# IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

**Exam** : **3V0-41.22**

**Title** : Advanced Deploy VMware NSX-T Data Center 3.x

**Version** : DEMO

1.Task 1

You are asked to prepare a VMware NSX-T Data Center ESXi compute cluster Infrastructure. You will prepare two ESXi servers in a cluster for NSX-T overlay and VLAN use.

All configuration should be done using the NSX UI.

• NOTE: The configuration details in this task may not be presented to you in the order in which you must complete them.

• Configure a new Transport Node profile and add one n-VDS switch. Ensure Uplink1and Uplink 2 of your configuration use vmnic2 and vmnic3 on the host.

Configuration detail:

| | |
|---|---|
| Name: | RegionA01-COMP01-TNP |
| Type: | n-VDS switch |
| Mode: | standard |
| n-VDS Switch Name: | N-VDS-1 |
| Transport Zones: | TZ-Overlay-1 and TZ-VLAN-1 |
| NIOC profile: | nsx-default-nioc-hostswitch-profile |
| Uplink Profile: | RegionA01-COMP01-UP |
| LLDP Profile: | LLDP [send packet disabled] |
| IP Assignment: | TEP-Pool-02 |

Hint: The Transport Zone configuration will be used by another administrator at a later time.

- Configure a new VLAN backed transport zone.

Configuration detail:

- Configure a new uplink profile for the ESXi servers.

Configuration detail:

| | |
|---|---|
| Name: | RegionA01-COMP01-UP |
| Teaming Policy: | Load Balance source |
| Active adapters: | Uplink1 and Uplink2 |
| Transport VLAN: | 0 |

- Configure a new IP Pool for ESXi overlay traffic with

Configuration detail:

| | |
|---|---|
| Name: | TEP-Pool-02 |
| IP addresses range: | 192.168.130.71 - 192.168.130.74 |
| CIDR: | 192.168.130.0/24 |
| Gateway: | 192.168.130.1 |

- Using the new transport node profile, prepare ESXi cluster RegionA01-COMP01 for NSX Overlay and VLAN use.

Complete the requested task.

NOTE: Passwords are contained in the user_readme.txt. Configuration details may not be provided in the correct sequential order. Steps to complete this task must be completed in the proper order. Other tasks are dependent on the completion Of this task. You may want to move to other tasks/steps while waiting for configuration changes to be applied. This task should take approximately 20 minutes to complete.

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

**Answer:**

To prepare a VMware NSX-T Data Center ESXi compute cluster infrastructure, 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 > Profiles > Transport Node Profiles and click Add Profile.
- Enter a name and an optional description for the transport node profile.
- In the Host Switches section, click Set and select N-VDS as the host switch type.
- Enter a name for the N-VDS switch and select the mode as Standard or Enhanced Datapath, depending on your requirements.
- Select the transport zones that you want to associate with the N-VDS switch. You can select one overlay transport zone and one or more VLAN transport zones.
- Select an uplink profile from the drop-down menu or create a custom one by clicking New Uplink Profile.
- In the IP Assignment section, select Use IP Pool and choose an existing IP pool from the drop-down menu or create a new one by clicking New IP Pool.
- In the Physical NICs section, map the uplinks to the physical NICs on the host. For example, map Uplink 1 to vmnic2 and Uplink 2 to vmnic3.
- Click Apply and then click Save to create the transport node profile.
- Navigate to System > Fabric > Nodes > Host Transport Nodes and click Add Host Transport Node.
- Select vCenter Server as the compute manager and select the cluster that contains the two ESXi servers that you want to prepare for NSX-T overlay and VLAN use.
- Select the transport node profile that you created in the previous steps and click Next.
- Review the configuration summary and click Finish to start the preparation process.

The preparation process may take some time to complete. You can monitor the progress and status of the host transport nodes on the Host Transport Nodes page. Once the preparation is complete, you will see two host transport nodes with a green status icon and a Connected state. You have successfully prepared a VMware NSX-T Data Center ESXi compute cluster infrastructure using a transport node profile.

2.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.
See the Explanation part of the Complete Solution and step by step instructions.
**Answer:**
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.

3.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 |

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

4.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.
See the Explanation part of the Complete Solution and step by step instructions.
**Answer:**
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 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.

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

**Answer:**

To troubleshoot ICMP traffic and make any necessary changes to the Boston application security policy, 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 Security > Distributed Firewall and select the firewall policy that applies to the Boston application. For example, select Boston-web-Application.
- Click Show IPSec Statistics and view the details of the firewall rule hits and logs. You can see which rules are matching the ICMP traffic and which actions are taken by the firewall.
- If you find that the ICMP traffic is allowed by a rule that is not intended for it, you can edit the rule and change the action to Drop or Reject. You can also modify the source, destination, or service criteria of the rule to make it more specific or exclude the ICMP traffic.
- If you find that the ICMP traffic is not matched by any rule, you can create a new rule and specify the action as Drop or Reject. You can also specify the source, destination, or service criteria of the rule to match only the ICMP traffic from the main console to the Boston web VMs.
- After making the changes, click Publish to apply the firewall policy.
- Verify that the ICMP traffic is blocked by pinging the Boston web VMs from the main console again.You should see a message saying “Request timed out” or “Destination unreachable”.