Pass Guaranteed Quiz 2026 VMware 3V0-41.22: Useful Advanced Deploy VMware NSX-T Data Center 3.X Free Exam Questions

P.S. Free 2026 VMware 3V0-41.22 dumps are available on Google Drive shared by DumpTorrent: https://drive.google.com/open?id=1dembny7hTZauqjPBtAwBYuOpXkxD_7vJ

We regularly update our valid VMware 3V0-41.22 certification test preparation material to keep them in line with the current VMware 3V0-41.22 exam content and industry standards. Professionals from different countries give us their valuable feedback to refine 3V0-41.22 Actual Dumps even more.

What is the salary of the VMware 3V0-41.22 Exam

The Average salary of different countries for Advanced Deploy VMware professionals:

- India: INR 5001216 per year
- UK: Pounds 52395 per year
- United States: USD 64,000 per year

>> 3V0-41.22 Free Exam Questions <<

New 3V0-41.22 Test Practice - 3V0-41.22 Mock Test

DumpTorrent provides the most up-to-date Advanced Deploy VMware NSX-T Data Center 3.X 3V0-41.22 exam questions and practice material to assist you in preparing for the VMware 3V0-41.22 exam. Our Advanced Deploy VMware NSX-T Data Center 3.X 3V0-41.22 exam questions preparation material helps countless people worldwide in becoming certified professionals. Our Advanced Deploy VMware NSX-T Data Center 3.X 3V0-41.22 Exam Questions are available in three simple formats, allowing customers to select the most appropriate option according to their needs.

VMware Advanced Deploy VMware NSX-T Data Center 3.X Sample Questions (Q14-Q19):

NEW QUESTION # 14
SIMULATION
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:

NSX IPSec Session Name:	IPSEC
Remote IP:	192.168.140.2
Local Networks:	10.10.10.0/24
Remove Networks:	10.10.20.0/24
Pre-shared Key:	VMware1!VMware1!

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 # 15
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 # 16
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

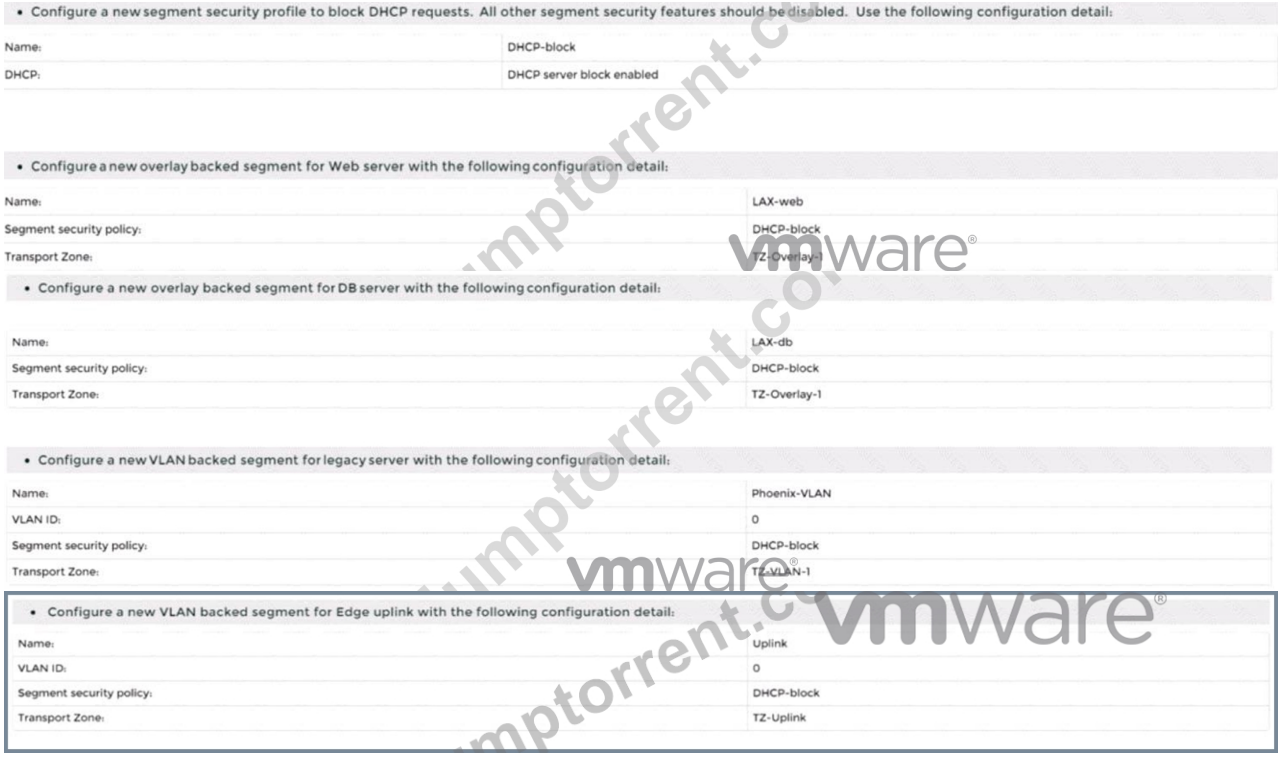
Complete the requested configuration.
Notes: Passwords are contained in the user_readme.txt. This task is not dependent on other tasks. This task should take approximately 10 minutes to complete.

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 # 17
Task 2
You are asked to deploy three Layer 2 overlay-backed segments to support a new 3-tier app and one Layer 2 VLAN-backed segment for support of a legacy application. The logical segments must block Server DHCP requests. Ensure three new overlay-

backed segments and one new VLAN-backed logical segment are deployed to the RegionA01-COPMOI compute cluster. All configuration should be done utilizing the NSX UI.
You need to:



- Configure a new segment security profile to block DHCP requests. All other segment security features should be disabled. Use the following configuration detail:

Name:	DHCP-block
DHCP:	DHCP server block enabled

- Configure a new overlay backed segment for Web server with the following configuration detail:

Name:	LAX-web
Segment security policy:	DHCP-block
Transport Zone:	TZ-Overlay-1

- Configure a new overlay backed segment for DB server with the following configuration detail:

Name:	LAX-db
Segment security policy:	DHCP-block
Transport Zone:	TZ-Overlay-1

- Configure a new VLAN backed segment for legacy server with the following configuration detail:

Name:	Phoenix-VLAN
VLAN ID:	0
Segment security policy:	DHCP-block
Transport Zone:	TZ-VLAN-1

- Configure a new VLAN backed segment for Edge uplink with the following configuration detail:

Name:	Uplink
VLAN ID:	0
Segment security policy:	DHCP-block
Transport Zone:	TZ-Uplink

Complete the requested task.
Notes: Passwords are contained in the user_readme.txt. Task 2 is dependent on the completion of Task 1.
Other tasks are dependent on completion of this task. You may want to move to the next tasks while waiting for configuration changes to be applied. 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 three layer 2 overlay-backed segments and one layer 2 VLAN-backed segment, 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 click Add Segment.
Enter a name for the segment, such as Web-01.
Select Tier-1 as the connectivity option and choose an existing tier-1 gateway from the drop-down menu or create a new one by clicking New Tier-1 Gateway.
Enter the gateway IP address of the subnet in a CIDR format, such as 192.168.10.1/24.
Select an overlay transport zone from the drop-down menu, such as Overlay-TZ.
Optionally, you can configure advanced settings such as DHCP, Metadata Proxy, MAC Discovery, or QoS for the segment by clicking Set Advanced Configs.
Click Save to create the segment.
Repeat steps 2 to 8 for the other two overlay-backed segments, such as App-01 and DB-01, with different subnet addresses, such as 192.168.20.1/24 and 192.168.30.1/24.
To create a VLAN-backed segment, click Add Segment again and enter a name for the segment, such as Legacy-01.
Select Tier-0 as the connectivity option and choose an existing tier-0 gateway from the drop-down menu or create a new one by clicking New Tier-0 Gateway.
Enter the gateway IP address of the subnet in a CIDR format, such as 10.10.10.1/24.
Select a VLAN transport zone from the drop-down menu, such as VLAN-TZ, and enter the VLAN ID for the segment, such as 100.
Optionally, you can configure advanced settings such as DHCP, Metadata Proxy, MAC Discovery, or QoS for the segment by clicking Set Advanced Configs.
Click Save to create the segment.
To apply a segment security profile to block DHCP requests on the segments, navigate to Networking > Segments > Segment Profiles and click Add Segment Profile.

Select Segment Security as the profile type and enter a name and an optional description for the profile.
Toggle the Server Block and Server Block - IPv6 buttons to enable DHCP filtering for both IPv4 and IPv6 traffic on the segments that use this profile.
Click Save to create the profile.
Navigate to Networking > Segments and select the segments that you want to apply the profile to.
Click Actions > Apply Profile and select the segment security profile that you created in step 18.
Click Apply to apply the profile to the selected segments.
You have successfully deployed three layer 2 overlay-backed segments and one layer 2 VLAN-backed segment with DHCP filtering using NSX-T Manager UI.

NEW QUESTION # 18
SIMULATION
Task 5
You are asked to configure a micro-segmentation policy for a new 3-tier web application that will be deployed to the production environment.
You need to:

- Configure Tags with the following configuration detail:

Tag Name	Member
Boston	Boston-web-01a, Boston-web-02a, Boston-app-01a, Boston-db-01a
Boston-Web	Boston-web-01a, Boston-web-02a
Boston-App	Boston-app-01a
Boston-DB	Boston-db-01a

- Configure Security Groups (use tags to define group criteria) with the following configuration detail:

Boston
Boston Web-Servers
Boston App-Servers
Boston DB-Servers

- Configure the Distributed Firewall Exclusion List with the following configuration detail:

Virtual Machine:	core-A

- Configure Policy & DFW Rules with the following configuration detail:

Policy Name:	Boston-Web-Application
Applied to:	Boston
New Services:	TCP-8443, TCP-3051

- Policy detail:

Rule Name	Source	Destination	Service	Action
Any-to-Web	Any	Boston Web-Servers	HTTP,HTTPS	ALLOW
Web-to-App	Boston Web-Servers	Boston App-Servers	TCP-8443	ALLOW
App-to-DB	Boston App-Servers	Boston DB-Servers	TCP-3051	ALLOW

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. The task steps are not dependent on one another. Subsequent tasks may require completion of this task. This task should take approximately 25 minutes to complete.

Answer:

Explanation:
See the Explanation part of the Complete Solution and step by step instructions Explanation:
Step-by-Step Guide
Creating Tags and Security Groups
First, log into the NSX-T Manager GUI and navigate to Inventory > Tags to create tags like "BOSTON-Web" for web servers and assign virtual machines such as BOSTON-web-01a and BOSTON-web-02 a. Repeat for "BOSTON-App" and "BOSTON-DB" with their respective VMs. Then, under Security > Groups, create security groups (e.g., "BOSTON Web-Servers") based on these tags to organize the network logically.
Excluding Virtual Machines
Next, go to Security > Distributed Firewall > Exclusion List and add the "core-A" virtual machine to exclude it from firewall rules, ensuring it operates without distributed firewall restrictions.
Defining Custom Services
Check Security > Services for existing services. If "TCP-9443" and "TCP-3051" are missing, create them by adding new services with the protocol TCP and respective port numbers to handle specific application traffic.

Setting Up the Policy and Rules
Create a new policy named "BOSTON-Web-Application" under Security > Distributed Firewall > Policies. Add rules within this policy:
Allow any source to "BOSTON Web-Servers" for HTTP/HTTPS.
Permit "BOSTON Web-Servers" to "BOSTON App-Servers" on TCP-9443.
Allow "BOSTON App-Servers" to "BOSTON DB-Servers" on TCP-3051. Finally, save and publish the policy to apply the changes.
This setup ensures secure, segmented traffic for the 3-tier web application, an unexpected detail being the need to manually create custom services for specific ports, enhancing flexibility.
Survey Note: Detailed Configuration of Micro-Segmentation Policy in VMware NSX-T Data Center 3.x This note provides a comprehensive guide for configuring a micro-segmentation policy for a 3-tier web application in VMware NSX-T Data Center 3.x, based on the task requirements. The process involves creating tags, security groups, excluding specific virtual machines, defining custom services, and setting up distributed firewall policies. The following sections detail each step, ensuring a thorough understanding for network administrators and security professionals.
Background and Context
Micro-segmentation in VMware NSX-T Data Center is a network security technique that logically divides the data center into distinct security segments, down to the individual workload level, using network virtualization technology. This is particularly crucial for a 3-tier web application, comprising web, application, and database layers, to control traffic and enhance security. The task specifies configuring this for a production environment, with notes indicating passwords are in user_readme.txt and no need to wait for configuration changes, as processing may take time.
Step-by-Step Configuration Process
Step 1: Creating Tags
Tags are used in NSX-T to categorize virtual machines, which can then be grouped for policy application. The process begins by logging into the NSX-T Manager GUI, accessible via a web browser with admin privileges. Navigate to Inventory > Tags, and click "Add Tag" to create the following:
Tag name: "BOSTON-Web", assigned to virtual machines BOSTON-web-01a and BOSTON-web-02a.
Tag name: "BOSTON-App", assigned to BOSTON-app-01a.
Tag name: "BOSTON-DB", assigned to BOSTON-db-01a.
This step ensures each tier of the application is tagged for easy identification and grouping, aligning with the attachment's configuration details.
Step 2: Creating Security Groups
Security groups in NSX-T are logical constructs that define membership based on criteria like tags, enabling targeted policy application. Under Security > Groups, click "Add Group" to create:
Group name: "BOSTON Web-Servers", with criteria set to include the "BOSTON-Web" tag.
Group name: "BOSTON App-Servers", with criteria set to include the "BOSTON-App" tag.
Group name: "BOSTON DB-Servers", with criteria set to include the "BOSTON-DB" tag.
This step organizes the network into manageable segments, facilitating the application of firewall rules to specific tiers.
Step 3: Excluding "core-A" VM from Distributed Firewall
The distributed firewall (DFW) in NSX-T monitors east-west traffic between virtual machines. However, certain VMs, like load balancers or firewalls, may need exclusion to operate without DFW restrictions. Navigate to Security > Distributed Firewall > Exclusion List, click "Add", select "Virtual Machine", and choose "core-A". Click "Save" to exclude it, ensuring it bypasses DFW rules, as per the task's requirement.
Step 4: Defining Custom Services
Firewall rules often require specific services, which may not be predefined. Under Security > Services, check for existing services "TCP-9443" and "TCP-3051". If absent, create them:
Click "Add Service", name it "TCP-9443", set protocol to TCP, and port to 9443.
Repeat for "TCP-3051", with protocol TCP and port 3051.
This step is crucial for handling application-specific traffic, such as the TCP ports mentioned in the policy type (TCP-9443, TCP-3051), ensuring the rules can reference these services.
Step 5: Creating the Policy and Rules
The final step involves creating a distributed firewall policy to enforce micro-segmentation. Navigate to Security > Distributed Firewall > Policies, click "Add Policy", and name it "BOSTON-Web-Application". Add a section, then create the following rules:
Rule Name: "Any-to-Web"
Source: Any (select "Any" or IP Address 0.0.0.0/0)
Destination: "BOSTON Web-Servers" (select the group)
Service: HTTP/HTTPS (predefined service)
Action: Allow
Rule Name: "Web-to-App"
Source: "BOSTON Web-Servers"
Destination: "BOSTON App-Servers"
Service: TCP-9443 (custom service created earlier)

Action: Allow
Rule Name: "App-to-DB"
Source: "BOSTON App-Servers"
Destination: "BOSTON DB-Servers"
Service: TCP-3051 (custom service created earlier)
Action: Allow
After defining the rules, click "Save" and "Publish" to apply the policy. This ensures traffic flows as required: any to web servers for HTTP/HTTPS, web to app on TCP-9443, and app to database on TCP-3051, while maintaining security through segmentation.
Additional Considerations
The task notes indicate no need to wait for configuration changes, as processing may take time, and steps are not dependent, suggesting immediate progression is acceptable. Passwords are in user_readme.txt, implying the user has necessary credentials. The policy order is critical, with rules processed top-to-bottom, and the attachment's "Type: TCP-9443, TCP-3051" likely describes the services used, not affecting the configuration steps directly.
Table: Summary of Configuration Details
Component
Details
Tags
BOSTON-Web (BOSTON-web-01a, BOSTON-web-02a), BOSTON-App (BOSTON-app-01a), BOSTON-DB (BOSTON-db-01a) Security Groups BOSTON Web-Servers (tag BOSTON-Web), BOSTON App-Servers (tag BOSTON-App), BOSTON DB-Servers (tag BOSTON-DB) DFW Exclusion List Virtual Machine: core-A Custom Services TCP-9443 (TCP, port 9443), TCP-3051 (TCP, port 3051) Policy Name BOSTON-Web-Application Firewall Rules Any-to-Web (Any to Web-Servers, HTTP/HTTPS, Allow), Web-to-App (Web to App-Servers, TCP-9443, Allow), App-to-DB (App to DB-Servers, TCP-3051, Allow) This table summarizes the configuration, aiding in verification and documentation.
Unexpected Detail
An unexpected aspect is the need to manually create custom services for TCP-9443 and TCP-3051, which may not be predefined, highlighting the flexibility of NSX-T for application-specific security policies.
Conclusion
This detailed process ensures a robust micro-segmentation policy, securing the 3-tier web application by controlling traffic between tiers and excluding specific VMs from DFW, aligning with best practices for network security in VMware NSX-T Data Center 3.x.

NEW QUESTION # 19
.....

- Valid 3V0-41.22 Exam Sims □ Valid 3V0-41.22 Study Notes □ Exam 3V0-41.22 Topic □ Search for " 3V0-41.22 " and easily obtain a free download on 【 www.pdfvce.com 】 □3V0-41.22 Latest Test Practice
- How Can You Pass the VMware 3V0-41.22 Exam Quickly and Easily? □ The page for free download of ➠ 3V0-41.22 □ on （ www.easy4engine.com ） will open immediately □Authentic 3V0-41.22 Exam Questions
- Authentic 3V0-41.22 Exam Questions □ 3V0-41.22 Test Questions □ Latest 3V0-41.22 Exam Camp □ Immediately open ▷ www.pdfvce.com ◁ and search for ✔ 3V0-41.22 □✔□ to obtain a free download □3V0-41.22 Valid Exam Tips
- Reliable VMware 3V0-41.22 Free Exam Questions - The Best www.pass4test.com - Leading Provider in Qualification Exams □ Search for ⇛ 3V0-41.22 ⇚ and download exam materials for free through { www.pass4test.com } □Valid 3V0-41.22 Study Notes
- pct.edu.pk, 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, www.stes.tyc.edu.tw, 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, teachladakh.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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, zenwriting.net, Disposable vapes

P.S. Free & New 3V0-41.22 dumps are available on Google Drive shared by DumpTorrent: https://drive.google.com/open?id=1dembny7hTZauqjPBtAwBYuOpXkxD_7vJ