

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

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 Execute. 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 3

What should an NSX administrator check to verify that VMware Identity Manager Integration Is successful?

- A. From VMware Identity Manager the status of the remote access application must be green.
- B. From the NSX UI the status of the VMware Identity Manager Integration must be "Enabled".
- C. From the NSX CLI the status of the VMware Identity Manager Integration must be "Configured".
- D. From the NSX UI the URI in the address bar must have "locaNfatse" part of it.

Answer: B

Explanation:

From the NSX UI the status of the VMware Identity Manager Integration must be "Enabled". According to the VMware NSX Documentation¹, after configuring VMware Identity Manager integration, you can validate the functionality by checking the status of the integration in the NSX UI. The status should be "Enabled" if the integration is successful. The other options are either incorrect or not relevant.

NEW QUESTION 4

Which two statements are true for IPSec VPN? (Choose two.)

- A. VPNs can be configured on the command line Interface on the NSX manager.
- B. IPSec VPN services can be configured at Tier-0 and Tier-1 gateways.
- C. IPSec VPNs use the DPDK accelerated performance library.
- D. Dynamic routing Is supported for any IPSec mode In NSX.

Answer: BC

Explanation:

According to the VMware NSX 4.x Professional documents and tutorials, IPSec VPN secures traffic flowing between two networks connected over a public network through IPSec gateways called endpoints. NSX Edge supports a policy-based or a route-based IPSec VPN. Beginning with NSX-T Data Center 2.5, IPSec VPN services are supported on both Tier-0 and Tier-1 gateways¹. NSX Edge also leverages the DPDK accelerated performance library to optimize the performance of

IPSec VPN2.

NEW QUESTION 5

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 6

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. Keycloak 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 7

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 8

When configuring OSPF on a Tier-0 Gateway, which three of the following must match in order to establish a neighbor relationship with an upstream router? (Choose three.)

- A. Naming convention
- B. MTU of the Uplink
- C. Subnet mask
- D. Address of the neighbor
- E. Protocol and Port
- F. Area ID

Answer: BCF

Explanation:

According to the VMware NSX Documentation, these are the three parameters that must match in order to establish an OSPF neighbor relationship with an upstream router on a tier-0 gateway:

- MTU of the Uplink: The maximum transmission unit (MTU) of the uplink interface must match the MTU of the upstream router interface. Otherwise, OSPF packets may be fragmented or dropped, causing neighbor adjacency issues.
- Subnet mask: The subnet mask of the uplink interface must match the subnet mask of the upstream router interface. Otherwise, OSPF packets may not reach the correct destination or be rejected by the upstream router.
- Area ID: The area ID of the uplink interface must match the area ID of the upstream router interface. Otherwise, OSPF packets may be ignored or discarded by the upstream router.

NEW QUESTION 9

Which is an advantage of a L2 VPN in an NSX 4.x environment?

- A. Enables Multi-Cloud solutions
- B. Achieve better performance
- C. Enables VM mobility with re-IP
- D. Use the same broadcast domain

Answer: D

Explanation:

L2 VPN is a feature of NSX that allows extending Layer 2 networks across different sites or clouds over an IPsec tunnel. L2 VPN has an advantage of enabling VM mobility with re-IP, which means that VMs can be moved from one site to another without changing their IP addresses or network configurations. This is possible because L2 VPN allows both sites to use the same broadcast domain, which means that they share the same subnet and VLAN .

NEW QUESTION 10

When deploying an NSX Edge Transport Node, what two valid IP address assignment options should be specified for the TEP IP addresses? (Choose two.)

- A. Use an IP Pool
- B. Use a DHCP Server
- C. Use RADIUS
- D. Use a Static IP List
- E. Use BootP

Answer: AD

Explanation:

When deploying an NSX Edge Transport Node, two valid IP address assignment options that should be specified for the TEP IP addresses are Use an IP Pool and Use a Static IP List. These options allow the u assign TEP IP addresses from a predefined range of IP addresses or a manually entered list of IP addresses, respectively345. The other options are incorrect because they are not supported methods for assigning TEP IP addresses. There is no option to use a DHCP server, RADIUS, or BootP for TEP IP address assignment in NSX-T345. References: NSX-T Edge TEP networking options, Multi-TEP High Availability, Create an Pool for Host Tunnel Endpoint IP Addresses

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 11

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

If the packet matches source, destination, service, profile and applied to fields, apply the action defined.

If the rule table action is allow, create an entry in the connection table and forward the packet.

Packet arrives at dvfilter connection table, if matching entry in the table, process the packet.

If the rule table action is reject or deny, take that action.

If connection table has no match, compare the packet to the rule table.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The correct order of the rule processing steps of the Distributed Firewall is as follows:

- Packet arrives at vfilter connection table. If matching entry in the table, process the packet.

- If connection table has no match, compare the packet to the rule table.
- If the rule table action is allow, create an entry in the connection table and forward the packet.
- If the rule table action is reject or deny, take that action.

This order is based on the description of how the Distributed Firewall works in the web search results¹. The first step is to check if there is an existing connection entry for the packet in the vfilter connection table, which is a cache of flow entries for rules with an allow action. If there is a match, the packet is processed according to the connection entry. If there is no match, the packet is compared to the rule table, which contains all the security policy rules. The rules are evaluated from top to bottom until a match is found. The match criteria include source, destination, service, profile and applied to fields. The action defined by the matching rule is applied to the packet. The action can be allow, reject or deny. If the action is allow, a new connection entry is created for the packet and the packet is forwarded to its destination. If the action is reject or deny, the packet is dropped and an ICMP message or a TCP reset message is sent back to the source.

NEW QUESTION 15

Which CLI command is used for packet capture on the ESXi Node?

- A. tcpdump
- B. debug
- C. pktcap-uw
- D. set capture

Answer: C



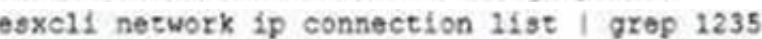
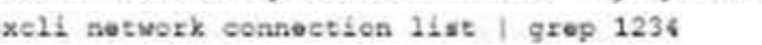
Explanation:

According to the VMware Knowledge Base, this CLI command is used for packet capture on the ESXi node. pktcap-uw stands for Packet Capture User World and is a tool that allows you to capture packets from various points in the network stack of an ESXi host. You can use this tool to troubleshoot network issues or analyze traffic flows.

The other options are either incorrect or not available for this task. tcpdump is not a valid CLI command for packet capture on the ESXi node, as it is a tool that runs on Linux systems, not on ESXi hosts. debug is not a valid CLI command for packet capture on the ESXi node, as it is a generic term that describes the process of finding and fixing errors, not a specific tool or command. set capture is not a valid CLI command for packet capture on the ESXi node, as it does not exist in the ESXi CLI.

NEW QUESTION 20

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 22

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

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

Answer: ABD

Explanation:

* A. Can be used as an Exterior Gateway Protocol. This is correct. BGP is a protocol that can be used to exchange routing information between different autonomous systems (AS). An AS is a network or a group of networks under a single administrative control. BGP can be used as an Exterior Gateway Protocol (EGP) to connect an AS to other ASes on the internet or other external networks¹

* B. It supports a 4-byte autonomous system number. This is correct. BGP supports both 2-byte and 4-byte AS numbers. A 2-byte AS number can range from 1 to 65535, while a 4-byte AS number can range from 65536 to 4294967295. NSX supports both 2-byte and 4-byte AS numbers for BGP configuration on a Tier-0 Gateway²

* C. The network is divided into areas that are logical groups. This is incorrect. This statement describes OSPF, not BGP. OSPF is another routing protocol that operates within a single AS and divides the network into areas to reduce routing overhead and improve scalability. BGP does not use the concept of areas, but rather uses attributes, policies, and filters to control the routing decisions and traffic flow³

* D. FIGRP is disabled by default. This is correct. FIGRP stands for Fast Interior Gateway Routing Protocol, which is an enhanced version of IGRP, an obsolete routing protocol developed by Cisco. FIGRP is not supported by NSX and is disabled by default on a Tier-0 Gateway.

* E. BGP is enabled by default. This is incorrect. BGP is not enabled by default on a Tier-0 Gateway. To enable BGP, you need to configure the local AS number and the BGP neighbors on the Tier-0 Gateway using the NSX Manager UI or API.

To learn more about BGP configuration on a Tier-0 Gateway in NSX, you can refer to the following resources:

- VMware NSX Documentation: Configure BGP ¹
- VMware NSX 4.x Professional: BGP Configuration
- VMware NSX 4.x Professional: BGP Troubleshooting

NEW QUESTION 23

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

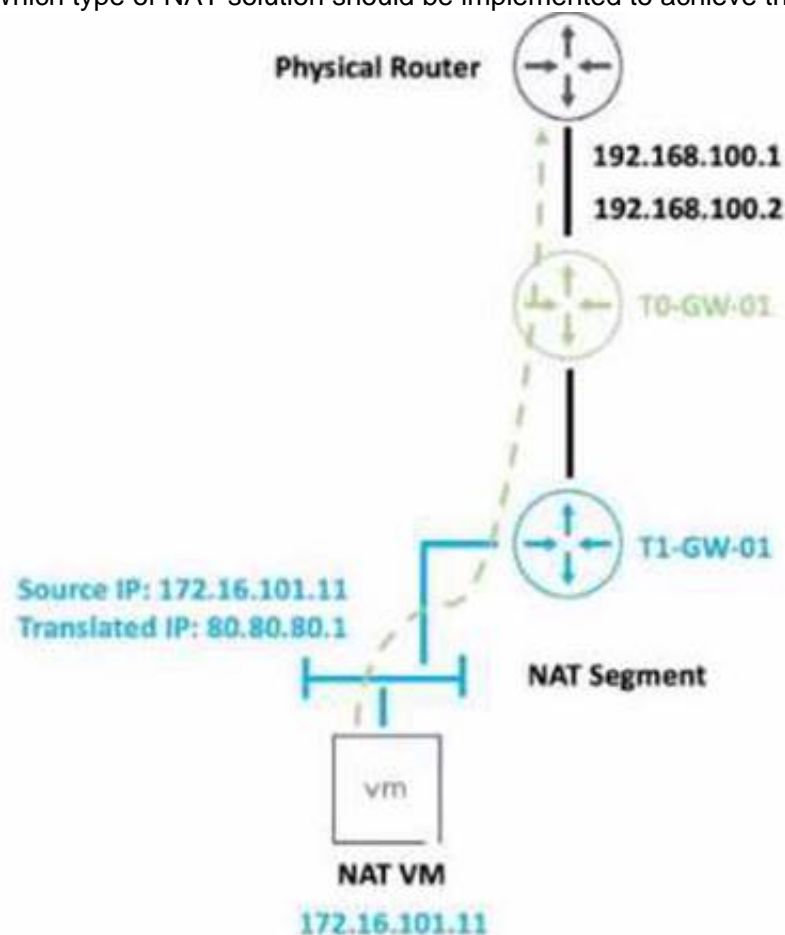
The other options are not valid solutions for this error. Reinstalling the NSX VIBs on the ESXi host will not fix the time synchronization issue. Changing the time zone on the ESXi host may cause more discrepancies with the NSX Manager. Reconfiguring the ESXi host with a local NTP server may not be compatible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

NEW QUESTION 27

Refer to the exhibit.

An administrator would like to change the private IP address of the NAT VM 172.16.101.11 to a public address of 80.80.80.1 as the packets leave the NAT-Segment network.

Which type of NAT solution should be implemented to achieve this?



- A. DNAT
- B. SNAT
- C. Reflexive NAT
- D. NAT64

Answer: B

Explanation:

SNAT stands for Source Network Address Translation. It is a type of NAT that translates the source IP address of outgoing packets from a private address to a public address. SNAT is used to allow hosts in a private network to access the internet or other public networks¹

In the exhibit, the administrator wants to change the private IP address of the NAT VM 172.16.101.11 to a public address of 80.80.80.1 as the packets leave the NAT-Segment network. This is an example of SNAT, as the source IP address is modified before the packets are sent to an external network.

According to the VMware NSX 4.x Professional Exam Guide, SNAT is one of the topics covered in the exam objectives²

To learn more about SNAT and how to configure it in VMware NSX, you can refer to the following resources: ➤ VMware NSX Documentation: NAT 3

- VMware NSX 4.x Professional: NAT Configuration 4
- VMware NSX 4.x Professional: NAT Troubleshooting 5

<https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-7AD2C384-4303-4D6C-A>

NEW QUESTION 30

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 32

What is the VMware recommended way to deploy a virtual NSX Edge Node?

- A. Through the OVF command line tool
- B. Through the vSphere Web Client
- C. Through automated or Interactive mode using an ISO
- D. Through the NSXUI

Answer: D

Explanation:

Through the NSX UI. According to the VMware NSX Documentation², you can deploy NSX Edge nodes as virtual appliances through the NSX UI by clicking Add Edge Node and providing the required information. The other options are either outdated or not applicable for virtual NSX Edge nodes.

<https://docs.vmware.com/en/VMware-NSX/4.1/installation/GUID-E9A01C68-93E7-4140-B306-19CD6806199>

NEW QUESTION 37

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 39

Which two commands does an NSX administrator use to check the IP address of the VMkernel port for the Geneve protocol on the ESXi transport node? (Choose two.)

- A. esxcfg-nics -l
- B. esxcli network ip interface ipv4 get
- C. esxcli network nic list
- D. esxcfg-vmknic -l
- E. net-dvs

Answer: BD

Explanation:

To check the IP address of the VMkernel port for the Geneve protocol on the ESXi transport node, an NSX administrator can use the following commands:

➤ esxcli network ip interface ipv4 get: This command displays the IPv4 configuration of all VMkernel interfaces on the host, including their IP addresses, netmasks, and gateways. The Geneve protocol uses a VMkernel interface named geneve0 by default¹

➤ esxcfg-vmknic -l: This command lists all VMkernel interfaces on the host, along with their MAC addresses, MTU, and netstack. The Geneve protocol uses a netstack named nsx-overlay by default

NEW QUESTION 42

Which CLI command shows syslog on NSX Manager?

- A. get log-file auth.log
- 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 43

An administrator has deployed 10 Edge Transport Nodes in their NSX Environment, but has forgotten to specify an NTP server during the deployment. What is the efficient way to add an NTP server to all 10 Edge Transport Nodes?

- A. Use Transport Node Profile
- B. Use the CU on each Edge Node
- C. Use a Node Profile
- D. Use a PowerCU script

Answer: C

Explanation:

A node profile is a configuration template that can be applied to multiple NSX Edge nodes or transport nodes at once. A node profile can include settings such as NTP server, DNS server, syslog server, and so on¹. By using a node profile, an administrator can efficiently configure or update the network settings of multiple NSX Edge nodes or transport nodes in a single operation². The other options are incorrect because they are either not efficient or not supported. Using the CLI on each Edge node would require manual and repetitive commands for each node, which is not efficient. Using a Transport Node Profile would not work, because a Transport Node Profile is used to configure the NSX-T Data Center components on a transport node, such as the transport zone, the N-VDS, and the uplink profiles³. Using a PowerCLI script might work, but it would require writing and testing a custom script, which is not as efficient as using a built-in feature like a node profile.

<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-B4AE1432-690E-480E-91C4-903C1E549>

NEW QUESTION 47

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 48

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 51

Which VMware GUI tool is used to identify problems in a physical network?

- A. VMware Aria Automation
- B. VMware Aria Orchestrator
- C. VMware Site Recovery Manager
- D. VMware Aria Operations Networks

Answer: D

Explanation:

According to the web search results, VMware Aria Operations Networks (formerly vRealize Network Insight) is a network monitoring tool that can help monitor, discover and analyze networks and applications across clouds¹. It can also provide enhanced troubleshooting and visibility for physical and virtual networks². The other options are either incorrect or not relevant for identifying problems in a physical network. VMware Aria Automation is a cloud automation platform that can help automate the delivery of IT services. VMware Aria Orchestrator is a cloud orchestration tool that can help automate workflows and integrate with other systems. VMware Site Recovery Manager is a disaster recovery solution that can help protect and recover virtual machines from site failures.

NEW QUESTION 55

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 60

Which NSX CLI command is used to change the authentication policy for local users?

- A. Set cli-timeout
- B. Get auth-policy minimum-password-length
- C. Set hardening- policy
- D. Set auth-policy

Answer: D

Explanation:

According to the VMware NSX Documentation⁴, the set auth-policy command is used to change the authentication policy settings for local users, such as password length, lockout period, and maximum authentication failures. The other commands are either used to view the authentication policy settings (B), change the CLI session timeout (A), or change the hardening policy settings ©.

NEW QUESTION 61

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 66

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 71

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 72

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 74

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 79

.....

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](#)