VCP-NV 6.0 Study guide by Rich Dowling (@virtRich)

https://richdowling.wordpress.com

Contents

VCP-NV 6.0 Study guide by Rich Dowling (@virtRich)

https://richdowling.wordpress.com

VCP-NV 6.0 Study guide by Rich Dowling (@virtRich)

https://richdowling.wordpress.com

Section 1 – Define VMware NSX Technology and Architecture

Objective 1.1 – Describe the Benefits of a VMware NSX Implementation

Benefits:

- Increased efficiency and agility through automation
- Independent of hardware
- Easy 3rd party integration through APIs
- Non-disruptive deployment (using L2 bridging)

Knowledge

- Identify challenges within a physical network interface
    - complex and vendor specific
    - provision is slow
    - workload placement and mobility limited by physical topology
    - inflexible dedicated hardware creates artificial barriers
    - efficiency is reduced by fragmentation
    - VLAN/Firewall rule sprawl

- Explain common VMware NSX terms
    - NSX Edge – Services Router, load balancing, N-S routing
    - NSX vSwitch – An extended Distributed vSwitch, with VXLAN, Distributed Logical Router and Distributed Firewall hypervisor extension modules.
    - Consumption layer – Where the workload resides
    - Management Plane - NSX Manager
    - Control Plane - NSX Controller
    - Data Plane – Services layer, logical switch (open vswitch or NSX switch), distributed logical router, distributed firewall
    - MTU – Maximum Transmission Unit (limit on packet size)
    - VTEP – VXLAN Tunnel End Point(s). Used to transport the encapsulated traffic between hosts/edges.
    - Overlay network - flexible logical L2 overlay over existing IP networks on existing physical infrastructure without the need to re-architect any of the data center networks. Provides E-W and N-S communication while maintaining isolation between tenants.
- Describe and differentiate functions and services performed by VMware NSX
    - Logical Firewall
      The Distributed Firewall component of Logical Firewall allows you to segment virtual datacenter entities like virtual machines based on VM names and attributes, user identity, vCenter objects like datacenters, and hosts as well as traditional networking attributes like IP addresses, VLANs, etc. The Edge Firewall component helps you achieve key perimeter security needs such as building DMZs based on IP/VLAN constructs, tenant to tenant isolation in multi-tenant virtual data centers, Network Address Translation (NAT), partner (extranet) VPNs, and User based SSL VPNs. The Flow Monitoring feature displays network activity between virtual machines at the application protocol level. You can use this information to audit network traffic, define and refine firewall policies, and identify threats to your network.

- Logical Load Balancer
  The NSX Edge load balancer enables network traffic to follow multiple paths to a specific destination. It distributes incoming service requests evenly among multiple servers in such a way that the load distribution is transparent to users. Load balancing thus helps in achieving optimal resource utilization, maximizing throughput, minimizing response time, and avoiding overload. NSX Edge provides load balancing up to Layer 7.
- Logical VPN
  SSL VPN-Plus allows remote users to access private corporate applications. IPSec VPN offers site-to-site connectivity between an NSX Edge instance and remote sites. L2 VPN allows you to extend your datacenter by allowing virtual machines to retain network connectivity across geographical boundaries.

- Logical L2 – Switch
  creates logical broadcast domains or segments to which an application or tenant virtual machine can be logically wired. This allows for flexibility and speed of deployment while still providing all the characteristics of a physical network's broadcast domains (VLANs) without physical Layer 2 sprawl or spanning tree issues.

- Logical L3 – Router
  NSX extends dynamic routing intelligence, to where the workloads reside, for doing East-West routing. This allows more direct virtual machine to virtual machine communication without the costly or timely need to extend hops. At the same time, NSX also provides North-South connectivity, thereby enabling tenants to access public networks.

- Service Composer
  helps you provision and assign network and security services to applications in a virtual infrastructure. You map these services to a security group, and the services are applied to the virtual machines in the security group. Data Security provides visibility into sensitive data stored within your organization's virtualized and cloud environments. Based on the violations reported by NSX Data Security, you can ensure that sensitive data is adequately protected and assess compliance with regulations around the world.

- Describe common use cases for VMware NSX
  - DataCenter Automation
    - Automate network provisioning via API
    - Streamline DMZ changes
  - Self Service Enterprise IT
    - Rapid application deployment with automated network and service provisioning for private clouds and test/dev environments
    - Isolated dev, test and prod environments on same physical infrastructure
  - Multi-tenant clouds
    - Automate network provisioning for tenants with customisation and complete isolation
    - Maximise hardware sharing across tenants
  - DataCenter Simplification
    - Network isolation
    - Freedom of VLAN/Firewall rule sprawl

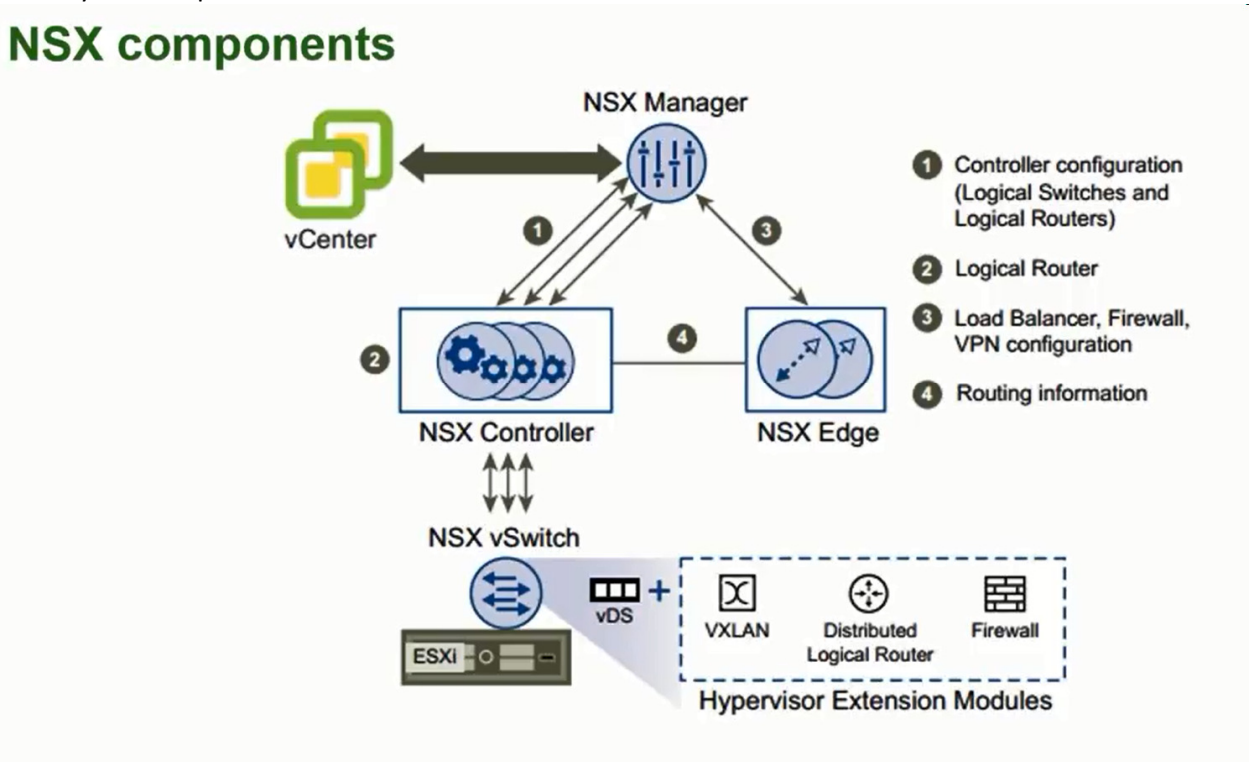
Tools

- VMware NSX Datasheet
- VMware NSX Network Virtualization Platform white paper
- VMware NSX Network Virtualization Design Guide

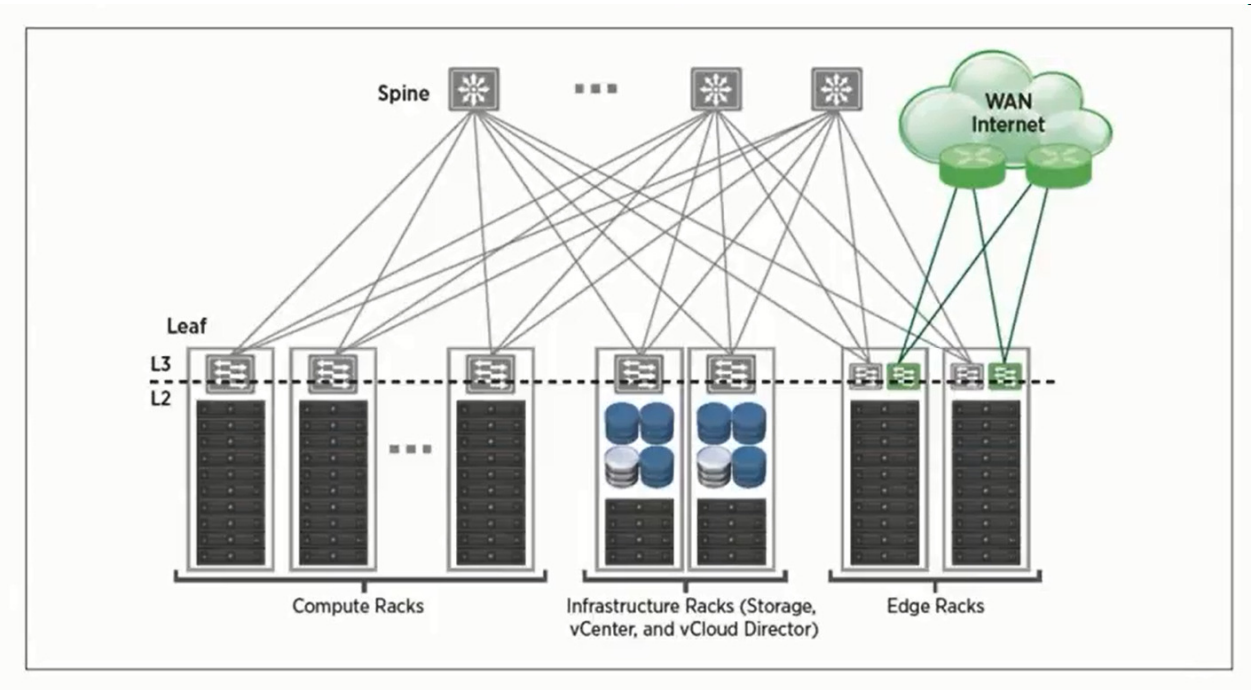
Objective 1.2 – Describe VMware NSX Architecture

Knowledge

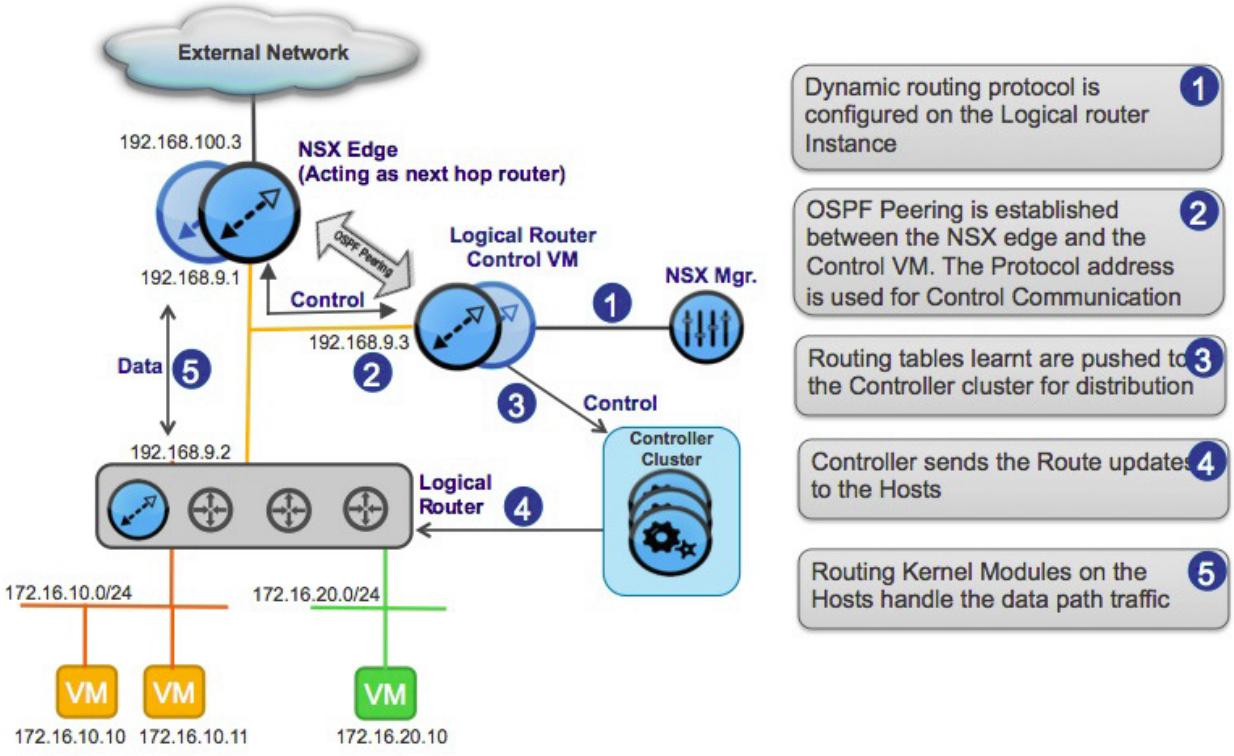
- Identify the components in a VMware NSX stack



  - NSX Manager - The NSX manager provides the single point of configuration and the REST API entry-points in a vSphere environment for NSX.
  - NSX Controller – manages NSX vSwitches, sends Router/Switch/Firewall config to NSX vSwitch
  - NSX Edge – Load Balancer, Firewall, VPN configuration
  - NSX vSwitch – vDS + Hypervisor Extentsion Modules (VXLAN, DLR, Firewall)
- Identify common physical network topologies
  (see design guide, especially leaf and spine)



- Describe a basic VMware NSX topology



- Differentiate functional services delivered by a VMware NSX stack
  - Dynamic routing
  - Firewall
  - NAT
  - DHCP
  - Site-to-site VPN (IPSEC)

- L2 VPN (stretch Datacenter)
- SSL VPN-Plus (users)
- Load Balancing
- High Availability
- Distributed Firewall

Tools

- VMware NSX Network Virtualization Design Guide
- NSX Administration Guide

Objective 1.3 – Differentiate VMware Network and Security Technologies

Knowledge

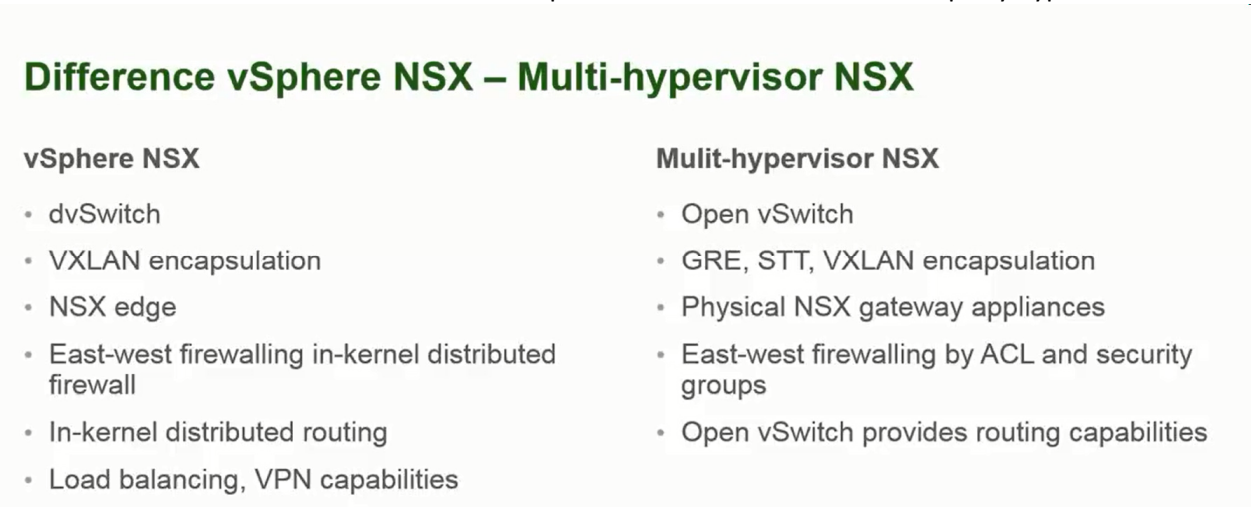
- Identify upgrade requirements for ESXi hosts
  - vCenter 5.5 or later
  - ESXi 5.0 or later (unicast mode only available with ESXi 5.5)
  - vHW 7+ and VMware tools 8.6+ reqd for vshield endpoint and data security.
  - Specific upgrade procedure for vCNS
  - vShield App needs to be on 5.5+
- Identify steps required to upgrade a vSphere implementation
  - Upgrade to NSX Manager (can load vib into vCNS upgrade page)
  - Upgrade Logical Switches
  - Upgrade to NSX Firewall
  - Upgrade NSX Edge
  - Upgrade vShield Endpoint
  - "Upgrade" NSX Data Security (actually an uninstall before NSX Manager upgrade/reinstall)
  - Upgrade Partner Solutions

- Describe core vSphere networking technologies
  - Already covered by VCP-DCV study guides – Networking for VMware Administrators book
  - Ensure you know about Port mirroring and Netflow

- Describe vCloud Networking and Security technologies
  - Firewall – Stateful inspection firewall that can be applied either at the perimeter of the virtual data center or at the virtual network interface card (vNIC) level directly in front of specific workloads. The firewall-rule table is designed for ease of use and automation with VMware vCenter™ objects for simple, reliable policy creation. Stateful failover enables high availability for business-critical applications.
  - VPN – Industry-standard IPsec and SSL VPN capabilities that securely extend the virtual data center. Site-to-site VPN support links virtual data centers and enables hybrid cloud computing at low cost. The SSL VPN capability delivers remote administration into the virtual data center through a bastion host, the method favoured by auditors and compliance regulators.
  - Load balancer – A virtual-appliance–based load balancer to scale application delivery without the need for dedicated hardware. Placed at the edge of the virtual data center, the load balancer supports Web-, SSL- and TCP-based scale-out for high-volume applications.
  - VXLAN – Technology that, along with VMware vSphere Distributed Switch, creates Layer 2 logical networks across non-contiguous clusters or pods without the need for VLANs

(multicast required). This enables you to scale your applications across clusters and pods and improve compute utilization.
    - Instrumentation – Granular network traffic telemetry that enables rapid troubleshooting and incident response. Traffic counters for sessions, packets and bytes provide visibility into the virtual network and streamline firewall-rule creation.
    - Management – Integrates with vCenter Server and vCloud Director to provide separation of duties with role- based access control (RBAC) while providing a central point of configuration and control for network and security services.
    - vCloud Ecosystem Framework – Integrates partner services at either the vNIC or the virtual edge using REST APIs.

- Describe and differentiate VMware NSX for vSphere and VMware NSX for third-party hypervisors



Tools

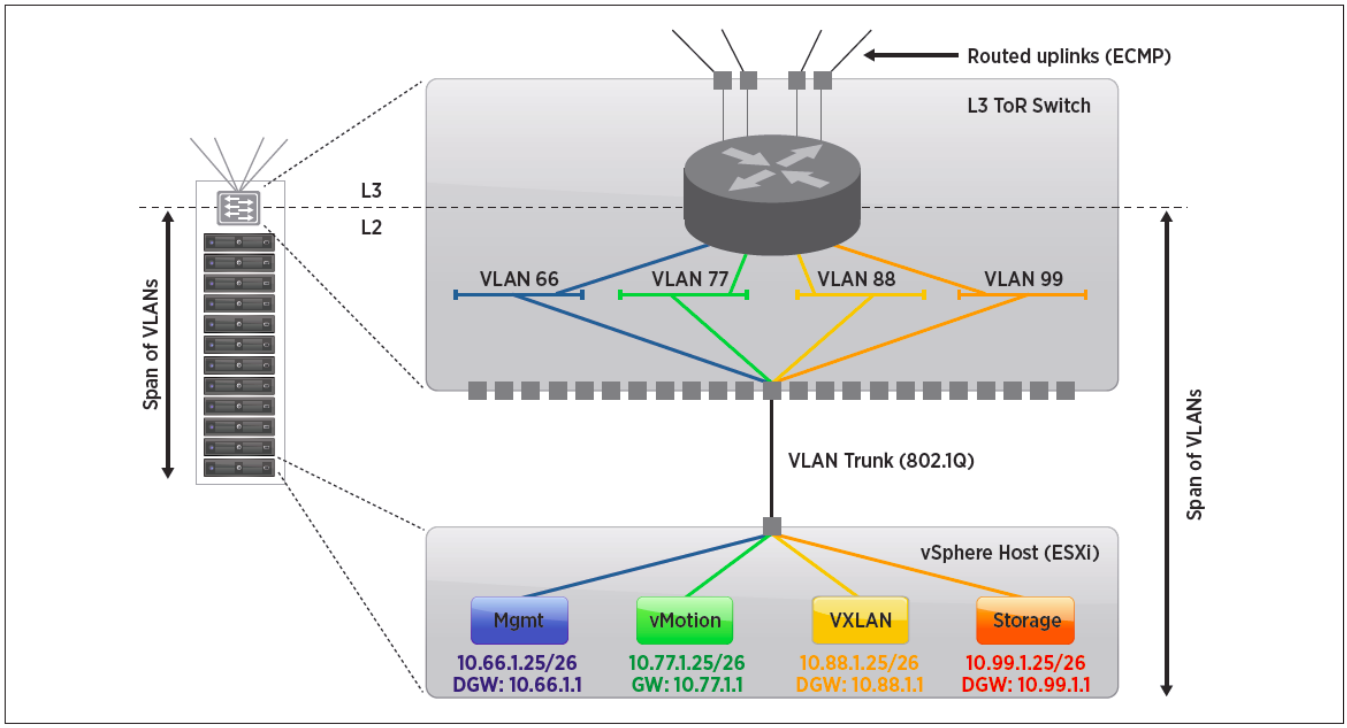
- vSphere Installation and Setup Guide
- vSphere Upgrade Guide
- vSphere Networking Guide
- VMware vCloud Networking and Security Overview white paper
- NSX Administration Guide
- NSX User's Guide

Objective 1.4 – Contrast Physical and Virtual Network Technologies

Knowledge

- Differentiate logical and physical topologies
  Any given node in a network has one or more physical links to other devices in the network; graphically mapping these links results in a geometric shape that can be used to describe the physical topology of the network. Conversely, mapping the data flow between the components determines

the logical topology of the network.



- Physical
  The cabling layout used to link devices is the physical topology of the network. This refers to the layout of cabling, the locations of nodes, and the interconnections between the nodes and the cabling. eg Server Port, Rack switch, Leaf switch, Spine layer

  - Simple – configuration must be simple. Much of the general config must be identical on every component. Differences in configuration would soon become unmanageable
  - Scalable - the number of racks supported in a fabric is dictated by the total number of ports available across all spine switches and the oversubscription that is acceptable.
  - High-bandwidth - In spine–leaf switch topologies, oversubscription typically occurs—if at all—at one point: the leaf switch. The calculation is simple: total amount of bandwidth available to all servers connected to a given leaf switch divided by the aggregate amount of uplink bandwidth provides the oversubscription. More or less bandwidth can be made available to a rack by virtue of provisioning more or fewer uplinks
  - Fault-tolerant - Multipathing-capable fabrics handle box or link failures, reducing the need for manual network maintenance and operations
  - QoS-providing – L2 QoS is “Class of Service”, L3 QoS is “DSCP marking”. QoS values are used to decide which traffic is prioritised or dropped if there is congestion.
  - Firewalls only at routable interfaces
- Logical
  The logical topology, is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices. Logical topologies are usually Shared Media, or Token Based.

- Differentiate logical and physical components (i.e. switches, routers, etc.)
  - Switches
    - Physical Switch – ports are either single VLAN or Trunk ports. Limited set of 4096 VLANs per fabric.
    - NSX vSwitch – abstracts the physical network and provides access-level switching in the hypervisor. It is central to network virtualization because it enables logical networks that are independent of physical constructs such as VLAN. A Logical switch is distributed and can span arbitrarily large compute clusters, allowing for VM mobility within the datacenter without limitations of the physical L2 boundary.
  - Routers
    - Physical router – fixed topology, traffic forced to "hairpin" out from hosts to route between VLANs.
    - Logical router enables E-W routing to remain within the host rather than hair-pinning out to a physical router
- Differentiate logical and physical services (i.e. firewall, NAT, etc.)
  - Firewall
    - Physical firewalls are part of the routing topology, and traffic has to pass through it to be inspected. They suffer from rule sprawl, as rules are added but rarely removed, due to the perceived risk of removing an "in use" rule.
    - Distributed firewalls can protect individual VMs, have dynamic rulesets, allow rules on userids. By only having "relevant" rules pushed down from the NSX Manager, performance is increased in comparison with comparing against the whole rulebase.
  - NAT
    - NAT is normally performed by firewalls, but can be done by routers. Choice of Destination, Source, or Hide NAT.
    - Performed by the NSX Edge. Choice of Destination or Source NAT. Must be used when there is overlapping tenant addressing
  - Load Balancing
    - In the physical network this is usually provided by a physical appliance (e.g. F5 device). Normally requires manual configuration for any new services.
    - NSX load balancing is fully programmable via API, and scales to support very demanding applications (up to 9Gbps throughput, 1M concurrent connections)
- Differentiate between physical and logical security constructs
  Physical security constructs are generally tied to dedicated hardware, and are inflexible, and difficult to integrate with automation.
  Logical security constructs in NSX are tightly integrated into vSphere making rule creation faster and less error prone. Rules can include dynamic groups and be configured by automation.

  - Service Composer
    - Create rules to dynamically put VMs in specific groups (move to isolated network if infected)
    - Simple dynamic security policies without the need for phusical subnets, VLANS, ACLs or firewall rules.
  - Endpoint Security
    - VMware endpoint service used by 3rd parties to protect VMs without in-guest agents. E.g. for anti-virus, IDS/IPS
    - Ties in with Service Composer to allow automated provisioning of Security Virtual Appliances and orchestration of policy.
  - Data Security
    - Needs vShield endpoint

- Provides visibility into sensitive data stored within VMs
- Policy driven
- Support for PCI, PHI, PII types of restricted data

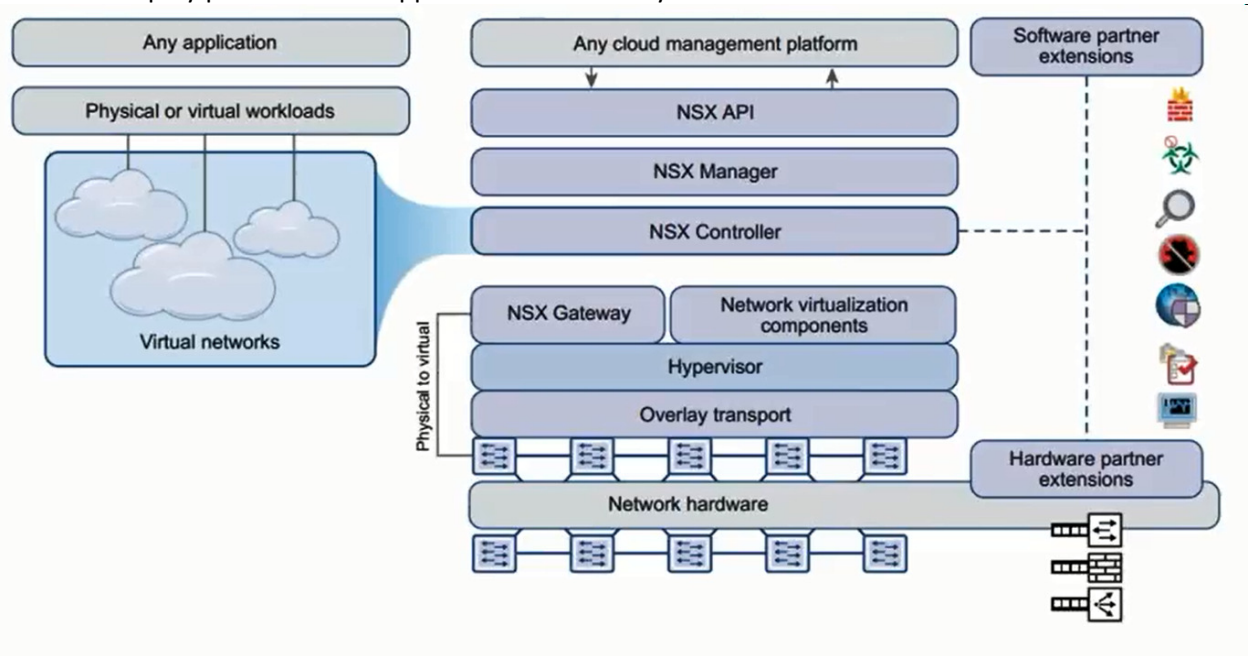
Tools

- VMware NSX Network Virtualization Design Guide
- NSX User's Guide

Objective 1.5 –Explain VMware NSX Integration with Third-Party Products and Services

Knowledge

- Describe integration with third-party hypervisors
  - Openvswitch used for integration with KVM/Xen
  - Doesn't have in-kernel mode modules
- Describe integration with third-party cloud automation
  - Uses a RESTful API to integrate with cloud automation
- Describe integration with third-party services
  - Registered automatically or manually to NSX Manager
  - Service Definitions may need to be created
  - Then Deploy partner virtual appliance automatically to chosen clusters



  - Network services
    - L2 Gateway, Load Balancing
  - Security services
    - Firewall, Anti-virus, IDS/IPS
- Describe integration with third-party hardware
  - Newer F5 devices can participate as part of the transport zone by interacting with the NSX API
  - Network Interface Cards (NICs)
    - Ensure consistent mapping of uplinks on the vDS to the network fabric

- Terminating overlay networks
  - Overlay network terminated by VTEP or Edge
  - To support VTEP in switch, it must support the Open VSwitch Database (OSVDB)

- Manually register a third-party service with NSX
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click Service Definitions.
  - Click the New Service Definition (+) icon.
  - Type a name and version for the service that you are inserting.
  - Select the service manager and type a description for the service. Your service manager manages your services in the NSX environment.
  - Select the deployment mechanism for the solution.
  - Add the required attributes by clicking the New Attribute (+) icon.
  - Click Next and select the service categories within which you want to add the solution.
  - Click Next.
  - The Configure Service Manager page is displayed only if you selected New Service Manager in step 5.
  - On the Configure service manager page, configure the service manager for the service you are adding.
    - Type a name and description for the service manager.
    - In Administrative URL, type the URL of the solution provider's service manager.
    - In Base API URL, type the URL of the web site where the service manager's REST APIs are available and the thumbprint of the service manager.
    - In Credentials, type the username and password for logging in to the service manager.
    - In Vendor Details, type the solution provider's ID and name.
    - Click Next.
  - On the Add service configuration page, click the New Service Definition (+) icon to add one or more
  - service configurations.
  - Click Next.
  - On the Add profile configuration page, add one or more service profiles.
    - Type the configuration ID, name, and description for the profile.
    - Add one or more attributes by clicking the New Attribute (+) icon.
    - Click OK.
    - On the Add profile configuration page, click Next.
  - Select the required transports and click Next.
  - Review settings and click Finish.

- Install a third-party service with NSX
  - Click Networking & Security and then click Installation.
  - Click the Service Deployments tab and click the New Service Deployment (+) icon.
  - In the Deploy Network and Security Services dialog box, select the appropriate solution(s).
  - In Specify schedule (at the bottom of the dialog box), select Deploy now to deploy the solution immediately or select a deployment date and time.
  - Click Next.
  - Select the datacenter and cluster(s) where you want to deploy the solution and click Next.
  - On the Select storage page, select the datastore on which to add the solution service virtual machines storage or select Specified on host.The selected datastore must be available on all hosts in the selected cluster. If you selected Specified on host, the datastore for the ESX host

must be specified in the AgentVM Settings of the host before it is added to the cluster. See vSphere API/SDK Documentation.
- Click Next.
- On the Configure management network page, select the distributed virtual port group to host the management interface. This port group must be able to reach the NSX Manager's port group. If the network is set to Specified on host, the network to be used must be specified in the Agent VM Settings > Network property of each host in the cluster. See vSphere API/SDK Documentation. When you add a host(s) to the cluster, the Agent VM Settings > Network property for the host must be set before it is added to the cluster. The selected port group must be available on all hosts in the selected cluster.
- In IP assignment, select one of the following: DHCP, An IP Pool
- Click Next and then click Finish on the Ready to complete page.
- Monitor the deployment till the Installation Status displays Successful. If the status displays Failed, click the icon next to Failed and take action to resolve the error.

Tools
- NSX Administration Guide
- Next Generation Security with VMware NSX and Palo Alto Networks VM-Series white paper
- Deploying VMware NSX with Cisco UCS and Nexus 7000

Objective 1.6 –Explain VMware NSX Integration with vCloud Automation Center (vCAC)

Knowledge
- Describe integration with vCAC
  - It allows users to create complete application templates which combine compute, storage, networking and security services in a blueprint for on-demand deployment
  - It allows for security automation workflows to be integrated with compute automation
  - With Layer 2 VPN on NSX Edge, enterprises can migrate workloads, consolidate datacenters, or create stretched application tiers across multiple datacenters. Service providers can offer tenant on-boarding and cloud bursting services where tenant application networks are preserved across datacenters without the need for NSX on customer premises.
  - Helps you optimize resource utilization and scale by dynamically connecting self-service applications to NSX logical networks while ensuring that infrastructure security policies are automatically applied to isolate and protect the applications
- Explain NSX deployment capabilities built into vCAC
  - Application-specific networks may be defined in a multimachine blueprint for vCloud Networking and Security and NSX.
- List NSX components that can be pre-created using vCAC
  - Logical Router
  - Logical Switch
  - Virtual Network Adapters
  - Virtual Load Balancers
- Describe Network Profiles available in vCAC
  - They perform 2 main functions:
    - NIC configuration (IP, Subnet Mask, Default Gateway, DNS)
    - NSX Edge Services Router configuration (Route, NAT, Drop)
  - 5 main types

        - External Profile – Used to pass config information to catalog items that are not associated with a blueprint, or to provide information which is used to configure the NSX Edge Services Router
        - 1-to-1 NAT Profile – Used to conserve externally routable IP addresses.
        - 1-to-Many NAT Profile – As above, but no Source NAT.
        - Private Profile – No external connectivity
        - Routed Profile – IP range must be unique, IP addressing uses a valid external range.
- Explain NSX preparation tasks that must be completed prior to attaching a network profile to a blueprint
    - Create Logical Distributed routers
    - Create Transport Zones
    - ?? Not sure if anything else is required.
- Explain vCAC preparation tasks that must be completed prior to deploying a machine with on-demand network services
    - Add NSX Manager to vSphere endpoint
    - Configure reservations
        - External Network Profiles
        - Transport Zone
        - Routed Gateway
    - Configure Blueprints – Multi-machine
        - Configure transport zone
        - Configure network profile
        - Add VM blueprints
        - Identify any Security Groups required
        - Edit network -> associate network profile, configure additional services like load balancer

Tools

- IaaS Configuration for Virtual Platforms
- IaaS Configuration for Multi-Machine Services
- Also see http://blogs.vmware.com/management/2014/05/vcac-nsx-dynamically-configuring-application-specific-network-services.html

Section 2 – Plan and Configure vSphere Networking

Objective 2.1 – Define Benefits of Running VMware NSX on Physical Network Fabrics

Knowledge

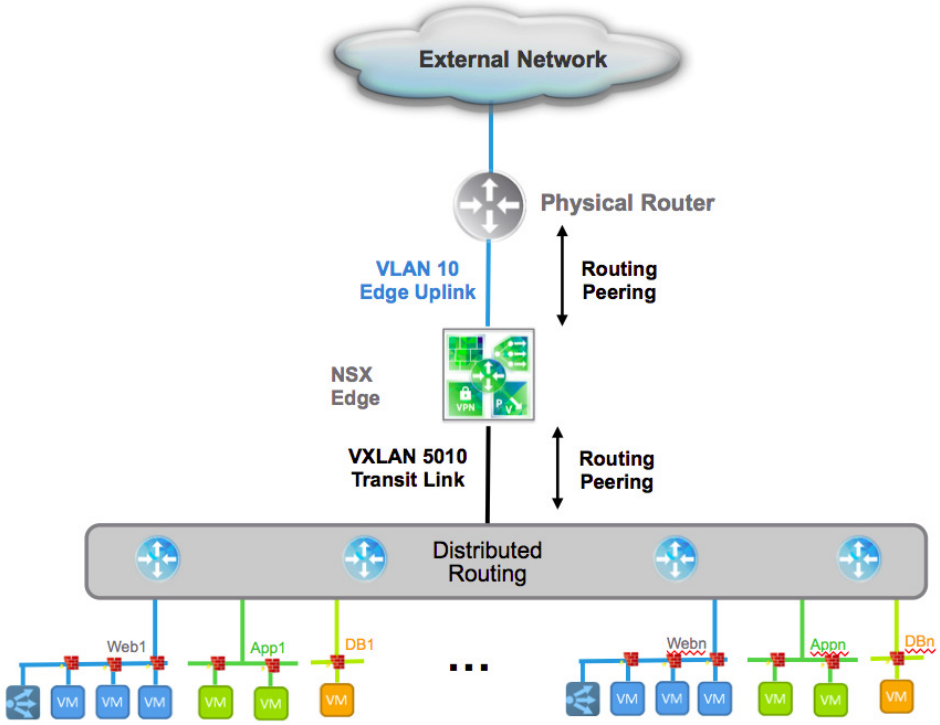
- Identify physical network topologies (Layer 2 Fabric, Multi-Tier, Leaf/Spine, etc.)
    - L2 is the data link layer in ISO. Communication via MAC addresses (IPs looked up to MAC)
    - 3 tier network –
        - Core – routing between distribution switches, VPN, internet (Nexus 7000/9000)
        - Distribution – L3 routing between connected access switches (Nexus 5000)
        - Access – top of rack switches, typically L2 only, or fabric extender
        - Reduces structured cabling
    - Collapsed core
        - Core and distribution are combined
        - Top of rack switches may be L2 or L3
        - More likely for 100% virtualised DC
    - Leaf/Spine
        - Like collapsed core but all links are forwarding
        - Because all links are forwarding, gives real horizontal scalability benefits
        - Can't use Spanning Tree (as it is a path blocking protocol)
    - Traffic flows
        - East-West – ie between application layer. E-W flows have to be routed (hair-pinning)
        - North-South – up to internet/vpn, down to physical DB
    - Traffic flows in NSX
        - East-West – uses distributed routers/logical switches to keep the traffic in virt layer. Only a single L2 network use in the Transport Zone for VM to VM traffic
        - North-South – uses "edge" logical routers which sit on perimeter, can have ECMP load balancing of up to 8 devices, and OSPF used to control traffic flow.
        - F5 have created a VTEP which means physical F5 can be E-W traffic.

- Identify physical network trends
    - Multi-tier networks are migrating to Spine-Leaf networks because of Cloud Computing
    - Port speeds are increasing 1G->10G->40G

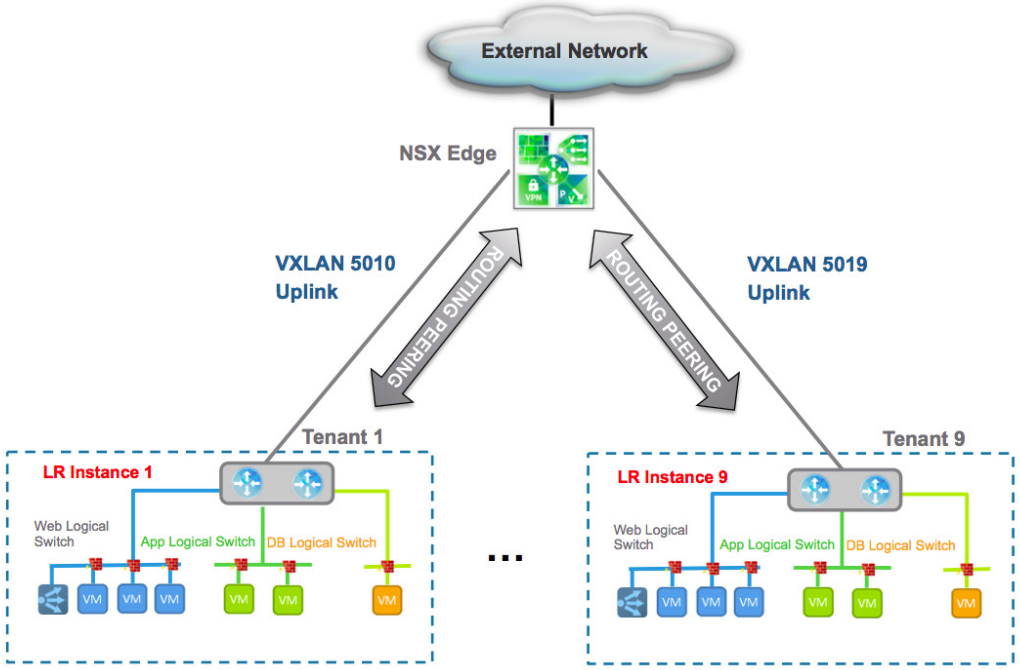
- Explain the purpose of a Spine node
    - Part of the aggregation/spine layer that provides connectivity between racks

- Explain the purpose of a Leaf node
    - Typically located inside a rack and provides network access to the servers inside that rack

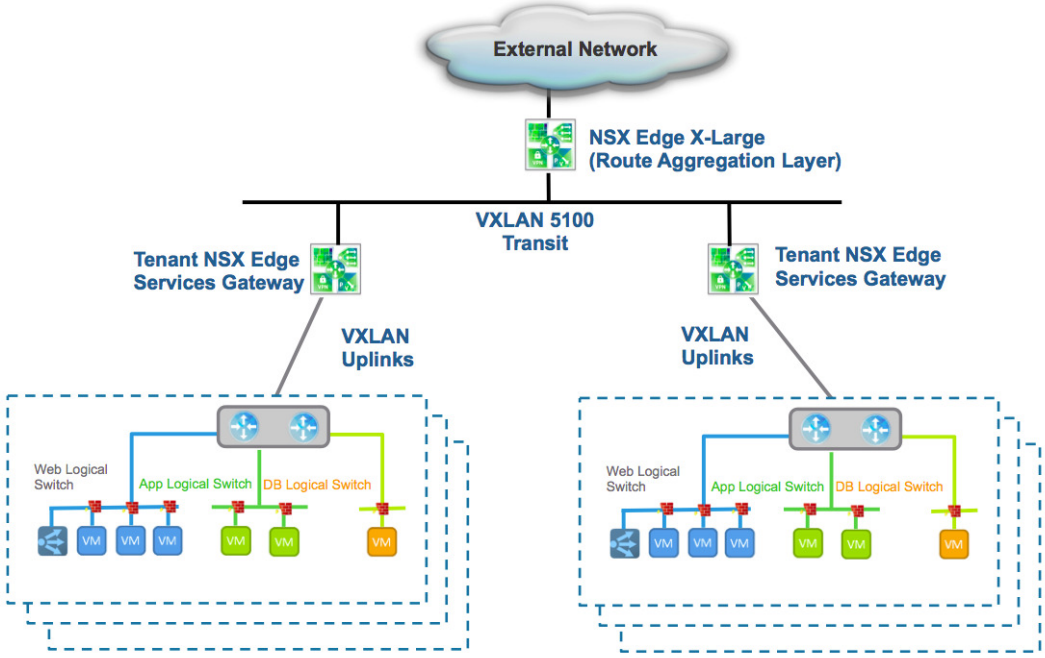
- Identify virtual network topologies (Enterprise, Service Provider Multi-Tenant, Multi-Tenant Scalable)
    - Enterprise



- Service Provider – Multi-Tenant



- Multi-Tenant Scalable



- Explain benefits of Multi-Instance TCP/IP stack
  - Helps you move to a software defined datacenter model.
  - Useful in environments that are nearing the 4000 VLAN limitation
  - Abstracts the VM layer from the physically allocated VLANs

- Describe challenges in a Layer 2 Fabric topology
  - Scalability (arp/mac table size)
  - Broadcast, Unknown unicast, and Multicast (BUM) traffic flooding

- Describe challenges in a Multi-Tier topology
  - Scalability
  - Fault tolerance
  - Energy efficiency
  - Cross-sectional bandwidth
  - Higher layers are highly oversubscribed

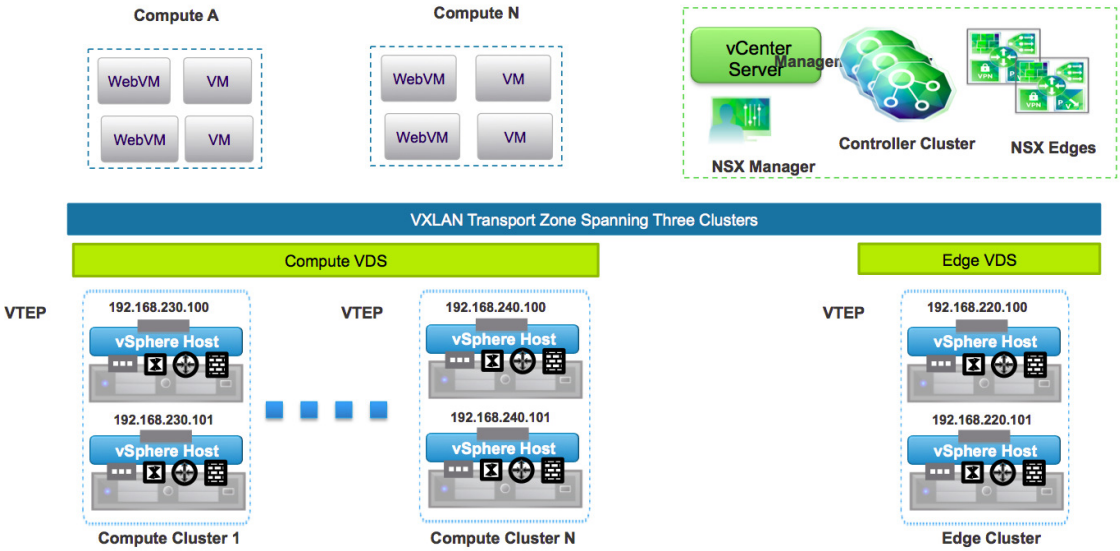
- Describe challenges in a Leaf/Spine topology
  - Specific VLANs exist only in a single rack
  - Full Mesh connectivity between Leaf and Spine layers becomes complex as size increases.
  - Can't use Spanning Tree multipathing – use ECMP, TRILL, ISIS etc

- Differentiate physical/virtual QoS implementation
  - Physical
    - Generally marked for QoS by an ingress router interface
    - Difficult to manage
    - Different tenants may have different QoS values
    - Supports L2 QoS sometimes referred to as "Class of Service" (CoS) and L3 QoS referred to as "DSCP marking"
  - Virtual

- Marked for QoS by the Hypervisor
- Network infrastructure must trust values set by the Hypervisor (trusted boundary)
- NSX can either trust and DSCP marking applied by a VM or explicitly modify and set it at the Logical Switch level.

- Differentiate single/multiple vSphere Distributed Switch (vDS) Distributed Logical Router implementations
  - Single vDS
    - Can share compute resources between Compute and Edge clusters
    - One of the requirements of a single-VDS–based design is that a single VLAN is defined for VXLAN transport network.

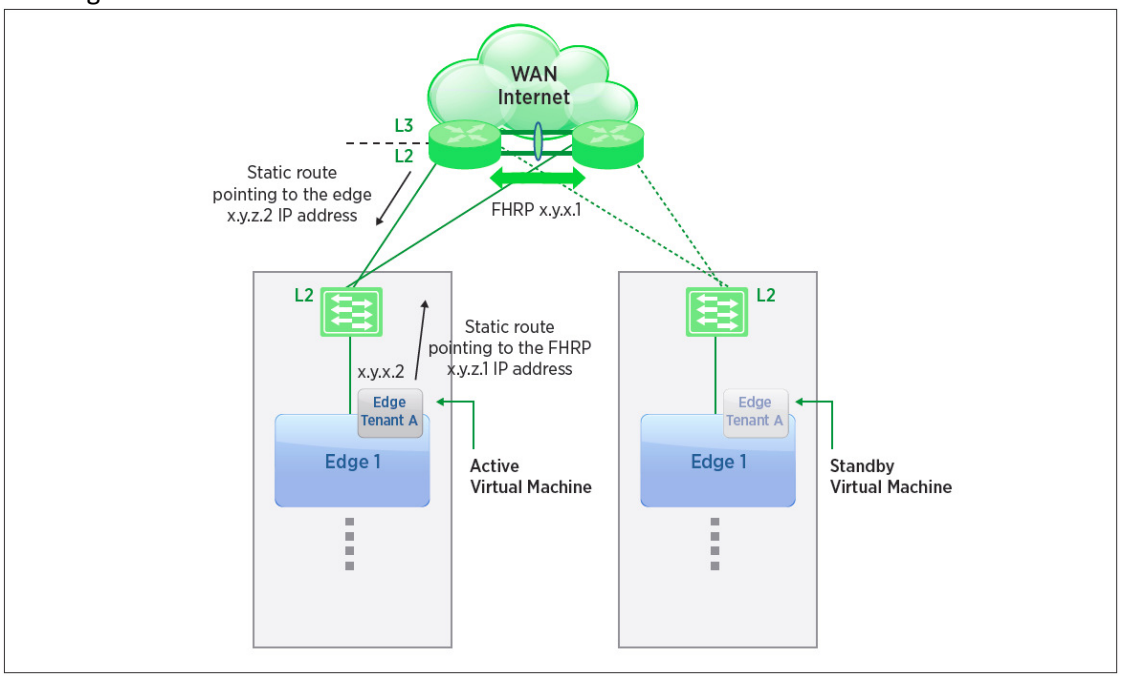
  - Multiple vDS



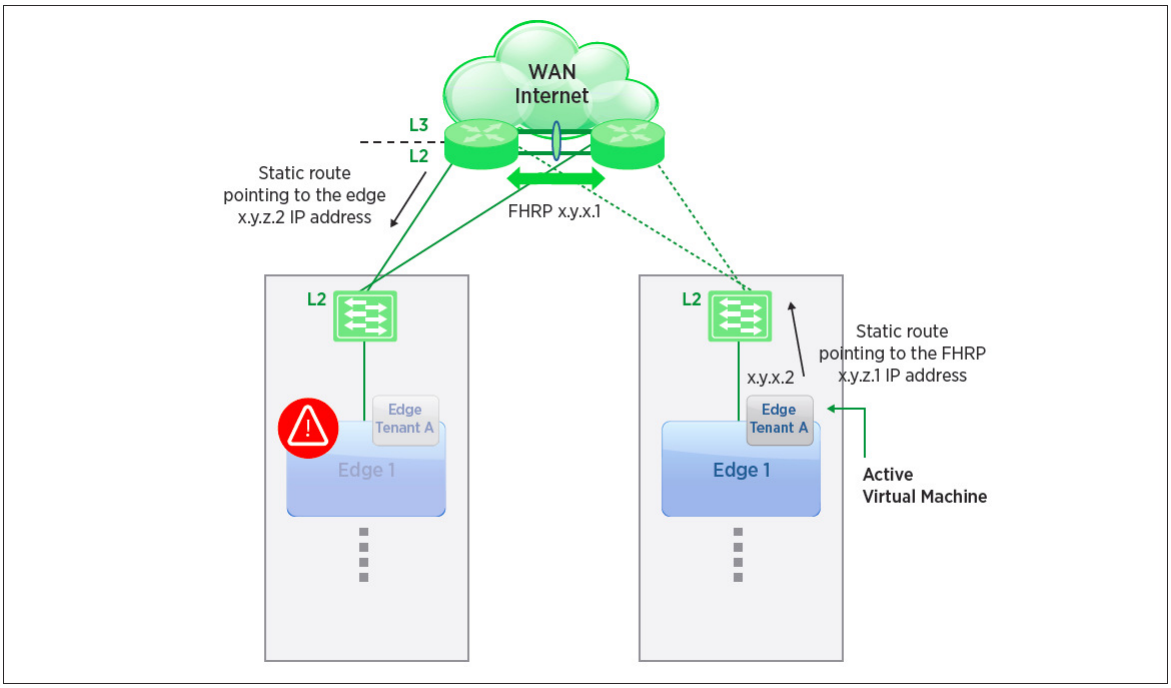
    - Although a design with a single VDS spanning both compute and edge cluster is possible, there are several advantages in keeping separate VDS for compute and edge:
      - Flexibility of span of operational control: typically compute/virtual infrastructure admin and network admin are separate entities and thus each domain can manage the cluster specific tasks. These benefits are already a factor in designing a dedicated cluster and rack for specific services and further substantiated by the VDS design choices.
      - Flexibility in managing uplink connectivity on computes and edge clusters - see for example the above discussion on uplink design and the recommendation of using different teaming options for compute and edge clusters.
      - Typically the VDS boundary is aligned with the transport zone and thus VMs connected to logical switches can span the transport zone. However, the vMotion boundary is always limited by the extension of a VDS, so keeping a separate VDS for compute resources ensures that those workloads will never be moved (by mistake or by choice) to ESXi hosts dedicated to other services.
      - Flexibility in managing VTEP configuration – see above discussion on VTEP design choices.

- Avoiding exposing VLAN-backed port-groups used by the services deployed in the edge racks (NSX L3 routing and NSX L2 bridging) to the compute racks..

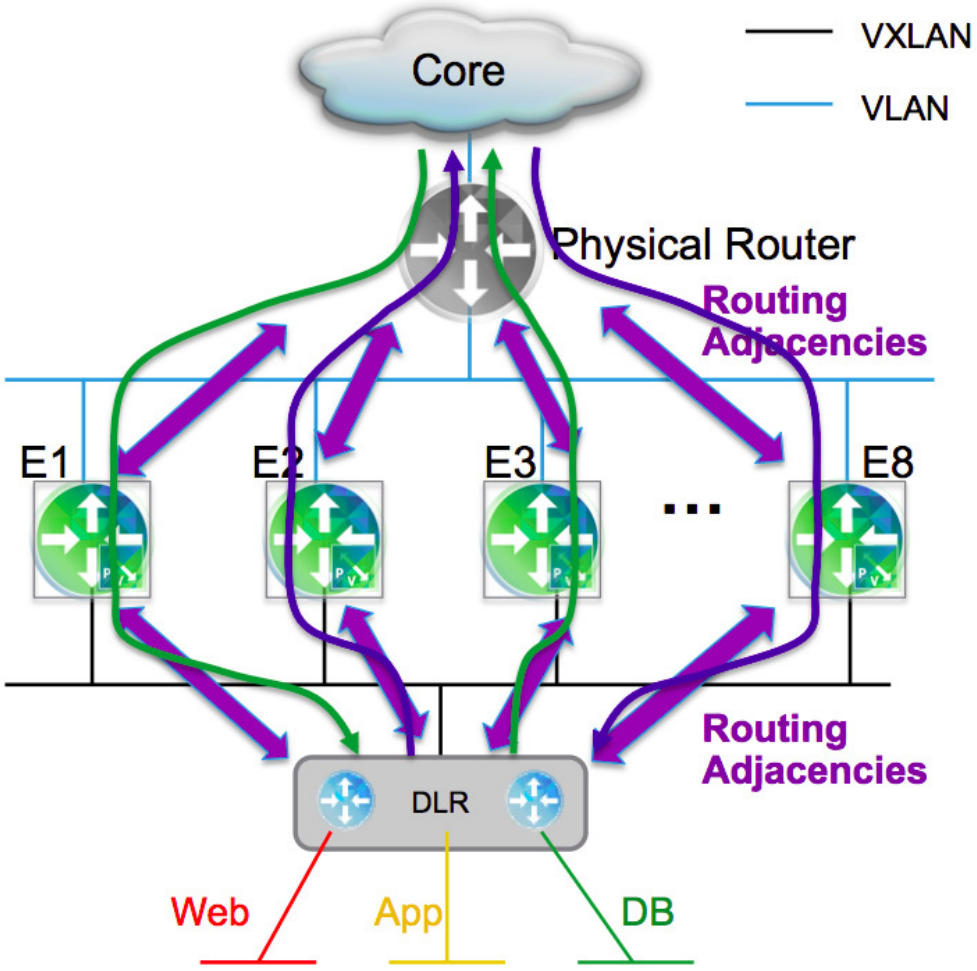
- Differentiate NSX Edge High Availability (HA)/Scale-out NSX Edge HA implementations
  - NSX Edge HA



If the active edge fails, the standby takes over and assumes the outside IP address of the previously active edge. To notify the upstream infrastructure (the L2 switches that potentially interconnect the Edge and the first physical router) a GARP message is sent out. For this mechanism to work, a VLAN must be extended between the edge racks. Tunnel interfaces connecting the VXLAN endpoints do not have to extend any VLAN. Before the failover, the hypervisor VTEPs sent traffic to the VTEP of the hypervisor hosting the edge. After failover, that traffic is sent to the VTEP of the hypervisor that hosts the newly active edge.

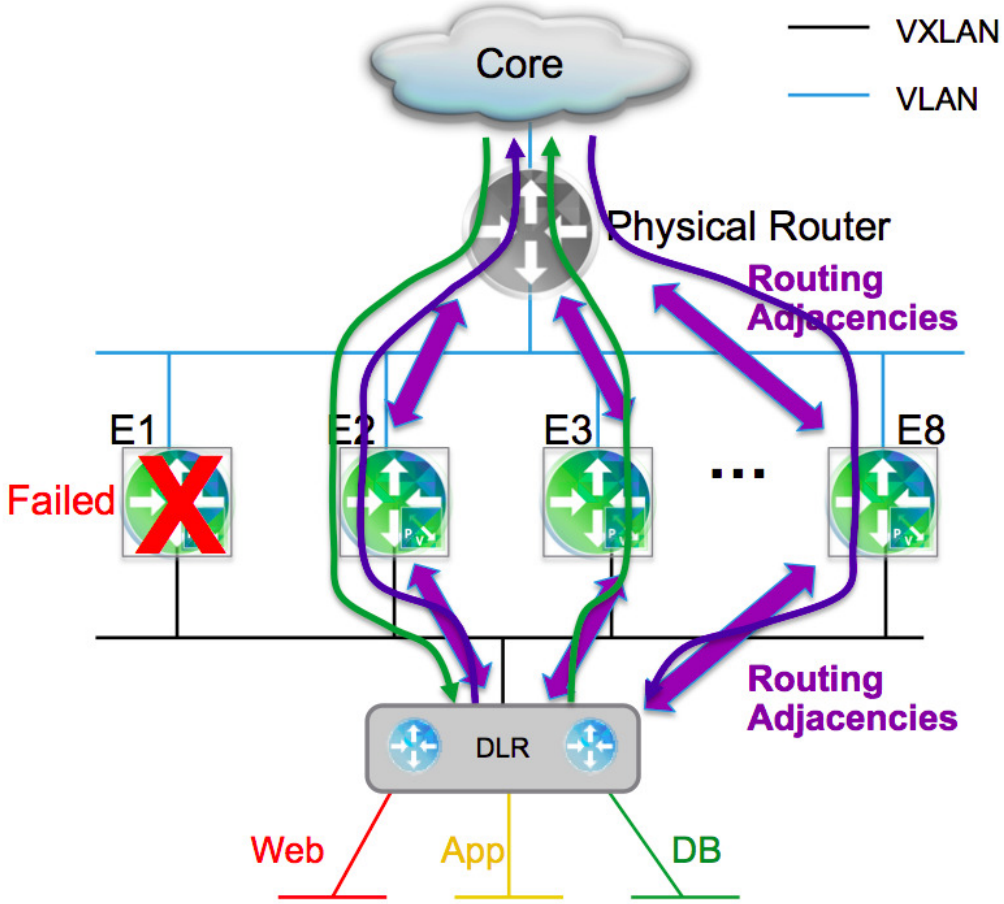


- Scale out NSX Edge HA

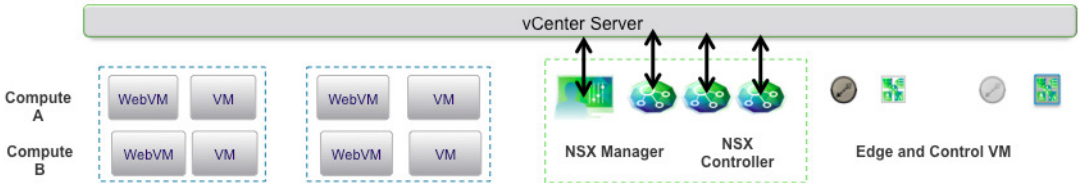


NSX 6.1 introduces support for Active/Active HA using ECMP
This HA model provides two main advantages:

- 1. An increased available bandwidth for north-south communication (up to 80 Gbps per tenant).
- 2. A reduced traffic outage (in terms of % of affected flows) for NSX Edge failure scenarios.



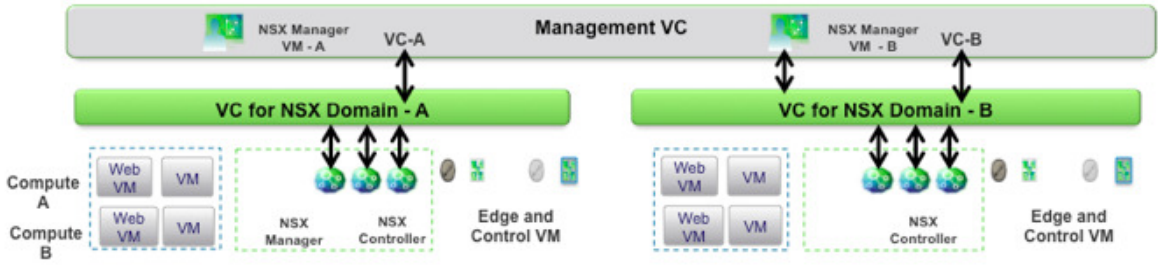
- Differentiate Collapsed/Separate vSphere Cluster topologies
  - Collapsed vSphere Cluster topology



- In small/medium data center deployments a single vCenter is usually deployed for managing all the NSX components. The recommendation is still to dedicate separate clusters and set of racks for compute resources. It is also recommended to deploy separate edge and management clusters to accommodate future growth.

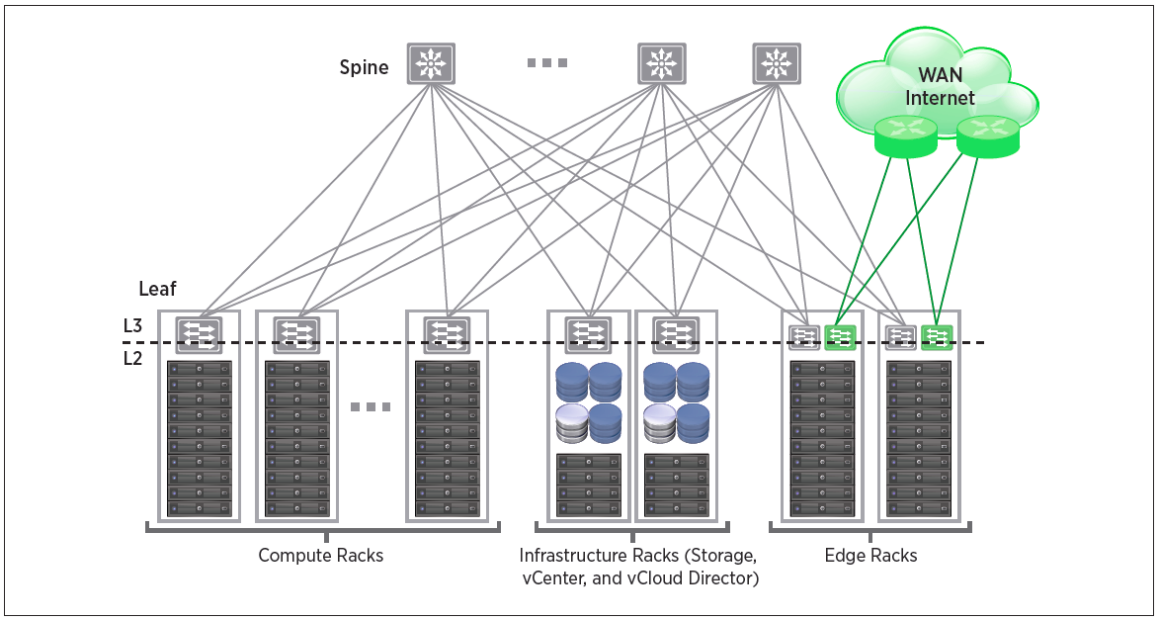
- The edge and management racks are usually consolidated and the corresponding clusters of ESXi hosts share Top-of-Rack connectivity,

- Separate vSphere Cluster topology
  Most enterprise deployments make use of a dedicated vCenter for the management cluster. This vCenter is usually already deployed even before the NSX platform is introduced in the architecture. When that happens, one or more dedicated vCenter servers part of the management cluster are usually introduced to manage the resources of the NSX domain (edge and compute clusters),

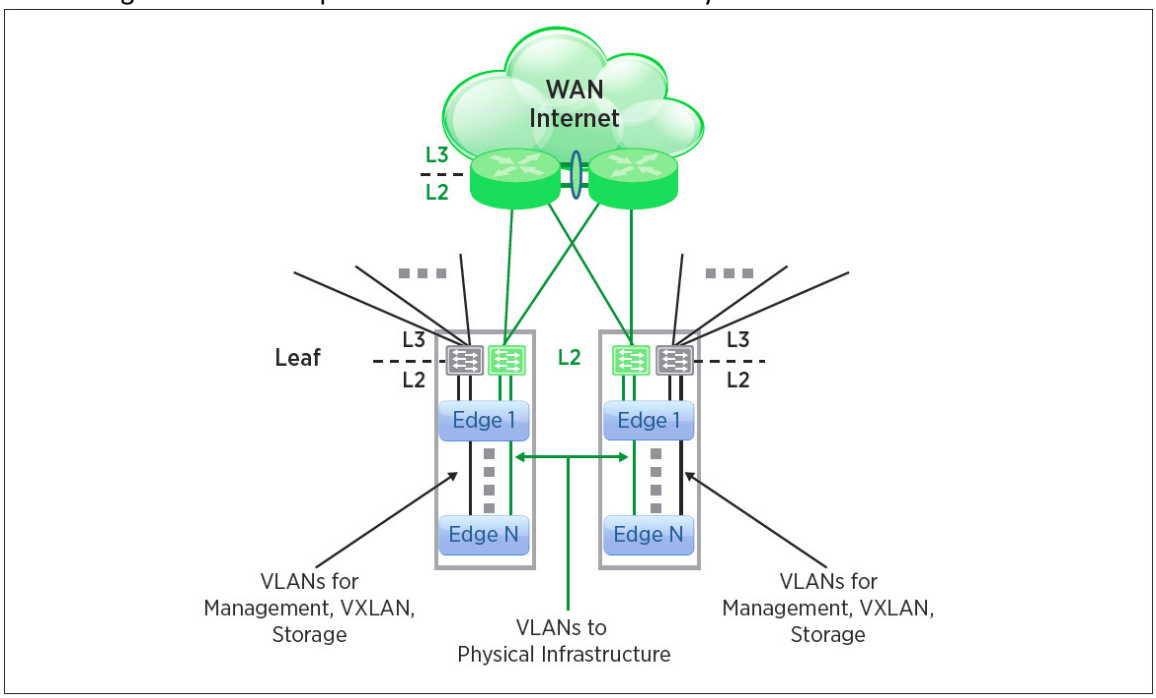


  There are several advantages in adopting such approach:
  - Avoids circular dependencies – the management cluster should always be outside of the domain it manages.
  - Mobility of management cluster for remote DC operation.
  - Integration with existing vCenter.
  - Ability to deploy more than one NSX-domain.
  - Upgrade of main vCenter does not affect the NSX domains.
  - SRM and other explicit state management are possible.
  - Additionally, a large-scale design employs one or more dedicated racks (infrastructure racks) and ToR switches to host the management cluster.

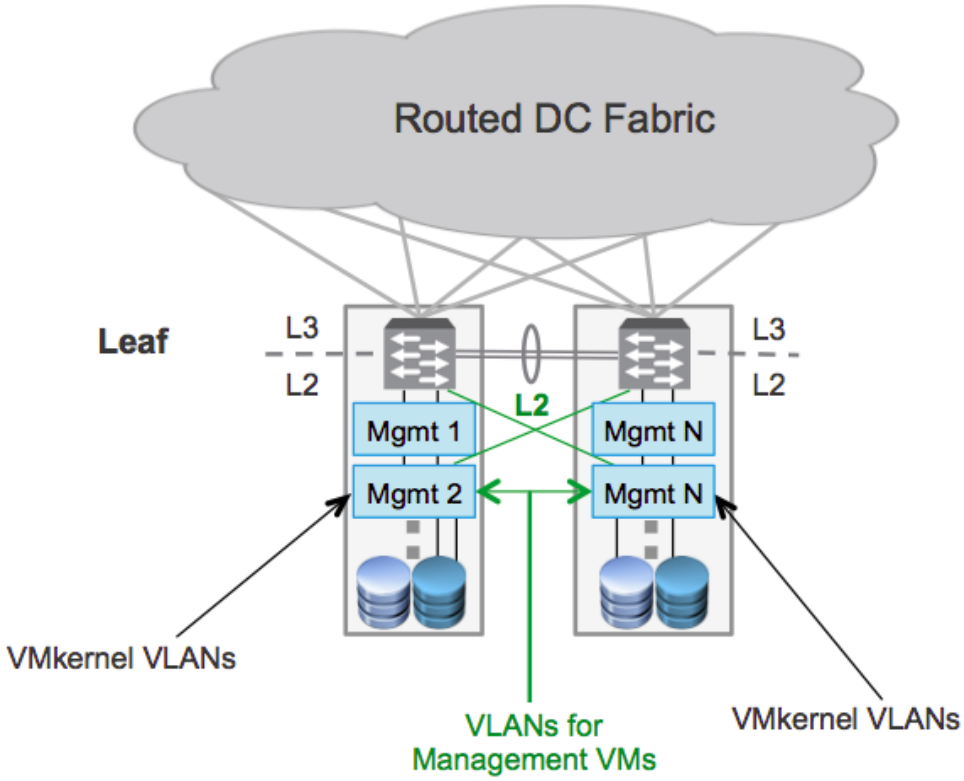
- Differentiate Layer 3 and Converged cluster infrastructures
  - Layer 3 in Access Layer
    This architecture is designed to allow for future growth, working for deployments that begin small but can grow to large-scale while keeping the same overall architecture.
    The guiding principle is that VLANs do not span beyond a single rack. This has a significant impact on how a physical switching infrastructure can be built and how well it scales.



Edge Racks using HA need a VLAN to be extended between the edge racks. Tunnel interfaces connecting the VXLAN endpoints do not need to extend any VLAN.



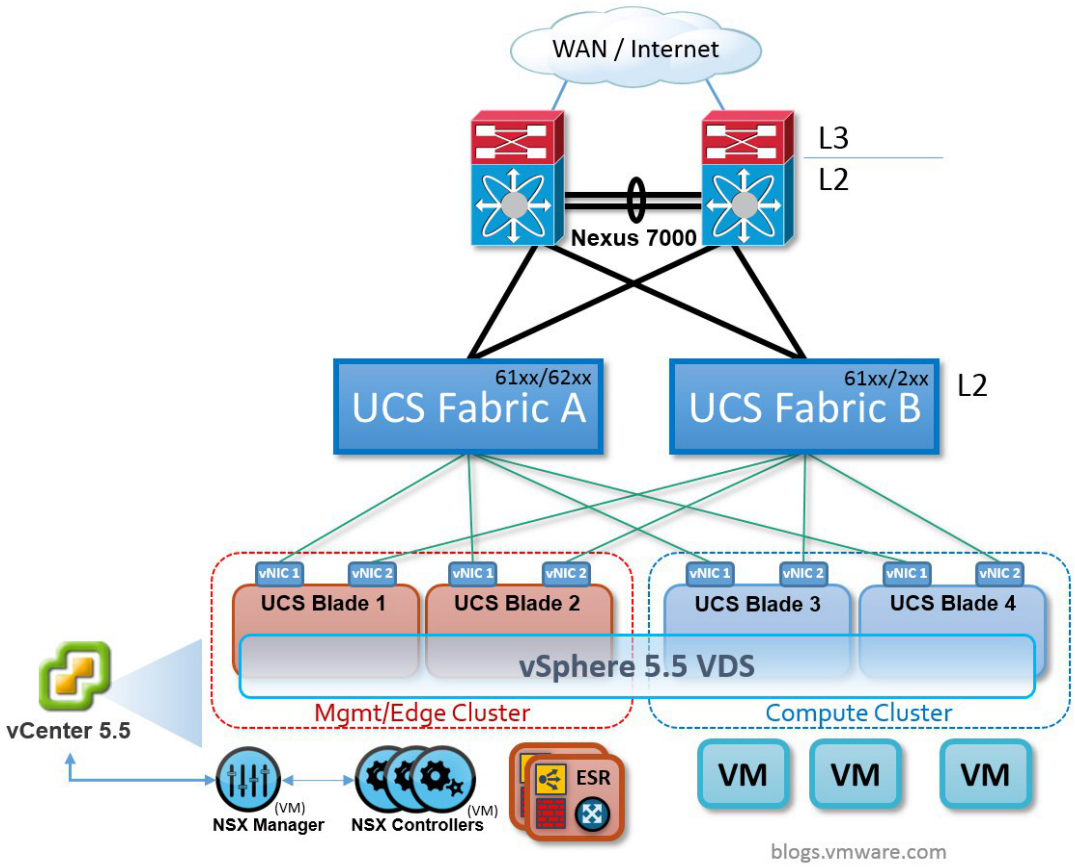
If the Management cluster is deployed across 2 racks (to survive a rack failure scenario) they require extending VLANs across those racks for management workloads such as VCenter, NSX Controllers, NSX Manager, and IP Storage. The recommended way to provide this is using dedicated cross-rack L2 cables to interconnect the ToR switches and dual home every server to both ToR switches



- Converged cluster

  With a converged cluster, the Management and Edge are provided in the same vSphere

cluster, with a shared L2 layer. This limits the scalability.



Tools

- VMware NSX Network Virtualization Design Guide
- NSX User's Guide

Objective 2.2 – Describe Physical Infrastructure Requirements for a VMware NSX Implementation

Knowledge

- Identify management and edge cluster requirements
    - Minimum 2 hosts per cluster
    - Minimum 1 vCenter, Optimally one dedicated vCenter for management cluster + one for each NSX domain
    - Management and edge clusters can be combined but this limits future expansion
    - Management and edge clusters need to share Top of Rack connectivity (L2 shared for Mgmt, L2 shared for Edge to External)
    - Recommended to deploy dedicated compute clusters rather than combining with Mgmt/Edge

- Describe minimum/optimal physical infrastructure requirements for a VMware NSX implementation
    - Servers
        - 2+ hosts per Cluster
        - 3+ hosts for Management Cluster
    - Clusters
        - Minimum : 1 Compute cluster + 1 Edge/Management cluster
        - Optimal : 1+ Compute cluster, 1 Management cluster, 1 Edge cluster
    - Network
        - Minimum
            - 1Gb fabric
            - Minimum 4 NIC per host unless 10GigE
            - Edge racks are normally the only racks connected to the external physical network
            - Management racks need to share L2 connectivity
        - Optimal
            - 10Gb fabric (VMware ran performance tests on 10Gb X540 Intel NICs)
            - Leaf-Spine fabric
            - Separate Edge routers connected to Edge racks.

- Describe how traffic types are handled in a physical infrastructure

  The following 4 traffic types should be in segregated VLANs

    - VXLAN Traffic
      A VTEP IP address is associated to a VMkernel interface on the host. This is used to transporting VXLAN frames across the fabric. VXLAN tunnels are initiated and terminated by VTEP interfaces. This encapsulation ensures the external fabric never sees the VM IP or MAC. Because VXLAN provisioning is done at the cluster level, there is a challenge in assigning the IP address.
        - If “Use IP Pool” is used, then only a single IP address range can be applied to a cluster, of which the hosts may be in different VLANs. Then manual configuration

would be required to change the VTEP IP addresses on a per host basis at command line.
    - If "Use DHCP" option is used, the VTEP will receive a valid IP for the VLAN it is in, depending on the specific rack it is connected to. This is the recommended approach for production deployments.

  - Management Traffic
    Management traffic is sourced and terminated by the management VMkernel interface on the host and includes the communication between vCenter Server and hosts as well as communication with other management tools such as NSX Manager.
    A single VDS can span multiple hypervisors that are deployed beyond a single leaf switch. Because no VLANs can be extended beyond a leaf switch, the management interfaces of hypervisors participating in a common VDS and connected to separate leaf switches are in separate IP subnets.

  - vSphere vMotion Traffic
    From a VMware support point of view, the historical recommendation has always been to deploy all the VMkernel interfaces used for vMotion as part of a common IP subnet. This is clearly not possible when designing the network for network virtualization using L3 in the access layer, where it is mandated to select different subnets in different racks for those VMkernel interfaces. Until this design is fully and officially supported by VMware, it is recommended that users go through the RPQ process so VMware can validate the design on a case-by-case basis.

  - Storage Traffic
    A VMkernel interface is used to provide features such as shared or non-directly attached storage. Typically, we refer to storage that can be attached via an IP connection—NAS or iSCSI, for example—rather than FC or FCoE. From an IP addressing standpoint, the same rules that apply to management traffic apply to storage VMkernel interfaces. The storage VMkernel interface of servers inside a rack—that is, connected to a leaf switch is part of the same IP subnet.
    This subnet, however, cannot span beyond this leaf switch. Therefore, the storage VMkernel interface IP of a host in a different rack is in a different subnet.

- Determine use cases for available virtual architectures
  - Enterprise
    An enterprise wishes to host multiple applications and provide connectivity among the different tiers of the application as well as connectivity to the external network.

  - Multiple Tenant
    A service provider environment has multiple tenants and each tenant can have different requirements in terms of number of isolated logical networks and other network services such as LB, Firewall, and VPN etc. A single NSX Edge is limited to 9 tenants and these tenants cannot have overlapping IP addressing.

  - Multi-Tenant Scalable
    A large service provider can have an additional layer of aggregation (a route aggregation Edge) which allows multiple groups of up to 9 tenants. It also permits overlapping IP addressing between groups of tenants.

- Describe ESXi host vmnic requirements
    - Minimum 2x physical NIC if 10GigE
    - Minimum 4x physical NIC if 1GigE
    - Different traffic types should be on different VLANs

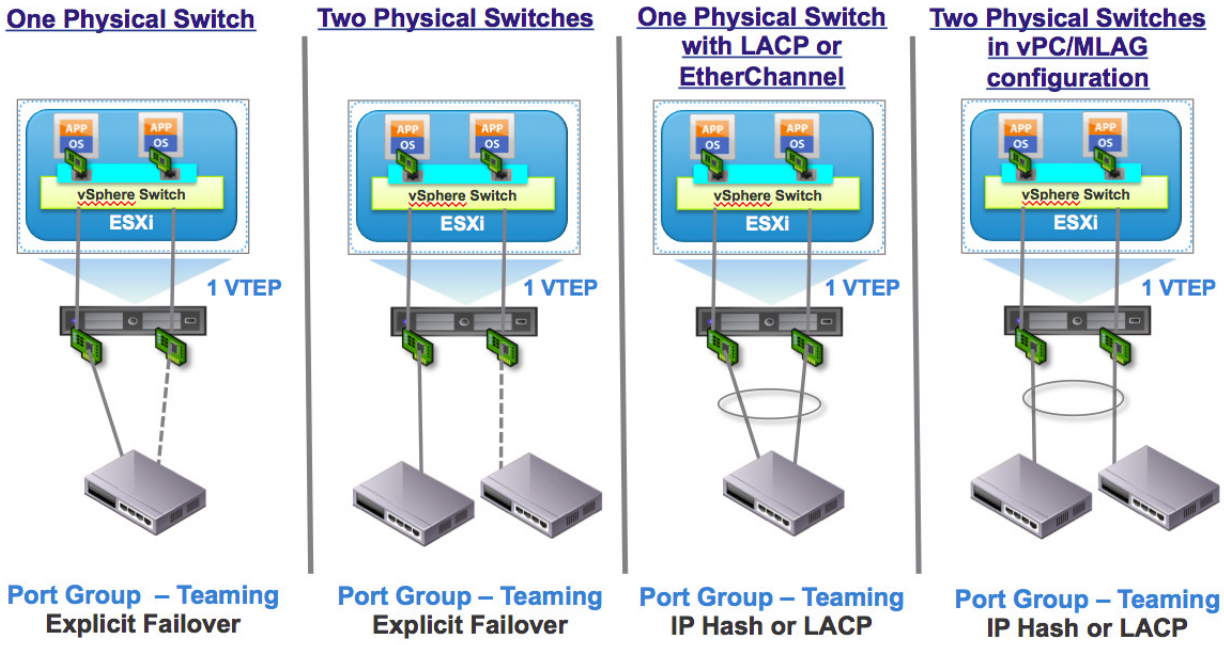
- Differentiate virtual to physical switch connection methods

  The design criteria used for connecting hosts are as follows:
    - The type of traffic carried – VXLAN, vMotion, Management, Storage. Specific focus in this case is on VXLAN traffic as it is the specific additional traffic type found in NSX-v deployments.
    - Type of isolation required based on traffic SLA – dedicated uplinks (for example for vMotion/Management) vs. shared uplinks.
    - Type of cluster – compute workloads, edge and management with or without storage etc.
    - Amount of bandwidth required for VXLAN traffic that may determine the decision of deploying a single or multiple VTEPs.

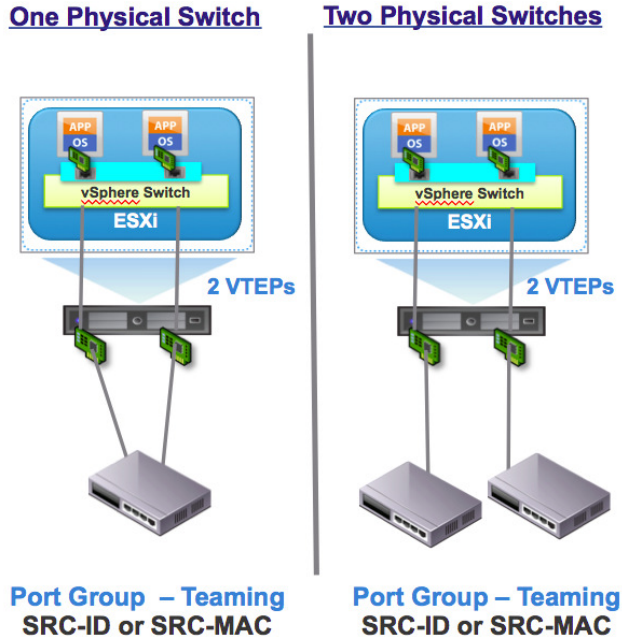
      The options for teaming on the portgroup used for VXLAN are as follows. The option must be specified when deploying the VXLAN.

Teaming and Failover Mode	NSX Support	Multi-VTEP Support	Uplink Behavior 2x10G
Route based on Originating Port	✓	✓	Both Active
Route based on Source MAC hash	✓	✓	Both Active
LACP	✓	×	Flow Based - Both Active
Route based on IP Hash (Static EtherChannel)	✓	×	Flow Based - Both Active
Explicit Failover Order	✓	×	Only One Active
Route based on Physical NIC Load (LBT)	×	×	×

    - Using a single VTEP



- Multiple VTEPs



- The selection criteria for type of uplink configuration to deploy can be based on the following considerations:
  - Simplicity of configuration – single VTEP vs. Physical switch configurations.
  - BW Required for each type of traffic.
  - Convergence requirement.
  - Cluster specifics – compute, edge and management.
  - The uplink utilization factors – flow based vs. MAC based.

  The recommended teaming mode for VXLAN traffic for ESXi hosts in Compute Clusters is LACP. It provides sufficient utilization of both links and reduced failover time. It also offers simplicity of VTEP configuration and troubleshooting at the expense of extra configuration and co-ordination with the physical switch. Obviously, ToR diversity for ESXi attachment can

only be achieved assuming the deployed physical switches support a type of multi-chassis etherchannel capability, like vPC (Cisco) or MLAG (Arista, Juniper, etc.).

For ESXi hosts part of the edge clusters is instead recommended avoiding the LACP or Static EtherChannel options. Because the NSX Edge must establish routing adjacencies with the next hop L3 devices – generally the ToR switches – an LACP/EtherChannel connection would complicate this and/or be unsupported. Therefore the recommendation for Edge Clusters is to select Explicit Failover Order or SRC-ID/SRC-MAC Hash as the teaming order for VXLAN traffic

- Describe VMkernel networking recommendations
  - 3 VIBs installed on each host – VXLAN, Distributed Firewall, Logical Router. These are vmkernel modules.
  - Separate vmkernel NIC interfaces should be configured for the following services:
    - Management
    - VMotion
    - IP Storage (if used)
    - VTEP
  - If Source Port or Source MAC teaming are used, NSX creates multiple VTEP to load balance
  - If LACP, Failover, or Etherchannel are used, NSX creates 1 VTEP by default
  - DHCP should be used for VTEP IP configuration to avoid manual configuration of each VTEP address.

Tools

- VMware NSX Network Virtualization Design Guide
- NSX User's Guide

Section 3 – Configure and Manage vSphere Networking

Objective 3.1 – Configure and Manage vSphere Standard Switches (vSS)

Knowledge

- Identify vSS capabilities

    - Routes traffic internally between virtual machines and links to external networks
    - Allows for multiple port groups configured with different policies
        - Allows for VLANs
        - Create network labels for virtual machine virtual adapters to attach to (is unique within the current datacenter)
    - Balance communication across multiple network adapters for load and/or resilience
    - Configurable to handle physical NIC failure by failing over to another physical NIC
    - Maximum of 256 port groups
    - Supports EtherChannel but not LACP
    - Source Port and Source MAC Load Balancing but not LBT

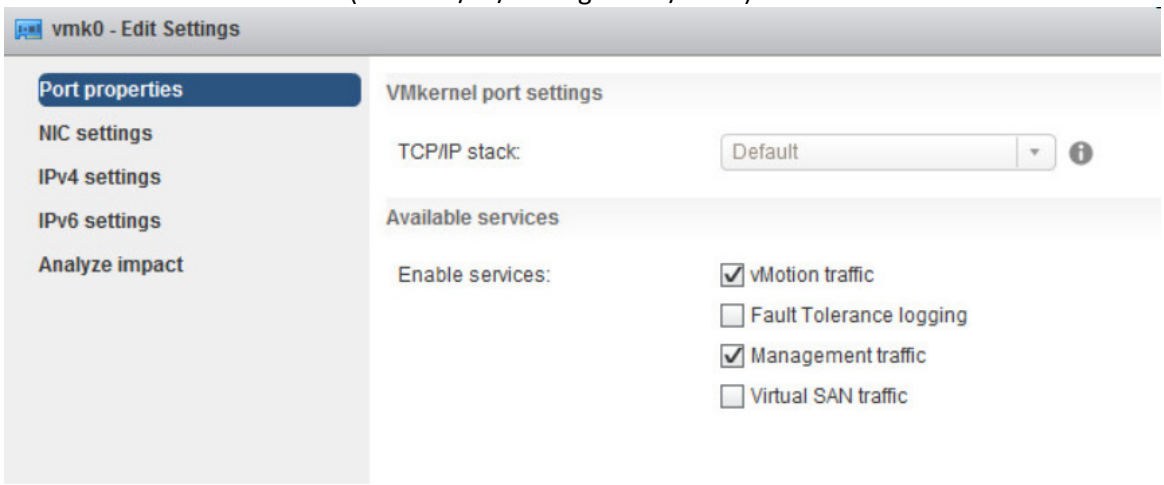
    - vSS-dSS comparison

Feature	vSS	vDS
Centralised Management & Control Plane (vCenter)	No	Yes
Security – Promiscuous Mode, Forged Transmits, MAC Address Changes	Yes	Yes
Analyse Impact	Yes	Yes
Health Check	No	Yes
Backup/Restore vSwitch Config	No	Yes
Egress Traffic Shaping	Yes	Yes
Ingress Traffic Shaping	No	Yes
Network I/O Control	No	Yes
Teaming & Failover – Originating Virtual Port, IP Hash, Source MAC Hash, Explicit Failover Order	Yes	Yes
Teaming & Failover – LBT (Physical NIC Load)	No	Yes
NetFlow & Port Mirroring	No	Yes
Portgroup – VLAN & Trunking (to VM)	Yes	Yes
Portgroup - Private VLANs	No	Yes
VXLAN & LACP (LAG), SRIOV	No	Yes

- Configuration Maximums

Feature	vSphere 5.1	vSphere 5.5
Virtual N/W SW Ports per Hosts	4096	4096
Maximum Active Ports per Host	1050	1016
vDS Ports per vCenter	60,000	60,000
Static Portgroups per vCenter	10,000	10,000
Hosts per vDS	500	1,000
Concurrent vMotions per Host (1Gb)/(10Gb)	4 / 8	4 / 8
LACP per vDS	1	64
Uplink Ports per LACP	4	32
Uplink Ports per Team	32	32
SRIOV Virtual Functions per Host	64 (Emulex) / 43 (Intel)	64
SRIOV 10Gb pNICs	4	8

- Add/Configure/Remove vmnics on a vSS
  Use C# client, Web client, esxcli, PowerCLI
  - Add via Web Client:
    - Hosts and Cluster view
    - Select host
    - Manage > Networking > Virtual Switches
    - Click on “Manage the physical network adapters connected to the selected switch”
      
    - Click the “+” and select the vmnic to add
- Configure vmkernel ports for network services
  - Easiest to select in GUI (Web client or C#)
  - Tickboxes to enable services (vMotion/FT/Management/vSAN)



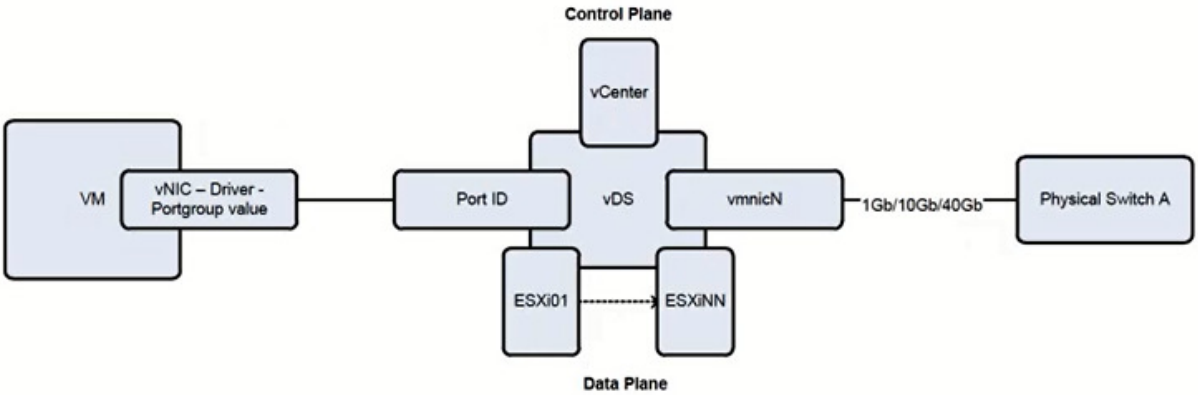
- Add/Edit/Remove port groups on a vSS
  Use C# client, Web client, esxcli, PowerCLI
  - Add viaWeb Client
    - Go to Hosts and Cluster view
    - Select host
    - Manage > Networking > Virtual Switches

        - Click on "Add host networking" 
        - Select "Virtual Machine Port Group for a Standard Switch", Next
        - Select "Select an existing standard switch", Next
        - Input the Network Label (name of the Port Group) and VLAN ID
        - Next, and Finish
- Determine use cases for a vSphere Standard Switch
    - No Ent+ license
    - Management cluster

Tools
- vSphere Installation and Setup Guide
- vSphere Networking Guide
- vSphere Web Client
- vSphere Client

Objective 3.2 – Configure and Manage vSphere Distributed Switches (vDS)

Knowledge
- Identify vDS capabilities
  All vSS capabilities plus:
    - Maintains a single configuration across all hosts
    - Ensures VMs see consistent network provision regardless of the host they are on
    - Allows the use of NetFlow, Port Mirroring and Private VLANs
    - Performs traffic shaping ingress as well as egress
    - Allows use of LACP for teaming
    - Allows use of Load Based Teaming
    - … see comparison table in 3.1 for more.



- Create/Delete a vDS
    - C# client, Web client, PowerCLI
    - Create with Web Client:
        - Go to vCenter Home and Networking
        - Right click on the Datacenter object and select "New Distributed Switch"
        - Name the vDS and click Next
        - Select the version (4.0-5.5), Next
        - Choose the number of Uplinks, whether NIOC is enabled and whether a default port group is created, according to what you wish to create.

        - Click Next, and Finish

- Add/Remove ESXi hosts from a vDS
    - Easiest through GUI, same for following items
    - Add hosts with Web Client:
        - Go to vCenter Home and Networking
        - Expand the Datacenter object
        - Right click on the vDS object and select “Add and Manage Hosts”
        - Leave the radio button on “Add hosts”, Next
        - Click “New hosts…” and select the hosts to add, OK, and Next
        - You can now select to manage the host nics, the vmknics, migrate VM networking and change advanced settings. Leave the defaults and click Next
        - For each host nic you want to use, click on it, then click on “Assign Uplink” to assign it to a vDS uplink, Next
        - Choose to create new vmknics or assign existing ones to port groups on the new vDS, Next
        - Check the impact on existing network services on the next screen, Next
        - Click Finish to apply the changes

- Edit general vSphere vDS settings
    - Advanced settings includes MTU
    - Edit settings with Web Client:
        - Go to vCenter Home and Networking
        - Expand the Datacenter object
        - Right click on the vDS object and select “Edit Settings”
        - Amend Uplinks/Network IO control in the General tab, or MTU, Discovery protocol and admin contact in the Advanced tab
        - Click OK to apply the changes

- Add/Configure/Remove dvPortgroups
    - New Distributed Port Group with Web Client:
        - Go to vCenter Home and Networking
        - Expand the Datacenter object
        - Right click on the vDS object and select “New Distributed Port Group”
        - Name the port group and click Next
        - Enter the configuration details for this port group (binding type, no of ports, VLAN etc) and if necessary select the “Advanced” checkbox to customize the default policies)
        - Click Next, and FInish

- Configure dvPort settings
    - Configure dvPort settings with Web Client
        - Go to vCenter Home and Networking
        - Expand the Datacenter object
        - Select vDS object and click on the Ports tab
        - Select the Port in the list and click the pencil icon to edit.
        - Edit the settings in the dialog box, and click OK to save

- Add/Remove uplink adapters to dvUplinkgroups
    - Add uplink adapters with Web Client

        - Go to vCenter Home and Networking
        - Expand the Datacenter object
        - Right click on the vDS object and select “Add and Manage Hosts”
        - Select “Manage host networking”, Next
        - Click “Attached Hosts”
        - Select the hosts to manage, OK, Next
        - Select only “Manage physical adapters”, Next
        - Click on the vmnic to assign, and then select “Assign uplink”
        - Choose the Uplink, OK, Next
        - Check the impact on existing network services on the next screen, Next
        - Click Finish to apply the changes

- Create/Configure/Remove virtual adapters
    - Create virtual adapters with Web Client
        - Go to vCenter Home and Networking
        - Expand the Datacenter object
        - Right click on the vDS object and select “Add and Manage Hosts”
        - Select “Manage host networking”, Next
        - Click “Attached Hosts”
        - Select the hosts to manage, OK, Next
        - Select only “Manage VMkernel adapters”, Next
        - Click “New adapter”
        - Choose the port group, Next
        - Choose the port properties and services, Next
        - Set the IP address (or leave as DHCP), Next
        - Click Finish

- Migrate virtual adapters to/from a vSS
    - Migrate virtual adapters with Web Client
        - Go to vCenter Home and Networking
        - Expand the Datacenter object
        - Right click on the vDS object and select “Add and Manage Hosts”
        - Select “Manage host networking”, Next
        - Click “Attached Hosts”
        - Select the hosts to manage, OK, Next
        - Select only “Manage VMkernel adapters”, Next
        - Select the vmknic to migrate
        - Click “Assign port group” and choose the new Distributed Port Group to assign to
        - Click Ok, and Next
        - Check the impact on existing network services on the next screen, Next
        - Click Finish to apply the changes

- Migrate virtual machines to/from a vDS
    - Migrate virtual machines with Web Client
        - Go to vCenter Home and Networking
        - Right click on the Datacenter object and select “Migrate VM to Another Network”
        - Choose the source network in the “Specific network” box
        - Choose the destination network, Next
        - Choose the VMs to migrate, Next
        - Click Finish

- Monitor dvPort state
  - Monitor dvPort state with Web Client
    - Go to vCenter Home and Networking
    - Expand the Datacenter object
    - Click on the vDS object
    - Manage > Ports
    - Find the port ID in the list
    - Select the port ID and the status will show below

- Determine use cases for a vDS
  - Must have Enterprise Plus licensing
  - Simpler to manage large numbers of hosts with a vDS rather than making sure their vSS and Port Groups are in sync.
  - If you need to use NetFlow, Port Mirroring or Private VLANs
  - If you want to use "Load Based Teaming"
  - If you want to use Network IO Control or Network Resource Pools

Tools
- vSphere Installation and Setup Guide
- vSphere Networking Guide
- vSphere Web Client
- vSphere Client

Objective 3.3 – Configure and Manage vSS and vDS Policies

Knowledge
- Identify common vSS and vDS policies
  - Common Security Policies
    - Promiscuous Mode (default is reject) – When enabled, allows a VM to see all traffic passing through the vSwitch
    - MAC address changes (default is accept) – Determine whether a VM is permitted to receive traffic on a changed MAC address. May be required for NLB or Windows Clustering.
    - Forged Transmits (default is accept) – Determine whether a VM is permitted to transmit traffic on a changed MAC address.

- Configure dvPortgroup blocking policies
  - Block single port with Web Client
    - Go to vCenter Home and Networking
    - Expand the Datacenter object
    - Click on the vDS object
    - Manage > Ports
    - Find the port ID in the list
    - Select the port ID click the pencil icon to edit
    - Go to the Miscellaneous section and select "Block port", and change the Override to "yes"
    - Click OK to apply the setting

    - Block all ports on a Distributed Port Group with Web Client
        - Go to vCenter Home and Networking
        - Expand the Datacenter object
        - Right click on the vDS object and select “Edit settings”
        - Go to the Miscellaneous section and change “Block all ports” to “yes”
        - Click OK to apply the setting

- Configure load balancing and failover policies
    - vSS – Default policies are set on the vswitch, these can be overridden on the port group.
    - vDS – Policies are set on each Distributed Port Group
    - Load Balancing
        - Route basd on IP hash – requires Etherchannel (or LACP on vDS) on the physical switch
        - Route based on source MAC hash – similar to above, but doesn’t need channel bonding
        - Router basd on originating virtual port – traffic exits through the same port it came in on
        - Use explicit failover order – no load balancing, just failover
        - Route based on physical NIC load (vDS only) – distributes the load based on traffic volume
    - Network Failover Detection
        - Link Status Only – This uses the link state of the physical NIC. If the switch fails or the cable gets unplugged, the failure will be detected and failover will be initiated. This cannot detect if the switch becomes isolated, or misconfigured.
        - Beacon Probing – This sends and listens for beacon probes on all NICs that are part of the team. This is used to determine whether a NIC has connectivity, and can detect more failures than LSO. **Do not use in conjunction with IP hash Load Balancing**
        - Notify Switches – If set to “yes” then physical switches will be notified to update MAC/ARP tables in the event of a failover. **Do not use when using Microsoft NLB in unicast mode.**
        - Failback Policy – If set to “yes” then return to the original configuration after a NIC failure has been resolved, if set to “no” continue in failover mode.
- Configure VLAN settings
    - vSS
        - Configured on the port group, under Edit Settings and Properties, configure the chosen VLAN ID or set to 0 to use the base VLAN on the physical switch port.
    - vDS
        - Configured on the distributed port group, under Manage, Settings, Edit, VLAN
            - None – no VLAN tagging
            - VLAN – Enter the VLAN ID to be used
            - VLAN Trunking – Enter the range of VLANs to be trunked
            - Private VLAN – Enter the private VLAN to be used (must be configured on the vDS first)

- Configure traffic shaping policies
    - vSS
        - Configured on the vSwitch or port group, under Edit Settings and Properties
        - Applies only to egress traffic
    - vDS

        - Configured on the distributed port group, under Manage, Settings, Edit, Traffic Shaping
        - Applies to ingress and/or egress traffic
    - Policies:
        - Average Bandwidth – determines the Kbits/sec allowed to traverse each port, averaged over time.
        - Peak Bandwidth – the maximum rate the bandwidth can burst to
        - Burst Size – the amount of data allowed to burst up to the Peak Bandwidth rate
    - Network IO Control – under "Resource Allocation" tab, only applies to egress traffic. Create a new policy group and apply to a port group

- Enable TCP Segmentation Offload (TOE) support for a virtual machine
    - TOE is enabled when using the VMXNet3 network adapter

- Enable Jumbo Frame support on appropriate components
    - Enable on the vSwitch (vSS or vDS), enable on vmknics, enable on VMs by installing the VMXNet3 adapter and enabling within the Guest OS.
    - Normally only enable for iSCSI and/or vMotion

- Determine appropriate VLAN configuration for a vSphere implementation
    - There is no single appropriate configuration to put here. Understand the following:
        - External Switch Tagging – all tagging occurs at the physical switch
        - Virtual Switch Tagging – all tagging occurs at the virtual switch. The physical switch ports must be configured as trunk ports. Port groups must have the VLAN ID specified.
        - Virtual Machine Tagging – tagging is done by the VM. The Guest OS must be able to handle 802.1Q traffic. The physical switch ports must be configured as trunk ports.
        - Private VLANs – Understand PVLANs and where/why to use them.

Tools

- vSphere Installation and Setup Guide
- vSphere Networking Guide
- vSphere Web Client
- vSphere Client

Section 4 – Install and Upgrade VMware NSX

Objective 4.1 – Configure Environment for Network Virtualization

Knowledge

- Configure the physical infrastructure (MTU, Dynamic Routing for edge, etc.)
    - MTU needs to be 1600 for transport zone
      Can use 1550 if you aren't going to have VLAN tagging in the VM Guest OS
      Has been suggested that 1600 is the minimum recommended in 6.0, and 1550 is the minimum recommended in 6.1
    - Configure OSPF adjacency for routing on Edge (or BGP, ISIS equivalent)

- Prepare a new vSphere infrastructure
    - Configure Quality of Service (QoS)
        - L2/L3 fabric must be configured to trust the hypervisor for QoS marking – hypervisor is the trusted boundary.
    - Configure Link Aggregation Control Protocol (LACP)
        - Can use LACP or Etherchannel for the Transport network, but only a single VTEP is supported with bonded channels.

- Configure an existing vSphere infrastructure
    - Ensure DNS entries are configured correctly for all components
    - Requires vSphere 5.5 and vCenter 5.5
    - Upgrade VMware Tools – minimum 8.6, vHW 7+
    - Must use Enterprise+ license

- Explain how IP address assignments work in VMware NSX
    - Can use IP Pools or DHCP to assign addresses for NSX components. DHCP allows configuration of VTEP on different VLANs, whereas IP Pools require the same VLAN or manual configuration to change after install.

- Identify minimum permissions required to deploy NSX in a vSphere environment
    - Administrative access to vCenter – required to synchronise the NSX Manager with vCenter

Tools

- vSphere Networking Guide
- NSX Administration Guide
- vSphere Web Client

Objective 4.2 – Deploy VMware NSX Components

Knowledge

- Install NSX Manager
    - Deploy OVF Template
    - Select source (URL or Browse to local file)
    - Review details (shows product, version, size, description etc)
    - Accept EULA
    - Specify a name (NSX Manager) and location (folder or datacenter)

  - Select the storage (datastore)
  - Setup networks (which port group the VM will be on)
  - Customize template (enter passwords, network properties)
  - Ready to complete (review config and click Finish)

- Register NSX Manager with vCenter Server
  - Connect to NSX Manager Web Frontend
  - Manage vCenter Registration
  - Click on Edit
  - Enter DNS name, username, password
  - Yes to proceed with this registration
  - Yes to proceed with the SSL certificate
  - Shows status “Connected”

- Install NSX License
  - Open the Web Client
  - Navigate to Administration > Licensing
  - Click “+” under License Keys
  - Paste in the NSX license key and click Finish

- Prepare ESXi hosts
  - Log in to Web Client
  - Navigate to Networking & Security
  - Installation/Host Preparation
  - Select the Cluster and click “Install”
  - This installs VIBs to hosts

- Deploy NSX Controllers
  - Must be odd number of Controllers – recommended 3
  - Use anti-affinity rules to keep separate (create manually)
  - Web Client, Networking & Security
  - Installation
  - Click “+” by NSX Controller nodes
  - Enter Datacenter, Cluster/RP, Datastore, Host, Connected To, IP Pool, Password
  - VM is then deployed and built

- Assign Segment ID pool and Multicast addresses
  - Log in to Web Client
  - Navigate to Networking & Security
  - Installation/Logical Network Preparation
  - Click “Segment ID”
  - Click “Edit”
  - Enter the Segment ID pool range
  - If Multicast addressing is to be used, click the “Enable multicast addressing” checkbox, and enter the multicast addresses range.
  - Click OK.

- Configure VXLAN Transport
  - VXLAN Replication Modes:

        - Unicast – Ease of entry. More work for hypervisor, but requires fewer network changes.
        - Hybrid – Requires IGMP Snooping on the switch. Uses multicast locally, but unicast across WAN.
        - Multicast – Offload more work to network infrastructure

    - Log in to Web Client
    - Navigate to Networking & Security
    - Installation/Host Preparation
    - Select the Cluster and click on "Configure" under the VXLAN column
    - Select the Switch, VLAN, MTU, choice of DHCP/IP Pool, Teaming policy, VTEP ID
        - If using IP Pool, all hosts need to be on shared L2, or manually reconfigured afterwards.
    - Click on "Transport Zones"
    - Click on "+" to start the New Transport Zone dialog
    - Enter Name, Description, Control Plane Mode (Multicast/Unicast/Hybrid), and choose the Clusters to Add.

- Install NSX Edge
    - A VM that provides services such as VPN, Stretch L2, Dynamic Routing etc
    - Log in to Web Client
    - Navigate to Networking & Security
    - Click on NSX Edges
    - Click on "+"
    - Select Edge Services Gateway
    - Select checkbox option to choose High Availability if required
    - Enter the Name, Hostname, Description, Tenant
    - Enter CLI credentials (enable SSH if required)
    - Configure the Datacenter, Appliance size
    - Configure interfaces (need Internal and Uplink)
    - Choose correct MTU (1500 for internal)

- Install vShield Endpoint
    - On NSX 6.1 vShield Endpoint has been replaced with the Data Security and Guest Introspection appliances

    - Log in to Web Client
    - Navigate to Networking & Security
    - Click on Installation and Service Deployments
    - Click "+" and the "Deploy Network & Security Services" dialog starts
    - Select "VMware Endpoint", Next
    - Select the Cluster to deploy the Endpoints to, Next
    - Select the Datastore on which to place the Endpoint, Next
    - Select the Management Network for the Endpoint, Next
    - The Endpoints are now deployed from OVFs
    - Monitor the Installation status and it will go from In Progress to Succeeded.

- Install Data Security
    - Log in to Web Client

  - Navigate to Networking & Security
  - Click on Data Security
  - Click on Edit for “Regulations and standards to detect”
  - Click on “All”
  - Select the regulations to monitor for, Next
  - Enter Data Patterns, if prompted to enter them for the chosen regulations
  - Click Finish
  - Click on Edit for “Files to scan”
  - Make changes to the Size/Modified Date/File Extension Type if necessary
  - Click Save
  - Click Publish Changes
  - Click Start

- Create an IP pool
  - Log in to Web Client
  - Navigate to Networking & Security
  - Click on NSX Managers
  - Click on the IP address of the NSX Manager
  - Navigate to “Manage” and “Grouping Objects”
  - Select IP Pools, and click on “+” to add a new IP pool
  - Enter the Name of the pool, Gateway, Prefix length, Primary DNS, Secondary DNS, DNS Suffix and Static IP Pool details.
  - Click OK.

Tools
- NSX Installation and Upgrade Guide
- NSX Manager
- vSphere Web Client

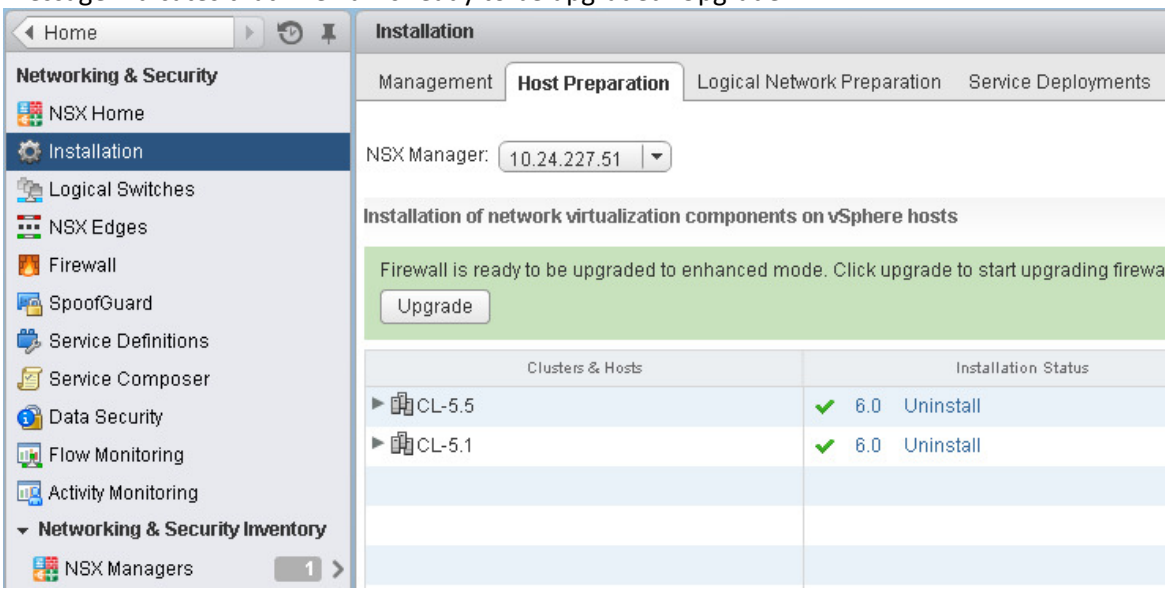
Objective 4.3 – Upgrade Existing vCNS/NSX Implementation

Knowledge
- Verify upgrade prerequisites have been met
  - Vcenter 5.5 required
  - Can only upgrade from vShield 5.5 to NSX Manager, not 6.0
- Upgrade vCNS 5.5 to NSX 6.x
  - Download the upgrade bundle
  - From within vShield Manager, Settings & Reports, Browse and upload the file
  - Click Install and the appliance will reboot
  - Login to NSX manager to confirm the upgrade

- Upgrade vCNS Virtual Wires to NSX Logical Switches
  - From vSphere Web Client, open Network & Security
  - Navigate to Host preparation area
  - Click “Update” – status will change from Legacy to Enabled
  - VIBS are pushed to nodes (using DRS and Maintenance Mode)
  - Install NSX Controllers and create Logical Network

- Upgrade to NSX Components

- Upgrade to NSX Firewall
- Prerequisites
  - vShield Manager has been upgraded to NSX Manager.
  - Virtual wires have been upgraded to NSX Logical Switches. For non-VXLAN users, network virtualization components have been installed.
- Procedure
  - After you update all the clusters in your infrastructure while upgrading to NSX logical switches (or installing network virtualization components), a pop up message indicates that Firewall is ready to be upgraded. Upgrade



  - Click Upgrade.
  - After the upgrade is complete, the Firewall column displays Enabled.
  - Inspect each upgraded section and rule to ensure it works as intended.
- What to do next
  - Once you upgrade firewall to NSX, you should move the grouping objects used by firewall rules to global scope. To do this, use NSX APIs to create new grouping objects with the same members and then update the relevant firewall rules with the new IDs.

- Upgrade to NSX Edge
  - From vSphere Web Client, open Network & Security
  - Navigate to NSX Edge
  - Select Upgrade from Actions
  - Check version number and deploy status

- Upgrade vShield Endpoint from 5.5 to 6.x
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click Installation.
  - Click the Service Deployments tab.
  - vShield Endpoint 5.5 deployments are displayed and the Installation Status column says Upgrade Available.
  - In the Installation Status column for vShield Endpoint, click the arrow next to Upgrade Available.

        - Select the Data store and Network and click OK.

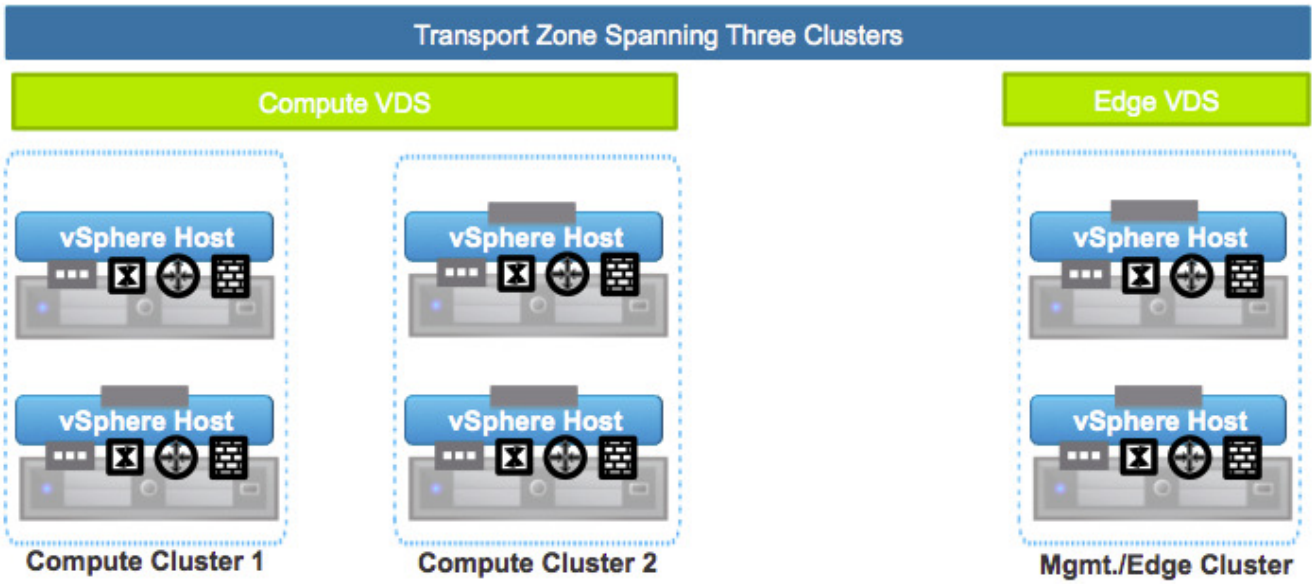
    - Upgrade to NSX Data Security
        - NSX Data Security does not support a direct upgrade. You must uninstall the current Data Security software before upgrading to NSX Manager. After NSX Manager is upgraded, you can install NSX Data Security version 6.0. If you upgraded to NSX Manager without uninstalling Data Security, you must do so using a REST call.
        - Pre-NSX Data Security policies and violation reports are carried over to the vSphere Web Client, but you can run a Data Security scan only after installing NSX Data Security version 6.0.
- Upgrade NSX Manager from 6.0 to 6.x
    - Download upgrade bundle from VMware
    - Open NSX Manager web front end, and navigate to Manage area
    - Click Upgrade
    - Wait for upgrade to finish, login and confirm version number

- Update vSphere Clusters after NSX upgrade
    - From vSphere Web Client, open Network & Security
    - Navigate to Host preparation, and click Update (remember to post host into Maint Mode)

Tools
- NSX Installation and Upgrade Guide
- vSphere Web Client

Objective 4.4 – Expand Transport Zone to Include New Cluster(s)

Knowledge
- Explain the function of a Transport Zone



    - A transport Zone defines a collection of ESXi hosts that can communicate with each other across a physical network.

- It extends across one or more ESXi clusters, and in a loose sense defintes the span of logical switches.

- Add a Transport Zone
  - Log in to the vSphere Web Client.
  - Navigate to “Networking & Security” and “Installation”.
  - Click “Logical Network Preparation” and then click “Transport Zones”.
  - Click the “New Transport Zone” icon.
  - In the New Transport Zone dialog box, type a name and description for the transport zone.
  - Depending on whether you have a controller node in your environment, or you want to use multicast addresses, select the control plane mode.
    - Multicast: Multicast IP addresses on physical network are used for the control plane. This mode is recommended only when you are upgrading from older VXLAN deployments. Requires PIM/IGMP on physical network.
    - Unicast : The control plane is handled by an NSX controller. All unicast traffic leverages headend replication. No multicast IP addresses or special network configuration is required.
    - Hybrid : The optimized unicast mode. Offloads local traffic replication to physical network (L2 multicast). This requires IGMP snooping on the first-hop switch, but does not require PIM. First-hop switch handles traffic replication for the subnet.
  - Select the clusters to be added to the transport zone.
  - Click OK.

- Expand/Contract a Transport Zone
  - Expand:
    - Log in to the vSphere Web Client.
    - Navigate to “Networking & Security” and “Installation”.
    - Click “Logical Network Preparation” and then click “Transport Zones”.
    - Click a transport zone.
    - In Transport Zones Details, click the Add Cluster icon.
    - Select the clusters you want to add to the transport zone.
    - Click OK.
  - Contract
    - Log in to the vSphere Web Client.
    - Navigate to “Networking & Security” and “Installation”.
    - Click “Logical Network Preparation” and then click “Transport Zones”.
    - Double-click a transport zone.
    - In Transport Zones Details, click the Remove Clusters icon.
    - Select the clusters you want to remove.
    - Click OK.

- Edit a Transport Zone
  - Log in to the vSphere Web Client.
  - Navigate to “Networking & Security” and “Installation”.
  - Click “Logical Network Preparation” and then click “Transport Zones”.
  - Double-click a transport zone.
    The Summary tab displays the name and description of the transport zone as well as the number of logical switches associated with it. Transport Zone Details displays the clusters in the transport zone.

  - Click the Edit Settings icon in the Transport Zone Details section to edit the name or description of the transport zone.
  - Click OK.

- Change the Control Plane mode for a Transport Zone
  - Log in to the vSphere Web Client.
  - Navigate to “Networking & Security” and “Installation”.
  - Click “Logical Network Preparation” and then click “Transport Zones”.
  - Double-click a transport zone.
    The Summary tab displays the name and description of the transport zone as well as the number of logical switches associated with it. Transport Zone Details displays the clusters in the transport zone.
  - Click the Edit Settings icon in the Transport Zone Details section to edit the control plane mode of the transport zone.
  - Select Migrate existing Logical Switches to the new control plane mode to change the control plane more for existing logical switches linked to this transport zone. If you do not select this check box, only the logical switches linked to this transport zone after the edit is done will have the new control plane mode.
  - Click OK.

Tools

- NSX Installation and Upgrade Guide
- NSX Administration Guide
- vSphere Web Client

Section 5 – Configure VMware NSX Virtual Networks

Objective 5.1 – Create and Administer Logical Switches

Knowledge

- Configure IP address assignments

  I'm not clear what is being asked for here, the only relevant section I can find is in the design guide, and is basically the following:

  - The IP address assignment depends on whether the virtual machine is connected to a logical switch through a NAT or a non-NAT configuration
    - NAT
      In the deployments where organizations have limited IP address space, NAT is used to provide address translation from private IP space to the limited public IP addresses. By utilizing Edge services router, users can provide individual tenants with the ability to create their own pool of private IP addresses, which ultimately get mapped to the publicly routable external IP address of the external Edge services router interface.

    - Non-NAT
      Organizations that are not limited by routable IP addresses, have virtual machines with public IP addresses or do not want to deploy NAT can use static and dynamic routing features available with the NSX platform. In the NSX platform two different modes of logical routing is supported. One is called distributed routing and the other one as centralized routing. The distributed routing provides better throughput and performance for the East West traffic while the centralized routing handles the North South traffic.

- Add/Remove a logical switch
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click Logical Switches.
  - Click the New Logical Switch icon.
  - Type a name and description for the logical switch.
  - Select the transport zone in which you want to create the virtualized network. The Scope Details panel displays the clusters that are part of the selected transport zone and the services available to be deployed on the scope.
  - By default, the logical switch inherits the control plane mode from the transport zone. You can change it to one of the other available modes:
    - Unicast: The control plane is handled by an NSX controller. All traffic replication is handled locally by the hypervisor. No multicast IP addresses or special network configuration is required.
    - Hybrid: The optimized unicast mode. Offloads local traffic replication to physical network. This requires IGMP snooping on the first-hop switch, but does not require PIM. First-hop switch handles traffic replication for the subnet.
    - Multicast: Multicast IP addresses on physical network are used for the control plane. This mode is recommended only when you are upgrading from older VXLAN deployments. Requires PIM/IGMP on physical network.

- Click OK.

- Modify control plane mode
  - Login to the vSphere Web Client
  - Click Networking & Security and then click Logical Switches.
  - Select the logical switch that you want to edit.
  - Click the Edit icon
  - By default, the logical switch inherits the control plane mode from the transport zone. You can change it to one of the other available modes:
    - Unicast: The control plane is handled by an NSX controller. All traffic replication is handled locally by the hypervisor. No multicast IP addresses or special network configuration is required.
    - Hybrid: The optimized unicast mode. Offloads local traffic replication to physical network. This requires IGMP snooping on the first-hop switch, but does not require PIM. First-hop switch handles traffic replication for the subnet.
    - Multicast: Multicast IP addresses on physical network are used for the control plane. This mode is recommended only when you are upgrading from older VXLAN deployments. Requires PIM/IGMP on physical network.
  - Click OK

- Connect a logical switch to an NSX Edge gateway
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click Logical Switches.
  - Select the logical switch that you want to connect an NSX Edge.
  - Click the Add Edge Gateway () icon.
  - Select the NSX Edge to which you want to connect the logical switch and click Next.
  - Select the interface that you want to connect to the logical switch and click Next.
  - A logical network is typically connected to an internal interface.
  - On the Edit Edge Gateway Interface page, type a name for the NSX Edge interface.
  - Click Internal or External to indicate whether this is an internal or external interface.
  - Select the connectivity status of the interface.
  - If the NSX Edge to which you are connecting the logical switch has Manual HA Configuration selected, specify two management IP addresses in CIDR format.
  - Edit the default MTU if required.
  - Click Next.
  - Review the NSX Edge connection details and click Finish.

- Deploy services to a logical switch
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click Logical Switches.
  - Select the logical switch on which you want to deploy services.
  - Click the Add Service Profile () icon.
  - Select the service and service profile that you want to apply.
  - Click OK.

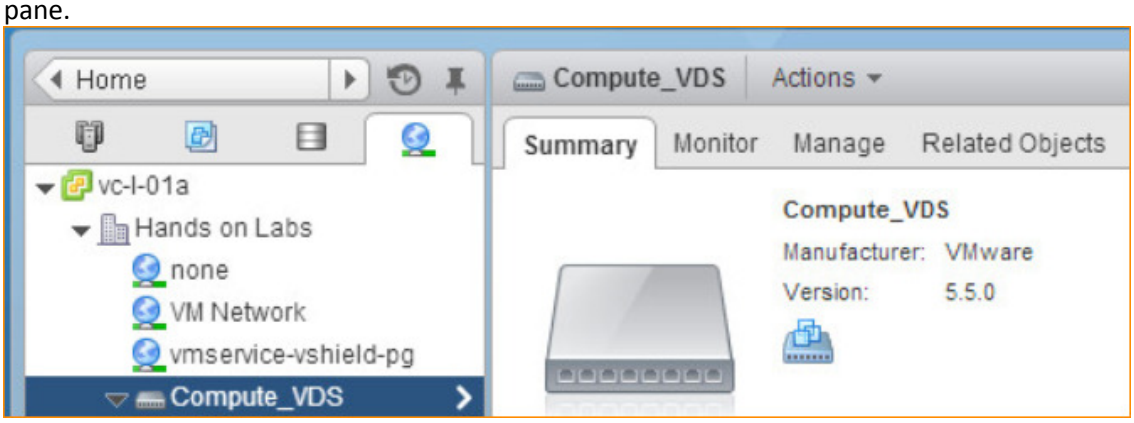
- Connect/Disconnect virtual machines
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click Logical Switches.
  - Select the Logical Switch to which you want to add virtual machines.

- Click the Add "+" icon.
- Select the vNics that you want to connect.
- Click Next.
- Review the vNics you selected.
- Click Finish.

- Test logical switch connectivity
  - A ping test checks if two hosts in a VXLAN transport network can reach each other.
  - Log in to the vSphere web client.
  - Click Networking & Security and then click Logical Switches.
  - In the Name column, click the logical network that you want to test
  - Click the Hosts tab.
  - Select a host.
  - Click the More Actions () icon and select Test Connectivity. The Test Connectivity Between Hosts in the Network dialog box opens. The host you selected in step 5 appears in the Source host field. Select Browse to select a different source host.
  - Select the size of the test packet.
    VXLAN standard size is 1550 bytes (should match the physical infrastructure MTU) without fragmentation. This allows NSX to check connectivity and verify that the infrastructure is prepared for VXLAN traffic.
    Minimum packet size allows fragmentation. Hence, NSX can check only connectivity but not whether the infrastructure is ready for the larger frame size.
  - In the Destination panel, click Browse Hosts.
  - In the Select Host dialog box, select the destination host.
  - Click Select.
  - Click Start Test.
  - The host-to-host ping test results are displayed.

- Determine distributed virtual switch type and version for a given NSX implementation
  - There are 2 types of vSwitch supported for VMware NSX
    - VMware Distributed vSwitch (vDS)
    - Open vSwitch (OVS)
  - The following types of vswitch are not supported for the NSX transport layer
    - VMware Standard vSwitch (vSS)
    - Cisco Nexus 1000v
  - The version of vSwitch can be found here:
    - Log in to the vSphere web client.
    - Click Networking

- Click on a vSwitch, and the manufacturer and version are displayed on the right hand pane.



Tools

- NSX Installation and Upgrade Guide
- NSX Administration Guide
- NSX Manager
- vSphere Web Client

Objective 5.2 – Configure VXLAN

Knowledge

- Identify where to install and configure VXLAN
  - VXLAN is installed and configured on all ESXi hosts that need to communicate within a Transport Zone.
  - Not normally installed/configured on hosts that are just part of the management cluster

- Identify physical network requirements
  - Physical infrastructure MTU is at least 50 bytes more than the MTU of the virtual machine vNIC.
  - DHCP is available on VXLAN transport VLANs if you are using DHCP for IP assignment for VMKNics
  - 5- tuple hash distribution should be enabled for Link Aggregation Control Protocol (LACP).
  - VXLAN traffic should be placed on a separate VLAN from other traffic (Mgmt, vMotion etc)

- Prepare a cluster for VXLAN
  - In the Installation tab, click Host Preparation.
  - For each cluster, click Install in the Installation Status column.
    NOTE While the installation is in progress, do not deploy, upgrade, or uninstall any service or component.
  - Monitor the installation till the Installation Status column displays a green check mark

    Three VIBs are installed and registered with all hosts within the prepared cluster - VXLAN, Distributed Firewall, and Logical Routing.

- Determine the appropriate teaming policy for a given implementation
  - You should choose a teaming policy for VXLAN transport based on the topology of your physical switches.

For certain teaming modes, VMware software creates multiple VTEPs to load balance traffic between the physical vNICs.

Teaming Mode	Multiple VTEPs Created	vDS Version
Source Port	Yes	5.5
LACPv2	No	5.5
LBT	Yes	5.5
Source MAC (MAC Hash)	Yes	5.5
Failover	No	5.1 and later
Ether channel NOTE If you are using blade chassis, ensure that it supports ether channel before choosing this teaming mode.	No	5.1 and later
LACPv1	No	5.1

- Add/Edit/Expand/Contract transport zones
  - See Objective 4.4!

- Prepare VXLAN Tunnel End Points (VTEPs) on clusters
  - Navigate to the Installation > Host Preparation tab.
  - For the cluster on which you want to configure VXLAN, click Configure in the VXLAN column.
  - In the Configuring VXLAN networking dialog box, select the switch to which you want to map the cluster.
  - Type the VLAN transport.
  - Type the Maximum Transmission Units (MTU) for the virtual distributed switch.
    MTU is the maximum amount of data that can be transmitted in one packet before it is divided into smaller packets. VXLAN traffic frames are slightly larger in size because of the encapsulation, so the MTU for each switch must be set to 1550 or higher.
  - In VMKNic IP Addressing, specify the IP pool to be used for the Management and Edge cluster. Use DHCP or IP pool.
  - If you selected Use IP Pool, select an IP pool
  - Select the VMKNic Teaming Policy for the vSwitch. The NIC teaming policy determines the load balancing and failover settings of the virtual switch.
  - Edit the VTEP value, if required.
    VTEP (VXLAN Tunnel End Points) is the number of dvUplinks on the switch, which load balances traffic between multiple PNICs. VMware recommends that you do not edit the default VTEP value. This field is disabled if the teaming policy you selected does not require multiple VTEPs (ether channel, failover, LACPv1, or LACPv2).
  - Click OK

Tools

- NSX Installation and Upgrade Guide
- NSX Administration Guide
- NSX Manager
- vSphere Web Client

Objective 5.3 – Configure and Manage Layer 2 Bridging

Knowledge

- Identify High Availability requirements for Layer 2 Bridging
    - If High Availability is enabled on the Logical Router and the primary NSX Edge virtual machine goes down, the bridge is automatically moved over to the host with the secondary virtual machine. For this seamless migration to happen, VLAN must have been configured on the host that has the secondary NSX Edge virtual machine.
      Therefore, to enable HA for L2 Bridging, you need to enable HA for the Logical Router to which it is attached.

- Add a Layer 2 Bridge to an NSX Edge device
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click NSX Edges.
    - Double-click the NSX Edge to which you are adding the Bridge.
    - Click Manage and then click Bridging.
    - Click the Add icon.
    - Type a name for the bridge.
    - Select the logical switch that you want to create a bridge for.
    - Select the distributed virtual port group that you want to bridge the logical switch to.
    - Click OK.

- Determine when Layer 2 Bridging would be required for a given NSX implementation
    - You can create an L2 bridge between a logical switch and a VLAN, which enables you to migrate virtual workloads to physical devices with no impact on IP addresses. A logical network can leverage a physical gateway and access existing physical network and security resources by bridging the logical switch broadcast domain to the VLAN broadcast domain.

- Determine when multiple Layer 2 Bridges are required for a given NSX implementation
    - The L2 bridge runs on the host that has the NSX Edge logical router virtual machine. An L2 bridge instance maps to a single VLAN, but there can be multiple bridge instances.
      This means that you need multiple L2 Bridges if you need to bridge multiple VLANs into NSX.

Tools

- NSX Installation and Upgrade Guide
- NSX Administration Guide
- NSX Manager
- vSphere Web Client

Objective 5.4 – Configure and Manage Logical Routers

Knowledge

- Describe and differentiate router interfaces
    - Distributed Logical Routers have LIFs (Logical InterFaces) which connect to Logical Switches.
    - Edge Logical Routers have Internal interfaces and Uplink interfaces.
    - Management interfaces are used for out-of-band access to the logical router.

- Determine controller and logical switch requirements for logical router deployment

  - You must have at least three controller nodes and one logical switch in your environment before installing a logical router.

- Add a logical router
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Click the Add "+" icon.
  - In the Add Edge Gateway wizard, select Logical (Distributed) Router.
  - Select Enable High Availability to enable and configure high availability (HA).
  - Type a name for the NSX Edge virtual machine.
  - This name appears in your vCenter inventory. The name should be unique across all Edges within a single tenant.
  - (Optional) Type a host name for the NSX Edge virtual machine.
    This name appears in CLI. If you do not specify the host name, the Edge ID is displayed in CLI.
  - (Optional) Type a description and tenant for this NSX Edge.
  - Click Next.

    Specify the CLI Credentials for Logical Router:
    Edit the credentials to be used for logging in to the Command Line Interface (CLI).

  - On the CLI Credentials page, specify the CLI credentials for your NSX Edge virtual machine.
  - CLI user name Edit if required.
  - CLI password
  - (Optional) Click Enable SSH access if required.
  - Click Next.

    The Edge Appliances page appears.

- Configure distributed routing
  - On the Deployment Configuration page, select the datacenter where you want to place the NSX Edge virtual machine.
  - In NSX Edge Appliances, click the Add ( ) icon to add an appliance.
    If you had selected Enable HA on the Name and Description page, you can add two appliances. If you add a single appliance, NSX Edge replicates its configuration for the standby appliance ensures that the two HA NSX Edge virtual machines are not on the same ESX host even after you use DRS and vMotion (unless you manually vMotion them to the same host).
  - In the Add Edge Appliance dialog box, select the cluster or resource pool and datastore for the appliance.
  - (Optional) Select the host on which the appliance is to be added.
  - (Optional) Select the vCenter folder within which the appliance is to be added.
  - Click OK.
  - Click Next.

    The Interfaces Configuration page appears.

- Configure a management interface
  - On the Interfaces page, type the IP address for the management interface.

- In Management Interface Configuration, click Select next to the Connected To field and select the logical switch or port group that you want to set as the management interface. Add "+" icon to add a subnet for the management interface.
- In the Add Subnet dialog box, click the Add "+" icon.
- Type the IP address of the subnet and click OK. If you add more than one subnet, select the primary subnet.
- Type the subnet prefix length and click OK.
- In Configure Interfaces, click the Add "+" icon to add a traffic interface and type a name for the interface.
- Select Internal or Uplink to indicate whether this is an internal or external interface.
- Select the port group or VXLAN virtual wire to which this interface should be connected.
  - Click Select next to the Connected To field.
  - Depending on what you want to connect to the interface, click the Virtual Wire or Distributed Portgroup tab.
  - Select the appropriate virtual wire or port group.
  - Click OK.
- Select the connectivity status for the interface.
- In Configure Subnets, click the Add "+" icon to add a subnet for the interface.
- In Add Subnet, click the Add "+" icon to add an IP address.
- Type the IP address.
- You must add an IP address to an interface before using it on any feature configuration.
- Click OK.
- Type the subnet prefix length.
- Click OK and then click OK again.
- Click Next.

The Default Gateway page appears.

- Configure High Available for a logical router
  - Type the period in seconds within which, if the backup appliance does not receive a heartbeat signal from the primary appliance, the primary appliance is considered inactive and the back up appliance takes over. The default interval is 15 seconds.
  - (Optional) Type two management IP addresses in CIDR format to override the local link IPs assigned to the HA virtual machines.
  - Ensure that the management IP addresses do not overlap with the IPs used for any other interface and do not interfere with traffic routing. You should not use an IP that exists somewhere else on your network, even if that network is not directly attached to the NSX Edge.
  - Click Next.

  Confirm Settings and Install the Logical Router:

  - On the Summary page, review the settings for the NSX Edge.
  - Click Previous to modify the settings
  - Click Finish to accept the settings and install the NSX Edge router.

- Configure edge routing
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click an NSX Edge.

- Click Routing and then click Global Configuration.
- To configure dynamic routing, click Edit next to Dynamic Routing Configuration.
  - Router ID is a unique identifier to identify the peer that is sending routes. Select an external interface who's IP you want to use as the Router ID or select Custom ID and type an IP address.
  - Do not enable any protocols here.
  - Select Enable Logging to save logging information and select the log level.
- Click Publish Changes.

- Configure routing protocols
  - Static
    - To configure for Static routing, ensure you do not configure dynamic routing (shown in the step above), and configure a default gateway and relevant static routes as shown in the sections below.

  - OSPF
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click NSX Edges.
    - Double-click an NSX Edge.
    - Click Routing and then click OSPF.
    - Do one of the following.
      - For an Edge services gateway Click Enable.
      - For a logical router
        - Click Edit at the top right corner of the window.
        - Click Enable OSPF.
        - In Forwarding Address, type an IP address that is to be used by the router datapath module in the hosts to forward datapath packets.
        - In Protocol Address, type a unique IP address within the same subnet as the Forwarding Address. Protocol address is used by the protocol to form adjacencies with the peers.
    - In Area Definitions, click the Add icon.
    - Type an Area ID. NSX Edge supports an area ID in the form of an IP address or decimal number.
    - Select Stub in the Type field. Typically, there is no hierarchical routing beyond the stub.
    - Select the type of Authentication. OSPF performs authentication at the area level, hence all routers within the area must have the same authentication and corresponding password configured. For MD5 authentication to work, both the receiving and transmitting routers must have the same MD5 key.
      - None: No authentication is required, which is the default value.
      - Password: In this method of authentication, a password is included in the transmitted packet.
      - MD5: This authentication method uses MD5 (Message Digest type 5) encryption. An MD5 checksum is included in the transmitted packet.
    - For Password or MD5 type authentication, type the password or MD5 key.
    - Click OK.
    - In Area to Interface Mapping, click the Add icon to map the interface that belongs to the OSPF area.
    - Select the interface that you want to map and the OSPF area that you want to map it to.
    - Hello Interval displays the default interval between hello packets that are sent on the interface. Edit the default value if required.

- Dead Interval displays the default interval during which at least one hello packet must be received from a neighbour before the router declares that neighbour down. Edit the default interval if required.
- Priority displays the default priority of the interface. The interface with the highest priority is the designated router. Edit the default value if required.
- Cost of an interface displays the default overhead required to send packets across that interface. The cost of an interface is inversely proportional to the bandwidth of that interface. Edit the default value if required.
- Click OK and then click Publish Changes.

- BGP
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click an NSX Edge.
  - Click Routing and then click BGP.
  - Click Edit.
  - In the Edit BGP Configuration dialog box, click Enable BGP.
  - Type the router ID in Local AS. Type the Local AS. This is advertised when BGP peers with routers in other autonomous systems (AS). The path of ASs that a route traverses is used as one metric when selecting the best path to a destination.
  - Click Save.
  - In Neighbors, click the Add icon.
  - Type the IP address of the neighbour.
  - Type the remote AS.
  - Edit the default weight for the neighbour connection if required.
  - Hold Down Timer displays interval (180 seconds) after not receiving a keep alive message that the software declares a peer dead. Edit if required.
  - Keep Alive Timer displays the default frequency (60 seconds) with which the software sends keep alive messages to its peer. Edit if required.
  - If authentication is required, type the authentication password. Each segment sent on the connection between the neighbours is verified. MD5 authentication must be configured with the same password on both BGP neighbours, otherwise, the connection between them will not be made.
  - To specify route filtering from a neighbour, click the Add icon in the BGP Filters area.
  - Select the direction to indicate whether you are filtering traffic to or from the neighbour.
  - Select the action to indicate whether you are allowing or denying traffic.
  - Type the network in CIDR format that you want to filter to/from the neighbour.
  - Type the IP prefixes that are to be filtered and click OK.
  - Click Publish Changes.

- IS-IS
  The IS-IS protocol is currently experimental
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click an NSX Edge.
  - Click Routing and then click IS-IS.
  - Click Edit and then click Enable IS-IS.
  - Type the System ID and select the IS-IS type.
    Level 1 is intra-area, Level 2 is inter-area, and Level 1-2 is both. Level 2 routers are inter-area routers that can only form relationships with other Level 2 routers. Routing

information is exchanged between Level 1 routers and other Level 1 routers, and Level 2 routers only exchange information with other Level 2 routers. Level 1-2 routers exchange information with both levels and are used to connect the inter-area routers with the intra-area routers.

- Type the Domain Password and Area Password. The area password is inserted and checked for Level 1 link state packets, and the domain password for Level 2 link state packets.
- Define the IS-IS areas.
  - Click the Add icon in Areas.
  - Type up to three area IP addresses.
  - Click Save.
- Configure interface mapping.
  - Click the Add icon in Interface Mapping.
  - Choose the Circuit Type to indicate whether you are configuring the interface for Level-1, Level-2, or Level-1-2 adjacency.
  - Hello Interval displays the default interval in milliseconds between hello packets that are sent on the interface. Edit the default value if required.
  - Hello Multiplier displays the default number of IS-IS hello packets a neighbour must miss before it is declared down. Edit the default value if required.
  - LSP Interval displays the time delay in milliseconds between successive IS-IS link-state packet (LSP) transmissions. Edit the default value if required.
  - Metric displays default metric for the interface. This is used to calculate the cost from each interface via the links in the network to other destinations. Edit the default value if required.
  - Priority displays the priority of the interface. The interface with the highest priority becomes the designated router. Edit the default value if required.
  - In Mesh Group, type the number identifying the mesh group to which this interface belongs. Edit the default value if required.
  - Type the authentication password for the interface and click OK. Edit the default value if required.
- Click Publish Changes.

- Configure default gateway
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click an NSX Edge.
  - Click Routing and then click Global Configuration.
  - To specify the default gateway, click Edit next to Default Gateway.
    - Select an interface from which the next hop towards the destination network can be reached.
    - Type the gateway IP if required.
    - Edit the MTU if required and type a description.
    - Click Save.
  - Click Publish Changes.

- Add/Delete a static route
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.

  - Double-click an NSX Edge.
  - Click the Manage tab and then click the Routing tab.
  - Select Static Routes from the left panel.
  - Click the Add “+” icon.
  - Type a description for the static route.
  - Select the interface on which you want to add a static route.
  - Type the Network in CIDR notation.
  - Type the IP address of the Next Hop.
  - For MTU, edit the maximum transmission value for the data packets if required. The MTU cannot be higher than the MTU set on the NSX Edge interface.
  - Click OK.

- Determine if cross-protocol route sharing is needed for a given NSX implementation
  - By default, routers share routes with other routers running the same protocol. In a multi-protocol environment, you must configure route redistribution for cross-protocol route sharing.

Tools

- NSX Installation and Upgrade Guide
- NSX Administration Guide
- NSX Manager
- NSX CLI
- vSphere Web Client

Section 6 – Configure and Manage NSX Network Services

Objective 6.1 – Configure and Manage Logical Load Balancing

Knowledge

- Identify general ESXi host troubleshooting guidelines
    - I believe this has been erroneously left in from the VCP-DCV Blueprint Section 6.1.
      If you want to study this anyway, I would check out the numerous VCP5-DCV study guides around on the web.

- Configure global load balancing configuration
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click NSX Edges.
    - Double-click an NSX Edge.
    - Click Manage and then click the Load Balancer tab.
    - Click Edit.
    - Select the check boxes next to the options you want to enable.
        - Enable Loadbalancer
          Allows the NSX Edge load balancer to distribute traffic to internal servers for load balancing.
        - Enable Service Insertion
          allows the load balancer to work with third party vendor appliances.
        - Acceleration Enabled
          When enabled, the NSX Edge load balancer uses the faster L4 LB engine rather than L7 LB engine.
        - Logging
          NSX Edge load balancer collects traffic logs. You can also choose the log level.
    - Click OK.

- Create a service monitor
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click NSX Edges.
    - Double-click an NSX Edge.
    - Click Manage and then click the Load Balancer tab.
    - In the left navigation panel, click Service Monitoring.
    - Click the Add icon.
    - Type a name for the service monitor.
    - Type the interval at which a server is to be pinged.
    - Type the maximum time in seconds within which a response from the server must be received.
    - Type the number of times the server must be pinged before it is declared down.
    - Select the way in which you want to send the health check request to the server.
    - For HTTP and HTTPS traffic, perform the steps below.
        - In Expect, type the string that the monitor expects to match in the status line of HTTP response (for example, HTTP/1.1).
        - Select the method to be used to detect server status.
        - Type the URL to be used in the sample request.
        - If you selected the POST method, type the data to be sent.

        - In Receive, type the string to be matched in the response content.
          If Expect is not matched, the monitor does not try to match the Receive content.
        - (Optional) In Extension, type advanced monitor parameters as key=value pairs.
          For example, warning=10 indicates that if a server does not respond within 10 seconds, its status is set as warning.
    - Click OK.

- Add/Edit/Delete a server pool
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click NSX Edges.
    - Double-click an NSX Edge.
    - Click Manage and then click the Load Balancer tab.
    - In the left navigation panel, click Pools.
    - Type a name and description for the load balancer pool.
    - Select a balancing method for each enabled service.
        - IP_HASH
          Selects a server based on a hash of the source and destination IP address of each packet.
        - LEAST_CONN Distributes client requests to multiple servers based on the number of connections already on the server. New connections are sent to the server with the fewest connections.
        - ROUND_ROBIN Each server is used in turn according to the weight assigned to it. This is the smoothest and fairest algorithm when the server's processing time remains equally distributed.
        - URI The left part of the URI (before the question mark) is hashed and divided by the total weight of the running servers. The result designates which server will receive the request. This ensures that a URI is always directed to the same server as long as no server goes up or down.
    - Add members to the pool.
        - Click the Add icon.
        - Type the name and IP address of the server member.
        - Type the port where the member is to receive traffic on and the monitor port where the member is to receive health monitor pings.
        - In Weight, type the proportion of traffic this member is to handle.
        - Type the maximum number of connections the member can handle.
        - Type the minimum number of connections a member should handle before traffic is redirected to the next member.
        - Click OK.
    - Transparent indicates whether client IP addresses are visible to the backend servers. If Transparent is not selected (default value), backend servers see the traffic source IP as a Load balancer internal IP. If Transparent is selected, source IP is the real client IP and NSX Edge must be set as the default gateway to ensure that return packets go through the NSX Edge device.
    - Click OK.

- Add/Edit/Delete an application profile
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click NSX Edges.
    - Double-click an NSX Edge.
    - Click Manage and then click the Load Balancer tab.

- In the left navigation panel, click Application Profiles.
- Click the Add icon.
- Type a name for the profile and select the traffic type for which you are creating the profile.
- Type the URL to which you want to re-direct HTTP traffic. For example, you can direct traffic from http://myweb.com to https://myweb.com.
- Specify persistence for the profile. Persistence tracks and stores session data, such as the specific pool member that serviced a client request. This ensures that client requests are directed to the same pool member throughout the life of a session or during subsequent sessions.
  Cookie persistence inserts a cookie to uniquely identify the session the first time a client accessed the site and then refers to that cookie in subsequent requests to persist the connection to the appropriate server. Type the cookie name and select the mode by which the cookie should be inserted.
  SOURCEIP persistence tracks sessions based on the source IP address. When a client requests a connection to a virtual server that supports source address affinity persistence, the load balancer checks to see if that client previously connected, and if so, returns the client to the same pool member.
  Microsoft Remote Desktop Protocol (MSRDP) persistence maintains persistent sessions between Windows clients and servers that are running the Microsoft Remote Desktop Protocol (RDP) service. The recommended scenario for enabling MSRDP persistence is to create a load balancing pool that consists of members running Windows Server 2003 or Windows Server 2008, where all members belong to a Windows cluster and participate in a Windows session directory.

Traffic Type	Persistence Method Supported
TCP	SOURCEIP, MSRDP
HTTP	Cookie, SOURCEIP
HTTPS	Cookie, ssl_session_id (SSL Passthrough enabled) , SOURCEIP

- If you are creating a profile for HTTPS traffic, complete the steps below. The following HTTPS traffic pattern are allowed.
  client -> HTTPS -> LB -> HTTP -> servers
  client -> HTTPS -> LB -> HTTPS -> servers
  client -> HTTP-> LB -> HTTPS -> servers

  - Select Insert X-Forwarded-For HTTP header for identifying the originating IP address of a client connecting to a web server through the load balancer.
  - Select the certificate/CAs/CRLs used to decrypt HTTPS traffic in Virtual Server certificates.
  - Define the certificate/CAs/CRLs used to authenticate the load balancer from the server side in Pool Certificates.

- In Cipher, select the cipher algorithms (or cipher suite) negotiated during the SSL/TLS handshake.
  Specify whether client authentication is to be ignored or required. If set to required, the client must provide a certificate after the request or the handshake is aborted.
- Click OK.

- Add/Edit/Delete virtual servers
  - Log in to the vSphere Web Client.

- Click Networking & Security and then click NSX Edges.
- Double-click an NSX Edge.
- Click Manage and then click the Load Balancer tab.
- In the left navigation panel, click Virtual Servers.
- Click the Add "+" icon.
- Type a name for the virtual server.
- (Optional) Type a description for the virtual server.
- Type the IP address that the load balancer is listening on. Type the protocol that the virtual server will handle.
- Type the protocol that the virtual server will handle.
- Type the port number that the load balancer will listen on.
- Select the application profile to be associated with the virtual server. You can associate only an application profile with the same protocol as the virtual server that you are adding. The services supported by the selected pool appear.
- Select the application rule to be associated with the virtual server.
- In Connection Limit, type the maximum concurrent connections that the virtual server can process.
- In Connection Rate Limit, type the maximum incoming new connection requests per second.
- Click OK.

- Configure global server load balancing
  - I have spent a great deal of time trying to find something in the given documentation relating to this, to no avail. My understanding is that "Global Server Load Balancing" is to do with directing user requests to their geographically local datacenter, by manipulating the DNS response. However there is nothing to do with this in the NSX documentation that I can see. A number of 3rd party vendors have stated they will provide this via a service, but I have yet to uncover any configuration guides.

- Determine appropriate NSX Edge instance size based on load balancing requirements
  - The Large NSX Edge has more CPU, memory, and disk space than the Compact NSX Edge, and supports a bigger number of concurrent SSL VPN-Plus users.
  - The X-Large NSX Edge is suited for environments which have Load Balancer with millions of concurrent sessions.
  - The Quad Large NSX Edge is recommended for high throughput and requires a high connection rate.

Tools

- NSX Installation and Upgrade Guide
- NSX Administration Guide
- HAProxy Configuration Manual
- NSX Manager
- vSphere Web Client

Objective 6.2 – Configure and Manage Logical Virtual Private Networks (VPN)

Knowledge

- Configure IPSec VPN
  - Add/Edit/Disable IPSec VPN Service
    - Enable

- Log in to the vSphere Web Client.
- Click Networking & Security and then click NSX Edges.
- Double-click an NSX Edge.
- Click the Manage tab and then click the VPN tab.
- Click IPSec VPN.
- Click Enable.

- Specify Global IPSec Configuration
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click an NSX Edge.
  - Click the Manage tab and then click the VPN tab.
  - Click IPSec VPN.
  - Click Change next to Global configuration status.
  - Type a global pre-shared key for those sites whose peer endpoint is set to any and select Displayshared key to display the key.
  - Select Enable certificate authentication and select the appropriate certificate.
  - Click OK.

- Configure IPSec VPN parameters
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click an NSX Edge.
  - Click the Manage tab and then click the VPN tab.
  - Click IPSec VPN.
  - Click the Add “+” icon.
  - Type a name for the IPSec VPN.
  - Type the IP address of the NSX Edge instance in Local Id. This will be the peer Id on the remote site.
  - Type the IP address of the local endpoint.
    If you are adding an IP to IP tunnel using a pre-shared key, the local Id and local endpoint IP can be the same.
  - Type the subnets to share between the sites in CIDR format. Use a comma separator to type multiple subnets.
  - Type the Peer Id to uniquely identify the peer site. For peers using certificate authentication, this ID must be the common name in the peer's certificate. For PSK peers, this ID can be any string. VMware recommends that you use the public IP address of the VPN or a FQDN for the VPN service as the peer ID.
  - Type the IP address of the peer site in Peer Endpoint. If you leave this blank, NSX Edge waits for the peer device to request a connection.
  - Type the internal IP address of the peer subnet in CIDR format. Use a comma separator to type multiple subnets.
  - Select the Encryption Algorithm
  - In Authentication Method, select one of the following:
    - **PSK (Pre Shared Key)** Indicates that the secret key shared between NSX Edge and the peer site is to be used for authentication. The secret key can be a string with a maximum length of 128 bytes.
    - **Certificate** Indicates that the certificate defined at the global level is to be used for authentication.

- Type the shared key in if anonymous sites are to connect to the VPN service.
- Click Display Shared Key to display the key on the peer site.
- In Diffie-Hellman (DH) Group, select the cryptography scheme that will allow the peer site and the NSX Edge to establish a shared secret over an insecure communications channel.
- Edit the default MTU if required.
- Select whether to enable or disable the Perfect Forward Secrecy (PFS) threshold. In IPsec negotiations, Perfect Forward Secrecy (PFS) ensures that each new cryptographic key is unrelated to any previous key.
- Click OK.

  NSX Edge creates a tunnel from the local subnet to the peer subnet.
- Edit IPSec VPN Service
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click an NSX Edge.
  - Click the Monitor tab and then click VPN tab.
  - Click IPSec VPN.
  - Select the IPSec service that you want to edit.
  - Click the Edit icon.
  - Make the appropriate edits.
  - Click OK.

- Disable IPSec VPN Service
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click an NSX Edge.
  - Click the Monitor tab and then click VPN tab.
  - Click IPSec VPN.
  - Select the IPSec service that you want to disable.
  - Click the Disable icon.

- Enable logging
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click an NSX Edge.
  - Click the Manage tab and then click the VPN tab.
  - Click IPSec VPN.
  - Click next to Logging Policy and click Enable logging to log the traffic flow between the local subnet and peer subnet and select the logging level.
  - Select the log level and click Publish Changes .

- Configure Layer 2 VPN
  - Enable Layer 2 VPN
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click NSX Edges.
    - Double-click an NSX Edge.
    - Click the Manage tab and then click the VPN tab.
    - Click L2 VPN.

        - Click Enable

    - Add Layer 2 VPN Client/Server
        - Client:
            - Log in to the vSphere Web Client.
            - Click Networking & Security and then click NSX Edges.
            - Double-click an NSX Edge.
            - Click the Manage tab and then click the VPN tab.
            - Click L2 VPN, select Client, and click Change.
            - Expand Client Details and type the server address to which the VPN is to be connected. The address can be the host name or IP address.
            - If required, edit the default port to which the VPN is to be connected.
            - Select the internal interface on the NSX Edge to be stretched. The interface must be connected to a dvport group or logical switch.
            - Type a description.
            - Expand User Details and type the same user credentials as specified on the L2 VPN server.
            - If the client NSX Edge does not have direct access to the internet and needs to reach the source (server) NSX Edge via a proxy server, expand Proxy Settings.
            - To enable only secure proxy connections, select Enable Secure Proxy.
            - Type the proxy server address, port, user name, and password.
            - Do one of the following.
                - To enable server certificate validation, select Validate Server Certificate and select the appropriate certificate.
                - To disable server certificate validation, un-select Validate Server Certificate.
            - Click OK.

        - Server:
            - Log in to the vSphere Web Client.
            - Click Networking & Security and then click NSX Edges.
            - Double-click an NSX Edge.
            - Click the Manage tab and then click the VPN tab.
            - Click L2 VPN, select Server, and click Change.
            - Expand Server Details.
            - In Listener IP, type the primary or secondary IP address of an external interface of the NSX Edge.
            - The default port for the L2 VPN service is 443. Edit this if required.
            - Select the encryption method.
            - Select the internal interface of the NSX Edge which is being stretched. This interface must be connected to a dv port group or logical switch.
            - Type a description.
            - Expand User Details and type the user name and password.
            - In Server Certificates, do one of the following.
                - Select Use System Generated Certificate to use a self-signed certificate for authentication.
                - Select the signed certificate to be used for authentication.

- Click OK.

- View Layer 2 VPN Statistics
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click an NSX Edge.
  - Click the Manage tab and then click the VPN tab.
  - Click L2 VPN.
  - Click Fetch Status and expand Tunnel Status.

- Configure Network Access/Web Access SSL VPN-Plus
  - Edit Client Configurations
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click NSX Edges.
    - Double-click an NSX Edge.
    - Click the Monitor tab and then click the SSL VPN-Plus tab.
    - Select Client Configuration from the left panel.
    - Select the Tunneling Mode.
      In split tunnel mode, only the VPN flows through the NSX Edge gateway. In full tunnel, the NSX Edge gateway becomes the remote user's default gateway and all traffic (VPN, local, and internet) flows through this gateway.
    - If you selected the full tunnel mode:
      - Select Exclude local subnets to exclude local traffic from flowing through the VPN tunnel.
      - Type the IP address for the default gateway of the remote user's system.
    - Select Enable auto reconnect if you would like the remote user to automatically reconnect to the SSL VPN client after getting disconnected.
    - Select Client upgrade notification for the remote user to get a notification when an upgrade for the client is available. The remote user can then choose to install the upgrade.
    - Click OK.

  - Edit General Settings
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click NSX Edges.
    - Double-click an NSX Edge.
    - Click the Monitor tab and then click the SSL VPN-Plus tab.
    - Select General Settings from the left panel.
    - Make required selections.
      - **Prevent multiple logon using same username**
        Allow a remote user to login only once with a username.
      - **Enable compression**
        Enable TCP based intelligent data compression and improve data transfer speed.
      - **Enable logging**
        Maintain a log of the traffic passing through the SSL VPN gateway.
      - **Force virtual keyboard**
        Allow remote users to enter web or client login information only via the virtual keyboard.

- **Randomize keys of virtual keyboard**
  Make the virtual keyboard keys random.
- **Enable forced timeout**
  Disconnect the remote user after the specified timeout period is over. Type the timeout period in minutes.
- **Session idle timeout**
  If there is no activity on the user session for the specified period, end the user session after that period is over.
- **User notification**
  Type a message to be displayed to the remote user after he logs in.
- **Enable public URL access**
  Allow remote user to access any site which is not configured (and not listed on web portal) by administrator.

- Click OK.

- Edit Web Portal Designs
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click a vShield Edge.
  - Click the Manage tab and then click the SSL VPN-Plus tab.
  - Select Portal Customization from the left panel.
  - Type the portal title.
  - Type the remote user's company name.
  - In Logo, click Change and select the image file for the remote user's logo.
  - In Colors, click the color box next to numbered item for which you want to change the color, and select the desired color.
  - If desired, change the client banner.
  - Click OK.

- Add/Edit/Delete IP Pools
  - Add:
    - Click Networking & Security and then click NSX Edges.
    - Double-click a vShield Edge.
    - Click the Manage tab and then click the SSL VPN-Plus tab.
    - In the SSL Vpn-Plus tab, select IP Pools from the left panel.
    - Click the Add “+” icon.
    - Type the begin and end IP address for the IP pool.
    - Type the netmask of the IP pool.
    - Type the IP address which is to add the routing interface in the NSX Edge gateway.
    - (Optional) Type a description for the IP pool.
    - Select whether to enable or disable the IP pool.
    - (Optional) In the Advanced panel, type the DNS name.
    - (Optional) Type the secondary DNS name.
    - Type the connection-specific DNS suffix for domain based host name resolution.
    - Type the WINS server address.
    - Click OK.
  - Edit:

- Log in to the vSphere Web Client.
- Click Networking & Security and then click NSX Managers.
- Click an NSX Manager in the Name column and then click the Manage tab.
- Click the Grouping Objects tab and then click IP Pool.
- Select the IP pool that you want to edit.
- Click the Edit (Pencil) icon.
  The Edit IP Pool dialog box opens.
- Make the required edits.
- Click OK.

- Enable/Disable IP Pools
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click an NSX Edge.
  - Click the Monitor tab and then click the SSL VPN-Plus tab.
  - Select IP Pool from the left panel.
  - Select the IP pool that you want to enable/disable
  - Click the Enable (Tick) icon or Disable (No Entry) icon

- Add/Edit/Delete Private Networks
  - In the SSL Vpn-Plus tab, select Private Networks from the left panel.
  - Click the Add ( ) icon
  - Type the private network IP address.
  - Type the netmask of the private network.
  - (Optional) Type a description for the network.
  - Specify whether you want to send private network and internet traffic over the SSL VPN-Plus enabled NSX Edge or directly to the private server by bypassing the NSX Edge.
  - If you selected Send traffic over the tunnel, select Enable TCP Optimization to optimize the internet speed.
    Conventional full-access SSL VPNs tunnel sends TCP/IP data in a second TCP/IP stack for encryption over the internet. This results in application layer data being encapsulated twice in two separate TCP streams. When packet loss occurs (which happens even under optimal internet conditions), a performance degradation effect called TCP-over-TCP meltdown occurs. In essence, two TCP instruments are correcting a single packet of IP data, undermining network throughput and causing connection timeouts. TCP Optimization eliminates this TCP-over-TCP problem, ensuring optimal performance.
  - Type the port numbers that you want to open for the remote user to access the corporate internal servers/machines like 3389 for RDP, 20/21 for FTP, and 80 for http. If you want to give unrestricted access to the user, you can leave the Ports field blank.
  - Specify whether you want to enable or disable the private network.
  - Click OK.

- Enable/Disable Private Networks
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click an NSX Edge.

- Click the Monitor tab and then click the SSL VPN-Plus tab.
- Select Private Networks from the left panel.
- Click the network that you want to enable/disable/delete
- Click the Enable icon (Tick)/Disable icon (No entry sign)/Delete icon (cross)
- The selected network is enabled/disabled/deleted

- Add/Edit/Delete Installation Packages
  - In the SSL Vpn-Plus tab, select Installation Package from the left panel.
  - Click the Add "+" icon.
  - Type a profile name for the installation package.
  - In Gateway, type the IP address or FQDN of the public interface of NSX Edge. This IP address or FQDN is binded to the SSL client. When the client is installed, this IP address or FQDN is displayed on the SSL client.
  - Type the port number that you specified in the server settings for SSL VPN-Plus.
  - (Optional) To bind additional NSX Edge uplink interfaces to the SSL client,
    - Click the Add "+" icon.
    - Type the IP address and port number.
    - Click OK.
  - The installation package is created for Windows operating system by default. Select Linux or Mac to create an installation package for Linux or Mac operating systems as well.
  - (Optional) Enter a description for the installation package.
  - Select Enable to display the installation package on the Installation Package page.
  - Select the following options as appropriate.
    - **Start client on logon**
      The SSL VPN client is started when the remote user logs on to his system.
    - **Allow remember password**
      Enables the option.
    - **Enable silent mode installation**
      Hides installation commands from remote user.
    - **Hide SSL client network adapter**
      Hides the VMware SSL VPN-Plus Adapter, which is installed on the remote user's computer along with the SSL VPN installation package.
    - **Hide client system tray icon**
      Hides the SSL VPN tray icon which indicates whether the VPN connection is active or not.
    - **Create desktop icon**
      Creates an icon to invoke the SSL client on the user's desktop.
    - **Enable silent mode operation**
      Hides the pop-up that indicates that installation is complete.
    - **Server security certificate validation**
      The SSL VPN client validates the SSL VPN server certificate before establishing the secure connection.
  - Click OK.

- Add/Edit/Delete Users
  - In the SSL Vpn-Plus tab, select Users from the left panel.
  - Click the Add "+" icon.
  - Type the user ID.

        - Type the password.
        - Retype the password.
        - (Optional) Type the first and last name of the user.
        - (Optional) Type a description for the user.
        - In Password Details, select Password never expires to always keep the same password for the user.
        - Select Allow change password to let the user change the password.
        - Select Change password on next login if you want the user to change the password the next time he logs in.
        - Set the user status.
        - Click OK.

    - Add/Edit/Delete Login/Logoff script
        - In the SSL Vpn-Plus tab, select Login/Logoff Scripts from the left panel.
        - Click the Add "+" icon.
        - In Script, click Browse and select the script you want to bind to the NSX Edge gateway.
        - Select the Type of script.
            - Login - Performs the script action when remote user logs in to SSL VPN.
            - Logoff - Performs the script action when remote user logs out of SSL VPN.
            - Both - Performs the script action both when remote user logs in and logs out of SSL VPN.
        - Type a description for the script.
        - Select Enabled to enable the script.
        - Click OK.

    - Enable/Disable Login/Logoff script
        - Log in to the vSphere Web Client.
        - Click Networking & Security and then click NSX Edges.
        - Double-click an NSX Edge.
        - Click the Manage tab and then click the SSL VPN-Plus tab.
        - Select Login/Logoff Scripts from the left panel.
        - Select a script and click the Enable (Tick) icon/Disable (No entry sign) icon

- Determine appropriate VPN service type for a given NSX implementation
    - SSL VPN-Plus allows remote users to access private corporate applications.
        - Network Access SSL VPN-Plus requires users to download a client to access private networks.
        - Web Access SSL VPN-Plus allows users to access private networks without a hardware or software SSL client
    - IPSec VPN offers site-to-site connectivity between an NSX Edge instance and remote sites.
    - L2 VPN allows you to extend your datacenter by allowing virtual machines to retain network connectivity across geographical boundaries.

- Determine appropriate NSX Edge instance size based on load balancing requirements
    - The Large NSX Edge has more CPU, memory, and disk space than the Compact NSX Edge, and supports a bigger number of concurrent SSL VPN-Plus users.

- The X-Large NSX Edge is suited for environments which have Load Balancer with millions of concurrent sessions.
- The Quad Large NSX Edge is recommended for high throughput and requires a high connection rate.

Tools

- NSX Installation and Upgrade Guide
- NSX Administration Guide
- NSX Manager
- vSphere Web Client

Objective 6.3 – Configure and Manage DHCP/DNS/NAT

Knowledge

- Add/Edit a DHCP IP pool
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click an NSX Edge.
  - Click the Manage tab and then click the DHCP tab.
  - Click the Add "+" icon (or select the pool and click Edit)
  - Configure the pool.
    - **Auto Configure**
      DNS Select to use the DNS service configuration for the DHCP binding.
    - **Lease never expires**
      Select to bind the address to the MAC address of the virtual machine forever. If you select this, Lease Time is disabled.
    - **Start IP**
      Type the starting IP address for the pool.
    - **End IP**
      Type the ending IP address for the pool.
    - **Domain** Name
      Type the domain name of the DNS server. This is optional.
    - **Primary Name Server**
      If you did not select Auto Configure DNS, type the Primary Nameserver for the DNS service. You must enter the IP address of a DNS server for hostname-to-IP address resolution. This is optional.
    - **Secondary Name Server**
      If you did not select Auto Configure DNS, type the Secondary Nameserver for the DNS service. You must enter the IP address of a DNS server for hostname-to-IP address resolution. This is optional.
    - **Default Gateway**
      Type the default gateway address. If you do not specify the default gateway IP address, the internal interface of the NSX Edge instance is taken as the default gateway. This is optional.
    - **Lease Time**
      Select whether to lease the address to the client for the default time (1 day), or type a value in seconds. You cannot specify the lease time if you selected Lease never expires. This is optional.

- Click OK.

- Enable a DHCP IP pool
  I assume this should say “enable the DHCP Service”
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click an NSX Edge.
  - Click the Manage tab and then click the DHCP tab.
  - Click Enable.
  - Select Enable logging if required and select the log level.
  - Click Publish Changes.

- Add/Edit DHCP static binding
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click an NSX Edge.
  - Click the Manage tab and then click the DHCP tab.
  - Select Bindings from the left panel.
  - Click the Add “+” icon (or select the binding and click Edit)
  - Configure the binding.
    - **Auto Configure DNS**
      Select to use the DNS service configuration for the DHCP binding.
    - **Lease never expires**
      Select to bind the address to the MAC address of the virtual machine forever.
    - **Interface**
      Select the NSX Edge interface to bind.
    - **VM Name**
      Select the virtual machine to bind.
    - **VM vNIC Index**
      Select the virtual machine NIC to bind to the IP address.
    - **Host Name**
      Type the host name of the DHCP client virtual machine.
    - **IP Address**
      Type the address to which to bind the MAC address of the selected virtual machine.
    - **Domain Name**
      Type the domain name of the DNS server.
    - **Primary Name Server**
      If you did not select Auto Configure DNS, type the Primary Nameserver for the DNS service. You must enter the IP address of a DNS server for hostname-to-IP address resolution.
    - **Secondary Name Server**
      If you did not select Auto Configure DNS, type the Secondary Nameserver for the DNS service. You must enter the IP address of a DNS server for hostname-to-IP address resolution.
    - **Default Gateway**
      Type the default gateway address. If you do not specify the default gateway IP address, the internal interface of the NSX Edge instance is taken as the default gateway.

        - **Lease Time**
          If you did not select "Lease never expires", select whether to lease the address to the client for the default time (1 day), or type a value in seconds.
    - Click Add.
    - Click Publish Changes.

- Configure DNS services
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click NSX Edges.
    - Double-click a NSX Edge.
    - Click the Manage tab and then click the Settings tab.
    - In the DNS Configuration panel, click Change.
    - Click Enable DNS Service to enable the DNS service.
    - Type IP addresses for both DNS servers.
    - Change the default cache size if required.
    - Click Enable Logging to log DNS traffic and select the log level
      Generated logs are sent to the syslog server.
    - Click Ok.

- Add Source NAT (SNAT) rule
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click NSX Edges.
    - Double-click an NSX Edge.
    - Click the Manage tab and then click the NAT tab.
    - Click the Add "+" icon and select Add SNAT Rule.
    - Select the interface on which to add the rule.
    - Type the original source IP address in one of the following formats.
        - IP address eg 192.0.2.0
        - IP address range eg 192.0.2.0-192.0.2.24
        - IP address/subnet eg 192.0.2.0/24
        - "any"
    - Type the translated (public) source IP address in one of the following formats
        - IP address eg 192.0.2.0
        - IP address range eg 192.0.2.0-192.0.2.24
        - IP address/subnet eg 192.0.2.0/24
        - "any
    - Select Enabled to enable the rule.
    - Click Enable logging to log the address translation.
    - Click OK to add the rule.
    - Click Publish Changes.

- Add Destination NAT (DNAT) rule
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click NSX Edges.
    - Double-click an NSX Edge.
    - Click the Manage tab and then click the NAT tab.
    - Click the Add "+" icon and select Add DNAT Rule.
    - Select the interface on which to apply the DNAT rule.
    - Type the original (public) IP address in one of the following formats.
        - IP address eg 192.0.2.0

        - IP address range eg 192.0.2.0-192.0.2.24
        - IP address/subnet eg 192.0.2.0/24
        - "any"
    - Type the protocol
    - Type the original port or port range.
        - Port number eg 80
        - Port range eg 80-85
        - "any"
    - Type the translated IP address in one of the following formats.
        - IP address eg 192.0.2.0
        - IP address range eg 192.0.2.0-192.0.2.24
        - IP address/subnet eg 192.0.2.0/24
        - "any"
    - Type the translated port or port range.
        - Port number eg 80
        - Port range eg 80-85
        - "any"
    - Select Enabled to enable the rule.
    - Select Enable logging to log the address translation.
    - Click Add to save the rule.

Tools

- NSX Administration Guide
- NSX Manager
- vSphere Web Client

Objective 6.4 – Configure and Manage Edge Services High Availability

Knowledge

- Describe NSX Edge High Availability
    - High Availability (HA) ensures that an NSX Edge appliance is always available by installing an active pair of Edges on your virtualized infrastructure. You can enable HA either when installing NSX Edge or on an installed NSX Edge instance.
    - The primary NSX Edge appliance is in the active state and the secondary appliance is in the standby state. NSX Edge replicates the configuration of the primary appliance for the standby appliance or you can manually add two appliances.

- Explain Edge High Availability best practices
    - VMware recommends that you create the primary and secondary appliances on separate resource pools and datastores. If you create the primary and secondary appliances on the same datastore, the datastore must be shared across all hosts in the cluster for the HA appliance pair to be deployed on different ESX hosts.
        - *This seems to conflict with the statement "Two virtual machines are deployed on vCenter in the same resource pool and datastore as the appliance you configured"*

- Describe service availability during an Edge High Availability failover
    - If a heartbeat is not received from the primary appliance within the specified time (default value is 15 seconds – 3x 5s, can be reduced to 6 seconds – 3x 2s), the primary appliance is declared dead. The standby appliance moves to the active state, takes over the interface

configuration of the primary appliance, and starts the NSX Edge services that were running on the primary appliance. When the switch over takes place, a system event is displayed in the System Events tab of Settings & Reports. Load Balancer and VPN services need to re-establish TCP connection with NSX Edge, so service is disrupted for a short while. Virtual wire connections and firewall sessions are synched between the primary and standby appliances, so there is no service disruption during switch over.

- Differentiate NSX Edge High Availability and vSphere High Availability
  - NSX Edge High Availability is stateful, and uses 2 running VMs. In the event of failure of the host server where the Primary VM is running, the Secondary VM takes over the service.
  - vSphere High Availability monitors for a host failure and restarts any lost VMs on other hosts in the cluster. This is used to restart the original Primary VM in the event of a host failure, so that an NSX Edge HA pair still remains in the event of a further failure.

- Configure NSX Edge High Availability
  - Configure heartbeat settings
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click NSX Edges.
    - Double-click an NSX Edge.
    - Click the Manage tab and then click the Settings tab.
    - In the HA Configuration panel, click Change.
    - In the Change HA Configuration dialog box, enter the “Declare Dead Time” The default is 15 seconds.
    - Click OK.

  - Configure management IP addresses
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click NSX Edges.
    - Double-click an NSX Edge.
    - Click the Manage tab and then click the Settings tab.
    - In the HA Configuration panel, click Change.
    - In the Change HA Configuration dialog box, choose the appropriate vNIC, and enter the Management IPs
    - Click OK.

- Modify an existing Edge High Availability deployment
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click an NSX Edge.
  - Click the Manage tab and then click the Settings tab.
  - In the HA Configuration panel, click Change.
  - In the Change HA Configuration dialog box, make changes as appropriate.
  - Click OK.

- Determine resource pool requirements for a given Edge High Availability configuration
  - For high availability, verify that the resource pool has enough capacity for both HA virtual machines to be deployed.

Tools

- NSX Administration Guide

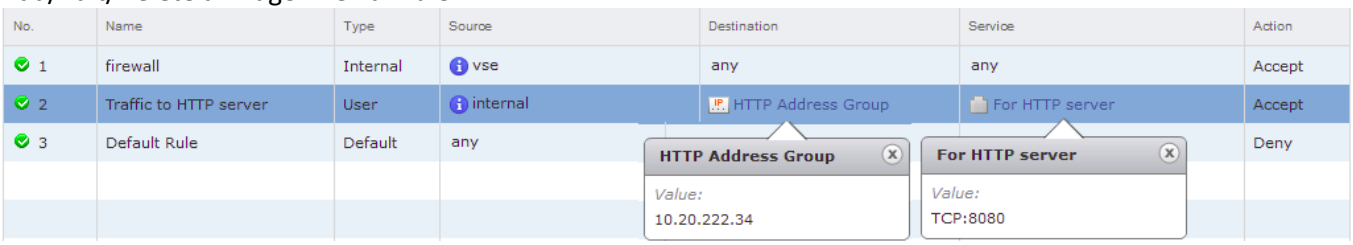
- NSX Manager
- vSphere Web Client

Section 7 – Configure and Administer Network Security

Objective 7.1 – Configure and Administer Logical Firewall Services

Knowledge

- Add/Edit/Delete an Edge Firewall rule



  - Add:
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click NSX Edges.
    - Double-click an NSX Edge.
    - Click the Manage tab and then click the Firewall tab.
    - Do one of the following.
      - To add a rule at a specific place in the firewall table
        - Select a rule.
        - In the No. column, click the Pencil icon and select Add Above or Add Below.
        - A new any any allow rule is added below the selected rule. If the system defined rule is the only rule in the firewall table, the new rule is added above the default rule.
      - To add a rule by copying a rule
        - Select a rule.
        - Click the Copy icon.
        - Select a rule.
        - In the No. column, click and select Paste Above or Paste Below.
      - To add a rule anywhere in the firewall table
        - Click the Add “+” icon.
        - A new any any allow rule is added below the selected rule. If the system defined rule is the only rule in the firewall table, the new rule is added above the default rule.
        - The new rule is enabled by default.

    - Point to the Name cell of the new rule and click [+]
    - Type a name for the new rule.
    - Point to the Source cell of the new rule and click [+] or [IP]
    - If you clicked [IP], type an IP address.
      - Select an object from the drop-down and then make the appropriate selections.
        If you select vNIC Group, and then select vse, the rule applies to traffic generated by the NSX Edge. If you select internal or external, the rule applies to traffic coming from any internal or uplink interface of the selected NSX Edge instance. The rule is automatically updated when you configure additional interfaces.
        If you select IP Sets, you can create a new IP address group. Once you create the new group, it is automatically added to the source column.

- Click OK

- Point to the Destination cell of the new rule and click [+] or [IP].
  - Select an object from the drop-down and then make the appropriate selections.
    If you select vNIC Group, and then select vse, the rule applies to traffic generated by the NSX Edge. If you select internal or external, the rule applies to traffic going to any internal or uplink interface of the selected NSX Edge instance. The rule is automatically updated when you configure additional interfaces.
    If you select IP Sets, you can create a new IP address group. Once you create the new group, it is automatically added to the source column. Click OK.

- Point to the Service cell of the new rule and click [+] or [∩]
  - If you clicked [+] , select a service. To create a new service or service group, click New. Once you create the new service, it is automatically added to the Service column.
  - If you clicked [∩] , select a protocol. You can specify the source port by clicking the arrow next to Advance options. VMware recommends that you avoid specifying the source port from release 5.1 onwards. Instead, you can create a service for a protocol-port combination.
    NOTE NSX Edge only supports services defined with L3 protocols.

- Point to the Action cell of the new rule and click [+]
  - Click Deny to block traffic from or to the specified source and destination.
  - Click Log to log all sessions matching this rule.
    Enabling logging can affect performance.
  - Type comments if required.
  - Click [>] next to Advance options.
  - To apply the rule to the translated IP address and services for a NAT rule, select Translated IP for Match on.
  - Click Enable Rule Direction and select Incoming or Outgoing. VMware does not recommend specifying the direction for firewall rules.
  - Click OK

- Click Publish Changes to push the new rule to the NSX Edge instance.

- Edit:
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click an NSX Edge.
  - Click the Monitor tab and then click the Firewall tab.
  - Select the rule to edit
    NOTE You cannot change an auto-generated rule or the default rule, except for changing the Action on the default rule.
  - Make the desired changes and click OK.
  - Click Publish Changes.

- Delete:
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click an NSX Edge.

        - Click the Monitor tab and then click the Firewall tab.
        - Select the rule to delete
          NOTE You cannot delete an auto-generated rule or the default rule.
        - Click Delete "X" and click OK.
        - Click Publish Changes.

- Configure Source/Destination/Service/Action rule components
    - Configure Source:
        - Point to the Source cell of the rule and click [+] or [IP]
        - If you clicked [IP], type an IP address.
            - Select an object from the drop-down and then make the appropriate selections.
              If you select vNIC Group, and then select vse, the rule applies to traffic generated by the NSX Edge. If you select internal or external, the rule applies to traffic coming from any internal or uplink interface of the selected NSX Edge instance. The rule is automatically updated when you configure additional interfaces.
              If you select IP Sets, you can create a new IP address group. Once you create the new group, it is automatically added to the source column.
            - Click OK

    - Configure Destination:
        - Point to the Destination cell of the rule and click [+] or [IP].
            - Select an object from the drop-down and then make the appropriate selections.
              If you select vNIC Group, and then select vse, the rule applies to traffic generated by the NSX Edge. If you select internal or external, the rule applies to traffic going to any internal or uplink interface of the selected NSX Edge instance. The rule is automatically updated when you configure additional interfaces.
              If you select IP Sets, you can create a new IP address group. Once you create the new group, it is automatically added to the source column.
            - Click OK.

    - Configure Service:
        - Point to the Service cell of the rule and click [+] or [∩]
            - If you clicked [+] , select a service. To create a new service or service group, click New. Once you create the new service, it is automatically added to the Service column.
            - If you clicked [∩] , select a protocol. You can specify the source port by clicking the arrow next to Advance options. VMware recommends that you avoid specifying the source port from release 5.1 onwards. Instead, you can create a service for a protocol-port combination.
              NOTE NSX Edge only supports services defined with L3 protocols.

    - Configure Action:
        - Point to the Action cell of the rule and click [+]
            - Click Deny to block traffic from or to the specified source and destination.
            - Click Log to log all sessions matching this rule.
              Enabling logging can affect performance.
            - Type comments if required.
            - Click [>] next to Advance options.

        - To apply the rule to the translated IP address and services for a NAT rule, select Translated IP for Match on.
        - Click Enable Rule Direction and select Incoming or Outgoing. VMware does not recommend specifying the direction for firewall rules.
        - Click OK

    - Click Publish Changes to push the updated rule to the NSX Edge instance.

- Change the order of an Edge Firewall rule
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click NSX Edges.
    - Double-click an NSX Edge.
    - Click the Monitor tab and then click the Firewall tab.
    - Select the rule for which you want to change the priority.
      NOTE You cannot change the priority of auto-generated rules or the default rule.
    - Click the "Move Up" or "Move Down" icon.
    - Click OK.
    - Click Publish Changes.

- Change the priority of an Edge Firewall rule
    - Changing the priority means the same thing as changing the order.

Tools
- NSX Administration Guide
- vSphere Web Client

Objective 7.2 – Configure Distributed Firewall Services

Knowledge
- Differentiate between Layer 2 and Layer 3 rules
    - Layer 2 rules are between VMs on the same logical switch, and are based on the contents of the Ethernet packet header rather than the IP packet header. Packets are filtered based on the MAC address, rather than the IP address.
      L2 rules are mapped to L2 OSI model: only MAC addresses can be used in the source and destination fields – and only L2 protocols can be used in the service fields (like ARP for instance).

    - Layer 3 rules are between IP addresses or IP address ranges. Packets are filtered on the IP header and potentially also the TCP or UDP header.
      L3/L4 rules are mapped to L3/L4 OSI model: policy rules can be written using IP addresses and TCP/UDP ports.
      It is important to remember that L2 rules are always enforced before L3/L4 rules. As a concrete example, if the L2 default policy rule is modified to 'block', then all L3/L4 traffic will be blocked as well by DFW (no more ping work for example)

- Differentiate between entity-based and identity-based rules
    - Entity based rules are based on VMware vCenter objects like datacenters and clusters and virtual machine names; network constructs like IP or IPSet addresses, VLAN (DVS port-

groups), VXLAN (logical switches), security groups.

- Identity based rules are based on user or group identity from Active Directory. Administrators can enforce access control based on the user's group membership as defined in the enterprise Active Directory. Here are some scenarios where identity-based firewall rules can be used:
  - User accessing virtual applications using a laptop or mobile device where AD is used for user authentication
  - User accessing virtual applications using VDI infrastructure where the virtual machines are Microsoft Windows based

- Identify firewall rule entities
  - VMware vCenter objects like datacenters and clusters and virtual machine names;
  - Network constructs like IP or IPSet addresses, VLAN (DVS port-groups), VXLAN (logical switches), security groups.

- Explain rule processing order
  - L2 rules are always enforced before L3/L4 rules
  - User-defined pre rules have the highest priority and are enforced in top-to-bottom ordering with a per-virtual NIC level precedence.
  - Next Auto-plumbed rules.
  - Then Local rules defined at an NSX Edge level.
  - Then Service Composer rules - a separate section for each policy. You cannot edit these rules in the Firewall table, but you can add rules at the top of a security policy firewall rules section. If you do so, you must re-synchronize the rules in Service Composer. For more information, see Service Composer.
  - Finally Default Distributed Firewall rule

- Explain rule segregation
  - You can add a section to segregate firewall rules. For example, you might want to have the rules for sales and engineering departments in separate sections.

- Add/Delete a Distributed Firewall rule
  - Add:
    - In the vSphere Web Client, navigate to Networking & Security > Firewall.
    - Ensure that you are in the General tab to add an L3 rule. Click the Ethernet tab to add an L2 rule.
    - In the section in which you add a rule, click Add rule (add icon) icon.
    - A new any any allow rule is added at the top of the section. If the system-defined rule is the only rule in the section, the new rule is added above the default rule.
    - If you want to add a rule at a specific place in a section, select a rule. In the No. column, click edit and select Add Above or Add Below.
    - Point to the Name cell of the new rule and click [+]
    - Type a name for the new rule.
    - Point to the Source cell of the new rule and click [+] or [IP]
    - If you clicked [IP], select the IP address format (IPv4/v6) and type an IP address.
    - To specify source as an object other than a specific IP address.
      - In View, select a container from which the communication originated. Objects for the selected container are displayed.

- Select one or more objects and click add.
  You can create a new security group or IPSet. Once you create the new object, it is added to the source column by default. For information on creating a new security group or IPSet, see Network and Security Objects.
- To specify a source port, click Advance options and type the port number or range.
- Select Negate Source to exclude this source port from the rule.
  If Negate Source is selected, the rule applied to traffic coming from all sources except for the source you specified in the previous step.
  If Negate Source is not selected, the rule applies to traffic coming from the source you specified in the previous step.
- Click OK.

- Point to the Destination cell of the new rule and click [+] or [IP].
  - If you clicked [IP], select the IP address format (IPv4/v6) and type an IP address.
  - To specify destination as an object other than a specific IP address.
    - In View, select a container which the communication is targeting
      Objects for the selected container are displayed.
    - Select one or more objects and click add.
      You can create a new security group or IPSet. Once you create the new object, it is added to the Destination column by default. For information on creating a new security group or IPSet, see Network and Security Objects.
    - To specify a destination port, click Advance options and type the port number or range.
    - Select Negate Destination to exclude this destination port from the rule.
      If Negate Destination is selected, the rule applied to traffic going to all destinations except the destination you specified in the previous step.
      If Negate Destination is not selected, the rule applies to traffic going to the destination you specified in the previous step.
  - Click OK.

- Point to the Service cell of the new rule and click [+] or [∩]
  - If you clicked [+] , select a service. To create a new service or service group, click New. Once you create the new service, it is automatically added to the Service column.
    Click OK
  - If you clicked [∩] , select the service protocol.
    Distributed Firewall supports ALG (Application Level Gateway) for the following protocols: FTP, CIFS, ORACLE TNS, MS-RPC, and SUN-RPC.
    Type the port number and click OK

- Point to the Action cell of the new rule and click [+]
  Make appropriate selections as described in the list below and click OK.
  - Allow
    Allows traffic from or to the specified source(s), destination(s), and service(s).
  - Block
    Blocks traffic from or to the specified source(s), destination(s), and service(s).
  - Reject
    Sends reject message for unaccepted packets.
    RST packets are sent for TCP connections.

ICMP messages with administratively prohibited code are sent for UDP, ICMP, and other IP connections.
- Log
  Logs all sessions matching this rule. Enabling logging can affect performance.
- Do not log
  Does not log sessions.

- Click Publish Changes to push the new rule to the NSX Edge instance.

- Configure Source/Destination/Service/Action rule components
  - Point to the Source cell of the rule and click [+] or [IP]
    - If you clicked [IP], select the IP address format (IPv4/v6) and type an IP address.
    - To specify source as an object other than a specific IP address.
      - In View, select a container from which the communication originated.
        Objects for the selected container are displayed.
      - Select one or more objects and click Add.
        You can create a new security group or IPSet. Once you create the new object, it is added to the source column by default. For information on creating a new security group or IPSet, see Network and Security Objects.
      - To specify a source port, click Advance options and type the port number or range.
      - Select Negate Source to exclude this source port from the rule.
        If Negate Source is selected, the rule applied to traffic coming from all sources except for the source you specified in the previous step.
        If Negate Source is not selected, the rule applies to traffic coming from the source you specified in the previous step.
      - Click OK.

  - Point to the Destination cell of the rule and click [+] or [IP].
    - If you clicked [IP], select the IP address format (IPv4/v6) and type an IP address.
    - To specify destination as an object other than a specific IP address.
      - In View, select a container which the communication is targeting
        Objects for the selected container are displayed.
      - Select one or more objects and click add.
        You can create a new security group or IPSet. Once you create the new object, it is added to the Destination column by default. For information on creating a new security group or IPSet, see Network and Security Objects.
      - To specify a destination port, click Advance options and type the port number or range.
      - Select Negate Destination to exclude this destination port from the rule.
        If Negate Destination is selected, the rule applied to traffic going to all destinations except the destination you specified in the previous step.
        If Negate Destination is not selected, the rule applies to traffic going to the destination you specified in the previous step.
    - Click OK.

  - Point to the Service cell of the rule and click [+] or [∩]

        - If you clicked [+] , select a service. To create a new service or service group, click New. Once you create the new service, it is automatically added to the Service column.
          Click OK
        - If you clicked [∩] , select the service protocol.
          Distributed Firewall supports ALG (Application Level Gateway) for the following protocols: FTP, CIFS, ORACLE TNS, MS-RPC, and SUN-RPC.
          Type the port number and click OK

    - Point to the Action cell of the rule and click [+]
      Make appropriate selections as described in the list below and click OK.
        - Allow
          Allows traffic from or to the specified source(s), destination(s), and service(s).
        - Block
          Blocks traffic from or to the specified source(s), destination(s), and service(s).
        - Reject
          Sends reject message for unaccepted packets.
          RST packets are sent for TCP connections.
          ICMP messages with administratively prohibited code are sent for UDP, ICMP, and other IP connections.
        - Log
          Logs all sessions matching this rule. Enabling logging can affect performance.
        - Do not log
          Does not log sessions.

- Change the order of a Distributed Firewall rule
    - In the vSphere Web Client, navigate to Networking & Security > Firewall.
    - Select the rule that you want to move.
    - Click the Move rule up or Move rule down icon.
    - Click Publish Changes.

- Add/Merge/Delete a Distributed Firewall rule section
    - Add:
        - In the vSphere Web Client, navigate to Networking & Security > Firewall.
        - Ensure that you are in the General tab to add a section for L3 rules. Click the Ethernet tab to add a section for L2 rules.
        - Click the Add Section icon.
        - Type a name for the section and specify the position for the new section. Section names must be unique within NSX Manager.
        - Click OK.
    - Merge:
        - In the vSphere Web Client, navigate to Networking & Security > Firewall.
        - For the section you want to merge, click the Merge icon and specify whether you want to merge this section with the section above or below.
        - Rules from both sections are merged. The new section keeps the name of the section with which the other section is merged.
        - Click Publish Changes.
    - Delete:
        - In the vSphere Web Client, navigate to Networking & Security > Firewall.

        - Ensure that you are in the General tab to delete a section for L3 rules. Click the Ethernet tab to delete a section for L2 rules.
        - Click the Delete section (X) icon for the section you want to delete.
        - Click OK and then click Publish Changes.
          The section, as well as all rules in that section, is deleted.

- Determine publishing requirements for rules in a given NSX implementation
    - The Applied To column can be used to define the scope of rule publishing
      User can decide to publish policy rule to all clusters where DFW was enabled or restrict publication to a specific object as listed below:
        - **Cluster**
          Selecting Cluster will push the rule down to all VM/vNIC on the ESXi cluster.
        - **Datacenter**
          Selecting Datacenter will push the rule down to all VM/vNIC on the Datacenter.
        - **Distributed Port Group**
          Selecting DVS port-group will push the rule down to all VM/vNIC on the Datacenter.
        - **Host**
          Selecting Host will push the rule down to all VM/vNIC on the ESXi host.
        - **Legacy port group**
          Selecting Legacy port group will push the rule down to all VM/vNIC on the VSS port-group.
        - **Logical Switch**
          Selecting Logical Switch will push the rule down to all VM/vNIC connected on this Logical Switch (or VXLAN) segment .
        - **Security Group**
          Selecting Security Group will push the rule down to all VM/vNIC defined within the Security Group.
        - **Virtual Machine**
          Selecting Virtual Machine will push the rule down to all vNIC of this VM.
        - **vNIC**
          Selecting vNIC will push the rule down to this particular vNIC instance.

- Import/Export Distributed Firewall Configuration
    - Import
        - Log in to the vSphere Web Client.
        - Click Networking & Security and then click Firewall.
        - Click the Firewall tab.
        - Click the Saved Configurations tab.
        - Click the Import configuration icon.
        - Click Browse and select the file containing the configuration that you want to import.
          Rules are imported based on the rule names. During the import, Firewall ensures that each object referenced in the rule exists in your environment. If an object is not found, the rule is marked as invalid.
          If a rule referenced a dynamic security group, the dynamic security group is created in NSX Manager during the import.

    - Export
        - Log in to the vSphere Web Client.
        - Click Networking & Security and then click Firewall.
        - Click the Export configuration icon.

        - To save the firewall configuration as an XML file, click Download.
        - Select the directory where you want to save the file and click Save.
          Your firewall configuration (both L2 and L3) is saved in the specified directory.

- Load Distributed Firewall configuration
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click Firewall.
    - Ensure that you are in the General tab to load an L3 firewall configuration. Click the Ethernet tab to load an L2 firewall configuration.
    - Click the Load configuration icon.
    - Select the configuration to load and click OK.
      The current configuration is replaced by the selected configuration.

- Determine need for excluding virtual machines from distributed firewall protection
    - You can exclude a set of virtual machines from firewall protection. If a virtual machine has multiple vNICs, all of them are excluded from protection.
    - NSX Manager and service virtual machines are automatically excluded from firewall protection. In addition, you should exclude the vCenter server and partner service virtual machines to allow traffic to flow freely.
    - Excluding virtual machines from firewall protection is useful for instances where vCenter Server resides in the same cluster where firewall is being utilized. After enabling this feature, no traffic from excluded virtual machines will go through the Firewall.
      NOTE vCenter Server can be moved to a cluster that is protected by firewall, but it must already exist in the exclusion list to avoid any connection issues.

- Configure and manage SpoofGuard
    - Create a SpoofGuard policy
        - Log in to the vSphere Web Client.
        - Click Networking & Security and then click SpoofGuard.
        - Click the Add icon.
        - Type a name for the policy.
        - Select Enabled or Disabled to indicate whether the policy is enabled.
        - For Operation Mode, select one of the following:
            - **Automatically Trust IP Assignments on Their First Use**
              Select this option to trust all IP assignments upon initial registration with the NSX Manager.
            - **Manually Inspect and Approve All IP Assignments Before Use**
              Select this option to require manual approval of all IP addresses. All traffic to and from unapproved IP addresses is blocked.
        - Click “Allow local address as valid address in this namespace” to allow local IP addresses in your setup.
          When you power on a virtual machine but it is unable to connect to the DHCP server, a local IP address is assigned to it. This local IP address is considered valid only if the SpoofGuard mode is set to Allow local address as valid address in this namespace. Otherwise, the local IP address is ignored.
        - Click Next.
        - To specify the scope for the policy, click Add and select the networks, distributed port groups, or
        - logical switches that this policy should apply to.
          A port group or logical switch can belong to only one SpoofGuard policy.

        - Click OK and then click Finish.

- Approve IP addresses
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click SpoofGuard.
    - Select a policy.
      Policy details are displayed below the policy table.
    - In View, click one of the option links.
        - **Active Virtual NICs**
          List of all validated IP addresses
        - **Active Virtual NICs Since Last Published**
          List of IP addresses that have been validated since the policy was last updated
        - **Virtual NICs IP Required Approval**
          IP address changes that require approval before traffic can flow to or from these virtual machines
        - **Virtual NICs with Duplicate IP**
          IP addresses that are duplicates of an existing assigned IP address within the selected datacenter
        - **Inactive Virtual NICs**
          List of IP addresses where the current IP address does not match the published IP address
        - **Unpublished Virtual NICs IP**
          List of virtual machines for which you have edited the IP address assignment but have not yet published
    - Do one of the following.
        - To approve a single IP address, click Approve next to the IP address.
        - To approve multiple IP addresses, select the appropriate vNICs and then click Approve Detected IP(s).

- Edit/Clear IP addresses
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click SpoofGuard.
    - Select a policy.
      Policy details are displayed below the policy table.
    - In View, click one of the option links.
        - **Active Virtual NICs**
          List of all validated IP addresses
        - **Active Virtual NICs Since Last Published**
          List of IP addresses that have been validated since the policy was last updated
        - **Virtual NICs IP Required Approval**
          IP address changes that require approval before traffic can flow to or from these virtual machines
        - **Virtual NICs with Duplicate IP**
          IP addresses that are duplicates of an existing assigned IP address within the selected datacenter

- **Inactive Virtual NICs**
  List of IP addresses where the current IP address does not match the published IP address
- **Unpublished Virtual NICs**
  IP List of virtual machines for which you have edited the IP address assignment but have not yet published

- To Edit, for the appropriate vNIC, click the Edit icon and make appropriate changes.
- To clear a single IP address, click Clear next to the IP address.
- To clear multiple IP addresses, select the appropriate vNICs and then click "Clear Approved IP(s)".
- Click OK.

Tools

- NSX Administration Guide
- vSphere Web Client

Objective 7.3 – Configure and Manage Service Composer

Knowledge

- Identify assets that can be used with a Security Group

  Security groups may be static (including specific virtual machines) or dynamic where membership may be defined in one or more of the following ways:
  - vCenter containers (clusters, port groups, or datacenters)
  - Security tags, IPset, MACset, or even other security groups. For example, you may include a criteria to add all members tagged with the specified security tag (such as AntiVirus.virusFound) to the security group.
  - Directory Groups (if NSX Manager is registered with Active Directory)
  - Regular expressions such as virtual machines with name VM1

    Note that security group membership changes constantly. For example, a virtual machine tagged with the AntiVirus.virusFound tag is moved into the Quarantine security group. When the virus is cleaned and this tag is removed from the virtual machine, it again moves out of the Quarantine security group

- Identify services contained in a Security Policy

  A security policy is a collection of the following service configurations.
  - **Firewall rules**
    Rules that define the traffic to be allowed to, from, or within the security group.
    Applies to vNIC
  - **Endpoint service**
    Data Security or third party solution provider services such as anti-virus or vulnerability management services.
    Applies to virtual machines
  - **Network introspection services**
    Services that monitor your network such as IPS.

Applies to virtual machines

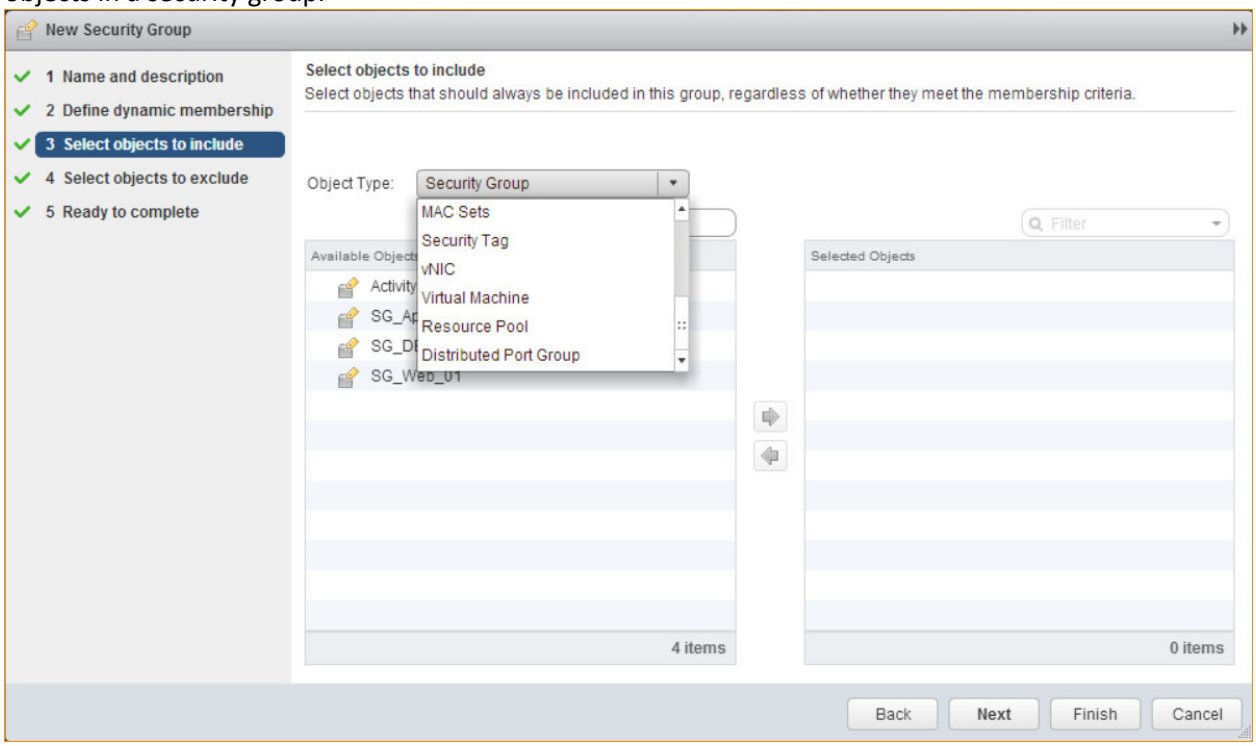
- Identify common Service Composer use cases
  - Orchestrating security between multiple services
  - Deploying security services on demand
  - Quarantining Infected VMs
  - Quarantining vulnerable VMs

- Differentiate Security Groups and Security Policies
  A Security Group is **what** you want to protect, a Security Policy is **how** you want to protect it.

- Create/Edit a Security Group in Service Composer
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click Service Composer.
  - Click the Security Groups tab and then click the Add Security Group icon.
  - Type a name and description for the security group and click Next.
  - On the Dynamic Membership page, define the criteria that an object must meet for it to be added to the security group you are creating.
    For example, you may include a criteria to add all members tagged with the specified security tag (such as AntiVirus.virusFound) to the security group. Security tags are case sensitive.
    NOTE If you define a security group by virtual machines that have a certain security tag applied to them, you can create a dynamic or conditional workflow. The moment the tag is applied to a virtual machine, the virtual machine is automatically added to that security group.
    Or you can add all virtual machines containing the name W2008 AND virtual machines that are in the logical switch global_wire to the security group.

  - Click Next.
  - On the Select objects to include page, select the tab for the resource you want to add and select one or more resource to add to the security group. You can include the following

objects in a security group.



- Other security groups to nest within the security group you are creating.
- Cluster
- Virtual wire
- Network
- Virtual App
- Datacenter
- IP sets
- AD groups
  NOTE The AD configuration for NSX security groups is different from the AD configuration for vSphere SSO. NSX AD group configuration is for end users accessing guest virtual machines while vSphere SSO is for administrators using vSphere and NSX.
- MAC Sets
- Security tag
- vNIC
- Virtual Machine
- Resource Pool
- Distributed Virtual Port Group
  The objects selected here are always included in the security group regardless of whether or not they match the dynamic criteria.
  When you add a resource to a security group, all associated resources are automatically added. For example, when you select a virtual machine, the associated vNIC is automatically added to the security group.

- Click Next and select the objects that you want to exclude from the security group.
  The objects selected here are always excluded from the security group even if they match the dynamic criteria or are selected in the include list.

- Click Finish.

  Membership of a security group is determined as follows:
  {Expression result (derived from step 4) + Inclusions (specified in step 6} - Exclusion (specified in step 7) which means that inclusion items are first added to the expression result. Exclusion items are then subtracted from the combined result.

- Create/Edit/Delete a Security Policy
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click Service Composer.
  - Click the Security Policies tab.
  - Click the Create Security Policy icon.
  - In the Add Security Policy dialog box, type a name for the security policy.
  - Type a description for the security policy.
    NSX assigns a default weight (highest weight +1000) to the policy. FoVDSr example, if the highest weight amongst the existing policy is 1200, the new policy is assigned a weight of 2200.
    Security policies are applied according to their weight - a policy with the higher weight has precedence over a policy with a lower weight.

  - Select Inherit security policy from specified policy if you want the policy that you are creating to receive services from another security policy. Select the parent policy.
    All services from the parent policy are inherited by the new policy.

  - Click Next.
  - In the Endpoint Services page, click the Add Endpoint Service "+" icon.
    (This is "Guest Introspection Services in NSX 6.1)
    - In the Add Endpoint Service dialog box, type a name and description for the service.
    - Specify whether you want to apply the service or block it.
      When you inherit a security policy, you may choose to block a service from the parent policy.
    - Select the type of service.
      If you select Data Security, you must have a data security policy in place. See Chapter 12, "Data Security," on page 139.
    - If you chose to apply the Endpoint service, select the service name and service configuration.
      Service configuration refers to vendor templates. These configurations are defined in third party consoles and are registered along with partner services. Tagging and untagging of virtual machines depends on the service configuration selected for the security policy.
    - In State, specify whether you want to enable the selected Endpoint service or disable it.
      You can add Endpoint services as placeholders for services to be enabled at a later time. This is especially useful for cases where services need to be applied on-demand (for example, new applications).
    - Select whether the Endpoint service is to be enforced (i.e. it cannot be overridden).
      If you enforce an Endpoint service in a security policy, other policies that inherit this security policy would require that this policy be applied before the other child policies. If this service is not enforced, an inheritance selection would add the parent policy after the child policies are applied.

- Click OK.

  You can add additional Endpoint services by following the above steps. You can manage the Endpoint services through the icons above the service table.
  You can export or copy the services on this page by clicking the icon on the bottom right side of the Endpoint Services page.

- Click Next.
- On the Firewall page, click the Add Firewall Rule "+" icon.
  Here, you are defining firewall rules for the security groups(s) that this security policy will be applied to.
  - Type a name and description for the firewall rule you are adding.
  - Select Allow or Block to indicate whether the rule needs to allow or block traffic to the selected destination.
  - Select the source for the rule. By default, the rule applies to traffic coming from the security groups to which this policy gets applied to. To change the default source, click Change and select the appropriate security groups.
  - Select the destination for the rule.

    NOTE Either the Source or Destination (or both) must be security groups to which this policy gets applied to.

    Say you create a rule with the default Source, specify the Destination as Payroll, and select Negate Destination. You then apply this security policy to security group Engineering. This would result in Engineering being able to access everything except for the Payroll server.

  - Select the services and/or service groups to which the rule applies to.
  - Select Enabled or Disabled to specify the rule state.
  - Select Log to log sessions matching this rule.
    Enabling logging may affect performance.
  - Click OK.

    You can add additional firewall rules by following the above steps. You can manage the firewall rules through the icons above the firewall table.
    You can export or copy the rules on this page by clicking the export icon on the bottom right side of the Firewall page.

    The firewall rules you add here are displayed on the Firewall table. VMware recommends that you do not edit Service Composer rules in the firewall table. If you must do so for an emergency troubleshooting, you must re-synchronize Service Composer rules with firewall rules by selecting Synchronize Firewall Rules from the Actions menu in the Security Policies tab.

- Click Next.
  The Network Introspection Services page displays NetX services that you have integrated with your VMware virtual environment.

- Click the Add Network Introspection Service "+ icon.

- In the Add Network Introspection Service dialog box, type a name and description for the service you are adding.
- Select whether or not to redirect to service.
- Select the service name and profile.
- Select the source and destination
- Select the protocol.
  You can specify the protocol type, source port advanced options, and destination port.
- Select whether to enable or disable the service.
- Select Log to log sessions matching this rule.
- Click OK.

  You can add additional network introspection services by following the above steps.
  You can manage the network introspection services through the icons above the service table.
  You can export or copy the services on this page by clicking the icon on the bottom right side of the Network Introspection Service page.

  - Click Finish.

    The security policy is added to the policies table. You can click the policy name and select the appropriate tab to view a summary of the services associated with the policy, view service errors, or edit a service.

- Map a Security Policy to a Security Group
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click Service Composer.
  - Click the Security Policy tab.
  - Select a security policy and click the Apply Security Policy icon.
  - Select the security group that you want to apply the policy to.

    If you select a security group defined by virtual machines that have a certain security tag applied to them, you can create a dynamic or conditional workflow. The moment the tag is applied to a virtual machine, the virtual machine is automatically added to that security group.

  - Click the Preview Service Status icon to see the services that cannot be applied to the selected security group and the reason for the failure.

    For example, the security group may include a virtual machine that belongs to a cluster on which one of the policy services has not been installed. You must install that service on the appropriate cluster for the security policy to work as intended.

  - Click OK.

- Add/Edit/Delete a Security Tag
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Managers.
  - Click an NSX Manager in the Name column and then click the Manage tab.
  - Click the Security Tags tab.

- Add:
  - Click the New Security Tag “+” icon.
  - Type a name and description for the tag and click OK.
- Edit:
  - Select a security tag and click the Edit Security Tag (Pencil) icon.
  - Make the appropriate changes and click OK.
- Delete:
  - Select a security tag and click the Delete Security Tag “X” icon.

- Assign and view a Security Tag
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Managers.
  - Click an NSX Manager in the Name column and then click the Manage tab.
  - Click the Security Tags tab.
  - Assign:
    - Select a security tag and click the Assign Security Tag “+” icon.
    - Select one or more virtual machines and click OK.
  - View:
    - A list of tags applied in your environment is displayed along with details about the virtual machines to which those tags have been applied. Note down the exact tag name if you plan on adding a security group to include virtual machines with a specific tag.
    - Click the number in the VM Count column to view the virtual machines to which that tag in that row has been applied.

Tools

- NSX Administration Guide
- vSphere Web Client

Section 8 – Perform Operations Tasks in a VMware NSX Environment

Objective 8.1 – Configure Roles, Permissions, and Scopes

Knowledge

- Identify default roles
  - **Enterprise Administrator**
    NSX operations and security.
  - **NSX Administrator**
    NSX operations only: for example, install virtual appliances, configure port groups.
  - **Security Administrator**
    NSX security only: for example, define data security policies, create port groups, create reports for NSX modules.
  - **Auditor**
    Read only.

    There are also two scopes available:
  - **No restriction**
    Access to entire NSX system.
  - **Limit access scope**
    Access to a specified Edge.

- Explain Single Sign-On (SSO) integration
  - NSX supports Single Sign On (SSO), which enables NSX to authenticate users from other identity services such as Active Directory, NIS, and LDAP.
    User management in the vSphere Web Client is separate from user management in the CLI of any NSX component.
  - Integrating the single sign on (SSO) service with NSX improves the security of user authentication for vCenter users and enables NSX to authenticate users from other identity services such as AD, NIS, and LDAP.
    With SSO, NSX supports authentication using authenticated Security Assertion Markup Language (SAML) tokens from a trusted source via REST API calls. NSX Manager can also acquire authentication SAML tokens for use with other VMware solutions.

- Assign a role to a vCenter Server user
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Managers.
  - Click an NSX Manager in the Name column and then click the Manage tab.
  - Click Users.
  - Click Add.
    The Assign Role window opens.
  - Click Specify a vCenter user or Specify a vCenter group.
  - Type the vCenter User or Group name for the user.
    NOTE If the vCenter user is from a domain (such as a SSO user), then you must enter a fully qualified windows domain path. This will allow the default NSX Manager user (admin) as well as the SSO default user (admin) to login to NSX Manager. This user name is for login to the NSX Manager user interface, and cannot be used to access NSX Manager CLIs.

- Click Next.
- Select the role for the user and click Next. For more information on the available roles, see "Managing User Rights," on page 20.
- Select the scope for the user and click Finish.
  The user account appears in the Users table.

- Assign objects to a user
  After you create users and groups and define roles, you must assign the users and groups and their roles to the relevant inventory objects. You can assign the same permissions at one time on multiple objects by moving the objects to a folder and setting the permissions on the folder.

  - Browse to the object in the vSphere Web Client object navigator.
  - Click the Manage tab and select Permissions.
  - Click Add Permission.
  - Click Add.
  - Identify the user or group to assign to this role.
    - Select the domain where the user or group is located from the Domain drop-down menu.
    - Type a name in the Search box or select a name from the list.
      The system searches user names, group names, and descriptions.
    - Select the user and click Add.
      The name is added to either the Users or Groups list.
    - (Optional) Click Check Names to verify that the user or group exists in the database.
    - Click OK.
  - Select a role from the Assigned Role drop-down menu.
    The roles that are assigned to the object appear in the menu. The privileges contained in the role are listed in the section below the role title.
  - (Optional) Deselect the Propagate to Child Objects check box.
    The role is applied only to the selected object and does not propagate to the child objects.
  - Verify that the users and groups are assigned to the appropriate permissions and click OK.
    The server adds the permission to the list of permissions for the object.
    The list of permissions references all users and groups that have roles assigned to the object and indicates where in the vCenter Server hierarchy the role is assigned.

- Configure SSO
  - Log in to the NSX Manager virtual appliance.
  - Under Appliance Management, click Manage Settings.
  - Click NSX Management Service.
  - Click Edit next to Lookup Service.
  - Type the name or IP address of the host that has the lookup service.
  - Change the port number if required. The default port is 7444.
    The Lookup Service URL is displayed based on the specified host and port.
  - Type the vCenter administrator user name and password (for example, administrator@vsphere.local).
    This enables NSX Manager to register itself with the Security Token Service server.
  - Click OK.

    Confirm that the Lookup Service status is Connected.

- Enable/Disable a user account

  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Managers.
  - Click an NSX Manager in the Name column and then click the Manage tab.
  - Click Users.
  - Select a user account.
  - Click the Enable or Disable icon.

- Edit/Delete a user account
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Managers.
  - Click an NSX Manager in the Name column and then click the Manage tab.
  - Click Users.
  - Edit:
    - Select the user you want to edit.
    - Click Edit.
    - Make changes as necessary.
    - Click Finish to save your changes.
  - Delete:
    - Select a user account.
    - Click Delete.
    - Click OK to confirm deletion.
      If you delete a vCenter user account, only the role assignment for NSX Manager is deleted. The user account on vCenter is not deleted.

Tools
- NSX Administration Guide
- vSphere Web Client

Objective 8.2 – Describe NSX Automation

Knowledge
- Identify API-only functionality
  - Integration with Cloud Management Platforms
  - Updating the MoId of the resource pool, datastore, or dvPortGroup using a REST API call, when an NSX Edge needs to be redeployed and one of the original resource pool, datastore or dvPortGroup is no longer valid.

- Explain how REST APIs work
  - REST, an acronym for REpresentational State Transfer, is a term that has been widely employed to describe an architectural style characteristic of programs that rely on the inherent properties of hypermedia to create and modify the state of an object that is accessible at a URL.

  - Once a URL of such an object is known to a client, the client can use an HTTP GET request to discover the properties of the object. These properties are typically communicated in a structured document with an HTTP Content-Type of XML that provides a representation of the state of the object. In a RESTful workflow, documents (representations of object state) are passed back and forth (transferred) between a client and a service with the explicit

assumption that neither party need know anything about an entity other than what is presented in a single request or response.
The URLs at which these documents are available are often "sticky," in that they persist beyond the lifetime of the request or response that includes them. The other content of the documents is nominally valid until the expiration date noted in the HTTP Expires header.

- Describe how to use the NSX API in a supported browser
  - To use the REST API in Firefox
    - Locate the RESTClient Mozilla add-on, and add it to Firefox.
    - Click Tools > REST Client to start the add-on.
    - Click Login and enter the NSX login credentials, which then appear encoded in the Request Header.
    - Select a method such as GET, POST, or PUT, and type the URL of a REST API. You might be asked to accept or ignore the lack of SSL certificate. Click Send.
      Response Header, Response Body, and Rendered HTML appear in the bottom window.

  - To use the REST API in Chrome
    - Search the Web to find the Simple REST Client, and add it to Chrome.
    - Click its globe-like icon to start it in a tab.
    - The Simple REST Client provides no certificate-checking interface, so use another Chrome tab to accept or ignore the lack of SSL certificate.
    - Type the URL of a REST API, and select a method such as GET, POST, or PUT.
    - In the Headers field, type the basic authorization line, as in the Important note above. Click Send.
      Status, Headers, and Data appear in the Response window.

- Identify port requirements for the NSX API
  - The NSX Manager requires port 443/TCP for REST API requests.

- Describe common use cases for VMware NSX API
  - Integration with Cloud Management Platforms:
    - Creating new Logical Switches
    - Creating new Logical Routers
    - Attaching VMs to Logical Switches
    - Configuring Load Balancers
    - Updating Firewall rules

- Explain how to access the VMware NSX API
  - You have several choices for programming the NSX REST API: using Firefox, Chrome, or cURL. To make XML responses more legible, you can copy and paste them into an XML friendly editor such as xmlcopyeditor or pspad.

- Modify an existing API workflow
  - I'm not really sure what this is getting at. There's nothing in the vSphere API Guide about modifying workflows – it's more of a reference guide for the API options.

    The closest thing I've found on the web is this posting http://virtuallygone.wordpress.com/2014/03/27/automating-firewall-rule-creation-in-nsx-with-vco-and-vcac-part-one-rest-host-configuration-in-vco/ on creating an NSX API

Workflow, which I guess you could do, and then modify it.

Tools

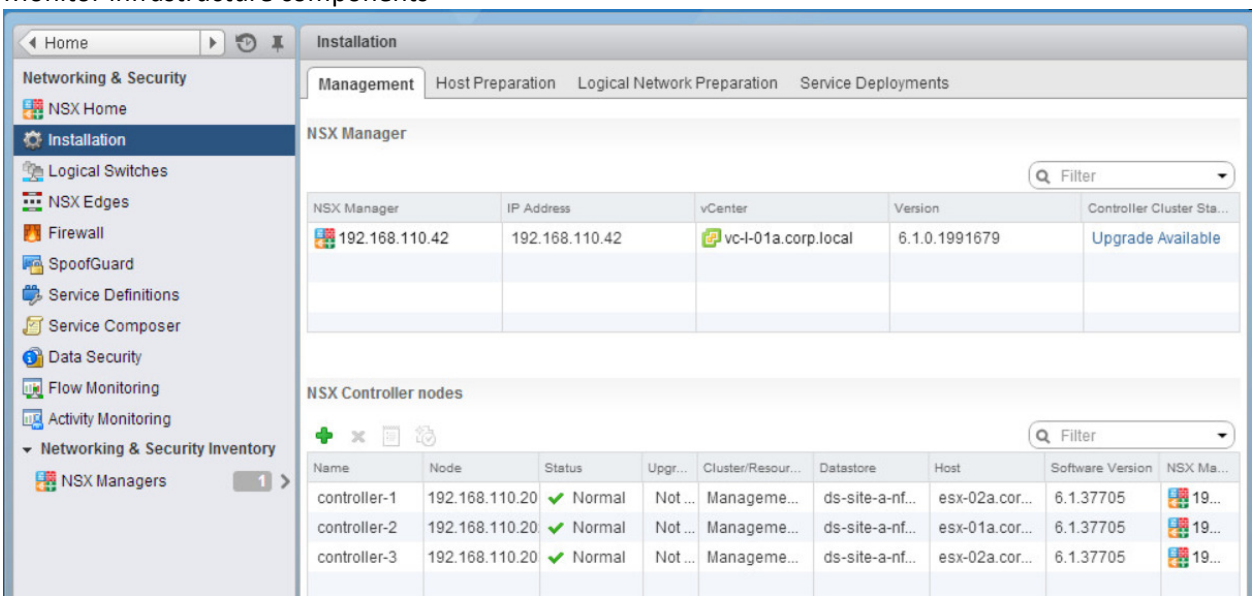
- NSX vSphere API Guide
- NSX API

Objective 8.3 – Monitor a VMware NSX Implementation

Knowledge

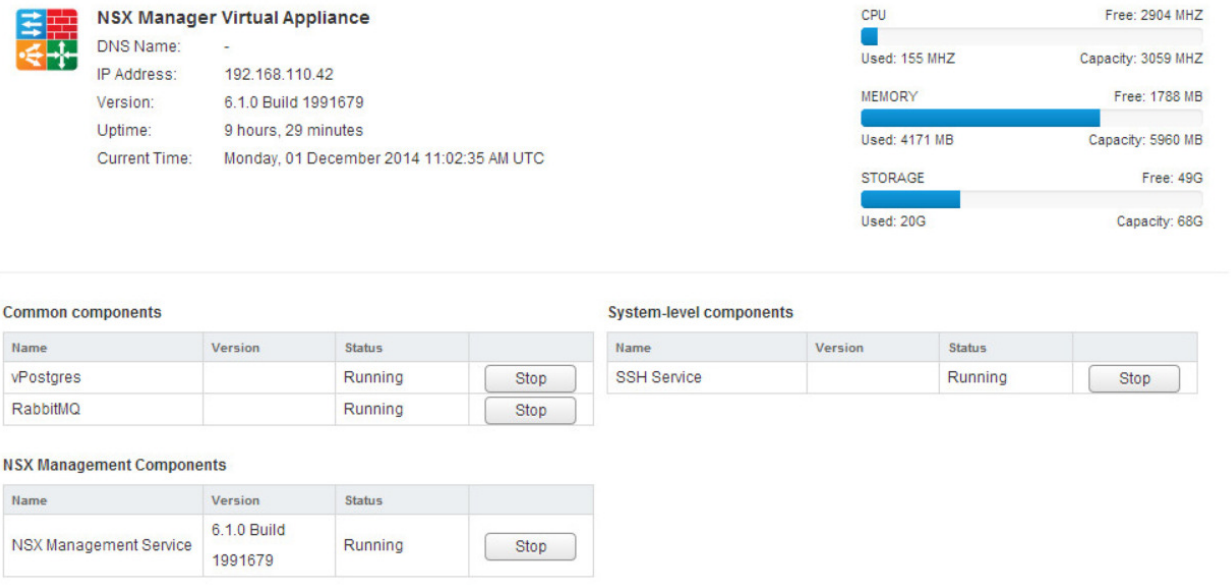
- Identify available monitoring methods (UI, CLI, API, etc.)
  - UI
    - Web Client
      - High level view of the status of vSphere and NSX components.
    - Flow Monitoring
      - Flow Monitoring is a traffic analysis tool that provides a detailed view of the traffic to and from protected virtual machines. When flow monitoring is enabled, its output defines which machines are exchanging data and over which application. This data includes the number of sessions and packets transmitted per session.
        Session details include sources, destinations, applications, and ports being used. Session details can be used to create firewall allow or block rules.
    - Activity Monitoring
      - Activity Monitoring provides visibility into your virtual network to ensure that security policies at your organization are being enforced correctly.
        A Security policy may mandate who is allowed access to what applications. The Cloud administrator can generate Activity Monitoring reports to see if the IP based firewall rule that they set is doing the intended work. By providing user and application level detail, Activity Monitoring translates high level security policies to low level IP address and network based implementation.
  - CLI
    - Used for NSX Manager, Controllers, Edges & Hosts
      - Manager is mainly for config rather than monitoring
      - Controllers can show bridges, instances, interfaces, routers, stats and status
      - Edges can show firewall flows, routing protocol details, VPN details, loadbalancer details, service monitors, and general status.
  - API
    - The NSX API can be used to enable/disable Activity Monitoring Data Collection, and query user/inbound/outbound/VM/AD Group activity.
  - Syslog
    - All NSX components can be configured to send logs to a Syslog server.

- Monitor infrastructure components

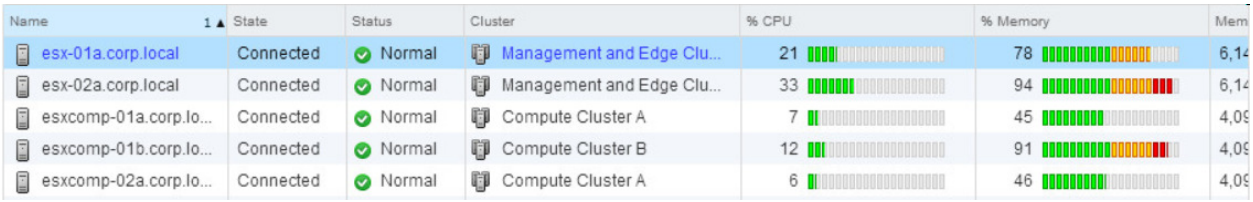


  - Control Cluster Health
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click Installation
    - NSX Controller nodes are shown, including Software Version and health Status.

  - Manager Health
    - Log in to the NSX Manager Web Interface



  - Hypervisor Health
    - Log in to the vSphere Web Client.
    - Click Hosts & Clusters, then Related Objects, and Hosts.



Name	State	Status	Cluster	% CPU	% Memory	Mem
esx-01a.corp.local	Connected	Normal	Management and Edge Clu...	21	78	6,14
esx-02a.corp.local	Connected	Normal	Management and Edge Clu...	33	94	6,14
esxcomp-01a.corp.lo...	Connected	Normal	Compute Cluster A	7	45	4,09
esxcomp-01b.corp.lo...	Connected	Normal	Compute Cluster B	12	91	4,09
esxcomp-02a.corp.lo...	Connected	Normal	Compute Cluster A	6	46	4,09

- Perform Inbound/Outbound activity monitoring
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then Activity Monitoring.
  - Select the Inbound Activity or Outbound Activity tab
  - Change the filters as desired and click Search

- Enable data collection for single/multiple virtual machines
  - Single
    - Log in to the vSphere Web Client.
    - Click vCenter and then click VMs and Templates.
    - Select a virtual machine from the left inventory panel.
    - Click the Manage tab and then click the Settings tab.
    - Click NSX Activity Monitoring from the left panel.
    - Click Edit.
    - In the Edit NSX Activity Monitoring Data Collection Settings dialog box, click Yes.
  - Multiple
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click Service Composer.
    - Click the Security Groups tab.
    - Select the Activity Monitoring Data Collection security group and click the Edit (Pencil) icon
    - Follow the wizard to add virtual machines to the security group.
      Data collection is enabled on all virtual machines you added to this security group, and disabled on any virtual machines you excluded from the security group.

- Perform virtual machine activity monitoring
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then Activity Monitoring.
  - Select the VM Activity tab
  - Change the filters as desired and click Search

- Monitor activity between inventory containers (security groups, AD groups)
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then Activity Monitoring.
  - Select the Inter Container Interaction tab in the left pane.
  - Click the link next to Originating from.
    All groups discovered through guest introspection are displayed.
  - Select the type of user group that you want to view resource utilization for.
  - In Filter, select one or more group and click OK.
  - In Where the destination is, select is or is not to indicate whether the selected group should be included in or excluded from the search.
  - Click the link next to Where the destination is.

    - Select the group type.
    - In Filter, select one or more group and click OK.
    - Click the "During period" icon and select the time period for the search.
    - Click Search.

- Analyze network and security metrics in vCOPS
    - Need to have Management Pack for NSX loaded in vCOPs
      See VMworld recorded session MGT1878 for a walkthrough
    - NSX Main - can see top Logical Networks / VMs by traffic throughput
    - NSX Topology - can drill down to show topology, also show metrics for the selected object.
    - NSX Edge Services – Show high level view of Edge services and their metrics.

- Monitor logical networks and services
    - Identify available statistics/counters
        - Controller
            - Controller CLI:
                - show control-cluster logical-routers
                - show control-cluster logical-routers vdr-stats logicalRouterID
        - Edge
            - Log in to the vSphere Web Client.
            - Click Networking & Security and then NSX Edges
            - Double click on an NSX Edge and select Monitor and Statistics:
              Interface throughput (per interface)
              Concurrent connections (FW/LB)
    - Network/service health
        - Easily viewed through vCOPs with NSX Management Plugin. Heat map can be displayed for Virtual and Physical networks.

    - Configure and collect data from network
        - Log in to the vSphere Web Client.
        - Click Networking & Security and then Flow Monitoring
        - Select Configuration
        - Configure the Flow Collections, making modifications to Flow Exclusion if required
        - Click on IPFix and edit the IPFix domain, timeout and collector IPs as required.
        - Click Publish Changes

Tools

- NSX Administration Guide
- NSX Command Line Interface Reference Guide
- NSX Controller CLI
- vSphere Web Client
- vCenter Operations Manager (vCOPS)

Objective 8.4 – Perform Auditing and Compliance

Knowledge

- Identify applicable logs for auditing
    - NSX Manager – Syslog, System Event Report, Virtual Appliance Events, Audit Log
    - NSX Edge – Syslog

  - Firewall – Syslog

- Identify permissions for auditing
  - Security Administrator - NSX security only: for example, define data security policies, create port groups, create reports for NSX modules, Create and publish policies and view violation reports. Cannot start or stop a data security scan
  - NSX Administrator - Start and stop data security scans
  - Auditor - View configured policies and violation reports.

- Identify common data security regulations supported by NSX Data Security
  - A regulation is a data privacy law for protecting PCI (Payment Card Industry), PHI (Protected Health Information) and PII (Personally Identifiable Information) information.

- Identify common file formats supported by NSX Data Security
  - Archive, CAD, Database, PDF, Mail, Multimedia, Presentation, Spreadsheet, Text/Markup, Word Processing.

- Describe and differentiate information available in audit logs
  - Audit logs include audit records for situations like admin login, configuration change, etc. Audit records provide granular details of all changes.
  - NSX Manager retains up to 1000,000 audit logs

- Use flow monitoring to audit firewall rules
  - Log in to the vSphere Web Client.
  - Select Networking & Security from the left navigation pane and then select Flow Monitoring.
  - Ensure that you are in the Dashboard tab.
  - Click Flow Monitoring.
    The page might take several seconds to load. The top of the page displays the percentage of allowed traffic, traffic blocked by firewall rules, and traffic blocked by SpoofGuard. The multiple line graph displays data flow for each service in your environment. When you point to a service in the legend area, the plot for that service is highlighted.
  - Traffic statistics are displayed in three tabs:
    - Top Flows displays the total incoming and outgoing traffic per service over the specified time period based on the total bytes value (not based on sessions/packets). The top five services are displayed. Blocked flows are not considered when calculating top flows.
    - Top Destinations displays incoming traffic per destination over the specified time period. The top five destinations are displayed.
    - Top Sources displays outgoing traffic per source over the specified time period. The top five sources are displayed.
  - Click the Details by Service tab.
    Details about all traffic for the selected service are displayed. Click Load More Records to display additional flows. The Allowed Flows tab displays the allowed traffic sessions and the Blocked Flows tab displays the blocked traffic.
    You can search on service names.
  - Click an item in the table to display the rules that allowed or blocked that traffic flow.
  - Click the Rule Id for a rule to display the rule details.

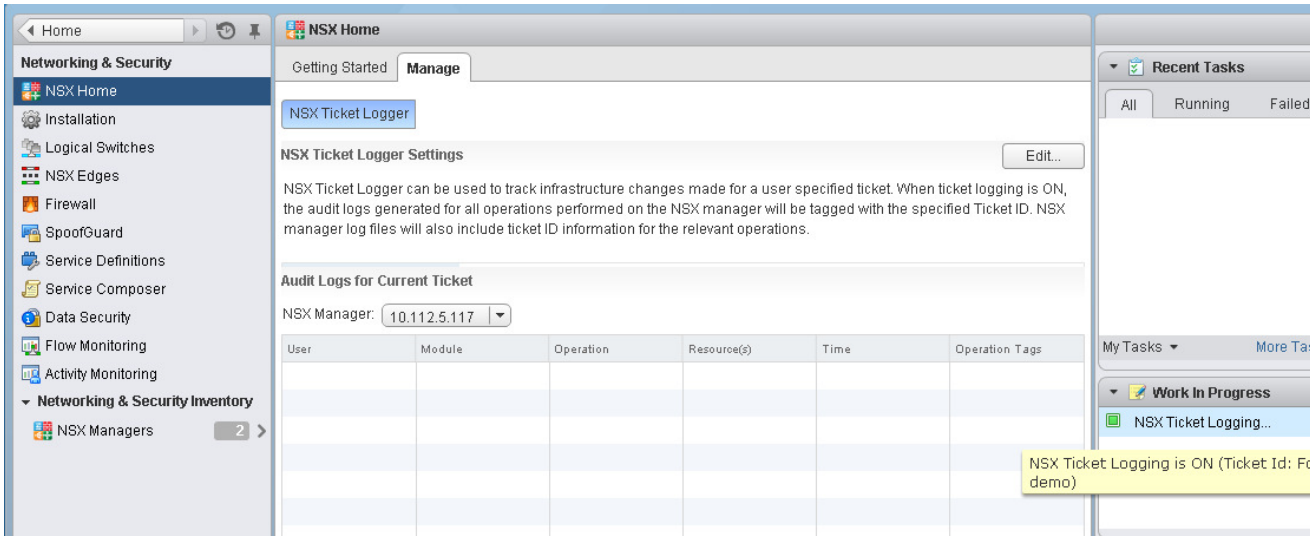
- Audit deleted users

- Log in to the vSphere Web Client.
- Click Networking & Security and then click NSX Managers.
- Click a vCNS server in the Name column and then click the Monitor tab.
- Click the Audit Logs tab
- Enter “Delete” into the filter box and press enter

- Audit infrastructure changes

  The NSX Ticket Logger allows you to track the infrastructure changes that you make. All operations are tagged with the specified ticket ID, and audit logs for these operations include the ticket ID. Log files for these operations are tagged with the same ticked ID.

  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click the Manage tab.
  - Click Edit next to NSX Ticket Logger Settings.
  - Type a ticket ID and click Turn On.
  - The NSX Ticket Logging pane is displayed at the right side of the vSphere Web Client window. Audit logs for the operations that you perform in the current UI session include the ticket ID in the Operation Tags column.



  - If multiple vCenter Servers are being managed by the vSphere Web Client, the ticket ID is used for logging on all applicable NSX Managers.

    Ticket logging is session based. If ticket logging is on and you log out or if the session is lost, ticket logging will be turned off by default when you re-login to the UI. When you complete the operations for a ticket, you turn logging off by repeating steps 2 and 3 and clicking Turn Off.

- View NSX Manager audit logs and change data
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Managers.
  - Click a vCNS server in the Name column and then click the Monitor tab.
  - Click the Audit Logs tab.
  - To view details of an audit log, click the text in the Operation column. When details are available for an audit log, the text in the Operation column for that log is clickable.

- In the Audit Log Change Details, select Changed Rows to display only those properties whose values have changed for this audit log operation.

- Configure NSX Data Security
  To configure NSX Data Security, you need to perform the following configurations
  - Ensure the Data Security and Endpoint services are installed
  - Create a Data Security policy
  - Create a Security Policy
  - Map the Security Policy to a Security Group

- Create a Data Security policy
  To detect sensitive data in your environment, you must create a data security policy. You must be a Security Administrator to create policies.
  To define a policy, you must specify the following:
  - Regulations
    A regulation is a data privacy law for protecting PCI (Payment Card Industry), PHI (Protected Health Information) and PII (Personally Identifiable Information) information. You can select the regulations that your company needs to comply to. When you run a scan, Data Security identifies data that violates the regulations in your policy and is sensitive for your organization.
    - Log in to the vSphere Web Client.
    - Click Networking and Security and then click Data Security.
    - Click the Manage tab.
    - Click Edit and click All to display all available regulations.
    - Select the regulations for which you want to detect compliance.
    - Click Next.
    - Certain regulations require additional information for NSX Data Security to recognize sensitive data. If you selected a regulation that monitors Group Insurance Numbers, Patient Identification Numbers, Medical Record Numbers, Health Plan Beneficiary Numbers, US Bank Account Numbers, Custom Accounts, or Student identification numbers, specify a regular expression pattern for identifying that data.
      NOTE Check the accuracy of the regular expression. Specifying incorrect regular expressions can slow down the discovery process.
    - Click Finish.
    - Click Publish Changes to apply the policy.

  - File filters
    You can create filters to limit the data being scanned and exclude file types unlikely to contain sensitive data from the scan.
    - In the Manage tab of the Data Security panel, click Edit next to Files to scan.
    - You can either monitor all files on the virtual machines in your inventory, or select the restrictions you want to apply.
      - Monitor all files on the guest virtual machines
        NSX Data Security scans all files.
      - Monitor only the files that match the following conditions
        Select the following options as appropriate.
        - **Size** indicates that NSX Data Security should only scan files less than the specified size.
        - **Last Modified Date** indicates that NSX Data Security should scan only files modified between the specified dates.

        - **Types:** Select Only files with the following extensions to enter the file types to scan. Select All files, except those with extensions to enter the file types to exclude from the scan.
    - Click Save.
    - Click Publish Changes to apply the policy.

- View and download compliance reports
    - Log in to the vSphere Web Client.
    - Click Networking and Security and then click Data Security.
    - Click the Reports tab.
    - Specify whether you want to view a Violation counts or Violating files report.

- Create a regular expression
  A regular expression is a pattern that describes a certain sequence of text characters, otherwise known as strings. You use regular expressions to search for, or match, specific strings or classes of strings in a body of text.
  Using a regular expression is like performing a wildcard search, but regular expressions are far more powerful. Regular expressions can be very simple, or very complex. An example of a simple regular expression is cat.
  This finds the first instance of the letter sequence cat in any body of text that you apply it to. If you want to make sure it only finds the word cat, and not other strings like cats or hepcat, you could use this slightly more complex one: \bcat\b.
  This expression includes special characters that make sure a match occurs only if there are word breaks on both sides of the cat sequence. As another example, to perform a near equivalent to the typical wildcard search string c+t, you could use this regular expression: \bc\w+t\b.
  This means find a word boundary (\b) followed by a c, followed by one or more non-whitespace, nonpunctuation characters (\w+), followed by a t, followed by a word boundary (\b). This expression finds cot, cat, croat, but not crate.
  Expressions can get very complex. The following expression finds any valid email address. \b[A-Za-z0-9._%-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,4}\b

Tools
- NSX Administration Guide
- NSX Ticket Logger
- vSphere Web Client

Objective 8.5 – Administer Logging

Knowledge
- Identify content contained in technical support bundles
    - Product specific diagnostic logs.
- Identify where to locate component/service specific log information
    - All log information is sent to the configured syslog servers
- Explain usage of CLI for logging
    - The CLI can be used to show log information
        - NSX Manager
            - Show manager log
            - Show manager log last

        - NSX Edge
            - Show log
            - Show log follow
            - Show log last
            - Show log reverse
- Configure Syslog(s)
    - NSX Manager
        - Log in to the NSX Manager virtual appliance
        - Under Appliance Management, click Manage Appliance Settings.
        - From the Settings panel, click General.
        - Click Edit next to Syslog Server.
        - Type the IP address of the syslog server.
        - Type the port and protocol for the syslog server.
          If you do not specify a port, the default UDP port for the IP address/host name of the syslog server is used.
        - Click OK.
    - NSX Edge
        - Log in to the vSphere Web Client.
        - Click Networking & Security and then click NSX Edges.
        - Double-click a NSX Edge.
        - Click the Manage tab and then click the Settings tab.
        - In the Details panel, click Change next to Syslog servers.
        - Type the IP address of both remote syslog servers and select the protocol.
        - Click OK to save the configuration.
    - NSX Controller
        - The only way to configure syslog export on the NSX controllers is by the REST API
            - Request:
              POST https:///api/2.0/vdn/controller/{controller-id}/syslog
            - Request Body:
              <ip address>
              514
              UDP
              INFO
    - Firewall
        - You must configure the remote syslog server for each cluster that has firewall enabled. The remote syslog server is specified in the Syslog.global.logHost attribute

- Configure logging for Dynamic Routing information
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click NSX Edges.
    - Double-click a Distributed Router.
    - Click the Manage tab and then click the Routing tab.
    - Select Global Configuration and click Edit by Dynamic Routing Configuration
    - Click Enable Logging to log Dynamic Routing Config traffic, and select the log level.
      Generated logs are sent to the syslog server.
    - Click Ok.

- Log Distributed Firewall rule processing information
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click NSX Edges.

  - Double-click a Distributed Router.
  - Click the Manage tab and then click the Firewall tab.
  - For each rule to log, click on the [+] by "Accept"
  - In the Pop-up box click Log to log traffic matched by that rule. Generated logs are sent to the syslog server.
  - Click Ok.

- Log Edge Firewall rule processing information
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click a NSX Edge.
  - Click the Manage tab and then click the Firewall tab.
  - For each rule to log, click on the [+] by "Accept"
  - In the Pop-up box click Log to log traffic matched by that rule. Generated logs are sent to the syslog server.
  - Click Ok.

- Log address translation information
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click a NSX Edge.
  - Click the Manage tab and then click the NAT tab.
  - For each rule to log, click on the rule to select it, then click the Edit (Pencil) icon
  - In the Pop-up box click Enable logging to log traffic matched by that rule. Generated logs are sent to the syslog server.
  - Click Ok.

- Log VPN traffic
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click a NSX Edge.
  - Click the Manage tab and then click the VPN tab.
  - Expand the Logging Policy subsection
  - Click Enable Logging to log VPN traffic and select the log level. Generated logs are sent to the syslog server.
  - Click Ok.

- Configure basic/advanced Load Balancer logging
  - Basic
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then click NSX Edges.
    - Double-click a NSX Edge.
    - Click the Manage tab and then click the Load Balancer tab.
    - Click Edit
    - Scroll to the bottom and click Logging to log LB traffic and select the log level. Generated logs are sent to the syslog server.
    - Click Ok.

  - Advanced

By default, NSX load balancer supports basical logging. You can create an application rule as follows to view more detailed logging messages for troubleshooting.

```
# log the name of the virtual server
capture request header Host len 32

# log the amount of data uploaded during a POST
capture request header Content-Length len 10

# log the beginning of the referrer
capture request header Referer len 20

# server name (useful for outgoing proxies only)
capture response header Server len 20

# logging the content-length is useful with "option logasap"
capture response header Content-Length len 10

# log the expected cache behaviour on the response
capture response header Cache-Control len 8

# the Via header will report the next proxy's name
capture response header Via len 20

# log the URL location during a redirection
capture response header Location len 20
```

After you associate the application rule to the virtual server, logs include detailed messages

- Log DHCP assignments
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click a NSX Edge.
  - Click the Manage tab and then click the DHCP tab.
  - Click Enable Logging to log DHCP traffic and select the log level. Generated logs are sent to the syslog server.
  - Click Ok.

- Log DNS resolutions
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click a NSX Edge.
  - Click the Manage tab and then click the Settings tab.
  - In the DNS Configuration panel, click Change.
  - Click Enable Logging to log DNS traffic and select the log level. Generated logs are sent to the syslog server.
  - Click Ok.

- Log security policy session information
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click Service Composer.

  - Click the Security Policies tab.
  - Select the Security Policy to which you wish to add logging.
  - Click the Manage tab then Information Security
  - Select Firewall Rules then click Edit
  - Select the Rule to add logging to, and click the Edit (Pencil) icon
  - Scroll down, and select Log, click OK
  - Click OK
  - Repeat for the Network Introspection Services

- Download NSX Edge tech support logs
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Select an NSX Edge instance.
  - Click the "More Actions" icon and select Download Tech Support Logs.
  - After the tech support logs are generated, click Download.
  - In the Select location for download dialog box, browse to the directory where you want to save the log file.
  - Click Save.
  - Click Close.

- Generate NSX Manager tech support logs
  - Log in to the NSX Manager virtual appliance.
  - Under Appliance Management, click Manage Appliance Settings.
  - Click and then click Download Tech Support Log.
  - Click Download.
  - After the log is ready, click the Save to download the log to your desktop. The log is compressed and has the file extension .gz.

Tools
• NSX Administration Guide
• NSX Command Line Interface Reference Guide
• NSX Edge CLI
• vSphere Web Client
• Log Insight
• Syslog

Objective 8.6 – Backup and Recover Configurations

Knowledge

- Identify remote backup destinations
  - Backups can be sent to remote FTP or SFTP servers

- Explain how to backup and recover various components
  - You can back up and restore your NSX Manager data, which can include system configuration, events, and audit log tables. Configuration tables are included in every backup. Backups are saved to a remote location that must be accessible by the NSX Manager.

- Schedule backups

    - See Perform NSX Manager backup operations, below

- Export/Restore vSphere Distributed Switch configuration
    - Export
        - Browse to a distributed switch in the vSphere Web Client navigator.
        - Right-click the distributed switch and click All vCenter Actions > Export Configuration.
        - Select the Export the distributed switch configuration or Export the distributed switch configuration and all port groups option.
        - (Optional) Enter notes about this configuration in the Description field.
        - Click OK.
        - Click Yes to save the configuration file to your local system.
    - Restore
        - Browse to a distributed switch in the vSphere Web Client navigator.
        - Right-click the distributed switch and click All vCenter Actions > Restore Configuration.
        - Browse for the configuration backup file to use.
        - Select the Restore distributed switch and all port groups or Restore distributed switch only option and click Next.
        - Review the summary information for the restore.
        - Click Finish.

- Import/Export Service Composer profiles
    - Import
        - Log in to the vSphere Web Client.
        - Click Networking & Security and then click Service Composer.
        - Click the Security Policies tab.
        - Click Actions and then click the Import Service Configuration icon.
        - Select the configuration file that you want to import.
        - If desired, type a suffix to be added to the security policies and security groups that are being imported.
          If you specify a suffix, it is added to the security policy names being imported thus ensuring that they have unique names.
        - Click Next.
          Service Composer verifies that all services referred to in the configuration are available in the destination environment. If not, the Manage Missing Services page is displayed, where you can map missing services to available target services.
          The Ready to complete page displays the security policies along with associated objects (security groups on which these have been applied, as well as Endpoint services, firewall rules, and network introspection services) to be imported.
        - Click Finish.
          The imported security policies are added to the top of the security policy table (above the existing policies) in the target NSX Manager. The original order of the imported policies is preserved.
    - Export
        - Log in to the vSphere Web Client.
        - Click Networking & Security and then click Service Composer.
        - Click the Security Policies tab.
        - Select the security policy that you want to export.
        - Click Actions and then click the Export Service Configuration icon.
        - Type a name and description for the configuration that you are exporting.

        - If desired, type a prefix to be added to the security policies and security groups that are being exported.
          If you specify a prefix, it is added to the target security policy names thus ensuring that they have unique names.
        - Click Next.
        - In the Select security policies page, select the security policy that you want to export and click Next.
        - The Ready to complete page displays the security policies along with associated objects (security groups on which these have been applied, as well as Endpoint services, firewall rules, and network introspection services) to be exported.
        - Click Finish.
        - Select the directory on your computer where you want to download the exported blueprint and click Save.

- Perform NSX Manager backup and restore operations
    - Backup
        - Log in to the NSX Manager Virtual Appliance.
        - Under Appliance Management, click Backups & Restore.
        - To specify the backup location, click Change next to FTP Server Settings.
            - Type the IP address or host name of the backup system.
            - From the Transfer Protocol drop-down menu, select either SFTP or FTP, based on what the destination supports.
            - Edit the default port if required.
            - Type the user name and password required to login to the backup system.
            - In the Backup Directory field, type the absolute path where backups will be stored.
            - Type a text string in Filename Prefix.
              This text is prepended to each backup filename for easy recognition on the backup system. For example, if you type ppdb, the resulting backup is named as ppdbHH_MM_SS_DayDDMonYYYY.
            - Type the pass phrase to secure the backup.
            - Click OK.
        - To specify schedule details, click Change next to Scheduling.
            - From the Backup Frequency drop-down menu, select Hourly, Daily, or Weekly. The Day of Week, Hour of Day, and Minute drop-down menus are disabled based on the selected frequency. For example, if you select Daily, the Day of Week drop-down menu is disabled as this field is not applicable to a daily frequency.
            - For a weekly backup, select the day of the week the data should be backed up.
            - For a weekly or daily backup, select the hour at which the backup should begin.
            - Select the minute at which the backup should begin and click Schedule.
        - To exclude logs and flow data from being backed up, click Change next to Exclude.
            - Select the items you want to exclude from the backup.
            - Click OK.
    - Restore
        - Log in to the NSX Manager Virtual Appliance.
        - Under Appliance Management, click Backups & Restore.
        - In the Backups History section, select the check box for the backup to restore.

        - Click Restore.
        - Click OK to confirm.

Tools

- NSX Administration Guide
- vSphere Web Client

Section 9 – Troubleshoot a VMware Network Virtualization Implementation

Objective 9.1 – Identify Tools Available for Troubleshooting

Knowledge

- Identify filters available for packet capture
  - NSX Edge CLI
  - pktcap-uw
  - tcpdump-uw
  - Flow Monitoring

- Capture and trace uplink, vmknic, and physical NIC packets
  - Uplink

    debug packet display interface
    - Displays all packets captured by an NSX Edge interface, similar to a tcpdump. Enabling this command can impact NSX Edge performance. To disable the display of packets, use no before the command.
    - Synopsis
      [no] debug packet display interface (intif | extif) [EXPRESSION]
  - vmknic
    - To view a live capture of a vmkernel ports traffic:
      # pktcap-uw --vmk vmkX
  - pNic
    - To view a live capture of a specific physical network card on the host vmnic:
      # pktcap-uw --uplink vmnicX

- Identify and track NSX infrastructure changes
  - NSX Ticket Logger – See Objective 8.4

- Output packet data for use by a protocol analyzer
  - To capture the output to a file, use -o option:
    # pktcap-uw --vmk vmk# -o file.pcap

- Capture and analyze traffic flows
  - Log in to the vSphere Web Client.
  - Select Networking & Security from the left navigation pane and then select Flow Monitoring.
  - Ensure that you are in the Dashboard tab.
  - Click Flow Monitoring.
  - The page might take several seconds to load. The top of the page displays the percentage of allowed traffic, traffic blocked by firewall rules, and traffic blocked by SpoofGuard. The multiple line graph displays data flow for each service in your environment. When you point to a service in the legend area, the plot for that service is highlighted.
  - Traffic statistics are displayed in three tabs:
  - Top Flows displays the total incoming and outgoing traffic per service over the specified time period based on the total bytes value (not based on sessions/packets). The top five services are displayed. Blocked flows are not considered when calculating top flows.

- Top Destinations displays incoming traffic per destination over the specified time period. The top five destinations are displayed.
- Top Sources displays outgoing traffic per source over the specified time period. The top five sources are displayed.
- Click the Details by Service tab.
- Details about all traffic for the selected service are displayed. Click Load More Records to display additional flows. The Allowed Flows tab displays the allowed traffic sessions and the Blocked Flows tab displays the blocked traffic.
- You can search on service names.
- Click an item in the table to display the rules that allowed or blocked that traffic flow.
- Click the Rule Id for a rule to display the rule details.

- Mirror network traffic for analysis
  - Netflow/IPFix
    - Log in to the vSphere Web Client.
    - Click Networking & Security and then Flow Monitoring
    - Select Configuration
    - Configure the Flow Collections, making modifications to Flow Exclusion if required
    - Click on IPFix and edit the IPFix domain, timeout and collector IPs as required.
    - Click Publish Changes

  - vDS port mirroring
    - Log in to the vSphere Web Client.
    - Browse to a distributed switch in the vSphere Web Client
    - Click the Manage tab and select Settings > Port Mirroring
    - Click New.
    - Select the session type for the port mirroring session.
      - Distributed Port Mirroring
        Mirror packets from a number of distributed ports to other distributed ports on the same host. If the source and the destination are on different hosts, this session type does not function.
      - Remote Mirroring Source
        Mirror packets from a number of distributed ports to specific uplink ports on the corresponding host.
      - Remote Mirroring Destination
        Mirror packets from a number of VLANs to distributed ports.
      - Encapsulated Remote Mirroring (L3) Source
        Mirror packets from a number of distributed ports to remote agent's IP addresses. The virtual machine's traffic is mirrored to a remote physical destination through an IP tunnel.
      - Distributed Port Mirroring (legacy)
        Mirror packets from a number of distributed ports to a number of distributed ports and/or uplink ports on the corresponding host.
    - Click Next
    - Set the session properties. Different options are available for configuration depending on which session type you selected.
      - Name
        You can enter a unique name for the port mirroring session, or accept the automatically generated session name.

- Status
  Use the drop down menu to enable or disable the session.
- Session type
  Displays the type of session you selected.
- Normal I/O on destination ports
  Use the drop-down menu to allow or disallow normal I/O on destination ports. This property is only available for uplink and distributed port destinations.
  If you disallow this option, mirrored traffic will be allowed out on destination ports, but no traffic will be allowed in.
- Mirrored packet length (Bytes)
  Use the check box to enable mirrored packet length in bytes. This puts a limit on the size of mirrored frames. If this option is selected, all mirrored frames are truncated to the specified length.
- Sampling rate
  Select the rate at which packets are sampled. This is enabled by default for all port mirroring sessions except legacy sessions.
- Description
  You have the option to enter a description of the port mirroring session configuration.

- Click Next.
- Select the source of the traffic to be mirrored and the traffic direction. Depending on the type of port mirroring session you selected, different options are available for configuration.
  - Add existing ports from a list
    Click Select distributed ports. A dialog box displays a list of existing ports. Select the check box next to the distributed port and click OK. You can choose more than one distributed port.
  - Add existing ports by port number
    Click Add distributed ports, enter the port number and click OK.
  - Set the traffic direction
    After adding ports, select the port in the list and click the ingress, egress, or ingress/egress button. Your choice appears in the Traffic Direction column.
  - Specify the source VLAN
    If you selected a Remote Mirroring Destination sessions type, you must specify the source VLAN. Click Add to add a VLAN ID. Edit the ID by using the up and down arrows, or clicking in the field and entering the VLAN ID manually.
- Click Next.
- Select the destination for the port mirroring session. Depending on which type of session you chose, different options are available.
  - Select a destination distributed port
    Click Select distributed ports to select ports from a list, or click Add distributed ports to add ports by port number. You can add more than one distributed port.
  - Select an uplink
    Select an available uplink from the list and click Add to add the uplink to the port mirroring session. You can select more than one uplink.
  - Select ports or uplinks

Click Select distributed ports to select ports from a list, or click Add distributed ports to add ports by port number. You can add more than one distributed port.
- Click Add uplinks to add uplinks as the destination. Select uplinks from the list and click OK.
- Specify IP address
  Click Add. A new list entry is created. Select the entry and either click Edit to enter the IP address, or click directly in the IP Address field and type the IP address. A warning appears if the IP address is invalid.

- Click Next.
- Review the information that you entered for the port mirroring session on the Ready to complete page.
- (Optional) Use the Back button to edit the information.
- Click Finish.

- Perform a network health check
  - Enabling or disabling the vSphere Distributed Switch health check in the vSphere Web Client
    Notes: Health check monitors for changes in vSphere distributed switch configurations. You must enable vSphere distributed switch health check to perform checks on distributed switch configurations.
    Health check is available only in ESXi 5.1 and later distributed switches. You can view health check information only through the vSphere Web Client 5.1 or later.
    - Browse to a vSphere distributed switch in the vSphere Web Client.
    - Click the Manage tab.
    - Click Settings and then click Health check.
    - To enable or disable health check, click Edit.
    - Select from the dropdown to enable or disable health check options.
      The options include:
      - VLAN and MTU – Reports the status of distributed uplink ports and VLAN ranges
      - Teaming and Failover – Checks for any configuration mismatch between ESXi and the physical switch used in the teaming policy.
    - Click OK.
  - Viewing the vSphere Distributed Switch health check information
    Note: After enabling health check, you can view the vSphere distributed switch health check information in the vSphere Web Client.

    - Browse to a vSphere distributed switch in the vSphere Web Client.
    - Click the Monitor tab and click Health.
    - In the Health Status Details section, click one of these tab to view the health status:
    - VLAN
    - MTU
    - Teaming and Failover

- Configure vSphere Distributed Switch alarms
  - Browse to a vSphere distributed switch in the vSphere Web Client.
  - Click the Manage tab and Alarm Definitions
  - Click + to add an alarm
  - Enter the Alarm name and Description

  - Next
  - Add Events and Conditions to trigger the alarm
  - Next
  - Optional: Click + to add actions on alarm state changes
  - Click Finish

Tools

- NSX Administration Guide
- vSphere Networking Guide
- vSphere Command-Line Interface Concepts and Examples
- vSphere Web Client
- NSX Ticket Logger
- ESXi Host CLI
- pktcap-uw
- Netflow
- RSPAN/ERSPAN
- VDS Health Check

Objective 9.2 – Troubleshoot Common NSX Installation/Configuration Issues

Knowledge

- Identify ports required for NSX communication
  - **443/TCP**
    Downloading the OVA file on the ESX host for deployment
    Using REST APIs
    Using the NSX Manager user interface
  - **80/TCP**
    Initiating connection to the vSphere SDK
    Messaging between NSX Manager and NSX host modules
  - **1234/TCP**
    Communication between ESX Host and NSX Controller Clusters
  - **56711**
    Rabbit MQ (messaging bus technology)
  - **22/TCP**
    Console access (SSH) to CLI. By default, this port is closed.

- Troubleshoot lookup service configuration
  - Confirm that the user has admin privileges.
  - Verify whether NSX Manager and Lookup service appliances are in time sync. To achieve this, use same NTP server configurations at NSX Manager and Lookup service.
  - Check DNS settings for name resolution.

- Troubleshoot vCenter Server link
  - Check DNS settings.
  - Confirm that user has administrative privileges.

- Troubleshoot licensing issues
  - Validate that the vSphere Web Client is successfully installed. Starting with vCenter Server 5.0, License Reporting is a component of the vSphere Web Client. To access it, the Web client

must be installed and vCenter Server must be registered to it. For more information, see the Install and Start the vSphere Web Client section of the vSphere Installation and Setup guide.

- Verify that vCenter Server and the vSphere Client workstation can communicate with the Web Client Server. For more information, see Testing network connectivity with the ping command (KB1003486).
- Verify that name resolution to the Web Client server is correctly configured from vCenter Server and the vSphere Client workstation. For more information, see Configuring name resolution for VMware vCenter Server (KB1003735).
- Check the vSphere Client log (viclient-x-xxxx.log located at %USERPROFILE%\AppData\Local\VMware\vpx) to validate the URL used to connect to the Web Client server.
  You see messages similar to:
  [viclient:QuickInf:M: 7] 2012-02-27 12:15:22.227 FlexWebContainer.NavigateToUrl(nav): https:// webclient/csharp-app/?extensionId=vsphere.license.licenseReportView&context=CB1D4EA7-F6A8-46DA-81CA-99ADCF95359A:Folder:group-d1&locale=en_US&j_serviceUrl=https://vcenterserver&j_serviceGuid=CB1D4EA7-F6A8-46DA-81CA-99ADCF95359A&j_thumbprint=98:CC:31:66:6C:4F:85:6E:A6:09:09:89:22:28:90:23:23:DC:82:E8&j_qsCookie=JSESSIONID=6atwl6n6g00cht1apfj5tp47, vmware_soap_session=d0122775-e4b2-427b-9195-12ccf3a53b4c&sessionTicket=cst-VCT-5292c695-1069-a798-c4d7-08e3ad48fe04--tp-98-CC-31-66-6C-4F-85-6E-A6-09-09-89-22-28-90-23-23-DC-82-E8

  Where webclient is the address of the Web Client Server and vcenterserver is the address of vCenter server. If either of these values are incorrect, unregister and then register vCenter Server to the vSphere Web Client from the Web client Administration application. This application is located on the server running the vSphere Web Client. To launch the application, navigate to Start > Programs > VMware > VMware vSphere Web Client > vSphere Administration Application.
- Validate that the vCenter Server proxy.xml file (located at C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter) has the appropriate configuration for the Web Client. A correct configuration appears similar to:

  ```
  <e id="19">
  <_type>vim.ProxyService.RedirectSpec</_type>
  <accessMode>httpsOnly</accessMode>
  <hostName> webclient</hostName>
  <port> 9443</port>
  <redirectType>permanent</redirectType>
  <serverNamespace>/vsphere-client</serverNamespace>
  </e>
  ```

  Where webclient is the address of the Web Client server. If either the port or the address to the Web client is incorrect, correct and then restart the VMware VirtualCenter Server service.

- Troubleshoot permissions issues
  - There are 4 User Roles:
    - **Enterprise Administrator**
      NSX Operations and Security

        - **NSX Administrator**
          NSX Operations only (install virtual appliances, configure port groups etc)
        - **Security Administrator**
          NSX Security only (define Data Security policies, create port groups, create reports etc)
        - **Auditor**
          Read Only
    - An NSX User/Group can only have one role
    - You cannot add a role to a user/group, or remove an assigned role from a user/group, you can however change the assigned role for a user/group.

    - There are 2 scopes which determine what resources a particular user can view
        - No restriction
          Access to the entire NSX system
        - Limit access scope
          Access only a specified Edge.

    - A user can be a member of a number of groups, and will inherit combined role permissions from those groups. If the user has a directly assigned role, this overrides the group permissions.

    - Given the above overview of NSX permissions, check for permissions allocated directly to a user, also check membership of the groups that permissions have been allocated to, as well as any scope limitation.

- Troubleshoot host preparation issues
    - In the Installation tab, click Host Preparation.
    - For each cluster, click Install in the Installation Status column.
      Note - While the installation is in progress, do not deploy, upgrade, or uninstall any service or component.
    - Monitor the installation until the Installation Status column displays a green check mark.
      If the Installation Status column displays a red warning icon and says Not Ready, click Resolve. Clicking Resolve might result in a reboot of the host. If the installation is still not successful, click the warning icon. All errors are displayed. Take the required action and click Resolve again.
      When the installation is complete, the Installation Status column displays 6.1 and the Firewall column displays Enabled. Both columns have a green check mark. If you see Resolve in the Installation Status column, click Resolve and then refresh your browser window.

- Troubleshoot IP pool issues
    - I can't find anything in the admin or installation guides about this. I guess the obvious things are to ensure that the IP Pool configuration matches the subnet (correct subnet mask etc) and that it's not full.

Tools

- NSX Installation and Upgrade Guide
- NSX Administration Guide
- NSX Command Line Interface Reference Guide
- NSX Controller CLI

- vSphere Web Client

Objective 9.3 – Troubleshoot Common NSX Component Issues

Knowledge

- Differentiate NSX Edge logging and troubleshooting commands
  - Logging
    - show log <last *n*|follow|reverse>
      - Display the system log, last n lines, follow the log, show the log in reverse order
  - Troubleshooting
    - debug packet capture
      Similar to tcpdump
    - debug packet display interface
      Similar to tcpdump but for specific interface
    - ping <interface> addr
      ICMP ping, optionally choose the interface
    - show ….
      Large number of show commands, eg, arp, configuration
      [interface|dhcp|firewall|ipsec|loadbalancer|nat|ospf|syslog], ip [bgp|ospf|route]
      Too many to list here, see NSX CLI Guide for more details

- Verify NSX Controller cluster status and roles
  - SSH to one of your controller VM to use the CLI

```
# show control-cluster status

Type                Status
Since
--------------------------------------------------------------------------
-----------
Join status:        Join complete
09/14 14:08:46
Majority status:    Connected to cluster majority
09/18 08:45:16
Restart status:     This controller can be safely restarted
09/18 08:45:06
Cluster ID:         b20ddc88-cd62-49ad-b120-572c23108520
Node UUID:          b20ddc88-cd62-49ad-b120-572c23108520
```

  -

```
# show control-cluster roles
                            Listen-IP  Master?    Last-Changed  Count
api_provider         Not configured      Yes  09/18 08:45:17      6
persistence_server              N/A      Yes  09/18 08:45:17      5
switch_manager            127.0.0.1      Yes  09/18 08:45:17      6
logical_manager                 N/A      Yes  09/18 08:45:17      6
directory_server                N/A      Yes  09/18 08:45:17      6
```

- Verify NSX Controller node connectivity
  -

```
# show control-cluster connections

role                port            listening open conns
--------------------------------------------------------
api_provider        api/443         Y         1
```

```
------------------------------------------------------
persistence_server  server/2878     Y         2
                    client/2888     Y         3
                    election/3888   Y         0
------------------------------------------------------
switch_manager      ovsmgmt/6632    Y         0
                    openflow/6633   Y         0
------------------------------------------------------
system              cluster/7777    Y         2
```

The Controller cluster majority leader will be listening on port 2878 – other nodes have "-" in the listening column.
The number of "open conns" on the persistence server line should be the number of remaining nodes in the cluster eg 2 for a 3 node cluster.

- Check NSX Controller API service
  - `# show control-cluster connections`

```
role                port            listening open conns
------------------------------------------------------
api_provider        api/443         Y         1
------------------------------------------------------
```

- Validate VXLAN and Logical Router mapping tables
  - VXLAN
    From an ESXi host, use the esxcli command line

    #esxcli network vswitch dvs vmware vxlan network mac --vds-name [value] --vxlan-id value <--segment-id value --vtep-ip value>

IP	Segment ID	Is MTEP
192.168.0.2	192.168.0.0	False

  - Logical Router
    From the NSX controller

    show control-cluster logical-routers instance all

    This gives the LR instance IDs

    show control-cluster logical-routers interface-summary [instance ID]

Interface	Type	Id	IP[]
lif0	vlan	0	10.0.0.0/24
lif1	vlan	101	10.0.1.0/24
lif2	vxlan	5020	172.16.10.1/24

- List Logical Router instances and statistics
  - List instances
    show control-cluster logical-routers instance all
    or

show control-cluster logical-routers

- Statistics
  show control-cluster logical-routers stats

- Verify Logical Router interface and route mapping tables
  - # show control-cluster logical-routers interface-summary 1
    Interface Type Id IP[]
    lif0 vlan 0 10.0.0.0/24
    lif1 vlan 1 10.0.1.0/24

  - show control-cluster logical-routers routes 1
    LR-Id Destination Next-Hop
    1 70.70.70.0/24 10.0.1.2
    1 80.80.80.0/24 10.0.0.2

- Verify active controller connections
  - # show control-cluster core stats
    messages.received 40
    messages.received.dropped 0
    messages.transmitted 22
    messages.transmit.dropped 0
    messages.processing.dropped 0
    connections.up 2
    connections.down 0
    connections.timeout 0
    connections.active 2
    connections.sharding.subscribed 0

- View Bridge instances and learned MAC addresses
  - Dump bridge info
    # net-vdr --bridge -l <vdrName>

    VDR default+edge-1:1460487509 Bridge Information :

    Bridge config:
    Name:id mybridge:1
    Portset name:
    DVS name: Mgmt_Edge_VDS
    Ref count: 2
    Number of networks: 2
    Number of uplinks: 0

    Network 'vlan-100-type-bridging' config:
    Ref count: 2
    Network type: 1
    VLAN ID: 100
    VXLAN ID: 0
    Ageing time: 300

```
Fdb entry hold time:1
FRP filter enable:  1

    Network port '50331655' config:
    Ref count:        2
    Port ID:          0x3000007
    VLAN ID:          4095
    IOChains installed: 0

Network 'vxlan-5000-type-bridging' config:
Ref count:        2
Network type:     1
VLAN ID:          0
VXLAN ID:         5000
Ageing time:      300
Fdb entry hold time:1
FRP filter enable:  1

    Network port '50331655' config:
    Ref count:        2
    Port ID:          0x3000007
    VLAN ID:          4095
    IOChains installed: 0
```

- Lists MAC table, learnt on both VXLAN and VLAN sides

```
# net-vdr -b --mac default+edge-1

VDR default+edge-1:1460487509 Bridge Information :

Network 'vlan-100-type-bridging' MAC address table:
MAC table on PortID:            0x0
MAC table paging mode:          0
Single MAC address enable:      0
Single MAC address:             00:00:00:00:00:00
MAC table last entry shown:     00:50:56:91:5e:93 VLAN-VXLAN: 100-0 Port: 50331661
total number of MAC addresses:  1
number of MAC addresses returned: 1
MAC addresses:
Destination Address  Address Type  VLAN ID  VXLAN ID  Destination Port  Age
-------------------  ------------  -------  --------  ----------------  ---
00:50:56:91:5e:93    Dynamic       100      0         50331661  0

Network 'vxlan-5000-type-bridging' MAC address table:
MAC table on PortID:            0x0
MAC table paging mode:          0
Single MAC address enable:      0
Single MAC address:             00:00:00:00:00:00
MAC table  last entry shown:    00:50:56:ae:9b:be VLAN-VXLAN: 0-5000 Port: 50331650
total number of MAC addresses:  1
```

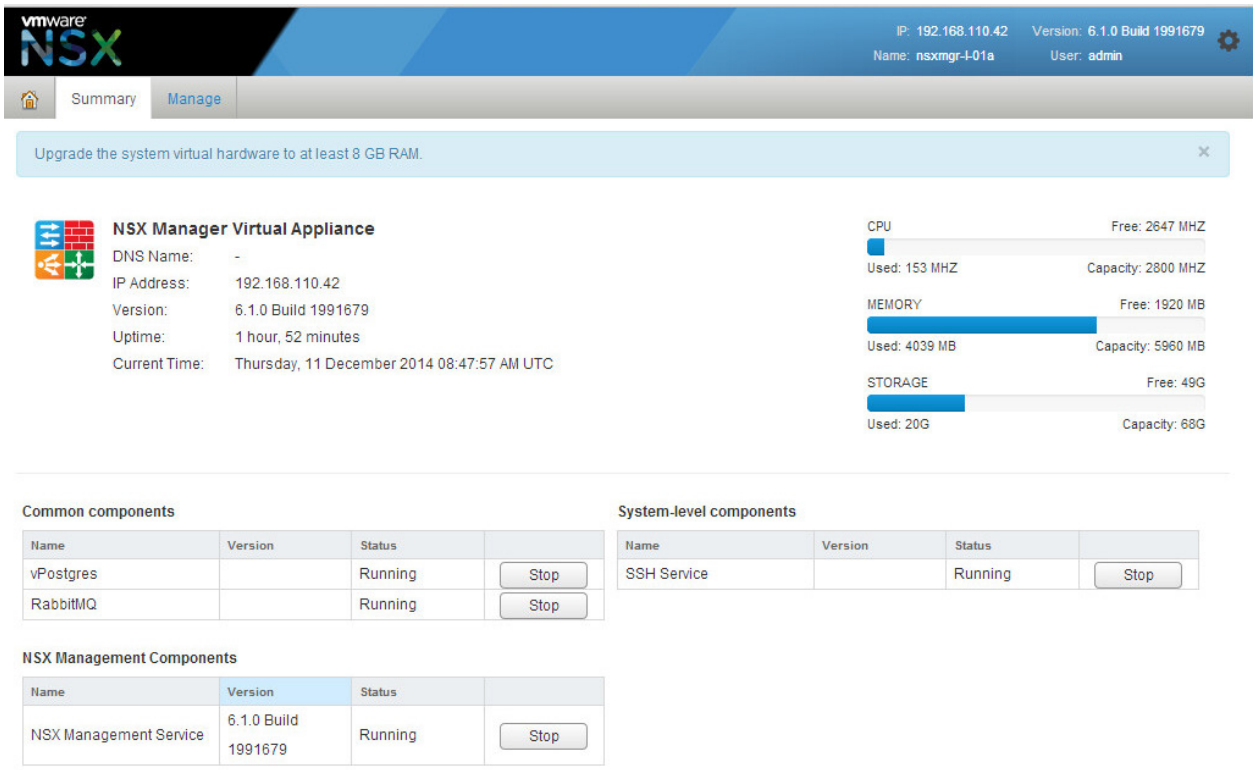
```
number of MAC addresses returned: 1
MAC addresses:
Destination Address  Address Type  VLAN ID  VXLAN ID  Destination Port  Age
-------------------  ------------  -------  --------  ----------------  ---
00:50:56:ae:9b:be    Dynamic          0     5000         50331650  0
```

- Display Logical Router instances
  - # net-vdr --instance -l

```
VDR Instance Information :
---------------------------

VDR Instance:           default+edge-1:1460487509
Vdr Name:               default+edge-1
Vdr Id:                 1460487509
Number of Lifs:         3
Number of Routes:       1
State:                  Enabled
Controller IP:          192.168.110.201
Control Plane Active:   Yes
Control Plane IP:       192.168.110.52
Edge Active:            Yes
```

- Verify NSX Manager services status
  - Service status can be view through the NSX Manager Web Interface



- View Logical Interfaces and routing tables
  - Logical interfaces
    From the CLI on an ESXi host
    # net-vdr --lif -l default+edge-1

    VDR default+edge-1:1460487509 LIF Information :

    Name: 570d45550000000c
    Mode: Routing, Distributed, Internal
    Id: Vxlan:5004
    Ip(Mask): 10.10.10.1(255.255.255.0)
    Connected Dvs: Mgmt_Edge_VDS
    VXLAN Control Plane: Enabled
    VXLAN Multicast IP: 0.0.0.1
    State: Enabled
    Flags: 0x2288

    Name: 570d45550000000b
    Mode: Bridging, Sedimented, Internal
    Id: Vlan:100
    Bridge Id: mybridge:1
    Ip(Mask): 0.0.0.0(0.0.0.0)
    Connected Dvs: Mgmt_Edge_VDS
    Designated Instance: No
    DI IP: 192.168.110.51

State: Enabled
Flags: 0xd4

Name: 570d45550000000a
Mode: Bridging, Sedimented, Internal
Id: Vxlan:5000
Bridge Id: mybridge:1
Ip(Mask): 0.0.0.0(0.0.0.0)
Connected Dvs: Mgmt_Edge_VDS
VXLAN Control Plane: Enabled
VXLAN Multicast IP: 0.0.0.1
State: Enabled
Flags: 0x23d4

- Routing
  # net-vdr -R -l default+edge-1

  VDR default+edge-1:1460487509 Route Table
  Legend: [U: Up], [G: Gateway], [C: Connected], [I: Interface]
  Legend: [H: Host], [F: Soft Flush] [!: Reject]

  Destination GenMask Gateway Flags Ref Origin UpTime Interface
  ---------- ------- ------- ----- --- ------ ------ ---------
  10.10.10.0 255.255.255.0 0.0.0.0 UCI 1 MANUAL 410777
  570d45550000000c

- Analyze NSX Edge statistics
  - Log in to the vSphere Web Client.
  - Click Networking & Security and then click NSX Edges.
  - Double-click an NSX Edge.
  - Click the Monitor tab.
  - Select the period for which you want to view the statistics.

Tools

- NSX Administration Guide
- NSX Command Line Interface Reference Guide
- NSX API Guide
- NSX Controller CLI
- NSX Edge CLI
- NSX API
- vSphere Web Client
- VDS Health Check
- net-dvr
- http://www.yet.org/2014/09/nsxv-troubleshooting/ - very useful for this section (it's where I've pulled a lot of the above from)

Objective 9.4 – Troubleshoot Common Connectivity Issues

Knowledge

- Review netcap logs for control plane connectivity issues
  - I believe this is a typo – should be netcpa logs

    ssh into the NSX controller and run:
    show log cloudnet/cloudnet_java-vnet-controller.log

    ssh into the ESX host and run:
    tail –f /var/log/netcpa.log

  - If you want to troubleshoot your User World Agent, you can increase the netcpa log level like this:

    Start by stopping the daemon
    # /etc/init.d/netcpad stop

    Enable write permisions on netcpa's config file:
    # chmod +wt /etc/vmware/netcpa/netcpa.xml

    Increase log level:
    # vi /etc/vmware/netcpa/netcpa.xml

    Change the XML's /config/log/level value to "verbose", save and restart netcpad
    # /etc/init.d/netcpad start

- Verify VXLAN, VTEP, MAC, and ARP mapping tables
  - VXLAN

    # show control-cluster vnet vxlan vni <vni>

    # esxcli network vswitch dvs vmware vxlan network list --vds-name=<VDS_NAME>
    VXLAN ID Multicast IP Control Plane Controller Connection Port Count MAC Entry Count ARP Entry Count MTEP Count
    -------- ------------------------ --------------------------------- -------------------- ---------- --------------- --------------- ----------
       5000 N/A (headend replication) Enabled (multicast proxy,ARP proxy) 192.168.110.202 (up) 1 1 0 0
       5004 N/A (headend replication) Enabled (multicast proxy,ARP proxy) 192.168.110.203 (up) 1 0 0 0

  - VTEP

    # show control-cluster vnet vxlan vtep-table <vni>

    # esxcli network vswitch dvs vmware vxlan network vtep list --vds-name=<VDS_NAME> --vxlan-id=<VXLAN_ID>

    # show control-cluster logical-switches vtep-records <ESXi_MGT_IP>

```
VNI     IP              Segment         MAC               Connection-ID
5001    192.168.150.51  192.168.150.0   00:50:56:60:6a:3a 2
```

- MAC

  # show control-cluster vnet vxlan mac-table <vni>

  # esxcli network vswitch dvs vmware vxlan network mac list –-vds-name=<VDS_NAME> --vxlan-id=<VXLAN_ID>

  # show control-cluster logical-switches mac-records <ESXi_MGT_IP>

- ARP

  # show control-cluster vnet vxlan mac-table <vni>

  # esxcli network vswitch dvs vmware vxlan network arp list --vds-name=<VDS_NAME> --vxlan-id=<VXLAN_ID>

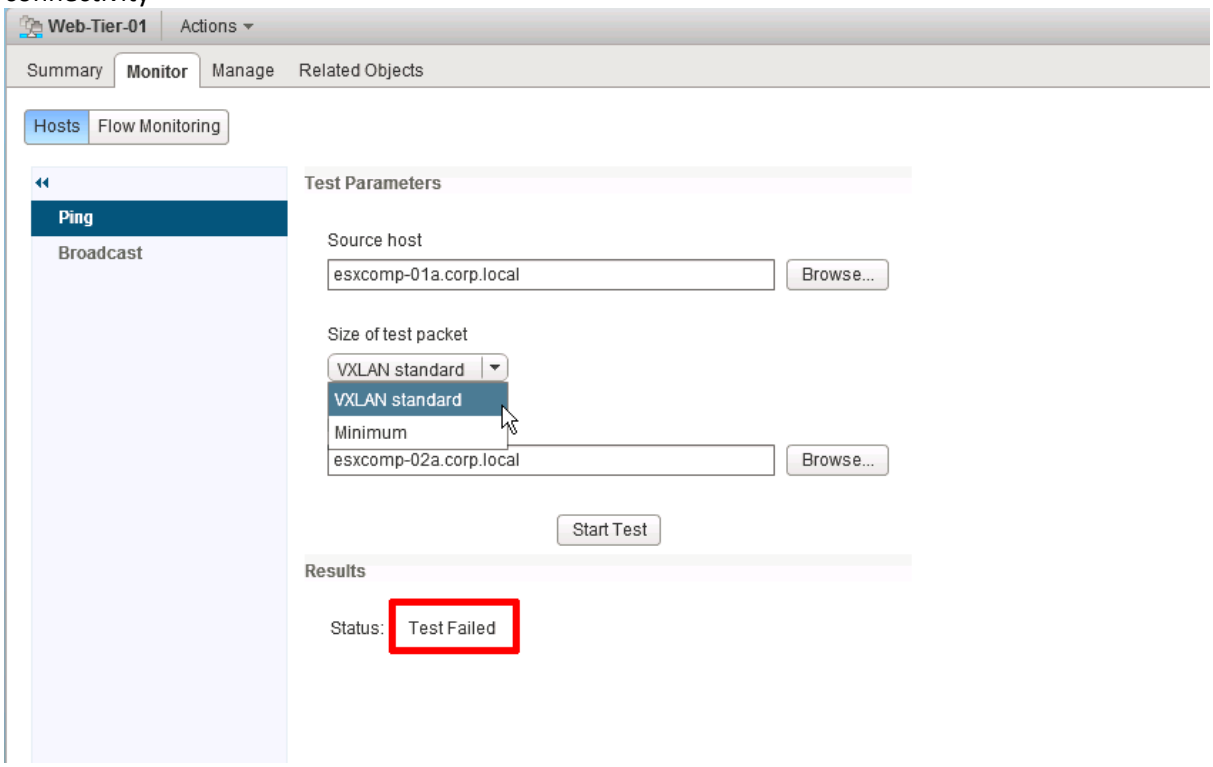
  # show control-cluster logical-switches arp-records <ESXi_MGT_IP>

- List VNI configuration
  - From the NSX Controller CLI
    - List
      # show control-cluster vnet vxlan vni –l
    - Display
      # show control-cluster vnet vxlan vni <vni>

- View VXLAN connection tables and statistics
  - Connection tables
    - # show control-cluster vnet vxlan connection-table <vni>
  - Statistics
    - # show control-cluster vnet vxlan vni-stats <vni>

- Perform VTEP connectivity tests

- At a logical switch level on the monitoring tab, use unicast or broadcast test to verify VTEP connectivity



Tools

- NSX Administration Guide
- NSX Command Line Interface Reference Guide
- vSphere Command-Line Interface Concepts and Examples
- NSX Controller CLI
- vSphere Web Client
- ESXi Host CLI
- esxcli
- http://www.slideshare.net/fullscreen/VMworld/vmworld-2013-operational-best-practices-for-nsx-in-vmware-environments
- And a big thanks to http://www.yet.org/2014/09/nsxv-troubleshooting/ again for this section.

Objective 9.5 – Troubleshoot Common vSphere Networking Issues

Knowledge

- Verify network configuration
  - Use host profiles where possible to ensure consistent configuration
  - Use vDS where possible to minimise configuration effort across multiple hosts
  - Check configuration of Port Groups / dvPort Groups
  - Check Load Balancing and Failover Policies
  - Check Security Policies (Promiscuous Mode, Forged Transmits etc)
  - Verify that VLAN settings are correct and consistent across a cluster

- Verify a given virtual machine is configured with the correct network resources
  KB1003893

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003893 is a good resource for this but as a start:

- Check that the network associated with the VM's vNIC exists, and the spelling is consistent across the infrastructure.
- Check that the "connected" checkbox for the vNIC is checked.
- Ensure the networking is configured correctly within the Guest OS
- Verify that the vSwitch has sufficient ports to support the VM
- Check the uplinks for the vSwitch are consistent (same VLANS)

- Troubleshoot virtual switch and port group configuration issues
  - Correct spelling of port group names is important and is case sensitive. Consistency of naming and Security Configuration is vital for the smooth running of the infrastructure.
  - Ensure switches are configured correctly (as per point 1) and with sufficient available ports.

- Troubleshoot physical network adapter configuration issues
  - Ensure all physical NICs assigned to a vSwitch are configured with the same speed, duplex and VLANs on the physical switch
  - If using IP Hash as the load balancing method, ensure Link Aggregation is configured on the switch.
  - You can use CDP or LLDP to assist with network troubleshooting, it will identify the switch ports that are connected to each pNIC.

- Identify the root cause of a network issue based on troubleshooting information
  - The root cause is likely to fall into one of 4 main areas:
    - VM
    - Port Group / vSwitch configuration
    - Host Uplinks
    - Physical Switch configuration
  - Use the above notes to assist with determining the area at fault – working from the VM down is probably easiest.
  - vmkping –D can be used to ping out through vmknics

Tools

- vSphere Networking Guide
- vSphere Troubleshooting Guide
- vSphere Command-Line Interface Concepts and Examples
- vSphere Web Client
- vSphere Client
- Some of the above has been pulled from VCP5-DCV study guides such as http://www.virtuallanger.com/2012/01/09/vcp-5-objective-6-2-perform-basic-vsphere-network-troubleshooting/ and http://blog.mwpreston.net/vcp-5/vcp-5-objective-6-2-perform-basic-vsphere-network-troubleshooting/

Exam Hints

Know the differences between vSS and vDS
Know what a VTEP is
Know what "MTU" means
Know what Multicast is and its limitations

VCP-NV 6.0 Study guide by Rich Dowling (@virtRich)

https://richdowling.wordpress.com

Know the upgrade path to NSX 6
Know the difference between traditional edge networking and the new world of distributed routers and firewalls
Know that you don't need vSphere to use NSX – you can run it over KVM and/or XEN and get the same network abstraction (using Openvswitch)
Know everything written in the design guide about Spine & Leaf
Do the VMware sample questions, treat as an open book exam