

VMware NSX-T Data Center: Troubleshooting and Operations

Lab Manual

NSX-T Data Center 3.0



VMware® Education Services
VMware, Inc.
www.vmware.com/education

VMware NSX-T Data Center: Troubleshooting and Operations [V3.0]

Lab Manual - Prerelease

NSX-T Data Center 3.0

Part Number EDU-EN-NSXTTO3-LAB (06/2020)

Copyright © 2020 VMware, Inc. All rights reserved. This manual and its accompanying materials are protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. VMware ESXi™, VMware Go™, VMware Horizon, VMware Horizon® View™, VMware NSX®, VMware NSX® Edge™, VMware NSX® for vSphere®, VMware NSX® Manager™, VMware NSX-T™ Data Center, VMware Pivotal Labs® Navigator™, VMware vCenter Server®, VMware vCenter® Log Insight™, VMware Verify™, VMware View®, VMware vRealize®, VMware vRealize® Log Insight™, VMware vRealize® Log Insight™ for vCenter™, VMware vSphere®, VMware vSphere® Client™, VMware vSphere® Distributed Switch™, VMware vSphere® vMotion®, and VMware vSphere® Web Client are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

The training material is provided “as is,” and all express or implied conditions, representations, and warranties, including any implied warranty of merchantability, fitness for a particular purpose or noninfringement, are disclaimed, even if VMware, Inc., has been advised of the possibility of such claims. This training material is designed to support an instructor-led training course and is intended to be used for reference purposes in conjunction with the instructor-led training course.

The training material is not a standalone training tool. Use of the training material for self-study without class attendance is not recommended. These materials and the computer programs to which it relates are the property of, and embody trade secrets and confidential information proprietary to, VMware, Inc., and may not be reproduced, copied, disclosed, transferred, adapted or modified without the express written approval of VMware, Inc.

Typographical Conventions

The following typographical conventions are used in this course.

Conventions	Usage and Examples
Monospace	Identifies command names, command options, parameters, code fragments, error messages, filenames, folder names, directory names, and path names: <ul style="list-style-type: none">• Run the <code>esxtop</code> command.• ... found in the <code>/var/log/messages</code> file.
Monospace Bold	Identifies user inputs: <ul style="list-style-type: none">• Enter <code>ipconfig /release</code>.
Boldface	Identifies user interface controls: <ul style="list-style-type: none">• Click the Configuration tab.
<i>Italic</i>	Identifies book titles: <ul style="list-style-type: none">• <i>vSphere Virtual Machine Administration</i>
< >	Indicates placeholder variables: <ul style="list-style-type: none">• <ESXi_host_name>• ... the Settings/<Your_Name>.txt file

Contents

Lab 1 Reviewing the Lab Structure and Environments	1
Task 1: Review the Lab Environment Configuration.....	1
Task 2: Review the Production Environment Overview	3
Task 3: Review the Staging Environment Overview	5
Task 4: Review the Development and QA Environment Overview	7
Task 5: Review the Lab Types	8
Task 6: Review Best Practices to Access the Lab Environment.....	9
Lab 2 NSX-T Data Center Operations and Troubleshooting Tools	10
Task 1: Prepare for the Lab	10
Task 2: Configure Syslog in NSX Manager and Review the Collected Logs.....	11
Task 3: Configure Syslog in an NSX Edge Node and Review Collected Logs	12
Task 4: Generate a Technical Support Bundle for NSX Manager	13
Task 5: Configure a Traceflow Session.....	14
Task 6: Examine the Traceflow Output	15
Lab 3 NSX Management Cluster Verification	17
Task 1: Prepare for the Lab	18
Task 2: Verify the NSX Management Cluster Status from the UI	19
Task 3: Verify the NSX Management Cluster Status from the NSX CLI	20
Lab 4 NSX Management Cluster Break-Fix Scenario.....	22
Task 1: Read the Scenario Description.....	22
Task 2: Confirm the Problem	23
Task 3: Troubleshoot and Fix the Problem	25
Task 4: Verify That the Problem Is Fixed	27

Lab 5 Infrastructure Preparation Verification.....	28
Task 1: Prepare for the Lab	29
Task 2: Verify the Transport Node Preparation Prerequisites	29
Task 3: Verify the Transport Node Preparation from the NSX UI.....	32
Task 4: Verify the Transport Node Preparation from the ESXi CLI.....	34
Task 5: Verify the Transport Node Preparation from the KVM CLI	36
Task 6: Verify the NSX Edge Configuration from the NSX CLI	37
Lab 6 NSX Infrastructure Preparation Break-Fix Scenario 1	39
Task 1: Read the Scenario Description.....	39
Task 2: Confirm the Problem	40
Task 3: Troubleshoot and Fix the Problem	41
Task 4: Verify That the Problem Is Fixed	41
Lab 7 NSX Infrastructure Preparation Break-Fix Scenario 2	42
Task 1: Read the Scenario Description.....	42
Task 2: Confirm the Problem	43
Task 3: Troubleshoot and Fix the Problem	44
Task 4: Verify That the Problem Is Fixed	44
Lab 8 NSX Infrastructure Preparation Challenge Scenario	45
Task 1: Read the Scenario Description.....	45
Task 2: Confirm the Problem	46
Task 3: Troubleshoot and Fix the Problem	47
Task 4: Verify That the Problem Is Fixed	47
Lab 9 Logical Switching Verification.....	48
Task 1: Prepare for the Lab	49
Task 2: Verify Segments from the NSX UI	50
Task 3: Verify Logical Switches from the NSX CLI.....	50
Task 4: Verify Logical Switches from the ESXi CLI	54
Task 5: Verify Logical Switches from the KVM CLI	56
Lab 10 Logical Switching Break-Fix Scenario 1.....	60
Task 1: Read the Scenario Description.....	60
Task 2: Confirm the Problem	61
Task 3: Troubleshoot and Fix the Problem	62
Task 4: Verify That the Problem Is Fixed	62

Lab 11 Logical Switching Break-Fix Scenario 2	63
Task 1: Read the Scenario Description.....	63
Task 2: Confirm the Problem	64
Task 3: Troubleshoot and Fix the Problem	65
Task 4: Verify That the Problem Is Fixed	65
Lab 12 Logical Switching Challenge Scenario	66
Task 1: Read the Scenario Description.....	66
Task 2: Confirm the Problem	67
Task 3: Troubleshoot and Fix the Problem	68
Task 4: Verify That the Problem Is Fixed	68
Lab 13 Logical Routing Verification	69
Task 1: Prepare for the Lab	70
Task 2: Verify the Tier-1 and Tier-0 Gateways from the NSX UI	70
Task 3: Verify the Logical Routers from the NSX CLI on the NSX Manager Instance	70
Task 4: Verify the Logical Routers from the NSX CLI on the ESXi Host	72
Task 5: Verify the Logical Routers from the NSX CLI on the KVM Host.....	75
Task 6: Verify the Logical Routers from the NSX CLI on the NSX Edge Nodes	76
Lab 14 Logical Routing Break-Fix Scenario 1.....	80
Task 1: Read the Scenario Description.....	80
Task 2: Confirm the Problem	81
Task 3: Troubleshoot and Fix the Problem	82
Task 4: Verify That the Problem Is Fixed	82
Lab 15 Logical Routing Break-Fix Scenario 2	83
Task 1: Read the Scenario Description.....	83
Task 2: Confirm the Problem	84
Task 3: Troubleshoot and Fix the Problem	85
Task 4: Verify That the Problem Is Fixed	85
Lab 16 Logical Routing Break-Fix Scenario 3	86
Task 1: Read the Scenario Description.....	86
Task 2: Confirm the Problem	87
Task 3: Troubleshoot and Fix the Problem	88
Task 4: Verify That the Problem Is Fixed	88

Lab 17 Logical Routing Challenge Scenario 1	89
Task 1: Read the Scenario Description.....	89
Task 2: Confirm the Problem	90
Task 3: Troubleshoot and Fix the Problem	91
Task 4: Verify That the Problem Is Fixed	91
Lab 18 Logical Routing Challenge Scenario 2	92
Task 1: Read the Scenario Description.....	92
Task 2: Confirm the Problem	93
Task 3: Troubleshoot and Fix the Problem	94
Task 4: Verify That the Problem Is Fixed	95
Lab 19 Distributed Firewall Verification.....	96
Task 1: Prepare for the Lab.....	97
Task 2: Enable Distributed Firewall Rules	98
Task 3: Test the Connectivity Between Three-Tier App Machines.....	99
Task 4: Verify DFW Rules from the ESXi CLI.....	101
Task 5: Verify DFW Rules from the KVM CLI	105
Task 6: Prepare for the Next Lab.....	107
Lab 20 Distributed Firewall Break-Fix Scenario 1.....	108
Task 1: Read the Scenario Description.....	108
Task 2: Confirm the Problem	109
Task 3: Troubleshoot and Fix the Problem	110
Task 4: Verify That the Problem Is Fixed	110
Lab 21 Distributed Firewall Break-Fix Scenario 2	111
Task 1: Read the Scenario Description.....	111
Task 2: Confirm the Problem	112
Task 3: Troubleshoot and Fix the Problem	113
Task 4: Verify That the Problem Is Fixed	113
Lab 22 Distributed Firewall Challenge Scenario	114
Task 1: Read the Scenario Description.....	114
Task 2: Confirm the Problem	115
Task 3: Troubleshoot and Fix the Problem	116
Task 4: Verify That the Problem Is Fixed	116

Lab 23 Gateway Firewall Verification.....	117
Task 1: Prepare for the Lab.....	118
Task 2: Test Connectivity	118
Task 3: Enable Gateway Firewall Rules.....	119
Task 4: Test Connectivity	119
Task 5: Verify Gateway Rules from the NSX Edge CLI	120
Task 6: Prepare for the Next Lab.....	122
Lab 24 Gateway Firewall Break-Fix Scenario 1.....	123
Task 1: Read the Scenario Description.....	123
Task 2: Confirm the Problem	125
Task 3: Troubleshoot and Fix the Problem	125
Task 4: Verify That the Problem Is Fixed	125
Lab 25 Gateway Firewall Break-Fix Scenario 2	126
Task 1: Read the Scenario Description.....	126
Task 2: Confirm the Problem	128
Task 3: Troubleshoot and Fix the Problem	128
Task 4: Verify That the Problem Is Fixed	128
Lab 26 Load Balancer Verification.....	129
Task 1: Prepare for the Lab.....	129
Task 2: Verify the Load Balancer Operation	131
Task 3: Verify the Load Balancer Configuration from the NSX CLI.....	133
Task 4: Prepare for the Next Lab.....	136
Lab 27 Load Balancer Break-Fix Scenario 1.....	137
Task 1: Read the Scenario Description.....	137
Task 2: Confirm the Problem	138
Task 3: Troubleshoot and Fix the Problem	139
Task 4: Verify That the Problem Is Fixed	139
Lab 28 Load Balancer Break-Fix Scenario 2	140
Task 1: Read the Scenario Description.....	140
Task 2: Confirm the Problem	141
Task 3: Troubleshoot and Fix the Problem	142
Task 4: Verify That the Problem Is Fixed	142

Lab 29 IPSEC VPN Break-Fix Scenario	143
Task 1: Read the Scenario Description.....	143
Task 2: Confirm the Problem	144
Task 3: Troubleshoot and Fix the Problem	145
Task 4: Verify That the Problem Is Fixed	145
Lab 30 L2 VPN Verification	146
Task 1: Prepare for the Lab	147
Task 2: Verify the IPsec VPN from the NSX CLI	148
Task 3: Verify the L2 VPN from the NSX CLI	150
Task 4: Verify the Operation of the VPN Setup	153
Lab 31 L2 VPN Break-Fix Scenario	155
Task 1: Read the Scenario Description.....	155
Task 2: Confirm the Problem	157
Task 3: Troubleshoot and Fix the Problem	157
Task 4: Verify That the Problem Is Fixed	157
Lab 32 L2 VPN Challenge Scenario	158
Task 1: Read the Scenario Description.....	158
Task 2: Confirm the Problem	160
Task 3: Troubleshoot and Fix the Problem	160
Task 4: Verify That the Problem Is Fixed	160
Lab 33 Datapath Troubleshooting for the E-W Packet Capture	161
Task 1: Use Traceflow	161
Task 2: Perform Data Collection for Packet Capture	163
Task 3: Perform Packet Capture	167
Lab 34 Datapath Troubleshooting for the N-S Packet Capture	178
Task 1: Use Traceflow	178
Task 2: Perform Data Collection for Packet Capture	180
Task 3: Perform Packet Capture	187

Lab 1 Reviewing the Lab Structure and Environments

Objective and Tasks

Prepare for all labs by reviewing the lab structure and environments:

1. Review the Lab Environment Configuration
2. Review the Production Environment Overview
3. Review the Staging Environment Overview
4. Review the Development and QA Environment Overview
5. Review the Lab Types
6. Review Best Practices to Access the Lab Environment

Task 1: Review the Lab Environment Configuration

You review the lab environment configuration to be used in future labs.

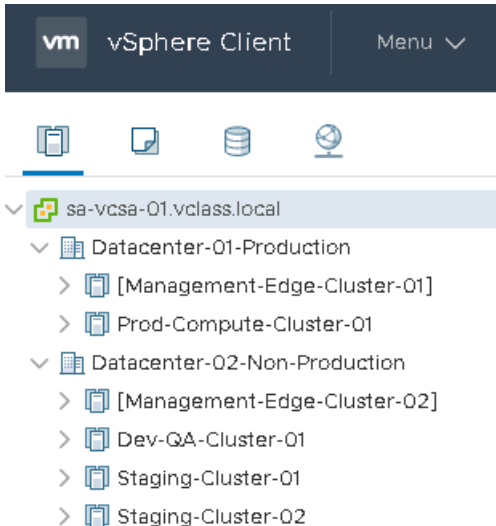
1. Read the information about your role at a fictional company.

You assume the role of the network administrator for the Virtual Coffee Beans Company. In preparation for an upcoming audit, your manager asked you to perform a series of verification checks on the company's Production environment. You must confirm that this environment is configured and working as expected. As part of your job, you must also investigate and fix any user-reported issues that might arise in the company's Non-Production environment.

2. Review the configuration information.

The following software-defined data centers (SDDC) are available as part of the vSphere environment:

- DataCenter-01-Production: Contains two vSphere clusters representing a healthy and working environment. This environment is used for validating the NSX-T Data Center components.
- DataCenter-02-Non-Production: Contains four vSphere clusters representing a problematic environment and is used for troubleshooting the NSX-T Data Center problems.



The SDDCs provide infrastructure services for the company's environments and business units:

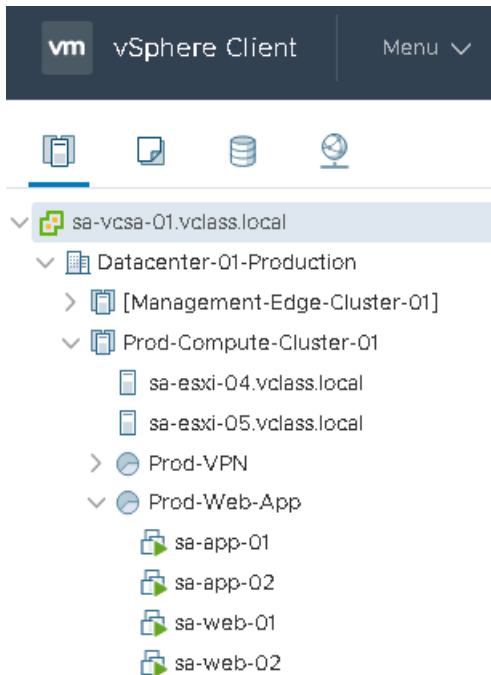
- Production (Prod):
 - Hosts the production (Prod) workloads across various business units and the company's remote office branch office (ROBO) implementation.
 - Runs on the DataCenter-01-Production data center and represents a healthy and working environment.
 - Is used for lab tasks that involve the verification of the NSX-T Data Center components

- Non-Production (Non-Prod):
 - Hosts the workloads from the Development (DEV), Staging (STG), and QA (QA) business units.
 - Runs on the DataCenter-02-Non-Production data center and represents a misconfigured and nonworking environment.
 - Is used for lab tasks that involve troubleshooting the NSX-T Data Center problems.

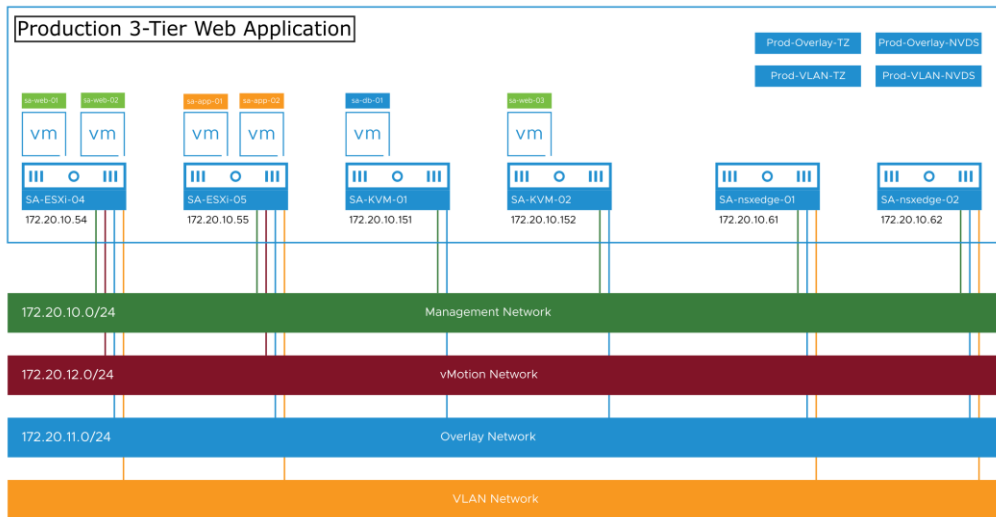
Task 2: Review the Production Environment Overview

The production environment runs a three-tier web application with database, application, and web tiers running across ESXi and KVM hosts. You review an overview of the Production environment components to be used in future labs.

1. Review the configuration of the three-tier web application and the corresponding vCenter Server inventory items.



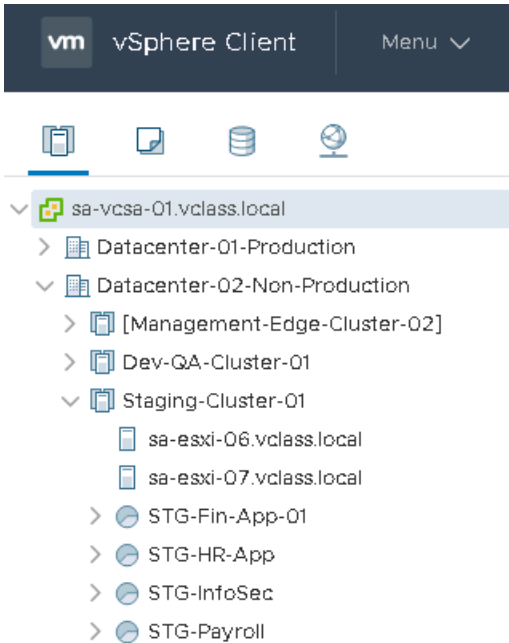
- Review the topology for the Production environment.



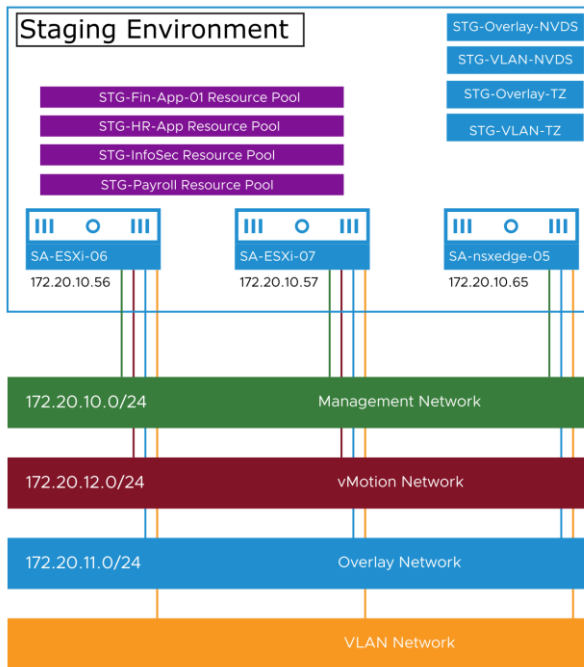
Task 3: Review the Staging Environment Overview

The Staging (STG) environment runs on a dedicated cluster in the Non-Production SDDC. You review an overview of the Staging environment components to be used in future labs.

1. Review the configuration of the Staging environment and the corresponding vCenter Server inventory items.



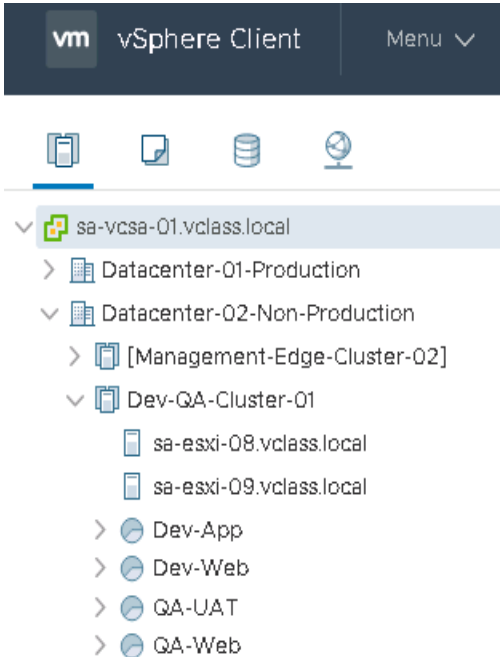
- Review the topology for the Staging environment.



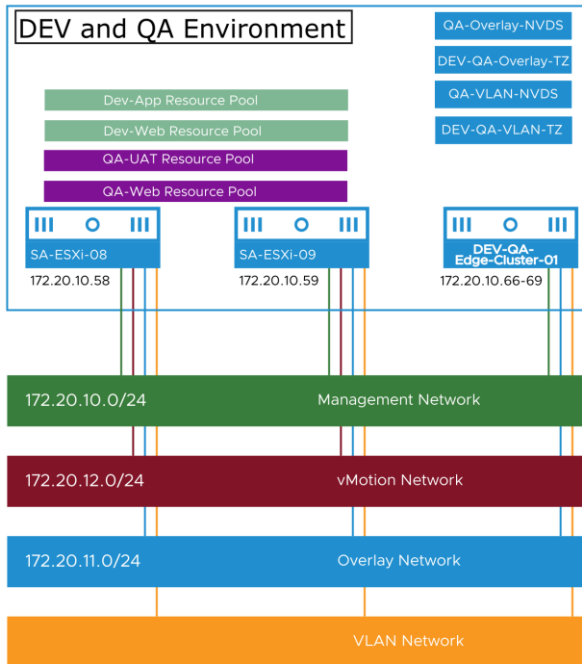
Task 4: Review the Development and QA Environment Overview

The Development and QA environments run on the same vSphere cluster in the Non-Production SDDC and share some NSX components. You review an overview of the components of these environments to be used in future labs.

1. Review the configuration of the Development and QA environments and the corresponding vCenter Server inventory items.



2. Review the topology for these environments.



Task 5: Review the Lab Types

You review the information about the different types of lab activities.

1. Review the information about the Verification lab activities.

In Verification labs, you explore and gather information from the healthy Production environment. You record the relevant information in the student worksheet.

2. Review the information about the Break-Fix Scenario and Challenge Scenario lab activities.

- In Break-Fix Scenario and Challenge Scenario labs, you troubleshoot and fix problems in the Non-Production environment.
- The Challenge Scenario labs are optional and involve a higher difficulty level.

You might need to use supplemental materials, such as knowledge base articles or user documentation, to resolve the problems in these labs.

Task 6: Review Best Practices to Access the Lab Environment

You review the best practices that enable you to effectively perform future labs.

1. Review the best practices that you must follow across all labs.
 - You use Remote Desktop Protocol (RDP) to enter the environment and access the student desktop.
 - The student desktop resides on the Management network (SA-Management). You use the student desktop to validate the environment, run commands on NSX-T Data Center components, and troubleshoot Break-Fix Scenario labs.
 - Notepad++ is installed on the student desktop and can be accessed from the taskbar. You can use Notepad++ to save the command outputs and log events that you gather during the labs. You must create one file per lab task to organize the content for future reference.
 - Depending on the type of lab being performed (Verification, Break-Fix Scenario, or Challenge Scenario), you log in to either the Production or Non-Production NSX-T Data Center instances. Browser bookmarks are provided for each instance.
 - In the Verification labs, you gather information. You can record this information in the student worksheet.

Lab 2 NSX-T Data Center Operations and Troubleshooting Tools

Objective and Tasks

Configure Syslog, generate a support bundle, and use Traceflow:

1. Prepare for the Lab
2. Configure Syslog in NSX Manager and Review the Collected Logs
3. Configure Syslog in an NSX Edge Node and Review the Collected Logs
4. Generate a Technical Support Bundle for NSX Manager
5. Configure a Traceflow Session
6. Examine the Traceflow Output

Task 1: Prepare for the Lab

You log in to the vSphere Client UI and the NSX UI.

1. From your student desktop, log in to the vSphere Client UI.
 - a. Open Chrome.
 - b. Select the **vSphere Site-A > vSphere Client (SA-VCSA-01)** bookmark.
 - c. On the login page, enter **administrator@vsphere.local** as the user name and **VMware1!** as the password.
2. Log in to the NSX UI.
 - a. Open another tab in Chrome.
 - b. Select the **NSX-T Data Center > NSX Manager (Prod)** bookmark.
 - c. On the login page, enter **admin** as the user name and **VMware1!VMware1!** as the password.

Task 2: Configure Syslog in NSX Manager and Review the Collected Logs

You configure a Syslog server address in NSX Manager, and you review the collected logs from the remote Syslog collector.

1. From MTPuTTY, click **sa-nsxmgr-01** under **Production - NSX Inventory**.
2. Configure NSX Manager to send the UDP info-level log messages to the vRealize Log Insight server.

```
set logging-server sa-vrli-01.vclass.local:514 proto udp
level info
```

You can use the DNS name or the IP address of the Syslog server in your configuration.

3. Verify your logging configuration.

```
get logging-server
```
4. Log in to the vRealize Log Insight UI.
 - a. Open another tab in Chrome.
 - b. Select the **NSX-T Data Center > vRealize Log Insight** bookmark.
 - c. On the login page, enter **admin** as the user name and **VMware1!** as the password.
5. In the vRealize Log Insight UI header, click **Interactive Analytics**.
6. Verify that the log messages from the NSX Manager component appear in the Events pane.

Events	Field Table	Event Types	Event Trends	1 to 50 out of 4,605 events	View ▾	Sort: Newest First ▾
5/6/2020 04:12:14.912	2020-05-06T11:12:29.186Z	sa-nsxmgr-01.vclass.local NSX 6245 - [nsx@6876 comp="nsx-manager" level="WARNING" subcomp="manager"] com.vmware.nsx.rpc.transport.netty.KeepAliveFsm@7420cdc9: Could not update keepalive rtt. Keepalive request was not flushed.	source event_type hostname appname procid msgid			
5/6/2020 04:12:14.129	2020-05-06T11:12:28.403Z	sa-nsxmgr-01 NSX 916 - [nsx@6876 comp="nsx-manager" subcomp="mpa-client" tid="1192" level="INFO"] [HostNodeStatusVertical] SendRequest: To Master APH, Publish, type (com.vmware.nsx.management.agg_service.node.NodeStatusPropertiesMsg) correlationId () Success.	source event_type hostname appname procid msgid			

7. Return to the SA-NSX-Manager-01 MTPuTTY session and remove the Syslog server configuration.

```
del logging-server sa-vrli-01.vclass.local:514 proto udp
level info
```

- Verify that the logging server is removed.

```
get logging-server
```

A blank system prompt must be returned.

Task 3: Configure Syslog in an NSX Edge Node and Review Collected Logs

You configure a Syslog server address in NSX Edge, and you review the collected logs from the remote Syslog collector.

- From MTPuTTY, double-click **sa-nsxedge-01**.

- Configure the NSX Edge node with a DNS server.

```
set name-servers 172.20.10.10
```

- Configure the NSX Edge node to send TCP info-level log messages to the Syslog server.

```
set logging-server sa-vrli-01.vclass.local:514 proto tcp
level info
```

- Verify your logging configuration.

```
get logging-servers
```

- Return to the vRealize Log Insight UI and click **Interactive Analytics** to refresh the displayed data.

- Verify that the log messages from the NSX Edge node appear in the events pane.

Events	Field Table	Event Types	Event Trends	1 to 50 out of 1,563 events	View ▾	Sort: Newest First ▾
5/6/2020 04:21:36.131	2020-05-06T11:21:03.152Z	sa-nsxedge-01	NSX 26598 - [nsx@6876 comp="nsx-edge" subcomp="cpu_usage_monitor" username="root" level="INFO"] Acquired Lock on file, proceeding to check for CPU usage			
		source	event_type	hostname	appname	procid msgid
5/6/2020 04:21:36.123	2020-05-06T11:21:03.141251+00:00	sa-nsxedge-01	NSX 3250 FIREWALL [nsx@6876 comp="nsx-edge" subcomp="datapathd.firewallgr" level="INFO"] HTTP method with url: https://publicsuffix.org/list/public_suffix_list.dat, body:			
		source	event_type	hostname	appname	procid msgid

- Return to the sa-nsxedge-01 MTPuTTY session and remove the Syslog server configuration.

```
del logging-server sa-vrli-01.vclass.local:514 proto tcp
level info
```

8. Verify that the logging server is removed.

```
get logging-server
```

A blank system prompt must be returned.

9. Close all MTPuTTY sessions and the vRealize Log Insight UI browser tab.

Task 4: Generate a Technical Support Bundle for NSX Manager

You generate a technical support bundle to gather log and configuration information for NSX Manager.

1. On the NSX UI Home page, select **System > Support Bundle**. Support Bundle is located under the Settings section of the side menu.
2. At the Request Bundle step, verify that **Management Nodes** is selected from the **Type** drop-down menu.
3. From the Available pane, select the **sa-nsxmgr-01** check box and click the right arrow to move it to the Selected pane.
4. Set the log age (days) to 1 by clicking the down arrow.
5. Turn on the **Include core files and audit logs** toggle to display **Yes**.
6. Click **START BUNDLE COLLECTION**.

In the Status step, you monitor the collection progress. This process might take up to 15 minutes to complete. When the support bundle is ready, the **DOWNLOAD** button appears.

1. Request Bundle

2. Status

Task started at

May 6, 2020 4:40:21 AM by admin

Task ended at

May 6, 2020 4:54:40 AM

Status

Completed

100%

NEW BUNDLE REQUEST

Support Bundle

893.9 MB

DOWNLOAD

DELETE

Details

Show: ALL 1 SUCCESSFUL 0 FAILED

Node	ID	IP Address	Status	Details	Size ↑
sa-nsxmgr-01	af68...d479	172.20.10.41	● Successful	nsx_manager_af681d...	893.9 MB

NOTE

You do not need to wait for the generation of the support bundle to complete. You can return later if you want to download and examine the contents of the support bundle.

Task 5: Configure a Traceflow Session

You specify the source VM and the destination VM of a Traceflow session.

1. Open MTPuTTY and open an SSH session to the SA-KVM-01 host, located in the `Production-Infrastructure` folder.
 - a. Power on the sa-db-01 VM.

```
$ sudo virsh start sa-db-01
```
 - b. Verify that the sa-db-01 VM is powered on.

```
$ sudo virsh list --all
```
2. On the NSX UI Home page, select **Plan and Troubleshoot > Troubleshooting Tools > Traceflow**.
3. On the **Traceflow** tab, configure the VM details.
 - a. In the main pane, configure the details.

Option	Action
IP Address	Select IPv4 (default).
Traffic Type	Select Unicast (default).
Protocol Type	Select ICMP (default).

- b. In the Source pane, configure the source VM details.

Option	Action
Type	Select Virtual Machine (default).
VM Name	Select sa-app-01 .
Virtual Interface	Select Network adapter 1 (default).

- c. In the Destination pane, configure the destination VM details.

Option	Action
Type	Select Virtual Machine (default).
VM Name	Select sa-db-01 .
Virtual Interface	Select T1-DB-01 (default).

4. Click **TRACE**.

Task 6: Examine the Traceflow Output

You examine the Traceflow output to determine how the packet is introduced in the datapath, which components are involved, and how the packet is delivered.

1. If a trace observation warning message appears, ignore and close the message because your lab runs in a nested ESXi environment.



Traceflow round has multiple physical received observations. Please check whether the underlayer switch flood packets. Your hypervisor may be in nested environment.



2. Verify that the Traceflow output that appears includes the network diagram at the top and the observations pane with the steps of the packet at the bottom.

Traceflow

IP Type: IPv4

Traffic Type: Unicast

Protocol Type: ICMP

Source: sa-app-01

IP: 172.16.20.11

MAC: 00:50:56:ae:55:36

Destination: sa-db-01

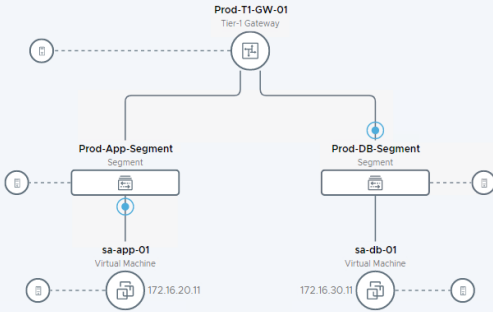
IP: 172.16.30.11

MAC: 00:23:20:44:72:e8

May 6, 2020, 7:03:06 AM

RETRACE

EDIT



Observations

All

1 Delivered

0 Dropped

Physical Hop Count	Observation Type	Transport Node	Component	Timestamp
0	Injected	sa-esxi-05.vclass.local	Network adapter 1	07:03:16.030.491
0	Received	sa-esxi-05.vclass.local	Distributed Firewall	07:03:16.030.528
0	Forwarded	sa-esxi-05.vclass.local	Distributed Firewall (Rule ID: 2)	07:03:16.030.562

3. In the first row of the packet walk in the Observations pane, verify that a packet is introduced through the transport node.
4. In the second and third rows, verify that the distributed firewall receives the packet, applies firewall rules, and forwards the packet to the Prod-App-Segment segment.
5. In the fourth through seventh rows, verify that Prod-App-Segment, which is attached to the Prod-T1-GW-01 gateway, receives and forwards the packet to the Prod-DB-Segment segment.
6. In the eighth and ninth rows, verify that the source TEP and destination TEP IP addresses appear.

The source and the destination VMs reside on different hosts.

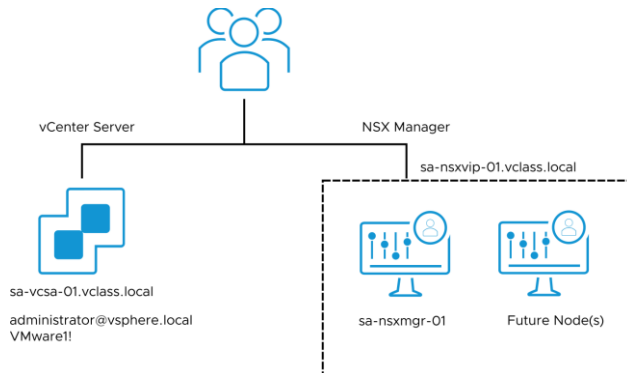
7. In the 10th and 11th rows, verify that the distributed firewall receives the packet and applies firewall rules, if any, at the destination host.
8. In the last row, verify that the packet is delivered to the destination VM's port.

Lab 3 NSX Management Cluster Verification

Objective and Tasks

Verify the formation of the management cluster:

1. Prepare for the Lab
2. Verify the NSX Management Cluster Status from the UI
3. Verify the NSX Management Cluster Status from the NSX CLI



Task 1: Prepare for the Lab

You log in to the vSphere Client UI and the NSX UI.

1. From your student desktop, log in to the vSphere Client UI.
 - a. Open Chrome.
 - b. Click the **vSphere Site-A > vSphere Client (SA-VCSA-01)** bookmark.
 - c. On the login page, enter **administrator@vsphere.local** as the user name and **VMware1!** as the password.
2. Log in to the NSX UI.
 - a. Open another tab in Chrome.
 - b. Select the **NSX-T Data Center > NSX Manager (Prod)** bookmark.
 - c. On the login page, enter **admin** as the user name and **VMware1!VMware1!** as the password.

Task 2: Verify the NSX Management Cluster Status from the UI

You verify the NSX management cluster status from the NSX UI.

- From the NSX UI, verify the NSX Management cluster status.
 - Click **System > Appliances**
 - Click **VIEW DETAILS** to obtain information about individual nodes in the cluster.
- Use the information in the NSX UI to record the status and configuration of the NSX management cluster in the Value column of this table in your student worksheet. Note that it is necessary to click VIEW DETAILS on the node to display some of the details required to populate the table.

IMPORTANT

In all Verification lab tasks, you record the information in the tables in your student worksheet.

NSX UI Management Cluster Verification for sa-nsxmgr-01

Parameter	Value
Cluster (status of)	
Cluster ID	
Virtual IP	
Node UUID	
Operational Status of MANAGER	

- Verify that the NSX management cluster status appears as STABLE and the cluster node status appears as Available.

Task 3: Verify the NSX Management Cluster Status from the NSX CLI

You verify the NSX management cluster status from the `nsxcli` command line.

1. Open MTPuTTY from the taskbar on the student desktop.
2. Double-click **sa-nsxmgr-01** in the `Production - NSX Inventory` folder to log in to the `nsxcli` command line.
As there is an NSX Manager instance with a similar name in the Non-Production environment, ensure that you have logged in to the correct NSX Manager instance before proceeding further.
3. Disable the CLI timeout.

```
sa-nsxmgr-01> set cli-timeout 0
```
4. Query the status of the NSX management cluster.

```
sa-nsxmgr-01> get cluster status
```
5. Use the information in the command output to record the status and configuration of the NSX management cluster in the Value column of this table in your student worksheet.

NSX Management Cluster Status Verification using NSX CLI

Parameter	Value
Cluster ID	
Overall status	
DATASTORE group status	

The UUID and status of NSX Manager nodes running other groups such as `CLUSTER_BOOT_MANGER`, `MANAGER`, `POLICY`, and `HTTPS` also appear.

6. Query the NSX management cluster configuration.

```
sa-nsxmgr-01> get cluster config
```

7. Use the information in the command output to record the status and configuration of the NSX CLI management cluster in the Value column of this table in your student worksheet.

NSX Management Cluster Configuration Verification using NSX CLI

Parameter	Value
Cluster ID	
Number of nodes in the cluster	
Node UUID	
HTTPS Port	
DATASTORE Port	
IP Address	

- a. Verify that the Node UUID recorded here is same as the UUID recorded using NSX UI in the previous task.
 - b. Verify that the IP Address recorded here is the node IP address and not the cluster virtual IP recorded in the previous task.
8. Verify that each NSX Manager node is joined to the cluster by ensuring that the node status is set to JOINED.

Lab 4 NSX Management Cluster Break-Fix Scenario

Objective and Tasks

Identify, diagnose, and resolve an NSX management cluster problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify that the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

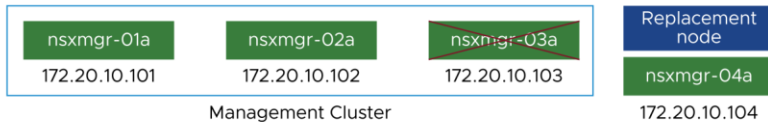
One of the NSX Manager VMs configured in the existing three-node NSX management cluster has failed and is unrecoverable. The failure occurred because the ESXi server hardware malfunctioned.

VMware Support advises removing the failed NSX Manager instance from the existing NSX management cluster and creating a three-node cluster with a new NSX Manager VM.

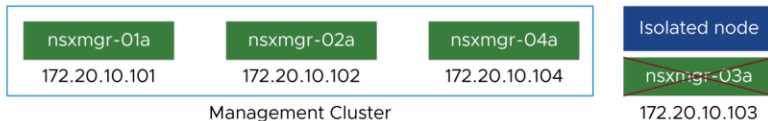
2. Review details about the lab environment and the course of action.

- The existing NSX management cluster was configured with the nsxmgr-01a, nsxmgr-02a, and nsxmgr-03a nodes. The nsxmgr-03a node has failed and is unrecoverable.
- The nsxmgr-04a node is already deployed and runs on the standalone sa-esxi-13.vclass.local ESXi host.
- The nsxmgr-03a node should be detached from the existing NSX management cluster.
- The nsxmgr-04a node should be joined to the existing NSX management cluster.

- At the beginning of the lab, one of the cluster nodes (nsxmgr-03) is in the DOWN status



- At the end of the lab the cluster must include the following nodes:



When this lab concludes, a three-node NSX management cluster must be configured with the nsxmgr-01a, nsxmgr-02a, and nsxmgr-04a nodes.

Task 2: Confirm the Problem

You confirm a problem that was reported by the help desk: nsxmgr-03a has failed in a three-node management cluster.

The NSX Manager VMs are in the vCenter Server inventory under the Management-Edge-Cluster-02 cluster in the Datacenter-02-Non-Production data center.

1. In Chrome, open the **NSX-T DataCenter > NSX Manager (Non-Prod)** bookmark.
2. Log in to NSX Manager by entering **admin** as the user name and **VMware1!VMware1!** as the password .
3. From the NSX UI, select **System > Appliances**.
4. Verify the management cluster status.

The status must appear as DEGRADED.

5. Verify the cluster connectivity status of the 172.20.10.103 member node.

The status must appear as Unavailable.

6. In MTPuTTY, double-click **nsxmgr-01a** in the Non Production - NSX Inventory folder.
7. Verify that the NSX Manager name is nsxmgr-01a.

NOTE

Before performing the next step, verify that the NSX Manager name is correct. The NSX Manager name must be nsxmgr-01a in the Non Production - NSX Inventory folder in MTPuTTY.

8. Verify the management cluster status.

```
nsxmgr-01a> get cluster status
```

In the command output, nsxmgr-03a is DOWN.

9. Verify the HTTP service state on nsxmgr-01a with the `get service http` command.

Example:

```
nsxmgr-01a> get service http
Service name:                http
Service state:            running
Logging level:               info
Session timeout:             1800
Connection timeout:          30
Client API rate limit:       100 requests/sec
Client API concurrency limit: 40 connections
Global API concurrency limit: 199 connections
Redirect host:                (not configured)
Basic authentication:         enabled
Cookie-based authentication:  enabled
```

10. (Optional) If the HTTP service has stopped on nsxmgr-01a, start the HTTP service.

```
nsxmgr-01a> start service http
```

11. In the MTPuTTY window, find nsxmgr-02a under the Non Production - NSX Inventory folder and double-click **nsxmgr-02a** to connect through SSH.

12. Verify the HTTP service state on nsxmgr-02a.

```
nsxmgr-02a> get service http
```

13. (Optional) If the HTTP service has stopped on nsxmgr-02a, start the HTTP service.

```
nsxmgr-02a> start service http
```

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in this course to troubleshoot and fix the problem.

1. Open MTPuTTY and click the **nsxmgr-01a** tab.

NOTE

Before performing the next step, verify that the NSX Manager name is correct. The NSX Manager name must be nsxmgr-01a in the Non Production - NSX Inventory folder in MTPuTTY.

2. Verify the status and retrieve the UUID.

- a. Verify the management cluster status.

```
nsxmgr-01a> get cluster status
```

In the command output, the cluster status is DEGRADED and the nsxmgr-03a status is DOWN.

- b. Copy the nsxmgr-03a UUID and paste it in a Notepad file.

The nsxmgr-03a manager UUID appears under Manager Group in the get cluster status command output.

- c. (Optional) If the % The get cluster status operation cannot be processed currently, please try again later message appears, wait for 2 minutes and run the get cluster status command again.

3. Remove the failed NSX Manager node on nsxmgr-01.

```
detach node <nsxmgr-03a-node-UUID>
```

Example:

```
nsxmgr-01a> detach node 61ca1d42-a537-fb2b-458c-3352cabb97ae
Node has been detached. Detached node must be deleted permanently.
```

4. Verify the cluster status.

```
nsxmgr-01a> get cluster status
```

In the command output, the cluster group status is STABLE and all the references to the nsxmgr-03a node are removed from the cluster.

5. Obtain the NSX Manager thumbprint.

- a. Retrieve the thumbprint.

```
nsxmgr-01a> get certificate api thumbprint
```

Example:

```
nsxmgr-01a> get certificate api thumbprint
17f9165415bd7ed8c7e7764b019a75b621b67190ac14fa660a5be46ed
6bd5523
```

- b. Copy the retrieved thumbprint to the Notepad file.

6. Obtain the cluster ID.

- a. Retrieve the cluster ID.

```
nsxmgr-01a> get cluster config
```

Example:

```
nsxmgr-01a> get cluster config
Cluster Id: cfec1b3b-290c-441e-a0a3-f14ad389f932
Cluster Configuration Version: 8
```

- b. Copy the retrieved cluster ID to the Notepad file.

7. In MTPuTTY, double-click **nsxmgr-04a** in the Non Production - NSX Inventory folder.

8. Join nsxmgr-04a to the existing management cluster.

```
nsxmgr-04a> join 172.20.10.101 cluster-id <Cluster-ID>
thumbprint <nsxmgr-01a-thumbprint> username admin password
VMware1!VMware1!
```

Example:

```
nsxmgr-04a> join 172.20.10.101 cluster-id cfec1b3b-290c-
441e-a0a3-f14ad389f932 thumbprint
17f9165415bd7ed8c7e7764b019a75b621b67190ac14fa660a5be46ed6bd
5523 username admin password VMware1!VMware1!
Data on this node will be lost. Are you sure? (yes/no): yes
Join operation successful. Services are being restarted.
Cluster may take some time to stabilize.
```

The join command typically takes up to 10 minutes to successfully join nsxmgr-04a to the management cluster.

9. Verify the cluster status on nsxmgr-04a.

```
nsxmgr-04a> get cluster status
```

If the nsxmgr-04a status is DOWN, wait for a few more minutes and run the `get cluster status` command again. In the command output, the management cluster must be formed with the nsxmgr-01a, nsxmgr-02a, and nsxmgr-04a nodes.

10. Open Chrome and click **NSX Manager (Non Prod)** in the NSX-T Data Center bookmarks folder.
 - a. If necessary, log in to nsxmgr-01a with `admin` as the user name and `VMware1!VMware1!` as the password.
11. Select **System > Appliances**.

In the management cluster status, three NSX Manager nodes (sa-nsxmgr-01a : 172.20.10.101, nsxmgr-02a : 172.20.10.102, nsxmgr-04a : 172.20.10.104) appear and the management cluster status is STABLE.

Task 4: Verify That the Problem Is Fixed

You verify that the three-node management cluster is configured and that the status is UP.

1. Open MTPuTTY and click the **nsxmgr-01a** tab.
2. Verify the cluster status.

```
get cluster status
```

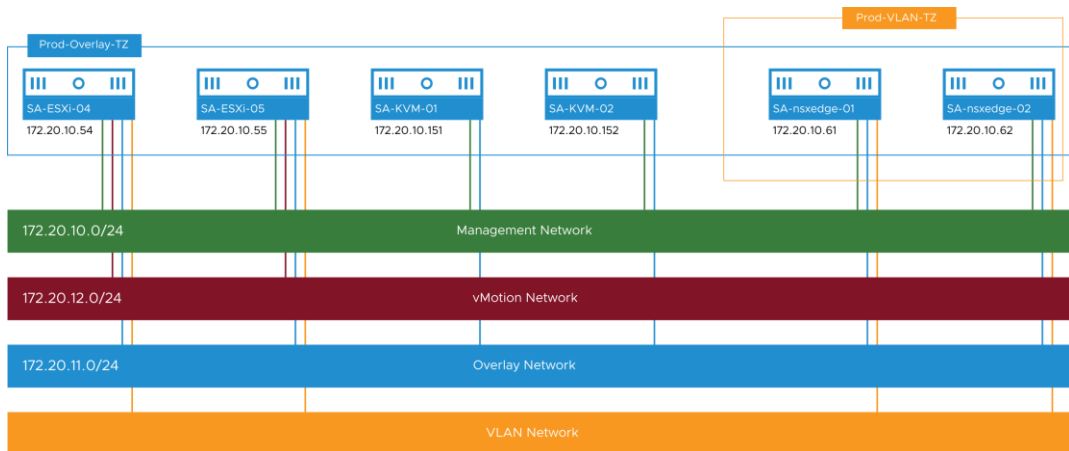
The nsxmgr-01a, nsxmgr-02a, and nsxmgr-04a nodes appear in the command output with the UP status.

Lab 5 Infrastructure Preparation Verification

Objective and Tasks

Verify the transport node preparation prerequisites and status:

1. Prepare for the Lab
2. Verify the Transport Node Preparation Prerequisites
3. Verify the Transport Node Preparation from the NSX UI
4. Verify the Transport Node Preparation from the ESXi CLI
5. Verify the Transport Node Preparation from the KVM CLI
6. Verify the NSX Edge Configuration from the NSX CLI



Task 1: Prepare for the Lab

You prepare for the lab by logging in to the NSX UI.

1. Log in to the NSX UI.
 - a. Open another tab in Chrome.
 - b. Select the **NSX-T Data Center > NSX Manager (Prod)** bookmark.

NOTE

You log in to the Production NSX Manager UI with URL <https://sa-nsxvip-01.vclass.local/login.jsp?> to perform this task.

- c. On the login page, enter **admin** as the user name and **VMware1!VMware1!** as the password .

Task 2: Verify the Transport Node Preparation Prerequisites

You verify the transport node prerequisites from the NSX UI.

1. Verify the compute manager registration.
 - a. From the NSX UI, select **System > Fabric > Compute Managers**.
 - b. Use the information in the NSX UI to record the configuration and status details for the `sa-vcsa-01.vclass.local` compute manager in the Value column of this table in your student worksheet.

Compute Manager Details for sa-vcsa-01.vclass.local

Parameter	Value
Type	
Registration status	
Version	
Connection status	

2. Verify the transport zone configuration.

- a. From the NSX UI, select **System > Fabric > Transport Zones**.
- b. Verify that the Prod-Overlay-TZ and Prod-VLAN-TZ transport zones exist.
- c. Click the **Prod-Overlay-TZ** transport zone and use the information that appears to record the transport zone details in the Value column of this table in your student worksheet.

Transport Zone Details for Prod-Overlay-TZ

Parameter	Value
Traffic type	
Switch name	
Number of Transport Nodes	
Number of Switches	

- d. Click the **Prod-VLAN-TZ** transport zone and use the information that appears to record the transport zone details in the Value column of this table in your student worksheet.

Transport Zone Details for Prod-VLAN-TZ

Parameter	Value
Traffic type	
Switch name	
Number of Transport Nodes	
Number of Switches	

3. Verify the uplink profiles.
 - a. Select **System > Fabric > Profiles** and click the **Uplink Profiles** tab.
 - b. On the **Uplink Profiles** tab, verify that ESXi-Host-Uplink-Profile and KVM-Hosts-Uplink-Profile were created to be used for ESXi and KVM transport nodes.
 - c. Record the configuration details for KVM-Hosts-Uplink-Profile in the Value column of this table in your student worksheet.

Uplink Profile Details: KVM-Hosts-Uplink-Profile

Parameter	Value
Teaming policy	
Active uplinks	
MTU	

4. Verify the configuration of the IP pools.
 - a. Select **Networking > IP Address Pools**.
 - b. On the **IP ADDRESS POOLS** tab, verify that TEP-IP-Pool exists and the status of the IP address pool is Success.
 - c. Click the **1** numbered link in the Subnets column and click the arrow to expand the IP range information.
 - d. Record the IP range information of the TEP-IP-Pool in the Value column of this table in your student worksheet.

Subnet IP Range Details for TEP-IP-Pool

Parameter	Value
IP ranges	172.20._____ - 172.20._____
CIDR	172.20._____
Gateway	172.20._____

Task 3: Verify the Transport Node Preparation from the NSX UI

You verify the KVM and ESXi transport nodes configuration from the NSX UI.

The sa-kvm-01.vclass.local, sa-kvm-02.vclass.local, sa-esxi-04.vclass.local, and sa-esxi-05.vclass.local nodes are already configured as transport nodes in the Production environment.

1. Verify the host transport nodes.

- a. From the NSX UI, select **System > Fabric > Nodes > Host Transport Nodes**.
- b. From the **Managed by** drop-down menu, select **None: Standalone Hosts** and verify that sa-kvm-01.vclass.local and sa-kvm-02.vclass.local are configured as transport nodes.
- c. Use the information available in the NSX UI to record the configuration of the sa-kvm-01.vclass.local host transport node in the Value column of this table in your student worksheet.
Click the information icon next to the Up status to display additional information about the manager connectivity, controller connectivity, PNIC/bond status, and tunnel status.

Host Transport Node Details for sa-kvm-01.vclass.local

Parameter	Value
Node status	
NSX Configuration (state)	
OS type	
TEP IP address	
Manager Connectivity	
Controller Connectivity	
Transport Zones	

- i. Verify that the TEP IP address recorded here is from the IP range recorded in the previous task.
- d. On the **Host Transport Nodes** tab, select **sa-vcasa-01.vclass.local** from the **Managed by** drop-down menu.
- e. Expand **Prod-Compute-Cluster-01 (2)**.

You might need to resize the columns to see the full name of the vSphere clusters.

- f. Verify that sa-esxi-04.vclass.local and sa-esxi-05.vclass.local are configured as transport nodes.
- g. Record the configuration and state of the sa-esxi-04.vclass.local host transport node in the Value column of this table in your student worksheet.

Host Transport Node Details for sa-esxi-04.vclass.local

Parameter	Value
Node status	
NSX configuration (state)	
OS type	
TEP IP address	
Manager Connectivity	
Controller Connectivity	
Transport Zones	

- i. Verify that the TEP IP address recorded here is from the IP range recorded in the previous task.
- h. Click the information icon next to the Up status to display additional information about the manager connectivity, controller connectivity, PNIC/bond status, and tunnel status.

The status should be Up for all components.

2. Verify the Edge Transport Nodes.
 - a. From the NSX UI, select **System > Fabric > Nodes > Edge Transport Nodes**.
 - b. Find sa-nsxedge-01.

- c. Record the configuration and state of sa-nsxedge-01 in the Value column of this table in your student worksheet.

Edge Transport Node Configuration Details for sa-nsxedge-01

Parameter	Value
Node status	
Configuration state	
TEP IP address	
Deployment type	
Manager connectivity	
Transport Zones	
Edge Cluster	

Task 4: Verify the Transport Node Preparation from the ESXi CLI

You use the native ESXi commands to query the list of NSX-T Data Center packages and modules installed on the ESXi host. You also retrieve the configuration information of the IP addresses, TEP, and NSX-T Data Center modules.

1. Open MTPuTTY from the taskbar and double-click **SA-ESXi-04** from the *Production – Infrastructure* folder.
2. Use the relevant information from various command outputs to record the details for ESXi host sa-esxi-04 in the Value column of this table in your student worksheet.

The substeps include the commands that must be run.

NSX-T Data Center Configuration Details of the sa-esxi-04 host

Parameter	Value
nsx-proxy vib acceptance level	
Status of the nsxt-vswitch kernel module	
vmk10 IPv4 address	
vmk50 IPv4 address	

- a. List the NSX-T Data Center packages installed on ESXi.

```
[root@sa-esxi-04:~] esxcli software vib list | egrep "Name|nsx|vsip"
```
- b. List the kernel modules installed on ESXi.

```
[root@sa-esxi-04:~] esxcli system module list | egrep "Name|nsx"
```
- c. List the VMkernel IPv4 address list.

```
[root@sa-esxi-04:~] esxcli network ip interface ipv4 address list
```
3. List the TCP/IP stacks available on the transport node.

```
[root@sa-esxi-04:~] esxcli network ip netstack list
```

 - a. Verify that the VXLAN and hyperbus interfaces exist.
4. List the vSwitches available on the ESXi transport host.

```
[root@sa-esxi-04:~] esxcfg-vswitch -l
```

 - a. Verify that Prod-Overlay-NVDS is configured with Uplinks vmnic5 and vmnic4.
5. Query the NSX-Proxy agent service status.

```
[root@sa-esxi-04:~] /etc/init.d/nsx-proxy status
```

 - a. Verify that the status of nsx-proxy is running.
6. Query network connections between the ESXi host and the NSX Management plane.

```
[root@sa-esxi-04:~] esxcli network ip connection list | grep 1234
```

 - a. Verify that open and ESTABLISHED connections exist between the ESXi host and the NSX Management plane on port 1234.
7. Query network connections between the ESXi host and the NSX Control plane.

```
[root@sa-esxi-04:~] esxcli network ip connection list | grep 1235
```

 - a. Verify that open and ESTABLISHED connections exist between the ESXi host and the NSX Control plane on port 1235.

Task 5: Verify the Transport Node Preparation from the KVM CLI

You query the NSX-T Data Center packages and NSX Managed Virtual Distributed Switch (N-VDS) configuration from the command line.

1. Open MTPuTTY from the taskbar and double-click **SA-KVM-02** in the Production - Infrastructure folder.
2. At the SA-KVM-02 VM command line, switch the user to root.

```
vmware@sa-kvm-02:~$ sudo -i
```
3. Use the relevant information from various command outputs to record the details for the sa-kvm-02 Kernel-based Virtual Machine (KVM) host in the Value column of this table in your student worksheet.

The substeps include the commands that must be run.

NSX-T Data Center Configuration Details of KVM host sa-kvm-02

Parameter	Value
Architecture of the NSX agent package	
IP address of the nsx-vtep0.0 network interface	
Name of the Open vSwitch bridge with the hyperbus port	

- a. List the NSX-T Data Center packages installed on the Ubuntu KVM host.

```
root@sa-kvm-02:~# dpkg --get-architecture | egrep "Name|nsx"
```
 - b. Run the `ifconfig` command to list the interfaces to verify the interfaces from the KVM command line.

```
root@sa-kvm-02:~# ifconfig
```

The IPv4 address of the nsx-vtep0.0 interface was created when the Ubuntu KVM host was configured as a transport node.
 - c. Query the Open vSwitch configuration.

```
root@sa-kvm-02:~# ovs-vsctl show
```

The command output lists the bridges named `nsx-managed` and `nsx-switch.0` that were configured during the transport node preparation.
4. Query the NSX-Proxy agent service status.

```
root@sa-kvm-02:~# service nsx-proxy status
```
 5. Verify that the status of NSX proxy is running.

6. Verify that the Ubuntu KVM host and the NSX Management plane are connected.
 - a. Run the `netstat -nap | grep 1234` command.


```
root@sa-kvm-02:~# netstat -nap | grep 1234
```
 - b. Verify that open and ESTABLISHED connections exist between the KVM host and NSX Management plane on port 1234.
7. Verify that the Ubuntu KVM host and the NSX Control plane are connected.
 - a. Run the `netstat -nap | grep 1235` command.


```
root@sa-kvm-02:~# netstat -nap | grep 1235
```
 - b. Verify that open and ESTABLISHED connections exist between the KVM host and NSX Control plane on port 1235.

Task 6: Verify the NSX Edge Configuration from the NSX CLI

You log in to the sa-nsxedge-01 NSX Edge node to query the information from the NSX CLI.

1. Open MTPuTTY and double-click **sa-nsxedge-01** in the Production NSX Inventory folder.
2. Use the relevant information from various command outputs to record the details for NSX Edge sa-nsxedge-01 in the Value column of this table in your student worksheet. The substeps include the commands that must be run.

Selected Configuration Details of the sa-nsxedge-01 NSX Edge node

Parameter	Value
Minimum password length	
Node UUID	
Name of the network interfaces used to carry VM traffic	
Channel used to connect to NSX-Manager	
Physical port of the Prod-VLAN-NVDS host switch	
Local VTEP IP of the Prod-Overlay-NVDS host switch	
Encapsulation type used on all tunnel ports	

- a. Display the configuration information about the NSX Edge node.
`sa-nsxedge-01> get configuration`
- b. Display the node UUID.
`sa-nsxedge-01> get node-uuid`
- c. List the interfaces and the capabilities of the NICs.
`sa-nsxedge-01> get interfaces`
- d. Query which NSX Manager instance is managing this NSX Edge node.
`sa-nsxedge-01> get managers`
- e. Display the host switches (N-VDS) installed on the NSX Edge node.
`sa-nsxedge-01> get host-switches`
- f. List the tunnel ports.
`sa-nsxedge-01> get tunnel-ports`
- g. List the VTEPs.
`sa-nsxedge-01> get vteps`

Lab 6 NSX Infrastructure

Preparation Break-Fix Scenario 1

Objective and Tasks

Identify, diagnose, and resolve an infrastructure preparation problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify That the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the future course of action.

1. Read the scenario description.

A junior colleague tried to add the sa-esxi-12 ESXi host as a host transport node to the staging environment. The addition failed and your colleague has asked for your assistance.

You assist your colleague to get NSX configured on the ESXi host.

At the end of this lab, the sa-esxi-12 host must display a successful configuration status in the NSX UI.

2. Review details about the lab environment and the course of action.
 - The sa-esxi-12 host is already deployed and running in vCenter Server under Staging-Cluster-02 cluster in the Datacenter-02-Non-Production data center.
 - The sa-esxi-12 host is added to MTPuTTY under the Non-Production - Infrastructure folder.
 - The fully qualified domain name (FQDN) of the ESXi host is sa-esxi-12.vclass.local.
 - The IP address of the ESXi host is 172.20.10.73.
 - Credentials for the ESXi host:
 - User name: root
 - Password: VMware1!
 - The node switch should use the following configuration settings:
 - Transport zone: STG-Overlay-TZ
 - Uplink profile: ESXi-Host-Uplink-Profile
 - IP assignment: TEP-IP-Pool
 - Teaming Policy Switch Mapping: Active > vmnic4, Standby > vmnic5
- Use the default values for all the other settings.

Task 2: Confirm the Problem

You confirm a problem that was reported by your colleague: Adding the sa-esxi-12.vclass.local host transport node failed.

1. In Chrome, click the **NSX-T Datacenter > NSX Manager (Non Prod)** bookmark.
2. Log in to NSX Manager by entering **admin** as the user name and **VMware1!VMware1!** as the password.
3. From the NSX UI, click **System > Fabric > Nodes** and click the **Host Transport Nodes** tab.
4. From the **Managed by** drop-down menu, select **None: Standalone Hosts**. Ignore the status of the already added transport nodes, these problems will be fixed in later labs.
5. Click **Add** and add sa-esxi-12.vclass.local as a new transport node.

Use the configuration details provided from the scenario in the Add Transport Node wizard.

6. Verify the configuration status of sa-esxi-12.vclass.local.

The Configuration State appears as NSX Install Failed.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem .

1. Use the available techniques and tools to troubleshoot and fix the problem.

- Lecture manual for this course
- Lab environment worksheet
- NSX Manager and ESXi host log files
- VMware knowledge base articles at <http://kb.vmware.com>
- Other online technical resources

2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the sa-esxi-12.vclass.local host transport node is successfully configured for NSX.

1. In Chrome, select the **Breakfix labs** bookmarks folder and click **NSX Manager**.
2. Log in to NSX Manager by entering **admin** as the user name and **VMware1!VMware1!** as the password.
3. From the NSX UI, click the **System > Fabric > Nodes > Host Transport Nodes** tab.
4. From the **Managed by** drop-down menu, select **None: Standalone Hosts**.
5. Verify the configuration status of sa-esxi-12.vclass.local.

The configuration state appears as Success.

Lab 7 NSX Infrastructure Preparation

Break-Fix Scenario 2

Objective and Tasks

Identify, diagnose, and resolve an infrastructure preparation problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify that the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

Your colleague has manually deployed a virtual machine to be used as an NSX Edge in the Staging environment. You must add and configure this virtual machine as an NSX Edge transport node.

NOTE

Do not deploy a new NSX Edge node. You must add the NSX Edge node that is already deployed.

At the end of this lab, the following requirements must be met:

- The sa-nsxedge-11 host must display a successful configuration status in the NSX UI.
- You must be able to ping the TEP IP of the edge transport node.

2. Review details about the lab environment and the course of action.
 - The sa-nsxedge-11 edge VM is already deployed and running in the vCenter Server inventory under the Management-Edge-Cluster-02 cluster in the Datacenter-02-Non-Production data center.
 - The sa-nsxedge-11 edge VM is added to MTPuTTY under the Non-Production - Infrastructure folder.
 - The fully qualified domain name (FQDN) of the edge VM is sa-nsxedge-11.vclass.local.
 - The IP address of the edge VM is 172.20.10.111.
 - Credentials of the edge VM:
 - User name: admin
 - Password: VMware1!VMware1!
 - The node switch should use the following configuration settings:
 - Transport zone: STG-Overlay-TZ
 - Uplink profile: nsx-edge-single-nic-uplink-profile
 - IP assignment: IP Pool TEP-IP-Pool
 - Active uplink: fp-eth0
- Use the default values for all the other settings.

Task 2: Confirm the Problem

You confirm that sa-nsxedge-11 is not added to NSX as an edge transport node.

1. In Chrome, select the **NSX-T Data Center** bookmarks folder and click **NSX Manager (Non-Prod)**.
2. Log in to NSX Manager by entering **admin** as the user name and **VMware1!VMware1!** as the password .
3. From the NSX UI, click the **System > Fabric > Nodes > Edge Transport Nodes** tab.
4. Verify that the sa-nsxedge-11 edge node is not configured as an edge transport node in NSX-T Data Center.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem.

1. Use the available techniques and tools to troubleshoot and fix the problem.
 - Lecture manual for this course
 - Lab environment worksheet
 - NSX Manager and ESXi host log files
 - VMware knowledge base articles at <http://kb.vmware.com>
 - Other online technical resources
2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the sa-nsxedge-11 edge transport node is successfully configured for NSX.

1. In Chrome, select the **Breakfix labs** bookmarks folder and click **NSX Manager**.
2. Log in to NSX Manager by entering **admin** as the user name and **VMware1!VMware1!** as the password .
3. From the NSX UI, click the **System > Fabric > Nodes > Edge Transport Nodes** tab.
4. Verify the configuration status of sa-nsxedge-11.

The configuration state appears as Success.

5. From the TEP IP Addresses column, record the TEP IP of sa-nsxedge-11. _____
6. Use the TEP IP that you recorded to ping , from the student desktop, to the TEP IP address of sa-nsxedge-11.

The ping receives a successful reply.

Lab 8 NSX Infrastructure Preparation Challenge Scenario

Objective and Tasks

Identify, diagnose, and resolve an infrastructure preparation problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify that the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

A junior colleague tried to add the sa-kvm-03 Ubuntu Kernel-based Virtual Machine (KVM) host as a host transport node to the Staging environment. Adding the node failed and your colleague asked for your assistance.

You assist your colleague to configure NSX on the KVM host.

At the end of this lab, a successful configuration status must appear for the sa-kvm-03 host in the NSX UI.

2. Review details about the lab environment and the course of action.
 - The sa-kvm-03 host is already deployed. vCenter Server does not manage this host.
 - The sa-kvm-03 host is added to MTPuTTY under the Non-Production - Infrastructure folder.
 - The sa-kvm-03 node is of the Ubuntu KVM type.
 - The FQDN of the KVM host is sa-kvm-03.vclass.local.
 - The IP address of the KVM host is 172.20.10.153.
 - Credentials of the KVM host:
 - User name: vmware
 - Password: VMware1!
 - The node switch should use the following configuration settings:
 - Transport zone: STG-Overlay-TZ
 - Uplink profile: nsx-default-uplink-hostswitch-profile
 - IP assignment: IP Pool TEP-IP-Pool
 - Teaming policy switch mapping: Active > eth2, Standby > eth3
- Use the default values for all the other settings.

Task 2: Confirm the Problem

You confirm a problem that was reported by your colleague: Adding the sa-kvm-03.vclass.local host transport node failed.

1. In Chrome, select the **NSX-T Data Center** bookmarks folder and click **NSX Manager (Non-Prod)**.
2. Log in to NSX Manager by entering **admin** as the user name and **VMware1!VMware1!** as the password.
3. From the NSX UI, click the **System > Fabric > Nodes > Host Transport Nodes** tab.
4. From the **Managed by** drop-down menu, select **None: Standalone Hosts**.
5. Click **ADD** to add sa-kvm-03.vclass.local as a new transport node.

You can use the configuration details from the scenario description in the Add Transport Node wizard.

6. Verify the configuration state of sa-kvm-03.vclass.local.

The status appears as NSX Install Failed.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem.

1. Use the available techniques and tools to troubleshoot and fix the problem.
 - Lecture manual for this course
 - Lab environment worksheet
 - NSX Manager and ESXi host log files
 - VMware knowledge base articles at <http://kb.vmware.com>
 - Other online technical resources
2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the sa-kvm-03.vclass.local host transport node is successfully configured for NSX.

1. In Chrome, select the **NSX-T Data Center** bookmarks folder and click **NSX Manager (Non-Prod)**.
2. Log in to NSX Manager by entering **admin** as the user name and **VMware1!VMware1!** as the password.
3. From the NSX UI, click the **System > Fabric > Nodes > Host Transport Nodes** tab.
4. From the **Managed by** drop-down menu, select **None: Standalone Hosts**.
5. Verify the configuration status of sa-kvm-03.vclass.local.

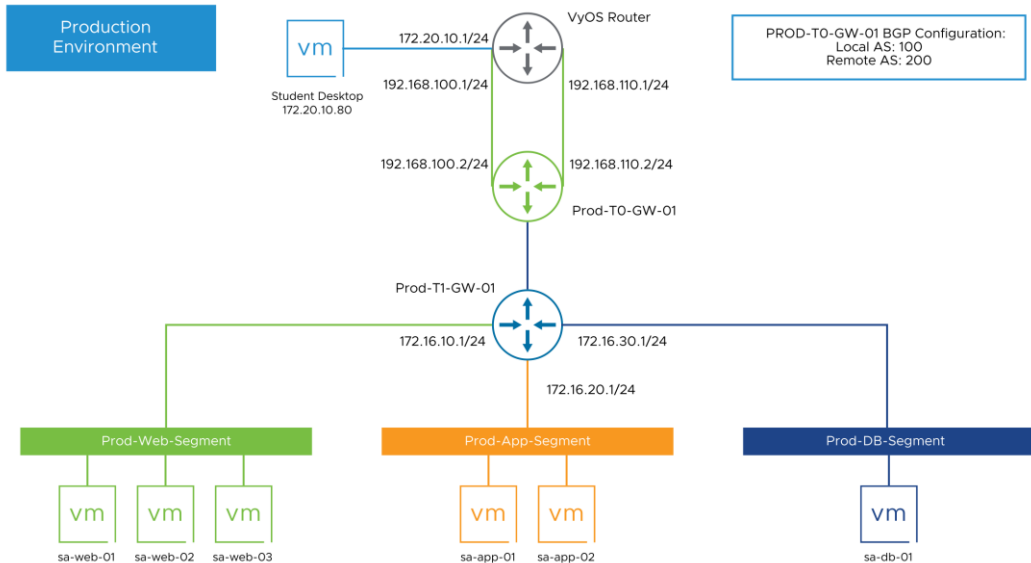
The configuration state appears as Success.

Lab 9 Logical Switching Verification

Objective and Tasks

Verify logical switches from the UI and the CLI:

1. Prepare for the Lab
2. Verify Segments from the NSX UI
3. Verify Logical Switches from the NSX CLI
4. Verify Logical Switches from the ESXi CLI
5. Verify Logical Switches from the KVM CLI



Task 1: Prepare for the Lab

You log in to the vSphere Client UI and the NSX UI.

1. From your student desktop, log in to the vSphere Client UI.
 - a. Open Chrome.
 - b. Click the **vSphere Site-A > vSphere Client (SA-VCSA-01)** bookmark.
 - c. On the login page, enter the **administrator@vsphere.local** as the user name and the **VMware1!** as the password.
2. Log in to the NSX UI.
 - a. Open another tab in Chrome.
 - b. Click the **NSX-T Data Center > NSX Manager (Prod)** bookmark.
 - c. On the login page, enter the **admin** as the user name and the **VMware1!VMware1!** as the password .
3. Open MTPuTTY and open an SSH session to the sa-kvm-01 host.
 - a. Verify that sa-db-01 is powered on.

```
$ sudo virsh list --all
```

You powered on sa-db-01 in an earlier lab.
 - b. if necessary, power-on the sa-db-01 VM.

```
$ sudo virsh start sa-db-01
```
4. In MTPuTTY, open an SSH session to the sa-kvm-02 host.
 - a. Power on the sa-web-03 VM.

```
$ sudo virsh start sa-web-03
```
 - b. Verify that the sa-web-03 VM is powered on.

```
$ sudo virsh list --all
```

Task 2: Verify Segments from the NSX UI

You verify the status of the Prod-Web-Segment segment from the NSX UI.

1. From the NSX UI, navigate to **Networking > Segments**.
2. Find the Prod-Web-Segment segment and verify that its status is Success.

Task 3: Verify Logical Switches from the NSX CLI

You run the `nsxcli` commands to retrieve the configuration of the Prod-Web-Segment logical switch.

1. Open MTPuTTY from the taskbar and click the **sa-nsxmgr-01** tab.
2. Query the logical switches configured in NSX Manager.
 - a. Run the `get logical-switches` command.

```
sa-nsxmgr-01> get logical-switches
```

The VNI, UUID, name, and type of the segment appear.
 - b. Record the logical switch VNI and UUID of Prod-Web-Segment in the Value column of this table in your student worksheet.

You use these details in the upcoming lab tasks.

Segment Configuration Details for Prod-Web-Segment

Parameter	Value
Name	Prod-Web-Segment
VNI	
UUID	
Type	

NOTE

The command output displays that multiple logical switches were created, including the Prod-Web-Segment logical switch. These preconfigured logical switches are part of the topology and will be used in later labs.

3. Query the logical switch ports connected to Prod-Web-Segment.

```
get logical-switch <Prod-Web-Segment-UUID> ports
```

Replace <Prod-Web-Segment-UUID> with the Prod-Web-Segment UUID that you recorded.

Example: sa-nsxmgr-01> get logical-switch 5a17d7e8-f64d-4130-8ebe-e391faf30027 ports

NOTE

To query the ports configured on the segment, you must use the UUID of the segment. Do not use the VNI.

4. List the transport node table of the Prod-Web-Segment logical switch.

```
sa-nsxmgr-01> get logical-switch <Prod-Web-Segment-VNI>  
transport-node-table
```

Example: sa-nsxmgr-01> get logical-switch 69632 transport-node-table

The command output shows the list of transport nodes that Prod-Web-Segment spans across the transport zone. The transport nodes are only visible in this output when at least one powered-on VM is connected to the logical switch.

NOTE

You can also use the UUID of the segment to query the transport node table.

Example: sa-nsxmgr-01> get logical-switch <Prod-Web-Segment-UUID> transport-node-table

5. Generate traffic (ping) from the sa-web-01 VM.
- a. From the vSphere Client, select **sa-web-01** and click **Launch Web Console** in the right pane.
 - b. If needed, log in to the sa-web-01 VM.
 - User name: root
 - Password: VMware!l
 - c. Initiate a series of pings from the sa-web-01 VM to the sa-web-02 and sa-web-03 VMs.

```
sa-web-01:~# ping -c 2 172.16.10.12
```

```
sa-web-01:~# ping -c 2 172.16.10.13
```

6. Use the relevant information from various command outputs to record the details in the Value column of this table in your student worksheet.

The substeps include the commands that must be run.

Verify Logical Switches from NSX Manager CLI

Switch Table	Entry	Value
arp-table	MAC of sa-web-01 (172.16.10.11)	
mac-table	VTEP-IP associated with sa- web-01 MAC	
mac-table	VTEP-IP associated with sa- web-02 MAC	
vtep	TransportNode-ID associated with sa-web-01	

- a. Click the **sa-nsxmgr-01** tab in MTPuTTY and query the arp-table.

```
sa-nsxmgr-01> get logical-switch <Prod-Web-Segment-VNI>  
arp-table
```

Example: sa-nsxmgr-01> get logical-switch 69632 arp-table

The VNI of the Prod-Web-Segment, IP address and MAC address of the VMs, and the UUIDs of the transport node where VMs are running appear.
- b. From the arp-table output, record the MAC address of the sa-web-01 virtual machine (IP 172.16.10.11) in the table.

- c. List the mac-table of the Prod-Web-Segment segment.

```
sa-nsxmgr-01> get logical-switch <Prod-Web-Segment-VNI>  
mac-table
```

Example: sa-nsxmgr-01> get logical-switch 69632 mac-table

The VNI of logical switches, VM MAC address, TEP IP, and UUID of the transport nodes appear.

- d. From the mac-table output, record the VTEP-IP associated with the MAC address of the sa-web-01 virtual machine in the table.
- e. List the tep-table of a Prod-Web-Segment logical switch.

```
sa-nsxmgr-01> get logical-switch <Prod-Web-Segment-VNI>  
vtep
```

Example: sa-nsxmgr-01> get logical-switch 69632 vtep

The vtep label (in hexadecimal), IP address, MAC address, UUIDs of the transport nodes, and TEP encapsulation details appear.

- f. From the output of the vtep table, record the transport node ID associated with the sa-web-01 virtual machine in the table.

- 7. Display names of the transport nodes.

```
sa-nsxmgr-01> get nodes
```

You can use the output to identify the transport node on which the sa-web-01 virtual machine is running.

Task 4: Verify Logical Switches from the ESXi CLI

You use the `nsxcli` command line on the `sa-esxi-04` host to retrieve the configuration of the Prod-Web-Segment logical switch.

1. Open MTPuTTY from the taskbar and click the **SA-ESXi-04** tab.
2. If you are in the root privileged mode, run the `nsxcli` command to enter the `nsxcli` command line.

```
[root@sa-esxi-04:~] nsxcli
```

3. Query the logical-switches seen on the ESXi host.

```
sa-esxi-04.vclass.local> get logical-switches
```

This command lists the VNI, logical switch UUID, DVS name, and VIF numbers.

4. From the command output, verify the VNI and UUID of the Prod-Web-Segment logical switch to verify the realization of the Prod-Web-Segment logical switch on ESXi.

You recorded the VNI and UUID of the Prod-Web-Segment logical switch in a previous task.

5. Query information about the Prod-Web-Segment segment.

```
sa-esxi-04.vclass.local> get logical-switch <Prod-Web-Segment-VNI>
```

The segment configuration, including replication mode, ARP and Multicast proxy status, transport binding, VLAN ID, and Admin state appear.

Example: `sa-esxi-04.vclass.local> get logical-switch 69632`

6. Record configuration details for Prod-Web-Segment in the Value column of this table in your student worksheet.

Prod-Web-Segment Logical Switch Configuration Details

Parameter	Value
DVS name	
Controller IP	
Replication mode	
Transport binding	

7. Initiate pings from the sa-web-01 VM.
 - a. From vSphere Web Client, select **sa-web-01** and click **Launch Web Console** in the right pane.
 - b. If needed, log in to the sa-web-01 VM.
 - User name: root
 - Password: VMware!l
 - c. Initiate a series of pings from the sa-web-01 VM (172.16.10.11) to the sa-web-02 and sa-web-03 VMs.

```
sa-web-01:~# ping -c 2 172.16.10.12
```

```
sa-web-01:~# ping -c 2 172.16.10.13
```

8. Use the relevant information from various command outputs to record the details in the Value column of this table in your student worksheet.

The substeps include the commands that must be run.

Verify Logical Switches from ESXi CLI

Switch Table	Entry	Value
arp-table	MAC of sa-web-02 (172.16.10.12)	
mac-table	VTEP IP (outer IP) used for sa-web-02 traffic	
vtep-table	VTEP Label of VTEP IP used for sa-web-02	

- a. Click the **SA-ESXi-04** tab in MTPuTTY and query the arp-table.


```
sa-esxi-04.vclass.local> get logical-switch <Prod-Web-Segment-VNI> arp-table
```

Example: sa-esxi-04.vclass.local> get logical-switch 69632 arp-table

The IP address and MAC addresses of the VMs that are connected to the Prod-Web-Segment segment appear.
- b. From the arp-table output, record the MAC address of the sa-web-02 virtual machine (IP address 172.16.10.12) in the table.

- c. Query the mac-table of the Prod-Web-Segment segment.

```
sa-esxi-04.vclass.local> get logical-switch <Prod-Web-Segment-VNI> mac-table
```

The inner MAC, outer MAC, outer IP, and flags appear.

```
Example: sa-esxi-04.vclass.local> get logical-switch 69632 mac-table
```

- d. From the mac-table output, record the VTEP IP address associated with the sa-web-02 virtual machine in the table.

- i. Verify that the sa-web-02 VTEP IP (outer IP) recorded here matches the value recorded, in the previous task, from NSX manager.

- e. Query the vtep-table of the Prod-Web-Segment logical switch.

```
sa-esxi-04.vclass.local> get logical-switch <Prod-Web-Segment-VNI> vtep-table
```

The IP and MAC of TEP, segment ID, Is MTEP (True/False), and BFD count appear.

```
Example: sa-esxi-04.vclass.local> get logical-switch 69632 vtep-table
```

- f. From the vtep-table output, record the VTEP label associated with sa-web-02 virtual machine in the table.

Task 5: Verify Logical Switches from the KVM CLI

You use the NSX CLI on the sa-kvm-02 host to retrieve the configuration of the Prod-Web-Segment logical switch.

1. Open MTPuTTY from the taskbar and click the **SA-KVM-02** tab.
2. At the SA-KVM-02 VM command line, change the user to root.

```
vmware@sa-kvm-02:~$ sudo -i
```

3. Retrieve the interfaceid of the sa-web-03 virtual machine from the virtual machine configuration:

```
root@sa-kvm-02:~# virsh dumpxml sa-web-03 | grep interfaceid
```

Record the interfaceid for later: _____

4. Run the nsxcli command to enter the nsxcli command line.

```
root@sa-kvm-02:~# nsxcli
```

5. Query the logical switches realized on the KVM host.

```
sa-kvm-02> get logical-switches
```

The logical switch UUID realized on KVM, VNI/VLAN ID, and the number of ports that are connected to the logical switch on that host appear.

6. Query the information about the Prod-Web-Segment segment.

```
sa-kvm-02> get logical-switch <Prod-Web-Segment-VNI>
```

The command output includes the segment UUID, VNI, replication mode, link status and VIF, MAC, ARP, and TEP counts.

Example: `sa-kvm-02> get logical-switch 69632`

7. Query the switch ports connected to the Prod-Web-Segment segment.

```
sa-kvm-02> get logical-switch <Prod-Web-Segment-VNI> ports
```

This command lists the port UUID to which the VM is connected, the port status, the VIF UUID, and snoop mode (ARP, DHCP) to learn the IP/MAC association.

Example: `sa-kvm-02> get logical-switch 69632 ports`

- a. Verify that the VIF UUID in the command output matches the interfaceid from the `virsh dumpxml` command recorded earlier in this task.
8. Initiate pings from the sa-web-01 VM.
 - a. Navigate to the sa-web-01 VM console.
 - b. If needed, log in to the sa-web-01 VM.
 - User name: root
 - Password: VMware!!
 - c. Initiate a series of pings from the sa-web-01 VM (172.16.10.11) to the sa-web-02 and sa-web-03 VMs.

```
sa-web-01:~# ping -c 2 172.16.10.12
sa-web-01:~# ping -c 2 172.16.10.13
```

9. Use the relevant information from various command outputs to record the details in the Value column of this table in your student worksheet.

The substeps include the commands that must be run.

Verify Logical Switches from KVM CLI

Switch Table	Entry	Value
arp-table	MAC of sa-web-01 (172.16.10.11)	
mac-table	VTEP Label used for sa- web-01 traffic	
vtep	VTEP IP used for sa-web-01 traffic	

- a. Click the **sa-kvm-02** tab in MTPuTTY and query the arp-table of the Prod-Web-Segment segment.

```
sa-kvm-02> get logical-switch <Prod-Web-Segment-VNI> arp-table
```

Example: sa-kvm-02> get logical-switch 69632 arp-table

- b. From the arp-table output, record the MAC of the sa-web-01 VM in the table.

- c. Query the mac-table of the Prod-Web-Segment segment.

```
sa-kvm-02> get logical-switch <Prod-Web-Segment-VNI> mac-table
```

The MAC address of the vNIC appears.

Example: sa-kvm-02> get logical-switch 69632 mac-table

- d. From the mac-table output, record the VTEP label used for the sa-web-01 traffic in the table.

- i. Verify that the sa-web-01 VTEP IP (outer IP) recorded here matches the value recorded, in the earlier task, from NSX manager.

- e. List the vtep-table of the Prod-Web-Segment logical switch.

```
sa-kvm-02> get logical-switch <Prod-Web-Segment-VNI> vtep
```

The label and TEP IP addresses appear.

Example: sa-kvm-02> get logical-switch 69632 vtep

- f. From the vtep-table output, record the VTEP IP used for the sa-web-01 traffic in the table.

Lab 10 Logical Switching Break-Fix Scenario 1

Objective and Tasks

Identify, diagnose, and resolve an NSX logical switch problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify that That the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

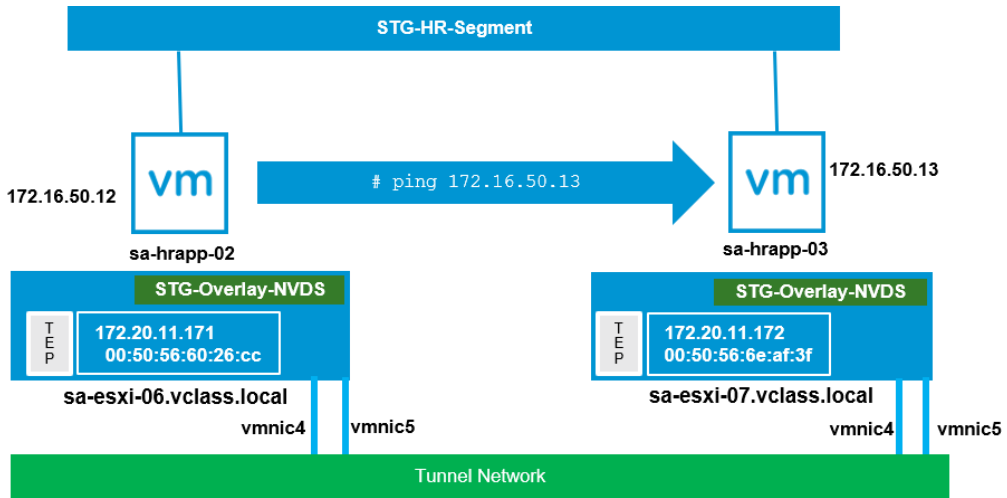
In an NSX environment, VMs connected to the same segment and residing on separate ESXi hosts cannot communicate with each other.

The sa-hrapp-02 VM runs on sa-esxi-06 and the sa-hrapp-03 VM runs on sa-esxi-07. Both VMs are connected to STG-HR-Segment.

You go to <https://sa-nsxvip-02.vclass.local/login.jsp?>, log in to the Non-Production NSX UI, and confirm and resolve the reported issue.

IMPORTANT

You cannot ping the VMs in STG-HR-Segment from outside the segment. This behavior is expected.



Task 2: Confirm the Problem

You confirm a problem that was reported by the help desk: Users cannot ping between the sa-hrapp-02 and sa-hrapp-03 VMs.

1. In Chrome, log in to vCenter Server with the vSphere Client.
2. Enter **administrator@vsphere.local** as the user name and **VMware1!** as the password .
3. Expand **Datacenter-02-Non-Production > Staging-Cluster-01 > STG-HR-APP** resource pool in vCenter inventory.
4. Open a console window to the sa-hrapp-02 VM.
 - a. Select **sa-hrapp-02** and from the Summary tab click **Launch Web Console**.
 - b. Log in by entering **root** as the user name and **VMware1!** as the password.
5. At the sa-hrapp-02 command prompt, ping the sa-hrapp-03 VM IP address.

ping -c 3 172.16.50.13

The ping must not be successful.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem.

1. Use the available techniques and tools to troubleshoot and fix the problem.
 - Lecture manual for this course
 - Lab environment worksheet
 - NSX Manager and ESXi host log files
 - VMware knowledge base at <http://kb.vmware.com>
 - Other online technical resources
2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the connectivity between the sa-hrapp-02 and sa-hrapp-03 servers is restored.

IMPORTANT

Do not continue to the next lab until the problem is fixed.

1. At the sa-hrapp-02 command prompt, test the connectivity.
`ping -c 3 172.16.50.13`

Lab 11 Logical Switching Break-Fix Scenario 2

Objective and Tasks

Identify, diagnose, and resolve an NSX logical switch problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify That the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

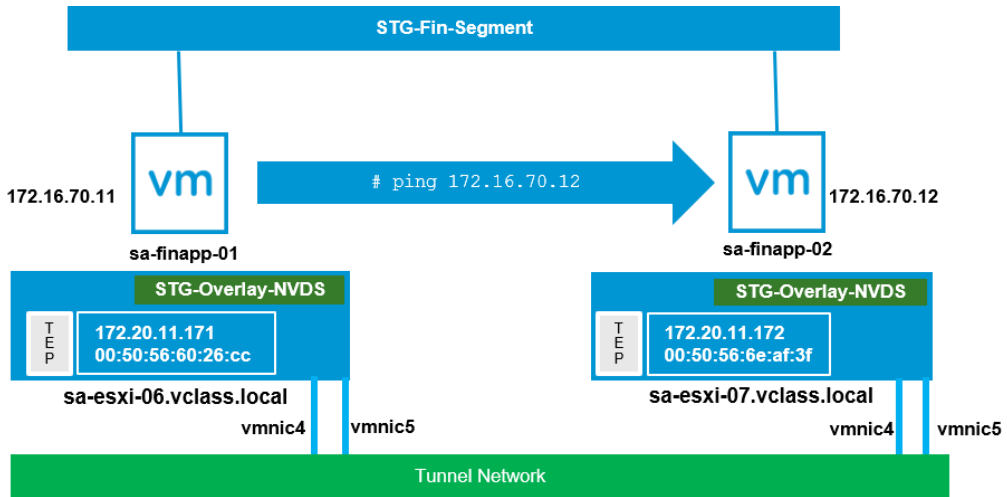
An NSX administrator applied a new security configuration at a segment port, which caused communication loss between several VMs.

The sa-finapp-01 and sa-finapp-02 VMs are unable to ping each other.

You go to <https://sa-nxvip-02.vclass.local/login.jsp?>, log in to the Non-Production NSX UI, and confirm and resolve the reported issue.

IMPORTANT

You cannot ping the VMs in the STG-FIN-Segment from outside the segment. This behavior is expected.



Task 2: Confirm the Problem

You confirm a problem that was reported by the help desk: VM sa-finapp-01 cannot communicate with VM sa-finapp-02. Pings between these VMs failed.

1. In Chrome, navigate to **vSphere Site-A > vSphere Client (SA-VCSA-01)**.
2. Log in to vCenter Server by entering **administrator@vsphere.local** as the user name and **VMware1!** as the password .
3. Expand the **Datacenter-02-Non-Production > Staging-Cluster-01 > STG-Fin-App-01** resource pool.
4. Select the **sa-finapp-01** VM and from the Summary tab, click **Launch Web Console**.
5. Log in to the VM by entering **root** as the user name and **VMware1!** as the password .
6. At the sa-finapp-01 command prompt, ping sa-finapp-02.

```
ping -c 3 172.16.70.12
```

The ping command must not be successful.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem.

1. Use the available techniques and tools to troubleshoot and fix the problem.
 - Lecture manual for this course
 - Lab environment worksheet
 - NSX Manager and ESXi host log files
 - VMware knowledge base articles at <http://kb.vmware.com>
 - Other online technical resources
2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the connectivity to the sa-finapp-02 VM from the sa-finapp-01 VM is restored.

1. At the sa-finapp-01 command prompt, test the connectivity.

```
ping -c 3 172.16.70.12
```

Lab 12 Logical Switching Challenge Scenario

Objective and Tasks

Identify, diagnose, and resolve a distributed firewall problem:

1. Problem Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify That the Problem Is Fixed

Task 1: Read the Scenario Description

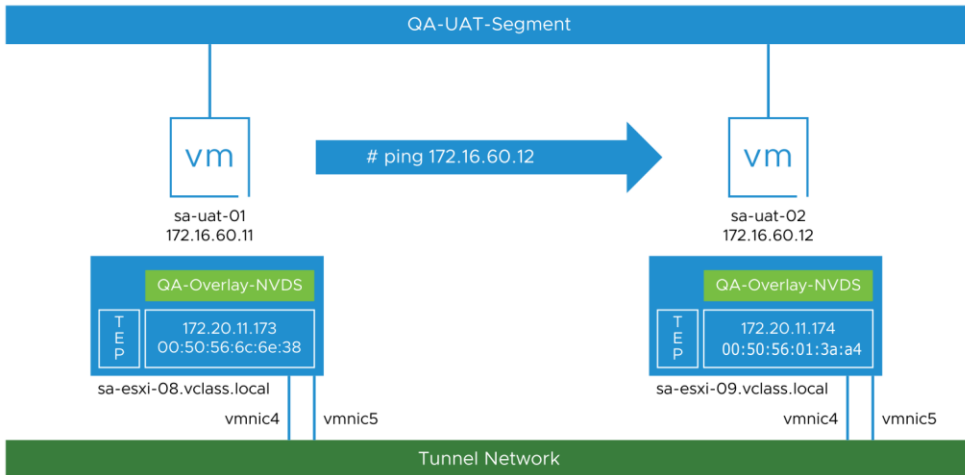
You read the scenario description and determine the course of action.

1. Read the scenario description.

You must troubleshoot and fix a problem reported to the help desk. Network connectivity does not exist between VMs in QA-UAT-Segment. The sa-uat-01 VM runs on the sa-esxi-08 host and the sa-uat-02 VM runs on the sa-esxi-09 host. The VMs cannot ping each other.

IMPORTANT

You cannot ping the VMs in QA-UAT-Segment from outside the segment. This behavior is expected.



Task 2: Confirm the Problem

You confirm a problem that was reported by the help desk: Network connectivity is not working between the sa-uat-01 and sa-uat-02 VMs.

1. In Chrome, log in to the vCenter Server with the vSphere Client.
2. Enter **administrator@vsphere.local** as the username and **VMware1!** as the password.
3. Expand **Datacenter-02-Non-Prod > Dev-QA-Cluster-01 > QA-UAT** in the vCenter Server inventory.
4. Select the **sa-uat-01** VM from the right pane and click **Launch Web Console**.
5. Log in to the sa-uat-01 VM by entering **root** as the username and **VMware1!** as the password.
6. Test connectivity to sa-uat-02.

```
ping -c 3 172.16.60.12
```

The ping command must not be successful.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem.

1. Use the available techniques and tools to troubleshoot and fix the problem.
 - Lecture manual for this course
 - Lab environment worksheet
 - NSX Manager and ESXi host log files
 - VMware knowledge base articles at <http://kb.vmware.com>
 - Other online technical resources
2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the connectivity between the VMs in QA-UAT-Segment is restored.

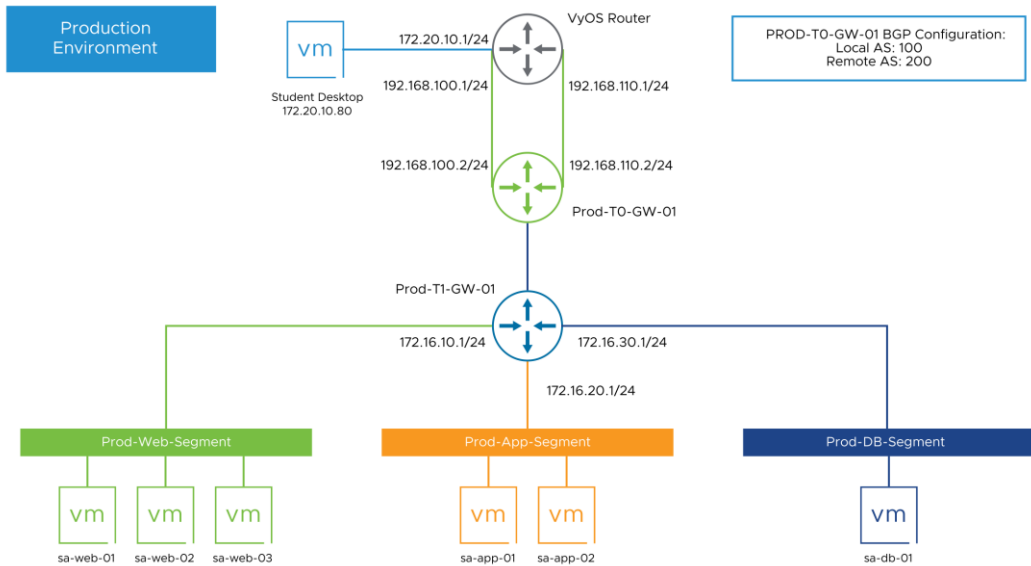
1. Open the sa-uat-01 VM console.
2. At the sa-uat-01 command prompt, test network connectivity to the sa-uat-02 VM.
`ping -c 3 172.16.60.12`

Lab 13 Logical Routing Verification

Objective and Tasks

Verify the logical router configuration from the UI and the CLI:

1. Prepare for the Lab
2. Verify the Tier-1 and Tier-0 Gateways from the NSX UI
3. Verify the Logical Routers from the NSX CLI on the NSX Manager Instance
4. Verify the Logical Routers from the NSX CLI on the ESXi Host
5. Verify the Logical Routers from the NSX CLI on the KVM Host
6. Verify the Logical Routers from the NSX CLI on the NSX Edge Node



Task 1: Prepare for the Lab

You log in to the NSX UI.

1. Log in to the NSX UI.
 - a. Open a tab in Chrome.
 - b. Select the **NSX-T Data Center > NSX Manager (Prod)** bookmark.
 - c. On the login page, enter **admin** as the user name and **VMware1!VMware1!** as the password.

Task 2: Verify the Tier-1 and Tier-0 Gateways from the NSX UI

You verify the status of the Tier-1 and Tier-0 gateways from the NSX UI.

1. From the NSX UI, navigate to **Networking > Tier-1 Gateways**.
2. Find the **Prod-T1-GW-01** gateway and verify that its status is Success.
3. Navigate to **Networking > Tier-0 Gateways**.
4. Find the **Prod-T0-GW-01** gateway and verify that its status is Success.

Task 3: Verify the Logical Routers from the NSX CLI on the NSX Manager Instance

You query the logical router configuration from the NSX command line on NSX Manager.

1. From MTPuTTY, open an SSH connection to sa-nxsmgr-01.
2. List the logical routers configured on NSX Manager.

```
sa-nxsmgr-01> get logical-routers
```

The logical router ID (in hexadecimal) , logical-router name, router type, cluster ID, and UUIDs appear.

3. Verify the configuration for the Prod-T0-GW-01 and Prod-T1-GW-01 gateways.
 - Prod-T1-GW-01 has one distributed router (DR) instance created.
 - Prod-T0-GW-01 has one distributed router (DR) instance and two service router (SR) instances created. Two SR instances are created because Prod-T0-GW-01 is configured to be in active-active high availability mode. Observe that the ClusterID is shared by both SR instances.

Additional Tier-0 and Tier-1 gateways are also created. These gateways are preconfigured as per the topology to facilitate upcoming lab tasks.

- Record the LR-ID and UUID of the SR and DR instances for the Prod-T0-GW-01 and Prod-T1-GW-01 gateways in the UUID column of this table in your student worksheet.

Logical Router UUIDs

Router-Type	LR-Name	LR-ID	UUID
Distributed Router Tier1	DR-Prod-T1-GW-01	0x_____	
Distributed Router Tier0	DR-Prod-T0-GW-01	0x_____	
Service Router Tier0	SR-Prod-T0-GW-01	0x_____	
Service Router Tier0	SR-Prod-T0-GW-01	0x_____	

You can use the `find` command with the LR-Name to limit the output to the logical router of interest.

```
Example: sa-nsxmgr-01> get logical-routers | find DR-Prod-T1
0x1801      DR-Prod-T1-GW-01
DISTRIBUTED_ROUTER_TIER1
8ce15a84-a572-43c2-b7a0-ff8c5e551448
```

- List the logical switches configured on the NSX Manager instance.

```
sa-nsxmgr-01> get logical-switches
```

The TRANSIT type logical switches that are used to connect:

- DR and SR of a Tier-0/Tier-1 gateway
- Tier-1 with Tier-0 gateways

Task 4: Verify the Logical Routers from the NSX CLI on the ESXi Host

You query logical router information from the NSX CLI on the ESXi host.

1. From MTPuTTY, open an SSH connection to SA-ESXi-05.
2. Enter the NSX command line.

```
[root@sa-esxi-05:~] nsxcli
```

3. List the logical routers present on this transport node.

```
sa-esxi-05.vclass.local> get logical-routers
```

The VDR UUID, LIF num, and route num information appear.

4. Use the UUIDs recorded from the NSX Manager instance to verify that the DR instances of Prod-T0-GW-01 and Prod-T1-GW-01 gateways are realized on the ESXi host.

The Tier-0 gateway distributed router (Prod-T0-GW-01) appears on the ESXi hosts only after the Tier-1 gateway (Prod-T1-GW-01) is connected to the Tier-0 gateway (Prod-T0-GW-01).

5. Query the Prod-T0-GW-01 distributed logical router information.

```
sa-esxi-05.vclass.local> get logical-router <DR-Prod-T0-GW-01-UUID>
```

Information about the logical router, such as LIF number, route number, state, and so on, appear.

```
Example: sa-esxi-05.vclass.local> get logical-router 152b6f28-b5de-4d69-9c1b-a4cdc01518bb
```

6. Query the LIF information of the Prod-T1-GW-01 distributed logical router.

```
sa-esxi-05.vclass.local> get logical-router <DR-Prod-T1-GW-01-UUID> interfaces
```

The LIF UUID, mode, overlay VNI, state, IP/mask, and so on appear

```
Example: sa-esxi-05.vclass.local> get logical-router 8ce15a84-a572-43c2-b7a0-ff8c5e551448 interfaces
```

7. Record the overlay/VNI, mode, IP/mask and MAC of each interface in this table in your student worksheet.

Prod-T1-GW-01 (Tier 1 DR) LIF Configuration Details

Overlay VNI	Mode	IP/Mask (IPv4)	MAC

- The LIFs in Routing mode are the connections to the segments
- The LIF in Routing-LinkLif mode is the connection to the Tier-0 gateway (Prod-T0-GW-01)
- The DR interfaces connecting to Segments has same MAC address.

8. List the logical switches information.

```
sa-esxi-05.vclass.local> get logical-switches
```

In addition to the segment logical switches, several system-created TRANSIT logical switches that are used to connect Tier-1-DR to Tier-0-DR appear.

a. Compare the VNIs with the Overlay VNIs that you recorded in the previous step.

9. Exit nsxcli and return to the root user command prompt.

```
sa-esxi-05.vclass.local> exit
```

10. List the logical routers on the ESXi host.

```
[root@sa-esxi-05:~] net-vdr -I --brief -l
```

The DR UUID and ID, number of LIFs, number of routes, state, and so on appear.

NOTE

This command is an alternative to the nsxcli `get logical-routers` command.

11. List the detailed LIF information about the Prod-T1-GW-01 distributed router.

```
[root@sa-esxi-05:~] net-vdr --lif --brief -l <DR-Prod-T1-GW-01-UUID>
```

Example: [root@sa-esxi-05:~] net-vdr --lif --brief -l 8ce15a84-a572-43c2-b7a0-ff8c5e551448

The LIFs in R-L and R modes appear.

The LIF with R-L mode is the linked port to connect the Tier-1 DR with the Tier-0 DR, and the LIF with R mode are the routing downlinks to the segments.

NOTE

This command is an alternative to the `nsxcli get logical-routers <UUID> interfaces` command.

12. List the detailed LIF information about the Prod-T0-GW-01 distributed router.

```
[root@sa-esxi-05:~] net-vdr --lif --brief -l <DR-Prod-T0-GW-01-UUID>
```

Example: [root@sa-esxi-05:~] net-vdr --lif --brief -l 152b6f28-b5de-4d69-9c1b-a4cdc01518bb

The DR UUID, LIF information, LIF ID, mode, state, IP/mask, MAC address, and LIF UUID information appear.

13. Record the overlay VNI, mode, and IP/mask (IPv4) in this table in your student worksheet.

Prod-T0-GW-01 (Tier 0 DR) LIF Configuration Details

Overlay VNI	Mode	IP/Mask (IPv4)
-------------	------	----------------

The command output displays the LIFs in R-L and R-B modes:

- The LIF with R-B mode is the Routing-Backplane (R-B) to connect the Tier-0 DR to the Tier-0 SR.
- The LIF with R-L mode is the linked port to connect the Tier-1 DR with the Tier-0 DR. Compare the Id and IP/mask on this side of the connection with the overlay/VNI and IP/mask recorded earlier on the Tier1 DR.

- The LIF with R,DL mode is the connection from the Tier-0 DR to the load balancer Tier-1 DR that is used in a later lab.

Task 5: Verify the Logical Routers from the NSX CLI on the KVM Host

You query the logical router information from the NSX CLI on KVM.

1. From MTPuTTY, open an SSH connection to SA-KVM-01.
2. At the SA-KVM-01 command line, switch the user to root.

```
vmware@sa-kvm-01:~$ sudo -i
```

3. Enter the NSX CLI.

```
root@sa-kvm-01:~# nsxcli
```

4. Query the logical routers.

```
sa-kvm-01> get logical-routers
```

NOTE

If the command returns an empty list, virtual machines are currently not running on this KVM transport node, and you must start the sa-db-01 virtual machine.

5. Verify that the router UUIDs are identical to those recorded in the earlier task that used NSX CLI on the NSX Manager Instance (sa-nxmgr-01).

6. Query the information about the Prod-T0-GW-01 logical router.

```
sa-kvm-01> get logical-router <DR-Prod-T0-GW-01 UUID>
```

This command lists the UUID, ID, and interfaces configured on the Tier-0 gateway.

Example: sa-kvm-01> get logical-router 152b6f28-b5de-4d69-9c1b-a4cdc01518bb

7. Query the information about the Prod-T1-GW-01 logical router.

```
sa-kvm-01> get logical-router <DR-Prod-T1-GW-01 UUID>
```

The UUID, ID, and interfaces configured on the Tier-1 gateway appear.

Example: sa-kvm-01> get logical-router 8ce15a84-a572-43c2-b7a0-ff8c5e551448

- Record the interface details of the Prod-T1-GW-01 logical router in the Value column of this table in your student worksheet.

Prod-T1-GW-01 (Tier 1 DR) Interface Details

Parameter	Value
Router ID	
Interface IP/Mask (Ipv4)	

- Compare the interface IPs with the IPs that you recorded in the previous task that used NSX CLI on the ESXi Host (sa-esxi-05)

Task 6: Verify the Logical Routers from the NSX CLI on the NSX Edge Nodes

You query the logical router information from the NSX CLI on the NSX Edge nodes.

- From MTPuTTY, open an SSH connection to the **sa-nsxedge-01** tab.
- List the logical routers.

```
sa-nsxedge-01> get logical-routers
```

The UUID, VRF, name, type, and so on of the logical routers appear.

- Record the UUID and VRF of the SR and DR logical routers in this table in your student worksheet.

Record of Logical Router UUIDs for nsx-edge-01

Type	Name	VRF	UUID
DISTRIBUTED_ROUTER_TIER1	DR-Prod-T1-GW-01		
DISTRIBUTED_ROUTER_TIER0	DR-Prod-T0-GW-01		
SERVICE_ROUTER_TIER0	SR-Prod-T0-GW-01		

- Verify that the router UUIDs are identical to the UUIDs that you recorded in the earlier task that used the NSX CLI on NSX Manager (sa-nsxmgr-01).

Only one of the active-active Tier-0 service routers appear on sa-nsxedge-01. The other service router resides on sa-nsxedge-02.

- Enter the vrf mode of the Tier-0 service router.

```
sa-nsxedge-01> vrf <VRF-ID-of-SR-Prod-T0-GW-01>
```

This command enters the VRF context mode of the logical router.

```
Example: sa-nsxedge-01> vrf 5
```

The vrf ID might be different in your lab environment.

- Display the summarized BGP neighbor information.

```
sa-nsxedge-01(tier0_sr)> get bgp neighbor summary
```

The router ID, local AS, neighbor IP, remote AS, state, and other details appear.

7. Record details about the SR-Prod-T0-GW-01 neighbors in this table in your student worksheet.

Neighbors of Router ID 192.168.100.2

Neighbor	AS	State

Two neighbors are available because the Tier-0 service router is configured with two uplinks to the upstream physical router. The neighbor in the established state is reversed on the other partner in the active-active service router running on sa-nsxedge-02.

8. Query the BGP neighbor.
 - a. Run the `sa-nsxedge-01(tier0_sr)> get bgp neighbor` command.
 - b. Press Ctrl+C or q to exit reviewing the neighbor details.

9. Display the routing table.

```
sa-nsxedge-01(tier0_sr)> get route
```

The list of routes learned from bgp, connected, ipv4, ipv6, nat, and static appear.

The following list of flags is used to categorize every learned route:

Flags:

```
t0c - Tier0-Connected, t0s - Tier0-Static, B - BGP,  
t0n - Tier0-NAT, t1s - Tier1-Static, t1c - Tier1-Connected,  
t1n: Tier1-NAT, t1l: Tier1-LB VIP, t1ls: Tier1-LB SNAT,  
t1d: Tier1-DNS FORWARDER, t1ipsec: Tier1-IPSec, isr: Inter-SR,  
> - selected route, * - FIB route
```

10. Display the directly connected routes.

```
sa-nsxedge-01(tier0_sr)> get route connected
```

11. Display the routes learned through BGP.

```
sa-nsxedge-01(tier0_sr)> get route bgp
```


- Record the gateway and interface used to reach the Prod-App-Segment (172.16.20.0/24) in this table in your student worksheet.

sa-nsxedge-01 BGP details for Prod-App-Segment (172.16.20.0/24)

Gateway	Interface
---------	-----------

- Display details of the logical router interfaces.

```
sa-nsxedge-01(tier0_sr)> get interfaces
```

- Record the name and UUID of the interface used to reach Prod-App-Segment (172.16.20.0/24) in this table in your student worksheet.

You recorded the interface used in a previous step.

sa-nsxedge-01 Interface Details for Prod-App-Segment

Name	Interface	UUID
------	-----------	------

- Display the logical routers forwarding table.

```
sa-nsxedge-01(tier0_sr)> get forwarding
```

The UUID of the service router, VRF ID, LR ID, logical router name and logical router type appear. The forwarding table displays the IP prefix, gateway IP, type, UUID of logical router interface/port, and gateway MAC address.

- Verify that the gateway IP and interface/port UUID for the Prod-App-Segment (172.16.20.0/24) are identical to those recorded earlier for the BGP route.

Lab 14 Logical Routing Break-Fix Scenario 1

Objective and Tasks

Identify, diagnose, and resolve an NSX logical routing problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify That the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

An NSX administrator reconfigured a Tier-1 gateway, and the VMs connected to its segments are unable to establish connectivity with an external network.

2. Review details about the issue and the course of action.

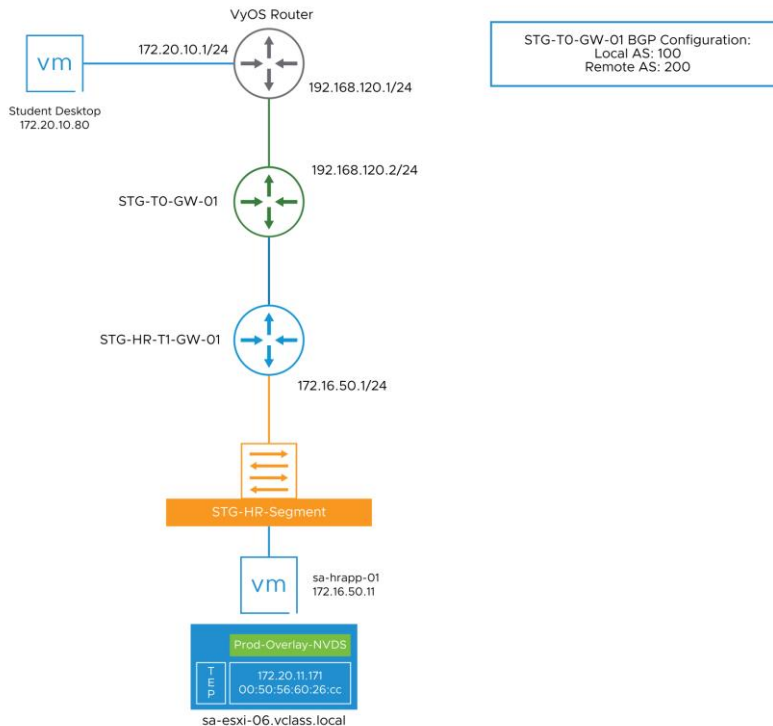
The following components are used in the scenario:

- STG-T0-GW-01 gateway
- STG-HR-T1-GW-01 gateway
- STG-HR-Segment segment
- sa-hrapp-01 VM (172.16.50.11) and student-desktop (172.20.10.80)

The communication between the sa-hrapp-01 VM and the student desktop failed after the reconfiguration of the STG-HR-T1-GW-01 gateway.

You go to <https://sa-nsxvip-02.vclass.local/login.jsp?>, log in to the Non-Production NSX UI, and confirm and resolve the reported issue.

At the end of the lab, sa-hrapp-01 VM (172.16.50.11) and student desktop (172.20.10.80) should ping each other.



Task 2: Confirm the Problem

You confirm a problem that was reported by the help desk: The sa-hrapp-01 VM cannot communicate with student desktop IP 172.20.10.80 and pings between these servers failed.

1. In Chrome, log in to vCenter Server with the vSphere Client.
2. Enter **administrator@vsphere.local** as the user name and **VMware1!** as the password .
3. Expand **Datacenter-02-Non-Production > Staging-Cluster-01 > STG-HR-App** in the vCenter Server inventory.
4. Select **sa-hrapp-01** and click **Open Web Console** on the **Summary** tab in the right pane.
5. Log in to the sa-hrapp-01 VM by entering **root** as the user name and **VMware1!** as the password.

6. At the command prompt, ping the student desktop IP address 172.20.10.80.

```
ping -c 3 172.20.10.80
```

The ping command must not be successful.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem.

1. Use the available techniques and tools to troubleshoot and fix the problem.

- Lecture manual for this course
- Lab environment worksheet
- NSX Manager and ESXi host log files
- VMware knowledge base articles at <http://kb.vmware.com>
- Other online technical resources

IMPORTANT

You must correct multiple misconfigurations to resolve the problem.

2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the connectivity to the student desktop is restored.

IMPORTANT

Do not continue to the next lab until the problem is fixed.

1. At the sa-hrapp-01 command prompt, test the connectivity.

```
ping -c 3 172.20.10.80
```

Lab 15 Logical Routing Break-Fix Scenario 2

Objective and Tasks

Identify, diagnose, and resolve an NSX logical routing problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify That the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

An NSX administrator reconfigured a BGP peer on a Tier-0 gateway, which resulted in network loss for VMs connected to a specific segment. These VMs are unable to establish connectivity with external services.

2. Review details about the issue and the course of action.

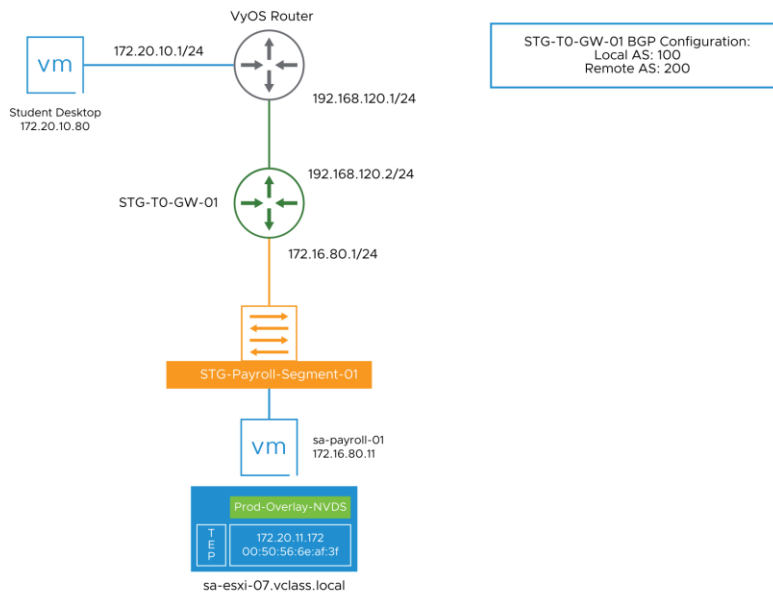
The following components are used in the scenario:

- STG-T0-GW-01 gateway
- STG-Payroll-Segment-01
- sa-payroll-01 VM (172.16.80.11) and student desktop (172.20.10.80)

The ping between the sa-payroll-01 VM and the student desktop failed.

You go to <https://sa-nsxvip-02.vclass.local/login.jsp?>, log in to the Non-Production NSX UI, and troubleshoot and fix this issue.

At the end of the lab, you must be able to establish a ping between sa-payroll-01 and the student desktop.



Task 2: Confirm the Problem

You confirm a problem that was reported by the help desk: The sa-payroll-01 VM cannot communicate with the student desktop. Pings between the sa-payroll-01 VM and the student desktop fail.

1. In Chrome, log in to vCenter Server with the vSphere Client.
2. Enter **administrator@vsphere.local** as the user name and **VMware1!** as the password.
3. Expand **Datacenter-02-Non-Production > Staging-Cluster-01 > STG-Payroll** in the vCenter Server inventory.
4. In the Navigator pane, select **sa-payroll-01** and click **Launch Web Console** in the right pane.
5. Log in to the sa-payroll-01 VM by entering **root** as the user name and **VMware1!** as the password.
6. At the command prompt, ping the student desktop.

```
ping -c 3 172.20.10.80
```

The ping command must not be successful.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem.

1. Use the available techniques and tools to troubleshoot and fix the problem.
 - Lecture manual for this course
 - Lab environment worksheet
 - NSX Manager and ESXi host log files
 - VMware knowledge base articles at <http://kb.vmware.com>
 - Other online technical resources
2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the connectivity to the sa-payroll-01 VM from the student desktop is restored.

IMPORTANT

Do not continue to the next lab until the problem is fixed.

1. At the sa-payroll-01 command prompt, test the connectivity.
`ping -c 3 172.20.10.80`

Lab 16 Logical Routing Break-Fix Scenario 3

Objective and Tasks

Identify, diagnose, and resolve an NSX logical routing problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify That the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

An NSX administrator added a new Tier-1 gateway for STG-Payroll-Segment-02, which resulted in network loss for VMs connected to the segment. These VMs are unable to establish connectivity with external services.

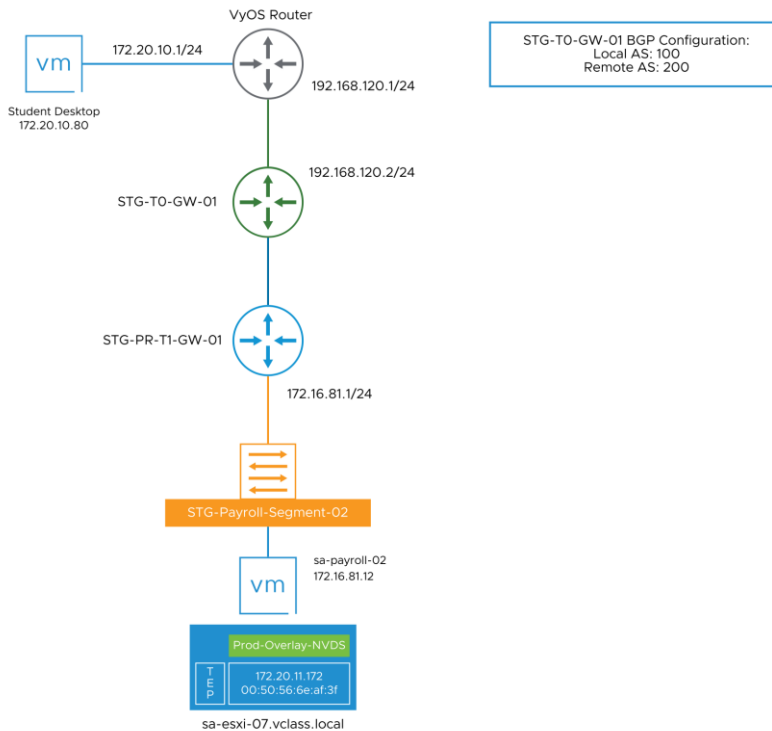
2. Review details about the issue and the course of action.

The following components are used in the scenario:

- STG-T0-GW-01 and STG-PR-T1-GW-01 gateways
- STG-Payroll-Segment-02
- sa-payroll-02 VM and student desktop (172.20.10.80)

The ping between the sa-payroll-02 VM and the student desktop failed.

You go to <https://sa-nsxvip-02.vclass.local/login.jsp?>, log in to the Non-Production NSX UI, and troubleshoot and fix this issue.



Task 2: Confirm the Problem

You confirm a problem that was reported by the help desk: The sa-payroll-02 VM cannot communicate with the student desktop. Pings between the sa-payroll-02 VM and the student desktop fail.

1. In Chrome, log in to vCenter Server with the vSphere Client.
2. Enter **administrator@vsphere.local** as the user name and **VMware1!** as the password .
3. Expand **Datacenter-02-Non-Production** > **Staging-Cluster-01** > **STG-Payroll** in the vCenter Server inventory.
4. In the Navigator pane, click **sa-payroll-02** and select **Launch Web Console** in the right pane.
5. Log in to the sa-payroll-02 VM by entering **root** as the user name and **VMware1!** as the password .

6. At the command prompt, ping the student desktop.

```
ping -c 3 172.20.10.80
```

The ping command must not be successful.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem.

1. Use the available techniques and tools to troubleshoot and fix the problem.

- Lecture manual for this course
- Lab environment worksheet
- NSX Manager and ESXi host log files
- VMware knowledge base articles at <http://kb.vmware.com>
- Other online technical resources

2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the connectivity to the sa-payroll-02 VM from the student desktop is restored.

1. At the sa-payroll-02 command prompt, test the connectivity.

```
ping -c 3 172.20.10.80
```

Lab 17 Logical Routing Challenge

Scenario 1

Objective and Tasks

Identify, diagnose, and resolve an NSX logical routing problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify That the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

Because of a planned maintenance activity, BGP peering with the upstream router IP 192.168.140.1 is down. IP 192.168.140.1 is directly connected through Tier-0 uplink 1. However, the alternate upstream router IP 192.168.150.1 is still accessible. Since the maintenance window started, none of the web servers are accessible from the student desktop despite Tier-0 being configured in active-standby mode with two uplinks.

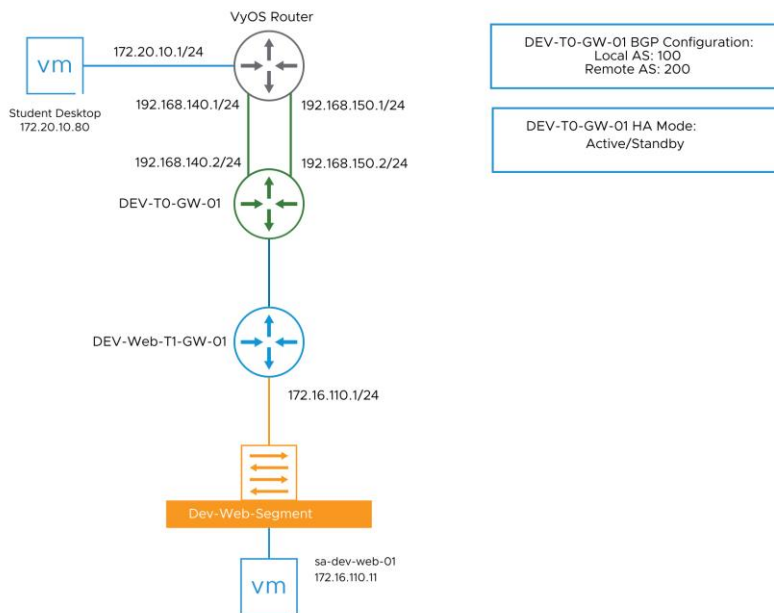
2. Review details about the issue and the course of action.

The following components are used in the scenario:

- DEV-TO-GW-01 and DEV-Web-T1-GW-01 gateways
- Dev-Web-Segment
- sa-devweb-01 VM and student desktop (172.20.10.80)

The ping between the sa-devweb-01 VM and the student desktop failed.

You go to <https://sa-nsxvip-02.vclass.local/login.jsp?>, log in to the NSX UI, and fix this issue.



Task 2: Confirm the Problem

You confirm a problem that was reported by the help desk: The sa-devweb-01 VM cannot communicate with the student desktop. Pings between the sa-devweb-01 VM and the student desktop fail.

1. In Chrome, log in to vCenter Server with the vSphere Client.
2. Enter **administrator@vsphere.local** as the user name and **VMware1!** as the password .
3. Expand **Datacenter-02-Non-Production > Dev-QA-Cluster-01 > Dev-Web** in the vCenter Server inventory.
4. In the Navigator pane, click **sa-devweb-01** and select **launch Web Console** on the **Summary** tab in the right pane.
5. Log in to the sa-devweb-01 VM by entering **root** as the username and **VMware1!** as the password .

6. At the command prompt, ping the student desktop.

```
ping -c 3 172.20.10.80
```

The ping command must not be successful.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem.

1. Use the available techniques and tools to troubleshoot and fix the problem.

- Lecture manual for this course
- Lab environment worksheet
- NSX Manager and ESXi host log files
- VMware knowledge base articles at <http://kb.vmware.com>
- Other online technical resources available

2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the connectivity to the student desktop from the sa-devweb-01 VM is restored.

1. At the sa-devweb-01 command prompt, test the connectivity.

```
ping -c 3 172.20.10.80
```

Lab 18 Logical Routing Challenge

Scenario 2

Objective and Tasks

Identify, diagnose, and resolve an NSX logical routing problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify That the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

After a recent configuration change, one of the DEV App servers can access the Internet while the other server cannot. Both DEV App servers can reach the student desktop.

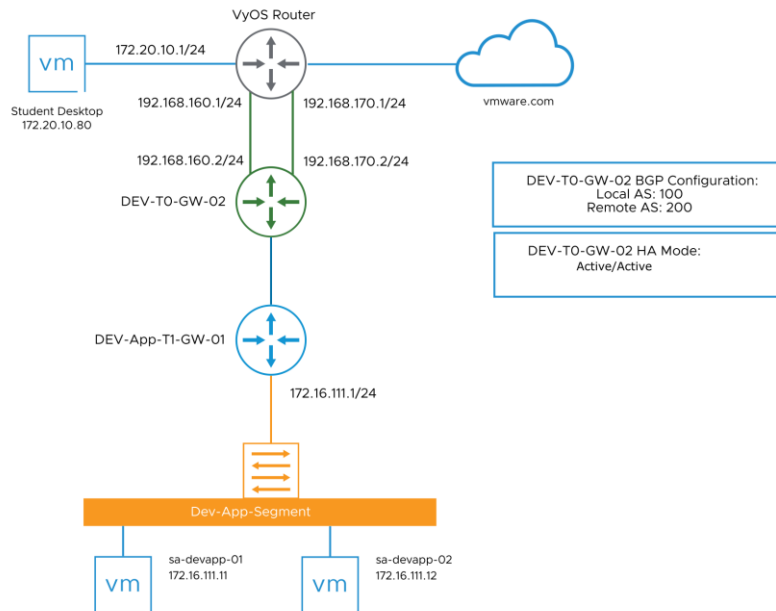
2. Review details about the issue and the course of action.

The following components are used in the scenario:

- DEV-T0-GW-02 and DEV-App-T1-GW-01 gateways
- DEV-App-Segment
- sa-devapp-01, sa-devapp-02 VMs
- student desktop (172.20.10.80)
- vmware.com

Only one of the VMs connected to DEV -App-Segment is able to successfully ping the internet.

You go to <https://sa-nxvip-02.vclass.local/login.jsp?>, log in to the NSX UI, and fix this issue.



Task 2: Confirm the Problem

You confirm a problem that was reported by the help desk: The sa-devapp-01 VM cannot communicate with the Internet. Pings between the sa-devapp-01 VM and vmware.com fail. The sa-devapp-02 VM attached to the same segment can ping vmware.com.

1. In Chrome, log in to vCenter Server with the vSphere Client.
2. Enter **administrator@vsphere.local** as the user name and **VMware1!** as the password .
3. Expand **Datacenter-02-Non-Production > Dev-QA-Cluster-01 > Dev-App** in the vCenter Server inventory.
4. In the Navigator pane, select **sa-devapp-01** and click **Launch Web Console**.
5. Log in to the sa-devapp-01 VM by entering **root** as the username and **VMware1!** as the password.
6. At the command prompt, ping the student desktop.

```
ping -c 3 172.20.10.80
```

The ping is successful.

7. At the command prompt, ping the Internet.

```
ping -c 3 vmware.com
```

The ping may or may not be successful.

8. In the vSphere Client, right-click **sa-devapp-02** and select **Launch Web Console**.
9. Log in to the sa-devapp-02 VM by entering **root** as the user name and **VMware1!** as the password .
10. At the command prompt, ping the student desktop.

```
ping -c 3 172.20.10.80
```

The ping is successful.

11. At the command prompt, ping the Internet.

```
ping -c 3 vmware.com
```

The result of this ping should be the opposite of that seen on sa-devapp-01.

Only one of the sa-devapp-01 and sa-devapp-02 VMs should not be able to ping the internet.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem.

1. Use the available techniques and tools to troubleshoot and fix the problem.

- Lecture manual for this course
- Lab environment worksheet
- NSX Manager and ESXi host log files
- VMware knowledge base articles at <http://kb.vmware.com>
- Other online technical resources

2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the connectivity works from both DEV App VMs to the Internet.

NOTE

The problem is not fixed until both VMs are able to ping the Internet without packet loss.

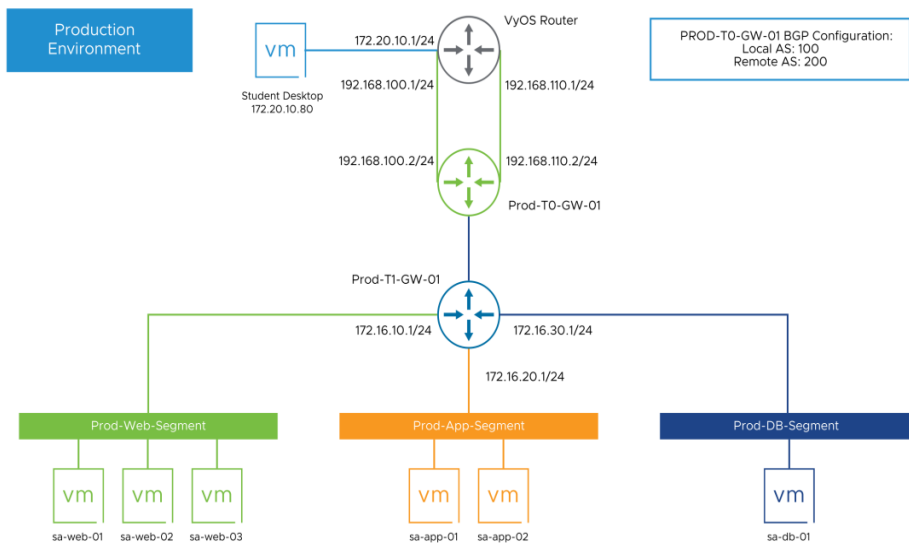
1. At the sa-devapp-01 command prompt, test the connectivity.
`ping -c 10 vmware.com`
2. At the sa-devapp-02 command prompt, test the connectivity.
`ping -c 10 vmware.com`
3. Close the consoles of the sa-devapp-01 and sa-devapp-02 VMs.

Lab 19 Distributed Firewall Verification

Objective and Tasks

Verify distributed firewall rules:

1. Prepare for the Lab
2. Enable Distributed Firewall Rules
3. Test the Connectivity Between Three-Tier App Machines
4. Verify DFW Rules from the ESXi CLI
5. Verify DFW Rules from the KVM CLI
6. Prepare for the Next Lab



Task 1: Prepare for the Lab

You log in to the vSphere Web Client UI and the NSX UI.

1. From your student desktop, log in to the vSphere Web Client UI.
 - a. Open Chrome.
 - b. Select the **vSphere Site-A > vSphere Web Client (SA-VCSA-01)** bookmark.
 - c. On the login page, enter **administrator@vsphere.local** as the user name and **VMware1!** as the password.
2. Log in to the NSX UI.
 - a. Open another tab in Chrome.
 - b. Select the **NSX-T Datacenter > NSX Manager (Prod)** bookmark.

NOTE

You go to <https://sa-nsxvip-01.vclass.local/login.jsp?> and log in to the Production NSX UI to perform this task.

- c. On the login page, enter **admin** as the user name and **VMware1!VMware1!** as the password.
3. Open MTPuTTY and open an SSH session to the sa-kvm-01 host.
 - a. Verify that sa-db-01 is powered on.

```
$ sudo virsh list --all
```

You powered on sa-db-01 in an earlier lab.
 - b. if necessary, power-on the sa-db-01 VM.

```
$ sudo virsh start sa-db-01
```

Task 2: Enable Distributed Firewall Rules

You enable distributed firewall rules to manage traffic in the three-tier app.

1. From the NSX UI, select **Security > East West Security > Distributed Firewall**.
2. Click the **CATEGORY SPECIFIC RULES** tab.
3. Click the **APPLICATION** tab.
4. Expand the **Web Traffic** policy.
5. Complete recording the details of the rules in this policy in this table in your student worksheet.

Web Traffic Policy Configuration Details

Rule Name	Source	Destination	Services	Actions
Allow Web Traffic	WEB-VMs	App-VMs		
Allow MySQL Traffic	App-VMs	DB-VMs		
Drop All Other Traffic	WEB-VMs	WEB-VMs		
	App-VMs	App-VMs		
	DB-VMs	DB-VMs		

6. Click the Edit menu (vertical ellipsis) of the Web Traffic policy and click **Enable All Rules**.
7. Navigate to the top-right corner of the screen and click **PUBLISH**.

Task 3: Test the Connectivity Between Three-Tier App Machines

You test the connectivity between the three-tier app machines to validate the distributed firewall rules.

1. Open MTPuTTY from the taskbar and double-click **sa-web-01** in the **Production-VMs Inventory** folder.
2. At the sa-web-01 command prompt, test the ICMP connectivity.

All pings should fail because you configured a rule to drop all traffic that is not explicitly allowed.

- a. Ping the sa-web-02 virtual machine.

```
sa-web-01:~ # ping -c 2 172.16.10.12
```

- b. Ping the sa-web-03 virtual machine.

```
sa-web-01:~ # ping -c 2 172.16.10.13
```

- c. Ping the sa-app-01 virtual machine.

```
sa-web-01:~ # ping -c 2 172.16.20.11
```

- d. Ping the sa-db-01 virtual machine.

```
sa-web-01:~ # ping -c 2 172.16.30.11
```

3. From the sa-web-01 MTPuTTY session, request a HTTP webpage from sa-app-01.

```
sa-web-01:~ # curl http://172.16.20.11
```

```
<html>
<head>
<title>NSX for vSphere Training</title>
</head>
<body bgcolor="#FFFFFF" text="#00005A" link="#0066FF"
alink="#3399FF" vlink="#2222BB">
<p>
Click on the link below to access the NSX Training test web
application:
</p>
<table>
<tr><td><a href="https://web-app.corp.local/cgi-bin/nsx-
webapp.cgi">ABC Medical Point of Sale App</a></td>
<tr><td><a href="https://secured-
app.corp.local/finance/data.html">ABC Medical Finance
Data</a></td>
</table>
</html>
```

```
sa-web-01:~ #
```

The HTTP response that is returned from sa-app-01 confirms that HTTP is allowed from sa-web-01 to sa-app-01.

4. Test the SQL access.
 - a. Open MTPuTTY and double-click **sa-app-01** in the Production-VMs Inventory folder.
 - b. Connect to the SQL database and enter **VMware1!** when prompted for the password.

```
sa-app-01:~ # mysql -u root -h 172.16.30.11 -p
```
 - c. Verify that the mysql> prompt is available to query the database.
 - d. Press Ctrl+C to exit.
5. Verify that only MySQL traffic is allowed between sa-app-01 and sa-db-01.

6. From the sa-app-01 MTPuTTY session, try to open an SSH session to sa-db-01.

```
sa-app-01:~ # ssh 172.16.30.11
```

The connection times out eventually. If you do not want to wait for the session to time out, you can press Ctrl+C to exit.

7. From MTPuTTY, close the **sa-web-01** and **sa-app-01** tabs.

Task 4: Verify DFW Rules from the ESXi CLI

You use the native ESXi commands to query the distributed firewall rules applied to the sa-web-01 VM.

1. Open MTPuTTY from the taskbar and click the **SA-ESXi-04** tab.
2. Retrieve the name of the dvfilter associated with the vNIC of the sa-web-01 VM.

```
[root@sa-esxi-04:~] summarize-dvfilter | grep -A10 sa-web-01
```

```
world 2100383 vmm0:sa-web-01 vcUuid:'50 2e 10 d1 f7 0c 8c 27-bb
cd cb 7f 68 11 98 32'
port 67108874 sa-web-01.eth0
vNic slot 2
name: nic-266125-eth0-vmware-sfw.2
agentName: vmware-sfw
state: IOChain Attached
vmState: Detached
failurePolicy: failClosed
serviceVMID: none
filter source: Dynamic Filter Creation
```

The vmware-sfw software construct stores and enforces DFW rules in the ESXi hosts. The summarize-dvfilter command is used to retrieve the name of vmware-sfw associated with the vNIC of a particular VM. This example seeks to retrieve the vmware-sfw name of the sa-web-01 VM, which is nic-266125-eth0-vmware-sfw.2. This identifier is used to query the rules associated with the vNIC of this VM. The identifier might be different in your environment.

- Record the details of the distributed firewall dvfilter applied to the sa-web-01 VM in this table in your student worksheet.

sa-web-01 dvfilter Configuration Details

Parameter	Value
agentName	
name	
vNIC slot	

- Retrieve the distributed firewall rules associated with a dvfilter.

```
[root@sa-esxi-04:~] vsipioctl getrules -f <dvfilter-name>
```

The rules attached to the sa-web-01 VM appear.

Example:

```
[root@sa-esxi-04:~] vsipioctl getrules -f nic--eth0-vmware-sfw.2
ruleset mainrs {
# generation number: 0
# realization time : 2019-06-29T22:22:31
rule 6147 at 1 inout protocol tcp from addrset 60bleebe-8e8b-4b67-b59a-cd11b487cc9e to addrset 63ab77d1-e479-47e1-bed6-8c3206663fb4 port 80 accept;
rule 6146 at 2 inout protocol tcp from addrset 63ab77d1-e479-47e1-bed6-8c3206663fb4 to addrset c0588656-3376-4d2a-98e0-b21dc51db062 port 3306 accept;
rule 6145 at 3 inout protocol any from addrset rsrc6145 to addrset rsrc6145 drop;rule 6144 at 4 inout protocol any from any to any accept;
rule 2 at 5 inout protocol any from any to any accept;
}
ruleset mainrs_L2 {
# generation number: 0
# realization time : 2019-06-29T22:22:31
rule 1 at 1 inout ethertype any stateless from any to any accept;
}
```

Rule 6147 is created to allow traffic between the Prod-Web-Tier and Prod-App-Tier over the HTTP port (80):

The following UUIDs also appear:

- 60b1eebe-8e8b-4b67-b59a-cd11b487cc9e is the UUID of the Web-VMs address sets and groups used for the rule configuration.
- 63ab77d1-e479-47e1-bed6-8c3206663fb4 is the UUID of the App-VMs address sets and groups used for the rule configuration.
- c0588656-3376-4d2a-98e0-b21dc51db062 is the UUID of the DB-VMs address sets and groups used for the rule configuration.

NOTE

The UUIDs of the address sets are different in your lab environment.

5. Record the information of the MySQL traffic rule (port 3306) in the Value column of this table in your student worksheet.

MySQL Firewall Rule Configuration Details

Parameter	Value
Rule number	
Direction (in/out/inout)	
Protocol	
Source (from addrset)	
Destination (to addrset)	
Port	
Action (accept/reject/drop)	

6. Retrieve the IP and MAC addresses associated with the distributed firewall rules for a dvfilter.

```
[root@sa-esxi-04:~] vsipioctl getaddrsets -f <dvfilter-name>
```

Example: [root@sa-esxi-04:~] vsipioctl getaddrsets -f nic-266125-eth0-vmware-sfw.2

7. Use the addrsets that you recorded in a previous step and record the source and destination IPs of the mySQL rule in the Value column of this table in your student worksheet.

mySQL Rule addrset Configuration Details

Parameter	Value
Source IP	
Destination IP	

8. Obtain the distributed firewall configuration for a dvfilter.

```
[root@sa-esxi-04:~] vsipioctl getfwconfig -f <dvfilter-name>
```

A list of firewall rules enforced at the VNIC of the VM, the address set with an IP, and MAC addresses appear.

Example: [root@sa-esxi-04:~] vsipioctl getfwconfig -f nic-266125-eth0-vmware-sfw.2

NOTE

The `vsipioctl getfwconfig` command gives the combined output of both `getrules` and `getaddrsets`.

Task 5: Verify DFW Rules from the KVM CLI

You use the Open vSwitch commands to query distributed firewall rule information. The Open vSwitch module installed on the KVM host implements the firewall services.

1. Open MTPuTTY from the taskbar and double-click **SA-KVM-01** to connect over SSH.
2. Switch the user to root.

```
vmware@sa-kvm-01:~$ sudo -i
```

3. Retrieve the virtual interface identifier for the vNICs that have associated distributed firewall rules on SA-KVM-01.

```
root@sa-kvm-01:~# ovs-appctl -t /var/run/openvswitch/nsxa-  
ctl dfw/vif
```

The Virtual Interface (Vif) ID appears. This ID is needed to query the distributed firewall rules associated with a VM.

SA-KVM-01 runs a single VM called sa-db-01 and the port used by the sa-db-01 VM is labelled T1-DB-01.

Example:

```
root@sa-kvm-01:~# ovs-appctl -t /var/run/openvswitch/nsxa-  
ctl dfw/vif  
Vif ID : 57601300-2e82-48c4-8c27-1e961ac70e81  
Port name : T1-DB-01  
Port number : 1
```

4. Record the VIF details in the Value column of this table in your student worksheet.

sa-db-01 VIF Details

Parameter	Value
-----------	-------

Vif ID	
--------	--

5. Retrieve the distributed firewall rules associated with a virtual interface.

```
root@sa-kvm-01:~# ovs-appctl -t /var/run/openvswitch/nsxa-ctl dfw/rules <VIF-ID>
```

The VIF ID and the ruleset details appear. The ruleset typically has one or more rules.

Each rule has the following items:

- Rule number
- Rule direction
- Protocol
- Address set
- Port number
- Action

```
Example: root@sa-kvm-01:~# ovs-appctl -t /var/run/openvswitch/nsxa-ctl dfw/rules 57601300-2e82-48c4-8c27-1e961ac70e81
```

6. Record the information of the MySQL (port 3306) traffic rule in the Value column of this table in your student worksheet.

MySQL Traffic Rule Configuration Details

Parameter	Value
Rule number	
From addrset (source)	
To addrset (destination)	
Port	
Action	

- a. Verify that the Rule Number recorded here is identical to that recorded in the previous task on the ESXi transport node.

7. Retrieve the IP and MAC addresses associated with the distributed firewall rules for a dvfilter.

```
root@sa-kvm-01:~# ovs-appctl -t /var/run/openvswitch/nsxa-  
ctl dfw/addrset <addrset>
```

```
Example:root@sa-kvm-01:~# ovs-appctl -t  
/var/run/openvswitch/nsxa-ctl dfw/addrset 9117b4ea-c90b-  
4b0c-a860-96c2540eed13
```

8. Use the addrsets recorded in a previous step to record the source and destination IPs of the HTTP rule in the Value column of this table in your student worksheet.

MySQL Rule addrset Configuration Details

Parameter	Value
Source IP	
Destination IP	

- a. Verify that the MySQL rule address set source and destination IPs recorded here are identical to that recorded in the previous task on the ESXi transport node.

Task 6: Prepare for the Next Lab

You disable the distributed firewall rules to prepare for the upcoming labs.

1. From the NSX UI, navigate to **Security > East West Security > Distributed Firewall**.
2. Click the **CATEGORY SPECIFIC RULES** tab.
3. Click the **APPLICATION** tab.
4. Click the **Edit** menu (vertical ellipsis) of the **Web Traffic** policy and click **Disable All Rules**.
5. Click **PUBLISH** in the upper-right corner.

Lab 20 Distributed Firewall Break-Fix Scenario 1

Objective and Tasks

Identify, diagnose, and resolve an NSX distributed firewall problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify That the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

Recently, a team member made some changes to the configuration of the NSX-T Data Center distributed firewall. After making these changes, an SSH connection cannot be established from sa-infosec-01 to sa-infosec-02.

2. Review details about the issue and the course of action.

The following components are used in the scenario:

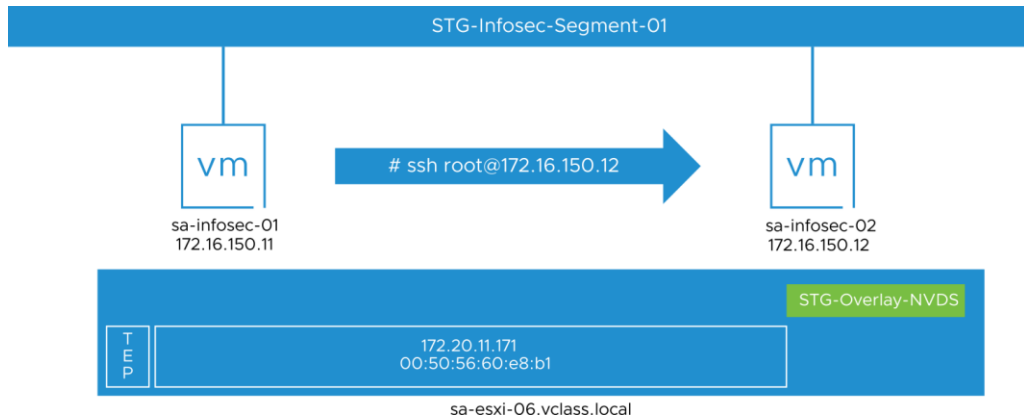
- STG-Infosec-Segment-01
- sa-infosec-01 virtual machine
- sa-infosec-02 virtual machine

You go to <https://sa-nsxvip-02.vclass.local/login.jsp?>, log in to the Non-Production NSX UI, and fix this issue.

To resolve the problem, you must open an SSH connection from sa-infosec-01 to sa-infosec-02 (172.16.150.12).

IMPORTANT

Disabling the distributed firewall or the default Block_All_Traffic are not valid solutions.



Task 2: Confirm the Problem

You confirm a problem that was reported by the help desk: sa-infosec-01 cannot connect to sa-infosec-02 through SSH.

1. In Chrome, log in to vCenter Server with the vSphere Client.
2. Enter **administrator@vsphere.local** as the user name and **VMware1!** as the password.
3. Expand **Datacenter-02-Non-Production > Staging-Cluster-01 > STG-InfoSec** in the vCenter Server inventory.
4. In the Navigator pane, click **sa-infosec-01** and select **Launch Web Console** from the virtual machine summary page.
5. Log in to the sa-infosec-01 VM by entering **root** as the user name and **VMware1!** as the password.
6. At the command prompt, open an SSH connection to sa-infosec-02.

```
ssh root@172.16.150.12
```

The SSH connection attempt fails with a connection refused message.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem.

1. Use the available techniques and tools to troubleshoot and fix the problem.
 - Lecture manual for this course
 - Lab environment worksheet
 - NSX Manager and ESXi host log files
 - VMware knowledge base articles at <http://kb.vmware.com>
 - Other online technical resources
2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the SSH connectivity from sa-infosec-01 to sa-infosec-02 is restored.

1. From the sa-infosec-01 command prompt, access the sa-infosec-02 command prompt.

```
ssh root@172.16.150.12
```


Use VMware1! as the password.
2. Enter `exit` to close the SSH session and return to the sa-infosec-01 command prompt.

Lab 21 Distributed Firewall Break-Fix Scenario 2

Objective and Tasks

Identify, diagnose, and resolve an NSX distributed firewall problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify That the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

Recently, a team member made some changes to the configuration of the NSX-T Data Center distributed firewall. After making these changes, an SSH connection cannot be established from sa-infosec-03 to sa-tlsvm-01.

2. Review details about the issue and the course of action.

The following components are used in the scenario:

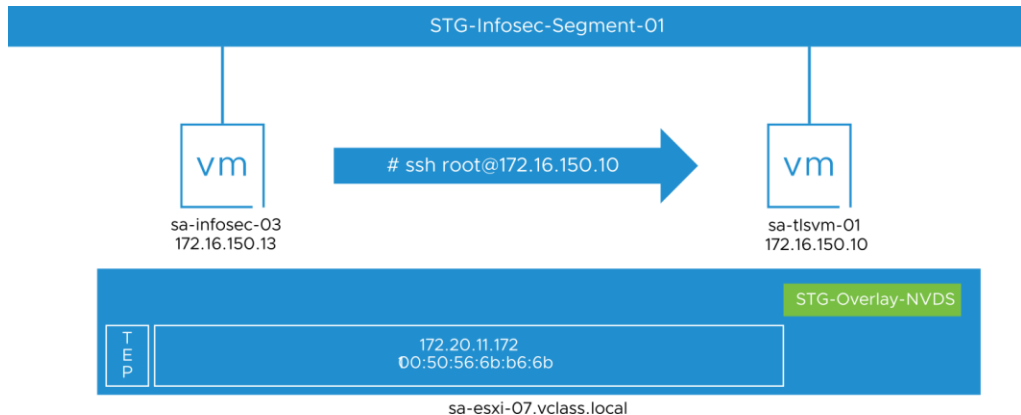
- STG-Infosec-Segment-01
- sa-infosec-03 virtual machine
- sa-tlsvm-01 virtual machine

You go to <https://sa-nsxvip-02.vclass.local/login.jsp?>, log in to the Non-Production NSX UI, and fix this issue.

To resolve the problem, you must open an SSH connection from sa-infosec-03 to sa-tlsvm-01 (172.16.150.10).

IMPORTANT

Disabling the distributed firewall or the default Block_All_Traffic are not valid solutions.



Task 2: Confirm the Problem

You confirm a problem that was reported by the help desk: sa-infosec-03 cannot connect to sa-tlsvm-01 through SSH.

1. In Chrome, log in to vCenter Server with the vSphere Client.
2. Enter **administrator@vsphere.local** as the user name and **VMware1!** as the password .
3. Expand **Datacenter-02-Non-Production > Staging-Cluster-01 > STG-InfoSec** in the vCenter Server inventory.
4. In the Navigator pane, click **sa-infosec-03** and select **Launch Web Console** from the virtual machine summary page.
5. Log in to the sa-infosec-03 VM by entering **root** as the username and **VMware1!** as the password .
6. At the command prompt, open an SSH connection to sa-tlsvm-01.

```
ssh root@172.16.150.10
```

The connection fails with a connection reset by peer error.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem.

1. Use the available techniques and tools to troubleshoot and fix the problem.
 - Lecture manual for this course
 - Lab environment worksheet
 - NSX Manager and ESXi host log files
 - VMware knowledge base articles at <http://kb.vmware.com>
 - Other online technical resources
2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the SSH connectivity from sa-infosec-03 to sa-tlsvm-01 is restored.

1. From the sa-infosec-03 command prompt, access the sa-tlsvm-01 command prompt.

```
ssh root@172.16.150.10
```


Use VMware1! as the password.
2. Enter **exit** to close the SSH session and return to the sa-infosec-03 command prompt.

Lab 22 Distributed Firewall Challenge Scenario

Objective and Tasks

Identify, diagnose, and resolve an NSX distributed firewall problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify That the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

Recently, a team member made some changes to the configuration of the NSX-T Data Center distributed firewall. After making these changes, accessing `http://sa-tlsvm-01.vclass.local` from `sa-infosec-03` is not possible.

2. Review details about the issue and the course of action.

The following components are used in the scenario:

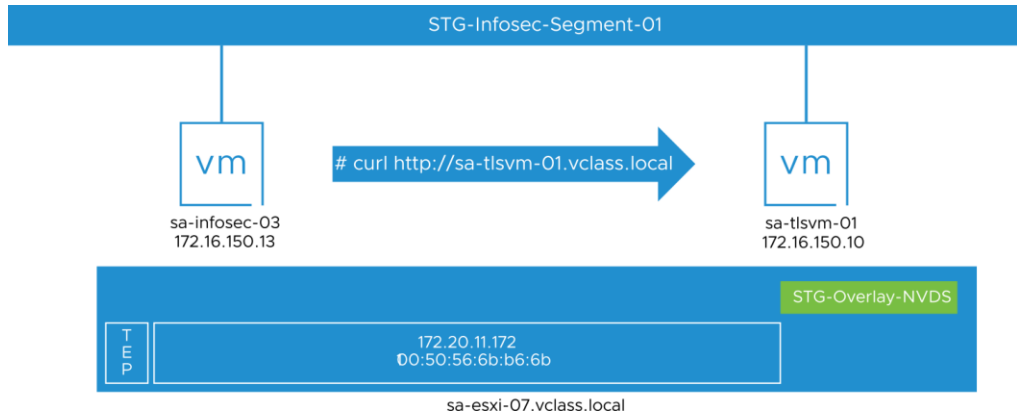
- STG-Infosec-Segment-01
- sa-infosec-03 virtual machine
- sa-tlsvm-01 virtual machine
- `http://sa-tlsvm-01.vclass.local` webpage

You go to <https://sa-nxsvip-02.vclass.local/login.jsp?>, log in to the Non-Production NSX UI, and fix this issue.

To resolve the problem, you must be able to access the webpage at <http://sa-tlsvm-01.vclass.local> from sa-infosec-03.

IMPORTANT

Disabling the distributed firewall or the default Block_All_Traffic are not valid solutions.



Task 2: Confirm the Problem

You confirm a problem that was reported by the help desk: sa-infosec-03 cannot access <http://sa-tlsvm-01.vclass.local>.

1. In Chrome, log in to vCenter Server with the vSphere Client.
2. Enter **administrator@vsphere.local** as the user name and **VMware1!** as the password .
3. Expand **Datacenter-02-Non-Production > Staging-Cluster-01 > STG-InfoSec** in the vCenter Server inventory.
4. In the Navigator pane, click **sa-infosec-03** and select **Launch Web Console** from the virtual machine summary page.
5. Log in to the sa-infosec-03 VM by entering **root** as the user name and **VMware1!** as the password.
6. At the command prompt, view the webpage.

```
curl http://sa-tlsvm-01.vclass.local
```

The curl command must not be successful.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem.

1. Use the available techniques and tools to troubleshoot and fix the problem.
 - Lecture manual for this course
 - Lab environment worksheet
 - NSX Manager and ESXi host log files
 - VMware knowledge base articles at <http://kb.vmware.com>
 - Other online technical resources
2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the SSH connectivity from sa-infosec-03 to `http://sa-tlsvm-01.vclass.local` is restored.

1. At the sa-infosec-03 command prompt, view the webpage.

```
curl http://sa-tlsvm-01.vclass.local
```

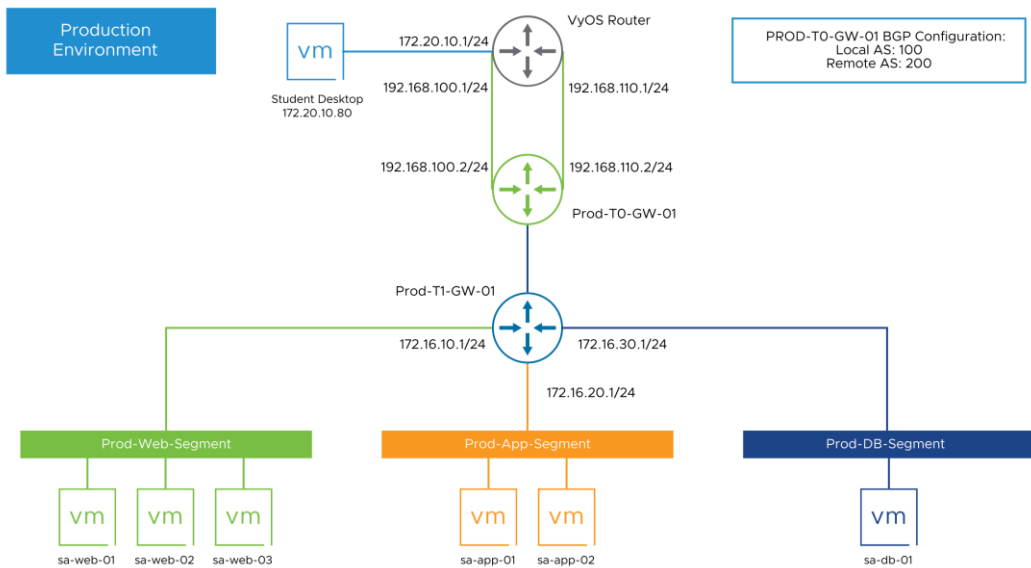
A response appears with the HTML code of the webpage.

Lab 23 Gateway Firewall Verification

Objective and Tasks

Verify gateway firewall rules:

1. Prepare for the Lab
2. Test Connectivity
3. Enable Gateway Firewall Rules
4. Test Connectivity
5. Verify Gateway Rules from the NSX Edge CLI
6. Prepare for the Next Lab



Task 1: Prepare for the Lab

You log in to the vSphere Web Client UI and the NSX UI.

1. From your student desktop, log in to the vSphere Web Client UI.
 - a. Open Chrome.
 - b. Select the **vSphere Site-A > vSphere Client (SA-VCSA-01)** bookmark.
 - c. On the login page, enter **administrator@vsphere.local** as the user name and **VMware1!** as the password.
2. Log in to the NSX UI.
 - a. Open another tab in Chrome.
 - b. Select the **NSX-T Data Center > NSX Manager (Prod)** bookmark.

NOTE

You go to <https://sa-nsxvip-01.vclass.local/login.jsp?>, log in to the Production NSX Manager UI, and perform this task.

- c. On the login page, enter **admin** as the user name and **VMware1!VMware1!** as the password.
3. Open MTPuTTY and open an SSH session to the sa-kvm-01 host.
 - a. Verify that sa-db-01 is powered on.

```
$ sudo virsh list --all
```

You powered on sa-db-01 in an earlier lab.
 - b. if necessary, power-on the sa-db-01 VM.

```
$ sudo virsh start sa-db-01
```

Task 2: Test Connectivity

You verify the SSH connectivity before enabling gateway firewall rules.

1. Open MTPuTTY and expand the **Production-VMs Inventory** folder.
2. Double-click **sa-web-01** and verify that you can open SSH sessions to the web server.
3. Double-click **sa-app-01** and verify that you can open SSH sessions to the applications servers.
4. Double-click **sa-db-01** and verify that you can open SSH sessions to the database server.
5. In MTPuTTY, close all open ssh session tabs for sa-web-01, sa-app-01, and sa-db-01.

Task 3: Enable Gateway Firewall Rules

You enable gateway firewall rules to manage SSH traffic to the virtual machines in the three-tier app.

1. From the NSX UI, select **Security > North South Security > Gateway Firewall**.
2. Click the **GATEWAY SPECIFIC RULES** tab.
3. Verify that **Prod-T0-GW-01** is selected from the **Gateway** drop-down menu.
4. Expand **Block-SSH-Policy** and complete recording the configuration of the Block-SSH-from-Outside rule in this table in your student worksheet.

Block-SSH-from-Outside Firewall Rule Configuration Details

Sources	Destinations	Services	Actions
Block-SSH-from-Outside	Web-VMs App-VMs DB-VMs		

5. Click the **Edit** menu (vertical ellipsis) for Block-SSH-Policy and click **Enable All Rules**.
6. Navigate to the top-right corner of the screen and click **PUBLISH**.

Task 4: Test Connectivity

You verify the SSH connectivity after enabling gateway firewall rules.

1. Open MTPuTTY and expand the **Production-VMs Inventory** folder.
2. Double-click **sa-web-01** and verify that you can no longer open SSH sessions to the web servers.
3. Double-click **sa-app-01** and verify that you can no longer open SSH sessions to the application servers.
4. Double-click **sa-db-01** and verify that you can no longer open SSH sessions to the database server.

Task 5: Verify Gateway Rules from the NSX Edge CLI

You verify the gateway firewall rule information from the NSX Edge command line.

- 1. Open MTPuTTY, expand the **Production-NSX Inventory** folder, and click **sa-nsxedge-01**.
- 2. Retrieve all edge interfaces that have firewall rules configured.

```
sa-nsxedge-01> get firewall interfaces
```

Example:

```
sa-nsxedge-01> get firewall interfaces
Interface : 1a99f0e7-3394-4977-ae6f-e8388418fd60
Type : UPLINK
Sync enabled : false
Name : Uplink-01-Intf
VRF ID : 5
Contextentity : fdc41c7d-04fd-4937-8869-e841e900d844
Context name : SR-Prod-T0-GW-01
```

The Block-SSH-from_Outside rule was applied to the Uplink-01-Intf interface.

- 3. Record details of the Uplink-01-Intf interface in the Value column of this table in your student worksheet.

Uplink-01-Intf Configuration Details

Parameter	Value
Type	
Interface (UUID)	
Context Name	

NOTE

The other interface (Uplink-02-Intf) on which the rule is applied is present on sa-nsxedge-02.

4. Run the following command to query the gateway firewall rules associated with the UPLINK interface.

```
sa-nsxedge-01> get firewall <uuid> ruleset rules
```

Example:

```
sa-nsxedge-01> get firewall 42c1e4df-797e-49b0-a0b6-e41f9bfd9efd ruleset rules
<snip>
Rule ID : 6148
Rule : inout protocol tcp stateless from any to addrset {172.16.10.11, 172.16.10.12, 172.16.10.13, 172.16.20.11, 172.16.30.11} port 22 interface addrset {42c1e4df-797e-49b0-a0b6-e41f9bfd9efd, d8401057-b3c1-4da4-bc15-209d7f8f6305} drop
<snip>
sa-nsxedge-01>
```

5. Record details of the gateway firewall rule that blocks SSH traffic (port 22) in the Value column of this table in your student worksheet.

SSH Firewall Rule Configuration Details

Parameter	Value
Rule ID	
Direction (in/out/inout)	
Protocol	
From (source)	
To (destination)	
Port	
Action (accept/reject/drop)	

Task 6: Prepare for the Next Lab

You disable the gateway firewall rules to prepare for the upcoming labs.

1. From the NSX Manager UI, navigate to **Security > North South Security > Gateway Firewall**.
2. Click the **GATEWAY SPECIFIC RULES** tab and select **Prod-T0-GW-01** from the **Gateway** drop-down menu.
3. Click the **Edit** menu (vertical ellipsis) of Block-SSH-Policy and click **Disable All Rules**.
4. In the top-right corner, click **PUBLISH**.

Lab 24 Gateway Firewall Break-Fix Scenario 1

Objective and Tasks

Identify, diagnose, and resolve an NSX gateway firewall problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify That the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

Recently, a team member made some changes to the configuration of the NSX-T Data Center gateway firewall. After making these changes, you cannot ping the student desktop from sa-infosec-01.

2. Review details about the issue and the course of action.

The following components are used in the scenario:

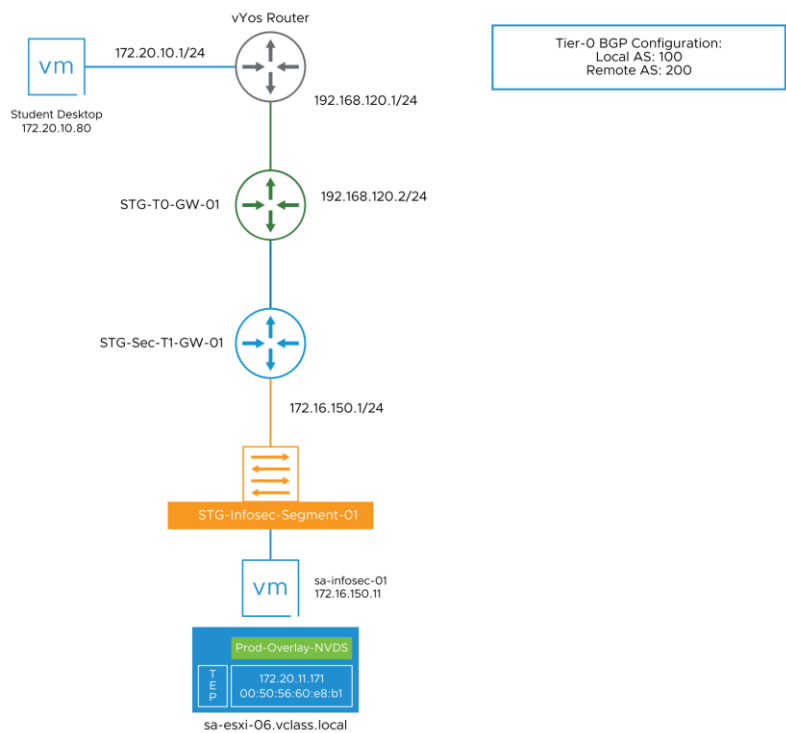
- STG-T0-GW-01 and STG-Sec-T1-GW-01 gateways
- STG-Infosec-Segment-01 segment
- sa-infosec-01 virtual machine
- Student desktop

You go to <https://sa-nxvip-02.vclass.local/login.jsp?>, log in to the Non-Production NSX UI, and fix this issue.

To resolve the problem, you must be able to ping the student desktop (172.20.10.80) from sa-infosec-01.

IMPORTANT

You must resolve the (Break-Fix Scenario 1) Logical Switching problem affecting sa-esxi-06 before you can complete this lab. Disabling the gateway firewall is not a valid solution.



Task 2: Confirm the Problem

You confirm a problem that was reported by the help desk: sa-infosec-01 cannot ping the student desktop.

1. In Chrome, log in to vCenter Server with the vSphere Client.
2. Enter **administrator@vsphere.local** as the user name and **VMware1!** as the password.
3. Expand **Datacenter-02-Non-Production > Staging-Cluster-01 > STG-InfoSec** in the vCenter Server inventory.
4. In the Navigator pane, click **sa-infosec-01** and select **Launch Web Console** from the virtual machine summary page.
5. Log in to the sa-infosec-01 VM by entering **root** as the username and **VMware1!** as the password.
6. At the command prompt, ping the student desktop.

```
ping -c 3 172.20.10.80
```

The ping command must not be successful.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem.

1. Use the available techniques and tools to troubleshoot and fix the problem.
 - Lecture manual for this course
 - Lab environment worksheet
 - NSX Manager and ESXi host log files
 - VMware knowledge base articles at <http://kb.vmware.com>
 - Other online technical resources
2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the connectivity to the student desktop from sa-infosec-01 VM is restored.

1. At the sa-infosec-01 command prompt, ping the student desktop.

```
ping -c 3 172.20.10.80
```

Lab 25 Gateway Firewall Break-Fix Scenario 2

Objective and Tasks

Identify, diagnose, and resolve an NSX gateway firewall problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify That the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

During a maintenance window, a team member recently reconfigured the gateway firewall policy that allowed the sa-infosec-02 VM to successfully ping a DNS server (8.8.8.8) on the Internet. The sa-infosec-02 user cannot ping 8.8.8.8 from sa-infosec-02.

2. Review details about the issue and the course of action.

The following components are used in the scenario:

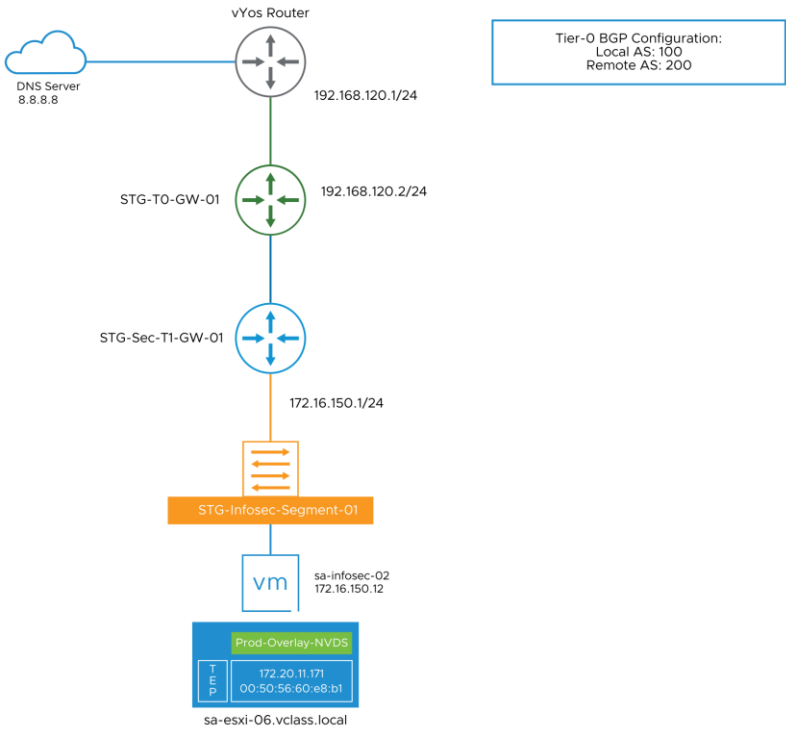
- STG-T0-GW-01 and STG-Sec-T1-GW-01 gateways
- STG-Infosec-Segment-01 segment
- sa-infosec-02 virtual machine
- A public DNS server 8.8.8.8

You go to <https://sa-nsxvip-02.vclass.local/login.jsp?>, log in to the Non-Production NSX UI, and fix this issue.

To resolve the problem, you must be able to ping the 8.8.8.8 from sa-infosec-02.

IMPORTANT

You must resolve the (Break-Fix Scenario 1) Logical Switching problem affecting sa-esxi-06 before you can complete this lab. Disabling the gateway firewall is not a valid solution.



Task 2: Confirm the Problem

You confirm a problem that was reported by the help desk: sa-infosec-02 cannot ping the public DNS server 8.8.8.8.

1. In Chrome, log in to vCenter Server with the vSphere Client.
2. Enter **administrator@vsphere.local** as the user name and **VMware1!** as the password.
3. Expand **Datacenter-02-Non-Production > Staging-Cluster-01 > STG-InfoSec** in the vCenter Server inventory.
4. In the Navigator pane, click **sa-infosec-02** and select **Launch Web Console** from the virtual machine summary page.
5. Log in to the sa-infosec-02 VM by entering **root** as the user name and **VMware1!** as the password.
6. At the command prompt, ping the student desktop.

```
ping -c 3 8.8.8.8
```

The ping command must not be successful.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem.

1. Using the available techniques and tools to troubleshoot and fix the problem.
 - Lecture manual for this course
 - Lab environment worksheet
 - NSX Manager and ESXi host log files
 - VMware knowledge base articles at <http://kb.vmware.com>
 - Other online technical resources
2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the connectivity to 8.8.8.8 from sa-infosec-02 VM is restored.

1. At the sa-infosec-02 command prompt, ping the public DNS server.

```
ping -c 3 8.8.8.8
```

Lab 26 Load Balancer Verification

Objective and Tasks

Verify load balancer configuration from the NSX CLI:

1. Prepare for the Lab
2. Verify the Load Balancer Operation
3. Verify the Load Balancer Configuration from the NSX CLI
4. Prepare for the Next Lab

Task 1: Prepare for the Lab

You log in to the NSX UI and verify the gateway for the Prod-Web-Segment segment.

1. Open MTPuTTY and open an SSH session to the sa-kvm-02 host.
 - a. Verify that sa-web-03 is powered on.

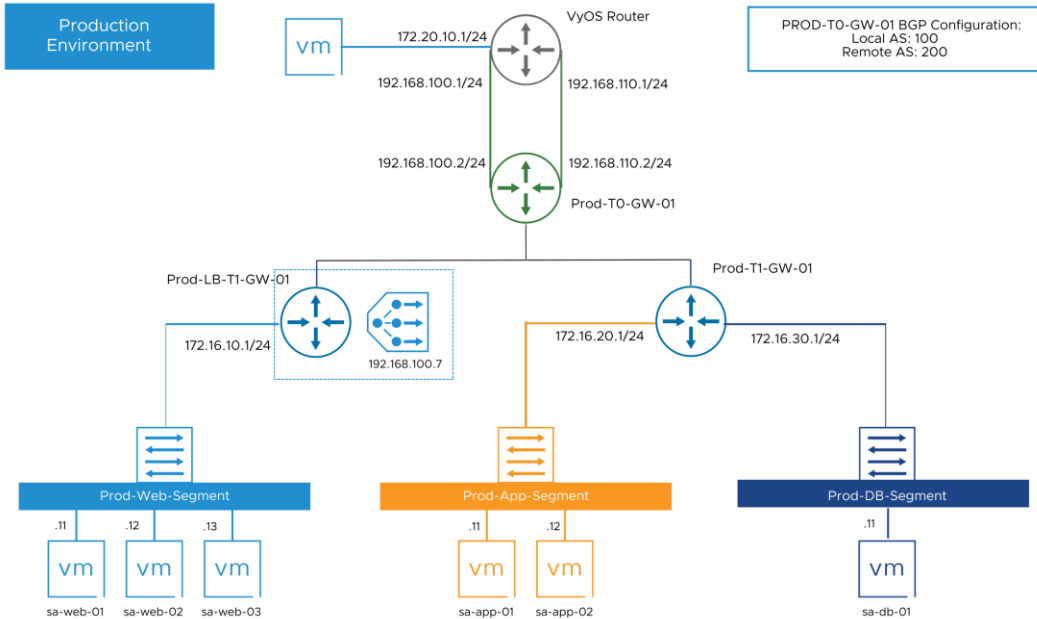
```
$ sudo virsh list --all
```

You powered on sa-web-03 in an earlier lab.
 - b. If necessary, power-on the sa-web-03 VM.

```
$ sudo virsh start sa-web-03
```
2. Log in to the NSX UI.
 - a. Select the **NSX-T Data Center > Prod Manager (Prod)** bookmark.
 - b. On the login page, enter **admin** as the user name and **VMware1!VMware1!** as the password.

3. Connect the Prod-Web-Segment segment to the Prod-LB-T1-GW-01 Tier-1 gateway.
 - a. From the NSX UI, navigate to **Networking > Connectivity > Segments**.
 - b. Click the vertical ellipsis and click **EDIT** for Prod-Web-Segment.
 - c. From the **Connectivity** drop-down menu, select **Prod-LB-T1-GW-01**.
 - d. Click **SAVE** and **CLOSE EDITING**.

After you make this change, the topology of the three-tier application in the Production environment is changed.



Task 2: Verify the Load Balancer Operation

You verify that the HTTP traffic is being handled by both back-end web servers in a round-robin method.

1. Use Firefox to verify the access to the load balancer VIP.

NOTE

Do not use Chrome for this step.

- a. From the student desktop, open Firefox and open the **3-Tier-App > Production > LB VIP** bookmark.

The webpage appears with the Web-Server name and the IP address from which the page is loaded.

- b. Refresh the browser to verify that both back-end web servers are used because of the configured round-robin method.

Because of the browser cache behavior, you might need to press Ctrl+F5 (force refresh) to see the load-balanced traffic between the two web servers.

The client's HTTP requests alternate between Web-Server-01 and Web-Server-02.

2. Use the `curl` command to verify access to the load balancer VIP.

- a. From the student desktop, open the Windows command prompt and access the load balancer VIP address.

```
curl -i http://192.168.100.7
```

The HTML body section of the text contains the Web-Server name and the IP address from which the page is loaded.

- b. Run the same `curl` command again to verify that both back-end web servers are being used in a round-robin method.

```
C:\Windows\system32>curl -i http://192.168.100.7
HTTP/1.1 200 OK
Date: Wed, 23 Jan 2019 22:23:53 GMT
Server: Apache/2.2.12 (Linux/SUSE)
Last-Modified: Tue, 28 Aug 2018 14:18:17 GMT
ETag: "16f4-75-5747f835afc40"
Accept-Ranges: bytes
Content-Length: 117
Content-Type: text/html

<html>
<head>
<title>NSX-T Data Center Labs</title>
</head>
<body>
<b>Web-Server-02 172.16.10.12</b>
</body>
</html>

C:\Windows\system32>curl -i http://192.168.100.7
HTTP/1.1 200 OK
Date: Wed, 23 Jan 2019 22:24:35 GMT
Server: Apache/2.2.12 (Linux/SUSE)
Last-Modified: Tue, 28 Aug 2018 14:20:50 GMT
ETag: "4b69-75-5747f8c799480"
Accept-Ranges: bytes
Content-Length: 117
Content-Type: text/html

<html>
<head>
<title>NSX-T Data Center Labs</title>
</head>
<body>
<b>Web-Server-01 172.16.10.11</b>
</body>
</html>

C:\Windows\system32>
```

Task 3: Verify the Load Balancer Configuration from the NSX CLI

You log in to sa-nsxedge-01 and use the NSX command line to query the load-balancer configuration information.

1. From MTPuTTY, click **sa-nsxedge-01**.

2. Verify the load balancer configuration.

```
sa-nsxedge-01> get load-balancer
```

3. Record the configuration details of the load balancer in the Value column of this table in your student worksheet.

Load balancer configuration details

Parameter	Value
Display name	
UUID	
Size	
Virtual server Id	

4. Verify the virtual server configuration.

```
sa-nsxedge-01> get load-balancer <UUID> virtual-server
```

Example: sa-nsxedge-01> get load-balancer 67af385f-1b6d-4241-a7cc-3901f38a7372 virtual-server

5. Record configuration details of the virtual server in the Value column of this table in your student worksheet.

Virtual Server Configuration Details

Parameter	Value
Display name	
Ipv4 IP address	
Enabled	
IP Protocol	
Pool ID	

6. Verify the load balancer virtual server status.

```
sa-nsxedge-01> get load-balancer <UUID> virtual-server  
<virtualserver-UUID> status
```

Example: sa-nsxedge-01> get load-balancer 67af385f-1b6d-4241-a7cc-3901f38a7372 virtual-server 6b411d2f-08cf-4acc-884b-ec6bad36f860 status

7. Record status details of the virtual server in the Value column of this table in your student worksheet.

Virtual Server Status Details

Parameter	Value
Display name	
IP	
Port	
Status	

8. Display the load balancer statistics.

```
sa-nsxedge-01> get load-balancer <UUID> virtual-server  
<virtualserver-UUID> stats
```

The sessions, bytes, and packets statistics for the virtual server appear.

Example:sa-nsxedge-01> get load-balancer 67af385f-1b6d-4241-a7cc-3901f38a7372 virtual-server 6b411d2f-08cf-4acc-884b-ec6bad36f860 stats

9. Verify the server pool configuration.

```
sa-nsxedge-01> get load-balancer <UUID> pools
```

Example: sa-nsxedge-01> get load-balancer 67af385f-1b6d-4241-a7cc-3901f38a7372 pools

- Record configuration details of the server pool in the Value column of this table in your student worksheet.

Server Pool Configuration Details

Parameter	Value
Display name	
Algorithm	
Number of members in the pool	
Ipv4 Ip Addresses of pool members	

- View the health check table.

```
sa-nsxedge-01> get load-balancer <UUID> health-check-table
```

```
Example: sa-nsxedge-01> get load-balancer 67af385f-1b6d-4241-a7cc-3901f38a7372 health-check-table
```

- Record details about the health of each pool member in this table in your student worksheet.

Pool Member Health

Name	STATUS
172.16.10.11:80	
172.16.10.12:80	
172.16.10.13:80	

- Review the error log that can be used to troubleshoot any load balancer issues.

```
sa-nsxedge-01> get load-balancer <UUID> error-log
```

The error log appears. Use the arrow keys to navigate. The error log might be empty in your lab environment.

```
Example: sa-nsxedge-01> get load-balancer 67af385f-1b6d-4241-a7cc-3901f38a7372 error-log
```

- Enter **q** to close the error log and return to the command prompt.

Task 4: Prepare for the Next Lab

You connect the Prod-Web-Segment segment to the Prod-T1-GW-01 gateway.

1. Click the **NSX Manager (Prod)** tab in Chrome.
If the NSX UI session has expired, log in with admin as the user name and VMware1!VMware1! as the password.
2. Attach the Prod-Web-Segment segment to the Prod-T1-GW-01 Tier-1 gateway.
 - a. From the NSX UI, navigate to **Networking > Connectivity > Segments**.
 - b. Click the vertical ellipsis and click **EDIT** for Prod-Web-Segment.
 - c. From the **Connectivity** drop-down menu, select **Prod-T1-GW-01**.
 - d. Click **SAVE** and **CLOSE EDITING**.

Lab 27 Load Balancer Break-Fix Scenario 1

Objective and Tasks

Identify, diagnose, and resolve an NSX load balancer problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify That the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

An administrator configured the NSX-T Data Center load balancer to load balance the QA web server traffic. But the end users are unable to access the QA website by using the load-balanced address.

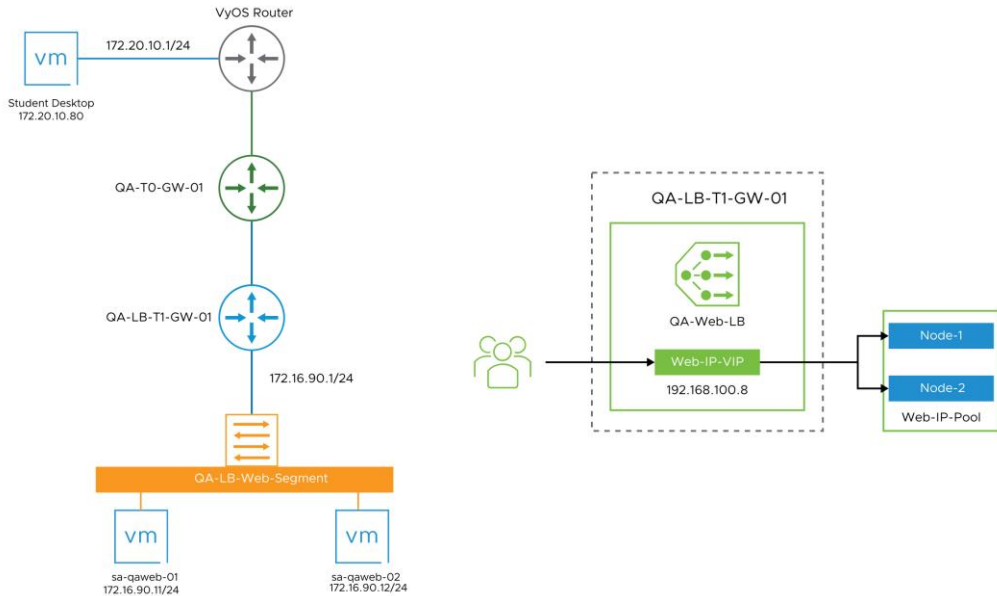
2. Review details about the issue and the course of action.

The NSX-T Data Center load balancer configuration includes the following components:

- QA-LB-T1-GW-01 and QA-T0-GW-01 gateways
- QA-Web-LB load balancer (VIP 192.168.100.8)
- QA-LB-Web-Segment
- sa-qaweb-01 and sa-qaweb-02 VMs

The problem is resolved when the student desktop can reach the web server VIP at <http://192.168.100.8/>.

You log in to the Non-Production NSX Manager UI with URL <https://sa-nsxvip-02.vclass.local/login.jsp?> to confirm and resolve the reported issue.



Task 2: Confirm the Problem

You confirm a problem that was reported by the help desk: The load balancer configured with VIP 192.168.100.8 does not work.

1. From your student desktop, open Firefox and try to access the web server VIP address.
You can use one of the following ways to access the web server VIP address:
 - Go to <http://192.168.100.8>.
 - Select the **3-Tier-App > Non-Production > QA LB VIP** bookmark.
2. Verify that the website cannot be reached.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem.

1. Use the available techniques and tools to troubleshoot and fix the problem.
 - Lecture manual for this course
 - Lab environment worksheet
 - NSX Manager and ESXi host log files
 - VMware knowledge base articles at <http://kb.vmware.com>
 - Other online technical resources
2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the connectivity to the student desktop is restored.

IMPORTANT

Do not continue to the next lab until the problem is fixed.

1. From your student desktop, open a tab in Chrome.
2. Access the load balancer VIP address at <http://192.168.100.8>.

This problem is fixed when the load balancer VIP address is reachable and one of the back-end web servers can be accessed.

Lab 28 Load Balancer Break-Fix Scenario 2

Objective and Tasks

Identify, diagnose, and resolve an NSX load balancer problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify That the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

An administrator configured the NSX-T Data Center load balancer to redistribute the traffic between the web servers. However, the load balancing does not work as intended, and every time a user accesses the webpage, requests are sent to only one server.

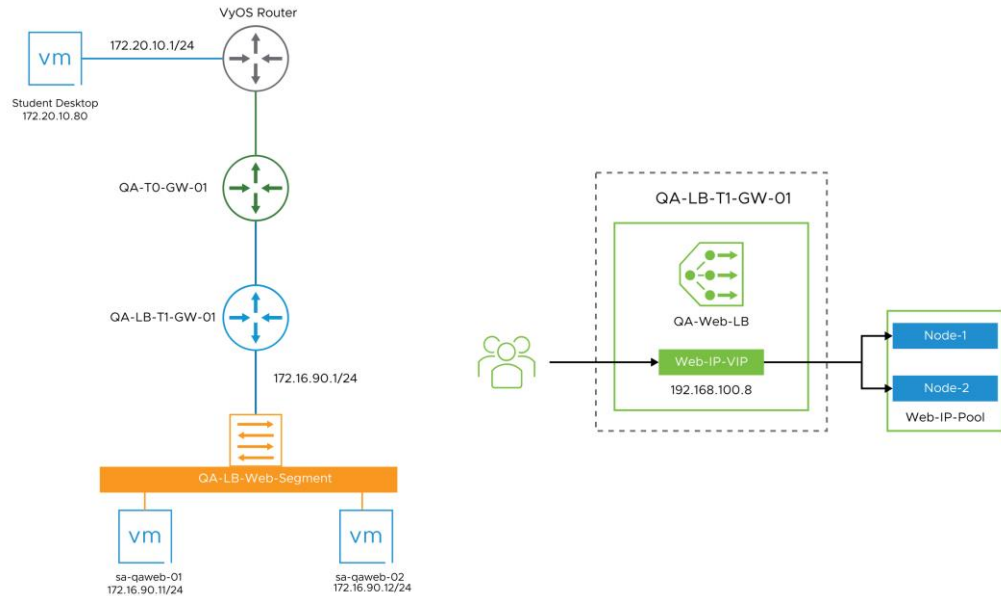
2. Review details about the issue and the course of action.

The NSX-T Data Center load balancer configuration includes the following components:

- QA-LB-T1-GW-01 and QA-T0-GW-01 gateways
- QA-Web-LB load balancer (VIP 192.168.100.8)
- QA-LB-Web-Segment
- sa-qaweb-01 and sa-qaweb-02 VMs

The problem is resolved when traffic to <http://192.168.100.8> is equally distributed between the sa-qaweb-01 and sa-qaweb-02 nodes.

You log in to the Non-Production NSX Manager UI with URL <https://sa-nsxvip-02.vclass.local/login.jsp?> to confirm and resolve the reported issue.



Task 2: Confirm the Problem

You confirm a problem that was reported by the help desk: The load redistribution is not functional for the web servers when accessing the LB VIP on <http://192.168.100.8>.

1. From your student desktop, open Firefox and try to access the load balancer VIP address.

NOTE

Do not use Chrome for this task

You can use one of the following ways to access the web server VIP address:

- Go to <http://192.168.100.8>.
 - Select the **3-Tier-App > Non-Production > QA LB VIP** bookmark.
2. Record the web server IP address shown on the webpage. _____

3. Press Ctrl+F5 to force refresh the webpage.
If load balancing works, the webpage displays a different web server IP address.
4. Verify that all requests are being served from a single web server IP address.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem.

1. Use the available techniques and tools to troubleshoot and fix the problem.
 - Lecture manual for this course
 - Lab environment worksheet
 - NSX Manager and ESXi host log files
 - VMware knowledge base articles at <http://kb.vmware.com>
 - Other online technical resources
2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the connectivity to the student desktop is restored.

1. From your student desktop, open Firefox and access the web server VIP address at <http://192.168.100.8>.
2. Record the web server IP address shown on the webpage. _____
3. Press Ctrl+F5 to force refresh the webpage.

The webpage displays a different web server IP address.

Lab 29 IPSEC VPN Break-Fix Scenario

Objective and Tasks

Identify, diagnose, and resolve an NSX load balancer problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify That the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

A colleague is setting up an IPSEC VPN between the Production and Non Production sites and needs your help. The VPN Service, Local Endpoints and IPSEC session have already been created at both the Production and Non-Production sites. The problem is that the status of the IPSEC Session between the sites is Down.

2. Review details about the issue and the course of action.

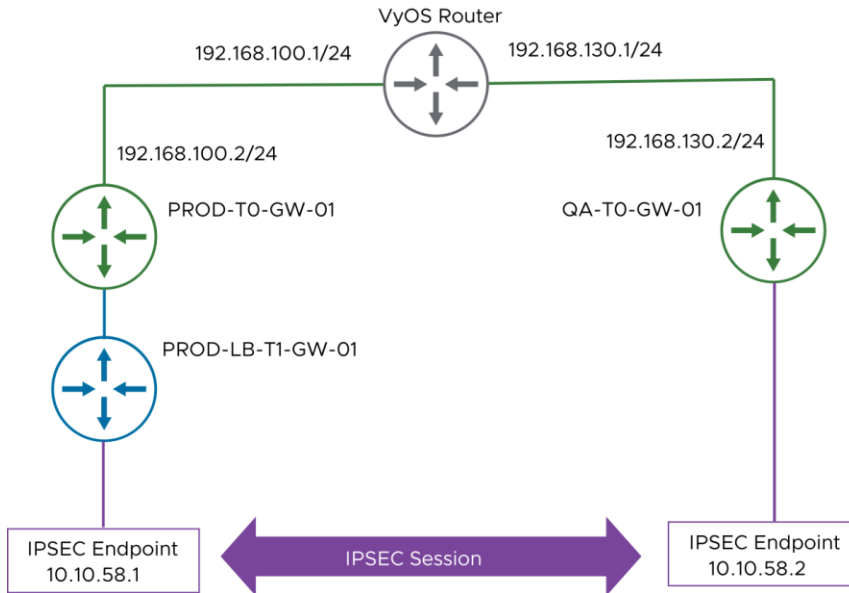
The following components are used in the scenario:

- PROD-LB-T1-GW-01 Tier-1 gateway at the production site.
- QA-TO-GW-01 Tier 0 gateway at the non-production site.

You go to <https://sa-nsxvip-02.vclass.local/login.jsp?>, log in to the Non-Production NSX UI, and fix this issue.

Do not make any changes on the Production side of the IPSEC VPN configuration.
Do not make any changes on the Tier0 and Tier 1 gateways.

The problem is resolved when the IPSEC session between the sites has the status Success.



Task 2: Confirm the Problem

You confirm a problem as reported by your colleague. The IPSEC session between the Prod and Non-Prod sites is down.

1. In Chrome, log in to Non-Production NSX UI using the **NSX-T Data Center > NSX Manager (Prod)** bookmark.
 - a. Enter **admin** as the user name and **VMware1!VMware1!** as the password.
2. Navigate to **Networking > VPN > IPSEC SESSIONS** in the NSX UI.
3. Verify that the status of **Prod-IPSEC-Session** is Down. If the status is Unknown, click the Refresh icon.

The session must not show the status Success.
4. In Chrome, log in to Non-Production NSX UI using the **NSX-T Data Center > NSX Manager (Non-Prod)** bookmark.
 - a. Enter **admin** as the user name and **VMware1!VMware1!** as the password.
5. Navigate to **Networking > VPN > IPSEC SESSIONS** in the NSX UI.

6. Verify that the status of NonProd-IPSEC-Session is Down. If the status is Unknown, click the Refresh icon.

The session must not show the status Success.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem.

1. Use the available techniques and tools to troubleshoot and fix the problem.
 - Lecture manual for this course
 - Lab environment worksheet
 - NSX Manager and ESXi host log files
 - VMware knowledge base articles at <http://kb.vmware.com>
 - Other online technical resources
2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the IPSEC VPN session is successfully established between the Production and Non-Production environments.

1. In Chrome, log in to Non-Production NSX UI using the **NSX-T Data Center > NSX Manager (Non-Prod)** bookmark.
 - a. Enter **admin** as the user name and **VMware1!VMware1!** as the password.
2. Navigate to **Networking > VPN > IPSEC SESSIONS** in the NSX UI.
3. Verify that the status of NonProd-IPSEC-Session is Success.

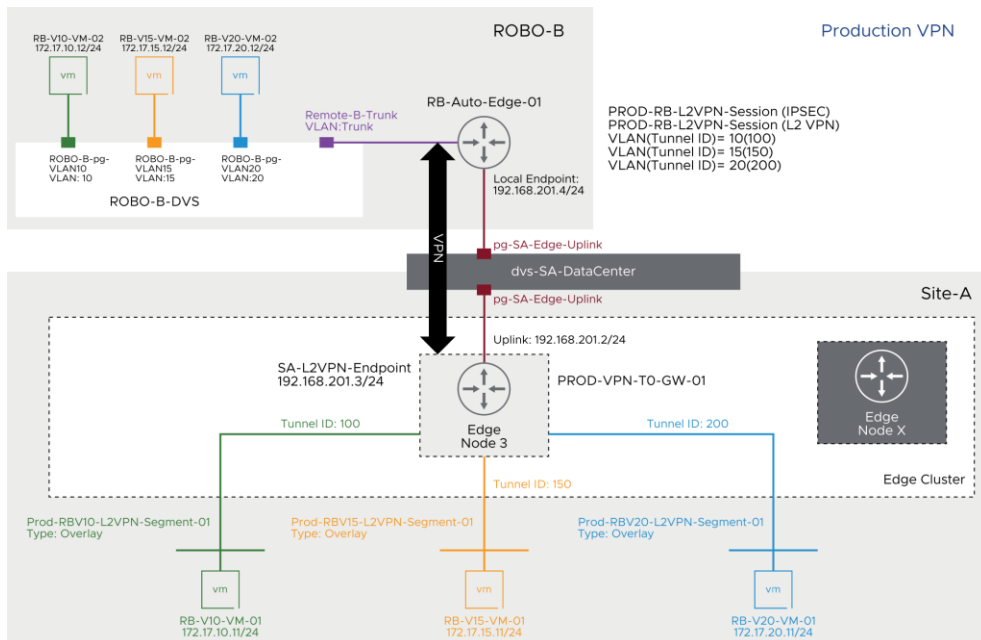
The session must not show the status Down or Unknown.

Lab 30 L2 VPN Verification

Objective and Tasks

Verify the VPN tunnel and verify the operation:

1. Prepare for the Lab
2. Verify the IPsec VPN from the NSX CLI
3. Verify the L2 VPN from the NSX CLI
4. Verify the Operation of the VPN Setup



Task 1: Prepare for the Lab

You log in to the vSphere Client UI and the NSX UI.

1. From your student desktop, log in to the vSphere Client UI.
 - a. Open Chrome.
 - b. Click the **vSphere Site A > vSphere Client (SA-VCSA-01)** bookmark.
 - c. On the login page, enter **administrator@vsphere.local** as the user name and **VMware1!** as the password.
2. Log in to the NSX UI.
 - a. Open another tab in Chrome.
 - b. Click the **NSX-T Data Center > NSX Manager (Prod)** bookmark.

NOTE

You go to <https://sa-nsxvip-01.vclass.local/login.jsp?> and log in to the Production NSX UI.

- c. On the login page, enter **admin** as the user name and **VMware1!VMware1!** as the password.

Task 2: Verify the IPsec VPN from the NSX CLI

You use the NSX CLI to verify the status and configuration of the IPsec VPN.

1. From MTPuTTY, double-click **sa-nsxedge-03** under the Production-NSX Inventory folder.

2. Disable the command-line timeout.

```
sa-nsxedge-03> set cli-timeout 0
```

3. Display the list of IPsec VPN sessions.

```
sa-nsxedge-03> get ipsecvpn session summary
```

The status of the IPsec VPN session appears with the session ID (SID). The SID can be used with other CLI commands to obtain more detailed information about the sessions.

Example:

```
sa-nsxedge-03> get ipsecvpn session summary
Version SID Compliance Suite Type Auth Status
```

```
-----
IKEv2 8193 NONE Route PSK Up
```

```
-----
SID: Session ID *: Last Known Failure
```

```
sa-nsxedge-03>
```

4. Record the IPsec VPN SID. _____
5. Query the IPsec VPN SID that you recorded.

```
sa-nsxedge-03> get ipsecvpn session sessionid <sessionid>
```

Additional session information, including details per tunnel, appear.

Example: sa-nsxedge-03> get ipsecvpn session sessionid 8193

6. Use the command output to record the values in this table in your student worksheet.

sa-nsxedge-03: IPsec Session Details

Parameter	Value
IKE Session ID (SID)	
UUID	
Type	
Session status	
Local IP	
Peer IP	
Virtual Tunnel Interface (VTI) UUID	
Tunnel status	

The UUID is referenced later.

7. From MTPuTTY, double-click **auto-edge-01** under the Production-NSX Inventory folder.

8. Disable the command-line timeout.

```
auto-edge-01> set cli-timeout 0
```

9. Display the list of IPsec VPN sessions.

```
auto-edge-01> get ipsecvpn session summary
```

The status of the IPsec VPN session with the SID appears. The SID can be used with other CLI commands to obtain more detailed information about the sessions.

10. Record the IPsec SID. _____

The SID is the same as that recorded by you earlier on the Tier-0 NSX Edge instance.

11. Query the IPsec SID that you recorded.

```
auto-edge-01> get ipsecvpn session sessionid
```

Additional session information, including details per tunnel, appear.

Example: auto-edge-01> get ipsecvpn session sessionid 8193

12. Use the command output to record the values in this table in your student worksheet.

auto-edge-01: IPsec Session Details

Parameter	Value
IKE Session ID (SID)	
UUID	
Session status	
Local IP	
Peer IP	

The local and peer IPs are reversed when compared to the values that you recorded earlier. The UUID is referenced later.

Task 3: Verify the L2 VPN from the NSX CLI

You use the NSX CLI to verify the status and configuration of the L2 VPN session.

1. From MTPuTTY, click the **sa-nsxedge-03** tab.
2. List the L2 VPN sessions.

```
sa-nsxedge-03> get l2vpn sessions
```

Example:

```
sa-nsxedge-03> get l2vpn sessions
Session : 7f40715a-b17c-4b18-bf87-1874ff5d0bc3
Tunnel : 9a389768-fc98-5e43-b1a0-2ed387b89de2
IPSec Session : 30ca37c6-8c3d-485a-a979-effce6b776c
Status : UP
sa-nsxedge-03>
```

The status of L2 VPN sessions appears with the associated session, tunnel, and IPsec UUIDs. These values can be used with other CLI commands to obtain more detailed information about the sessions.

3. Display the configuration of the L2 VPN sessions.

```
sa-nsxedge-03> get l2vpn sessions config
```

Additional session information, including details about the transport tunnels, appears.

4. Use the command output to record the values in this table in your student worksheet.

sa-nsxedge-03: L2 VPN Session Details

Parameter	Value
DISPLAY_NAME	
ID (session ID)	
IPSEC_VPN_SESSION_ID	
TUNNEL ENCAPSULATION PROTOCOL	

5. Verify that the IPsec VPN session ID that you recorded matches the UUID that you recorded in the previous task for the NSX Edge IPsec session details.
6. Display information about the L2 VPN session's logical-switches:

```
sa-nsxedge-03> get l2vpn session <uuid> logical-switches
```

The switches, port, and tunnel UUIDs, as well as the VNI and tunnel ID used by this VPN, appear.

The UUID is the L2 VPN Session ID that you recorded earlier. If needed, use the `get l2vpn sessions` command to obtain it again.

Example: `sa-nsxedge-03> get l2vpn session 7f40715a-b17c-4b18-bf87-1874ff5d0bc3 logical-switches`

7. Use the command output to update this table, with the VNI and tunnel ID values, in your student worksheet.

sa-nsxedge-03: L2 VPN VNI and Tunnel Details

VNI	Tunnel ID

8. From MTPuTTY, click the **auto-edge-01** tab.

9. Display the configuration of the L2 VPN sessions.

```
auto-edge-01> get l2vpn sessions config
```

Session information, including details about the transport tunnels, appears.

10. Use the command output to record the values in this table in your student worksheet.

auto-edge-01: L2 VPN Session Details

Parameter	Value
DISPLAY_NAME	
ID (session ID)	
IPSEC_VPN_SESSION_ID	
TUNNEL ENCAPSULATION PROTOCOL	

11. Verify that the IPsec session ID that you recorded matches the UUID that you recorded in the previous task for the Autonomous Edge IPsec session details.
12. Display information about the L2 VPN session's logical-switch.

```
auto-edge-01> get l2vpn session <uuid> logical-switches
```

The switch, port, and tunnel UUIDs, as well as VNI and tunnel ID used by this VPN, appear.

The UUID is the L2 VPN Session ID that you recorded earlier. If needed, use the `get l2vpn sessions` command to obtain it again.

Example: `auto-edge-01> get l2vpn session ed3e5342-2206-43cd-895c-1a7cb739c68b logical-switches`

13. Use the command output to update the table in your student worksheet with the VLAN and tunnel ID values.

auto-edge-01: L2 VPN VLAN and Tunnel Details (Part 2)

VLAN	Tunnel ID

14. Verify that tunnel ID 100 is present in the output you recorded on both auto-edge-01 and sa-nsxedge-03.

As per the topology at the beginning of this lab, tunnel 100 is used in the configuration of the VPN that connects the RB-V10-VM-01 and RB-V10-VM-02 virtual machines.

Task 4: Verify the Operation of the VPN Setup

You verify the proper operation of the VPN tunnel deployed by opening consoles to the two L2 VPN VMs and by using ping to reach across the VPN.

1. In the NSX UI, navigate to **Networking > Network Services > VPN > L2 VPN SESSIONS**.
2. Verify that the status of PROD-RB-L2VPN-Session is Success.
3. Click the Information icon beside the status for L2VPN-Session to display additional information about the tunnel status.

Both the tunnel and IKE status are Up.
4. In the vSphere Client inventory, ensure that RB-Auto-Edge-01 and RB-V10-VM-02 are running on the sa-esxi-02.vclass.local ESXi host.
 - a. Under Hosts and Clusters view, expand **Datacenter-01-Production > Management-Edge-Cluster-01 > ROBO-B**.
 - b. Verify that both the NSX Autonomous Edge (RB-Auto-Edge-01) and the RB-V10-VM-02 virtual machines reside on the sa-esxi-02.vclass.local ESXi host.
 - c. (Optional) If the virtual machines do not reside on the ESXi host, use vSphere vMotion to migrate the VMs.
5. In the vSphere Client, verify the network connectivity of RB-V10-VM-02.
 - a. Under Hosts and Clusters view, expand **Datacenter-01-Production > Management-Edge-Cluster-01 > ROBO-B**.
 - b. Right-click **RB-V10-VM-02** and select **Edit Settings**.
 - c. Verify that Network adapter 1 has the ROBO-B-pg-VLAN-10 value and is connected.
 - d. (Optional) Click **Browse**, select **ROBO-B-pg-VLAN-10** from the drop-down menu, and click **OK**.

6. In the vSphere Client, verify the network connectivity of RB-V10-VM-01.
 - a. Under Hosts and Clusters view, expand **Datacenter-01-Production > Prod-Compute-Cluster-01 > Prod-VPN**.
 - b. Right-click the **RB-V10-VM-01** virtual machine and select **Edit Settings**.
 - c. Verify that Network adapter 1 has the **Prod-RBV10-L2VPN-Segment-01** value and is connected
 - d. (Optional) Click **Browse**, select **Prod-RBV10-L2VPN-Segment-01** from the drop-down menu, and click **OK**.
7. In the vSphere Client, open a web console to RB-V10-VM-01.
8. Log in to the RB-V10-VM-01 VM with **root** as the user name and **VMware1!** as the password .
9. Verify connectivity with RB-V10-VM-02.

```
ping -c 3 172.17.10.12
```

The ping completes successfully.
10. Return to the vSphere Client and open a web console to RB-V10-VM-02.
11. Log in to the RB-V10-VM-02 VM with **root** as the user name and **VMware1!** as the password .
12. Verify bidirectional connectivity from RB-V10-VM-02 to RB-V10-VM-01.

```
ping -c 3 172.17.10.11
```

The ping completes successfully. You verified bidirectional communication between the two VMs at the end of the VPN tunnel.

Lab 31 L2 VPN Break-Fix Scenario

Objective and Tasks

Identify, diagnose, and resolve an NSX load balancer problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify That the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

After a recent change in the configuration of the Production L2 VPN, users reported that the RB-V15-VM-01 virtual machine is unable to communicate with the RB-V15-VM-02 virtual machine at the remote site. You must identify and resolve the issue.

IMPORTANT

A single L2 VPN session carries traffic with more than one tunnel ID. Changes that you make must not affect traffic from other virtual machines.

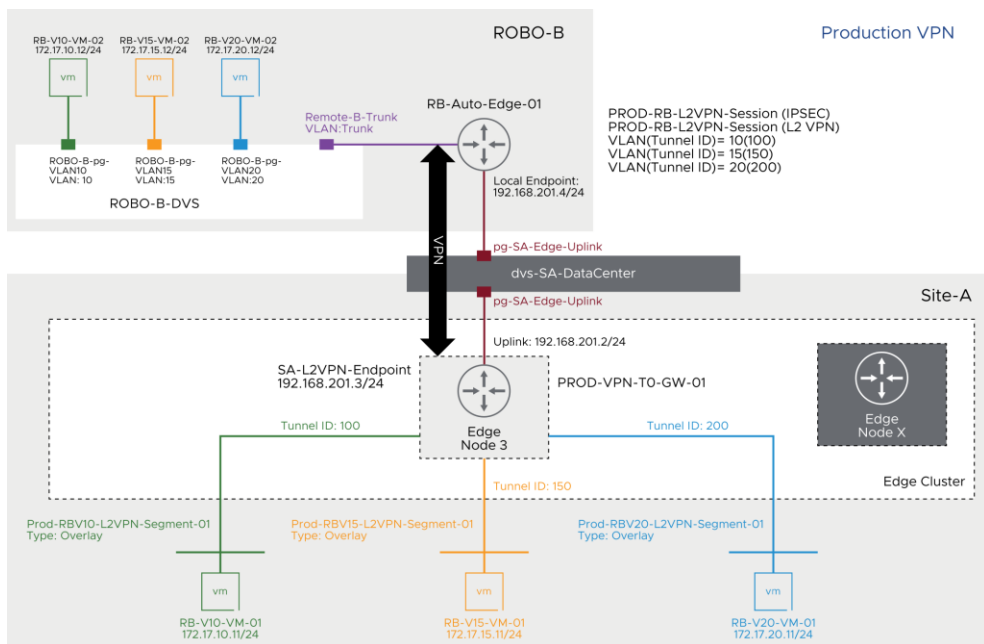
2. Review details about the issue and the course of action.

The following components are used in the scenario:

- Local Site-A and remote site ROBO-B
- PROD-VPN-T0-GW-01 Tier-0 gateway and RB-Auto-Edge-01 Autonomous Edge
- Prod RBV15-L2VPN-Segment-01 segment and ROBO-B-pg-VLAN15 port group
- RB-V15-VM-01 and RB-V15-VM-02 virtual machines

You go to <https://sa-nsxvip-01.vclass.local/login.jsp?>, log in to the Production NSX UI, and fix this issue.

The problem is resolved when you can ping RB-V15-VM-02 (172.17.15.12) from RB-V15-VM-01 (172.17.15.11).



Task 2: Confirm the Problem

You confirm a problem that was reported by the help desk: The RB-V15-VM-01 virtual machine is unable to ping the RB-V15-VM-02 virtual machine at the remote site.

1. In Chrome, log in to vCenter Server with the vSphere Client.
2. Enter **administrator@vsphere.local** as the user name and **VMware1!** as the password.
3. Expand **Datacenter-01-Production > Prod-Compute-Cluster-01 > Prod-VPN** in the vCenter Server inventory.
4. In the Navigator pane, click **RB-V15-VM-01** and select **Launch Web Console** on the virtual machine summary page.
5. Log in to the RB-V15-VM-01 VM by entering **root** as the user name and **VMware1!** as the password.
6. At the command prompt, ping the remote network.

```
ping -c 3 172.17.15.12
```

The ping command must not be successful.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem.

1. Use the available techniques and tools to troubleshoot and fix the problem.
 - Lecture manual for this course
 - Lab environment worksheet
 - NSX Manager and ESXi host log files
 - VMware knowledge base articles at <http://kb.vmware.com>
 - Other online technical resources
2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the connectivity to the remote RB-V15-VM-01 virtual machine is restored.

1. At the RB-V15-VM-01 command prompt, test the connectivity.

```
ping -c 3 172.17.15.12
```

Lab 32 L2 VPN Challenge Scenario

Objective and Tasks

Identify, diagnose, and resolve an NSX load balancer problem:

1. Read the Scenario Description
2. Confirm the Problem
3. Troubleshoot and Fix the Problem
4. Verify That the Problem Is Fixed

Task 1: Read the Scenario Description

You read the scenario description and determine the course of action.

1. Read the scenario description.

After a recent change in the configuration of the Production VPN, users reported that the RB-V20-VM-01 virtual machine is unable to communicate with the RB-V20-VM-02 virtual machine at the remote site. You must identify and resolve the issue.

IMPORTANT

A single L2 VPN session carries traffic with more than one tunnel ID. Changes that you make must not affect traffic from other virtual machines.

The following components are used in the scenario:

- The problem is resolved when you can ping RB-V20-VM-02 (172.17.20.12) from RB-V20-VM-01 (172.17.20.11).



Task 2: Confirm the Problem

You confirm a problem that was reported by the help desk: The RB-V20-VM-01 virtual machine is unable to ping the RB-V20-VM-02 virtual machine at the remote site.

1. In Chrome, log in to vCenter Server with the vSphere Client.
2. Enter **administrator@vsphere.local** as the user name and **VMware1!** as the password.
3. Expand **Datacenter-01-Production > Prod-Compute-Cluster-01 > Prod-VPN** in the vCenter Server inventory.
4. In the Navigator pane, click **RB-V20-VM-01** and select **Launch Web Console** on the virtual machine summary page.
5. Log in to the RB-V20-VM-01 VM by entering **root** as the user name and **VMware1!** as the password.
6. At the command prompt, ping the remote network.

```
ping -c 3 172.17.20.12
```

The ping command must not be successful.

Task 3: Troubleshoot and Fix the Problem

You use the techniques and tools acquired in the course to troubleshoot and fix the problem .

1. Use the available techniques and tools to troubleshoot and fix the problem.
 - Lecture manual for this course
 - Lab environment worksheet
 - NSX Manager and ESXi host log files
 - VMware knowledge base articles at <http://kb.vmware.com>
 - Other online technical resources
2. If you cannot fix the problem, ask your instructor for help.

Task 4: Verify That the Problem Is Fixed

You verify that the connectivity to the remote virtual machine RB-V20-VM-02 is restored.

1. At the RB-V20-VM-01 command prompt, test the connectivity.

```
ping -c 3 172.17.20.12
```

Lab 33 Datapath Troubleshooting for the E-W Packet Capture

Objective and Tasks

Troubleshoot the E-W packet capture:

1. Use Traceflow
2. Perform Data Collection for Packet Capture
3. Perform Packet Capture

Task 1: Use Traceflow

1. Open **Chrome** browser from the taskbar > Click on **NSX-T Data Center** folder > Click **NSX Manager (Prod)** bookmark
2. Log in to the NSX Manager with admin as username and VMware1!VMware1! as password
3. Click on **Plan & Troubleshoot**
4. Click on **Traceflow**
5. On the **Traceflow** tab, configure the VM details.
 - a. In the main pane, configure the details.

Option	Action
IP Address	Select IPv4 .
Traffic Type	Select Unicast (default).
Protocol Type	Select ICMP (default).

b. In the Source pane, configure the source VM details.

Option	Action
Type	Select Virtual Machine (default).
VM Name	Select sa-web-01 .
Virtual Interface	Select Network adapter 1 (default).

c. In the Destination pane, configure the destination VM details.

Option	Action
Type	Select Virtual Machine .
VM Name	Select sa-app-01
Virtual Interface	Select Network adapter 1 (default).

6. Click **TRACE**
7. From the Traceflow observations window record the requested details in the table.

Traceflow Observations

Question	Answer
What is the ESXi Host Name on which sa-web-01 VM is running?	
What is the distributed firewall rule (ID) applied to vNIC?	
What is the segment name to which VM is Connected?	
What is the VNI ID of a segment?	
What is the Tier-1 gateway name to which the segment is connected?	
What is the logical switch VNI ID that connects the Prod-App-Segment to the Tier1 gateway?	

What is the sa-esxi-04.vclass.local local endpoint IP address ?

What is the sa-esxi-04.vclass.local Remote endpoint IP address ?

What is the distributed firewall rule # applied to sa-app-01 virtual Interface?

What the Interface name that delivered the packet to destination?

Task 2: Perform Data Collection for Packet Capture

In this task, you will use the commands to query the information about sa-web-01, sa-esxi-04 and sa-app-01 and sa-esxi-05 through the CLI and GUI.

1. Record the IP address, MAC address and ESXi host details of the **sa-web-01 VM** from the vSphere Client.
 - a. Log in to the vSphere Client with `administrator@vsphere.local` as username and `VMware1!` as password.
 - b. Expand **DataCenter-01-Production** > Expand **Prod-Compute-Cluster-01** cluster > Expand **Prod-Web-App** resource pool.
 - c. Click on **sa-web-01 VM** and then click on **Summary** tab

Record the following details of sa-web-01 VM in the Value column

sa-web-01 details from vSphere Client

Parameter	Value
IP Address	
MAC Address	
Host	

2. Record the **sa-web-01** VM port number, Client name, MAC and uplink details from the **sa-ESXi-04** host command line:

- a. Open **MTPuTTY** from the taskbar and Expand **Production-Infrastructure** folder from bookmarks and double-click on **SA-ESXi-04**

- b. On sa-esxi-04 host, run the following command to list the ports

```
[root@sa-esxi-04:~] nsxcli --cmd get ports
```

sa-web-01 details from sa-esxi-04 command line.

Parameter	Client	MAC	Uplink
sa-web-01			
vdrport			
vmk10			
vmk50			

3. On the sa-esxi-04 host, run the following command to collect the dvFilter name of sa-web-01 virtual machine.

```
[root@sa-esxi-04:~] summarize-dvfilter | grep -A5 sa-web-01
```

Identify dvFilter Name of sa-web-01

Parameter	Value
dvFilter Name	

4. On the sa-esxi-04 host, run the following command to collect the host switch uplink Information:

```
[root@sa-esxi-04:~] esxcfg-vswitch -l
```

sa-esxi-04 host uplink configuration information

vSwitch Name	Uplinks
Prod-Overlay-NVDS	

5. On the sa-esxi-04 host, run the following command to find the local TEP IP of an ESXi host:

```
[root@sa-esxi-04:~] nsxcli --cmd get host-switch Prod-Overlay-NVDS tunnels
```

From the command output, record the Local IP address, which is the TEP IP of an ESXi host.

Example:

```
[root@sa-esxi-04:~] nsxcli --cmd get host-switch Prod-Overlay-NVDS tunnels
```

6. On the sa-esxi-04 host, run the following command to record the sa-ESXi-04 host VMKernel IP address Information

```
[root@sa-esxi-04:~] esxcfg-vmknic -l
```

sa-esxi-04 host VMKernel information

VMKernel	IP Address	MAC Address
vmk0 (Management)		
vmk10 (TEP interface)		
vmk50 (hyperbus interface)		

7. Record the IP address, MAC address and ESXi host details of the sa-app-01 VM from the vSphere Client.

- a. Expand **DataCenter-01-Production** > Expand **Prod-Compute-Cluster-01** cluster > Expand **Prod-Web-App** resource pool

- b. Click on **sa-app-01 VM** and then click on **Summary** tab

Record the following details of sa-app-01 VM in the Value column

sa-app-01 details from vSphere Client

Parameter	Value
IP Address	
MAC Address	
Host	

8. Record the sa-app-01 VM port number, Client name, MAC and uplink details from the sa-ESXi-05 host command line:
 - a. Open **MTPuTTY** from the taskbar and Expand **Production-Infrastructure** folder from bookmarks and double-click on **SA-ESXi-05**
 - b. On the **sa-esxi-05** host, run the following command to list the ports:

```
[root@sa-esxi-05:~] nsxcli --cmd get ports
```

sa-app-01 details from sa-esxi-05 command line.

Parameter	PortNum	Client	MAC	Uplink
sa-app-01				
vdrport				
vmk10				
vmk50				

9. On the **sa-esxi-05** host, run the following command to collect the dvFilter name of **sa-app-01** virtual machine.

```
[root@sa-esxi-05:~] summarize-dvfilter | grep -A5 sa-app-01
```

Identify dvFilter Name of sa-app-01

Parameter	Value
dvFilter Name	

10. Record the hostswitch uplink Information from sa-esxi-05 command line:
 - a. From the sa-esxi-05 command line, run the following command:

```
[root@sa-esxi-05:~] esxcfg-vswitch -l
```

sa-esxi-04 host uplink configuration information

vSwitch Name	Uplinks
Prod-Overlay-NVDS	

11. Run the following command to find the Local TEP IP of an ESXi host:

```
[root@sa-esxi-05:~] nsxcli --cmd get host-switch Prod-Overlay-NVDS tunnels
```

From the command output, record the Local IP address, which is the TEP IP of an ESXi host.

Example:

```
[root@sa-esxi-05:~] nsxcli --cmd get host-switch Prod-Overlay-NVDS tunnels
```

12. Record the sa-ESXi-05 host VMKernel IP address Information from command line:

- a. Run the following command to collect the VMKernel IP and MAC address information:

```
[root@sa-esxi-05:~] esxconfig-vmknic -l
```

sa-esxi-05 host VMKernel information

VMKernel	IP Address	MAC Address
vmk0 (Management)		
vmk10 (TEP interface)		
vmk50 (hyperbus interface)		

Task 3: Perform Packet Capture

You use the nsxcli commands to capture and analyze the ICMP traffic between sa-web-01 and sa-app-01 and sa-esxi-04 and sa-esxi-05 hosts.

1. Log in to the **sa-web-01** console from the vSphere Client.
 - a. Open the Chrome browser from the taskbar and click **vSphere Client**.
 - b. Log in to vCenter Server by entering username **administrator@vsphere.local** and **VMware1!** as password
 - c. Locate the **sa-web-01** VM from the **Prod-Compute-Cluster-01** cluster.
 - d. Select **sa-web-01** and from the virtual machine summary page, select **Launch Web Console**.
 - e. Log in to the **sa-web-01** VM by entering user name **root** and password **VMware1!**.

2. Run the ping command to initiate a ping from sa-web-01 to 172.20.10.10 IP address.
 - a. From the sa-web-01 VM command line, run the following command.
sa-web-01:~# ping 172.16.20.11

Leave the ping command open, do not interrupt the ping.

3. Open **MTPuTTY** and double-click **SA-ESXi-04** to connect through SSH client where **sa-web-01** VM is running on it.
4. On the sa-esxi-04, run the following command to enter into the nsxcli command line.

```
[root@sa-esxi-04:~] nsxcli
```

5. On the sa-esxi-04, run the following command to check the possible options available with the start capture command

```
sa-esxi-04.vclass.local> start capture <Press-Return-KEY>
% Command not found: start capture
```

Possible alternatives:

```
start capture dvfilter <esx-dvfilter-name>
start capture interface <interface-name> [direction
<direction>] [file <filename>] [count <packet-count>]
[expression <expression>]
start capture trace
```

You will use these command options in this lab task to capture the traffic.

6. On sa-esxi-04 host, run the following command to capture the VMs traffic with the sa-web-01 Client name.

You will use the sa-web-01 client name that you have collected in **Task 2 Step 2** .

```
sa-esxi-04.vclass.local> start capture interface <sa-web-01-
client-name> direction input expression ipproto 0x01
```

Example:

```
sa-esxi-04.vclass.local> start capture interface sa-web-
01.eth0 direction input expression ipproto 0x01
```

- a. After 5 seconds, press CTRL+C to stop the packet capture.

Record the "ICMP echo request" details from the packet capture to understand the source and destination details.

Packet Capture at the vNIC of the sa-web-01 VM

Parameter	Value
Source MAC	
Destination MAC	
Source IP	
Destination IP	

7. On sa-esxi-04 host, run the following command to capture sa-web-01 VM traffic on an ESXi host before the dvfilter is applied to the vNIC of a VM.

You will use the dvfilter name of the VM that you have collected in **Task 2 Step 3**.

```
sa-esxi-04.vclass.local> start capture dvfilter <dvfilter-name>
stage pre expression ipproto 0x01
```

Example:

```
sa-esxi-04.vclass.local> start capture dvfilter nic-266104-
eth0-vmware-sfw.2 stage pre expression ipproto 0x01
```

Packet Capture Before the dvFilter is Applied to the vNIC of sa-web-01 VM

Parameter	Value
Source MAC	
Destination MAC	
Source IP	
Destination IP	

- a. After 5 seconds, press CTRL+C to stop the packet capture.

Record the "ICMP echo request" details from the packet capture to understand the source and destination details.

8. On sa-esxi-04, run the following command to capture sa-web-01 VM traffic on an ESXi host after the dvfilter is applied to the vNIC of a VM.

You will use the sa-web-01 dvfilter name that you have collected in **Task 2 Step 3**.

```
sa-esxi-04.vclass.local> start capture dvfilter <sa-web-01-  
dvfilter-name> stage post expression ipproto 0x01
```

Example:

```
sa-esxi-04.vclass.local> start capture dvfilter nic-266104-  
eth0-vmware-sfw.2 stage post expression ipproto 0x01
```

- a. After 5 seconds, press CTRL+C to stop the packet capture.

Record the "ICMP echo request" details from the packet capture to understand the source and destination details.

Packet Capture After the dvFilter is Applied to the vNIC of sa-web-01 VM

Parameter	Value
Source MAC	
Destination MAC	
Source IP	
Destination IP	

9. On sa-esxi-04, run the following command to capture the VMs traffic at the vdrport.

You will use the vdrport client name that you have recorded in the **Task 2 Step 2**

```
sa-esxi-04.vclass.local> start capture interface <vdrPort-  
Client-name> expression ipproto 0x01
```

Example:

```
sa-esxi-04.vclass.local> start capture interface vdr-vdrPort  
expression ipproto 0x01
```

- a. After 5 seconds, press CTRL+C to stop the packet capture.

Record the "ICMP echo request" details from the packet capture to understand the source and destination details.

Packet capture at the vdrPort On sa-esxi-04 Host

Parameter	Value
Source MAC	
Destination MAC	
Source IP	
Destination IP	

10. On sa-esxi-04, run the following command to capture the egress traffic at the ESXi host N-VDS uplink interface.

You will use the Prod-Overlay-NVDS uplink interface that you have collected in **Task 2 Step 4**.

For the sa-app-01 ESXi host TEP IP refer to the **Task 2 Step 7**.

```
sa-esxi-04.vclass.local> start capture interface <Prod-Overlay-NVDS-Uplink> direction output expression ip <sa-app-01-ESXi-Host>
```

Example:

```
sa-esxi-04.vclass.local> start capture interface vmnic4 direction output expression ip 172.20.11.154
```

- a. After 5 seconds, press CTRL+C to interrupt the packet capture.

Record the "ICMP echo request" details from the packet capture to understand the source and destination details.

Packet Capture at the Uplink on sa-esxi-04 host

Parameter	Value
Outer MAC Header Source	
Outer MAC Header Destination	
Outer IP Header Source	
Outer IP Header Destination	
Destination Port	
Destination VM's VNI	
Inner MAC Address Source	
Inner MAC Address Destination	
Inner Source IP	
Inner Destination IP	

- 11. From **MTPuTTY** window click on the **SA-ESXi-05** tab

If the **SA-ESXi-05** is closed, you can locate the **SA-ESXi-05** under the **Production-Infrastructure** folder in the MTPuTTY bookmarks.

- a. Run the following command to enter the nsxcli command line.

```
[root@sa-esxi-05:~] nsxcli
```

12. On the sa-esxi-05 host, run the following command to capture the ingress traffic at the ESXi host N-VDS uplink interface.

You will use the Prod-Overlay-NVDS uplink interface that you have collected in **Task 2 Step 10**.

For the sa-web-01 ESXi host TEP IP refer to the **Task 2 Step 6**.

```
sa-esxi-05.vclass.local> start capture interface <Prod-Overlay-NVDS-Uplink> direction output expression ip <sa-web-01-ESXi-Host>
```

Example:

```
sa-esxi-05.vclass.local> start capture interface vmnic4 direction input expression ip 172.20.11.153
```

- a. After 5 seconds, press CTRL+C to interrupt the packet capture.

Record the "ICMP echo request" details from the packet capture to understand the source and destination details.

Packet Capture at the Uplink on sa-esxi-05 host

Parameter	Value
Outer MAC Header Source	
Outer MAC Header Destination	
Outer IP Header Source	
Outer IP Header Destination	
Destination Port	
Destination VM's VNI	
Inner MAC Address Source	
Inner MAC Address Destination	
Inner Source IP	
Inner Destination IP	

13. Run the following command to capture the VMs traffic at the switchport.

You will use the sa-app-01 PortNum that you have recorded in the **Task 2 Step 8**

```
sa-esxi-05.vclass.local> start capture interface <sa-app-01-PortNum> direction output expression ipproto 0x01
```

Example:

```
sa-esxi-05.vclass.local> start capture interface 100663328  
direction output expression ipproto 0x01
```

- a. After 5 seconds, press CTRL+C to stop the packet capture.

Record the "ICMP echo request" details from the packet capture to understand the source and destination details.

Packet Capture at the Switch Port of sa-app-01 VM

Parameter	Value
Source MAC	
Destination MAC	
Source IP	
Destination IP	

14. Run the following command to capture VMs traffic on an ESXi host before the dvfilter applied to the vNIC of a VM.

You will use the dvfilter name of the VM that you have collected in **Task 2 Step 9**.

```
sa-esxi-05.vclass.local> start capture dvfilter <sa-app-01-  
dvfilter-name> stage pre expression ipproto 0x01
```

Example:

```
sa-esxi-05.vclass.local> start capture dvfilter nic-266109-  
eth0-vmware-sfw.2 stage pre expression ipproto 0x01
```

Packet Capture Before the dvFilter is Applied to the vNIC of sa-app-01 VM

Parameter	Value
Source MAC	
Destination MAC	
Source IP	
Destination IP	

- a. After 5 seconds, press CTRL+C to stop the packet capture.

Record the "ICMP echo request" details from the packet capture to understand the source and destination details.

15. Run the following command to capture VMs traffic on an ESXi host before the dvfilter applied to the vNIC of a VM.

You will use the dvfilter name of the VM that you have collected in **Task 2 Step 9**.

```
sa-esxi-05.vclass.local> start capture dvfilter <sa-app-01-  
dvfilter-name> stage post expression ipproto 0x01
```

Example:

```
sa-esxi-05.vclass.local> start capture dvfilter nic-266109-  
eth0-vmware-sfw.2 stage post expression ipproto 0x01
```

Packet Capture After the dvFilter is Applied to the vNIC of sa-app-01 VM

Parameter	Value
Source MAC	
Destination MAC	
Source IP	
Destination IP	

- a. After 5 seconds, press CTRL+C to stop the packet capture.

Record the "ICMP echo request" details from the packet capture to understand the source and destination details.

16. Run the following command to capture VMs traffic on an ESXi host before the dvfilter applied to the vNIC of a VM.

You will use the sa-app-01 client name to capture the outgoing traffic at the vNIC of the VM

```
sa-esxi-05.vclass.local> start capture interface <sa-app-01-  
client-name> direction output expression ipproto 0x01
```

Example:

```
sa-esxi-05.vclass.local> start capture interface sa-app-  
01.eth0 direction output expression ipproto 0x01
```

Packet Capture at the vNIC of sa-app-01 VM

Parameter	Value
Source MAC	
Destination MAC	
Source IP	
Destination IP	

- a. After 5 seconds, press CTRL+C to stop the packet capture.

Record the "ICMP echo request" details from the packet capture to understand the source and destination details.

- 17. Stop the ping to 172.16.20.11 IP address.

- a. Open **sa-web-01** VM console from vSphere Client.
- b. Press CTRL +C to stop the ping to 172.16.20.11

Lab 34 Datapath Troubleshooting for the N-S Packet Capture

Objective and Tasks

Troubleshoot the N-S packet capture:

1. Use Traceflow
2. Perform Data Collection for Packet Capture
3. Perform Packet Capture

Task 1: Use Traceflow

1. Open **Chrome** browser from the taskbar > Click on **NSX-T Data Center** folder > Click **NSX Manager (Prod)** bookmark
2. Log in to the NSX Manager with admin as username and VMware1!VMware1! as password
3. Click on **Plan & Troubleshoot**
4. Click on **Traceflow**
5. On the **Traceflow** tab, configure the VM details.
 - a. In the main pane, configure the details.

Option	Action
IP Address	Select IPv4 .
Traffic Type	Select Unicast (default).
Protocol Type	Select ICMP (default).

- b. In the Source pane, configure the source VM details.

Option	Action
Type	Select Virtual Machine (default).
VM Name	Select sa-web-01 .
Virtual Interface	Select Network adapter 1 (default).

- c. In the Destination pane, configure the destination VM details.

Option	Action
Type	Select IP-MAC .
Layer	Layer 3
IP Address	172.20.10.10

6. Click **TRACE**
7. From the Traceflow observations window record the requested details in the table.

Traceflow Observations

Question	Answer
What is the ESXi Host Name on which sa-web-01 VM is running?	
What is the distributed firewall rules (ID) applied to vNIC?	
What is the segment name to which VM is Connected?	
What is the VNI ID of the segment?	
What is the Tier-1 gateway name to which the segment is connected?	
What is the transit logical switch VNI ID that connects the Tier1 gateway with Tier-0 gateway?	
What is the Tier-1 gateway logical router port connecting to the Tier-0 Gateway?	
What is the Tier-0 gateway logical router port connecting to the Tier-0 Gateway?	
What is the ESXi host local endpoint IP address (TEP IP Address)?	

What is the NSX Edge End Point IP Address?

What is the Interface on the Edge to which the gateway firewall rules are applied?

What is the firewall rule ID applied to Interface?

What the Interface name that delivered the packet to destination?

Task 2: Perform Data Collection for Packet Capture

In this lab task, you will record the sa-web-01, sa-esxi-04, sa-nsxedge-02 and sa-esxi-02 details and use them in the upcoming lab tasks to perform the packet capture.

1. Record the IP address, MAC address and ESXi host details of the sa-web-01 VM from the vSphere Client.
 - a. Log in to the vSphere Client with `administrator@vsphere.local` as username and `VMware1!` as password.
 - b. Expand **DataCenter-01-Production** > Expand **Prod-Compute-Cluster-01** cluster > Expand **Prod-Web-App** resource pool
 - c. Click on **sa-web-01 VM** and then click on **Summary** tab

Record the following details of sa-web-01 VM in the following table.

sa-web-01 details from vSphere Client

Parameter	Value
IP Address	
MAC Address	
Host	

2. From the sa-esxi-04 host command line, record the sa-web-01 VM port number, Client name, MAC and uplink details.
 - a. Open **MTPuTTY** from the taskbar and Expand **Production-Infrastructure** folder from bookmarks and double-click on **SA-ESXi-04**
 - b. Run the following command to list the ports

```
[root@sa-esxi-04:~] nsxcli --cmd get ports
```

c. <Optional> Run the following command to query the N-VDS ports information:

```
[root@sa-esxi-04:~] nsxdep-cli vswitch instance list  
sa-web-01 details from sa-esxi-04 command line.
```

Parameter	PortNum	Client	MAC	Uplink
sa-web-01				
vdrport				
vmk10				
vmk50				

3. On the sa-esxi-04 host, run the following command to collect the dvFilter name of sa-web-01 virtual machine.

```
[root@sa-esxi-04:~] summarize-dvfilter | grep -A5 sa-web-01
```

Identify dvFilter Name of sa-web-01

Parameter	Value
dvFilter Name	

4. On the sa-esxi-04 host, run the following command to record the host switch uplink Information :

```
[root@sa-esxi-04:~] esxcfg-vswitch -l
```

sa-esxi-04 host uplink configuration information

vSwitch Name	Uplinks
Prod-Overlay-NVDS	

- On the sa-esxi-04 host, run the following command to find the Local TEP IP of an ESXi host:

```
[root@sa-esxi-04:~] nsxcli --cmd get host-switch Prod-Overlay-NVDS tunnels
```

From the command output, record the Local IP address, which is the TEP IP of an ESXi host.

sa-esxi-04 host TEP IP

Parameter	Value
Local TEP IP	

- On the sa-esxi-04 host, run the following command to record the VMkernel IP address Information:

```
[root@sa-esxi-04:~] esxcfg-vmknic -l
```

sa-esxi-04 host VMKernel information

VMKernel	IP Address	MAC Address
vmk0 (Management)		
vmk10 (TEP interface)		
vmk50 (hyperbus interface)		

- Open **MTPuTTY** from the taskbar and Expand **Production-NSX Inventory** folder from bookmarks and double-click on **sa-nsxedge-02**
- On sa-nsxedge-02, run the following command to list the local TEP IP address.

```
sa-nsxedge-02> get vteps
```

From the command output record the **Local VTEP IP** address.

sa-nsxedge-02 TEP IP

Parameter	Value
Local VTEP IP	

9. On sa-nsxedge-02, run the following command to list the logical routers:

```
sa-nsxedge-02> get logical-routers
```

From the command output, you can see that the VRF 0 is the TUNNEL.

- a. Run the following command to enter into the Tunnel vrf context:

```
sa-nsxedge-02> vrf 0
```

- b. Run the following command to list interfaces on the TUNNEL vrf context.

```
sa-nsxedge-01(vrf)> get interfaces
```

From the command output, you can see IP/Mask 172.20.11.156/24 is assigned to the port-type called uplink.

To monitor and capture the traffic going through the NSX Edge tunnels, you use the uplink interface uuid . The uplink interface IP address is the NSX Edge TEP IP address.

NSX Edge TEP Interface Details

Parameter	Value
Interface	
Port-type	
IP/Mask	
MAC	
MTU	

- c. Type exit to exit from the vrf context.

```
sa-nsxedge-02(vrf)> exit
```

10. On sa-nsxedge-02, run the following command to list the gateway firewall interfaces

```
sa-nsxedge-02> get firewall interfaces
```

NSX Edge Uplink Interface "Uplink-02-Intf" Details

Parameter	Value
Interface	
Type	
Name	Uplink-02-Intf
VRF ID	
Context name	

11. On sa-nsxedge-02, run the following command to list the logical-router port interface UUID, name, IP, MAC and RX/TX packets

```
sa-nsxedge-02> get logical-router interface stats | find  
name | IP/ | MAC | interface | -Packets
```

NSX Edge Uplink Interface "Uplink-02-Intf" Details

Parameter	Value
Uplink interface UUID	
Name	
IP/Mask	
MAC Address	

12. On the sa-nsxedge-02, run the following command to list the logical-router port UUID for the Prod-T0-GW-01 Tier-1 gateway.

- a. Run the following command to list the logical routers

```
sa-nsxedge-02> get logical-routers
```

From the command output, identity the vrf ID of SR-Prod-T0-GW-01 gateway.

- b. Run the following command to enter into the SR vrf context.

```
sa-nsxedge-02> vrf <vrf-id-of-SR-Prod-T0-GW-01>
```

example:

```
sa-nsxedge-02> vrf 2
```

- c. Run the following command to identify the backplane interface details.

```
sa-nsxedge-02(tier0_sr)> get interfaces
```

From the command output record the details of the backplane "bp-sr1-port" port in the following table.

Uplink port details

Parameter	Value
Uplink interface UUID	
IfUid	
Port-type	
IP/Mask	
MAC	
VNI	

- d. Type `exit` to exit from the Tier-0 SR vrf content

13. Record the ESXi host details of the **sa-nsxedge-02** VM from the vSphere Client.
 - a. <optional> Log in to the vSphere Client with `administrator@vsphere.local` as username and `VMware1!` as password.
 - b. Expand **DataCenter-01-Production** > Expand **Management-Edge-Cluster-01** cluster > Expand **Prod-Edges** resource pool
 - c. Click on **sa-nsxedge-02 VM** and then click on **Summary** tab

Record the following details of sa-web-01 VM in the Value column

sa-nsxedge-02 details from vSphere Client

Parameter	Value
IP Address	
Host	

14. From the MTPuTTY window, click on **SA-ESXi-02**
15. On the sa-esxi-02 host, run the following command to note the sa-nsxedge-02.eth2 interface uplink mapping:

```
[root@sa-esxi-02:~] esxtop
```

- a. press `n` key from the keyboard to go to the networking view of esxtop.
- b. Record the `TEAM-PNIC` mapped to `sa-nsxedge-02.eth2` interface (Example: `vmnic3`).

sa-nsxedge-02 details from vSphere Client

USED-BY	TEAM-PNIC
sa-nsxedge-02.eth2	

```
67108891 526897:sa-nsxedge-02.eth2 vmnic3 DvsPortset-0
.....
```

- c. press `q` to exit from the esxtop.

Task 3: Perform Packet Capture

You use the nsxcli commands to capture and analyze the ICMP traffic between VMs and ESXi hosts.

1. Log in to the **sa-web-01** console from the vSphere Client.
 - a. Open the Chrome browser from the taskbar and click **vSphere Client**.
 - b. Log in to vCenter Server by entering user name **administrator@vsphere.local** and **VMware1!** as password
 - c. Locate the **sa-web-01** VM from the **Prod-Compute-Cluster-01** cluster.
 - d. Select **sa-web-01** and from the virtual machine summary page, select **Launch Web Console**.
 - e. Log in to the **sa-web-01** VM by entering user name **root** and password **VMware1!**.
2. Run the ping command to initiate a ping from sa-web-01 to 172.20.10.10 IP address.
 - a. From the sa-web-01 VM command line, run the following command.
`sa-web-01:~# ping 172.20.10.10`

Leave the ping command open, do not interrupt the pings.

3. Open **MTPuTTY** and double-click **SA-ESXi-04** to connect through SSH client as **sa-web-01** VM is running on this host.
4. On the sa-esxi-04 host, run the following command to enter the nsxcli command line.
`[root@sa-esxi-04:~] nsxcli`
5. On the sa-esxi-04 host, run the following command to capture the VMs traffic with the sa-web-01 Client name.

You will use the sa-web-01 client name that you have collected in **Task 2 Step 2**.

```
sa-esxi-04.vclass.local> start capture interface <sa-web-01-Client-name> expression ipproto 0x01
```

Example:

```
sa-esxi-04.vclass.local> start capture interface sa-web-01.eth0 expression ipproto 0x01
```

- a. After 5 seconds, press CTRL+C to stop the packet capture.

Record the "ICMP echo request" details from the packet capture to understand the source and destination details.

Packet Capture at the vNIC of the sa-web-01 VM

Parameter	Value
Source MAC	
Destination MAC	
Source IP	
Destination IP	

6. On the sa-esxi-04 host, run the following command to capture VMs traffic on an ESXi host before the dvfilter applied to the vNic of a VM.

You will use the dvfilter name of the VM that you have collected in **Task 2 Step 3**.

```
sa-esxi-04.vclass.local> start capture dvfilter <sa-web-01-  
dvfilter-name> stage pre expression ipproto 0x01
```

Example:

```
sa-esxi-04.vclass.local> start capture dvfilter nic-266190-  
eth0-vmware-sfw.2 stage pre expression ipproto 0x01
```

- a. After 5 seconds, press CTRL+C to stop the packet capture.

Record the "ICMP echo request" details from the packet capture to understand the source and destination details.

Packet Capture Before the dvFilter is Applied to the vNIC of sa-web-01 VM

Parameter	Value
Source MAC	
Destination MAC	
Source IP	
Destination IP	

7. On the sa-esxi-04 host, run the following command to capture VMs traffic on an ESXi host after the dvfilter applied to the vNic of a VM.

You will use the dvfilter name of the VM that you have collected in **Task 2 Step 3**.

```
sa-esxi-04.vclass.local> start capture dvfilter <sa-web-01-  
dvfilter-name> stage post expression ipproto 0x01
```

Example:

```
sa-esxi-04.vclass.local> start capture dvfilter nic-266190-  
eth0-vmware-sfw.2 stage post expression ipproto 0x01
```

- a. After 5 seconds, press CTRL+C to stop the packet capture.

Record the "ICMP echo request" details from the packet capture to understand the source and destination details.

Packet Capture After the dvFilter is Applied to the vNIC of sa-web-01 VM

Parameter	Value
Source MAC	
Destination MAC	
Source IP	
Destination IP	

8. On the sa-esxi-04 host, run the following command to capture the VMs traffic at the vdrport.

You will use the vdrport name that you have recorded in the **Task 2 Step 2**.

```
sa-esxi-04.vclass.local> start capture interface <vdr-  
vdrPort> expression ipproto 0x01
```

Example:

```
sa-esxi-04.vclass.local> start capture interface vdr-vdrPort  
expression ipproto 0x01
```

From the packet capture, you will see three MAC addresses, where 02:50:56:56:44:52 is the Logical Router Port MAC Address to which Segment is connected, 02:50:56:56:44:55 is the Linked Router Port MAC address which connects Tier-1 Distributed Router (DR) with Tler-0 Distributed Router (DR), and 02:50:56:56:52:01 is the Tier-0 Service Router (SR) MAC address.

- a. After 5 seconds, press CTRL+C to stop the packet capture.
9. On the sa-esxi-04 host, run the following command to capture the egress traffic at the ESXi host N-VDS uplink interface.

You will use the Prod-Overlay-NVDS interface that you have collected in **Task 2 Step 4**.
For the sa-nxedge-02 TEP IP refer to the Task 2 Step 9

```
sa-esxi-04.vclass.local> start capture interface <Prod-Overlay-NVDS-Uplink> direction output expression ip <sa-nxedge-02-TEP-IP>
```

Example:

```
sa-esxi-04.vclass.local> start capture interface vmnic4 direction output expression ip 172.20.11.156
```

- a. After 5 seconds, press CTRL+C to interrupt the packet capture.

Record the details of the ICMP echo request from the packet capture in the following table.

Packet Capture at the Uplink on sa-esxi-04 host

Parameter	Value
Outer MAC Header Source	
Outer MAC Header Destination	
Outer IP Header Source	
Outer IP Header Destination	
Destination Port	
Destination VM's VNI	
Inner MAC Address Source	
Inner MAC Address Destination	
Inner Source IP	
Inner Destination IP	

10. From **MTPuTTY** window, click on **SA-ESXi-02** to connect to the ESXi host where the sa-nsxedge-02 VM is running.

- a. On the sa-esxi-02 host, run the following command to capture the ICMP echo request message received over the vmnic2 adapter.

```
[root@sa-esxi-02:~] pktcap-uw --uplink vmnic2 --dir 0 --
overlay geneve --srcip 172.20.11.153 -o - | tcpdump-uw -r
- -nn | grep ICMP
```

After the icmp echo request is received at the ESXi host uplink, the hypervisor forwards the traffic to the NSX Edge TEP interface (TUNNEL port) to decapsulate the Geneve packet.

- b. After 5 seconds, press CTRL+C to stop the packet capture.
11. Open **MTPuTTY** from the taskbar and click on **sa-nsxedge-02** tab.
12. On the sa-nsxedge-02 node, run the following command to check all the options available with the `start capture` command on NSX Edge.

```
sa-nsxedge-02> start capture <Press ENTER Key from Keyboard>
```

Example:

```
sa-nsxedge-02> start capture
% Command not found: start capture
```

Possible alternatives:

```
start capture interface <interface-name> [direction
<direction>] [core <core-id>] [snaplen <capture-snaplen-arg>]
[file <filename>] [expression <expression>]
start capture interface <interface-name> [direction
<direction>] [file <filename>] [count <packet-count>]
[expression <expression>]
```

You will use the `start capture interface` command with different options to capture the traffic on the NSX Edge.

13. On the sa-nsxedge-02 node, run the following command to capture the traffic at the Tunnel port with uplink Interface UUID (NSX Edge TEP IP) that you have noted in **Task 2 Step 9**.

```
sa-nsxedge-02> start capture interface <Prod-T0-GW-01-
Uplink-interface-UUID> direction input expression ip
172.20.11.153
```

From the packet capture, you can see an encapsulated ICMP echo request is received from the 172.20.11.153 (sa-esxi04 IP address).

Example:

```
sa-nsxedge-02> start capture interface 98f2e7b7-3165-5db1-
bbae-70041267c16d direction input expression ip
172.20.11.153
```

- a. After 5 seconds press CTRL + C to stop packet capture

From the packet capture, record the ICMP echo request details in the following table.

Packet Capture at the sa-nsxedge-02 Tunnel Port

Parameter	Value
Outer MAC Header Source	
Outer MAC Header Destination	
Outer IP Header Source	
Outer IP Header Destination	
Destination Port	
Destination VM's VNI	
Inner MAC Address Source	
Inner MAC Address Destination	
Inner Source IP	
Inner Destination IP	

14. On the sa-nsxedge-02 node, run the following command to capture the traffic at the Tier-0 Transit link port (also called as backplane).

You will use the interface UUID that you have collected in the **Task 2 Step 12**.

```
sa-nsxedge-02> start capture interface <SR-Prod-T0-GW-01-bp-sr-1-port> direction input
```

Example:

```
sa-nsxedge-02> start capture interface 7c82ef74-da83-4b80-bb5d-16def9f291a6 direction input
```

From the packet capture, record the ICMP echo request details in the following table.

Packet Capture at the Prod-T0-GW-01 Transit Link Port

Parameter	Value
Source MAC	
Destination MAC	
Source IP	
Destination IP	

15. On the sa-nsxedge-02 node, run the following command to list the firewall rules applied at the uplink of the Tier-0 Gateway.

You will use the Uplink Interface UUID that you have recorded in the **Task 2 Step 10**.

```
sa-nsxedge-02> get firewall <Prod-T0-GW-01-Uplink-Interface-UUID> ruleset rules
```

Example:

```
sa-nsxedge-02> get firewall d8401057-b3c1-4da4-bc15-209d7f8f6305 ruleset rules
```

From the command output, you can see there are two Firewall rules with the Rule IDs ____ and ____ are the default rules that accepts all the traffic.

16. On the sa-nsxedge-02 node, run the following command to capture the outgoing traffic from the Tier-0 Gateway Uplink.

You will use the Uplink Interface UUID noted in the **Task 2 Step 11**.

```
sa-nsxedge-02> start capture interface <Prod-T0-GW-01-  
Uplink-Interface-UUID> direction output expression ipproto  
0x01
```

Example:

```
sa-nsxedge-02> start capture interface d8401057-b3c1-4da4-  
bc15-209d7f8f6305 direction output expression ipproto 0x01
```

Packet Capture at the Prod-T0-GW-01 Uplink Interface

Parameter	Value
Source MAC	
Destination MAC	
Source IP	
Destination IP	

17. From the MTPuTTY window, click on **SA-ESXi-02** tab as the sa-nsxedge-02 VM is running on this host.
18. On the sa-esxi-02 host, run the following command to capture the outgoing traffic at the ESXi host uplink through the vmnic3 interface.

```
[root@sa-esxi-02:~] pktcap-uw --uplink vmnic3 --dir 1 --  
proto 0x01 -o - | tcpdump-uw -r - -nn
```

Capture outgoing traffic at the ESXi host uplink where NSX Edge is running

Parameter	Value
Source IP	
Destination IP	

19. the sa-esxi-02 host, run the following command to capture the incoming traffic on the ESXi host uplink to capture the ICMP reply message.

```
[root@sa-esxi-02:~] pktcap-uw --uplink vmnic3 --dir 0 --  
proto 0x01 -o - | tcpdump-uw -r - -nn
```

Capture Incoming traffic at the ESXi host uplink where NSX Edge is running

Parameter	Value
Source IP	
Destination IP	

