VMware NSX-T 2.4 2V0-41.19
Exam Study Guide

Section 2 – VMware Products and Solutions

Objective 2.1 - Describe the VMware Virtual Cloud Network Vision

Framework for connecting and protecting workloads across different environments.

Objective 2.2 - Outline the solutions of NSX Portfolio

Includes: NSX-T DC, NSX Cloud, AppDefense, SD-WAN, NSX Hybrid Connect
Provides: Security, Integration, Extensibility, Automation, Elasticity

Objective 2.3 - List the use-cases for NSX Data Center

Security, Multi-cloud Networking, Automation and Cloud Native(for Containers and K8s)

Objective 2.4 - Explain the value proposition and features of NSX

Separate from vSphere, NSX is a platform, Provides services(NAT, VPN, etc) and is Networking (Bridging, switching, routing, BGP, etc.)
Automation – tags, inventory, API's
Operations – dashboards, LI, RBAC
Troubleshooting – Trace, monitoring

Objective 2.5 - Identify Physical and Virtual Infrastructure Requirements for NSX-T Data Center

NSX Manager = XS/S/M/L

XS	is cloud device. You don't use it in NSX DC.
S	is for labs.
M	is normal
L	is for > 64 hosts

XS	2/8/200
S	4/16/200
M	6/24/200
L	12/48/200
	Cpu/memory/gb disk

Transport traffic can either have it's own physical nic or share with management traffic.
NSX Cluster VIF always points to Master.
MPA – Management Plane Assistant – exists on TZ nodes – stats/status
Default Profiles are modifiable.
Physical Requirements:

1 NSX Manager
Edge/Transport Nodes
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/2.4/installation/GUID-14183A62-8E8D-43CC-92E0-E8D72E198D5A.html
Supported vSphere versions 6.5 U2+
There are bare metal requirements for putting NSX Manager

Objective 2.6 - Describe NSX Architecture and Component sub-systems

Management, control, & data planes => mgmt & control is combined in NSX-T
3 Node management cluster
Performs Policy, Management and Control roles (3x3)
- This 3 node cluster where all three roles live on every node but each one is the lead for one role.

Provides API, HTML, CLI
NVDS = NSX Virtual Distributed Switch
NVDS is opaque in vSphere view(read only)
NVDS is managed outside of vCenter – from NSX Manager
NVDS requires physical NIC's that are currently assigned/used by existing switches.
NVDS is installed on every transport node.
KVM hosts can't do LAG, only ESXi hosts.
NSX-T can mix KVM and ESXi Hosts in the same NSX Transport zone.
NVDS names must be unique to the transport zone.
Overlay Transport Zone = TEP's network between hosts. Is a logical scope of communications between hosts.
VLAN Transport Zone = connection for northbound traffic to the VLAN's.
Manually enter anti-affinity rules for the 3 nodes and the edge nodes <-best practices.

<u>Major Architectural Components:</u>
NSX Management Cluster – management & control
Transport Nodes - data
Edge Nodes -data
NVDS – data
OVS - data
Know the difference between management, data plane, control plane

Objective 2.7 - Differentiate the functionalities of Management Plane, Control Plane, Data Plane, and Consumption Planes

Management Plane – Policy & Management
Control Plane – Controller Role, split into ccp and lcp(Control Cluster Plane and Local Cluster Plane)
Data Plane – status, failover of multiple links or tunnels, packet forwarding,

Stats, where logical switching, distributed routing, centralized routing, and firewall filtering happens

Comprised of hypervisor nodes, bare metal nodes, and edge cluster nodes

Policy *selection* happens in the UI

Choices gets pushed to Policy Manager in cluster – Policy Manager validates the selected policies are "doable." Once validated, Policy Manager sends to NSX Manager. NSX Manager writes changes in the CorfuDB and sends to Control Plane(CCP) which sends to LCP(cluster pushes out to nodes(TZ nodes=LCP)).

Objective 2.8 - Define NSX-T Data Center Terminology

There are too many to list here.

N-VDS = Deployed by NSX Manager

In esxi, it is like VDS

In kvm, it is OVS.

vCSA can't modify, can only view(hence, the devices are referred to as "opaque")

Objective 2.9 - Describe the Logical Switching Architecture and Features

Logical Switch = Virtual L2 broadcast domain

In NSX, switches are segments created on the NVDS's and utilize the Geneve protocol(with VNI's) to move traffic.

LS's are segments. LS = Logical Switch = Segments

Segment	=	VLAN	=	Portgroup
NSX		Cisco		VDS

Segments have the same features as VDS(COS, ARP, IP Discovery, Ingress, SpoofGuard profiles. Security is for Bridge functions.

When LS is created within a transport zone, it inherits TZ type(overlay or vlan)

NVDS – delivered to transport nodes as part of overlay.

Segments are part of NVDS.

NVDS is another switch and requires unused physical nic's on each host.

TEP – Tunnel End Point = MAC info is pushed up to CCP

TEP = uses Geneve(Generic Network Virtualization), Geneve ENCAPSULATES, NOT ENCRYPT! It CAN be sniffed by wireshark. Adds 100 to the old 1500MTU = 1600 MTU needed for all ESXi TZ hosts TEP Physical nics. Uses UDP 6081. Hence, L2 *over* L3.

VNI – Virtual Network ID – virtual network identifier that acts like a VLAN ID in the Geneve network

Ccp sends updated tables back down to TZ nodes = >this is ARP suppression method

"LIF" is port that a vm is connected on the NSX-T switch itself

Geneve uses VNI, like VLAN but more(VLAN max in one network is 4096, VNI max is 16777215.

To achieve network virtualization, the controllers have to config nodes with network flow tables for each segment.

Flow tables:

TEP: vni to tep ip

ARP: vm mac to vm ip

MAC: vm mac to tep ip

Mac table changes are pushed to CCP in the following scenarios:

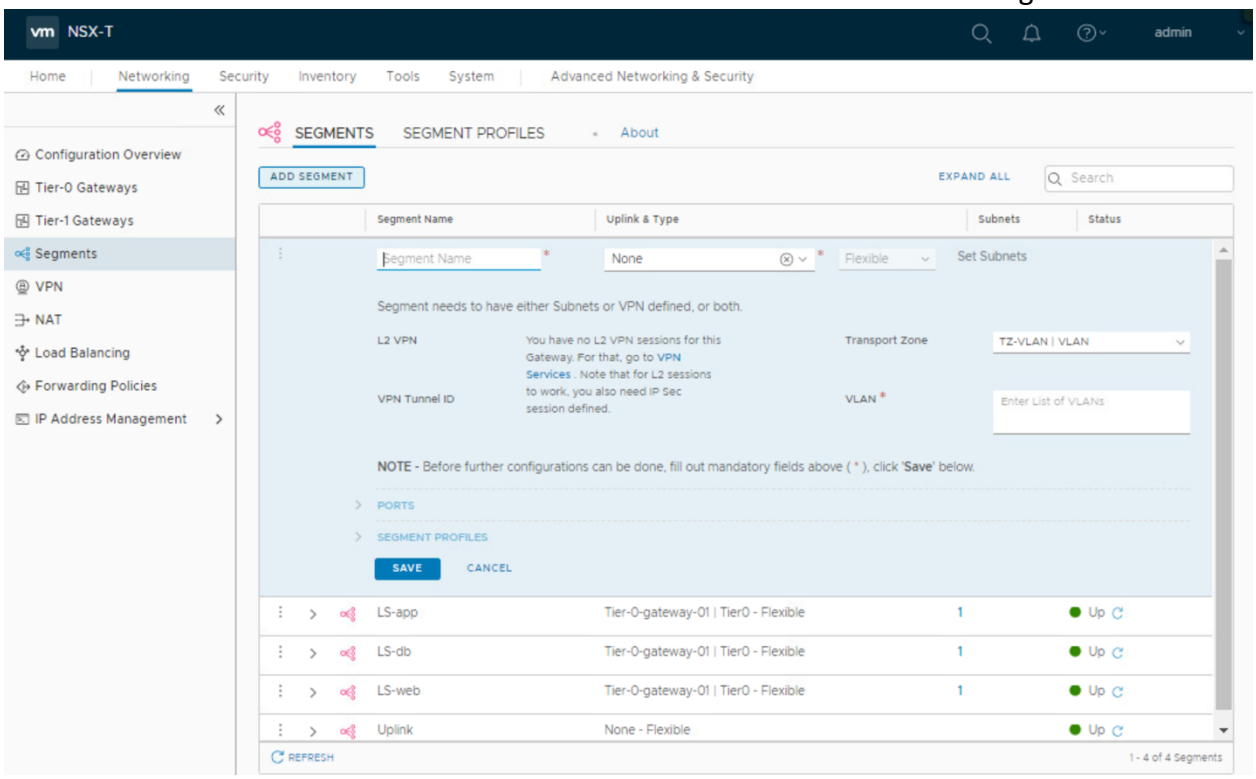
When vm is connected to segment (Mac to VNI association)

When vm is powered on(mac to tep association)

BUM Traffic – is processed in 2 ways:

Head Replication – to all TEP's that have same VNI instantiated

Hierarchical Replication – to MTEP's only(Master TEP in each location). MTEP's communicate with local TZ hosts and sends info back. This is the default behavior because it generates less traffic.



Objective 2.10 - Describe the Logical Routing Architecture and Features

Routing is done through virtual routers.

There are two types of routers: T0 & T1

The T0 sits on physical or virtual appliances called Edge nodes.

T0 = North/South (acts like service provider), they can also serve T1 functionality

T1 = East/West

DR = Distributed Router – goes on TZ nodes

SR = Service Router - goes on North/South edge nodes

Every gateway=router can perform DR & SR functions.

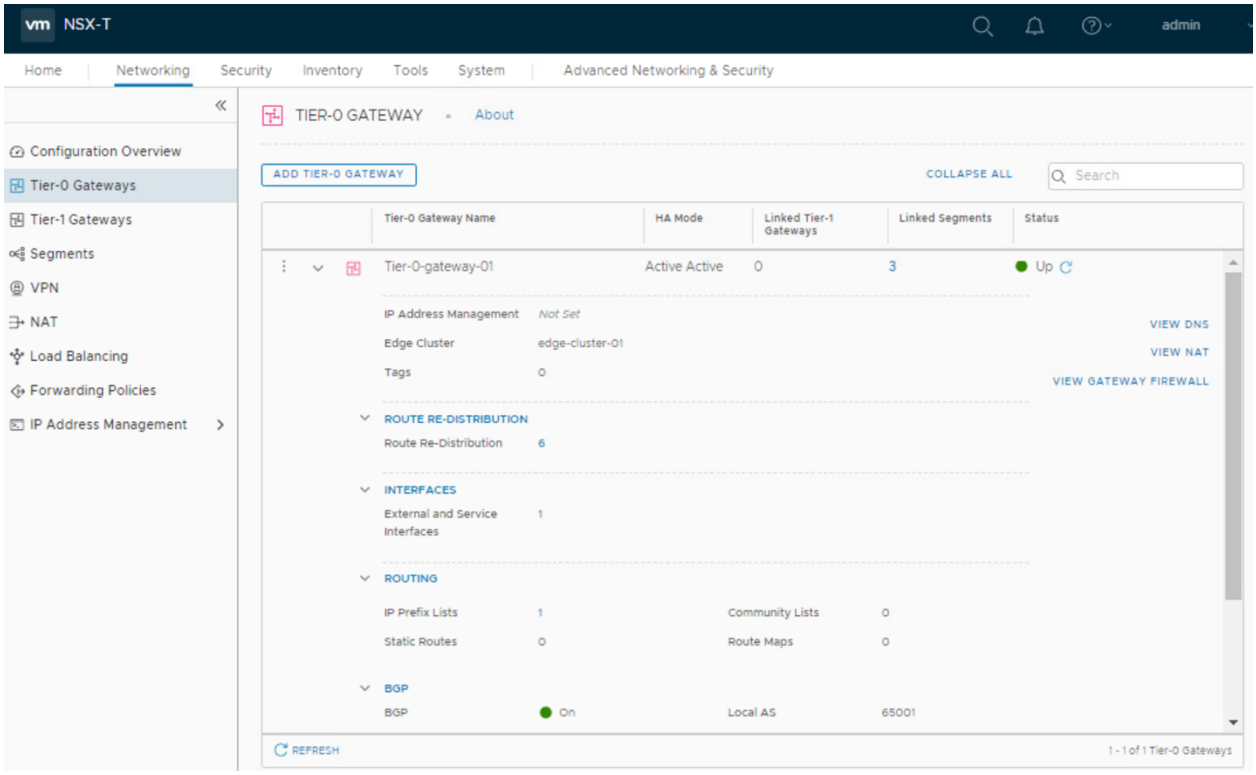
*When you turn on SR, gateway automatically creates the DR to SR connection. <-useful for troubleshooting with traceroute(you can change the network if needed)

Once traffic is detected, all tables are populated.

Simplified UI = new NSX-T features(preferred and recommended)

Advanced UI = legacy NSX-T view.

All components created in Simplified UI will show up in Advanced, but components created in Advanced will NOT show up in Simplified UI. All modifications in the simplified UI will overwrite what is in the Advanced UI.



Edge Nodes = Appliances

Not distributed services

Can use DPDK

S/M/L

Min 2, Max 10 with 8 active/active and 2 standby per Edge Cluster(remember, not bound by vSphere cluster max's)

Bc it's always in HA mode

16 max Edge Clusters in 2.4 (160 Edge Nodes)

Does not support AMD processors, only a list of Intel processors

https://docs.vmware.com/en/VMware-NSX-T-Data-Center/2.4/installation/GUID-22F87CA8-01A9-4F2E-B7DB-9350CA60EA4E.html

Edge Cluster HA Mode: Active/Active & Active/Passive

Difference between HA Modes is Active/active must consider reconvergence time for dynamic routing – leading to network interruption only for those connections that were on the failed active node.

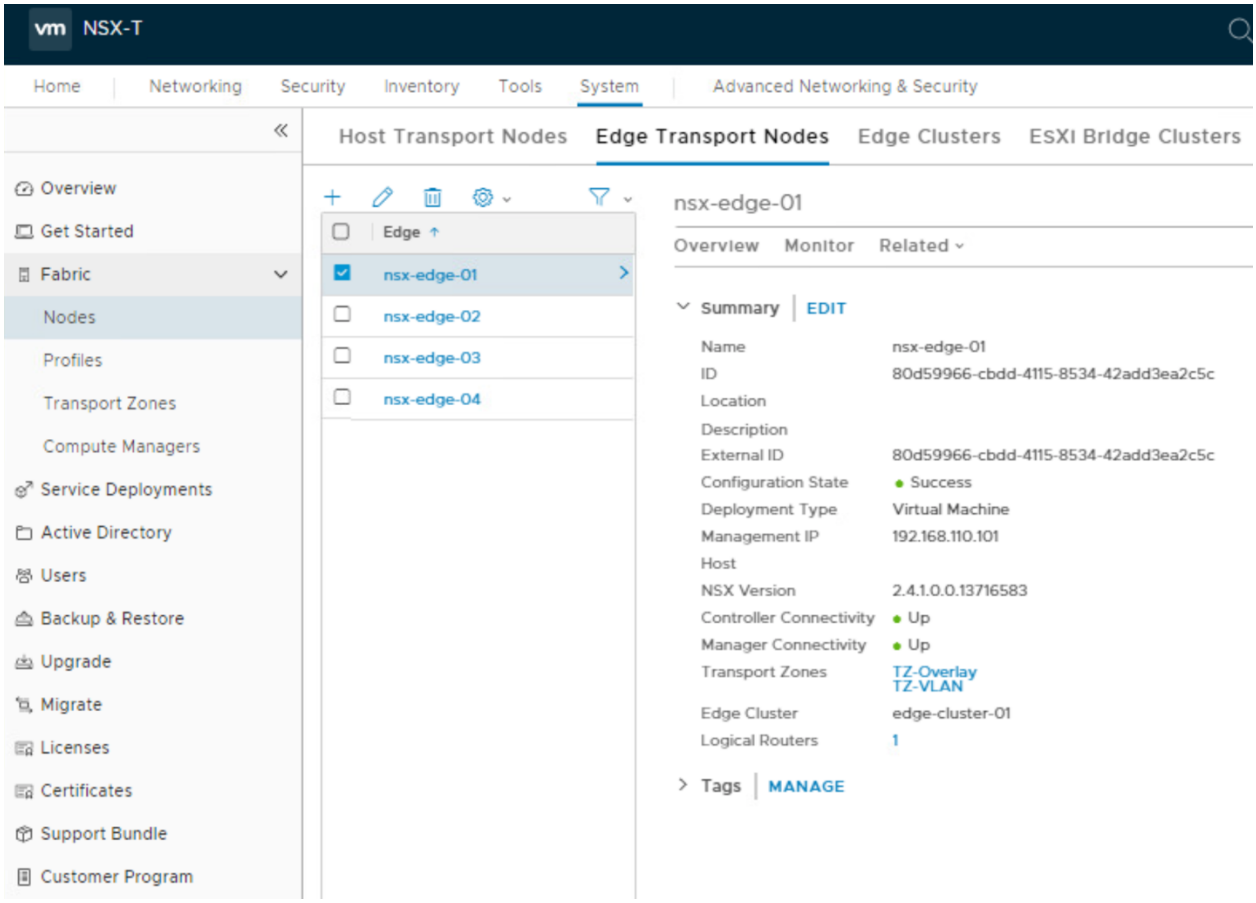
Active/passive is however long failover time is – all connections.

1 NVDS = can participate in more than one Transport zone(can be one overlay and/or vlan)

An SR is installed on an Edge Node. It's a Router – T0

Services: DHCP, NAT, stateless services

Segment Profiles = to automate creation of segments/logical switch.



T0 Capabilities:

1. Static Routing
2. Dynamic Routing(BGP)- both iBGP & eBGP
3. BFD – bidirectional forwarding detection
4. ECMP w/physical gateways

T0 Routing Features:

eBGP
iBGP
Route aggregation
Community Lists
IP Prefixes
Route Maps
Allow AS – in
ECMP – HA and can use both paths in active-active mode

IP Prefix – deny or allow which networks can be seen/you list which ones you want to see
Route Maps – take precedence over IP Prefixes

When T0's are in Active-Standby configuration, BFD(Bidirectional Forwarding Detection) does the following:

1. Standby uses overlay and management network w/heartbeat w/3 hello's failures threshold.
2. If active node detects upstream failure, then active node will failover to standby

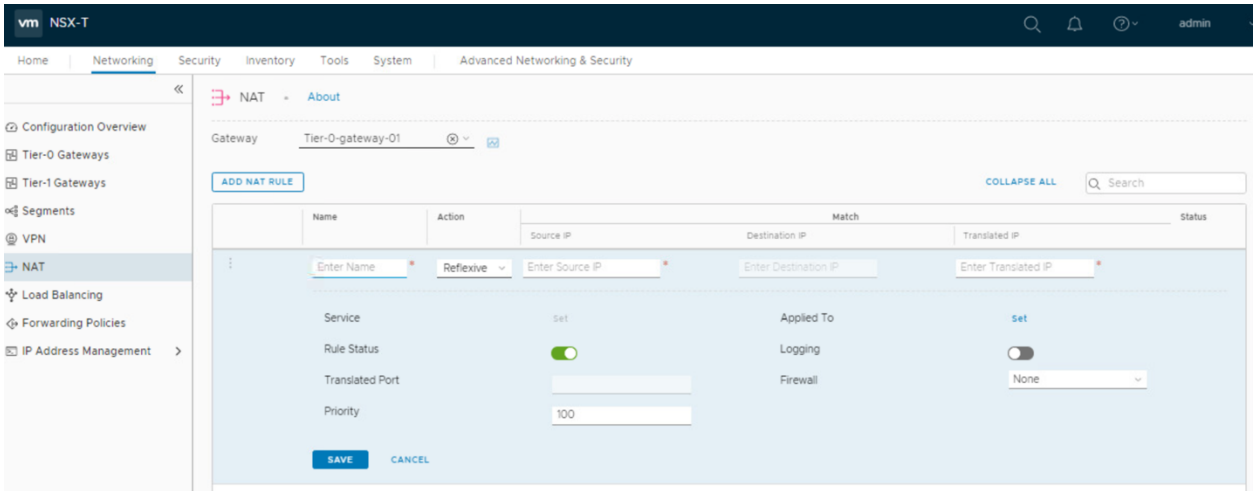
Preemptive = will fail BACK(Default)
Non-preemptive = NO failback to original active node

Bridging – is meant for temporary purposes
Need a VLAN backed T0
Splitting subnet across physical and virtual workloads
Leveraging network services from either physical or virtual for both workloads
A Bridge Node = TZ node or Edge Node(preferred)
2 Ways of doing Bridging in 2.4: via ESXi Bridge Clusters or via Edge Bridge Profiles.
ESXi Bridge Clusters - Create/Install via System – Fabric – Nodes – ESXi Bridge Clusters
Edge Bridge Profiles - Bridge Profiles – specify VLAN vs Logical Switch(VNI) mapping and primary/backup nodes. Profiles are only used on Edge nodes.
Bridging connected via Networking – Segments – Edit Switch – Advanced Configuration – Related
Or
Go straight to Advanced Networking & Security - Switching – Switch-Related – select ESXi Bridge Cluster or Edge Node Profiles.

Single Tier Routing vs Multitier Routing – you must know the difference – know how to do a packet walk.
Single Tier Routing – there's only T0 router, no T1's.
Multitier – uses both T0 and T1's.
T0/T1's do a "party trick" where they move the packet from one network to another within
Only switches do the Geneve encapsulation, NOT T0/T1's.
T1/T0 DR's are chained to Segments on the esxi hosts/TZ nodes once connected.
One T0 DR will be on Edge Node and that will be the one that sends packets north.
Why Single Tier vs Multi Tiered Routing Topology:
Use T1's for multitenancy/privacy
T0's have limit to how many segments it can service
Services – do they have to be active/active or can they be active/passive and this determines which you use
Active/passive required for stateful services(like VPN, stateful NAT)
Centralized Service Port – can hang off of a T1 and provide service insertion services(non distributed services available on VLAN networks)
Types of logical router interfaces:
Uplink – T0 to physical devices
Downlink – segments to gateways
RouterLink – T0 to T1's
Intra-tier transit link – internal between DR and SR functionality
Centralized Service Port(CSP) – special interface for VLAN services(also a downlink)

Objective 2.11 - Describe the NSX-T Data Center Network Services

NAT
SNAT/DNAT = 1 to many
Reflexive NAT = 1:1 stateless

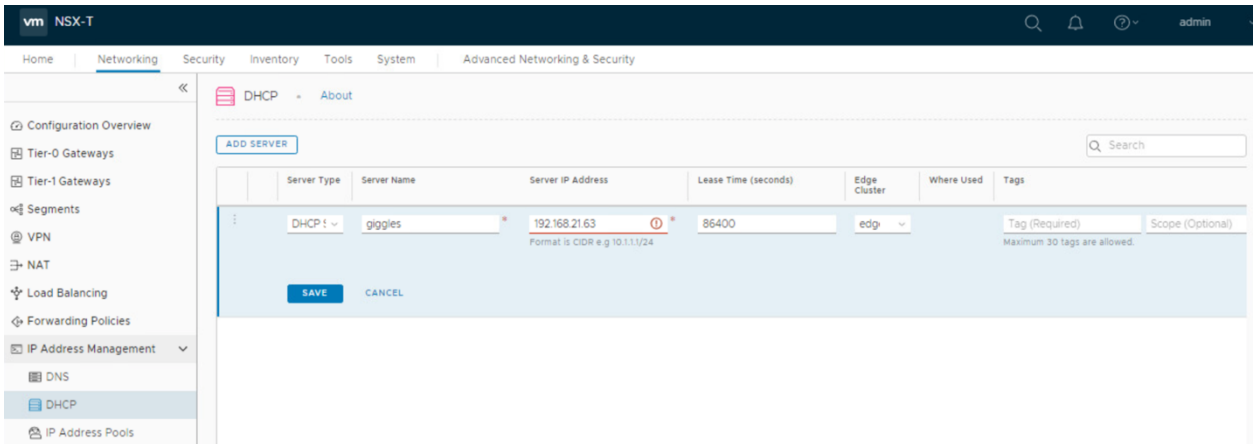


DHCP

2 DHCP Services: Server and Relay

Must be on T0 SR

it is run as a service on Edge clusters



Load Balancing

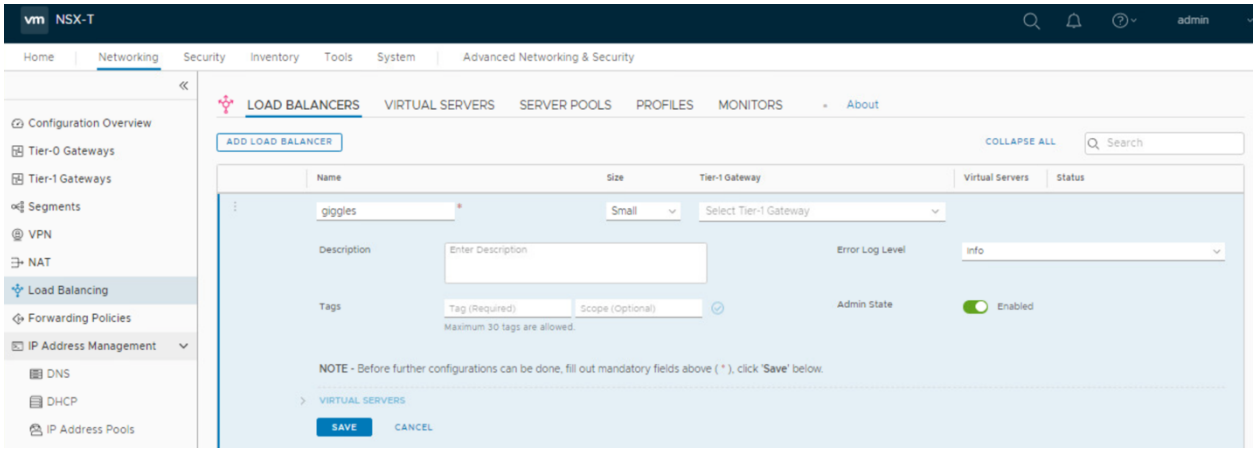
Why load balance? For service scalability and availability.

Balancing TCP or UDP traffic as a L4 & HTTP/S as a L7

LB only available on T1 (in NSX-T 2.4)

L4 = TCP & UDP

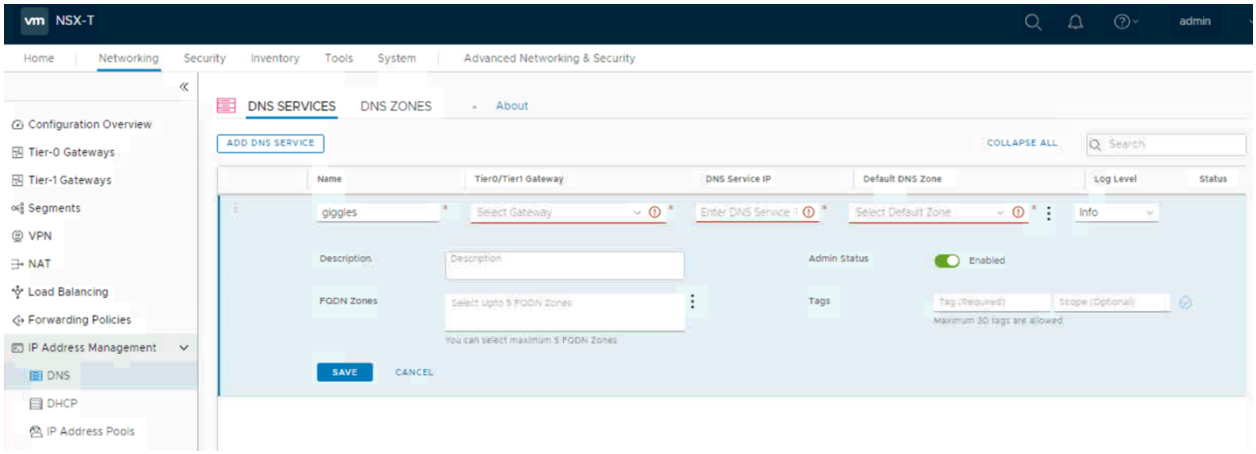
- L7 = HTTP/S
- On T1, implemented via profiles against the servers
- A LB attaches to only one T1
- Sizes available: S/M/L – sizing is important on edge nodes as the edge node must be able to scale.
- LB Modes: Inline & 1 Arm
- LB uses: virtual servers, server pods, profiles(apps,persistence, SSL), monitors



DNS

T1 can be DNS caches – this decreases traffic and increases privacy bc upstream provider does not see all your queries.

Forwarders in “DNS Relay” Mode



IPSec VPN & L2 VPN

IPSec is a protocol suite(family).

You can only use this on a T0 when it is in Active-Standby HA Mode.

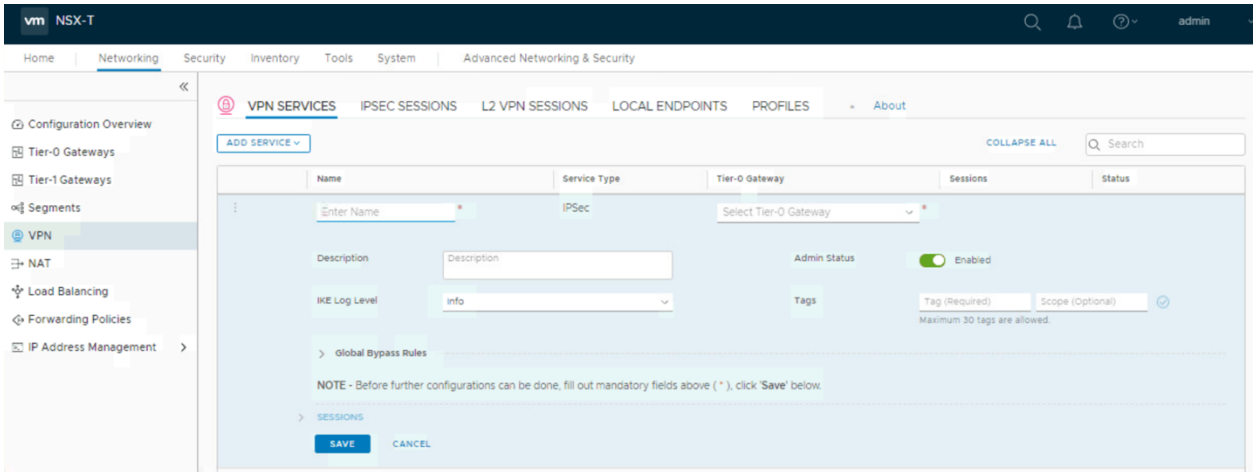
VPN session info is not synced. If failover happens to standby, VPN tunnel will be reinstantiated.

Route(Preferred and recommended) & Policy Based – on T0’s only + req’s Edge Nodes

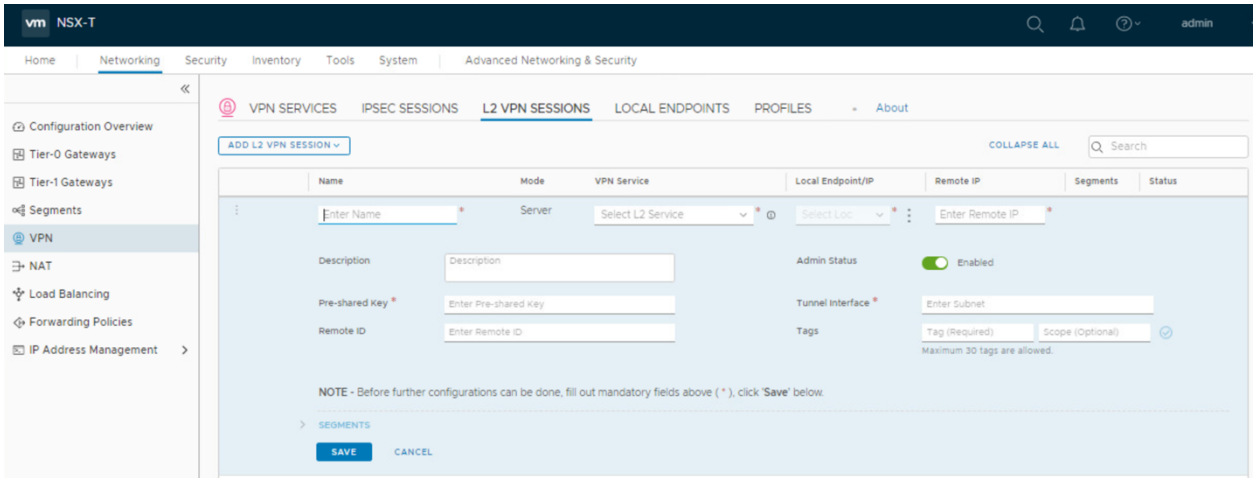
IP Sec uses headers – either AH(Authentication) or ESP(Encapsulating Security Payload)

IP Sec Menu items: services, IP Sec Sessions, L2 VPN, Local Endpoints

Profiles: DPD(Dead Peer Detection), IKE Profiles, IPSec Profiles



L2 VPN
only compatible with NSX environment
only preshared key authentication method available.
uses GRE Encapsulation



Objective 2.12 - Explain the Edge Architecture and Features

Edge Architecture consists of Edge Clusters.
Edge Clusters are made up of 2 or more Edge Nodes in Active-Active or Active-Standby Mode.
Edge Nodes can be VM's or Bare Metal.
Edge Node VM's are deployed via NSX Manager and/or OVA.

Plant T0 on Edge Device
Edge device connects to physical nic's for 1. Overlay + 2. Management

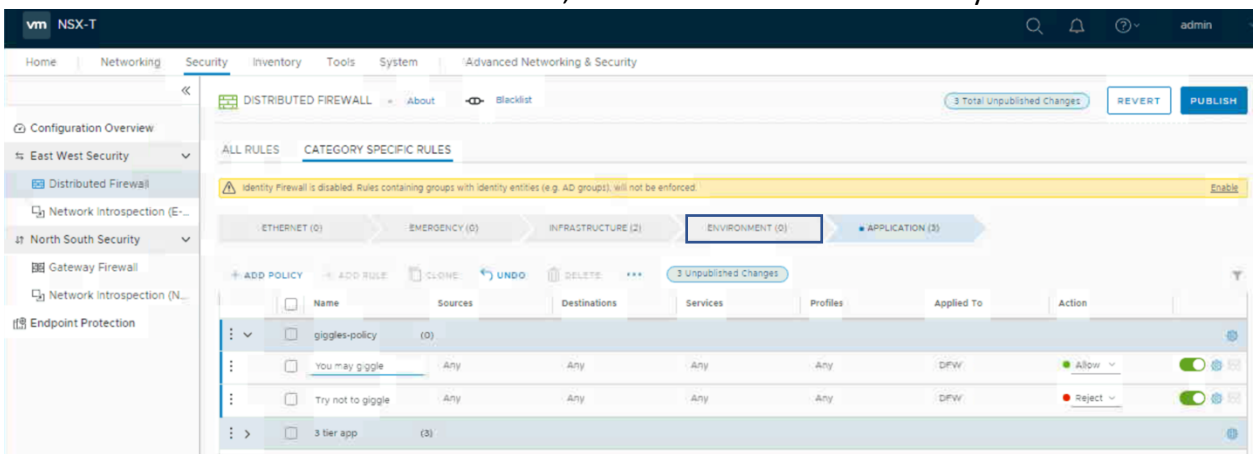
Objective 2.13 - Explain the NSX Security Architecture and Features

Consists of 2 Firewalls, Service Insertion, and Endpoint Protection
Firewalls: Gateway & Distributed
Granular Security at the VM level via Distributed Firewall.
Distributed Firewall = logically divides datacenter into distinct security segments.

Operates at the VMnic level.
Gateway Firewall(perimeter firewall)
- to/from physical environments
- like portbased firewalls
- backed by Edge Cluster
- at uplink of T0/T1

Distributed Firewall features:
- uses NSX's UI
- L2 stateless firewall rules
- L3 stateless and stateful firewall rules
- L7 aware firewall capabilities – aware of the user

Key Concepts:
- Domain – logical grouping of security zones w/rules and groups. You can't modify default domain
- Security – collection of rules and service configurations
- Firewall Rule – instructions to allow/deny
- Group – group of stuff/ppl
- Service – like HTTP, HTTPS, FTP, SSH, etc.
- Context profile
- The distributed firewall can have 70,000 rules but each vnic can only have a few thousand rule applied.

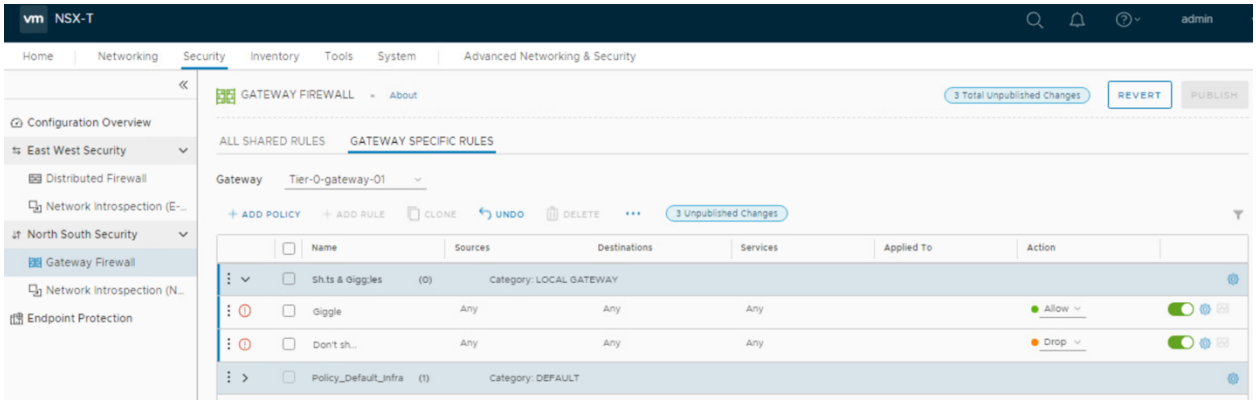


With the Distributed Firewall

RabbitMQ is used over port 5671 between NSX Manager & MPA on host
MPA and NSX-Proxy implement DFW rules to VSIP, VSIP sends to vm's vnic.

With Gateway Firewall

For Gateway firewall rules, you pick the perimeter device to apply rules to (T0/T1)
Categories will be processed from left to right for both types of firewalls.
Settings for a rule via the Gear icon – Ipv4/6, Logging, Direction



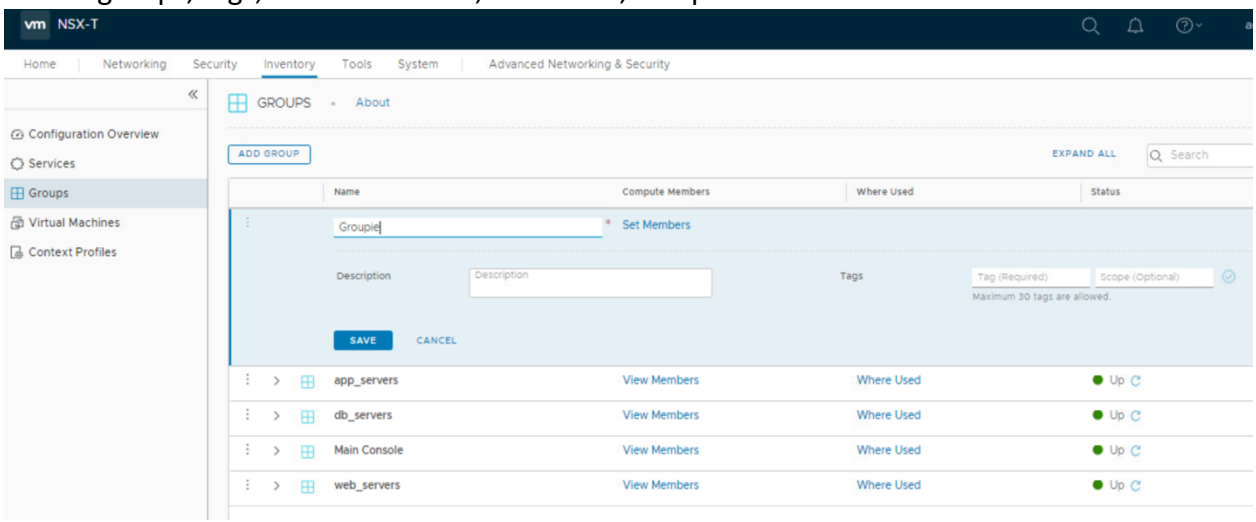
NSX Policy Manager

4 types of policies: DFW, GF, N/S Network introspection, E/W network introspection

Put the most granular policy on top

Application Section has policies: TCP strict, stateful(default on), lock(administrative)

NSX Groups can be based on: static or dynamic vm's, logical ports, IP sets, MAC sets, AD user groups and nested groups, tags, machine names, OS names, computer names



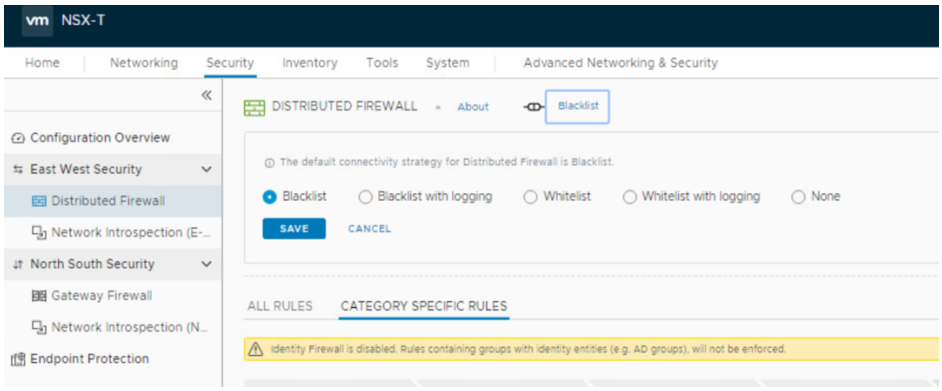
L7 Context Profile can be applied in rule = matching string to make decisions on drop/no drop

Inventory – context profiles(there are system predefined ones)

Logs at /var/log/dfwpktlogs.log on each transport node

Blacklist & Whitelist options = only allowing whitelisting is zero trust implementation

Default is blacklist only which is closer to what customer's are operating in now.

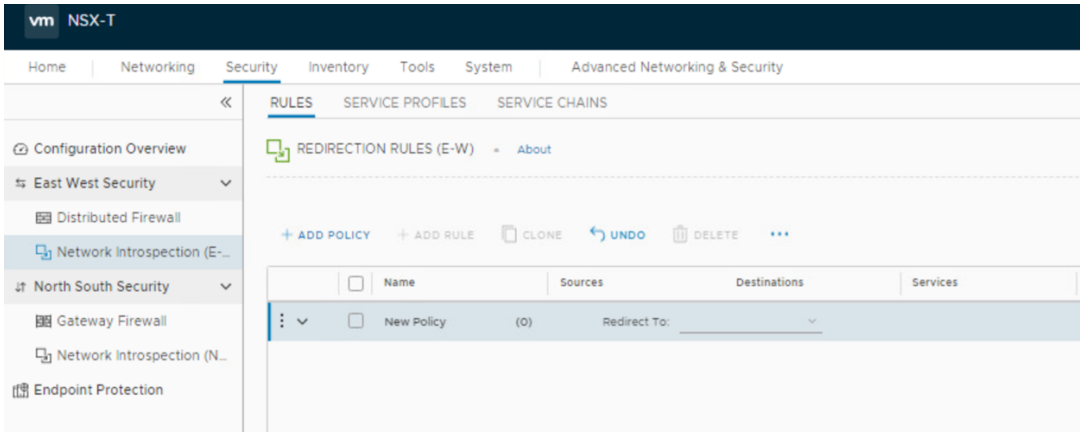


Service Insertion

Service insertion can be done on N/S or E/W on T1/T0

insertion point are on uplinks of T0/T1 GW

SVM – Service Virtual Machine – partner deployed near NSX Edge node



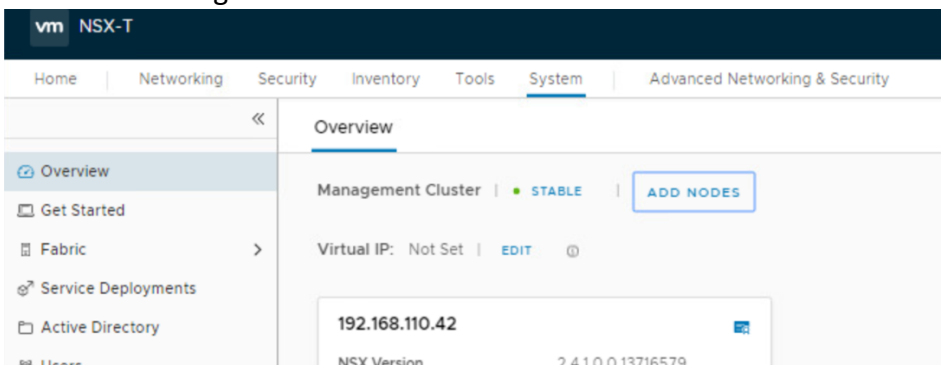
Objective 2.14 - Identify the supported integration platforms of NSX-T (Containers, Public Cloud, Private Cloud, Hybrid Cloud, DevOps tools, 3rd Party etc.)

Section 4 – Installing, Configuring, and Setup

Objective 4.1 - Outline the installation and preparation workflow of NSX-T Data Center

From vCenter server

1. Deploy NSX Manager OVA
2. Login
3. Tie to vCenter(From the Compute Manage menu in System)
4. Add the 2 additional Nodes
5. Config virtual cluster IP



From KVM

1. NSX Manager QCOW2 Image cp'ed to KVM Hosts
2. Create guest info via CLI
3. Run cmd "guestfish" to QCOW2
4. run cmd "virt-install" to deploy NSX Manager Node

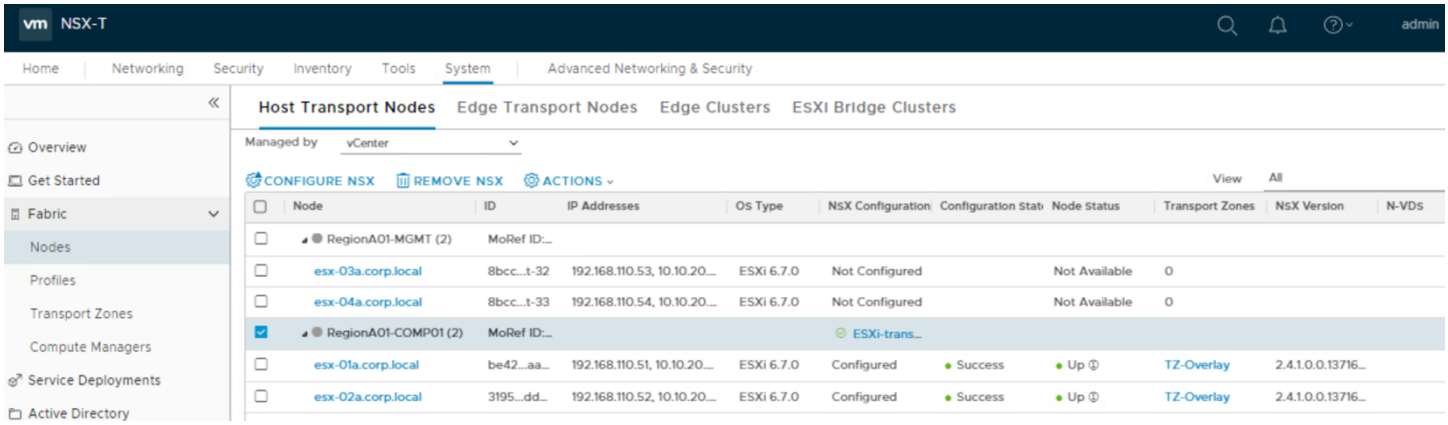
Objective 4.2 - Deploy and Configure NSX-T Data Center Environment

Once NSX Controller Cluster has been installed,
Create an IP Pool (Networking – IP Address Management – IP Pools) for the TEP's.
Use Compute Manager (Under system) to connect to a vCenter as necessary.
Apply NSX to the cluster – this will install the needed VIB's to all the hosts in the cluster.

Objective 4.3 - Configure Hypervisor Networking [vSphere and KVM] for NSX-T Data Center

Installing/Add ESXi Hosts to NSX:

1. Create Overlay and VLAN(outbound) Transport Zones
    a. System – Fabric – Transport Zones
2. Create IP Pools for TEP's
    a. Networking- IP Address Management – Add IP Pools
3. Prep ESXi Hosts
    a. System – Fabric – Nodes – Host Transport Nodes – Select vCenter Cluster
        i. Create Transport Node Profile during this

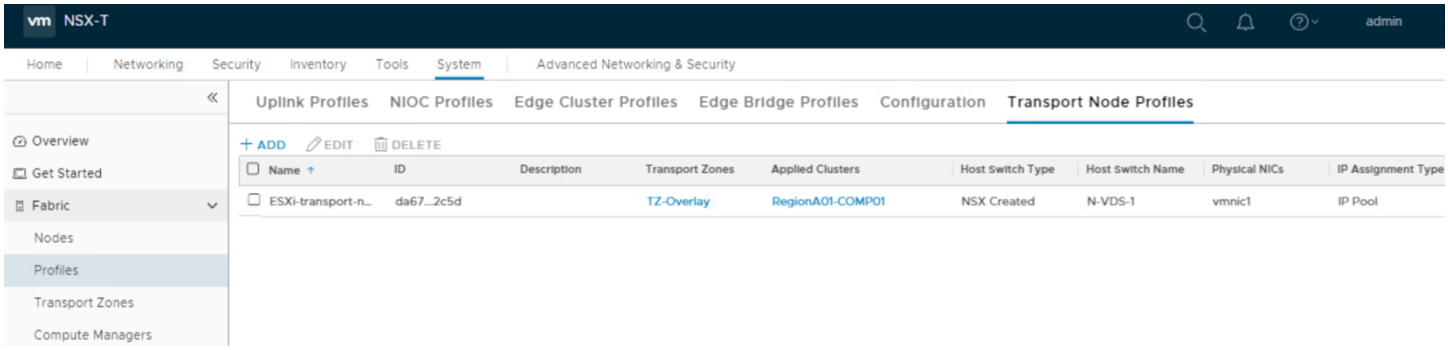


Installing/Add KVM Hosts to NSX:

1. Create Overlay and VLAN(outbound) Transport Zones
    a. System – Fabric – Transport Zones
2. Create IP Pools for TEP's
    a. Networking- IP Address Management – Add IP Pools
3. Use standalone hosts & add manually using IP, username and password

Transport Node Profile has:

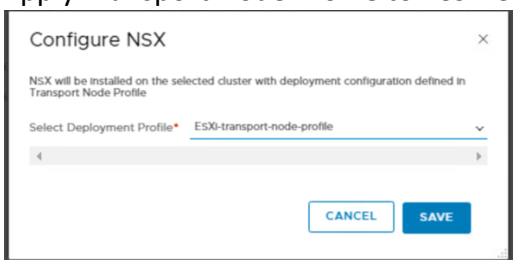
Transport Zones
Hosts
NVDS Confi
Uplink Profiles
IP Assignment
Physical NIC Assignment
VMK NIC and Physical NIC migration



Before you apply a profile, you need:

- ESXi hosts in vCenter
- ESXi hosts in a cluster
- Transport zone created
- IP Address Pool/DHCP on network
- vCenter added in computer manager to NSX Manager

Go to System – Fabric – Nodes – Host Transport Nodes – Managed by VCSA – configure NSX
Apply Transport Node Profile to vCSA Cluster

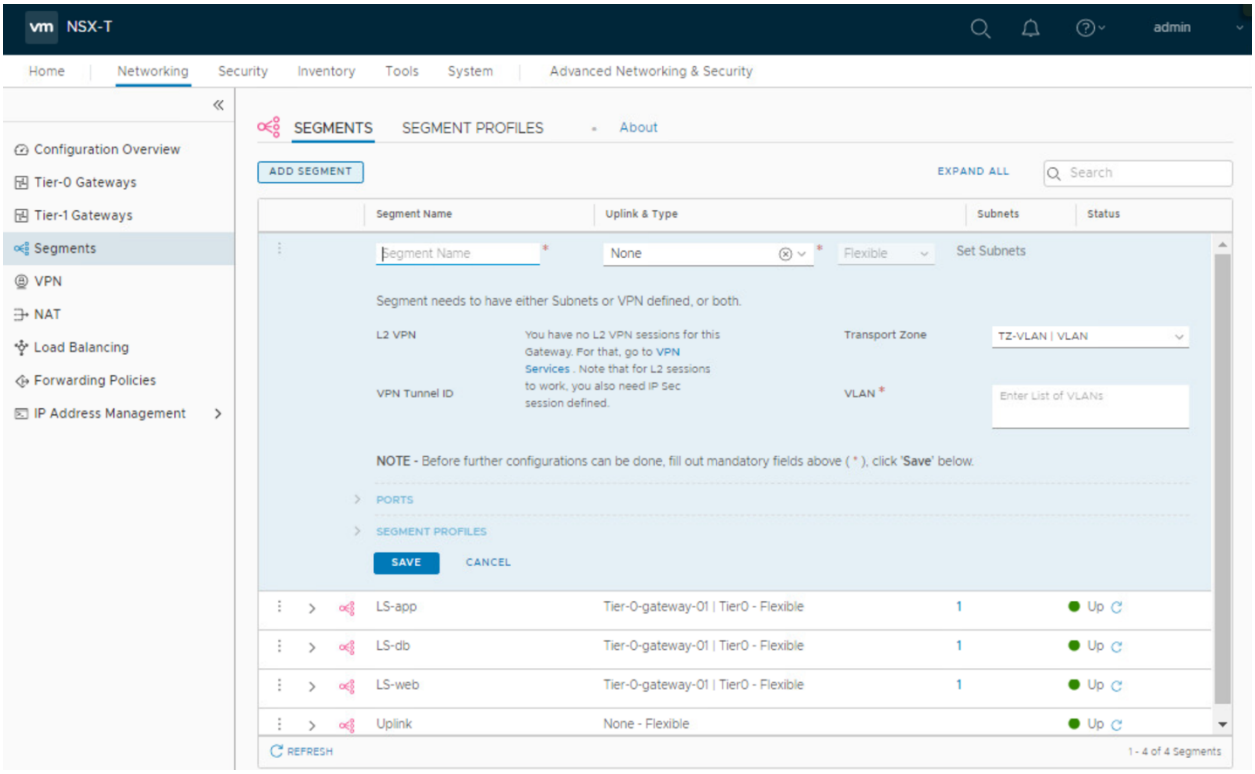


Objective 4.4 - Configure and manage Logical Switching Features

PreReq's:

1. NSX Management Cluster
2. Transport Nodes

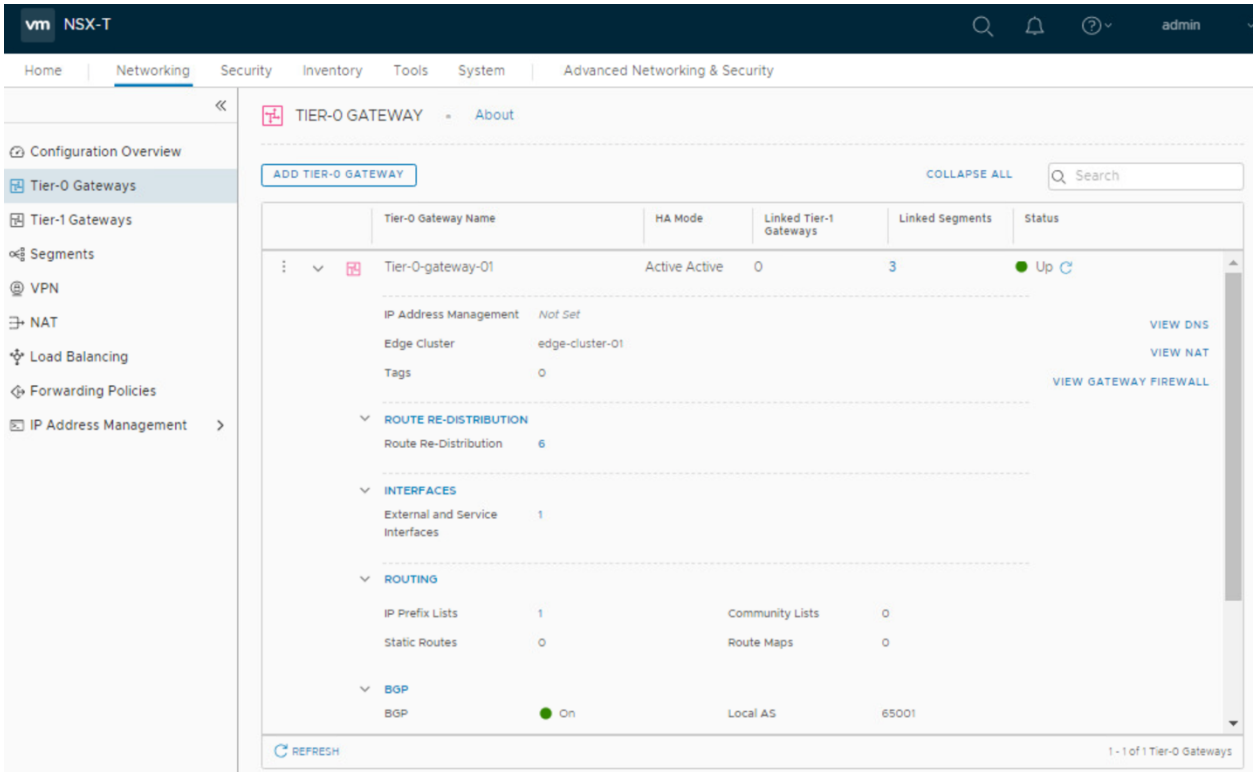
Create segment(Logical Switch)
Networking – Switches – Add Segment



KVM – manually find UUID to assign to port on segment.

Objective 4.5 - Configure and manage Logical Routing Features

Req's creating segments configured to active edge nodes.
T0 – Create
Networking – Tier 0 Gateways – Add T0
T0 Config Interface:
Name
HA Mode
Pick Edge Cluster
Interfaces -> add the segments to the edge nodes
Static Routes -> add as needed

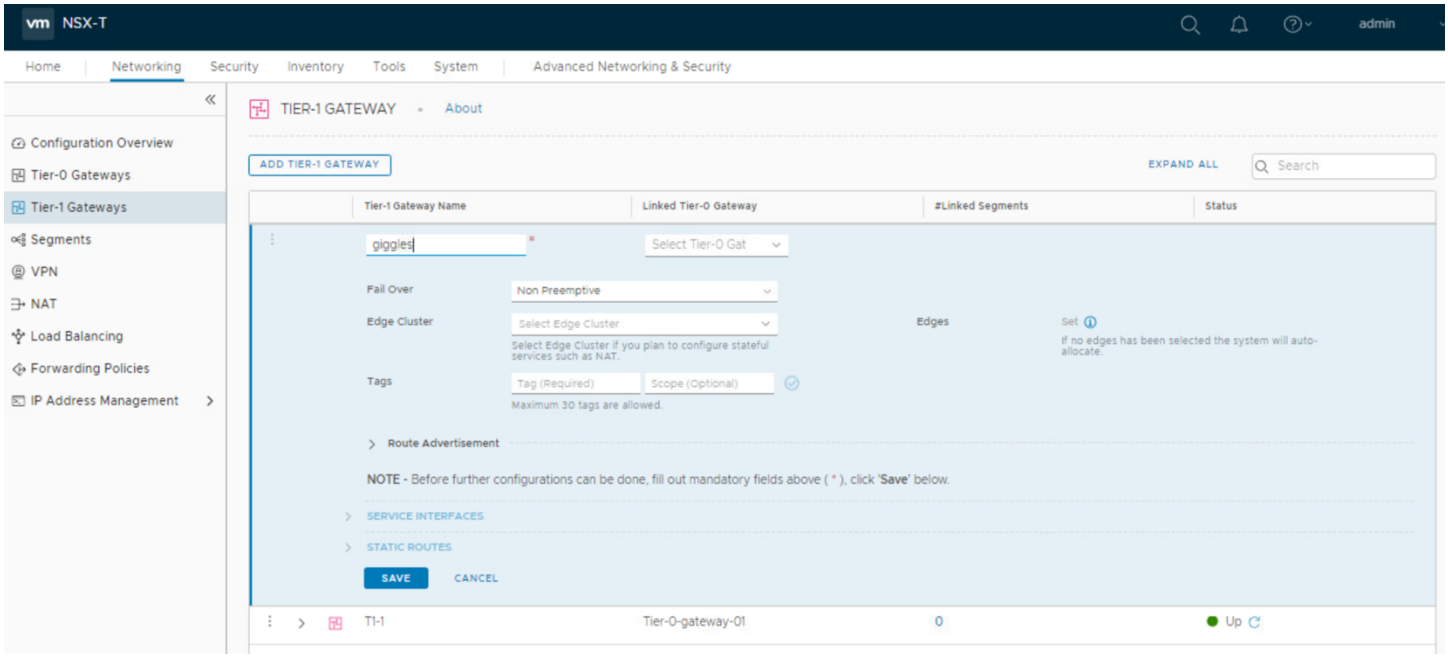


T1 Create

Networking - Tier 1 Gateways – Add T1

T1 Config:

Define T0, failover policy, edge cluster(if you turn on services on this T1)
In Edit, link to T0
In the T1 linking of T0 option is when connection between T0 & T1 is made
Turn on route advertisement if we want the T0 to be able to route back down to the T1 segment.
Networking – Segments – modify segment w/subnets GW T1 <-the gateway follows the segment, not the gw.



Edge Clusters

Prerequisites:

NSX Management Cluster
TZ Zones + Nodes(w/NVDS)
Edge Nodes
Must be connected to management network

NSX Edge VM

S/M/L – all VMW HW v11/vSphere 6+
2/4/200
4/8/200
8/32/200 – only 1 LB
8/32/200 – NSX Bare Metal – can do 720 LB's but has HW requirements

Install

System – Fabric – Nodes – Edge Transport Nodes
Or
Deploy OVF, from NSX Manager – get certificate api thumbprint and use "join management-plane command"

Although either T1/T0 can do stateful and stateless, recommend to put stateful services on T1 and stateless on T0.

*make routing decisions closest to vm(on exam) and that is usually on the DR.

Map edge interfaces to 2 physical nic's – 1 on mgmt and 1 on TEP network

Segment gateway address is a configured at switch/segment.

Objective 4.6 - Configure NSX-T Edge Nodes and Edge Cluster

To add a Edge Node:

System – Fabric – Nodes – Edge Nodes – add node

Designate the right interfaces to the underlying physical nics and which transport zones to service.

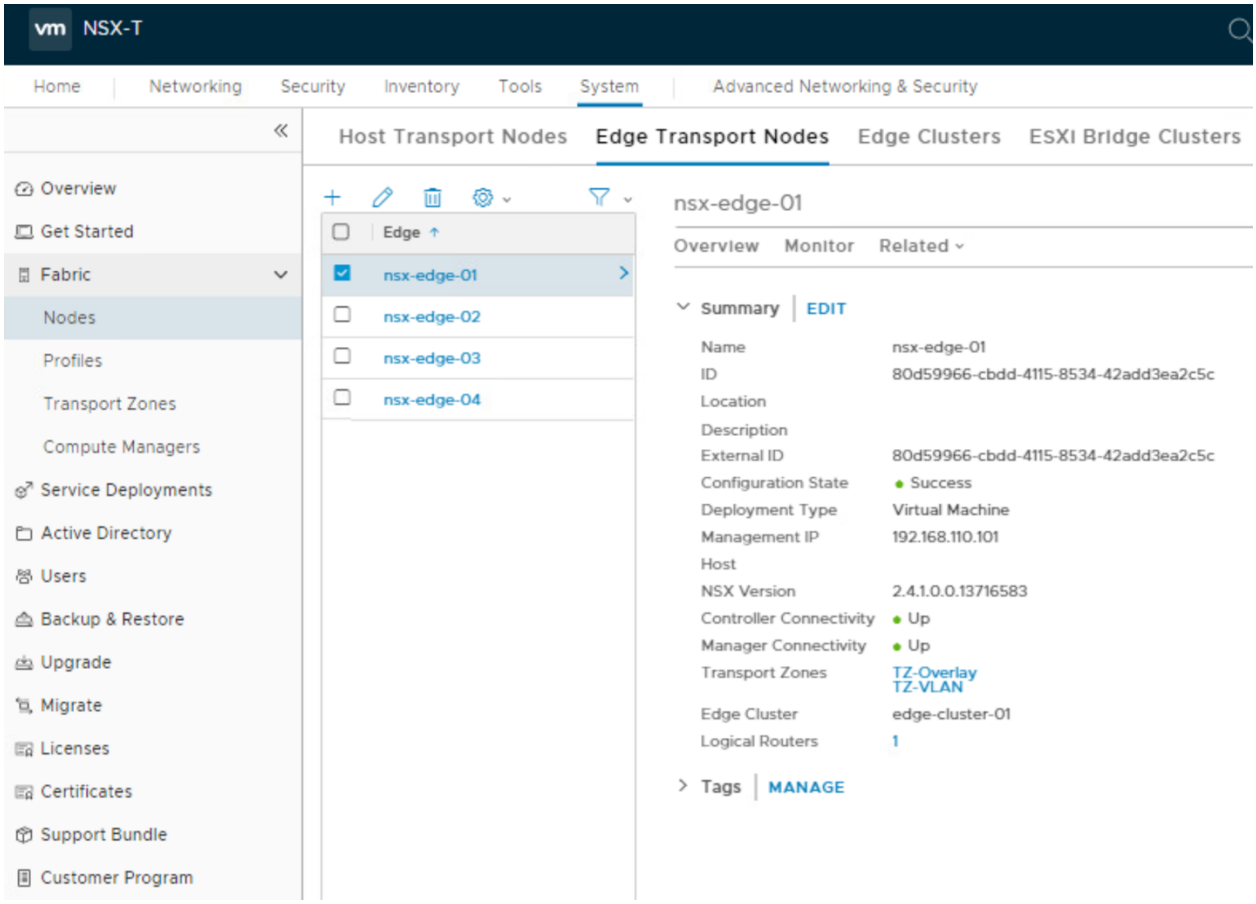
then Edge clusters – create and add nodes to cluster

Edge Cluster Uplink Profiles available: Failover Order, Load Balance Source, Load Balanced Source MAC.

On ESXi, port can be physical or LAG's

On KVM, can only use Failover Order & only 1 LAG can be created with physical nics.

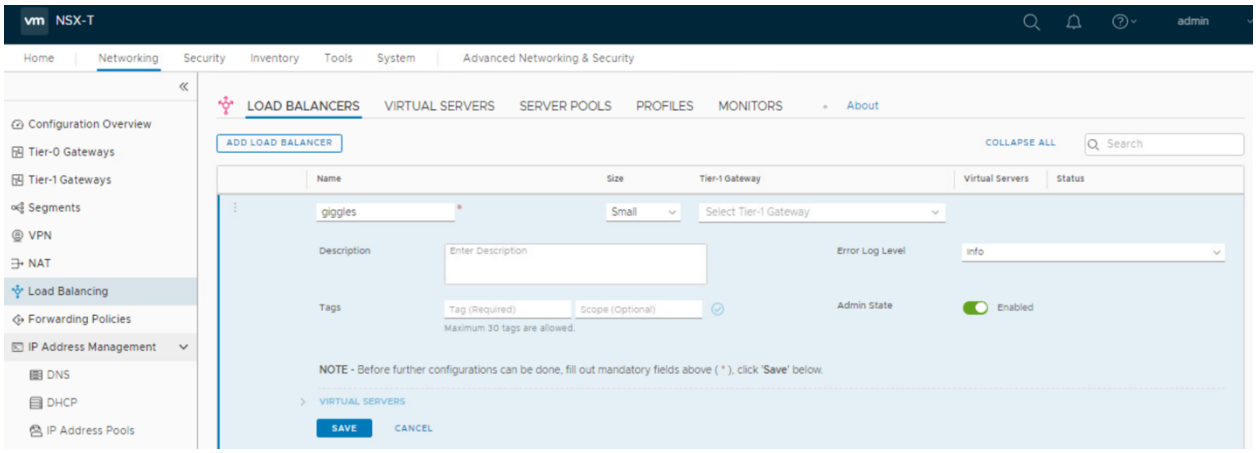
NIOC Profiles only work on ESXi hosts.



Objective 4.7 - Configure NSX-T Data Center Network Services [Layer-3]

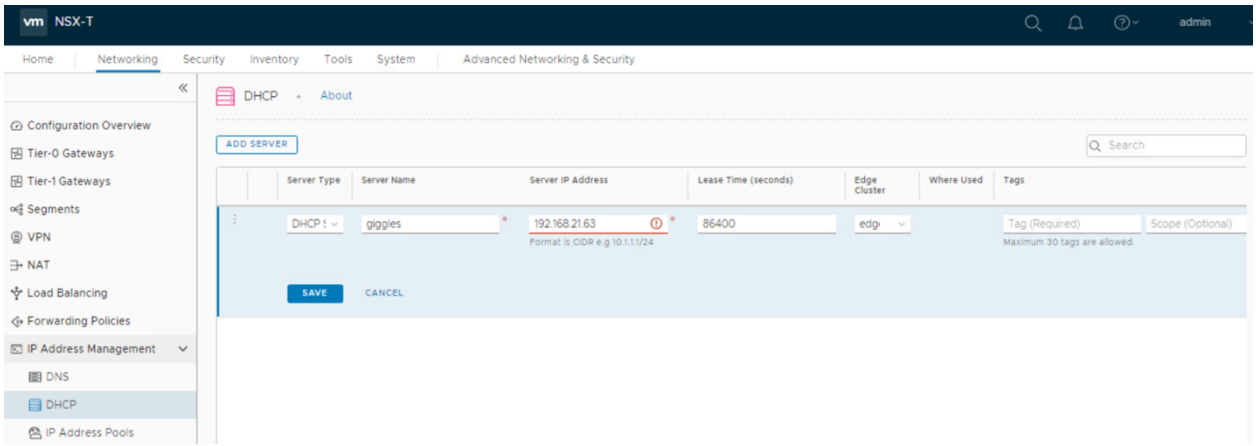
Load Balancers:

To create LB –> Create virtual server – Config profile – create server pool – config monitors
On interface, Networking – Load Balancing – Load Balancers – Add



DHCP:

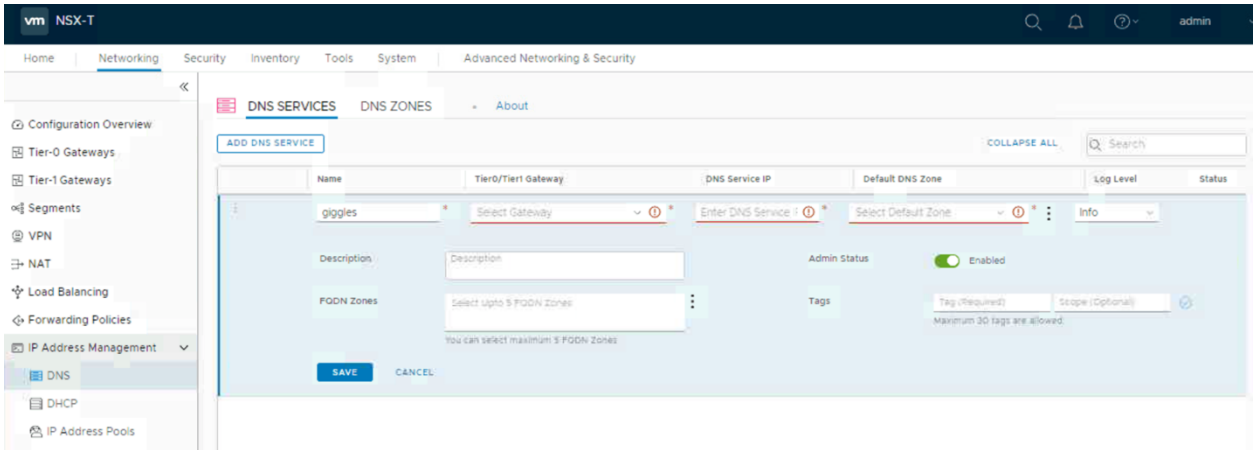
Step 1: Networking – IP Address Management – DHCP – add Server(pick relay or server)
Step 2: Config T0/T1 with DHCP info
Step 3: Modify or while creating new segment, add DHCP range.
Step 4: Add VM to segment with DHCP server.
A lot of DHCP details can be viewed in Advanced UI.



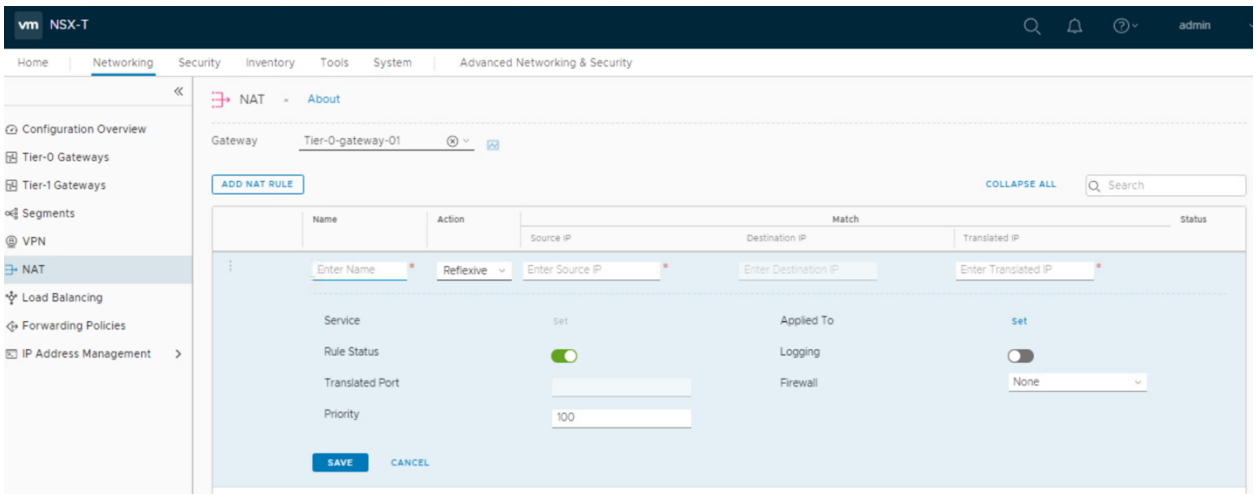
DNS Zones:

is LOCAL zones that are internal

DNS Service:
points to DNS server
Networking – IP Address Management – DNS



NAT
On T0/1
NAT in Active/Standby
NAT on T0 in Active/Active Edges bc stateful
Networking – NAT(Firewall sequence order applies)
Remember to select router where NAT will be

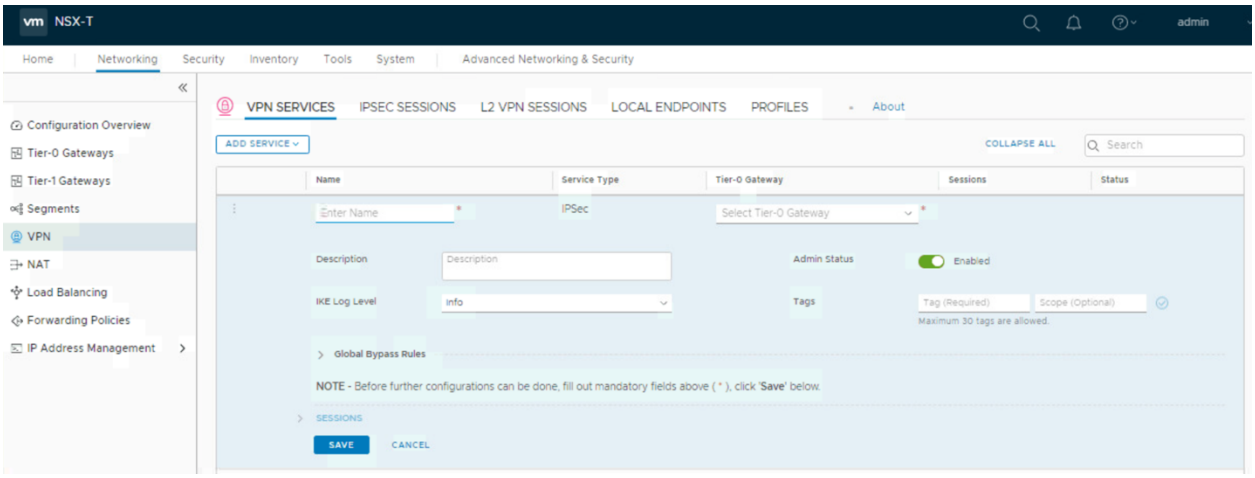


IPSec VPN & L2 VPN

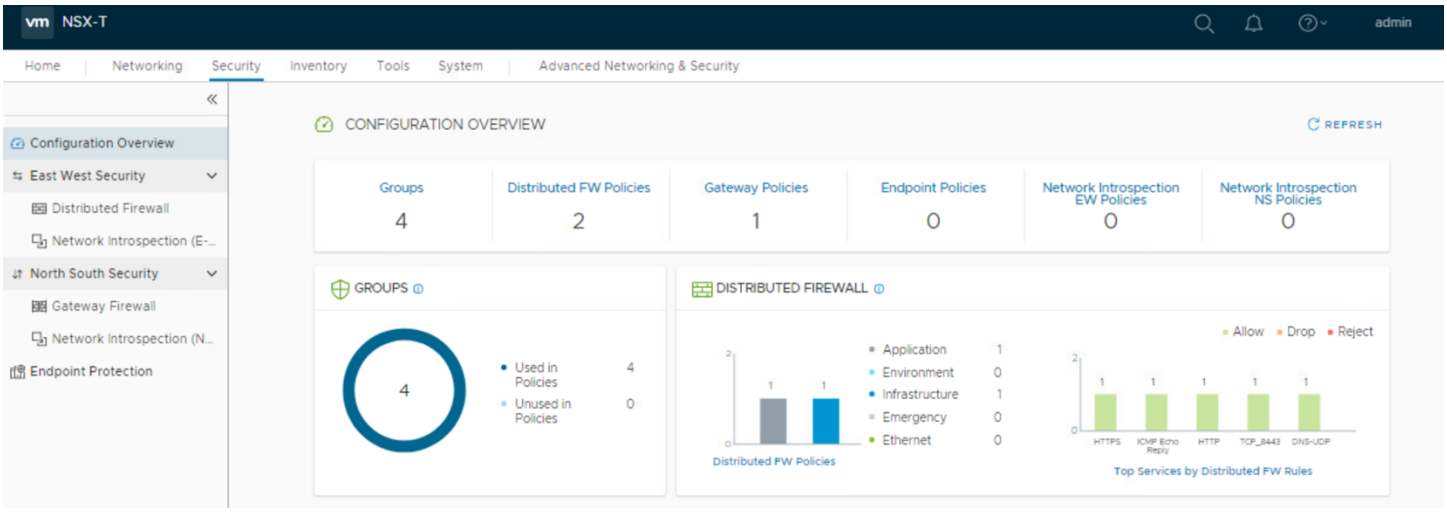
Create/enable IPSec VPN on existing GW – Add local end point & create Route or Policy based IPSEC

Go to Networking – VPN – VPN Services – Add Service

Create IPSec Sessions(Create profile in the process)



Objective 4.8 - Configure NSX Security Features



Objective 4.9 - Configure Service Insertion with NSX-T Data Center

To Configure,

1. Register – manual via partner instructions
2. Deploy at System – Service Deployments – Deployment – then deploy to cluster
3. Configure traffic redirection at Security – Network Introspection

Once done registering, System – Service Deployment – Catalog to view services available.

A service profile is an instantiation of vendor template(workstation, server, malware, antivirus)

Maximum services in a Service Chain is 16

traffic will go through these sequence of services.

Network Introspection is just like firewall rules in that they use the NSX groups available.

EndPoint Protection

- windows only vm's
- happens INSIDE vm

The endpoint protection is enforced via policies and these policies follows the vm no matter where it goes.
Menu looks like this:

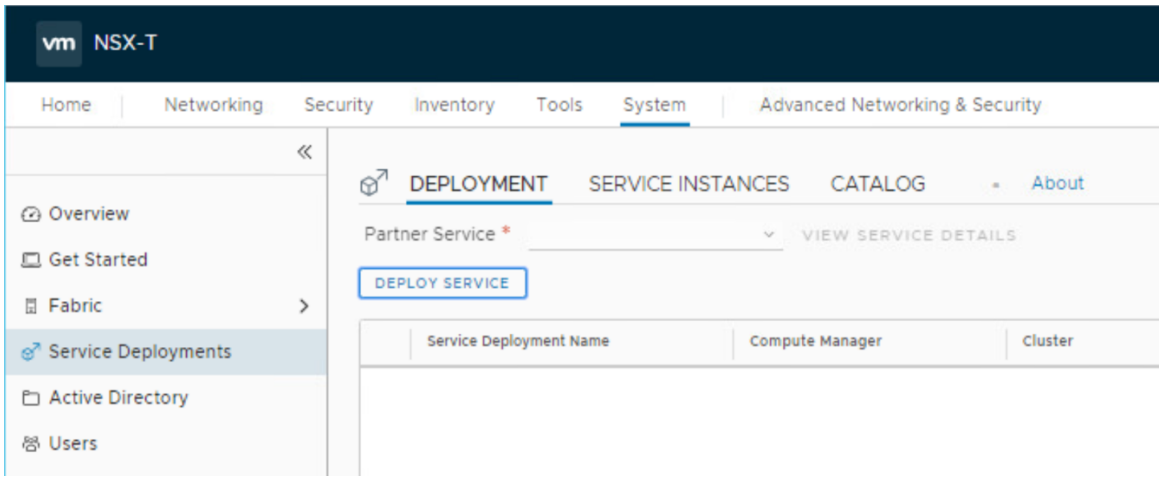
System

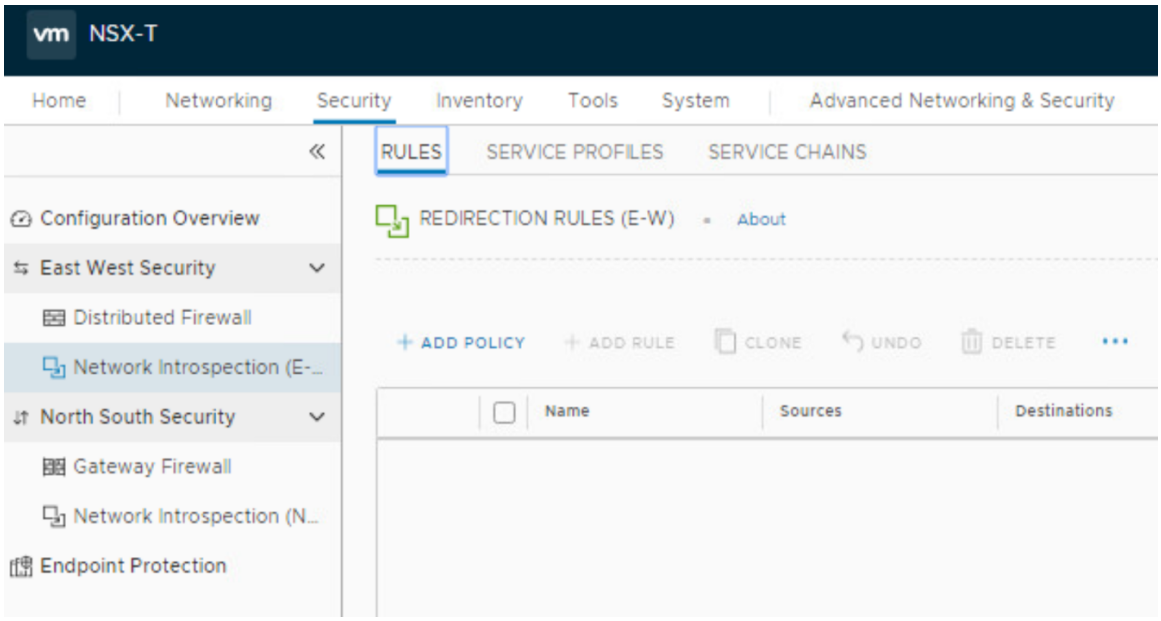
Service Deployments

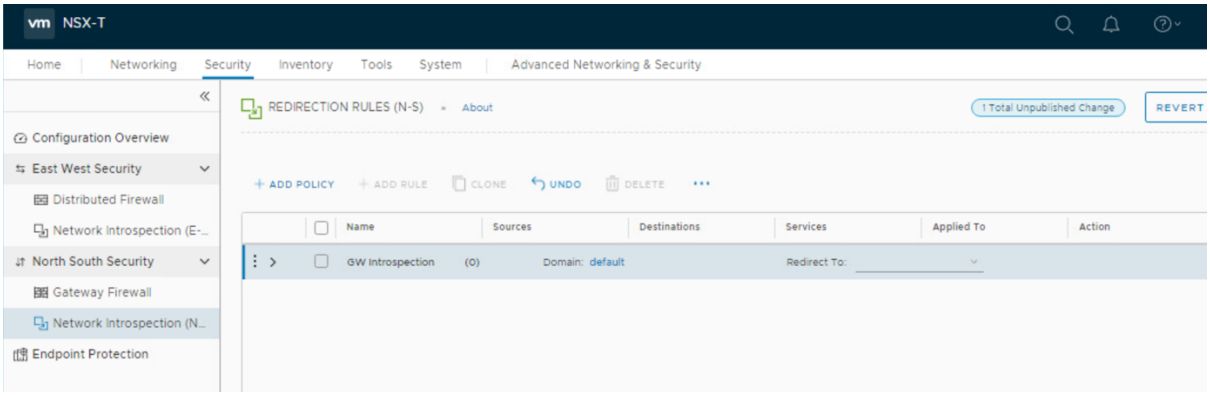
Deployment

Service Instances

Catalog






vm NSX-T
Home
Networking
Security
Inventory
Tools
System
Advanced Networking & Security
Configuration Overview
East West Security
Distributed Firewall
Network Introspection (E-...
North South Security
Gateway Firewall
Network Introspection (N...
Endpoint Protection
REDIRECTION RULES (N-S)
About
1 Total Unpublished Change
REVERT
ADD POLICY
ADD RULE
CLONE
UNDO
DELETE
Name
Sources
Destinations
Services
Applied To
Action
GW Introspection
(0)
Domain: default
Redirect To:

Section 6 – Troubleshooting and Repairing

Objective 6.1 - Identify the default log file locations of NSX-T Data Center components

NSX Policy Manager
- /var/log/policy/policy.log

NSX Manager
- /var/log/syslog
- /var/log/proton/nsxapi.log
- /var/log/nsx-audit.log

NSX Controller
- /var/log/cloudnet/nsx-ccp.log

ESXi Host
- /var/log/cfgAgent.log

KVM Host
- /var/log/vmware/nsx-syslog
- /var/log/syslog
- /var/log/openvswitch/ovs-vswitchd.log

-Two ways to view Policy Mgr Logs: NSX Manager CLI or NSX Manager root privilege mode
-Export syslogs via command on nsx mgr & edge nodes –> set logging-server …..
You can use this same command to determine what gets sent.
-export esxi & kvm logs manually on hosts
Protocols used to transfer the log data: TCP, UDP, & TLS
Severity Levels 0 →7 (emergency → Debug)

Objective 6.2 - Compare and Contrast Tools Available for Troubleshooting

IPFix – captures information about traffic flows over network
Ideal destination for flows is vRealize Network Insight for ingestion and analyzing
2 Types/Menu items – Firewall IPFix Profiles & Switch IPFix Profiles/Collectors(like vRNI, which is included in 2 highest versions of NSX)
You apply the IPFix profiles to objects like segments and segment ports.
Make sure you do not block port 4739

Port Mirroring - Forward traffic somewhere(analyzer) for inspection
Remote L3 SPAN or Logical SPAN available
Logical SPAN – analyzer is on same L2 segment
Remote L3 SPAN – send traffic to different segment analyzer

In Advanced Networking & Security menu, you have:

Traceflow is only available in Advanced UI Interface - inspects the path of traffic, can indicate down node or blocking fw rules. Works across all NSX
TZ nodes.
- tests network by injecting packets

you can specifiy unicast, broadcast, multicast, source, or destination
it will paint packetwalk in a diagram
help find bottlenecks/failures

Port Connection – very similar to Traceflow but with more granular information.

is packet capture at NSX Manager, Edge nodes, and Transport nodes
"start capture interface"
"set capture session"

Packet Captures

@ NSX mgr cluster level
Start capture interface int file count
@NSX Edge level
Set capture session # interface port-uuid direction
@ESXi level
Pktcap-uw – collect packets
tcpdump-uw – view packets
@KVM level
Tcpdump

Objective 6.3 - Troubleshoot Common NSX Installation/Configuration Issues

Corrupt download of OVA and/or QCOW2 images – check hash files
Check that ESXi has enough compute power
DNS, GW, subnet masks – incorrect network details
Remember the 12 character password requirement
Blocked ports btw hosts and vcsa
Time sync between devices
Check the following logs for errors:
NSX API Logs @/var/log/proton/nsxapi.log
Syslog @ /var/log/syslog.log
Corfu @ /var/log/corfu/
Cluster Bootstrap Mgr(CBM) @ /var/log/cbm
Get services – shows whether the service is running
Get service name
Get cluster status
Get interfaces
Get configuration – show ntp servers, hostname, domain settings that have been inputted
Get managers – view the 3 roles are up on the controllers

On esxi/kvm hosts, nsxcli is available to run commands

Objective 6.4 - Troubleshoot Common NSX Component Issues

For switching issues,

Validate switch config on hosts:

On esxi hosts, esxcfg-vswitch -l ←this will show the connected NVDS

Show TEP config on esxi hosts:

Esxcli network ip interface ipv4 get

Will show vmk10 ←this is TEP

Will show vmk50 ← this is intratier routing/networking

*Use vmkping to use TEP's to ping each other:

Vmkping ++netstack-vxlan ip -s 1572 (-s is size to check MTU size)

For Routing issues,

Usually advertisement isn't checked

BGP misconfiguration

On edge,

*Get logical-router ← look for SR and run vrf against it to get routing entries on that edge

Get bgp neighbor summary ← check for config and look for ESTAB, ACTIVE is premature and not working yet

Get bgp ipv4 ← show next hops and connected networks

*T1 in SR – Check status of HA to view which is active?

*How to check Tunnel Status on Edge? In GUI and on Edge itself

Check to view TEP are listed on the Edges' Monitor Page

For firewall issues,

Ppl tend to forget to Publish

Ppl also tend to forget to enable rules

Get firewall summary ← to view status

For checking whether the firewall rules are on transport nodes, several command line tools will expose the rules at the esxi, kvm, and edge nodes.

*How to check the firewall rules on an esxi host?

Nsxcli

➔ get firewall ….

Objective 6.5 - Troubleshoot Common Connectivity Issues

Can't login using WS1/Identity Manager? Use default NSX login at:
https://nsxmgrFQDN/login.jsp?local=true

Objective 6.6 - Troubleshoot Common physical infrastructure Issues

Nothing added here as we expect the minimally qualified candidate to already be familiar with required underlying physical infrastructure.

Section 7 – Administrative and Operational Tasks

Objective 7.1 - List Operations Tasks in a VMware NSX Environment (syslog, backup/restore. etc.)

Covered in logging section above.

Objective 7.2 - Configure roles and permissions for NSX-T Data Center environment

VMware Identity Manager(is IDaaS) – integrated with NSX-T and can leverage existing authentication services like AD

- PreReq:
  - Identity Mgr OVF
    - Identity sources
    - Authentication Methods
    - Access Policies
- Then build an OAuth client for NSX-T
- Input SHA-256 thumbprint in NSX

There are only two built in accounts in NSX-T you can use to login: admin & audit

Local users can do: CLI, APi, UI

- pw policy: 12 char,1 upper, 1 lower, 1 #, 1 special
- policies controlled via nsx cli

Identity Mgr users can do: CLI & UI only

- Policies controlled in vIDM

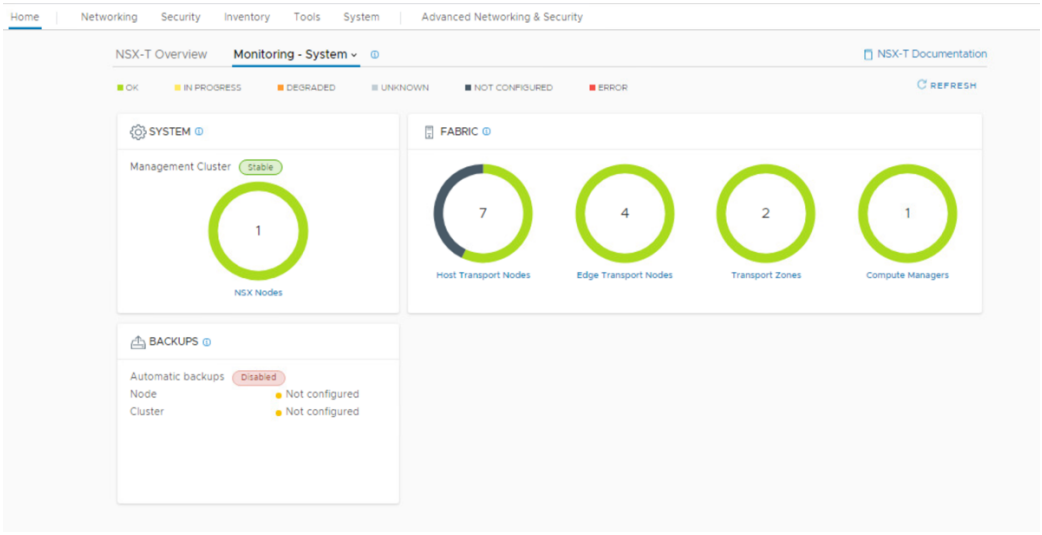
11 Preconfigured roles inside NSX (cannot be modified in any way but you can add someone to multiple roles)

Objective 7.3 - Generate Log bundles

System – Support Bundle – select which logs to package up locally

Objective 7.4 - Monitor a VMware NSX Implementation

Home page has Overview and Dashboards to view health of NSX



NSX Commandlines – from NSX-T 2.4 ICM

On NSX Manager VM

get logical-switches => get VNI's
get logical-switches VNI# vtep <- shows hosts info
mac
arp
get logical-switch segmentUUID# => shows host connections on this segment(LS)
get cluster status
get services
set cli-timeout 0
set service ssh start-on-boot
set service ssh start
get service ssh
set auth-policy minimum-password length length
set auth-policy api lockout-period period
set auth-policy api lockout-reset-period period
set auth-policy api max-auth-failures number
set auth-policy cli lockout-period period
set auth-policy cli max-auth-failures number
get log-file policy.log – via NSX CLI
tail /var/log/policy/policy.log – via NSX mgr root privilege mode
set logging-server fqdn/ip:port protocol level on management and edge nodes – syslog exporting

On NSX Edge Nodes

get load-balancers
get load-balancer UUID
get virtual-server VSID
get load-balancer UUID pools
get dns-forwarders status – indicates which edge node is active
get dns-forwarder config
get dhcp servers
get dhcp ip-pods
get ipsecvpn session active
get ipsecvpn session status
get ipsecvpn session summary
get l2vpn sessions
get l2vpn session config

On ESXi Hosts

nsxcli
get logical-switches
esxcli software vib list|grep nsx
To configure esxi to set logs out:
esxcli network firewall ruleset set -r syslog -e true
+
Esxcli system syslog config set—loghost=hostname:port
+
Esxcli system syslog reload

On KVM Hosts

dpkg -l|grep nsx

ship logs out:
root in
touch /etc/rsyslog.d/40-vmware-remote-logging.conf
echo *.*@<syslog_server_ip>:514;RFC5424fmt> /etc/rsyslog.d/40-vmware-remote-logging.conf
systemctl restart syslog

Misc Study Materials:

NSX-T 2.4 ICM (Install, Configure, & Manage Course)
https://mylearn.vmware.com/mgrReg/courses.cfm?ui=www_edu&a=one&id_subject=88522

or

NSX-T 2.4 ICM On Demand Course offered in the VMware Learning Zone:
https://mylearn.vmware.com/mgrReg/courses.cfm?ui=www_edu&a=one&id_subject=90573

On VMware Learning Zone, there are Certification Exam Prep videos.
VMware Professional NSX-T Data Center 2.4 Exam Prep:
https://vmwarelearningzone.vmware.com/oltpublish/site/program.do?dispatch=showCourseSession&id=5c0e080a-e426-11e9-b1f7-0cc47a3505aa

Quizlet Flash Cards for practicing NSX-T 2.4 information:
https://quizlet.com/_8f7j78?x=1jqt&i=2lgim6