# Table of Contents

Lab Overview - HOL-1803-03-NET - VMware NSX: Operations and Visability ............2
  Lab Guidance ..................................................................................................................3
Module 1 - Log Insight Management Pack Review (15 minutes) .................................9
  Introduction .....................................................................................................................10
  Install Log Insight Content Pack ................................................................................12
  Module 1 Conclusion ......................................................................................................17
Module 2 - Log Insight Dashboards for NSX (15 minutes) ......................................19
  Introduction .....................................................................................................................20
  Examine various Dashboards ......................................................................................22
  Interactive Analytics ......................................................................................................28
  Module 2 Conclusion ......................................................................................................37
Module 3 - Flow Monitoring Configuration (30 minutes) ...........................................39
  Introduction to Improved Operational Visibility with Flow Monitoring ..................40
  Tour of Flow Monitoring ..............................................................................................41
  Monitoring the Flows of a Virtual Machine .................................................................51
  Application Rule Manager ............................................................................................61
  Module 3 Conclusion ......................................................................................................81
Module 4 - Traceflow with NSX (30 minutes) ............................................................83
  Introduction to improved operational visibility with Traceflow .................................84
  Traceflow between two Virtual Machines .................................................................85
  Module 4 Conclusion ......................................................................................................109
Module 5 - The NSX Central CLI (15 minutes) ..........................................................111
  Introduction to Improved Operation Visibility with Central CLI ..............................112
  Troubleshooting Logical Switches ..............................................................................115
  Troubleshooting Distributed Logical Routers .............................................................127
  Troubleshooting Edge Service Gateways ....................................................................135
  Troubleshooting Distributed Firewall ..........................................................................142
  Module 5 Conclusion ......................................................................................................151
Module 6 - Endpoint Monitoring with NSX (15 minutes) ........................................153
  Introduction .....................................................................................................................154
  Endpoint Monitoring Data Collection .........................................................................156
  Module 6 Conclusion ......................................................................................................177
Lab Overview - HOL-1803-03-NET - VMware NSX: Operations and Visability
Lab Guidance

Note: It will take more than 90 minutes to complete this lab. You should expect to only finish 2-3 of the modules during your time. The modules are independent of each other so you can start at the beginning of any module and proceed from there. You can use the Table of Contents to access any module of your choosing.

The Table of Contents can be accessed in the upper right-hand corner of the Lab Manual.

Welcome to the VMware NSX Operations and Visibility Lab. Within this lab we will guide you through all of the tools at your disposal to assist in not only troubleshooting, but also gaining additional operational visibility into your infrastructure. We start off by reviewing the NSX Content pack for Log Insight and the new dashboard functionality that it serves up into Log Insight. We then look at the tool natively built into NSX which include Flow Monitoring, Traceflow and Central CLI. The complete Lab Module list is below and all modules are completely independent so you can freely move between different modules.

Lab Module List:

- **Module 1 - Log Insight Management Pack Review** (15 minutes) - Basic - This module covers the basics of the NSX Log Insight Management Pack and how to install it within Log Insight.
- **Module 2 - Log Insight Dashboards** (15 minutes) - Basic - This module covers the Log Insight Dashboard and how to successfully navigate around the interface.
- **Module 3 - Flow Monitoring Configuration** (15 minutes) - Basic - This module covers the basics of NSX Flow Monitoring. It starts off by giving you a tour of all the available options and then how to monitor the flows of a particular VMs vNIC.
- **Module 4 - Traceflow** (15 minutes) - Basic - This module covers the basics of Traceflow and how to initiate a Traceflow between two VMs to view an "Allowed" and "Blocked" result.
- **Module 5 - Central CLI** (15 minutes) - Basic - This module shows the power of Central CLI and how you can easily retrieve valuable information relating to NSX via a single Central CLI.
- **Module 6 - Endpoint Monitoring** (15 minutes) - Basic - Endpoint Monitoring enables you to profile applications inside the guest including visibility into specific application processes and their associated network connections

Lab Captains:

- Module 1 - Mostafa Magdy, Sr. Systems Engineer, Canada
- Module 2 - Mostafa Magdy, Sr. Systems Engineer, Canada
- Module 3 - Mostafa Magdy, Sr. Systems Engineer, Canada
This lab manual can be downloaded from the Hands-on Labs Document site found here:

http://docs.hol.vmware.com

This lab may be available in other languages. To set your language preference and have a localized manual deployed with your lab, you may utilize this document to help guide you through the process:


**Location of the Main Console**

1. The area in the RED box contains the Main Console. The Lab Manual is on the tab to the Right of the Main Console.
2. A particular lab may have additional consoles found on separate tabs in the upper left. You will be directed to open another specific console if needed.
3. Your lab starts with 90 minutes on the timer. The lab cannot be saved. All your work must be done during the lab session. But you can click the **EXTEND** to increase your time. If you are at a VMware event, you can extend your lab time twice, for up to 30 minutes. Each click gives you an additional 15 minutes.
Outside of VMware events, you can extend your lab time up to 9 hours and 30 minutes. Each click gives you an additional hour.

**Alternate Methods of Keyboard Data Entry**

During this module, you will input text into the Main Console. Besides directly typing it in, there are two very helpful methods of entering data which make it easier to enter complex data.

**Click and Drag Lab Manual Content Into Console Active Window**

You can also click and drag text and Command Line Interface (CLI) commands directly from the Lab Manual into the active window in the Main Console.

**Accessing the Online International Keyboard**

You can also use the Online International Keyboard found in the Main Console.

1. Click on the Keyboard Icon found on the Windows Quick Launch Task Bar.
**Click once in active console window**

In this example, you will use the Online Keyboard to enter the "@" sign used in email addresses. The "@" sign is Shift-2 on US keyboard layouts.

1. Click once in the active console window.
2. Click on the **Shift** key.

**Click on the @ key**

1. Click on the "@ key".

Notice the @ sign entered in the active console window.
Activation Prompt or Watermark

When you first start your lab, you may notice a watermark on the desktop indicating that Windows is not activated.

One of the major benefits of virtualization is that virtual machines can be moved and run on any platform. The Hands-on Labs utilizes this benefit and we are able to run the labs out of multiple datacenters. However, these datacenters may not have identical processors, which triggers a Microsoft activation check through the Internet.

Rest assured, VMware and the Hands-on Labs are in full compliance with Microsoft licensing requirements. The lab that you are using is a self-contained pod and does not have full access to the Internet, which is required for Windows to verify the activation. Without full access to the Internet, this automated process fails and you see this watermark.

This cosmetic issue has no effect on your lab.

Look at the lower right portion of the screen
Please check to see that your lab is finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes. If after 5 minutes your lab has not changed to "Ready", please ask for assistance.
Module 1 - Log Insight Management Pack Review (15 minutes)
Introduction

Traditional log management tools are not suitable for a dynamic hybrid cloud environment. This is due, in part, to the fact that traditional tools do not leverage logs and other machine-data strategically to generate insights and troubleshoot IT infrastructure issues. In addition, machine-generated log data is massive in scale and difficult to capture and manage. Further, siloed approaches to virtual and physical infrastructure management lead to finger pointing and fire drills. Finally, other solutions may need additional piecemeal software in order to work with vSphere, and may not always support the latest version.

Log Insight Description

VMware vRealize Log Insight addresses these challenges and enables improved quality of service, operational efficiency and continuous compliance. The following is a list of Log Insight's capabilities:

- Collects and analyzes all types of machine-generated log data, e.g., application logs, network traces, configuration files, messages, performance data, and system state dumps
• Enables administrators to connect to everything in their environment, e.g., operating systems, applications, storage arrays, firewalls, network devices, etc., providing a single location to collect, store, and analyze logs at scale
• Features an intuitive GUI-based interface that makes it easy to run interactive searches as well as deep analytical queries for quick, actionable insights.
• Includes new cluster technology to allow your log analytics efforts to scale to new heights.
• Automatically chooses the best visualization for your data, saving you valuable time
• Adds structure to all types of unstructured log data, enabling administrators to troubleshoot quickly, without needing to know the data beforehand
• Delivers real-time monitoring, search, and log analytics, coupled with a dashboard for stored queries, reports, and alerts, enabling correlation of events across multiple tiers of a hybrid cloud environment
• Helps users find virtual infrastructure problems with the addition of Intelligent Grouping, a machine-learning technology that can group related data together to aid in detecting problems rapidly
• Comes with built-in knowledge and native support for vSphere and other VMware products, like Horizon® View, vRealize™ Operations Suite™ and vRealize Automation and NSX
• VMware and third-party extensions available on the VMware solution exchange
• Integrates with the VMware vRealize Operations platform to bring unstructured data (e.g., log files) together with structured data (e.g., metrics and KPIs), offering a significantly enhanced solution for end-to-end operations management

Installation of Log Insight

Log Insight is installed as a virtual appliance. By default, the Log Insight virtual appliance has 2 vCPUs, 4GB of virtual memory, and 144GB of disk space provisioned. Log Insight uses 100GB of the disk space to store raw data, index, metadata, and so on. There are many different factors that can impact the sizing of the virtual appliance. These discussions are beyond the scope of this lab. A deeper discussion of the vRealize Log Insight platform can also be found in:

HOL-1806-01 Module 2

The full documentation set can also be found at https://www.vmware.com/support/pubs/log-insight-pubs.html For the purposes of this lab, the log Insight Appliance has already been installed. In the next section, we will log into the appliance and install the NSX Content Pack.
Install Log Insight Content Pack

In this module, we will be installing the Log Insight content pack for NSX. This will contain all the dashboards related to NSX.

Open google Chrome from the Control Center Desktop

From the control center desktop, click on the Google Chrome icon from the Desktop.
Install LogInsight content pack

Login to VRealize LogInsight

1. CLICK on the vRealize LogInsight bookmark.
2. Login with the following credentials:

Username is **admin**

Password is **VMware1!**
Install the LogInsight content pack

From the main login screen,

1. CLICK on the drop-down for settings.

2. SELECT CONTENT PACKS from the drop-down menu.
1. In the bottom left-hand corner of the menu, CLICK on **Import Content Pack**.

2. In the resulting file window, navigate to the **Desktop> VRealize Log Insight NSX Content Pack 3.6 > VMware-NSX-vSphere_3_6.vlcp**.

3. Double-Click **on the file name** or CLICK **Open**.

4. CLICK on the **Import Button** to complete the installation of the content pack.
Complete the installation

VMware - NSX-vSphere Setup Instructions

Forward all logging components to the Log Insight server including:
1. Use the Log Insight vSphere integration to forward logs for all ESXi servers
2. NSX-vSphere Manager
3. NSX-vSphere Controller(s)
4. All NSX-vSphere edge devices

For detailed setup instructions refer to the following resources:
* NSX Operations Guide
* About NSX Logs

1. CLICK OK.

Once the import is complete, the content pack is installed and you can begin to explore the dashboards and other widgets in Log Insight specific to NSX.
Module 1 Conclusion

In this module we managed to install the NSX content pack for LogInsight. In the next lesson, we'll look at some of the dashboards.

You've finished Module 1

Congratulations on completing Module 1.

If you are looking for additional information on LogInsight, try one of these:

- Go to https://tinyurl.com/yctzxt6y

Proceed to any module below which interests you most.

Lab Module List:

- **Module 1 - Log Insight Management Pack Review** (15 minutes) - Basic - This module covers the basics of the NSX Log Insight Management Pack and how to install it within Log Insight.
- **Module 2 - Log Insight Dashboards** (15 minutes) - Basic - This module covers the Log Insight Dashboard and how to successfully navigate around the interface.
- **Module 3 - Flow Monitoring Configuration** (30 minutes) - Basic - This module covers the basics of NSX Flow Monitoring. It starts off by giving you a tour of all the available options and then how to monitor the flows of a particular VMs vNIC.
- **Module 4 - Traceflow** (30 minutes) - Basic - This module covers the basics of Traceflow and how to initiate a Traceflow between two VMs to view an "Allowed" and "Blocked" result.
- **Module 5 - Central CLI** (15 minutes) - Basic - This module shows the power of Central CLI and how you can easily retrieve valuable information relating to NSX via a single Central CLI.
- **Module 6 - Endpoint Monitoring** (15 minutes) - Basic - This module shows an overview of Endpoint Monitoring and how you can easily monitor internal guest processes for specific VMs

Lab Captain:

- **Module 1 through 6 - Mostafa Magdy, Senior Systems Engineer, Canada**

How to End Lab
To end your lab click on the END button.
Module 2 - Log Insight
Dashboards for NSX (15 minutes)
Introduction

The NSX for vSphere Log Insight Content Pack provides powerful operational reporting and alerting visibility for all sources of log data within NSX. Each major NSX function (logical switching, routing, distributed firewalls, VXLAN gateways, and edge services) is represented within this content pack via custom dashboards, filters, and alerts. This graphically rich, content pack is essential for analyzing and identifying NSX configuration, performance, security and trend related problems. The twelve NSX dashboards are easily selectable with intuitive mouse clicks. NSX log data is quickly sorted based upon user defined time intervals, and within seconds the data is presented graphically via bar graphs, pie charts and raw data collection widgets.

Dashboard overview

In this module we'll look at the different dashboards available from the NSX content pack.
To get a full list of the widgets that are available in the pack:

1. Click on the **top right corner**.
2. Select **Content packs**.
3. Select **VMware - NSX-vSphere**.
4. Select **Dashboards** at the top of the page to view a full list of the available reports.
Examine various Dashboards

In this lesson we'll be taking a tour around dashboards and what to expect from a reporting perspective.

Navigate to Dashboards and select the custom date and time

From this page click Dashboards.
Selecting the dataset

For the purposes of this lab, we'll be selecting a specific date to reflect the data we want to demo.

1. Click on the drop down menu representing the time range.
2. Select Custom time range.

Selecting the dates

1. Click on the Calendar icon.
2. Select the following date 1st of March 2017 till 14th of June 2017.

Custom date

![Custom date input field with dates selected from 1st March 2017 to 14th June 2017]
Once the dates are selected per the snapshot, click update to refresh the graphs.

Please note: Graphs might be different from one session to another. In this module we will try to provide a general overview on what to expect and how to easily show information that can help you troubleshoot a problem.

1. Click on the top corner button of the browser.
2. Click on the "-" next to zoom to be able to fit the whole dashboard in your screen and not have to scroll down.
1. Click on **NSX-vSphere - Overview**.
2. Click on the "i" for a description of the specific dashboard.

The NSX-vSphere Overview is the main entry point. This dashboard displays all problems/alerts reflected in the entire content pack. Therefore, under normal operating circumstances the dashboard should not contain any data. Once a log appears on a widget, read the widgets information in order to navigate to the appropriate dashboard for a more detailed view of the information associated with the problem.

**Distributed Firewall - Overview**

1. Click on **Distributed Firewall - Overview**.
2. You can use the filters to narrow down the results displayed by **Hostname**, **Firewall Rule ID** or **Firewall Rule Action**. More filters can be added to narrow it down even more.

3. **Firewall audit events by operation**: Is a graphical representation of audit events by operation, such as create, delete or update. You can investigate the actual changes made by looking at the Audit logs file on the NSX manager.

4. You can also take a quick look at the newly published firewall rules along with the timestamp, Source NSX manager, action, ...etc.

Firewall dashboards provide widgets that contain many different views of firewall data. These visualizations are aggregated to show various slices of an NSX-vSphere environment at the hypervisor, vm and application level.

**New Dashboards part of the 3.6 release**

![Dashboard Widgets]

New dashboards have been introduced in this release for edge load balancing service. These dashboards are available with NSX Manager 6.3 or later.

- **Load Balancer - General**: Contains 3 widgets which display load balancer service status for all edges, all VIP statuses, and load balancer alerts.
• **Load Balancer -Instance:** Displays load balancer throughput, RAM usage, concurrent connections and new connections, as well as all VIP statuses for selected load balancer instance.
• **Load Balancer -VIP:** Displays concurrent and new connections, as well as pool member statuses.
• **Load Balancer -VIP HTTP(S):** Displays web access related statistics for selected VIP and has 2 widgets. One widget displays VIP average response times and the other displays VIP response errors.

**Guest Introspection**

1. Guest introspection is a service that is deployed from NSX Manager to offload security functions to a dedicated security appliance on each host; thus removing the need for an AV agent within the guest operating system.

Using the Guest Introspection driver baked into VMware Tools and a third party service virtual machine, such as McAfee MOVE, all virtual machines are protected by real-time inspection as soon as they are powered on. This reduces administrative and guest memory overheads, whilst standardizing deployments.
Interactive Analytics

Interactive analytics allow interaction with logs in real time enabling the Administrator to select a specific event, show all the logs related to that event and then filter out the incidents.

Create a scenario - packet drop

On your vSphere web client,
1. Click the **home button**.
2. Click **Networking and Security**.

![Image of Firewall interface]

1. Click on **Firewall**.
2. Click on the + icon.

![Image of Firewall rule creation]

We will now create a firewall rule to simulate a packet drop scenario.

1. Hover with your mouse pointer at the top right corner of each column to edit the value. You can use the following values:
   
   - **Name**: *Fin Web to HR Web block*.
   - **Source**: *fin-web-01a.corp.local*.
   - **Destination**: *hr-web-01a.corp.local*.
   - **Service**: *ICMP*.
   - **Action**: *Block*.
Make sure you enable logging in action column.

![Fin Web to HR Web block - Edit Action](image1)

This is what the rule should look like, go ahead and publish the rule to activate it.

![Publish Changes](image2)

1. Click on **Publish Changes**.

Verify rule has been published.

**Test firewall rule**

```
root@fin-web-01a [ ~ ]# ping 172.16.60.10
PING 172.16.60.10 (172.16.60.10) 56(84) bytes of data.
64 bytes from 172.16.60.10: icmp_seq=0 ttl=64 time=5.84 ms
64 bytes from 172.16.60.10: icmp_seq=1 ttl=64 time=5.85 ms
--- 172.16.60.10 ping statistics ---
11 packets transmitted, 0 received, 100% packet loss, time 0.000 ms
```
• using putty login to **Fin-web-01a**.
• Ping **HR-web-01a** (172.16.60.10).
• FW rule should **drop** the packets.

**Navigate to LogInsight**

1. Click on the bookmark to go to the LogInsight Interface.
2. Use the following Credentials to login

User name: **admin**
Verify result from Dashboards

1. Click **Dashboards**.
2. Click **Distributed Firewall - Overview**.
3. Change your time range to be from the **1st of March 2017 till the 15th of June 2017** (time of the development of this module - you can find a detailed step by step in the previous lab: [Examine various Dashboards](#)).
4. Click **refresh**.
5. Using your mouse go to the Firewall actions dashboard and hover over the dropped packed portion of the bar. **Left Click** on the bar.
6. Select **Interactive Analytics**.

In this view, in the Firewall Actions dashboard, select the drop event on the 13th of June. If you hover with your mouse on top of it, you should get event id **30**.
Interactive Analytics

1. You can start by selecting the bar that is the closest representation of the time that you want investigate.
2. In the Filter section you can dynamically extract any field from the data by providing a regular expression. The extracted fields can be used for selection, projection, and aggregation, similar to how the fields that are extracted at parse time are used.
3. This shows a list of the data classifications and keywords that you can choose to show or hide. you can also choose to assign a specific value to further filter your results.

The resulting information shows that 172.16.60.20 (fin-web-01a) was issuing a ping to 172.16.60.10 (hr-web-01a) and it was dropped due to FW rule # 1018.
Event representation

You can change the event representation by:

1. Selecting the time frame, in our example 1 bar = 10 minutes.
2. Changing the chart type.
Publishing to Dashboard

If you believe the work you've done here might require some close follow-up for the next couple of days, you can export this filtered view to your dashboards.

1. Click **Add to Dashboard**.
2. Fill the fields using the following information:
   1. Name: **Fin Web to HR Web block**
   2. Notes: **Chart showing the dropped ICMP packets between fin-web-01a.corp.local and hr-web-01a.corp.local**
3. Click **ADD**.

Check out custom Dashboards
1. Click **Dashboards**.
2. Click **My Dashboards**.
3. Verify the customer dashboards shows the same events that we witnessed in the interactive analytics.
Module 2 Conclusion

In this module, we looked at the different dashboards available in the NSX content pack for Log Insight. We focused on the distributed firewall dashboards.

Finally we looked at Interactive analytics and how we can monitor events live to help provide a root cause analysis for incidents

You've finished Module 2

Congratulations on completing Module 2.

If you are looking for additional information on Flow Monitoring visit the URL below:

- Go to [https://tinyurl.com/y9ttkoq](https://tinyurl.com/y9ttkoq)

Proceed to any module below which interests you most.

Lab Module List:

- **Module 1 - Log Insight Management Pack Review** (15 minutes) - Basic - This module covers the basics of the NSX Log Insight Management Pack and how to install it within Log Insight.
- **Module 2 - Log Insight Dashboards** (15 minutes) - Basic - This module covers the Log Insight Dashboard and how to successfully navigate around the interface.
- **Module 3 - Flow Monitoring Configuration** (30 minutes) - Basic - This module covers the basics of NSX Flow Monitoring. It starts off by giving you a tour of all the available options and then how to monitor the flows of a particular VMs vNIC.
- **Module 4 - Traceflow** (30 minutes) - Basic - This module covers the basics of Traceflow and how to initiate a Traceflow between two VMs to view an "Allowed" and "Blocked" result.
- **Module 5 - Central CLI** (15 minutes) - Basic - This module shows the power of Central CLI and how you can easily retrieve valuable information relating to NSX via a single Central CLI.
- **Module 6 - Endpoint Monitoring** (15 minutes) - Basic - This module shows an overview of Endpoint Monitoring and how you can easily monitor internal guest processes for specific VMs

Lab Captain:

- **Module 1 through 6 - Mostafa Magdy, Senior Systems Engineer, Canada**
How to End Lab

To end your lab click on the **END** button.
Module 3 - Flow Monitoring Configuration (30 minutes)
Introduction to Improved Operational Visibility with Flow Monitoring

Flow Monitoring is a traffic analysis tool that provides a detailed view of the traffic to and from virtual machines. When flow monitoring is enabled, its output defines which machines are exchanging data and over which application. This data includes the number of sessions and packets transmitted per session. Session details include sources, destinations, applications, and ports being used. Session details can be used to create firewall allow or block rules.

You can view TCP and UDP connections to and from a selected vNIC. You can also exclude flows by specifying filters.

Flow Monitoring can thus be used as a forensic tool to detect rogue services and examine outbound sessions.
Tour of Flow Monitoring

Flow Monitoring is accessed via the Network and Security tab within vSphere Web Client.

Launch the Google Chrome browser

Click on the Chrome browser icon from within the taskbar or on the desktop of the main console.

vCenter - Region A bookmark

1. If the page does not automatically default to the vSphere Web Client page click on the vCenter - Region A link in the bookmarks bar.

Login to the vSphere Web Client

If you are not already logged into the vSphere Web Client:

(The home page should be the vSphere Web Client. If not, Click on the vSphere Web Client Taskbar icon for Google Chrome.)

1. Click the checkmark next to Use windows session authentication.
2. Click Login
Navigate to Networking & Security

1. From within the vSphere Web Client click on the **Networking & Security** tab.
Navigate to Flow Monitoring

1. From within the Networking & Security tab click on the Flow Monitoring tab.

Flow Monitoring tabs

Within Flow Monitoring we have five tabs available:

1. **Dashboard** - Displays Top Flows, Top Destinations and Top Sources and allows you to modify the time interval that you are currently viewing.
2. **Details by Service** - Displays Allowed and Blocked Flows by service.
3. **Live Flow** - Enables you to monitor the flows or a particular vNIC from within your infrastructure.
4. **Configuration** - Enables Flow Monitoring and allows you to exclude certain flows.
5. **Application Rule Manager** - Simplifies the process of microsegmenting an application by creating security groups and firewall rules for existing applications.
Modifying the Time Interval

1. If you are not already at the **Dashboard** tab then please click on it.
2. In order to modify the time interval you may need to move the screen focus to the right by using the windows arrows. You can modify the time interval by clicking on the calendar icon.
3. Select the time frame to view.
4. Leave the default value of **Last 15 minutes** and click **OK** to continue.
Flow Monitoring Dashboard

1. Clicking on the Dashboard tab shows you a list of flow information from within the environment which includes actual flows, and statistical information around the percentage of flows allowed, blocked by rules or blocked by spoofguard.

You can also view Top Flows, Top Destinations and Top Sources occurring within your environment.
Flow Monitoring Details by Service

1. **Details by Service** shows flow statistics based on services within the environment.

Allowed Flows

1. **Allowed Flows** shows you all flows within the environment that have been allowed either by the default ANY-ANY-Allow rule or by a specific rule added.
Add rule via Allowed Flows

If you see a flow within the environment that should be blocked or allowed you can add a rule to the Distributed Firewall to allow or block it depending on your security requirements:

1. Click on the associated flow.
2. Click on the Add Rule link to insert a new rule.
3. Enter the required information regarding the rule such as Name, Destination, Action, Enabled, Logging, Applied To and Section name.
4. Click OK to confirm and add the rule to the ruleset.
Blocked Flows

1. **Blocked Flows** show you all flows that have been blocked by the distributed firewall.

Flow Monitoring Configuration

1. Click on the Flow Monitoring **Configuration** tab.
2. You have the ability to Enable or Disable Flow Monitoring, by default Flow Monitoring is disabled so you have to manually enable it. Within the lab this has already been enabled.
Flow Exclusion

Within Flow Monitoring you can filter the data being displayed by specifying exclusion criteria. For example, you may want to exclude a proxy server to avoid seeing duplicate flows. Or if you are running a Nessus scan on a virtual machines in your inventory, you may want to exclude the scan flows from being collected.

1. Click on the **Flow Exclusion** tab.
2. Click on one of the Exclusion filter that you want to modify. In this example we clicked on **Collect Layer2 Flows**.
3. Click **Save** to confirm.

**IPFix**

Within Flow Monitoring you can filter the data being displayed by specifying exclusion criteria. For example, you may want to exclude a proxy server to avoid seeing duplicate flows. Or if you are running a Nessus scan on a virtual machines in your inventory, you may want to exclude the scan flows from being collected.

1. Click on the **Flow Exclusion** tab.
2. Click on one of the Exclusion filter that you want to modify. In this example we clicked on **Collect Layer2 Flows**.
3. Click **Save** to confirm.
You can also configure Flow Monitoring to export flows to a 3rd party collector.

1. Simply **Edit** the IPFix configuration.
2. Enable IPFix Configuration and set the Observation DomainID as well as Active Flow Export Timeout values.
3. Click **OK** to confirm your settings.

### Publish Changes

![Publish Changes](image)

1. Click **Publish Changes** to confirm the settings.

If you get the below error, that’s fine as we haven’t configured a Collector IP. Please ignore

### IPFix Collectors

![IPFix Collectors](image)

1. To add collectors to send the flows to click on the green plus icon.
2. Enter the required information such as Collector IP and UDP port.
3. Click **OK** to confirm.
Monitoring the Flows of a Virtual Machine

Now that we've walked through the configuration options available for Flow Monitoring, let's start monitoring some flows which will include allowed and blocked flows.

Enable Flow Monitoring Distributed Firewall rule

The first step that we need complete is to enable the Distributed Firewall rule that will block communication from web-01a.corp.local (172.16.10.11) to app-01.corp.local (172.16.20.11). This will allow us to test Flow Monitoring and show the difference between an allowed and blocked flow.

Navigate to Networking & Security

1. From the vCenter Web Client home screen click on the Network & Security tab to access the NSX interface.
Navigate to Firewall

1. Click on the **Firewall** tab.
2. Click on the arrow to expand the section called **Flow Monitoring & Trace Flow Rules-Disabled by Default**.
3. Click the Green tick to enable the Flow Monitoring Test rule. Make sure the Source is `web-01.corp.local` and the Destination is `app-01.corp.local` & `web-02.corp.local` and that the Service is **any**.
4. Click **Publish Changes** to push the rules down to the hypervisor.

Verify the Publish has succeeded

1. Verify that the publish operation has completed successfully (Please note the date of your publish will not be identical to the screenshot).

Monitoring Flows

We are now ready to monitor flows and see the results of a flow that is allowed and a flow that has been blocked.
Navigate to Flow Monitoring

1. Click on the Flow Monitoring tab.
2. Click on the Live Flow dashboard.
3. Click the Select link to select a virtual machine network interface card to monitor.
1. Within the search field type `web-01a.corp.local` and press enter.
2. Click on the `web-01a.corp.local` virtual machine.
3. Click on the right arrow.
Select the VNIC

1. Select the vNIC that you wish to monitor.
2. Click OK to confirm.
Start Monitoring

1. Click on the **Start** button to start monitoring flows to and from the vNIC.
2. Optionally change the Refresh Rate by clicking on the drop down menu and selecting a new refresh rate.

When traffic flows through the vNIC they will be highlighted in different colours:

- **Green** - These are new and active flows.
- **Yellow** - These are existing flows that have changed their state.
- **Red** - These are flows that have been terminated.

Flows will appear X amount of seconds depending on the refresh rate that has been selected, by default this is every 5 seconds.

Open a new tab in your browser

1. Click on the new tab icon within the browser to open a new tab.
Customer DB App

Service Temporarily Unavailable

The server is temporarily unable to service your request due to maintenance downtime or capacity problems. Please try again later.

Apache/2.2.15 (CentOS) Server at webapp.corp.local Port 443

1. Click on the **Customer DB App** bookmark which will eventually show a **Service Temporarily Unavailable** webpage because we blocked all access from **web-01a.corp.local (172.16.10.11)** to **app-01a.corp.local (172.16.20.11)**.

Viewing Active and Blocked flows

If you click back to the vSphere Web Client tab you should see some flows.

The green flows are showing active flows from the **Main Console (192.168.110.10)** which is where the Chrome browser is running to **web-01a.corp.local (172.16.10.11)**.

The red flow is showing a blocked from from **web-01a.corp.local (172.16.10.11)** to **app-01a.corp.local (172.16.20.11)** as this is being blocked by the NSX distributed firewall.
Refreshing the Customer DB App web page

1. If you missed it simply go back to the Customer DB App tab.
2. Click on the browser refresh button.
3. Click back to the vSphere Web Client tab.

Filtering Flows

Since NSX 6.2.3 you now have the ability to filter on specific flows based on source and destination IP addresses. This allows you to easily focus on the flows that you are interested in and discard all the unnecessary ones.

1. Once you are monitoring a vNIC click on the filter button.
2. Select either Source IP or Destination IP.
3. Enter the IP address you wish to filter on.

This is just to display functionality, no need to add any filters.
Finishing with Flow Monitoring

Once you have finished playing with Flow monitoring it's time to clear up the environment.

Stopping Flow Monitoring

1. Click on the Stop button to stop Flow Monitoring. If you were to browse to another tab within Networking & Security this would accomplish the same task.

Navigate to Firewall

1. Click on the Firewall tab.
2. Click on the arrow to expand the section called **Flow Monitoring & Trace Flow Rules-Disabled by Default**.
3. Click the **Green tick** to disable the Flow Monitoring Test rule.
4. Click **Publish Changes** to push the rules down to the hypervisor.

**Verify the Publish has succeeded (Copy)**

1. Verify that the publish operation has completed successfully (Please note the date of your publish will not be identical to the screenshot). The rule has now been disabled.
**Application Rule Manager**

The Application Rule Manager tool is a new tool that was introduced in NSX 6.3. ARM simplifies the process of microsegmenting an application by creating security groups and firewall rules for existing applications.

Flow monitoring is used for long term data collection across the system, while the application rule manager is used for a targeted modeling of an application.

There are three steps in the application rule manager workflow:

1. Select virtual machines (VMs) that form the application and need to be monitored. Once configured, all incoming and outgoing flows for a defined set of VNICs (Virtualized Network Interface Cards) on the VMs are monitored. There can be up to five sessions collecting flows at a time.
2. Stop the monitoring to generate the flow tables. The flows are analyzed to reveal the interaction between VMs. The flows can be filtered to bring the flow records to a limited working set.
3. Use flow tables to create grouping objects such as security groups, IP sets, services and service groups and firewall rules.

**Application Rule Manager Flows**

Before we can view flow data for VMs, we need to gather it first. To start gathering, navigate to the Application Rule Manager tab and click **Start New Session**.
Navigate to Application Rule Manager

1. Click on the **Flow Monitoring** tab.
2. Click on the **Application Rule Manager** dashboard.
3. Click the **Start New Session** to start gathering data.
Select web-01a.corp.local

1. In the session name type **new fin app**.
2. For the Object Type, select **Virtual Machine**.
3. Use the Filter to narrow down the results by typing **fin**
4. Select the following VMs: **fin-web-01a.corp.local**, **fin-app-01a.corp.local** and **fin-db-01a.corp.local**
5. Click on the right arrow.
6. Click **OK**.
ARM will now start collecting data on flows between the 3 selected VMs. The more time you leave it the more information you will have for the analysis. For lab purposes, we will leave it for 3 minutes. while you're waiting, open new tabs and click on the different application bookmarks (Customer DB App, Finance DB App and HR DB App) in your browser to generate traffic. Please note that the number of flows may vary from one student to another.

1. Click Stop to stop the collection.
2. Click Yes to confirm.
View Flows

We can see a list of IPs in the source column connecting to IPs in the Destination column using a couple of services like HTTP, HTTPS .. etc
Check out sources

1. Click on Source to see a list of the vnics being monitored

Check out Flows

1. Click on Flows to see the total duration gathering data
Start Analysis

1. Click on the **Analyze** for NSX to start analyzing the collected data.

NSX will replace IPs by higher level constructs like VM names.

Processed View

We now have a processed view and NSX has replaced the IPs with VM names.
Find out more information

1. Click on the VM name **fin-web-01a.corp.local** to find more information about it. Do the same for the services to reveal communication between any source and any destination in the processed view.

You can leverage this view to create your firewall rules in a very simple and quick fashion.
Creating Firewall rules from the processed view

1. Click on the row for which you would like to create a firewall rule. In our example, we selected to create a firewall rule for all the services between the Web tier fin-web-01a.corp.local and the App-tier fin-app-01a.corp.local.
2. Click **Actions**.
3. Click **Create Firewall Rule**.
New firewall rule for the Web-Tier

1. Type in a name for your New Firewall rule. We used: **FIN_Web_to_App**.
2. For the applied to nic, remove everything except for the **fin-web-01a.corp.local** - Network
3. Select **Allow**.
4. Click **OK**.
Go ahead and try to create one for the **FIN_App_to_DB**. This is what it should look like:

![New Firewall Rule](image)

**New Firewall rules tab**

![Flow Details](image)
Click on **Firewall rules** tab to see a list of the firewall rules that you just created. Firewall rules in here can be edited at any point by changing any of the represented fields **Source**, **Destination**, **Service**.... etc. then pushed to be applied and published. We will try that later.

**Managing traffic between App and DB tiers using Security Group**

1. Click **View Flows**.
2. Select a row where the **fin-DB-01a.corp.local** is the destination.
3. Click the small gear next to the **Source**.
4. Select **Create Security Group and Replace**.

As your environment scales you’ll find that operationally it could be much easier to start creating security groups versus creating individual rules per tenant/VM. Other available options are:

- **Replace with any**
- **Replace with membership**; if the VM already belongs to a security group.
- **Create IPSet and Replace**; assign a preset range of IPs to be allowed or blocked.
- **Add to existing IPSet and Replace**; use a predefined IPSet.
Create Security Group

1. Input **New_APP_SG** for the name of the security group.
2. Click **Next**.

1. Select **Select objects to include**.
2. For Object Type, select **Virtual Machine** from the drop down menu.
3. For the filter type **app**.
4. Select **fin-app-01a.corp.local**.
5. Click **arrow**.
6. Click **Finish**.

You can use the same methodology for the Destination

**Creating a firewall rule using the security groups**

1. Choose the security group
2. Click **Create Firewall Rule**
3. Click **Add Rule**
1. Click on the row that you would like to create a firewall rule for. In our example, we selected to create a firewall rule for all the services between the App SG New_APP_SG and the DB tier New_DB_SG.
2. Click Actions.
3. Click Create Firewall Rule.

![New Firewall Rule](image)

1. Name: APP_to_DB
2. Source: New_APP_SG
3. Destination: New_DB_SG
4. Action: Allow
5. Direction: In/Out
1. In the Name field put **APP_to_DB**.
2. Clear the service ports because you want local traffic between the App and the DB.
3. Clear the vnics of the individual VMs because you will be selecting the SG instead.
4. Click **Select**.

![Diagram showing how to select Security Group](image-url)
1. For Object Type, select **Security Group** from the drop down menu.
2. Select **New_APP_SG**.
3. Click **arrow**.
4. Click **OK**.

![Diagram of New Firewall Rule](image)

1. Click **OK**.

This was another way to create firewall rules. As a final rule try to create a rule where the source is any and the destination is Web.
Activate firewall rules

1. Select **Firewall rules**.
2. For the section name, we can enter **FIN_APP_rules**.
3. For the insert above, Select **Default Section Layer3**.
4. Click **OK**.

In the screenshots you might notice firewall rules like **Any_to_Web** that were created similar to the previous examples that we walked you through. This is just for demonstration purposes.

**Verify the firewall rules have been published**

Last publish operation succeeded 6/3/2017 12:02:45 AM
Verify firewall rules in NSX manager

Verify the rules have been pushed out to the main firewall view by navigating to Networking & Security.

1. Select Firewall.
2. Click on drop down arrow next to FIN_APP_rules.
3. Verify those are the same rules that were created earlier in the lab.
Clean up for ARM

You have now experienced a glimpse of how ARM can simplify the creation of firewall rules that are application centric. Please go ahead and delete the rules you created.

1. Click the x next to the FIN_APP_rules.
2. Click Yes to confirm deletion.

Click Publish Changes.

Verify the changes have been applied.
Module 3 Conclusion

In this module we showed the various options that can be configured as part of Flow Monitoring as well as the ability to actually monitor allowed or denied flows to and from a virtual machines network interface card. Flow monitoring is very useful in troubleshooting connectivity as well as helping to lock down the application by only allowing flows the application requires.

You've finished Module 3

Congratulations on completing Module 3.

If you are looking for additional information on Flow Monitoring visit the URL below:

- Go to https://tinyurl.com/y9s328qj

Proceed to any module below which interests you most.

Lab Module List:

- **Module 1 - Log Insight Management Pack Review** (15 minutes) - Basic - This module covers the basics of the NSX Log Insight Management Pack and how to install it within Log Insight.
- **Module 2 - Log Insight Dashboards** (15 minutes) - Basic - This module covers the Log Insight Dashboard and how to successfully navigate around the interface.
- **Module 3 - Flow Monitoring Configuration** (30 minutes) - Basic - This module covers the basics of NSX Flow Monitoring. It starts off by giving you a tour of all the available options and then how to monitor the flows of a particular VMs vNIC.
- **Module 4 - Traceflow** (30 minutes) - Basic - This module covers the basics of Traceflow and how to initiate a Traceflow between two VMs to view an "Allowed" and "Blocked" result.
- **Module 5 - Central CLI** (15 minutes) - Basic - This module shows the power of Central CLI and how you can easily retrieve valuable information relating to NSX via a single Central CLI.
- **Module 6 - Endpoint Monitoring** (15 minutes) - Basic - This module shows an overview of Endpoint Monitoring and how you can easily monitor internal guest processes for specific VMs

Lab Captain:

- **Module 1 through 6 - Mostafa Magdy, Senior Systems Engineer, Canada**
How to End Lab

To end your lab click on the **END** button.
Module 4 - Traceflow with NSX (30 minutes)
Introduction to improved operational visibility with Traceflow

Traceflow is a feature that improves operational visibility and troubleshooting NSX within your virtual environment. Traceflow allows you to inject a packet into the vNIC, which has no reliance on the guest operating system, and follow it through the various distributed firewall policies all the way through to the destination virtual machine. Traceflow supports both L2 and L3 destinations and allows you to quickly identify problems and pinpoint an issue in the NSX data path.
Traceflow between two Virtual Machines

Within the module we are going to walk you through performing a Traceflow between two virtual machines and analysing the results of a successful and blocked packet flows.

Accessing the vSphere Web Client

Before we can perform a Traceflow we need to login to the vSphere Web Client.

Launch the Chrome web browser

Launch the Chrome browser shortcut from the desktop or the taskbar.

Access the vSphere Web Client

1. From within the Chrome bookmarks menu bar click on the vCenter - Region A bookmark.

Login to the vSphere Web Client
If you are not already logged into the vSphere Web Client:

(The home page should be the vSphere Web Client. If not, Click on the vSphere Web Client Taskbar icon for Google Chrome.)

1. Check **Use Windows session authentication**.
2. Click **Login**

### Enable Traceflow Distributed Firewall rule

The first step that we need to complete is to enable the Distributed Firewall rule that will block communication from **web-01a.corp.local (172.16.10.11)** to **web-02a.corp.local (172.16.10.12)**. This will allow us to perform a Traceflow between the two virtual machines on the same L2 segment.

### Navigate to Networking & Security

1. From the vCenter Web Client **home** button.
2. CLICK on the **Network & Security** tab to access the NSX interface.
Navigate to Firewall

1. Click on the **Firewall** tab.
2. Click on the arrow to expand the section called **Flow Monitoring & Trace Flow Rules-Disabled by Default**.
3. Click the **Green tick** to enable the Flow Monitoring Test rule **ID:1006**. The coming steps will show you how to create one:
1. Click on the small pencil icon to add a source.

1. From the Object Type drop-down menu select **Virtual Machine**.
2. Select **web-01a.corp.local**
3. Click the **arrow** to add the virtual machine to the rule.
4. Click **OK**.

Repeat the above steps for the Destination and select **web-02a.corp.local**.

For the service part,
1. From the Object Type drop-down menu select **Service**.
2. Select **HTTP**
3. Click the **arrow** to add the virtual machine to the rule.
4. Click **OK**.

![Rule 1 - Edit Action](image)

1. For Action, select **Block**.
2. Select **Save**.

![Configuration](image)

This is what final rule should look like.

1. Select **Publish Changes**.
Verify the Publish has succeeded

1. Verify that the publish operation has completed successfully (Please note the date of your publish will not be identical to the screenshot).

Perform a Traceflow

1. Within the Networking & Security tab click on Traceflow.

Traffic Type

1. If you click on the Traffic Type drop down menu you have the option to select Unicast, L2 Multicast of L2 Broadcast traffic to simulate. Leave the option set as Unicast.
Select the source virtual machine

1. Click on the **Select** link next to Source.
2. Within the search field type **web-01a.corp.local** and press enter.
3. Click on the right arrow next to the virtual machine that will be your source.
Source virtual machine vNIC

1. Click on the vNIC that you want to inject the packet into.
2. Click OK to confirm the selection.
1. Click on the **Select** link next to the Destination. You can either perform a L2 or L3 Traceflow based on destination IP or MAC address or select a particular virtual machine.
1. Check the option to **Select Destination vNIC**.
2. Click on the right arrow next to the virtual machine that will be your source, in this case, **web-02a.corp.local**.
1. Click on the vNIC that you want to inject the packet into.
2. Click **OK** to confirm the selection.
Clicking on the **Advanced Options** arrow allows you to configure additional options relating to the packet you are about to inject into the vNIC. You can configure the Protocol which can be either ICMP, TCP or UDP as well as ICMP ID, Sequence, Timeout, Frame size and TTL. Additional options are presented based on the protocol that you select. In this example we will be using TCP which allows you to additionally configure the Source and Destination port as well as any TCP Flags that you may wish to set.

1. Click on the arrow next to **Advanced Options**.
2. Change the Protocol to **TCP**.
3. Set the **Destination Port** to **80**.
4. Ensure the **SYN** TCP Flag is checked.
5. Click **Trace** to inject the packet and start following it through the infrastructure.

### Long Running Task

Clicking on the **Long Running Task** allows you to continue polling the network if the task is taking longer than expected.
1. If you receive a message box advising that the current task is taking too long to complete and do you want to continue polling click Yes. This is due to the effects of the nested environment for which this lab is running in.

**Reviewing Traceflow results**

![Traceflow results table](image)

1. Once the results have been returned you should see the end result being that the packet was **Dropped** due to the rule we enabled earlier.
2. We can follow the packet and see that it was injected into the vNIC and then received by the egress firewall and blocked by **Rule 1007**. If this was unexpected behaviour then we could investigate rule 1005 so see if this should be in place or not.

**Disable Traceflow Distributed Firewall rule**

If we now disable the Distributed Firewall rule to allow communication from **web-01a.corp.local (172.16.10.11)** to **web-02a.corp.local (172.16.10.11)** we can perform the Traceflow again and see a successful packet delivery.
Navigate to Firewall

1. Click on the **Firewall** tab.
2. Click on the arrow to expand the section called **Flow Monitoring Rules-Disabled by Default**.
3. Click the **Green tick** to disable the Flow Monitoring Test rule.
4. Click **Publish Changes** to push the rules down to the hypervisor.

Verify the Publish has succeeded

1. Verify that the publish operation has completed successfully (Please note the date of your publish will not be identical to the screenshot).
Perform a Traceflow

1. Within the **Networking & Security** tab click on **Traceflow**.
Select the source virtual machine

1. Click on the Select link next to Source.
2. Within the search field type `web-01a.corp.local` and press enter.
3. Click on the right arrow next to the virtual machine that will be your source.
Source virtual machine vNIC

1. Click on the vNIC that you want to inject the packet into.
2. Click **OK** to confirm the selection.
Select the destination

1. Click on the **Select** link next to the Destination. You can either perform a L2 or L3 Traceflow based on destination IP or MAC address or select a particular virtual machine.
1. Check the option to **Select Destination vNIC**.
2. Click on the right arrow next to the virtual machine that will be your source.
1. Click on the vNIC that you want to inject the packet into.
2. Click **OK** to confirm the selection.
**Advanced Options**

Clicking on the **Advanced Options** arrow allows you to configure additional options relating to the packet you are about to inject into the vNIC. You can configure the Protocol which can be either ICMP, TCP or UDP as well as ICMP ID, Sequence, Timeout, Frame size and TTL. Additional options are presented based on the protocol that you select. In this example we will be using TCP which allows you to additionally configure the Source and Destination port as well as any TCP Flags that you may wish to set.

1. Click on the arrow next to **Advanced Options**.
2. Change the Protocol to **TCP**.
3. Set the **Destination Port** to **80**.
4. Ensure the **SYN** TCP Flag is checked.
5. Click **Trace** to inject the packet and start following it through the infrastructure.

**Long Running Task**

![Long Running Task](image)
1. If you receive a message box advising that the current task is taking too long to complete and do you want to continue polling click Yes. This is due to the effects of the nested environment for which this lab is running in.

**Reviewing Traceflow results**

1. Once the results have been returned you should see the end result being that the packet was now Delivered. This was due to the rule we previously disabled.
2. We can follow the packet and see that it was injected into the vNIC, passes the distributed firewall on egress and then encapsulated and delivered to the receiving host and then successful passes through the distributed firewall on ingress.
3. You may have to scroll down to see the full Traceflow information
Filtering results

1. You also have the ability to filter the results based on Observation Type, Component Type, Component Name and Host by clicking on the filter icon and selecting the appropriate criteria.
2. Select the appropriate filter criteria.
3. Click **Apply**.
Module 4 Conclusion

In this module we showed how to perform a Traceflow between two virtual machines and the expected results from both a successful and failed delivery attempt. We also showed how additional options could also be configured to perform a Traceflow based on ports rather than ICMP as well as filtering the response.

You've finished Module 4

Congratulations on completing Module 4.

If you are looking for additional information on Traceflow visit the URL below:

Go to https://tinyurl.com/y8dkb4kj

Proceed to any module below which interests you most.

Lab Module List:

- **Module 1 - Log Insight Management Pack Review** (15 minutes) - Basic - This module covers the basics of the NSX Log Insight Management Pack and how to install it within Log Insight.
- **Module 2 - Log Insight Dashboards** (15 minutes) - Basic - This module covers the Log Insight Dashboard and how to successfully navigate around the interface.
- **Module 3 - Flow Monitoring Configuration** (30 minutes) - Basic - This module covers the basics of NSX Flow Monitoring. It starts off by giving you a tour of all the available options and then how to monitor the flows of a particular VMs vNIC.
- **Module 4 - Traceflow** (30 minutes) - Basic - This module covers the basics of Traceflow and how to initiate a Traceflow between two VMs to view an "Allowed" and "Blocked" result.
- **Module 5 - Central CLI** (15 minutes) - Basic - This module shows the power of Central CLI and how you can easily retrieve valuable information relating to NSX via a single Central CLI.
- **Module 6 - Endpoint Monitoring** (15 minutes) - Basic - This module shows an overview of Endpoint Monitoring and how you can easily monitor internal guest processes for specific VMs

Lab Captain:

- **Module 1 through 6 - Mostafa Magdy, Senior Systems Engineer, Canada**
How to End Lab

To end your lab click on the **END** button.
Module 5 - The NSX Central CLI (15 minutes)
Introduction to Improved Operation Visibility with Central CLI

In this module, you will be exploring Central CLI, which is a tool to assist in operational activities when working with NSX for vSphere.

Prior to Central CLI if an administrator wanted to gain details on constructs such as the NSX Edge Gateways (as well as the services running on them), Distributed Logical Routers, and Logical Switches, they would require console access to one or more of the following:

- NSX Manager
- NSX Controllers
- NSX Edge Gateways

With Central CLI one can simply gain access to the console of the NSX Manager for gaining such details, rather than jumping between multiple console/SSH sessions. This provides administrators with a more streamlined path for accessing operational data, and can help speed up the troubleshooting of issues that may occur within an environment where NSX for vSphere is deployed.

Before going into more detail about what those new commands are, and the types of scenarios you will be going through in this module, please proceed to the next step where you will be performing a number of setup steps to get logged into the primary NSX Manager.

Setup

You will be performing a number of commands on the primary NSX Manager (nsxmgr-01a.corp.local) via the Windows SSH client PuTTY.

Opening PuTTY

1. Click on the Putty icon located on the taskbar.
Configuring NSX Manager SSH Connection in PuTTY

Within the PuTTY Configuration window, to load the connection details for the primary NSX Manager (nsxmgr-01a.corp.local).

1. Search for the session labelled `nsxmgr-01a.corp.local` under the Saved Sessions list and click on it.
2. Click the Open button.

NSX Manager Command Prompt

1. Enter `VMware1!` as the password.
NSX Centralized CLI Command List

Before continuing, it is worth taking a look at a list of the available commands within NSX Manager. To do this simply type in the following command at the command prompt:

```
list
```

As you can see, there are quite a few new options available for obtaining information from the NSX Manager CLI, including options that used to require an administrator to gain console access to individual NSX Edge Gateways, ESXi Hosts, or NSX Controllers.

1. You might have to scroll up and down within the PuTTY window to view the entire list of commands.

Please leave this PuTTY window open, and proceed to the next step, where you will start with taking a look at some commands that will help out in troubleshooting VXLAN connectivity.
Troubleshooting Logical Switches

Prior to Central CLI it was necessary to SSH/console into the NSX Manager, ESXi hosts, and NSX Controllers to get troubleshooting information for constructs like:

- VTEPs (VXLAN Tunnel Endpoints)
- VNIs (VXLAN Network Identifiers)
- ARP/MAC/IP tables for Logical Switches
- General Control Plane Information

In this section, you will be exposed to a number of commands available from the NSX Manager CLI to allow an administrator to gather details regarding the above in one place. Continue to the next step to start gathering details about the vSphere Clusters, ESXi Hosts, and Virtual Machines on matters pertaining to network virtualization.

**Note:** You may find it useful to increase the width of the PuTTY window, or maximize the size of the window before proceeding as some of the output from the following commands may run over more than one line, which may make it difficult to read.

**Cluster/Host/VM Details**

For a majority of the commands covered in this module, it's required to know a specific Host-iD (ESXi Host), Domain-iD (vSphere Cluster), VM-iD (Virtual Machine), and/or vNIC-iD (Virtual NIC on Virtual Machine). The following commands will walk you through how to obtain those values. The specific IDs will be mentioned in the later sections of this module, but this is how one would normally find those identifiers.

**Listing all clusters**

```
show cluster all
```

To list all clusters run the following command:

```
show cluster all
```

The output received should be similar to the screenshot above. With columns for:

- Cluster Name - The name of the vSphere cluster.
Let us find out more information about **RegionA01-COMP01** so continue to the next step to find out how to retrieve a list of hosts for that cluster.

### Showing all hosts in a cluster

To list the set of hosts in a vSphere cluster, run the following command:

```bash
show cluster domain-c26
```

The output received should look like what's shown in the screenshot, with columns for:

- **Host Name** - The fully qualified domain name (FQDN) of the ESXi host in the vSphere Cluster.
- **Host ID** - Unique identifier for the ESXi host (to be used later in this module).
- **Installation Status** - Whether or not the necessary network virtualization components (ESXi VIBs for VXLAN, Distributed Firewall, and Logical Routers)

Perhaps in a troubleshooting scenario it's found that a VM that's lacking connectivity happens to be a host that isn't fully prepared for NSX, and does not have a status of "Ready" for it's installation status of network virtualization components? Now you know a quick way to query hosts to find out without having to log into the vSphere Web Client.

### Specific Host Health (Healthy)

```bash
show host host-31 health-status
```

Status: HEALTHY

nsxmgr-01a.corp.local>
This command allows the ability to quickly review the health of a specific host. The command runs 30+ checks in one command which includes network configuration, VXLAN configuration and resource utilization.

```
show host host-31 health-status
```

The status will show either Healthy, Unhealthy or Critical depending on the severity of the errors.

**Specific Host Health (Unhealthy)**

```
nsxmgr-01a> show host host-31 health-status
CRITICAL, VXLAN VDS "RegionA01-vDS-COMP" has no vmknic.
Status: CRITICAL
```

This shows an unhealthy host. For this example We removed the VXLAN VMkernel (VMK) interface from the host to produce the error.

**Specific Host Details**

```
nsxmgr-01a.corp.local> show host host-31
Datacenter: RegionA01
Cluster: RegionA01-COMP01
Host: esx-02a.corp.local

No.  VM Name               VM Id   Power Status
1    win-xp-01.corp.local   vm-290   on
2    db-01a.corp.local     vm-277   on
3    web-01a.corp.local    vm-272   on
```

```
nsxmgr-01a.corp.local> show host host-29
Datacenter: RegionA01
Cluster: RegionA01-COMP01
Host: esx-01a.corp.local

No.  VM Name               VM Id   Power Status
1    web-03a.corp.local    vm-275   on
2    web-02a.corp.local    vm-273   on
3    app-01a.corp.local    vm-278   on
4    hr-db-01a.corp.local  vm-287   on
5    fin-db-01a.corp.local vm-281   on
```

To list the Virtual Machines (VMs) on each of the hosts, run the following two commands:

```
show host host-31
```
show host host-29

The values host-31 and host-29 refer to the Host IDs of both esx-01a.corp.local and esx-02a.corp.local, respectively. These values will be passed into the show host command to retrieve the following values about the VMs running on these hosts:

- **VM Name** - The name of the Virtual Machine as it's seen in the vSphere Client.
- **VM ID** - Unique identifier for the VM (to be used later in this module).
- **Power Status** - Whether or not the Virtual Machine is currently powered on.

Going forward, you will be singling out the virtual machine **web-01a**, so the VM ID **vm-272** will be used quite often for other commands used in this module. To find out more about the vNIC details of **web-01a** proceed to the next step.

### Specific VM Details

```plaintext
show vm vm-272
```

Enumerating the vNIC details of a VM can be performed with the following command:

show vm vm-272

Here, we are passing the VM ID of **vm-272** which is referring to the VM **web-01a**. The output received should be similar to the screenshot shown, with the following properties:

- **Vnic Name** - The name of the vNIC as seen on the VM **web-01a**. In this case, it is `web-01a.corp.local - Network adapter 1`
- **Vnic ID** - Unique identifier for this specific vNIC object. In this case, it is `50084a2c-2d2a-10cf-5d05-4bc5f5bab1b1.000` which is a value to be used later in this module for other commands.
- **Filters** - This refers to the Distributed Firewall (DFW) Filter ID applied to the VM. There will be more details on that later in this module.
Next, to gather more details regarding that specific vNIC.

**Specific vNIC Details**

To obtain further details about the vNIC of a VM, use the command "show vnic <vNIC ID>." For the vNIC of the **web-01a** VM, enter in the following command, please feel free to copy the vnic instead of typing the whole command:

```bash
show vnic 50084a2c-2d2a-10cf-5d05-4bc5f5bab1b1.000
```

In the results, you will notice the following details being returned:

- **MAC Address** - The MAC address of the vNIC on the VM **web-01a**
- **Port Group ID** - Unique identifier for the distributed virtual switch portgroup. In this case, it is **dvportgroup-246**
- **Filters** - As shown in the previous command, the unique identifier for the DFW filter is also displayed for this vNIC.
- **VXLAN** - Information related to the VXLAN configuration such as ID, Multicast IP, VTEPs etc.

Now that you have been introduced to some preliminary commands to gather information such as the VM ID, vNIC ID, Host ID, and Cluster ID, you will be using those to dive into some additional details about the Logical Switches themselves in the next section.

**Logical Switch Commands**

Next up, you'll be going through the set of options available in the "show logical-switch" command. Specifically, you'll be going through the following scenarios:

- List all Logical Switches
- Logical Switch Details on a Host - Verbose
List all Logical Switches

To list all the Logical Switches under the management of this NSX Manager, run the following command:

```
show logical-switch list all
```

If the command has been run successfully, you should see results similar to the screenshot. The values you should observe returned from this command are:

- **Name** - The name of the logical switch.
- **UUID** - A unique identifier for the logical switch.
- **VNI** - The VXLAN Network Identifier that the logical switch sits on.
- **Trans Zone Name** - The name of the transport zone that the Logical Switch resides in.
- **Trans Zone ID** - The unique identifier of the transport zone that the Logical Switch resides in.

Next, you'll be obtaining some additional details on logical switches specific to an ESXi host.
Logical Switch Details On a Host - Verbose

To list the verbose details of all logical switches on a host, run the following command:

```
show logical-switch host host-29 verbose
```
This will display quite a lot of information regarding the logical switches running on the host, and you will need to use the space key to fully scroll through all of it before getting the command prompt to come back up again. Some details worth noting here are:

- Control Plane Sync Status and UDP Port Used for the Control Plane.
- Details regarding the Distributed Virtual Switch for which the Logical Switches reside upon.
- Number of Logical Switches recognized by the host currently.
- Detail specific to a Logical Switch, including:
  - VXLAN Network Identifier (VNI)
  - Multicast IP (if the replication mode is set to be Multicast or Hybrid. Unicast is utilized in this lab, so "N/A" is expected.)
  - NSX Controller which currently has the slice for the Logical Switch
  - Number of MAC and ARP Entry Counts

Next, you will observe some statistics pertaining to logical switches on a particular ESXi host.

**Logical Switch Details On a Host - Statistics**

```
nsxmgr-01a.corp.local> show logical-switch host host-29 statistics

tx.passThrough: 0
tx.vxlanTotal: 0
tx.clone: 0
tx.tso: 0
tx.csun: 0
tx.drop.invalidFrame: 0
tx.drop.guestTag: 0
tx.drop.noResource: 0
tx.drop.invalidState: 10
rx.passThrough: 0
rx.vxlanTotal: 0
rx.clone: 0
rx.drop.invalidFrame: 0
rx.drop.notExist: 198376
rx.drop.noResource: 0
forward.pass: 0
forward.reject: 0
forward.rpl: 0
arpProxy.reply.total: 5
arpProxy.reply.fail: 0
arpProxy.request.total: 0
arpProxy.request.fail: 0
mcastProxy.tx.total: 0
mcastProxy.tx.fail: 0
mcastProxy.rx.total: 0
mcastProxy.rx.fail: 0
cdo.replicate.tx.total: 0
cdo.replicate.tx.fail: 0
cdo.mcastProxy.tx.total: 0
cdo.mcastProxy.tx.fail: 0
nsxmgr-01a.corp.local>
```
To obtain statistics regarding logical-switches on a host, run the following command:

```
show logical-switch host host-29 statistics
```

In the case of a lack of L2 traffic between VMs on the same Logical Switch on different ESXi hosts, the counters here would be of use to watch for troubleshooting purposes.

### List all Hosts With VMs on a specific VNI

If you wanted to know what hosts have VMs on a specific VXLAN Network Identifier (VNI), you can run the following command:

```
show logical-switch list vni 5000 host
```

Here, we're displaying all ESXi hosts that currently have VMs on a specific VNI. The details shown are:

- **ID** - This is specifically referring to the Host ID, a unique identifier for the ESXi host.
- **HostName** - The fully qualified domain name for the ESXi host.
- **VdsName** - The Distributed Virtual Switch that the ESXi host resides on with the associated logical switch/VNI.

### List VTEP IP Addresses and MAC Addresses on a Controller Slice for a specific VNI

```
show logical-switch controller controller-2 vni 5000 vtep
```

<table>
<thead>
<tr>
<th>VNI</th>
<th>IP</th>
<th>Segment</th>
<th>MAC</th>
<th>Connection-ID</th>
<th>Is-Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>5000</td>
<td>192.168.130.51</td>
<td>192.168.130.0</td>
<td>00:50:56:56:b1:ce</td>
<td>4</td>
<td>YES</td>
</tr>
<tr>
<td>5000</td>
<td>192.168.130.53</td>
<td>192.168.130.0</td>
<td>00:50:56:56:b1:b7</td>
<td>7</td>
<td>YES</td>
</tr>
<tr>
<td>5000</td>
<td>192.168.130.54</td>
<td>192.168.130.0</td>
<td>00:50:56:56:98:4d</td>
<td>1</td>
<td>YES</td>
</tr>
</tbody>
</table>
To determine if a particular VNI has VTEP/MAC Table information on a NSX Controller, perform the following command:

```bash
show logical-switch controller controller-2 vni 5000 vtep
```

It's possible that this command may not return any details, so if that occurs, replace the `controller-2` in the command above with either `controller-1` or `controller-3`. The IP addresses shown here refer to the VTEP IP addresses on the ESXi hosts.

**List ARP Table Entries on a Controller Slice for a specific VNI**

To list ARP Table entries for a specific VNI on a NSX Controller, run the following command:

```bash
show logical-switch controller controller-2 vni 5000 arp
```

As before, it's possible that this command may not return any details, so if that occurs, replace the `controller-2` in the command above with either `controller-1` or `controller-3`. The IP address shown here belongs to a VM. If there are no entries try pinging `web-01a` or `web-02a` from the main console.

**List MAC/VTEP Table Entries on a Controller Slice for a specific VNI**

To display the MAC Address/VTEP table for a given VNI on a NSX Controller, input the following command:

```bash
show logical-switch controller controller-2 vni 5000 mac
```
If no results return, try again with one of the other two NSX Controllers.

**Show Statistics for a specific VNI on a Controller**

To display a number of statistics pertaining to the VNI on a NSX Controller, run the following command:

```
show logical-switch controller controller-2 vni 5000 statistics
```

**Show Slice Detail for Joined-VNIs on a Specific Host**

To show details pertaining to joined VNIs for a specific host on a NSX Controller, provide the command:

```
show logical-switch controller controller-2 host 192.168.110.51 joined-vnis
show logical-switch controller controller-2 host 192.168.110.52 joined-vnis
```

In this command, **controller-2** can be replaced with either **controller-1** or **controller-3**, and the host IP referenced here is for ESXi host's VTEP IP address. In the screenshot above, the VTEP IP addresses for hosts **esx-01a.corp.local** (**192.168.110.51**) and **esx-02a.corp.local** (**192.168.110.52**) are provided.
That only covers some of the new commands available regarding Logical Switches. In the next part, you'll be exploring what's available for troubleshooting Distributed Logical Routers.
Troubleshooting Distributed Logical Routers

Next, you will learn about some of the commands available to troubleshoot the distributed logical routers you have deployed in your NSX for vSphere environment. Before we jump into the commands themselves, take a look at the next page to get a refresher on some of the unique identifiers that will be utilized for some of these commands, and what they refer to. Feel free to come back to that page during the rest of the steps in this section if you want.

Reference IDs

As with the logical switch commands, there are a number of unique identifiers to be referenced when running some of the new logical-router commands in the NSX Manager CLI. These are provided here for ease of reference:

**vSphere Clusters**

RegionA01-MGMT01 : domain-c121
RegionA01-COMP01 : domain-c26
RegionA01-COMP02 : domain-c265

**ESXi Hosts**

esx-01a.corp.local : host-29
esx-02a.corp.local : host-31

**Virtual Machines**

web-01a.corp.local : vm-272
web-02a.corp.local : vm-273
web-03a.corp.local : vm-275
app-01a.corp.local : vm-278
db-01a.corp.local : vm-277
Logical Router Commands

Now that you have a refresher on some of the identifiers for the objects you will be looking at, move on to the next step to learn how to obtain a list of all deployed distributed logical routers.

List all Logical Routers

To list all distributed logical routers, run the following command:

```
show logical-router list all
```

The following values will be returned:

- Edge-ID - The unique identifier of the Control VM for the Distributed Logical Router
- VDR-Name - The name of the Distributed Logical Router.
- VDR-ID - The unique identifier of the Distributed Logical Router.
- #Lifs - Number of Logical Interfaces connected to the Logical Router.

Show ESXi Hosts where a Logical Router Exists

To display what ESXi hosts a specific Distributed Logical Router exists, enter the following commands:

```
show logical-router list dlr edge-2 host
```

To display what ESXi hosts a specific Distributed Logical Router exists, enter the following commands:
show logical-router list dlr edge-2 host

That will return the unique ID of the ESXi host, as well as the "friendly" host name of the ESXi host where a given DLR is recognized.

**Show Logical Router Connection Details on a specific ESXi Host**

```
nsxmgr-01a.corp.local> show logical-router host host-29 connection
Host locale Id: 42080ad5-d890-04c9-31c2-8a457c5588ed
Connection Information: 
------------------------
DvsName   VdrPort   NumLifs   VdrVmac
--------   -------   --------   -------
RegionA01-vDS-COMP vdrPort 3 02:50:56:56:44:52
 Vdr Switch Port: 33554442
 Teaming Policy: Default Teaming
 Uplink: uplink1(33554436): 00:50:56:f6:94:bc (Team member)
 Uplink: uplink2(33554434): 00:50:56:f6:b0:c2 (Team member)

Stats: Pkt Dropped  Pkt Replaced  Pkt Skipped
Input : 0           0            930324938
Output: 5           0            3508410

nsxmgr-01a.corp.local> show logical-router host host-31 connection
Host locale Id: 42080ad5-d890-04c9-31c2-8a457c5588ed
Connection Information: 
------------------------
DvsName   VdrPort   NumLifs   VdrVmac
--------   -------   --------   -------
RegionA01-vDS-COMP vdrPort 3 02:50:56:56:44:52
 Vdr Switch Port: 33554442
 Teaming Policy: Default Teaming
 Uplink: uplink1(33554436): 00:50:56:f6:64:d4 (Team member)
 Uplink: uplink2(33554434): 00:50:56:f7:e8:ea (Team member)

Stats: Pkt Dropped  Pkt Replaced  Pkt Skipped
Input : 0           0            929413352
Output: 6           0            3881147
```
To display physical network connection information for a given ESXi host where a distributed logical router is deployed on, run the following commands:

```
show logical-router host host-29 connection
show logical-router host host-31 connection
```

This will display information regarding the Distributed Virtual Switch that the logical routers on the ESXi host utilize, as well as the number of logical interfaces (LIFs).

Additionally, information regarding the uplinks used by the DVS, and statistics regarding the number of packets dropped, replaced, and skipped are shown.
Show Verbose Information for a specific Logical Router on a specific ESXi Host

A good quick way to obtain useful information regarding a DLR on a specific ESXi host can be to run the following command (shown here for two hosts):

```
show logical-router host host-29 dlr edge-2 verbose
```

```
show logical-router host host-31 dlr edge-2 verbose
```

Details such as the name of the DLR, the DLR ID, the number of LIFs and routes, the type of DLR (global or universal), and the NSX Controller owning the slice pertaining to this DLR are shown.
Show ARP Table Entries for a specific Logical Router on a specific ESXi Host

Another useful command which can display the ARP table for a given DLR on an ESXi host is the following (once again, shown for two different hosts):

```
show logical-router host host-29 dlr edge-2 arp
```

```
show logical-router host host-31 dlr edge-2 arp
```

One will notice that some of the IP addresses appear on both hosts, that would be because these are the interfaces of the logical-routers themselves (which would exist on all hosts).
Show Routing Table Entries for a specific Logical Router on a specific ESXi Host

It is definitely useful to be able to obtain routing table information for a given logical-router, and rather than SSH'ing to every host to obtain that information, one can run the following command within the NSX Manager:

```
show logical-router host host-29 dlr edge-2 route
```

```
show logical-router host host-31 dlr edge-2 route
```

Show LIF Configuration on a Controller for a specific Logical Router

To display the Logical Interface (LIF) configuration present on a controller for a given DLR, run the following command:

```
show logical-router controller controller-3 dlr edge-2 interface
```

```
138800000000a
138800000000b
1388000000002
```
The IP address of the LIF will be shown, as well as the unique ID for the LIF (see the column "Id"). If the command does not return anything, try replacing "controller-1" with "controller-2" or "controller-3".

### Show Brief Details on a Controller for a specific Logical Router

Rather than running the aforementioned verbose command, one can obtain a smaller subset of information for a given DLR on a specific controller by running the following command:

```plaintext
show logical-router controller controller-3 dlr edge-2 brief
```

Information shown includes:

- **LR-ID** - The unique identifier of the Distributed Logical Router.
- **LR-Name** - The name of the Distributed Logical Router.
- **Universal** - This identifies a DLR as being a Universal DLR (value will be true) or a Global DLR (value will be false).
- **Service-Controller** - This displays the NSX Controller owning the slice for this specific DLR.
- **Egress-Locale** - This will identify the Egress-Locale ID if the DLR is a Universal DLR, or "local" if it's a Global DLR.
- **In-Sync** - If the DLR is a Universal DLR, then this will display the current synchronization status of the Universal DLR, and if the DLR is a Global DLR, it will show "N/A".

Next up, you will learn about one of the biggest time savers Central CLI offers - the ability to obtain information about NSX Edge Gateways, all without having to enable SSH on an Edge (or console into one)!
Troubleshooting Edge Service Gateways

Remember when one had to enable SSH or utilize a VMRC session to get access to an Edge Gateway and obtain details about the services running on it?

Those days are gone; welcome to the age of Central CLI.

This section will go over some of the many options available to the NSX Administrator with regards to the Edge Gateways. Provided in the next step are a set of Reference IDs for the vSphere clusters, ESXi hosts, and Virtual Machines in the environment for easy reference. After that, you will jump right in to going over some of the Edge Gateway related commands available in Central CLI located on the NSX Manager.

Reference IDs

These are provided here for ease of reference:

**vSphere Clusters**

RegionA01-MGMT01 : domain-c121
RegionA01-COMP01 : domain-c26
RegionA01-COMP02 : domain-c265

**ESXi Hosts**

esx-01a.corp.local : host-29
esx-02a.corp.local : host-31

**Virtual Machines**

web-01a.corp.local : vm-272
web-02a.corp.local : vm-273
web-03a.corp.local : vm-275
app-01a.corp.local : vm-278
As mentioned before, feel free to come back to the Reference-IDs section if you happen to forget how to obtain any of the unique identifiers for objects like clusters, hosts, or VMs. Next up, you'll learn how to obtain a list of all deployed NSX Edge Gateways in an environment.

**Show all NSX Edge Gateways**

To list all deployed NSX Edge Gateways for a given NSX Manager (this will not show Edge Gateways across multiple sites), run the following command:

```
show edge all
```

The values returned refer to the following:

- **Edge ID** - The unique identifier of the NSX Edge Gateway.
- **Name** - The friendly name of the NSX Edge Gateway.
- **Size** - This refers to the size of the NSX Edge Gateway. C = Compact, L = Large, X = X-Large, Q = Quad-Large
- **Version** - This will show the software version of the Edge. (This command can be especially handy when looking to identify NSX Edge Gateways that are running out-of-date code).
- **Status** - This refers to the current status of the NSX Edge Gateway.
Now that you're able to identify the list of NSX Edge Gateways, as well as their unique identifier (the Edge ID value), continue to the next step to learn how to show more details about a specific Edge Gateway.

**Show Details of a specific NSX Edge Gateway**

To get a quick view of what services are enabled on an Edge Gateway, as well as some other miscellaneous information, input the following command:

```
show edge edge-1
```

Returned is the following data:

- Details such as the friendly name of the Edge, the size of the Edge, what ESXi host it's currently running on, and if it's currently deployed or not.
- One can see whether or not if any of the various Edge Gateway Services are enabled here.

Given that one can tell the routing service is running from the above command, let's take a look at some more details about how routing is configured.
Show Routing Service Details on a specific NSX Edge Gateway

To show the routing configuration of an Edge Gateway, run the following command:

```
show edge edge-1 configuration routing-global
```

What will be returned is a JSON message detailing the various details of the routing configuration.

Retrieve Flow Table for a specific NSX Edge Gateway

To display the current flowtable of a given NSX Edge Gateway (edge-1 is used in this example), enter the following command:

```
show edge edge-1 flowtable
```

Returned will be the total number of flows currently active on the Edge Gateway, showing details such as the protocol in use, the source/destination IP addresses, the
source/destination ports, and the number of packets and bytes seen for the particular flow.

Display BGP Details on a specific NSX Edge Gateway

Displaying dynamic routing information quickly for any Edge Gateway is a huge benefit of the new Central CLI, and in this example you'll be taking a look at the BGP details for the Edge Gateway Perimeter-Gateway-01. To do so, enter the command:

```
show edge edge-1 ip bgp
```

In addition to the ability to display dynamic routing details, one can also show the routing table of a given edge. Continue to the next step to learn how to do so.
Display Routing Table Information on a specific NSX Edge Gateway

To retrieve the routing table of a particular Edge Gateway, type the following command in (once again, the Edge Gateway Perimeter-Gateway-01 is used here):

```
show edge edge-1 ip route
```

This command will show all static and dynamically obtained routes for the Edge Gateway.
Display Top 10 Flows per Firewall Rule on a specific NSX Edge Gateway

In case you also wanted to be able to obtain more details regarding the firewall on the Edge Gateway, such as the top flows matching for any particular firewall rule, the following command can be utilized:

```
show edge edge-1 firewall flows topN 10
```

Next, you'll learn about some of Central CLI commands available for obtaining information about the Distributed Firewall.
Troubleshooting Distributed Firewall

In this last section of the module for exploring Central CLI, you’ll be looking at some of the commands available to deal with the Distributed Firewall (DFW). As in previous sections, the next step will include a list of Reference IDs for objects such as vSphere clusters, ESXi Hosts, and VMs for quick reference.

Reference IDs

These are provided here for ease of reference:

**vSphere Clusters**

RegionA01-MGMT01 : domain-c121
RegionA01-COMP01 : domain-c26
RegionA01-COMP02 : domain-c265

**ESXi Hosts**

esx-01a.corp.local : host-29
esx-02a.corp.local : host-31

**Virtual Machines**

web-01a.corp.local : vm-272
web-02a.corp.local : vm-273
web-03a.corp.local : vm-275
app-01a.corp.local : vm-278
db-01a.corp.local : vm-277
hr-db-01a.corp.local : vm-287
fin-db-01a.corp.local : vm-281
win-xp-01.corp.local : vm-290
Accessing the vSphere Web Client

Before we can view Distributed Firewall rules via Central CLI we need to enable a rule.

Launch the Chrome web browser

Launch the Chrome browser shortcut from the desktop or the taskbar.

Access the vSphere Web Client

1. From within the Chrome bookmarks menu bar click on the vCenter - Region A bookmark.

Login to the vSphere Web Client

If you are not already logged into the vSphere Web Client:

(The home page should be the vSphere Web Client. If not, Click on the vSphere Web Client Taskbar icon for Google Chrome.)

1. Click checkmark next to Windows session authentication
2. Click Login

Enable Traceflow Distributed Firewall rule

The first step that we need to complete is to enable the Distributed Firewall rule that will block communication from web-01a.corp.local (172.16.10.11) to
web-02a.corp.local \textbf{(172.16.10.11)}. This will allow us to see the rule actually pushed down to the hypervisor and applied to \textit{web-01a.corp.local} that will be visible in Central CLI.

**Navigate to Networking & Security**

![Navigation Screenshot]

1. From the vCenter Web Client home screen click on the \textbf{Network & Security} tab to access the NSX interface.

**Verify the Publish has succeeded**

![Publish Success Screenshot]

1. Verify that the publish operation has completed successfully (Please note the date of your publish will not be identical to the screenshot).

Navigate back to your Central CLI PuTTY session to continue with the lab.

**Distributed Firewall Commands**

Next you will learn how to show the current status of the Distributed Firewall on all vSphere clusters managed by a particular NSX Manager.
Show Distributed Firewall Status on all vSphere Clusters

To show the current status of the Distributed Firewall on a cluster, run the following command:

```
show dfw cluster all
```

This will provide the following details:

- **Cluster Name** - The friendly name of the vSphere Cluster.
- **Cluster ID** - The unique identifier of the vSphere Cluster.
- **Datacenter Name** - The datacenter object for which the vSphere Cluster belongs to.
- **Firewall Status** - The current status of the Distributed Firewall on this vSphere cluster.

In case there's a particular host in a cluster for which you are noticing some issues pertaining to the DFW on, the next command may come in handy.

Show Distributed Firewall Status on a specific vSphere Cluster

To show the installation status of the Distributed Firewall service on all hosts for a given vSphere cluster, issue the following command (RegionA01-COMP01 is used below):

```
show dfw cluster domain-c26
```

This will provide the following details:

- **Host Name** - The FQDN of the ESXi host in the vSphere cluster.
- Host ID - The unique identifier of the ESXi host in the vSphere cluster.
- Installation Status - The current status of the Distributed Firewall vSphere Installation Bundle (VIB) on the ESXi host.

To drill down even further to the Host level, continue on to the next step.

**Show Virtual Machines running on a host**

```
nsxmgr-01a.corp.local> show dfw host host-29
```

This will provide the following details:

- VM Name - The FQDN of the VM's running on the Host.
- VM ID - The unique identifier of the VM's on the Host.
- Power Status - If the VM is powered on or not. The VM needs to be powered on before you can view the firewall rules associated with it.

To drill down even further to the VM level, continue on to the next step.
Show Virtual Machine Distributed Firewall Details for a specific VM

To enumerate the specific DFW filters on a specific Virtual Machine (VM), as well as the vNICs on that VM, run the following command (web-01a.corp.local is used here as an example):

```
show dfw vm vm-272
```

Worth mentioning are the following returned details:

- **Virtual Nics List** - This section details each of the virtual machine NICs attached to the VM, as well as the vNIC IDs, and DFW filters applied.
- **vNIC ID** - This is the unique identifier of the virtual machine NIC. This is especially important for the next commands you will be running in this section of the lab.
- **Filters** - This list refers to the individual DFW filters applied to the vNIC. The values here are unique identifiers for the filters in question.

Please note that the Filter ID that you see within your pod may differ from the one in the screenshot or within this manual. Please use the Filter ID returned within your pod for the remainder of this manual.

You can take the values from the list of filters and vNICs to obtain more details pertaining to the Distributed Firewall and how it's applied to a VM. Continue to the next step to learn how.
Generating Traffic to web-01a.corp.local

Before continuing you should generate some traffic to web-01a.corp.local otherwise you may not see any results. Instead you will likely see a No Records Found message.

1. Within your browser repeatedly click on the Customer DB App bookmark (5 times should be enough). This will generate traffic to web-01a.corp.local and eventually you will receive a Service Temporarily Unavailable message which is fine. We just want traffic being generated so we view additional information in the following steps.

Show Rules on a specific Virtual Machine vNIC

```
show dfw host host-31 filter nic-69041-eth0-vmware-sfw.2 rules
```

```
ruleset domain-c26 {
    # Filter rules
    rule 1007 at 1 inout protocol tcp from address ip-vm-272 to address ip-vm-273 port 80 drop;
    rule 1005 at 2 inout protocol tcp from any to address ip-isp-2 port 53 accept;
    rule 1005 at 3 inout protocol udp from any to address ip-isp-2 port 53 accept;
    rule 1005 at 4 inout protocol udp from any to address ip-isp-2 port 123 accept;
    rule 1005 at 5 inout protocol udp from any to address ip-isp-2 port 123 accept;
    rule 1005 at 6 inout protocol udp from any to address ip-isp-2 port 443 accept;
    rule 1005 at 7 inout protocol udp from any to address ip-isp-2 port 443 accept;
    rule 1005 at 8 inout protocol udp from any to address ip-isp-2 port 1024 accept;
    rule 1005 at 9 inout protocol udp from any to address ip-isp-2 port 1024 accept;
    rule 1005 at 10 inout protocol udp from any to address ip-isp-2 port 68 accept;
    rule 1005 at 11 inout protocol ipv6-icmp icmptype 135 from any to any accept;
    rule 1005 at 12 inout protocol ipv6-icmp icmptype 136 from any to any accept;
    rule 1005 at 13 inout protocol ipv6-icmp icmptype 137 from any to any accept;
    rule 1005 at 14 inout protocol ipv6-icmp icmptype 137 from any to any accept;
    rule 1005 at 15 inout protocol ipv6-icmp icmptype 137 from any to any accept;
}
```

```
ruleset domain-c26_L2 {
    # Filter rules
    rule 1004 at 1 inout ethertype any from any to any accept;
}
```

```
nsxmgr-01a.corp.local>  
```
To display the firewall rules attached to any specific filter attached to a Virtual Machine's vNIC, run the following command (the vNIC for app-01a is used in this example):

```
show dfw host host-31 filter <FilterID> rules
```

Please remember to use the Filter ID that was returned from step "Show Virtual Machines Distributed Firewall Details for a specific VM"

The output will be the actual rules for the specific filter passed with the command.

### Show Distributed Firewall Statistics for a specific Virtual Machine vNIC

To show usage statistics for a given DFW filter, perform the following command (once again, the filter applied to the vNIC for web-01a is used here):

```
show dfw host host-31 filter <FilterID> stats
```

Please remember to use the Filter ID that was returned from step "Show Virtual Machines Distributed Firewall Details for a specific VM"

Displayed will be the number of times a particular DFW rule has been utilized for the given vNIC's filter passed to the command. To obtain further details regarding each flow that matches a given filter, continue to the last step of this section.
Show Distributed Firewall Flow Details for rules applied to a specific Virtual Machine vNIC

To display flow details for a given DFW filter, use the following command:

```
show dfw host host-31 filter <FilterID> flows
```

Please remember to use the Filter ID that was returned from step "Show Virtual Machines Distributed Firewall Details for a specific VM"

In the above example we can see that we have flows from the main console (192.168.110.10) going to web-01a.corp.local (172.16.10.11).
Module 5 Conclusion

In this module we showed the how to use the Central CLI commands available within NSX Manager to gather information and help troubleshoot your environment from a single interface. We covered gathering information from Logical Switches, Distributed Logical Routers, Edge Service Gateways as well as the Distributed Firewall.

You've finished Module 5

Congratulations on completing Module 5.

If you are looking for additional information on Central CLI visit the URL below:

Go to https://tinyurl.com/y9ezapa9

Proceed to any module below which interests you most.

Lab Module List:

- **Module 1 - Log Insight Management Pack Review** (15 minutes) - Basic - This module covers the basics of the NSX Log Insight Management Pack and how to install it within Log Insight.
- **Module 2 - Log Insight Dashboards** (15 minutes) - Basic - This module covers the Log Insight Dashboard and how to successfully navigate around the interface.
- **Module 3 - Flow Monitoring Configuration** (30 minutes) - Basic - This module covers the basics of NSX Flow Monitoring. It starts off by giving you a tour of all the available options and then how to monitor the flows of a particular VMs vNIC.
- **Module 4 - Traceflow** (30 minutes) - Basic - This module covers the basics of Traceflow and how to initiate a Traceflow between two VMs to view an "Allowed" and "Blocked" result.
- **Module 5 - Central CLI** (15 minutes) - Basic - This module shows the power of Central CLI and how you can easily retrieve valuable information relating to NSX via a single Central CLI.
- **Module 6 - Endpoint Monitoring** (15 minutes) - Basic - This module shows an overview of Endpoint Monitoring and how you can easily monitor internal guest processes for specific VMs

Lab Captain:

- **Module 1 through 6 - Mostafa Magdy, Senior Systems Engineer, Canada**
How to End Lab

To end your lab click on the END button.
Module 6 - Endpoint Monitoring with NSX (15 minutes)
Introduction

In this module we will be discussing Endpoint monitoring, this is a new feature that was introduced in NSX 6.3.

Endpoint Monitoring enables you to profile applications inside the guest including visibility into specific application processes and their associated network connections. Used together, you have end-to-end visibility of your applications and simplified firewall rule creation to help operationalize micro-segmentation even faster and more effectively than ever before.

How does it work?

Endpoint Profiling is done via the existing Server Activity Monitoring Resultant static analysis of processes making network connections is reported in the UI.

Security group can be selected for monitoring. After profiling, users can see a list of:

- Details of each process running on each VM
- VM to VM communication
- Process to Process communication

You can also see a visual representation of the VMs and SG

- Intra and Inter Security Group communication

Users can sort and filters VM specific flows vs application specific flows

Scaleability

- Maximum 20 VMs in monitored Security Group
- Maximum 5 million flow records
- Can co-exist with Flow Monitoring

Requirements

- Enterprise License
- VMtools and Guest Introspection Service VM
Interoperability

- SAM backend DB is used to store Application Flow information
- Server Activity Monitoring Feature itself is being deprecated (warning message) but not disabled
Endpoint Monitoring Data Collection

Application owner will provide a set of VMs (maximum 20) that will be a representative state of its application for profiling. The profiling will be done via existing server activity monitoring. The resultant static analysis of processes in the guest making network connections will then be processed by NSX manager and reported in the UI.

Server Activity Monitoring has to be enabled for this feature. This implies – VMTools (File and Network drivers) and Guest Introspection Service in deployed.

User will have to deploy Guest Introspection Service on the required clusters where the applications are deployed. They will also deploy VMtools with file and network drivers enabled in virtual machines.

Prerequisites

1. Guest introspection must be installed on Virtual Machines (VMs).
2. VMware Tools must be running and current on your Windows desktop VMs.
3. Security Groups with 20 or fewer VMs are needed for data collection before Endpoint Monitoring can begin.
4. Data collection must be enabled for one or more virtual machines on a vCenter Server before running an Endpoint Monitoring report. Before running a report, ensure that the enabled virtual machines are active and are generating network traffic.
1. **Deploy Guest Introspection**

1. Click **Home** icon.
2. Click **Networking & Security**.

1. Select **Installation**.
2. Select **Service Deployments** tab.
3. Click + icon to deploy Guest Introspection.
Guest Introspection deployment wizard

[Diagram of the Guest Introspection deployment wizard with highlighted steps 1 and 2]
1. Select **Guest Introspection** service.
2. Click **Next**.
1. Select RegionA01-COMP01.
2. Click Next.

1. Leave default values.
2. Click Next
1. Click **Finish**.

Wait a few minutes for the installation to complete and then confirm successful installation to the cluster.
Verify Guest Introspection installation on hosts

1. Click **Home** icon.
2. Click **Hosts and Clusters**.

1. Expand the **RegionA01-COMP1** folder.
2. Expand the **ESX Agents** folder
3. Verify both Guest Introspection VMs are operational and deployed on each host.
4. Verify both VMs have an IP address assigned.
2. Install VMware tools

VMware tools must be installed on the VM that is being monitored with Endpoint Monitoring. In order to ensure all required filter drivers are installed, perform a complete install. This should already be done for you, in this lab we will be showing you how to do it.


   ![Image of VMware tools installation process]

   **1.** Click `Update VMware Tools`.
   **2.** Select `Interactive Upgrade`.
   **3.** Click `Upgrade`.

   VMware Tools includes drivers to improve graphics, mouse, networking, and storage for VMware virtual devices.

   The disk image with VMware Tools will be mounted onto the virtual CD/DVD drive. The guest OS of the virtual machine must be running. Then, go to the console to run the VMware Tools Upgrade wizard from the virtual CD/DVD.
1. Select **Update VMware Tools**.
2. Select **Interactive Upgrade**.
3. Click **Upgrade**.

![Remote Console Image]

1. Launch **remote console**.

![Remote Console Login Image]

1. Login in with username **administrator** and password **VMware1!**.
2. Click **OK**.
Installing VMware Tools

1. Click Next.

Choose Setup Type

Please select a setup type.

- **Typical**
  
  Installs the program features used by this VMware product only. Select this option if you intend to run this virtual machine only with this VMware product.

- **Complete**
  
  Installs all program features. Select this option if you intend to run this virtual machine on multiple VMware products.

- **Custom**
  
  Lets you choose which program features to install and where to install them. Only advanced users should select this option.
Choose the **Complete** installation option to ensure all the required drivers are installed.

After installation finishes, click **Yes** to restart the VM.

### 3. Create Security Group

We need to create a Security Group and Firewall rule to allow `win-xp-01.corp.local` to communicate.
1. Using vSphere web client, go to NSX home and then click on Service Composer.
2. Select Security Groups tab.
3. Click on new Security Group icon

Create a new security group using the following characteristics:

- **Name:** Endpoint - windows XP
- Define dynamic membership: ignore, click **Next**
- Select objects to include: Object Type: Virtual Machine: **win-xp-01.corp.local**
- Select objects to exclude: ignore, click **Next**
- Click **Finish**.
4. Add Firewall Rule

1. Click on **Firewall**.
2. Right-click the arrow and choose **Add section**.

   1. Add a new section above and name it: **Endpoint FW rules**.
   2. Click Add a new section above section and name it **Endpoint**.

   ![Diagram of adding a new section with name](image)
Click the + icon to add a new rule.

1. Click **Endpoint Monitoring**.
2. Click **Summary**.
3. Click **Start Collecting Data**.

### Adding a new rule to the newly created FW section

Add a rule in the new section with the following parameters:

You can edit the value for each column by clicking on the pencil on the top right corner.
1. Name: **Allow win-xp**
2. Source: **Endpoint - Windows XP** (security group)
3. Destination: **any**
4. Service: **any**
5. Action: **Allow**
6. Applied To: **win-xp-01.corp.local** (virtual machine)
7. Click **Publish Changes**.

Verify the new firewall rule has been published.

**Begin Endpoint monitoring**

Now that we have installed VMware tools and deployed Guest Introspection, we can start Endpoint Monitoring.
1. Using vSphere web client, go to NSX home and then click **Endpoint Monitoring**.
2. Click **Start Collecting Data** on the top right of the screen and choose **Add section**.

![Image of NSX Endpoint Monitoring configuration](image)

1. Click **Select your security group here**.
2. Select **Endpoint - Windows XP**.
3. Click **OK**.
4. Switch Data Collection to **ON**.
5. Click **OK**.

1. Click **Select your security group here**.
2. Select **Endpoint - Windows XP**.
3. Click **OK**.
4. Switch Data Collection to **ON**.
5. Click **OK**.
Generating traffic on the monitored VM

Generate some network traffic by opening a few applications on `win-xp-01.corp.local`

Using vSphere web client, go to **Hosts and Clusters**, select `win-xp-01.corp.local` and click **Launch Remote Console**.

1. Login with username `corp\Administrator` and password `VMware1!`
2. Perform the following steps inside the RDP session to generate some flows. You can also use any other application/destination of choice if you prefer.
3. Open a console window and type `ftp ftpsite.vmware.com` to initiate an FTP connection. No need to log in.
4. Open a Putty window and open an SSH session to `172.16.60.20`
5. Open Firefox and open the 3-tier App `http://172.16.60.20`
View Endpoint Monitoring Results

Now we can look at the discovered flows and process to flow mapping in Endpoint Monitoring.
1. Using vSphere web client, go to NSX home and then click **Endpoint Monitoring**

2. Click **Stop Collecting Data** on the top right of the screen and confirm you want to stop the collection process.

3. In the summary page, you should see 1 VM is running, and at a number of processes are generating a larger number of flows.

4. Click on the VM flows tab, which represents the VMs that are communicating. The bubble chart shows the `win-xp-01.corp.local` VM has initiated flows with a few destinations. Click on the Line in between the bubbles to find the flows that you generated in the previous step.

   ![Bubble Chart](image)

   ![Table](image)
Now Click on the **Process flows** tab, which shows each process that is generating flows, along with process and flow details.

Verify the Process Version information that is displayed matches with the version of that application (**Putty**, **Firefox**) on the VM. Go back to the Remote Console to verify this.
Click line in between the bubbles to confirm the flow information matches with the flows that you generated in the previous step for each application.

Lab end

You have now completed the overview lab on Endpoint monitoring. Thank you for taking the time to go through the lab.
Module 6 Conclusion

In this module we showed an overview on Endpoint Monitoring. We provided a highlevel description on how it works, we went through the pre-requisites and configured an example. Endpoint Monitoring enables you to profile applications inside the guest including visibility into specific application processes and their associated network connections.

You've finished Module 6

Congratulations on completing Module 6.

If you are looking for additional information on Flow Monitoring visit the URL below:

- Go to https://tinyurl.com/y98jwm4y

Proceed to any module below which interests you most.

Lab Module List:

- **Module 1 - Log Insight Management Pack Review** (15 minutes) - Basic - This module covers the basics of the NSX Log Insight Management Pack and how to install it within Log Insight.
- **Module 2 - Log Insight Dashboards** (15 minutes) - Basic - This module covers the Log Insight Dashboard and how to successfully navigate around the interface.
- **Module 3 - Flow Monitoring Configuration** (30 minutes) - Basic - This module covers the basics of NSX Flow Monitoring. It starts off by giving you a tour of all the available options and then how to monitor the flows of a particular VMs vNIC.
- **Module 4 - Traceflow** (30 minutes) - Basic - This module covers the basics of Traceflow and how to initiate a Traceflow between two VMs to view an "Allowed" and "Blocked" result.
- **Module 5 - Central CLI** (15 minutes) - Basic - This module shows the power of Central CLI and how you can easily retrieve valuable information relating to NSX via a single Central CLI.
- **Module 6 - Endpoint Monitoring** (15 minutes) - Basic - This module shows an overview of Endpoint Monitoring and how you can easily monitor internal guest processes for specific VMs

Lab Captain:

- Module 1 through 6 - Mostafa Magdy, Senior Systems Engineer, Canada
How to End Lab

To end your lab click on the **END** button.
Conclusion

Thank you for participating in the VMware Hands-on Labs. Be sure to visit http://hol.vmware.com/ to continue your lab experience online.

Lab SKU: HOL-1803-03-NET

Version: 20180215-205108