DELLEMC

Dell EMC + VMware Cloud Infrastructure Platform for NFV

VMware vCloud NFV 1.5 - NFVI Solution Service Provider Solutions Group April 2017

Revisions

Date	Description
April 2017	Initial release

Copyright © 2017 Dell Inc. or its subsidiaries. All Rights Reserved. Except as stated below, no part of this document may be reproduced, distributed or transmitted in any form or by any means, without express permission of Dell.

You may distribute this document within your company or organization only, without alteration of its contents.

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.

Trademarks used in this text: Dell[™], the Dell logo, Dell Boomi[™], PowerEdge[™], PowerVault[™], PowerConnect[™], OpenManage[™], EqualLogic[™], Compellent[™], KACE[™], FlexAddress[™], Force10[™] and Vostro[™] are trademarks of Dell Inc. EMC VNX®, and EMC Unisphere® are registered trademarks of Dell. Other Dell trademarks may be used in this document. VMware®, Virtual SMP®, VMware vMotion®, VMware vCenter®, VMware vSphere®, VMware Capacity Planner™, VMware ESX®, VMware ESXi[™], VMware® Integrated OpenStack, VMware NSX®, VMware NSX® Edge[™], VMware NSX® for vSphere®, VMware NSX® Manager™, VMware Power CLI, VMware Site Recovery Manager[™], VMware Tools[™], VMware vCenter Server[®], VMware vCenter Server[®] Appliance[™], VMware vCloud Director®, VMware vCloud®, VMware vCloud® NFV™, VMware vRealize®, VMware vRealize® Log Insight[™], VMware vRealize® Operations Insight[™], VMware vRealize® Operations ManagerTM, VMware vRealize[®] Operations Management PackTM, VMware vRealize[®] OperationsTM, VMware vRealize® Orchestrator™. VMware vRealize® Suite Advanced. VMware vSphere® Data Protection[™], VMware vSphere® Distributed Resource Scheduler[™], VMware vSphere® Distributed SwitchTM, VMware vSphere® High Availability, VMware vSphere® PowerCLITM, VMware vSphere® Replication™, VMware vSphere® vMotion® and VMware vSphere® Web Client are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron[™]. AMD Phenom[™] and AMD Sempron[™] are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Broadcom® and NetXtreme® are registered trademarks of QLogic is a registered trademark of QLogic Corporation. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or names or their products and are the property of their respective owners. Dell disclaims proprietary interest in the marks and names of others.

Table of Contents

1	Overv	view	5
2	How	to use this guide	6
3	Dell E	EMC Hardware Requirements	7
4	Softw	vare Requirements	8
	4.1	VMWare	8
	4.2	Miscellaneous	8
	4.3	License Requirements	8
5	Refer	rence Architecture	9
	5.1	Logical topology	9
	5.2	Physical Topology	10
6	VMW	are virtualization platform	11
	6.1	Install ESXi on Servers	11
	6.1.1	Verify the SD card module is present	11
	6.1.2	Set the boot sequence to boot the device from SD card	12
	6.1.3	Use Vmware ESXi installer to install the hypervisor	12
	6.1.4	Configure the management interface	14
	6.2	Install vCenter Server	15
	6.2.1	Mount VCSA ISO	16
	6.2.2	Install External PSC	16
	6.2.3	Deploy the vCenter appliance	20
	6.2.4	Deploy second EPSC and vCenter	24
	6.3	Build datacenter	25
	6.3.1	Add Licenses	25
	6.3.2	Create datacenter and clusters	25
	6.3.3	Add Hosts to clusters	26
	6.4	Configure host networking	27
	6.4.1	Management Networking	28
	6.4.2	Migrate the second uplink port to DvSwitch	31
	6.4.3	Infrastructure Networking	33
	6.4.4	VxLAN Data Networking	40
	6.5	Enable VSAN	41
	6.5.1	Enable VSAN in cluster	41
	6.5.2	Assign VSAN license key to cluster	42
	6.5.3	Claim the hard disks for VSAN	42

6.6	Install NSX
6.6.1	Deploy NSX manager
6.6.2	Register NSX manager with vCenter
6.6.3	Deploy NSX controllers
6.6.4	Exclude VMs from Firewall
6.6.5	Install NSX Kernel Modules
6.6.6	Configure VxLAN
6.6.7	Assign segment ID
6.6.8	Add a Transport Zone
6.6.9	Create logical switch
6.6.10	Deploy and configure Distributed Logical Router53
6.6.11	Deploy Edge services gateway55
6.6.12	Configure OSPF on DLR
6.6.13	Route redistribution and firewall configuration
6.6.14	Configure OSPF on ESG63
6.7	Install vCloud Director
6.7.1	Install and Bringup Windows VM64
6.7.2	Install SQL Server in Windows VM64
6.7.3	Configure the SQL Server
6.7.4	Setup DNS server and add entries
6.7.5	Install and Bring up RedHat Enterprise Linux VM71
6.7.6	Start and Stop vCloud director

1 Overview

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

2 How to use this guide

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

3 Dell EMC Hardware Requirements

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

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

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

 Table 1
 Dell EMC Hardware components

4 Software Requirements

4.1 VMWare

The table below lists all the mandatory components required:

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

Table 2 VMware software components

4.2 Miscellaneous

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

 Table 3
 Miscellaneous software components

4.3 License Requirements

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

Table 4 License Requirements

5 Reference Architecture

5.1 Logical topology

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

Virtual SAN Enabled Cluster Infrastructure Networks Virtual SAN Network Virtual SAN Network	Management Cluster	NSX Manager		PSC PSC VCenter Server	NSX Manager VCloud Director	Replication
ESXI Management			Edge Cluster			Resource Cluster
Virtual SAN Enabled Cluster		DLR NSX Controller (1) NSX NSX NSX NSX Controller (2) NSX Controller (3)	ESG (1) ESG (2) ESG (3)			F VNF F VNF VNF
	Legend	Management Cluster VIM Components	Operations Management Components	Resource / Edge (VIM Compone	Cluster nts Telco Wo	orkloads

Figure 1 VMware Cluster design

5.2 Physical Topology



Figure 2 VMware Block design



Legend:

VM public

6 VMWare virtualization platform

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

6.1 Install ESXi on Servers

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

6.1.1 Verify the SD card module is present

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

Default iDRAC Username : root Password : calvin

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

System Setup		Help About Exit
System BIOS		
System BIOS Settings • Integrated Devices		
Internal USB Port	······ ⊛ On _ Off	-
Integrated RAID Controller	•••••• 💿 Enabled 🔿 Disabled	
Integrated Network Card 1	······ ● Enabled	
I/OAT DMA Engine	O 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	-
		-
This option enables/disables the USB 3.0 support When this field is set to Disabled (default), the U	rt. SB devices (Press <f1> for more help)</f1>	
PowerEdge R730 Service Tag : 6KP3F42		Back
Figure 3 System BIOS Settings		

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

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

Figure 4 Change Order Dialog Box

6.1.3 Use Vmware ESXi installer to install the hypervisor

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



Figure 5 Dell ESXi Boot Menu

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

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) DELL PERC H730 Mini (naa.644a84202ece29001cf7d) DELL IDSDM (mpx.vmhba32:C0:T0:L0) Remote: (none)	186.31 GiB 558.38 GiB 14.92 GiB
(Esc) Cancel (F1) Details (F5) Refresh (Enter)	Cont inue

Figure 6 Confirm SD card is selected

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

Enter a root password
Root password: ******* Confirm password: ****** _ Passwords match.
(Esc) Cancel (F9) Back (Enter) Continue

Figure 7 Enter root password

Repeat this process for all the servers in the setup.

6.1.4 Configure the management interface

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

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

Figure 8 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
<pre>CD> View Details</pre>	<pre>Space> Toggle Selected</pre>	<pre><enter> OK <esc> Cancel</esc></enter></pre>

Figure 9 Select management network connection





6.2 Install vCenter Server

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

6.2.1 Mount VCSA ISO

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

2	2
vCenter Server	Appliance [™] 6.0
Install	Upgrade

Figure 11 vCenter Server Appliance install

6.2.2 Install External PSC

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

VMware vCenter Server Applianc	e Deployment		
 1 End User License Agreement 2 Connect to target server 	Connect to target server Specify the ESXi host or vCenter	Server on which to deploy the vCenter Se	erver Appliance.
 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 Configure database 10 Network Settings 11 Ready to complete 	FQDN or IP Address: User name: Password: Make sure the ESXI host i When deploying to a vSpt portgroup. After deployme	yet is an ESXi host: s not in lock down mode or maintenance here Distributed Switch (VDS), the applian int, it can be moved to a static or dynamic	mode. nce must be deployed to an ephemeral portgroup.
			Net Set Out
		Datk	Cancer

Figure 12 Connect to target server

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

🚰 VMware vCenter Server Appliance Deployment			
 1 End User License Agreement 2 Connect to target server 	Set up virtual machine Specify virtual machine setting:	s for the vCenter Server Appliance to be	deployed.
 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 Configure database 10 Network Settings 11 Ready to complete 	Appliance name: OS user name: OS password: Confirm OS password:	VIM EPSC root	• •
		Back	Next Finish Cancel

Figure 13 Set up virtual machine

Choose EPSC as show below.



Figure 14 Select deployment type

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

Mware vCenter Server Appliance Deployment			
 1 End User License Agreement 2 Connect to target server 	Set up Single Sign-on (SSO) Create or join a SSO domain. A	n SSO configuration cannot be changed at	fter deployment.
 3 Set up virtual machine 4 Select deployment type 	 Create a new SSO domain Join an SSO domain in an e 	existing vCenter 6.0 platform services contro	oller
5 Set up Single Sign-on 6 Select appliance size	vCenter SSO User name:	administrator	
7 Select datastore	vCenter SSO Password:	••••••	0
8 Network Settings 9 Ready to complete	Confirm password:	••••••	
	SSO Domain name:	vsphere.local	0
	SSO Site name:	SantaClara	0
	A Before proceeding, make Active Directory domain name	e sure that the vCenter Single Sign-On don e.	nain name used is different than your
		Back	Next Finish Cancel



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

🚰 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 Sing on 	Select datastore Select the storage location for this deployment The following datastores are accessible. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.			configuration files		
 ✓ 6 Select appliance size 	Name	Туре	Capacity	Free	Provisioned	Thin Provisioning
7 Select datastore	tempHD	VMFS	558.75 GB	557.8 GB	0.95 GB	true
8 Network Settings 9 Ready to complete						
	Enable Thin Di	sk Mode 🚯				
				Back	Next Finish	Cancel

Figure 16 Select datastore

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

🚰 VMware vCenter Server Applianc	e Deployment	
✓ 1 End User License Agreement	Choose a network:	VM Network 🔻 🗊
2 Connect to target server		
3 Set up virtual machine	IP address family:	IPv4 v
4 Select deployment type	Maharahatara	
5 Set up Single Sign-on	Network type:	static v
 7 Select datastore 	Network address:	170 16 114 10
8 Network Settings	Heard and a solution of the so	172.10.114.10
9 Ready to complete	System name [FQDN or IP address]:	172.16.114.10
	Subnet mask:	255.255.255.0
	Network gateway:	172.16.114.1
	Network DNS Servers (separated by commas)	8.8.8.8
	Configure time sync:	Synchronize appliance time with ESXi host Use NTP servers (Separated by commas)
	Enable ssh	•
		Back Next Finish Cancel

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

Figure 17 Network Settings

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

T VMware vCenter Server Appliance Deployment			
 VMware vCenter Server Applianc 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 Select appliance size 7 Select datastore 8 Network Settings 9 Ready to complete 	e Deployment Ready to complete Please review your settings before starting the installation. Target server info: 172.16.114.101 Name: VIM EPSC Installation type: Install Deployment type: Platform Services Controller Datastore: tempHD Disk mode: thick Network mapping: Network to VM Network IP allocation: IPv4, static Host Name SSO User name = administrator SSO Site name = SantaClara SSO Lara		
	Network 11P address = 172.16.114.10 Host Name - unimpsc Network 1 netmask = 255.255.255.0 Default gateway = 172.16.114.1 DNS = 8.8.8 Back Next Finish Cancel		

Figure 18 Complete installation

19 Dell EMC + VMware Cloud Infrastructure Platform for NFV VMware vCloud NFV 1.5 - NFVI Solution

6.2.3 Deploy the vCenter appliance

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

T VMware vCenter Server Appliance Deployment			
 1 End User License Agreement 2 Connect to target server 	Connect to target server Specify the ESXI host or vCenter Server on which to deploy the vCenter Server Appliance.		
3 Set up virtual machine	FQDN or IP Address:	172.6.114.102	
4 Select deployment type 5 Set up Single Sign-on	User name:	root	•
6 Single Sign-on Site 7 Select appliance size	Password:]
8 Select datastore 9 Configure database 10 Network Settings 11 Ready to complete	 Before proceeding, if the tar Make sure the ESXi host When deploying to a vSp portgroup. After deployment 	get is an ESXI host: is not in lock down mode or maintenance here Distributed Switch (VDS), the applia ent, it can be moved to a static or dynamic	mode. nce must be deployed to an ephemeral ; portgroup.
		Back	Next Finish Cancel

Figure 19 Connect to target server

Configure the vCenter appliance name.

🚰 VMware vCenter Server Appliance Deployment			
 1 End User License Agreement 2 Connect to target server 	Set up virtual machine Specify virtual machine setting	s for the vCenter Server Appliance to be de	ployed.
3 Set up virtual machine 4 Select deployment type	Appliance name:	VIM vCenter	0
5 Configure Single Sign-On	OS user name:	root	
7 Select datastore	OS password:	••••••	0
8 Configure database 9 Network Settings	Confirm OS password:	•••••	
10 Ready to complete			
		Back	Next Finish Cancel
Figure 20 Set up vir	tual machine		

20 Dell EMC + VMware Cloud Infrastructure Platform for NFV VMware vCloud NFV 1.5 - NFVI Solution

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





Configure the EPSC SSO password to authenticate vCenter.

Mware vCenter Server Appliance Deployment			
 1 End User License Agreement 2 Connect to target server 	Configure Single Sign-On (SS Connect vCenter Server to a St be changed after deployment.	D) SO domain in an existing platform services controller. An SSO configuration cannot	
 3 Set up virtual machine 4 Select deployment type 5 Configure Single Sign-On 	Platform Services Controller FQDN or IP address:	172.16.114.10	
6 Select appliance size	vCenter SSO User name:	administrator	
7 Select datastore 8 Configure database	vCenter SSO password:		
9 Network Settings 10 Ready to complete	vCenter Single Sign-On HTTPS Port:	443	
	▲ Before proceeding, make s Single Sign-On domain that you	sure you provide the password of the user 'administrator' in the existing vCenter u configured during Platform Services Controller deployment.	
		Back Next Finish Cancel	

Figure 22 Configure Single Sign-On

21 Dell EMC + VMware Cloud Infrastructure Platform for NFV VMware vCloud NFV 1.5 - NFVI Solution Based on the deployment size, chose the appliance size.

VMware vCenter Server Appliance	e Deployment	
 1 End User License Agreement 2 Connect to target server 	Select appliance size Specify a deployment size for the r	ew appliance
 3 Set up virtual machine 4 Select deployment type 	Appliance size:	Tiny (up to 10 hosts, 100 VMs)
✓ 5 Configure Single Sign-On 6 Select appliance size		
7 Select datastore	Description:	
8 Configure database	This will deploy a Tiny VM config These resources will be used by	ured with 2 vCPUs and 8 GB of memory and requires 120 GB of disk space. the vCenter Server services.
9 Network Settings		
10 Ready to complete		
		Back Next Finish Cancel



Use the embedded database and configure the Network settings.

Mware vCenter Server Appliance Deployment					
 1 End User License Agreement 2 Connect to target server 	Choose a network:	VM Network 🔻	0	*	
 3 Set up virtual machine 4 Select deployment type 	IP address family:	IPv4 v]	l	
 5 Configure Single Sign-On 6 Select appliance size 	Network type:	static •]		
 7 Select datastore 8 Configure database 	Network address:	172.16.114.11]		
9 Network Settings 10 Ready to complete	System name [FQDN or IP address]:	172.16.114.11] 0		
	Subnet mask:	255.255.255.0]		
	Network gateway:	172.16.114.1]		
	Network DNS Servers (separated by commas)	8.8.8.8]		
	Configure time sync:	 Synchronize appliance time with ESX Use NTP servers (Separated by com 	Ki host mas)	l	
	I Enable ssh			-	
		Back	Next Finish Cancel]	

Figure 24 Network Settings

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

Mware vCenter Server Appliance Deployment			
 1 End User License Agreement 2 Connect to target server 	Ready to complete Please review your set	ings before starting the installation.	
 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 	Target server info: Name: Installation type: Deployment type: Deployment configuration: Datastore: Disk mode: Network mapping: IP allocation: Host Name Time synchronization: Database: Properties:	172.16.114.101 VIM vCenter Install vCenter Server Tiny (up to 10 hosts, 100 VMs) tempHD thick Network 1 to VM Network IPv4 , static Synchronize appliance time with ESXi host embedded SSH enabled = True SSO User name = administrator Single Sign-On instance IP = 172.16.114.10 SSO Domain name = vsphere.local Network 11P address = 172.16.114.11 Host Name = 172.16.114.11 Network 11P address = 172.16.114.11 Network 11 metmask = 255.255.255.0 Defaultgateway = 172.16.114.1 DNS = 8.8.88	
		Back	Next Finish Cancel

Figure 25 Complete installation

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

VMware vCenter Server Appliance Deployment	
Installation Complete	
Your vCenter Server is successfully installed.	
Post install steps:	
 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. 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: <u>https://172.16.114.11/vsphere-client</u> as administrator@vsphere.local	
	Close

Figure 26 vSphere web client URL

6.2.4 Deploy second EPSC and vCenter

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

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

Mware vCenter Server Appliance Deployment				
 I End User License Agreement 2 Connect to target server 3 Set up virtual machine 4 Select deployment type 	Ready to complete Please review your s Target server info: Name: Installation type:	ettings before starting the installation. 172.16.114.103 Compute EPSC Install		
 5 Set up Single Sign-on 6 Select appliance size 7 Select datastore 8 Network Settings 9 Ready to complete 	Deployment type: Datastore: Disk mode: Network mapping: IP allocation: Host Name Time synchronizatio	Platform Services Controller temp103 thick Network 1 to VM Network IPv4, static		
	Properties:	SSH enabled = True SSO User name = administrator SSO Domain name = vsphere.local SSO Site name = SantaClara Network 1 IP address = 172.16.114.12 Host Name = 172.16.114.12 Network 1 netmask = 255.255.0 Default gateway = 172.16.114.1 DNS = 8.8.8.8		
		Back	Next	Finish Cancel

Figure 27 EPSC configuration

Mware vCenter Server Appliance Deployment					
1 End User License Agreement	Ready to complete Please review your set	ings before starting the installation.			
 3 Set up virtual machine 4 Select deployment type 	Target server info: Name:	172.16.114.104 Compute vCenter			
✓ 5 Configure Single Sign-On	Deployment type: Deployment type: Deployment	Install vCenter Server Tiny (up to 10 hosts 100 VMs)			
 v o select appliance size v 7 Select datastore 	configuration: Datastore:	temp104			
 8 Configure database 9 Network Settings 	Disk mode: Network mapping: IP allocation:	thick Network 1 to VM Network IPv4_static			
10 Ready to complete	Host Name Time synchronization: Database: Properties:	Synchronize appliance time with ESXi host embedded SSH enabled = True SSO User name = administrator Single Sign-On instance IP = 172.16.114.12 SSO Domain name = vsphere.local Network 1IP address = 172.16.114.13 Host Name = 172.16.114.13 Network 1 netmask = 255.255.255.0 Default gateway = 172.16.114.1 DNS = 8.8.8.8			
		Back	Next	Finish	Cancel

Figure 28 Compute vCenter configuration

24 Dell EMC + VMware Cloud Infrastructure Platform for NFV VMware vCloud NFV 1.5 - NFVI Solution

6.3 Build datacenter

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

6.3.1 Add Licenses

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

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

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



Figure 29 Add license keys

Repeat this exercise for both VIM vCenter and Compute vCenter

6.3.2 Create datacenter and clusters

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

Navigato	r			Ŧ
Home				0
ŋ	B		Q	
v 🗗 172 .	16.105.21			
🗕 🖬 M	WC vCloud	I VIM		
Þ 🛙	I VIM			>
igure 30	MIV C			

²⁵ Dell EMC + VMware Cloud Infrastructure Platform for NFV VMware vCloud NFV 1.5 - NFVI Solution

Navigator				Ŧ
Administration			• 🔊	
		9		
- 🕝 172.16.105.23				
VWC POC				
👂 🙀 Compute				>
▶ 🗊 Edge				

Figure 31 Compute and Edge

6.3.3 Add Hosts to clusters

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

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

1 Add Host		(°)
1 Name and location	Enter the name or IP addres	s of the host to add to vCenter Server.
2 Connection settings	Host name or IP address:	172.16.105.12
3 Host summary	Location:	Compute
4 Ready to complete		



1 Add Host		• • •
 1 Name and location 2 Connection settings 3 Host summary 4 Ready to complete 	Enter the administrative account information for the host. The vSphere Web Client will use this information to and establish a permanent account for its operations. User name: root Password: ****	connect to the host



🔁 Add Host		(?)
✓ 1 Name and location	Name	172.16.105.12
 2 Connection settings 	Vendor	Dell Inc.
✓ 3 Host summary	Model	PowerEdge R730
4 Assign license	Version	VMware ESXi 5.5.0 build-2068190
5 Lockdown mode 6 Ready to complete	Virtual Machines	



📳 Add Host			? ₩
✓ 1 Name and location	Assign an existing license key 🔹		
 2 Connection settings 	License Key	Product	Usage
✓ 3 Host summary	🔘 🔑 (No License Key)	Evaluation Mode	0
✓ 4 Assign license		VMware vSphere 5 Enterprise Plus (unlimited cores per CPU)	14 CPUs
5 Lockdown mode			
6 Ready to complete			

Figure 35 Assign License

🕤 Add Host	() »
 1 Name and location 2 Connection settings 	When enabled, lockdown mode prevents remote users from logging directly into this host. The host will only be accessible through local console or an authorized centralized management application.
 ✓ 3 Host summary ✓ 4 Assign license 	If you are unsure what to do, leave this box unchecked. You can configure lockdown mode later by editing Security Profile in host settings.
✓ 5 Lockdown mode	Enable lockdown mode
6 Ready to complete	
Figure 36	Lockdown mode (Leave unchecked)

🕤 Add Host		(°))
 1 Name and location 	Name	172.16.105.12
 2 Connection settings 	Version	VMware ESXi 5.5.0 build-2068190
✓ 3 Host summary	License Key	
 4 Assign license 	Networks	VM Network
✓ 5 Lockdown mode	Datastores	vsanDatastore
6 Ready to complete	Lockdown Mode	Disabled
		Back Next Finish Cancel

Figure 37 Ready to complete

6.4 Configure host networking

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

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

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

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

6.4.1 Management Networking

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

6.4.1.1 Create DvSwitch

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

🏻 🏝 New Distributed Switch						? ₩
1 Name and location	Ready to complete Review your settings selections before	e finishing the wizard.				
 Z Select version 3 Edit settings 	No					
4 Ready to complete	Name: Version:	Management 6.0.0				
	Number of uplinks:	2				
	Network I/O Control:	Enabled				
	Default port group:	Mgmt DvSwitch PG				
	Suggested next actions New Distributed Port Group Add and Manage Hosts These actions will be available	e in the Actions menu of the new distr	ibuted switch.			
			Back	Next	Finish	Cancel

Figure 38 DvSwitch configuration

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

. 🔊 Management - Edit Settings		0
General Advanced	MTU (Bytes): Multicast filtering mode:	9000 + Basic +
	Discovery protocol	
	Туре:	Link Layer Discovery Protocol
	Operation:	Both ·

Figure 39 Change MTU and discovery protocol

6.4.1.2 Add first uplink port and VMkernel ports

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

Select new hosts			×
Incompatible Hosts		Q Filter	•)
Host	Host State	Cluster	
172.16.114.102	Connected	Management (VIM)	
172.16.114.103	Connected	Management (VIM)	
172.16.114.104	Connected	Management (VIM)	
A Find -		3 item	s
		OK Cancel	

Figure 40 Select the hosts in the VIM cluster

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

	A	dd and Manage Hosts						?		
~	1	Select task Select hosts	Manage physical network adapters Add or remove physical network adapters	anage physical network adapters Id or remove physical network adapters to this distributed switch.						
~	3	Select network adapter tasks	🖬 Assign uplink 🛛 Reset changes 🌘	🔒 View :	settings					
	4	Manage physical network adapters	Host/Physical Network Adapters	1 🛦	In Use by Switch	Uplink	Uplink Port Group			
	5	Manage VMkernel network adapters	 172.16.114.102 On this switch 					*		
	6	Analyze impact	对 vmnic3 (Assigned)		-	Uplink 2	Management-DVUplink			
	7	Ready to complete	- On other switches/unclaimed							
			ymnic0			-	-			
			💓 vmnic1			-				
			vmnic2		vSwitch0	-				
			对 vmnic4		Infrastructure	-	-			
			对 vmnic5		Infrastructure	-	-			
			💌 vmnic6			-	-			
			💌 vmnic7							

Figure 41 Manage physical network adapters

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

Manage VMkernel network adapters

Assign port group 🕂 New adapter	/ Edit	adapter 💥 Remove 🐚 R	leset changes 🚯 View sett	ings
Host/VMkernel Network Adapters	1 🔺	In Use by Switch	Source Port Group	Destination Port Group
				4
📷 vmk0 (Reassigned)		vSwitch0	Management Network	Mgmt DvSwitch PG

Figure 42 Manage VMkernal network adapters

Manage and assign VMkernel network adapters to the distributed switch.

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

44	쐂 🕼 🐢 🚯		(overview) 🔹 💐	. 🢁 🔍 C
Properties				
Topology	🚨 Mgmt DvSwitch PG 🛛 🚯	•	Management-DVUplinks-60	()
LACP	VLAN ID:		The Uplink 1 (0 NIC Adapters)	
Private VLAN	VMkernel Ports (3) vmk0 : 172 16 114 103		Uplink 2 (3 NIC Adapters)	
NetFlow	vmk0 : 172.16.114.102		vmnic3 172.16.114.102	6
Port mirroring	vmk0 : 172.16.114.104		vmnic3 172.16.114.103	6
Health check	Virtual Machines (0)	JD 4		
		\square		

Figure 43 Migrate to DvSwitch

6.4.1.3 Migrate VMs to DvSwitch

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

Add and Manage Hosts	
 ✓ 1 Selecttask ✓ 2 Select hosts 	Select network adapter tasks Select the network adapter tasks to perform.
 Select network adapter tasks Migrate VM networking Ready to complete 	 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

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

Add and Manage Hosts					?		
1 Select task 2 Select hosts	Migrate VM networking Select virtual machines or network adapters i	to migra	te to the distributed sw	ritch.			
3 Select network adapter tasks 4 Migrate VM networking	Assign VMs or network adapters to a destination port group to migrate them. Press and hold down the CTRL key, and then click the VMs to select multiple items.						
5 Ready to complete	🚨 Assign portgroup 🛛 😭 Reset changes 👔	🚹 View	settings				
	Host/Virtual Machine/Network Adapter	1 🔺	NIC Count	Source Port Group	Destination Port Group		
	▼ 172.16.114.102						
	🕨 🚰 Compute EPSC		1				
	🕨 🖶 NSX Manager		1				
	- 172.16.114.103						
	🕨 🚰 Compute vCenter		1				
	▶ 🔂 VIM EPSC		1				
	172.16.114.104						
	VIM vCenter		1				
	 Add and Manage Hosts 1 Select task 2 Select hosts 3 Select network adapter tasks 4 Mgrate VM networking 5 Ready to complete 	Add and Manage Hosts 1 Select task 2 Select hosts 3 Select network adapter tasks 4 Migrate VM networking 5 Ready to complete • ② 172.16.114.102 • ③ 172.16.114.103 • ③ 172.16.114.103 • ③ 172.16.114.104 • ⑤ VIM vCenter • ③ 172.16.114.104 • ⑤ VIM vCenter • ⑥ VIM vCenter • ⑧ VIM vCenter • ⑨ VI	Add and Manage Hosts 1 Select task 2 Select hosts 3 Select network adapter tasks 4 Migrate VM networking 5 Ready to complete • ② Assign port group • ③ Reset changes • View HestVirtual Machine/Network Adapter 1 • ③ Compute EPSC • ③ NSX Manager • ③ 172.16.114.103 • ③ Compute VCenter • ③ VIM EPSC • ③ 172.16.114.104 • ④ VIM vCenter • ⑤ VIM vCenter • ⑥ VIM vCenter • ⑥ VIM vCenter • ⑥ VIM vCenter • ⑧ VIM vCenter • ⑧ VIM vCenter • ◎ V	Add and Manage Hosts 1 Select task 2 Select hosts 3 Select network adapter tasks 4 Migrate VM networking 5 Ready to complete • ② 172.16.114.102 • ③ 172.16.114.103 • ③ 172.16.114.103 • ③ 172.16.114.104 • ⑤ VIM EPSC 1 • ⑤ VIM EPSC 1 • ⑤ VIM VCenter 1 • ⑤ VIM vCenter 1 • ⑥ • Ø VIM vCenter 1 • ◎ VIM vCenter • ◎ VIM vCenter 1 • ◎ VIM vCenter • ◎ VIM vCenter	Add and Manage Hosts 1 Select task Mgrate VM networking Select virtual machines or network adapters to migrate to the distributed switch. 3 Select network adapter tasks Assign VMs or network adapters to a destination port group to migrate them. Press and hold down the VMs to select multiple items. 5 Ready to complete Assign port group Image Reset changes Image VMs wettings Host/Virtual Machine/Network Adapter 1 MIC Count Source Port Group Image Compute EPSC 1 Image Compute EPSC 1 Image Compute VCenter 1 Image Compute VCenter 1 Image Compute VCenter 1 Image Compute Compute VCenter 1 Image Compute VCenter 1 Image Compute		



6.4.2 Migrate the second uplink port to DvSwitch

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

Manage physical network adapters Add or remove physical network adapters to this distributed switch.					
💼 Assign uplink 🏾 🗙 Unassign adapi	ter 🕐 Re	set changes 🚯 Vi	ew settings		
Host/Physical Network Adapters	1 🔺	In Use by Switch	Uplink	Uplink Port Group	
▼ 172.16.114.102					*
✓ On this switch					
🗾 vmnic2 (Assigned)		vSwitch0	Uplink 1	Management-DVUplink	
vmnic3		Management	Uplink 2	Management-DVUplink	

Figure 46 Manage physical network adapters

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

→ Management Actions →	Ξ×.
Getting Started Summary Mo	onitor Manage Related Objects
Settings Alarm Definitions Tag	gs Permissions Network Protocol Profiles Ports Resource Allocation
••	🖄 🕼 🐢 🕄 (overview) 🔹 🔍 📿
Properties	
Topology	🚨 Mgmt DvSwitch PG 🚯 🍖 🔽 Management-DVUplinks-60 🚯
LACP	VLAN ID: v 🖬 Uplink 1 (3 NIC Adapters)
Private VLAN	▼ VMkernel Ports (3)
NetFlow	vmk0 : 172.16.114.103 (1) - vmnic2 172.16.114.104 (1)
Port mirroring	vmik0 : 172 16 114 102
Portinitoring	Virtual Machines (5)
Неалл спеск	VIM EPSC
	Compute EPSC 👂 🚯 🕞 🚺 👘 vmnic3 172.16.114.103 🚯
	NSX Manager 👂 🚯 🕂 🖸
	Compute vCenter
	VIM vCenter

Figure 47 Host Management Networking configuration

6.4.2.1 Management DvSwitch for Compute vCenter

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



Figure 48 Management DvSwitch

🚨 Mgmt DvSwitch PG	6	Management-DVUplinks-21	6
VLAN ID:		🔻 🛅 Uplink 1 (8 NIC Adapters)	
▼ VMkernel Ports (8)		vmnic2 172.16.114.112	6
vmk0 : 172.16.114.112		vmnic2 172.16.114.105	6
vmk0: 172.16.114.105		vmnic2 172.16.114.111	6
vmk0 : 172.16.114.108		vmnic2 172.16.114.108	6
vmk0 : 172.16.114.111		vmnic2 172.16.114.110	6
vmk0 : 172.16.114.110		vmnic2 172.16.114.106	6
vmk0: 172.16.114.107		vmnic2 172.16.114.107	6
vmk0: 172.16.114.106		vmnic2 172.16.114.109	6
vmk0 : 172.16.114.109		v 📷 Uplink 2 (8 NIC Adapters)	
Virtual Machines (0)		vmnic3 172.16.114.112	6
		vmnic3 172.16.114.105	6
		vmnic3 172.16.114.111	6
		vmnic3 172.16.114.108	6
		vmnic3 172.16.114.110	6
		vmnic3 172.16.114.106	6
		vmnic3 172.16.114.107	6
		vmnic3 172.16.114.109	6

Figure 49 Management DvSwitch

6.4.3 Infrastructure Networking

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

6.4.3.1 Create a DvSwitch

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

🄚 New Distributed Switch			(?) ₩	
 1 Name and location 2 Select version 	Ready to complete Review your settings selections before finishing the wizard.			
✓ 3 Edit settings	Name:	Compute Infrastructure		
4 Ready to complete	Version:	6.0.0		
	Number of uplinks:	2		
	Network I/O Control:	Enabled		
	Suggested next actions			
	New Distributed Port Group			
	😡 Add and Manage Hosts			
	These actions will be available in the Actions menu of the new distributed switch.			

Figure 50 DvSwitch configuration

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

😡 Compute Infrastructure - Edit S	ettings		?
General Advanced	MTU (Bytes): Multicast filtering mode:	9000 • Basic •	
	Discovery protocol		
	Type:	Link Layer Discovery Protocol	
	Operation:	Both 🔹	

Figure 51 MTU and Discovery protocol

6.4.3.2 Add the necessary infrastructure port groups

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

2 New Distributed Port Group					
 1 Select name and location 2 Configure settings 	Ready to complete Review the changes before proceeding.				
3 Ready to complete	Distributed port group name: Port binding: Number of ports: Port allocation: Network resource pool: VLAN ID:	Compute VSAN PG Static binding 8 Elastic (default) 1000			

Figure 52 Compute VSAN PG port-group

😫 New Distributed Port Group					
1 Select name and location Ready to complete Design the shares a before second integration					
✓ 2 Configure settings	Review the changes before proceeding.				
3 Ready to complete	Distributed port group name:	Compute vMotionPG			
	Port binding:	Static binding			
	Number of ports:	8			
	Port allocation:	Elastic			
	Network resource pool:	(default)			
	VLAN ID:	1001			

Figure 53 Compute vMotionPG port-group

2	Level 2018 New Distributed Port Group						
~	1 Select name and location	Ready to complete					
~	2 Configure settings						
	3 Ready to complete	Distributed port group name:	Compute Replication PG				
		Port binding:	Static binding				
		Number of ports:	8				
		Port allocation:	Elastic				
		Network resource pool:	(default)				
		VLAN ID:	1002				



6.4.3.3 Configure LACP in the uplink ports

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

New Link Aggregation Group	(?
Name: Number of ports: Mode: Load balancing mode:	Iacp1 2 Active Source and destination IP address, TCP/UDP port and VLAN
Port policies	
You can apply VLAN and NetF Unless overridden, the policie	Tow policies on individual LAGs within the same uplink port group. es defined at uplink port group level will be applied.
VLAN type:	Override VLAN trunking 🔹
VLAN trunk range:	0-4094
NetFlow:	Override Disabled -
	OK Cancel

Figure 55 Create a new link aggregation group

Settings	Alarm Definitions	Tags	Permissions	Network Pro	tocol Profiles	Ports	Resource Allocation		
••		L	АСР						
Topol Prope	ogy rties		The enhanced L using dynamic I	.ACP support ink aggregati	on a vSphere on.	distribut	ied switch lets you con	nect ESXi hosts to physical switches by	?
LACP			Migrating netw	ork traffic to	LAGs				
Private VLAN			+					Q Filter	•
NetFlo	W		LAG Name	Number of P	Mode	VLAN			
Port n	nirroring		lacp1	2	Active	Inherite	d from uplink port grou	р	
Health	i check								

Figure 56 LACP settings

6.4.3.4 Add host uplink ports to DvSwitch

Click on Actions \rightarrow Add and Manage Hosts. Select all the hosts in the given cluster.

Select new hosts		۲
Incompatible Hosts		Q Filter -
V Host	Host State	Cluster
172.16.114.105	Connected	Compute
172.16.114.106	Connected	🗊 Compute
172.16.114.107	Connected	Compute
7 3 172.16.114.108	Connected	🗊 Compute
172.16.114.109	Connected	🗊 Edge
172.16.114.110	Connected	🗊 Edge
172.16.114.111	Connected	🗊 Edge
172.16.114.112	Connected	🗊 Edge
M Q Find -		8 items
		OK Cancel

Figure 57 Add host uplink ports to DvSwitch

In each host, select the two 10G uplink ports allocated for Infrastructure as uplink ports to be part of LACP channel members.
1	Add and Manage Hosts						
	Select task 2. Select hosts	Manage physical network adapters Add or remove physical network adapter	ange physical network adapters dd or remove physical network adapters to this distributed switch.				
~ :	 3 Select network adapter tasks Assign uplink Reset changes (1) View settings 						
~ [adapters	Host/Physical Network Adapters 1	In Use by Switch	Uplink	Uplink Port Group		
5	Manage VMkernel network				*		
	adapters	✓ On this switch					
6	Analyze impact	vmnic4 (Assigned)		lag1-0	Compute Infrastr-DVUplin		
7	Ready to complete	vmnic5 (Assigned)		lag1-1	Compute Infrastr-DVUplin		
		✓ On other switches/unclaimed					
		vmnic0			-		
		vmnic1			-		
		vmnic2	Management		-		
		vmnic3	Management		-		
		vmnic6					
		对 vmnic7			-		

Figure 58 Manage physical network adapters

6.4.3.5 Add VMKernel adapter for each of the services

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

3 172.16.114.105 - Add Networking						
 1 Select target device 2 Connection settings 	Ready to complete Review your settings selections before finishing the wizard.					
✓ 2a Port properties	Distributed port group:	Compute VSAN PG				
✓ 2b IPv4 settings	Distributed switch:	Compute Infrastructure				
3 Ready to complete	TCP/IP stack:	Default				
	vMotion traffic:	Disabled				
	Provisioning traffic:	Disabled				
	Fault Tolerance logging:	Disabled				
	Management traffic:	Disabled				
	vSphere Replication traffic:	Disabled				
	vSphere Replication NFC traffic:	Disabled				
	Virtual SAN traffic:	Enabled				
	IPv4 settings					
	IPv4 address:	172.17.0.105 (static)				
	Subnet mask:	255.255.255.0				



172.16.114.105 - Add Networking	🔋 172.16.114.105 - Add Networking				
 1 Select target device 2 Connection settings 	Ready to complete Review your settings selections before finishing the wizard.				
✓ 2a Port properties	Distributed port group:	Compute vMotion PG			
✓ 2b IPv4 settings	Distributed switch:	Compute Infrastructure			
3 Ready to complete	TCP/IP stack: Whotion traffic: Provisioning traffic: Fault Tolerance logging: Management traffic: vSphere Replication traffic: vSphere Replication NFC traffic: Virtual SAN traffic: IPv4 settings	Default Enabled Enabled Disabled Disabled Disabled Disabled Disabled			
	Subnet mask:	255.255.255.0			

Figure 60 Compute vMotion PG port-group

37 Dell EMC + VMware Cloud Infrastructure Platform for NFV VMware vCloud NFV 1.5 - NFVI Solution

172.16.114.106 - Add Networking	172.16.114.106 - Add Networking				
 1 Select target device 2 Connection settings 	Ready to complete Review your settings selections before finishing the wizard.				
 ✓ 2a Port properties 	Distributed port group:	Compute Replication PG			
 2b IPv4 settings 	Distributed switch:	Compute Infrastructure			
3 Ready to complete	TCP/IP stack:	Default			
	vMotion traffic:	Disabled			
	Provisioning traffic:	Disabled			
	Fault Tolerance logging:	Disabled			
	Management traffic:	Disabled			
	vSphere Replication traffic:	Enabled			
	vSphere Replication NFC traffic:	Enabled			
	Virtual SAN traffic:	Disabled			
	IPv4 settings				
	IPv4 address:	172.17.2.106 (static)			
	Subnet mask:	255.255.255.0			



Manage VMkernel network adapters Manage and assign VMkernel network adapters to the distributed switch.					
🙎 Assign port group 斗 New adapter 🍐	🖉 Edit adapter 🗙 Remove 👩	Reset changes 🚯 View s	ettings		
Host/VMkernel Network Adapters	1 🛦 In Use by Switch	Source Port Group	Destination Port Group		
			A		
📷 vmk1 (new)	Compute Infrastructure		Compute VSAN PG		
🗾 vmk2 (new)	Compute Infrastructure		Compute vMotion PG		
📷 vmk3 (new)	Compute Infrastructure		Compute Replication PG		
📷 vm k0	Management	Mgmt DvSwitch PG	Do not migrate		

Figure 62 Assign VMkernel network adapters

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

🕼 Add and Manage Hosts	Add and Manage Hosts (?)		
✓ 1 Select task	Ready to complete		
✓ 2 Select hosts	Review your settings selections before infisting the wizard.	-	
✓ 3 Select network adapter tasks	Number of managed hosts		
✓ 4 Manage physical network adapters	Hosts to add: 4		
✓ 5 Manage VMkernel network	Number of network adapters for update		
adapters	Physical network adapters: 8		
 6 Analyze impact 	New VMkernel network adapters: 12		
7 Ready to complete			

Figure 63 Ready to complete

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

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



Figure 64 Migrating Network Traffic to LAGs

Choose to configure teaming and failover checkboxes.

🍰 Compute Infrastructure - Manag	e Distributed Port Groups				(?) H
 1 Select port group policies 2 Select port groups 3 Configure policies 	Select port groups Select the port groups on this dis	tributed switch that y	ou want to edit.		
3a Teaming and failover	Name	Status	Port Binding	VMs	Å.
4 Ready to complete	🚨 Compute VSAN PG	Normal	Static binding		
	2 Compute vMotion PG	 Normal 	Static binding		
	🚨 Compute Replication PG	Normal	Static binding		

Figure 65 Configure teaming and failover



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

Figure 66 Configure teaming and failover

39 Dell EMC + VMware Cloud Infrastructure Platform for NFV VMware vCloud NFV 1.5 - NFVI Solution A fully configured DvSwitch will look like the screenshot shown below. This image shows the Compute cluster, make sure to repeat this process in each cluster (Edge and VIM).



Figure 67 Fully configured DvSwitch

6.4.4 VxLAN Data Networking

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



Figure 68 VxLAN Data Networking

6.5 Enable VSAN

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

6.5.1 Enable VSAN in cluster

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

Compute - Edit Virtual SAN Settings					
Turn ON Virtual SAN					
Add disks to storage	Manual Requires manual claiming of any new disks on the included hosts to the shared storage.	ł			
	OK Cance				

Figure 69 Add disks to storage

6.5.2 Assign VSAN license key to cluster

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

Compute - Assign Li	icense Key						
Assign an existing licer	nse key 🛛 🔻						
License Key		Product	Usage	Capacity	Label	Expires	
🔵 🔑 (No License K	ey)	Evaluation Mode	4	Unlimited		2/1/2016	
. 🤌 💶		Virtual SAN 5.5	8 CPUs	16 CPUs	VSAN	11/2/2016	
License Key: 6400M-T7LD0-K8U71-03CKM-2H72J Product: Virtual SAN 5.5							
apacity / Available:	16 CPUs / 8 CPUs						
abel:	VSAN						
							OK Cance

Figure 70 Assign License Key

6.5.3 Claim the hard disks for VSAN

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

172.16.105.12 - Create Disk Group

First, select a single SSD disk to serve as a write cache and read buffer.

				Q Filter		-
Name	Drive Type	Capacity	Transport Type			
Isso Local ATA Disk (naa.55cd2e404c044c17)	SSD	186.31 GB	Parallel SCSI			
A4.					1 items	- -

Then, select one or many disks to serve as data disks.

					Q Filter 🔹
	Name	Drive Type	Capacity	Transport Type	
\checkmark	Local DELL Disk (naa.644a84202ec97f001cf7	Non-SSD	558.38 GB	Parallel SCSI	
M					1 items 📑 👻
					OK Cancel

Figure 71 Create Disk Group

6.6 Install NSX

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

6.6.1 Deploy NSX manager

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

?

Deploy OVF Template		(3) **					
1 Source ✓ 1a Select source	Review details Verify the OVF template	details					
1b Review details 1c Accept EULAs	The OVF package options below an	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.					
2 Destination	🖌 Accept extra confi	guration options					
2a Select name and folder	Product	NSX Manager					
2b Select storage	Version	6.2.0-2986609					
2c Setup networks	Vendor	VMware, Inc.					
2 d Customize template	Publisher	VMware, Inc. (Trusted certificate)					
5 Ready to complete	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 v					
	Extra configuration	vshield.vmtype = Manager vshield.vmtversion = 6.2.0 vshield.vmtbuild = 2986609 keyboard.typematicMinDelay = 2000000					
		Back Next Finish Cancel					

Figure 72 OVF template details

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

Dep	Deploy OVF Template (?) >>							
~	Source Setup networks 1 a Select source Configure the networks the deployed template should use							
~	1b Review details	Source	Destination	Configuration				
~	1c Accept EULAs	VSMgmt	VM Network	o				
	2 Destination		VM Network					
~	2a Select name and folder		VSAN VIM PG					
~	2b Select storage							
~	2c Setup networks	IP protocol: IPv4	IP allocation: Static - Manual					
	2d Customize template							
	3 Ready to complete	Source: VSMgmt - Description This network provides connectivity to this v	irtual machine.					

Figure 73 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 74 Configure username and password

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

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 75 Network Properties

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

6.6.2 Register NSX manager with vCenter

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

Show next... Collapse all...

NSX Manager Virtual Appliance Management

View Summary	Download Tech Support Log
Manage Appliance Settings	Backup & Restore
Manage vCenter Registration	Upgrade



Click vCenter server **Edit** button and provide 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 hos CPU and memory reservation vCenter on NSX Manager, y Client and log back in to ena	ted by a vCenter Server Appliance, please ensure that appropriate on is given to this appliance VM. After successful configuration of you need to log out of any active client sessions on vSphere Web able NSX user interface components.							
vCenter Server:	172.16.105.20							
vCenter User Name:	administrator@vsphere.local							
Password:	Password:							
Modify plugin script download location								
	OK Canc	el						

Figure 77 vCenter Server

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

Home							
Inventories							
6		B		Q		0	<mark>바</mark> 아이
vCenter	Hosts and Clusters	VMs and Templates	Storage	Networking	Hybrid Cloud	vCenter Orchestrator	Networking & Security

Figure 78 VMware vSphere web client

46 Dell EMC + VMware Cloud Infrastructure Platform for NFV VMware vCloud NFV 1.5 - NFVI Solution

6.6.3 Deploy NSX controllers

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

Add Static IP Pool								
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							
	OK Cancel							

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

Figure 79 NSX controller IP address pool

Add Controller				?
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 Chan	ge	Remove
IP Pool:	*	Controllers		Select
Password:	*	*****		
Confirm password:	*	****		
		ОК		Cancel
Figure 80 Add Conti	rol	ler		

47 Dell EMC + VMware Cloud Infrastructure Platform for NFV VMware vCloud NFV 1.5 - NFVI Solution

NSX Controller nodes								
🕂 🗶 🔄 🍪 🎆 Actions 🔍 🔍								
Controller IP Address ID		Status	Software Version	NSX Manager				
172.16.105.31	controller-1	🛟 Deploying	6.2.44780	172.16.105.21				
Figure 81 NSX Controller Nodes								

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

NSX Controller nodes								
🔶 🗙 🛅 🇞 🎲 Actions 🔍 🔍								
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 82 Three NSX controllers

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

6.6.4 Exclude VMs from Firewall

It is recommended that the vCenter VM be excluded from the firewall protection. To do this, navigate from Home \rightarrow Networking & Security \rightarrow NSX Managers \rightarrow Manage \rightarrow Exclusion list. Click on the (+) symbol and add the vCenter VM in 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.							
Q Filter				Q Filter	•		
Available Objects		Selected	l Objects				
✓ 🗗 vCenter_5.5		🗸 🖗	vCenter_5.5				
1 itoms					1 itome		
Titems					T Items		
				ОК	Cancel		

Figure 83 Exclude vCenter VM from firewall protection

6.6.5 Install NSX Kernel Modules

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

NSX Component Installation on Hosts								
log Actions								
Install	Installation Status	Firewall	VXLAN					
Compute	✔ 6.2.0	✓ Enabled	Not Configured					
▶ 🛱 VIM Not Installed Not Configured Not Configured								

Figure 84 NSX Kernel Modules

6.6.6 Configure VxLAN

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

Compute - Configure VXL	N Networking	(?) ₩
Switch:	Compute VxLAN	•
VLAN:	0	
MTU:	9000	
VMKNic IP Addressing:	Use DHCP	
	Use IP Pool VXLAN VTE	· •
VMKNic Teaming Policy:	Enhanced LACP	•
VTEP:	1	
	ОК	Cancel

Figure 85 Configure VXLAN Networking

Installation							
Management Host Prepa	Logical Network Preparation	Service Deployments					
15X Manager 172 16:114	16 🔻						
VXLAN Transport Segme	nt ID Transport Zones						
Clusters & Hosts	Configuration Status	Switch	VLAN	MTU	VMRNic IP Addressing	Teaming Policy	VTEP
▼ [A]Edge	🖌 Unconfigure	Edge VxLAN	0	9000	IP Pool	Enhanced LACP	4
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		
/ I削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		
172.16.114.105	🖌 Ready				vmk4: 172.17.3.107		

Figure 86 VXLAN IP addresses

6.6.7 Assign segment ID

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

Edit Segment IDs and Multicast Address Allocation						
Provide a Segment ID ;	oool and Multicast range unique to this NSX Manager.					
Segment ID pool: * 5000-6000						
	(In the range of 5000-16777215)					
Enable Multicast ad	dressing					
Multicast addresses are	e required only for Hybrid and Multicast control plane modes.					
	OK Cance	<u>ال</u>				

Figure 87 Segment IDs

6.6.8 Add a Transport Zone

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

New 1	Fransport Zon	e		Ċ	2)))
					_
Name	:	VxLAN Transport Zone	3		
Descri	iption:				
Replic	ation mode:	 Multicast 			1
		Multicast on Physica	I network used for VXLAN control pla	ine.	
		 Unicast 			
		VXLAN control plan	e handled by NSX Controller Cluster		
		 Hybrid 			
		Optimized Unicast r	node. Offloads local traffic replication	to physical network.	
Select clu	usters that will	be part of the Transport	Zone		
	Name		NSX vSwitch	Status	
\checkmark	D Compute	•	WXLAN DataSwitch	📀 Normal	
	🗊 VIM		C VxLAN DataSwitch	📀 Normal	
				OK Canc	el

Figure 88 VxLAN Transport Zone

6.6.9 Create logical switch

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

MWC EPC Demo DC	Top Level Objects Hos	ts Virtual Machines	vApps [Datastores	Datastore Clu	usters Networks	Distributed Switche	s	
		- G 🗛 🔞 🚳	Actions 👻				 	🕻 🔍 Filter	•
172.16.105.13	Name	1 🔺	State	Stat	tus	Provisioned Space	Used Space	Host CPU	Host Mem
172.16.105.14	WinClone		Powered (On 🥑	Normal	24.11 GB	6.92 GB	0 MHz	1,849 MB
172.16.105.15	Windows		Powered (On 🥑	Normal	20.11 GB	6.94 GB	0 MHz	2,966 MB
Windows									
Eiguro 90) Virtual Maa	hinon							

Figure 89 Virtual Machines

Navigate to Home \rightarrow Networking & Security \rightarrow 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 Switc	h	? »
Name:	* WinNet	
Description:		
Transport Zone:	* VxLAN Transport Zone	Change Remove
Replication mode:	Multicast	
	Multicast on Physical network used for VXLAN control pla	ane.
	 Unicast 	
	VXLAN control plane handled by NSX Controller Cluster	-
	O Hybrid	
	Optimized Unicast mode. Offloads local traffic replication	n to physical network.
Enable IP Disco	very	
🖌 Enable MAC Lea	rning	
		OK Cancel

Figure 90 Create a new logical switch

NSX Manager: 172.16.105.21								
+ ∕ × 1 🖗 🗞 🎞 @ Actions -								
Name 1	Status	Transport Zone	Scope	Segment ID	Control Plane Mode	Description	Tenant	
n CloneNet	 Normal 	VxLAN Transport Zone	Global	5001	Unicast		virtual wire tenant	
🛬 WinNet	 Normal 	VxLAN Transport Zone	Global	5000	Unicast		virtual wire tenant	

Figure 91 Transport zone

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 Provide the selection of the								
	Name	Network	Host					
	🛤 WinClone	WinClone - Network adapter 1 (CloneNet)	172.16.105.15					

Figure 92 Virtual machine configuration

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



Figure 93 vSwitch port-group

6.6.10 Deploy and configure Distributed Logical Router

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

N	ew NSX	Edge			?	••
~	1 Nan	ne and description	Name and des	scription		
~	2 Set	tings	Install Type:			-
	3 Con	nfigure deployment	motan rype.	Provides common gateway services such as DHCP, Firewall,		
	4 Con	nfigure interfaces		VPN, NAT, Routing and Load Balancing.		
5 Default gateway settings			● Logical (Distributed) Router			
	6 Rea	idy to complete		Provides Distributed Routing and Bridging capabilities.		
			Name:	* DLR		
			Hostname:	DLR		
			Description:			
			Tenant:			
			🖌 Deploy Ed	lge Appliance		
			Deploys NSX	Edge Appliance to support Firewall and Dynamic routing.		
			Enable Hig	gh Availability		
			Enable HA, fo	or enabling and configuring High Availability.		

Figure 94 Create Distributed logical routers

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

Ne	ew NSX Edge		? ₩
~	1 Name and description	Settings	
~	2 Settings		
~	3 Configure deployment	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	
	4 Configure interfaces	User Name: * admin	
	5 Default gateway settings	Password **********	
	6 Ready to complete	Confirm password: *	
		✓ Enable SSH access	
		Edge Control Level Logging EMERGENCY 🔹	
		Set the Edge Control Level Logging	

Figure 95 Distributed logical router settings

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

Ne	New NSX Edge 📀 🕨							
~	I Name and description Configure deployment							
~	2 Settings	Datacapter: *						
~	3 Configure deployment	NSX Edge Appliances						
	4 Configure interfaces							
	5 Default gateway settings							
	6 Ready to complete	Resource Pool	Host	Datastore	Folder			
		VIM	172.16.105.10	datastore_10	Discovered virtu			
		Specifying a resour Edge appliance. Ap Edge Appliance.	ce pool and datastor pliance configuratior	e is mandatory for co i is mandatory if you	onfiguring the NSX want to deploy NSX			

Figure 96 Configure deployment

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

Ne	New NSX Edge (?)>							
~	1 Name and description Configure interfaces							
~	2 Settings	UA Interface Confi	HA Interface Configuration					
~	3 Configure deployment	Connected To:						
	4 Configure interfaces	Connected 10.						
	5 Default gateway settings	Configure interface	es of this NSX Edge	•				
	6 Ready to complete	🕈 / 🗙						
		Name	IP Address	Subnet Prefix Length	Connected To			
		WinNet	192.168.1.250*	24	WinNet			
		CloneNet	192.168.2.250*	24	CloneNet			

Figure 97 Configure interfaces

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

6.6.11 Deploy Edge services gateway

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

6.6.11.1 Create a logical switch

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

没 Edit		? »
Name:	* DLR-ESG Network	
Description:	192.168.100.0/24	
Replication mode:	O Multicast	
	Multicast on Physical network used for VXLAN control plane.	
	 Unicast 	
	VXLAN control plane handled by NSX Controller Cluster.	
	O Hybrid	
	Optimized Unicast mode. Offloads local traffic replication to physical networ	k.
🖌 Enable IP Disco	very	
Enable MAC Lea	rning	
	OK Can	cel

Figure 98 Create logical switch

6.6.11.2 Create a distributed switch

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



6.6.11.3 Create uplink port in DLR

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

Edit Logical Router Inte	erface					?
Name: * Type: Connected To: Connectivity Status: Configure Subnets:	DLR ESG link Internal DLR-ESG Netw OConnected	Uplink vork Dis	sconnected		Change	Remove
🔶 🥖 🗙			Subast Profix Logath	Q Filter		
192.168.100.1			24	1		
MTU:	1500					
					ок	Cancel

Figure 100 Edit logical router interface

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

Edit Default Gatewa	У	?
Interface:	DLR ESG link	· ·)
Gateway IP:	* 192.168.100.250	
MTU:	* 1500	
Admin Distance:	* 1	
Description:		
		OK Cancel

Figure 101 Edit the default gateway

6.6.11.4 Add an ESG

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

New NSX Edge		? ₩
1 Name and description	Name and description	
✓ 2 Settings		
3 Configure deployment	Install Type: (•) Edge Services Gateway	
4 Configure interfaces	Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.	
5 Default gateway settings	 Logical (Distributed) Router 	
6 Firewall and HA	Provides Distributed Routing and Bridging capabilities.	
7 Ready to complete	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 102 Deploy ESG

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

Nev	/ NSX Edge				?
~	1 Name and description	Configure deployme	nt		
~	2 Settings	(
	3 Configure deployment	Datacenter: *	MWC EPC Demo D	C •	
	4 Configure interfaces	Appliance Size: (Compact 		
	5 Default gateway settings	(X-Large		
(6 Firewall and HA	(Quad Large		
	7 Ready to complete	NSX Edge Applianc	es		
		+ / ×			
		Resource Pool	Host	Datastore	Folder
		VIM	172.16.105.10	datastore_10	Discovered virtu



Configure the internal and uplink interfaces for the ESG.

Add NSX Edge Interfac	:e	(1
vNIC#:	0	
Name:	* DLR ESG link	
Type:	Internal O Uplink	
Connected To:	DLR-ESG Network	Change Remove
Connectivity Status:	Connected Disconnected	
+ / ×	Q F	ilter
Primary IP Address	Secondary IP Address S	ubnet Prefix Length
192.168.100.250	2	4 😒
MAC Addresses:		
	You can specify a MAC address or leave it blank for auto ge two different MAC addresses are required.	neration. In case of HA,
MTU:	1500	
Options:	Enable Proxy ARP Send ICMP Redirect	
	Reverse Path Filter Enabled 🔹	
Fence Parameters:		
	Example: ethernet0.filter1.param1=1	
		OK Cancel

Figure 104 Add NSX interface - internal

Add NSX Edge Interfac	e		?
VNIC#:	1		
Name:	* To DvSwitch]
Type:	O Internal O Uplink		
Connected To:	Edge gateway PG	Change Remove	
Connectivity Status:	Connected Disconnected		
+ / ×	Q Fil	Iter	
Primary IP Address	Secondary IP Address Su	ibnet Prefix Length	
172.16.106.10	8		
MAC Addresses: MTU: Options: Fence Parameters:	You can specify a MAC address or leave it blank for auto ger two different MAC addresses are required. 1500 C Enable Proxy ARP Send ICMP Redirect Reverse Path Filter Enabled • Example: ethernet0.filter1.param1=1	neration. In case of HA,]
	(OK Cance	

Figure 105 Add NSX interface - uplink

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

New NSX Edge		(?) >>
 1 Name and description 	Default gateway settings	
✓ 2 Settings	Carefornia Default Colonia	
✓ 3 Configure deployment	Configure Default Gateway	
✓ 4 Configure interfaces	vNIC: * To DvSwitch	
✓ 5 Default gateway settings	Gateway IP: * 172.16.106.1	
 6 Firewall and HA 	MTU: 1500	
7 Ready to complete		

Figure 106 Default gateway settings

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

New NSX Edge			(?) H
 1 Name and description 	Firewall and HA	ß	
✓ 2 Settings		d de la companya de l	
 3 Configure deployment 	Configure Firewall	default policy	
 4 Configure interfaces 	Default Traffic Policy:	Accept Deny	
✓ 5 Default gateway settings	Logging:	O Enable O Disable	
6 Firewall and HA	Configure IIA naroma	lara	

Figure 107 Configure firewall policy

Review the configured options and click Finish.

New NSX Edge						(?)
✓ 1 Name and description	Ready to comple	ete				
✓ 2 Settings	Name and desc	ription				
✓ 3 Configure deployment	Name:	E	SG-1			
✓ 4 Configure interfaces	Install Type:	E	Edge Serv	ices Gat	eway	
✓ 5 Default gateway settings	Tenant:					
✓ 6 Firewall and HA	Size:	(Compact			
7 Ready to complete	HA:	[Disabled			
	Automatic Rule Generation: Enabled					
	NSX Edge Applia	ances				
	Resource Pool			Host		
	VIM			172.16	.105.10	
	Interfaces					
	vNIC#	Name	IP Addre	55	Subnet Prefix Length	Connected To
	0	DLR ESG link	192.168	8.100.25	24	DLR-ESG Net
	1	To DvSwitch	172.16.	106.10*	24	Edge gateway
			Back	Ne	ext Fini	ish Cancel

Figure 108 NSX configuration

6.6.12 Configure OSPF on DLR

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

Edit Dynamic R	outing Configuration	?
Router ID : *	DLR ESG link - 192	
Log Level .	OK Cance	el

Figure 109 Edit DLR configuration

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

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.)	
OK Can	cel

Figure 110 OSPF configuration

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

New Area Definition		?
Area ID : * Type : Authentication : Value :	0 Normal None	
	OK Cance	<u>ال</u>

Figure 111 Area definition

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

New Area to Interfa	ce Mapping	?
Interface : DL Area : * 0	R ESG link -	ing
- Advanced		
Hello Interval *	10	(seconds)
Dead Interval *	40	(seconds)
Priority *	128]
Cost*	1	
	ОК	Cancel

Figure 112 Area interface mapping

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

4	OSPF Configuration	on :				Edit	Delete
Global Configuration	Status :	√ E	nabled				
OSPF	Protocol Address	s: 192.1	168.100.100				
BGP	Forwarding Addr	ess: 192.1	168.100.1				
Route Redistribution	Graceful Restart	: 🗸 E	nabled				
	Default Originate	: ⊘ D	isabled				
	Area Definitions :						
	🕈 🥖 🗙					Q Filter	
	Area ID		Туре		Authentics	ation	
	0		Normal		None		
							1 item
	Area to Interface I	Mapping :					
	🕈 🥖 🗙					Q Filter	
	Interface	Area ID	Hello Interval (sec	Dead Interval (sec	Priority	Cost	
	DLR ESG link	0	10	40	128	1	

Figure 113 OSPF configuration

6.6.13 Route redistribution and firewall configuration

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

Route Redistributi	on table :		
+ / x ==	4		Q Filter 🔸
Learner	From	Prefix	Action
OSPF	Connected	Any	Permit

Figure 114 Route redistribution

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

⊘ 3	ssh	User	any	聞Compute 聞 ^{VIM} (1) 192.168.100.100	any
------------	-----	------	-----	---	-----

Figure 115 SSH firewall filter

6.6.14 Configure OSPF on ESG

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

OSPF Configuration :					Edit	Delete
Status :	Enabled					
Graceful Restart :	🖌 Enabled					
Default Originate :	 Enabled 	 Enabled 				
Area Definitions :						
+ / ×					Q Filter	-
Area ID		Туре		Authentics	ation	
0		Normal		None		
						1 items
Area to Interface Map	oping :					
💠 🥒 🗙					Q Filter	•
VNIC A	vrea ID	Hello Interval (sec	Dead Interval (sec	Priority	Cost	
DLR ESG link (0	10	40	128	1	

Figure 116 Configure OSPF in ESG

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

6.7 Install vCloud Director

6.7.1 Install and Bringup Windows VM

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

6.7.2 Install SQL Server in Windows VM

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

1	SQL Server 2012 Setup
Setup Role Click the SQL Server Feature In:	stallation option to individually select which feature components to install, or click a
Setup Support Rules Setup Role Feature Selection Installation Rules Instance Configuration Disk Space Requirements Server Configuration Database Engine Configuration Analysis Services Configuration Reporting Services Configuration Distributed Replay Controller Distributed Replay Controller Distributed Replay Client Error Reporting Installation Configuration Rules Ready to Install Installation Progress Complete	 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.
	Kext > Cancel Help

Figure 117 Install SQL Server

Create a named instance of your choice.

1	SQL S	erver 2012 Setu	qı		_ D X
Instance Configuration Specify the name and instance	ID for the instance of SQL Serv	er. Instance ID bec	omes part of the	installation path.	
Setup Support Rules Setup Role Feature Selection	 Default instance Named instance: 	dellvcddb			
Instance Configuration Disk Space Requirements Server Configuration Database Engine Configuration	Instance ID: Instance root directory: 	MSSQLSERVER C:\Program File	s\Microsoft SQL S	Server\	
Analysis Services Configuration Reporting Services Configuration Distributed Replay Controller Distributed Replay Client Error Reporting Installation Configuration Rules Ready to Install Installation Progress Complete	SQL Server directory: C:\Program Files\Microsoft SQL Server\MS Analysis Services directory: C:\Program Files\Microsoft SQL Server\MS Reporting Services directory: C:\Program Files\Microsoft SQL Server\MS		ierver\MSSQL11.MSSQLS ierver\MSAS11.MSSQLSE ierver\MSRS11.MSSQLSE	L11.MSSQLSERVER 11.MSSQLSERVER 11.MSSQLSERVER	
	Instance Name Instan	nce ID F	eatures	Edition	Version
		<	Back N	ext > Cancel	Help

Figure 118 Configure SQL instance

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

1	S	QL Server 2012 Setup					x	
Database Engine Configuration Specify Database Engine authentication security mode, administrators and data directories.								
Setup Support Rules Setup Support Rules Setup Role Feature Selection Installation Rules Instance Configuration Disk Space Requirements Server Configuration Database Engine Configuration Analysis Services Configuration Reporting Services Configuration Distributed Replay Controller Distributed Replay Controller Distributed Replay Controller Error Reporting Installation Configuration Rules Ready to Install Installation Progress Complete	Server Configuration Specify the authent Authentication Mod O Windows authen Mixed Mode (SQ Specify the password: Confirm password: Confirm password: Specify SQL Server a WIN-537PNO1EIAQ Add Current User	Data Directories FILESTREAM Cation mode and administrators for e cication mode . Server authentication and Window: d for the SQL Server system administrators e dministrators Administrator (Administrator) Add Remove	the Database Engir s authentication) trator (sa) account.	SQL Server a have unrestr to the Datab	dministra icted act	ators cess ne.	-	
		< Back	Next >	Cancel	н	lelp		

Figure 119 Configure password

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

1	SQL Server 2012 Setup
Ready to Install Verify the SQL Server 2012 feat Setup Support Rules Setup Role	Ready to install SQL Server 2012:
Feature Selection Installation Rules Instance Configuration Disk Space Requirements Server Configuration Database Engine Configuration Analysis Services Configuration Reporting Services Configuration Distributed Replay Controller Distributed Replay Client Error Reporting Installation Configuration Rules	Shared features Integration Services 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 Service Configuration Account: NT Service/SQL Server Distributed Replay Client Service Configuration Account: NT Service/SQL Server Distributed Replay Client Service Configuration Account: NT Service/SQL Server Distributed Replay Client Service Configuration Account: NT Service/SQL Server Distributed Replay Client Service Configuration Account: NT Service/SQL Server Distributed Replay Client Service Configuration Account: NT Service/SQL Server Distributed Replay Client Service Configuration Account: NT Service/SQL Server Distributed Replay Client Service Configuration Service Configuration Account: NT Service/SQL Server Distributed Replay Client Service Configuration
Ready to Install Installation Progress Complete	Working Directory: C:\Program Files (x8b)\Microsoft SQL Server\DReplayClient\Workini =
	< Back Install Cancel Help

Figure 120 SQL install

6.7.3 Configure the SQL Server

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

sļ	Connect to Server				
SQL Serv	/er ⁻ 2012				
Server type:	Database Engine	~			
Server name:	WIN-537PN01EIA0\DELLVCDDB				
Authentication:	SQL Server Authentication	~			
Login:	sa	~			
Password:	********				
	Remember password				
Connect	Cancel Help Options	>>			

Figure 121 Connect to SQL sever

6.7.3.1 Create a new user for vCloud

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

3	Login -	New		– – X
Select a page	🔄 Script 👻 🛐 Help			
original Server Roles Iser Mapping Image Securables Image Status	Login name: Windows authentication SQL Server authentication Password: Confirm password: Specify old password Old password: Enforce password expira User must change passw Mapped to certificate Mapped to asymmetric key			Search
Connection	Map to Credential		~	Add
Server: WIN-537PN01EIA0\DELLVCDDE Connection: sa I View connection properties	Mapped Credentials	Credential	Provider	
Progress				Remove
C Ready	Default database: Default language:	master <default></default>	~]
			ОК	Cancel

Figure 122 New vCloud user

6.7.3.2 Create a new Database

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

🔋 New Database 📃 🗖 🗙					
Select a page	🔄 Script 👻 📑	Help			
Options Filegroups	Database name:		veddb		
	Owner:	vner: vcdmgr			
	🔽 Use full-text in	ndexing			
	Database files: Logical Name	File Type	Filegroup	Initial Size (MB)	Autogrowth / Maxsize Pat
	voddb log	Rows Data	PRIMARY Not Applicable	1,024	By 512 MB, Unlimited C:\ Bu 128 MB Limited to 2000 MB C:\
Connection					
Server: WIN-537PN01EIA0\DELLVCDDE					
Connection: sa					
View connection properties					
Progress					
Ready	<	Ш			Add Remove
					OK Cancel

Figure 123 New Database

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

8	New Database 📃 🗖 🗖					
Select a page	🔄 Script 👻 🚺 Help					
Prilegroups	Collation:	Latin1_G	eneral_CS_AS			
	Recovery model:	Simple	Simple			
	Compatibility level:	SQL Serv	ver 2012 (110)	~		
	Containment type:	None		~		
	Other options:					
	Auto Shrink		False	^		
	Auto Update Statistics		True			
	Auto Update Statistics A	synchronously	False			
	⊿ Containment	Containment				
	Default Fulltext Languag	ie LCID	1033	=		
	Default Language		English			
	Nested Triggers Enabled	1	True			
	Transform Noise Words		False			
0 1	Two Digit Year Cutoff	Two Digit Year Cutoff				
Connection	⊿ Cursor		1			
Server:	Close Cursor on Commit	Enabled	False			
WIN-537PN01EIA0\DELLVCDDE	Default Cursor	Default Cursor GLOBAL				
Connection:	4 FILESTREAM					
sa	FILESTREAM Directory	Name	0//			
	FILESTREAM Non-Tran	sacted Access	Uff			
Mew connection properties						
	Allow Shapshot Isolation		False False	~ ~ ~		
Progress	ANSENDED Detaut		Faise			
Ready	Allow Snapshot Isolation	n				
				OK Cancel		

Figure 124 Configure database

6.7.3.3 Configure the database

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

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

6.7.4 Setup DNS server and add entries

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

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

New Zone Wizard	x			
Zone Name What is the name of the new zone?				
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: delinfv.com				
< Back Next >	Cancel			

Figure 125 Creating new zone

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

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: 172 .16 .114 . The network ID is the portion of the IP ad network ID in its normal (not reversed) or If you use a zero in the network ID, it will network ID 10 would create zone 10.in-ad zone 0.10.in-addr.arpa.	network ID or the name of the zone. Idresses that belongs to this zone. Enter the der. appear in the zone name. For example, ddr.arpa, and network ID 10.0 would create				
Reverse lookup zone name: 114.16.172.in-addr.arpa					
	< Back Next > Cancel				
L					

Figure 126 New zone wizard

Right click on Forward Lookup Zones \rightarrow Dell EMCnfv.com \rightarrow 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		
Add Host Cancel		

Figure 127 New Host

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

6.7.5 Install and Bring up RedHat Enterprise Linux VM

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

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

6.7.5.1 Configure Firewall rules in RH

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

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

-A RH-Firewall-1-INPUT -i ethl -m state --state NEW -m tcp -p tcp -dport 22 -j ACCEPT # vCloud Remote Console -A RH-Firewall-1-INPUT -i ethl -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

72 Dell EMC + VMware Cloud Infrastructure Platform for NFV VMware vCloud NFV 1.5 - NFVI Solution
-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 AMOP 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

73 Dell EMC + VMware Cloud Infrastructure Platform for NFV VMware vCloud NFV 1.5 - NFVI Solution

6.7.5.2 Install VMware public keys

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

cd /install/

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

6.7.6 Start and Stop vCloud director

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

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

6.7.6.1 Create SSL certificate

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

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

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

6.7.6.2 Continue with the installation

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

Database name- vcddbDatabase instance - Dell EMCvcddbUsername- vcdmgrPassword- <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] $6. \quad [0:0:0:0:0:0:0:1]$ 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

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 ~]#