

# NSX-T 3.0: Operation Guide

VMware Networking





# **Table of contents**

NSX-T 3.0: Operation Guide
1. Overview
2. VMware NSX Architecture
3. Visibility Tools $\ldots$
4 Operations Utilities
5 Troubleshooting Tools & Case Study
Appendix
i. Remote User Authentication and RBAC
ii. NSX Certificate management



# NSX-T 3.0: Operation Guide

# 1. Overview

Operations and visibility are key metrics that enterprise assess the risk and success of their businesscritical applications. NSX-T is a software defined network platform when deployed touches every aspect of enterprise connectivity and thus understanding, leverage and building successful operational design and best practices can define a difference between a successful and a failed environment.

NSX-T provides several tools and utilities to simplify daily operations and provide the level of visibility an enterprise-grade SDN solution requires. They can be classified into three main categories:

- 1. **Visibility** -Tools provides information about the health and status of the NSX components, traffic statistics or visibility of the different systems connected to NSX
- 2. **Operations** Tools and utilities focused on simplifying installation and other common tasks like upgrading the system, backup/restore or getting the corresponding support bundles
- 3. Troubleshooting Tools help finding out problems or configuration issues when something does not work

NSX-T also works with other VMware and 3<sup>rd</sup> party operational tools. For example, **vRealize Network Insight**(vRNI) which is a comprehensive operational tool for the entire SDDC environment. This guide outlines how to utilize vRNI to monitor and troubleshoot NSX deployment. This guide also outlines **vRealize Log Insight(vRLI)** Content Pack which was developed for NSX-

Τ.

The following sections describe the NSX installation process, tools, remote authentication, and Rolebased access control (RBAC) including two-factor authentication.





# 2. VMware NSX Architecture

VMware NSX-Tis designed to address application frameworks and architectures that have heterogeneous endpoints and technology stacks. In addition to vSphere, these environments may include other hypervisors, containers, bare metal operating systems, and public clouds. NSX-T allows IT and development teams to choose the technologies best suited for their applications. NSX-T is also designed for management, operations, and consumption by development organizations in addition to

IT.



Figure 2-1 VMware Networking and Security Key Use Cases

VMware NSX consists of several products work seamlessly to cover numerous use cases and provides complete, state-of-the-art, easy to use, end-to-end networking and security solution regardless of where the workloads are hosted.

• VMware NSX Data Center – virtualization and security platform extend software defined networking across data centers, clouds, and endpoints.

• VMware NSX SD-WAN by VeloCloud – assures enterprise and cloud application performance over Internet and hybrid WAN while simplifying deployments and reducing costs.

• VMware NSX Cloud – delivers consistent and operationally scalable micro-segmentation security for applications running natively in public clouds.

This guide focuses on VMware NSX-T Data Center, and sets the foundation to operate, manage and troubleshoot the core VMware NSX product.

## 2.1 VMware NSX-T Data Center Overview

VMware NSX-T Data Center is the core component of the VMware NSX-T solution. It delivers consistent networking and security across multiple hypervisors and workloads (VMs, containers and bare metal servers).

It aims at building agile, secure and flexible private clouds, which can be interconnected and extended to public clouds (either built





on VMware technologies or native public clouds) the moment business demand requires it.

VMware NSX-T consists of three separate but integrated planes—management, control, and data. These planes are implemented as sets of processes, modules, and agents residing on three nodes— manager, controller, and transport nodes.



Figure 2-2 VMware NSX Data Center Architecture for Private Cloud

Please see detail explanation in the Reference Design Guide https://communities.vmware.com/docs/DOC-37591

• NSX Virtual Switch: The NSX-T virtual switch comes in two forms - NSX Virtual

Distributed Switch (N-VDS) and VDS with NSX. On ESXi hosts both the N-VDS and VDS with NSX i (NSX-T 3.0 onward) is supported. With any other kind of transport node (KVM hypervisors, Edges, bare metal servers, cloud VMs etc.) the N-VDS is the only switch supported. VDS with NSX has few specific operational considerations. Please refer to <u>https://kb.vmware.com/s/article/79872</u> for further details.

• **Hypervisor Transport Nodes:** Hypervisor transport nodes are hypervisors prepared and configured for NSX-T. The N-VDS provides network services to the virtual machines running on those hypervisors. NSX-T currently supports VMware ESXi<sup>™</sup> and KVM hypervisors. The NVDS implementation of KVM is based on the Open vSwitch (OVS) and platform independent. It can be ported to other hypervisors and serves as the foundation for the implementation of NSX-T in other environments (e.g., cloud, containers, etc.).

• **Edge Nodes:** VMware NSX® Edge nodes are physical or virtual appliances dedicated to running network services that cannot be distributed to the hypervisor nodes. These include dynamic routing protocols, NAT (Network Address Translation), Load Balancing or VPNs (Virtual Private Cloud), to name a few. VMware NSX Edges are grouped in one or several clusters, representing a pool of capacity.

For further details about VMware NSX-T Data Center architecture and features, please review the VMware NSX-T Reference Design Guide and the latest NSX-T Documentation available at <u>https://communities.vmware.com/docs/DOC-37591</u>





# 3. Visibility Tools



NSX provides comprehensive monitoring tools through NSX native monitoring capability and integration with 3<sup>rd</sup> party tools.

This section describes the following tools:

- 3.1 Dashboards
- 3.2 Counters/Stats/Tables
- 3.3 Monitor Logical Switch Port Activity
- 3.4 BGP Neighbor Status, Geneve Tunnel Status
- 3.5 VM Inventory
- 3.6 Search Utility
- 3.7 APIs, CLI, Central CLI

## 3.1 Dashboards and Overview

NSX-T includes an out-of-the-box dashboard that allows administrators to check the status of the primary NSX components in a single pane of glass.





Networking Security Inv	ventory Plan & Troublesh	oot System		PO	LICY MANAG
Overview Alarms I Monit	toring - System 👻 🛈				?
OK IN PROGRESS DEG	RADED UNKNOWN	NOT CONFIGURED ERROR			$\mathbb{C}$ refresh
SYSTEM ®	🔥 Alarm(s): 4	FABRIC @			
Management Cluster Stable		$\circ$		-	
		5 4	9	1	
3					
		Host Transport Nodes Edge Transport Node	s Transport Zones	Compute Ma	inagers
NSX Nodes		Host Transport Nodes Edge Transport Node	s Transport Zones	Compute Ma	inagers
NSX Nodes		Host Transport Nodes Edge Transport Node	s Transport Zones	Compute Ma	inagers
NSX Nodes		Host Transport Nodes Edge Transport Node	s Transport Zones	Compute Ma	inagers
NSX Nodes	impleted at	Host Transport Nodes Edge Transport Node	s Transport Zones	Compute Mi	inagers
NSX Nodes	ompleted at 5/2020 22:25 PM ompleted at	Host Transport Nodes Edge Transport Node	s Transport Zones	Compute M	inagers
NSX Nodes	impleted at 5/2020 22:25 PM impleted at 5/2020 22:24 PM	Host Transport Nodes Edge Transport Node	s Transport Zones	Compute Mi	inagers
NSX Nodes  NSX Nodes  Automatic backups Disabled Node Co Cluster C000	impleted at 5/2020 22:25 PM impleted at 5/2020 22:24 PM	Host Transport Nodes Edge Transport Node	s Transport Zones	Compute Mi	inagers

Figure 3-1-1: Dashboard from NSX-T 3.0

Details of NSX-T dashboards in NSX-T 3.0 release is listed below.

• **System dashboard** comprises the following four widgets:

o *Hosts* – multi-widget with two parts showing the following information:

- Deployment status of the installation of NSX software on the different hosts
- Connectivity status of the communication between the hosts and the NSX

#### Manager

o *Edges* – multi-widget with two parts showing the following information:

- Deployment status of the installation of NSX software on the different edges
- Connectivity status of the communication between the edges and the NSX

#### Manager

- Transport Nodes donut widget showing information about the status of the different transport nodes
- Transport Zones donut widget showing information about the status of the different transport zones
- **Clusters dashboard** shows the health status of the management cluster as shown below.



NSX-T 3.0: Operation Guide



Figure 3-1-2: Manager Dashboard from NSX-T 3.0

- Networking dashboard consists of the following widgets o Tier-0 Gateways o Tier-1 Gateways o Segments
  - VPN
  - Load Balancing

Home Networking St	ecurity Inventory Plan & Troubles	hoot System Adva	nced Networking & Securit	y			
«	NETWORK OVERVIEW						
Network Overview	Configuration Capacity						CREFRES
Connectivity 🔁 Tier-0 Gateways	NETWORKING Tier-O Gateways	Tier-1 Gateways	Segments	IP ADDRESS MANAGEM	HENT DHCP Servers	IP Pools	
🔁 Tier-1 Gateways 📢 Segments	1	0	3	0	0	1	
Network Services	NETWORK SERVICES	NAT Rules		Load Balancer	Forwardin	a Policies	
@ VPN → NAT	0	0		0	0		
Load Balancing Forwarding Policies	TIER-0 GATEWAYS D		TIER-1 GATEWAY	ο .			
IP Management	Tier-0 Gateway running BGP	BGP enabled, 0 no peer BGP enabled, 0 peer configured BGP disabled, 0 peer configured		0 Number of	Tier-1s per Tier-D Gateway		
Settings	or segments O						
	Connected to Tier-1 Ga	Not Connected NATed Routed teway	1 0 0	2 Connected	• Conne • Not Conne • to VMs	icted 3 O	
	O VPN O		V LOAD BALANCER	s o			
		Layer 2 0     Policy Based 0     Route Based 0	Load Balancer O Pools	Virtual Servers O Pool members		L4 TCP     L4 UDP     HTTP     HTTP5	0000

Figure 3-1-3: Networking Dashboard from NSX-T 3.0

• Security dashboard composed of the following widgets o Distributed FW o Network Introspection o Endpoint Protection



Home Networking Sec	SECURITY OVERVIEW	t System Advanced Net	working & Security		
Security Overview	Configuration Capacity				C REFRES
2ast West Security Distributed Firewall Network Introspection (E-W)	Distributed FW Policies	Gateway Policies	Endpoint Policies	Network Introspection EW Policies	Network Introspection NS Policies
lorth South Security Gateway Pirewall Network Introspection (N-S)	DISTRIBUTED FIREWALL ©				• Allow • Drop • Rejec
ndpoint Protection		Application     Environment     Infrastructure     Emergency     Ethernet	0 0 0	1	
ettings	Distributed FW Policies	- Lu Hinney	•	Top Services by Distribut	ted FW Rules
	10	fop Profile 0 Other Profiles 0 No profile 10	* Ho	st agent + Service VM	File     Introspection     running     File     File     O     Introspection     status
	VM Distribution by Service Profile		Components having its	Configured VMs runn Introspection	ing File

Figure 3-1-4: Security Dashboard from NSX-T 3.0

me Networking	g Security Inventory Plan & Troubleshoot Sys	tem Advanced Networking & Security			
	Overview Monitoring - System ~ 0		Document	ation	
	OK IN PROGRESS DEGRADED	UNKNOWN NOT CONFIGURED	C REFRE	зн	
	<ul><li>⟨ĵ⟩ system ⊕</li></ul>	FABRIC 0			
	Management Cluster Stable	$\cap$	$\sim$		
	з	4 Degraded 1	2		
	NSX Nodes	Host Click to view details Host Transport Nodes Edge Transport Nodes Transport Nodes	sport Zones Compute Managers		
	NSX Nodes	Host Transport Nodes Edge Transport Nodes Tran	sport Zones Compute Managers		

Users can hover over the different widgets to get additional details about their system:

Figure 3-1-5: Hovering over the widgets

By clicking a component, users can automatically navigate to the configuration page of the corresponding component to get detail status of the component. For example, after clicking the *Transport Nodes* widget, users can see the page shown below.

Host Transport Nodes	Edge Transport Nodes	Edge Clusters	ESXi Bridge Clusters	NCP Clusters

¢ co	CONFIGURE NSX 🗓 REMOVE NSX 🛛 🛱 ACTIONS 🗸								View	All	
	Node	ID	IP Addresses	OS Type	NSX Configuration	NSX Version	Host Switches	Tunnels	TEP IP Addresses	Node Status	Alarms
	# TNP-Test (2)	MoRef ID:								2 Hosts Up (1)	
	10.114.220.143	f0c74bc7	10.114.220.143, 1	ESXi 7.0.0	A NSX Mainte	3.0.1.0.0.1	1	↑ 5	192.168.100.143	• Up 🛈	0
	10.114.220.153	fd06a048	10.114.220.153, 1	ESXi 7.0.0	NSX Install F	3.0.1.0.0.1	1	Not Available		Not Available	0
	<ul> <li>Physical-NSX (2)</li> </ul>	MoRef ID:								• 2 Hosts Up	
	10.114.220.133	ca88a7e8	10.114.220.133, 1	ESXi 7.0.0	• Success	3.1.0.0.0.1	1	<b>↑</b> 4	192.168.100.133	• Up 🛈	0
5	10.114.220.233	22e650a6	10.114.220.233,	ESXi 7.0.0	NSX Install F	3.0.1.0.0.1	1	↑ 5		Not Available	o

Figure 3-1-6: Transport Nodes configuration page





For the *Backups* widget, clicking on the *CONFIGURE* footer takes users to the backup's configuration page.

#### 3.1.1 Dashboards Color Code

The dashboards page includes a legend with the possible different status of the components.

OK	IN PROGRESS	DEGRADED	■ NOT CONFIGURED	ERROR

Figure 3-1-7: Possible status

When system detects issues, these colors are used to report them.

Overview Alarms  Monitoring - Netwo	rking & Security 💙	(
SUCCESS IN PROGRESS UNKNOWN	UNINITIALIZED ERROR	CREFRESI
⊕ SECURITY ©	S GATEWAYS S	SEGMENTS O
6 3	) ( , ) (	1 9
Groups Distributed FW F	tolicies Tier-O Gateways Tier	r-1 Gateways
≪ LOAD BALANCERS ⊕		
	Layer 2	<u>•</u>
	Policy Based	0

Figure 3-1-8: Dashboard reporting issues

The green status (*Ok*) is used when everything works fine, and the red one (*Error*) when there are major issues impacting NSX functionality.

The blue status, Pending and In Progress, are used to report the installation of NSX software on hosts and edges.

Status *Degraded* and *Unknown* (yellow and grey) are used to report the status of Transport Nodes and Transport Zones, which are computed as described in the following paragraphs.

#### **Transport Node Status**

It is based on four different status:

- Manager Connectivity Status
- Controller Connectivity Status
- pNIC/Bond Status
- Overlay Tunnel Status

Based on them, the overall Transport Node Status is computed as follows:

- **UP** if all four previous status are UP
- Degraded if at least one of status is Degraded or Controller Connectivity Status is down
- Down if either pNIC/Bond Status or Tunnel Status is down
- Unknown if Manager Connectivity Status is down





**Note:** Hypervisors report *Tunnel Status* as *Down* when they don't have workloads connected to NSX Logical Networks, which means they don't have any Geneve tunnel established with other Transport Nodes.

#### **Transport Zone Status**

When all Transport Nodes in a Transport Zone share the same status, the Transport Zone status is easily computed:

- If all Transport Nodes are UP, the Transport Zone status is UP
- If all Transport Nodes are Down, the Transport Zone status is Down
- If all Transport Nodes are *Degraded*, the Transport Zone status is **Degraded**
- If all Transport Nodes are Unknown, the Transport Zone status is Unknown

When there are Transport Nodes with different status, the Transport Zone status is computed as follows:

- If some (but not all) Transport Nodes are Down or Degraded, then the Transport Zone is Degraded
- If there are no Transport Nodes in a Transport Zone, then the Transport Zone status is **Unknown**

• If none of the Transport Nodes are *Down* or *Degraded*, but some of the Transport Nodes are in *Unknown* state, then the Transport Zone status is **Unknown** 

The following figure depicts the Transport Zone widget reporting one *Degraded* and one *Unknown* Transport Zone with corresponding detailed status.

• tz-overlay01 has some but not all Transport Nodes Down, and thus its status is Degraded

• tz-vlan01 has no Transport Nodes *Down* or *Degraded*, but some of them are in *Unknown* state, thus its overall status is *Unknown* 



Figure 3-1-10: Transport Zone Status

Nevertheless, whenever the dashboard reports any color other than green, it is a good practice to click on the affected widget to get further details in order to determine the root cause of the issue.

#### 3.1.2 Custom Dashboards

Besides the out-of-the-box dashboards described on the previous section, it is possible to define custom dashboards in NSX-T. Custom dashboards allow to easily monitor specific use cases, which may be relevant for deployments, but may not be included out-of-the box.



vm NSX		Q @ A &
«	Overview Custom	
② Dashboard		CREFRESH
▷ Getting Started		
> 🖻 Tools		
> org Load Balancing	LB Overview	Security Overview Dashboard
Firewall  Encryption  Routing	LB Services 1 Virtual Servers 2 Pools 1	DFW Status   ENABLED DNE Status  INSTALLED_DISABLED
t, Switching	Web Front End	Web Front End
> 🗄 Inventory	Virtual Server Status	
>	Virtual server # 1/2.18.0.00 Pool Min Active Members 1	3 Pool Members
	CONFIGURE SERVICE	Web Front End
	Logical Ports	
	Admin Status Operational Status	

Figure 3-1-11: Sample NSX-T Custom Dashboards

Custom dashboards were introduced in NSX-T 2.1. The following five widgets are supported in the initial release.

1. Label Value Widget – Data is displayed as text with the possibility of adding status icons and tooltips. No additional graphical representation is allowed.

Encryption status	INSTALLED_DISABLED	
Allow mirroring	🔴 true	
Port mirroring e	nabled	

Figure 3-1-12: Label Value Widget

2. Donut Widget - Data is displayed in a circle, which can have different colors depending on the corresponding status.



Figure 3-1-13: Donut Widget



3. Sectioned Donut - Several data sources are represented as different sections of the same donut widget.

File Systems of 10.16	50.145.244	
	8 File Systems	
	File Systems of 10.160.145.244	

Figure 3-1-13: Sectioned Widget

4. Multi-widget - A donut splits into halves, representing different (but typically related) information on each of them.



Figure 3-1-14: Multi Widget

5. Widget Container – A container groups related donut widgets together.

Clusters	
1 Nodes	1 Nodes
Manager Cluster	Controller Cluster

Figure 3-1-15: Widget Container

Custom dashboards are configured, updated and deleted through NSX-T Manager APIs. Please refer to the Dashboard section of NSX-T API documentation for further details.

#### 3.2 Counters, Statistics and Tables

Counters, statistics, and tables provide visibility on different aspects of the traffic that goes through NSX. The table below summarizes the major statistics and tables exposed through the NSX Manager:



Component	Statistics Gathered
NSX Manager Node	CPU, Memory, Disk, Interface Stats (Packet Count / Bytes)
Transport Node (ESXi, KVM, Edge)	System status (CPU/Memory/File System/Uptime/Load Avg) Physical and VM interface status (Rx/Tx bytes) Communication Channel Health
Logical Switch (Segment)	Interface Stats (Bytes, Packet Count, Rx/Tx) TEP table, MAC table, Switch Security (Blocked Packets)
Logical Router (T0/T1 Gateway)	Interface Stats (Bytes, Packet Count, Rx/Tx) Forwarding Table, ARP tables, Routing table NAT stats
Distributed Firewall	Per-rule flow stats (Number of sessions allowed/blocked, bytes, packets)
L2 Bridge	Port stats, Status, Cluster status

Figure 3-1-17: NSX-T Summary of Statistics and Tables

There is an aggregation service framework that runs within the NSX Manager and exposes public facing REST APIs.

• Node statistics (like CPU, Memory, Disk, or Interface-related information) are exposed by the NSX Manager Nodes and Transport Nodes (i.e., ESXi, KVM and NSX Edge Nodes).

• Additionally, each function running on the Transport Nodes (Logical Switching, Logical Routing, NAT and DFW) exposes operational data relevant to that function.

• On-demand statistics such as Interface statistics, MAC address tables or TEP tables, are queried at real-time while bulk statistics (typically aggregation of distributed stats) are collected by polling periodically.

This framework is consumed internally by the graphical user interface, Port-connect Tool and Traceflow, which are two features covered later this guide.



Figure 3-1-18: NSX-T Aggregation Service Framework





NSX-T counters, statistics and tables can be found by navigating to the corresponding NSX-T UI pages, as explained on the following sections.

#### 3.2.1 Transport Node Counters/Stats/Tables

Transport Node information is available under *Fabric* > *Nodes* > *Transport Nodes*. By clicking on a specific node, and moving to its *Monitor* tab, the following information is exposed:

- System Usage including CPU, memory, file system information, load and uptime
- Transport Node Status including status of the connectivity to Manager and Controllers, pNIC/Bond status.
- **Tunnel Status** status and remote transport node of the overlay tunnels established by the host.

Note: Both Transport Node status and Tunnel status reported every 3 minutes on ESXi/KVM/BM and every 30 seconds on Edge node. The status on the UI needs to be refreshed manually.

• **Network Interface** – list of network interfaces on the node, including admin and link status,

MTU, interface details (MAC address, IP address, network mask) and traffic statistics (Total Bytes, Total Packets, Dropped Packets, Error Count)



Figure 3-1-19: Transport Node Counters/Stats/Tables

#### 3.2.2 Layer 2 Counters/Stats/Tables

Layer 2 information can be found on different tabs. Those related to logical ports provide individual information for a specific port while those related to logical switches provide aggregated information for that logical switch.

#### For Logical Switches

On the NSX Manager UI, switch to Manager UI from Policy UI first, then navigate to the *Switching* menu, ensure the *Switches* tab is selected, click on the switch you want to see information for, and finally click on its *Monitor* tab. Details are then displayed, including:

Cumulative Traffic statistics for Unicast, Broadcast and Multicast, and Dropped packets

• Additional switch-aggregated statistics for blocked traffic, including the reason for traffic being dropped (Spoof Guard, BPDU filter, DHCP Server Block or DHCP Client Block)



vm NSX-T					Q	Δ		6	admin ~
Home Networking Sec	curity Inventory Plan & Troubleshoot	System					F	POLICY MAN	AGER (1)
*	Switches Ports Switching Profile	es Edge Bridge Profiles							
Network Overview	+ / 1 0 ~	Seg-Vlan100							×
Connectivity	Logical Switch 🕈	Overview Monitor Manag	je v Related v						
Tier-O Logical Routers	Ge Seg-App-Vlan20								
Tier-1 Logical Routers	Seg-ESXi-MGT-Vlan140	Switch Status & Statistics DC	WNLOAD MAC-TEP TABLE	DOWNLOAD TEP	TABLE	REFRE	SH		
🔄 Logical Switches	Gereg-UL1-Vlan146	Operational Status: Success Failure Message None							
	Seg-Vlan100	Last Updated at Oct 15, 2	020 2:06:12 PM						
Network Services	Gervian100-0L	VIF Traffic Statistics							
- NAT	□⊖ Seg-Vian140	Traffic (Cumulative) Tran	smitted Bytes Transmi	tted Packets	Receive	ed Bytes		Received Pac	kets
🐗 Load Balancing	Geg7-App-Vlan20	Unicast	452.06 MB	6,781,596		49	2.95 MB		4,511,271
	G Seg7-DB-Vlan30	Multicast & Broadcast	20.92 MB	306,379		3	9.63 MB		77,832
IP Management	G Seg7-Infra-Vlan110	Dropped	0.00 Bytes	0		0.0	0 Bytes		0
DHCP		TOTAL	472.99 MB	7,087,975		50	2.59 MB		4,589,103
IP Address Pools		Blocked Packets Statistics							
Settings		Traffic / Feature	Blocked By			Packets			
🚱 Global Networking Config		IPv4	Spoof Guard						0
		IPv6	Spoof Guard						0
		ARP	Spoof Guard						0
		ND	Spoof Guard						0
		Non IP	Spoof Guard						0
		All	BPDU Filter						0
		IPv4	DHCP Server Blo	k					0
		IPv6	DHCP Server Blo	:k					0
	< > 1-9/9	IPv4	DHCP Client Bloc	<i>c</i>					0

Figure 3-1-20: Logical Switch Counters and Stats

From the same page, it is also possible to download TEP and MAC-TEP tables for the switch:

Switches Ports Switching Pro	files Edge Bridge F	Profiles			
+ ∥ @ .	Seg-Vlan100				×
□     Logical Switch ↑       □     ⊖       Seg-App-Vlan20	Overview Monitor	Manage - Related -	/		
Geg-ESXi-MGT-Vlan140	Switch Status & Statistic	CS DOWNLOAD MAC-	TEP TABLE DOWNLO	AD TEP TABLE REFRE	SH
□⊖ Seg-UL1-Vlan146	Operational Status:	Success			
Seg-Vlan100	Last Updated at	Nov 20, 2020 4:31:13 AM			
□⊖ Seg-Vlan140	VIF Traffic Statistics				
□⊖ Seg7-App-Vlan20	Traffic (Cumulative)	Transmitted Bytes	Transmitted Packets	Received Bytes	Received Packets
□⊖ Seg7-DB-Vlan30	Unicast	452.06 MB	6,781,599	492.95 MB	4,511,271
□⊖ Seg7-Infra-Vlan110	Multicast & Broadcast	25.02 MB	362,068	12.69 MB	102,476
	Dropped	0.00 Bytes	0	0.00 Bytes	0
	TOTAL	477.09 MB	7,143,667	505.64 MB	4,613,747
	Blocked Packets Statisti	cs			

Figure 3-1-21: Logical Switch tables

For both tables, users get the option to download information from the Controller Cluster or from the specific Transport Node they may be interested in.





- I dilute Micsson	it wone		Failure McSodu	as none	
Download M	AC-VTEP Table - te01-web	×	Download \	/TEP Table - te01-web	×
Source	Central Control Plane Transport Node	25	Source	<ul> <li>Central Control Plane</li> <li>Transport Node</li> </ul>	
Transport Node*	I.	~ 2.8	Transport Node*	T	~
	edge01	5		edge01	
	edge02	g		edge02	
	edge03			edge03	
	esxi-01	4,2		esxi-01	
Charles 100 and	esxi-02		Plocked Dack	esxi-02	
	kvm-01		DIVEREU Pack	kvm-01	
Traffic / Feat	kvm-02		Traffic / Featu	kvm-02	
		< > 1-7/7	IPv6		< > 1-7/7

Figure 3-1-22: Logical Switch table details

#### **For Logical Ports**

On the NSX Manager UI, navigate to the *Switching* menu, ensure the *Ports* tab is selected, click on the switch you want to see information for, and finally click on its *Monitor* tab. Details are then displayed, including:

• **Port-specific Traffic statistics** for Unicast, Broadcast and Multicast, and Dropped packets

• Additional port-specific statistics for blocked traffic, including the reason for traffic being dropped (Spoof Guard, BPDU filter, DHCP Server Block or DHCP Client Block)

Switches Ports Switching Profile	s Edge Bridge Profi	es			
+ 2 m @ ~	App-VM-20.10/App	-VM-20.10.vmx@ca88a3	8fe-97f6-45e9-9f0b-2	21ad	×
Logical Port 🕆	Overview Monitor	Manage 🗸 Related 🗸			
□⊖ 7-T0-Test-Int-UL1-ulp					
App-VM-20.10/App-VM-20.10.vmx@ca>	Port Status & Statistics	DOWNLOAD MAC TABLE	BEGIN TRACKING REFRI	ESH	
CentOS/CentOS.vmx@ca88a3fe-97f6	Operational Status:	Up			
DB-VM-30.10/DB-VM-30.10.vmx@22e6	MAC Learning Statistics				
DB-VM-30.20/DB-VM-30.20.vmx@f0c	Number of MACs Learned	0			
DB-VM-30.30/DB-VM-30.30.vmx@fd0	Packets Allowed without M	IAC Learning 0			
□⊖ infra-Seg7-DB-Vlan130-lp	Traffic Statistics	MAC Learning 0			
□⊖ infra-Seg77-App-Vlan20-lp	Traffic (Cumulative)	Transmitted Bytes	Transmitted Packets	Received Bytes	Received Packets
□⊖ kvm-vm2	Unicast	25.37 KB	270	23.31 KB	263
nsx-mgr-137/nsx-mgr-137.vmx@f0c789	Multicast & Broadcast	15.89 MB	222,202	9.54 MB	111,181
nsx-mgr-147/nsx-mgr-147.vmx@f0c789	Dropped	0.00 Bytes	4	0.00 Bytes	12
nsx-mgr-157/nsx-mgr-157.vmx@f0c789	TOTAL	15.91 MB	222,476	9.56 MB	111,456
vmknic@50286d93c7817ad6-16bc335a					
vmknic@n-vds-1@f0c78923-a0ab-477d	Blocked Packets Statistic	S			
Vyatta-Router/Vyatta-Router.vmx@ca	Traffic / Feature	Blocked B	Зу	Packets	
Vyatta-Router/Vyatta-Router.vmx@ca	IPv4	Spoof Gu	lard		0
Windows-Jumphost/Windows-Jumpho	IPv6	Spoof Gu	lard		0
Windows-Jumphost/Windows-Jumpho	ARP	Spoof Gu	lard		0
< > 1-18 / 18	ND	Spoof Gu	Jard		0

Figure 3-1-23: Logical Port counters and stats

From the same page, it is also possible to download the MAC table for ports on ESXi hypervisors:



Swi	tches Ports Switching Profiles	Edge Bridge Profi	les					
+	2 ū @ -	App-VM-20.10/App	o-VM-20.10.	vmx@ca88a	3fe-97f6-45e9-9f	0b-21ad		×
	Logical Port 🔿	Overview Monitor	Manage 🗸	Related 🗸				
	7-T0-Test-Int-UL1-ulp							
	App-VM-20.10/App-VM-20.10.vmx@ca>	Port Status & Statistics	DOWNLOAD	MAC TABLE	BEGIN TRACKING R	EFRESH		
	CentOS/CentOS.vmx@ca88a3fe-97f6	Operational Status: Last Updated at	• Up Nov 23, 2020 4:	42:59 AM				
	DB-VM-30.10/DB-VM-30.10.vmx@22e6	MAC Learning Statistics						
	DB-VM-30.20/DB-VM-30.20.vmx@f0c	Number of MACs Learned		0				
	DB-VM-30.30/DB-VM-30.30.vmx@fd0	Packets Allowed without I	MAC Learning	0				
	infra-Seg7-DB-Vlan130-lp	Traffic Statistics	inde counting	0				
	infra-Seg77-App-Vlan20-lp	Traffic (Cumulative)	Transmitted	Bytes	Transmitted Packets	Received Bytes	Received Packets	
	kvm-vm2	Unicast		25.37 KB		270 23.3	KB	263
	nsx-mgr-137/nsx-mgr-137.vmx@f0c789	Multicast & Broadcast		15.89 MB	222.	202 9.54	MB 11	11,181
	nsx-mgr-147/nsx-mgr-147.vmx@f0c789	Dropped		0.00 Bytes		4 0.00 B	/tes	12
	nsx-mgr-157/nsx-mgr-157.vmx@f0c789	TOTAL		15.91 MB	222,	476 9.56	MB 111	,456
	vmknic@50286d93c7817ad6-16bc335a							
	vmknic@n-vds-1@f0c78923-a0ab-477d	Blocked Packets Statisti	CS					
	Vyatta-Router/Vyatta-Router.vmx@ca	Traffic / Feature		Blocked	Ву	Packets		
	Vyatta-Router/Vyatta-Router.vmx@ca	IPv4		Spoof G	uard			0
0	Windows-Jumphost/Windows-Jumpho	IPv6		Spoof G	uard			0
	Windows-Jumphost/Windows-Jumpho	ARP		Spoof G	uard			0
	< > 1-18 / 18	ND		Spoof G	uard			0

Figure 3-1-24: Logical Port tables

Which is downloaded as a .csv file:

you want to download the MAC Table for Logical .vmx@5d57b9ba-8631-4632-b70c-54fbea768a42	ort "web-01a_1/v	web-
.vmx@5d57b9ba-8631-4632-b70c-54fbea768a42		
	(Source: Transp	ort Node
DOWNLO	D CAN	CEL

Figure 3-1-25: Logical Port table details

#### 3.2.3 Layer 3 Counters/Stats/Tables

This section describes the different statistics available for routed ports.

#### **Router Port Statistics**

To check statistics of the traffic that goes through each router port (Layer 3 router interfaces), navigate to the *Routing* menu, click on the name of the router you are interested in, select the *Configuration* tab and then *Router Ports* on its drop-down menu.

On the *Logical Router Ports* pane, there is a *Statics* column. Clicking on the icon provides access to the statistics through each specific port (Layer 3 interface). If the port is part of the distributed component (DR) of an NSX Logical Router, it is then possible to get per-node statistics or aggregated statistics, as it can be seen on the picture:



**	Routers NAT									
Dashboard     Getting Started     Tools	+ v Ø 🗈 🛞 v	t1-router01 Overview Configurat	tion <sub>v</sub> Ro	uting Services						
Coad Balancing	to-router th-router01	Logical Router Ports	DELETE (	ACTIONS V		Statistics: tenan	t01-app		×	
Encryption		Logical Roy ID	Type Linked	IP Address/mask 100.64.80.1/31	Connecte	Transport Node*	All			Statisti
Routing		venant0 7888d	Downlink	172.16.20.1/24	(LinkedF	Last Updated at: 2/8	edge02 edge03 kvm-02		I	đ
Switching		tenant0356af_	Downlink	172.16.30.1/24	⇔ te01- ( ♡ te0	Data	esxi-01 edge01			đ
Fabric		tenant0fb6c6_	Downlink	172.16.10.1/24	te01- ( ♡ te0	Dropped Packets	3298178	6053138 0		al.
> system										

Per-node Layer 3 statistics

If the port is part of the services component (SR) of an NSX Logical Router, traffic statistics are related to the Edge node where such port is defined:

vm NSX							0 A	8
«	Routers NAT							
② Dashboard								
Getting Started		t1-router01						×
> 🖹 Tools		Overview Configuration Routing Services		Statistics: Linke	dPort_t0-rout	ter ×		
> 🕫 Load Balancing	tt-router01	Logical Router Ports						
E Firewall	t1-router02	+ ADD CEDIT I DELETE ACTIONS -		Transport Node*	edge03 edge03	~		
Encryption		Logical Rou ID Type IP Address/mask	Connecto	Statistics			Statisti	cs
Routing		LinkedP., 498b5., Linked., 100.64.80.1/31	③ t0-ro	Last Updated at: 2/8	/2018, 1:32:17 AM		all.	
Routing			teo1-		Received	Transmitted	d	
> ie DDI			( 🗆 te0	Data	5 KB	15 KB		
Switching		tenant0356af Downlink 172.16.30.1/24	teo1-	Total Packets	56	281	Ila	
> I Inventory		tenanto finde 6 Downlink 17316101/04	to teo	Dropped Packets	8	27	1	-
> 🔶 Fabric		O CENERIO_ DOCC. DOWNERK 172.10.10.1724	( C te01-w	eb-rport )				
> @ System								
	< → 19/3	T COLUMNS C REFRESH Last updated; 4 Minutes Ago			¢ BACK	NEXT > 1-4 of 4 Log	ical Router Por	rts

Figure 3-1-26: Edge-based Layer 3 statistics

#### **ARP Tables**

NSX-T also exposes the ARP tables of the router ports, which can be downloaded from the NSX UI as *.csv* files. Like the Layer 3 statistics, ARP tables are available on the *Logical Router Ports* pane. To access them, select the router port you are interested in and on the *Actions* menu, select *Download ARP Table*:



«	Routers NAT		
Dashboard Getting Started Tools Get Load Balancing	+ • 0 0 0 • t0- Logical Router † 0 0 v 0 0 v 0 0 v 0 0 0 0 0 0 0 0 0 0	router erview Configuration Routing Services	
Eirewall	tt-router01	ADD 🖉 EDIT 📋 DELETE 🎯 ACTIONS 🗸	
Encryption	0	Logical Rou ID Type Manage Tags onnected To Transport Node Relay Service LinkedPddb1_9Linked Download ARP Table 11-router01	Statistic
Routing	0	LinkedP., bd6a3., Linked., 100.64.80.2/31	at
DDI		LinkedPbd03Linked 100.64.80.4/31	al.
Switching		uplink01 977a7 Uplink 192.168.140.3/24 <sup>t</sup> ⇒ uplink-ls01 edge01 ( <sup>(□</sup> t0-uplink01)	4
Fabric		uplink02 2307f. Uplink 192.168.150.3/24 **- uplink-is02 edge02 ( 🗘 to-uplink02 )	4
System			

Figure 3-1-27: Downloading ARP Tables

If the port is part of the distributed component (DR), it is possible to download the table for a specific node, while if it is part of the service component (SR), it is possible to download the ARP table from the Edge node where such port is defined:

Download ARP Table - LinkedPo	rt_t1-router01 × Dov	wnload ARP Table - uplink	D1 ×
Transport Node	× 🗸 Trans	sport Node	×
edge03		edge01	
esxi-02			
edge01		DO	WNLOAD CANCEL
kvm-01			
esxi-01			
edge02			
kvm-02			

Figure 3-1-28: Downloading ARP tables from DR vs SR ports

#### **Forwarding Tables**

Finally, NSX-T allows to download from its UI the routing and forwarding tables of the different routers (in *.csv* files). They are available on the *Routing* menu, under the *Routers* tab. Then, to download the table, select the router you are interested in, and from the *Actions* drop-down menu, select the type of table you want to download:





n NSX						~ @ 4
«	Routers NAT					
Dashboard						
> Getting Started	+ ADD + 🖉 EDIT 📋 DELETE	ACTIONS      ✓			Q, Search	
Tools	Logical Router † IC	Connect to Tier-O Router	Connected Tier-0 Router	High Availability Mode	Transport Zone	Edge Cluster
a seed Protocolog	🖬 t0-router d	Disconnect from Tier-O Router		Active-Active	tz-vlan	edge-cluster-01
<ul> <li>Load balancing</li> </ul>	t1-router01 9	Generate BGP Summary	t0-router	Active-Standby	tz-overlay	edge-cluster-lb
Firewall	t1-router02 e	Download Routing Table	t0-router			
Encryption		Download Debug Information				
Routing						
6 DDI						
Switching						
(P)						
Inventory						
Fabric						
System						

Figure 3-1-29: Downloading Routing Tables

Note: Routing table is only available for Tier0 Routers

It is possible to download the forwarding table from any node in the transport zone, while the routing table is only available for the Edge Nodes:

Download F	Forwarding Table - t1-router01	×	Download F	Routing Table - tO-router	×
Transport Node*	edge01	~	Transport Node*	edge01	~
	edge01		1000	edge01	
	edge02		Network	edge02	
	edge03		Source		
	esxi-01				
	esxi-02				
	kvm-01			DOWNLOAD	EL
	kvm-02				

Figure 3-1-30: Downloading Forwarding vs Routing Table

Also, it is possible to specify filters when downloading the routing table, to narrow down the amount of information retrieved:

	5	
Transport Node*	edge01	~
Network	10.10.30.0/24	
Source		~
	BGP	
	Static	
	Connected	

Figure 3-1-31: Downloading Specific Routing Information





As noted, before, as to Tier0 routers both routing and forwarding tables are available. The routing table includes routes from the Service Router component only, while the forwarding table includes routes from the Distributed component:

12	A	B	C	D	E	F	G
1	route_type	network	logical_router	next_hop	admin_distance	lr_component_id	lr_component_type
2	b	10.10.20.0/24		192.168.140.1	20	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
3	b	10.10.30.0/24		192.168.140.1	20	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
4	b	10.20.20.0/24		192.168.140.1	20	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
5	b	10.20.30.0/24		192.168.140.1	20	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
6	b	30.0.0/8		192.168.140.1	20	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
7	rl	100.64.80.0/31		169.254.0.1	0	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
8	rl	100.64.80.2/31		169.254.0.1	0	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
9	rl	100.64.80.4/31		169.254.0.1	0	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
10	с	169.254.0.0/28		169.254.0.2	0	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
11	ns	172.16.10.0/24		169.254.0.1	3	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
12	t1l	172.16.10.10/32		169.254.0.1	3	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
13	ns	172.16.20.0/24		169.254.0.1	3	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
14	ns	172.16.30.0/24		169.254.0.1	3	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
15	b	192.168.0.0/24		192.168.140.1	20	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
16	b	192.168.100.0/24		192.168.140.1	20	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
17	b	192.168.110.0/24		192.168.140.1	20	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
18	b	192.168.120.0/24		192.168.140.1	20	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
19	b	192.168.130.0/24		192.168.140.1	20	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
20	С	192.168.140.0/24		192.168.140.3	0	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
21	b	192.168.150.0/24		192.168.140.1	20	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
22	b	192.168.200.0/24		192.168.140.1	20	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIER0
23	b	192.168.210.0/24		192.168.140.1	20	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
24	b	192.168.220.0/24		192.168.140.1	20	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIER0
25	b	192.168.230.0/24		192.168.140.1	20	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO
26	b	192.168.240.0/24		192.168.140.1	20	c9393d0c-1fcf-4c34-889d-2da1eeee25b8	SERVICE_ROUTER_TIERO

Figure 3-1-32: Sample Routing Table of a Tier0 Router

-	A	B	c	D	E		G	H
1	route_type	network	logical_router_port_id	next_hop	admin_distant	clr_component_id	Ir_compone	nt_type
2	route	10.10.20.0/24	2307d6b0-913c-4abd-83bf-e8144572f114	192.168.150.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
3	route	10.10.30.0/24	2307d6b0-913c-4abd-83bf-e8144572f114	192.168.150.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
4	route	10.20.20.0/24	2307d6b0-913c-4abd-83bf-e8144572f114	192.168.150.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TalERO
5	route	10.20.30.0/24	2307d6b0-913c-4abd-83bf-e8144572f114	192.168.150.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
6	route	30.0.0/8	2307d6b0-913c-4abd-83bf-e8144572f114	192.168.150.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
7	route	100.64.80.0/31	245131f5-4912-4c62-89ba-e6e84406fb2f	169.254.0.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
8	route	100.64.80.2/31	245131f5-4912-4c62-89ba-e6e84406fb2f	169.254.0.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
9	route	100.64.80.4/31	245131f5-4912-4c62-89ba-e6e84406fb2f	169.254.0.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
10	route	172.16.10.0/24	245131f5-4912-4c62-89ba-e6e84406fb2f	169.254.0.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
11	route	172.16.10.10/32	245131f5-4912-4c62-89ba-e6e84406fb2f	169.254.0.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
12	route	172.16.20.0/24	245131f5-4912-4c62-89ba-e6e84406fb2f	169.254.0.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
13	route	172.16.30.0/24	245131f5-4912-4c62-89ba-e6e84406fb2f	169.254.0.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
14	route	192.168.0.0/24	2307d6b0-913c-4abd-83bf-e8144572f114	192.168.150.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
15	route	192.168.100.0/24	2307d6b0-913c-4abd-83bf-e8144572f114	192.168.150.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
16	route	192.168.110.0/24	2307d6b0-913c-4abd-83bf-e8144572f114	192.168.150.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
17	route	192.168.120.0/24	2307d6b0-913c-4abd-83bf-e8144572f114	192.168.150.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
18	route	192.168.130.0/24	2307d6b0-913c-4abd-83bf-e8144572f114	192.168.150.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
19	route	192.168.140.0/24	2307d6b0-913c-4abd-83bf-e8144572f114	192.168.150.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
20	route	192.168.200.0/24	2307d6b0-913c-4abd-83bf-e8144572f114	192.168.150.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
23	route	192.168.210.0/24	2307d6b0-913c-4abd-83bf-e8144572f114	192.168.150.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
27	route	192.168.220.0/24	2307d6b0-913c-4abd-83bf-e8144572f114	192.168.150.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
23	route	192.168.230.0/24	2307d6b0-913c-4abd-83bf-e8144572f114	192.168.150.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE_RC	DUTER_TIERO
24	route	192.168.240.0/24	2307d6b0-913c-4abd-83bf-e8144572f114	192.168.150.1	0	e668ccc3-f787-4c96-84d4-ad845478089d	SERVICE RO	NITER TIERO
25	route	0.0.0/0	481ab2ea-7b92-471b-9d1a-29226bf9f708	169.254.0.3	0	c91eb7c5-0297-4fed-9c22-b96df1c9b80f	DISTRIBUTE	D_ROUTER_TIERO
26	route	172.16.10.0/24	ddb16484-d12e-42da-bf2e-4d59f7139ace	100.64.80.1	0	c91eb7c5-0297-4fed-9c22-b96df1c9b80f	DISTRIBUTE	D_ROUTER_TIERO
27	route	172.16.10.10/32	ddb16484-d12e-42da-bf2e-4d59f7139ace	100.64.80.1	0	c91eb7c5-0297-4fed-9c22-b96df1c9b80f	DISTRIBUTE	D_ROUTER_TIERO
28	route	172.16.20.0/24	ddb16484-d12e-42da-bf2e-4d59f7139ace	100.64.80.1	0	c91eb7c5-0297-4fed-9c22-b96df1c9b80f	DISTRIBUTE	D_ROUTER_TIERO
29	route	172.16.30.0/24	ddb16484-d12e-42da-bf2e-4d59f7139ace	100.64.80.1	0	c91eb7c5-0297-4fed-9c22-b96df1c9b80f	DISTRIBUTE	D_ROUTER_TIER0
30	route	192.168.140.0/24	481ab2ea-7b92-471b-9d1a-29226bf9f708	169.254.0.2	0	c91eb7c5-0297-4fed-9c22-b96df1c9b80f	DISTRIBUTE	D_ROUTER_TIERO
31	route	192.168.140.3/32	481ab2ea-7b92-471b-9d1a-29226bf9f708	169.254.0.2	0	c91eb7c5-0297-4fed-9c22-b96df1c9b80f	DISTRIBUTE	D_ROUTER_TIERO
32	route	192.168.150.0/24	481ab2ea-7b92-471b-9d1a-29226bf9f708	169.254.0.3	0	c91eb7c5-0297-4fed-9c22-b96df1c9b80f	DISTRIBUTE	D_ROUTER_TIERO
33	route	192.168.150.3/32	481ab2ea-7b92-471b-9d1a-29226bf9f708	169.254.0.3	0	c91eb7c5-0297-4fed-9c22-b96df1c9b80f	DISTRIBUTE	D_ROUTER_TIERO

Figure 3-1-33: Sample Forwarding Table of a Tiero Router

For Tier1 routers, only the forwarding table is available. The information may vary depending on which node it is downloaded from (i.e., hypervisor or Edge node) and if the Tier1 router has Services Router component or not:

I	12	A	B	C	D	E	F	G
I	1	route_type	network	logical_router_port_id	next_hop	admin_distance	lr_component_id	lr_component_type
I	2	NSX_INTERNAL	0.0.0.0/0	93799da6-bca2-47bc-b9d8-30d51209a00e	169.254.0.2	0	9333c94e-5938-46b4-8c7d-5e6ac2c8b7b5	DISTRIBUTED_ROUTER_TIER1
1	3	CONNECTED	169.254.0.0/28	93799da6-bca2-47bc-b9d8-30d51209a00e	0.0.0.0	0	9333c94e-5938-46b4-8c7d-5e6ac2c8b7b5	DISTRIBUTED_ROUTER_TIER1
I	4	CONNECTED	172.16.10.0/24	fb6cbf5b-3c40-419c-80c4-b8b44c0c6e71	0.0.0.0	0	9333c94e-5938-46b4-8c7d-5e6ac2c8b7b5	DISTRIBUTED_ROUTER_TIER1
I	5	NSX_INTERNAL	172.16.10.10/32	93799da6-bca2-47bc-b9d8-30d51209a00e	169.254.0.2	0	9333c94e-5938-46b4-8c7d-5e6ac2c8b7b5	DISTRIBUTED_ROUTER_TIER1
I	6	CONNECTED	172.16.20.0/24	788829d9-a9fe-4f0b-9d76-99d7077fd5fa	0.0.0.0	0	9333c94e-5938-46b4-8c7d-5e6ac2c8b7b5	DISTRIBUTED_ROUTER_TIER1
1	7	CONNECTED	172.16.30.0/24	356ac247-ccea-420c-a2bc-96c9c71bfbc8	0.0.0.0	0	9333c94e-5938-46b4-8c7d-5e6ac2c8b7b5	DISTRIBUTED_ROUTER_TIER1

Figure 3-1-34: Sample Tier1 Router Forwarding Table from Hypervisor Node

	A	В	C	D	E	F	G
1	route_type	network	logical_router_port_id	next_hop	admin_distance	lr_component_id	lr_component_type
2	route	0.0.0.0/0	498b1a03-3077-412a-bde4-47ee3da4567c	100.64.80.0	0	676b7edf-6dae-4374-81c2-aff0b4346cfe	SERVICE_ROUTER_TIER1
3	route	172.16.10.0/24	a660347b-5d71-4907-8082-f73c110766d4	169.254.0.1	0	676b7edf-6dae-4374-81c2-aff0b4346cfe	SERVICE_ROUTER_TIER1
4	route	172.16.20.0/24	a660347b-5d71-4907-8082-f73c110766d4	169.254.0.1	0	676b7edf-6dae-4374-81c2-aff0b4346cfe	SERVICE_ROUTER_TIER1
5	route	172.16.30.0/24	a660347b-5d71-4907-8082-f73c110766d4	169.254.0.1	0	676b7edf-6dae-4374-81c2-aff0b4346cfe	SERVICE_ROUTER_TIER1
6	route	0.0.0.0/0	93799da6-bca2-47bc-b9d8-30d51209a00e	169.254.0.2	0	9333c94e-5938-46b4-8c7d-5e6ac2c8b7b5	DISTRIBUTED_ROUTER_TIER1
7	route	172.16.10.10/32	93799da6-bca2-47bc-b9d8-30d51209a00e	169.254.0.2	0	9333c94e-5938-46b4-8c7d-5e6ac2c8b7b5	DISTRIBUTED_ROUTER_TIER1





Figure 3-1-35: Sample Tier1 Router (with SR Component) Forwarding Table from Edge Node

#### 3.2.4 Security Counters/Stats/Tables

NSX-T also provides statistics and counters for the Distributed Firewall (DFW), the Gateway Firewall, and for the NAT service.

#### **NSX Distributed Firewall Counters**

The NSX Distributed Firewall exposes per-rule statistics, that show the number of packets, bytes and sessions that have matched each of the rules. Per Rule Level Stats aggregated every 15 Minutes from all the Transport Nodes. Each rule will have the hit count, packet count, session count, byte count and popularity index. Rule statistics can be reset using "Reset All Rules Stats".

	IBUTE	D FIREWALL						ACTION	S Y REVERT	PUE	BLISH
ALL RULE	S	CATEGORY SPECIFI	CRULES								
ET	HERNE	r (I)	EMERGENCY (4)	INFRASTRUCTURE (	3) ENVIRON	NMENT (6)	APPLICATION (13)				
+ ADD P	OLICY	+ ADD RULE	CLONE +	) UNDO						$\boxtimes$	Ξ
		Name	ID	Sources	Collapse All Policy	tices	Profiles	Rule Hits Statistics			
: >		PROD-MRS-APP (6	) Applied To	DFW	Reset All Rules Stat	s		Hit Count Session Count	9338 O		0
÷ ~		DEV-MRS-APP (6)	Applied To	DFW				Popularity Index	9	E	0
÷		TO-MRS-WEB	3110	Any	SO DEV-MRS	O HTTPS	🐻 ssl	Max Popularity Index Max Session Count	3190 276010		2
÷		WEB-to-MID	3111	DEV-MRS	SO DEV-MRS-M_	🔘 НТТР	🛃 нттр	Total Session Count Flow Statistics	523556		2
1		MID-to-DB	3112	88 DEV-MRS-M_	CONTRACTOR DEV-MRS-DB	O MySQL	MYSQL	Packet Count Byte Count	9338 522928	i	2
1		TO-MRS-APP	3099	Any	BO DEV-MRS-A	O HTTPS	🐻 SSL	Note: The above stats may be st aggregated stats are computed	ale because every 15 minutes.		
÷		MRS-to-MRS	3100	BO DEV-MRS-A_	BO DEV-MRS-A	Any	None				2
÷		DenyAny	3101	Any	Any	Any	None	Reje			
: >		Default Layer3 S	(1) Applied To	DFW					Success	sC C	0

Figure 3-1-36: NSX Distributed Firewall statistics

#### **Gateway Firewall Counters**

Similarly, Gateway Firewall provides per-rule statistics.

D POLICY	+ ADD RULE	CLONE CLONE	DELETE	072			· · · · · · · · ·	Filter by Name, F	Path and more
	Name	ID	Sources		ces	Profiles	Applied To	Action	
	TENANT-1 (	) Category:	LOCAL GATEWAY	Collapse All Policy					In Progress C
	Rule-1	3113	Any	Reset All Rules Stats	HTTPS	🐻 SSL	PROD-ZONE-GW	• Allow ~	•
	Policy_Default_Infra (	) Category:	DEFAULT						
							Rule Hi	ts Statistics	
							Hit Cour	st	142
							Session	Count	19
							Popular	ty Index	17
							Max Poj	sularity Index	3356
							Max Ses	sion Count	19
							Total Se	ssion Count	26
							1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		
							Flow St	atistics	
							Flow St Packet	atistics Count	592

Figure 3-1-37: Gateway Firewall statistics



NSX-T 3.0: Operation Guide

Note: Gateway firewall is only available on the routers that have deployed the Service Router (SR) component.

#### **NAT Counters**

Finally, NSX provides counters for the NAT rules configured. To access these counters, once on the *Routing* menu, select the *Services* tab and then, on the drop-down menu, select *NAT*.

Note: NAT is provided as a centralized service, and as such, an SR component must be instantiated on the Edge cluster.

Once on the NAT page, click on the bars icon to get per-rule statistics:



Figure 3-1-38: NAT per-rule statistics

#### 3.3 Monitor Logical Switch Port activity

Counters and stats described in previous sections, show cumulative data gathered over time. Sometimes, it is also required to monitor the activity of a specific logical port over a specific period especially for troubleshooting purposes. NSX provides a port activity tracking tool that allows for that. It is available through the *Switching* menu, under the *Port* tab. After highlighting the specific port, the *Monitor* tab must be selected, and then the *Begin Tracking*.



+ 4	n 🖗 🗸	App-VM-20.10/	App-VM-20.10	0.vmx@ca88a3	fe	,
	Logical Port 1	Overview Monit	or Manage -	Related ~		
	7-TO-Test-Int-UL1-ulp					
-	App-VM-20.10/App-VM>	Port Status & Statis		AD MAC TABLE	EGIN TRACKING	REFRESH
	CentOS/CentOS.vmx@c	Operational Status: Last Updated at	• Up Oct 27, 2020	4·16:31 AM		
	DB-VM-30.10/DB-VM-3	MAC Learning Stati	stics			
	DB-VM-30.20/DB-VM-3	Number of MACs Lea	irned	0		
	DB-VM-30.30/DB-VM-3	Packets Allowed with Packets Dropped wit	out MAC Learning hout MAC Learning	0		
0	infra-Seg7-DB-Vlan130	Traffic Statistics				
0	infra-Seg77-App-Vlan2	Traffic (Cumulative)	Transmitted Bytes	Transmitted Packet	Received Bytes	Received Packets
Θ	kvm-vm2	Unicast	25 19 KB	267	23 31 KB	263
	nsx-mgr-137/nsx-mgr-1	Multicast & Bro	12 21 MR	19/ 912	7 02 MR	02.496
	nsx-mgr-147/nsx-mgr-1	Dropped	0.00 Rytes	104,012	0.00 Puter	52,400
	nsx-mgr-157/nsx-mgr-1	TOTAL	0.00 Bytes	4	0.00 Bytes	00.701
7	vmknic@50286d93c781	TOTAL	13.24 MB	185,083	7.95 MB	92,761

Figure 3-2-1: Logical Port Begin Tracking

After clicking on *Begin Tracking*, a new window pops-up. It shows the different counters for the selected port, and automatically refreshes every 10 seconds. Once the window is closed, port tracking finishes and the information is eliminated:

vm NSX								¢
LAB-01-TENANT-01	-APP-01-APP_1/LAB-0	D1-TENAN	T-01-APP-01-APP.vm	x@0278b2	28a-f713-4fe8-b8a9	-a6ca4d926	101	TRACKING
PORT - MONITOR						LAST UP	DATED	Oct 27, 2020 10:33:58 PI
Traffic (Cumulative)	Transmitted Bytes		Transmitted Packets		Received Bytes		Received	Packets
Unicast	0.00 Bytes		0		0.00 Bytes		0	
		2.01 GB		30,943,482		2.31 GB		30,954,203
Multicast & Broadcast	0.00 Bytes		0		600.00 Bytes ٨		10 🔨	
		12.92 MB		182,458	-	397.11 MB	-	6,896,129
Dropped	0.00 Bytes		0		0.00 Bytes		0	
		0.00 Bytes		0		0.00 Bytes		12
TOTAL		2.03 GB		31,125,940		2.70 GB		37,850,344

Figure 3-2-2: A logical port tracking in progress

## 3.4 BGP Neighbor Status, Geneve Tunnel Status

Besides counters, statistics and tables for the traffic through the NSX fabric, it is also possible to monitor the status of two other important aspects of a typical NSX deployment: BGP Neighbor Status and Geneve Tunnel Status.

#### 3.4.1 BGP Neighbor Status

BGP (Border Gateway Protocol) is one of the most popular options for establishing routing adjacencies between NSX and existing networks. It can be configured on the Tier-0 Logical Router and, once configured, it is possible to download the routing tables as specified on 3.2.3 Layer 3 Counters/Stats/Tables and it is also possible to check the status of the BGP neighbors from the NSX UI.

To access BGP Neighbor Status information, administrators need to navigate to the *Routing* menu, then highlight the corresponding Tier-0 router, and finally, on the *Actions* drop-down menu, select *Generate BGP Summary*:





«	Tier-0 Logical Route	ers				
② Network Overview	+ ADD ØEDIT 📋 DE	LETE	ACTIONS ~		Q Search	
Connectivity	Logical Router ↑	ID	Connect to Tier-O Router	Mode	Transport Zone	Edge Cluster
Tier-0 Logical Routers		1f73	Disconnect from Tier-O Router Manage Tags		LAB-01-nsx-uplinks-vl	LAB-01-EDGE-CLUSTE
🔁 Tier-1 Logical Routers	PROXY-ARP-TO	c5fi	Generate BGP Summary		LAB-01-nsx-uplinks-vl	LAB-01-EDGE-CLUSTE
E Logical Switches	□⊖ VRF-A	ec8	Download Routing Table Download Forwarding Table			LAB-01-EDGE-CLUSTE
Network Services			Download Debug Information			
→ NAT						
we coau balancing						

Figure 3-3-1: Generating BGP Summary

By default, the summary shows information from all Edge nodes where the Tier-0 is deployed, but it can be filtered to a specific Edge node if required:

ansport Node		×	~					
GP Summary	LAB-01-EDGE-02							
	LAB-01-EDGE-01							
Transport Node	Source Addres	Neighbor Add	Remote AS	Connection Status	Messages Rec	Messages Sen	Connection Dr	Established
LAB-01-EDGE-02	172.16.110.2	172.16.110.11	65000	<ul> <li>Established</li> </ul>	127796	116145	0	1
LAB-01-EDGE-02	172.16.100.2	172.16.100	65000	<ul> <li>Established</li> </ul>	127813	116145	0	1
LAB-01-EDGE-02	169.254.0	169.254.0	65100	<ul> <li>Established</li> </ul>	6968647	6968609	1	2
LAB-01-EDGE-01	172.16.110.1	172.16.110.11	65000	<ul> <li>Established</li> </ul>	127864	116146	0	1
LAB-01-EDGE-01	0.0.0.0	172.16.100	65000	Active	38	34	1	1
LAB-01-EDGE-01	169.254.0	169.254.0	65100	<ul> <li>Established</li> </ul>	6968610	6968651	1	2
COLUMNS   C	; REFRESH Last Update	d: a few secon	ds ago			< BACK	NEXT > 1-	6 of 6 records

Figure 3-3-2: Sample BGP Summary output

#### 3.4.2 Geneve Tunnel Status

NSX uses GENEVE (GEneric NEtwork Virtualization Encapsulation) as its overlay mechanism. For any given Transport Node (a node participating on the forwarding of NSX Logical Networks), is it possible to check the status of the Geneve tunnels it stablishes with other NSX transport nodes. Geneve tunnel status information is available under the *Fabric* menu, *Transport Nodes* tab. Then it is required to highlight the transport node to be checked, and finally, Geneve tunnel information is under the transport node *Monitor* tab.





vm NSX			Q Ø	
«	Hosts Edges Edge Clusters	Bridges Transport Nodes		
② Dashboard				
Getting Started	+ 0 1 0 • 5	edge01		
Contracts	Transport Node 1	Overview Monitor		
- 1003	esxi-01			
off Load Balancing	esxi-02	V System Usage REFRESH		
E Firewall	edge01	CPU Cores 2 Average 0.87 / 1.1 / 1.59 Uptime 2 weeks, 5 days Last 2/12/2018, 7:42:46 AM		
Encryption	edge02	Load Updated		
0.0	edge03	Total Total Total Total Total	Total	Total
· Routing	kvm-01	4GB 4GB 9GB 18GB 394MB 944MB	19GB	19GE
DDI				
Switching	L KVIPO2	Memory Swap /var/log / /run /boot	/config	/imag
(i) touristance		8		•
Inventory				
Pabric		Controller Connectivity • Up Manager Connectivity • Up		
Nodes		PNIC/Bond Status • 4 Up • 0 Down		
Profiles		Turnel Flaker, ALL, FUE, A DOMN.		_
Transport Zones		Turnel Status: ALL S OF O DOWN Priter by BrD Status: ALL		~
Compute Managers		geneve3232297_ • Up 0 - No Diagnostic GENEVE tp-eth0 192.168.240.101 esxi-0	ote Transport Nod	
System		geneve3232297 • Up 0 - No Diagnostic GENEVE fp-eth0 192.168.240.102 kvm-4	51	-1
		geneve3232297_ • Up 0 - No Diagnostic GENEVE fp-eth0 192:168.240.103 kvm-4	52	
		geneve3232297	02	
		C BACK NEXT > 1-S of S records		-
	c > 1.77	1		

Figure 3-3-3: GENEVE Tunnel Status

For faster tunnel failure detection, NSX uses BFD control packets, which are encapsulated in Geneve and exchanged between the different transport nodes. The Transport Node *Monitor* page allows to filter the list of tunnels based on their BFD status:

Controller Connectivity • Up			Manager Connectivity	• Up	
PNIC/Bond Status • 4 Up • 0	Down				
Tunnel Status: ALL 5 UP 0 D	OWN		Filter by	y BFD Status:	ALL
Tunnel Name Status BF	D Diagnostic Code	Encap	Encap Interface	Remote IP	ALL
geneve3232297 • Up 0 -	No Diagnostic	GENEVE	tp-eth0	192.168.240.1	0 - No Diagnostic
geneve3232297 • Up 0 -	No Diagnostic	GENEVE	fp-eth0	192.168.240.1	<ol> <li>Control Detection Time Expired</li> <li>Echo Function Failed</li> </ol>
geneve3232297 • Up 0 -	No Diagnostic	GENEVE	fp-eth0	192.168.240.1	3 - Neighbor Signaled Session Dov
geneve3232297 • Up 0 -	No Diagnostic	GENEVE	fp-eth0	192.168.240.1	4 - Forwarding Plane Reset 5 - Path Down
< BACK NEXT > 1-5 of 5 reco	ords				6 - Concatenated Path Down
					7 - Administratively Down
Network Interface					8 - Reverse Concatenated Path Do

*Figure 3-3-4: Geneve tunnels by BFD status* 

#### 3.5 Monitor Edge Node

Edge resource utilization related information can be found on the Edge Monitor page. You can see number of CPU cores are allocated for an edge node and distribution of the cores between Datapath and Services.



Host Transport Nodes Edge Transport Nodes Edg	ge Clusters ESXi Bridge Cl	usters NCP Clusters	5	
+ 🖉 🗇 🗸	7 - Edge7-141			
Edge	Overview Monitor T	unnels Related -		
Edge-1-148				
Edge7-141	>			
Edge7-151	CPU Cores	Alarms	Last Updated Timestamp	(UTC)
edge-2-158			Sep 10, 2020, 4:15:08 PM	C
	Total	Overall	Uptime	
	8 Allocated	1	10 weeks, 3 days	
	Datapath CPU ()		Services CPU ()	
	Utilization	Cores	Utilization	Cores
	3.48%	6 Allocated	5.47%	2 Allocated
	Highest Utilization for a s	ingle core: 5.77%	Highest Utilization for a sir	ngle core: 7.25%
	Overall Disk Utilization Utilization Per Partition ( /config 0.05 /	D 8.63 GB /tmp	{(availab 0.01 /3.69 GB /run	le}} GB of ((total)) GB Used 0.01 /3.12 GB
	Memory Pools ()			
	Name	Utilization	Alarms	Description
		No Merr	nory Pool found.	

Figure 3-4-1: Geneve tunnels by BFD status

## 3.6 VM Inventory

NSX-T is decoupled from vCenter, but it reads VM information directly from the different hypervisors it supports (vSphere, RHEL KVM, Ubuntu KVM). This information is leveraged by several features, like the NSX Groups used in firewall policies, or the logical port VIF attachment points.

NSX offers an inventory of the discovered VMs under the *Inventory* menu and *Virtual Machines* section. It includes all VMs which exist on the hosts, either they are connected to NSX logical networks or not.





vm NSX				Q @ A &
«	Virtual Machines			
② Dashboard				
Getting Started	S MANAGE TAGS			Q Search
> 🖹 Tools	Virtual Machine 1	External ID	Source	Tags
> 😤 Load Balancing	app-01a	50354c6f	esxi-01	0
	db-01a	f481644e	kvm-01	0
in Firewall	k8s-node01	50352513	esxi-02	0
Encryption	k8s-node02	50357b36	esxi-01	0
Routing	web-01a	503560c9	esxi-02	0
DDI	web-02a	5035d864	esxi-02	0
5 Switching	web-03	c00f600a	kvm-02	0
- Inventory				
Groups				
Services				
Virtual Machines				
Fabric				
System				

Figure 3-5-1: NSX VM inventory

By clicking on the VM name provides additional details for a given VM, including attachment information that allows to determine if it is connected to NSX or not.

Virtual Machines		Virtual Machines	
Virtual Machine +	db-01a	Virtual Machine +	k8s-node02
app Ola deb-Ola deb-Ola bits-node00 bits-	Overview         Related           >         Summary         db-01s           Numin         db-01s         H813537-bea7-4611-bdda-5013stacs544e           Host Local ID         M813537-bea7-4611-bdda-5013stacs544e           Source         kem-01           Power State         # Roming           P-Addresses         17.28-83.01	Versime Accesses     des Ota     des Ota	Overview         Related           > Summary
○ web-03	MCC Addresses 5254.0044.0641 Vill Attachments dal95(t=46354.464.4632970029840 Logical Plants db=704/kmm01 Transport Node km=-01 ➤ Tags MANAGE	web-03	Source ess (9) Prover State & Roming Br Addressies 100-075 Marchadessies 100-075 Marchadessies 100-075 Marchadessies 100-050564freb53389 MAC Addresses 0055565888 VM Attachemists Transport Node 2 Tags MAAACE

Figure 3-5-2: VMs attached and not attached to NSX Logical Networks

## 3.7 Search Utility

NSX includes a utility that allows to search for objects using different criteria from the NSX inventory. To access the tool, users must click on the magnifying glass available on the top-right corner of the NSX UI.



Figure 3-6-1: Launching NSX Search Utility

Then, they can enter the pattern they are looking for, and they will get a list of the objects (possibly of different kinds) sorted by relevance.



vm NSX-T		Q	众 ⑦∽ C admin
Home Networking Security In	nventory Plan & Troubleshoot	System	POLICY MANAGER
C seg			🙁 🗔 tit
mac discovery segment profile           entitie           qos segment profile			→ GO TO (5)
Name         security segment profile           segment         segment port           service segment         spoof guard segment profile	Tags Last Modified Time	Status Alarms	<ul> <li>Policy Views (5)</li> <li>Networking &gt; Segments</li> <li>Networking &gt; Segments &gt;</li> <li>Edge Bridge Profiles</li> <li>Networking &gt; Segments &gt;</li> <li>Metadata Proxy</li> </ul>
			B Networking > Segments > Segment Profiles 대 Security > Network

Figure 3-6-2: NSX Search

Q	segment port where adm	in state = UP				⊗ 🖹 ₩ 🛛 ×
$\bigcirc$	ENTITIES					
Se	egment Ports					
	Name	Resource Type	Tags	Last Modified Time	Status	Alarms
>	nsx-mgr-137/nsx-mgr-137.vmx@fOc	Segment Ports	0	2020/05/18, 11:15 AM	● Success C	0
>	Vyatta-Router/Vyatta-Router.vmx	Segment Ports	0	2020/06/25, 09:25 AM	Success C	0 —
>	DB-VM-30.30/DB-VM-30.30.vmx@	Segment Ports	0	2020/06/15, 07:25 PM	● Success C	0 —
>	DB-VM-30.10/DB-VM-30.10.vmx@2	Segment Ports	0	2020/06/15, 02:55 PM	● Success C	0 —
>	DB-VM-30.20/DB-VM-30.20.vmx@	Segment Ports	0	2020/06/16, 10:20 AM	Success C	0 —
>	kvm-vm2	Segment Ports	0	2020/07/30, 03:38 PM	● Success C	0
>	vmknic@50286d93c7817ad6-16bc3	Segment Ports	0	2020/10/17, 08:01 AM	● Success C	0 —
>	Windows-Jumphost/Windows-Jum	Segment Ports	0	2020/06/10, 04:55 PM	Success C	0 —

Figure 3-6-3: NSX Search Result

## 3.8 APIs, CLI, Central CLI

The visibility options described so far are based on the NSX Manager UI. This section focuses on API and CLI access.

#### 3.8.1 NSX APIs

NSX Manager provides a programmatic API to automate management activities. The API follows a resource-oriented Representational State Transfer (REST) architecture, using JSON object encoding. Clients interact with the API using RESTful web service calls over the HTTPS protocol. API documentation is available under VMware's official, public NSX documentation at <u>https://docs.vmware.com/en/VMware-NSX-T/index.html</u>, and it is embedded in the NSX Manager itself which can be accessed even in offline NSX deployments.

For that, it is only required to click on the *Help* icon on the top-right corner of the NSX Manager UI and then select *API Documentation* on the drop-down menu. Here is an example.





⊂ ↓ ?`	admin ~
Help	LICY MANAGER
API Documentation	
About	
End User License Agreement	

Figure 3-7-1: Accessing NSX Manager embedded API documentation

This will launch a new window, where the NSX API documentation is available. This information is automatically generated from the NSX code:

## NSX-T Data Center REST API 3.0 🛊

API Reference Related Code Samples VMware NSX-T API Guide Table of Contents NSX-T Data Center 3.0.0.0.0 1 Overview 2 All Methods 3 API Methods 3.1 Cloud Service Manager 3.1.1 AWS 3.1.1 VPCS 3.1.1.1 VPCS 3.1.1.1 Security Grou Overview Introduction NSX-T Data Center provides a programmatic API to automate management activities. The API follows a resource-oriented Representational State Transfer (REST) architecture, using JSON object encoding. Clients interact with the API using RESTful web service calls over the HTTPS protocol. 3.1.1.1.1 Security Groups 3.1.1.1.2 Service Endpoints 3.1.1.12 Service Endpoi 3.1.2 AWS Accounts 3.1.3 AWS Catewary AMIS 3.1.4 AWS Catewary AMIS 3.1.4 AWS Regulars 3.1.6 AWS key Pairs 3.1.6 AWS VPCS 3.1.8 AWS VPCS 3.1.9 Accounts Statistics 3.1.9 Accounts Statistics 3.1.10 Azure 3.1.10.2 Vinets 3.1.10.2 Vinets Each API method is identified by a request method and URI. Method parameters are specified as key-value pairs appended to the URI. Unless otherwise noted, request and response bodies are encoded using JSON, and must conform to the JSON schema associated with each method. The content type of each request and reply is "application/gion" unless otherwise specified. Each request that can be made is documented in the API Methods section. The associated request and response body schemas are documented in the API Schemas section. API Policy: Changes, Deprecations and Removals VMware NSX Data Center may add new features in both major and minor releases as designed as an increment of the "x" digit and "y" digit of the x.y.z product version. These new features may lead to additional APIs or non-breaking changes to existing APIs to support the new feature. 3.1.10.1 Security Groups 3.1.10.2 Vnets 3.1.10.2 Vnets 3.1.10.2.1 Service Endpoints 3.1.11 Azure Accounts 3.1.11 Azure Caletways 3.1.13 Azure IP Allocations 3.1.14 Azure Resjons 3.1.15 Azure Resjons 3.1.16 Azure Resjons 3.1.16 Azure Vnets 3.1.17 Cloud Service Manager 3.1.19 Proxy Server Profile 3.1.20 VPN 3.1.21 Virtual Machines 3.1.21 Virtual Machines 3.1.21 Tirewall Rules 3.2 Federation At least one year prior to the removal of any deprecated API VMware will document the APIs that are planned to be removed in the NSX Data Center API Guide by marking them with "deprecated" in this document. If available, replacement APIs will also be documented. API removal can be in a major or minor release but not in maintenance releases. NSX Data Center APIs marked as "experimental" or that are not documented in the NSX Data Center API Guide are not subject to this policy. This indicates that the API may be changed or removed without notice in a future NSX-T Data Center release. **Request Failures** It is possible for any request to fail. Errors are reported using standard HTTP response codes. It should be assumed the following errors could be returned by any API method: 301 Moved Permanently, 307 Temporary Redirect, 400 Bad Request, 401 Unauthorized, 403 Forbidden, 429 Too Many Requests, 500 Internal Server Error, 503 Service Unavailable. Where other errors may be returned, the type of error is indicated in the API method description. All errors are documented in the API Errors section. 3.2 Federation 3.2.1 Infra **Request Authentication** 

Figure 3-7-2: NSX Manager embedded API documentation

NSX APIs follow the specifications of the OpenAPI initiative (<u>https://www.openapis.org/</u>), which enables developers and third-party ecosystem to build applications and services around NSX, by standardizing on how REST APIs are described.

It is possible to download the OpenAPI specifications directly from the NSX Manager, by issuing one of the calls below described on the NSX API documentation:

- GET <u>https://<nsx-mgr>/api/v1/spec/openapi/nsx\_api.yaml</u>
- GET <u>https://<nsx-mgr>/api/v1/spec/openapi/nsx\_api.json</u>

<b>OpenAPI Specification of NSX-T Manager API</b> You can get an OpenAPI specification of the NSX-T Manager API with one of the following calls:	
<ul> <li>GET https://<nsx-mgr>/api/v1/spec/openapi/nsx_api.yaml</nsx-mgr></li> <li>GET https://<nsx-mgr>/api/v1/spec/openapi/nsx_api.json</nsx-mgr></li> </ul>	

Figure 3-7-3: Downloading NSX OpenAPI Specification



NSX-T 3.0: Operation Guide

This specification can be later imported into tools like Postman (<u>https://www.getpostman.com/</u>), to get the complete list of NSX APIs ready to consume.

Additionally, there are Python and Java SDKs (Software Development Kits) available for NSX, which can be downloaded from the *Drivers & Tools* section under the NSX Downloads page at <u>https://my.vmware.com</u>.

lect	VMware NSX-T is our next     environments, container dep	generation product that provides a scalable network virtualization and micro-segmentation platform for multi-hypervisor ployments and native workloads running in public cloud environments.	Product Resources	
	Customers who have purch	ased VMware NSX can download their relevant installation package from the product download tab below.	View My Download History	
	Read More		Product Info	
			Documentation	
			Community	
	Driver / Tool	Release Date		
	and a state of a state of			
>	NSX Container Plugin			
>	NSX Container Plugin VMware OpenStack Neutron Plugin	1,		
>	NSX Container Plugin VMware OpenStack Neutron Plugin Automation Tools and SDK(s)	1		
>	NSX Container Plugin VMware OpenStack Neutron Plugin Automation Tools and SDK(s) VMware NSX Automation SDK 2.1 for Pyr	1 thon 2017-12-21	Go to Downloads	
> ~	NSX Container Plugin VMware OpenStack Neutron Plugin Automation Tools and SDK(s) VMware NSX Automation SDK 2.1 for Py VMware NSX Automation SDK 2.1 for Jax	thon 2017-12-21 va 2017-12-21	Go to Downloads Go to Downloads	
> ~	NSX Container Plugin VMware OpenStack Neutron Plugin Automation Tools and SDK(s) VMware NSX Automation SDK 2.1 for Pyi VMware NSX Automation SDK 2.1 for Jax VMware NSX Automation SDK 2.0 for Pyi	thon 2017-12-21 va 2017-12-21 thon 2017-09-07	Go to Downloads Go to Downloads Go to Downloads	
>	NSX Container Plugin Vilware OpenStack Neutron Plugin Automation Tools and SDK(s) Vilware NSX Automation SDK 2.1 for Pyr Vilware NSX Automation SDK 2.0 for Pyr Vilware NSX Automation SDK 2.0 for Pyr Vilware NSX Automation SDK 2.0 for Jax	2017-12-21           va         2017-12-21           thon         2017-12-21           thon         2017-09-07           va         2017-09-07	Go to Downloads Go to Downloads Go to Downloads Go to Downloads Go to Downloads	

Figure 3-7-4: NSX SDKs on my.vmware.com

Alternatively, NSX SDKs can also be downloaded from https://code.vmware.com/sdks

Networking and Security	
VMware NSX-T for Java	VMware NSX-T for Python
NSX for vSphere HW VTEP Integration SDK ■	NSX for vSphere Partner SDK for Network Introspection and End Point Security $\begin{array}{c} \blacksquare \end{array}$



#### 3.8.2 NSX CLI

There is an NSX-specific CLI available on NSX appliances (i.e. Managers and Controllers) and on the hypervisor Transport Nodes.

The way to invoke the NSX CLI varies depending on the type of node. Here are the details.

1. **NSX Appliances (Managers, Controllers, Edges)** - Administrators should SSH into the appliance, and log-in with the *admin* credentials. They will automatically get into the NSX CLI mode.

**Note:** There is also a *root* user ID to log-in into the NSX appliances, but as stated by the log-in banner, it should only be used when asked by VMware support team.

2. Hypervisor Transport Nodes - Once on the hypervisor CLI, administrators should issue the command nsxcli to enter the





NSX CLI. Be aware it may require root privileges.

For example, for a ESXi transport node:

[root@esxcomp-01a:~] **nsxcli** esxcomp-01a.corp.local> esxcomp-01a.corp.local> esxcomp-01a.corp.local> get log logicalrouter Logical router logical-routers Logical routers logical-switch Logical switch logical-switch-port Logical switch port logical-switches Logical switches esxcomp-01a.corp.local> get log

And for an Ubuntu-based KVM transport node:

vmware@kvm-01:~\$ nsxcli -bash: /bin/nsxcli: Permission denied vmware@kvm-01:~\$								
vmware@kvm-01:~\$ sudo nsxcli [sudo] password for vmware:								
kvm-01> kvm-01> kvm-01> get log								
logical-router Logical router logical-routers Logical routers logic switches kvm-01> get log	cal-switch Logical switch logical-switches Logical							

The list of available commands may vary depending on the type of node been managed. There is a public, detailed NSX CLI documentation available at <a href="https://docs.vmware.com/en/VMware-NSXT/index.html">https://docs.vmware.com/en/VMware-NSXT/index.html</a>.

vm VMware Docs	Q Search for VMware Product Information 🛞 🛞 VMware Pages MyLibrary Login							
VMware NSX-T Data Center	Product Documentation							
호] Expand All	VMware NSX-T Data Center Documentation							
∨ 2.5	a f 🛩 in							
> Release Notes	VMware NSX-T <sup>IM</sup> Data Center (formerly NSX-T) provides an agile software-defined infrastructure to build cloud-native application environments.							
NSX-T Data Center Installation Guide	NSX-T Data Center is focused on providing networking, security, automation, and operational simplicity for emerging application frameworks and architectures that have							
NSX-T Data Center Administration Guide	heterogeneous endpoint environments and technology stacks. NSX-T Data Center supports cloud-native applications, bare metal workloads, multi-hypervisor environments,							
NSX-T Data Center Upgrade Guide	public clouds, and multiple clouds.							
NSX-T Data Center Migration Coordinator Guide	NSX-T Data Center is designed for management, operation, and consumption by development organizations. NSX-T Data Center allows IT and development teams to select the technologies best suited for their applications.							
VMware NSX-T Data Center Plugin for OpenStack Neutron Installation Guide	Use the navigation on the left to browse the available NSX-T Data Center documentation including the API and CLI guides.							
NSX Container Plug-in for Kubernetes and Cloud Foundry - Installation and Administration Guide	To access the PDP format of NSX-1 Data Center documentation, select a guide and click the PDP icon 因. Additional Resources							
NSX Container Plug-in for OpenShift - Installation and Administration Guide	NSX-T Data Center Reference Design Guide     NSX-T Data Center Product Page							
> API and CLI Guides	NSAT Data Center Hands-on Labs (HOL)     NSAT Data Center Hands-on Labs (HOL)							
√ 2.4	NSX-T Data Center Training and Demo videos							
> Release Notes	Most Helpful Topics							
NSX-T Data Center Installation Guide								
NSX-T Data Center Administration Guide	Create an NSoroup Overview of NSV-T							
NSX-T Data Center Upgrade Guide	NSX-T Container Plug-in for OpenShift - Installation and Administration Guide							
NSX-T Data Center REST API Reference Guide 🕼								
NSX-T Data Center CLI Reference Guide								



**Note:** As stated on the NSX Command Line Interface Reference guide, command syntax and output format of NSX-T commands are not guaranteed to be the same from release to release. Thus, for automation tasks it is **recommended** to use the API.





#### 3.8.3 NSX Central CLI

To avoid changing interfaces and for those cases where NSX admins/operators may not have access to hypervisors CLI, NSX introduces a feature called **Central CLI**, which allows to run a command on any NSX appliance or transport node, directly from the NSX Manager CLI.

Furthermore, Central CLI permits to run the same command on multiple nodes at the same time, including nodes of multiple types (for example, run the same command on a Controller, an ESXi hypervisor and a KVM hypervisor).

To use Central CLI, admins must access the CLI of the NSX Manager, and once there, issue the on command:

on	n <registered-node-uuid> exec [<command/>]</registered-node-uuid>								
	Run command on registered cluster/fabric nodes								
	Option	Description							
	<registered-node-uuid></registered-node-uuid>	First UUID of any registered node							
	Mode Basic								
	<b>Availability</b> Manager								

Figure 3-7-7: Invoking NSX Manager Central CLI

After entering the on keyword, admins can click on Tab or the question mark to get a list of the nodes where they can run the desired command:

```
nsxmgr-01a> on
264d494a-ee24-41ce-8ca4-80015cf10000 kvmcomp-02a.corp.local
31150b76-06b4-4b45-9704-d7c89fe53ebf esxcomp-02a@corp.local
422ee699-f4d1-5216-e6ed-ea9e3b4fcec5 nsxmgr-01a
53206bfa-5b8c-11e7-b489-005056ae5144 edgenode-01a
5ed9afd8-5b8c-11e7-9c6e-00505688557f edgenode-02a
97f4dd41-faa1-40bc-b54e-ca2010bb36cc kvmcomp-01a.corp.local
a4e7bcdb-5d18-4d42-ae7b-4be04e85f47c esxcomp-01a@corp.local
d3e7be01-1cf5-4cf6-bf59-0574b243a267 nsxctrl-01a
```

Figure 3-7-8: Listing available nodes in Central CLI

To select a node, admins should enter their UUID. It is enough to enter the first characters and click on the Tab key to get the rest of the string autocompleted. Once one node is selected, it is removed from the list of available nodes.

On the example, the admin has already selected *edgenode-01a* (UUID 53206bfa-5b8c-11e7-b489005056ae5144), and thus it is not offered as a possible selection again.



```
nsxmgr-01a> on 53206bfa-5b8c-11e7-b489-005056ae5144
  264d494a-ee24-41ce-8ca4-80015cf10000
                                        kvmcomp-02a.corp.local
 31150b76-06b4-4b45-9704-d7c89fe53ebf
                                        esxcomp-02a@corp.local
 422ee699-f4d1-5216-e6ed-ea9e3b4fcec5
                                        nsxmgr-01a
  5ed9afd8-5b8c-11e7-9c6e-00505688557f
                                        edgenode-02a
 97f4dd41-faa1-40bc-b54e-ca2010bb36cc
                                        kvmcomp-01a.corp.local
  a4e7bcdb-5d18-4d42-ae7b-4be04e85f47c
                                        esxcomp-01a@corp.local
 d3e7be01-1cf5-4cf6-bf59-0574b243a267
                                        nsxctrl-01a
                                        Execute command
  exec
```

Figure 3-7-9: Selecting nodes in Central CLI

To select additional nodes, admins must simply append their UUIDs to the existing list. Once the desired list of nodes is completed, admins should append the **exec keyword**. Central CLI will then show the list of available commands to run on the selected nodes:

ISYIIRL-019	> OIL 22560014-200C-1161-0402-0020209622144 26024109-209C-1161-2006-002020892211 6Ke					
clear	Clear setting					
del	Delete configuration					
detach	Detach from NSX cluster					
exit	Exit from current mode					
get	Retrieve the current configuration					
[trunca	ted output]					
vrf	Enter VRF context mode					
<cr></cr>	Execute command					
1	Output modifiers					

Figure 3-7-10: Listing available Central CLI commands

The output of Central CLI identifies which information belongs to each of the nodes where the command is run. The example below, shows the output of the command *get logical-routers* executed on a KVM hypervisor, a NSX Controller and NSX Edge at the same time:

nsxmgr01> on 37056955-a96d-456a-87a9-43eaadca1490 88ff5965-3481-4498-8665-98e91ff24dc8 13960378-b96f-11a7-ae57-00505695581e exec get logical-routers								
88ff5905	-3d81-4e98-8d65-98	e91ff24dc8 kvm	kvm-01					
c91eb7 9333c9	Log Router UUID 'c5-0297-4fed-9c22- '4e-5938-46b4-8c7d-	ical Routers Summ b96df1c9b80f 5e6ac2c8b7b5	ID 9 8	Port Count 2 5				
37b569b5	-a96d-4b6a-87a9-43	eaadca1490 ctl	nsxcontrol	ler01				
LR-ID 0x8	LR-Name DR-t1-router01	Hosts[] 192.168.110.54 192.168.110.53 192.168.110.57 192.168.110.55	Service-C 192.168.1	ontroller Router 10.16 DISTRI	-Type BUTED_ROUTER_TIER1	ClusterId	UUID 9333c94e-5938-46b4-8c7d-5e6ac2c8b7b5	
0x9	DR-t0-router	192.168.110.54 192.168.110.54 192.168.110.53 192.168.110.57 192.168.110.55 192.168.110.58	192.168.1	10.16 DISTRI	BUTED_ROUTER_TIER0		c91eb7c5-0297-4fed-9c22-b96df1c9b80f	
0xa 0xb	SR-t0-router SR-t0-router	192.168.110.57 192.168.110.58	192.168.1 192.168.1	10.16 SERVIC 10.16 SERVIC	E_ROUTER_TIER0 E_ROUTER_TIER0	00002000 - 0000 - 0000 - 0000 - 00000000	c9393d0c-1fcf-4c34-889d-2da1eeee25b8 e668ccc3-f787-4c96-84d4-ad845478089d	
13960378	-b96f-11e7-ae57-00	5056b5581e edg	edge01					
Logical UUID 736a80e3 c9393d0c 9333c94e c91eb7c5	Router -23f6-5a2d-81d6-bb -1fcf-4c34-889d-2d -5938-46b4-8c7d-5e -0297-4fed-9c22-b9	VRF efb2786666 0 aleeee25b8 1 6ac2c8b7b5 2 6df1c9b80f 3	LR-ID 0 10 8 9	Name SR-t0-router DR-t1-router01 DR-t0-router	Type TUNNEL SERVICE_ROUTER_TIERØ DISTRIBUTED_ROUTER_TIER DISTRIBUTED_ROUTER_TIERØ	Ports 3 5 7 4		
nsxmgr01	>							

Figure 3-7-11: Output of a Central CLI command

Sometimes, admins need to run multiple commands on a specific node. To simplify that process and the syntax of the commands to be used, Central CLI allows set a session to a specific remote node. Once on session mode, admins can enter the command in simple NSX CLI syntax, without having to prefix it with *on <UUID> exec*:



```
nsxmanager> on 0c90e0fe-647a-410f-826b-8e72498f52df exec
Entering session mode
SESSION-MODE>
SESSION-MODE>
SESSION-MODE> get logical-
logical-router Logical router
logical-routers Logical routers
logical-switch Logical switch
logical-switches Logical switches
SESSION-MODE>
```

Figure 3-7-12: Central CLI Session Mode




## 4 Operations Utilities

This section outlines NSX operational utilities listed below: o NSX Upgrade

o NSX Manager Backup/Restore o Support Bundle

## 4.1 NSX Upgrades

Starting from 2.4 release, NSX-T supports two upgrade modes, the maintenance upgrade mode and in-place upgrade mode. As to the maintenance upgrade mode, in addition to simplifying installation, Compute Managers also allow for upgrading hosts without impacting workload connectivity.

Cluster information read from the Computer Managers is leveraged by NSX to put hosts automatically into maintenance mode (workloads are migrated to additional resources and the original host gets empty). Only after that, NSX will update them, thus keeping workload connectivity at all times during host upgrades.

With the in-place upgrade mode, the workload VMs will not be migrated during the upgrade. The benefit of in-place upgrade mode is it takes less time to upgrade the host. The downside of the inplace upgrade mode is that the workload VMs might experience some packet lost.



## 4.1.1 Upgrade Coordinator

Upgrade Coordinator is a self-contained web application that runs on the NSX Manager and provides a single pane of glass for managing NSX upgrades. Key features are listed below.

- Checks existing version is upgradeable to the new one before starting the upgrade
- Allows to define upgrade plans for the different infrastructure components
- Performs upgrade in the correct order, ensuring stage success and managing retries of failed components
- Tracks and reports upgrade status
- Retains upgrade history

NSX upgrade utilities are available on System > Lifecycle Management > Upgrade, under the Upgrade tab.





vm NSX-T		Q	Ц <b>,</b>	<b>?</b> ~	admin	~
Home Networking Se	urity Inventory Plan & Troubleshoot System Advanced Networking & Security					
«	1. Bundle and Status 2. Edges 3. Hosts 4. Management Nodes					0
<ul> <li>2 System Overview</li> <li>Configuration         <ul> <li>Appliances</li> <li>Get Started</li> <li>Fabric</li> <li>Fabric</li> <li>Service Deployments</li> <li>Active Directory</li> </ul> </li> </ul>	Upload Upgrade Bundle O Upload MUB file O Upload from remote location Enter UPL* UPLOAD					
Lifecycle Management						
ద్ద Upgrade 'ந, Migrate						
Settings & Users Leenses Certificates Support Bundle Customer Experience Impr Proxy Settings						

Figure 4-1: NSX Upgrade Utility

Followings are to access Upgrade Coordinator:

1. Download NSX Master Upgrade Bundle from <a href="https://my.vmware.com/">https://my.vmware.com/</a>:

NSX 2.5.1 Upgrade Bundle File size: 9.14 GB File type: mub	Download Now
Name: VMware-NSX-upgrade-bundle-2.5.1.0.0.15314288.mub Release Date: 2019-12-19 Build Number: 15314288	NSX 2.5.1 Upgrade Bundle  Use this file to upgrade from existing installations of NSX-T 2.x release to the NSX-T 2.5.1 version. Please see the VMware Product Interoperability Matrices for supported upgrade paths.  MD5SUM: 4f361a1320cf50df184a31273bc95f16 SHA1SUM: ce5930f501b216e48d0d0050a7d94c4dce7d9df8 SHA256SUM: 9fc0bb344ca917a903f80c6303b234da52cf05837b7ea9bcebb175f 9bd184a4d

Figure 4-2: NSX Master Upgrade Bundle

2. On the NSX Manager UI, access *Systems > Lifecycle Management* menu, and on the *Upgrade* tab, click on *PROCEED TO UPGRADE* to upload the master upgrade bundle:

Upload Upgrade Bundle Upload MUB file Upgrade bundle (.mub)* VMware-NSX-upgrade-bund		
VMware-NSX-upgrade-bund		
	e-2.5.1.0.0.15314288.mub	BROWSE
UPLOAD		
<ul> <li>Upload from remote location</li> </ul>		

Figure 4-3: Uploading Master Upgrade Bundle

3. Once the master upgrade file is uploaded, NSX presents a *BEGIN UPGRADE* button. Clicking on it starts the first step of the Upgrade Process, which is upgrading the Upgrade Coordinator itself:



Figure 4-4

4. Once the Upgrade Coordinator is upgraded, the *BUNDLE AND STATUS* page is presented, where upgrade coordinator shows an overview of the system, reporting the issues it finds (if any):

1. Bundle and Status	2. Edges	3. Hosts	4. Management Nodes		
Upgrade Summary SI	now Upgrade History 业 EXPORT PRE CHE	CKs CsV	Upgrade Coordinator	Version: 2.5.1.0.0.153142	92
Edges		Hosts		Management N	Nodes
Upgrade Not Star	ted	Upgrade N	lot Started	Upgrade Not S	tarted
Target Version:     2       From Version:     2       Pre Check Status:     N	251.0.0.15314297 24.0.0.0.12454265 (2) No checks performed	Target Versio From Version Pre Check Sta	n: 2.5.1.0.0.15314289 2.4.0.0.0.12454259 (4) atus: No checks performed	Target Version: From Version: Pre Check Status:	2.5.1.0.0.15314292 2.4.0.0.0.12456291 (1) No checks performed
Upload Upgrade Bundle O Upload MUB file Upload from remote I Enter URL •	ocation				
	UPLOAD				

Figure 4-5: Upgrade Coordinator Bundle and Status page

5. Run re-check, fix any reported issues.



1. Bundle and Status 2. Edges 3. Hos	ts 4. Management Nodes	
Upgrade Summary Show Upgrade History 答 RUN PRE CHECKS 호 보 EXPORT PRE CHECKS C	Upgrade Coordinator Ver SV Last Pre Check Run: Fe	rsion: 2.5.1.0.0.15314292 ab 18, 2020 10:43:52 AM
Edges	Hosts	Management Nodes
Upgrade Not Started Target Version: 2.5.1.0.0.15314297 From Version: 2.4.0.0.0.12454265 (2) Pre Check Status:  Ø No Edge(s) with Issues  \$	Upgrade Not Started Target Version: 2.5.1.0.0.15314289 From Version: 2.4.0.0.012454259 (4) Pre Check Status: © 2 Host(s) with Issues	Upgrade Not Started Target Version: 2.5.1.0.0.15314292 From Version: 2.4.0.0.0.12456291 (1) Pre Check Status: ①1 Node(s) with Issues ◆
Upload Upgrade Bundle O Upload MUB file Upload from remote location Exter LID *		

## 4.1.2 Edge Upgrade

1. Bundle and Status 2. Ed	ges	3. Hosts		4. Management Nodes					0
Plan	RESET				Progress				
Upgrade order across groups	🔾 Serial	0	Parallel		Status	A Not Started 0%	► START		
Pause upgrade condition	When an up	grade unit fa	ils to upgrade		Details				
	∐ After each g	group comple	tes						
	By default, upgra	ade will pause	after all group	s are completed.					
Educ Course									
Edge Groups									
Group Name	ACTIONS ~	ID	Units	Upgrade Order within Group	State	Upgrade Status	Progress	Post Check Status	
edgegroup-sa-nsxedge-c	luster-01	0d0834_	2	Sertal	Enabled	Not Started	0%	No checks performed	
COLUMNS C REFRESH									

The Edge is the first NSX component to be upgraded after Upgrade Coordinator. Upgrade

Coordinator creates **one Upgrade Group for each existing Edge Cluster**, and it is not possible to move one Edge node from one group to another. Also, Edge **nodes inside each group are upgraded in serial mode**, this way only the upgrading node is down while all other nodes in the cluster remain active to continuously forward traffic. This setting is not customizable.

The Edge Upgrade page allows to customize the following upgrade options.

- 1. Define upgrade order between Edge groups (parallel vs serial)
- Serial mode upgrades groups consecutively, one after another
- Parallel mode upgrades all groups simultaneously





2. Decide if Upgrade Coordinator should pause automatically and when:

• *When an upgrade unit fails to upgrade* – This setting is checked by default and cannot be unselected for Edge upgrade. Upgrade will pause if any individual Edge upgrade fails.

- After each group completes Upgrade pauses after each Edge group finishes upgrading
  - 3. Reorder upgrade sequence between groups
- Once an Edge group is selected, the ACTIONS menu allows to modify its upgrade order related to all other groups (Reorder)

• Alternatively, a "dotted icon" made of two columns of four periods each, will show up when hovering over the name of the Edge groups. Clicking on them, allows to drag the corresponding group out of his position, to drop it at a new one, highlighted by a green line with small green arrows at each end.

Click on "Start" to start Edge upgrade.

	ges	3. Hosts		4. Management Nodes					
lan					Progress				
lpgrade order across groups	🔾 Serial	<b>0</b> P	arallel		Status	🔅 In Progress 📘 10%	II PAUSE		
ause upgrade condition	🔳 When an u	pgrade unit fa	ls to upgrad	le	Details	[172.20.10.61] Edge d160dc0f-25	0a-4bb7-9c7b-0	0915ccb83ebd ha	as entered maintenance mode
	∐ After each	group comple	tes.		MODE INFORM	ATION			
	By default, upg	rade will pause	after all group	ps are completed.	MORE INFORM	ATION			
dae Groups								Pause upgrade to	make changes to plan settings and gr
RUN POST CHECKS	ACTIONS -								
Group Name		ID	Units	Upgrade Order within Group	State	Upgrade Status	Progres	55	Post Check Status
dgegroup-sa-nsxedge-c	luster-01	0d0834	2	Serial	Enabled	In Progress		10%	No checks performed

Figure: Edge Upgrade





#### 4.1.3 Host Upgrade

NSX-T 3.0: Operation Guide

The Host Upgrade page allows to customize the upgrade sequence of hosts, disable certain hosts from upgrade, or pause the upgrade at various stages of the upgrade process.

Upgrade Coordinator creates a default Upgrade Plan that assigns hosts into different groups. On the default plan, vSphere and KVM hosts are assigned different groups. Additional groups can be created, and groups suggested by Upgrade Coordinator can be modified.

1. Bundle and Status 2. Edge	95	3. Ho	osts	4. Management I	Nodes					0
Plan	RESET					Progress				
Upgrade order across groups	<ul> <li>Sertal</li> </ul>		O Parallel			Status	A Not Started	0% STA	RT	
Pause upgrade condition	Vhen an up	pgrade i	unit fails to up	ograde		Details				
	L After each	group c	ompletes							
	By default, upgr	rade will	pause after all	groups are completed.						
Used Crowner										
Host Groups				2						
	TE = RUN	POST	Units	2 ACTIONS ~	State		Ungrade Mode	Upgrade Status	Progress	Post Check Status
Group for SA-Compute-01	da0	)4 -	2	Sertal	Enabled		In-place	Not started	0%	No checks performed
Group for newly added UBI	UNTU 58b	5 a	2	Parallel	Enabled		In-place	Not Started	0%	No checks performed
Group for SA Compute 02	000	)4 c	0	Sortal	<ul> <li>Enabled</li> </ul>		Maintonanco	Not Started	0%	No checks performed
🗇 COLUMNS   🖉 REFRESH	Last Updated:	a few s	econds ago						< BACK I	NEXT > 1-3 of 3 Groups
Do not power-off or reboot the nodes wh	en upgrade is in pr	ogress. Th	ney may be reboo	oted automatically as part of the	upgrade process.					BACK





Host Upgrade customization options allow the followings:

- 1. Define host to group membership
- By creating new host groups and assigning hosts to them
- By editing existing host groups and modifying their host membership

Host Groups + ADD ⊘ EDIT Ü DELETE ③	ACTIONS ~			
Group	ID	Upgrade Units	Upgrade Order within Gr	State
Group for newly added UBUNTU	d56dOaab	2	Parallel	Enabled
Group for compA	8353c19	2	Serial	Enabled

Figure 4-8: Adding or Editing Host Groups

**Note:** When using Compute Managers, host groups are automatically created for the DRS enabled, vSphere clusters that are part of the upgrade. It is not possible to add other standalone vSphere hosts to such groups.

- 2. Define upgrade order inside each group (parallel vs serial)
- Serial mode upgrades host inside the group consecutively—one after another
- Parallel mode upgrades host inside the group simultaneously

tate	Enabled	
pgrade Units		
	Available (4)	Selected* (2)
	🗋 esxi-01 🌲	🗌 kvm-02
	esxi-02.co	kvm-01
	kvm-01	D
	kvm-02 🔻	
lpgrade Order vithin Group	🔿 Serial 🔹 O Para	allel

**Note:** When overall Parallel mode and host group Parallel modes are selected, some limits are enforced to guarantee NSX performance. Thus, not all hosts may be upgraded simultaneously. Please check the NSX-T Administration Guide to find the limits on each version.



- 3. Define upgrade order between groups (parallel vs serial)
- Serial mode upgrades groups consecutively (i.e., one after another)
- Parallel mode upgrades all groups simultaneously

Plan		
Overall group upgrade order	<ul> <li>Serial</li> </ul>	Parallel
Pause upgrade	When an up	grade unit fails to up
condition	After each g	group completes
	By default, upgra	ade will pause after all g

Figure 4-9: Overall Groups Upgrade Order

4. Decide if Upgrade Coordinator should pause automatically and when:

• When an upgrade unit fails to upgrade – Upgrade pauses if any individual host upgrade fails. This selection allows admins to fix the error and resume the upgrade.

• After each group completes – Upgrade pauses after each host group finishes upgrading

Plan			
Overall group upgrade order	<ul> <li>Serial</li> </ul>	• Parallel	
Pause upgrade	When an upgr	rade unit fails to upgrade	
condition	After each gro	oup completes	
	By default, upgrade	e will pause after all groups a	re completed.

Figure 4-10: Pause Upgrade Conditions

5. Reorder host upgrade sequence inside groups

• Once a host inside a host group is selected, the ACTIONS menu allows to change it to a different group or to modify its upgrade order inside the current one (Reorder)

State: Enabled, Upgrade O	rder: Parallel		
🔅 ACTIONS 🗸			
Change Group	ID	IP Address	Details
Reorder	6380b10d	192.168.110.56	HYPERVISOR_VERSI
🗹 kvm-01	88ff4dc8	192.168.110.55	HYPERVISOR_VERSI

Figure 4-11: Changing Upgrade Sequence of one host



Alternatively, a "dotted icon" made of two columns of four periods each, will show up when hovering over the name of the host groups:

Group for new	ly added UBUNTUK	/M hosts
State: Disabled, Upgra	de Order: Parallel	
Upgrade Unit	ID	IP Address
kvm-02	6380b10d	192.168.110.56
kvm-01	88ff4dc8	192.168.110.55

#### Figure 4-12: Dotted Icon by Hosts

By clicking on them, allows to drag the corresponding host group out of his position, to drop it at a new one, highlighted by a green line with small green arrows at each end:

ate: Disabled, Upgrade (	Order: Parallel				
Upgrade Unit	ID	IP Address	Details	Upgrade Status	Progress
kvm-02	6380b10d	192.168.110.56	HYPERVISOR_VERSL.	Not Started	0%
kvm-01	88ff4dc8	192.168.110.55	HYPERVISOR_VERSL.	Not Started	0%
kvm-02	6380b10d	192.168.110.56	HYPERVISOR_VERSL.	Not Started	0%

Figure 4-13: Drag and Drop hosts

6. Reorder upgrade sequence between groups

• Once a host group is selected, the ACTIONS menu allows to modify its upgrade order related to all other groups (Reorder)

+ ADD 🖉 EDIT 🔟 DELETE	🕸 ACTIONS Y		
Group	Reorder	Upgrade Units	Upgrade Order within G
Group for newly added UBUNTU	Set State	2	Parallel
Group for compA	Set Opgrade Order	2	Serial

Figure 4-14: Modifying Upgrade Sequence between Host Groups

Note that Set Upgrade Order option allows to set either Serial or Parallel upgrade mode for the hosts inside the group, but it does not influence the position on which the group will be upgraded (related to all other groups).

Alternatively, a "dotted icon" made of two columns of four periods each, will show up when hovering over the name of the host groups:



+ ADD 🖉 EDIT 🔋	🗓 DELETE 🛛 🛞 ACTION	S ¥
Group	ID	Upgi
Group for compA	8353c19	
Group for newly ad	de d56d0aab	

Figure 4-15: Dotted Icon by Host Groups

Clicking on them, allows to drag the corresponding host group out of his position, to drop it at a new one, highlighted by a green line with small green arrows at each end:

Host Groups	LETE @ ACTIONS ~							
Group	ID	Upgrade Units		Upgrade Order within Grou	State	Upgrade Status	Progress	
Group for newly adde	d56dOaab		2	Parallel	Disabled	Not Started		0%
Group for compA	8353c19		2	Serial	Disabled	Not Started		0%
Group for newly adde_ t selected row	d56dOaab		2	Parallel	Disabled	Not Started		0%

Figure 4-16: Drag and Drop Host Groups

7. Enable/disable groups from upgrade plan

• Once a host group is selected, the *ACTIONS* menu allows to set its state as *Enabled* (hosts inside the group will be upgraded) or *Disabled* (hosts inside the group will not be upgraded).

ADD 🖉 EDIT 🗒 DELETE 🧔	ACTIONS -		1		
Group	Reorder	Upgrade Units		Upgrade Order within Gr	State
Group for newly added UBUNTU.	Set State	> Enabled	2	Parallel	Enabled
Crown for compA	Set Upgrade Order	Disabled	2	Serial	<ul> <li>Enabled</li> </ul>

Figure 4-17: Include/Exclude Host Groups from the Upgrade Plan

Once the required customizations are defined, the next step is to click on the start button for the upgrade to start.

Admins will be presented a warning message about the need of putting vSphere hosts into Maintenance Mode:

Hos	t Upgrade Prerequisites	×
?	VC managed ESX hosts with fully automated DRS will be autom maintenance mode during upgrade. Please ensure other ESX h maintenance mode manually, before starting the upgrade.	natically put in osts are put in
	CONTINUE	CANCEL

Figure 4-18: Host Upgrade Prerequisites message





Requirements are:

- With maintenance mode upgrade:
  - When using Compute Managers, vSphere hosts in clusters configured with fully automated DRS will be automatically put into maintenance mode, thus, no further action is required
  - vSphere hosts not managed by Computer Managers, registered with NSX need to be put into Maintenance Mode manually, before starting the upgrade

• With In-Place upgrade o There is no requirement to migrate the VMs or put the hosts into maintenance mode or similar. A short traffic disruption may happen during the upgrade process. KVM only have In-Place upgrade mode.

Once requirements are fulfilled, admins can click on *CONTINUE* to start hosts upgrade. The overall progress bar, and host group specific progress bars, will indicate the evolution of the upgrade process. Admins can also click on *PAUSE* at any time to request the upgrade to stop. This manual pause request will not pause the hosts currently been upgraded, it will pause the upgrade process only after the in-progress hosts upgrade is complete (either succeed or failed).

Once the upgrade is paused, admins can modify the settings of their upgrade plan, if they want to.

8. Run Post Check to verify everything is OK after the upgrade.

1. Bundle and Status 2. Edg	les	3. Hosts	4. Management Nodes					٢
Plan				Progres	5			
Upgrade order across groups	Sortal	O Parallel		Status	Successful	100%		
Pause upgrade condition	When an upp	trade unit fails to up	grade	Details				
	After each gr	roup completes						
	Bu default unerer	do will course office off	mouns are completed					
Host Groups	ETE 🖀 RUN P	OST CHECKS	ACTIONS ~					
Group Name	ID	Units	Upgrade Order within Group	State	Upgrade Mode	Upgrade Status	Progress	Post Check Status
Group for Validation-Clust	er-01 da04	c28 2	Serial	<ul> <li>Enabled</li> </ul>	Maintenance	Successful	100%	No lost(s) with issues
Group 1 for UBUNTUKVM	9a4dd	198 2	Parallel	<ul> <li>Enabled</li> </ul>	In-place	<ul> <li>Successful</li> </ul>	100%	No lost(s) with issues
COLUMNS   C REFRESH	Last Updated: a	minute ago					C 84	LCR NERT > 1-2 of 2 Groups
Do not power-off or reboot the nodes w	ihen upgrade is in prog	ress. They may be rebool	ted automatically as part of the upgrade pr	ocess.				BACK

**Note:** Upgrade Coordinator cannot proceed to the next step (i.e., Manager Upgrade) until all hosts are upgraded. Should there were issues preventing a successful upgrade of the Hosts, please contact VMware Support Services.

#### 4.1.4 Manager Node Upgrade

The last step on the upgrade sequence is upgrading the NSX Manager. As in the case of the Controllers, the only available option is to start the Manager upgrade.

NSX Manager is rebooted during the process, thus its UI becomes inaccessible for some time. Note: As a best practice, it is



recommended to ensure an update backup of the NSX Manager is available before starting its upgrade.

vm NSX-T					Q LI (	?)∽ admin	
Home Networking S	ecurity Inventory Tools System	n Advanced Netv	vorking & Security				
«	1. Bundle and Status 2. Edges	3. Hosts	4. Management Nodes				0
Overview Get Started Fabric Set Service Deployments CActive Directory	Progress Status A Not Started 0% Details Management Nodes	► START					
령 Users	Upgrade Unit	ID	IP Address	Upgrade Status	Progress		
🚔 Backup & Restore	sa-nsxmgr-01	af68d479	172.20.10.41	Not Started		0%	
📥 Upgrade							
恒, Migrate							
Licenses							
Certificates							
③ Support Bundle							
E Customer Program							
Enforcement Points							

Figure 4-19: NSX Manager Upgrade

## 4.2 NSX Manager Backup/Restore

#### 4.2.1 NSX Manager Backup

NSX includes the ability to backup and restore the Manager configuration, so that it can be recovered should it become inoperable for any reason. The NSX Manager stores the desired state for the virtual network. If it becomes inoperable, the data plane is not affected, but configuration changes cannot be made.

Backups are saved to a remote server using the SFTP protocol (SSH File Transfer Protocol). By design, the **NSX Manager is not** allowed to modify/delete existing backups on the destination server, thus, an automated task should be created on the server if deleting old backups and cleanup is required.

For better flexibility and ensuring that recent backups are always available, NSX offers the options to run manual and/or scheduled backups.

The Manager Backup comprises of three different types of backups, all of which happen automatically when scheduled configuration is selected:

- Node backups include the NSX Manager appliance configuration
- **Cluster backups** include the desired state of the virtual network

NSX Manager backup configuration is available under *System* > *Lifecycle Management* > *Backup*.



#### 🖆 Backup & Restore

ISX Configuration					
FTP Server	Port	Protocol	Directory Path	Schedule   Disab	led START BACKU
0.114.220.136 EDIT	22	SFTP	/var/tmp	At Interval Of 1 Hrs	DIT
✓ Last Backup Statu	s 🔹 Succi	essful			
Node		Successful		Cluster	Successful
Start Time		Monday, Octobe	er 5, 2020 at 10:23:34 PM GMT-04	I:00 Start Time	Monday, October 5, 2020 at 10:23:34 PM GMT-04:00
End Time		Monday, October 5, 2020 at 10:25:06 PM GMT-04:00		1:00 End Time	Monday, October 5, 2020 at 10:24:53 PM GMT-04:00
Backup History	Packup			Appliance EODN or IR Address	Applance II III D
<ul> <li>Backup History</li> <li>Date and Time of</li> </ul>	f Backup			Appliance FQDN or IP Address	RESTORE. Appliance UUID
Backup History     Date and Time of     Monday, Octob	f Backup ber 5, 2020 at	10:23:34 PM GMT-1	04:00	Appliance FQDN or IP Address 10.114.220.137	RESTORE Appliance UUID 17631d26-bfca-4c3a-9a49-44197c2e0555
Backup History     Date and Time of     Monday, Octob     Sunday, October	f Backup ber 5, 2020 at er 4, 2020 at 3	10:23:34 PM GMT-1 3:00:00 PM GMT-0	04:00	Appliance FQDN or IP Address 10.114.220.137 10.114.213.14	Appliance UUID         If7631d26-bfca-4c3a-9a49-44f97c2e0555         c9802d42-5420-91ef-a64d-27a7b3ef282c
<ul> <li>Backup History</li> <li>Date and Time o</li> <li>Monday, Octob</li> <li>Sunday, Octob</li> <li>Sunday, Septer</li> </ul>	f Backup Her 5, 2020 at er 4, 2020 at 3 mber 27, 2020	10:23:34 PM GMT- 3:00:00 PM GMT-C at 3:00:00 PM GM	04:00 94:00 41:00	Appliance FQDN or IP Address 10.114.220.137 10.114.213.14 10.114.213.14	Appliance UUID           17631d26-bfca-4c3a-9a49-44f97c2e0555           c9802d42-5420-91ef-a64d-27a7b3ef282c           c9802d42-5420-91ef-a64d-27a7b3ef282c
<ul> <li>Backup History</li> <li>Date and Time o</li> <li>Monday, Octob</li> <li>Sunday, Octob</li> <li>Sunday, Septer</li> <li>Sunday, Septer</li> <li>Sunday, Septer</li> </ul>	f Backup Ver 5, 2020 at er 4, 2020 at 3 nber 27, 2020 nber 20, 2020	10:23:34 PM GMT- 1:00:00 PM GMT-C 1 at 3:00:00 PM GM 1 at 3:00:00 PM GM	04:00 94:00 94:00 94:00 94:00 94:00	Appliance FQDN or IP Address 10.114.220.137 10.114.213.14 10.114.213.14 10.114.213.14	Appliance UUID           17631d26-bfca-4c3a-9a49-44f97c2e0555           c9802d42-5420-91ef-a64d-27a7b3ef282c           c9802d42-5420-91ef-a64d-27a7b3ef282c           c9802d42-5420-91ef-a64d-27a7b3ef282c           c9802d42-5420-91ef-a64d-27a7b3ef282c           c9802d42-5420-91ef-a64d-27a7b3ef282c

3.0.0.0.0.15946739-c9802d42-5420-91ef-a64d-27a7b3ef282c-10.114.213.14
backup-2020-05-22T03_20_18UTC
cluster_backup-c9802d42-5420-91ef-a64d-27a7b3ef282c-10.114.213.14-nsx-controller.tar
node_backup-c9802d42-5420-91ef-a64d-27a7b3ef282c-10.114.213.14.tar

Figure 4-20: NSX Manager Backups

**Note:** The backup file will be created with the IP address of the manager node where the backup is performed. So you need to make sure to HTTPS to the individual IP address of manager node when you run the backup instead of using the cluster VIP.

#### 4.2.2 NSX Manager Restore

Should the NSX Manager become inoperable, it can be recovered from a previous backup, if it exists.

A successful recovery requires the followings:

• The passphrase specified when the backup was created

• A new NSX Manager appliance, deployed with the same IP address or the same FQDN and software version than the one to be restored

**Note:** It is not supported to restore a backup on the same NSX Manager appliance where the backup was taken. Please see other important notes on the following link.

https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.0/administration/GUID-9749F04115E5-4662-85E7-756D4B071C17.html

Once the new Manager appliance is deployed, admins must navigate to *System > Tools > Utilities > Restore*, and fill out the required backup server configuration.



«	SUPPORT BUNDLE	BACKUP RESTORE UP	GRADE			
Dashboard						
Tools		Edit File Ser	ver Configuration	×		
B Firewall	1. CONFIGURATION 2. RE	STORE	5			1
Encryption	File Server Configuration	IP/Host*	192.168.130.151			(
Routing	IP/Host	Port*	22	\$		
DDI	Port 22 Protocol SF	Protocol	sftp			
Switching	Username Destination Directory					
Inventory	Available Backups	Username *	vmware			
Fabric	Backup File Time	Password		Node UUID		
System		Destination Director	ry* /backups			
rust						
onfiguration	COLUMNS   Ø REFRESH	H Last I			< BACK NEXT >	No Backu
tilities		SSH fingerprint * 0	v//WxVvu4xnGWHPVG6fUVaInnfzN+	+FJssje+UYtZQ		
sers						

Figure 4-21: Configuring NSX Manager Restore

NSX Manager reboots when restore is started. Once its GUI is responsive after reboot, log in and navigate to the Restore tab. If the hosts managed by the new NSX Manager are the same when the backup was taken, the restore process will proceed and finish successfully without further admin intervention:

SUPPORT BUNDLE	BACKUP	RESTORE	UPGRADE	
1. CONFIGURATION 2		TUS 3. RESTO	ORE COMPLETE	
Success: You have 1 St	JCCESS(S)			
Restore process finish	ed successfully.			
Status: • Succeeded				
Backup File Timestamp	9/27/2017, 2:28	3:26 AM PDT		
Restore Started At	9/27/2017, 2:40	0:25 AM PDT		
Restore Ended At	9/27/2017, 2:47	50 AM PDT		

Figure 4-22: Successful NSX Manager Restore

If the hosts managed by the new NSX Manager are different than the ones when the backup was taken, two things can happen:

1. Fabric nodes were deleted since the backup was taken – At some point the restore process will pause and ask the admin to manually add them.





Figure 4-23: Fabric nodes that failed to discover the NSX Manager

Once they are added to the new NSX Manager, the admin must select *I have finished all steps above* and click on *RESOLVE*. The restore process will resume and finish successfully.

Support Bundle	Backup	Restore	Upgrade
1. CONFIGURATION	2. RESTORE S	STATUS 3.	RESTORE COMPLETE
Success: You have 1     Restore process finit	Success(s)	y.	
Status: • Succeeded			
Backup File Timestamp	3/15/2018,	5:22:36 AM PD	т
Restore Started At	3/19/2018,	6:14:33 AM PD	r
Restore Ended At	3/19/2018,	6:33:12 AM PD1	r

Figure 4-24: Fabric nodes that failed to discover the NSX Manager

- Fabric nodes were added since the backup was taken the restore process will pause several times. On the first two
  pauses, the NSX Manager will ask the admin to run two different scripts, available in a specific directory of the nodes
  themselves:
  - 1. One will unregister the hosts as NSX Fabric Nodes
  - 2. The other will unregister the hosts as NSX Transport Nodes

Once the restore finishes successfully, the admin will need to add such nodes back to the new NSX Manager.



Suspended For	Manual Steps		Suspended Fo	or Manual Steps		×
Listing fabric nodes tha 1. For each of the hosts liste 2. Run /opt/vmware/nsx-cli/ 3. The typical reason for thi after a backup. After restori about this host. Running the restore process is complete ID	t require a reset during inventory reconciliation d.log in to the node with root access bin/scripts/reset_nsx_after_mp_restore.sh fabric_node situation is that you registered a host with the NSX Manager ng the backup, the NSX Manager no longer has information script tells the host that it is no longer registered. After the d, you can re-register the host IP Address	*	Listing transport nod 1. For each of the hosts is 2. Run /opt/vmware/nsx- 3. The typical reason for the backup, you made the information about the tra the restore process is co 4. Note: One or more VM after the restore. Therefore	es that require a reset during inven- sted, log in to the node with root access clifbily/sciptu/reset_nss_after_mc_restor this situation is that before the backup yo host a transport node. After restoring th insport node, Running the script tells the h mpleted_you can add the transport node is on these nodes may be attached to the ore, the VMs may lose network connectivity	tory reconciliation e.sh transport_node u registered a host as a fabric node, and after e backup, the NSX Manager no longer has ost that it is no longer a transport node. After again following logical switches that no longer exist y after the restore and the reset actions.	*
00296511	[192.168.110.53]		ID	IP Address	Description	
5d578a42	[192.168.110.54]		00296511	[192.168.110.53]	transport node ld: 0029fb09	
C BACK NEXT > 1-	2 of 2 records s above RESUME	*	5d578a42	[192.168.110.54]	transport node kt: 5d57b9ba	•

Figure 4-25: Fabric and Transport nodes that must be removed from the new NSX Manager

Then, the restore process will pause some more times to ask the admin confirmation before deleting the nodes from the NSX databases.

Suspended For	Manual Steps	× Suspended	For Manual Steps ×
Deleting transport nodes 1. Transport nodes associated the database 2. The typical reason for this completing the restore, the M these fabric nodes from the a	s from the database during inventory reco d with each of the fabric nodes listed will be dele situation is that the you deleted a host after back ISX Manager will delete the transport nodes asso tabbase.	onciliation A Deleting fabric no- ted from 1. Each of the fabric no- 1. Each of the fabric no- 1. Each of the fabric no- 2. The typical reason completing the restor database.	des from DB during inventory reconciliation nodes listed will be deleted from the database for this situation is that the you deleted a host after backup. After re, the NSX Manager will delete these fabric nodes from the
ID	IP Address	ID	IP Address
29acb068	[192.168.110.53, 10.10.20.53, f	29acb068	[192.168.110.53, 10.10.20.53, fe80::25_
dc63b607	[192.168.110.54, 10.10.20.54, f	dc63b607	[192.168.110.54, 10.10.20.54, fe80::25
( BACK NEXT ) 1-	t of 2 records	< BACK NEXT	> 1-2 of 2 records
I have finished all steps	above	I have finished all	II steps above
		-	
		RESUME	

Figure 4-26: Restore process asking the admin for confirmation before proceeding

Once all steps are taken, the process will resume and will eventually finish successfully.

estore Upgrade
TUS 3. RESTORE COMPLETE
6:30 AM PDT
6:30 AM PDT 33 AM PDT

Figure 4-27: NSX Manager restore finished successfully





## 4.3 Support Bundle

When dealing with IT solutions, it is sometimes required to open a support case with the vendor and get the support logs/bundles from different components.

NSX provides a central location to collect support bundles from registered cluster and fabric nodes, and to download those bundles to the admin station or to have them automatically uploaded to a file server.

Support Bundle central collection location is available under *System* > *Utilities* > *Support Bundle*. Admins can select an arbitrary number of NSX components from different nodes (i.e., managers, controllers, edges, hosts, public cloud gateways) and get the logs from them all automatically.

Admins can specify if they want to include core and audit logs, and if they want to get all available logs or only the ones from a specific number of days.

Note: Core files and audit logs may contain sensitive information such as passwords or encryption keys.



Figure 4-28: Central collection of logs

When the option *Upload bundle to remote file server* is selected, the admin is requested to add details of such a remote file server.

og age (days)	2	\$			
ore files and audit logs	Core files contain s memory at that time	ystem Information ie). If you choose to	and all information stored in memory a send the support bundle to VMware,	t the time of the dump (this may include confidential, sensit it will be used to provide you with support, fix problems an	lve or perso d Improve t
pload bundle to remote	file server				
IP/Host name*	192.168.130.151		Username*	vmware	
Port	22	\$	Password*		
Protocol	O SCP () S	SFTP	SSH fingerprint*	SHA256:YPb//WxVvu4x	
Destination path*	/tmp/supportb	undle			
Manager upload	Disable	d		10	
	upload the bundle	to the destination s	erver. Note: For ESX Hosts, support bi	anager, when disabled, the target hodes will directly undle upload is always done by the NSX manager.	

Figure 4-29: Configuring support bundle to be uploaded to a remote file server

Once the bundle collection process concludes, there is no additional action required from the admin since the bundle is automatically uploaded to the server.



SUPPORT BUND	LE BACKUP RESTORE	UPGRADE		
	2. STATUS			
Task started at	9/27/2017, 8:44:29 AM by admin			
Task ended at	9/27/2017, 9:03:00 AM			
Destination file server	192.168.130.151			
Destination path	/tmp/supportbundle			
Status	Completed 100%	NEW BUNDLE REQUEST		
Details				
Show: ALL 1	SUCCESSFUL O FAILED			
Node		ID	Status	Details
nsxmgr-01a		422ecec5	Successful	nsx_manager_422ee699-f4d1-5216-e6ed-ea9e3b4fcec5_20170927_154430.tgz

*Figure 4-30: Support bundle uploaded to a remote file server* 

If no remote file server is configured, the admin must click on the *DOWNLOAD* button to have the bundle download into his/her laptop/station:

SUPPORT BUN	DLE BACKUP RESTOR	E UPGRADE		
	E 2. STATUS			
Task started at	9/27/2017, 9:04:28 AM by admin			
Task ended at	9/27/2017, 9:22:41 AM			
Status	Completed 100%	DOWNLOAD NEW BUI	NDLE REQUEST	
Details				
Show: ALL	1 SUCCESSFUL O FAILED			
Mada		ID	Status	Details
Node				

Figure 4-31: Download Support bundle to management laptop/station

## 4.4 Work with Services on NSX Managers

#### 4.4.1 Use CLI to enable/disable services on the NSX manager

To start / stop a service on NSX manager, use NSX CLI

Start service Stop service

NSX-T 3.0: Operation Guide



nsx-mgr-137> start service		
applianceproxy	Applianceproxy service	
async_replicator	Async_replicator service	
cluster_manager	Cluster manager service	
cm-inventory	CM-inventory service	
controller	Controller service	
http	HTTP service	
idps-reporting	Idps-reporting service	
install-upgrade	Install-upgrade service	
intelligence-upgrade-coordinator	Intelligence-upgrade-coordinator service	
liagent	Log Insight service	
manager	Manager service	
mgmt-plane-bus	Management Plane Bus service	
migration-coordinator	Migration-coordinator service	
node-stats	Node stats service	
nsx-message-bus	NSX Message Bus service (deprecated since NSX 3.0.0)	
nsx-platform-client	Nsx-platform-client service	
nsx-upgrade-agent	NSX Upgrade Agent service	
ntp	NTP service	
policy	Policy service	
search	Search service	
snmp	SNMP service	
ssh	SSH service	
syslog	Syslog service	
telemetry	Telemetry service	
ui-service	UI service	
	Fig.	ure 4-32

Start service CLI

## To set start a service on boot, use NSX CLI: set service

nsx-mgr-137> set servi	ce
async_replicator	NSX async replicator service
controller	Controller service
http	HTTP service
install-upgrade	install-upgrade service
manager	NSX manager service
nsx-exporter	NSX exporter service
nsx-platform-client	NSX platform client service
ntp	NTP service
policy	Policy
snmp	SNMP service
ssh	SSH service

Figure 4-33 Set service CLI

## 4.4.2 Use UI to configure centralized node configuration

Syslog server and SNMP server can be configured use centralized node configuration. The configuration will be applied to all NSX managers.





vm NSX-T				ΟŢ	@~ 🕻	admin ~
Home Networking See	curity Inventory Plan & Troubleshoot	System			POLIC	Y MANAGER 1
*	Uplink Profiles NIOC Profiles	Edge Cluster Profiles	Configuration	Transport N	lode Profiles	Node Profiles
<ul> <li>System Overview</li> <li>Configuration         <ul> <li>Appliances</li> <li>Location Manager</li> <li>Quick Start</li> <li>Fabric</li> <li>Fabric</li> <li>Nodes</li> </ul> </li> <li>Profiles</li> <li>Transport Zones</li> </ul>	Name All NSX Nodes	All NSX Nodes       Overview       > Summary       EDIT       Syslog Servers       + ADD       Server       10.114.220.225	ETE Port 514	Protocol	Log	X
Compute Managers Settings <sup>of</sup> Service Deployments <sup>in</sup> Identity Firewall AD Lifecycle Management <sup>in</sup> Backup & Restore <sup>in</sup> Upgrade <sup>in</sup> Manata		SNMP Polling > v2c > v3 SNMP Traps > v2c > v3 SNMP Traps				
Settings	1-1/1	Authentication Protocol Privacy Protocol	SHA1 AES128			

Figure 4-34 Centralized Node Configuration





## 5 Troubleshooting Tools & Case Study

This section describes the following tools:

- 1. NSX Alarm / Event
- 2. Logging, vRealize Log Insight and Splunk
- 3. Port Connection Tool (available on Manager UI) and Traceflow
- 4. IPFIX
- 5. Port Mirroring (Local SPAN, L3 SPAN, Packet Captures)

## 5.1 NSX Alarm / Event

This section outlines NSX alarm/event.



Starting from NSX-T 3.0, NSX can alert as to alarming conditions by using the Alarms/Events framework. Each individual NSX component constantly scans and monitors their predefined alarm conditions. When the alarm condition occurs, the system emits event. The events will be sent to the NSX manager. The alarm instances can be viewed via the manager UI and can also be queried via NSX API. If Watchers are registered with NSX manager and they will receive notifications of alarms.

NSX can also integrate with existing monitoring infrastructure by sending out events via log messages to syslog or traps to SNMP server when an alarm condition occurs.

NSX-manager, Transport Node, Edge node, NCP and services like load balancer, firewall and VPN are the components that currently support the Alarm/Event framework.

## 5.1.2 Monitoring NSX with Alarm Dashboard

This section covers monitoring NSX with Alarm Dashboard.



SX-T					ς Δ	\	admin
Networking Security Inven	tory Plan & Troubleshoot S	ystem				POLICY	MANAGER
Overview Alarms () Monitor	ing Dashboards 🗸						0
larms Alarm Definitions						C REFRE	SH
Active Alarms	То	p Features with the Mos	t Alarms	Top Event	s by Occurrence		T
4 Open Ackn	O owledged/Suppressed	8 6 Infoastructure Load Ridancer 3 Communication	6 4 4 Winner Trigs Haath Mongar Irealty	10 0 Intrati Comm	Ballion Parvicon Load Balover Management	3 Transport Node Healt.	
ACTION -				EXPAN	D ALL Filter by Name. Path an	nd more	=
Feature	Event Type	Node	Entity Name	Severity	Last Reported Time	Alarm State	
Password Management	Password Expiration Approaching	Edge-1-148	Edge-1-148	. Medium	Apr 13, 2020, 10:43:08 AM	Open	
Transport Node Health	NVDS Uplink Down			• Medium	Apr 13, 2020, 10:29:00 AM	Open	
> Infrastructure Communication	Edge Tunnels Down	edge-2-158	edge-2-158	Critical	Apr 9, 2020, 5:38:17 PM	Resolved	
Infrastructure Communication	Edge Tunnels Down	Edge-1-148	Edge-1-148	• Critical	Apr 9, 2020, 5:38:16 PM	Resolved	
Load Balancer  Load Balancer	Edge Health	Edge CP	J Usage High Edge-1-148		Edge-1-148	e Medium	Apr 22, 2020, 1 AM
Coad Balancer	Description	The CPU usad	e on Edge node 4702e650-469	c-4a9c-9798-510	d1b010541b has reached 20% v	which is at or abo	ive the high threshol
> Infrastructure Communicat	Recommended Activ	on Please review	the configuration, running services to other Edge podes for t	es and sizing of	f this Edge node. Consider adju	usting the Edge a	ppliance form facto
intrastructure Communicat	First Reported	Apr 22, 2020	11:10:27 AM	and approximate the			
C REFRESH	Resolved	Apr 22, 2020	11:11:27 AM by system				

-----

The alarm dashboard shows all the alarm instances. From here, users can see which node generates the alarm, the severity of the alarm, last time the alarm being reported, and the state of the alarm.

Also, users can take action to acknowledge, resolve and suppress an alarm instance.

I want to mention that acknowledge and resolve will not make the alarm go away if the alarm condition still exists. Only when the real issue is resolved, the alarm can be in resolve state.

## 5.1.3 Pre-defined Alarm / Event in NSX Manager

This section outlines pre-defined Alarm/Event in the NXS Manager.

NSX-	Т					QĹ	∫ ?∽ ad
	Ne	tworking Security I	nventory Plan & Troubleshoot System				POLICY M
Over	view	Alarms 🜖 🛛 Moni	toring Dashboards  ~				
Alarm	S	Alarm Definitions			EXPAND ALL	Filter by Name, Path	and more
		Feature	Event Type	Severity	Enabled	Create Alarms	Create SNMP Trap
	>	Alarm Management	Alarm Service Overloaded	Critical	Yes	Yes	Yes
1	>	Alarm Management	Heavy Volume Of Alarms	• Critical	Yes	Yes	Yes
	E	dit icates	Certificate Expiration Approaching	• Medium	Yes	Yes	Yes
		Description	A certificate is approaching expiration.				
		SNMP OID For Event true	1.3.6.1.4.1.6876.120.1.0.3.0.1	Threshold	30 D		
		SNMP OID For Event false	1.3.6.1.4.1.6876.120.1.0.3.0.2	Sensitivity(%)	100 @		
-	>	Certificates	Certificate Expired	Critical	Yes	Yes	Yes
1	>	Certificates	Certificate Is About To Expire	• High	Yes	Yes	Yes
1	>	Cni Health	Hyperbus Manager Connection Down	• Medium	Yes	Yes	Yes
-	>	DHCP	Pool Lease Allocation Failed	• High	Yes	Yes	Yes
1	>	DHCP	Pool Overloaded	• Medium	No	Yes	Yes
1	>	Distributed Firewall	DFW CPU Usage Very High	Critical	Yes	Yes	Yes
:	>	Distributed Firewall	DFW Memory Usage Very High	Critical	Yes	Yes	Yes
		DNC		- I limb	Mere	Mee	1422

All the pre-defined alarms are listed under the Alarm definitions on the Manager UI.

More details of each alarm can be found here on the following link.



https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.0/administration/GUID-23FB78F5E0AF-40E3-9450-0B957B374383.html

## 5.1.4 Configuring Alarm / Event behavior

The alarm can be enabled or disabled which means the alarm condition will be monitored or not. Creating alarm means whether an alarm is going to be created when the alarm condition occurs. You can enable/disable SNMP traps. For some alarm, you can change threshold and sensitivity here.



## 5.2 Logging, vRealize Log Insight and Splunk

This section documents logging, vRealize Log Insight and Splunk.

## 5.2.1 Logging

The logging of NSX appliance and NSX components on KVM host follows the RFC 5424 format. The logging of NSX components running on ESXi hosts uses ESXi logging format.

RFC 5424 defines the following format for log messages as demonstrated below. < facility \* 8 + severity > version UTC-TZ hostname APP-NAME procid MSGID [structured-data] msg





## Log Message Decode (RFC5424)

180 = Facility*8+ Priority NSX Facility uses Local6(22) 180->WARNING 1: Version 1 Timestamp in UTC-TZ <180>1 2010-00 2011 20 04 4 Subcomp = "manager"] com.	Hostnam Hostnam nsx-mg vmware.nsx. keepalive rtt	r-01 NSX 6334 [nsx@687 rpc.transport.netty.KeepA	b nsx-ma nspresents nare 6 comp="nsx-ma liveFsm@7683896 ot flushed	o EMERGENCE 176 1 ALERT 177 2 CRITICAL 178 3 ERROR 179 4 WARNING 180 5 NOTICE 181 6 INFORMATIONAL 182 7 DEBUG 183 mager" level="WARN" e8: Could not update
		Actual Message		
	Component Error Code	Code	Meaning	Recommended Action
C	CP2010130	BROKER_CONFIG_FILE_IS_NOT_PROVIDE D	Broker file is absent	1.Check CCP-MP connection status 2.Verify if bootstrap.config is present
L	CP00021	ERR_MEMORY_ALLOC_FAILED	Cfgagent runs out of memory.	Need to check why the memory runs out. Need to check whether it needs to enlarge the reserved memory size.

Which produces a sample log message like the following:

<187>1 2016-03-15T22:53:00.114Z nsx-manager NSX - SYSTEM [nsx@6876 comp="nsx-manager" errorCode="MP4039" subcomp="manager"] Connection verification failed for broker '10.160.108.196'. Marking broker unhealthy.

In NSX, the structured-data piece of every message includes the component (i.e., comp) and subcomponent (i.e., subcomp) information to help identify the source of the message.

NSX produces regular logs and audit logs (i.e., facility local6, which has a numerical value of

22). Also, all API calls trigger an audit log. The long audit logs split into multiple pieces. You can filter the logs with splitID to see all the pieces for the same log message. Here is an example.



NSX logs are stored in the directory /var/log, on all NSX appliances, ESXi hosts and KVM hosts.

There are several ways to access NSX logs:

1. When logged in as admin on the NSX appliances - log messages can be accessed with the following CLI command





### get log-file <auth.log | http.log | kern.log | manager.log | node-mgmt.log | syslog>

- 2. **On hosts and when logged in as root on the NSX appliances** log messages are available on the */var/log/* directory. There are multiple log files available and Linux commands like *tac*, *tail*, *grep* or *more* can be used.
- 3. **Configuring log forwarding to a remote syslog server** Remote logging is supported on NSX Manager, NSX Controller, NSX Edge, and hypervisors. It must be configured on each node individually. Be aware that, as previously stated, facilities *local6* must be included to have relevant NSX log messages forwarded.

The following command will forward all *INFO* level logs, which will be fine for typical NSX deployments: **set logging-server** <**SERVER-IP-ADDRESS**> **proto udp level info** 

ESXi and KVM hosts require different configuration procedures. Please check the NSX-T Administration Guide for further details about NSX logs.

#### 4. Configuring log filter

The messages sent to remote collector can be filtered, here is an example: set logging-server" command with options including level, facility, messageid, and structureddata

Nsx-mgr-01> set logging-server 1.1.1.1 proto udp level warning facility local6 messageid switching structured-data audit="true",comp="nsx-manager"

#### Notes:

- 1. Logging needs to be configured individually on each device
- 2. Remote logging level should be higher (number is smaller) than the local logging level
- 3. That not all process/daemons currently support a CLI to change logging level, but most of them do

### 5. Important logs:

get cluster status (nsxcli)	get services (nsxcli)	get log-file (nsxcli)	login as root (Linux)
DATASTORE	datastore		/var/log/corfu/corfu.9000.log
CLUSTER_BOOT_MANAGER	cluster_manager		/var/log/cbm/cbm.log
CONTROLLER	controller		/var/log/cloudnet/nsx-ccp.log
MANAGER	manager	manager.log	/var/log/proton/nsxapi.log
POLICY	policy	policy.log	/var/log/policy/policy.log
HTTPS	http	http.log	/var/log/proxy/reserve-proxy.log

## NSX audit log /var/log/nsx-audit.log

Overall log	
/var/log/syslog	

Normally the user only needs to look at the syslog. Important messages from individual logs will be in syslog. Additional information might be available in individual logs. The "comp" and "subcomp" fields indicate the corresponding individual log,



For example, this message is in the syslog,

<179>1 2020-10-06T10:50:00.262-04:00 nsx-mgr-137 NSX 14066 POLICY [nsx@6876 comp="nsx-manager" errorCode="MP600" level= "ERROR" subcomp="policy"] Error retrieving runtime status for sections: [f3988e17-5470-4be6-ab42-bca834597f63, 8af236fd -ea5d-4139-981a-93ee54bf8b57, 4e6b562d-6924-4b77-915d-9c996750e145, 193a1928-3e95-4e06-b85b-1419a22a0716, ff1d80a6-f7b0 -4104-9bc9-7fc29f2dc82f]

The subcomp is policy, you can go to policy.log to find more information in case there's a need.

2020-10-06110:50:00.2332 ERROR populateRealizedStatelaskExecutor-27 FirewallNsxTRestUtils - POLICY [nsx@68/6 comp="nsx-manager" errorCode="
MP600" level="ERROR" subcomp="policy"] Error retrieving runtime status for sections: [f3988e17-5470-4be6-ab42-bca834597f63, 8af236fd-ea5d-4
139-981a-93ee54bf8b57, 4e6b562d-6924-4b77-915d-9c996750e145, 193a1928-3e95-4e06-b85b-1419a22a0716, ff1d80a6-f7b0-4104-9bc9-7fc29f2dc82f]
2020-10-06T10:50:00.233Z WARN populateRealizedStateTaskExecutor-27 FirewallBaseProviderNsxT - POLICY [nsx@6876 comp="nsx-manager" level="W
ARNING" subcomp="policy"] Due to error in retrieving the runtime status of sections, skipping this batch [f3988e17-5470-4be6-ab42-bca834597
f63, 8af236fd-ea5d-4139-981a-93ee54bf8b57, 4e6b562d-6924-4b77-915d-9c996750e145, 193a1928-3e95-4e06-b85b-1419a22a0716, ff1d80a6-f7b0-4104-9
bc9-7fc29f2dc82f].

## 5.2.2 vRealize Log Insight

VMware provides an NSX-T Log Insight Content Pack that collects, consolidates and correlates NSXT information that is then displayed in vRealize Log Insight in an intuitive and easy-to-consume. The Content Pack includes multiple widgets and dashboards related to the different NSX-T networking services, including infrastructure, switching, routing, distributed firewall, DHCP and backup.

As a sample, the screenshot below shows traffic patterns through the distributed firewall.



Figure 5-1: vRealize Log Insight NSX-T Distributed Firewall Traffic

Users can create customize dashboard to monitor the pre-defined events.





vm Log Insight	Dashboards Interactive Analytics	💄 admin 📃
Custom Dashboards <sup>V</sup> My Dashboards Critical NSX Alerts <sup>Shared</sup> Dashboards	Custom time range         6/1/2020, 00:00:00.000         7/20/2020, 10:17:32.989         C           Display legend on all widgets ①            C           + ADD FILTER	۵.
Content Pack Dashboards Content Pack Dashboards Content Pack Dashboards VMware - NSX-T VMware - vRops 6.7+ VMware - vSAN VMware - vSphere	Node Down	Jul 13
	2 0 Jun 1 Jun 15 Jun 29 Jul 13	

Log Insight Content Pack also has built-in alerts which can be configured to send out notification via email.

Vm NSX	Version: Author: Website: Namespace: Description:	e - NS 3.9 VMware, In http://www com.vmwar The NSX-T	C. ymware.com re.nsxt Log Insight content pack provides health status Expand	
Dashboards	Queries	Alerts	Agent Groups Extracted Fields	
Alerts				
Alert Name			Notes	Recommendation
SysCpuUsag	e O		CPU usage is above 95% for more than 10 minutes.	N/A
SysMemUsa	ge O		Memory usage is above 95% for more than 10 minutes.	N/A
SysDiskUsag	ie O		Disk usage for one or more partitions is above 89% for more than 10 minutes.	N/A
PasswordExp	biry O		Password for appliance user account is about to expire or expired.	N/A
CertificateEx	piry O		One or more CA signed certificate is expired.	N/A
ClusterNode	Status 🔘		Local edge cluster node is down.	N/A
BackupFailu	re O		NSX scheduled backup operation failed.	N/A
VipLeadersh	ip O		NSX Management cluster VIP is down.	N/A
ApiRateLimit			Client API reached 80% of the configured threshold.	N/A
CorfuQuorur	nLost 🔘		Two nodes went down in the cluster and lost corfu quorum.	N/A



## **ClusterFailoverStatus**



loginsight@example.com <loginsight@example.com> To: • Jing Shi

This alert is about your Log Insight installation on https://10.114.220.225/

Hi,

Log Insight found the following 1 event matching the criteria for alert "ClusterFailoverStatus":

```
2020-07-17T21:05:38.564318+00:00 Edge7-141 NSX 16 FABRIC [nsx@6876 comp="nsx-edge" subcomp="nsx-edge-
nsxa.ha_cluster" level="WARN" eventId="vmwNSXClusterFailoverStatus"]
{"event_state":1,"event_external_reason":"Service router switches over from Active to Down.
","event_src_comp_id":"f32ed045-8ad6-40fa-9eb5-0130452f3b43","event_sources":{"id":"38d2756e-c8c4-435f-a6b9-
acee2493cldl","router_id":"ec4e0426-198c-417a-ab17-b17365d3ladl"}}
```

Friday, July 17, 2020 at 5:09 PM

Additional notes for this alert:

SR high availability state changed or active/standby services failover.

Note: To avoid raising duplicate alerts, this alert will now be snoozed for the next 5 minutes (the search period for this alert).

For more details, please view the search results.

To make changes to this alert, please visit the alert page.

A complete list of pre-defined alerts can be found here:

https://docs-staging.vmware.com/en/draft/VMware-NSX-T-Data-

Center/3.0/administration/GUID-8E3CA63B-71F8-4F47-88A6-DC5FA714DE8B.html

#### 5.2.3 Splunk

VMware also provides a VMware-supported Splunk app for NSX-T. It is available at <u>https://my.vmware.com/</u>. Once on the NSX-T Data Center product page, navigate to the Drivers & Tools tab:

)0	wnload	VMware NSX-T Data Center			
elect	Version:	VMware NSX-T Data Center is our next generation product that provides a scalable network virtualization and micro-segmentation pla hypervised environments, container deployments and native workloads running in public doud environments. Customers who have purchased VMware NSX-T Data Center can download their relevant instalation package from the product down	atform for multi-	Product Resources	
		Read More		Product Info	
				Documentation	
				Community	
Proc	duct Downloads	Drivers & Tools Open Source Custom ISOs Release Date			
Proc	Driver / Tool	Drivers & Tools Open Source Custom ISOs Release Date			
Proc	duct Downloads Driver / Tool NSX Contained	Drivers & Tools Open Source Custom ISOs Release Date r Plugin			
Proc	duct Downloads Driver / Tool NSX Container VMware NSX-1	Drivers & Tools Open Source Custom ISOs Release Date r Plugin T Data Center OpenStack Neutron Plugin			
Proc	duct Downloads Driver / Tool NSX Container VMware NSX-1 VMware NSX-1	Drivers & Tools Open Source Custom ISOs			
Proc > > >	Driver / Tool NSX Containe VMware NSX-1 VMware NSX-1	Drivers & Tools         Open Source         Custom ISOs           Release Date           ar Plugin           T Data Center OpenStack Neutron Plugin           T Data Center Terraform Provider           T Data Center App for Splunk			
Proc > >	Driver / Tool NSX Containe VMware NSX-1 VMware NSX-1 VMware NSX-1 VMware NSX-1	Drivers & Tools     Open Source     Custom ISOs       Rolesse Date       Rolesse Date       Tolas Center OpenStack Neutron Plugin       T Data Center OpenStack Neutron Plugin       T Data Center App for Splunk       T Data Center App for Splunk       2018-08-05		Go to Downloads	

Figure 5-2: Downloading VMware supported Splunk app for NSX-T

It includes the same widgets and dashboards than the NSX-T Log Insight Content Pack.



NSX-T-Content Pack Dashboard The NSX-T Log insight content pack provides health status dashboards for the logical switching and routing, distribu- your NIX infrastructure.	ted firewall, and DHCP components	that make up the NEX infrastructure. It also provides key sudt logs for tracking create, add and delete changes to
All time v Submit		
NSX - Infrastructure NSX - Audit - Overview NSX - Logical Switch - Overview NSX - Logical Router - Ov	erview NSX - Distributed Firewa	I - Overview NSX - Distributed Firewall - Traffic NSX - DHCP - Overview
NSX Manager : Communication Errors		Transport Node - NSX Manager : Communication Errors
Count of events over time grouped by hostname		Count of events over time grouped by hostname
500		10 200
250	10.160.130.172 10.161.248.51 10.192.159.216 ank%-simanager	
Thu Jul 13 Thu Jul 20 Thu Jul 27 Thu Aug 3 Thu Aug 10 2017	ankiis-ns7-1-edge	Mon Jul 27 2010/Her 2100/Her 2100/Her 200/Her 2017 
Transport Node - Controller : Communication Errors		Controller : Communication Errors
Count of events over time grouped by hostname		Count of events over time grouped by hostname
No results found.		No results found.
- Chathy dan Ba Errors .	<1m ago	Other Errors
Count of events over time grouped by hostname		Count of events over time grouped by hostname
4 2 Thu Jul 13 Thu Jul 20 Thu Jul 27 Thu Aug 3 Thu Aug 3 Thu Aug 1 Thu Aug 3 Thu Aug 3 Th	10.160.130.172 10.161.248.51	N 125 330.17 PM 7 M 14 2017 Time
_ume		_ume

Figure 5-3: NSX-T Splunk app NSX-T Infrastructure dashboards

## 5.2.4 Logging recommendation

If Log Insight is used as the logging server, it's recommended to use protocol "li" or "li-tls" since they are optimized for transfer the log messages to the Log Insight server.

### 5.2.4.1 Logging with Protocol li-tls:

Notes: If Log Insight doesn't have a signed CA, this is an example on how to use OpenSSL on the NSX manager appliance to prepare for the certificate for Lab purpose only.

- i) Private key for CA
- ii) CA certificate (root certificate) iii) Private key for LogInsight server iv) Certificate for LogInsight server

Example showing the step to configure li-tls:

- 1. On NSX manager, change to directory /image/vmware/nsx/file-store
- 2. Create the private key for CA openssl genrsa -out ca\_private.key 4096
- 3. Create the CA certificate (root certificate) openssl req -new -key ca private.key -x509 -out ca.crt -days 3650
- 4. Create private key and certificate request for LogInsight server openssI req -new -nodes -newkey rsa:4096 -keyout Ll.key out Ll.req
- 5. Sign the certificate request for LogInsight server openssl x509 -req -in Ll.req -CA ca.crt -CAkey ca\_private.key -CAcreateserial -out Ll.crt -days 3650 f. Put key and crt into pem file cat Ll.key Ll.crt ca.crt > Ll.pem

g. To configure the server certificate on Log Insight, go to Administration  $\rightarrow$  SSL and upload a new certificate file (LI.pem)



vm Log Insight	Dashboards Interactive Analytics	💄 admin 🚍
Management System Monitor Cluster Access Control User Alerts Hosts Agents Event Forwarding License Certificates Integration vSphere vRealize Operations Configuration General Time Authentication SMTP Archiving	SSL     Certificate Information       Custor     Owner:       Custor     Cuality       State Or Province CA       Cuality     PA       Organization     UNMware       Organization     UNMware       Organization     UNMware       Country     US       State Or Province CA     Locality       Locality     PA       Country     US       Country     US       Locality     PA       Country     US       Locality     PA       Corganization     Mware       Organization     Organization       Locality     PA       Organization     Mware       Organization     Mware       Organization     Mware       Organization     Mware       Organization     Mware       Organization     Mware       Organization     Mware <td></td>	

To configure logging-server with li-tls:

nsx-mgr-137> set logging-server 10.114.220.225:9543 proto li-tls level info serverca ca.crt

## 5.2.4.2 Logging with Protocol li-tls:

# 1) Notes: If Log Insight doesn't have a signed CA, this is an example on how to use XCA to prepare for the certificate for Lab purpose only.

To download XCA tool: https://hohnstaedt.de/xca/index.php/download

Detailed manual is available at https://hohnstaedt.de/xca/index.php/documentation/manual

- 1. In XCA create a new database at Files  $\rightarrow$  New DataBase. If a database is already created, open it at Files  $\rightarrow$  Open DataBase.
- 2. In the Private Keys tab, create a Private key by clicking "New Key" and fill the required information.





Pivate Keys       Certificate signing requests       Certificate in the rew key and select the desired keyste         Name       A Certificate and Key management       Import PFX (PKCS#12)         Show Details       Bit         Regering       Carcel         Keysize       2048 bit         Remember as default       Certificate signing requests         Certificate and Key management       Delete         Keysize       2048 bit         Remember as default       Certificate and Key management         Certificate and Key management       Delete         Database: /Users/shil/(crt_uingLab.xdb       Search		000		xc	ertificate	and Key manage	ement
Internal name       Type       Size       Use       Password       New Key         K Certificate and Key management       Import       Import <th></th> <th></th> <th>Private Keys</th> <th>Certificate signin</th> <th>ig request</th> <th>certificate:</th> <th>s Templates Revocation lists</th>			Private Keys	Certificate signin	ig request	certificate:	s Templates Revocation lists
X Certificate and Key management		Inter	nal name 🔺 🔤	/pe Size	Use	Password	New Key
New Key       Import         Picy register       Import         Key Vyge       RSA         Key vyge       <		X Certificate and H	key management				Export
New Key       Import PFX (PKCS#12)         Piese give a name to the new key and select the desired keysize       Show Details         Name       Ckey         Keysize       2048 bit         Remember as default       Create         Database: /Users/shij/ort_JingLab.xdb       Search         X Certificate and Key management       Frivate Keys         Private Keys       Certificate signing requests       Certificates         Thermal name       Type       Size       Use         CA_key       RSA       2048 bit       0 Common         NSX-mgr157_key       RSA       2048 bit       0 Common         MSX-mgr157_key       RSA       2048 bit       0 Common	New Key			is			Import
We properties       Show Details         Name       CA_key         Key type       RSA         Remember as default       Cancel         Database:       // Users/shij/crt_lingLab.xdb         Sarch       X Certificate and Key management         Private       Key S         Certificate signing requests       Certificates         Internal name       Type       Size         Ligerver_key       RSA       2048       bit       0         Miternal name       Type       Size       Use       Passworn         Key Key       RSA       2048       bit       0       Common         MSX-mgr157_key       RSA       2048       bit       0       Common         Mont       NSX-mgr157_key       RSA       2048       bit       0       Common         Mont       NSX-mgr157_key       RSA       2048       bit       0       Common         Mont       Show Details       Delete       Delete <th>New Key</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>Import PFX (PKCS#12)</th>	New Key						Import PFX (PKCS#12)
Name       Ca.key         Keysize       2048 bit         Remember as default       Cencel         Database:       ////////////////////////////////////	Key properties	name to the new key	and select the des	ared keysize			Show Details
Keytype       RSA       Reversize       2048 bit       Reversize       Reversize       2048 bit       Reversize       Reverereversize       Reversize	Name	CA_key					Delete
Keysize       2048 bit         Remember as default       Cancel         Cancel       Creato         Database: /Users/shiji/crt_JingLab.xdb       Search         X Certificate and Key management       X Certificate signing requests         Private Keys       Certificate signing requests         Cach_key       RSA         2048       Dit         L1_server_key       RSA         2048       Dit         NSX-mgr157_key       RSA         2048       Dit         0       Common         Kport       Import         Monor       Show Details         Delete       Delete	Keytype	RSA		0			
Remember as default       Cancel         Cancel       Create         Database: /Users/shilj/crt_JingLab.xdb       Search         X Certificate and Key management       X Certificate signing requests         Private Keys       Certificate signing requests       Certificates         Internal name       Type       Size       Use         CA_key       RSA       2048       bit       1         CA_key       RSA       2048       bit       0       Common         LI_server_key       RSA       2048       bit       0       Common         NSX-mgr157_key       RSA       2048       bit       0       Common         NSX-mgr157_key       RSA       2048       bit       0       Common         Import       PFX (PKCS#12)       Show Details       Delete	Keysize	2048 bit		<b>_</b>			
Cancel       Create         Database: /Users/shilj/crt_JingLab.xdb       Search         X Certificate and Key management       X Certificate signing requests         Private Keys       Certificate signing requests       Certificates         Internal name       Type       Size       Use         CA_key       RSA       2048       bit       1         L1_server_key       RSA       2048       bit       0       Common         NSX-mgr157_key       RSA       2048       bit       0       Common         Mort       NSX-mgr157_key       RSA       2048       bit       0       Common         Mort       NSX-mgr157_key       RSA       2048       bit       0       Common         Mort       PFX (PKCS#12)       Show Details       Delete	Remember	as default					
Database: /Users/shiji/crt_lingLab.xdb       Search         X Certificate and Key management <ul> <li>Private Keys</li> <li>Certificate signing requests</li> <li>Certificates</li> <li>Templates</li> <li>Revocation lists</li> </ul> Internal name       Type       Size       Use       Passwort         CA_key       RSA       2048       bit       1       Common         L1_server_key       RSA       2048       bit       0       Common       Export         NSX-mgr157_key       RSA       2048       bit       0       Common       Import         Import       Import       Import PFX (PKCS#12)       Show Details       Delete       Delete			Cancel	Create			
Database: /Users/shlij/crt_JingLab.xdb       Search         X Certificate and Key management       X Certificate signing requests       Certificates       Templates       Revocation lists         Internal name       Type       Size       Use       Passwort       New Key         L1_server_key       RSA       2048       bit       0       Common       Export         NSX-mgr157_key       RSA       2048       bit       0       Common       Import         MSX-mgr157_key       RSA       2048       bit       0       Common       Export         Show Details       Delete       Delete       Delete       Delete       Delete							
New Key       New Key         LI_server_key       RSA       2048       Details         NSX-mgr157_key       RSA       2048       Details         Delete       Delete       Delete	1.1						
Private Keys       Certificate signing requests       Certificates       Templates       Revocation lists         Internal name       ^       Type       Size       Use       Passwor         CA_key       RSA       2048 bit       1       Common       New Key         LI_server_key       RSA       2048 bit       0       Common       Export         NSX-mgr157_key       RSA       2048 bit       0       Common       Export         Import       Import       Import PFX (PKCS#12)       Show Details       Delete	0	Database	: /Users/shiji/crt_Ji	ngLab.xdb	-	Search	
X Certificate and Key management      Private Keys     Certificate signing requests     Certificates     Type     Size     Use     Passwor     CA_key     RSA     2048 bit     1 Common     Export     Inserver_key     RSA     2048 bit     0 Common     Export     Import     Import     Import     Import     Import PFX (PKCS#12)     Show Details     Delete							
Private Keys       Certificate signing requests       Certificates       Templates       Revocation lists         Internal name       ^       Type       Size       Use       Passwor         CA_key       RSA       2048 bit       1       Common       New Key         LI_server_key       RSA       2048 bit       0       Common       Export         NSX-mgr157_key       RSA       2048 bit       0       Common       Import         Import PFX (PKCS#12)       Show Details       Delete       Delete	•••		Х	Certificate and	Key ma	nagement	
Internal name       Type       Size       Use       Passwor         CA_key       RSA       2048 bit       1       Common         LI_server_key       RSA       2048 bit       0       Common         NSX-mgr157_key       RSA       2048 bit       0       Common         Import       Import       Import PFX (PKCS#12)         Show Details       Delete		Private Keys	Certificate sigr	ing requests	Certifi	cates Terr	aplates Revocation lists
LI_server_key RSA 2048 bit 0 Common NSX-mgr157_key RSA 2048 bit 0 Common Import Import PFX (PKCS#12) Show Details Delete		ernal name A_key	^ Type RSA	Size 2048 bit	Use 1	Passwor Common	New Key
NSX-mgr157_key KSA 2048 bit 0 Common Import Import PFX (PKCS#12) Show Details Delete	C LI	_server_key	RSA	2048 bit	0	Common	Export
Import PFX (PKCS#12) Show Details Delete	C NS	SX-mgr157_ke	Y RSA	2048 bit	0	Common	Import
Show Details Delete							Import PFX (PKCS#12)
Delete							Show Details
Delete							Show Details
							Delete
Database: /Users/shiji/crt_JingLab.xdb Search	Database: /Us	sers/shiji/crt_Jing	Lab.xdb		Search		

3. In the Certificates tab, create a root CA certificate by clicking "New Certificate" and fill the required information. Note that CRL Distribution Point (CDP) is mandatory because CRL checking is enabled by default on the NSX manager. If CDP is not available, refer to the next section "Disabling CRL checking" for details.





	X Certificate and	Key management	
Private Keys Certificate	signing requests	Certificates Te	emplates Revocation lists
Internal name	CA Seria	al Expiry dat	New Certificate
			Export
			Import
			Show Details
			Delete
			Import PKCS#12
			Import PKCS#7
			Plain View
			Tarmingto (
			Dingroof Time
atabase: /Users/shiji/crt_JingLab.xdb		Search	





Certificate and Key management	• •	X Certi	ficate and Key management
Create v509 Certificate	Create	v509 Certificate	
Course Subject Extensions Key usage Netscane	Advanced Comment	Source Subject Etensions	Kay usage National Comment
Signing request	Auvanced Comment	source subject Eltensions	Key usage werscape Auvanced Comment
	<ul> <li>Dis</li> </ul>	stinguished name	
Copy extensions from the request	Show request	countryName US	organizationalUnitName NSBU
Modify subject of the request	st	tateOrProvinceName CA	commonName CA_JingLab
Signing	0	rganizationName VMware	UTINIMUU 633
Create a self signed certificate		Туре	Content Add
	0		Delete
Signature algorithm SHA 256			
Template for the new certificate			
[default] CA			
Apply extensions	Apply subject Apply all	vate key	
		CA_key (RSA:2048 bit)	Used keys too Generate a new key
	Cancel OK		Cancel OK
X Certificate and Key management		• × Ce	ertificate and Key management
X Certificate and Key management		• x Ce	ertificate and Key management
X Certificate and Key management Create x509 Certificate	Cres	• X Ce ate x509 Certificate	ertificate and Key management
Create x509 Certificate Source Subjec Extensions Key usage Netscape	Advanced Comment	X Ce ate x509 Certificate Source Subject Extension	ertificate and Key management
X Certificate and Key management Create x509 Certificate Source Subjec Extensions Key usage Netscape X509v3 Basic Constraints	Advanced Comment Key identifier	X Ce     Ate x509 Certificate     Source Subject Extension     Ko90v3 Key Usage     Critical	ertificate and Key management
X Certificate and Key management Create x509 Certificate Source Subjec Cetansions Key usage Netscape X509v3 Basic Constraints Type Certification Authority Certification Authority Certification	Advanced Comment Key identifier X50903 Subject Key identifier	X Ce     Ate x509 Certificate     Source Subject Extension     Color3 Key Usage     Critical     Digital Signature	artificate and Key management
X Certificate and Key management Create x509 Certificate Source Subject Cettensions Key usage Netscape X509v3 Basic Constraints Type Certification Authority Path length Critical	Cree Advanced Comment Key identifier X509v3 Subject Key identifier X509v3 Authority Key identifier	X Ce ate x509 Certificate     Source Subject Extension     Source Subject Extension     Critical     Digital Signature     Non Repudiation     Key Encipherment	ertificate and Key management
X Certificate and Key management Create x509 Certificate      Source Subjective Key usage Netscape     X509v3 Basic Constraints     Type Certification Authority     Path length     Critical     Validity Time rance	Cree Advanced Comment Key identifier X509v3 Subject Key identifier X509v3 Authority Key identifier	X Ce     Ate x509 Certificate     Source Subject Extension     Source Subject Extension     Critical     Digital Signature     Non Repudition     Key Encipherment     Data Encipherment     Key Agreement	et/ficate and Key management
X Certificate and Key management Create x509 Certificate Source Subjec extinsions Key usage Netscape X509v3 Basic Constraints Type Certification Authority © Path length Critical Validity Time range Liste before 2020-01-01/314/45 CMT	Cree Advanced Comment Key identifier X509v3 Authority Key Identifier	X Ce     Stop Certificate     Source Subject Extension     Source Subject Extension     Solv3 Key Usage     Ortical     Digital Signature     Non Republicition     Key Encloherment     Key Encloherment     Cettigate Sign     Cettigate     Subject     Sub	ertificate and Key management
X Certificate and Key management Create x509 Certificate Source Subjective Key usage Netscape Validation Authority Path length Critical Validaty Time range 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Advanced       Comment         Key identifier       X509v3 Subject Key identifier         X509v3 Authority Key identifier         Years       Apply	X Ce     Store Subject Extension     Source Subject Extension     Source Subject Extension     Store Subject Extension     Critical     Digital Signature     Non Republiciton     Key Encipherment     Data Encipherment     Certificate Sign     CRL	ertificate and Key management
Create x509 Certificate Source Subjee Extensions Key usage Netscape St009v3 Basic Constraints Type Certification Authority Path length Path length Time range Not before 2020-10-01 14:45 GMT Inidinight Local	Advanced Comment Key identifier X509v3 Subject Key identifier X509v3 Authority Key identifier Years C Apply time No well-defined expiration	X Ce     Store Subject Extension     Source Subject Extension     Source Subject Extension     Critical     Digital Signature     Non Republicition     Key Encipherment     Data Encipherment     Critical	ertificate and Key management
Create x509 Certificate Source Subjer Extensions Key usage Netscape St00v3 Basic Constraints Type Certification Authority Path length Not before 2020-10-01 14:45 GMT Immer range I Mot after 2021-10-01 14:45 GMT Immer range I Imminght Local	Advanced Comment Key identifier X509v3 Subject Key identifier X509v3 Authority Key identifier Years Apply time No well-defined expiration	X Ce     Ats x509 Certificate     Source Subject Extension     Source Subject Extension     Critical     Digital Signature     Non Republiciton     Key Encipherment     Data Encipherment     Critical     Critical     Critical     Critical     CRL Sign     CRL	ertificate and Key management
Create x509 Certificate Source Subject Extensions Key usage Netscape Sto0v3 Basic Constraints Type Certification Authority Path length Not before 2020-10-01 14:45 GMT  Image I Mot after 2021-10-01 14:45 GMT  Image I Image	Advanced Comment Key identifier X509v3 Subject Key identifier X509v3 Authority Key identifier Vears C Apply time No well-defined expiration	X Ce     Ats x509 Certificate     Source Subject Extension     Source Subject Extension     Critical     Digital Signature     Non Republicition     Key Encipherment     Data Encipherment     Critical     Cri	ertificate and Key management
X Certificate and Key management Create x509 Certificate Source Subjec Extensions Key usage Netscape Validity Path length Not before 2020-10-01 14:45 GMT  I Midnight Local X509V3 Subject Alternative Name X509V3 Issuer Alternative Name	Advanced Comment Key identifier X509v3 Subject Key identifier X509v3 Authority Key identifier X509v3 Authority Key identifier time No well-defined expiration Edit Edit	Accession of the second s	rtificate and Key management
X Certificate and Key management Create x509 Certificate Source Subjec Extensions Key usage Netscape X509v3 Basic Constraints Type Certification Authority Path length Validity Time range Validity Time range Unit before 2020-10-01 14:45 GMT  I Midnight Local X509v3 Subject Alternative Name X509v3 Subject Alternative Name X509v3 Subject Alternative Name X509v3 CRL Distribution Points VIII:http://10.114.220.137/JingLab.cc	Advanced Comment Key identifier X509v3 Subject Key identifier X509v3 Authority Key identifier X509v3 Authority Key identifier Users Apply time No well-defined expiration Edit Edit Edit	Accession of the second s	rtificate and Key management
X Certificate and Key management Create x509 Certificate Source Subjec Extensions Key usage Netscape X509v3 Basic Constraints Type Certification Authority Path length Validity Time range Validity Time range Unit before 2020-10-01 14:45 GMT  I Midnight Local X509v3 Subject Alternative Name X509v3 CRL Distribution Points URI:http://10.114.220.137/JingLab.cc	Advanced Comment Key identifier X509v3 Subject Key identifier X509v3 Authority Key identifier X509v3 Authority Key identifier Users Apply time No well-defined expiration Edit Edit Edit Edit	Acceleration     Source Subject Extension     Source Subject Extension     Source Subject Extension     Critical     Digital Signature     Non Repudiation     Key Encipherment     Key Agreement     Certificate Sign     CRL Sign     Encipher Only     Decipher Only	rtificate and Key management
X Certificate and Key management Create x509 Certificate Source Subjec Extensions Key usage Netscape Your a subjec Certification Authority Path length Validity Ualidity Ualidity Time range Ualidity Time range Ualidity U	Advanced Comment Key identifier X509v3 Subject Key identifier X509v3 Authority Key identifier X509v3 Authority Key identifier Years O Apply time No well-defined expiration Edit Edit Edit	Acceleration     Source Subject Extension     Source Subject Extension     Critical     Digital Signature     Non Repudiation     Koy Anceloherment     Koy Agreement     Certificate Sign     CRL Sign     Encipher Only     Decipher Only	rtificate and Key management



4. Once the root CA certificate is created, select the created CA certificate and click "New Certificate" to create a leaf certificate that is signed by the root CA certificate:



A GOLUNG	ate and Key management		• •	X Certific	ate and Key management	
ate x509 Certificate			Create x509 Certificate			
Source Subject Extensions	Key usage Netscape	Advanced Comment	Source	Subject Extensions	Key usage Netscape	Advanced Comment
Signing request			Internal Name NSX-mg	r157_crt		
Sign this Certificate signing request		0	Distinguished name			
Convextensions from the request			countryName	US	organizationalUnitNan	ne NSBU
			stateOrProvinceName	CA	commonName	10.114.220.157
			localityName	PA	emailAddress	
Signing			organizationName	VMware		
Create a self signed certificate			Туре		Content	Add
<ul> <li>Use this Certificate for signing</li> </ul>	CA_crt					Delete
ignature algorithm	SHA 256					
Template for the new certificate						
[default] CA		0				
	Annual submariant	Annis subject	Private key			
	Apply extensions	Apply subject Apply all	NSX-mgr157_key (R	SA:2048 bit)	🖸 Used ke	eys too Generate a new key
X Certifica	ate and Key management		• •	X Cert	ificate and Key management	
te x509 Certificate			Create x509 Certificate			А
Source Subject Extensions	Key usage Netscape	Advanced Comment	Source	Subject Extensions	Key usage Netscape	Advanced Comment
K509v3 Basic Constraints						
		Key identifier	X509v3 Key Usage		X509v3 Extended	Key Usage
Type End Entity		Key identifier	X509v3 Key Usage Critical		X509v3 Extended Critical	Key Usage
Type End Entity		Key identifier X509v3 Subject Key Identifier X509v3 Authority Key Identifier	X509v3 Key Usage Critical Digital Signature Non Repudiation		X509v3 Extended Critical TLS Web Server	Key Usage er Authentication
Type End Entity Path length	Critical	Key identifier X509v3 Subject Key Identifier X509v3 Authority Key Identifier	X509v3 Key Usage Critical Digital Signature Non Repudiation Key Encipherment		X509v3 Extended Critical TLS Web Serv TLS Web Clien	Key Usage er Authentication t Authentication
Type End Entity Path length	Critical	Key identifier X509v3 Subject Key identifier X509v3 Authority Key identifier	x509v3 Key Usage Critical Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement		X509v3 Extended Critical TLS Web Sarv TLS Web Clien E-mail Protect Time Stamping	Key Usage er Authentication t Authentication
Type End Entity Path length validity	Critical	Key identifier X509v3 Subject Key Identifier X509v3 Authority Key Identifier	x509v3 Key Usage Critical Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement Certificate Sign CBI. Sign		X509v3 Extended Critical TLS Web Serv TLS Web Clien E-mail Protect Time Stamping Microsoft India	Key Usage ar Authentication t Authentication on idual Code Signing mercial Code Signing
Type End Entity Path length alidity Not before 2020-10-0115:45 GMT	Critical	Key identifier X509v3 Subject Key identifier X509v3 Authority Key identifier	X509v3 Key Usage Critical Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement Certificate Sign CRL Sign Encipher Only		X509v3 Extended Critical TLS Web Serve TLS Web Client E-mail Protect Time Stamping Microsoft Indi Microsoft Com Microsoft Com	Key Usage ar Authentication t. Authentication dual Code Signing mercial Code Signing List Signing
Type End Entity Path length Auldity Not before 2020-10-01 15:45 GMT	Critical Time range	Key identifier X509v3 Subject Key identifier X509v3 Authority Key identifier	x509v3 Key Usage Critical Digital Signature Non Republistion Key Encipherment Data Encipherment Certificata Sign CRL Sign Encipher Only Decipher Only		X509v3 Extended Critical TLS Web Serve TLS Web Client Firms Stamping Microsoft India Microsoft Trus Microsoft Serve Microsoft Serve Microsoft Serve	Key Usage r Authentication r Authentication on fuldial Code Signing mercial Code Signing r Gated Crypto ypted File System
Type End Entity Path length Validity Not before 2020-10-01 15:45 GMT  Validity	Critical	Key identifier X509v3 Subject Key identifier X509v3 Authority Key identifier Years O Apply I time No well-defined expiration	x309v3 Key Usage Critical Digital Signature Non Repudiation Key Encipherment Data Encipherment Certificate Sign CRL Sign Encipher Only Decipher Only		X509v3 Extended Critical TLS Web Sarr E-mail Protect Time Stamping Microsoft Com Microsoft Trus Microsoft Trus Microsoft From Microsoft Protect Microsoft Protect	key Usage r Authentication r Authentication on idual Code Signing mercial Code Signing t Gated Crypto yptod File System r Gated Crypto
Type End Entity Path length validity Not before 2020-10-01 15:45 GMT  validity Not after 2021-10-01 15:19 GMT  validity	Critical Time range 1 Midnight Loce	Key identifier X509v3 Subject Key identifier X509v3 Authority Key identifier Years Apply I time No well-defined expiration	x309v3 Key Usage Critical Digital Signature Non Republistion Key Encipherment Data Encipherment Certificant Sign CRL Sign Encipher Only Decipher Only		X509v3 Extended Critical TLS Web Sarr LS Web Clerr E-mail Protect Time Stamping Microsoft Fain Microsoft Fain Microsoft Fain Microsoft Sarr Microsoft Ears Microsoft Ears Microsoft Ears Microsoft Ears	key Usage ar Authentication t Authentication on idual Code Signing tList Signing rescial Code Signing List Signing or Gated Crysto pyted File System or Gated Crysto File Recovery tem
Type End Entity Path length Validity Not before 2020-10-01 15:45 GMT  COLORIDATION Not after 2021-10-01 15:19 GMT COLORIDATION COLORIDA	Critical Time range 1 Midnight Loca	Key identifier X509v3 Subject Key Identifier X509v3 Authority Key Identifier Years Apply I time No well-defined expiration Edit	x309v3 Key Usage Critical Digital Signature Non Republiation Key Encipherment Data Encipherment Cartificate Sign CRL Sign Encipher Only Decipher Only		X509v3 Extended Critical TLS Web Sam E-mail Protect Time Stamping Microsoft Tindh Microsoft Com Microsoft Serv Microsoft Serv	key Usage ar Authentication t Authentication idual Code Signing mercial Code Signing mercial Code Signing er Cated Crysto ysted File System er Gated Crysto File Recovery tem
Type End Entity Path length Validity Not before 2020-10-01 15:45 GMT  Validity Not after 2021-10-01 15:19 GMT  Validity 509v3 Subject Alternative Name 509v3 Subject Alternative Name	Critical Time range 1 Midnight Loca	Key identifier X509v3 Subject Key Identifier X509v3 Authority Key Identifier Years Apply I time No well-defined expiration Edit Edit	X509v3 Key Usage Critical Digital Signature Non Repudiation Key Encipherment Data Encipherment Cartificate Sign CRL, Sign Encipher Only Decipher Only		X509v3 Extended Critical TLS Web Sem E-mail Protect Time Stamping Microsoft Timb Microsoft Tom Microsoft Sem Microsoft Sem Microsoft Sen Microsoft Sen Microsoft Sen Microsoft Sen Microsoft Sen Microsoft Sen Pisee Laser Pisee User Piseculty enc	key Usage ar Authentication t Authentication t Authentication idual Code Signing mercial Code Signing t List Signing er Gated Crysto ypted File System er Gated Crysto lie Recovery tem entity
Type End Entity Path length Validity Not before 2020-10-01 15-45 GMT  Validity S09v3 Subject Alternative Name S09v3 Issuer Alternative Name	Critical Time range 1 Midnight Loco	Key identifier X509v3 Subject Key Identifier X509v3 Authority Key Identifier Years Apply I time No well-defined expiration Edit Edit	x509v3 Key Usage Critical Digital Signature Non Republishon Key Encipherment Data Encipherment Certificate Sign CRL Sign Encipher Only Decipher Only		X500+3 Extended Critical TLS Web Saver E-mail Protect Time Stamping Microsoft Com Microsoft Trus Microsoft Trus Microsoft Ers IPSec End Sy IPSec Tunel IPSec User IPSec User IPSEC IP	key Usage  r Authentication r Authentication on idual Code Signing mercial Code Signing r Gated Crypto pyted File System er Gated Crypto File Recovery tem entity rtcard Login
Type End Entity Path length Validity Not before 2020-10-01 15-45 GMT COUPLING SOBV3 Subject Alternative Name SOBV3 Issuer Alternative Name SOBV3 CRL Distribution Points URL:http	Critical Time range 1 Midnight Loca	Key identifier X509v3 Subject Key Identifier X509v3 Authority Key Identifier Years C Apply I time No well-defined expiration Edit Edit Edit	x509v3 Key Usage Critical Digital Signature Non Republistion Key Encipherment Data Encipherment Certificate Sign CRL Sign Encipher Only Decipher Only		X500+3 Extended Oritical TLS Veb Serier E-mail Protect Time Stamping Microsoft Com Microsoft Com Microsoft Trus Microsoft Ers IPSec End Sy IPSec Tunel IPSec User IPSec User IPS	Key Usage  r Authentication r Authentication on idual Code Signing mercial Code Signing re Gated Crypto pyted File System er Gated Crypto File Recovery tem entity rtcard Login
Type End Entity Path length Validity Not before 2020-10-01 15:45 GMT  Validity Not after 2021-10-01 15:19 GMT  Validity S09V3 Subject Alternative Name S09V3 Issuer Alternative Name S09V3 CRL Distribution Points V URI:http uthority Information Access	Critical Time range 1 Midnight Locz	Key identifier X509v3 Subject Key Identifier X509v3 Authority Key Identifier Years Apply I time No well-defined expiration Edit Edit Edit Edit	x309v3 Key Usage Critical Digital Signature Non Republiation Key Encipherment Data Encipherment Certificata Sign Encipher Only Decipher Only		X509v3 Extended Critical TLS Web Save E-mail Protect Time Stamping Microsoft Com Microsoft Trus Microsoft Save Microsoft FFS IPSac End Syv IPSac Tunel IPSac Usir Microsoft Save Descurity on Microsoft Save Descurity on Microsoft Save IPSac Usir IPSac Usir Microsoft Save Descurity on Microsoft Save Microsoft Sav	key Usage r Authentication r Authentication on idual Code Signing mercial Code Signing r Gated Crypto Fig Stytem er Gated Crypto Fig Recovery tem ientity tcard Login esponse
Type End Entity Path length Validity Not before 2020-10-01 15-45 GMT  Validity Not after 2021-10-01 15-19 GMT  Validity 1509v3 Subject Alternative Name 509v3 CRL Distribution Points Uthority Information Access	Critical Critical I I I I I I I I I I I I I I I I I I I	Key identifier X509v3 Subject Key identifier X509v3 Authority Key identifier Years Apply al time No well-defined expiration Edit Edit Edit Edit Edit	x509v3 key Usage Critical Digital Signature Non Republiation Data Encipherment Data Encipherment Certificate Sign CRL Sign Encipher Only Decipher Only		X009/3 Extended Critical TLS Veb Serie E-mail Protect Time Stamping Microsoft Com Microsoft Trus Microsoft Ers Microsoft Ers IPSec Ibar Pisec Tonel IPSec User IPSec User IPSec User IPSec User IPSec Vest PIP EAP veer Lan Signing KDC R	key Usage  r Authentication r Authentication on t tutteriticates recalled Code Signing mercial Code Signing or Gated Crysto pyted File System or Gated Crysto File Recovery tem entity rtcard Login esponse
Type End Entity Path length Validity Not before 2020-10-01 15:45 GMT  Validity Not after 2021-10-01 15:19 GMT  Validity S09v3 Subject Alternative Name S09v3 Ssubject Alternative Name U09v3 CRL Distribution Points V URI:http uthority Information Access	Critical Critical	Key identifier X509v3 Subject Key identifier X509v3 Authority Key identifier Years Apply at time No well-defined expiration Edit Edit Edit Edit	x509v3 Key Usage Critical Digital Signature Non Republishion Key Encipherment Data Encipherment Certificate Sign CRL Sign Encipher Only Decipher Only		X009/3 Extended Oritical TLS Veb Serr E-mail Protect Time Stamping Microsoft Com Microsoft Com Microsoft Trus Microsoft Ers IPSec Ibar Pisec Tunel IPSec User IPSec User Pisec Tunel IPSec User IPSec User Pisec International Composition Microsoft Small OCSP Signing EAP over Lan Signing KDC R	key Usage  r Authentication r Authentication on idual Code Signing mercial Code Signing rer Gated Crypto yoted File System er Gated Crypto File Recovery tem entity rtcard Login esponse
Type End Entity Path length Validity Not before 2020-10-01 15:45 GMT  K509v3 Subject Alternative Name (509v3 Subject Alternative Name (509v3 Subject Alternative Name (509v3 CRL Distribution Points (V URL:http uthority Information Access C OCSP	Critical Critical Time range 1 Midnight Loci	Key identifier X509v3 Subject Key identifier X509v3 Authority Key identifier Years Apply at time No well-defined expiration Edit Edit Edit Edit	x309v3 Key Usage Critical Digital Signature Non Republishion Key Encipherment Data Encipherment Certificata Sign CRL Sign Encipher Only Decipher Only		X009/3 Extended Critical TLS Web Sare E-mail Protect Time Stamping Microsoft Com Microsoft Com Microsoft Ers Picke: Eds Sy Picke: Com Discont Ers Picke: Com Dicke: Com Discont Ers Pic	key Usage r Authentication tauthentication disal Code Signing mercial Code Signing er Gated Crypto prodef File System er Gated Crypto File Recovery ter entity rtcard Login esponse





A

Add

Delete

Cancel OK

X Certificate and Key management		Second Se	artificate and Key management
Create x509 Certificate  Source Subject Extensions Key usage Netscape  XK09v3 Basic Constraints  Type Ind Entity Path length Critical  Validity Time range 1 Mot before 2020-10-01 15:54 GMT  1 Midnight Loca	Advanced Comment Key identifier X509V3 Subject Key identifier X509V3 Authority Key identifier Years © Apply time No well-defined expiration	Create x509 Certificate Source Subject Extension X509-X Key Usage Critical Digital Signature Non Repudiation Key Encipherment Data Encipherment Certificate Sign CRL Sign Encipher Only Decipher Only	tilicate and Key management
X509v3 Subject Alternative Name X509v3 Issuer Alternative Name X509v3 CRL Distribution Points Authority Information Access	Edit Edit Edit Edit Cancel OK		Microsoft EFS File Recovery PSec End System PSec Trunnel PSec User P security end entity Microsoft Smartcard Login OCSP Signing EAP over PPP EAP over Lan Signing KDC: Response

	X Certificate and H	Key manage	ment	
Private Keys Certificate	e signing requests	Certificates	Templates	Revocation lists
Internal name ^ CA_crt	commonName CA_JingLab 10.114.220.225	CA Ves	7876	New Certificate
NSX-mgr157 crt	10.114.220.157	No	1402	Export
				Import
				Show Details
				Delete
				Import PKCS#12
				Import PKCS#7
				Plain View
			J	Dunderoo Jim
Database: /Users/shiji/crt_JingLab.xdb	Ş	Search		

5. Export the keys and certificates have been created:

[shiji-a01:cr	't_JingLab	shiji\$	ls -al		
total 40					
drwxr-xr-x	7 shiji	staff	224 Oct	1 13:24	
drwx+	222 shiji	staff	7104 Oct	1 13:22	
-rw-rr	1 shiji	staff	1318 Oct	1 13:23	CA_crt.crt
-rw-rr	1 shiji	staff	1326 Oct	1 13:24	LI_server_crt.crt
-rw	1 shiji	staff	1679 Oct	1 13:23	LI_server_key.pem
-rw-rr	1 shiji	staff	1326 Oct	1 13:24	NSX-mgr157_crt.crt
-rw	1 shiji	staff	1675 Oct	1 13:23	NSX-mgr157_key.pem
shiji-a01:cr	t_JingLab	shiji\$			

6. Prepare for certification files will be needed by the LogInsight clients which are the NSX manager/Edge node/Transport Node and LogInsight server which is the LogInsight itself.

The certification file needed by the LogInsight client includes client certificate, CA certificate. The order of the certificates is



important, the client certificate followed by CA certificate.

## [shiji-a01:crt\_JingLab shiji\$ cat NSX-mgr157\_crt.crt CA\_crt.crt > NSX-mgr157\_crt\_full.pem

The certification file needed by the LogInsight server include private key of LI server, certificate of LI server and certificate of CA.

## [shiji-a01:crt\_JingLab shiji\$ cat LI\_server\_key.pem LI\_server\_crt.crt CA\_crt.crt > LI\_crt\_full.pem

7. For NSX manager, put the certificate and key files under /image/vmware/nsx/file-store. For Edge node, put the certificate and key files under /var/vmware/nsx/file-store. Make sure the files have corrected permission.

[root@nsx-mg	gr	-157:	/image/vmw	vare/i	nsx/f	'file-store# ls -al *crt* *key*	
-rw-rr	1	root	www-data	1318	0ct	: 1 18:42 CA_crt.crt	
-rw-rr	1	root	www-data	2644	0ct	: 1 18:44 NSX-mgr157_crt_full.per	m
-rw-rr	1	root	www-data	1675	0ct	: 1 18:43 NSX-mgr157_key.pem	

8. Configure logging with TLS on NSX manager / Edge node ( LogInsight client )

nsx-mgr-157> set logging-server 10.114.220.225 proto tls level info serverca CA_crt.crt clientca CA_crt.cr]
t certificate NSX-mgr157_crt_full.crt key NSX-mgr157_key.pem
nsx-mgr-157> get logging-servers
10.114.220.225:6514 proto tls level info serverca CA_crt.crt clientca CA_crt.crt certificate NSX-mgr157_cr
t_full.crt key NSX-mgr157_key.pem

9. Configure Log Insight

vm Log Insight	Dashboards Interactive Analytics	🛓 admin 🛛 🚍
Management System Monitor Cluster Access Control User Alerts Hosts Agents Event Forwarding	SSL Configuration CUSTOM SSL CERTIFICATE Existing Certificate  Custom VIEW DETAILS New Certificate File (PEM format) Choose File No file chosen	
License	Require SSL Connection	
Certificates Integration vSphere vRealize Operations	SAVE RESET TO DEFAULTS	
Configuration		
General Time		
Authentication		
SMTP		
Archiving SSL		


Certificate Infor	mation		
Owner:         US           Country         US           State Or Province         CA           Locality         PA           Organization         VMware           Organization Unit NSBU         Common Name	0.225		
Issuer: Country US State Or Province CA Locality PA Organization VMware Organization Unit NSBU Common Name CA_Jingl	Lab		
Validity period: From 10/1/2020, 19:27:00 Until 10/1/2021, 19:20:00	Serial Number: 7705b1e6	Owner: Country State Or Province Locality Organization Organization Unit Common Name	US CA PA VMware NSBU CA_JingLab
Issuer: Country US State Or Province CA Locality PA Organization VMware Organization Unit NSBU Common Name CA_Jingl	Lab		
Validity period: From 10/1/2020, 19:20:00 Until 10/1/2021, 19:20:00	Serial Number: 69778176		CANCEL

10. Verify Log Insight can receive the logs from the clients.

vm Log	g Insight	Dashboards	Interactiv	e Analytics						💄 admin 😑
				_						<b>i</b> l
	10:22:30 10:23:00		10:24:00	10:24:30	10:25:00	10:	25:30	10:3	26:00 10:26	:30 10:27:00
Count of eve	ents + + over time + Apply	Reset					1	bar = 5	seconds 👻 Char	t Type 🛛 II. Automatic 👻
				<b>☆</b> ▼ Lates	t 5 minutes o	of data	~	Q	*	<b>*</b>   <b>*</b>   <b>*</b>
	201 <b>M</b> 10			10/2/20	020,10:22:07	.839 to	10/2/202	0,10:27:0	)7.838	
V courco	Contains	10114	2201E7							
X source	Contains		.220.157 A)							
+ ADD FILT	ER × CLEAR ALL FILTERS		.220.157							
+ ADD FILT CONTENT F	ER × CLEAR ALL FILTERS PACKS ~ (Extract all fields)	(10.114	.220.157 x							
+ ADD FILT CONTENT F	ER × CLEAR ALL FILTERS PACKS ~ (Extract all fields) Field Table Event Types Eve	nt Trends	.220.157	1 to 50 out of 1,94	រៅ events Cc	l <b>umns →</b> Sort	t: Newest Fir	st <del>v</del>	Fields d	)
+ ADD FILT CONTENT F Events timestamp	ER × CLEAR ALL FILTERS PACKS ~ (Extract all fields) Field Table Event Types Event	nt Trends	source	1 to 50 out of 1,94 event_type	M events Co	l <mark>lumns                                    </mark>	t: Newest Fir	st ▼ msgid	Fields	3
+ ADD FILT CONTENT F Events timestamp 10/2/2020, 10:27:07.774	ER × CLEAR ALL FILTERS PACKS (Extract all fields) Field Table Event Types Eve text 2020-10-02T14:27:11.906Z nsx-mgr-157 [nsx06876 comp="nsx-manager" subcomp=	nt Trends	source	1 to 50 out of 1,94 event_type v4_5454a3c1	M events Co hostname nsx-mgr~ 157	appname NSX	t: Newest Fir procid 3300	st ▼ msgid -	Fields + appname + event_type + hostname + msgid	þ
+ ADD FILT CONTENT F Events timestamp 10/2/2020, 10:27:07.774 10/2/2020, 10:27:07.273	ER         × CLEAR ALL FILTERS           PACKS         (Extract all fields)           Field Table         Event Types         Event Types           text         (Extract all fields)           2020-16-02114:27:11.9042.nsx-mgn-157         (Insv6876 comp*"nsx-mgnager" subcomp apm_unix(sudo:session): session close		source 10.114.220.157	1 to 50 out of 1,94 event_type v4_5454a3c1 v4_3b2221a0	H events Co hostname nsx-mgr- 157 nsx-mgr- 157	appname NSX sudo	: Newest Fin procid 3300	st ▼ msgid -	Fields // + appname + event_type + hostname + msgid + procid + source	•
+ ADD FILT CONTENT F Events timestamp 10/2/2020, 10:27:07.273 10/2/2020, 10:27:07.273 10/2/2020, 10:27:07.273	ER         × CLEAR ALL FILTERS           PACKS ~         (Extract all fields)           Field Table         Event Types         Event           text         2020-10-02714:27:11.90426:00:00 nsx-mgr-157         Ensview76 comp="nsx-manager" subcomp=mgu_nix(subcisesion): session close           2020-10-02714:27:11.90426:00:00 nsx-mgu_nux(subcisesion): session close         2020-10-02714:27:11.90456:00:00 nsx-mgu_nux(subcisesion): session close           2020-10-02714:27:11.90456:00:00 nsx-mgu_nux(subcisesion): session close         2020-10-02714:27:11.905566:00:00 nsx-mgr-157	nt Trends tisk 3300 - "node-mgmt" for user root ngr-157 sudo tigr-157 audispd -	source 10.114.220.157 10.114.220.157	1 to 50 out of 1,94 event_type v4_5454a3c1 v4_5b2221a0 v4_b1d10791	Hevents Co hostname nsx-mgr- 157 nsx-mgr- 157	appname NSX sudo audispd	: Newest Fin procid 3300 -	st • msgid - -	Fields + appname + event_type + hostname + msgid + procid + source	þ

11. To troubleshoot certificate issues, check the syslog to see any related error messages:





<179>1 2020-10-01T15:03:09.290-04:00 nsx-mgr-157 NSX 5982 SYSTEM [nsx@6876 comp="nsx-manager" errorCode="MP2076" level="ERROR" reqId="295e3 d1d-0bdc-4c5d-b963-4030d9a6ab37" subcomp="manager" username="admin"] Certificate chain validation failed. Make sure a valid chain is provid ed in order leaf, intermediate, root certificate. <179>1 2020-10-01T19:03:09.296Z nsx-mgr-157 NSX 3300 - [nsx@6876 comp="nsx-manager" subcomp="node-mgmt" username="root" level="ERROR" error Code="NODE10"] Unable to import certificate. status: 400 <179>1 2020-10-01T19:03:09.296Z nsx-mgr-157 NSX 3300 - [nsx@6876 comp="nsx-manager" subcomp="node-mgmt" username="admin" level="ERROR" error Code="NODE10"] Failed to create certificate PEM file /config/vmware/nsx-manager" subcomp="node-mgmt" username="admin" level="ERROR" error Code="NODE10"] Failed to create certificate PEM file /config/vmware/nsx-mode-api/syslog/7b52fc17-92ac-471e-892d-5849180f29b1\_cert.pem for logging server 10.114.220.225:6514 <179>1 2020-10-01T19:03:10.139Z nsx-mgr-157 NSX 13979 - [nsx@6876 comp="nsx-cli" subcomp="node-mgmt" username="admin" level="ERROR" errorCode="('CLI10',)"] Error setting logging server: {'error\_message': 'Error, importing TLS certificate.', 'module\_name': 'node-services', 'error code="36415}

#### Notes on how to disable CRL checking:

The crl\_checking\_enabled flag is a part of SecurityGlobalConfig which is a part of api/v1/globalconfigsTo get the current SecurityGlobalConfig when logged into a manager:

root@manager1:~# curl -k -X GET -H 'accept: application/json'

https://127.0.0.1/api/v1/global-

```
configs/SecurityGlobalConfig -u 'admin:VMwarensbu_1' {
```

- "crl\_checking\_enabled" : true,
- "ca\_signed\_only" : false,
- "resource\_type" : "SecurityGlobalConfig",
- "id" : "c80387b9-3c80-46ae-970d-6590d06acba8",
- "display\_name" : "c80387b9-3c80-46ae-970d-6590d06acba8",
- "\_create\_user" : "system",
- "\_system\_owned" : false,
- "\_create\_time" : 1574364819458,
- "\_last\_modified\_user" : "system",
- "\_last\_modified\_time" : 1574364819493,
- "\_protection" : "NOT\_PROTECTED",
- "\_revision" : 2 }

To update it when logged into a manager:

-root@manager1:~#curl -i -k -H

Content-type:application/json -u 'admin:VMwarensbu\_1' T CRL\_FALSE https://127.0.0.1/api/v1/global-configs/SecurityGlobalConfig where CRL FALSE file will contain:

```
{
```

- "crl\_checking\_enabled" : false,
- "resource\_type": "SecurityGlobalConfig",
- "\_revision" : 2
- }

#### **5.3 Connection Tools**

Port Connection Tool and Traceflow are two great tools for troubleshooting communication between workloads running in NSX. They show real-time information of the topology and detect issues (if any), thus reduce the time it takes to find out what is preventing such communication. The following diagrams depicts a sample Network Topology.

#### 5.3.1 Network Topology Tool

by Broadcom

## NSX-T 3.0: Operation Guide



Network Topology provides an overview of the NSX environment. It can be exported as PDF as well.

#### 5.3.2 Port Connection Tool

Port Connection Tool provides visual information of the logical and physical connectivity between the interfaces of two workloads running in NSX, including VMs and containers.

It shows a visual map with layers that display realized state data such workload information, Logical Port status and Tunnel-health status, representing hop by hop connectivity between various points in the path.

It is possible to click on any of the components in the visual output to reveal more information about them. If issues are found, the corresponding components are displayed in yellow or red.



Figure 5-4: Port Connection Tool visualizations, without and with port issues (resp.)

#### 5.3.3 Traceflow

Traceflow takes troubleshooting a step further by injecting a packet at the logical port of the source workload and displaying the step-by-step path a packet takes until it reaches the destination workload. Admins can specify multiple characteristics of the



packet to match their troubleshooting needs.

Traffic Type:*	Unicast 🗸				
Source		5	Destination		
Гуре	Virtual Machine	~	Туре	Virtual Machine	~
/M Name*		~	VM Name*		~
Frame Size	64	\$ \$	Protocol Type	ICMP	~
Timeout (ms)	10000	\$	ICMP ID	TCP	
Ethertype	2048	\$	Sequence	ICMP	
Payload Type	Base64	~			



The trace packet traverses the logical switch overlay but is not visible to interfaces attached to the logical switch, meaning, no packet is delivered to the intended recipients. Traceflow output includes a table listing Observation Type (i.e., Delivered, Dropped, Received, Forwarded), Transport Node, Component, and the Port Connection Tool graphical map of the topology if unicast and logical switch are selected as destinations. By clicking on the components in the visual output reveals more information.

Source	Destination	RE-TRACE	EDIT NEW TRACE	1		
Virtual Machine web02	Virtual Machine db01					
IP/MAC 172.16.10.12/00:50:56:b5:ff:	cf IP/MAC 172.16.30.11/52:54:00:8f:77:	17				
race Results						
web	db	Show: ALL 1	DELIVERED O DROPPED			
— —		Physical Hc Ob	servation Type	Transport Node	Component	
t1-router		0 4	Injected	esxi-02.corp.local	Network adapter 1	
web02	(D) db01	o 🖕	Received	esxi-02.corp.local	Distributed Firewall	
		0 3	Forwarded	esxi-02.corp.local	Distributed Firewall (Rule ID: 2)	
sxi-02.corp	kvm-02	0 3	Forwarded	esxi-02.corp.local	to web	
		o 🖕	Received	esxi-02.corp.local	🛞 t1-router	
		0 3	Forwarded	esxi-02.corp.local	log t1-router	
		o 🖕	Received	esxi-02.corp.local	⇔ db	
		0 3	Forwarded	esxi-02.corp.local	Remote IP : 192.168.210.101	
		1 4	Received	kvm-02	Remote IP : 192.168.210.104	
192.168.210.1 192.168.210.		1.4	Received	kvm-02	Distributed Firewall	
		1.13	Forwarded	kvm-02	Distributed Firewall (Rule ID: 2)	
		1 -	Delivered	kym-02	C db01/kym-02	

Figure 5-6: Traceflow output, delivered packet

In case of connectivity issues, the table of observations and the visual output may provide different information. In the example below, the diagram shows the physical and logical port connectivity between the source and destination workloads while Traceflow observations report that the packet being injected is being dropped by the distributed firewall rule ID 1031.



Source	Destination	RE-TRACE	EDIT NEW TRACE	)		
Virtual Machine web02	Virtual Machine db01					
P/MAC 172.16.10.12/00:50:56:b5:ff:cf	IP/MAC 172.16.30.11/52:54:00:8f:77:17					
race Results						
web	db	Show: ALI	O DELIVERED 1 DROPPED			
		Physical Ho	Observation Type	Transport Node	Component	
t1-router		0	Oropped by Firewall: 1031	esxi-02.corp.local	C web02/web02.vmx@9ccflabc-77_	
web02	db01					
ui 03	h== 01					
~~~~~						
(and)	(mm)					
192.168.210.1 192.168.210.1.	TN., URUNTUKVM					
11 - 1.00						

Figure 5-7: Traceflow output, distributed firewall dropping the packet

#### 5.4 IPFIX



IPFIX stands for IP Flow Information eXport and IP stands for Internet Protocol. It is a standard protocol for the format and export of network flow information, which is collected by a remote IPFIX collector which typically displays the information in an easy-to-understand way.

When IPFIX is enabled in NSX, all configured host transport nodes send IPFIX messages to the collectors using port 4739. For ESXi hosts, NSX automatically opens port 4739. For KVM hosts, NSX does not automatically open the port, admins must manually open port 4739.

NSX supports IPFIX for switches and firewalls as listed below:

• For switches, network flow at VIFs (virtual interfaces) and pNICs (physical NICs) is exported • For firewalls, network flow that is managed by the distributed firewall component is exported. Also, NSX permits the use of different IPFIX collectors and configuration profiles for both switches and firewalls.





vm NSX					۹	0	Ą	8
《 Dashboard >	SWITCH IPFIX COLLECTORS	SWITCH IPFIX PROFILES	FIREWALL IPFIX COLLECTORS	FIREWALL IPFIX PROFILES				
🖻 Tools 🗸 🗸	<ul> <li>Collectors (1)</li> </ul>					co	NFIGURE CO	LLECTORS
Port Connection	IP Address			Port				
Traceflow	192.168.110.10							4739
Port Mirroring Session	<ul> <li>Collection Options</li> </ul>							EDIT
IPFIX	Observation Domain ID 7							
vm NSX					۹	Ø	۵	٤
vm NSX «	SWITCH IPFIX COLLECTORS	SWITCH IPFIX PROFILES	FIREWALL IPFIX COLLECTORS	FIREWALL IPFIX PROFILES	۹	Ø	۵	٤
vm NSX « @ Dashboard >	SWITCH IPFIX COLLECTORS	SWITCH IPFIX PROFILES	FIREWALL IPFIX COLLECTORS	FIREWALL IPFIX PROFILES	۹	Ø	۵	٤
vm NSX ≪ ② Dashboard > Tools ∨	SWITCH IPFIX COLLECTORS	SWITCH IPFIX PROFILES	FIREWALL IPFIX COLLECTORS	FIREWALL IPFIX PROFILES	Q	Ø	۵	گ T
vm     NSX       ≪        Dashboard     >       Tools     ~       Port Connection	SWITCH IPFIX COLLECTORS	SWITCH IPFIX PROFILES	FIREWALL IPFIX COLLECTORS	FIREWALL IPFIX PROFILES	Q	Collecto	۵ r Count	ð
✓m NSX	SWITCH IPFIX COLLECTORS	SWITCH IPFIX PROFILES	FIREWALL IPFIX COLLECTORS	FIREWALL IPFIX PROFILES	۹	Collecto	Count Count	0
✓ ✓ NSX	SWITCH IPFIX COLLECTORS	SWITCH IPFIX PROFILES	FIREWALL IPFIX COLLECTORS	FIREWALL IPFIX PROFILES	Q	Collecto	Count	0

Figure 5-8: IPFIX configuration menus

Please check the NSX Administration Guide for further details about IPFIX configuration.

#### 5.5 Port Mirroring

NSX supports several types of port mirroring and offers flexibility for the admins to choose the one that fits better their troubleshooting/monitoring needs. NSX supports the following port mirroring types:

• **Local SPAN** – To be used when both NICs, source and destination of the mirroring session, are on the same Transport Node. It does support PNICs or VNICs as the source and only VNICs as the destination of the capture.

- **Remote SPAN** It offers two variants:
  - RSPAN Source Session Mirror network traffic from virtual machine interfaces to specific physical NICs over RSPAN VLAN IDs
  - RSPAN Destination Session Mirror network traffic from RSPAN VLAN IDs to specific virtual machine interfaces.

Both require the use of an Encapsulation VLAN ID, and the original VLAN of the traffic being captured and be preserved.

• **Remote L3 SPAN** – Forwards captured traffic to a remote IP address (destination server), encapsulated in one of the three following protocols: o GRE o ERSPAN type two o ERSPAN type three

Configuration options vary depending on the selected encapsulation mode.

• **Logical SPAN** – Source and destination of the traffic being capture must reside on the same NSX Logical Switch. This mode of SPAN continues to work even in the event of VM VMotions.

**Note:** Configuration options and restrictions may vary depending on the selected mirroring mode. Please check *NSX-T* Administration Guide for details.

All Port Mirroring configuration options are available under *Tools > Port Mirroring Session*.



vm NSX				
«	Port Mirroring Session	on		
Q Search		_		
② Dashboard	+ ADD - O EDIT	DELETE O ACTIONS	· ·	
Getting Started	Local SPAN	ID	Session Type	Sources
∨ 🖻 Tools	Remote L3 SPAN			140 3633
Port Connection	Logical SPAN			
Traceflow				
Port Mirroring Session				
IPFIX				

Figure 5-9: Configuring Port Mirroring Sessions

From the very same menu it is possible to review the details and/or delete the session once the relevant traffic has been captured.

Port	Mirroring Session					
+ AC	D - 🖉 EDIT 🗒 DELI	ETE 🔞 ACTIONS 🗸				
	Session Name	ID	Session Type	Sources	Destinations	Direction
	Local SPAN	c92f8a0e	Local Session	1 Port, 1 Pnic	1 Port	Bidirectional
	Logical SPAN	959d81f7	Logical Session	1 Port	1 Port	Bidirectional
	Remote L3 SPAN	e343e538	L3 Port Session	1 Port, 1 Switch	1 IP Address	Bidirectional
	Remote Source SPAN	77e1b31f	RSPAN Source	1 Port	1 Phic	Bidirectional

Figure 5-10: Reviewing Port Mirroring Sessions

#### 5.6 Packet Captures

In case of troubleshooting or monitoring requirements, it is possible to capture data plane packets on NSX Transport Nodes (i.e., Edges, KVM hosts, ESXi hosts).

On KVM and Edge node, there is a common command, *start capture*, that can be leveraged on those Transport Nodes, though options may vary depending on the node types.

kvm-01> star interface	t capture Interface configuration	nsxedge01> start capture interface Interface configuration
kvm-01>		nsxedge01>
	esxi-01.corp.local> sta dvfilter dvFilter m interface Interface trace Enable Pace esxi-01.corp.local>	art capture name configuration cket Capture Trace Mode

Figure 5-11: Packet Capture command outputs from different nodes

Packet capture commands allow to specify *expressions* or *parameters* so that only relevant traffic is captured.

On ESXi host, pktcap-uw is a powerful packet capture tool which captures packet at different points inside ESXi hosts and shows packet going through different processes on the data path.



[root@ESXi-133:~] pktcap-uwtracesrcip=192.168.100.143dstip=192.168.50.141vni=0										
06:03:48.654666[5] Captured at PktFree point, Drop Reason 'VXLAN Module Drop'. Drop Function 'VDL2UplinkInput'. TSO not enabled, Checksum not offloaded and verified, SourcePort 2214592562, VLAN tag 100, length 144.										
PATH:										
+- [06:03:48.654634] UplinkRcvKernel										
+- [06:03:48.654635]   (3) PortInput   2214592562										
+- [06:03:48.654635]   IOChain     FC_LookupInput@com.vmware.nsx.fc#1.1.7.0.16404614										
+- [06:03:48.654643]   IOChain     VDL2UplinkInput@com.vmware.nsx.12#1.1.7.0.16404614 (Decap/BFD Process)										
+- [06:03:48.654663]   (4) Drop										
+- [06:03:48.654665]   PktFree										
Segment[0] 9088 bytes:										
)x0000: 0050 56a8 0dc3 0050 566a 0761 0800 4500										
xx0010: 0082 0000 4000 4011 21fe c0a8 648f c0a8										
0x0020: 328d fa15 17c1 006e 9a93 0780 6558 0000										
0x0030: 0000 0104 0106 0021 7bf9 e708 5880 0000										
x0040: 0000 0000 0000 0000 0000 0000 000										
x0050: 56a8 0dc3 0050 566a 0761 0800 4500 0034										
x0060: 0000 0000 ff11 a34b c0a8 648f c0a8 328d										
x0070: c042 0ec8 0020 0000 20a0 0318 4fda 34f0										
x0080: f810 0c2e 0001 86a0 000f 4240 0000 0000										

Section 6.7 provides a packet capture case study with pktcap-uw.

Details of pktcap-uw can be found here, https://docs.vmware.com/en/VMwarevSphere/7.0/com.vmware.vsphere.networking.doc/GUID-5CE50870-81A9-457E-BE56C3FCEEF 3D0D5.html

Captures can be saved into a file that can be copied to the administrator station for further analysis with tools like Wireshark.

```
nsxedge01> start capture interface fp-eth0 file edge-capture-01.pcap
Capture to file initiated, enter Ctrl-C to terminate
^C
359 packets captured
359 packets received by filter
0 packets dropped by kernel
nsxedge01>
nsxedge01>
nsxedge01> get files
Directory of filestore:/
                 39413 May 30 2018 02:45:08 UTC backup_restore_helper.py
       -rw-
                 46010 Aug 08 2018 08:30:18 UTC edge-capture-01.pcap
24923 May 30 2018 02:45:08 UTC aggsvc_poll_intervals_change_helper.py
       -rw-
       -rw-
nsxedge01>
nsxedge01>
nsxedge01> copy file edge-capture-01.pcap url scp://admin@192.168.110.10/
admin@192.168.110.10's password:
nsxedge01>
```

Figure 5-12: Saving a Packet Capture to a file and copying it to a remote destination

	SFTP_Root		
e Share View			
C:\SFTP_Root			V C Sea
Name	Date modified	Туре	Size
🔚 edge-capture-01.pcap	8/8/2018 1:30 AM	Wireshark capture	45 KB
Eigung = 100 Declas	+ Cantuma file massined at a	nom ata daatin atian	

by Broadcom © VMware LLC.



Please check the latest VMware NSX-T Command Line Interface Guide available for further details.

#### 5.7 Case Study - Troubleshooting Tunnel Issue

In NSX-T, Geneve Tunnel is used to carry overlay traffic. The tunnel status needs to be up for the overlay packets to move between hosts and Edge nodes. Tunnel down is an often-seen issue. BFD is used to detect the tunnel status. We will first understand how BFD works then we are going to show how to troubleshoot the issue step by step through 2 case studies.

Tunnel Status:	ALL 1 UP	3 DOWN		Filter by	BFD Status:	ALL	~
Source IP	Remote IP	Status	BFD Diagnostic Code	Remote Transport Noc	Encap Interfac	Encap	Tunnel Name
192.168.100	192.168.50	• Down	0 - No Diagnostic	Edge7-141	vmk11	GENEVE	geneve32
192.168.100	192.168.50	• Down	0 - No Diagnostic	Edge7-151	vmk11	GENEVE	geneve32
192.168.100	192.168.10	• Up	0 - No Diagnostic	10.114.220.143	vmk11	GENEVE	geneve32
192.168.100	192.168.20	• Down	0 - No Diagnostic	10.114.220.233	vmk11	GENEVE	geneve32
					< BACK	NEXT >	1 - 4 of 4 records

#### Understand BFD

BFD is used to detect faults between VTEPs on two hosts or Edge nodes connected by the tunnel. BFD packet is encapsulated in GENEVE encapsulation with VNI 0.

After a BFD session is established, BFD control packets will be sent between two nodes periodically. If one side misses 3 consecutive BFD packets, the path will be marked down.

This is how BFD packet flow looks like. It helps to understand the state of the BFD session.







## Case Study – Working case Tunnel Between Two Hosts on the Same VTEP Vlan Setup



In this example, the VTEPs of ESXi Host-143 and ESXi Host-133 are on the same vlan and the tunnel is working fine. Here we provide a working packet capture to show how the correct packets look like at each point.

First, we identify the collecting points where we want to capture the packets. In this case, we will be capturing the packet at bule 1, 2, 3 and 4 and green 1, 2, 3 and 4.

On the source host, the original BFD packet can be captured at point 1, the encapsulated BFD packet can be captured at point 2.



On the destination host, the encapsulated BFD packet can be captured at point 3, the encapsulated BFD packet can be captured at point 2.







#### Similar packet trace for the other direction.







	[root@ESXi-133:-] pktcap-uwuplink vmnic0capture PortOutput -o -ltcpdump-uw -enr -   grep BFD   grep 143 11:55:18.250113 00:50:56:6e:fa:f4 > 00:50:56:6a:07:61, ethertype IPv4 (0x0800), length 66: 192.168.100.133.49167 > 192.168.100.143.3784: BFDv1, Control, State Up, Flags: [none], length: 24
2	[root@ESXi-133:-] pktcap-uwuplink vmnic0capture PktFree -o - tcpdump-uw -enr -   grep BFD   grep 143
0	07:54:41.550220 00:50:56:6e:fa:f4 > 00:50:56:6a:07:61, ethertype IPv4 (0x0800), length 144: 192.168.100.133.61555 > 192.168.100.143.6081: Geneve, Flags [O], vni 0x0, proto TEB (0x6558), options [28 bytes]: 00:50:56:6e:fa:f4 > 00:50:56:6a:07:61, ethertype IPv4 (0x0800), length 66: 192.168.100.133.49167 > 192.168.100.143.3784: BFDv1, Control, State Up, Flags: [none], length: 24
(3)	[root@ESXi-143:-] pktcap-uwuplink vmnic0capture Portinput -o - tcpdump-uw -enr -   grep BFD   grep 133
)	07:58:24.981816 00:50:56:6e:fa:f4 > 00:50:56:6a:07:61, ethertype IPv4 (0x0800), length 144: 192.168.100.133.61555 > 192.168.100.143.6081; Geneve, Flags [O], vni 0x0, proto TEB (0x6558), options [28 bytes]: 00:50:56:6e:fa:f4 > 00:50:56:6a:07:61, ethertype IPv4 (0x0800), length 66: 192.168.100.133.49167 > 192.168.100.143.3784; BFDv1, Control, State Up, Flags: [none], length: 24
(4)	[root@ESXi-143:-] pktcap-uwuplink vmnic0capture PktFree -o -ltcpdump-uw -enr -   grep BFD   grep 133
0	12:06:55.033190 00:50:56:6e:fa:f4 > 00:50:56:6a:07:61, ethertype IPv4 (0x0800), length 66: 192.168.100.133.49167 > 192.168.100.143.3784: BFDv1, Control, State Up, Flags: [none], length: 24

## Case Study – nonworking case Tunnel Between Edge and Nested Host

- Edge Node is on a Transport Node, a router VM is workload VM on another Transport Node.
- Edge TEP is vlan 50 and TN TEP is vlan 100
- vmkping works between the EN TEP an TN TEP







Tunnel down most often is caused by underlay IP connectivity issue, invalid setup or realization issue. In both cases, we can identify the issue by looking at BFD status, capturing BFD packet and checking corresponding log. The following case is an example of invalid setup. The Edge VM is on a Transport Node ESXi-143. The VTEP of the Edge VM is in Vlan50, the VTEP of the Transport Node is in Vlan100. A Router VM is on Transport Node ESXi-133 whose VTEP is also in Vlan100. The tunnel between Edge node and Transport Node 143 is down. The trace shows the BFD packet from Edge Node 141 can reach Transport Node 143 but not the other way around. The reason is that the BFD packet sending from ESXi-143 is going to a VTEP in Vlan50, but Transport Node ESXi-133 doesn't have a VTEP in Vlan50, so the BFD packet is dropped by the VxLAN module.

There are troubleshooting steps to identify the issue,

1<sup>st</sup>, To verify IP connectivity between TEPs with vmkping. vmkping ++netstack=vxlan 192.168.50.141

Notes: MTU issue could impact workload traffic but it will NOT cause the tunnel in down state

2<sup>nd</sup>, check BFD session status:

On Edge Node:

#### Edge7-141> get bfd-sessions | find Dest\_port|Encap|address|State

Dest_port	: 4784
Encap	: vlan
Local_address	: 192.168.50.141
Remote_address	: 192.168.50.151
State	: up
Dest_port	: 3784
Encap	: geneve
Local_address	: 192.168.50.141
Remote_address	: 192.168.100.143
State	: down

On Transport Node:

[root@ESXi -133:~] nsxdp-cli bfd sessions list





Remote	Loc	cal	local_d	isc remote	_disc recvd _s	sent loca	al_state	local_diag	client flap	192	.168.100.133
e60e03bb	0	0	134981	down	No Diagnostic	vdl2 C	S				
192.168.50.1	41										
192.168.200.	233	192.168	8.100.133	b9c7 ec6f	abc5507a	135106	179012	init	No Diagnostic	vdl2	0
192.168.100.	143	192.168	8.100.133	ba50e211	8757285e	41400	41392	up	No Diagnostic	vdl2	1
192.168.50.1	51	192.168	8.100.133	58143144	555005d8	141350	134938	init	No Diagnostic	vdl2	0

From the BFD session state, you can tell the which side doesn't receive expected the BFD packets. The "init" of the local\_state means the node has received the BFD packet from the remote peer, the "down" of local\_state means the node didn't receive any BFD packet from the remote peer.

#### 2<sup>nd</sup>, Trace BFD packet

Identify the capture point for BFD packet from Edge-141 to ESXi-143. This is the working direction.











[root@ESXi-143:~] pktcap-uwtracesr	cip=192.168.50.141dstip=192	.168.100.143vni=0
13:17:05.111415[14] Captured at PktFree 100, length 66. PATH:	point, TSO not enabled, Checks	um not offloaded and verified, SourcePort 2315255859, VLAN tag
+- [13.17.05 111404]	UnlinkBoyKernel	
	BortTorut   2215255950	(mpi c0)
	(10) FOI CINPUC   2313233839	
+- [13:17:05.111404]	IOChain	FC_LookupInput@com.vmware.nsx.ic#1.1.7.0.16404614
+- [13:17:05.111406]	IOChain	VDL2UplinkInput@com.vmware.nsx.12#1.1.7.0.16404614 (decap)
+- [13:17:05.111414]	(11) PktFree	
Segment[0] 9038 bytes:		
0x0000: 0050 566a 0761 0000 0000 0000 0	800 45c0	
0x0010: 0034 328d 0000 ff11 6ffe c0a8 3	28d c0a8	
0x0020: 648f ede3 0ec8 0020 3e5f 2040 0	318 f810	ECVI 142
0x0030: 0c2e 0000 0000 000f 4240 000f 4	240 0000	ESXI-143
0x0040: 0000		

#### Packets captured at each point:

	Edge7-141> start capture interface fp-ethO
	15:04:35.260449 00:50:56:a8:e5:4f > 00:50:56:a8:89:e0, ethertype IPv4 (0x0800), length 116: 192.168.50.141.34154 > 192.168.100.143.6081; Geneve, Flags [O], vni 0x0, proto TEB (0x6558): 00:00:00:00:00:00:00 > 00:00:00:00:00:00; ethertype IPv4 (0x0800), length 66: 192.168.50.141.60899 > 192.168.100.143.3784; BFDv1, Control, State Down, Flags: [none], length: 24
2	[root@ESXI-143:-] pktcap-uwuplink vmnic0capture PortOutput -o -ltcpdump-uw -enr -   grep BFD   grep 141
	12:34:55.119271 00:50:56:a8:e5:4f > 00:50:56:a8:89:e0, ethertype IPv4 (0x0800), length 116: 192.168.50.141.34154 > 192.168.100.143.6081; Geneve, Flags [O], vni 0x0, proto TEB (0x6558): 00:00:00:00:00:00:00:00:00:00:00:00:00
(3)	[root@ESXi-143:-] pktcap-uwuplink vmnic0capture PktFree -o -[tcpdump-uw -enr -   grep BFD   grep 141
)	12:38:40.061321 00:50:56:a8:e5:4f > 00:50:56:a8:89:e0, ethertype IPv4 (0x0800), length 116: 192.168.50.141.34154 > 192.168.100.143.6081: Geneve, Flags [O], vni 0x0, proto TEB (0x6558): 00:00:00:00:00:00:00:00:00:00:00:00:00
(4)	[root@ESXi-133:-]pktcap-uwUplink vmnicOcapture PortInput -o - tcpdump-uw -enr -   grep BFD   grep 141
	12:45:28.456375 00:50:56:a8:e5:4f > 00:50:56:a8:89:e0, ethertype IPv4 (0x0800), length 116: 192.168.50.141.34154 > 192.168.100.143.6081: Geneve, Flags [O], vni 0x0, proto TEB (0x6558): 00:00:00:00:00:00:00 > 00:00:00:00:00:00; ethertype IPv4 (0x0800), length 66: 192.168.50.141.60899 > 192.168.100.143.3784: BFDv1, Control, State Down, Flags: [none], length: 24
5	[root@ESXi-133:-] pktcap-uwswitchport 67108956capture PortOutput -o - tcpdump-uw -enr -   grep BFD   grep 141
	12:47:08.640814 00:50:56:a8:e5:4f > 00:50:56:a8:89:e0, ethertype IPv4 (0x0800), length 116: 192.168.50.141.34154 > 192.168.100.143.6081: Geneve, Flags [O], vni 0x0, proto TEB (0x6558): 00:00:00:00:00:00:00:00:00:00:00:00:00

Notes: the packet is coming on vlan 50, Host133's TEP is on vlan 100, so the packet will not get decapsulated



Flags: [none], length: 24

vvatta@vvatta:~\$ monitor interfaces ethernet eth3 traffic 192.168.50.141 -> 192.168.100.143 UDP Source port: 34154 Destination port: 6081 vyatta@vyatta:~\$ monitor interfaces ethernet eth2 traffic 192.168.50.141 -> 192.168.100.143 UDP Source port: 34154 Destination port: 6081 [8] [root@ESXI-133:~] pktcap-uw --switchport 67108955 --capture PortInput -o -ltcpdump-uw -enr - | grep 141 13:24:57.977701 00:50:56:a8:0d:c3 > 00:50:56:6a:07:61, ethertype IPv4 (0x0800), length 116: 192.168.50.141.34154 > 192.168.100.143.6081: Geneve, Flags [O], vni 0x0, proto TEB (0x6558): 00:00:00:00:00:00:00:00:00:00:00; ethertype IPv4 (0x0800), length 66: 192.168.50.141.60899 > 192.168.100.143.3784: BFDv1, Control, State Down, Flags: [none], length: 24 (9) [root@ESXi-133:-] pktcap-uw --uplink vmnicO --capture PortOutput -o -ltcpdump-uw -enr - | grep 141 13:30:44.864447 00:50:56:a8:0d:c3 > 00:50:56:6a:07:61, ethertype IPv4 (0x0800), length 116: 192.168.50.141.34154 > 192.168.100.143.6081: Geneve, Flags [O], vni 0x0, proto TEB (0x6558): 00:00:00:00:00:00:00 > 00:00:00:00:00:00:00; ethertype IPv4 (0x0800), length 66: 192.168.50.141.60899 > 192.168.100.143.3784; BFDv1, Control, State Down, Flags: [none], length: 24 (io) [root@ESXi-143:-] pktcap-uw --uplink vmnic0 --capture PortInput -o -ltcpdump-uw -enr - | grep BFD | grep 141 13:37:04.764773 00:50:56:a8:0d:c3 > 00:50:56:6a:07:61, ethertype IPv4 (0x0800), length 116: 192.168.50.141.34154 > 192.168.100.143.6081: Geneve, Flags [O], vni 0x0, Down, Flags: [none], length: 24 (1) [root@ESXi-143:-] pktcap-uw --uplink vmnicO --capture PktFree -o -ltcpdump-uw -enr - | grep BFD | grep 141 13:30:47.965663 00:00:00:00:00:00:00 > 00:50:56:6a:07:61, ethertype IPv4 (0x0800), length 66: 192.168.50.141.60899 > 192.168.100.143.3784: BFDv1, Control, State Down,

#### Identify the capture point for the BFD packet from ESXi-143 to Edge-141. This is the non-working direction.





## Packet captured at each point

	[root@ESXI-143:~] pktcap-uwuplink vmnic0capture PortOutput -o -ltcpdump-uw -enr -   grep 141   grep BFD
	08:53:49.985612 00:50:56:6a:07:61 > 00:50:56:a8:0d:c3, ethertype IPv4 (0x0800), length 66: 192.168.100.143.49218 > 192.168.50.141.3784: BFDv1, Control, State Init, Flags: [Poll], length: 24
2	[root@ESXI-143:-] pktcap-uwuplink vmnic0capture PktFree -o - tcpdump-uw -enr -   grep 141   grep BFD
	08:55:12.985648 00:50:56:6a:07:61 > 00:50:56:a8:0d:c3, ethertype IPv4 (0x0800), length 144: 192.168.100.143.64021 > 192.168.50.141.6081: Geneve, Flags [O], vni 0x0, proto TEB (0x6558), options [28 bytes]: 00:50:56:6a:07:61 > 00:50:56:a8:0d:c3, ethertype IPv4 (0x0800), length 66: 192.168.100.143.49218 > 192.168.50.141.3784: BFDv1, Control, State Init, Flags: [Pol], length: 24
(3)	[root@ESXI-133:-] pktcap-uwuplink vmnic0capture PortInput -o - tcpdump-uw -enr -   grep 141   grep BFD
)	08:56:55.658306 00:50:56:6a:07:61 > 00:50:56:a8:0d:c3, ethertype IPv4 (0x0800), length 144: 192.168.100.143.64021 > 192.168.50.141.6081: Geneve, Flags [O], vni 0x0, proto TEB (0x6558), options [28 bytes]: 00:50:56:6a:07:61 > 00:50:56:a8:0d:c3, ethertype IPv4 (0x0800), length 66: 192.168.100.143.49218 > 192.168.50.141.3784: BFDv1, Control, State Init, Flags: [Poll], length: 24
4	[root@ESXi-133:~] pktcap-uwuplink vmnic0capture Dropdir 0stage 0 -o -   tcpdump-uw -enr -   grep 192.168.100.143
	19:14:25.516900 00:50:56:6a:07:61 > 00:50:56:a8:0d:c3, ethertype IPv4 (0x0800), length 144: 192.168.100.143.60247 > 192.168.50.151.6081: Geneve, Flags [0], vni 0x0, proto TEB (0x6558), options [28 bytes]: 00:50:56:6a:07:61 > 00:50:56:a8:0d:c3, ethertype IPv4 (0x0800), length 66: 192.168.100.143.49194 > 192.168.50.151.3784: BFDv1, Control, State Init, Flags: [Poll], length: 24

3<sup>rd</sup>, Checking BFD counter and corresponding log



NSX-T 3.0: Operation Guide

#### BFD packet drop counter:

```
[root@ESXi-133:~] net-vdl2 -S -s VDS7 | grep drop
tx.drop.invalidFrame: 0
tx.drop.guestTag: 0
tx.drop.insertGuestVlan: 0
tx.drop.noResource: 0
tx.drop.invalidState: 0
rx.drop.invalidFrame: 0
rx.drop.removeGuestVlan: 0
rx.drop.notExist: 0
rx.drop.noResource: 0
rx.drop.reassembly: 0
rx.drop.reachedMaxFragsLimit: 0
rx.drop.invalidSourceIP: 0
rx.drop.invalidSourceMAC: 0
rx.drop.invalidDestIP: 0
bfd.tx.drop.total: 0
bfd.rx.drop.total: 1009331 <-- incrementing
```

#### Vmkernel.log contains BFD log information:

```
[root@ESXi-143:~] net-vdl2 -L log
Log level: 0
[root@ESXi-143:~] net-vdl2 -L log 2
[root@ESXi-143:~] net-vdl2 -L log
Log level: 2
[root@ESXi-133:~] tail -f /var/log/vmkernel.log | grep -i vdl2
2020-06-30T12:47:32.438Z cpu43:2098287) VDL2DecapBFDPktGeneve:2050:[nsx@6876 comp="nsx-esx"
subcomp="vdl2-16404614" errorCode="ESX177"][switch:DvsPortset-2] Wrong Destination : No underlying
device for major,minor
[root@ESXi-143:~] net-vdl2 -L log 0
```

#### 5.8 vRealize Network Insight

This section demonstrates how to use Network Insight to monitor and troubleshoot NSX.

To monitor NSX, the NSX manager dashboard shows of the events, properties, topology information of NSX management cluster.







The events are detected with the predefined health check rules. The health checklist was developed from the operational perspective based on common issues in customer deployments of NSX. Among those rules, some of them are computed by vRNI independently, while others are the result of querying NSX alarms with API. The alarm natively generated by NSX are all in NSX-T System Event.

15 eve	ents EXPAND ALL COLLAPSE AI	L \$	
	NSX-T System Event [4 events - Show all] Edge NIC Link Status Down Severity: Critical Manager: 10.114.220.140 Defined By: System Event tags: NSX-T NSX-T manager:	2 days	
	One or more Fabric Nodes are added as standalone hosts in NSX-T		
	E One or more Fabric Nodes are added as standalone hosts in NSX-T. Virtual Machines on those hosts will not be visible in vRh	25 days	
	NSX-T System Event [5 events - Show all]		
	Manager Disk Usage High Severity: Warning Manager: 10.114.220.140 Defined By: System Event tags: NSX-T NSX-T manage	33 days	
	SNMP Service has stopped		
	$\pm$ One of the Services of the NSX-T Management Node, namely SNMP Service has stopped running.	33 days	
	NSX-T MP Node Liagent service has stopped [2 events - Show all]		
	One of the Services of the NSX-T Management Node, namely LI Agent Service has stopped running. Severity: Warning Man	33 days	
	SNMP Service has stopped		
	$oxed{H}$ One of the Services of the NSX-T Management Node, namely SNMP Service has stopped running.	33 days	
	NSX-T is not scheduled for backup		
	T Manager backup is not scheduled.		

We can view event details and configure how the notification should be sent out either via email or SNMP.





To send notification for the event computed by vRNI, click on more Option, then Edit Event. You can simply Enable Notification for this specific event.

SNMP Service has stopped			
One of the Services of the NSX-	I Management Node, namely SNMP Service has stopped running.	33 days	
NSX-T MP Node Liagent servi	ce has stopped [2 events - Show all]	Edit event	
One of the Services of the NSX-T	Management Node, namely Ll Agent Service has stopped running. Severity: Warning	Archive	
One of the s Description stopped rur	Services of the NSX-T Management Node, namely SNMP Service has nning.		
Type Problem			
Event tags	restore defaults		
Severity Warning	restore defaults		
Include/Exclude entities Event generation can be partially enabled	d/disabled on selected entities		
	EXCLUSION LIST		
Conditions * NSX-T Ma	anagement Node 🗸 nsx-mgr-137,	1	
Add anoth	er Condition		
Enable Notifications Configure when the notifications should I	be sent		
Email frequency	Never V		
Send notification emails to:	shiji@vmware.com		
To send SNMP trap, Configure SNMP	Trap C <sup>2</sup>		
SUBMIT CANCEL			

To enable notification for a specific event in NSX-T system Events, search the event first then create the notification.



NSX-T System Event [4 events - Collapse]		
Edge NIC Link Status Down	2 davs	
Severity: Critical		
Manager: 10.114.220.140		
Defined By: System		
Event tags: NSX-T		
NSX-T manager: 10.114.220.140		
Source Component: Edge7-141		
NSX-T Event Type: edge_nic_link_status_down		
Status: OPEN		
Message: Edge node NIC fp-eth2 link is down.		
Created at: Aug 22, 16:27		
Last Modified at: Aug 22, 18:57		
Recommendation: On the Edge node confirm if the NIC link is physically down by invoking the NSX CLI command `get		
interfaces`. If it is down, verify the cable connection.		
<ul> <li>Manager Memory Usage High</li> <li>Severity: Warning</li> <li>Manager: 10.114.220.140</li> <li>Defined By: System</li> <li>Event tags: NSX-T</li> <li>NSX-T manager: 10.114.220.140</li> <li>Source Component: nsx-mgr-147</li> <li>NSX-T Event Type: manager_memory_usage_high</li> <li>Status: OPEN</li> <li>Message: The memory usage on Manager node 068894d9-3cb5-4d1e-9501-761e56632ca9 has reached 82% which is at or above the high threshold value of 80%.</li> <li>Created at: Aug 22, 17:17</li> <li>Last Modified at: Aug 22, 17:17</li> </ul>	2 days	
Recommendation: Please review the configuration, running services and sizing of this Manager node. Consider adjusting the		
Manager appliance form factor size.		

# For example, to create notification for the link down event on Edge node 141, we search the event first, nsx-t event where Problem Entity = 'Edge7-141' and Event Codes =

✓ nsx-t event	where Problem Entity = 'Edge7-141' and Event Codes = 'edge_nic_link_status_down'	x
Showing 1 result for NSX-T Event w	here Problem Entity = 'Edge7-141' and Event Codes = 'edge_nic_link_status_down' over time ra	ange Aug 24, 16:33 - Aug 25, 16:33 🍂 🍂 🕄
Sort		EXPAND ALL COLLAPSE ALL
Select an option 🛛 🗸 Dsc 🗸	NSX-T System Event	
Filters	Edge NIC Link Status Down Severity: Critical Manager: 10.114 220.140	3 days :
ADD MORE FILTERS	Defined By: System Event tags: NSX-T NSX-T manager: 10.114.220.140	Create alarm
	Source Component: Edge7-141	
Edge7-141 (1)	NSX-1 Event Type: edge_nic_link_status_down Status: OPEN Message: Edge node NIC fp-eth2 link is down.	
Vendor Event ID	Created at: Aug 22, 16:27 Last Modified at: Aug 22, 18:57 Decommendation: On the Edge and confirm if the NIC link is physically down by investiga the NIC	V CI I command 'act interfaces'. If it is down, work the
▶ Status	cable connection.	A CLI Command ger internaces . In it is dowin, verny the
▶ Archived		
▶ Severity		
Event Tags / Category		
Defined By		
▶ Manager 🖸		

This is email notification that you will receive:



[vRNI Event] Edge-141 Link Down	
VRNI@vmware.com <vrni@vmware.com> To: 0 Jing Shi</vrni@vmware.com>	Sunday, August 23, 2020 at 3:18 PM
VMware vRealize Network Insight	
Event Notification	
Edge-141 Link Down - 1 events Event Search: nsx-t event where event codes = "edge_nic_link_status_down" and problem entity = 'edge7-141' returned 2 results Changes: added NSXTSystemEvent, NSXTSystemEvent Severity: Info Defined By: User	Aug 23, 19:17
You can configure email frequency and other options on the <u>Settings Page.</u>	

The complete list of events being monitored by vRNI is here:

https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.0/administration/GUID-7E5F74FB14A5-41B9-B806-E6B9AC30BF00.html





## Appendix

#### i. Remote User Authentication and RBAC

NSX-T appliances have two built-in local users—admin and audit. Users cannot create additional local users. However, user can leverage their existing directory services to add remote users and assign role-based Access Control (RBAC) to the NSX-T management.

NSX-T provides the following options for remote authentication:

1- Integration with VMware Identity Manager (vIDM) / VMware Workspace One 2- Direct integration with LDAP server – Microsoft Active Directory (AD) or OpenLDAP.



Figure 0-1 RBAC

The NSX-T integration with VIDM/LDAP enables remote users from the organization's user directory service to be mapped to a predefined RBAC role on NSX-T. NSX-T has 11 predefined RBAC roles across different feature verticals with NSX, as shown in the following table.



RBAC Role	Permission
Enterprise Administrator	Super user; full access on all
Network Engineer	Full access on networking services, e.g. switching & routing
Network Operator	Read access on networking services, with the permission to run monitoring & trouble shooting tools
Security Engineer	Full access on security features.
Security Operator	Read access on security services, with the permission to run monitoring & trouble shooting tools
Load Balancer Admin	Full access to Load Balancer configuration
Load Balancer Auditor	Read access to Load Balancing Configuration
Auditor	Read access on all
NETX Partner Admin	Network Introspection workflow and policy.
GI Partner Admin	Guest Introspection workflow and policy.
VPN Admin	VPN workflow admin.

As an organization, you can leverage either of these remote authentication options based on your requirements. Direct LDAP integration is a straightforward option to operate, as you can leverage existing LDAP servers directly for NSX-T management. However, VIDM integration requires VIDM platform deployment on top of your existing directory service for user authentication. However, VIDM integration provides additional directory service options (in addition to AD & Open LDAP) and more advanced remote authentication options like 2-factor authentication, Single Sign-On, etc.

The following section covers More details for each of the options.

#### i. Direct Integration with LDAP Server (AD/OpenLDAP) for RBAC

The NSX direct LDAP integration provides a simple and easy to operate option for remote authentication and can be enabled using the following simple steps:

- 1. Add Identity Source with Domain Name, Type, Base DN and Associated LDAP Server
- Supports LDAP, LDAPS & 'startTLS' over LDAP.
- Three Identity Source/Domain supported.
- Granular Base DN options

密し	JSERS ROLES LDAP V	MWARE IDENTITY MANAGER			
ADD Maxim	IDENTITY SOURCE	3 Identity Source	e/Domain supported.		1 LDAP server per domain. LDAP Server HA is done from
	Name	Domain Name	Туре	LDAP Servers	the server side.
	NSXLAB-AD	nsxad.com Brample: vmware.com	Active Directory over LDAP	1 Set LDAP	Server met-ab 01 (Midaa berwer )
	Base DN	OU=IT,DC=nsxad,DC=com		Descript no	autranal9 LB4P Police D44 2016 Put Consultan Salaa D44 2016 2009 ar Chark Michae 0 Chark Michae
	SAVE CANCEL	Brample: CN=Users.DC=VMware.DC=	com	a Q a	in turns Star The contract
1	> VMware-AD	vmware.com	Active Directory over LDAP	1	ne Genergy Administration (dimonal cont and caucify another a samely the statigated fame



.

- 2. Assign RBAC Role to the "users or groups" from the configured domain
- Search for LDAP users/group by Typing in 3 characters
- User can have more than one RBAC role assigned, E.g., Network Engineer & LB Admin

2	榕 USERS ROLES LD	AP VM	NA	RE IDENTITY MANA	AGER	
	ADD ~					
Ð	Role Assignment for VIDM	_		Notice Security	Role	2
3	Role Assignment for LDAP	X	Home	Networking Security	inventory Plan & Troubleshoot System	n
1	Principal Identity with Role	G	6	器 USERS ROLES LDAF	VMWARE IDENTITY MANAGER	
>	globalmanageridentity	G	0	User/User Group Name		Roles
7	i localmanageridentity	G 	2	NSXLAB-AD 🛞 👻	nsx v *	Network Engineer X Select Roles
			7	: 🖄 admin	은 nsx-net-admin-01@nsxad.com	nterprise Admin
		0	1	i audit	A nsx-sec-admin-01@nsxad.com	Nuditor
				8 bhatg@vmware.com	CN=nsx sec admin 01,OU=IT,DC=nsxad,DC=com	nterprise Admin
				globalmanageridentity	CN=nsx-net-admins,OU=IT,DC=nsxad,DC=com	nterprise Admin
		6	9	localmanageridentity	答 nsx-sec-admins@nsxad.com	uditor

Once a remote user or user group has been assigned with the RBAC role, the User can now use UI or API to manage and operate NSX-T.

VMware® NSX-T™	1- User logs in with domain name.
	2- NSX Manger sends bind request to associated domain LDAP server.
nsx-net-admin-01@nsxad.com	3- Bind Response will have AuthN Success or Failure.
	4- NSX Manager provides appropriate access privilege based on assigned role for the user or group.
Loo IN VMware® NSX-T™	LDAP bind request LDAP bind response
admin	
LOG IN	

#### ii. Integration with vIDM for RBAC

NSX-T integration with vIDM provides following benefits related to user authentication:

- Support for extensive AAA Systems, including o AD-based LDAP, OpenLDAP
  - RADIUS
  - SmartCards / Common Access Cards o RSA Secure ID

• Enterprise Single Sign-On o Common authentication platform across multiple VMware solutions o Seamless single sign-on experience

This section covers the main steps on NSX-T to integrate with vIDM and to configure roles that grant different privileges to different users/groups. However, this does not cover the deployment or configuration of VMware Identity Manager. Please refer to VIDM document for details.





Assuming that both NSX-T Manager and vIDM appliances are deployed, powered on and configured with the basic management details (IP address, admin users, etc.), the integration requires the following steps:

On VIDM Platform:

- 1. Creating an OAuth client ID for the NSX-T Manager.
- 2. Get the vIDM appliance thumbprint.
- 3. Add an Active Directory (AD) server to vIDM as a user directory service.

On NSX-T Manager:

4. Register NSX-T Manager with vIDM using the OAuth client ID created 5. **Assign RBAC Role** to the "users or groups" from the configured domain.

#### (ii) Registering NSX-T Manager with vIDM using the OAuth client ID created

Once the OAuth Client ID, Shared Secret and the vIDM thumbprint are available, **NSX-T Manager can be registered with vIDM** using following UI workflow:

1. Navigate to System -> Users and Roles -> VMWARE IDENTITY MANAGER 2. Click on the *EDIT* top right corner to register NSX-T manager with VIDM.



Enabling vIDM on NSX-T

- 3. On the window that pops-up:
- Enable VMware Identity Manager Integration
- Enter the FQDN of the vIDM appliance
- Enter the OAuth Client ID created in vIDM previously
- Enter the Shared Secret associated with the OAuth Client ID
- Enter the SHA-256 thumbprint of the vIDM appliance obtained previously
- Enter the FQDN of the NSX-T Manager appliance Click on Save





Integration			
VMware Identity Manager			
VMware Identity Manager	colo-vshield3-dhcp168.eng.vmware.co	*	
Appliance	Enter Fully Qualified Domain Name (FQDN) e.g		
	identity.domain.com		
OAuth Client ID	NSX_client_credentials_client_ID		
OAuth Client Secret		*	
SSL Thumbprint	BF838E7A1CF7B84F7B556F35E0D9A	*	
NSX Appliance	nsx-mgr.corp.local	*	
	Fully Qualified Domain Name (FQDN) is		
	recommended e.g. policy.domain.com		

Configuring vIDM on NSX-T

**Note:** What is entered on the NSX Manager Appliance field must be used for accessing NSX after the integration. If the FQDN is used but then try to access the NSX Manager through its IP address, remote user authentication will fail with a "Must provide a *matching redirect uri*" error message.

4. Back on the Configuration window, vIDM connection shows as Up and vIDM Integration as Enabled as shown in figure below.

ŝ	USERS	ROLES	LDAP	VMWARE IDENTITY MANAGER
/M	ware Ide	ntity Mana	ager	
	External Loa	ad Balancer Ir	ntegration	Disabled
	VMware Ide	entity Manage	er Connectio	n 🕒 Up
	VMware Ide	entity Manage	r Integration	Enabled
	VMware Ide	ntity Manage	r Appliance	colo-vshield3-dhcp168.eng.vmware.com
	OAuth Clien	it ID		NSX_client_credentials_client_ID
	NSX Applia	nce		nsx-mgr.corp.local

NSX-T to vIDM Connection Up

5. At this point, there is a successful communication between the NSX-T Manager and the vIDM appliance.

(iii) Configuring different roles in NSX-T for the users retrieved from AD via vIDM

Once vIDM has retrieved the specified users from Active Directory, we can assign them different roles in NSX. For that:

1. On the NSX-T Manager UI, navigate to System -> User and Roles, and select the Users Click on the ADD -> Role Assignment for VIDM



ත් USERS	ROLES	LDAP	VMWARE IDENTITY MANAGER
ADD ~			
Role Assignm	ent for VID	м	
Role Assignm	ient for LDA	P	

NSX Users Role Assignments

2. On the window that pops-up, select a remote user or group to be assigned a role. Typing in minimum three characters under user/Group, would automatically query configured VIDM/AD to get all possible user/group matching the given string. Select the user/group to assign one or more roles from the list. Click Save when finished.

l	Jser/User Group Name	Roles
	clay	V * Network Engineer X
ſ	<pre>     clay_user_VPN@testad3.local     clay_user_VPN clay_user_VPN_ln </pre>	Select Roles
	<pre>&amp; clay_user_Nl@testad3.local clay_user_Nl clay_user_Nl_In</pre>	Enterprise Admin
ĺ	<pre>clay_use, clay_user_Ni@testad3.local clay_user_LBAU_fn clay_user_LBAU_In</pre>	Auditor
	clay_user_EA@testad3.local clay_user_EA_fn clay_user_EA_In	Enterprise Admin
1		Auditor
	Clay_user_SE@testad3.local       clay_user_SE_fn clay_user_SE_n        Clay_user_SO@testad3.local       clay_user_SO_fn clay_user_SO_in	Auditor

NSX VIDM users Role assignment

3. Repeat the process to assign roles to more users and/or groups

User/User Group Name     Roles     Type       i     & admin     Enterprise Admin     Local User       i:     & audit     Auditor     Local User       i:     & bhatg@vmware.com     Enterprise Admin     LDAP User       i:     & clay_user_Ni@testad3.local     Network Engineer.     VIDM User	?
User/User Group Name         Roles         Type           I:         & admin         Enterprise Admin         Local User           I:         & audit         Auditor         Local User           I:         & bhatg@vmware.com         Enterprise Admin         LDAP User           I:         & clay_user_Ni@testad3.local         Network Engineer         VIDM User	
Admin     Enterprise Admin     Local User       Auditor     Local User       Auditor     Local User       Abstg@vmware.com     Enterprise Admin       Auditor     LDAP User       Action     Retwork Engineer	
Auditor     Local User       bhatg@vmware.com     Enterprise Admin     LDAP User       clay_user_Ni@testad3.local     Network Engineer     VIDM User	
& bhatg@vmware.com     Enterprise Admin     LDAP User       & clay_user_Ni@testad3.local     Network Engineer     VIDM User	
: A clay_user_Ni@testad3.local Network Engineer VIDM User	
globalmanageridentity Enterprise Admin Principal Identity	User
Le localmanageridentity Auditor Principal Identity	User

Configured Users with Role assignment

**Note:** Privileges are calculated per feature. Users with no explicit role assigned will inherit the role(s) of their group. Users with explicit roles assigned enjoy the highest privileges of any of them. A detailed list of Roles and Permissions is available on the <u>NSX-</u><u>T Admin Guide</u>.





- 4. Log out from the NSX web interface.
- 5. After integration with vIDM, the NSX-T login page redirects to Workspace login page. Login with remote user with correct system domain.

	Workspace ONE*
use cla	ername y_user_NI@testad3.local
pa	ssword
	testad3.local
	Sign in
	Forgot password?
	Change to a different domain

Login into NSX with a remote user

6. Once authentication is successful, the user is taken to the NSX home page.



Successful Remote User login





#### ii. NSX Certificate management

As part of security compliance many organizations want to replace certificates with organization's CA signed certificate on all of the systems/devices/appliances deployed in their environment.

This section will cover what are the different NSX-T platform certificates and how these can be replaced with CA signed certificate for compliance adherence.

#### **NSX Certificates Type**

NSX uses multiple self-signed certificate (X509 RSA 2048/SHA256) for both External & Internal communication. Only, External (UI/API) & Inter-site certificates (NSX federation) can be replaced by user (API only) with another o Self-Signed-Cert on NSX

o Imported Certificates signed by CA

**NSX Internal certificates** are not exposed or replaceable by user with NSX-T 3.0 release. The following Figure provides the list of External certificates and its details for a given three node NSX Manager cluster.



On a standalone NSX manager cluster you would have following certificates exposed to user and can be replaceable:

- NSX Manager Cluster/VIP certificate- Used with Cluster Virtual IP and one certificate per Cluster.
- NSX Manager Node certificate This is used with individual Manager node IP and will be one per manager node.

The other two certs shown are used with NSX Federation solution. However, this is exposed on a standalone NSX manager as well, which do not have to be part of Federation. These certificates are not used in a non-federated environment.

- NSX Federation PI (Principal Identity Cert)- This is used between NSX Global manager and Local manager.
- NSX APH-AR certificate- used for inter-site communication when federation is enabled





#### i. Replacing Self Signed Certificate with CA signed Certificate

NSX certificate can be replaced with CA signed certificate using following steps:

1- Import CA signed certificate. - As shown in the figure make sure to copy certificate chain in following order: "Leaf - Intermediate -Root Cert"

		Import Certif	icate For a ord	chain certificate copy cert in followin ler: "Leaf – Intermediate –Root Cert"
Ho	me Networking Security Inver	Name *	nsx-mgr-vip-ca-cert	
>>	Certificates CSRs CRLs	Certificate Contents *	Leaf cert Intermediate CA cert Root CA cert	BROWSE
۵	<b>劉 IMPORT ~</b> 前 DELETE	Private Key	Leaf Cert Private Key <	Copy Private Key of Leaf Certificate
ŵ	Import Certificate	Passphrase		
Ø	Import CA Certificate	Description		
	tomcat cartificate for pode dc02-ps:	Service Certificate	No Cervice	Certificate Option as NO
		Turn Service Certificate o	in to use the certificate with services such as Li Iff to use the certificate with NSX Manager app	aad Balancer and VPN. Jilance nodes.
				CANCEL IMPORT

2- Replace Self-Signed certificate with imported CA signed certificate. The NSX Certificate replacement is supported using following API workflow. UI support is not available as of NSXT 3.0.

1. Get Certificate ID of the new certificate from the NSX UI or API.

LocalManager		ager	local-manager	• 6/25/2020 - 9/2	Self Signed
mp-cluster certific	97b8bd27-0d97-444c-8cbd-c4b1d1814126		dc02-nsx-mgr-A1	• 6/25/2020 - 9/2	Self Signed
nsx-mgr-cluster-ca	-cert 97b84126 nsx-mg	gr-01	NSX LAB CA	• 7/14/2020 - 4/10	Certificate

2. Validate the certificate using following API:

GET https://<nsx-mgr>/api/v1/trust-management/certificates/<certificate-id>?action=validate

3. To replace NSX Manager CLUSTER/VIP certificate use following API. This API call can be done to any of the Nodes in the cluster.

POST https://<nsx-mgr>/api/v1/cluster/api-certificate?action=set\_cluster\_certificate&certificate\_id= <certificate-id>

4. To replace NSX Manager NODE certificate use following API. Since it is node specific certificate replacement, This API call needs to go to individual NSX manager for which you want to replace the certificate.

POST https://<nsx-

mgr>/api/v1/node/services/http?action=apply\_certificate&certificate\_id=<certificate-id>





This completes certificate replacement workflow, and NSX manager starts using new CA signed certificate when user access the NSX manager UI or API.

Regarding NSX federation certificate replacement which are exposed on NSX manager even in nonfederated environment, only PI certificate can be replaced with NSX-T 3.0 release. APH-AR cert replacement will be supported in later releases. User can use following API call to replace NSX Federation PI Certificate.

POST https://<nsx-mgr>/api/v1/trust-management/certificates?action=set\_pi\_certificate\_for\_federation

{

"cert\_id": "77c5dc5c-6ba5-4e74-a801-c27dc09be76b",

"service\_type": "LOCAL\_MANAGER"

}









