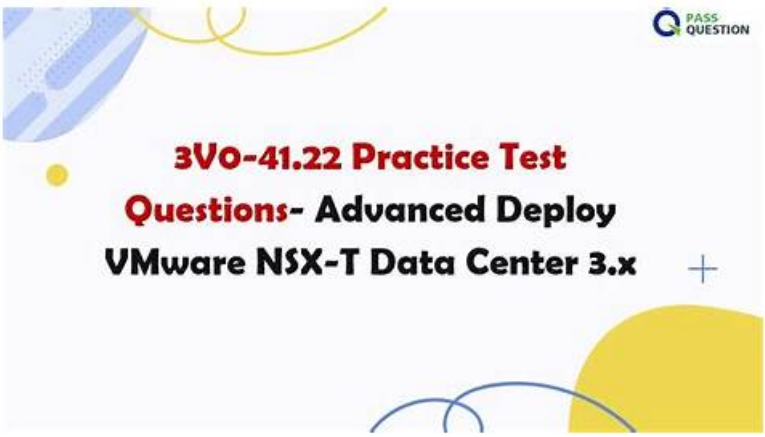
Exam 3V0-41.22 VCE



BTW, DOWNLOAD part of PassLeaderVCE 3V0-41.22 dumps from Cloud Storage: https://drive.google.com/open?id=1TFihNytruiP38R5owjrrVO_tL-0jXIsj

If you are still unsure whether to pursue VMware 3V0-41.22 exam questions for VMware Advanced Deploy VMware NSX-T Data Center 3.X exam preparation, you are losing the game at the first stage in a fiercely competitive marketplace. VMware 3V0-41.22 Questions are the best option for becoming VMware Advanced Deploy VMware NSX-T Data Center 3.X.

Earning the VMware 3V0-41.22 Certification can be a valuable asset for professionals who work in industries such as cloud computing, virtualization, networking, and security. Advanced Deploy VMware NSX-T Data Center 3.X certification demonstrates a high level of expertise in deploying and managing NSX-T Data Center environments, which can help professionals advance their careers and increase their earning potential.

VMware 3V0-41.22 certification is a valuable asset for IT professionals who want to advance their careers in network virtualization and cloud computing. It demonstrates the candidate's proficiency in deploying and managing advanced NSX-T features, which are essential for modern data centers. Advanced Deploy VMware NSX-T Data Center 3.X certification also enhances the candidate's credibility and marketability, making them more attractive to potential employers.

>> Valid 3V0-41.22 Exam Labs <<

Reliable 3V0-41.22 Braindumps Ebook, Valid Test 3V0-41.22 Test

Our team of experts updates actual VMware 3V0-41.22 questions regularly so you can prepare for the 3V0-41.22 exam according to the latest syllabus. Additionally, we also offer up to 1 year of free 3V0-41.22 exam questions updates. We have a 24/7 customer service team available for your assistance if you get stuck somewhere. Buy 3V0-41.22 Latest Questions of PassLeaderVCE now and get ready to crack the 3V0-41.22 certification exam in a single attempt.

VMware certifications are recognized worldwide and are highly valued by employers. Holding a VMware certification demonstrates that you have the expertise and skills needed to design, deploy, and manage VMware technologies in a real-world environment. The VMware 3V0-41.22 Certification is an excellent way for IT professionals to validate their knowledge and skills in deploying VMware NSX-T Data Center 3.X and to advance their careers in the field of network virtualization and security.

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

NEW QUESTION # 15
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 # 16
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 # 17
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:	5
Ingress traffic rate limits:	100 Mbps for average, 200 Mbps for peak

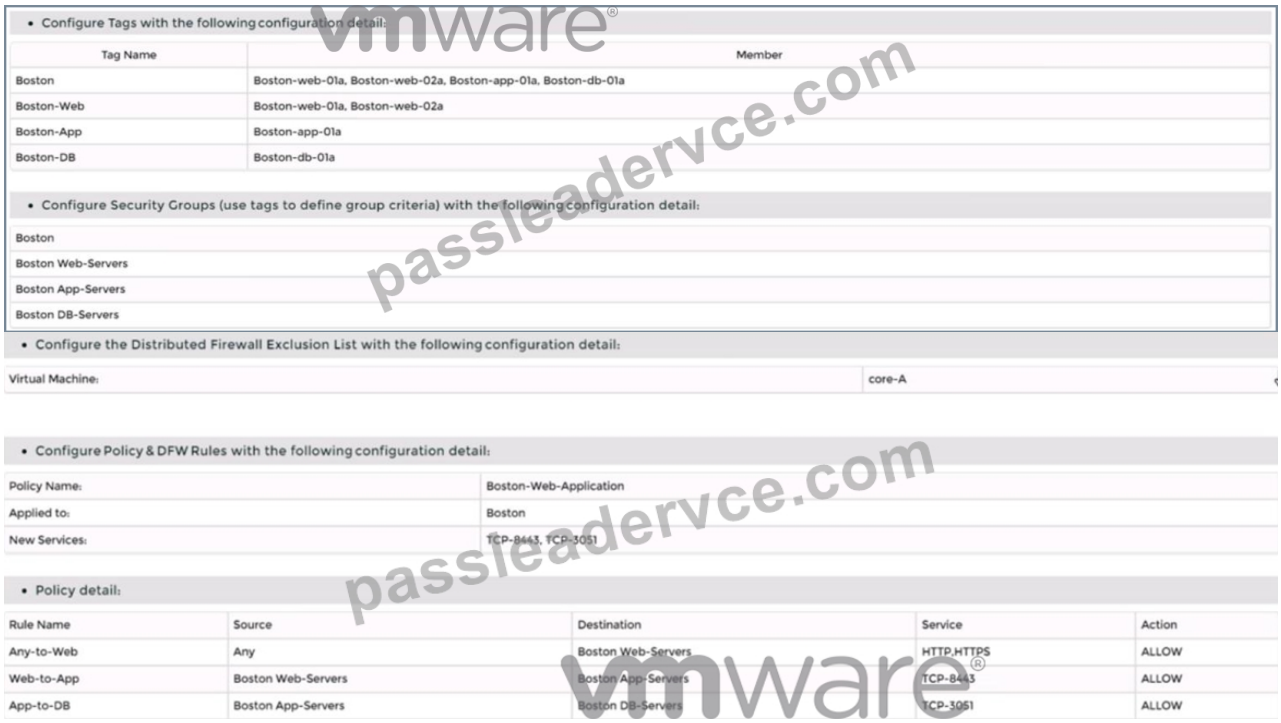
* Apply the profile on the 'phoenix-VLAN' segment
Complete the requested task.
Notes: Passwords are contained in the user_readme.txt.
take approximately 5 minutes to complete.
Subsequent tasks may require the completion of this task.
This task should See the Explanation part of the Complete Solution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

Answer:

Explanation:
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 # 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-9443, 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
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 IS 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 # 20

......

Reliable 3V0-41.22 Braindumps Ebook: https://www.passleadervce.com/VCAP-NV-Deploy-2023/reliable-3V0-41.22-exam-learning-guide.html