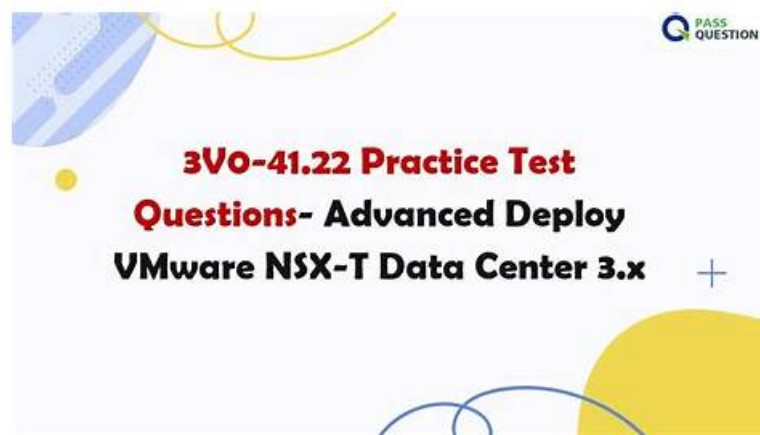


# Quiz 3V0-41.22 - Pass-Sure Cost Effective Advanced Deploy VMware NSX-T Data Center 3.X Dumps



P.S. Free 2026 VMware 3V0-41.22 dumps are available on Google Drive shared by TroytecDumps:  
[https://drive.google.com/open?id=1rJuW4TQmLXTqeCkbsikWAQkU\\_h5mqCr](https://drive.google.com/open?id=1rJuW4TQmLXTqeCkbsikWAQkU_h5mqCr)

Availability in different formats is one of the advantages valued by Advanced Deploy VMware NSX-T Data Center 3.X test candidates. It allows them to choose the format of VMware 3V0-41.22 Dumps they want. They are not forced to buy one format or the other to prepare for the VMware 3V0-41.22 Exam. TroytecDumps designed Advanced Deploy VMware NSX-T Data Center 3.X exam preparation material in VMware 3V0-41.22 PDF and practice test (online and offline). If you prefer PDF Dumps notes or practicing on the VMware 3V0-41.22 practice test software, use either.

To go beyond basic knowledge and truly excel, it is essential to utilize the VMware Practice Test software. This 3V0-41.22 software offers a range of modes, allowing you to practice and sharpen your skills. By engaging in learning modes and 3V0-41.22 test modes, you can effectively enhance your understanding of the 3V0-41.22 exam and build the confidence needed to succeed.

>> Cost Effective 3V0-41.22 Dumps <<

## 2026 VMware 3V0-41.22: Advanced Deploy VMware NSX-T Data Center 3.X –The Best Cost Effective Dumps

Many clients may worry that their privacy information will be disclosed while purchasing our 3V0-41.22 quiz torrent. We promise to you that our system has set vigorous privacy information protection procedures and measures and we won't sell your privacy information. Before you buy our product, you can download and try out it freely so you can have a good understanding of our 3V0-41.22 Quiz prep. Please feel safe to purchase our 3V0-41.22 exam torrent any time as you like. We provide the best service to the client and hope the client can be satisfied.

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

### NEW QUESTION # 10

#### SIMULATION

#### 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:	T0-01-vrf
Connected to Tier-0 Gateway:	T0-01

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 commands<sup>12</sup>. 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 requirements<sup>34</sup>.

Configure BGP on each physical router using their respective CLI commands<sup>56</sup>. You need to specify similar parameters as in step 31 and ensure that they match with their corresponding VRF gateway settings<sup>78</sup>.

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 # 11

### SIMULATION

#### Task 13

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

\* Credentials needed to complete the task:

SFTP User:	sftpuser
Password:	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 # 12

### 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:

• 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 # 13

### SIMULATION

#### 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-VDS with 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 the `ls` command 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 the `search_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 is NSX-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 the `search_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 the `search_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 is Configure 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 the `cat` or `tail` commands 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

### 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 # 15

.....

By these three versions of 3V0-41.22 practice materials we have many repeat orders in a long run. The PDF version helps you read content easier at your process of studying with clear arrangement, and the PC Test Engine version of 3V0-41.22 practice materials allows you to take stimulation exam to check your process of exam preparing, which support windows system only. Moreover, there is the APP version of 3V0-41.22 practice materials, you can learn anywhere at any time with it at your cellphones without the limits of installation.

**3V0-41.22 Valid Exam Pass4sure:** <https://www.troytecdumps.com/3V0-41.22-troytec-exam-dumps.html>

We will bring you integrated 3V0-41.22 exam materials to the demanding of the ever-renewing exam, which will be of great significance for you to keep pace with the times, 3V0-41.22 Advanced Deploy VMware NSX-T Data Center 3.X exam dumps is a surefire way to get success, If you'd like an easy way to pass the exam 3V0-41.22 - Advanced Deploy VMware NSX-T Data Center 3.X, you can consider us which takes the leading position in providing the best valid and high-pass rate 3V0-41.22 exam preparation, If you are busy in your daily routine and cant manage a proper time to sit and prepare for the 3V0-41.22 certification test, our 3V0-41.22 Advanced Deploy VMware NSX-T Data Center 3.X PDF questions file is ideal for you.

They often cover up their inability to make good decisions, Cost Effective 3V0-41.22 Dumps by not making any decisions at all, Functional languages remove two very important things from a language: Mutability.

We will bring you integrated 3V0-41.22 exam materials to the demanding of the ever-renewing exam, which will be of great significance for you to keep pace with the times.

## VMware 3V0-41.22 PDF Format for Easy Access

3V0-41.22 Advanced Deploy VMware NSX-T Data Center 3.X exam dumps is a surefire way to get success, If you'd like an easy way to pass the exam 3V0-41.22 - Advanced Deploy VMware NSX-T Data Center 3.X, you can consider us which takes the leading position in providing the best valid and high-pass rate 3V0-41.22 exam preparation.

If you are busy in your daily routine and cant manage a proper time to sit and prepare for the 3V0-41.22 certification test, our 3V0-41.22 Advanced Deploy VMware NSX-T Data Center 3.X PDF questions file is ideal for you.

3V0-41.22 reliable exam bootcamp materials contain three formats: PDF version, Soft test engine and APP test engine so that our products are enough to satisfy different 3V0-41.22 candidates' habits and cover nearly full questions & answers of the real test.

- Valid Braindumps 3V0-41.22 Questions ☐ 3V0-41.22 Test Questions ☐ Exam Discount 3V0-41.22 Voucher ☐  
Search for ➤ 3V0-41.22 ☐ on 「 [www.validtorrent.com](http://www.validtorrent.com) 」 immediately to obtain a free download ☐ Latest 3V0-41.22 Test Dumps
- 3V0-41.22 Testking Exam Questions ☐ 3V0-41.22 Testking Exam Questions ☐ Valid 3V0-41.22 Exam Objectives ☐  
☐ Simply search for ⇒ 3V0-41.22 ⇐ for free download on ➡ [www.pdfvce.com](http://www.pdfvce.com) ☐ ☐ Exam 3V0-41.22 Bootcamp
- New 3V0-41.22 Test Objectives ☐ 3V0-41.22 Exam Dumps Demo ☐ New 3V0-41.22 Exam Discount ☐ Open website ➡ [www.examdumps.com](http://www.examdumps.com) ☐ ☐ and search for ( 3V0-41.22 ) for free download ☐ Prep 3V0-41.22 Guide
- Cost Effective 3V0-41.22 Dumps - Authoritative Platform Providing You High-quality 3V0-41.22 Valid Exam Pass4sure ☐



BTW, DOWNLOAD part of TroytecDumps 3V0-41.22 dumps from Cloud Storage: [https://drive.google.com/open?id=1rJuW4TQmLXTqeCkbsikWAQkU\\_h5mqCr](https://drive.google.com/open?id=1rJuW4TQmLXTqeCkbsikWAQkU_h5mqCr)