

Exam Questions 2V0-41.23

VMware NSX 4.x Professional

<https://www.2passeasy.com/dumps/2V0-41.23/>



NEW QUESTION 1

Which three NSX Edge components are used for North-South Malware Prevention? (Choose three.)

- A. Thin Agent
- B. RAPID
- C. Security Hub
- D. IDS/IPS
- E. Security Analyzer
- F. Reputation Service

Answer: BCD

Explanation:

<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-69DF70C2-1769-4858-97E7-B757CAED>

NEW QUESTION 2

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 3

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

- A. Multicast
- B. Unicast
- C. Anycast
- D. Broadcast

Answer: B

Explanation:

Unicast is the traffic type that an NSX administrator should use for validating connectivity between App and DB virtual machines that reside on different segments. According to the VMware documentation¹, unicast traffic is the traffic type that is used to send a packet from one source to one destination. Unicast traffic is the most common type of traffic in a network, and it is used for applications such as web browsing, email, file transfer, and so on². To perform a traceflow with unicast traffic, the NSX administrator needs to specify the source and destination IP addresses, and optionally the protocol and related parameters¹. The traceflow will show the path of the packet across the network and any observations or errors along the way³. The other options are incorrect because they are not suitable for validating connectivity between two specific virtual machines. Multicast traffic is the traffic type that is used to send a packet from one source to multiple destinations simultaneously². Multicast traffic is used for applications such as video streaming, online gaming and group communication⁴. To perform a traceflow with multicast traffic, the NSX administrator needs to specify the source IP address and the destination multicast IP address¹. Broadcast traffic is the traffic type that is used to send a packet from one source to all devices on the same subnet². Broadcast traffic is used for applications such as ARP, DHCP, and network discovery. To perform a traceflow with broadcast traffic, the NSX administrator needs to specify the source IP address and the destination MAC address as FF:FF:FF:FF:FF:FF¹. Anycast traffic is not a valid option, as it is not supported by NSX Traceflow. Anycast traffic is a traffic type that is used to send a packet from one source to the nearest or best destination among a group of devices that share the same IP address. Anycast traffic is used for applications such as DNS, CDN, and load balancing.

NEW QUESTION 4

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 5

In an NSX environment, an administrator is observing low throughput and congestion between the Tier-0 Gateway and the upstream physical routers. Which two actions could address low throughput and congestion? (Choose two.)

- A. Configure NAT on the Tier-0 gateway.
- B. Configure ECMP on the Tier-0 gateway.
- C. Deploy Large size Edge node/s.
- D. Add an additional vNIC to the NSX Edge node.
- E. Configure a Tier-1 gateway and connect it directly to the physical routers.

Answer: BC

Explanation:

ECMP (Equal Cost Multi-Path) is a routing protocol that increases the north and south communication bandwidth by adding an uplink to the tier-0 logical router and configure it for each Edge node in an NSX Edge cluster². The ECMP routing paths are used to load balance traffic and provide fault tolerance for failed paths². The tier-0 logical router must be in active-active mode for ECMP to be available². A maximum of eight ECMP paths are supported². Configuring ECMP on the tier-0 gateway can address low throughput and congestion by distributing the traffic among multiple paths and avoiding bottlenecks.

Deploying Large size Edge node/s can also address low throughput and congestion by providing more resources (memory, CPU, disk) for the Edge node to handle the network traffic. The NSX Edge VM system requirements vary depending on the appliance size, which affects the bandwidth, NAT/firewall, load balancer, and VPN capabilities of the Edge node¹. A Large size Edge node has 32 GB memory, 8 vCPU, 200 GB disk space, and can support 2-10 Gbps bandwidth, L2-L4 features, and L7 load balancer¹. An Extra Large size Edge node has 64 GB memory, 16 vCPU, 200 GB disk space, and can support more than 10 Gbps bandwidth, L2-L4 features, L7 load balancer, and VPN¹. Deploying a larger size Edge node can improve the performance and capacity of the tier-0 gateway. References: 2: Understanding ECMP Routing - VMware Docs(<https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-443B6B0D-F179-42NSX-Edge-VM-System-Requirements-VMware>)

Docs(<https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/installation/GUID-22F87CA8-01A9-4F2E>)

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 command is used to display the network configuration of the Tunnel Endpoint (TEP) IP on a bare metal transport node?

- A. tepconfig
- B. ifconfig
- C. tcpdump
- D. debug

Answer: B

Explanation:

The command ifconfig is used to display the network configuration of the Tunnel Endpoint (TEP) IP on a bare metal transport node². The TEP IP is assigned to a network interface on the bare metal server that is used for overlay traffic. The ifconfig command can show the IP address, netmask, broadcast address, and other information of the network interface. For example, the following command shows the network configuration of the TEP IP on a bare metal transport node with interface name ens192:

```
ifconfig ens192
```

The output of the command would look something like this:

```
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 10.10.10.10 netmask 255.255.255.1 broadcast 10.10.10.255 inet6 fe80::250:56ff:fe9a:1b8c prefixlen 64 scopeid 0x20<link> ether 00:50:56:9a:1b:8c txqueuelen 1000 (Ethernet) RX packets 123456 bytes 123456789 (123.4 MB) RX errors 0
```

```
dropped 0 overruns 0 frame 0 TX packets 234567 bytes 234567890 (234.5 MB) TX errors 0 dropped 0
```

```
overruns 0 carrier 0 collisions 0
```

The TEP IP in this example is 10.10.10.10. References:

➤ [IBM Cloud Docs](#)

NEW QUESTION 8

Where does an administrator configure the VLANs used in VRF Lite? (Choose two.)

- A. segment connected to the Tier-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 9

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-nexedge-01> get gateways
```

Logical Router					
UUID	VRF	GW-ID	Name	Type	
Ports					
736a80e3-23f6-5a2d-81d6-bbefb2786666	0	0		TUNNEL	3
B10ef54e-d5f3-49e5-99b7-8a51366d0592	1	1025	SR-T1-LR-01	SERVICE_ROUTER_TIER1	5
5a5ddd63-3764-4d28-b92e-ee4c964a0df0	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: DF

Explanation:

BGP will be configured on the T0 SR. Connect to the VRF for the T0 SR and run get bgp neighbor once connected to it.

<https://docs.vmware.com/en/VMware-Validated-Design/5.1/sddc-deployment-of-vmware-nsx-t-workload-domain>

For the BGP configuration on NSX-T, the Tier-0 Service Router (SR) is typically where BGP is configured. To check the BGP neighbor status:

Connect to the VRF for the T0 SR, which is VRF 3 based on the provided output. Run the command to get BGP neighbor status once connected to it.

NEW QUESTION 10

Which two built-in VMware tools will help Identify the cause of packet loss on VLAN Segments? (Choose two.)

- A. Flow Monitoring
- B. Packet Capture
- C. Live Flow
- D. Activity Monitoring
- E. Traceflow

Answer: BE

Explanation:

According to the VMware NSX Documentation¹, Packet Capture and Traceflow are two built-in VMware tools that can help identify the cause of packet loss on VLAN segments.

Packet Capture allows you to capture packets on a specific interface or segment and analyze them using tools such as Wireshark or tcpdump. Packet Capture can help you diagnose network issues such as misconfigured MTU, incorrect VLAN tags, or firewall drops.

Traceflow allows you to inject synthetic packets into the network and trace their path from source to destination. Traceflow can help you verify connectivity, routing, and firewall rules between virtual machines or segments. Traceflow can also show you where packets are dropped or modified along the way.

NEW QUESTION 10

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 14

Match the NSX Intelligence recommendations with their correct purpose.

Recommendations:

security policy
recommendations

security group
recommendations

service
recommendations

Purposes:

Are service objects that were used by applications in the VMs or physical servers that an administrator had specified, but the services are not yet defined in the NSX inventory.

Are VMs or physical servers whose traffic flows were analyzed for the time period and the boundary an administrator had specified.

Are East-West distributed firewall (DFW) security policies in the application category.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- Security policy recommendations: Are East-West distributed firewall (DFW) security policies in the application category12.
- Security group recommendations: Are VMs or physical servers whose traffic flows were analyzed for the time period and the boundary you had specified12.
- Service recommendations: Are service objects that were used by applications in the VMs or physical servers that you had specified, but the services are not yet defined in the NSX inventory12.

NEW QUESTION 19

Which troubleshooting step will resolve an error with code 1001 during the configuration of a time-based firewall rule?

- A. Reinstalling the NSX VIBs on the ESXi host.
- B. Restarting the NTPservice on the ESXi host.
- C. Changing the lime zone on the ESXi host.
- D. Reconfiguring the ESXI host with a local NTP server.

Answer: B

Explanation:

According to the web search results, error code 1001 is related to a time synchronization issue between the ESXi host and the NSX Manager. This can cause problems when configuring a time-based firewall rule, which requires the ESXi host and the NSX Manager to have the same time zone and NTP server settings . To resolve this error, you need to restart the NTP service on the ESXi host to synchronize the time with the NSX Manager. You can use the following command to restart the NTP service on the ESXi host:

```
/etc/init.d/ntpd restart
```

The other options are not valid solutions for this error. Reinstalling the NSX VIBs on the ESXi host will not fix the time synchronization issue. Changing the time zone on the ESXi host may cause more discrepancies with the NSX Manager. Reconfiguring the ESXi host with a local NTP server may not be compatible with the NSX Manager's NTP server.

NEW QUESTION 24

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.

NEW QUESTION 26

Which of the two following characteristics about NAT64 are true? (Choose two.)

- A. NAT64 is stateless and requires gateways to be deployed in active-standby mode.
- B. NAT64 is supported on Tier-1 gateways only.
- C. NAT64 is supported on Tier-0 and Tier-1 gateways.
- D. NAT64 requires the Tier-1 gateway to be configured in active-standby mode.
- E. NAT64 requires the Tier-1 gateway to be configured in active-active mode.

Answer: CD

Explanation:

<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-69604E49-BC8B-4777-BFD8-B98F8D1F>

NEW QUESTION 28

Which two BGP configuration parameters can be configured in the VRF Lite gateways? (Choose two.)

- A. Graceful Restart
- B. BGP Neighbors
- C. Local AS
- D. Route Distribution
- E. Route Aggregation

Answer: BD

Explanation:

According to the VMware NSX Documentation¹, you can configure BGP neighbors for VRF-Lite by specifying the neighbor IP address, remote AS number, source IP address, and route filter. You can also configure route distribution for VRF-Lite by selecting the route redistribution sources and the route map to apply.

<https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-4CB5796A-1CED-4F0E-A>

NEW QUESTION 32

What needs to be configured on a Tier-0 Gateway to make NSX Edge Services available to a VM on a VLAN-backed logical switch?

- A. Downlink Interface
- B. VLAN Uplink
- C. Loopback Router Port
- D. Service Interface

Answer: B

Explanation:

To make NSX Edge Services available to a VM on a VLAN-backed logical switch, you need to configure a VLAN Uplink on the Tier-0 Gateway. A VLAN Uplink is a logical interface that connects the Tier-0 Gateway to the physical network and provides external connectivity for the NSX Edge Services¹. A VLAN Uplink can be configured on the NSX Manager UI by selecting Networking > Tier-0 Gateways > Interfaces > Set > Add Interface¹.

<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-D641380B-4C8E-4C8A-AF64-4261A266>

NEW QUESTION 34

As part of an organization's IT security compliance requirement, NSX Manager must be configured for 2FA (two-factor authentication).

What should an NSX administrator have ready before the integration can be configured? O

- A. Active Directory LDAP integration with OAuth Client added
- B. VMware Identity Manager with an OAuth Client added
- C. Active Directory LDAP integration with ADFS
- D. VMware Identity Manager with NSX added as a Web Application

Answer: B

Explanation:

To configure NSX Manager for two-factor authentication (2FA), an NSX administrator must have VMware Identity Manager (vIDM) with an OAuth Client added. vIDM provides identity management services and supports various 2FA methods, such as VMware Verify, RSA SecurID, and RADIUS. An OAuth Client is a configuration entity in vIDM that represents an application that can use vIDM for authentication and authorization. NSX Manager must be registered as an OAuth Client in vIDM before it can use 2FA. References: : VMware NSX-T Data Center Installation Guide, page 19. : VMware NSX-T Data Center Administration Guide, page 102. : VMware Blogs: Two-Factor Authentication with VMware NSX-T

NEW QUESTION 38

Which CLI command would an administrator use to allow syslog on an ESXi transport node when using the esxcli utility?

- A. esxcli network firewall ruleset set -r syslog -e true
- B. esxcli network firewall ruleset -e syslog
- C. esxcli network firewall ruleset set -r syslog -e false
- D. esxcli network firewall ruleset set -a -e false

Answer: A

Explanation:

To allow syslog on an ESXi transport node, the administrator needs to use the esxcli utility to enable the syslog ruleset in the ESXi firewall. The correct syntax for this command is esxcli network firewall ruleset set

-r syslog -e true, where -r specifies the ruleset name and -e specifies whether to enable or disable it. The options are incorrect because they either use an invalid syntax, such as omitting the ruleset name or

using -a instead of -r, or they disable the syslog ruleset instead of enabling it, which is the opposite of what question asks. References: [ESXi Firewall Command-Line Interface], [Configure Syslog on ESXi Hosts]

NEW QUESTION 40

Which three selections are capabilities of Network Topology? (Choose three.)

- A. Display how the different NSX components are interconnected.
- B. Display the uplink configured on the Tier-0 Gateways.
- C. Display how the Physical components are interconnected.
- D. Display the VMs connected to Segments.
- E. Display the uplinks configured on the Tier-1 Gateways.

Answer: ABD

Explanation:

According to the VMware NSX Documentation, these are three of the capabilities of Network Topology, which is a graphical representation of your network infrastructure in NSX:

- Display how the different NSX components are interconnected: You can use Network Topology to view how your segments, gateways, routers, firewalls, load balancers, VPNs, and other NSX components are connected and configured in your network.
- Display the uplink configured on the Tier-0 Gateways: You can use Network Topology to view the uplink interface and segment that connect your tier-0 gateways to your physical network. You can also view the VLAN ID and IP address of the uplink interface.
- Display the VMs connected to Segments: You can use Network Topology to view the VMs that are attached to your segments. You can also view the IP address and MAC address of each VM.

NEW QUESTION 44

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 49

Which of the following exist only on Tier-1 Gateway firewall configurations and not on Tier-0?

- A. Applied To
- B. Actions
- C. Profiles
- D. Sources

Answer: A

Explanation:

According to the VMware NSX Documentation, Applied To is a feature that exists only on tier-1 gateway firewall configurations and not on tier-0. Applied To allows you to specify which logical router ports or segments are affected by a firewall rule. This can help reduce the scope and improve the performance of firewall rules. By default, gateway firewall rules are applied to all the available uplinks and service interfaces on a selected gateway. For URL filtering, Applied To can only be Tier-1 gateways.

<https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-DE6FE8CB-017E-41C8-8>

NEW QUESTION 54

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 filler?

- 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 59

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 64

What are two supported host switch modes? (Choose two.)

- A. DPDK Datapath
- B. Enhanced Datapath
- C. Overlay Datapath
- D. Secure Datapath
- E. Standard Datapath

Answer: BE

Explanation:

The host switch modes determine how the NSX network and security stack is allocated on the underlying host CPU or DPU. There are two supported host switch modes: Enhanced Datapath and Standard

Datapath¹. Enhanced Datapath mode leverages the DPU to offload the NSX datapath processing from the host CPU, while Standard Datapath mode uses the host CPU for the NSX datapath processing¹. DPDK Datapath, Overlay Datapath, and Secure Datapath are not valid host switch modes for NSX 4.x. References: NSX Features

NEW QUESTION 68

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 70

Which two statements describe the characteristics of an Edge Cluster in NSX? (Choose two.)

- A. Can have a maximum of 8 edge nodes
- B. Can have a maximum of 10 edge nodes
- C. Must have only active-active edge nodes
- D. Can contain multiple types of edge nodes (VM or bare metal)
- E. Must contain only one type of edge nodes (VM or bare metal)

Answer: AE

Explanation:

Two statements that describe the characteristics of an Edge Cluster in NSX are:

- An Edge Cluster can have a maximum of 8 edge nodes². This is the upper limit for scaling out the Edge Cluster and providing high availability and load balancing for network services.
- An Edge Cluster must contain only one type of edge nodes (VM or bare metal)³. This is because different types of edge nodes have different performance and resource requirements, and mixing them in the same cluster can cause inconsistency and instability. The other options are incorrect because they do not describe the characteristics of an Edge Cluster in NSX. An Edge Cluster can have either active-active or active-standby edge nodes, depending on the configuration and services⁴. An Edge Cluster cannot contain multiple types of edge nodes, as explained above. References: Enhanced NSX Edge and Networking Services in NSX 4.0.1.1, NSX Edge Installation Requirements, NSX-T Edge Node Cluster

NEW QUESTION 71

Which statement is true about an alarm in a Suppressed state?

- A. An alarm can be suppressed for a specific duration in seconds.
- B. An alarm can be suppressed for a specific duration in days.
- C. An alarm can be suppressed for a specific duration in minutes.
- D. An alarm can be suppressed for a specific duration in hours.

Answer: D

Explanation:

The answer is D. An alarm can be suppressed for a specific duration in hours.

According to the VMware NSX documentation, an alarm can be in one of the following states: Open, Acknowledged, Suppressed, or Resolved¹²

An alarm in a Suppressed state means that the status reporting for this alarm has been disabled by the user for a user-specified duration¹²

When a user moves an alarm into a Suppressed state, they are prompted to specify the duration in hours. After the specified duration passes, the alarm state reverts to Open. However, if the system determines the condition has been corrected, the alarm state changes to Resolved¹³

To learn more about how to manage alarm states in NSX, you can refer to the following resources:

- VMware NSX Documentation: Managing Alarm States 1
- VMware NSX Documentation: View Alarm Information 2
- VMware NSX Intelligence Documentation: Manage NSX Intelligence Alarm States 3 <https://docs.vmware.com/en/VMware-NSX-Intelligence/1.2/user-guide/GUID-EBD3C5A8-F9AB-4A22-BA40->

NEW QUESTION 75

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 76

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 2V0-41.23 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 2V0-41.23 Product From:

<https://www.2passeasy.com/dumps/2V0-41.23/>

Money Back Guarantee

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