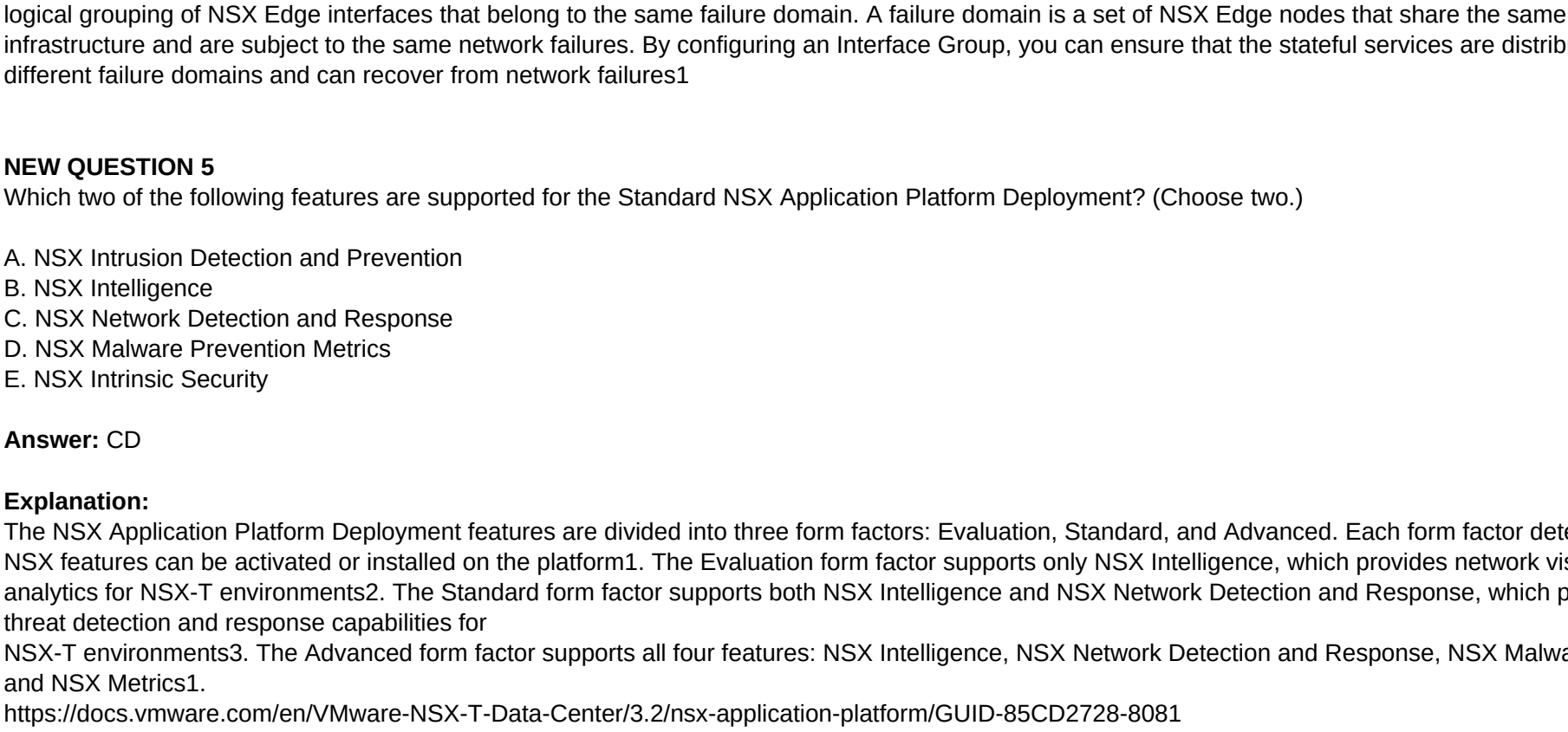
A. NSX Intrusion Detection and Prevention
B. NSX Intelligence
C. NSX Network Detection and Response
D. NSX Malware Prevention Metrics
E. NSX Intrinsic Security

Answer: CD

Explanation:
The NSX Application Platform Deployment features are divided into three form factors: Evaluation, Standard, and Advanced. Each form factor determines which NSX features can be activated or installed on the platform1. The Evaluation form factor supports only NSX Intelligence, which provides network visibility and analytics for NSX-T environments2. The Standard form factor supports both NSX Intelligence and NSX Network Detection and Response, which provides network threat detection and response capabilities for
NSX-T environments3. The Advanced form factor supports all four features: NSX Intelligence, NSX Network Detection and Response, NSX Malware Prevention, and NSX Metrics1.
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/nsx-application-platform/GUID-85CD2728-8081

NEW QUESTION 6
Refer to the exhibit.
An administrator configured NSX Advanced Load Balancer to load balance the production web server traffic, but the end users are unable to access the production website by using the VIP address.
Which of the following Tier-1 gateway route advertisement settings needs to be enabled to resolve the problem? Mark the correct answer by clicking on the image.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
The correct answer is to enable the option All LB VIP Routes on the Tier-1 gateway route advertisement settings. This option allows the Tier-1 gateway to advertise the NSX Advanced Load Balancer LB VIP routes to the Tier-0 gateway and other peer routers, so that the end users can reach the production website by using the VIP address1. The other options are not relevant for this scenario.
To mark the correct answer by clicking on the image, you can click on the toggle switch next to All LB VIP Routes to turn it on. The switch should change from gray to blue, indicating that the option is enabled. See the image below for reference:

NEW QUESTION 7
In which VPN type are the Virtual Tunnel interfaces (VTI) used?

A. Route & SSL based VPNs
B. Route-based VPN
C. Policy & Route based VPNs
D. SSL-based VPN

Answer: B

Explanation:
Route-based VPN is a VPN type that uses Virtual Tunnel interfaces (VTI) to establish IPSec tunnels between an NSX Edge node and remote sites2. A VTI is a logical interface that is assigned an IP address and is associated with a physical or virtual interface. The VTI acts as an end point of the IPSec tunnel and routes traffic between the NSX Edge node and the remote site2. Route & SSL based VPNs, Policy & Route based VPNs, and SSL-based VPN are not VPN types that use VTI. References: Virtual Private Network (VPN)

NEW QUESTION 8
How does the Traceflow tool identify issues in a network?

A. Compares the management plane configuration states containing control plane traffic and error reporting from transport node agents.
B. Compares intended network state in the control plane with Tunnel End Point (TEP) keepalives in the data plane.
C. Injects ICMP traffic into the data plane and observes the results in the control plane.
D. Injects synthetic traffic into the data plane and observes the results in the control plane.

Answer: D

Explanation:
The Traceflow tool identifies issues in a network by injecting synthetic traffic into the data plane and observing the results in the control plane. This allows the tool to identify any issues in the network and provide a detailed report on the problem. You can use the Traceflow tool to test connectivity between any two endpoints in your NSX-T Data Center environment.

NEW QUESTION 9
Where in the NSX UI would an administrator set the time attribute for a time-based Gateway Firewall rule?

A. The option to set time-based rule is a clock Icon in the rule.
B. The option to set time based rule is a field in the rule Itself.
C. There Is no option in the NSX U
D. It must be done via command line interface.
E. The option to set time-based rule is a clock Icon in the policy.

Answer: D

Explanation:
According to the VMware documentation1, 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.
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-8572496E-A60E-48C3-A016-4A081AC8

NEW QUESTION 10
Which three protocols could an NSX administrator use to transfer log messages to a remote log server? (Choose three.)

A. HTTPS
B. TCP
C. SSH
D. UDP
E. TLS
F. SSL

Answer: BDE

Explanation:
An NSX administrator can use TCP, UDP, or TLS protocols to transfer log messages to a remote log server. These protocols are supported by NSX Manager, NSX Edge, and hypervisors for remote logging. A Log Insight log server supports all these protocols, as well as LI and LI-TLS, which are specific to Log Insight and optimize network usage. HTTPS, SSH, and SSL are not valid protocols for remote logging in NSX-T Data Center. References: : VMware NSX-T Data Center Administration Guide, page 102. : VMware Docs: Configure Remote Logging

NEW QUESTION 10
Where does an administrator configure the VLANs used In VRF Lite? (Choose two.)

A. segment connected to the Tler-1 gateway
B. uplink trunk segment
C. downlink interface of the default Tier-0 gateway
D. uplink Interface of the VRF gateway
E. uplink interface of the default Tier-0 gateway

Answer: BD

Explanation:
According to the VMware NSX Documentation, these are the two places where you need to configure the VLANs used in VRF Lite:

- Uplink trunk segment: This is a segment that connects a tier-0 gateway to a physical network using multiple VLAN tags. You need to configure the VLAN IDs for each VRF on this segment.
- Uplink interface of the VRF gateway: This is an interface that connects a VRF gateway to an uplink trunk segment using a specific VLAN tag. You need to configure the VLAN ID for each VRF on this interface.

NEW QUESTION 14
When a stateful service is enabled for the first lime on a Tier-0 Gateway, what happens on the NSX Edge node'

A. SR is instantiated and automatically connected with DR.
B. DR Is instantiated and automatically connected with SR.
C. SR and DR Is instantiated but requites manual connection.
D. SR and DR doesn't need to be connected to provide any stateful services.

Answer: A

Explanation:
The answer is A. SR is instantiated and automatically connected with DR.
SR stands for Service Router and DR stands for Distributed Router. They are components of the NSX Edge node that provide different functions1
The SR is responsible for providing stateful services such as NAT, firewall, load balancing, VPN, and DHCP. The DR is responsible for providing distributed routing and switching between logical segments and the physical network1
When a stateful service is enabled for the first time on a Tier-0 Gateway, the NSX Edge node automatically creates an SR instance and connects it with the existing DR instance. This allows the stateful service to be applied to the traffic that passes through the SR before reaching the DR2
According to the VMware NSX 4.x Professional Exam Guide, understanding the SR and DR components and their functions is one of the exam objectives3
To learn more about the SR and DR components and how they work on the NSX Edge node, you can refer to the following resources:

- VMware NSX Documentation: NSX Edge Components 1
- VMware NSX 4.x Professional: NSX Edge Architecture
- VMware NSX 4.x Professional: NSX Edge Routing

NEW QUESTION 17
What are two functions of the Service Engines in NSX Advanced Load Balancer? (Choose two.)

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: CE

Explanation:
The Service Engines in NSX Advanced Load Balancer are VM-based applications that handle all data plane operations by receiving and executing instructions from the Controller. The Service Engines perform the following functions:

- They perform application load-balancing operations for all client- and server-facing network interactions. They support various load-balancing algorithms, health monitors, SSL termination, and persistence profiles.
- They provide a user interface to perform configuration and management tasks. The user interface is accessible through a web browser or a REST API. The user interface allows the user to create and modify virtual services, pools, health monitors, policies, analytics, and other load-balancing settings
https://docs.vmware.com/en/VMware-Telco-Cloud-Platform/3.0/vmware-telco-cloud-reference-architecture-gui

NEW QUESTION 18
Which two are requirements for FQDN Analysis? (Choose two.)

A. The NSX Edge nodes require access to the Internet to download category and reputation definitions.
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. A layer 7 gateway firewall rule must be configured on the Tier-1 gateway uplink.
E. A layer 7 gateway firewall rule must be configured on the Tier-0 gateway uplink.

Answer: AD

Explanation:
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-C5CD87FD-8095-49F3-97CE-E606AB89

NEW QUESTION 22
NSX improves the security of today's modern workloads by preventing lateral movement, which feature of NSX can be used to achieve this?

A. Network Segmentation
B. Virtual Security Zones
C. Edge Firewalling
D. Dynamic Routing

Answer: A

Explanation:
According to the web search results, network segmentation is a feature of NSX that improves the security of today’s modern workloads by preventing lateral movement. Lateral movement is a technique used by attackers to move from one compromised system to another within a network, exploiting vulnerabilities or credentials . Network segmentation prevents lateral movement by dividing a network into smaller segments or zones, each with its own security policies and controls. This way, if one segment is compromised, the attacker cannot access other segments or resources . NSX enables network segmentation by using micro-segmentation, which applies granular firewall rules at the virtual machine level, regardless of the physical network topology .

NEW QUESTION 27
The security administrator turns on logging for a firewall rule. Where is the log stored on an ESXi transport node?

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-A

NEW QUESTION 30
An administrator has a requirement to have consistent policy configuration and enforcement across NSX instances.
What feature of NSX fulfills this requirement?

A. Load balancer
B. Federation
C. Multi-hypervisor support
D. Policy-driven configuration

Answer: B

Explanation:
Federation is a feature of NSX that allows the administrator to manage multiple NSX instances with a single pane of glass view, create gateways and segments that span one or more locations, and configure and enforce firewall rules consistently across locations1. Federation provides centralized policy management for security and networking services for all locations and pushes it down to NSX Local Managers at the respective sites for enforcement1. Federation also enables disaster recovery and workload mobility scenarios by providing consistent network and security policies across different sites1. References: 1: NSX Federation - VMware Docs(https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-D5B6DC79-6733-44

NEW QUESTION 32
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?

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

NEW QUESTION 34
Which two logical router components span across all transport nodes? (Choose two.)

A. SFRVICE_ROUTER_TJER0
B. TIERO_DISTRI BUTE D_ ROUTER
C. DISTRIBUTED_R0UTER_TIER1
D. DISTRIBUTED_ROUTER_TIER0
E. SERVICE_ROUTER_TIERl

Answer: CD

Explanation:
https://docs.vmware.com/en/VMware-Validated-Design/5.0.1/com.vmware.vvd.sddc-nsxt-design.doc/GUID-74

NEW QUESTION 35
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.

NEW QUESTION 39
Which two statements are correct about East-West Malware Prevention? (Choose two.)

A. A SVM is deployed on every ESXi host.
B. NSX Application Platform must have Internet access.
C. An agent must be installed on every ESXi host.
D. An agent must be installed on every NSX Edge node.
E. NSX Edge nodes must have Internet access.

Answer: AE

Explanation:
East-West Malware Prevention is a feature of NSX Advanced Threat Prevention that can detect and prevent malicious files in the network traffic between virtual machines (east-west) and between the data center and the external network (north-south). To enable this feature, a Service Virtual Machine (SVM) is deployed on every ESXi host to intercept and analyze the files in the east-west traffic. An agent must also be installed on every NSX Edge node to intercept and analyze the files in the north-south traffic. The NSX Application Platform is a cloud-based service that provides threat intelligence and analysis for the NSX Malware Prevention feature. The NSX Application Platform must have Internet access to receive updates and send files for analysis. The NSX Edge nodes must also have Internet access to communicate with the NSX Application Platform.
References:
- Overview of NSX IDS/IPS and NSX Malware Prevention
- Administering NSX Malware Prevention

NEW QUESTION 42
An NSX administrator would like to export syslog events that capture messages related to NSX host preparation events. Which message ID (msgld) should be used in the syslog export configuration command as a filler?

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

Answer: D

Explanation:
According to the VMware NSX Documentation2, 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 events2. SYSTEM captures messages related to NSX system events, such as login, logout, or configuration changes2. GROUPING captures messages related to NSX grouping objects, such as security groups, security tags, or IP sets2.
https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-CC18C0E3-D076-41AA-8B8C-133650FD

NEW QUESTION 47
When collecting support bundles through NSX Manager, which files should be excluded for potentially containing sensitive information?

A. Controller Files
B. Management Files
C. Core Files
D. Audit Files

Answer: C

Explanation:
According to the VMware NSX Documentation1, core files and audit logs can contain sensitive information and should be excluded from the support bundle unless requested by VMware technical support. Controller files and management files are not mentioned as containing sensitive information.

NEW QUESTION 51
Which three security features are dependent on the NSX Application Platform? (Choose three.)

A. NSX Intelligence
B. NSX Firewall
C. NSX Network Detection and Response
D. NSX TLS Inspection
E. NSX Distributed IDS/IPS
F. NSX Malware Prevention

Answer: ACF

Explanation:
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/nsx-application-platform/GUID-42EDE0AD-CD

NEW QUESTION 56
A customer is preparing to deploy a VMware Kubernetes solution in an NSX environment. What is the minimum MTU size for the UPLINK profile?

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). References: : 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.

NEW QUESTION 60
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. BFD
C. Cost
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 .

NEW QUESTION 65
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

2V0-41.23 Practice Exam Features:

* 2V0-41.23 Questions and Answers Updated Frequently

* 2V0-41.23 Practice Questions Verified by Expert Senior Certified Staff

* 2V0-41.23 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 2V0-41.23 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year