Best VMware 3V0-41.22 Vce & 3V0-41.22 Latest Exam Simulator

P.S. Free & New 3V0-41.22 dumps are available on Google Drive shared by Exams4Collection: https://drive.google.com/open?id=1YIgtmKweJWOQbX7j4F4Lj6NcwIcziqv_

As our loyal customers wrote to us that with the help of our 3V0-41.22 exam questions, they have successfully passed the exam and achieved the certification. They are now living the life they desired before. While you are now hesitant for purchasing our 3V0-41.22 Real Exam, some people have already begun to learn and walk in front of you! So what you should do is to make the decision to buy our 3V0-41.22 practice engine right now. The time and tide wait for no man!

VMware 3V0-41.22 exam is designed to test the candidate's knowledge of the advanced deployment of VMware NSX-T Data Center 3.X. VMware NSX-T Data Center is a network virtualization and security platform that enables the creation of entire networks in software, providing greater flexibility and faster deployment. 3V0-41.22 Exam covers a broad range of topics related to the NSX-T Data Center 3.X, including multi-site deployments, infrastructure and workload security, and advanced policies and services.

>> Best VMware 3V0-41.22 Vce <<

3V0-41.22 Latest Exam Simulator - Test 3V0-41.22 Assessment

The hit rate of 3V0-41.22 study engine is very high. Imagine how happy it would be to take a familiar examination paper in a familiar

environment! You can easily pass the exam, after using 3V0-41.22 training materials. You no longer have to worry about after the exam. At the moment you put the paper down you can walk out of the examination room with confidence. 3V0-41.22 study engine is so amazing. What are you waiting for?

To prepare for the VMware 3V0-41.22 exam, candidates should have a solid understanding of networking fundamentals, virtualization concepts, and cloud computing. They should also have hands-on experience in deploying and managing VMware NSX-T Data Center 3.X in a production environment. VMware recommends attending the Advanced NSX-T Data Center course before taking 3V0-41.22 Exam.

VMware Advanced Deploy VMware NSX-T Data Center 3.X Sample Questions (Q11-Q16):

NEW QUESTION # 11
SIMULATION
Task 13
You have been asked to configure the NSX backups for the environment so that if the NSX Manager fails it can be restored with the same IP address to the original primary Data Center that is in an Active / Standby configuration. Backups should be scheduled to run once every 24 hours as well as when there are changes published to the NSX environment. Ensure that backups are completed on their respective environment. Verify the backup file has been created on the SFTP server.
* Credentials needed to complete the task:

SFTP User:	sftpuser
Password:	VMware1!
SFTP IP:	192.168.110.91
Hostname:	ubuntu-01.corp.local

You need to:
* Verify that an SFTP server is available on the network and obtain SFTP Fingerprint.
* Configure NSX Backups via NSX Appliance Backup
* Configure Scheduling Criteria
Backup Configuration Criteria

Backup Schedule:	Once backup per 24 hours
Additional Backup Triggers:	Detect NSX configuration (5 min time interval)
Primary Data Center Configuration:	Active / Standby
Backup locations:	All backups on respective NSX environment
Additional Notes:	NSX Manager shall be restored with same IP address
Directory Path:	/data
Passphrase:	VMware1!

Complete the requested task.
Notes: Passwords are contained in the user_readme.txt. This task is not dependent on other tasks. 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 configure the NSX backups for the environment, you need to follow these steps:
Verify that an SFTP server is available on the network and obtain SFTP fingerprint. You can use the search_web("SFTP server availability") tool to find some information on how to set up and check an SFTP server. You can also use the ssh-keyscan command to get the fingerprint of the SFTP server. For example, ssh-keyscan -t ecdsa sftp_server will return the ECDSA key of the sftp_server. You can compare this key with the one displayed on the NSX Manager UI when you configure the backup settings.
Configure NSX Backups via NSX Appliance Backup. Log in to the NSX Manager UI with admin credentials. The default URL is https://<nsx-manager-ip-address>. Select System > Lifecycle Management > Backup & Restore. Click Edit under the SFTP Server label to configure your SFTP server. Enter the FQDN or IP address of the backup file server, such as 10.10.10.100. The protocol text box is already filled in. SFTP is the only supported protocol. Change the default port if necessary. The default TCP port is 22. In the Directory Path text box, enter the absolute directory path where the backups will be stored, such as /dat a. The directory must already exist and cannot be the root directory (/). Avoid using path drive letters or spaces in directory names; they are not supported. In the Passphrase text box, enter a passphrase that will be used to encrypt and decrypt the backup files, such as VMware1!. Click Save to create the backup configuration.
Configure Scheduling Criteria. On the Backup & Restore page, click Edit under the Schedule label to configure your backup schedule. Select Enabled from the drop-down menu to enable scheduled backups. Select Daily from the Frequency drop-down menu to run backups once every 24 hours. Select a time from the Time drop-down menu to specify when the backup will start, such as 12:00 AM. Select Enabled from the Additional Backup Trigger drop-down menu to run backups when there are changes

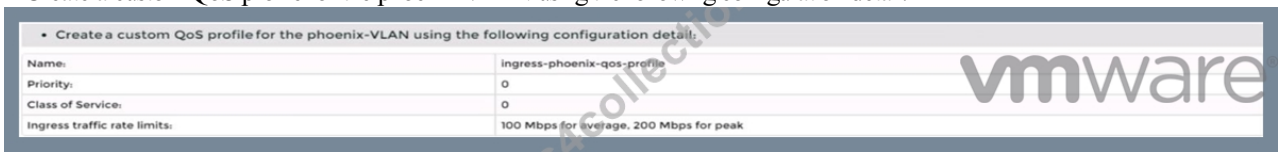
published to the NSX environment. Click Save to create the backup schedule.
Verify that a backup file has been created on the SFTP server. On the Backup & Restore page, click Start Backup to run a manual backup and verify that it completes successfully. You should see a message saying "Backup completed successfully". You can also check the status and details of your backups on this page, such as backup size, duration, and timestamp. Alternatively, you can log in to your SFTP server and check if there is a backup file in your specified directory path, such as /data.

NEW QUESTION # 12
Task 10
You have been notified by the Web Team that they cannot get to any northbound networks from their Tampa web servers that are deployed on an NSX-T network segment. The Tampa web VM's however can access each other.
You need to:
* Troubleshoot to find out why the Tampa web servers cannot communicate to any northbound networks and resolve the issue.
Complete the requested task. TO verify your work. ping the Control Center @ 192.168.110.10 Notes: Passwords are contained in the user_readme.txt. This task is dependent on Task 4. Some exam candidates may have already completed this task if they had done more than the minimum required in Task 4.
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 why the Tampa web servers cannot communicate to any northbound networks, 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 > Tier-0 Gateway and select the tier-0 gateway that connects the NSX-T network segment to the northbound networks. For example, select T0-GW-01.
Click Interfaces > Set and verify the configuration details of the interfaces. Check for any discrepancies or errors in the parameters such as IP address, subnet mask, MTU, 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 tier-0 gateway and the northbound networks. 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 router command to check the status of the routing 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 northbound devices.
After resolving the issues, verify that the Tampa web servers can communicate to any northbound networks by pinging the Control Center @ 192.168.110.10 from one of the web servers.

NEW QUESTION # 13
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:



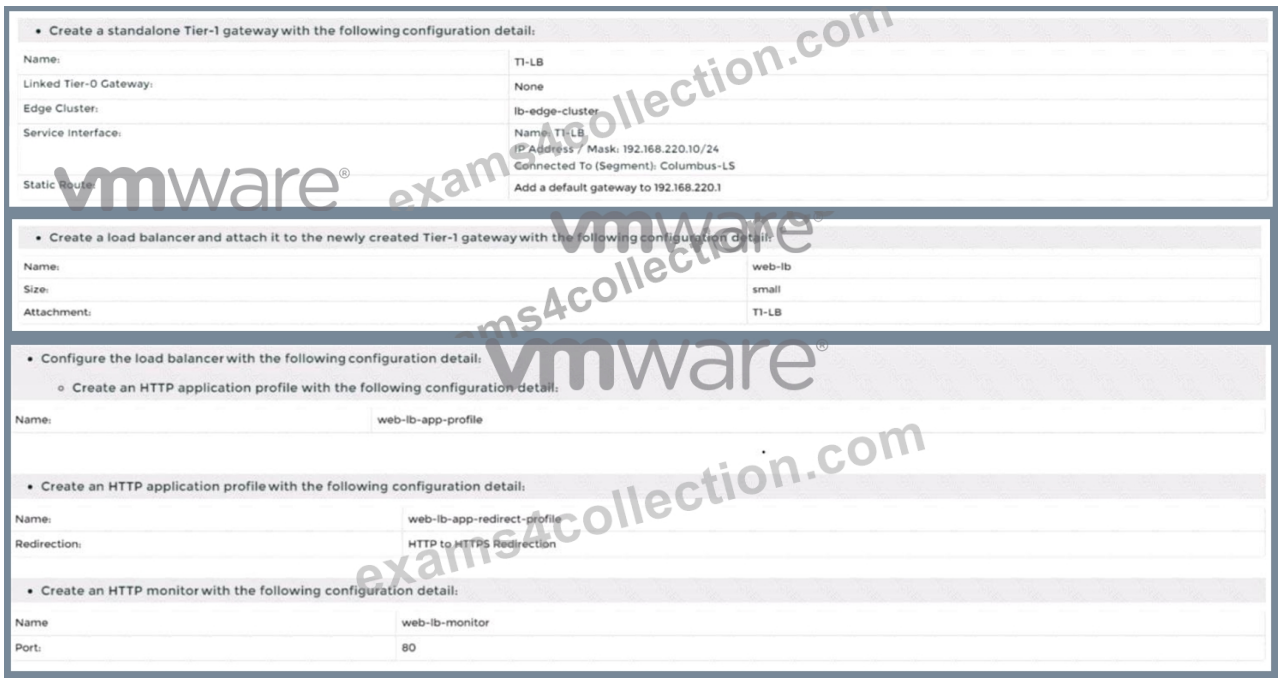
* Apply the profile on the 'phoenix-VLAN' segment
Complete the requested task.
Notes: Passwords are contained in the user_readme.txt.
take approximately 5 minutes to complete.
Subsequent tasks may require the completion of this task. This task should

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 # 14
Task4
You are tasked with creating a logical load balancer for several web servers that were recently deployed.
You need to:



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 # 15
Task 8
You are tasked With troubleshooting the NSX IPSec VPN service Which has been reported down. Verify the current NSX configuration is deployed and resolve any issues.
You need to:
* Verify the present configuration as provided below:

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 NSX IPSec VPN service that has been reported down, 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 > VPN > IPSec VPN and select the IPSec VPN session that is down. You can identify the session by its name, local endpoint, remote endpoint, and status.
Click Show IPSec Statistics and view the details of the IPSec VPN session failure. You can see the error message, the tunnel state, the IKE and ESP status, and the statistics of the traffic sent and received.
Compare the configuration details of the IPSec VPN session with the expected configuration as provided below. Check for any discrepancies or errors in the parameters such as local and remote endpoints, local and remote networks, IKE and ESP profiles, etc.
If you find any configuration errors, click Actions > 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 local and remote endpoints. You can use ping or traceroute commands from the NSX Edge CLI to test the connectivity. You can also use show service ipsec command to check the status of IPSec VPN 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 third-party device.
After resolving the issues, verify that the IPSec VPN session is up and running by refreshing the IPSec VPN page on the NSX Manager UI. You can also use show service ipsec sp and show service ipsec sa commands on the NSX Edge CLI to check the status of security policy and security association for the IPSec VPN session.

NEW QUESTION # 16
.....

www.prep4pass.com □ enter 《 3V0-41.22 》 and obtain a free download □3V0-41.22 Test Discount

- palangshim.com, gxfk.fktime.com, www.stes.tyc.edu.tw, pedforsupplychain.my.id, learn.stmarysfarm.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, rock2jazz.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that Exams4Collection 3V0-41.22 dumps now are free: https://drive.google.com/open?id=1YIgtmKweJWOQbX7j4F4Lj6NcwIcziqv_