Dell EMC + VMware Cloud Infrastructure Platform for NFV

VMware vCloud NFV 1.5 - NFVI Solution

Service Provider Solutions Group
April 2017

Revisions

Date	Description
April 2017	Initial release

Table of Contents

1 Overview

This document provides guidance in deploying a Greenfield carrier cloud solution to run VNF workloads hosted on Dell EMC hardware virtualized with the help of VMware vCloud platform for NFV. In addition, vCloud platform helps manage the virtualized resources and monitor the hardware and software health during post deployment operations.

2 How to use this guide

This document assists telecommunication and solution architects, as well as sales engineers, field consultants, advanced services specialists, and customers who are responsible for telco cloud / NFV services or building an infrastructure to maximize the benefits of using the Dell EMC NFVI with VMware NFV bundle of solutions.

3 Dell EMC Hardware Requirements

VMWare vCloud NFV compute and storage resources need to be VSAN Ready. A complete and up-to-date list of VSAN Ready Dell EMC platforms is available at:

http://vsanreadynode.vmware.com/RN/RN?

Dell EMC PowerEdge R730		9 (min)
Components	CPU	Intel Xeon® E5-2680v3 2.5Ghz 2 sockets, 12 cores
	RAM	192 GB (128 GB min)
	HDD	2x600GB (800 GB min)
	SSD	1x400GB (1/3rd of HDD min)
	SD cards	2x16GB
	NIC	2x10G 2P Intel X520 1x1G 2P Intel I350 or 1x1G 4P BCM5720
Dell EMC Networking S6010		4
Dell EMC Networking S4048		1

Table 1 Dell EMC Hardware components

4 Software Requirements

4.1 VMWare

The table below lists all the mandatory components required:

Component	Version	ETSI Functional Block
VMWare ESXi	6.0 U2	NFVI
VMWare Virtual SAN Std	6.2	NFVI
VMWare vCloud Director for Service Providers	8.10	VIM
VMWare Integrated OpenStack	2.0.3	VIM
VMWare vRealize Operations Advanced	6.2.1	NFVI Operations Management
VMWare vRealize Log Insight	3.3.1	NFVI Operations Management
VMWare vSphere Replication	6.1.1	NFVI
VMWare vSphere Data Protection	6.1.2	NFVI Operations Management
VMWare vCenter Server	6.0.U2	VIM
VMWare NSX for vSphere	6.2.4	NFVI & VIM
VMWare Site Recovery Manager	6.1.1	NFVI Operations Management

Table 2 VMware software components

4.2 Miscellaneous

Component	Version	Description/Function
Java	NA	Any compatible version
vSphere client	6	Any compatible version with ESXi 6
DHCP server	NA	Optional Preconfigured DHCP server to service IP requests for ESXi and other applications
DNS server	NA	Optional DNS server to resolve various hosts, VMs and applications.
NTP server	NA	Optional to start deployment, best practice is to have a dedicated NTP server

Table 3 Miscellaneous software components

4.3 License Requirements

Application	Quantity
ESXi	Number of CPU sockets
VSAN	Number of CPU sockets
NSX	Number of CPU sockets
vCenter Server Appliance	Number of instances
vCloud Director	Number of VMs
vRealize Operations manager	Number of VMs
vRealize Log Insights	Number of CPU sockets
SQL Server Enterprise edition	1 SQL server license

Table 4 License Requirements

5 Reference Architecture

5.1 Logical topology

VMware vCloud NFV architecture is based on three Clusters: Management, Edge and Resource. It is recommended that each cluster have minimum of four nodes. All the clusters are based on VSAN storage and require homogenous NFVI within the same cluster.

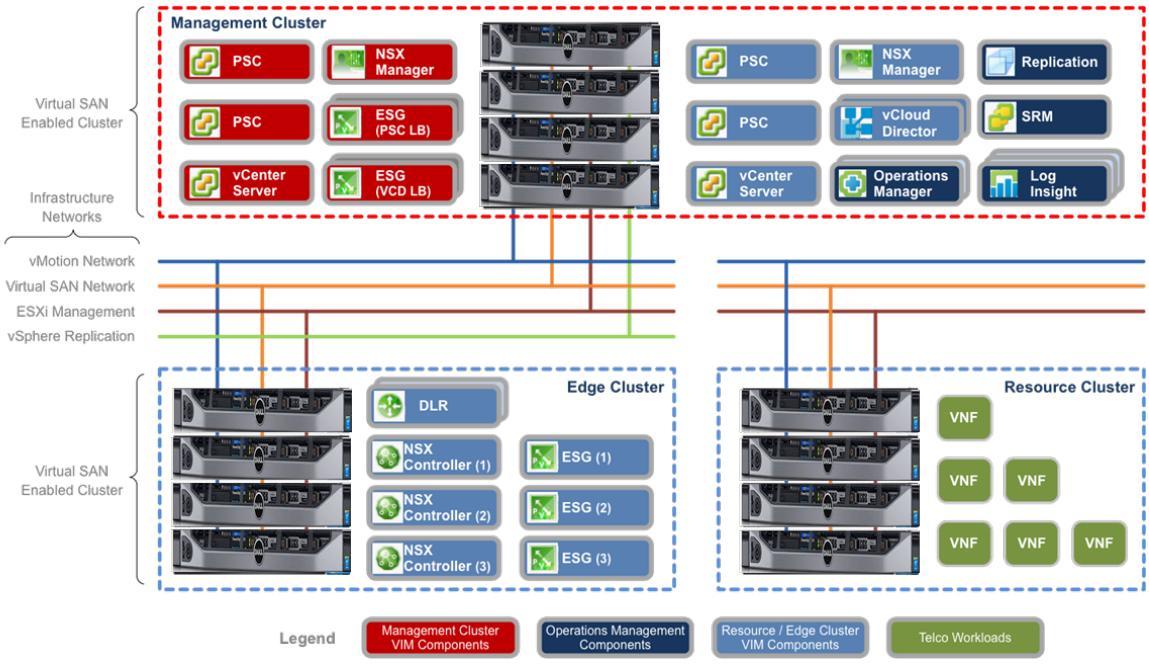

Figure 1 VMware Cluster design

5.2 Physical Topology

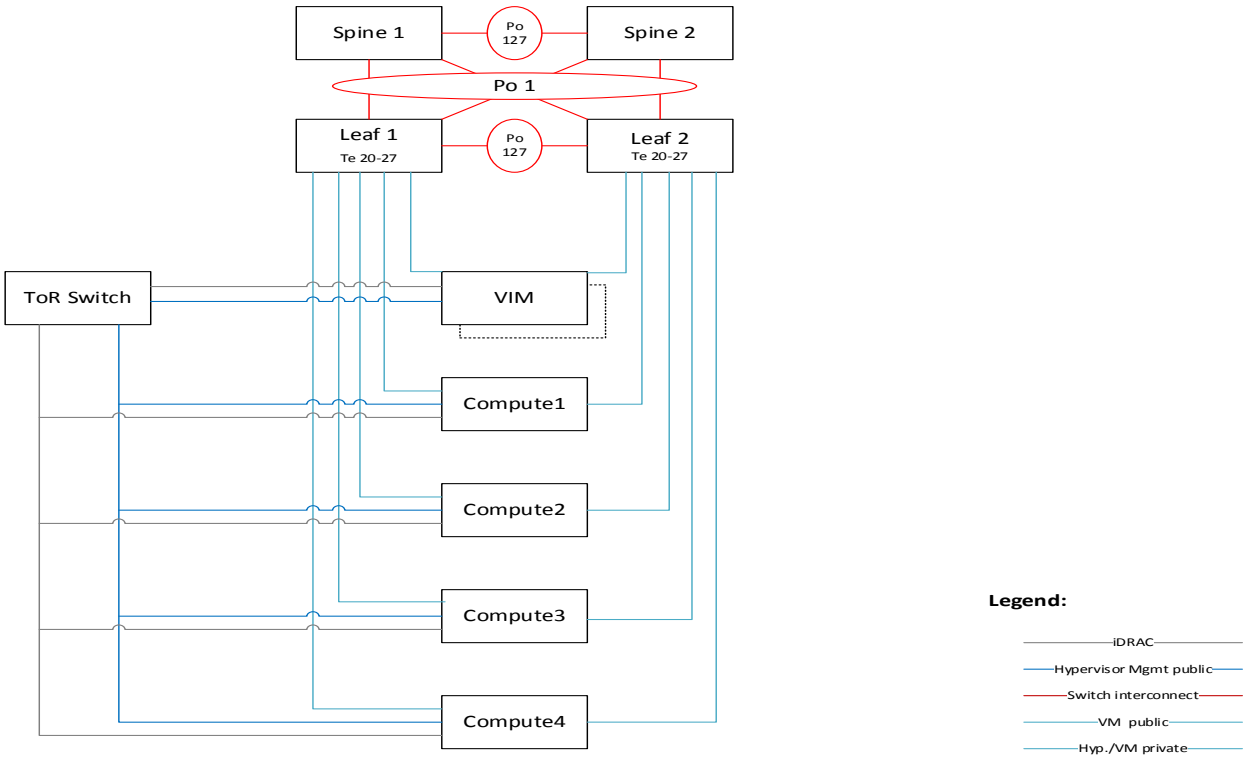

Figure 2 VMware Block design

6 VMWare virtualization platform

The following are the steps required to bring up the VMWare virtualization platform.

6.1 Install ESXi on Servers

ESXi Hypervisors need to be installed in the physical server harddisk. The hard disk in which ESXi hypervisors are installed cannot be used by storage clustering applications like VSAN. To avoid losing hundreds of GBs of standard disk storage for clustering, installing the hypervisors on the internal SD card module is recommended.

6.1.1 Verify the SD card module is present

Not all servers come with internal SD card modules. So before proceeding with the installation, make sure internal SD card modules are installed in the system. To verify this, launch iDRAC and enter system setup. Navigate to S**ystem BIOS → Integrated Devices**

Default iDRAC Username : root Password : calvin

Under Integrated Devices, verify you see SD card related fields are present. If these fields are missing, then the host does not have a SD card controller or SD cards in it.

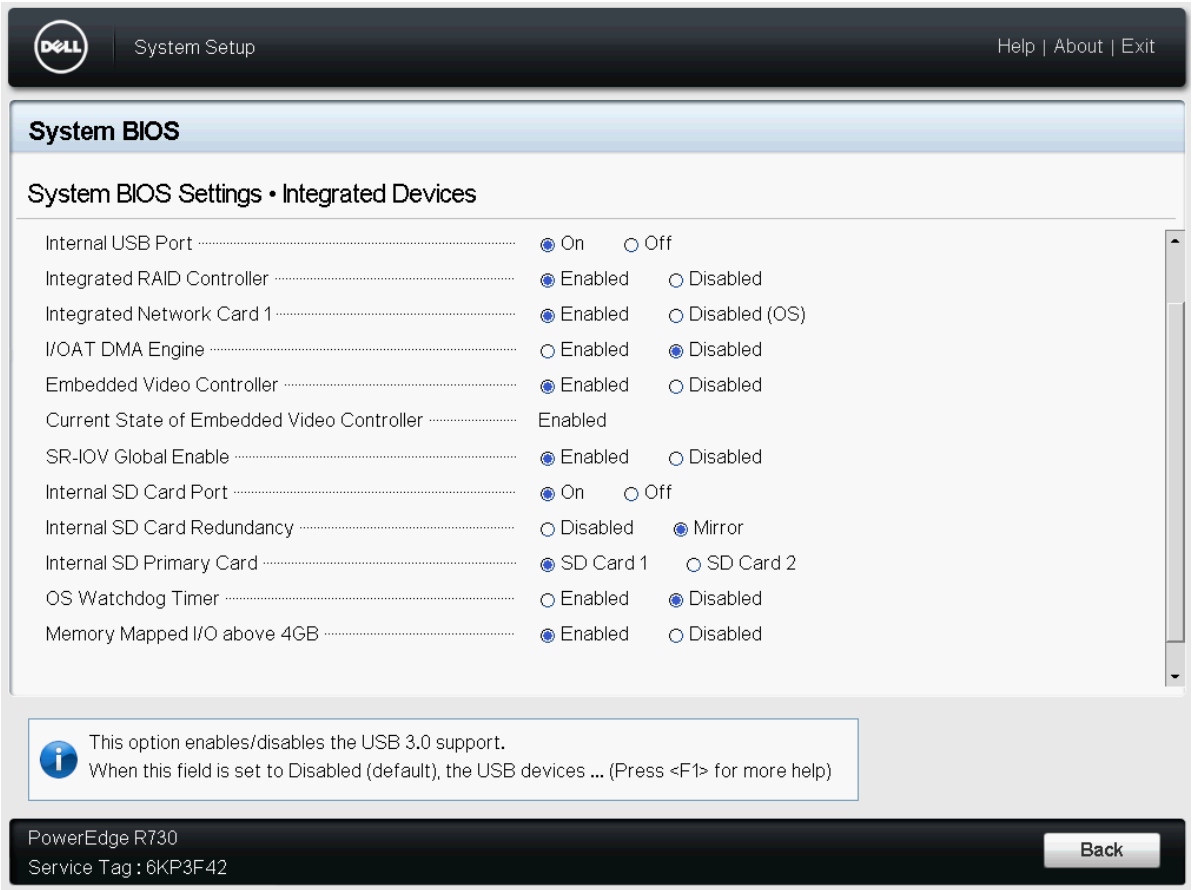

Figure 3 System BIOS Settings

6.1.2 Set the boot sequence to boot the device from SD card

By default, most systems will be set to boot from the HDD or SSD drives. When you install ESXi on the SD card the system may not boot from this partition. To remedy this issue, it is necessary to set the boot parameters properly under the **System BIOS → Boot setting → BIOS Boot Settings → Hard-Disk Drive Sequence**.

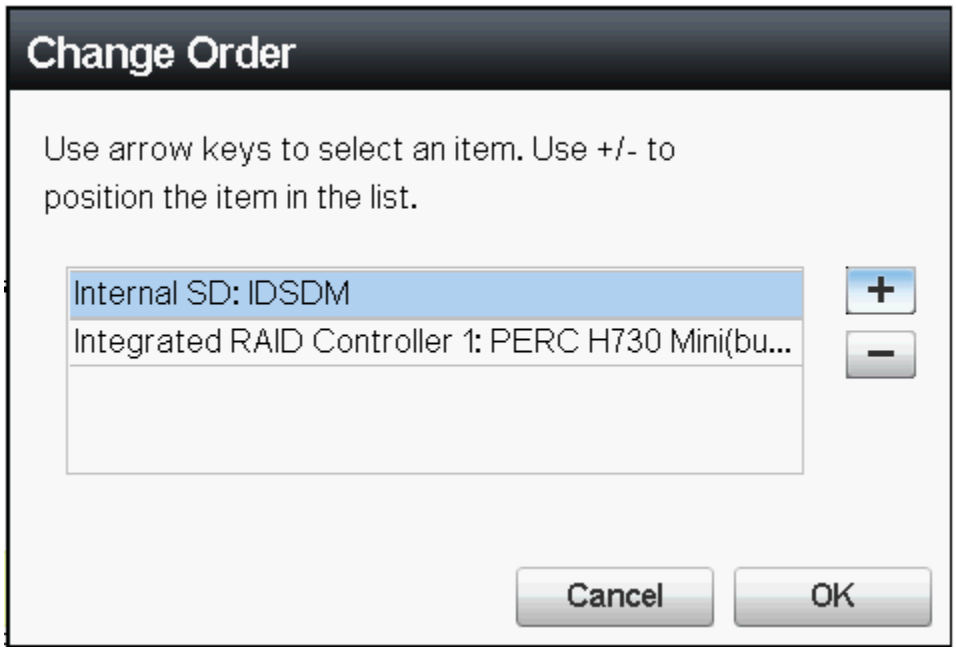

Figure 4 Change Order Dialog Box

6.1.3 Use Vmware ESXi installer to install the hypervisor

Either using the CD drive in the server or with an ISO image start the ESXi installation process. With the ISO image, in the iDRAC, connect virtual media and click Map CD/DVD from the local drive. Point to the local ISO image file. Set the **Next boot option** to boot via virtual CD/DVD/ISO and reboot the system. Choose the installer option as shown below and continue with the installation process.

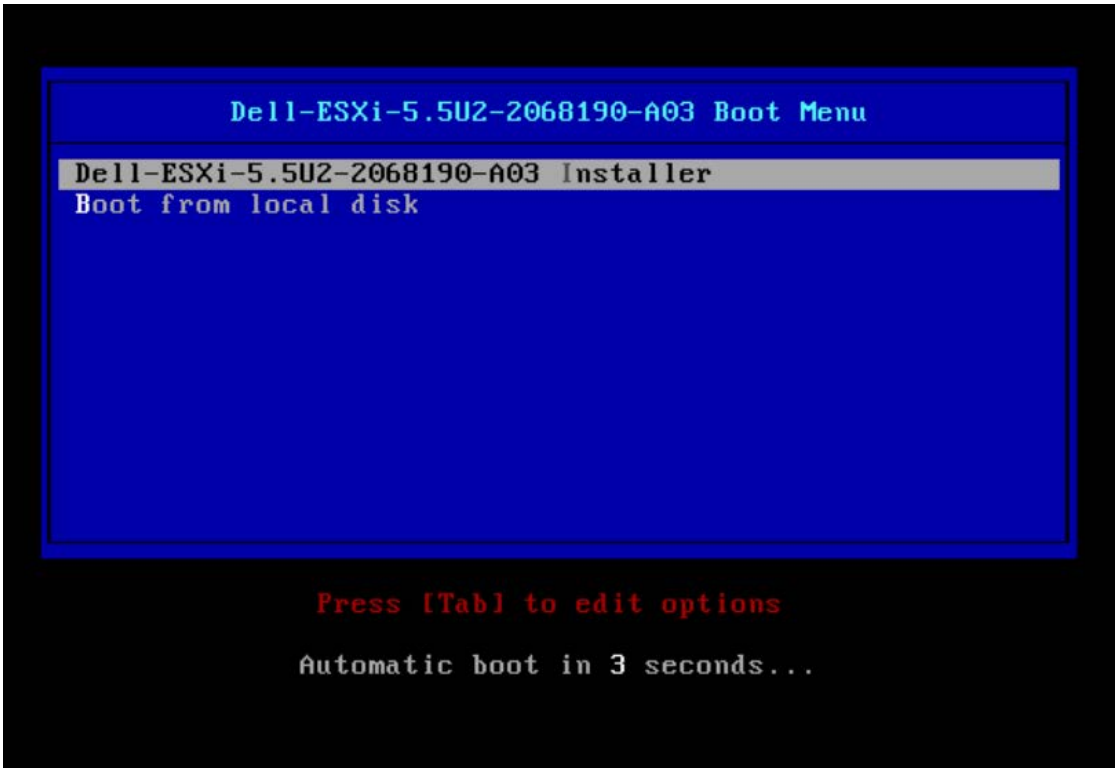

Figure 5 Dell ESXi Boot Menu

Make sure you are installing the ESXi hypervisor in the SD card of the server.

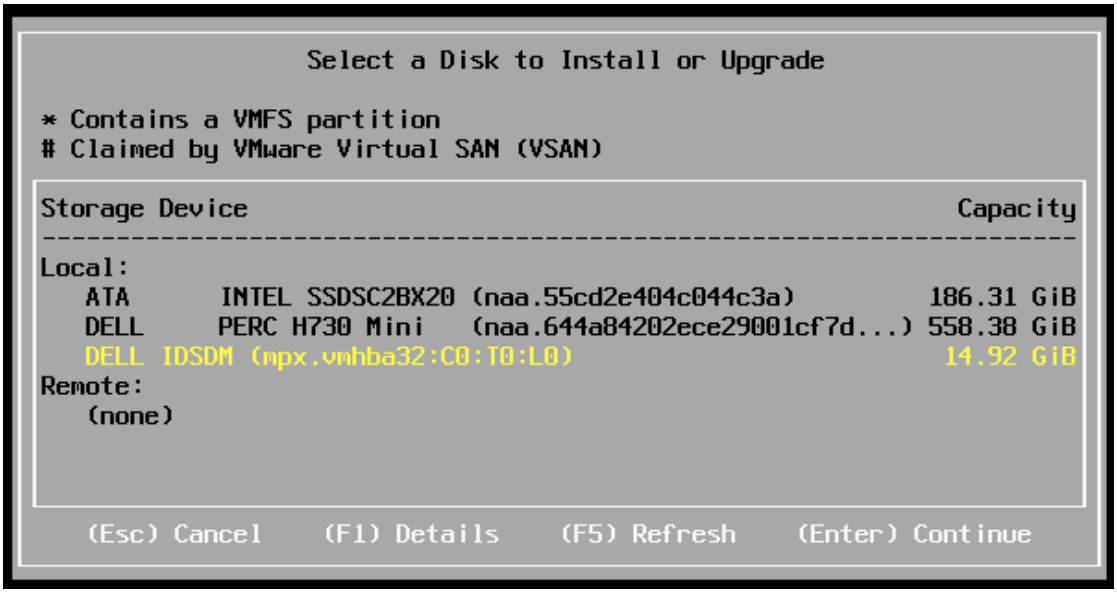

Figure 6 Confirm SD card is selected

During the installation process, configure the root user password for the hypervisor of your choice. Be sure to configure same password across all the ESXi installations. So the hosts can be added to vCenter with a consistent process.

Figure 7 Enter root password

Repeat this process for all the servers in the setup.

6.1.4 Configure the management interface

Post installation, it is necessary to configure the management IP address for the hypervisors, which will be managed by vSphere client. By entering the root username/password configured during installation, the user should be able to login and configure the hypervisors. Navigate to **Configure Management Network**, Under **Network Adapters**. Choose the NIC interface that will be acting as the management interface from the list of available NICs. Configure Vlans for the management port (if any). If a DHCP server is not providing the IP address, choose static configuration and assign a management IP address to the server and repeat the same process for all the servers.

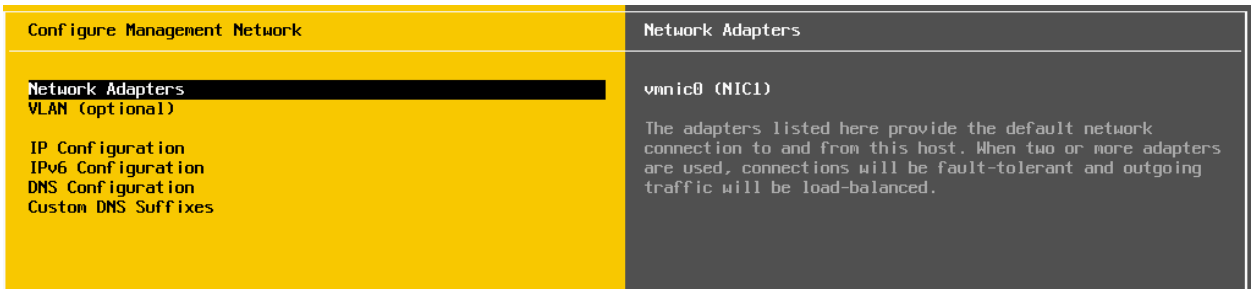

Figure 8 Configure Management Network

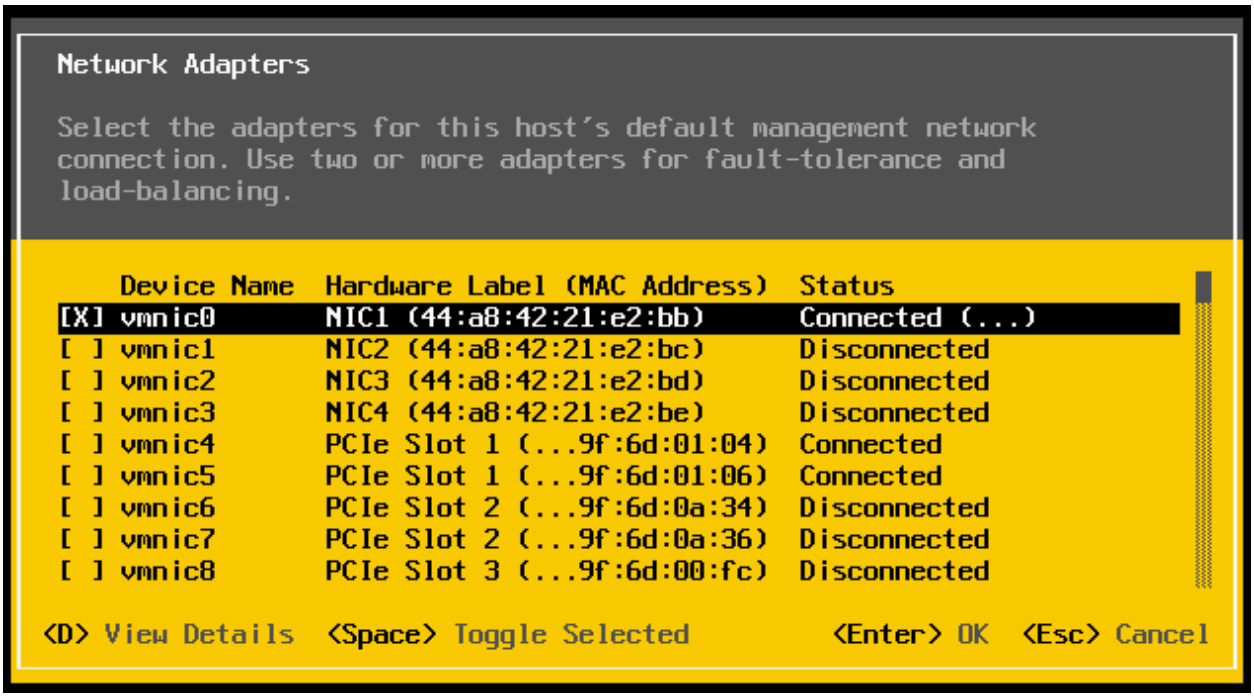

Figure 9 Select management network connection

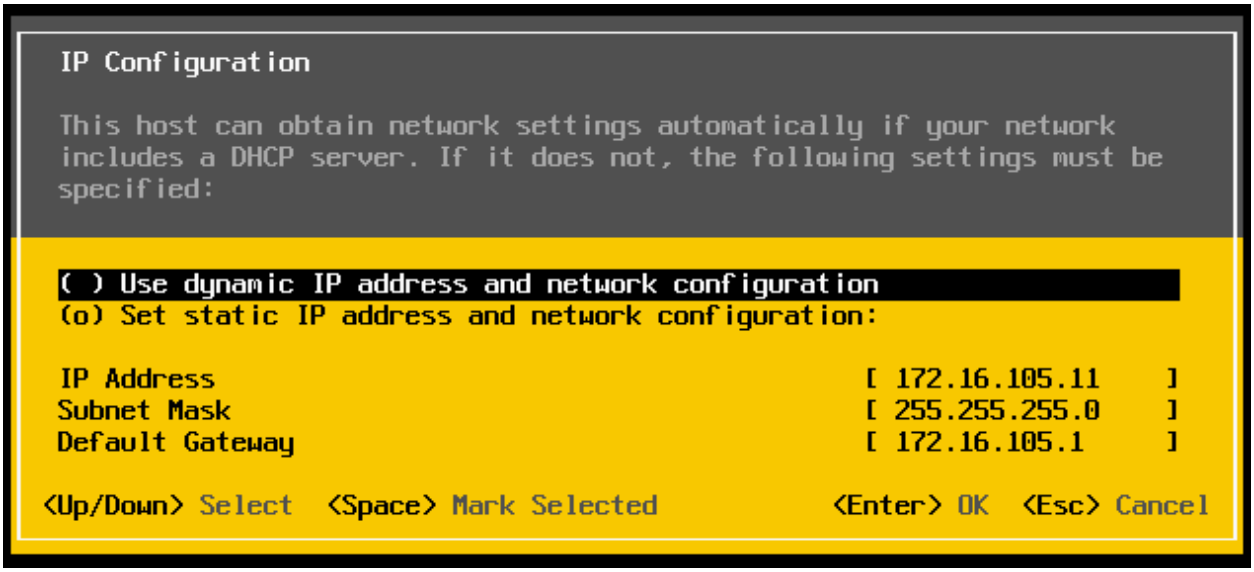

Figure 10 IP Configuration

6.2 Install vCenter Server

Installation of vCenter server 6 is a two-step process. We need to install External platform services controller (EPSC) and vCenter server appliance. EPSC is used for various backend services and all the user interactions to the vCenter will go through the vCenter server appliance only. As shown in the VM placement diagram, we need to deploy two sets of vCenter Server one to manage the VIM cluster and another to manage the Compute & Edge cluster.

6.2.1 Mount VCSA ISO

Confirm you have access to the management IP addresses of the hypervisors. In a virtual CD drive, load the 'VMware-VCSA-all-6.0.0-3040890' ISO image. Browse to the virtual CD drive and click vcsa-setup.html. If the browser prompts for a missing plugin, install the plugin and restart the process. In the browser, click **Install**.

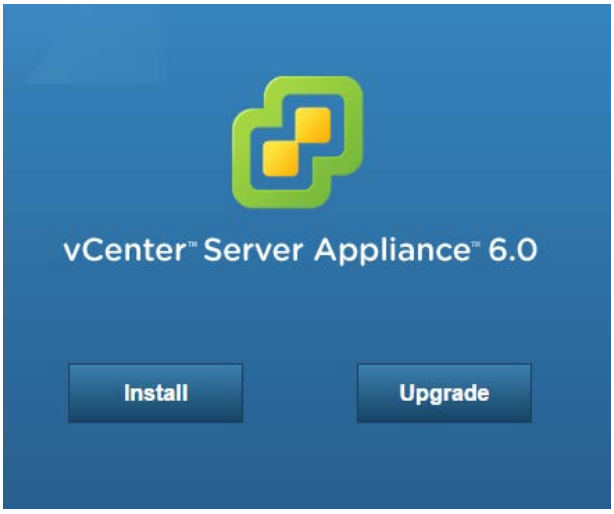

Figure 11 vCenter Server Appliance install

6.2.2 Install External PSC

Enter the IP address of one of the hosts that will be part of VIM cluster. Enter the ESXi root username/password and click **Next**.

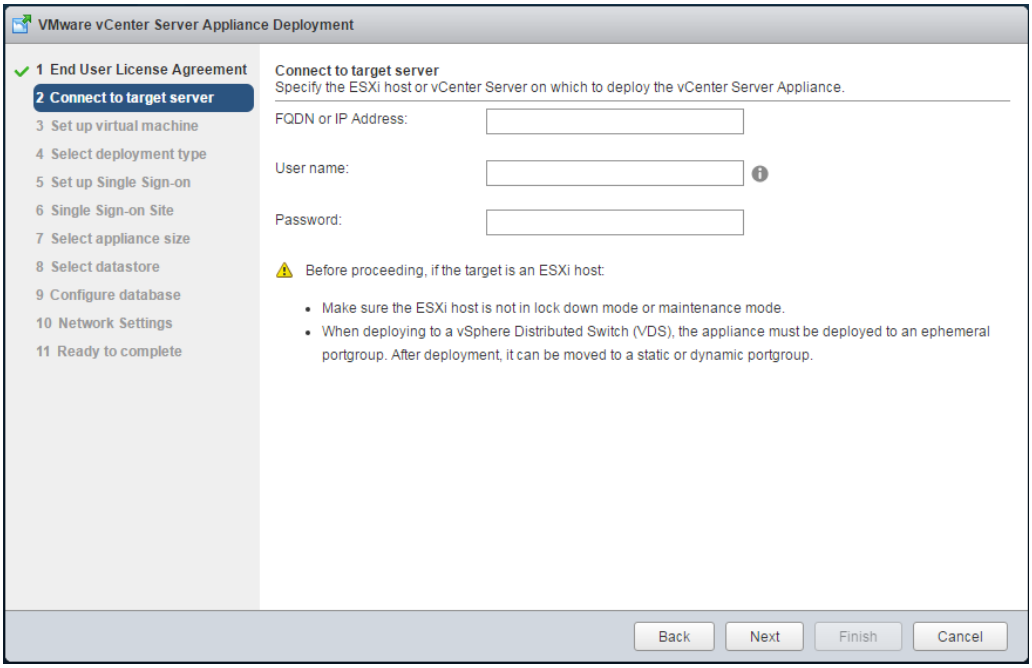

Figure 12 Connect to target server

For the first deployment, we will deploy EPSC/vCenter for VIM. In the second installation, we will deploy the Compute and Edge. Name the appliance and configure root password of choice for each deployment.

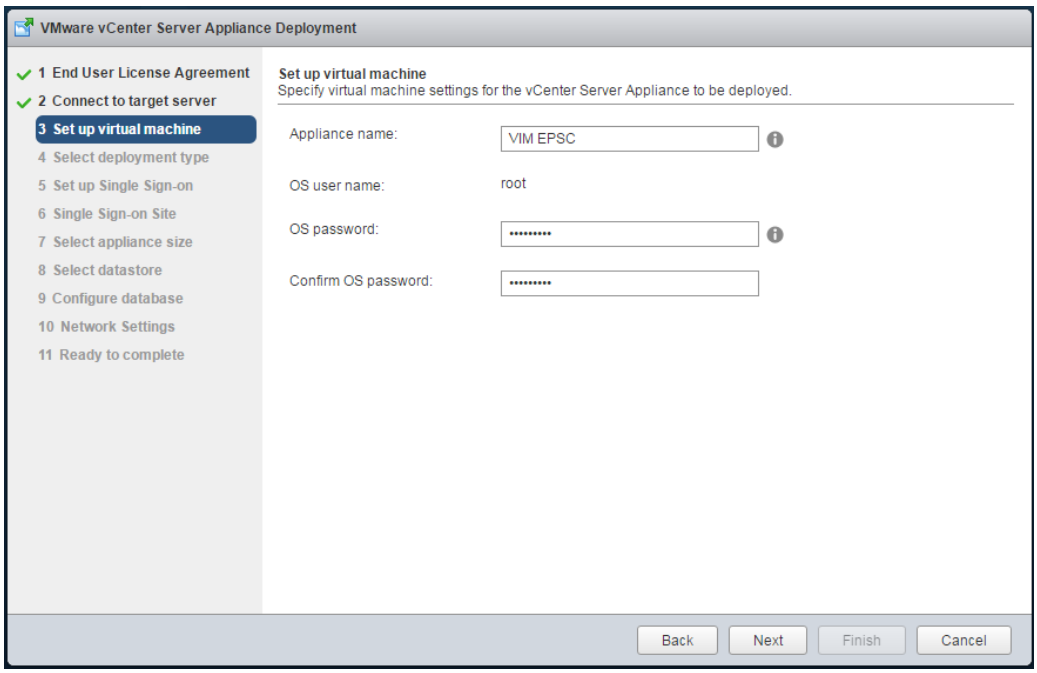

Figure 13 Set up virtual machine

Choose EPSC as show below.

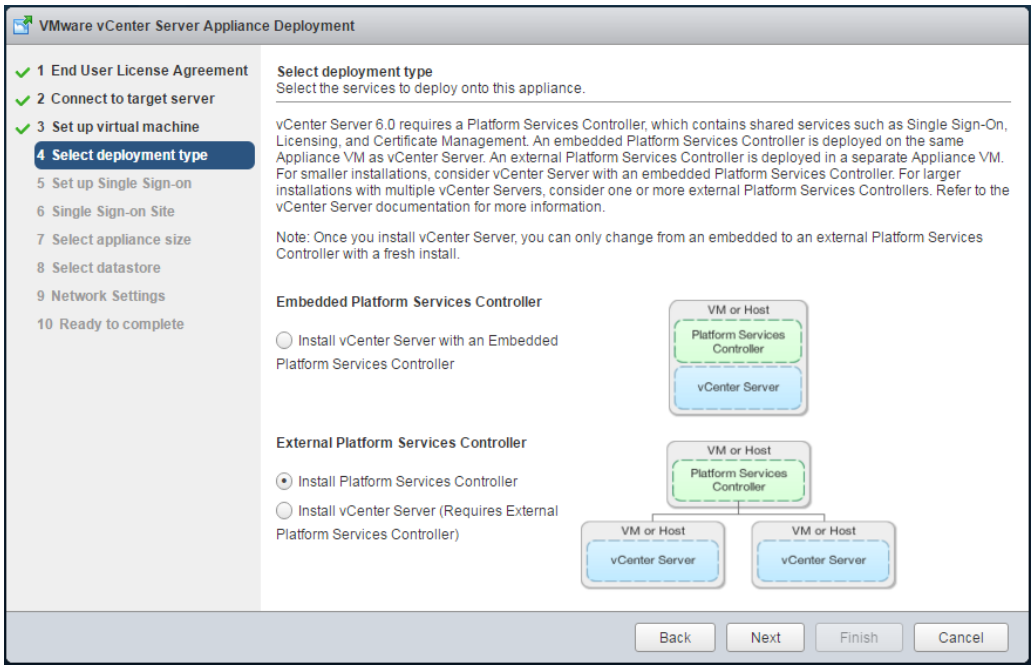

Figure 14 Select deployment type

Configure SSO with authentication password of your choice, domain name and site name.

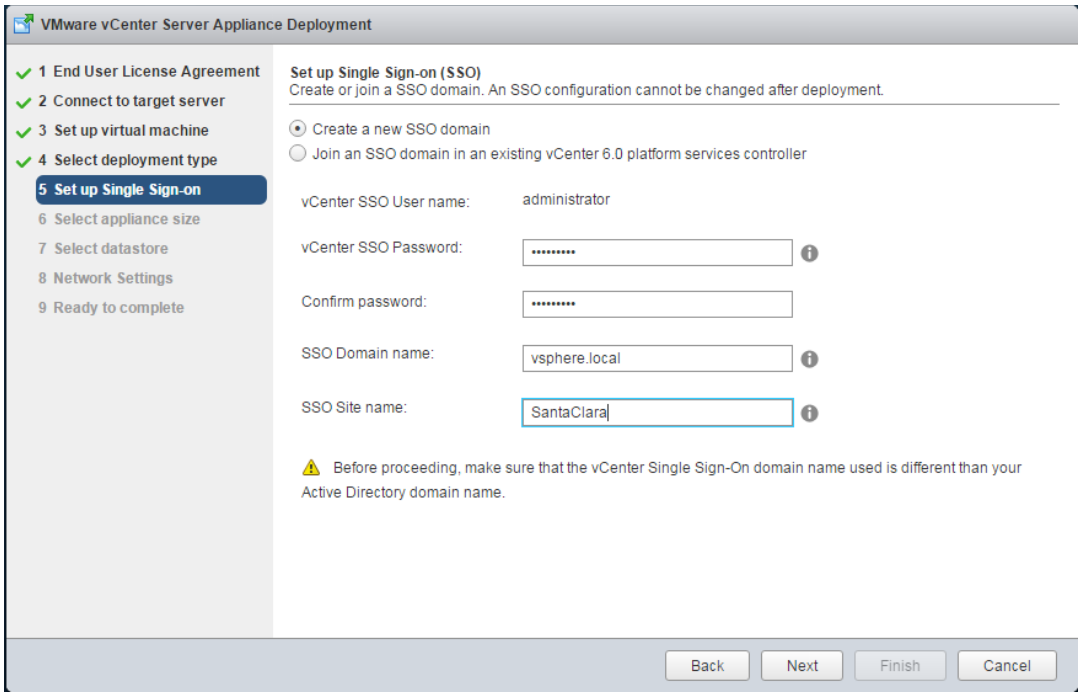

Figure 15 Set up Single Sign-on

Select the host datastore in which the user wants to deploy the VM and click Next.

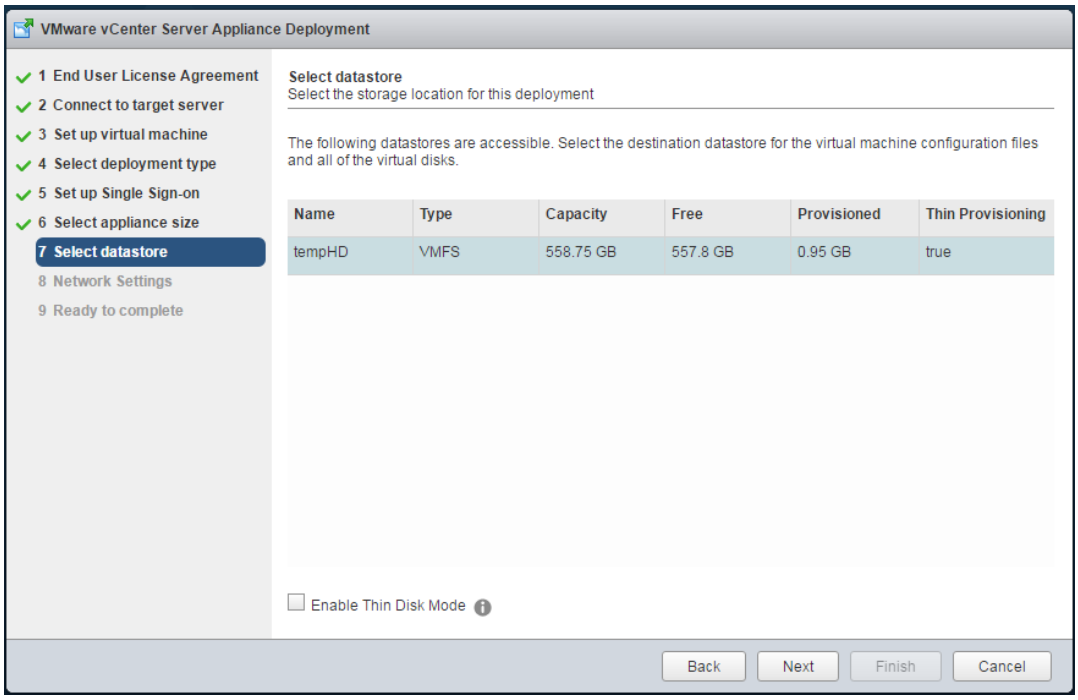

Figure 16 Select datastore

Configure the network settings for the vCenter server using a static configuration or through a DHCP server. Enter a system name if a DNS server is already configured. Use the ESXi host to synchronize time if no NTP server is configured.

Note: Do not enter a system name without configuring a DNS Server on the network.

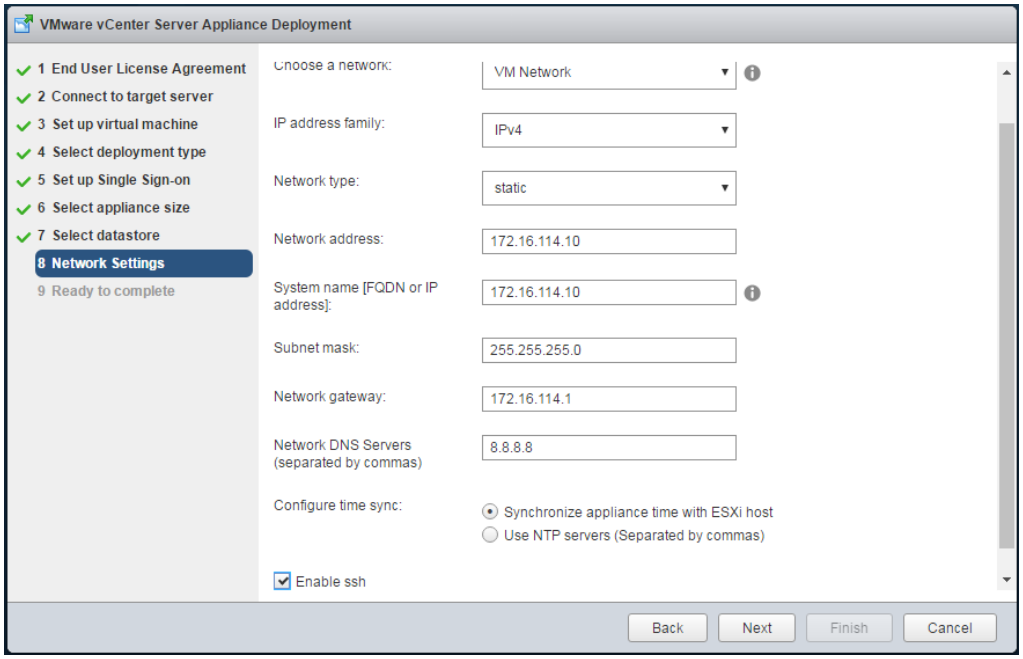

Figure 17 Network Settings

Verify the configuration, click **Finish** and wait for the ESPC to deploy fully. Deploying the EPSC will take up to 10 minutes.

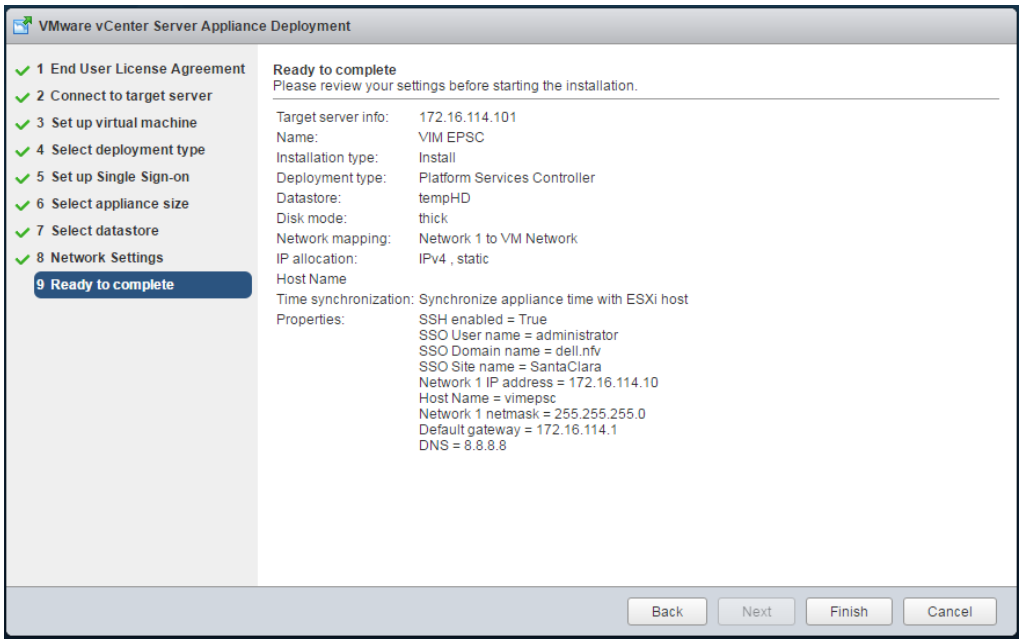

Figure 18 Complete installation

6.2.3 Deploy the vCenter appliance

After the EPSC installation is complete, restart the installation to deploy vCenter server appliance. Provide a different host IP address in the VIM cluster to deploy vCenter. This is a best practice to ensure anti-affinity, not a strict requirement.

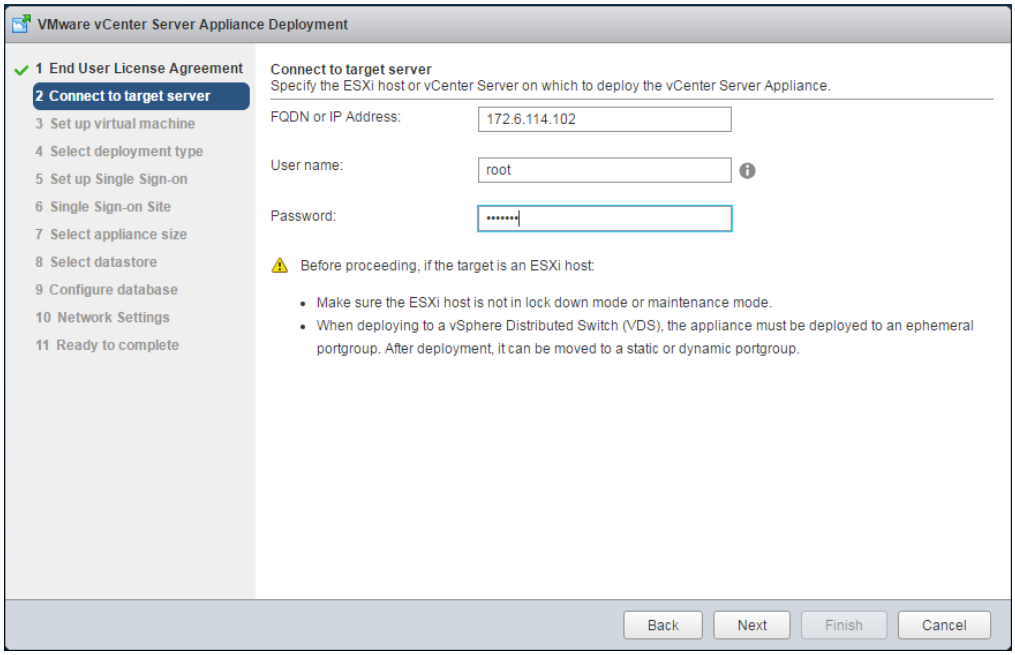

Figure 19 Connect to target server

Configure the vCenter appliance name.

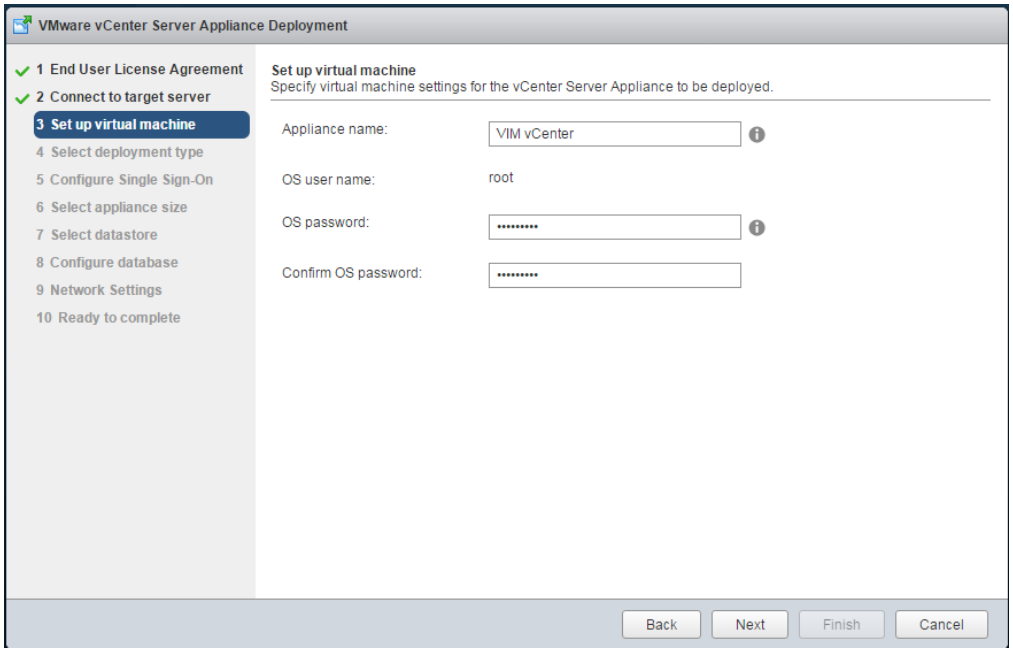

Figure 20 Set up virtual machine

After configuring the root password (typically same as ESPC) select the vCenter server install instead of PSC.

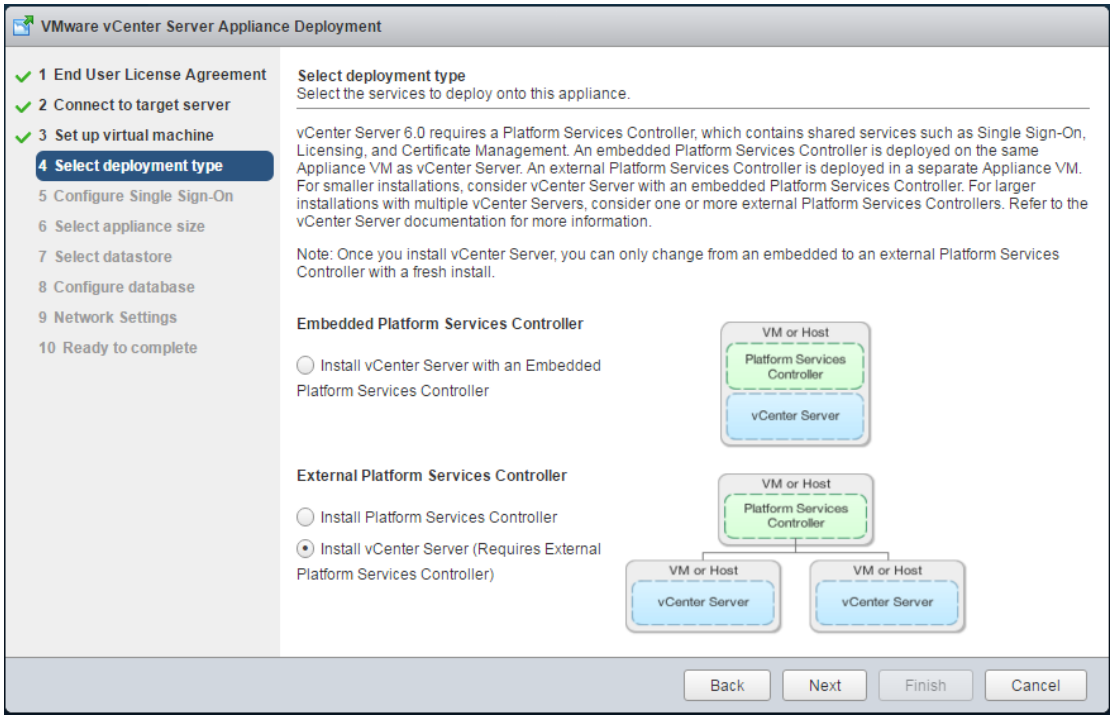

Figure 21 Select deployment type

Configure the EPSC SSO password to authenticate vCenter.

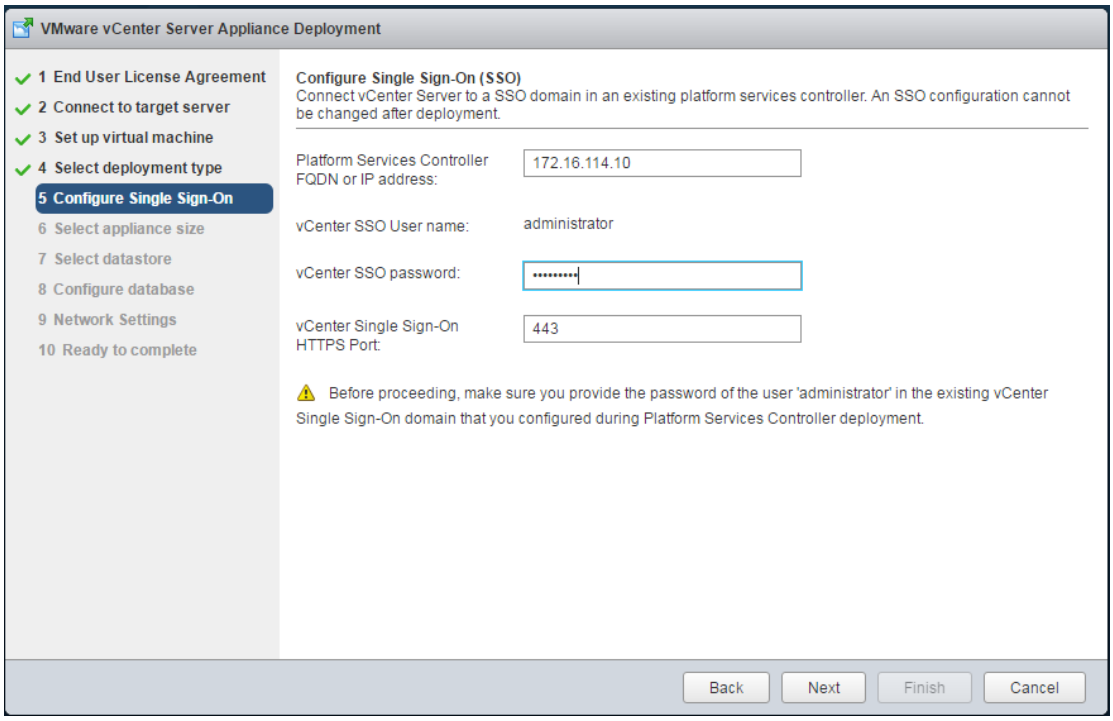

Figure 22 Configure Single Sign-On

Based on the deployment size, chose the appliance size.

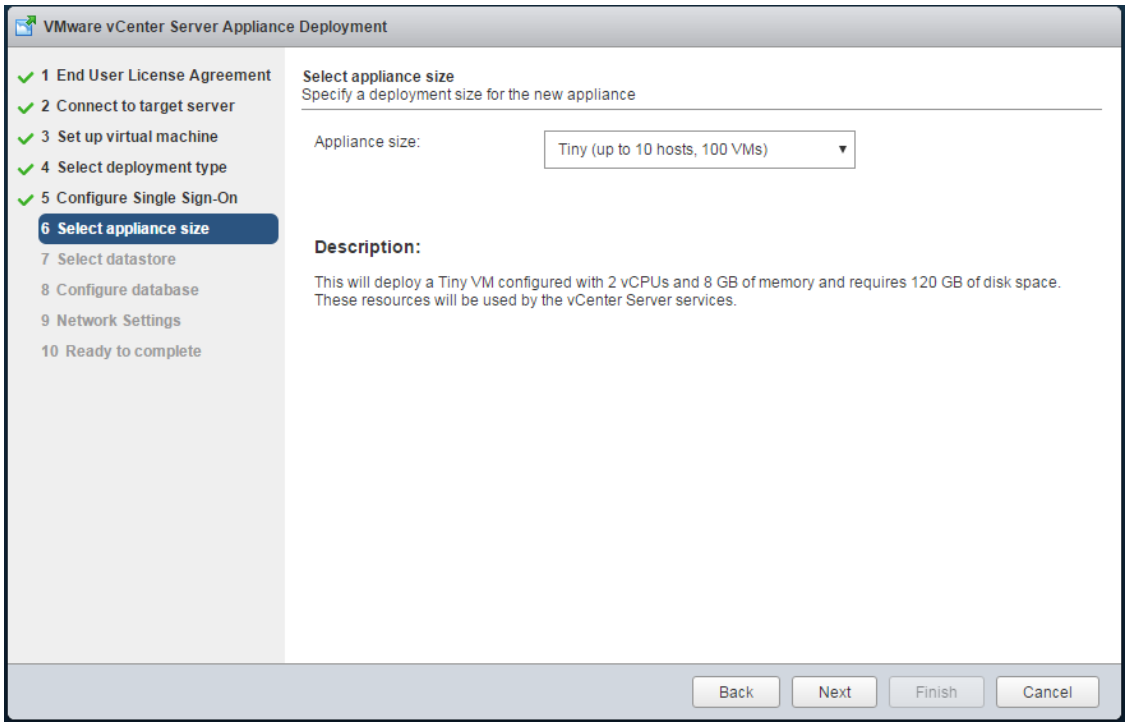

Figure 23 Select appliance size

Use the embedded database and configure the Network settings.

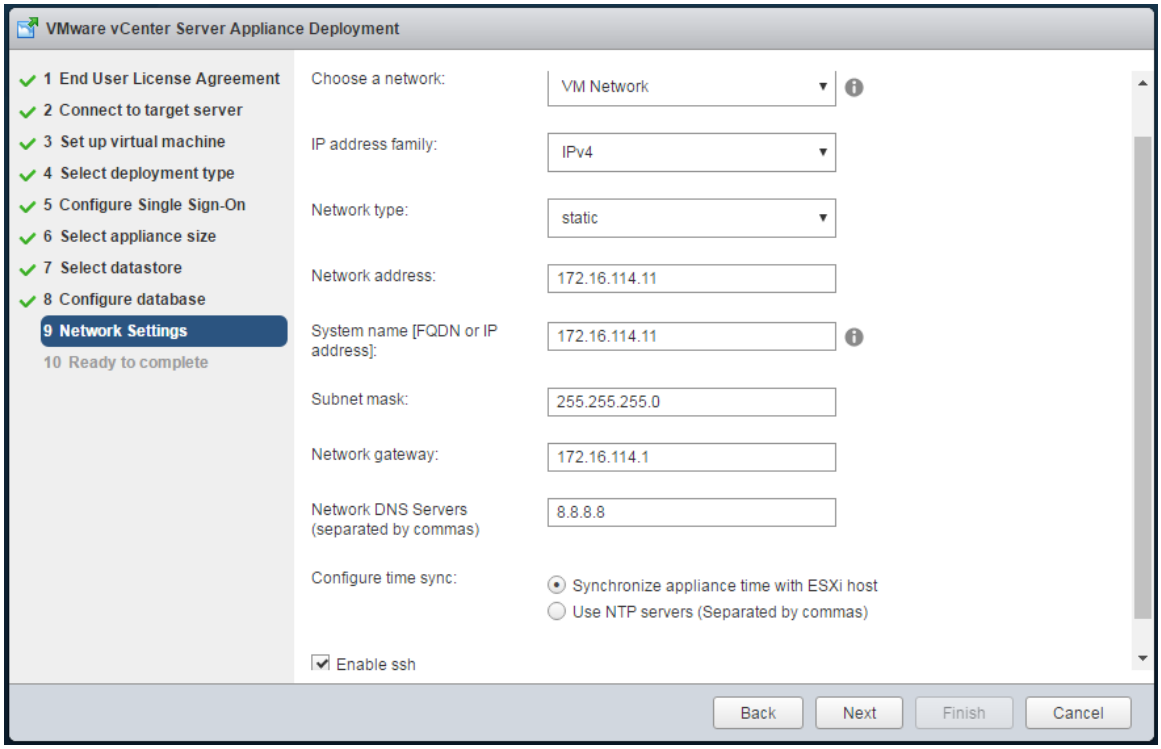

Figure 24 Network Settings

Review the configurations and click **Finish**. Wait for vCenter appliance to deploy, which will take up to 10 minutes.

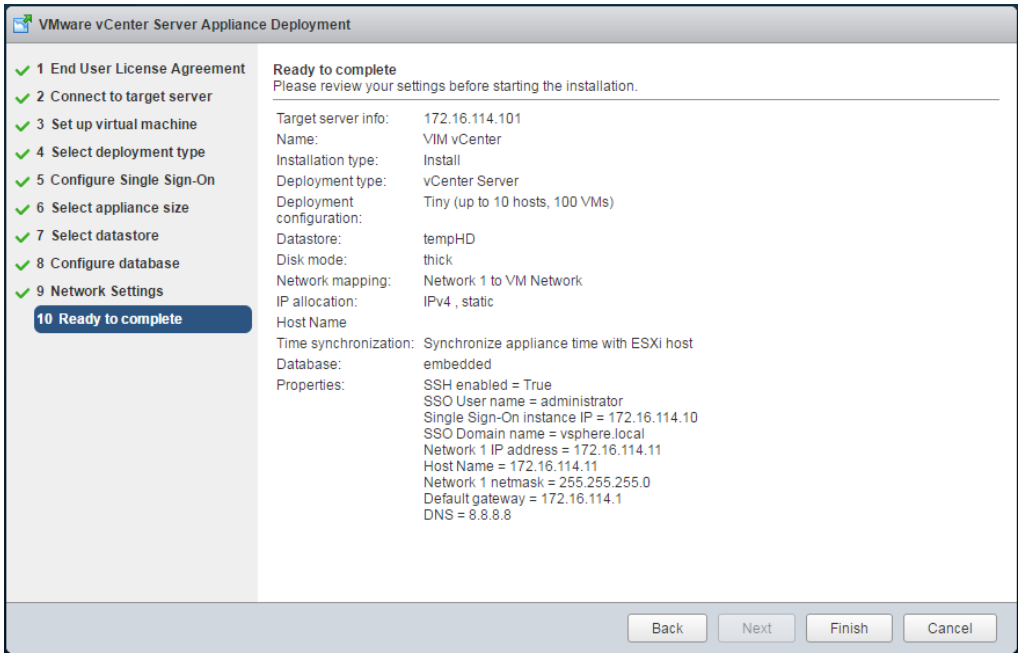

Figure 25 Complete installation

Once the installation is complete, login to vSphere web client with the URL provided post installation.

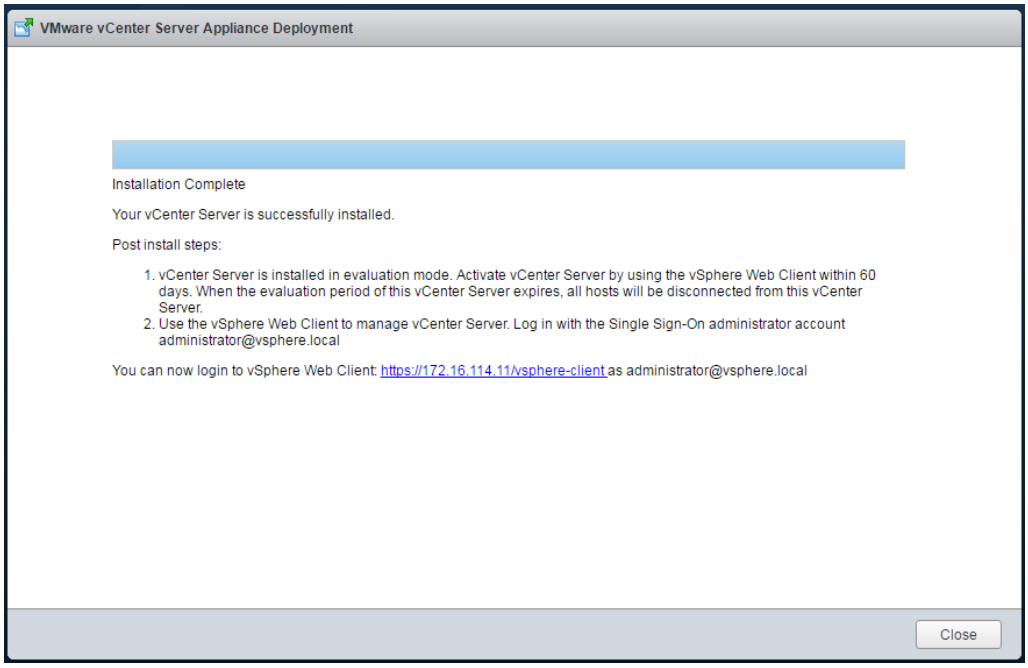

Figure 26 vSphere web client URL

6.2.4 Deploy second EPSC and vCenter

Once the first vCenter is fully deployed, restart the EPSC and vCenter installation and deploy the second instance of vCenter to manage Compute and Edge clusters. Make sure to install the application on a different host that is part of the VIM cluster.

The following figures show the final Compute EPSC and vCenter Server configurations for review before deployment.

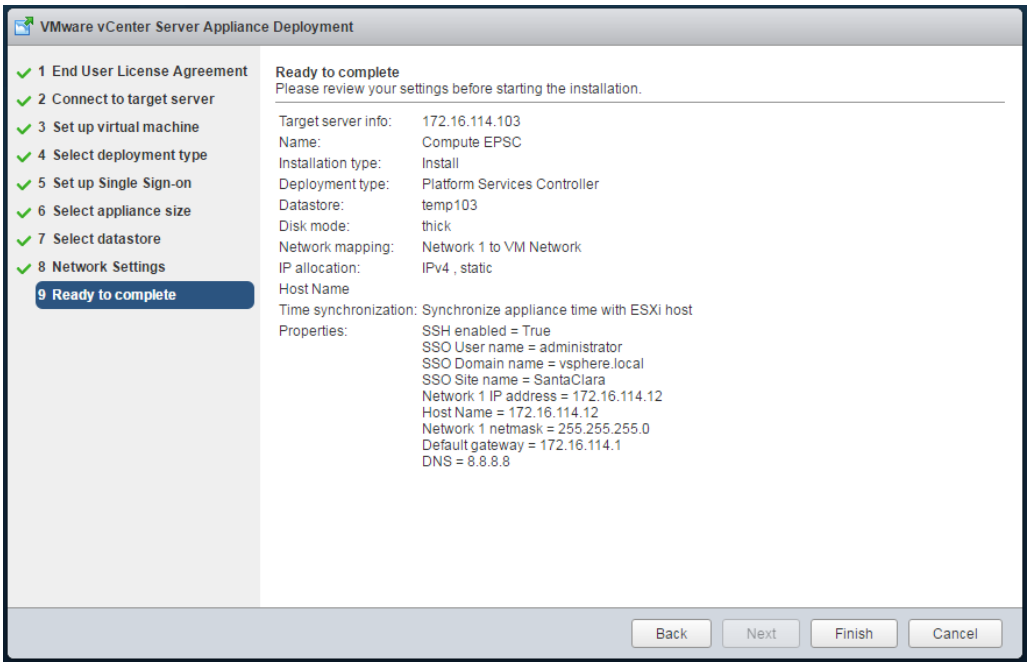

Figure 27 EPSC configuration

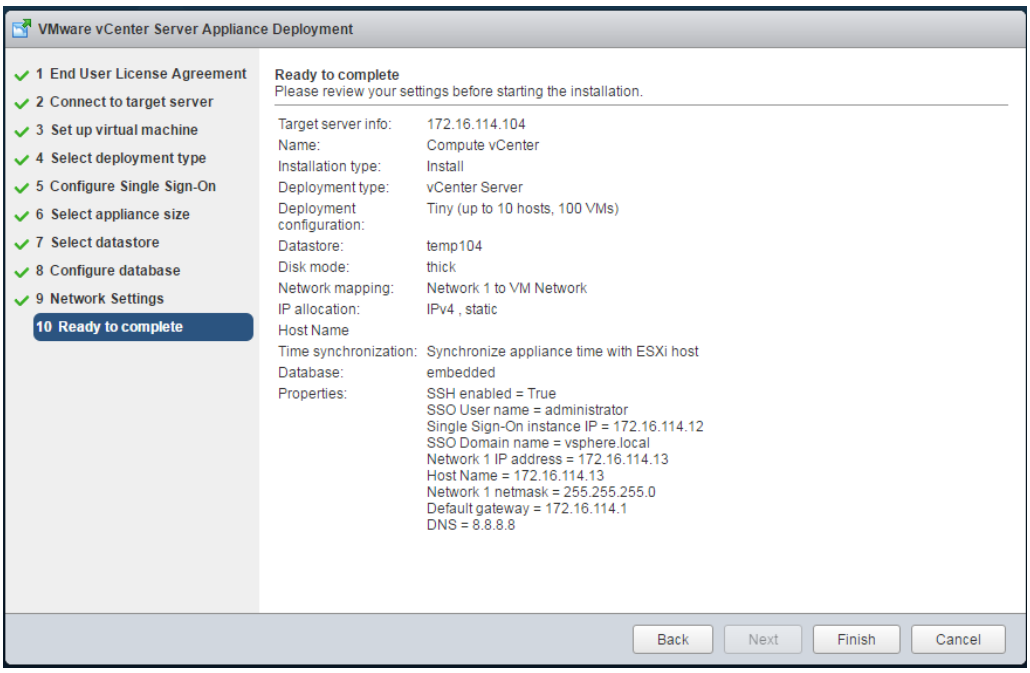

Figure 28 Compute vCenter configuration

6.3 Build datacenter

Once the the vCenter appliance is deployed successfully, all the data center resource components (compute, storage and networking) Can be managed using the vmware vSphere web client. The URL for the web client is: https://<vcenter-appliance>:9443/vsphere-client/

6.3.1 Add Licenses

Before we adding hosts to create the data center, add the following four licenses to vCenter application as follows. V

- Center license for the vCenter appliance
- vSphere Enterprise plus license for the total number of CPU cores that could be managed via vCenter
- VSAN license for managing server datastores
- NSX license for managing host VxLAN networking.

From the home screen click, **Administration → Licenses**. Under the License Keys tab, Click on the (**+**) sign to add the License keys.

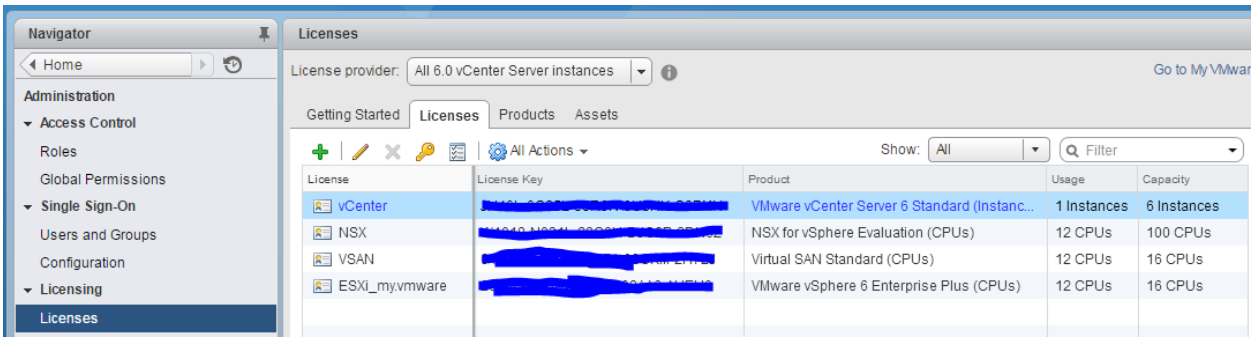

Figure 29 Add license keys

Repeat this exercise for both VIM vCenter and Compute vCenter

6.3.2 Create datacenter and clusters

Login to the VIM vCenter appliance and navigate from the **vCenter home screen → Host and clusters**. Click the vCenter IP and create a new data center with the name of your choice. Create the various clusters as needed. In the VIM vCenter we will create VIM cluster only. In the Compute vCenter we will create two clusters (Compute and Edge). Do not enable vSphere HA, vSphere DRS and VSAN in this step.

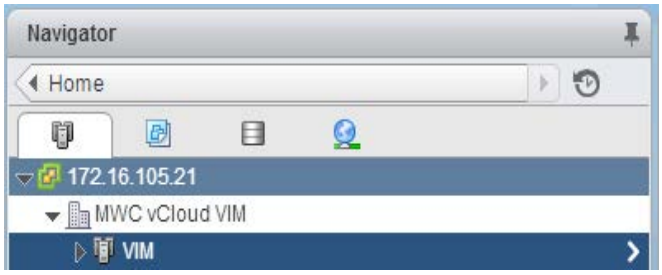

Figure 30 VIM

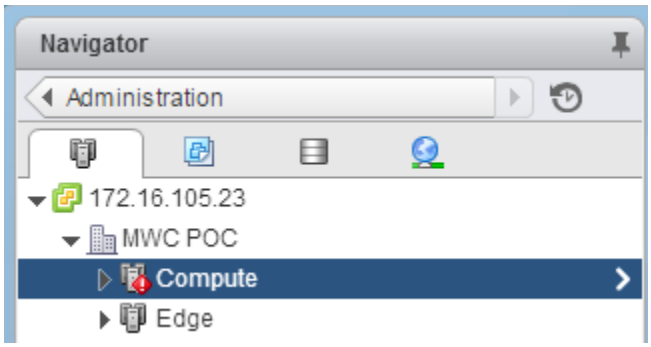

Figure 31 Compute and Edge

6.3.3 Add Hosts to clusters

Under each respective cluster, click on Add a host to add ESXi hypervisor installed hosts to the clusters. Use the license keys installed earlier to the hosts when needed. Follow the following six steps process to add a host to a cluster.

1. Enter the IP address of the host
2. Enter the login credentials (Provided during ESXi installation)
3. Review Host summary page
4. Assign License
5. Lockdown mode (Leave this unchecked)
6. Ready to complete

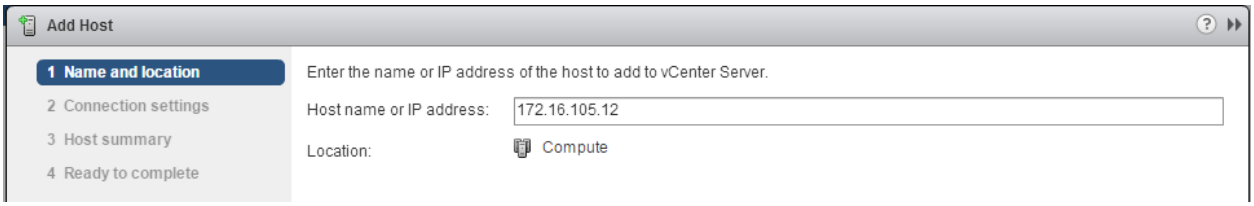

Figure 32 Enter the IP address of the host

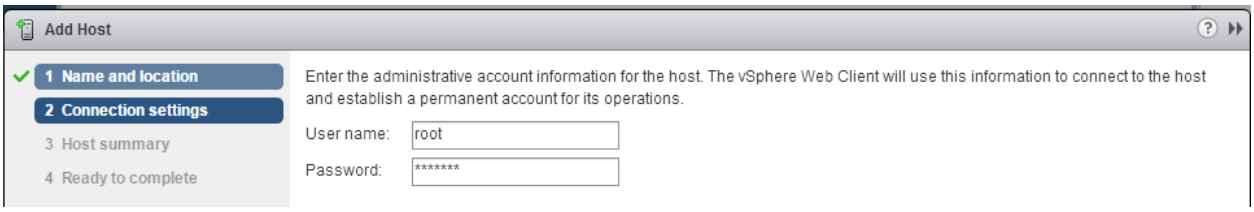

Figure 33 Enter the login credentials (Provided during ESXi installation)

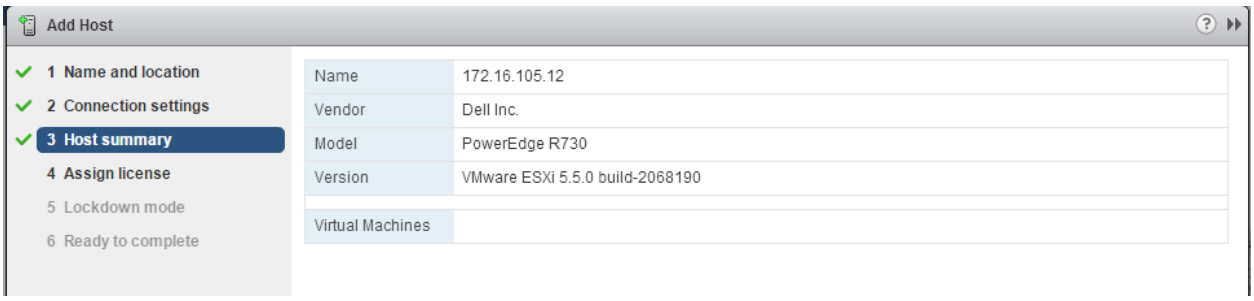

Figure 34 Review Host summary page

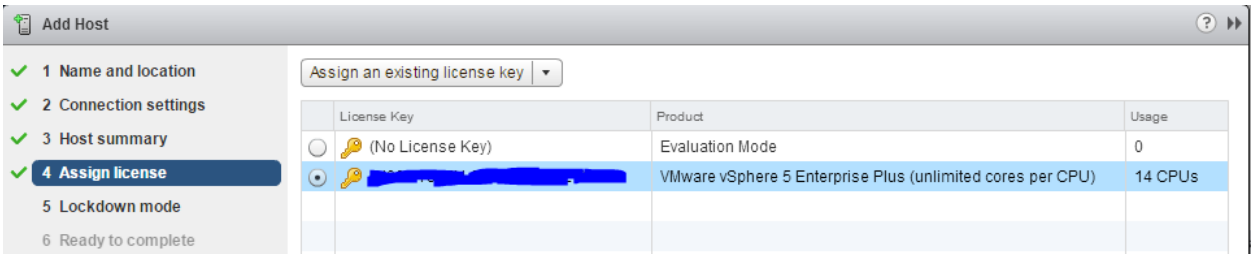

Figure 35 Assign License

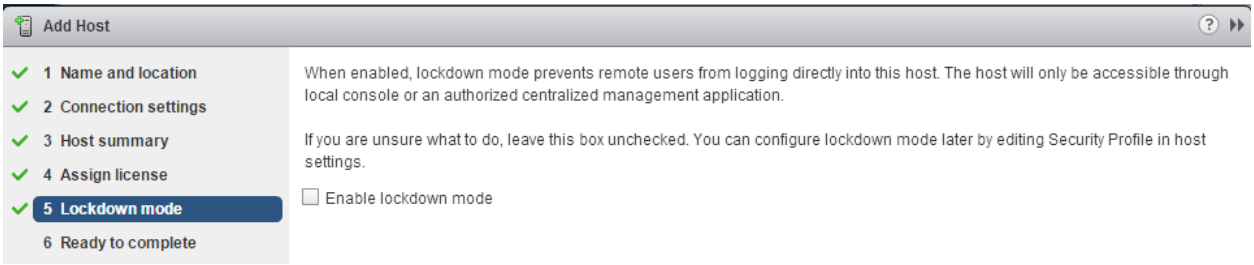

Figure 36 Lockdown mode (Leave unchecked)

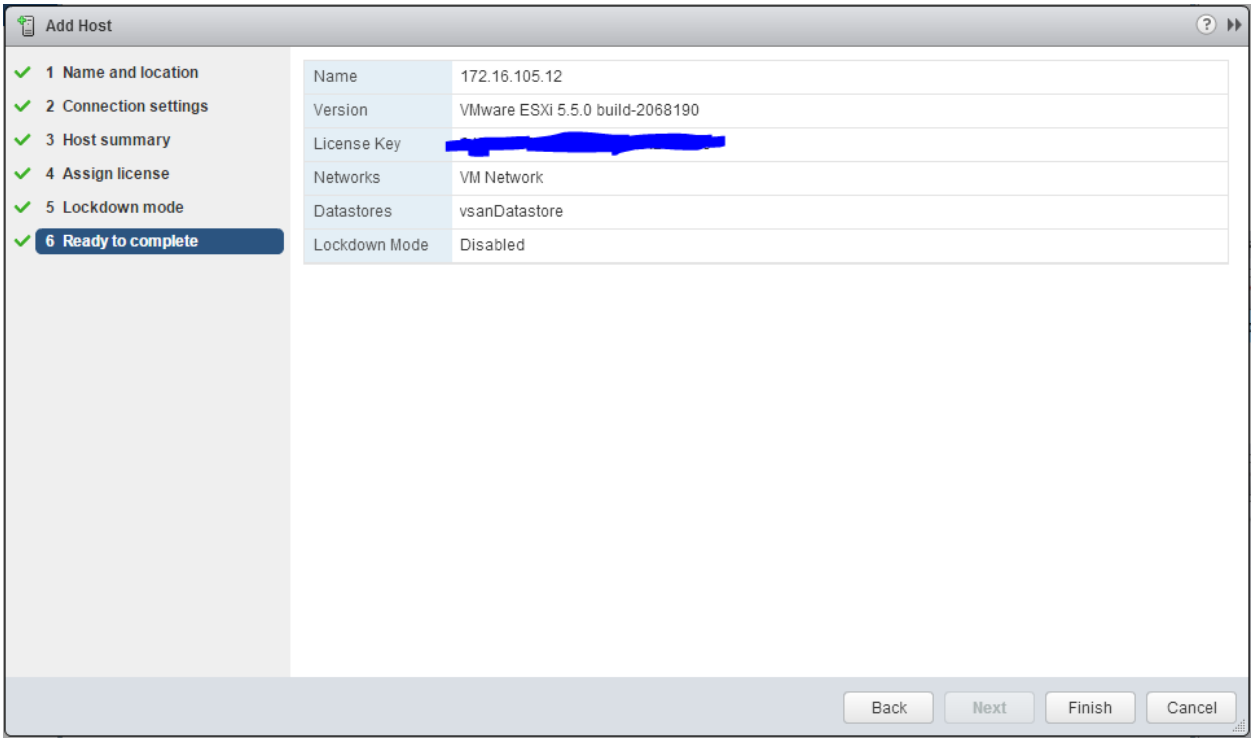

Figure 37 Ready to complete

6.4 Configure host networking

Each host in each cluster typically needs to be configured with a minimum of three different types of networks. Configuring host networking using Distributed vSwitch (DvSwitch) is a simple and effective way to manage networking uniformly. Configuring DvSwitch is a three step process.

1. Create a distributed vSwitch (MTU/LLDP).

2. Configure uplink link ports (LACP or NIC Teaming).
3. Configure port groups (VLAN/VMkernel ports if necessary).

It is important to avoid single point failures in the uplink, a minimum of two uplink ports per DvSwitch connecting to two different physical switch is a best practice.

6.4.1 Management Networking

By default, during ESXi installation on a host, vSwitch0 is created with the management port chosen during ESXi installation as an Uplink port and a VMKernel interface with the Management IP as part of Management network is created.

6.4.1.1 Create DvSwitch

Navigate to **Home → Networking → <*Your DC*> → Actions → Distributed Switch → Create New Distributed vSwitc**h. Configure the name, version and number of uplinks in the switch. Finally review the configuration and click **Finish** to create a DvSwitch.

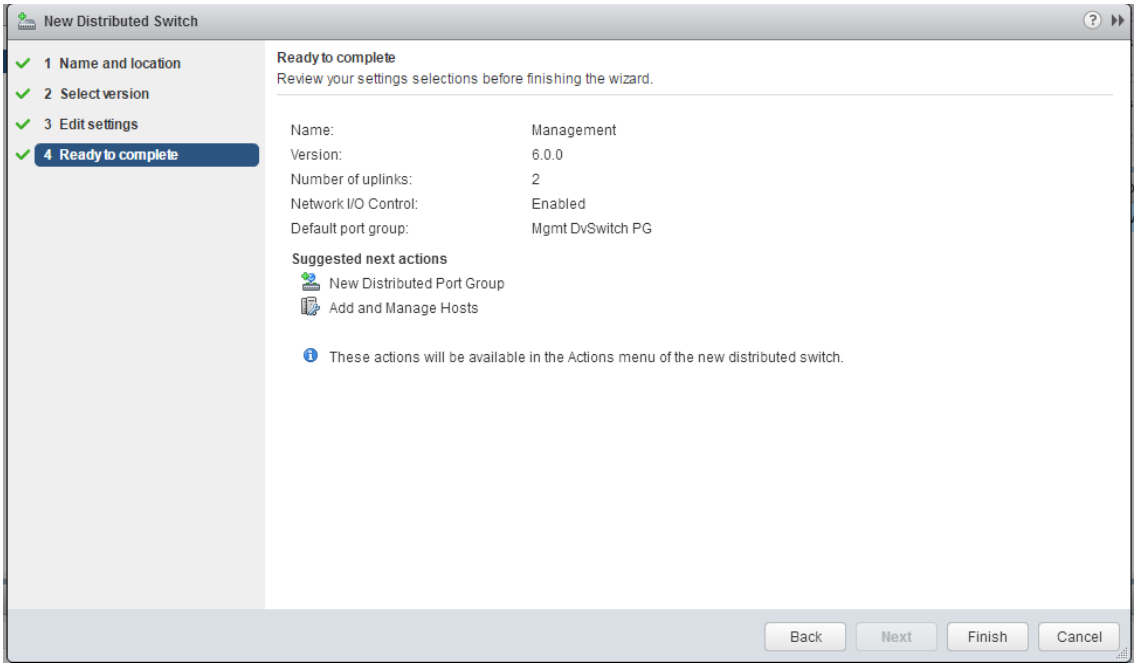

Figure 38 DvSwitch configuration

Select the newly created DvSwitch and select **Actions → Settings → Edit Settings → Advanced** to change the MTU and discovery protocol.

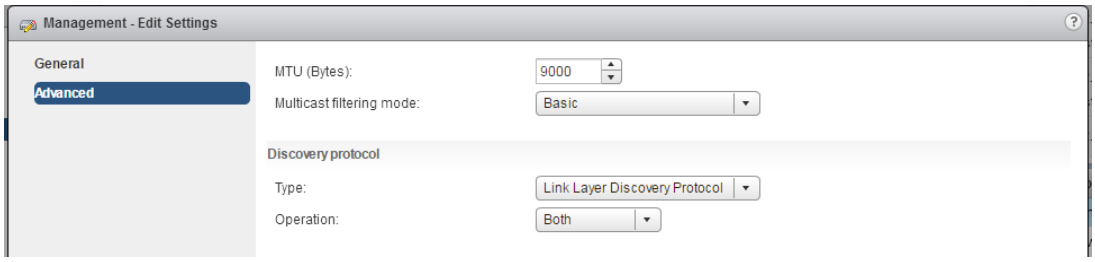

Figure 39 Change MTU and discovery protocol

6.4.1.2 Add first uplink port and VMkernel ports

Configuring the Management Networking needs to be carefully done in a multi-step process because we have to migrate both physical uplink ports, VMkernel ports and vCenter appliance related VMs. Click on **Actions → Add and Manage Hosts**. Select all the hosts in the VIM cluster.

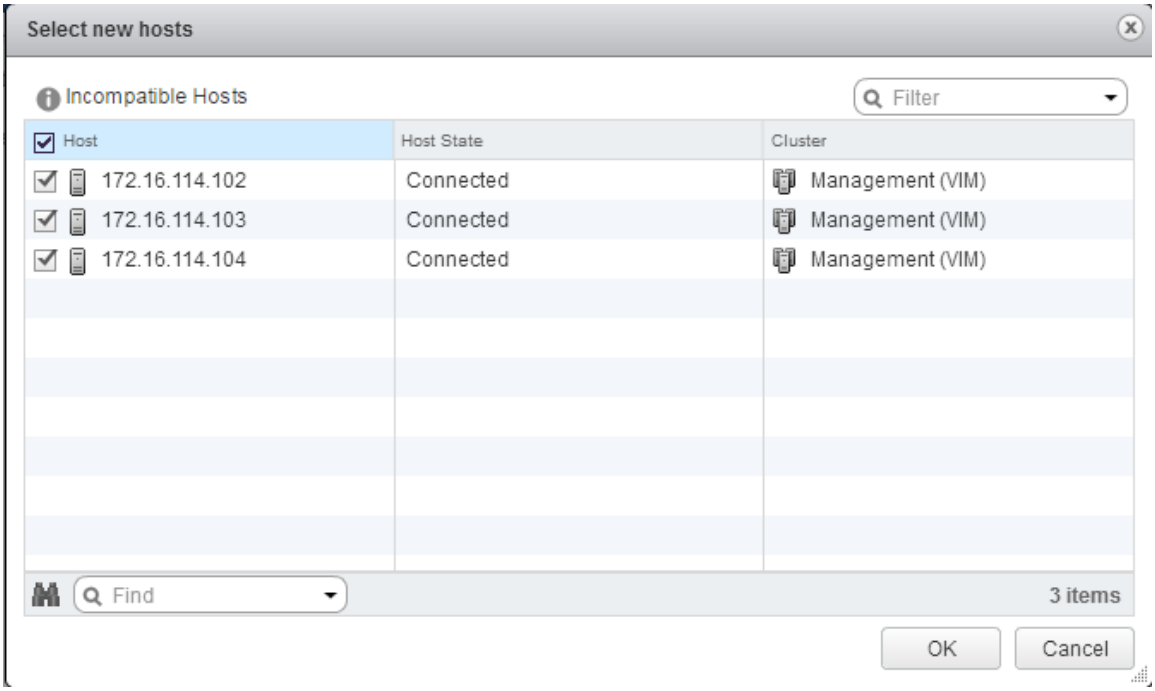

Figure 40 Select the hosts in the VIM cluster

Make sure to select the second management port from each host that is not part of vSwitch0 and click **Next**.

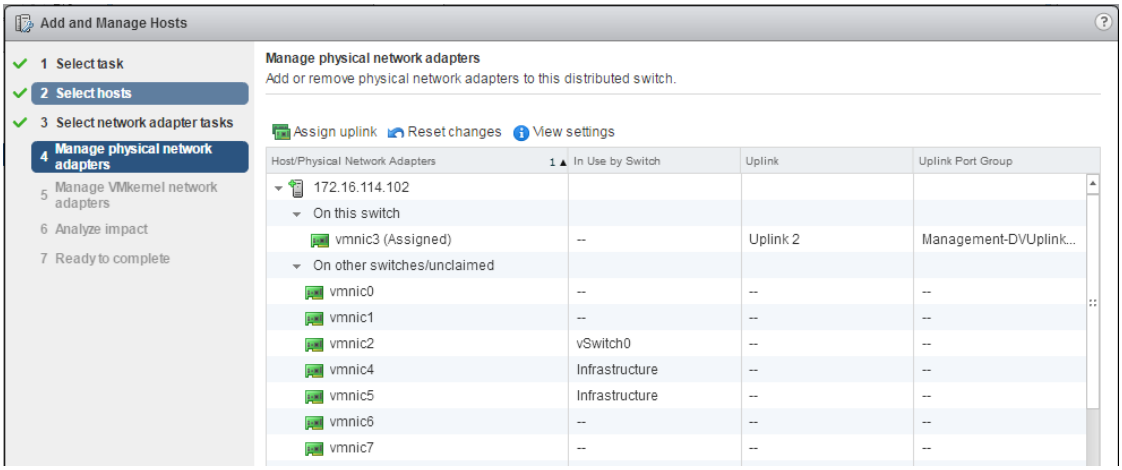

Figure 41 Manage physical network adapters

Assign the vmk0 to the newly created Mgmt DvSwitch PG in each host.

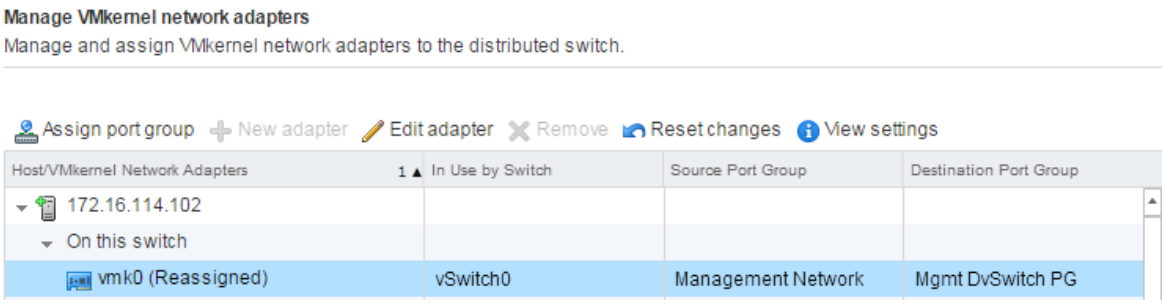

Figure 42 Manage VMkernal network adapters

Confirm there is no impact due to this configuration change and click **Finish** to migrate the host VMkernel network and an uplink port to the newly created DvSwitch.

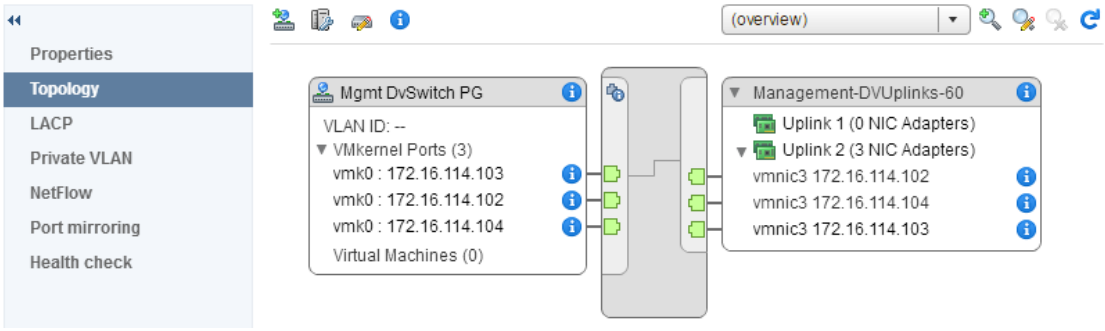

Figure 43 Migrate to DvSwitch

6.4.1.3 Migrate VMs to DvSwitch

Click on **Actions → Add and Manage Hosts → Manage Host Networking** and again select all three hosts from the attached hosts. Unselect **Manage physical adapters** and **VMkernel adapters** and select **Migrate virtual machine networking**

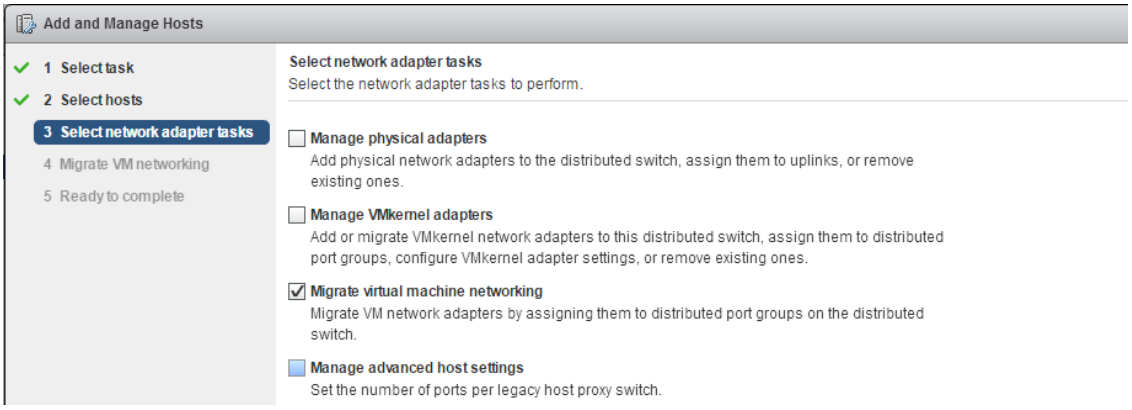

Figure 44 Select network adapter tasks

Assign the port group in vCenter appliance related VMs to the Mgmt DvSwitch port groups.

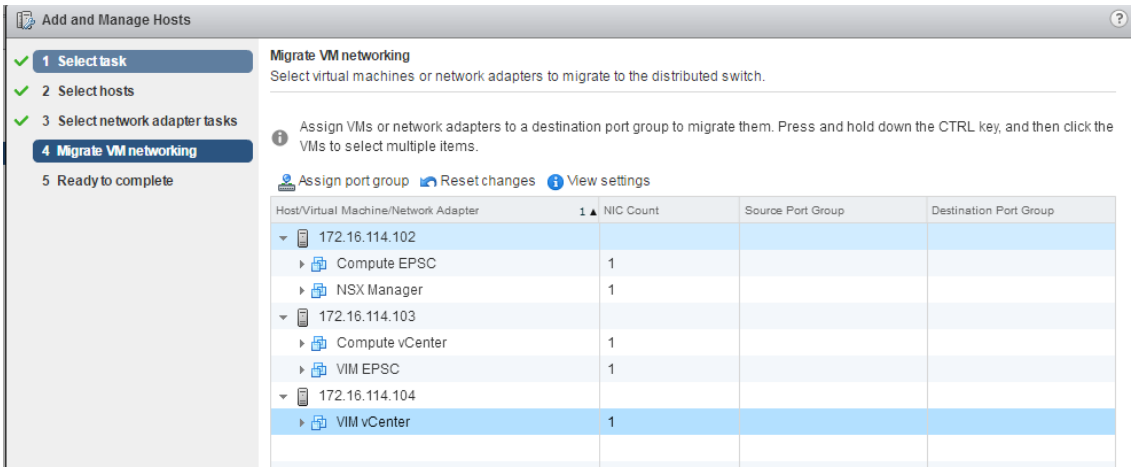

Figure 45 Migrate VM networking

6.4.2 Migrate the second uplink port to DvSwitch

Click on **Actions → Add and Manage Hosts → Manage Host Networking** and again select all three hosts from the attached hosts. Unselect Manage VMKernel adapters and click **Next**. For each host, select the management port uplink that is part of vSwitch0 to Uplink1 of DvSwitch.

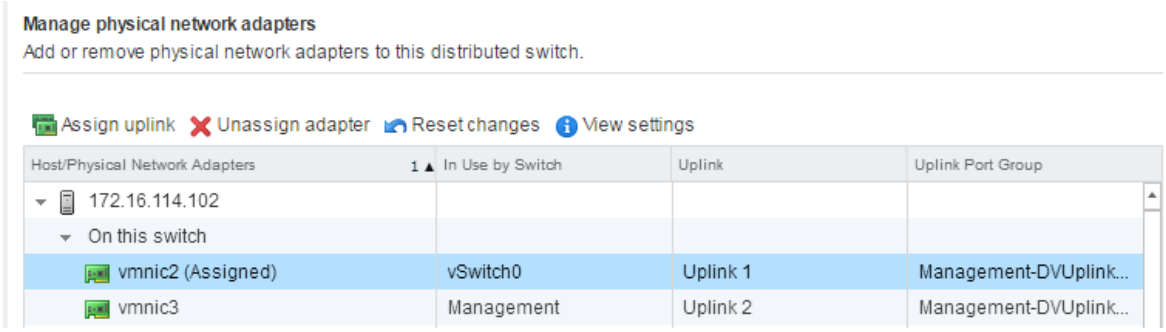

Figure 46 Manage physical network adapters

Confirm there is no impact due to this configuration change and click **Finish** to complete host Management Networking configuration.

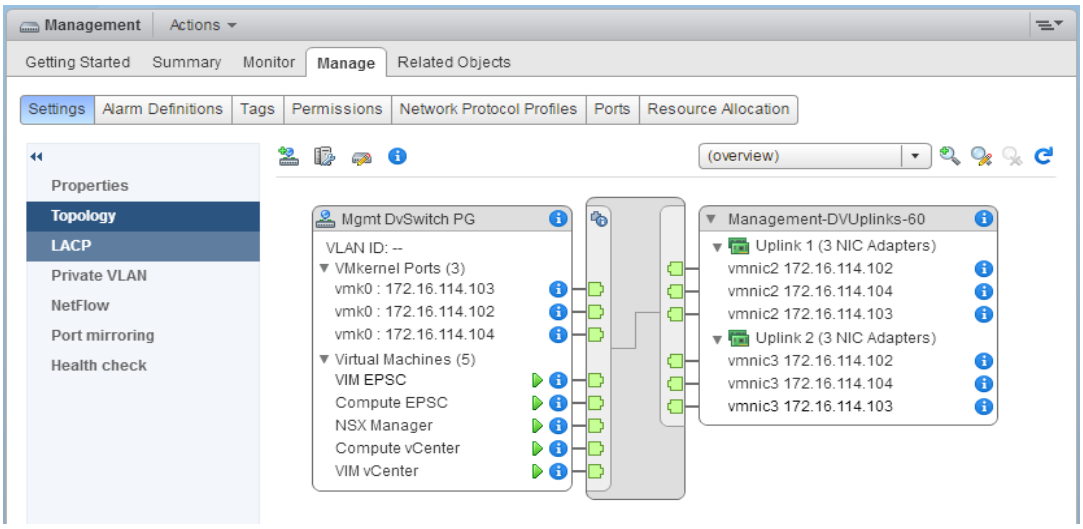

Figure 47 Host Management Networking configuration

6.4.2.1 Management DvSwitch for Compute vCenter

Repeat the previous four steps in the Compute vCenter with hosts from both Compute and Edge cluster in a single Management DvSwitch. Assuming this is a green field deployment, Compute vCenter will not have any VMs to migrate, so migrate only the uplink ports one by one.

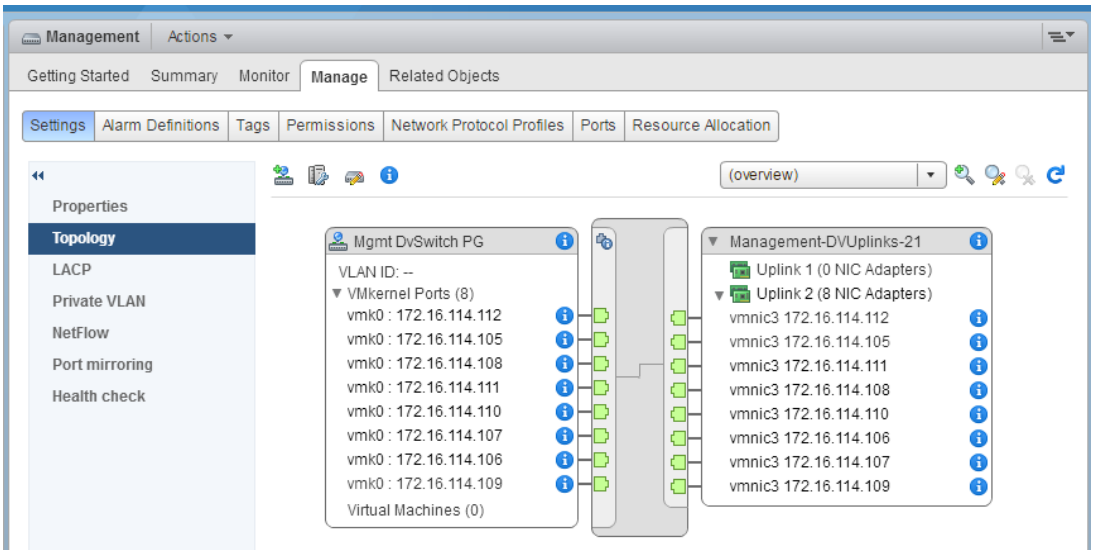

Figure 48 Management DvSwitch

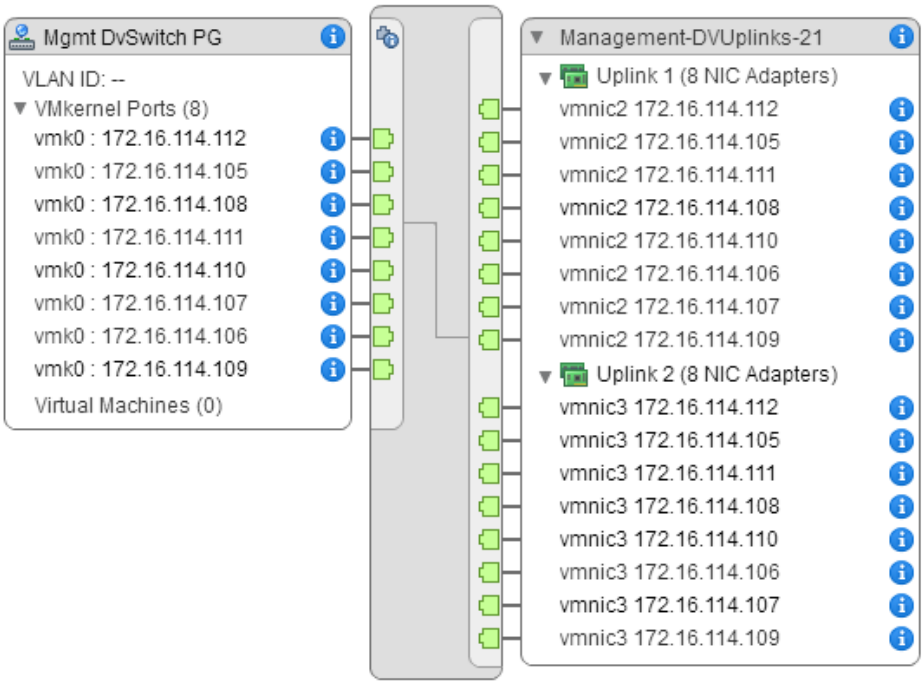

Figure 49 Management DvSwitch

6.4.3 Infrastructure Networking

In VMware vCloud, infrastructure network provisioning involves allocating network resources for VSAN, vMotion and Replication. All three infrastructure components will share the same set of uplink ports.

6.4.3.1 Create a DvSwitch

Under networking tab, create a distributed switch by assigning Name, choose the total number of uplink ports to be 2 and unselect “Create a default port group”.

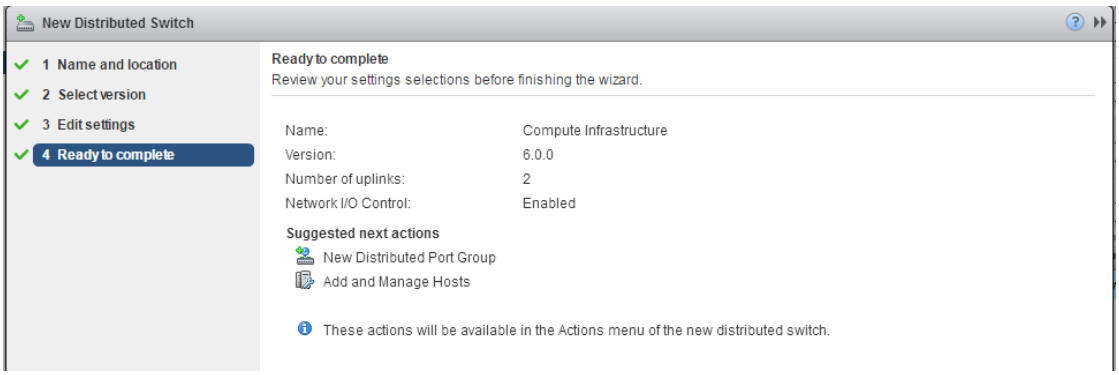

Figure 50 DvSwitch configuration

Select the newly created DvSwitch and select **Actions → Settings → Edit Settings → Advanced** to change the MTU and discovery protocol.

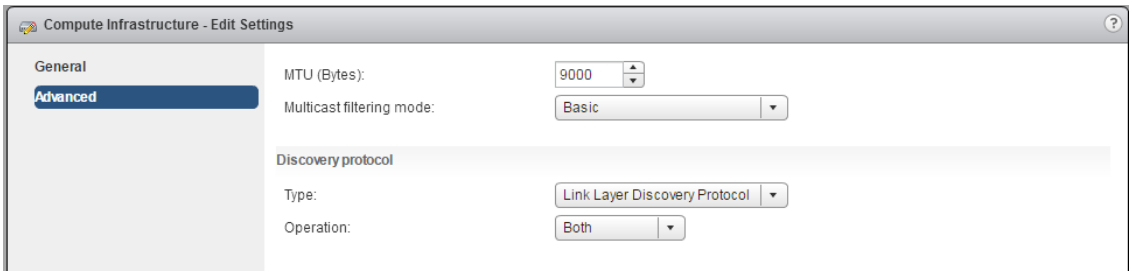

Figure 51 MTU and Discovery protocol

6.4.3.2 Add the necessary infrastructure port groups

As per the Vlans configured in the Leaf switch, associate the infrastructure port-groups with the respective Vlans.

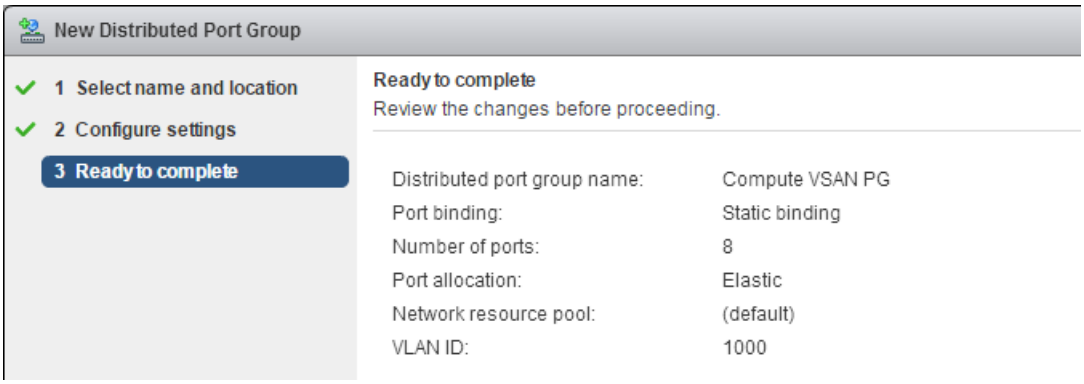

Figure 52 Compute VSAN PG port-group

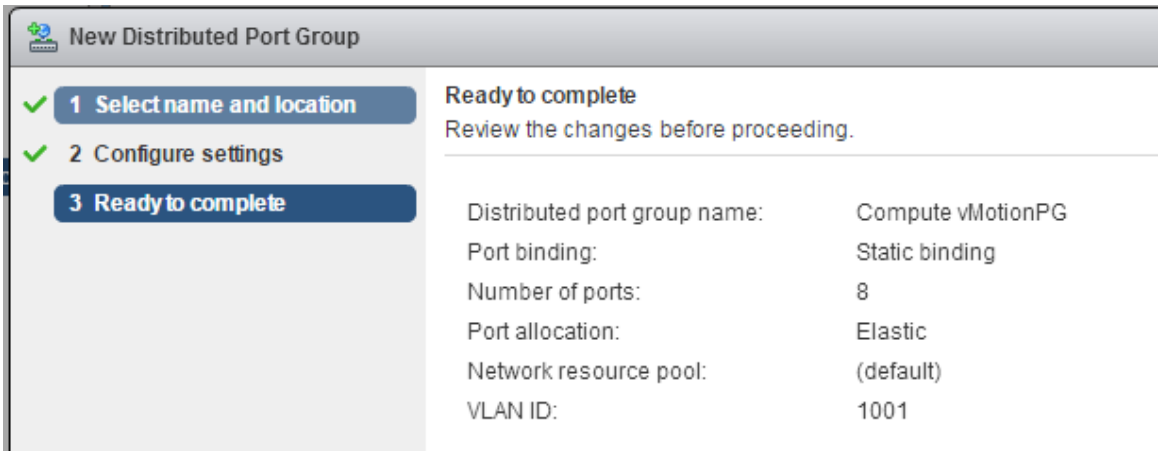

Figure 53 Compute vMotionPG port-group

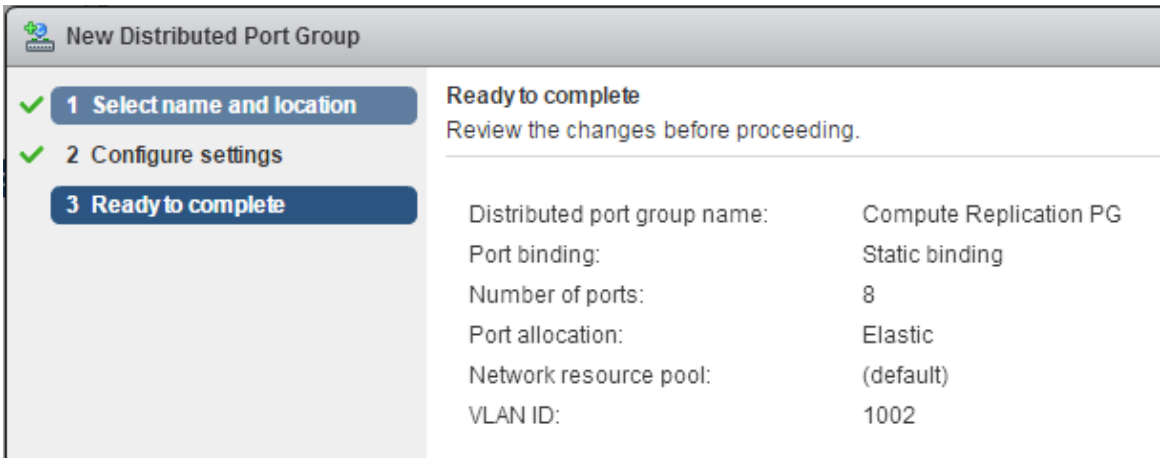

Figure 54 Compute Replication PG port-group

6.4.3.3 Configure LACP in the uplink ports

Under **Compute Infrastructure DvSwitch → Manage → Settings → LACP** create a new Link aggregation group by the name e.g. lacp1, change the mode from Passive to Active and click OK. Changing to a different load-balancing mode for the LACP LAG is optional, in the example below it is left as the default.

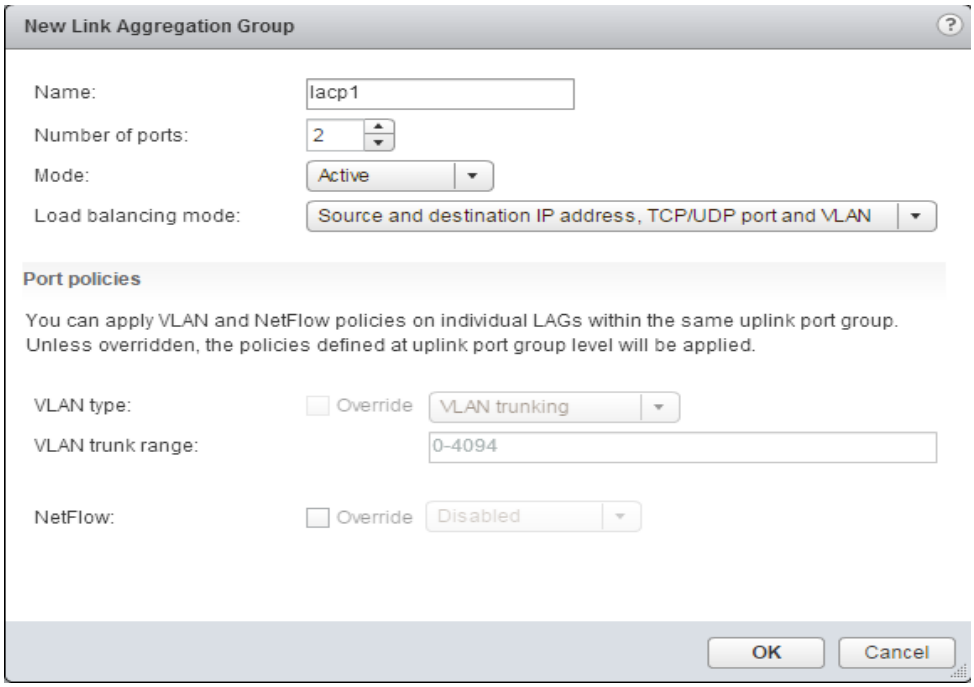

Figure 55 Create a new link aggregation group

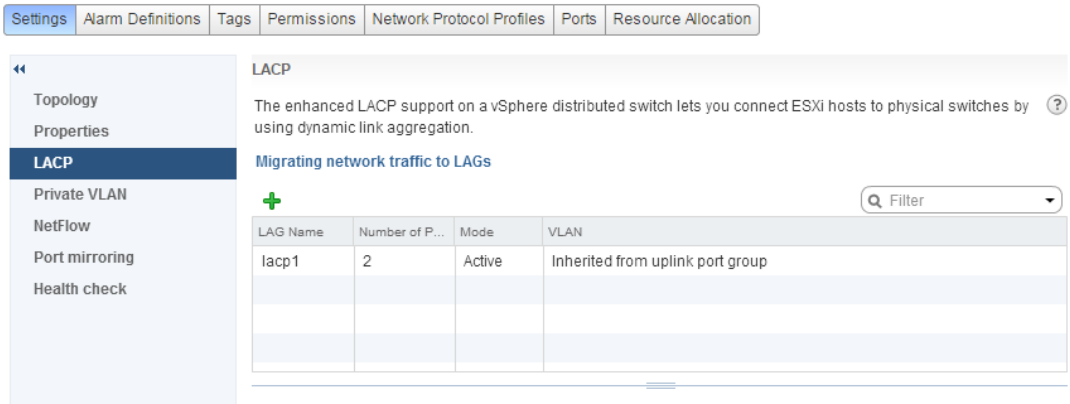

Figure 56 LACP settings

6.4.3.4 Add host uplink ports to DvSwitch

Click on **Actions → Add and Manage Hosts**. Select all the hosts in the given cluster.

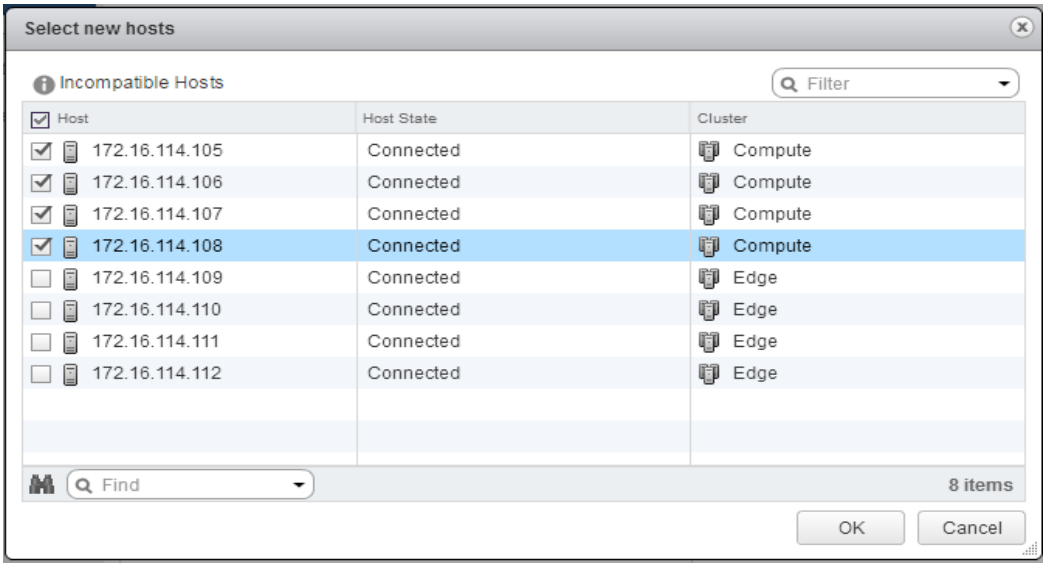

Figure 57 Add host uplink ports to DvSwitch

In each host, select the two 10G uplink ports allocated for Infrastructure as uplink ports to be part of LACP channel members.

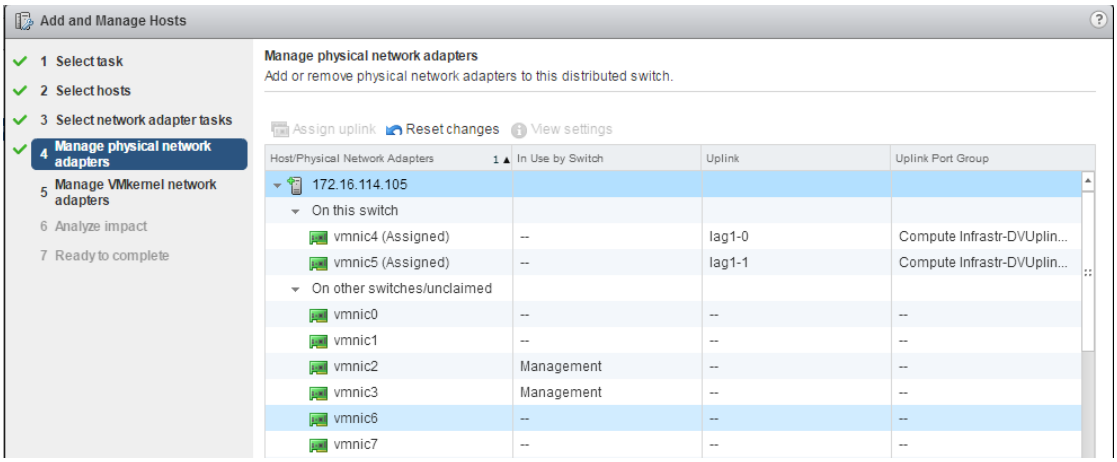

Figure 58 Manage physical network adapters

6.4.3.5 Add VMKernel adapter for each of the services

VSAN/vMotion/Replication each requires their own VMKernel adapters. Click on **New Adapter** in each host and configure three VMkernel Adapters for each of the hosts in the DvSwitch.

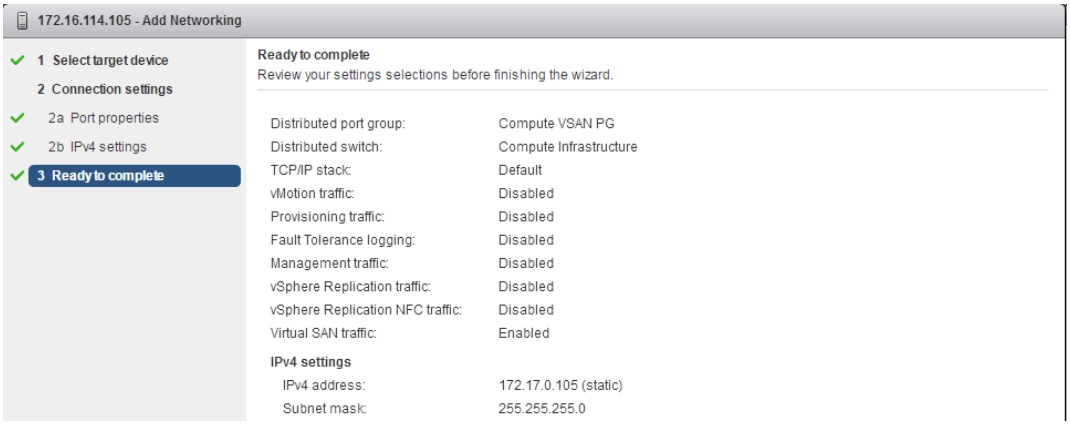

Figure 59 Compute VSAN PG port-group

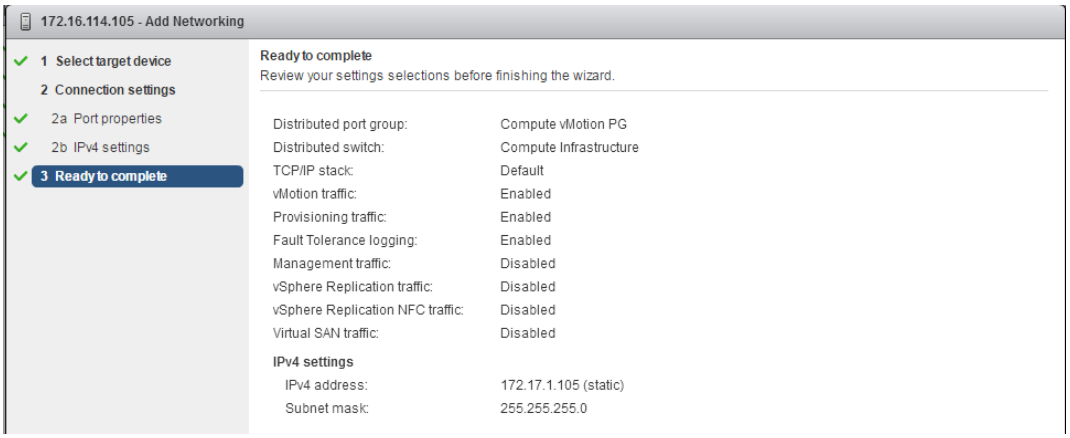

Figure 60 Compute vMotion PG port-group

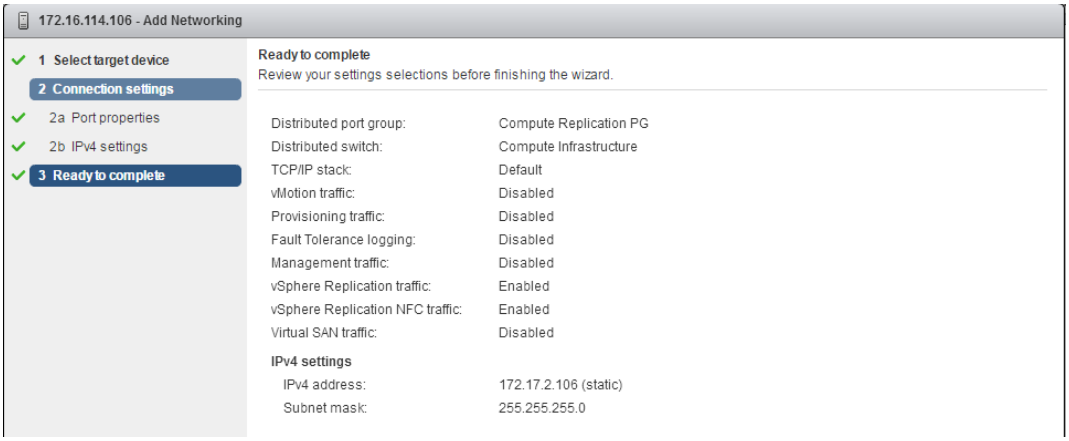

Figure 61 Compute Replication PG port-group

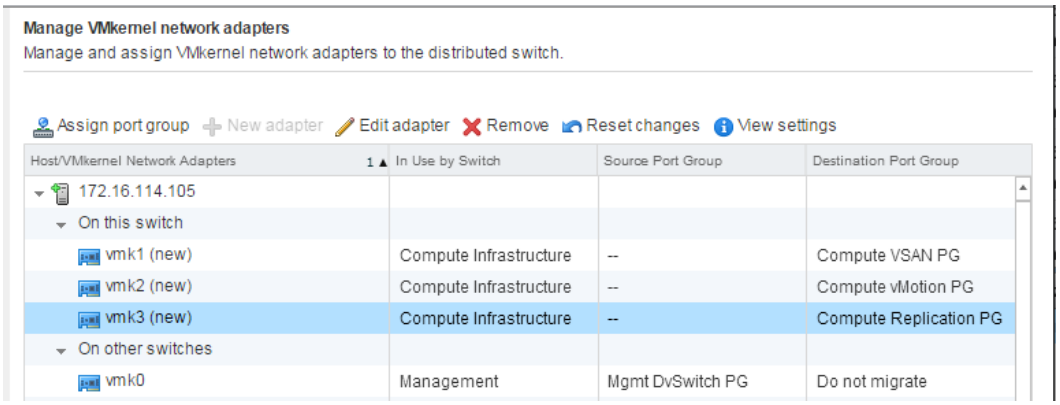

Figure 62 Assign VMkernel network adapters

Verify the configuration is correct and click **Finish**.

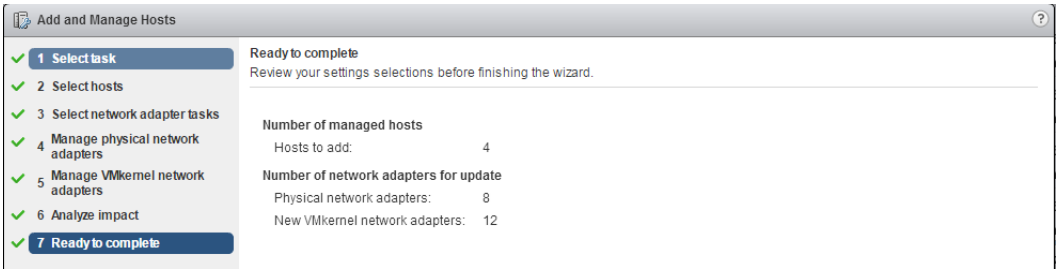

Figure 63 Ready to complete

6.4.3.6 Associate port group to VLAN and LACP uplink ports as active ports

Once the LAG creation is successful, the created port group needs to be associated with LACP uplinks. The example shown here is a Greenfield implementation so when we click **DvSwitch → Manage → LACP → Migrating network traffic to LAGs.** On this page, we move to step 3.

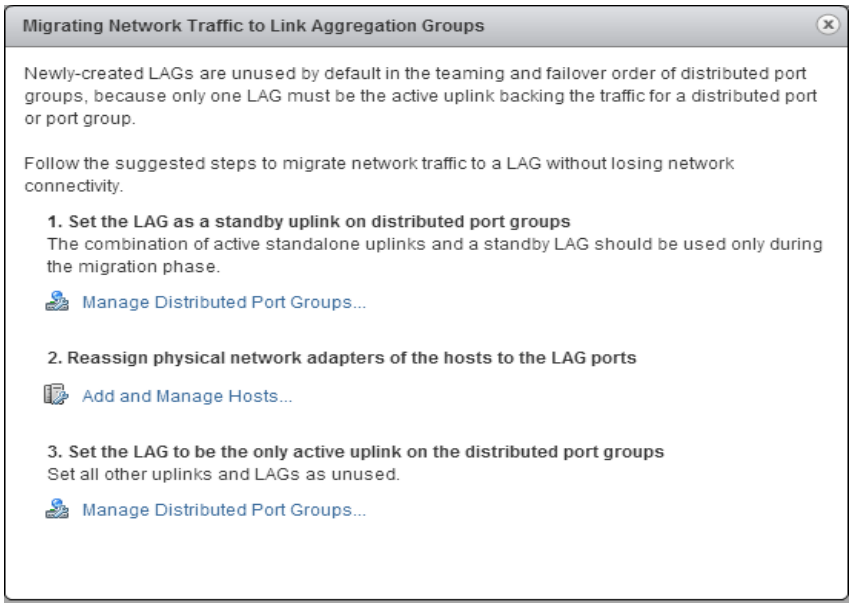

Figure 64 Migrating Network Traffic to LAGs

Choose to configure teaming and failover checkboxes.

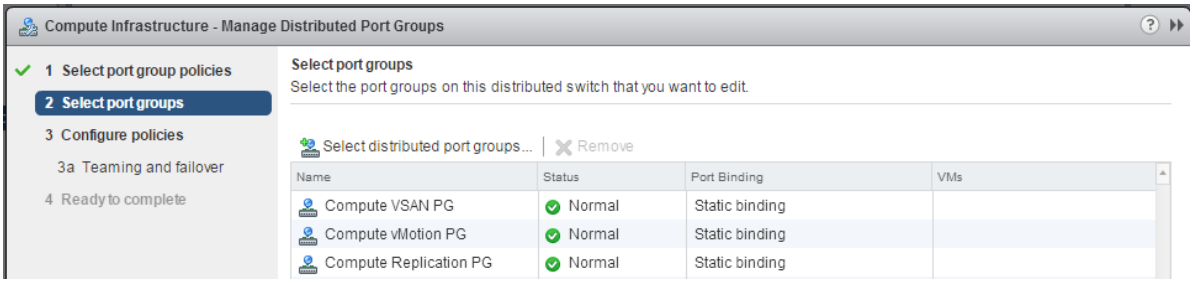

Figure 65 Configure teaming and failover

Change LACP to Active and Uplink ports to Unused, Click **Next** and **Finish**

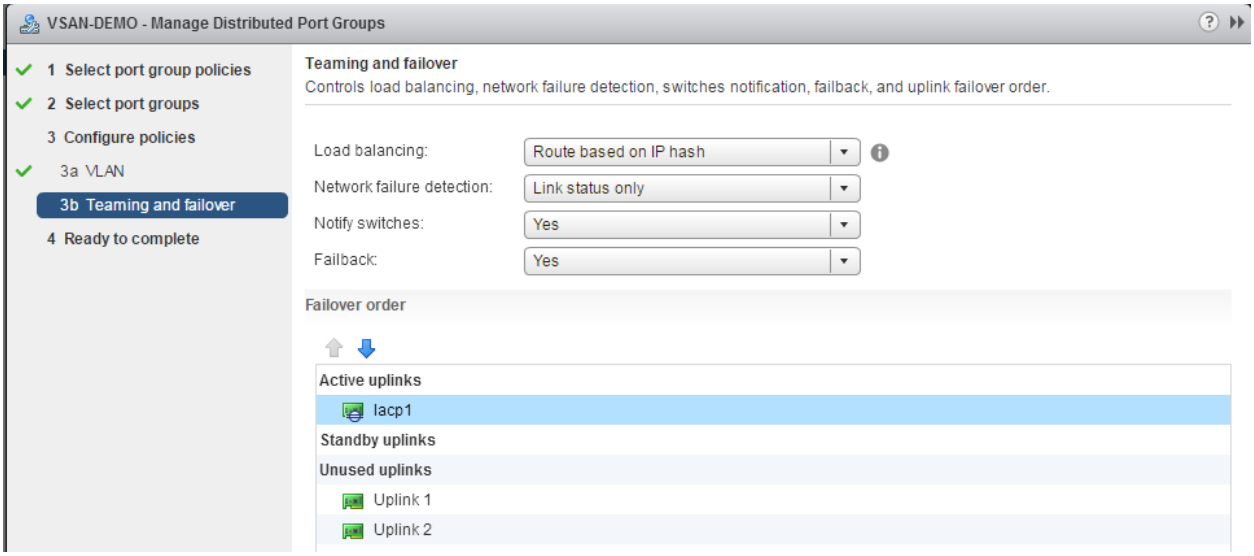

Figure 66 Configure teaming and failover

A fully configured DvSwitch will look like the screenshot shown below. This image shows the Compute cluster, make sure to repeat this process in each cluster (Edge and VIM).

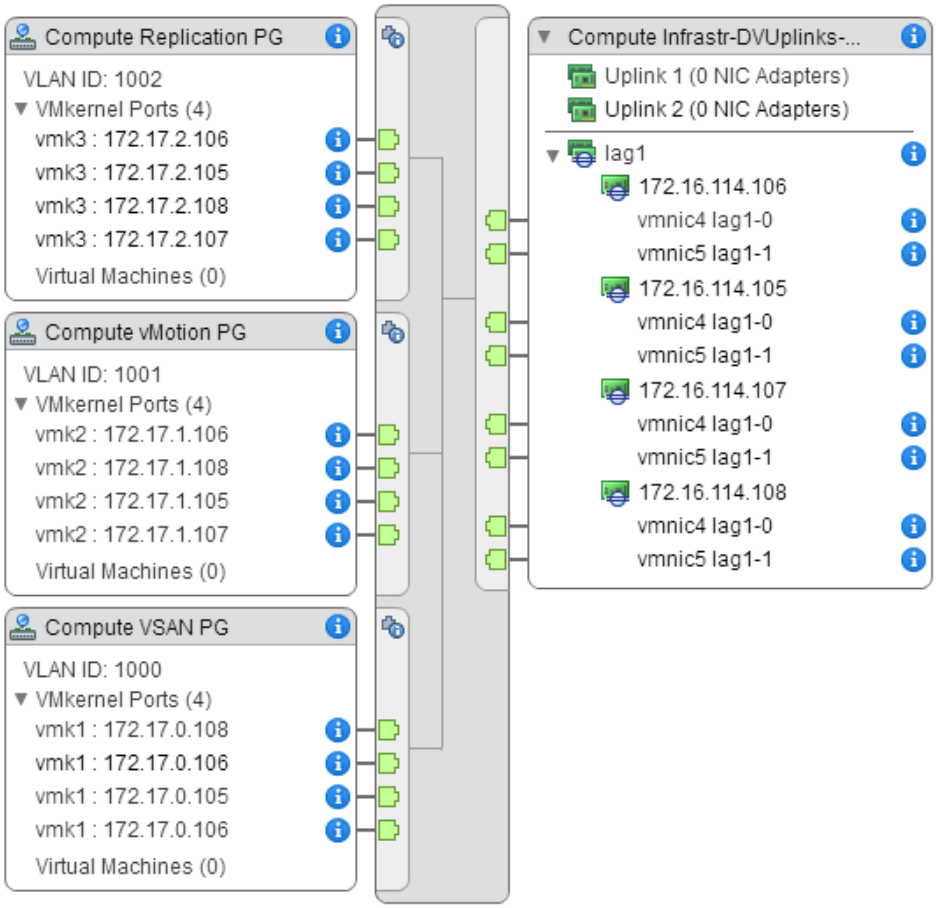

Figure 67 Fully configured DvSwitch

6.4.4 VxLAN Data Networking

Configuring VxLAN data network is similar to Infrastructure networking except the VMkernel adapters do not have to be created. During the NSX host preparation phase, VMKernel ports are associated with the host automatically. Create DvSwitches for Compute and Edge clusters.

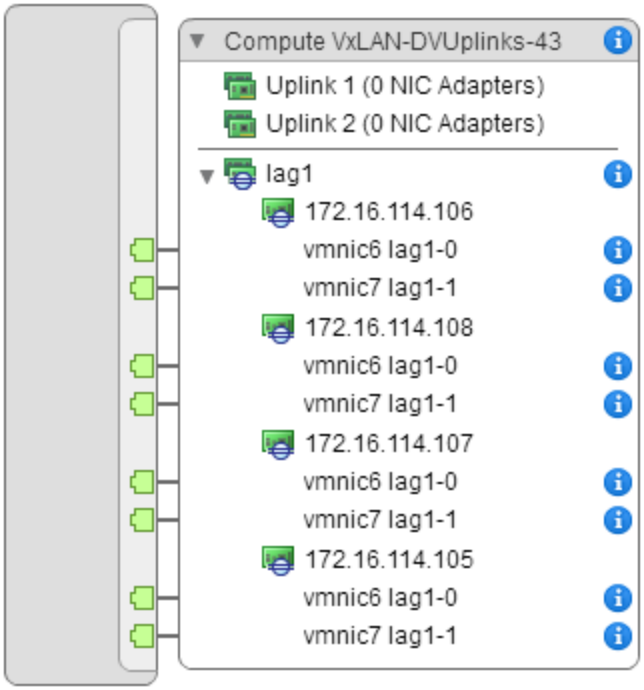

Figure 68 VxLAN Data Networking

6.5 Enable VSAN

Virtual SAN is a hypervisor-converged, software-defined storage solution for the software-defined data center (SDDC). It is the first policy-driven storage product designed for VMware vSphere environments that simplifies and streamlines storage provisioning and management.

6.5.1 Enable VSAN in cluster

The second step after completing VSAN networking is to turn on VSAN on the cluster. Under **Hosts and cluster → Select the cluster → Manage → General** under Virtual SAN. Make sure to select Manual mode of claiming the disk storage.

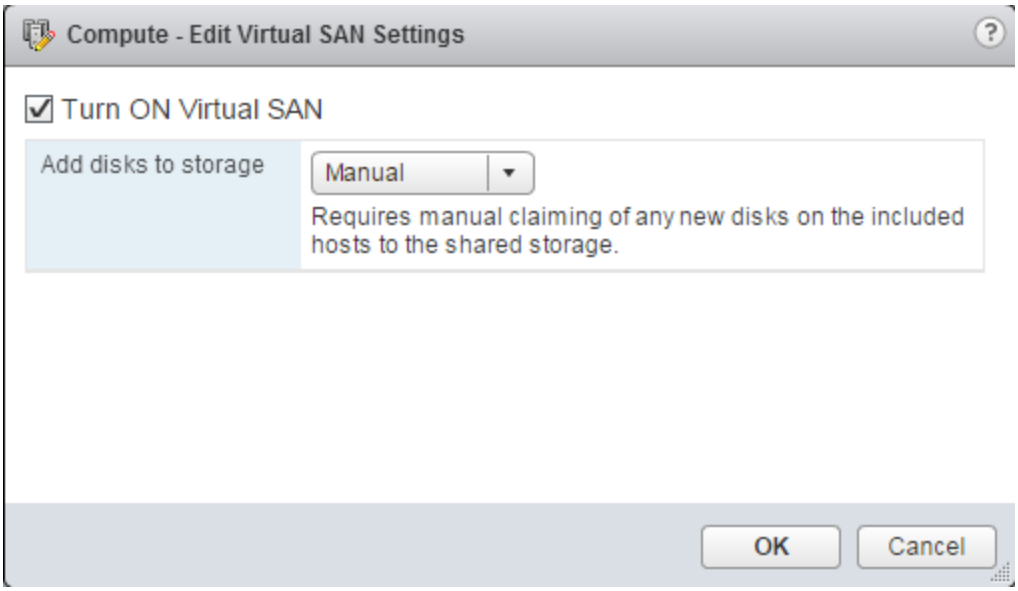

Figure 69 Add disks to storage

6.5.2 Assign VSAN license key to cluster

Under **Hosts and cluster → Manage → Virtual SAN Licensing,** click **Assign License key** to assign a License key to the cluster. The number of CPUs used is based on the number of CPU cores present in the given cluster.

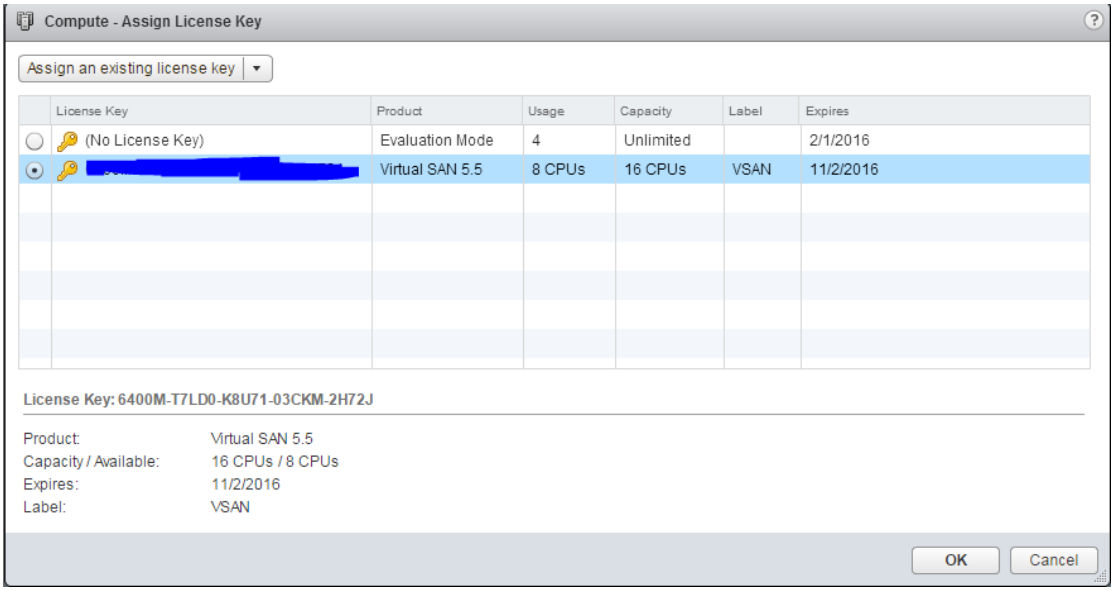

Figure 70 Assign License Key

6.5.3 Claim the hard disks for VSAN

After assigning the license key, go to Disk management, click **Create Disk Group** and select the SSD HD drives from each host and click **OK**. To complete the process, repeat these steps on each host in each cluster that has eligible hard disks.

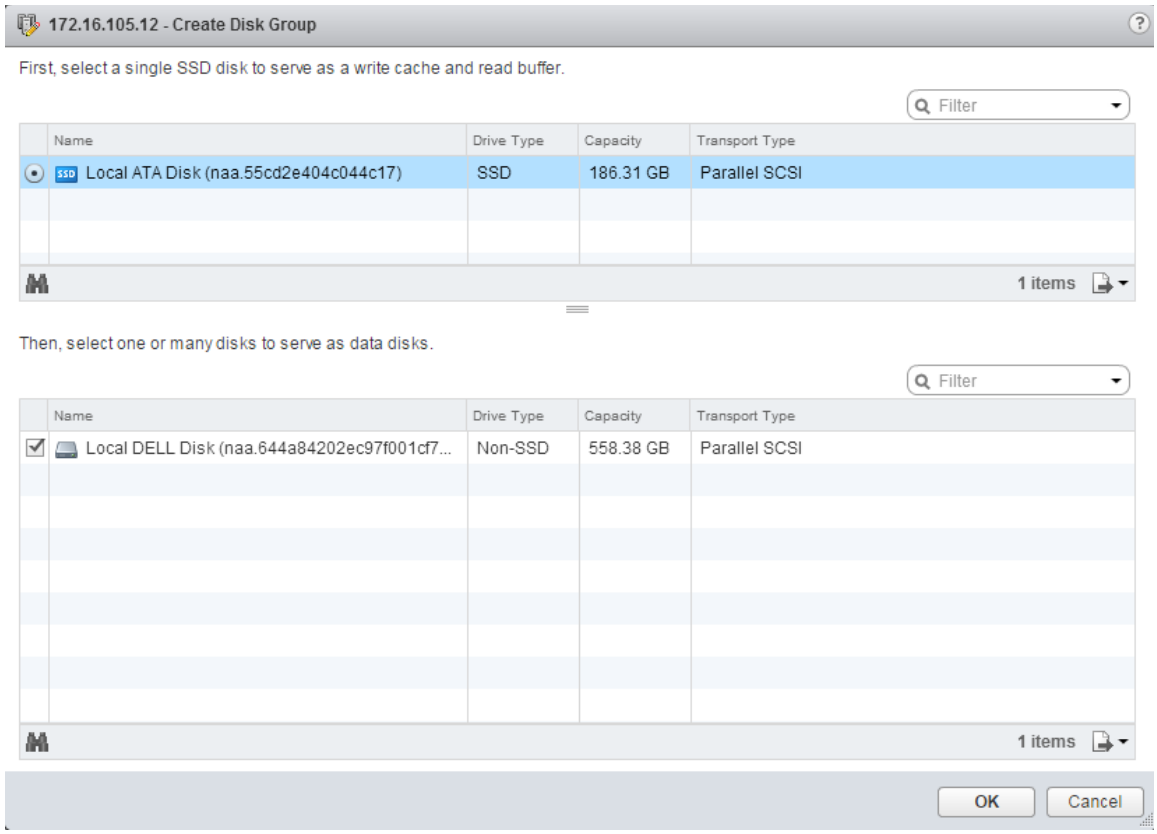

Figure 71 Create Disk Group

6.6 Install NSX

With NSX, virtualization delivers for networking what it has already delivered for compute and storage. There are three major components that need to be installed in a vSphere environment to make NSX fully operational. These components are NSX manager, NSX controllers and NSX edge gateway services. For additional installation help, refer to the following: http://pubs.vmware.com/NSX-62/topic/com.vmware.ICbase/PDF/nsx_62_install.pdf.

6.6.1 Deploy NSX manager

Even though NSX has various components and multiple steps are required to complete the installation, similar to vCenter appliance, all the NSX components can be deployed from the NSX manager virtual appliance. This makes the installation process simple and straightforward. Locate the host machine on which to install NSX manager and select the **Deploy OVF template**. Locate the NSX manager appliance OVA file and click **Next**, select the check box **Accept extra configuration options** and click **Next**.

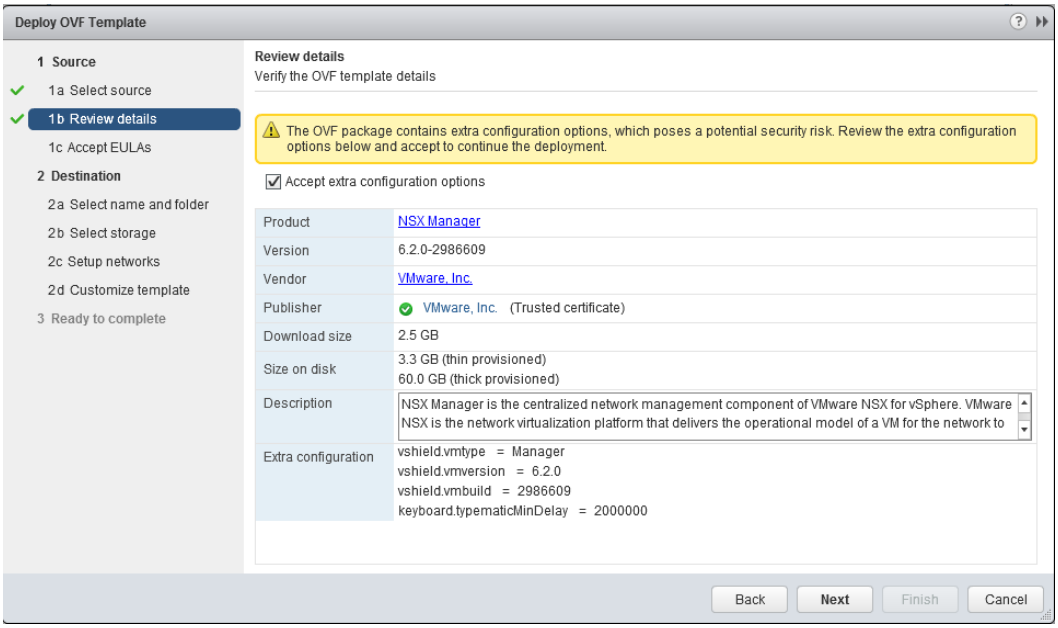

Figure 72 OVF template details

Follow the installation instructions and in the Setup Networks step ensure NSX manager is deployed in the same port group that contains the vCenter appliance.

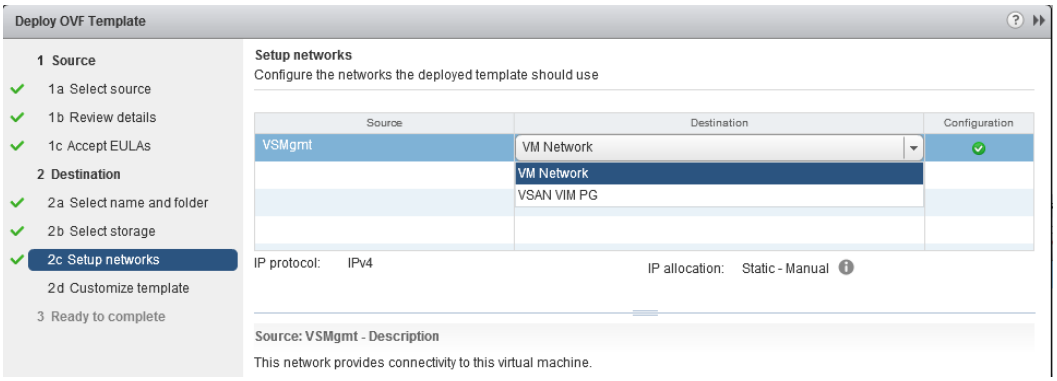

Figure 73 Setup Networks

Configure the admin user password and CLI privilege mode password of your choice

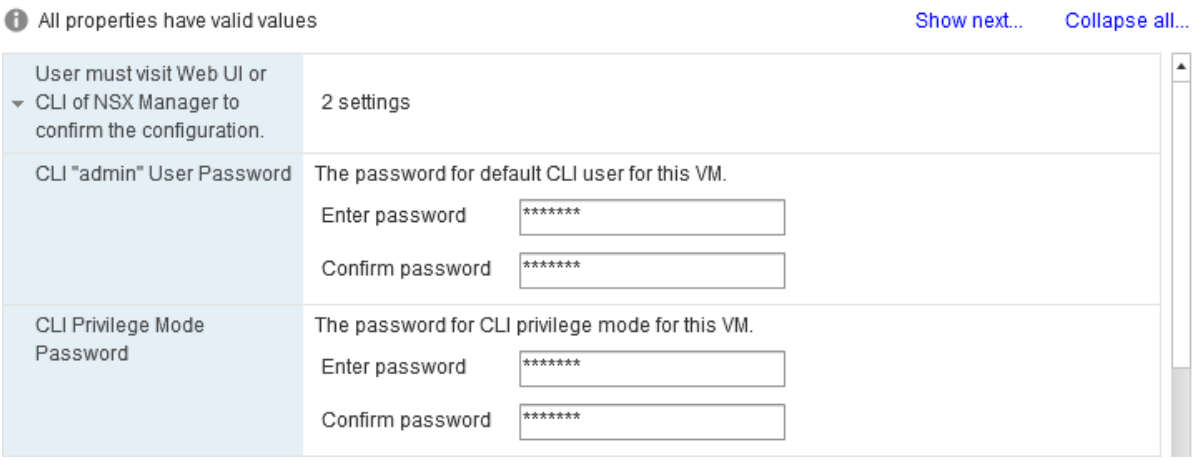

Figure 74 Configure username and password

Click **Show Next** to configure the Host name, management IP address, mask and gateway. Make sure to enable SSH service at the bottom as well.

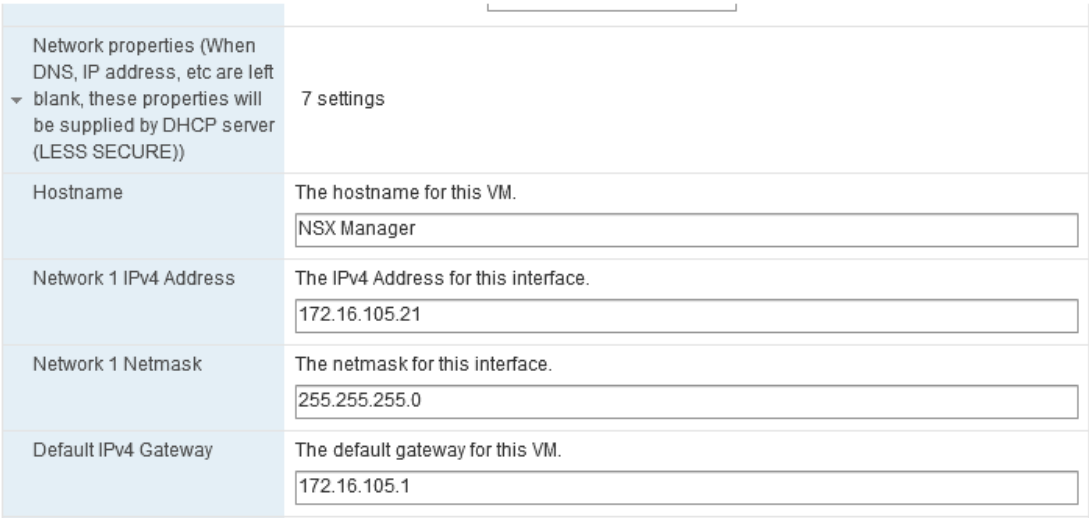

Figure 75 Network Properties

Verify all configurations are correct, then select **Turn on VM** to deploy.

6.6.2 Register NSX manager with vCenter

Open NSX manager by entering the NSX manager IP in a browser and use the login credentials that were configured during the NSX manager deployment. Select **Manage vCenter Registration**.

Figure 76 NSX Manager

Click vCenter server **Edit** button and provide the vCenter server IP, username and password, Click **Yes** when you are prompted to trust the certificate.

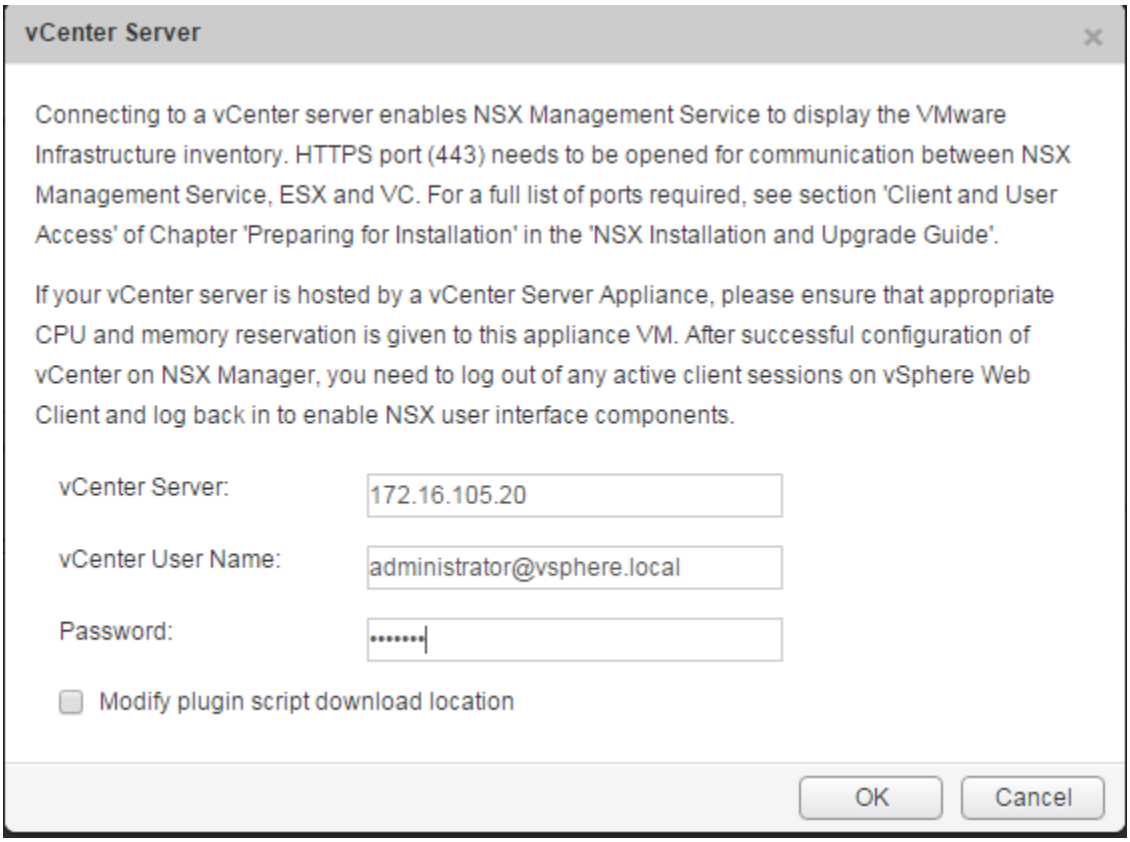

Figure 77 vCenter Server

Logout and Login to the VMware vSphere web client. A new Icon is shown (Figure 78) confirming the NSX registration is successful.

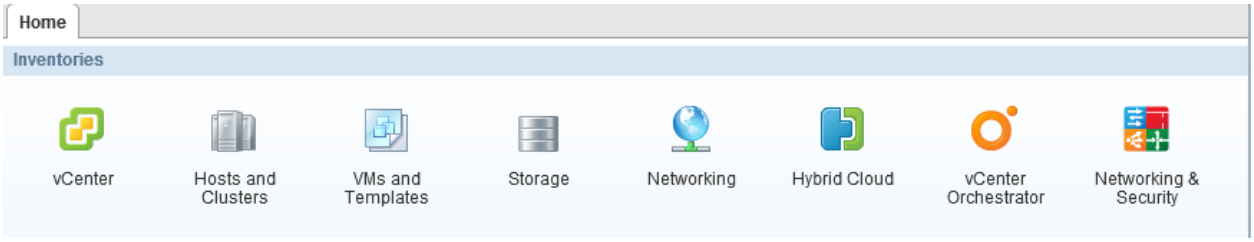

Figure 78 VMware vSphere web client

6.6.3 Deploy NSX controllers

To deploy the NSX controllers navigate to **Home → Networking & Security → Installation** and select the Management tab. Click on (**+**) sign under NSX controller nodes. Fill out all the details in the Add Controller dialog box.

Note: Decide on a pool of 10 IP addresses to assign NSX controllers

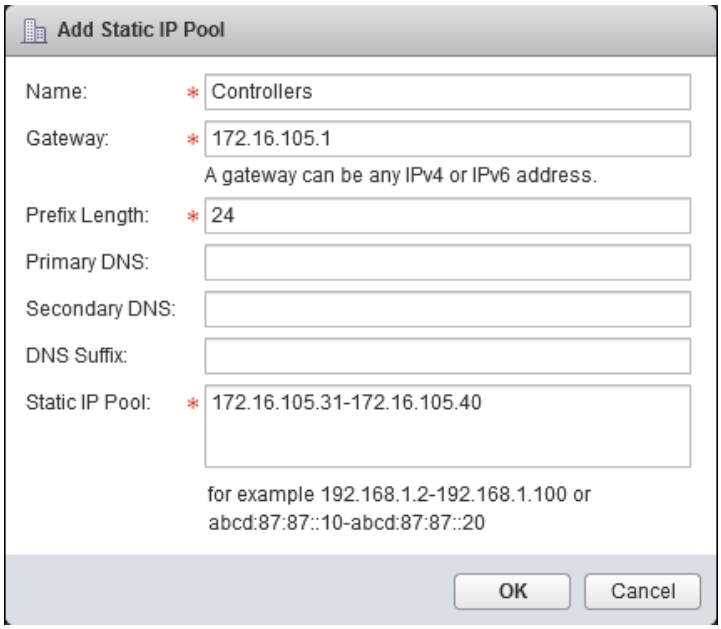

Figure 79 NSX controller IP address pool

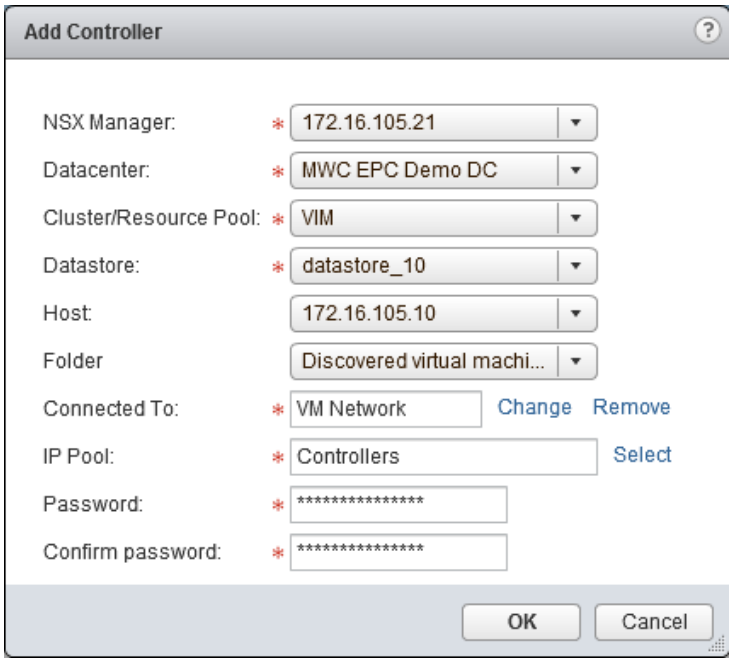

Figure 80 Add Controller

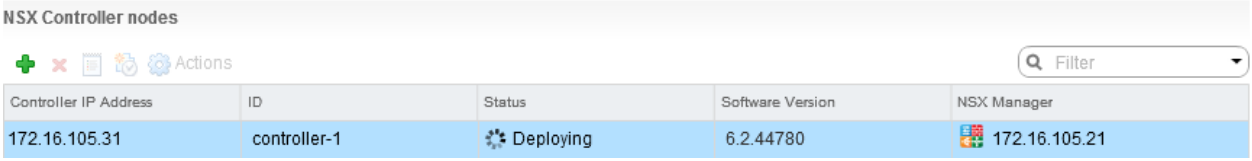

Figure 81 NSX Controller Nodes

Once the first controller is deployed, continue this process two more times to deploy three NSX controllers.

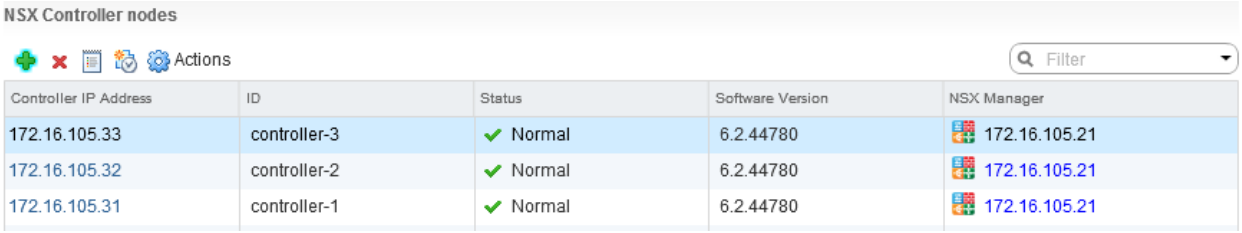

Figure 82 Three NSX controllers

Note: Sometimes the deployment may fail, simply retry the process and it will succeed.

6.6.4 Exclude VMs from Firewall

It is recommended that the vCenter VM be excluded from the firewall protection. To do this, navigate from **Home → Networking & Security → NSX Managers → Manage → Exclusion** list. Click on the (**+**) symbol and add the vCenter VM in exclusion list.

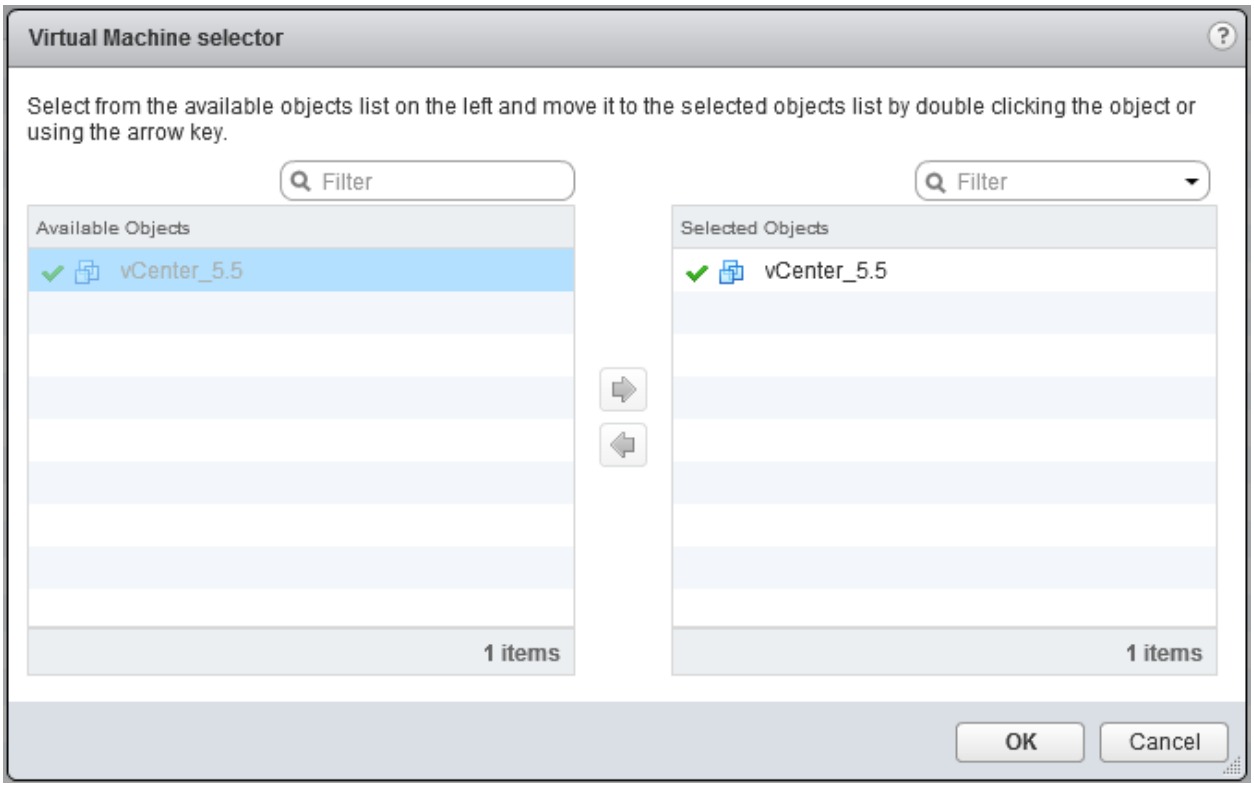

Figure 83 Exclude vCenter VM from firewall protection

6.6.5 Install NSX Kernel Modules

The host preparation process installs NSX kernel modules in the ESXi hosts that are members of vCenter clusters and builds NSX control plane and management-plane fabric. To start this process, navigate to **Home → Networking & Security → Installations → Host Preparation → Actions** and select **Install** for all the necessary clusters.

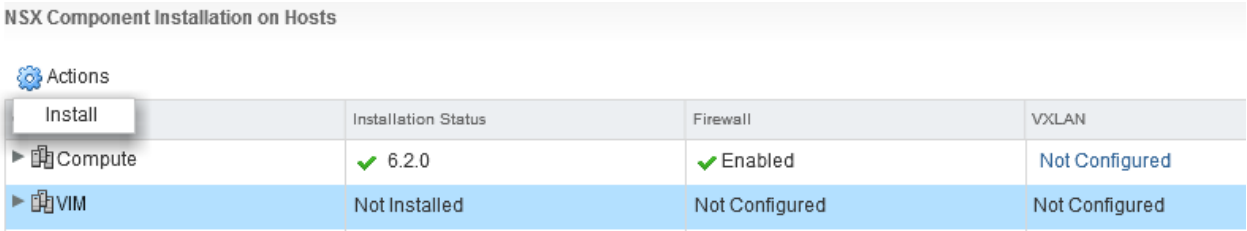

Figure 84 NSX Kernel Modules

6.6.6 Configure VxLAN

Determine the Vlan and Pool of IP address for VxLAN VTEPs. Navigate to **Home → Networking & Security → Installations → Host Preparation**. Under VXLAN column select Configure VXLAN. Create a pool similar to the NSX controller for VTEPs and assign the pool here.

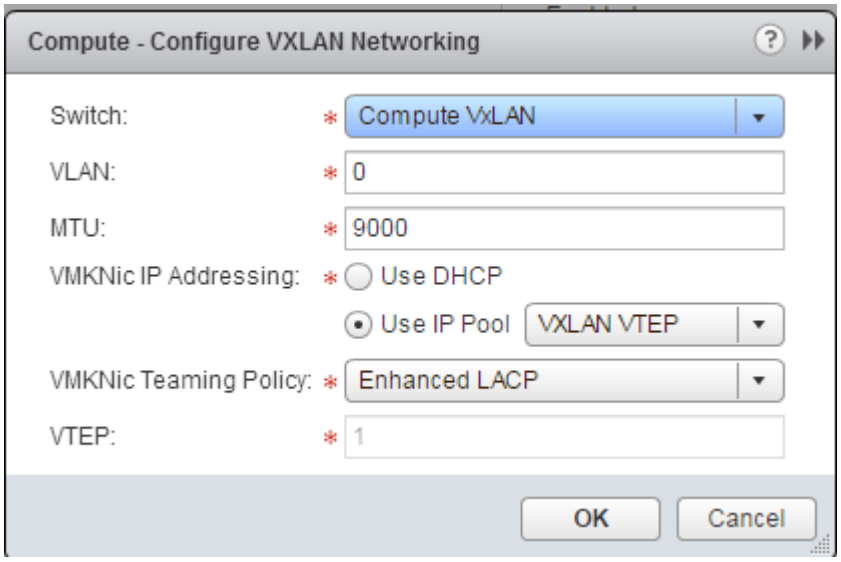

Figure 85 Configure VXLAN Networking

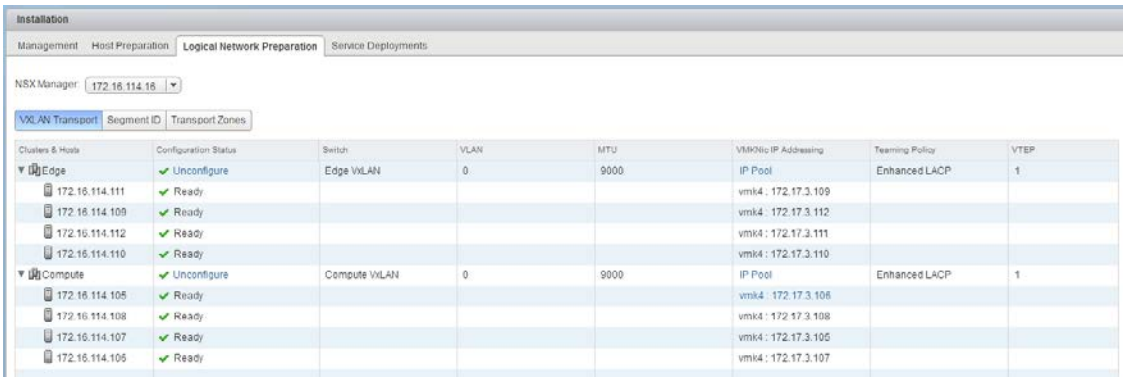

Figure 86 VXLAN IP addresses

6.6.7 Assign segment ID

The Segment ID determines the total number of logical switches that can be created in a given port group. NSX limits this number to 10,000 per port group and in most cases 1000 segments is enough. To configure this, navigate to **Home → Networking & Security → Installations → Logical Network Preparation → Segment ID** and click **Edit**.

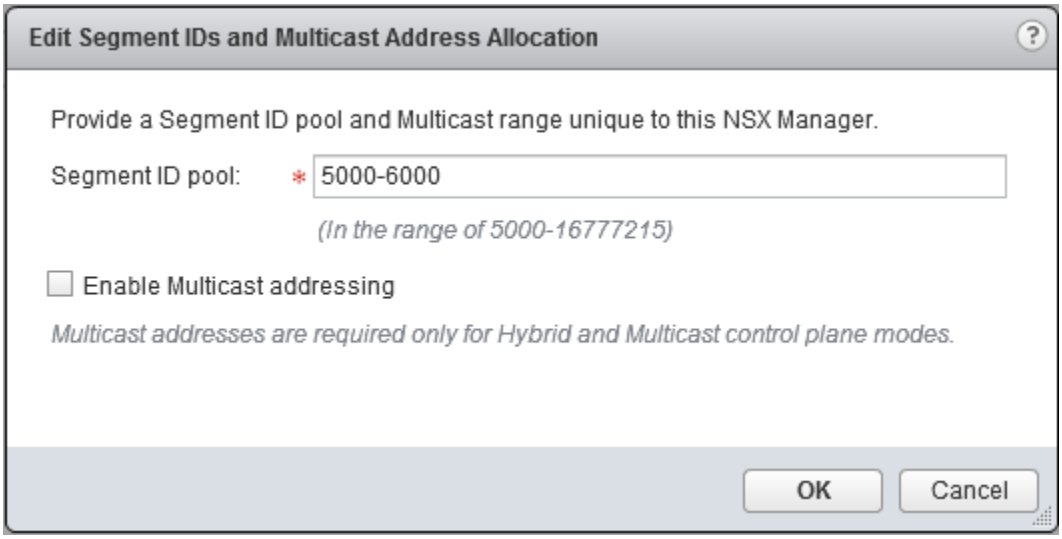

Figure 87 Segment IDs

6.6.8 Add a Transport Zone

The Transport zone controls which hosts can be reached by a logical switch. Transport zones can reach across clusters. DLR and ESG can route within a logical switch in a single transport zone only. This should be kept in mind when transport zones are designed. In this setup, the transport zone is spanned across both Compute and VIM.

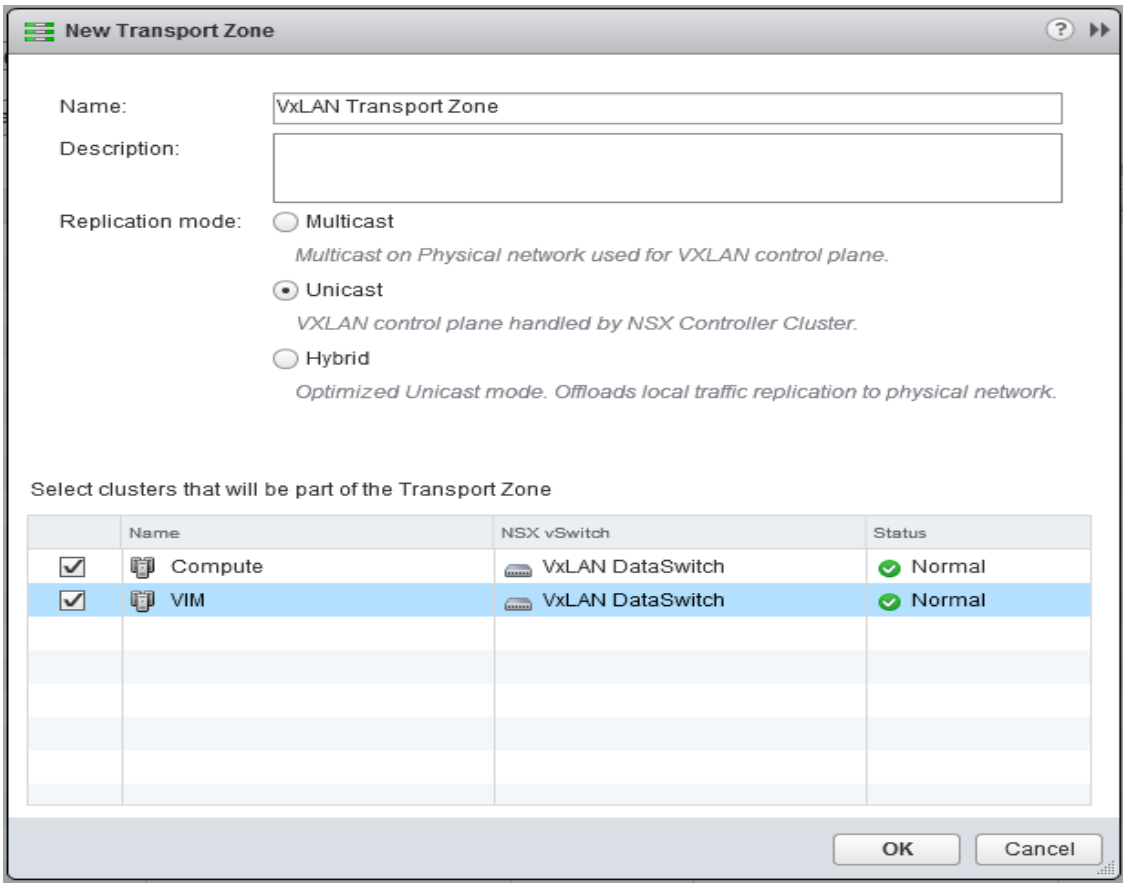

Figure 88 VxLAN Transport Zone

6.6.9 Create logical switch

The logical switch reproduces switching functionality in a virtual environment completely decoupled from the underlying hardware. When two logical switches are part of two different logical networks, a distributed logical router is needed to communicate between the logical networks. To demonstrate logical switch functionality create two VMs with a single NIC in each one of them.

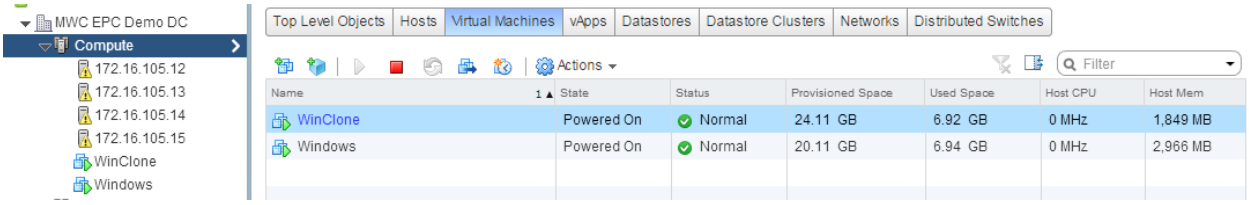

Figure 89 Virtual Machines

Navigate to **Home → Networking & Security → Logical Switches** and select the (**+**) sign to add a logical switch. Configure a name for the Logical switch and assign it to a transport zone. Create and enable IP Discovery and MAC learning as needed.

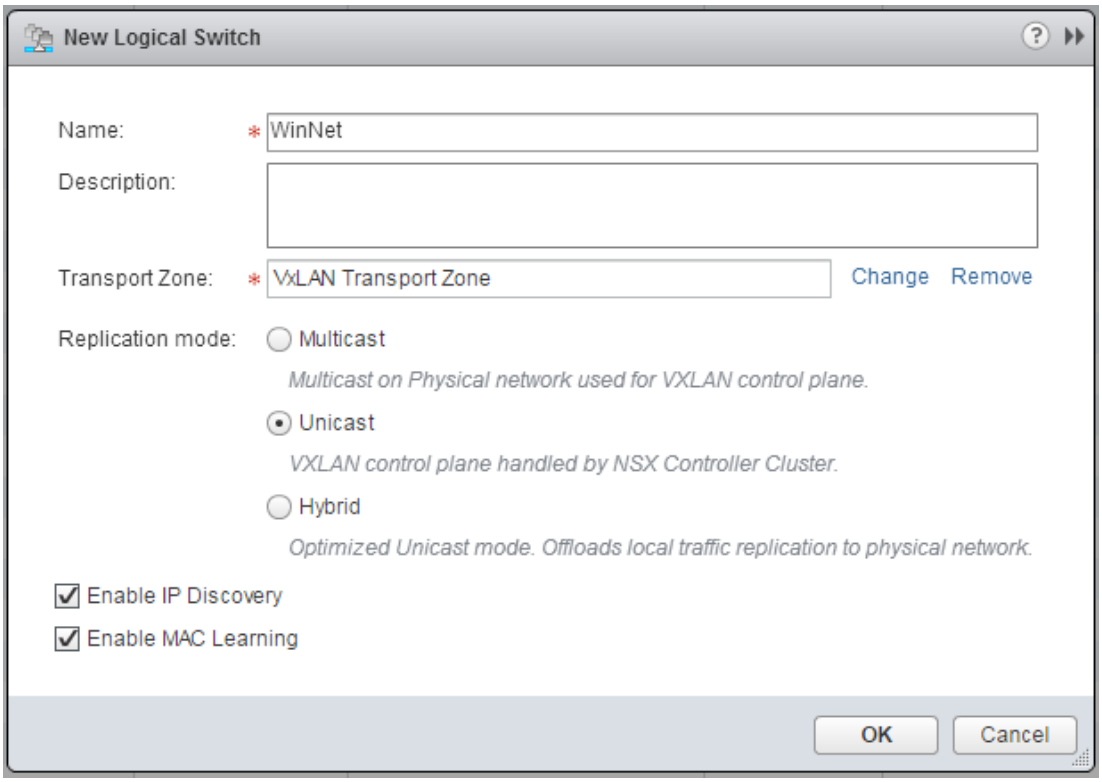

Figure 90 Create a new logical switch

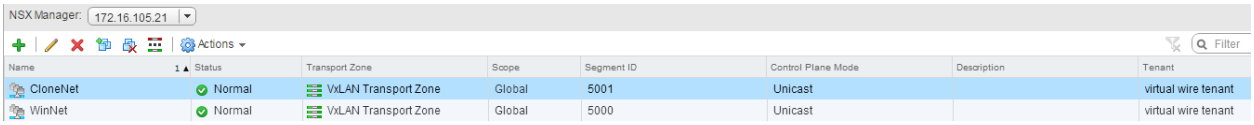

Figure 91 Transport zone

Click on **Add Virtual machine** to assign the logical network to respective VM NIC ports

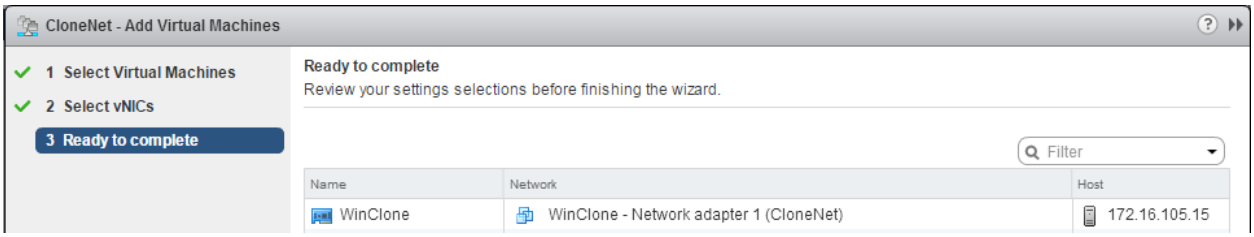

Figure 92 Virtual machine configuration

Once the VM to logical switch assignment is complete, the distributed vSwitch port-group will look as follows.

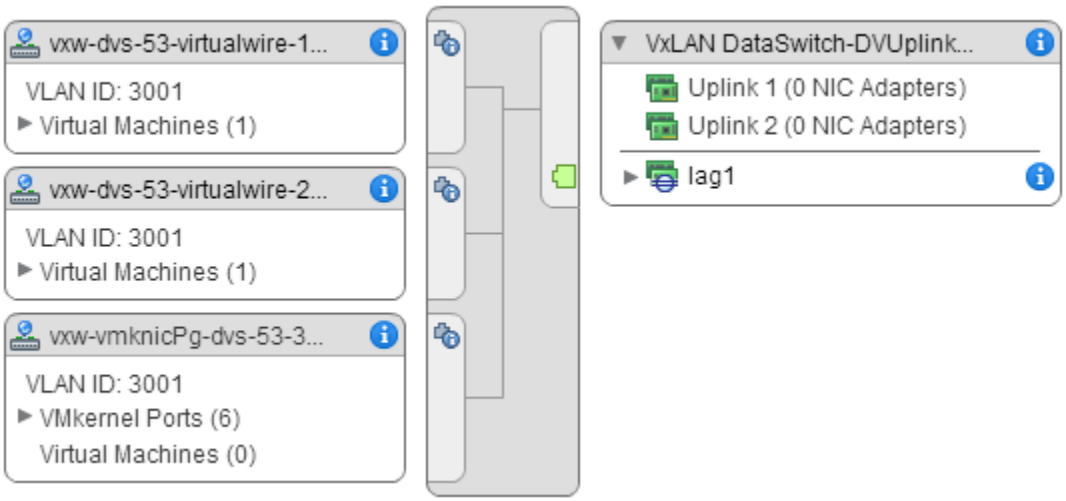

Figure 93 vSwitch port-group

6.6.10 Deploy and configure Distributed Logical Router

A Distributed Logical Router (DLR) is a virtual appliance that is deployed though the NSX manager that contains the routing control plane. DLR control plane function relies on NSX controller cluster to push routing updates to kernel modules. To deploy a DLR, navigate to **Home → Networking & Security → NSX Edges** and select (**+**).

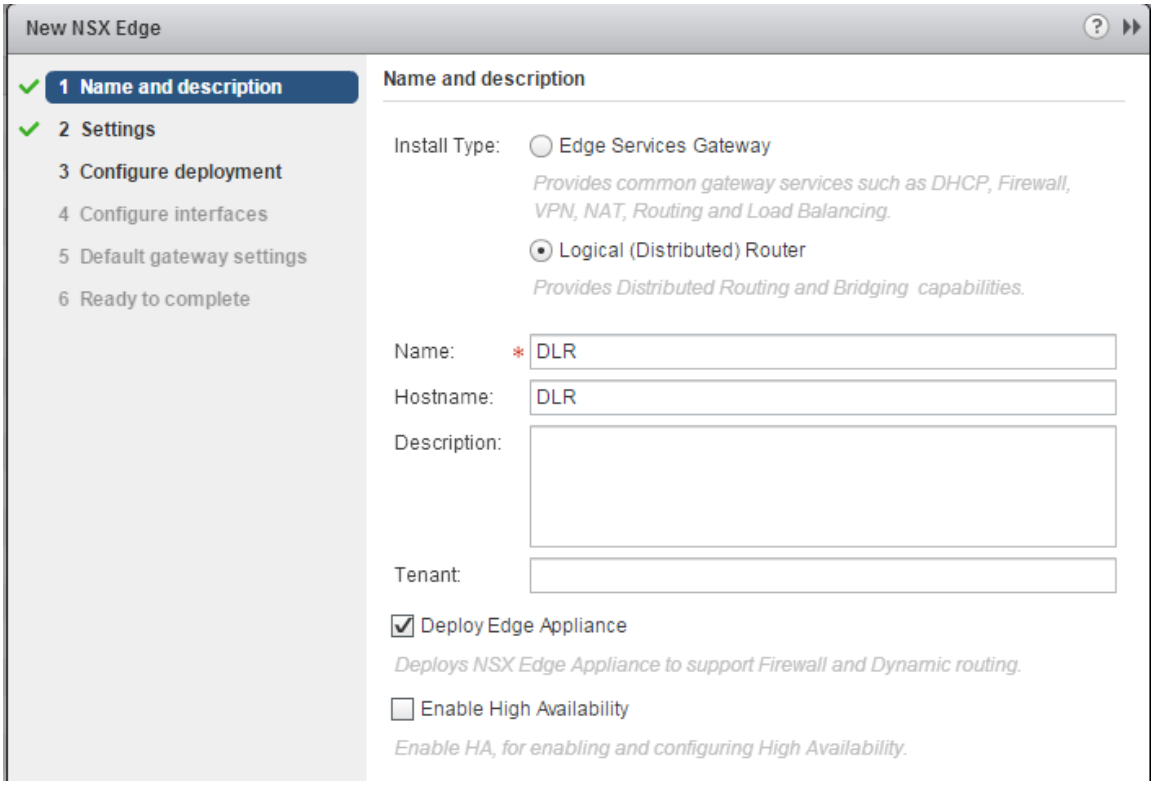

Figure 94 Create Distributed logical routers

Fill out the password for the DLR (*Hint: Configure same password as NSX controllers for easy management*).

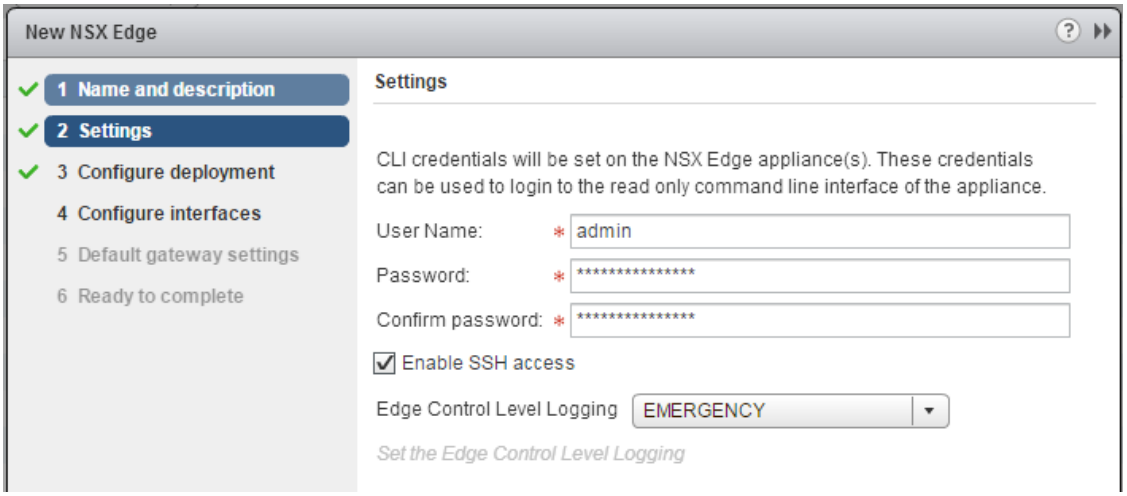

Figure 95 Distributed logical router settings

Select the Cluster/Host in which the DLR needs to be deployed.

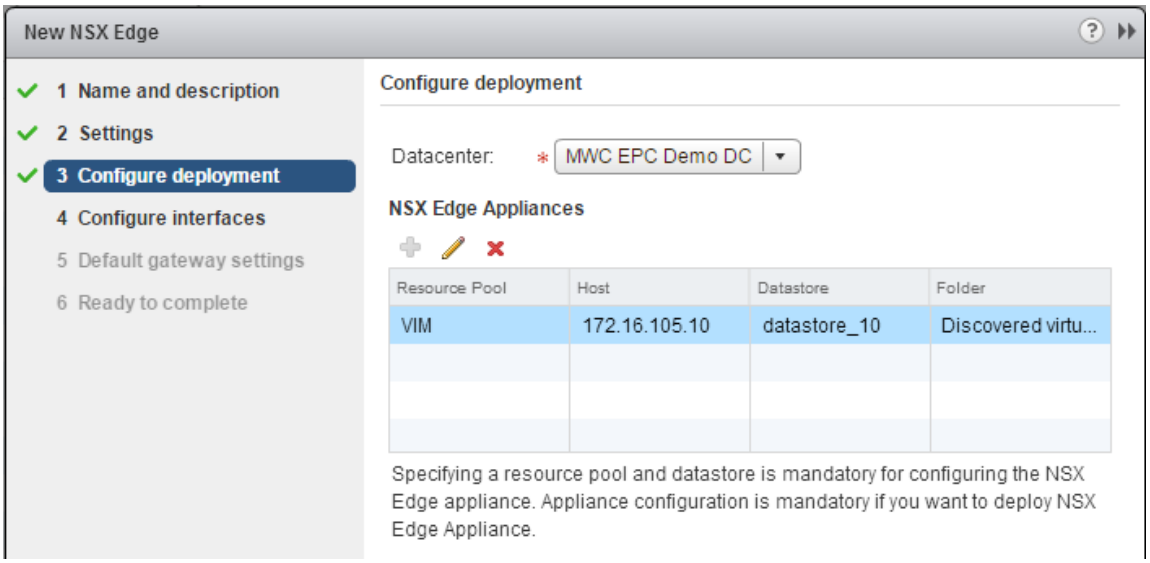

Figure 96 Configure deployment

Select the port group through which the DLR can be reached, and configure the connected interface of the DLR. The connected interface IP is the gateway IP of the VMs in the given logical switch.

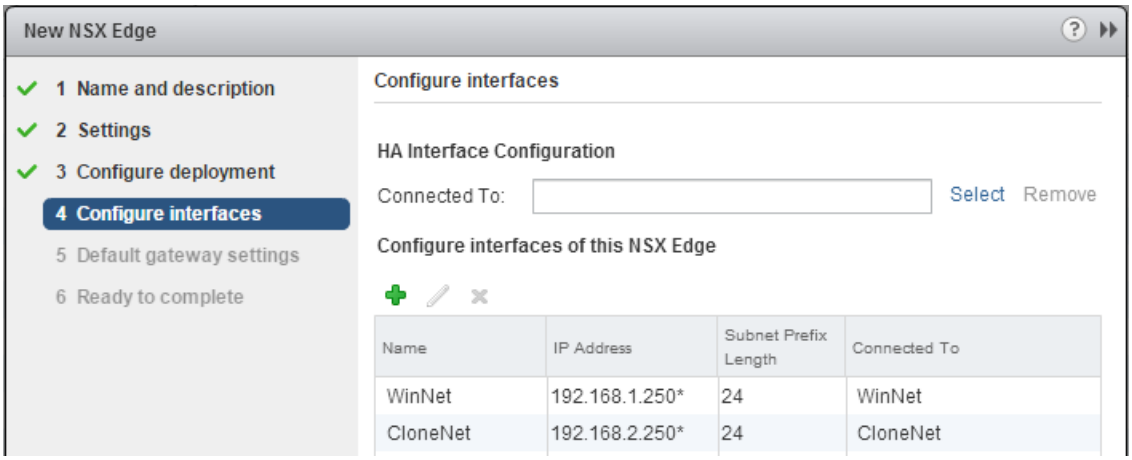

Figure 97 Configure interfaces

This completes the DLR deploy and configuration process and VMs across logical switches will be able to communicate between them.

6.6.11 Deploy Edge services gateway

To deploy an Edge Services Gateway, we need to satisfy certain prerequisites that include creating a logical switch to connect DLR with ESG, creating a virtual distributed switch in hosts for non-VXLAN traffic to communicate with outside world and deploying the actual ESG appliance.

6.6.11.1 Create a logical switch

A logical switch needs to be created to establish connectivity between the DLR uplink and the ESG internal link.

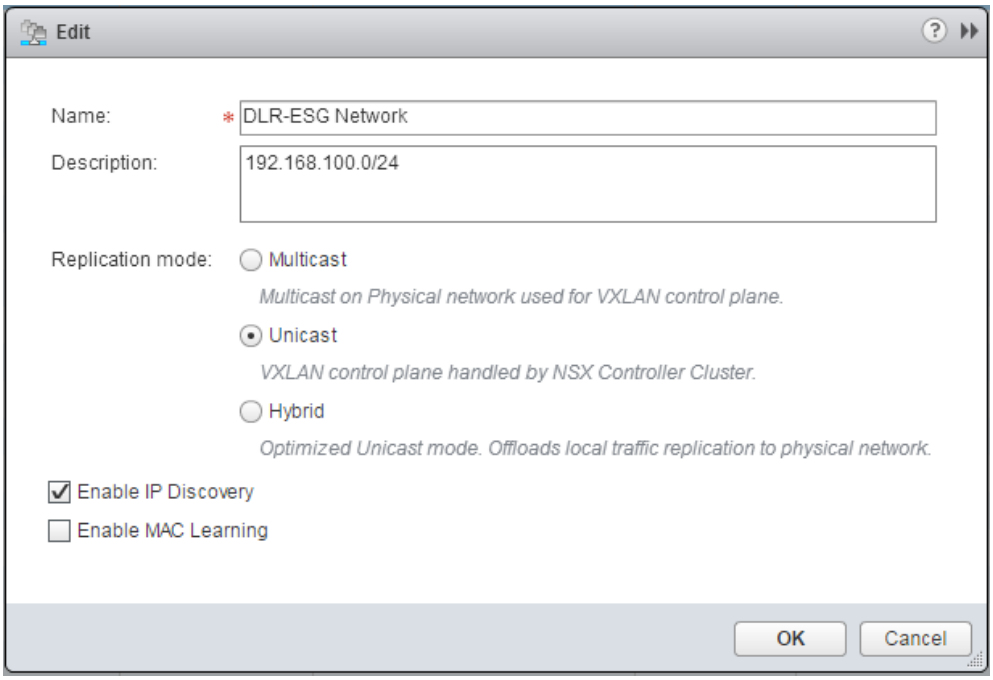

Figure 98 Create logical switch

6.6.11.2 Create a distributed switch

On the VIM cluster hosts, we need to create a vSphere distributed switch to enable the ESG appliance to communicate to the outside world. Follow the previous distributed switch creation example and create a new one with uplinks from the VIM cluster as shown in the diagram.

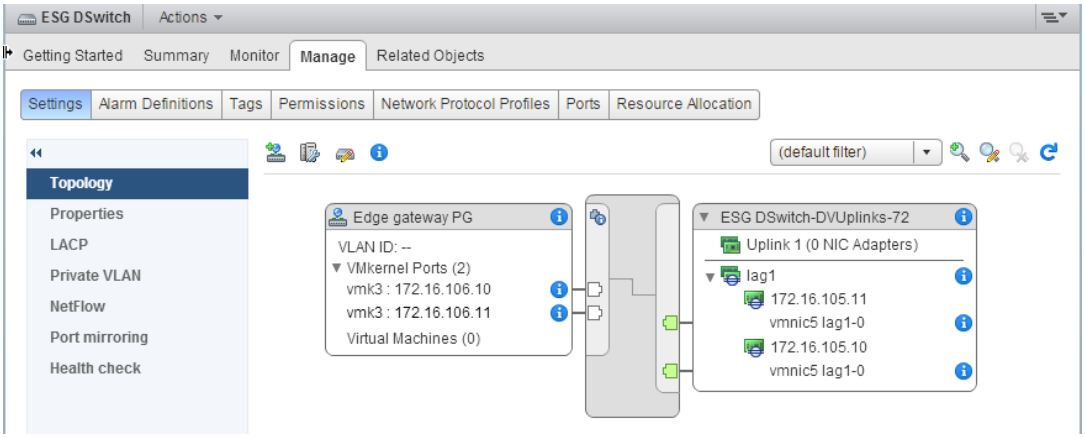

Figure 99

6.6.11.3 Create uplink port in DLR

When initially created DLRs have two links to enable routing between the logical switch networks only. In this step, we will create an uplink port to connect to ESG and configure ESG IP as default gateway. Navigate to **Home → Networking & Security → NSX Edges → DLR → Manage → Settings → Interfaces** and select the (**+**) sign.

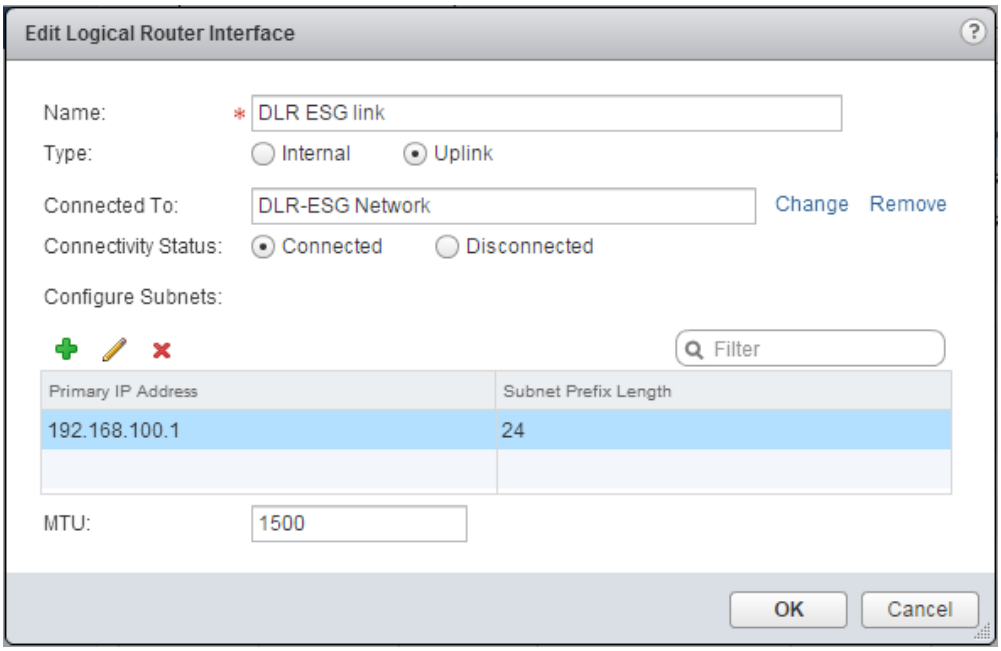

Figure 100 Edit logical router interface

Navigate to **Routing → Global Configuration → Default Gateway** and select the **Edit** button to configure the default gateway.

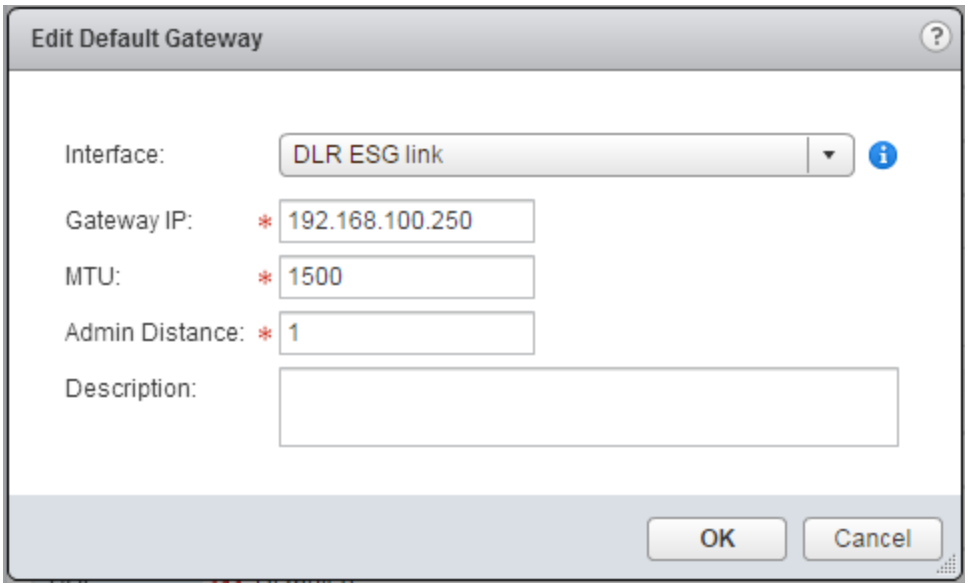

Figure 101 Edit the default gateway

6.6.11.4 Add an ESG

With the necessary configuration complete, we can deploy the ESG appliance. To deploy, navigate to **Home → Networking & Security → NSX Edges** and select (**+**).

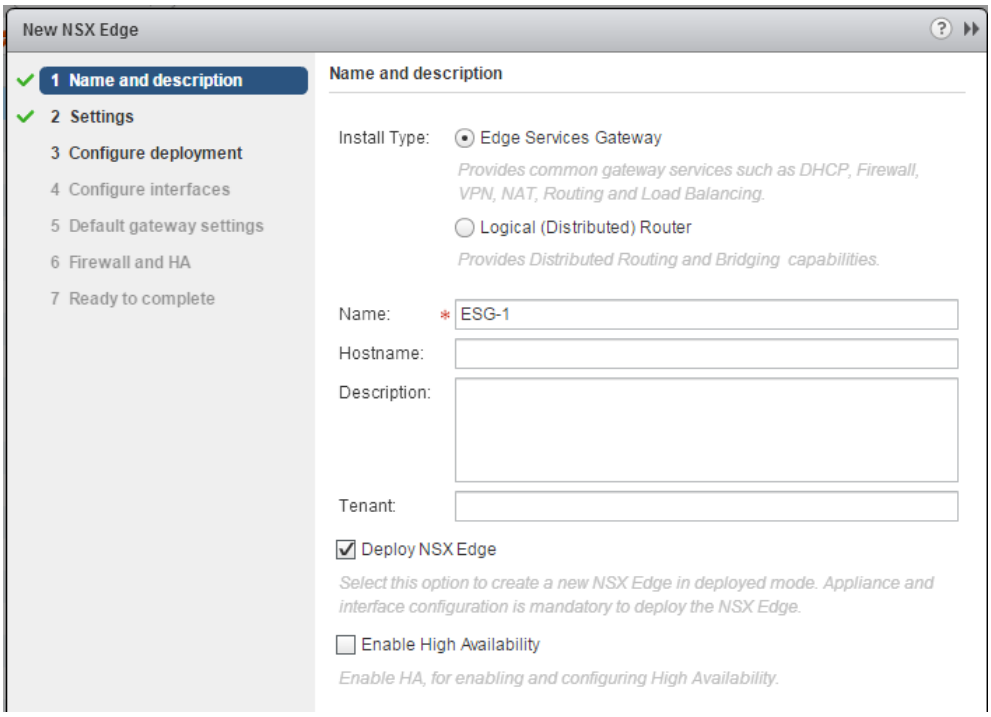

Figure 102 Deploy ESG

Configure the SSH access password and click **Next**. Under the Configure Deployment section, select the **Compact** Appliance size and place the appliance in the VIM cluster.

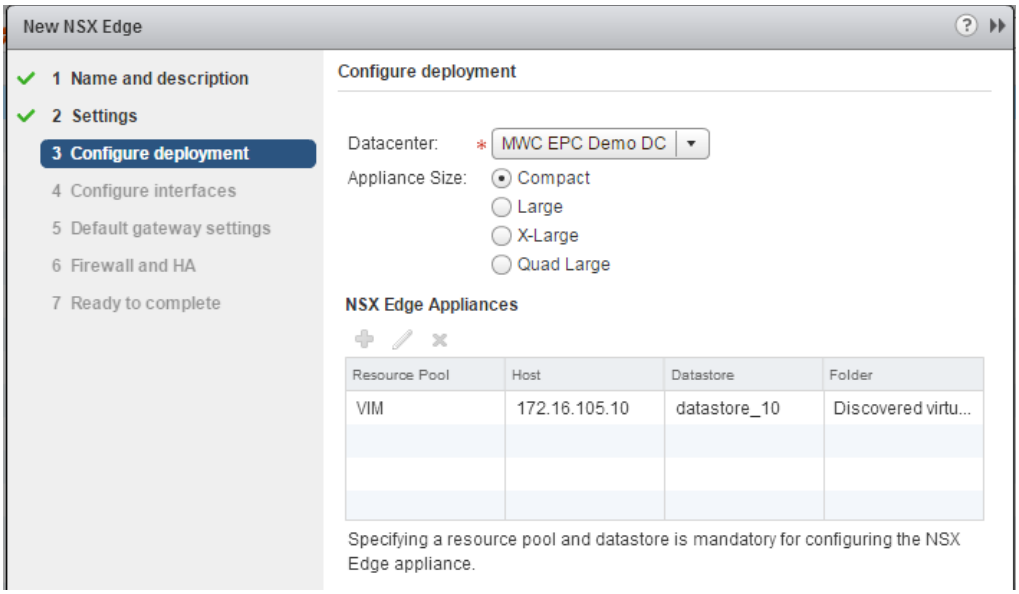

Figure 103 Configure deployment

Configure the internal and uplink interfaces for the ESG.

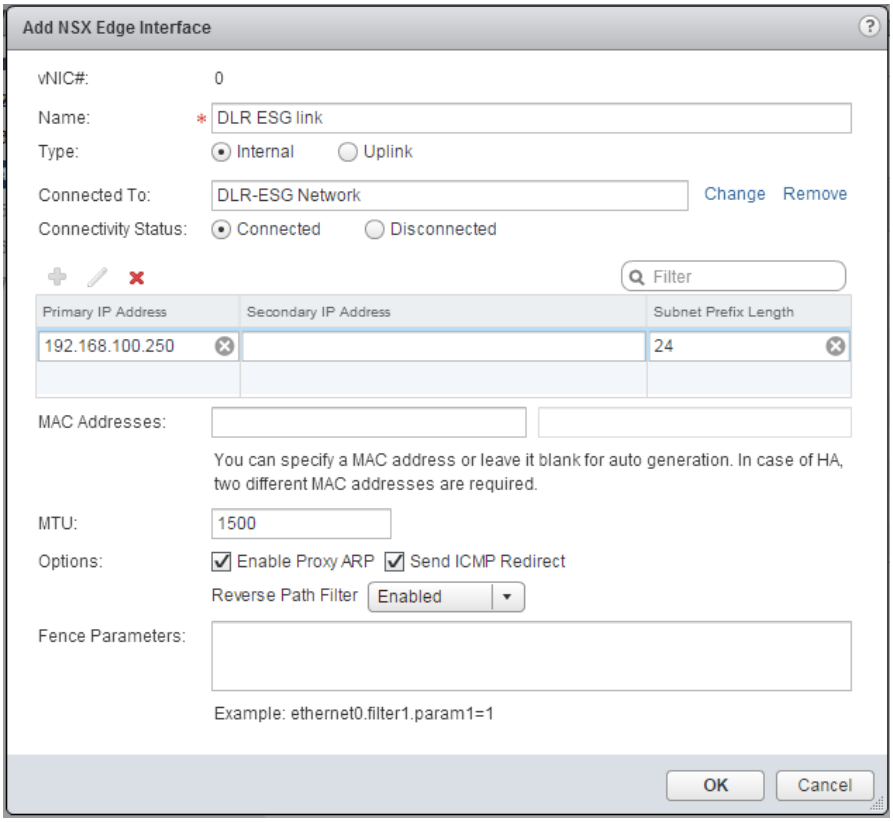

Figure 104 Add NSX interface - internal

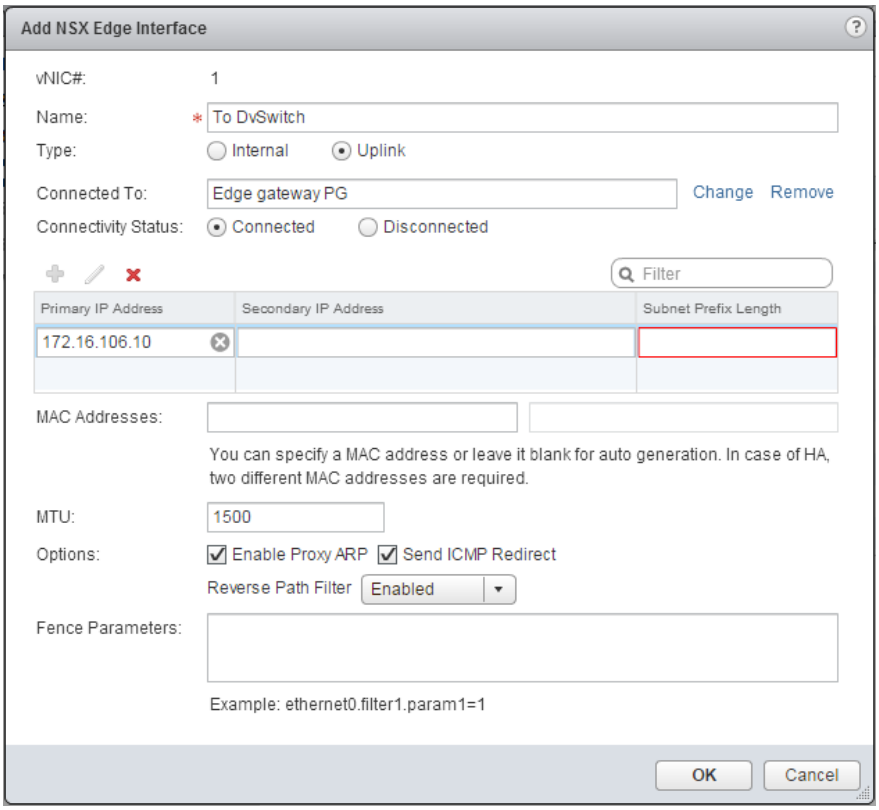

Figure 105 Add NSX interface - uplink

Under the Default Gateway Settings, configure the uplink physical port gateway IP to reach the outside world

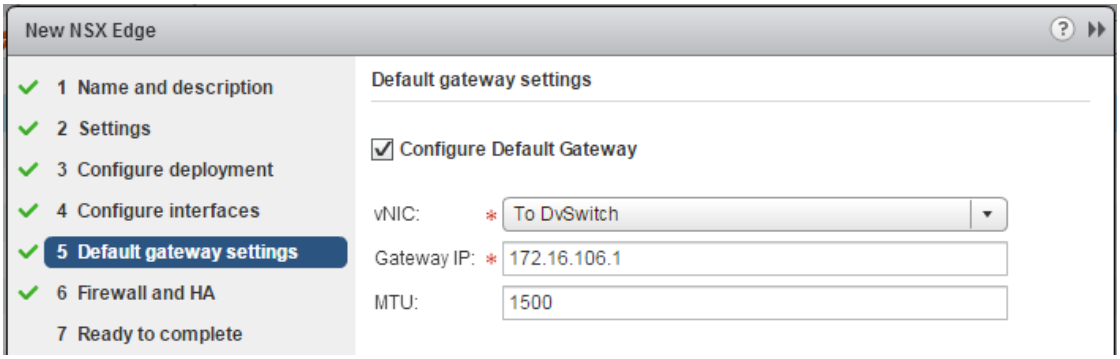

Figure 106 Default gateway settings

Make sure to enable Firewall with Default Traffic policy accept and click **Next**.

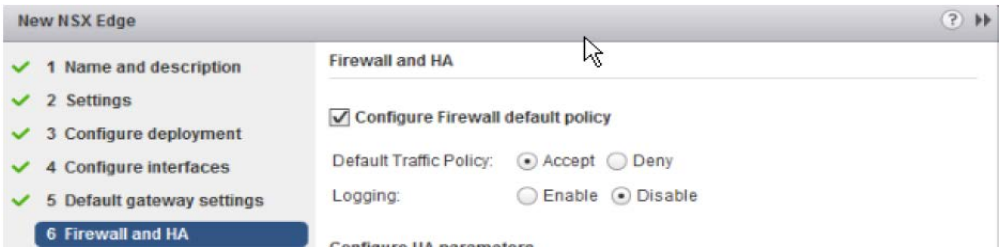

Figure 107 Configure firewall policy

Review the configured options and click **Finish**.

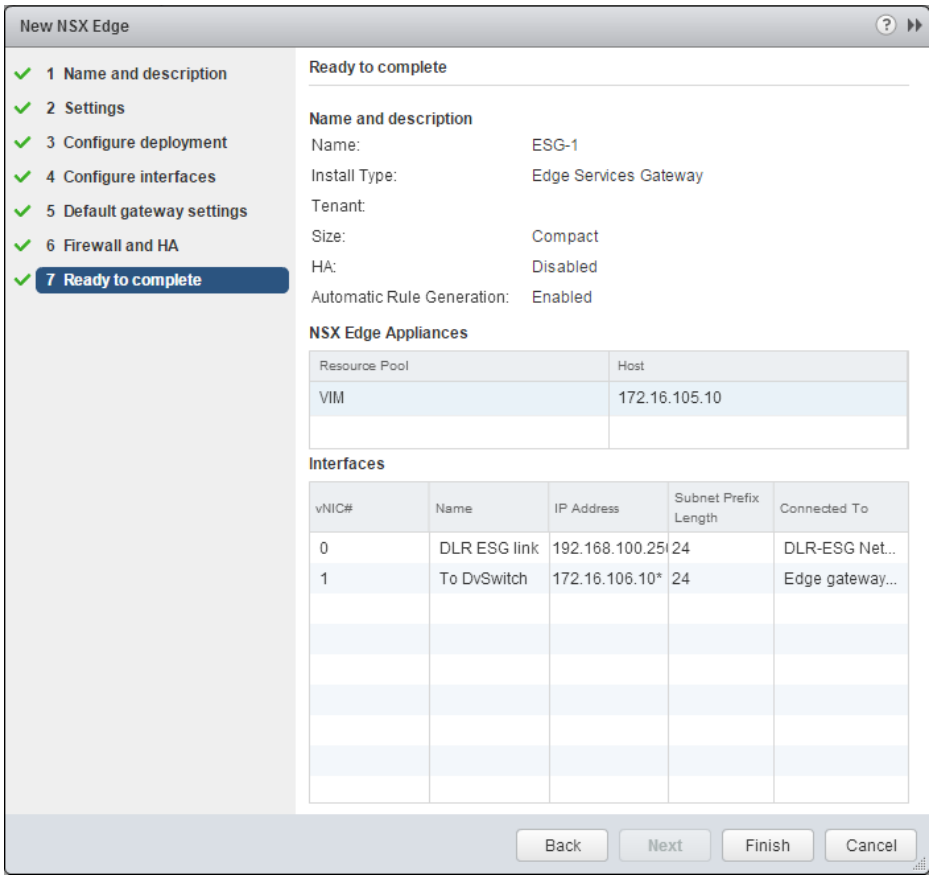

Figure 108 NSX configuration

6.6.12 Configure OSPF on DLR

The link between ESG and DLR is a router-to-router connection. For ESG to reach logical networks connected to DLR, we need to enable a routing protocol to enable reachability. To enable OSPF, navigate to **Home → Networking & Security → NSX Edges → DLR → Manage →Routing → Global Configuration** and assign a Router ID for Dynamic Routing Configuration.

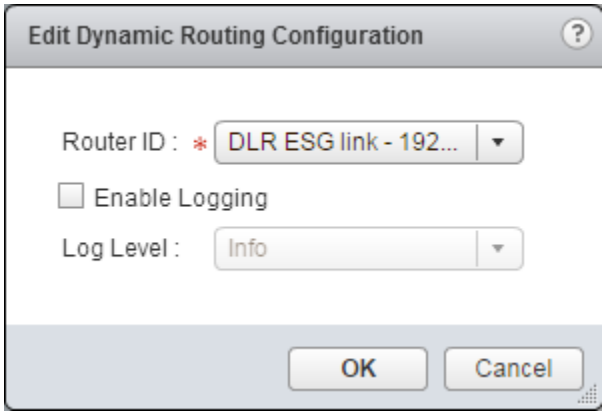

Figure 109 Edit DLR configuration

Navigate to OSPF section, Configure the Forwarding address same as the Uplink interface IP and a unique unused IP address in the same subnet as the uplink interface.

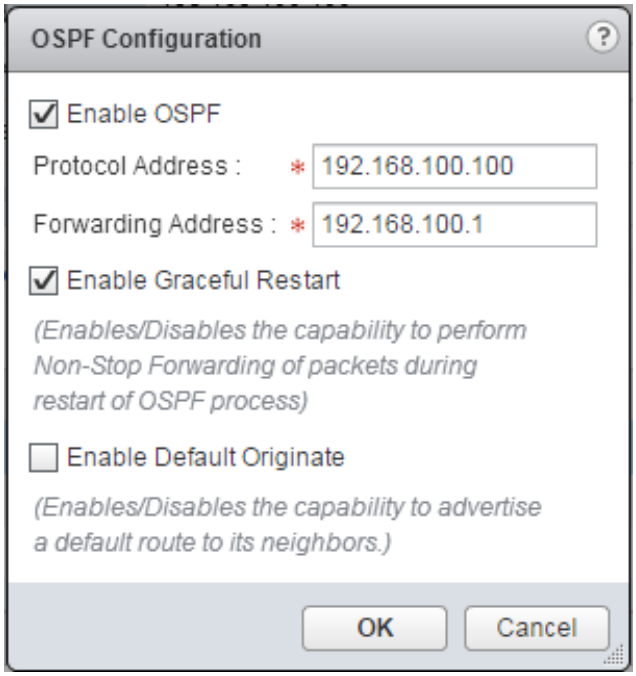

Figure 110 OSPF configuration

Under Area definitions, remove the default NSSA Type Area 51 and configure **Normal Type Area 0**.

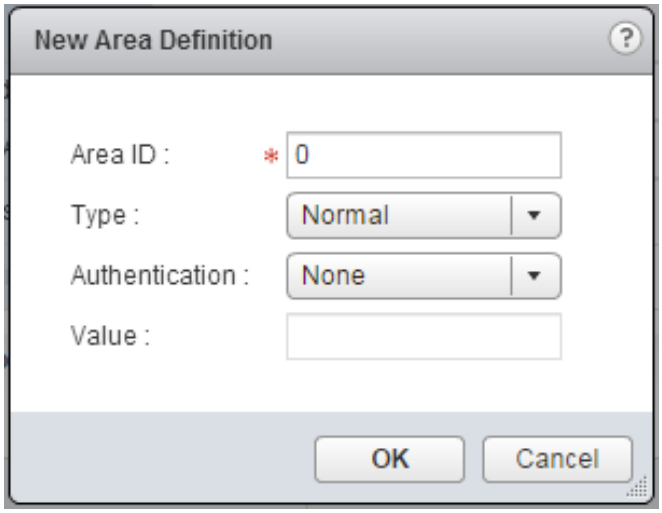

Figure 111 Area definition

Assign the configured Area to DLR – ESG link under Area to Interface Mapping

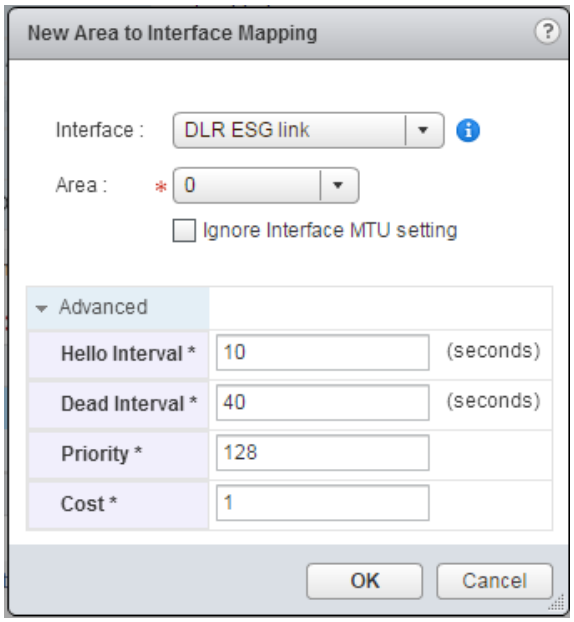

Figure 112 Area interface mapping

Review all the changes and click **Publish Changes**.

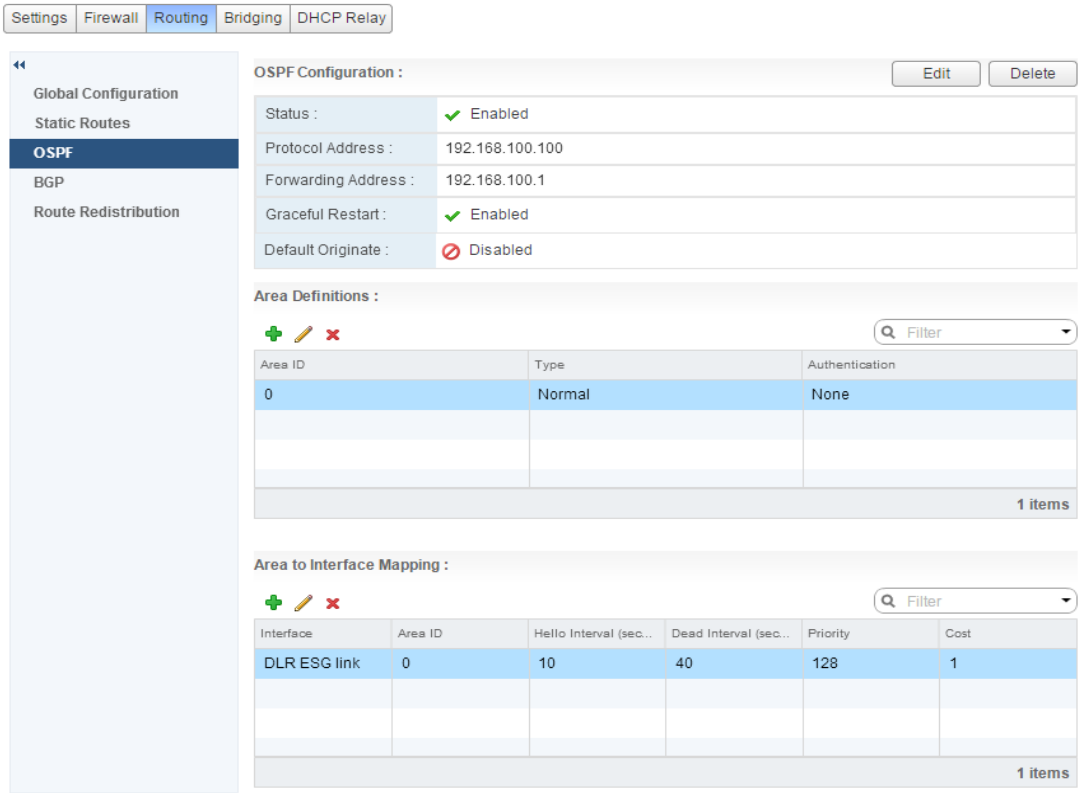

Figure 113 OSPF configuration

6.6.13 Route redistribution and firewall configuration

Even though we enable OSPF in the uplink port of DLR, the internal links are not part of OSPF database yet. To bring internal links to OSPF, select **Route Redistribution** and make sure the connected routes are part of route redistribution table.

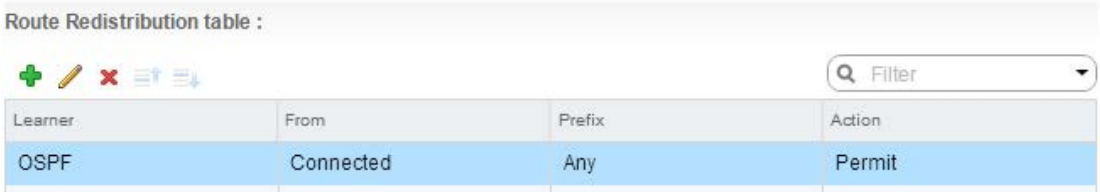

Figure 114 Route redistribution

Configure a firewall filter for SSH to logical router protocol address as well.

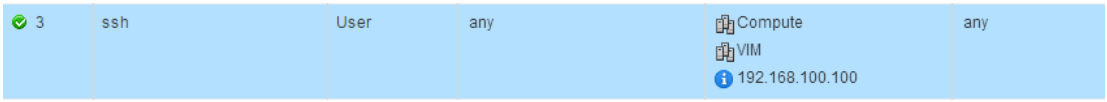

Figure 115 SSH firewall filter

6.6.14 Configure OSPF on ESG

Configuring OSPF in ESG is similar to DLR. We have to configure router ID, under OSPF configuration when we enable OSPF protocol, make sure to enable **Default Originate** to propagate a default route down to DLR.

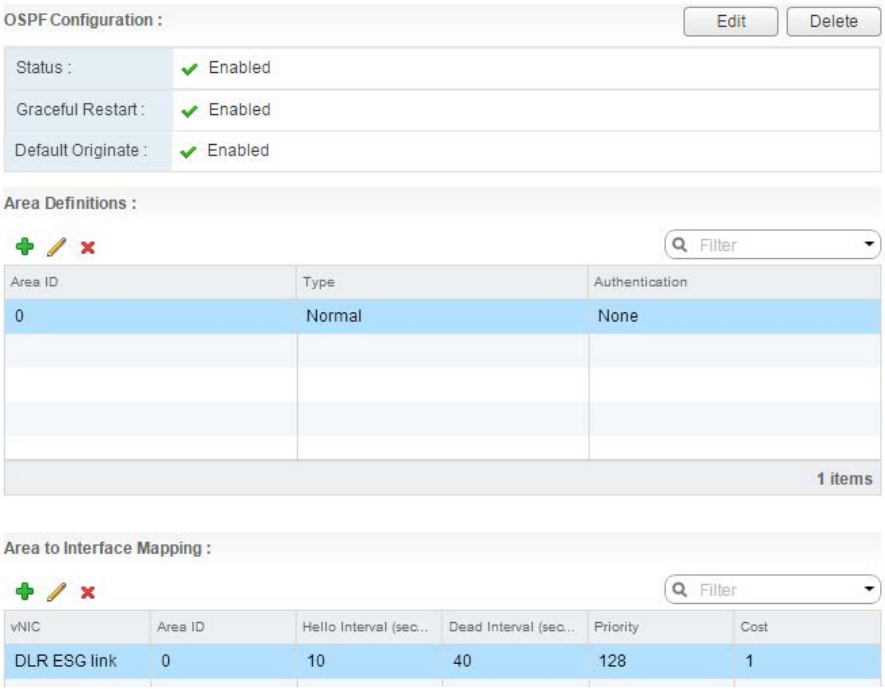

Figure 116 Configure OSPF in ESG

Redistribute the connected interfaces of ESG to OSPF database like was done for DLR.

6.7 Install vCloud Director

6.7.1 Install and Bringup Windows VM

To host a SQL server like Windows SQL server 2012, bring up a windows VM with four CPUs, 16 GB RAM and 100GB HD. The VM only needs one NIC; make sure it is part of the management network.

6.7.2 Install SQL Server in Windows VM

With VCD, 8.0 SQL Express editions are not compatible. Make sure to get a licensed edition like SQL Server Enterprise 2012. Mount the ISO image in the VM CD drive and double click on Setup to start the installation process. Select **All features** with the defaults under Setup Role.

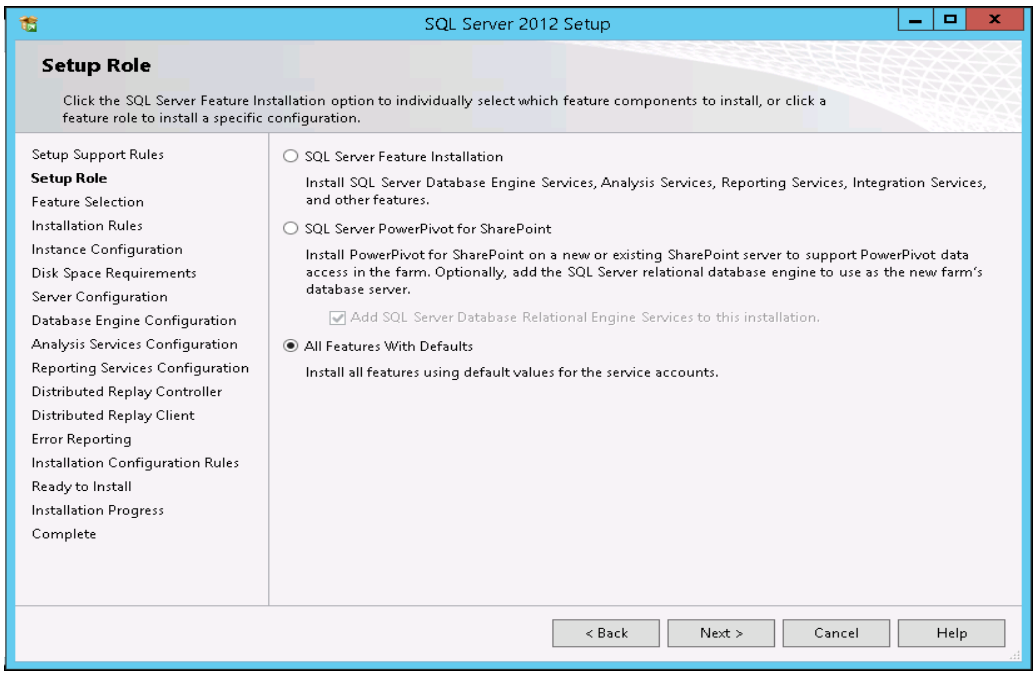

Figure 117 Install SQL Server

Create a named instance of your choice.

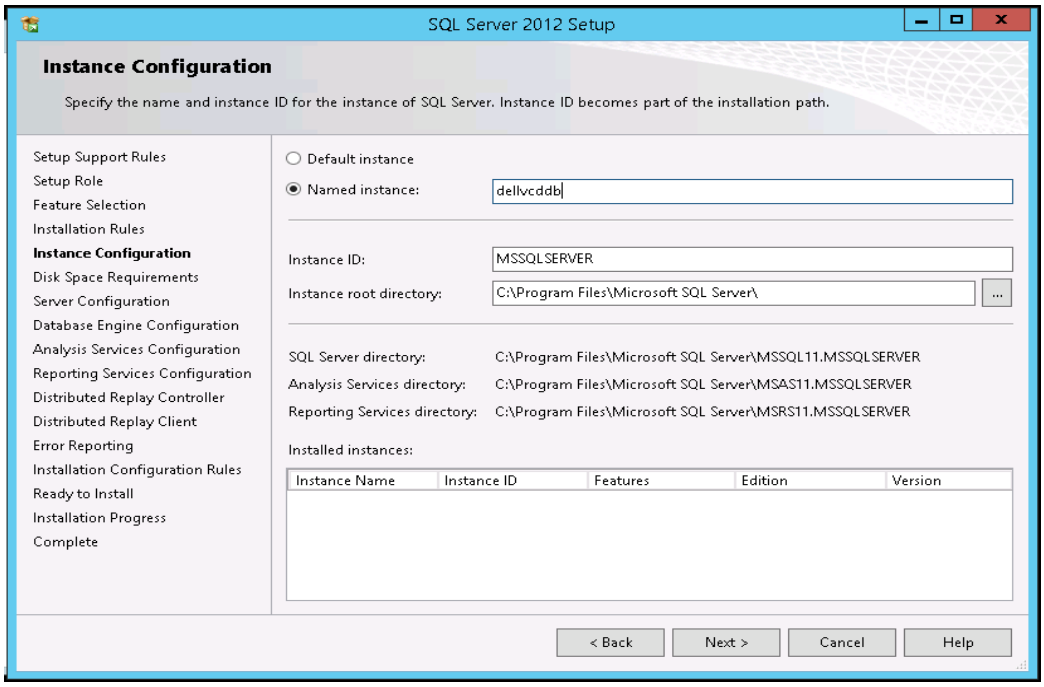

Figure 118 Configure SQL instance

Continue to click **Next**, during database engine configuration, configure a password for the administrator by choosing **Mixed Mode** and click **Next**.

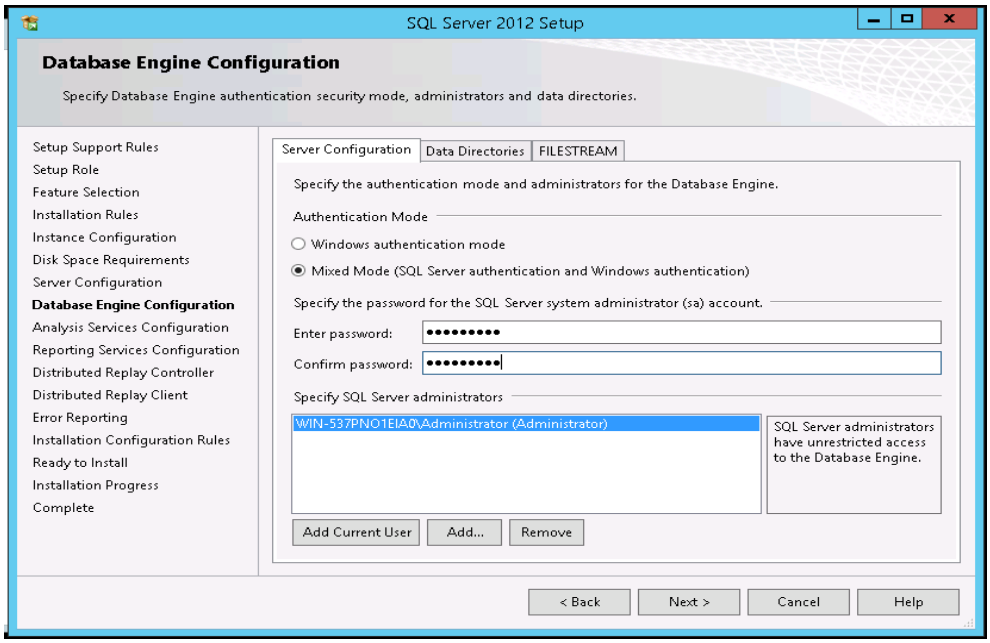

Figure 119 Configure password

Do not configure any other service and click **Install** when you are ready to install.

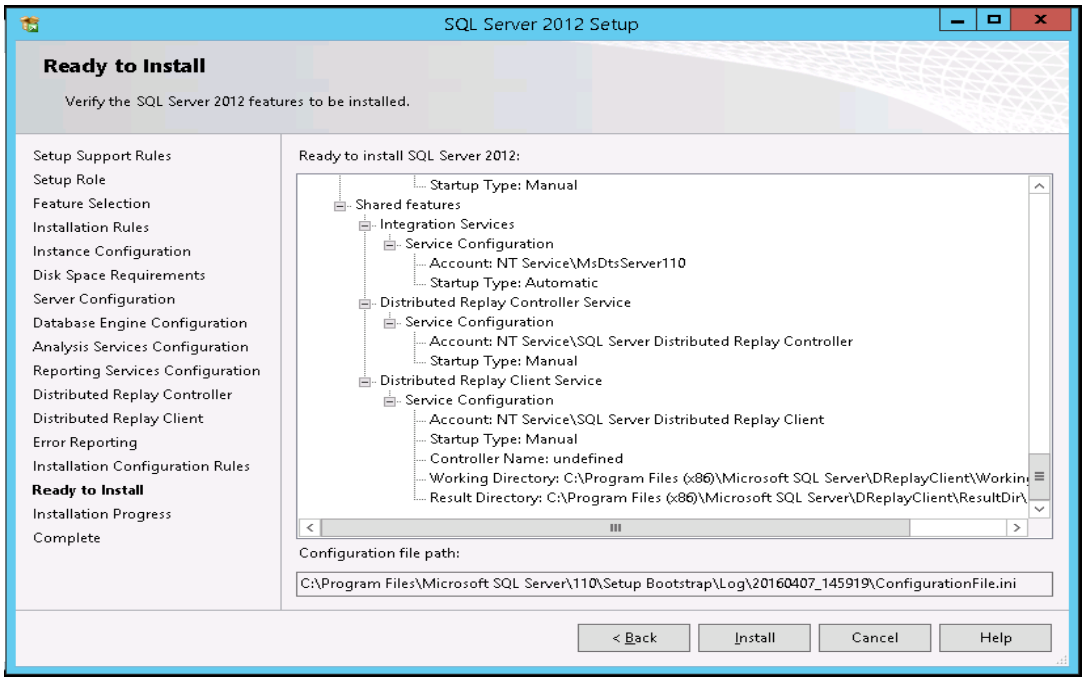

Figure 120 SQL install

6.7.3 Configure the SQL Server

Open Microsoft SQL Server Studio and login using mixed mode with username ‘sa’ and the password we created during installation.

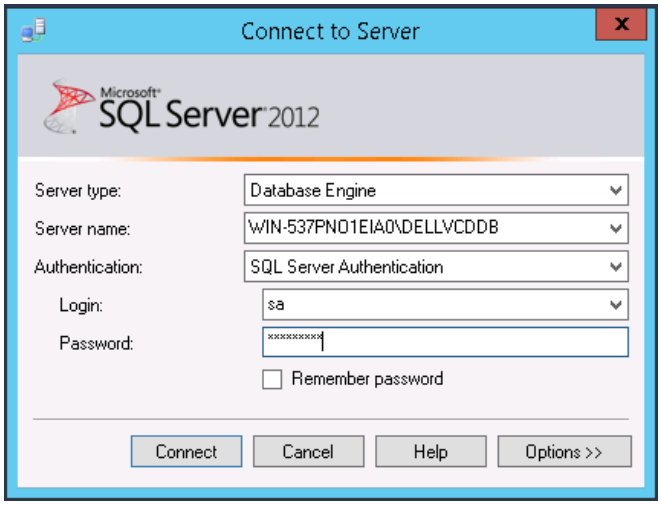

Figure 121 Connect to SQL sever

6.7.3.1 Create a new user for vCloud

Right click on **Security** to create a new login for the SQL server, uncheck **Enforce password expiration**.

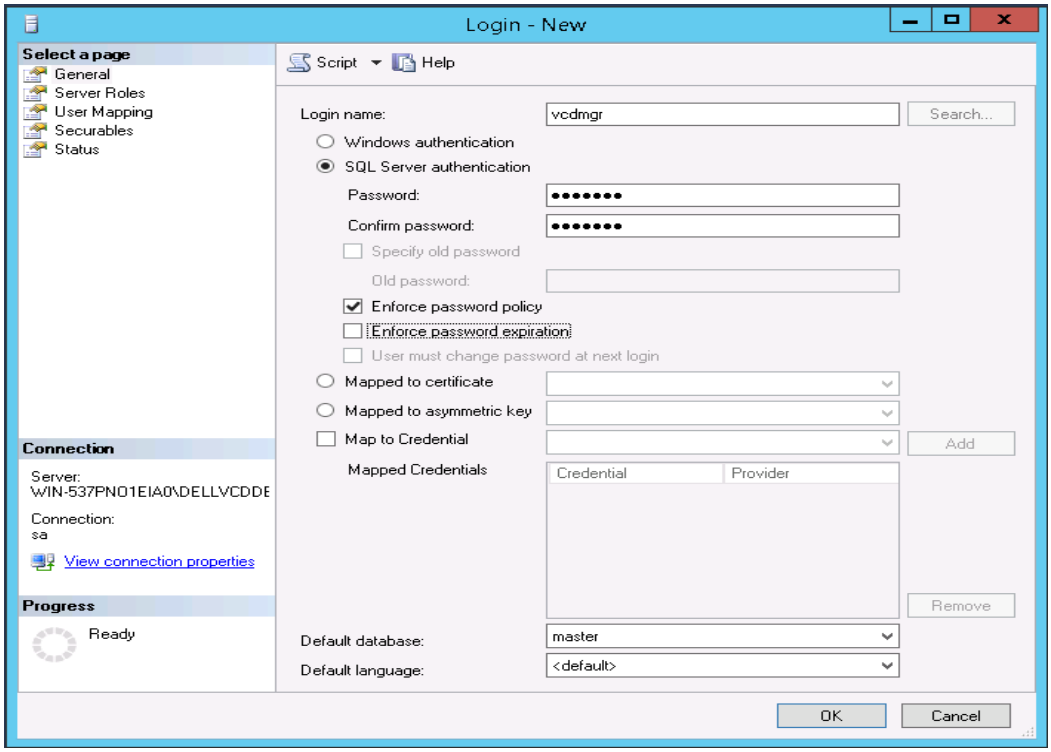

Figure 122 New vCloud user

6.7.3.2 Create a new Database

Create a new database for vCloud and assign the new user that was just created as the owner. Change the Initial size of Row Data and Log file size to 1024 and 128 and Autogrowth to 512 MB and 128 MB with Limited Growth to 2000MB as shown below. Do not click Ok.

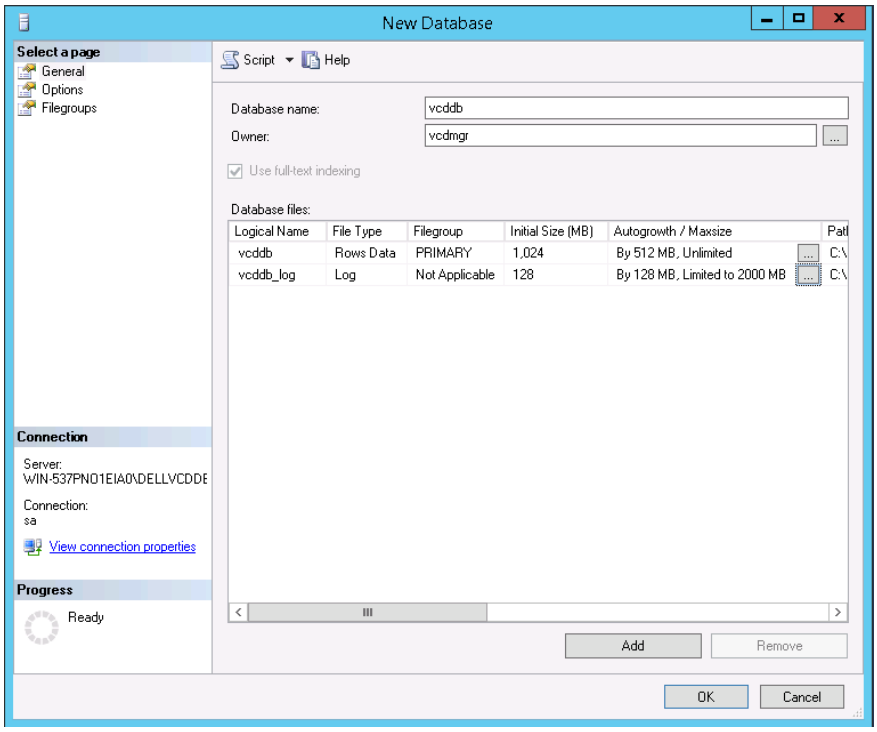

Figure 123 New Database

Navigate to Options and configure the Collation from the default to **Latin1_General_CS_AS** and Recovery model to **Simple** and Click **OK**.

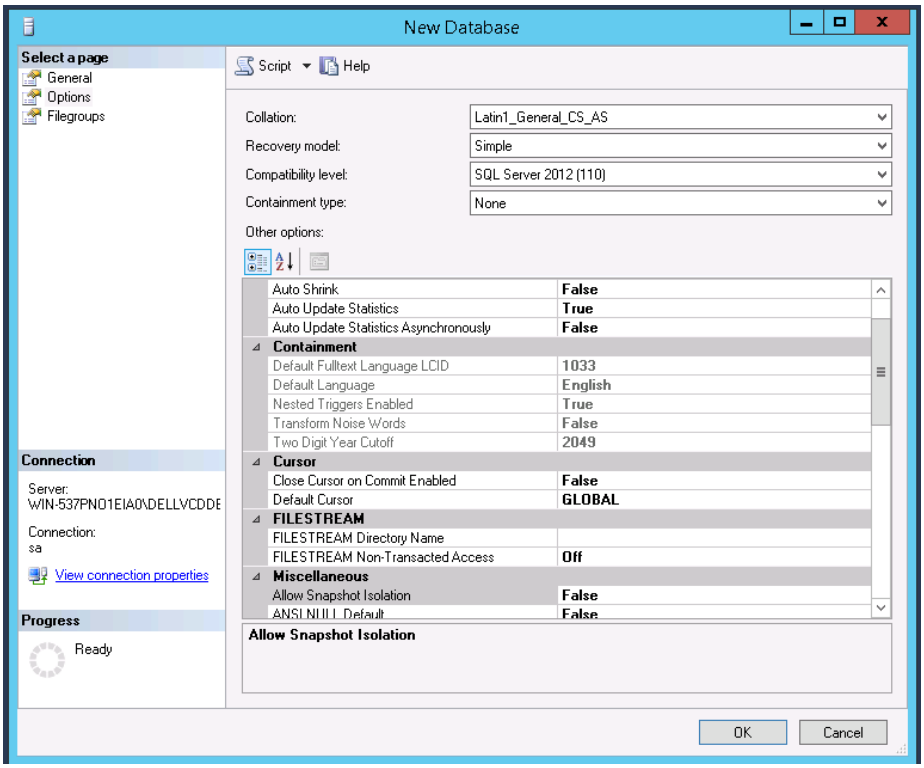

Figure 124 Configure database

6.7.3.3 Configure the database

Copy the script below or from the vCloud installation guide and select **New Query**. Change the name [] bracket to the name of the database that was created in previous step and click **Execute**.

```
USE [vcddb]
GO
ALTER DATABASE [vcddb] SET RECOVERY SIMPLE;
ALTER DATABASE [vcddb] SET SINGLE_USER WITH ROLLBACK IMMEDIATE;
ALTER DATABASE [vcddb] SET ALLOW_SNAPSHOT_ISOLATION ON;
EXEC sp_addextendedproperty @name = N'ALLOW_SNAPSHOT_ISOLATION', @value
= 'ON';
ALTER DATABASE [vcddb] SET READ_COMMITTED_SNAPSHOT ON WITH NO_WAIT;
EXEC sp_addextendedproperty @name = N'READ_COMMITTED_SNAPSHOT', @value =
 'ON';
ALTER DATABASE [vcddb] SET MULTI_USER;
GO
```

6.7.4 Setup DNS server and add entries

Note: In vCloud director installation, this is an important step. Setting up the DNS server with the wrong hostname of a RHEL VM will result in the vCloud director application failing to start.

In the windows VM, enable DNS server using server manager. **Navigate to Tools → DNS** to launch DNS manager. Create a forward lookup zone with a name like Dell EMCnfv.com and continue clicking **Next**, then click **Finish**. If you have a dedicated DNS server in your setup, the following steps should be completed on that DNS server.

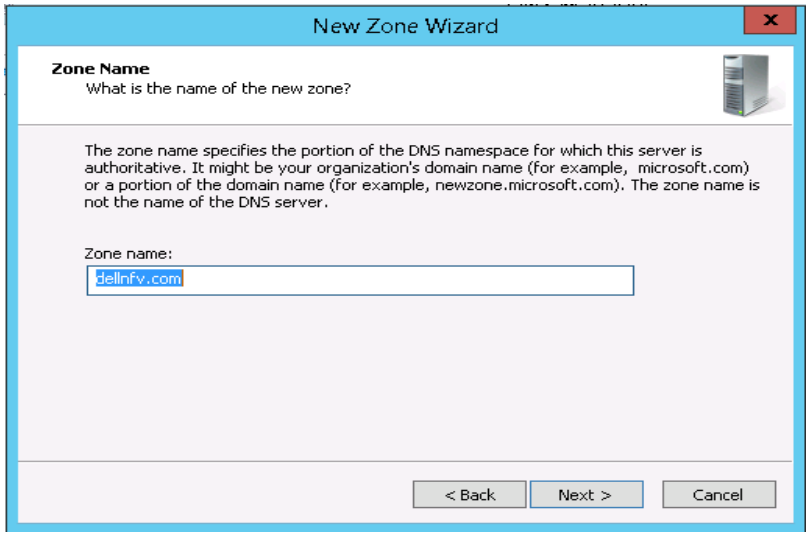

Figure 125 Creating new zone

Create a reverse lookup zone with the Network ID of the management subnet of the given deployment. Continue clicking **Next**, then click **Finish**.

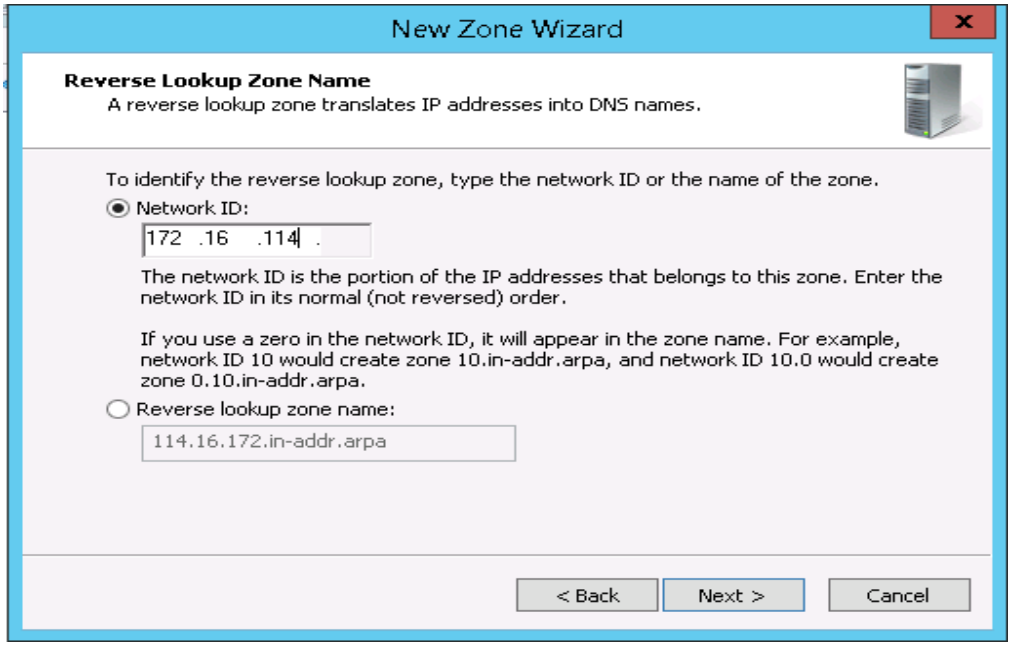

Figure 126 New zone wizard

Right click on **Forward Lookup Zones → Dell EMCnfv.com → New Host (A or AAAA)** and add a new entry for vCloud director.

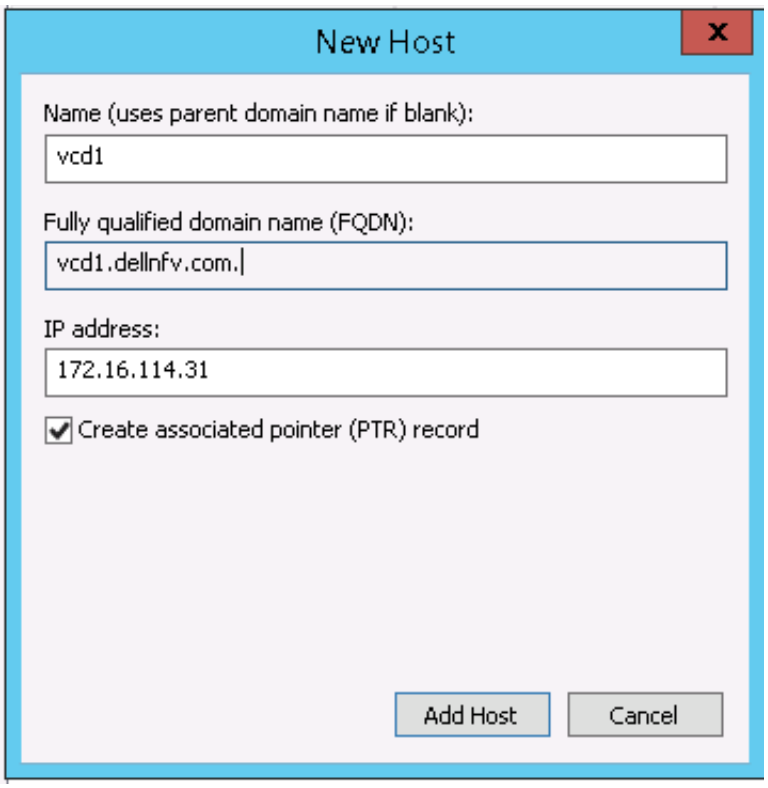

Figure 127 New Host

Note the FQDN and the IP address configured in this step, this same name and IP address should be used while creating the RH VM in the next step.

6.7.5 Install and Bring up RedHat Enterprise Linux VM

Create a VM with four CPUs, 4 GB RAM, 20GB HDD and two NICs. Make sure to configure both NICs in the management network DvSwitch. Follow the steps in the link below, if there are any doubts in creating the RHEL VM. Configure the hostname during installation by replacing localhost.localdomain with **vcd1.Dell EMCnfv.com** as configured in the DNS server. Configure the NIC1 IP as the same IP configured in the DNS server. Configure your RHEL login to subscribe and download the updates and applications.

http://www.kendrickcoleman.com/index.php/Tech-Blog/how-to-install-vcloud-director-on-rhel-62-no-gui.html

6.7.5.1 Configure Firewall rules in RH

Configure the iptables as below. The rules are based on this article

```
# Begin listing vCloud Director Ports Needed
# vCloud WebServices
-A RH-Firewall-1-INPUT -i eth0 -m state --state NEW -m tcp -p tcp --
dport 443 -j ACCEPT
# vCloud Optional
-A RH-Firewall-1-INPUT -i eth0 -m state --state NEW -m tcp -p tcp --
dport 80 -j ACCEPT
# SSH
```

```
-A RH-Firewall-1-INPUT -i eth1 -m state --state NEW -m tcp -p tcp --
dport 22 -j ACCEPT
# vCloud Remote Console
-A RH-Firewall-1-INPUT -i eth1 -m state --state NEW -m tcp -p tcp --
dport 902 -j ACCEPT
-A RH-Firewall-1-INPUT -i eth1 -m state --state NEW -m tcp -p tcp --
dport 903 -j ACCEPT
#NFS Trasfer Service from other vCD Cells - Add for every vCD Cell
-A RH-Firewall-1-INPUT -d IP_of_vCD-Cell -i eth0 -m state --state
NEW -m tcp -p tcp --dport 111 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_vCD-Cell -i eth0 -m state --state
NEW -m udp -p udp --dport 111 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_vCD-Cell -i eth0 -m state --state
NEW -m tcp -p tcp --dport 920 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_vCD-Cell -i eth0 -m state --state
NEW -m udp -p udp --dport 920 -j ACCEPT
#NFS Transfer Service NFS Datastore
-A RH-Firewall-1-INPUT -d IP_of_NFS_Server -m state --state NEW -m
tcp -p tcp --dport 111 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_NFS_Server -m state --state NEW -m
tcp -p tcp --sport 111 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_NFS_Server -m state --state NEW -m
udp -p udp --dport 111 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_NFS_Server -m state --state NEW -m
udp -p udp --sport 111 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_NFS_Server -m state --state NEW -m
tcp -p tcp --dport 920 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_NFS_Server -m state --state NEW -m
tcp -p tcp --sport 920 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_NFS_Server -m state --state NEW -m
udp -p udp --dport 920 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_NFS_Server -m state --state NEW -m
udp -p udp --sport 920 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_NFS_Server -m state --state NEW -m
tcp -p tcp --dport 2049 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_NFS_Server -m state --state NEW -m
tcp -p tcp --sport 2049 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_NFS_Server -m state --state NEW -m
tcp -p tcp --dport 32803 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_NFS_Server -m state --state NEW -m
udp -p udp --dport 32769 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_NFS_Server -m state --state NEW -m
tcp -p tcp --dport 892 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_NFS_Server -m state --state NEW -m
udp -p udp --dport 892 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_NFS_Server -m state --state NEW -m
tcp -p tcp --dport 875 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_NFS_Server -m state --state NEW -m
udp -p udp --dport 875 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_NFS_Server -m state --state NEW -m
tcp -p tcp --dport 662 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_NFS_Server -m state --state NEW -m
udp -p udp --dport 662 -j ACCEPT
#DNS - Configure for every DNS Server
-A RH-Firewall-1-INPUT -d IP_of_DNS_Server -m state --state NEW -m
tcp -p tcp --dport 53 -j ACCEPT
```

```
-A RH-Firewall-1-INPUT -d IP_of_DNS_Server -m state --state NEW -m
udp -p udp --dport 53 -j ACCEPT
#NTP - Configure for every NTP Server
-A RH-Firewall-1-INPUT -d IP_of_NTP_Server -m state --state NEW -m
tcp -p tcp --dport 123 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_NTP_Server -m state --state NEW -m
udp -p udp --dport 123 -j ACCEPT
#LDAP - Confiugre for every LDAP Server
-A RH-Firewall-1-INPUT -d IP_of_LDAP_Server -m state --state NEW -m
tcp -p tcp --dport 389 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_LDAP_Server -m state --state NEW -m
udp -p udp --dport 389 -j ACCEPT
#SMTP - Configure for every SMTP Server
-A RH-Firewall-1-INPUT -d IP_of_SMTP_Server -m state --state NEW -m
tcp -p tcp --dport 25 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_SMTP_Server -m state --state NEW -m
udp -p udp --dport 25 -j ACCEPT
#Syslog - Configure for every Sysog Server
-A RH-Firewall-1-INPUT -d IP_of_Syslog_Server -m state --state NEW -
m udp -p udp --dport 514 -j ACCEPT
#vCenter & ESX the simple way
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport
443 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport
902 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport
903 -j ACCEPT
#vCenter & ESX - Configure for every vCenter & ESXi_Server
#-A RH-Firewall-1-INPUT -d IP_of_vCenter&ESXi_Server -m state --
state NEW -m tcp -p tcp --dport 443 -j ACCEPT
#-A RH-Firewall-1-INPUT -d IP_of_vCenter&ESXi_Server -m state --
state NEW -m tcp -p tcp --dport 902 -j ACCEPT
#-A RH-Firewall-1-INPUT -d IP_of_vCenter&ESXi_Server -m state --
state NEW -m tcp -p tcp --dport 903 -j ACCEPT
#Default Microsoft SQL Connections
-A RH-Firewall-1-INPUT -d IP_of_SQL_Server -m state --state NEW -m
tcp -p tcp --dport 1433 -j ACCEPT
#Default Oracle Port Connections
-A RH-Firewall-1-INPUT -d IP_of_Oracle_Server -m state --state NEW -
m tcp -p tcp --dport 1521 -j ACCEPT
#AMQP Messaging for task extensions (if Server exists)
-A RH-Firewall-1-INPUT -d IP_of_AMQP_Server -m state --state NEW -m
tcp -p tcp --dport 5672 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_AMQP_Server -m state --state NEW -m
udp -p udp --dport 5672 -j ACCEPT
#ActiveMQ between vCD Cells
-A RH-Firewall-1-INPUT -d IP_of_vCD-Cell -m state --state NEW -m tcp
-p tcp --dport 61611 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_vCD-Cell -m state --state NEW -m tcp
-p tcp --dport 61616 -j ACCEPT
#ActiveMQ to Server
-A RH-Firewall-1-INPUT -d IP_of_ActiveMQ -m state --state NEW -m tcp
-p tcp --dport 61611 -j ACCEPT
-A RH-Firewall-1-INPUT -d IP_of_ActiveMQ -m state --state NEW -m tcp
-p tcp --dport 61616 -j ACCEPT
# End listing vCloud Director Ports Needed
```

6.7.5.2 Install VMware public keys

The installation file for vCloud Director is digitally signed to secure your environment. To install the product, you must verify the signature by downloading and installing the VMware public key in your environment.

```
cd /install/
wget http://packages.vmware.com/tools/keys/VMWARE-PACKAGING-GPG-DSA-KEY.pub
wget http://packages.vmware.com/tools/keys/VMWARE-PACKAGING-GPG-RSA-KEY.pub
rpm --import /install/VMWARE-PACKAGING-GPG-DSA-KEY.pub
rpm --import /install/VMWARE-PACKAGING-GPG-RSA-KEY.pub
```

6.7.6 Start and Stop vCloud director

Download the vCloud director binary and copy the file to /install. Change the permission using the following command to make the binary executable. Execute the binary and when prompted to proceed further, press **n** to stop the installation

```
cd /install
chmod u+x vmware-vcloud-director-5.1.1-868405.bin
./vmware-vcloud-director-5.1.1-868405.bin
n
```

6.7.6.1 Create SSL certificate

Enter the following command to create SSL certificate. The commands are based on this article.

```
/opt/vmware/vcloud-director/jre/bin/keytool -genkey -keystore
/opt/vmware/vcloud-director/data/transfer/certificates.ks -storetype JCEKS -
storepass passwd -keyalg RSA -validity 731 -alias http

/opt/vmware/vcloud-director/jre/bin/keytool -genkey -keystore
/opt/vmware/vcloud-director/data/transfer/certificates.ks -storetype JCEKS -
storepass passwd -keyalg RSA -validity 731 -alias consoleproxy
```

6.7.6.2 Continue with the installation

Navigate to the /opt/vmware/vcloud-director/bin directory and continue with the installation.This is based on the SQL server installation documented earlier.

Database name - vcddb
Database instance - Dell EMCvcddb
Username - vcdmgr
Password - <passwd>

```
[root@vcd1 bin]# ./configure
Welcome to the vCloud Director configuration utility.

You will be prompted to enter a number of parameters that are necessary to
configure and start the vCloud Director service.
```

```
Please indicate which IP address available on this machine should be used for
the HTTP service and which IP address should be used for the remote console
proxy.

The HTTP service IP address is used for accessing the user interface and the
REST API. The remote console proxy IP address is used for all remote console
(VMRC)
connections and traffic.

Please enter your choice for the HTTP service IP address:
    1. 172.16.114.26
    2. 172.16.114.27
    3. 127.0.0.1
    4. [fe80:0:0:0:250:56ff:fe8e:631]
    5. [fe80:0:0:0:250:56ff:fe8e:f2f2]
    6. [0:0:0:0:0:0:0:1]
Choice [default=1]:
Using default value "172.16.114.26" for HTTP service.


Please enter your choice for the remote console proxy IP address:
    1. 172.16.114.27
    2. 127.0.0.1
    3. [fe80:0:0:0:250:56ff:fe8e:631]
    4. [fe80:0:0:0:250:56ff:fe8e:f2f2]
    5. [0:0:0:0:0:0:0:1]
Choice [default=1]:
Using default value "172.16.114.27" for remote console proxy.


Please enter the path to the Java keystore containing your SSL certificates
and
private keys: /opt/vmware/vcloud-director/data/transfer/certificates.ks
Please enter the password for the keystore:

If you would like to enable remote audit logging to a syslog host please
enter
the hostname or IP address of the syslog server. Audit logs are stored by
vCloud Director for 90 days. Exporting logs via syslog will enable you to
preserve them for as long as necessary.

Syslog host name or IP address [press Enter to skip]:
No syslog host was specified, disabling remote audit logging.

generating new UUID: 52fd4b99-570b-4ca5-9bd7-9c05acb0d156
The following database types are supported:
    1. Oracle
    2. Microsoft SQL Server
    3. vPostgres
Enter the database type [default=1]: 2
Enter the host (or IP address) for the database: 172.16.114.25
Enter the database port [default=1433]:
Using default value "1433" for port.

Enter the database name [default=vcloud]: vcddb
```

```
Enter the database instance [Press enter to use the server's default
instance]: Dell EMCvcddb
Enter the database username: vcdmgr
Enter the database password:
Connecting to the database:
jdbc:jtds:sqlserver://172.16.114.25:1433/vcddb;socketTimeout=90;instance=Dell
EMCvcddb;prepareSQL=2
...................................../Database configuration complete.

vCloud Director configuration is now complete.

Once the vCloud Director server has been started you will be able to
access the first-time setup wizard at this URL:
    https://172.16.114.26

Would you like to start the vCloud Director service now? If you choose not
to start it now, you can manually start it at any time using this command:
service vmware-vcd start

Start it now? [y/n] y

Starting vmware-vcd-watchdog:                              [  OK  ]
Starting vmware-vcd-cell                                   [  OK  ]

The vCD service will be started automatically on boot.  To disable this,
use the following command: chkconfig --del vmware-vcd

[root@vcd1 ~]# service vmware-vcd status
vmware-vcd-watchdog is running
vmware-vcd-cell is running
[root@vcd1 ~]#
```