

FlexPod Data Center with VMware vSphere 5.1 and Cisco Nexus 7000 with 7-Mode

Deployment Guide for FlexPod with VMware vSphere 5.1 and Cisco Nexus 7000 with Data ONTAP 8.1.2 Operating in 7-Mode Last Updated: November 23, 2013



Building Architectures to Solve Business Problems

cisco.





About the Authors

Lindsey Street, Systems Architect, Infrastructure and Cloud Engineering, NetApp Systems

Lindsey Street is a systems architect in the NetApp Infrastructure and Cloud Engineering team. She focuses on the architecture, implementation, compatibility, and security of innovative vendor technologies to develop competitive and high-performance end-to-end cloud solutions for customers. Lindsey started her career in 2006 at Nortel as an interoperability test engineer, testing customer equipment interoperability for certification. Lindsey has her Bachelors of Science degree in Computer Networking and her Master's of Science in Information Security from East Carolina University.

John George, Reference Architect, Infrastructure and Cloud Engineering, NetApp Systems

John George is a Reference Architect in the NetApp Infrastructure and Cloud Engineering team and is focused on developing, validating, and supporting cloud infrastructure solutions that include NetApp products. Before his current role, he supported and administered Nortel's worldwide training network and VPN infrastructure. John holds a Master's degree in computer engineering from Clemson University.

Chris O'Brien, Technical Marketing Manager, Server Access Virtualization Business Unit, Cisco Systems

Chris O'Brien is currently focused on developing infrastructure best practices and solutions that are designed, tested, and documented to facilitate and improve customer deployments. Previously, O'Brien was an application developer and has worked in the IT industry for more than 15 years.

Chris Reno, Reference Architect, Infrastructure and Cloud Engineering, NetApp Systems

Chris Reno is a reference architect in the NetApp Infrastructure and Cloud Enablement group and is focused on creating, validating, supporting, and evangelizing solutions based on NetApp products. Before being employed in his current role, he worked with NetApp product engineers designing and developing innovative ways to perform Q and A for NetApp products, including enablement of a large grid infrastructure using physical and virtualized compute resources. In these roles, Chris gained expertise in stateless computing, netboot architectures, and virtualization.

About Cisco Validated Design (CVD) Program

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit:

http://www.cisco.com/go/designzone

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLEC-TIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUP-PLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at http://www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2013 Cisco Systems, Inc. All rights reserved.

cisco.



VMware vSphere 5.1 on FlexPod Data ONTAP Operating in 7-Mode Deployment Guide

Overview

Industry trends indicate a vast data center transformation toward shared infrastructures. By using virtualization, enterprise customers have embarked on the journey to the cloud by moving away from application silos and toward shared infrastructure, thereby increasing agility and reducing costs. Cisco and NetApp have partnered to deliver FlexPod, which serves as the foundation for a variety of workloads and enables efficient architectural designs that are based on customer requirements.

Audience

This document describes the architecture and deployment procedures of an infrastructure composed of Cisco®, NetApp®, and VMware® virtualization that uses FCoE-based storage serving NAS and SAN protocols. The intended audience for this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineering, and customers who want to deploy the core FlexPod architecture with NetApp Data ONTAP® operating in 7-mode.

Architecture

The FlexPod architecture is highly modular or "podlike." Although each customer's FlexPod unit varies in its exact configuration, after a FlexPod unit is built, it can easily be scaled as requirements and demand change. The unit can be scaled both up (adding resources to a FlexPod unit) and out (adding more FlexPod units).

Specifically, FlexPod is a defined set of hardware and software that serves as an integrated foundation for both virtualized and nonvirtualized solutions. VMware vSphere® built on FlexPod includes NetApp storage, NetApp Data ONTAP, Cisco networking, the Cisco Unified Computing SystemTM (Cisco UCS®), and VMware vSphere software in a single package. The design is flexible enough that the networking, computing, and storage can fit in one data center rack or be deployed according to a customer's data center design. Port density enables the networking components to accommodate multiple configurations of this kind.



One benefit of the FlexPod architecture is the ability to customize or "flex" the environment to suit a customer's requirements. This is why the reference architecture detailed in this document highlights the resiliency, cost benefit, and ease of deployment of an FCoE-based storage solution. A storage system capable of serving multiple protocols across a single interface allows for customer choice and investment protection because it truly is a wire-once architecture.

Figure 1 shows the VMware vSphere built on FlexPod components and the network connections for a configuration with FCoE-based storage. This design uses the Cisco Nexus® 5548UP, Cisco Nexus 2232PP FEX, and Cisco UCS C-Series and B-Series with the Cisco UCS virtual interface card (VIC) and the NetApp FAS family of storage controllers connected in a highly available design using Cisco Virtual PortChannels (vPCs). This infrastructure is deployed to provide FCoE-booted hosts with file- and block-level access to shared storage datastores. The reference architecture reinforces the "wire-once" strategy, because as additional storage is added to the architecture; be it FC, FCoE, or 10 Gigabit Ethernet, no recabling is required from the hosts to the Cisco UCS fabric interconnect.

Figure 1 VMware vSpahere Built on Flexpod Components



The reference configuration includes:

- Two Cisco Nexus 5548UP switches
- Two Cisco Nexus 2232PP fabric extenders
- Two Cisco UCS 6248UP fabric interconnects

- Support for 16 Cisco UCS C-Series servers without any additional networking components
- Support for 8 Cisco UCS B-Series servers without any additional blade server chassis
- Support for hundreds of Cisco UCS C-Series and B-Series servers by way of additional fabric extenders and blade server chassis
- One NetApp FAS3250-A (HA pair) operating in 7-mode

Storage is provided by a NetApp FAS3250-AE (HA configuration in two chassis) operating 7-Mode. All system and network links feature redundancy, providing end-to-end high availability (HA). For server virtualization, the deployment includes VMware vSphere. Although this is the base design, each of the components can be scaled flexibly to support specific business requirements. For example, more (or different) servers or even blade chassis can be deployed to increase compute capacity, additional disk shelves can be deployed to improve I/O capacity and throughput, and special hardware or software features can be added to introduce new capabilities.

This document guides you through the low-level steps for deploying the base architecture, as shown in Figure 1. These procedures cover everything from physical cabling to compute and storage configuration to configuring virtualization with VMware vSphere.

Software Revisions

It is important to note the software versions used in this document. Table 1 details the software revisions used throughout this document.

Layer	Compute	Version or Release	Details
Compute	Cisco UCS Fabric Interconnect	2.1(1b)	Embedded management
	Cisco UCS C 200 M2 Server	2.1(1b)	Software bundle release
	Cisco UCS C 220 M3 Server	2.1(1b)	Software bundle release
	Cisco UCS B 200 M2 Server	2.1(1b)	Software bundle release
	Cisco UCS B 200 M3 Server	2.1(1b)	Software bundle release
	Cisco eNIC	2.1.2.38	Ethernet driver for Cisco VIC
	Cisco fNIC	1.5.0.20	FCoE driver for Cisco VIC
Network	Cisco Nexus Switch	5.2(1)N1(3)	Operating system version
Storage	NetApp FAS3250-A	Data ONTAP 8.1.2 operating in 7-mode	Operating system version

Table 1 Software Revisions

Layer	Compute	Version or Release	Details
Software	Cisco UCS Hosts	VMware vSphere ESXi [™] 5.1	Operating system version
	Microsoft [®] .NET Framework	3.5.1	Feature enabled within Windows® operating system
	Microsoft SQL Server®	Microsoft SQL Server 2008 R2 SP1	VM (1 each): SQL Server DB
	VMware vCenter TM	5.1	VM (1 each): VMware vCenter
	NetApp OnCommand®	5.1	VM (1 each): OnCommand
	NetApp Virtual Storage Console (VSC)	4.1	Plug-in within VMware vCenter
	Cisco Nexus 1110-x	4.2.1.SP1.5.1a	Virtual Services Appliance (VSA)
	Cisco Nexus 1000v	4.2.1.SV2.1.1a	Virtual services blade within the VSA
	NetApp NFS Plug-in for VMware vStorage APIs for Array Integration (VAAI)	1.0-018	Plug-in within VMware vCenter
	NetApp FAS/V-Series vSphere Storage APIs for Storage Awareness (VASA) Provider	1.0	VM (1 each): NetApp VASA Provider

Table 1 Software Revisions

Configuration Guidelines

This document provides details for configuring a fully redundant, highly available configuration for a FlexPod unit with IP-based storage. Therefore, reference is made to which component is being configured with each step, either A or B. For example, controller A and controller B are used to identify the two NetApp storage controllers that are provisioned with this document, and Nexus A and Nexus B identify the pair of Cisco Nexus switches that are configured. The Cisco UCS fabric interconnects are similarly configured. Additionally, this document details steps for provisioning multiple Cisco UCS hosts, and these are identified sequentially: VM-Host-Infra-01, VM-Host-Infra-02, and so on. Finally, to indicate that you should include information pertinent to your environment in a given step, <text> appears as part of the command structure. See the following example for the vlan create command:

I

```
controller A> vlan create
Usage:
    vlan create [-g {on|off}] <ifname> <vlanid_list>
    vlan add <ifname> <vlanid_list>
    vlan delete -q <ifname> [<vlanid_list>]
    vlan modify -g {on|off} <ifname>
    vlan stat <ifname> [<vlanid_list>]
Example:
controller A> vlan create vif0 <management VLAN ID>
```

This document is intended to enable you to fully configure the customer environment. In this process, various steps require you to insert customer-specific naming conventions, IP addresses, and VLAN schemes, as well as to record appropriate MAC addresses. Table 2 describes the VLANs necessary for deployment as outlined in this guide. The VM-Mgmt VLAN is used for management interfaces of the VMware vSphere hosts. Table 3 lists the VSANs necessary for deployment as outlined in this guide. The VSANs necessary for deployment as outlined in this guide. Table 4 lists the configuration variables that are used throughout this document. Table 4 can be completed based on the specific site variables and used in implementing the document configuration procedures.

If you use separate in-band and out-of-band management VLANs, you must create a Layer 3 route between these VLANs. For this validation, a common management VLAN was used.

VLAN Name	VLAN Purpose	ID Used in Validating This Document
Mgmt in band	VLAN for in-band management interfaces	3175
Mgmt out of band	VLAN for out-of-band management interfaces	3171
Native	VLAN to which untagged frames are assigned	2
NFS	VLAN for NFS traffic	3170
FCoE - A	VLAN for FCoE traffic for fabric A	101
FCoE - B	VLAN for FCoE traffic for fabric B	102
vMotion	VLAN designated for the movement of VMs from one physical host to another	3173
VM Traffic	VLAN for VM application traffic	3174
Packet Control	VLAN for Packet Control traffic	3176

Table 2 Necessary VLANs

Table 3 Necessary VSANs

I

VSAN Name	VSAN Purpose	ID Used in Validating This Document
VSAN A	VSAN for fabric A traffic. ID matches FCoE-A VLAN	101
VSAN B	VSAN for fabric B traffic. ID matches FCoE-B VLAN	102

Table 4 Created VMware Virtual Machine

Virtual Machine Description	Host Name
vCenter SQL Server database	
vCenter Server	
NetApp Virtual Storage Console (VSC) and NetApp OnCommand® core	
NetApp vSphere Storage APIs for Storage Awareness (VASA) Provider	

1

Table 5Configuration Variables

Variable	Description	Customer Implementation Value
< <var_controller1>></var_controller1>	Storage Controller 1 Host Name	-
< <var_controller1_e0m_ip>></var_controller1_e0m_ip>	Out-of-band management IP for Storage Controller 1	
< <var_controller1_mask>></var_controller1_mask>	Out-of-band management network netmask	
< <var_controller1_mgmt_gateway>></var_controller1_mgmt_gateway>	Out-of-band management network default gateway	
< <var_adminhost_ip>>></var_adminhost_ip>	Administration Host Server IP	
< <var_timezone>></var_timezone>	FlexPod time zone (for example, America/New_York)	
< <var_location>></var_location>	Node location string	
< <var_dns_domain_name>></var_dns_domain_name>	DNS domain name	
< <var_nameserver_ip>></var_nameserver_ip>	DNS server IP(s)	
< <var_sp_ip>></var_sp_ip>	Out-of-band service processor management IP for each storage controller	
< <var_sp_mask>></var_sp_mask>	Out-of-band management network netmask	
< <var_sp_gateway>></var_sp_gateway>	Out-of-band management network default gateway	
< <var_mailhost>></var_mailhost>	Mail server host name	
< <var_mailhost_ip>></var_mailhost_ip>	Mail server IP	
< <var_password>></var_password>	Global default administrative password	
< <var_controller2>></var_controller2>	Storage Controller 2 Host Name	
< <var_controller2_e0m_ip>></var_controller2_e0m_ip>	Out-of-band management IP for Storage Controller 2	

VMware vSphere 5.1 on FlexPod Data ONTAP Operating in 7-Mode Deployment Guide

Variable	Description	Customer Implementation Value
< <var_controller2_mask>></var_controller2_mask>	Out-of-band management network netmask	
< <var_controller2_mgmt_gateway>></var_controller2_mgmt_gateway>	Out-of-band management network default gateway	
< <var_#_of_disks>></var_#_of_disks>	Number of disks to assign to each storage controller	
< <var_nfs_ip>></var_nfs_ip>	NFS VLAN IP for each storage controller	
< <var_nfs_mask>></var_nfs_mask>	NFS VLAN netmask	
< <var_nfs_license>></var_nfs_license>	Data ONTAP NFS License Code	
< <var_cf_license>></var_cf_license>	Data ONTAP Cluster Failover License Code	
< <var_fc_license>></var_fc_license>	Data ONTAP Fiber Channel Protocol License Code	
< <var_date>></var_date>	Current time in [[[[CC]yy]mm]dd]hhmm[.ss]] format	
< <var_global_ntp_server_ip>></var_global_ntp_server_ip>	NTP server IP address	
< <var_state>></var_state>	State or province name	
< <var_city>></var_city>	City name	
< <var_org>></var_org>	Organization or company name	
< <var_unit>></var_unit>	Organizational unit name	
< <var_controller1_fqdn>></var_controller1_fqdn>	Storage Controller 1 Fully Qualified Domain Name (FQDN)	
< <var_admin_email>></var_admin_email>	Administrator e-mail address	
< <var_key_length>></var_key_length>	Number of bits in SSL/SSH Security Key	
< <var_controller2_fqdn>></var_controller2_fqdn>	Storage Controller 2 FQDN	
< <var_snaprestore_license>></var_snaprestore_license>	Data ONTAP SnapRestore License Code	
< <var_flex_clone_license>></var_flex_clone_license>	Data ONTAP FlexClone License Code	
< <var_raidsize>></var_raidsize>	RAID group size for each Storage Controller	
< <var_url_boot_software>></var_url_boot_software>	Data ONTAP 8.1.2 URL; format: http://	
< <var_oncommand_server_fqdn>></var_oncommand_server_fqdn>	OnCommand/VSC Virtual Machine FQDN	
< <var_snmp_community>></var_snmp_community>	SNMP v1/v2 community name	
< <var_country_code>></var_country_code>	Two-letter country code	
< <var_nexus_a_hostname>></var_nexus_a_hostname>	Cisco Nexus A host name	
< <var_nexus_a_mgmt0_ip>></var_nexus_a_mgmt0_ip>	Out-of-band Cisco Nexus A management IP address	

Table 5Configuration Variables

I

Γ

		Customer
Variable	Description	Implementation Value
< <var_nexus_a_mgmt0_netmask>></var_nexus_a_mgmt0_netmask>	Out-of-band management network netmask	
< <var_nexus_a_mgmt0_gw>></var_nexus_a_mgmt0_gw>	Out-of-band management network default gateway	
< <var_controller2_nfs_ip>></var_controller2_nfs_ip>	NFS VLAN IP for storage controller 2	
< <var_nexus_b_hostname>></var_nexus_b_hostname>	Cisco Nexus B host name	
< <var_nexus_b_mgmt0_ip>></var_nexus_b_mgmt0_ip>	Out-of-band Cisco Nexus B management IP address	
< <var_nexus_b_mgmt0_netmask>></var_nexus_b_mgmt0_netmask>	Out-of-band management network netmask	
< <var_nexus_b_mgmt0_gw>></var_nexus_b_mgmt0_gw>	Out-of-band management network default gateway	
< <var_ib-mgmt_vlan_id>></var_ib-mgmt_vlan_id>	In-band management network VLAN ID	
< <var_native_vlan_id>></var_native_vlan_id>	Native VLAN ID	
< <var_nfs_vlan_id>></var_nfs_vlan_id>	NFS VLAN ID	
< <var_pkt-ctrl_vlan_id>></var_pkt-ctrl_vlan_id>	Cisco Nexus 1000v packet control VLAN ID	
< <var_vmotion_vlan_id>></var_vmotion_vlan_id>	VMware vMotion® VLAN ID	
< <var_vm-traffic_vlan_id>></var_vm-traffic_vlan_id>	VM traffic VLAN ID	
< <var_ucs_cluster_ip>></var_ucs_cluster_ip>	Cisco UCS Manager cluster IP address	
< <var_controller1_nfs_ip></var_controller1_nfs_ip>	NFS VLAN IP for storage controller 1	
< <var_ftp_server>></var_ftp_server>	Accessible FTP Server IP	
< <var_nexus_vpc_domain_id>></var_nexus_vpc_domain_id>	Unique Cisco Nexus switch VPC domain ID	
< <var_nexus_1110x-1>></var_nexus_1110x-1>	Cisco Nexus 1110X-1 host name	
< <var_nexus_1110x-2>></var_nexus_1110x-2>	Cisco Nexus 1110X-2 host name	
< <var_fabric _a_fcoe_vlan_id="">></var_fabric>	Fabric A FCoE VLAN ID	
< <var_vsan_a_id>></var_vsan_a_id>	Fabric A VSAN ID	
< <var_fabric_b_fcoe_vlan_id>></var_fabric_b_fcoe_vlan_id>	Fabric B FCoE VLAN ID	
< <var_vsan_b_id>></var_vsan_b_id>	Fabric B VSAN ID	
< <var_vsm_domain_id>></var_vsm_domain_id>	Unique Cisco Nexus 1000v virtual supervisor module (VSM) domain ID	
< <var_vsm_mgmt_ip>></var_vsm_mgmt_ip>	Cisco Nexus 1000v VSM management IP address	
< <var_vsm_mgmt_mask>></var_vsm_mgmt_mask>	In-band management network netmask	
< <var_vsm_mgmt_gw>></var_vsm_mgmt_gw>	In-band management network default gateway	

1

Table 5Configuration Variables

Veriable	Description	Customer Implementation
	Cises Name 1000: VSM best name	value
< <var_vsm_nostname>></var_vsm_nostname>	Cisco Nexus 10000 V SM host name	
< <var_ucs_clustername>></var_ucs_clustername>	Cisco UCS Manager cluster host name	
< <var_ucsa_mgmt_1p>></var_ucsa_mgmt_1p>	out-of-band management IP address	
< <var_ucsa_mgmt_mask>></var_ucsa_mgmt_mask>	Out-of-band management network netmask	
< <var_ucsa_mgmt_gateway>></var_ucsa_mgmt_gateway>	Out-of-band management network default gateway	
< <var_ucsb_mgmt_ip>></var_ucsb_mgmt_ip>	Cisco UCS FI B out-of-band management IP address	
< <var_cimc_ip>></var_cimc_ip>	Out-of-band management IP for each Cisco Nexus 1110-X CIMC	
< <var_cimc_mask>></var_cimc_mask>	Out-of-band management network netmask	
< <var_cimc_gateway>></var_cimc_gateway>	Out-of-band management network default gateway	
< <var_1110x_domain_id>></var_1110x_domain_id>	Unique Cisco Nexus 110-X domain ID	
< <var_1110x_vsa>></var_1110x_vsa>	Virtual storage appliance (VSA) host name	
< <var_1110x_vsa_ip>></var_1110x_vsa_ip>	In-band VSA management IP address	
< <var_1110x_vsa_mask>></var_1110x_vsa_mask>	In-band management network netmask	
< <var_1110x_vsa_gateway>></var_1110x_vsa_gateway>	In-band management network default gateway	
< <var_vmhost_infra01_ip>></var_vmhost_infra01_ip>	VMware ESXi host 01 in-band management IP	
< <var_vmhost_infra02_ip>></var_vmhost_infra02_ip>	VMware ESXi host 02 in-band management IP	
< <var_nfs_vlan_id_ip_host-01>></var_nfs_vlan_id_ip_host-01>	NFS VLAN IP address for ESXi host 01	
< <var_nfs_vlan_id_mask_host-01>></var_nfs_vlan_id_mask_host-01>	NFS VLAN netmask for ESXi host 01	
< <var_vmotion_vlan_id_ip_host-01>></var_vmotion_vlan_id_ip_host-01>	vMotion VLAN IP address for ESXi host 01	
< <var_vmotion_vlan_id_mask_host-01></var_vmotion_vlan_id_mask_host-01>	vMotion VLAN netmask for ESXi host 01	
< <var_nfs_vlan_id_ip_host-02>></var_nfs_vlan_id_ip_host-02>	NFS VLAN IP address for ESXi host 02	
< <var_nfs_vlan_id_mask_host-02>></var_nfs_vlan_id_mask_host-02>	NFS VLAN netmask for ESXi host 02	
< <var_vcenter_server_ip>></var_vcenter_server_ip>	vCenter Server IP	
< <var_vm_host_infra_01_a_wwpn>></var_vm_host_infra_01_a_wwpn>	WWPN of VM-Host-Infra-01 vHBA-A	
< <var_vm_host_infra_02_a_wwpn>></var_vm_host_infra_02_a_wwpn>	WWPN of VM-Host-Infra-02 vHBA-A	

Table 5Configuration Variables

Γ

Variable	Description	Customer Implementation Value
< <var_controller1_1a_wwpn>></var_controller1_1a_wwpn>	WWPN of storage controller 1 port 1a	
< <var_controller2_1a_wwpn>></var_controller2_1a_wwpn>	WWPN of storage controller 2 port 1a	
< <var_vm_host_infra_01_b_wwpn>></var_vm_host_infra_01_b_wwpn>	WWPN of VM-Host-Infra-01 vHBA-B	
< <var_vm_host_infra_02_b_wwpn>></var_vm_host_infra_02_b_wwpn>	WWPN of VM-Host-Infra-02 vHBA-B	
< <var_controller1_1b_wwpn>></var_controller1_1b_wwpn>	WWPN of storage controller 1 port 1b	
< <var_controller2_1b_wwpn>></var_controller2_1b_wwpn>	WWPN of storage controller 2 port 1b	

1

Table 5Configuration Variables

Physical Infrastructure

FlexPod Cabling on Data ONTAP Operating in 7-Mode

Figure 2 shows the cabling diagram for a FlexPod configuration using Data ONTAP operating on 7-mode.



ſ

Figure 2 Flexpod Cabling Diagram in Data ONTAP 7-Mode

The information provided in Table 6 through Table 17 corresponds to each connection shown in Figure 2.

1

1

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 5548	Eth1/1	10GbE	NetApp controller 1	e1a
Switch A	Eth1/2	10GbE	NetApp controller 2	e1a
	Eth1/11	10GbE	Cisco UCS fabric interconnect A	Eth1/19
	Eth1/12	10GbE	Cisco UCS fabric interconnect B	Eth1/19
	Eth1/13	10GbE	Cisco Nexus 5548 B	Eth1/13
	Eth1/14	10GbE	Cisco Nexus 5548 B	Eth1/14
	Eth1/15	1GbE	Cisco Nexus 1110-X A	LOM A
	Eth1/16	1GbE	Cisco Nexus 1110-X B	LOM A
	Eth1/31	10GbE	Cisco UCS fabric interconnect A	Eth1/31
	Eth1/32	10GbE	Cisco UCS fabric interconnect A	Eth1/32
	MGMT0	1GbE	1GbE management switch	Any

Table 6 Cisco Nexus 5548 A Cabling Information



For devices requiring GbE connectivity, use the GbE Copper SFP+s (GLC-T=).

Local Device	Local Port	Connection	Remote Device	Remote Ports
Cisco Nexus 5548	Eth1/1	10GbE	NetApp controller 1	e1a
Switch B	Eth1/2	10GbE	NetApp controller 2	e41
	Eth1/11	10GbE	Cisco UCS fabric interconnect A	Eth1/20
	Eth1/12	10GbE	Cisco UCS fabric interconnect B	Eth1/20
	Eth1/13	10GbE	Cisco Nexus 5548 A	Eth1/13
	Eth1/14	10GbE	Cisco Nexus 5548 A	Eth1/14
	Eth1/15	1GbE	Cisco Nexus 1110-X A	LOM B
	Eth1/16	1GbE	Cisco Nexus 1110-X B	LOM B
	Eth1/31	10GbE	Cisco UCS fabric interconnect B	Eth1/31
	Eth1/32	10GbE	Cisco UCS fabric interconnect B	Eth1/32
	MGMT0	1GbE	GbE management switch	Any

Table 7 Cisco Nexus 5548 B Cabling Information



Γ

For devices requiring GbE connectivity, use the GbE Copper SFP+s (GLC-T=).

Table 8	NetApp Controller 1	Cabling Information
		0

Local Device	Local Port	Connection	Remote Device	Remote Port
NetApp Controller 1	e0M	100MbE	100MbE management switch	Any
	e0P	1 GbE	SAS shelves	ACP port
	e1a	10GbE	Cisco Nexus 5596 A	Eth1/1
	e1b	10GbE	Cisco Nexus 5596 B	Eth1/1

Table 9 NetApp Controller 2 Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
NetApp Controller e	e0M	100MbE	100MbE management switch	Any
e0P	e0P	1 GbE	SAS shelves	ACP port
	ela	10GbE	Cisco Nexus 5596 A	Eth1/2
	e1b	10GbE	Cisco Nexus 5596 B	Eth1/2

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric	Eth1/19	10GbE	Cisco Nexus 5548 A	Eth1/11
Interconnect A	Eth1/20	10GbE	Cisco Nexus 5548 B	Eth1/11
	Eth1/1	10GbE	Cisco UCS Chassis Fabric Extender (FEX) A /Cisco Nexus 2232PP FEX A	
	Eth1/2	10GbE	Cisco UCS Chassis Fabric Extender (FEX) A /Cisco Nexus 2232PP FEX A	
	Eth1/3	10GbE	Cisco UCS Chassis Fabric Extender (FEX) A /Cisco Nexus 2232PP FEX A	
	Eth1/4	10GbE	Cisco UCS Chassis Fabric Extender (FEX) A /Cisco Nexus 2232PP FEX A	
	Eth1/5	10GbE	Cisco UCS Chassis Fabric Extender (FEX) A /Cisco Nexus 2232PP FEX A	
	Eth1/6	10GbE	Cisco UCS Chassis Fabric Extender (FEX) A /Cisco Nexus 2232PP FEX A	
	Eth1/31	10GbE	Cisco Nexus 5548 A	Eth1/31
	Eth1/32	10GbE	Cisco Nexus 5548 A	Eth1/32
	MGMT0	1GbE	1GbE management switch	Any
	L1	1GbE	Cisco UCS fabric interconnect B	L1
	L2	1GbE	Cisco UCS fabric interconnect B	L2

1

Table 10 Cisco UCS Fabric Interconnect A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric	Eth1/19	10GbE	Cisco Nexus 5548 A	Eth1/12
Interconnect B	Eth1/20	10GbE	Cisco Nexus 5548 B	Eth1/12
	Eth1/1	10GbE	Cisco UCS Chassis FEX B/Cisco Nexus 2232PP FEX B	
	Eth1/2	10GbE	Cisco UCS Chassis FEX B/Cisco Nexus 2232PP FEX B	
	Eth1/3	10GbE	Cisco UCS Chassis FEX B/Cisco Nexus 2232PP FEX B	
	Eth1/4	10GbE	Cisco UCS Chassis FEX B/Cisco Nexus 2232PP FEX B	
	Eth1/5	10GbE	Cisco UCS Chassis FEX B/Cisco Nexus 2232PP FEX B	
	Eth1/6	10GbE	Cisco UCS Chassis FEX B/Cisco Nexus 2232PP FEX B	
	Eth1/31	10GbE	Cisco Nexus 5548 B	Eth1/31
	Eth1/32	10GbE	Cisco Nexus 5548 B	Eth1/32
	MGMT0	1GbE	GbE management switch	Any
	L1	1GbE	Cisco UCS fabric interconnect A	L1
	L2	1GbE	Cisco UCS fabric interconnect A	L2

Table 11 Cisco UCS Fabric Interconnect B Cabling Information

L

Γ

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus	Port 1	1GbE	Cisco UCS C-Series 1	M1
2232PP Fabric	Port 2	10GbE	Cisco UCS C-Series 1	Port 0
Extender (FEX A)	Port 3	1GbE	Cisco UCS C-Series 2	M1
	Port 4	10GbE	Cisco UCS C-Series 2	Port 0
	Port 5	1GbE	Cisco UCS C-Series 3	M1
	Port 6	10GbE	Cisco UCS C-Series 3	Port 0
	Port 7	1GbE	Cisco UCS C-Series 4	M1
	Port 8	10GbE	Cisco UCS C-Series 4	Port 0
	Port 2/1	10GbE	Cisco UCS fabric interconnect A	
	Port 2/2	10GbE	Cisco UCS fabric interconnect A	

1

Table 12 Cisco Nexus 2232PP FEX A

Table 13Cisco Nexus 2232PP FEX B

Local Device	Local Port	Connection	Remote Devices	Remote Port
Cisco Nexus	Port 1	1GbE	Cisco UCS C-Series 1	M2
2232PP Fabric Extender (EEX B)	Port 2	10GbE	Cisco UCS C-Series 1	Port 1
Extender (FEX D)	Port 3	1GbE	Cisco UCS C-Series 2	M2
	Port 4	10GbE	Cisco UCS C-Series 2	Port 1
	Port 5	1GbE	Cisco UCS C-Series 3	M2
	Port 6	10GbE	Cisco UCS C-Series 3	Port 1
	Port 7	1GbE	Cisco UCS C-Series 4	M2
	Port 8	10GbE	Cisco UCS C-Series 4	Port 1
	Port 2/1	10GbE	Cisco UCS fabric interconnect B	
	Port 2/2	10GbE	Cisco UCS fabric interconnect B	

Table 14 Cisco UCS C-Series 1

I

Γ

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS C-Series Server 1	M1	1GbE	Cisco Nexus 2232PP Fabric Extender A (FEX A)	Port 1
	M2	1GbE	Cisco Nexus 2232PP Fabric Extender B (FEX B)	Port 1
	Port0	10GbE	Cisco Nexus 2232PP Fabric Extender B (FEX A)	Port 2
	Port1	10GbE	Cisco Nexus 2232PP Fabric Extender B (FEX B)	Port 2

Table 15Cisco UCS C-Series 2

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS C-Series Server 2	co UCS M1 1GbE Cisco Nexus 2232PP Fabric eries Server 2 Extender A (FEX A)	Port 3		
	M2	1GbE	Cisco Nexus 2232PP Fabric Extender B (FEX B)	Port 3
	Port0	10GbE	Cisco Nexus 2232PP Fabric Extender A (FEX A)	Port 4
	Port1	10GbE	Cisco Nexus 2232PP Fabric Extender B (FEX B)	Port 4

Table 16Cisco UCS C-Series 3

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS C-Series Server 3	M1	1GbE	Cisco Nexus 2232PP Fabric Extender A (FEX A)	Port 5
	M2	1GbE	Cisco Nexus 2232PP Fabric Extender B (FEX B)	Port 5
	Port0	10GbE	Cisco Nexus 2232PP Fabric Extender A (FEX A)	Port 6
	Port1	10GbE	Cisco Nexus 2232PP Fabric Extender B (FEX B)	Port 6

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS C-Series Server 4	M1	1GbE	Cisco Nexus 2232PP Fabric Extender A (FEX A)	Port 7
	M2	1GbE	Cisco Nexus 2232PP Fabric Extender B (FEX B)	Port 7
	Port0	10GbE	Cisco Nexus 2232PP Fabric Extender A (FEX A)	Port 8
	Port1	10GbE	Cisco Nexus 2232PP Fabric Extender B (FEX B)	Port 8

1

Table 17	Cisco UCS	C-Series 4

Storage Configuration

Controller FAS32xx Series

Requirement	Reference	Comments
Physical site where storage system needs to be installed must be ready	Site Reference Guide: http://support.netapp.com/NOW /public/knowledge/docs/hardwar e/NetApp/site/pdf/site.pdf	Refer to the "Site Preparation" section
Storage system connectivity requirements	Site Reference Guide: http://support.netapp.com/NOW /public/knowledge/docs/hardwar e/NetApp/site/pdf/site.pdf	Refer to the "System Connectivity Requirements" section
Storage system general power requirements	Site Reference Guide: http://support.netapp.com/NOW /public/knowledge/docs/hardwar e/NetApp/site/pdf/site.pdf	Refer to the "Circuit Breaker, Power Outlet Balancing, System Cabinet Power Cord Plugs, and Console Pinout Requirements" section
Storage system model-specific requirements	Site Reference Guide: http://support.netapp.com/NOW /public/knowledge/docs/hardwar e/NetApp/site/pdf/site.pdf	Refer to the "FAS32xx/V32xx Series Systems" section

Table 18

18 Controller FAS32XX Series Prerequisites

System Configuration Guides

System configuration guides provide supported hardware and software components for the specific Data ONTAP version. These online guides provide configuration information for all NetApp storage appliances currently supported by the Data ONTAP software. They also provide a table of component compatibilities.

1. Make sure that the hardware and software components are supported with the version of Data ONTAP that you plan to install by checking the System Configuration Guides at:

https://now.netapp.com/NOW/knowledge/docs/hardware/NetApp/syscfg/

2. Click the appropriate NetApp storage appliance and then click the component you want to view. Alternatively, to compare components by storage appliance, click a component and then click the NetApp storage appliance you want to view.

Controllers

Follow the physical installation procedures for the controllers in the FAS32xx documentation in NetApp Support site at:

https://now.netapp.com/NOW/knowledge/docs/hardware/filer/210-05224+A0.pdf

Disk Shelves DS2246 Series

DS2246 Disk Shelves

To install a disk shelf for a new storage system, see:

https://now.netapp.com/NOW/knowledge/docs/hardware/filer/210-04881+A0.pdf

For information on cabling with the controller model, see SAS Disk Shelves Universal SAS and ACP Cabling Guide at:

https://now.netapp.com/NOW/knowledge/docs/hardware/filer/215-05500_A0.pdf

The following information applies to DS2246 disk shelves:

- SAS disk drives use software-based disk ownership. Ownership of a disk drive is assigned to a specific storage system by writing software ownership information on the disk drive rather than by using the topography of the storage system's physical connections.
- Connectivity terms used: shelf-to-shelf (daisy-chain), controller-to-shelf (top connections), and shelf-to controller (bottom connections).
- Unique disk shelf IDs must be set per storage system (a number from 0 through 98).
- Disk shelf power must be turned on to change the digital display shelf ID. The digital display is on the front of the disk shelf.
- Disk shelves must be power-cycled after the shelf ID is changed for it to take effect.
- Changing the shelf ID on a disk shelf that is part of an existing storage system running Data ONTAP requires that you wait at least 30 seconds before turning the power back on so that Data ONTAP can properly delete the old disk shelf address and update the copy of the new disk shelf address.
- Changing the shelf ID on a disk shelf that is part of a new storage system installation (the disk shelf is not yet running Data ONTAP) requires no wait; you can immediately power-cycle the disk shelf.

Data ONTAP 8.1.2

Complete the Configuration Worksheet

Before running the setup script, complete the configuration worksheet from the product manual.

For more information on Configuration Worksheet, see:

https://library.netapp.com/ecm/ecm_get_file/ECMM1249829

Note

To access Configuration Worksheet, you need to have access to NetApp Support site: http://now.netapp.com/

Assign Controller Disk Ownership and initialize storage

This section provides details for assigning disk ownership and disk initialization and verification.

Typical best practices should be followed when determining the number of disks to assign to each controller head. You may choose to assign a disproportionate number of disks to a given storage controller in an HA pair, depending on the intended workload.

In this reference architecture, half the total number of disks in the environment is assigned to one controller and the remainder to its partner.

Detail	Detail Value
Controller 1 MGMT IP	< <var_controller1_e0m_ip>></var_controller1_e0m_ip>
Controller 1 netmask	< <var_controller1_mask>></var_controller1_mask>
Controller 1 gateway	< <var_controller1_mgmt_gateway>></var_controller1_mgmt_gateway>
URL of the Data ONTAP boot software	< <var_url_boot_software>></var_url_boot_software>
Controller 2 MGMT IP	< <var_controller2_e0m_ip>></var_controller2_e0m_ip>
Controller 2 netmask	< <var_controller2_mask>></var_controller2_mask>
Controller 2 gateway	< <var_controller2_mgmt_gateway>></var_controller2_mgmt_gateway>

Table 19 Controller Details

Controller1

1. Connect to the storage system console port. You should see a Loader-A prompt. However, if the storage system is in a reboot loop, Press Ctrl-C to exit the Autoboot loop when you see this message:

Starting AUTOBOOT press Ctrl-C to abort ...

- 2. If the system is at the LOADER prompt, enter the following command to boot Data ONTAP: autoboot
- 3. During system boot, press Ctrl-C when prompted for the Boot Menu:

Press Ctrl-C for Boot Menu ...



У

- **13.** When you see "Press Ctrl-C for Boot Menu": Ctrl-C
- **14.** To enter Maintenance mode boot, select option 5.
- **15.** When you see the question "Continue to Boot?" type yes.

У

16. To verify the HA status of your environment, enter:

ha-config show

<u>Note</u>

If either component is not in HA mode, use the ha-config modify command to put the components in HA mode.

17. To see how many disks are unowned, enter:

disk show -a

Note

• No disks should be owned in this list.

18. Assign disks.

disk assign -n <<var_#_of_disks>>

- **Note** This reference architecture allocates half the disks to each controller. However, workload design could dictate different percentages.
- **19.** Reboot the controller.

halt

20. At the LOADER-A prompt, enter:

autoboot

21. Press Ctrl-C for Boot Menu when prompted.

Ctrl-C

22. Select option 4 for Clean configuration and initialize all disks.

4

- 23. Answer yes to zero disks, reset config and install a new file system.
 - У

y

24. Enter yes to erase all the data on the disks.



The initialization and creation of the root volume can take 75 minutes or more to complete, depending on the number of disks attached. When initialization is complete, the storage system reboots. You can continue to controller 2 configuration while the disks for controller 1 are zeroing.

Controller 2

1. Connect to the storage system console port. You should see a Loader-A prompt. However if the storage system is in a reboot loop, Press Ctrl-C to exit the Autoboot loop when you see this message:

```
Starting AUTOBOOT press Ctrl-C to abort ...
```

- 2. If the system is at the LOADER prompt, enter the following command to boot Data ONTAP: autoboot
- 3. During system boot, press Ctrl-C when prompted for the Boot Menu:

Press Ctrl-C for Boot Menu...

Note If 8.1.2 is not the version of software being booted, follow the steps to install new software. If 8.1.2 is the version being booted, then proceed with step 14, maintenance mode boot

4. To install new software first select option 7.

7

5. Enter yes for performing a nondisruptive upgrade.

У

6. Select e0M for the network port you want to use for the download.

e0M

7. Enter yes to reboot now.

У

8. Enter the IP address, netmask and default gateway for e0M in their respective places.

```
<<var_controller2_e0m_ip>>
<<var_controller2_mask>>
<<var_controller2_mgmt_gateway>>
```

9. Enter the URL where the software can be found.

<u>Note</u>

This Web server must be pingable.

<<var_url_boot_software>>

10. Press Enter for the username, indicating no user name.

Enter

- **11.** Enter yes to set the newly installed software as the default to be used for subsequent reboots. y
- **12**. Enter yes to reboot the node.

У

- **13.** When you see "Press Ctrl-C for Boot Menu": Ctrl-C
- 14. To enter Maintenance mode boot, select option 5:

5

- **15.** If you see the question "Continue to Boot?" type yes.
- **16.** To verify the HA status of your environment, enter:

ha-config show



- If either component is not in HA mode, use the ha-config modify command to put the components in HA mode.
- 17. To see how many disks are unowned, enter:

disk show -a



Run Setup Process

When Data ONTAP is installed on a new storage system, the following files are not populated:

- /etc/rc
- /etc/exports
- /etc/hosts
- /etc/hosts.equiv

Controller 1

1. Enter the configuration values the first time you power on the new system. The configuration values populate these files and configure the installed functionality of the system.

I

2. Enter the following information:

Please enter the new hostname []:<<var_controller1>>
Do you want to enable IPv6? [n]: Enter

Do you want to configure interface groups? [n]: Enter

Please enter the IP address for Network Interface e0a []: Enter



Press Enter to accept the blank IP address.

Should interface e0a take over a partner IP address during failover? [n]: Enter Please enter the IP address for the Network Interface e0b []:Enter Should interface e0b take over a partner IP address during failover? [n]: Enter Please enter the IP address for the Network Interface ela []:Enter Should interface ela take over a partner IP address during failover? [n]: Enter Please enter the IP address for the Network Interface elb []:Enter Should interface elb take over a partner IP address during failover? [n]: Enter

Please enter the IP address for Network Interface eOM []: <<var_controller1_e0m_ip>> Please enter the netmaskfor the Network Interface eOM [255.255.255.0]: <<var_controller1_mask>>

Should interface eOM take over a partner IP address during failover? [n]: y Please enter the IPv4 address or interface name to be taken over by eOM []: eOM Please enter flow control for eOM {none, receive, send, full} [full]: Enter

Note

If additional interface cards are installed in your storage controller, you will have additional questions about the interfaces on those cards.

3. Enter the following information:

Please enter the name or IP address of the IPv4 default gateway: <<var_controller1_mgmt_gateway>>

The administration host is given root access to the storage system's / etc files for system administration. To allow /etc root access to all NFS clients enter RETURN below. Please enter the name or IP address for administrative host: <<var_adminhost_ip>>

Please enter timezone [GTM]: <<var_timezone>> Note:Example time zone: America/New_York. Where is the filer located? <<var_location>> Enter the root directory for HTTP files [home/http]: Enter Do you want to run DNS resolver? [n]: y Please enter DNS domain name []: <<var_dns_domain_name>> Please enter the IP address for first nameserver []: <<var_nameserver_ip>> Do you want another nameserver? [n]:

Note

Optionally enter up to three name server IP addresses.

Do you want to run NIS client? [n]: Enter Press the Return key to continue through AutoSupport message Would you like to configure SP LAN interface [y]: Enter Would you like to enable DHCP on the SP LAN interface [y]: n Please enter the IP address for the SP: <<var_sp_ip>> Please enter the netmask for the SP []: <<var_sp_mask>> Please enter the IP address for the SP gateway: <<var_sp_gateway>> Please enter the name or IP address of the mail host [mailhost]: <<var_mailhost>> Please enter the IP address for <<var_mailhost>> []: <<var_mailhost_ip>> New password: <<var_password>> Retype new password <<var_password>>

4. Enter the root password to log in to controller 1.

Controller 2

- 1. Enter the configuration values the first time you power on the new system. The configuration values populate these files and configure the installed functionality of the system.
- 2. Enter the following information:

```
Please enter the new hostname []: <<var_controller2>>
Do you want to enable IPv6? [n]: Enter
Do you want to configure interface groups? [n]: Enter
Please enter the IP address for Network Interface e0a []: Enter
Note:Press Enter to accept the blank IP address.
Should interface e0a take over a partner IP address during failover? [n]: Enter
Please enter the IP address for the Network Interface e0b []:Enter
Should interface e0b take over a partner IP address during failover? [n]: Enter
Please enter the IP address for the Network Interface e1a []:Enter
Should interface e1a take over a partner IP address during failover? [n]: Enter
Please enter the IP address for the Network Interface e1b []:Enter
Should interface e1b take over a partner IP address during failover? [n]: Enter
Please enter the IP address for the Network Interface e1b []:Enter
Should interface e1b take over a partner IP address during failover? [n]: Enter
Please enter the IP address for Network Interface e0M []:
<<var controller2 e0m ip>>
```

```
<<var_controller2_e0m_ip>>
Please enter the netmaskfor the Network Interface e0M [255.255.255.0]:
<<var_controller2_mask>>
```

```
Should interface eOM take over a partner IP address during failover? [n]: y
Please enter the IPv4 address or interface name to be taken over by eOM []: eOM
Please enter flow control for eOM {none, receive, send, full} [full]: Enter
```

Note

If additional interface cards are installed in your storage controller, you will have additional questions about the interfaces on those cards.

3. Enter the following information:

Please enter the name or IP address of the IPv4 default gateway: <<var_controller2_mgmt_gateway>>

The administration host is given root access to the storage system's / etc files for system administration. To allow /etc root access to all NFS clients enter RETURN below.

Please enter the name or IP address for administrative host: <<var_adminhost_ip>>

Please enter timezone [GTM]: <<var_timezone>>
Note:Example time zone: America/New_York.
Where is the filer located? <<var_location>>
Enter the root directory for HTTP files [home/http]: Enter
Do you want to run DNS resolver? [n]: y
Please enter DNS domain name []: <<var_dns_domain_name>>
Please enter the IP address for first nameserver []: <<var_nameserver_ip>>
Do you want another nameserver? [n]:

Note

Optionally enter up to three name server IP addresses.

Do you want to run NIS client? [n]: Enter Press the Return key to continue through AutoSupport message Would you like to configure SP LAN interface [y]: Enter Would you like to enable DHCP on the SP LAN interface [y]: n Please enter the IP address for the SP: <<var_sp_ip>> Please enter the netmask for the SP []: <<var_sp_mask>> Please enter the IP address for the SP gateway: <<var_sp_gateway>> Please enter the name or IP address of the mail host [mailhost]: <<var_mailhost>> Please enter the IP address for <<var_mailhost>> []: <<var_mailhost_ip>> New password: <<var_password>> Retype new password <<var_password>>

4. Enter the root password to log in to controller 2.

Upgrade the Service Processor on Each Node to the Latest Release

With Data ONTAP 8.1.2, you must upgrade to the latest Service Processor (SP) firmware to take advantage of the latest updates available for the remote management device.

- 1. Using a web browser, connect to: http://support.netapp.com/NOW/cgi-bin/fw.
- **2.** Navigate to the Service Process Image for installation from the Data ONTAP prompt page for your storage platform.
- 3. Proceed to the Download page for the latest release of the SP Firmware for your storage platform.
- **4.** Using the instructions on this page, update the SPs on both controllers. You will need to download the .zip file to a web server that is reachable from the management interfaces of the controllers.

64-Bit Aggregates in Data ONTAP 7-Mode

A 64-bit aggregate containing the root volume is created during the Data ONTAP setup process. To create additional 64-bit aggregates, determine the aggregate name, the node on which to create it, and how many disks it will contain. Calculate the RAID group size to allow for roughly balanced (same size) RAID groups of between 12 and 20 disks (for SAS disks) within the aggregate. For example, if 52 disks were being assigned to the aggregate, select a RAID group size of 18. A RAID group size of 18 would yield two 18-disk RAID groups and one 16-disk RAID group. Keep in mind that the default RAID group size is 16 disks, and that the larger the RAID group size, the longer the disk rebuild time in case of a failure.

Controller 1

Execute the following command to create a new aggregate:

aggr create aggr1 -B 64 -r <<var_raidsize>> <<var_#_of_disks>>



Leave at least one disk (select the largest disk) in the configuration as a spare. A best practice is to have at least one spare for each disk type and size.

Controller 2

Execute the following command to create a new aggregate:

aggr create aggr1 -B 64 -r <<var_raidsize>> <<var_#_of_disks>>



Leave at least one disk (select the largest disk) in the configuration as a spare. A best practice is to have at least one spare for each disk type and size.

Flash Cache

Controller 1 and Controller 2

Execute the following commands to enable Flash Cache:

```
options flexscale.enable on
options flexscale.lopri_blocks off
options flexscale.normal_data_blocks on
```



For directions on how to configure Flash Cache in metadata mode or low-priority data caching mode, see TR-3832: Flash Cache and PAM Best Practices Guide at: http://media.netapp.com/documents/tr-3832.pdf. Before customizing the settings, determine whether the custom settings are required or whether the default settings are sufficient.

IFGRP LACP

Since this type of interface group requires two or more Ethernet interfaces and a switch that supports LACP, make sure that the switch is configured properly.

Controller 1 and Controller 2

Run the following command on the command line and also add it to the /etc/rc file, so it is activated upon boot:

```
ifgrp create lacp ifgrp0 -b port ela elb
wrfile -a /etc/rc "ifgrp create lacp ifgrp0 -b ip ela elb"
```



All interfaces must be in down status before being added to an interface group.

VLAN

Controller 1 and Controller 2

Follow these steps to create a VLAN interface for NFS data traffic.

```
vlan create ifgrp0 <<var_nfs_vlan_id>>
wrfile -a /etc/rc "vlan create ifgrp0 <<var_nfs_vlan_id>>"
```

IP Config

Controller 1 and Controller 2

Run the following commands on the command line.

```
ifconfig ifgrp0-<<var_nfs_vlan_id>> <<var_nfs_ip>> netmask <<var_nfs_mask>> mtusize
9000 partner ifgrp0-<<var_nfs_vlan_id>>
wrfile -a /etc/rc " ifconfig ifgrp0-<<var_nfs_vlan_id>> <<var_nfs_ip>> netmask
<<var_nfs_mask>> mtusize 9000 partner ifgrp0-<<var_nfs_vlan_id>>"
```

Cisco Discovery Protocol

Follow these steps to enable Cisco Discovery Protocol (CDP) on controller 1 and controller 2.

Controller 1 and Controller 2

Enable CDP

options cdpd.enable on

Active-Active Controller Configuration

Controller 1 and Controller 2

Enable two storage controllers to an active-active configuration.

- Enter the cluster license on both nodes.
 license add <<var_cf_license>>
- 2. Reboot each storage controller. reboot
- 3. Log back in to both controllers.

Controller 1

Enable failover on Controller 1, if it is not enabled already. cf enable

NFSv3

Controller 1 and Controller 2

1. Add a license for NFS.

license add <<var_nfs_license>>

2. Set the following recommended options that enable NFS version 3.

```
options nfs.tcp.enable on
options nfs.udp.enable off
options nfs.v3.enable on
```

3. Enable NFS.

nfs on

FCP

Controller 1 and Controller 2

1. License FCP.

license add <<var_fc_license>>

2. Start the FCP service.

fcp start

3. Record the WWPN or FC port name for later use.

fcp show adapters

NTP

The following commands configure and enable time synchronization on the storage controller. You must have either a publically available IP address or your company's standard NTP server name or IP address.

Controller 1 and Controller 2

1. Run the following commands to configure and enable the NTP server:

date <<var_date>>

2. Enter the current date in the format of [[[[CC]yy]mm]dd]hhmm[.ss]].

For example: date 201208311436; would set the date to August 31st 2012 at 14:36.

options timed.servers <<var_global_ntp_server_ip>>
options timed.enable on

Data ONTAP SecureAdmin

Secure API access to the storage controller must be configured.

Controller 1

1. Issue the following as a one-time command to generate the certificates used by the Web services for the API.

```
secureadmin setup ssl
SSL Setup has already been done before. Do you want to proceed? [no] y
Country Name (2 letter code) [US]: <<var_country_code>>
State or Province Name (full name) [California]: <<var_state>>
Locality Name (city, town, etc.) [Santa Clara]: <<var_city>>
Organization Name (company) [Your Company]: <<var_org>>
Organization Unit Name (division): <<var_unit>>
Common Name (fully qualified domain name) [<<var_controller1_fqdn>>]: Enter
Administrator email: <<var_admin_email>>
Days until expires [5475] : Enter
Key length (bits) [512] : <<var_key_length>>
Note:NetApp recommends that your key length be 1024.
```

```
After the initialization, the CSR is available in the file /etc/keymgr/csr/secureadmin_tmp.pem.
```

2. Configure and enable SSL and HTTPS for API access using the following options.

```
options httpd.access none
options httpd.admin.enable off
options httpd.admin.ssl.enable on
options ssl.enable on
```

Controller 2

1. Issue the following as a one-time command to generate the certificates used by the Web services for the API.

```
secureadmin setup ssl
SSL Setup has already been done before. Do you want to proceed? [no] y
Country Name (2 letter code) [US]: <<var_country_code>>
State or Province Name (full name) [California]: <<var_state>>
Locality Name (city, town, etc.) [Santa Clara]: <<var_city>>
Organization Name (company) [Your Company]: <<var_org>>
Organization Unit Name (division): <<var_unit>>
Common Name (fully qualified domain name) [<<var_controller2_fqdn>>]: Enter
Administrator email: <<var_admin_email>>
Days until expires [5475] : Enter
Key length (bits) [512] : <<var_key_length>>
```

```
Note
```

NetApp recommends that your key length be 1024.

After the initialization, the CSR is available in the file /etc/keymgr/csr/secureadmin_tmp.pem.

2. Configure and enable SSL and HTTPS for API access using the following options.

```
options httpd.access none
options httpd.admin.enable off
options httpd.admin.ssl.enable on
options ssl.enable on
```

Secure Shell

SSH must be configured and enabled.

Controller 1 and Controller 2

1. Use the following one-time command to generate host keys.

```
secureadmin disable ssh
secureadmin setup -f -q ssh 768 512 1024
```

2. Use the following options to configure and enable SSH.

```
options ssh.idle.timeout 60
options autologout.telnet.timeout 5
```

SNMP

Controller 1 and Controller 2

1. Run the following commands to configure SNMP basics, such as the local and contact information. When polled, this information displays as the sysLocation and sysContact variables in SNMP.

```
snmp contact "<<var_admin_email>>"
snmp location "<<var_location>>"
snmp init 1
options snmp.enable on
```

2. Configure SNMP traps to send them to remote hosts, such as a DFM server or another fault management system.

snmp traphost add <<var_oncommand_server_fqdn>>

SNMPv1

Controller 1 and Controller 2

Note

1. Set the shared secret plain-text password, which is called a community.

```
snmp community delete all
snmp community add ro <<var_snmp_community>>
```

Use the delete all command with caution. If community strings are used for other monitoring products, the delete all command will remove them.

I

SNMPv3

SNMPv3 requires a user to be defined and configured for authentication.

Controller 1 and Controller 2

Create a user called snmpv3user.

```
useradmin role add snmp_requests -a login-snmp
useradmin group add snmp_managers -r snmp_requests
useradmin user add snmpv3user -g snmp_managers
New Password: <<var_password>>
Retype new password: <<var_password>>
```

AutoSupport HTTPS

AutoSupportTM sends support summary information to NetApp through HTTPS.

Controller 1 and Controller 2

Execute the following commands to configure AutoSupport:
```
options autosupport.noteto <<var_admin_email>>
```

Security Best Practices

Apply the following commands according to local security policies.

Controller 1 and Controller 2

Run the following commands to enhance security on the storage controller:

```
options rsh.access none
options webdav.enable off
options security.passwd.rules.maximum 14
options security.passwd.rules.minimum.symbol 1
options security.passwd.lockout.numtries 6
options autologout.console.timeout 5
```

Install Remaining Required Licenses and Enable MultiStore

Controller 1 and Controller 2

Install the following licenses to enable SnapRestore® and FlexClone®.

```
license add <<var_snaprestore_license>>
license add <<var_flex_clone_license>>
options licensed_feature.multistore.enable on
```

Enable NDMP

Run the following commands to enable NDMP.

Controller 1 and Controller 2

options ndmpd.enable on

Create FlexVol Volumes

Controller 1

Follow these steps to create two volumes on controller 1:

```
vol create esxi_boot -s none aggr1 100g
snap reserve esxi_boot 0
sis on /vol/esxi_boot
vol create infra_swap -s none aggr1 100g
snap reserve infra_swap 0
snap sched infra_swap 0 0 0
```

Controller 2

Follow these steps to create two volumes on controller 2:

```
vol create infra_datastore_1 -s none aggr1 500g
snap reserve infra_datastore_1 0
sis on /vol/infra_datastore_1
vol create OnCommandDB -s none aggr1 200g
snap reserve OnCommandDB 0
sis on /vol/OnCommandDB
```

NFS Exports

Follow these steps to create NFS exports on each controller.

Controller 1

```
exportfs -p
sec=sys,rw=<<var_vm_infra01_nfs_host_ip>>:<<var_vm_infra02_nfs_host_ip>>,root=<<var_vm_infra01_nfs_host_ip>>:<<var_vm_infra02_nfs_host_ip>>,nosuid /vol/infra_swap
exportfs -p
```

```
sec=sys,ro,rw=<<var_adminhost_ip>>:<<var_vm_infra01_nfs_host_ip>>:<<var_vm_infra02_nfs
_host_ip>>,root==<<var_adminhost_ip>>:<<var_vm_infra01_nfs_host_ip>>:<<var_vm_infra02_
nfs_host_ip>>,nosuid /vol/vol0
```

Controller 2

```
exportfs -p
sec=sys,rw=<<var_vm_infra01_nfs_host_ip>>:<<var_vm_infra02_nfs_host_ip>>,root=<<var_vm_infra01_nfs_host_ip>>:<<var_vm_infra02_nfs_host_ip>>,nosuid /vol/infra_datastore_1
```

```
exportfs -p
sec=sys,ro,rw=<<var_adminhost_ip>>:<<var_vm_infra01_nfs_host_ip>>:<<var_vm_infra02_nfs
_host_ip>>,root==<<var_adminhost_ip>>:<<var_vm_infra01_nfs_host_ip>>:<<var_vm_infra02_
nfs_host_ip>>,nosuid /vol/vol0
```

I

LUN Creation

Follow these steps to create two LUNs on controller 1.

Controller 1

lun create -s 10g -t vmware -o noreserve /vol/esxi_boot/VM-Host-Infra-01
lun create -s 10g -t vmware -o noreserve /vol/esxi_boot/VM-Host-Infra-02

Server Configuration

FlexPod Cisco UCS Base

Perform Initial Setup of Cisco UCS 6248 Fabric Interconnect for FlexPod Environments

This section provides detailed procedures for configuring the Cisco Unified Computing System (Cisco UCS) for use in a FlexPod environment. The following steps are necessary to provision the Cisco UCS C-Series and B-Series servers and should be followed precisely to avoid improper configuration.

Cisco UCS 6248UP Fabric Interconnect A

To configure the Cisco UCS for use in a FlexPod environment, follow these steps:

1. Connect to the console port on the first Cisco UCS 6248 fabric interconnect.

Enter the configuration method: console Enter the setup mode; setup newly or restore from backup.(setup/restore)? setup You have choosen to setup a a new fabric interconnect? Continue? (y/n): yEnforce strong passwords? (y/n) [y]: y Enter the password for "admin": <<var_password>> Enter the same password for "admin": <<var_password>> Is this fabric interconnect part of a cluster (select 'no' for standalone)? (yes/no) [n]: y Which switch fabric (A|B): A Enter the system name: <<var_ucs_clustername>> Physical switch Mgmt0 IPv4 address: <<var_ucsa_mgmt_ip>> Physical switch Mgmt0 IPv4 netmask: <<var_ucsa_mgmt_mask>> IPv4 address of the default gateway: <<var_ucsa_mgmt_gateway>> Cluster IPv4 address: <<var_ucs_cluster_ip>> Configure DNS Server IPv4 address? (yes/no) [no]: y DNS IPv4 address: <<var_nameserver_ip>> Configure the default domain name? y Default domain name: <<var_dns_domain_name>> Join centralized management environment (UCS Central)? (yes/no) [n]: Enter

- **2.** Review the settings printed to the console. If they are correct, answer yes to apply and save the configuration.
- 3. Wait for the login prompt to make sure that the configuration has been saved.

Cisco UCS 6248UP Fabric Interconnect B

To configure the Cisco UCS for use in a FlexPod environment, follow these steps:

1. Connect to the console port on the second Cisco UCS 6248 fabric interconnect.

Enter the configuration method: console Installer has detected the presence of a peer Fabric interconnect. This Fabric interconnect will be added to the cluster. Do you want to continue {y|n}? y Enter the admin password for the peer fabric interconnect: <<var_password>> Physical switch Mgmt0 IPv4 address: <<var_ucsb_mgmt_ip>> Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): Y

2. Wait for the login prompt to make sure that the configuration has been saved.

FlexPod Cisco UCS FCoE vSphere on Data ONTAP 7-Mode

Log in to Cisco UCS Manager

To log in to the Cisco Unified Computing System (UCS) environment, follow these steps:

- 1. Open a Web browser and navigate to the Cisco UCS 6248 fabric interconnect cluster address.
- 2. Click the Launch UCS Manager link to download the Cisco UCS Manager software.
- 3. If prompted to accept security certificates, accept as necessary.
- 4. When prompted, enter admin as the user name and enter the administrative password.
- 5. Click Login to log in to Cisco UCS Manager.

Upgrade Cisco UCS Manager Software to Version 2.1(1b)

This document assumes the use of Cisco UCS 2.1(1b). To upgrade the Cisco UCS Manager software and the UCS 6248 Fabric Interconnect software to version 2.1(1b), see Cisco UCS Manager Install and Upgrade Guides at: http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/upgrading/from2.0/to2.1/b_UpgradingCi scoUCSFrom2.0To2.1.html

Add Block of IP Addresses for KVM Access

To create a block of IP addresses for server Keyboard, Video, Mouse (KVM) access in the Cisco UCS environment, follow these steps:

Note

This block of IP addresses should be in the same subnet as the management IP addresses for the Cisco UCS Manager.

- 1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
- 2. Choose Pools > root > IP Pools > IP Pool ext-mgmt.
- 3. In the Actions pane, choose Create Block of IP Addresses.
- **4.** Enter the starting IP address of the block and the number of IP addresses required, and the subnet and gateway information.
- 5. Click **OK** to create the IP block.
- 6. Click OK in the confirmation message window.

Synchronize Cisco UCS to NTP

To synchronize the Cisco UCS environment to the NTP server, follow these steps:

- 1. In Cisco UCS Manager, click the Admin tab in the navigation pane.
- 2. Choose All > Timezone Management.
- 3. In the Properties pane, choose the appropriate time zone in the Timezone menu.
- 4. Click Save Changes, and then click OK.
- 5. Click Add NTP Server.

- 6. Enter <<var_global_ntp_server_ip>> and click OK.
- 7. Click OK.

Edit Chassis Discovery Policy

Setting the discovery policy simplifies the addition of B-Series Cisco UCS chassis and of additional fabric extenders for further C-Series connectivity.

To modify the chassis discovery policy, follow these steps:

- 1. In Cisco UCS Manager, click the **Equipment** tab in the navigation pane and choose Equipment in the list on the left.
- 2. In the right pane, click the Policies tab.
- **3.** Under Global Policies, set the Chassis/FEX Discovery Policy to 2-link or set it to match the number of uplink ports that are cabled between the chassis or fabric extenders (FEXes) and the fabric interconnects.
- 4. Set the Link Grouping Preference to Port Channel.
- 5. Click Save Changes.
- 6. Click OK.

Enable Server and Uplink Ports

To enable server and uplink ports, follow these steps:

- 1. In Cisco UCS Manager, click the Equipment tab in the navigation pane.
- 2. Choose Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module.
- **3.** Expand Ethernet Ports.
- 4. Choose the ports that are connected to the chassis or to the Cisco 2232 FEX (two per FEX), right-click them, and choose Configure as Server Port.
- 5. Click Yes to confirm server ports and click OK.
- 6. Verify that the ports connected to the chassis or to the Cisco 2232 FEX are now configured as server ports.

t Summary		New - 🕞 Options	: 🙆 🔒 🔺 Pendir	ng Activities 👩	Exit			
				1	2			
0 6 7 1	>> 👸 Equ	pment 🕨 🎫 Fabric I	Interconnects 🕨 🎫 Fa	bric Interconnect	A (primary) 🕨 🎫 Fi	xed Module 🕨 🗐 Etl	nernet Ports	
	Ethernet	Ports						
ment Servers LAN SAN VM Admin	C Ether			econfigured 🖂	Nahwark 🖂 Samuar	C ECaE Halah	Linified Links 🖂 Appl	line
Filter: Al	encer -	Export @ Print 1		nconingurea 💟	Vecwork V Server	V PODE Opinik V	Onined Opink V Appi	Man
	Slot	Port ID	MAC	If Role	If Type	Overall Status	Administrative State	
=	1	1	54:7F:EE:23:52	Server	Physical	🕇 Up	1 Enabled	
Equipment	. 1	2	54:7F:EE:23:52	Server	Physical	t Up	1 Enabled	
Chassis	1	3	54:7F:EE:23:52	Server	Physical	1 Up	1 Enabled	_
Rack-Mounts	1	4	54:7F:EE:23:52	Server	Physical	1 Up	1 Enabled	
E-M FEX	1	5	54:7F:EE:23:52	Unconfigured	Physical	V Sfp Not Pres	Disabled	1
Servers	1	6	54:7F:EE:23:52	Unconfigured	Physical	V Sfp Not Pres	Disabled	
Fabric Interconnects	1	7	54:7F:EE:23:52	Unconfigured	Physical	V Sfp Not Pres	Disabled	-
Fixed Module	1	8	54:7F:EE:23:52	Unconfigured	Physical	V Sfp Not Pres	Disabled	-
	1	9	54:7F:EE:23:52	Unconfigured	Physical	V Sfp Not Pres	Disabled	-
Port 1	1	10	54:7F:EE:23:52	Unconfigured	Physical	V Sfp Not Pres	Disabled	-
	1	11	54:7F:EE:23:52	Unconfigured	Physical	V Sfp Not Pres	Disabled	-
-I Port 3	1	12	54:7F:EE:23:52	Unconfigured	Physical	V Sfp Not Pres	Disabled	_
	E 1	13	54:7F:EE:23:52	Unconfigured	Physical	V Sfp Not Pres	Disabled	-
	1	14	54:7F:EE:23:52	Unconfigured	Physical	V Sfp Not Pres	Disabled	-
Port 6	1	15	54:7F:EE:23:52	Unconfigured	Physical	V Sfp Not Pres	Disabled	-
Port 7	1	16	54:7F:EE:23:52	Unconfigured	Physical	Sfp Not Pres	Disabled	-
Port 8	1	17	54:7F:EE:23:52	Unconfigured	Physical	V Sfp Not Pres	Disabled	
Port 10	1	18	54:7F:EE:23:52.	Unconfigured	Physical	Sfp Not Pres	Disabled	-
Port 11	1	19	54:7E:EE:23:52	Unconfigured	Physical	Admin Down	Disabled	_
	1	20	54:7E:EE:23:52	Unconfigured	Physical	Admin Down	Disabled	-
	1	21	54·7E·EE·23·52	Unconfigured	Physical	Sto Not Pres		-
	1	22	54-7E-EE-23-52	Unconfigured	Physical	Sfp Not Pres	Disabled	-
	1	23	54-7E-FE-23-52	Unconfigured	Physical	Sto Not Pres		-
	1	24	54:7E:EE:23:52	Unconfigured	Physical	Sfp Not Pres	Disabled	_
- Port 17	1	25	54:7E:EE:23:52	Unconfigured	Physical	Sto Not Pres		_
Port 18	1	25	E4:7E:EE:23:52	Unconfigured	Dhusical	Sto Not Pres	Disabled	_
Port 20	1	27	54.7E.EE.22.52	Unconfigured	Physical	Sto Not Pres	Disabled	_
Port 21	1	29	E4.7E.EE.22.52	Unconfigured	Dhusical	Sto Nak Dros	Disabled	_
Port 22	1	20	54:/F:EE:23:52	Unconfigured	Physical	Cfa Nat Dass	Disabled	
Port 23	1	29	54:/F:EE:23:52	Junconngured	Physical	V Srp Not Pres	 Uisabled 	_

Figure 3 Configured Server Ports

- 7. Choose ports 19 and 20 that are connected to the Cisco Nexus 5548 switches, right-click them, and choose Configure as Uplink Port.
- 8. Click Yes to confirm uplink ports and click OK.
- **9.** Choose ports 31 and 32, which will serve as FCoE uplinks to the Cisco Nexus 5548 switches; right-click them; and choose Configure as FCoE Uplink Port.
- 10. Click Yes to confirm FCoE uplink ports and click OK.
- Choose Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.
- **12.** Expand Ethernet Ports.
- **13.** Choose the ports that are connected to the chassis or to the Cisco 2232 FEX (two per FEX), right-click them, and choose **Configure as Server Port**.
- 14. Click Yes to confirm server ports and click OK.
- **15.** Choose ports 19 and 20 that are connected to the Cisco Nexus 5548 switches, right-click them, and choose **Configure as Uplink Port**.

1

16. Click Yes to confirm the uplink ports and click OK.

- **17.** Choose ports 31 and 32 that will serve as FCoE uplinks to the Cisco Nexus 5548 switches, right-click them, and choose **Configure as FCoE Uplink Port**.
- 18. Click Yes to confirm FCoE uplink ports and click OK.

Acknowledge Cisco UCS Chassis and FEX

To acknowledge all Cisco UCS chassis and external 2232 FEX modules, follow these steps:

- 1. In Cisco UCS Manager, click the **Equipment** tab in the navigation pane.
- 2. Expand Chassis.
- 3. Choose each chassis that is listed, right-click on each chassis and choose Acknowledge Chassis.

Figure 4

ſ

Acknowledging Cisco UCS Chassis



- 4. Click Yes and then click OK to complete acknowledging the chassis.
- 5. If C-Series servers are part of the configuration, expand Rack Mounts and FEX.
- 6. Right-click each FEX that is listed and choose Acknowledge FEX.



Figure 5 Acknowledging Cisco UCS Fabric Extenders

7. Click Yes and then click OK to complete acknowledging the FEX.

Create Uplink Port Channels to Cisco Nexus 5548 Switches

To configure the necessary port channels out of the Cisco UCS environment, follow these steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.



Note In this procedure, two port channels are created: one from fabric A to both Cisco Nexus 5548 switches and one from fabric B to both Cisco Nexus 5548 switches.

- 2. Under LAN > LAN Cloud, expand the Fabric A tree.
- 3. Right-click Port Channels.
- 4. Choose Create Port Channel.
- 5. Enter 13 as the unique ID of the port channel.
- 6. Enter vPC-13-N5548 as the name of the port channel.
- 7. Click Next.

Figure 6 Creating Port Channels

A Create Port Channel	
Unified C	Computing System Manager
Create Port Channel	Set Port Channel Name 0
1. √ <u>Set Port Channel Name</u> 2. □ _{Add Ports}	D: 13
	Name: 0
	< Prev Next > Finish Cancel

- 8. Choose the following ports to be added to the port channel:
 - Slot ID 1 and port 19
 - Slot ID 1 and port 20
- 9. Click >> to add the ports to the port channel.
- **10**. Click **Finish** to create the port channel.
- 11. Click OK.
- 12. In the navigation pane, under LAN > LAN Cloud, expand the fabric B tree.
- 13. Right-click Port Channels.
- **14.** Choose Create Port Channel.
- **15**. Enter 14 as the unique ID of the port channel.
- **16.** Enter vPC-14-N5548 as the name of the port channel.
- 17. Click Next.
- **18.** Choose the following ports to be added to the port channel:
 - Slot ID 1 and port 19
 - Slot ID 1 and port 20
- **19**. Click >> to add the ports to the port channel.
- 20. Click Finish to create the port channel.
- 21. Click OK.

ſ

Create an Organization

Organizations are used to organize resources and restrict access to various groups within the IT organization, thereby enabling multi-tenancy of the compute resources.



Although this document does not assume the use of organizations this procedure provides instructions for creating one.

To configure an organization in the Cisco UCS environment, follow these steps:

- 1. In Cisco UCS Manager, from the New menu in the toolbar at the top of the window, choose Create Organization.
- 2. Enter a name for the organization.
- **3.** (Optional) Enter a description for the organization.
- 4. Click OK.
- 5. Click OK in the confirmation message window.

Create MAC Address Pools

To configure the necessary MAC address pools for the Cisco UCS environment, follow these steps:

- 1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
- 2. Choose **Pools** > **root**.



Note In this procedure, two MAC address pools are created, one for each switching fabric.

- 3. Right-click MAC Pools under the root organization.
- 4. Choose Create MAC Pool to create the MAC address pool.
- **5.** Enter MAC_Pool_A as the name of the MAC pool.
- 6. (Optional) Enter a description for the MAC pool.
- 7. Click Next.
- 8. Click Add.
- 9. Specify a starting MAC address.



Note For the FlexPod solution, the recommendation is to place 0A in the next-to-last octet of the starting MAC address to identify all of the MAC addresses as fabric A addresses.

10. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources.

Figure 7 Creating MAC Address Pool for Fabric A

🌲 Create a Block of MAC Addresses	×
Create a Block of MAC Addresses	0
First MAC Address: 00:25:85:07:0A:00 To ensure uniqueness of MACs in the LAN fabric, you are strongly encouraged to use the following MAC prefix: 00:25:85:xx:xx:xx	Size: 32 🛨
	OK Cancel

- 11. Click OK.
- 12. Click Finish.
- 13. In the confirmation message window, click OK.
- 14. Right-click MAC Pools under the root organization.
- 15. Choose Create MAC Pool to create the MAC address pool.
- **16**. Enter MAC_Pool_B as the name of the MAC pool.
- **17.** (Optional) Enter a description for the MAC pool.
- 18. Click Next.
- 19. Click Add.
- **20.** Specify a starting MAC address.

Note

- For the FlexPod solution, the recommendation is to place 0B in the next to last octet of the starting MAC address to identify all the MAC addresses in this pool as fabric B addresses.
 - **21.** Specify a size for the MAC address pool that is sufficient to support the available blade or server resources.

Figure 8 Creating MAC Address Pool for Fabric B

📥 Create a Block of MAC Addresses	×
Create a Block of MAC Addresses	0
First MAC Address: 00:25:85:07:08:00 To ensure uniqueness of MACs in the LAN fabric, you are strongly encouraged to use the following MAC prefix: 00:25:85:xx:xx:xx	Size: 32 🛨
	OK Cancel

- 22. Click OK.
- 23. Click Finish.
- 24. In the confirmation message window, click OK.

Create WWNN Pools

To configure the necessary World Wide Node Name (WWNN) pools for the Cisco UCS environment, follow these steps:

- 1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
- 2. Choose **Pools** > **root**.
- **3**. Right-click WWNN Pools.
- 4. Choose Create WWNN Pool.
- 5. Enter WWNN_Pool as the name of the WWNN pool.
- 6. (Optional) Add a description for the WWNN pool.
- 7. Click Next.
- 8. Click Add to add a block of WWNNs.
- 9. Keep the default block of WWNNs, or specify a base WWNN.
- **10.** Specify a size for the WWNN block that is sufficient to support the available blade or server resources.

Figure 9 Creating WWNN Pool

🛕 Create WWN Block	— ×
Create WWN Block	0
From: 20:00:00:25:B5:01:00:00 To ensure uniqueness of WWNs in the SAN fabric, you are strongly encouraged to use the following WWN prefix: 20:00:00:25:b5:xx:xx:xx	Size: 32 🜩
	OK Cancel

- 11. Click **OK**.
- 12. Click Finish.
- **13**. Click **OK**.

Create WWPN Pools

To configure the necessary World Wide Port Name (WWPN) pools for the Cisco UCS environment, follow these steps:

1

1. In Cisco UCS Manager, click the SAN tab in the navigation pane.

2. Choose **Pools** > **root**.



In this procedure, two WWPN pools are created: one for fabric A and one for fabric B.

- **3**. Right-click WWPN Pools.
- 4. Choose Create WWPN Pool.
- 5. Enter WWPN_Pool_A as the name of the WWPN pool for fabric A.
- 6. (Optional) Enter a description for this WWPN pool.
- 7. Click Next.
- 8. Click Add to add a block of WWPNs.
- 9. Specify the starting WWPN in the block for fabric A.

- **Note** For the FlexPod solution, the recommendation is to place 0A in the next-to-last octet of the starting WWPN to identify all the WWPNs in this pool as fabric A addresses.
- **10.** Specify a size for the WWPN block that is sufficient to support the available blade or server resources.

Figure 10 Creating WWPN Pool

🖨 Create WWN Block	×
Create WWN Block	Q
From: 20:00:00:25:B5:01:0A:00 To ensure uniqueness of WWNs in the SAN fabric, you are strongly encouraged to use the following WWN prefix: 20:00:00:25:b5:xx:xx:xx	Size: 32
	OK Cancel

- 11. Click OK.
- **12**. Click **Finish** to create the WWPN pool.
- 13. Click OK.
- 14. Right-click WWPN Pools.
- **15.** Choose Create WWPN Pool.
- **16.** Enter WWPN_Pool_B as the name for the WWPN pool for fabric B.
- **17.** (Optional) Enter a description for this WWPN pool.
- 18. Click Next.
- **19**. Click **Add** to add a block of WWPNs.

20. Enter the starting WWPN address in the block for fabric B.



For the FlexPod solution, the recommendation is to place 0B in the next to last octet of the starting WWPN to identify all the WWPNs in this pool as fabric B addresses.

- **21.** Specify a size for the WWPN block that is sufficient to support the available blade or server resources.
- 22. Click OK.
- 23. Click Finish.
- 24. Click OK.

Create UUID Suffix Pool

To configure the necessary universally unique identifier (UUID) suffix pool for the Cisco UCS environment, follow these steps:

- 1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
- 2. Choose **Pools** > **root**.
- 3. Right-click UUID Suffix Pools.
- 4. Choose Create UUID Suffix Pool.
- 5. Enter UUID_Pool as the name of the UUID suffix pool.
- 6. (Optional) Enter a description for the UUID suffix pool.
- 7. Keep the prefix at the derived option.
- 8. Click Next.
- 9. Click Add to add a block of UUIDs.
- 10. Keep the From field at the default setting.
- 11. Specify a size for the UUID block that is sufficient to support the available blade or server resources.

I

Figure 11 Creating UUID Suffix Pool

A Create a Block of UUID Suffixes	×
Create a Block of UUID Suffixes	0
From: 0000-0000000001 Size: 32 -	
OK	Cancel

- 12. Click OK.
- 13. Click Finish.

14. Click OK.

Create Server Pool

To configure the necessary server pool for the Cisco UCS environment, follow these steps:

<u>Note</u>

Consider creating unique server pools to achieve the granularity that is required in your environment.

- 1. In Cisco UCS Manager, click the **Servers** tab in the navigation pane.
- 2. Choose **Pools** > **root**.
- **3**. Right-click Server Pools.
- 4. Choose Create Server Pool.
- 5. Enter Infra_Pool as the name of the server pool.
- 6. (Optional) Enter a description for the server pool.
- 7. Click Next.
- 8. Choose two servers to be used for the VMware management cluster and click >> to add them to the Infra_Pool server pool.
- 9. Click Finish.
- 10. Click OK.

Create VLANs

To configure the necessary virtual local area networks (VLANs) for the Cisco UCS environment, follow these steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.



te In this procedure, five VLANs are created.

- 2. Choose LAN > LAN Cloud.
- **3.** Right-click VLANs.
- 4. Choose Create VLANs.
- 5. Enter IB-MGMT-VLAN as the name of the VLAN to be used for management traffic.
- 6. Keep the Common/Global option selected for the scope of the VLAN.
- 7. Enter <<var_ib-mgmt_vlan_id>> as the ID of the management VLAN.
- 8. Keep the Sharing Type as None.
- 9. Click OK, and then click OK again.

Create VLANs			×
Create VLANS			v
VLAN Name/Prefix: IB-MGMT-VLAN			
Multicast Policy Name: <not set=""></not>			
⊙ Common/Global C Fabric A C Fabric B C Both Fabrics Configured Differently			
You are creating global VLANs that map to the same VLAN IDs in all available fabrics.			
Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")			
VLAN IDs: 3175			
Sharing Type: 💽 None 🔿 Primary 💭 Isolated			
	Check Overlap	OK _	Cancel

Figure 12 Creating VLAN for Management Traffic

1

1

- 10. Right-click VLANs.
- 11. Choose Create VLANs.
- 12. Enter NFS-VLAN as the name of the VLAN to be used for NFS.
- **13.** Keep the Common/Global option selected for the scope of the VLAN.
- **14.** Enter the <<var_nfs_vlan_id>> for the NFS VLAN.
- **15.** Keep the Sharing Type as None.
- 16. Click OK, and then click OK again.

Create VLANs	0
VLAN Name/Prefix: NF5-YLAN Multicast Policy Name: <not set=""> Create Multicast Policy</not>	
Common/Global C Fabric A C Fabric B C Both Fabrics Configured Differently	
You are creating global VLANs that map to the same VLAN IDs in all available fabrics. Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")	
VLAN IDs: 3170	
Sharing Type: Toolie Continuity Consoled	
Che	.Overlap OK Cancel

Figure 13 Creating VLAN for NFS Traffic

- **17.** Right-click VLANs.
- **18.** Choose Create VLANs.
- $\label{eq:linear} \textbf{19.} \quad \text{Enter vMotion-VLAN} \text{ as the name of the VLAN to be used for vMotion.}$
- **20.** Keep the Common/Global option selected for the scope of the VLAN.
- **21**. Enter the <<var_vmotion_vlan_id>> as the ID of the vMotion VLAN.
- **22**. Keep the Sharing Type as None.
- 23. Click OK, and then click OK again.
- 24. Right-click VLANs.

ſ

- **25.** Choose Create VLANs.
- **26.** Enter VM-Traffic-VLAN as the name of the VLAN to be used for the VM traffic.
- **27.** Keep the Common/Global option selected for the scope of the VLAN.
- **28.** Enter the <<var_vm-traffic_vlan_id>> for the VM Traffic VLAN.

- **29**. Keep the Sharing Type as None.
- **30**. Click **OK**, and then click **OK** again.

🛕 Create VLANs	
Create VLANs	0
VLAN Name/Prefix: VM-Traffic-VLAN	
Multicast Policy Name: <not set=""></not>	
Common/Global Fabric A Fabric B Both Fabrics Configured Differently	
You are creating global VLANs that map to the same VLAN IDs in all available fabrics.	
Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")	
VLAN IDs: 3174	
Sharing Type: None Primary Isolated	
Check Overla	p OK Cancel

Figure 14 Creating VLAN for VM Traffic

1

- **31**. Right-click VLANs.
- 32. Choose Create VLANs.
- **33.** Enter Native-VLAN as the name of the VLAN to be used as the native VLAN.
- 34. Keep the Common/Global option selected for the scope of the VLAN.
- **35.** Enter the <<var_native_vlan_id>> as the ID of the native VLAN.
- **36.** Keep the Sharing Type as None.
- 37. Click OK, and then click OK again.

📥 Create VLANs	
Create VLANs	0
VLAN Name/Prefix: Native-VLAN	
Common/Global Fabric A Fabric B Both Fabrics Configured Differently	
You are creating global VLANs that map to the same VLAN IDs in all available fabrics.	
Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45") VLAN IDs: 2	
Sharing Type: None Primary Isolated	
	Check Overlap OK Cancel

Figure 15 Creating Native VLAN

- **38.** Expand the list of VLANs in the navigation pane, right-click the newly created Native-VLAN and choose Set as Native VLAN.
- **39**. Click **Yes**, and then click **OK**.

Create VSANs and FCoE Port Channels

I

To configure the necessary virtual storage area networks (VSANs) and FCoE uplink port channels for the Cisco UCS environment, follow these steps:

- 1. In Cisco UCS Manager, click the ${\bf SAN}$ tab in the navigation pane.
- 2. Expand the SAN > SAN Cloud tree.
- 3. Right-click VSANs.
- 4. Choose Create VSAN.
- 5. Enter VSAN_A as the name of the VSAN for fabric A.

- 6. Keep the Disabled option selected for FC Zoning.
- 7. Click the Fabric A radio button.
- 8. Enter <<var_vsan_a_id>> as the VSAN ID for fabric A.
- **9.** Enter <<var_fabric_a_fcoe_vlan_id>> as the FCoE VLAN ID for fabric A.



Note For the FlexPod solution, it is recommended to use the same ID for the VSAN and the FCoE VLAN required for fabric A.

1

10. Click OK, and then click OK again to create the VSAN.

Figure 16 Creating VSAN for Fabric A

📥 Create VSAN	
Create VSAN	0
Name: VSAN_A	
FC Zoning Settings	
FC Zoning: O Disabled C Enabled	
Do NOT enable zoning for this VSAN if the fabric interconner upstream switch that has zoning enabled on the same VSAN	t is connected to an
🔿 Common/Global 💿 Fabric A 🕥 Fabric B 🔿 Both Fabric	s Configured Differently
You are creating a local VSAN in fabric 4 that many to	A VI AM can be used to carry ECoE traffic and can be manual
a VSAN ID that exists only in fabric A.	to this VSAN.
Enter the VSAN ID that maps to this VSAN.	Enter the VLAN ID that maps to this VSAN.
VSAN ID: 101	FCoE VLAN: 101
	OK Cancel

- 11. Right-click VSANs.
- **12.** Choose Create VSAN.
- **13.** Enter VSAN_B as the name of the VSAN for fabric B.
- 14. Keep the Disabled option selected for FC Zoning.

- **15.** Click the **Fabric B** radio button.
- **16.** Enter <<var_vsan_b_id>> as the VSAN ID for fabric B.
- **17.** Enter <<var_fabric_b_fcoe_vlan_id>> as the FCoE VLAN ID for fabric B.



18. Click OK, and then click OK again to create the VSAN.

Figure 17 Creating VSAN for Fabric B

📥 Create VSAN	
Create VSAN	0
Name: VSAN_B	
FC Zoning Settings	
FC Zoning: Disabled Enabled	
Do NOT enable zoning for this VSAN if the fabric interconnect upstream switch that has zoning enabled on the same VSAN.	t is connected to an
Common/Global Fabric A Fabric B Fabric B	s Configured Differently
You are creating a local VSAN in Fabric B that maps to a VSAN ID that exists only in fabric B.	A VLAN can be used to carry FCoE traffic and can be mapped to this VSAN.
Enter the VSAN ID that maps to this VSAN.	Enter the VLAN ID that maps to this VSAN.
VSAN ID: 102	FCoE VLAN: 102
	OK Cancel

- **19**. In the navigation pane, under **SAN** > **SAN** Cloud, expand the Fabric A tree.
- 20. Right-click FCoE Port Channels.
- **21**. Choose Create FCoE Port Channel.
- **22.** Enter 1 for the port channel ID and Po1 for the port channel name.
- 23. Click Next.

ſ

24. Choose ports 31 and 32 and click >> to add the ports to the port channel.

- 25. Click Finish.
- 26. check the check box for Show Navigator for FCoE Port-Channel 1 (Fabric A).
- **27.** Click **OK** to create the port channel.
- 28. In the right pane, under Properties, choose VSAN VSAN_A for Fabric A in the VSAN list.
- **29.** Click **Apply**, and then click **OK**.
- 30. Click OK to close the navigator.
- 31. In the navigation pane, under SAN > SAN Cloud, expand the fabric B tree.
- 32. Right-click FCoE Port Channels.
- **33.** Choose Create FCoE Port Channel.
- **34.** Enter 2 for the port channel ID and Po2 for the port channel name.
- 35. Click Next.
- **36.** Choose ports 31 and 32 and click >> to add the ports to the port channel.
- 37. Click Finish.
- **38.** Check the check box for Show Navigator for FCoE Port-Channel 2 (Fabric B).
- **39**. Click **OK** to create the port channel.
- 40. In the right pane, under Properties, choose VSAN VSAN_B for Fabric B.
- 41. Click Apply, and then click OK.
- 42. Click OK to close the navigator.

Create Host Firmware Package

Firmware management policies allow the administrator to select the corresponding packages for a given server configuration. These policies often include packages for adapter, BIOS, board controller, FC adapters, host bus adapter (HBA) option ROM, and storage controller properties.

To create a firmware management policy for a given server configuration in the Cisco UCS environment, follow these steps:

1

- 1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
- 2. Choose **Policies** > **root**.
- 3. Right-click Host Firmware Packages.
- 4. Choose Create Host Firmware Package.
- 5. Enter VM-Host-Infra as the name of the host firmware package.
- 6. Keep the radio button Simple selected.
- 7. Choose the version 2.1(1b) for both the Blade and Rack Packages.
- 8. Click **OK** to create the host firmware package.
- 9. Click OK.

	Figure 18	Creating Host Firmware Package	
🌲 Create Host Firmwa	re Package		×
Create Host I	Firmware Pa	ackage	0
Name: VM-Host-	-Infra	_	
Description:			
Hov	w would you like to a	configure the Host Firmware Package? 💿 Simple 🔘 Advance	d
Blade Package: 2.1(1b)	B 💌		
Rack Package: 2.1(1b)	IC 🔽		
		r	
			OK Cancel

Set Jumbo Frames in Cisco UCS Fabric

40

.

D. . /......

To configure jumbo frames and enable quality of service in the Cisco UCS Fabric, follow these steps:

- 1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
- 2. Choose LAN > LAN Cloud > QoS System Class.
- **3**. In the right pane, click the **General** tab.
- 4. On the Best Effort row, enter 9216 in the box under the MTU column.
- 5. Click Save Changes.
- 6. Click OK.

Γ

	🕒 🔘 🖬 New -	D Option	s 🕜 🕻	Pending Ad	tivities 🛛 👩 Exit					
V 🔼 🖾										
0 18 7 3	>> = LAN • 🙆 L	AN Cloud >	1 QoS 5	System Class					T Qo	5 System C
ipment Servers LAN SAN VM Admin	General Events F	SM								
Filter: All	Priority	Enabled	CoS	Packet Drop	Weight		Weight (%)	мти		Multicas
	Platinum		5		10	-	N/A	normal	-	
	Gold		4	V	9	-	N/A	normal	-	
- CLAN Cloud	Silver		2		8	-	N/A	normal	-	
E-ES Fabric A	Sirver		-		•		iva.	norma		-
	Bronze		1		7	•	N/A	normal	•	
Port-Channel 13 (vPC-13-N5548	Best Effort		Any		5	-	50	9216	-	
VI AN Optimization Sets	Fibre Channel		3		5	-	50	fc	-	N/A
VLANs										
- Tabric B										
Ort Channels										
Port-Chappel 14 (vPC-14-N5548										
The Televence 1/10										
Eth Interface 1/19										
Eth Interface 1/20										
Uplink Eth Interraces										
VLAN Optimization Sets										
VLANs										
QoS System Class										
QoS System Class										
VLANS VCOS System Class LAN Pin Groups SThreshold Policies										
VLANS VLANS VLANS VLANS VLANS VLANS VLAN Pin Groups VLAN Pin Groups VLAN Groups VLAN Groups										
VLANS VLANS VLAN Groups LAN Pin Groups VLAN Groups VLAN Groups VLAN Groups VLAN Groups VLAN Groups VLAN Groups										
VLANS VLAN S VLAN S VLAN Fin Groups VLAN S										
VLANS VGS System Class LAN Pin Groups VLAN Groups VLAN Groups VLAN MGMT-VLAN (3175) VLAN MGMT-VLAN (3175)										
VLANS QOS System Class LAN Pin Groups WLAN Groups VLAN Groups VLAN Groups VLAN MGMT-VLAN (3175) VLAN NFS-VLAN (3170)										
VLANS VLANS VLAN Pin Groups VLAN Groups VLAN Groups VLAN MGMT-VLAN (3175) VLAN NFS-VLAN (3170) VLAN Native-VLAN (2)										
VLANS VLANS VLANS VLAN Groups VLAN Groups VLAN Groups VLAN Groups VLAN S VLAN NGMT-VLAN (3175) VLAN NFS-VLAN (3170) VLAN Native-VLAN (2) VLAN VLATVE-CTI-VLAN (3176)										
VLANS VLANS VLANS VLANS VLAN Groups VLAN Groups VLAN Groups VLAN Groups VLAN S VLAN NFS-VLAN (3175) VLAN NS5-VLAN (3170) VLAN Native-VLAN (2) VLAN Vkt-Ctrl-VLAN (3176) VLAN VM-Traffic-VLAN (3174)										
VLANS VLAN Fin Groups VLAN Fin Groups VLAN Groups VLAN Groups VLAN MGMT-VLAN (3175) VLAN NFS-VLAN (3170) VLAN NFS-VLAN (2176) VLAN NFL-Ctrl-VLAN (3176) VLAN VM-Traffic-VLAN (3174) VLAN MGfradfit (1)										
VLANS VLANS VLAN Groups VLAN Groups VLAN Groups VLAN Groups VLAN S VLAN NS-VLAN (3175) VLAN NS-VLAN (3170) VLAN NS-VLAN (3176) VLAN VM-Traffic-VLAN (3174) VLAN default (1) VLAN default (1) VLAN VM-Traffic-VLAN (3173)										
VLANs VLANs VLANs VLANs VLAN Pin Groups VLAN Groups VLAN Groups VLAN Groups VLAN MGMT-VLAN (3175) VLAN NS-VLAN (3170) VLAN NAtive-VLAN (2) VLAN VL-Crt-VLAN (3176) VLAN VM-Traffic-VLAN (3174) VLAN default (1) VLAN vMotion-VLAN (3173)										
VLANs VLAN Groups VLAN Groups VLAN Groups VLAN MGMT-VLAN (3175) VLAN MGMT-VLAN (3175) VLAN NFS-VLAN (3170) VLAN NATive-VLAN (2) VLAN VAN-Traffic-VLAN (3174) VLAN VAN-Traffic-VLAN (3174) VLAN vMoton-VLAN (3173)										
VLAN s VLAN Groups VLAN Groups VLAN Groups VLAN Groups VLAN Groups VLAN S VLAN MGMT-VLAN (3175) VLAN NFS-VLAN (3170) VLAN NAIVe-VLAN (3170) VLAN VI-traffic-VLAN (3174) VLAN VI-traffic-VLAN (3174) VLAN VI-traffic-VLAN (3173) VLAN VI-traffic-VLAN (3173) Appliances Internal LAN										
VLAN S VLAN Fin Groups VLAN Groups VLAN Groups VLAN Groups VLAN MGMT-VLAN (3175) VLAN NFS-VLAN (3177) VLAN NAtive-VLAN (3176) VLAN NAtive-VLAN (3174) VLAN vMotion-VLAN (3173) VLAN vMotion-VLAN (3173) VLAN vMotion-VLAN (3173) Internal LAN Internal Fabric A					11					
VLANS VLANS VLANS VLANS VLAN Pin Groups VLAN Groups VLAN Groups VLAN Groups VLAN S VLAN MGMT-VLAN (3175) VLAN NF5-VLAN (3170) VLAN NAtive-VLAN (3176) VLAN VM-Traffic-VLAN (3174) VLAN vMotion-VLAN (3173) Appliances Internal Fabric A Internal Fabric A Internal Fabric B	4				m					
VLANS VLANS VLAN Pin Groups VLAN Groups VLAN Groups VLAN MGMT-VLAN (3175) VLAN MGMT-VLAN (3175) VLAN NFS-VLAN (3170) VLAN NFS-VLAN (3170) VLAN NHC-CH-VLAN (3176) VLAN VM-Traffic-VLAN (3174) VLAN VMotion-VLAN (3173) Appliances Internal LAN Appliances Internal Fabric A Internal Fabric B Internal Fabri	4				11			Save Changes	Re	set Values

Figure 19 Setting Jumbo Frame

Create Local Disk Configuration Policy (Optional)

A local disk configuration for the Cisco UCS environment is necessary if the servers in the environment do not have a local disk.



This policy should not be used on servers that contain local disks.

To create a local disk configuration policy, follow these steps:

- 1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
- 2. Choose **Policies** > **root**.
- 3. Right-click Local Disk Config Policies.
- 4. Choose Create Local Disk Configuration Policy.
- 5. Enter SAN-Boot as the local disk configuration policy name.

6. Change the mode to No Local Storage.

Figure 20

7. Click **OK** to create the local disk configuration policy.

Creating Local Disk Configuration Policy

	,
🛕 Create Local Disk Configuration Policy	— ×
Create Local Disk Configuration Policy	0
·····,	
Name: SAN-Boot	
Description:	
Mode: No Local Storage	
	OK Cancel

8. Click OK.

ſ

Create Network Control Policy for Cisco Discovery Protocol

To create a network control policy that enables Cisco Discovery Protocol (CDP) on virtual network ports, follow these steps:

- 1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
- 2. Choose **Policies** > **root**.
- 3. Right-click Network Control Policies.
- 4. Choose Create Network Control Policy.
- 5. Enter Enable_CDP as the policy name.

- 6. For CDP, choose the Enabled option.
- 7. Click **OK** to create the network control policy.

Figure 21 Creating Network Control Policy

🌲 Create Network C	ontrol Policy	×
Create Netv	vork Control Policy	0
Name:	Enable_CDP	
CDP:	C Disabled C Enabled	
MAC Register Mode:	Only Native Vlan C All Host Vlans	
Action on Uplink Fail:	Eink Down C Warning	
Forge: C Allow	C Deny	
		OK Cancel

8. Click OK.

Create Power Control Policy

To create a power control policy for the Cisco UCS environment, follow these steps:

- 1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
- 2. Choose **Policies** > **root**.
- 3. Right-click Power Control Policies.
- 4. Choose Create Power Control Policy.
- 5. Enter No-Power-Cap as the power control policy name.
- 6. Change the power capping setting to No Cap.
- 7. Click **OK** to create the power control policy.
- 8. Click OK.

Figure 22 Creating Power Control Policy

Create Power C	ontrol Policy	x
Create Po	wer Control Policy	Ø
Name: No-I	ower-Can	
Description:		
Power Cappin		
If you choose of its power group choose no-cap	 ap, the server is allocated a certain amount of power based on its priority within Priority values range from 1 to 10, with 1 being the highest priority. If you the server is exempt from all power capping. cap 	
Cisco UCS Manage power than is curr their priority.	r only enforces power capping when the servers in a power group require more ently available. With sufficient power, all servers run at full capacity regardless of	
	OK	el

Create Server Pool Qualification Policy (Optional)

To create an optional server pool qualification policy for the Cisco UCS environment, follow these steps:

6, Note

ſ

This example creates a policy for a B200-M3 server.

- 1. In Cisco UCS Manager, click the **Servers** tab in the navigation pane.
- 2. Choose **Policies** > **root**.
- 3. Right-click Server Pool Policy Qualifications.
- 4. Choose Create Server Pool Policy Qualification.
- 5. Enter UCSB-B200-M3 as the name for the policy.
- 6. Choose Create Server PID Qualifications.
- 7. Enter UCSB-B200-M3 as the PID.
- 8. Click **OK** to create the server pool qualification policy.
- 9. Click OK, and then click OK again.

	Figure 23	Creating Server P	ID Qualifications
🛕 Create Server PID	Qualifications		— ×-
Create Serv	/er PID Quali	fications	0
PID (RegEx): UCSB	-B200-M3		
			OK Cancel

Create Server BIOS Policy

To create a server BIOS policy for the Cisco UCS environment, follow these steps:

1

- 1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
- 2. Choose **Policies** > **root**.
- **3**. Right-click BIOS Policies.
- 4. Choose Create BIOS Policy.
- 5. Enter VM-Host-Infra as the BIOS policy name.
- 6. Change the Quiet Boot setting to Disabled.
- 7. Click **Finish** to create the BIOS policy.

1 iyuit 24

Creating BIOS Policy

Create BIOS Policy	Main	0
Y Main Processor Intel Directed IO RAS Memory Serial Port USB PCI Configuration Boot Options Server Management	Name: Reboot on BIOS Settings Change: Quiet Boot: Quiet Boot: Ost Error Pause: Ostabled Post Error Pause: Stay-off Iast-state Pront Panel Lockout: Ostabled Isabled Patform Default Pront Panel Lockout: Isabled Platform Default Platform Defaul	

8. Click OK.

I

Create vNIC/vHBA Placement Policy for Virtual Machine Infrastructure Hosts

To create a vNIC/vHBA placement policy for the infrastructure hosts, follow these steps:

- 1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
- 2. Choose **Policies** > **root**.
- 3. Right-click vNIC/vHBA Placement Policies.
- 4. Choose Create Placement Policy.
- 5. Enter VM-Host-Infra as the name of the placement policy.
- 6. Click 1 and Choose Assigned Only.
- 7. Click OK, and then click OK again.

	Figure 25	Creating Placemo	ent Polic
Create Placement Pol	icy		×
Create Placer	nent Policy	/	0
Na Virtual Slot Mapping Sche 4 Filter 👄 Export 没	me: VM-Host-Infr me: Round Rob	'a in ○ Linear Ordered	1
Virtual Slot	Selection	n Preference	
1	Assigne	d Only	
2	All		
3	All		
4	All		

Update default Maintenance Policy

To update the default Maintenance Policy, follow these steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.

1

1

- 2. Choose **Policies** > **root**.
- **3**. Choose **Maintenance Policies** > **default**.
- 4. Change the Reboot Policy to User Ack.
- 5. Click Save Changes.
- 6. Click **OK** to accept the change.



Figure 26 Updating Maintenance Policy

Create vNIC Templates

To create multiple virtual network interface card (vNIC) templates for the Cisco UCS environment, follow these steps:

- 1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
- 2. Choose **Policies** > **root**.
- **3**. Right-click vNIC Templates.
- 4. Choose Create vNIC Template.
- 5. Enter vNIC_Template_A as the vNIC template name.
- 6. Keep the radio button Fabric A selected.
- 7. Do not check the Enable Failover check box.
- 8. Under Target, make sure that the VM check box is not checked.
- 9. Click the Updating Template radio button as the Template Type.
- **10.** Under VLANs, check the check boxes for IB-MGMT-VLAN, NFS-VLAN, Native-VLAN, VM-Traffic-VLAN, and vMotion-VLAN.

- **11.** Set Native-VLAN as the native VLAN.
- **12**. For MTU, enter 9000.
- **13**. In the MAC Pool list, Choose MAC_Pool_A.
- 14. In the Network Control Policy list, Choose Enable_CDP.

1

- **15.** Click **OK** to create the vNIC template.
- 16. Click OK.

Figure 27 Creating vNIC Template for Fabric A

📥 Create vNIC Template					×
Create vNIC Temp	olate				0
Name:	vNIC_Template_	_A	_		<u>^</u>
Fabric ID:	Fabric A C F	abric B 🦵 Er	able Failover		
	Target ▼ Adapter ↓ VM				
Warning If VM is selected, a port profile If a port profile of the same nam	by the same name w ne exists, and updati	vill be created. ing template is	selected, it will be overwrit	iten	
Template Type:	C Initial Template	e 💿 Updatin	g Template		
Select	Name		Native VI AN	(m)	
	default		C.		
	IB-MGMT-VLAN		C C		
<u>v</u>	NFS-VLAN		C		
V	Native-VLAN		۹	-	
	·		*		
Create VLAN	9000				
MAC Pool:	MAC_Pool_A	-			
QoS Policy:	<pre> () (not set>) </pre>	-			
Network Control Policy:	Enable_CDP	-			
Pin Group:	() <not set=""></not>	-			
Stats Threshold Policy	default	-			
Dupamic WIC Connection Policy		-			
Dynamic wate connection Policy:	100500				-
				ОК	Cancel

- 17. In the navigation pane, click the LAN tab.
- **18**. Choose **Policies** > **root**.

- 19. Right-click vNIC Templates.
- 20. Choose Create vNIC Template.
- **21.** Enter vNIC_Template_B as the vNIC template name.
- 22. Click the radio button Fabric B.
- **23**. Do not check the Enable Failover check box.
- 24. Under Target, make sure the VM check box is not checked.
- 25. Click the Updating Template radio button as the template type.
- **26.** Under VLANs, check the check boxes for IB-MGMT-VLAN, NFS-VLAN, Native-VLAN, VM-Traffic-VLAN, and vMotion-VLAN.
- 27. Set Native-VLAN as the native VLAN.
- **28**. For MTU, enter 9000.
- **29**. In the MAC Pool list, Choose MAC_Pool_B.
- **30.** In the Network Control Policy list, Choose Enable_CDP.
- **31**. Click **OK** to create the vNIC template.
- 32. Click OK.

ſ

	[
Name	vNIC_Template_B			_
Description	:			
Fabric ID	🗧 🔿 Fabric A 💿 Fabric B	Enable Failover		
	0 Target			
	Adapter			
	<u> </u>			
Warning				
f VM is selected, a port profile	by the same name will be cr	eated.		
t a port profile of the same na	me exists, and updating tem	plate is selected, it will be overwrit	tten	
t a port profile of the same na	me exists, and updating tem	plate is selected, it will be overwrit	tten	
r a port profile of the same na Template Type	me exists, and updating tem	plate is selected, it will be overwril pdating Template	tten	
r a port profile of the same na Template Type VLANs	me exists, and updating tem	plate is selected, it will be overwril pdating Template	tten	
r a port profile of the same na Template Type VLANs Select	me exists, and updating tem	plate is selected, it will be overwril pdating Template Native VLAN	tten	
r a port profile of the same na Template Type VLANs Select	me exists, and updating tem	plate is selected, it will be overwrit pdating Template Native VLAN	tten	
r a port profile of the same na Template Type VLANs Select	me exists, and updating tem Initial Template © U Name default IB-MGMT-VLAN	plate is selected, it will be overwril pdating Template Native VLAN	Iten	
r a port profile of the same na Template Type VLANS Select I	Me exists, and updating tem	plate is selected, it will be overwrit pdating Template Native VLAN C C C	Iten	
T a port profile of the same na Template Type VLANS Select Select VLANS Select	me exists, and updating tem	plate is selected, it will be overwrit pdating Template Native VLAN C C C C C	tten	
T a port profile of the same na Template Type VLANS Select	Me exists, and updating tem	plate is selected, it will be overwrit pdating Template Native VLAN C C C	tten	
Template Type VLANS Select VLANS Create VLAN	me exists, and updating tem	plate is selected, it will be overwrit pdating Template Native VLAN O O O O	tten	
r a port profile of the same na Template Type VLANS Select Select VLANS Create VLAN	me exists, and updating tem	plate is selected, it will be overwrit pdating Template Native VLAN O O O O	tten	
r a port profile of the same na Template Type VLANS Select	me exists, and updating tem	plate is selected, it will be overwrit pdating Template Native VLAN C C C C	Iten	
r a port profile of the same na Template Type VLANS Select VLANS Create VLAN MTU MAC Pool OoS Policy	me exists, and updating tem	plate is selected, it will be overwrit pdating Template Native VLAN C C C	tten	
r a port profile of the same na Template Type VLANS Select VLANS Create VLAN MTU MAC Pool QoS Policy	me exists, and updating tem	plate is selected, it will be overwrit pdating Template Native VLAN C C C	tten	
r a port profile of the same na Template Type VLANS Select Create VLAN MTU MAC Pool QoS Policy Network Control Policy	me exists, and updating tem	plate is selected, it will be overwrit pdating Template Native VLAN C C C	tten	
r a port profile of the same na Template Type VLANS Select Create VLAN MAC Pool QoS Policy Network Control Policy Pin Group	me exists, and updating tem	plate is selected, it will be overwrit pdating Template Native VLAN O O O O	tten	
It a port profile of the same na Template Type VLANS Select Select Create VLAN Create VLAN MAC Pool QoS Policy Network Control Policy Pin Group Stats Threshold Policy	me exists, and updating tem Initial Template © U Name default IB-MGMT-VLAN NFS-VLAN NFS-VLAN Native-VLAN MAC_Pool_B Cnot set> Cnot set Cnot set Cnot set Cnot set Cnot set Cnot set Cnot set Cno	plate is selected, it will be overwrit pdating Template Native VLAN O O O O	tten	

Figure 28 Creating vNIC Template for Fabric B

1

Create vHBA Templates for Fabric A and Fabric B

To create multiple virtual host bus adapter (vHBA) templates for the Cisco UCS environment, follow these steps:

- 1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
- 2. Choose **Policies** > **root**.
- **3**. Right-click vHBA Templates.
- 4. Choose Create vHBA Template.
- **5.** Enter vHBA_Template_A as the vHBA template name.

- 6. Click the radio button Fabric A.
- 7. In the Select VSAN list, Choose VSAN_A.
- 8. In the WWPN Pool list, Choose WWPN_Pool_A.
- 9. Click **OK** to create the vHBA template.
- 10. Click OK.

Figure 29 Creating vHBA Template for Fabric A

📥 Create vHBA Templat	e	— ×
Create vHBA	Template	0
Name:	vHBA_Template_A	
Description:		
Fabric ID:	• A • B	
Select VSAN:	VSAN_A	🛨 Create VSAN
Template Type:	Initial Template Updating Template	
Max Data Field Size:	2048	
WWPN Pool:	WWPN_Pool_A	
QoS Policy:	<not set=""></not>	
Pin Group:	<not set=""></not>	
Stats Threshold Policy:	default 📉 🔽	
		OK Cancel

- **11**. In the navigation pane, click the **SAN** tab.
- **12**. Choose **Policies** > **root**.
- **13.** Right-click vHBA Templates.
- 14. Choose Create vHBA Template.
- **15.** Enter vHBA_Template_B as the vHBA template name.
- **16**. Click the radio button **Fabric B**.
- 17. In the Select VSAN list, Choose VSAN_B.
- **18**. In the WWPN Pool, Choose WWPN_Pool_B.
- **19**. Click **OK** to create the vHBA template.
- 20. Click OK.

I

F	igure 30	Creating vHBA Template for Fabric B	
📥 Create vHBA Templa	te		—
Create vHBA	Template		0
Name:	vHBA_Template	<u>_</u> B	
Description:			
Fabric ID:	🔿 A 💿 B		
Select VSAN:	UVSAN_B	•	🛨 Create VSAN
Template Type:	 Initial Template 	e 🕜 Updating Template	
Max Data Field Size:	2048		
WWPN Pool:	WWPN_Pool_B		
QoS Policy:	<not set=""></not>	-	
Pin Group:	<not set=""></not>		
Stats Threshold Policy:	default		
			OK Cancel

Create Boot Policies

This procedure applies to a Cisco UCS environment in which the storage FCoE ports are configured in the following ways:

- The FCoE ports 1a on storage controllers 1 and 2 are connected to the Cisco Nexus 5548 switch A.
- The FCoE ports 1b on storage controllers 1 and 2 are connected to the Cisco Nexus 5548 switch B.

Two boot policies are configured in this procedure:

- The first configures the primary target to be FCoE port 1a on storage controller 1.
- The second configures the primary target to be FCoE port 1b on storage controller 1.

To create boot policies for the Cisco UCS environment, follow these steps:

- 1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
- 2. Choose **Policies** > **root**.
- 3. Right-click Boot Policies.
- 4. Choose Create Boot Policy.
- 5. Enter Boot-Fabric-A as the name of the boot policy.
- 6. (Optional) Enter a description for the boot policy.
- 7. Keep the Reboot on Boot Order Change check box unchecked.
- 8. Expand the Local Devices drop-down menu and Choose Add CD-ROM.
- 9. Expand the vHBAs drop-down menu and Choose Add SAN Boot.
- 10. In the Add SAN Boot dialog box, enter Fabric-A in the vHBA field.
- 11. Make sure that the Primary radio button is selected as the SAN boot type.
- 12. Click OK to add the SAN boot initiator.

Figure 31 Adding SAN Boot Initiator for Fabric A

📥 Add SAN	Boot		×
Add S	AN Boot		0
vHBA: Fa	bric-A Primary C Secondary		
		ОК	Cancel

- 13. From the vHBA drop-down menu, choose Add SAN Boot Target.
- **14.** Keep 0 as the value for Boot Target LUN.
- **15.** Enter the WWPN for FCoE port 1a on storage controller 1.



I

To obtain this information, log in to storage controller 1 and run the **fcp show adapters** command. Make sure you enter the port name and not the node name.

- 16. Keep the Primary radio button selected as the SAN boot target type.
- 17. Click **OK** to add the SAN boot target.

Add SAN Boot Target Add SAN Boot Target	× ?
Boot Target LUN: 0 Boot Target WWPN: 50:0A:09:81:9D:02:4C:1A Type: • Primary • Secondary	
ОКС	ancel

Figure 32

18. From the vHBA drop-down menu, choose Add SAN Boot Target.

Adding SAN Boot Target for Fabric A

19. Keep 0 as the value for Boot Target LUN.

20. Enter the WWPN for FCoE port 1a on storage controller 2.



te To obtain this information, log in to storage controller 2 and run the **fcp show adapters** command. Make sure you enter the port name and not the node name.

- **21.** Click **OK** to add the SAN boot target.
- Figure 33

Adding Secondary SAN Boot Target for Fabric A

🗼 Add SAN Boot Target	×
Add SAN Boot Target	0
5	
Boot Target LUN: 0	
Boot Target WWPN: 50:0A:09:81:8D:02:4C:1A	
Type: 🖸 Primary 💿 Secondary	
<u>.</u>	
	OK Cancel

- 22. From the vHBA drop-down menu, choose Add SAN Boot.
- **23.** In the Add SAN Boot dialog box, enter Fabric-B in the vHBA box.
- **24.** The SAN boot type should automatically be set to Secondary, and the Type option should be unavailable.
- **25**. Click **OK** to add the SAN boot initiator.

Figure 34 Adding SAN Boot Initiator for Fabric B

🌲 Add SAN Boot		×
Add SAN Boot		0
una la tra al		
vHBA: [Fabric-B]		
Type: O Primary O Secondary		
	ОК	Cancel

- 26. From the vHBA drop-down menu, choose Add SAN Boot Target.
- **27.** Keep 0 as the value for Boot Target LUN.
- **28.** Enter the WWPN for FCoE port 1b on storage controller 1.



I

To obtain this information, log in to storage controller 1 and run the **fcp show adapters** command. Make sure you enter the port name and not the node name.

- **29**. Keep Primary as the SAN boot target type.
- **30**. Click **OK** to add the SAN boot target.

Add SAN Boot Target	× 8
Boot Target LUN: 0 Boot Target WWPN: 50:0A:09:82:9D:02:4C:1A Type: • Primary • Secondary	
OK Canc	el

Figure 35

31. From the vHBA drop-down menu, choose Add SAN Boot Target.

Adding Primary SAN Boot Target for Fabric B

- **32**. Keep 0 as the value for Boot Target LUN.
- **33.** Enter the WWPN for FCoE port 1b on storage controller 2.



Note To obtain this information, log in to storage controller 2 and run the **fcp show adapters** command. Make sure you enter the port name and not the node name.

1

34. Click **OK** to add the SAN boot target.

Figure 36 Adding Secondary SAN Boot Target

🌲 Add SAN Boot Target	×
Add SAN Boot Target	0
5	
Boot Target LUN: 0	
Boot Target WWPN: 50:0A:09:82:8D:02:4C:1A	
Type: 🗢 Primary 💿 Secondary	
	OK Caped

- **35.** Click **OK**, and then **OK** again to create the boot policy.
- 36. Right-click Boot Policies again.
- 37. Choose Create Boot Policy.
- **38**. Enter Boot-Fabric-B as the name of the boot policy.
- **39.** (Optional) Enter a description of the boot policy.
- **40.** Keep the Reboot on Boot Order Change check box unchecked.
- 41. From the Local Devices drop-down menu choose Add CD-ROM.
- 42. From the vHBA drop-down menu choose Add SAN Boot.
- 43. In the Add SAN Boot dialog box, enter Fabric-B in the vHBA box.
- 44. Make sure that the Primary radiobutton is selected as the SAN boot type.
- 45. Click OK to add the SAN boot initiator.

I

	Figure 37	Adding SAN Boot	Initiator for Fabric B
📥 Add SAN Boot			×
Add SAN E	Boot		0
VHBA: Fabric-B			
Type: • Primary	C Secondary		
		ОК	Cancel

- 46. From the vHBA drop-down menu, choose Add SAN Boot Target.
- **47.** Keep 0 as the value for Boot Target LUN.

48. Enter the WWPN for FCoE port 1b on storage controller 1.

Note To obtain this information, log in to storage controller 1 and run the **fcp show adapters** command. Make sure you enter the port name and not the node name.

1

49. Keep Primary as the SAN boot target type.

50. Click **OK** to add the SAN boot target.

Figure 38 Adding Primary SAN Boot Target for Fabric B

🌲 Add SAN Boot Target	×
Add SAN Boot Target	0
-	
Boot Target LUN: 0	
Boot Target WWPN: 50:0A:09:82:9D:02:4C:1A	
Type: Primary Secondary	
ОК СА	ancel

- **51.** From the vHBA drop-down menu, choose Add SAN Boot Target.
- **52.** Keep 0 as the value for Boot Target LUN.
- **53.** Enter the WWPN for FCoE port 1b on storage controller 2.



I

To obtain this information, log in to storage controller 2 and run the **fcp show adapters** command. Make sure you enter the port name and not the node name.

54. Click OK to add the SAN boot target.

Add SAN Boot Target	× ?
Boot Target LUN: 0 Boot Target WWPN: 50:0A:09:82:8D:02:4C:1A Type: Primary Secondary	
ОКС	ancel

Figure 39 Adding Secondary SAN Boot Target for Fabric B

- 55. From the vHBA menu, choose Add SAN Boot.
- 56. In the Add SAN Boot dialog box, enter Fabric-A in the vHBA box.
- **57.** The SAN boot type should automatically be set to Secondary, and the Type option should be unavailable.

1

1

58. Click OK to add the SAN boot initiator.

Figure 40 Adding SAN Boot for Fabric A

📥 Add	SAN Boot		×
Add	SAN Boot		0
VHRA-	Fabric-A	-	
WIDA.	0		
Туре:	Primary O Secondary		
		ОК	Cancel

- 59. From the vHBA menu, choose Add SAN Boot Target.
- **60**. Keep 0 as the value for Boot Target LUN.
- **61.** Enter the WWPN for FCoE port 1a on storage controller 1.



e To obtain this information, log in to storage controller 1 and run the fcp show adapters command. Make sure you enter the port name and not the node name.

- 62. Keep Primary as the SAN boot target type.
- 63. Click OK to add the SAN boot target.

Figure 41 Adding Primary SAN Boot Target for Fabric A

Add SAN Boot Target	× 0
Boot Target LUN: 0 Boot Target WWPN: 50:0A:09:81:9D:02:4C:1A Type: • Primary • Secondary	OK Cancel

- 64. From the vHBA drop-down menu, choose Add SAN Boot Target.
- **65**. Keep 0 as the value for Boot Target LUN.
- **66.** Enter the WWPN for FCoE port 1a on storage controller 2.



I

To obtain this information, log in to storage controller 2 and run the **fcp show adapters** command. Make sure you enter the port name and not the node name.

67. Click OK to add the SAN boot target.

Add SAN Boot Target Add SAN Boot Target	× 0
Boot Target LUN: 0 Boot Target WWPN: 50:0A:09:81:8D:02:4C:1A Type: C Primary C Secondary	

Figure 42

Adding Secondary SAN Boot Target for Fabric A

68. Click OK, and then click OK again to create the boot policy.

Create Service Profile Templates

In this procedure, two service profile templates are created: one for fabric A boot and one for fabric B boot. The first profile is created and then cloned and modified for the second host.

To create service profile templates, follow these steps:

- 1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
- 2. Choose Service Profile Templates > root.
- 3. Right-click root.
- 4. Choose Create Service Profile Template to open the Create Service Profile Template wizard.
- 5. Identify the Service Profile Template:
 - **a.** Enter VM-Host-Infra-Fabric-A as the name of the service profile template. This service profile template is configured to boot from node 1 on fabric A.

- b. Click the Updating Template radio button.
- **c.** Under UUID, choose UUID_Pool as the UUID pool.
- d. Click Next.

Figure 43

Details for Creating Service Profile Template

Create Service Profile Template	computing System Manager
Create Service Profile Template 1. Attribute 2. Networking 3. Storage 4. Zoning 5. VILC/VHBA Placement 6. Server Boot Order 7. Maintenance Policy 8. Server Assignment 9. Operational Policies	Output: With House Profile Computation Name: VPH-House-Infra-fabric-A The template will be created in the following organization. Its name must be unique within this organization. Where: will compute in the following organization. Its name must be unique within this organization. Type: Initial Template in Updating Template Specify how the UUID will be assigned to the server associated with the service generated by this template. UUID UUID_Pool(32/32) UUID Assignment: UUID_Pool(32/32) The unailability of the profile. The description can contain information about when and where the service profile should be used.
	< Prev Next > Finish Cancel

6. Configure the Networking options:

I

- a. Keep the default setting for Dynamic vNIC Connection Policy.
- **b.** Click the Expert radio button to configure the LAN connectivity.
- c. Click Add to add a vNIC to the template.
- d. In the Create vNIC dialog box, enter vNIC-A as the name of the vNIC.
- e. Check the Use vNIC Template check box.
- f. In the vNIC Template list, choose vNIC_Template_A.
- g. In the Adapter Policy list, choose VMWare.
- h. Click OK to add this vNIC to the template.

	Figure 44	Creating vNIC Using vNIC T	emplate	
🛕 Create vNIC			—	
Create vNI	C		6	
Name: vNIC-A				
Use vNIC Template:				
🛨 Create vNIC Te	0 mplate			
		Ъ		
vNIC Template:	NIC_Template_A 💌			
Adapter Perform	ance Profile		I	
Adapter Policy: M	1Ware 💌	+ Create Ethernet Adapter Policy		
0				
L			J	
			OK Cancel	

i. On the Networking page of the wizard, click Add to add another vNIC to the template.

- j. In the Create vNIC box, enter vNIC-B as the name of the vNIC.
- **k.** Check the Use vNIC Template check box.
- I. In the vNIC Template list, choose vNIC_Template_B.
- m. In the Adapter Policy list, choose VMWare.
- **n.** Click **OK** to add the vNIC to the template.
- **o.** Review the table in the Networking page to make sure that both vNICs were created.
- p. Click Next.

Figure 45 LAN Configuration Details

1. VIdentify Service Profile	Optionally specify LAN of	configuration information.			
2. √ <u>Networking</u> 3. √ <u>Storage</u> 4. ⊇ <u>Zoning</u> 5. ⊇ <u>vNIC/vHBA Placement</u>	Dynamic vNIC Connection Policy:	Select a Policy to use (no Dynam	ic vNIC Policy by default) 💌 📑	Create Dynamic vNIC Connection Policy	
Derver Boot Order Maintenance Policy Server Assignment Operational Policies	How would you Click Add to specify one or more v	like to configure LAN connect	ivity? Simple • Expert No	vNICs 🕜 Use Connectivity Policy	
	Name	MAC Address	Fabric ID	Native VLAN	C
		Derived	derived		-
		1	elete 🚹 Add 🌇 Modify		
	Click Add to specify one or more i	SCSI vNICs that the server should	elete 🚹 Add 🌇 Modify use.		
	Click Add to specify one or more i	SCSI vNICs that the server should verlay vNIC Name	elete 🚺 Add 🏬 Modify use. ISCSI Adapter Policy	MAC Address	٥
	Click Add to specify one or more i Name On	SCSI vNICs that the server should	elete 1 Add M Modify use. ISCSI Adapter Policy	MAC Address	0
	Click Add to specify one or more i Name On	SCSI vNICs that the server should verlay vNIC Name	elete 1 Add M Modify use. ISCSI Adapter Policy	MAC Address	0

7. Configure the Storage options:

ſ

- **a**. Choose a local disk configuration policy:
- If the server in question has local disks, choose default in the Local Storage list.
- If the server in question does not have local disks, choose SAN-Boot.
- **b.** Click the **Expert** radio button to configure the SAN connectivity.
- c. In the WWNN Assignment list, choose WWNN_Pool.
- d. Click Add at the bottom of the page to add a vHBA to the template.
- e. In the Create vHBA dialog box, enter Fabric-A as the name of the vHBA.
- f. Check the Use vHBA Template check box.
- g. In the vHBA Template list, choose vHBA_Template_A.
- h. In the Adapter Policy list, choose VMware.
- i. Click **OK** to add this vHBA to the template.

	Figure 46	Creating vHBA Using vHBA Tem	plate
🛕 Create vHBA			×
Create vH	BA		0
Nam Use vHBA Templat Create vHBA vHBA Template: Adapter Perform Adapter Policy:	e: Fabric-A e: V Template vHBA_Template_A mance Profile		
			OK Cancel

j. On the Storage page of the wizard, click **Add** at the bottom of the page to add another vHBA to the template.

- k. In the Create vHBA dialog box, enter Fabric-B as the name of the vHBA.
- I. Check the check box for Use HBA Template.
- **m.** In the vHBA Template list, choose vHBA_Template_B.
- n. In the Adapter Policy list, choose VMware.
- **o.** Click **OK** to add the vHBA to the template.
- **p.** Review the table in the Storage page to verify that both vHBAs were created.
- q. Click Next.

Figure 47 Storage Window Showing Created vHBAs

🛕 Create Service Profile Template

Unified	Computing	System	Manager
onnea	oompating	Cystem	manager

Create Service Profile Template 1. √Identify Service Profile	Storage Optionally specify disk policies and SAN co	onfiguration information.	(
Template 2. ✓ Networking 3. ✓ Storage. 4. □ Zoning 5. □ vMIC/VHBA Placement. 6. □ Server Boot Order. 7. □ Maintenance Policy. 8. □ Server Assignment.	Select a local disk configuration policy. Local Storage: SAN-Boot	 Mode: No Local Storage Protect Configuration: Yes If Protect Configuration is set, the local disk configuration is preserved is disassociated with the server. In that case, a configuration error will be raised when a new service profile 	if the service profile
9. Operational Policies	How would you like to configure 5 A server is identified on a SAN by its World Wide Node Ne world Wide Node Name WWNN Assignment: WWNN_Pool(32/32) The WWNN will be assigned from the selected pool. The available/total WWNNs are displayed after the p	AN connectivity? Simple Expert No vHBAs Use Connectivity Po ame (WWNN). Specify how the system should assign a WWNN to the server associ ool name.	licy ated with this
	Name VHBA Fabric-A VHBA If VHBA Fabric-B VHBA If	WWPN Derived Derived	\$
		Pelete Add Modfy	-
		<pre></pre>	Finish Cancel

- 8. Set no Zoning options and click Next.
- **9**. Set the vNIC/vHBA placement options.
 - a. In the Select Placement list, choose the VM-Host-Infra placement policy.
 - **b.** Choose vCon1 and assign the vHBAs/vNICs to the virtual network interfaces policy in the following order:
 - vHBA Fabric-A
 - vHBA Fabric-B
 - vNIC-A
 - vNIC-B
 - **c.** Review the table to verify that all vNICs and vHBAs were assigned to the policy in the appropriate order.
 - d. Click Next.

I

I	Figure 48	Placing vNIC an	d vHBA on Physical Ad	dapters		
📥 Create Service Profile Template						×
Unified	Compı	iting Syst	em Manage	er		
Create Service Profile Template 1. √Identify Service Profile Template 2. √Networking 3. √Storage 4. √Zoning 5. √vHIC/vHBA Placement 6. √Server Boot Order 7. Maintenance Policy 8. Server Assignment 9. Operational Policies	VNIC/vHB Specify ho vNIC/vHBA Placemen in a server hardware Select Placemen Virtual Network vNICs and vHBA performed expli automatically by vNIC/vHBA plac Please select on	A Placement w vNICs and vHBAs are plant tspecifies how vNICs and vHBA configuration independent way. WHHost-Infra Interface connection provides a r is are assigned to one of Virtual Net relecting "any". ement on physical network interface and of voltage of the second of the second of the second of the second the virtual Network Interface and of the virtual Network Interface and of the virtual Network Interface and of whether the second of the seco	ced on physical network adapter s are placed on physical network adapt cereate Placement Policy create Placement Policy nechanism of placing vNICs and vHBAs letwork Interface connection specified twork Interface connection is used by v ace is controlled by placement preferen one or more vNICs or vHBAs	S ers (mezzanine) on physical network ac below. This assignment AVIC or vHBA or it can b ices.	lapters. : can be be done	0
	VNICS VHRA	c	Name	Order	Selection Preference	
			E S vCon 1		Assigned Only	
	Name			1		
				2		
		>> assign >>		3		
		<< remove <<	VNIC VNIC-B	4		
			-S vCon 2		All	
			🗐 vCon 3		All	
			-SvCon 4		All	
				🔺 Move Up 🔍 Mov	re Down	
		<u> </u>				
				< F	rev Next > Finish	Cancel

- **10.** Set the Server Boot Order:
 - **a**. In the Boot Policy list, choose Boot-Fabric-A.
 - **b.** Review the table to verify that all boot devices were created and identified. Verify that the boot devices are in the correct boot sequence.

1

c. Click Next.

Figure 49 Setting Boot Order for the Service Profile Template

📥 Create Service Profile Template × Unified Computing System Manager 0 Server Boot Order Create Service Profile Template Optionally specify the boot policy for this service profile template. 1. √Identify Service Profile Template Select a boot policy. 2. VNetworking 3. √<u>Storage</u> 4. √Zoning Boot Policy: Boot-Fabric-A Create Boot Policy 5. VVNIC/VHBA Placement 6. √<u>Server Boot Order</u> 7. Maintenance Policy Name: Boot-Fabric-A 8. Server Assignment Description: 9. Operational Policies Reboot on Boot Order Change: No Enforce vNIC/vHBA/iSCSI Name: Yes WARNINGS: The type (primary/secondary) does not indicate a boot order presence. The type (primary/secondary) does not indicate a boot order presence. The effective order of boot devices within the same device class (LAN/Storage/ISCSI) is determined by PCIe bus scan order. If Enforce vNIC/vHBA/ISCSI Name is selected and the vNIC/vHBA/ISCSI does not exist, a config error will be reported. If it is not selected, the vNICs/vHBA/ISCSI are selected if they exist, otherwise the vNIC/vHBA/ISCSI with the lowest PCIe bus scan order is used. Boot Order 🛨 🖃 🕰 Filter 👄 Export 😸 Print ₽ Order VNIC/VHBA/ISCSI VNIC WWN Name Type Lun ID CD-ROM 1 🗄 📃 Storage 2 SAN primary Fabric-A Primary SAN Target primary Primary 20:01:00:A0:98:37:79:A0 0 SAN Target secondary Secondary 0 20:03:00:A0:98:37:79:A0 SAN secondary Fabric-B Secondary E SAN Target primary Primary 0 20:02:00:A0:98:37:79:A0 E SAN Target secondary Secondary 0 20:04:00:A0:98:37:79:A0 Set iSCSI Boot Parameters Create iSCSI vNIC < Prev Next > Finish Cancel

- **11**. Add a Maintenance Policy:
 - a. Choose the Default Maintenance Policy.
 - b. Click Next.

I

	Figure 50	Choosing a Maint	enance Policy				
📥 Create Service Profile Templa	te						
Unified	Computi	ng System	Manager				_
Create Service Profile Template 1. ✓ Identify Service Profile Iemplate 2. ✓ Networking 3. ✓ Storage 4. ✓ Zoning 5. ✓ vNIC/vHBA Placement 6. ✓ Server Boot Order 7. ✓ Maintenance Policy 8. □ Server Assignment 9. □ Operational Policies	Maintenance Specify how disr associated with Maintenance Policy Select a maintenance that will be accessible Maintenance Policy Name: de Description: Reboot Policy: Us	Policy ruptive changes such as reboots this service profile. policy to include with this service profil to all service profiles.	e or create a new maintenance policy Create Maintenance Policy	e upgrades s	hould be appl	ied to the se	erver
				< Prev	Next >	Finish	Cancel

- **12.** Specify the Server Assignment:
 - **a**. In the Pool Assignment list, choose Infra_Pool.
 - **b.** (Optional) Choose a Server Pool Qualification policy.
 - c. Choose Down as the power state to be applied when the profile is associated with the server.

1

- **d.** Expand Firmware Management at the bottom of the page and choose VM-Host-Infra from the Host Firmware list.
- e. Click Next.

Figure 51 Assigning a Server Pool to the Service Profile Template

	igure er	Assigni			npiace		
Create Service Profile Template							
Unified (Compu	ting	System	Manager			
Create Service Profile Template 1. Videntify Service Profile	Server Ass Optionally s	ignmen pecify a serve	t er pool for this service p	rofile template.			
Iemplate 2. √Networking 3. √Storage 4. √Zoning 5. √vNIC/vHBA Placement	You can select a serv Pool Assignment:	ver pool you wai Infra_Pool	nt to associate with this ser	rice profile template.			
6. √ <u>Server Boot Order</u> 7. √ <u>Maintenance Policy</u> 8. √ <u>Server Assignment</u> 9. □ <u>Operational Policies</u>				Select the power state to be applied whe profile is associated with the server.	en this		
	The service profi If desired, you c To do so, select I Server Pool Qual Restrict M	le template will lan specify an ac the qualification ification: <a href="mailto:specify-an-action-
igration:">cnot igration:	be associated with one of th dditional server pool policy o from the list. set>	e servers in the selected pool. ualification that the selected server must m	neet.		
	Firmware Manae If you select a ho server that it is a Otherwise the sy Host Firmware	gement (BIOS ost firmware poli ssociated with. stem uses the f	5, Disk Controller, Adapt icy for this service profile, t irmware already installed or	er) ne profile will update the firmware on the the associated server.	8		
		a arriva in		Create Host Firmware Package	< Prev	Next >	Finish

13. Add Operational Policies:

ſ

- **a**. In the BIOS Policy list, choose VM-Host-Infra.
- **b.** Expand Power Control Policy Configuration and choose No-Power-Cap in the Power Control Policy list.

Cancel

Setting Operational Policy

1

🛕 Create Service Profile Template				×
Unified C	Computing System Manager			
Create Service Profile Template 1. √Identify Service Profile	Operational Policies Optionally specify information that affects how the system operates.			0
Template 2. √ Networking 3. √ Storage 4. √ Zoning 5. √ vNIC/vHBA Placement 6. √ Server Boot Order 7. √ Maintenance Policy	BIOS Configuration If you want to override the default BIOS settings, select a BIOS policy that will be associated with this service profile BIOS Policy: WM-Host-Infra T Create BIOS Policy	۲		
 √<u>Server Assignment</u> √<u>Operational Policies</u> 	External IPMI Management Configuration	8		
	Monitoring Configuration (Thresholds)	8		
	Power Control Policy Contiguration Power control policy determines power allocation for a server in a given power group. Power Control Policy: No-Power-Cap	8		
	Scrub Policy	8		
	< Prev	Next >	Finish	Cancel

- 14. Click **Finish** to create the service profile template.
- 15. Click **OK** in the confirmation message.
- **16**. Click the **Servers** tab in the navigation pane.
- **17.** Choose **Service Profile Templates** > **root**.
- **18.** Right-click the previously created VM-Host-Infra-Fabric-A template.
- 19. Choose Create a Clone.
- **20.** In the dialog box, enter VM-Host-Infra-Fabric-B as the name of the clone, choose the root Org, and click **OK**.

	riguie de	
Create Clone	e From VM-Host-Inf	fra-Fabric-A
CI	one Name: VM-Host-I Org: root	infra-Fabric-B
	K Cancel	Help

Figure 53 Cloning a Service Profile Template

21. Click OK.

I

Γ

- **22**. Choose the newly cloned service profile template and click the **Boot Order** tab.
- 23. Click Modify Boot Policy.
- 24. In the Boot Policy list, choose Boot-Fabric-B.

dify Boot Policy						
Delta Dest Cabria D						
olicy: Boot-Fabric-B	🛨 Crea	ite Boot Policy				
Name: Boot-	Fabric-B					
Description:						
boot on Boot Order Change: No						
ce vNIC/vHBA/iSCSI Name: Yes						
(NINGS:	indicata a hav	at order processe				
ffective order of boot devices with	indicate a boo	levice class (LAN/Storage/iSC	ST) is determine	d by PCIe bi	is scap order.	
force vNIC/vHBA/iSCSI Name i	is selected an	d the vNIC/vHBA/iSCSI does	not exist, a con	fig error will	be reported.	
not selected, the vNICs/vHBAs/iS0	CSI are select	ted if they exist, otherwise th	e vNIC/vHBA/is	SCSI with the	lowest PCIe bus scan order is u	used.
ot Order						
- A Sharles Sugart St Data						
- Plicer - Export - Prin	10					
ne	Order	VNIC/VHBA/iSCSI VNIC	Туре	Lun ID	WWN	Ę
e CD-ROM	Order 1	VNIC/VHBA/ISCSI VNIC	Туре	Lun ID	WWN	E.
CD-ROM Storage	Order 1 2	VNIC/VHBA/iSCSI VNIC	Туре	Lun ID	WWN	E
CD-ROM Storage SAN primary	Order 1 2	VNIC/VHBA/iSCSI VNIC	Type	Lun ID	WWN	F
CD-ROM Storage SAN primary SAN primary SAN Primary SAN Primary	Order 1 2	VNIC/VHBA/iSCSI VNIC	Type Primary Primary	Lun ID	WWN 20:02:00:A0:98:37:79:A0	F
CD-ROM Storage SAN primary SAN Target primary SAN Target primary SAN Target primary	Order 1 2	vNIC/vHBA/iSCSI vNIC	Type Primary Primary Secondary	Lun ID	WWN 20:02:00:A0:98:37:79:A0 20:04:00:A0:98:37:79:A0	•
CD-ROM CD-ROM Storage SAN primary SAN Target primary SAN Target primary SAN Target secondary SAN secondary	Order 1 2	VNIC/VHBA/iSCSI VNIC	Type Primary Primary Secondary Secondary	Lun ID 0 0	WWN 20:02:00:A0:98:37:79:A0 20:04:00:A0:98:37:79:A0	P
CD-ROM CD-ROM Storage SAN primary SAN Target primary SAN Target primary SAN secondary SAN secondary SAN Target primary	Order 1 2	VNIC/VHBA/iSCSI VNIC	Primary Primary Secondary Secondary Primary	Lun ID 0 0	WWN 20:02:00:A0:98:37:79:A0 20:04:00:A0:98:37:79:A0 20:01:00:A0:98:37:79:A0	P
CD-ROM CD-ROM Storage SAN primary SAN Target primary SAN Target primary SAN secondary SAN secondary SAN Target se	Order 1 2	VNIC/VHBA/iSCSI VNIC	Type Primary Primary Secondary Secondary Primary Secondary	Lun ID 0 0 0	WWN 20:02:00:A0:98:37:79:A0 20:04:00:A0:98:37:79:A0 20:01:00:A0:98:37:79:A0 20:01:00:A0:98:37:79:A0	
CD-ROM CD-ROM Storage SAN primary SAN Target primary SAN Secondary SAN Target primary SAN Target primary SAN Target primary SAN Target primary SAN Target secondary SAN Target secondary	Order 1 2	VNIC/VHBA/iSCSI VNIC	Type Primary Primary Secondary Primary Secondary Primary Secondary	Lun ID 0 0 0	WWN 20:02:00:A0:98:37:79:A0 20:04:00:A0:98:37:79:A0 20:01:00:A0:98:37:79:A0 20:03:00:A0:98:37:79:A0	~
CD-ROM CD-ROM Storage SAN primary SAN Target primary SAN Target secondary SAN Target primary SAN Target primary SAN Target primary SAN Target secondary SAN Target secondary SAN Target secondary	Order 1 2	VNIC/VHBA/iSCSI VNIC	Type Primary Primary Secondary Primary Secondary Primary Secondary	Lun ID 0 0 0 0	WWN 20:02:00:A0:98:37:79:A0 20:04:00:A0:98:37:79:A0 20:01:00:A0:98:37:79:A0 20:03:00:A0:98:37:79:A0	
CD-ROM CD-ROM Storage SAN primary SAN Target secondary	Order 1 2	vNIC/vHBA/iSCSI vNIC Fabric-B Fabric-A	Type Primary Primary Secondary Primary Secondary	Lun ID 0 0 0	WWN 20:02:00:A0:98:37:79:A0 20:04:00:A0:98:37:79:A0 20:01:00:A0:98:37:79:A0 20:03:00:A0:98:37:79:A0	R
e CD-ROM Storage SAN primary SAN Target primary SAN Target primary SAN secondary SAN Target primary SAN Target primary SAN Target secondary	Order 1 2 Boot Paramet	vNIC/vHBA/iSCSI vNIC Fabric-B Fabric-A	Type Primary Primary Secondary Primary Secondary	Lun ID 0 0 0	WWN 20:02:00:A0:98:37:79:A0 20:04:00:A0:98:37:79:A0 20:01:00:A0:98:37:79:A0 20:03:00:A0:98:37:79:A0	

Figure 54 Modifying Boot Policy

- 25. Click OK, and then click OK again.
- 26. In the right pane, click the Network tab and then click Modify vNIC/HBA Placement.
- 27. Expand vCon 1 and move vHBA Fabric-B ahead of vHBA Fabric-A in the placement order.

1

Figure 55 Modifying Placement Policy

	cifies how vNICs and vHBA	is are placed on physical network adap	ters (mezzanine)		
hardware config	guration independent way.	•			
Placement: VM-	-Host-Infra	Create Placement Policy			
Network Interfa	ace connection provides a	mechanism of placing vNICs and vHBA	s on physical network adapters	5.	
and vHBAs are a med explicitly by	assigned to one of Virtual N selecting which Virtual Ne	Network Interface connection specified twork Interface connection is used by	below. This assignment can be vNIC or vHBA or it can be done	e	
atically by select	ting "any".	work interface connection is used by	WILC OF WHEN OF IL CAIL DE GOIN	•	
VHBA placement	on physical network interfa	ace is controlled by placement prefere	nces.		
select one Virtu	al Network Interface and o	one or more vNICs or vHBAs			
		Virtual Network Interfaces Policy (r	read only)		
Cs VHBAs		Virtual Network Interfaces Policy (r Name	read only) Order	Selection Preference	
Cs vHBAs		Virtual Network Interfaces Policy (r Name I - S vCon 1	read only) Order	Selection Preference Assigned Only	
Cs vHBAs		Virtual Network Interfaces Policy (r Name IIII vCon 1 VFBA Fabric-B	read only) Order 1	Selection Preference Assigned Only	
Cs vHBAs Name III	>> assian >>	Virtual Network Interfaces Policy (r Name P-SS vCon 1 	read only) Crder	Selection Preference Assigned Only	
Cs vHBAs Name (C)	>> assign >>	Virtual Network Interfaces Policy (r Name Con 1 VHBA Fabric-8 VHBA Fabric-A VHBA Fabric-A	read only) Crder Crder Crder	Selection Preference Assigned Only	
Cs vHBAs Name (C)	>> assign >> << remove <<	Virtual Network Interfaces Policy (n Name P-55 vCon 1 VHBA Fabric-8 VHBA Fabric-A VHIC vNIC-A VHIC vNIC-A	read only) Order 1 2 3 4	Selection Preference Assigned Only	
Cs vHBAs Name C	>> assign >> < <remoye <<<="" th=""><th>Virtual Network Interfaces Policy (n Name P-SS vCon 1 VHBA Fabric-8 VHBA Fabric-A VHIC vNIC-A VHIC vNIC-8 VCon 2</th><th>read only) Order 1 2 3 4</th><th>Selection Preference Assigned Only All</th><th></th></remoye>	Virtual Network Interfaces Policy (n Name P-SS vCon 1 VHBA Fabric-8 VHBA Fabric-A VHIC vNIC-A VHIC vNIC-8 VCon 2	read only) Order 1 2 3 4	Selection Preference Assigned Only All	
CS VHBAS	>> assign >> << remoye <<	Virtual Network Interfaces Policy (n Name P-SS vCon 1 VHBA Fabric-8 VHBA Fabric-A VHIC vNIC-A VHIC vNIC-A VHIC vNIC-8 VCon 2 S vCon 3	read only) Order 1 2 3 4	Selection Preference Assigned Only All All	
Cs vHBAs Name [C]	>> assign >> << remove <<	Virtual Network Interfaces Policy (n Name VHBA Fabric-8 VHBA Fabric-8 VHBA Fabric-A VHIC vNIC-A VHIC vNIC-A VHIC vNIC-8 VCon 2 S vCon 3 S vCon 4	read only) Order	Selection Preference Assigned Only All All	
CS VHBAS	>> assign >> << remoye <<	Virtual Network Interfaces Policy (n Name P-SS vCon 1 VHBA Fabric-8 VHBA Fabric-A VHIC vNIC-A VHIC vNIC-A VHIC vNIC-8 VCon 2 S vCon 3 S vCon 4	need only) Order	Selection Preference Assigned Only All All All	
CS VHBAS	>> assign >> << remove <<	Virtual Network Interfaces Policy (r Name P-SS vCon 1 VHBA Fabric-8 VHBA Fabric-A VHIC vNIC-A VHIC vNIC-A VHIC vNIC-8 VCon 2 S vCon 3 S vCon 4	need only) Order	Selection Preference Assigned Only All All All	
Cs VHBAs Name [C]	>> assign >> << remove <<	Virtual Network Interfaces Policy (r Name P-SS vCon 1 VHBA Fabric-8 VHBA Fabric-A VHIC vNIC-A VHIC vNIC-A VHIC vNIC-8 VCon 2 S vCon 3 S vCon 4	read only) Order 1 2 3 4 Move Up Move Dov	Selection Preference Assigned Only All All All	
Cs VHBAs Name C	>> assign >> << remove <<	Virtual Network Interfaces Policy (r Name Con 1 VHBA Fabric-8 VHBA Fabric-A VHIC VNIC-A VHIC VNIC-A VHIC VNIC-8 VCon 2 SVCon 3 SVCon 4	read only) Order 1 2 3 4 Move Up Move Dov	Selection Preference Assigned Only All All All	

28. Click OK, and then click OK again.

Create Service Profiles

ſ

To create service profiles from the service profile template, follow these steps:

- 1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
- 2. Choose Service Profile Templates > root > Service Template VM-Host-Infra-Fabric-A.
- 3. Right-click VM-Host-Infra-Fabric-A and choose Create Service Profiles from Template.
- 4. Enter VM-Host-Infra-0 as the service profile prefix.
- 5. Enter 1 as the number of service profiles to create.
- 6. Click **OK** to create the service profile.

Figure 56	Creating Service Profile f	rom a Service Profile Templat
A Create Service Profiles From Templa	ate	×
Create Service Profile	s From Template	0
Naming Prefix: VM-Host-Infra-0		
Number: 1		
	ОК	Cancel

- 7. Click **OK** in the confirmation message.
- 8. Choose Service Profile Templates > root > Service Template VM-Host-Infra-Fabric-B.
- 9. Right-click VM-Host-Infra-Fabric-B and choose Create Service Profiles from Template.
- **10.** Enter VM-Host-Infra-0 as the service profile prefix.
- **11.** Enter 1 as the number of service profiles to create.
- **12.** Click **OK** to create the service profile.

Figure 57 Creating Service Profile from a Service Profile Template

A Create Service Profiles From Template	×
Create Service Profiles From Template	0
Naming Prefix: VM-Host-Infra-0 Number: 1	
ОК	Cancel

13. Click OK in the confirmation message.

Verify that the service profiles VM-Host-Infra-01 and VM-Host-Infra-02 have been created. The service profiles are automatically associated with the servers in their assigned server pools.

14. (Optional) Choose each newly created service profile and enter the server host name or the FQDN in the User Label field in the General tab. Click Save Changes to map the server host name to the service profile name.

Add More Servers to FlexPod Unit

Additional server pools, service profile templates, and service profiles can be created in the respective organizations to add more servers to the FlexPod unit. All other pools and policies are at the root level and can be shared among the organizations.

Gather Necessary Information

After the Cisco UCS service profiles have been created, each infrastructure blade in the environment will have a unique configuration. To proceed with the FlexPod deployment, specific information must be gathered from each Cisco UCS blade and from the NetApp controllers. Insert the required information into Table 20 and Table 21.

Table 20FC Port Names for Storage Controllers 1 and 2

Storage Controller	FCoE Port	FC Port Name
1	1a	
1	1b	
2	1a	
2	1b	



To gather the FC port name information, run the fcp show adapters command on the storage controller.

Table 21 vHBA WWPNs for Fabric A and Fabric B

Cisco UCS Service Profile Name	Fabric A vHBA WWPN	Fabric B vHBA WWPN
VM-Host-infra-01		
VM-Host-infra-02		



To gather the vHBA WWPN information, launch the Cisco UCS Manager GUI. In the navigation pane, click the **Servers** tab. Expand **Servers** > **Service Profiles** > **root**. Click each service profile and then click the **Storage** tab in the right pane. In Table 21, record the WWPN information that is displayed in the right pane for both the Fabric A vHBA and the Fabric B vHBA for each service profile.

Storage Networking

FlexPod Cisco Nexus Base

Table 22 Flexpod Cisco Nexus Base Prerequisite

Description

The Cisco Nexus switch must be running Cisco Nexus NX-OS 5.2(1)N1(3) or late

The following procedures describe how to configure the Cisco Nexus switches for use in a base FlexPod environment. Follow these steps precisely; failure to do so might result in an improper configuration.

Set Up Initial Configuration

Cisco Nexus A

To set up the initial configuration for the Cisco Nexus A switch on <<var_nexus_A_hostname>>, follow these steps:

Configure the switch.



On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning.

```
Abort Power on Auto Provisioning and continue with normal setup? (yes/no) [no]:
ves
Do you want to enforce secure password standard (yes/no): yes
Enter the password for the "admin": <<var_password>>
Confirm the password for "admin": <<var_password>>
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]: Enter
Configure read-only SNMP community string (yes/no) [n]: Enter
Configure read-write SNMP community string (yes/no) [n]: Enter
Enter the switch name: <<var_nexus_A_hostname>>
Continue with out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
Mgmt0 IPv4 address: <<var_nexus_A_mgmt0_ip>>
Mgmt0 IPv4 netmask: <<var_nexus_A_mgmt0_netmask>>
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway: <<var_nexus_A_mgmt0_gw>>
Enable the telnet service? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter
Type of ssh key you would like to generate (dsa/rsa): rsa
Number of key bits <768-2048> : 1024
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address: <<var_global_ntp_server_ip>>
Enter basic FC configurations (yes/no) [n]: Enter
Would you like to edit the configuration? (yes/no) [n]: Enter
2. Review the configuration summary before enabling the configuration.
Use this configuration and save it? (yes/no) [y]: Enter
```

Cisco Nexus B

To set up the initial configuration for the Cisco Nexus B switch on <<var_nexus_B_hostname>>, follow these steps:

1. Configure the switch.



On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning.

```
Abort Power on Auto Provisioning and continue with normal setup? (yes/no) [no]:
ves
Do you want to enforce secure password standard (yes/no): yes
Enter the password for the "admin": <<var_password>>
Confirm the password for "admin": <<var_password>>
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]: Enter
Configure read-only SNMP community string (yes/no) [n]: Enter
Configure read-write SNMP community string (yes/no) [n]: Enter
Enter the switch name: <<var_nexus_B_hostname>>
Continue with out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
Mgmt0 IPv4 address: <<var_nexus_B_mgmt0_ip>>
Mgmt0 IPv4 netmask: <<var_nexus_B_mgmt0_netmask>>
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway: <<var_nexus_B_mgmt0_gw>>
Enable the telnet service? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter
Type of ssh key you would like to generate (dsa/rsa): rsa
Number of key bits <768-2048> : 1024
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address: <<var_global_ntp_server_ip>>
Enter basic FC configurations (yes/no) [n]: Enter
Would you like to edit the configuration? (yes/no) [n]: Enter
```

2. Review the configuration summary before enabling the configuration.

Use this configuration and save it? (yes/no) [y]: Enter

FlexPod Cisco Nexus FCoE Storage vSphere on Data ONTAP 7-Mode

Enable Licenses

Cisco Nexus A

To license the Cisco Nexus A switch on <<var_nexus_A_hostname>>, follow these steps:

- 1. Log in as admin.
- 2. Run the following commands:

```
config t
feature fcoe
feature npiv
feature lacp
feature vpc
```

Cisco Nexus B

To license the Cisco Nexus B switch on <<var_nexus_B_hostname>>, follow these steps:

- **1**. Log in as admin.
- 2. Run the following commands:

```
config t
feature fcoe
feature npiv
feature lacp
feature vpc
```

Set Global Configurations

Cisco Nexus 5548 A and Cisco Nexus 5548 B

To set global configurations, follow these steps on both switches:

Run the following commands to set global configurations and jumbo frames in QoS:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
port-channel load-balance ethernet source-dest-port
policy-map type network-qos jumbo
class type network-qos class-default
mtu 9216
exit
class type network-qos class-fcoe
pause no-drop
mtu 2158
exit
exit
system qos
service-policy type network-qos jumbo
exit
copy run start
```

Create VLANs

Cisco Nexus 5548 A and Cisco Nexus 5548 B

To create the necessary virtual local area networks (VLANs), follow these steps on both switches:

I

From the global configuration mode, run the following commands:

```
vlan <<var_ib-mgmt_vlan_id>>
name IB-MGMT-VLAN
exit
vlan <<var_native_vlan_id>>
name Native-VLAN
exit
vlan <<var_nfs_vlan_id>>
name NFS-VLAN
exit
vlan <<var_pkt-ctrl_vlan_id>>
name Packet-Control-VLAN
exit
vlan <<var_wmotion_vlan_id>>
name vMotion-VLAN
exit
```

```
vlan <<var_vm-traffic_vlan_id>>
name VM-Traffic-VLAN
exit
```

Add Individual Port Descriptions for Troubleshooting

Cisco Nexus 5548 A

To add individual port descriptions for troubleshooting activity and verification for switch A, follow these steps:

From the global configuration mode, run the following commands:

```
interface Eth1/1
description <<var_node01>>:e3a
exit
interface Eth1/2
description <<var_node02>>:e3a
exit
interface Eth1/11
description <<var_ucs_clustername>>-A:1/19
exit
interface Eth1/12
description <<var_ucs_clustername>>-B:1/19
exit
interface Eth1/13
description <<var_nexus_B_hostname>>:1/13
exit
interface Eth1/14
description <<var_nexus_B_hostname>>:1/14
exit
interface eth1/31
description <<var_ucs_clustername>>-A:1/31
exit
interface eth1/32
description <<var_ucs_clustername>>-A:1/32
exit
```

Cisco Nexus 5548 B

I

To add individual port descriptions for troubleshooting activity and verification for switch B, follow these steps:

From the global configuration mode, run the following commands:

```
interface Eth1/1
description <<var_node01>>:e4a
exit
interface Eth1/2
description <<var_node02>>:e4a
exit
interface Eth1/11
description <<var_ucs_clustername>>-A:1/20
exit
interface Eth1/12
description <<var_ucs_clustername>>-B:1/20
exit
interface Eth1/13
description <<var_nexus_A_hostname>>:1/13
exit
interface Eth1/14
description <<var_nexus_A_hostname>>:1/14
```

```
exit
interface eth1/31
description <<var_ucs_clustername>>-B:1/31
exit
interface eth1/32
description <<var_ucs_clustername>>-B:1/32
exit
```

Create Port Channels

Cisco Nexus 5548 A and Cisco Nexus 5548 B

To create the necessary port channels between devices, follow these steps on both switches:

From the global configuration mode, run the following commands:

```
interface Po10
description vPC peer-link
exit
interface Eth1/13-14
channel-group 10 mode active
no shutdown
exit
interface Poll
description <<var_node01>>
exit
interface Eth1/1
channel-group 11 mode active
no shutdown
exit
interface Pol2
description <<var_node02>>
exit
interface Eth1/2
channel-group 12 mode active
no shutdown
exit
interface Po13
description <<var_ucs_clustername>>-A
exit
interface Eth1/11
channel-group 13 mode active
no shutdown
exit
interface Pol4
description <<var_ucs_clustername>>-B
exit
interface Eth1/12
channel-group 14 mode active
no shutdown
exit
copy run start
```

Configure Port Channels

Cisco Nexus 5548 A and Cisco Nexus 5548 B

To configure the port channels, follow these steps on both switches: From the global configuration mode, run the following commands:

```
interface Pol0
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_nfs_vlan_id>>,
<<var_pkt-ctrl_vlan_id>>, <<var_vmotion_vlan_id>>, <<var_vm-traffic_vlan_id>>
spanning-tree port type network
no shutdown
exit.
interface Poll
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_nfs_vlan_id>>
spanning-tree port type edge trunk
no shutdown
exit
interface Po12
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_nfs_vlan_id>>
spanning-tree port type edge trunk
no shutdown
exit
interface Po13
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_nfs_vlan_id>>,
<<var_vmotion_vlan_id>>, <<var_vm-traffic_vlan_id>>
spanning-tree port type edge trunk
no shutdown
exit
interface Po14
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan
<<var_ib-mgmt_vlan_id>>, <<var_nfs_vlan_id>>, <<var_vmotion_vlan_id>>,
<<var_vm-traffic_vlan_id>>
spanning-tree port type edge trunk
no shutdown
exit
copy run start
```

Configure Virtual Port Channels

Cisco Nexus 5548 A

To configure virtual port channels (vPCs) for switch A, follow these steps:

From the global configuration mode, run the following commands:

```
vpc domain <<var_nexus_vpc_domain_id>>
role priority 10
peer-keepalive destination <<var_nexus_B_mgmt0_ip>> source <<var_nexus_A_mgmt0_ip>>
auto-recovery
exit
interface Po10
vpc peer-link
exit
interface Po11
vpc 11
exit
interface Po12
vpc 12
```

```
exit
interface Pol3
vpc 13
exit
interface Pol4
vpc 14
exit
copy run start
```

Cisco Nexus 5548 B

To configure vPCs for switch B, follow these steps:

From the global configuration mode, run the following commands.

```
vpc domain <<var_nexus_vpc_domain_id>>
role priority 20
peer-keepalive destination <<var_nexus_A_mgmt0_ip>> source <<var_nexus_B_mgmt0_ip>>
auto-recovery
exit
interface Po10
vpc peer-link
exit
interface Poll
vpc 11
exit
interface Po12
vpc 12
exit
interface Po13
vpc 13
exit
interface Po14
vpc 14
exit.
copy run start
```

Configure Ports for Cisco Nexus 1110-X Virtual Appliances

Cisco Nexus 5548 A

To configure the ports in switch A that are connected to the Cisco Nexus 1110-X, follow these steps:

From the global configuration mode, run the following commands:

```
interface Eth1/15
description <<var_nexus_1110x-1>>:Eth1
switchport mode trunk
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_pkt-ctrl_vlan_id>>
speed 1000
spanning-tree port type edge trunk
no shutdown
exit
interface Eth1/16
description <<var_nexus_1110x-2>>:Eth1
switchport mode trunk
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_pkt-ctrl_vlan_id>>
speed 1000
spanning-tree port type edge trunk
no shutdown
exit
copy run start
```

I

Cisco Nexus 5548 B

To configure the ports in switch B that are connected to the Cisco Nexus 1110-X, follow these steps:

From the global configuration mode, run the following commands:

```
interface Eth1/15
description <<var_nexus_1110x-1>>:Eth2
switchport mode trunk
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_pkt-ctrl_vlan_id>>
speed 1000
spanning-tree port type edge trunk
no shutdown
exit.
interface Eth1/16
description <<var_nexus_1110x-2>>:Eth2
switchport mode trunk
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_pkt-ctrl_vlan_id>>
speed 1000
spanning-tree port type edge trunk
no shutdown
exit
copy run start
```

Uplink into Existing Network Infrastructure

Depending on the available network infrastructure, several methods and features can be used to uplink the FlexPod environment. If an existing Cisco Nexus environment is present, NetApp recommends using vPCs to uplink the Cisco Nexus 5548 switches included in the FlexPod environment into the infrastructure. The previously described procedures can be used to create an uplink vPC to the existing environment. Make sure to run copy run start to save the configuration on each switch after configuration is completed.

Create VSANs, Assign and Enable Virtual Fibre Channel Ports

This procedure sets up Fibre Channel over Ethernet (FCoE) connections between the Cisco Nexus 5548 switches, the Cisco UCS Fabric Interconnects, and the NetApp storage systems.

Cisco Nexus 5548 A

To configure virtual storage area networks (VSANs), assign virtual Fibre Channel (vFC) ports, and enable vFC ports on switch A, follow these steps:

From the global configuration mode, run the following commands:

```
vlan <<var_fabric_a_fcoe_vlan_id>>
name FCoE_Fabric_A
fcoe vsan <<var_vsan_a_id>>
exit
interface pol1
switchport trunk allowed vlan add <<var_fabric_a_fcoe_vlan_id>>
exit
interface vfc11
switchport description <<var_node01>>:3a
bind interface Eth1/1
switchport trunk allowed vsan <<var_vsan_a_id>>
no shutdown
exit
interface pol2
switchport trunk allowed vlan add <<var_fabric_a_fcoe_vlan_id>>
```

```
exit
interface vfc12
switchport description <<var_node02>>:3a
bind interface Eth1/2
switchport trunk allowed vsan <<var_vsan_a_id>>
no shutdown
exit
interface po15
description <<var_ucs_clustername>>-A:FCoE
exit
interface Eth1/31-32
channel-group 15 mode active
exit
interface po15
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_fabric_a_fcoe_vlan_id>>
spanning-tree port type edge trunk
no shutdown
exit
interface vfc15
switchport description <<var_ucs_clustername>>-A:FCoE
bind interface po15
switchport trunk allowed vsan <<var_vsan_a_id>>
no shutdown
vsan database
vsan <<var_vsan_a_id>> name Fabric_A
vsan <<var_vsan_a_id>> interface vfc11
vsan <<var_vsan_a_id>> interface vfc12
vsan <<var_vsan_a_id>> interface vfc15
exit
```

Cisco Nexus 5548 B

To configure VSANs, assign vFC ports, and enable vFC ports on switch B, follow these steps:

From the global configuration mode, run the following commands:

```
vlan <<var_fabric_b_fcoe_vlan_id>>
name FCoE_Fabric_B
fcoe vsan <<var_vsan_b_id>>
exit
interface poll
switchport trunk allowed vlan add <<var_fabric_b_fcoe_vlan_id>>
exit
interface vfc11
switchport description <<var_node01>>:4a
bind interface Eth1/1
switchport trunk allowed vsan <<var_vsan_b_id>>
no shutdown
exit
interface po12
switchport trunk allowed vlan add <<var_fabric_b_fcoe_vlan_id>>
exit
interface vfc12
switchport description <<var_node02>>:4a
bind interface Eth1/2
switchport trunk allowed vsan <<var_vsan_b_id>>
no shutdown
exit
interface po15
description <<var_ucs_clustername>>-B:FCoE
exit.
interface Eth1/31-32
```

```
channel-group 15 mode active
exit
interface po15
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_fabric_b_fcoe_vlan_id>>
spanning-tree port type edge trunk
no shutdown
exit
interface vfc15
switchport description <<var_ucs_clustername>>-B:FCoE
bind interface po15
switchport trunk allowed vsan <<var_vsan_b_id>>
no shutdown
vsan database
vsan <<var_vsan_b_id>> name Fabric_B
vsan <<var_vsan_b_id>> interface vfc11
vsan <<var_vsan_b_id>> interface vfc12
vsan <<var_vsan_b_id>> interface vfc15
exit
```

Create Device Aliases

Cisco Nexus 5548 A

To configure device aliases and zones for the primary boot paths of switch A on <<var_nexus_A_hostname>>, follow these steps:

From the global configuration mode, run the following commands:

```
device-alias database
device-alias name VM-Host-Infra-01_A pwwn <<var_vm_host_infra_01_A_wwpn>>
device-alias name VM-Host-Infra-02_A pwwn <<var_vm_host_infra_02_A_wwpn>>
device-alias name <<var_controller1>>_1a pwwn <<var_controller1_1a_wwpn>>
device-alias name <<var_controller2>>_1a pwwn <<var_controller2_1a_wwpn>>
exit
device-alias commit
```

Cisco Nexus 5548 B

To configure device aliases and zones for the boot paths of switch B on <<var_nexus_B_hostname>>, follow these steps:

From the global configuration mode, run the following commands:

```
device-alias database
device-alias name VM-Host-Infra-01_B pwwn <<var_vm_host_infra_01_B_wwpn>>
device-alias name VM-Host-Infra-02_B pwwn <<var_vm_host_infra_02_B_wwpn>>
device-alias name <<var_controller1>>_1b pwwn <<var_controller1_1b_wwpn>>
device-alias name <<var_controller2>>_1b pwwn <<var_controller2_1b_wwpn>>
exit
device-alias commit
```

Create Zones

Cisco Nexus 5548 A

To create zones for the service profiles on switch A, follow these steps:

1. Create a zone for each service profile.

```
zone name VM-Host-Infra-01_A vsan <<var_vsan_a_id>>
member device-alias VM-Host-Infra-01_A
member device-alias <<var_controller1>>_1a
member device-alias <<var_controller2>>_1a
exit
zone name VM-Host-Infra-02_A vsan <<var_ vsan_a_id>>
member device-alias VM-Host-Infra-02_A
member device-alias <<var_controller1>>_1a
member device-alias <<var_controller2>>_1a
exit
```

2. After the zone for the Cisco UCS service profiles has been created, create the zone set and add the necessary members.

```
zoneset name FlexPod vsan <<var_ vsan_a_id>>
member VM-Host-Infra-01_A
member VM-Host-Infra-02_A
exit
```

3. Activate the zone set.

```
zoneset activate name FlexPod vsan <<var_ vsan_a_id>>
exit
copy run start
```

Cisco Nexus 5548 B

To create zones for the service profiles on switch B, follow these steps:

1. Create a zone for each service profile.

```
zone name VM-Host-Infra-01_B vsan <<var_ vsan_b_id>>
member device-alias VM-Host-Infra-01_B
member device-alias <<var_controller1>>_1b
member device-alias <<var_controller2>>_1b
exit
zone name VM-Host-Infra-02_B vsan <<var_ vsan_b_id>>
member device-alias VM-Host-Infra-02_B
member device-alias <<var_controller1>>_1b
member device-alias <<var_controller2>>_1b
exit
```

2. After all of the zones for the Cisco UCS service profiles have been created, create the zone set and add the necessary members.

1

```
zoneset name FlexPod vsan <<var_ vsan_b_id>>
member VM-Host-Infra-01_B
member VM-Host-Infra-02_B
exit
```

3. Activate the zone set.

```
zoneset activate name FlexPod vsan <<var_ vsan_b_id>>
exit
copy run start
```
Storage Part 2

Data ONTAP 7-Mode SAN Boot Storage Setup

The following subsections create initiator groups (igroups) on storage controller 1 and map the SAN boot LUNs to these igroups so that VMware ESXi can be installed on the LUNs for the two management hosts created.

Create Igroups

Enter the following commands to create two igroups:

Controller 1 Command Line Interface

```
igroup create -f -t vmware VM-Host-Infra-01 <<var_vm_host_infra_01_A_wwpn >>
<<var_vm_host_infra_01_B_wwpn >>
igroup create -f -t vmware VM-Host-Infra-02 <<var_vm_host_infra_02_A_wwpn >>
<<var_vm_host_infra_02_B_wwpn >>
```



To view the two igroups just created, type igroup show.

Controller 2 Command Line Interface

Map Boot LUNs to Igroups

Enter the following commands to map the boot LUNS to igroups.

Controller 1 Command Line Interface

lun map /vol/esxi_boot/VM-Host-Infra-01 VM-Host-Infra-01 0
lun map /vol/esxi_boot/VM-Host-Infra-02 VM-Host-Infra-02 0

VMware vSphere 5.1 Setup

FlexPod VMware ESXi 5.1 FCoE 7-Mode

This section provides detailed instructions for installing VMware ESXi 5.1 in a FlexPod environment. After the procedures are completed, two FCP-booted ESXi hosts will be provisioned. These deployment procedures are customized to include the environment variables.



Several methods exist for installing ESXi in a VMware environment. These procedures focus on how to use the built-in Keyboard, Video, Mouse (KVM) console and virtual media features in Cisco UCS Manager to map remote installation media to individual servers and connect to their Fibre Channel Protocol (FCP) boot Logical Unit Numbers (LUNs).

Log in to Cisco UCS 6200 Fabric Interconnect

Cisco UCS Manager

The IP KVM enables the administrator to begin the installation of the operating system (OS) through remote media. It is necessary to log in to the UCS environment to run the IP KVM.

To log in to the Cisco UCS environment, follow these steps:

- 1. Open a Web browser and enter the IP address for the Cisco UCS cluster address. This step launches the Cisco UCS Manager application.
- 2. Log in to Cisco UCS Manager by using the admin user name and password.
- 3. From the main menu, click the Servers tab.
- 4. Choose Servers > Service Profiles > root > VM-Host-Infra-01.
- 5. Right-click VM-Host-Infra-01 and choose KVM Console.
- 6. Choose Servers > Service Profiles > root > VM-Host-Infra-02.
- 7. Right-click VM-Host-Infra-02 and choose KVM Console Actions > KVM Console.

Set Up VMware ESXi Installation

ESXi Hosts VM-Host-Infra-01 and VM-Host-Infra-02

To prepare the server for the OS installation, follow these steps on each ESXi host:

- 1. In the KVM window, click the Virtual Media tab.
- 2. Click Add Image.
- 3. Browse to the ESXi installer ISO image file and click Open.
- 4. Check the Mapped check box to map the newly added image.
- 5. Click the KVM tab to monitor the server boot.
- 6. Boot the server by selecting Boot Server and click OK. Then click OK again.

Install ESXi

ESXi Hosts VM-Host-Infra-01 and VM-Host-Infra-02

To install VMware ESXi to the SAN-bootable LUN of the hosts, follow these steps on each host:

- 1. On reboot, the machine detects the presence of the ESXi installation media. Choose the ESXi installer from the menu that is displayed.
- 2. After the installer is finished loading, press Enter to continue with the installation.
- 3. Read and accept the end-user license agreement (EULA). Press F11 to accept and continue.

- 4. Choose the NetApp LUN that was previously set up as the installation disk for ESXi and press Enter to continue with the installation.
- 5. Choose the appropriate keyboard layout and press Enter.
- 6. Enter and confirm the root password and press Enter.
- 7. The installer issues a warning that existing partitions will be removed from the volume. Press F11 to continue with the installation.
- 8. After the installation is complete, uncheck the Mapped check box (located in the Virtual Media tab of the KVM console) to unmap the ESXi installation image.



Note The ESXi installation image must be unmapped to make sure that the server reboots into ESXi and not into the installer.

- **9.** The Virtual Media window might issue a warning stating that it is preferable to eject the media from the guest. Because the media cannot be ejected and it is read-only, simply click **Yes** to unmap the image.
- 10. From the KVM tab, press Enter to reboot the server.

Set Up Management Networking for ESXi Hosts

Adding a management network for each VMware host is necessary for managing the host. To add a management network for the VMware hosts, follow these steps on each ESXi host:

ESXi Host VM-Host-Infra-01

To configure the VM-Host-Infra-01 ESXi host with access to the management network, follow these steps:

- 1. After the server has finished rebooting, press F2 to customize the system.
- 2. Log in as root and enter the corresponding password.
- 3. Choose the Configure the Management Network option and press Enter.
- 4. (Optional) Choose the VLAN option and press Enter.
- 5. Enter the <<var_ib-mgmt_vlan_id>> and press Enter.
- 6. From the Configure Management Network menu, choose IP Configuration and press Enter.
- 7. Choose the Set Static IP Address and Network Configuration option by using the space bar.
- 8. Enter the IP address for managing the first ESXi host: <<var_vm_host_infra_01_ip>>.
- 9. Enter the subnet mask for the first ESXi host.
- 10. Enter the default gateway for the first ESXi host.
- 11. Press Enter to accept the changes to the IP configuration.
- 12. Choose the IPv6 Configuration option and press Enter.
- 13. Using the spacebar, deselect Enable IPv6 (restart required) and press Enter.
- 14. Choose the DNS Configuration option and press Enter.



Because the IP address is assigned manually, the DNS information must also be entered manually.

- 15. Enter the IP address of the primary DNS server.
- 16. (Optional) Enter the IP address of the secondary DNS server.
- 17. Enter the fully qualified domain name (FQDN) for the first ESXi host.
- **18.** Press Enter to accept the changes to the DNS configuration.
- 19. Press Esc to exit the Configure Management Network submenu.
- 20. Press Y to confirm the changes and return to the main menu.
- 21. The ESXi host reboots. After reboot, press F2 and log back in as root.
- **22.** Choose **Test Management Network** to verify that the management network is set up correctly and press **Enter**.
- 23. Press Enter to run the test.
- 24. Press Enter to exit the window.
- 25. Press Esc to log out of the VMware console.

ESXi Host VM-Host-Infra-02

To configure the VM-Host-Infra-02 ESXi host with access to the management network, follow these steps:

- 1. After the server has finished rebooting, press F2 to customize the system.
- 2. Log in as root and enter the corresponding password.
- 3. Choose the Configure the Management Network option and press Enter.
- 4. Choose the VLAN (Optional) option and press Enter.
- 5. Enter the <<var_ib-mgmt_vlan_id>> and press Enter.
- 6. From the Configure Management Network menu, choose IP Configuration and press Enter.
- 7. Choose the Set Static IP Address and Network Configuration option by using the space bar.
- 8. Enter the IP address for managing the second ESXi host: <<var_vm_host_infra_02_ip>>.
- 9. Enter the subnet mask for the second ESXi host.
- **10.** Enter the default gateway for the second ESXi host.
- 11. Press Enter to accept the changes to the IP configuration.
- 12. Choose the IPv6 Configuration option and press Enter.
- 13. Using the spacebar, deselect Enable IPv6 (restart required) and press Enter.
- 14. Choose the DNS Configuration option and press Enter.

- **Note** Because the IP address is assigned manually, the DNS information must also be entered manually.
- 15. Enter the IP address of the primary DNS server.

- 16. (Optional) Enter the IP address of the secondary DNS server.
- 17. Enter the FQDN for the second ESXi host.
- 18. Press Enter to accept the changes to the DNS configuration.
- 19. Press Esc to exit the Configure Management Network submenu.
- 20. Press Y to confirm the changes and return to the main menu.
- 21. The ESXi host reboots. After reboot, press F2 and log back in as root.
- 22. Choose Test Management Network to verify that the management network is set up correctly and press Enter.
- 23. Press Enter to run the test.
- 24. Press Enter to exit the window.
- 25. Press Esc to log out of the VMware console.

Download VMware vSphere Client and vSphere Remote CLI

To download the VMware vSphere Client and install Remote CLI, follow these steps:

- 1. Open a Web browser on the management workstation and navigate to the VM-Host-Infra-01 management IP address.
- **2.** Download and install both the vSphere Client and the Windows version of vSphere Remote Command Line.



Note These applications are downloaded from the VMware Web site and Internet access is required on the management workstation.

Log in to VMware ESXi Hosts by Using VMware vSphere Client

ESXi Host VM-Host-Infra-01

To log in to the VM-Host-Infra-01 ESXi host by using the VMware vSphere Client, follow these steps:

- 1. Open the recently downloaded VMware vSphere Client and enter the IP address of VM-Host-Infra-01 as the host you are trying to connect to: <<var_vm_host_infra_01_ip>>.
- **2.** Enter root for the user name.
- 3. Enter the root password.
- 4. Click Login to connect.

ESXi Host VM-Host-Infra-02

To log in to the VM-Host-Infra-02 ESXi host by using the VMware vSphere Client, follow these steps:

- 1. Open the recently downloaded VMware vSphere Client and enter the IP address of VM-Host-Infra-02 as the host you are trying to connect to: <<var_vm_host_infra_02_ip>>.
- **2.** Enter root for the user name.
- 3. Enter the root password.
- Click Login to connect.

Download Updated Cisco VIC enic and fnic Drivers

To download the Cisco virtual interface card (VIC) enic and fnic drivers, follow these steps:



The enic version used in this configuration is 2.1.2.38, and the fnic version is 1.5.0.20.

 Open a Web browser on the management workstation and navigate to http://software.cisco.com/download/release.html?mdfid=283853163&softwareid=283853158&rele ase=2.0(5)&relind=AVAILABLE&rellifecycle=&reltype=latest

Login and choose the driver ISO for version 2.1(1a). Download the ISO file. Once the ISO file is downloaded, either burn the ISO to a CD or map the ISO to a drive letter. Extract the following files from within the VMware directory for ESXi 5.1:

- Network net-enic-2.1.2.38-10EM.500.0.0.472560.x86_64.zip
- Storage scsi-fnic-1.5.0.20-10EM.500.0.0.472560.x86_64.zip
- 2. Document the saved location.

Load Updated Cisco VIC enic and fnic Drivers

ESXi Hosts VM-Host-Infra-01 and VM-Host-Infra-02

To load the updated versions of the enic and fnic drivers for the Cisco VIC, follow these steps for the hosts on each vSphere Client:

- 1. From each vSphere Client, choose the host in the inventory.
- 2. Click the Summary tab to view the environment summary.
- 3. From **Resources** > **Storage**, right-click datastore1 and choose Browse Datastore.
- 4. Click the fourth button and choose Upload File.
- 5. Navigate to the saved location for the downloaded enic driver version and choose net-enic-2.1.2.38-10EM.500.0.0.472560.x86_64.zip.
- 6. Click **Open** to open the file.
- 7. Click Yes to upload the .zip file to datastore1.
- 8. Click the fourth button and choose Upload File.
- **9.** Navigate to the saved location for the downloaded fnic driver version and choose scsi-fnic-1.5.0.20-10EM.500.0.0.472560.x86_64.zip.
- 10. Click Open to open the file.
- **11.** Click **Yes** to upload the .zip file to datastore1.
- **12.** From the management workstation, open the VMware vSphere Remote CLI that was previously installed.
- **13.** At the command prompt, run the following commands to account for each host (enic):

```
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> software vib
install --no-sig-check -d
/vmfs/volumes/datastore1/net-enic-2.1.2.38-10EM.500.0.0.472560.x86_64.zip
esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>> software vib
install --no-sig-check -d
/vmfs/volumes/datastore1/net-enic-2.1.2.38-10EM.500.0.0.472560.x86_64.zip
```

14. At the command prompt, run the following commands to account for each host (fnic):

esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> software vib install --no-sig-check -d /vmfs/volumes/datastore1/scsi-fnic-1.5.0.20-10EM.500.0.0.472560.x86_64.zip esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>> software vib install --no-sig-check -d /vmfs/volumes/datastore1/scsi-fnic-1.5.0.20-10EM.500.0.0.472560.x86_64.zip

- 15. From the vSphere Client, right-click each host in the inventory and choose **Reboot**.
- 16. Choose Yes to continue.
- 17. Enter a reason for the reboot and click OK.
- **18.** After the reboot is complete, log back in to both hosts using the vSphere Client.

Set Up VMkernel Ports and Virtual Switch

ESXi Host VM-Host-Infra-01

To set up the VMkernel ports and the virtual switches on the VM-Host-Infra-01 ESXi host, follow these steps:

- 1. From each vSphere Client, choose the host in the inventory.
- 2. Click the Configuration tab.
- 3. Click Networking in the Hardware pane.
- 4. Click **Properties** on the right side of vSwitch0.
- 5. Choose the vSwitch configuration and click Edit.
- 6. From the General tab, change the MTU to 9000.
- 7. Click **OK** to close the properties for vSwitch0.
- 8. Choose the Management Network configuration and click Edit.
- 9. Change the network label to VMkernel-MGMT and check the Management Traffic check box.
- 10. Click **OK** to finalize the edits for Management Network.
- 11. Choose the VM Network configuration and click Edit.
- **12.** Change the network label to IB-MGMT Network and enter <<var_ib-mgmt_vlan_id>> in the VLAN ID (Optional) field.
- 13. Click OK to finalize the edits for VM Network.
- 14. Click Add to add a network element.
- 15. Choose VMkernel and click Next.
- **16.** Change the network label to VMkernel-NFS and enter <<var_nfs_vlan_id>> in the VLAN ID (Optional) field.
- 17. Click Next to continue with the NFS VMkernel creation.
- **18.** Enter the IP address <<var_nfs_vlan_id_ip_host-01>> and the subnet mask <<var_nfs_vlan_id_mask_host01>> for the NFS VLAN interface for VM-Host-Infra-01.
- 19. Click Next to continue with the NFS VMkernel creation.
- 20. Click Finish to finalize the creation of the NFS VMkernel interface.
- 21. Choose the VMkernel-NFS configuration and click Edit.
- 22. Change the MTU to 9000.

- 23. Click OK to finalize the edits for the VMkernel-NFS network.
- 24. Click Add to add a network element.
- 25. Choose VMkernel and click Next.
- **26.** Change the network label to VMkernel-vMotion and enter **<<var_vmotion_vlan_id>>** in the VLAN ID (Optional) field.
- 27. Check the Use This Port Group for vMotion check box.
- 28. Click Next to continue with the vMotion VMkernel creation.
- **29.** Enter the IP address <<var_vmotion_vlan_id_ip_host-01>> and the subnet mask <<var_vmotion_vlan_id_mask_host-01>> for the vMotion VLAN interface for VM-Host-Infra-01.
- **30.** Click **Next** to continue with the vMotion VMkernel creation.
- 31. Click Finish to finalize the creation of the vMotion VMkernel interface.
- 32. Choose the VMkernel-vMotion configuration and click Edit.
- **33.** Change the MTU to 9000.
- 34. Click OK to finalize the edits for the VMkernel-vMotion network.
- **35.** Close the dialog box to finalize the ESXi host networking setup. The networking for the ESXi host should be similar to Figure 58.



Figure 58 vSphere Client Showing VMKernel Ports and Virtual Switch

ESXi Host VM-Host-Infra-02

To set up the VMkernel ports and the virtual switches on the VM-Host-Infra-02 ESXi host, follow these steps:

- **1.** From each vSphere Client, choose the host in the inventory.
- **2**. Click the **Configuration** tab.
- 3. Click Networking in the Hardware pane.
- 4. Click **Properties** on the right side of vSwitch0.
- 5. Choose the vSwitch configuration and click Edit.
- 6. From the General tab, change the MTU to 9000.
- 7. Click **OK** to close the properties for vSwitch0.

- 8. Choose the Management Network configuration and click Edit.
- 9. Change the network label to VMkernel-MGMT and check the Management Traffic check box.
- **10.** Click **OK** to finalize the edits for Management Network.
- 11. Choose the VM Network configuration and click Edit.
- 12. Change the network label to IB-MGMT Network and enter <<var_ib-mgmt_vlan_id>> in the VLAN ID (Optional) field.
- 13. Click OK to finalize the edits for VM Network.
- 14. Click Add to add a network element.
- 15. Choose VMkernel and click Next.
- **16.** Change the network label to VMkernel-NFS and enter <<var_nfs_vlan_id>> in the VLAN ID (Optional) field.
- 17. Click Next to continue with the NFS VMkernel creation.
- **18.** Enter the IP address <<var_nfs_vlan_id_ip_host-02>> and the subnet mask <<var_nfs_vlan_id_mask_host02>> for the NFS VLAN interface for VM-Host-Infra-02.
- 19. Click Next to continue with the NFS VMkernel creation.
- 20. Click Finish to finalize the creation of the NFS VMkernel interface.
- 21. Choose the VMkernel-NFS configuration and click Edit.
- 22. Change the MTU to 9000.
- 23. Click OK to finalize the edits for the VMkernel-NFS network.
- 24. Click Add to add a network element.
- 25. Choose VMkernel and click Next.
- **26.** Change the network label to VMkernel-vMotion and enter <<var_vmotion_vlan_id>> in the VLAN ID (Optional) field.
- 27. Check the Use This Port Group for vMotion check box.
- 28. Click Next to continue with the vMotion VMkernel creation.
- **29.** Enter the IP address <<var_vmotion_vlan_id_ip_host-02>> and the subnet mask <<var_vmotion_vlan_id_mask_host-02>> for the vMotion VLAN interface for VM-Host-Infra-02.
- **30.** Click Next to continue with the vMotion VMkernel creation.
- 31. Click Finish to finalize the creation of the vMotion VMkernel interface.
- 32. Choose the VMkernel-vMotion configuration and click Edit.
- **33**. Change the MTU to 9000.
- 34. Click OK to finalize the edits for the VMkernel-vMotion network.
- **35.** Close the dialog box to finalize the ESXi host networking setup. The networking for the ESXi host should be similar to Figure 59.



Figure 59 vSphere Client Showing VMKernel Ports and Virtual Switch

Mount Required Datastores

ESXi Hosts VM-Host-Infra-01 and VM-Host-Infra-02

To mount the required datastores, follow these steps on each ESXi host:

- 1. From each vSphere Client, choose the host in the inventory.
- 2. Click the **Configuration** tab to enable configurations.
- 3. Click **Storage** in the Hardware pane.
- 4. From the Datastore area, click Add Storage to open the Add Storage wizard.
- 5. Choose Network File System and click Next.

- 6. The wizard prompts for the location of the NFS export. Enter <<var_controller2_nfs_ip>> as the IP address for NFSIP Address for Controller 2.
- 7. Enter /vol/infra_datastore_1 as the path for the NFS export.
- 8. Make sure that the Mount NFS read only check box is unchecked.
- 9. Enter infra_datastore_1 as the datastore name.
- 10. Click Next to continue with the NFS datastore creation.
- 11. Click Finish to finalize the creation of the NFS datastore.
- 12. From the Datastore area, click Add Storage to open the Add Storage wizard.
- 13. Choose Network File System and click Next.
- **14.** The wizard prompts for the location of the NFS export. Enter <<var_controller1_nfs_ip>> as the IP address for NFSIP Address for Controller 1.
- 15. Enter /vol/infra_swap as the path for the NFS export.
- 16. Make sure that the Mount NFS read only check box is unchecked.
- 17. Enter infra_swap as the datastore name.
- **18.** Click **Next** to continue with the NFS datastore creation.
- 19. Click Finish to finalize the creation of the NFS datastore.

Configure NTP on ESXi Hosts

ESXi Hosts VM-Host-Infra-01 and VM-Host-Infra-02

To configure Network Time Protocol (NTP) on the ESXi hosts, follow these steps on each host:

- 1. From each vSphere Client, choose the host in the inventory.
- 2. Click the **Configuration** tab to enable configurations.
- 3. Click Time Configuration in the Software pane.
- 4. Click **Properties** at the upper right side of the window.
- 5. At the bottom of the Time Configuration dialog box, click **Options**.
- 6. In the NTP Daemon Options dialog box, follow these steps:
 - a. Click General in the left pane and choose Start and stop with host.
 - b. Click NTP Settings in the left pane and click Add.
- 7. In the Add NTP Server dialog box, enter <<var_global_ntp_server_ip>> as the IP address of the NTP server and click **OK**.
- 8. In the NTP Daemon Options dialog box, check the Restart NTP Service to Apply Changes check box and click **OK**.
- 9. In the Time Configuration dialog box, follow these steps:
 - a. Check the NTP Client Enabled check box and click OK.
 - **b.** Verify that the clock is now set to approximately the correct time.



The NTP server time may vary slightly from the host time.

Move VM Swap File Location

ESXi Hosts VM-Host-Infra-01 and VM-Host-Infra-02

To move the VM swap file location, follow these steps on each ESXi host:

- 1. From each vSphere Client, choose the host in the inventory.
- 2. Click the Configuration tab to enable configurations.
- 3. Click Virtual Machine Swapfile Location in the Software pane.
- 4. Click Edit at the upper right side of the window.
- 5. Choose Store the swapfile in a swapfile datastore selected below.
- 6. Select infra_swap as the datastore in which to house the swap files.
- 7. Click **OK** to finalize moving the swap file location.

FlexPod VMware vCenter 5.1

The procedures in the following subsections provide detailed instructions for installing VMware vCenter 5.1 in a FlexPod environment. After the procedures are completed, a VMware vCenter Server will be configured along with a Microsoft SQL Server database to provide database support to vCenter. These deployment procedures are customized to include the environment variables.



This procedure focuses on the installation and configuration of an external Microsoft SQL Server 2008 R2 database, but other types of external databases are also supported by vCenter. For information about how to configure the database and integrate it into vCenter, see the VMware vSphere5.1 documentation at: http://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html

To install VMware vCenter 5.1, an accessible Windows Active Directory® (AD) Domain is necessary. If an existing AD Domain is not available, an AD virtual machine, or AD pair, can be set up in this FlexPod environment. See "Appendix" section on page 192 for this setup.

Build Microsoft SQL Server VM

ESXi Host VM-Host-Infra-01

To build a SQL Server virtual machine (VM) for the VM-Host-Infra-01 ESXi host, follow these steps:

- 1. Log in to the host by using the VMware vSphere Client.
- 2. In the vSphere Client, choose the host in the inventory pane.
- 3. Right-click the host and choose New Virtual Machine.
- 4. Click Custom and then click Next.
- 5. Enter a name for the VM. Click Next.
- 6. Choose infra_datastore_1. Click Next.
- 7. Choose Virtual Machine Version: 8. Click Next.
- Verify that the Windows option and the Microsoft Windows Server 2008 R2 (64-bit) version are selected. Click Next.

- 9. Choose two virtual sockets and one core per virtual socket. Click Next.
- 10. Choose 4GB of memory. Click Next.
- **11**. Choose one network interface card (NIC).
- 12. For NIC 1, choose the IB-MGMT Network option and the VMXNET 3 adapter. Click Next.
- 13. Keep the LSI Logic SAS option for the SCSI controller selected. Click Next.
- 14. Keep the Create a New Virtual Disk option selected. Click Next.
- 15. Make the disk size at least 60GB. Click Next.
- 16. Click Next.
- 17. Check the Edit the Virtual Machine Settings Before Completion check box. Click Continue.
- **18.** Choose the **Options** tab.
- 19. Choose Boot Options.
- 20. Check the Force BIOS Setup check box.
- 21. Click Finish.
- 22. From the left pane, expand the host field by clicking the plus sign (+).
- 23. Right-click the newly created SQL Server VM and click Open Console.
- 24. Click the third button (green right arrow) to power on the VM.
- **25.** Click the ninth button (CD with a wrench) to map the Windows Server 2008 R2 SP1 ISO, and then choose **Connect to ISO Image on Local Disk**.
- 26. Navigate to the Windows Server 2008 R2 SP1 ISO, select it, and click Open.
- **27.** In the BIOS Setup Utility window and use the right arrow key to navigate to the Boot menu. Use the down arrow key to select CD-ROM Drive. Press the plus (+) key twice to move CD-ROM Drive to the top of the list. Press F10 and Enter to save the selection and exit the BIOS Setup Utility.
- **28.** The Windows Installer boots. Choose the appropriate language, time and currency format, and keyboard. Click **Next**.
- 29. Click Install Now.
- **30.** Make sure that the Windows Server 2008 R2 Standard (Full Installation) option is selected. Click **Next**.
- 31. Read and accept the license terms and click Next.
- **32.** Choose Custom (Advanced). Make sure that Disk 0 Unallocated Space is selected. Click **Next** to allow the Windows installation to complete.
- **33.** After the Windows installation is complete and the VM has rebooted, click **OK** to set the Administrator password.
- **34.** Enter and confirm the Administrator password and choose the blue arrow to log in. Click **OK** to confirm the password change.
- **35.** After logging in to the VM desktop, from the VM console window, choose the VM menu. Under Guest, choose Install/Upgrade VMware Tools. Click **OK**.
- **36.** If prompted to eject the Windows installation media before running the setup for the VMware tools, click **OK**, then click **OK**.
- **37.** In the dialog box, choose Run setup64.exe.
- 38. In the VM ware Tools installer window, click Next.

- **39**. Make sure that Typical is selected and click Next.
- 40. Click Install.
- 41. Click Finish.
- 42. Click Yes to restart the VM.
- **43.** After the reboot is complete, choose the VM menu. Under Guest, choose Send Ctrl+Alt+Del and then enter the password to log in to the VM.
- **44.** Set the time zone for the VM, IP address, gateway, and host name. Add the VM to the Windows AD domain.



45. If necessary, activate Windows.

46. Log back in to the VM and download and install all required Windows updates.

Note This process requires several reboots.

Install Microsoft SQL Server 2008 R2

vCenter SQL Server VM

To install SQL Server on the vCenter SQL Server VM, follow these steps:

- 1. Connect to an AD Domain Controller in the FlexPod Windows Domain and add an admin user for the FlexPod using the Active Directory Users and Computers tool. This user should be a member of the Domain Administrators security group.
- 2. Log in to the vCenter SQL Server VM as the FlexPod admin user and open Server Manager.
- 3. Expand Features and click Add Features.
- 4. Expand .NET Framework 3.5.1 Features and choose only .NET Framework 3.5.1.

rigure		GIVEI
Add Features Wizard		×
Features Confirmation Progress Results	Select one or more features to install on this server. Eeatures: Image: Image: Image	Description: <u>Microsoft .NET Framework 3.5.1</u> combines the power of the .NET Framework 2.0 APIs with new technologies for building applications
	Background Intelligent Transfer Service (BITS) BitLocker Drive Encryption BranchCache Connection Manager Administration Kit Desktop Experience DirectAccess Management Console Group Policy Management Ink and Handwriting Services Internet Printing Client Internet Storage Name Server LPR Port Monitor Message Queuing Multipath I/O Network Load Balancing Peer Name Resolution Protocol Quality Windows Audio Video Experience Remote Assistance More about features	 Install Cancel

Figure 60 Adding Features for Installing SQL Server

- 5. Click Next.
- 6. Click Install.
- 7. Click Close.
- Open Windows Firewall with Advanced Security by navigating to Start > Administrative Tools > Windows Firewall with Advanced Security.
- 9. Choose Inbound Rules and click New Rule.
- 10. Choose Port and click Next.
- **11.** Choose TCP and enter the specific local port 1433. Click Next.
- 12. Choose Allow the Connection. Click Next, and then click Next again.
- 13. Name the rule SQL Server and click Finish.
- 14. Close Windows Firewall with Advanced Security.
- **15.** In the vCenter SQL Server VMware console, click the ninth button (CD with a wrench) to map the Microsoft SQL Server 2008 R2 ISO. Choose Connect to ISO Image on Local Disk.

- 16. Navigate to the SQL Server 2008 R2 ISO, select it, and click Open.
- **17.** In the dialog box, click Run setup.exe.
- 18. In the SQL Server Installation Center window, click Installation on the left.

- 🗆 ×

- **19.** Choose New Installation or Add Features to an Existing Installation.
- 20. Click OK.
- 21. Choose Enter the Product Key. Enter a product key and click Next.
- 22. Read and accept the license terms and choose whether to check the second check box. Click Next.
- 23. Click Install to install the setup support files.
- 24. Address any warnings except for the Windows firewall warning. Click Next.



The Windows firewall issue was addressed in Step 13.

- 25. Choose SQL Server Feature Installation and click Next.
- 26. Under Instance Features, choose only Database Engine Services.
- 27. Under Shared Features, choose Management Tools > Basic and Management Tools > Complete. Click Next.

Figure 61 Selecting SQL Server Features

SQL Server 2008 R2 Setup

Г	eau	ure	Sel	ecu	On

Select the Standard features to install.

Setup Role Instance Features Server features are instance- aware and have their own registry hives. They support Instance Configuration Instance Configuration Quid-Services Server Replication Disk Space Requirements Reporting Services Shared Features Shared Features Disk Space Requirements Shared Features Database Engine Configuration Disk Space Requirements Shared Features Database Engine Configuration Rules Disk Space Requirements Studio Client Tools Connectivity Installation Progress Client Tools SDK SQL Server Robids Compatibility Client Tools SDK SQL Server Robids Complete Management Tools - Complete SQL Client Connectivity SDK Microsoft Sync Framework Microsoft Sync Framework Redistributable Feature directory: C:\Program Files\Microsoft SQL Server\	Setup Support Rules	Eeatures:	Description:
Select All Linselect All Shared feature directory: C:\Program Files\Microsoft SQL Server\ Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\	Setup Role Feature Selection Installation Rules Instance Configuration Disk Space Requirements Server Configuration Database Engine Configuration Error Reporting Installation Configuration Rules Ready to Install Installation Progress Complete	Instance Features Image: Database Engine Services SQL Server Replication Full-Text Search Analysis Services Reporting Services Shared Features Business Intelligence Development Studio Client Tools Connectivity Integration Services Client Tools Soncetivity Integration Services Client Tools Backwards Compatibility Client Tools SOK SQL Server Books Online Management Tools - Basic Management Tools - Complete SQL Client Connectivity SDK Microsoft Sync Framework Redistributable Features	Server features are instance- aware and have their own registry hives. They support multiple instances on a computer.
		Select All Unselect All Shared feature directory: C:\Program Files\Microsoft SQL Server\ Shared feature directory (x86)	er\

體 SQL

- 28. Click Next.
- 29. Keep Default Instance selected. Click Next.

SQL Server 2008 R2 Setup					_ 🗆 🗵
Instance Configuration					
Specify the name and instance ID fo	r the instance of SQL Serve	r. Instance ID bec	omes part of the instal	ation path.	
Setup Support Rules	Default instance				
Setup Role Feature Selection	C Named instance:	MSSQLSERVER			
Installation Rules					
Instance Configuration	Instance <u>I</u> D:	MSSQLSERVER			
Server Configuration	Instance root directory:	C:\Program Files	Microsoft SQL Server\		
Database Engine Configuration					
Error Reporting	SQL Server directory:	C:\Program Files	Microsoft SQL Server\	MSSQL10_50.MSSQLSE	RVER
Ready to Install	Installed instances:				
Installation Progress	Instance Name	Instance ID	Features	Edition	Version
Complete					

- 30. Click Next for Disk Space Requirements.
- 31. For the SQL Server Agent service, click in the first cell in the Account Name column and then click <<Browse...>>.

- 32. Enter the local machine administrator name (for example, systemname\Administrator), click Check Names, and click OK.
- 33. Enter the administrator password in the first cell under Password.
- 34. Change the startup type for SQL Server Agent to Automatic.
- 35. For the SQL Server Database Engine service, choose Administrator in the Account Name column and enter the administrator password again. Click Next.

Figure 63 Configuring SQL Server

I

ſ

SQL Server 2008 R2 Setup					_
Server Configuration					
Specify the service accounts and col	llation configuration.				
ietup Support Rules ietup Role Feature Selection	Service Accounts Collation	e a separate account for each SQI	L Server service.		
installation Rules	Service	Account Name	Password	Startup Typ	в
nstance Configuration	SQL Server Agent	Administrator	•••••	Automatic	•
isk Space Requirements	SQL Server Database Engine	Administrator	•••••	Automatic	-
erver Configuration	SQL Server Browser	NT AUTHORITY\LOCAL S		Disabled	-
omplete					
		rout 1		. 1	

36. Choose Mixed Mode (SQL Server Authentication and Windows Authentication). Enter and confirm the password for the SQL Server system administrator (sa) account, click Add Current User, and Click **Next**.

Figure 64 Configuring Database Engine

SQL Server 2008 R2 Setup Database Engine Confid	 uration
Specify Database Engine authentic	ation security mode, administrators and data directories.
Setup Support Rules Setup Role Feature Selection Installation Rules Instance Configuration Disk Space Requirements Server Configuration Database Engine Configuration Error Reporting Installation Configuration Rules Ready to Install Installation Progress Complete	Account Provisioning Data Directories FILESTREAM Specify the authentication mode and administrators for the Database Engine. Authentication Mode O Windows authentication mode Mixed Mode (SQL Server authentication and Windows authentication) Specify the password for the SQL Server system administrator (sa) account. Enter password: Confirm password: Specify SQL Server administrators
Lompiete	ICE vceru-solmin (cet 1 admin) SQL Server administrators have unrestricted access to the Database Engine. Add Current User Add

- 37. Choose whether to send error reports to Microsoft. Click Next.
- 38. Click Next.
- 39. Click Install.
- 40. After the installation is complete, click Close to close the SQL Server installer.
- 41. Close the SQL Server Installation Center.
- **42.** Install all available Microsoft Windows updates by navigating to **Start > All Programs > Windows Update**.
- Choose Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio to open the SQL Server Management Studio.
- **44.** Under Server Name, choose the local machine name. Under Authentication, choose SQL Server Authentication. Enter sa in the Login field and enter the sa password. Click **Connect**.

- 45. Click New Query.
- 46. Run the following script, substituting the vpxuser password for <Password>:

use [master]

```
go
   CREATE DATABASE [VCDB] ON PRIMARY
   (NAME = N'vcdb', FILENAME = N'C:\VCDB.mdf', SIZE = 2000KB, FILEGROWTH = 10% )
   LOG ON
   (NAME = N'vcdb_log', FILENAME = N'C:\VCDB.ldf', SIZE = 1000KB, FILEGROWTH = 10%)
   COLLATE SQL_Latin1_General_CP1_CI_AS
   go
   use VCDB
   go
   sp_addlogin @loginame=[vpxuser], @passwd=N'<Password>', @defdb='VCDB',
   @deflanguage='us_english'
   go
   ALTER LOGIN [vpxuser] WITH CHECK_POLICY = OFF
   qo
   CREATE USER [vpxuser] for LOGIN [vpxuser]
   go
   use MSDB
   go
   CREATE USER [vpxuser] for LOGIN [vpxuser]
   go
   use VCDB
   go
   sp_addrolemember @rolename = 'db_owner', @membername = 'vpxuser'
   go
   use MSDB
   go
   sp_addrolemember @rolename = 'db_owner', @membername = 'vpxuser'
   go
 Note
```

Figure 65 illustrates the script.

I



Figure 65 Executing the Query

- 47. Click Execute and verify that the query executes successfully.
- 48. Close Microsoft SQL Server Management Studio.
- 49. Disconnect the Microsoft SQL Server 2008 R2 ISO from the SQL Server VM.

Build and Set Up VMware vCenter VM

Build VMware vCenter VM

To build the VMware vCenter VM, follow these steps:

- Using the instructions for building a SQL Server VM provided in the section "Build Microsoft SQL Server VM," build a VMware vCenter VM with the following configuration in the <<var_ib-mgmt_vlan_id>> VLAN:
 - 4GB RAM
 - Two CPUs
 - One virtual network interface
- **2.** Start the VM, install VMware Tools, and assign an IP address and host name to it in the Active Directory domain.

I

Set Up VMware vCenter VM

To set up the newly built VMware vCenter VM, follow these steps:

- 1. Log in to the vCenter VM as the FlexPod admin user and open Server Manager.
- 2. Expand Features and click Add Features.
- 3. Expand .NET Framework 3.5.1 Features and choose only .NET Framework 3.5.1.
- 4. Click Next.
- 5. Click Install.
- 6. Click Close to close the Add Features wizard.
- 7. Close Server Manager.
- **8.** Download and install the client components of the Microsoft SQL Server 2008 R2 Native Client from the Microsoft Download Center.
- Create the vCenter database data source name (DSN). Choose Start > Administrative Tools > Data Sources (ODBC) to open Data Sources (ODBC).
- **10.** Choose the System DSN tab.
- 11. Click Add.
- 12. Choose SQL Server Native Client 10.0 and click Finish.
- **13.** Name the data source VCDB. In the Server field, enter the IP address of the vCenter SQL server. Click **Next**.

Figure 66 Creating New Data Source

Create a New Data Sou	rce to SQL Server	×
SQL Server 2008 R2	This wizard will help you create an ODBC data source that you can use connect to SQL Server. What name do you want to use to refer to the data source? Name: VCDB How do you want to describe the data source? Description: Which SQL Server do you want to connect to? Server: 192.168.175.214	
	Finish <u>N</u> ext > Cancel Help	

14. Choose With SQL Server authentication using a login ID and password entered by the user. Enter vpxuser as the login ID and the vpxuser password. Click **Next**.

SQL Server 2008 R2	How should SQL Server verify the authenticity of the login ID?
	Password: ••••••• Connect to SQL Server to obtain default settings for the additional configuration options.
	< <u>B</u> ack <u>N</u> ext > Cancel Help

Figure 67 Login Credentials for SQL Server

15. Choose Change the Default Database To and choose VCDB from the list. Click Next.

1

Freate a New Data Sou	rce to SQL Server	×
6	Change the default database to:	
	VCDB	
SQL Server 2008 R2	Mirror server:	
	SPN for mirror server (Optional):	
	Attach database filename:	
	Use ANSI quoted identifiers.	
Real Providence	✓ Use ANSI nulls, paddings and warnings.	
	< <u>B</u> ack <u>N</u> ext > Cancel	Help

Figure 68 Setting Up the Database

16. Click Finish.

17. Click Test Data Source. Verify that the test completes successfully.

Figure 69	Verifying ODBC Data Source
-----------	----------------------------

Microsoft SQL Server Native Client Version 10.50.1600 Running connectivity tests Attempting connection	~
Connection established Verifying option settings Disconnecting from server TESTS COMPLETED SUCCESSFULLY!	
	7

- 18. Click OK and then click OK again.
- 19. Click OK to close the ODBC Data Source Administrator window.
- Install all available Microsoft Windows updates by navigating to Start > All Programs > Windows Update.



Note A restart might be required.

Install VMware vCenter Server

vCenter Server VM

To install vCenter Server on the vCenter Server VM, follow these steps:

- 1. In the vCenter Server VMware console, click the ninth button (CD with a wrench) to map the VMware vCenter ISO and choose Connect to ISO Image on Local Disk.
- 2. Navigate to the VMware vCenter 5.1 (VIMSetup) ISO, select it, and click Open.
- 3. In the dialog box, click **Run autorun.exe**.
- 4. In the VMware vCenter Installer window, make sure that VMware vCenter Simple Install is selected and click Install.

Figure 70

Installing VMware vSphere

伊 VMware vCenter Installer



- 5. Click Yes at the User Account Control warning.
- 6. Click Next to install vCenter Single Sign On.
- 7. Click Next.
- Accept the terms of the license agreement and click **Next**. 8.
- 9. Enter and confirm <<var_password>> for admin@System-Domain. Click Next.
- 10. Keep the radio button checked to install a local Microsoft SQL Server 2008 R2 Express instance and click Next.
- 11. Enter and confirm <<var_password>> for both user names. Click Next.
- 12. Verify the vCenter VM FQDN and click Next.
- 13. Leave Use network service account selected and click Next.
- 14. Click Next to select the default destination folder.
- 15. Click Next to select the default HTTPS port.
- 16. Click Install to install vCenter Single Sign On.

- 17. Click Yes at the User Account Control warning.
- **18**. Click **Yes** at the User Account Control warning.
- **19.** Enter the vCenter 5.1 license key and click **Next**.
- **20.** Choose Use an Existing Supported Database. Choose VCDB from the Data Source Name list and click **Next**.

Figure 71 Selecting Database for VMware vSphere

🙀 VMware vCenter Simple Ins	tall	×
Database Options Select an ODBC data source for	r vCenter Server.	
vCenter Server requires a databa	ase.	
C Install a Microsoft SQL Server hosts and 50 virtual machines	r 2008 Express instance (for small deployments: s)	up to 5
Use an existing supported data	tabase	
Data Source Name (DSN):	VCDB (MS SQL)	
InstallShield	< Back Next >	Cancel

21. Enter the vpxuser password and click Next.

ſ

Fig	Figure 72 Entering Data		atabase Login C	base Login Credentials	
VMware vCenter Simple	e Install				
Database Options					
Enter database server cre	edentials.				
DSN:	VCDB				
ODBC Driver:	SQL Se	rver Native Clie	ent 10.0		
Database <u>u</u> ser name:	vpxuse	r			
Database password:	••••	•••••			
tallShield					
		< Back	Next >	Cancel	

- 22. Review the warning and click OK.
- 23. Click Next to use the SYSTEM Account.
- 24. Click Next to accept the default ports.
- 25. Choose the appropriate inventory size. Click Next.
- 26. Click Install.
- 27. Click Finish.
- **28.** Click **OK** to confirm the installation.
- 29. Click Exit in the VMware vCenter Installer window.
- **30.** Disconnect the VMware vCenter ISO from the vCenter VM.
- **31.** Install all available Microsoft Windows updates by navigating to **Start > All Programs > Windows Updates**.



• A restart might be required.

Set Up vCenter Server

vCenter Server VM

To set up vCenter Server on the vCenter Server VM, follow these steps:

1. Using the vSphere Client, log in to the newly created vCenter Server as the FlexPod admin user.

2. Click Create a data center.

- **3**. Enter FlexPod_DC_1 as the data center name.
- 4. Right-click the newly created FlexPod_DC_1 data center and choose New Cluster.
- 5. Name the cluster FlexPod_Management and click the check boxes for Turn On vSphere HA and Turn on vSphere DRS. Click Next.

🕗 New Cluster Wizard	
Cluster Features What features do you want t	o enable for this cluster?
Cluster Features vSphere DRS Power Management vSphere HA Virtual Machine Options VM Monitoring VMware EVC VM Swapfile Location Ready to Complete	Name FlexPod_Management Cluster Features Select the features you would like to use with this cluster. ✓ Turn On vSphere HA vSphere HA detects failures and provides rapid recovery for the virtual machines running within a cluster. Core functionality includes host and virtual machine monitoring to minimize downtime when heartbeats cannot be detected. vSphere HA must be turned on to use Fault Tolerance. ✓ Turn On vSphere DRS vSphere DRS enables vCenter Server to manage hosts as an aggregate pool of resources. Cluster resources can be divided into smaller resource pools for users, groups, and virtual machines. vSphere DRS automatically, suggesting placement when virtual machines are powered on, and migrating running virtual machines to balance load and enforce resource allocation policies. vSphere DRS and VMware EVC should be enabled in the cluster in order to permit placing and migrating VMs with Fault Tolerance turned on, during load balancing.
Help	< Back Next > Cancel

- 6. Accept the defaults for vSphere DRS. Click Next.
- 7. Accept the defaults for Power Management. Click Next.
- 8. Accept the defaults for vSphere HA. Click Next.
- 9. Accept the defaults for Virtual Machine Options. Click Next.
- 10. Accept the defaults for VM Monitoring. Click Next.
- 11. Accept the defaults for VMware EVC. Click Next.

ſ



If mixing UCS B or C-Series M2 and M3 servers within a vCenter cluster, it is necessary to enable VMware Enhanced vMotion Compatibility (EVC) mode. For more information about setting up EVC mode, see Enhanced vMotion Compatibility (EVC) Processor Support at: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&e xternalId=1003212

- 12. Choose Store the swapfile in the datastore specified by the host. Click Next.
- 13. Click Finish.
- 14. Right-click the newly created FlexPod_Management cluster and choose Add Host.
- **15.** In the Host field, enter either the IP address or the host name of the VM-Host-Infra_01 host. Enter root as the user name and the root password for this host. Click **Next**.
- 16. Click Yes.
- 17. Click Next.
- **18.** Choose Assign a New License Key to the Host. Click Enter Key and enter a vSphere license key. Click **OK**, and then click **Next**.
- 19. Click Next.
- 20. Click Next.
- 21. Click Finish. VM-Host-Infra-01 is added to the cluster.
- 22. Repeat this procedure to add VM-Host-Infra-02 to the cluster.

FlexPod Cisco Nexus 1110-X and 1000V vSphere

The following sections provide detailed procedures for installing a pair of high-availability (HA) Cisco Nexus 1110-X Virtual Services Appliances (VSAs) in a FlexPod configuration. Primary and standby Cisco Nexus 1000V Virtual Supervisor Modules (VSMs) are installed on the 1110-Xs. By the end of this section, a Cisco Nexus 1000V distributed virtual switch (DVS) will be provisioned. This procedure assumes that the Cisco Nexus 1000V software version 4.2(1)SV2(1.1a) has been downloaded from www.cisco.com and expanded. This procedure also assumes that VMware vSphere 5.1 Enterprise Plus licensing is installed.

Configure CIMC Interface on Both Cisco Nexus 1110-Xs

Cisco Nexus 1110-X A and Cisco Nexus 1110-X B

To configure the Cisco Integrated Management Controller (CIMC) interface on the Cisco Nexus 1110-X VSAs, follow these steps:

- 1. Using the supplied dongle, connect a monitor and USB keyboard to the KVM console port on the front of the Cisco Nexus 1110-X virtual appliance.
- 2. Reboot the virtual appliance.
- 3. Press F8 when prompted to configure the CIMC interface.
- 4. Using the spacebar, set the NIC mode to Dedicated.
- 5. Clear the check box for DHCP enabled.
- 6. Set the CIMC IP address (<<var_cimc_ip>>) in the out-of -band management VLAN.

- 7. Set the CIMC subnet mask (<<var_cimc_mask>>).
- 8. Set the CIMC gateway (<<var_cimc_gateway>>).
- 9. Set the NIC redundancy to None.
- **10.** Set and reenter the CIMC default password (<<var_password>>).
- **11**. Press F10 to save the configuration.
- 12. Continue pressing F5 until Network settings configured is shown.
- **13**. Press Esc to reboot the virtual appliance.

Configure Serial over LAN for Both Cisco Nexus 1110-Xs

Cisco Nexus 1110-X A and Cisco Nexus 1110-X B

I

To configure serial over LAN on the Cisco Nexus 1110-X VSAs, follow these steps:

- 1. Use a Web browser to open the URL at http://<<var_cimc_ip>>.
- 2. Log in to the CIMC with the admin user id and the CIMC default password (<<var_password>>).
- 3. In the left column, click **Remote Presence**.
- 4. Click the Serial over LAN tab.
- 5. Check the Enabled check box for Serial over LAN Properties.
- 6. From the Baud Rate drop-down menu, choose 9600 bps.
- 7. Click Save Changes.

Cisco Integrated Management Cor	ntroller WebUI - Windows Internet Explorer		
Cisco Integ	rated Management Controller	CIMC Hostname: Logged in as:	값 값 않 ucs-c220-m3 admin@192.168.17 Log Out
Overall Server Status Good Server Admin Summary Inventory Sensors System Event Log Remote Presence BIOS Power Policies Fault Summary	C C Comport Lan Properties Enabled: Com Port: com0		
		Save Change	Reset Values

Figure 74 Configuring Serial Over LAN on Cisco Nexus 1110-Xs

1

1

- 8. Log out of the CIMC Web interface.
- 9. Use an SSH client to connect to <<var_cimc_ip>> with the default CIMC user name and password.
- **10.** Run connect host.



Figure 75 Execute Command for Connecting the Host

Configure Cisco Nexus 1110-X Virtual Appliances

Cisco Nexus 1110-X A

To configure Cisco Nexus 1110-X A, follow these steps:

1. Reboot the virtual appliance. The appliance should boot into a setup mode.

```
Enter the password for "admin": <<var_password>>
Confirm the password for "admin": <<var_password>>
Enter HA role[primary/secondary]: primary
Enter network-uplink type <1-5>: 1
Enter control VLAN <1-3967, 4048-4093>: <<var_pkt-ctrl_vlan_id>>
Enter the domain<1-4095>: <<var_1110x_domain_id>>
Enter management vlan <1-3967, 4048-4093>: <<var_ib-mgmt_vlan_id>>
Would you like to enter the basic system configuration dialogue (yes/no): yes
Create another login account (yes/no) [n]: Enter
Configure read-only SNMP community string (yes/no)[n]: Enter
Configure read-write SNMP community string (yes/no)[n]: Enter
Enter the VSA name : <<var_1110x_vsa>>
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
Mgmt0 IP address type V4/V6? (V4): Enter
Mgmt0 IPv4 address : <<var_1110x_vsa_ip>>
Mgmt0 IPv4 netmask : <<var_1110x_vsa_mask>>
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway : <<var_1110x_vsa_gateway>>
Configure advanced IP options? (yes/no) [n]: Enter
Enable the telnet service? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter
Type of ssh key you would like to generate (das/rsa) [rsa]: Enter
Number of rsa key bits <768-2048> [1024]: Enter
Enable the http server? (yes/no) [y]: Enter
Configure the ntp server? (yes/no) [n]: y
```

NTP server IPv4 address: <<var_global_ntp_server_ip>>

2. Review the configuration summary. If everything is correct, enter no to skip editing the configuration.

Would you like to edit the configuration? (yes/no) [n]: Enter Use this configuration and save it? (yes/no) [y]: Enter

3. The Cisco Nexus 1110-X saves the configuration and reboots. After reboot, log back in as admin.

Cisco Nexus 1110-X B

To configure the Cisco Nexus 1110-X B, follow these steps:

1. Reboot the virtual appliance. The appliance should boot into a setup mode.

Enter the password for "admin": <<var_password>>

Note

This is the same password that you entered on the primary Cisco Nexus 1110-X.

2. Enter the admin password again to confirm: <<var_password>>.

```
Enter HA role[primary/secondary]: secondary
Enter network-uplink type <1-5>: 1
Enter control vlan <1-3967, 4048-4093>: <<var_pkt-ctrl_vlan_id>>
Enter the domain id<1-4095>: <<var_1110x_domain_id>>
```



This is the same unique Cisco Nexus 1110 domain ID entered on Cisco Nexus 1110-X A.

Enter management vlan <1-3967, 4048-4093>: <<var_ib-mgmt_vlan_id>>

3. The Cisco Nexus 1110-X saves the configuration and reboots.

Set Up the Primary Cisco Nexus 1000V VSM

Cisco Nexus 1110-X A

To set up the primary Cisco Nexus 1000V VSM on the Cisco Nexus 1110-X A, follow these steps:

1. Continue periodically running the following command until module 2 (Cisco Nexus 1110-X B) has a status of ha-standby.

show module

2. Enter the global configuration mode and create a virtual service blade.

```
config t
virtual-service-blade VSM-1
dir /repository
```

3. If the desired Cisco Nexus 1000V ISO file (nexus-1000v.4.2.1.SV2.1.1a.iso) is not present on the Cisco Nexus 1110-X, run the copy command to copy it to the Cisco Nexus 1110-X disk. You must place the file either on an FTP server or on a UNIX® or Linux® machine (using scp) that is accessible from the Cisco Nexus 1110-X management interface. An example copy command from an FTP server is copy ftp://<<var_ftp_server>>/nexus-1000v.4.2.1.SV2.1.1a.iso/repository/.

```
virtual-service-blade-type new nexus-1000v.4.2.1.SV2.1.1a.iso
interface control vlan <<var_pkt-ctrl_vlan_id>>
```

```
interface packet vlan <<var_pkt-ctrl_vlan_id>>
enable primary
Enter vsb image:[nexus-1000v.4.2.1.SV2.1.1a.iso] Enter
Enter domain id[1-4095]: <<var_vsm_domain_id>>
```

```
Note
```

This domain ID should be different than the VSA domain ID.

```
Enter SVS Control mode (L2 / L3): [L3] Enter
Management IP version [V4/V6]: [V4] Enter
Enter Management IP address: <<var_vsm_mgmt_ip>>
Enter Management subnet mask: <<var_vsm_mgmt_mask>>
IPv4 address of the default gateway: <<var_vsm_mgmt_gateway>>
Enter HostName: <<var_vsm_hostname>>
Enter the password for 'admin': <<var_password>>
copy run start
```

4. Run show virtual-service-blade summary. Continue periodically entering this command until the primary VSM-1 has a state of VSB POWERED ON.

Set Up the Secondary Cisco Nexus 1000V VSM

To set up the secondary Cisco Nexus 1000V VSM on Cisco Nexus 1110-X B, follow these steps in two subsections:

Cisco Nexus 1110-X A

Run system switchover to activate Cisco Nexus 1110-X B.

Cisco Nexus 1110-X B

1. Log in to Cisco Nexus 1110-X B as the admin user.

```
config t
virtual-service-blade VSM-1
dir /repository
```

2. If the desired Cisco Nexus 1000V ISO file (nexus-1000v.4.2.1.SV2.1.1a.iso) is not present on the Cisco Nexus 1110-X, run the copy command to copy it to the Cisco Nexus 1110-X disk. You must place the file either on an FTP server or on a UNIX or Linux machine (using the scp command) that is accessible from the Cisco Nexus 1110-X management interface. An example copy command from an FTP server is copy ftp:// <<var_ftp_server>>/nexus-1000v.4.2.1.SV2.1.1a.iso /repository/.

```
enable secondary
Enter vsb image: [nexus-1000v.4.2.1.SV2.1.1a.iso] Enter
Enter domain id[1-4095]: <<var_vsm_domain_id>>
Enter SVS Control mode (L2 / L3): [L3] Enter
Management IP version [V4/V6]: [V4] Enter
Enter Management IP address: <<var_vsm_ mgmt_ip>>
Enter Management subnet mask: <<var_vsm_ mgmt_mask>>
IPv4 address of the default gateway: <<var_vsm_mgmt_gateway>>
Enter HostName: <<var_vsm_hostname>>
```

- **3**. Enter the admin password <<var_password>>.
- 4. Type show virtual-service-blade summary. Continue periodically entering this command until both the primary and secondary VSM-1s have a state of VSB POWERED ON.

```
copy run start
```

5. Run system switchover on Cisco Nexus 1110-X B to activate Cisco Nexus 1110-X A. This causes Cisco Nexus 1110-X B to reboot.

Install Virtual Ethernet Module on Each ESXi Host

vCenter Server VM

To install the Virtual Ethernet Module (VEM) on the ESXi hosts, follow these steps:

- 1. Launch a Web browser to http://<<var_vsm_mgmt_ip>>.
- 2. Right-click the cross_cisco-vem-v152-4.2.1.2.1.1a.0-3.1.1.vib hyperlink and choose Save target as.
- **3.** Save the file as cross_cisco-vem-v152-4.2.1.2.1.1a.0-3.1.1.vib, type All Files, on the Desktop of the management workstation.
- 4. From the main window in the vSphere Client connected to vCenter, choose the first server in the list under the FlexPod Management cluster.
- 5. Click the Summary tab.
- 6. Under Storage on the right, right-click infra_datastore_1 and choose Browse Datastore.
- 7. Choose the root folder (/) and click the third button at the top to add a folder.
- 8. Name the folder VEM and click OK.
- 9. On the left, choose the VEM folder.
- **10.** Click the fourth button at the top and choose Upload File.
- **11.** Navigate to the cross_cisco-vem-v152-4.2.1.2.1.1a.0-3.1.1.vib file and click **Open**.
- 12. Click Yes. The VEM file should now appear in the VEM folder in the datastore.
- **13.** Open the VMware vSphere CLI command prompt.
- 14. For each ESXi host in the VMware vSphere CLI, run the following command:

esxcli -s <Host Server IP> -u root -p <Root Password> software vib install -v /vmfs/volumes/infra_datastore_1/VEM/cross_cisco-vem-v152-4.2.1.2.1.1a.0-3.1.1.vib


Register Cisco Nexus 1000V as a vCenter Plug-in

To register the Cisco Nexus 1000V as a vCenter plug-in, follow these steps:

- 1. Using a Web browser, navigate to the <<var_vsm_mgmt_ip>> using http://<<var_vsm_mgmt_ip>>.
- 2. Right-click the cisco_nexus_1000v_extension.xml hyperlink and choose Save target as.
- **3**. Save the XML file to the local desktop.
- 4. In the vSphere Client connected to vCenter, choose Plug-ins > Manage Plug-ins.
- 5. Right-click the white space in the window and choose New Plug-in.
- 6. Browse to the desktop and choose the cisco_nexus_1000v_extension.xml document that was previously saved. Click **Open**.
- 7. Click Register Plug-in.
- 8. Click Ignore.
- 9. Click OK.
- **10.** The Cisco_Nexus_1000V should now appear in the list of available plug-ins.
- 11. Click Close to close the Plug-in Manager.

Perform Base Configuration of the Primary VSM

To perform the base configuration of the primary VSM, follow these steps:

- 1. Using an SSH client, log in to the primary Cisco Nexus 1000V VSM as admin.
- **2**. Run the following configuration commands.

```
config t
svs connection vCenter
protocol vmware-vim
remote ip address <<var_vcenter_server_ip>> port 80
```

```
vmware dvs datacenter-name FlexPod_DC_1
connect
exit
ntp server <<var_global_ntp_server_ip>> use-vrf management
vlan <<var_ib-mgmt_vlan_id>>
name IB-MGMT-VLAN
vlan <<var_nfs_vlan_id>>
name NFS-VLAN
vlan <<var_vmotion_vlan_id>>
name vMotion-VLAN
vlan <<var_vm-traffic_vlan_id>>
name VM-Traffic-VLAN
vlan <<var_native_vlan_id>>
name Native-VLAN
exit
port-profile type ethernet system-uplink
vmware port-group
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_nfs_vlan_id>>,
<<var_vmotion_vlan_id>>, <<var_vm-traffic_vlan_id>>
channel-group auto mode on mac-pinning
no shutdown
system vlan <<var_mgmt_vlan_id>>, <<var_nfs_vlan_id>>, <<var_vmotion_vlan_id>>,
<<var_vm-traffic_vlan_id>>
system mtu 9000
state enabled
port-profile type vethernet IB-MGMT-VLAN
vmware port-group
switchport mode access
switchport access vlan <<var_ib-mgmt_vlan_id>>
no shutdown
system vlan <<var_ib-mgmt_vlan_id>>
state enabled
port-profile type vethernet NFS-VLAN
vmware port-group
switchport mode access
switchport access vlan <<var_nfs_vlan_id>>
no shutdown
system vlan <<var_nfs_vlan_id>>
state enabled
port-profile type vethernet vMotion-VLAN
vmware port-group
switchport mode access
switchport access vlan <<var_vmotion_vlan_id>>
no shutdown
system vlan <<var_vmotion_vlan_id>>
state enabled
port-profile type vethernet VM-Traffic-VLAN
vmware port-group
switchport mode access
switchport access vlan <<var_vm-traffic_vlan_id>>
no shutdown
system vlan <<var_vm-traffic_vlan_id>>
state enabled
port-profile type vethernet n1kv-L3
capability 13control
vmware port-group
switchport mode access
switchport access vlan <<var_ib-mgmt_vlan_id>>
no shutdown
system vlan <<var_ib-mgmt_vlan_id>>
state enabled
exit
```

copy run start

Migrate Networking Components for ESXi Hosts to Cisco Nexus 1000V

vSphere Client Connect to vCenter

I

To migrate the networking components for the ESXi hosts to the Cisco Nexus 1000V, follow these steps:

- 1. In the VMware vSphere Client connected to vCenter, choose Home > Networking.
- **2.** Expand the vCenter, DataCenter, and Cisco Nexus 1000V folders. choose the Cisco Nexus 1000V switch.
- 3. Under Basic Tasks for the vSphere distributed switch, choose Add a Host.
- 4. For both hosts, choose vmnic1 and choose the system-uplink Uplink port group. Click Next.

Figure 77 Adding Host to the vSphere Distributed Switch

🛃 Add Host to vSphere Distributed Swi	tch				
Select Hosts and Physical Adapters Select hosts and physical adapters t	o add to this vS	phere distributed switch.			
Select Host and Physical Adapters				Settings	View Incompatible Hosts
Network Connectivity	Host/Physical	adapters	In use by switch	Settings	Uplink port group
Virtual Machine Networking	- 🖌	cec220-1.ice.rtp.netap		View Details	
Ready to Complete	Select p	hysical adapters			
		vmnic0	vSwitch0	View Details	Select an uplink port gr
	🗹 💷	vmnic1		View Details	system-uplink
	- 🖌	ceucsbc-2-b1.ice.rtp.ne		View Details	
	Select p	hysical adapters			
		vmnic0	vSwitch0	View Details	Select an uplink port gr
	I 💀 💀	vmnic1		View Details	system-uplink 🛛 💌
Help				≤ Back N	ext ≥ Cancel

5. For all VMkernel ports, choose the appropriate Destination Port Group from the Cisco Nexus1000V, making sure to choose the "n1kv-L3" destination port group for the MGMT VMkernel ports. Click Next.

Figure 78 Assigning Port Groups

🛃 Add Host to vSphere Distributed Sw	itch			
Network Connectivity				
Select port group to provide networ	rk connectivity for the adapte	rs on the vSphere distribu	uted switch.	
Select Host and Physical Adapters	 Assign adapters to a de 	stination port group to m	igrate them. Ctrl+click to mult	i-select.
Network Connectivity	Host/Virtual adapter	Switch	Source port group	Destination port group
virtual Machine Networking Ready to Complete	🖃 📋 icef1-h11.ice.rtp.r	netapp		
Ready to Complete	vmk2	vSwitch0	VMkernel-vMotion	vMotion-VLAN
	wnk1	vSwitch0	VMkernel-NFS	NFS-VLAN
	🛄 vmk0	vSwitch0	VMkernel-MGMT	n1kv-L3
	🖃 📋 icef1-h6.ice.rtp.ne	etapp		
	wmk2	vSwitch0	VMkernel-vMotion	vMotion-VLAN
	vmk1	vSwitch0	VMkernel-NFS	NFS-VLAN
	vmk0	vSwitch0	VMkernel-MGMT	n1kv-L3 💌
	Virtual adapter details			Assign port group
	vmk0			<u> </u>
	vMotion:	Disabled		
	Fault tolerance logging:	Disabled		
	Management traffic:	Enabled		
	iSCSI part hindiga:	Disabled		
	iscsi port binding:			-
Help			<u> </u>	Next ≥ Cancel
				11

1

6. Choose the Migrate Virtual Machine Networking check box. Expand each VM and choose the port groups for migration individually. Click **Next**.

Figure 79 Choosing Port Groups for Each VMs

Add Host to vSphere Distributed Swit Virtual Machine Networking Select virtual machines or network	ch adapters to migrate to the vSphere	distributed switch.			
Select Host and Physical Adapters Network Connectivity	Migrate virtual machine netwo	orking ers to a destination port	t group to migrate the	m. Ctrl+click to mull	i-select.
Virtual Machine Networking	Host/Virtual machine/Network add	apter NIC count	Source port group	Destination port	group
Ready to Complete	E icef1-b5 ice rtp. petapp	com	1	1	5 P
	E S icef1-vc	1		Do not migrate	
	Network adapter	1	IB-MGMT Network	IB-MGMT-VLAN	
	E S icef1-vcsal	. 1	10 martinethorit	Do not migrate	
	Network adapter	1	IB-MGMT Network	IB-MGMT-VI AN	- I
	Network adapter details				Assign port group
	Network adapter 1				
	MAC address: 00	:0c:29:eb:65:d4			
	Adapter type: VN	XNET 3			
	Port group: IB	-MGMT Network			
Help	1		< Ba	ick Next >	Cancel

- 7. Click Finish. Wait for the migration process to complete.
- 8. In the vSphere Client window, choose Home > Hosts and Clusters.
- **9.** Choose the first ESXi host and click the **Configuration** tab. In the Hardware box, choose Networking.
- **10.** Make sure that vSphere Standard Switch is selected at the top next to View. vSwitch0 should not have any active VMkernel or VM Network ports on it. On the upper right of vSwitch0, click Remove.
- 11. Click Yes.
- **12.** After vSwitch0 has disappeared from the screen, click **vSphere Distributed Switch** at the top next to View.
- 13. Click Manage Physical Adapters.
- 14. Scroll down to the system-uplink box and click Add NIC.
- **15.** choose vmnic0 and click **OK**.

- 16. Click OK to close the Manage Physical Adapters window. Two system uplinks should now be present.
- 17. choose the second ESXi host and click the **Configuration** tab. In the Hardware field, click Networking.
- 18. Make sure vSphere Standard Switch is selected at the top next to View. vSwitch0 should have no active VMkernel or VM Network ports on it. On the upper right of vSwitch0, click Remove.
- 19. Click Yes.
- 20. After vSwitch0 has disappeared from the screen, click vSphere Distributed Switch at the top next to View.
- 21. Click Manage Physical Adapters.
- **22**. Scroll down to the system-uplink box and click **Add NIC**.
- **23.** choose vmnic0 and click **OK**.
- 24. Click OK to close the Manage Physical Adapters window. Two system-uplinks should now be present.
- 25. From the SSH client that is connected to the Cisco Nexus 1000V, run show interface status to verify that all interfaces and port channels have been correctly configured.

2400450475	00 D TTU						
Se 192.168.175.1	193 - Putty						
2012 Jun 1	22:14:45 icefxp1-vs	m %VEM_MGR	-2-MOD_ONL	INE: Modu	le 3 is	online	
icefxpl-vsm#	show interface sta	itus					
Port	Name	Status	Vlan	Duplex	Speed	Tvpe	
mgmtO		up	routed	full	1000		
Eth3/1		up	trunk	full	10G		
Eth3/2		up	trunk	full	10G		
Eth4/1		up	trunk	full	10G		
Eth4/2		up	trunk	full	10G		
Po1		up	trunk	full	10G		
Po2		up	trunk	full	10G		
Veth1	VMware VMkernel,	v up	3175	auto	auto		
Veth2	VMware VMkernel,	v up	3170	auto	auto		
Veth3	VMware VMkernel,	v up	3173	auto	auto		
Veth4	VMware VMkernel,	v up	3175	auto	auto		
Veth5	VMware VMkernel,	v up	3170	auto	auto		
Veth6	VMware VMkernel,	v up	3173	auto	auto		
Veth7	icefxp1-vc, Netw	or up	3175	auto	auto		
Veth8	icefxp1-vcsql, N	let up	3175	auto	auto		
contro10		up	routed	full	1000		
icefxp1-vsm#	E 📕						

Figure 80 Verifying Interfaces and Port Channels

26. Run show module and verify that the two ESXi hosts are present as modules.

🔗 ice	f1-vsm								×
icef:	1-vsm(co	onfig)# s	show :	module					
Mod	Ports	Module-7	Гуре			Model		Status	
1	0	Virtual	Supe	rvisor Modul	.e	Nexus1000V		ha-standby	
2	0	Virtual	Supe	rvisor Modul	.e	Nexus1000V		active *	
3	248	Virtual	Ethe	rnet Module		NA		ok	
4	248	Virtual	Ethe	rnet Module		NA		ok	
Mod	នឃ			Hw					
1	4.2(1)	5V2(1.1a)		0.0					
2	4.2(1)\$	5V2(1.1a)		0.0					
3	4.2(1):	5V2(1.1a)		VMware ESXi	5.1.0 Re	leasebuild-83846	3 (3	.1)	
4	4.2(1)\$	3V2(1.1a)		VMware ESXi	5.1.0 Re	leasebuild-83846	3 (3	.1)	
Mod	MAC-Ado	iress (es)				Serial-Num			
1	00-19-0)7-6c-5a-	-a8 t	0 00-19-07-6	c-62-a8	NA			
2	00-19-0	07-6c-5a-	-a8 t	0 00-19-07-6	c-62-a8	NA			
3	02-00-0)c-00-03-	-00 t	o 02-00-0c-0	0-03-80	NA			
4	02-00-0)c-00-04-	-00 t	o 02-00-0c-0	0-04-80	NA			
									=
Mod	Server-	-IP	Se	rver-UUID		S	erve	r-Name	
Moi	ce								-

Figure 81 Verifying the ESXi Hosts are Shown as Modules

- 27. Run copy run start.
- 28. Type exit two times to log out of the Cisco Nexus 1000v.

FlexPod Management Tool Setup

NetApp Virtual Storage Console (VSC) 4.1 Deployment Procedure

VSC 4.1 Preinstallation Considerations

I

The following licenses are required for VSC on storage systems running Data ONTAP 8.1.2 7-mode:

- Protocol licenses (NFS and FCP)
- FlexClone (for provisioning and cloning only)
- SnapRestore (for backup and recovery)
- SnapManager suite

Install VSC 4.1

To install the VSC 4.1 software, follow these steps:

- Using the instructions in section "Build Microsoft SQL Server VM," build a VSC and an OnCommand virtual machine with 4GB RAM, two CPUs, and one virtual network interface in the <<var_ib-mgmt_vlan_id>> VLAN. The virtual network interface should be a VMXNET 3 adapter. Bring up the VM, install VMware Tools, assign IP addresses, and join the machine to the Active Directory domain. Install the current version of Adobe Flash Player on the VM. Install all Windows updates on the VM.
- 2. Log in to the VSC and OnCommand VM as the FlexPod admin user.
- Download the x64 version of the Virtual Storage Console 4.1 at: http://support.netapp.com/NOW/cgi-bin/software/?product=Virtual+Storage+Console&platform= VMware+vSphere from the NetApp Support site.
- 4. Right-click the file downloaded in step 3 and choose Run As Administrator.
- 5. Click Yes at the User Access Control warning.
- 6. On the Installation wizard Welcome page, click Next.
- 7. choose the backup and recovery capability. Click Next.

Note The backup and recovery capability requires an additional license.

Figure 82 Selecting the Desired Capabilities of VSC 4.1

capability requires the
+

8. Click Next to accept the default installation location.

	Figure 83	Installation Loca	ation		
😽 NetApp®	Virtual Storage Console	4.1 for VMware vSph	ere - InstallShi	eld Wizard	×
Destination	Folder				
Click Nex	t to install to this folder, or d	ick Change to install to a	a different folder.		
	Install NetApp® Virtual Stor	age Console 4.1 for VM	ware vSphere to:		
	C:\Program Files\WetApp\Vir	tual Storage Console\		Change	
InstallShield -					
		< Back	Next >	Cancel	1
					-

9. Click Install.

Γ

10. Click Finish.

Figure 84 Ready to Install VSC 4.1
🐙 NetApp® Virtual Storage Console 4.1 for VMware vSphere - InstallShield Wizard 🛛 🎽
Ready to Install the Program The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Virtual Storage Console for VMware vSphere must be registered with vCenter for the plugin to function. You may register once installation/upgrade completes or you can register at any time by visiting the following URL:
https://localhost:8143/Register.html
InstallShield < Back Install Cancel

Register VSC with vCenter Server

To register the VSC with the vCenter Server, follow these steps:

- **1.** A browser window with the registration URL opens automatically when the installation phase is complete.
- 2. Click **Continue** to this website (not recommended).
- **3.** In the Plug-in Service Information section, choose the local IP address that the vCenter Server uses to access the VSC server from the drop-down list.
- 4. In the vCenter Server Information section, enter the host name or IP address, user name (FlexPod admin user), and user password for the vCenter Server. Click **Register** to complete the registration.

I

	iyure oʻ	Registering VSC with vCenter Server
vSphere Plugin Regi	istration - \	Windows Internet Explorer
🔊 🗢 🧭 https:/	//localhost:8	143/R 🔎 💌 🚱 🔄 🎽 🎽 🧭 vSphere Plugin Registration 🛛 🗙 🔛
vSphere Plugin Registrat	tion	
To register the Virtual St olugin and provide the v and password. — Plugin service informa	torage Conso Center Serve	ole, select the IP Address you would like to use for the er's IP address and port along with a valid user name
Host name or IP Addres	ss: 19	2.168.175.191
Host name or IP Addres vCenter Server inform Host name or IP Addres	nation	92.168.175.191 92.168.175.188
Host name or IP Addres vCenter Server inform Host name or IP Addres Port:	ss: 19 nation ss: 19 44	92.168.175.191 92.168.175.188 #3
Host name or IP Addres vCenter Server inform Host name or IP Addres Port: User name:	ss: 19 nation ss: 19 44 ice	22. 168. 175. 191 ■ 22. 168. 175. 188 43 =Vjcef1-admin

Discover and Add Storage Resources

ſ

To discover storage resources for the Monitoring and Host Configuration and the Provisioning and Cloning capabilities, follow these steps:

- 1. Using the vSphere Client, log in to the vCenter Server as FlexPod admin user. If the vSphere Client was previously opened, close it and then reopen it.
- 2. Click the Home tab in the left side of the vSphere Client window.
- 3. Under Solutions and Applications, click NetApp.

🛃 srvc-apps-2.5rv	vcEng.rtp.netapp.c	om - vSphere Clie	ent		
<u>F</u> ile <u>E</u> dit Vie <u>w</u> I	nventory <u>A</u> dministra	tion <u>P</u> lug-ins <u>H</u> elj	Þ		
🖸 🗈 🛕	Home				Search Invento 🝳
	Ú2			-	
Storage Providers	vCenter Service Status				
Management					
2		6	•		-
Scheduled Tasks	Events	Maps	Host Profiles	VM Storage Profiles	Customization Specifications Manager
Solutions and Ap	oplications				
•					
NetApp					-
Recent Tasks		Name,	Target or Status conta	ins: •	Clear ×

Figure 86 Adding Storage Resource

4. Click Yes when the security certificate warning appears. To view the certificate, click View Certificate.

1

Security Alert	X	Certificate	×
The identity of this web site or the cannot be verified.	integrity of this connection	General Details Certification Pa	eth
▲ The security certificate was not chosen to trust. View th you want to trust the certifyi ✓ The security certificate date ✓ The security certificate has of the page you are trying to Do you want to proceed? Yes	issued by a company you have e certificate to determine whether ng authority. : is valid. a valid name matching the name o view. 	Field Version Serial number Signature algorithm Valid from Valid to Subject Learn more about certificate deta	Value V1 01 38 05 56 15 f4 sha1R5A sha1 10.61.171.153 Tuesday, June 19, 2012 11:2 Friday, June 17, 2022 11:22:0 10.61.171.153 V
			OK

Figure 87 Certificate Details

- 5. In the navigation pane, choose Monitoring and Host Configuration if it is not selected by default
- 6. In the list of storage controllers, right-click the first controller listed and choose Modify Credentials.
- 7. Enter the storage cluster management IP address in the Management IP address field. Enter admin for the User name, and the admin password for the Password. Make sure that Use SSL is selected. Click **OK**.
- 8. Click **OK** to accept the controller privileges.

I

🕑 ICEF1-VC.ice.rtp.netapp.c	om - vSphere Client						[
<u>Eile Edit View</u> Inventory §	Administration Plug-ins Help						
🖸 🗈 🔥 Home 🕨	Solutions and Applications	🖪 NetApp 🕨 🕻	ICEF1-VC.ic	e.rtp.netapp.o	com	Search Inv	ventory
Monitoring and Host Configuration	Storage Controllers					Add Delete	Edit Update
 Overview 	Controller [^]	IP Address	Version	Status	Free Capacity V	AAI Capable Sup	ported Protocols
Storage Details - SAN	🖃 🎟 HA Pair:icef1-st1a/icef	1-st1b					
Storage Details - NAS	ing Controller: icef1-st1a	192.168.171.1	44 8.1.2 7	Normal	7.27TB (95%) E	nabled NFS	FC/FCoE
Data Collection	I Controller: icef1-st1b	192.168.171.1	45 8.1.2 7	Normal	7.23TB (95%) E	nabled NFS	FC/FCoE
Tools							
Discovery Status							
Provisioning and Cloning							
Optimization and	ESX Hosts						
Migration	Hostname	IP Address	Version	Status	Adapter Setting	gs MPIO Settings	NFS Settings
Backup and Recovery	icef1-h11.ice.rtp.netapp.com	192.168.175.100	5.1.0	Alert	Normal	Normal	Alert
	icef1-h6.ice.rtp.netapp.com	192.168.175.63	5.1.0	Alert	Normal	Normal	Alert
About							
Recent Tasks				Name, Ta	rget or Status contai	ns: 🕶	Clear
Name	Target Status	Details		Initiate	d by VCenter S	5erver Req	uested Start Ti 🤜
NetApp Storage Discov	FlexPod_DC_1 📀 Comple	eted [icef1-st1	b] Discovery co	m ICE\icel	f1-ad 🛃 ICE	F1-VC.ice.r 2/28	/2013 9:07:29 AM
NetApp Storage Discov	FlexPod_DC_1 📀 Comple	eted [icef1-st1	a] Discovery co	m ICE\icel	f1-ad 🛃 ICE	F1-VC.ice.r 2/28	/2013 9:04:58 AM
•							
🚰 Tasks 🞯 Alarms 📃					License Period:	189 days remaining	ICE\icef1-admin

Figure 88 vSphere Client Showing Storage Controllers

1

Optimal Storage Settings for ESXi Hosts

VSC allows for the automated configuration of storage-related settings for all ESXi hosts that are connected to NetApp storage controllers. To use these settings, follow these steps:

- 1. Choose individual or multiple ESXi hosts.
- 2. Right-click and choose Set Recommended Values for these hosts.

🛃 ICEF1-VC.ice.rtp.netapp.c	om - vSphere Client							_
<u>File E</u> dit Vie <u>w</u> Inventory &	Administration Plug-ins Help	,						
🖸 🔝 🛕 Home 🕨	Solutions and Application	ns 🕨 🔽	NetApp 🕨 🕻	DICEF1-VC.ic	e.rtp.netapp.	com	Search In	iventory
Monitoring and Host Configuration	Storage Controllers						Add Delete	Edit Update
▶ Overview	Controller [^]		IP Address	Version	Status	Free Capacity	VAAI Capable Su	oported Protocols
Storage Details - SAN	🗆 🚟 HA Pair:icef1-st	la/icef1-s	t1b	,		,		
Storage Details - NAS	Controller: icef1-st1a		192.168.171.1	44 8.1.2 7	Normal	7.27TB (95%)	Enabled NFS	S, FC/FCoE
Data Collection	E Controller: icef1-st1b		192.168.171.1	45 8.1.2 7	Normal	7.23TB (95%)	Enabled NFS	S, FC/FCoE
Tools								
Discovery Status								
Provisioning and Cloning Optimization and	ESX Hosts							
Migration	Hostname ¹	IP/	Address	Version	Status	Adapter Settin	ngs MPIO Settings	NFS Settings
Backup and Recovery	icef1-h11.ice.rtp.neta	pp.com 19	2 168 175 100	510	Alert	Normal	Normal	Alert
	icef1-h6.ice.rtp.netap	p.con	Set Recommen	ded Values	Alert	Normal	Normal	Alert
About			Show Details Skip Host					
Recent Tasks					Name, Ta	rget or Status conta	ains: 🕶	Clear
Name	Target Sta	tus	Details		Initiate	d by VCenter	Server Re	quested Start Ti 🤜
NetApp Storage Discov	FlexPod_DC_1	Completed	[icef1-st1	b] Discovery co	m ICE\ice	f1-ad 🛃 🖸	EF1-VC.ice.r 2/2	8/2013 9:07:29 AM
NetApp Storage Discov	FlexPod_DC_1	Completed	j Licer1-st1	aj Discovery co	m ICE\ice	ri-ad 🔂 IC	EF1-VC.ice.r 2/2	8/2013 9:04:58 AM
								
🚰 Tasks 🞯 Alarms						License Period	: 189 days remaining	g ICE\icef1-admin

Figure 89 Setting Recommended Values for the Hosts

3. Check the settings to apply to selected vSphere hosts. Click **OK** to apply the settings.

ſ

This functionality sets values for HBAs and CNAs, sets appropriate paths and path-selection plug-ins, and verifies appropriate settings for software-based I/O (NFS and iSCSI).

 Figure 90
 Recommended Settings for NetApp Storage System

 NetApp Recommended Settings
 Image: Configures and the settings for NetApp storage systems.

 Image: MPIO Settings
 Image: Configures preferred paths for NetApp storage systems. Determines which of the available paths are Primary paths (as opposed to Proxy paths which transverse the interconnect cable), and sets the preferred path to one of those paths.

 Image: NFS Settings
 Sets the recommended NFS Heartbeat settings for NetApp storage systems.

Note

Depending on what changes have been made, the servers might require a restart for network-related parameter changes to take effect. If no reboot is required, the Status value is set to Normal. If a reboot is required, the Status value is set to Pending Reboot. If a reboot is required, the ESX or ESXi servers should be placed into Maintenance Mode, evacuate (if necessary), and be restarted before proceeding.

VSC 4.1 Provisioning and Cloning Setup

Provisioning and cloning in VSC 4.1 helps administrators to provision both VMFS and NFS datastores at the data center, datastore cluster, or host level in VMware environments.

- 1. In a vSphere Client connected to vCenter, choose Home > Solutions and Applications > NetApp and click the Provisioning and Cloning tab on the left. Choose Storage controllers.
- 2. In the main part of the window, right-click <<var_controller1>> and choose Resources.
- **3.** In the <<var_controller1>> resources window, use the arrows to move volumes ifgrp0-<<var_nfs_vlan_id>>, esxi_boot and aggr1 to the right. Also choose the Prevent further changes check box as shown in Figure 91.

ef1-st1a resour	ces		×
Configure the inte on the left contain the interfaces, vo	rfaces, volume, and aggregates y a all of the available interfaces, vo lumes, and aggregates that can b	ou would like to use for provisioning and cloning below. umes, and aggregates respectively. The list on the righ e used for provisioning or cloning.	The lists t contains
Interfaces:		 ifgrp0-3170 - 192.168.170.14 ● ● ● 	4
Volumes:	infra_swap vol0	<pre> esxi_boot esxi_boot esxi_boot esxi_boot </pre>	
Aggregates:	aggrO	<pre>aggr1 </pre>	
7 Prevent furth	er changes		
		Save	Cancel

Figure 91 List of Parameters of Storage Controller 1 Ready for Provisioning and Cloning

4. Click Save.

Γ

- 5. In the main part of the window, right-click <<var_controller2>> and choose Resources.
- 6. In the <<var_controller2>> resources window, use the arrows to move volumes ifgrp0-<<var_nfs_vlan_id>>, infra_datastore_1 and aggr1 to the right. choose the Prevent Further changes check box as shown in Figure 92.

	Figure 92	List of Parame	eters	of Storage Controller 2 Ready for	Provi
icef1-st1b resources	i				×
Configure the interfac on the left contain all the interfaces, volume	es, volume, and aggr of the available interf s, and aggregates th	egates you would like t aces, volumes, and ag at can be used for pro	to use gregal visioni	for provisioning and cloning below. The lists tes respectively. The list on the right contain ing or cloning.	в
Interfaces:			* + *	ifgrp0-3170 - 192.168.170.145	
Volumes:	vol0			infra_datastore_1	
Aggregates:	aggrO		\$ + *	aggr1	
Prevent further c	hanges		1	ſ	
				Save Cancel	

.

~

...

. .

7. Click Save.

~~

VSC 4.1 Backup and Recovery

Adding Storage Systems to the Backup and Recovery Capability

Before you begin using the Backup and Recovery capability to schedule backups and restore your datastores, virtual machines, or virtual disk files, you must add the storage systems that contain the datastores and virtual machines for which you are creating backups.

۵, Note

The Backup and Recovery capability does not use the user credentials from the Monitoring and Host Configuration capability.

Follow these steps to add the storage systems to the Backup and Recovery capability:

o 10.61.188.98 - Remote I	Desktop Connection		Contraction of the second	Standards 1774	All Sharings and Success	Provinsi State of the second state of the
srvc-apps-2.SrvcEng.rtp	.netapp.com - vSphere Client					
File Edit View Inventory	Administration Plug-ins Help					
🖸 🔝 🏠 Home	Solutions and Applications Solutions	NetApp 🕨 🛃 srvc-a	pps-2.SrvcEng.rtp.netap	op.com		
Monitoring and Host Configuration	General Single File Restore					
Provisioning and Cloning	Setup - General					
	vCenter Server					
Dptimization and Migration	Server:	10.61.188.98				
Packup and Decoupry	Port number:	443				
backup allu kecuvery	User.	administrator				
Getting Started	Storage Systems					
Backup	Name					Address
Restore	10.61.180.86					10.61.180.86
k Setup	10.61.180.57					10.61.180.57
Single Cile Destante	10.61.180.50		🛃 Add Storage S	ystem	×	10.61.180.50
Single hie Restore			Storage system:		_	
			Liser:			
			Descuende			
			Password:			
				[1	
				Add	Cancel	

Figure 93 Adding Storage System to Backup and Recovery Capability

- 1. Click **Backup and Recovery** and then click **Setup**.
- 2. Click Add. The Add Storage System dialog box appears.
- 3. Type the DNS name or IP address and the user credentials of the storage cluster.
- 4. Click Add to add the storage cluster.

Backup and Recovery Configuration

I

To configure a backup job for a datastore, follow these steps:

- 1. Click Backup and Recovery, then choose Backup.
- 2. Click Add. The Backup wizard appears.

	Figure 94	Configuring Backup	
🛃 Backup Wizard			2
Job Specify a na	ame for the backu	up job that you want to create.	
Job Name			
Virtual Entities	Name:	VSC_backup	
Spanned Entities	Description:	VM backup	
Scripts	Options -		
Schedule		Initiate SnapMirror update	
User Credentials		✓ Perform VMware consistency snapshot	
Backup Recention		Include datastores with independent disks	
Ready to Complete			
		<back next=""> Cance</back>	1

I

- **3**. Type a backup job name and description.
- **4.** If you want to create a VMware snapshot for each backup, choose Perform VMware consistency snapshot in the options pane.
- 5. Click Next.
- 6. choose infra_datastore_1 and then click is to move it to the selected entities. Click Next.

🛃 Backup Wizard		
Entities Specify the v	irtual entities you need to backup.	
Job Name Virtual Entities Spanned Entities Scripts Schedule User Credentials Backup Retention Ready to Complete	Entities: FlexPod_DC_1 Available Entities: datastore1 datastore1(1) infra_swap	Selected Entities:

Figure 95 Selecting Entities to Backup

7. choose one or more backup scripts if available and click Next.

Γ

8. choose the hourly, daily, weekly, or monthly schedule that you want for this backup job and click Next.

	Figure 96	Setting Schedule for Backup
🛃 Backup Wizard		×
Schedule You can spec	ify an hourly, daily, v	weekly, monthly or no schedule at all for the backup job.
Job Name Virtual Entities Spanned Entities Scripts Schedule User Credentials Backup Retention Ready to Complete	Perform this back Hourly Daily Weekly Monthly One time only Hourly schedule Backups will be performed	ckup © © © © v v v v v v e details erformed
	Every: At: Starting:	1 hour 11: 49 AM 07/08/2012
	5	<pre></pre>

9. Use the default vCenter credentials or type the user name and password for the vCenter Server and click **Next**.

1

10. Specify backup retention details as per requirements. Enter an e-mail address for receiving e-mail alerts. You can add multiple e-mail addresses by using semicolons to separate e-mail addresses. Click **Next**.

ah Nama		
intual Entities	Retention	
panned Entities	• A maximum of days:	
cripts	C A maximum of backups:	
ichedule	C Never expires	
Iser Credentials		
ackup Retention	Email alerts	
teady to Complete	Source email address:	test1@example.com
	Destination email address (s):	test2@example.com
	SMTP host:	smtp.example.com
	Notify on:	Aheravs
	Send test email	

Figure 97 Specifying Backup Retention Period

I

Γ

11. Review the summary page and click **Finish**. If you want to run the job immediately, choose the Run Job Now option and then click **Finish**.

Summary Review this summary b	efore completing this wizard.	ng options:	
icual criticies ipanned Entities ichedule Iser Credentials iackup Retention teady to Complete Performation Backup Email Email	e: ription: orm VMware consistency snapshot: al entities to be backed up: orm this backup: up retention: notification will be sent on: notification will be sent from: notification will be sent to:	vsc_backup1 VM backup Yes ab_esx_test vSphere51_1 Every 1 hour at 11:49 starting 7/8/2012 Maximum of 1 day Always test1@example.com test2@example.com	•

12. On the management interface of storage controller 2, automatic Snapshot copies of the infrastructure datastore volume can be disabled by typing the command:

```
snap sched infra_datastore_1 0 0 0
```

13. Also, to delete any existing automatic Snapshot copies that have been created on the volume type the following command:

```
snap list infra_datastore_1
snap delete infra_datastore_1 <snapshot name>
```

OnCommand Unified Manager 5.1

Create Raw Device Mapping (RDM) Datastore

From the VMware vCenter Client, do as follows:

 In the VMware vCenter Client, from Home > Inventory > Hosts and Clusters, right-click the FlexPod_Management cluster.

- 2. choose NetApp > Provisioning and Cloning > Provision Datastore.
- 3. Make sure the Infra_Vserver is selected in Vserver drop-down menu and click Next.
- 4. choose VMFS as the Datastore type and click Next.

- 5. choose FCP as the Protocol type, set the Size to 100, enter the datastore name as RDM_Map, check the check box to create new volume container, choose aggr02 as the Aggregate, check the Thin Provision check box, and click Next.
- 6. Verify settings and click Apply.

Install .NET Framework 3.5.1 Feature

From the Virtual Storage Console (VSC) and OnCommand VM:

- 1. Log in to the VSC and OnCommand VM as the FlexPod admin and open Server Manager.
- 2. Click Features and click Add Features.
- 3. Expand .NET Framework 3.5.1 Features and choose only .NET Framework 3.5.1.

Figure 99 Selecting Features to be Installed on the Server

Add Features Wizard		×
Select Features		
Features Confirmation Progress Results	Select one or more features to install on this server. Eeatures:	Description: <u>Microsoft .NET Framework 3.5.1</u> combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
	<u>More about reatures</u>	> Install Cancel

- 4. Click Next.
- 5. Click Install.
- 6. Click Close.

ſ

7. Close Server Manager.

Install SnapDrive 6.4.2

Follow these steps to install SnapDrive® 6.4.2:

- 1. Download SnapDrive 6.4.2 from the NetApp Support Site.
- **2.** Browse to the location of the SnapDrive installation package and double-click the executable file. This launches the SnapDrive installation wizard and opens the Welcome page.
- 3. Click Next in the Welcome page of the SnapDrive installation wizard.
- 4. If this is a new SnapDrive installation, read and accept the license agreement. Click Next.
- 5. If this is a SnapDrive upgrade, choose Modify/Upgrade in the Program Maintenance page. Click Next.
- 6. choose "Per Storage System" as the license type. Click Next.



• In the case of upgrading SnapDrive, the license information will already be populated.

- In the case of selecting storage system licensing, SnapDrive can be installed without entering a license key. SnapDrive operations can be executed only on storage systems that have a SnapDrive or SnapManager license installed.
- In the case of clustered Data ONTAP 8.1-based systems, the storage system licensing for SnapDrive is bundled with the other SnapManager product licenses. They are now a single license called the SnapManager_suite license.
- 7. In the Customer Information page, type the user name and organization name. Click Next.
- 8. The Destination Folder page prompts for a directory in which to install SnapDrive on the host. For new installations, by default this directory is C:\Program Files\NetApp\SnapDrive\.To accept the default, click Next.
- **9.** Check the Enable VirtualCenter or ESX Server Settings check box. Enter the IP address, user name, and password for the vCenter Server and click **Next**.



Selecting Enable VirtualCenter or ESX Server Settings enables SnapDrive to use RDM pass-through LUNs. choose this option to use RDM pass-through disks. By default, this option is not selected.

Figure 100 Specifying Account Information for Installing SnapDrive 6.4.2

🙀 SnapDrive® - Installation Wizard			
VirtualCenter or ESX Server Web Set Specify account information for the install	r vice Credentia ed services.	ls	NetApp
Finable VirtualCenter or ESX Server Se	ettings		
Enables LUN provisioning and Sna ESX Server Guest OS using FC HB VirtualCenter or ESX Server user specified account is a member of IP address / Name:	apshot copy ma As or ESX iSCSI account userna f the VirtualCen	nagement supp (RDM) initiators ame and passwo ter or ESX Serve	ort with VMware . Specify rd. Ensure that the r local root group.
192.168.175.188			
User name:			
ice\icef1-admin			
Password:			
•••••			
Confirm Password:			
InstallShield	< Back	Next >	Cancel

10. Check the Enable SnapManager for Virtual Infrastructure Configuration Details check box. Enter the IP address of the VSC and OnCommand Server, and accept the default port. Click **Next**.

Figure 101	Specifying	Virtual Infrastructure	Details
------------	------------	------------------------	---------

🕞 SnapDrive® - Installation Wizard	
SnapManager for Virtual Infrastructure Details	NetApp
🔽 Enable SnapManager for Virtual Infrastructure Configuration Details	
Enable Snapshot management of VMDK disks on NFS and VM ensure SnapManager for Virtual Infrastructure server is pro mentioned IP Address/Name and Port.	FS datastores. Please perly configured at
IP address / Name:	
192.168.175.191	
Port(Default: 8043)	
8043	
InstallShield	
< Back Njixt >	Cancel

ſ

11. Enter your credentials or follow these steps to select a user account:

- **a.** In the Enter object name to select box, enter the local machine administrator in Domain name/user name format. Click **Add**.
- b. Click Check Names.
- c. Click OK.
- d. Enter the Administrator password.
- e. Click Next.
- f. Click OK.

Figure 102 Specifying SnapDrive Service Credentials

🙀 SnapDrive® - Installation Wizard			
SnapDrive Service Credentials Specify account information for the insta	lled services.		NetApp
Ensure that the specified accourd group of this system. See the Suffer for more details about service a Account information as "Domain"	nt is a member napDrive Insta account require n Name\User N	of the local adm lation and Admin ments. Please p ame" format.	inistrators nistration Guide rovide the
Note: NetApp VSS hardware provider	registration also	requires user accou	unt information.
Account:			
ICEF 1-VSC-OC \Administrator			Add
Password:			N
•••••			6
Confirm Password:			
•••••			
InstallShield			
	< Back	Next >	Cancel

<u>Note</u>

The specified account must be a member of the local administrators' group of this system.

12. In the SnapDrive Web Service Configuration page, keep the default ports unless any of them are already being used exclusively by another service. Click **Next**.

BrapDrive® - Installation Wizard SnapDrive Web Service Configuration Specify SnapDrive Web Service Configuration	×
SnapDrive Web Service Tcp/Ip Endpoint (Port) SnapDrive Web Service HTTP Endpoint (Port) SnapDrive Web Service HTTPS Endpoint (Port)	808 4094 4095
InstallShield < Ba	ck Next > Cancel

Figure 103

ſ

- **13**. In the Transport Protocol Default Setting screen:
 - a. choose Enable Transport Protocol Settings.

SnapDrive Web Service Configuration

- **b.** choose HTTPS as the transport protocol.
- c. Enter the user name (vsadmin) and password for the Infra_Vserver vserver.
- d. Verify that port ID is set to 443 and click Next.

				2
ransport Protocol	Default Setting			
Specify Default Tran	sport Setting for Storag	e System(s)		NetApp
🔽 Enable Transpor	t Protocol Settings			
	C <u>R</u> PC			
	○ <u>н</u> ттр			
	HTTP <u>S</u>			
Specify the user nar User Name:	ne and password for the	• HTTP/HTTP	S Protocol selection.	
proot Password:				
••••••				
Port ID: 443				

14. Click Next > Next > Install > Finish.

- **15.** From the Start menu, open SnapDrive.
- 16. In the left pane, expand the local machine and choose Disks.
- **17.** In the right pane, choose Create Disk.
- 18. In the create disk Wizard Window, click Next.
- 19. In the storage system name field, enter the Infra_Vserver management IP address, and click Add.

1

- 20. In the list that appears, choose OnCommandDB.
- 21. Enter OnCommandDB for the LUN Name and click Next.

Create Disk Wizard	X
Provide a Storage System Name, LUN P Enter the Storage System Name and	Path and Name LUN path information below.
Select an existing Storage System, or	enter a new Storage System name and press "Add".
Storage System Name: 192.168.171	.145 💌 Add
Name 🛆	Туре
> 🖃 📖 192.168.171.145	storage system
🖶 🕀 📋 infra_datastore_1	volume
🖶 🗄 OnCommandDB	volume
💼 🗄 🗍 RDM_Map	volume
LUN <u>P</u> ath: //oi/	
LUN N <u>a</u> me:	
LUN <u>D</u> escription:	
	< Back Next > Cancel

Figure 105 Adding LUN Information

- 22. Make sure the LUN type is set to Dedicated and click Next.
- 23. Assign drive letter O and set LUN size to 100GB. Click Next.

Figure 106 Entering LUN Properties

Drive Parameters	
Assign a Drive Let Use a Volume Mou Do not assign a Drive	ter: O int Point: rive letter or Volume Mount Point
Snapshot Copies	
Do you want to limit th	ne maximum disk size to accommodate at least one snapshot on the volume?
🙆 Limit 🛛 🙆 Do n	ot limit
limit 😡 Do n	ot limit
limit OD n LUN Size Maximum:	ot limit 16349.9 GB
imit iDon LUN Size Maximum: Minimum:	ot limit 16349.9 GB 64 MB

ſ

24. Choose all initiators on the Initiator List, and click Next.

25. Choose manual as the Initiator group management, and click Next.

1

26. Choose the MGMT-Hosts igroup, and click Next.

Figure 107	Specifying igroups for the LUN
------------	--------------------------------

Create Disk Wizard	
Select Initiator Groups Select igroups to be used by this LUN.	P.
Specify the igroups to be used for mapping this LUN.	
➤ ● MGMT-Hosts	
Click Manage Igroup to start the manage igroup wizard. The Manage Igroup wizard allo add, delete and rename igroups. Manage Igroup	ows you to
< <u>B</u> ack <u>N</u> ext > Car	ncel

27. Choose the RDM_Map Datastore in the Select Datastore section. Click Next.

Figure 108 Selecting a Datastore to Store LUN Mapping

Specify datasto	re to store RDM	LUN mapping	files.		
elect the data	store on which t	to store the RI	OM LUN mapping	. You will use	disk map to
nis datastore to	o access the LUI	ν.			
Store with V	'irtual Machine				
	ill store the DDM	LLUM manning	files with the da	tastore when	e virtual machir
SnapDrive w	ni store the KDP	r con mapping	THEF WHAT SHE ME	Contractor to the terminal	
SnapDrive w is stored.	III SLUTE LITE KUP	r con mapping	THE WAT STE GE		
SnapDrive w is stored. Specify datas	store	r con mapping			
SnapDrive w is stored. Specify datas SnapDrive w	store ill store the RDM	I LUN mapping	files on the sele	cted datastor	e.
SnapDrive w is stored. Specify datas SnapDrive w	store the RDM	I LUN mapping	files on the sele	cted datastor File system	e.
SnapDrive w is stored. Specify datas SnapDrive w Name datastore 1	store ill store the RDM Total capa 5 GB	I LUN mapping Free space 4 GB	files on the sele	cted datastor File system VMFS	e. Shared No
SnapDrive w is stored. Specify datas SnapDrive w Name datastore1 RDM_Map	store fill store the RDM Total capa 5 GB 100 GB	I LUN mapping Free space 4 GB 99 GB	files on the sele URL ds:///vmfs/v ds:///vmfs/v	cted datastor File system VMFS VMFS	e. Shared No Yes
SnapDrive w is stored. Specify datas SnapDrive w Name datastore 1 RDM_Map	store ill store the RDM Total capa 5 GB 100 GB	I LUN mapping Free space 4 GB 99 GB	files on the sele URL ds:///vmfs/v	Cted datastor File system VMFS VMFS	e. Shared No Yes
SnapDrive w is stored. Specify datas SnapDrive w Name datastore 1 RDM_Map	store ill store the RDM Total capa 5 GB 100 GB	I LUN mapping Free space 4 GB 99 GB	files on the sele URL ds:///vmfs/v Gs:///vmfs/v	cted datastor File system VMFS VMFS	e. Shared No Yes

- **28**. Click **Finish** to create the disk.
- 29. Close SnapDrive.

Install NetApp OnCommand Core Package

To install the OnCommand Unified Manager Core Package, follow these steps:

- 1. To download the OnCommand Unified Manager Core Package for Windows, click here.
- 2. Using the FlexPod admin credentials, log in to the VSC and OnCommand VM.
- **3.** Identify the DataFabric® Manager Server license key before starting the installation. The DataFabric Manager Server license key
- 4. Navigate to the path or directory containing the downloaded file and launch the file.
- 5. In the Security Warning message, click Yes to start the installation.
- 6. In the Welcome screen, click Next.
- 7. Accept the AutoSupport notice and click Next.
- 8. Identify whether the OnCommand Unified Manager instance should manage systems with clustered Data ONTAP or 7-Mode and click Next.



- For a 7-Mode environment, either the Express edition or the Standard edition of the software is available.
- If the infrastructure has both 7-Mode and clustered Data ONTAP systems, two OnCommand instances are needed to manage the respective 7-Mode or clustered Data ONTAP systems.
- 9. choose Standard edition and click Next.

- 10. Enter the 14-character license key when prompted and click Next.
- **11.** choose the installation location, if different from the default.

Note Do not change the default location of the local Temp Folder directory, or the installation will fail. The installer automatically extracts the installation files to the %TEMP% location.

12. Follow the remaining setup prompts to complete the installation.

From an MS-DOS command prompt, follow these steps as an administrator:

13. In preparation for the database movement to the previously created LUN from local storage, stop all OnCommand Unified Manager services and verify that the services have stopped.

dfm service stop dfm service list

14. Move the data to the previously created LUN.

Note

The **dfm datastore setup help** command provides switch options available with the command.

```
dfm datastore setup 0:\
```

15. Start OnCommand Unified Manager and then verify that all services have started.

```
dfm service start
dfm service list
```

16. Generate an SSL key.

```
dfm ssl server setup
Key Size (minimum = 512..1024..2048..) [default=512]: 1024
Certificate Duration (days) [default=365]: Enter
Country Name (e.g., 2 letter code): <<var_country_code>>
State or Province Name (full name): <<var_state>>
Locality Name (city): <<var_city>>
Organization Name (e.g., company): <<var_org>>
Organizational Unit Name (e.g., section): <<var_ unit>>
Common Name (fully-qualified hostname): <<var_oncommand_server_fqdn>>
Email Address: <<var_admin_email>>
```

Note

The SSL key command fails if certain command line option inputs do not follow specified character lengths (for example, a two-letter country code), and any multiword entries must be encased in double quotation marks, for example, "North Carolina."

17. Turn off automatic discovery.

dfm option set discoverEnabled=no

18. Set the protocol security options for communication with various devices.

dfm service stop http dfm option set httpsEnabled=yes dfm option set httpEnabled=no dfm option set httpsPort=8443 dfm option set hostLoginProtocol=ssh dfm option set hostAdminTransport=https



21. Set up OnCommand Unified Manager to send AutoSupport through HTTPS to NetApp.

dfm option set SMTPServerName=<<var_mailhost>>
dfm option set autosupportAdminContact=<<var_storage_admin_email>>
dfm option set autosupportContent=complete
dfm option set autosupportProtocol=https

22. Manually add the storage cluster to the OnCommand server.

dfm host add <<var_cluster1>>
dfm host add <<var_cluster2>>

23. Set the array login and password credentials in OnCommand Unified Manager. This is the root or administrator account.

dfm host set <<var_cluster1>> hostlogin=root
dfm host set <<var_cluster1>> hostPassword=<<var_password>>
dfm host set <<var_cluster2>> hostlogin=root
dfm host set <<var_cluster2>> hostPassword=<<var_password>>

24. List the storage systems discovered by OnCommand Unified Manager and their properties.

dfm host list
dfm host get <<var_cluster1>>
dfm host get <<var_cluster2>>

25. Test the network configuration and connectivity between the OnCommand server and the named host. This test helps identify misconfigurations that prevent the OnCommand server from monitoring or managing a particular appliance. The test should be the first command used if a problem using the OnCommand server occurs with only some of the appliances.

dfm host diag <<var_cluster1>>
dfm host diag <<var_cluster2>>

26. (optional) Configure an SNMP trap host.

dfm alarm create -T <<var_oncommand_server_fqdn>>

27. Configure OnCommand Unified Manager to generate and send e-mails for every event whose importance ranks as critical or higher.

dfm alarm create -E <<var_admin_email>> -v Critical

28. Create a manual backup.

dfm backup create -t snapshot

29. Schedule backups to a virtual backup directory on the 100GB FC LUN.

dfm option set backupRetentionCount=20

dfm backup schedule set -t snapshot -D 21:00

- **30.** To open Windows Firewall with Advanced Security, click Start > Administrative Tools > Windows Firewall with Advanced Security.
- 31. Choose Inbound Rules.
- 32. Click New Rule.
- 33. Choose Port and click Next.
- 34. Leave TCP selected and enter 8443 in the Specific local ports text box. Click Next.
- 35. Click Next.
- 36. Click Next.
- 37. Name the rule OnCommand Console External Access and click Finish.
- 38. Click New Rule.
- 39. Choose Port and click Next.
- 40. Choose UDP and enter 162 in the Specific local ports text box. Click Next.
- 41. Click Next.
- 42. Click Next.
- 43. Name the rule OnCommand SNMP Trap and click Finish.
- 44. Close Windows Firewall with Advanced Security.

NetApp NFS Plug-In 1.0 for VMware VAAI

Enable VMware vStorage for NFS in Data ONTAP 7-Mode

To enable VMware vStorage for NFS when Data ONTAP is operating in 7-mode, follow these steps:

- 1. From a Secure Shell (SSH) session on each storage controller, log in with the root user name and password.
- 2. Enable vStorage on the storage system.

options nfs.vstorage.enable on

Install NetApp NFS Plug-In for VMware VAAI

To install the NetApp NFS plug-in for VMware vStorage APIs for Array Integration (VAAI), follow these steps:

- From the vSphere console of the VSC and OnCommand virtual machine (VM), go to the Software Downloads page in the NetApp Support site.
- 2. Scroll down to locate the NetApp NFS Plug-in for VMware VAAI, choose the ESXi platform, and click Go.
- 3. Download the .vib file of the most recent plug-in version.
- **4.** Verify that the file name of the .vib file matches the predefined name that VSC 4.1 for VMware vSphere uses: NetAppNasPlugin.vib.


- 6. In the VMware vSphere Client connected to the vCenter Server, choose Home > Solutions and Applications > NetApp.
- 7. In the Monitoring and Host Configuration capability navigation pane, choose Tools.
- 8. Under NFS Plug-in for VMware VAAI, click Install on Host.

I

Provisioning and Closing Milk Tools Milk Tools Milk Tools Overview Milk Tools Milk Tools Milk Tools Milk Tools Overview Range Details - SAN Milk Tools Milk Tools Milk Tools Overview Range Details - SAN Milk Tools Details - SAN Milk Tools Details - MAS Details - SAN Details - SAN Details - SAN Details - MAS Details - SAN Details - SAN Details - SAN Details - SAN Details - SAN Details - SAN Details - SAN Details - SAN Details - SAN Details - SAN Details - SAN Details - SAN Details - SAN Details - SAN Details - SAN Details - SAN Details - SAN Details - SAN Details - SAN Details - SAN Details - SAN Goverload Deverview Details - SAN Goverload Deverview Milk Heile to a new, properly aligned - Nitz work Hile to a new, properly aligned - Nitz work Hile to a new, properly aligned - Nitz work Hile to a new, properly aligned - Nitz work Hile to a new, properly aligned - Nitz work Hile to a new, properly aligned - Nitz work Hile to a new, properly aligned - Nitz work Hile to a new, properly aligned - Nitz work Hile to a new, properly aligned - Nitz wor	7	com - vSohere Client				
Image: Solutions and Applications IP IP Provided Integrations IP IP Provided Integration IP Provided IP Pro	Eile Edit View Inventory	Administration Plug-ins Help				
Maintoring and Hot Conflored MRK Tools Overview Storage DataS - SAN Storage DataS - SAN Storage DataS - SAN Data Collecton This ESX concole-based tool bets and aligns guest file systems on a VMDK for VMFS and NFS didatores. Aligning the file system block boundaries to the underlying NeLAgo storage system LUN ensures the best storage performance. The data is migrated from a backup of the original -fild. wmdk file to a new, properly aligned -fild. wmdk file. Storage DataS - MAS Data Collecton Image DataS - SAN Storage DataS - MAS Data Collecton Image DataS - SAN Storage DataS - MAS Data Collecton • Tools Image DataS - SAN Storage DataS - MAS Data Collecton Image DataS - SAN Storage DataS - SAN Data Collecton Image DataS - SAN Storage DataS	🖬 🗈 🟠 Home	🕨 🗿 Solutions and Applications 🔹 📊 NetAp	ip 🕨 🛃 ICEF1-	-VC.ice.rtp.netapp.com		Search Inventory
Overview Storage Details - SAN Storage Details - SAN Storage Details - SAN Storage Details - SAN Details - SAN Storage Details - NAS Details - SAN Data Collection Image Details - SAN > Tools Details - SAN Details - SAN Details - SAN Storage Details - NAS Details - SAN Data Collection Image Details - SAN > Tools Deventional Decovery Status Cuest OS Tools Outer OS Inneod scripts are used to at the SCS IO lineout values for supported guest operating systems. The timeout values ensure correct failover behavior. Right click the tools URL to copy it to the clipboard. Linux OS Https://192.108.175.194.8143/vsclpublic/writable/minux_gos_timeout.install iso Windowe OS Https://192.108.175.194.8143/vsclpublic/writable/minux_gos_timeout.install iso Nindowe OS Https://192.108.175.194.8143/vsclpublic/writable/colaris_gos_timeout.install iso <t< td=""><td>Monitoring and Host Configuration</td><td>MBR Tools</td><td></td><td></td><td></td><td></td></t<>	Monitoring and Host Configuration	MBR Tools				
NFS Plug-in for VMware VAAI Provisioning and Cloning Optimization and Migration Backup and Recovery About Install on Host Install on Host Vame Target Status Details	Overview Storage Details - SAN Storage Details - NAS Data Collection • Tools Discovery Status	This ESX console-based tool tests and align underlying NetApp storage system LUN ens- aligned -flat.vmdk file. Guest OS Tools Guest OS timeout scripts are used to set th Right click the tools URL to copy it to the clip Linux OS https://192.168.175.194:8143/vsc/public/wr Solaris OS https://192.168.175.194:8143/vsc/public/wr	s guest file system ures the best store wnload X 4.x) e SCSI I/O timeout v iboard. itable/linux_gos_tim itable/windows_go itable/solaris_gos_	ns on a VMDK for VMFS and NFS d age performance. The data is migra Download (For ESXi 4.x and ESXi 5.x) values for supported guest operation neout-install iso os_timeout.iso timeout-install iso	atastores. Aligning the ted from a backup of t	file system block boundaries to the he original -flat.vmdk file to a new, properly t values ensure correct failover behavior.
Optimization and Migration NFS Plug-in for VMware VAAI version: 1.0-018 Note: Before you install the NFS Plug-in for VMware VAAI, check the Release Notes for more information concerning the latest version of the plug-in. Backup and Recovery Install on Host About Install on Host ecent Tasks Name, Target or Status contains: • Clear Vame Target Status Details Initiated by vCenter Server Requested Start Ti v	Provisioning and Cloning	The NFS Plug-in for VMware VAAI is a soft enable VMware to execute various primitiv	ware library that in es on files stored o	tegrates with VMware's Virtual Dis n NetApp storage systems. You ca	k Libraries, which are n install the plugin on a	installed on the ESXi hosts. These libraries a host using VSC.
Backup and Recovery Plug-in. About Install on Host ecent Tasks Name, Target or Status contains: Name Target Status Details	Optimization and Migration	NFS Plug-in for VMware VAAI version: Note: Before you install the NFS Plug-in	1.0-018) for VMware VA	Al, check the Release Notes for	more information	concerning the latest version of the
About Install on Host Install	Backup and Recovery	plug-ín.				
Initiated by Venter Server Requested Start Ti	About			Install	on Host	
Name Target Status Details Initiated by vCenter Server Requested Start Ti v	Recent Tasks				Name, Target or Statu	is contains: - Clear
	Name	Target Status	Details		Initiated by v	Ienter Server Requested Start Ti 🗸

Figure 109 Installing NFS Plug-in for VMware VAAI on Host

1

9. Choose all ESXi hosts and click Install, and then click Yes.

<u>)</u> Note

The Monitoring and Host Configuration capability automatically installs the plug-in on the hosts selected.

JCEF1-VC.ice.rtp.netapp.	com - vSphere Client	telo					
E E Arrentory	Golutions and Applica	ations 🕨 🗾 NetApp	ICEF1-VC.ice.rtp.r	etapp.com		💦 🗸 Search I	nventory
Monitoring and Host Configuration	MBR Tools					_	
Overview Storage Details - SAN	This ESX console-bas underlying NetApp sto aligned -flat.vmdk file.	ed tool tests and aligns g rage system LUN ensure	uest file systems on a VMD s the best storage perform	K for VMFS and NFS datastores ance. The data is migrated from	a backup of the fi a backup of th	ile system block bo e original -flat.vmc	oundaries to the Ik file to a new, proper
Storage Details - NAS	[1	NFS Plug-in for VMwar	e VAAI				×
Data Collection • Tools		Select the hosts on whi selectable.	ch you want to install the N	FS Plug-in for VMware VAAI. Inc	compatible ESX,	/ESXi hosts are no	:
Discovery Status		🔽 🗐 icef1-h6.ice.r	tp.netapp.com: 192.16	3.175.63			
	Guest OS Tools	🔽 🛙 icef1-h11.ice	rtp.netapp.com: 192.1	58.175.100			
	Guest OS timeout sc Right click the tools L						ailover behavior.
	Linux OS https://192.168.175.1						
	Windows OS https://192.168.175.1						
	Solaris OS https://192.168.175.1						
	NFS Plug-in for VMv						
Provisioning and Cloning	The NFS Plug-in for V enable VMware to e						s. These librarie
Optimization and Migration	NFS Plug-in for VN	vare VAAI version: 1.0-			Install	Cancel	
Padua and Paraway	Note: Before you ik. plug-in.	stall the NFS Plug-in fo	- VMwaro-VAAI, chock t	he Release Holes for more i	nformation or	oncorning the la	way version of the
васкир апо кесочегу					-		
About				Install on Host			
lecent Tasks				Name, T	arget or Status	contains: 👻 🗌	
Name	Target	Status	Details	Initiate	ed by VCe	nter Server	Requested Start Ti

Figure 110 Selecting All the ESXi Host for Installing NFS Plug-in

I

Γ

10. Choose **Home > Inventory > Host and Clusters**.

11. For each host (one at a time), right-click the host and choose Enter Maintenance Mode.



Figure 111 Entering Maintenance Mode in vSPhere Client

12. Click Yes, click Yes again, and then click OK.

Note It might be necessary to migrate all VMs away from the host.

- 13. After the host is in maintenance mode, right-click the host and choose Reboot.
- 14. Enter a reason for the reboot and click OK.

- **15.** After the host reconnects to the vCenter Server, right-click the host and choose Exit Maintenance Mode.
- 16. Make sure that all ESXi hosts get rebooted.

NetApp VASA Provider

Install NetApp VASA Provider

I

To install NetApp VASA Provider, follow these steps:

- Using the previous instructions for virtual machine creation, build a VASA Provider virtual machine with 2GB RAM, two CPUs, and one virtual network interface in the <<var_ib-mgmt_vlan_id>> VLAN. The virtual network interface should be a VMXNET 3 adapter. Bring up the VM, install VMware Tools, assign IP addresses, and join the machine to the Active Directory domain.
- 2. Log into the VASA Provider VM as the FlexPod admin user.
- 3. Download NetApp VASA Provider from the NetApp Support site.
- 4. Run the executable file netappyp-1-0-winx64.exe to start the installation.

Figure 112 Preparing to Install NetApp VASA provider

NetApp FAS && V-Series VAS/	A Provider - InstallShield Wizard
	Preparing to Install
0	NetApp FAS & V-Series VASA Provider Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.
	Extracting: NetApp FAS V-Series VASA Provider.msi
NY L	
	Lancel

- 5. On the Welcome page of the installation wizard, click Next.
- 6. Choose the installation location and click Next.

estination Click Ne:	n Folder xt to install to this folder, or clid	:k Change to insta	all to a different fo	older.
D	Install NetApp FAS & V-Serie C:\Program Files\NetApp\VA	s VASA Provider t 5A\	0:	Change
allShield -		< Back	Next >	Gancel

1

7. On the Ready to Install page, click Install.



🕞 NetApp FAS & Y-Series VASA Provi	ider 1.0		×
Ready to Install the Program The wizard is ready to begin installatio	n,		
Click Install to begin the installation.			
If you want to review or change any o exit the wizard.	f your installation s	ettings, click Back. Cl	ick Cancel to
InstallShield	< Back	Install	Cancel

8. Click **Finish** to complete the installation.



Figure 115 Installation Completed

Configure NetApp VASA Provider

After NetApp VASA Provider is installed, it must be configured to communicate with the vCenter Server and retrieve storage system data. During configuration, specify a user name and password to register NetApp VASA Provider with the vCenter Server, and then add the storage systems before completing the process.

Add Storage Systems

The NetApp VASA Provider dialog box can be used to add the storage systems from which NetApp VASA Provider collects storage information. Storage systems can be added at any time.

To add a storage system, follow these steps:

- 1. Double-click the VASA Configuration icon on your Windows desktop or right-click the icon and choose Open to open the NetApp FAS/V-Series VASA Provider dialog box.
- 2. Click Add to open the Add Storage System dialog box.

Figure 116

NetApp FAS/¥-Se	eries VASA Provider 1.0					
VASA Provider				Storage Systems -		
Enter a user nam	e and password for initial commu	unication with vCe	nter Server	Registered Storage	Systems	
User Name:	ice\icef1-admin		Save	1		
Password:	•••••		Edit			
Status:	😑 NetApp VASA Provider service	is running				
Alarm Thresholds						
Threshold values	s are saved when you click the OK	button				
	Volume	Aggregate				
Nearly Full Thre	shold (%): 85	90				
Full Threshold (%): 90	95				
VMware vCenter						
Ser <u>v</u> er Address		Port: 443	Register Provider	1		
User Na <u>m</u> e:			Unregister Provider			
Pass <u>w</u> ord:			l	Add	Remove	Edit
Or copy the URL	below to register VASA Provider (from VMware vSpl	here Client			
VASA URL:	https://ICEF1-VASA.ice.rtp.netapp	p.com:8443/services,	/vasaService			
				-	ок	Cancel

3. Enter the host name or IP address, port number, and user name and password for the storage system.

1

1

Figure 117 Entering Storage System Login Credentials

Adding Storage Systems

📊 Add Storage 🤉	ōystem	×
i Enter St	orage System Credential Information	
St <u>o</u> rage System:	192.168.171.144	_
Protocol:		
Port:	443	
<u>U</u> ser:	root	
P <u>a</u> ssword:	••••••	
	OK <u>C</u> ancel	

- 4. Click **OK** to add the storage system.
- 5. Add both storage systems to the VASA Provider.

Register NetApp VASA Provider with vCenter Server

To establish a connection between the vCenter Server and NetApp VASA Provider, NetApp VASA Provider must be registered with the vCenter Server. The vCenter Server communicates with NetApp VASA Provider to obtain the information that NetApp VASA Provider collects from registered storage systems.

To register NetApp VASA Provider with the vCenter Server, follow these steps:

1. Under Alarm Thresholds, accept or change the default threshold values for volume and aggregate. These values specify the percentages at which a volume or aggregate is full or nearly full.

The default threshold values are the following:

- 85% for a nearly full volume
- 90% for a full volume
- 90% for a nearly full aggregate
- 95% for a full aggregate

Note

After you finish registering NetApp VASA Provider with the vCenter Server, any changes made to the default threshold values are saved only when you click OK.

- 2. Under VMware vCenter, enter the host name or IP address of the vCenter Server machine and the user name and password for the vCenter Server.
- 3. Specify the port number to use, or accept the default port number for the vCenter Server.
- 4. Click Register Provider.
- 5. Click **OK** to commit all the details and register NetApp VASA Provider with the vCenter Server.



To use the vSphere Client to register NetApp VASA Provider with the vCenter Server, copy the URL from the VASA URL field and paste it into the vCenter Server.

NetApp FAS/V-Se	eries VASA Provider 1.0					
VASA Provider				Storage Systems —		
Enter a user nam	e and password for initial commu	nication with vCenter	Server	Registered Storage S	Systems	
User Name:	ice\icef1-admin		Save	icef1-st1a (192.168	.171.144)	
Password:	•••••		Edit	icef1-st1b (192.168	.171.145)	
Status:	\ominus NetApp VASA Provider service i	s running				
Alarm Thresholds						
Threshold values	are saved when you click the OK	button				
	Volume	Aggregate				
Nearly Full Thre	shold (%): 85	90				
Full Threshold (%): 90	95				
VMware vCenter						
Ser <u>v</u> er Address	: 192.168.175.188	Port: 443 🛨	Register Provider			
User Name:	ice\icef1-admin		Unregister Provider			
Pass <u>w</u> ord:	•••••			Add	Remove	Edit
Or copy the URL	below to register VASA Provider fi	rom ¥Mware vSphere	Client			
VASA URL:	https://ICEF1-VASA.ice.rtp.netapp	.com:8443/services/vasa	Service			
				-	OK	Cancel

Figure 118 Registering NetApp VASA Provider with VMware vCenter

1

1

6. Click **OK** to close the VASA Configuration.

Verify VASA Provider in vCenter

- **1**. Log in to vCenter using vSphere Client.
- 2. Click the Home tab at the upper-left portion of the window.
- 3. In the Administration section, click Storage Providers.
- 4. Click Refresh All. The NetApp VASA Provider (NVP) should now appear as a vendor provider.

D isclust us issues a	taan com uCabour (liant				
Cerxp1-vc.ice.rtp.ne	tapp.com - vSphere L	lient				
File Edit View Invent	ory <u>A</u> dministration <u>P</u> lug)-ins <u>H</u> eip				
💽 💽 🏠 Hon	ne 🕨 🦓 Administration	n 🕨 🔯 Stora	ge Providers 🛛 🦻 ice	fxp1-vc.ice.rtp.netapp.com	😽 🗸 Search Inve	entory 🔍
					Add Remove Re	fresh All Sync
Name		URL			Last Refresh Time	Last Sync
NVP		https://icef	xp1-vasa.ice.rtp.netapp	.com:8443/services/vasaService	6/6/2012 10:31:44 A	M 6/6/2012 1
Vendor Provider De	tails					
Provider Name:	NVP		API Version:	1.0		
Provider Status:	online		Default Namespace:	ONTAP		
Provider Version:	1.0					
Supported Vendor ID	5	Supported N	1odel IDs			
Recent Tasks				Name, Target or Sta	atus contains: 👻	Clear ×
Name	Target	Status	Details	Initiated	by vCenter Server	Requested Start Ti
•						<u>•</u>
77 Taska 🔗 Alama				Lie	ense Period: 100 davs remaining	Administrator

Figure 119 NetApp VASA Provider is Listed as Vendor Provider

- 5. Click the **Home** tab in the upper-left portion of the window.
- 6. In the Inventory section, click **Datastores and Datastore Clusters**.
- 7. Expand the vCenter and the data center. Choose a datastore.

ſ

8. Click the Summary tab. Verify that a System Storage Capability appears under Storage Capabilities.



Figure 120 Summary Showing System Storage Capability Under Storage Capabilities

Appendix

Build Windows Active Directory Server VM(s)

ESXi Host VM-Host-Infra-01

To build an Active Directory Server virtual machine (VM) for the VM-Host-Infra-01 ESXi host, follow these steps:

- 1. Log in to the host by using the VMware vSphere Client.
- 2. In the vSphere Client, choose the host in the inventory pane.
- 3. Right-click the host and choose New Virtual Machine.
- 4. Choose Custom and click Next.
- 5. Enter a name for the VM. Click Next.
- 6. Choose infra_datastore_1. Click Next.
- 7. Choose Virtual Machine Version: 8. Click Next.

- Verify that the Windows option and the Microsoft Windows Server 2008 R2 (64-bit) version are selected. Click Next.
- 9. Choose two virtual sockets and one core per virtual socket. Click Next.
- 10. Choose 4GB of memory. Click Next.
- **11**. Choose one network interface card (NIC).
- 12. For NIC 1, choose the IB-MGMT Network option and the VMXNET 3 adapter. Click Next.
- 13. Keep the LSI Logic SAS option for the SCSI controller selected. Click Next.
- 14. Keep the Create a New Virtual Disk option selected. Click Next.
- 15. Make the disk size at least 60GB. Click Next.
- 16. Click Next.
- 17. Check the check box for Edit the Virtual Machine Settings Before Completion. Click Continue.
- **18**. Click the **Options** tab.
- 19. choose Boot Options.
- **20.** Check the Force BIOS Setup check box.
- 21. Click Finish.
- 22. From the left pane, expand the host field by clicking the plus sign (+).
- 23. Right-click the newly created AD Server VM and click Open Console.
- 24. Click the third button (green right arrow) to power on the VM.
- **25.** Click the ninth button (CD with a wrench) to map the Windows Server 2008 R2 SP1 ISO, and then choose Connect to ISO Image on Local Disk.
- 26. Navigate to the Windows Server 2008 R2 SP1 ISO, select it, and click Open.
- **27.** In the BIOS Setup Utility window and use the right arrow key to navigate to the Boot menu. Use the down arrow key to choose CD-ROM Drive. Press the plus (+) key twice to move CD-ROM Drive to the top of the list. Press F10 and Enter to save the selection and exit the BIOS Setup Utility.
- **28.** The Windows Installer boots. Choose the appropriate language, time and currency format, and keyboard. Click **Next**.
- 29. Click Install now.
- **30.** Make sure that the Windows Server 2008 R2 Standard (Full Installation) option is selected. Click **Next**.
- **31.** Read and accept the license terms and click **Next**.
- **32.** Choose Custom (Advanced). Make sure that Disk 0 Unallocated Space is selected. Click **Next** to allow the Windows installation to complete.
- **33.** After the Windows installation is complete and the VM has rebooted, click **OK** to set the Administrator password.
- **34.** Enter and confirm the Administrator password and click the blue arrow to log in. Click **OK** to confirm the password change.
- **35.** After logging in to the VM desktop, from the VM console window, choose the VM menu. Under Guest, choose Install/Upgrade VMware Tools. Click **OK**.
- **36.** If prompted to eject the Windows installation media before running the setup for the VMware tools, click **OK**, then click **OK**.
- 37. In the dialog box, choose Run setup64.exe.

- 38. In the VM ware Tools installer window, click Next.
- **39.** Make sure that Typical is selected and click Next.
- 40. Click Install.
- 41. Click Finish.
- 42. Click Yes to restart the VM.
- **43.** After the reboot is complete, choose the VM menu. Under Guest, choose Send Ctrl+Alt+Del. Then enter the password to log in to the VM.
- 44. Set the time zone for the VM, IP address, gateway, and host name.

Note A reboot is required.

- 45. If necessary, activate Windows.
- 46. Download and install all required Windows updates.



Note This process requires several reboots.

- 47. Open Server Manager.
- 48. On the left, click Roles, the choose Add Roles on the right.
- 49. Click Next.
- 50. In the list, check the check box next to Active Directory Domain Services.
- 51. In the popup, click Add Required Features to add .NET Framework 3.5.1.

Figure 121 Selecting Roles to Install on the Server

Add Roles Wizard

Γ

Select Server Rol	25
Before You Begin Server Roles Active Directory Domain Services Confirmation Progress Results	Select one or more roles to install on this server. Roles: Description: Active Directory Certificate Services Active Directory Domain Services (AD. DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network administrators. AD DS uses domain controllers to give network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process. DHCP Server DNS Server Fax Server File Services Web Server (IIS) Windows Deployment Services Windows Server Update Services Windows Server roles Windows Server roles Windows Server roles
	< Previous Next > Install Cancel

- 52. Click Next.
- 53. Click Next.

Figure 122	Confirming Installation Selections
Add Roles Wizard	
Confirm Installatio	on Selections
Before You Begin Server Roles Active Directory Domain Services	To install the following roles, role services, or features, click Install.
Confirmation Progress	This server might need to be restarted after the installation completes. Active Directory Domain Services
Results	(i) After you install the AD DS role, use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.
	NET Framework 3.5.1 NET Framework 3.5.1 Print, e-mail, or save this information
	< Previous Next > Install Cancel

1

54. Click Install.

Figure 123 Installation Completion Summary

Add Roles Wizard

ſ

Installation Resu	lts					
Before You Begin Server Roles Active Directory Domain Services	The following roles, role services, or features wer	re installed successfully:				
Confirmation	Active Directory Domain Services	🔮 Installation succeeded				
Progress Results	The following role services were installed: Active Directory Domain Controller (i) Use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.					
	Close this wizard and launch the Active Direct	ory Domain Services Installation Wizard (dcpromo.exe).				
	 .NET Framework 3.5.1 Features 	🥑 Installation succeeded				
	The following features were installed: .NET Framework 3.5.1					
	Print, e-mail, or save the installation report					
	< <u>Pre</u>	evious Next > Close Cancel				

- **55.** In the middle of the window, click **Close** this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe).
- 56. In the Active Directory Domain Services Installation Wizard, click Next.
- 57. Click Next.
- 58. Choose Create a new domain in a new forest and click Next.

hoose a Deployment Configuration You can create a domain controller for an e	existing forest or for a new forest.	
C Existing forest		
\mathbf{C} Add a domain controller to an exist	ing domain	
C Greate a new domain in an existing This server will become the first do	g forest main controller in the new domain.	
Create a new domain in a new forest		
More about possible deployment configurati	ions	

59. Type the FQDN of the Windows domain for this FlexPod and click **Next**.

1

Figure 125 Naming the Forest Root Domain

The first domain in the forest is the forest root domain. Its name is also the name of the forest.	
Type the fully qualified domain name (FQDN) of the new forest root domain.	
EQDN of the forest root domain:	
icef1.ice.rtp.netapp.com	
Z Back Nevt >	Cancel

I

Γ

- 60. Choose the appropriate forest functional level and click Next.
- 61. Keep DNS server selected and click Next.

litional Domain Controller Options		
Select additional options for this domain cor	ntroller.	
DNS server		
🔽 <u>G</u> lobal catalog		
<u>Read-only domain controller (RODC)</u>		
Additional information:		
We recommend that you install the DNS S controller.	Server service on the first domain	Y
More about additional domain controller op	<u>ptions</u>	

62. If one or more DNS servers exist that this domain can resolve from, Click **Yes** to create a DNS delegation. If this is AD server is being created on an isolated network, click **No**, to not create a DNS delegation. The remaining steps in this procedure assume a DNS delegation is not created. Click **Next**.

Controller

- 63. Click Next to accept the default locations for database and log files.
- **64.** Enter and confirm <<var_password>> for the Directory Services Restore Mode Administrator Password. Click Next.
- 65. Review the Summary information and click Next. Active Directory Domain Services will install.
- 66. Click Finish.
- 67. Click Restart Now to restart the AD Server.
- 68. After the machine has rebooted, log in as the domain Administrator.
- 69. Open the DNS Manager by clicking Start > Administrative Tools > DNS.
- 70. (Optional) Add Reverse Lookup Zones for your IP address ranges.
- **71.** Expand the Server and Forward Lookup Zones. Choose the zone for the domain. Right-click and choose New Host (A or AAAA). Populate the DNS Server with Host Records for all components in the FlexPod.
- **72.** (Optional) Build a second AD server VM. Add this server to the newly created Windows Domain and activate Windows. Install Active Directory Domain Services on this machine. Launch dcpromo.exe at the end of this installation. Choose to add a domain controller to a domain in an

existing forest. Add this domain controller to the domain created earlier. Complete the installation of this second domain controller. After vCenter Server is installed, affinity rules can be created to keep the two AD servers running on different hosts.

Configuring Cisco VM-FEX with the UCS Manager

Background

FlexPod for VMware utilizes distributed virtual switching to manage the virtual access layer from a central point. While previous versions of FlexPod have only described the use of the Cisco Nexus 1000V, there exists an option to use the built-in virtual switching functionality delivered through hardware on the Cisco UCS known as VM-FEX. This has several advantages:

- There is no need for extra HW such as Cisco Nexus 1110-X.
- Cisco UCS provides a central configuration environment with which the administrator is already familiar.
- Compared to using the Cisco Nexus 1000v as virtual appliances within vCenter itself, this setup avoids an SPOF and common restart issues when running the distributed switches in an environment in which they are required for the network functionality of the ESX servers on which they are running. This is a common problem that needs to be addressed in the solution design.

In other words, it dramatically simplifies the hardware setup and operation by optimally utilizing the new hardware features.

Process Overview

This section provides a detailed overview of VM-FEX setup, configuration, and operation using Cisco UCS Manager.

This section describes:

- Initial setup and configuration
- Operation, that is, adding networks for additional tenants

For configuration details, see Configuration Guide: http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/vm_fex/vmware/gui/config_guide/2.1/b_ GUI_VMware_VM-FEX_UCSM_Configuration_Guide_2_1.html

Initial Setup

For initial setup, follow these steps:

- 1. Create a vNIC connection policy in Cisco UCS Manager.
- 2. Create a server BIOS policy.
- 3. Clone an existing service profile.
- 4. Install the VEM software on the ESX server.
- 5. Install the plug-in into vCenter.

Create a Dynamic vNIC Connection Policy

To define the dynamic vNIC connection policy that vNICs created from a vNIC template should use, follow these steps in Cisco UCS Manager:

- 1. Log in to Cisco UCS Manager.
- 2. Click the LAN tab in the left navigation pane and click LAN > Policies > root > Sub-organizations (name of the suborganization if applicable) > Dynamic vNIC Connection Profile.
- 3. Right-click and choose Create Dynamic vNIC Connection Policy to start the wizard.
- **4.** Type a name and description for the vNIC connection policy. Choose VMWare from the Adapter Policy drop-down menu. Choose the Protected option. Click **OK**.

Note

- The Protected option allows the vNIC to use both fabric A and fabric B.
 - With Cisco UCS C-Series servers, the number of dynamic vNICs that can be used depends on the hardware in use. Refer to appendix 13.3, "VM-FEX Virtual Interfaces."



🚔 Create Dynamic vNIC (Connection Policy		×
Create Dynami	c vNIC Connection Policy		0
Name: Number of Dynamic vNICs: Adapter Policy: Protection:	FEX 64 WMWare Protected Pref A Protected Pref B Protected	Description:	1 cand

Create a Server BIOS Policy

To define the BIOS policy for a service profile that supports VM-FEX on ESXi, follow these steps in Cisco UCS Manager:

I

- Click the Server tab in the left navigation pane, and choose Server > Policies > root > Sub-organizations (name of the suborganization if applicable) > BIOS Policies.
- 2. Right-click and choose Create BIOS Policy to start the wizard.
- 3. Type a name for the policy and retain the platform defaults.



4. For Virtualization Technology (VT) and Direct Cache Access, choose enabled.

I

Create BIOS Policy			×
Unified C	omputing	System Manager	
Create BIOS Policy	Processor		0
2. √ Processor 3. ☐ Intel Directed IO 4. ☐ RAS Memory 5. ☐ Serial Port 6. ☐ USB 7. ☐ PCI Configuration 8. ☐ Boot Options 9. ☐ Server Management	Turbo Boost: Enhanced Intel Speedstep: Hyper Threading: Core Multi Processing: Execute Disabled Bit: Virtualization Technology (VT): Direct Cache Access: Processor C State: Processor C State: Processor C3 Report: Processor C6 Report: Processor C7 Report:	C disabled C enabled © Platform Default C disabled C enabled © Platform Default C disabled C enabled © Platform Default Platform Default C disabled C enabled © Platform Default C disabled © enabled © Platform Default C disabled © enabled © Platform Default C disabled C enabled © Platform Default	
	Max Variable MTRR Setting:	C auto-max C 8 C Platform Default	

1

- 5. Click Next.
- **6.** For VT For Directed IO, choose enabled.

🚖 Create BIOS Policy		×
Unified C	omputing System Manager	
Create BIOS Policy	Intel Directed IO	Ø
 √<u>Main</u> 2. √<u>Processor</u> 3. √<u>Intel Directed IO</u> 4. □<u>RAS Memory</u> 5. □<u>Serial Port</u> 6. □<u>USB</u> 7. □<u>PCI Configuration</u> 8. □<u>Boot Options</u> 9. □<u>Server Management</u> 	VT For Directed IO: (disabled (enabled (Platform Default Interrupt Remap: disabled (enabled (Platform Default Coherency Support: disabled (enabled (Platform Default ATS Support: disabled (enabled (Platform Default Pass Through DMA Support: disabled (enabled (Platform Default	
	<pre> < Prev Next > Finish</pre>	Cancel

Figure 130 Intel Directed IO Settings for BIOS Policy

- 7. Click Next.
- 8. The remaining sections of the Create BIOS Policy wizard (RAS Memory, Serial Port, USB, PCI Configuration, Boot Options, and Server Management) can retain the Platform Default option. Click Next on each of these windows and then click Finish to complete the wizard.

Create a VM-FEX Enabled Service Profile Template

I

To create a Cisco UCS service profile using VM-FEX, clone a previously defined Cisco UCS service profile and apply the dynamic vNIC and BIOS policies by following these steps in the Cisco UCS Manager:

- 1. Click the Servers tab in the left navigation pane and expand the Service Profile Templates.
- 2. Right-click VM-Host-Infra-Fabric-A and choose Create a Clone.
- 3. Type a clone name and choose an organizational owner for the new service profile template.

Fig	gure 131	Cloning Ser	vice Profil	e Template
Create Clone From V	M-Host-Inf	ra-Fabric-B	×	
? Clone Name:				
Org:			-	
OK	Cancel	Help		

- 4. Click **OK** when notified that the service profile clone was successfully created. The Service Template navigation window appears.
- **5.** Click the **Network** tab and choose **Change Dynamic vNIC Connection Policy** under the Actions section of the working pane. The Change Dynamic vNIC Connection Policy form appears.
- **6.** Choose Use a Dynamic vNIC Connection Policy from the drop-down menu and the previously created Dynamic vNIC policy. Click **OK**.

Figure 132 Changing the Dynamic vNIC Connection Policy

😓 Change Dynamic vNIC Connection Policy	×
Change Dynamic vNIC Connection Policy	0
Select the Dynamic vNIC Connection Policy	
ОК Са	ncel

7. Click OK when notified that the vNIC connection policy was successfully modified.

1

8. From the Service Template properties window, click the Policies tab.

9. Expand the BIOS Policies in the Policies section of the working pane.

10. Choose the previously defined FEX BIOS policy and click OK.

Properties for: Service Template	//H-Host-Infra-V/MFEX-Fabric-B	_O×
Actions	Policies	
S Change Serial over LAN Policy	BIOS Policy	8
	BIOS Policy: FEX Create BIOS Policy	
	Firmware Policies	8
	IPMI Access Profile Policy	8
	Power Control Policy	8
	Scrub Policy	8
	Serial over LAN Policy	8
	Stats Policy	8
	OK Apply Cancel	Help

Figure 133 Choosing a BIOS Policy

Create VM-FEX Service Profile

ſ

To create service profiles from the service profile template, follow these steps:

- 1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
- 2. Choose Service Profile Templates > Service Template VM-Host-Infra-VMFEX-Fabric-A.
- 3. Right-click VM-Host-Infra-FEX-Fabric-A and choose Create Service Profiles from Template.
- 4. Enter VM-Host-FEX-0 as the service profile prefix.
- 5. Enter 1 as the number of service profiles to create.
- 6. Click OK to create the service profile.

Figure 134	reating Service Profile from Template
🚖 Create Service Profiles From Tem	late X
Create Service Profile	s From Template 🤍 🥹
Naming Prefix: VM-Host-FEX- Number: 1	OK Cancel

- 7. Click **OK** in the confirmation message.
- **8.** Verify that the service profile VM-Host-FEX-1 has been created. The service profile is automatically associated with the servers in their assigned server pools.

Install and Set Up VMware ESXi

Refer to section 11.1 to install and completely set up VMware ESXi version 5.1 on the two ESXi hosts. After ESXi setup is complete, add the two new hosts to VMware vCenter.

Download Cisco VEM Software Bundle

To download the Cisco UCS B-Series or C-Series server drivers, follow these steps:



The following bundle was used during validation cisco-vem-v151-5.1-1.1.1.vib.

- 1. Open a Web browser on the management workstation and navigate to the following Cisco Download Software pages:
 - a. Downloads Home > Products > Servers Unified Computing > Cisco UCS B-Series Blade Server Software > Unified Computing System (UCS) Drivers-2.1(1d)
 - b. Downloads Home > Products > Servers Unified Computing > Cisco UCS C-Series Rack-Mount UCS-Managed Server Software > Unified Computing System (UCS) Drivers-1.4(5b)
- 2. Follow the steps necessary to download the software bundles located on the ISO image.
- **3.** Mount the ISO image and copy the appropriate vib file from the VMware > VM-FEX > Cisco directory to the local machine.
- 4. From the vCenter vSphere Client, choose the infra_datastore_1 in the Inventory > Datastores and Datastore Clusters navigation menu.
- 5. Under the Basic Tasks choose Browse this Datastore
- **6.** Choose the root folder (/) and click the third button at the top to add a folder.

- 7. Name the folder VM-FEX and click OK.
- 8. On the left, choose the VM-FEX folder.
- 9. Click the fourth button at the top and choose Upload File.
- **10.** Navigate to the cisco-vem-v151-5.1-1.1.1.1.vib file and click Open.
- Click Yes to upload the .vib file to infra_datastore_1.
 The VM-FEX file should now appear in the VM-FEX folder in the datastore.

Install the FEX Virtual Ethernet Module on Each ESXi Host

To install the Virtual Ethernet Module (VEM) on the ESXi hosts, follow these steps:

- 1. Open the VMware vSphere CLI command prompt.
- 2. For each ESXi host in the VMware vSphere CLI, run the following command:

```
esxcli -s <host_ip> -u root -p <host_password> software vib install -v
/vmfs/volumes/infra_datastore_1/VM-FEX/cisco-vem-v151-5.1-1.1.1.vib
```

Integrate Cisco UCS with vCenter

To integrate Cisco UCS Manager and vCenter, follow these steps:

- 1. Log in to the Cisco UCS Manager.
- 2. In the navigation pane, click the VM tab, and in the VM tab, expand the All folder. Choose the VMware node, and in the Working Area, click the **General** tab.
- 3. Choose Configure VMware Integration in the Actions area to start the Configuration wizard.

Figure 135 Configuring VMware Integration



4. Follow the instructions and click **Export** and complete the steps to install the UCSM extension file in vCenter.

Figure 136

Exporting vCenter Extension Plug-in

I

1

e VMware Integration

Configure VMware Integration		×
Unified C	omputing System Manager	
Configure VMware Integration	Install Plug-in on vCenter Server To establish the relationship and communication between Cisco UCS Manager and VMware vCenter, one or more extension XML files need to be installed on the vCenter server. To create the extension XML file for vCenter 4.0 update or later, click the Export button below. To create the eight extension XML files for vCenter 4.0, click the Export Multiple button below. To create the eight extension XML files for vCenter 4.0, click the Export Multiple button below. vCenter Extension plug-in Export Export Export Multiple After exporting the XML extension file(s), copy them to the vCenter server. To install the extension file(s) in vCenter, log into the vCenter server through the vSphere client. From the Plug-ins menu, choose Plug-in Manager. Right-click in the Plug-in Manager window and select New Plug-in In the Register Plug-in dialog, click the Browse button to locate the XML extension file(s) you copied to the server.	2
	After installing the extension XML file(s), click the Register Plug-in button in the Register Plug-in dialog. Once the plug-in registration process completes, return to this wizard and click the Next button below.	

- 5. Click Next.
- 6. Enter the VMware vCenter Server name, vCenter Server host name or IP address, vCenter data center name, DVS folder, and DVS name.
- 7. Click Next.

Figure 137

I

Γ

Defining VMware DVS

Unified C	omputing System Manager
 onfigure VMware Integration 1. √<u>Install Plug-in on vCenter</u> Server 2. X <u>Define VMware</u> <u>Distributed Virtual</u> <u>switch(DVS)</u> 3. Define Port Profile 4. Doply Port Profiles to Virtual Machines in vCenter Server 	Define VMware Distributed Virtual Switch(DVS)

8. Create the FEX-MGMT port profile, choose the MGMT-VLAN, and indicate it is the native VLAN.

Figure 13	8 Defining Port	Profile for VMware Integra	tion	
onfigure VMware Integration	41			
Unified Co	omputin	g System I	Manager	
igure VMware Integration	Define Port Pr	ofile		
1. √Install Plug-in on vCenter				
Server	Deat Death			
2. V Define VMware Distributed	Port Profile			
3. √ Define Port Profile	Name:	FEX-MGMT		-
4. Apply Port Profiles to	OoS Policy:	<not set=""></not>		
Virtual Machines in vCenter	Network Control Policy	(not set)		
Server	Network Condition Policy.			
	Max Ports:	64		
	Pin Group:	<not set=""></not>		
	VLANs			
	Select	Name	Native VLAN	12
		default	0	^
		Foobar 1_public	0	
		MGMT-VLAN	•	
		NFS-VLAN	C	
		Native-VLAN	0	_
		Packet-Control-VLAN	<u> </u>	
		Service-HA	0	
		ServiceNodeServices	0	
		VM-Trame-VLAN	0	
		VINOBOIT-VEAN		
	a fil strai			
	Profile Client			
	Name	E FEX-MGMT	_	
	Description			
	Description			
	Datacente			
	Folder	UVS-FEX		
	Distributed Virtual Switch	n: DVS-FEX		
		<u> </u>		

1

- 9. Click Next.
- 10. When finishing the wizard, the Cisco UCS Manager connects to vCenter and adds the plug-in.

Figure 139

VMware Integration is succesful

figure VMware Integration	Apply Port Profiles to Virtual Machines in vCenter Server
 √<u>Install Pluq-in on vCenter</u> Server √<u>Define VMware Distributed</u> <u>Virtual Switch(DVS)</u> √<u>Define Port Profile</u> √<u>Apply Port Profiles to</u> <u>Virtual Machines in</u> <u>vCenter Server</u> 	After you complete this wizard, use VMware vCenter to create the virtual machines (VMs). Associate the VMs with the distributed virtual switch (DVS). Associate the port profiles (available as port groups) with the DVS.
	Configure VMware Integration × VCenter v50-appliance successfully created. Show Navigator for vCenter v50-appliance OK

The ESXi host will require additional hypervisor vNICs to support VMware vMotion, and NFS traffic uses the generic port-profile creation steps documented in section "Standard Operations" to establish a FEX-vMotion and FEX-NFS Port Profile.

Validate Setting in VMware vCenter

ſ

To validate the successful installation of the Cisco UCS Manager plug-in, follow these steps:

- **1.** Log in to the vCenter Server.
- 2. In the Main menu, choose Plug-ins > Manage Plug-ins.

The popup windows shows that the Cisco UCS Manager is already integrated in vCenter.

Plug-ir	Name	Vendor	Version	Status	Description	Progress	Error
Instal	ed Plug-ins						
3	VMware vCenter Storage Monitoring Service	VMware Inc.	5.1	Enabled	Storage Monitoring and		
					Reporting		
VCenter Service Status		VMware, Inc.	5.1	Enabled	Displays the health status of		
					vCenter services		
3	vCenter Hardware Status	VMware, Inc.	5.1	Enabled	Displays the hardware status of		
					hosts (CIM monitoring)		
3	Virtual Storage Console	NetApp, Inc.	4.1	Enabled	Virtual Storage Console for		
					VMware vSphere		
vaila	ble Plug-ins						
3	Cisco_Nexus_1000V_99499089	Cisco Systems, Inc.	1.0.0	No client side d			
3	Cisco_VN_Manager_1603529443	Cisco Systems, Inc.	1.0.0	No client side d			
3	Cisco-UCSM-r9-ucs-fi	Cisco Systems, Inc.	1.0.0	No client side d			
(Î)							li li
	1						
He	p						Close

Figure 140 Cisco UCS Manager Integrated in vCenter

3. Click Inventory > Networking to see FEX added to distributed switch from Cisco UCS Manager.

Figure 141	Verifying	FEX-DVS in	Cisco	UCS	Manage
------------	-----------	------------	-------	-----	--------



Standard Operations

The VM-FEX environment supports the addition of port profiles to the distributed switch. The following section describes how to add these distributed port groups.

Add Distributed Port Group to the VDS (vSphere Distributed Switch)

Port Profiles

Port profiles contain the properties and settings that you can use to configure virtual interfaces in Cisco UCS for VM-FEX. The port profiles are created and administered in Cisco UCS Manager. After a port profile is created, assigned to, and actively used by one or more distributed virtual switches (DVSs), any changes made to the networking properties of the port profile in Cisco UCS Manager are immediately applied to those DVSs.

In VMware vCenter, a port profile is represented as a port group. Cisco UCS Manager pushes the port profile names to VMware vCenter, which displays the names as port groups. None of the specific networking properties or settings in the port profile is visible in VMware vCenter. You must configure at least one port profile client for a port profile if you want Cisco UCS Manager to push the port profile to VMware vCenter.

Port Profile Client

The port profile client determines the DVSs to which a port profile is applied. By default, the port profile client specifies that the associated port profile applies to all DVSs in VMware vCenter. However, you can configure the client to apply the port profile to all DVSs in a specific data center or data center folder or to only one DVS.

Create a VM-FEX Port Profile

Follow these steps to create VM-FEX port profiles for use on the Cisco UCS distributed virtual switch.

- 1. Log in to Cisco UCS Manager.
- 2. Click the VM tab.
- 3. Right-click **Port Profile** > Create Port Profile.
- 4. Enter the name of the Port Profile.
- 5. (Optional) Enter a description.
- 6. (Optional) Choose a QoS policy.
- 7. (Optional) Choose a network control policy.
- **8.** Enter the maximum number of ports that can be associated with this port profile. The default is 64 ports.



Note The maximum number of ports that can be associated with a single DVS is 4096. If the DVS has only one associated port profile, that port profile can be configured with up to 4096 ports. However, if the DVS has more than one associated port profile, the total number of ports associated with all of those port profiles combined cannot exceed 4096.

9. (Optional) Choose High Performance.

Note Select None—Traffic to and from a virtual machine passes through the DVS.

Select High Performance— Traffic to and from a virtual machine bypasses the DVS and hypervisor and travels directly between the virtual machines and a virtual interface card (VIC) adapter.

- **10.** Choose the VLAN.
- **11**. Choose Native-VLAN.
- 12. Click OK.

🚖 Create Po	ort Profile			×
Create	Port Profile			0
Netv	Name: Description: QoS Policy: <not se<br="">work Control Policy: <not se<br="">Max Ports: 64 rk IO Performance: Pin Group: <not se<br="">Mame default Foobar 1_public MGMT-VLAN NFS-VLAN NFS-VLAN NFS-VLAN NFS-VLAN NFS-VLAN Native-VLAN Service-HA ServiceNodeServices VM-Traffic-VLAN vMotion-VLAN</not></not></not>	t>	ance Native VLAN O O O O O O O O O O O O O O O O O O O	
				OK Cancel

1

Figure 142 Creating Port Profile

Or
Create P	ort Profile Port Profi	le				× 0
Net Host Netwo	Name: Description: QoS Policy: work Control Policy: Max Ports: ork IO Performance: Pin Group:	FEX-Traffic-V <not set=""> <not set=""> 64 C None C H <not set=""></not></not></not>	LAN High Performance			
Select	1	Name	[Native VLAN	[]	
Г	default			0	A	
	Foobar 1_public			0		
	MGMT-VLAN			0		
	NFS-VLAN			C		
	Native-VLAN			0		
	Packet-Control-VLA	N		С		
	Service-HA			0		
	ServiceNodeService	s		0		
	VM-Traffic-VLAN			O		
	vMotion-VLAN			0		
					-	OK Cancel

Figure 143 Creating Port Profile with High Performance

The port profile created will appear in the working pane.

Create the Port Profile Client

ſ

To create the client profile for use in the Cisco UCS virtual distributed switch, follow these steps:

- 1. In the navigation pane under the VM tab, expand All > Port Profiles. Right-click the Port Profile and click Create Profile Client.
- 2. Choose the data center created in your vCenter Server, folder, and distributed virtual switch created in section "Integrate Cisco UCS with vCenter."
- 3. Click OK.

	Figure 144	Creating Profile Client		
🍙 Create Profile Client				
Create Profile	Client			
Name:				
Description:	4			
Datacenter:	All			
Folder:	All			
Distributed Virtual Switch:	Al			
			OK	Cance
	Or			
	Figure 145	Creating Profile Client for DVS-FEX		
🚔 Create Profile Client				
Create Profile	Client			(
Name:	FEX-Traffic-VLAN			
Description:				
Datacenter:	r9-dc-1			
Distributed Virtual Switch:	DVS-FEX			
Obtroated in tool Smith.	D			
		F		
			OK	Cancel

The client profile created will appear in your distributed virtual switch DVS-FEX in vCenter as a port group.

I

1

Repeat these steps as necessary for the workloads in the environment.

Migrate Networking Components for ESXi Hosts to Cisco DVS-FEX

vCenter Server VM

ſ

To migrate the networking components for the ESXi hosts to the Cisco FEX-DVS, follow these steps:

- 1. In the VMware vSphere client connected to vCenter, choose Home > Networking.
- 2. Expand the vCenter, DataCenter, and DVS-FEX folders. choose the DVS-FEX switch.
- 3. Under Basic Tasks for the vSphere distributed switch, choose Add a Host.
- 4. For both hosts, choose vmnic1 and choose the uplink-pg-DVS-FEX Uplink port group. Click Next.

Figure 146 Selecting Physical Adapters to Add to the Vsphere Distributed Switch

🚱 Add Host to vSphere Distributed Swi	itch				_ D ×
Select Hosts and Physical Adapters Select hosts and physical adapters t	to add to this v	/Sphere distributed switch			
Select Host and Physical Adapters				Settings	View Incompatible Hosts
Network Connectivity	Host/Physic	cal adapters	In use by switch	Settings	Uplink port group
Virtual Machine Networking	• 🗆 🗎	r9-infra-2.ridge9.com		View Details	
Ready to Complete	•	r9-infra-3.ridge9.com		View Details	
	• 🗆 🗎	r9-infra-4.ridge9.com		View Details	
	•	r9-infra-5.ridge9.com		View Details	
	• 🗆 🗎	r9-infra-6.ridge9.com		View Details	
		r9-infra-8.ridge9.com		View Details	
	Select	physical adapters			
		vmnic0	vSwitch0	View Details	uplink-pg-DVS-FEX
		vmnic1	vSwitch0	View Details	uplink-pg-DVS-FEX
Help				< Back N	lext > Cancel

5. For all VMkernel ports, choose the appropriate destination Port Group from the Cisco DVS-FEX. Click **Next**.

Figure 147 Selecting Destination Port Grou
--

Select port group to provide net	work connectivity for the adapters on	the vopnere distribution	ared switch.	-1			
elect Host and Physical Adapters letwork Connectivity intra Machine Networking	 Assign adapters to a destination port group to migrate them. Ctrl+click to multi-select. Virtual NICs marked with the warning sign might lose network connectivity unless they are migrated to the vSphere distributed switch. Select a destination port group in order to migrate them. 						
eady to Complete	Host/Virtual adapter	Switch	Source port group	Destination port group			
	□ R r9-infra-8.ridge9.com vmk0 vmk1 vmk2	vSwitch0 vSwitch0 vSwitch0	VMkernel-MGMT VMkernel-NFS VMkernel-vMotion	FEX-MGMT FEX-NFS FEX-vMotion			
	Virtual adapter details			Assign port group			

6. Check the Migrate Virtual Machine Networking check box. Expand each VM and choose the port groups for migration individually. Click **Next**.

1

Figure 148 Selecting Port Groups on Each VM to Migrate Individually

🛃 Add Host to vSphere Distributed Sw	itch	
Virtual Machine Networking Select virtual machines or network	idapters to migrate to the vSphere distributed switch.	
Select Host and Physical Adapters Network Connectivity Virtual Machine Networking Ready to Complete	Migrate virtual machine networking Assign VMs or network adapters to a destination por Host/Virtual machine/Network adapter NIC count icef1-b1.ice.rtp.netanp.com	t group to migrate them. Ctrl+click to multi-select. Source port group Destination port group
	icef1-vc Network adapter 1	Do not migrate IB-MGMT Network FEX-IB-MGMT
	Icer1-vcsql Metwork adapter 1 W2K8R2X64GPT-VM 1	Do not migrate IB-MGMT Network FEX-IB-MGMT Do not migrate
	Network adapter 1 icef1-h2.ice.rtp.netapp.com icef1-iscsi-rdm 1	IB-MGMT Network FEX-IB-MGMT Do not migrate
	Lean Network adapter 1	ID-Manii Network
	, Network adapter details	Assign port group
	Network adapter 1 MAC address: 00:50:56:a4:64:21 Adapter type: VMXNET 3 Port group: IB-MGMT Network	
Help		≤ Back Next ≥ Cancel

- 7. Click Finish. Wait for the migration process to complete.
- 8. In the vSphere Client window, choose Home > Hosts and Clusters.
- **9.** Choose the first ESXi host and click the **Configuration** tab. In the Hardware field, choose Networking.
- **10.** Make sure that vSphere Standard Switch is selected at the top next to View. vSwitch0 should not have any active VMkernel or VM Network ports on it. On the upper right of vSwitch0, click Remove.
- 11. Click Yes.
- **12.** After vSwitch0 has disappeared from the screen, click **vSphere Distributed Switch** at the top next to View.
- 13. Click Manage Physical Adapters.
- 14. In the uplink-pg-DVS-FEX field click Add NIC.
- **15.** Choose vmnic0 and click **OK**.
- 16. Click OK to close the Manage Physical Adapters window. Two uplinks should now be present.

- **17.** Choose the second ESXi host and click the Configuration tab. In the Hardware field, choose Networking.
- **18.** Make sure vSphere Standard Switch is selected at the top next to View. vSwitch0 should have no active VMkernel or VM Network ports on it. On the upper right of vSwitch0, click Remove.
- 19. Click Yes.
- 20. After vSwitch0 has disappeared from the screen, click vSphere Distributed Switch.
- 21. Click Manage Physical Adapters.
- 22. In the uplink-pg-DVS-FEX field click Add NIC.
- 23. Choose vmnic0 and click OK.
- 24. Click OK to close the Manage Physical Adapters window. Two uplinks should now be present.

VM-FEX Virtual Interfaces

In a blade server environment, the number of vNICs and vHBAs configurable for a service profile is determined by adapter capability and the amount of virtual interface (VIF) namespace available in the adapter. In Cisco UCS, portions of VIF namespace are allotted in chunks called VIFs. Depending on your hardware, the maximum number of VIFs is allocated on a predefined, per-port basis.

The maximum number of VIFs varies based on hardware capability and port connectivity. For each configured vNIC or vHBA, one or two VIFs are allocated. Standalone vNICs and vHBAs use one VIF, and failover vNICs and vHBAs use two.

The following variables affect the number of VIFs available to a blade server, and therefore, the number of vNICs and vHBAs you can configure for a service profile.

- The maximum number of VIFs supported on your fabric interconnect
- How the fabric interconnects are cabled
- If the fabric interconnect and IOM are configured in fabric port channel mode

For more information about the maximum number of VIFs supported by your hardware configuration, refer to the Cisco UCS 6100 and 6200 Series Configuration Limits for Cisco UCS Manager for your software release. Table 23 and Table 24 reference these limits.

Table 23 VM-FEX Environment Configuration Limits

Feature	Cisco UCS 6200 Series Fabric Interconnect
Host per DVS	52
DVSs per Cisco UCS Domain	1
vCenter Server units per Cisco UCS Domain	4
Port profiles per Cisco UCS Domain	512
Dynamic ports per port profile	4096
Dynamic ports per DVS	4096

Acknowledge Link Between FEX and Fl	Maximum VIFs (vNICs+vHBAs) per VIC Adapter in Single-Wire Management	Maximum VIFs (vNICs+vHBAs) per VIC Adapter in Dual-Wire Management
1	12	13
2	27	28
4	57	58
8	117	118

Table 24 Cisco UCS Fabric Interconnect and Cisco UCS C-Series Server VIF Support



- For a non-VIC adapter the maximum number of vNICs is two and the maximum number of vHBAs is two.
- If the server in single-wire mode has two VIC adapters, the maximum number of VIFs (vNICs + vHBAs) available for the second adapter would be same as for an adapter in a dual-wire mode server.
- For more information on Cisco UCS C-Series Server integration into UCSM, see: http://www.cisco.com/en/US/docs/unified_computing/ucs/c-series_integration/ucsm2.1/b_UCSM2 -1_C-Integration.pdf

Cisco Nexus 5548 Example Configurations

Cisco Nexus 5548 A

```
!Command: show running-config
!Time: Mon Feb 25 18:52:54 2013
version 5.2(1)N1(3)
feature fcoe
switchname icef1-sw1
feature npiv
no feature telnet
cfs eth distribute
feature lacp
feature vpc
feature lldp
username admin password 5 $1$bzvqy03B$xPzr5b6TKfwPE2vWVj25A/ role network-admin
banner motd #Nexus 5000 Switch
ip domain-lookup
class-map type qos class-fcoe
class-map type queuing class-fcoe
 match gos-group 1
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
 match qos-group 2
class-map type network-qos class-fcoe
 match qos-group 1
class-map type network-qos class-all-flood
```

```
match qos-group 2
class-map type network-qos class-ip-multicast
 match gos-group 2
policy-map type network-qos jumbo
  class type network-qos class-fcoe
   pause no-drop
   mtu 2158
  class type network-qos class-default
   mtu 9216
   multicast-optimize
system qos
  service-policy type queuing input fcoe-default-in-policy
  service-policy type queuing output fcoe-default-out-policy
  service-policy type gos input fcoe-default-in-policy
  service-policy type network-qos jumbo
snmp-server user admin network-admin auth md5 0x9f7f45ac8ee14ff3cf5e72e22bb95942 priv
0x9f7f45ac8ee14ff3cf5e72e22bb95942 localizedkey
ntp server 192.168.171.4 use-vrf management
vrf context management
  ip route 0.0.0.0/0 192.168.171.1
vlan 1
vlan 2
 name Native-VLAN
vlan 101
  fcoe vsan 101
  name FCoE_Fabric_A
vlan 3170
  name NFS-VLAN
vlan 3173
  name vMotion-VLAN
vlan 3174
 name VM-Traffic-VLAN
vlan 3175
 name IB-MGMT-VLAN
vlan 3176
 name Packet-Control-VLAN
spanning-tree port type edge bpduguard default
spanning-tree port type network default
port-channel load-balance ethernet source-dest-port
vpc domain 23
  role priority 10
 peer-keepalive destination 192.168.171.70 source 192.168.171.69
  auto-recoverv
port-profile default max-ports 512
vsan database
  vsan 101 name "Fabric_A"
device-alias database
  device-alias name icef1-st1a_1a pwwn 50:0a:09:81:9d:02:4c:1a
  device-alias name icef1-st1a_1a pwwn 50:0a:09:81:8d:02:4c:1a
  device-alias name VM-Host-Infra-01_A pwwn 20:00:00:25:b5:01:0a:0f
  device-alias name VM-Host-Infra-02_A pwwn 20:00:00:25:b5:01:0a:1f
device-alias commit
fcdomain fcid database
  vsan 101 wwn 50:0a:09:81:88:12:85:b3 fcid 0x550000 dynamic
  vsan 101 wwn 50:0a:09:81:9d:02:4c:1a fcid 0x550001 dynamic
Т
               [icef1-st1a_1a]
  vsan 101 wwn 50:0a:09:81:88:22:87:76 fcid 0x550020 dynamic
  vsan 101 wwn 50:0a:09:81:8d:02:4c:1a fcid 0x550021 dynamic
1
               [icef1-st1b:1a]
  vsan 101 wwn 22:ca:54:7f:ee:23:52:7f fcid 0x550040 dynamic
  vsan 101 wwn 20:00:00:25:b5:01:0a:0f fcid 0x550041 dynamic
Т
               [VM-Host-Infra-01_A]
```

```
vsan 101 wwn 20:00:00:25:b5:01:0a:1f fcid 0x550042 dynamic
!
              [VM-Host-Infra-02_A]
interface port-channel10
  description vPC peer-link
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3170,3173-3176
  spanning-tree port type network
  vpc peer-link
interface port-channel11
  description icef1-st1a
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 101,3170
  spanning-tree port type edge trunk
  vpc 11
interface port-channel12
  description icef1-st1b
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 101,3170
  spanning-tree port type edge trunk
  vpc 12
interface port-channel13
  description icef1-uc1-A
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3170,3173-3175
  spanning-tree port type edge trunk
  vpc 13
interface port-channel14
  description icef1-uc1-B
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3170,3173-3175
  spanning-tree port type edge trunk
  vpc 14
interface port-channel15
  description icef1-uc1-A:FCoE
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 101
  spanning-tree port type edge trunk
interface port-channel20
  description icecore Uplink
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3175
  spanning-tree port type network
  vpc 20
interface vfc11
  bind interface Ethernet1/1
  switchport trunk allowed vsan 101
  switchport description icef1-st1a:1a
 no shutdown
```

```
interface vfc12
 bind interface Ethernet1/2
  switchport trunk allowed vsan 101
  switchport description icef1-st1b:1a
 no shutdown
interface vfc15
 bind interface port-channel15
  switchport trunk allowed vsan 101
  switchport description icef1-uc1-A:FCoE
 no shutdown
vsan database
  vsan 101 interface vfc11
  vsan 101 interface vfc12
 vsan 101 interface vfc15
interface Ethernet1/1
  description icef1-st1a:e1a
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 101,3170
  channel-group 11 mode active
interface Ethernet1/2
  description icef1-st1b:e1b
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 101,3170
  channel-group 12 mode active
interface Ethernet1/3
interface Ethernet1/4
interface Ethernet1/5
interface Ethernet1/6
interface Ethernet1/7
interface Ethernet1/8
interface Ethernet1/9
interface Ethernet1/10
interface Ethernet1/11
 description icef1-uc1-A:1/19
 switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3170,3173-3175
  channel-group 13 mode active
interface Ethernet1/12
  description icef1-uc1-B:1/19
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3170,3173-3175
  channel-group 14 mode active
interface Ethernet1/13
  description icef1-sw2:1/13
  switchport mode trunk
```

VMware vSphere 5.1 on FlexPod Data ONTAP Operating in 7-Mode Deployment Guide

I

```
switchport trunk native vlan 2
  switchport trunk allowed vlan 3170,3173-3176
  channel-group 10 mode active
interface Ethernet1/14
  description icef1-sw2:1/14
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3170,3173-3176
  channel-group 10 mode active
interface Ethernet1/15
  description icef1-1110x-1:Eth1
  switchport mode trunk
  switchport trunk allowed vlan 3175-3176
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet1/16
  description icef1-1110x-2:Eth1
  switchport mode trunk
  switchport trunk allowed vlan 3175-3176
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet1/17
interface Ethernet1/18
interface Ethernet1/19
interface Ethernet1/20
 description icecore:Eth1/7 Uplink
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3175
  spanning-tree port type network
  channel-group 20 mode active
interface Ethernet1/21
interface Ethernet1/22
interface Ethernet1/23
interface Ethernet1/24
interface Ethernet1/25
interface Ethernet1/26
interface Ethernet1/27
interface Ethernet1/28
interface Ethernet1/29
interface Ethernet1/30
interface Ethernet1/31
  description icef1-uc1-A:1/31
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 101
```

```
channel-group 15 mode active
interface Ethernet1/32
 description icef1-uc1-A:1/32
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 101
  channel-group 15 mode active
interface mgmt0
  ip address 192.168.171.69/24
line console
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.5.2.1.N1.3.bin
boot system bootflash:/n5000-uk9.5.2.1.N1.3.bin
!Full Zone Database Section for vsan 101
zone name VM-Host-Infra-01_A vsan 101
   member pwwn 20:00:00:25:b5:01:0a:0f
                [VM-Host-Infra-01_A]
1
   member pwwn 50:0a:09:81:9d:02:4c:1a
1
                [icef1-st1a_1a]
   member pwwn 50:0a:09:81:8d:02:4c:1a
!
                [icef1-st1b_1a]
zone name VM-Host-Infra-02_A vsan 101
   member pwwn 20:00:00:25:b5:01:0a:1f
                [VM-Host-Infra-02_A]
1
   member pwwn 50:0a:09:81:9d:02:4c:1a
                [icef1-st1a_1a]
ļ
   member pwwn 50:0a:09:81:8d:02:4c:1a
                [icef1-st1b_1a]
1
zoneset name FlexPod vsan 101
   member VM-Host-Infra-01_A
   member VM-Host-Infra-02_A
zoneset activate name FlexPod vsan 101
```

Cisco Nexus 5548 B

```
!Command: show running-config
!Time: Mon Feb 25 18:54:02 2013
version 5.2(1)N1(3)
feature fcoe
switchname icef1-sw2
feature npiv
no feature telnet
cfs eth distribute
feature lacp
feature vpc
feature lldp
username admin password 5 $1$uCGfL31v$UuLHg53DEK3VvDGkbjUGb1 role network-admin
banner motd #Nexus 5000 Switch
#
ip domain-lookup
class-map type qos class-fcoe
class-map type queuing class-fcoe
 match qos-group 1
class-map type queuing class-all-flood
```

```
match qos-group 2
class-map type queuing class-ip-multicast
 match gos-group 2
class-map type network-qos class-fcoe
 match qos-group 1
class-map type network-qos class-all-flood
 match qos-group 2
class-map type network-qos class-ip-multicast
 match qos-group 2
policy-map type network-qos jumbo
  class type network-qos class-fcoe
   pause no-drop
   mtu 2158
  class type network-gos class-default
   mtu 9216
   multicast-optimize
system qos
  service-policy type queuing input fcoe-default-in-policy
  service-policy type queuing output fcoe-default-out-policy
  service-policy type qos input fcoe-default-in-policy
  service-policy type network-qos jumbo
snmp-server user admin network-admin auth md5 0x2bd90b73090e2a5ffe4b35ead5f6e070 priv
0x2bd90b73090e2a5ffe4b35ead5f6e070 localizedkey
ntp server 192.168.171.4 use-vrf management
vrf context management
  ip route 0.0.0.0/0 192.168.171.1
vlan 1
vlan 2
  name Native-VLAN
vlan 102
  fcoe vsan 102
 name FCoE Fabric B
vlan 3170
 name NFS-VLAN
vlan 3173
 name vMotion-VLAN
vlan 3174
 name VM-Traffic-VLAN
vlan 3175
 name IB-MGMT-VLAN
vlan 3176
 name Packet-Control-VLAN
spanning-tree port type edge bpduguard default
spanning-tree port type network default
port-channel load-balance ethernet source-dest-port
vpc domain 23
  role priority 20
  peer-keepalive destination 192.168.171.69 source 192.168.171.70
 auto-recoverv
port-profile default max-ports 512
vsan database
  vsan 102 name "Fabric_B"
device-alias database
  device-alias name icef1-st1a_1b pwwn 50:0a:09:82:9d:02:4c:1a
  device-alias name icef1-st1b_1b pwwn 50:0a:09:82:8d:02:4c:1a
  device-alias name VM-Host-Infra-01_B pwwn 20:00:25:b5:01:0b:0f
  device-alias name VM-Host-Infra-02_B pwwn 20:00:00:25:b5:01:0b:1f
device-alias commit
fcdomain fcid database
  vsan 102 wwn 50:0a:09:83:88:22:87:76 fcid 0x3f0000 dynamic
  vsan 102 wwn 50:0a:09:82:9d:02:4c:1a fcid 0x3f0001 dynamic
I.
               [icef1-st1a_1b]
```

```
vsan 102 wwn 50:0a:09:83:88:12:85:b3 fcid 0x3f0020 dynamic
 vsan 102 wwn 50:0a:09:82:8d:02:4c:1a fcid 0x3f0021 dynamic
Т
               [icef1-st1b_1b]
 vsan 102 wwn 22:cb:54:7f:ee:23:8b:3f fcid 0x3f0040 dynamic
  vsan 102 wwn 20:00:00:25:b5:01:0b:1f fcid 0x3f0041 dynamic
              [VM-Host-Infra-02_B]
1
 vsan 102 wwn 20:00:00:25:b5:01:0b:0f fcid 0x3f0042 dynamic
              [VM-Host-Infra-01_B]
1
interface port-channel10
  description vPC peer-link
 switchport mode trunk
 switchport trunk native vlan 2
  switchport trunk allowed vlan 3170,3173-3176
  spanning-tree port type network
  vpc peer-link
interface port-channel11
  description icef1-st1a
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 102,3170
  spanning-tree port type edge trunk
  vpc 11
interface port-channel12
  description icef1-st1b
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 102,3170
  spanning-tree port type edge trunk
  vpc 12
interface port-channel13
  description icef1-uc1-A
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3170,3173-3175
  spanning-tree port type edge trunk
  vpc 13
interface port-channel14
  description icef1-uc1-B
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3170,3173-3175
  spanning-tree port type edge trunk
  vpc 14
interface port-channel15
  description icef1-uc1-B:FCoE
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 102
  spanning-tree port type edge trunk
interface port-channel20
  description icecore Uplink
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3175
  spanning-tree port type network
  vpc 20
```

```
interface vfc11
 bind interface Ethernet1/1
  switchport trunk allowed vsan 102
  switchport description icef1-st1a:1b
 no shutdown
interface vfc12
  bind interface Ethernet1/2
  switchport trunk allowed vsan 102
  switchport description icef1-st1b:1b
 no shutdown
interface vfc15
 bind interface port-channel15
  switchport trunk allowed vsan 102
  switchport description icef1-uc1-B:FCoE
 no shutdown
vsan database
  vsan 102 interface vfc11
  vsan 102 interface vfc12
 vsan 102 interface vfc15
interface Ethernet1/1
  description icef1-st1a:e1b
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 102,3170
  channel-group 11 mode active
interface Ethernet1/2
  description icef1-st1b:e1b
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 102,3170
  channel-group 12 mode active
interface Ethernet1/3
interface Ethernet1/4
interface Ethernet1/5
interface Ethernet1/6
interface Ethernet1/7
interface Ethernet1/8
interface Ethernet1/9
interface Ethernet1/10
interface Ethernet1/11
  description icef1-uc1-A:1/20
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3170,3173-3175
  channel-group 13 mode active
interface Ethernet1/12
  description icef1-uc1-B:1/20
  switchport mode trunk
  switchport trunk native vlan 2
```

```
switchport trunk allowed vlan 3170,3173-3175
  channel-group 14 mode active
interface Ethernet1/13
  description icef1-sw1:1/13
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3170,3173-3176
  channel-group 10 mode active
interface Ethernet1/14
  description icef1-sw1:1/14
 switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3170,3173-3176
 channel-group 10 mode active
interface Ethernet1/15
  description icef1-1110x-1:Eth2
  switchport mode trunk
  switchport trunk allowed vlan 3175-3176
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet1/16
  description icef1-1110x-2:Eth2
  switchport mode trunk
  switchport trunk allowed vlan 3175-3176
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet1/17
interface Ethernet1/18
interface Ethernet1/19
interface Ethernet1/20
 description icecore:Eth1/8 Uplink
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3175
  spanning-tree port type network
  channel-group 20 mode active
interface Ethernet1/21
interface Ethernet1/22
interface Ethernet1/23
interface Ethernet1/24
interface Ethernet1/25
interface Ethernet1/26
interface Ethernet1/27
interface Ethernet1/28
interface Ethernet1/29
interface Ethernet1/30
```

VMware vSphere 5.1 on FlexPod Data ONTAP Operating in 7-Mode Deployment Guide

```
interface Ethernet1/31
  description icef1-uc1-B:1/31
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 102
  channel-group 15 mode active
interface Ethernet1/32
  description icef1-uc1-B:1/32
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 102
  channel-group 15 mode active
interface mgmt0
  ip address 192.168.171.70/24
line console
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.5.2.1.N1.3.bin
boot system bootflash:/n5000-uk9.5.2.1.N1.3.bin
!Full Zone Database Section for vsan 102
zone name VM-Host-Infra-01_B vsan 102
   member pwwn 20:00:00:25:b5:01:0b:0f
I.
                [VM-Host-Infra-01_B]
   member pwwn 50:0a:09:82:9d:02:4c:1a
                [icef1-st1a_1b]
!
   member pwwn 50:0a:09:82:8d:02:4c:1a
                [icef1-st1b_1b]
!
zone name VM-Host-Infra-02_B vsan 102
   member pwwn 20:00:00:25:b5:01:0b:1f
1
                [VM-Host-Infra-02_B]
    member pwwn 50:0a:09:82:9d:02:4c:1a
!
               [icef1-st1a_1b]
   member pwwn 50:0a:09:82:8d:02:4c:1a
!
                [icef1-st1b_1b]
zoneset name FlexPod vsan 102
   member VM-Host-Infra-01 B
   member VM-Host-Infra-02_B
zoneset activate name FlexPod vsan 102
```