VMware

3V0-41.22

Advanced Deploy VMware NSX-T Data Center 3.X

QUESTION & ANSWERS

QUESTION: 1

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/syslogEnable 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 :

See the Explanation part of the Complete Solution and step by step instructions.

Explanation/Reference:

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 proto level [facility]

[messageid] [serverca] [clientca] [certificate] [key

] [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.

QUESTION: 2

Task 14

An administrator has seen an abundance of alarms regarding high CPU usage on the NSX Managers. The

administrator has successfully cleared these alarms numerous times in the past and is aware of the issue. The

administrator feels that the number of alarms being produced for these events is overwhelming the log files.

You need to:

• Review CPU Sensitivity and Threshold values.

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 5 minutes to complete.

Answer :

See the Explanation part of the Complete Solution and step by step instructions.

Explanation/Reference:

To review CPU sensitivity and threshold values, you need to follow these steps:

Log in to the NSX Manager UI with admin credentials. The default URL is

https://.

Navigate to System > Settings > System Settings > CPU and Memory Thresholds.

You will see the current values for CPU and memory thresholds for NSX Manager, NSX Controller, and

NSX Edge. These values determine the percentage of CPU and memory usage that will trigger an alarm

on the NSX Manager UI.

You can modify the default threshold values by clicking Edit and entering new values in the text boxes.

For example, you can increase the CPU threshold for NSX Manager from 80% to 90% to reduce the

number of alarms for high CPU usage. Click Save to apply the changes.

You can also view the historical data for CPU and memory usage for each component by clicking View

Usage History. You can select a time range and a granularity level to see the usage trends and patterns

over time

QUESTION: 3

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:	VMware1!
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:	VMware1!

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 :

See the Explanation part of the Complete Solution and step by step instructions.

Explanation/Reference:

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 thesearch_web("SFTP server availability")tool to find some information on how to set up and check an SFTP server. You can also use thessh-keyscancommand to get the fingerprint of the SFTP server. For example,ssh-keyscan -t ecdsa sftp_serverwill 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://. 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.

QUESTION: 4

Task 11

upon testing the newly configured distributed firewall policy for the Boston application. it has been discovered

that the Boston-Web virtual machines can be “pinged" via ICMP from the main console. Corporate policy does not allow pings to the Boston VMs.

You need to:

• Troubleshoot ICMP traffic and make any necessary changes to the Boston application security policy.

Complete the requested task.

Notes: Passwords are contained in the user _readme.txt. This task is dependent on Task 5.