

VMware

Exam Questions 2V0-41.23

VMware NSX 4.x Professional



NEW QUESTION 1

What are two valid options when configuring the scope of a distributed firewall rule? (Choose two.)

- A. DFW
- B. Tier-1 Gateway
- C. Segment
- D. Segment Port
- E. Group

Answer: CE

Explanation:

* C. Segment. This is correct. A segment is a logical construct that represents a layer 2 broadcast domain and a layer 3 subnet in NSX. A segment can be used to group and connect virtual machines, containers, or bare metal hosts that belong to the same application or service. A segment can also be used as the scope of a distributed firewall rule, which means that the rule will apply to all the traffic that enters or exits the segment¹²

* E. Group. This is correct. A group is a logical construct that represents a collection of objects in NSX, such as segments, segment ports, virtual machines, IP addresses, MAC addresses, tags, or security policies. A group can be used to define dynamic membership criteria based on various attributes or filters. A group can also be used as the scope of a distributed firewall rule, which means that the rule will apply to all the traffic that matches the group membership criteria³²

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

Which field in a Tier-1 Gateway Firewall would be used to allow access for a collection of trustworthy web sites?

- A. Source
- B. Profiles -> Context Profiles
- C. Destination
- D. Profiles -> L7 Access Profile

Answer: D

Explanation:

The field in a Tier-1 Gateway Firewall that would be used to allow access for a collection of trustworthy web sites is Profiles -> L7 Access Profile. This field allows the user to create a Layer 7 access profile that defines list of allowed or blocked URLs based on categories, reputation, or custom entries¹. The user can then apply the L7 access profile to a firewall rule to control the traffic based on the URL filtering criteria¹. The other options are incorrect because they are not related to URL filtering. The Source field specifies the source IP address or group of the firewall rule¹. The Destination field specifies the destination IP address or group of the firewall rule¹. The Profiles -> Context Profiles field allows the user to create a context profile that defines a list of application signatures or attributes that can be used to identify and classify network traffic¹. References: Gateway Firewall

NEW QUESTION 4

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.)

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

Answer: CD

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 .

<https://blogs.vmware.com/networkvirtualization/2017/11/remote-user-authentication-and-rbac-with-nsx-t.html>

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

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 7

Which table on an ESXi host is used to determine the location of a particular workload for a frame-forwarding decision?

- A. TEP Table
- B. MAC Table
- C. ARP Table
- D. Routing Table

Answer: B

Explanation:

The MAC table on an ESXi host is used to determine the location of a particular workload for a frame-forwarding decision. The MAC table maps the MAC addresses of the workloads to their corresponding tunnel endpoint (TEP) IP addresses. The TEP IP address identifies the ESXi host where the workload resides. The MAC table is populated by learning the source MAC addresses of the incoming frames from the workloads. The MAC table is also synchronized with other ESXi hosts in the same transport zone by using the NSX Controller.

<https://nsx.techzone.vmware.com/resource/nsx-reference-design-guide>

NEW QUESTION 8

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 UI
- 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 9

Which two of the following are used to configure Distributed Firewall on VDS? (Choose two.)

- A. vSphere API
- B. NSX API
- C. NSX CU
- D. vCenter API
- E. NSX UI

Answer: BE

Explanation:

According to the VMware NSX Documentation, these are two of the ways that you can use to configure Distributed Firewall on VDS:

- NSX API: This is a RESTful API that allows you to programmatically configure and manage Distributed Firewall on VDS using HTTP methods and JSON payloads. You can use tools such as Postman or curl to send API requests to the NSX Manager node.
- NSX UI: This is a graphical user interface that allows you to configure and manage Distributed Firewall on VDS using menus, tabs, buttons, and forms. You can access the NSX UI by logging in to the NSX Manager node using a web browser.

<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-0DEF9F18-608D-4B5C-9175-5514750E9>

NEW QUESTION 10

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 1235`
- C. `esxcli network ip connection list | grep 1235`
- D. `esxcli network connection list | grep 1234`

Answer: A

Explanation:

The NSX Manager management plane communicates with the transport nodes by using APH Server over NSX-RPC/TCP through port 1234. CCP communicates with the transport nodes by using APH Server over NSX-RPC/TCP through port 1235.

NEW QUESTION 10

Which three data collection sources are used by NSX Network Detection and Response to create correlations/Intrusion campaigns? (Choose three.)

- A. Files and anti-malware (file events from the NSX Edge nodes and the Security Analyzer)
- B. East-West anti-malware events from the ESXi hosts
- C. Distributed Firewall flow data from the ESXi hosts
- D. IDS/IPS events from the ESXi hosts and NSX Edge nodes
- E. Suspicious Traffic Detection events from NSX Intelligence

Answer: ADE

Explanation:

The correct answers are A. Files and anti-malware (file) events from the NSX Edge nodes and the Security Analyzer, D. IDS/IPS events from the ESXi hosts and NSX Edge nodes, and E. Suspicious Traffic Detection events from NSX Intelligence. According to the VMware NSX Documentation³, these are the three data collection sources that are used by NSX Network Detection and Response to create correlations/intrusion campaigns.

The other options are incorrect or not supported by NSX Network Detection and Response. East-West anti-malware events from the ESXi hosts are not collected by NSX Network Detection and

Response³. Distributed Firewall flow data from the ESXi hosts are not used for correlation/intrusion campaigns by NSX Network Detection and Response³.

<https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-14BBE50D-9931-4719-8F>

NEW QUESTION 13

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

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

Answer: C

Explanation:

A valid insertion point for North-South network introspection is Tier-0 gateway. North-South network introspection is a service insertion feature that allows third-party network services to be integrated with

NSX. North-South network introspection enables traffic redirection from the uplink of an NSX Edge node to a service chain that consists of one or more service profiles¹. The Tier-0 gateway is the logical router that connects the NSX Edge node to the physical network and provides North-South routing and network services².

<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-D5933474-34A2-4DCE-AE9B-A82FF33>

NEW QUESTION 14

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 19

An architect receives a request to apply distributed firewall in a customer environment without making changes to the network and vSphere environment. The architect decides to use Distributed Firewall on VDS.

Which two of the following requirements must be met in the environment? (Choose two.)

- A. vCenter 8.0 and later
- B. NSX version must be 3.2 and later
- C. NSX version must be 3.0 and later
- D. VDS version 6.6.0 and later

Answer: BD

Explanation:

Distributed Firewall on VDS is a feature of NSX-T Data Center that allows users to install Distributed Security for vSphere Distributed Switch (VDS) without the need to deploy an NSX Virtual Distributed Switch (N-VDS). This feature provides NSX security capabilities such as Distributed Firewall (DFW), Distributed IDS/IPS, Identity Firewall, L7 App ID, FQDN Filtering, NSX Intelligence, and NSX Malware Prevention. To enable this feature, the following requirements must be met in the environment:

- The NSX version must be 3.2 and later¹. This is the minimum version that supports Distributed Security for VDS.
- The VDS version must be 6.6.0 and later¹. This is the minimum version that supports the NSX host preparation operation that activates the DFW with the default rule set to allow.

References:

- Overview of NSX IDS/IPS and NSX Malware Prevention

NEW QUESTION 24

An administrator is configuring service insertion for Network Introspection. Which two places can the Network Introspection be configured? (Choose two.)

- A. Host pNIC
- B. Partner SVM
- C. Tier-0 gateway
- D. Tier-1 gateway
- E. Edge Node

Answer: AB

Explanation:

Network Introspection is a service insertion feature that allows third-party network security services to monitor and analyze the traffic between virtual machines. Network Introspection can be configured on the host pNIC or on the partner SVM, depending on the type of service and the deployment model. The host pNIC configuration is used for services that require traffic redirection from the physical network to the service virtual machine. The partner SVM configuration is used for services that require traffic redirection from the virtual network to the service virtual machine. Network Introspection cannot be configured on the Tier-0 or Tier-1 gateways, as they are not part of the data plane where the service insertion occurs. Network Introspection also cannot be configured on the edge node, as it is a logical construct that hosts the Tier-0 and Tier-1 gateways. References: Distributed Service Insertion, NSX Securing “Anywhere” Part IV

NEW QUESTION 27

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 31

Which CLI command shows syslog on NSX Manager?

- 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.

NSX Cli command get log-file <filename>

get log-file <filename> follow

Below are commonly used log files, there are many more log files

get log-file <auth.log | controller | controller-error | http.log | kern.log | manager.log | node-mgmt.log | policy.log | syslog> [follow]

use [follow] to continuing monitor Example: get log-file syslog follow get log-file syslog

NEW QUESTION 35

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 .

NEW QUESTION 36

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

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.

NEW QUESTION 39

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 42

Which VPN type must be configured before enabling a L2VPN?

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.

<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-86C8D6BB-F185-46DC-828C-1E1876B8>

NEW QUESTION 45

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 vmk00 -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 VMware 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 46

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

- A. SFRVICE_ROUTER_TJERO
- B. TIERO_DISTRI BUTE D_ ROUTER
- C. DISTRIBUTED_ROUTER_TIER1
- D. DISTRIBUTED_ROUTER_TIER0
- E. SERVICE_ROUTER_TIER1

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 47

How is the RouterLink port created between a Tier-1 Gateway and Tier-0 Gateway?

- A. Manually create a Logical Switch and connect to both Tier-1 and Tier-0 Gateways.
- B. Automatically created when Tier-1 is created.
- C. Manually create a Segment and connect to both Tier-1 and Tier-0 Gateways.
- D. Automatically created when Tier-1 is connected with Tier-0 from NSX UI.

Answer: D

Explanation:

According to the VMware NSX 4.x Professional documents and tutorials, a RouterLink port is a logical port that connects a Tier-1 gateway to a Tier-0 gateway.

This port is automatically created when a Tier-1 gateway is associated with a Tier-0 gateway from the NSX UI or API. The RouterLink port enables routing between the two gateways and carries all the routing protocols and traffic. There is no need to manually create a logical switch or segment for this purpose1.

NEW QUESTION 52

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. SYSTEM
- C. GROUPING
- D. FABRIC

Answer: D

Explanation:

According to the VMware NSX Documentation2, the FABRIC message ID (msgid) 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 56

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 58

Which steps are required to activate Malware Prevention on the NSX Application Platform?

- A. Select Cloud Region and Deploy Network Detection and Response.
- B. Activate NSX Network Detection and Response and run Pre-checks.
- C. Activate NSX Network Detection and Response and Deploy Malware Prevention.
- D. Select Cloud Region and run Pre-checks.

Answer: D

Explanation:

To activate Malware Prevention on the NSX Application Platform, the steps are:

- In the NSX Manager UI, select System and in the Configuration section, select NSX Application Platform.
- Navigate to the Features section, locate the NSX Malware Prevention feature card, and click Activate or anywhere in the card.
- In the NSX Malware Prevention activation window, select one of the available cloud regions from which you can access the NSX Advanced Threat Prevention cloud service.
- Click Run Prechecks. This precheck process can take some time as the system validates that the minimum license requirement is met and that it is eligible for use with the NSX Advanced Threat Prevention cloud service. The system also validates that the selected cloud region is reachable.
- Click Activate. This step can take some time¹. Therefore, the correct answer is D. The other options are incorrect because they involve activating or deploying NSX Network Detection and Response, which is a different feature from Malware Prevention. References: Activate NSX Malware Prevention

NEW QUESTION 59

Which CLI command does an NSX administrator run on the NSX Manager to generate support bundle logs if the NSX UI is inaccessible?

- A. set support-bundle file vcpnv.tgz
- B. esxcli system syslog config logger set - -id=nsxmanager
- C. vm-support
- D. get support-bundle file vcpnv.tgz

Answer: D

Explanation:

To generate the support bundle logs on the NSX Manager via API, the NSX administrator needs to use the POST method with the URL https://nsxmgr_ip/api/1.0/appliance-management/techsupportlogs/NSX, where nsxmgr_ip is the IP address of the NSX Manager¹. This will create a tech support bundle file with a name like vcpnv.tgz. To download the generated tech support bundle file via CLI, the NSX administrator needs to use the get support-bundle file vcpnv.tgz command on the NSX Manager¹. The other commands are incorrect because they either do not generate or download the support bundle logs, or they are not related to the NSX Manager.

NEW QUESTION 62

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 66

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 67

An administrator has been tasked with implementing the SSL certificates for the NSX Manager Cluster VIP. Which is the correct way to implement this change?

- A. Send an API call to `https://<nsx-mgr>/api/v1/cluster/api-certificate? action=set_cluster_certificate&certificate_id=<certificate_id>` Send an API call to `https://<nsx-mgr>/api/v1/cluster/api-certificate?action=set_cluster_certificate&certificate_id=<certificate_id>`
- B. Send an API call to `https://<nsx-mgr>/api/v1/node/services/http? action=apply_certificate&certificate_id=<certificate_id>` Send an API call to `https://<nsx-mgr>/api/v1/node/services/http?action=apply_certificate&certificate_id=<certificate_id>`
- C. SSH as admin into the NSX manager with the cluster VIP IP and run `nsxcli cluster certificate vip install <certificate_id>` SSH as admin into the NSX manager with the cluster VIP IP and run `nsxcli cluster certificate vip install <certificate_id>`
- D. SSH as admin into the NSX manager with the cluster VIP IP and run `nsxcli cluster certificate node install <certificate_id>` SSH as admin into the NSX manager with the cluster VIP IP and run `nsxcli cluster certificate vip install <certificate_id>`

Answer: A

Explanation:









<https://docs.vmware.com/en/VMware-Validated-Design/5.0.1/com.vmware.vvd.sddc-nsxt-domain-deploy.doc/G>

NEW QUESTION 68

Refer to the exhibits.

Drag and drop the NSX graphic element icons on the left found in an NSX Intelligence visualization graph to its correct description on the right.

Answer Area

			This icon represents a physical server that is part of your NSX environment. A physical server can belong to more than one group.
			This icon represents a group on which security policies, including East-West firewall rules, can be applied. A group can be a collection of VMs, physical servers, or sets of IP addresses.
			This is the icon for the public IP addresses on the Internet. If at least one compute entity in your NSX environment communicated with a public IP address during the selected time period, that traffic flow is included in the current visualization.
			This is the icon used for a virtual machine (VM) that is part of your NSX environment. A VM can belong to more than one group.

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

<https://docs.vmware.com/en/VMware-NSX-Intelligence/4.0/user-guide/GUID-DC78552B-2CC4-410D-A6C9-3>

NEW QUESTION 71

• • • • •

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The 2V0-41.23 Practice Test Here](#)