

Free PDF VMware - 3V0-41.22–Trustable Test Pdf



VMware

3V0-22.21N
Advanced Deploy VMware vSphere 7.x

- Up to Date products, reliable and verified.
- Questions and Answers in PDF Format.

Full Version Features:

- 90 Days Free Updates
- 30 Days Money Back Guarantee
- Instant Download Once Purchased
- 24 Hours Live Chat Support

For More Information:

<https://www.testsexpert.com/>

• Product Version

Visit us at <https://www.testsexpert.com/3v0-22-21n>

BTW, DOWNLOAD part of VCE Dumps 3V0-41.22 dumps from Cloud Storage: https://drive.google.com/open?id=1nvbF5XT4Bswzxd48d_yyxaeBJGFhxPKB

One of the best features of VMware 3V0-41.22 exam dumps is its Advanced Deploy VMware NSX-T Data Center 3.X exam passing a money-back guarantee. Now with VCE Dumps 3V0-41.22 exam dumps your investment is secured with a money-back guarantee. If you fail in VMware 3V0-41.22 Exam despite using VCE Dumps Exam Questions you can claim your paid amount.

There are three versions of 3V0-41.22 training materials for the candidate of you, and different versions have different advantages, you can use it in accordance with your own habit. Free update for each version for one year, namely, you don't need to buy the same version for many times, and the update version will send to you automatically. You will get the latest version of 3V0-41.22 Training Materials.

>> 3V0-41.22 Test Pdf <<

Newest 3V0-41.22 Test Pdf – 100% Pass-Sure Advanced Deploy VMware NSX-T Data Center 3.X Exam Learning

If you want to achieve that you must boost an authorized and extremely useful certificate to prove that you boost good abilities and plenty of knowledge in some area. Passing the test 3V0-41.22 certification can help you realize your goal and if you buy our 3V0-41.22 latest torrent you will pass the exam successfully. Our product boosts many merits and high passing rate. Our products have 3

versions and we provide free update of the 3V0-41.22 Exam Torrent to you. If you are the old client you can enjoy the discounts.

VMware 3V0-41.22 exam is a specialist-level certification exam that validates the candidate's ability to design, implement, and manage NSX-T Data Center 3.X-based solutions. 3V0-41.22 exam measures the candidate's knowledge and skills in areas such as NSX-T Data Center architecture, installation, configuration, and management of NSX-T Data Center components, advanced networking and security features, and integration with other VMware products and solutions. Advanced Deploy VMware NSX-T Data Center 3.X certification exam is designed for experienced professionals who are responsible for deploying and managing NSX-T Data Center 3.X in complex enterprise environments.

VMware 3V0-41.22 Certification Exam is a valuable credential that demonstrates the candidates' expertise in advanced deployment of VMware NSX-T Data Center 3.X. Advanced Deploy VMware NSX-T Data Center 3.X certification is recognized globally and is highly respected by IT professionals and employers. Achieving this certification can open up new career opportunities and increase the earning potential of candidates.

VMware Advanced Deploy VMware NSX-T Data Center 3.X Sample Questions (Q13-Q18):

NEW QUESTION # 13

SIMULATION

Task 12

An issue with the Tampa web servers has been reported. You would like to replicate and redirect the web traffic to a network monitoring tool outside Of the NSX-T environment to further analyze the traffic.

You are asked to configure traffic replication to the monitoring software for your Tampa web overlay segments with bi-directional traffic using this detail:

Session Name:	Network-Monitor-01
Network Appliance Name/Group:	NM-01
Direction:	Bi Directional
TCP/IP Stack:	Default
Encapsulation Type:	GRE

Complete the requested configuration.

Notes: Passwords are contained in the user_readme.txt. This task is not dependent on other tasks. 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 configure traffic replication to the monitoring software for your Tampa web overlay segments with bi-directional 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 and select the Tampa web overlay segment that you want to replicate the traffic from. For example, select Web-01 segment that you created in Task 2.

Click Port Mirroring > Set > Add Session and enter a name and an optional description for the port mirroring session. For example, enter Tampa-Web-Monitoring.

In the Direction section, select Bi-directional as the direction from the drop-down menu. This will replicate both ingress and egress traffic from the source to the destination.

In the Source section, click Set and select the VMs or logical ports that you want to use as the source of the traffic. For example, select Web-VM-01 and Web-VM-02 as the source VMs. Click Apply.

In the Destination section, click Set and select Remote L3 SPAN as the destination type from the drop-down menu. This will allow you to replicate the traffic to a remote destination outside of the NSX-T environment.

Enter the IP address of the destination device where you have installed the network monitoring software, such as 10.10.10.200.

Select an existing service profile from the drop-down menu or create a new one by clicking New Service Profile. A service profile defines the encapsulation type and other parameters for the replicated traffic.

Optionally, you can configure advanced settings such as TCP/IP stack, snap length, etc., for the port mirroring session.

Click Save and then Close to create the port mirroring session.

You have successfully configured traffic replication to the monitoring software for your Tampa web overlay segments with bi-directional traffic using NSX-T Manager UI.

NEW QUESTION # 14

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 # 15

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:	T0-01
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-vr
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 # 16

SIMULATION

Task 4

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: TI-LB IP Address: 192.168.220.10/24 Connected To (Segment): Columbus-L5
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:	TI-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, fail 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 # 17

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:	VMware!!
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:	VMware!!

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 /data. 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 # 18

.....

Passing the 3V0-41.22 exam has never been so efficient or easy when getting help from our 3V0-41.22 training materials. This way is not only financially accessible, but time-saving and comprehensive to deal with the important questions emerging in the real exam. All exams from different suppliers will be easy to handle. Actually, this 3V0-41.22 Exam is not only practical for working or studying conditions, but a manifest and prestigious show of your personal ability.

3V0-41.22 Exam Learning: <https://www.vcedumps.com/3V0-41.22-examcollection.html>

- Test 3V0-41.22 Collection □ Latest 3V0-41.22 Exam Questions Vce □ 3V0-41.22 Frequent Update □ The page for free download of 【 3V0-41.22 】 on ☀ www.examsreviews.com □ ☀ □ will open immediately □ 3V0-41.22 Frequent Update
- New Soft 3V0-41.22 Simulations □ 3V0-41.22 Exam Reference □ 3V0-41.22 Exam Preview □ Enter (www.pdfvce.com) and search for ☀ 3V0-41.22 □ ☀ □ to download for free □ Test 3V0-41.22 Collection
- Hot 3V0-41.22 Test Pdf 100% Pass | Valid 3V0-41.22: Advanced Deploy VMware NSX-T Data Center 3.X 100% Pass □ Download (3V0-41.22) for free by simply entering ➤ www.getvalidtest.com □ website □ 3V0-41.22 Exam Outline
- VMware 3V0-41.22 Questions - Latest Preparation Material [2025] ♣ Search for ▷ 3V0-41.22 ◁ and download exam materials for free through ➡ www.pdfvce.com □ □ 3V0-41.22 Exam Discount Voucher
- 2025 Trustable 100% Free 3V0-41.22 – 100% Free Test Pdf | Advanced Deploy VMware NSX-T Data Center 3.X Exam Learning □ Open ⇒ www.real4dumps.com ⇐ enter [3V0-41.22] and obtain a free download □ Study Guide 3V0-41.22 Pdf
- 3V0-41.22 Exam Preview □ 3V0-41.22 Best Practice □ 3V0-41.22 Valid Dumps Ebook □ Go to website ☀ www.pdfvce.com □ ☀ □ open and search for ➡ 3V0-41.22 □ to download for free □ 3V0-41.22 Updated Dumps
- 3V0-41.22 Exam Preview □ 3V0-41.22 Exam Reference ◁ 3V0-41.22 Valid Dumps Ebook □ Simply search for □ 3V0-41.22 □ for free download on 《 www.testsdumps.com 》 □ 3V0-41.22 Exam Reference
- 2025 Trustable 100% Free 3V0-41.22 – 100% Free Test Pdf | Advanced Deploy VMware NSX-T Data Center 3.X Exam Learning □ Search for ▷ 3V0-41.22 ◁ and obtain a free download on □ www.pdfvce.com □ □ Reliable 3V0-41.22 Dumps Files
- Test 3V0-41.22 Questions Fee □ 3V0-41.22 Exam Reference □ 3V0-41.22 Exam Preview □ Search for □ 3V0-41.22 □ and download it for free immediately on ⇒ www.examcollectionpass.com ⇐ □ 3V0-41.22 Best Practice
- Obtain Latest 3V0-41.22 Test Pdf - All in Pdfvce □ ☀ www.pdfvce.com □ ☀ □ is best website to obtain ➡ 3V0-41.22 □ for free download □ 3V0-41.22 Updated Dumps
- 2025 Trustable 100% Free 3V0-41.22 – 100% Free Test Pdf | Advanced Deploy VMware NSX-T Data Center 3.X Exam

Learning \ Search for ▷ 3V0-41.22 ◁ and download it for free immediately on ➡ www.free4dump.com ☐ ☐ Latest 3V0-41.22 Exam Questions Vce

- 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, ncon.edu.sa, tedcole945.bloggactif.com, www.stes.tyc.edu.tw, edu.ahosa.com.ng, adamree449.bloggazzo.com, techsafetycourses.com, hackingworlds.com, www.comsenz-service.com, Disposable vapes

2025 Latest VCE Dumps 3V0-41.22 PDF Dumps and 3V0-41.22 Exam Engine Free Share: https://drive.google.com/open?id=1nvbF5XT4Bswzxd48d_yyxaeBJGFhxPKB