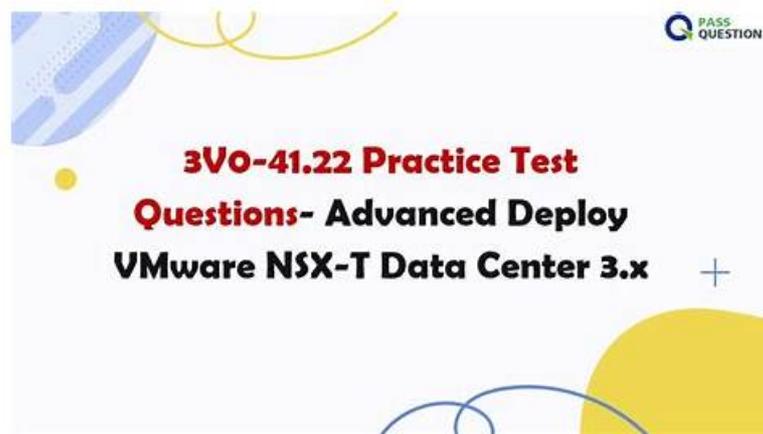


Benefits of Taking VMware 3V0-41.22 Practice Exams



P.S. Free 2026 VMware 3V0-41.22 dumps are available on Google Drive shared by Prep4sureGuide: https://drive.google.com/open?id=14n2v6pko5duJhdHkcbToyY7Tw_wQ3IT9

Because the registration fee is expensive, you have to win your Advanced Deploy VMware NSX-T Data Center 3.X to make all the spending worth it. Failing on your VMware 3V0-41.22 exam will not only cause you to lose money but also time and energy. On the other hand, winning a Advanced Deploy VMware NSX-T Data Center 3.X will open up so many doors that can bring you much forward on your career path. Of all the preparation resources for the Advanced Deploy VMware NSX-T Data Center 3.X 3V0-41.22 Exam available in the market, this VMware 3V0-41.22 braindumps are one of the most reliable materials. The development of these 3V0-41.22 question dumps involves feedback from hundreds of VMware professionals around the world. They also revise the VMware 3V0-41.22 exam questions regularly to keep them relevant to the latest Advanced Deploy VMware NSX-T Data Center 3.X exam.

For more information about the VMware 3V0-41.22 exam visit the following reference link:

VMware 3V0-41.22 Exam Reference link

>> Exam 3V0-41.22 Tutorial <<

3V0-41.22 Latest Study Materials, 3V0-41.22 Practice Test

In recruiting employees as IT engineers many companies look for evidence of all-round ability especially constantly studying ability more their education background. 3V0-41.22 dumps torrent can help you fight for VMware certification and achieve your dream in the shortest time. If you want to stand out from the crowd, purchasing a valid 3V0-41.22 Dumps Torrent will be a shortcut to success. It will be useful for you to avoid detours and save your money & time.

VMware Advanced Deploy VMware NSX-T Data Center 3.X Sample Questions (Q15-Q20):

NEW QUESTION # 15

Task4

You are tasked with creating a logical load balancer for several web servers that were recently deployed.

You need to:

• Create a standalone Tier-1 gateway with the following configuration detail:	
Name:	TI-LB
Linked Tier-0 Gateway:	None
Edge Cluster:	lb-edge-cluster
Service interface:	Name: T1-LB IP Address / Mask: 192.168.220.10/24 Connected To (Segment): Colimbus-LS
Static Route:	Add a default gateway to 192.168.220.1

• Create a load balancer and attach it to the newly created Tier-1 gateway with the following configuration detail:

Name:	web-lb
Size:	small
Attachment:	T1-LB

• Configure the load balancer with the following configuration detail:

- Create an HTTP application profile with the following configuration detail:

Name:	web-lb-app-profile
-------	--------------------

• Create an HTTP application profile with the following configuration detail:

Name:	web-lb-app-redirect-profile
Redirection:	HTTP to HTTPS Redirection

• Create an HTTP monitor with the following configuration detail:

Name:	web-lb-monitor
Port:	80

• Create an L7 HTTP virtual server with the following configuration detail:

Name:	web-lb-virtual-server
IP Address:	192.168.220.20
Port:	80
Load Balancer:	web-lb
Server Pool:	None
Application Profile:	web-lb-app-redirect-profile

• Create an L4 TCP virtual server with the following configuration detail:

Name:	web-lb-virtual-server-https
IP Address:	192.168.220.20
Port:	443
Load Balancer:	web-lb
Server Pool:	Columbus-web-servers
Application Profile:	default-tcp-lb-app-profile

Complete the requested task.

Notes:

Passwords are contained in the user_readme.txt. Do not wait for configuration changes to be applied in this task as processing may take some time to complete.

This task should take up to 35 minutes to complete and is required for subsequent tasks.

Answer:

Explanation:

See the Explanation part of the Complete Solution and step by step instructions.

Explanation

To create a logical load balancer for several web servers, you need to follow these steps:

Log in to the NSX Manager UI with admin credentials. The default URL is

https://<nsx-manager-ip-address>.

Navigate to Networking > Load Balancing > Load Balancers and click Add Load Balancer.

Enter a name and an optional description for the load balancer. Select the tier-1 gateway where you want to attach the load balancer from the drop-down menu or create a new one by clicking New Tier-1 Gateway. Click Save.

Navigate to Networking > Load Balancing > Application Profiles and click Add Application Profile.

Enter a name and an optional description for the application profile. Select HTTP as the application type from the drop-down menu. Optionally, you can configure advanced settings such as persistence, X-Forwarded-For, SSL offloading, etc., for the application profile. Click Save.

Navigate to Networking > Load Balancing > Monitors and click Add Monitor.

Enter a name and an optional description for the monitor. Select HTTP as the protocol from the drop-down menu. Optionally, you can configure advanced settings such as interval, timeout, fall count, rise count, etc., for the monitor. Click Save.

Navigate to Networking > Load Balancing > Server Pools and click Add Server Pool.

Enter a name and an optional description for the server pool. Select an existing application profile from the drop-down menu or create a new one by clicking New Application Profile. Select an existing monitor from the drop-down menu or create a new one by clicking New Monitor. Optionally, you can configure advanced settings such as algorithm, SNAT translation mode, TCP multiplexing, etc., for the server pool. Click Save.

Click Members > Set > Add Member and enter the IP address and port number of each web server that you want to add to the server pool. For example, enter 192.168.10.10:80 and 192.168.10.11:80 for two web servers listening on port 80. Click Save and then Close.

Navigate to Networking > Load Balancing > Virtual Servers and click Add Virtual Server.

Enter a name and an optional description for the virtual server. Enter the IP address and port number of the virtual server that will

receive the client requests, such as 10.10.10.100:80. Select HTTP as the service profile from the drop-down menu or create a new one by clicking New Service Profile. Select an existing server pool from the drop-down menu or create a new one by clicking New Server Pool.

Optionally, you can configure advanced settings such as access log, connection limit, rate limit, etc., for the virtual server. Click Save.

You have successfully created a logical load balancer for several web servers using NSX-T Manager UI.

NEW QUESTION # 16

Task 9

TO prepare for Virtual machine migration from VLAN-backed port groups to an overlay segment in NSX, a test bridge has been configured. The bridge is not functioning, and the -Bridge-VM- is not responding to ICMP requests from the main console.

You need to:

* Troubleshoot the configuration and make necessary changes to restore access to the application.

Complete the requested task.

Notes: Passwords are contained in the user_readme.txt. This task is not dependent on another. This task should take approximately 15 minutes to complete.

Answer:

Explanation:

See the Explanation part of the Complete Solution and step by step instructions.

Explanation

To troubleshoot the bridge configuration and restore access to the application, you need to follow these steps:

Log in to the NSX Manager UI with admin credentials. The default URL is

<https://<nsx-manager-ip-address>>.

Navigate to Networking > Segments and select the overlay segment that is bridged to the VLAN-backed port group. For example, select Web-01 segment that you created in Task 2.

Click Bridge > Set and verify the configuration details of the bridge. Check for any discrepancies or errors in the parameters such as bridge name, bridge ID, VLAN ID, edge node, etc.

If you find any configuration errors, click Edit and modify the parameters accordingly. Click Save to apply the changes.

If you do not find any configuration errors, check the connectivity and firewall rules between the overlay segment and the VLAN-backed port group. You can use ping or traceroute commands from the NSX Edge CLI or the vSphere Web Client to test the connectivity. You can also use show service bridge command to check the status of the bridge service on the NSX Edge.

If you find any connectivity or firewall issues, resolve them by adjusting the network settings or firewall rules on the NSX Edge or the vSphere Distributed Switch.

After resolving the issues, verify that the bridge is functioning and the Bridge-VM is responding to ICMP requests from the main console. You can also check the MAC addresses learned by the bridge on both sides of the network using show service bridge mac command on the NSX Edge CLI.

NEW QUESTION # 17

SIMULATION

Task 6

You are asked to integrate NSX manager with LDAP to better control NSX administrators' roles and responsibilities. Ensure users can manage the NSX environment utilizing Active Directory login credentials.

You need to:

* Configure NSX Manager LDAP integration to the corp.local domain using the following configuration detail:

• Configure NSX Manager LDAP integration to the corp.local domain using the following configuration detail:	
LDAP Identity source name:	corp.local
Domain Name:	corp.local
BASE DN:	DC=CORP, DC=local
Type:	Active Directory over LDAP
Active Directory host name:	controlcenter.corp.local
LDAP Protocol:	LDAP
LDAP Port:	389
User Start TLS:	disabled
Bind identity user name:	administrator@corp.local
Bind identity password:	VMware!!

* Configure the user nsx-admin@corp.local Active Directory account as an Enterprise Admin access role.

Complete the requested task.

Notes:

Passwords are contained in the user_readme.txt. You may want to move to other tasks/steps while waiting for configuration changes to be applied. This task should take approximately 15 minutes to complete.

Answer:

Explanation:

See the Explanation part of the Complete Solution and step by step instructions Explanation:

To integrate NSX Manager with LDAP to better control NSX administrators' roles and responsibilities, you need to follow these steps:

Log in to the NSX Manager UI with admin credentials. The default URL is <https://<nsx-manager-ip-address>>.

Navigate to System > User Management > LDAP and click Add Identity Source.

Enter a name for the identity source, such as corp.local.

Enter the domain name of your Active Directory server, such as DC=corp,DC=local.

Select Active Directory over LDAP as the type from the drop-down menu.

Click Set to configure LDAP servers. You can add up to three LDAP servers for failover support, to each domain.

Enter the hostname or IP address of your LDAP server, such as corpdserver.corp.local.

Select LDAP as the protocol from the drop-down menu.

Enter the port number for the LDAP server, such as 389.

Click Connection Status to test the connection to the LDAP server. If successful, you will see a green check mark and a message saying "Connection successful".

Optionally, you can enable StartTLS to use encryption for the LDAP connection. To do this, toggle the Use StartTLS button and enter the certificate of the LDAP server in PEM format in the text box below.

Click Save to add the LDAP server.

Repeat steps 6 to 12 to add more LDAP servers if needed.

Enter the bind entry user name and password for the LDAP server, such as Administrator@corp.local and VMware!@.

Click Save to create the identity source.

Navigate to System > User Management > Users and Roles and click Add Role Assignment for LDAP.

Select corp.local as the domain from the drop-down menu.

Enter nsx-admin@corp.local in the search box and select it from the list that appears.

Select Enterprise Admin as the role from the drop-down menu.

Click Save to assign the role to the user.

You have successfully integrated NSX Manager with LDAP and configured nsx-admin@corp.local Active Directory account as an Enterprise Admin access role.

NEW QUESTION # 18

SIMULATION

Task 7

you are asked to create a custom QoS profile to prioritize the traffic on the phoenix-VLAN segment and limit the rate of ingress traffic.

You need to:

* Create a custom QoS profile for the phoenix-VLAN using the following configuration detail:

• Create a custom QoS profile for the phoenix-VLAN using the following configuration detail:	
Name:	ingress-phoenix-qos-profile
Priority:	0
Class of Service:	0
Ingress traffic rate limit:	100 Mbps for average, 200 Mbps for peak

* Apply the profile on the 'phoenix-VLAN' segment

Complete the requested task.

Notes: Passwords are contained in the user_readme.txt.

take approximately 5 minutes to complete.

Subsequent tasks may require the completion of this task. This task should

Answer:

Explanation:

See the Explanation part of the Complete Solution and step by step instructions Explanation:

To create a custom QoS profile to prioritize the traffic on the phoenix-VLAN segment and limit the rate of ingress traffic, you need to follow these steps:

Log in to the NSX Manager UI with admin credentials. The default URL is <https://<nsx-manager-ip-address>>.

Navigate to Networking > Segments > Switching Profiles and click Add Switching Profile. Select QoS as the profile type. Enter a name and an optional description for the QoS profile, such as phoenix-QoS.

In the Mode section, select Untrusted as the mode from the drop-down menu. This will allow you to set a custom DSCP value for the outbound IP header of the traffic on the segment.

In the Priority section, enter 46 as the DSCP value. This will mark the traffic with Expedited Forwarding (EF) per-hop behavior, which is typically used for high-priority applications such as voice or video.

In the Class of Service section, enter 5 as the CoS value. This will map the DSCP value to a CoS value that can be used by VLAN-based logical ports or physical switches to prioritize the traffic.

In the Ingress section, enter 1000000 as the Average Bandwidth in Kbps. This will limit the rate of inbound traffic from the VMs to the logical network to 1 Mbps.

Optionally, you can also configure Peak Bandwidth and Burst Size settings for the ingress traffic, which will allow some burst traffic above the average bandwidth limit for a short duration.

Click Save to create the QoS profile.

Navigate to Networking > Segments and select the phoenix-VLAN segment that you want to apply the QoS profile to. Click Actions > Apply Profile and select phoenix-QoS as the switching profile that you want to apply to the segment. Click Apply to apply the profile to the segment.

You have successfully created a custom QoS profile and applied it to the phoenix-VLAN segment.

NEW QUESTION # 19

SIMULATION

Task 3

You are asked to deploy a new instance of NSX-T into an environment with two isolated tenants. These tenants each have separate physical data center cores and have standardized on BCP as a routing protocol.

You need to:

• Configure a new Edge cluster with the following configuration detail:	
Name:	edge-cluster-01
Edge cluster profile:	nsx-default-edge-high-availability-profile
Includes Edges:	nsx-edge-01 and nsx-edge-02
• Configure a Tier-0 Gateway with the following configuration detail:	
Name:	TO-01
HA Mode:	Active Active
Edge cluster:	edge-cluster-01
• Configure two ECMP Uplinks to provide maximum throughput and fault tolerance. Use the following configuration detail:	
◦ Uplink-1	
Type:	External
Name:	Uplink-1
IP Address/Mask:	192.168.100.2/24
Connected to:	Uplink
Edge Node:	nsx-edge-01
• Uplink-2	
Type:	External
Name:	Uplink-2
IP Address/Mask:	192.168.100.3/24
Connected to:	Uplink
Edge Node:	nsx-edge-02
• Configure BGP on the Tier-0 Gateway with the following detail:	
Local AS:	65001
BGP Neighbors:	IP Address: 192.168.100.1 BFD: Disabled Remote AS Number: 65002
Additional Info:	All other values should remain at default while ensuring that ECMP is On
Source Addresses:	192.168.100.2 and 192.168.100.3
• Configure VRF Lite for the secondary tenant with the following detail:	
Name:	TO-01-vrf
Connected to Tier-0 Gateway:	TO-01

Complete the requested task.

Notes: Passwords are Contained in the user_readme.txt. Task 3 is dependent on the Completion Of Task and 2. Other tasks are dependent On the Completion Of this task. Do not wait for configuration changes to be applied in this task as processing may take up to 10 minutes to complete. Check back on completion. This task should take approximately 10 minutes to complete.

Answer:

Explanation:

See the Explanation part of the Complete Solution and step by step instructions Explanation:

To deploy a new instance of NSX-T into an environment with two isolated tenants, you need to follow these steps:

Log in to the NSX Manager UI with admin credentials. The default URL is <https://<nsx-manager-ip-address>>.

Navigate to System > Fabric > Nodes > Edge Transport Nodes and click Add Edge VM.

Enter a name and an optional description for the edge VM. Select the compute manager, cluster, and resource pool where you want to deploy the edge VM. Click Next.

Select the deployment size and form factor for the edge VM. For this task, you can select Medium as the size and VM as the form factor. Click Next.

Select the datastore and folder where you want to store the edge VM files. Click Next.

Configure the management network settings for the edge VM. Enter a hostname, a management IP address, a default gateway, a DNS server, and a domain search list. Optionally, you can enable SSH and join the edge VM to a domain. Click Next.

Configure the transport network settings for the edge VM. Select an N-VDS as the host switch type and enter a name for it. Select an uplink profile from the drop-down menu or create a new one by clicking New Uplink Profile. Map the uplinks to the physical NICs on the edge VM. For example, map Uplink 1 to fp-eth0 and Uplink 2 to fp-eth1. Optionally, you can configure IP assignment, MTU, or LLDP for the uplinks. Click Next.

Review the configuration summary and click Finish to deploy the edge VM.

Repeat steps 2 to 8 to deploy another edge VM for redundancy.

Navigate to Networking > Tier-0 Gateway and click Add Gateway > VRF.

Enter a name and an optional description for the VRF gateway. Select an existing tier-0 gateway as the parent gateway or create a new one by clicking New Tier-0 Gateway.

Click VRF Settings and enter a VRF ID for the tenant. Optionally, you can enable EVPN settings if you want to use EVPN as the control plane protocol for VXLAN overlay networks.

Click Save to create the VRF gateway.

Repeat steps 10 to 13 to create another VRF gateway for the second tenant with a different VRF ID.

Navigate to Networking > Segments and click Add Segment.

Enter a name and an optional description for the segment. Select VLAN as the connectivity option and enter a VLAN ID for the segment. For example, enter 128 for Tenant A's first uplink VLAN segment.

Select an existing transport zone from the drop-down menu or create a new one by clicking New Transport Zone.

Click Save to create the segment.

Repeat steps 15 to 18 to create three more segments for Tenant A's second uplink VLAN segment (VLAN ID 129) and Tenant B's uplink VLAN segments (VLAN ID 158 and 159).

Navigate to Networking > Tier-0 Gateway and select the VRF gateway that you created for Tenant A.

Click Interfaces > Set > Add Interface.

Enter a name and an optional description for the interface.

Enter the IP address and mask for the external interface in CIDR format, such as 10.10.10.1/24.

In Type, select External.

In Connected To (Segment), select the VLAN segment that you created for Tenant A's first uplink VLAN segment (VLAN ID 128).

Select an edge node where you want to attach the interface, such as Edge-01.

Enter the Access VLAN ID from the list as configured for the segment, such as 128.

Click Save and then Close.

Repeat steps 21 to 28 to create another interface for Tenant A's second uplink VLAN segment (VLAN ID 129) on another edge node, such as Edge-02.

Repeat steps 20 to 29 to create two interfaces for Tenant B's uplink VLAN segments (VLAN ID 158 and 159) on each edge node using their respective VRF gateway and IP addresses.

Configure BGP on each VRF gateway using NSX UI or CLI commands¹². You need to specify the local AS number, remote AS number, BGP neighbors, route redistribution, route filters, timers, authentication, graceful restart, etc., according to your requirements³⁴.

Configure BGP on each physical router using their respective CLI commands⁵⁶. You need to specify similar parameters as in step 31 and ensure that they match with their corresponding VRF gateway settings⁷⁸.

Verify that BGP sessions are established between each VRF gateway and its physical router neighbors using NSX UI or CLI commands . You can also check the routing tables and BGP statistics on each device .

You have successfully deployed a new instance of NSX-T into an environment with two isolated tenants using VRF Lite and BGP.

NEW QUESTION # 20

.....

