2V0-41.23Q&As

VMware NSX 4.x Professional

Pass VMware 2V0-41.23 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/2v0-41-23.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by VMware Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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.

Correct Answer: AB

Reference: https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-0A8BF7D8-9C2E-48A5-8219-17C00F1EC13A.html https://www.wwt.com/blog/primer-series-napp-malware-prevention

QUESTION 2

What are three NSX Manager roles? (Choose three.)

A. master

B. cloud

C. zookeepet

D. manager

E. policy

F. controller

Correct Answer: DEF

According to the VMware NSX 4.x Professional documents and tutorials, an NSX Manager is a standalone appliance that hosts the API services, the management plane, control plane, and policy management. The NSX Manager has three built-in roles: policy, manager, and controller2. The policy role handles the declarative configuration of the system and translates it into desired state for the manager role. The manager role receives and validates the configuration from the policy role and stores it in a distributed persistent database. The manager role also publishes the configuration to the central control plane. The controller role implements the central control plane that computes the network state based on the configuration and topology information3. The other roles (master, cloud, and zookeeper) are not valid NSX Manager roles.

QUESTION 3

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.

Correct Answer: B

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.

QUESTION 4

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

A. TEP Table

B. MAC Table

C. ARP Table

D. Routing Table

Correct Answer: B

The MAC table on an ESXi host is used to determine the location of a particular workload for a frame-forwarding decision. The MAC table maps the MAC addresses of the workloads to their corresponding tunnel endpoint (TEP) IP addresses. The TEP IP address identifies the ESXi host where the workload resides. The MAC table is populated by learning the source MAC addresses of the incoming frames from the workloads. The MAC table is also synchronized with other ESXi hosts in the same transport zone by using the NSX Controller.
https://nsx.techzone.vmware.com/resource/nsx-reference-design-guide Reference: https://www.oreilly.com/library/view/mastering-vmware-vsphere/9781787286016/6e81703b-29e7-4249-a823-1ba6a17d7f3a.xhtml

---

QUESTION 5

A security administrator needs to configure a firewall rule based on the domain name of a specific application.

Which field in a distributed firewall rule does the administrator configure?

A. Profile

B. Service

C. Policy

D. Source

Correct Answer: A

To configure a firewall rule based on the domain name of a specific application, the administrator needs to use the Profile field in a distributed firewall rule. The Profile field allows the administrator to select a context profile that contains one or

more attributes for filtering traffic. One of the attributes that can be used is Domain (FQDN) Name, which specifies the fully qualified domain name of the application. For example, if the administrator wants to filter traffic to *.office365.com,

they can create a context profile with the Domain (FQDN) Name attribute set to *.office365.com and use it in the Profile field of the firewall rule.

References:

Filtering Specific Domains (FQDN/URLs)

FQDN Filtering

QUESTION 6

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: Which two commands must be executed to check BGP neighbor status? (Choose two.)

```
sa-nsxedge-01> get gateways
Logical Router
UUID                                   VRF    GW-ID    Name              Type                        Ports
736a80e3-23f6-5a2d-81d6-bbefb2786666   0      0                          TUNNEL                      3
810ef54e-d5f3-49e5-99b7-8a51366d0592   1      1025     SR-T1-LR-01       SERVICE_ROUTER_TIER1        8
5a5ddd63-3764-4d28-b82e-ee4c964a0dfd   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
```

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

Correct Answer: DF

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-domains-withmultiple-availability-zones/GUID-8BD4228A-75C6-4C60-80B4-538D4297E11A.html 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.

QUESTION 7

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

Correct Answer: C

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 encapsulation3. 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

---

QUESTION 8

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

Correct Answer: D

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.

QUESTION 9

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 ate interconnected.

D. Display the VMs connected to Segments.

E. Display the uplinks configured on the Tier-1 Gateways.

Correct Answer: ABD

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.

https://docs.vmware.com/en/VMware-NSX/4.0/administration/GUID-A75B2553-7595-40B9-A902-854941BB06FD.html

QUESTION 10

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

A. SFRVICE_ROUTER_TJER0

B. TIERO_DISTRI BUTE D_ ROUTER

C. DISTRIBUTED_R0UTER_TIER1

D. DISTRIBUTED_ROUTER_TIER0

E. SERVICE_ROUTER_TIERl

Correct Answer: CD

https://docs.vmware.com/en/VMware-Validated-Design/5.0.1/com.vmware.vvd.sddc-nsxt-design.doc/GUID-74141ABD-C9AF-4A92-8338-092CD67EB56E.html https://www.delltechnologies.com/asset/en-us/products/converged-infrastructure/technical-support/docu96042.pdf

QUESTION 11

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

Correct Answer: C

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

QUESTION 12

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

Correct Answer: B

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-D5B6DC79-6733-44A7-8072-50221CF2122A.html)

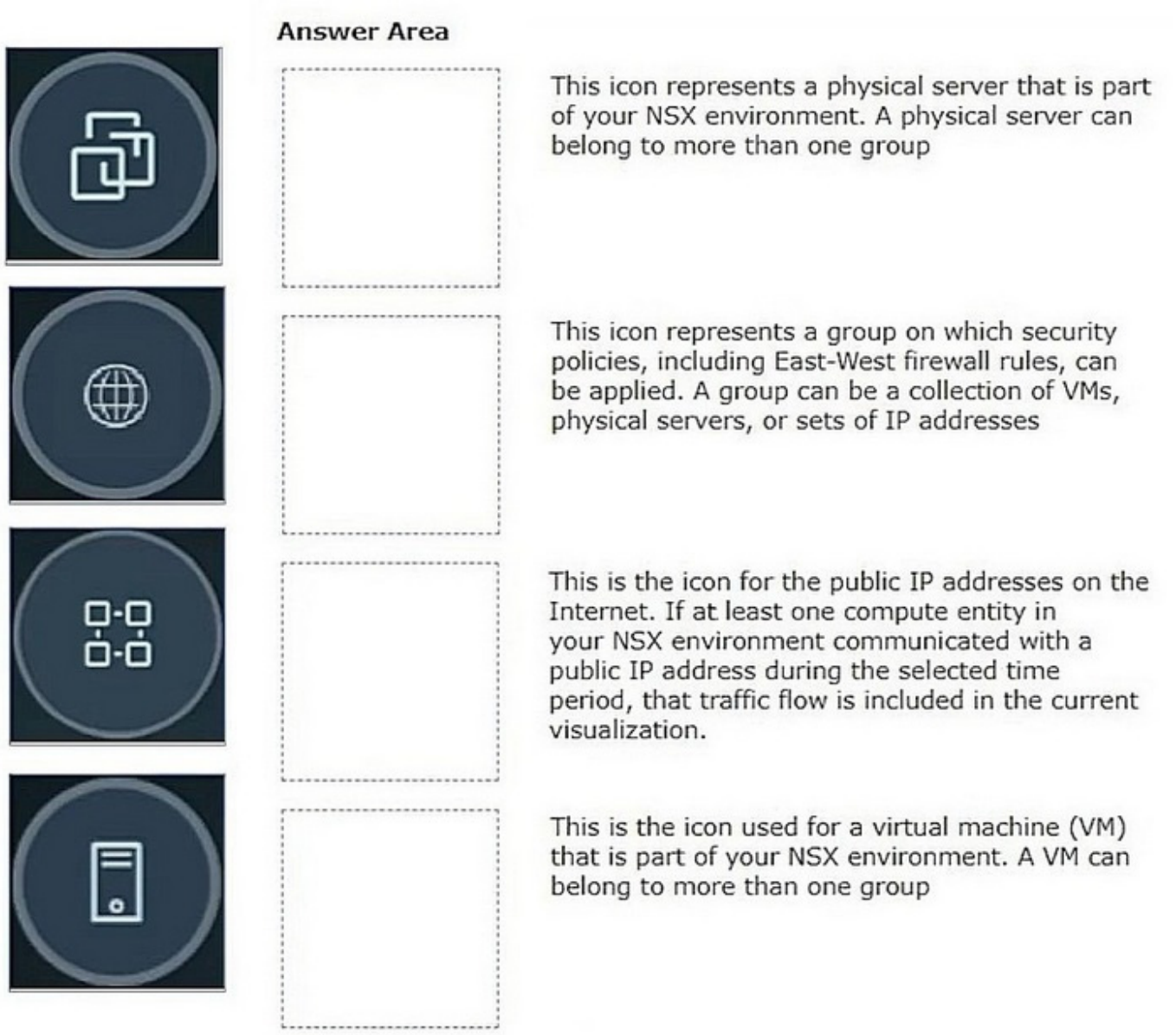
QUESTION 13

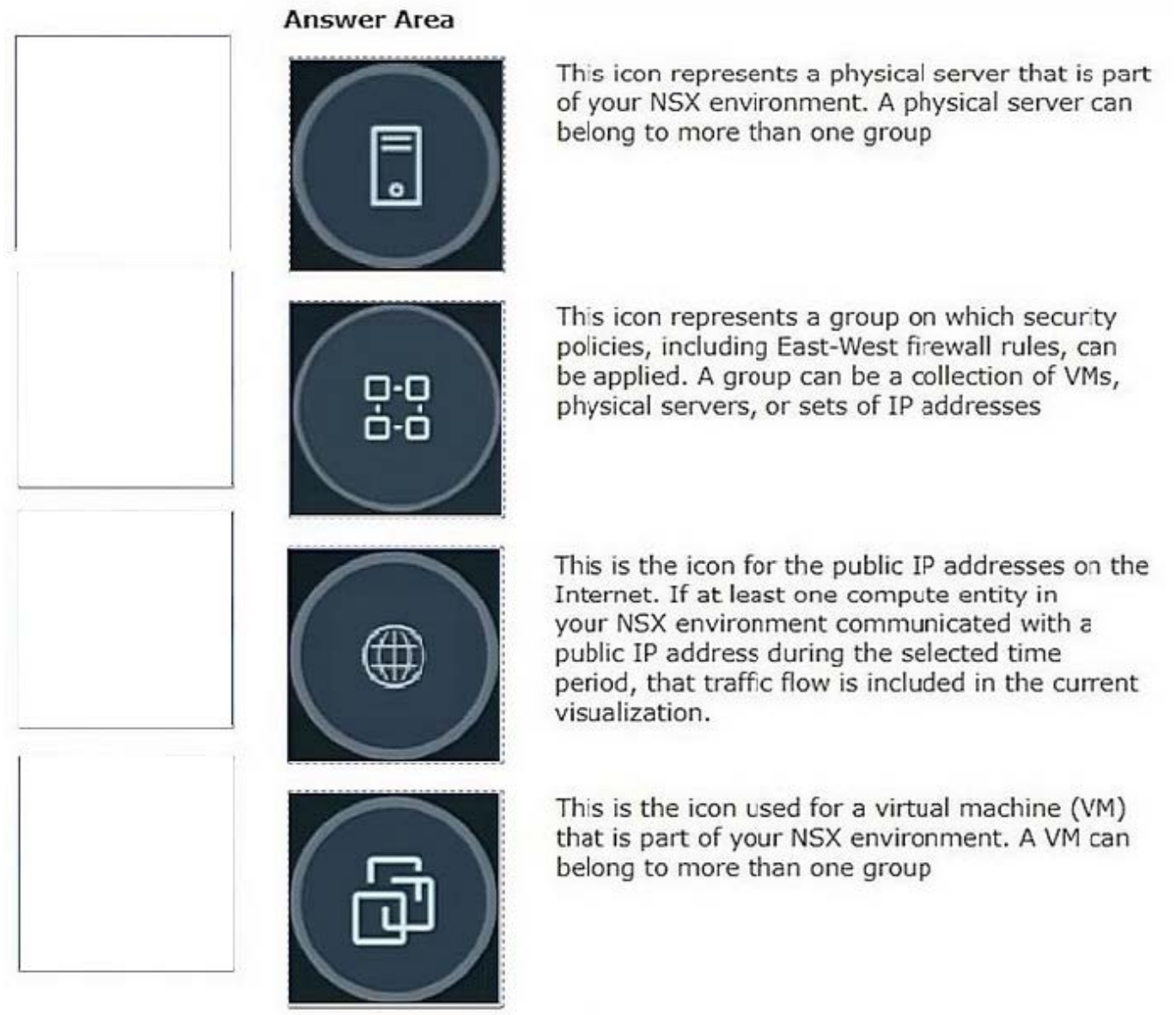
DRAG DROP

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.

Select and Place:

Correct Answer:





QUESTION 14

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-1l

B. esxcli network ip interface ipv4 get

C. esxcli network nic list

D. esxcfg-vmknic-1

E. net-dvs

Correct Answer: BD

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

https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/installation/GUID-B7E7371E-A9F6-4880-B184-E00A62C0C818.html https://www.vmadmin.co.uk/resources/35-esxserver/49-vmkniccmd

QUESTION 15

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

Correct Answer: AE

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 Reference: https ://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-41CC06DF-1CD4-4233-B43E-492A9A3AD5F6.html https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/6.4/ com.vmware.nsx.admin.doc/GUID-D44C8923-992F-4695-B9C0-5CC271679D09.html