# Free Questions for 2V0-41.23 by actualtestdumps

## Shared by Kirkland on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

# Question 1

**Question Type: MultipleChoice**

Which two steps must an NSX administrator take to integrate VMware Identity Manager in NSX to support role-based access control? (Choose two.)

## Options:

**A-** Create a SAML authentication in VMware Identity Manager using the NSX Manager FQDN.

**B-** Enter the Identity Provider (IdP) metadata URL in NSX Manager.

**C-** Create an OAuth 2.0 client in VMware Identity Manager.

**D-** Add NSX Manager as a Service Provider (SP) in VMware Identity Manager.

**E-** Enter the service URL, Client Secret, and SSL thumbprint in NSX Manager.

## Answer:

C, E

## Explanation:

https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-EAAD1FBE-F750-4A5A-A3BF-92B1E7D016FE.html

# Question 2

**Question Type:** **MultipleChoice**

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.)

## Options:

**A-** esxcfg-nics -1l

**B-** esxcli network ip interface ipv4 get

**C-** esxcli network nic list

**D-** esxcfg-vmknic -1

**E-** net-dvs

## Answer:

B, D

### 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

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 3

**Question Type:** **MultipleChoice**

Which three protocols could an NSX administrator use to transfer log messages to a remote log server? (Choose three.)

### Options:

**A-** HTTPS

**B-** TCP

**C-** SSH

**D-** UDP

**E-** TLS

**F-** SSL

### Answer:

B, D, E

### Explanation:

An NSX administrator can use TCP, UDP, or TLS protocols to transfer log messages to a remote log server. These protocols are supported by NSX Manager, NSX Edge, and hypervisors for remote logging. A Log Insight log server supports all these protocols, as well as LI and LI-TLS, which are specific to Log Insight and optimize network usage. HTTPS, SSH, and SSL are not valid protocols for remote logging in NSX-T Data Center.References: : VMware NSX-T Data Center Administration Guide, page 102.: VMware Docs: Configure Remote Logging

## Question 4

**Question Type:** **MultipleChoice**

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

## Options:

**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

# Question 5

**Question Type:** **MultipleChoice**

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

## Options:

**A-** NSX for vSphere Edge

**B-** 3rd party Hardware VPN Device

**C-** NSX Autonomous Edge

**D-** NSX Edge

## Answer:

C, D

## Explanation:

The following L2 VPN clients are recommended:

1. NSX Managed NSX Edge in a separate NSX Managed environment.

* Overlay and VLAN segments can be extended.

2. Autonomous Edge:

* Enables L2 VPN access from a non-a NSX environment to NSX environments.

* Deployed by using an OVF file on a host that is not managed by NSX.

* Only VLAN segments can be extended.

# Question 6

**Question Type: MultipleChoice**

Which of the following settings must be configured in an NSX environment before enabling stateful active-active SNAT?

## Options:

**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