

# VMware

## Exam Questions 2V0-41.23

VMware NSX 4.x Professional



#### NEW QUESTION 1

Which two of the following will be used for Ingress traffic on the Edge node supporting a Single Tier topology? (Choose two.)

- A. Inter-Tier interface on the Tier-0 gateway
- B. Tier-0 Uplink interface
- C. Downlink Interface for the Tier-0 DR
- D. Tier-1 SR Router Port
- E. Downlink Interface for the Tier-1 DR

**Answer:** BC

#### Explanation:

The two interfaces that will be used for ingress traffic on the Edge node supporting a Single Tier topology are:

- > B. Tier-0 Uplink interface
- > C. Downlink Interface for the Tier-0 DR

The Tier-0 Uplink interface is the interface that connects the Tier-0 gateway to the external network. It is used to receive traffic from the physical router or switch that is the next hop for the Tier-0 gateway. The Tier-0 Uplink interface can be configured with a static IP address or use BGP to exchange routes with the external network.

The Downlink Interface for the Tier-0 DR is the interface that connects the Tier-0 gateway to the workload segments. It is used to receive traffic from the VMs or containers that are attached to the segments. The Downlink Interface for the Tier-0 DR is a logical interface (LIF) that is distributed across all transport nodes that host the segments. The Downlink Interface for the Tier-0 DR has an IP address that acts as the default gateway for the VMs or containers on the segments.

#### NEW QUESTION 2

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 Documentation<sup>1</sup>, 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 3

An NSX administrator is reviewing syslog and notices that Distributed Firewall Rules hit counts are not being logged. What could cause this issue?

- A. Syslog is not configured on the ESXi transport node.
- B. Zero Trust Security is not enabled.
- C. Syslog is not configured on the NSX Manager.
- D. Distributed Firewall Rule logging is not enabled.

**Answer:** D

#### NEW QUESTION 4

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 5

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 Tler-0 and Tler-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 gateways<sup>1</sup>. NSX Edge also leverages the DPDK accelerated performance library to optimize the performance of IPsec VPN<sup>2</sup>.

**NEW QUESTION 6**

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 failures<sup>1</sup>

**NEW QUESTION 7**

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 8**

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 cluster<sup>2</sup>. The ECMP routing paths are used to load balance traffic and provide fault tolerance for failed paths<sup>2</sup>. The tier-0 logical router must be in active-active mode for ECMP to be available<sup>2</sup>. A maximum of eight ECMP paths are supported<sup>2</sup>. 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 node<sup>1</sup>. 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 balancer<sup>1</sup>. 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 VPN<sup>1</sup>. 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 9**

Which NSX feature can be leveraged to achieve consistent policy configuration and simplicity across sites?

- A. VRF Lite
- B. Ethernet VPN
- C. NSX MTML5 UI
- D. NSX Federation

**Answer: D**

**Explanation:**

According to the VMware NSX Documentation, this is the NSX feature that can be leveraged to achieve consistent policy configuration and simplicity across sites:

➤ NSX Federation: This feature allows you to create and manage a global network infrastructure that spans across multiple sites using a single pane of glass. You can use this feature to synchronize policies, segments, gateways, firewalls, VPNs, load balancers, and other network services across sites.

**NEW QUESTION 10**

Which two choices are use cases for Distributed Intrusion Detection? (Choose two.)

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

**Answer:** BE

**Explanation:**

According to the VMware NSX Documentation, these are two of the use cases for Distributed Intrusion Detection, which is a feature of NSX Network Detection and Response:

- Quarantine workloads based on vulnerabilities: You can use Distributed Intrusion Detection to detect vulnerabilities in your workloads and apply quarantine actions to isolate them from the network until they are remediated.
- Identify security vulnerabilities in the workloads: You can use Distributed Intrusion Detection to scan your workloads for known vulnerabilities and generate reports that show the severity, impact, and remediation steps for each vulnerability.

**NEW QUESTION 10**

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 node. 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 13**

Where is the insertion point for East-West network introspection?

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

**Answer:** C

**Explanation:**

The insertion point for East-West network introspection is the Guest VM vNIC. Network introspection is a service insertion feature that allows third-party network services to be integrated with NSX. Network introspection enables traffic redirection from the Guest VM vNIC to a service virtual machine (SVM) that runs the partner service. The SVM can then inspect, monitor, or modify the traffic before sending it back to the original destination<sup>1</sup>. The other options are incorrect because they are not the insertion points for East-West network introspection. The Tier-0 router is used for North-South routing and network services. The partner SVM is the service virtual machine that runs the partner service, not the insertion point. The host physical NIC is not involved in network introspection. References: Network Introspection Settings

**NEW QUESTION 15**

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 18

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 21

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 profiles<sup>1</sup>. 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 services<sup>2</sup>.

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

#### NEW QUESTION 26

Match the NSX Intelligence recommendations with their correct purpose.

Recommendations:	Purposes:
security policy recommendations	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.
security group recommendations	Are VMs or physical servers whose traffic flows were analyzed for the time period and the boundary an administrator had specified.
service recommendations	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 category<sup>12</sup>.
- Security group recommendations: Are VMs or physical servers whose traffic flows were analyzed for the time period and the boundary you had specified<sup>12</sup>.
- 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 inventory<sup>12</sup>.

#### NEW QUESTION 28

An administrator wants to validate the BGP connection status between the Tier-O Gateway and the upstream physical router. What sequence of commands could be used to check this status on NSX Edge node?

- A. `set vrf <ID>show logical-routers show <LR-D> bgp`
- B. `show logical-routers get vrfshow ip route bgp`
- C. `get gateways vrf <number>get bgp neighbor`
- D. `enable <LR-D> get vrf <ID>show bgp neighbor`

**Answer:** C

**Explanation:**

The sequence of commands that could be used to check the BGP connection status between the Tier-O Gateway and the upstream physical router on NSX Edge node is `get gateways`, `vrf <number>`, `get bgp neighbor`. These commands can be executed on the NSX Edge node CLI after logging in as `admin6`. The first command, `get gateways`, displays the list of logical routers (gateways) configured on the Edge node, along with their IDs and VRF numbers<sup>7</sup>. The second command, `vrf <number>`, switches to the VRF context of the desired Tier-O Gateway, where `<number>` is the VRF number obtained from the previous command<sup>7</sup>. The third command, `get bgp neighbor`, displays the BGP neighbor summary for the selected VRF, including the neighbor IP address, AS number, state, uptime, and prefixes received<sup>8</sup>. The other options are incorrect because they either use invalid or incomplete commands or do not switch to the correct VRF context. References: NSX-T Command-Line Interface Reference, NSX Edge Node CLI Commands, Troubleshooting BGP on NSX-T Edge Nodes

**NEW QUESTION 31**

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 33**

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 38**

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 41**

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 default<sup>1</sup>
- `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 44

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 45

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 50

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

- A. VXIAN
- B. UDP
- C. STT
- D. TEP

**Answer:** D

#### Explanation:

According to the VMware NSX Documentation, TEP stands for Tunnel End Point and is a logical interface that must be configured on transport nodes for encapsulation and decapsulation of Geneve protocol. Geneve is a tunneling protocol that encapsulates the original packet with an outer header that contains metadata such as the virtual network identifier (VNI) and the transport node IP address. TEPs are responsible for adding and removing the Geneve header as the packet traverses the overlay network.

#### NEW QUESTION 53

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 failed 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 58

Which two are supported by L2 VPN clients? (Choose two.)

- A. NSX for vSphere Edge
- B. 3rd party Hardware VPN Device
- C. NSX Autonomous Edge
- D. NSX Edge

**Answer:** AD

**Explanation:**

L2 VPN clients are supported by NSX for vSphere Edge and NSX Edge. NSX for vSphere Edge is a virtual appliance that provides network services such as routing, firewalling, load balancing, VPN, and NAT for NSX Data Center for vSphere environments. NSX Edge is a virtual appliance that provides network services such as routing, firewalling, load balancing, VPN, and NAT for NSX-T Data Center environments. Both NSX for vSphere Edge and NSX Edge can act as L2 VPN clients to extend layer 2 networks across multiple sites using L2 VPN service over SSL or IPSec tunnels

**NEW QUESTION 62**

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 locations<sup>1</sup>. 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 enforcement<sup>1</sup>. Federation also enables disaster recovery and workload mobility scenarios by providing consistent network and security policies across different sites<sup>1</sup>. 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 67**

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 Services<sup>1</sup>. A VLAN Uplink can be configured on the NSX Manager UI by selecting Networking > Tier-0 Gateways > Interfaces > Set > Add Interface<sup>1</sup>.  
<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-D641380B-4C8E-4C8A-AF64-4261A266>

**NEW QUESTION 72**

An NSX administrator has deployed a single NSX Manager node and will be adding two additional nodes to form a 3-node NSX Management Cluster for a production environment. The administrator will deploy these two additional nodes and Cluster VIP using the NSX UI. What two are the prerequisites for this configuration? (Choose two.)

- A. All nodes must be in separate subnets.
- B. The cluster configuration must be completed using API.
- C. NSX Manager must reside on a Windows Server.
- D. All nodes must be in the same subnet.
- E. A compute manager must be configured.

**Answer:** DE

**Explanation:**

According to the VMware NSX Documentation, these are the prerequisites for adding nodes to an NSX Management Cluster using the NSX UI:

- All nodes must be in the same subnet and have IP connectivity with each other.
- A compute manager must be configured and associated with the NSX Manager node.
- The NSX Manager node must have a valid license.
- The NSX Manager node must have a valid certificate.

**NEW QUESTION 75**

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 VMwar kernel ports for tunnel end point communication. This command uses the geneve netstack, which is the default netstack for NSX-T. The `-d` option sets the DF (Don't Fragment) bit in the IP header, which prevents the packet from being fragmented by intermediate routers. The `-s 1572` option sets the packet size to 1572 bytes, which is the maximum payload size for a geneve encapsulated packet with an MTU of 1600 bytes.

The `<destination IP address>` is the IP address of the remote ESXi host or VM. References: : VMware NS Data Center Installation Guide, page 19. : VMware Knowledge Base: Testing MTU with the `vmkping` command (1003728). : VMware NSX-T Data Center Administration Guide, page 102.

**NEW QUESTION 76**

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 80**

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

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

**Answer:** A

**Explanation:**

According to the VMware NSX 4.x Professional documents and tutorials, BFD is a failover detection protocol that provides fast and reliable detection of link failures between two routing devices. BFD can be used with ECMP routing to monitor the health of the ECMP paths and trigger a route change in case of a failure<sup>12</sup>. BFD is supported by both BGP and OSPF routing protocols in NSX-T3. BFD can also be configured with different timers to achieve different detection times<sup>3</sup>.

**NEW QUESTION 85**

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 clouds<sup>1</sup>. It can also provide enhanced troubleshooting and visibility for physical and virtual networks<sup>2</sup>. 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 88**

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 91

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 95

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 96

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 Documentation<sup>4</sup>, 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 100

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

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

**Answer:** A

#### Explanation:

The RouterLink port is automatically created when a Tier-1 Gateway is connected with a Tier-0 Gateway from the NSX UI<sup>1</sup>. The RouterLink port is a logical interface that is assigned an IP address and is associated with a physical or virtual interface. The RouterLink port acts as an end point of the IPsec tunnel and routes traffic between the Tier-1 Gateway and the Tier-0 Gateway<sup>2</sup>. The other options are incorrect because they involve manual creation of logical switches or segments, which are not required for RouterLink port creation. References: Configure NSX for Virtual Networking from vSphere Client, Virtual Private Network (VPN)

#### NEW QUESTION 104

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 Documentation<sup>1</sup>, 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 106**

An administrator has connected two virtual machines on the same overlay segment. Ping between both virtual machines is successful. What type of network boundary does this represent?

- A. Layer 2 VPN
- B. Layer 2 bridge
- C. Layer 2 broadcast domain
- D. Layer 3 route

**Answer:** C

**Explanation:**

An overlay segment is a logical construct that provides Layer 2 connectivity between virtual machines that are attached to it. An overlay segment can span multiple hosts and can be extended across different subnets or locations using Geneve encapsulation<sup>3</sup>. Therefore, two virtual machines on the same overlay segment belong to the same Layer 2 broadcast domain, which means they can communicate with each other using their MAC addresses without requiring any routing. The other options are incorrect because they involve Layer 3 or higher network boundaries, which require routing or tunneling to connect different segments. References: VMware NSX Documentation

**NEW QUESTION 111**

Which two CLI commands could be used to see if vmnic link status is down? (Choose two.)

- A. esxcfg-nics -l
- B. esxcli network nic list
- C. esxcli network vswitch dvs vmware list
- D. esxcfg-vmknic -l
- E. esxcfg-vmsvc/get.network

**Answer:** AB

**Explanation:**

esxcfg-nics -l and esxcli network nic list are two CLI commands that can be used to see the vmnic link status on an ESXi host. Both commands display information such as the vmnic name, driver, link state, speed, and duplex mode. The link state can be either Up or Down, indicating whether the vmnic is connected or not. For example, the output of esxcfg-nics -l can look like this:

Name	PCI	Driver	Link	Speed	Duplex	MAC Address	MTU	Description
vmnic0	0000:02:00:0	igbn	Up	1000Mbps	Full	00:50:56:01:2a:3b	1500	Intel Corporation I350 Gigabit Network Connection
vmnic1	0000:02:00:1	igbn	Down	0Mbps	Half	00:50:56:01:2a:3c	1500	Intel Corporation I350 Gigabit Network Connection

**NEW QUESTION 113**

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 Resolved<sup>12</sup>

An alarm in a Suppressed state means that the status reporting for this alarm has been disabled by the user for a user-specified duration<sup>12</sup>

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 Resolved<sup>13</sup>

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

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

**NEW QUESTION 118**

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](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 120

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 125

.....

## 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](#)**