Dell EMC + VMware Cloud Infrastructure Platform for NFV

VMware vCloud NFV 1.5 – Dell EMC ScaleIO and NFVI Installation Guide

Service Provider Solutions Group
April 2017

A Dell EMC Installation Guide

Revisions

Date	Description
April 2017	Initial release

THIS DOCUMENT IS PROVIDED “AS-IS”, AND WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED. IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE SPECIFICALLY DISCLAIMED. PRODUCT WARRANTIES APPLICABLE TO THE DELL PRODUCTS DESCRIBED IN THIS DOCUMENT MAY BE FOUND AT: http://www.dell.com/learn/us/en/vn/terms-of-sale-commercial-and-public-sector-warranties

Performance of network reference architectures discussed in this document may vary with differing deployment conditions, network loads, and the like. Third party products may be included in reference architectures for the convenience of the reader. Inclusion of such third party products does not necessarily constitute Dell’s recommendation of those products. Please consult your Dell representative for additional information.

Table of contents

1 Overview

This document provides guidance in deploying a cloud solution to run VNF workloads hosted on Dell EMC hardware virtualized with the help of VMware vCloud platform for NFV and using Dell EMC ScaleIO as a shared storage solution. In addition, the 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, sales engineers, field consultants, advanced services specialists and customers who are responsible for Telco cloud / NFV services, in building an infrastructure to maximize the benefits of using the Dell EMC ScaleIO with Dell EMC VMware NFV solution bundle.

3 Dell EMC Hardware Requirements

A complete up-to-date list of vCloud NFV-ScaleIO ready Dell EMC platforms for vCloud is available at: http://www.vmware.com/resources/compatibility

Dell EMC PowerEdge R730		9 (minimum)
Components	CPU	Intel Xeon® E5-2680v3 2.5Ghz 2 sockets, 12 cores
	RAM	192 GB (128 GB min)
	HDD	2x600G SAS (800 GB min)
	SSD	1x200G (1/3rd of HDD min)
	SD cards	2x16
	NIC	8x10G 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 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
ScaleIO	2.0.0.3	Any compatible version
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	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	SQL server license

Table 4 License requirements

5 Reference Architecture

5.1 Logical topology

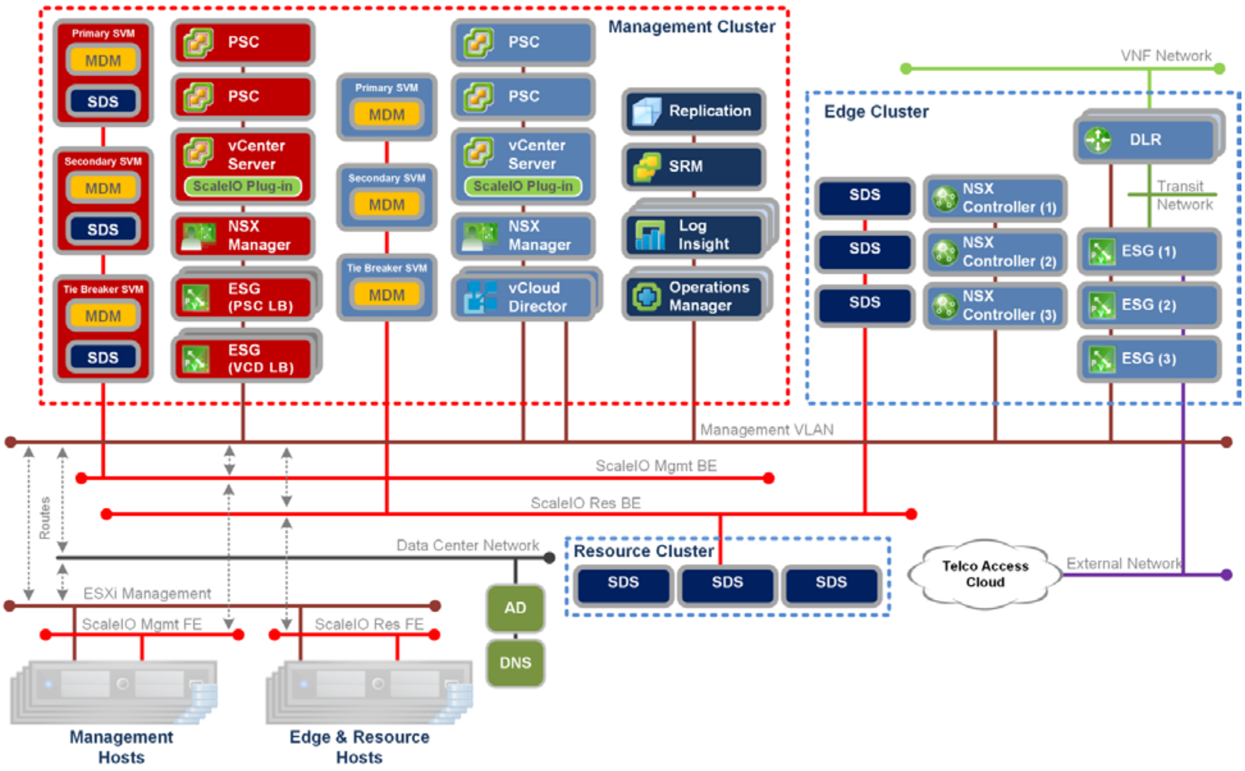


Figure 1 Logical topology

5.2 Physical Topology

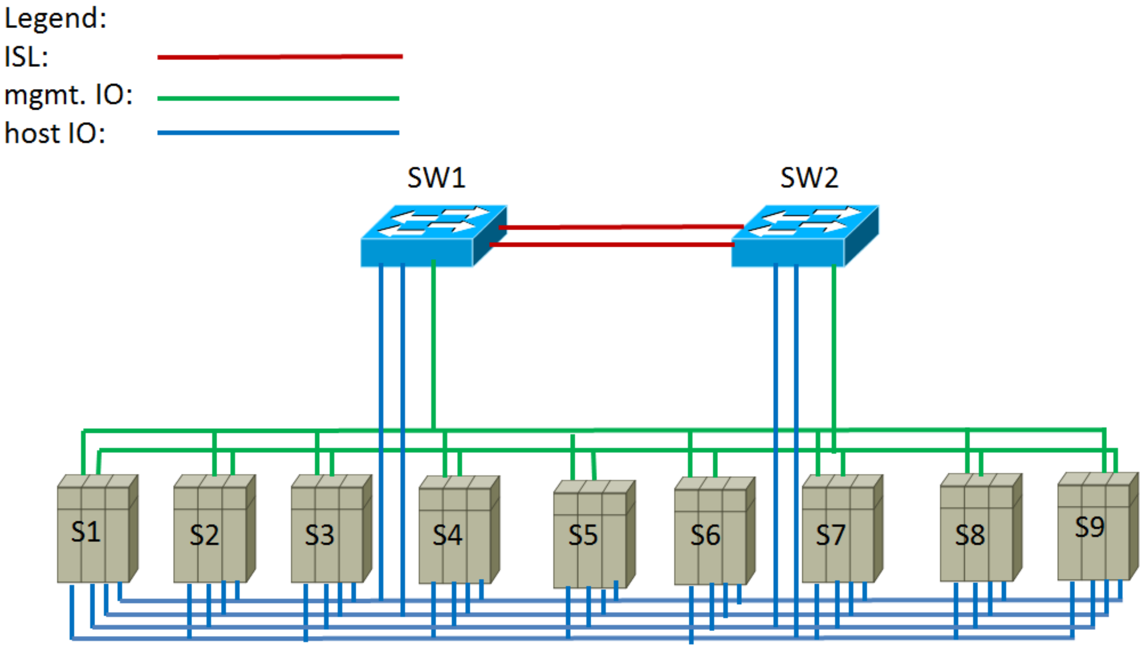


Figure 2 Physical topology

The Reference test bed sits in a rack comprised of one Dell Management Switch and pair of Dell Leaf/ToR Switches (virtualized to behave as a single Switch) alongside Dell R730 Servers. Each Server has four dual-port 10 GbE NICs configured to support bonded 40 GbE HostIO and 20 GbE Management and Fault-Tolerant ScaleIO networks. The Appendix section of this document captures additional details about the test bed. Table 5 shows the Bonding Map.

	NIC Port	Switch	SW Pport	Bond	
server1	p1p1	sw1	Te0/64	po64	
iDrac: 172.16.104.10	p1p2	sw2	Te0/64	po64	
	p2p1	sw1	Te0/65		SIO-1
	p2p2	sw2	Te0/65		SIO-2
	p4p1	sw1	Te0/80	po80	
	p4p2	sw2	Te0/80	po80	
	p5p1	sw1	Te0/81	po80	
	p5p2	sw2	Te0/81	po80	
server2	p1p1	sw1	Te0/66	po66	
iDrac: 172.16.104.11	p1p2	sw2	Te0/66	po66	
	p2p1	sw1	Te0/67		SIO-1
	p2p2	sw2	Te0/67		SIO-2
	p4p1	sw1	Te0/82	po82	
	p4p2	sw2	Te0/82	po82	
	p5p1	sw1	Te0/83	po82	
	p5p2	sw2	Te0/83	po82	
server3	p1p1	sw1	Te0/68	po68	
iDrac: 172.16.104.12	p1p2	sw2	Te0/68	po68	
	p2p1	sw1	Te0/69		SIO-1
	p2p2	sw2	Te0/69		SIO-2
	p4p1	sw1	Te0/84	po84	
	p4p2	sw2	Te0/84	po84	
	p5p1	sw1	Te0/85	po84	
	p5p2	sw2	Te0/85	po84	
server4	p1p1	sw1	Te0/70	po70	
iDrac: 172.16.104.13	p1p2	sw2	Te0/70	po70	
	p2p1	sw1	Te0/71		SIO-1
	p2p2	sw2	Te0/71		SIO-2
	p4p1	sw1	Te0/86	po86	
	p4p2	sw2	Te0/86	po86	
	p5p1	sw1	Te0/87	po86	
	p5p2	sw2	Te0/87	po86	
server5	p1p1	sw1	Te0/72	po72	
iDrac: 172.16.104.14	p1p2	sw2	Te0/72	po72	
	p2p1	sw1	Te0/73		SIO-1
	p2p2	sw2	Te0/73		SIO-2
	p4p1	sw1	Te0/88	po88	
	p4p2	sw2	Te0/88	po88	
	p5p1	sw1	Te0/89	po88	
	p5p2	sw2	Te0/89	po88	
server6	p1p1	sw1	Te0/74	po74	
iDrac: 172.16.104.15	p1p2	sw2	Te0/74	po74	
	p2p1	sw1	Te0/75		SIO-1
	p2p2	sw2	Te0/75		SIO-2
	p4p1	sw1	Te0/90	po90	
	p4p2	sw2	Te0/90	po90	
	p5p1	sw1	Te0/91	po90	
	p5p2	sw2	Te0/91	po90	
server7	p1p1	sw1	Te0/76	po76	
iDrac: 172.16.104.16	p1p2	sw2	Te0/76	po76	
	p2p1	sw1	Te0/77		SIO-1
	p2p2	sw2	Te0/77		SIO-2
	p4p1	sw1	Te0/92	po92	
	p4p2	sw2	Te0/92	po92	
	p5p1	sw1	Te0/93	po92	
	p5p2	sw2	Te0/93	po92	
server8	p1p1	sw1	Te0/78	po78	
iDrac: 172.16.104.17	p1p2	sw2	Te0/78	po78	
	p2p1	sw1	Te0/79		SIO-1
	p2p2	sw2	Te0/79		SIO-2
	p4p1	sw1	Te0/94	po94	
	p4p2	sw2	Te0/94	po94	
	p5p1	sw1	Te0/95	po94	
	p5p2	sw2	Te0/95	po94	
server9	p1p1	sw1	Te0/96	po96	
iDrac: 172.16.104.18	p1p2	sw2	Te0/96	po96	
	p2p1	sw1	Te0/97		SIO-1
	p2p2	sw2	Te0/97		SIO-2
	p4p1	sw1	Te0/98	po98	
	p4p2	sw2	Te0/98	po98	
	p5p1	sw1	Te0/99	po98	
	p5p2	sw2	Te0/99	po98	

Table 5 Bonding details

6 Steps to bring up the VMware virtualization platform

6.1 Install ESXi on Servers

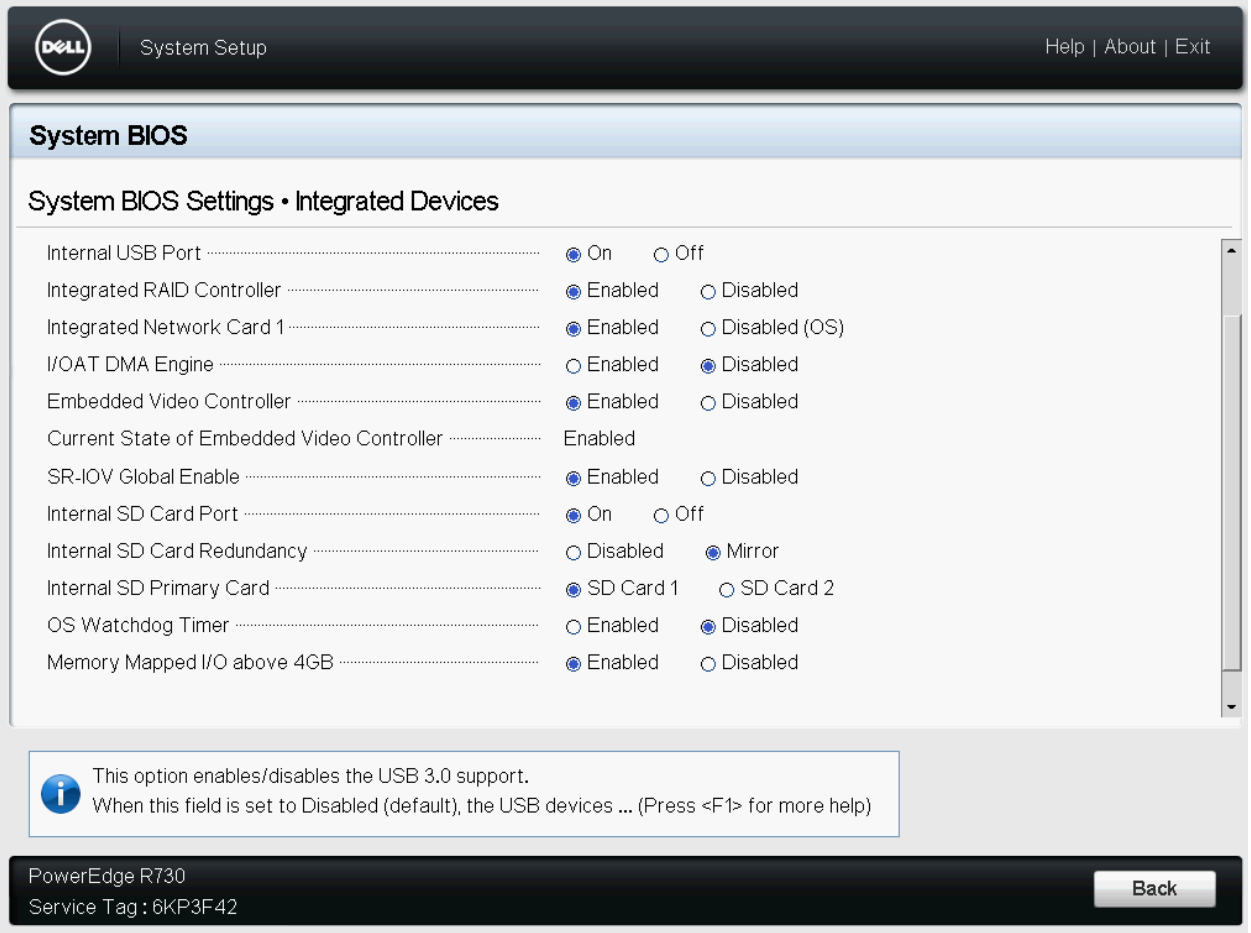
ESXi Hypervisors need to be installed on a physical server hard disk. The hard disk on which ESXi hypervisors are installed cannot be used by storage clustering applications like VSAN. To avoid losing hundreds of GBs of standard disk storage for clustering, installing the hypervisors on the internal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

6.1.1 Verify the SD card module is present

Not all servers come with internal SD card modules. Therefore, before proceeding with the installation, make sure an internal SD card module is in the system. To verify this, launch iDRAC and enter system setup. Navigate to **System BIOS → Integrated Devices**.

Default iDRAC Username*: root*   Password: *calvin*

Under Integrated Devices, verify the SD card related fields are present. If these fields are missing, the host does not have a SD card controller or a SD card is not inserted.



System BIOS

System BIOS Settings • Integrated Devices

Internal USB Port	● On	○ Off
Integrated RAID Controller	● Enabled	○ Disabled
Integrated Network Card 1	● Enabled	○ Disabled (OS)
I/OAT DMA Engine	○ Enabled	● Disabled
Embedded Video Controller	● Enabled	○ Disabled
Current State of Embedded Video Controller	Enabled	
SR-IOV Global Enable	● Enabled	○ Disabled
Internal SD Card Port	● On	○ Off
Internal SD Card Redundancy	○ Disabled	● Mirror
Internal SD Primary Card	● SD Card 1	○ SD Card 2
OS Watchdog Timer	○ Enabled	● Disabled
Memory Mapped I/O above 4GB	● Enabled	○ Disabled

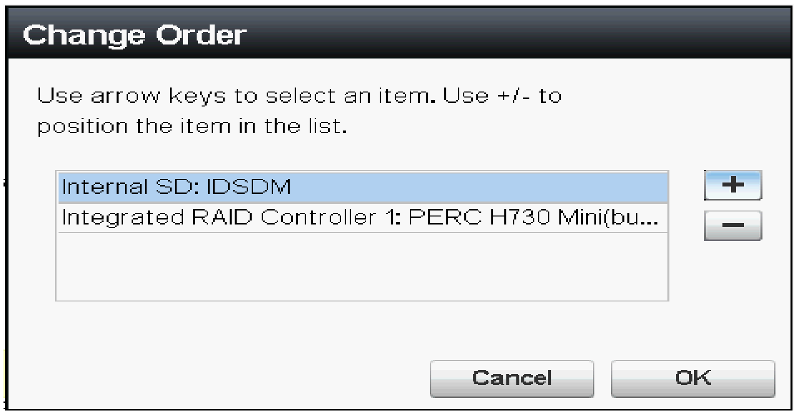
This option enables/disables the USB 3.0 support.
When this field is set to Disabled (default), the USB devices ... (Press <F1> for more help)

PowerEdge R730
Service Tag : 6KP3F42

Figure 3 System BIOS – Integrated Devices

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

By default, most systems are set to boot from the HDD or SSD drives and may not boot when ESXi is installed on a partition on the SD card in the system. Therefore, it is necessary to set the proper boot parameters under the **System BIOS → Boot setting → BIOS Boot Settings → Hard-Disk Drive Sequence**.



Change Order

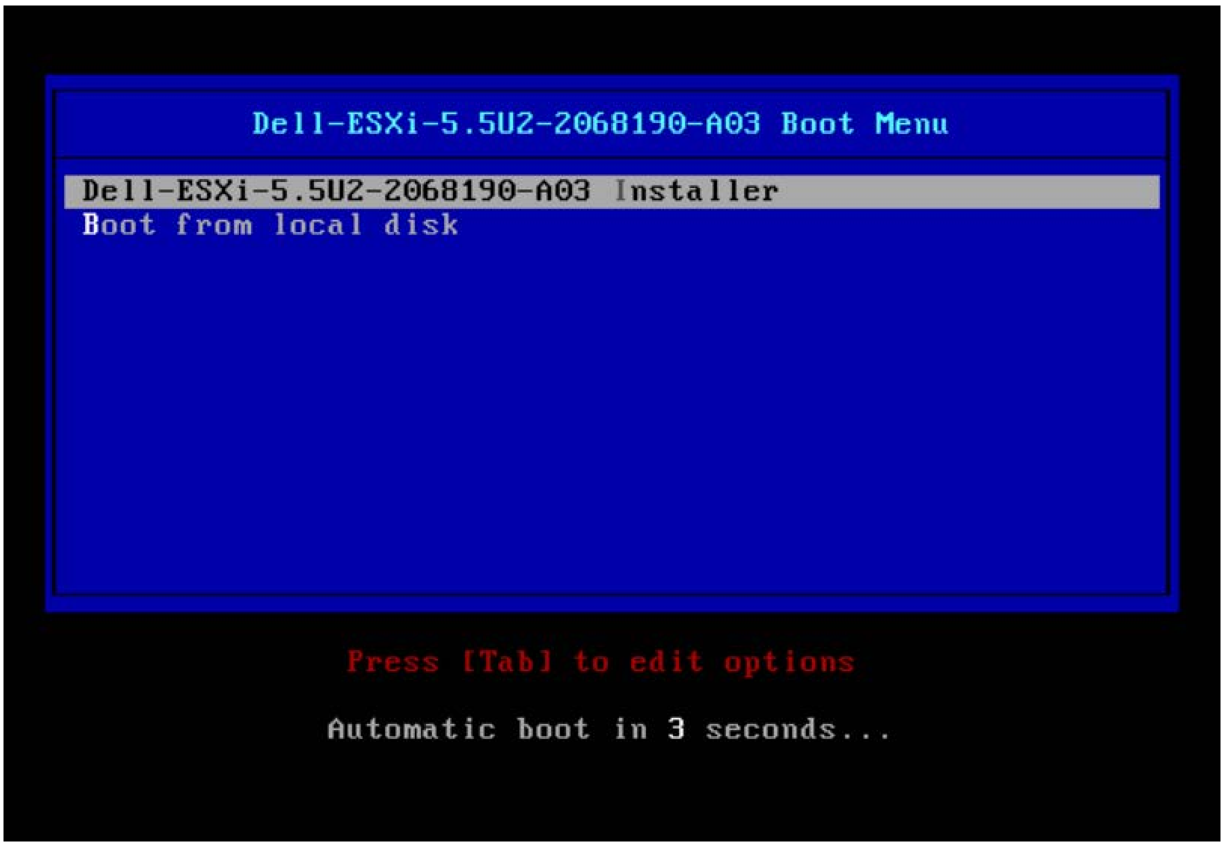
Use arrow keys to select an item. Use +/- to position the item in the list.

Internal SD: IDSDM
Integrated RAID Controller 1: PERC H730 Mini(bu...

Table 6 Change Boot order

6.1.3 Use VMware ESXi installer to install the hypervisor

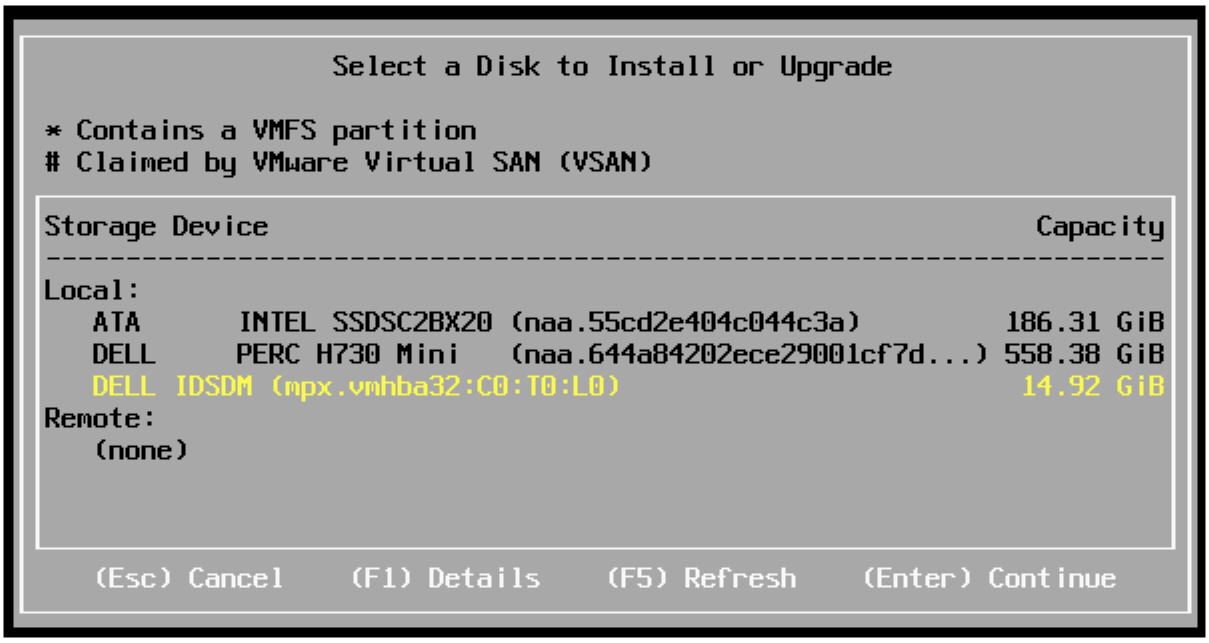
Either using the CD drive in the server or an ISO image, start the ESXi installation process. To use an ISO image, use the iDRAC option to connect virtual media and click **Map CD/DVD from the local drive**. Point to the local ISO image file and set the Next boot option to boot via virtual CD/DVD/ISO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



```
Dell-ESXi-5.5U2-2068190-A03 Boot Menu

Dell-ESXi-5.5U2-2068190-A03 Installer
Boot from local disk

Press [Tab] to edit options

Automatic boot in 3 seconds...
```

Figure 4 Installer option

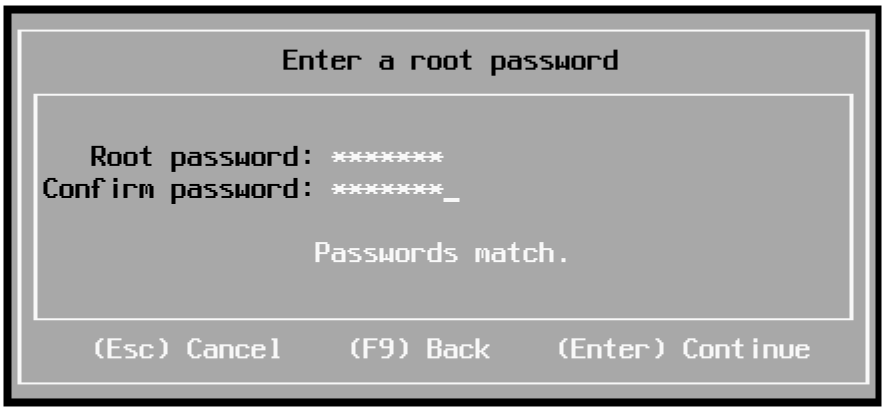
Note: Make sure you are installing the ESXi hypervisor on the SD card in the server.



```
                     Select a Disk to Install or Upgrade

* Contains a VMFS partition
# Claimed by VMware Virtual SAN (VSAN)

Storage Device                                                      Capacity
----------------------------------------------------------------------------
Local:
   ATA       INTEL SSDSC2BX20 (naa.55cd2e404c044c3a)         186.31 GiB
   DELL      PERC H730 Mini   (naa.644a84202ece29001cf7d...) 558.38 GiB
   DELL IDSDM (mpx.vmhba32:C0:T0:L0)                          14.92 GiB
Remote:
   (none)

   (Esc) Cancel     (F1) Details     (F5) Refresh     (Enter) Continue
```

Figure 5 Select a Disk to Install

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



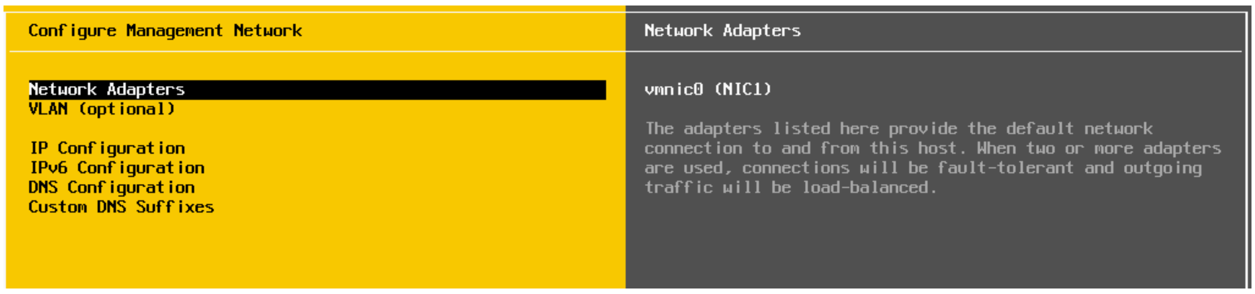
```
                 Enter a root password

    Root password: ********
 Confirm password: ********_

                 Passwords match.

    (Esc) Cancel     (F9) Back     (Enter) Continue
```

Figure 6 Configure password

Repeat this process for all the servers in the setup.

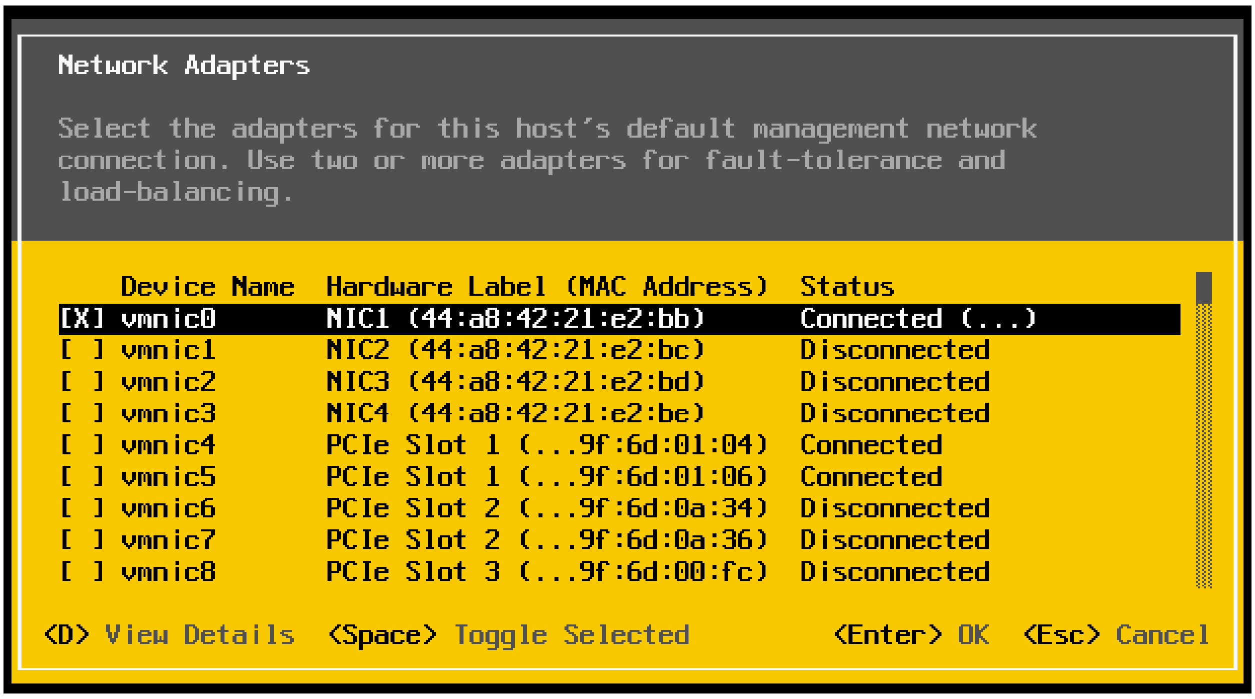
6.1.4 Configure the management interface

Post installation, it is necessary to configure the management IP address for the hypervisors so they can be managed by the 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 and choose the NIC interface, which will be acting as the management interface, from the list of available NICs. If no DHCP server is providing the IP address, choose static configuration and assign a management IP address to the server. Repeat the same process for all the servers.



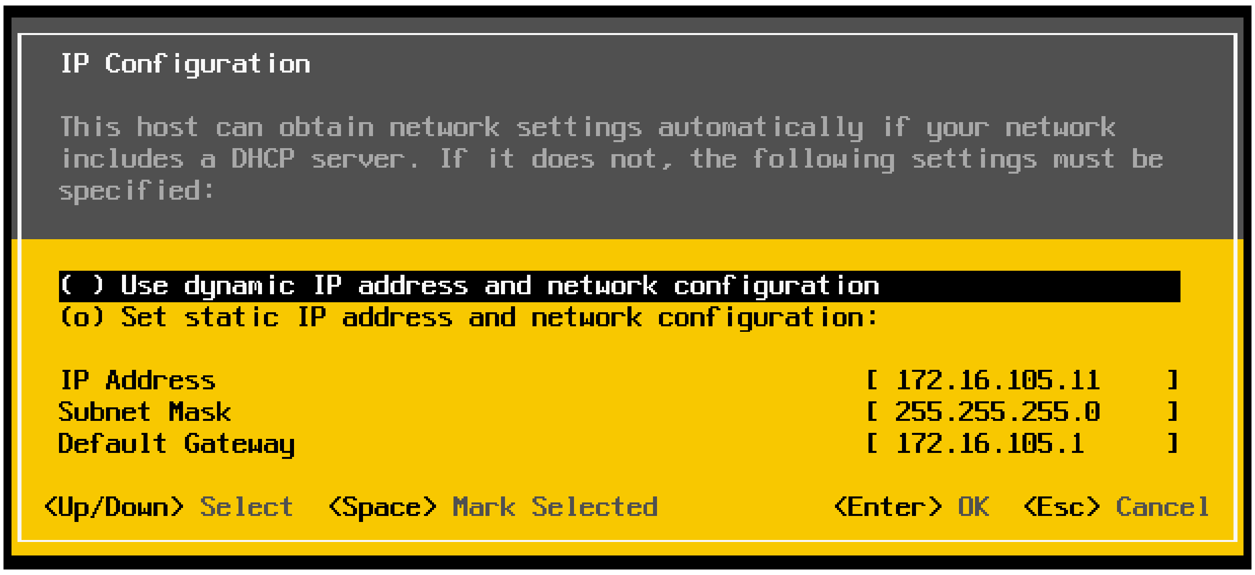
```
Configure Management Network                 Network Adapters

Network Adapters                             vmnic0 (NIC1)
VLAN (optional)
                                             The adapters listed here provide the default network
IP Configuration                             connection to and from this host. When two or more adapters
IPv6 Configuration                           are used, connections will be fault-tolerant and outgoing
DNS Configuration                            traffic will be load-balanced.
Custom DNS Suffixes
```

Figure 7 Configure Management Network



```
Network Adapters

Select the adapters for this host's default management network
connection. Use two or more adapters for fault-tolerance and
load-balancing.

    Device Name  Hardware Label (MAC Address)  Status
[X] vmnic0       NIC1 (44:a8:42:21:e2:bb)      Connected (...)
[ ] vmnic1       NIC2 (44:a8:42:21:e2:bc)      Disconnected
[ ] vmnic2       NIC3 (44:a8:42:21:e2:bd)      Disconnected
[ ] vmnic3       NIC4 (44:a8:42:21:e2:be)      Disconnected
[ ] vmnic4       PCIe Slot 1 (...9f:6d:01:04)  Connected
[ ] vmnic5       PCIe Slot 1 (...9f:6d:01:06)  Connected
[ ] vmnic6       PCIe Slot 2 (...9f:6d:0a:34)  Disconnected
[ ] vmnic7       PCIe Slot 2 (...9f:6d:0a:36)  Disconnected
[ ] vmnic8       PCIe Slot 3 (...9f:6d:00:fc)  Disconnected

<D> View Details  <Space> Toggle Selected       <Enter> OK  <Esc> Cancel
```

Figure 8 Select Network Adapters



```
IP Configuration

This host can obtain network settings automatically if your network
includes a DHCP server. If it does not, the following settings must be
specified:

( ) Use dynamic IP address and network configuration
(o) Set static IP address and network configuration:

IP Address                                         [ 172.16.105.11    ]
Subnet Mask                                        [ 255.255.255.0    ]
Default Gateway                                    [ 172.16.105.1     ]

<Up/Down> Select  <Space> Mark Selected         <Enter> OK  <Esc> Cancel
```

Figure 9 IP Configuration

6.2 Install ADS and DNS server

Create a Windows VM

To add a new role to Windows Server 2012, use Server Manager. Start Server Manager, click the **Manage** menu and select **Add Roles and Features**.

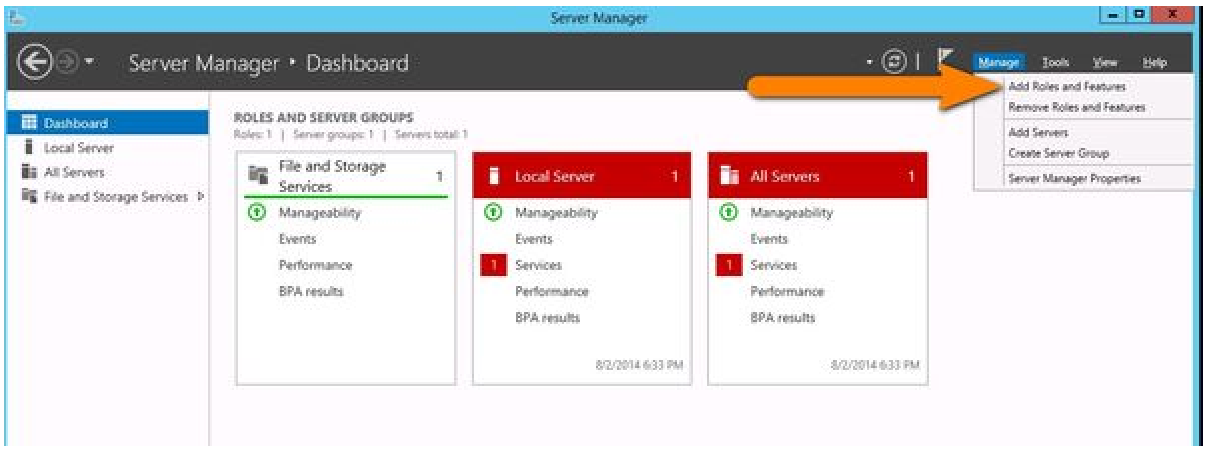
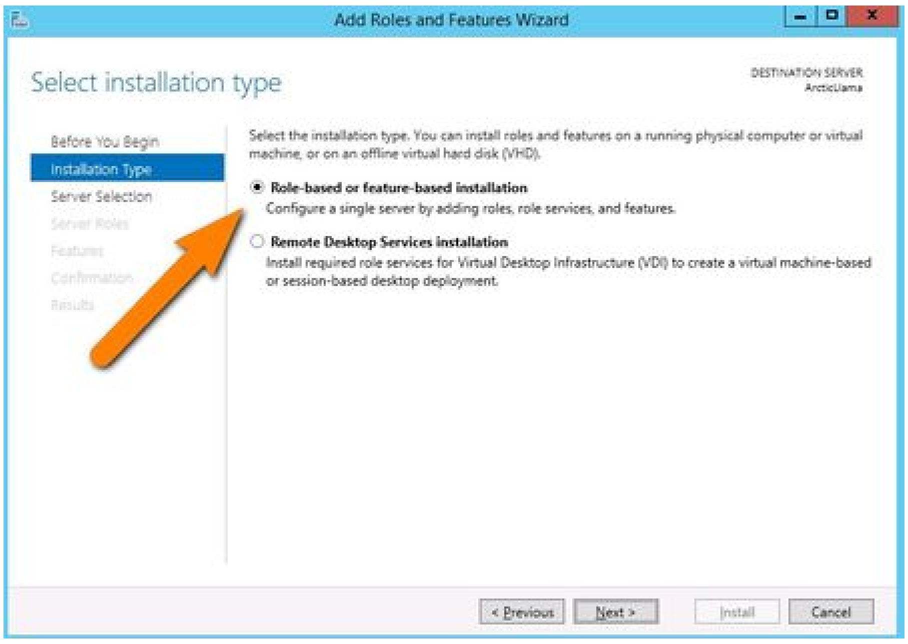


Figure 10 Add Roles and Features

Click **Next** on the **Add Roles and Features Wizard Before you begi**n pop up window. (If you previously checked **Skip this page by default**, this page will not appear.)

Select the installation type. For DNS servers, select the **Role-based** or **feature-based installation.**



Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

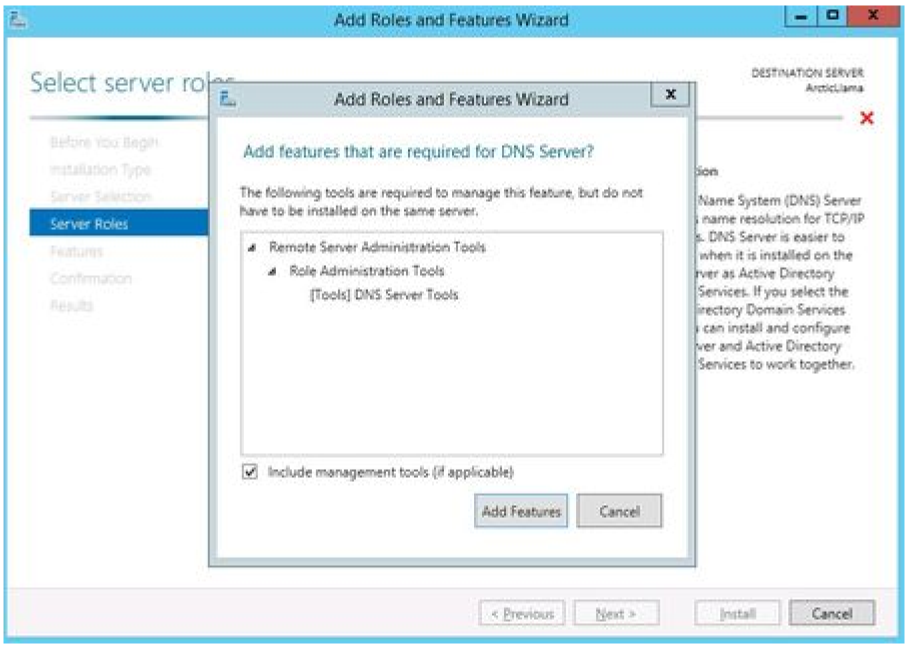
Figure 11 Select installation type

Configure DNS Server:

Next, choose which server to install the DNS server role from the server pool. Select the server, and click **Next**.

At this point, a pop-up window will open indicating that additional tools are required to manage the DNS Server. These tools do not necessarily have to be installed on the same server as the DNS role. If your organization only does remote administration, you do not have to install the DNS Server Tools.

However, in a crunch a user sitting at the server console or remotely using the console may need to manage the DNS Server directly. In this case, it is helpful to have the tools installed locally. Unless company policy forbids it, it is typically prudent to install the management tools on the server where the DNS will be housed.



Add features that are required for DNS Server?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
  - Role Administration Tools
    - [Tools] DNS Server Tools

☑ Include management tools (if applicable)

ion

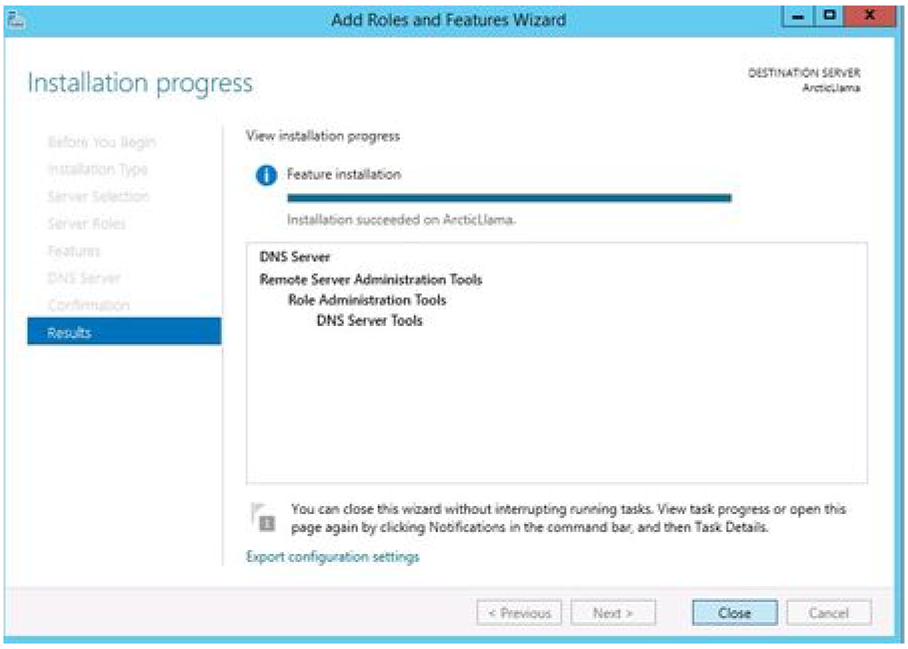
Name System (DNS) Server
name resolution for TCP/IP
s. DNS Server is easier to
when it is installed on the
rver as Active Directory
Services. If you select the
irectory Domain Services
can install and configure
ver and Active Directory
Services to work together.

Figure 12 Add Roles and Features Wizard

Now the Features window should open. Click **Next** as no changes are needed here.

Next is an informational window about DNS Server and what it does, click **Next** to move on.

This is the final confirmation screen before installation completes. There is a check box to restart the destination server automatically. Installing the DNS Server does not require a restart, so unless downtime has been scheduled, keep this box unchecked.



View installation progress

Feature installation

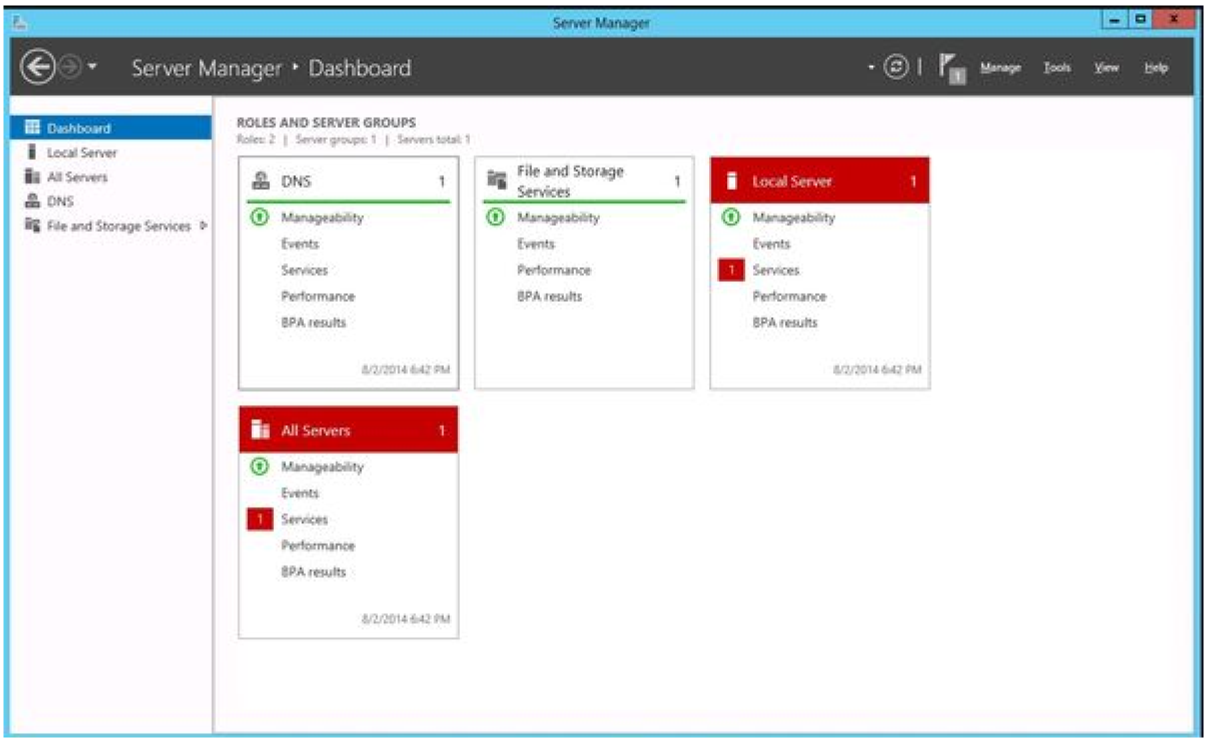
Installation succeeded on ArcticLlama.

DNS Server
Remote Server Administration Tools
    Role Administration Tools
        DNS Server Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Figure 13 Installation progress

The DNS Server role should now be installed on the server. There should be a new DNS Role tile in Server Manager.



ROLES AND SERVER GROUPS
Roles: 2 | Server groups: 1 | Servers total: 1

DNS 1
Manageability
Events
Services
Performance
BPA results
8/2/2014 6:42 PM

File and Storage Services 1
Manageability
Events
Performance
BPA results

Local Server 1
Manageability
Events
1 Services
Performance
BPA results
8/2/2014 6:42 PM

All Servers 1
Manageability
Events
1 Services
Performance
BPA results
8/2/2014 6:42 PM

Figure 14 Server Manager – DNS tile

6.3 Install NTP server

Create a Windows VM and Install NTP Services as follows:

Run the following commands using PowerShell as admin:

```
w32tm /config /manualpeerlist:pool.ntp.org /syncfromflags:MANUAL
w32tm /config /reliable:yes
Stop-Service w32time
Start-Service w32time
w32tm /query /status
```

6.4 Install vCenter Server

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

6.4.1 Mount VCSA ISO

Make sure you have access to the management IP addresses of the hypervisors from the system you are working on. 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.htm**l. If prompted for a missing plugin, install the plugin and restart the process. In the browser, click **Install**.

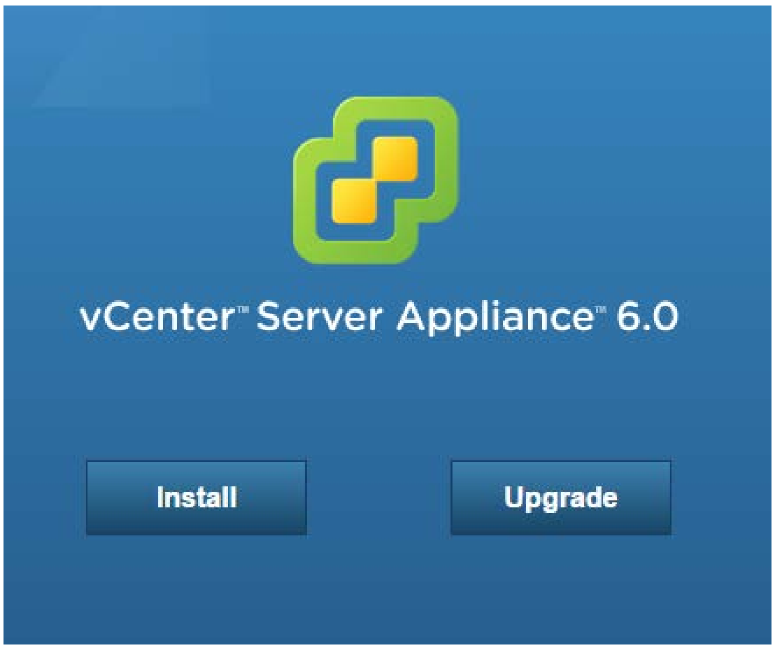
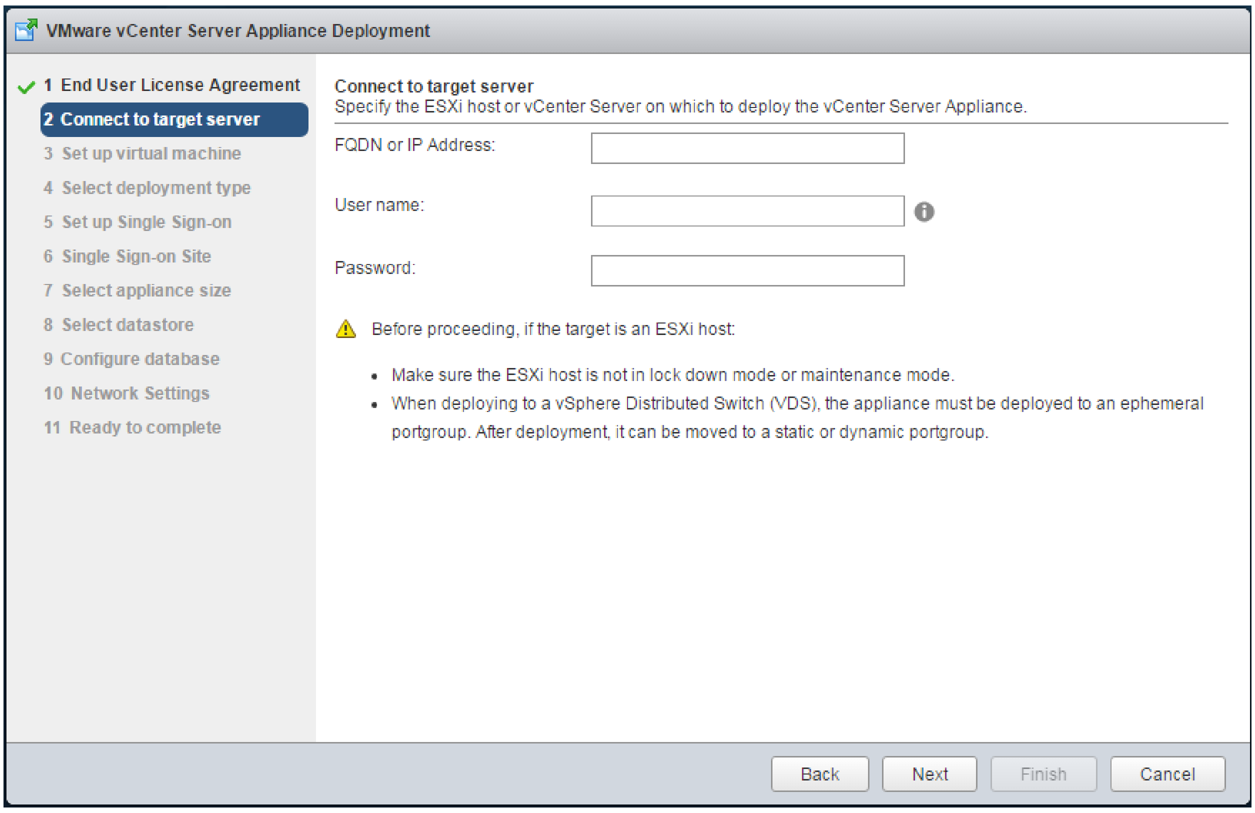


Figure 15 Install vCenter Server Appliance

6.4.2 Install External PSC

Enter the IP address of any one of the hosts that will be part of the VIM cluster. (Username/password is same as the ESXi root username/password) and click **Next**.



Connect to target server
Specify the ESXi host or vCenter Server on which to deploy the vCenter Server Appliance.

FQDN or IP Address:

User name:

Password:

Before proceeding, if the target is an ESXi host:

- Make sure the ESXi host is not in lock down mode or maintenance mode.
- When deploying to a vSphere Distributed Switch (VDS), the appliance must be deployed to an ephemeral portgroup. After deployment, it can be moved to a static or dynamic portgroup.

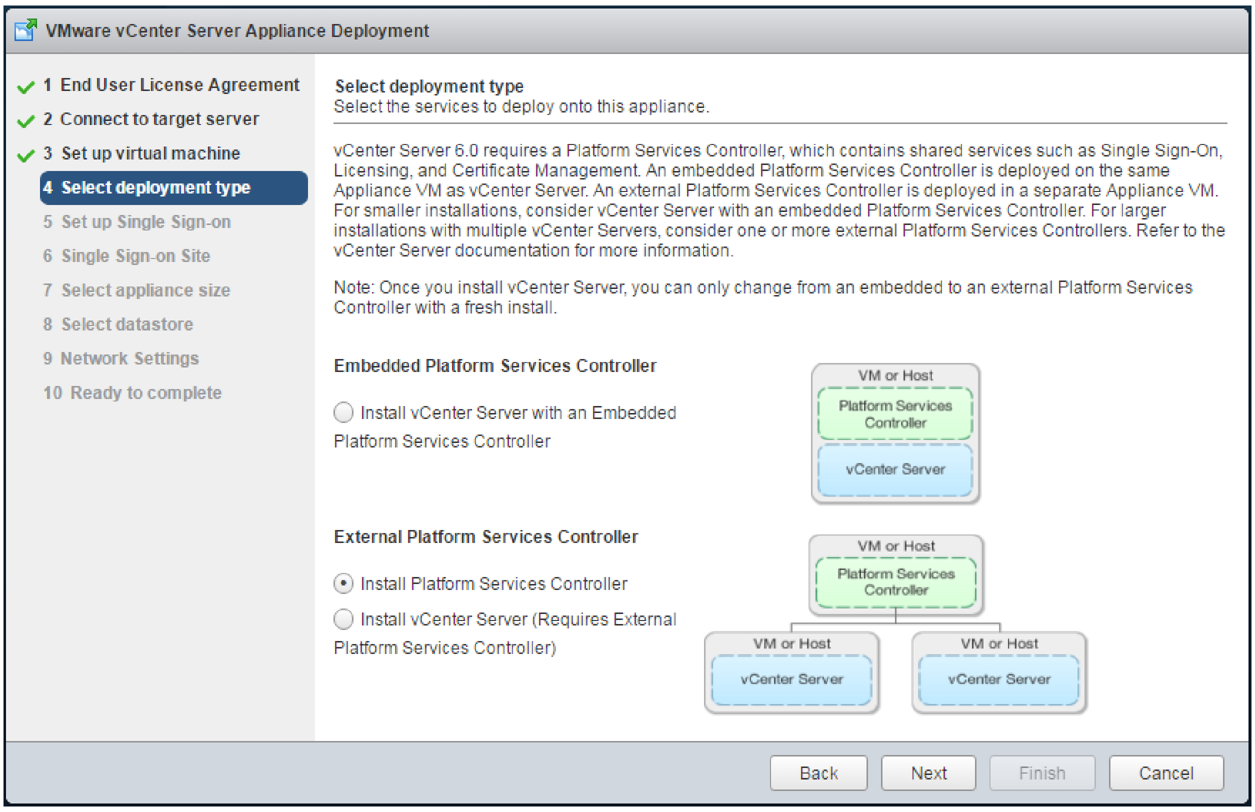
Figure 16 vCenter Server Appliance

First deployment - deploy EPSC/vCenter for Management Cluster.

Second installation - deploy EPSC/vCenter for Compute & Edge cluster.

Name the appliance and configure root password of your choice for each deployment.

Choose EPSC as show below.



VMware vCenter Server Appliance Deployment

- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- 4 Select deployment type
- 5 Set up Single Sign-on
- 6 Single Sign-on Site
- 7 Select appliance size
- 8 Select datastore
- 9 Network Settings
- 10 Ready to complete

Select deployment type
Select the services to deploy onto this appliance.

vCenter Server 6.0 requires a Platform Services Controller, which contains shared services such as Single Sign-On, Licensing, and Certificate Management. An embedded Platform Services Controller is deployed on the same Appliance VM as vCenter Server. An external Platform Services Controller is deployed in a separate Appliance VM. For smaller installations, consider vCenter Server with an embedded Platform Services Controller. For larger installations with multiple vCenter Servers, consider one or more external Platform Services Controllers. Refer to the vCenter Server documentation for more information.

Note: Once you install vCenter Server, you can only change from an embedded to an external Platform Services Controller with a fresh install.

Embedded Platform Services Controller

○ Install vCenter Server with an Embedded Platform Services Controller

External Platform Services Controller

● Install Platform Services Controller

○ Install vCenter Server (Requires External Platform Services Controller)

Figure 17 Select deployment type

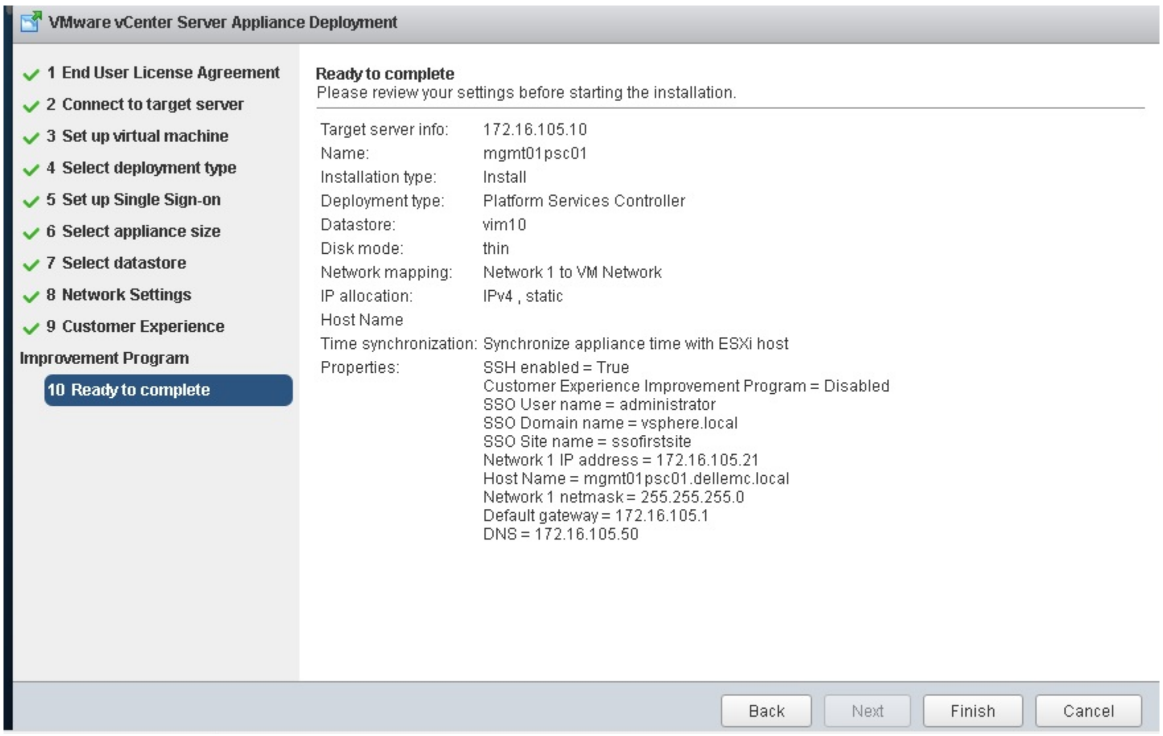
Configure SSO with the authentication password of your choice, domain name and site name.

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

Configure the network settings for the vCenter server either using a static IP or using a DHCP server, system name (if a DNS server is already configured) and use the ESXi host to synchronize time if no NTP server is configured.

Note: Do not assign a system name without first configuring a DNS in the network.

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



Ready to complete
Please review your settings before starting the installation.

Target server info:	172.16.105.10
Name:	mgmt01psc01
Installation type:	Install
Deployment type:	Platform Services Controller
Datastore:	vim10
Disk mode:	thin
Network mapping:	Network 1 to VM Network
IP allocation:	IPv4 , static
Host Name	
Time synchronization:	Synchronize appliance time with ESXi host
Properties:	SSH enabled = True Customer Experience Improvement Program = Disabled SSO User name = administrator SSO Domain name = vsphere.local SSO Site name = ssofirstsite Network 1 IP address = 172.16.105.21 Host Name = mgmt01psc01.dellemc.local Network 1 netmask = 255.255.255.0 Default gateway = 172.16.105.1 DNS = 172.16.105.50

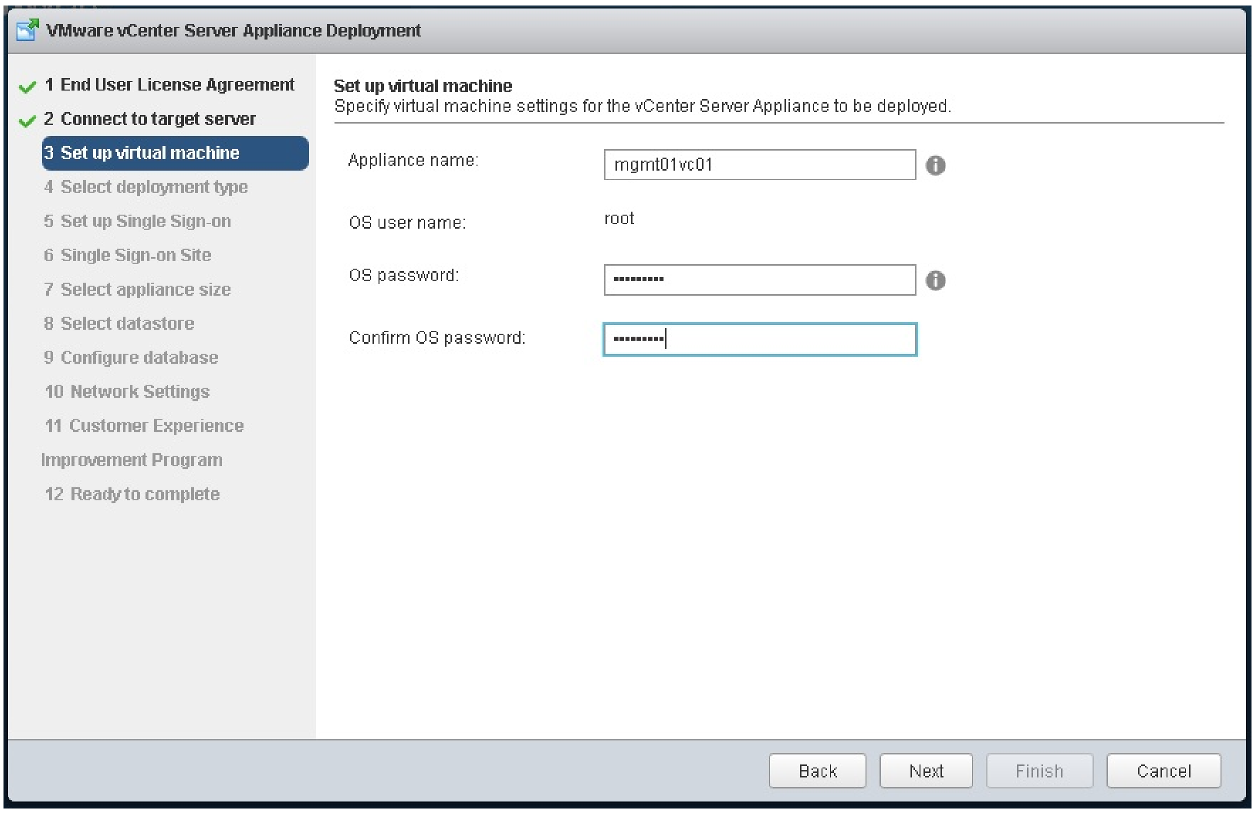
Figure 18 Ready to complete installation

6.4.3 Deploy the vCenter appliance

After the EPSC installation is complete, restart the installation to deploy vCenter server appliance.

Give a different host IP address in the management cluster to deploy vCenter. This is a best practice to ensure anti affinity, and is not a strict requirement.

Configure the vCenter appliance name.

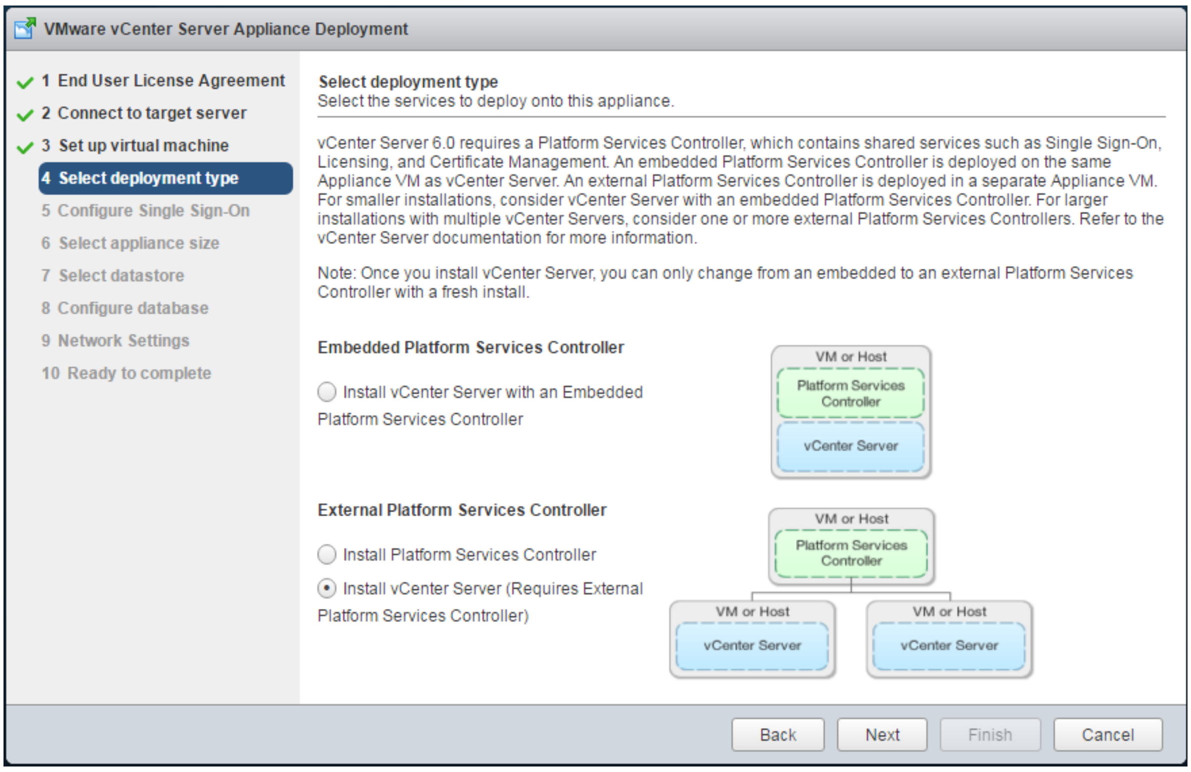


Set up virtual machine
Specify virtual machine settings for the vCenter Server Appliance to be deployed.

Appliance name:	mgmt01vc01
OS user name:	root
OS password:	••••••••••
Confirm OS password:	••••••••••

Figure 19 Set up virtual machine

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



VMware vCenter Server Appliance Deployment

- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- 4 Select deployment type
- 5 Configure Single Sign-On
- 6 Select appliance size
- 7 Select datastore
- 8 Configure database
- 9 Network Settings
- 10 Ready to complete

Select deployment type
Select the services to deploy onto this appliance.

vCenter Server 6.0 requires a Platform Services Controller, which contains shared services such as Single Sign-On, Licensing, and Certificate Management. An embedded Platform Services Controller is deployed on the same Appliance VM as vCenter Server. An external Platform Services Controller is deployed in a separate Appliance VM. For smaller installations, consider vCenter Server with an embedded Platform Services Controller. For larger installations with multiple vCenter Servers, consider one or more external Platform Services Controllers. Refer to the vCenter Server documentation for more information.

Note: Once you install vCenter Server, you can only change from an embedded to an external Platform Services Controller with a fresh install.

Embedded Platform Services Controller

○ Install vCenter Server with an Embedded Platform Services Controller

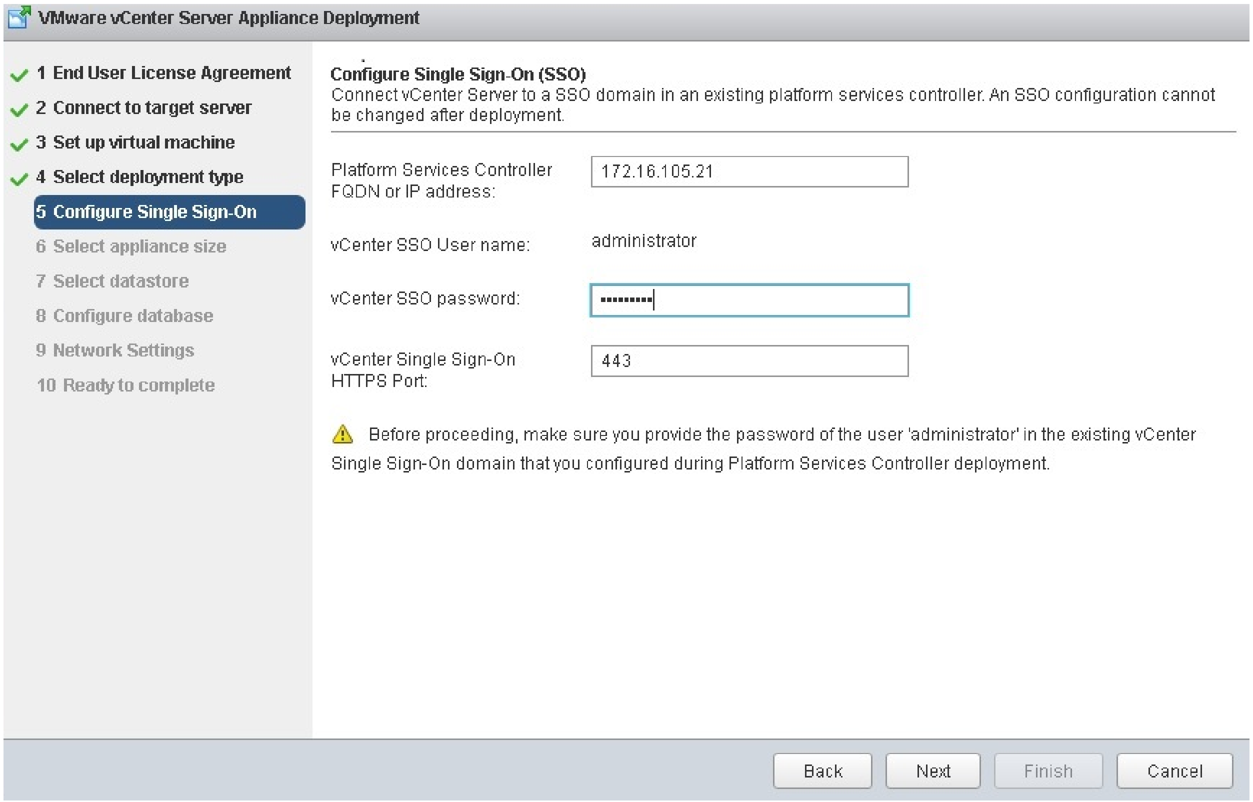
External Platform Services Controller

○ Install Platform Services Controller

● Install vCenter Server (Requires External Platform Services Controller)

Figure 20 Select deployment type

Configure the EPSC SSO password to authenticate vCenter.



VMware vCenter Server Appliance Deployment

- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- ✓ 4 Select deployment type
- 5 Configure Single Sign-On
- 6 Select appliance size
- 7 Select datastore
- 8 Configure database
- 9 Network Settings
- 10 Ready to complete

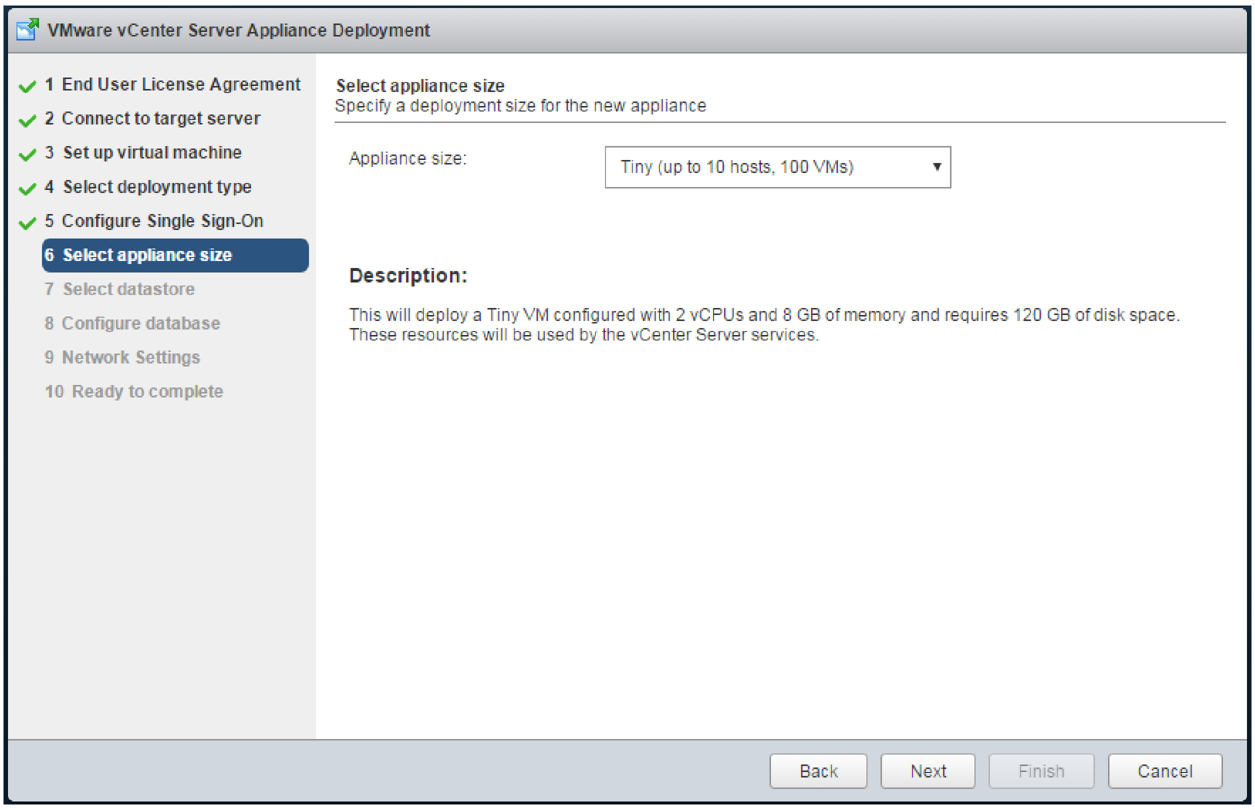
Configure Single Sign-On (SSO)
Connect vCenter Server to a SSO domain in an existing platform services controller. An SSO configuration cannot be changed after deployment.

Platform Services Controller FQDN or IP address:	172.16.105.21
vCenter SSO User name:	administrator
vCenter SSO password:	••••••••••
vCenter Single Sign-On HTTPS Port:	443

⚠ Before proceeding, make sure you provide the password of the user 'administrator' in the existing vCenter Single Sign-On domain that you configured during Platform Services Controller deployment.

Figure 21 Configure Single Sign-On

Select the appliance size based on the deployment size.



VMware vCenter Server Appliance Deployment
✓ 1 End User License Agreement
✓ 2 Connect to target server
✓ 3 Set up virtual machine
✓ 4 Select deployment type
✓ 5 Configure Single Sign-On
6 Select appliance size
7 Select datastore
8 Configure database
9 Network Settings
10 Ready to complete
Back
Next
Finish
Cancel

Select appliance size
Specify a deployment size for the new appliance

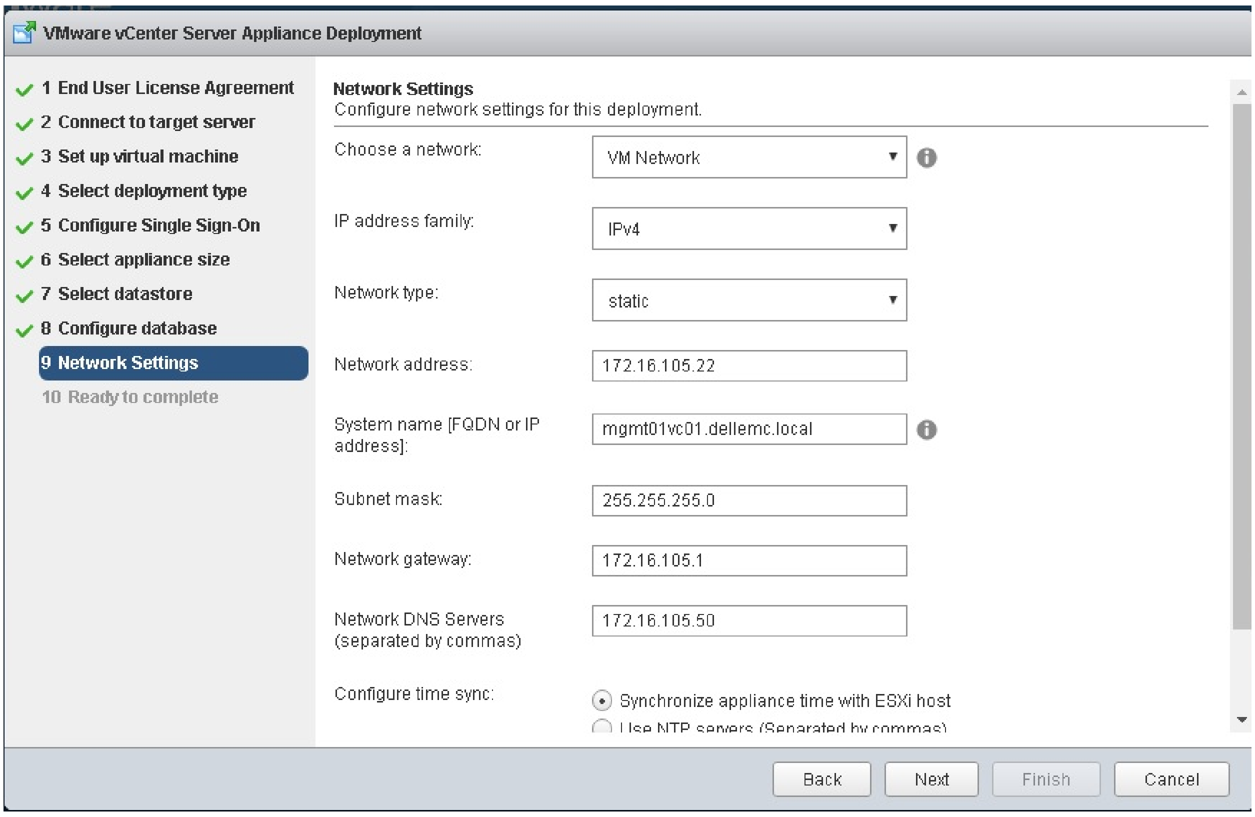
Appliance size: Tiny (up to 10 hosts, 100 VMs)

Description:

This will deploy a Tiny VM configured with 2 vCPUs and 8 GB of memory and requires 120 GB of disk space. These resources will be used by the vCenter Server services.

Figure 22 Select appliance size

Use the embedded database and configure the Network settings.


VMware vCenter Server Appliance Deployment
✓ 1 End User License Agreement
✓ 2 Connect to target server
✓ 3 Set up virtual machine
✓ 4 Select deployment type
✓ 5 Configure Single Sign-On
✓ 6 Select appliance size
✓ 7 Select datastore
✓ 8 Configure database
9 Network Settings
10 Ready to complete
Back
Next
Finish
Cancel

Network Settings
Configure network settings for this deployment.

Choose a network: VM Network

IP address family: IPv4

Network type: static

Network address: 172.16.105.22

System name [FQDN or IP address]: mgmt01vc01.dellemc.local

Subnet mask: 255.255.255.0

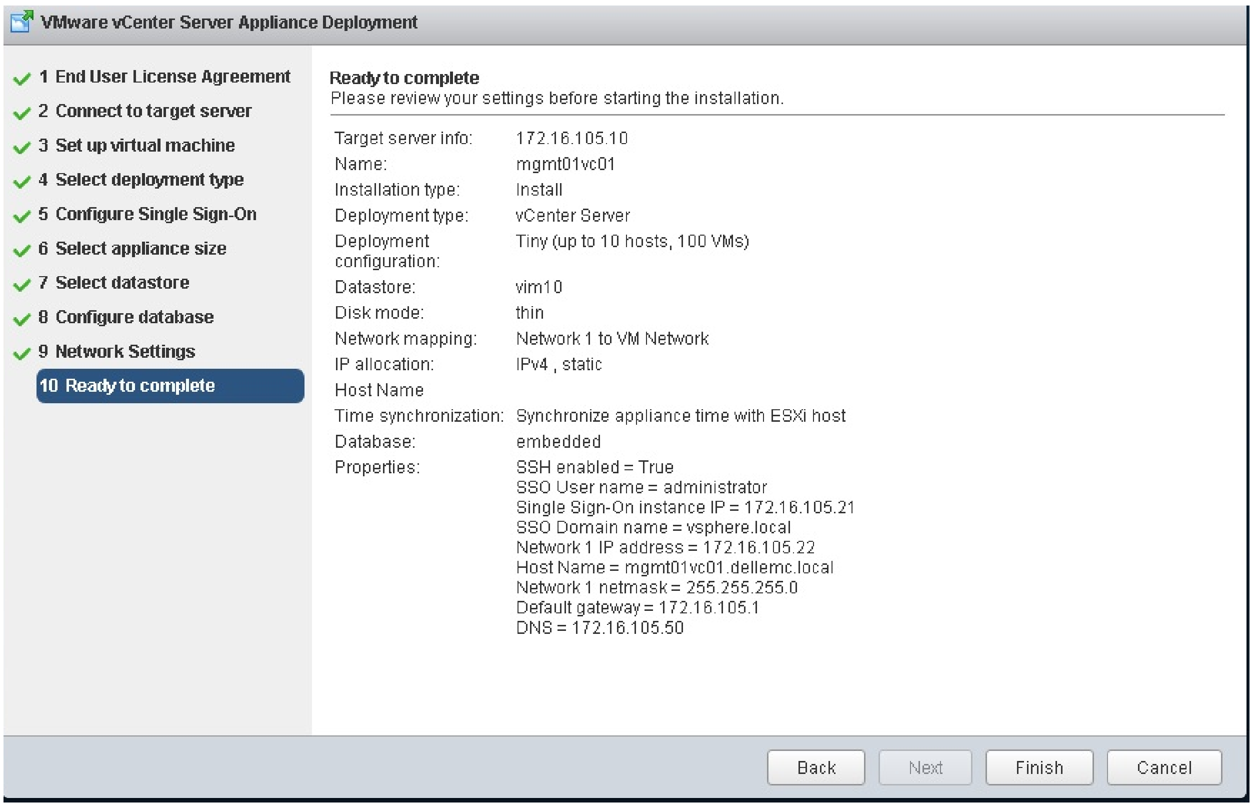
Network gateway: 172.16.105.1

Network DNS Servers (separated by commas): 172.16.105.50

Configure time sync: ● Synchronize appliance time with ESXi host
○ Use NTP servers (Separated by commas)

Figure 23 Network Settings

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

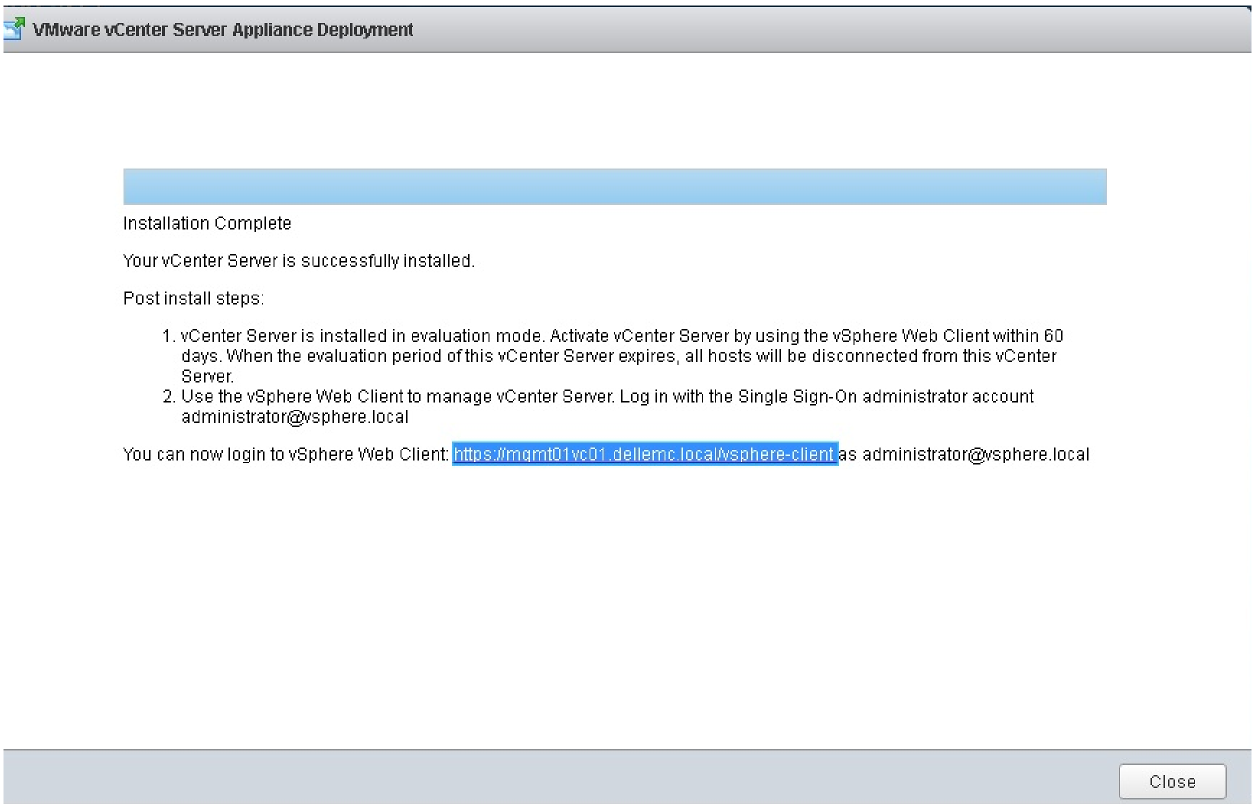

VMware vCenter Server Appliance Deployment
✓ 1 End User License Agreement
✓ 2 Connect to target server
✓ 3 Set up virtual machine
✓ 4 Select deployment type
✓ 5 Configure Single Sign-On
✓ 6 Select appliance size
✓ 7 Select datastore
✓ 8 Configure database
✓ 9 Network Settings
10 Ready to complete
Back
Next
Finish
Cancel

Ready to complete
Please review your settings before starting the installation.

Target server info:	172.16.105.10
Name:	mgmt01vc01
Installation type:	Install
Deployment type:	vCenter Server
Deployment configuration:	Tiny (up to 10 hosts, 100 VMs)
Datastore:	vim10
Disk mode:	thin
Network mapping:	Network 1 to VM Network
IP allocation:	IPv4 , static
Host Name	
Time synchronization:	Synchronize appliance time with ESXi host
Database:	embedded
Properties:	SSH enabled = True SSO User name = administrator Single Sign-On instance IP = 172.16.105.21 SSO Domain name = vsphere.local Network 1 IP address = 172.16.105.22 Host Name = mgmt01vc01.dellemc.local Network 1 netmask = 255.255.255.0 Default gateway = 172.16.105.1 DNS = 172.16.105.50

Figure 24 Ready to complete

Once the installation is complete, it is possible to login to the vSphere web client using the URL given post installation.



Installation Complete

Your vCenter Server is successfully installed.

Post install steps:

1. vCenter Server is installed in evaluation mode. Activate vCenter Server by using the vSphere Web Client within 60 days. When the evaluation period of this vCenter Server expires, all hosts will be disconnected from this vCenter Server.
2. Use the vSphere Web Client to manage vCenter Server. Log in with the Single Sign-On administrator account administrator@vsphere.local

You can now login to vSphere Web Client: https://mgmt01vc01.dellemc.local/vsphere-client as administrator@vsphere.local

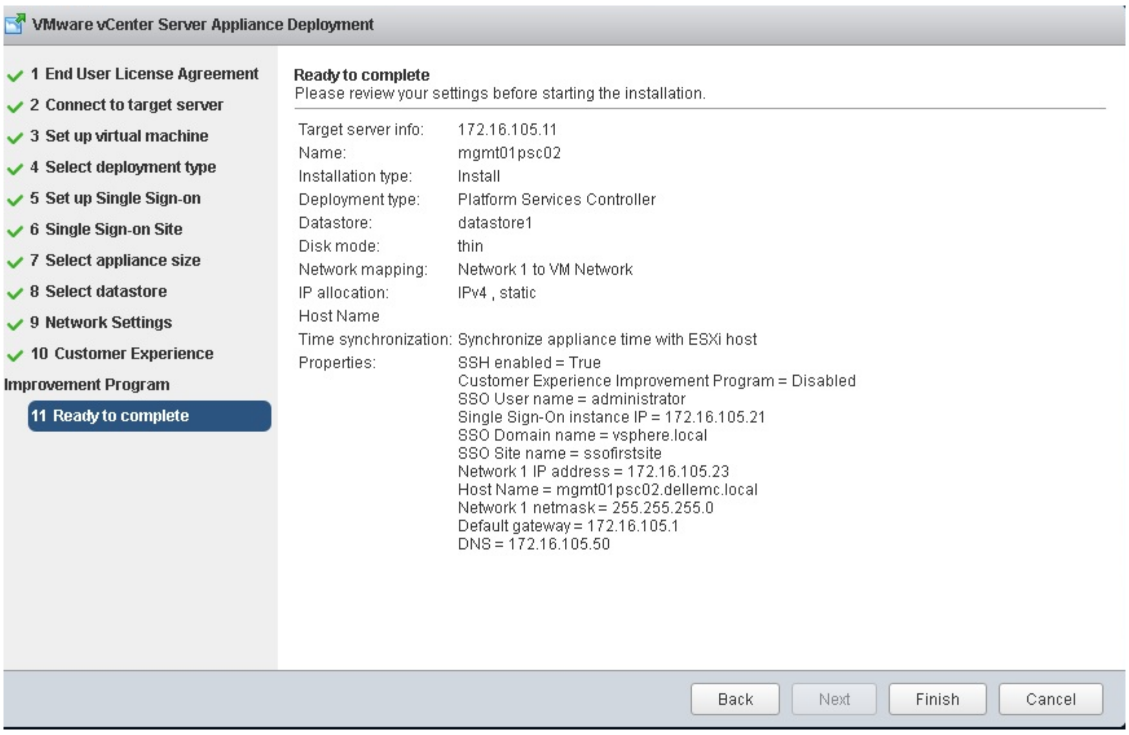
Figure 25 vSphere web client URL

6.4.4 Deploy second EPSC and vCenter

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

Review the Compute EPSC and vCenter configuration before deployment.

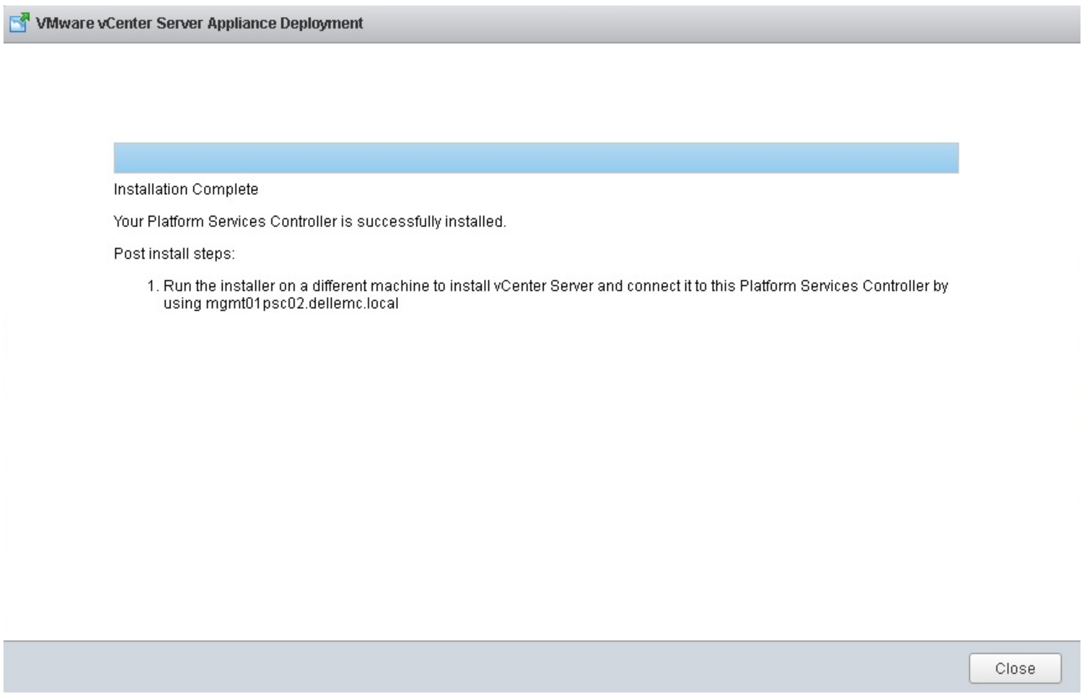
Second EPSC Configuration


VMware vCenter Server Appliance Deployment
✓ 1 End User License Agreement
✓ 2 Connect to target server
✓ 3 Set up virtual machine
✓ 4 Select deployment type
✓ 5 Set up Single Sign-on
✓ 6 Single Sign-on Site
✓ 7 Select appliance size
✓ 8 Select datastore
✓ 9 Network Settings
✓ 10 Customer Experience Improvement Program
11 Ready to complete
Back
Next
Finish
Cancel

Ready to complete
Please review your settings before starting the installation.

Target server info: 172.16.105.11
Name: mgmt01psc02
Installation type: Install
Deployment type: Platform Services Controller
Datastore: datastore1
Disk mode: thin
Network mapping: Network 1 to VM Network
IP allocation: IPv4 , static
Host Name
Time synchronization: Synchronize appliance time with ESXi host
Properties: SSH enabled = True
Customer Experience Improvement Program = Disabled
SSO User name = administrator
Single Sign-On instance IP = 172.16.105.21
SSO Domain name = vsphere.local
SSO Site name = ssofirstsite
Network 1 IP address = 172.16.105.23
Host Name = mgmt01psc02.dellemc.local
Network 1 netmask = 255.255.255.0
Default gateway = 172.16.105.1
DNS = 172.16.105.50

Figure 26 Second EPSC Configuration



Installation Complete

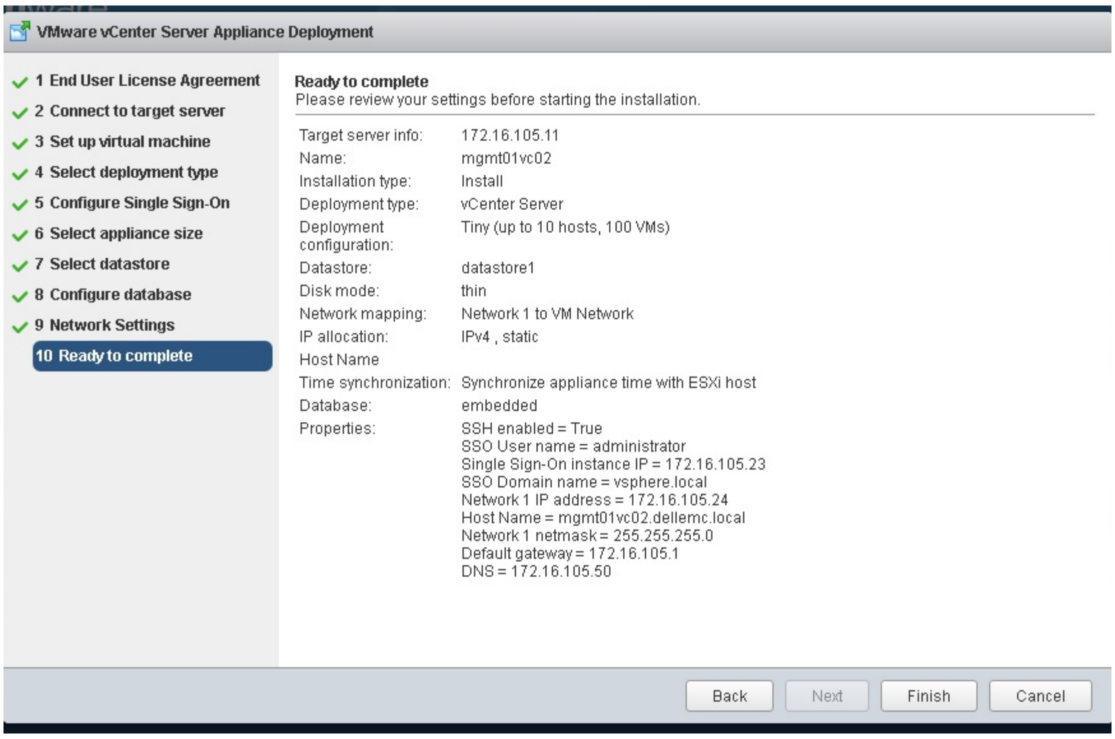
Your Platform Services Controller is successfully installed.

Post install steps:

1. Run the installer on a different machine to install vCenter Server and connect it to this Platform Services Controller by using mgmt01psc02.dellemc.local

Figure 27 Installation Complete

Second VC Configuration



Ready to complete

Please review your settings before starting the installation.

Target server info:	172.16.105.11
Name:	mgmt01vc02
Installation type:	Install
Deployment type:	vCenter Server
Deployment configuration:	Tiny (up to 10 hosts, 100 VMs)
Datastore:	datastore1
Disk mode:	thin
Network mapping:	Network 1 to VM Network
IP allocation:	IPv4 , static
Host Name	
Time synchronization:	Synchronize appliance time with ESXi host
Database:	embedded
Properties:	SSH enabled = True SSO User name = administrator Single Sign-On instance IP = 172.16.105.23 SSO Domain name = vsphere.local Network 1 IP address = 172.16.105.24 Host Name = mgmt01vc02.dellemc.local Network 1 netmask = 255.255.255.0 Default gateway = 172.16.105.1 DNS = 172.16.105.50

Figure 28 Second VC Configuration

6.5 Build datacenter

Once 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/

Management VC: https://172.16.105.22:9443/vsphere-client/

Edge and Resource VC: https://172.16.105.24:9443/vsphere-client/

6.6 Add Licenses

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

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

To add the licenses, login to vCenter server, then from the home screen click **Administration → Licenses**. Under the License Keys tab, click on the (**+**) sign to add the License keys.

6.7 Create datacenter and clusters

Login to the management cluster vCenter appliance and navigate from the home screen tyo **vCenter → 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 management vCenter only a management cluster should be created.

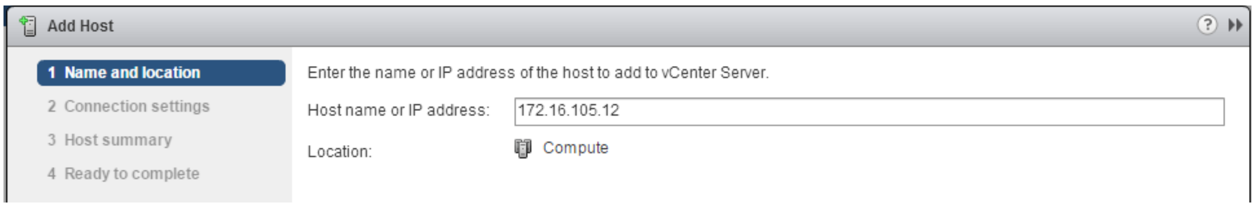
In the Compute vCenter, create two clusters: Compute and Edge. Do not enable vSphere HA and vSphere DRS in this step.

6.8 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. Use the following 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

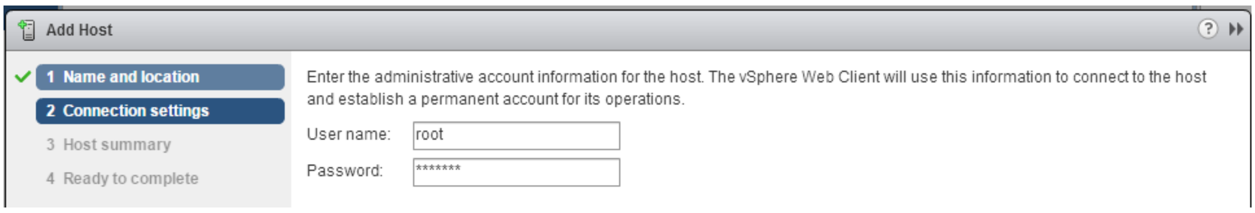


Enter the name or IP address of the host to add to vCenter Server.

Host name or IP address: 172.16.105.12

Location: Compute

Figure 29 Host name or IP address



Enter the administrative account information for the host. The vSphere Web Client will use this information to connect to the host and establish a permanent account for its operations.

User name: root

Password: *******

Figure 30 User name and Password

6.9 Configure host networking

Each host in each cluster typically needs to be configured with minimum of three different types of networks.

Configuring host networking using Distributed vSwitch (DvSwitch) is simple and effective way to manage networking uniformly.

Configuring DvSwitch is a three-step process.

1. Creating a distributed vSwitch (MTU/LLDP)
2. Configuring uplink link ports (LACP or NIC Teaming)
3. Configuring port groups (VLAN/VMkernel ports if necessary)

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

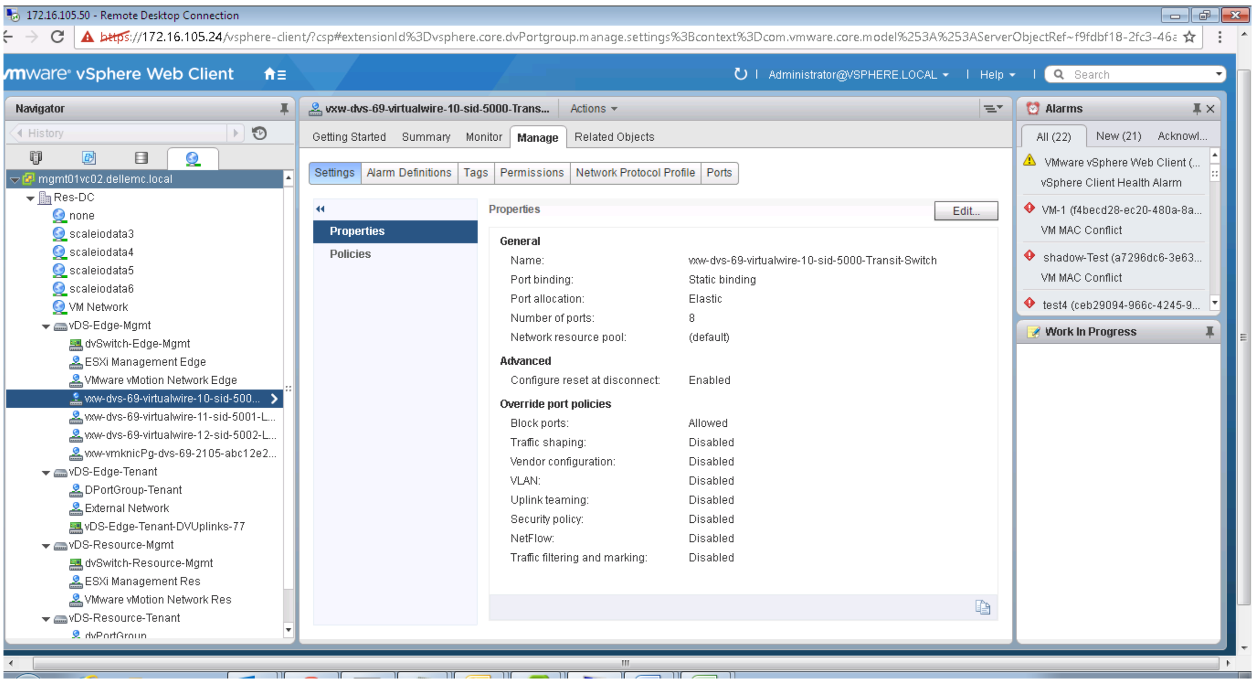
6.9.1 Management Networking

By default, during ESXi installation in a host, vSwitch0 is created with the management port selected during ESXi installation as the Uplink port.

6.9.1.1 VDS Installation

Log into the vSphere web client.

Click on the Networking tab as shown below.


172.16.105.50 - Remote Desktop Connection
https://172.16.105.24/vsphere-client/?csp#extensionId%3Dvsphere.core.dvPortgroup.manage.settings%3Bcontext%3Dcom.vmware.core.model%253A%253AServerObjectRef~f9fdbf18-2fc3-46a
vmware vSphere Web Client
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
History
mgmt01vc02.dellemc.local
Res-DC
none
scaleiodata3
scaleiodata4
scaleiodata5
scaleiodata6
VM Network
vDS-Edge-Mgmt
dvSwitch-Edge-Mgmt
ESXi Management Edge
VMware vMotion Network Edge
vxw-dvs-69-virtualwire-10-sid-500...
vxw-dvs-69-virtualwire-11-sid-5001-L...
vxw-dvs-69-virtualwire-12-sid-5002-L...
vxw-vmknicPg-dvs-69-2105-abc12e2...
vDS-Edge-Tenant
DPortGroup-Tenant
External Network
vDS-Edge-Tenant-DVUplinks-77
vDS-Resource-Mgmt
dvSwitch-Resource-Mgmt
ESXi Management Res
VMware vMotion Network Res
vDS-Resource-Tenant
dvPortGroup
vxw-dvs-69-virtualwire-10-sid-5000-Trans...
Actions
Getting Started
Summary
Monitor
Manage
Related Objects
Settings
Alarm Definitions
Tags
Permissions
Network Protocol Profile
Ports
Properties
Policies
Edit...
Alarms
All (22)
New (21)
Acknowl...
VMware vSphere Web Client (...
vSphere Client Health Alarm
VM-1 (f4becd28-ec20-480a-8a...
VM MAC Conflict
shadow-Test (a7296dc6-3e63...
VM MAC Conflict
test4 (ceb29094-966c-4245-9...
Work In Progress

Properties

General

Name: vxw-dvs-69-virtualwire-10-sid-5000-Transit-Switch
Port binding: Static binding
Port allocation: Elastic
Number of ports: 8
Network resource pool: (default)

Advanced

Configure reset at disconnect: Enabled

Override port policies

Block ports: Allowed
Traffic shaping: Disabled
Vendor configuration: Disabled
VLAN: Disabled
Uplink teaming: Disabled
Security policy: Disabled
NetFlow: Disabled
Traffic filtering and marking: Disabled

Figure 31 Networking tab

Right click the cluster (Res-DC in the screenshot) and click **New Distributed Switch** to create the switch.

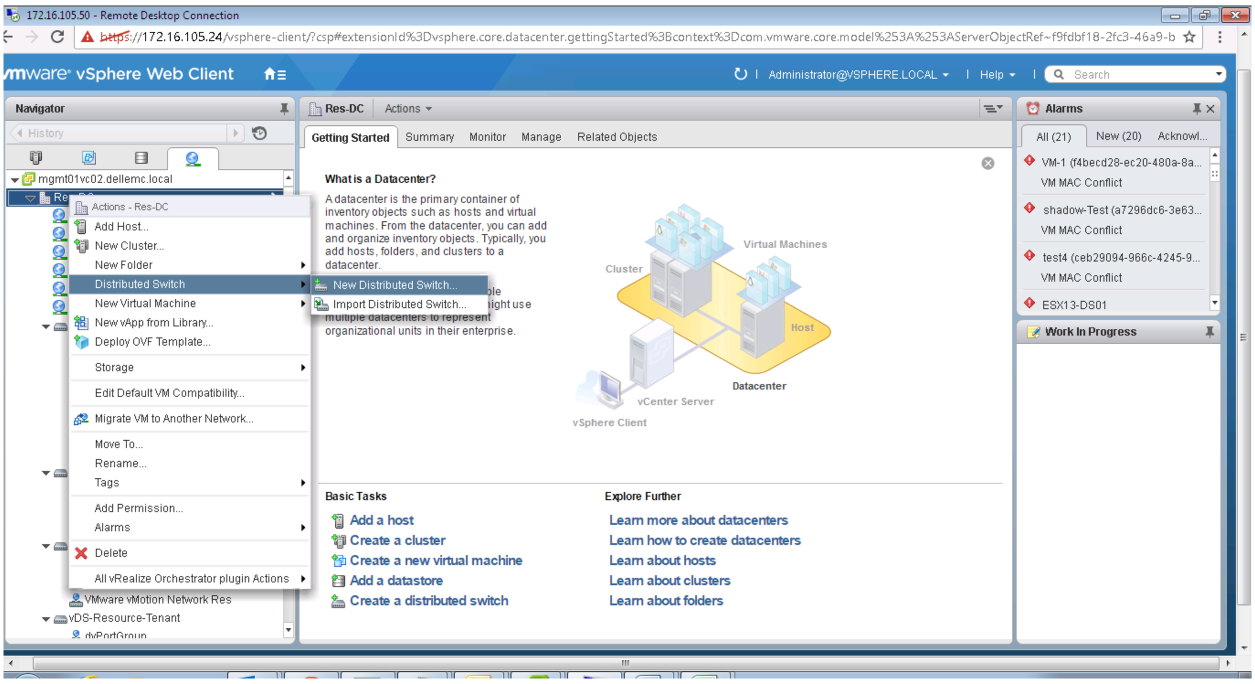
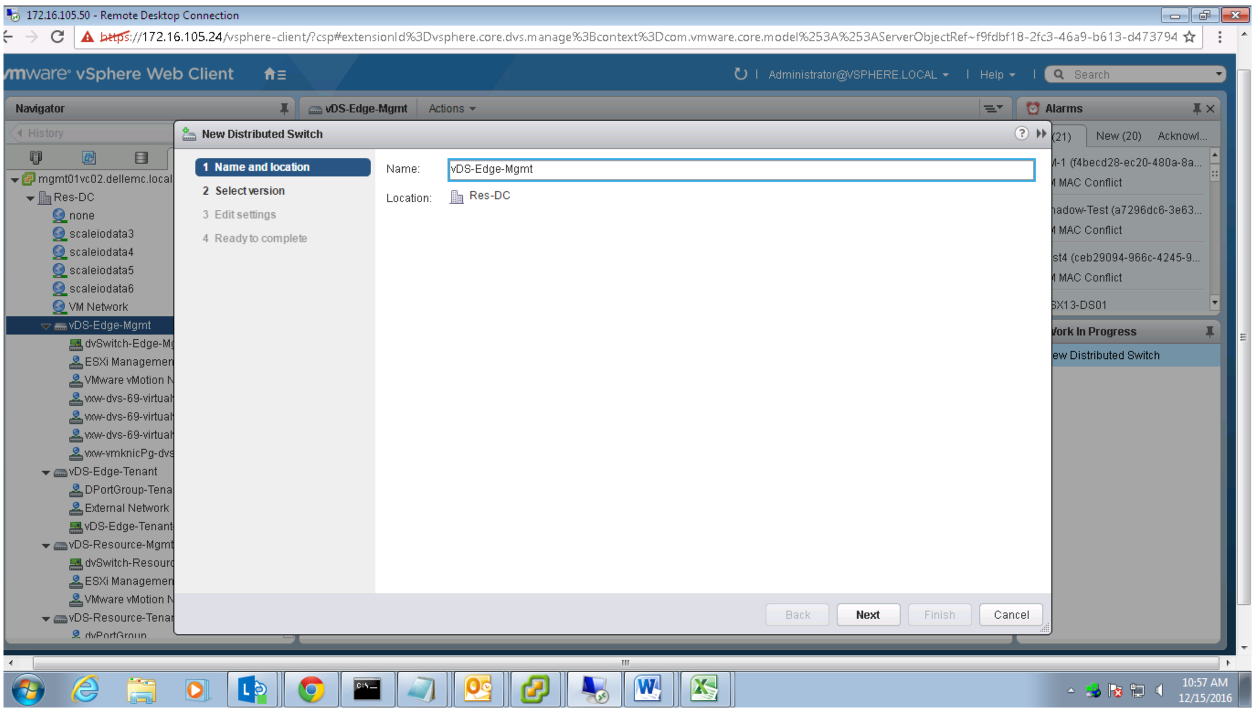


Figure 32 Create New Distributed Switch



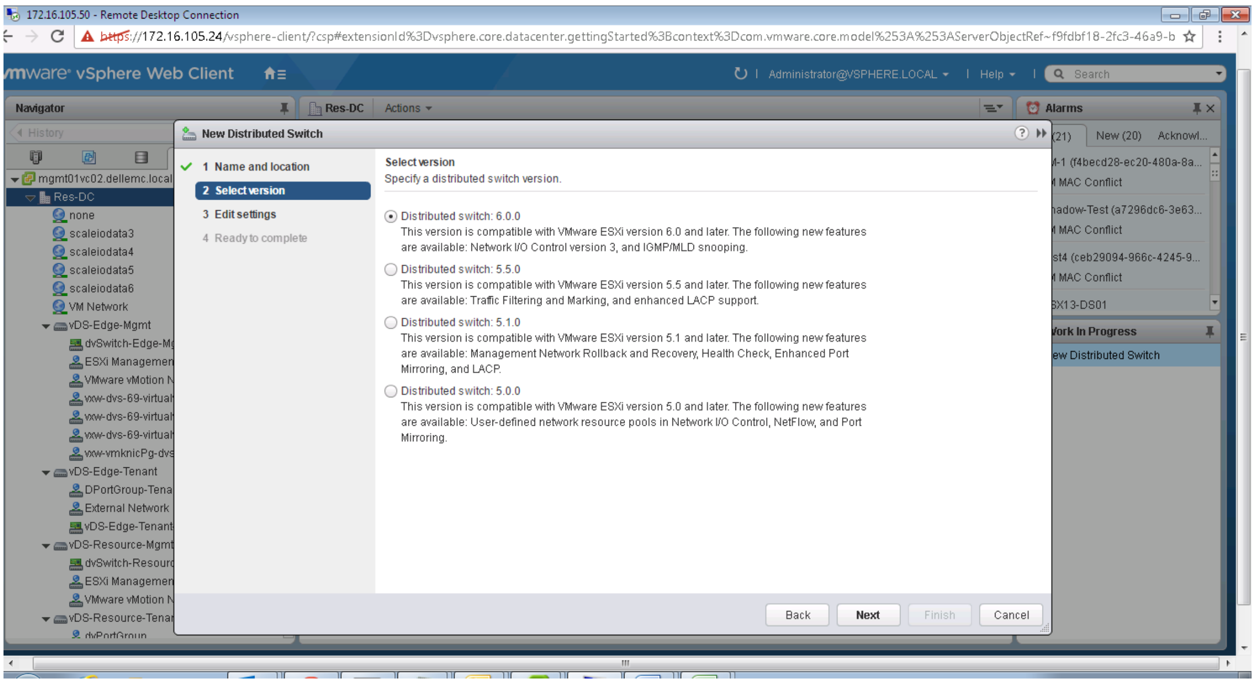
Name: vDS-Edge-Mgmt

Location: Res-DC

Figure 33 New Distributed switch

Give the distributed switch a name of your choice.

Select the version and click **Next**.



Select version
Specify a distributed switch version.

● Distributed switch: 6.0.0
This version is compatible with VMware ESXi version 6.0 and later. The following new features are available: Network I/O Control version 3, and IGMP/MLD snooping.

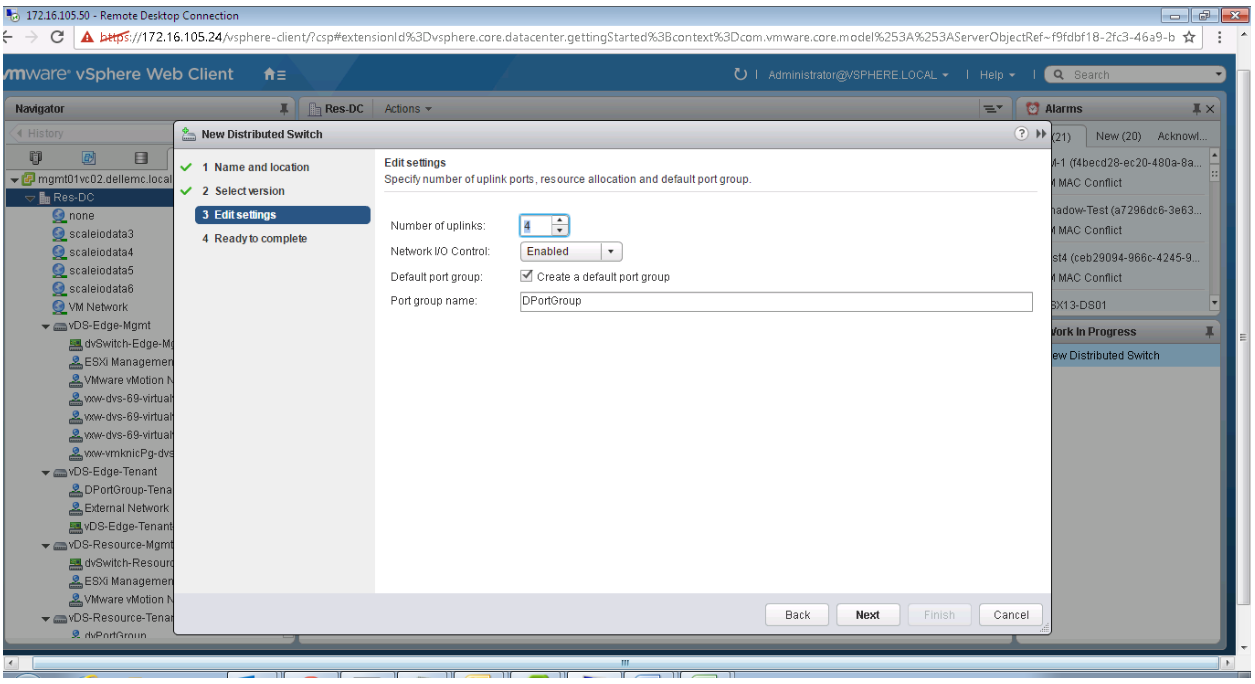
○ Distributed switch: 5.5.0
This version is compatible with VMware ESXi version 5.5 and later. The following new features are available: Traffic Filtering and Marking, and enhanced LACP support.

○ Distributed switch: 5.1.0
This version is compatible with VMware ESXi version 5.1 and later. The following new features are available: Management Network Rollback and Recovery, Health Check, Enhanced Port Mirroring, and LACP.

○ Distributed switch: 5.0.0
This version is compatible with VMware ESXi version 5.0 and later. The following new features are available: User-defined network resource pools in Network I/O Control, NetFlow, and Port Mirroring.

Figure 34 Select version for distributed switch

Select the number of uplinks and click **Next**.



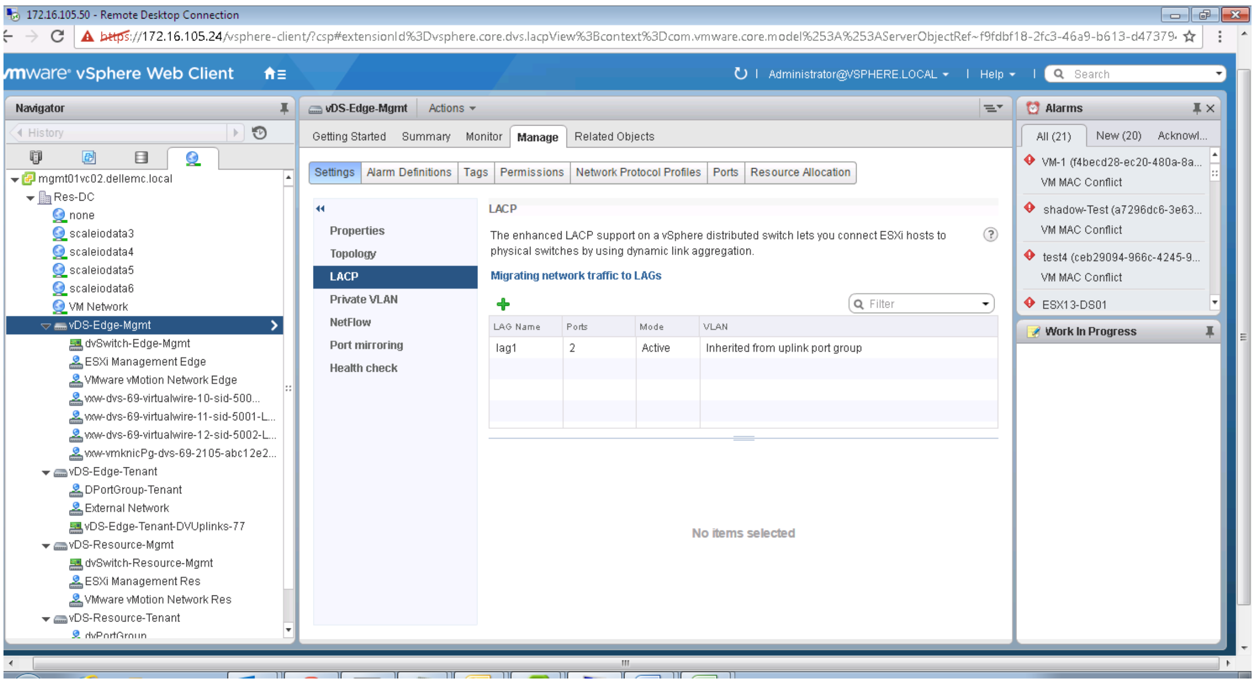
Edit settings
Specify number of uplink ports, resource allocation and default port group.

Number of uplinks: 4
Network I/O Control: Enabled
Default port group: ☑ Create a default port group
Port group name: DPortGroup

Figure 35 Select number of uplinks

Click **Finish** to complete.

Click **Switch**, select the Manage tab and click **LACP configuration**.



vDS-Edge-Mgmt — Manage — Settings — LACP

The enhanced LACP support on a vSphere distributed switch lets you connect ESXi hosts to physical switches by using dynamic link aggregation.

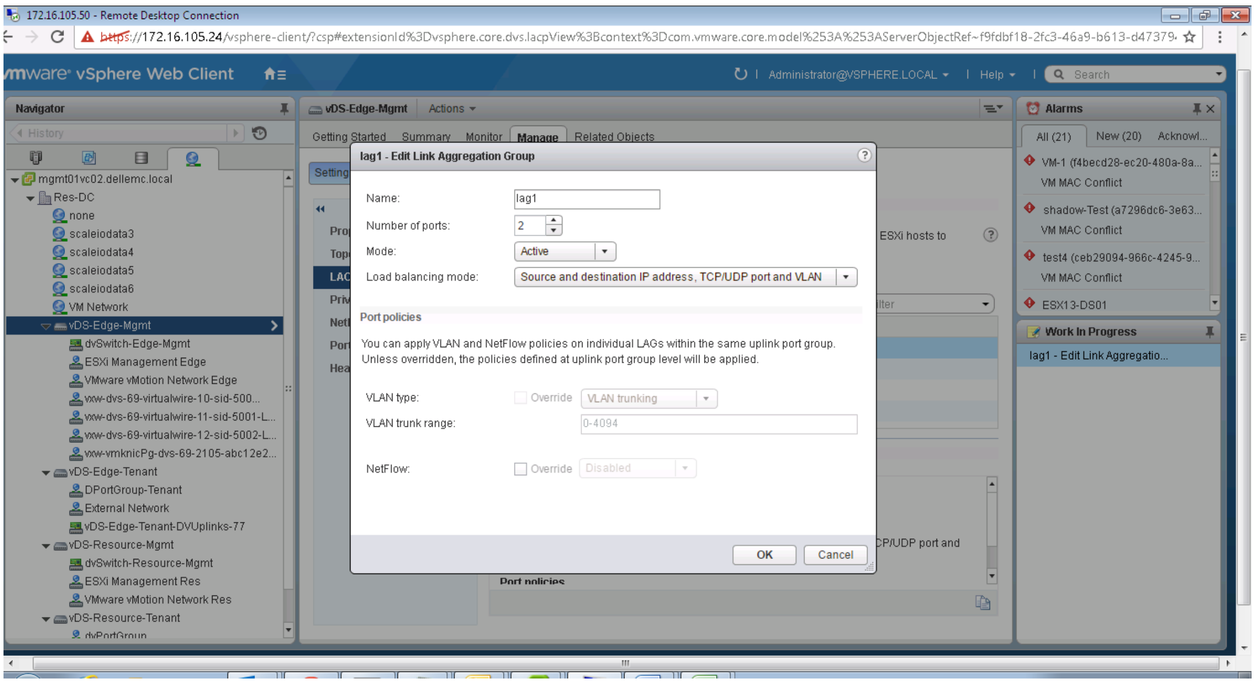
Migrating network traffic to LAGs

LAG Name	Ports	Mode	VLAN
lag1	2	Active	Inherited from uplink port group

No items selected

Figure 36 LACP configuration

Add lag1 with the configuration shown.



lag1 - Edit Link Aggregation Group

Name: lag1

Number of ports: 2

Mode: Active

Load balancing mode: Source and destination IP address, TCP/UDP port and VLAN

Port policies

You can apply VLAN and NetFlow policies on individual LAGs within the same uplink port group. Unless overridden, the policies defined at uplink port group level will be applied.

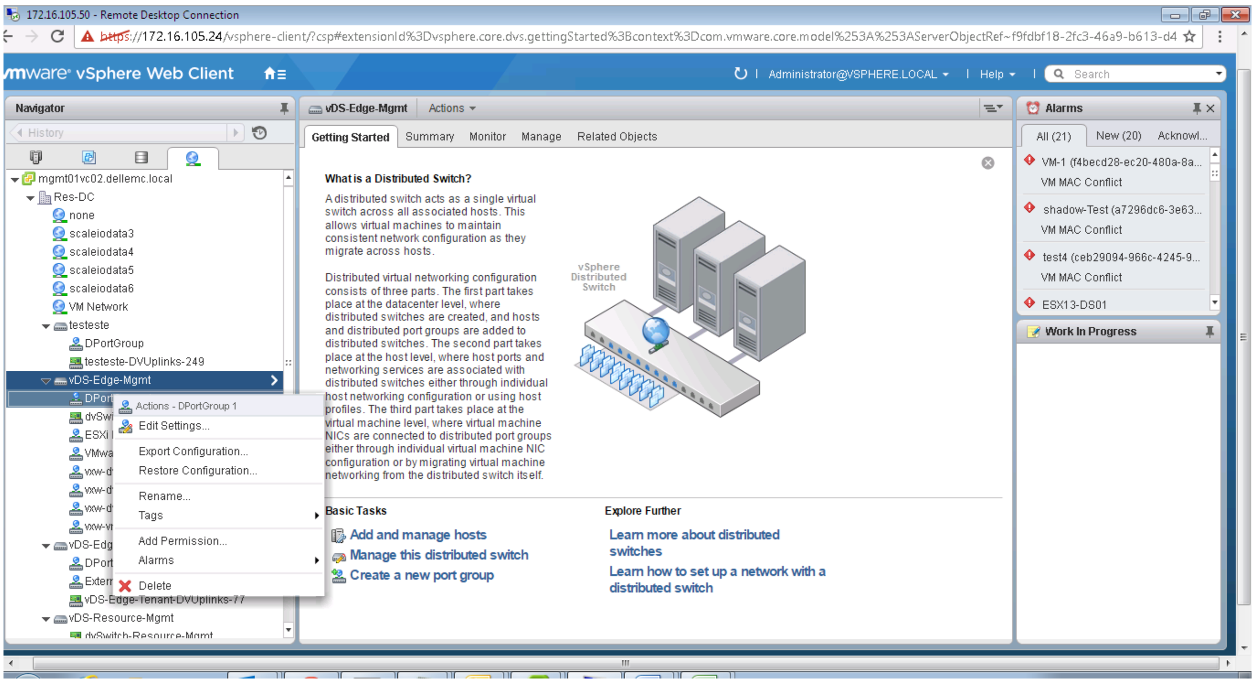
VLAN type: □ Override VLAN trunking

VLAN trunk range: 0-4094

NetFlow: □ Override Disabled

Figure 37 Lag1 configuration

Default port group will be created under the switch.



What is a Distributed Switch?

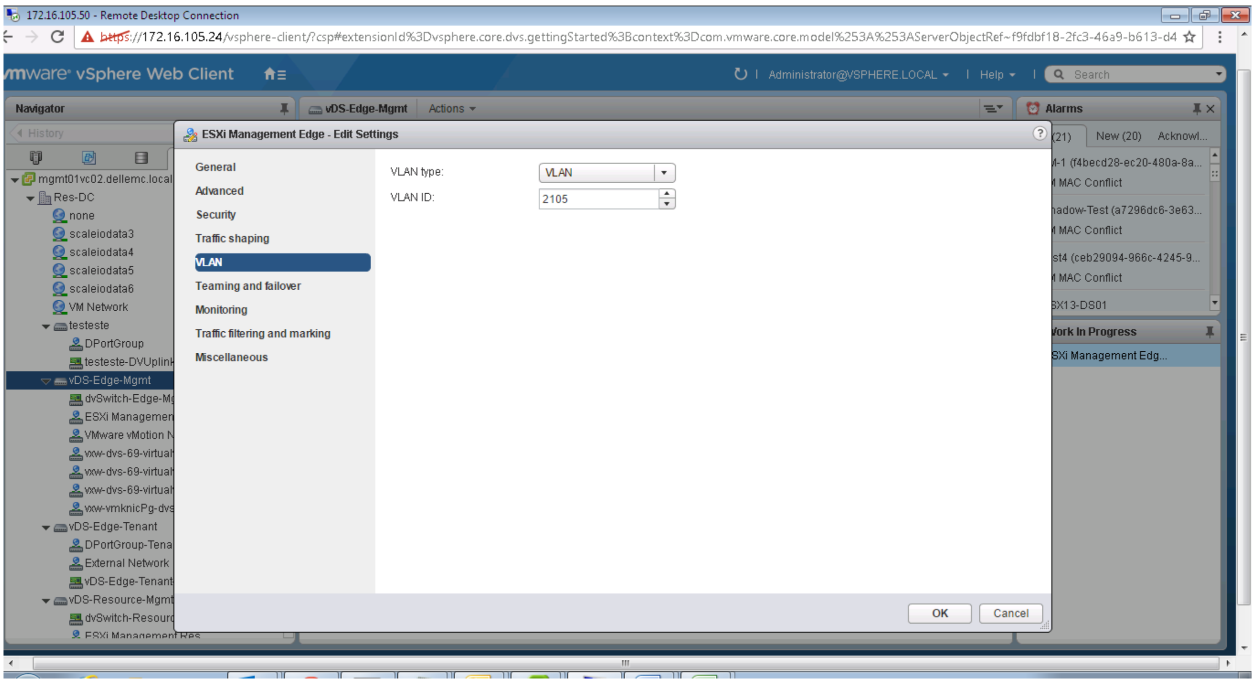
A distributed switch acts as a single virtual switch across all associated hosts. This allows virtual machines to maintain consistent network configuration as they migrate across hosts.

Distributed virtual networking configuration consists of three parts. The first part takes place at the datacenter level, where distributed switches are created, and hosts and distributed port groups are added to distributed switches. The second part takes place at the host level, where host ports and networking services are associated with distributed switches either through individual host networking configuration or using host profiles. The third part takes place at the virtual machine level, where virtual machine NICs are connected to distributed port groups either through individual virtual machine NIC configuration or by migrating virtual machine networking from the distributed switch itself.

Figure 38 Default port group

Right Click and click **Edit Settings** and edit the port as required.

Name the port as required.



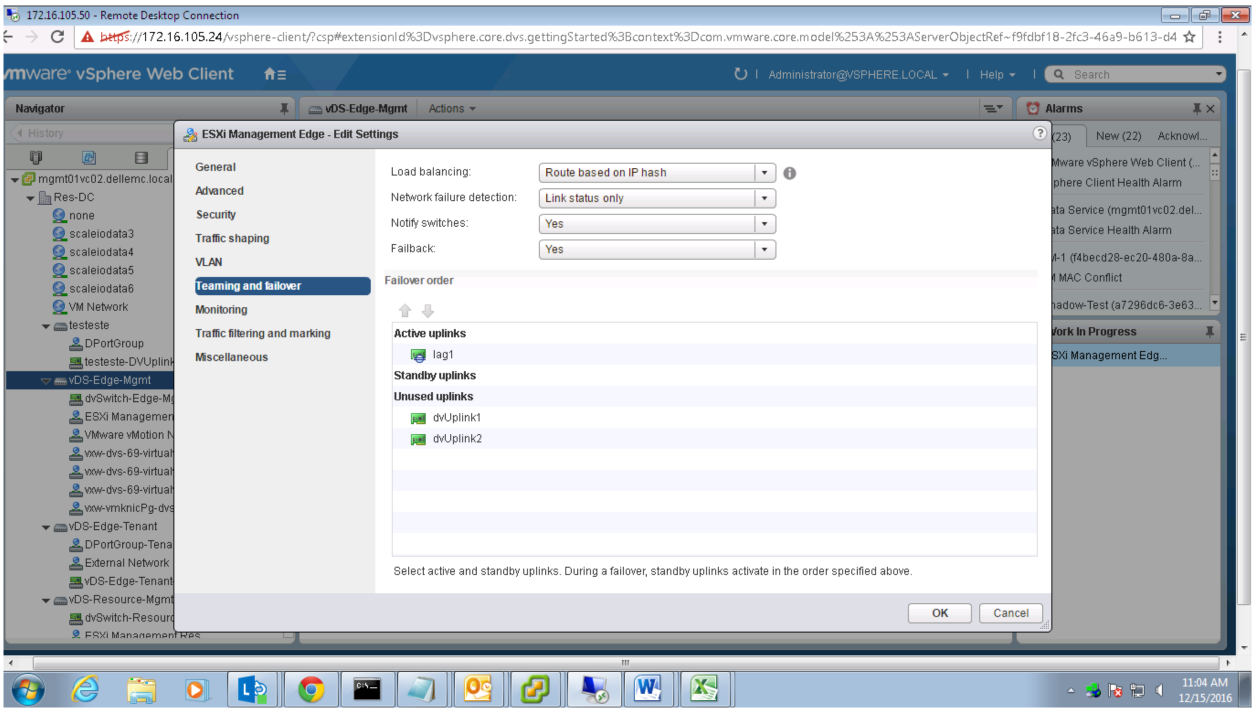
VLAN type: VLAN

VLAN ID: 2105

Figure 39 Configuring port group

Select the VLAN as per your design.

In the teaming and failover configuration, configure the settings as below. Please note lag1 should be under active uplinks.



ESXi Management Edge - Edit Settings

- General
- Advanced
- Security
- Traffic shaping
- VLAN
- **Teaming and failover**
- Monitoring
- Traffic filtering and marking
- Miscellaneous

Load balancing: Route based on IP hash

Network failure detection: Link status only

Notify switches: Yes

Failback: Yes

Failover order

Active uplinks
- lag1

Standby uplinks

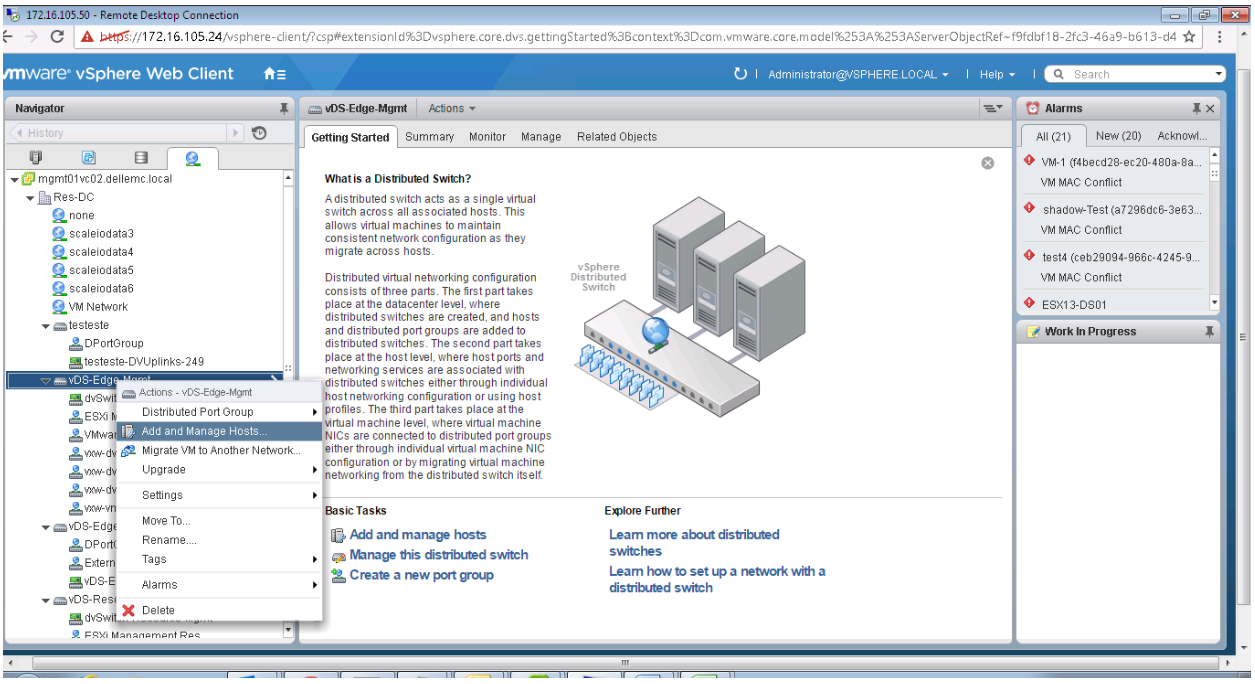
Unused uplinks
- dvUplink1
- dvUplink2

Select active and standby uplinks. During a failover, standby uplinks activate in the order specified above.

Figure 40 Teaming and failover configuration

The other settings should not be changed.

Right click the **vDS** and click **Add and Manage Hosts**.



What is a Distributed Switch?

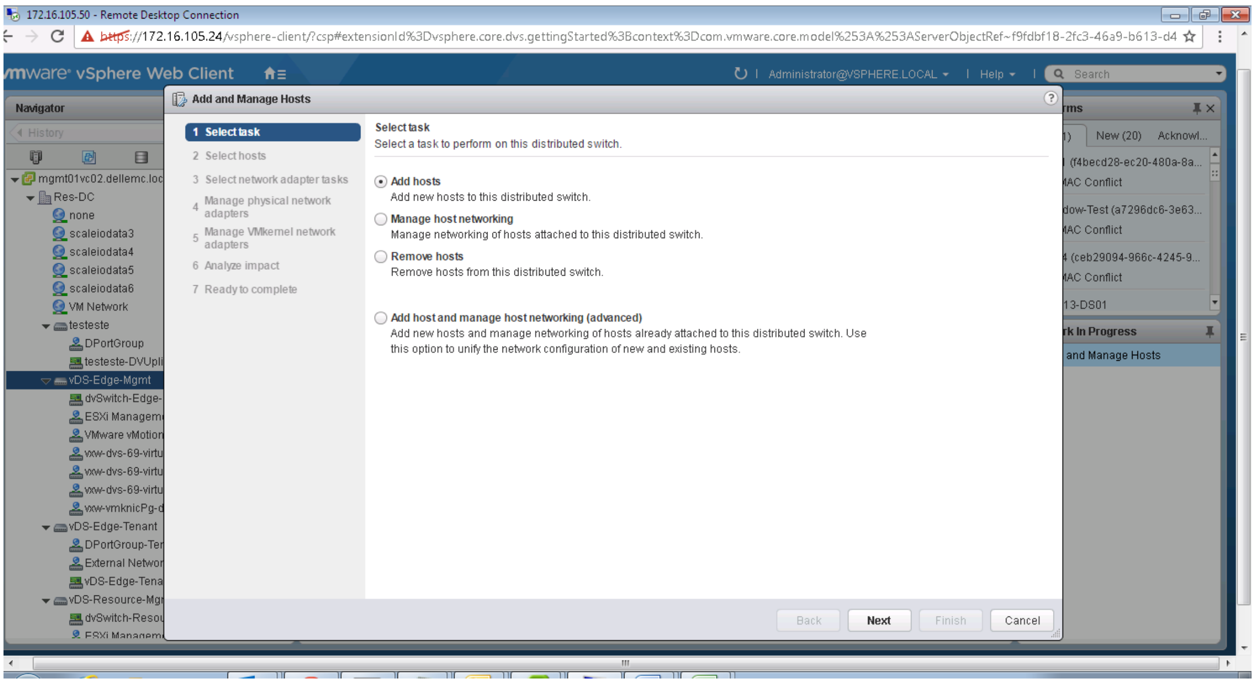
A distributed switch acts as a single virtual switch across all associated hosts. This allows virtual machines to maintain consistent network configuration as they migrate across hosts.

Distributed virtual networking configuration consists of three parts. The first part takes place at the datacenter level, where distributed switches are created, and hosts and distributed port groups are added to distributed switches. The second part takes place at the host level, where host ports and networking services are associated with distributed switches either through individual host networking configuration or using host profiles. The third part takes place at the virtual machine level, where virtual machine NICs are connected to distributed port groups either through individual virtual machine NIC configuration or by migrating virtual machine networking from the distributed switch itself.

Basic Tasks
- Add and manage hosts
- Manage this distributed switch
- Create a new port group

Explore Further
- Learn more about distributed switches
- Learn how to set up a network with a distributed switch

Figure 41 Add and Manage Hosts



Add and Manage Hosts

1 Select task
2 Select hosts
3 Select network adapter tasks
4 Manage physical network adapters
5 Manage VMkernel network adapters
6 Analyze impact
7 Ready to complete

Select task
Select a task to perform on this distributed switch.

● Add hosts
Add new hosts to this distributed switch.

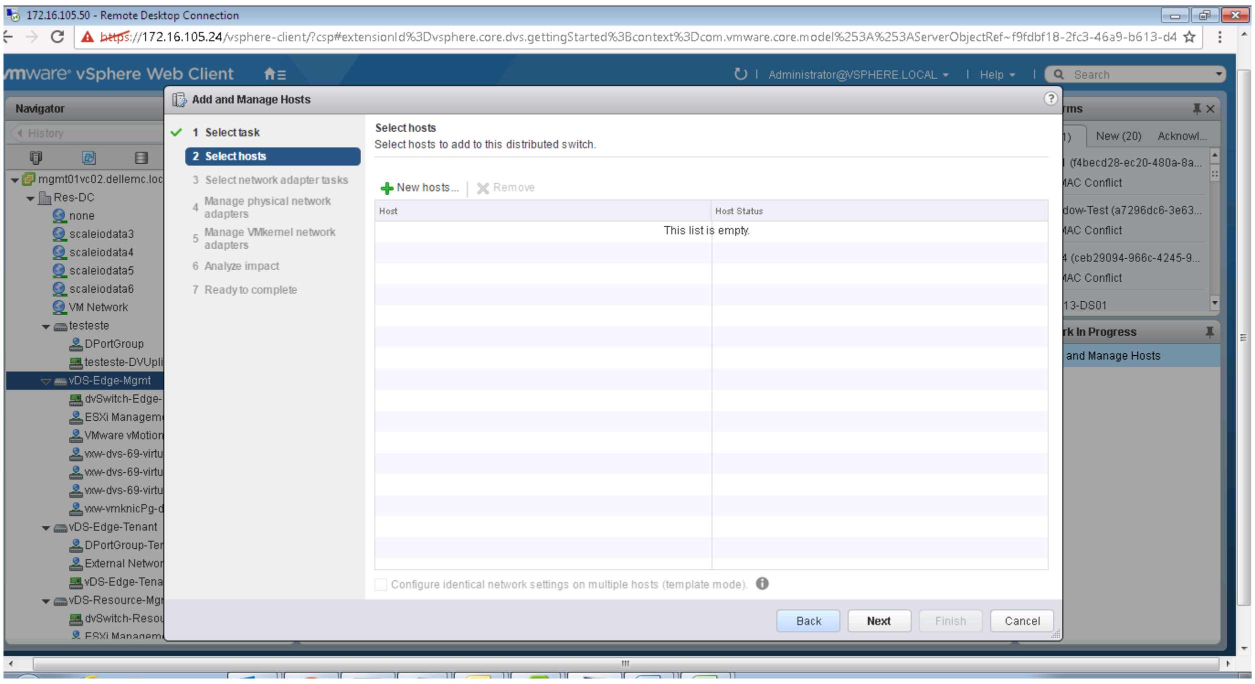
○ Manage host networking
Manage networking of hosts attached to this distributed switch.

○ Remove hosts
Remove hosts from this distributed switch.

○ Add host and manage host networking (advanced)
Add new hosts and manage networking of hosts already attached to this distributed switch. Use this option to unify the network configuration of new and existing hosts.

Figure 42 Add Hosts

Click **New Hosts**.



Add and Manage Hosts

✓ 1 Select task
2 Select hosts
3 Select network adapter tasks
4 Manage physical network adapters
5 Manage VMkernel network adapters
6 Analyze impact
7 Ready to complete

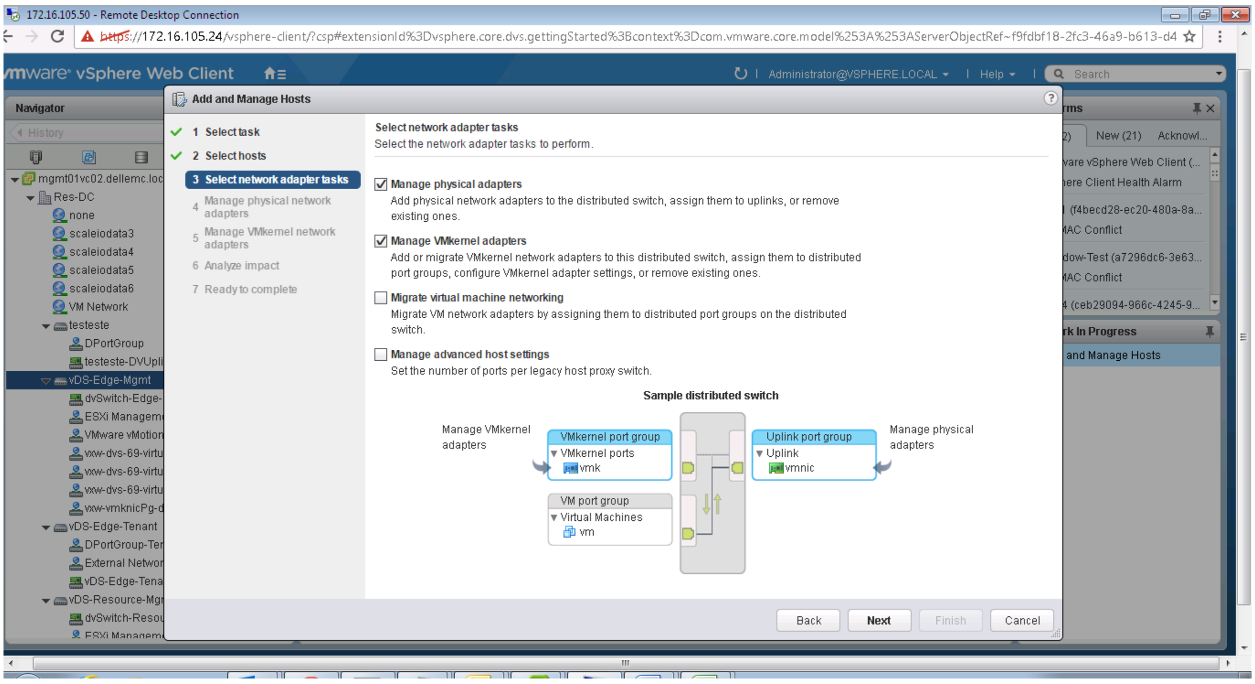
Select hosts
Select hosts to add to this distributed switch.

Host	Host Status
This list is empty.	

□ Configure identical network settings on multiple hosts (template mode).

Figure 43 New Hosts

Select the host that will be attached. Do not select all hosts, they will be added one at a time.



Add and Manage Hosts

- ✓ 1 Select task
- ✓ 2 Select hosts
- 3 Select network adapter tasks
- 4 Manage physical network adapters
- 5 Manage VMkernel network adapters
- 6 Analyze impact
- 7 Ready to complete

Select network adapter tasks
Select the network adapter tasks to perform.

☑ **Manage physical adapters**
Add physical network adapters to the distributed switch, assign them to uplinks, or remove existing ones.

☑ **Manage VMkernel adapters**
Add or migrate VMkernel network adapters to this distributed switch, assign them to distributed port groups, configure VMkernel adapter settings, or remove existing ones.

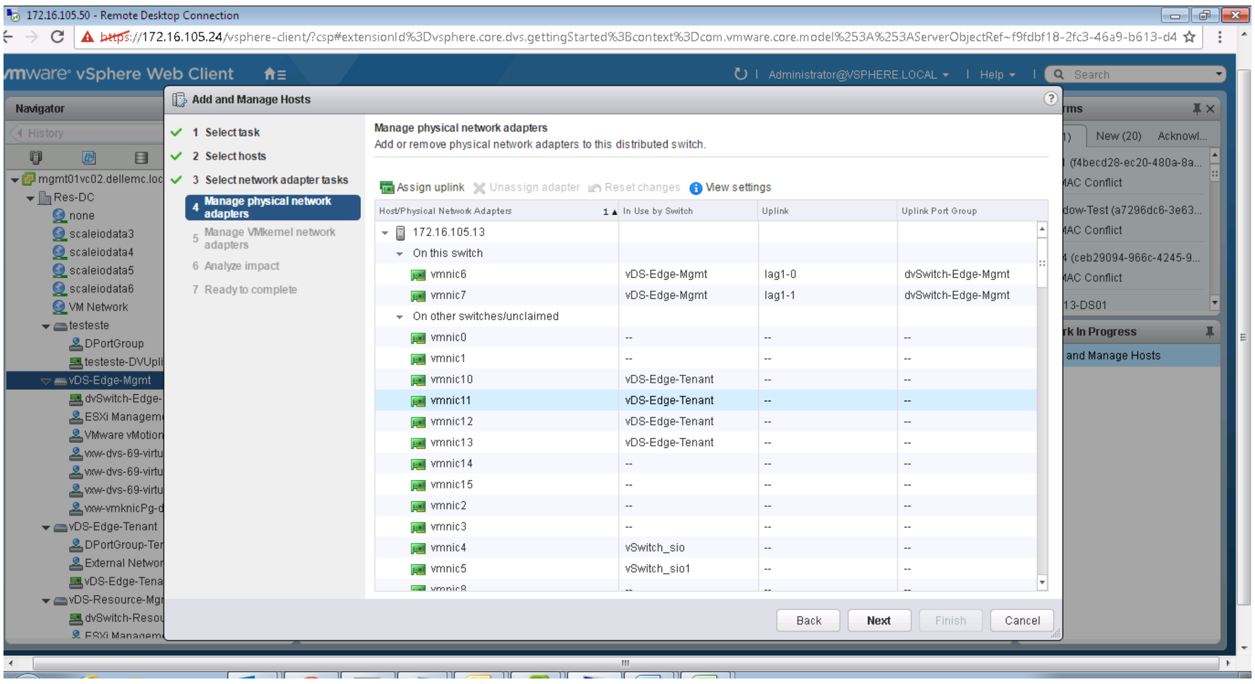
☐ **Migrate virtual machine networking**
Migrate VM network adapters by assigning them to distributed port groups on the distributed switch.

☐ **Manage advanced host settings**
Set the number of ports per legacy host proxy switch.

Figure 44 Select network adapter tasks

Click **Next** to manage the adapters.

Select the adapters from “On other switch” section and click **Assign Uplink**. Select lag1-0.



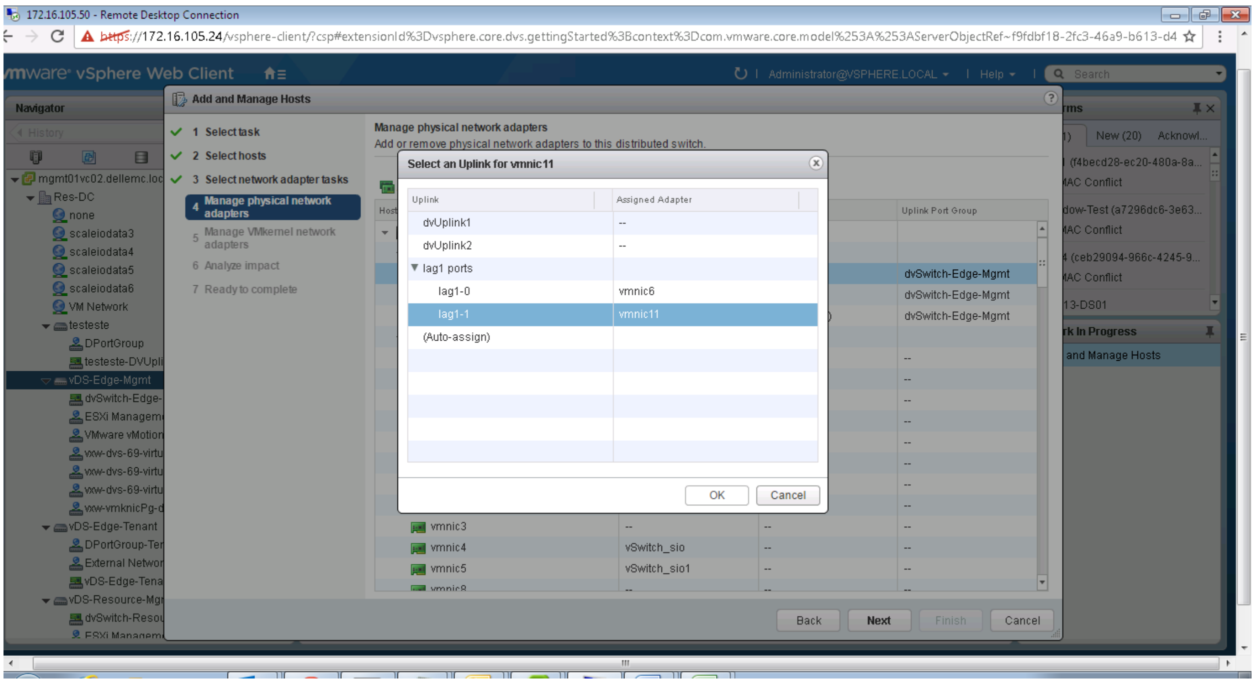
Add and Manage Hosts

- ✓ 1 Select task
- ✓ 2 Select hosts
- ✓ 3 Select network adapter tasks
- 4 Manage physical network adapters
- 5 Manage VMkernel network adapters
- 6 Analyze impact
- 7 Ready to complete

Manage physical network adapters
Add or remove physical network adapters to this distributed switch.

Host/Physical Network Adapters	In Use by Switch	Uplink	Uplink Port Group
172.16.105.13			
On this switch			
vmnic6	vDS-Edge-Mgmt	lag1-0	dvSwitch-Edge-Mgmt
vmnic7	vDS-Edge-Mgmt	lag1-1	dvSwitch-Edge-Mgmt
On other switches/unclaimed			
vmnic0	--	--	--
vmnic1	--	--	--
vmnic10	vDS-Edge-Tenant	--	--
vmnic11	vDS-Edge-Tenant	--	--
vmnic12	vDS-Edge-Tenant	--	--
vmnic13	vDS-Edge-Tenant	--	--
vmnic14	--	--	--
vmnic15	--	--	--
vmnic2	--	--	--
vmnic3	--	--	--
vmnic4	vSwitch_sio	--	--
vmnic5	vSwitch_sio1	--	--
vmnic8	--	--	--

Figure 45 Select adapters



Add and Manage Hosts

1 Select task
2 Select hosts
3 Select network adapter tasks
4 Manage physical network adapters
5 Manage VMkernel network adapters
6 Analyze impact
7 Ready to complete

Manage physical network adapters

Add or remove physical network adapters to this distributed switch.

Select an Uplink for vmnic11

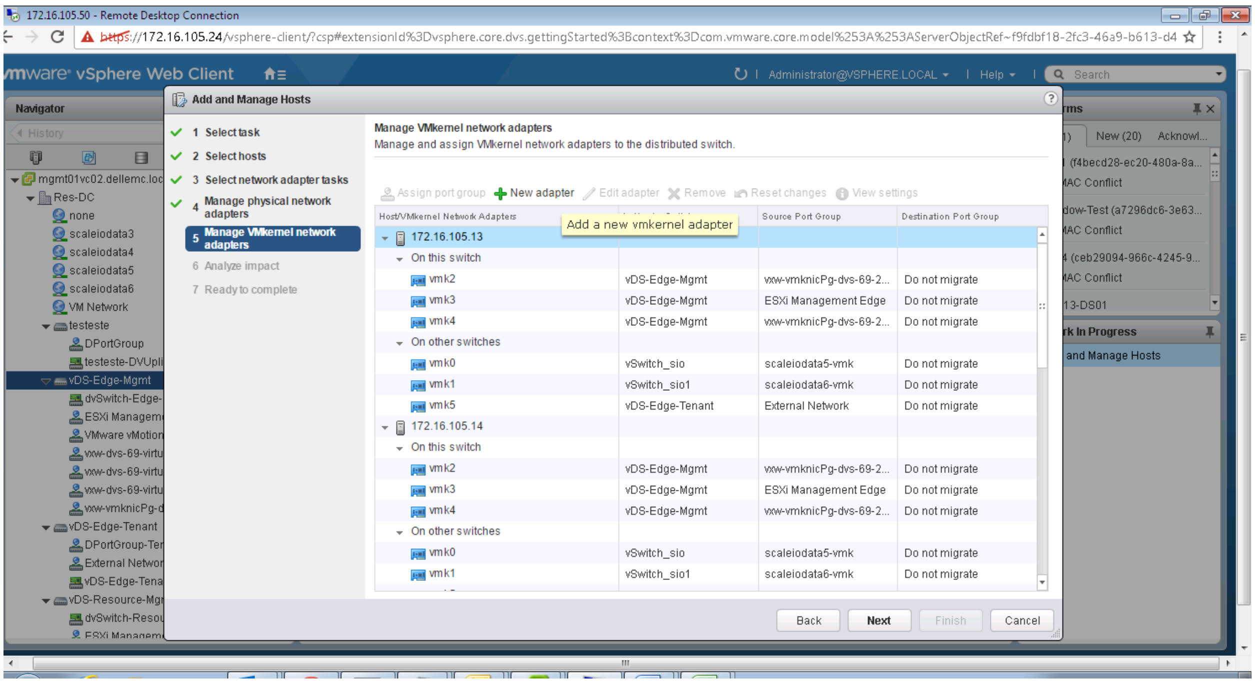
Uplink	Assigned Adapter
dvUplink1	--
dvUplink2	--
▼ lag1 ports	
lag1-0	vmnic6
lag1-1	vmnic11
(Auto-assign)	

OK Cancel

Back Next Finish Cancel

Figure 46 Select Uplink

Add a new adapter.



Add and Manage Hosts

1 Select task
2 Select hosts
3 Select network adapter tasks
4 Manage physical network adapters
5 Manage VMkernel network adapters
6 Analyze impact
7 Ready to complete

Manage VMkernel network adapters

Manage and assign VMkernel network adapters to the distributed switch.

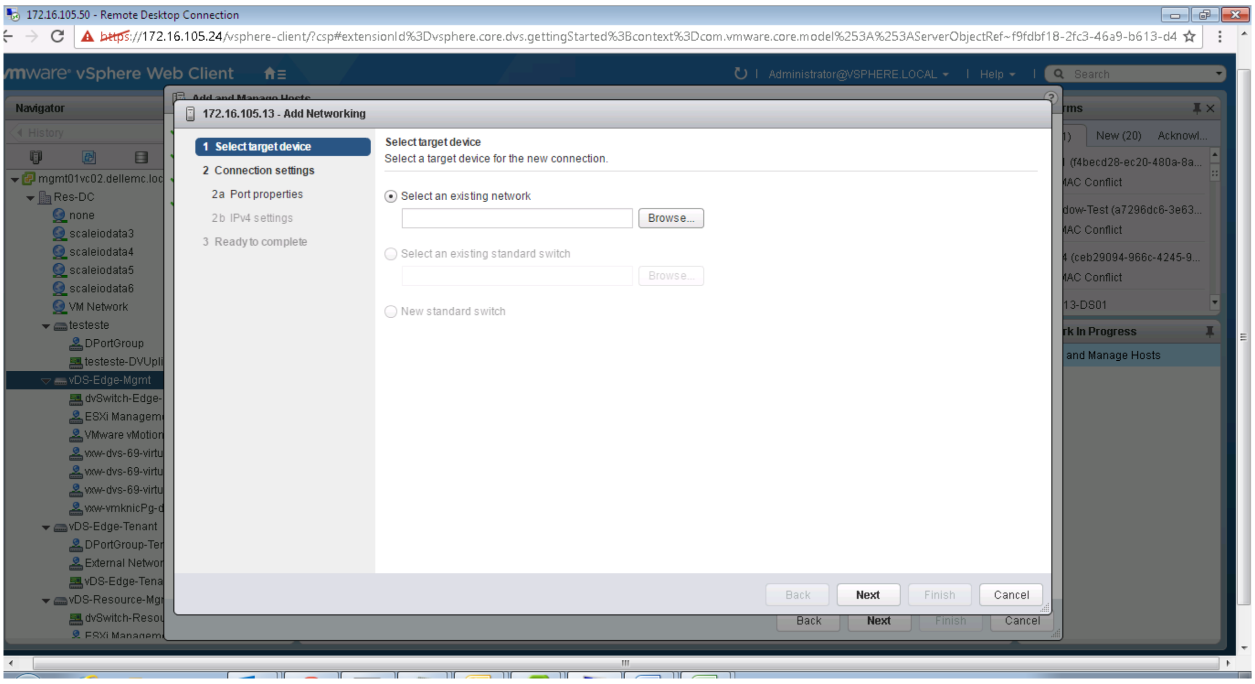
Assign port group | New adapter | Edit adapter | Remove | Reset changes | View settings

Add a new vmkernel adapter

Host/VMkernel Network Adapters		Source Port Group	Destination Port Group
172.16.105.13			
On this switch			
vmk2	vDS-Edge-Mgmt	vxw-vmknicPg-dvs-69-2...	Do not migrate
vmk3	vDS-Edge-Mgmt	ESXi Management Edge	Do not migrate
vmk4	vDS-Edge-Mgmt	vxw-vmknicPg-dvs-69-2...	Do not migrate
On other switches			
vmk0	vSwitch_sio	scaleiodata5-vmk	Do not migrate
vmk1	vSwitch_sio1	scaleiodata6-vmk	Do not migrate
vmk5	vDS-Edge-Tenant	External Network	Do not migrate
172.16.105.14			
On this switch			
vmk2	vDS-Edge-Mgmt	vxw-vmknicPg-dvs-69-2...	Do not migrate
vmk3	vDS-Edge-Mgmt	ESXi Management Edge	Do not migrate
vmk4	vDS-Edge-Mgmt	vxw-vmknicPg-dvs-69-2...	Do not migrate
On other switches			
vmk0	vSwitch_sio	scaleiodata5-vmk	Do not migrate
vmk1	vSwitch_sio1	scaleiodata6-vmk	Do not migrate

Back Next Finish Cancel

Figure 47 Add a new adapter



Select target device
Select a target device for the new connection.

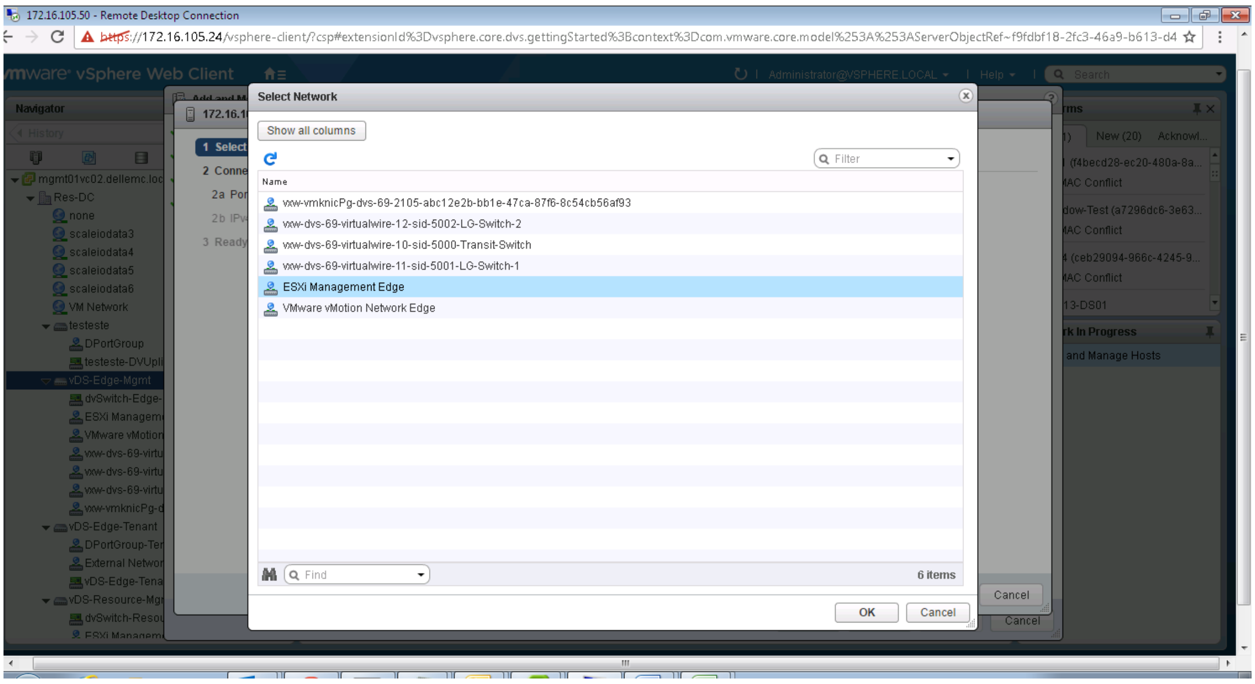
● Select an existing network

○ Select an existing standard switch

○ New standard switch

Figure 48 Select an existing network

Select the network by clicking **Browse**, the portgroup that was modified earlier should be listed.

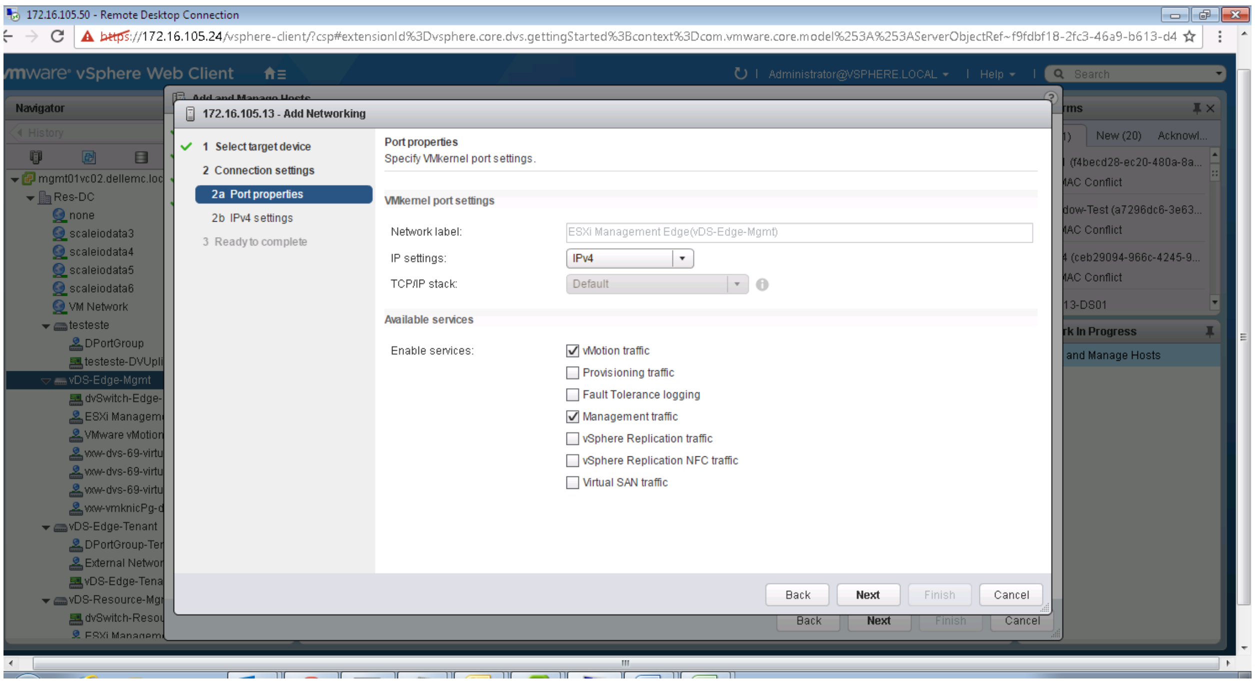

172.16.105.50 - Remote Desktop Connection
vmware vSphere Web Client
Select Network
Show all columns
Filter
Name
Find
OK
Cancel

Name
vxw-vmknicPg-dvs-69-2105-abc12e2b-bb1e-47ca-87f6-8c54cb56af93
vxw-dvs-69-virtualwire-12-sid-5002-LG-Switch-2
vxw-dvs-69-virtualwire-10-sid-5000-Transit-Switch
vxw-dvs-69-virtualwire-11-sid-5001-LG-Switch-1
ESXi Management Edge
VMware vMotion Network Edge

6 items

Figure 49 Select Network

Select the port group, click **OK** then click **Next**. Select vmotion and management traffic.


172.16.105.13 - Add Networking

- ✓ 1 Select target device
- 2 Connection settings
- 2a Port properties
- 2b IPv4 settings
- 3 Ready to complete

Port properties
Specify VMkernel port settings.

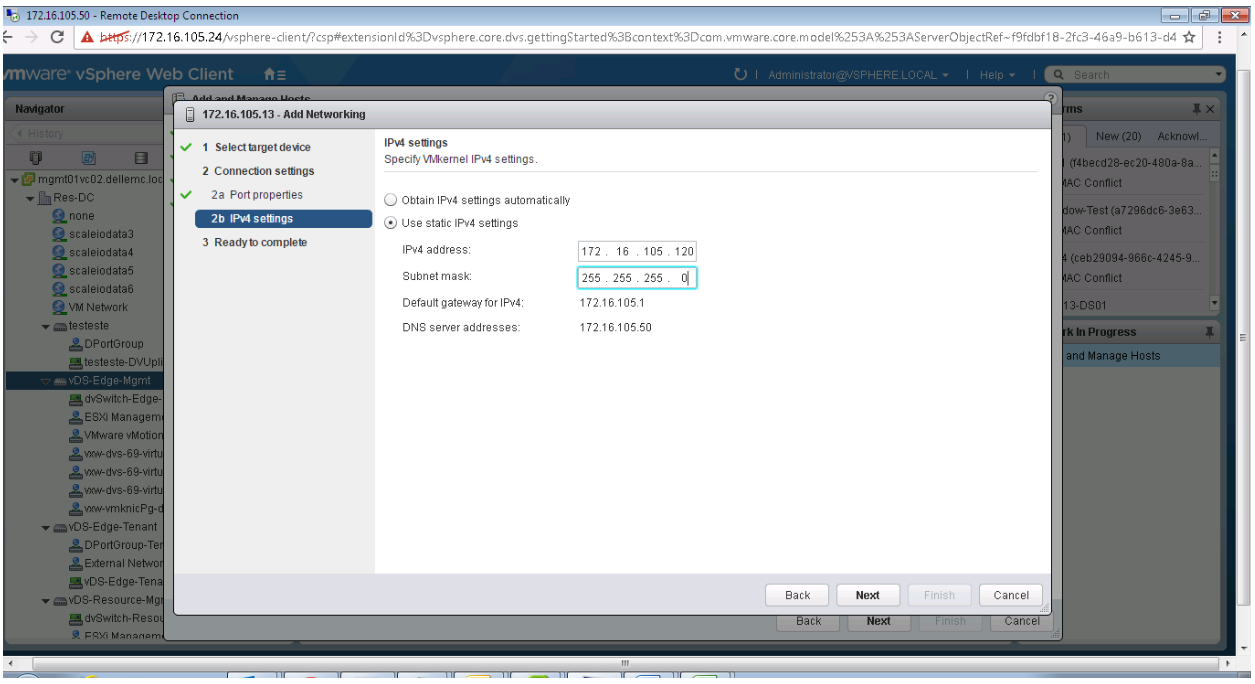
VMkernel port settings

Network label: ESXi Management Edge(vDS-Edge-Mgmt)
IP settings: IPv4
TCP/IP stack: Default

Available services

Enable services:
☑ vMotion traffic
□ Provisioning traffic
□ Fault Tolerance logging
☑ Management traffic
□ vSphere Replication traffic
□ vSphere Replication NFC traffic
□ Virtual SAN traffic

Figure 50 Port properties


172.16.105.13 - Add Networking

- ✓ 1 Select target device
- 2 Connection settings
- ✓ 2a Port properties
- 2b IPv4 settings
- 3 Ready to complete

IPv4 settings
Specify VMkernel IPv4 settings.

○ Obtain IPv4 settings automatically
● Use static IPv4 settings

IPv4 address: 172 . 16 . 105 . 120
Subnet mask: 255 . 255 . 255 . 0
Default gateway for IPv4: 172.16.105.1
DNS server addresses: 172.16.105.50

Figure 51 IPv4 settings

Provide an available IP address from your IP list, click **Next** and click **Finish** to complete the configuration. The IP address in the preceding figure is for reference, please use the IP from your IP list.

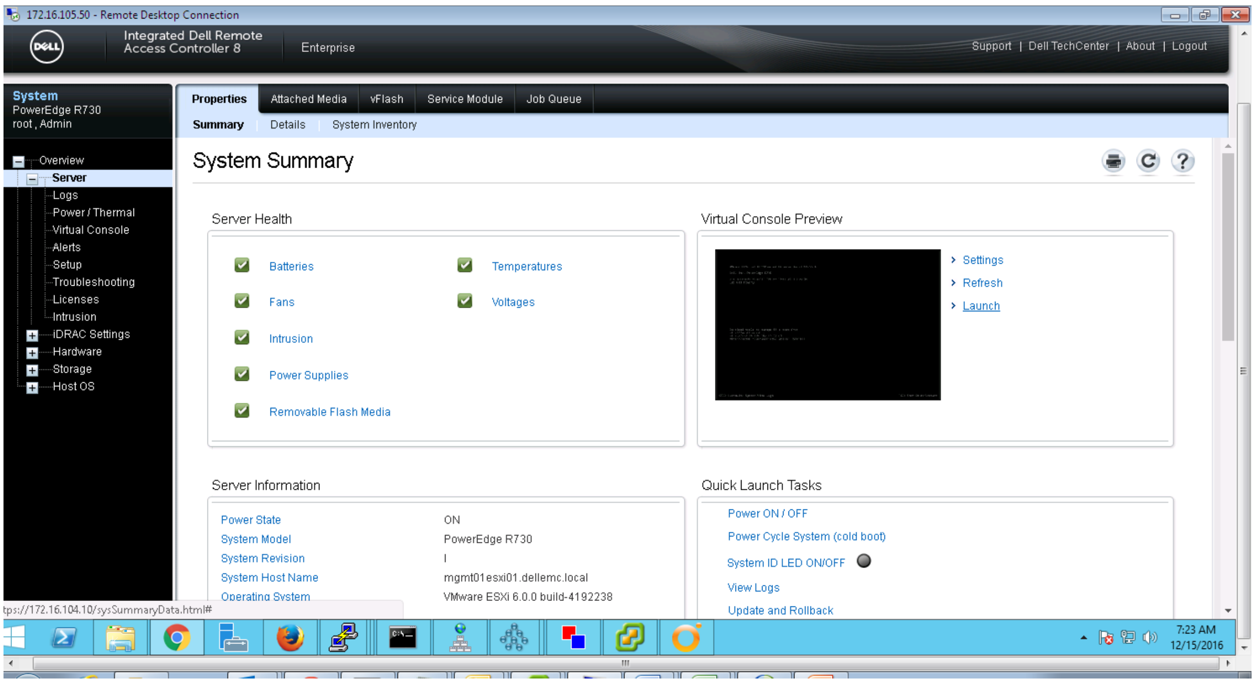
The VDS switch configuration is complete. Later migrate all the VMs to this new switch.

6.9.1.2 VDS Migration

Ensure the IP provided in the preceding figure can be pinged (172.16.105.120).

Login using the vSphere client using the IP address from the previous step. Once logged in click the configuration tab. The vSphere standard switch and vSphere distributed switch should be listed. Navigate to the vSphere standard switch and click **Remove** to remove this switch. Close vSphere client. Through the browser, access the iDRAC of the ESXI host on which the ports were configured.

Launch the ESXI host from the iDRAC browser using Launch option.



System Summary

Server Health

- ✓ Batteries
- ✓ Temperatures
- ✓ Fans
- ✓ Voltages
- ✓ Intrusion
- ✓ Power Supplies
- ✓ Removable Flash Media

Virtual Console Preview

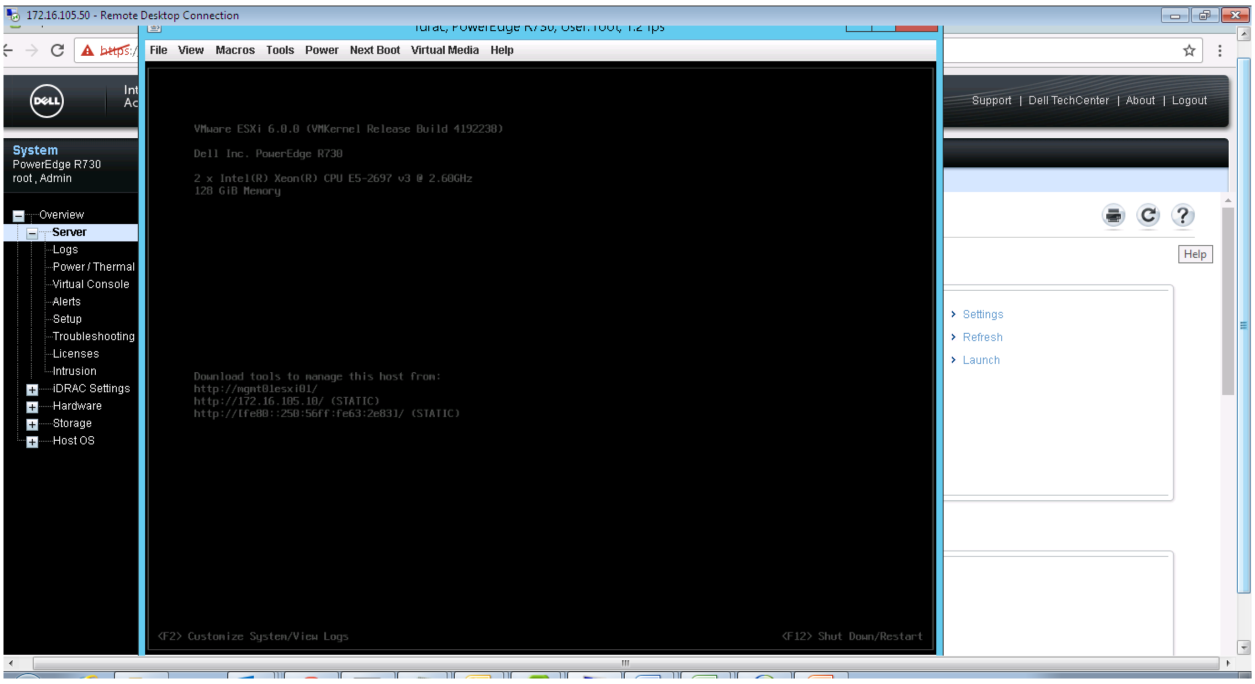
Server Information

Power State	ON
System Model	PowerEdge R730
System Revision	I
System Host Name	mgmt01esxi01.dellemc.local
Operating System	VMware ESXi 6.0.0 build-4192238

Quick Launch Tasks

- Power ON / OFF
- Power Cycle System (cold boot)
- System ID LED ON/OFF ●
- View Logs
- Update and Rollback

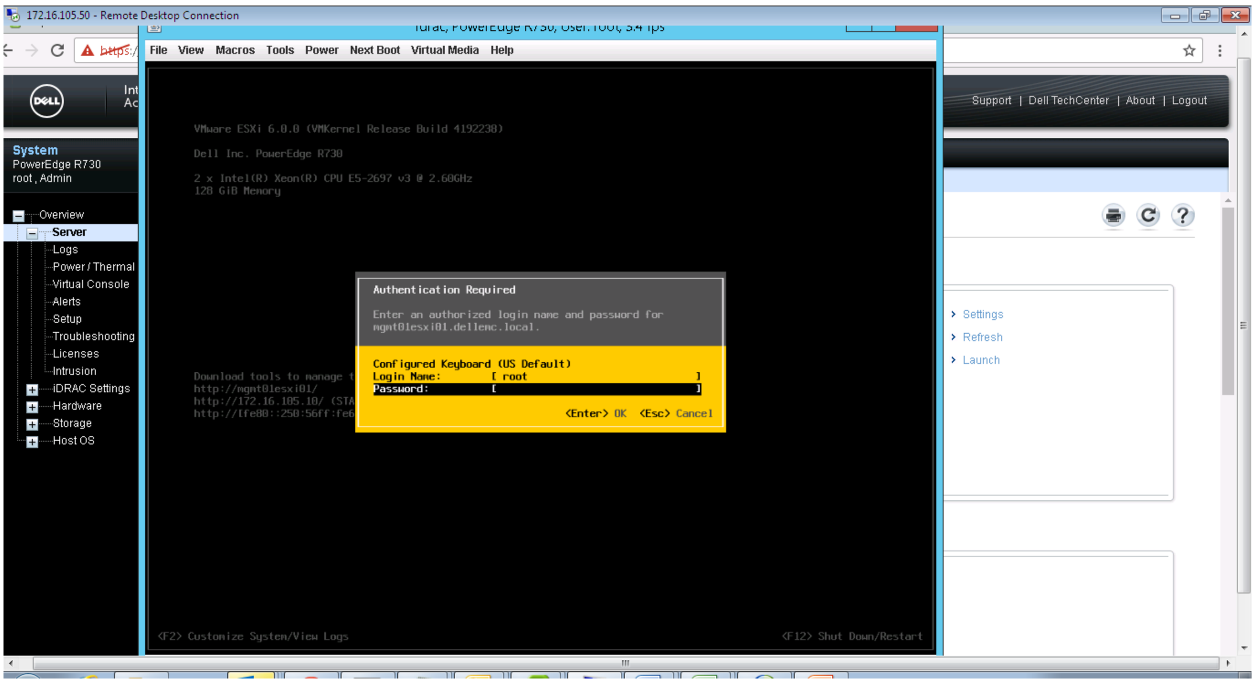
Figure 52 System summary



```
VMware ESXi 6.0.0 (VMKernel Release Build 4192238)

Dell Inc. PowerEdge R730

2 x Intel(R) Xeon(R) CPU E5-2697 v3 @ 2.60GHz
128 GiB Memory


Download tools to manage this host from:
http://mgmt01esxi01/
http://172.16.105.10/ (STATIC)
http://[fe80::250:56ff:fe63:2e83]/ (STATIC)

<F2> Customize System/View Logs                    <F12> Shut Down/Restart
```

Figure 53 iDRAC browser

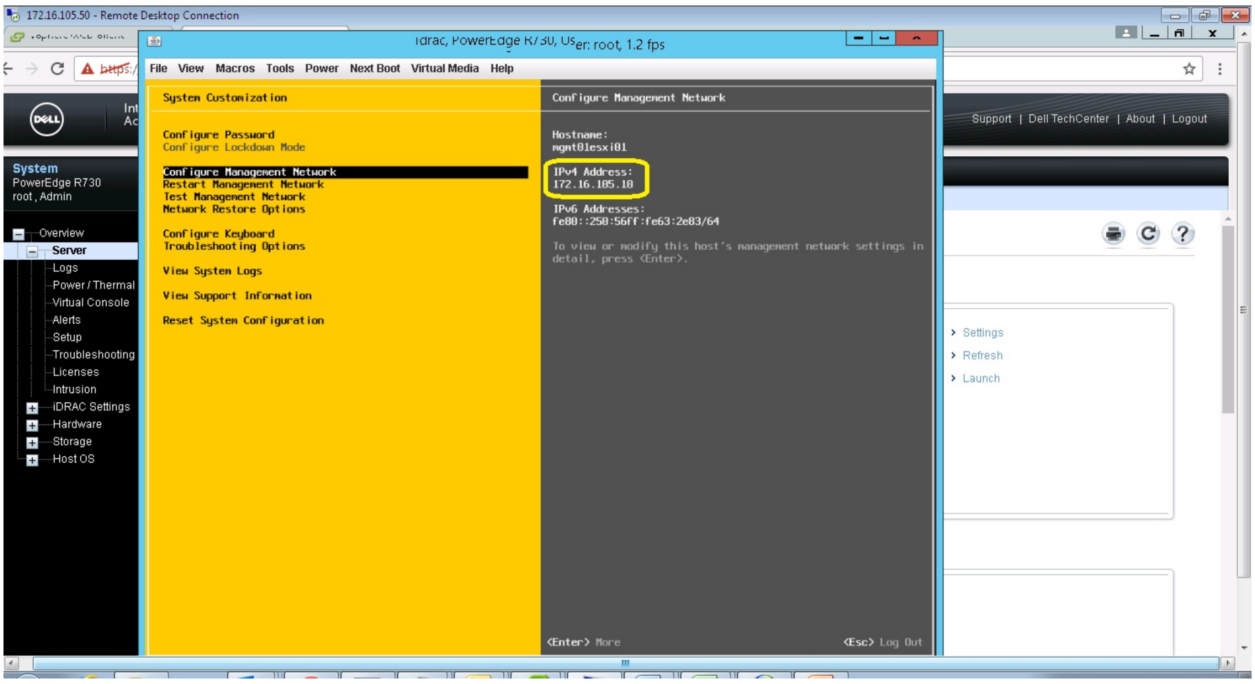
Click F2.



```
Authentication Required

Enter an authorized login name and password for
mgmt01esxi01.dellemc.local.

Configured Keyboard (US Default)
Login Name:          [ root                              ]
Password:            [                                   ]

                                   <Enter> OK  <Esc> Cancel
```

Figure 54 Authentication Required

Enter the password for root. The new IP should be listed as the IPV4 address as shown below. Change the IP address of this host to original IP address of the host.


172.16.105.50 - Remote Desktop Connection
Idrac, PowerEdge R730, User: root, 1.2 fps
File View Macros Tools Power Next Boot Virtual Media Help
System
PowerEdge R730
root , Admin
Overview
Server
Logs
Power / Thermal
Virtual Console
Alerts
Setup
Troubleshooting
Licenses
Intrusion
iDRAC Settings
Hardware
Storage
Host OS
Support | Dell TechCenter | About | Logout
Settings
Refresh
Launch

```
System Customization                    Configure Management Network

Configure Password                      Hostname:
Configure Lockdown Mode                 mgnt01esxi01

Configure Management Network            IPv4 Address:
Restart Management Network              172.16.105.10
Test Management Network
Network Restore Options                 IPv6 Addresses:
                                        fe80::250:56ff:fe63:2e83/64
Configure Keyboard
Troubleshooting Options                 To view or modify this host's management network settings in
                                        detail, press <Enter>.
View System Logs

View Support Information

Reset System Configuration

                                        <Enter> More                    <Esc> Log Out
```

Figure 55 IPv4 Address

This completes the migration. If necessary, login to this host using the vSphere client and manually move the VMs from the VSS to VDS.

7 ScaleIO Installation and Configuration

7.1 Install Dell EMC ScaleIO

To install ScaleIO on ESXi the following is required:

- A Windows host (for PowerCLI)
- PowerCLI
- Java 1.8
- The ScaleIO software
- Three vSwitch port groups

7.1.1 Register and Install ScaleIO Plugin

Download the latest ScaleIO version for VMware. In this solution, Version: **v.2.0.0.3** is used.

Download and install VMware vSphere PowerCLI in the webserver or host where the ScaleIO plugin is downloaded.

Extract the contents of downloaded ScaleIO software zip file (ScaleIO_VMware_v2.0.zip).

Using PowerCLI for VMware set to Run as Administrator, run the following command:

```
Set-ExecutionPolicy AllSigned
```

```
Run the script: ScaleIOPluginSetup-2.0-7536.0.ps1
```

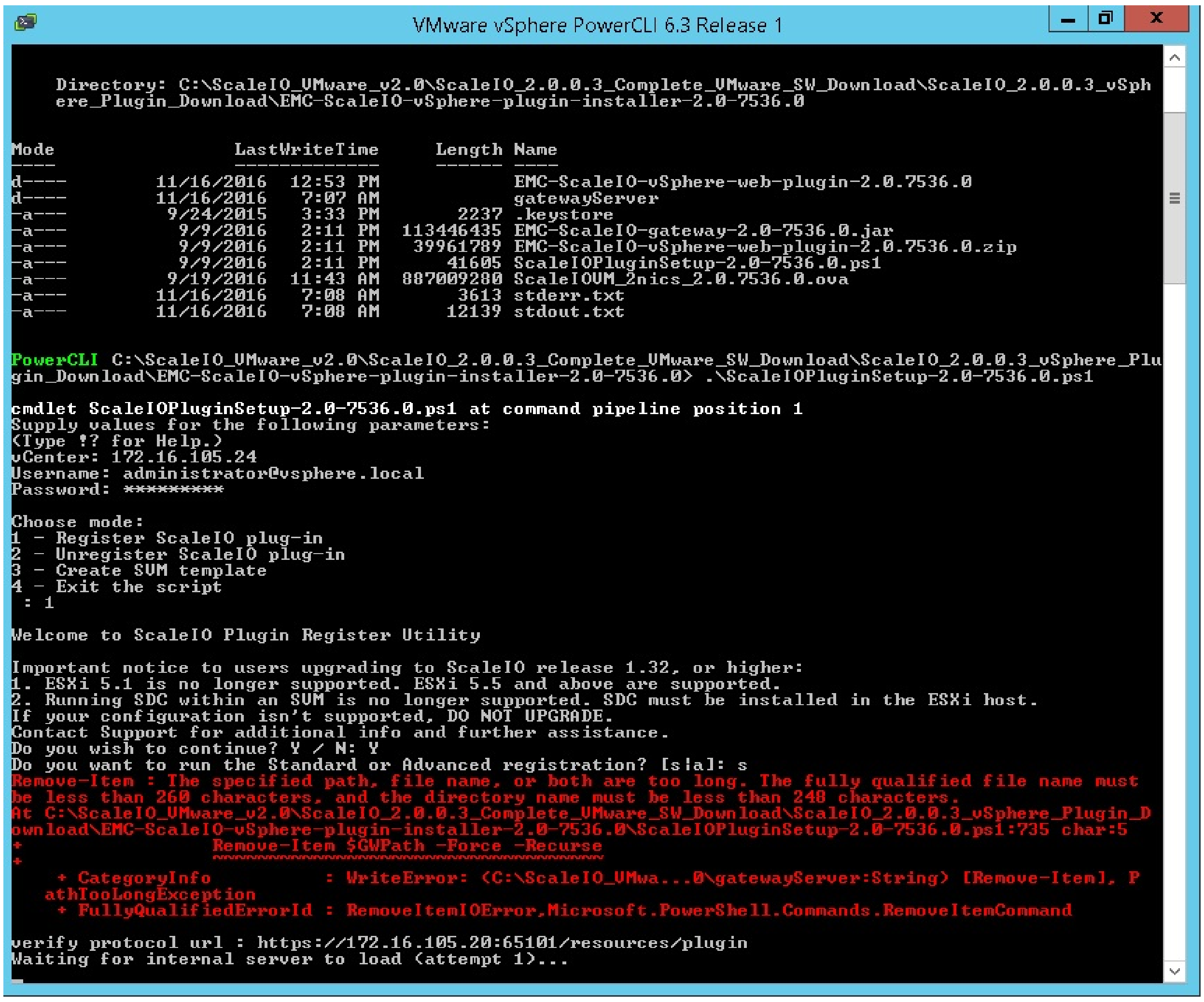
```
PowerCLI
C:\ScaleIO_VMware_v2.0\ScaleIO_2.0.0.3_Complete_VMware_SW_Download\Scal

eIO_2.0.0.3_vSphere_Plugin_Download\EMC-ScaleIO-vSphere-plugin-installer-
2.0-753

6.0> .\ScaleIOPluginSetup-2.0-7536.0.ps1
```

Enter the vCenter address, username and password. When prompted:

Choose **1**

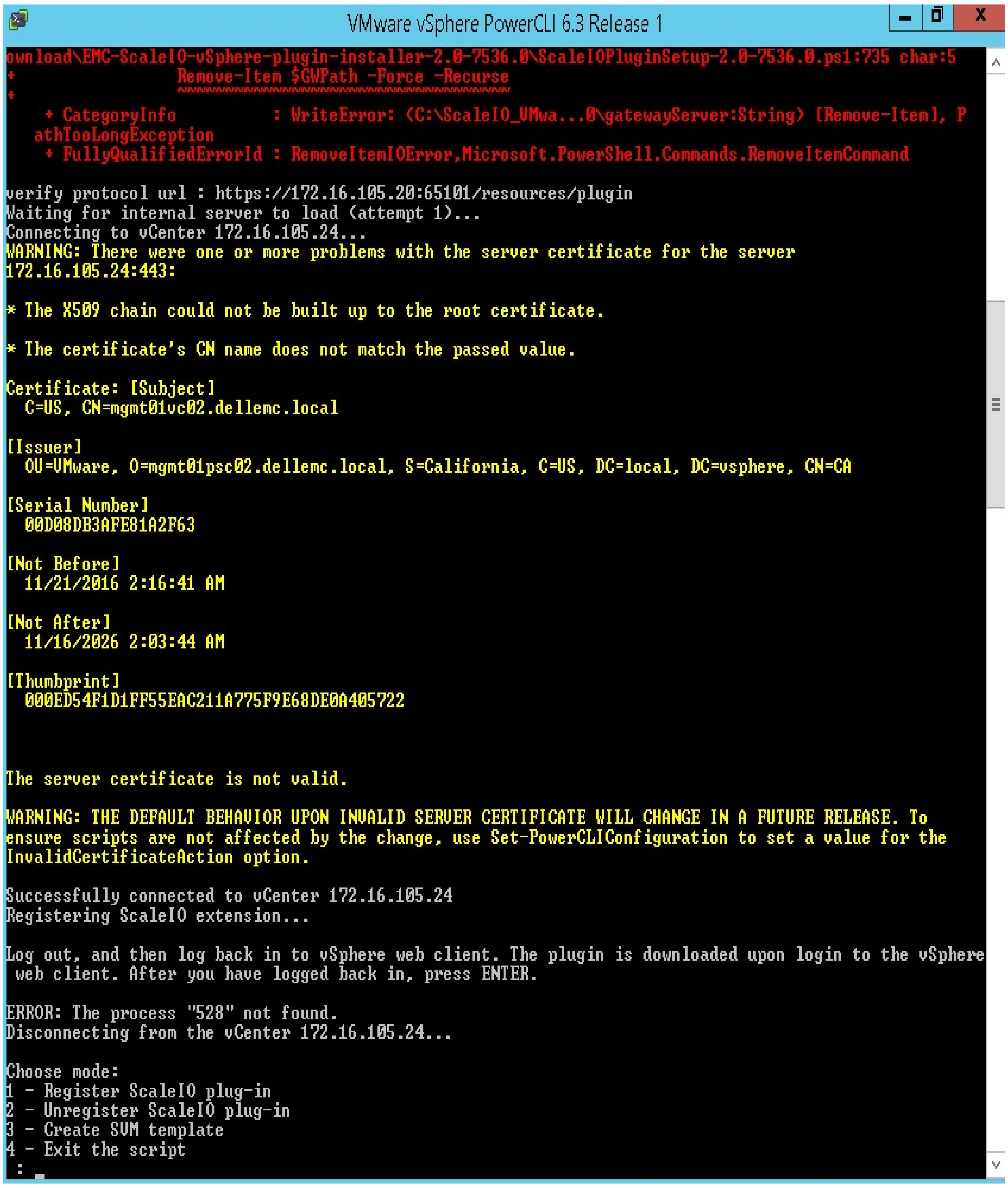
Type **Y**

Chose **S** (standard)



```
    Directory: C:\ScaleIO_VMware_v2.0\ScaleIO_2.0.0.3_Complete_VMware_SW_Download\ScaleIO_2.0.0.3_vSph
    ere_Plugin_Download\EMC-ScaleIO-vSphere-plugin-installer-2.0-7536.0


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----        11/16/2016  12:53 PM            EMC-ScaleIO-vSphere-web-plugin-2.0.7536.0
d----        11/16/2016   7:07 AM            gatewayServer
-a---         9/24/2015   3:33 PM       2237 .keystore
-a---          9/9/2016   2:11 PM  113446435 EMC-ScaleIO-gateway-2.0-7536.0.jar
-a---          9/9/2016   2:11 PM   39961789 EMC-ScaleIO-vSphere-web-plugin-2.0.7536.0.zip
-a---          9/9/2016   2:11 PM      41605 ScaleIOPluginSetup-2.0-7536.0.ps1
-a---         9/19/2016  11:43 AM  887009280 ScaleIOVM_2nics_2.0.7536.0.ova
-a---        11/16/2016   7:08 AM       3613 stderr.txt
-a---        11/16/2016   7:08 AM      12139 stdout.txt


PowerCLI C:\ScaleIO_VMware_v2.0\ScaleIO_2.0.0.3_Complete_VMware_SW_Download\ScaleIO_2.0.0.3_vSphere_Plu
gin_Download\EMC-ScaleIO-vSphere-plugin-installer-2.0-7536.0> .\ScaleIOPluginSetup-2.0-7536.0.ps1

cmdlet ScaleIOPluginSetup-2.0-7536.0.ps1 at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
vCenter: 172.16.105.24
Username: administrator@vsphere.local
Password: *********

Choose mode:
1 - Register ScaleIO plug-in
2 - Unregister ScaleIO plug-in
3 - Create SVM template
4 - Exit the script
 : 1

Welcome to ScaleIO Plugin Register Utility

Important notice to users upgrading to ScaleIO release 1.32, or higher:
1. ESXi 5.1 is no longer supported. ESXi 5.5 and above are supported.
2. Running SDC within an SVM is no longer supported. SDC must be installed in the ESXi host.
If your configuration isn't supported, DO NOT UPGRADE.
Contact Support for additional info and further assistance.
Do you wish to continue? Y / N: Y
Do you want to run the Standard or Advanced registration? [s|a]: s
Remove-Item : The specified path, file name, or both are too long. The fully qualified file name must
be less than 260 characters, and the directory name must be less than 248 characters.
At C:\ScaleIO_VMware_v2.0\ScaleIO_2.0.0.3_Complete_VMware_SW_Download\ScaleIO_2.0.0.3_vSphere_Plugin_D
ownload\EMC-ScaleIO-vSphere-plugin-installer-2.0-7536.0\ScaleIOPluginSetup-2.0-7536.0.ps1:735 char:5
+                  Remove-Item $GWPath -Force -Recurse
+                  ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : WriteError: (C:\ScaleIO_VMwa...0\gatewayServer:String) [Remove-Item], P
   athTooLongException
    + FullyQualifiedErrorId : RemoveItemIOError,Microsoft.PowerShell.Commands.RemoveItemCommand

verify protocol url : https://172.16.105.20:65101/resources/plugin
Waiting for internal server to load (attempt 1)...
_
```

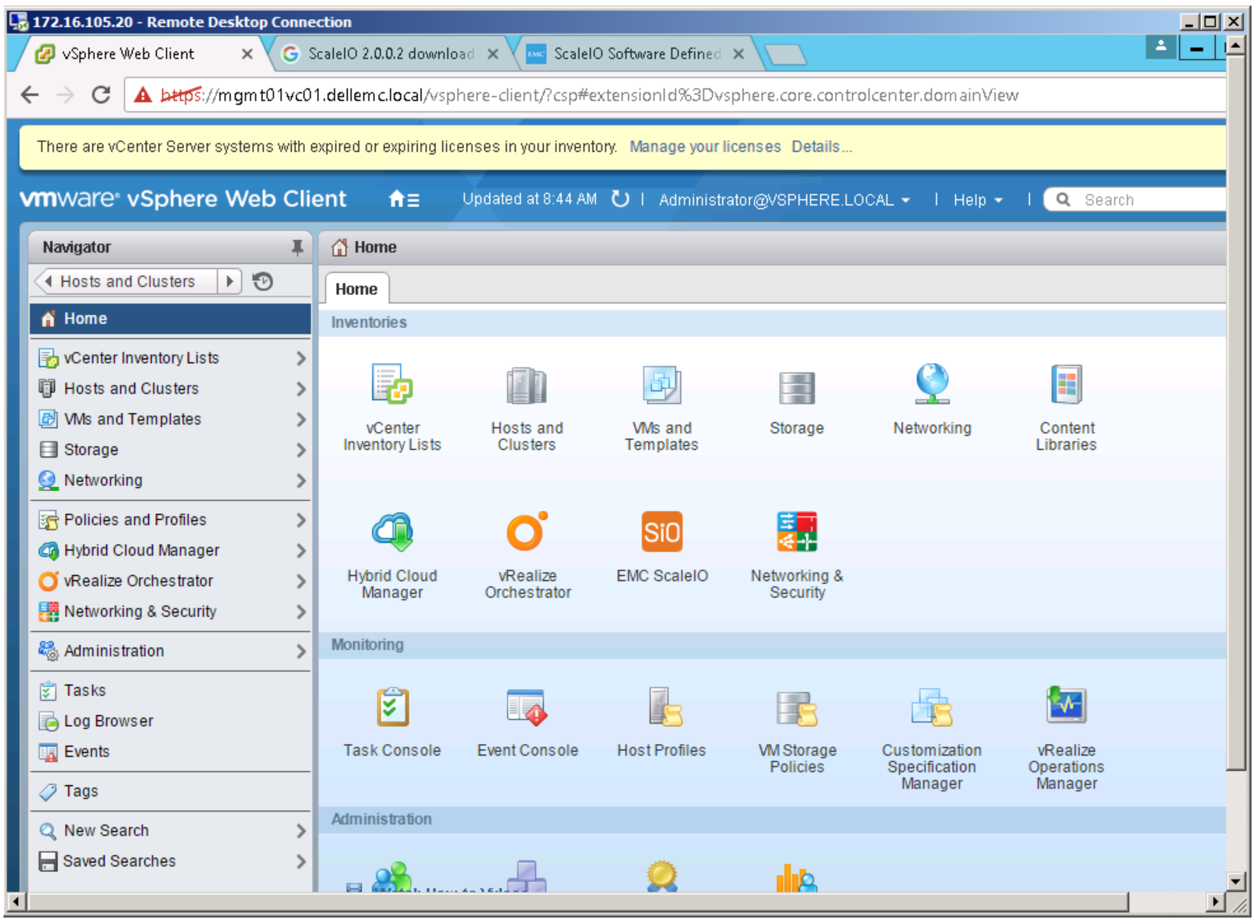
Figure 56 Run Script - ScaleIOPluginSetup-2.0-7536.0.ps1



```
ownload\EMC-ScaleIO-vSphere-plugin-installer-2.0-7536.0\ScaleIOPluginSetup-2.0-7536.0.ps1:735 char:5
+                 Remove-Item $GWPath -Force -Recurse
                  ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+
    + CategoryInfo          : WriteError: (C:\ScaleIO_VMwa...0\gatewayServer:String) [Remove-Item], P
   athTooLongException
    + FullyQualifiedErrorId : RemoveItemIOError,Microsoft.PowerShell.Commands.RemoveItemCommand

verify protocol url : https://172.16.105.20:65101/resources/plugin
Waiting for internal server to load (attempt 1)...
Connecting to vCenter 172.16.105.24...
WARNING: There were one or more problems with the server certificate for the server
172.16.105.24:443:

* The X509 chain could not be built up to the root certificate.

* The certificate's CN name does not match the passed value.

Certificate: [Subject]
  C=US, CN=mgmt01vc02.dellemc.local

[Issuer]
  OU=VMware, O=mgmt01psc02.dellemc.local, S=California, C=US, DC=local, DC=vsphere, CN=CA

[Serial Number]
  00D08DB3AFE81A2F63

[Not Before]
  11/21/2016 2:16:41 AM

[Not After]
  11/16/2026 2:03:44 AM

[Thumbprint]
  000ED54F1D1FF55EAC211A775F9E68DE0A405722



The server certificate is not valid.

WARNING: THE DEFAULT BEHAVIOR UPON INVALID SERVER CERTIFICATE WILL CHANGE IN A FUTURE RELEASE. To
ensure scripts are not affected by the change, use Set-PowerCLIConfiguration to set a value for the
InvalidCertificateAction option.

Successfully connected to vCenter 172.16.105.24
Registering ScaleIO extension...

Log out, and then log back in to vSphere web client. The plugin is downloaded upon login to the vSphere
 web client. After you have logged back in, press ENTER.

ERROR: The process "528" not found.
Disconnecting from the vCenter 172.16.105.24...

Choose mode:
1 - Register ScaleIO plug-in
2 - Unregister ScaleIO plug-in
3 - Create SVM template
4 - Exit the script
 : _
```

Figure 57 Run Script - ScaleIOPluginSetup-2.0-7536.0.ps1

Close any browser accessing the vCenter Web Client, and then reopen it. The plugin should be registered.



~~https~~://mgmt01vc01.dellemc.local/vsphere-client/?csp#extensionId%3Dvsphere.core.controlcenter.domainView

There are vCenter Server systems with expired or expiring licenses in your inventory. Manage your licenses Details...

Figure 58 vCenter Web Client

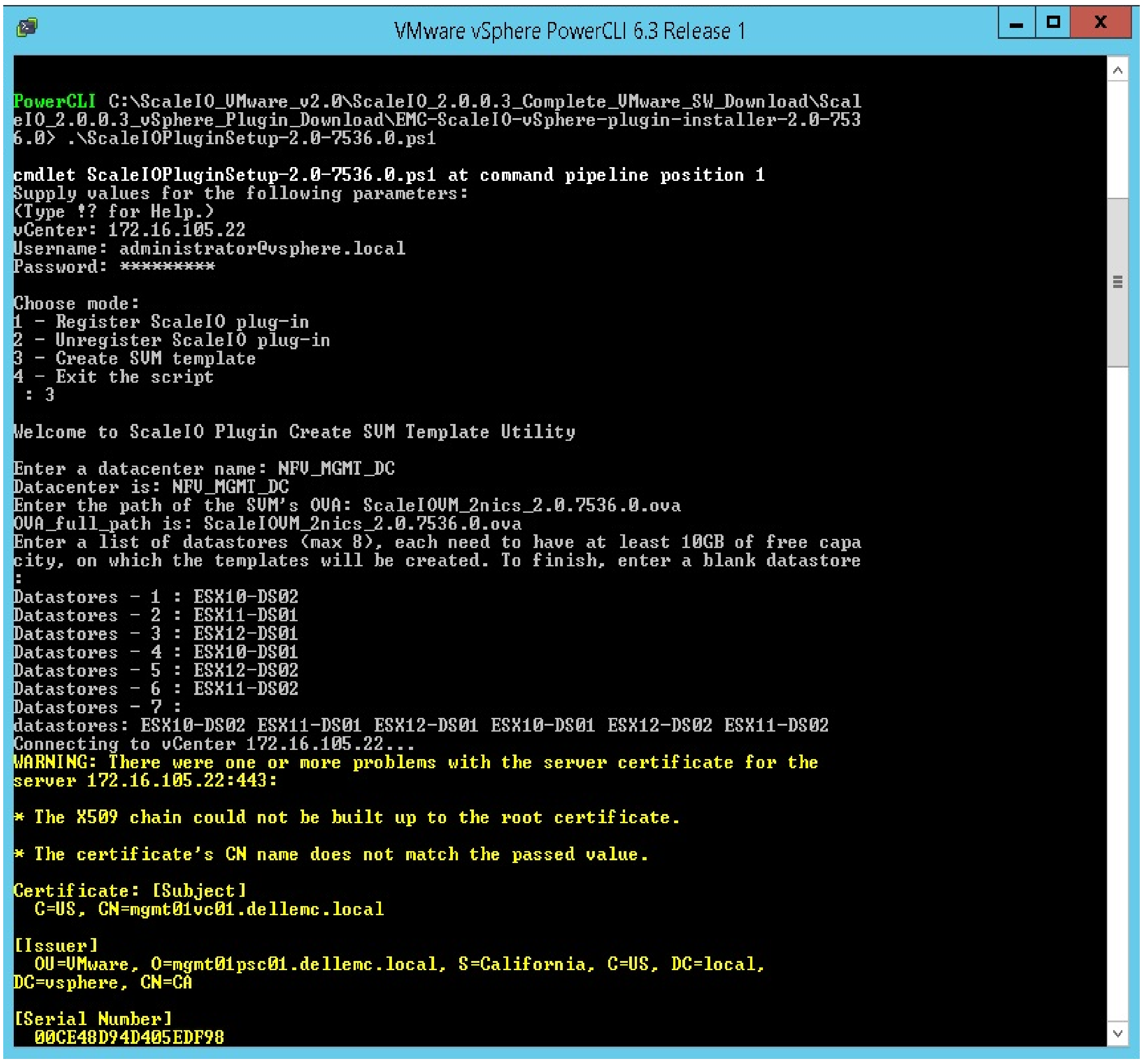
At the PowerCLI prompt, press **Enter**.

7.1.2 Create a ScaleIO template

Run the .PS1 script again. Choose ***3***.

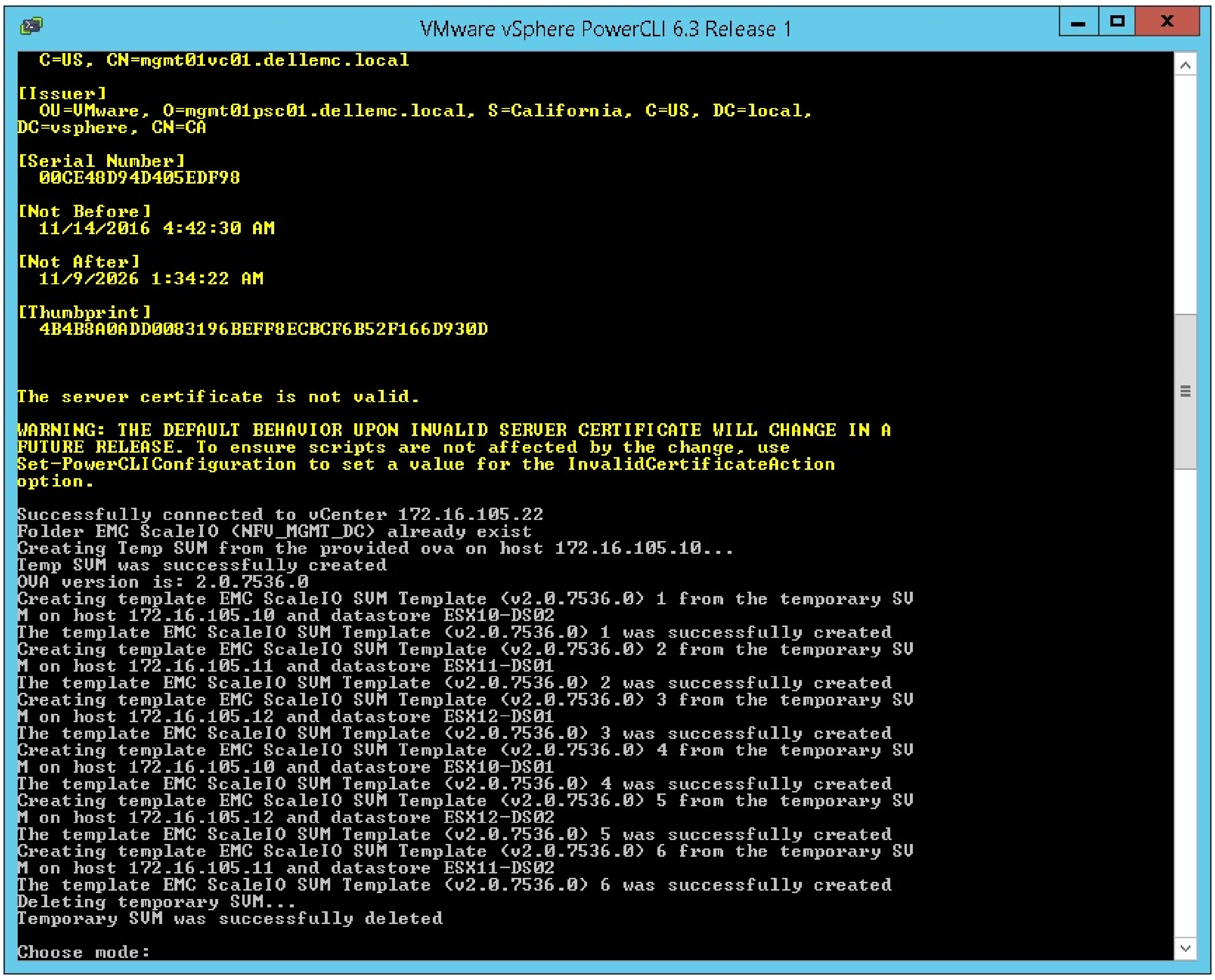
Type the name of your vCenter datacenter.

Type the path to the **ScaleIOVM_2nics_2.0.7536.0.ova** OVA file.



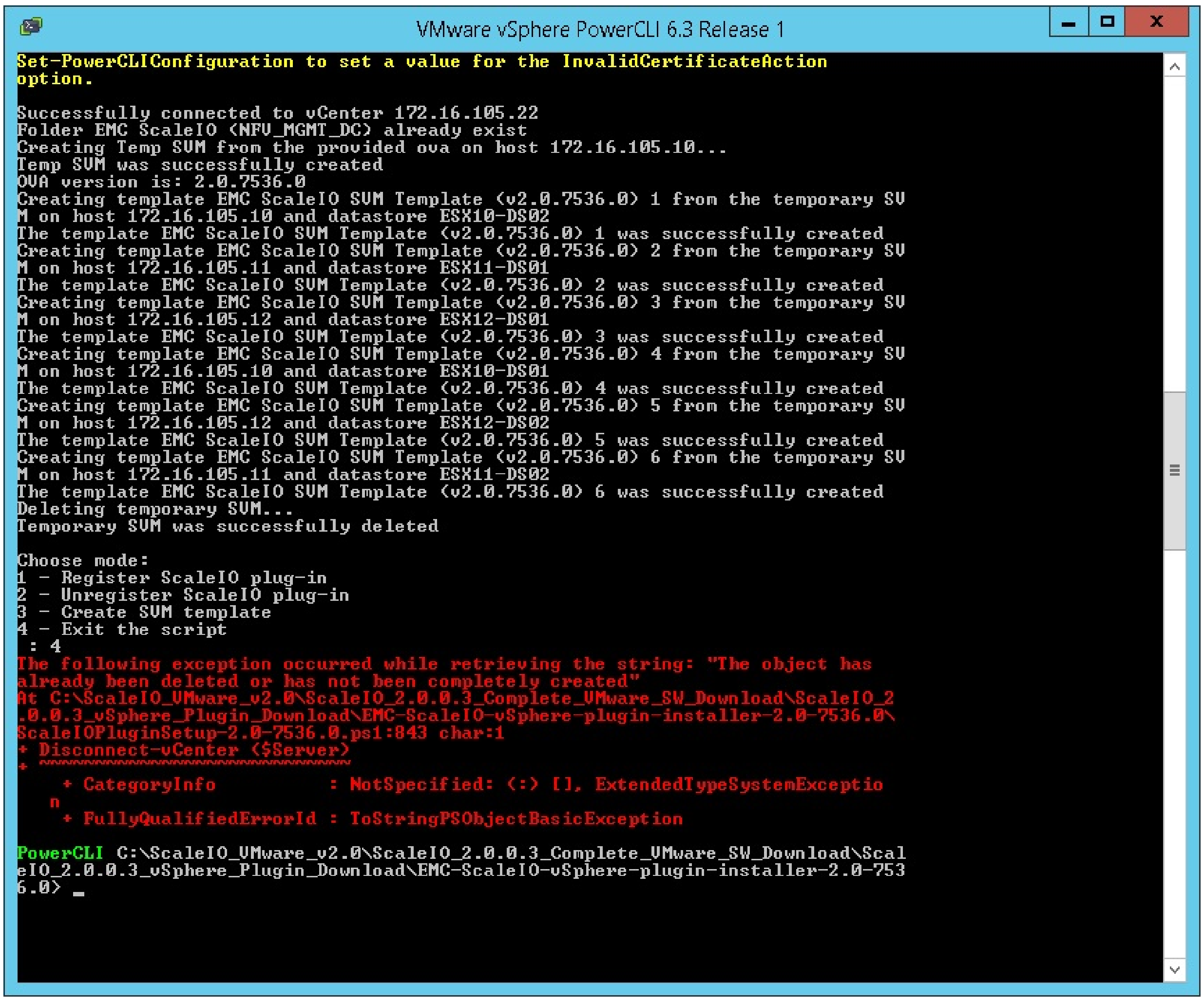
```
PowerCLI C:\ScaleIO_VMware_v2.0\ScaleIO_2.0.0.3_Complete_VMware_SW_Download\Scal
eIO_2.0.0.3_vSphere_Plugin_Download\EMC-ScaleIO-vSphere-plugin-installer-2.0-753
6.0> .\ScaleIOPluginSetup-2.0-7536.0.ps1

cmdlet ScaleIOPluginSetup-2.0-7536.0.ps1 at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
vCenter: 172.16.105.22
Username: administrator@vsphere.local
Password: *********

Choose mode:
1 - Register ScaleIO plug-in
2 - Unregister ScaleIO plug-in
3 - Create SVM template
4 - Exit the script
 : 3

Welcome to ScaleIO Plugin Create SVM Template Utility

Enter a datacenter name: NFV_MGMT_DC
Datacenter is: NFV_MGMT_DC
Enter the path of the SVM's OVA: ScaleIOVM_2nics_2.0.7536.0.ova
OVA_full_path is: ScaleIOVM_2nics_2.0.7536.0.ova
Enter a list of datastores (max 8), each need to have at least 10GB of free capa
city, on which the templates will be created. To finish, enter a blank datastore
:
Datastores - 1 : ESX10-DS02
Datastores - 2 : ESX11-DS01
Datastores - 3 : ESX12-DS01
Datastores - 4 : ESX10-DS01
Datastores - 5 : ESX12-DS02
Datastores - 6 : ESX11-DS02
Datastores - 7 :
datastores: ESX10-DS02 ESX11-DS01 ESX12-DS01 ESX10-DS01 ESX12-DS02 ESX11-DS02
Connecting to vCenter 172.16.105.22...
WARNING: There were one or more problems with the server certificate for the
server 172.16.105.22:443:

* The X509 chain could not be built up to the root certificate.

* The certificate's CN name does not match the passed value.

Certificate: [Subject]
  C=US, CN=mgmt01vc01.dellemc.local

[Issuer]
  OU=VMware, O=mgmt01psc01.dellemc.local, S=California, C=US, DC=local,
DC=vsphere, CN=CA

[Serial Number]
  00CE48D94D405EDF98
```

Figure 59 Enter datacenter name



```
  C=US, CN=mgmt01vc01.dellemc.local

[Issuer]
  OU=VMware, O=mgmt01psc01.dellemc.local, S=California, C=US, DC=local,
DC=vsphere, CN=CA

[Serial Number]
  00CE48D94D405EDF98

[Not Before]
  11/14/2016 4:42:30 AM

[Not After]
  11/9/2026 1:34:22 AM

[Thumbprint]
  4B4B8A0ADD0083196BEFF8ECBCF6B52F166D930D


The server certificate is not valid.

WARNING: THE DEFAULT BEHAVIOR UPON INVALID SERVER CERTIFICATE WILL CHANGE IN A
FUTURE RELEASE. To ensure scripts are not affected by the change, use
Set-PowerCLIConfiguration to set a value for the InvalidCertificateAction
option.

Successfully connected to vCenter 172.16.105.22
Folder EMC ScaleIO (NFV_MGMT_DC) already exist
Creating Temp SVM from the provided ova on host 172.16.105.10...
Temp SVM was successfully created
OVA version is: 2.0.7536.0
Creating template EMC ScaleIO SVM Template (v2.0.7536.0) 1 from the temporary SV
M on host 172.16.105.10 and datastore ESX10-DS02
The template EMC ScaleIO SVM Template (v2.0.7536.0) 1 was successfully created
Creating template EMC ScaleIO SVM Template (v2.0.7536.0) 2 from the temporary SV
M on host 172.16.105.11 and datastore ESX11-DS01
The template EMC ScaleIO SVM Template (v2.0.7536.0) 2 was successfully created
Creating template EMC ScaleIO SVM Template (v2.0.7536.0) 3 from the temporary SV
M on host 172.16.105.12 and datastore ESX12-DS01
The template EMC ScaleIO SVM Template (v2.0.7536.0) 3 was successfully created
Creating template EMC ScaleIO SVM Template (v2.0.7536.0) 4 from the temporary SV
M on host 172.16.105.10 and datastore ESX10-DS01
The template EMC ScaleIO SVM Template (v2.0.7536.0) 4 was successfully created
Creating template EMC ScaleIO SVM Template (v2.0.7536.0) 5 from the temporary SV
M on host 172.16.105.12 and datastore ESX12-DS02
The template EMC ScaleIO SVM Template (v2.0.7536.0) 5 was successfully created
Creating template EMC ScaleIO SVM Template (v2.0.7536.0) 6 from the temporary SV
M on host 172.16.105.11 and datastore ESX11-DS02
The template EMC ScaleIO SVM Template (v2.0.7536.0) 6 was successfully created
Deleting temporary SVM...
Temporary SVM was successfully deleted

Choose mode:
```

Figure 60 Creating ScaleIO SVM Template



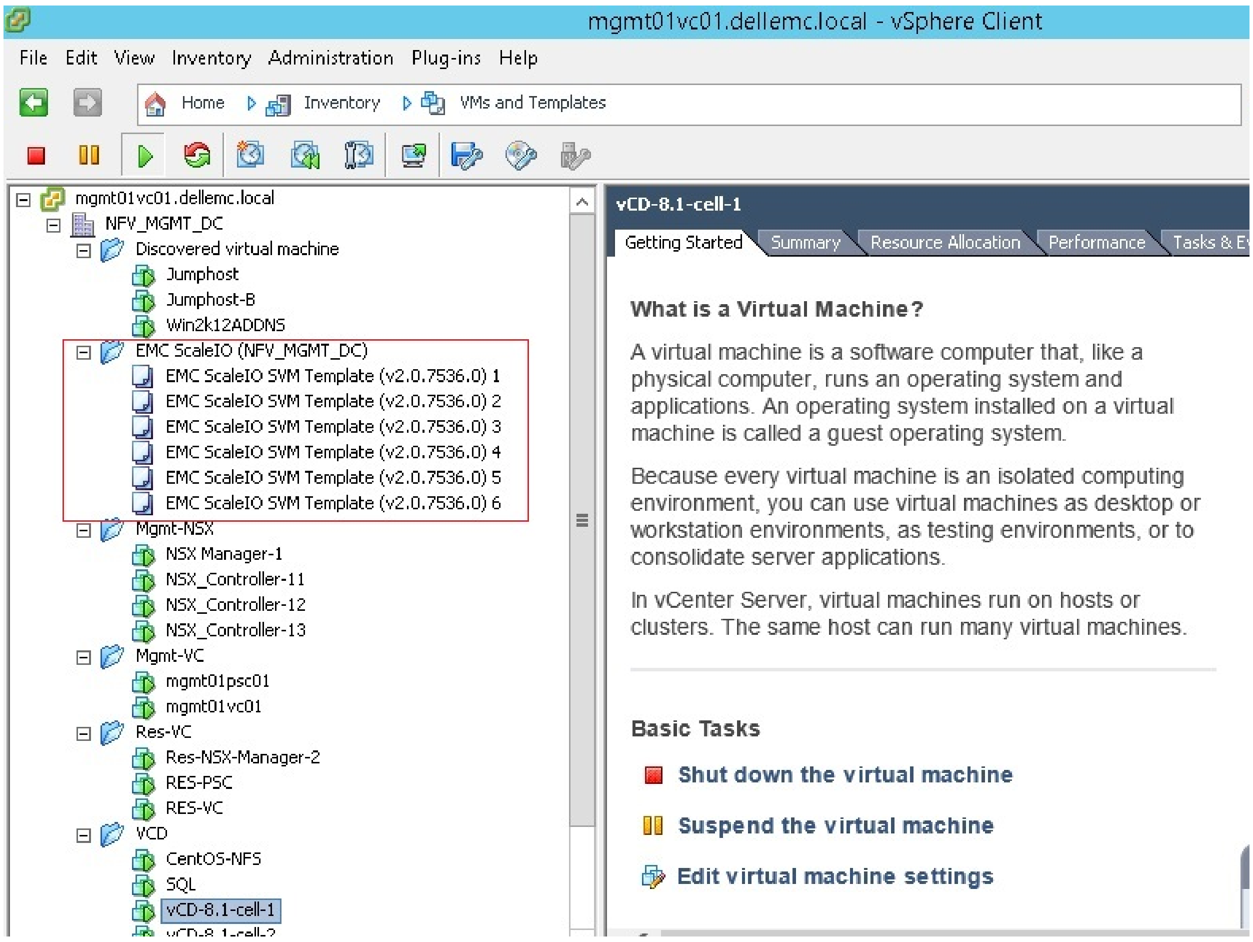
```
Set-PowerCLIConfiguration to set a value for the InvalidCertificateAction
option.

Successfully connected to vCenter 172.16.105.22
Folder EMC ScaleIO (NFV_MGMT_DC) already exist
Creating Temp SVM from the provided ova on host 172.16.105.10...
Temp SVM was successfully created
OVA version is: 2.0.7536.0
Creating template EMC ScaleIO SVM Template (v2.0.7536.0) 1 from the temporary SV
M on host 172.16.105.10 and datastore ESX10-DS02
The template EMC ScaleIO SVM Template (v2.0.7536.0) 1 was successfully created
Creating template EMC ScaleIO SVM Template (v2.0.7536.0) 2 from the temporary SV
M on host 172.16.105.11 and datastore ESX11-DS01
The template EMC ScaleIO SVM Template (v2.0.7536.0) 2 was successfully created
Creating template EMC ScaleIO SVM Template (v2.0.7536.0) 3 from the temporary SV
M on host 172.16.105.12 and datastore ESX12-DS01
The template EMC ScaleIO SVM Template (v2.0.7536.0) 3 was successfully created
Creating template EMC ScaleIO SVM Template (v2.0.7536.0) 4 from the temporary SV
M on host 172.16.105.10 and datastore ESX10-DS01
The template EMC ScaleIO SVM Template (v2.0.7536.0) 4 was successfully created
Creating template EMC ScaleIO SVM Template (v2.0.7536.0) 5 from the temporary SV
M on host 172.16.105.12 and datastore ESX12-DS02
The template EMC ScaleIO SVM Template (v2.0.7536.0) 5 was successfully created
Creating template EMC ScaleIO SVM Template (v2.0.7536.0) 6 from the temporary SV
M on host 172.16.105.11 and datastore ESX11-DS02
The template EMC ScaleIO SVM Template (v2.0.7536.0) 6 was successfully created
Deleting temporary SVM...
Temporary SVM was successfully deleted

Choose mode:
1 - Register ScaleIO plug-in
2 - Unregister ScaleIO plug-in
3 - Create SVM template
4 - Exit the script
 : 4
The following exception occurred while retrieving the string: "The object has
already been deleted or has not been completely created"
At C:\ScaleIO_VMware_v2.0\ScaleIO_2.0.0.3_Complete_VMware_SW_Download\ScaleIO_2
.0.0.3_vSphere_Plugin_Download\EMC-ScaleIO-vSphere-plugin-installer-2.0-7536.0\
ScaleIOPluginSetup-2.0-7536.0.ps1:843 char:1
+ Disconnect-vCenter ($Server)
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [], ExtendedTypeSystemExceptio
   n
    + FullyQualifiedErrorId : ToStringPSObjectBasicException

PowerCLI C:\ScaleIO_VMware_v2.0\ScaleIO_2.0.0.3_Complete_VMware_SW_Download\Scal
eIO_2.0.0.3_vSphere_Plugin_Download\EMC-ScaleIO-vSphere-plugin-installer-2.0-753
6.0> _
```

Figure 61 Register ScaleIO with vCenter

Note: In this solution, the ScaleIO template will be installed on three of the management cluster ESXi hosts. So, provide the datacenter name of each ESXi host to create a ScaleIO template.

Observe the template is created (The example shows six templates, but only four are required for each vCenter).

Management VC ScaleIO templates:



mgmt01vc01.dellemc.local
NFV_MGMT_DC
Discovered virtual machine
Jumphost
Jumphost-B
Win2k12ADDNS
EMC ScaleIO (NFV_MGMT_DC)
EMC ScaleIO SVM Template (v2.0.7536.0) 1
EMC ScaleIO SVM Template (v2.0.7536.0) 2
EMC ScaleIO SVM Template (v2.0.7536.0) 3
EMC ScaleIO SVM Template (v2.0.7536.0) 4
EMC ScaleIO SVM Template (v2.0.7536.0) 5
EMC ScaleIO SVM Template (v2.0.7536.0) 6
Mgmt-NSX
NSX Manager-1
NSX_Controller-11
NSX_Controller-12
NSX_Controller-13
Mgmt-VC
mgmt01psc01
mgmt01vc01
Res-VC
Res-NSX-Manager-2
RES-PSC
RES-VC
VCD
CentOS-NFS
SQL
vCD-8.1-cell-1

What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

In vCenter Server, virtual machines run on hosts or clusters. The same host can run many virtual machines.

Basic Tasks

Shut down the virtual machine

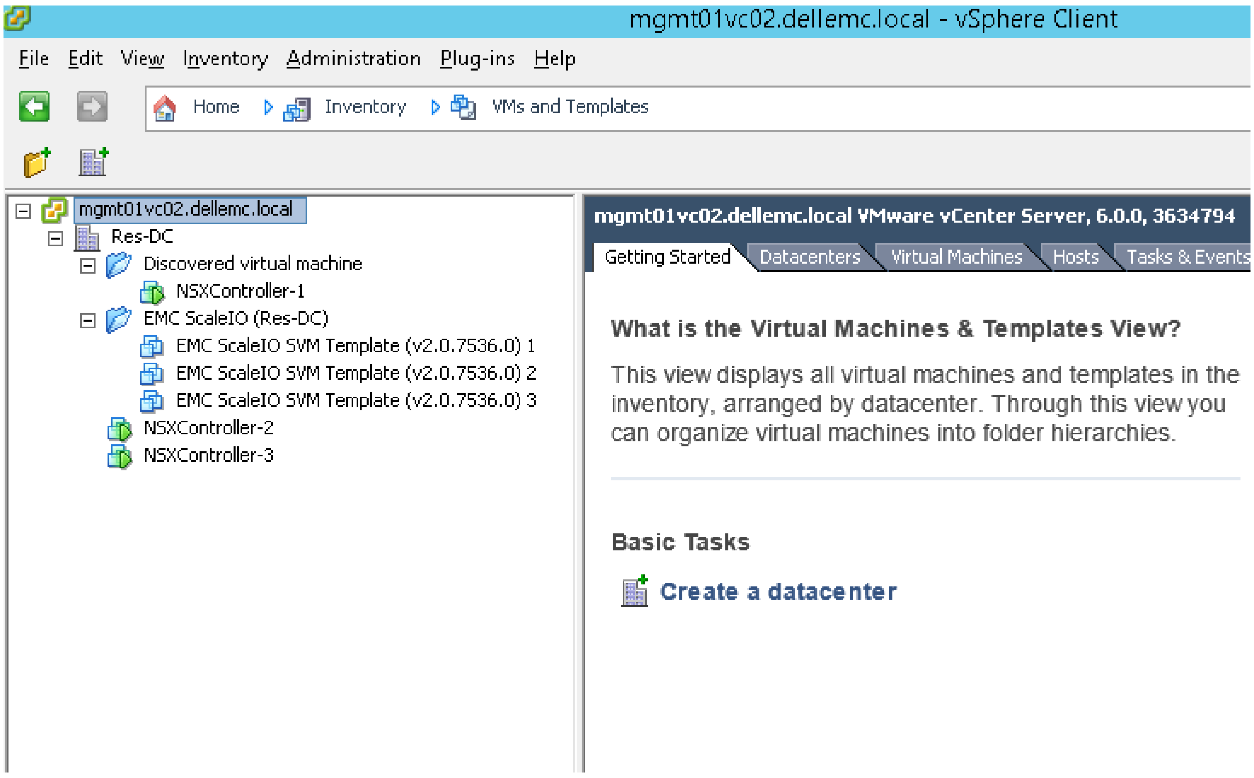
Suspend the virtual machine

Edit virtual machine settings

Figure 62 Management VC ScaleIO templates

Follow the similar procedure mentioned in Section 1.1.1 and Section 1.1.2 of ScaleIO User's Guide to register the ScaleIO plugin and create the ScaleIO template on the second vCenter Server (The Edge and Resource VC)

Resource & Edge VC ScaleIO templates:


mgmt01vc02.dellemc.local - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home
Inventory
VMs and Templates
Getting Started
Datacenters
Virtual Machines
Hosts
Tasks & Events

mgmt01vc02.dellemc.local
Res-DC
Discovered virtual machine
NSXController-1
EMC ScaleIO (Res-DC)
EMC ScaleIO SVM Template (v2.0.7536.0) 1
EMC ScaleIO SVM Template (v2.0.7536.0) 2
EMC ScaleIO SVM Template (v2.0.7536.0) 3
NSXController-2
NSXController-3

mgmt01vc02.dellemc.local VMware vCenter Server, 6.0.0, 3634794

What is the Virtual Machines & Templates View?

This view displays all virtual machines and templates in the inventory, arranged by datacenter. Through this view you can organize virtual machines into folder hierarchies.

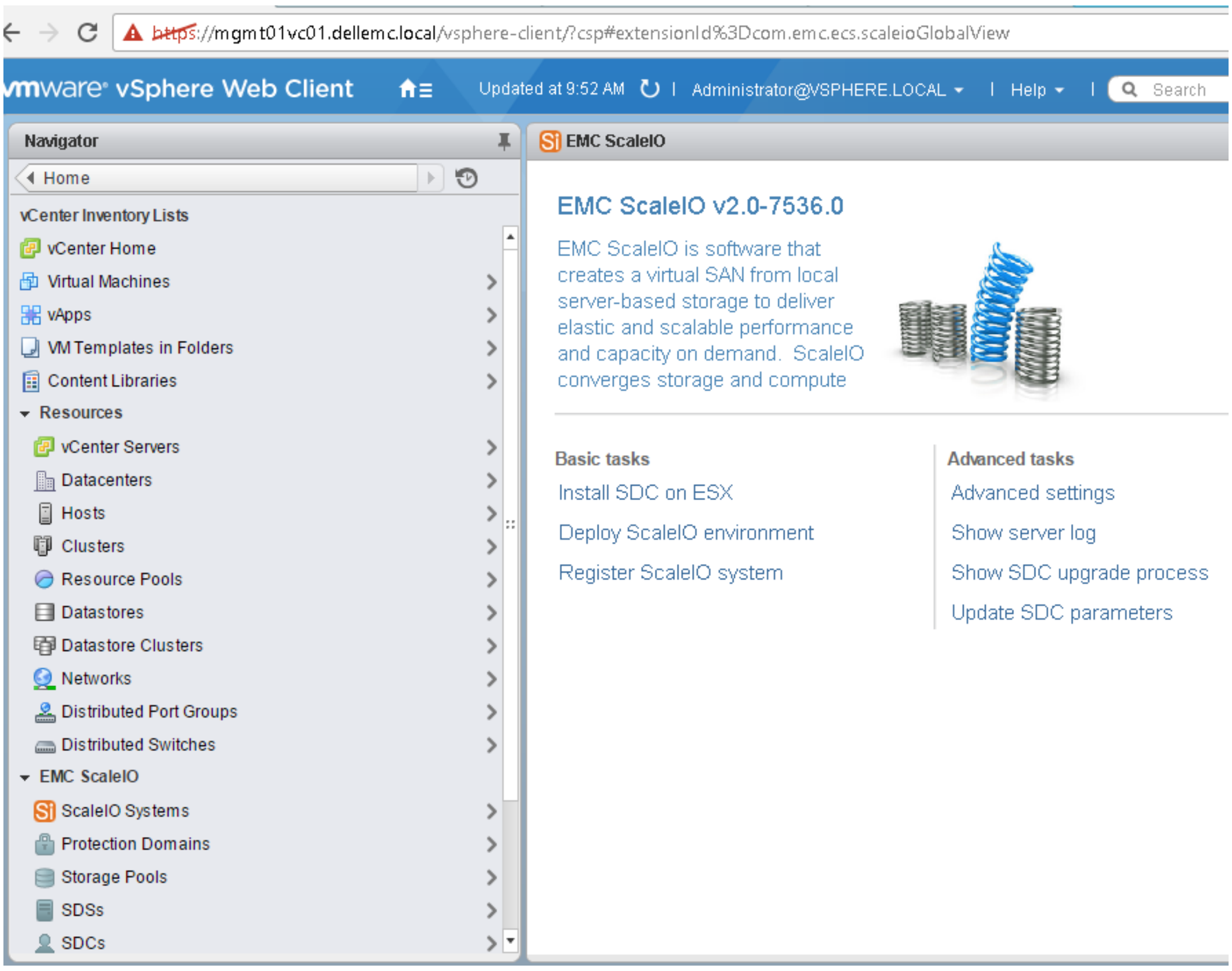
Basic Tasks

Create a datacenter

Figure 63 Resource & Edge VC ScaleIO templates

7.1.3 Configure a ScaleIO cluster

In the vCenter Web Client, click ScaleIO on the home screen:



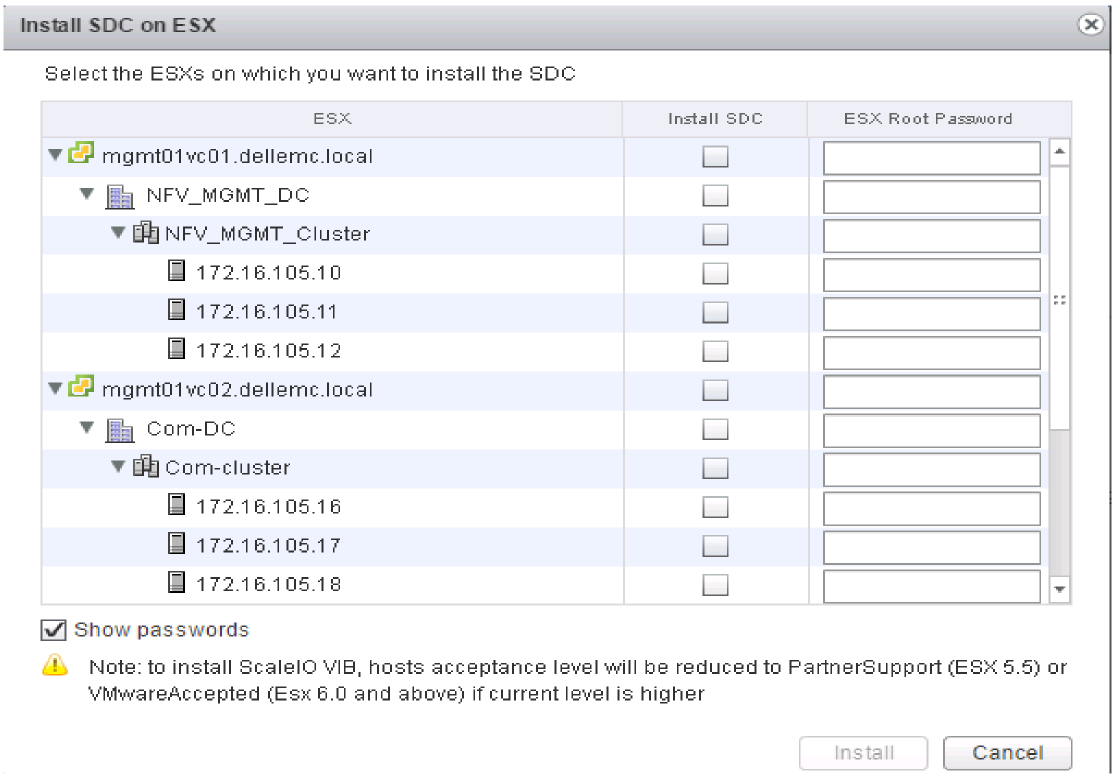
EMC ScaleIO v2.0-7536.0

EMC ScaleIO is software that creates a virtual SAN from local server-based storage to deliver elastic and scalable performance and capacity on demand. ScaleIO converges storage and compute

Figure 64 Configure ScaleIO cluster

Click Install SDC on ESX:

Select the hosts on which SDC will be installed. For each one, type the root password in the box provided, then click Install.



Install SDC on ESX

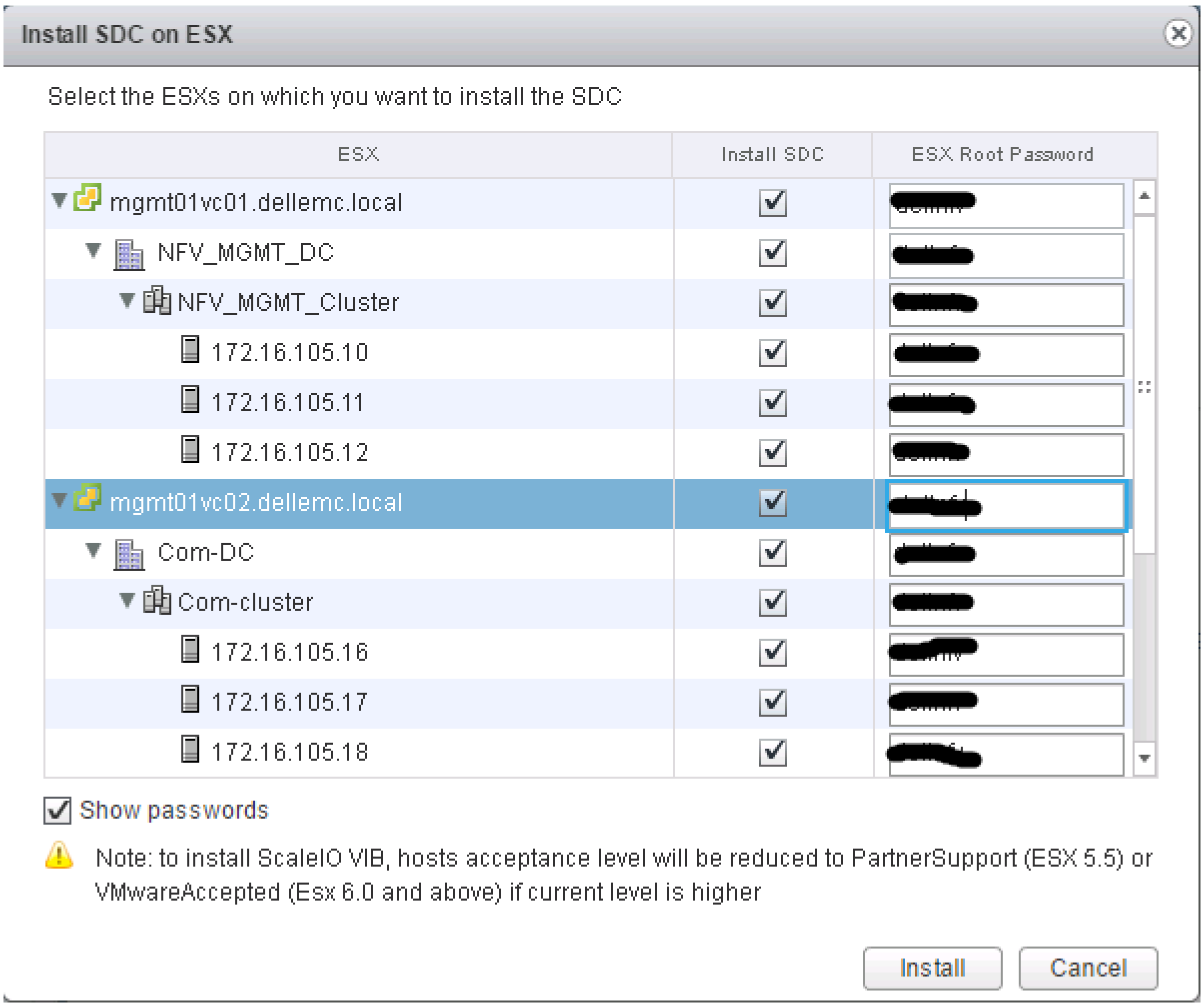
Select the ESXs on which you want to install the SDC

ESX	Install SDC	ESX Root Password
▼ mgmt01vc01.dellemc.local	□	
▼ NFV_MGMT_DC	□	
▼ NFV_MGMT_Cluster	□	
172.16.105.10	□	
172.16.105.11	□	
172.16.105.12	□	
▼ mgmt01vc02.dellemc.local	□	
▼ Com-DC	□	
▼ Com-cluster	□	
172.16.105.16	□	
172.16.105.17	□	
172.16.105.18	□	

☑ Show passwords

Note: to install ScaleIO VIB, hosts acceptance level will be reduced to PartnerSupport (ESX 5.5) or VMwareAccepted (Esx 6.0 and above) if current level is higher

Figure 65 Select hosts to install SDC



Install SDC on ESX

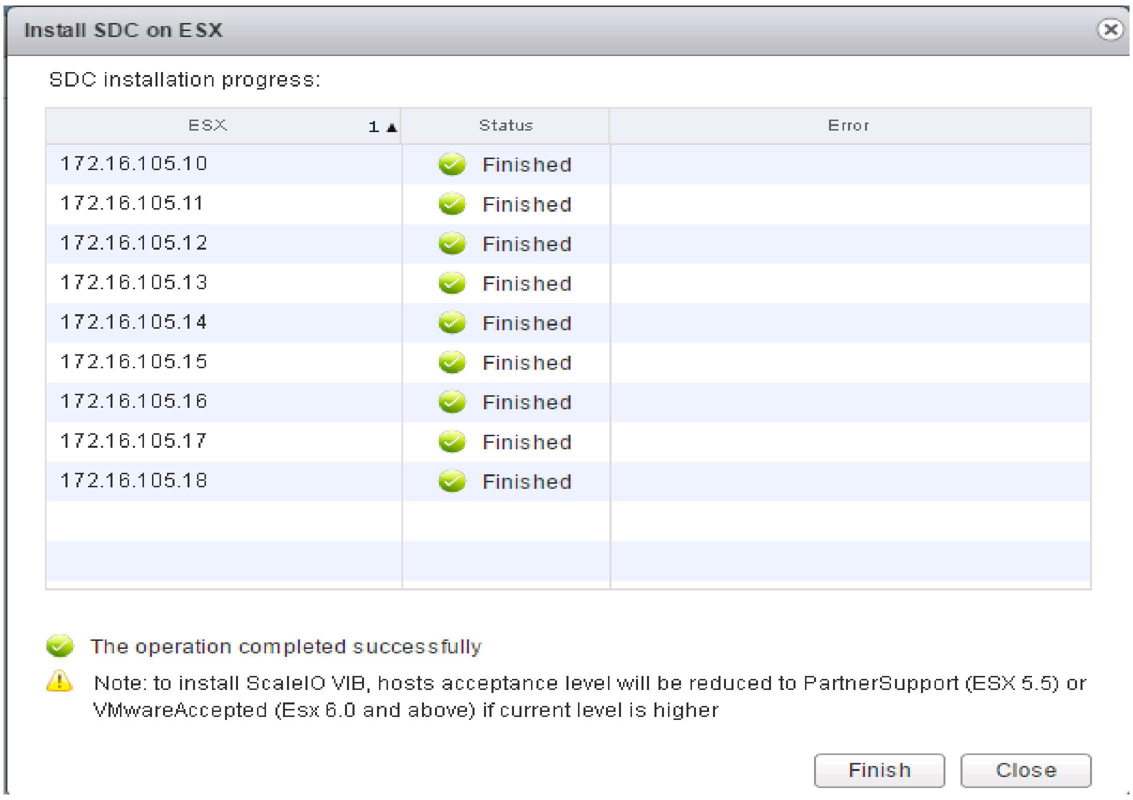
Select the ESXs on which you want to install the SDC

ESX	Install SDC	ESX Root Password
mgmt01vc01.dellemc.local	☑	[redacted]
NFV_MGMT_DC	☑	[redacted]
NFV_MGMT_Cluster	☑	[redacted]
172.16.105.10	☑	[redacted]
172.16.105.11	☑	[redacted]
172.16.105.12	☑	[redacted]
mgmt01vc02.dellemc.local	☑	[redacted]
Com-DC	☑	[redacted]
Com-cluster	☑	[redacted]
172.16.105.16	☑	[redacted]
172.16.105.17	☑	[redacted]
172.16.105.18	☑	[redacted]

☑ Show passwords

⚠ Note: to install ScaleIO VIB, hosts acceptance level will be reduced to PartnerSupport (ESX 5.5) or VMwareAccepted (Esx 6.0 and above) if current level is higher

Figure 66 Enter ESX Password



Install SDC on ESX

SDC installation progress:

ESX 1 ▲	Status	Error
172.16.105.10	✓ Finished	
172.16.105.11	✓ Finished	
172.16.105.12	✓ Finished	
172.16.105.13	✓ Finished	
172.16.105.14	✓ Finished	
172.16.105.15	✓ Finished	
172.16.105.16	✓ Finished	
172.16.105.17	✓ Finished	
172.16.105.18	✓ Finished	

✓ The operation completed successfully

⚠ Note: to install ScaleIO VIB, hosts acceptance level will be reduced to PartnerSupport (ESX 5.5) or VMwareAccepted (Esx 6.0 and above) if current level is higher

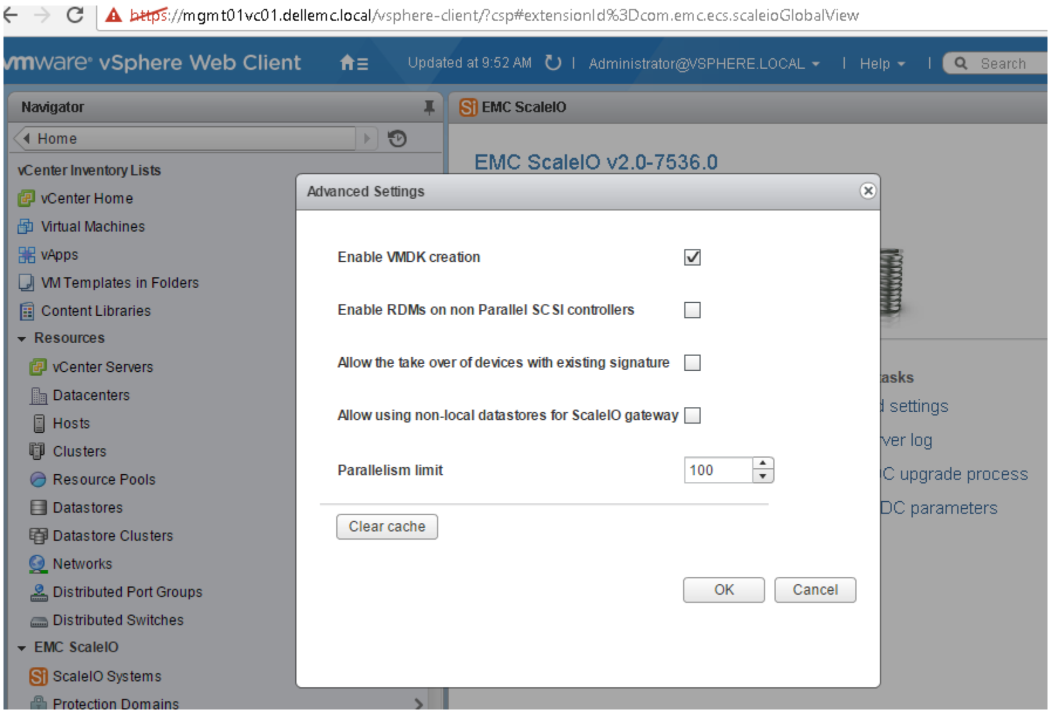
Figure 67 Installing SDC on ESX

Click **Finish** and reboot each host.

7.2 Configuring ScaleIO

Once the hosts have been rebooted, log back into the vCenter Web Client and click **ScaleIO**.

Before deploying the ScaleIO environment, select the **Enable VMDK Creation** option from the Advanced Settings.



Advanced Settings

Enable VMDK creation ☑

Enable RDMs on non Parallel SCSI controllers ☐

Allow the take over of devices with existing signature ☐

Allow using non-local datastores for ScaleIO gateway ☐

Parallelism limit 100

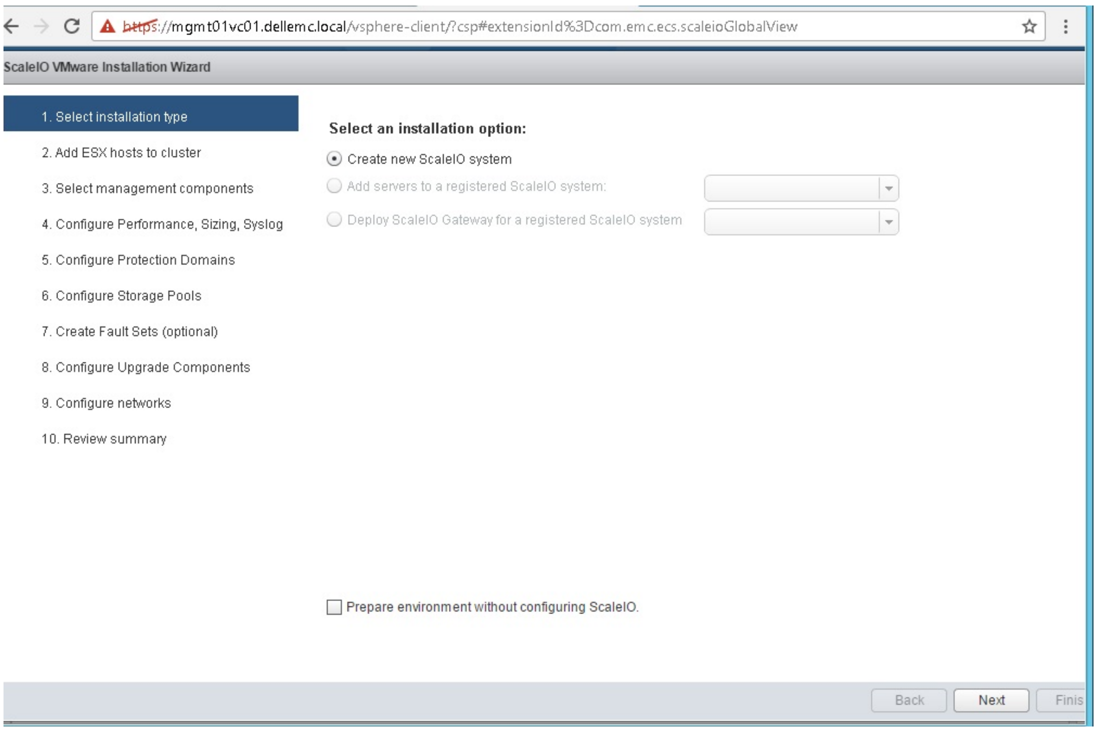
Clear cache

OK Cancel

Figure 68 Enable VMDK Creation

7.2.1 Create New Scale IO System

Click **Deploy ScaleIO environment**.



https://mgmt01vc01.dellemc.local/vsphere-client/?csp#extensionId%3Dcom.emc.ecs.scaleioGlobalView
ScaleIO VMware Installation Wizard

1. Select installation type
2. Add ESX hosts to cluster
3. Select management components
4. Configure Performance, Sizing, Syslog
5. Configure Protection Domains
6. Configure Storage Pools
7. Create Fault Sets (optional)
8. Configure Upgrade Components
9. Configure networks
10. Review summary

Select an installation option:

● Create new ScaleIO system

○ Add servers to a registered ScaleIO system:

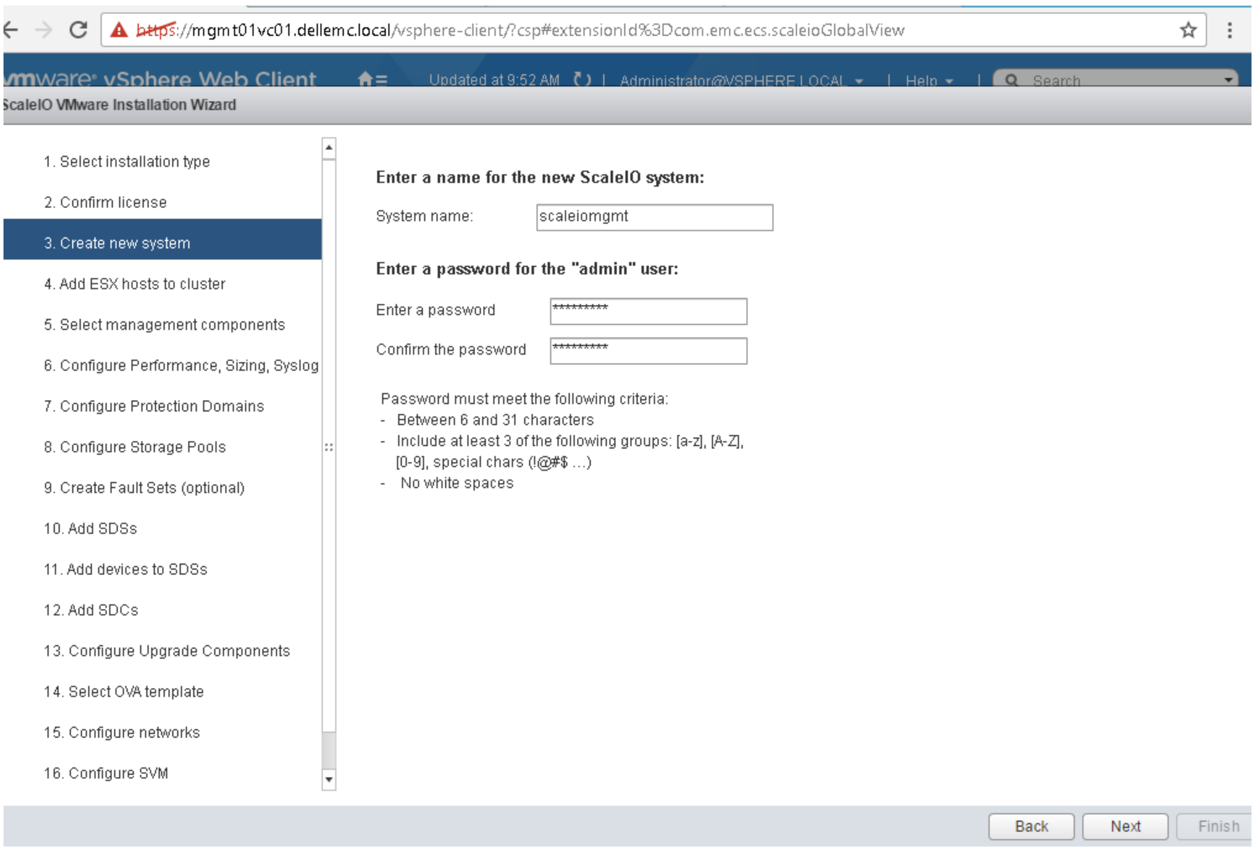
○ Deploy ScaleIO Gateway for a registered ScaleIO system

☐ Prepare environment without configuring ScaleIO.

Back Next Finis

Figure 69 Deploy ScaleIO environment

Enter a system name and password for the admin account. Click **Next**.


https://mgmt01vc01.dellemc.local/vsphere-client/?csp#extensionId%3Dcom.emc.ecs.scaleioGlobalView
vmware vSphere Web Client
Updated at 9:52 AM
Administrator@VSPHERE.LOCAL
Help
Search

ScaleIO VMware Installation Wizard

1. Select installation type
2. Confirm license
3. Create new system
4. Add ESX hosts to cluster
5. Select management components
6. Configure Performance, Sizing, Syslog
7. Configure Protection Domains
8. Configure Storage Pools
9. Create Fault Sets (optional)
10. Add SDSs
11. Add devices to SDSs
12. Add SDCs
13. Configure Upgrade Components
14. Select OVA template
15. Configure networks
16. Configure SVM

Enter a name for the new ScaleIO system:

System name: scaleiomgmt

Enter a password for the "admin" user:

Enter a password *********

Confirm the password *********

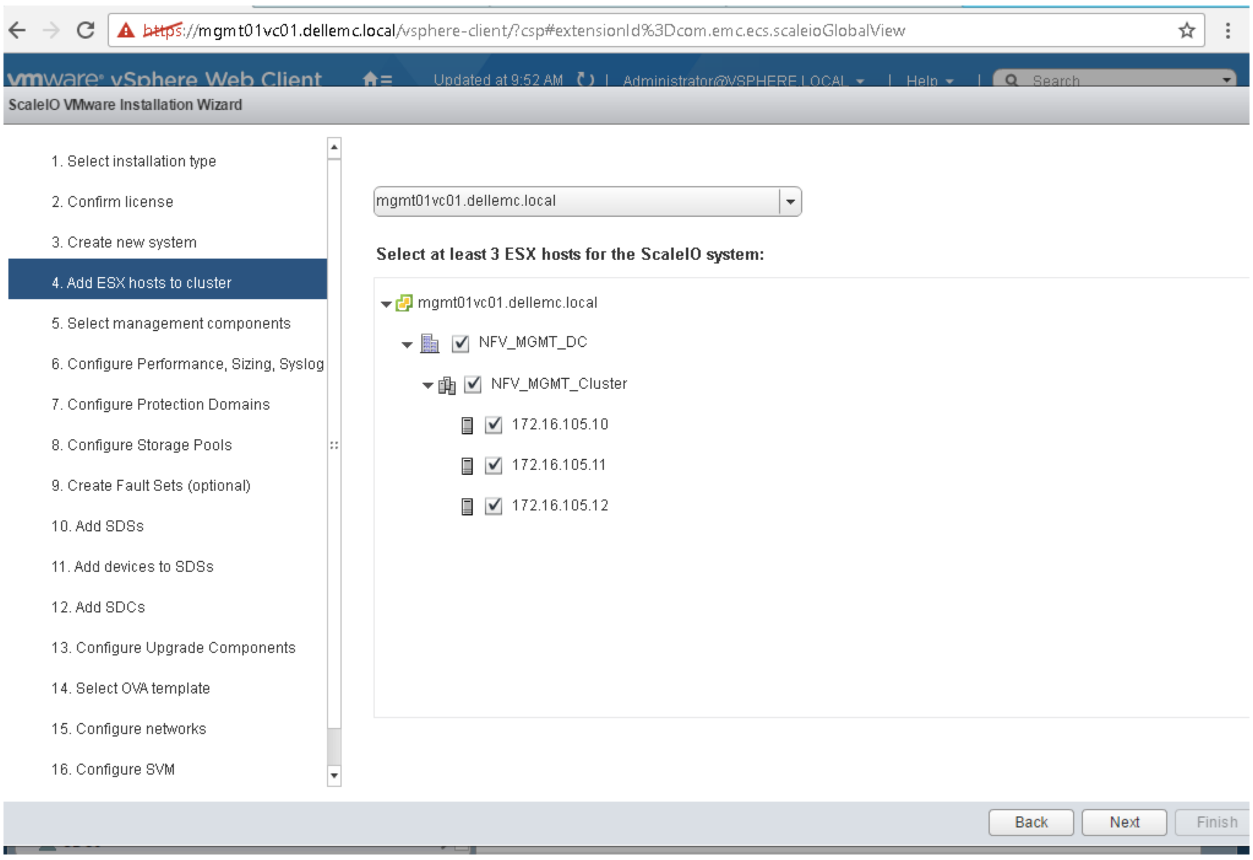
Password must meet the following criteria:
- Between 6 and 31 characters
- Include at least 3 of the following groups: [a-z], [A-Z], [0-9], special chars (!@#$ ...)
- No white spaces

Figure 70 Enter System Name

7.2.2 Select ESX hosts for the ScaleIO System

From the drop-down box, select your vCenter.

Select the hosts you wish to configure and click **Next**.


https://mgmt01vc01.dellemc.local/vsphere-client/?csp#extensionId%3Dcom.emc.ecs.scaleioGlobalView
vmware vSphere Web Client
Updated at 9:52 AM
Administrator@VSPHERE.LOCAL
Help
Search

ScaleIO VMware Installation Wizard

1. Select installation type
2. Confirm license
3. Create new system
4. Add ESX hosts to cluster
5. Select management components
6. Configure Performance, Sizing, Syslog
7. Configure Protection Domains
8. Configure Storage Pools
9. Create Fault Sets (optional)
10. Add SDSs
11. Add devices to SDSs
12. Add SDCs
13. Configure Upgrade Components
14. Select OVA template
15. Configure networks
16. Configure SVM

mgmt01vc01.dellemc.local

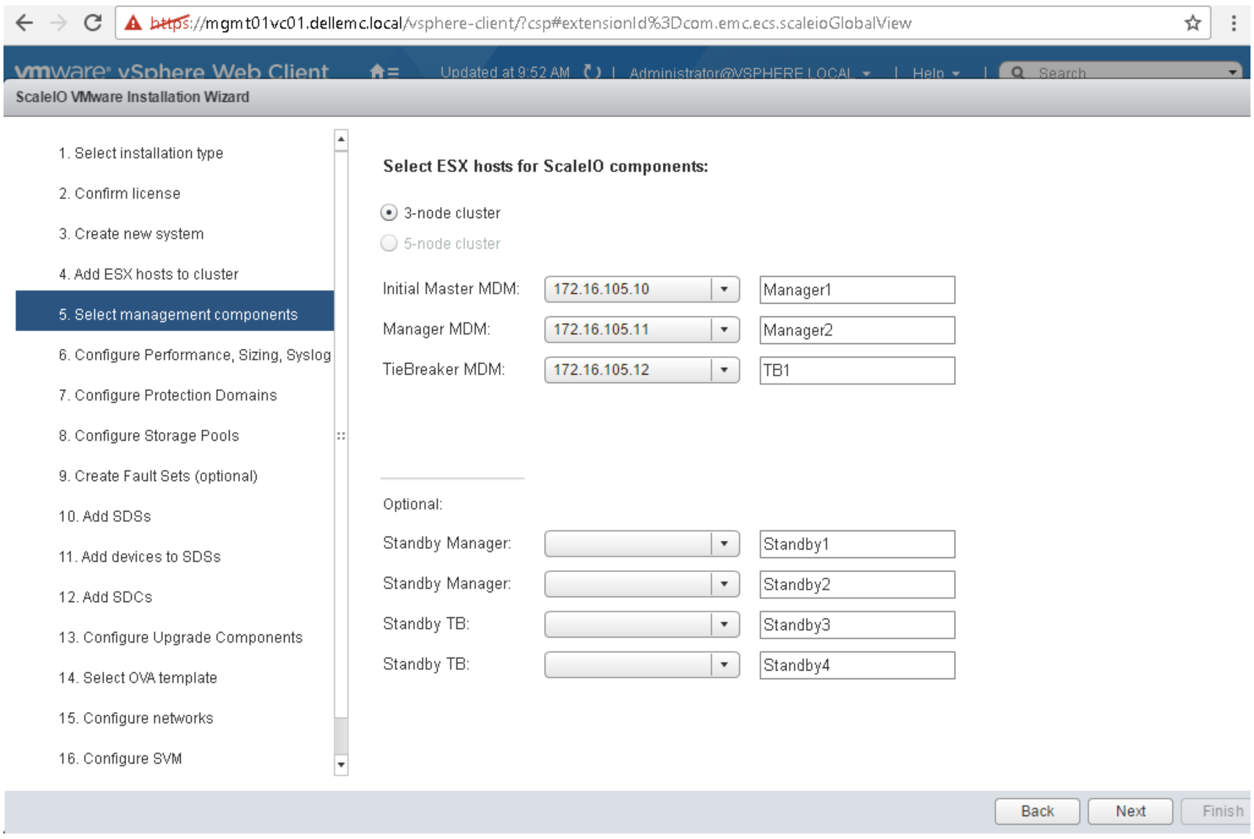
Select at least 3 ESX hosts for the ScaleIO system:

- mgmt01vc01.dellemc.local
  - ☑ NFV_MGMT_DC
    - ☑ NFV_MGMT_Cluster
      - ☑ 172.16.105.10
      - ☑ 172.16.105.11
      - ☑ 172.16.105.12

Figure 71 Select ESX hosts for the ScaleIO System

7.2.3 Add MDM hosts

Select which system should host a Meta-Data Manager (MDM) or tiebreaker. The management cluster has only three nodes or ESXi hosts.



https://mgmt01vc01.dellemc.local/vsphere-client/?csp#extensionId%3Dcom.emc.ecs.scaleioGlobalView

vmware® vSphere Web Client | Updated at 9:52 AM | Administrator@VSPHERE.LOCAL | Help | Search

ScaleIO VMware Installation Wizard

1. Select installation type
2. Confirm license
3. Create new system
4. Add ESX hosts to cluster
5. Select management components
6. Configure Performance, Sizing, Syslog
7. Configure Protection Domains
8. Configure Storage Pools
9. Create Fault Sets (optional)
10. Add SDSs
11. Add devices to SDSs
12. Add SDCs
13. Configure Upgrade Components
14. Select OVA template
15. Configure networks
16. Configure SVM

Select ESX hosts for ScaleIO components:

● 3-node cluster

○ 5-node cluster

Initial Master MDM:	172.16.105.10	Manager1
Manager MDM:	172.16.105.11	Manager2
TieBreaker MDM:	172.16.105.12	TB1

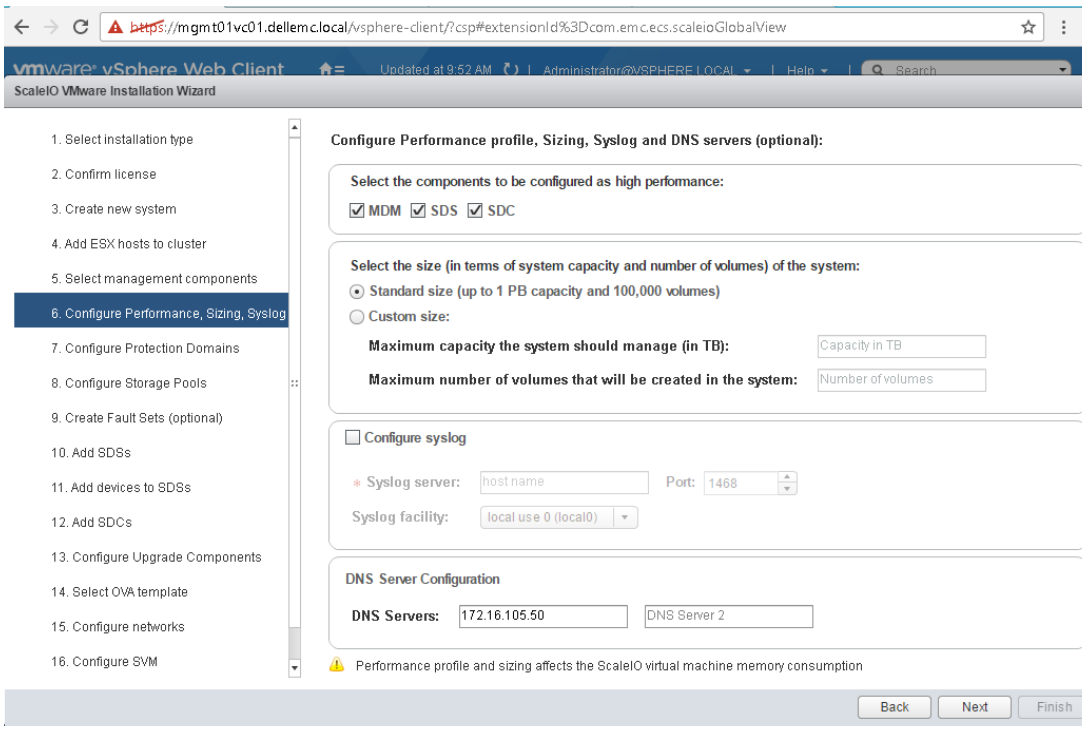
Optional:

Standby Manager:		Standby1
Standby Manager:		Standby2
Standby TB:		Standby3
Standby TB:		Standby4

Figure 72 Meta-Data Manager

Click **Next**.

Select **MDM**, **SDS** and **SDC** check boxes and then click **Next**.



https://mgmt01vc01.dellemc.local/vsphere-client/?csp#extensionId%3Dcom.emc.ecs.scaleioGlobalView

vmware® vSphere Web Client | Updated at 9:52 AM | Administrator@VSPHERE.LOCAL | Help | Search

ScaleIO VMware Installation Wizard

1. Select installation type
2. Confirm license
3. Create new system
4. Add ESX hosts to cluster
5. Select management components
6. Configure Performance, Sizing, Syslog
7. Configure Protection Domains
8. Configure Storage Pools
9. Create Fault Sets (optional)
10. Add SDSs
11. Add devices to SDSs
12. Add SDCs
13. Configure Upgrade Components
14. Select OVA template
15. Configure networks
16. Configure SVM

Configure Performance profile, Sizing, Syslog and DNS servers (optional):

Select the components to be configured as high performance:

☑ MDM ☑ SDS ☑ SDC

Select the size (in terms of system capacity and number of volumes) of the system:

● Standard size (up to 1 PB capacity and 100,000 volumes)

○ Custom size:

Maximum capacity the system should manage (in TB): Capacity in TB

Maximum number of volumes that will be created in the system: Number of volumes

□ Configure syslog

* Syslog server: host name Port: 1468

Syslog facility: local use 0 (local0)

DNS Server Configuration

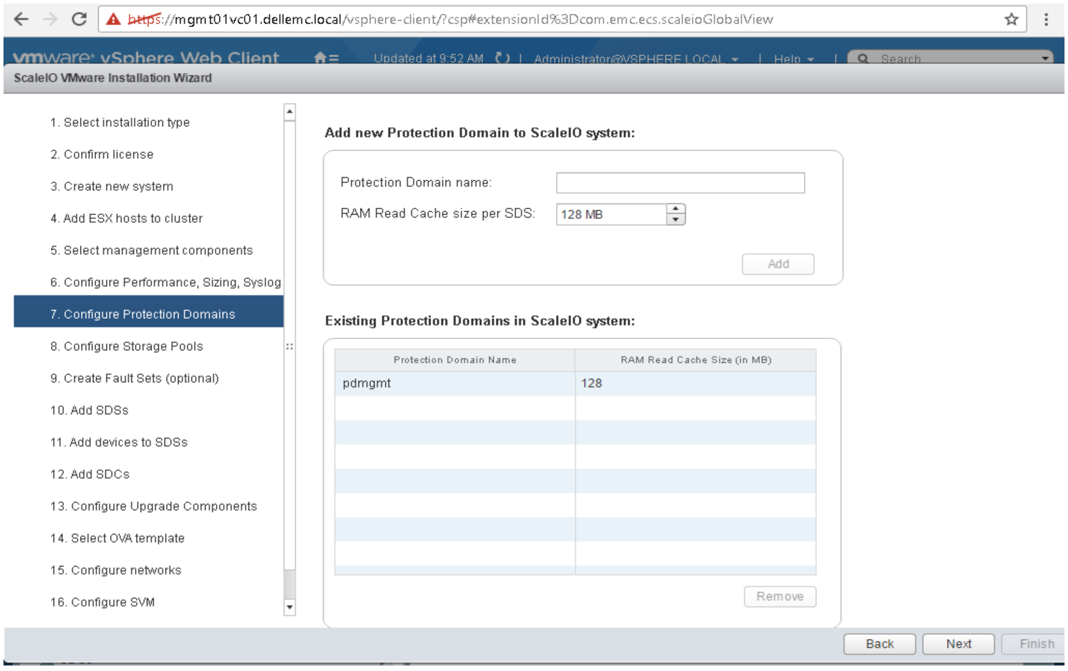
DNS Servers: 172.16.105.50 DNS Server 2

⚠ Performance profile and sizing affects the ScaleIO virtual machine memory consumption

Figure 73 Select MDM, SDS, SDC check boxes

7.2.4 Add Protection Domain

Enter a Name for the new Protection Domain, click **Add** and then click **Next**.



https://mgmt01vc01.dellemc.local/vsphere-client/?csp#extensionId%3Dcom.emc.ecs.scaleioGlobalView

ScaleIO VMware Installation Wizard

1. Select installation type
2. Confirm license
3. Create new system
4. Add ESX hosts to cluster
5. Select management components
6. Configure Performance, Sizing, Syslog
7. Configure Protection Domains
8. Configure Storage Pools
9. Create Fault Sets (optional)
10. Add SDSs
11. Add devices to SDSs
12. Add SDCs
13. Configure Upgrade Components
14. Select OVA template
15. Configure networks
16. Configure SVM

Add new Protection Domain to ScaleIO system:

Protection Domain name:

RAM Read Cache size per SDS: 128 MB

Existing Protection Domains in ScaleIO system:

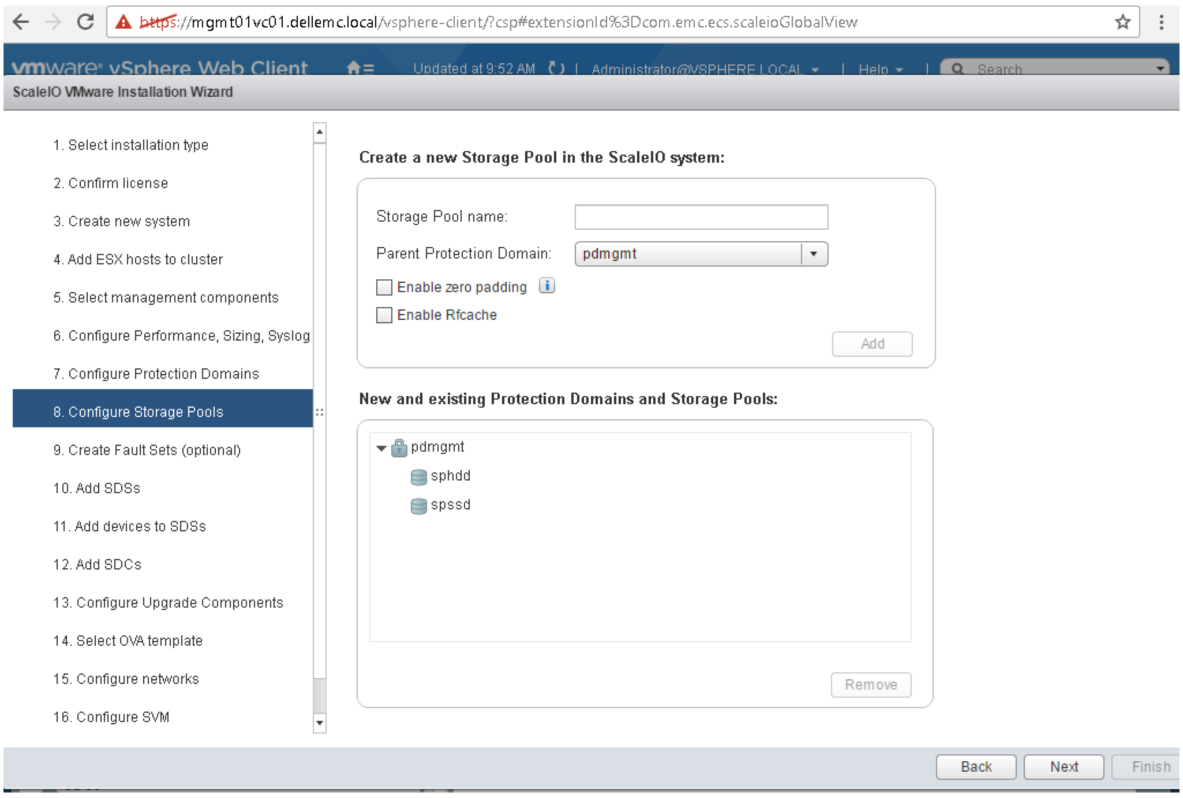
Protection Domain Name	RAM Read Cache Size (in MB)
pdmgmt	128

Figure 74 Protection Domain name

7.2.5 Add Storage Pools

In this environment two storage pools have been created; sphdd (low performance pool with HDDs) and spssd (high performance pool with SSDs).

Type a name for the Storage Pool and click Add, followed by **Next**.



https://mgmt01vc01.dellemc.local/vsphere-client/?csp#extensionId%3Dcom.emc.ecs.scaleioGlobalView

ScaleIO VMware Installation Wizard

1. Select installation type
2. Confirm license
3. Create new system
4. Add ESX hosts to cluster
5. Select management components
6. Configure Performance, Sizing, Syslog
7. Configure Protection Domains
8. Configure Storage Pools
9. Create Fault Sets (optional)
10. Add SDSs
11. Add devices to SDSs
12. Add SDCs
13. Configure Upgrade Components
14. Select OVA template
15. Configure networks
16. Configure SVM

Create a new Storage Pool in the ScaleIO system:

Storage Pool name:

Parent Protection Domain: pdmgmt

☐ Enable zero padding

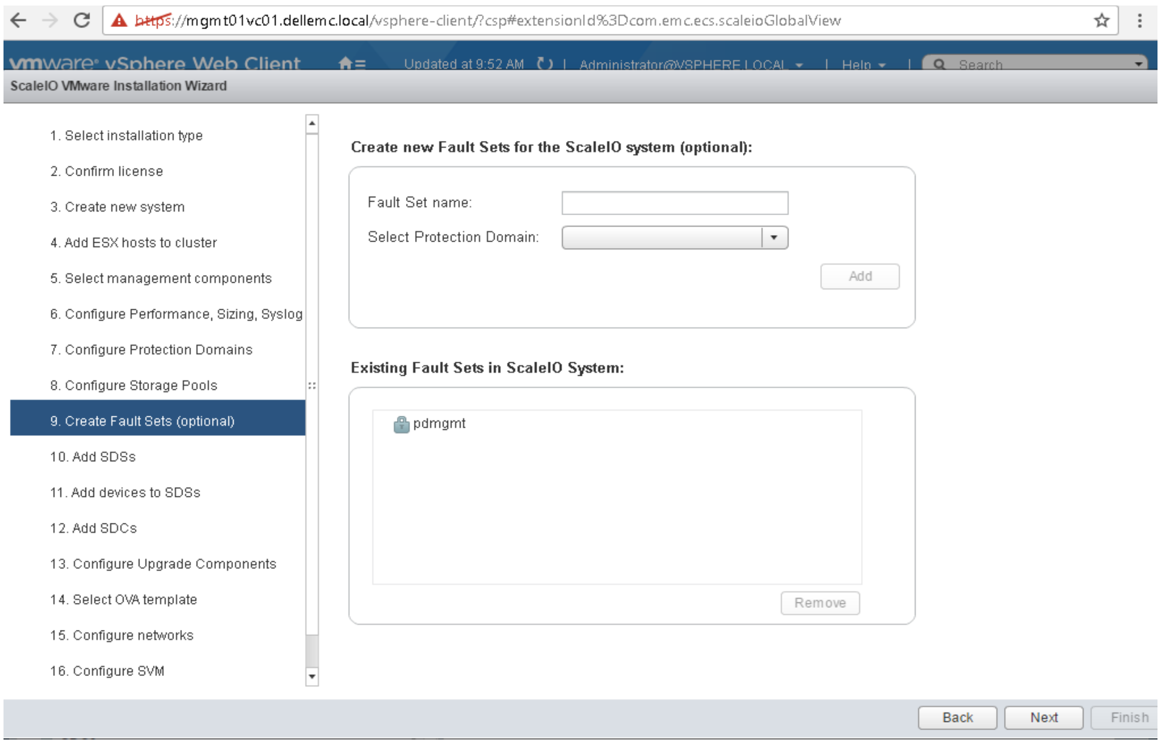
☐ Enable Rfcache

New and existing Protection Domains and Storage Pools:

- pdmgmt
  - sphdd
  - spssd

Figure 75 Storage Pool name

Click **Next.**



https://mgmt01vc01.dellemc.local/vsphere-client/?csp#extensionId%3Dcom.emc.ecs.scaleioGlobalView

ScaleIO VMware Installation Wizard

1. Select installation type
2. Confirm license
3. Create new system
4. Add ESX hosts to cluster
5. Select management components
6. Configure Performance, Sizing, Syslog
7. Configure Protection Domains
8. Configure Storage Pools
9. Create Fault Sets (optional)
10. Add SDSs
11. Add devices to SDSs
12. Add SDCs
13. Configure Upgrade Components
14. Select OVA template
15. Configure networks
16. Configure SVM

Create new Fault Sets for the ScaleIO system (optional):

Fault Set name:

Select Protection Domain:

Existing Fault Sets in ScaleIO System:

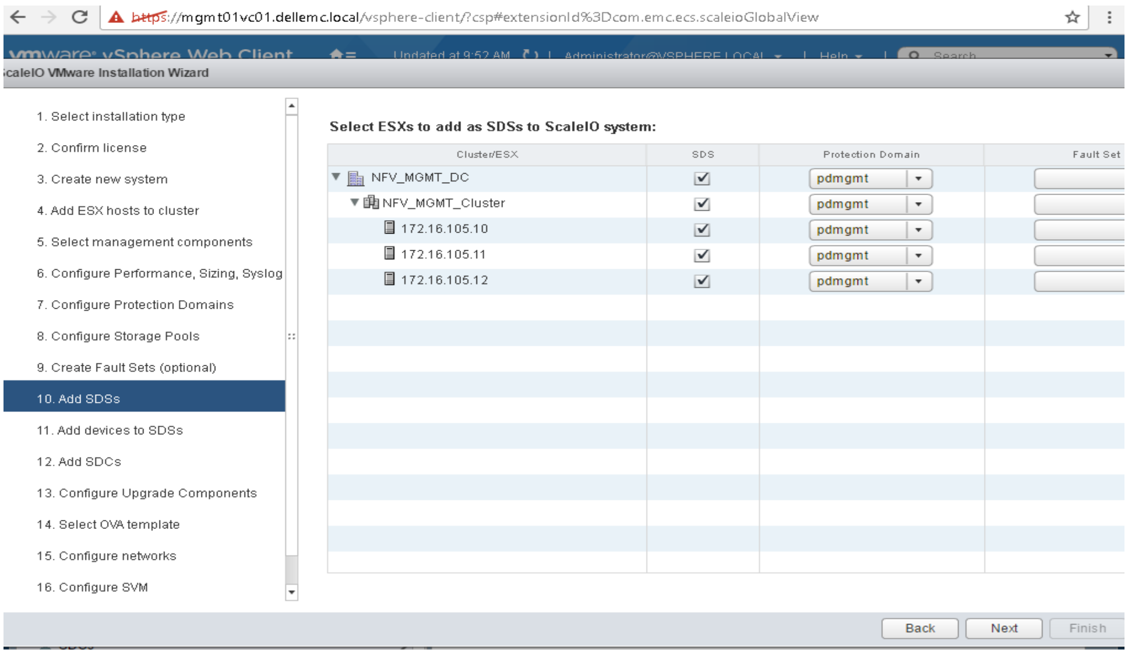
pdmgmt

Figure 76 Fault Sets

7.2.6 Add SDS Hosts

A ScaleIO Data Server (SDS) resides on each host that contributes storage. In this case, an SDS will exist on each ESXi host.

Select all hosts and click **Next**.



https://mgmt01vc01.dellemc.local/vsphere-client/?csp#extensionId%3Dcom.emc.ecs.scaleioGlobalView

caleIO VMware Installation Wizard

1. Select installation type
2. Confirm license
3. Create new system
4. Add ESX hosts to cluster
5. Select management components
6. Configure Performance, Sizing, Syslog
7. Configure Protection Domains
8. Configure Storage Pools
9. Create Fault Sets (optional)
10. Add SDSs
11. Add devices to SDSs
12. Add SDCs
13. Configure Upgrade Components
14. Select OVA template
15. Configure networks
16. Configure SVM

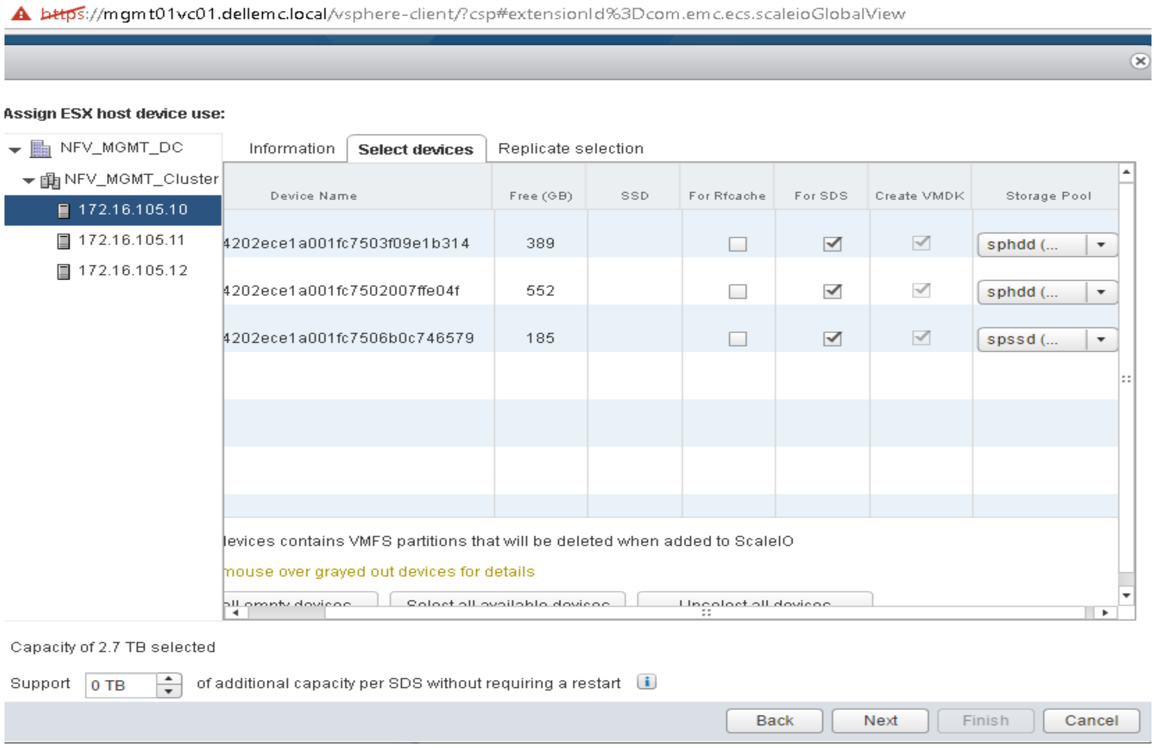
Select ESXs to add as SDSs to ScaleIO system:

Cluster/ESX	SDS	Protection Domain	Fault Set
NFV_MGMT_DC	☑	pdmgmt	
NFV_MGMT_Cluster	☑	pdmgmt	
172.16.105.10	☑	pdmgmt	
172.16.105.11	☑	pdmgmt	
172.16.105.12	☑	pdmgmt	

Figure 77 Select all hosts

Select the disks you would like to use and their respective storage pool. Click **Next**.

7.2.7 Add Devices from SDSs for Storage



https://mgmt01vc01.dellemc.local/vsphere-client/?csp#extensionId%3Dcom.emc.ecs.scaleioGlobalView

Assign ESX host device use:

- NFV_MGMT_DC
  - NFV_MGMT_Cluster
    - 172.16.105.10
    - 172.16.105.11
    - 172.16.105.12

Information | **Select devices** | Replicate selection

Device Name	Free (GB)	SSD	For Rfcache	For SDS	Create VMDK	Storage Pool
4202ece1a001fc7503f09e1b314	389		☐	☑	☑	sphdd (...
4202ece1a001fc7502007ffe04f	552		☐	☑	☑	sphdd (...
4202ece1a001fc7506b0c746579	185		☐	☑	☑	spssd (...

levices contains VMFS partitions that will be deleted when added to ScaleIO

mouse over grayed out devices for details

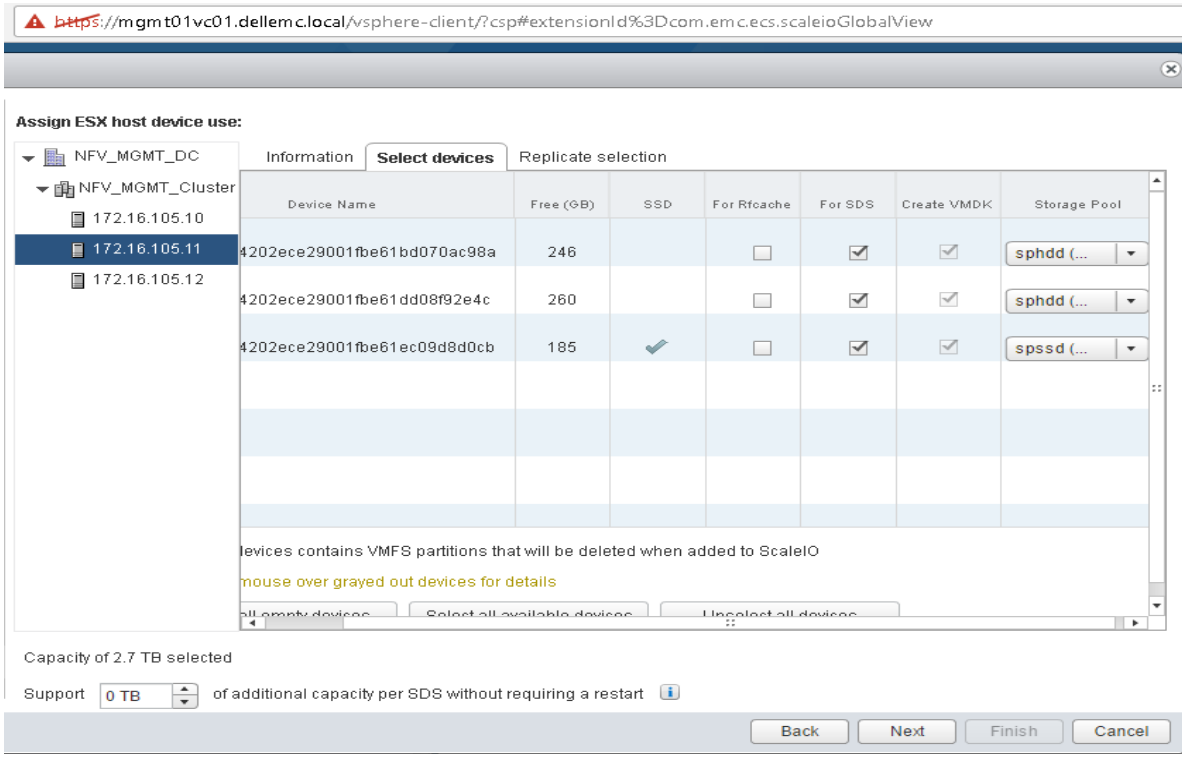
ll empty devices | Select all available devices | Unselect all devices

Capacity of 2.7 TB selected

Support 0 TB of additional capacity per SDS without requiring a restart

Back | Next | Finish | Cancel

Figure 78 Select disks to use for storage pool



https://mgmt01vc01.dellemc.local/vsphere-client/?csp#extensionId%3Dcom.emc.ecs.scaleioGlobalView

Assign ESX host device use:

- NFV_MGMT_DC
  - NFV_MGMT_Cluster
    - 172.16.105.10
    - 172.16.105.11
    - 172.16.105.12

Information | **Select devices** | Replicate selection

Device Name	Free (GB)	SSD	For Rfcache	For SDS	Create VMDK	Storage Pool
4202ece29001fbe61bd070ac98a	246		☐	☑	☑	sphdd (...
4202ece29001fbe61dd08f92e4c	260		☐	☑	☑	sphdd (...
4202ece29001fbe61ec09d8d0cb	185	✓	☐	☑	☑	spssd (...

levices contains VMFS partitions that will be deleted when added to ScaleIO

mouse over grayed out devices for details

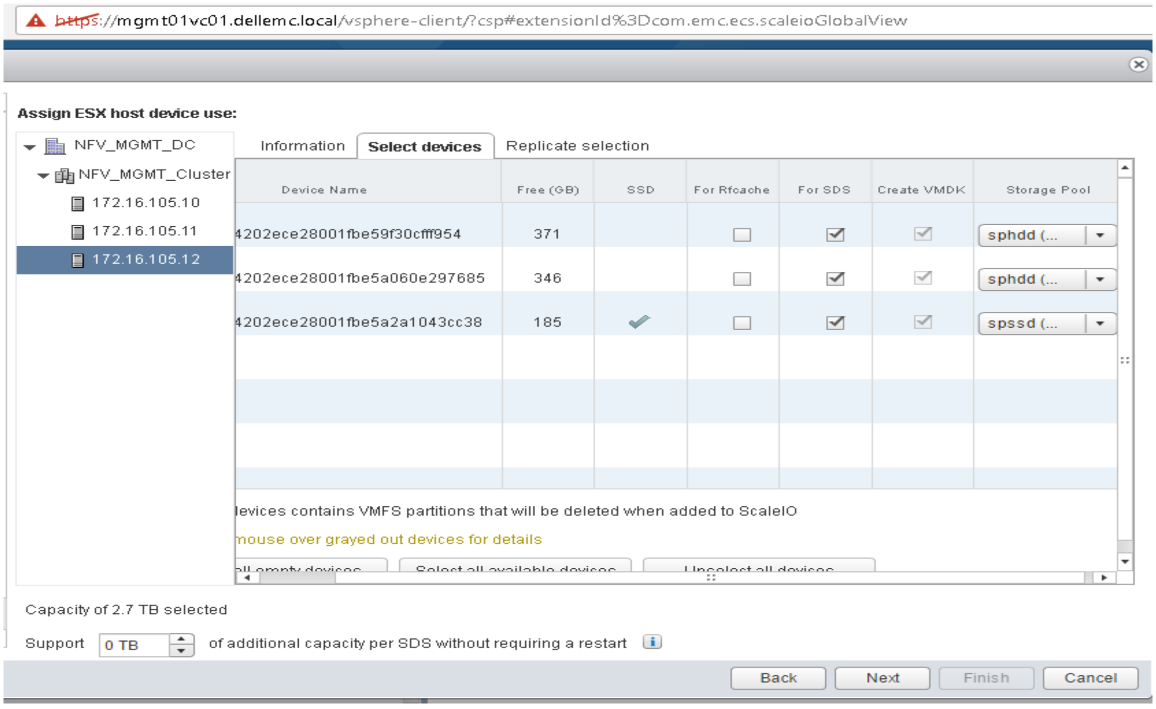
ll empty devices | Select all available devices | Unselect all devices

Capacity of 2.7 TB selected

Support 0 TB of additional capacity per SDS without requiring a restart

Back | Next | Finish | Cancel

Figure 79 Select disks to use for storage pool



https://mgmt01vc01.dellemc.local/vsphere-client/?csp#extensionId%3Dcom.emc.ecs.scaleioGlobalView

Assign ESX host device use:

- NFV_MGMT_DC
  - NFV_MGMT_Cluster
    - 172.16.105.10
    - 172.16.105.11
    - 172.16.105.12

Device Name	Free (GB)	SSD	For Rfcache	For SDS	Create VMDK	Storage Pool
4202ece28001fbe59f30cff954	371		□	☑	☑	sphdd (...
4202ece28001fbe5a060e297685	346		□	☑	☑	sphdd (...
4202ece28001fbe5a2a1043cc38	185	✓	□	☑	☑	spssd (...

levices contains VMFS partitions that will be deleted when added to ScaleIO

mouse over grayed out devices for details

Capacity of 2.7 TB selected

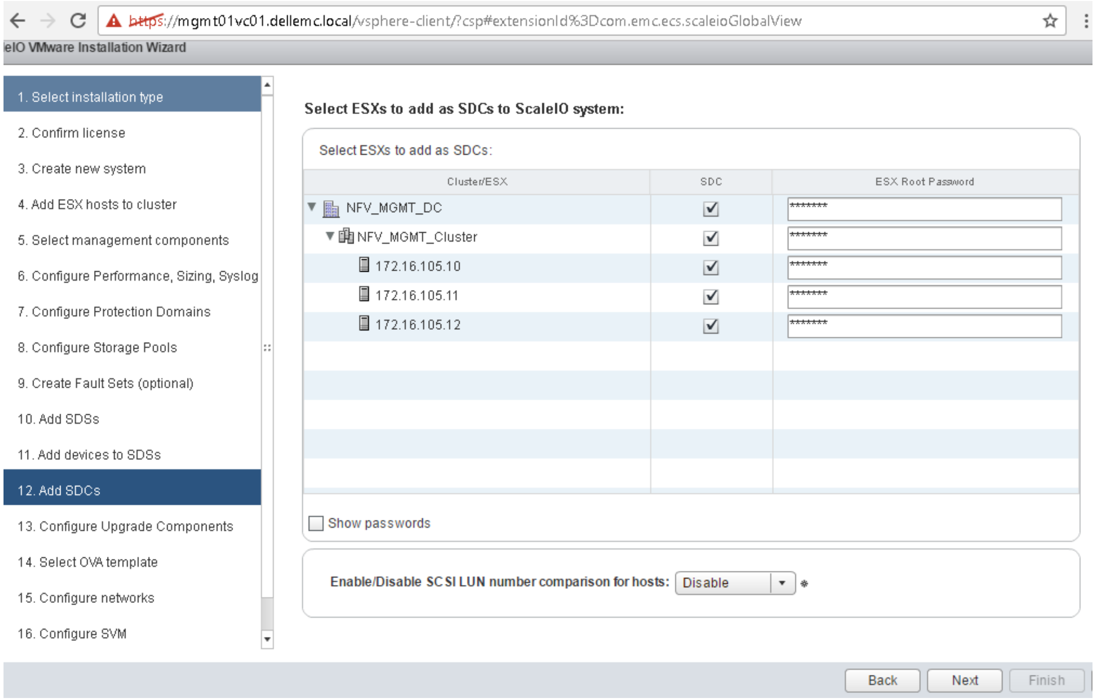
Support 0 TB of additional capacity per SDS without requiring a restart

Figure 80 Select disks to use for storage pool

7.2.8 Select SDCs

The ScaleIO Data Client (SDC) sits on each host that needs to access data served by the SDS. As there are only three nodes in this example, each host utilizes an SDC.

Select each host and type the root password in the box provided, followed by **Next**. From the drop-down box, select **Disable**, followed by **Next**.



https://mgmt01vc01.dellemc.local/vsphere-client/?csp#extensionId%3Dcom.emc.ecs.scaleioGlobalView

eIO VMware Installation Wizard

1. Select installation type
2. Confirm license
3. Create new system
4. Add ESX hosts to cluster
5. Select management components
6. Configure Performance, Sizing, Syslog
7. Configure Protection Domains
8. Configure Storage Pools
9. Create Fault Sets (optional)
10. Add SDSs
11. Add devices to SDSs
12. Add SDCs
13. Configure Upgrade Components
14. Select OVA template
15. Configure networks
16. Configure SVM

Select ESXs to add as SDCs to ScaleIO system:

Select ESXs to add as SDCs:

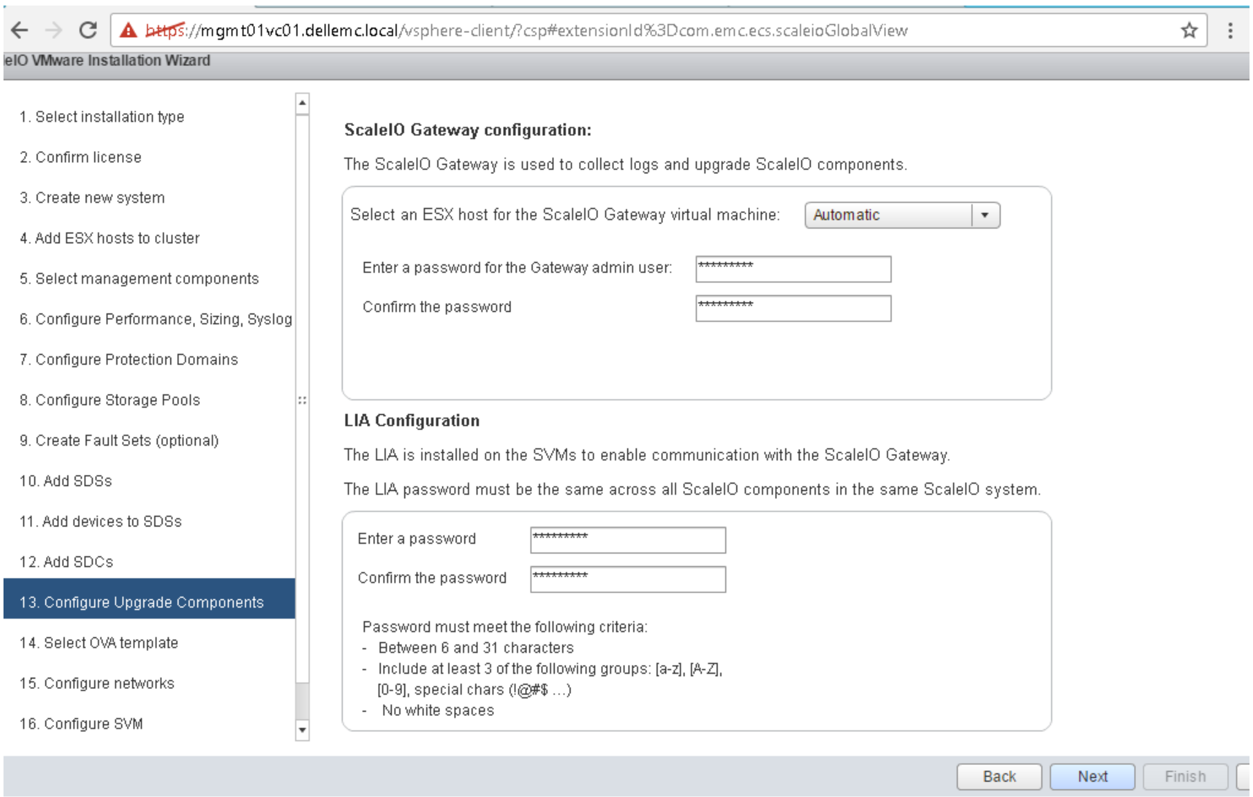
Cluster/ESX	SDC	ESX Root Password
NFV_MGMT_DC	☑	*******
NFV_MGMT_Cluster	☑	*******
172.16.105.10	☑	*******
172.16.105.11	☑	*******
172.16.105.12	☑	*******

□ Show passwords

Enable/Disable SCSI LUN number comparison for hosts: Disable *

Figure 81 Select SDCs

Choose a host to run the ScaleIO Gateway, and type a password in the box provided, followed by **Next**.



https://mgmt01vc01.dellemc.local/vsphere-client/?csp#extensionId%3Dcom.emc.ecs.scaleioGlobalView
eIO VMware Installation Wizard

1. Select installation type
2. Confirm license
3. Create new system
4. Add ESX hosts to cluster
5. Select management components
6. Configure Performance, Sizing, Syslog
7. Configure Protection Domains
8. Configure Storage Pools
9. Create Fault Sets (optional)
10. Add SDSs
11. Add devices to SDSs
12. Add SDCs
13. Configure Upgrade Components
14. Select OVA template
15. Configure networks
16. Configure SVM

ScaleIO Gateway configuration:

The ScaleIO Gateway is used to collect logs and upgrade ScaleIO components.

Select an ESX host for the ScaleIO Gateway virtual machine: Automatic

Enter a password for the Gateway admin user: **********

Confirm the password **********

LIA Configuration

The LIA is installed on the SVMs to enable communication with the ScaleIO Gateway.

The LIA password must be the same across all ScaleIO components in the same ScaleIO system.

Enter a password **********

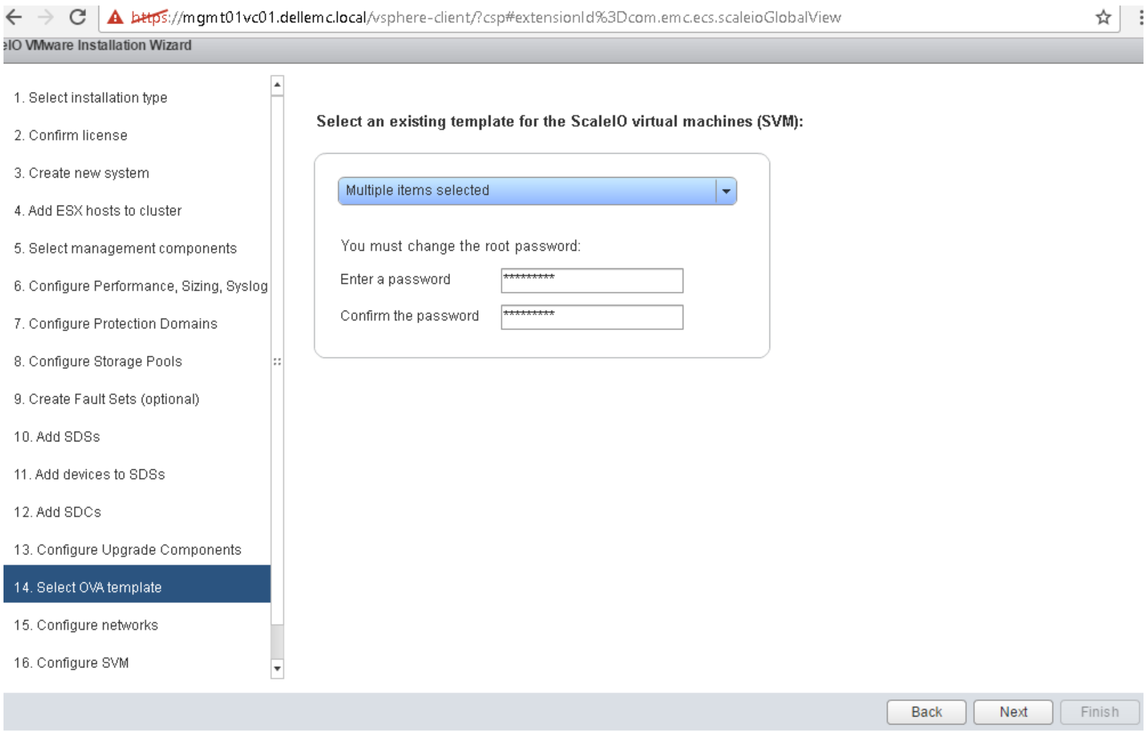
Confirm the password **********

Password must meet the following criteria:
- Between 6 and 31 characters
- Include at least 3 of the following groups: [a-z], [A-Z], [0-9], special chars (!@#$ ...)
- No white spaces

Figure 82 Enter password for ScaleIO Gateway

A ScaleIO virtual machine will be deployed from each template to each ESXi host. Each VM will run a SDS for serving storage and a MDM for managing storage. The SDC, which will consume the storage, is embedded directly into ESXi.

Type a password in the box provided. This will be the admin password for each ScaleIO virtual machine once it has been deployed.



https://mgmt01vc01.dellemc.local/vsphere-client/?csp#extensionId%3Dcom.emc.ecs.scaleioGlobalView
eIO VMware Installation Wizard

1. Select installation type
2. Confirm license
3. Create new system
4. Add ESX hosts to cluster
5. Select management components
6. Configure Performance, Sizing, Syslog
7. Configure Protection Domains
8. Configure Storage Pools
9. Create Fault Sets (optional)
10. Add SDSs
11. Add devices to SDSs
12. Add SDCs
13. Configure Upgrade Components
14. Select OVA template
15. Configure networks
16. Configure SVM

Select an existing template for the ScaleIO virtual machines (SVM):

Multiple items selected

You must change the root password:

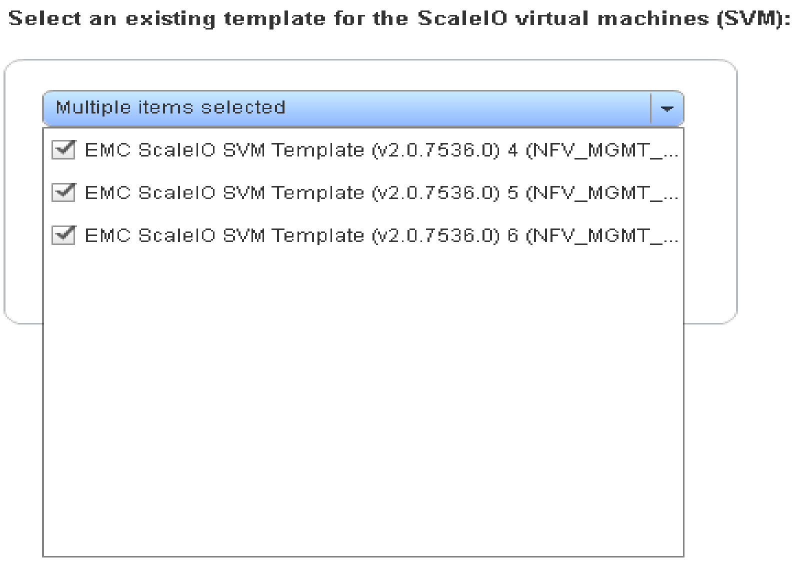
Enter a password **********

Confirm the password **********

Figure 83 Enter password for ScaleIO virtual machine

7.2.9 Select ScaleIO Template for SVM

From the drop-down box, select each template and click **Next**.



Select an existing template for the ScaleIO virtual machines (SVM):

Multiple items selected

- ☑ EMC ScaleIO SVM Template (v2.0.7536.0) 4 (NFV_MGMT_...
- ☑ EMC ScaleIO SVM Template (v2.0.7536.0) 5 (NFV_MGMT_...
- ☑ EMC ScaleIO SVM Template (v2.0.7536.0) 6 (NFV_MGMT_...

Figure 84 Select a template for SVM

7.2.10 Configure ScaleIO Network

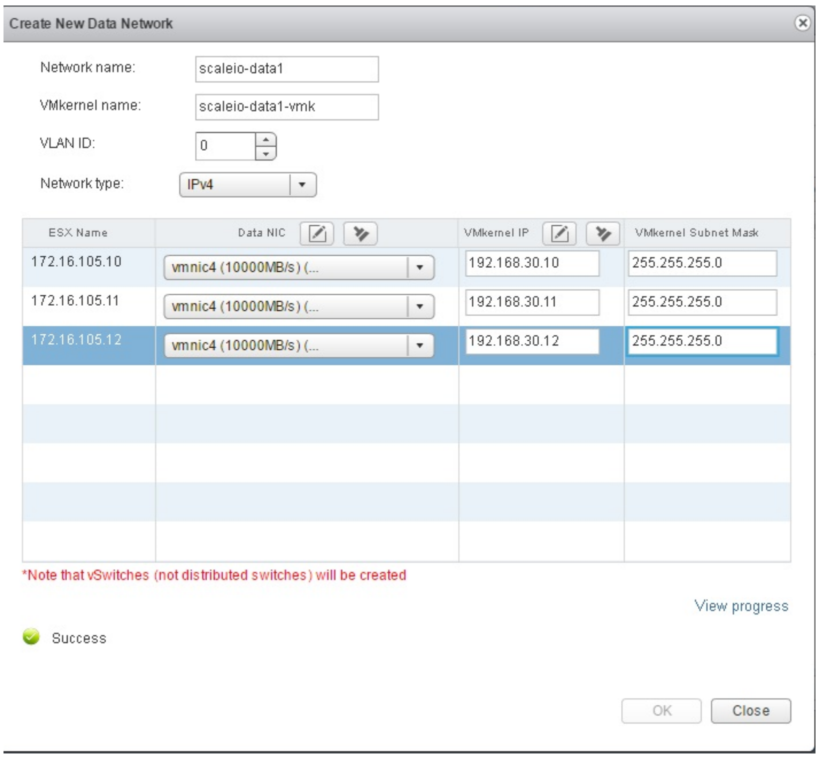
ScaleIO Network Configuration

For each network, use the drop-down box to select the appropriate network. In the following example, three port groups are created on the distributed vSwitch.

Click **Next**.

Configure each IP subnet as desired. When complete, click **Next**.

ScaleIO Data Network 1:



Create New Data Network

Network name: scaleio-data1

VMkernel name: scaleio-data1-vmk

VLAN ID: 0

Network type: IPv4

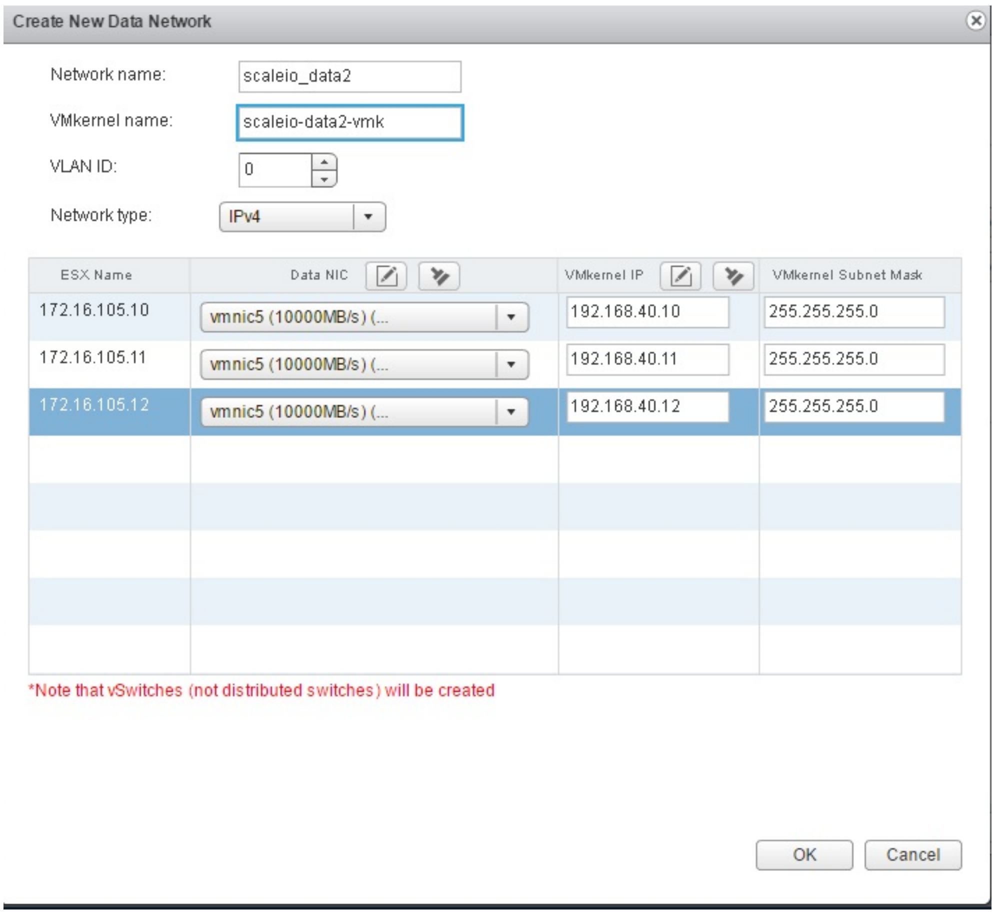
ESX Name	Data NIC	VMkernel IP	VMkernel Subnet Mask
172.16.105.10	vmnic4 (10000MB/s) (...	192.168.30.10	255.255.255.0
172.16.105.11	vmnic4 (10000MB/s) (...	192.168.30.11	255.255.255.0
172.16.105.12	vmnic4 (10000MB/s) (...	192.168.30.12	255.255.255.0

*Note that vSwitches (not distributed switches) will be created

Success

Figure 85 ScaleIO Data Network 1

ScaleIO Data Network 2:



Create New Data Network

Network name: scaleio_data2

VMkernel name: scaleio-data2-vmk

VLAN ID: 0

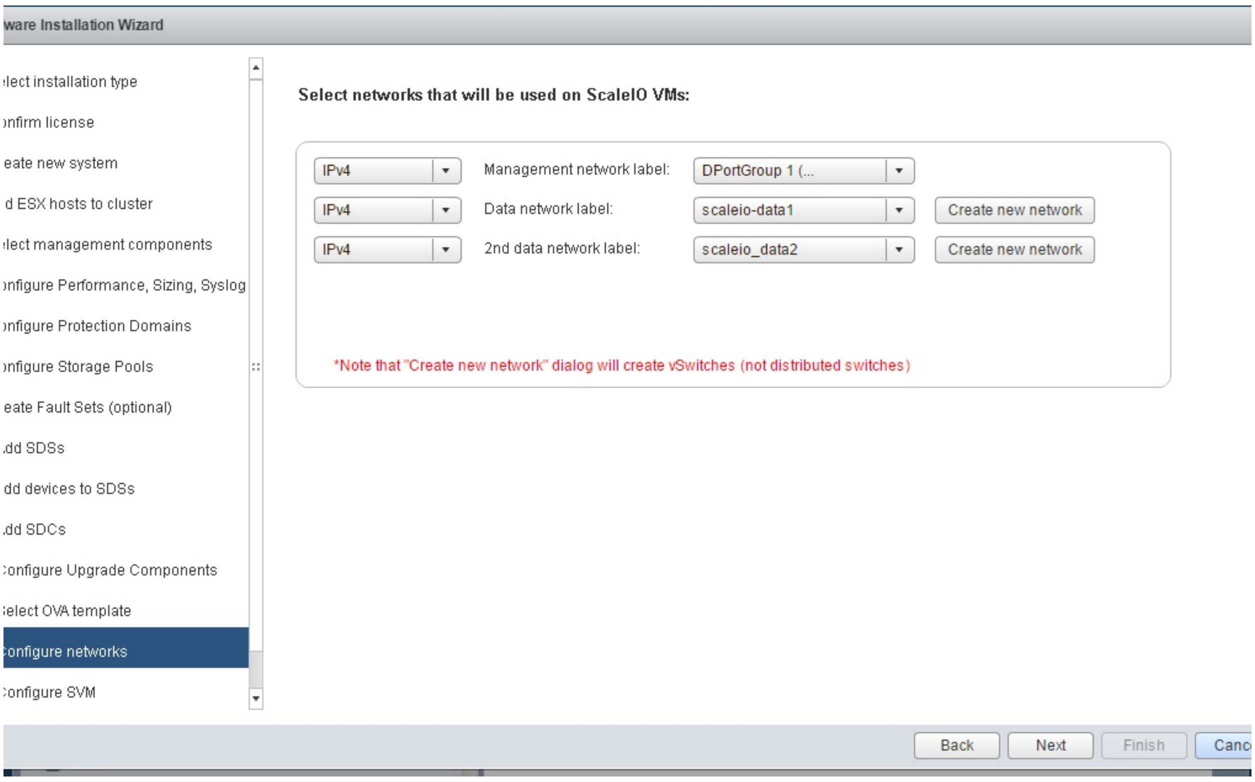
Network type: IPv4

ESX Name	Data NIC	VMkernel IP	VMkernel Subnet Mask
172.16.105.10	vmnic5 (10000MB/s) (...	192.168.40.10	255.255.255.0
172.16.105.11	vmnic5 (10000MB/s) (...	192.168.40.11	255.255.255.0
172.16.105.12	vmnic5 (10000MB/s) (...	192.168.40.12	255.255.255.0

*Note that vSwitches (not distributed switches) will be created

Figure 86 ScaleIO Data Network 2

Provide the appropriate VLAN IDs for the above networks.



ware Installation Wizard

Select networks that will be used on ScaleIO VMs:

IPv4 — Management network label: DPortGroup 1 (...

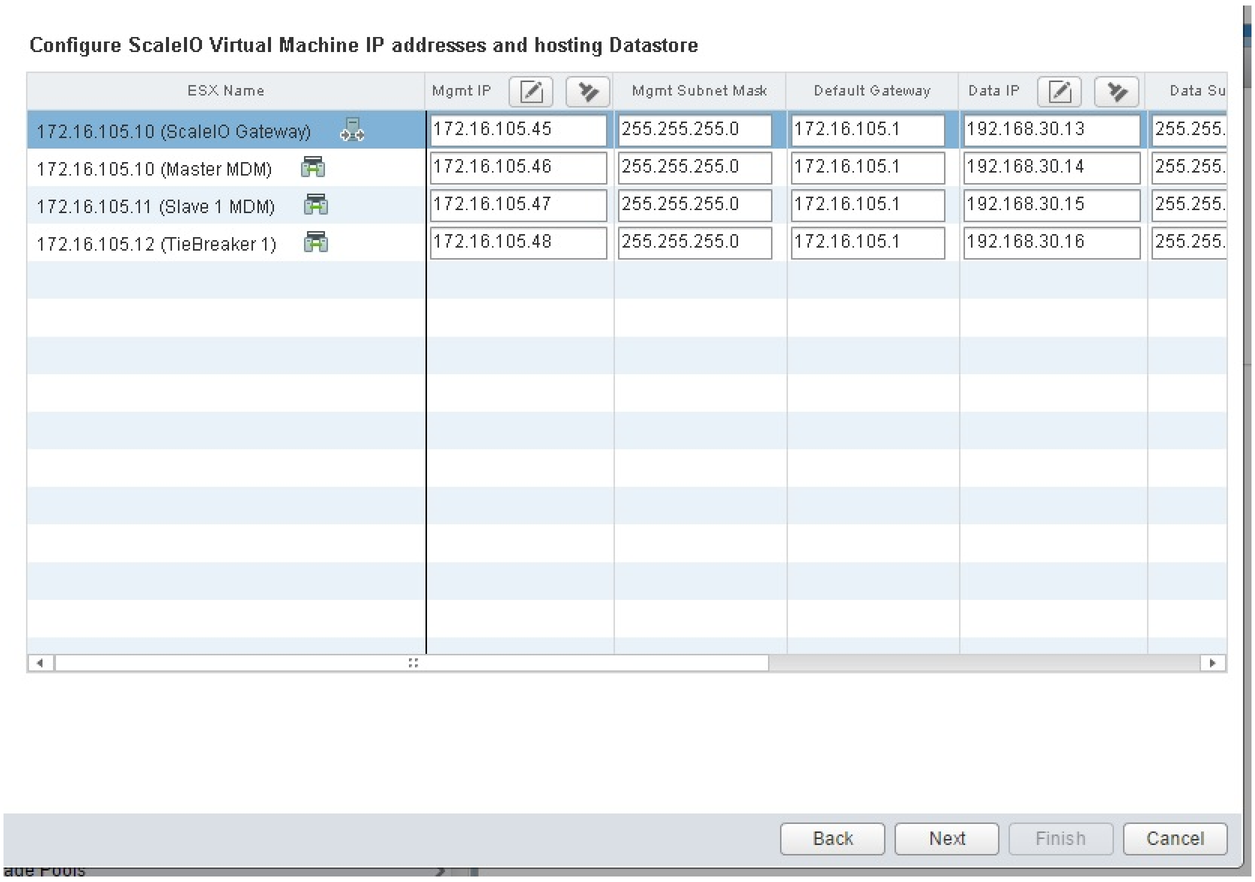
IPv4 — Data network label: scaleio-data1 — Create new network

IPv4 — 2nd data network label: scaleio_data2 — Create new network

*Note that "Create new network" dialog will create vSwitches (not distributed switches)

Figure 87 Provide VLAN IDs

7.2.11 Configure SVMs

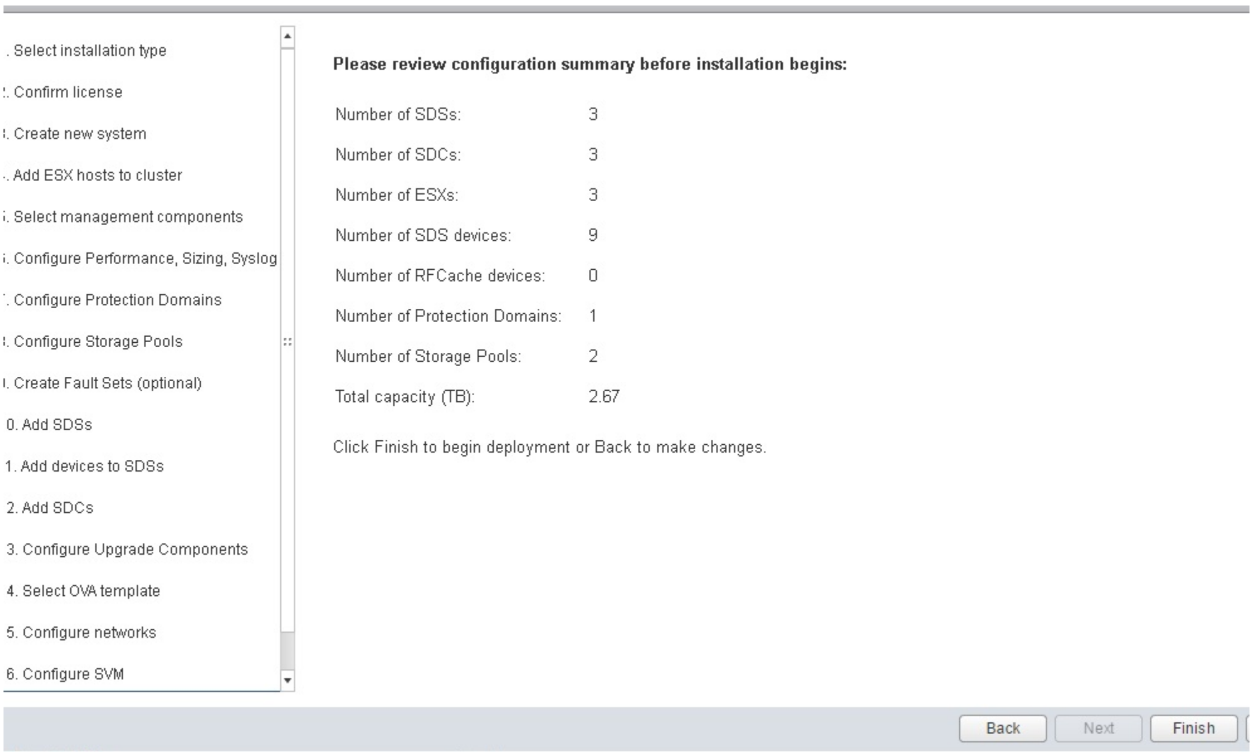


Configure ScaleIO Virtual Machine IP addresses and hosting Datastore

ESX Name	Mgmt IP	Mgmt Subnet Mask	Default Gateway	Data IP	Data Su
172.16.105.10 (ScaleIO Gateway)	172.16.105.45	255.255.255.0	172.16.105.1	192.168.30.13	255.255.
172.16.105.10 (Master MDM)	172.16.105.46	255.255.255.0	172.16.105.1	192.168.30.14	255.255.
172.16.105.11 (Slave 1 MDM)	172.16.105.47	255.255.255.0	172.16.105.1	192.168.30.15	255.255.
172.16.105.12 (TieBreaker 1)	172.16.105.48	255.255.255.0	172.16.105.1	192.168.30.16	255.255.

Figure 88 Configure SVMs

Click **Next**. Review the Configuration and click **Finish** to complete the ScaleIO Deployment.



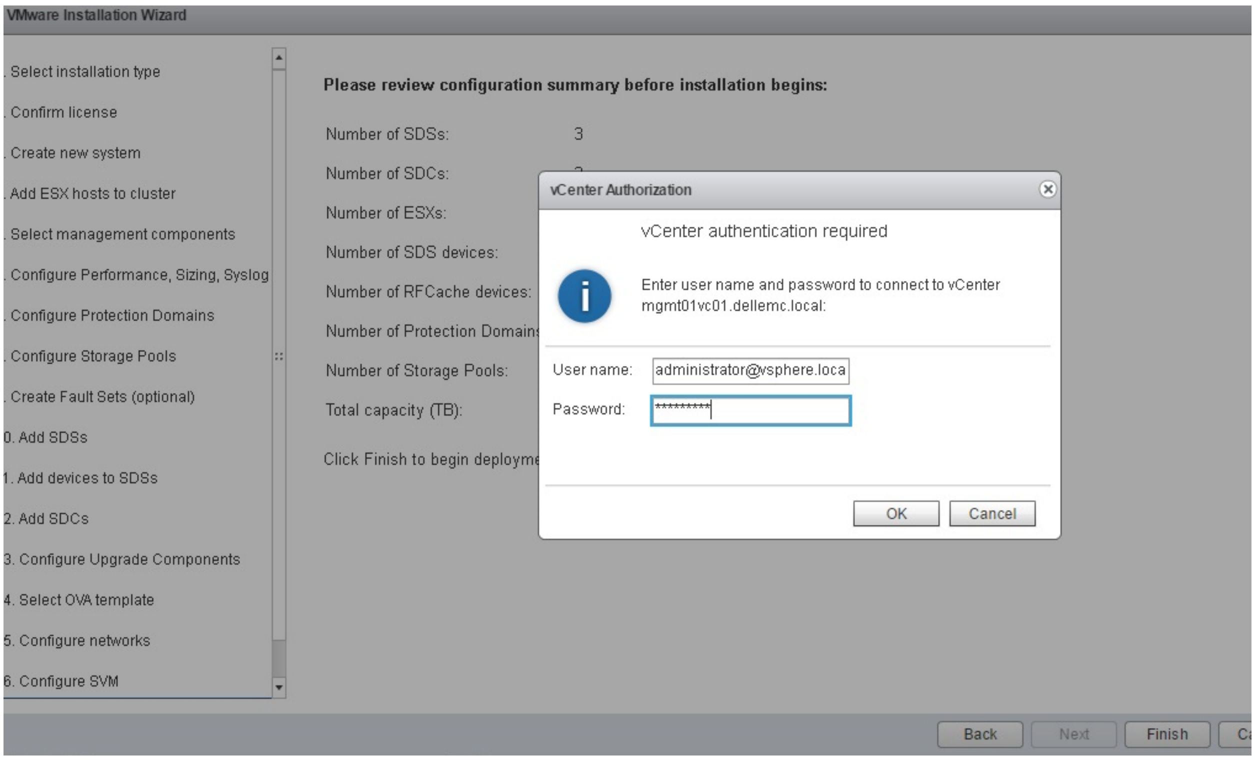
. Select installation type
:. Confirm license
:. Create new system
.. Add ESX hosts to cluster
;. Select management components
;. Configure Performance, Sizing, Syslog
'. Configure Protection Domains
:. Configure Storage Pools
I. Create Fault Sets (optional)
0. Add SDSs
1. Add devices to SDSs
2. Add SDCs
3. Configure Upgrade Components
4. Select OVA template
5. Configure networks
6. Configure SVM

Please review configuration summary before installation begins:

Number of SDSs:	3
Number of SDCs:	3
Number of ESXs:	3
Number of SDS devices:	9
Number of RFCache devices:	0
Number of Protection Domains:	1
Number of Storage Pools:	2
Total capacity (TB):	2.67

Click Finish to begin deployment or Back to make changes.

Figure 89 Review the configuration


VMware Installation Wizard

. Select installation type
. Confirm license
. Create new system
. Add ESX hosts to cluster
. Select management components
. Configure Performance, Sizing, Syslog
. Configure Protection Domains
. Configure Storage Pools
. Create Fault Sets (optional)
0. Add SDSs
1. Add devices to SDSs
2. Add SDCs
3. Configure Upgrade Components
4. Select OVA template
5. Configure networks
6. Configure SVM

Please review configuration summary before installation begins:

Number of SDSs: 3

Number of SDCs:

Number of ESXs:

Number of SDS devices:

Number of RFCache devices:

Number of Protection Domain

Number of Storage Pools:

Total capacity (TB):

Click Finish to begin deployme

vCenter Authorization

vCenter authentication required

Enter user name and password to connect to vCenter mgmt01vc01.dellemc.local:

User name: administrator@vsphere.loca

Password: *********

Figure 90 Enter Authentication

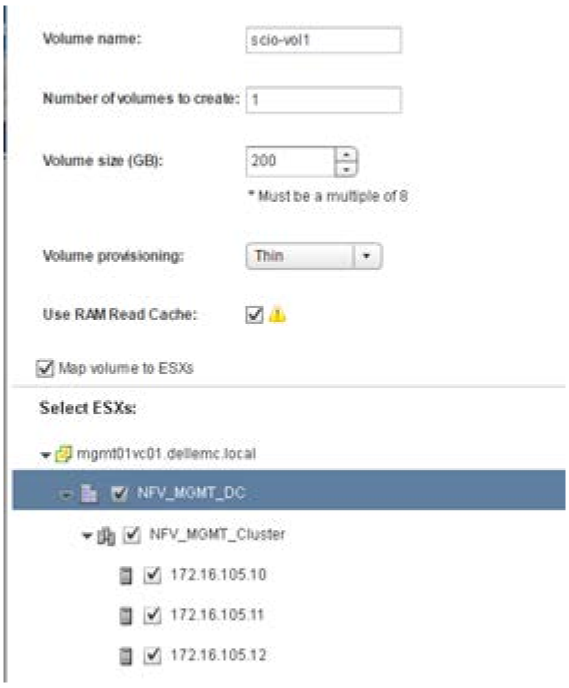
The Deployment Progress screen appears.

The ScaleIO Deployment is completed.

7.3 Creating and Mapping ScaleIO Volumes

Using the vSphere Web Client, select **EMC ScaleIO** from the home page.

In the left-hand pane, click **Storage Pools**. Any pools that have been created will be listed. Right-click a pool and select **Create Volume**.


Volume name: scio-vol1

Number of volumes to create: 1

Volume size (GB): 200

* Must be a multiple of 8

Volume provisioning: Thin

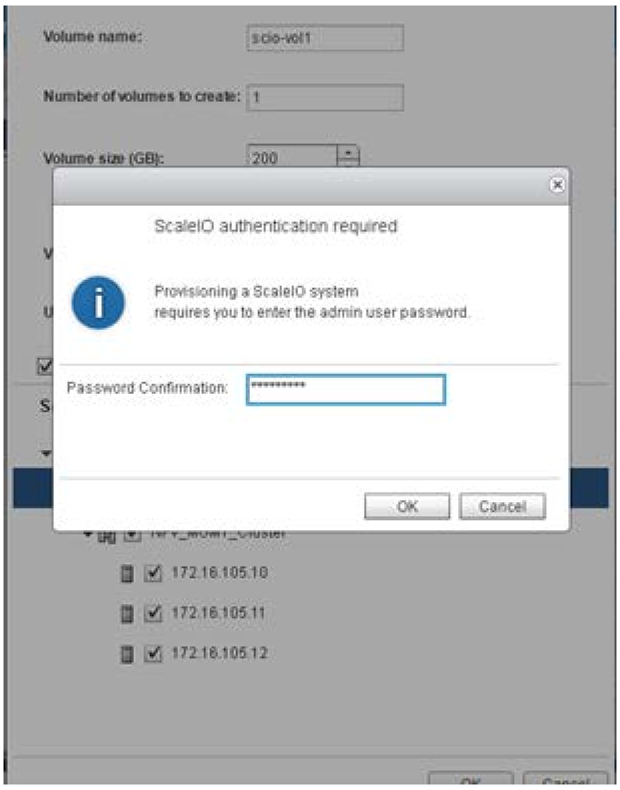
Use RAM Read Cache: ☑

☑ Map volume to ESXs

Select ESXs:

- mgmt01vc01.dellemc.local
  - ☑ NFV_MGMT_DC
    - ☑ NFV_MGMT_Cluster
      - ☑ 172.16.105.10
      - ☑ 172.16.105.11
      - ☑ 172.16.105.12

Figure 91 Select ESXs



Volume name: scio-vol1

Number of volumes to create: 1

Volume size (GB): 200

ScaleIO authentication required

Provisioning a ScaleIO system requires you to enter the admin user password.

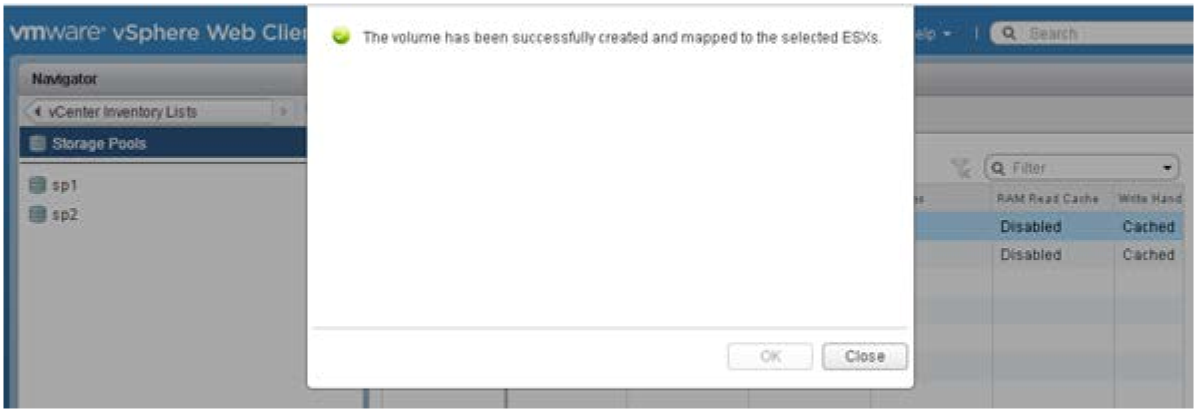
Password Confirmation: **********

Figure 92 ScaleIO authentication

Give the volume a name, configure the size, and select the SDCs (ESXi hosts) that will make up the volume.

Click **OK**.

Click **Close**.



The volume has been successfully created and mapped to the selected ESXs.

Figure 93 Volume successful created

The ScaleIO Volume is created successfully and mapped to the respective ESXi hosts.

Create a VMware datastore on ESXi hosts to access the ScaleIO Volume that was previously created.

8 Install NSX

With NSX, virtualization delivers for networking what it has already delivered for compute and storage. Three major components need to be installed in a vSphere environment to make NSX fully operational. The components are

- NSX manager
- NSX controllers
- NSX edge gateway services

For additional information, please check the following: (http://pubs.vmware.com/NSX-62/topic/com.vmware.ICbase/PDF/nsx_62_install.pdf)

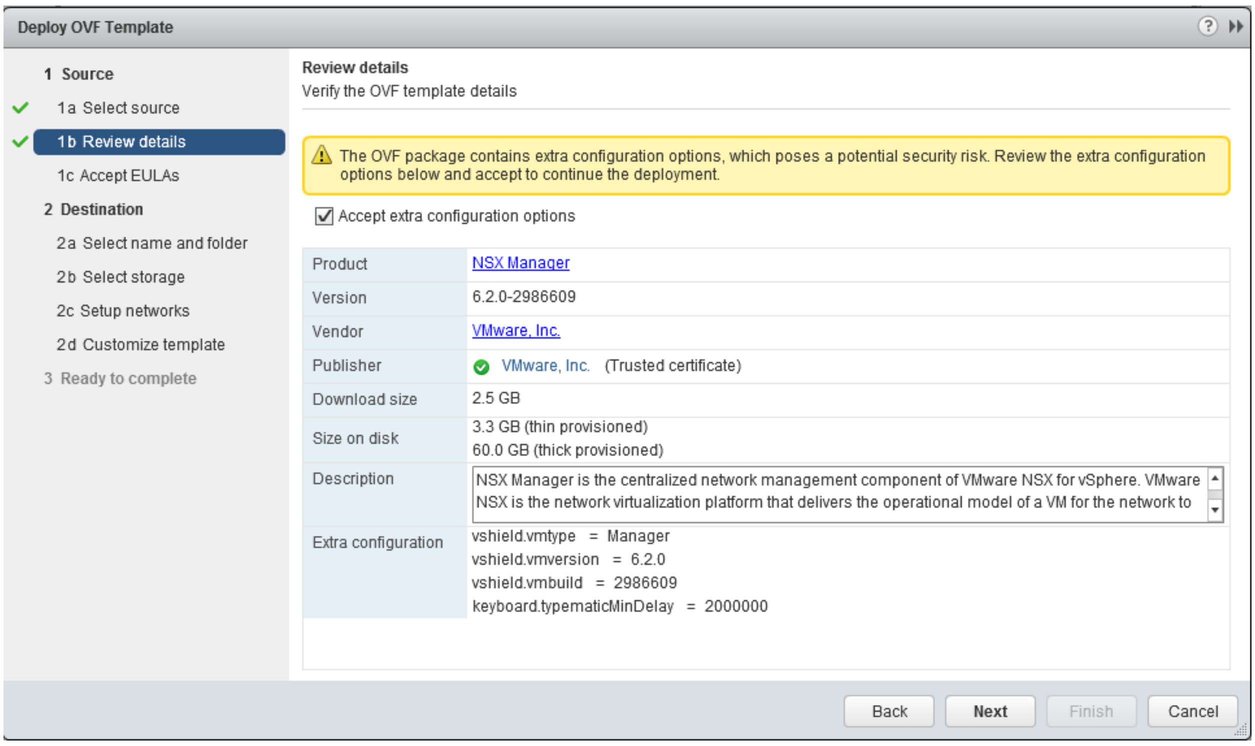
8.1 Deploy NSX manager

Even though NSX has various components and completing the installation requires multiple steps, 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 in which to install NSX manager and select **Deploy OVF template**.

Locate the NSX manager appliance OVA file and click **Next**, Select the check box: **Accept extra configuration options** and click **Next**.

Provide the IP address according to your environment.



Review details
Verify the OVF template details

The OVF package contains extra configuration options, which poses a potential security risk. Review the extra configuration options below and accept to continue the deployment.

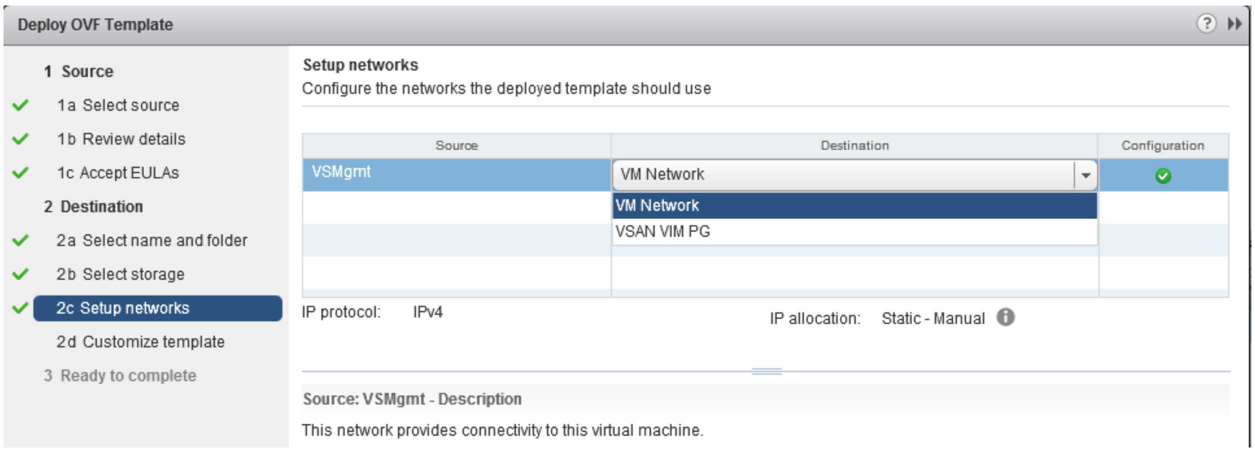
☑ Accept extra configuration options

Product	NSX Manager
Version	6.2.0-2986609
Vendor	VMware, Inc.
Publisher	✓ VMware, Inc. (Trusted certificate)
Download size	2.5 GB
Size on disk	3.3 GB (thin provisioned) 60.0 GB (thick provisioned)
Description	NSX Manager is the centralized network management component of VMware NSX for vSphere. VMware NSX is the network virtualization platform that delivers the operational model of a VM for the network to

Extra configuration	vshield.vmtype = Manager
	vshield.vmversion = 6.2.0
	vshield.vmbuild = 2986609
	keyboard.typematicMinDelay = 2000000

Figure 94 Review the OVF template details

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



Setup networks
Configure the networks the deployed template should use

Source	Destination	Configuration
VSMgmt	VM Network	✓

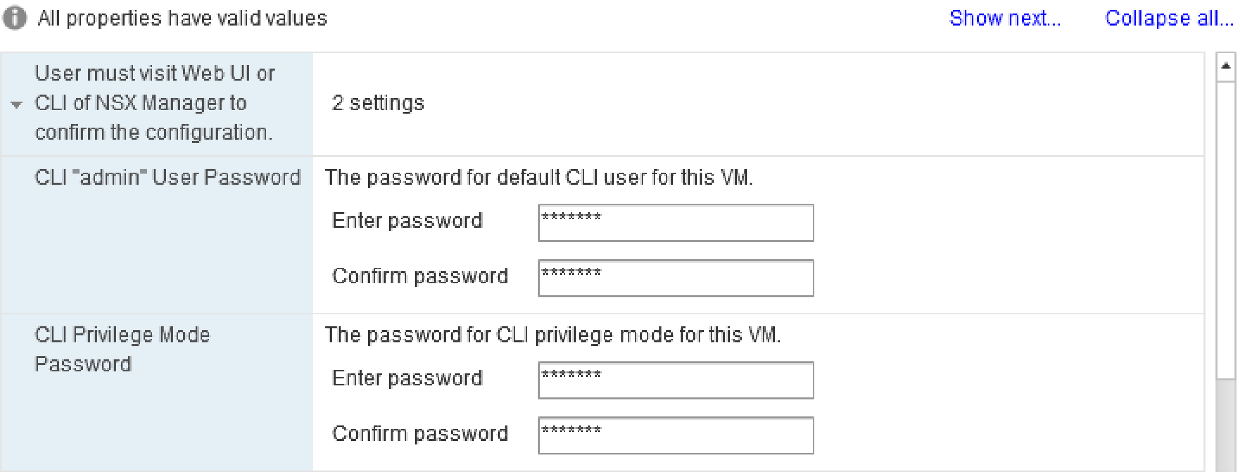
VM Network
VSAN VIM PG

IP protocol: IPv4 IP allocation: Static - Manual

Source: VSMgmt - Description
This network provides connectivity to this virtual machine.

Figure 95 Setup networks

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

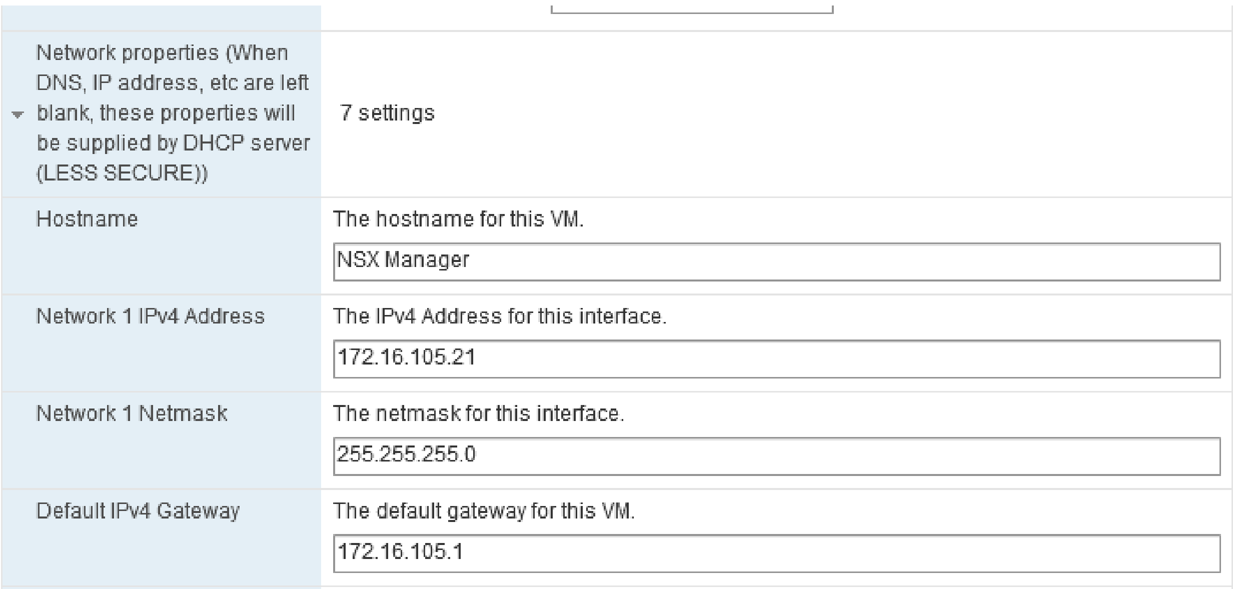


All properties have valid values

User must visit Web UI or CLI of NSX Manager to confirm the configuration.	2 settings
CLI "admin" User Password	The password for default CLI user for this VM. Enter password ******* Confirm password *******
CLI Privilege Mode Password	The password for CLI privilege mode for this VM. Enter password ******* Confirm password *******

Figure 96 Configure passwords

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



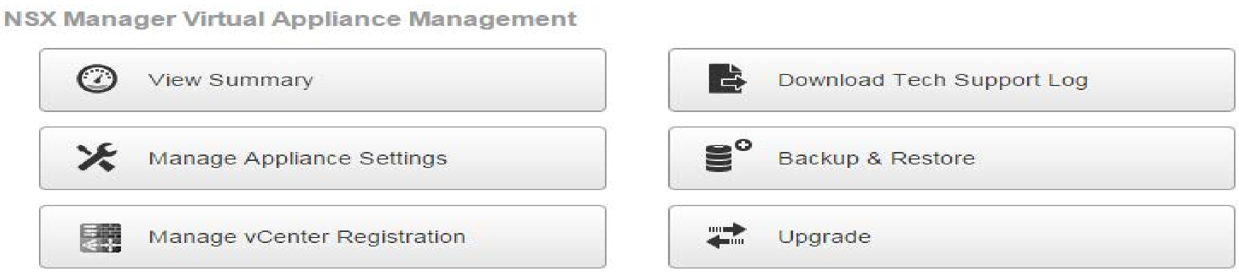
Network properties (When DNS, IP address, etc are left blank, these properties will be supplied by DHCP server (LESS SECURE))	7 settings
Hostname	The hostname for this VM. NSX Manager
Network 1 IPv4 Address	The IPv4 Address for this interface. 172.16.105.21
Network 1 Netmask	The netmask for this interface. 255.255.255.0
Default IPv4 Gateway	The default gateway for this VM. 172.16.105.1

Figure 97 Configure network properties

Verify all configurations are properly configured, select **Turn on VM**.

8.2 Register NSX manager with vCenter

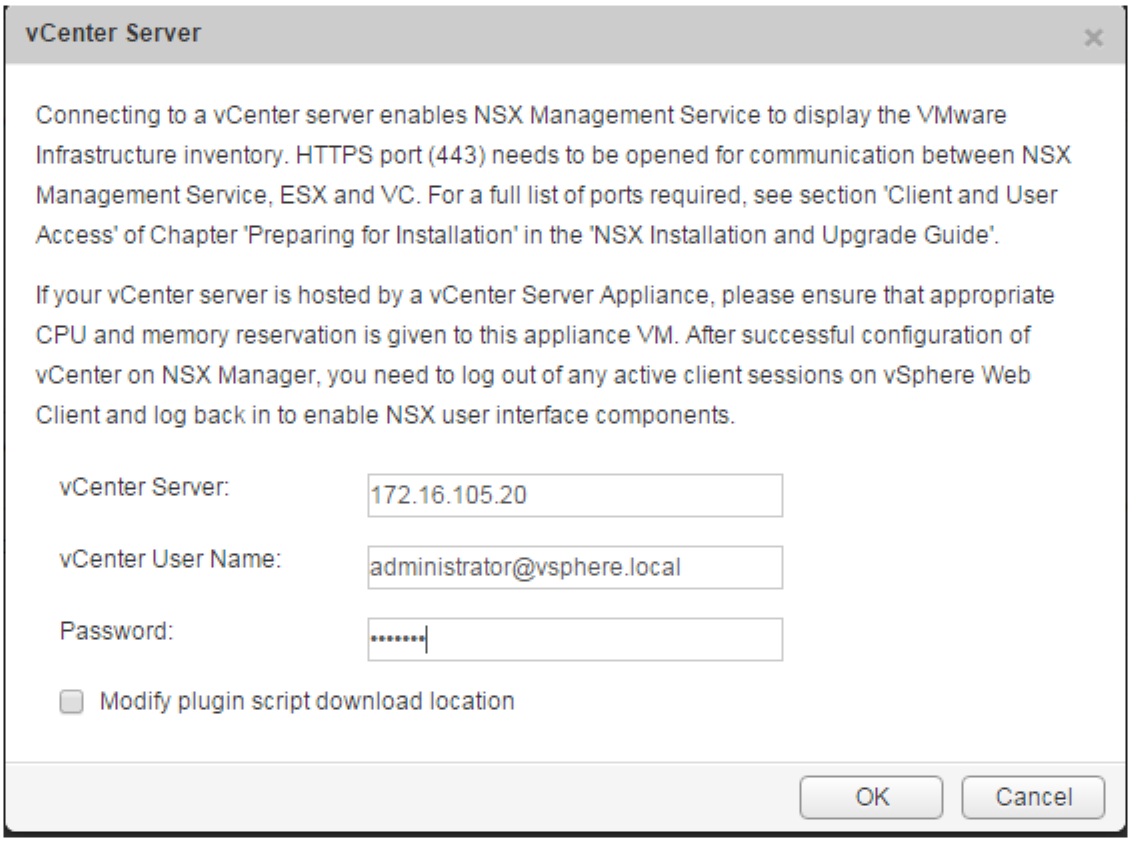
Open NSX manager by entering the NSX manager IP in a browser and use the login credentials that were configured during the NSX manager deployment. Select **Manage vCenter Registration**.



NSX Manager Virtual Appliance Management
View Summary
Manage Appliance Settings
Manage vCenter Registration
Download Tech Support Log
Backup & Restore
Upgrade

Figure 98 NSX Manager Virtual Appliance Management

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



vCenter Server

Connecting to a vCenter server enables NSX Management Service to display the VMware Infrastructure inventory. HTTPS port (443) needs to be opened for communication between NSX Management Service, ESX and VC. For a full list of ports required, see section 'Client and User Access' of Chapter 'Preparing for Installation' in the 'NSX Installation and Upgrade Guide'.

If your vCenter server is hosted by a vCenter Server Appliance, please ensure that appropriate CPU and memory reservation is given to this appliance VM. After successful configuration of vCenter on NSX Manager, you need to log out of any active client sessions on vSphere Web Client and log back in to enable NSX user interface components.

vCenter Server: 172.16.105.20

vCenter User Name: administrator@vsphere.local

Password: •••••••

☐ Modify plugin script download location

Figure 99 vCenter Server authentication

Logout and Login to the VMware vSphere web client. A new Icon appears as shown below confirming the NSX registration is successful.

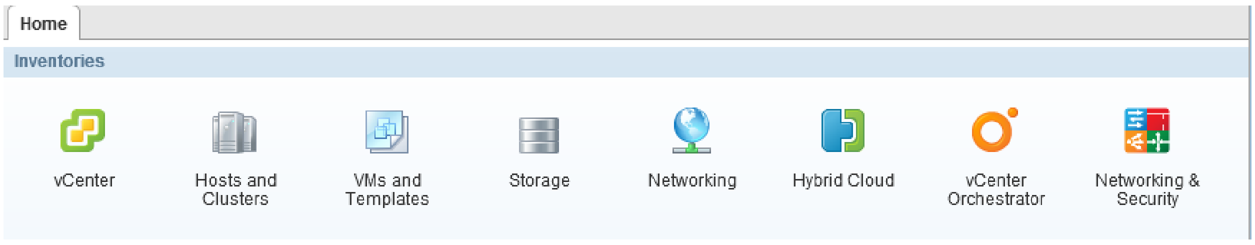
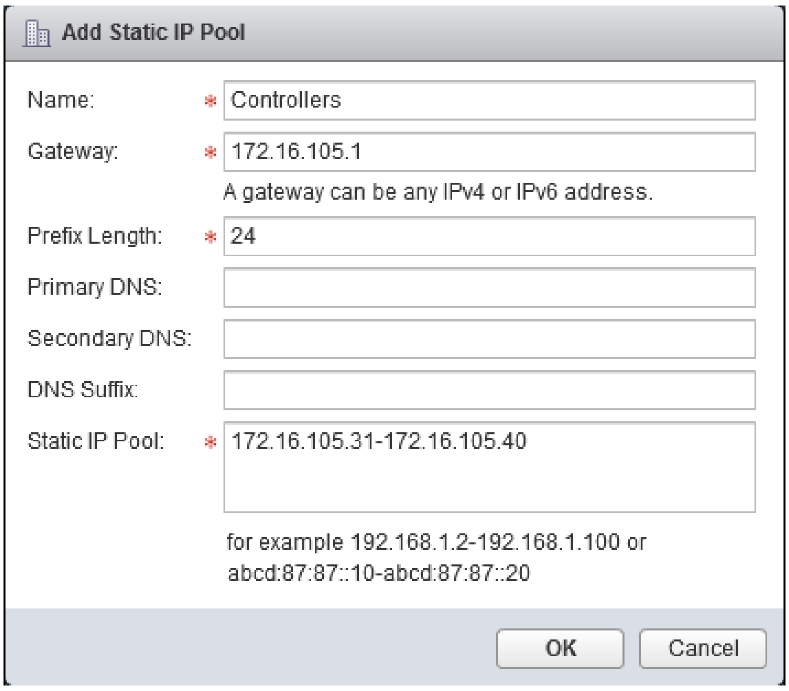


Figure 100 Successful NSX registration

8.3 Deploy NSX controllers

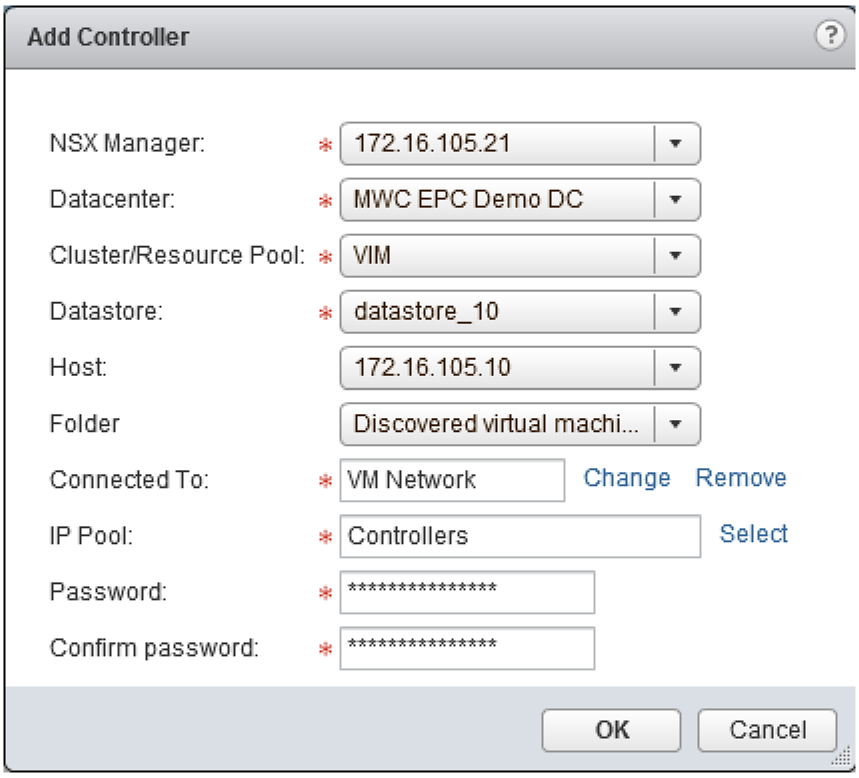
To deploy the NSX controllers navigate to Home → Networking & Security → Installation and select Management tab. Click on (+) sign under NSX controller nodes. Fill out all the details in the Add Controller dialog box.

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



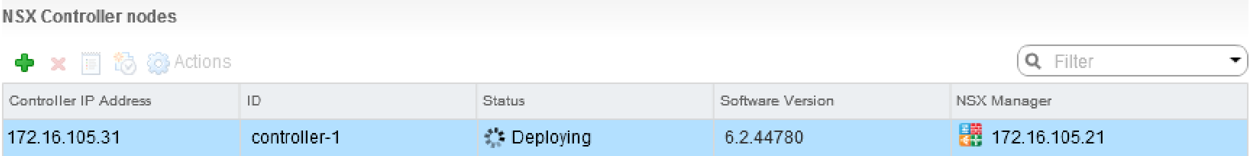
Name: *	Controllers
Gateway: *	172.16.105.1
	A gateway can be any IPv4 or IPv6 address.
Prefix Length: *	24
Primary DNS:	
Secondary DNS:	
DNS Suffix:	
Static IP Pool: *	172.16.105.31-172.16.105.40
	for example 192.168.1.2-192.168.1.100 or abcd:87:87::10-abcd:87:87::20

Figure 101 Add static IP pool



NSX Manager: *	172.16.105.21
Datacenter: *	MWC EPC Demo DC
Cluster/Resource Pool: *	VIM
Datastore: *	datastore_10
Host:	172.16.105.10
Folder	Discovered virtual machi...
Connected To: *	VM Network
IP Pool: *	Controllers
Password: *	***************
Confirm password: *	***************

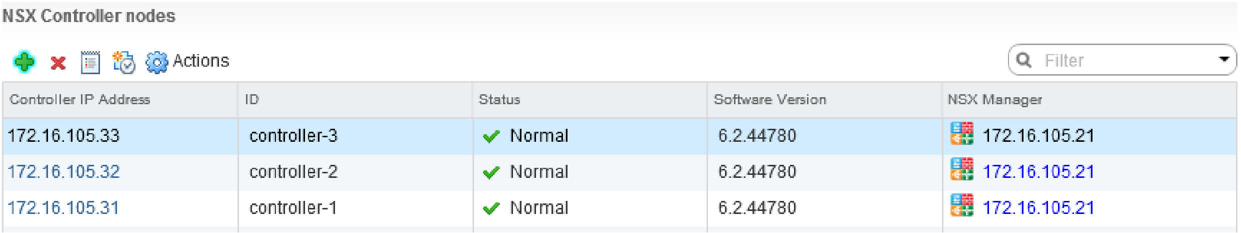
Figure 102 Add controller



Controller IP Address	ID	Status	Software Version	NSX Manager
172.16.105.31	controller-1	Deploying	6.2.44780	172.16.105.21

Figure 103 Deployed NSX controller

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



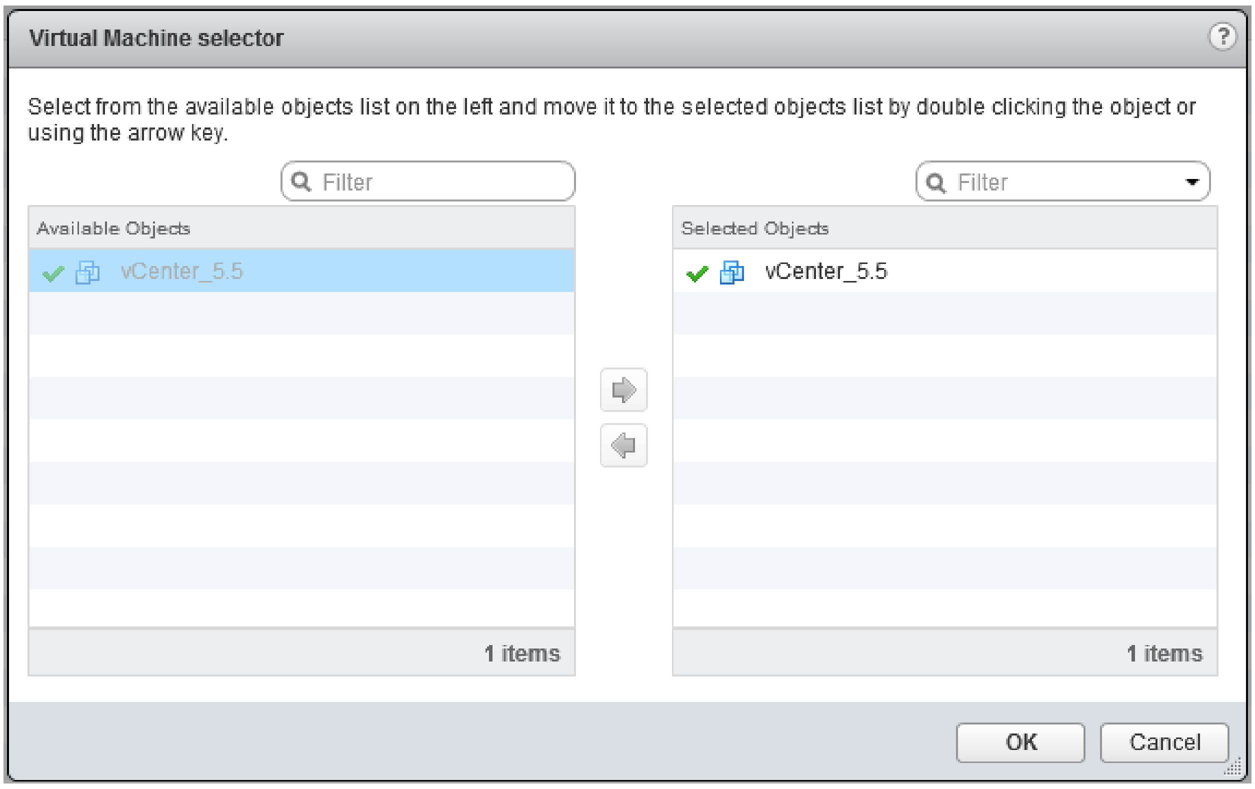
Controller IP Address	ID	Status	Software Version	NSX Manager
172.16.105.33	controller-3	✓ Normal	6.2.44780	172.16.105.21
172.16.105.32	controller-2	✓ Normal	6.2.44780	172.16.105.21
172.16.105.31	controller-1	✓ Normal	6.2.44780	172.16.105.21

Figure 104 Deploy additional NSX controllers

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

8.4 Exclude VMs from Firewall

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



Virtual Machine selector

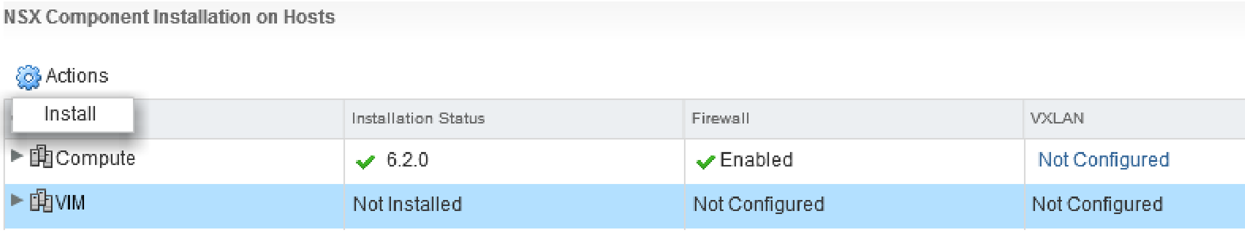
Select from the available objects list on the left and move it to the selected objects list by double clicking the object or using the arrow key.

Available Objects	Selected Objects
✓ vCenter_5.5	✓ vCenter_5.5
1 items	1 items

Figure 105 Exclude the vCenter VM from firewall protection

8.5 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.



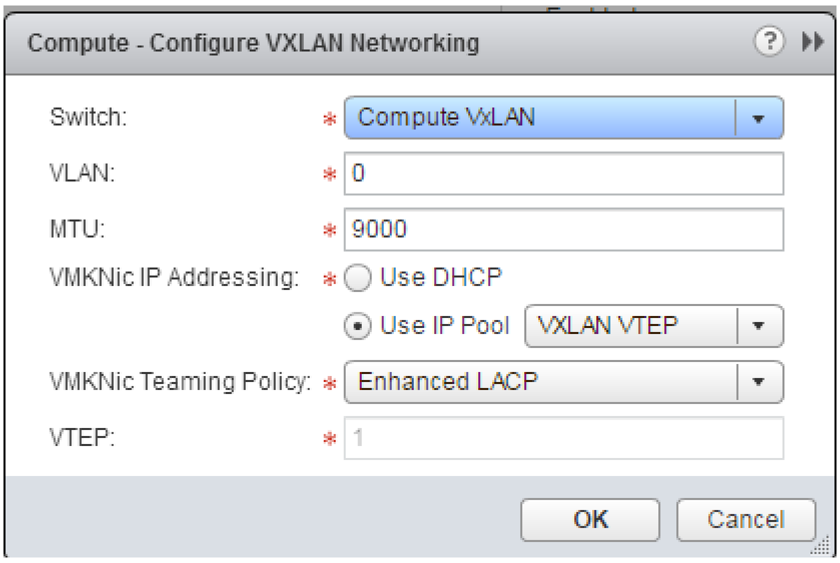
NSX Component Installation on Hosts

	Installation Status	Firewall	VXLAN
▶ Compute	✓ 6.2.0	✓ Enabled	Not Configured
▶ VIM	Not Installed	Not Configured	Not Configured

Figure 106 NSX component installation

8.6 Configure VXLAN

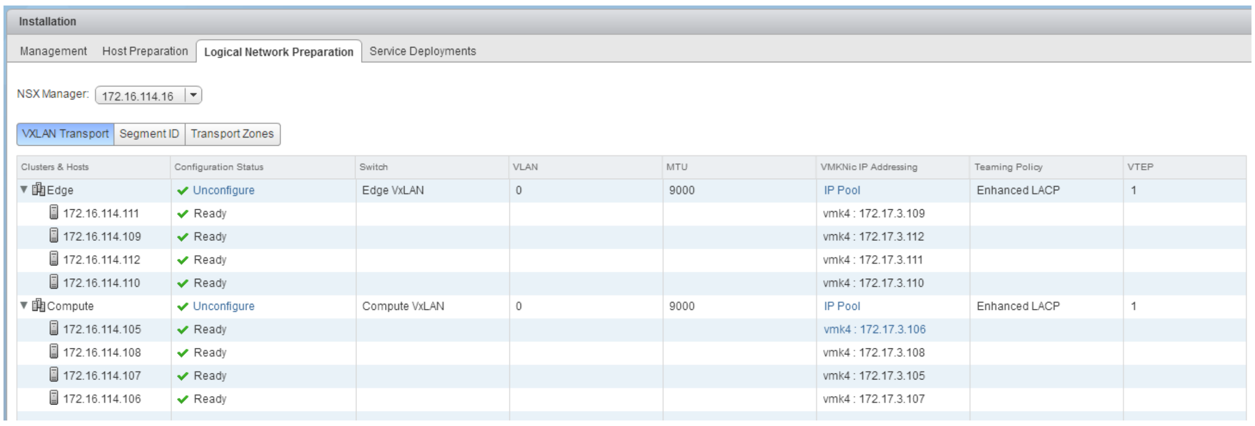
Determine the Vlan and Pool of IP address for VXLAN VTEPs. Navigate to **Home → Networking & Security → Installations → Host Preparation**. Under the VXLAN column, select **Configure VXLAN**. Create a pool similar to the NSX controller for VTEPs and assign the pool here.



Compute - Configure VXLAN Networking

Switch: *	Compute VxLAN
VLAN: *	0
MTU: *	9000
VMKNic IP Addressing: *	○ Use DHCP ● Use IP Pool VXLAN VTEP
VMKNic Teaming Policy: *	Enhanced LACP
VTEP: *	1

Figure 107 Configure VXLAN



Installation

Management | Host Preparation | Logical Network Preparation | Service Deployments

NSX Manager: 172.16.114.16

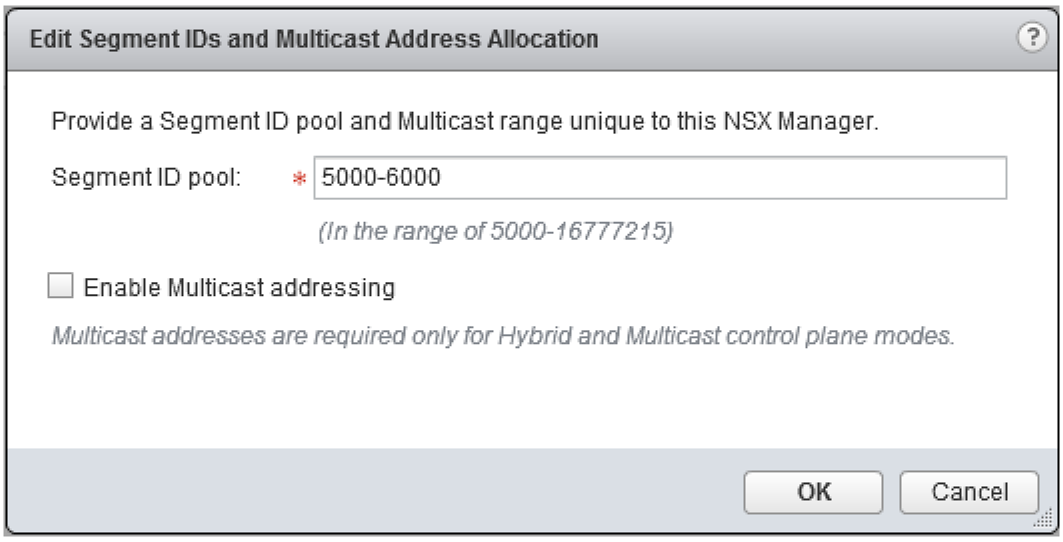
VXLAN Transport | Segment ID | Transport Zones

Clusters & Hosts	Configuration Status	Switch	VLAN	MTU	VMKNic IP Addressing	Teaming Policy	VTEP
Edge	✓ Unconfigure	Edge VxLAN	0	9000	IP Pool	Enhanced LACP	1
172.16.114.111	✓ Ready				vmk4 : 172.17.3.109		
172.16.114.109	✓ Ready				vmk4 : 172.17.3.112		
172.16.114.112	✓ Ready				vmk4 : 172.17.3.111		
172.16.114.110	✓ Ready				vmk4 : 172.17.3.110		
Compute	✓ Unconfigure	Compute VxLAN	0	9000	IP Pool	Enhanced LACP	1
172.16.114.105	✓ Ready				vmk4 : 172.17.3.106		
172.16.114.108	✓ Ready				vmk4 : 172.17.3.108		
172.16.114.107	✓ Ready				vmk4 : 172.17.3.105		
172.16.114.106	✓ Ready				vmk4 : 172.17.3.107		

Figure 108 VXLAN preparation

8.7 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 practically having 1000 segments is enough. To configure this, navigate to **Home → Networking & Security → Installations → Logical Network Preparation → Segment ID** and click **Edit**.



Edit Segment IDs and Multicast Address Allocation

Provide a Segment ID pool and Multicast range unique to this NSX Manager.

Segment ID pool: * 5000-6000

(In the range of 5000-16777215)

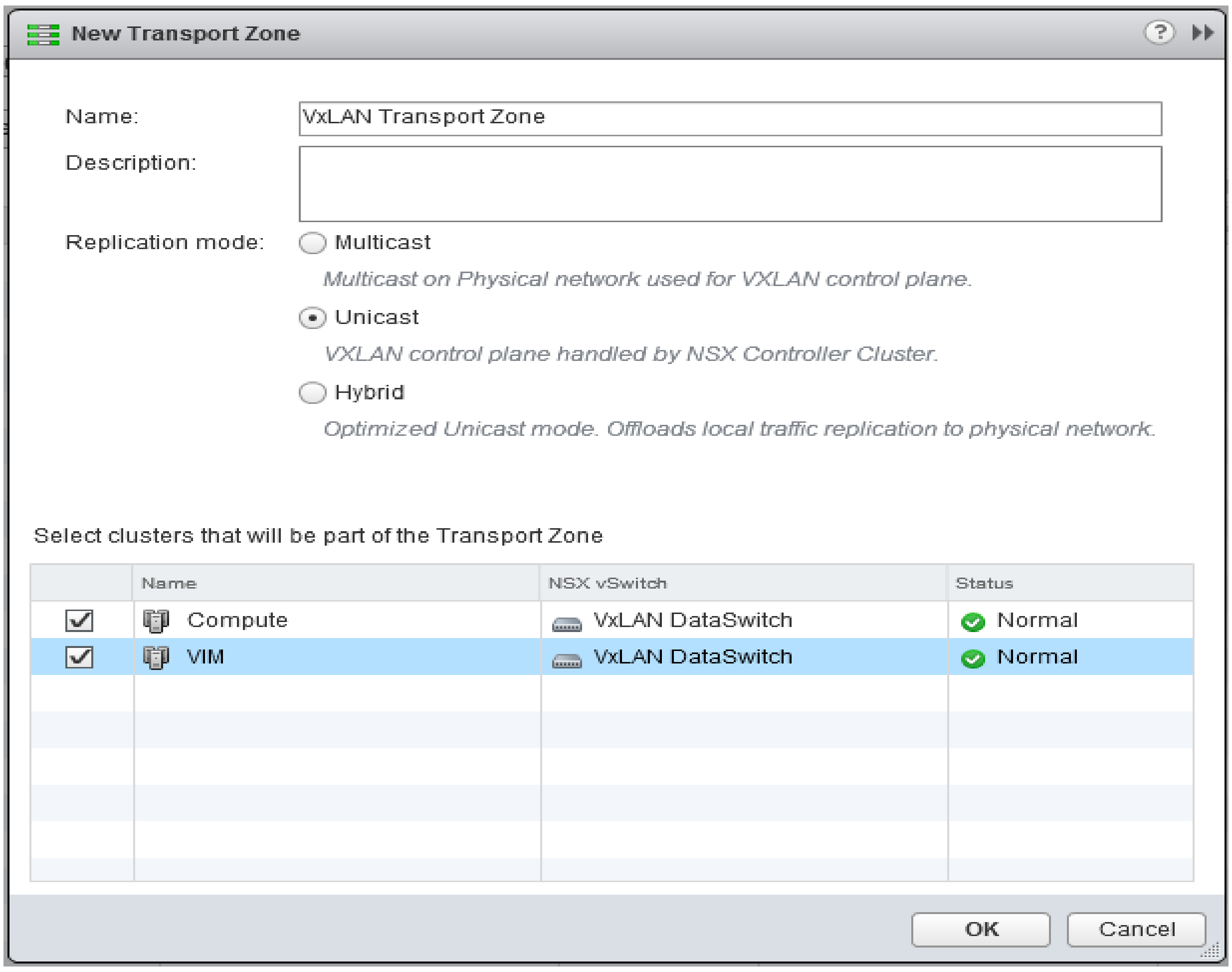
□ Enable Multicast addressing

Multicast addresses are required only for Hybrid and Multicast control plane modes.

Figure 109 Edit Segment IDs

8.8 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 only do routing within logical switch in a single transport zone. The transport zone should be designed with this in mind. In this setup, the transport zone is spanned across both Compute and VIM.



Name: VxLAN Transport Zone

Description:

Replication mode:

○ Multicast

Multicast on Physical network used for VXLAN control plane.

● Unicast

VXLAN control plane handled by NSX Controller Cluster.

○ Hybrid

Optimized Unicast mode. Offloads local traffic replication to physical network.

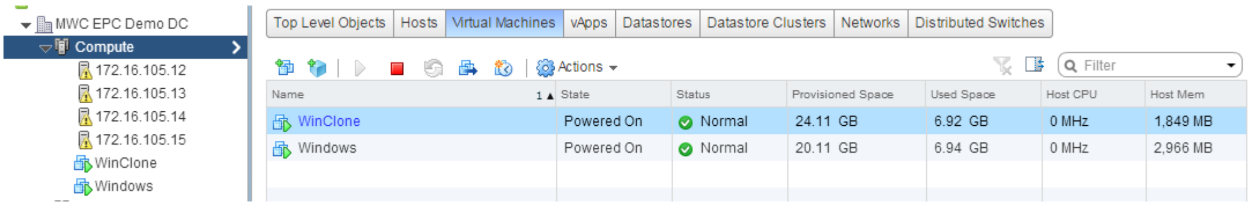
Select clusters that will be part of the Transport Zone

	Name	NSX vSwitch	Status
☑	Compute	VxLAN DataSwitch	✓ Normal
☑	VIM	VxLAN DataSwitch	✓ Normal

Figure 110 New transport zone

8.9 Create logical switch

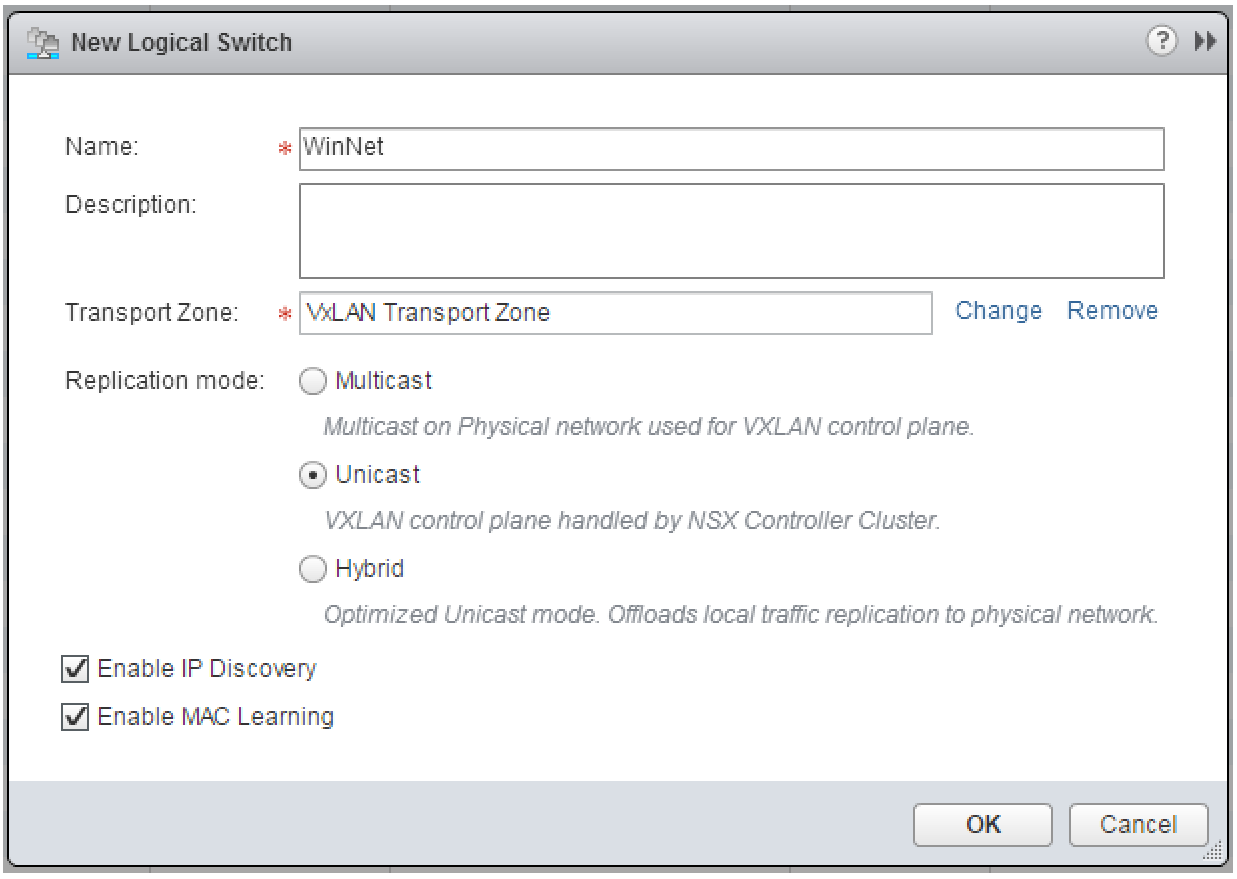
A logical switch reproduces switching functionality in a virtual environment completely decoupled from underlying hardware. When we have two logical switches as part of two different logical networks, we need a distributed logical router to communicate between the logical networks. To demonstrate logical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



Name	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
WinClone	Powered On	✓ Normal	24.11 GB	6.92 GB	0 MHz	1,849 MB
Windows	Powered On	✓ Normal	20.11 GB	6.94 GB	0 MHz	2,966 MB

Figure 111 Create logical switch

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.



New Logical Switch

Name: * WinNet

Description:

Transport Zone: * VXLAN Transport Zone Change Remove

Replication mode:

○ Multicast

Multicast on Physical network used for VXLAN control plane.

● Unicast

VXLAN control plane handled by NSX Controller Cluster.

○ Hybrid

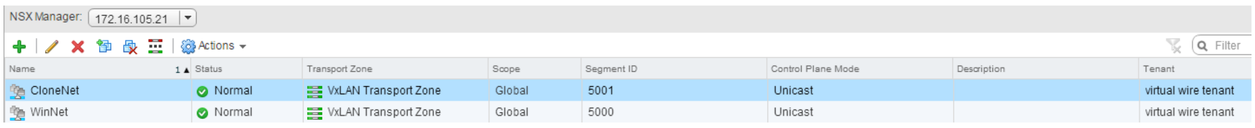
Optimized Unicast mode. Offloads local traffic replication to physical network.

☑ Enable IP Discovery

☑ Enable MAC Learning

OK Cancel

Figure 112 Create a new logical switch

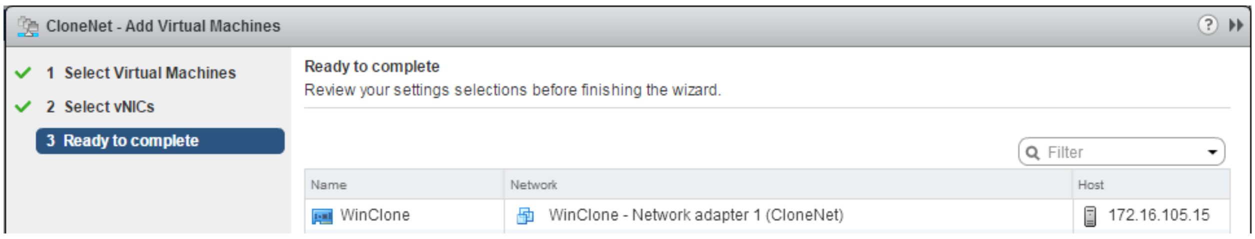


NSX Manager: 172.16.105.21

Name	Status	Transport Zone	Scope	Segment ID	Control Plane Mode	Description	Tenant
CloneNet	Normal	VxLAN Transport Zone	Global	5001	Unicast		virtual wire tenant
WinNet	Normal	VxLAN Transport Zone	Global	5000	Unicast		virtual wire tenant

Figure 113 New logical switch (WinNet)

Click on add Virtual machine to assign the logical network to respective VM NIC ports.



CloneNet - Add Virtual Machines

✓ 1 Select Virtual Machines

✓ 2 Select vNICs

3 Ready to complete

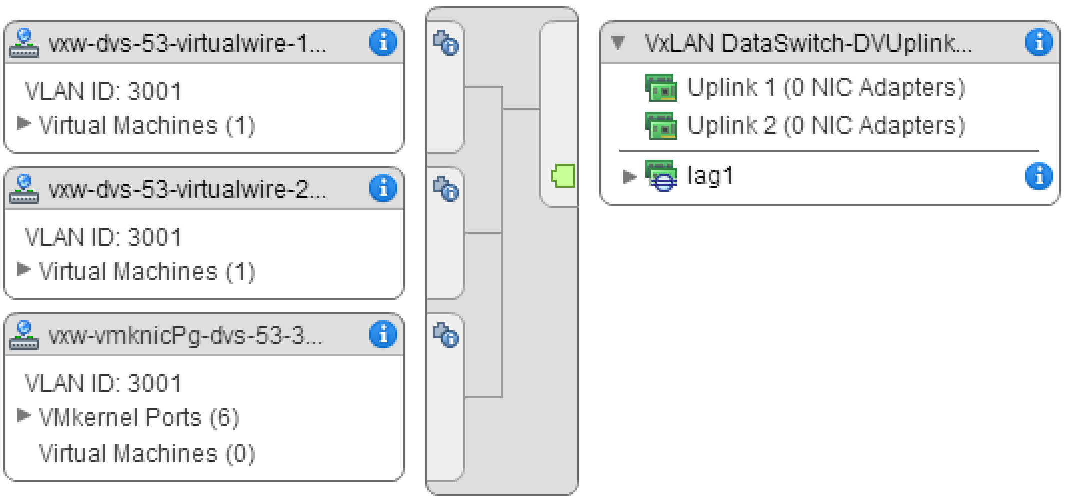
Ready to complete

Review your settings selections before finishing the wizard.

Name	Network	Host
WinClone	WinClone - Network adapter 1 (CloneNet)	172.16.105.15

Figure 114 Assign logical network to VM NIC ports

Once the VM to logical switch assignment is done, the distributed vSwitch portgroup will look as follows.



vxw-dvs-53-virtualwire-1...
VLAN ID: 3001
▶ Virtual Machines (1)

vxw-dvs-53-virtualwire-2...
VLAN ID: 3001
▶ Virtual Machines (1)

vxw-vmknicPg-dvs-53-3...
VLAN ID: 3001
▶ VMkernel Ports (6)
Virtual Machines (0)

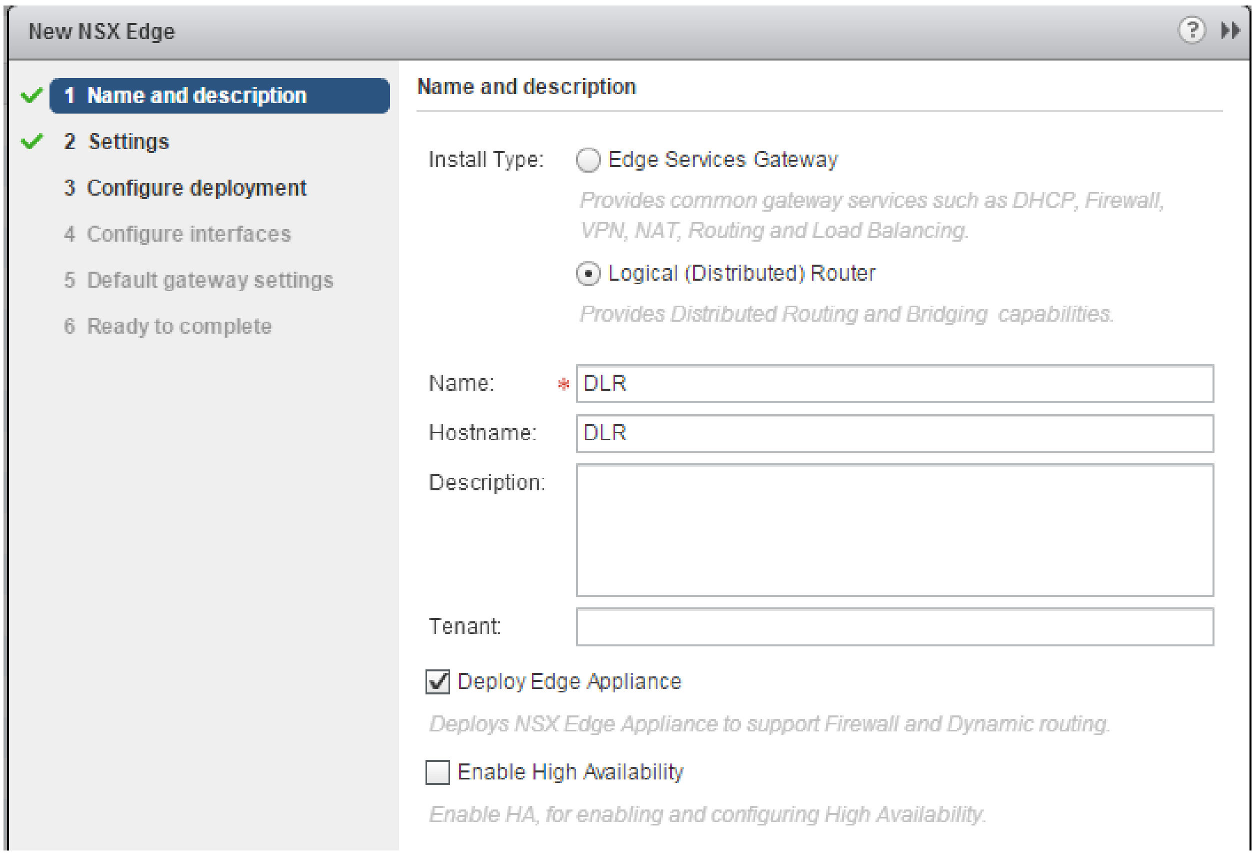
▼ VxLAN DataSwitch-DVUplink...
Uplink 1 (0 NIC Adapters)
Uplink 2 (0 NIC Adapters)
▶ lag1

Figure 115 Distributed vSwitch portgroup

8.10 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. The 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 (**+**).



Name and description

Install Type: ○ Edge Services Gateway

Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.

● Logical (Distributed) Router

Provides Distributed Routing and Bridging capabilities.

Name: * DLR

Hostname: DLR

Description:

Tenant:

☑ Deploy Edge Appliance

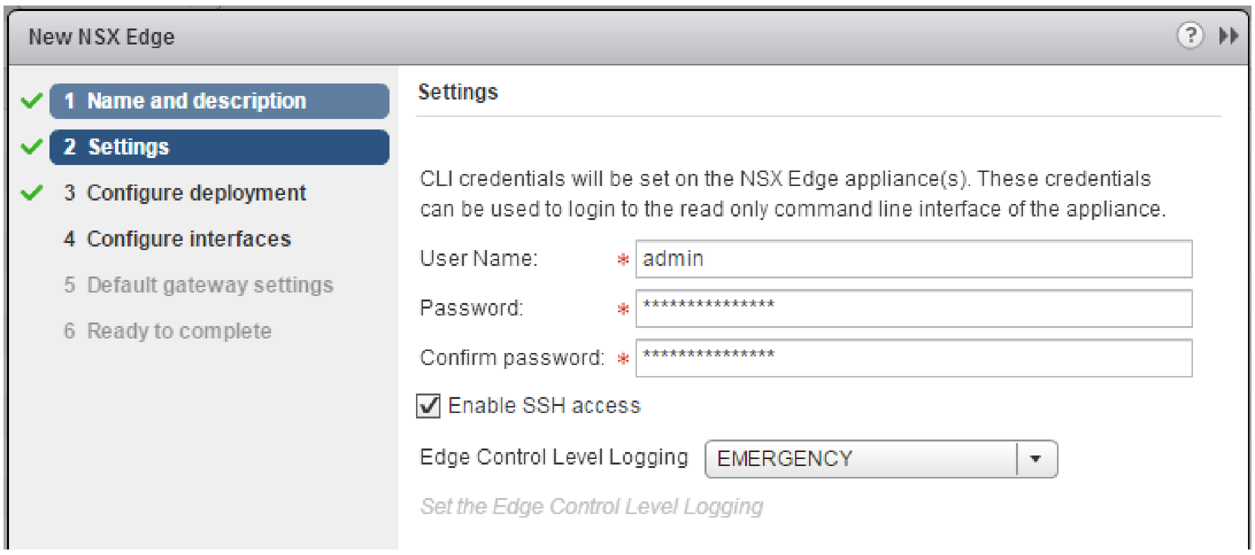
Deploys NSX Edge Appliance to support Firewall and Dynamic routing.

□ Enable High Availability

Enable HA, for enabling and configuring High Availability.

Figure 116 Deploy Distributed Logical Router

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



Settings

CLI credentials will be set on the NSX Edge appliance(s). These credentials can be used to login to the read only command line interface of the appliance.

User Name: * admin

Password: * ***************

Confirm password: * ***************

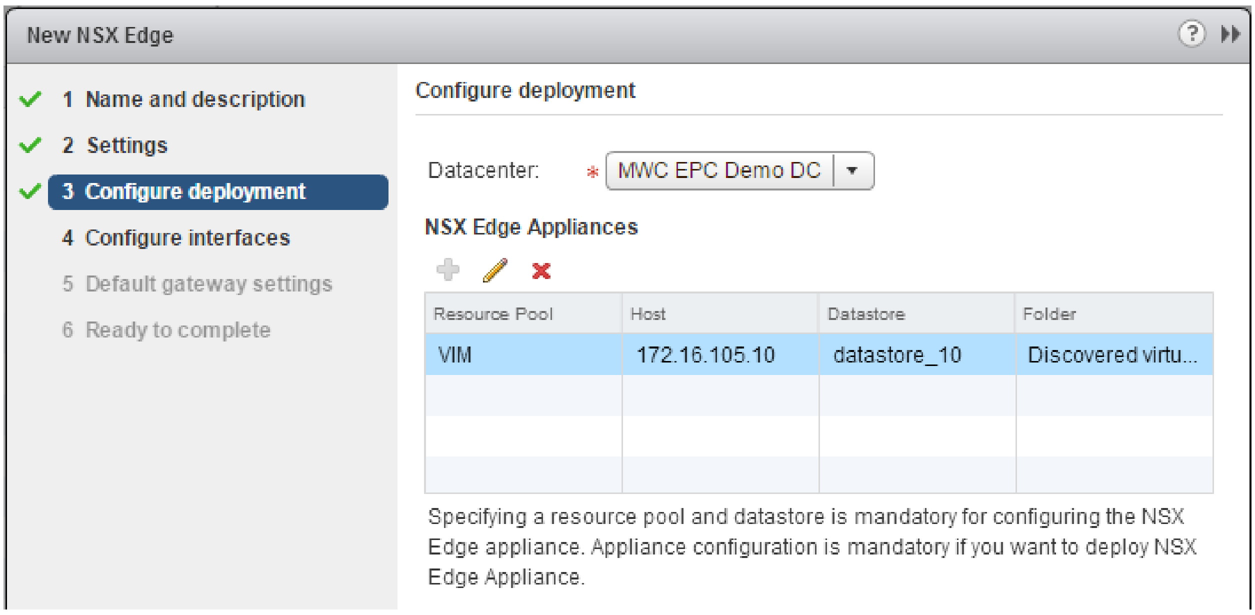
☑ Enable SSH access

Edge Control Level Logging: EMERGENCY

Set the Edge Control Level Logging

Figure 117 Configure password for DLR

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



Configure deployment

Datacenter: * MWC EPC Demo DC

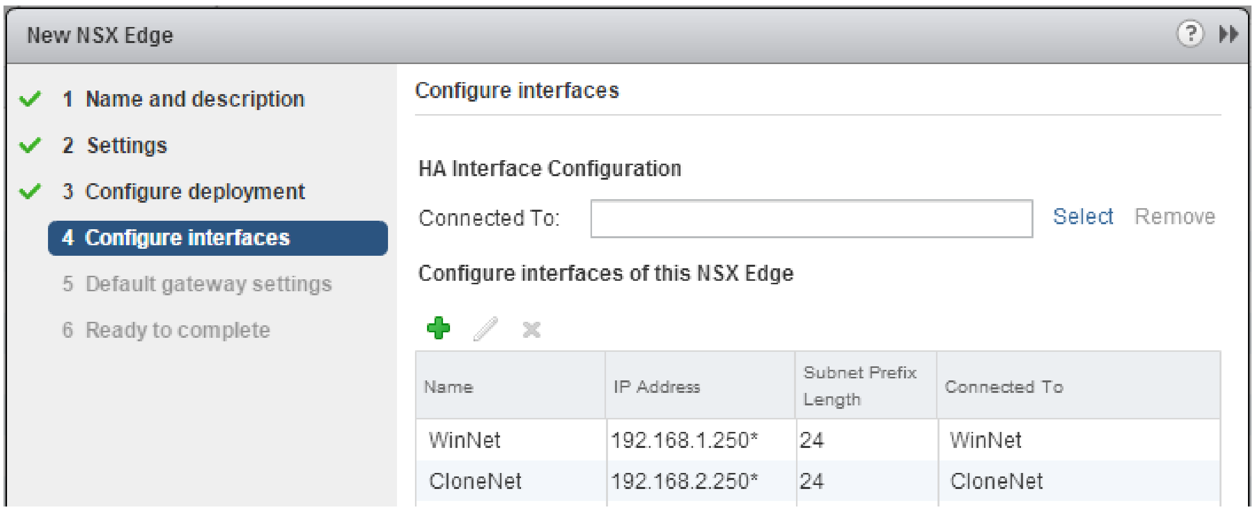
NSX Edge Appliances

Resource Pool	Host	Datastore	Folder
VIM	172.16.105.10	datastore_10	Discovered virtu...

Specifying a resource pool and datastore is mandatory for configuring the NSX Edge appliance. Appliance configuration is mandatory if you want to deploy NSX Edge Appliance.

Figure 118 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.



Configure interfaces

HA Interface Configuration

Connected To:

Configure interfaces of this NSX Edge

Name	IP Address	Subnet Prefix Length	Connected To
WinNet	192.168.1.250*	24	WinNet
CloneNet	192.168.2.250*	24	CloneNet

Figure 119 Configure interfaces

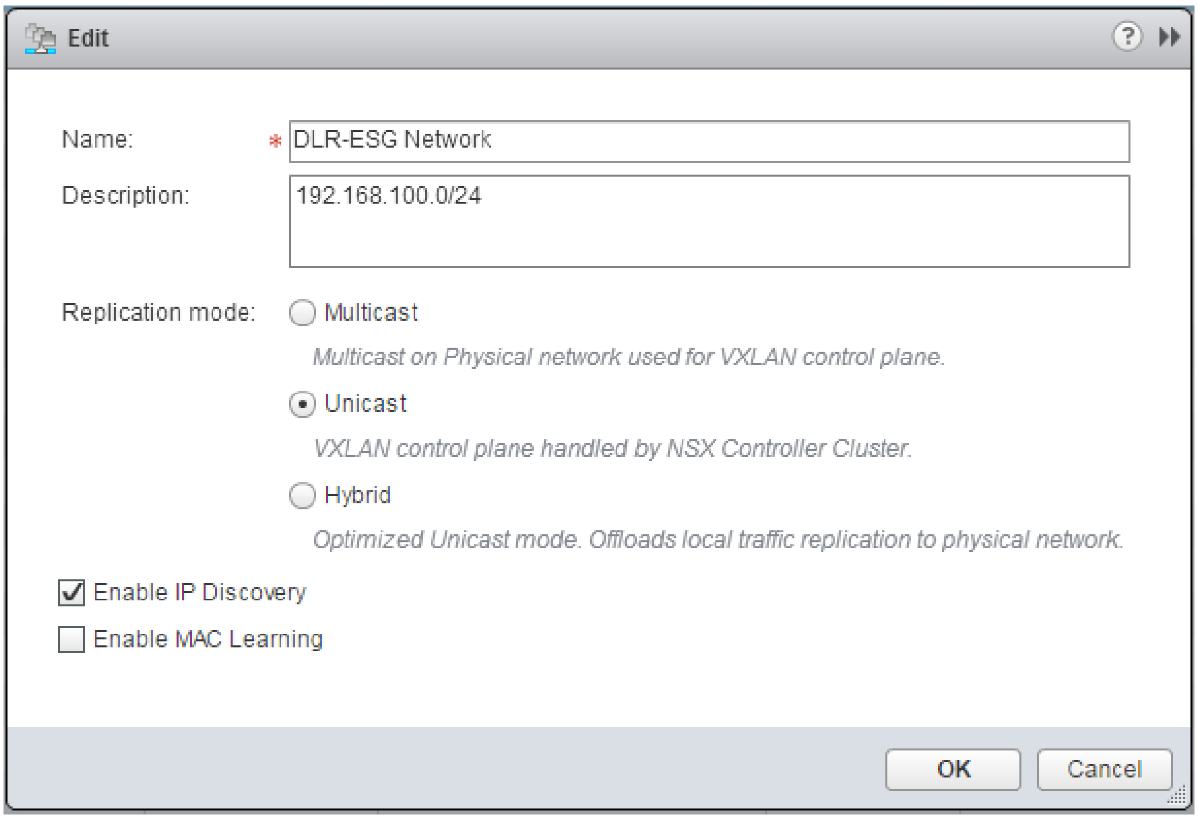
This completes the DLR deployment and configuration. Now the VMs across logical switches will be able to communicate.

8.11 Deploy Edge services gateway

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

8.11.1 Create a logical switch

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



Name: * DLR-ESG Network

Description: 192.168.100.0/24

Replication mode:

○ Multicast
Multicast on Physical network used for VXLAN control plane.

● Unicast
VXLAN control plane handled by NSX Controller Cluster.

○ Hybrid
Optimized Unicast mode. Offloads local traffic replication to physical network.

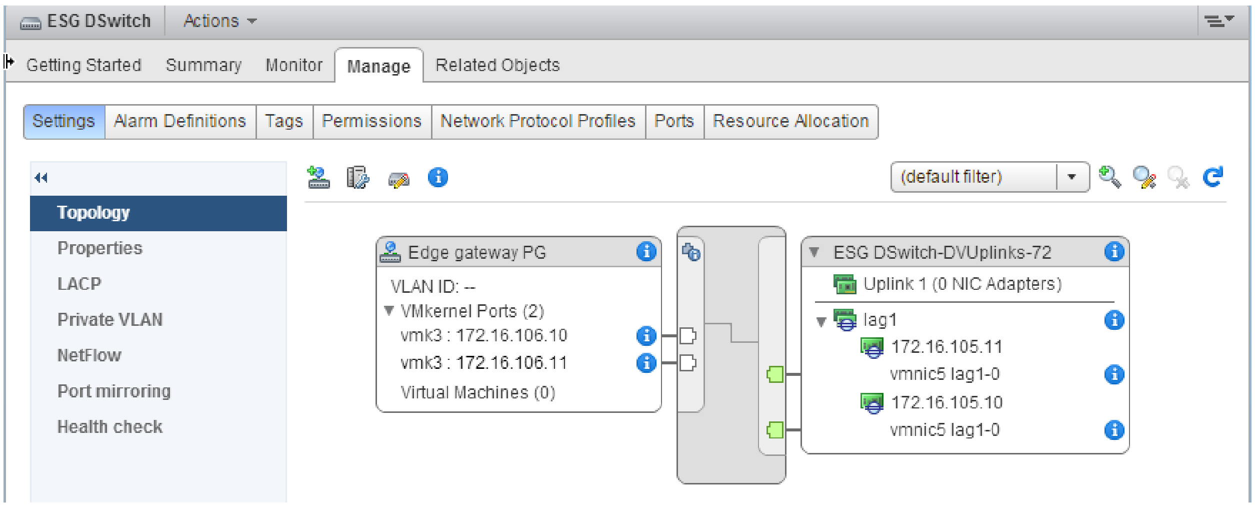
☑ Enable IP Discovery

☐ Enable MAC Learning

Figure 120 Create a logical switch

8.11.2 Create a distributed switch

On the VIM cluster hosts, a vSphere distributed switch needs to be created 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 VIM cluster as shown in the diagram.



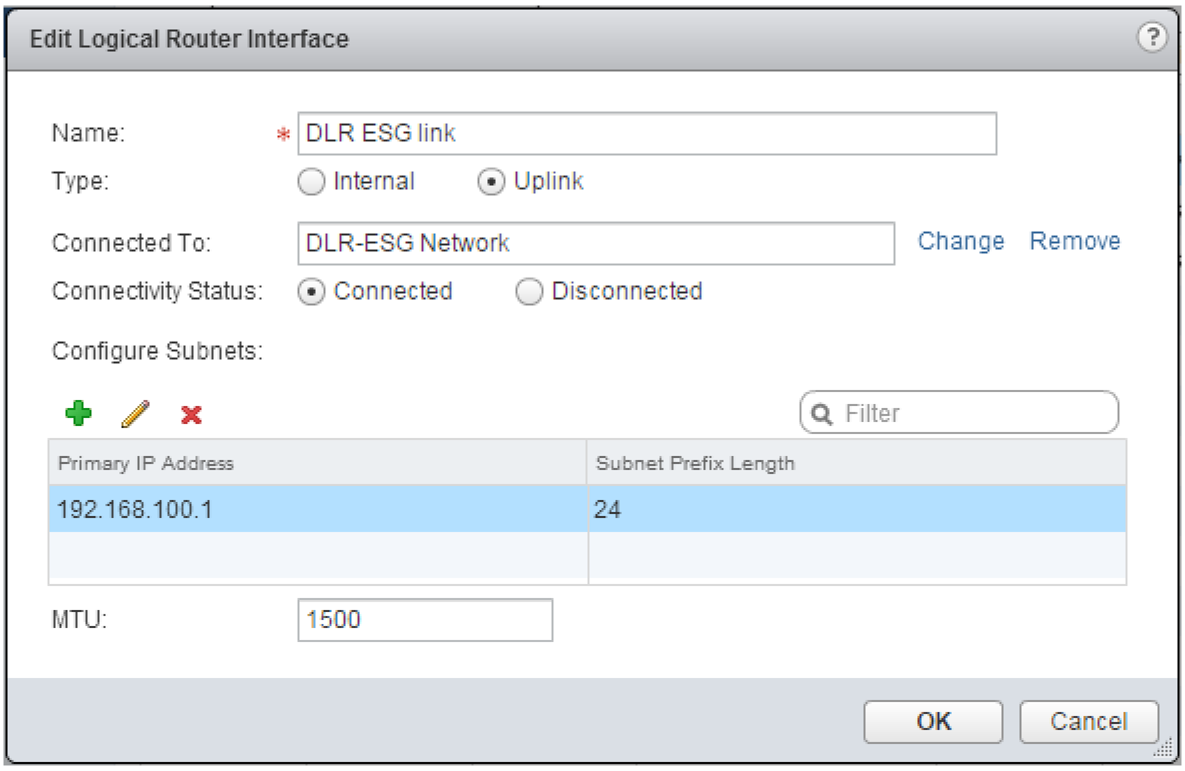
Edge gateway PG
VLAN ID: --
VMkernel Ports (2)
vmk3 : 172.16.106.10
vmk3 : 172.16.106.11
Virtual Machines (0)

ESG DSwitch-DVUplinks-72
Uplink 1 (0 NIC Adapters)
lag1
172.16.105.11
vmnic5 lag1-0
172.16.105.10
vmnic5 lag1-0

Figure 121 Create a distributed switch

8.11.3 Create uplink port in DLR

When initially created, DLR had only two links to enable routing between the logical switch networks. 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.



Edit Logical Router Interface

Name: * DLR ESG link

Type: ○ Internal ● Uplink

Connected To: DLR-ESG Network

Connectivity Status: ● Connected ○ Disconnected

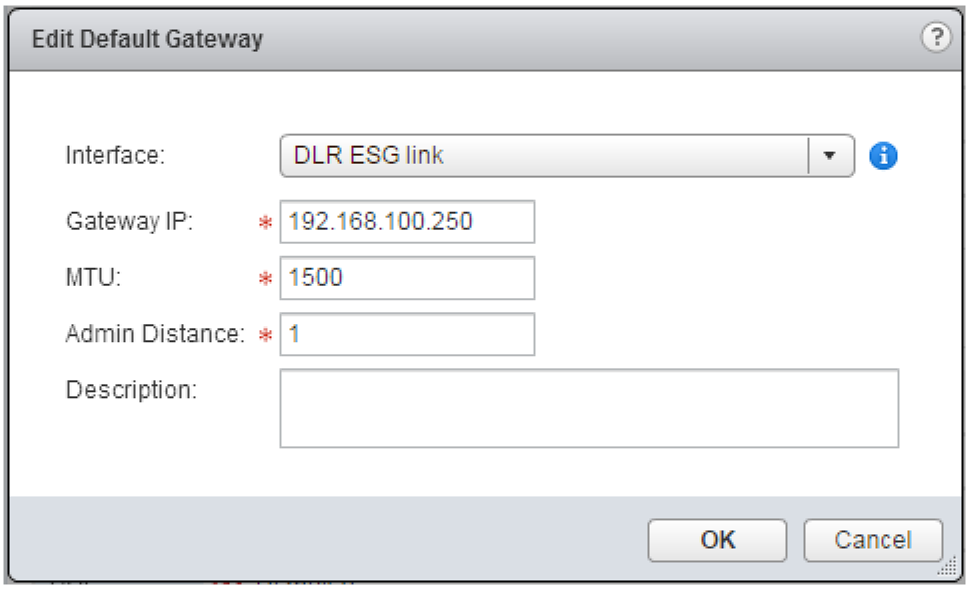
Configure Subnets:

Primary IP Address	Subnet Prefix Length
192.168.100.1	24

MTU: 1500

Figure 122 Edit logical router interface

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



Edit Default Gateway

Interface: DLR ESG link

Gateway IP: * 192.168.100.250

MTU: * 1500

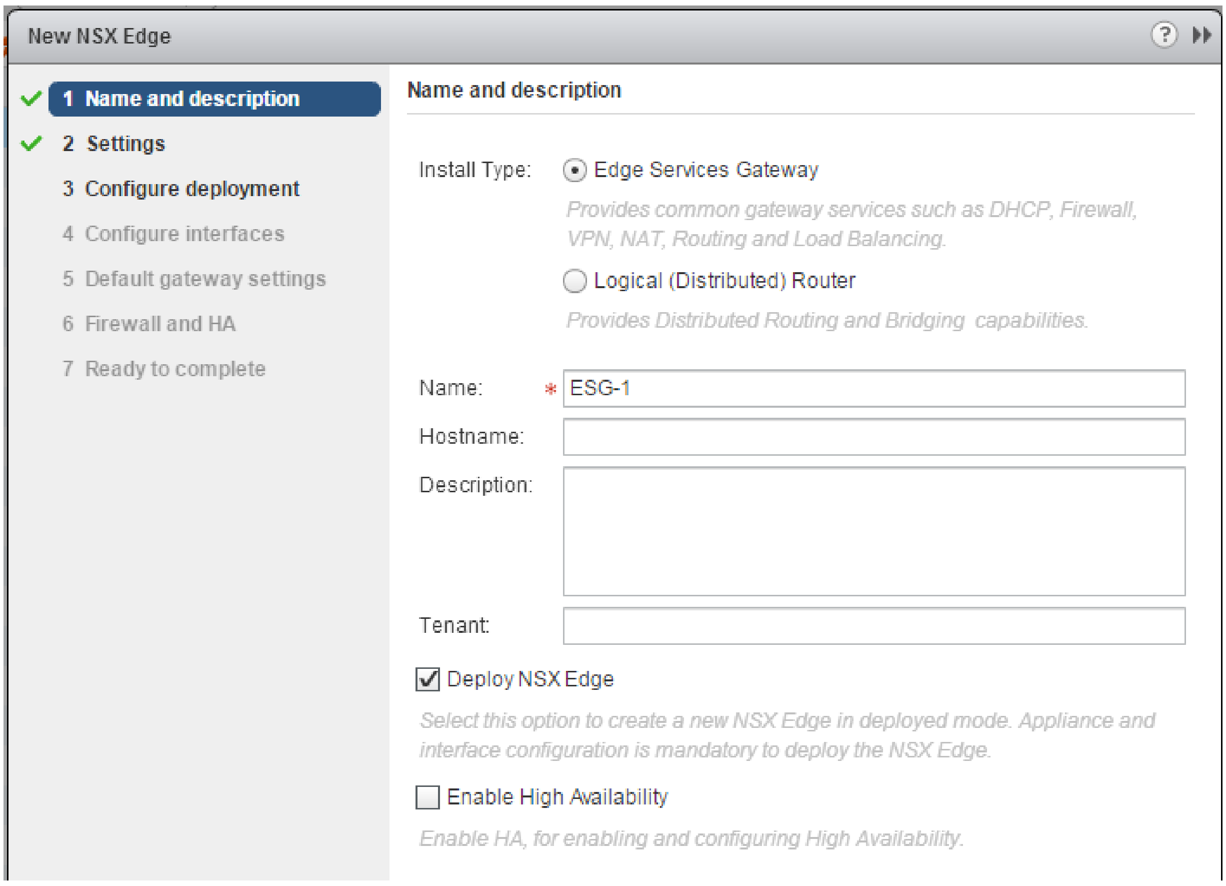
Admin Distance: * 1

Description:

Figure 123 Configure default gateway

8.11.4 Add an ESG

With all the necessary configurations completed, the ESG appliance can be deployed. To deploy, Navigate to **Home → Networking & Security → NSX Edges** and select (**+**).



New NSX Edge

Name and description

Install Type: ● Edge Services Gateway

Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.

○ Logical (Distributed) Router

Provides Distributed Routing and Bridging capabilities.

Name: * ESG-1

Hostname:

Description:

Tenant:

☑ Deploy NSX Edge

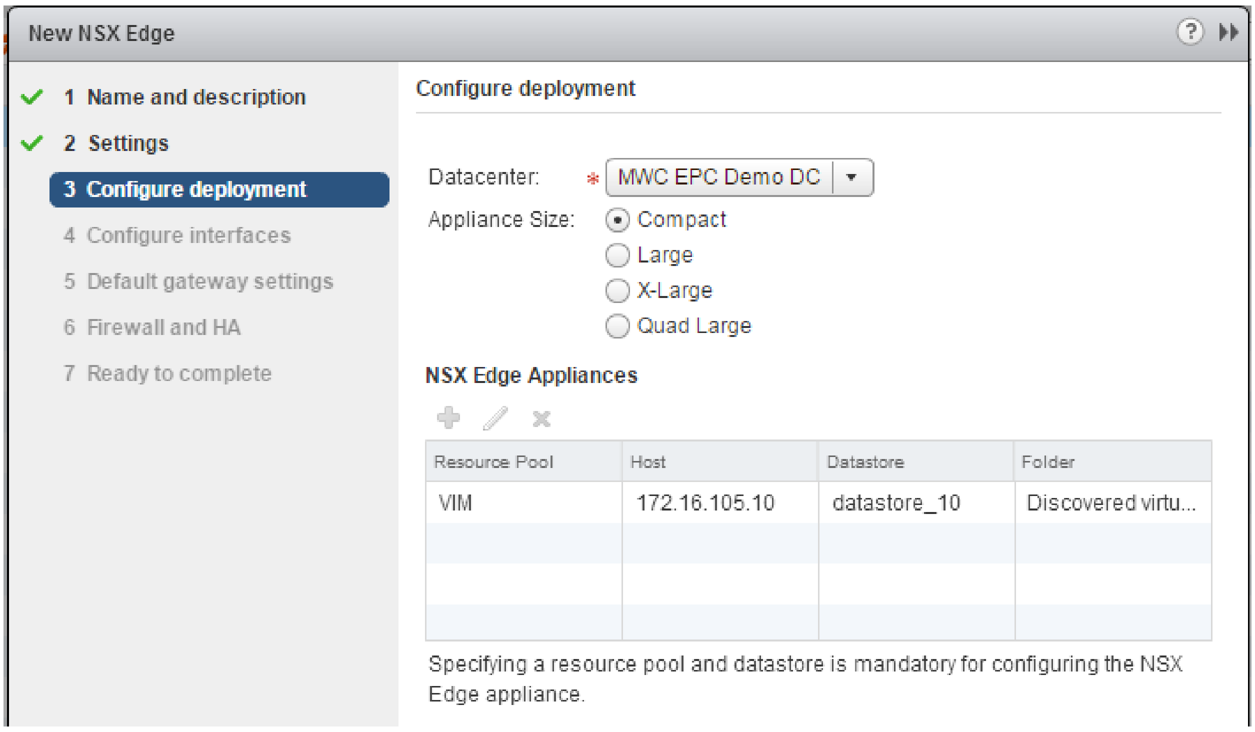
Select this option to create a new NSX Edge in deployed mode. Appliance and interface configuration is mandatory to deploy the NSX Edge.

□ Enable High Availability

Enable HA, for enabling and configuring High Availability.

Figure 124 Deploy ESG appliance

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.



New NSX Edge

Configure deployment

Datacenter: * MWC EPC Demo DC

Appliance Size: ● Compact ○ Large ○ X-Large ○ Quad Large

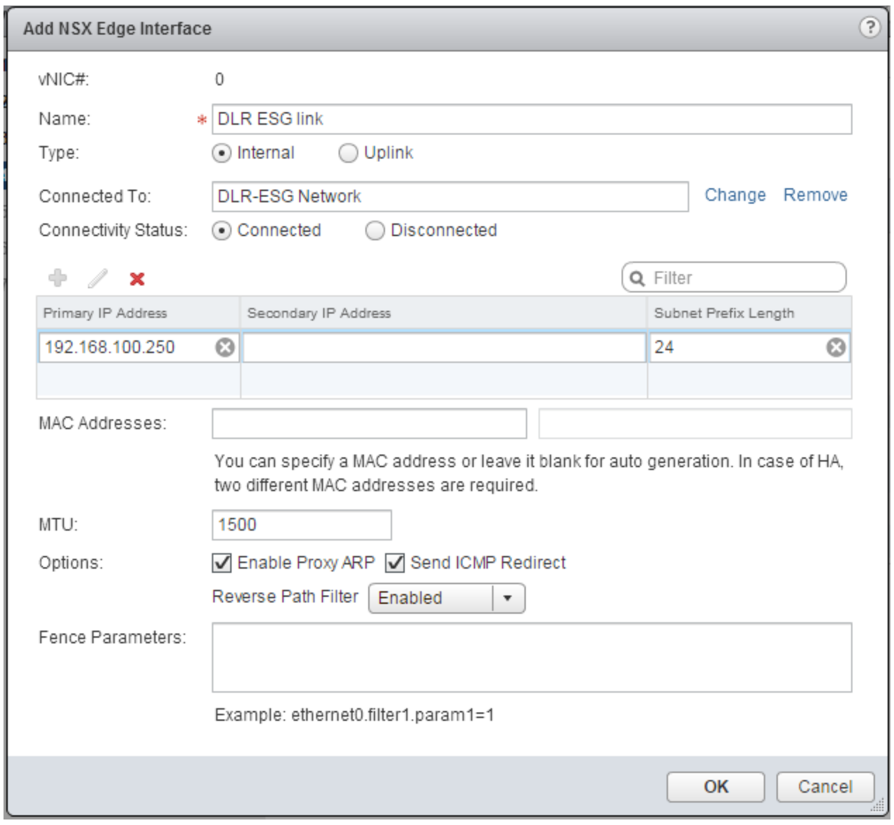
NSX Edge Appliances

Resource Pool	Host	Datastore	Folder
VIM	172.16.105.10	datastore_10	Discovered virtu...

Specifying a resource pool and datastore is mandatory for configuring the NSX Edge appliance.

Figure 125 Configure ESG deployment

Configure the internal and uplink interfaces for the ESG.



Add NSX Edge Interface

vNIC#: 0

Name: * DLR ESG link

Type: ● Internal ○ Uplink

Connected To: DLR-ESG Network Change Remove

Connectivity Status: ● Connected ○ Disconnected

Primary IP Address	Secondary IP Address	Subnet Prefix Length
192.168.100.250		24

MAC Addresses:

You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.

MTU: 1500

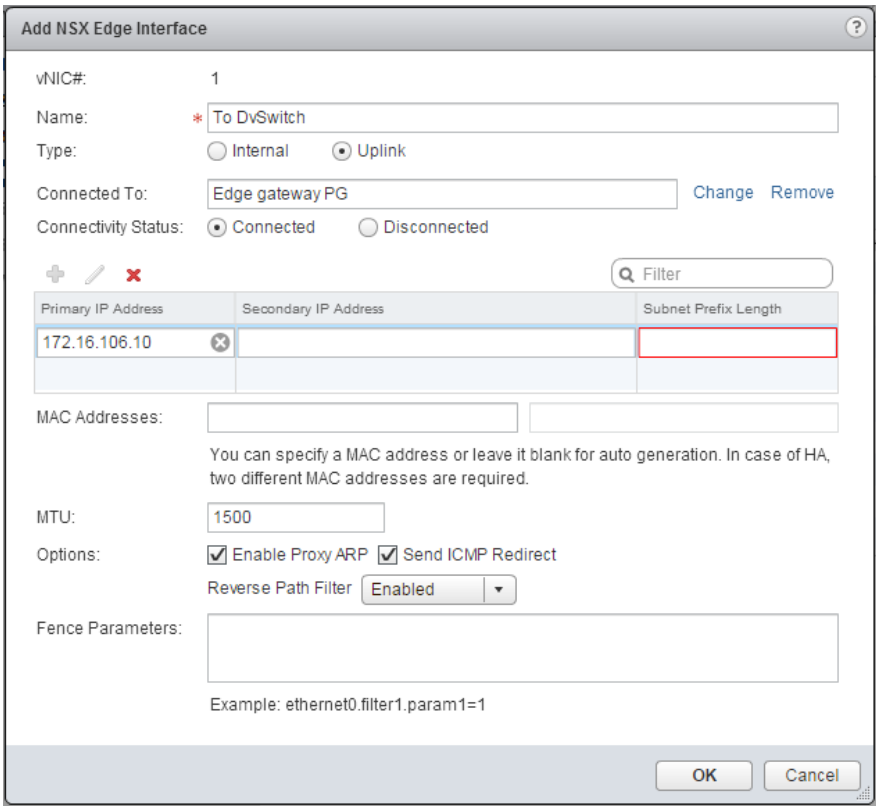
Options: ☑ Enable Proxy ARP ☑ Send ICMP Redirect

Reverse Path Filter: Enabled

Fence Parameters:

Example: ethernet0.filter1.param1=1

Figure 126 Add internal interface



Add NSX Edge Interface

vNIC#: 1

Name: * To DvSwitch

Type: ○ Internal ● Uplink

Connected To: Edge gateway PG Change Remove

Connectivity Status: ● Connected ○ Disconnected

Primary IP Address	Secondary IP Address	Subnet Prefix Length
172.16.106.10		

MAC Addresses:

You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.

MTU: 1500

Options: ☑ Enable Proxy ARP ☑ Send ICMP Redirect

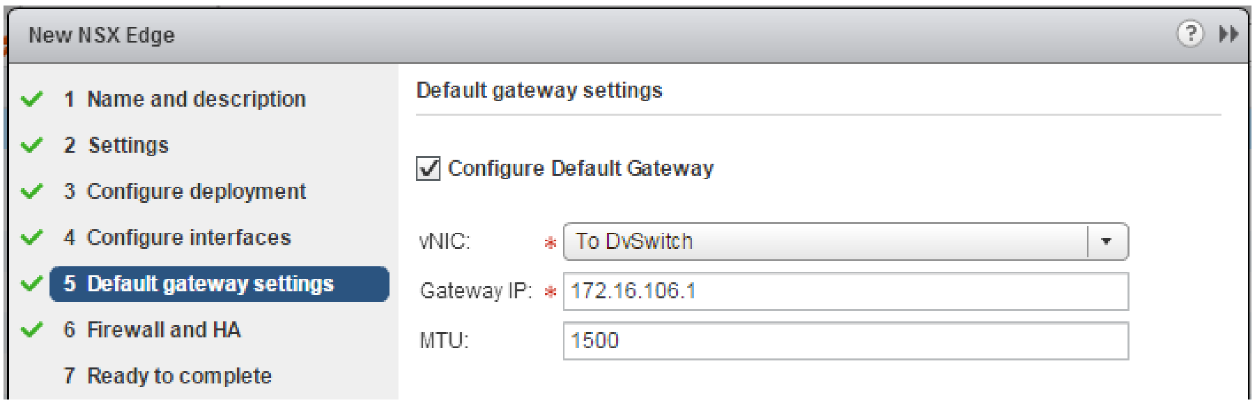
Reverse Path Filter: Enabled

Fence Parameters:

Example: ethernet0.filter1.param1=1

Figure 127 Add uplink interface

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



New NSX Edge

1. ✓ Name and description
2. ✓ Settings
3. ✓ Configure deployment
4. ✓ Configure interfaces
5. ✓ Default gateway settings
6. ✓ Firewall and HA
7. Ready to complete

Default gateway settings

☑ Configure Default Gateway

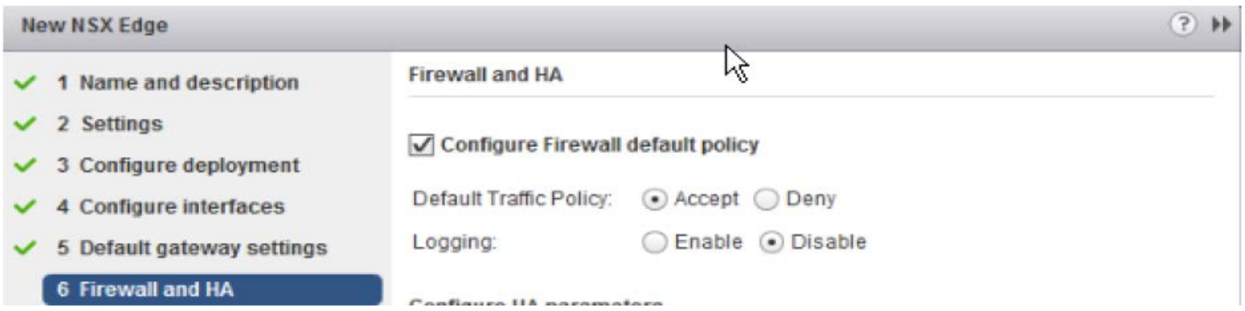
vNIC: * To DvSwitch

Gateway IP: * 172.16.106.1

MTU: 1500

Figure 128 Default gateway settings

Make sure to enable Firewall with Default Traffic policy by checking **Accept** and then **Next**.



Firewall and HA

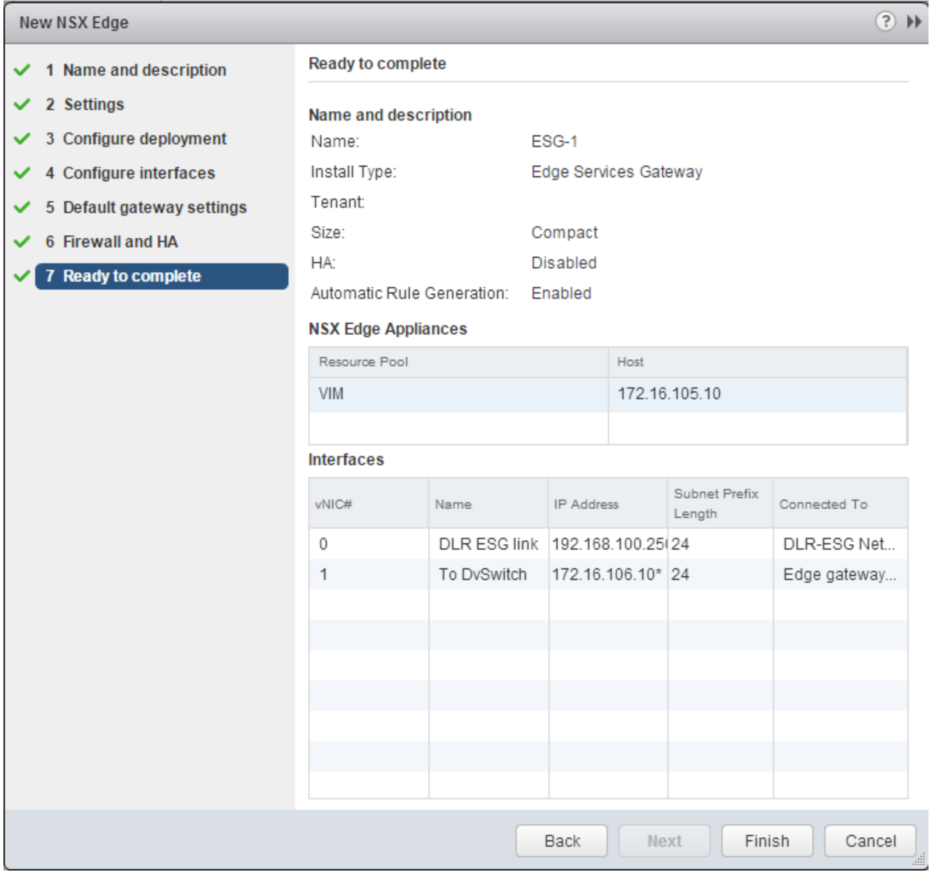
☑ Configure Firewall default policy

Default Traffic Policy: ● Accept ○ Deny

Logging: ○ Enable ● Disable

Figure 129 Enable Firewall default policy

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



Ready to complete

Name and description

Name:	ESG-1
Install Type:	Edge Services Gateway
Tenant:	
Size:	Compact
HA:	Disabled
Automatic Rule Generation:	Enabled

NSX Edge Appliances

Resource Pool	Host
VIM	172.16.105.10

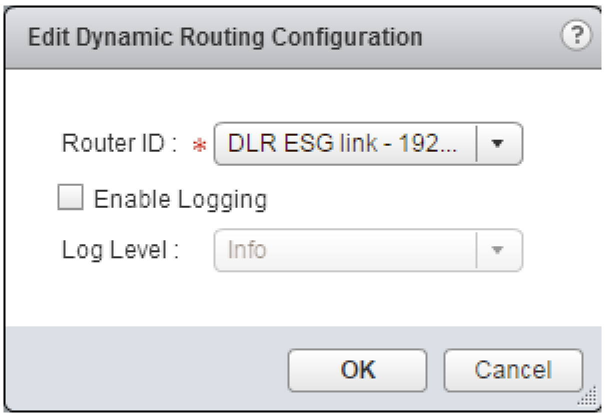
Interfaces

vNIC#	Name	IP Address	Subnet Prefix Length	Connected To
0	DLR ESG link	192.168.100.25	24	DLR-ESG Net...
1	To DvSwitch	172.16.106.10*	24	Edge gateway...

Figure 130 Complete the configuration

8.11.5 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 routing protocols 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.



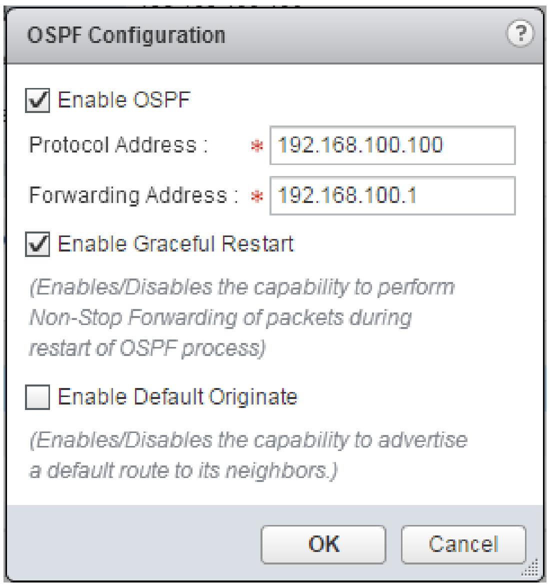
Router ID : * DLR ESG link - 192...

□ Enable Logging

Log Level : Info

Figure 131 Dynamic routing configuration

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



OSPF Configuration

☑ Enable OSPF

Protocol Address : * 192.168.100.100

Forwarding Address : * 192.168.100.1

☑ Enable Graceful Restart

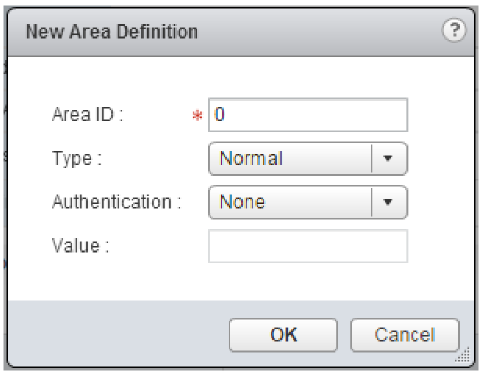
(Enables/Disables the capability to perform Non-Stop Forwarding of packets during restart of OSPF process)

☐ Enable Default Originate

(Enables/Disables the capability to advertise a default route to its neighbors.)

Figure 132 OSPF configuration

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

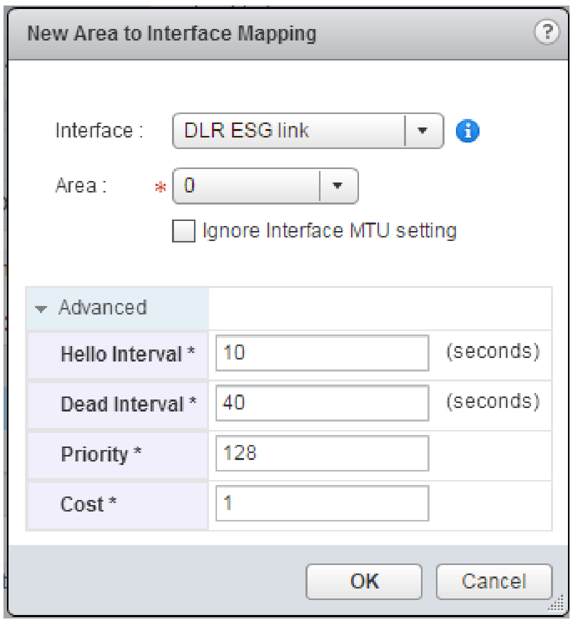


New Area Definition

Area ID : *	0
Type :	Normal
Authentication :	None
Value :	

Figure 133 Area definitions

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



New Area to Interface Mapping

Interface : DLR ESG link

Area : * 0

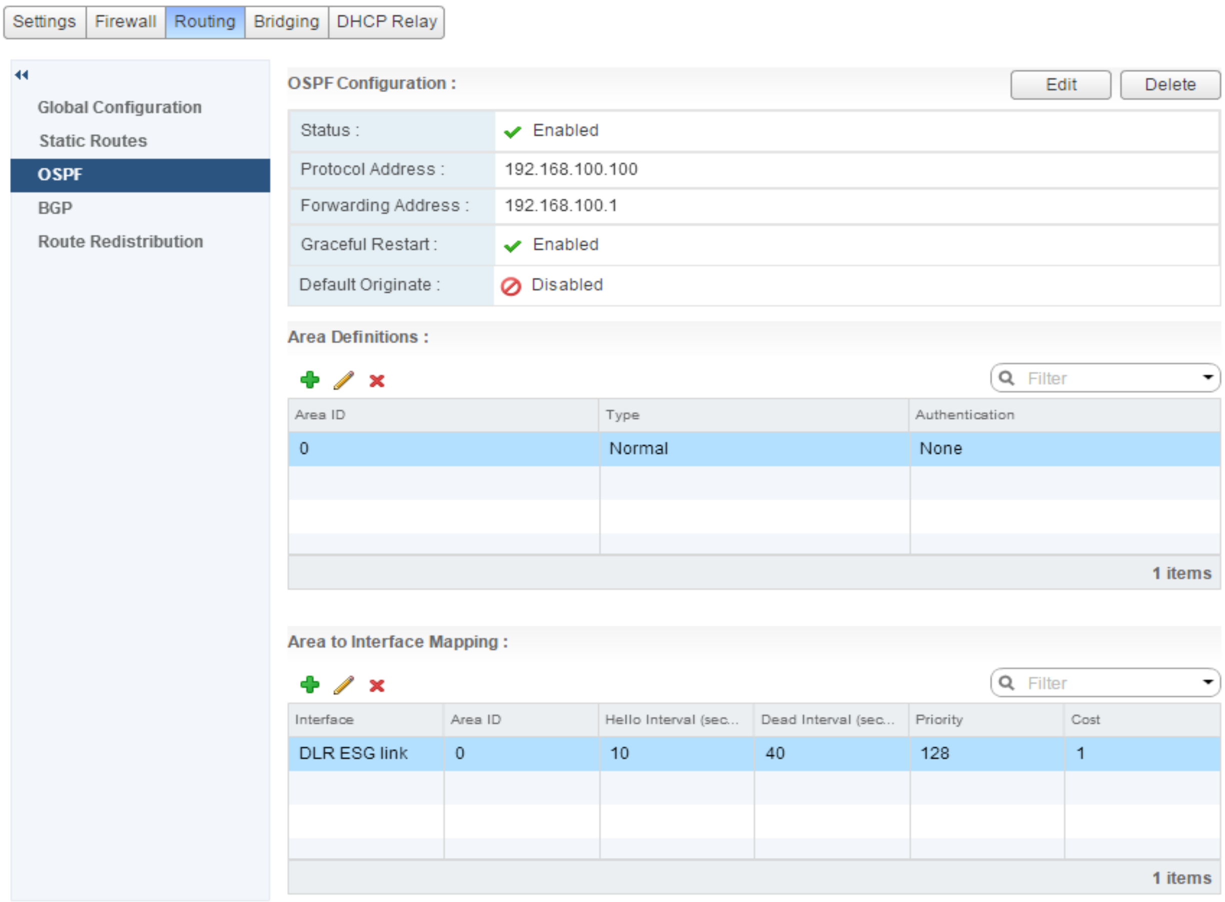
☐ Ignore Interface MTU setting

Advanced

Hello Interval *	10	(seconds)
Dead Interval *	40	(seconds)
Priority *	128	
Cost *	1	

Figure 134 Area to interface mapping

Review all the changes and click on publish changes.



OSPF Configuration :

Status :	✓ Enabled
Protocol Address :	192.168.100.100
Forwarding Address :	192.168.100.1
Graceful Restart :	✓ Enabled
Default Originate :	⊘ Disabled

Area Definitions :

Area ID	Type	Authentication
0	Normal	None

1 items

Area to Interface Mapping :

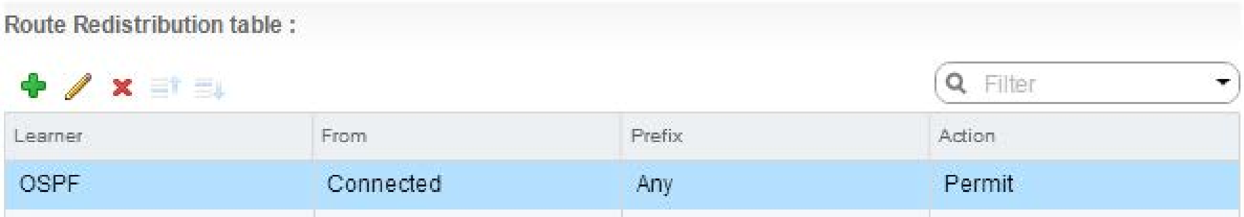
Interface	Area ID	Hello Interval (sec...	Dead Interval (sec...	Priority	Cost
DLR ESG link	0	10	40	128	1

1 items

Figure 135 Review OSPF configuration

8.11.6 Route redistribution and firewall configuration

Even though OSPF is enabled 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.

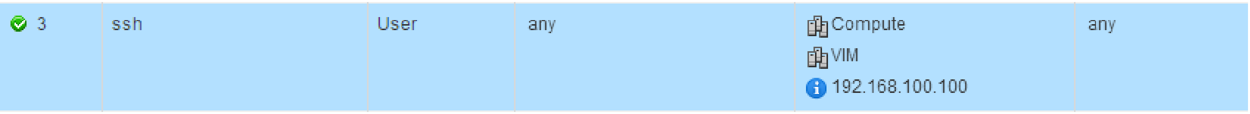


Route Redistribution table :

Learner	From	Prefix	Action
OSPF	Connected	Any	Permit

Figure 136 Route redistribution

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

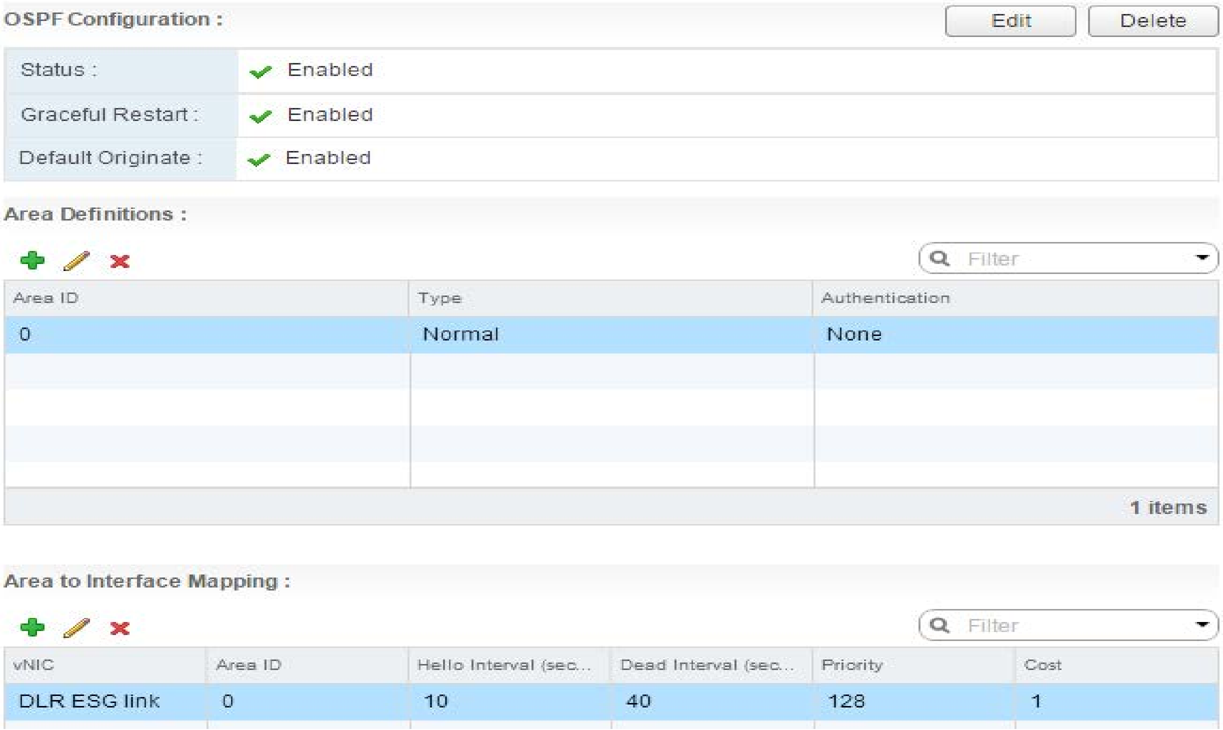


✓ 3	ssh	User	any	Compute VIM 192.168.100.100	any

Figure 137 Configure firewall filter

8.11.7 Configure OSPF on ESG

Configuring OSPF in ESG is similar to DLR. Configure the router ID, under OSPF configuration when enabling the OSPF protocol, make sure to enable Default Originate to propagate the default route down to DLR.



OSPF Configuration :

Status :	✓ Enabled
Graceful Restart :	✓ Enabled
Default Originate :	✓ Enabled

Area Definitions :

Area ID	Type	Authentication
0	Normal	None

1 items

Area to Interface Mapping :

vNIC	Area ID	Hello Interval (sec...	Dead Interval (sec...	Priority	Cost
DLR ESG link	0	10	40	128	1

Figure 138 Configure OSPF on ESG

Redistribute the connected interfaces of ESG to OSPF database similar DLR.

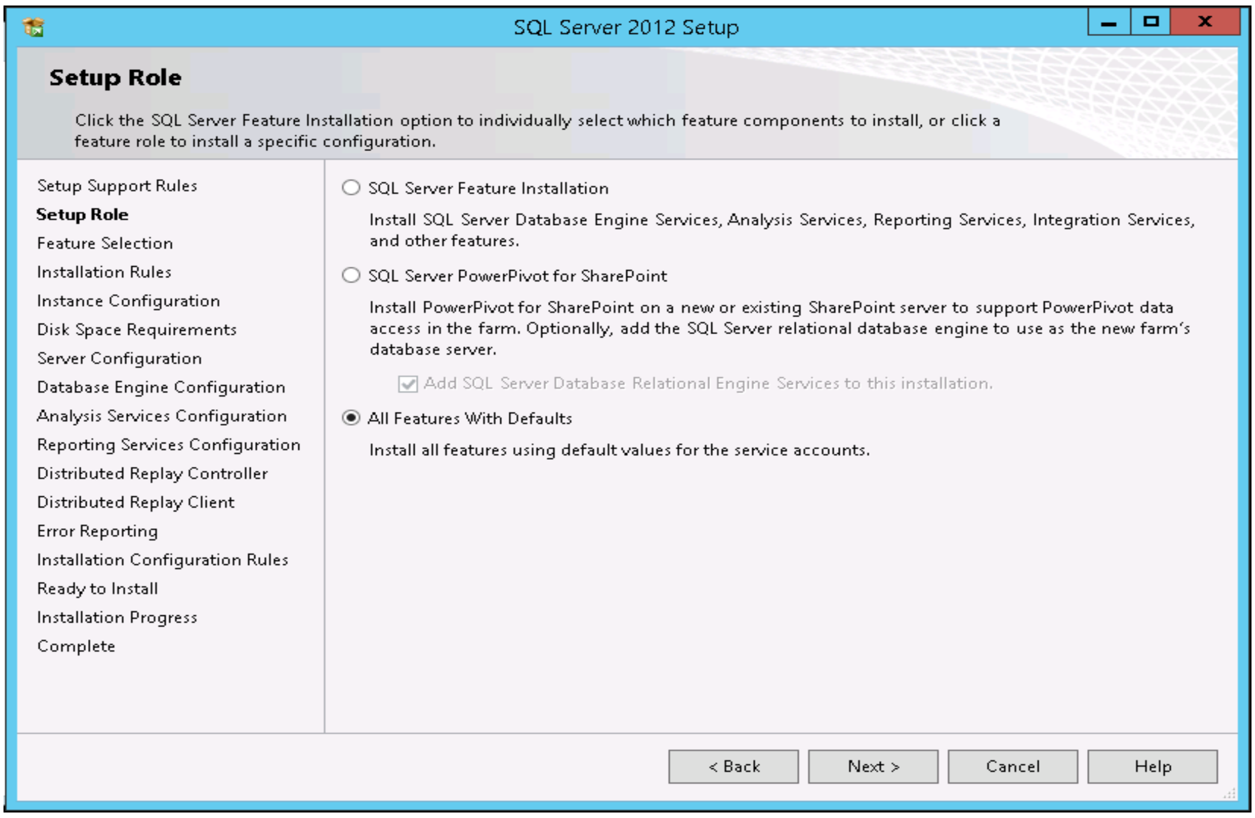
9 Install vCloud Director

9.1 Install and Bring up 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 requires only one NIC, and must be part of the management network.

9.2 Install SQL Server in Windows VM

VCD 8.0 and SQL Express editions are not compatible. Make sure to use a licensed edition such as 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 Defaults** under setup role.



Setup Role

Click the SQL Server Feature Installation option to individually select which feature components to install, or click a feature role to install a specific configuration.

○ SQL Server Feature Installation

Install SQL Server Database Engine Services, Analysis Services, Reporting Services, Integration Services, and other features.

○ SQL Server PowerPivot for SharePoint

Install PowerPivot for SharePoint on a new or existing SharePoint server to support PowerPivot data access in the farm. Optionally, add the SQL Server relational database engine to use as the new farm's database server.

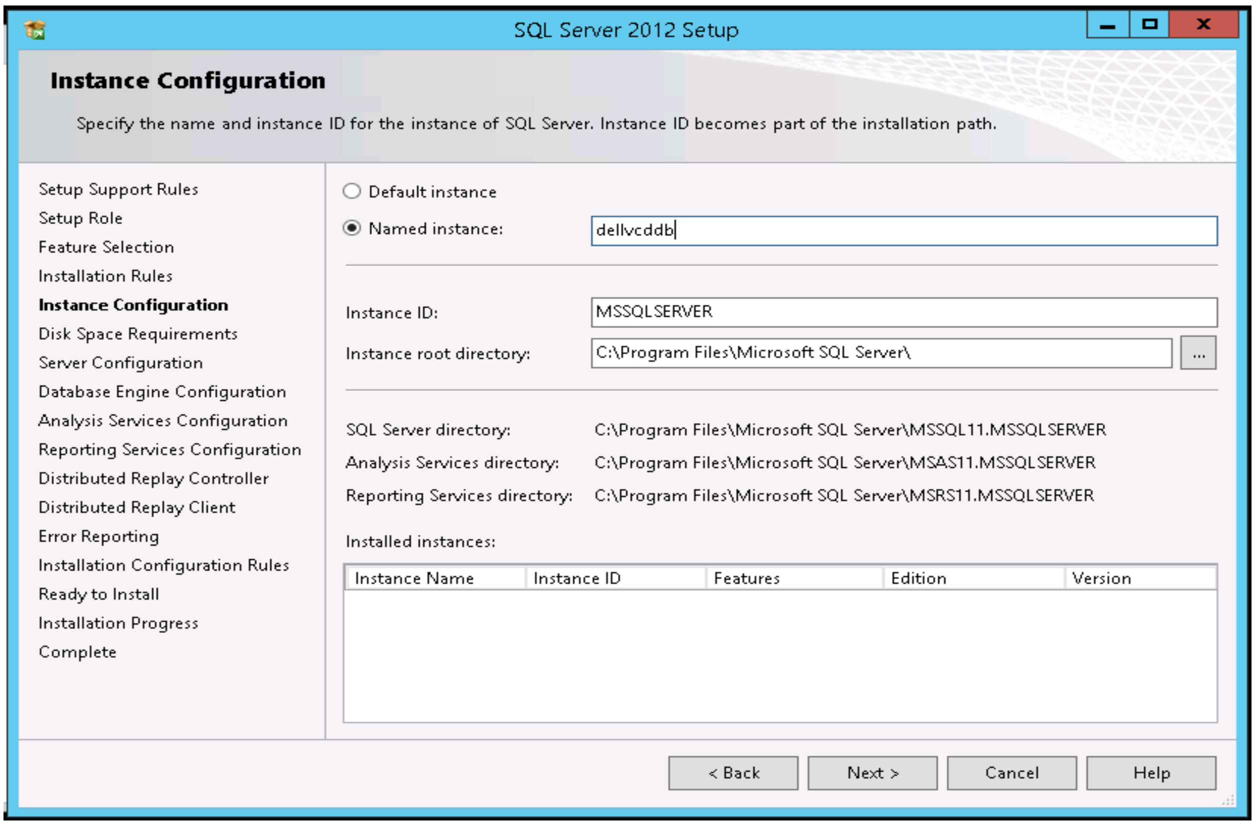
☑ Add SQL Server Database Relational Engine Services to this installation.

● All Features With Defaults

Install all features using default values for the service accounts.

Figure 139 Installing SQL

Create a named instance of your choice.



Instance Configuration

Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.

○ Default instance

● Named instance: dellvcddb

Instance ID: MSSQLSERVER

Instance root directory: C:\Program Files\Microsoft SQL Server\

SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER

Analysis Services directory: C:\Program Files\Microsoft SQL Server\MSAS11.MSSQLSERVER

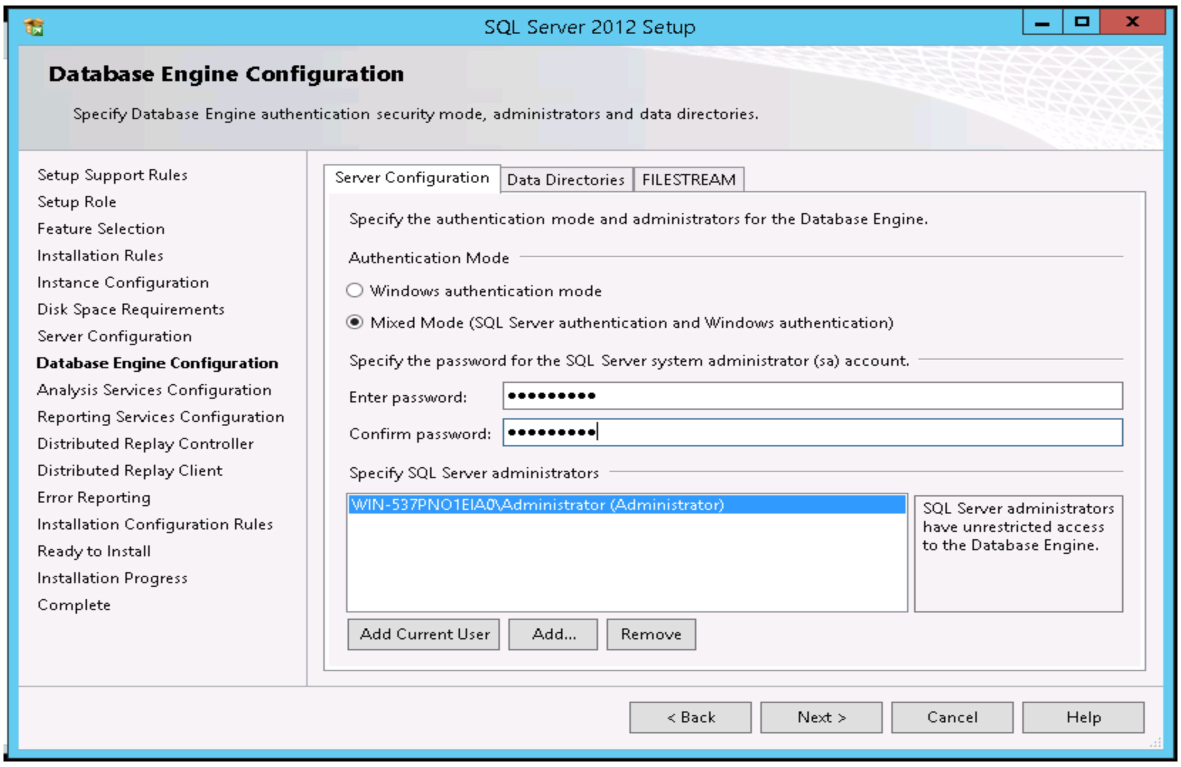
Reporting Services directory: C:\Program Files\Microsoft SQL Server\MSRS11.MSSQLSERVER

Installed instances:

Instance Name	Instance ID	Features	Edition	Version

Figure 140 Name the instance

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



SQL Server 2012 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators and data directories.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

○ Windows authentication mode

● Mixed Mode (SQL Server authentication and Windows authentication)

Specify the password for the SQL Server system administrator (sa) account.

Enter password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

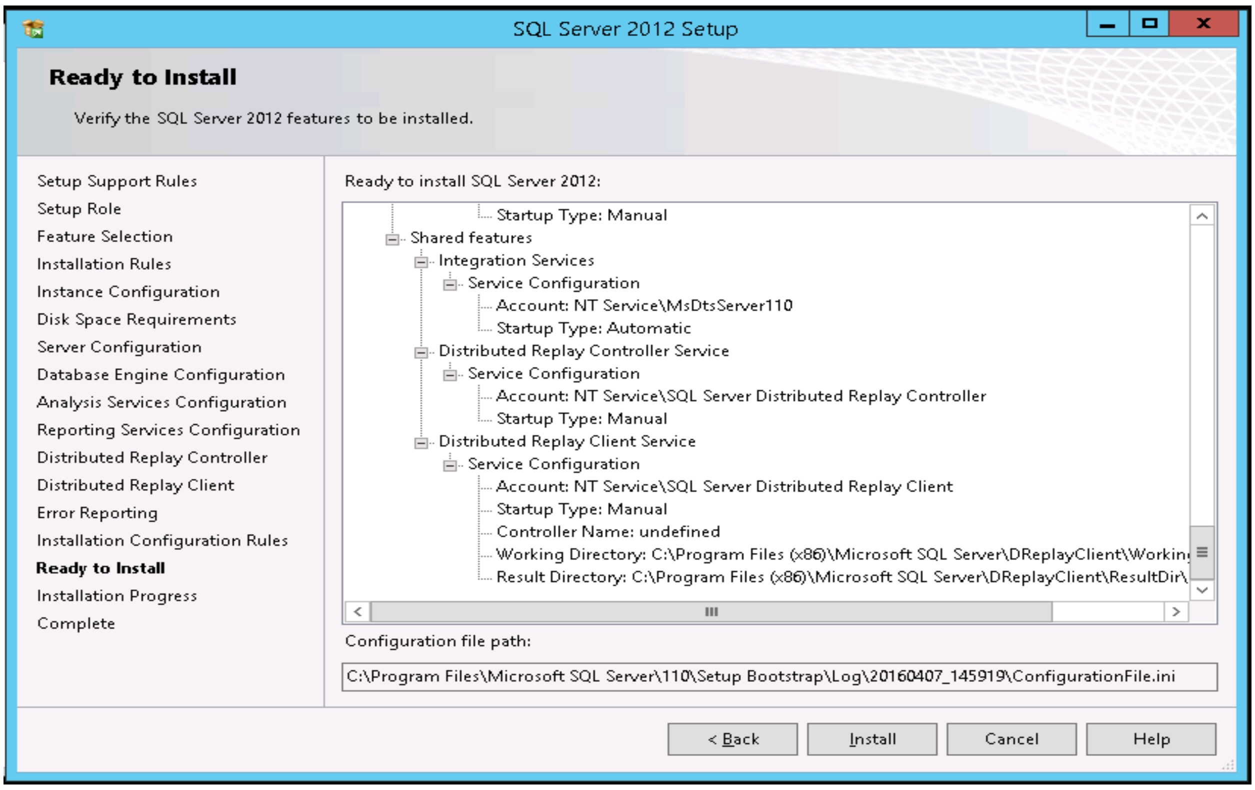
Specify SQL Server administrators

WIN-537PNO1EIA0\Administrator (Administrator)

SQL Server administrators have unrestricted access to the Database Engine.

Figure 141 Configure password

Do not configure any other services. Click **Install** to install SQL.



SQL Server 2012 Setup

Ready to Install

Verify the SQL Server 2012 features to be installed.

Ready to install SQL Server 2012:

```
            Startup Type: Manual
    Shared features
        Integration Services
            Service Configuration
                Account: NT Service\MsDtsServer110
                Startup Type: Automatic
        Distributed Replay Controller Service
            Service Configuration
                Account: NT Service\SQL Server Distributed Replay Controller
                Startup Type: Manual
        Distributed Replay Client Service
            Service Configuration
                Account: NT Service\SQL Server Distributed Replay Client
                Startup Type: Manual
                Controller Name: undefined
                Working Directory: C:\Program Files (x86)\Microsoft SQL Server\DReplayClient\Workin
                Result Directory: C:\Program Files (x86)\Microsoft SQL Server\DReplayClient\ResultDir\
```

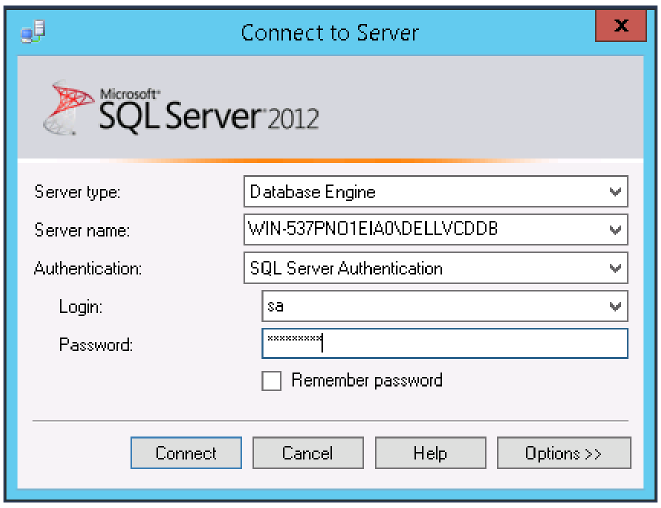
Configuration file path:

C:\Program Files\Microsoft SQL Server\110\Setup Bootstrap\Log\20160407_145919\ConfigurationFile.ini

Figure 142 Click Install

9.3 Configure the SQL Server

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



Server type: Database Engine

Server name: WIN-537PNO1EIA0\DELLVCDDB

Authentication: SQL Server Authentication

Login: sa

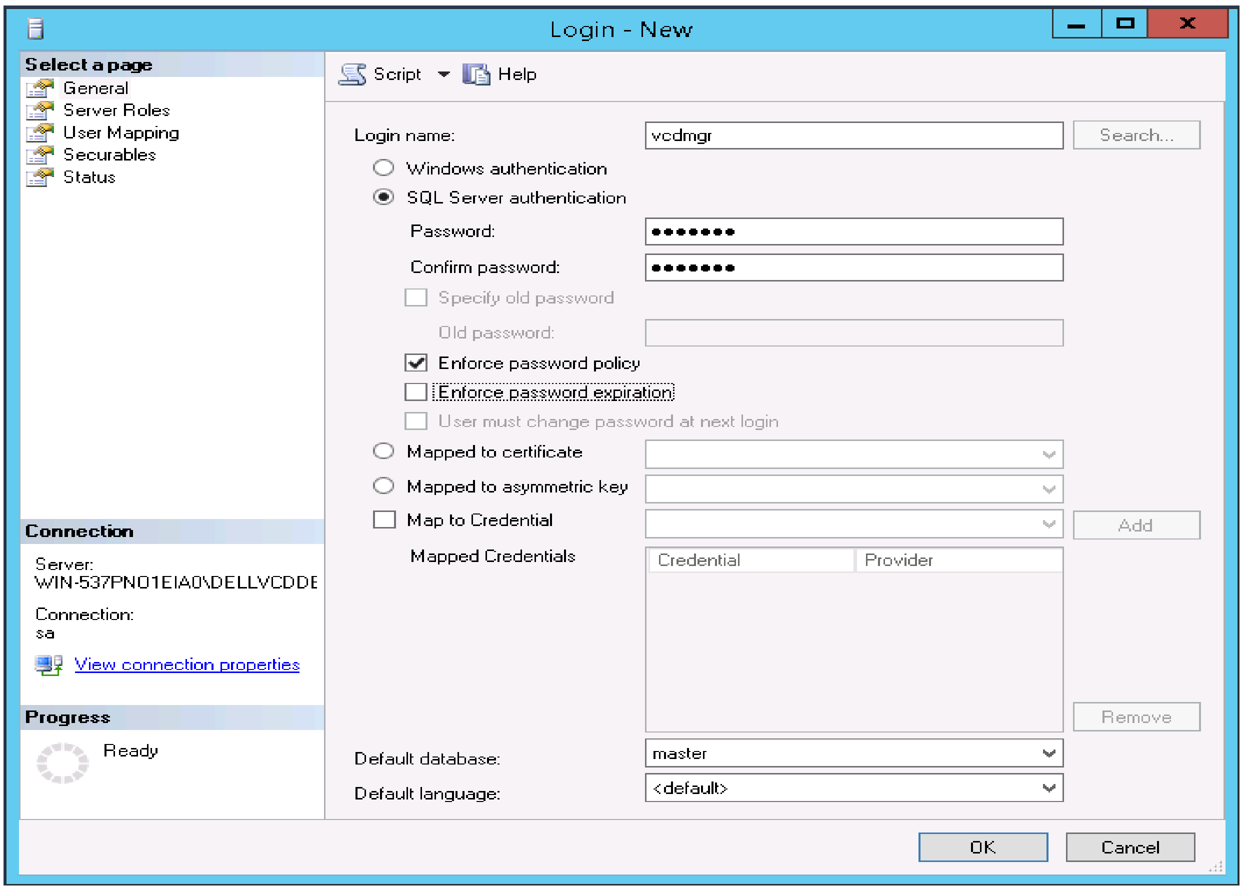
Password: *********

□ Remember password

Figure 143 Log in to SQL Server Studio

9.3.1 Create a new user for vCloud

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



Login name: vcdmgr

○ Windows authentication

● SQL Server authentication

Password: •••••••

Confirm password: •••••••

□ Specify old password

Old password:

☑ Enforce password policy

□ Enforce password expiration

□ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential

Mapped Credentials

Credential	Provider

Default database: master

Default language: <default>

Connection

Server: WIN-537PNO1EIA0\DELLVCDDE

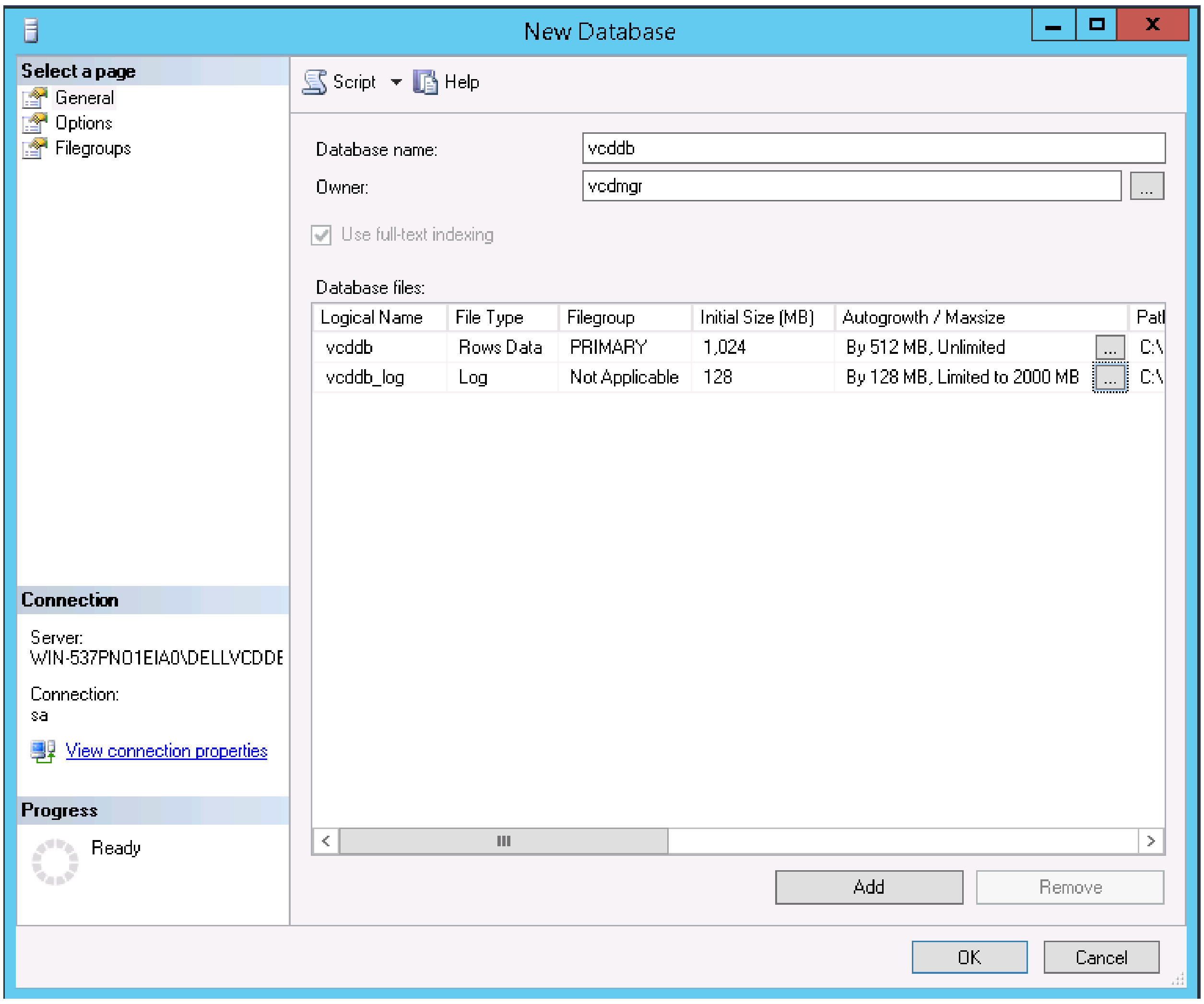
Connection: sa

Figure 144 Create a new login for SQL

9.3.2 Create a new Database

Create a new database for vCloud and assign the new user, which 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.



New Database

Select a page: General, Options, Filegroups

Database name: vcddb

Owner: vcdmgr

☑ Use full-text indexing

Database files:

Logical Name	File Type	Filegroup	Initial Size (MB)	Autogrowth / Maxsize	Path
vcddb	Rows Data	PRIMARY	1,024	By 512 MB, Unlimited	C:\
vcddb_log	Log	Not Applicable	128	By 128 MB, Limited to 2000 MB	C:\

Connection

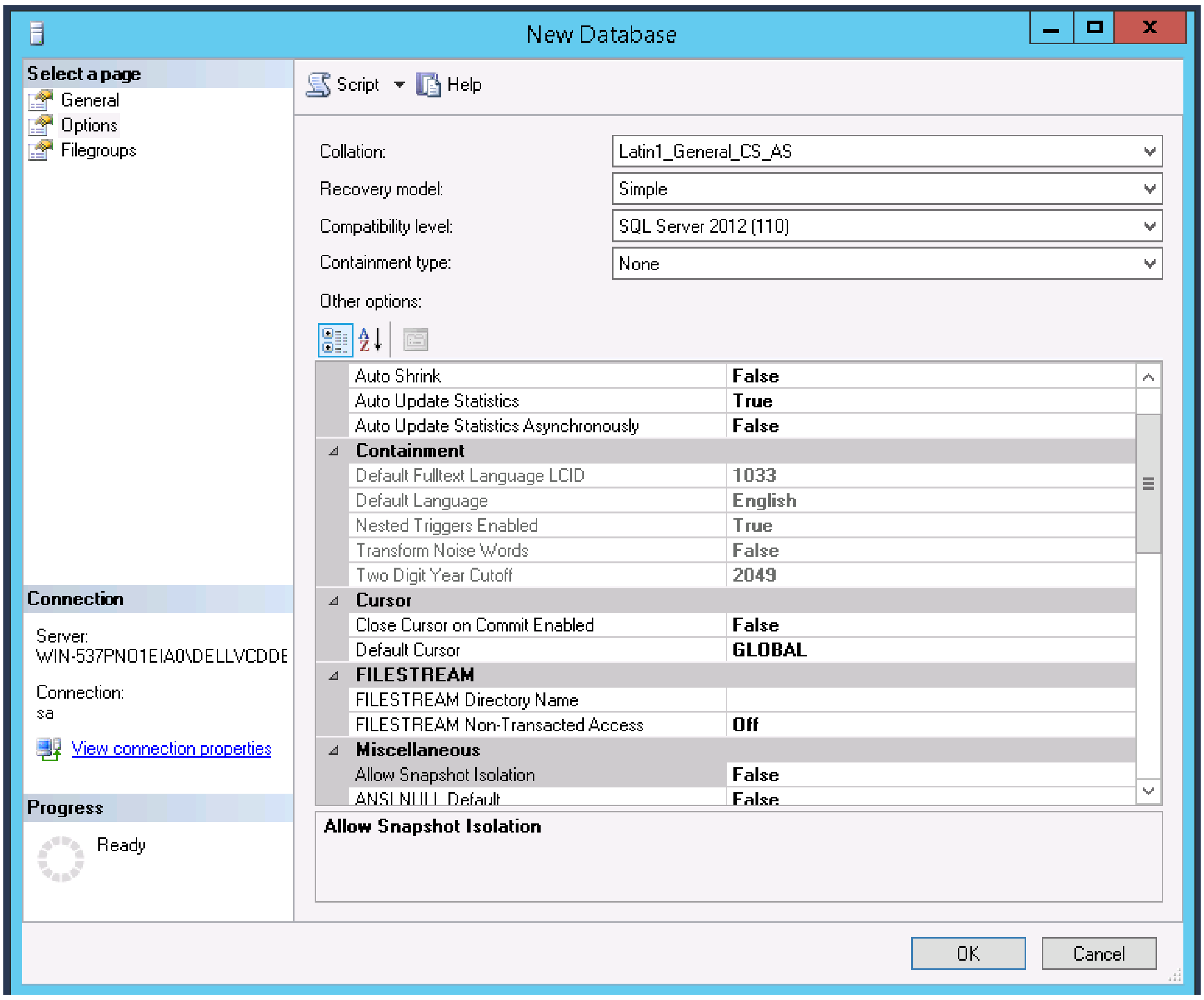
Server:
WIN-537PNO1EIA0\DELLVCDDE

Connection:
sa

Progress: Ready

Figure 145 Create a 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**.



New Database

Select a page: General, Options, Filegroups

Collation: Latin1_General_CS_AS

Recovery model: Simple

Compatibility level: SQL Server 2012 (110)

Containment type: None

Other options:

Auto Shrink	False
Auto Update Statistics	True
Auto Update Statistics Asynchronously	False
Containment	
Default Fulltext Language LCID	1033
Default Language	English
Nested Triggers Enabled	True
Transform Noise Words	False
Two Digit Year Cutoff	2049
Cursor	
Close Cursor on Commit Enabled	False
Default Cursor	GLOBAL
FILESTREAM	
FILESTREAM Directory Name	
FILESTREAM Non-Transacted Access	Off
Miscellaneous	
Allow Snapshot Isolation	False
ANSI NULL Default	False

Allow Snapshot Isolation

Connection

Server:
WIN-537PNO1EIA0\DELLVCDDE

Connection:
sa

Progress: Ready

Figure 146 Configure the database

9.3.3 Configure the database

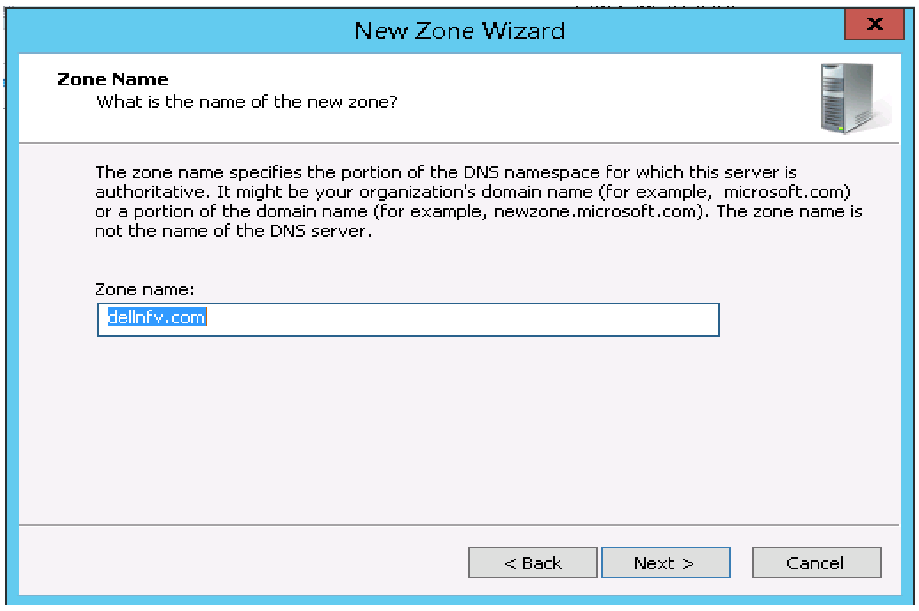
Copy the script below or from the vCloud installation guide and select new query. Change the name [] bracket to the name of the DB that was created in previous step and click **Execute**.

```
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', @va
lue = 'ON';
ALTER DATABASE [vcddb] SET READ_COMMITTED_SNAPSHOT ON WITH NO_WAIT;
EXEC sp_addextendedproperty @name = N'READ_COMMITTED_SNAPSHOT', @val
ue = 'ON';
ALTER DATABASE [vcddb] SET MULTI_USER;
GO
```

9.3.4 Setup DNS server and add entries

Note: This is an important step in the vCloud director installation. Setting up the DNS server with wrong hostname of RHEL VM will result in failure to start the vCloud director application.

In the windows VM, enable DNS server using server manager. Navigate to **Tools → DNS** to launch DNS manager. Create a forward lookup zone with the name 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 done on that DNS server.

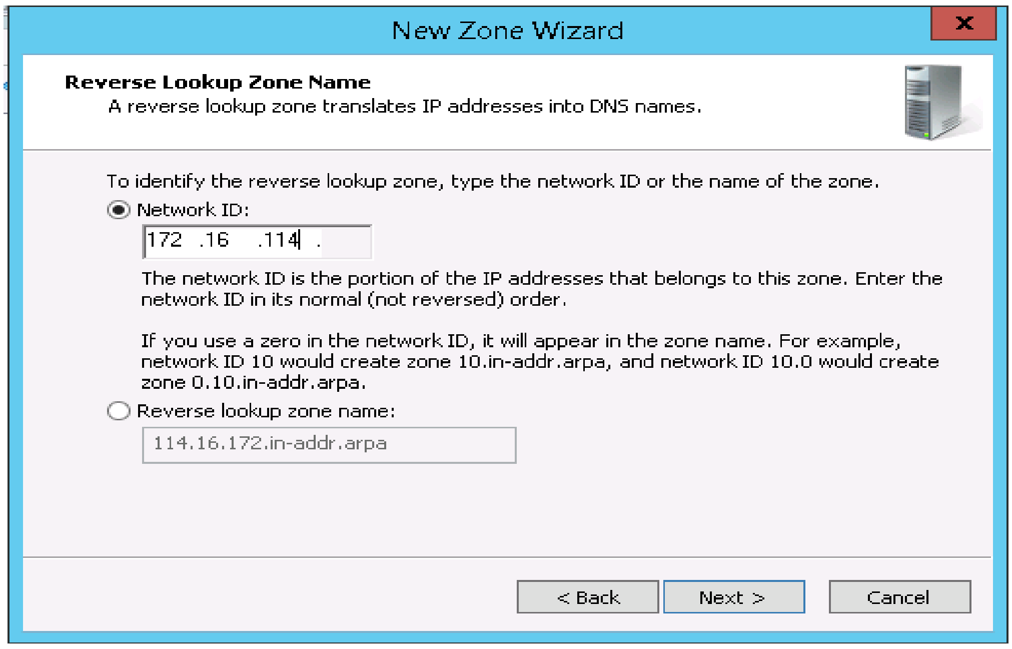


The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name: dellnfv.com

Figure 147 New Zone Wizard

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



New Zone Wizard

Reverse Lookup Zone Name

A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

● Network ID:

172 .16 .114 .

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

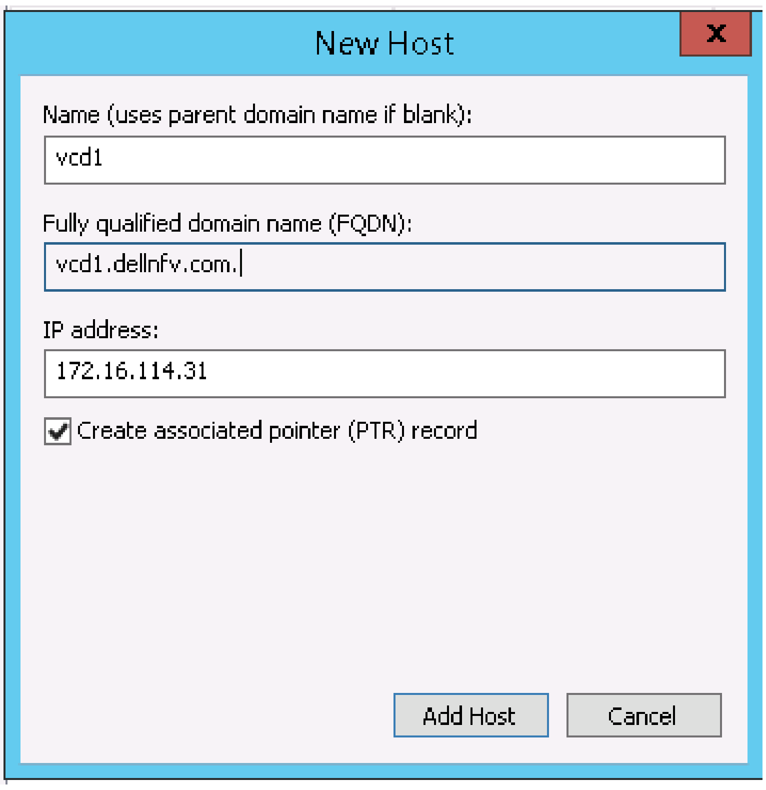
If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

○ Reverse lookup zone name:

114.16.172.in-addr.arpa

Figure 148 Create a Reverse Lookup Zone

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



New Host

Name (uses parent domain name if blank):

vcd1

Fully qualified domain name (FQDN):

vcd1.dellnfv.com.

IP address:

172.16.114.31

☑ Create associated pointer (PTR) record

Figure 149 New Host

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

9.3.5 Install and Bring up Red Hat 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 here in case 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 same as the IP configured in the DNS server. Configure your RHEL login to subscribe to download the updates and applications.

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

9.3.5.1 Configure Firewall rules in RH

Configure the iptables as below. These 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
```

9.3.5.2 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
```

9.3.6 Start and Stop vCloud director

Download the vCloud director binary and copy the file to location /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
```

9.3.6.1 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
```

9.3.6.2 Continue with the installation

Navigate to '/opt/vmware/vcloud-director/bin' directory and continue with the installation.

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 ~]#
```

10 Install vRealize Operations Manager (vROps)

Deploy the OVF template of the vROps in any of the ESXi host.

After successful deployment of the OVF deployment, open a browser with the IP address or FQDN of the vROps appliance.

After accepting the exception, you will be presented with three options for the initial setup. In this guide’s environment, **New Installation** is selected.

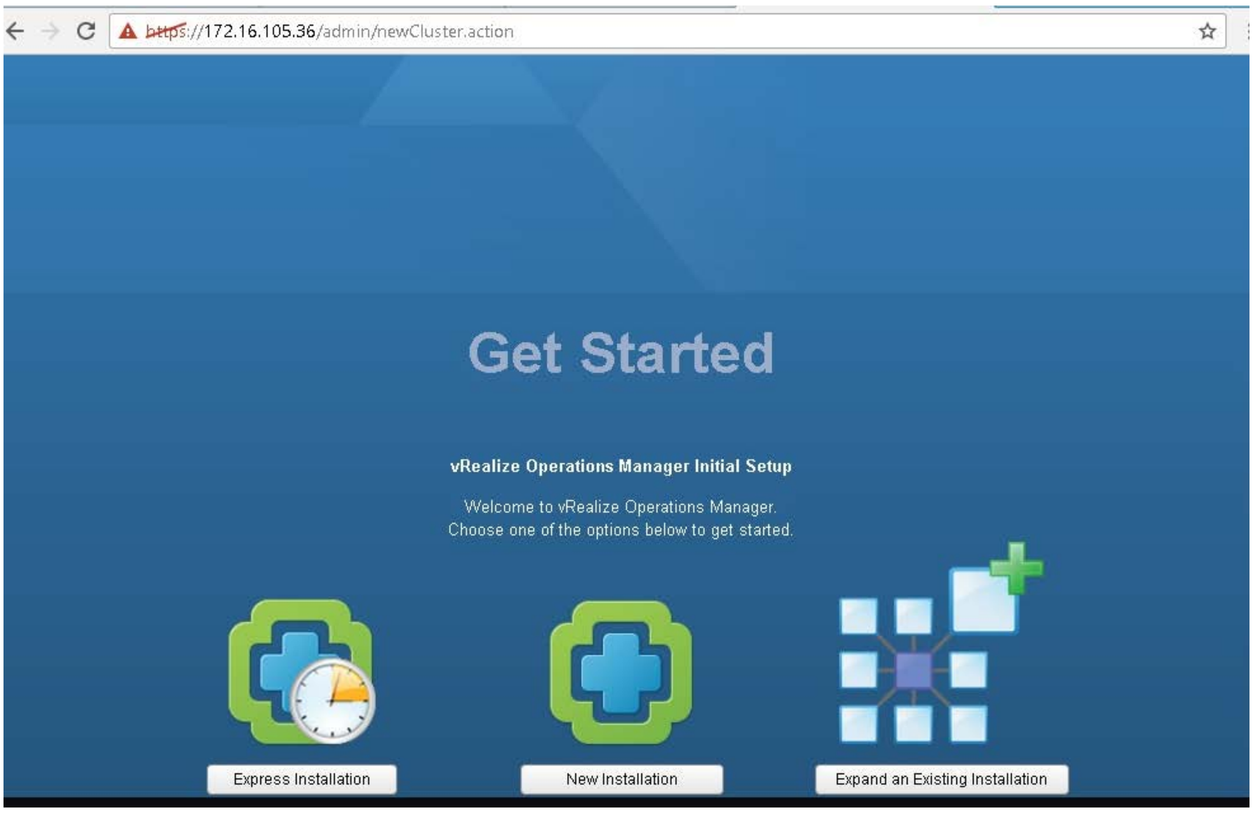
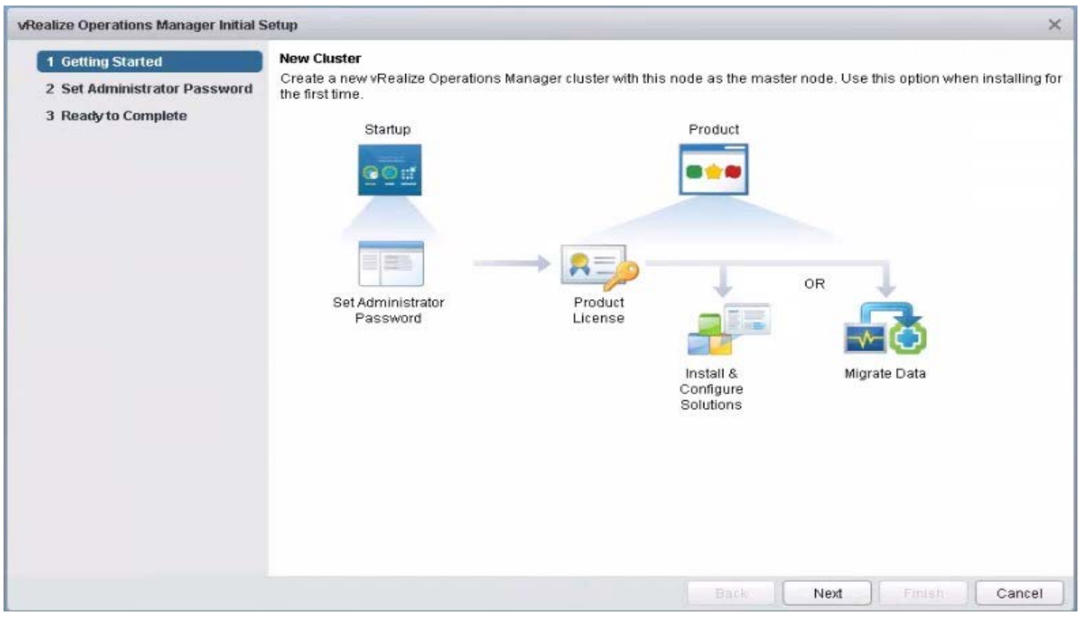

https://172.16.105.36/admin/newCluster.action
Get Started
vRealize Operations Manager Initial Setup
Welcome to vRealize Operations Manager.
Choose one of the options below to get started.
Express Installation
New Installation
Expand an Existing Installation

Figure 150 Install vRealize Operations Manager

As this is the first appliance, a warning message will be displayed. Click **Ye**s.

Click **Next**.


vRealize Operations Manager Initial Setup
1 Getting Started
2 Set Administrator Password
3 Ready to Complete
Startup
Product
Set Administrator Password
Product License
OR
Install & Configure Solutions
Migrate Data
Back
Next
Finish
Cancel

New Cluster

Create a new vRealize Operations Manager cluster with this node as the master node. Use this option when installing for the first time.

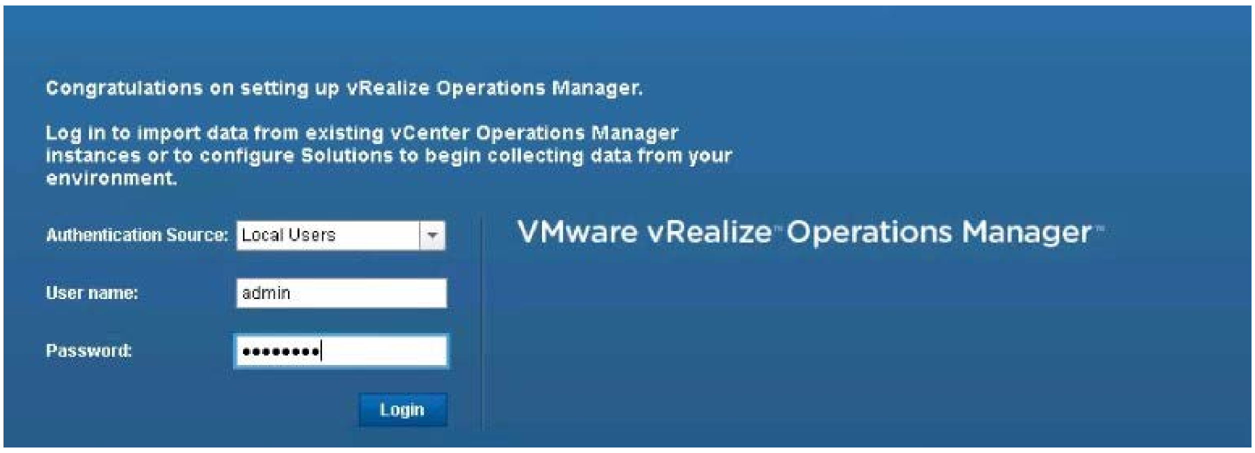
Figure 151 Install vRealize Operations Manager initial setup

Choose the Certificate. In this guide, default is selected. If you have a CA or self-Signed certificate available, it can be installed. Click **Nex**t.

Provide the Cluster Node Name and the NTP Server for your Environment. Click **Next**.

Click **Finish**.

After Clicking **Finish**, you will be redirected to the administration portal of vROps appliance. The vRealize operation cluster status needs to be started by clicking the **Start vRealize Operation Manager**. As this is the first appliance, a warning message will be presented. Click **Yes**, It will take 5-10 minutes complete setup and start the appliance services.



Congratulations on setting up vRealize Operations Manager.

Log in to import data from existing vCenter Operations Manager instances or to configure Solutions to begin collecting data from your environment.

Authentication Source: Local Users

User name: admin

Password: ••••••••

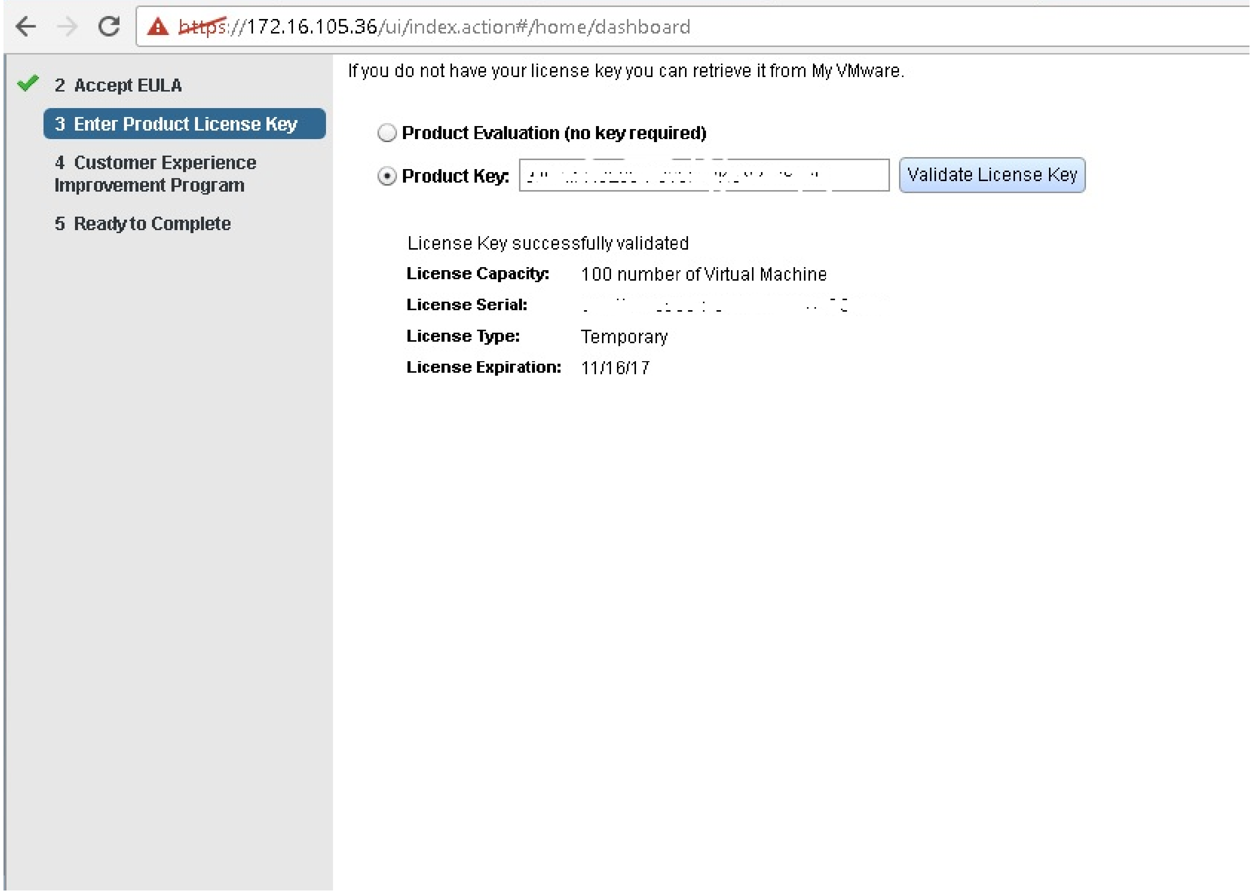
Figure 152 vROps Operations Manager

Once the appliance services have started, open the UI For your vROps appliance by entering the UI URL: https://fqdn or IP address of your vROps appliance/ui/
 and login to the portal with default local user ADMIN.

After login, the vROps Configuration page opens. Click **Next**.

Accept the EULA and click **Next**.

Enter the Product license key. You can also use the product evaluation key for a trial run. Click **Next**.



~~https~~://172.16.105.36/ui/index.action#/home/dashboard

✓ 2 Accept EULA
3 Enter Product License Key
4 Customer Experience Improvement Program
5 Ready to Complete

If you do not have your license key you can retrieve it from My VMware.

○ Product Evaluation (no key required)

● Product Key: [redacted]

License Key successfully validated

License Capacity: 100 number of Virtual Machine

License Serial: [redacted]

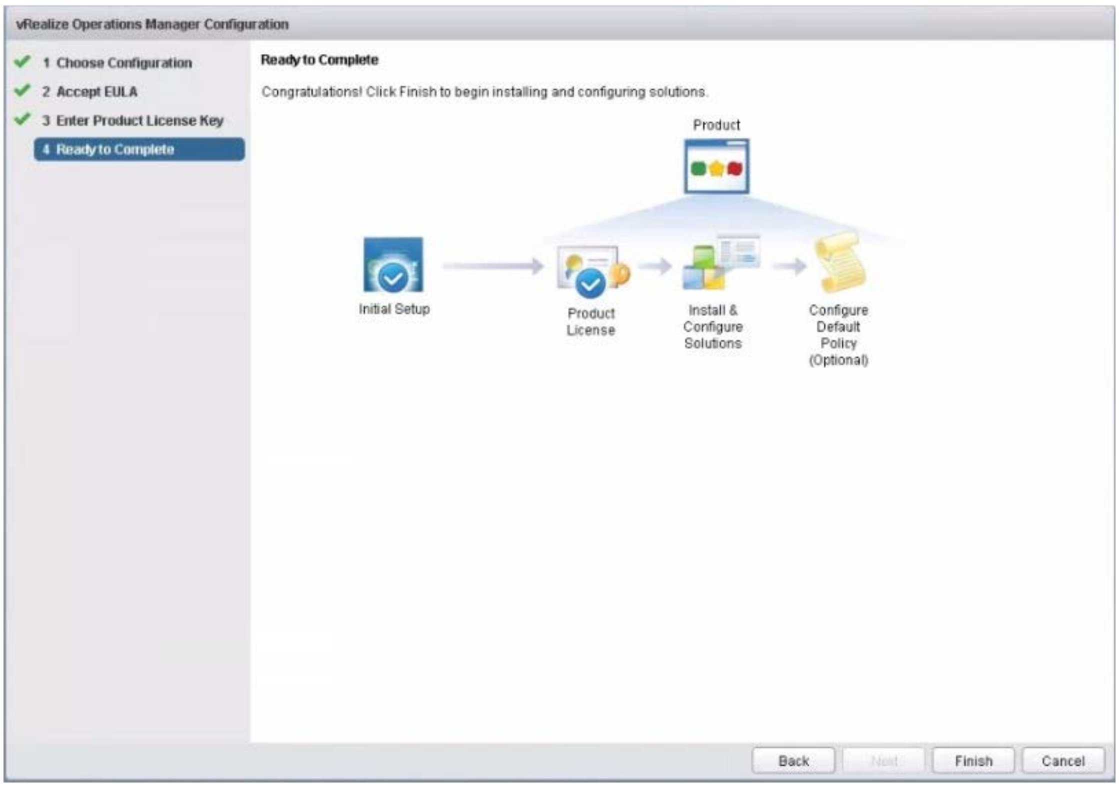
License Type: Temporary

License Expiration: 11/16/17

Figure 153 Enter product key

Select Customer Experience Improvement Program and click **Next**.

The configuration is now complete and the vCenter is ready to configure in the next step. Click **Finish**.



vRealize Operations Manager Configuration

- ✓ 1 Choose Configuration
- ✓ 2 Accept EULA
- ✓ 3 Enter Product License Key
- 4 Ready to Complete

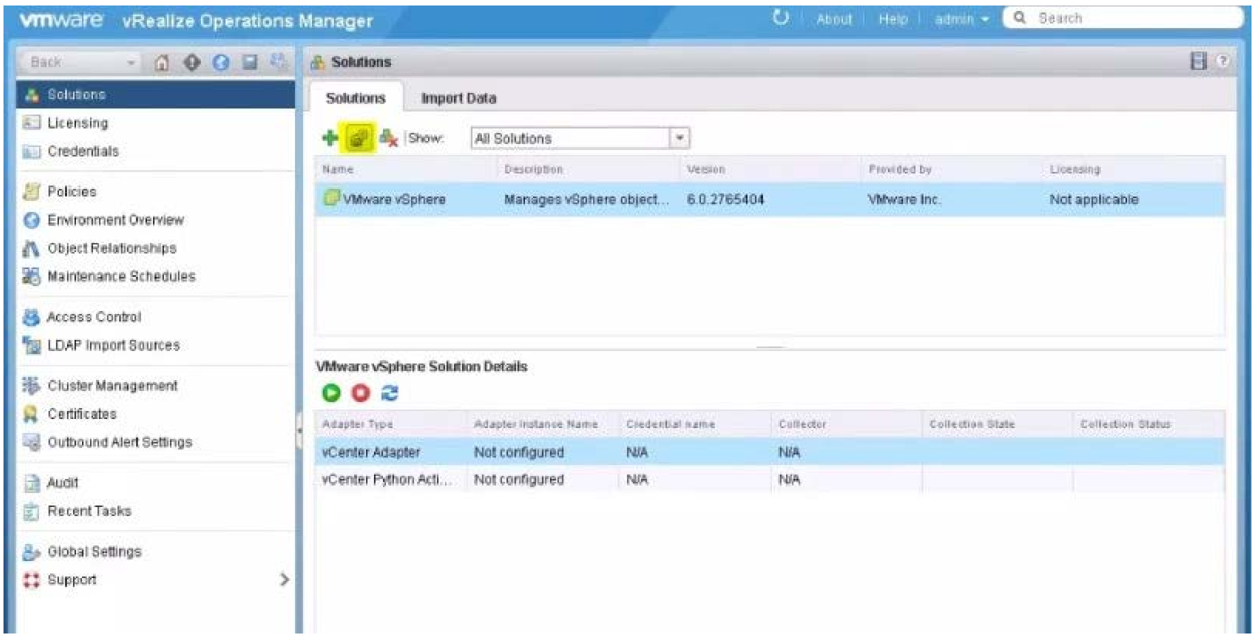
Ready to Complete

Congratulations! Click Finish to begin installing and configuring solutions.

Product
Initial Setup
Product License
Install & Configure Solutions
Configure Default Policy (Optional)
Back
Next
Finish
Cancel

Figure 154 Ready to complete vROps

The Solutions tab opens so the VMware vSphere can be configured by clicking the setting icon (highlighted in the following figure).



Show: All Solutions

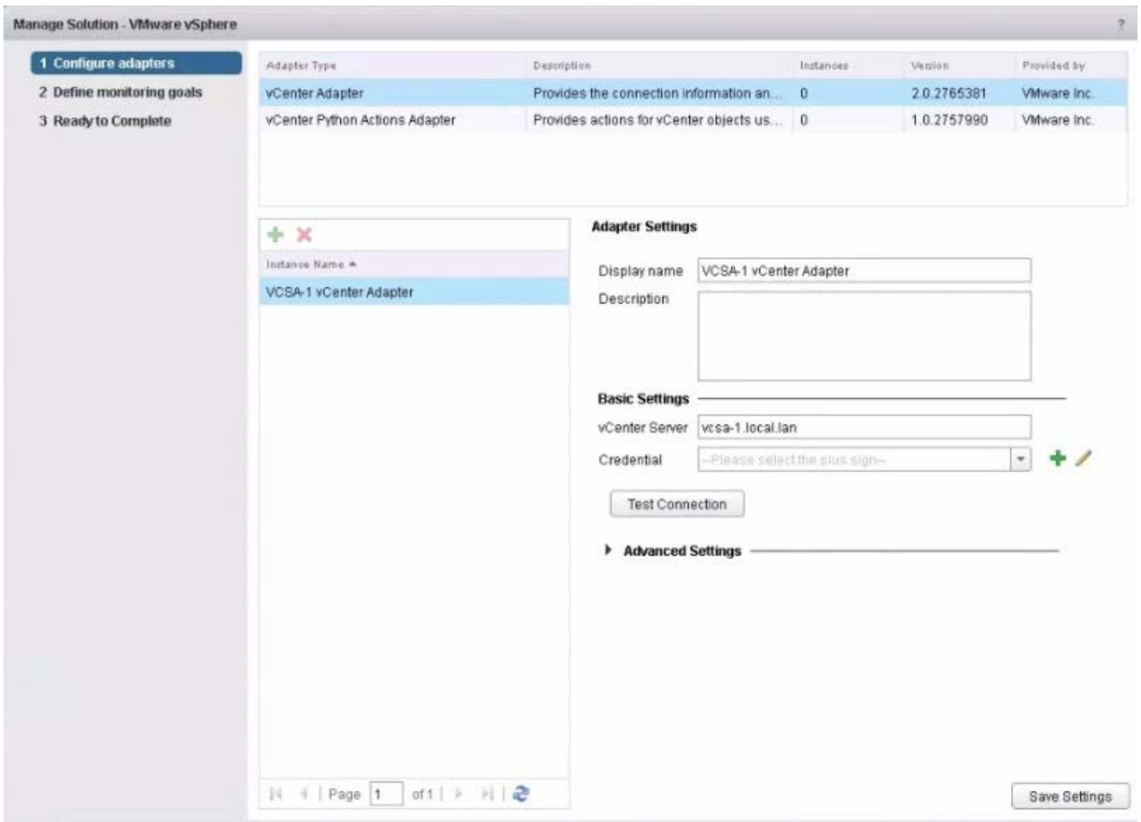
Name	Description	Version	Provided by	Licensing
VMware vSphere	Manages vSphere object...	6.0.2765404	VMware Inc.	Not applicable

VMware vSphere Solution Details

Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
vCenter Adapter	Not configured	N/A	N/A		
vCenter Python Acti...	Not configured	N/A	N/A		

Figure 155 Setting icon to configure VMware vSphere

The following information for vCenter needs to be entered here: Display name, Description, vCenter Server, Credential etc.



Manage Solution - VMware vSphere

1 Configure adapters
2 Define monitoring goals
3 Ready to Complete

Adapter Type	Description	Instances	Version	Provided by
vCenter Adapter	Provides the connection information an...	0	2.0.2765381	VMware Inc.
vCenter Python Actions Adapter	Provides actions for vCenter objects us...	0	1.0.2757990	VMware Inc.

Instance Name
VCSA-1 vCenter Adapter

Adapter Settings

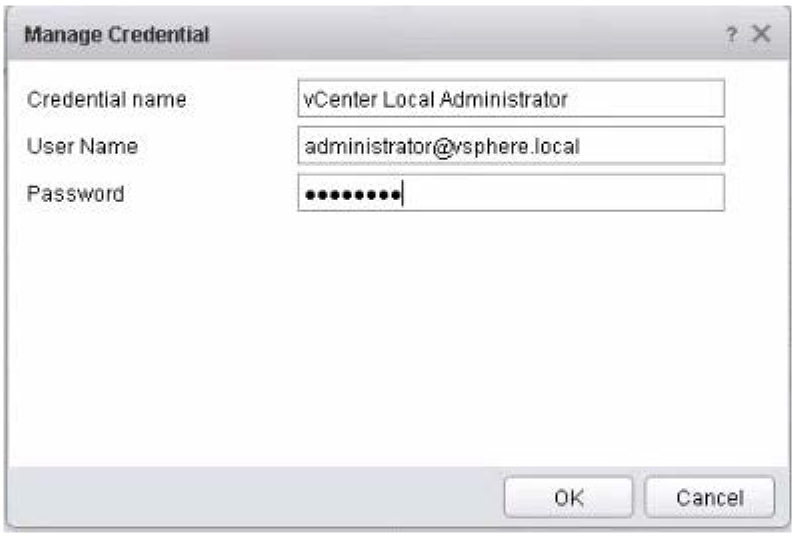
Display name: VCSA-1 vCenter Adapter
Description:

Basic Settings

vCenter Server: vcsa-1.local.lan
Credential: --Please select the plus sign--

Figure 156 Configure adapters

Input the credential after clicking on the credential plus icon.



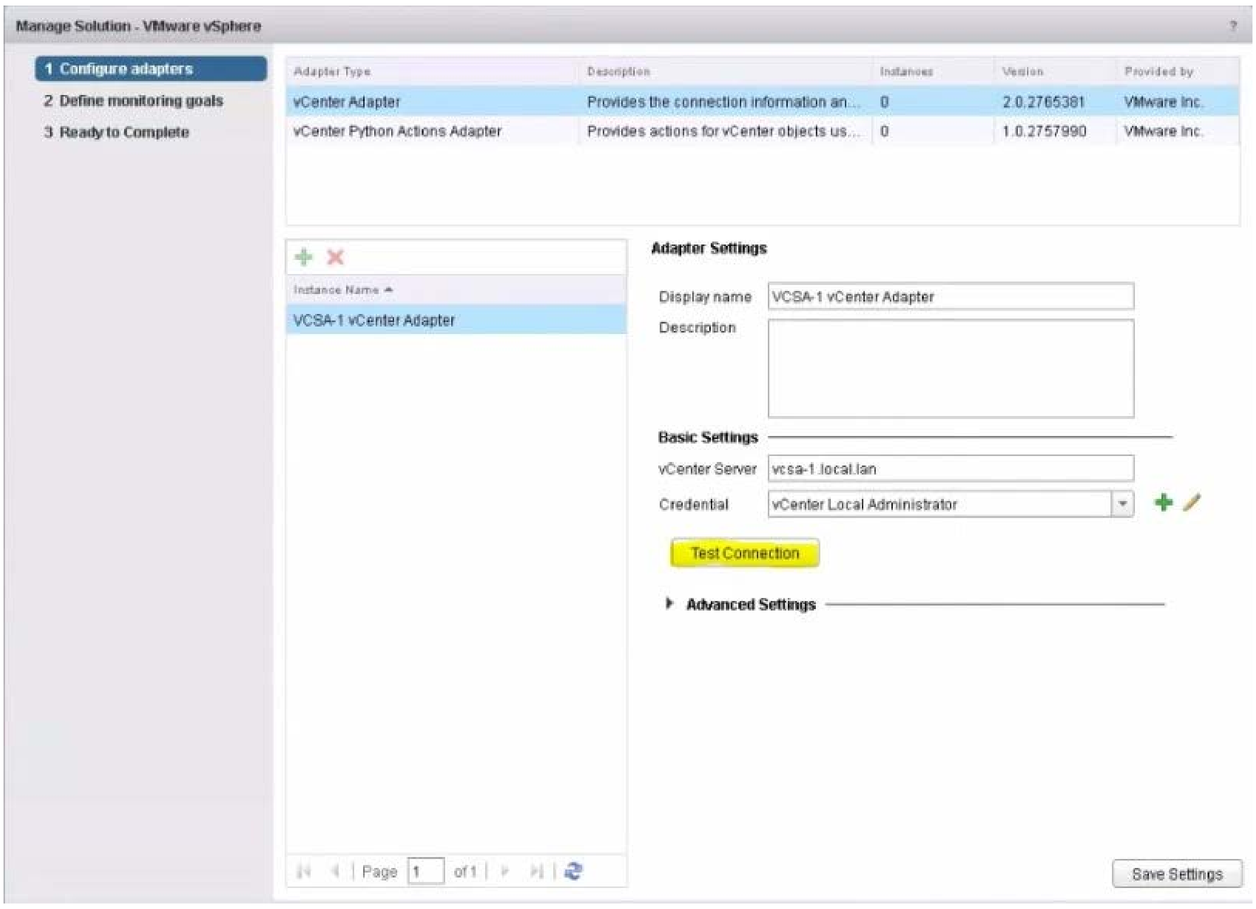
Manage Credential

Credential name: vCenter Local Administrator
User Name: administrator@vsphere.local
Password: ●●●●●●●●●

Figure 157 Input credential

Once all the information is entered, click **Test Connection** and it will communicate with vCenter and match the thumbprint and certificate. Click **OK**.

Click **OK** on Test Connection Successful.


Manage Solution - VMware vSphere

Adapter Type	Description	Instances	Version	Provided by
vCenter Adapter	Provides the connection information an...	0	2.0.2765381	VMware Inc.
vCenter Python Actions Adapter	Provides actions for vCenter objects us...	0	1.0.2757990	VMware Inc.

Instance Name
VCSA-1 vCenter Adapter

Adapter Settings

Display name: VCSA-1 vCenter Adapter

Description:

Basic Settings

vCenter Server: vcsa-1.local.lan

Credential: vCenter Local Administrator

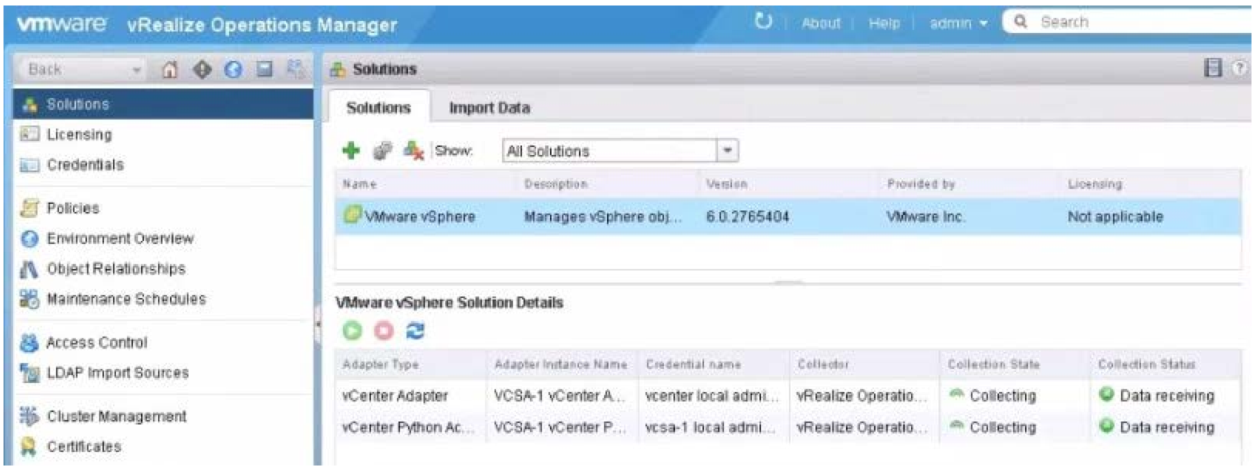
Figure 158 Test Connection

Click on **Save Settings** and select **Next**.

The Monitoring goal will be displayed with the default configuration page, select **Next**.

Click **Finish**.

The collection status now shows as Collecting in the collecting state column.



Show: All Solutions

Name	Description	Version	Provided by	Licensing
VMware vSphere	Manages vSphere obj...	6.0.2765404	VMware Inc.	Not applicable

VMware vSphere Solution Details

Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
vCenter Adapter	VCSA-1 vCenter A...	vcenter local admi...	vRealize Operatio...	Collecting	Data receiving
vCenter Python Ac...	VCSA-1 vCenter P...	vcsa-1 local admi...	vRealize Operatio...	Collecting	Data receiving

Figure 159 VMware vSphere solution details

Click on the home button at the top of the page to see the first Collection and Dashboards.

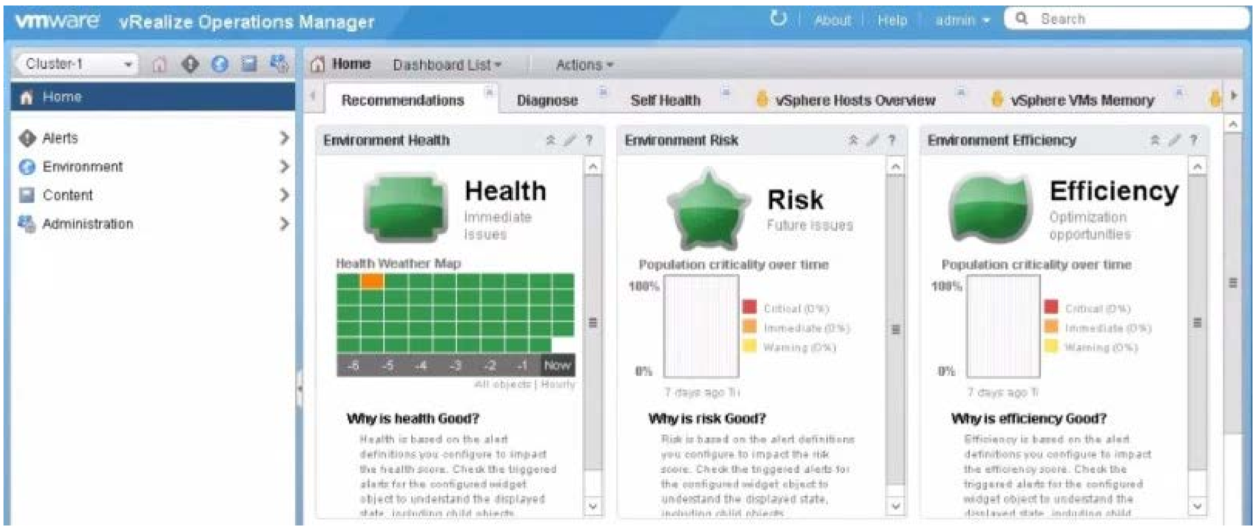


Figure 160 Dashboards

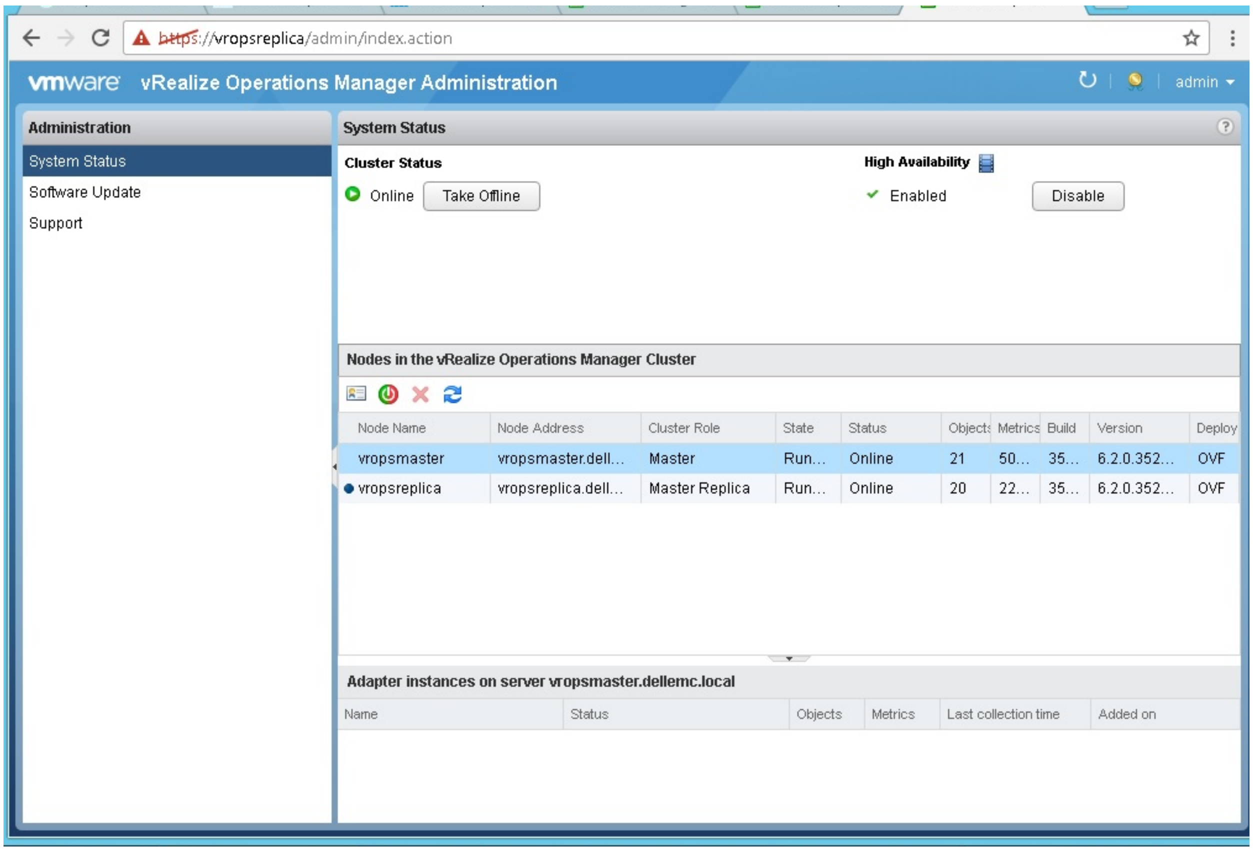
10.1 Install vROps Replica

Deploy another vRealize Operations Manager data node in the management cluster and convert it to a replica node vropseplica to form the vRealize Operations Manager cluster.

Connect both instances (vROps master and Replica) to the Management VLAN network.

Register a FQDN for both VMs in the DNS.

For detailed configuration steps, refer to the VMware vRealize Operations Manager 6.2 Help guide (https://www.vmware.com/support/pubs/vrealize-operations-manager-pubs.html)


https://vropsreplica/admin/index.action
vmware vRealize Operations Manager Administration
admin
Administration
System Status
Software Update
Support
System Status
Cluster Status
Online
Take Offline
High Availability
Enabled
Disable
Nodes in the vRealize Operations Manager Cluster

Node Name	Node Address	Cluster Role	State	Status	Objects	Metrics	Build	Version	Deploy
vropsmaster	vropsmaster.dell...	Master	Run...	Online	21	50...	35...	6.2.0.352...	OVF
vropsreplica	vropsreplica.dell...	Master Replica	Run...	Online	20	22...	35...	6.2.0.352...	OVF

Adapter instances on server vropsmaster.dellemc.local

Name	Status	Objects	Metrics	Last collection time	Added on

Figure 161 Install vROps Replica

11 Install VMware vRealize Log Insight

11.1 Installation

Deploy vRealize Log Insight instance VRLImaster into the management cluster in standalone mode.

Deploy two more vRealize Log Insight instances as worker nodes VRLIworker1 and VRLIworker2 in management cluster NFV_MGMT_CLUSTER and add it to VRLImaster to form the vRealize Log Insight HA cluster.

Connect all instances to the Management VLAN network.

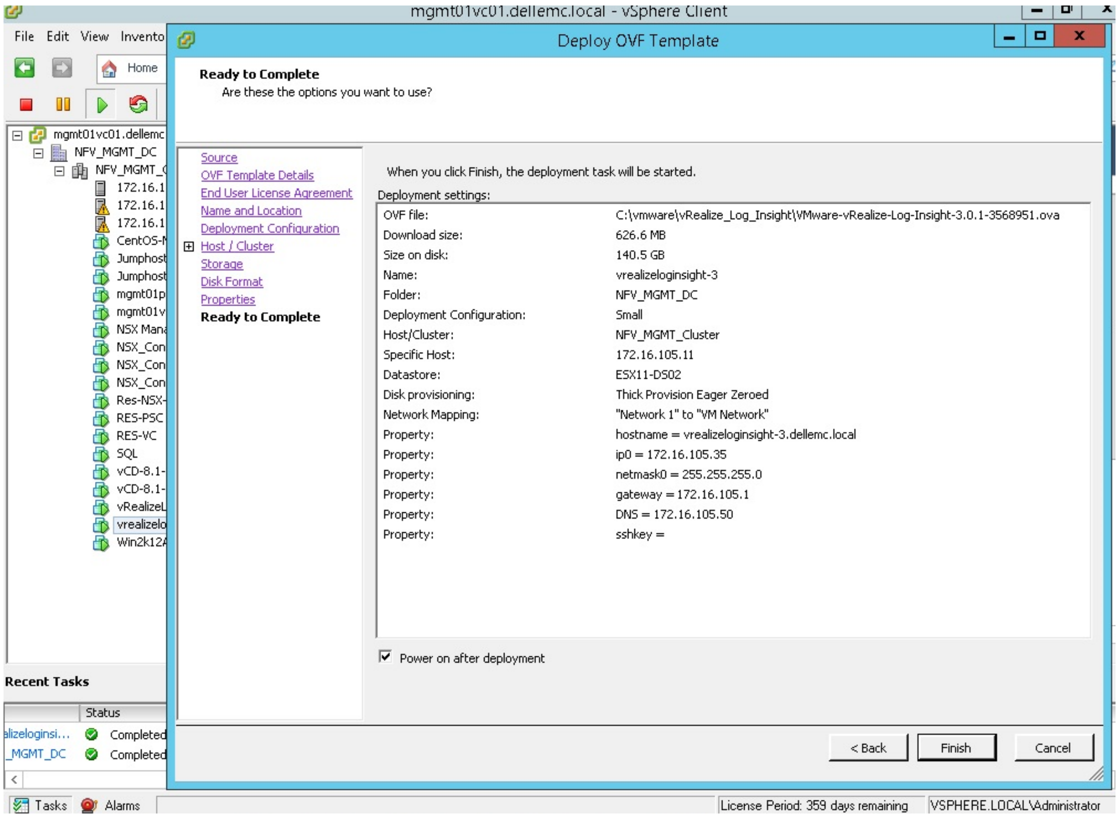
Register the FQDN for both VMs in the DNS.

Configure integrated load balancer between all instances.

For detailed installation steps, refer to the VMware vRealize Log Insight Information Center. (https://www.vmware.com/support/pubs/log-insight-pubs.html)

11.1.1 Configuration

Deploy the OVF template of Log Insight.



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\vmware\vRealize_Log_Insight\VMware-vRealize-Log-Insight-3.0.1-3568951.ova
Download size:	626.6 MB
Size on disk:	140.5 GB
Name:	vrealizeloginsight-3
Folder:	NFV_MGMT_DC
Deployment Configuration:	Small
Host/Cluster:	NFV_MGMT_Cluster
Specific Host:	172.16.105.11
Datastore:	ESX11-DS02
Disk provisioning:	Thick Provision Eager Zeroed
Network Mapping:	"Network 1" to "VM Network"
Property:	hostname = vrealizeloginsight-3.dellemc.local
Property:	ip0 = 172.16.105.35
Property:	netmask0 = 255.255.255.0
Property:	gateway = 172.16.105.1
Property:	DNS = 172.16.105.50
Property:	sshkey =

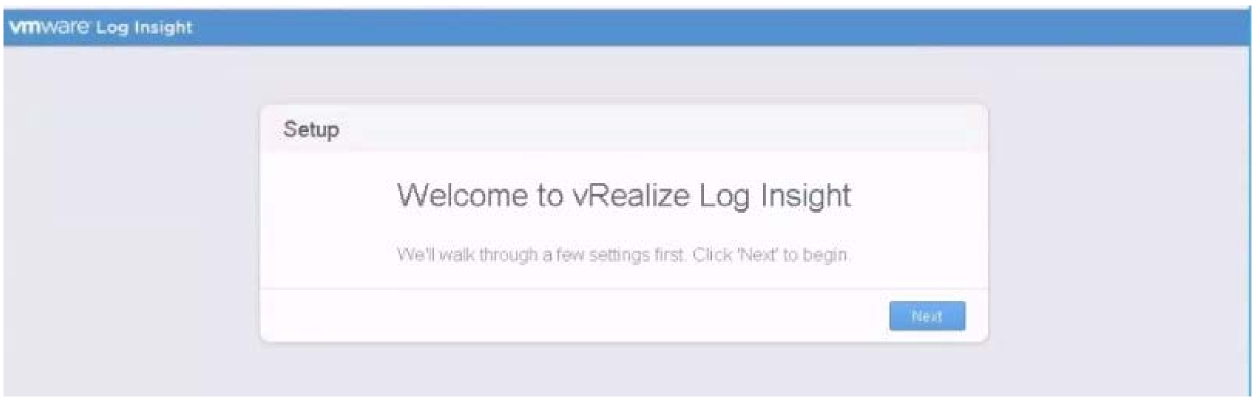
☑ Power on after deployment

Figure 162 Deploy the OVF template of Log Insight

Once the VM has fully booted and the welcome screen opens on the VM console, the appliance can be configured.

Point a browser to the IP address or FQDN of the Log Insight appliance.

The vRealize Log Insight welcome screen should open. Click **Next**.

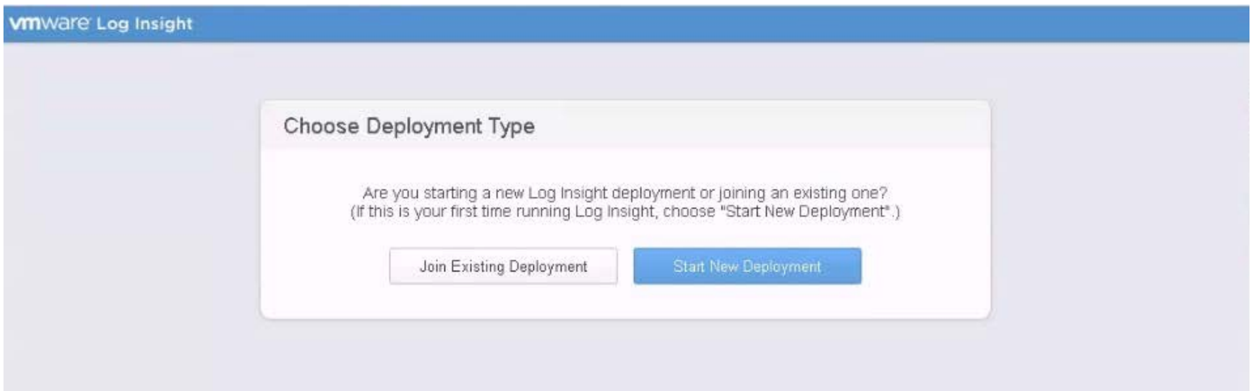


Setup

Welcome to vRealize Log Insight

We'll walk through a few settings first. Click 'Next' to begin.

Figure 163 vRealize welcome screen



Choose Deployment Type

Are you starting a new Log Insight deployment or joining an existing one?
(If this is your first time running Log Insight, choose "Start New Deployment".)

Figure 164 vRealize Deployment type

Provide an email address for the admin user. Provide a password for the built-in admin user. Click **Save** and **Continue**.

Enter the license key and click Add License Key.

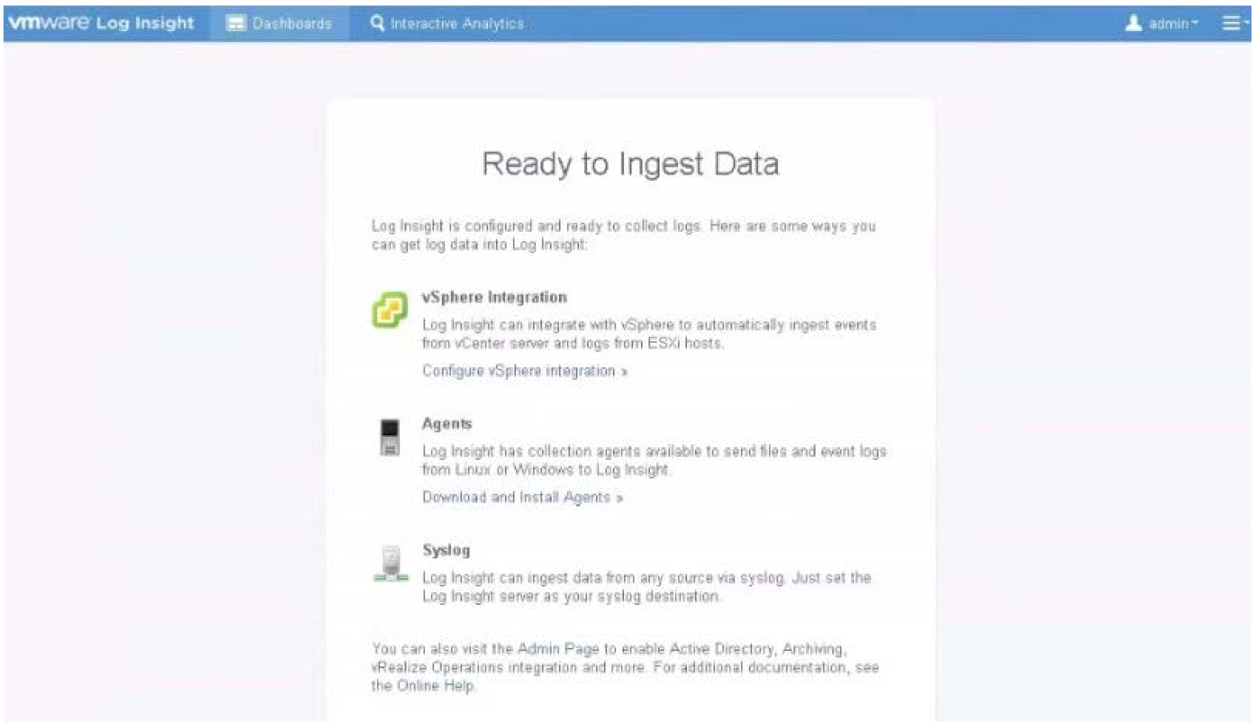
If the license key is valid, you will be able to proceed. Click **Continue**.

Enter a valid email address for system notifications. Note that these will be alerts related to the health of the Log Insight appliance itself, such as disk full alerts. If you wish to take part in the VMware Customer Experience Improvement Program, check the box. Click **Save** and **Continue**.

It is recommended that you synchronize server time with the same NTP servers used by the rest of your vSphere infrastructure. If an NTP server is not available (as in the example show in this guide), you can choose to synchronize time with the underlying ESXi host. Click **Save** and **Continue**.

If required, configure SMTP settings for sending emails alerts. Click **Save** and **Continue**.
At this stage, initial setup is nearly complete. Click **Finish**

The Configure vSphere Integration link splash screen is now presented.



Ready to Ingest Data

Log Insight is configured and ready to collect logs. Here are some ways you can get log data into Log Insight:

vSphere Integration
Log Insight can integrate with vSphere to automatically ingest events from vCenter server and logs from ESXi hosts.
Configure vSphere integration »

Agents
Log Insight has collection agents available to send files and event logs from Linux or Windows to Log Insight.
Download and Install Agents »

Syslog
Log Insight can ingest data from any source via syslog. Just set the Log Insight server as your syslog destination.

You can also visit the Admin Page to enable Active Directory, Archiving, vRealize Operations integration and more. For additional documentation, see the Online Help.

Figure 165 Ready to Ingest Data

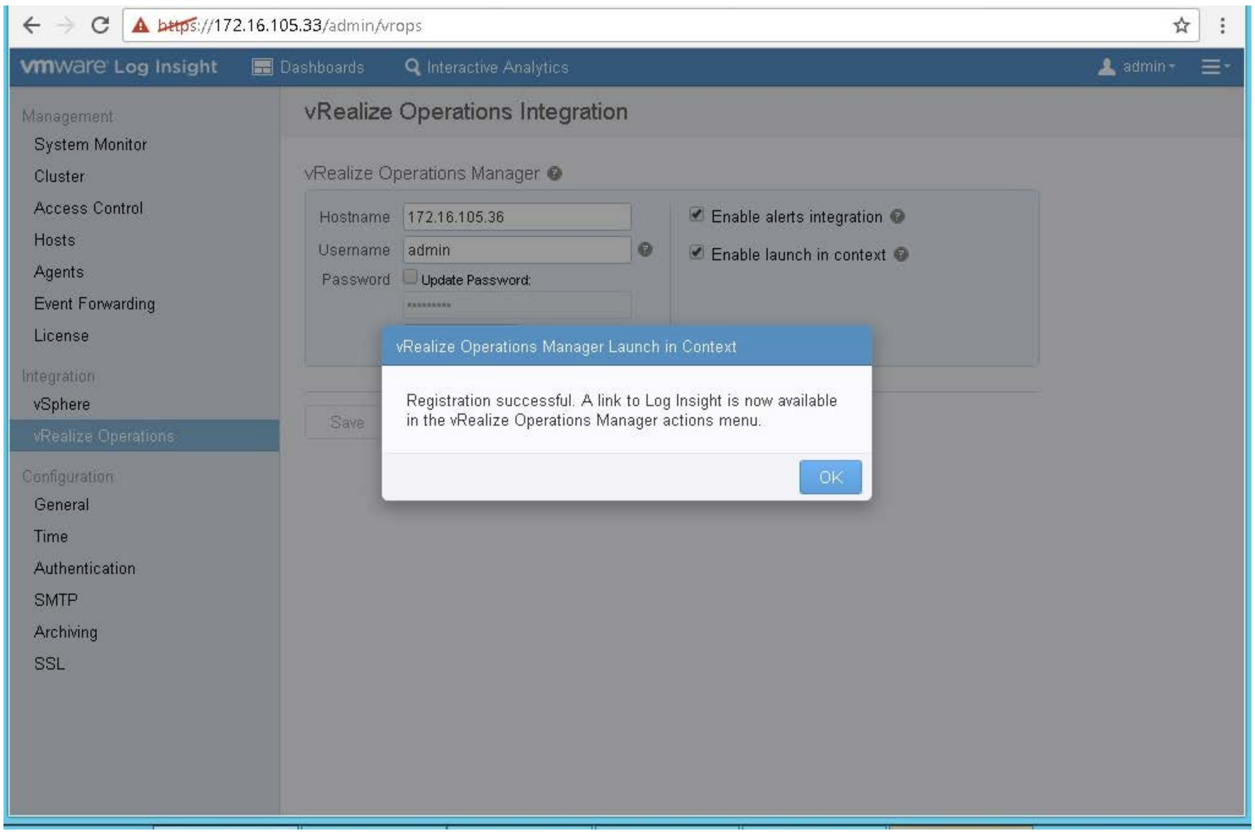
Under the Integration section on the left hand side, make sure the vSphere section is selected. Provide the FQDN of the vCenter server along with a user account and password with administrator rights to the vCenter object. Click **Test Connection**. If the test is successful, make sure that both boxes for collecting from vCenter and the ESXi hosts are checked and click **Save**.

All hosts managed by the specified vCenter server will be configured to send their logs to the Log Insight server.

Once the configuration of ESXi hosts has completed click **OK**.

Next, we will need to configure integration with vRealize Operations Manager. On the left hand side under Integration, click on **vRealize Operations**.

Provide the FQDN of the vRealize Operations manager server along with a local user account and password (The default vROps admin account is used in this guide). If the test is successful, make sure that both boxes for alerts integration and launch in context are checked and click **Save**.



~~https~~://172.16.105.33/admin/vrops

vRealize Operations Integration

vRealize Operations Manager

Hostname 172.16.105.36

Username admin

Password □ Update Password: *********

☑ Enable alerts integration

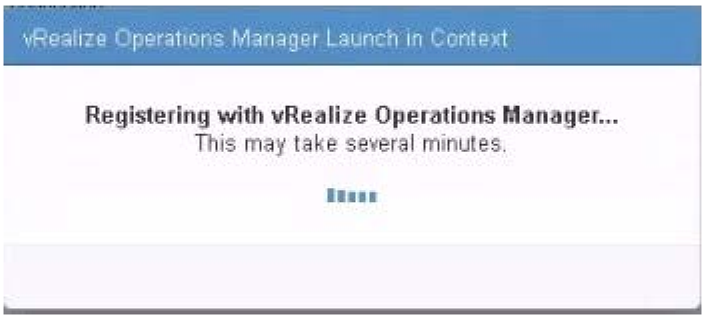
☑ Enable launch in context

vRealize Operations Manager Launch in Context

Registration successful. A link to Log Insight is now available in the vRealize Operations Manager actions menu.

Figure 166 Registration Successful

Registering with vRealize Operations Manager can take a while.

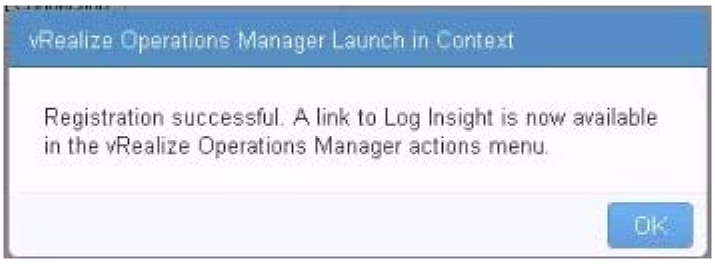


vRealize Operations Manager Launch in Context

Registering with vRealize Operations Manager...
This may take several minutes.

Figure 167 Registering with vRealize Operations Manager

Once the following Registration Successful message appears, click **OK**.



vRealize Operations Manager Launch in Context

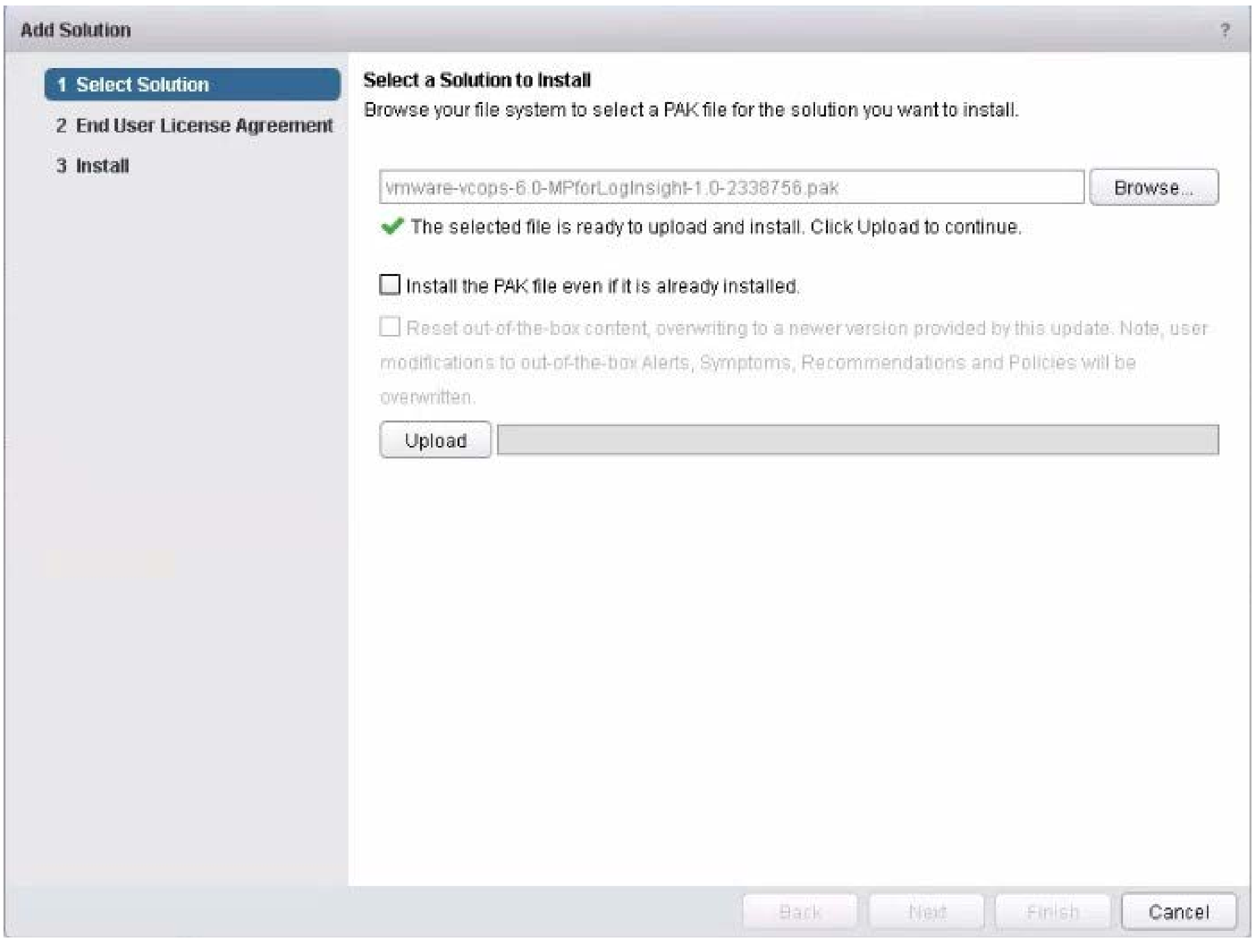
Registration successful. A link to Log Insight is now available in the vRealize Operations Manager actions menu.

Figure 168 Registration Successful

Click on the Interactive Analytics link at the top of the page and the events being gathered by Log Insight should be seen.

Now to complete the integration with vROps install and configure the Log Insight Management Pack.

Log in to vROps and go to the Solutions section of the administration page. Click on the green plus sign to add a new management pack.



Select a Solution to Install

Browse your file system to select a PAK file for the solution you want to install.

vmware-vcops-6.0-MPforLogInsight-1.0-2338756.pak

✓ The selected file is ready to upload and install. Click Upload to continue.

□ Install the PAK file even if it is already installed.

□ Reset out-of-the-box content, overwriting to a newer version provided by this update. Note, user modifications to out-of-the-box Alerts, Symptoms, Recommendations and Policies will be overwritten.

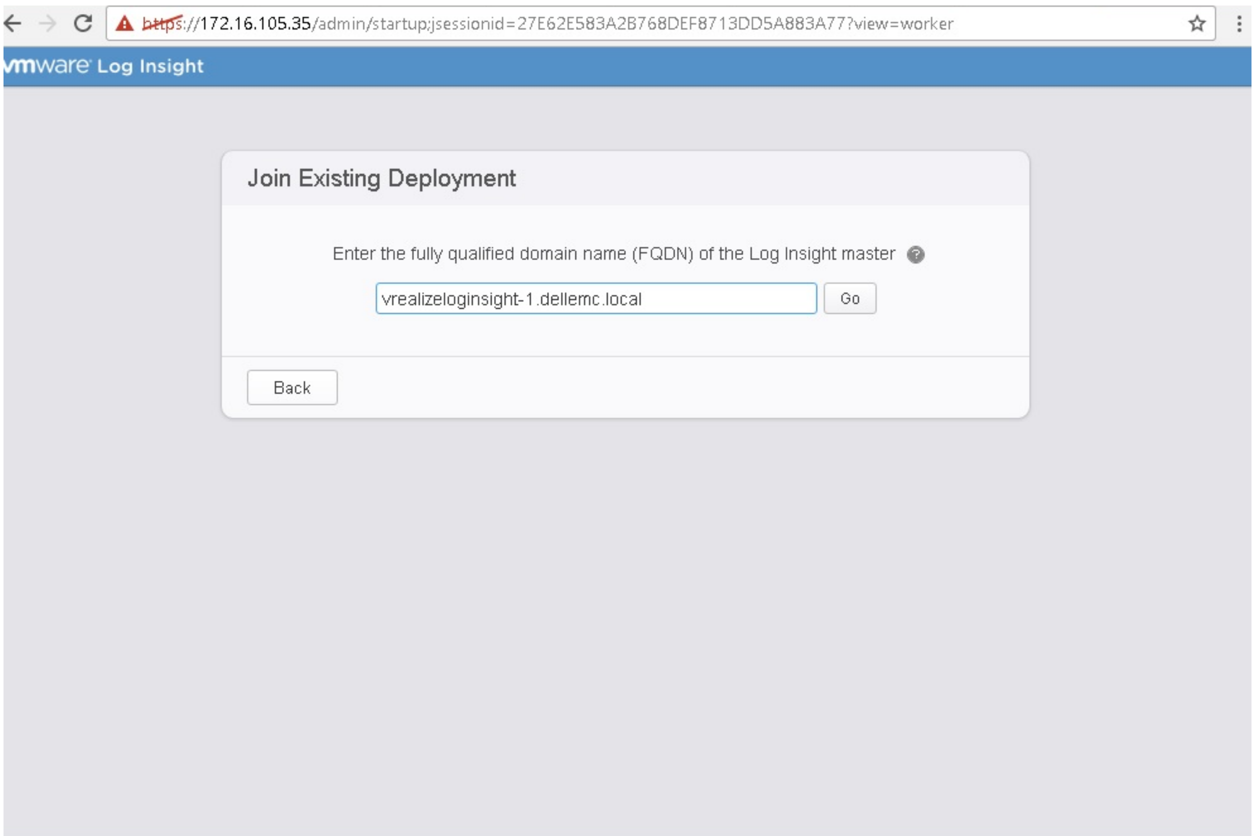
Figure 169 Select a solution to install

A new management pack is now listed under Solutions. No configuration of the vRealize Log Insight Adapter is needed.

To test that the integration between vROps and Log Insight is working, go to the Environment section of vROps and drill down to a cluster, host or virtual machine object. Clicking on the Actions drop-down menu above the Summary page for this object, you should now have an additional option – Search for logs in vRealize Log Insight. Click on this option.

Deploy two more vRealize Log Insight instances as worker nodes.

For Worker nodes, select J**oin Existing Deployment**.

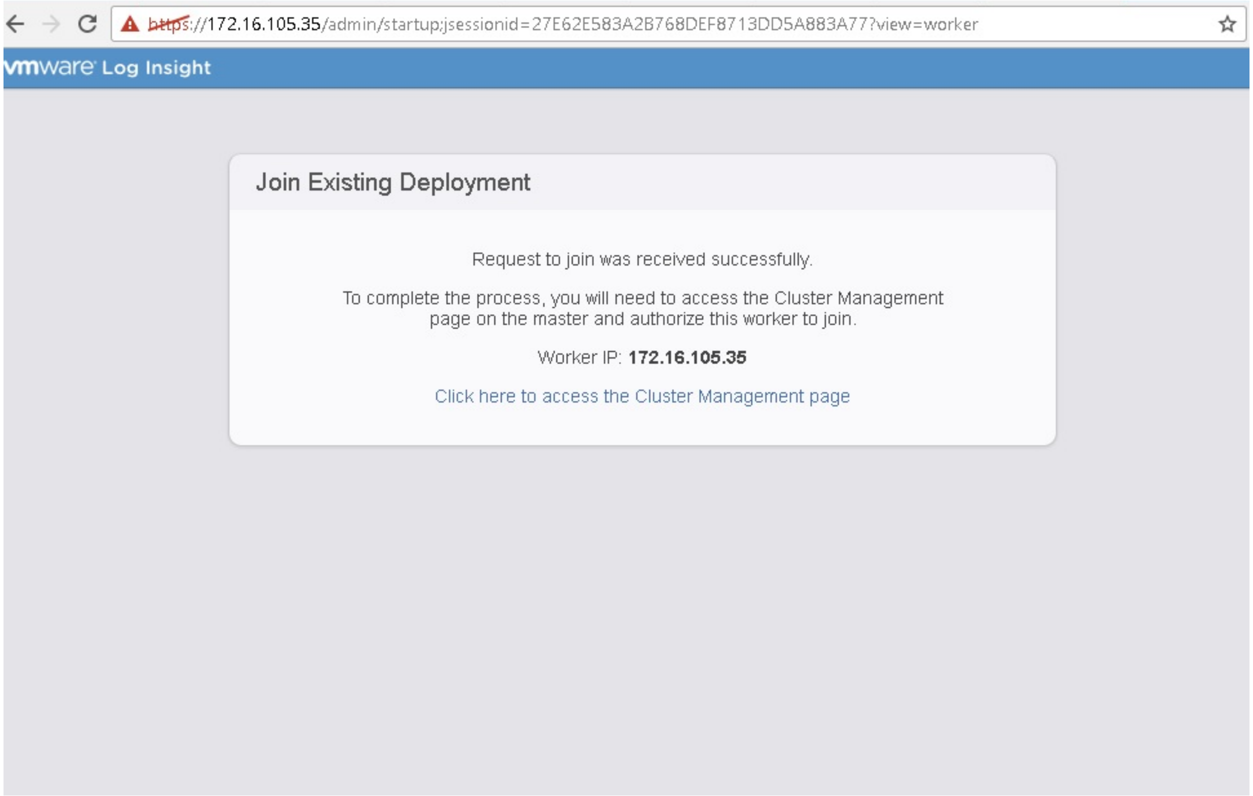

https://172.16.105.35/admin/startup;jsessionid=27E62E583A2B768DEF8713DD5A883A77?view=worker

Join Existing Deployment

Enter the fully qualified domain name (FQDN) of the Log Insight master

vrealizeloginsight-1.dellemc.local

Figure 170 Join existing deployment


https://172.16.105.35/admin/startup;jsessionid=27E62E583A2B768DEF8713DD5A883A77?view=worker

Join Existing Deployment

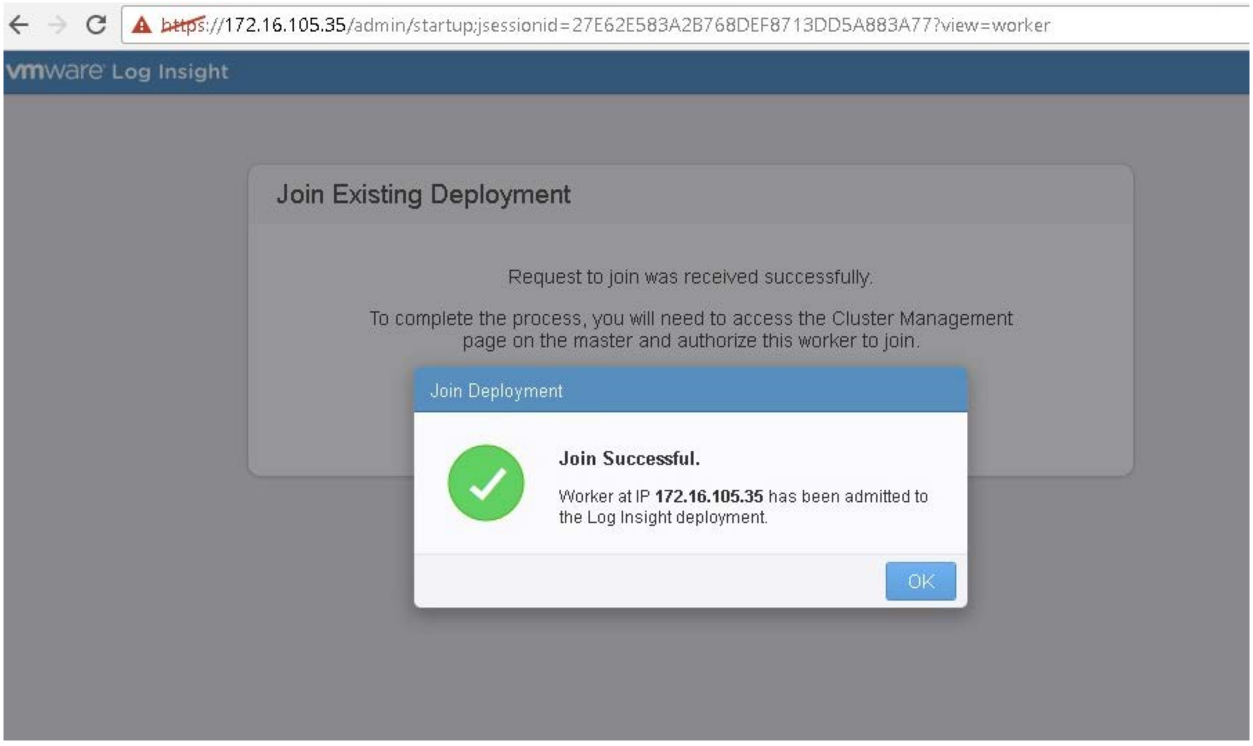
Request to join was received successfully.

To complete the process, you will need to access the Cluster Management page on the master and authorize this worker to join.

Worker IP: **172.16.105.35**

Click here to access the Cluster Management page

Figure 171 Successful join request



https://172.16.105.35/admin/startup;jsessionid=27E62E583A2B768DEF8713DD5A883A77?view=worker
vmware Log Insight
Join Deployment
OK

Join Existing Deployment

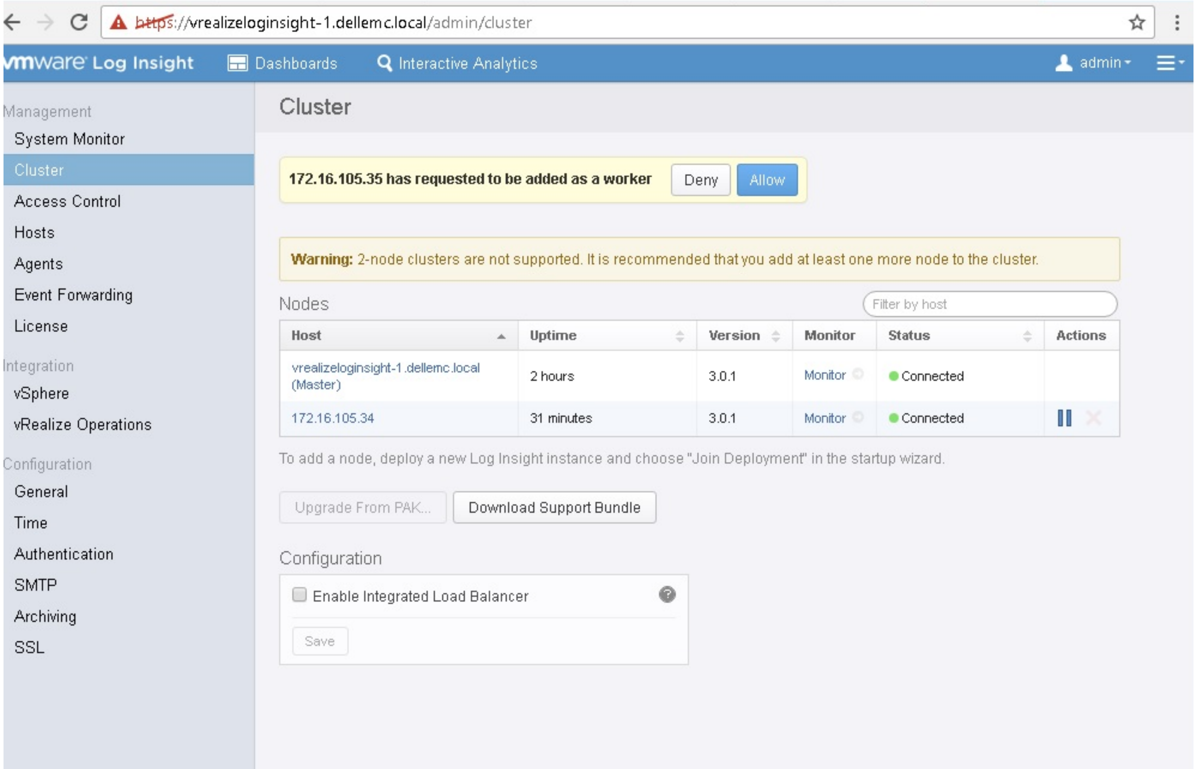
Request to join was received successfully.

To complete the process, you will need to access the Cluster Management page on the master and authorize this worker to join.

Join Successful.

Worker at IP **172.16.105.35** has been admitted to the Log Insight deployment.

Figure 172 Join Successful



Cluster

172.16.105.35 has requested to be added as a worker

Warning: 2-node clusters are not supported. It is recommended that you add at least one more node to the cluster.

Nodes

Host	Uptime	Version	Monitor	Status	Actions
vrealizeloginsight-1.dellemc.local (Master)	2 hours	3.0.1	Monitor	● Connected	
172.16.105.34	31 minutes	3.0.1	Monitor	● Connected	

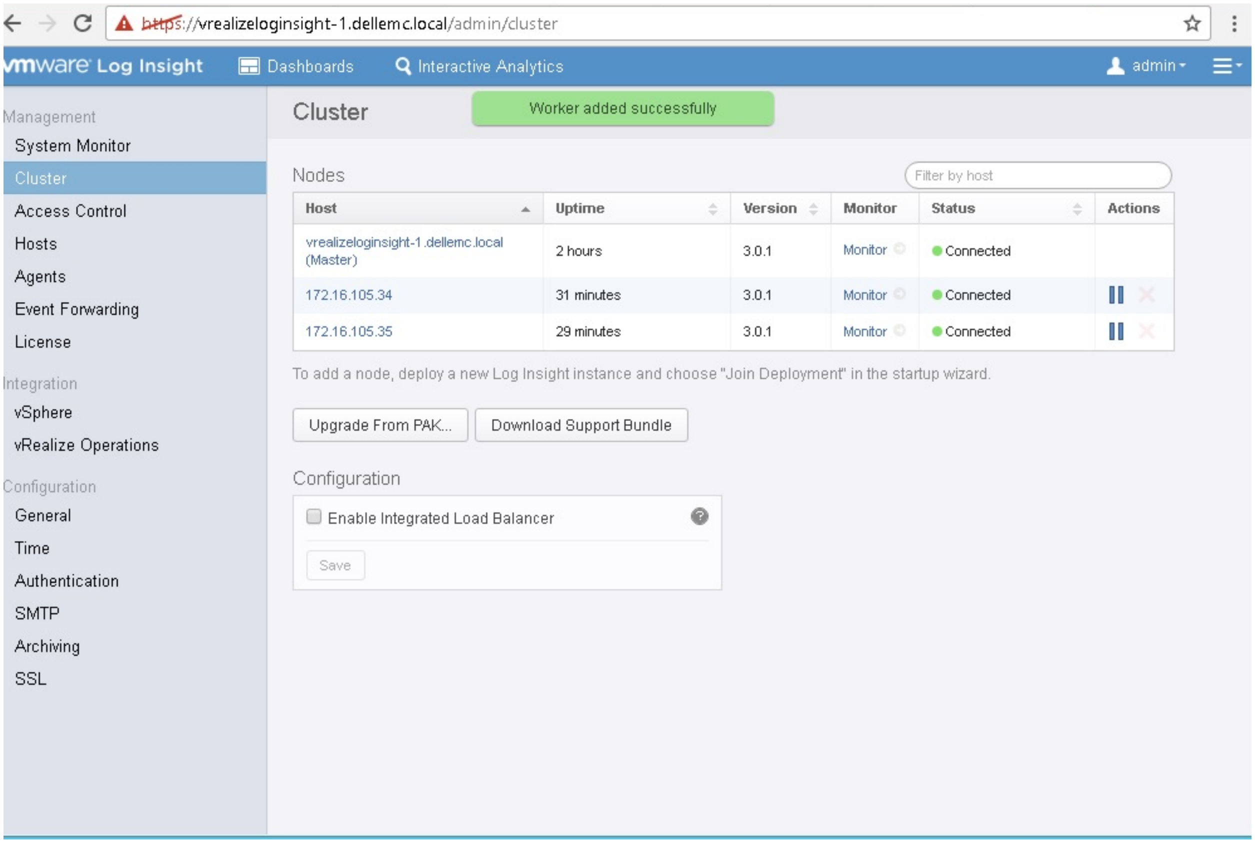
To add a node, deploy a new Log Insight instance and choose "Join Deployment" in the startup wizard.

Configuration

□ Enable Integrated Load Balancer

Figure 173 Allow worker to be added to the cluster

Both the worker nodes are joined successfully.



Worker added successfully

Host	Uptime	Version	Monitor	Status	Actions
vrealizeloginsight-1.dellemc.local (Master)	2 hours	3.0.1	Monitor	● Connected	
172.16.105.34	31 minutes	3.0.1	Monitor	● Connected	❚❚ ✕
172.16.105.35	29 minutes	3.0.1	Monitor	● Connected	❚❚ ✕

To add a node, deploy a new Log Insight instance and choose "Join Deployment" in the startup wizard.

□ Enable Integrated Load Balancer

Figure 174 Deploy the OVF template of Log Insight

12 Install VMware vSphere Data Protection (VDP)

12.1 Installation

Before you deploy vSphere Data Protection (VDP), you must add forward and reverse lookup entry to the DNS server for the VDP appliance’s IP address and Fully Qualified Domain Names (FQDN).

VDP leverages VMware Tools to synchronize time through NTP. All vSphere hosts and the vCenter server must have NTP configured properly. The VDP appliance gets the correct time through vSphere and must not be configured with NTP.

Create a separate shared data store VDP_Datastore visible to all hosts in NFV_MGMT_CLUSTER for the deployment of the VDP appliance. Data store size should be greater than 6TB.

VDP_Datastore can also be used to store the backup data or an external storage may be used for backup data.

Download the vSphere Data Protection appliance OVA file and deploy it in cluster NFV_MGMT_CLUSTER on VDP_Datastore.

Assign a static IP address from the Management VLAN network.

Refer to the deploying the OVF Template in the Administrators Guide for detailed steps

Refer to the vSphere Data Protection Administrators Guide for more details.

12.2 Configuration

After the appliance is deployed and powered on, in a browser window open **https://<IP_address_VDP_appliance>:8543/vdp-configure/**

Follow the steps under Initial Configuration in the vSphere Data Protection Administrators Guide.

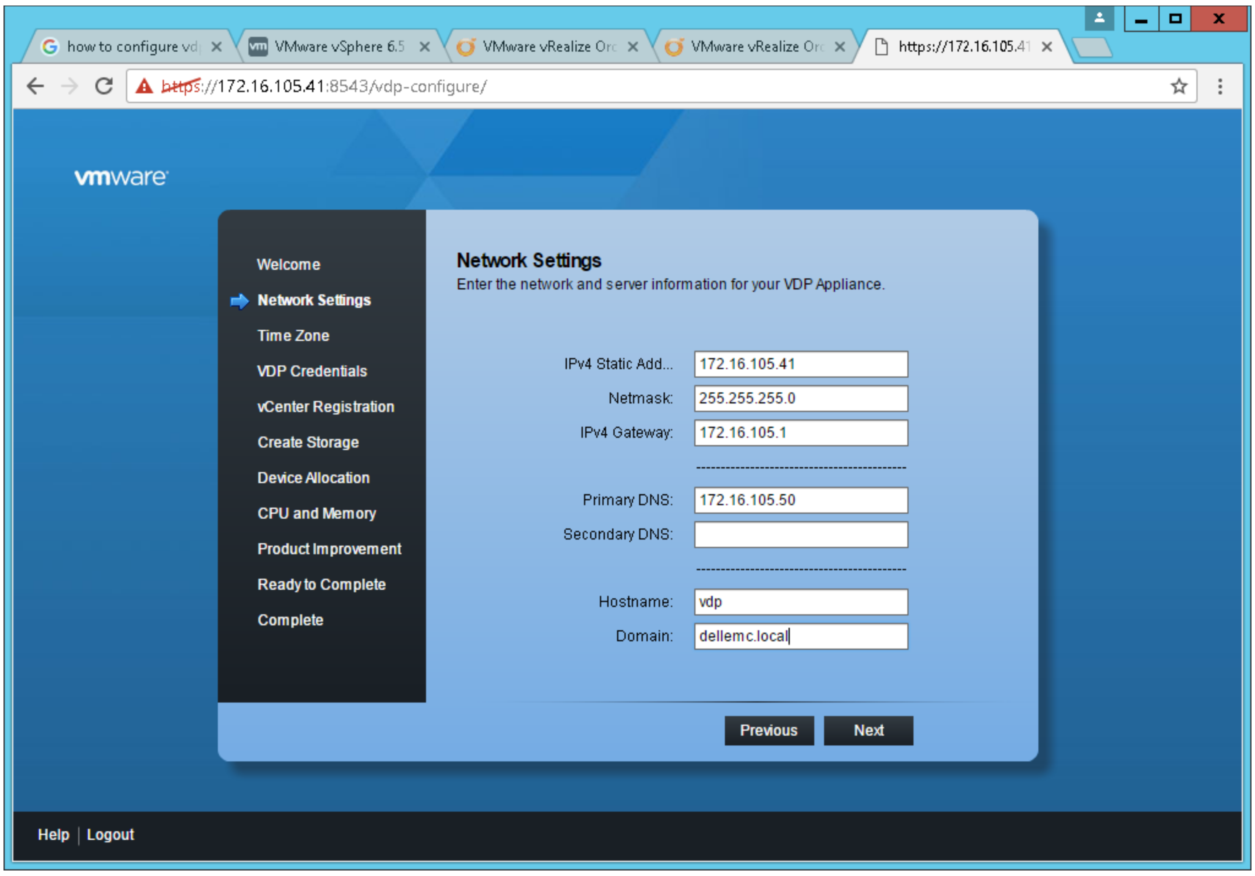
Register vCenter mgmt. with the appliance.

Create new storage of 6TB (min 0.5 TB) in the **Create New Storage** step.

Create backup data partition on a separate dedicated external storage device than the Virtual SAN datastore on which the management components are deployed.

To manage the backups, log in to the vSphere Web client of vCentermgmt and select vSphere Data Protection from the navigation menu after selecting the vSphere Data Protection Appliance.

Test the backup and restore.



Network Settings

Enter the network and server information for your VDP Appliance.

IPv4 Static Add...: 172.16.105.41

Netmask: 255.255.255.0

IPv4 Gateway: 172.16.105.1

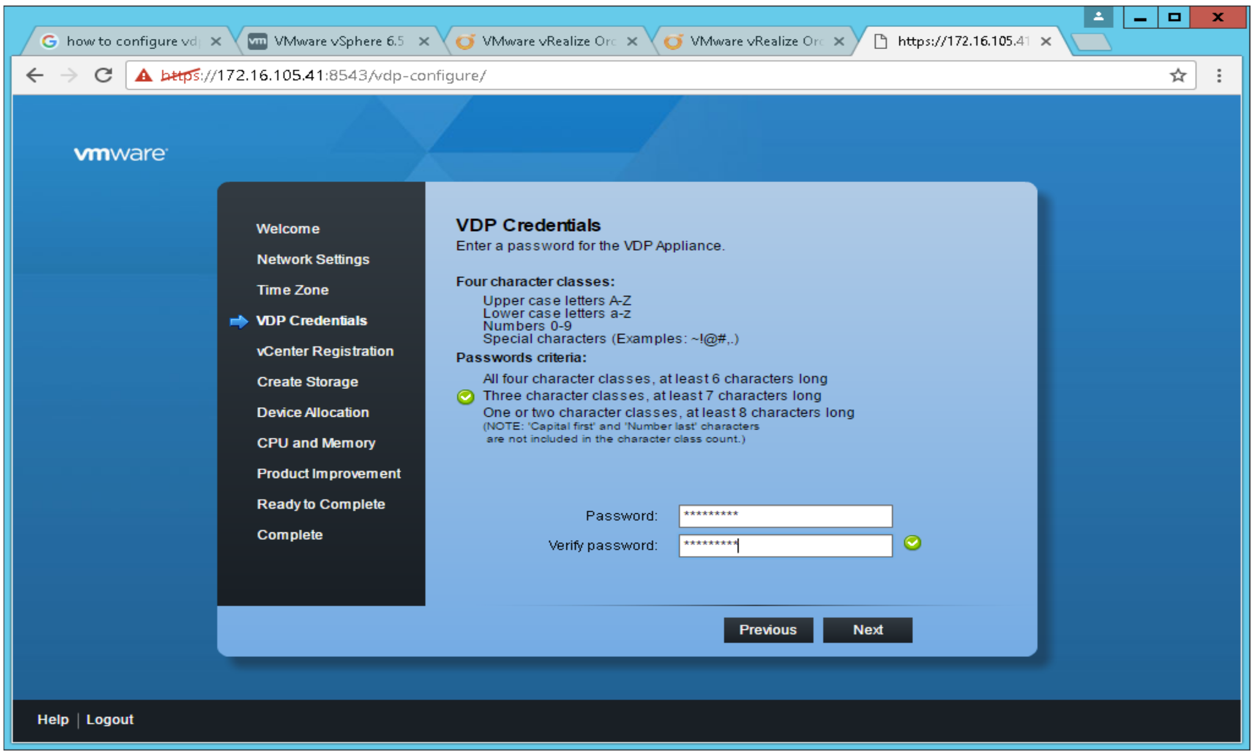
Primary DNS: 172.16.105.50

Secondary DNS:

Hostname: vdp

Domain: dellemc.local

Figure 175 Network Settings



VDP Credentials

Enter a password for the VDP Appliance.

Four character classes:

Upper case letters A-Z
Lower case letters a-z
Numbers 0-9
Special characters (Examples: ~!@#,.)

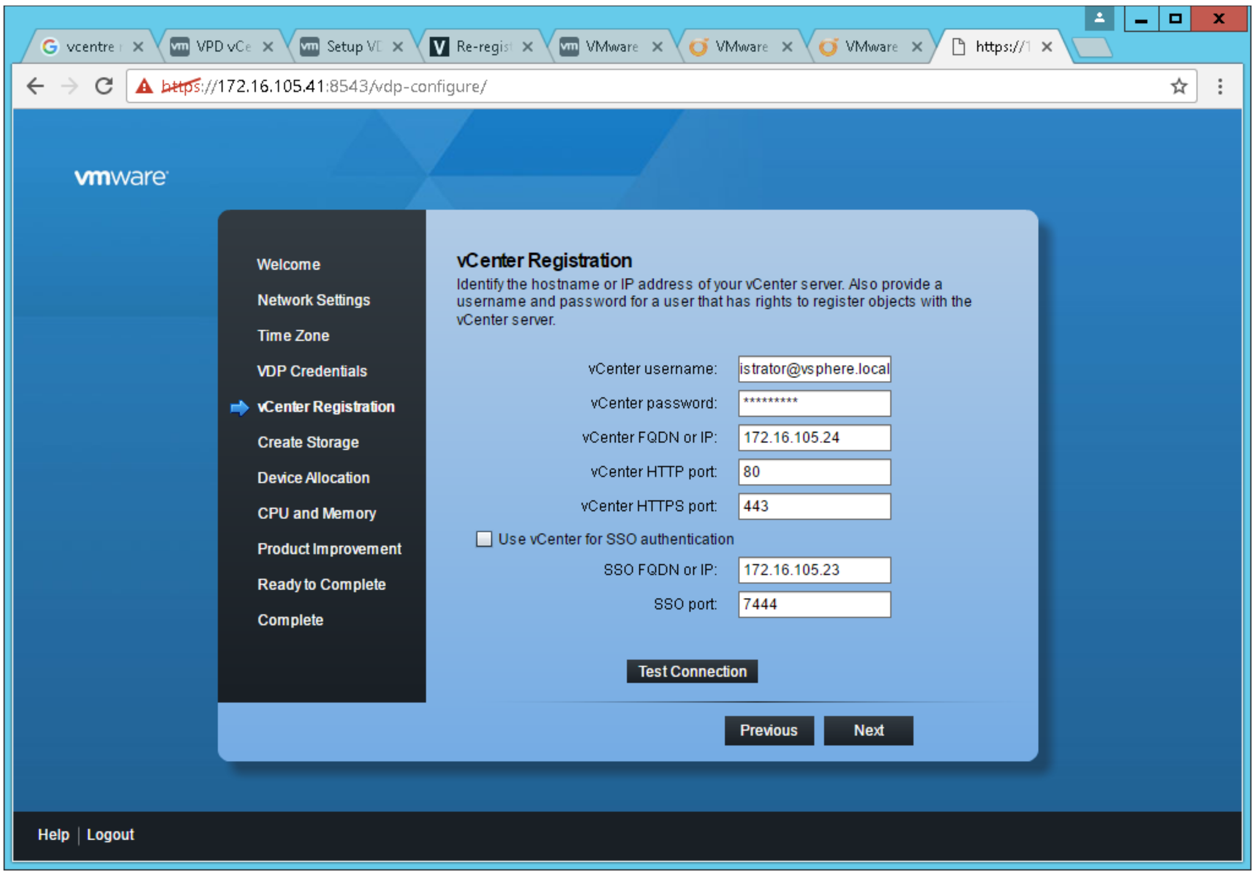
Passwords criteria:

All four character classes, at least 6 characters long
✓ Three character classes, at least 7 characters long
One or two character classes, at least 8 characters long
(NOTE: 'Capital first' and 'Number last' characters
are not included in the character class count.)

Password: *********

Verify password: ********* ✓

Figure 176 VDP Credentials

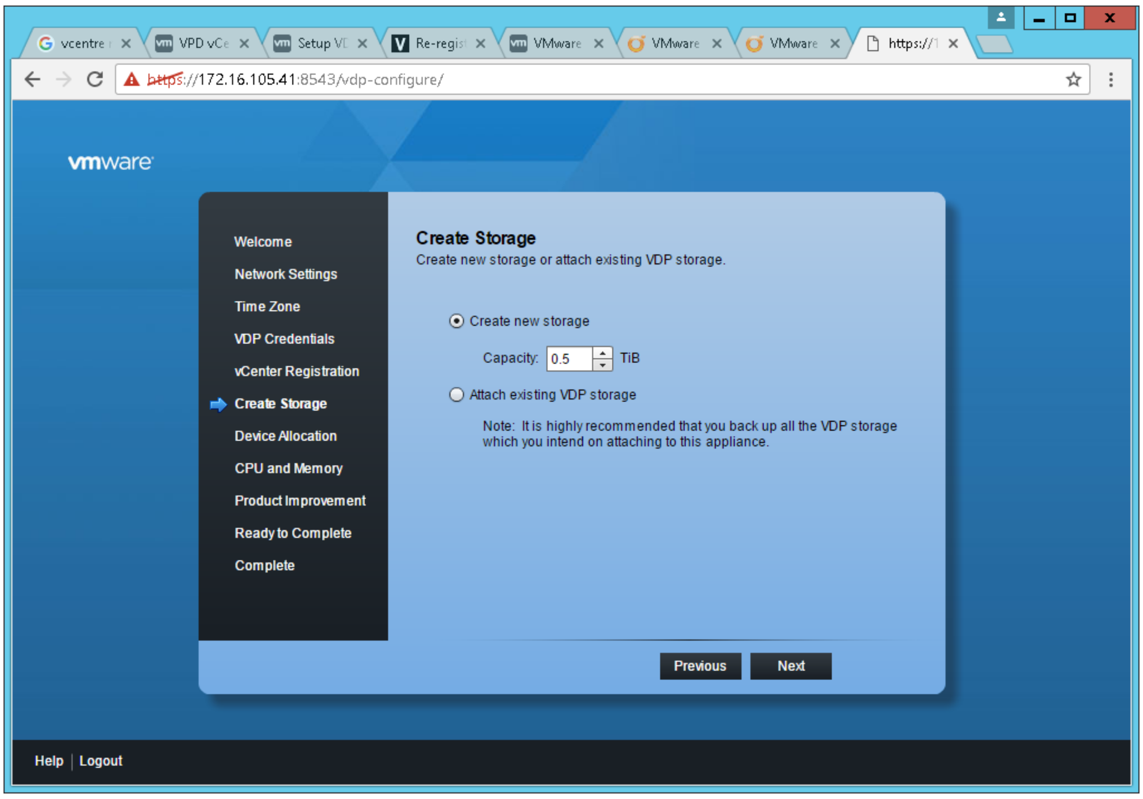


vCenter Registration

Identify the hostname or IP address of your vCenter server. Also provide a username and password for a user that has rights to register objects with the vCenter server.

vCenter username: istrator@vsphere.local
vCenter password: *********
vCenter FQDN or IP: 172.16.105.24
vCenter HTTP port: 80
vCenter HTTPS port: 443
☐ Use vCenter for SSO authentication
SSO FQDN or IP: 172.16.105.23
SSO port: 7444

Figure 177 vCenter Registration



Create Storage

Create new storage or attach existing VDP storage.

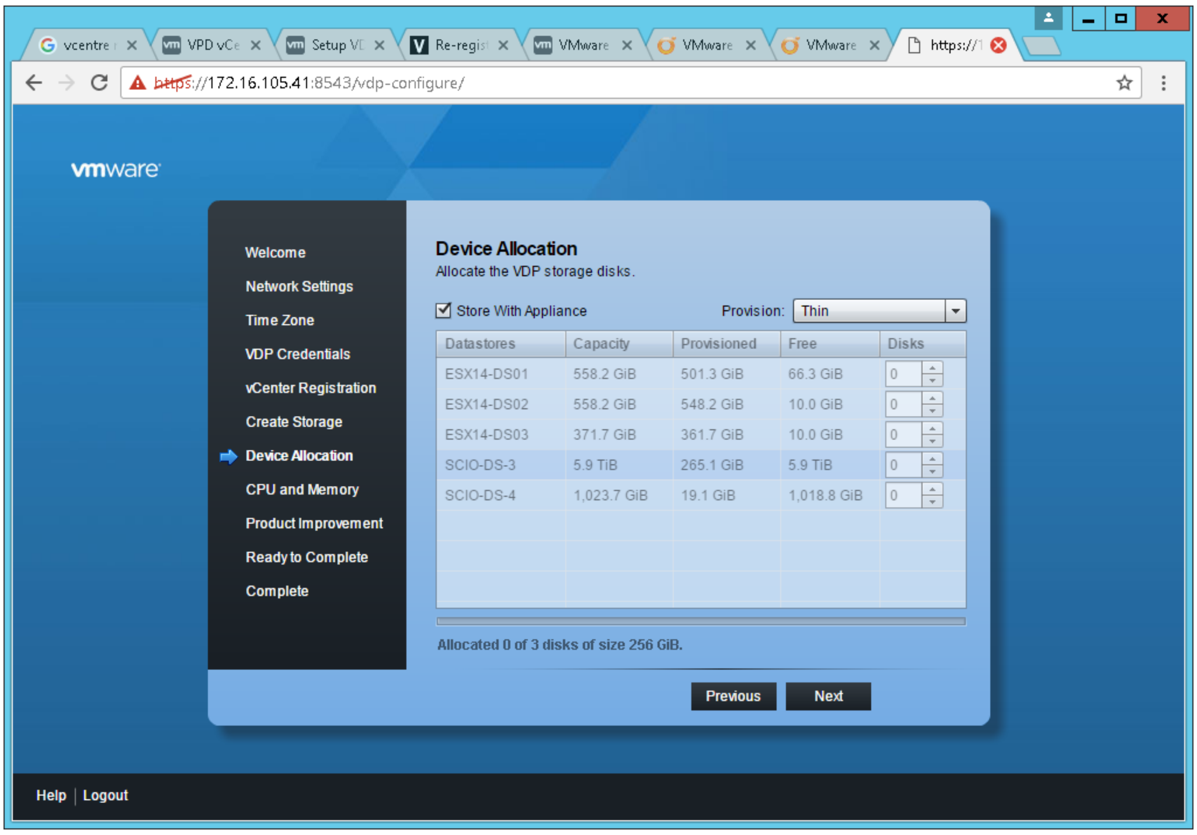
● Create new storage

Capacity: 0.5 TiB

○ Attach existing VDP storage

Note: It is highly recommended that you back up all the VDP storage which you intend on attaching to this appliance.

Figure 178 Create Storage



Device Allocation

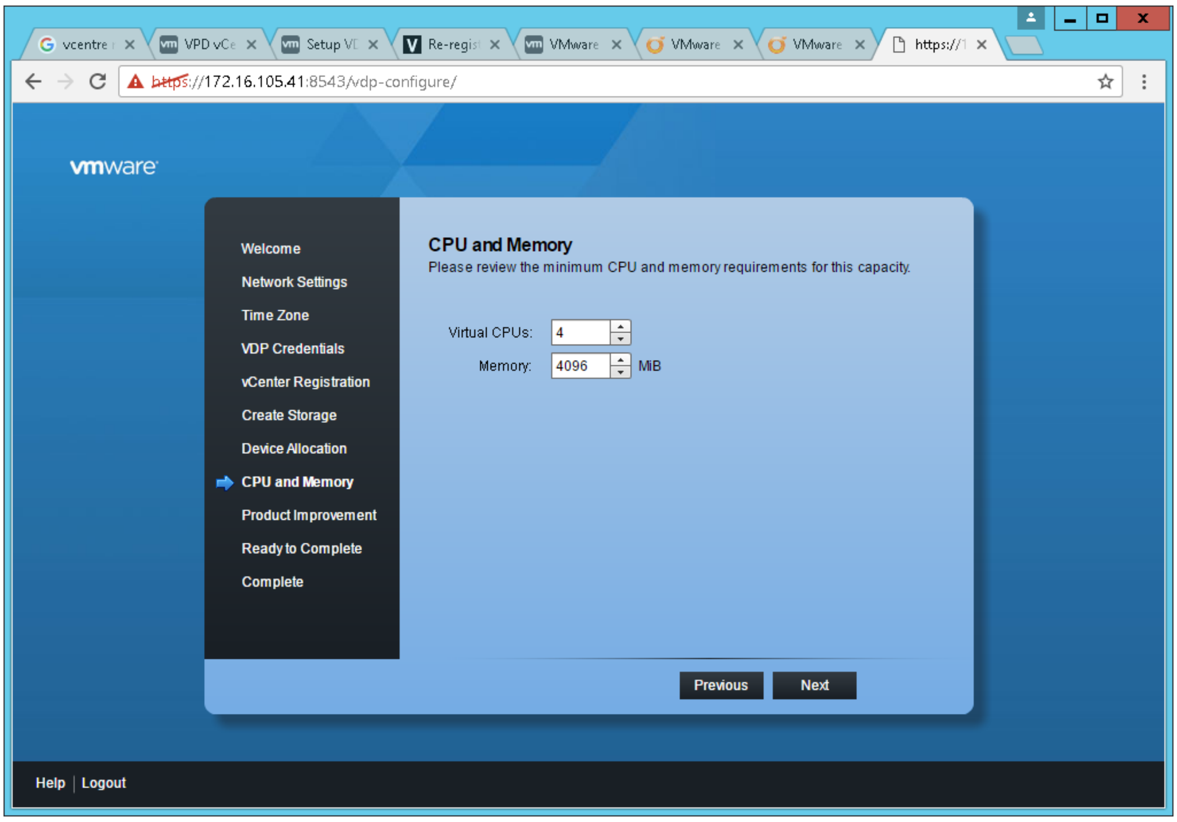
Allocate the VDP storage disks.

☑ Store With Appliance Provision: Thin

Datastores	Capacity	Provisioned	Free	Disks
ESX14-DS01	558.2 GiB	501.3 GiB	66.3 GiB	0
ESX14-DS02	558.2 GiB	548.2 GiB	10.0 GiB	0
ESX14-DS03	371.7 GiB	361.7 GiB	10.0 GiB	0
SCIO-DS-3	5.9 TiB	265.1 GiB	5.9 TiB	0
SCIO-DS-4	1,023.7 GiB	19.1 GiB	1,018.8 GiB	0

Allocated 0 of 3 disks of size 256 GiB.

Figure 179 Device Allocation



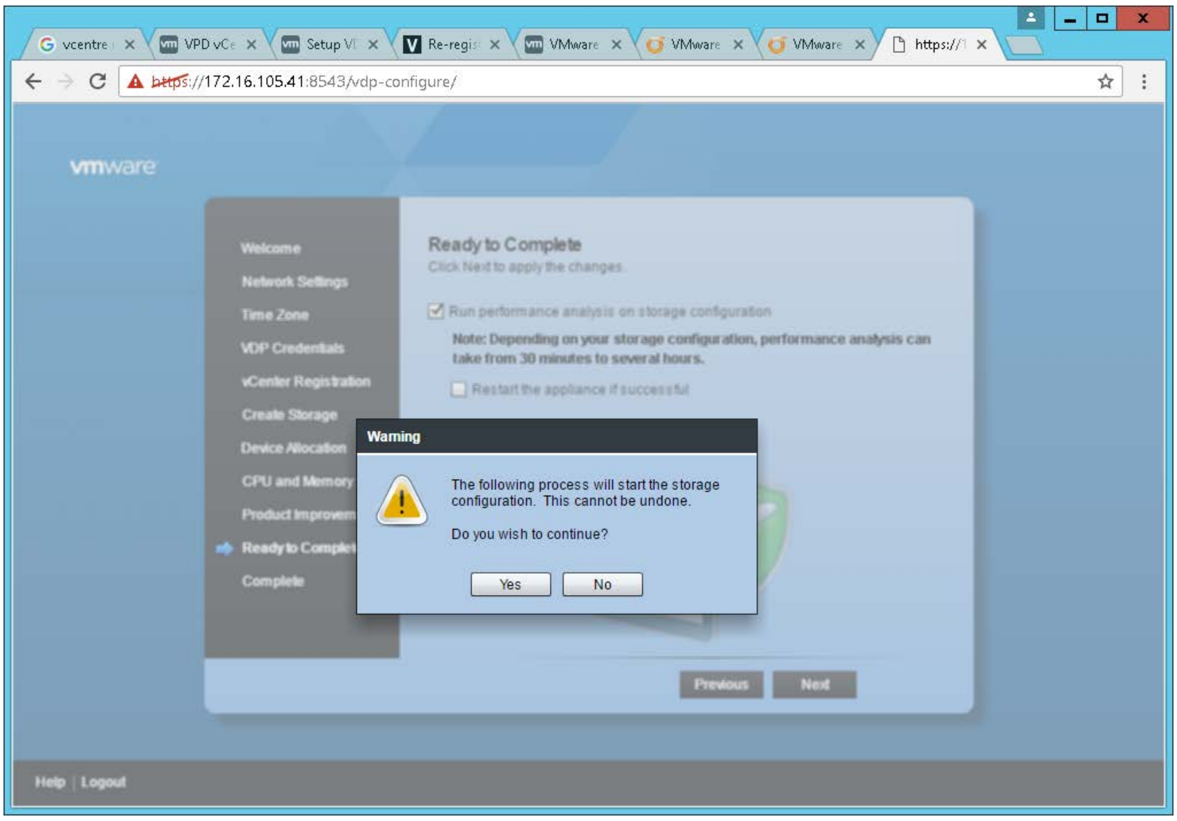
CPU and Memory

Please review the minimum CPU and memory requirements for this capacity.

Virtual CPUs: 4

Memory: 4096 MiB

Figure 180 CPU and Memory



Ready to Complete

Click Next to apply the changes.

☑ Run performance analysis on storage configuration

Note: Depending on your storage configuration, performance analysis can take from 30 minutes to several hours.

☐ Restart the appliance if successful

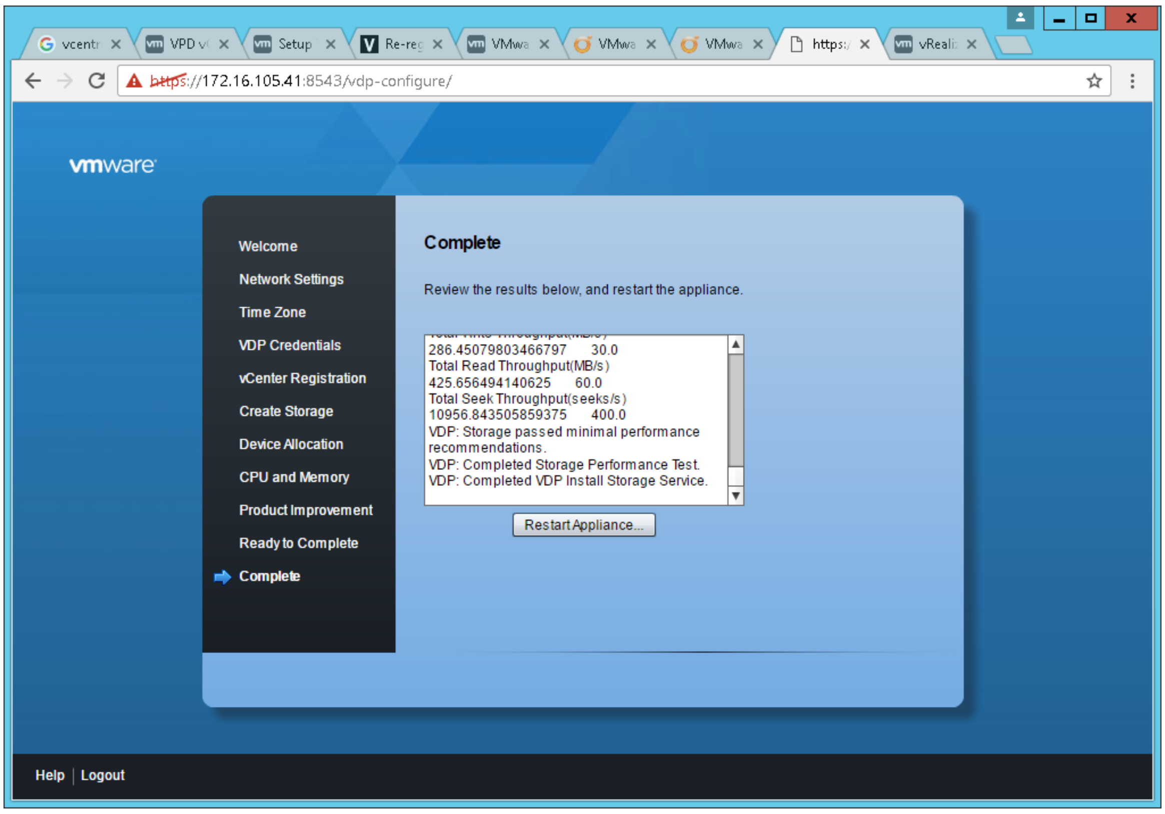
Warning

The following process will start the storage configuration. This cannot be undone.

Do you wish to continue?

Yes No

Figure 181 Start storage Configuration



Complete

Review the results below, and restart the appliance.

```
286.45079803466797     30.0
Total Read Throughput(MB/s)
425.656494140625     60.0
Total Seek Throughput(seeks/s)
10956.843505859375     400.0
VDP: Storage passed minimal performance
recommendations.
VDP: Completed Storage Performance Test.
VDP: Completed VDP Install Storage Service.
```

Restart Appliance...

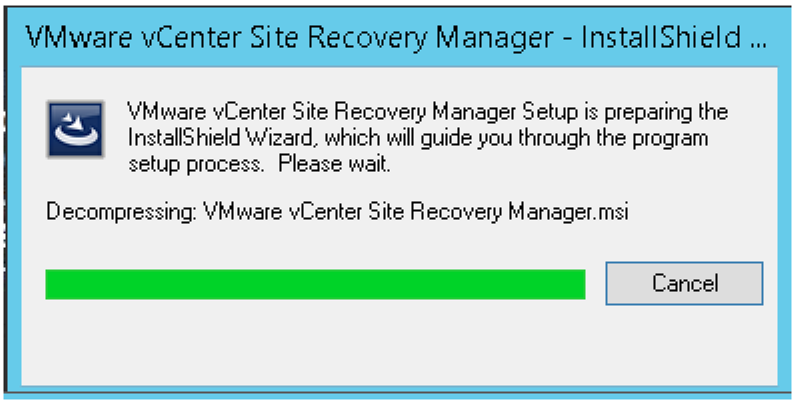
Figure 182 Installation complete

Install VMware vSphere Site Recovery Manager (SRM).

In this guide, SRM is installed but no replication is done since there are no multi-sites.

It can be installed on the same Windows servers as the vCenter 6 installs or a new Windows VM can be created and the SRM installable can be downloaded.

Launch the install from the downloaded executable.

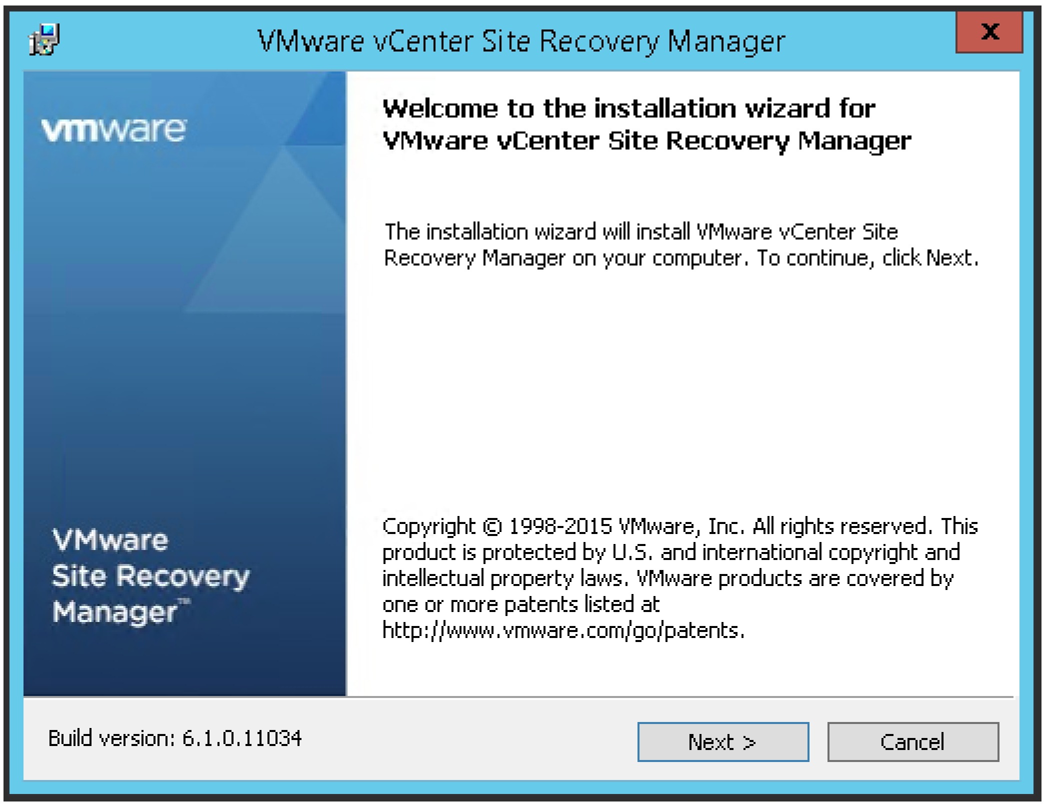

VMware vCenter Site Recovery Manager - InstallShield ...

VMware vCenter Site Recovery Manager Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.

Decompressing: VMware vCenter Site Recovery Manager.msi

Figure 183 SRM InstallShield Wizard

Figure 184 VMware Site Recovery Manager Setup


VMware vCenter Site Recovery Manager

Welcome to the installation wizard for VMware vCenter Site Recovery Manager

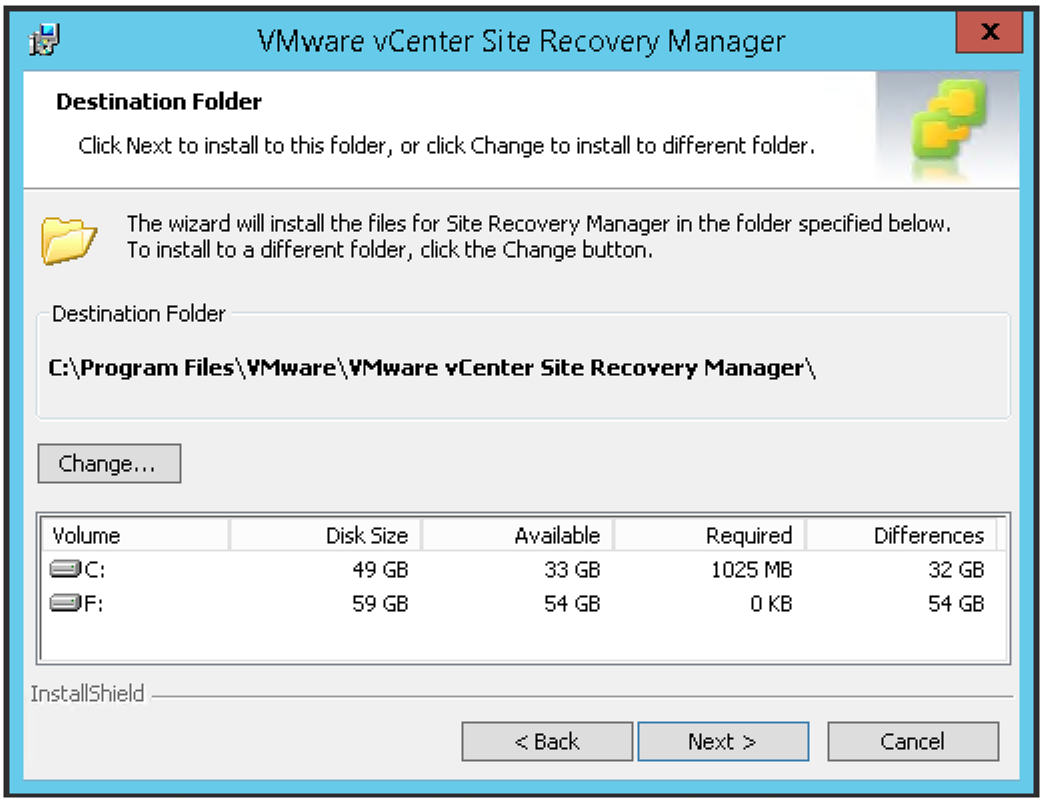
The installation wizard will install VMware vCenter Site Recovery Manager on your computer. To continue, click Next.

Copyright © 1998-2015 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

Build version: 6.1.0.11034

Figure 185 SRM installation wizard

If you wish to change the default installation folder, click **Change**. Click **Next** to accept the default installation folder.


VMware vCenter Site Recovery Manager

Destination Folder

Click Next to install to this folder, or click Change to install to different folder.

The wizard will install the files for Site Recovery Manager in the folder specified below. To install to a different folder, click the Change button.

Destination Folder

C:\Program Files\VMware\VMware vCenter Site Recovery Manager

Volume	Disk Size	Available	Required	Differences
C:	49 GB	33 GB	1025 MB	32 GB
F:	59 GB	54 GB	0 KB	54 GB

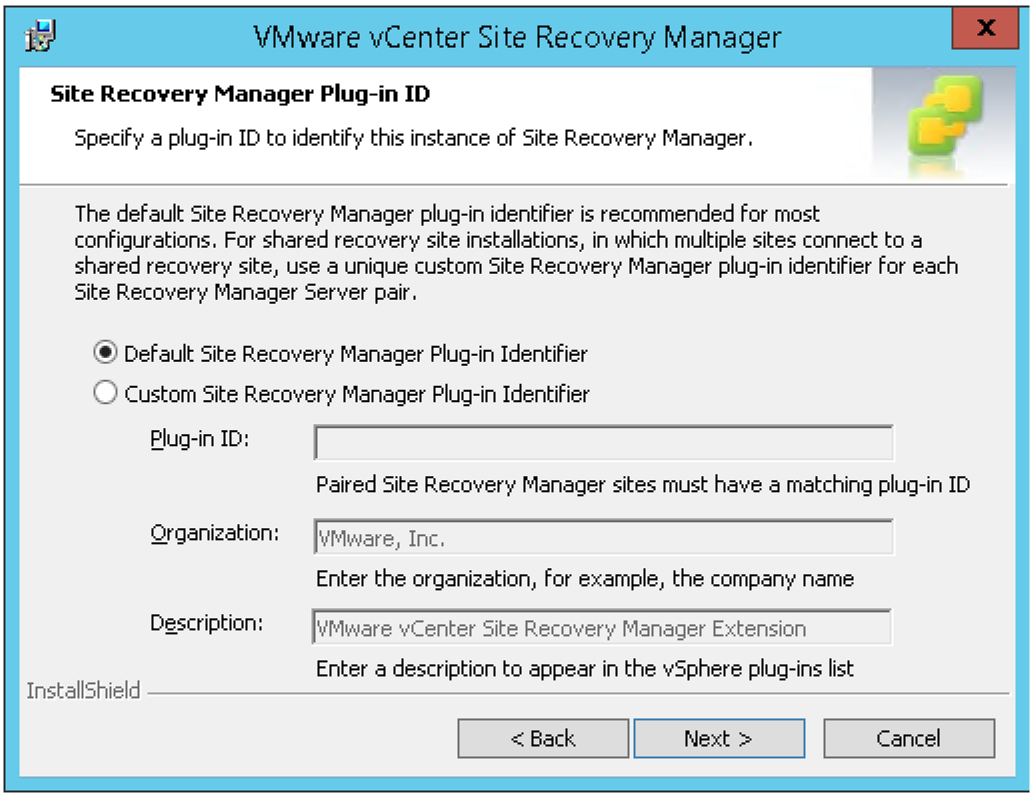
Figure 186 Installation Folder

Enter Platform Services Controller (PSC) details and click **Next**.

Verify the correct vCenter instance is selected and click **Next**.

Enter SRM extension details and click **Next** (Local site Name is vCenter FQDN and Local host is vCenter IP address in this environment).

Select the plugin identifier as per requirement and click **Next**. For reference on which option to use, read the description above selection buttons.


VMware vCenter Site Recovery Manager

Site Recovery Manager Plug-in ID

Specify a plug-in ID to identify this instance of Site Recovery Manager.

The default Site Recovery Manager plug-in identifier is recommended for most configurations. For shared recovery site installations, in which multiple sites connect to a shared recovery site, use a unique custom Site Recovery Manager plug-in identifier for each Site Recovery Manager Server pair.

● Default Site Recovery Manager Plug-in Identifier

○ Custom Site Recovery Manager Plug-in Identifier

Plug-in ID:

Paired Site Recovery Manager sites must have a matching plug-in ID

Organization: VMware, Inc.

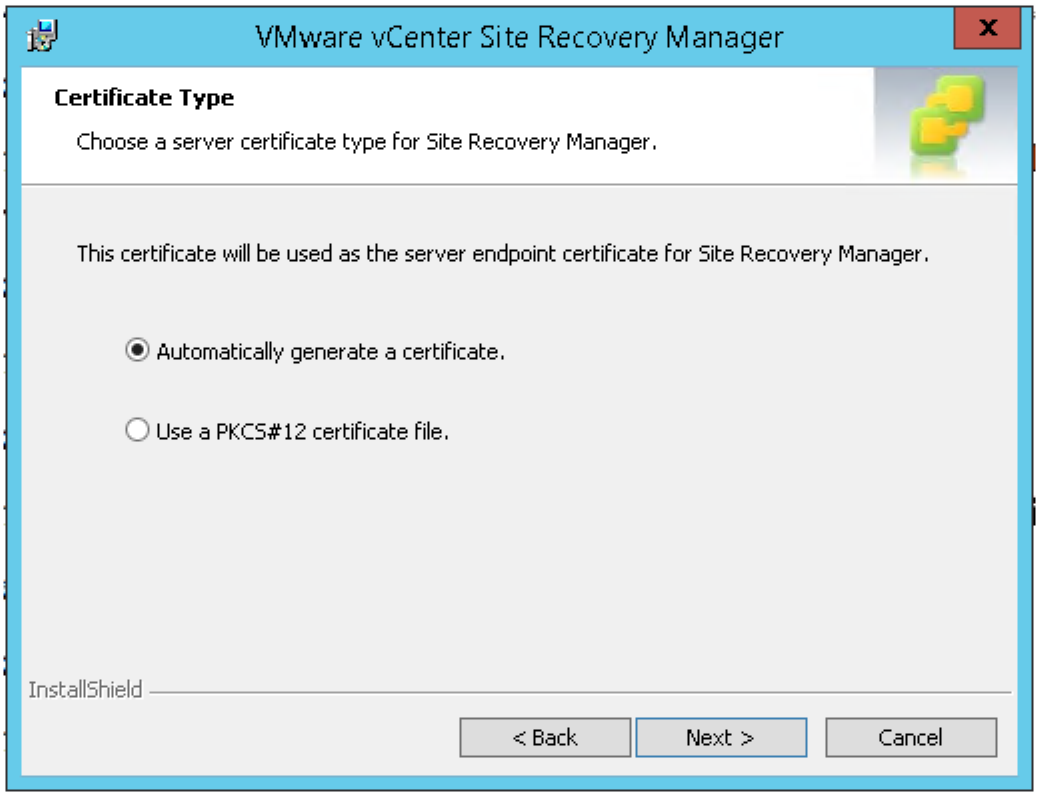
Enter the organization, for example, the company name

Description: VMware vCenter Site Recovery Manager Extension

Enter a description to appear in the vSphere plug-ins list

Figure 187 Site Recover Manager Plug-in

Select the method for certificate and click **Next**.


VMware vCenter Site Recovery Manager

Certificate Type

Choose a server certificate type for Site Recovery Manager.

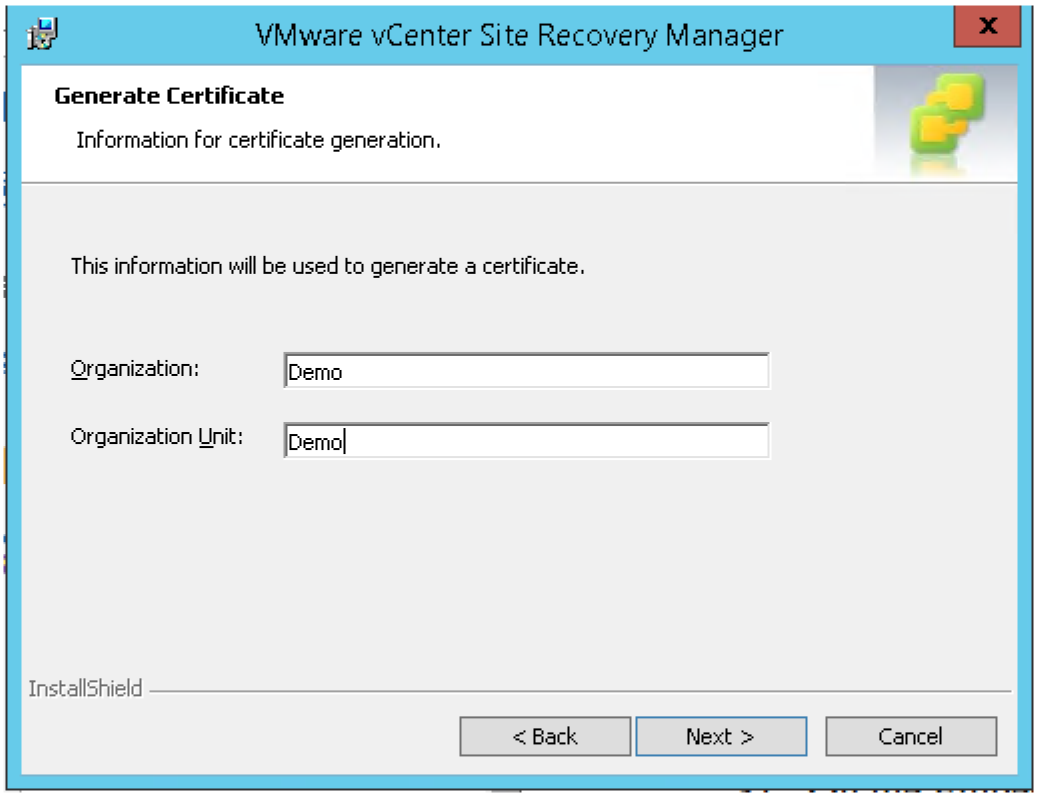
This certificate will be used as the server endpoint certificate for Site Recovery Manager.

● Automatically generate a certificate.

○ Use a PKCS#12 certificate file.

Figure 188 Select Certificate Type

Provide the details that will be used for certificate generation as per the previous selection.


VMware vCenter Site Recovery Manager

Generate Certificate

Information for certificate generation.

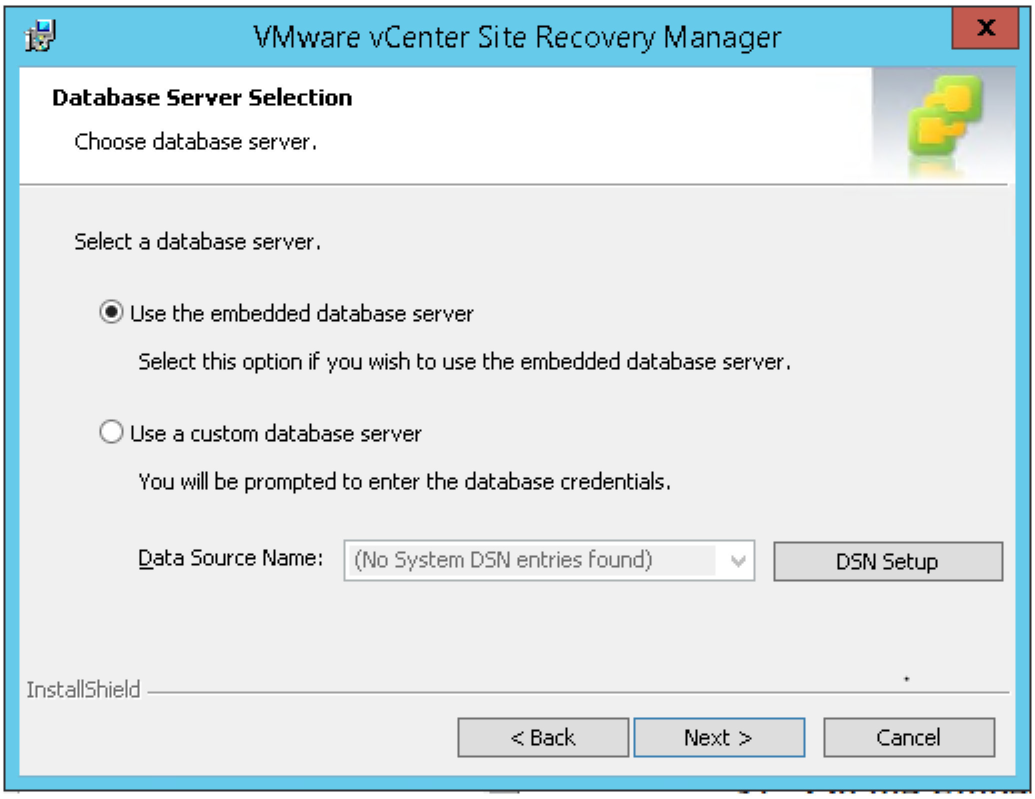
This information will be used to generate a certificate.

Organization: Demo

Organization Unit: Demo

Figure 189 Generate Certificate

Select the database instance as embedded or existing custom database and click **Next**.


VMware vCenter Site Recovery Manager

Database Server Selection

Choose database server.

Select a database server.

● Use the embedded database server

Select this option if you wish to use the embedded database server.

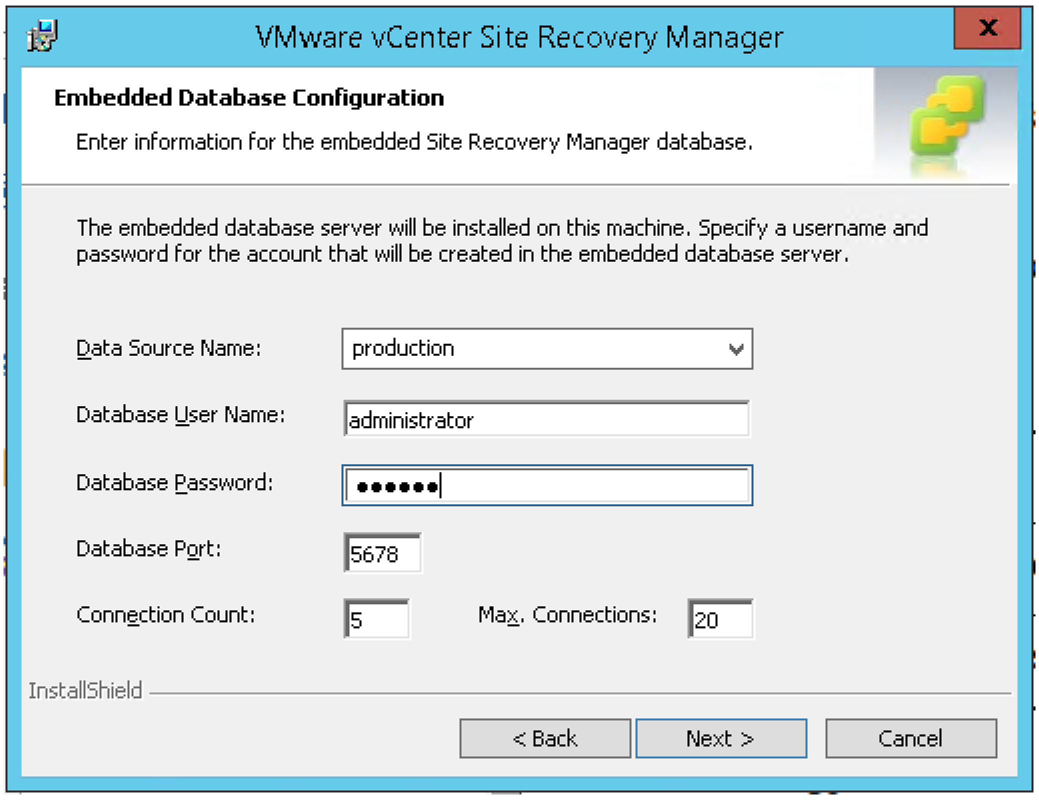
○ Use a custom database server

You will be prompted to enter the database credentials.

Data Source Name: (No System DSN entries found)

Figure 190 Database Server Selection

Provide details for connecting to database instance and click **Next**.


VMware vCenter Site Recovery Manager

Embedded Database Configuration

Enter information for the embedded Site Recovery Manager database.

The embedded database server will be installed on this machine. Specify a username and password for the account that will be created in the embedded database server.

Data Source Name: production

Database User Name: administrator

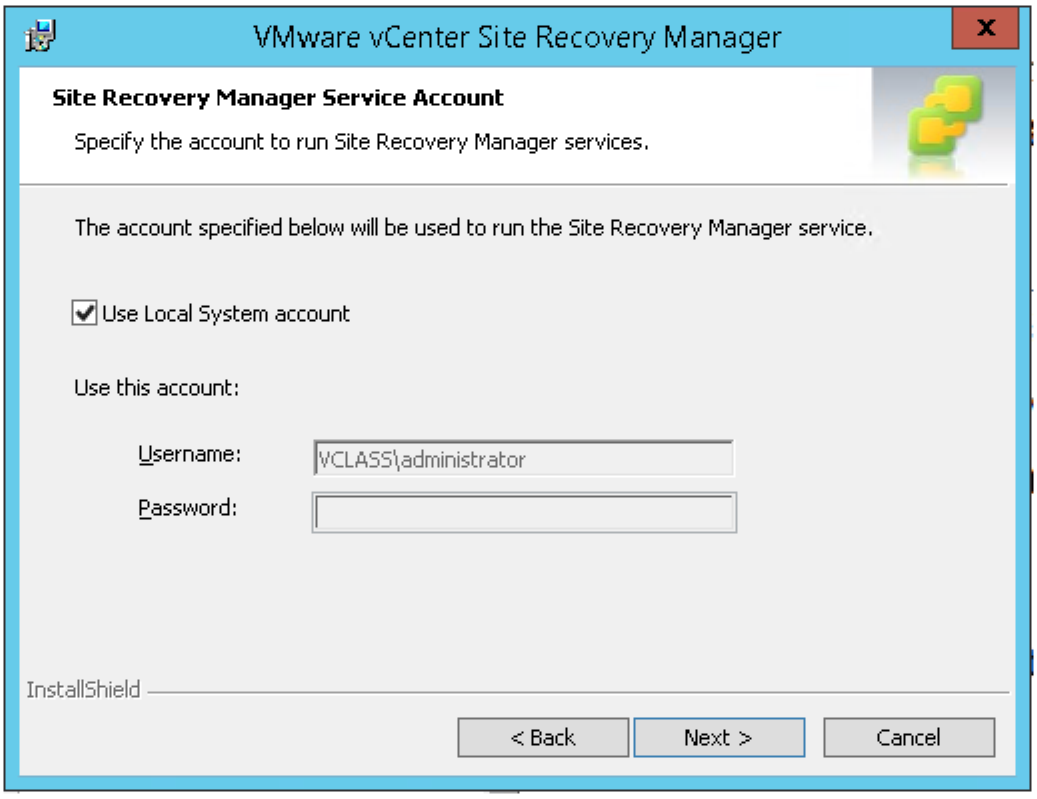
Database Password: ●●●●●●

Database Port: 5678

Connection Count: 5 Max. Connections: 20

Figure 191 Database connection details

Choose whether to use local account or domain account as service account for SRM. In this example, a local account is used.


VMware vCenter Site Recovery Manager

Site Recovery Manager Service Account

Specify the account to run Site Recovery Manager services.

The account specified below will be used to run the Site Recovery Manager service.

☑ Use Local System account

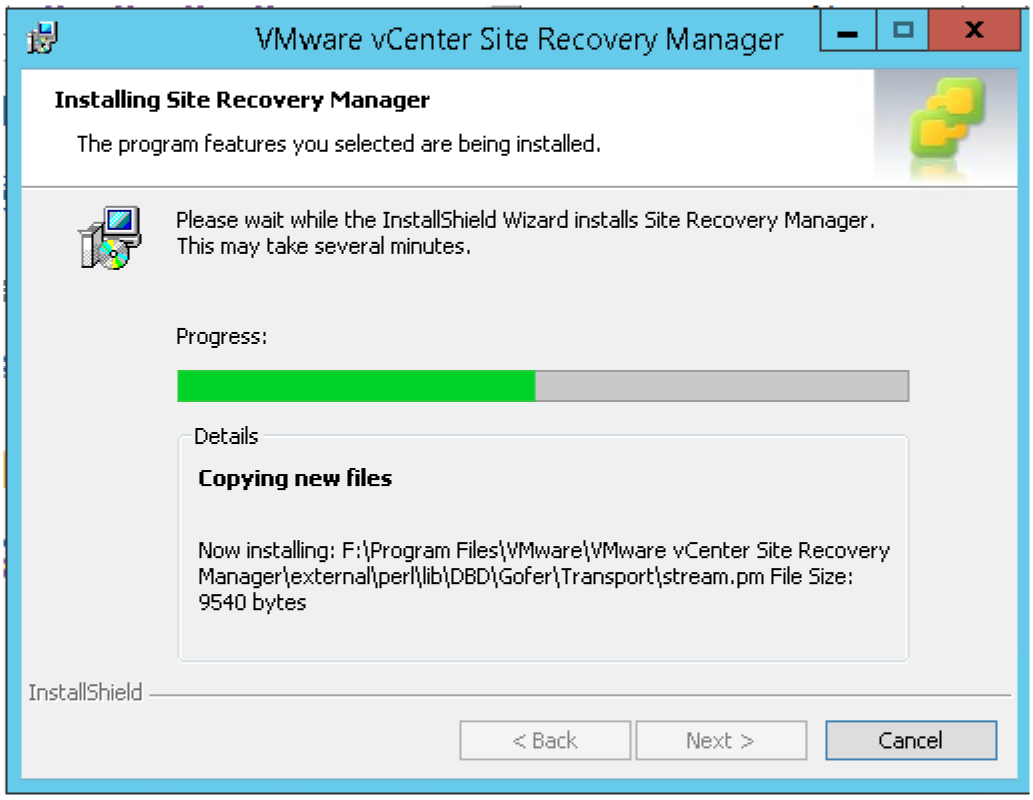
Use this account:

Username: VCLASS\administrator

Password:

Figure 192 Site Recovery Manager Service Account

Click **Next** and click Install on next window. This will start the install process as per the input provided during wizard.


VMware vCenter Site Recovery Manager

Installing Site Recovery Manager

The program features you selected are being installed.

Please wait while the InstallShield Wizard installs Site Recovery Manager. This may take several minutes.

Progress:

Details

Copying new files

Now installing: F:\Program Files\VMware\VMware vCenter Site Recovery Manager\external\perl\lib\DBD\Gofer\Transport\stream.pm File Size: 9540 bytes

Figure 193 Installing Site Recovery Manager

Once installation is complete, click **Finish**.

In order to verify the installation completion, check SRM service from Service management console.

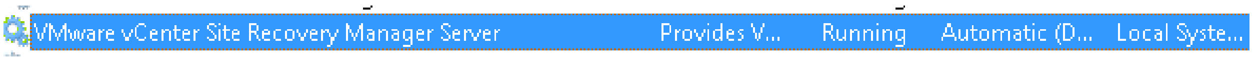

VMware vCenter Site Recovery Manager Server   Provides V...   Running   Automatic (D...   Local Syste...

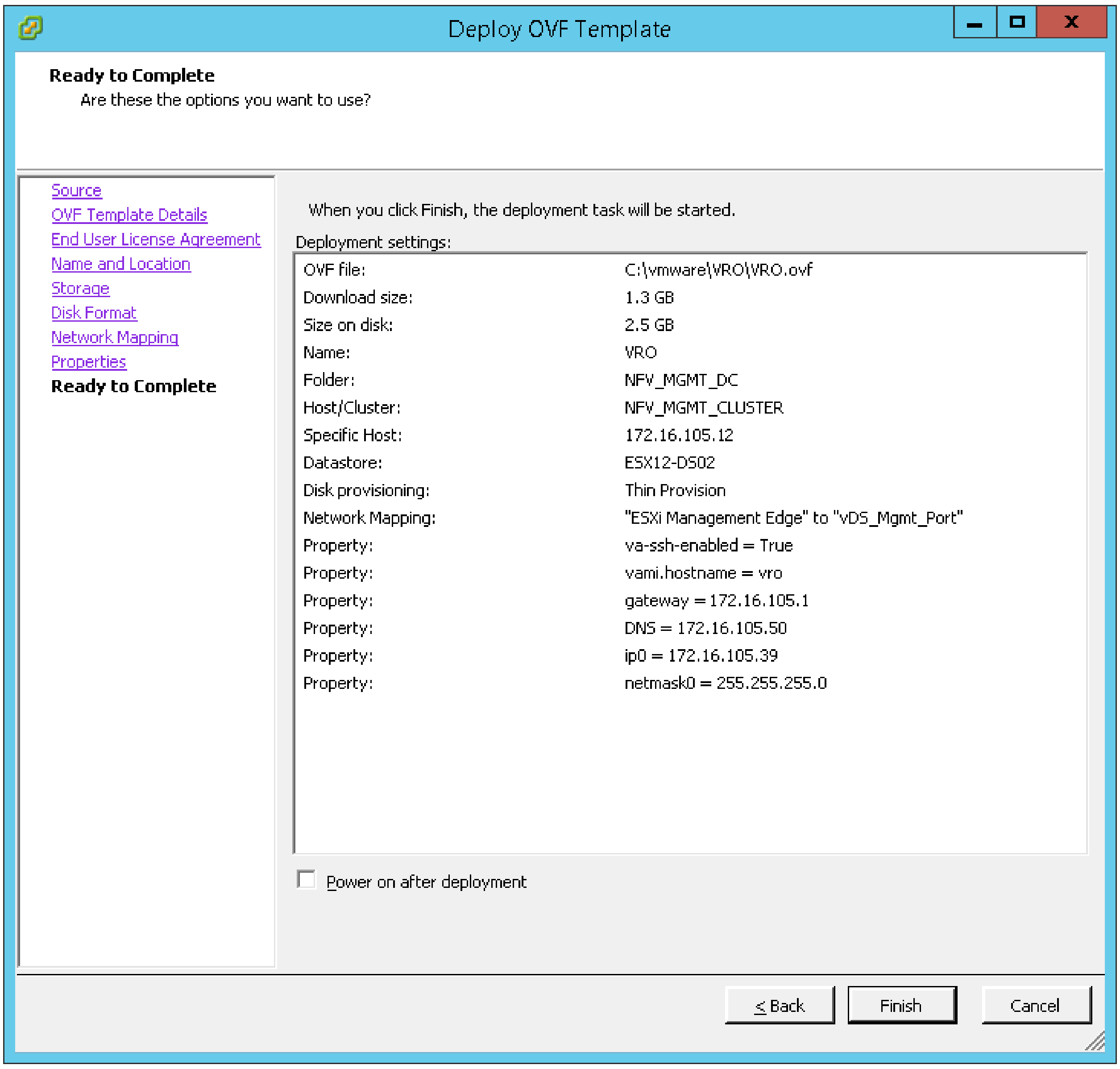
Figure 194 SRM service

Check in Web client home screen for the new options shown below.

Figure 195 New options on the Web client home screen

13 Install VMware vRealize Orchestrator (VRO)

Deploy OVA for VRO.



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\vmware\VRO\VRO.ovf
Download size:	1.3 GB
Size on disk:	2.5 GB
Name:	VRO
Folder:	NFV_MGMT_DC
Host/Cluster:	NFV_MGMT_CLUSTER
Specific Host:	172.16.105.12
Datastore:	ESX12-DS02
Disk provisioning:	Thin Provision
Network Mapping:	"ESXi Management Edge" to "vDS_Mgmt_Port"
Property:	va-ssh-enabled = True
Property:	vami.hostname = vro
Property:	gateway = 172.16.105.1
Property:	DNS = 172.16.105.50
Property:	ip0 = 172.16.105.39
Property:	netmask0 = 255.255.255.0

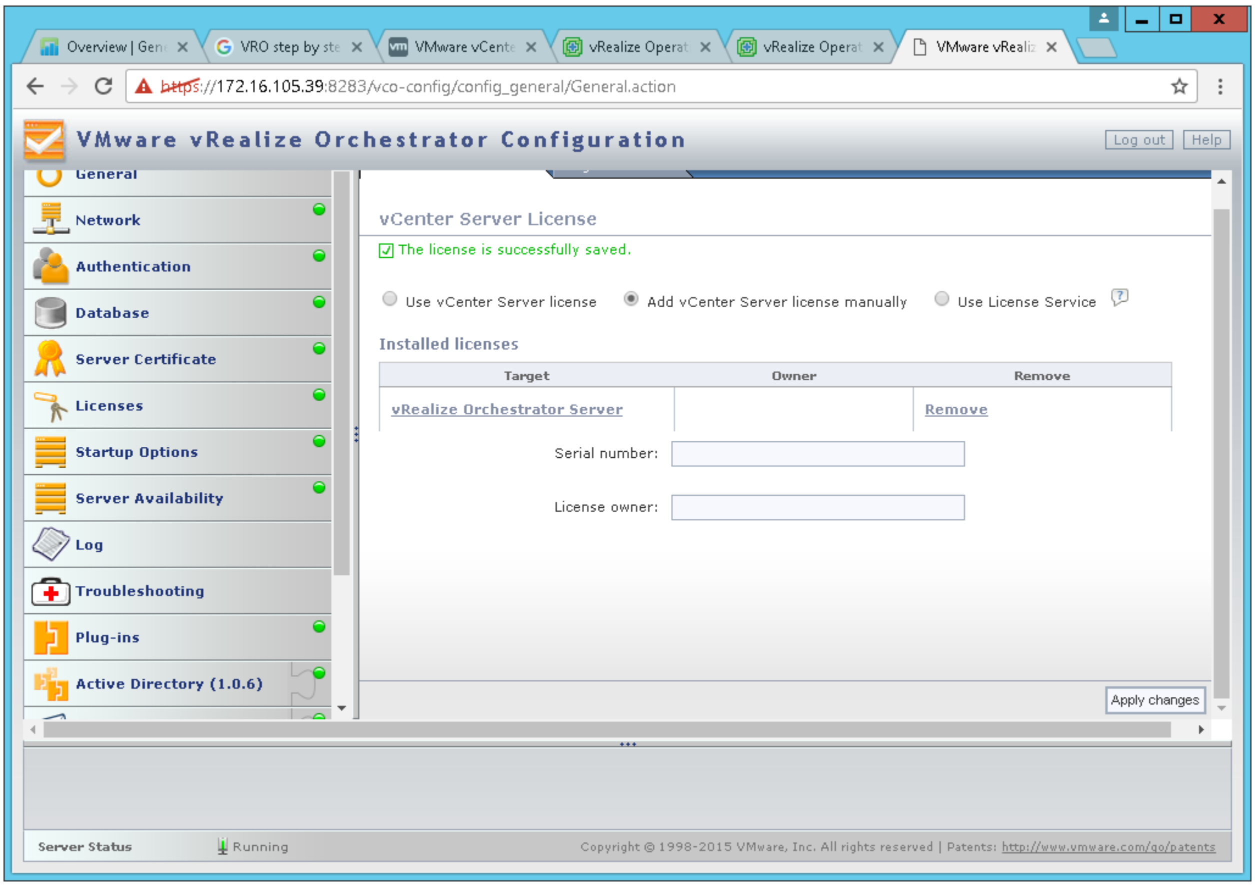
☐ Power on after deployment

Figure 196 OVF deployment template

Open a browser and go to https://<VRO url>:8283

Login with username vmware/<pwd>.

In the configuration window, verify SSL certificates.



https://172.16.105.39:8283/vco-config/config_general/General.action
VMware vRealize Orchestrator Configuration
Log out
Help
General
Network
Authentication
Database
Server Certificate
Licenses
Startup Options
Server Availability
Log
Troubleshooting
Plug-ins
Active Directory (1.0.6)
Apply changes
Server Status
Running
Copyright © 1998-2015 VMware, Inc. All rights reserved | Patents: http://www.vmware.com/go/patents

vCenter Server License

☑ The license is successfully saved.

○ Use vCenter Server license ● Add vCenter Server license manually ○ Use License Service

Installed licenses

Target	Owner	Remove
vRealize Orchestrator Server		Remove

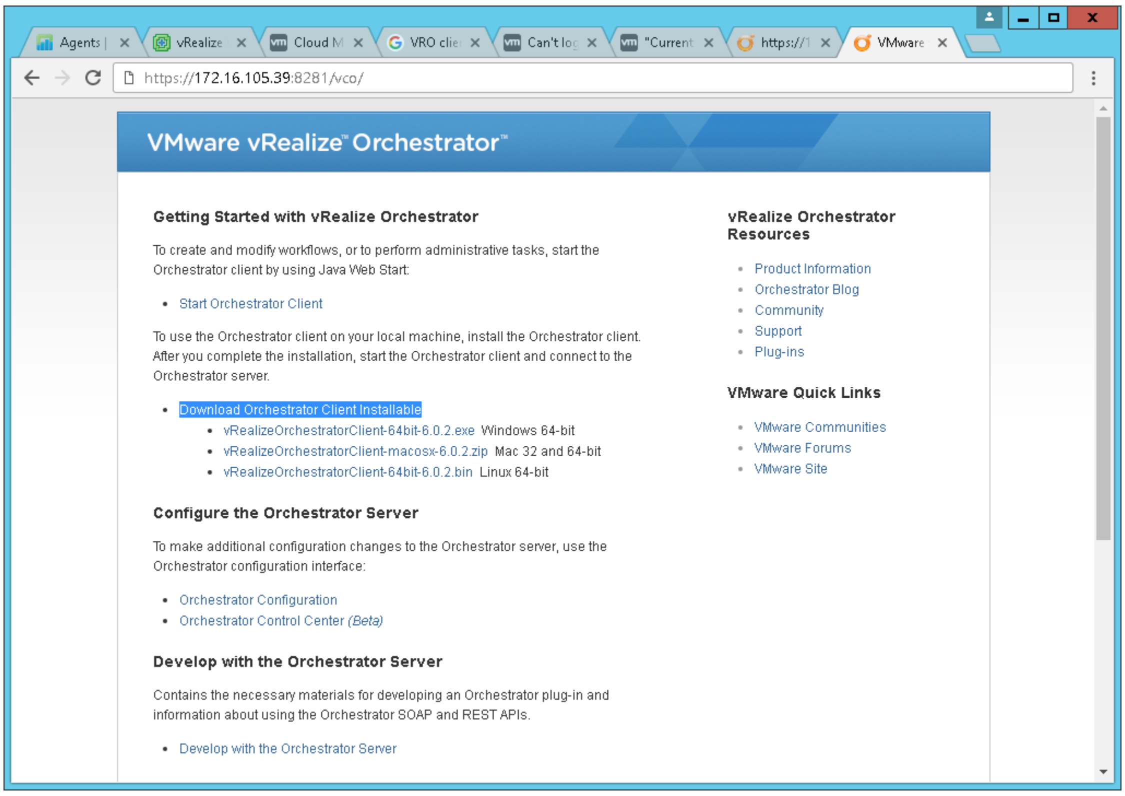
Serial number:

License owner:

Figure 197 Verify SSL certificates

Verify Orchestrator client login. Navigate to **https://<VRO url>:8281**

Click Start Orchestrator client. Download and run the client jnlp file, or install by clicking on the **Download Orchestrator Client** Installable.



https://172.16.105.39:8281/vco/
VMware vRealize® Orchestrator™

Getting Started with vRealize Orchestrator

To create and modify workflows, or to perform administrative tasks, start the Orchestrator client by using Java Web Start:

- Start Orchestrator Client

To use the Orchestrator client on your local machine, install the Orchestrator client. After you complete the installation, start the Orchestrator client and connect to the Orchestrator server.

- Download Orchestrator Client Installable
  - vRealizeOrchestratorClient-64bit-6.0.2.exe Windows 64-bit
  - vRealizeOrchestratorClient-macosx-6.0.2.zip Mac 32 and 64-bit
  - vRealizeOrchestratorClient-64bit-6.0.2.bin Linux 64-bit

Configure the Orchestrator Server

To make additional configuration changes to the Orchestrator server, use the Orchestrator configuration interface:

- Orchestrator Configuration
- Orchestrator Control Center *(Beta)*

Develop with the Orchestrator Server

Contains the necessary materials for developing an Orchestrator plug-in and information about using the Orchestrator SOAP and REST APIs.

- Develop with the Orchestrator Server

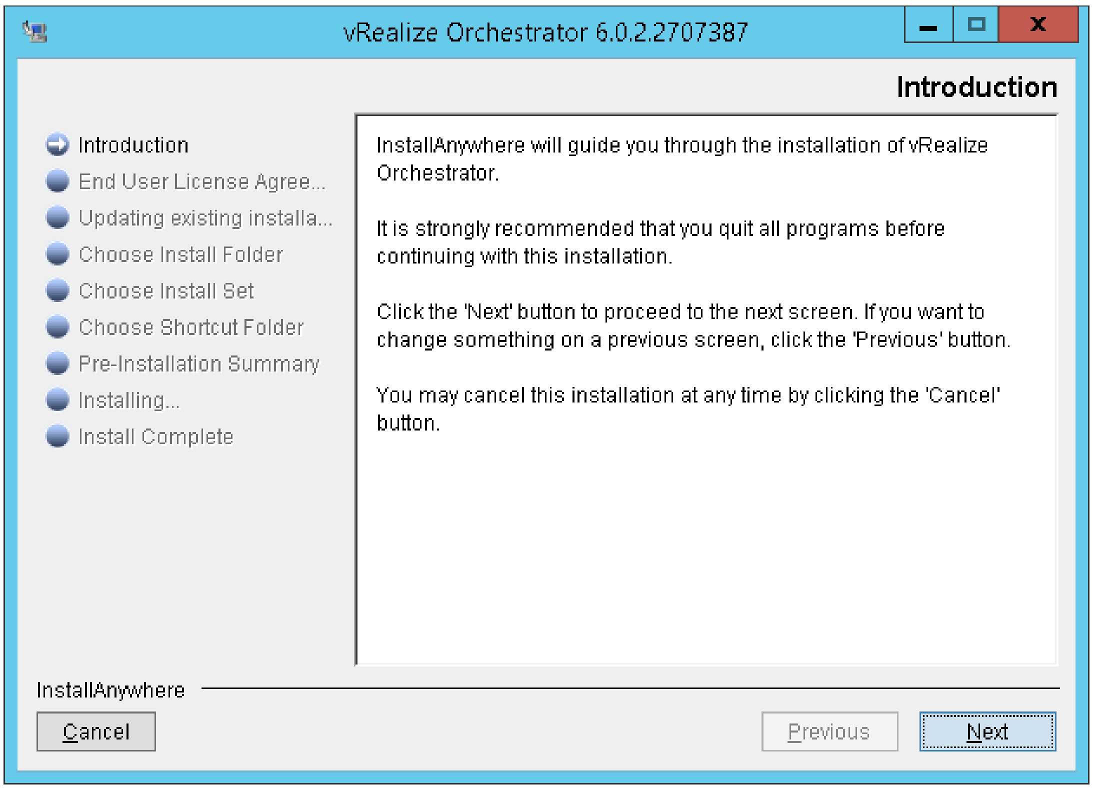
vRealize Orchestrator Resources

- Product Information
- Orchestrator Blog
- Community
- Support
- Plug-ins

VMware Quick Links

- VMware Communities
- VMware Forums
- VMware Site

Figure 198 Download Orchestrator Client Installable


vRealize Orchestrator 6.0.2.2707387

Introduction

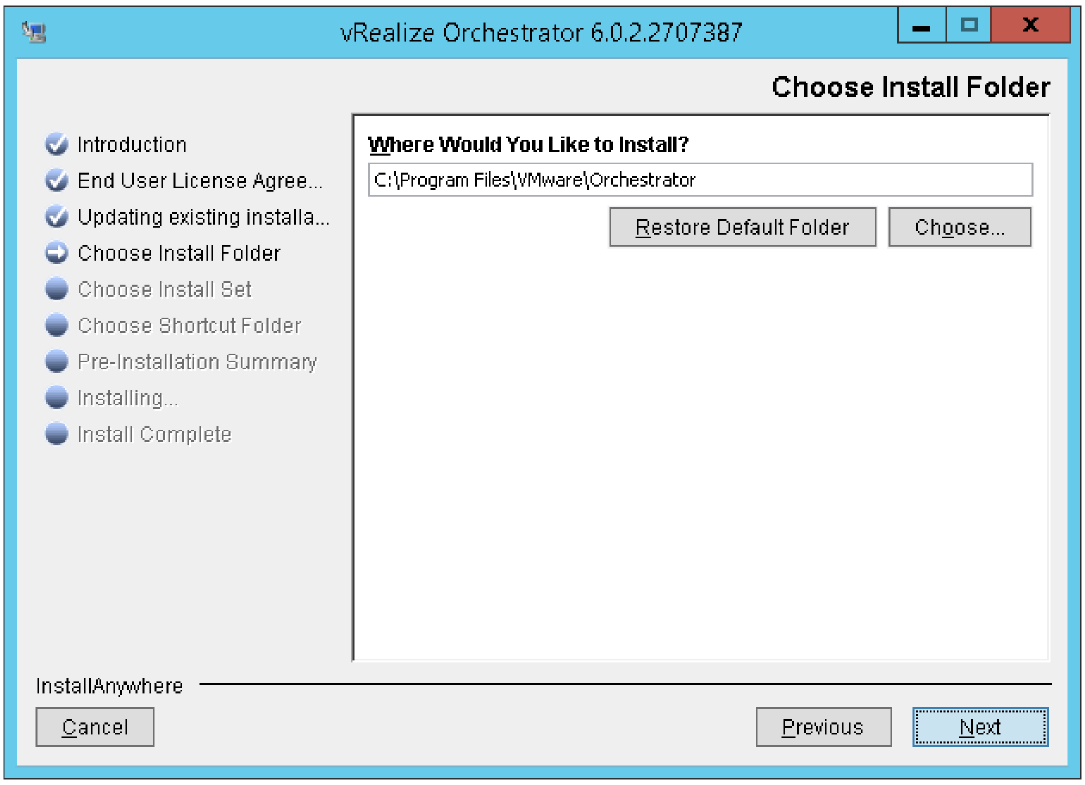
InstallAnywhere will guide you through the installation of vRealize Orchestrator.

It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

Figure 199 Installation wizard

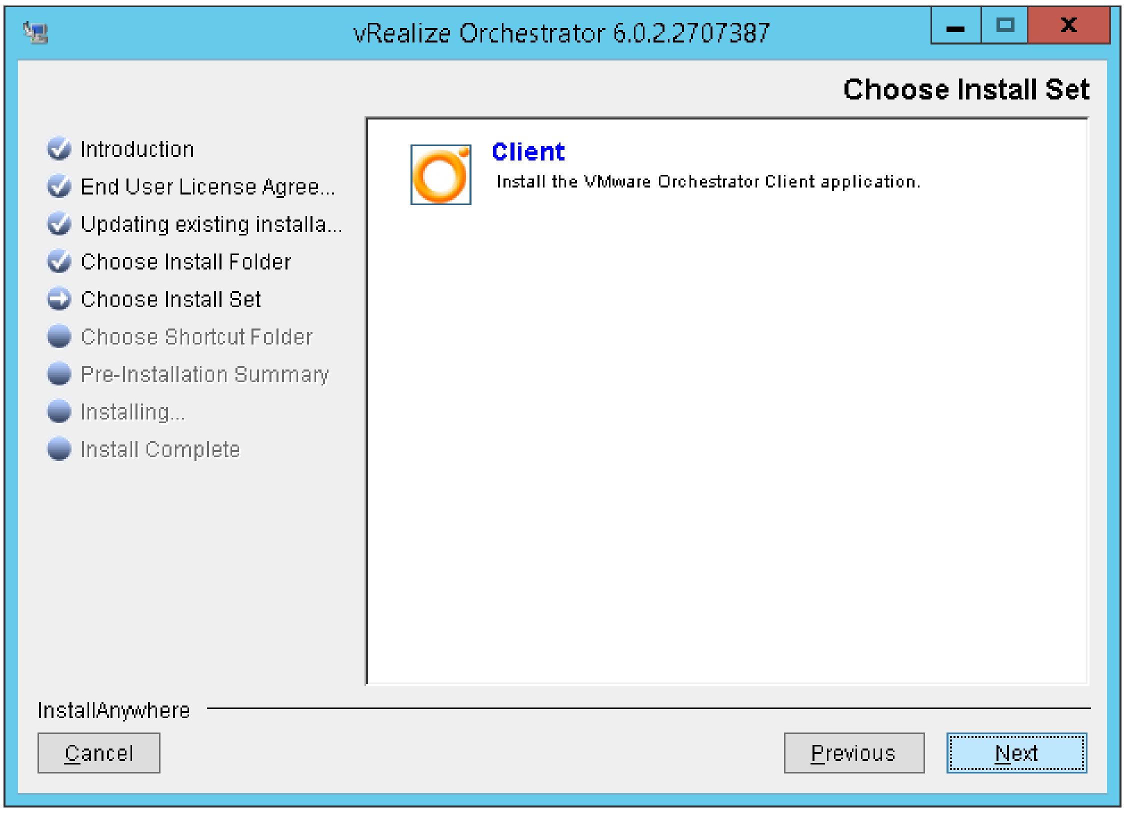

vRealize Orchestrator 6.0.2.2707387

Choose Install Folder

Where Would You Like to Install?

C:\Program Files\VMware\Orchestrator

Figure 200 Choose Install Folder



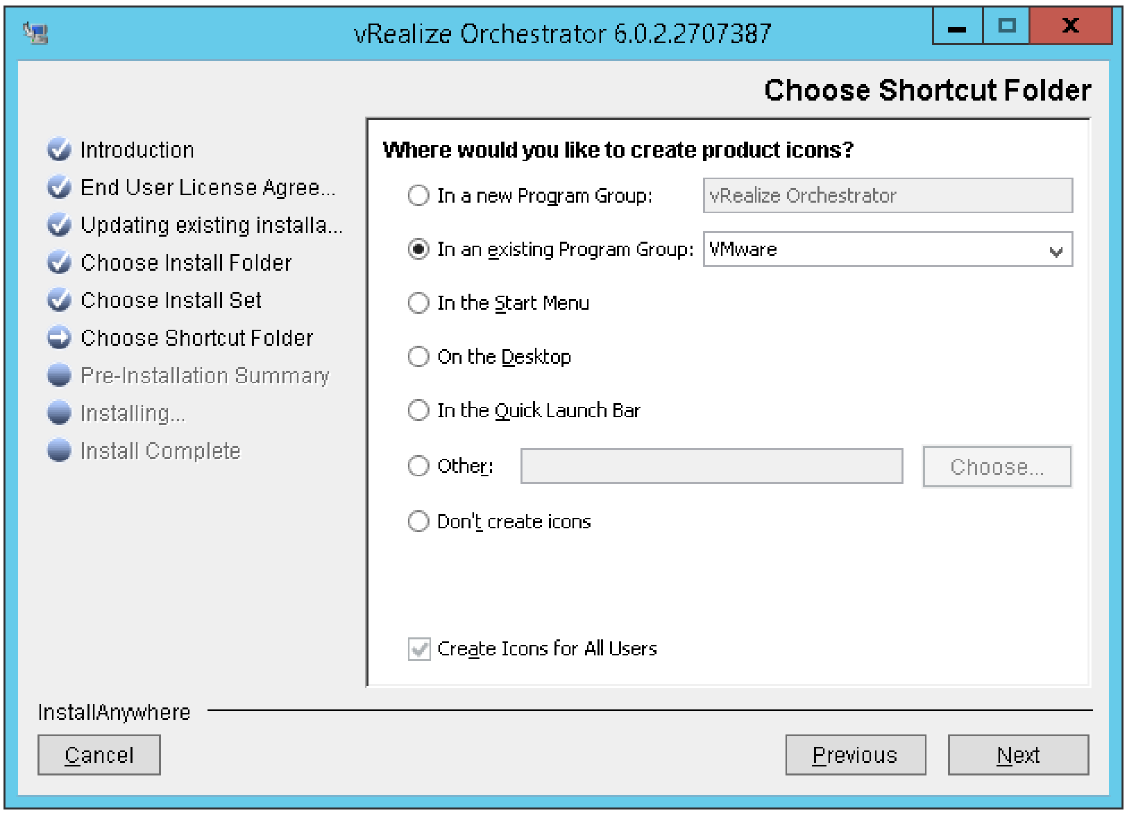
vRealize Orchestrator 6.0.2.2707387

Choose Install Set

- ✓ Introduction
- ✓ End User License Agree...
- ✓ Updating existing installa...
- ✓ Choose Install Folder
- ➔ Choose Install Set
- Choose Shortcut Folder
- Pre-Installation Summary
- Installing...
- Install Complete

Client
Install the VMware Orchestrator Client application.

Figure 201 Choose Install Set



vRealize Orchestrator 6.0.2.2707387

Choose Shortcut Folder

- ✓ Introduction
- ✓ End User License Agree...
- ✓ Updating existing installa...
- ✓ Choose Install Folder
- ✓ Choose Install Set
- ➔ Choose Shortcut Folder
- Pre-Installation Summary
- Installing...
- Install Complete

Where would you like to create product icons?

○ In a new Program Group: vRealize Orchestrator

● In an existing Program Group: VMware

○ In the Start Menu

○ On the Desktop

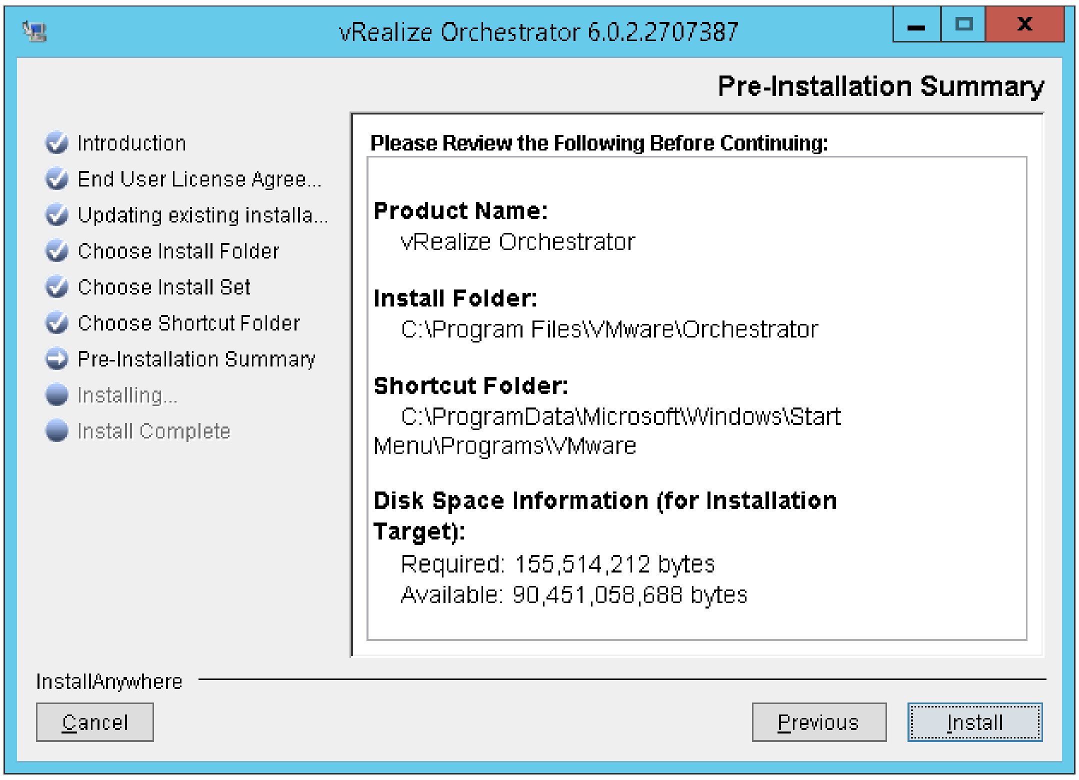
○ In the Quick Launch Bar

○ Other:

○ Don't create icons

☑ Create Icons for All Users

Figure 202 Choose Shortcut Folder



Pre-Installation Summary

Please Review the Following Before Continuing:

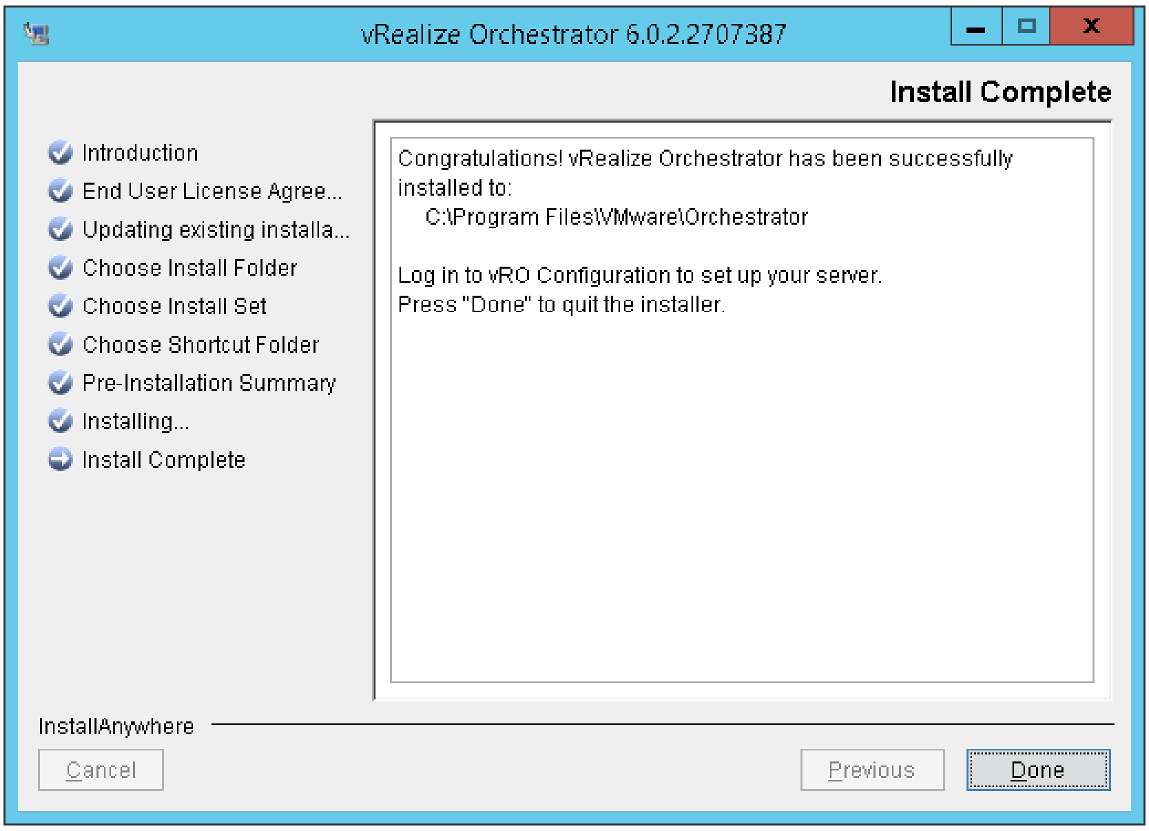
Product Name:
vRealize Orchestrator

Install Folder:
C:\Program Files\VMware\Orchestrator

Shortcut Folder:
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\VMware

Disk Space Information (for Installation Target):
Required: 155,514,212 bytes
Available: 90,451,058,688 bytes

Figure 203 Pre-Installation Summary

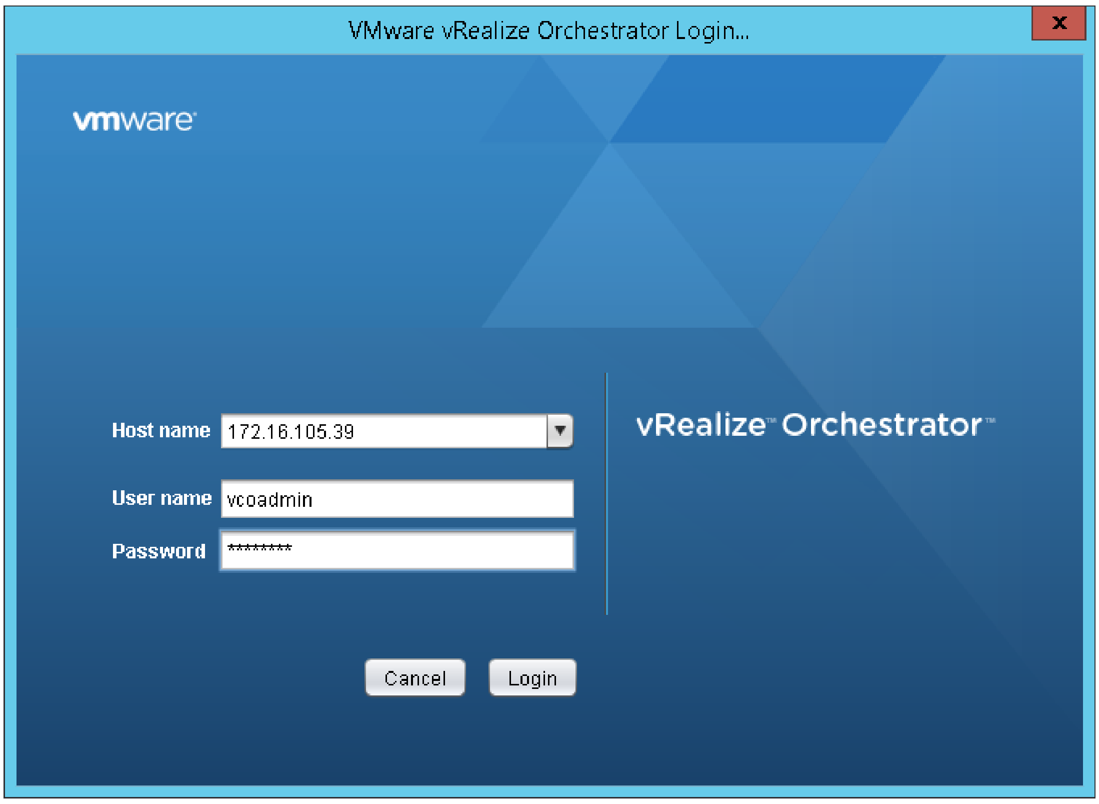


Install Complete

Congratulations! vRealize Orchestrator has been successfully installed to:
C:\Program Files\VMware\Orchestrator

Log in to vRO Configuration to set up your server.
Press "Done" to quit the installer.

Figure 204 Install Complete



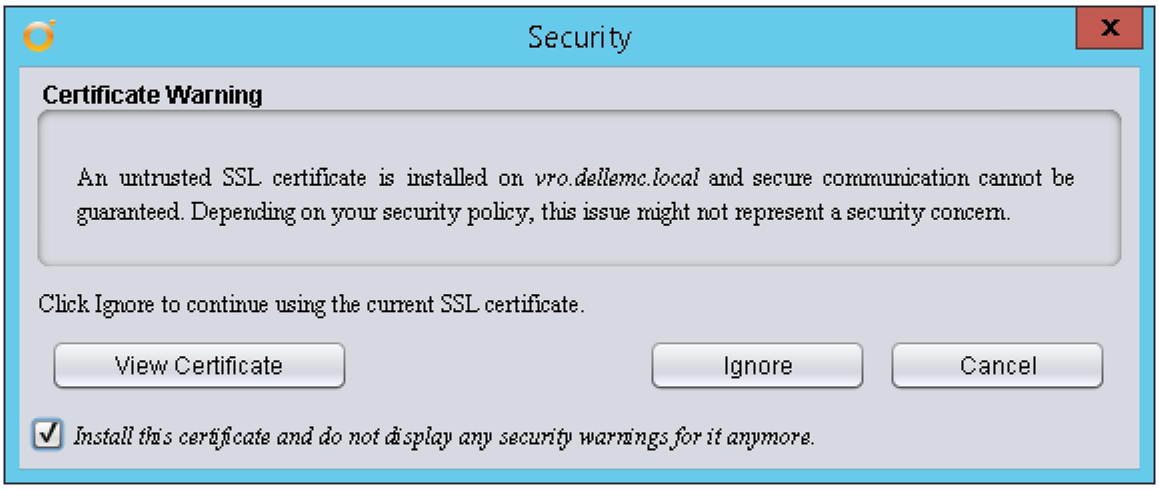
VMware vRealize Orchestrator Login...

Host name 172.16.105.39

User name vcoadmin

Password ********

Figure 205 VMware vRealize Orchestrator Login



Security

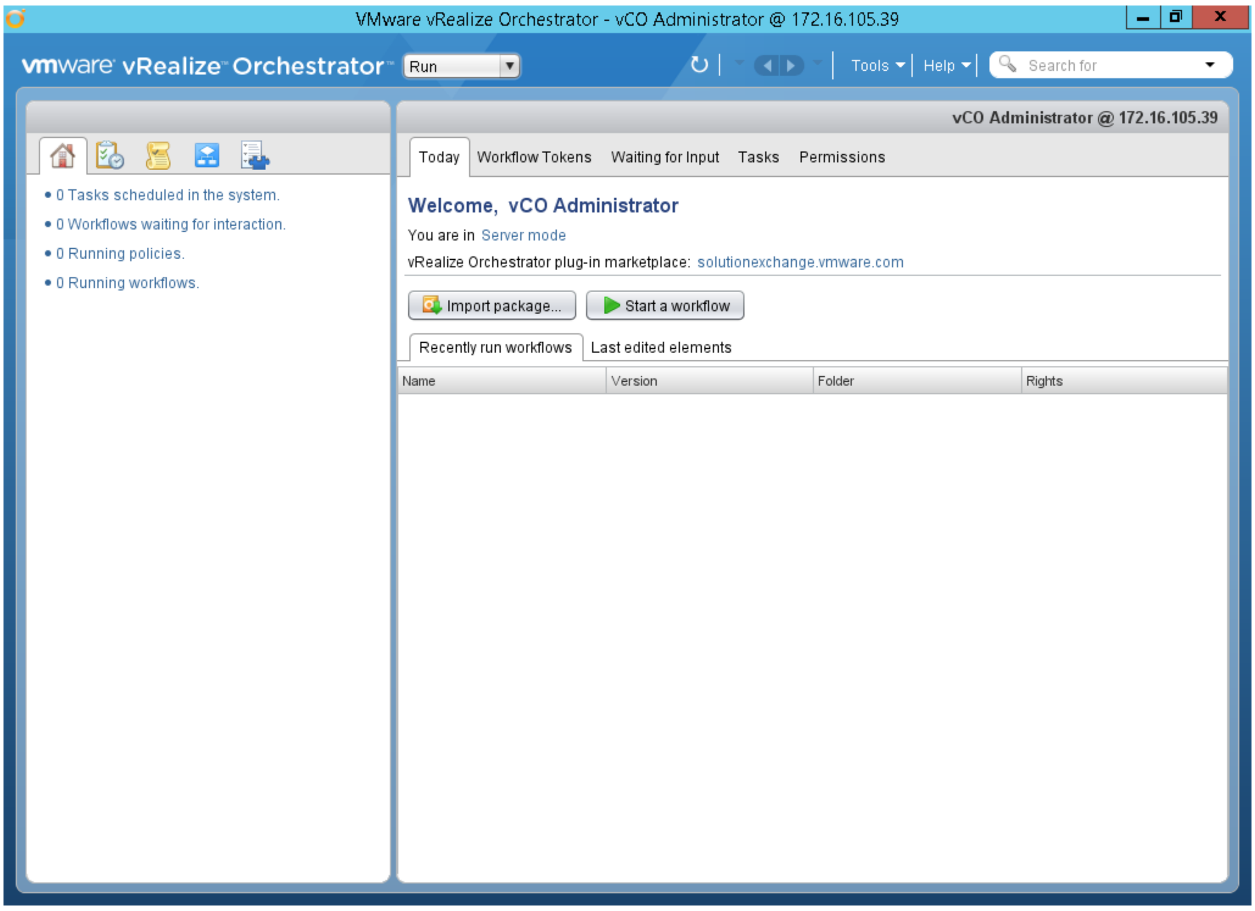
Certificate Warning

An untrusted SSL certificate is installed on *vro.dellemc.local* and secure communication cannot be guaranteed. Depending on your security policy, this issue might not represent a security concern.

Click Ignore to continue using the current SSL certificate.

☑ *Install this certificate and do not display any security warnings for it anymore.*

Figure 206 Security- Certificate Warning



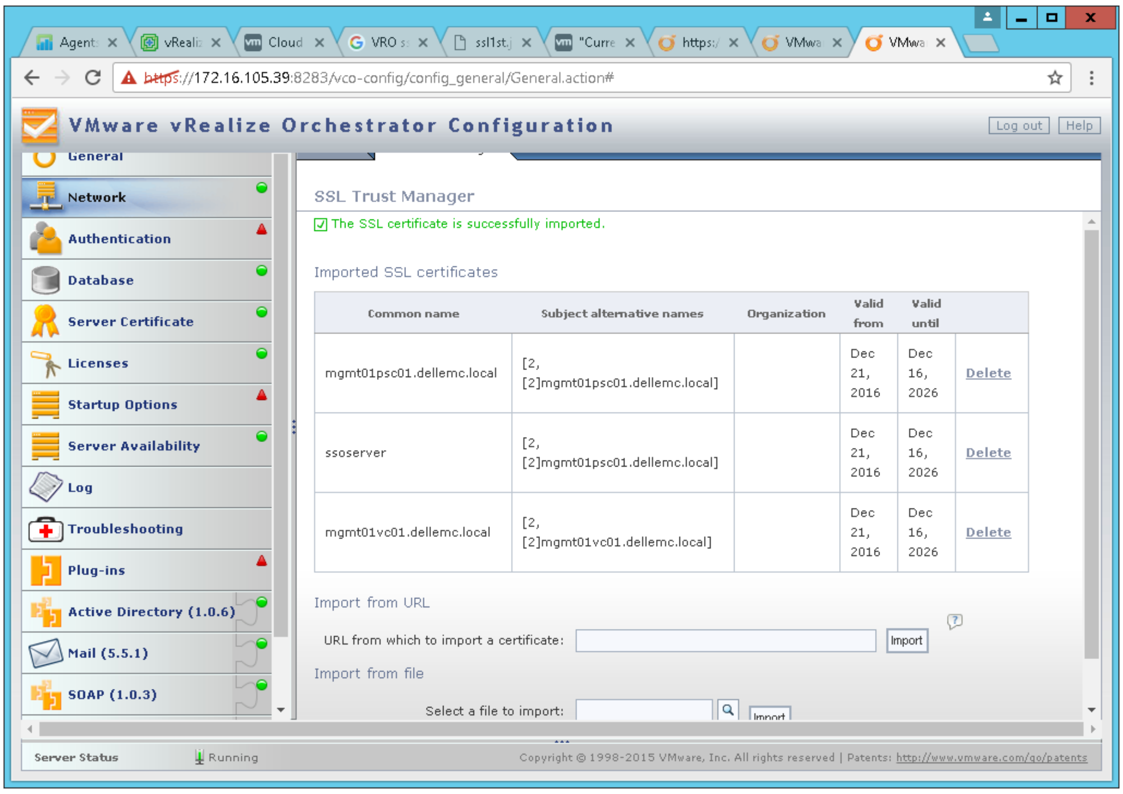
- 0 Tasks scheduled in the system.
- 0 Workflows waiting for interaction.
- 0 Running policies.
- 0 Running workflows.

Welcome, vCO Administrator

You are in Server mode

vRealize Orchestrator plug-in marketplace: solutionexchange.vmware.com

Figure 207 VMware vRealize Welcome page



https://172.16.105.39:8283/vco-config/config_general/General.action#
VMware vRealize Orchestrator Configuration
Log out
Help
General
Network
Authentication
Database
Server Certificate
Licenses
Startup Options
Server Availability
Log
Troubleshooting
Plug-ins
Active Directory (1.0.6)
Mail (5.5.1)
SOAP (1.0.3)
Server Status
Running
Copyright © 1998-2015 VMware, Inc. All rights reserved | Patents: http://www.vmware.com/go/patents

SSL Trust Manager

☑ The SSL certificate is successfully imported.

Imported SSL certificates

Common name	Subject alternative names	Organization	Valid from	Valid until	
mgmt01psc01.dellemc.local	[2, [2]mgmt01psc01.dellemc.local]		Dec 21, 2016	Dec 16, 2026	Delete
ssoserver	[2, [2]mgmt01psc01.dellemc.local]		Dec 21, 2016	Dec 16, 2026	Delete
mgmt01vc01.dellemc.local	[2, [2]mgmt01vc01.dellemc.local]		Dec 21, 2016	Dec 16, 2026	Delete

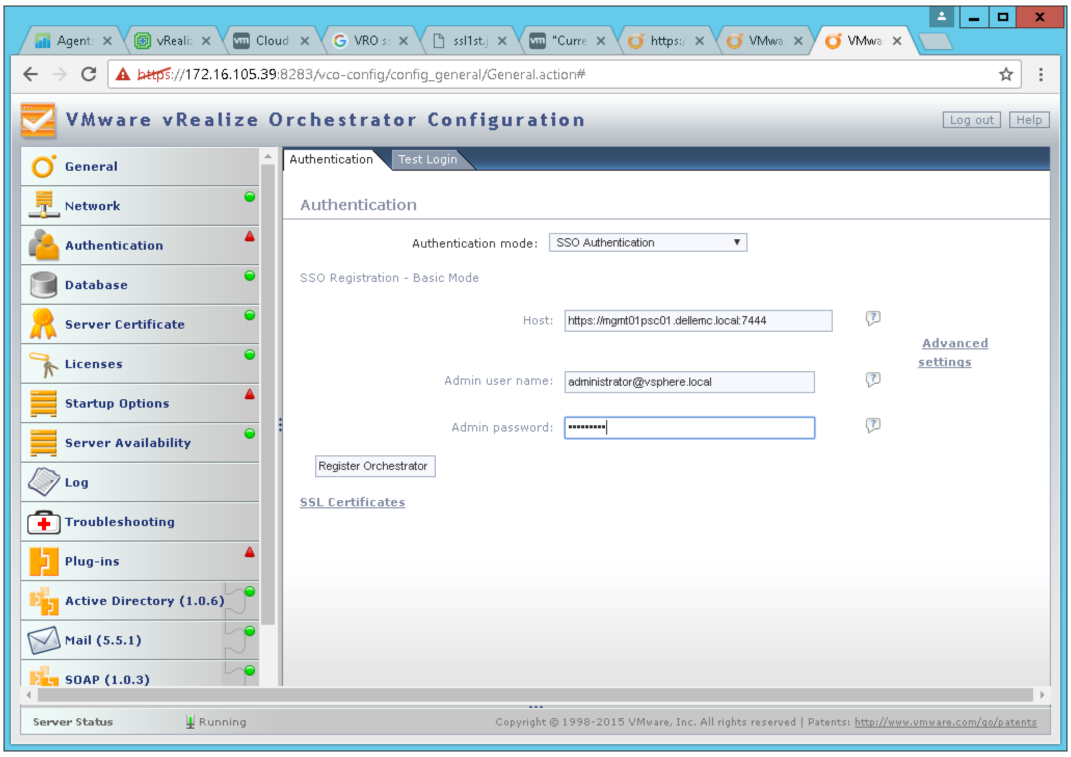
Import from URL

URL from which to import a certificate: Import

Import from file

Select a file to import: Import

Figure 208 SSL Trust Manager



Authentication

Authentication mode: SSO Authentication

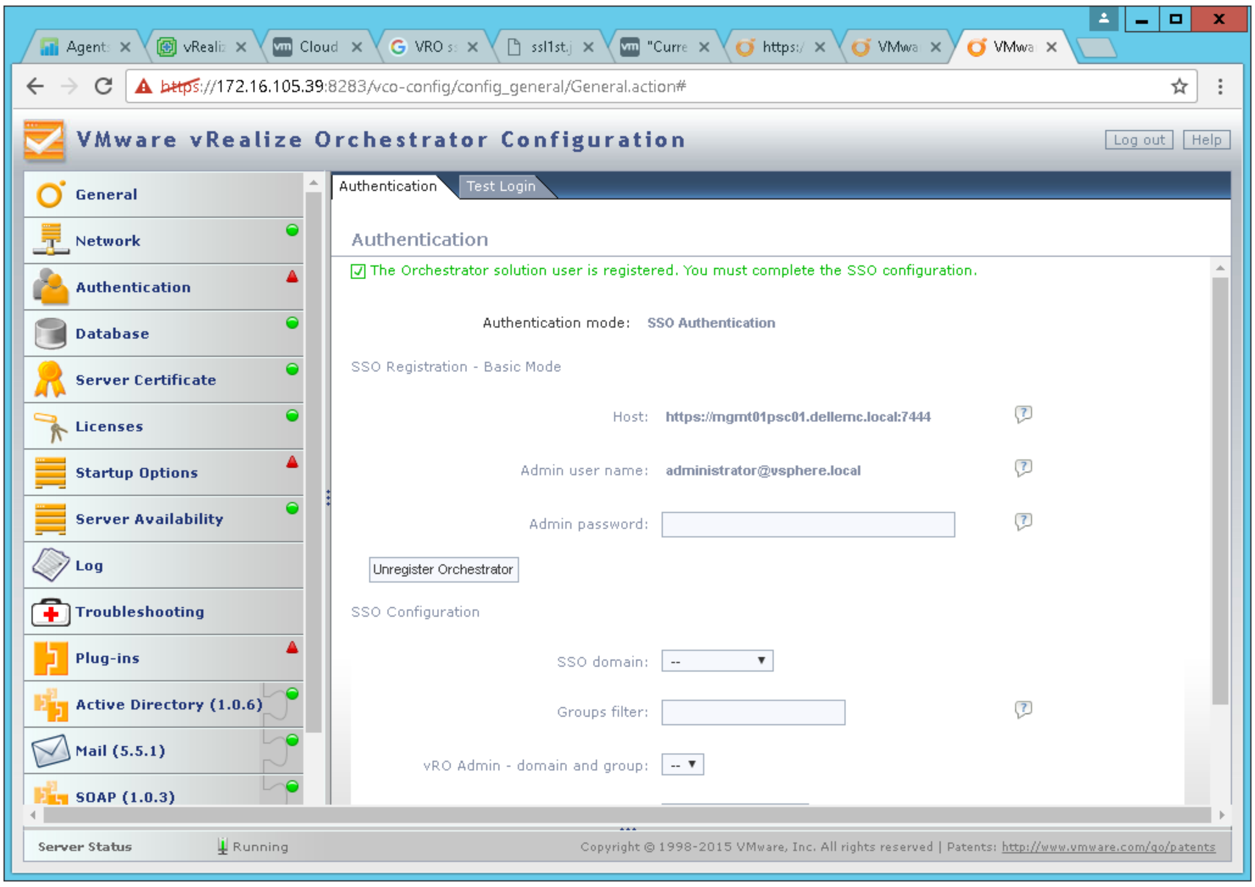
SSO Registration - Basic Mode

Host: https://mgmt01psc01.dellemc.local:7444

Admin user name: administrator@vsphere.local

Admin password: ••••••••••

Figure 209 SSO Authentication



Authentication

☑ The Orchestrator solution user is registered. You must complete the SSO configuration.

Authentication mode: SSO Authentication

SSO Registration - Basic Mode

Host: https://mgmt01psc01.dellemc.local:7444

Admin user name: administrator@vsphere.local

Admin password:

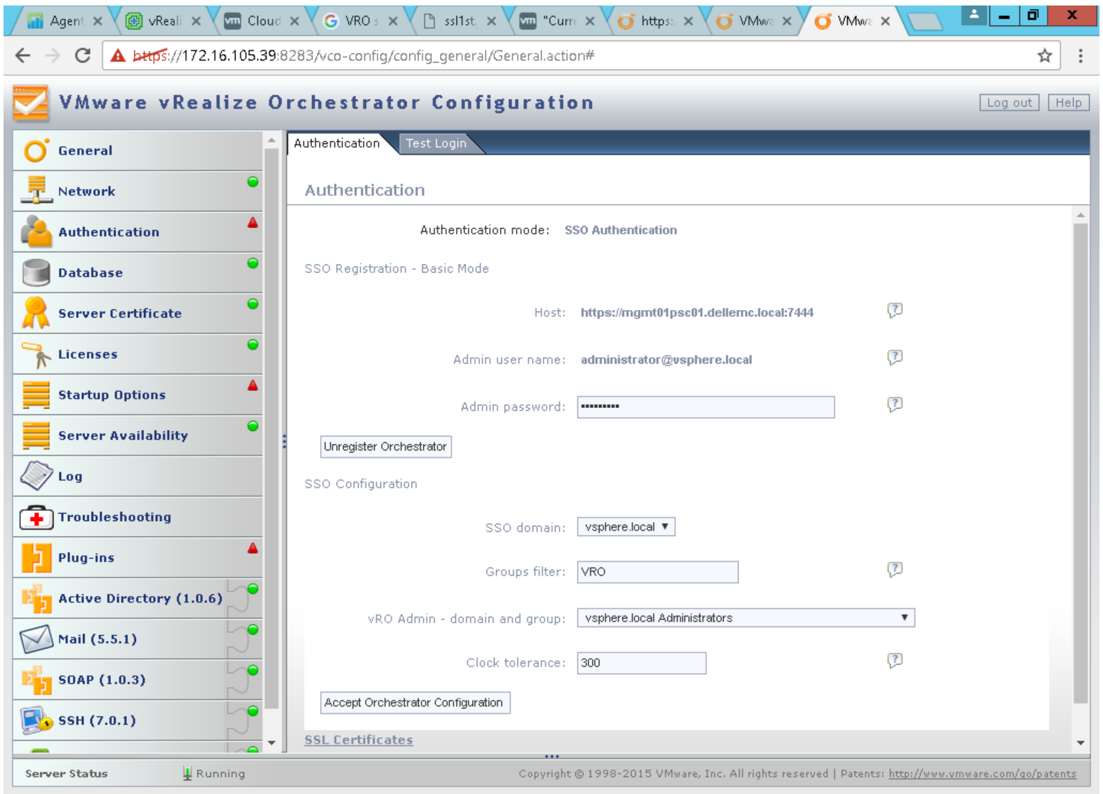
SSO Configuration

SSO domain: --

Groups filter:

vRO Admin - domain and group: --

Figure 210 SSO Configuration



Authentication

Authentication mode: SSO Authentication

SSO Registration - Basic Mode

Host: https://mgmt01psc01.dellemc.local:7444

Admin user name: administrator@vsphere.local

Admin password: ••••••••••

SSO Configuration

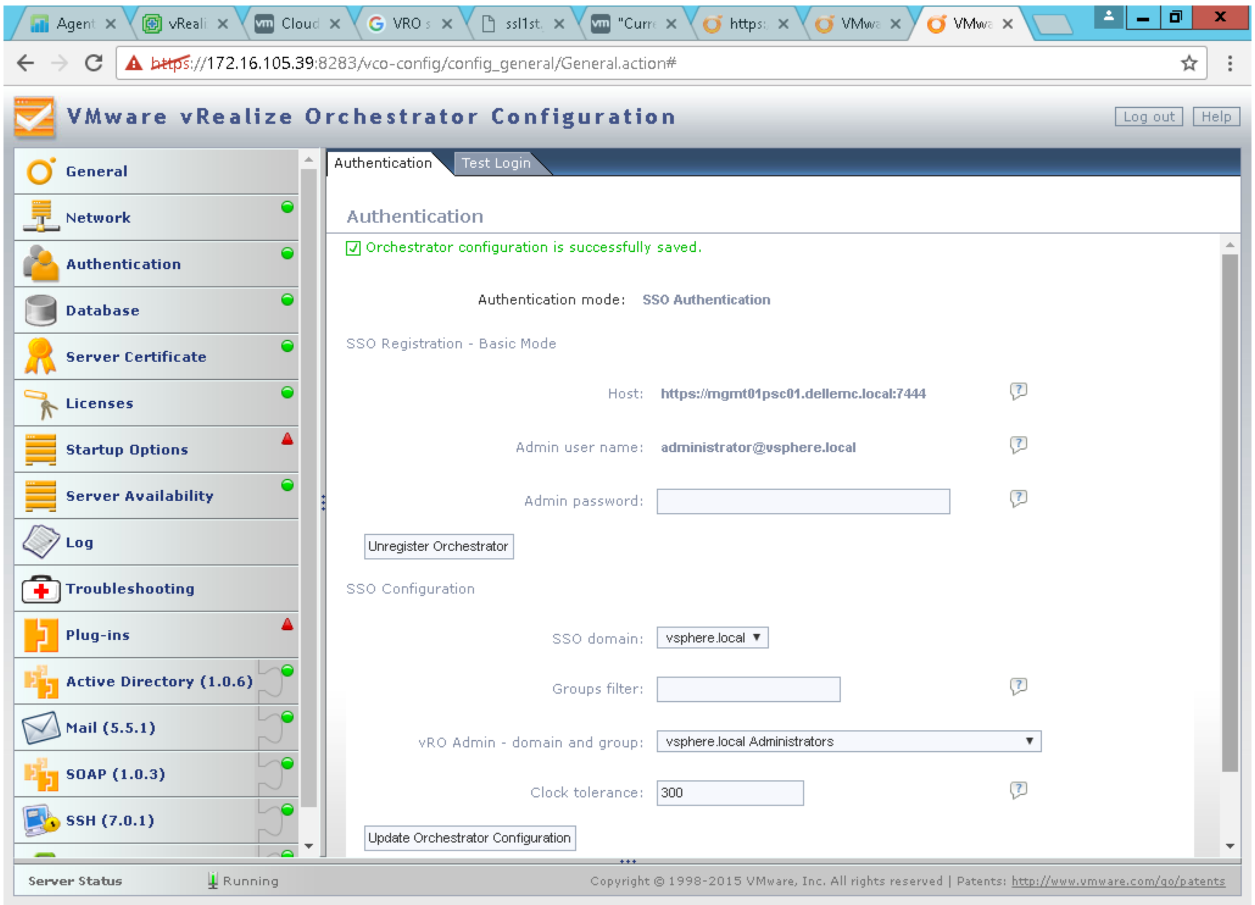
SSO domain: vsphere.local

Groups filter: VRO

vRO Admin - domain and group: vsphere.local Administrators

Clock tolerance: 300

Figure 211 SSO Configuration



Authentication

☑ Orchestrator configuration is successfully saved.

Authentication mode: SSO Authentication

SSO Registration - Basic Mode

Host: https://mgmt01psc01.dellemc.local:7444

Admin user name: administrator@vsphere.local

Admin password:

SSO Configuration

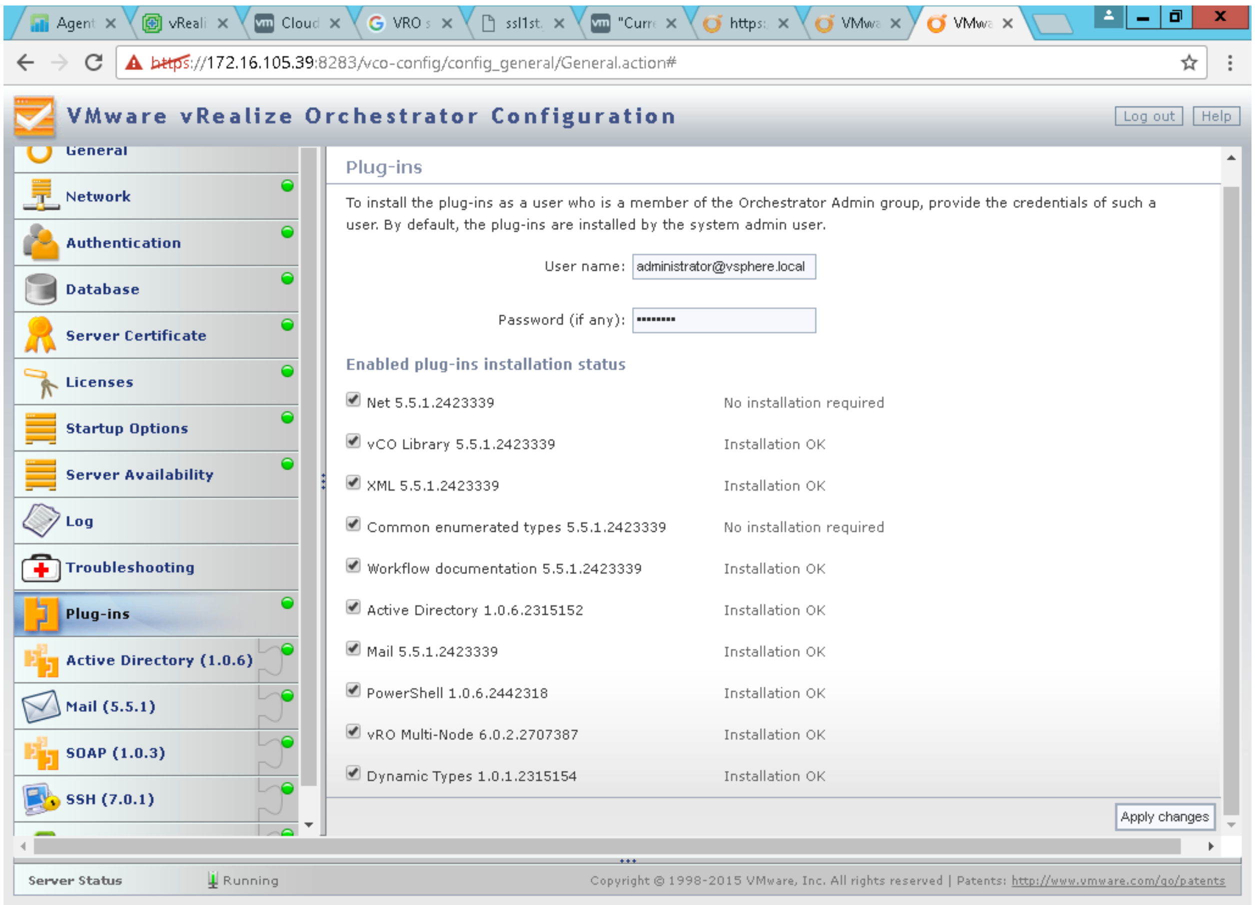
SSO domain: vsphere.local

Groups filter:

vRO Admin - domain and group: vsphere.local Administrators

Clock tolerance: 300

Figure 212 SSO Configuration



Plug-ins

To install the plug-ins as a user who is a member of the Orchestrator Admin group, provide the credentials of such a user. By default, the plug-ins are installed by the system admin user.

User name: administrator@vsphere.local

Password (if any): ••••••••

Enabled plug-ins installation status

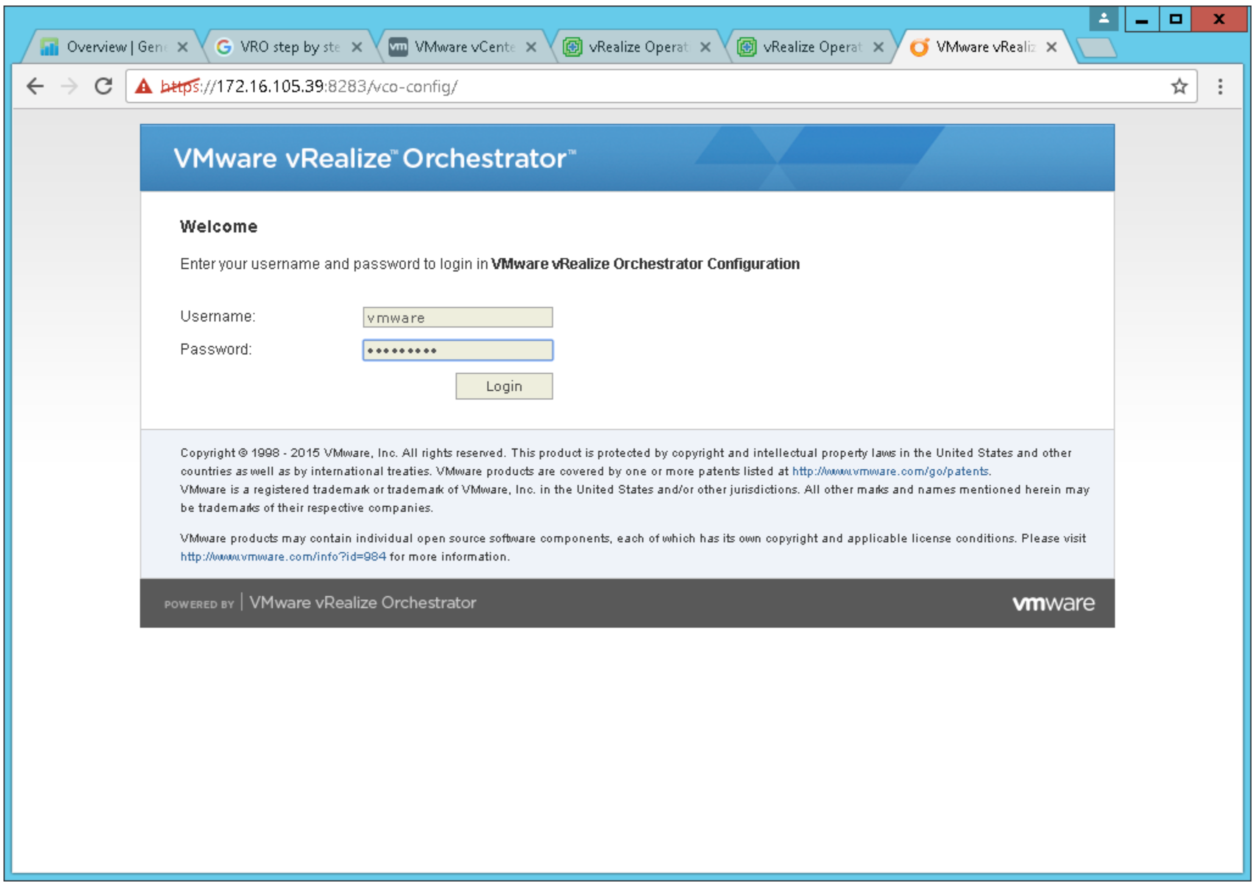
☑ Net 5.5.1.2423339	No installation required
☑ vCO Library 5.5.1.2423339	Installation OK
☑ XML 5.5.1.2423339	Installation OK
☑ Common enumerated types 5.5.1.2423339	No installation required
☑ Workflow documentation 5.5.1.2423339	Installation OK
☑ Active Directory 1.0.6.2315152	Installation OK
☑ Mail 5.5.1.2423339	Installation OK
☑ PowerShell 1.0.6.2442318	Installation OK
☑ vRO Multi-Node 6.0.2.2707387	Installation OK
☑ Dynamic Types 1.0.1.2315154	Installation OK

Apply changes

Server Status: Running

Copyright © 1998-2015 VMware, Inc. All rights reserved | Patents: http://www.vmware.com/go/patents

Figure 213 Plug-ins


Overview | Gen
VRO step by ste
VMware vCente
vRealize Operat
vRealize Operat
VMware vRealiz
https://172.16.105.39:8283/vco-config/
VMware vRealize® Orchestrator™
Login
POWERED BY | VMware vRealize Orchestrator
vmware

Welcome

Enter your username and password to login in **VMware vRealize Orchestrator Configuration**

Username: vmware

Password: •••••••••

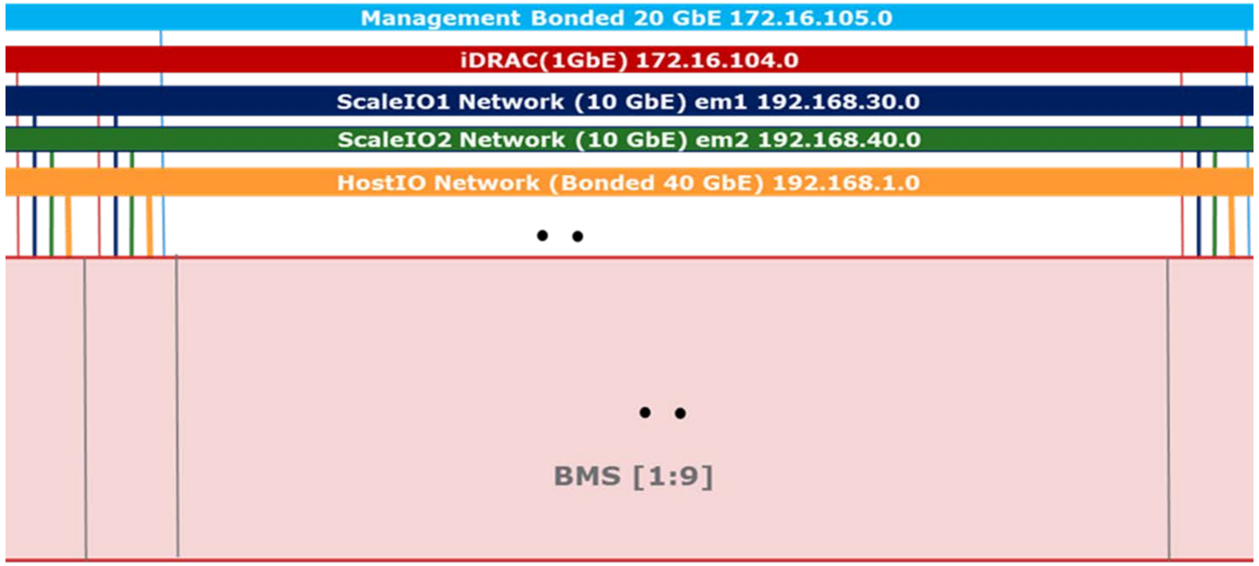
Copyright © 1998 - 2015 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.
VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware products may contain individual open source software components, each of which has its own copyright and applicable license conditions. Please visit http://www.vmware.com/info?id=984 for more information.

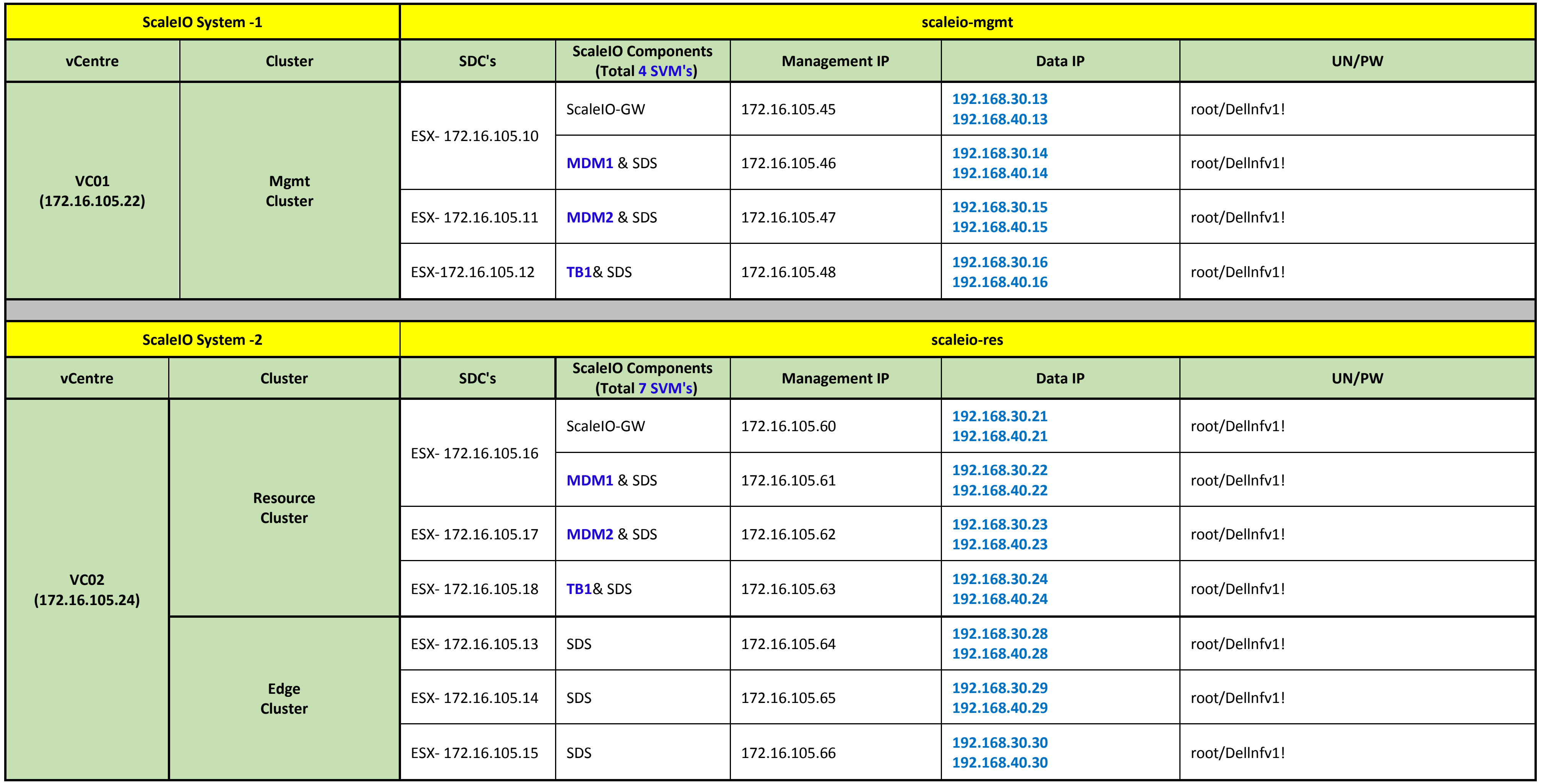
Figure 214 VMware vRealize Orchestrator

A Rack

Setup	Hostname	MAC	Device Type	IP	Vlan		Vlan			
Hawk	Management		Dell Networking S4048T	172.16.101.4	Untagged					
Hawk	Spine1		Dell Networking S6010	172.16.101.5	Untagged					
Hawk	Spine2		Dell Networking S6010	172.16.101.6	Untagged					
Hawk	Leaf1		Dell Networking S6010	172.16.101.7	Untagged					
Hawk	Leaf2		Dell Networking S6010	172.16.101.8	Untagged					
				iDRAC		**Hypervisor Mgmt IP**		Username	Password	
Hawk	VIM1	44:A8:42:26:BD:61	PowerEdge R730	172.16.104.10	2104	172.16.105.10	U 2105	root	dellnfv	
Hawk	VIM2	44:A8:42:07:FC:0B	PowerEdge R730	172.16.104.11	2104	172.16.105.11	U 2105	root	dellnfv	
Hawk	VIM3	44:A8:42:26:BE:6D	PowerEdge R730	172.16.104.12	2104	172.16.105.12	U 2105	root	dellnfv	
Hawk	Compute1	44:A8:42:26:C2:0E	PowerEdge R730	172.16.104.13	2104	172.16.105.13	U 2105	root	dellnfv	
Hawk	Compute2	44:A8:42:26:BC:E7	PowerEdge R730	172.16.104.14	2104	172.16.105.14	U 2105	root	dellnfv	
Hawk	Compute3	44:A8:42:22:C2:D6	PowerEdge R730	172.16.104.15	2104	172.16.105.15	U 2105	root	dellnfv	
Hawk	Edge1	44:A8:42:07:FC:23	PowerEdge R730	172.16.104.16	2104	172.16.105.16	U 2105	root	dellnfv	
Hawk	Edge2	44:A8:42:22:C5:B8	PowerEdge R730	172.16.104.17	2104	172.16.105.17	U 2105	root	dellnfv	
Hawk	Edge3	44:A8:42:26:BB:07	PowerEdge R730	172.16.104.18	2104	172.16.105.18	U 2105	root	dellnfv	


Management Bonded 20 GbE 172.16.105.0
iDRAC(1GbE) 172.16.104.0
ScaleIO1 Network (10 GbE) em1 192.168.30.0
ScaleIO2 Network (10 GbE) em2 192.168.40.0
HostIO Network (Bonded 40 GbE) 192.168.1.0
BMS [1:9]

B ScaleIO System



ScaleIO System -1		scaleio-mgmt				
vCentre	Cluster	SDC's	ScaleIO Components (Total 4 SVM's)	Management IP	Data IP	UN/PW
VC01 (172.16.105.22)	Mgmt Cluster	ESX- 172.16.105.10	ScaleIO-GW	172.16.105.45	192.168.30.13 192.168.40.13	root/Dellnfv1!
			MDM1 & SDS	172.16.105.46	192.168.30.14 192.168.40.14	root/Dellnfv1!
		ESX- 172.16.105.11	MDM2 & SDS	172.16.105.47	192.168.30.15 192.168.40.15	root/Dellnfv1!
		ESX-172.16.105.12	TB1& SDS	172.16.105.48	192.168.30.16 192.168.40.16	root/Dellnfv1!

ScaleIO System -2		scaleio-res				
vCentre	Cluster	SDC's	ScaleIO Components (Total 7 SVM's)	Management IP	Data IP	UN/PW
VC02 (172.16.105.24)	Resource Cluster	ESX- 172.16.105.16	ScaleIO-GW	172.16.105.60	192.168.30.21 192.168.40.21	root/Dellnfv1!
			MDM1 & SDS	172.16.105.61	192.168.30.22 192.168.40.22	root/Dellnfv1!
		ESX- 172.16.105.17	MDM2 & SDS	172.16.105.62	192.168.30.23 192.168.40.23	root/Dellnfv1!
		ESX- 172.16.105.18	TB1& SDS	172.16.105.63	192.168.30.24 192.168.40.24	root/Dellnfv1!
	Edge Cluster	ESX- 172.16.105.13	SDS	172.16.105.64	192.168.30.28 192.168.40.28	root/Dellnfv1!
		ESX- 172.16.105.14	SDS	172.16.105.65	192.168.30.29 192.168.40.29	root/Dellnfv1!
		ESX- 172.16.105.15	SDS	172.16.105.66	192.168.30.30 192.168.40.30	root/Dellnfv1!

C Reference

Additional information can be obtained at http://www.dell.com/nfv or by e-mailing nfv@dell.com.

If you need additional services or implementation help, please contact your Dell EMC sales representative.