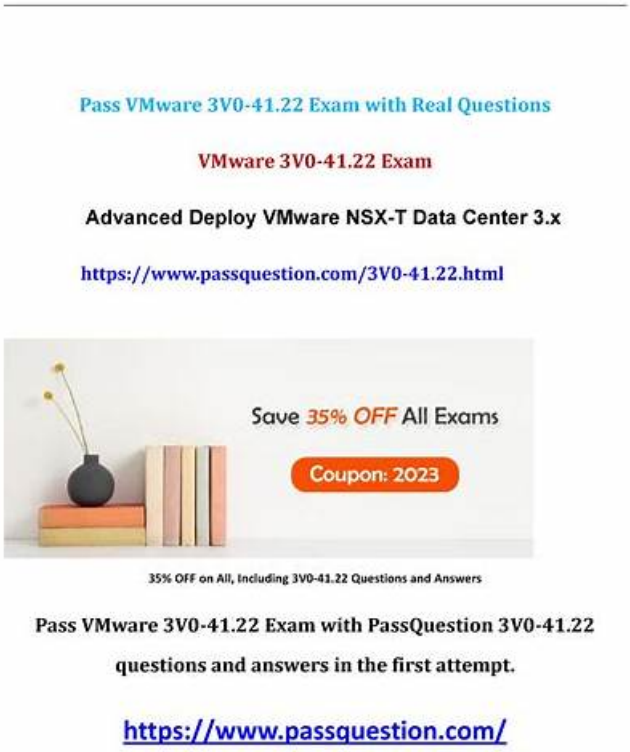
Exam 3V0-41.22 Practice & Latest 3V0-41.22 Test Questions



BTW, DOWNLOAD part of TestPassed 3V0-41.22 dumps from Cloud Storage: https://drive.google.com/open?id=1F46WuQw1BByQVVYNNX7uwbMtUYY0xKhe

The modern VMware world is changing its dynamics at a fast pace. To stay and compete in this challenging market, you have to learn and enhance your in-demand skills. Fortunately, with the Advanced Deploy VMware NSX-T Data Center 3.X (3V0-41.22) certification exam you can do this job nicely and quickly. To do this you just need to enroll in the 3V0-41.22 certification exam and put all your efforts to pass the Advanced Deploy VMware NSX-T Data Center 3.X (3V0-41.22) certification exam. After successful competition of the VMware 3V0-41.22 certification, the certified candidates can put their career on the right track and achieve their professional career objectives in a short time period.

Earning the VMware 3V0-41.22 certification demonstrates that an IT professional has the skills and knowledge required to deploy and manage VMware NSX-T Data Center 3.x in an enterprise environment. Advanced Deploy VMware NSX-T Data Center 3.X certification is recognized by many organizations and can help individuals advance their careers in network virtualization.

VMware 3V0-41.22 exam is designed for experienced NSX-T Data Center professionals who want to validate their advanced skills in deploying and managing NSX-T Data Center. 3V0-41.22 Exam is also suitable for architects, consultants, and engineers who want to demonstrate their expertise in designing and implementing complex NSX-T Data Center solutions. Upon passing the exam, the candidate earns the VMware Certified Advanced Professional - Network Virtualization 2021 (VCAP-NV 2021) certification, which is a valuable credential for NSX-T Data Center professionals.

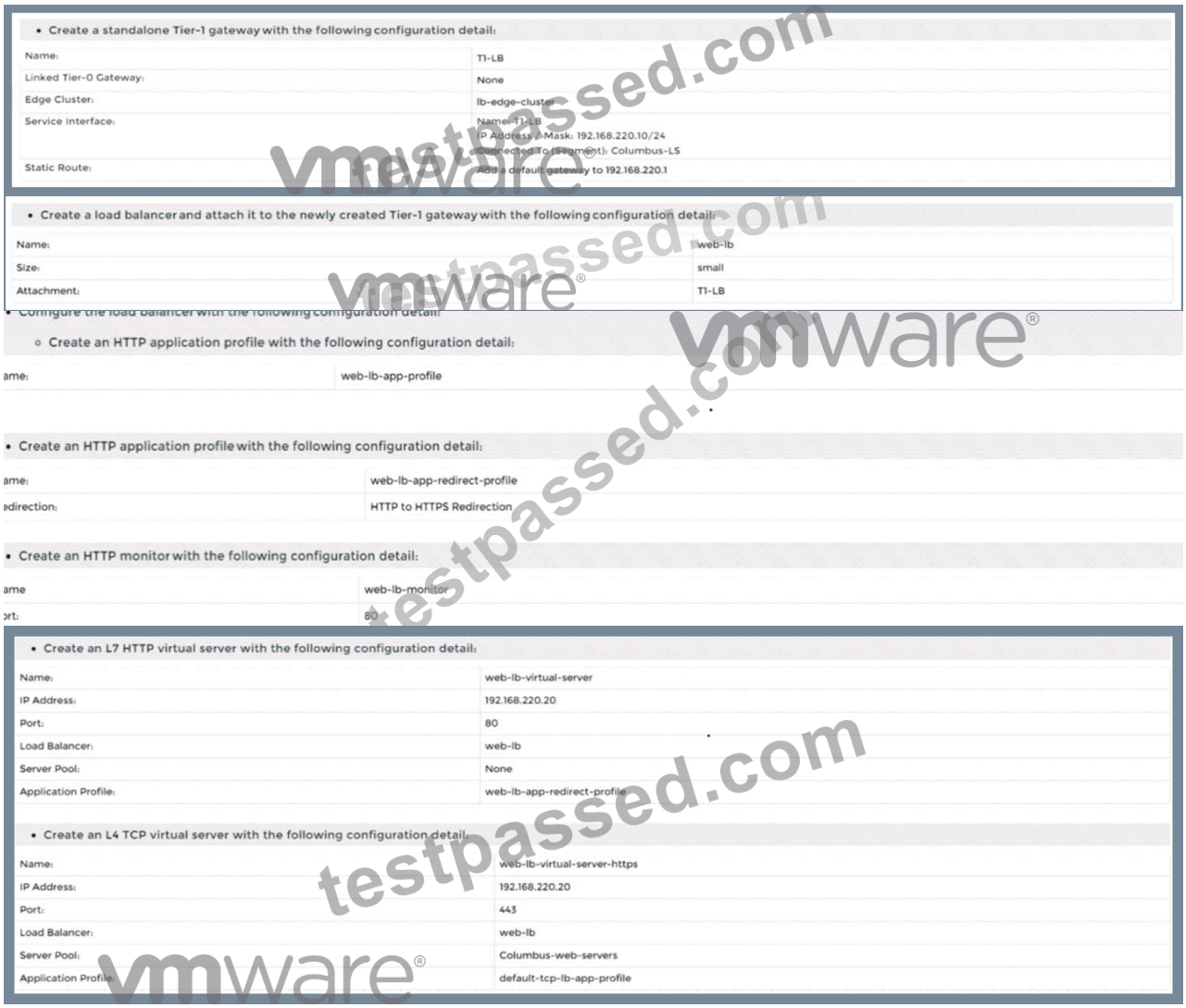
>> Exam 3V0-41.22 Practice <<

Trusted Exam 3V0-41.22 Practice & Useful VMware Certification Training - Trustworthy VMware Advanced Deploy VMware NSX-T Data Center 3.X

Our Advanced Deploy VMware NSX-T Data Center 3.X study question has high quality. So there is all effective and central practice for you to prepare for your test. With our professional ability, we can accord to the necessary testing points to edit 3V0-41.22 exam questions. It points to the exam heart to solve your difficulty. So high quality materials can help you to pass your exam effectively, make you feel easy, to achieve your goal. With the 3V0-41.22 Test Guide use feedback, it has 98%-100% pass rate. That's the truth from our customers. And it is easy to use for you only with 20 hours' to 30 hours' practice. After using the 3V0-41.22 test guide, you will have the almost 100% assurance to take part in an examination. With high quality materials and practices, you will get easier to pass the exam.

VMware Advanced Deploy VMware NSX-T Data Center 3.X Sample Questions (Q10-Q15):

NEW QUESTION # 10
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 # 11
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:	VMware1!

* 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 corpdcserver.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 VMware1!.
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 # 12
SIMULATION
Task 16
You are working to automate your NSX-T deployment and an automation engineer would like to retrieve your BOP routing information from the API.
You need to:
* Run the GET call in the API using Postman
* Save output to the desktop to a text file called API.txt
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 5 minutes to complete.

Answer:

Explanation:
See the Explanation part of the Complete Solution and step by step instructions Explanation:
To run the GET call in the API using Postman and save the output to the desktop to a text file called API.txt, you need to follow these steps:
Open Postman and create a new request tab. Select GET as the method from the drop-down menu.
Enter the URL of the NSX-T Policy API endpoint for retrieving the BGP routing table, such as https://<nsx-manager-ip-address>/policy/api/v1/infra/tier-0s/vmc/routing-table?enforcement_point_path=/infra/sites/default/enforcement-points/vmc-enforcementpoint Click the Authorization tab and select Basic Auth as the type from the drop-down menu. Enter your NSX-T username and password in the Username and Password fields, such as admin and VMware1!.
Click Send to execute the request and view the response in the Body tab. You should see a JSON object with the BGP routing table information, such as routes, next hops, prefixes, etc.
Click Save Response and select Save to a file from the drop-down menu. Enter API.txt as the file name and choose Desktop as the location. Click Save to save the output to your desktop.
You have successfully run the GET call in the API using Postman and saved the output to your desktop to a text file called API.txt.

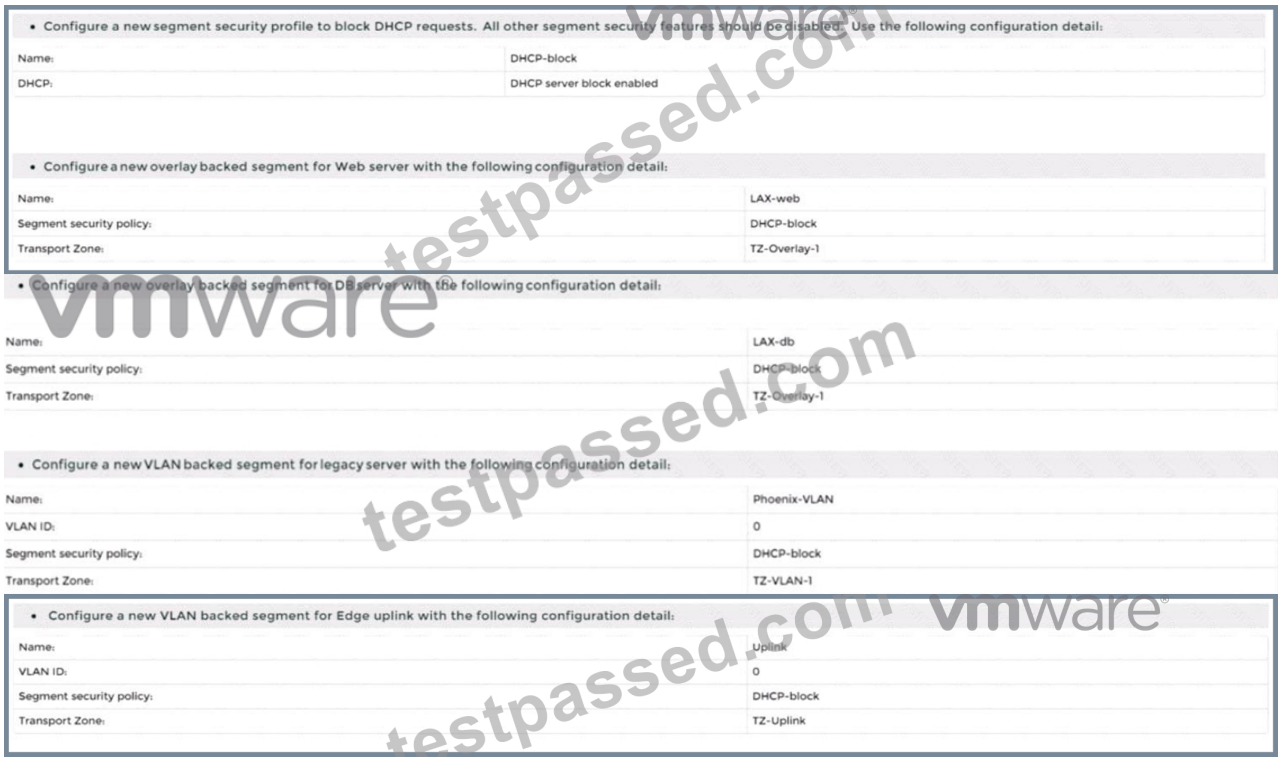
NEW QUESTION # 13
Task 15
You have been asked to enable logging so that the global operations team can view inv Realize Log Insight that their Service Level Agreements are being met for all network traffic that is going in and out of the NSX environment. This NSX environment is an Active / Active two Data Center design utilizing N-VDSwith BCP.
You need to ensure successful logging for the production NSX-T environment.
You need to:
Verify via putty with SSH that the administrator can connect to all NSX-Transport Nodes. You will use the credentials identified in Putty (admin).
Verify that there is no current active logging enabled by reviewing that directory is empty -/var/log/syslog-
Enable NSX Manager Cluster logging
Select multiple configuration choices that could be appropriate success criteria Enable NSX Edge Node logging Validate logs are generated on each selected appliance by reviewing the "/var/log/syslog" Complete the requested task.
Notes: Passwords are contained in the user _ readme.txt. complete.
These task steps are dependent on one another. 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 enable logging for the production NSX-T environment, you need to follow these steps:
Verify via putty with SSH that the administrator can connect to all NSX-Transport Nodes. You can use the credentials identified in Putty (admin) to log in to each transport node. For example, you can use the following command to connect to the sfo01w01en01 edge transport node:ssh admin@sfo01w01en01.
You should see a welcome message and a prompt to enter commands.
Verify that there is no current active logging enabled by reviewing that directory is empty
-/var/log/syslog-. You can use thelscommand to list the files in the /var/log/syslog directory. For example, you can use the following command to check the sfo01w01en01 edge transport node:ls
/var/log/syslog. You should see an empty output if there is no active logging enabled.
Enable NSX Manager Cluster logging. You can use thesearch_web("NSX Manager Cluster logging configuration")tool to find some information on how to configure remote logging for NSX Manager Cluster. One of the results isNSX-T Syslog Configuration Revisited - vDives, which provides the following steps:
Navigate to System > Fabric > Profiles > Node Profiles then select All NSX Nodes then under Syslog Servers click +ADD Enter the IP or FQDN of the syslog server, the Port and Protocol and the desired Log Level then click ADD Select multiple configuration choices that could be appropriate success criteria. You can use thesearch_web("NSX-T logging success criteria")tool to find some information on how to verify and troubleshoot logging for NSX-T. Some of the possible success criteria are:
The syslog server receives log messages from all NSX nodes
The log messages contain relevant information such as timestamp, hostname, facility, severity, message ID, and message content The log messages are formatted and filtered according to the configured settings The log messages are encrypted and authenticated if using secure protocols such as TLS or LI-TLS Enable NSX Edge Node logging. You can use thesearch_web("NSX Edge Node logging configuration")tool to find some information on how to configure remote logging for NSX Edge Node.
One of the results isConfigure Remote Logging - VMware Docs, which provides the following steps:
Run the following command to configure a log server and the types of messages to send to the log server. Multiple facilities or message IDs can be specified as a comma delimited list, without spaces.
set logging-server <hostname-or-ip-address [:port]> proto <proto> level <level> [facility <facility>]
[messageid <messageid>] [serverca <filename>] [clientca <filename>] [certificate <filename>] [key
<filename>] [structured-data <structured-data>]
Validate logs are generated on each selected appliance by reviewing the "/var/log/syslog". You can use thecatortailcommands to view the contents of the /var/log/syslog file on each appliance. For example, you can use the following command to view the last 10 lines of the sfo01w01en01 edge transport node:tail -n 10 /var/log/syslog. You should see log messages similar to this:
2023-04-06T12:34:56+00:00 sfo01w01en01 user.info nsx-edge[1234]: 2023-04-06T12:34:56Z nsx-edge[1234]: INFO: [nsx@6876 comp="nsx-edge" subcomp="nsx-edge" level="INFO" security="False"] Message from nsx-edge You have successfully enabled logging for the production NSX-T environment.

NEW QUESTION # 14
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:



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 # 15
.....