



FlexPod Datacenter with VMware vSphere 5.5 Update 2 and Cisco Nexus 9000 Application Centric Infrastructure (ACI)

Deployment Guide for FlexPod Datacenter with VMware vSphere 5.5 Update 2 and Cisco Nexus 9000 Application Centric Infrastructure (ACI)

Last Updated: August 10, 2015



Building Architectures to Solve Business Problems



About the Authors

Haseeb Niazi, Technical Marketing Engineer, Cisco UCS Data Center Solutions Engineering, Cisco Systems Inc.

Haseeb has over 15 years of experience at Cisco dealing in Data Center, Security, WAN Optimization, and related technologies. As a member of various solution teams and advanced services, Haseeb has helped many enterprise and service provider customers evaluate and deploy a wide range of Cisco solutions. Haseeb holds a master's degree in Computer Engineering from the University of Southern California.

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

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, Chris was an application developer and has worked in the IT industry for more than 15 years.

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

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.

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

Lindsey Street is a Solutions 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 Masters of Science in Information Security from East Carolina University.

Acknowledgments

For their support and contribution to the design, validation, and creation of this Cisco Validated Design, the authors would like to thank:

- Ranga Rao, Cisco Systems, Inc.
- Ramon Martinez, Cisco Systems, Inc.
- Chris Reno, NetApp

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 (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS 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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, Media-Tone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0809R)

© 2015 Cisco Systems, Inc. All rights reserved



FlexPod Datacenter with VMware vSphere 5.5 Update 2 and Cisco Nexus 9000 Application Centric Infrastructure (ACI)

About this Document

Cisco® Validated Designs include systems and solutions that are designed, tested, and documented to facilitate and improve customer deployments. These designs incorporate a wide range of technologies and products into a portfolio of solutions that have been developed to address the business needs of customers. 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. A FlexPod solution is a validated approach for deploying Cisco and NetApp technologies as a shared cloud infrastructure.

This document describes the Cisco and NetApp® VMware vSphere® 5.5 Update 2 on FlexPod® solution with Cisco Application Centric Infrastructure (ACI). Cisco ACI is a holistic architecture that introduces hardware and software innovations built upon the new Cisco Nexus® 9000 Series product line.

Audience

The audience of this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineers, and customers who want to take advantage of an infrastructure that is built to deliver IT efficiency and enable IT innovation.

Architecture

FlexPod is a defined set of hardware and software that serves as an integrated foundation for both virtualized and non-virtualized solutions. VMware vSphere® built on FlexPod includes NetApp storage, NetApp Data ONTAP, Cisco Nexus® networking, the Cisco Unified Computing System™ (Cisco UCS®), and VMware vSphere software in a single package. The design is flexible enough that the



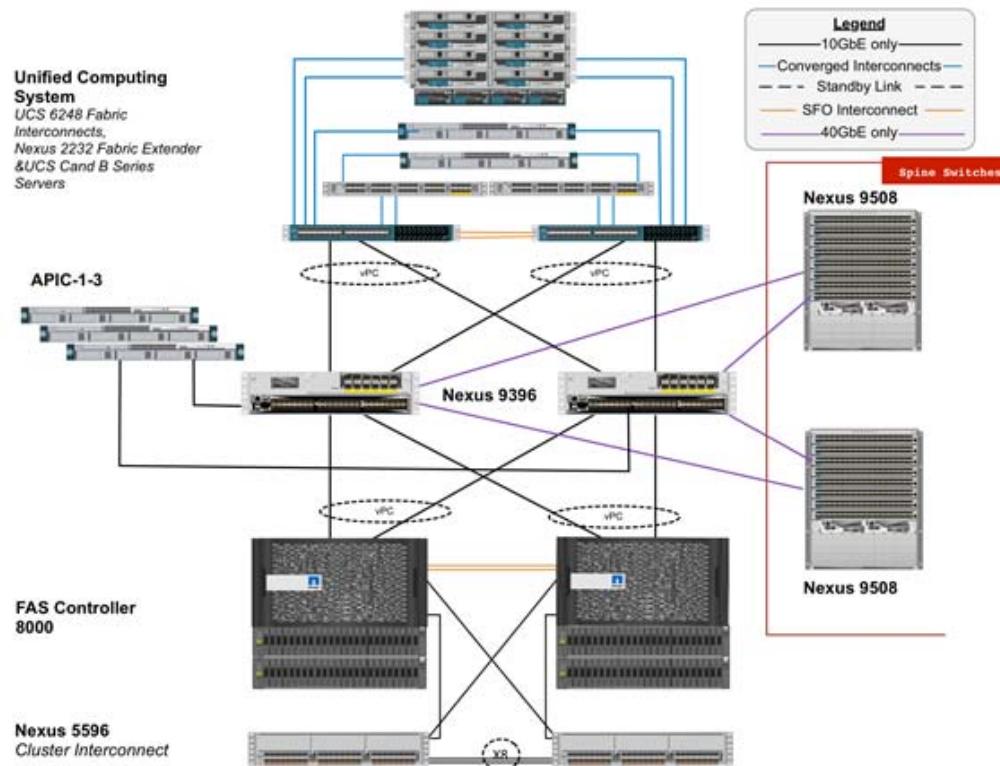
networking, computing, and storage can fit in one data center rack or be deployed according to a customer's data center design. Port density enables the networking components to accommodate multiple configurations of this kind.

One benefit of the FlexPod architecture is the ability to customize or "flex" the environment to suit a customer's requirements. A FlexPod 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). The reference architecture detailed in this document highlights the resiliency, cost benefit, and ease of deployment of an IP-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 IP-based storage. This design uses the Cisco Nexus 9000, Cisco Nexus 2232PP FEX, and Cisco UCS C-Series and B-Series servers and the NetApp FAS family of storage controllers connected in a highly available modular design. This infrastructure is deployed to provide iSCSI-booted hosts with file-level and block-level access to shared storage. The reference architecture reinforces the "wire-once" strategy, because as additional storage is added to the architecture, no re-cabling is required from the hosts to the Cisco UCS fabric interconnect.

The ACI switching architecture is laid out in a leaf-and-spine topology where every leaf connects to every spine using 40G Ethernet interface(s). The software controller, APIC, is delivered as an appliance and three or more such appliances form a cluster for high availability and enhanced performance.

Figure 1 *FlexPod Design with Cisco ACI and NetApp Data ONTAP*



The reference hardware configuration includes:

- Two Cisco Nexus 9396 switches

- Two Cisco Nexus 2232 fabric extenders
- Two Cisco UCS 6248UP fabric interconnects
- One NetApp FAS8040 (HA pair) running clustered Data ONTAP with Disk shelves

While not included in the FlexPod BOM, Cisco ACI spines and APIC controllers are integral part of Cisco ACI design. The following components were used in the validation efforts:

- Three APIC Controllers
- Two Cisco Nexus 9508 based spines

For server virtualization, the deployment includes VMware vSphere. Although this is the base design, each of the components can be scaled easily 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 capability and throughput, and special hardware or software features can be added to introduce new features.

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 network, compute and storage device configurations.

Software Revisions

[Table 1](#) details the software revisions used for validating various components of the Cisco Nexus 9000 based FlexPod architecture.

Table 1 Software Revisions

Layer	Device	Version or Release	Details
Compute	Cisco UCS Fabric Interconnects 6200 Series, UCS B-200 M3/M4, UCS C-220 M3	2.2(3d)	Includes the Cisco UCS-IOM 2208XP, Cisco UCS Manager, UCS VIC 1240, and UCS VIC 1340
	Cisco eNIC	2.1.2.42	
	Cisco fNIC	1.6.0.5	
Network	Cisco APIC	1.0(3k)*	
	Cisco Nexus 9000 iNX-OS	11.0(3k)	
Storage	NetApp FAS 8040	Data ONTAP 8.2.3	
	Nexus 5596 Cluster Switches	5.2(1)N1(1)	
Software	VMware vSphere ESXi	5.5u2**	
	VMware vCenter	5.5u2	
	OnCommand Unified Manager for clustered Data ONTAP	6.1	
	NetApp Virtual Storage Console (VSC)	5.0	

* Customers should always use the latest ACI software after consulting with their account team. The APIC screen captures in this Deployment Guide were captured in version 1.0(1e) and might be slightly different.

**Please consult the [Appendix D - Deploying VMware vSphere 5.1 Update 1](#) for the VMware 5.1 installation.

Configuration Guidelines

This document provides details for configuring a fully redundant, highly available configuration for a FlexPod unit with clustered Data ONTAP storage. Therefore, reference is made to which component is being configured with each step, either 01 or 02 or A and B. For example, node01 and node02 are used to identify the two NetApp storage controllers that are provisioned with this document, and Cisco Nexus A or Cisco Nexus B identifies the pair of Cisco Nexus switches that are configured. The Cisco UCS fabric interconnects are similarly configured. Additionally, this document details the 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 network port vlan create command:

Usage:

```
network port vlan create ?
  [-node] <nodename>                               Node
  { [-vlan-name] {<netport>|<ifgrp>}           VLAN Name
    | -port {<netport>|<ifgrp>}                 Associated Network Port
  [-vlan-id] <integer> }                           Network Switch VLAN Identifier
```

Example:

```
network port vlan -node <node01> -vlan-name i0a-<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 3 lists the virtual machines (VMs) necessary for deployment as outlined in this guide. [Table 2](#) describe the VLANs necessary for deployment as outlined in this guide.

Table 2 Necessary VLANs

VLAN Name	VLAN Purpose	ID Used in Validating This Document
Out of band Mgmt.	VLAN for out-of-band management interfaces	3177
Native	VLAN to which untagged frames are assigned	2
NFS LIF	VLAN for NFS LIF (NetApp) traffic	3170
NFS VMK	VLAN for NFS VMkernel (Infrastructure ESXi hosts) traffic	3270
iSCSI-A LIF	VLAN for Fabric A iSCSI LIF	901
iSCSI-B LIF	VLAN for Fabric B iSCSI LIF	902
iSCSI-A VMK	VLAN for Fabric A iSCSI VMKernel Port	911
iSCSI-B VMK	VLAN for Fabric B iSCSI VMKernel Port	912
Tenant Traffic	VLAN Range defined for ACI	1101-1200

[Table 3](#) lists the virtual machines (VMs) necessary for deployment as outlined in this document.

Table 3 Created VMware Virtual Machines

Virtual Machine Description	Host Name
Active Directory	
vCenter SQL Server database	
vCenter Server	
NetApp Virtual Storage Console (VSC) and NetApp OnCommand core	

Table 4 lists the configuration variables that are used throughout this document. This table can be completed based on the specific site variables and used in implementing the document configuration steps.

Table 4 Configuration Variables

Variable	Description
<<var_node01_mgmt_ip>>	Out-of-band management IP for cluster node 01
<<var_node01_mgmt_mask>>	Out-of-band management network netmask
<<var_node01_mgmt_gateway>>	Out-of-band management network default gateway
<<var_url_boot_software>>	Data ONTAP 8.2 URL; format: http://
<<var_node02_mgmt_ip>>	Out-of-band management IP for cluster node 02
<<var_node02_mgmt_mask>>	Out-of-band management network netmask
<<var_node02_mgmt_gateway>>	Out-of-band management network default gateway
<<var_clustername>>	Storage cluster host name
<<var_cluster_base_license_key>>	Cluster base license key
<<var_nfs_license>>	NFS license key
<<var_iscsi_license>>	iSCSI license key
<<var_password>>	Global default administrative password
<<var_clustermgmt_ip>>	In-band management IP for the storage cluster
<<var_clustermgmt_mask>>	Out-of-band management network netmask
<<var_clustermgmt_gateway>>	Out-of-band management network default gateway
<<var_dns_domain_name>>	DNS domain name
<<var_nameserver_ip>>	DNS server IP(s)
<<var_node_location>>	Node location string for each node
<<var_node01_sp_ip>>	Out-of-band cluster node 01 service processor management IP
<<var_node01_sp_mask>>	Out-of-band management network netmask
<<var_node01_sp_gateway>>	Out-of-band management network default gateway
<<var_node02_sp_ip>>	Out-of-band cluster node 02 device processor management IP
<<var_node02_sp_mask>>	Out-of-band management network netmask
<<var_node02_sp_gateway>>	Out-of-band management network default gateway
<<var_node01>>	Cluster node 01 hostname
<<var_node02>>	Cluster node 02 hostname
<<var_num_disks>>	Number of disks to assign to each storage controller
<<var_nfs_vlan_id>>	Infrastructure NFS VLAN ID for LIF
<<var_nfs_vlan_tenant>>	Tenant NFS VLAN ID for LIF (only required when deploying a tenant)

<<var_iscsi_vlan_A_id>>	Infrastructure iSCSI-A VLAN ID for LIF
<<var_iscsi_vlan_B_id>>	Infrastructure iSCSI-B VLAN ID for LIF
<<var_iscsi_vlan_A_tenant>>	Tenant iSCSI-A VLAN ID for LIF (optional)
<<var_iscsi_vlan_B_tenant>>	Tenant iSCSI-B VLAN ID for LIF (optional)
<<var_nfs_vlan_vmk>>	Infrastructure NFS VLAN ID for VMkernel Port
<<var_iscsi_vlan_A_vmk>>	Infrastructure iSCSI-A VLAN ID for VMkernel Port
<<var_iscsi_vlan_B_vmk>>	Infrastructure iSCSI-B VLAN ID for VMkernel Port
<<var_ib_mgmt_vlan_id>>	In-band management network VLAN ID
<<var_oob_mgmt_vlan_id>>	Out-of-band management network VLAN ID
<<var_timezone>>	FlexPod time zone (for example, America/New_York)
<<var_global_ntp_server_ip>>	NTP server IP address
<<var_snmp_contact>>	Administrator e-mail address
<<var_snmp_location>>	Cluster location string
<<var_oncommand_server_fqdn>>	VSC or OnCommand virtual machine fully qualified domain name (FQDN)
<<var_snmp_community>>	Storage cluster SNMP v1/v2 community name
<<var_mailhost>>	Mail server host name
<<var_storage_admin_email>>	Administrator e-mail address
<<var_esxi_host1_nfs_ip>>	NFS VLAN IP address for VMware ESXi host 1
<<var_esxi_host2_nfs_ip>>	NFS VLAN IP address for VMware ESXi host 2
<<var_node01_nfs_lif_infra_swap_ip>>	IP address of Infra Swap
<<var_node01_nfs_lif_infra_swap_mask>>	Subnet Mask of Infra Swap
<<var_node02_nfs_lif_infra_datastore_1_ip>>	IP address of Datastore 1
<<var_node02_nfs_lif_infra_datastore_1_mask>>	Subnet mask of Datastore 1
<<var_vserver_mgmt_ip>>	Management IP address for Vserver
<<var_vserver_mgmt_mask>>	Subnet mask for Vserver
<<var_routing_group>>	Routing group for Vserver
<<var_vserver_mgmt_gateway>>	Default Gateway for Vserver
<<var_vsadmin_password>>	Password for VS admin account
<<var_ucs_clustername>>	Cisco UCS Manager cluster host name
<<var_ucsa_mgmt_ip>>	Cisco UCS fabric interconnect (FI) A out-of-band management IP address
<<var_ucsa_mgmt_mask>>	Out-of-band management network netmask
<<var_ucsa_mgmt_gateway>>	Out-of-band management network default gateway

<<var_ucs_cluster_ip>>	Cisco UCS Manager cluster IP address
<<var_ucs_b_mgmt_ip>>	Cisco UCS FI B out-of-band management IP address
<<var_vm_host_infra_01_iqn>>	IQN of Infra 01
<<var_vm_host_infra_02_iqn>>	IQN of Infra 02
<<var_vm_host_infra_01_ip>>	VMware ESXi host 01 out-of-band management IP
<<var_vm_host_infra_02_ip>>	VMware ESXi host 02 out-of-band management IP
<<var_nfs_vlan_ip_host_01>>	ESXi host 1, NFS VLAN IP
<<var_nfs_vlan_ip_mask_host_01>>	ESXi host1, NFS VLAN subnet mask
<<var_nfs_vlan_ip_host_02>>	ESXi host 2, NFS VLAN IP
<<var_nfs_vlan_ip_mask_host_02>>	ESXi host2, NFS VLAN subnet mask
<<var_vcenter_server_ip>>	IP address of the vCenter Server
<<var_svm_mgmt_vlan_id>>	Infrastructure Vserver management VLAN ID
<<var_svm_mgmt_vlan_tenant>>	Tenant Vserver management VLAN ID
<<var_nfs_subnet_address>>	NFS subnet address
<<var_node02_nfs_lif_tenant_datastore_1_ip>>	Tenant Datastore 1 IP address
<<var_node02_nfs_lif_tenant_datastore_1_mask>>	Tenant Datastore 1 Subnet mask
<<var_node01_iscsi_lif01a_ip>>	iSCSI LIF 01a IP address
<<var_node01_iscsi_lif01a_mask>>	iSCSI LIF 01a subnet mask
<<var_node01_iscsi_lif01b_ip>>	iSCSI LIF 01b IP address
<<var_node01_iscsi_lif01b_mask>>	iSCSI LIF 01b subnet mask
<<var_node01_iscsi_lif02a_ip>>	iSCSI LIF 02a IP address
<<var_node01_iscsi_lif02a_mask>>	iSCSI LIF 02a subnet mask
<<var_node01_iscsi_lif02b_ip>>	iSCSI LIF 02b IP address
<<var_node01_iscsi_lif02b_mask>>	iSCSI LIF 02b subnet mask
<<var_node01_iscsi_tenant_lif01a_ip>>	Tenant iSCSI LIF 01a IP address
<<var_node01_iscsi_tenant_lif01a_mask>>	Tenant iSCSI LIF 01a subnet mask
<<var_node01_iscsi_tenant_lif01b_ip>>	Tenant iSCSI LIF 01b IP address
<<var_node01_iscsi_tenant_lif01b_mask>>	Tenant iSCSI LIF 01b subnet mask
<<var_node01_iscsi_tenant_lif02a_ip>>	Tenant iSCSI LIF 02a IP address
<<var_node01_iscsi_tenant_lif02a_mask>>	Tenant iSCSI LIF 02a subnet mask
<<var_node01_iscsi_tenant_lif02b_ip>>	Tenant iSCSI LIF 02b IP address
<<var_node01_iscsi_tenant_lif02b_mask>>	Tenant iSCSI LIF 02b subnet mask
<<var_vserver_mgmt_ip>>	Management IP address for Infrastructure Vserver
<<var_vserver_mgmt_mask>>	Management subnet mask for Infrastructure Vserver

<<var_vserver_tenant_mgmt_ip>>	Management IP address for Tenant Vserver
<<var_vserver_tenant_mgmt_mask>>	Management subnet mask for Tenant Vserver
<<var_vserver_mgmt_gateway>>	Management Gateway for Infrastructure Vserver
<<var_vserver_tenant_mgmt_gateway>>	Management Gateway for Tenant Vserver
<<var_oncommand_server_ip>>	IP address of the OnCommand Unified Manager
<<var_rule_index>>	Rule index number
<<var_vm_host_infra_01_A_wwpn>>	WWPN of Infra Datastore 01 A
<<var_vm_host_infra_01_B_wwpn>>	WWPN of Infra Datastore 01 B
<<var_vm_host_infra_02_A_wwpn>>	WWPN of Infra Datastore 02 A
<<var_vm_host_infra_02_B_wwpn>>	WWPN of Infra Datastore 02 B
<<var_server_nfs_vlan_id>>	NFS VLAN ID
<<var_nfs_lif02_ip>>	NFS LIF 02 IP Address
<<var_nfs_lif01_ip>>	NFS LIF 01 IP Address

Physical Infrastructure

FlexPod Cabling

The information in this section is provided as a reference for cabling the physical equipment in a FlexPod environment. To simplify cabling requirements, the tables include both local and remote device and port locations.

The tables in this section contain the details for the prescribed and supported configuration of the NetApp FAS8040 running clustered Data ONTAP 8.2.3. For any modifications of this prescribed architecture, consult the [NetApp Interoperability Matrix Tool \(IMT\)](#).

This document assumes that out-of-band management ports are plugged into an existing management infrastructure at the deployment site. These interfaces will be used in various configuration steps

Be sure to follow the cabling directions in this section. Failure to do so will result in necessary changes to the deployment procedures that follow because specific port locations are mentioned.

[Figure 2](#) shows a cabling diagram for a FlexPod configuration using the Cisco Nexus 9000 and NetApp storage systems with clustered Data ONTAP. The NetApp storage controller and disk shelves should be connected according to best practices for the specific storage controller and disk shelves. For disk shelf cabling, refer to the Universal SAS and ACP Cabling Guide

https://library.netapp.com/ecm/ecm_get_file/ECMM1280392.

Figure 2

FlexPod Cabling Diagram

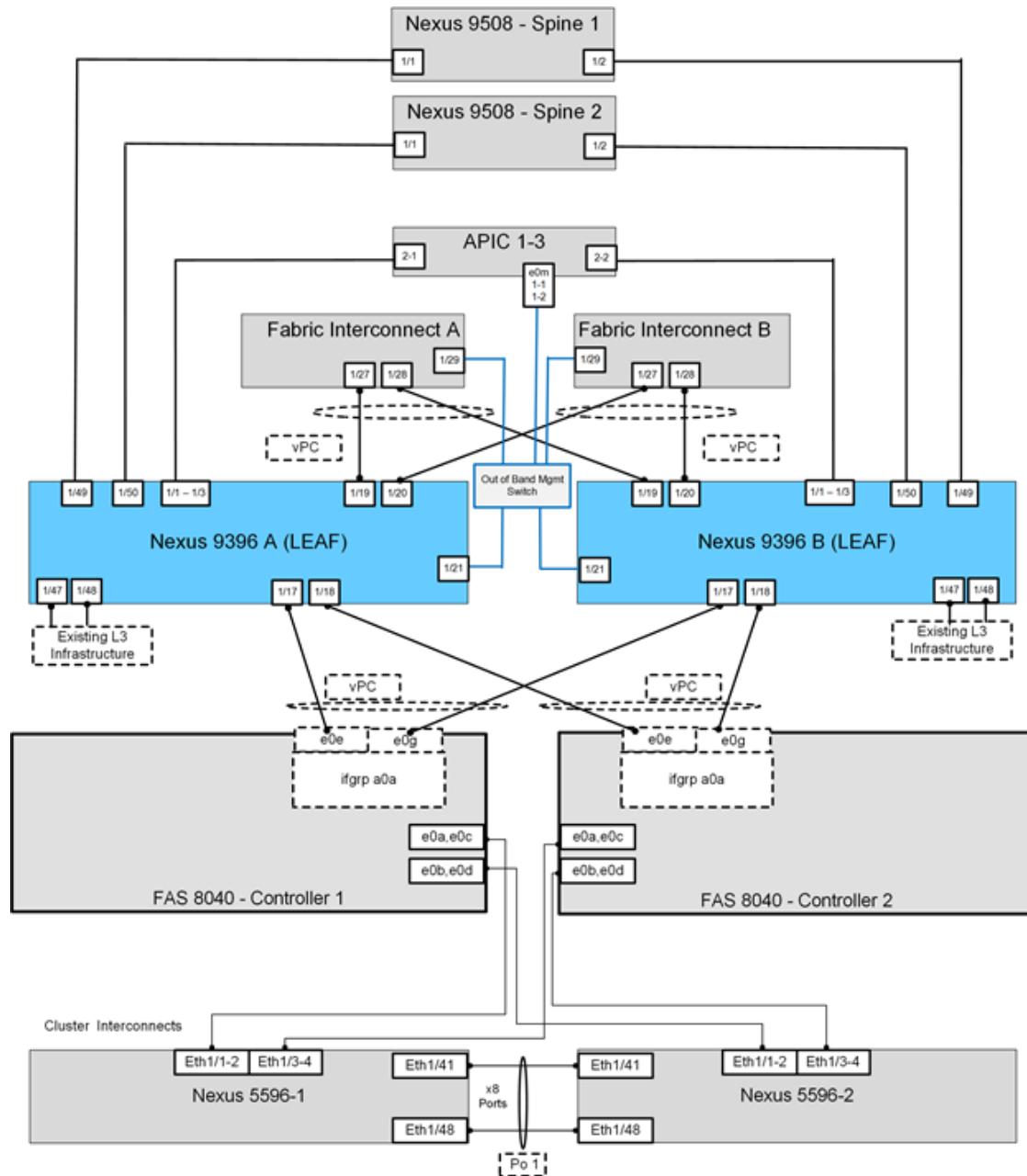


Table 5 through Table 17 provide the details of all the connections in use.

Table 5 Cisco Nexus 9396-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 9396 A	Eth1/1	10GbE	APIC 1	Eth 2-1
	Eth1/2	10GbE	APIC 2	Eth 2-1
	Eth1/3	10GbE	APIC 3	Eth 2-1
	Eth1/17	10GbE	NetApp controller 1	e0e
	Eth1/18	10GbE	NetApp controller 2	e0e
	Eth1/19	10GbE	Cisco UCS fabric interconnect A	Eth1/31
	Eth1/20	10GbE	Cisco UCS fabric interconnect B	Eth1/31
	Eth1/21	GbE	Common Services Mgmt. Switch	Any
	Eth1/49	40GbE	Cisco 9508 Spine 1	Eth1/1
	Eth1/50	40GbE	Cisco 9508 Spine 2	Eth1/1
	MGMT0	GbE	GbE management switch	Any



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

Table 6 Cisco Nexus 9396-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 9396 A	Eth1/1	10GbE	APIC 1	Eth 2-2
	Eth1/2	10GbE	APIC 2	Eth 2-2
	Eth1/3	10GbE	APIC 3	Eth 2-2
	Eth1/17	10GbE	NetApp controller 1	e0g
	Eth1/18	10GbE	NetApp controller 2	e0g
	Eth1/19	10GbE	Cisco UCS fabric interconnect A	Eth1/32
	Eth1/20	10GbE	Cisco UCS fabric interconnect B	Eth1/32
	Eth1/21	GbE	Common Services Mgmt. Switch	Any
	Eth1/49	40GbE	Cisco 9508 Spine 1	Eth1/2
	Eth1/50	40GbE	Cisco 9508 Spine 2	Eth1/2
	MGMT0	GbE	GbE management switch	Any



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

Table 7 NetApp Controller-1 Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
NetApp controller 1	e0M	100MbE	100MbE management switch	Any
	e0a	GbE	GbE management switch	Any
	e0P	GbE	SAS shelves	ACP port
	e0a	10GbE	Cisco Nexus 5596 A	Eth1/1
	e0b	10GbE	Cisco Nexus 5596 B	Eth1/1
	e0c	10GbE	Cisco Nexus 5596 A	Eth1/2
	e0d	10GbE	Cisco Nexus 5596 B	Eth1/2
	e0e	10GbE	Cisco Nexus 9000 A	Eth 1/17
	e0g	10GbE	Cisco Nexus 9000 B	Eth 1/17

When the term e0M is used, the physical Ethernet port to which the table is referring is the port indicated by a wrench icon on the rear of the chassis.

Table 8 NetApp controller 2 Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
NetApp controller 1	e0M	100MbE	100MbE management switch	Any
	e0a	GbE	GbE management switch	Any
	e0P	GbE	SAS shelves	ACP port
	e0a	10GbE	Cisco Nexus 5596 A	Eth1/3
	e0b	10GbE	Cisco Nexus 5596 B	Eth1/3
	e0c	10GbE	Cisco Nexus 5596 A	Eth1/4
	e0d	10GbE	Cisco Nexus 5596 B	Eth1/4
	e0e	10GbE	Cisco Nexus 9000 A	Eth 1/18
	e0g	10GbE	Cisco Nexus 9000 B	Eth 1/18

When the term e0M is used, the physical Ethernet port to which the table is referring is the port indicated by a wrench icon on the rear of the chassis.

Table 9 Cisco Nexus 5596-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 5596 A	Eth1/1	10GbE	NetApp controller 1	e0a
	Eth1/2	10GbE	NetApp controller 1	e0c
	Eth1/3	10GbE	NetApp controller 2	e0a
	Eth1/4	10GbE	NetApp controller 2	e0c
	Eth1/41	10GbE	Cisco Nexus 5596 B	Eth1/41
	Eth1/42	10GbE	Cisco Nexus 5596 B	Eth1/42
	Eth1/43	10GbE	Cisco Nexus 5596 B	Eth1/43
	Eth1/44	10GbE	Cisco Nexus 5596 B	Eth1/44
	Eth1/45	10GbE	Cisco Nexus 5596 B	Eth1/45
	Eth1/46	10GbE	Cisco Nexus 5596 B	Eth1/46
	Eth1/47	10GbE	Cisco Nexus 5596 B	Eth1/47
	Eth1/48	10GbE	Cisco Nexus 5596 B	Eth1/48
	MGMT0	GbE	GbE management switch	Any

Table 10 Cisco Nexus 5596-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 5596 B	Eth1/1	10GbE	NetApp controller 1	e0b
	Eth1/2	10GbE	NetApp controller 1	e0d
	Eth1/3	10GbE	NetApp controller 2	e0b
	Eth1/4	10GbE	NetApp controller 2	e0d
	Eth1/41	10GbE	Cisco Nexus 5596 A	Eth1/41
	Eth1/42	10GbE	Cisco Nexus 5596 A	Eth1/42
	Eth1/43	10GbE	Cisco Nexus 5596 A	Eth1/43
	Eth1/44	10GbE	Cisco Nexus 5596 A	Eth1/44
	Eth1/45	10GbE	Cisco Nexus 5596 A	Eth1/45
	Eth1/46	10GbE	Cisco Nexus 5596 A	Eth1/46
	Eth1/47	10GbE	Cisco Nexus 5596 A	Eth1/47
	Eth1/48	10GbE	Cisco Nexus 5596 A	Eth1/48
	MGMT0	GbE	GbE management switch	Any

Table 11 Cisco UCS Fabric Interconnect A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect A	Eth1/1	10GbE	Cisco UCS Chassis FEX A	IOM 1/1
	Eth1/2	10GbE	Cisco UCS Chassis FEX A	IOM 1/2
	Eth1/27	10GbE	Cisco Nexus 9000 A	Eth 1/19
	Eth1/28	10GbE	Cisco Nexus 9000 B	Eth 1/19
	Eth1/29	10GbE	Management Switch	Any
	Eth1/31	10GbE	Cisco Nexus 2232PP FEX A	Uplink 1
	Eth1/32	10GbE	Cisco Nexus 2232PP FEX A	Uplink 2
	MGMT0	GbE	GbE management switch	Any
	L1	GbE	Cisco UCS fabric interconnect B	L1
	L2	GbE	Cisco UCS fabric interconnect B	L2

Table 12 Cisco UCS Fabric Interconnect B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect A	Eth1/1	10GbE	Cisco UCS Chassis FEX B	IOM 1/1
	Eth1/2	10GbE	Cisco UCS Chassis FEX B	IOM 1/2
	Eth1/27	10GbE	Cisco Nexus 9000 A	Eth 1/20
	Eth1/28	10GbE	Cisco Nexus 9000 B	Eth 1/20
	Eth1/29	10GbE	Management Switch	Any
	Eth1/31	10GbE	Cisco Nexus 2232PP FEX B	Uplink 1
	Eth1/32	10GbE	Cisco Nexus 2232PP FEX B	Uplink 2
	MGMT0	GbE	GbE management switch	Any
	L1	GbE	Cisco UCS fabric interconnect B	L1
	L2	GbE	Cisco UCS fabric interconnect B	L2

Table 13 Cisco Nexus 2232 FEX A—Single Wire Management

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 2232PP FEX A	Port 1	10GbE	Cisco UCS C-Series 1	Port 0
	Port 2	10GbE	Cisco UCS C-Series 2	Port 0

Table 14 Cisco Nexus 2232 FEX B—Single Wire Management

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 2232PP FEX B	Port 1	10GbE	Cisco UCS C-Series 1	Port 1
	Port 2	10GbE	Cisco UCS C-Series 2	Port 1

Table 15 Cisco UCS C-Series 1

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS C-Series 1	Port 0	10GbE	Cisco Nexus 2232PP FEX A	Port 1
	Port 1	10GbE	Cisco Nexus 2232PP FEX B	Port 1

Table 16 Cisco UCS C-Series 2

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS C-Series 2	Port 0	10GbE	Cisco Nexus 2232PP FEX A	Port 2
	Port 1	10GbE	Cisco Nexus 2232PP FEX B	Port 2

Table 17 FAS8040 Card Layout

Slot	Part Number	Description
1	X1973A-R6	Flash Cache 2™ – 512GB

Storage Configuration

Controller FAS80XX Series

Refer to the [Site Requirements Guide](#) for planning the physical location of the storage systems. From the downloaded guide, refer to the following sections:

- Site Preparation
- System Connectivity Requirements
- Circuit Breaker, Power Outlet Balancing, System Cabinet Power Cord Plugs, and Console Pinout Requirements
- 80xx Series Systems

NetApp Hardware Universe

The NetApp Hardware Universe provides supported hardware and software components for the specific Data ONTAP version. It provides configuration information for all the NetApp storage appliances currently supported by the Data ONTAP software. It also provides a table of component compatibilities.

1. Confirm that the hardware and software components are supported with the version of Data ONTAP that you plan to install by checking the NetApp Hardware Universe at the [NetApp Support site](#).
2. Access the [Hardware Universe Application](#) to view the System Configuration guides. Click the "Controllers" tab to view the compatibility between Data ONTAP software versions and NetApp storage appliances with the desired specifications.
3. Alternatively, to compare components by storage appliance, click "Compare Storage Systems."

Controllers

Follow the physical installation procedures for the controllers in the [FAS80xx documentation](#) at the NetApp Support site.

Disk Shelves

NetApp storage systems support a wide variety of disk shelves and disk drives. The complete list of disk shelves that are supported is available at the [NetApp Support site](#).

When using SAS disk shelves with NetApp storage controllers, refer to the [SAS Disk Shelves Universal SAS and ACP Cabling Guide](#) for proper cabling guidelines.

Cisco NX5596 Cluster Network Switch Configuration

The Cisco Nexus 5596 cluster network switch configuration prerequisites are as follows:

- Rack and connect power to the new Cisco Nexus 5596 switches
- Provide a terminal session that connects to the switch's serial console port (9600, 8, n, 1)
- Connect the mgmt0 port to the management network and be prepared to provide IP address information
- Obtain password for admin
- Determine switch name
- Identify SSH key type (dsa, rsa, or rsa1)
- Set up an e-mail server for Cisco Smart Call Home and IP connectivity between the switch and the e-mail server
- Provide SNMP contact information for Cisco Smart Call Home (name, phone, street address)
- Identify a CCO ID associated with an appropriate Cisco SMARTnet® Service contract for Cisco Smart Call Home
- Enable Cisco SMARTnet Service for the device to be registered for Cisco Smart Call home

Initial Setup of Cisco Nexus 5596 Cluster Interconnect

The first time a Cisco Nexus 5596 cluster interconnect is accessed, it runs a setup program that prompts the user to enter an IP address and other configuration information needed for the switch to communicate over the management Ethernet interface. This information is required to configure and manage the switch. If the configuration must be changed later, the setup wizard can be accessed again by running the setup command in EXEC mode.

To set up the Cisco Nexus 5596 cluster interconnect, complete the following steps. These steps must be completed on both the cluster interconnects.

1. Provide applicable responses to the setup prompts displayed on the Cisco Nexus 5596 cluster interconnect.

```
Abort Power On Auto Provisioning and continue with normal setup
?(yes/no) [n]: yes
Do you want to enforce secure password standard (yes/no): yes
Enter the password for "admin": <password>
```

```

Confirm the password for "admin": <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 : <switchname>
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y] :
Enter
Mgmt0 IPv4 address : <ic_mgmt0_ip>
Mgmt0 IPv4 netmask : <ic_mgmt0_netmask>
Configure the default gateway? (yes/no) [y] : Enter
IPv4 address of the default gateway : <ic_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]: yes
NTP server IPv4 address : <ntp_server_ip>
Enter basic FC configurations (yes/no) [n]: Enter

```

2. At the end of the setup, the configuration choices are displayed. Verify the information and save the configuration at this time.

```

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

```

Download and Install NetApp Cluster Switch Software

When the Cisco Nexus 5596 is being used as a cluster network switch with Data ONTAP 8.2.3, it should be running NX-OS version 5.2(1)N1(1). The show version command from the switch command line interface shows the switch version currently running on the switch. If the currently running version is not 5.2(1)N1(1), go to the [NetApp Support](#) site and download and install NX-OS 5.2(1)N1(1) for the Cisco Nexus 5596 switch. Make sure both cluster interconnects are running NX-OS version 5.2(1)N1(1).

Download and Merge of NetApp Cluster Switch Reference Configuration File

Cluster network and management network switches are shipped without the configuration files installed. These files must be downloaded to the switches during deployment. Configuration files must be downloaded when the cluster network and management network switches are first installed or after the Cisco switch software is updated or reinstalled.

After the initial setup is complete, the NetApp cluster network switch reference configuration must be transferred to the switch and merged with existing configuration. Instructions for this task and the reference configuration files for the appropriate switches are available on the [NetApp Support](#) site.

To download configuration files to a host and install them on a Cisco Nexus 5596 switch, complete the following steps on both cluster interconnects:

1. Obtain a console connection to the switch. Verify existing configuration on the switch by running the show run command.
2. Log in to the switch. Verify that the host recognizes the switch on the network (for example, use the ping utility).
3. Enter the following command:

```
copy <transfer protocol>: bootflash: vrf management
```

4. Verify that the configuration file is downloaded.

```
***** Transfer of file Completed Successfully *****      Copy complete, now  
saving to disk (please wait)...
```

5. Enter the following command to view the saved configuration file.

```
dir bootflash:
```

6. Merge the configuration file into existing running-config. Run the following command, where <config file name> is the file name for the switch type. A series of warnings regarding PortFast is displayed as each port is configured.

```
copy <config file name> running-config
```

7. Verify the success of the configuration merge by running the show run command and comparing its output to the contents of the configuration file (a .txt file) that was downloaded.

- a. The output for both installed-base switches and new switches should be identical to the contents of the configuration file for the following items:

- banner (should match the expected version)
 - Switch port descriptions such as description Cluster Node x
 - The new ISL algorithm port-channel load-balance Ethernet source-dest-port
- b. The output for new switches should be identical to the contents of the configuration file for the following items:

- Port channel
 - Policy map
 - System QoS
 - Interface
 - Boot
- c. The output for installed-base switches should have the flow control receive and send values on for the following items:
- Interface port-channel 1 and 2
 - Ethernet interface 1/41 through Ethernet interface 1/48.

8. Copy the running-config to the startup-config.

```
copy running-config startup-config
```

Cisco Smart Call Home Setup

To configure Smart Call Home on a Cisco Nexus 5596 switch, complete the following steps:

1. Enter the mandatory system contact using the snmp-server contact command in global configuration mode. Then run the callhome command to enter callhome configuration mode.

```
NX-5596#config t  
NX-5596 (config)#snmp-server contact <sys-contact>  
NX-5596 (config)#callhome
```

2. Configure the mandatory contact information (phone number, e-mail address, and street address).

```
NX-5596 (config-callhome)#email-contact <email-address>  
NX-5596 (config-callhome)#phone-contact <+1-000-000-0000>
```

```
NX-5596 (config-callhome)#streetaddress <a-street-address>
```

3. Configure the mandatory e-mail server information. The server address is an IPv4 address, IPv6 address, or the domain-name of a SMTP server to which Call Home will send e-mail messages. Optional port number (default=25) and VRF may be configured.

```
NX-5596 (config-callhome)#transport email smtp-server <ip-address> port 25  
use-vrf <vrf-name>
```

4. Set the destination profile CiscoTAC-1 e-mail address to callhome@cisco.com.

```
NX-5596 (config-callhome)#destination-profile CiscoTAC-1 email-addr  
callhome@cisco.com
```

5. Enable periodic inventory and set the interval.

```
NX-5596 (config-callhome)#periodic-inventory notification  
NX-5596 (config-callhome)#periodic-inventory notification interval 30
```

6. Enable callhome, exit, and save the configuration.

```
NX-5596 (config-callhome)#enable  
NX-5596 (config-callhome)#end  
NX-5596#copy running-config startup-config
```

7. Send a callhome inventory message to start the registration process.

```
NX-5596#callhome test inventory  
trying to send test callhome inventory message  
successfully sent test callhome inventory message
```

8. Watch for an e-mail from Cisco regarding the registration of the switch. Follow the instructions in the e-mail to complete the registration for Smart Call Home.

SNMP Monitoring Setup

Configure SNMP by using the following example as a guideline. This example configures a host receiver for SNMPv1 traps and enables all link up/down traps:

```
NX-5596#config t  
NX-5596(config)# snmp-server host <ip-address> traps { version 1 }  
<community> [udp_port <number>]  
NX-5596(config)# snmp-server enable traps link
```

Clustered Data ONTAP 8.2.3

Complete the Configuration Worksheet

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

	How to Access the Configuration Worksheet Configuration Guide	Comments
Configuration Worksheet	https://library.netapp.com/ecm/ecm_download_file/ECMP1368696	Requires access to the NetApp Support site.

Table 18 Clustered Data ONTAP Software Installation Prerequisites

Cluster Detail	Cluster Detail Value
Cluster Node01 IP address	<<var_node01_mgmt_ip>>
Cluster Node01 netmask	<<var_node01_mgmt_mask>>
Cluster Node01 gateway	<<var_node01_mgmt_gateway>>
Data ONTAP 8.2.3 URL	<<var_url_boot_software>>
Cluster Node02 IP address	<<var_node02_mgmt_ip>>
Cluster Node02 netmask	<<var_node02_mgmt_mask>>
Cluster Node02 gateway	<<var_node02_mgmt_gateway>>

Node 1

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. Enable Autoboot.

```
setenv AUTOBOOT true
```
3. Allow the system to boot up.

```
autoboot
```
4. Press Ctrl-C when the Press Ctrl-C for Boot Menu message appears.



Note If Data ONTAP 8.2.3 is not the version of software being booted, proceed with the following steps to install new software. If Data ONTAP 8.2.3 is the version being booted, then select option 8 and yes to reboot the node. Then proceed with step 14.

5. To install new software, first select option 7.

```
7
```
6. Answer yes to perform an upgrade.

```
y
```
7. Select e0M for the network port you want to use for the download.

```
e0M
```
8. Select yes to reboot now.

```
y
```
9. After reboot, enter the IP address, netmask, and default gateway for e0M in their respective places.

```
<<var_node01_mgmt_ip>> <<var_node01_mgmt_mask>> <<var_node01_mgmt_gateway>>
```
10. Enter the URL where the software can be found.



Note This Web server must be pingable.

11. Press Enter for the user name, indicating no user name.

```
Enter
```
12. Enter yes to set the newly installed software as the default to be used for subsequent reboots.

```
y
```
13. Enter yes to reboot the node.

Y

Note

When installing new software, the system might perform firmware upgrades to the BIOS and adapter cards, causing reboots and possible stops at the LOADER prompt. If these actions occur, the system might deviate from this procedure.

14. Press Ctrl-C to exit autoboot when you see this message:

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

15. From the LOADER-A prompt, enter:

```
printenv
```

Note

If `bootarg.init.boot_clustered true` is not listed, the system is not set to boot in clustered Data ONTAP.

16. If the system is not set to boot in clustered Data ONTAP, at the LOADER prompt, enter the following command to make sure the system boots in clustered Data ONTAP:

```
setenv bootarg.init.boot_clustered true
setenv bootarg.bsdportname e0M
```

17. At the LOADER-A prompt, enter:

```
autoboot
```

18. When Press Ctrl-C for Boot Menu displays:

```
Ctrl - C
```

Note

The system may program the NVRAM and reboot at this point. If it does, wait for `Press Ctrl-C for Boot Menu` and press Ctrl-C.

19. Select option 4 for clean configuration and initialize all disks.

```
4
```

20. Answer yes to Zero disks, reset config and install a new file system.

```
Y
```

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

```
Y
```

Note

The initialization and creation of the root volume can take 75 minutes or more to complete, depending on the number of disks attached. After initialization is complete, the storage system reboots. You can continue to node 02 configuration while the disks for node 01 are zeroing.

Node 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. Enable Autoboot.

```
setenv AUTOBOOT true
```

3. Allow the system to boot up.

```
autoboot
```

4. Press Ctrl-C when Press Ctrl-C for Boot Menu is displayed.

Ctrl-C



Note If Data ONTAP 8.2.3 is not the version of software being booted, proceed with the following steps to install new software. If Data ONTAP 8.2.3 is the version being booted, then select option 8 and yes to reboot the node. Then proceed with step 14.

5. To install new software first, select option 7.

7

6. Answer yes to perform an upgrade.

Y

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

e0M

8. Select yes to reboot now.

Y

9. After reboot, enter the IP address, netmask, and default gateway for e0M in their respective places.

<<var_node02_mgmt_ip>> <<var_node02_mgmt_mask>> <<var_node02_mgmt_gateway>>

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



Note This web server must be pingable.

<<var_url_boot_software>>

11. Press Enter for the user name, indicating no user name.

Enter

12. Select yes to set the newly installed software as the default to be used for subsequent reboots.

Y

13. Select yes to reboot the node.

Y



Note When installing new software, the system might perform firmware upgrades to the BIOS and adapter cards, causing reboots and possible stops at the LOADER prompt. If these actions occur, the system might deviate from this procedure.

14. Press Ctrl-C to exit autoboot when you see this message:

Starting AUTOBOOT press Ctrl-C to abort...

15. From the LOADER-A prompt, enter:

printenv



Note If bootarg.init.boot_clustered true is not listed, the system is not set to boot in clustered Data ONTAP.

16. If the system is not set to boot in clustered Data ONTAP, at the LOADER prompt, enter the following command to make sure the system boots in clustered Data ONTAP:

```
setenv bootarg.init.boot_clustered true  
setenv bootarg.bsdportname e0M
```

17. At the LOADER-A prompt, enter:

autoboot

18. When you see Press Ctrl-C for Boot Menu, enter:

Ctrl - C



Note The system may program the NVRAM and reboot at this point. If it does, wait for Press Ctrl-C for Boot Menu and press Ctrl-C.

19. Select option 4 for clean configuration and initialize all disks.

4

20. Answer yes to Zero disks, reset config and install a new file system.

y

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

y



Note 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.

Cluster Create in Clustered Data ONTAP

Table 19 Cluster Create in Clustered Data ONTAP Prerequisites

Cluster Detail	Cluster Detail Value
Cluster name	<<var_clusternamespace>>
Clustered Data ONTAP base license	<<var_cluster_base_license_key>>
Cluster management IP address	<<var_clustermgmt_ip>>
Cluster management netmask	<<var_clustermgmt_mask>>
Cluster management port	<<var_clustermgmt_port>>
Cluster management gateway	<<var_clustermgmt_gateway>>
Cluster Node01 IP address	<<var_node01_mgmt_ip>>
Cluster Node01 netmask	<<var_node01_mgmt_mask>>
Cluster Node01 gateway	<<var_node01_mgmt_gateway>>

The first node in the cluster performs the cluster create operation. All other nodes perform a cluster join operation. The first node in the cluster is considered Node01.

1. The Cluster Setup wizard starts running on the console.

Welcome to the cluster setup wizard.

You can enter the following commands at any time:

"help" or "?" - if you want to have a question clarified,
 "back" - if you want to change previously answered questions, and
 "exit" or "quit" - if you want to quit the cluster setup wizard.

Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".

To accept a default or omit a question, do not enter a value.

Do you want to create a new cluster or join an existing cluster? {create, join}:



Note If a login prompt appears instead of the Cluster Setup wizard, start the wizard by logging in using the factory default settings and then enter the cluster setup command.

2. Enter the following command to create a new cluster:

```
create
```

3. Type no for single node cluster option

```
Do you intend for this node to be used as a single node cluster? {yes, no}  
[no]: Enter
```

4. Type yes for cluster network using network switches.

```
Will the cluster network be configured to use network switches? [yes]: Enter
```

5. To activate HA and set storage failover, complete the following step.

```
Non-HA mode, Reboot node to activate HA Do you want to reboot now to set  
storage failover (SFO) to HA mode? {yes, no} [yes]: Enter
```

6. Proceed with creating the cluster. Enter create on the cluster setup wizard.

```
create
```

7. Repeat steps 3 and 4, if the cluster setup wizard prompts again.

8. The system defaults are displayed. Type "no" for using the system defaults. Follow the below
prompts to configure the cluster ports.

```
Existing cluster interface configuration found:
```

Port	MTU	IP	Netmask
e0a	9000	169.254.224.172	255.255.0.0
e0c	9000	169.254.125.157	255.255.0.0

```
Do you want to use this configuration? {yes, no} [yes]:no
```

```
System Defaults: Private cluster network ports [e0a,e0c]. Cluster port MTU  
values will be set to 9000. Cluster interface IP addresses will be  
automatically generated. Do you want to use these defaults? {yes, no}  
[yes]: no
```

```
Step 1 of 5: Create a Cluster
```

```
You can type "back", "exit", or "help" at any question.
```

```
List the private cluster network ports [e0a,e0c]: e0a,e0b,e0c,e0d
```

```
Enter the cluster ports' MTU size [9000]: Enter
```

```
Enter the cluster network netmask [255.255.0.0]: Enter
```

```
Generating a default IP address. This can take several minutes...
```

```
Enter the cluster interface IP address for port e0a [169.254.174.78]: Enter
```

```
Generating a default IP address. This can take several minutes...
```

```
Enter the cluster interface IP address for port e0b [169.254.229.72]: Enter
```

```
Generating a default IP address. This can take several minutes...
```

```
Enter the cluster interface IP address for port e0c [169.254.202.208]: Enter
```

```
Generating a default IP address. This can take several minutes...
```

```
Enter the cluster interface IP address for port e0d [169.254.205.93]: Enter
```

9. The steps to create a cluster are displayed.

```
Enter the cluster name: <>var_clustername><
```

```

Enter the cluster base license key: <<var_cluster_base_license_key>>
Creating cluster <<var_clustername>>
Enter an additional license key [] :<<var_nfs_license>>
Enter an additional license key [] :<<var_iscsi_license>>

```

**Note**

The cluster is created. This can take a minute or two.

**Note**

For this validated architecture NetApp recommends installing license keys for SnapRestore®, FlexClone®, and SnapManager® Suite. Additionally, install all needed storage protocols licenses. For example, if iSCSI boot is used, install the iSCSI license. If FCoE boot is used, install the FCP license. After you finish entering the license keys, press Enter.

```

Enter the cluster administrators (username "admin") password:
<<var_password>>
Retype the password: <<var_password>>
Enter the cluster management interface port [e0e]: e0i
Enter the cluster management interface IP address: <<var_clustermgmt_ip>>
Enter the cluster management interface netmask: <<var_clustermgmt_mask>>
Enter the cluster management interface default gateway:
<<var_clustermgmt_gateway>>

```

10. Enter the DNS domain name.

```

Enter the DNS domain names:<<var_dns_domain_name>>
Enter the name server IP addresses:<<var_nameserver_ip>>

```

**Note**

If you have more than one name server IP address, separate them with a comma.

11. Set up the node.

```

Where is the controller located [] :<<var_node_location>>
Enter the node management interface port [e0M]: Enter
Enter the node management interface IP address: <<var_node01_mgmt_ip>>
Enter the node management interface netmask: <<var_node01_mgmt_mask>>
Enter the node management interface default
gateway:<<var_node01_mgmt_gateway>>

```

**Note**

The node management interface can be on the same subnet as the cluster management interface, or could be on a different subnet.

12. Type no for IPV4 DHCP on the service processor.

```
Enable IPv4 DHCP on the service processor interface [yes]: no
```

13. Set up the Service Processor (SP)

```

Enter the service processor interface IP address: <<var_node01_sp_ip>>
Enter the service processor interface netmask: <<var_node01_sp_mask>>
Enter the service processor interface default gateway:
<<var_node01_sp_gateway>>

```

14. Log in to the Cluster Interface with the admin user id and <<var_password>>.

Cluster Join in Clustered Data ONTAP

Table 20 Cluster Join in Clustered Data ONTAP Prerequisites

Cluster Detail	Cluster Detail Value
Cluster name	<<var_clusternname>>
Cluster management IP address	<<var_clustermgmt_ip>>
Cluster Node02 IP address	<<var_node02_mgmt_ip>>
Cluster Node02 netmask	<<var_node02_mgmt_mask>>
Cluster Node02 gateway	<<var_node02_mgmt_gateway>>

The first node in the cluster performs the cluster create operation. All other nodes perform a cluster join operation. The first node in the cluster is considered Node01, and the node joining the cluster in this example is Node02.

1. The Cluster Setup wizard starts running on the console of Node02.

```
Welcome to the cluster setup wizard.  
You can enter the following commands at any time:  
"help" or "?" - if you want to have a question clarified,  
"back" - if you want to change previously answered questions, and  
"exit" or "quit" - if you want to quit the cluster setup wizard.  
Any changes you made before quitting will be saved.  
You can return to cluster setup at any time by typing "cluster setup".  
To accept a default or omit a question, do not enter a value.  
Do you want to create a new cluster or join an existing cluster?  
{create, join}:
```



Note If a login prompt is displayed instead of the Cluster Setup wizard, start the wizard by logging in using the factory default settings, and then enter the cluster setup command.

2. Enter the following command to join a cluster:

```
join
```

3. To activate HA and set storage failover, complete the following steps.

```
Non-HA mode, Reboot node to activate HA Do you want to reboot now to set  
storage failover (SFO) to HA mode? {yes, no} [yes]: Enter
```

4. After the reboot, continue the Cluster Join process.

```
join
```

5. Data ONTAP detects existing cluster and agrees to join the same cluster. Follow the below prompts to join the cluster.

```
Existing cluster interface configuration found:
```

Port	MTU	IP	Netmask
e0a	9000	169.254.192.74	255.255.0.0
e0c	9000	169.254.54.42	255.255.0.0

```
Do you want to use this configuration? {yes, no} [yes]: no
```

```
System Defaults:
```

```
Private cluster network ports [e0a,e0c].
```

```
Cluster port MTU values will be set to 9000.
```

```
Cluster interface IP addresses will be automatically generated.
```

```
Do you want to use these defaults? {yes, no} [yes]: no
```

Step 1 of 3: Join an Existing Cluster

You can type "back", "exit", or "help" at any question.

```
List the private cluster network ports [e0a,e0c]: e0a,e0b,e0c,e0d
```

```
Enter the cluster ports' MTU size [9000]: Enter
```

```
Enter the cluster network netmask [255.255.0.0]: Enter
```

```
Generating a default IP address. This can take several minutes...
```

```
Enter the cluster interface IP address for port e0a [169.254.114.252]: Enter
```

```
Generating a default IP address. This can take several minutes...
```

```
Enter the cluster interface IP address for port e0b [169.254.30.16]: Enter
```

```
Generating a default IP address. This can take several minutes...
```

```
Enter the cluster interface IP address for port e0c [169.254.55.17]: Enter
```

```
Generating a default IP address. This can take several minutes...
```

```
Enter the cluster interface IP address for port e0d [169.254.117.17]: Enter
```

```
Enter the name of the cluster you would like to join [<<var_clusternname>>]:
```

Enter



Note

The node should find the cluster name.

6. Set up the node.

```
Enter the node management interface port [e0M]: Enter
```

```
Enter the node management interface IP address: <<var_node02_mgmt_ip>>
```

```
Enter the node management interface netmask [<<var_node02_mgmt_mask>>]:
```

Enter

```
Enter the node management interface default gateway
```

```
[<<var_node02_mgmt_gateway>>]: Enter
```



Note

The node management interface can be on the same subnet as the cluster management interface, or could be on a different subnet.

7. Type no for IPV4 DHCP on the service processor.

```
Enable IPV4 DHCP on the service processor interface [yes]: no
```

8. Set up the Service Processor (SP)

```
Enter the service processor interface IP address: <<var_node02_sp_ip>>
```

```
Enter the service processor interface netmask: <<var_node02_sp_mask>>
```

```
Enter the service processor interface default gateway:
```

```
<<var_node02_sp_gateway>>
```

Log in to the Cluster

Open either an SSH connection to the cluster management IP or host name and log in with the admin user with the password you provided earlier.

Zero All Spare Disks

- To zero all spare disks in the cluster, enter the following command.

```
disk zerospares
```



Note Disk auto-assign should have assigned half of the connected disks to each node in the HA pair. If a different disk assignment is required, disk auto-assignment will need to be disabled on both nodes in the HA pair using the `disk option modify` command. Spare disks can then be moved from one node to another using the `disk removeowner` and `disk assign` commands.

Set Onboard UTA2 ports personality

- Verify the "Current Mode" and "Current Type" of the ports by using the "ucadmin show" command.

```
icef1-stcl::> ucadmin show
          Current  Current  Pending  Pending
Node      Adapter  Mode    Type     Mode    Type   Status
-----  -----
icef1-stcl-01
          0e      cna    target   -       -       online
icef1-stcl-01
          0f      cna    target   -       -       online
icef1-stcl-01
          0g      cna    target   -       -       online
icef1-stcl-01
          0h      cna    target   -       -       online
icef1-stcl-02
          0e      cna    target   -       -       online
icef1-stcl-02
          0f      cna    target   -       -       online
icef1-stcl-02
          0g      cna    target   -       -       online
icef1-stcl-02
          0h      cna    target   -       -       online
8 entries were displayed.
```

- Verify that the Current Mode of the ports that are in use is "cna" and the Current Type is set to "target". If not, change the port personality by using the following command:

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode cna
              -type target
```



Note The ports must be offline to run the above command. To take an adapter offline, use the `fcp adapter modify <home node of the port> -adapter <port name> -state down` command. Ports must be converted in pairs, for example; e0e and e0f. A reboot will be required and the ports will need to be brought back to the up state.

Set Auto-Revert on Cluster Management

- To set the auto-revert parameter on the cluster management interface, enter:

```
network interface modify -vserver <<var_clusternamespace>> -lif cluster_mgmt
              -auto-revert true
```

Failover Groups Management in Clustered Data ONTAP

1. Create a management port failover group.

```
network interface failover-groups create -failover-group fg-cluster-mgmt
-node <<var_node01>> -port e0i
network interface failover-groups create -failover-group fg-cluster-mgmt
-node <<var_node02>> -port e0i
```

Assign Management Failover Group to Cluster Management LIF

1. Assign the management port failover group to the cluster management LIF.

```
network interface modify -vserver <<var_clusternamespace>> -lif cluster_mgmt
-failover-group fg-cluster-mgmt
```

Failover Groups Node Management in Clustered Data ONTAP

1. Create a management port failover group.

```
network interface failover-groups create -failover-group fg-node-mgmt01
-node <<var_node01>> -port e0M
network interface failover-groups create -failover-group fg-node-mgmt01
-node <<var_node01>> -port e0i
network interface failover-groups create -failover-group fg-node-mgmt02
-node <<var_node02>> -port e0M
network interface failover-groups create -failover-group fg-node-mgmt02
-node <<var_node02>> -port e0i
```

Assign Node Management Failover Groups to Node Management LIFs

1. Assign the management port failover group to the cluster management LIF.

```
network interface modify -vserver <<var_node01>> -lif mgmt1 -auto-revert
true -failover-group fg-node-mgmt01
network interface modify -vserver <<var_node02>> -lif mgmt1 -auto-revert
true -failover-group fg-node-mgmt02
```

Flash Cache in Clustered Data ONTAP

If Flash Cache cards are installed, complete the following steps to enable Flash Cache on each node:

1. Run the following commands from the cluster management interface:

```
system node run -node <<var_node01>> options flexscale.enable on
system node run -node <<var_node01>> options flexscale.lopri_blocks off
system node run -node <<var_node01>> options flexscale.normal_data_blocks on
system node run -node <<var_node02>> options flexscale.enable on
system node run -node <<var_node02>> options flexscale.lopri_blocks off
system node run -node <<var_node02>> options flexscale.normal_data_blocks on
```



Note

Data ONTAP 8.1 and later does not require a separate license for Flash Cache.



Note For directions on how to configure Flash Cache in metadata mode or low-priority data caching mode, refer to [TR-3832: Flash Cache Best Practices Guide](#). Before customizing the settings, determine whether the custom settings are required or if the default settings are sufficient.

Aggregates in Clustered Data ONTAP

An aggregate containing the root volume is created during the Data ONTAP setup process. To create additional aggregates, determine the aggregate name, the node on which to create it, and the number of disks it will contain.

1. To create new aggregates, enter the following command:

```
aggr create -aggregate aggr1_node1 -nodes <<var_node01>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_node2 -nodes <<var_node02>> -diskcount
<<var_num_disks>>
```



Note Retain 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.



Note Start with five disks initially; you can add disks to an aggregate when additional storage is required.



Note The aggregate cannot be created until disk zeroing completes. Use the aggr show command to display aggregate creation status. Do not proceed until both aggr1_node1 and aggr1_node2 are online.

2. Disable Snapshot™ copies for the two data aggregates recently created.

```
node run <<var_node01>> aggr options aggr1_node1 nosnap on
node run <<var_node02>> aggr options aggr1_node2 nosnap on
```

3. Delete any existing Snapshot copies for the two data aggregates.

```
node run <<var_node01>> snap delete -A -a -f aggr1_node1
node run <<var_node02>> snap delete -A -a -f aggr1_node2
```

4. Rename the root aggregate on node 01 to match the naming convention for this aggregate on node 02.

```
aggr show
aggr rename -aggregate aggr0 -newname <<var_node01_rootaggrname>>
```

Resize Node Root Volumes

To resize the node root volumes to avoid the root aggregate full warning, run the following commands.

1. Resize the node root volumes.

```
volume size -vserver <<var_node01>> -volume vol0 -new-size 250GB
volume size -vserver <<var_node02>> -volume vol0 -new-size 250GB
```

Storage Failover in Clustered Data ONTAP

To confirm that storage failover is enabled, run the following commands in a failover pair.

1. Verify the status of storage failover.

```
storage failover show
```

2. Both the nodes <>var_node01<> and <>var_node02<> must be capable of performing a takeover.

3. Proceed to step 5, if the nodes are capable of performing a takeover.

4. Enable failover on one of the two nodes.

```
storage failover modify -node <>var_node01<> -enabled true
```



Note

Enabling failover on one node enables it for both nodes.

5. Verify the HA status for two-node cluster.



Note

This step is not applicable for clusters with more than two nodes.

```
cluster ha show
```

6. Proceed to step 8 if high availability is configured.

7. Enable HA mode only for the two-node cluster.



Note

Do not run this command for clusters with more than two nodes because it will cause problems with failover.

```
cluster ha modify -configured true  
Do you want to continue? {y|n}: y
```

8. Verify that hardware assist is correctly configured and if needed modify the partner IP address.

```
storage failover hwassist show  
storage failover modify -hwassist-partner-ip <>var_node02_mgmt_ip<> -node <>var_node01<>  
storage failover modify -hwassist-partner-ip <>var_node01_mgmt_ip<> -node <>var_node02<>
```

Disable Flow Control on 10GbE and UTA2 Ports



Note

The NetApp best practice is to disable flow control on all the 10GbE and UTA2 ports that are connected to external devices.

1. To disable flow control and verify, run the following commands:

```
net port modify -node <>var_node01<> -port e0a,e0b,e0c,e0d,e0e,e0f,e0g,e0h
```

```
-flowcontrol-admin none
```

Warning: Changing the network port settings will cause a several second interruption in carrier.

```
Do you want to continue? {y|n}: y
```

```
net port modify -node <<var_node02>> -port e0a,e0b,e0c,e0d,e0e,e0f,e0g,e0h  
-flowcontrol-admin none  
Warning: Changing the network port settings will cause a several second  
interruption in carrier.  
Do you want to continue? {y|n}: y  
  
net port show -fields flowcontrol-admin
```

Disable Unused FCoE Ports

Unused data FCoE ports should be disabled. To disable these ports, complete the following steps:

1. Run the following commands:

```
fcp adapter modify -node <<var_node01>> -adapter 0e -state down  
fcp adapter modify -node <<var_node01>> -adapter 0g -state down  
fcp adapter modify -node <<var_node02>> -adapter 0e -state down
```

IFGRP LACP in Clustered Data ONTAP

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.

1. Run the following commands on the command line to create interface groups (ifgrps).

```
ifgrp create -node <<var_node01>> -ifgrp a0a -distr-func port -mode  
multimode_lacp  
network port ifgrp add-port -node <<var_node01>> -ifgrp a0a -port e0e  
network port ifgrp add-port -node <<var_node01>> -ifgrp a0a -port e0g  
ifgrp create -node <<var_node02>> -ifgrp a0a -distr-func port -mode  
multimode_lacp  
network port ifgrp add-port -node <<var_node02>> -ifgrp a0a -port e0e  
network port ifgrp add-port -node <<var_node02>> -ifgrp a0a -port e0g  
ifgrp show
```



Note

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



Note

The interface group name must follow the standard naming convention of a0x.



Note

Since the switches have not yet been configured, the interface groups will have no active ports.

VLAN in Clustered Data ONTAP

1. Create NFS VLANs.

```
network port vlan create -node <<var_node01>> -vlan-name  
a0a-<<var_nfs_vlan_id>>  
network port vlan create -node <<var_node02>> -vlan-name  
a0a-<<var_nfs_vlan_id>>
```

2. Create iSCSI VLANs.

```
network port vlan create -node <<var_node01>> -vlan-name
a0a-<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_node01>> -vlan-name
a0a-<<var_iscsi_vlan_B_id>>
network port vlan create -node <<var_node02>> -vlan-name
a0a-<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_node02>> -vlan-name
a0a-<<var_iscsi_vlan_B_id>>
```

3. Create In-Band Management VLANs.

```
network port vlan create -node <<var_node01>> -vlan-name
a0a-<<var_ib-mgmt_vlan_id>>
network port vlan create -node <<var_node02>> -vlan-name
a0a-<<var_ib-mgmt_vlan_id>>
```

Jumbo Frames in Clustered Data ONTAP

- To configure a clustered Data ONTAP network port to use jumbo frames (which usually have an MTU of 9,000 bytes), run the following command from the cluster shell:

```
network port modify -node <<var_node01>> -port a0a -mtu 9000
```

WARNING: Changing the network port settings will cause a several second interruption in carrier.

Do you want to continue? {y|n}: y

```
network port modify -node <<var_node02>> -port a0a -mtu 9000
```

WARNING: Changing the network port settings will cause a several second interruption in carrier.

Do you want to continue? {y|n}: y

```
network port modify -node <<var_node01>> -port a0a-<<var_nfs_vlan_id>> -mtu
9000
```

WARNING: Changing the network port settings will cause a several second interruption in carrier.

Do you want to continue? {y|n}: y

```
network port modify -node <<var_node02>> -port a0a-<<var_nfs_vlan_id>> -mtu
9000
```

WARNING: Changing the network port settings will cause a several second interruption in carrier.

Do you want to continue? {y|n}: y

```
network port show -fields mtu
```



Note

It is recommended to configure jumbo frames on this infrastructure.



Note When an interface group is configured with MTU 9000, all VLAN interfaces configured on that interface group will also have an MTU of 9000. All of the existing VLAN interfaces created here were created when the interface group's MTU was set to the default of 1500.

NTP in Clustered Data ONTAP

To configure time synchronization on the cluster, complete the following steps:

1. To set the time zone for the cluster, run the following command:

```
timezone <>var_timezone>>
```



Note For example, in the Eastern United States, the time zone is America/New_York.

2. To set the date for the cluster, run the following command:

```
date <>ccyy-mm-dd hh:mm.ss>
```



Note The format for the date is <[Century] [Year] [Month] [Day] [Hour] [Minute] . [Second]>; for example, 201409081735.17

3. Configure the Network Time Protocol (NTP) for each node in the cluster.

```
system services ntp server create -node <>var_node01>> -server <>var_global_ntp_server_ip>> system services ntp server create -node <>var_node02>> -server <>var_global_ntp_server_ip>>
```

SNMP in Clustered Data ONTAP

1. Configure SNMP basic information, such as the location and contact. When polled, this information is visible as the sysLocation and sysContact variables in SNMP.

```
snmp contact <>var_snmp_contact>>
snmp location "<>var_snmp_location>>" 
snmp init 1
options snmp.enable on
```

2. Configure SNMP traps to send to remote hosts, such as an OnCommand Unified Manager server or another fault management system.

```
snmp traphost add <>var_oncommand_server_fqdn>>
```

SNMPv1 in Clustered Data ONTAP

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

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

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

AutoSupport HTTPS in Clustered Data ONTAP

AutoSupport sends support summary information to NetApp through HTTPS.

- To configure AutoSupport, run the following command:

```
system node autosupport modify -node * -state enable -mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

Cisco Discovery Protocol in Clustered Data ONTAP

Enable Cisco Discovery Protocol (CDP) on the NetApp storage controllers by using the following procedure.



Note To be effective, CDP must also be enabled on directly connected networking equipment such as switches and routers.

To enable CDP on the NetApp storage controllers, complete the following step:

- Enable CDP on Data ONTAP.

```
node run -node <<var_node01>> options cdpd.enable on
node run -node <<var_node02>> options cdpd.enable on
```

Storage Virtual Machine (Vserver)

To create an infrastructure Vserver, complete the following steps:

- Run the Vserver setup wizard.

```
vserver setup
```

Welcome to the Vserver Setup Wizard, which will lead you through the steps to create a virtual storage server that serves data to clients.

You can enter the following commands at any time:

"help" or "?" if you want to have a question clarified,
 "back" if you want to change your answers to previous questions, and
 "exit" if you want to quit the Vserver Setup Wizard. Any changes you made before typing "exit" will be applied.

You can restart the Vserver Setup Wizard by typing "vserver setup". To accept a default or omit a question, do not enter a value.

Vserver Setup wizard creates and configures only data Vservers. If you want to create a Vserver with Infinite Volume use the vserver create command.

Step 1. Create a Vserver.

You can type "back", "exit", or "help" at any question.

- Enter the Vserver name.

Enter the Vserver name:Infra_Vserver

3. Select the Vserver data protocols to configure.

Choose the Vserver data protocols to be configured {nfs, cifs, fcp, iscsi, ndmp}: nfs,iscsi

4. Select the Vserver client services to configure.

Choose the Vserver client services to configure {ldap, nis, dns}:Enter

5. Enter the Vserver root volume aggregate:

Enter the Vserver's root volume aggregate {aggr1_node1, aggr1_node2} [aggr1_node1]: Enter

6. Enter the Vserver language setting, or "help" to see all languages [C.UTF-8]:

7. Enter the Vserver security style:

Enter the Vserver root volume's security style {mixed, ntfs, unix} [unix]: Enter

8. Answer no to Do you want to create a data volume?

Do you want to create a data volume? {yes, no} [Yes]: no

9. Answer no to Do you want to create a logical interface?

Do you want to create a logical interface? {yes, no} [Yes]: no

10. Answer no to Do you want to configure iSCSI?

Do you want to configure iSCSI? {yes, no} [yes]: no

11. Add the two data aggregates to the Infra_Vserver aggregate list for NetApp Virtual Console.

```
vserver modify -vserver Infra_Vserver -aggr-list aggr1_node1, aggr1_node2
```

Create Load Sharing Mirror of Vserver Root Volume in Clustered Data ONTAP

1. Create a volume to be the load sharing mirror of the infrastructure Vserver root volume on each node.

```
volume create -vserver Infra_Vserver -volume rootvol_m01 -aggregate aggr1_node1 -size 1GB -type DP  
volume create -vserver Infra_Vserver -volume rootvol_m02 -aggregate aggr1_node2 -size 1GB -type DP
```

2. Create a job schedule to update the root volume mirror relationships every 15 minutes.

```
job schedule interval create -name 15min -minutes 15
```

3. Create the mirroring relationships.

```
snapmirror create -source-path //Infra_Vserver/rootvol -destination-path //Infra_Vserver/rootvol_m01 -type LS -schedule 15min  
snapmirror create -source-path //Infra_Vserver/rootvol -destination-path //Infra_Vserver/rootvol_m02 -type LS -schedule 15min
```

4. Initialize the mirroring relationship.

```
snapmirror initialize-ls-set -source-path //Infra_Vserver/rootvol  
snapmirror show
```

iSCSI Service in Clustered Data ONTAP

1. Create the iSCSI service on each Vserver. This command also starts the iSCSI service and sets the iSCSI alias to the name of the Vserver.

```
iscsi create -vserver Infra_Vserver
```

```
iscsi show
```

HTTPS Access in Clustered Data ONTAP

Secure access to the storage controller must be configured.

1. Increase the privilege level to access the certificate commands.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. A self-signed certificate is already in place. Check it by using the following command:

```
security certificate show
```

3. For each Vserver shown, the certificate common name should match the DNS FQDN of the Vserver. The four default certificates should be deleted and replaced by either self-signed certificates or certificates from a Certificate Authority (CA) To delete the default certificates, run the following commands:



Note Deleting expired certificates before creating new certificates is best practice. Run the `security certificate delete` command to delete expired certificates. In the command below, use TAB completion to select and delete each default certificate.

```
security certificate delete [TAB] ...
```

Example: `security certificate delete -vserver Infra_Vserver -common-name 3.cert.1414163766 -ca 3.cert.1414163766 -type server -serial 544A6D36`

4. To generate and install self-signed certificates, run the following commands as one-time commands. Generate a server certificate for Infra_Vserver, the cluster Vserver, and each node Vserver. Again, use TAB completion to aid in completing these commands.

```
security certificate create [TAB] ...
```

Example: `security certificate create -common-name fvl2-infra.rtp.netapp.com -type server -size 2048 -country US -state "North Carolina" -locality "RTP" -organization "NetApp" -unit "ICE" -email-addr "abc@netapp.com" -expire-days 365 -hash-function SHA256 -vserver Infra_Vserver`

5. To obtain the values for the parameters that would be required in the following step, run the `security certificate show` command.

6. Enable each certificate that was just created using the `-server-enabled true` and `-client-enabled false` parameters. Again use TAB completion.

```
security ssl modify [TAB] ...
```

Example: `security ssl modify -vserver Infra_Vserver -server-enabled true -client-enabled false -ca fvl2-infra.fvl.rtp.netapp.com -serial 544A71D7 -common-name fvl2-infra.fvl.rtp.netapp.com`

7. Configure and enable SSL and HTTPS access and disable HTTP access.

```
system services web modify -external true -sslv3-enabled true
```

Warning: Modifying the cluster configuration will cause pending web service requests to be

interrupted as the web servers are restarted.

Do you want to continue {y|n}: y

```
system services firewall policy delete -policy mgmt -service http -action allow
```

```
system services firewall policy create -policy mgmt -service http -action deny -ip-list 0.0.0.0/0
```



Note It is normal for some of these commands to return an error message stating that the entry does not exist.

8. Change back to normal admin privilege level and set up to allow Vserver logs to be available by web.

```
set -privilege admin
vserver services web modify -name spi|ontapi|compat -vserver * -enabled true
```

NFSv3 in Clustered Data ONTAP

To configure NFS on the Vserver, run all commands.

1. Modify the initial default rule for the first ESXi host then create a new rule for each addition ESXi host in the default export policy.
2. For each ESXi host being created, assign a rule. Each host will have its own rule index. Your first ESXi™ host will have rule index 1, your second ESXi host will have rule index 2, and so on.

```
vserver export-policy rule modify -vserver Infra_Vserver -policyname default
-ruleindex 1 -protocol nfs -clientmatch <<var_esxi_host1_nfs_ip>> -rorule
sys -rwrule sys -superuser sys -allow-suid false
vserver export-policy rule create -vserver Infra_Vserver -policyname default
-ruleindex 2 -protocol nfs -clientmatch <<var_esxi_host2_nfs_ip>> -rorule
sys -rwrule sys -superuser sys -allow-suid false
vserver export-policy rule show
```

3. Assign the FlexPod export policy to the infrastructure Vserver root volume.

```
volume modify -vserver Infra_Vserver -volume rootvol -policy default
```

FlexVol in Clustered Data ONTAP

The following information is required to create a FlexVol® volume; the volume name and size, and the aggregate on which it will exist.

1. Create two VMware datastore volumes; a server boot volume and a volume to hold the OnCommand database LUN.
2. Update the Vserver root volume load sharing mirrors to make the NFS mounts accessible.

```
volume create -vserver Infra_Vserver -volume infra_datastore_1 -aggregate
aggr1_node2 -size 500GB -state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent-snapshot-space 0
```

```
volume create -vserver Infra_Vserver -volume infra_swap -aggregate
aggr1_node1 -size 100GB -state online -policy default -junction-path
/infra_swap -space-guarantee none -percent-snapshot-space 0 -snapshot-policy
none
```

```
volume create -vserver Infra_Vserver -volume esxi_boot -aggregate
aggr1_node1 -size 100GB -state online -policy default -space-guarantee none
-percent-snapshot-space 0
```

```
snapmirror update-ls-set -source-path //Infra_Vserver/rootvol
```

Create LUNs in Clustered Data ONTAP

1. Create two boot LUNS: VM-Host-Infra-01 and VM-Host-Infra-02.

```
lun create -vserver Infra_Vserver -volume esxi_boot -lun VM-Host-Infra-01
-size 10GB -ostype vmware -space-reserve disabled
lun create -vserver Infra_Vserver -volume esxi_boot -lun VM-Host-Infra-02
-size 10GB -ostype vmware -space-reserve disabled
```

Deduplication in Clustered Data ONTAP

1. Enable deduplication on appropriate volumes.

```
volume efficiency on -vserver Infra_Vserver -volume infra_datastore_1
volume efficiency on -vserver Infra_Vserver -volume esxi_boot
```

Failover Groups NAS in Clustered Data ONTAP

1. Create an NFS port failover group.

```
network interface failover-groups create -failover-group
fg-nfs-<<var_nfs_vlan_id>> -node <<var_node01>> -port
a0a-<<var_nfs_vlan_id>>
network interface failover-groups create -failover-group
fg-nfs-<<var_nfs_vlan_id>> -node <<var_node02>> -port
a0a-<<var_nfs_vlan_id>>
```

NFS LIF in Clustered Data ONTAP

1. Create an NFS logical interface (LIF).

```
network interface create -vserver Infra_Vserver -lif nfs_lif_infra_swap
-role data -data-protocol nfs -home-node <<var_node01>> -home-port
a0a-<<var_nfs_vlan_id>> -address <<var_node01_nfs_lif_infra_swap_ip>>
-netmask <<var_node01_nfs_lif_infra_swap_mask>> -status-admin up
-failover-policy nextavail -firewall-policy data -auto-revert true
-failover-group fg-nfs-<<var_nfs_vlan_id>>

network interface create -vserver Infra_Vserver -lif
nfs_lif_infra_datastore_1 -role data -data-protocol nfs -home-node
<<var_node02>> -home-port a0a-<<var_nfs_vlan_id>> -address
<<var_node02_nfs_lif_infra_datastore_1_ip>> -netmask
<<var_node02_nfs_lif_infra_datastore_1_mask>> -status-admin up
-failover-policy nextavail -firewall-policy data -auto-revert true
-failover-group fg-nfs-<<var_nfs_vlan_id>>
```



Note It is recommended to create a new LIF for each datastore.

Add Infrastructure Vserver Administrator

1. Add the infrastructure Vserver administrator and Vserver administration logical interface in the out-of-band management network with the following commands:

```
network interface failover-groups create -failover-group
fg-ivsmgmt-<<var_ib-mgmt_vlan_id>> -node <<var_node01>> -port
a0a-<<var_ib-mgmt_vlan_id>>
network interface failover-groups create -failover-group
fg-ivsmgmt-<<var_ib-mgmt_vlan_id>> -node <<var_node02>> -port
a0a-<<var_ib-mgmt_vlan_id>>

network interface create -vserver Infra_Vserver -lif vsmgmt -role data
-data-protocol none -home-node <<var_node02>> -home-port
a0a-<<var_ib-mgmt_vlan_id>> -address <<var_vserver_mgmt_ip>> -netmask
<<var_vserver_mgmt_mask>> -status-admin up -failover-policy nextavail
-firewall-policy mgmt -auto-revert true -failover-group
fg-ivsmgmt-<<var_ib-mgmt_vlan_id>>
```

Note: you will see that a routing group is created with the above command.
Use that routing group in the command below where you see
<<var_routing_group>>.

```
network routing-groups route create -vserver Infra_Vserver -routing-group
<<var_routing_group>> -destination 0.0.0.0/0 -gateway
<<var_vserver_mgmt_gateway>>

security login password -username vsadmin -vserver Infra_Vserver
Enter a new password: <<var_vsadmin_password>>
Enter it again: <<var_vsadmin_password>>

security login unlock -username vsadmin -vserver Infra_Vserver
```

Server Configuration

FlexPod Cisco UCS Base

Perform the 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 steps are necessary to provision the Cisco UCS B-Series and C-Series servers and should be followed precisely to avoid improper configuration.

Cisco UCS 6248 A

To configure the Cisco Unified Computing System for use in a FlexPod environment, complete the following 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 chosen to setup a new fabric interconnect? Continue? (y/n) : y
Enforce 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_ucs_mgmt_ip>>
Physical switch Mgmt0 IPv4 netmask: <<var_ucs_mgmt_mask>>
IPv4 address of the default gateway: <<var_ucs_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 6248 B

To configure the Cisco UCS for use in a FlexPod environment, complete the following 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_ucs_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.

Cisco UCS for Clustered Data ONTAP

Log in to Cisco UCS Manager

To log in to the Cisco Unified Computing System (UCS) environment, complete the following 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 2.2(3d)

This document assumes the use of Cisco UCS 2.2(3d). To upgrade the Cisco UCS Manager software and the UCS 6248 Fabric Interconnect software to version 2.2(3d), refer to [Cisco UCS Manager Install and Upgrade Guides](#).

Add a 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, complete the following steps:

1. This block of IP addresses should be in the same subnet as the management IP addresses for the Cisco UCS Manager.
2. In Cisco UCS Manager, click the LAN tab in the navigation pane.
3. Select Pools > root > IP Pools > IP Pool ext-mgmt.
4. In the Actions pane, select Create Block of IP Addresses.
5. Enter the starting IP address of the block and the number of IP addresses required, and the subnet and gateway information.
6. Click OK to create the IP block.
7. Click OK in the confirmation message.

Synchronize Cisco Unified Computing System to NTP

To synchronize the Cisco UCS environment to the NTP server, complete the following steps:

1. In Cisco UCS Manager, click the Admin tab in the navigation pane.
2. Select All > Timezone Management.
3. In the Properties pane, select 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 the Cisco UCS B-Series chassis and of additional fabric extenders for further C-Series connectivity.

To modify the chassis discovery policy, complete the following steps:

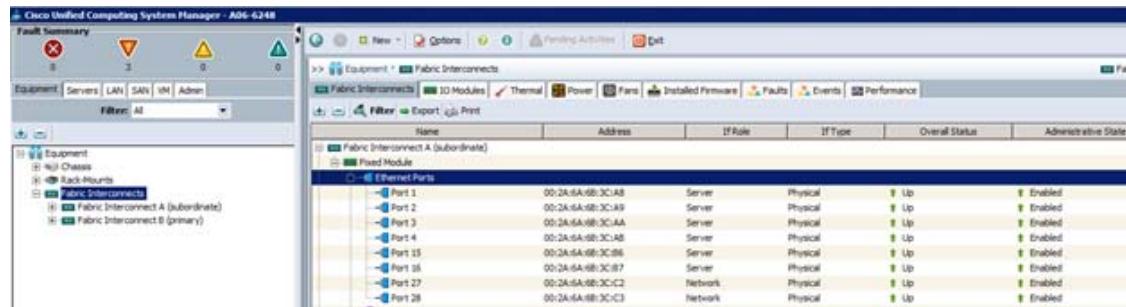
1. In Cisco UCS Manager, click the Equipment tab in the navigation pane and select Equipment in the list on the left.
2. In the right pane, click the Policies tab.
3. Under Global Policies, set the Chassis/FEX Discovery Policy to match the number of uplink ports that are cabled between the chassis or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

6. Click OK.

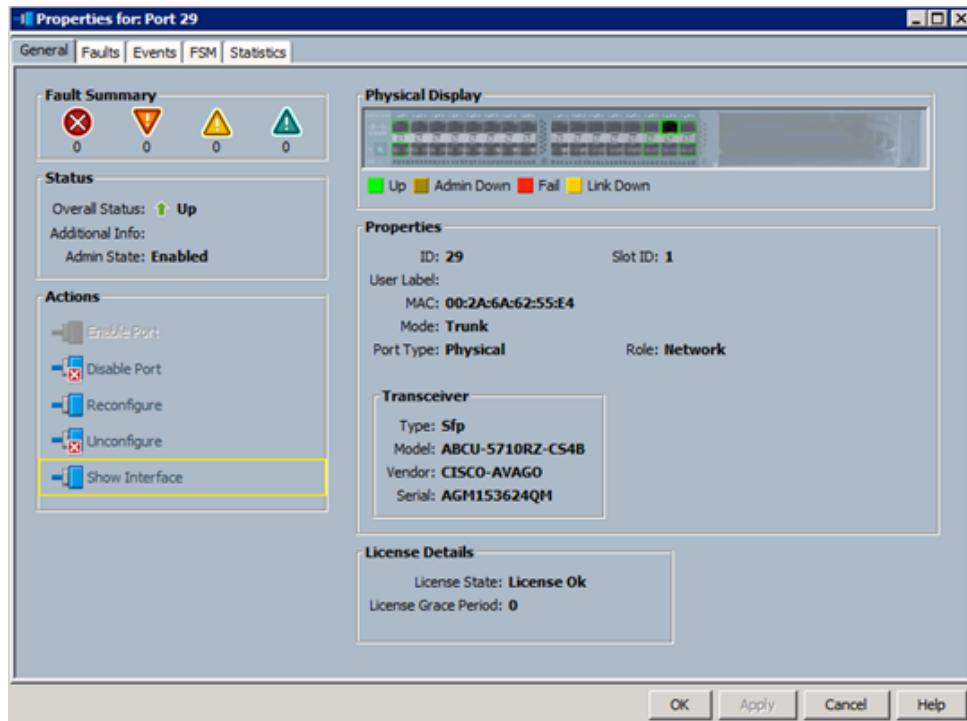
Enable Server and Uplink Ports

To enable server and uplink ports, complete the following steps:

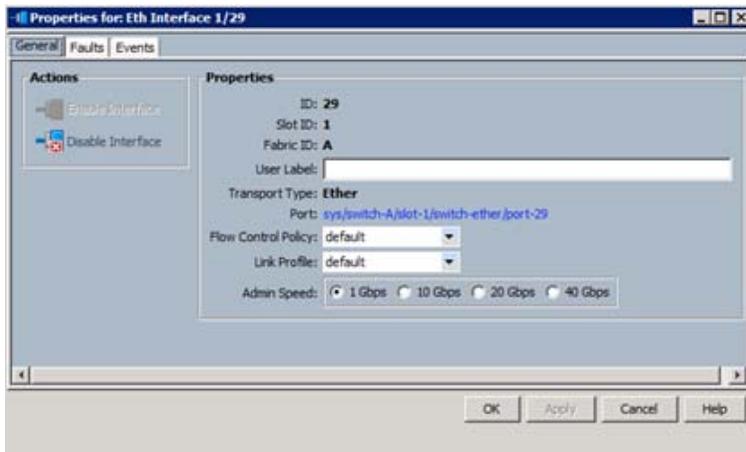
1. In Cisco UCS Manager, click the Equipment tab in the navigation pane.
2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module.
3. Expand Ethernet Ports.
4. Select the ports that are connected to the chassis, Cisco 2232 FEX (two per FEX), and direct connect Cisco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



7. Select ports 27 and 28 that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.
8. Click Yes to confirm uplink ports and click OK.
9. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.
10. Expand Ethernet Ports.
11. Select the ports that are connected to the chassis, C-series servers or to the Cisco 2232 FEX (two per FEX), right-click them, and select Configure as Server Port.
12. Click Yes to confirm server ports and click OK.
13. Select ports 27 and 28 that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.
14. Click Yes to confirm the uplink ports and click OK.
15. Select port 29 connected to out of band management network switch on each Fabric Interconnect and select Configure as Uplink Port.
16. Click Yes to confirm the uplink ports and click OK.
17. Optional: If the out of band management switch is 1Gbps switch, for the port 29 on each Fabric Interconnect, right click the interface and select Show Navigator.
18. Click Show Interface in the Properties window.



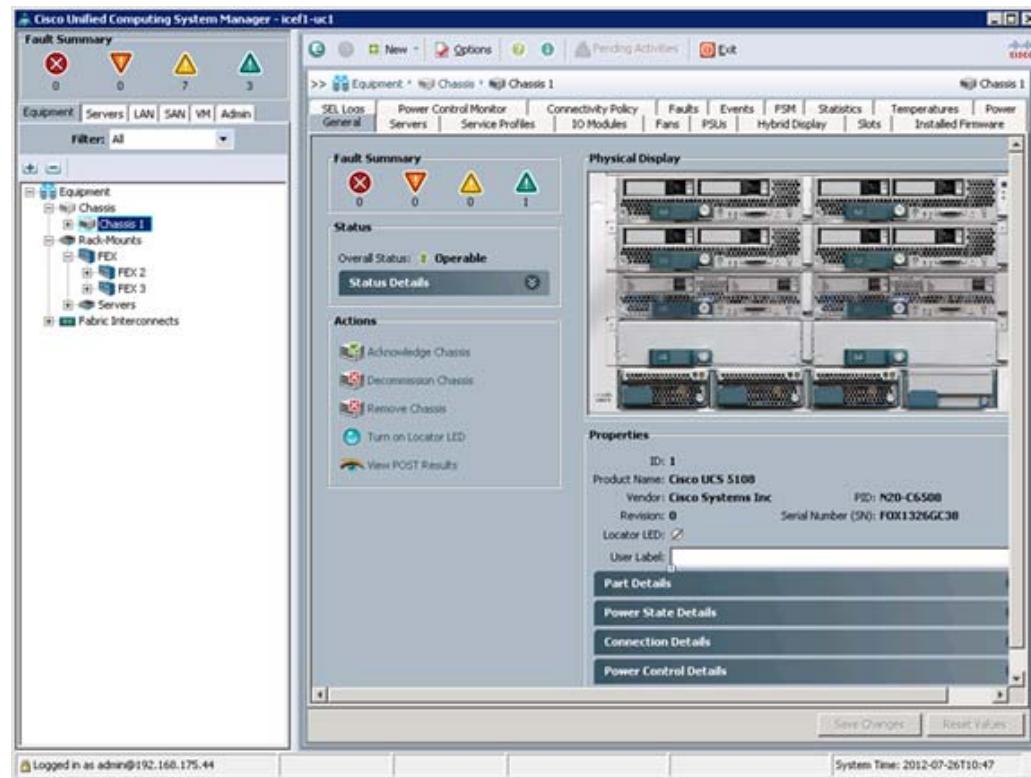
19. Select 1Gbps as the speed of the interface.



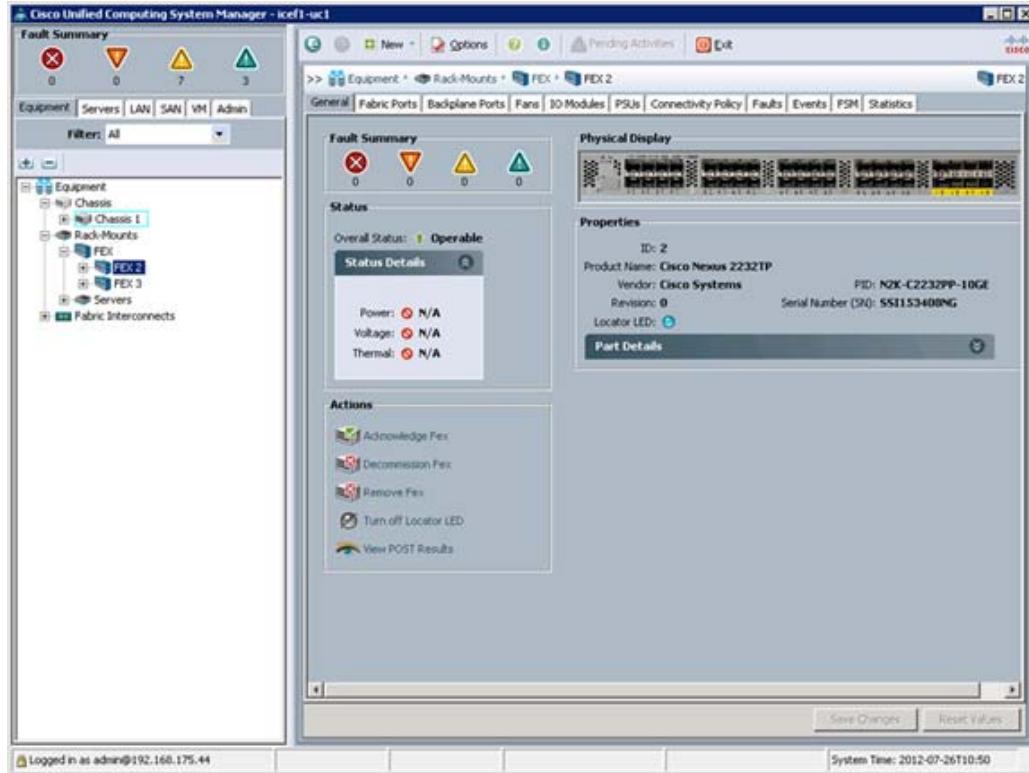
Acknowledge Cisco UCS Chassis and FEX

To acknowledge all Cisco UCS chassis and external 2232 FEX modules, complete the following steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane.
2. Expand Chassis and select each chassis that is listed.
3. Right-click each chassis and select Acknowledge Chassis.



4. Click Yes and then click OK to complete acknowledging the chassis.
5. If Cisco Nexus 2232 FEX are part of the configuration, expand Rack Mounts and FEX.
6. Right-click each FEX that is listed and select Acknowledge FEX.



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

Create Uplink Port Channels to Cisco Nexus Switches

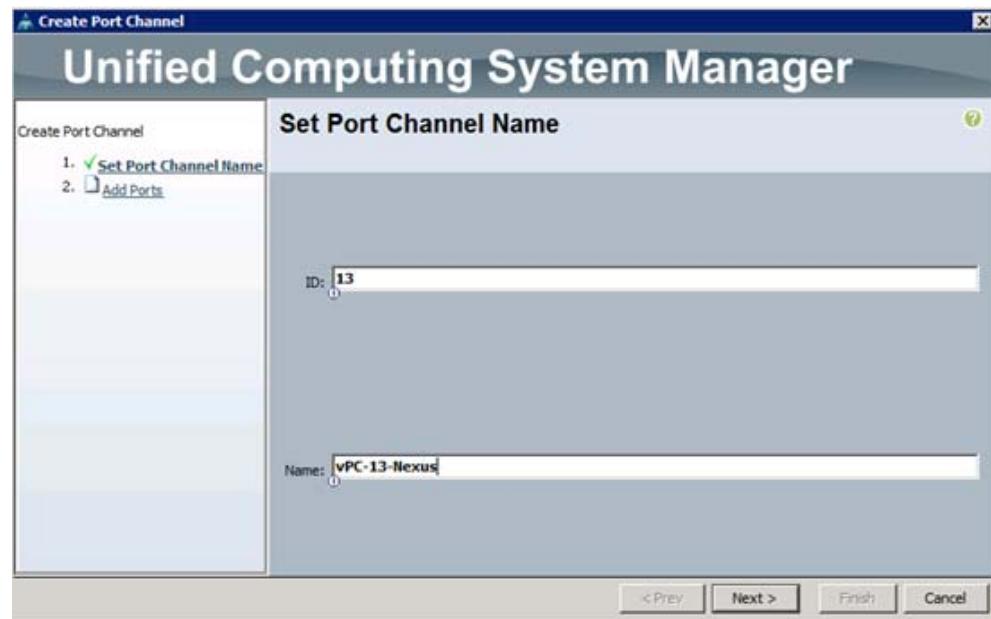
To configure the necessary port channels out of the Cisco UCS environment, complete the following steps:

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 switches and one from fabric B to both Cisco Nexus switches.

2. Under LAN > LAN Cloud, expand the Fabric A tree.
3. Right-click Port Channels.
4. Select Create Port Channel.



5. Enter 13 as the unique ID of the port channel.
6. Enter vPC-13-Nexus as the name of the port channel.
7. Click Next.
8. Select the following ports to be added to the port channel:
 - Slot ID 1 and port 27
 - Slot ID 1 and port 28
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. Select Create Port Channel.
15. Enter 14 as the unique ID of the port channel.
16. Enter vPC-14-NEXUS as the name of the port channel.
17. Click Next.
18. Select the following ports to be added to the port channel:
 - Slot ID 1 and port 27
 - Slot ID 1 and port 28
19. Click >> to add the ports to the port channel.
20. Click Finish to create the port channel.
21. Click OK.

Create MAC Address Pools

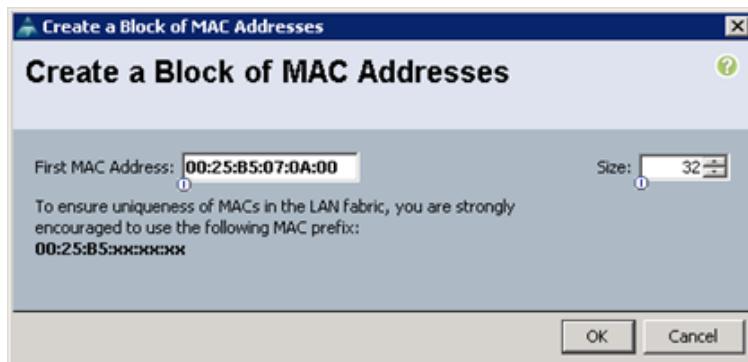
To configure the necessary MAC address pools for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select 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. Select Create MAC Pool to create the MAC address pool.

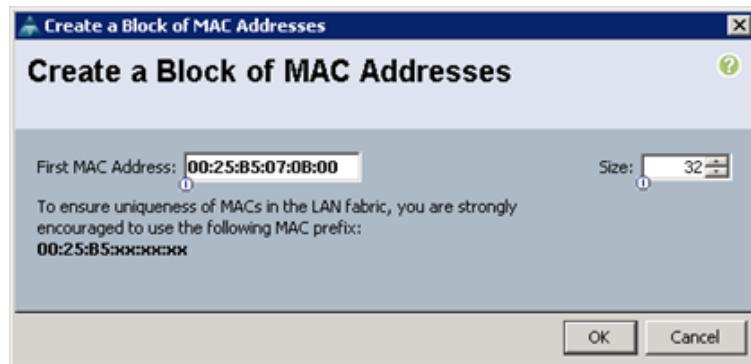


5. Enter MAC_Pool_A as the name of the MAC pool.
6. Optional: Enter a description for the MAC pool.
7. Click Next.
8. Click Add.
9. Specify a starting MAC address.



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.
11. Click OK.
12. Click Finish.
13. In the confirmation message, click OK.
14. Right-click MAC Pools under the root organization.
15. Select 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, it is recommended 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
22. Click OK.
23. Click Finish.
24. In the confirmation message, click OK.

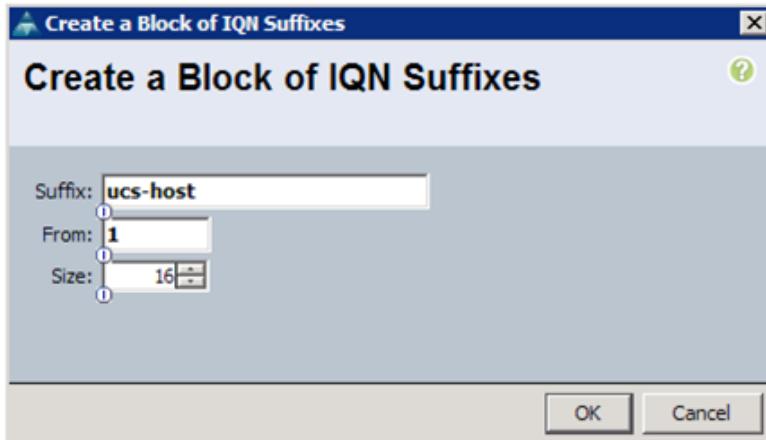
Create IQN Pools for iSCSI Boot

To configure the necessary IQN pools for the Cisco UCS environment, complete the following steps.

Cisco UCS Manager

1. Select the SAN tab on the left.
2. Select Pools > root.
3. Right-click IQN Pools under the root organization.
4. Select Create IQN Suffix Pool to create the IQN pool.
5. Enter `IQN_Pool` for the name of the IQN pool.
6. Optional: Enter a description for the IQN pool.
7. Enter `iqn.1992-08.com.cisco` as the prefix
8. Select Sequential for Assignment Order.
9. Click Next.
10. Click Add.

11. Enter ucs-host as the suffix.
12. Enter 1 in the From field.
13. Specify a size of the IQN block sufficient to support the available server resources.
14. Click OK.



15. Click Finish.
16. In the message box that displays, click OK.

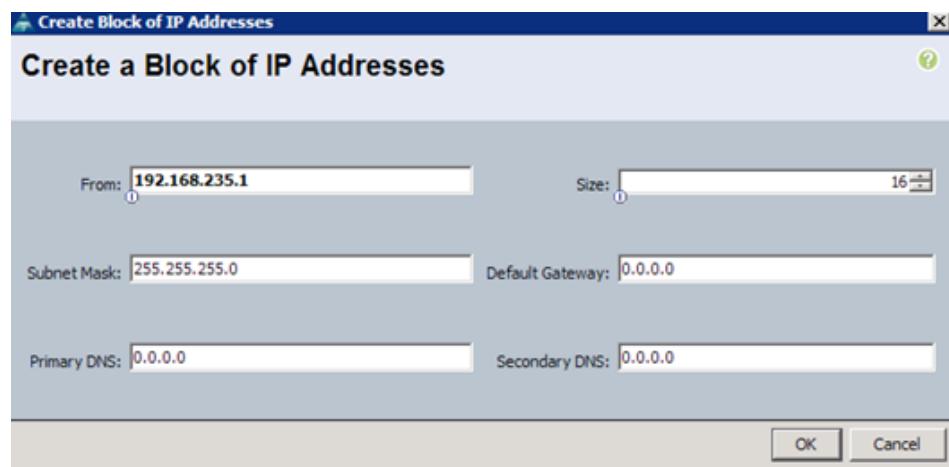
Create IP Pools for iSCSI Boot

These steps provide details for configuring the necessary IP pools iSCSI boot for the Cisco UCS environment.

Cisco UCS Manager

1. Select the LAN tab on the left.
2. Select Pools > root.
3. Two IP pools are created, one for each switching fabric.
4. Right-click IP Pools under the root organization.
5. Select Create IP Pool to create the IP pool.
6. Enter iSCSI_IP_Pool_A for the name of the IP pool.
7. Optional: Enter a description of the IQN pool.
8. Select Sequential for Assignment Order.
9. Click Next.
10. Click Add.
11. In the From field, enter the beginning of the range to assign as iSCSI IP addresses.
12. Set the size to enough addresses to accommodate the servers.
13. Click OK.
14. Click Finish.
15. Right-click IP Pools under the root organization.

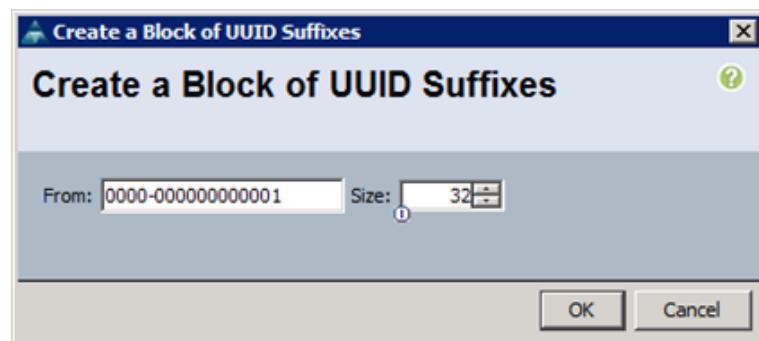
16. Select Create IP Pool to create the IP pool.
17. Enter `iSCSI_IP_Pool_B` for the name of the IP pool.
18. Optional: Enter a description of the IQN pool.
19. Select Sequential for Assignment Order.
20. Click Next.
21. Click Add.
22. In the From field, enter the beginning of the range to assign as iSCSI IP addresses.
23. Set the size to enough addresses to accommodate the servers.
24. Click OK.
25. Click Finish.



Create UUID Suffix Pool

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

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Pools > root.
3. Right-click UUID Suffix Pools.
4. Select 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.
12. Click OK.
13. Click Finish.
14. Click OK.

Create Server Pool

To configure the necessary server pool for the Cisco UCS environment, complete the following steps:

1. Consider creating unique server pools to achieve the granularity that is required in your environment.
2. In Cisco UCS Manager, click the Servers tab in the navigation pane.
3. Select Pools > root.
4. Right-click Server Pools.
5. Select Create Server Pool.
6. Enter `Infra_Pool` as the name of the server pool.
7. Optional: Enter a description for the server pool.
8. Click Next.
9. Select two (or more) servers to be used for the VMware management cluster and click `>>` to add them to the `Infra_Pool` server pool.
10. Click Finish.
11. Click OK.

Create VLANs

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

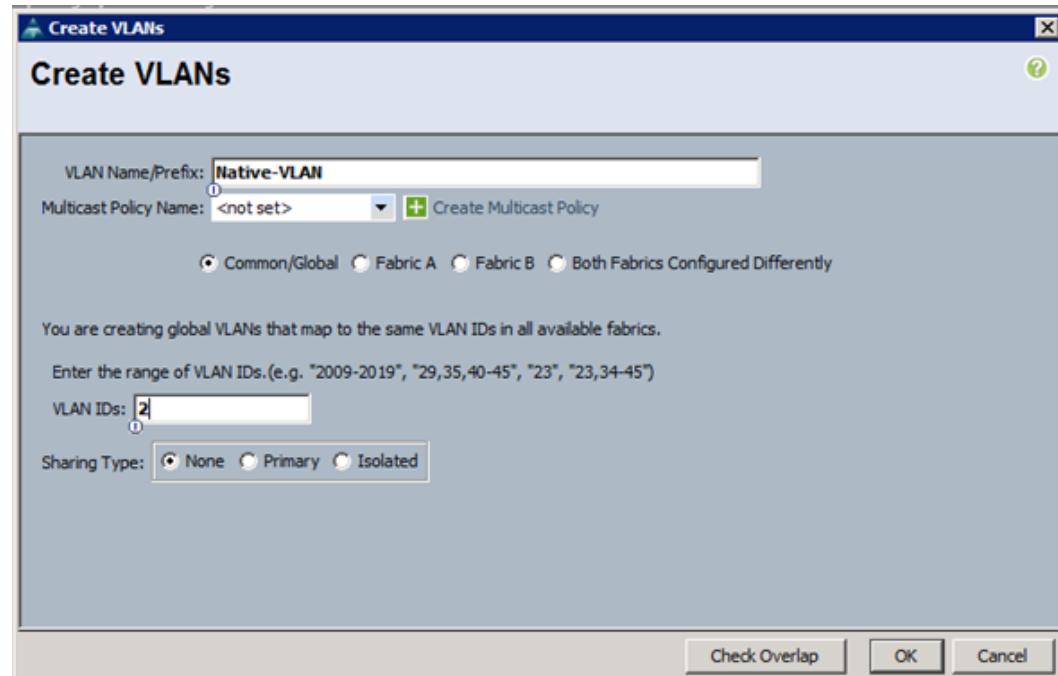
1. In Cisco UCS Manager, click the LAN tab in the navigation pane.



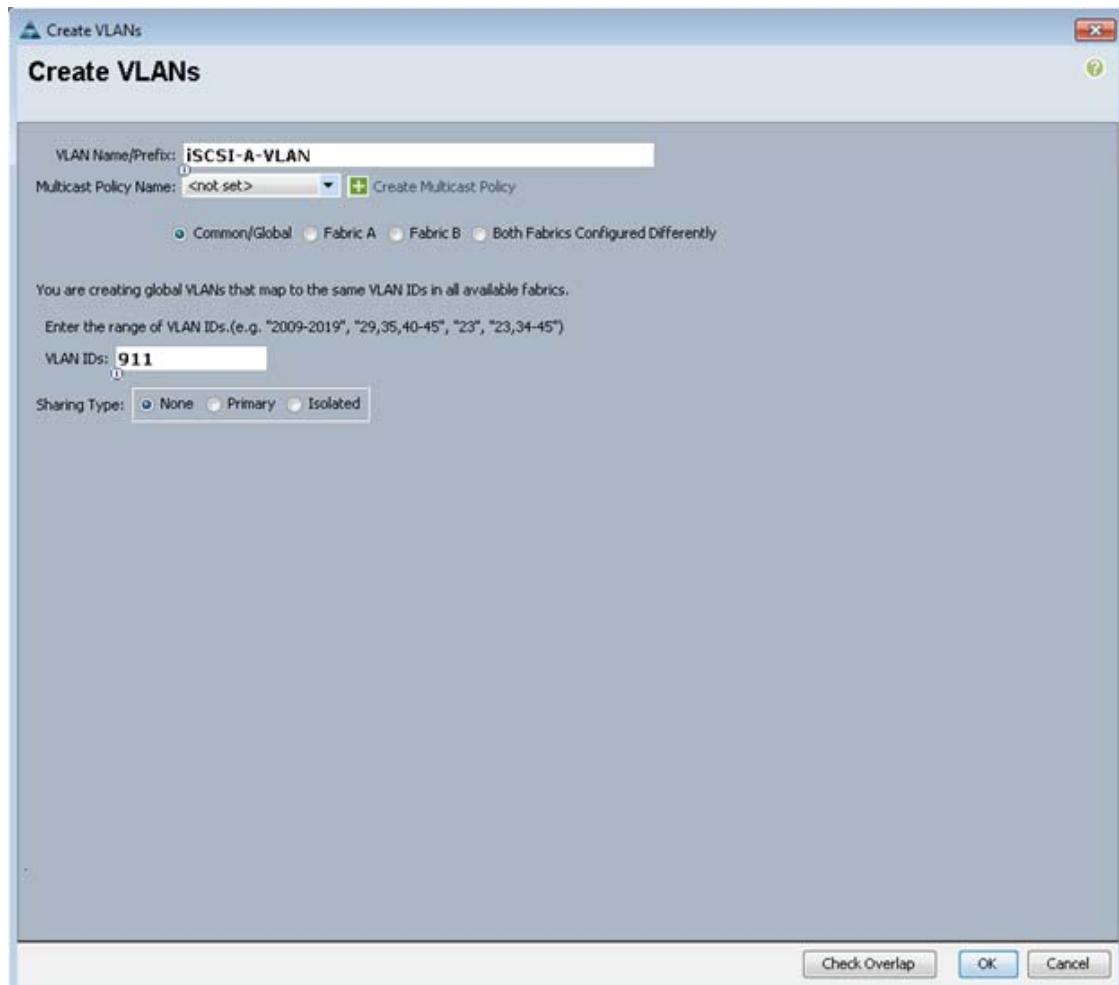
Note In this procedure, four unique VLANs and a range of 100 VLANs for APIC are created. The VLAN IDs used in this step are shown in [Table 2](#).

2. Select LAN > LAN Cloud.
3. Right-click VLANs.
4. Select Create VLANs.
5. Enter `Native-VLAN` as the name of the VLAN to be used as the native VLAN.

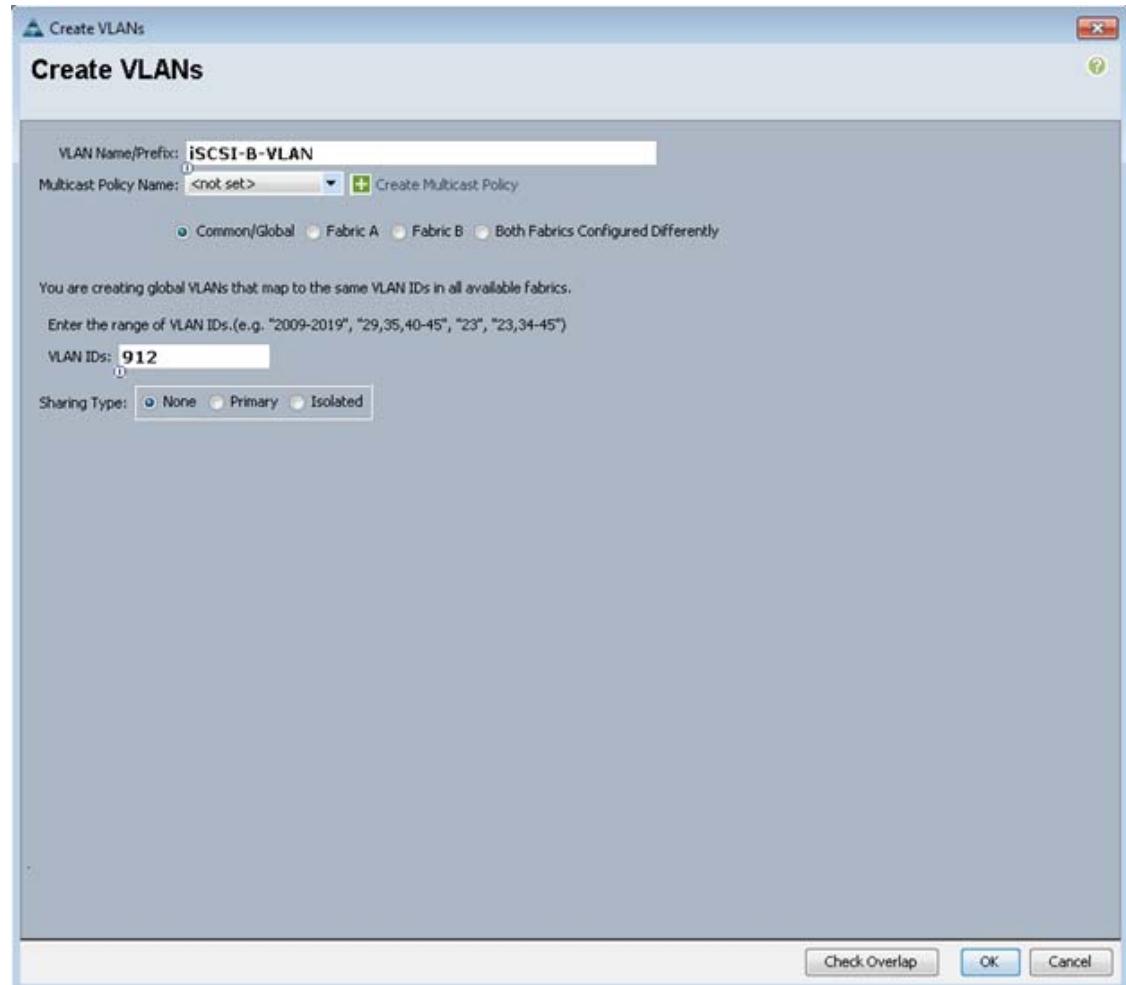
6. Keep the Common/Global option selected for the scope of the VLAN.
7. Enter the <2> as the ID of the native VLAN.
8. Keep the Sharing Type as None.
9. Click OK, and then click OK again.



10. Expand the list of VLANs in the navigation pane, right-click the newly created Native-VLAN and select Set as Native VLAN.
11. Click Yes, and then click OK.
12. Right-click VLANs.
13. Select Create VLANs.
14. Enter iSCSI-A-VLAN as the name of the VLAN to be used for the first iSCSI VLAN.
15. Keep the Common/Global option selected for the scope of the VLAN.
16. Enter the VLAN ID for the first iSCSI VLAN.
17. Click OK, then OK.

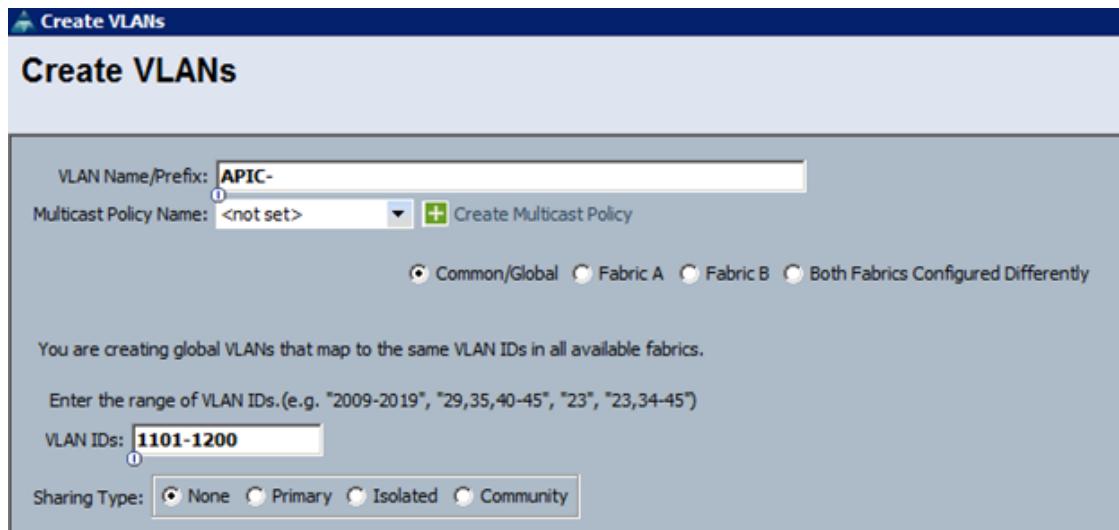


18. Right-click VLANs.
19. Select Create VLANs.
20. Enter iSCSI-B-VLAN as the name of the VLAN to be used for the second iSCSI VLAN.
21. Keep the Common/Global option selected for the scope of the VLAN.
22. Enter the VLAN ID for the second iSCSI VLAN.
23. Click OK, then OK.



24. Right-click VLANs.
25. Select Create VLANs
26. Enter OOB-Mgmt as the name of the VLAN to be used for management traffic.
27. Keep the Common/Global option selected for the scope of the VLAN.
28. Enter <3177> as the ID of the management VLAN.
29. Keep the Sharing Type as None.
30. Click OK, and then click OK again.
31. Right-click VLANs.
32. Select Create VLANs.
33. Enter INFRA-NFS as the name of the VLAN to be used for NFS VMk ports.
34. Keep the Common/Global option selected for the scope of the VLAN.
35. Enter the <3270> for the NFS VLAN.
36. Keep the Sharing Type as None.
37. Click OK, and then click OK again.
38. Right-click VLANs.

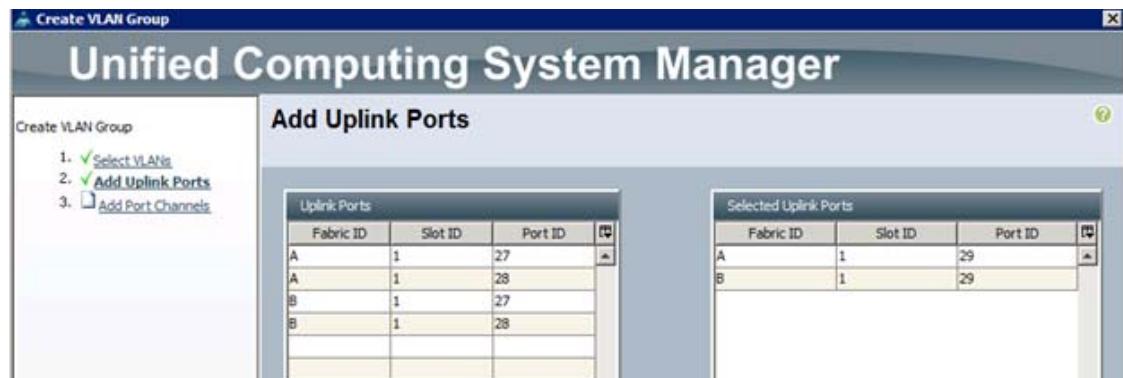
39. Select Create VLANs.
40. Enter APIC- as the prefix of the VLAN to be used for APIC.
41. Keep the Common/Global option selected for the scope of the VLAN.
42. Enter the <1101-1200> for VLAN IDs.
43. Keep the Sharing Type as None.
44. Click OK, and then click OK again.



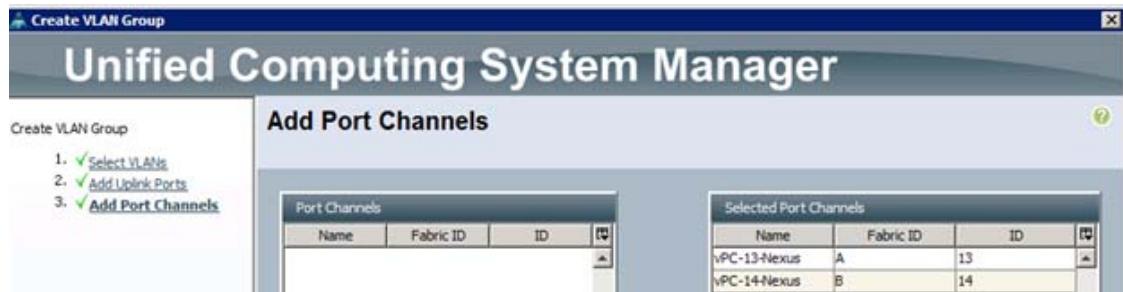
Create VLANs Groups

To configure split layer-2 domain in UCS, two VLAN groups need to be created and attached to different uplink ports. In the procedure below, a VLAN group OOB-Mgmt is configured only with out of band management VLAN (3177) and is attached to port 19 on each Fabric Interconnect. VLAN group Uplink-PortChannel is configured to carry all the remaining VLANs and is attached to port-channel 13 and 14.

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select LAN > LAN Cloud.
3. Right-click VLAN Groups.
4. Select Create VLAN Group.
5. Use OOB-Mgmt as the VLAN Group Name
6. Select the Native-VLAN (2) and OOB-Mgmt VLAN (3177). Click the radio button to set Native-VLAN as native VLAN.
7. Click Next to add Uplink Ports. Select Port 29 on both Fabric Interconnect A and B.



8. Click Finish.
9. Right-click VLAN Groups.
10. Select Create VLAN Group.
11. Use Uplink-PortChannel as the VLAN Group Name.
12. Select the Infra-NFS (3270), iSCSI-A-VLAN (911), iSCSI-B-VLAN (912) and APIC-1101 through APIC-1200 (all 100) VLANs.
13. Click Next twice to add Uplink Port Channels. Select Port Channel 13 and 14.



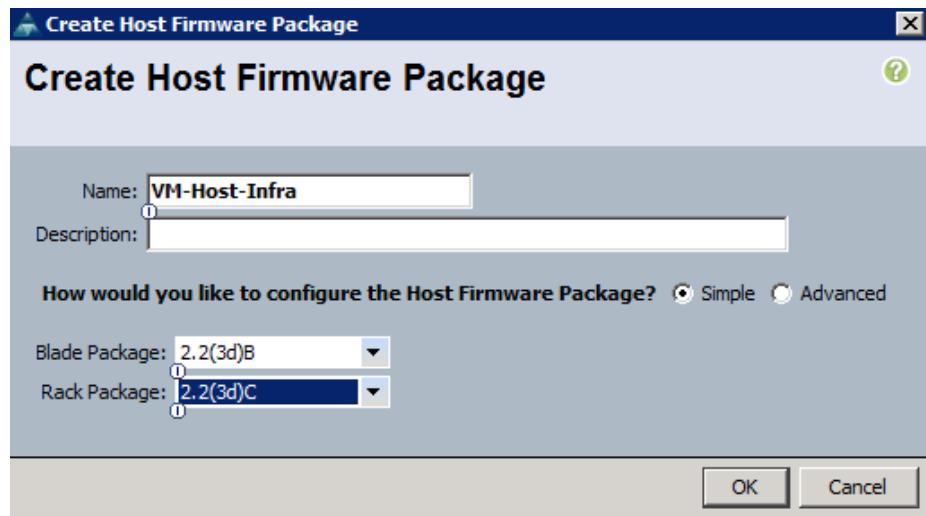
14. Click Finish.

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, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Host Firmware Packages.
4. Select Create Host Firmware Package.

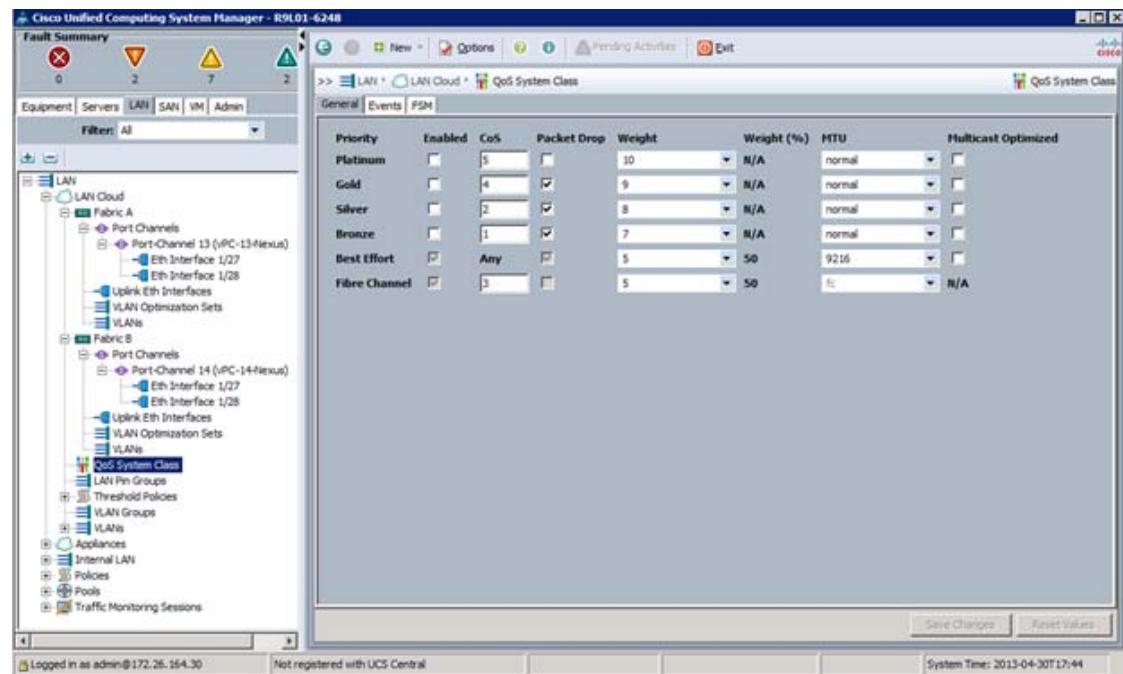


5. Enter VM-Host-Infra as the name of the host firmware package.
6. Leave Simple selected.
7. Select the version 2.2(3d) for both the Blade and Rack Packages.
8. Click OK to create the host firmware package.
9. Click OK.

Set Jumbo Frames in Cisco UCS Fabric

To configure jumbo frames and enable quality of service in the Cisco UCS fabric, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select 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 in the bottom of the window.
6. Click OK.

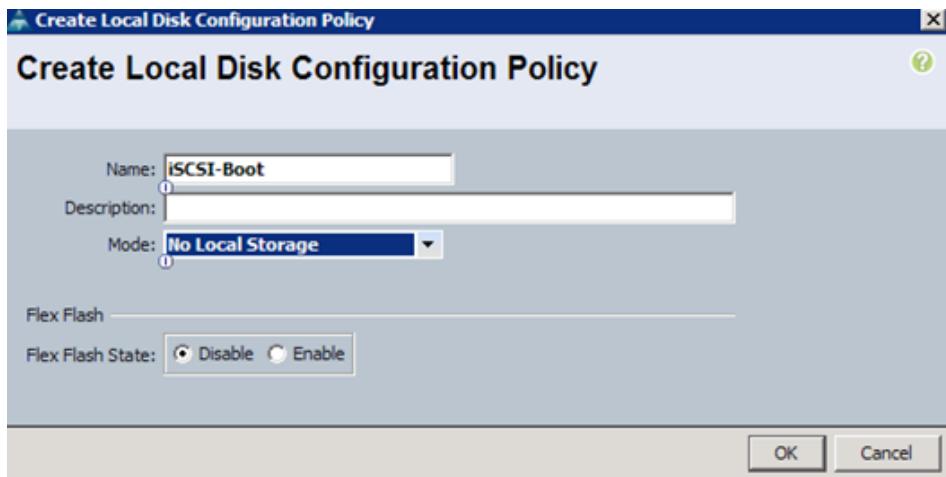
Create a Local Disk Configuration Policy (Optional)

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, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Local Disk Config Policies.
4. Select Create Local Disk Configuration Policy.

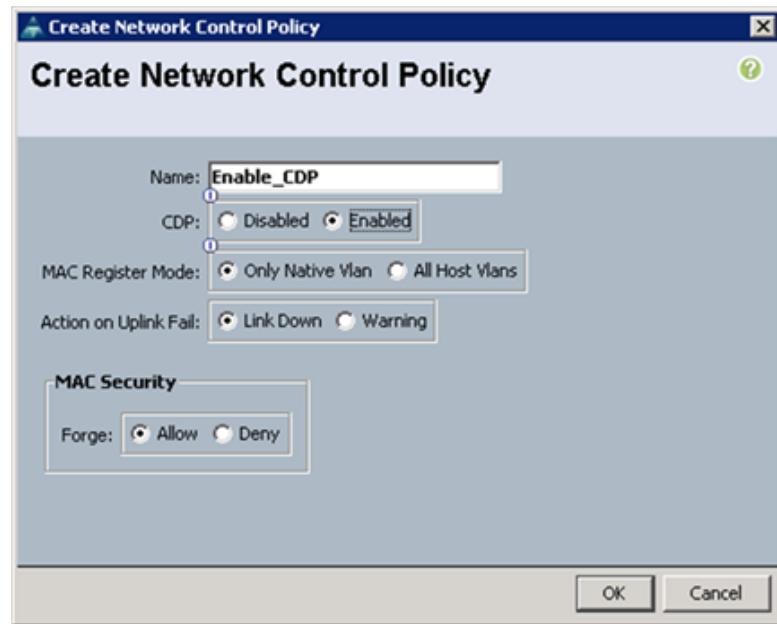


5. Enter iSCSI-Boot as the local disk configuration policy name.
6. Change the mode to No Local Storage.
7. Click OK to create the local disk configuration policy.
8. Click OK.

Create Network Control Policy for Cisco Discovery Protocol

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

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click Network Control Policies.
4. Select Create Network Control Policy.

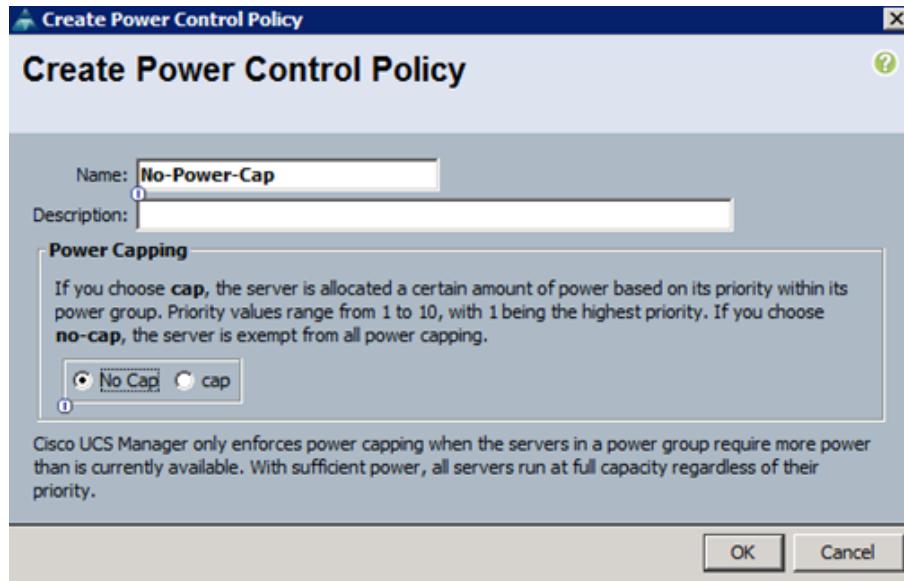


5. Enter Enable_CDP as the policy name.
6. For CDP, select the Enabled option.
7. Click OK to create the network control policy.
8. Click OK.

Create Power Control Policy

To create a power control policy for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Power Control Policies.
4. Select 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.

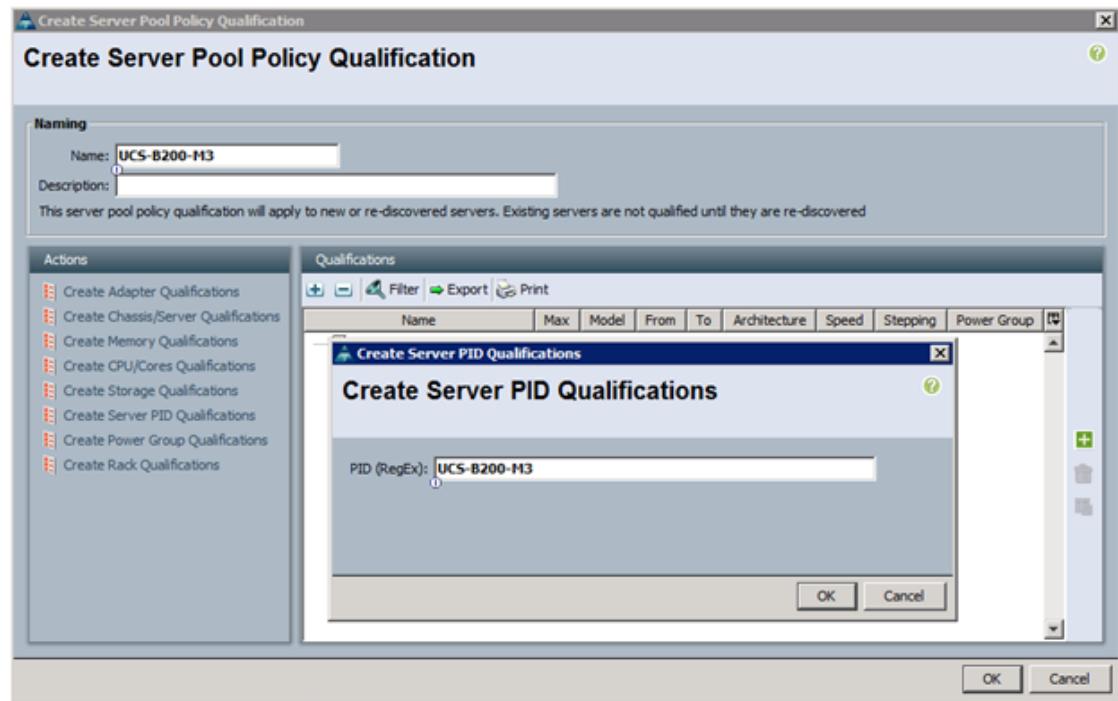
Create Server Pool Qualification Policy (Optional)

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



Note This example creates a policy for a Cisco UCS B200-M3 server.

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Server Pool Policy Qualifications.
4. Select Create Server Pool Policy Qualification.

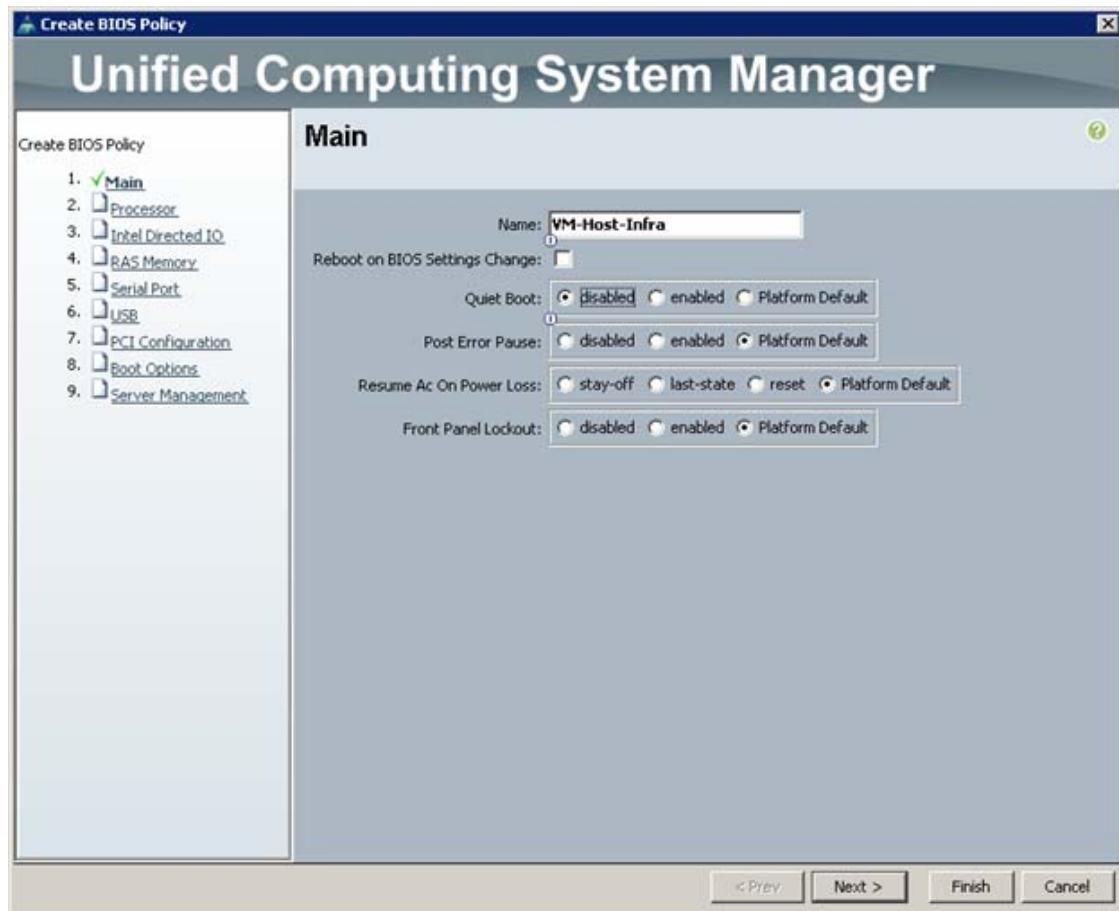


5. Enter UCSB-B200-M3 as the name for the policy.
6. Select Create Server PID Qualifications.
7. Enter UCSB-B200-M3 as the PID.
8. Click OK to create the server pool qualification policy.
9. Click OK, and then click OK again.

Create Server BIOS Policy

To create a server BIOS policy for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click BIOS Policies.
4. Select Create BIOS Policy.

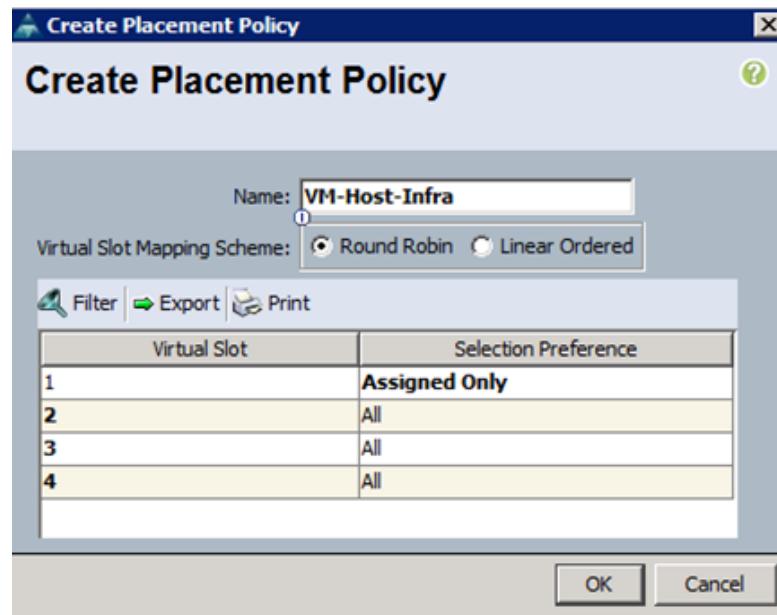


5. Enter VM-Host-Infra as the BIOS policy name.
6. Change the Quiet Boot setting to Disabled.
7. Click Finish to create the BIOS policy.
8. Click OK.

Create vNIC/vHBA Placement Policy for Virtual Machine Infrastructure Hosts

To create a vNIC/vHBA placement policy for the infrastructure hosts, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click vNIC/vHBA Placement Policies.
4. Select Create Placement Policy.

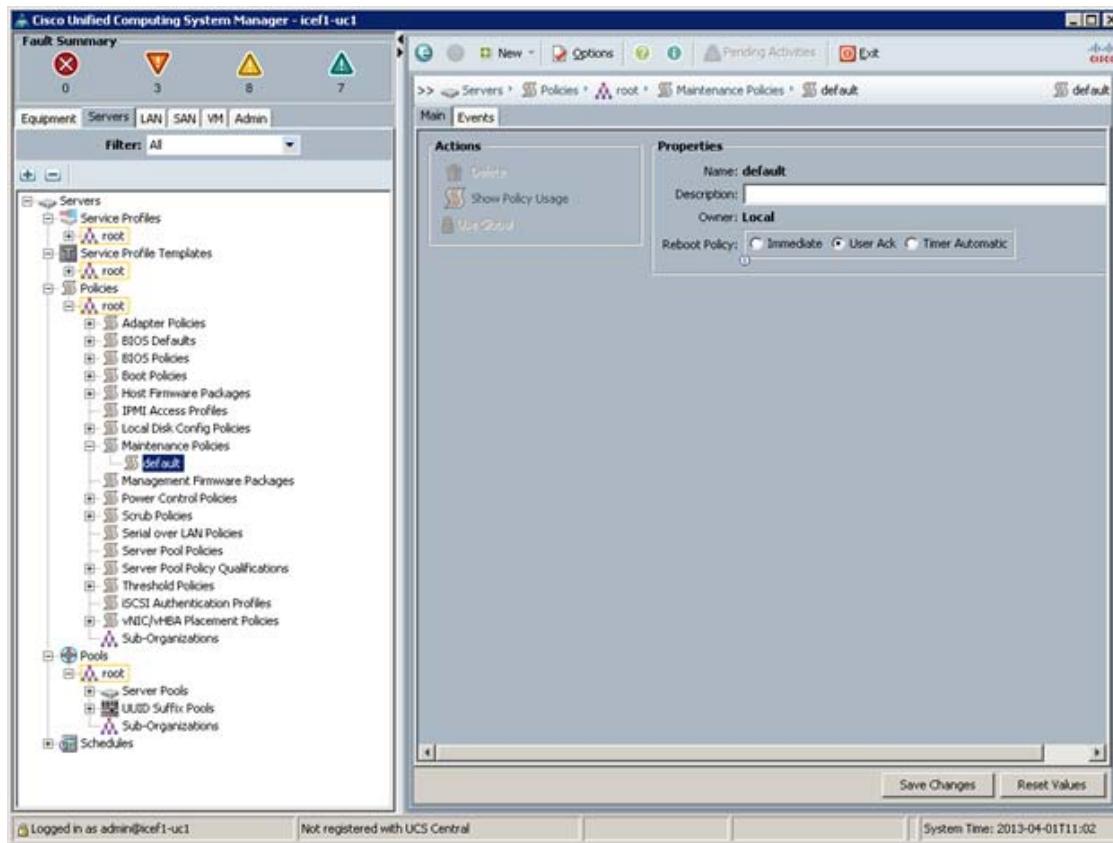


5. Enter VM-Host-Infra as the name of the placement policy.
6. Click 1 and select Assigned Only.
7. Click OK, and then click OK again.

Update Default Maintenance Policy

To update the default Maintenance Policy, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Select Maintenance Policies > default.



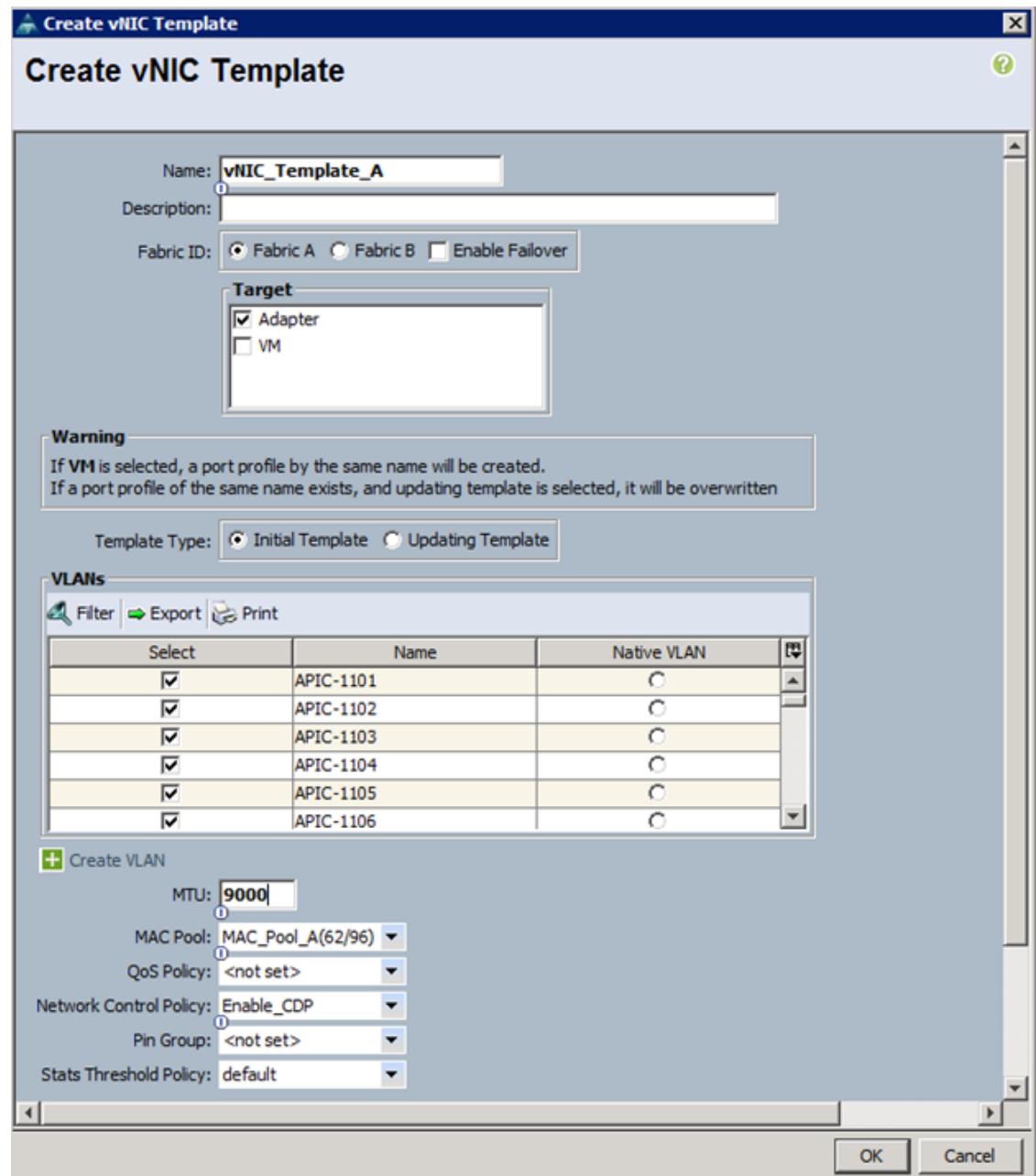
4. Change the Reboot Policy to User Ack.
5. Click Save Changes.
6. Click OK to accept the change.

Create vNIC Templates

To create multiple virtual network interface card (vNIC) templates for the Cisco UCS environment, complete the following steps. A total of eight vNIC Templates will be created. Infrastructure ESXi hosts use all eight templates (8 vNICs) while the application ESXi servers utilize only six (6 vNICs).

Create Data vNICs

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.



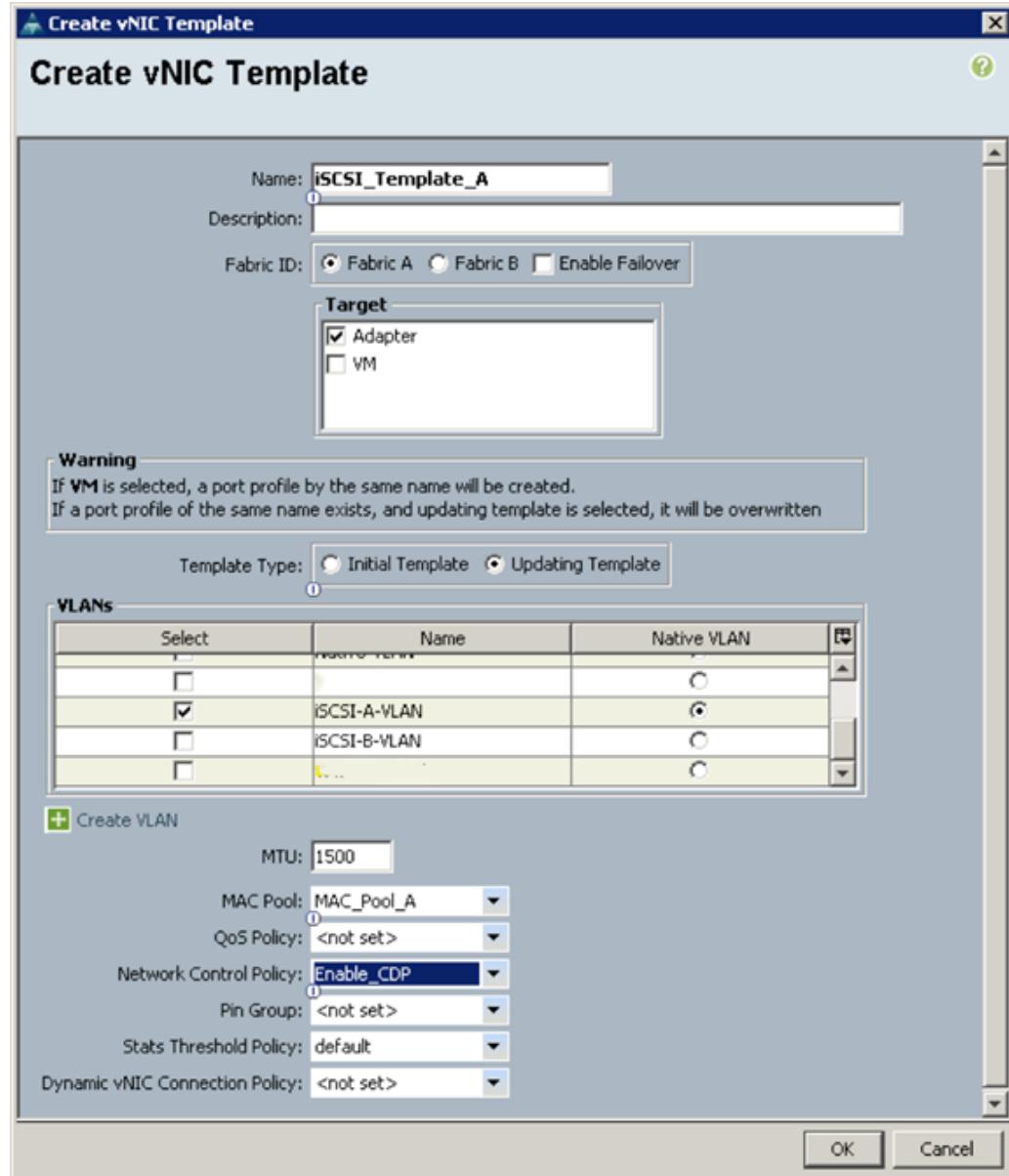
5. Enter `vNIC_Template_A` as the vNIC template name.
6. Keep Fabric A selected.
7. Do not select the Enable Failover checkbox.
8. Under Target, make sure that the VM checkbox is not selected.
9. Select Updating Template as the Template Type.
10. Under VLANs, select the checkboxes for APIC-1101 through APIC-1200, and default VLANs.
11. Set `default` as the native VLAN.

12. For MTU, enter 9000.
13. In the MAC Pool list, select `MAC_Pool_A`.
14. In the Network Control Policy list, select `Enable_CDP`.
15. Click OK to create the vNIC template.
16. Click OK.
17. In the navigation pane, select the LAN tab.
18. Select Policies > root.
19. Right-click vNIC Templates.
20. Select Create vNIC Template
21. Enter `vNIC_Template_B` as the vNIC template name.
22. Select Fabric B.
23. Do not select the Enable Failover checkbox.
24. Under Target, make sure the VM checkbox is not selected.
25. Select Updating Template as the template type.
26. Under VLANs, select the checkboxes for APIC-1101 through APIC-1200, and default VLANs.
27. Set `default` as the native VLAN.
28. For MTU, enter 9000.
29. In the MAC Pool list, select `MAC_Pool_B`.
30. In the Network Control Policy list, select `Enable_CDP`.
31. Click OK to create the vNIC template.
32. Click OK.

Create iSCSI vNICs

1. Select the LAN tab on the left.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter `iSCSI_Template_A` as the vNIC template name.
6. Leave Fabric A selected. Do not select the Enable Failover checkbox.
7. Under Target, make sure that the VM checkbox is not selected.
8. Select Updating Template for Template Type.
9. Under VLANs, select `iSCSI-A-VLAN (911)`.
10. Set `iSCSI-A-VLAN` as the native VLAN.
11. Under MTU, enter 1500.
12. From the MAC Pool list, select `MAC_Pool_A`.
13. From the Network Control Policy list, select `Enable_CDP`.
14. Click OK to complete creating the vNIC template.

15. Click OK.



16. Select the LAN tab on the left.
 17. Select Policies > root.
 18. Right-click vNIC Templates.
 19. Select Create vNIC Template.
 20. Enter iSCSI_Template_B as the vNIC template name.
 21. Select Fabric B. Do not select the Enable Failover checkbox.
 22. Under Target, make sure that the VM checkbox is not selected.
 23. Select Updating Template for Template Type.
 24. Under VLANs, select iSCSI-B-VLAN (912).

25. Set iSCSI-B-VLAN as the native VLAN.
26. Under MTU, enter 1500.
27. From the MAC Pool list, select MAC_Pool_B.
28. From the Network Control Policy list, select Enable_CDP.
29. Click OK to complete creating the vNIC template.
30. Click OK.

Create oob Mgmt vNICs

1. Select the LAN tab on the left.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter OOB-A as the vNIC template name.
6. Leave Fabric A selected. Do not select the Enable Failover checkbox.
7. Under Target, make sure that the VM checkbox is not selected.
8. Select Updating Template for Template Type.
9. Under VLANs, select OOB-Mgmt VLAN and Native-VLAN.
10. Set Native-VLAN as the native VLAN.
11. Under MTU, enter 1500. From the MAC Pool list, select MAC_Pool_A.
12. From the Network Control Policy list, select Enable_CDP.
13. Click OK to complete creating the vNIC template.
14. Click OK.
15. Select the LAN tab on the left.
16. Select Policies > root.
17. Right-click vNIC Templates.
18. Select Create vNIC Template.
19. Enter OOB-B as the vNIC template name.
20. Select Fabric B. Do not select the Enable Failover checkbox.
21. Under Target, make sure that the VM checkbox is not selected.
22. Select Updating Template for Template Type.
23. Under VLANs, select OOB-Mgmt VLAN and Native-VLAN.
24. Set Native-VLAN as the native VLAN.
25. Under MTU, enter 1500. From the MAC Pool list, select MAC_Pool_B.
26. From the Network Control Policy list, select Enable_CDP.
27. Click OK to complete creating the vNIC template.
28. Click OK.

Create Infrastructure NFS vNICs

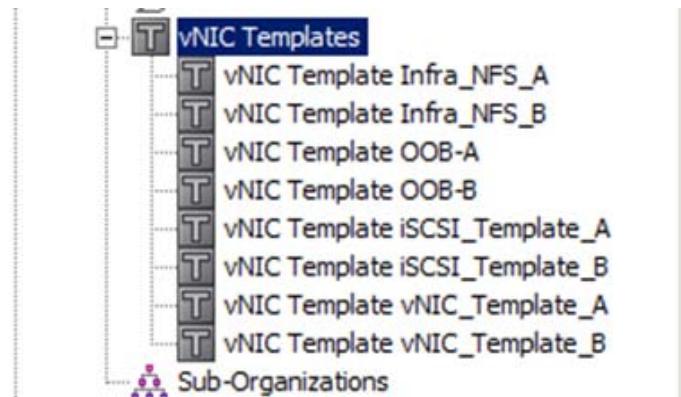


Note These vNICs will only be utilized on ESXi servers hosting Infrastructure services.

1. Select the LAN tab on the left.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter `Infra_NFS_A` as the vNIC template name.
6. Leave Fabric A selected. Do not select the Enable Failover checkbox.
7. Under Target, make sure that the VM checkbox is not selected.
8. Select Updating Template for Template Type.
9. Under VLANs, select `Infra-NFS (3270)` VLAN and `default`.
10. Set `default` as the native VLAN.
11. Under MTU, enter 9000. From the MAC Pool list, select `MAC_Pool_A`.
12. From the Network Control Policy list, select `Enable_CDP`.
13. Click OK to complete creating the vNIC template.
14. Click OK.
15. Select the LAN tab on the left.
16. Select Policies > root.
17. Right-click vNIC Templates.
18. Select Create vNIC Template.
19. Enter `Infra_NFS_B` as the vNIC template name.
20. Select Fabric B. Do not select the Enable Failover checkbox.
21. Under Target, make sure that the VM checkbox is not selected.
22. Select Updating Template for Template Type.
23. Under VLANs, select `Infra-NFS` VLAN and `default VLAN`.
24. Set `default` as the native VLAN.
25. Under MTU, enter 9000. From the MAC Pool list, select `MAC_Pool_B`.
26. From the Network Control Policy list, select `Enable_CDP`.
27. Click OK to complete creating the vNIC template.
28. Click OK.

At the end of the vNIC template creation, there should be eight vNIC templates available in the Cisco UCS Manager as shown in [Figure 3](#).

Figure 3 vNIC Templates



Create Boot Policies

This procedure applies to a Cisco UCS environment in which two iSCSI logical interfaces (LIFs) are on cluster node 1 (`iscsi_lif01a` and `iscsi_lif01b`) and two iSCSI LIFs are on cluster node 2 (`iscsi_lif02a` and `iscsi_lif02b`). One boot policy is configured in this procedure. This policy configures the primary target to be `iscsi_lif01a`.

To create boot policies for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Boot Policies.
4. Select Create Boot Policy.

The screenshot shows the "Properties" dialog for a new boot policy named "Boot-Fabric-A". The "Actions" panel includes options for Delete, Show Policy Usage, and Use Default. The "Properties" section shows:

- Name: **Boot-Fabric-A**
- Description: [empty]
- Owner: **Local**
- Reboot on Boot Order Change:
- Enforce vNIC/vHBA/iSCSI Name:
- Boot Mode: Legacy Uefi

A "Warning" box states: "The type (primary/secondary) does not indicate a boot order presence. The effective order of boot devices within the same device class (LAN/Storage/SCSI) 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/vHBAs/iSCSI are selected if they exist, otherwise the vNIC/vHBA/iSCSI with the lowest PCIe bus scan order is used."

The "Boot Order" table lists the boot sequence:

Name	Order	vNIC/vHBA/iSCSI vNIC	Type
CD/DVD	1		
ISCSI	2		
ISCSI		ISCSI-A-vNIC	Primary
ISCSI		ISCSI-B-vNIC	Secondary

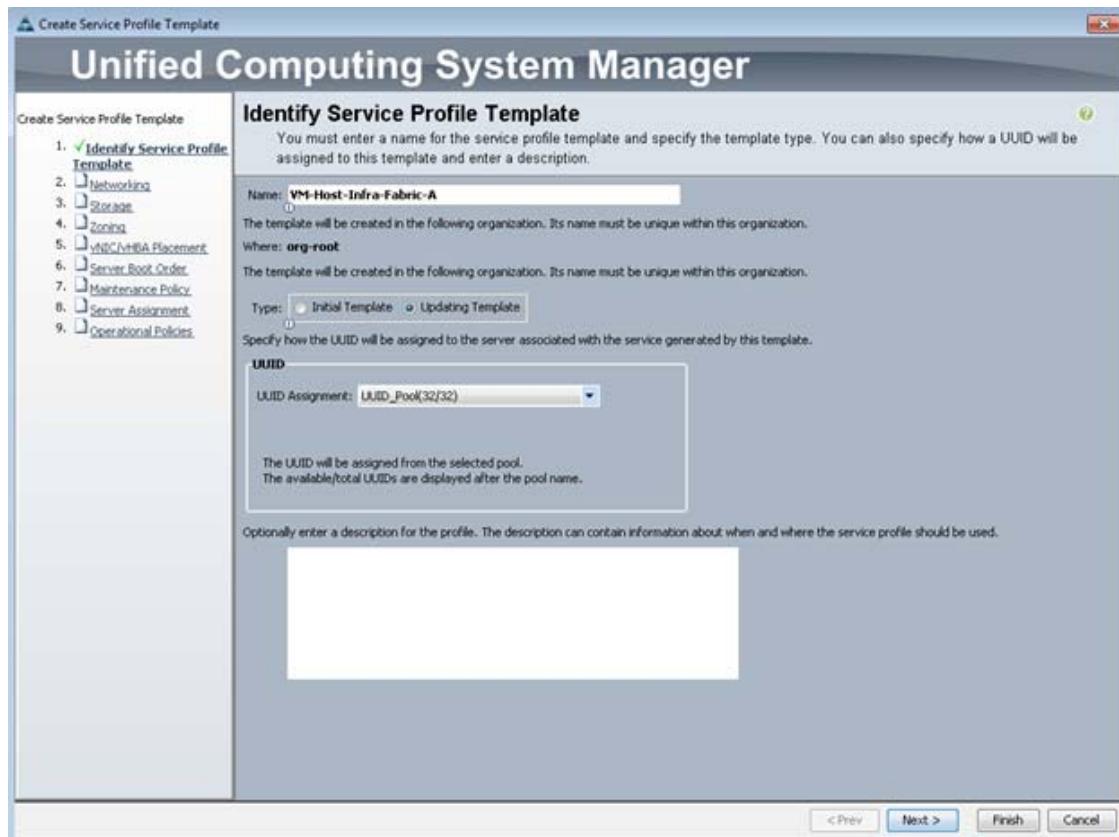
5. Enter Boot-Fabric-A as the name of the boot policy.
6. Optional: Enter a description for the boot policy.
7. Keep the Reboot on Boot Order Change option cleared.
8. Expand the Local Devices drop-down list and select Add CD-ROM.
9. Expand the iSCSI vNICs section and select Add iSCSI Boot.
10. In the Add iSCSI Boot dialog box, enter iSCSI-A-vNIC.
11. Click OK.
12. Select Add iSCSI Boot.
13. In the Add iSCSI Boot dialog box, enter iSCSI-B-vNIC.
14. Click OK.
15. Click OK to save the boot policy. Click OK to close the Boot Policy window.

Create Service Profile Template

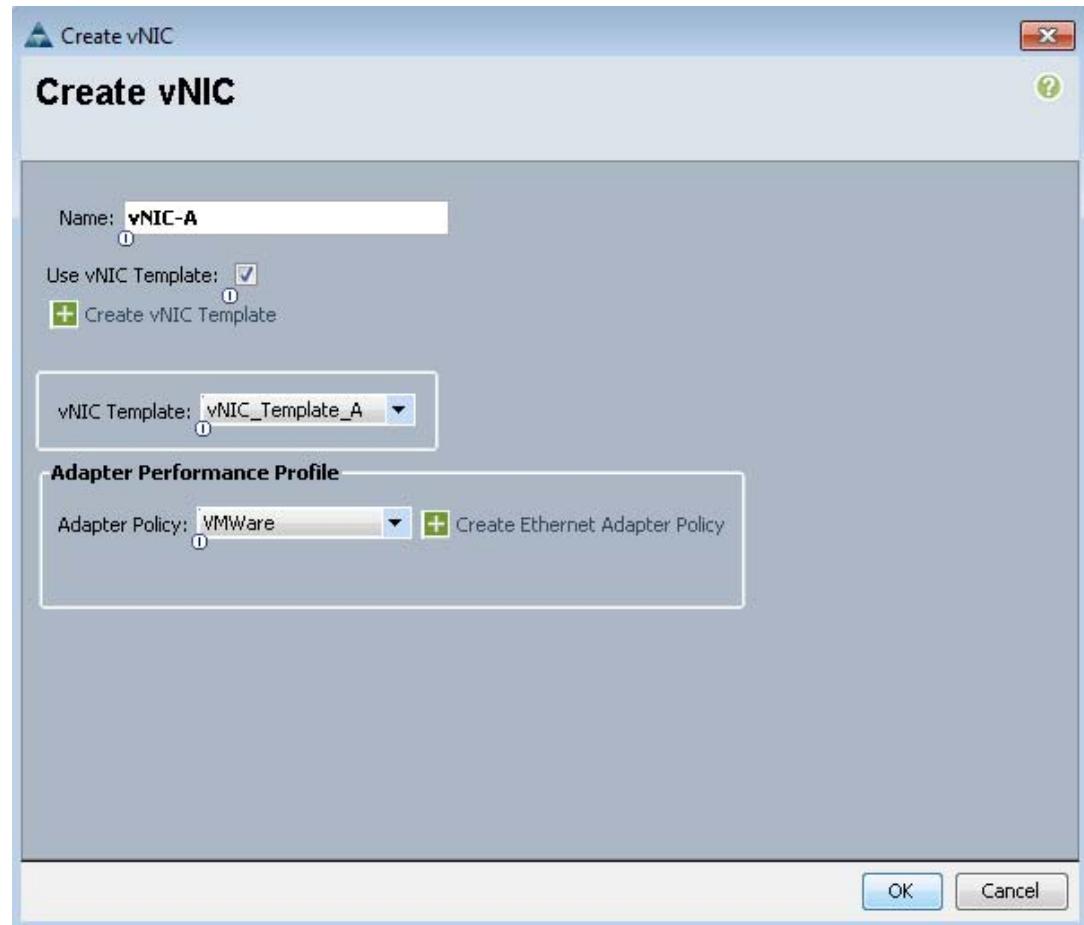
In this procedure, one service profile template for Infrastructure ESXi hosts is created for fabric A boot.

To create the service profile template, complete the following steps:

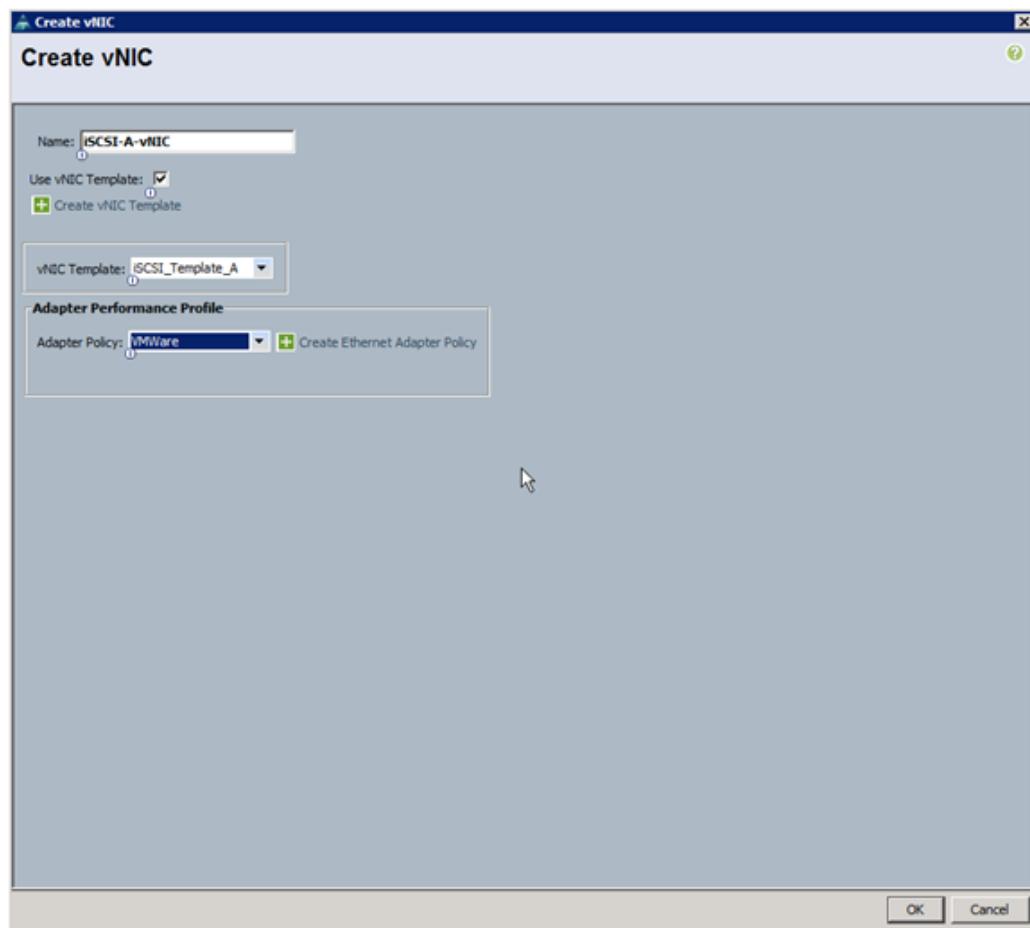
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root.
3. Right-click root.
4. Select Create Service Profile Template to open the Create Service Profile Template wizard.
5. Identify the service profile template:
 - a. Enter VM-Host-Infra-Fabric-A as the name of the service profile template. This service profile template is configured to boot from node 1 on fabric A.
 - b. Select the “Updating Template” option.
 - c. Under UUID, select UUID_Pool as the UUID pool.
 - d. Click Next.



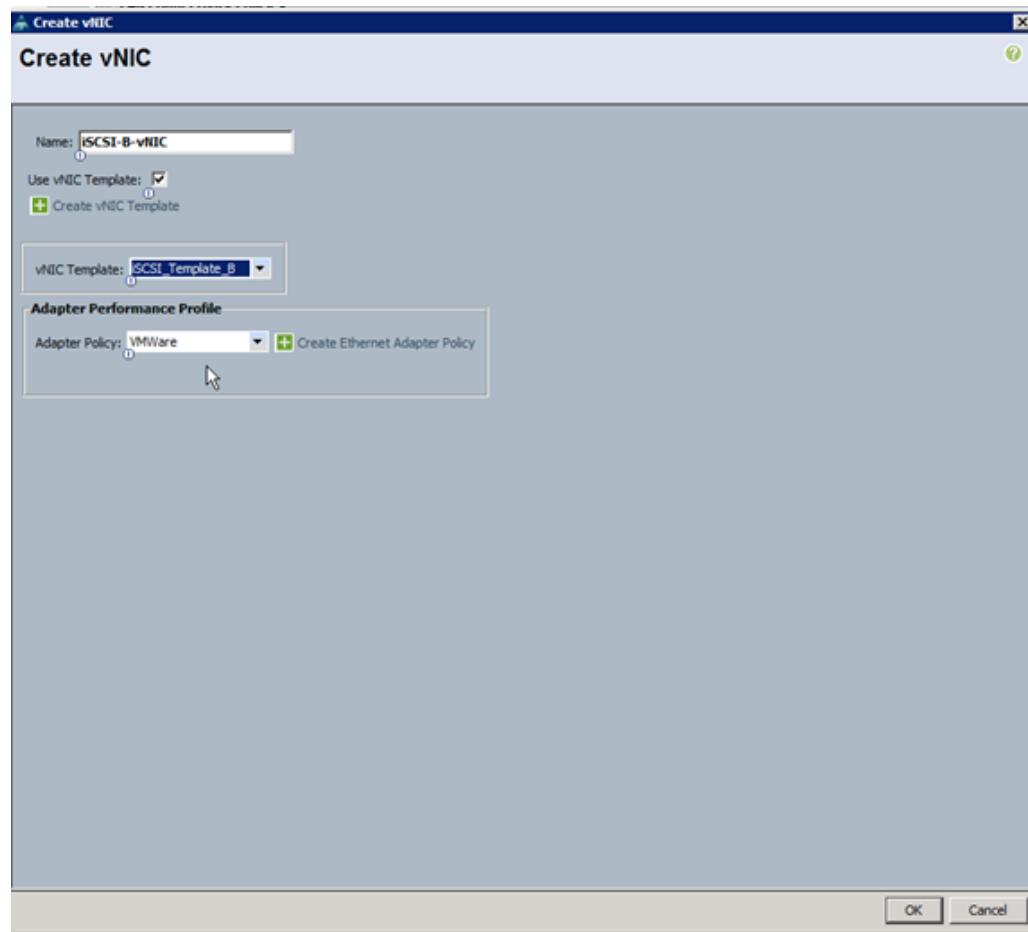
6. To configure the networking options, 8 vNIC interfaces will be added for Infrastructure ESXi hosts:
 - a. Keep the default setting for Dynamic vNIC Connection Policy.
 - b. Select the “Expert” option to configure the LAN connectivity.
 - c. Click the upper Add button to add a vNIC to the template.
 - d. In the Create vNIC dialog box, enter vNIC-A as the name of the vNIC.
 - e. Select the Use vNIC Template checkbox.
 - f. In the vNIC Template list, select vNIC_Template_A.
 - g. In the Adapter Policy list, select VMWare.
 - h. Click OK to add this vNIC to the template.



- i. On the Networking page of the wizard, click the upper Add button to add another vNIC to the template.
- j. In the Create vNIC box, enter vNIC-B as the name of the vNIC.
- k. Select the Use vNIC Template checkbox.
- l. In the vNIC Template list, select vNIC_Template_B.
- m. In the Adapter Policy list, select VMWare.
- n. Click OK to add the vNIC to the template.
- o. Click the upper Add button to add a vNIC to the template.
- p. In the Create vNIC dialog box, enter iSCSI-A-vNIC as the name of the vNIC.
- q. Select the Use vNIC Template checkbox.
- r. In the vNIC Template list, select iSCSI_Template_A.
- s. In the Adapter Policy list, select VMWare.
- t. Click OK to add this vNIC to the template.



- u. Click the upper Add button to add a vNIC to the template.



- v. In the Create vNIC dialog box, enter iSCSI-B-vNIC as the name of the vNIC.
- w. Select the Use vNIC Template checkbox.
- x. In the vNIC Template list, select iSCSI_Template_B.
- y. In the Adapter Policy list, select VMWare.
- z. Click OK to add this vNIC to the template.
- aa. On the Networking page of the wizard, click the upper Add button to add another vNIC to the template.
- ab. In the Create vNIC box, enter OOB-A as the name of the vNIC.
- ac. Select the Use vNIC Template checkbox.
- ad. In the vNIC Template list, select OOB-A.
- ae. In the Adapter Policy list, select VMWare.
- af. Click OK to add the vNIC to the template.
- ag. On the Networking page of the wizard, click the upper Add button to add another vNIC to the template.
- ah. In the Create vNIC box, enter OOB-B as the name of the vNIC.
- ai. Select the Use vNIC Template checkbox.

- aj. In the vNIC Template list, select OOB-B.
- ak. In the Adapter Policy list, select VMware.
- al. Click OK to add the vNIC to the template.

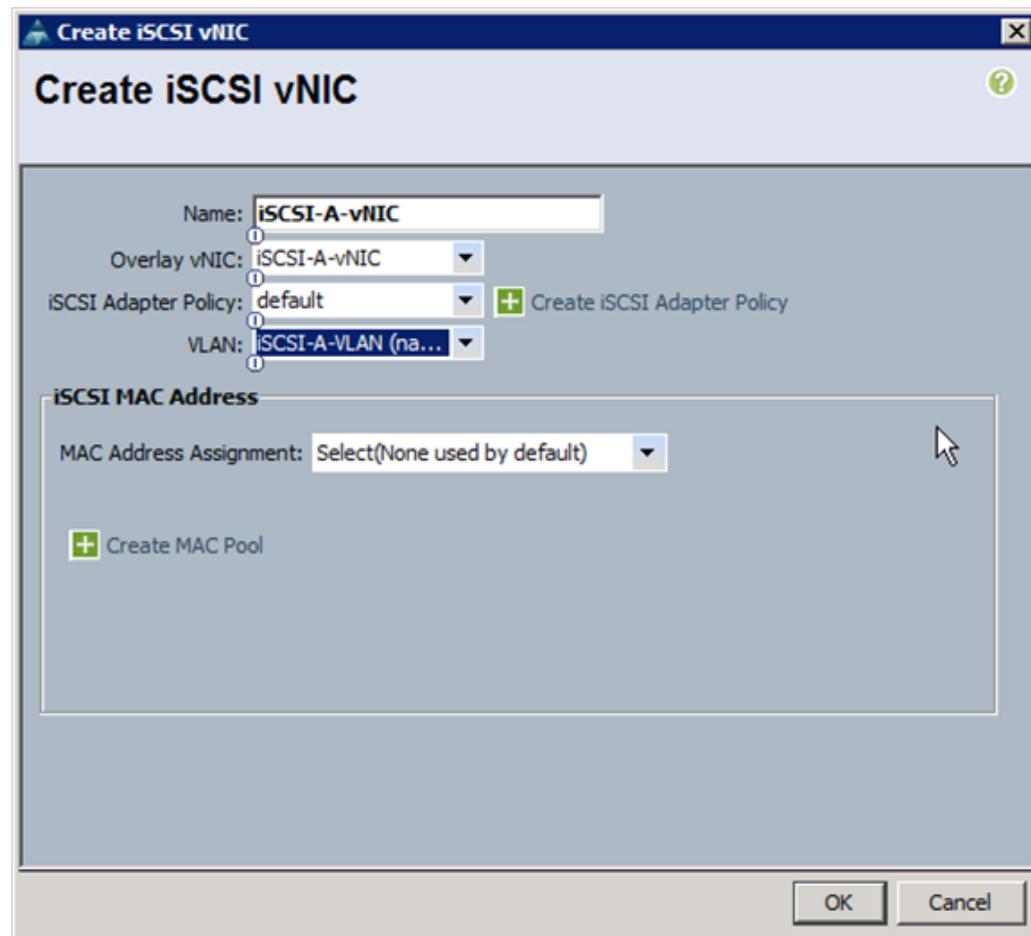


Note The next two vNIC interfaces are only needed for Infrastructure ESXi Hosts. These interfaces enable NFS access using NFS specific vSwitch and static EPG mapping. ESXi servers not hosting infrastructure VMs, use VDS for NFS access to application specific SVMs.

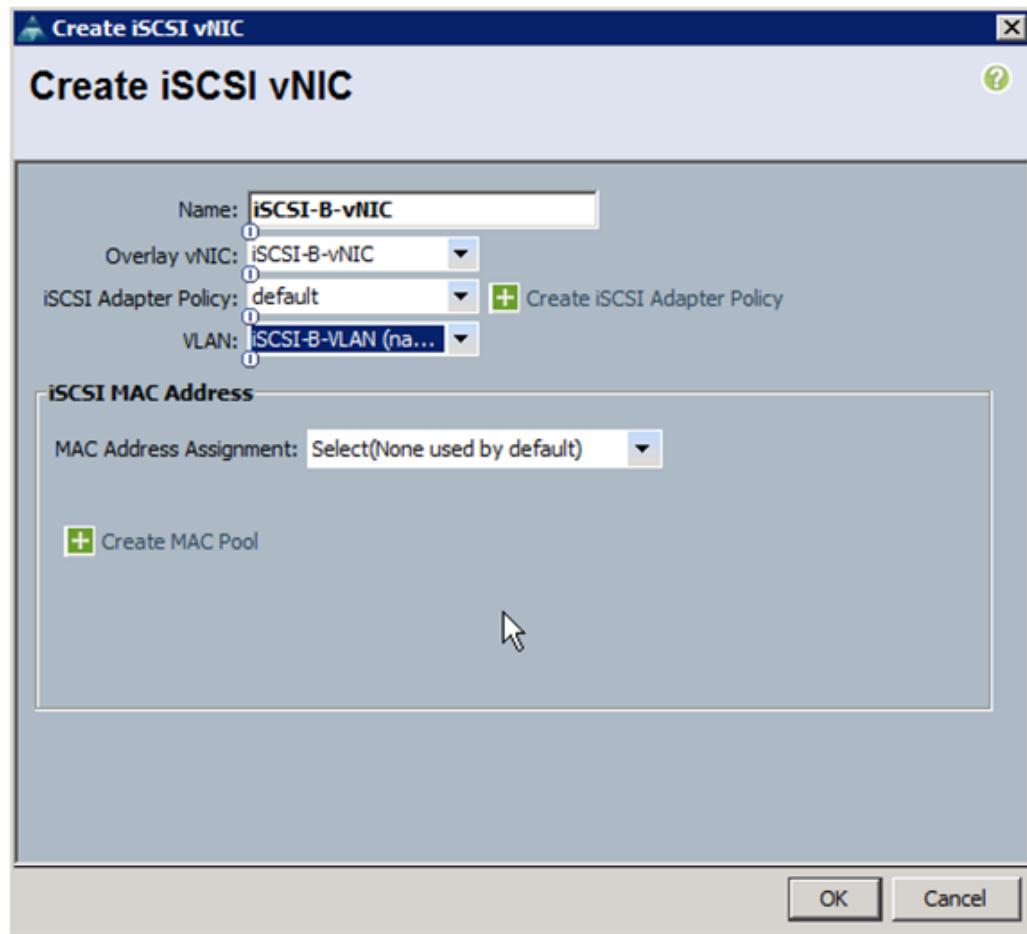
- am. On the Networking page of the wizard, click the upper Add button to add another vNIC to the template.
- an. In the Create vNIC box, enter NFS-A as the name of the vNIC.
- ao. Select the Use vNIC Template checkbox.
- ap. In the vNIC Template list, select Infra_NFS_A.
- aq. In the Adapter Policy list, select VMware.
- ar. Click OK to add the vNIC to the template.
- as. On the Networking page of the wizard, click the upper Add button to add another vNIC to the template.
- at. In the Create vNIC box, enter NFS-B as the name of the vNIC.
- au. Select the Use vNIC Template checkbox.
- av. In the vNIC Template list, select Infra_NFS_B.
- aw. In the Adapter Policy list, select VMware.
- ax. Click OK to add the vNIC to the template.
- ay. Verify that eight vNIC interfaces are present.

Name	MAC Address
vNIC NFS-A	Derived
vNIC NFS-B	Derived
vNIC OOB-A	Derived
vNIC OOB-B	Derived
vNIC iSCSI-A-vNIC	Derived
vNIC iSCSI-B-vNIC	Derived
vNIC vNIC-A	Derived
vNIC vNIC-B	Derived

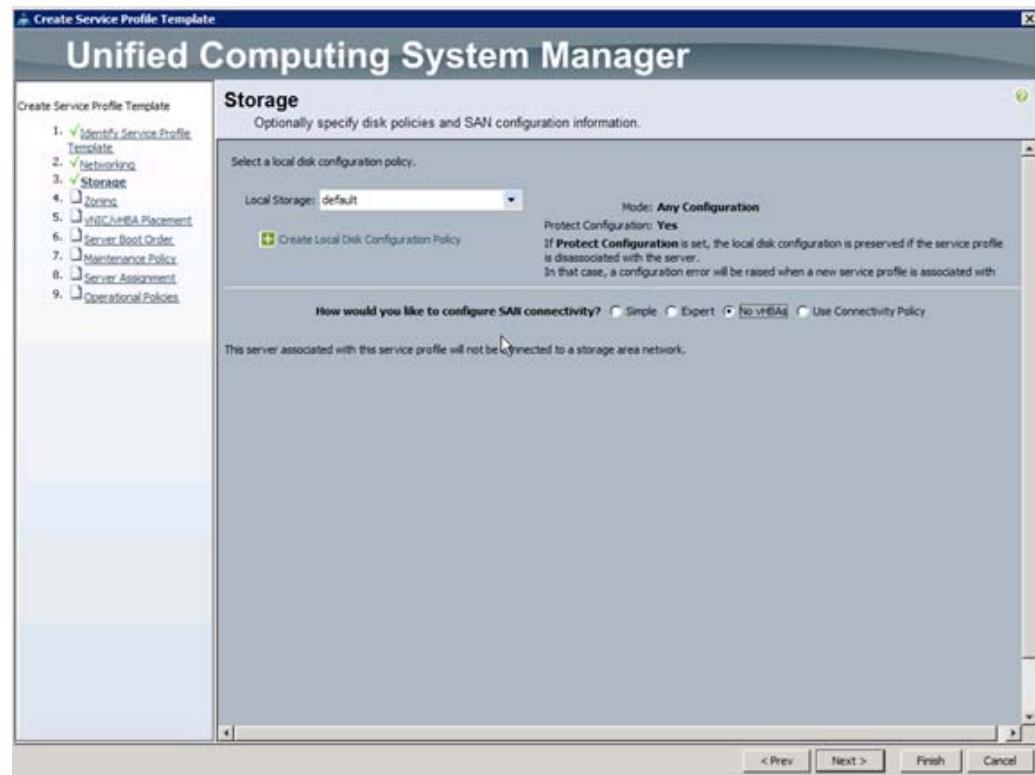
- az. Expand the iSCSI vNICs section (if not already expanded)
- ba. Select “iqn-pool” under “Initiator Name Assignment”
- bb. Click the **lower** Add button in the iSCSI vNIC section to define a vNIC.



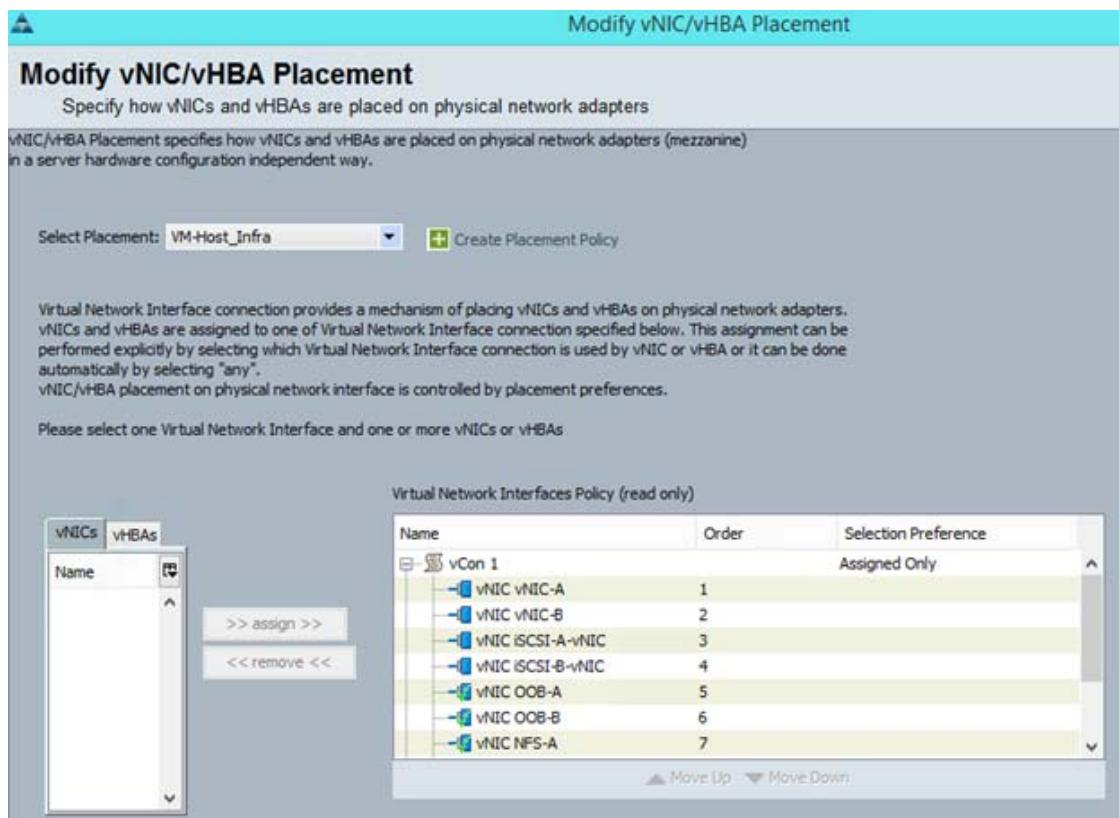
- bc. Enter iSCSI-A-vNIC as the name of the vNIC.
- bd. Select iSCSI-A-vNIC for Overlay vNIC .
- be. Set the iSCSI Adapter Policy to default.
- bf. Set the VLAN to iSCSI-A-VLAN.
- bg. Leave the MAC Address set to None.
- bh. Click OK.
- bi. Click the lower Add button in the iSCSI vNIC section to define a vNIC.



- bj. Enter **iSCSI -B -vNIC** as the name of the vNIC.
- bk. Set the Overlay vNIC to **iSCSI -B -vNIC**
- bl. Set the iSCSI Adapter Policy to **default**.
- bm. Set the VLAN to **iSCSI -B -VLAN**
- bn. Leave the MAC Address set to None.
- bo. Click OK.
- bp. Click OK.
- bq. Review the table in the Networking page to make sure that all vNICs were created.
- br. Click Next.
7. Configure the storage options:
- Select a local disk configuration policy:
 - If the server in question has local disks, select default in the Local Storage list.
 - If the server in question does not have local disks, select **iSCSI -Boot**.
 - Select the **No vHBAs** option for the “How would you like to configure SAN connectivity?” field.

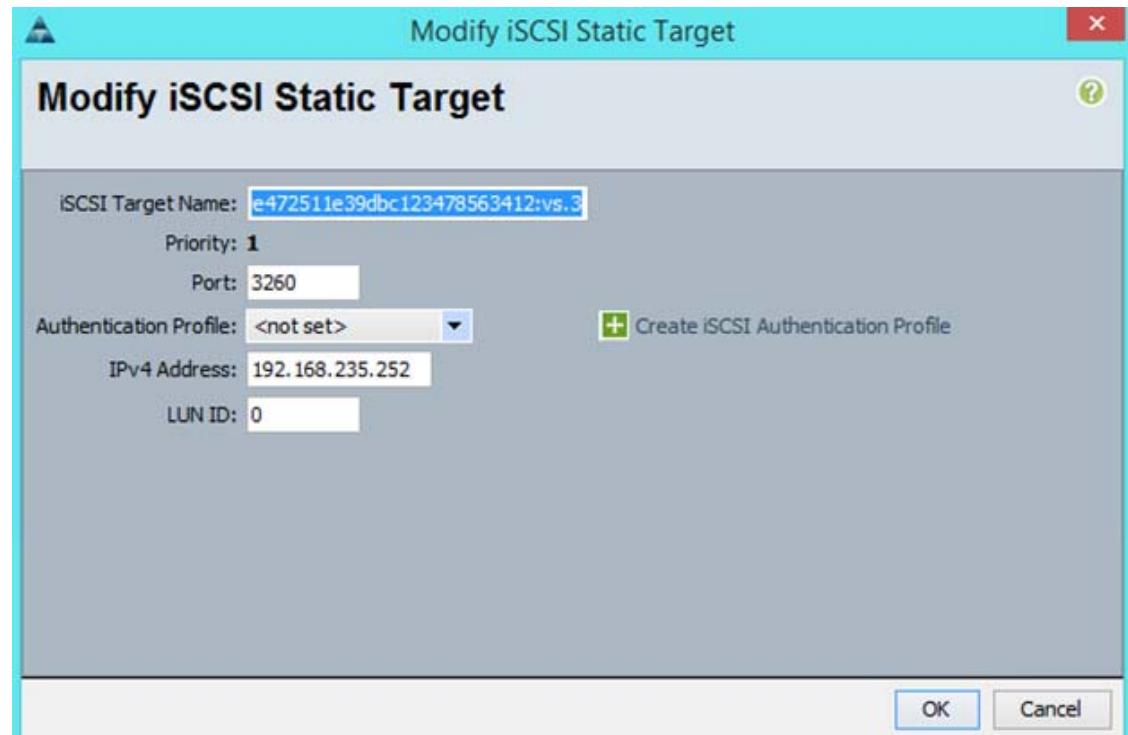


- c. Click Next.
8. Set no Zoning options and click Next.
9. Set the vNIC/vHBA placement options.

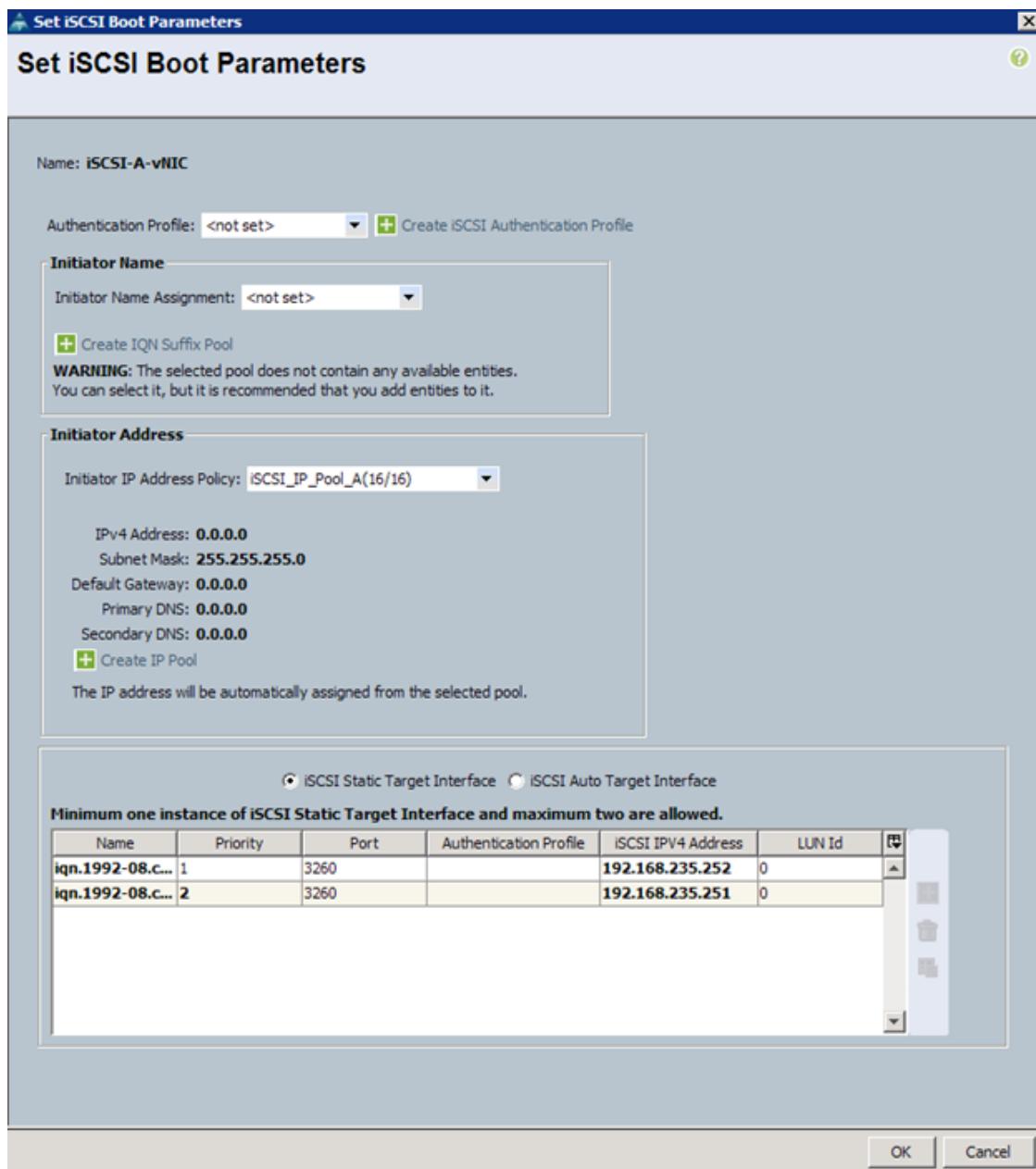


- a. In the “Select Placement” list, select the VM-Host-Infra placement policy.
 - b. Select vCon1 and assign the vHBAs/vNICs to the virtual network interfaces policy in the following order:
 - vNIC-A
 - vNIC-B
 - iSCSI-vNIC-A
 - iSCSI-vNIC-B
 - OOB-A
 - OOB-B
 - NFS-A
 - NFS-B
 - c. Review the table to verify that all vNICs and vHBAs were assigned to the policy in the appropriate order.
 - d. Click Next.
10. Set the server boot order:
- a. Select Boot-Fabric-A for Boot Policy.
 - b. In the Boot Order pane, select iSCSI -A-vNIC.
 - c. Click the “Set iSCSI Boot Parameters” button.

- d. Leave the “Set iSCSI Boot Parameters” dialog box <not set> to use the single Service Profile Initiator Name defined in the previous steps
- e. Set `iSCSI_IP_Pool_A` as the “Initiator IP address Policy”.
- f. Keep the “iSCSI Static Target Interface” button selected and click the  button.
- g. Log in to the storage cluster management interface and run the following command:
`iscsi nodename`
- h. Note or copy the iSCSI target name for `Infra_Vserver`.
- i. In the Create iSCSI Static Target dialog box, paste the iSCSI target node name from `Infra_Vserver` into the iSCSI Target Name field.

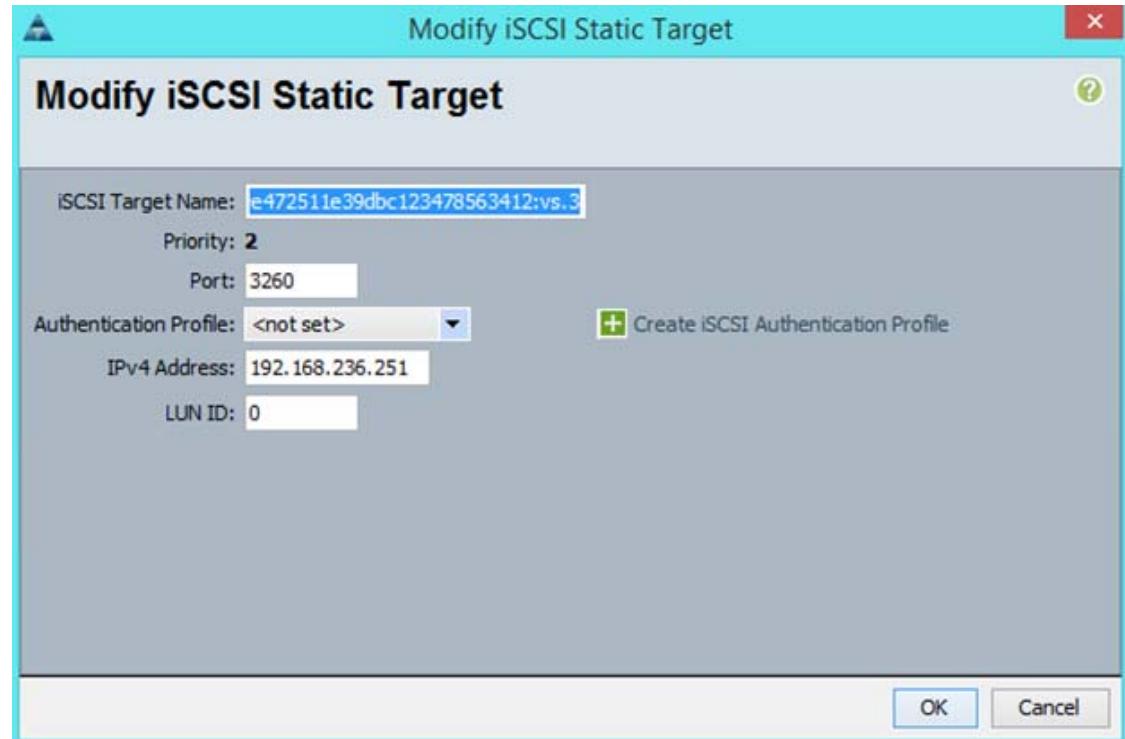


- j. Enter the IP address of `iSCSI_lif02a` for the IPv4 Address field.
- k. Click OK to add the iSCSI static target.
- l. Keep the iSCSI Static Target Interface option selected and click the  button.
- m. In the Create iSCSI Static Target window, paste the iSCSI target node name from `Infra_Vserver` into the iSCSI Target Name field.

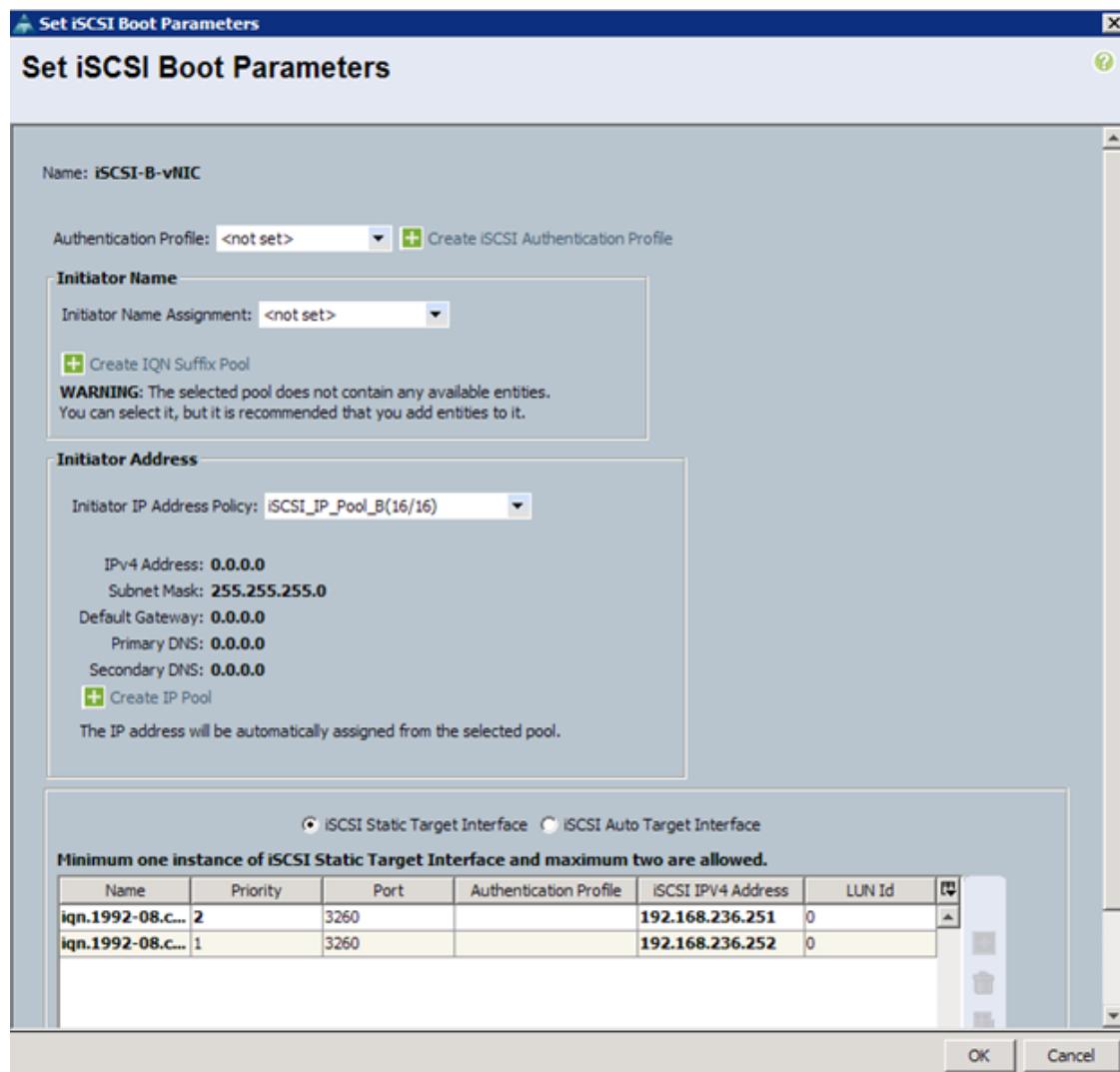


- n. Enter the IP address of `iscsi_lif01a` in the IPv4 Address field.
- o. Click OK.
- p. Click OK.
- q. In the Boot Order pane, select `iSCSI -vNIC-B`.
- r. Click the Set iSCSI Boot Parameters button.
- s. In the Set iSCSI Boot Parameters dialog box, set the leave the “Initiator Name Assignment” to `<not set>`.
- t. In the Set iSCSI Boot Parameters dialog box, set the initiator IP address policy to `iSCSI_IP_Pool_B`.

- u. Keep the iSCSI Static Target Interface option selected and click the  button.
- v. In the Create iSCSI Static Target window, paste the iSCSI target node name from Infra_Vserver into the iSCSI Target Name field (same target name as above).
- w. Enter the IP address of iscsi_lif02b in the IPv4 address field.



- x. Click OK to add the iSCSI static target.
- y. Keep the iSCSI Static Target Interface option selected and click the  button.
- z. In the Create iSCSI Static Target dialog box, paste the iSCSI target node name from Infra_Vserver into the iSCSI Target Name field.

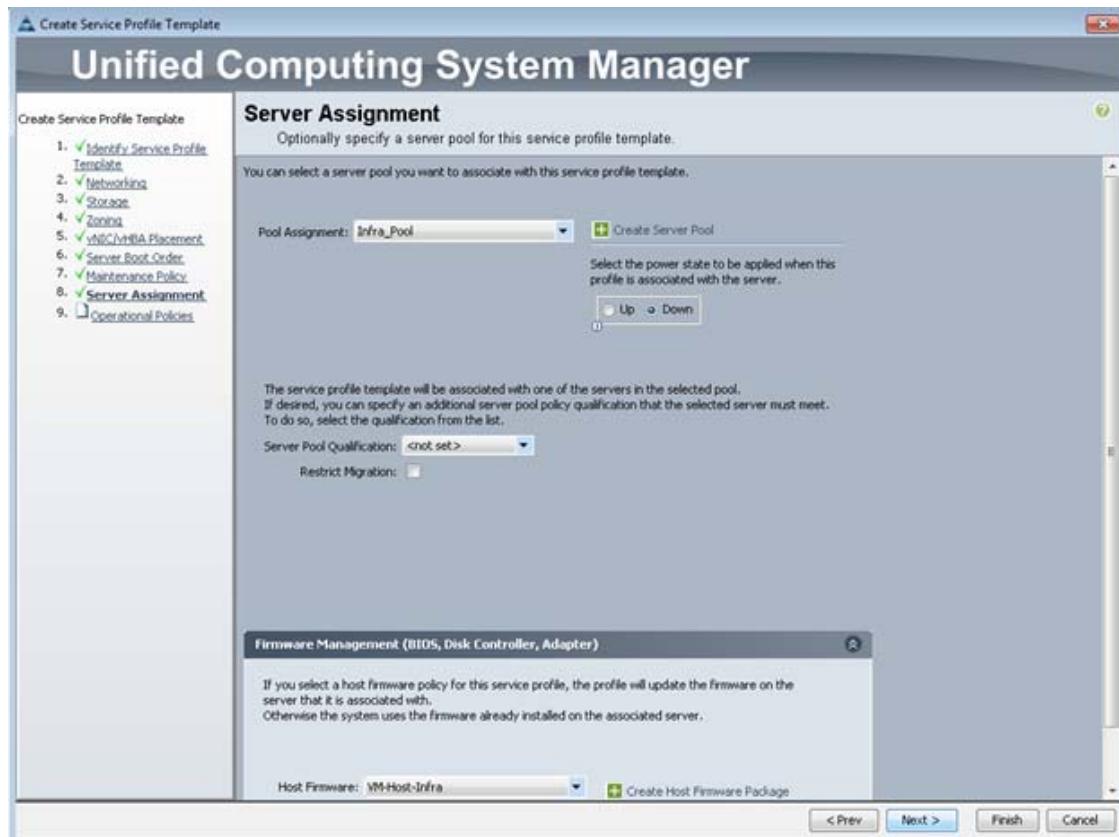


- aa. Enter the IP address of iscsi_lif01b in the IPv4 Address field.
 - ab. Click OK.
 - ac. Click OK.
 - ad. Review the table to make sure that all boot devices were created and identified. Verify that the boot devices are in the correct boot sequence.
 - ae. Click Next to continue to the next section.
11. Add a maintenance policy:
- a. Select the default Maintenance Policy.
 - b. Click Next.



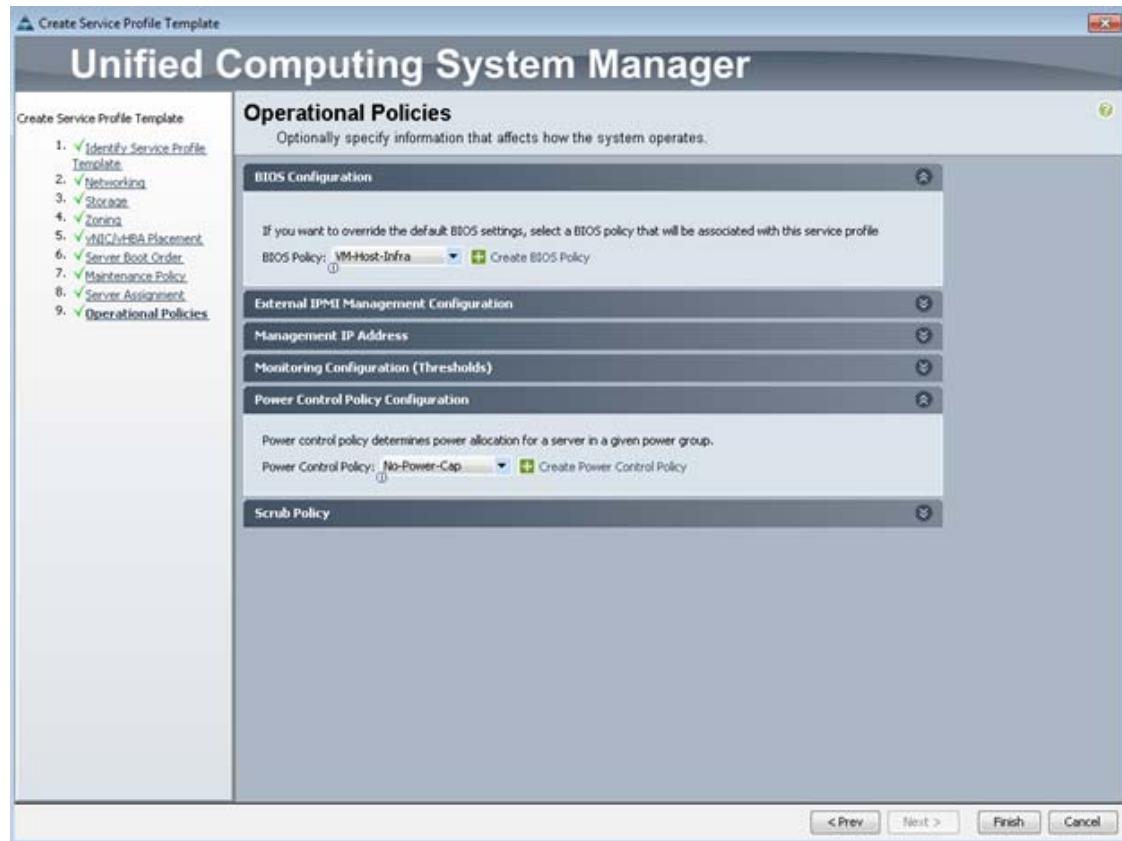
12. Specify the server assignment:

- a. In the Pool Assignment list, select `Infra_Pool`.
- b. Optional: Select a Server Pool Qualification policy.
- c. Select Down as the power state to be applied when the profile is associated with the server.
- d. Expand Firmware Management at the bottom of the page and select `VM-Host-Infra` from the Host Firmware list.
- e. Click Next.



13. Add operational policies:

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

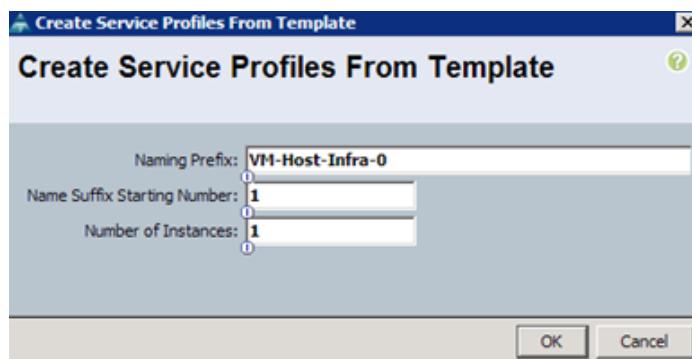


14. Click Finish to create the service profile template.
15. Click OK in the confirmation message.

Create Service Profiles

To create service profiles from the service profile template, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Service Template VM-Host-Infra-Fabric-A.
3. Right-click VM-Host-Infra-Fabric-A and select Create Service Profiles from Template.



4. Enter VM-Host-Infra-0 as the service profile prefix.
5. Enter 1 as “Name Suffix Starting Number”
6. Enter 1 as the “Number of Instances”.
7. Click OK to create the service profile.
8. Click OK in the confirmation message.

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 server and from the NetApp controllers. Insert the required information into [Table 21](#) and [Table 22](#).

Table 21 *iSCSI LIFs for iSCSI IQN*

Vserver	iSCSI Target IQN
Infra_Vserver	

To gather the iSCSI IQN, run the `iscsi show` command on the storage cluster management interface. For 7-Mode storage, run the `iscsi nodename` command on each storage controller.

Table 22 *vNIC iSCSI IQNs for Fabric A and Fabric B*

Cisco UCS Service Profile Name	iSCSI IQN	Variables
VM-Host-Infra-01		<< var_vm_host_infra_01_iqn>>
VM-Host-Infra-02		<< var_vm_host_infra_02_iqn>>



Note To gather the vNIC IQN 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 “iSCSI vNICs” tab on the right. Note “Initiator Name” displayed at the top of the page under “Service Profile Initiator Name.”

ACI Infrastructure Configuration

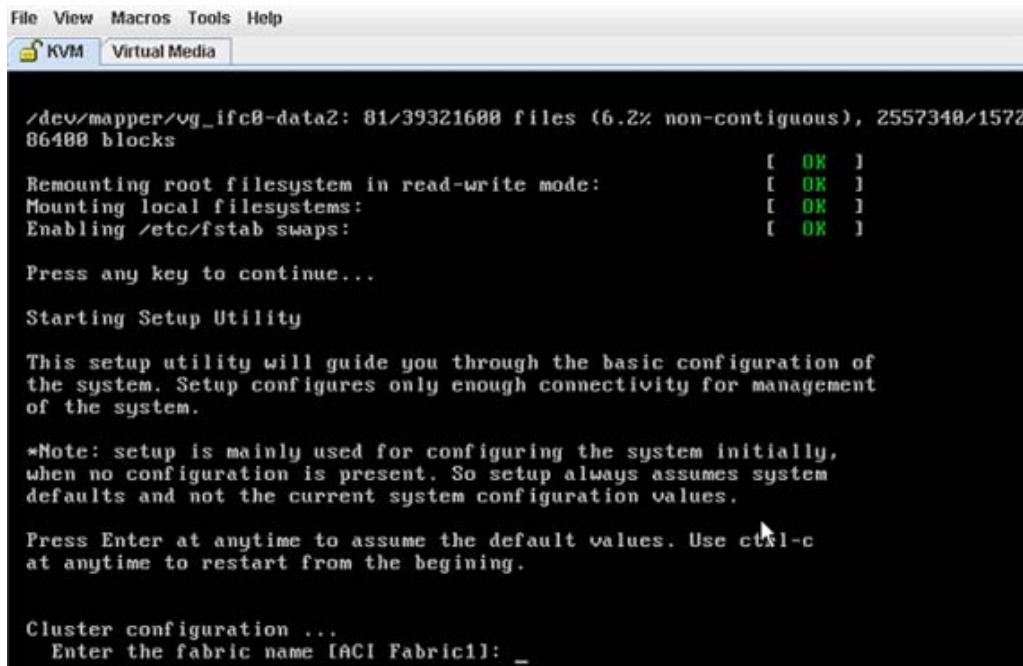
The following section provides a detailed procedure for configuring the Cisco ACI for use in a FlexPod environment. Follow these steps precisely because failure to do so could result in an improper configuration.

Physical Connectivity

Follow the physical connectivity guidelines for FlexPod as covered in the section [FlexPod Cabling](#). In ACI, both spine and leaf switches are configured using APIC; individual configuration of the switches is not required. APIC discovers the ACI infrastructure switches using LLDP and acts as the central point for the entire configuration.

Cisco APIC Initial Configuration Setup

1. Log into the APIC CIMC using a web browser and launch the KVM.
2. Browse to https://<cimc_ip_address>.
3. Log in using "admin" as username and use the password defined during CIMC setup.
4. From the "Server" tab on the left, select "Summary" and click "Launch KVM Console."
5. KVM application will be launched and initial APIC setup screen should be visible.



The screenshot shows a terminal window titled 'KVM' with a menu bar 'File View Macros Tools Help'. The window displays the following text:

```

File View Macros Tools Help
KVM Virtual Media

/dev/mapper/vg_ifc0-data2: 81/39321600 files (6.2% non-contiguous), 2557340/1572
86488 blocks
[ OK ]
Remounting root filesystem in read-write mode: [ OK ]
Mounting local filesystems: [ OK ]
Enabling /etc/fstab swaps: [ OK ]

Press any key to continue...

Starting Setup Utility

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

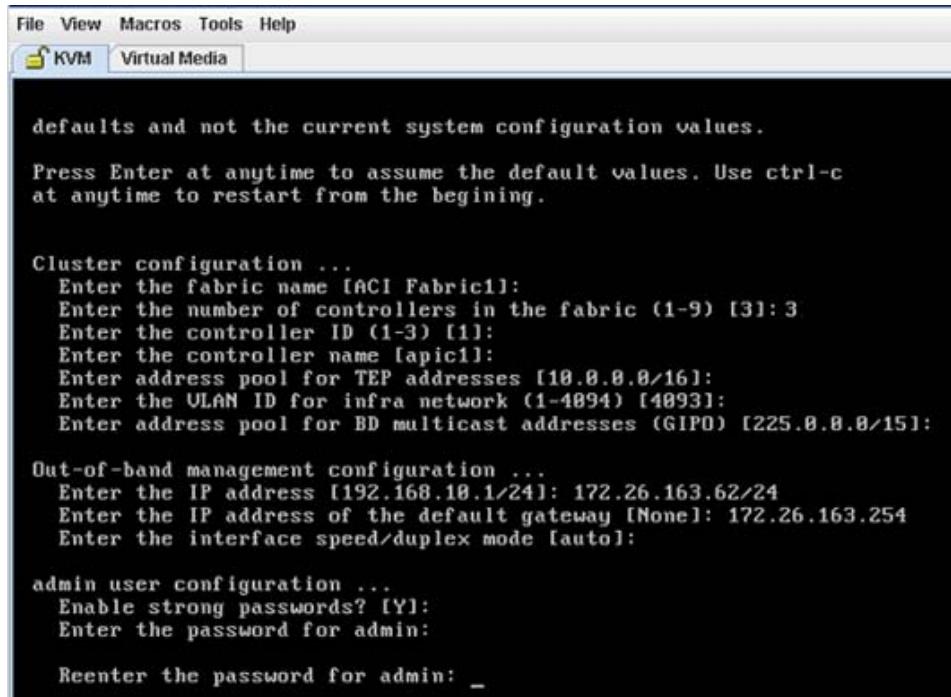
Press Enter at anytime to assume the default values. Use ctrl-c
at anytime to restart from the begining.

Cluster configuration ...
Enter the fabric name [ACI Fabric1]: _

```

6. Press <return> to select the default value for "Enter the fabric name". This value can be changed if desired.
7. Press <return> to select the default value for "Enter the number of controllers in the fabric". While the fabric can operate with a single APIC, 3 APICs are recommended for redundancy.
8. Enter the controller number currently being set up under "Enter the controller ID (1-3)". Please remember only controller number 1 will allow you to setup the admin password. Remaining controllers and switches sync their passwords to the admin password set on the controller 1.
9. Enter the controller name or choose default name for "Enter the controller name".
10. Press <return> to select the default pool under "Enter the address pool for TEP addresses". If the network is already in use, please choose a different range.
11. Press <return> to select the default vlan for "Enter the VLAN id for infra network."

12. Press <return> to select the default range for "Enter address pool for BD multicast addresses."
13. Enter appropriate values for the out of band management network configuration. The out of band management IP address will be used to access the APIC from client browsers.
14. Enter the admin password (controller 1 only).
15. Press <return> to accept the configuration without changes.
16. Let the APIC complete its boot process.
17. Repeat these steps for all three APIC controllers.



```

defaults and not the current system configuration values.
Press Enter at anytime to assume the default values. Use ctrl-c
at anytime to restart from the begining.

Cluster configuration ...
Enter the fabric name [ACI Fabric1]:
Enter the number of controllers in the fabric (1-9) [3]: 3
Enter the controller ID (1-3) [1]:
Enter the controller name [apic1]:
Enter address pool for TEP addresses [10.0.0.0/16]:
Enter the VLAN ID for infra network (1-4094) [4093]:
Enter address pool for BD multicast addresses (GIP0) [225.0.0.0/15]:

Out-of-band management configuration ...
Enter the IP address [192.168.10.1/24]: 172.26.163.62/24
Enter the IP address of the default gateway [None]: 172.26.163.254
Enter the interface speed/duplex mode [auto]: 

admin user configuration ...
Enable strong passwords? [Y]:
Enter the password for admin:
Reenter the password for admin: _

```



Note When APIC-1 boots up for the first time, it might take up to five minutes to allow login using the admin password set during the setup procedure. If something went wrong during the setup, APIC does allow login using a special user called "rescue-user". If admin password was never set or was not setup properly, rescue-user will allow access to APIC without any password. If an admin password was set previously, use rescue-user with the admin password.

Cisco ACI - Fabric Discovery

1. Log into the APIC GUI using a web browser.



Note For accessing APIC GUI, Google Chrome was utilized during validation

2. Browse to https://<Out of Band IP address of APIC 1>
3. Log in using "admin" as the username and use the password defined during initial setup.



4. Click FABRIC from the top bar. Under INVENTORY, expand Fabric Membership.
5. At least one of the leaves should be visible.

SERIAL NUMBER	NODEID	NODENAME	RACKNAME	MODEL	ROLE	IP	DECOMMISSIONED	SUPPORTED MODEL
SAL1815Q3J9	0			N9K-C9396PX	leaf	0.0.0.0	False	True

6. Click FABRIC from the top bar. Under INVENTORY, expand Fabric Membership.
7. Log into the leaf using console connection (admin/<no password needed>) and use the serial number to identify discovered leaf (Leaf-1 or Leaf-2 in the physical setup).


```
switch# show inventory
NAME: "Chassis",  DESCRIPTOR: "Nexus C9396PX Chassis"
PID: N9K-C9396PX          ,  VID: V02 ,  SN: SAL1815Q3J9
<snip>
```
8. Double-click the identified leaf description on the right and assign a NODE ID value of 101 and NODE NAME <device name>. Click UPDATE.

SERIAL NUMBER	NODEID	NODENAME	RACKNAME	MODEL	ROLE	IP	DECOMMISSIONED	SUPPORTED MODEL
SAL1815Q3J9	101	<device name>		N9K-C9396PX	leaf	0.0.0.0	False	True

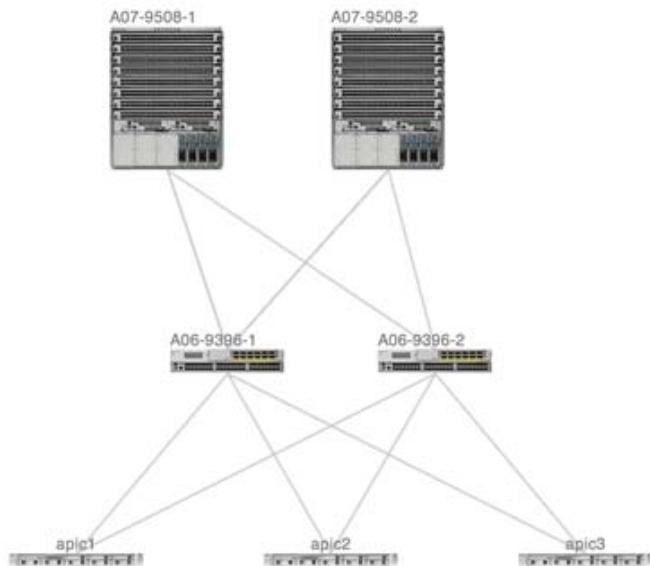
9. As the fabric discovery continues, both spines and leaves will start appearing under the Fabric Membership window. Repeat Step 7 to assign the NODE ID and NODE NAME to these devices.
10. When the NODE ID and NODE NAME values are assigned, APIC assigns IP addresses from TEP the pool defined during initial setup.

SERIALNUMBER	NODE ID	NODE NAME	RACKNAME	MODEL	ROLE	IP	DECOMMISSIONED	SUPPORTED MODEL
FGE1B100ACK	201	AOS-9508-1		MK-C9500	spine	10.0.8.94/32	False	True
SAL1B15Q3H	102	AOS-9396-2		MK-C9396PX	leaf	10.0.8.93/32	False	True
SAL1B15Q3JF	101	AOS-9396-1		MK-C9396PX	leaf	10.0.8.95/32	False	True

11. When both leaves and spines are added to the fabric, click Topology on the left. Three APICs, two leaves and two spines should be visible.

Figure 4

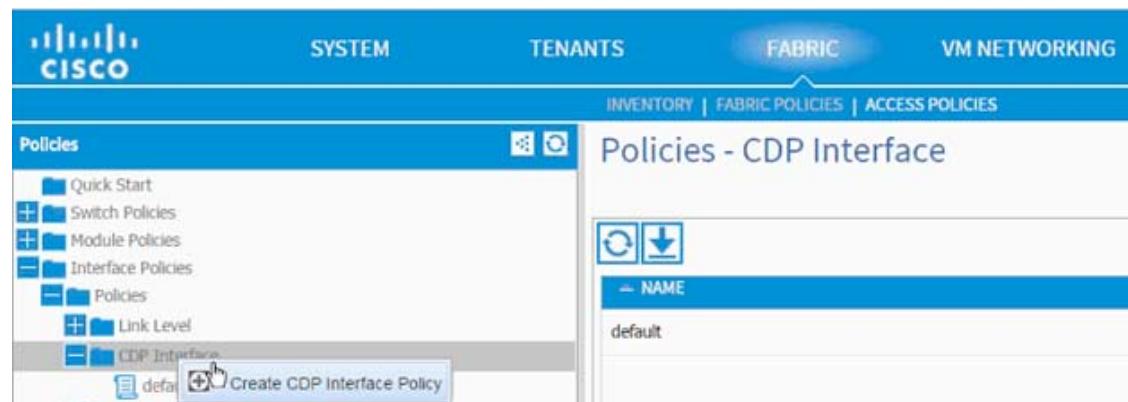
APIC - Topology



Cisco ACI - Defining Fabric Access Policies

In this section, various access policies such as CDP, LACP and LLDP will be defined. These policies will be used during the vPC and VM domain creation. To define fabric access policies, complete the following steps:

1. Click FABRIC and select ACCESS POLICIES under the sub-menu.
2. From the left menu bar, expand Interface Policies.
3. Expand Policies.
4. Right-click CDP Interface and select Create CDP Interface Policy.



5. In the menu box, enter CDP_Enabled as the policy name and set Admin State, Enabled.
6. Click SUBMIT.

CREATE CDP INTERFACE POLICY

Specify the CDP Interface Policy Identity

Name:	<input type="text" value="CDP_Enable"/>
Description:	<input type="text" value="optional"/>
Admin State:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

SUBMIT **CANCEL**

7. From the left menu bar, expand LLDP interface.
8. Right-click and select Create LLDP Interface Policy.
9. In the menu box, enter LLDP_Disabled as the policy name and set both Transmit State and Receive State, Disabled.
10. Click SUBMIT.

CREATE LLDP INTERFACE POLICY

i X

Specify the LLDP Interface Policy Properties

Name:

Description:

Receive State: Enabled
 Disabled

Transmit State: Enabled
 Disabled

SUBMIT **CANCEL**

11. Right-click and select Create LLDP Interface again.
12. In the menu box, enter LLDP_Enabled as the policy name and set both Transmit State and Receive State, Enabled.
13. Click SUBMIT.

CREATE LLDP INTERFACE POLICY

i X

Specify the LLDP Interface Policy Properties

Name:

Description:

Receive State: Enabled
 Disabled

Transmit State: Enabled
 Disabled

SUBMIT **CANCEL**

14. From the left menu bar, expand LACP.
15. Right-click and select Create LACP Policy.
16. In the menu box, enter LACP_Active as the policy name and select Mode and Active. Leave the remaining options as default
17. Click SUBMIT.

CREATE LACP POLICY

Specify the LACP Policy Identity

Name:

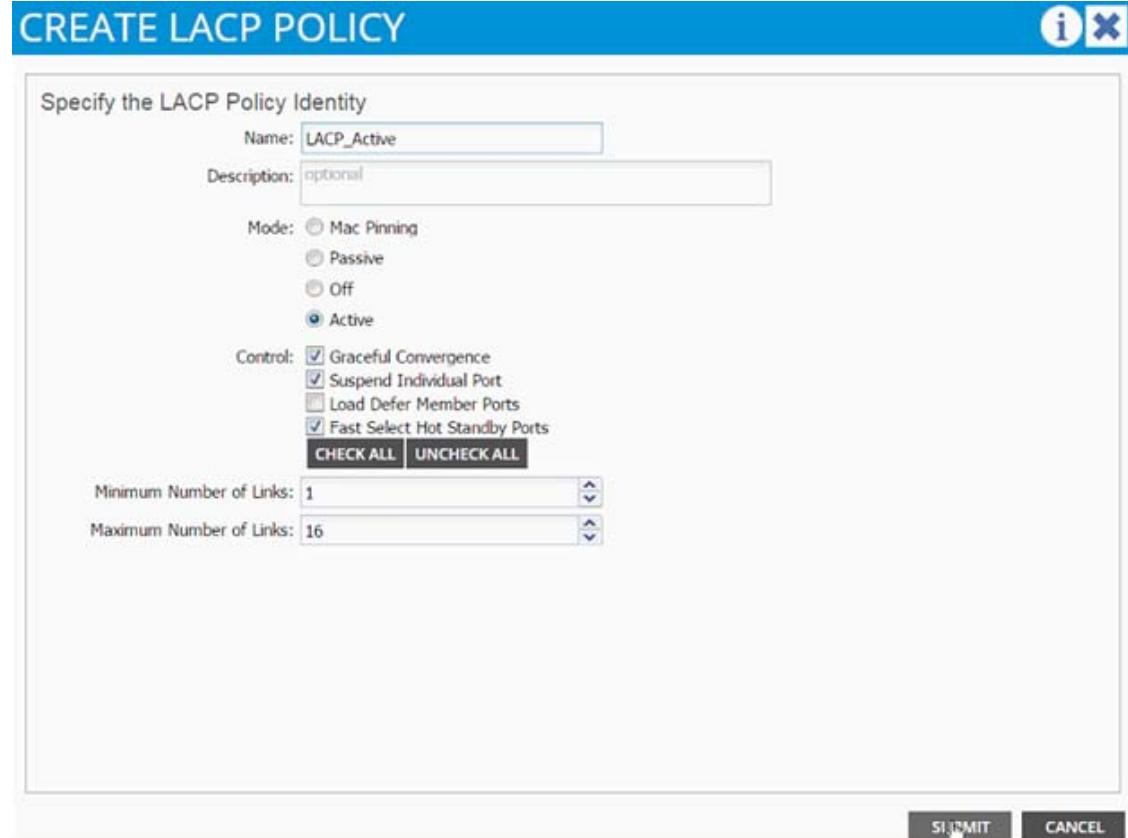
Description:

Mode: Mac Pinning
 Passive
 Off
 Active

Control: Graceful Convergence
 Suspend Individual Port
 Load Defer Member Ports
 Fast Select Hot Standby Ports

Minimum Number of Links:

Maximum Number of Links:



18. From the left menu bar, expand LACP.
19. Right-click and select Create LACP Policy.
20. In the menu box, enter LACP_MAC_Pinning as the policy name and select Mode and Mac Pinning. Leave remaining options as default.
21. Click SUBMIT.

CREATE LACP POLICY

Specify the LACP Policy Identity

Name:

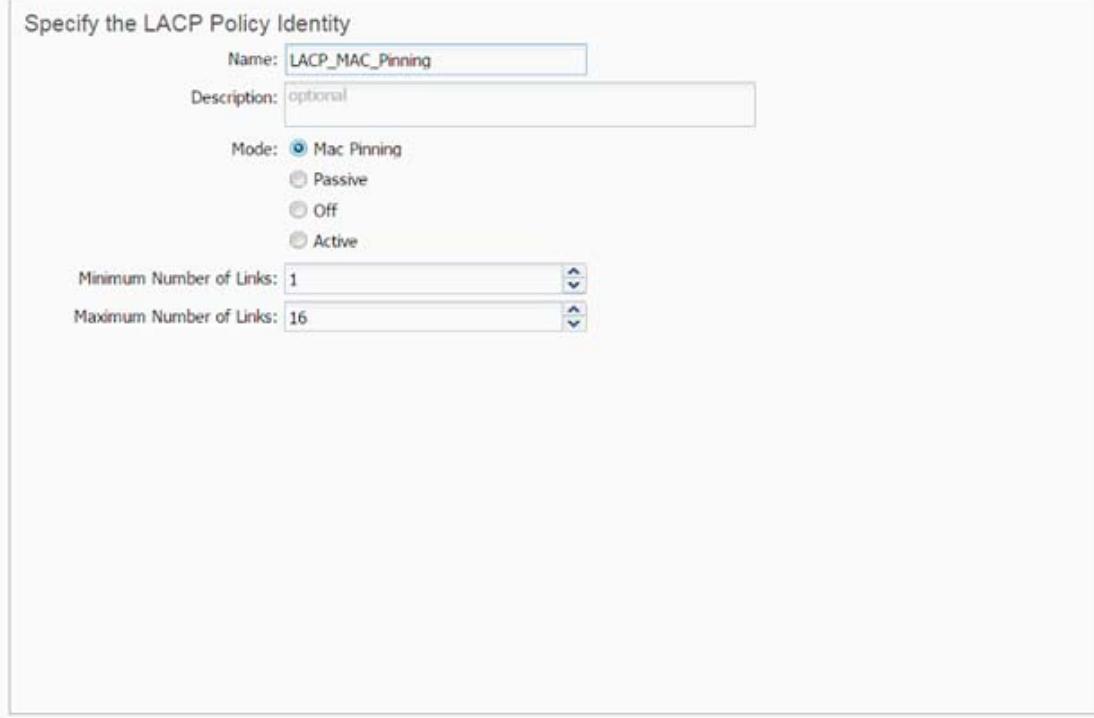
Description:

Mode: Mac Pinning
 Passive
 Off
 Active

Minimum Number of Links:

Maximum Number of Links:

SUBMIT **CANCEL**

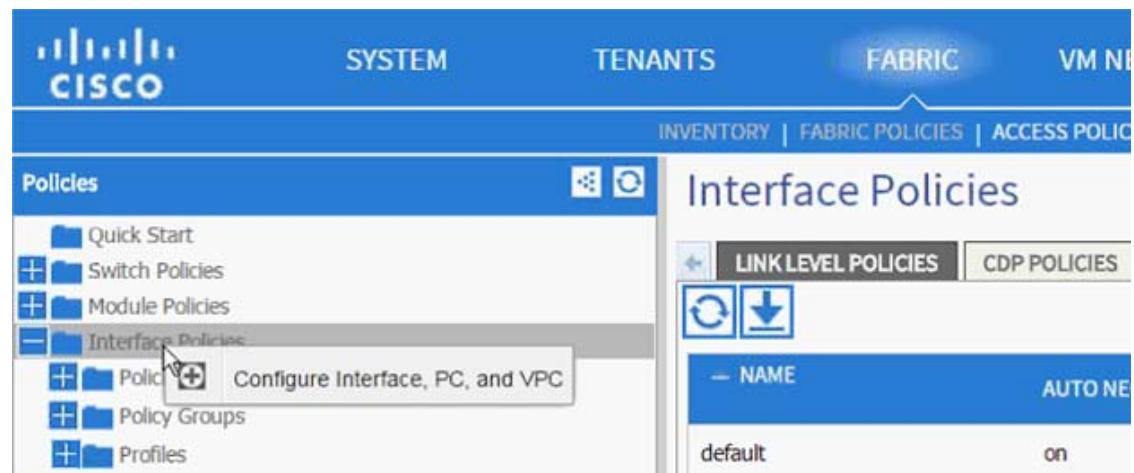


Cisco ACI - Creating vPC for Cisco UCS Fabric Interconnect A

In this section, vPC for Cisco UCS Fabric Interconnect A will be created using the interface creation wizard.

To create vPC for Cisco UCS Fabric Interconnect A, complete the following steps:

1. From the main menu, click FABRIC and select Access Policies.
2. Right-click Interface Policies and select Configure interface, PC and vPC.



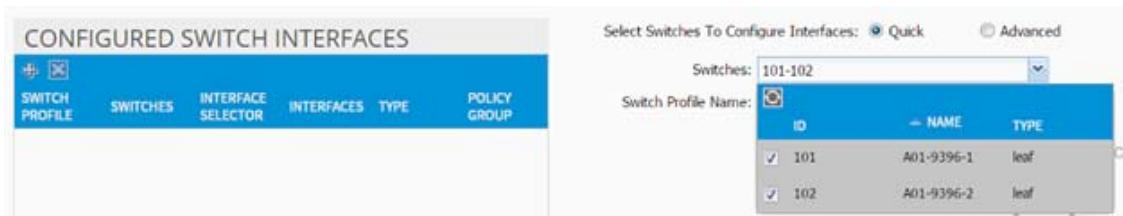
3. In the dialog box, click + under the vPC SWITCH PAIRS.
4. Enter 10 as vPC Domain ID.
5. From the Switch 1 and Switch 2 drop-down list select both leaves.
6. Click Save.



7. Validate that the create vPC domain appears under the vPC SWITCH PAIRS.

VPC SWITCH PAIRS		
+ [X]	— SWITCH 1	SWITCH 2
10	101	102

8. In the dialog box, click + under the CONFIGURED SWITCH INTERFACES.
9. From the Switches drop-down list and select both leaves.



10. Enter <sp-UCS-FI-1> as Switch Profile Name. UCS-FI-1 is the host name for Cisco UCS Fabric Interconnect A.
11. Click + to add interfaces
12. Select vPC radio button to configure vPC.
13. Enter 1/19 under Interfaces. This is the port on both switches where Fabric Interconnect A is connected.
14. Enter <ifs- UCS-FI-1> as Interface Selector Name.

Select Switches To Configure Interfaces: Quick Advanced

Switches: 101-102

Switch Profile Name: sp-A01-6248-1

Interface Type: Individual PC VPC

Interfaces: 1/19
Select interfaces by typing, e.g. 1/17-18 or use the mouse to click on the switch image below.

Interface Selector Name: ifs-A01-6348-1

15. From the vPC Policy Group drop-down list, select Create vPC Interface Policy Group. A new dialog box will appear.
16. Enter <pg- UCS-FI-1> as the name of the vPC INTERFACE POLICY GROUP in the dialog box.
17. Select various policy values from the drop-down menus.

CREATE VPC INTERFACE POLICY GROUP

Specify the Policy Group identity

Name: pg-A01-6248-1

Description: optional

Link Level Policy: default

CDP Policy: CDP_Enable

LLDP Policy: LLDP_Enabled

STP Interface Policy: default

LACP Policy: LACP_Active

Monitoring Policy: default

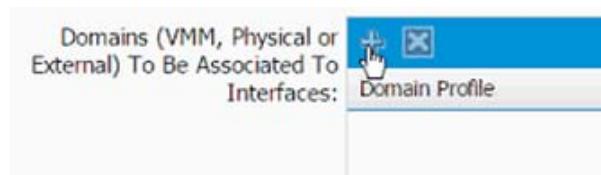
Override Policy Group:

Name	LACP Member Policy

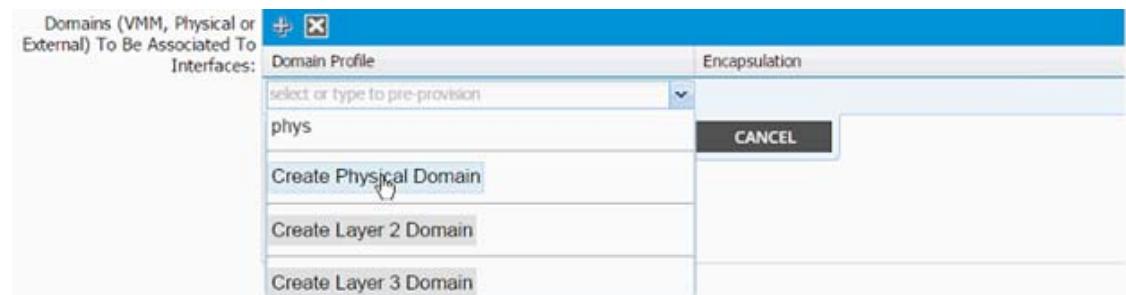
Attached Entity Profile: select an option

SUBMIT CANCEL

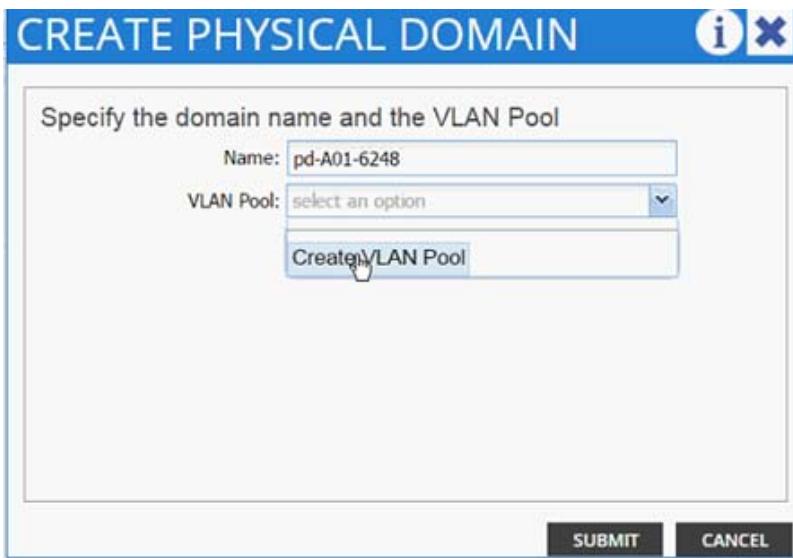
18. From the Attached Entity Profile drop-down list select Create Attachable Access Entity Profile. A new dialog box will appear.
19. The two Cisco UCS Fabric Interconnects will share this Attachable Entity Profile (AEP). Enter <aep-UCS-FI-hostname> as the Name (avoid using A or B at the end).
20. Click + to add Domain.



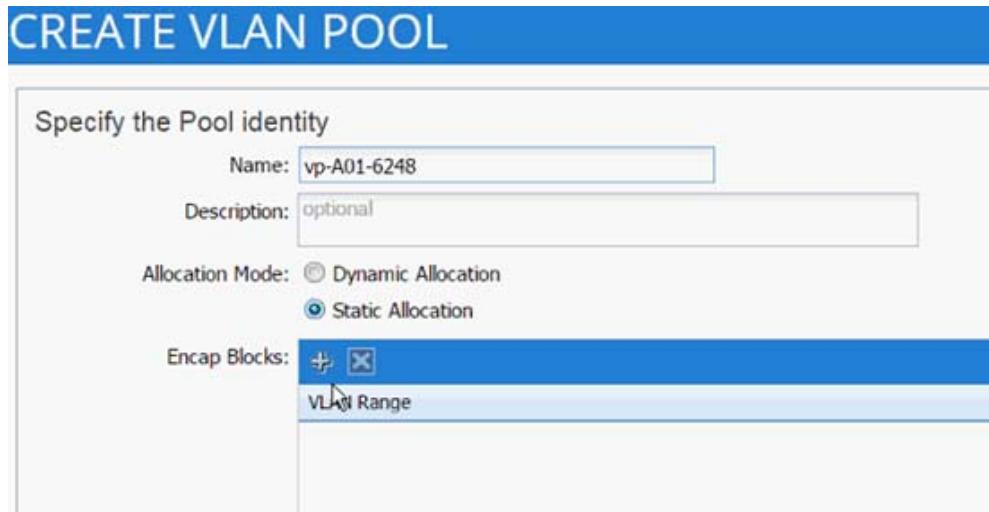
21. In the added domain, from the drop-down list select Create Physical Domain.



22. In the Create Physical Domain dialog box, enter <pd-UCS-FI hostname> as Name.
23. From the VLAN Pool drop-down list Create VLAN Pool.



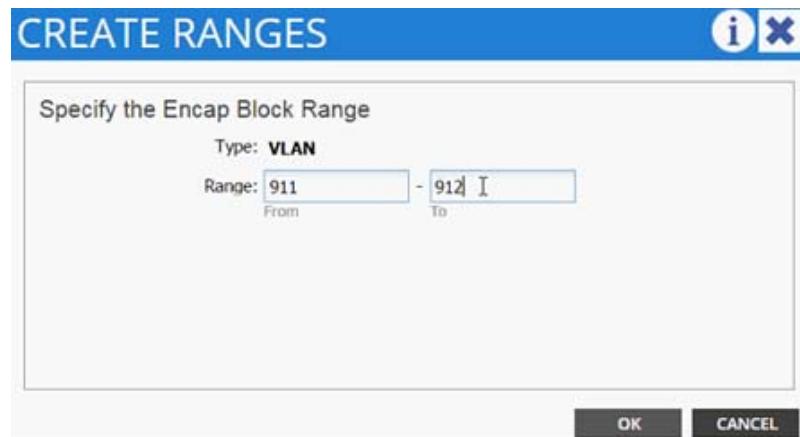
24. In the Create VLAN Pool dialog box, enter <vp-UCS-FI hostname> as Name.
25. Select Allocation Mode > Static Allocation.
26. Click + next to Encap Block.



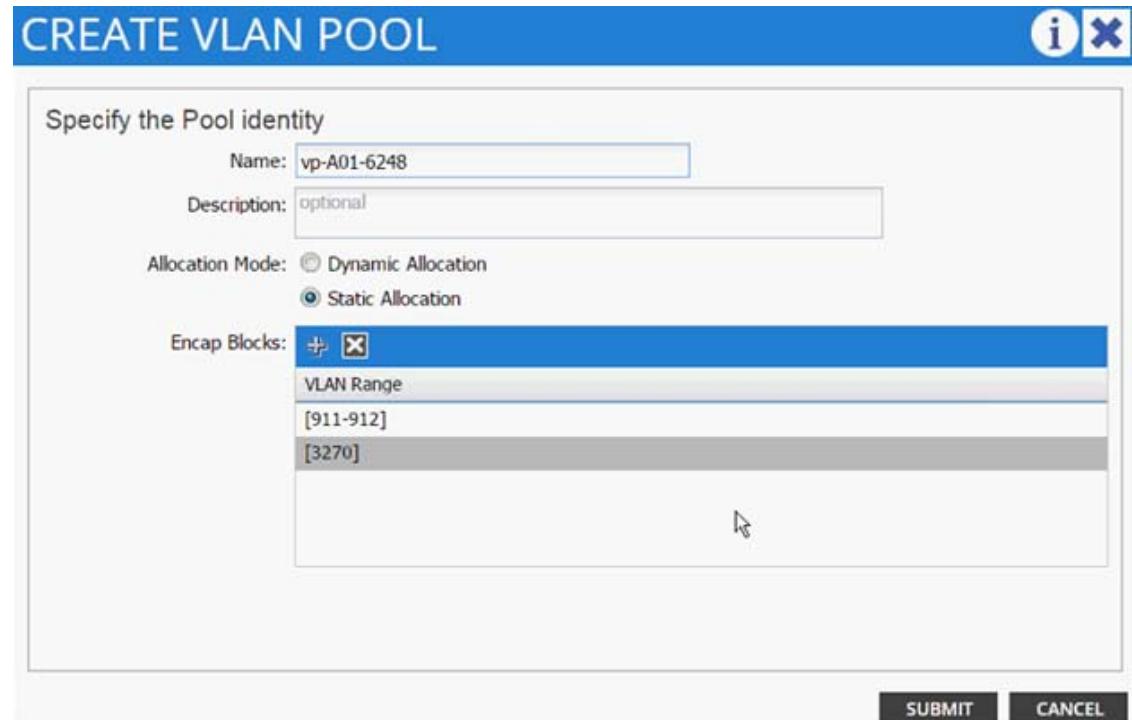
27. In the CREATE RANGES dialog box, enter the two iSCSI VLANs and the NFS VLAN.



Note In the screenshot below, 911, 912 are iSCSI VLANs and 3270 is the NFS VLAN configured on UCS.



28. Click OK.
29. Click + to add NFS VLAN and in the CREATE RANGES dialog box, enter range 3270-3270 (single VLAN).
30. Click OK.



31. Click SUBMIT to finish the VLAN pool creation.
32. Click SUBMIT to finish Physical Domain creation.

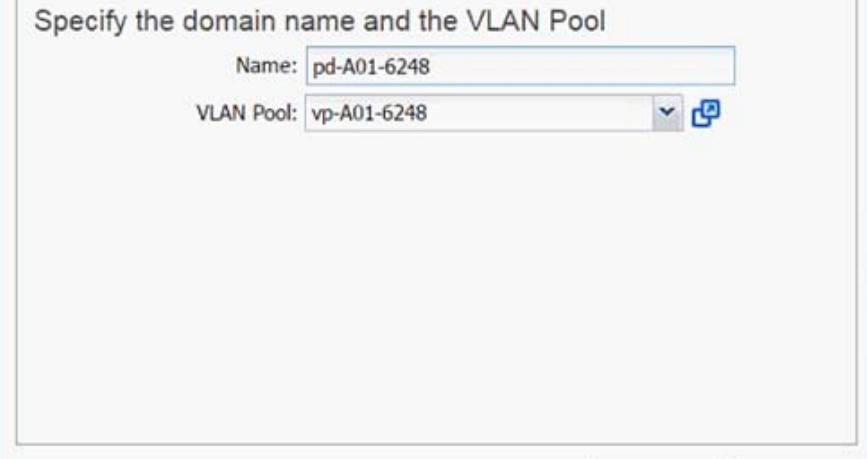
CREATE PHYSICAL DOMAIN

Specify the domain name and the VLAN Pool

Name: pd-A01-6248

VLAN Pool: vp-A01-6248

SUBMIT CANCEL



33. Click UPDATE to finish adding Physical domain to AEP.

CREATE ATTACHABLE ACCESS ENTITY PROFILE

Specify the name, domains and infrastructure encaps

Name: aep-A01-6248

Description: optional

Enable Infrastructure VLAN:

Domains (VMM, Physical or External) To Be Associated To

Interfaces:	Domain Profile	Encapsulation
	pd-A01-6248	<input type="button" value="UPDATE"/> <input type="button" value="CANCEL"/>



34. Click SUBMIT to finish adding AEP.

CREATE ATTACHABLE ACCESS ENTITY PROFILE

Specify the name, domains and infrastructure encaps

Name: aep-A01-6248

Description: optional

Enable Infrastructure VLAN:

Domains (VMM, Physical or External) To Be Associated To Interfaces:

Domain Profile	Encapsulation
Physical Domain - pd-A01-6248	from:vlan-911 to:vlan-912 from:vlan-3270 to:vlan-3270

SUBMIT **CANCEL**

35. Click SUBMIT to finish creating the vPC Interface Policy Group.

CREATE VPC INTERFACE POLICY GROUP

Specify the Policy Group identity

Name:	pg-A01-6248-1
Description:	optional
Link Level Policy:	default
CDP Policy:	CDP_Enable
LLDP Policy:	LLDP_Enabled
STP Interface Policy:	default
LACP Policy:	LACP_Active
Monitoring Policy:	default

Override Policy Group:

Name	LACP Member Policy

Attached Entity Profile: aep-A01-6248

SUBMIT **CANCEL**

36. From the Configure Interface, PC, vPC screen, click SAVE.

CONFIGURE INTERFACE, PC, AND VPC

CONFIGURED SWITCH INTERFACES

SWITCH PROFILE	SWITCHES	INTERFACE SELECTOR	INTERFACES	TYPES	POLICY GROUP
----------------	----------	--------------------	------------	-------	--------------

Select Switches To Configure Interfaces: Quick Advanced
Switches: 101-102
Switch Profile Name: sp-A01-6248-1

Interface Type: Individual PC VPC
Interfaces: 1/19
Select interfaces by typing, e.g., 1/1-1/18 or use the mouse to click on the switch image below.

Interface Selector Name: Ifs-A01-6248-1 VPC Policy Group: pg-A01-6248-1

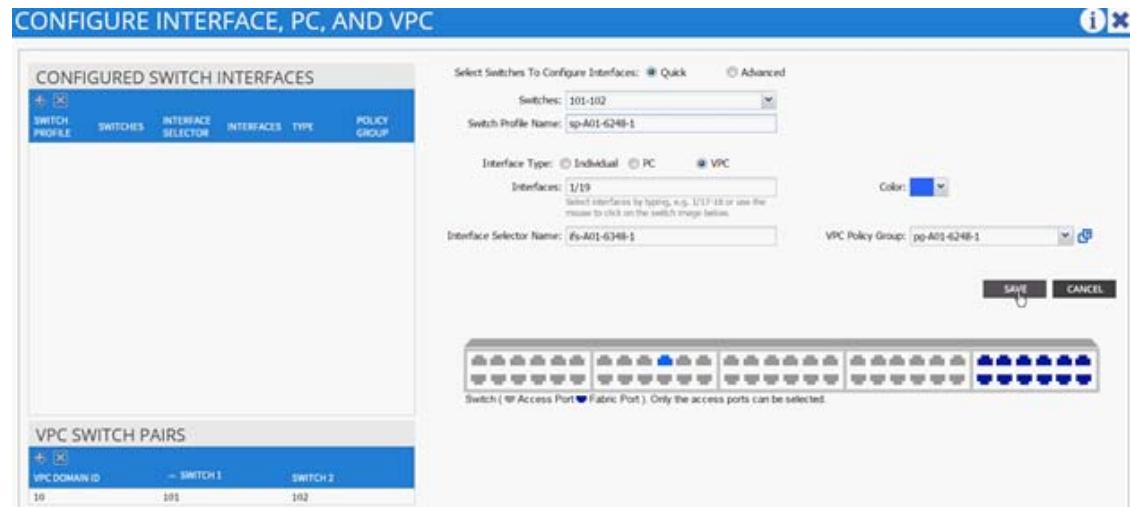
SAVE **CANCEL**

VPC SWITCH PAIRS

VPC DOMAIN ID	— SWITCH 1	SWITCH 2
10	101	102

Switch (Access Port Fabric Port). Only the access ports can be selected.

37. Click SAVE.



38. Click SUBMIT to finish the vPC creation using wizard.
39. Under Fabric, select Inventory.
40. From the left menu, expand Pod 1, expand Leaf-1 and expand Interfaces followed by vPC Interfaces.
41. Validate that the vPC domain 10 and the vPC exist.

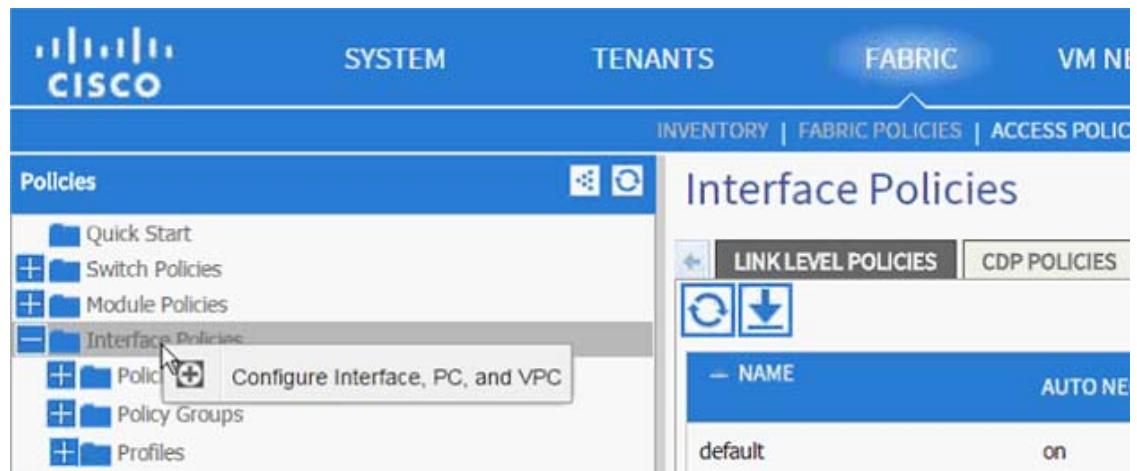


Note Log into the switch using the console and use the show port-channel summary command to verify the port-channel configuration. If Cisco Unified Computing System was configured correctly, the port-channel would show "UP."

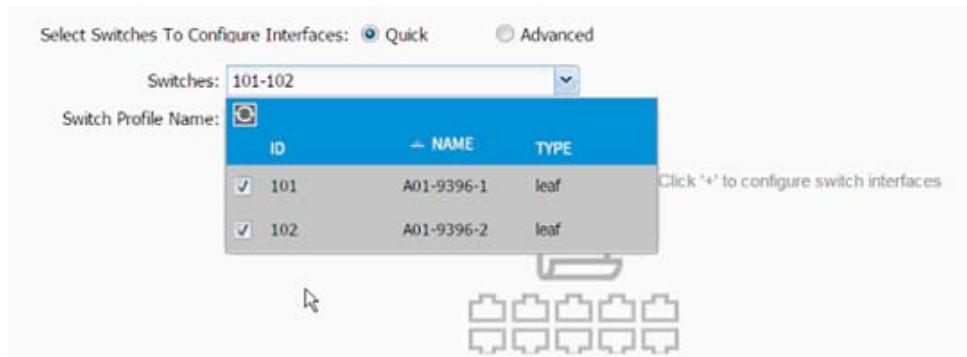
Cisco ACI - Creating vPC for Cisco UCS Fabric Interconnect B

In this section, vPC for Cisco UCS Fabric Interconnect B will be created using the interface creation wizard.

1. From the main menu, click FABRIC and select Access Policies.
2. Right-click Interface Policies and select Configure interface, PC and vPC.



3. In the dialog box, click + under the CONFIGURED SWITCH INTERFACES.
4. From the Switches drop-down list and select both leaves.



5. Enter <sp-UCS-FI-2> as the Switch Profile Name. UCS-FI-2 is the host name for the UCS Fabric Interconnect B.
6. Click + sign to add interfaces.
7. Select vPC radio button to configure vPC.
8. Enter 1/20 under Interfaces. This is the port on both switches where Fabric Interconnect B is connected.
9. Enter <if- UCS-FI-2> as the Interface Selector Name.

Select Switches To Configure Interfaces: Quick Advanced

Switches: 101-102

Switch Profile Name: sp-A01-6248-2

Interface Type: VPC Individual PC

Interfaces: 1/20
Select interfaces by typing, e.g. 1/17-18 or use the mouse to click on the switch image below.

Interface Selector Name: ifs-A01-6248-2

10. From the vPC Policy Group drop-down list click Create vPC Interface Policy Group. A new dialog box will appear.
11. Enter <pg- UCS-FI-2> as the name of the vPC INTERFACE POLICY GROUP in the dialog box.
12. Select various policy values from the drop-down menus.

CREATE VPC INTERFACE POLICY GROUP

Specify the Policy Group identity

Name:	pg-A01-6248-2						
Description:	optional						
Link Level Policy:	default						
CDP Policy:	CDP_Enable						
LLDP Policy:	LLDP_Enabled						
STP Interface Policy:	default						
LACP Policy:	LACP_Active						
Monitoring Policy:	default						
Override Policy Group:	<table border="1"> <tr> <td>+ <input type="button"/></td> <td><input type="button"/></td> </tr> <tr> <td>Name</td> <td>LACP Member Policy</td> </tr> <tr> <td colspan="2"><hr/></td> </tr> </table>	+ <input type="button"/>	<input type="button"/>	Name	LACP Member Policy	<hr/>	
+ <input type="button"/>	<input type="button"/>						
Name	LACP Member Policy						
<hr/>							
Attached Entity Profile:	select an option						

SUBMIT **CANCEL**

13. From the Attached Entity Profile drop-down list and select the shared AEP created in the previous section.
14. Click SUBMIT to finish creating the vPC Interface Policy Group.

CREATE VPC INTERFACE POLICY GROUP

i X

Specify the Policy Group identity					
Name:	pg-A01-6248-2				
Description:	optional				
Link Level Policy:	default				
CDP Policy:	CDP_Enable				
LLDP Policy:	LLDP_Enabled				
STP Interface Policy:	default				
LACP Policy:	LACP_Active				
Monitoring Policy:	default				
Override Policy Group:	<input style="margin-right: 10px;" type="button" value="+"/> <input type="button" value="X"/> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Name</th> <th style="width: 50%;">LACP Member Policy</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody></table>	Name	LACP Member Policy		
Name	LACP Member Policy				
Attached Entity Profile:	aep-A01-6248				

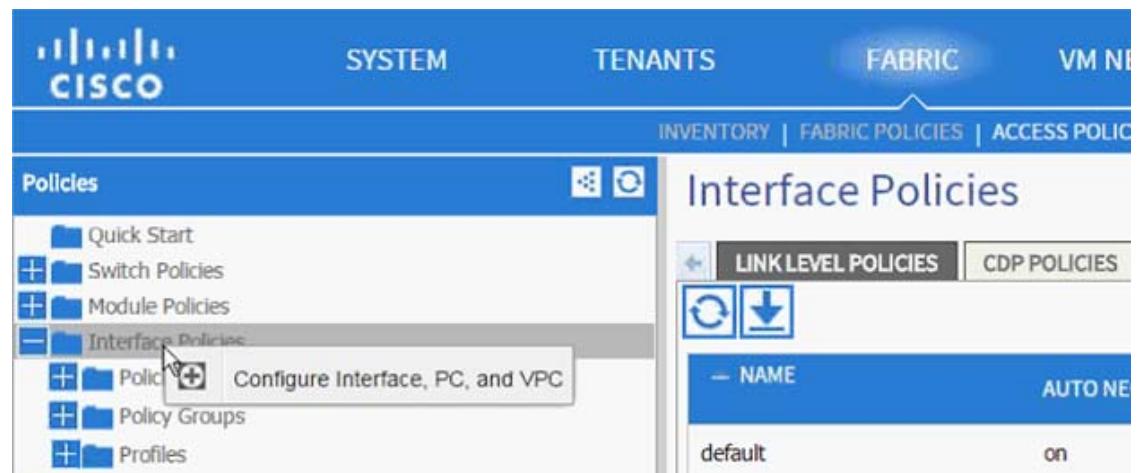
SUBMIT **CANCEL**

15. From the Configure Interface, PC, vPC screen, click SAVE.
16. Click SAVE.
17. Click SUBMIT to finish the vPC creation.
18. (Optional) Log into the individual leaf switches and use "show port-channel summary" and "show vpc" commands to verify the configuration.

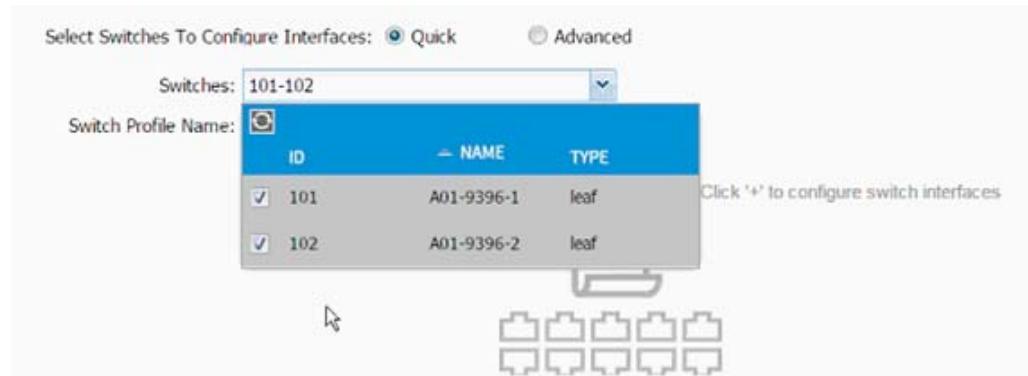
Cisco ACI - Creating vPC for NetApp Controller 1

In this section, the vPC for NetApp Controller 1 will be created using the interface creation wizard.

1. From the main menu, click FABRIC and select Access Policies.
2. Right-click Interface Policies and select Configure interface, PC and vPC.



3. In the dialog box, click + under the CONFIGURED SWITCH INTERFACES.
4. From the Switches drop-down list and select both leaves.



5. Enter <sp-NetAPP-1> as the Switch Profile Name. NetApp-1 is the host name for NetApp Controller 1.
6. Click + to add interfaces.
7. Select vPC radio button to configure vPC.
8. Enter 1/17 under Interfaces. This is the port on both switches where NetApp Controller 1 is connected.
9. Enter <iifs- NetApp-1> as the Interface Selector Name.

Select Switches To Configure Interfaces: Quick Advanced

Switches: 101-102

Switch Profile Name: sp-A02-NAPP-1

Interface Type: Individual PC VPC

Interfaces: 1/17
Select interfaces by typing, e.g. 1/17-18 or use the mouse to click on the switch image below.

Interface Selector Name: ifs-A02-NAPP-1

10. From the vPC Policy Group drop-down list click Create vPC Interface Policy Group. A new dialog box will appear
11. Enter <pg- NetApp-1> as the name of the vPC INTERFACE POLICY GROUP in the dialog box.
12. Select the various policy values from the drop-down lists.

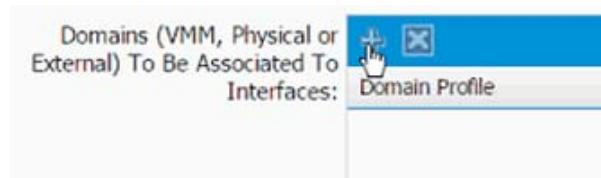
CREATE VPC INTERFACE POLICY GROUP

Specify the Policy Group identity

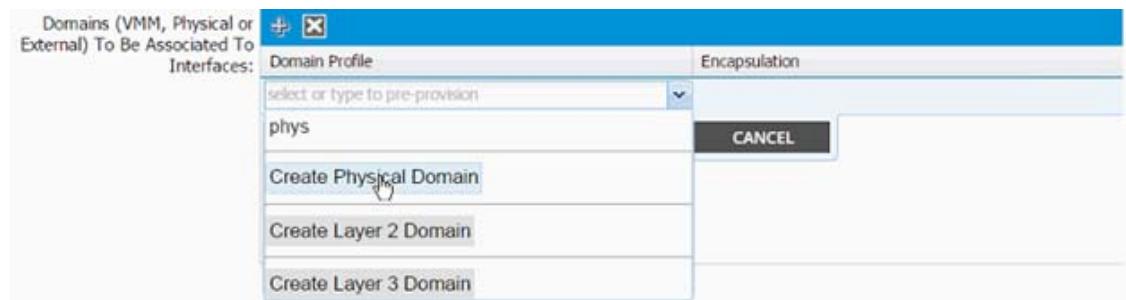
Name:	pg-A02-NAPP-1				
Description:	optional				
Link Level Policy:	default				
CDP Policy:	CDP_Enable				
LLDP Policy:	LLDP_Disabled				
STP Interface Policy:	default				
LACP Policy:	LACP_Active				
Monitoring Policy:	default				
Override Policy Group:	<input type="button" value="+"/> <input type="button" value="X"/> <table border="1"> <thead> <tr> <th>Name</th> <th>LACP Member Policy</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table>	Name	LACP Member Policy		
Name	LACP Member Policy				
Attached Entity Profile:	select an option <input type="button" value="..."/>				

SUBMIT CANCEL

13. From the Attached Entity Profile drop-down list click Create Attachable Access Entity Profile. A new dialog box will appear
14. The two NetApp Controllers will share the Attachable Entity Profile (AEP). Enter <aep-NetApp-hostname> as the Name. (Avoid using 1 or 2 at the end)
15. Click + to add Domain.



- In the added domain, from the drop-down list select Create Physical Domain.



- In the Create Physical Domain dialog box, enter <pd-NetApp-hostname> as the Name.
- From the VLAN Pool drop-down list select Create VLAN Pool.

CREATE PHYSICAL DOMAIN

Specify the domain name and the VLAN Pool

Name:	pd-A02-NAPP
VLAN Pool:	select an option vp-A01-8248 Create VLAN Pool
<input type="button" value="SUBMIT"/> <input type="button" value="CANCEL"/>	

- In the Create VLAN Pool dialog box, enter <vp-NetApp-hostname> as Name.
- Select Allocation Mode > Static Allocation.
- Click + next to Encap Block.

CREATE VLAN POOL

Specify the Pool identity

Name: vp-A01-NAPP
Description: optional

Allocation Mode: Dynamic Allocation Static Allocation

Encap Blocks:

- + VLAN Range

SUBMIT **CANCEL**

22. In the CREATE RANGES dialog box, enter the two iSCSI VLANs and the NFS VLAN.



In the screenshot below, 911, 912 are iSCSI VLANs and 3170 is the NFS VLAN configured on NetApp.

CREATE RANGES

Specify the Encap Block Range

Type: **VLAN**

Range: **911** - **912** To

OK **CANCEL**

23. Click OK.
24. Click + to add NFS VLAN and in the CREATE RANGES dialog box, enter range 3170-3170 (single VLAN).
25. Click OK.
26. Click SUBMIT to finish the VLAN pool creation.
27. Click SUBMIT to finish the Physical Domain creation.
28. Click UPDATE" to finish adding the Physical domain to AEP.
29. Click SUBMIT to finish adding AEP.

CREATE ATTACHABLE ACCESS ENTITY PROFILE



Specify the name, domains and infrastructure encaps

Name: aep-A02-NAPP

Description: optional

Enable Infrastructure VLAN:

Domains (VMM, Physical or External) To Be Associated To

Interfaces:



Domain Profile: Physical Domain - pd-A02-NAPP

Encapsulation

from:vlan-911 to:vlan-912
from:vlan-3170 to:vlan-3170

- Click SUBMIT to finish creating the vPC Interface Policy Group.

Specify the Policy Group identity

Name: pg-A02-NAPP-1

Description: optional

Link Level Policy: default



CDP Policy: CDP_Enable



LLDP Policy: LLDP_Disabled



STP Interface Policy: default



LACP Policy: LACP_Active



Monitoring Policy: default



Override Policy Group:



Name

LACP Member Policy

Attached Entity Profile: aep-A02-NAPP

SUBMIT

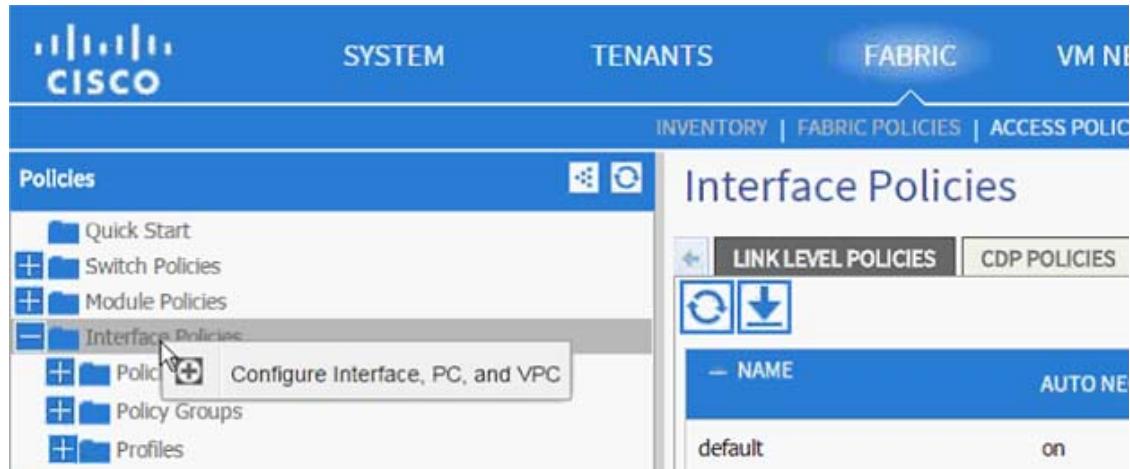
CANCEL

- From the Configure Interface, PC, vPC screen, click SAVE.
- Click SAVE.
- Click SUBMIT to finish the vPC creation using wizard.

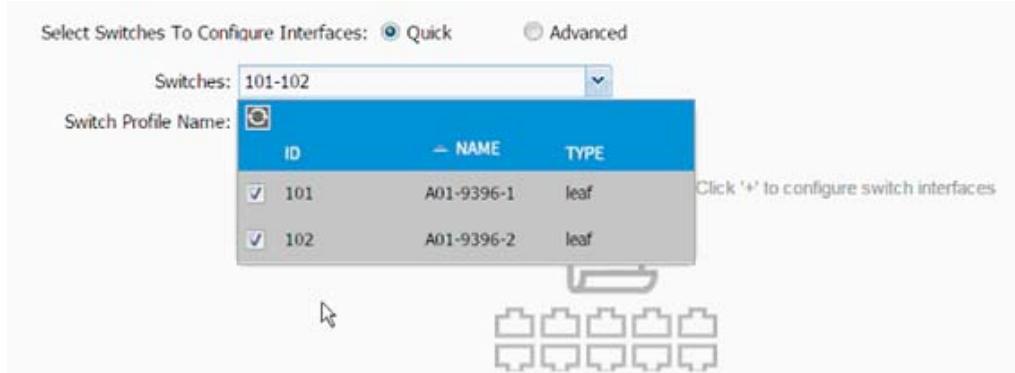
Cisco ACI - Creating vPC for NetApp Controller 2

In this section, the vPC for NetApp Controller 2 will be created using the interface creation wizard.

- From the main menu, click FABRIC and select Inventory.
- Expand Pod 1 and right-click on the first leaf and select Configure interface, PC and vPC.



- In the dialog box, click + under the CONFIGURED SWITCH INTERFACES.
- From the Switches drop-down list select both leaves.



- Enter <sp-NetAPP-2> as the Switch Profile Name. NetApp-2 is the host name for NetApp Controller 2.
- Click + to add interfaces.
- Select vPC radio button to configure vPC.
- Enter 1/18 under Interfaces. This is the port on both switches where NetApp Controller 2 is connected.
- Enter <if- NetApp-2> as the Interface Selector Name.

Select Switches To Configure Interfaces: Quick Advanced

Switches: 101-102

Switch Profile Name: sp-A02-NAPP-2

Interface Type: Individual PC VPC

Interfaces: 1/18
Select interfaces by typing, e.g. 1/17-18 or use the mouse to click on the switch image below.

Interface Selector Name: ifs-A02-NAPP-2

10. From the vPC Policy Group drop-down list click Create vPC Interface Policy Group. A new dialog box will appear.
11. Enter <pg- NetApp-2> as the name of the vPC INTERFACE POLICY GROUP in the dialog box.
12. Select various policy values from the drop-down lists.

CREATE VPC INTERFACE POLICY GROUP

Specify the Policy Group identity

Name:	pg-A02-NAPP-2				
Description:	optional				
Link Level Policy:	default				
CDP Policy:	CDP_Enable				
LLDP Policy:	LLDP_Disabled				
STP Interface Policy:	default				
LACP Policy:	LACP_Active				
Monitoring Policy:	default				
Override Policy Group:	<input type="button" value="+"/> <input type="button" value="X"/>				
<table border="1"> <thead> <tr> <th>Name</th> <th>LACP Member Policy</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table>		Name	LACP Member Policy		
Name	LACP Member Policy				
Attached Entity Profile:	<input type="button" value="select an option"/>				

SUBMIT CANCEL

13. From the Attached Entity Profile drop-down list select shared AEP created in the previous section.
14. Click SUBMIT to finish creating the vPC Interface Policy Group.

CREATE VPC INTERFACE POLICY GROUP

Specify the Policy Group identity

Name:	pg-A02-NAPP-2
Description:	optional
Link Level Policy:	default
CDP Policy:	CDP_Enable
LLDP Policy:	LLDP_Disabled
STP Interface Policy:	default
LACP Policy:	LACP_Active
Monitoring Policy:	default

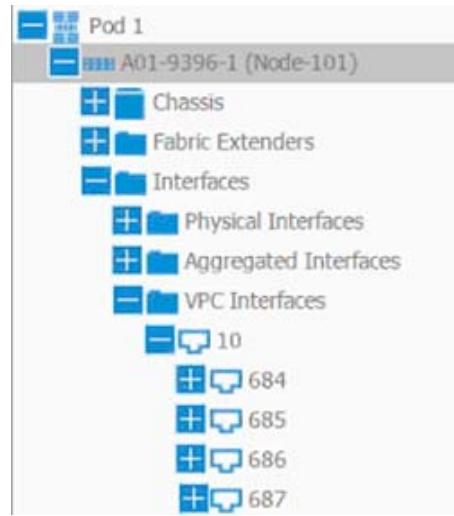
Override Policy Group:

Name	LACP Member Policy

Attached Entity Profile: aep-A02-NAPP

SUBMIT CANCEL

15. From the Configure Interface, PC, vPC screen, click SAVE.
16. Click SAVE.
17. Click SUBMIT to finish the vPC creation using wizard.
18. Expand the Pod 1 followed by the Leaf switch(s) on the left menu bar and then expand the Interfaces and vPC Interfaces.
19. Expand the vPC domain 10 and validate all the vPCs are configured and up (you will not see the VLAN being forwarded at this time).



20. Optional: Log into the leaf switches using the console and validate the port-channels are configured correctly. The output below assumes the NetApp and UCS port-channel configurations are in place.

```
A01-9396-1# show port-ch summary
Flags:  D - Down      P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        S - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met

Group Port-      Type     Protocol Member Ports
      Channel

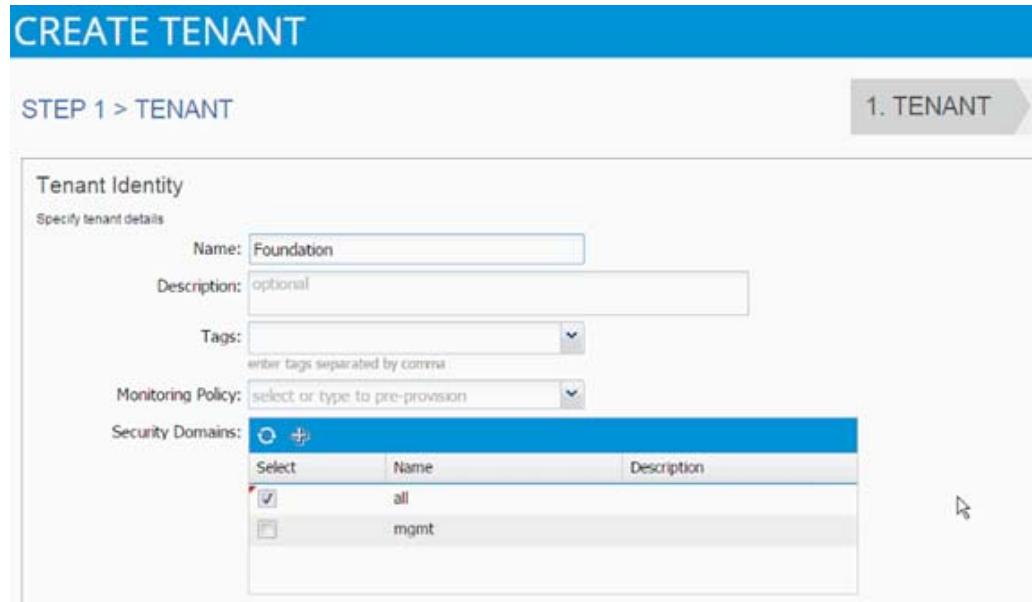
-----  

1    Po1 (SU)    Eth      LACP     Eth1/19 (P)
2    Po2 (SU)    Eth      LACP     Eth1/20 (P)
3    Po3 (SU)    Eth      LACP     Eth1/17 (P)
4    Po4 (SU)    Eth      LACP     Eth1/18 (P)
A01-9396-1# ■
```

Cisco ACI - Deploying Infrastructure (Foundation) Tenant

In this section, a new tenant will be deployed to host the infrastructure connectivity between the compute (VMware) and Storage (NetApp) environments.

1. From the main menu, click TENANTS and from the sub-menu click ADD TENANT.
2. In the CREATE TENANT dialog box, enter Foundation as the name of the tenant.
3. Click the checkbox next to all, under Security Domains.



4. Click Next.
5. Click + sign to add network.



6. In the CREATE NEW NETWORK dialog box, type Foundation as the Name. Leave everything else as default.
7. Click Next to move onto bridge domain creation.
8. Use bd-Internal as the Name of the bridge domain.
9. From the Forwarding drop-down list select Custom.

CREATE TENANT

STEP 2 > NETWORK

TENANT FOUNDATION
CREATE NEW NETWORK

The screenshot shows the 'CREATE TENANT' interface for 'STEP 2 > NETWORK'. It's titled 'TENANT FOUNDATION' and 'CREATE NEW NETWORK'. A green 'NET' icon is in the top right. The main section is titled 'Specify Bridge Domain for the Network'. It includes fields for 'Name' (bd-Internal), 'Description' (optional), 'Forwarding' (Optimize selected), 'IGMP Snoop Policy' (Optimize selected), and 'Config BD MAC Address' (checkbox). The 'IGMP Snoop Policy' dropdown has 'Custom' highlighted.

10. Check the boxes to enable Flooding and Routing.
11. Select default for the IGMP Snoop Policy.

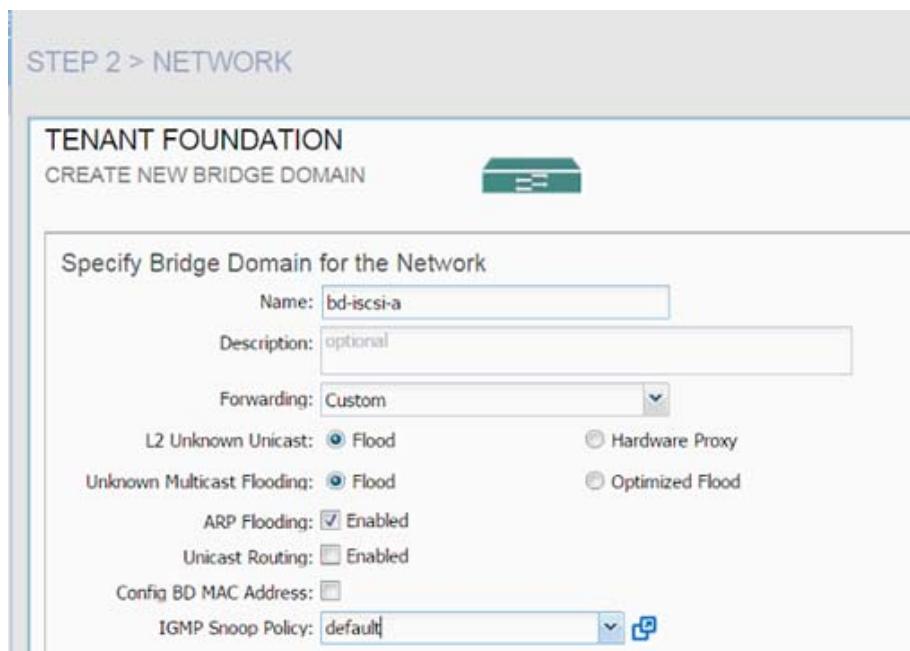
CREATE TENANT

STEP 2 > NETWORK

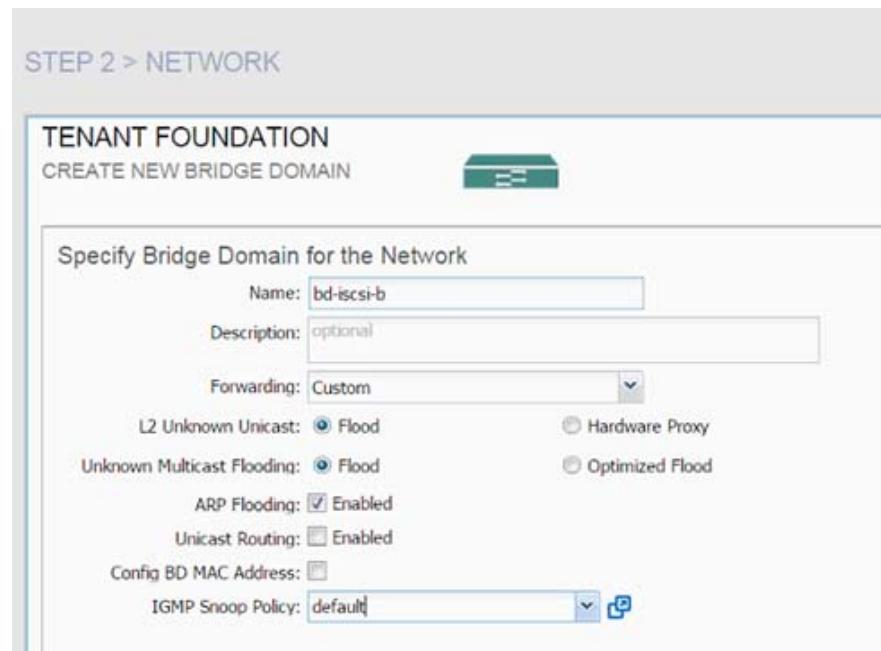
TENANT FOUNDATION
CREATE NEW NETWORK

This screenshot shows the same 'Create Tenant' interface as above, but with several checkboxes checked: 'L2 Unknown Unicast' (Flood selected), 'Unknown Multicast Flooding' (Flood selected), 'ARP Flooding' (Enabled checked), 'Unicast Routing' (Enabled checked), and 'Config BD MAC Address' (checkbox checked). The 'IGMP Snoop Policy' dropdown now shows 'default' selected.

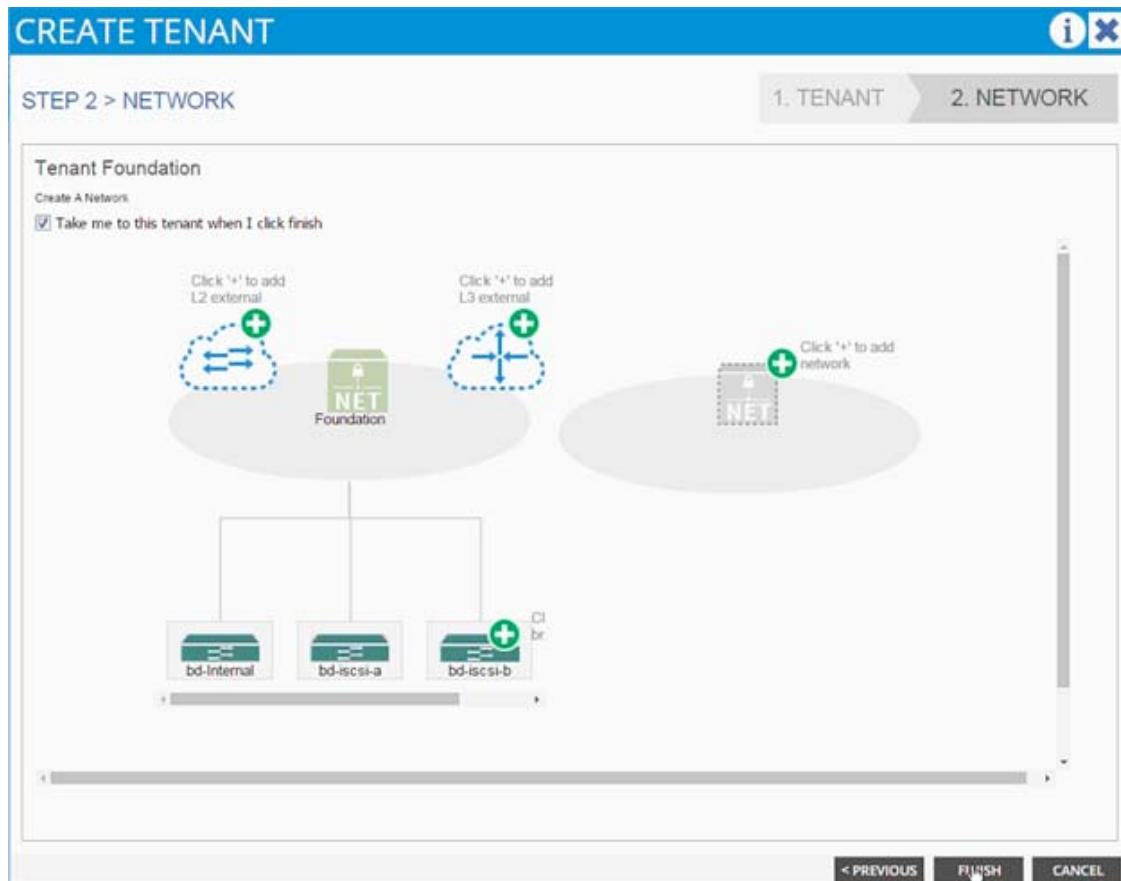
12. Click OK.
13. Click + sign next to the Bridge Domain to add another Bridge Domain.
14. Add bd-iSCSI-a as the Name.
15. Select Custom > Forwarding.
16. Enable Flooding and disable Unicast routing.
17. Set IGMP Snoop Policy to default.



18. Click Next.
19. Click OK.
20. Click + next to Bridge Domain to add another Bridge Domain.
21. Add bd-iSCSI-b as the Name.
22. Select Custom > Forwarding.
23. Enable Flooding and disable Unicast routing.
24. Set IGMP Snoop Policy to default.



25. Click Next.
26. Click OK.
27. Three Bridge Domains and the Foundation network should be visible in the CREATE TENANT dialog box.



28. Click Finish.
29. Verify the selected tenant is the newly created Foundation tenant by looking at the items highlighted in the top menu.



Application Profile Creation

In this section, two Application Profiles, iSCSI and NFS will be created.

iSCSI Application Profile Creation

1. Select Tenant and the newly created Foundation tenant from the top menu.
2. Expand Tenant Foundation in the left menu bar.
3. Right-click Application Profile and click Create Application Profiles.

4. In the CREATE APPLICATION PROFILE dialog box, enter iSCSI as the Name.
5. From the drop down menu, select default for the Monitoring Policy.
6. Click "+" next to EPG to add an EPG.

CREATE APPLICATION PROFILE

Specify Tenant Application Profile

Name:	iSCSI
Description:	optional
Tags:	<input type="text"/> enter tags separated by comma
Monitoring Policy:	default

EPGs

Name	Description

Contracts

Create EPGs on the left table to add contracts

7. In the CREATE APPLICATION EPG dialog box, enter "iscsi-a-lif" as the Name.
8. From the drop-down menu, select "bd-iscsi-a" as the Bridge Domain.
9. From the drop-down menu, select default for the Monitoring Policy.
10. Click Finish.

CREATE APPLICATION EPG

STEP 1 > IDENTITY

1. IDENTITY

Specify the EPG Identity

Name:	iscsi-a-lif						
Description:	optional						
Tags:	<input type="text"/>						
enter tags separated by comma							
QoS class:	Unspecified						
Custom QoS:	select or type to pre-provision						
Bridge Domain:	bd-iscsi-a						
Monitoring Policy:	default						
Associated Domain Profiles (VMs or bare metals):							
<input style="margin-right: 10px;" type="button" value="+"/> <input type="button" value="X"/> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Domain Profile</th> <th style="width: 30%;">Deployment Immediacy</th> <th style="width: 40%;">Resolution Immediacy</th> </tr> </thead> <tbody> <tr> <td colspan="3"></td> </tr> </tbody> </table>		Domain Profile	Deployment Immediacy	Resolution Immediacy			
Domain Profile	Deployment Immediacy	Resolution Immediacy					
Statically Link with Leaves/Paths: <input type="checkbox"/>							

< PREVIOUS **FINISH** **CANCEL**

11. Click "+" next to EPG to add another EPG.

EPGs

<input style="margin-right: 10px;" type="button" value="+"/>	<input type="button" value="X"/>
Name	Description

12. In the CREATE APPLICATION EPG dialog box, enter "iscsi-b-lif" as the Name.
 13. From the drop-down menu, select "bd-iscsi-b" as the Bridge Domain.
 14. From the drop-down menu, select default for the Monitoring Policy.
 15. Click Finish.
 16. Click "+" next to EPG to add another EPG.

EPGs

Name	Description
------	-------------

17. In the CREATE APPLICATION EPG dialog box, enter "iscsi-a-vmk" as the Name.
18. From the drop-down menu, select "bd-iscsi-a" as the Bridge Domain.
19. From the drop-down menu, select default for the Monitoring Policy.
20. Click Finish.
21. Click "+" next to EPG to add another EPG.

EPGs

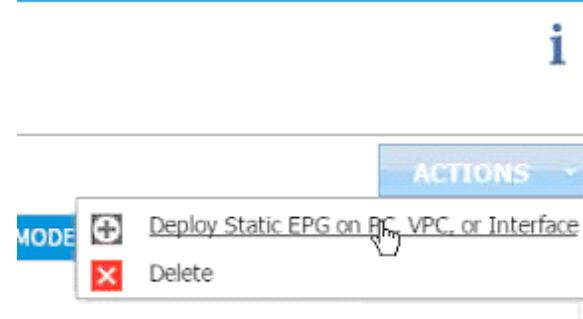
Name	Description
------	-------------

22. In the CREATE APPLICATION EPG dialog box, enter "iscsi-b-vmk" as the Name.
23. From the drop-down menu, select "bd-iscsi-b" as the Bridge Domain.
24. From the drop-down menu, select default for the Monitoring Policy.
25. Click Finish.
26. Click Submit to finish creating the Application Profile.

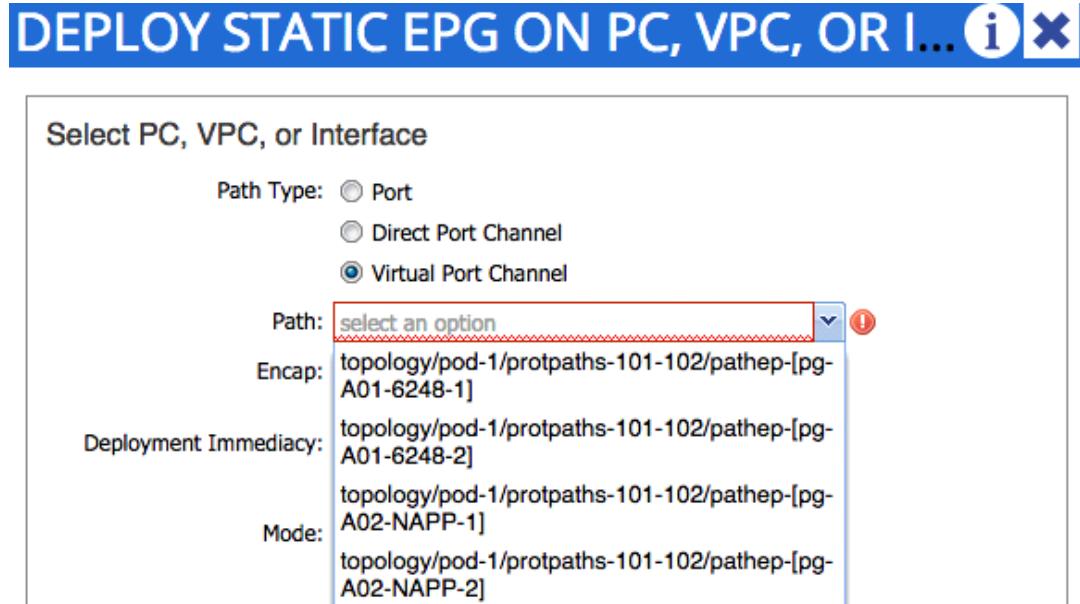
Setting Up the EPG "iscsi-a-lif"

To set up the EPG iscsi-a-lif, complete the following steps:

1. Expand the newly created iSCSI Application profile from the menu bar on the left.
2. Expand iSCSI, expand Application EPGs and expand EPG "iscsi-a-lif."
3. Click Static Bindings (Paths).
4. Click Action in the right-hand work area.
5. Click Deploy Static EPG on PC, vPC, or Interface.



6. In the DEPLOY STATIC EPG ON PC, vPC OR INTERFACE dialog box, select Virtual Port Channel as the Path Type.
7. From the drop-down menu Path, select NetApp Controller 1.



8. Enter `vlan-<<var_iscsi_vlan_A_id >>` for Encap (VLAN 901 is the iSCSI-A VLAN in the screen capture below).
9. Change Deployment Immediacy to Immediate.

DEPLOY STATIC EPG ON PC, VPC, OR I... i x

Select PC, VPC, or Interface

Path Type: Port
 Direct Port Channel
 Virtual Port Channel

Path: topology/pod-1/protpaths-101-102/pathep-[r] v +

Encap: vlan-901
For example, vlan-1

Deployment Immediacy: Immediate
 On Demand

Mode: Tagged
 Untagged
 802.1P Tag

SUBMIT CANCEL

10. Click Submit.
11. Repeat steps 4-10 for mapping NetApp Controller 2 path.
12. The Static bindings should display as shown below:

The screenshot shows the Cisco ACI Tenant Foundation interface. On the left, there is a navigation tree with 'Tenant Foundation' selected. Under 'Tenant Foundation', there are 'Application Profiles' (NFS, iSCSI), 'Application EPGs' (EPG iscsi-a-lif), and 'Contracts'. Under 'Contracts', 'Static Bindings (Paths)' is selected. On the right, a table titled 'Static Bindings (Paths)' displays two entries:

PATH	ENCAP
Node: Nodes-101-102	vlan-901
Node-101-102/pg-A02-NAPP-1	vlan-901
Node-101-102/pg-A02-NAPP-2	vlan-901

Setting Up the EPG "iscsi-b-lif"

To set up the EPG iscsi-b-lif, complete the following steps:

1. Expand the iSCSI Application profile from the menu bar on the left.
2. Expand iSCSI, expand Application EPGs and expand EPG "iscsi-b-lif".
3. Click Static Bindings (Paths).

4. Repeat Step 4-10 to add two static bindings for both NetApp controllers using `vlan-<<var_iscsi_vlan_B_id>>` as Encap.

The screenshot shows the Cisco ACI Tenant Foundation interface. On the left, the navigation bar includes 'Quick Start', 'Tenant Foundation' (selected), 'Application Profiles' (expanded, showing 'NFS' and 'iSCSI'), 'Application EPGs' (expanded, showing 'EPG iscsi-a-lif', 'EPG iscsi-a-vmk', and 'EPG iscsi-b-lif'), 'Contracts', and 'Static Bindings (Paths)' (selected). On the right, the 'Static Bindings (Paths)' panel displays a table with two entries:

PATH	ENCAP
Node: Nodes-101-102 Node-101-102/pg-A02-NAPP-1	vlan-902
Node-101-102/pg-A02-NAPP-2	vlan-902

Setting Up the EPG "iscsi-a-vmk"

To set up the EPG iscsi-a-vmk, complete the following steps:

1. Expand the iSCSI Application profile from the menu bar on the left.
2. Expand iSCSI, expand Application EPGs and expand EPG "iscsi-a-vmk".
3. Click on Static Bindings (Paths).
4. Repeat Step 30-36 to add two static bindings for both UCS Fabric Interconnects using `vlan-<<var_iscsi_vlan_A_vmk>>` as Encap.

The screenshot shows the Cisco ACI Tenant Foundation interface. On the left, the navigation bar includes 'Quick Start', 'Tenant Foundation' (selected), 'Application Profiles' (expanded, showing 'NFS' and 'iSCSI'), 'Application EPGs' (expanded, showing 'EPG iscsi-a-lif' and 'EPG iscsi-a-vmk'), 'Contracts', and 'Static Bindings (Paths)' (selected). On the right, the 'Static Bindings (Paths)' panel displays a table with two entries:

PATH	ENCAP
Node: Nodes-101-102 Node-101-102/pg-A01-6248-1	vlan-911
Node-101-102/pg-A01-6248-2	vlan-911

Setting Up the EPG "iscsi-b-vmk"

To set up the EPG iscsi-b-vmk, complete the following steps:

1. Expand the iSCSI Application profile from the menu bar on the left.
2. Expand iSCSI, expand Application EPGs and expand EPG "iscsi-b-vmk".
3. Click on Static Bindings (Paths).

- Repeat Step 4-10 to add two static bindings for both UCS Fabric Interconnects using `vlan-<<var_iscsi_vlan_B_vmk>>` as Encap.

PATH	ENCAP
Node: Nodes-101-102	
Node-101-102/pg-A01-6248-1	vlan-912
Node-101-102/pg-A01-6248-2	vlan-912

Setting Up the Provided Contracts

To set up the provided contracts, complete the following steps:

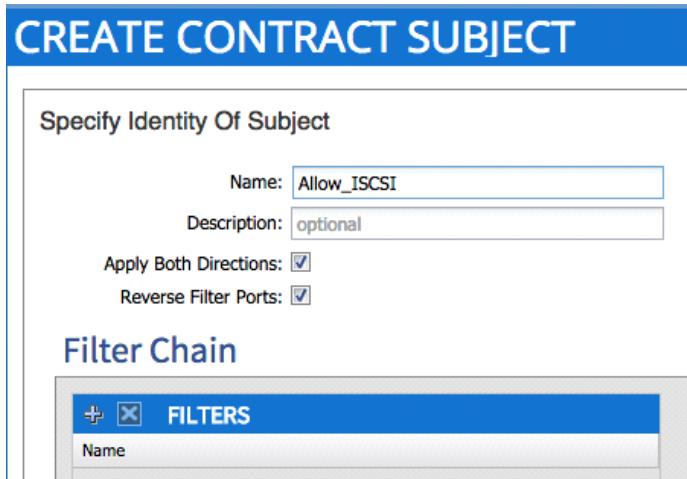
- Click EPG "iscsi-a-lif" in the left menu.
- Click Contracts under the EPG.
- Click ACTIONS and select Add Provided Contract.

TENANT NAME	CONTRACT NAME	CONTRACT TYPE	PROVIDED / CONSUMED	QOS CLASS	STATE	CONSUMER	PROVIDER	CON
Contract Type: Contract								

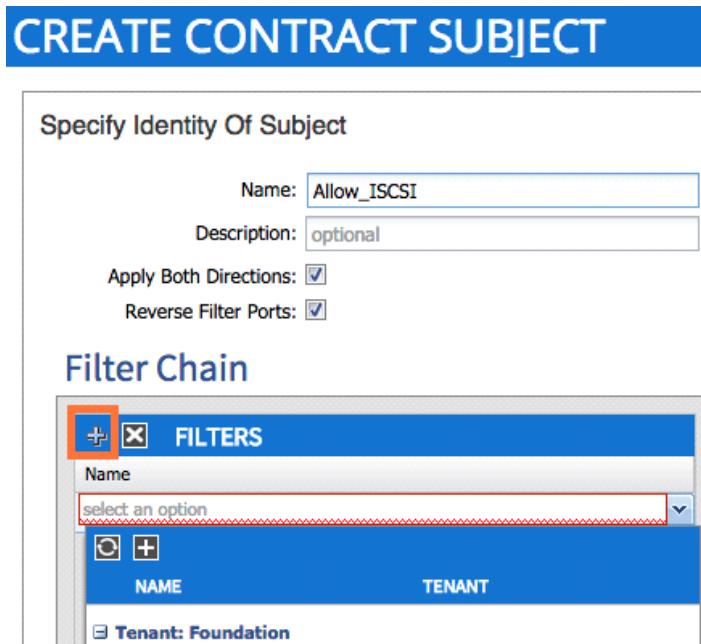
- From the ADD PROVIDED CONTRACT dialog box, select Create Contract under Contract.

- Enter Allow_ISCSI for the Name in the CREATE CONTRACT dialog box.
- Set Scope to Tenant.

7. Click "+" next to Subjects to add a new contract subject.
8. In the CREATE CONTRACT SUBJECT dialog box, enter Allow_ISCSI as the Name.
9. Click "+" under Filter Chain to add a new filter.



10. From the drop-down menu under FILTERS click "+".



11. In the CREATE FILTER dialog box, enter Allow_ISCSI as the Name. This example allows all the traffic for this contract.
12. Click "+" to add a filter.

CREATE FILTER

Specify the Filter Identity

Name:	Allow_ISCSI								
Description:	optional								
Entries:	<input type="button" value="+"/> <input type="button" value="X"/>								
<table border="1"> <thead> <tr> <th>Name</th> <th>EtherType</th> <th>ARP Flag</th> <th>IP Protocol</th> </tr> </thead> <tbody> <tr> <td>tcp3260</td> <td>IP</td> <td>Unspecified</td> <td>tcp</td> </tr> </tbody> </table>		Name	EtherType	ARP Flag	IP Protocol	tcp3260	IP	Unspecified	tcp
Name	EtherType	ARP Flag	IP Protocol						
tcp3260	IP	Unspecified	tcp						

13. Enter tcp3260 as the name of the filter.
14. From drop-down menu, select IP as EtherType.
15. From drop-down menu, select TCP as IP Protocol.
16. In Destination Port/Range type 3260 as both From and To ports.

CREATE FILTER

Specify the Filter Identity

Name:	Allow_ISCSI																		
Description:	optional																		
Entries:	<input type="button" value="+"/> <input type="button" value="X"/>																		
<table border="1"> <thead> <tr> <th>Name</th> <th>EtherType</th> <th>ARP Flag</th> <th>IP Protocol</th> <th>Allow Fragment</th> <th>Source Port / Range</th> <th>Destination Port / Range</th> <th>TCP Session Rules</th> </tr> </thead> <tbody> <tr> <td>tcp3260</td> <td>IP</td> <td>Unspecified</td> <td>tcp</td> <td><input type="checkbox"/></td> <td>From Unspecified</td> <td>To 3260</td> <td>From 3260</td> <td>To 3260</td> <td>Unspecified</td> </tr> </tbody> </table>		Name	EtherType	ARP Flag	IP Protocol	Allow Fragment	Source Port / Range	Destination Port / Range	TCP Session Rules	tcp3260	IP	Unspecified	tcp	<input type="checkbox"/>	From Unspecified	To 3260	From 3260	To 3260	Unspecified
Name	EtherType	ARP Flag	IP Protocol	Allow Fragment	Source Port / Range	Destination Port / Range	TCP Session Rules												
tcp3260	IP	Unspecified	tcp	<input type="checkbox"/>	From Unspecified	To 3260	From 3260	To 3260	Unspecified										

UPDATE CANCEL

17. Click Update.
18. Click Submit to create the filter.
19. Click Update to add the newly created filter to the filter chain.
20. Click OK to finish creating the Contract Subject.
21. Click Submit.
22. Click Submit again to finish adding a provided contract.
23. Verify the Provided Contract appears under the Contracts as shown below:

Tenant Foundation

- iSCSI
- Application EPGs
 - EPG iscsi-a-lif
 - Contracts
 - Static Bindings (Paths)
 - Static Bindings (Leaves)
 - Static EndPoint
 - Subnets

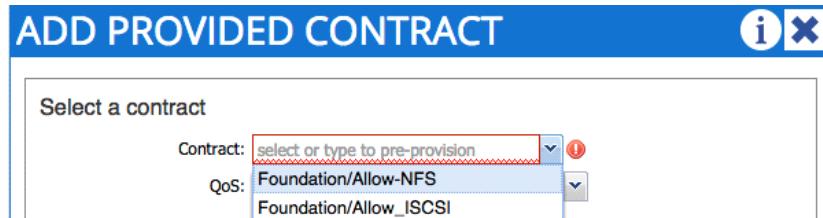
Contracts

TENANT NAME	CONTRACT NAME	CONTRACT TYPE	PROVIDED / CONSUMED	QOS CLASS	STATE
Foundation	Allow_ISCSI	Contract	Provided	Unspecified	formed

Contract Type: Contract

24. Click EPG "iscsi-b-lif" in the left menu.
25. Click Contracts under the EPG.

26. Click Actions and select Add Provided Contract.
27. From the drop-down menu, select the recently created Allow_ISCSI contract.



28. Click "SUBMIT" to add the "Allow_ISCSI" contract as the "Provided" contract for EPG iscsi-b-lif as well.

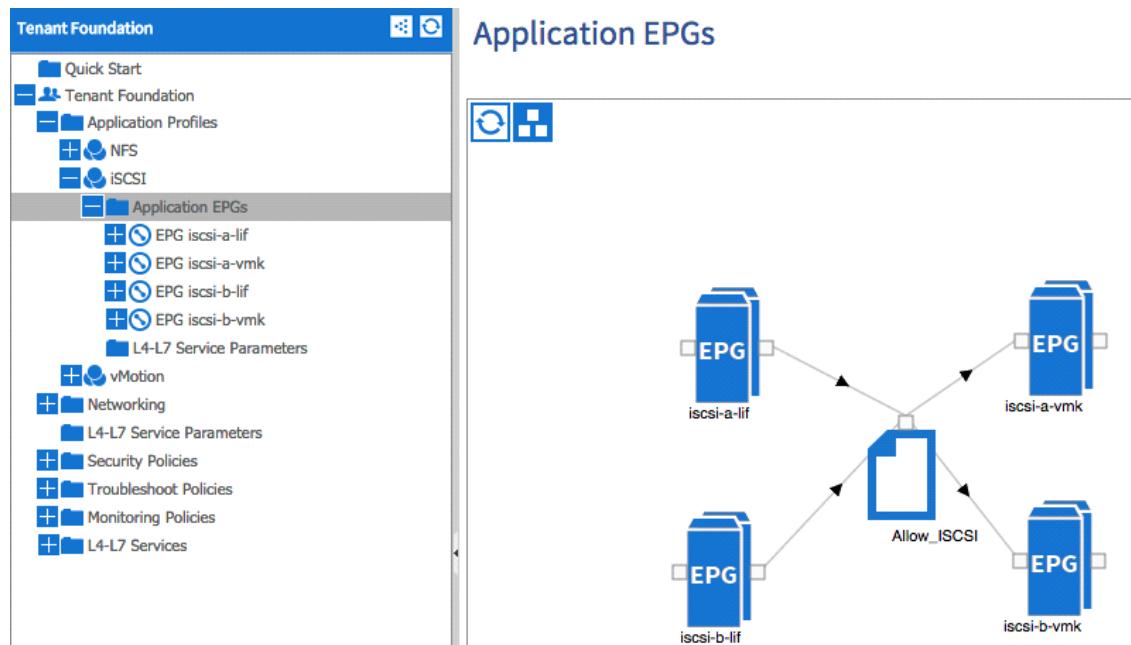
Setting Up the Consumes Contracts

To set up the Consumed contract, complete the following steps:

1. Click EPG "iscsi-a-vmk" in the left menu.
2. Click Contracts under the EPG.
3. In the ADD CONSUMED CONTRACT dialog box, from the drop-down menu select Foundation/Allow_ISCSI contract (defined in the previous step).



4. Click Submit.
5. Click on EPG "iscsi-b-vmk" in the left menu.
6. Click Contracts under the EPG.
7. In the ADD CONSUMED CONTRACT dialog box, from the drop-down menu select Foundation/Allow_ISCSI contract.
8. To validate the contract definition, click Application EPGs under Application Profile iSCSI in the left menu bar. The contract should appear as shown below:



Create the NFS Application Profile

To create the NFS application profile, complete the following steps:

1. Expand Tenant Foundation in the left menu bar.
2. Right-click Application Profile and click Create Application Profile.
3. In the CREATE APPLICATION PROFILE dialog box, enter NFS as the Name.
4. From the drop-down list, select default for Monitoring Policy.
5. Click + next to EPG to add an EPG.

CREATE APPLICATION PROFILE

Specify Tenant Application Profile

Name:	NFS
Description:	optional
Tags:	enter tags separated by comma
Monitoring Policy:	default

EPGs

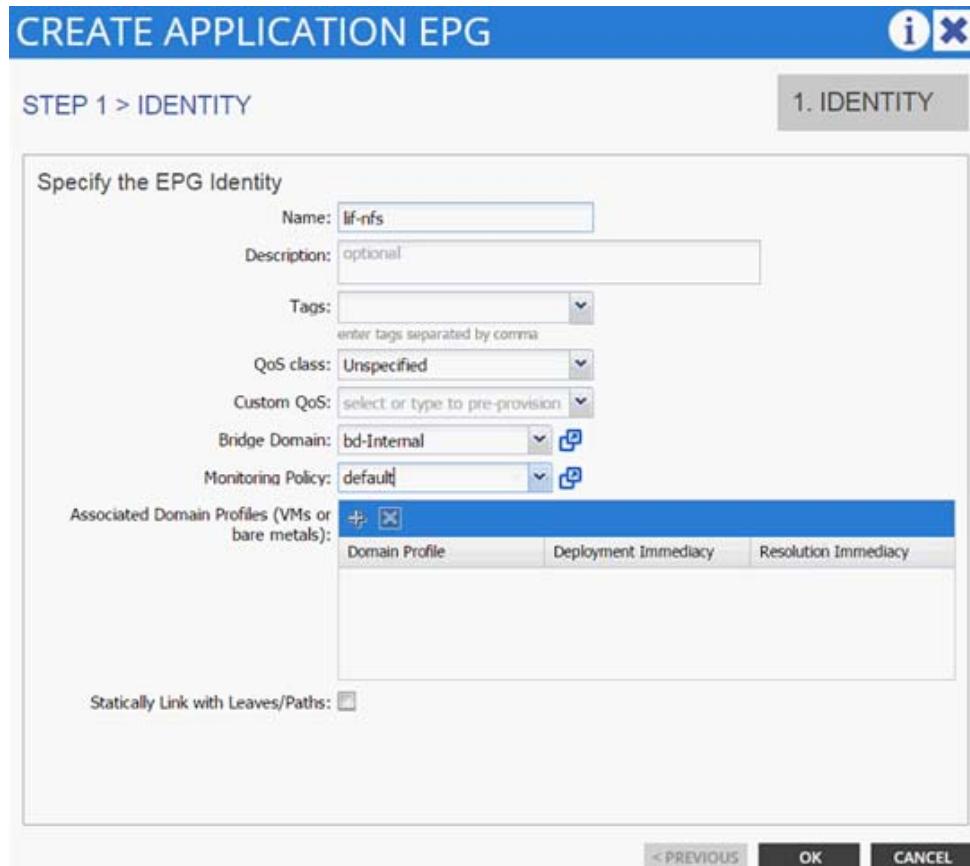
Name	Description
lif-nfs	

Contracts

Create EPGs on the left table to add contracts

6. In the CREATE APPLICATION EPG dialog box, enter lif-nfs as the Name.

7. From the drop-down list, select bd-internal as the Bridge Domain.
8. From the drop-down list, select default for Monitoring Policy.



9. Click OK.
10. Click + next to EPG to another EPG.

EPGs	
Name	Description
lif-nfs	

11. In the CREATE APPLICATION EPG dialog box, enter vmk-nfs as the Name.
12. From the drop-down list, select bd-internal as the Bridge Domain.
13. From the drop-down list, select default > Monitoring Policy.

CREATE APPLICATION EPG

STEP 1 > IDENTITY

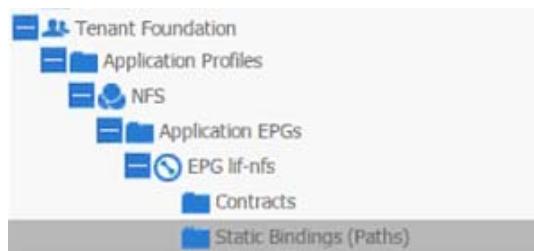
1. IDENTITY

Specify the EPG Identity

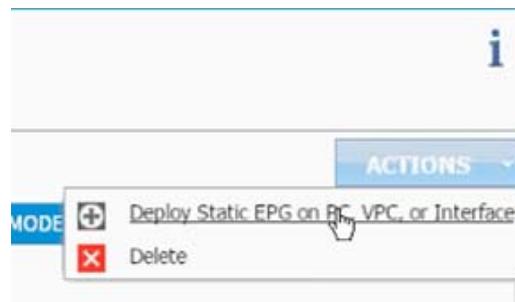
Name:	vmk-nfs						
Description:	optional						
Tags:	<input type="text"/>						
QoS class:	Unspecified						
Custom QoS:	select or type to pre-provision						
Bridge Domain:	bd-Internal						
Monitoring Policy:	default						
Associated Domain Profiles (VMs or bare metals):	<input type="button" value="+"/> <input type="button" value="X"/> <table border="1"> <thead> <tr> <th>Domain Profile</th> <th>Deployment Immediacy</th> <th>Resolution Immediacy</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Domain Profile	Deployment Immediacy	Resolution Immediacy			
Domain Profile	Deployment Immediacy	Resolution Immediacy					
Statically Link with Leaves/Paths:	<input type="checkbox"/>						

< PREVIOUS CANCEL

14. Click OK.
15. Click SUBMIT to finish creating the Application Profile.
16. Expand the newly created NFS Application profile from the menu bar on the left.
17. Expand NFS, expand Application EPGs and expand EPG lif-nfs.
18. Click Static Bindings (Paths).



19. Click Action.
20. Click Deploy Static EPG on PC, vPC, or Interface.



21. In the DEPLOY STATIC EPG ON PC, vPC OR INTERFACE dialog box, select Virtual Port Channel as the Path Type.
22. From the Path drop-down list, select NetApp Controller 1.

DEPLOY STATIC EPG ON PC, VPC, OR I... i X

Select PC, VPC, or Interface

Path Type: Virtual Port Channel

Path: !

Encap:

- topology/pod-1/protpaths-101-102/pathep-[pg-A01-6248-1]
- topology/pod-1/protpaths-101-102/pathep-[pg-A01-6248-2]
- topology/pod-1/protpaths-101-102/pathep-[pg-A02-NAPP-1] !
- topology/pod-1/protpaths-101-102/pathep-[pg-A02-NAPP-2]
- 802.1P Tag

Deployment Immediacy:

Mode:

SUBMIT CANCEL

23. Enter `vlan-< NFS LIF VLAN>` for Encap (VLAN 3170 is the NFS VLAN on NetApp Controller in the screenshot below).
24. Change Deployment Immediacy to Immediate.

DEPLOY STATIC EPG ON PC, VPC, OR I... i x

Select PC, VPC, or Interface

Path Type: Port
 Direct Port Channel
 Virtual Port Channel

Path: topology/pod-1/protpaths-101-102/pathep-[pg] [] []

Encap: vlan-3170
For example, vlan-1.

Deployment Immediacy: Immediate
 On Demand

Mode: Tagged
 Untagged
 802.1P Tag

SUBMIT CANCEL

25. Click Submit.
26. Validate the path appears in the work area on the right.

Static Bindings (Paths)		
PATH	ENCAP	DEPLOYMENT IMMEDIACY
Node: Nodes-101-102	vlan-3170	Immediate

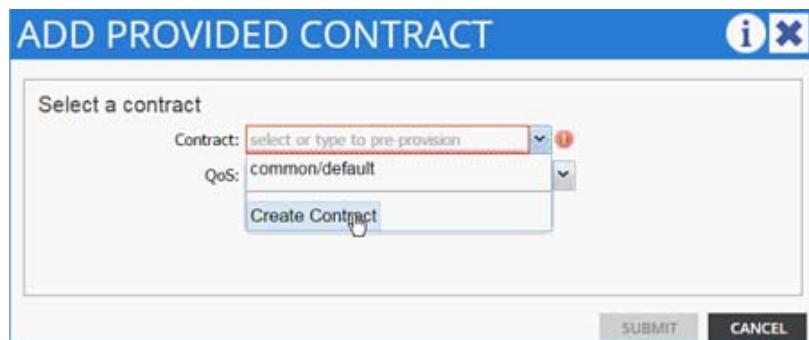
27. Repeat these steps for mapping the NetApp Controller 2 path.
28. Static bindings should be similar to the screenshot below.

Static Bindings (Paths)		
PATH	ENCAP	DEPLOYMENT IMMEDIACY
Node: Nodes-101-102	vlan-3170	Immediate
Node: Nodes-101-102	vlan-3170	Immediate

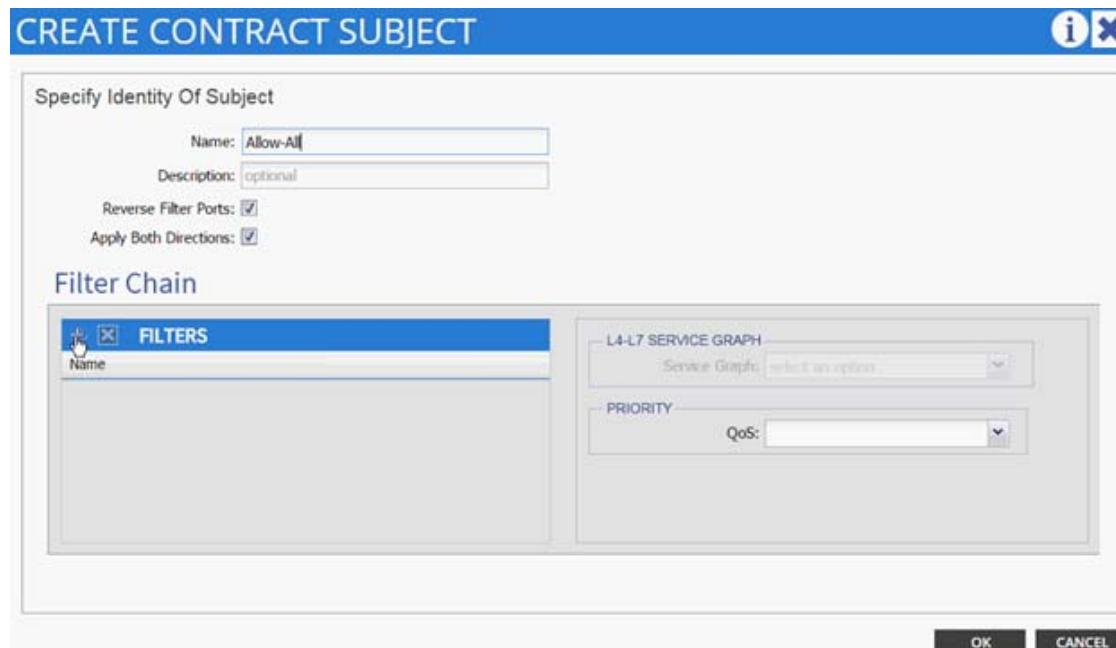
29. Click Contracts under the EPG lif-nfs.
30. Click Action and select Add Provided Contract.



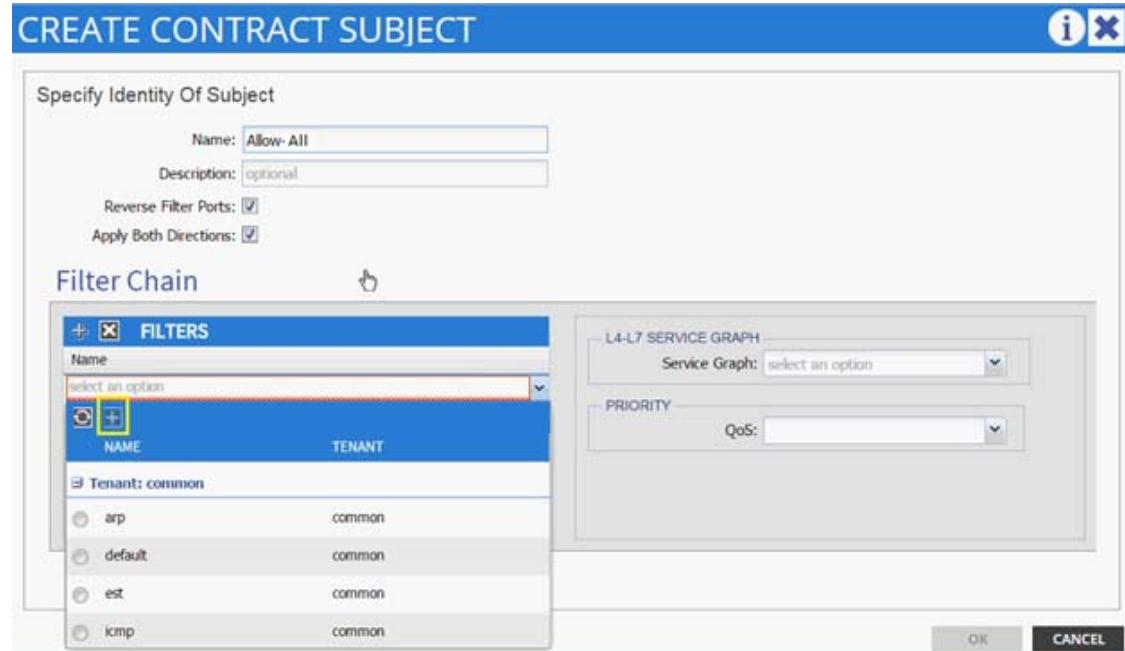
31. From the ADD PROVIDED CONTRACT dialog box, select Create Contract under Contract.



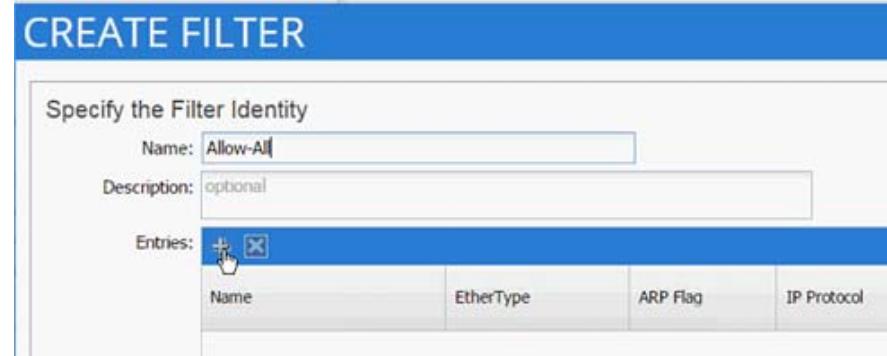
32. Enter Allow-NFS as Name in the CREATE CONTRACT dialog box.
33. Click + next to Subjects to add a new contract subject.
34. In the CREATE CONTRACT SUBJECT dialog box, enter Allow-All as the Name.
35. Click + under Filter Chain to add a new filter.



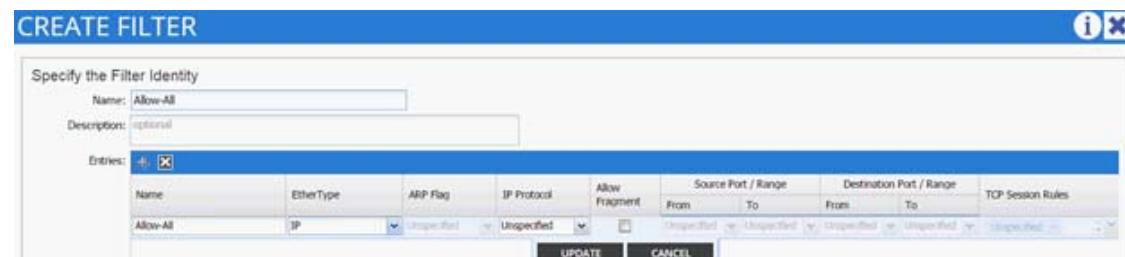
36. From the FILTERS drop-down list click +.



37. In the CREATE FILTER dialog box, enter Allow-All as the Name. In this example, allow all the traffic for this contract.
38. Click + to add a filter.

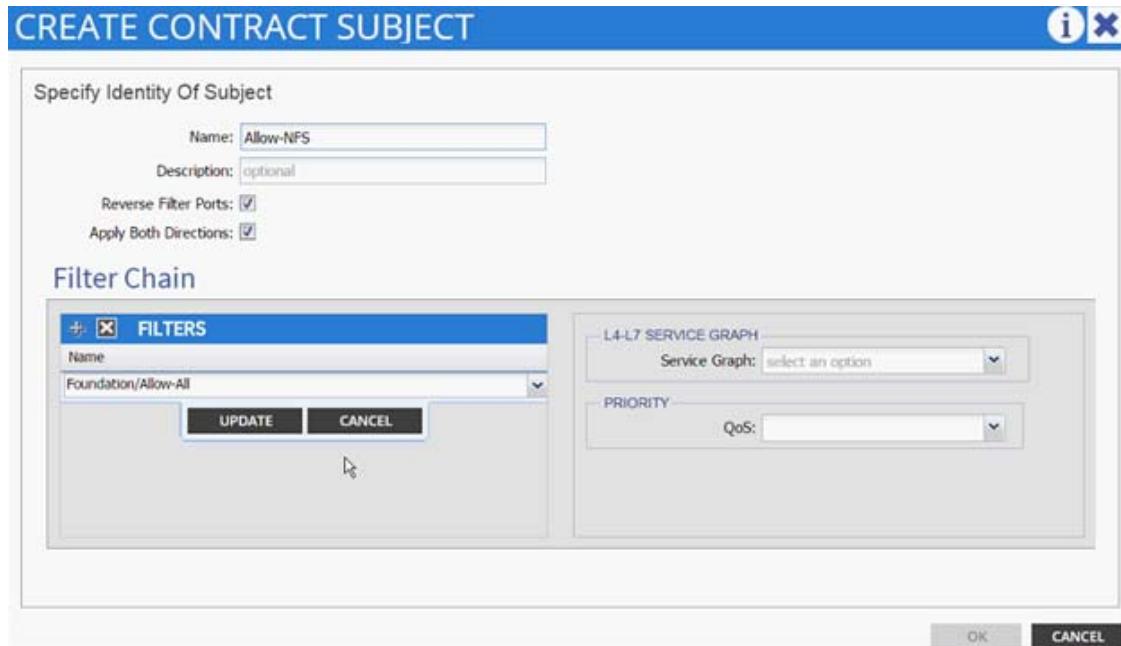


39. Enter Allow-All as the name of the filter.
40. From the drop-down list, select IP as Ethertype.

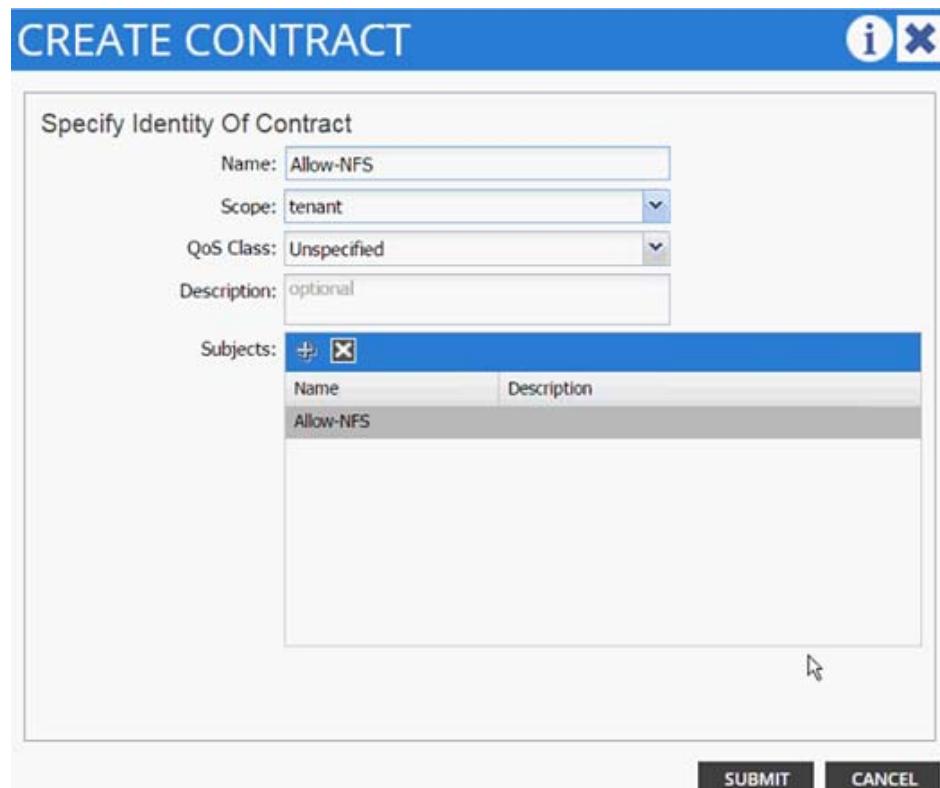


41. Click Update.

42. Click SUBMIT to create the filter.
43. Click UPDATE to add the newly created filter to the filter chain.



44. Click OK to finish creating the Contract Subject.
45. Change the Scope to "tenant" from the drop-down list.

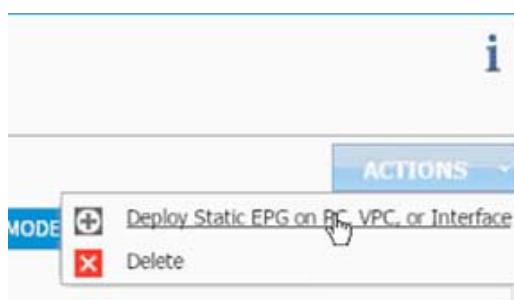


46. Click SUBMIT.
47. Click SUBMIT again to finish adding a provided contract.
48. Verify the Provided Contract appears under the Contracts.

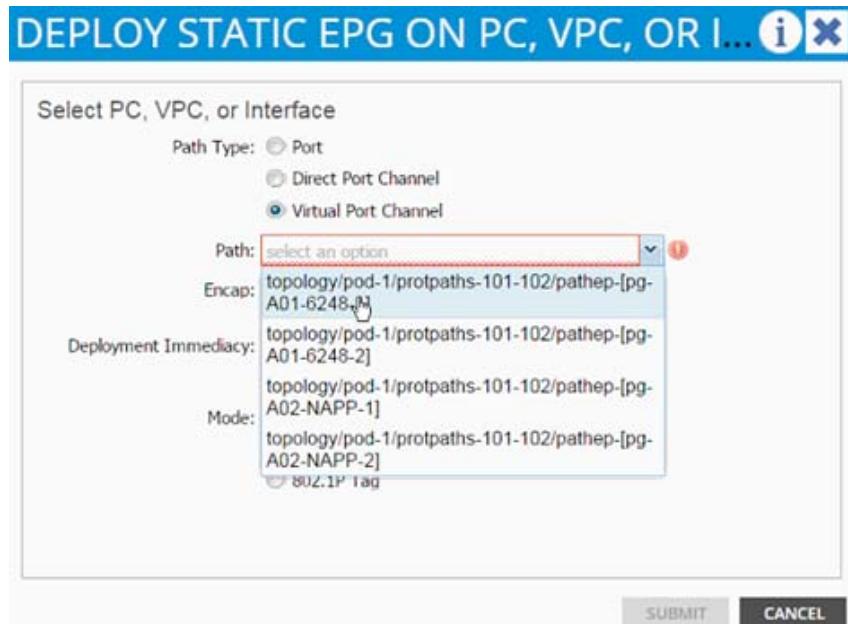
TENANT NAME	CONTRACT NAME	CONTRACT TYPE	PROVIDED / CONSUMED	QOS CLASS	STATE
Foundation	Allow-NFS	Contract	Provided	Unspecified	formed

49. Expand the NFS Application profile from the menu bar on the left.
50. Expand NFS, expand Application EPGs, and expand EPG vmk-nfs.
51. Click Static Bindings (Paths).

52. Click Action.
53. Click Deploy Static EPG on PC, vPC, or Interface.



54. In the DEPLOY STATIC EPG ON PC, vPC OR INTERFACE dialog box, select Virtual Port Channel as the Path Type.
55. From the Path drop-down list, select UCS Fabric Interconnect A.



- 56.** Enter `vlan-<NetApp VMK VLAN>` for Encap; VLAN 3270 is the NFS VLAN on UCS Fabric Interconnect in the screenshot below.



Note A VLAN on a certain path can only be mapped to a single EPG. Since VLAN 3170 (NFS VLAN on NetApp) is already mapped to EPG lif-NFS, VLAN 3270 was selected as the VLAN to host ESXi VMKernel ports. The VMKernel ports and the NetApp LIFs will still be defined in the same IP subnet; ACI Fabric will enable seamless IP connectivity when contracts are defined between the two EPGs.

- 57.** Change Deployment Immediacy to Immediate.

DEPLOY STATIC EPG ON PC, VPC, OR I... i X

Select PC, VPC, or Interface

Path Type: Port
 Direct Port Channel
 Virtual Port Channel

Path: topology/pod-1/protpaths-101-102/pathep-[pg] vlan-3270 [x]

Encap:
For example, vlan-1

Deployment Immediacy: Immediate
 On Demand

Mode: Tagged
 Untagged
 802.1P Tag

SUBMIT CANCEL

58. Click Submit.

59. Validate the path appears

PATH	ENCAP	DEPLOYMENT IMMEDIACY
Node: Nodes-101-102 Node-101-102/pg-A01-6248-1	vlan-3270	Immediate

60. Repeat these steps for mapping UCS Fabric Interconnect B path.

61. Static bindings should be similar to the screenshot below.

The screenshot shows the Cisco ACI Tenant Foundation interface. The left sidebar lists categories: Quick Start, Tenant Foundation, Application Profiles, NFS, Application EPGs, Contracts, Static Bindings (Paths), Static Bindings (Leaves), and Static EndPoint. The 'Static Bindings (Paths)' item is selected. The main panel displays 'Static Bindings (Paths)' with two entries:

PATH	ENCAP
Node: Nodes-101-102	vlan-3270
Node-101-102/pg-A01-6248-1	vlan-3270
Node-101-102/pg-A01-6248-2	vlan-3270

62. Click Contracts in the left menu.
63. Click Actions on the right and select Add Consumed Contract.

The screenshot shows the Cisco ACI Contracts interface. The left sidebar lists categories: Quick Start, Tenant Foundation, Application Profiles, NFS, Application EPGs, Contracts, Static Bindings (Paths), and Static Bindings (Leaves). The 'Contracts' item is selected. The main panel displays a table titled 'Contracts' with one row:

TENANT NAME	CONTACT NAME	CONTRACT TYPE	PROMISED / CONSUMED	QOS CLASS	STATE
					No items have been found. Select Actions to create a new item.

On the right, there is a 'Actions' menu with options: ADD Consumed Contract, ADD Consumed Contract Interface, ADD Provider Contract, ADD Tenant Contract, and Delete.

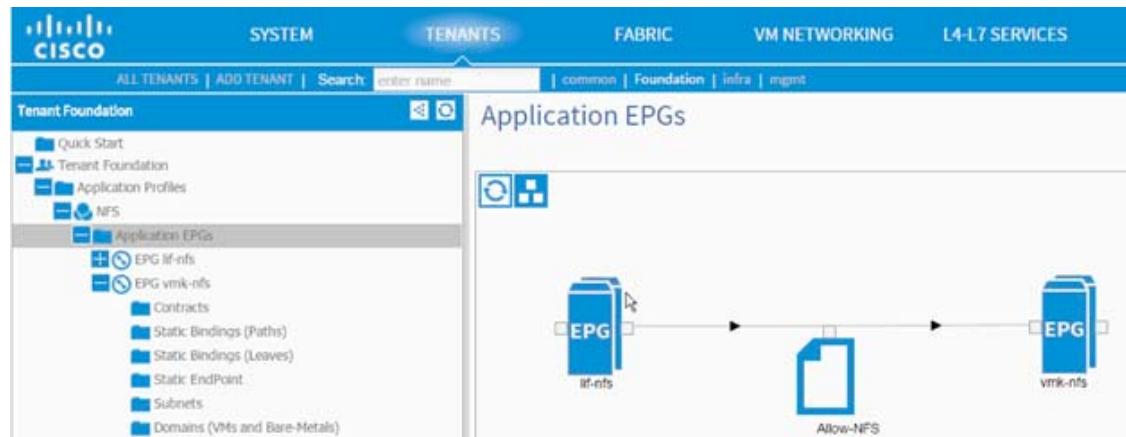
64. In the ADD CONSUMED CONTRACT dialog box, from the drop-down list select Foundation/Allow-NFS contract (defined previously).

The screenshot shows the 'ADD CONSUMED CONTRACT' dialog box. It has a title bar with 'ADD CONSUMED CONTRACT' and a close button. The main area is titled 'Select a contract' and contains two dropdown menus:

- Contract: Foundation/Allow-NFS
- QoS: Unspecified

At the bottom are 'SUBMIT' and 'CANCEL' buttons.

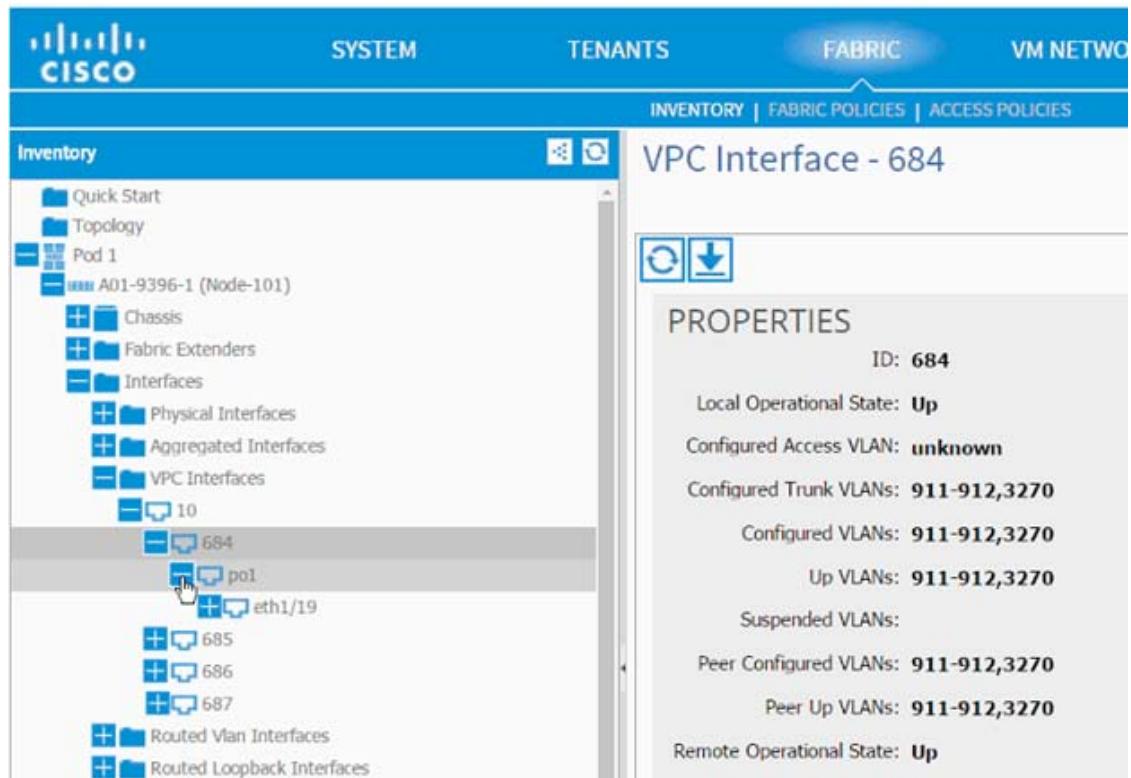
65. Click Submit.
66. To validate the contract definition, click Application EPGs under Application Profile NFS in the left menu bar. The contract should appear as shown in the screenshot below.



Path (vPC) Validation

Previously in this section, both the iSCSI and NFS paths and VLANs were mapped to the appropriate EPGs. These VLANs were also defined in the physical domains associated with the VPCs. At this point the Foundation tenant is deployed and should provide connectivity between the ESXi hosts and NetApp controllers. To validate connectivity, VPCs can be checked for appropriate VLAN forwarding.

1. To validate the VLAN forwarding on the vPC, select FABRIC from the top menu and select INVENTORY from the sub-menu.
2. Expand Pod 1, Leaf switch, Interfaces, and then vPC Interfaces.
3. Expand the vPC domain (10) and click a vPC.
4. As shown in the screenshot below, the vPC should show both the iSCSI and NFS VLANs being forwarded.



5. Repeat these steps to validate all the VPCs.
6. Optional: Log into the Leaf using CLI and issue a `show vpc` command.

```

Peer status : peer adjacency formed ok
vPC keep-alive status : Disabled
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 inconsistency reason : Consistency Check Not Performed
vPC role : primary
Number of vPCs configured : 4
Peer Gateway : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Enabled (timeout = 240 seconds)
Operational Layer3 Peer : Disabled

vPC Peer-link status
-----
id Port Status Active vlans
-- -- --
1 up -
vPC status
-----
id Port Status Consistency Reason Active vlans
-- -- --
684 Po1 up success success 911-912,327
0
685 Po2 up success success 911-912,327
0
686 Po3 up success success 911-912,317
0
687 Po4 up success success 911-912,317
0

```

Storage Part 2 - SAN Boot

Clustered Data ONTAP SAN Boot Storage Setup

iSCSI LIF in Clustered Data ONTAP

1. Create iSCSI logical interfaces (LIFs).

```

network interface create -vserver Infra_Vserver -lif iscsi_lif01a -role data
-data-protocol iscsi -home-node <<var_node01>> -home-port
a0a-<<var_iscsi_a_vlan_id>> -address <<var_node01_iscsi_lif01a_ip>> -netmask
<<var_node01_iscsi_lif01a_mask>> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false

network interface create -vserver Infra_Vserver -lif iscsi_lif01b -role data
-data-protocol iscsi -home-node <<var_node01>> -home-port
a0a-<<var_iscsi_b_vlan_id>> -address <<var_node01_iscsi_lif01b_ip>> -netmask
<<var_node01_iscsi_lif01b_mask>> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false

```

```

network interface create -vserver Infra_Vserver -lif iscsi_lif02a -role data
-data-protocol iscsi -home-node <<var_node02>> -home-port
a0a-<<var_iscsi_a_vlan_id>> -address <<var_node02_iscsi_lif02a_ip>> -netmask
<<var_node02_iscsi_lif02a_mask>> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false

network interface create -vserver Infra_Vserver -lif iscsi_lif02b -role data
-data-protocol iscsi -home-node <<var_node02>> -home-port
a0a-<<var_iscsi_b_vlan_id>> -address <<var_node02_iscsi_lif02b_ip>> -netmask
<<var_node02_iscsi_lif02b_mask>> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false

network interface show -vserver Infra_Vserver

```

Create igroups

- From the cluster management node SSH connection, enter the following:

```

igroup create -vserver Infra_Vserver -igroup VM-Host-Infra-01 -protocol
iscsi -ostype vmware -initiator <<var_vm_host_infra_01_iqn>>

igroup create -vserver Infra_Vserver -igroup VM-Host-Infra-02 -protocol
iscsi -ostype vmware -initiator <<var_vm_host_infra_02_iqn>>

igroup create -vserver Infra_Vserver -igroup MGMT-Hosts -protocol iscsi
-ostype vmware -initiator <<var_vm_host_infra_01_iqn>>,
<<var_vm_host_infra_02_iqn>>

```



Note

Use the values listed in [Table 21](#) for the IQN information.



Note

To view the three igroups just created, type `igroup show`.

Map Boot LUNs to igroups

- From the cluster management SSH connection, enter the following:

```

lun map -vserver Infra_Vserver -volume esxi_boot -lun VM-Host-Infra-01
-igroup VM-Host-Infra-01 -lun-id 0
lun map -vserver Infra_Vserver -volume esxi_boot -lun VM-Host-Infra-02
-igroup VM-Host-Infra-02 -lun-id 0

```

VMware vSphere 5.5 Setup

VMware ESXi 5.5 Update 2

This section provides detailed instructions for installing VMware ESXi 5.5 Update 2 in an environment. After the procedures are completed, two booted ESXi hosts will be provisioned.

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 boot logical unit numbers (LUNs).

Download Cisco Custom Image for ESXi 5.5.0 U2

1. Click the link [vmware login page](#)
2. Type your email or customer number and the password and then click Log in.
3. Click the link [CiscoCustomImage5.5.0U2](#).
4. Click Download Now.
5. Save it to your destination folder.

This ESXi 5.5.0 U2 Cisco custom image includes updates for the fnic and enic drivers. The versions that are part of this image are:

- Enic: 2.1.2.59
- Fnic: 1.6.0.12

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 Cisco UCS environment to run the IP KVM.

To log in to the Cisco UCS environment, complete the following 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. To download the Cisco UCS Manager software, click the Launch UCS Manager link.
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. To log in to Cisco UCS Manager, click Login.
6. From the main menu, click the Servers tab.
7. Select Servers > Service Profiles > root > VM-Host-Infra-01.
8. Right-click VM-Host-Infra-01 and select KVM Console.
9. If prompted to accept an Unencrypted KVM session, accept as necessary.
10. Select Servers > Service Profiles > root > VM-Host-Infra-02.
11. Right-click VM-Host-Infra-02. and select KVM Console.
12. If prompted to accept an Unencrypted KVM session, accept as necessary.

Set Up VMware ESXi Installation

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

To prepare the server for the OS installation, complete the following steps on each ESXi host:

1. In the KVM window, click the Virtual Media node.
2. If prompted to accept an Unencrypted KVM session, accept as necessary.
3. Click Add Image.
4. Browse to the ESXi installer ISO image file and click Open.
5. Select the Mapped checkbox to map the newly added image.
6. Click the KVM tab to monitor the server boot.
7. Boot the server by selecting Boot Server and clicking 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, complete the following steps on each host:

1. On reboot, the machine detects the presence of the ESXi installation media. Select the ESXi installer from the boot 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. Select the LUN that was previously set up as the installation disk for ESXi and press Enter to continue with the installation.
5. Select the appropriate keyboard layout and press Enter.
6. Enter and confirm the root password and press Enter.
7. The installer issues a warning that the selected disk will be repartitioned. Press F11 to continue with the installation.
8. After the installation is complete, click on the Virtual Media tab and clear the P mark next to the ESXi installation media. Click Yes.



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

9. 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, complete the following 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, complete the following steps:

1. After the server has finished rebooting, press F2 to customize the system.
2. Log in as `root`, enter the corresponding password, and press Enter to log in.
3. Select the Configure the Management Network option and press Enter.
4. Select the VLAN (Optional) option and press Enter.
5. Enter the <>var_oob_mgmt_vlan_id>> and press Enter.
6. Select Network Adapters option and select `vmnic4` (defined earlier as OOB vNIC) and press Enter.
7. From the Configure Management Network menu, select IP Configuration and press Enter.
8. Select the Set Static IP Address and Network Configuration option by using the space bar.
9. Enter the IP address for managing the first ESXi host: <>var_vm_host_infra_01_ip>>.
10. Enter the subnet mask for the first ESXi host.
11. Enter the default gateway for the first ESXi host.
12. Press Enter to accept the changes to the IP configuration.
13. Select the IPv6 Configuration option and press Enter.
14. Using the spacebar, unselect Enable IPv6 (restart required) and press Enter.
15. Select the DNS Configuration option and press Enter.



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

16. Enter the IP address of the primary DNS server.
17. Optional: Enter the IP address of the secondary DNS server.
18. Enter the fully qualified domain name (FQDN) for the first ESXi host.
19. Press Enter to accept the changes to the DNS configuration.
20. Press Esc to exit the Configure Management Network submenu.
21. Press Y to confirm the changes and return to the main menu.
22. The ESXi host reboots. After reboot, press F2 and log back in as root.
23. Select Test Management Network to verify that the management network is set up correctly and press Enter.
24. Press Enter to run the test.
25. Press Enter to exit the window.
26. 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, complete the following 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. Select the Configure the Management Network option and press Enter.
4. Select the VLAN (Optional) option and press Enter.
5. Enter the <>var_oob-mgmt_vlan_id>> and press Enter.
6. Select Network Adapters option and select vmnic4 (defined earlier as OOB vNIC) and press Enter.
7. From the Configure Management Network menu, select IP Configuration and press Enter.
8. Select the Set Static IP Address and Network Configuration option by using the space bar.
9. Enter the IP address for managing the second ESXi host: <>var_vm_host_infra_02_ip>>.
10. Enter the subnet mask for the second ESXi host.
11. Enter the default gateway for the second ESXi host.
12. Press Enter to accept the changes to the IP configuration.
13. Select the IPv6 Configuration option and press Enter.
14. Using the spacebar, clear Enable IPv6 (restart required) and press Enter.
15. Select the DNS Configuration option and press Enter.



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

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

Download VMware vSphere Client

To download the VMware vSphere Client, complete the following 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 the vSphere Client.



Note This application is downloaded from the VMware website and Internet access is required on the management workstation.

Download VMware vSphere CLI 5.5

1. Click the link [VMware vSphere CLI 5.5](#)
2. Select your OS and click Download.
3. Save it to the destination folder.
4. Run the VMware-vSphere-CLI-5.5.0.exe.
5. Click Next.
6. Accept the terms for the license and click Next.
7. Click Next on the Destination Folder screen.
8. Click Install.
9. Click Finish.



Note Install VMware vSphere CLI 5.5 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, complete the following 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, complete the following 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.

Set Up VMkernel Ports and Virtual Switch

ESXi Host VM-Host-Infra-01

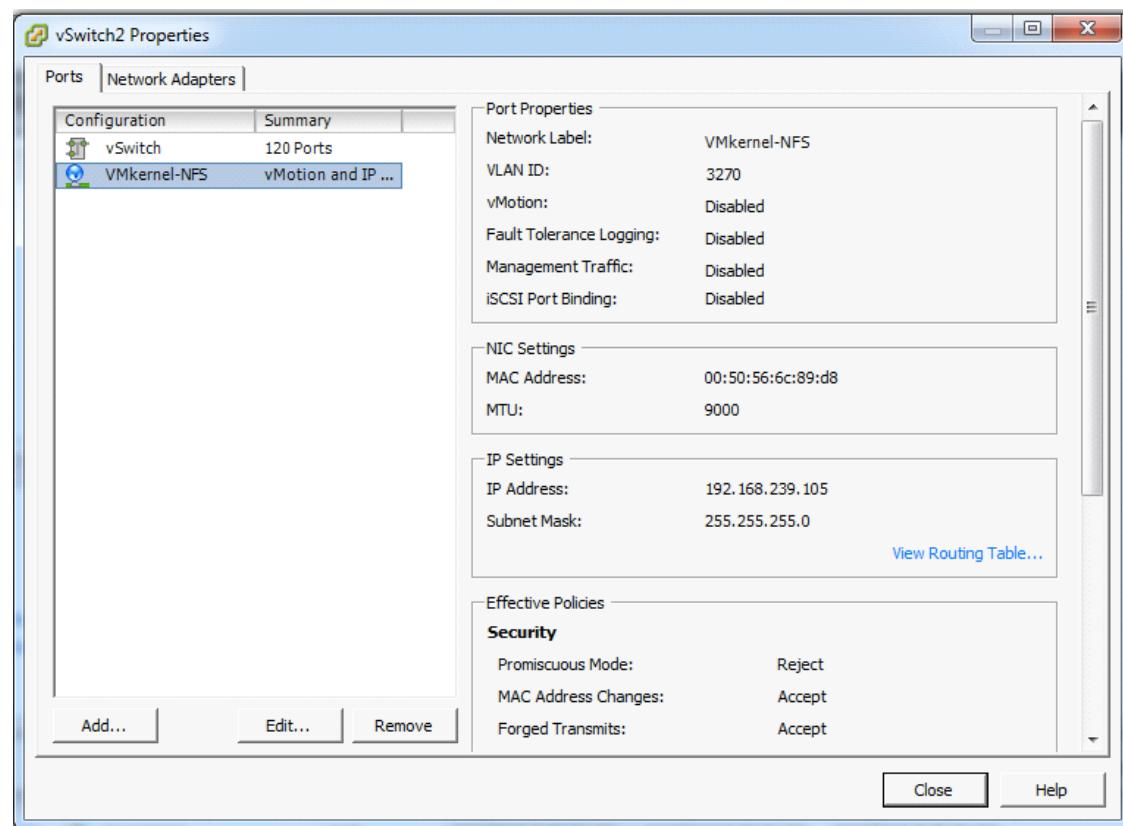
To set up the VMkernel ports and the virtual switches on the VM-Host-Infra-01 ESXi host, complete the following steps:

1. From the vSphere Client, select the host in the inventory.
2. Click the Configuration tab.
3. In the Hardware pane, click Networking.
4. On the right side of vSwitch0, click Properties.
5. Select the vSwitch configuration and click Edit.
6. From the General tab, change the MTU to 9000.
7. Click OK
8. Click Network Adapters tab, click Add
9. Select vmnic5 and click Next
10. Click Next and then click Finish
11. Click the Ports tab
12. Select the Management Network configuration and click Edit.
13. Change the network label to <VMkernel-MGMT> and select the Management Traffic checkbox.
14. Click OK to finalize the edits for Management Network.
15. Select the VM Network configuration and click Edit.
16. Change the network label to <MGMT Network> and enter <>var_ib-mgmt_vlan_id>> in the VLAN ID (Optional) field.
17. Click OK to finalize the edits for VM Network.
18. Click Close
19. On the right side of iScsiBootvSwitch, click Properties
20. Select iScsiBootPG and click Edit
21. Change the Network Label to <VMkernel-iSCSI-A>
22. Click Ok
23. Click Close
24. In the vSphere Standard Switch view, click Add Networking.
25. Select VMkernel and click Next.
26. Select Create a vSphere standard switch to create a new vSphere standard switch
27. Select the check boxes for the network adapter vmnic3
28. Click Next
29. Change the network label to <VMkernel-iSCSI-B>
30. Click Next
31. Enter the IP address and the subnet mask for the NFS VLAN interface for VM-Host-Infra-01

**Note**

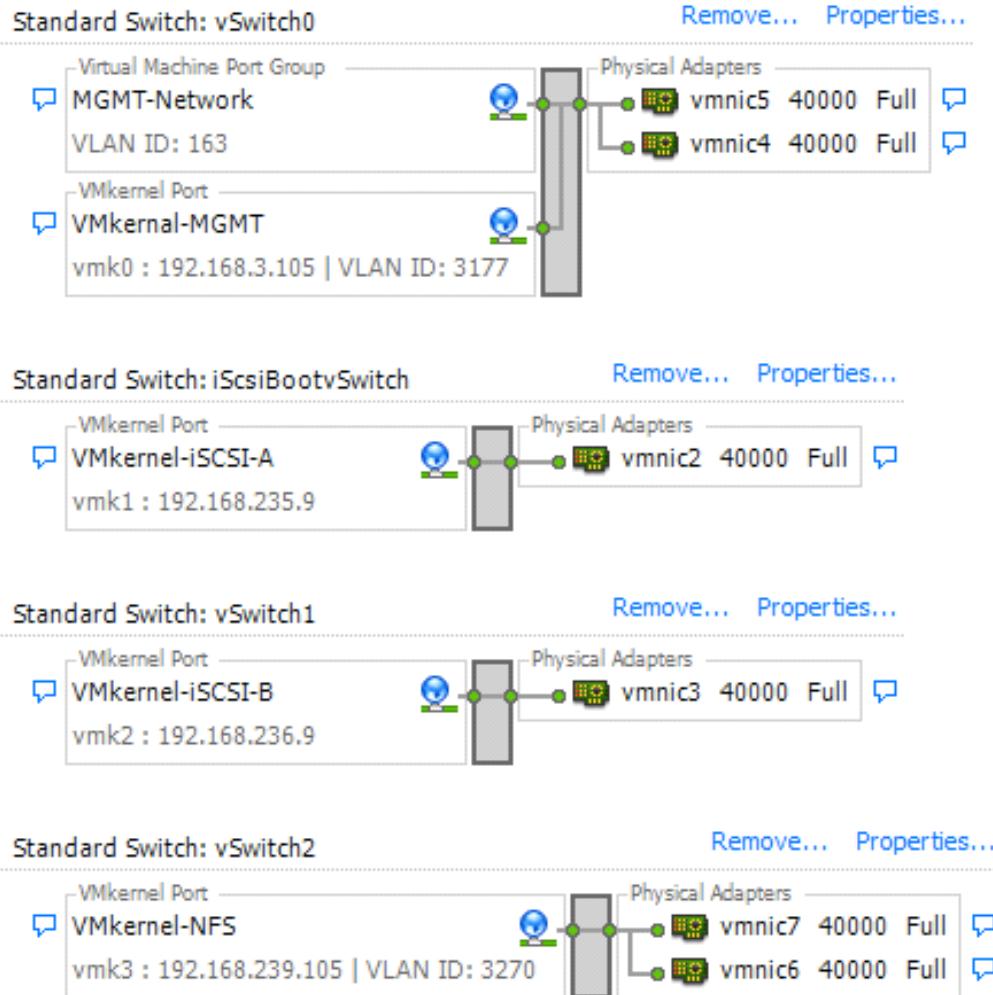
To obtain the iSCSI IP address information; login to the Cisco UCS Manager, In the servers tab select the service profiles template. Click the boot order tab and select the iSCSI-B-vNIC; click set iSCSI boot parameters; the IP address should appear as the initiator address.

32. Click Next.
33. Click Finish.
34. In the vSphere Standard Switch view, click Add Networking.
35. Select VMkernel and click Next.
36. Select Create a vSphere standard switch to create a new vSphere standard switch
37. Select vmnic6 and vmnic7 and click Next
38. Change the network label to <VMkernel-NFS> and enter <var_nfs_vlan_vmk> in the VLAN ID (Optional) field.
39. Click Next
40. Enter the IP address <>var_nfs_vlan_ip_host_01<> and the subnet mask <>var_nfs_vlan_ip_mask_host_01<> for the NFS VLAN interface for VM-Host-Infra-01.
41. To continue with the NFS VMkernel creation, click Next.
42. To finalize the creation of the NFS VMkernel interface, click Finish.
43. Select the <vSwitch> configuration and click Edit.
44. Change the MTU to 9000.
45. Click OK
46. Select the <VMkernel-NFS> configuration and click Edit.
47. Change the MTU to 9000.
48. Click OK to finalize the edits for the VMkernel-NFS network. The properties properties vSwitch2 should be similar to the following example:



49. To finalize the ESXi host networking setup, close the dialog box. The networking for the ESXi host should be similar to the following example:

Networking



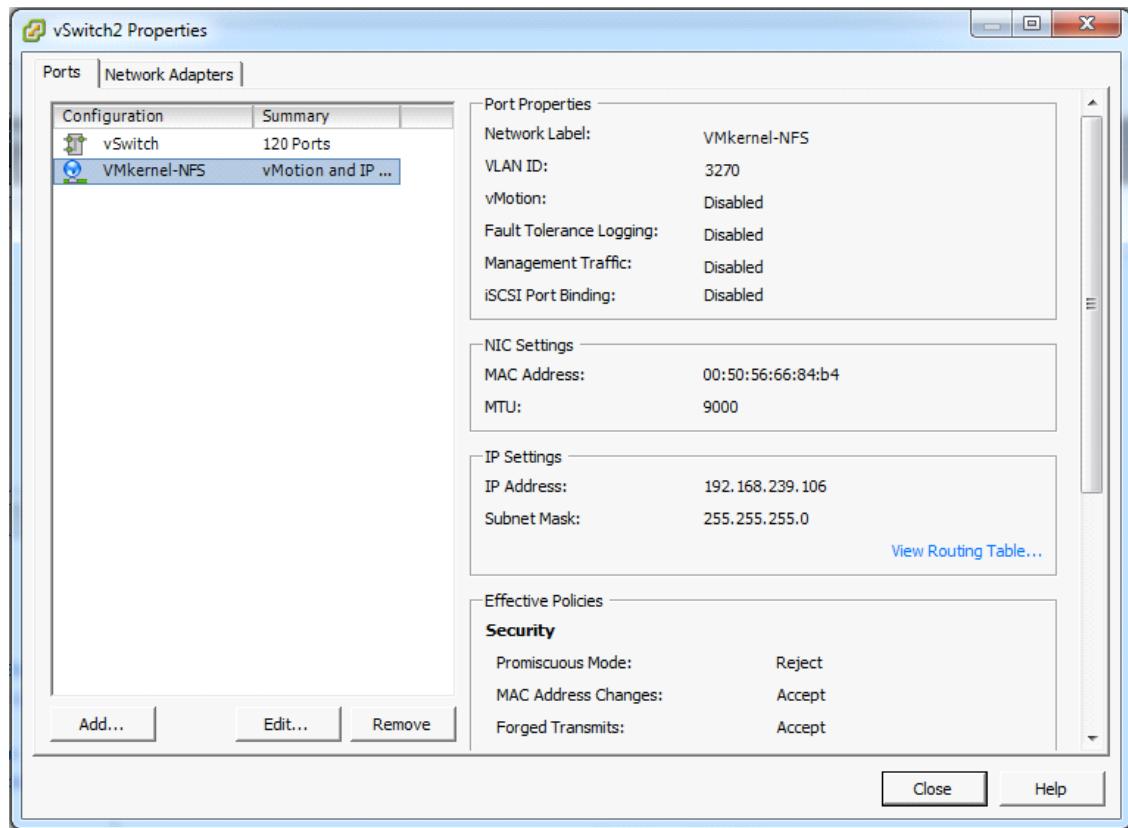
ESXi Host VM-Host-Infra-02

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

- From the vSphere Client, select the host in the inventory.
- Click the Configuration tab.
- In the Hardware pane, click Networking.
- On the right side of vSwitch0, click Properties.
- Select the vSwitch configuration and click Edit.
- From the General tab, change the MTU to 9000.
- Click OK.
- Click Network Adapters tab, click Add.

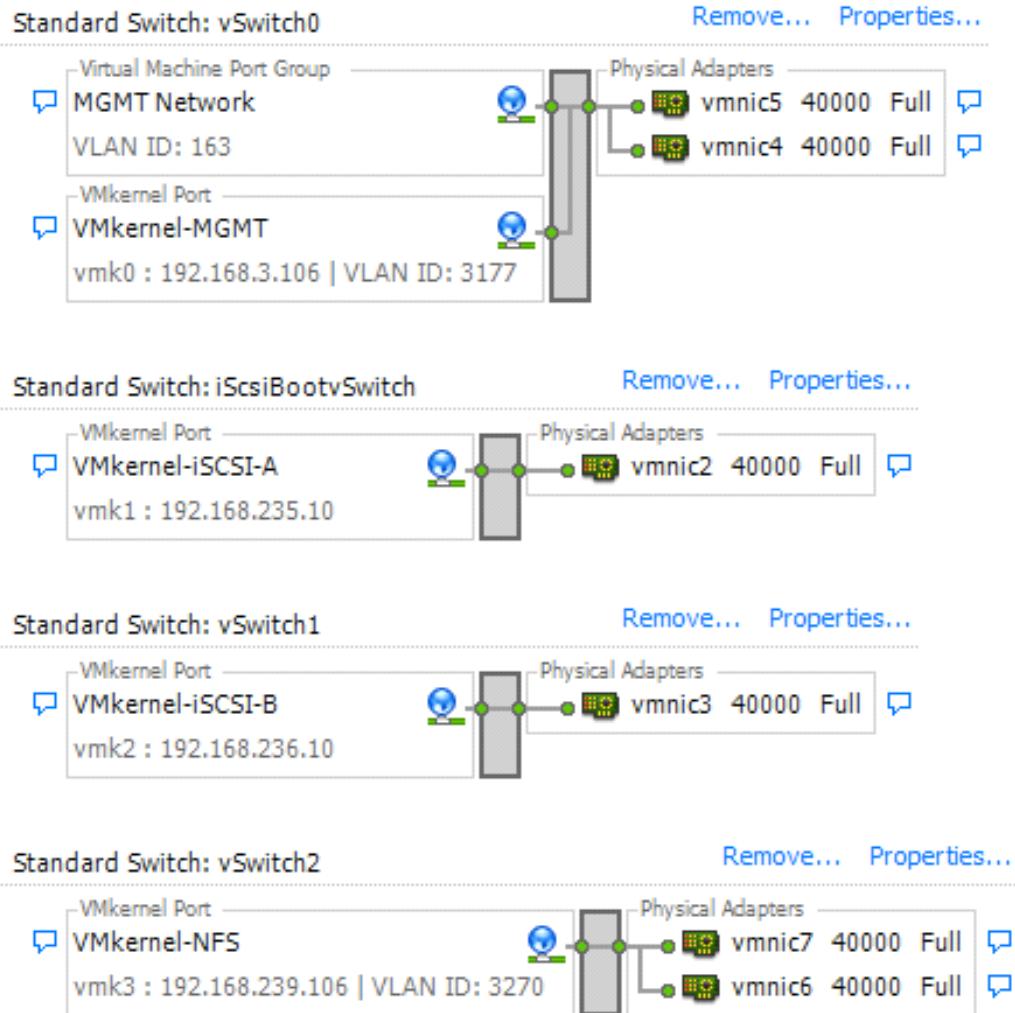
9. Select vmnic5 and click Next.
10. Click Next and then click Finish.
11. Click the Ports tab.
12. Select the Management Network configuration and click Edit.
13. Change the network label to <VMkernel-MGMT> and select the Management Traffic checkbox.
14. Click OK to finalize the edits for Management Network.
15. Select the VM Network configuration and click Edit.
16. Change the network label to <MGMT Network> and enter <<var_ib-mgmt_vlan_id>> in the VLAN ID (Optional) field.
17. Click OK to finalize the edits for VM Network.
18. Click Close.
19. On the right side of iScsiBootvSwitch, click Properties.
20. Select iScsiBootPG and click Edit.
21. Change the Network Label to <VMkernel-iSCSI-A>.
22. Click OK
23. Click Close.
24. In the vSphere Standard Switch view, click Add Networking.
25. Select VMkernel and click Next.
26. Select Create a vSphere standard switch to create a new vSphere standard switch.
27. Select the check boxes for the network adapter vmnic3.
28. Click Next.
29. Change the network label to <VMkernel-iSCSI-B>.
30. Click Next.
31. Enter the IP address and the subnet mask for the NFS VLAN interface for VM-Host-Infra-02 .
32. Click Next.
33. Click Finish.
34. In the vSphere Standard Switch view, click Add Networking.
35. Select VMkernel and click Next.
36. Select Create a vSphere standard switch to create a new vSphere standard switch.
37. Select vmnic6 and vmnic7 and click Next.
38. Change the network label to <VMkernel-NFS> and enter <<var_nfs_vlan_vmk>> in the VLAN ID (Optional) field.
39. Click Next.
40. Enter the IP address <<var_nfs_vlan_ip_host_02>> and the subnet mask <<var_nfs_vlan_ip_mask_host_02>> for the NFS VLAN interface for VM-Host-Infra-02.
41. To continue with the NFS VMkernel creation, click Next.
42. To finalize the creation of the NFS VMkernel interface, click Finish.
43. Select the <<vSwitch>> configuration and click Edit.

44. Change the MTU to 9000.
45. Click OK.
46. Select the <>VMkernel-NFS>> configuration and click Edit.
47. Change the MTU to 9000.
48. Click OK to finalize the edits for the VMkernel-NFS network. The properties vSwitch2 should be similar to the following example:



49. To finalize the ESXi host networking setup, close the dialog box. The networking for the ESXi host should be similar to the following example:

Networking

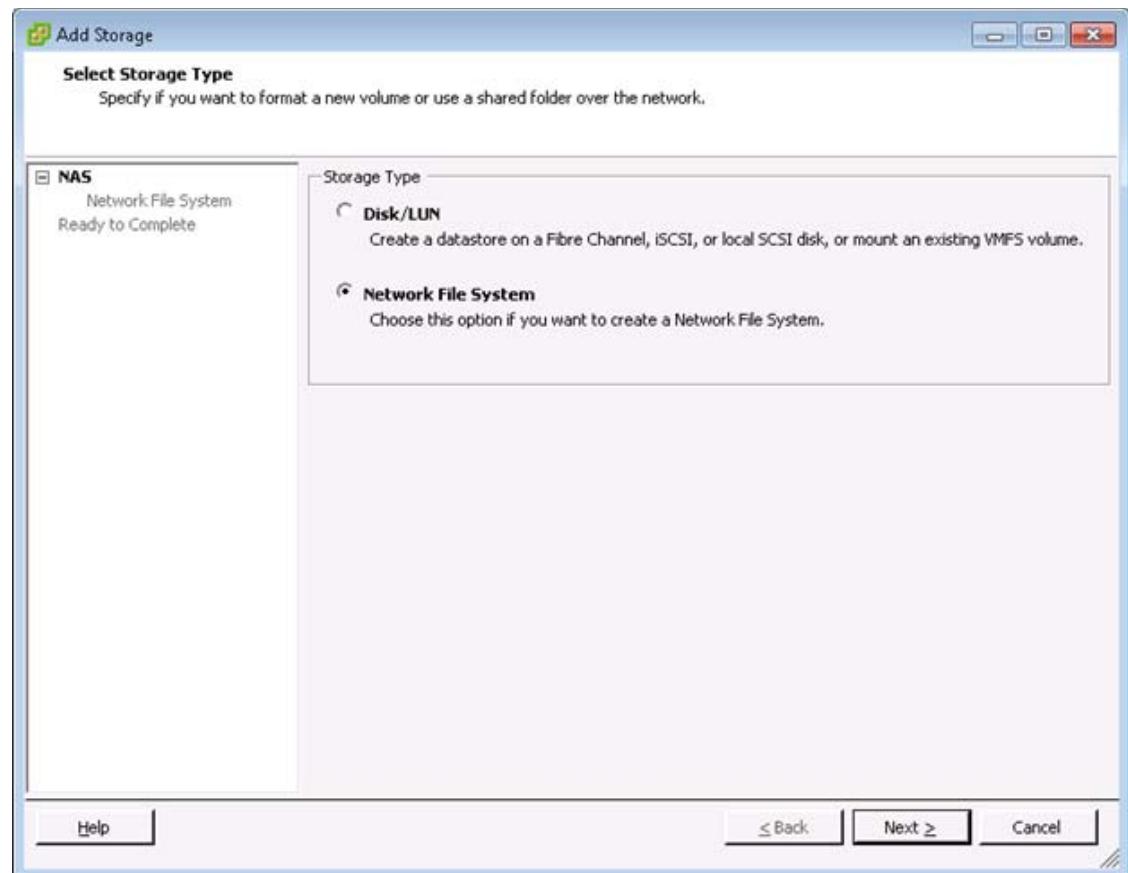


Mount Required Datastores

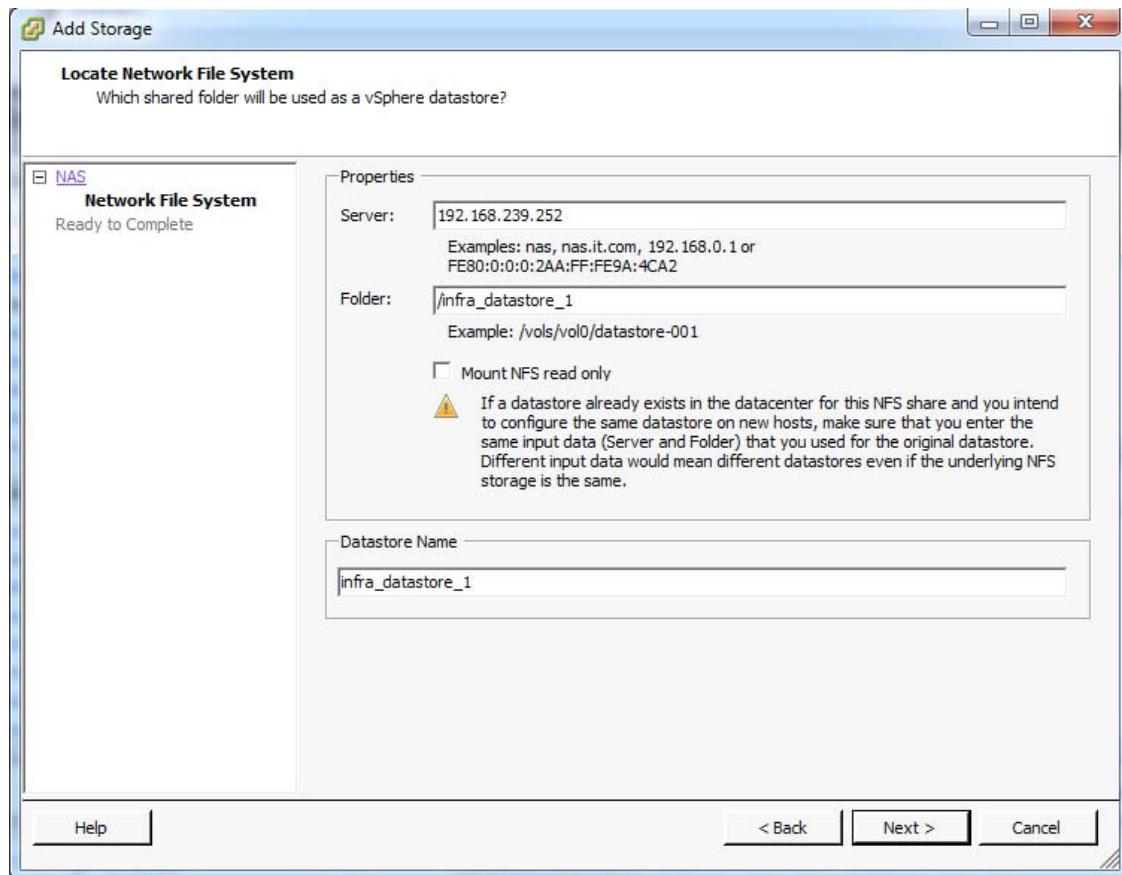
ESXi Hosts VM-Host-Infra-01 and VM-Host-Infra-02

To mount the required datastores, complete the following steps on each ESXi host:

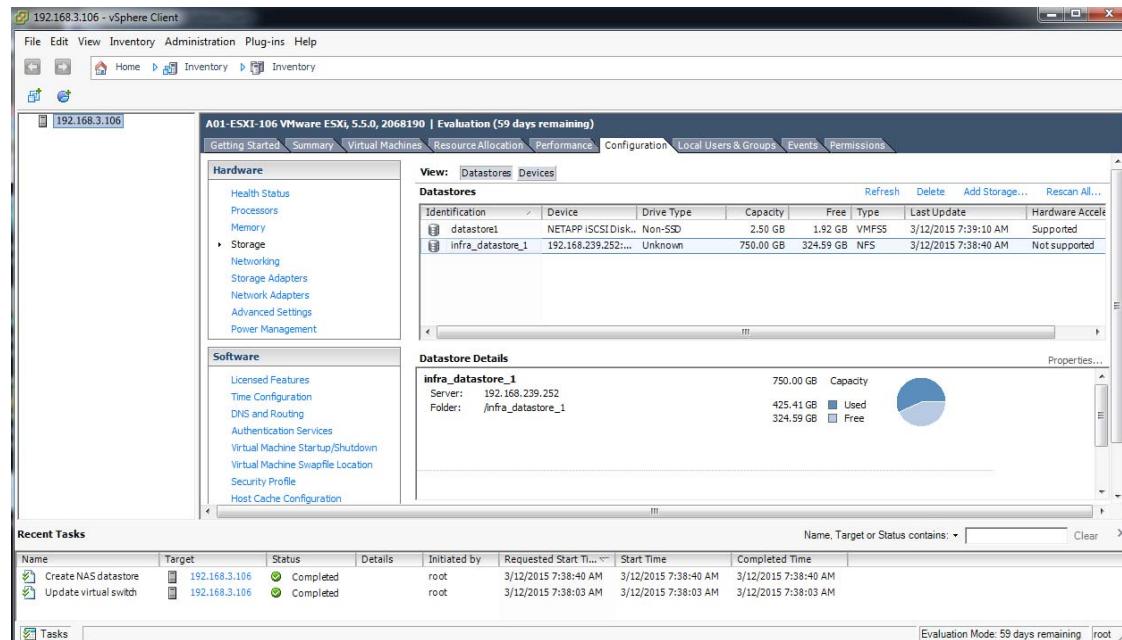
1. From the vSphere Client, select the host in the inventory.
2. To enable configurations, click the Configuration tab.
3. Click Storage in the Hardware pane.
4. From the Datastores area, click Add Storage to open the Add Storage wizard.



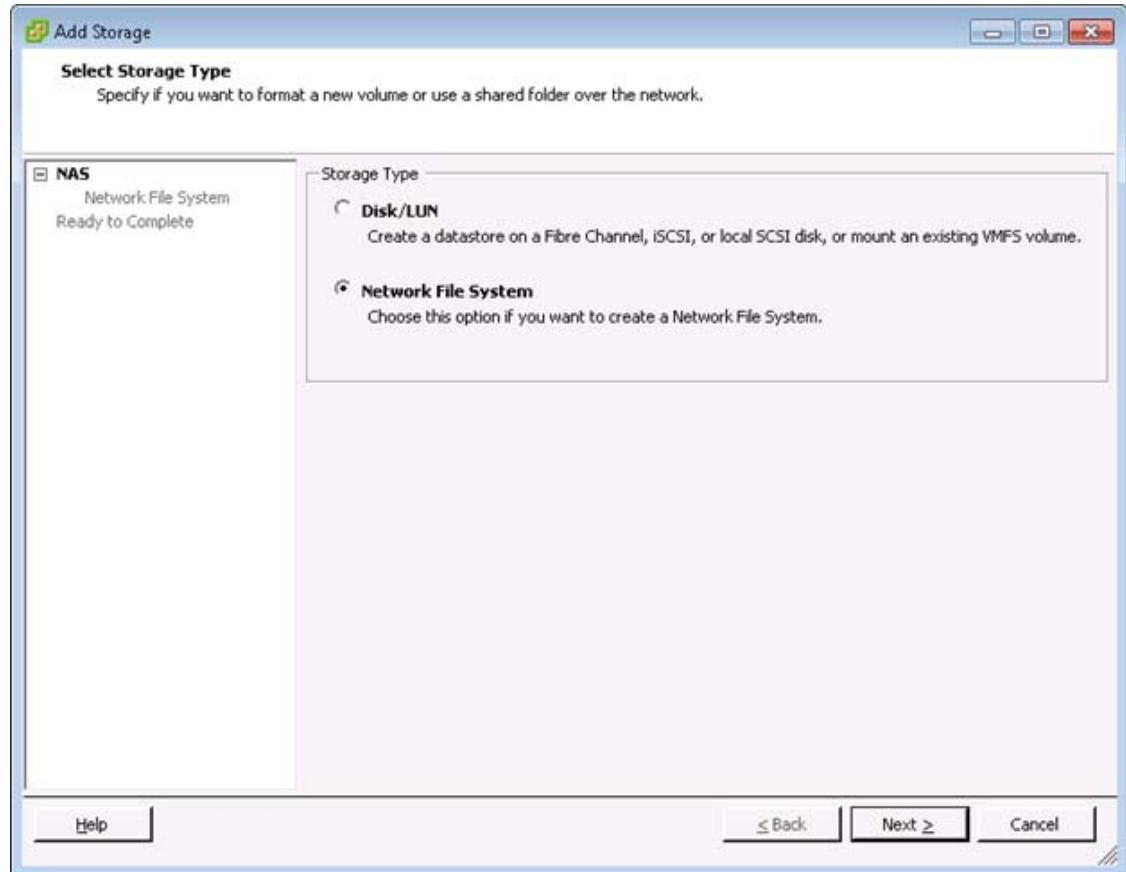
5. Select Network File System and click Next.
6. The wizard prompts for the location of the NFS export. Enter <<var_node02_nfs_lif_infra_datastore_1_ip>> as the IP address for nfs_lif_infra_datastore_1.
7. Enter /infra_datastore_1 as the path for the NFS export.
8. Confirm that the Mount NFS read only checkbox is not selected.
9. Enter infra_datastore_1 as the datastore name.



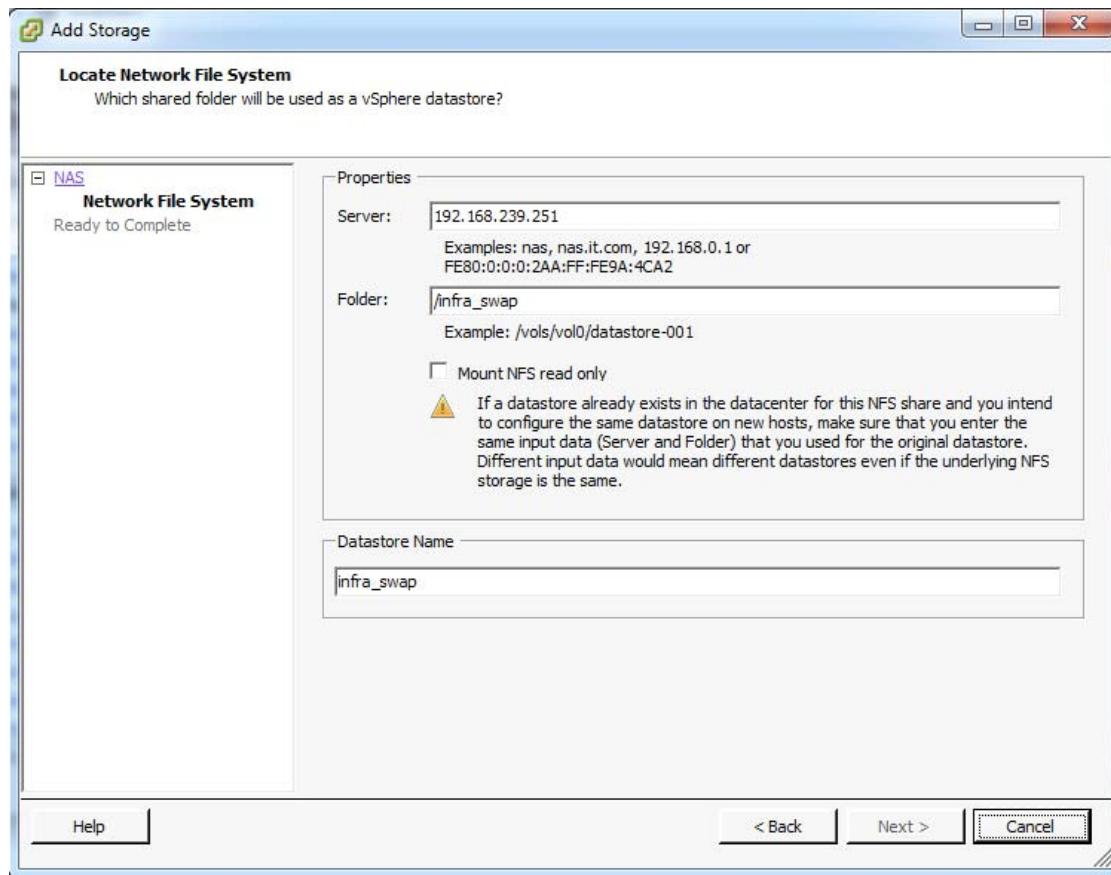
10. To continue with the NFS datastore creation, click Next.
11. To finalize the creation of the NFS datastore, click Finish.



12. From the Datastores area, click Add Storage to open the Add Storage wizard.



13. Select Network File System and click **Next**.
14. The wizard prompts for the location of the NFS export. Enter <<var_node01_nfs_lif_infra_swap_ip>> as the IP address for nfs_lif_infra_swap.
15. Enter /infra_swap as the path for the NFS export.
16. Confirm that the Mount NFS read only checkbox is not selected.
17. Enter infra_swap as the datastore name.



18. To continue with the NFS datastore creation, click Next.
19. To finalize the creation of the NFS datastore, click Finish.

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, complete the following steps on each host:

1. From the vSphere Client, select the host in the inventory.
2. To enable configurations, click the Configuration tab.
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 (ntpd) Options dialog box, complete the following steps:
 - a. Click General in the left pane and select 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, select the Restart NTP service to apply changes checkbox and click OK.
9. In the Time Configuration dialog box, complete the following steps:
 - a. Select the NTP Client Enabled checkbox and click OK.
 - b. Verify that the clock is now set to approximately the correct time.



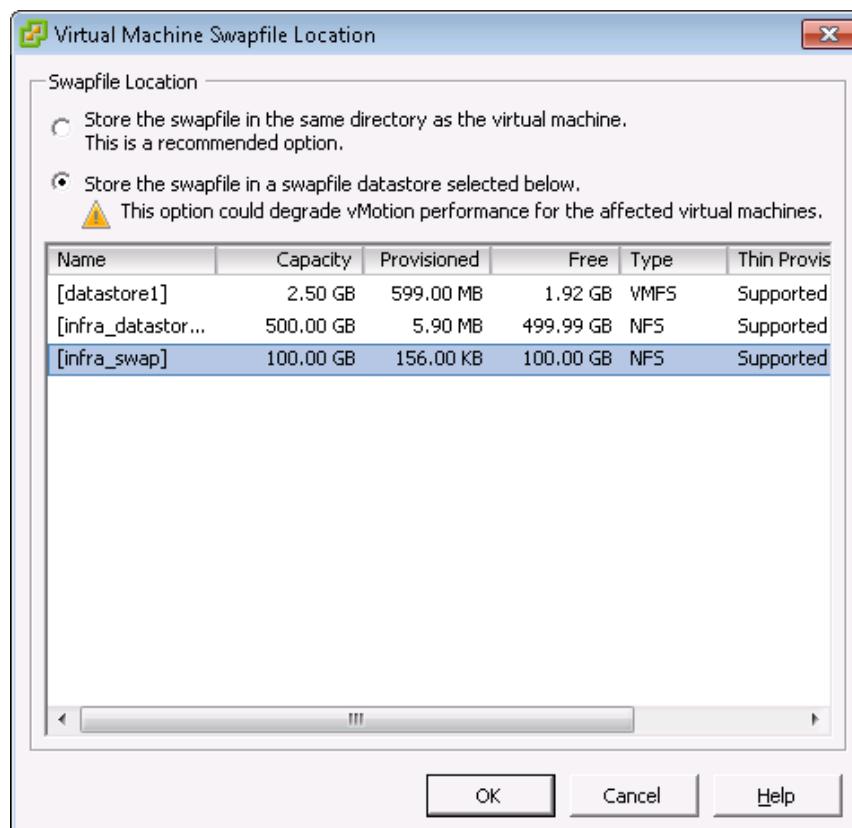
Note The NTP server time may vary slightly from the host time.

Move VM Swap File Location

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

To move the VM swap file location, complete the following steps on each ESXi host:

1. From the vSphere Client, select the host in the inventory.
2. To enable configurations, click the Configuration tab.
3. Click Virtual Machine Swapfile Location in the Software pane.
4. Click Edit at the upper-right side of the window.
5. Select Store the swapfile in a swapfile datastore selected below.
6. Select the <datastore_name> datastore in which to house the swap files.



7. Click OK to finalize moving the swap file location.

VMware vCenter 5.5 Update 2

The procedures in the following subsections provide detailed instructions for installing VMware vCenter 5.5 Update 2 in an environment. After the procedures are completed, a VMware vCenter Server will be configured.

Build Microsoft SQL Server Virtual Machine

To build a SQL Server Virtual Machine (VM) for the VM-Host-Infra-01, complete the following 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 <>datastore_name<>. Click Next.
7. Choose Virtual Machine Version: 8. Click Next.
8. Verify that the Windows option and the Microsoft Windows Server 2012 (64 Bit) version are selected. Click Next.
9. Choose two virtual sockets and one core per virtual socket. Click Next.
10. Choose 8GB of memory. Click Next.
11. Choose one network interface card (NIC)
12. For NIC 1, choose the <>var_oob_mgmt_vlan<> 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 80GB. Click Next.
16. Click Next.
17. Check the edit the virtual machine setting 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 file by click 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 2012 R2 ISO, and then choose Connect to ISO Image on Local Disk.
26. Navigate to Windows Server 2012 R2 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 Windows 2012 R2 Standard (Server with a GUI) option is selected. Click Next.
31. Read and accept the license terms and click Next.
32. Choose Custom (Advanced). Make sure that Disk0 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 Finish.
35. After logging into the VM desktop, from the VM console window, choose the VM menu. Under Guest, choose Install/Upgrade VMware Tools. Click OK.
36. Click OK “Installing the VMware tools package will greatly enhance graphics and mouse performance in your virtual machine.”
37. If prompted to eject the Windows installation media before running the setup for the VMware tools, Click **OK**, then click **OK**.
38. Navigate on the CD-ROM drive, choose Run setup64.exe.
39. In the VMware Tools installer window, click Next.
40. Make sure that Typical is selected and click Next.
41. Click Install.
42. Click Finish.
43. Click Yes to restart the VM.
44. After the reboot is complete, choose the VM menu. Under Guest, choose Ctrl+Alt+Del and then enter the password to log into the VM.
45. Set the time zone for the VM, IP address, gateway, and host name. Add the VM to the Windows AD domain.
46. If necessary, activate Windows.
47. Log back into the VM and download and install all required Windows updates.

Install Microsoft SQL Server 2012 SP1

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

1. Connect to an AD Domain Controller in the Windows Domain and add an admin user in Active Directory Users and Computer tool. This user should be member of the Domain Administrator Security Group.
2. Log into the vCenter SQL Server VM as the admin user.
3. Navigate to the c: drive and create a new folder called database.
4. Click Manage and then select Add Roles and Features to start the Add roles and Features Wizard.
5. Click Next.

6. On the Select installation screen, select Role-based or feature-based installation.
7. Select target Server and click Next.
8. Click Next on Server Roles.
9. On the Select Features screen, check the box .Net Framework 3.5 Features and click Next.
10. On the Confirm installation selections screen, a warning will be displayed asking Do you need to specify an alternate source path?. If the target computer does not have access to Windows Update, click the Specify an alternate source path link to specify the path to the \sources\sxs folder on the installation media and then click OK. After you have specified the alternate source, or if the target has access to Windows update, click the X next to the warning, and then click Install.
11. Click Close.
12. Open Server Manager click on Tools and then select Windows Firewall with Advanced Security.
13. Choose Inbound Rules and click New Rule.
14. Choose Port and click Next.
15. Choose TCP and enter specific local port 1433. Click Next.
16. Choose Allow the Connection. Click Next, and then click Next again.
17. Name the rule SQL Server and click Finish.
18. Close the Windows Firewall with Advanced Security.
19. In the vCenter SQL Server VMware console, click the ninth button (CD with a wrench) to map the Microsoft SQL Server 2012 SP1 ISO. Choose Connect to ISO Image on Local Disk.
20. Navigate to the SQL Server 2012 SP1, select it, and click open.
21. In the dialog box, click Run Setup.exe.
22. In the SQL Server Installation Center window, click Installation on the left.
23. Click on New SQL Server stand-alone installation or add features to an existing installation.
24. On Setup Support Rules screen, click OK.
25. Choose Enter the Product Key. Enter a product key and click Next.
26. Read and accept the license terms and choose whether to check the second check box. Click Next.
27. On the Product Updates screen, Click Next.
28. Click Show details>> Address any warning except for the Windows Firewall Warning. Click Next on Setup Support Rules screen.



Note The Windows Firewall issue was addressed in Step 16.

30. Choose SQL Server Feature Installation and click Next on the Setup Role screen.
31. Under Instance Features, Choose Only Database Engine Services.
32. Under Shared Features, choose Management Tools - Basic and Management Tools - Complete and click Next.
33. On the Installation Rules screen click Show details>> Address any warning and click Next.
34. Keep the Default instance selected. Click Next.
35. Click Next on the Disk Space Requirements screen.

36. For the SQL Server Agent Service and SQL Server Database Engine choose the first cell in the account Name column and then click <<Browse...>>.
37. Enter the local Machine Administrator name (for example, systemname\Administrator), Click Check names, and click OK.
38. In the password field enter your password.
39. Change the startup type for SQL Server Agent to Automatic, and Click Next.
40. Choose Mixed Mode (SQL Server and Windows Authentication). Enter and confirm the password for the SQL Server System Administrator (sa) account, Click Add Current User, and Click Next.
41. Choose whether to send error reports to Microsoft and click Next.
42. On the Installation Configuration Rules screen, Click Show details>> Address any warning. Click Next.
43. Click Install.
44. After the installation is complete, click Close.
45. Close the SQL Server Installation Center.
46. Install all available Microsoft updates by going to Control Panel and select Windows Updates.
47. Open SQL Server Management Studio.
48. 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.
49. Click New Query on the toolbar.
50. 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 = 4000KB, FILEGROWTH = 10%
)
LOG ON
(NAME = N'vcdb_log', FILENAME = N'C:\VCDB.ldf', SIZE = 1000KB, FILEGROWTH = 10%)
COLLATE SQL_Latin1_General_CI_AS
go
ALTER DATABASE [VCDB] SET RECOVERY SIMPLE
use VCDB
go
sp_addlogin @loginname=[vpxuser], @passwd=N'<password>', @defdb='VCDB',
@deflanguage='us_english'
go
ALTER LOGIN [vpxuser] WITH CHECK_POLICY = OFF
go
CREATE USER [vpxuser] for LOGIN [vpxuser]
go
use MSDB
go
CREATE USER [vpxuser] for LOGIN [vpxuser]
go
sp_addrolemember @rolename = 'db_owner', @membername = 'vpxuser'
go
use VCDB
go
sp_addrolemember @rolename = 'db_owner', @membername = 'vpxuser'

```

go



Note This example illustrates the script.

```

Object Explorer
WIN-15O52G351N1 (SQL Server 11.0.3)
+ Databases
+ Security
+ Server Objects
+ Replication
+ AlwaysOn High Availability
+ Management
+ Integration Services Catalogs
+ SQL Server Agent

SQLQuery2.sql - WIN-15O52G351N1.VCDB (sa (56)) * SQLQuery1.sql - WIN-15O52G351N1.VCDB (sa (52))
(NAME = N'vcdb', FILENAME = N'C:\VCDB.mdf', SIZE = 4000KB, FILEGROWTH = 10% )
LOG ON
(NAME = N'vcdb_log', FILENAME = N'C:\VCDB.ldf', SIZE = 1000KB, FILEGROWTH = 10% )
COLLATE SQL_Latin1_General_CI_AS
GO
ALTER DATABASE [VCDB] SET RECOVERY SIMPLE
USE VCDB
GO
sp_addlogin @username='vpuser', @password='password', @defdb='VCDB', @deflanguage='us_english'
GO
ALTER LOGIN [vpuser] WITH CHECK_POLICY = OFF
GO
CREATE USER [vpuser] FOR LOGIN [vpuser]
GO
USE MSDB
GO
CREATE USER [vpuser] FOR LOGIN [vpuser]
GO
sp_addrolemember @rolename = 'db_owner', @membername = 'vpuser'
GO
USE VCDB
GO
sp_addrolemember @rolename = 'db_owner', @membername = 'vpuser'
GO

```

51. Click Execute and verify that the query executes successfully.
52. Close Microsoft SQL Server Management Studio.
53. Disconnect the Microsoft SQL Server 2012 ISO from the SQL Server VM.

Build and Set Up VMware vCenter Virtual Machine

Build VMware vCenter Virutal Machine

To build the VMware vCenter virtual machine, complete the following steps:

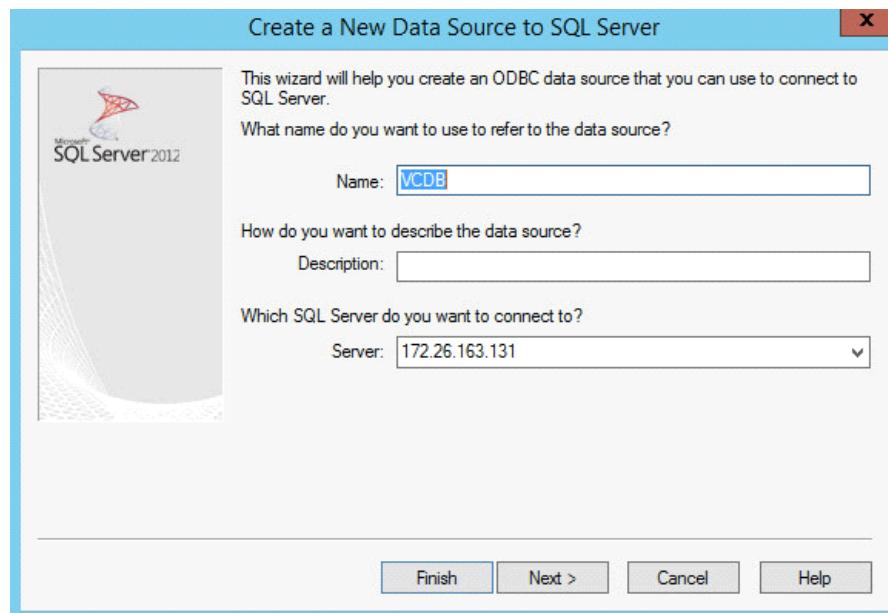
1. Using the instructions for building a SQL Server VM provided in the section "Build Microsoft SQL Server VM," build a VMware vCenter VM with the following configuration in the <>var_oob-mgmt_vlan_id>> VLAN:
 - 12GB RAM
 - Two CPUs
 - One virtual network interface
2. Start the VM, install VMware Tools, and assign an IP address and host name to it in the Active Directory domain.

Set UP VMware vCenter VM

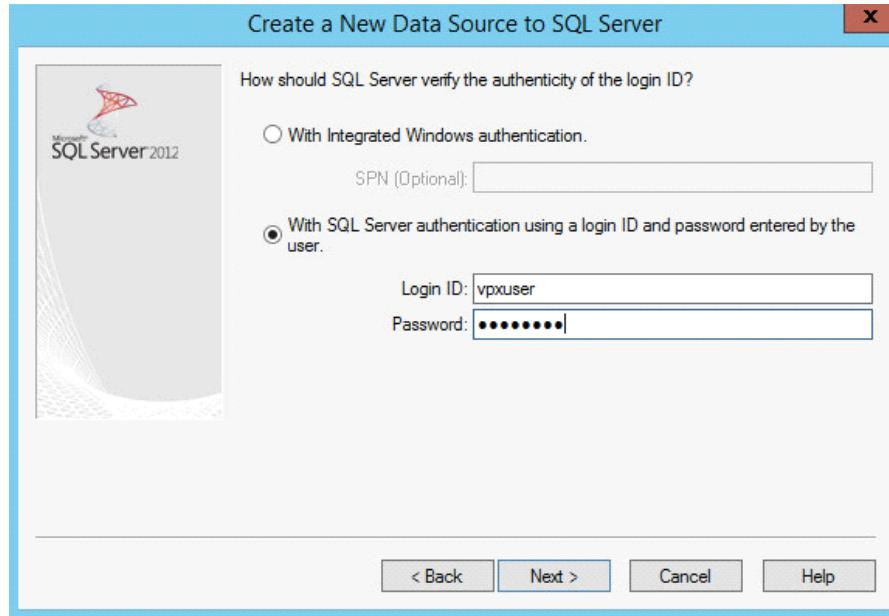
To setup the newly built VMware vCenter VM, complete the following steps:

1. Log into the vCenter VM as the admin user and open Server Manager
2. Click Manage and then select Add Roles and Features to start the Add roles and Features Wizard.
3. Click Next.
4. On the Select installation screen, select Role-based or feature-based installation.
5. Select target Server and Click Next.
6. Click Next on Server Roles.
7. On the Select Features screen, check the box .Net Framework 3.5 Features and click Next.

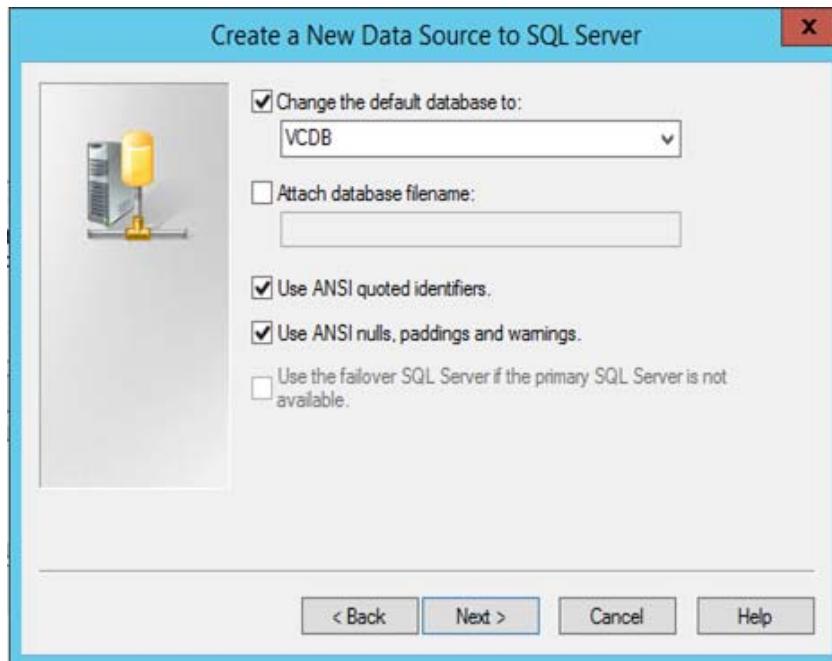
8. On the Confirm installation selections screen, a warning will be displayed asking Do you need to specify an alternate source path?. If the target computer does not have access to Windows Update, click the Specify an alternate source path link to specify the path to the \sources\sxs folder on the installation media and then click OK. After you have specified the alternate source, or if the target has access to Windows update, Click the X next to the warning, and then click Install.
9. Click Close.
10. Click the link [Windows SQL Server 2012 SP1 Feature Pack](#).
11. Click Download.
12. Select the file name ENU\x64\sqlncli.msi and click Next.
13. Save it to a destination folder and run it.
14. On the Microsoft SQL Server 2012 Native Client Setup click Next.
15. Accept the license terms and click Next.
16. Click Next.
17. Click Install.
18. Click Finish.
19. Create the vCenter database data source name (DSN). Open Data Source (ODBC) by selecting Server Manager > Tools > ODBC Data Sources (64-bit).
20. Click the System DSN tab.
21. Click Add.
22. Choose SQL Server Native Client 11.0 and Click Finish.
23. Name the data source VCDB. In the server, enter the IP address of the vCenter SQL server and
24. Click Next.



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

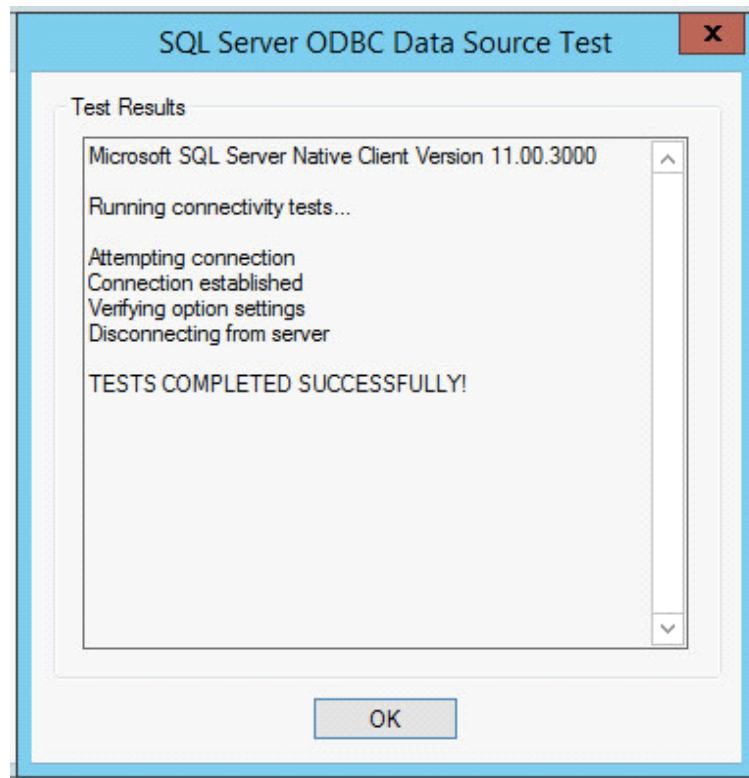


26. Choose Change the Default Database to and choose VCDB from the list. Click Next.



27. Click Finish.

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



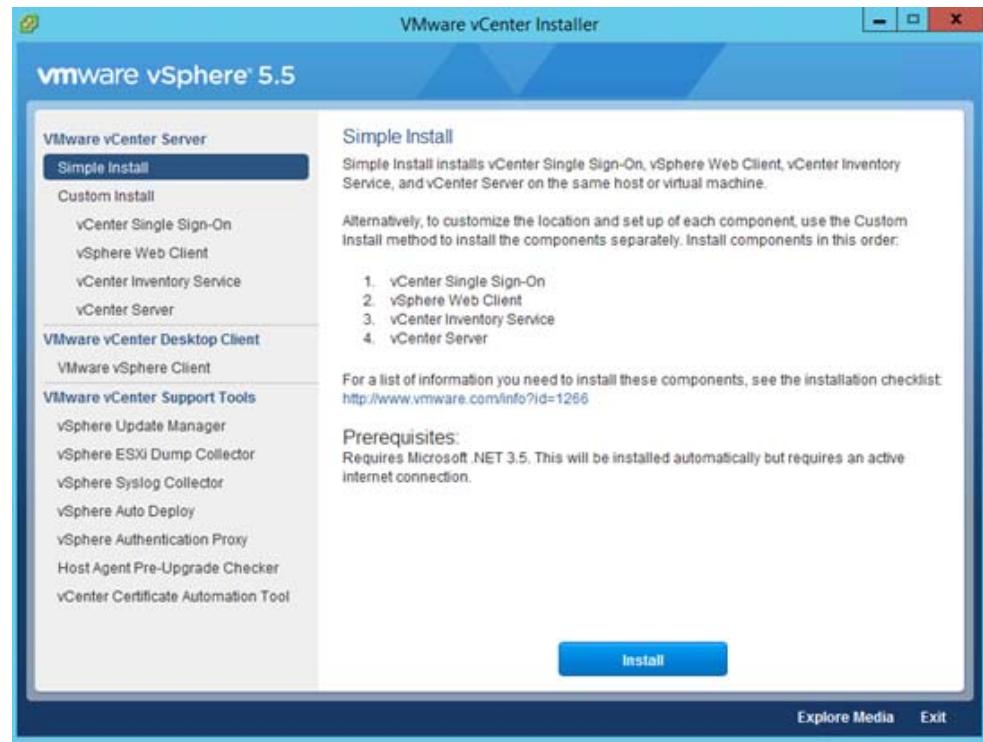
29. Click OK and then Click OK again.
30. Click OK to close the ODBC Data Source Administrator (64-bit) window.
31. Install all available Microsoft Windows updates by Right Click on Start > Control Panel > Windows Update.

Install VMware vCenter Server

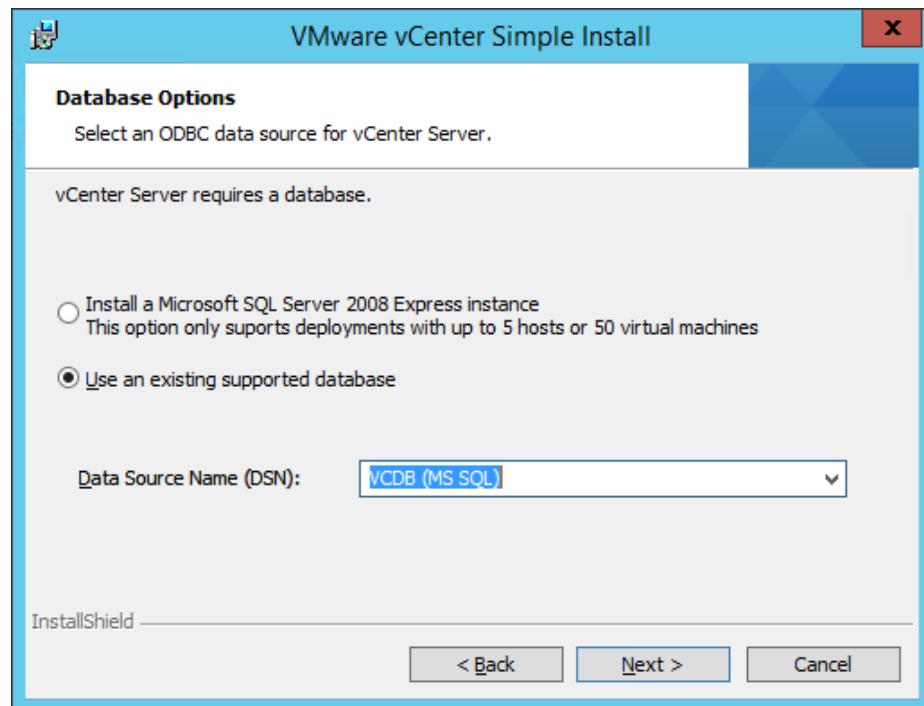
vCenter Server VM

To install vCenter on the vCenter Server VM, complete the following 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 5.5 (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.



5. Click Next on the Welcome to the vCenter Single Sign-On Setup screen.
6. Accept the terms of the license agreement and click Next.
7. Click Next on Simple Install Prerequisites check screen.
8. Enter and confirm <>var_password<> for administrator@vsphere.local . Click Next.
9. Click Next on Simple Install Configure Site window.
10. Click Next on Simple Install Port Setting window.
11. Click Next on Change destination folder.
12. Review the installation option and click Install.
13. Enter the vCenter 5.5 license key and click Next.
14. Choose Use an Existing Supported Database. Choose VCDB from the Data Source Name list and click Next.



15. Enter the vpxuser password and click Next.
16. Click Next vCenter Server Service Window.
17. Click Next on Configure Ports screen.
18. Choose the vCenter Server Configuration that best describe your setup. Click Next.
19. Choose the inventory size that that best describes your setup. Click Next.
20. Click Install.
21. Click Yes to accept and continue with SSL SHA1 SSO lookup Service Leaf certificate.
22. Click Install certificates.
23. Click Finish.
24. Click OK.

ESXI Dump Collector Setup

1. In the VMware vCenter Installer window, under vCenter Support Tools, select vSphere ESXi Dump Collector.
2. Click Install.
3. Select the appropriate language and click OK.
4. In the vSphere ESXi Dump Collector Installation Wizard, click Next.
5. Accept the terms in the License Agreement and click Next.
6. Click Next to accept the default Destination Folders.
7. Click Next to accept a Standalone installation
8. Click Next to accept the default ESXi Dump Collector Server Port (6500).

9. Select the VMware vCenter Server IP address from the drop-down menu. Click Next.
10. Click Install to complete the installation.
11. Click Finish.
12. Click Exit in the VMware vCenter Installer window.
13. Disconnect the VMware vCenter ISO from the vCenter VM.

**Note**

A restart might be required.

14. Back on the Management Workstation, search for Command Prompt and do a right-click on the Command Prompt entry and then click Run as administrator option to open elevated Command Prompt
15. For 64 bit OS go to C:\ProgramFiles(x86)\VMware\Vmware vSphere CLI\bin directory and for 32 bit OS is C:\ProgramFiles\VMware\Vmware vSphere CLI\bin
16. Set each ESXi Host to coredump to ESXi Dump Collector by running the following commands:

```
esxcli -s <>var_vm_host_infra_01_ip>> -u root -p <>var_password>> system
coredump network set --interface-name vmk0 --server-ipv4
<>var_vcenter_server_ip>> --server-port 6500
esxcli -s <>var_vm_host_infra_02_ip>> -u root -p <>var_password>> system
coredump network set --interface-name vmk0 --server-ipv4
<>var_vcenter_server_ip>> --server-port 6500

esxcli -s <>var_vm_host_infra_01_ip>> -u root -p <>var_password>> system
coredump network set --enable true
esxcli -s <>var_vm_host_infra_02_ip>> -u root -p <>var_password>> system
coredump network set --enable true

esxcli -s <>var_vm_host_infra_01_ip>> -u root -p <>var_password>> system
coredump network check
esxcli -s <>var_vm_host_infra_02_ip>> -u root -p <>var_password>> system
coredump network check
```

The screenshot shows an Administrator Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window displays a series of command-line entries using the esxcli command to configure two ESXi hosts (IPs 192.168.3.2 and 192.168.3.3) to send core dumps to a networked dump collector (IP 192.168.3.12) via port 6500. The commands include setting the interface name to vmk0, enabling the coredump feature, and performing a check to verify the configuration. The output shows the commands being run and the successful verification of the netdump server status.

```
C:\>Program Files (x86)\VMware\VMware vSphere CLI\bin>esxcli -s 192.168.3.2 -u ro
ot -p HighU0lt system coredump network set --interface-name vmk0 --server-ipv4
192.168.3.12 --server-port 6500

C:\>Program Files (x86)\VMware\VMware vSphere CLI\bin>esxcli -s 192.168.3.3 -u ro
ot -p HighU0lt system coredump network set --interface-name vmk0 --server-ipv4
192.168.3.12 --server-port 6500

C:\>Program Files (x86)\VMware\VMware vSphere CLI\bin>esxcli -s 192.168.3.2 -u ro
ot -p HighU0lt system coredump network set --enable true

C:\>Program Files (x86)\VMware\VMware vSphere CLI\bin>esxcli -s 192.168.3.3 -u ro
ot -p HighU0lt system coredump network set --enable true

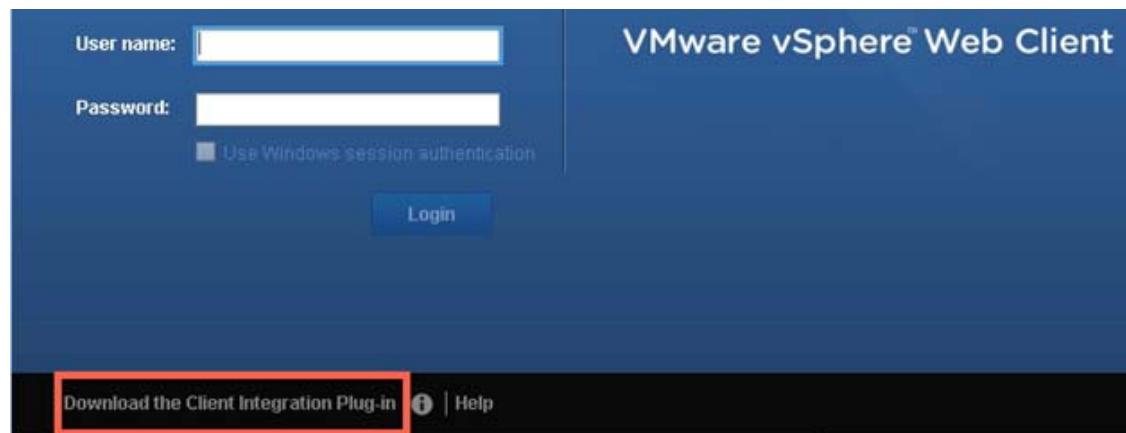
C:\>Program Files (x86)\VMware\VMware vSphere CLI\bin>esxcli -s 192.168.3.2 -u ro
ot -p HighU0lt system coredump network check
Verified the configured netdump server is running

C:\>Program Files (x86)\VMware\VMware vSphere CLI\bin>esxcli -s 192.168.3.3 -u ro
ot -p HighU0lt system coredump network check
Verified the configured netdump server is running

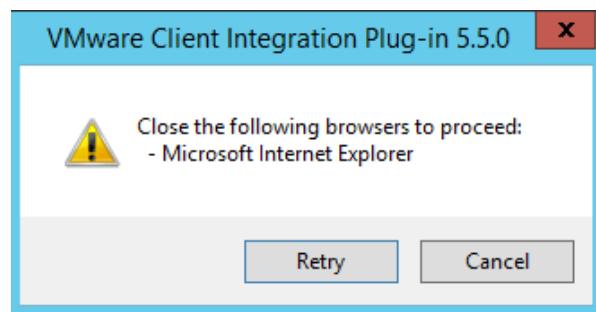
C:\>Program Files (x86)\VMware\VMware vSphere CLI\bin>
```

Login to vSphere Web Client

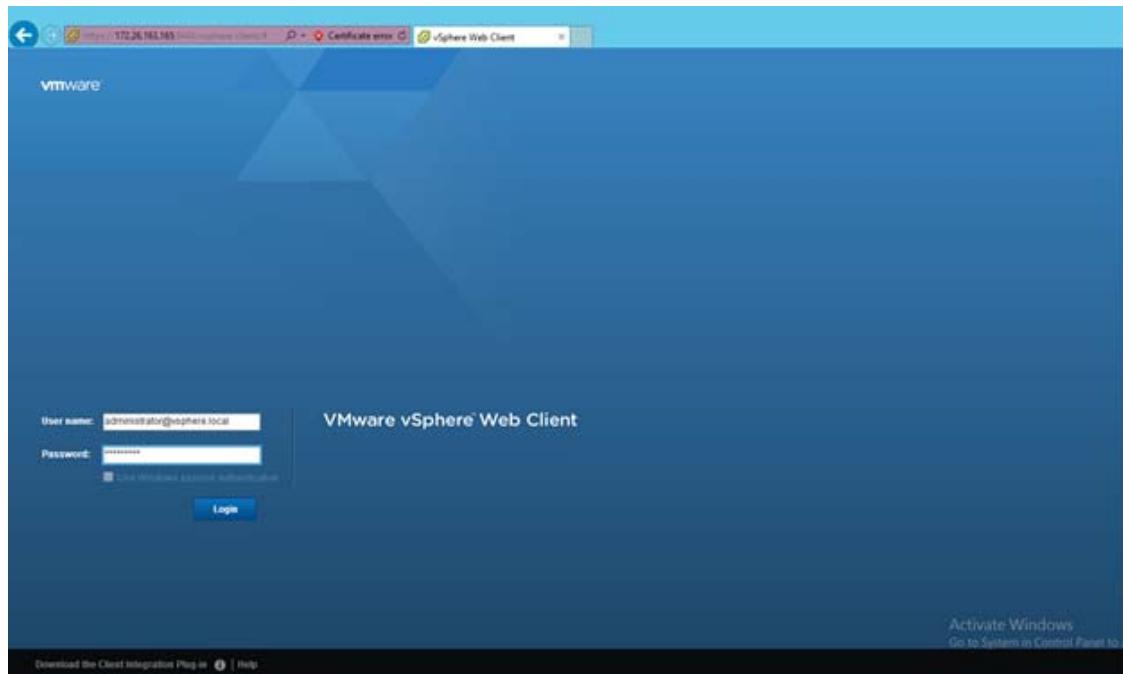
1. Using a web browser, navigate to the VMware vSphere Web Client site.
2. Click Download the Client Integration Plug-in.



3. Click Run.
4. Closed the indicate browser and click Retry.



5. Click Next.
6. Accept the license terms and Click Next.
7. Click Next on Destination Folder window.
8. Click Install.
9. Click Finish.
10. Using a web browser, navigate to https://<>var_vcenter_server_ip>>:9443/vsphere-client/#
11. In the user name type in administrator@vsphere.local and Password your <>password<>.



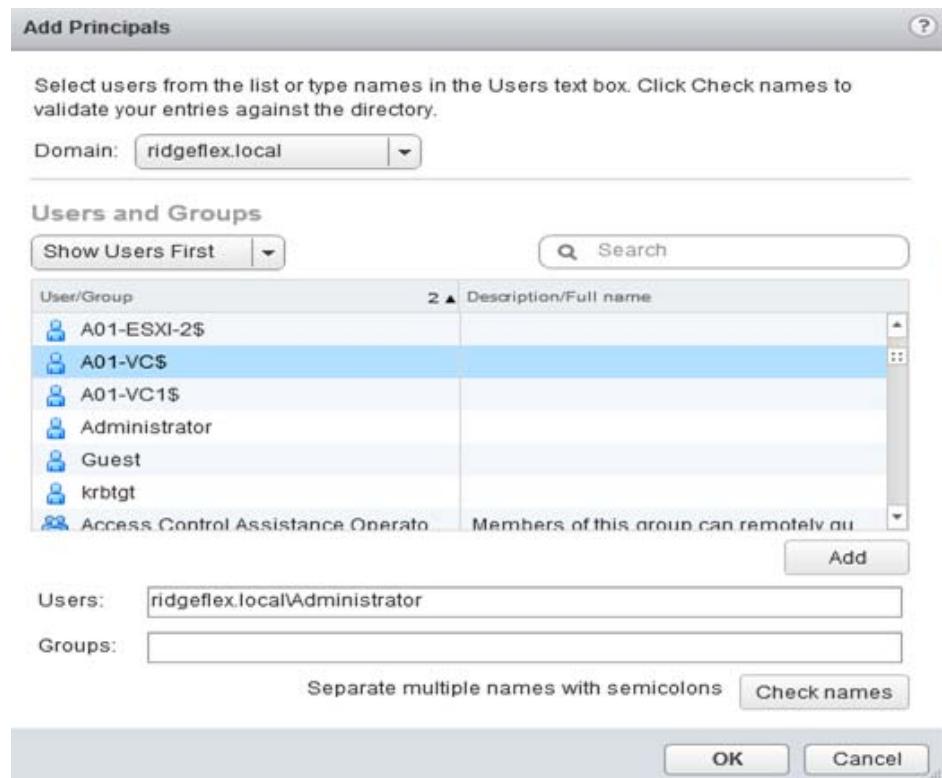
12. Click Login.

Adding the AD Account to Administrator Group and Delegate Permission on the vCenter

1. Log in to the vSphere Web Client as Administrator@vsphere.local.
2. From the home Location, navigate to >>Administration>>Single Sign-ON>>User and Groups>>.
3. Select the Groups.
4. Click on Administrators on Group Name.

Group Name	Domain	Description
Users	vsphere.local	
SolutionUsers	vsphere.local	Well-known solution users' group, which contains all...
DCAdmins	vsphere.local	
ExternalDPUsers	vsphere.local	Well-known external DP users' group, which register...
Administrators	vsphere.local	

5. Click the + on Group Members.
6. Change the Domain to <>domain>>.
7. Highlight the Administrator and click Add.



8. Click OK.
9. Navigate to > Home > vCenterServers and Click on your <>vcenter_server>>.
10. Click the Manage tab.
11. Click the Permissions tab.
12. Click + sign.
13. Click Add.
14. Select your domain.
15. Highlight Administrator and double-click it.
16. Click OK.
17. Change the Assigned Role to Administrator and click OK.
18. Log out from vSphere Web Client.
19. Log in to the vSphere Web Client as Administrator@<>domain>>.

Set Up vCenter Center with a Datacenter, Cluster, DRS and HA

1. In the vSphere Web Client, navigate to the >>vCenter>>vCenter Servers>>vCenter_name.
2. Select Actions > New Datacenter.

3. Rename the datacenter and click OK.
4. Browse to a datacenter in the vSphere Web Client navigator.
5. Right-click the datacenter and select New Cluster.
6. Select DRS and vSphere HA cluster features.
7. Select the DRS Turn ON check box.
8. Select the vSphere HA Turn ON check box.
9. Click OK.

Add Host to vCenter

1. In the vSphere Web Client, navigate to a datacenter, cluster, or folder within a datacenter.
2. Right-click the datacenter, cluster, or folder and select Add Host.
3. Type the IP address or the name of the host and click Next.
4. Type root credentials and click Next.
5. Click Yes to accept the certificate.
6. Review the host summary and click Next.
7. Assign a license key to the host. Click Next.
8. (Optional) Select Enable Lockdown Mode to disable remote access for the administrator account after vCenter Server takes control of this host and click Next.
9. (Optional) If you add the host to a datacenter or a folder, select a location for the virtual machines that reside on the host and click Next.
10. Review the summary and click Finish.

Cisco ACI - Virtual Machine Manager

The following section provides a detailed procedure for configuring the Cisco APIC to communicate and control VMware Distributed Switch (VDS). In this section, VMware vCenter attachment to ACI will be covered.

Defining VMware Distributed Switch Policies

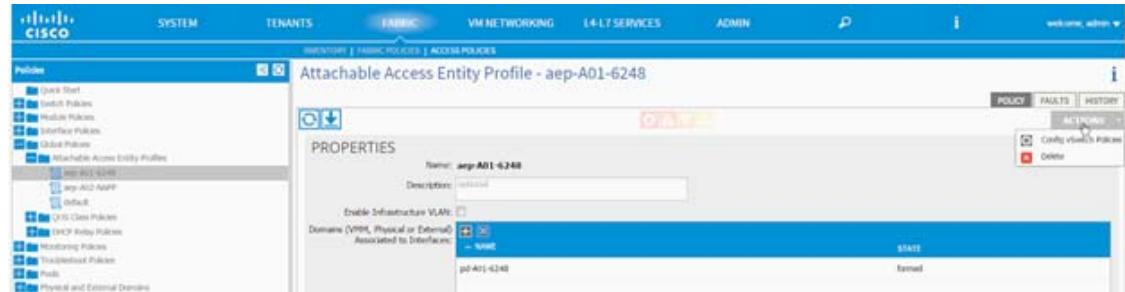
In the Cisco UCS environment, the VDS uplink configuration requires the following three parameters to be set:

- No Port-Channel for uplink ports
- CDP used as the discovery protocol
- LLDP disabled as the discovery protocol

This configuration requires modifying the Access Entity Profiles (AEP) defined for the Cisco UCS Fabric Interconnects; to do so, complete these steps:

1. From the top menu, select FABRIC.
2. Select ACCESS POLICIES from the sub menu.

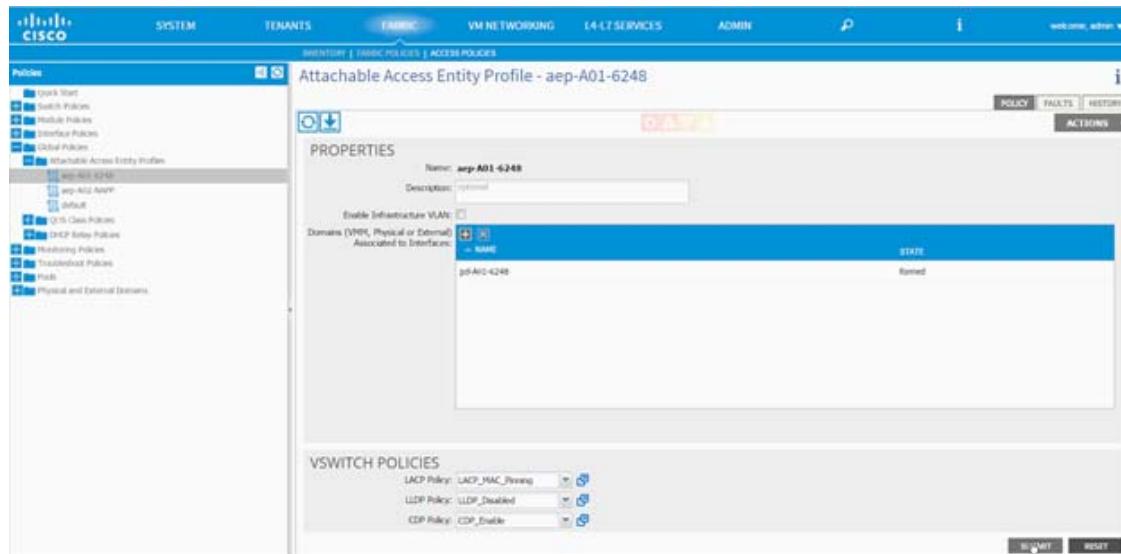
3. From the left menu bar, expand Global Policies and Attachable Access Entity Profiles.
4. Select aep-<UCS_FI> where UCS_FI is the name used for UCS Fabric Interconnect profile in the previous sections.
5. On the right, click Action and select Config vSwitch Policies.



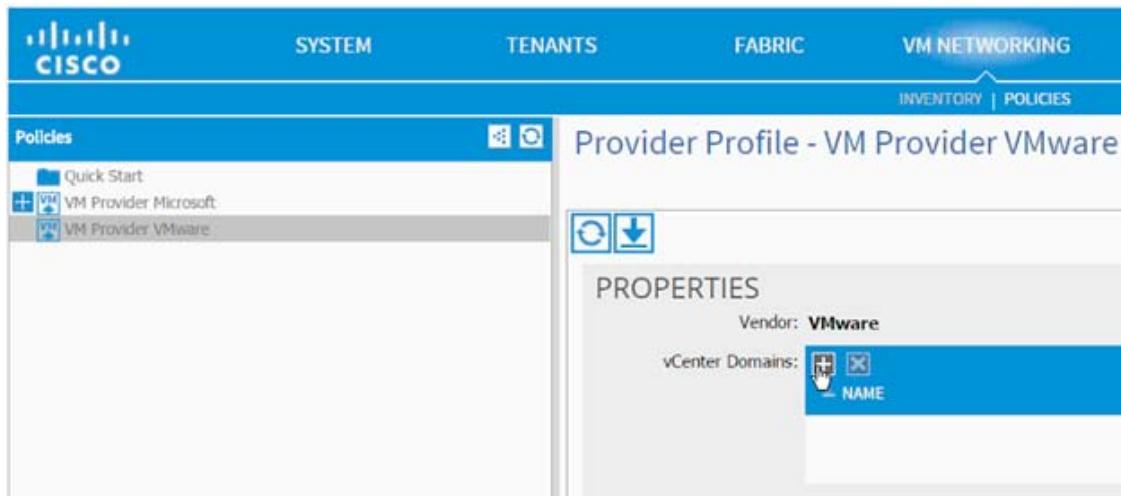
6. In the CONFIG VSWITCH POLICIES dialog box, select CDP_Enable as the CDP Policy.
7. Select LACP_MAC_Pinning as the LACP Policy.
8. Select LLDP_Disabled as the LLDP Policy.



9. Click SUBMIT.
10. Verify the resulting AEP configuration.



11. Click SUBMIT.
12. From the top menu, select VM NETWORKING.
13. Select POLICIES from the sub menu.
14. From the left menu bar, click VM Provider VMware.
15. Under PROPERTIES, click + to add vCenter Domains.



16. In the CREATE VCENTER DOMAIN dialog box, provide a Name" to identify the vCenter.
17. Make sure the VMware vSphere Distributed Switch is selected as the Virtual Switch.
18. From the Associated Attachable Entity drop-down list, select the AEP previously defined for UCS Fabric Interconnect
19. From the VLAN Pool drop-down list, select Create VLAN Pool.

CREATE VCENTER DOMAIN

Specify vCenter domain users and controllers

Name: A01-VC

Virtual Switch: VMWare vSphere Distributed Switch
 Cisco AVS

Associated Attachable Entity Profile: aep-A01-6248

VLAN Pool: select an option

vCenter Credentials: Create VLAN Pool

Profile Name Username

20. In the CREATE VLAN POOL dialog box, provide a name (for example, vp-<NAME_of_vCenter>) of the VLAN pool to be used for dynamically allocating VLANs to the EPGs.
21. Select Dynamic Allocation as the Allocation Mode.
22. Click + next to the Encap Blocks.

CREATE VLAN POOL

Specify the Pool identity

Name: vp-A01-VC

Description: optional

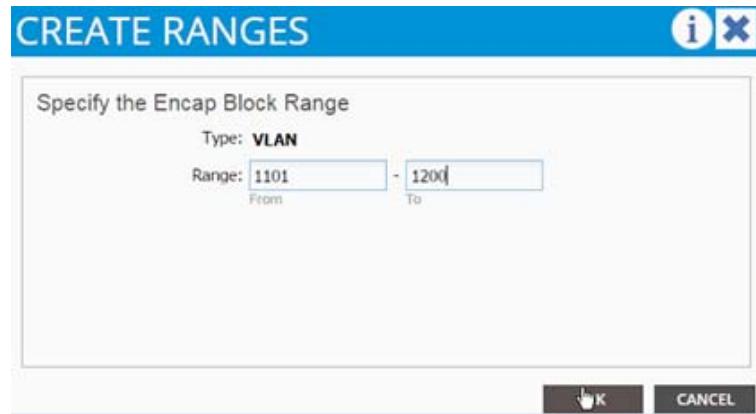
Allocation Mode: Dynamic Allocation
 Static Allocation

Encap Blocks: VLAN Range

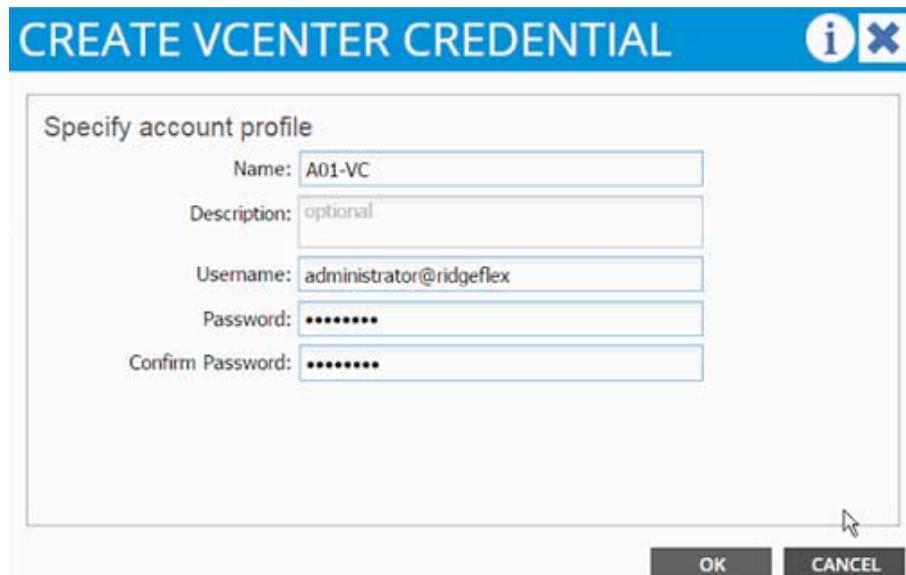
23. In the CREATE RANGES dialogue box add the VLAN range 1101 to 1200.



Note This range can be different depending on customer requirements.

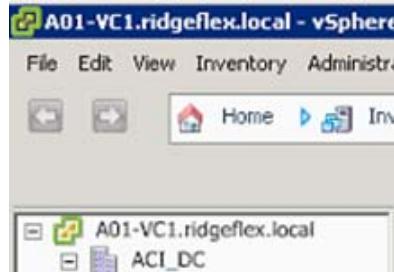


24. Click OK.
25. Click SUBMIT.
26. Click + sign next to vCenter Credentials.
27. In the CREATE VCENTER CREDENTIALS dialog box, add vCenter Name.
28. Add admin username for vCenter in the following format: user@DOMAIN.
29. Add the password for the admin user and confirm the password.



30. Click OK.
31. Click + next to vCenter/vShield.
32. In the CREATE VCENTER/VSHIELD CONTROLLER dialog box, select vCenter as the Type.
33. Add the Name of the vCenter Controller.
34. Add DNS name or IP address in Hostname (or IP Address).
35. Select the DVS Version from the drop-down list.
36. Select Enabled for the Stats Collection.

37. Type the name of the vCenter DataCenter; verify the name in the vCenter.



38. From the Associated Credentials drop-down list, select the vCenter credentials previously defined.

CREATE VCENTER/VSHIELD CONTROLLER

Specify controller profile

Type: vCenter
 vCenter + vShield

VCENTER CONTROLLER

Name:	A01-VCenter
Host Name (or IP Address):	172.26.163.50
DVS Version:	DVS Version 5.5
Stats Collection:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Datacenter:	ACI_DC
Management EPG:	select an option
Associated Credential:	A01-VC

39. Click OK.

40. vCenter domain is now defined.

CREATE VCENTER DOMAIN

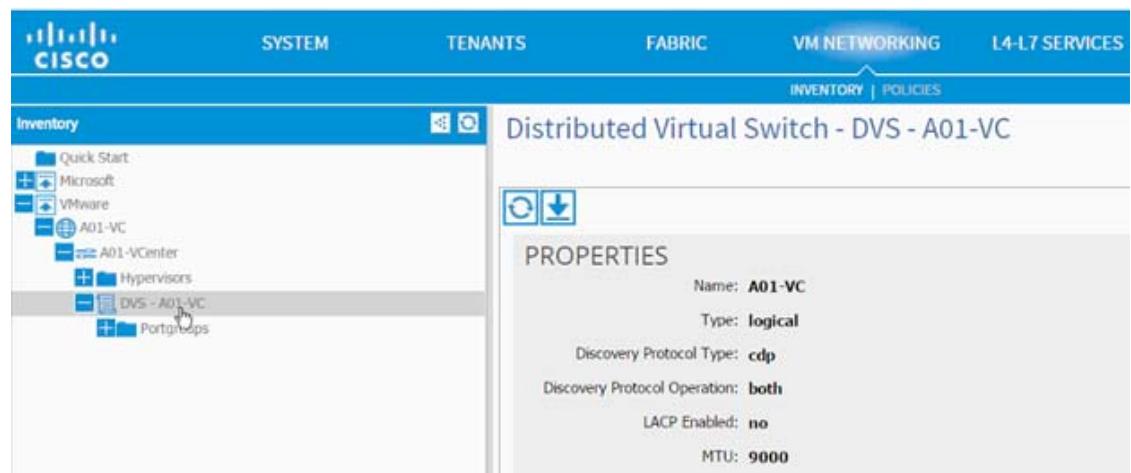
Specify vCenter domain users and controllers										
Name:	A01-VC									
Virtual Switch:	<input checked="" type="radio"/> VMWare vSphere Distributed Switch <input type="radio"/> Cisco AVS									
Associated Attachable Entity Profile:	aep-A01-6248	<input type="button" value=""/>								
VLAN Pool:	vp-A01-VC(dynamic)	<input type="button" value=""/>								
vCenter Credentials:	<table border="1"> <thead> <tr> <th>Profile Name</th> <th>Username</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>A01-VC</td> <td>administrator@ridgeflex</td> <td></td> </tr> </tbody> </table>		Profile Name	Username	Description	A01-VC	administrator@ridgeflex			
Profile Name	Username	Description								
A01-VC	administrator@ridgeflex									
vCenter/vShield:	<table border="1"> <thead> <tr> <th>Name</th> <th>IP</th> <th>Type</th> <th>Stats Collection</th> </tr> </thead> <tbody> <tr> <td>A01-VCenter</td> <td>172.26.163.50</td> <td>vCenter</td> <td>Enabled</td> </tr> </tbody> </table>		Name	IP	Type	Stats Collection	A01-VCenter	172.26.163.50	vCenter	Enabled
Name	IP	Type	Stats Collection							
A01-VCenter	172.26.163.50	vCenter	Enabled							
<input type="button" value="SUBMIT"/> <input type="button" value="CANCEL"/>										

41. Click Submit.

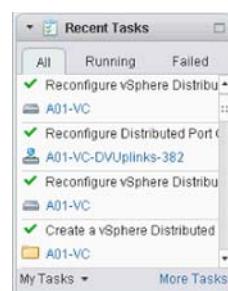
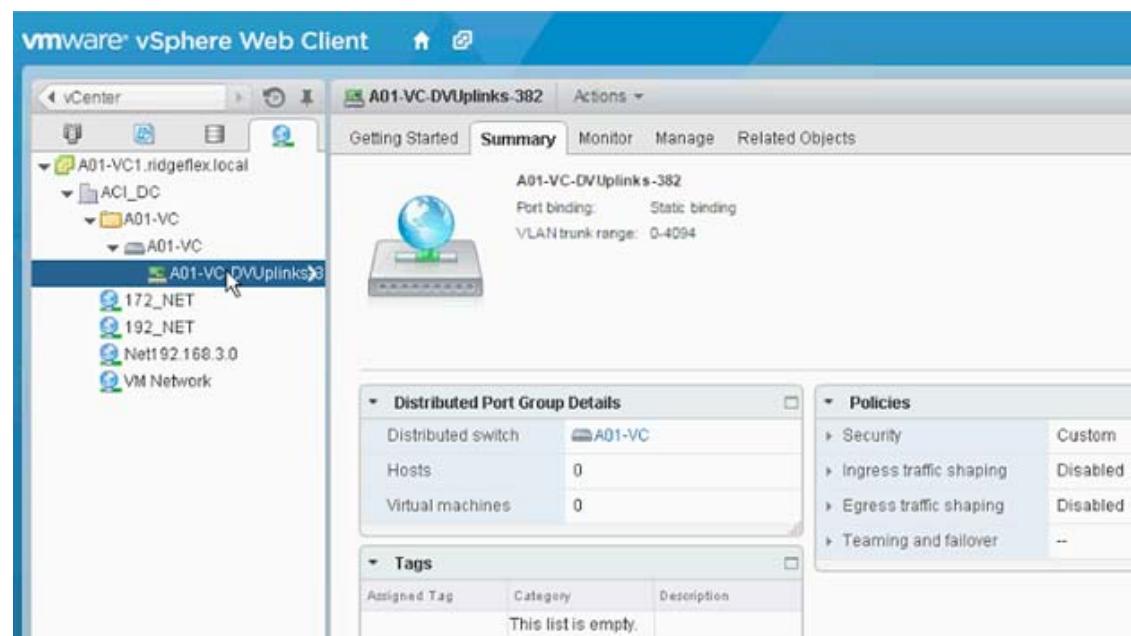
VMware Distributed Switch - Deployment Validation

The Cisco APIC defines a new VDS in the vCenter. This can be verified using both Cisco APIC as well as VMware vCenter.

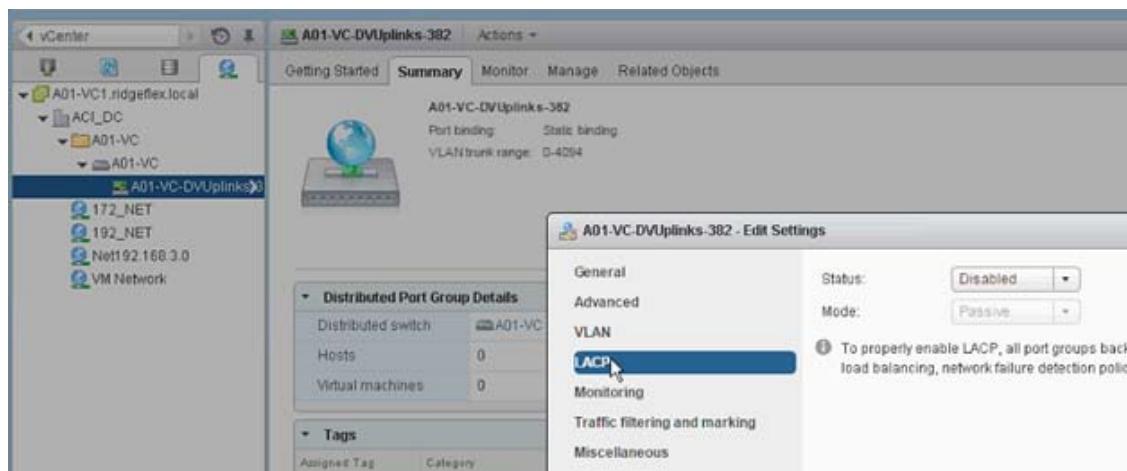
1. Log in to APIC, select VM NETWORKING from the top menu and INVENTORY from the submenu.
2. Expand VMware, vCenter and then DVS.



3. Validate the MTU size, LACP value (should be disabled) and Discovery Protocol (should be CDP).
4. Log in to the vCenter using the vSphere Client.
5. Browse to Networking. A new folder with VDS is available.



6. Right-click the Uplink PortGroup and click Edit Settings.
7. Click LACP.
8. Validate the Status is Disabled.

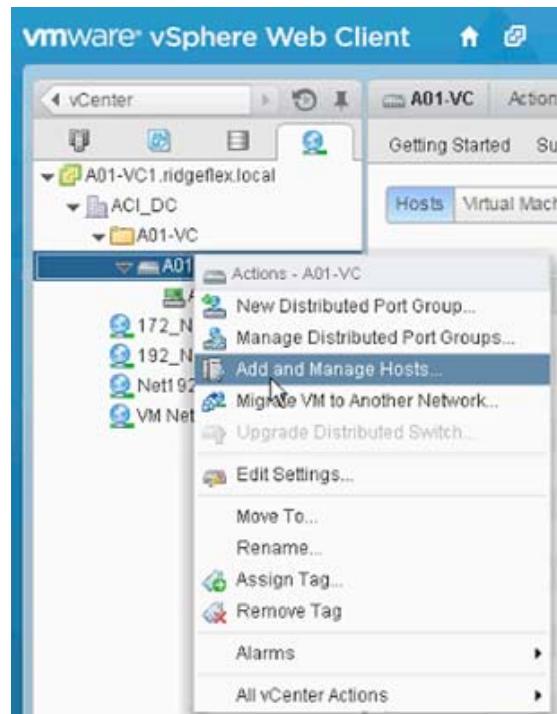


Adding Hosts to VMware Distributed Switch

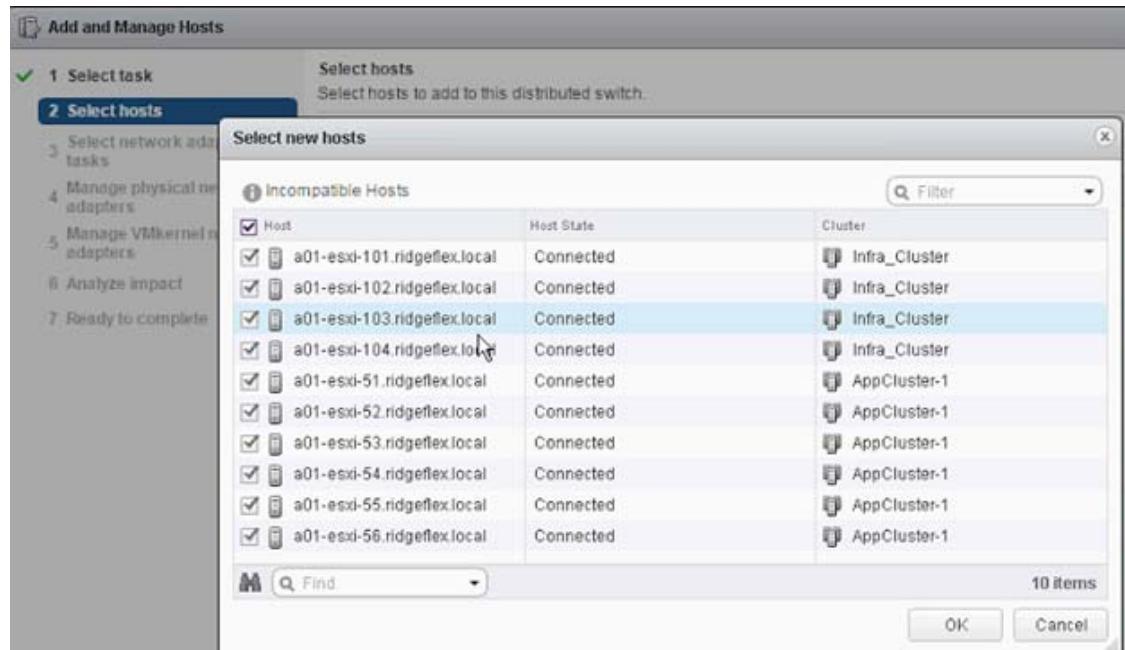
While Cisco APIC defines and configures the VDS automatically based on user configuration, the ESXi hosts need to be added to the VDS and Uplinks need to be defined manually.

To add hosts to the VMware distributed switch, complete the following steps:

1. From the networking tab in vSphere web client, right-click on the VDS and click Add and Manage Hosts.

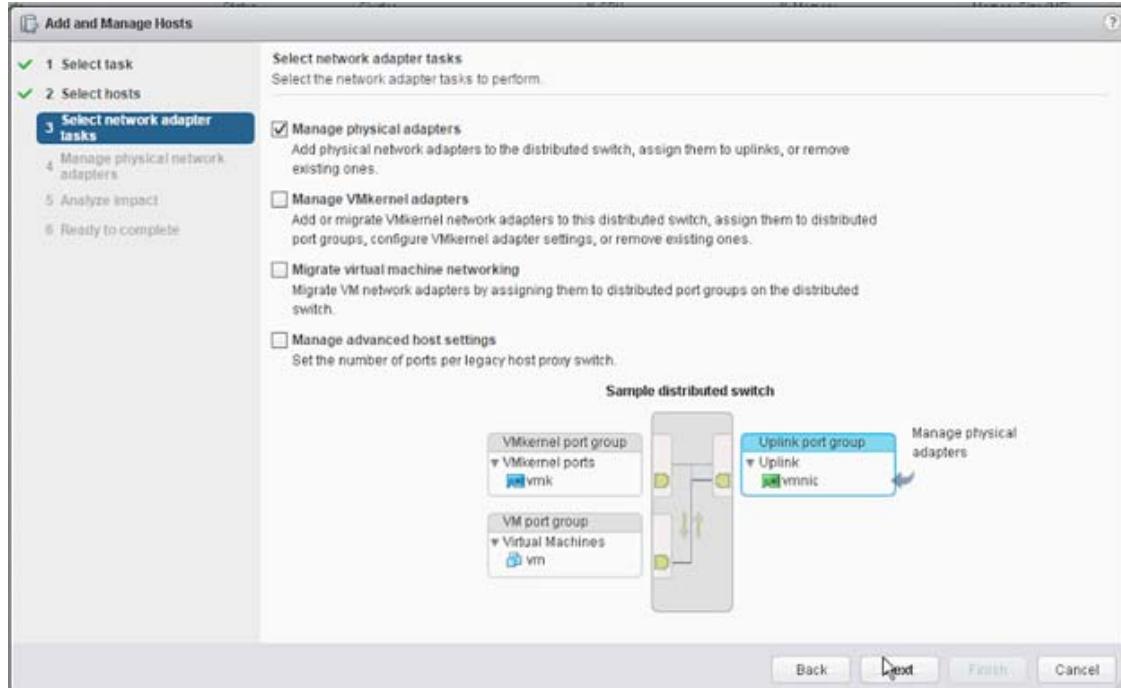


2. In the Add and Manage Hosts wizard, select Add hosts and click Next.
3. Click + to add New hosts.
4. Select all the hosts that need to be part of the VDS.
5. Click OK.

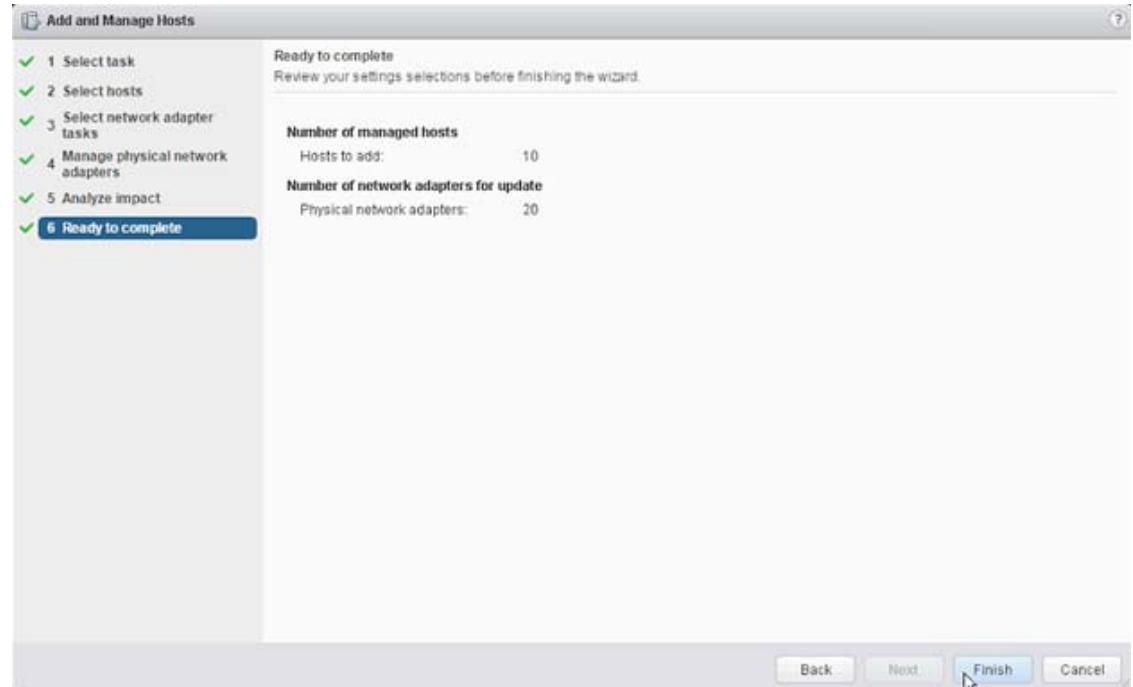


6. Click Next.

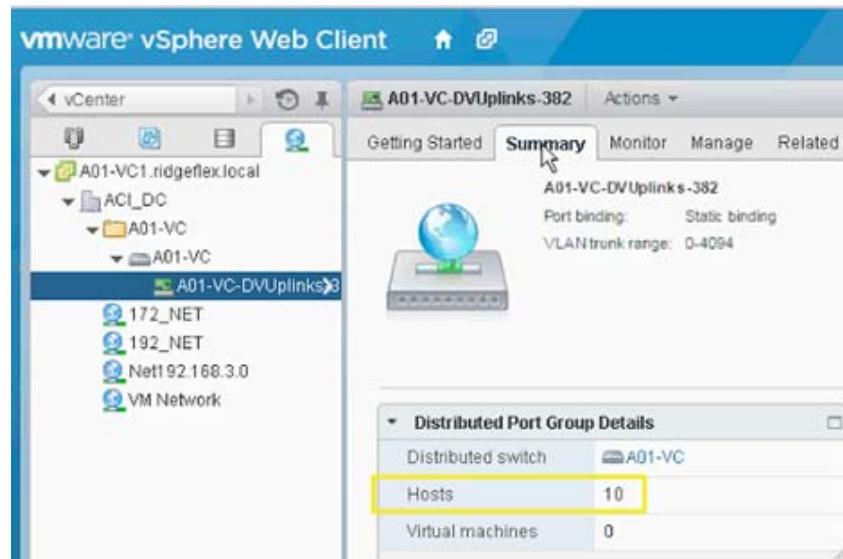
7. In the Select network adapter tasks, make sure only Manage Physical adapter tasks is selected.



8. Click Next.
9. From the Manage physical network adapters screen, select vmnic 0 and vmnic 1 to the uplink ports for all hosts.
10. Click Next.
11. Analyze the number of adapters being added and click Finish.



- When the update is completed, click the Uplink port-group and validate the correct number of hosts were added to VDS.



Application Profile vMotion

In this section, an Application Profile for vMotion traffic will be created. All ESXi hosts will be configured with a VMkernel Port to act as vMotion interface

vMotion - Application Profile Creation

To create a vMotion Application Profile, complete the following steps:

1. Go to the Tenant menu and select Foundation tenant from the top menu.
2. Expand Tenant Foundation in the left menu bar.
3. Right-click Application Profile and click Create Application Profiles.
4. In the CREATE APPLICATION PROFILE dialog box, enter vMotion as the Name.
5. From the drop-down menu, select default for Monitoring Policy.
6. Click “+” next to EPG to add an EPG.
7. Enter “vmk-vmotion” as the EPG Name.
8. Select “bd_Internal” as the Bridge Doamin.
9. Select default as the Monitoring Policy.
10. Click “+” next to Associated Domain Profile (VMs or bare metals).
11. From the drop-down menu, select A01-VC (recently created VMM domain).
12. Set Deployment Immediacy and Resolution Immediacy to Immediate.

CREATE APPLICATION EPG

STEP 1 > IDENTITY

1. IDENTITY

Specify the EPG Identity

Name:	vmk-vmotion						
Description:	optional						
Tags:	(empty)						
QoS class:	Unspecified						
Custom QoS:	select or type to pre-provision						
Bridge Domain:	bd_Internal						
Monitoring Policy:	default						
Associated Domain Profiles (VMs or bare metals):	<table border="1"> <tr> <th>Domain Profile</th> <th>Deployment Immediacy</th> <th>Resolution Immediacy</th> </tr> <tr> <td>A01-VC</td> <td>Immediate</td> <td>Immediate</td> </tr> </table>	Domain Profile	Deployment Immediacy	Resolution Immediacy	A01-VC	Immediate	Immediate
Domain Profile	Deployment Immediacy	Resolution Immediacy					
A01-VC	Immediate	Immediate					
<input type="button" value="UPDATE"/> <input type="button" value="CANCEL"/>							

Statically Link with Leaves/Paths:

< PREVIOUS **OK** **CANCEL**

13. Click Update.
14. Click OK.
15. Click Submit.

16. On vCenter Client, under Home > Inventory > Networking, make sure the port group Foundation|vMotion|vmk-vmotion is added.
17. On all the ESXi servers, add a VMKernel port, attach it to the Foundation|vMotion|vmk-vmotion port-group, set the MTU to 9000 and enable vMotion traffic.

Cisco ACI - Deploying a Tenant

This section details how to configure a tenant (Business Unit or Application) using ACI as follows:

- An SVM will be deployed for tenant (named App-A)
- An Application tenant will be created on APIC (named App-A)
- NFS access will be established
- NFS Datastore will be mounted onto the Application ESXi servers for VM deployment

These procedures will describe the interworking of Cisco APIC and VMware VDS. In the next section, communication between this tenant and an existing infrastructure (outside ACI fabric) will be enabled using OSPF routing.

Application Specific SVM Creation

VLAN in Clustered Data ONTAP

1. Create NFS VLANs.

```
network port vlan create -node <<var_node01>> -vlan-name
a0a-<<var_nfs_vlan_tenant>>
network port vlan create -node <<var_node02>> -vlan-name
a0a-<<var_nfs_vlan_tenant>>
```

2. Create iSCSI VLANs (Optional).

```
network port vlan create -node <<var_node01>> -vlan-name
a0a-<<var_iscsi_vlan_A_tenant>>
network port vlan create -node <<var_node01>> -vlan-name
a0a-<<var_iscsi_vlan_B_tenant>>
network port vlan create -node <<var_node02>> -vlan-name
a0a-<<var_iscsi_vlan_A_tenant>>
network port vlan create -node <<var_node02>> -vlan-name
a0a-<<var_iscsi_vlan_B_tenant>>
```

3. Create SVM Management VLANs.

```
network port vlan create -node <<var_node01>> -vlan-name
a0a-<<var_svm_mgmt_vlan_tenant>>
network port vlan create -node <<var_node02>> -vlan-name
a0a-<<var_svm_mgmt_vlan_tenant>>
```

MTU in Clustered Data ONTAP

1. All of the VLAN interfaces created above should have an MTU of 9000. Check this and set the SVM Management VLAN interface MTU to 1500.

```
network port show -fields mtu

network port modify -node <<var_node01>> -port
a0a-<<var_svm_mgmt_vlan_tenant>> -mtu 1500

WARNING: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y

network port modify -node <<var_node02>> -port
a0a-<<var_svm_mgmt_vlan_tenant>> -mtu 1500

WARNING: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
```



Note It is recommended to configure jumbo frames on this infrastructure.



Note When an interface group is configured with MTU 9000, all VLAN interfaces configured on that interface group will also have an MTU of 9000. All of the existing VLAN interfaces created here were created when the interface group's MTU was set to 9000.

Storage Virtual Machine (Vserver)

To create an infrastructure Vserver, complete the following steps:

1. Run the Vserver setup wizard.

```
vserver setup
```

Welcome to the Vserver Setup Wizard, which will lead you through
the steps to create a virtual storage server that serves data to clients.

You can enter the following commands at any time:
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the Vserver Setup Wizard. Any changes
you made before typing "exit" will be applied.

You can restart the Vserver Setup Wizard by typing "vserver setup". To
accept a default
or omit a question, do not enter a value.

Vserver Setup wizard creates and configures only data Vservers.
If you want to create a Vserver with Infinite Volume use the vserver create
command.

Step 1. Create a Vserver.
You can type "back", "exit", or "help" at any question.

2. Enter the Vserver name.

Enter the Vserver name:App-A

3. Select the Vserver data protocols to configure.

- Choose the Vserver data protocols to be configured {nfs, cifs, fcp, iscsi, ndmp}: nfs,iscsi
4. Select the Vserver client services to configure.
Choose the Vserver client services to configure {ldap, nis, dns}:Enter
 5. Enter the Vserver's root volume aggregate:
Enter the Vserver's root volume aggregate {aggr1_node1, aggr1_node2} [aggr1_node1]: Enter
 6. Enter the Vserver language setting, or "help" to see all languages [C.UTF-8]:
 7. Enter the Vserver's security style:
Enter the Vserver root volume's security style {mixed, ntfs, unix} [unix]: Enter
 8. Answer no to Do you want to create a data volume?
Do you want to create a data volume? {yes, no} [Yes]: no
 9. Answer no to Do you want to create a logical interface?
Do you want to create a logical interface? {yes, no} [Yes]: no
 10. Answer no to Do you want to configure iSCSI?
Do you want to configure iSCSI? {yes, no} [yes]: no
 11. Add the two data aggregates to the App-A Vserver aggregate list for tenant provisioning.
`vserver modify -vserver App-A -aggr-list aggr1_node1, aggr1_node2`
 12. Modify the NFS vstorage parameter on the App-A Vserver to allow the NetApp VAAI plugin to function.
`vserver nfs modify -vserver App-A -vstorage enabled`

Create Load Sharing Mirror of Vserver Root Volume in Clustered Data ONTAP

1. Create a volume to be the load sharing mirror of the infrastructure Vserver root volume on each node.
`volume create -vserver App-A -volume rootvol_m01 -aggregate aggr1_node1 -size 1GB -type DP`
`volume create -vserver App-A -volume rootvol_m02 -aggregate aggr1_node2 -size 1GB -type DP`
2. Create the mirroring relationships.
`snapmirror create -source-path //App-A/rootvol -destination-path //App-A/rootvol_m01 -type LS -schedule 15min`
`snapmirror create -source-path //App-A/rootvol -destination-path //App-A/rootvol_m02 -type LS -schedule 15min`
3. Initialize the mirroring relationship.
`snapmirror initialize-ls-set -source-path //App-A/rootvol`
`snapmirror show`

iSCSI Service in Clustered Data ONTAP

1. Create the iSCSI service on each Vserver. This command also starts the iSCSI service and sets the iSCSI alias to the name of the Vserver.
`iscsi create -vserver App-A`
`iscsi show`

HTTPS Access in Clustered Data ONTAP

Secure access to the storage controller must be configured.

1. Increase the privilege level to access the certificate commands.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. A self-signed certificate is already in place. Check it by using the following command:

```
security certificate show
```

3. For the App-A Vserver, the certificate common name should match the DNS FQDN of the Vserver. The four default certificates should be deleted and replaced by either self-signed certificates or certificates from a Certificate Authority (CA) To delete the default certificates, run the following commands:



Note Deleting expired certificates before creating new certificates is best practice. Run the `security certificate delete` command to delete expired certificates. In the command below, use TAB completion to select and delete each default certificate.

```
security certificate delete [TAB] ...
```

Example: `security certificate delete -vserver App-A -common-name 3.cert.1414163766 -ca 3.cert.1414163766 -type server -serial 544A6D36`

4. To generate and install a self-signed certificate, run the following command as a one-time command. Generate a server certificate for the App-A Vserver. Again, use TAB completion to aid in completing these commands.

```
security certificate create [TAB] ...
```

Example: `security certificate create -common-name app-a.ridgeflex.local -type server -size 2048 -country US -state "North Carolina" -locality "RTP" -organization "Cisco" -unit "SAVBU" -email-addr "abc@cisco.com" -expire-days 365 -hash-function SHA256 -vserver App-A`

5. To obtain the values for the parameters that would be required in the following step, run the `security certificate show` command.

6. Enable each certificate that was just created using the `-server-enabled true` and `-client-enabled false` parameters. Again use TAB completion.

```
security ssl modify [TAB] ...
```

Example: `security ssl modify -vserver App-A -server-enabled true -client-enabled false -ca app-a.ridgeflex.local -serial 544A71D7 -common-name app-a.ridgeflex.local`

7. Change back to normal the admin privilege level and set up to allow Vserver logs to be available by web.

```
set -privilege admin
```

```
vserver services web modify -name spi|ontapi|compat -vserver * -enabled true
```

NFSv3 in Clustered Data ONTAP

To configure NFS on the Vserver, run all commands.

1. Modify the initial default rule for the SVM NFS subnet in the default export policy.

```
vserver export-policy rule modify -vserver App-A -policyname default
-ruleindex 1 -protocol nfs -clientmatch <>var_nfs_subnet_address>> -rorule
sys -rwrule sys -superuser sys -allow-suid false
vserver export-policy rule show
```

2. Assign the FlexPod export policy to the App-A Vserver root volume.

```
volume modify -vserver App-A -volume rootvol -policy default
```

FlexVol in Clustered Data ONTAP

1. The following information is required to create a FlexVol® volume: the volume's name and size, and the aggregate on which it will exist. Create two NFS VMware datastore volumes and an iSCSI LUN volume. Also, update the Vserver root volume load sharing mirrors to make the NFS mounts accessible.

```
volume create -vserver App-A -volume app_a_datastore_1 -aggregate
aggr1_node2 -size 500GB -state online -policy default -junction-path
/app_a_datastore_1 -space-guarantee none -percent-snapshot-space 0
```

```
volume create -vserver App-A -volume iSCSI_LUN -aggregate aggr1_node1 -size
100GB -state online -policy default -space-guarantee none
-percent-snapshot-space 0
```

```
snapmirror update-ls-set -source-path //App-A/rootvol
```

Deduplication in Clustered Data ONTAP

1. Enable deduplication on appropriate volumes.

```
volume efficiency on -vserver App-A -volume app_a_datastore_1
volume efficiency on -vserver App-A -volume iSCSI_LUN
```

Failover Groups NAS in Clustered Data ONTAP

1. Create an NFS port failover group.

```
network interface failover-groups create -failover-group
fg-nfs-<<var_nfs_vlan_tenant>> -node <<var_node01>> -port
a0a-<<var_nfs_vlan_tenant>>
network interface failover-groups create -failover-group
fg-nfs-<<var_nfs_vlan_tenant>> -node <<var_node02>> -port
a0a-<<var_nfs_vlan_tenant>>
```

NFS LIF in Clustered Data ONTAP

1. Create an NFS logical interface (LIF).

```
network interface create -vserver App-A -lif nfs_lif_tenant_datastore_1
-role data -data-protocol nfs -home-node <<var_node02>> -home-port
a0a-<<var_nfs_vlan_tenant>> -address
<<var_node02_nfs_lif_tenant_datastore_1_ip>> -netmask
<<var_node02_nfs_lif_tenant_datastore_1_mask>> -status-admin up
-failover-policy nextavail -firewall-policy data -auto-revert true
-failover-group fg-nfs-<<var_nfs_vlan_tenant>>
```



Note It is recommended to create a new lif for each datastore.

iSCSI LIF in Clustered Data ONTAP (Optional)

1. Create iSCSI logical interfaces (LIFs).

```

network interface create -vserver App-A -lif iscsi_lif01a -role data
-data-protocol iscsi -home-node <<var_node01>> -home-port
a0a-<<var_iscsi_vlan_A_tenant>> -address
<<var_node01_iscsi_tenant_lif01a_ip>> -netmask
<<var_node01_iscsi_tenant_lif01a_mask>> -status-admin up -failover-policy
disabled -firewall-policy data -auto-revert false

network interface create -vserver App-A -lif iscsi_lif01b -role data
-data-protocol iscsi -home-node <<var_node01>> -home-port
a0a-<<var_iscsi_vlan_B_tenant>> -address
<<var_node01_iscsi_tenant_lif01b_ip>> -netmask
<<var_node01_iscsi_tenant_lif01b_mask>> -status-admin up -failover-policy
disabled -firewall-policy data -auto-revert false

network interface create -vserver App-A -lif iscsi_lif02a -role data
-data-protocol iscsi -home-node <<var_node02>> -home-port
a0a-<<var_iscsi_vlan_A_tenant>> -address
<<var_node02_iscsi_tenant_lif02a_ip>> -netmask
<<var_node02_iscsi_tenant_lif02a_mask>> -status-admin up -failover-policy
disabled -firewall-policy data -auto-revert false

network interface create -vserver App-A -lif iscsi_lif02b -role data
-data-protocol iscsi -home-node <<var_node02>> -home-port
a0a-<<var_iscsi_vlan_B_tenant>> -address
<<var_node02_iscsi_tenant_lif02b_ip>> -netmask
<<var_node02_iscsi_tenant_lif02b_mask>> -status-admin up -failover-policy
disabled -firewall-policy data -auto-revert false

network interface show -vserver App-A

```

Add App-A Vserver Administrator

1. Add the App-A Vserver administrator and Vserver administration logical interface in the SVM management network with the following commands:

```

network interface failover-groups create -failover-group
fg-app-a-vsmgmt-<<var_svm_mgmt_vlan_tenant>> -node <<var_node01>> -port
a0a-<<var_svm_mgmt_vlan_tenant>>
network interface failover-groups create -failover-group
fg-app-a-vsmgmt-<<var_svm_mgmt_vlan_tenant>> -node <<var_node02>> -port
a0a-<<var_svm_mgmt_vlan_tenant>>

network interface create -vserver App-A -lif vsmgmt -role data
-data-protocol none -home-node <<var_node02>> -home-port
a0a-<<var_svm_mgmt_vlan_tenant>> -address <<var_vserver_tenant_mgmt_ip>>
-netmask <<var_vserver_tenant_mgmt_mask>> -status-admin up -failover-policy
nextavail -firewall-policy mgmt -auto-revert true -failover-group
fg-app-a-vsmgmt-<<var_svm_mgmt_vlan_tenant>>

```

Note: you will see that a routing group is created with the above command. Use that routing group in the command below where you see <<var_routing_group>>.

```

network routing-groups route create -vserver App-A -routing-group
<<var_routing_group>> -destination 0.0.0.0/0 -gateway
<<var_vserver_tenant_mgmt_gateway>>

security login password -username vsadmin -vserver App-A
Enter a new password: <<var_vsadmin_password>>
Enter it again: <<var_vsadmin_password>>

security login unlock -username vsadmin -vserver Infra_Vserver

```

Application Tenant Creation on APIC

To create an Application Tenant on APIC, complete the following steps:

1. From the main menu, click TENANT and from the sub-menu click ADD TENANT.
2. In the CREATE TENANT dialog box, type <Name of Application> as the name of the tenant. This example used App-A as the name of the tenant.
3. Click the checkbox next to "all" under Security Domains.

The screenshot shows the 'CREATE TENANT' interface on the APIC. It's on 'STEP 1 > TENANT'. The '1. TENANT' tab is active. In the 'Tenant Identity' section, the 'Name' field contains 'App-A'. The 'Description' field is optional. The 'Tags' field is empty. The 'Monitoring Policy' dropdown is set to 'default'. Under 'Security Domains', there is a table with two rows: 'Select' and 'Name'. The 'all' domain is selected with a checked checkbox, and the 'mgmt' domain is unselected with an unchecked checkbox.

Select	Name	Description
<input checked="" type="checkbox"/>	all	
<input type="checkbox"/>	mgmt	

4. Click Next.
5. Click + sign to add network.

CREATE TENANT

STEP 2 > NETWORK

Tenant Foundation

Create A Network



6. In the CREATE NEW NETWORK dialog box, type App-A as the Name. Leave everything else as default.
7. Click Next.
8. Use bd-Internal as the Name of the bridge domain.
9. Select default for IGMP Snoop Policy.

TENANT APP-A

CREATE NEW NETWORK

NET

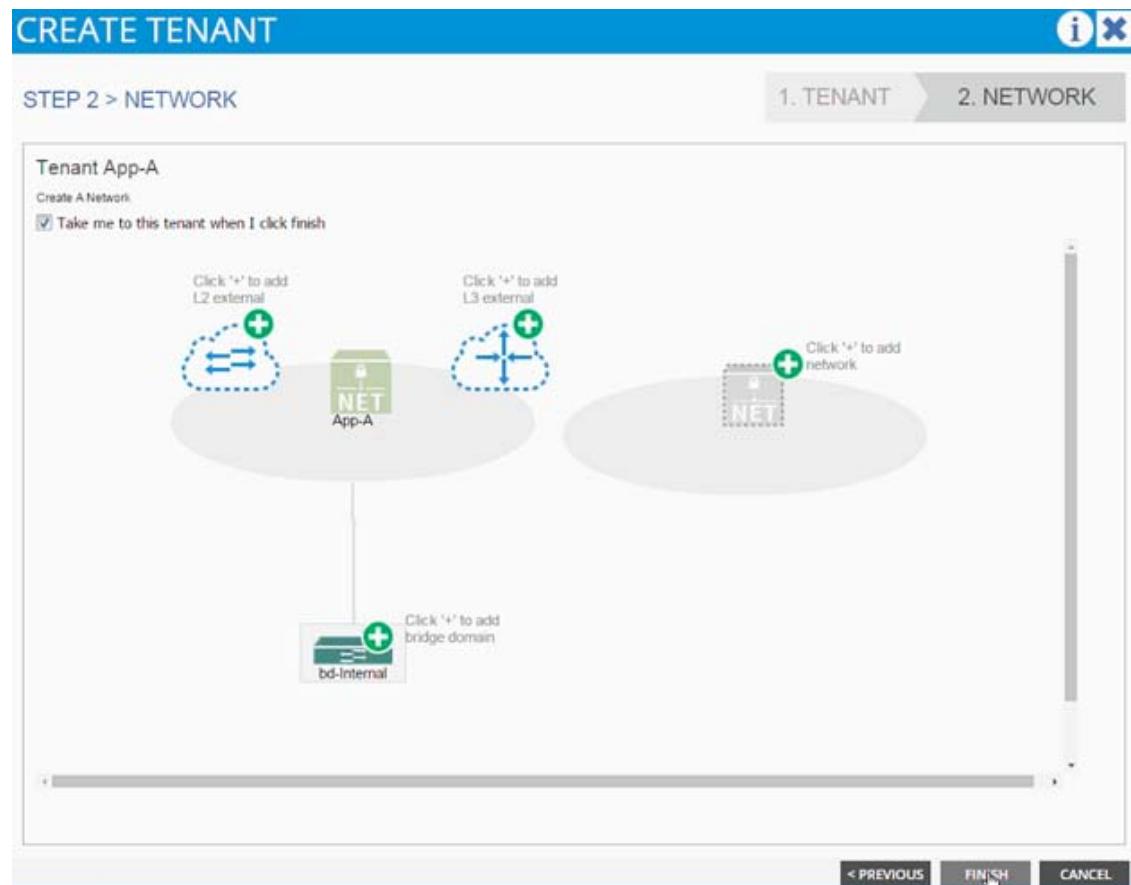
NETWORK > BRIDGE DOMAIN

Specify Bridge Domain for the Network

Name:	bd-Internal
Description:	optional
Forwarding:	Optimize
IGMP Snoop Policy:	default
Config BD MAC Address:	<input type="checkbox"/>
Subnets:	[+] [X]
Gateway Address Scope Subnet Control	
DHCP Labels:	[+] [X]
Name Scope DHCP Option Policy	

< PREVIOUS OK CANCEL

10. Click OK.
11. The Bridge Domains and App-A network should be visible in the CREATE TENANT dialog box.



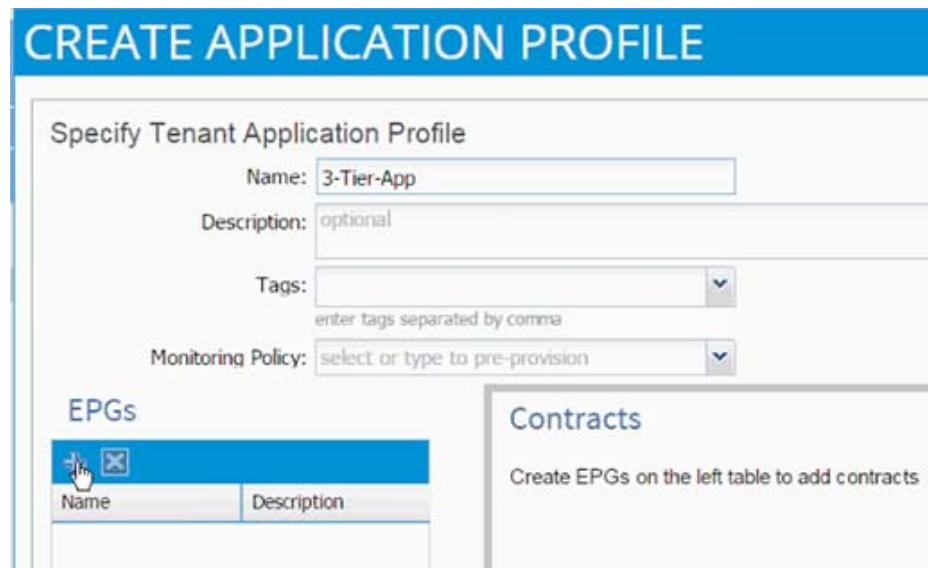
12. Click Finish.
13. Verify the selected tenant is the newly created App-A tenant by looking at the items highlighted in the top menu.



3-Tier App - Application Profile Creation and Adding EPG for Web Tier

In this section, an application profile to host the application will be created.

1. Select Tenant and the newly created App-A tenant from the top menu.
2. Expand Tenant App-A in the left menu bar.
3. Right-click Application Profile and click Create Application Profile.
4. In the CREATE APPLICATION PROFILE dialog box, enter 3-Tier-App as the Name.
5. From the drop-down list, select default for Monitoring Policy.
6. Click + next to EPG to add an EPG.



7. In the CREATE APPLICATION EPG dialog box, enter Web as the Name.
8. From the drop-down list, select bd-Internal as the Bridge Domain.
9. From the drop-down list, select default for Monitoring Policy.
10. Click OK.
11. Click + next to Associated Domain Profiles (VMs or Bare metals).
12. From the drop-down list, select the VMM domain previously defined.
13. Select Immediate for Deployment Immediacy.
14. Select Immediate for Resolution Immediacy.

CREATE APPLICATION EPG

STEP 1 > IDENTITY

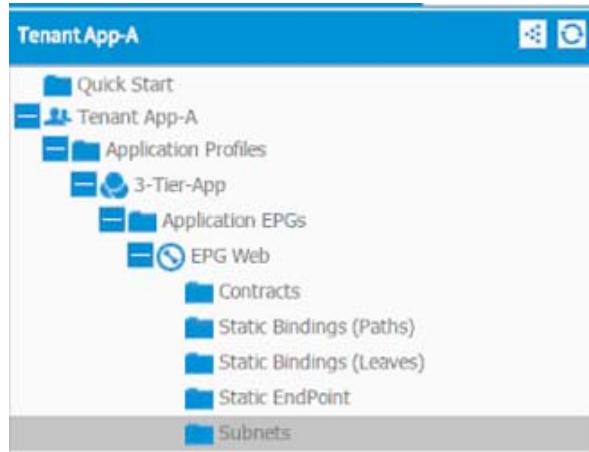
1. IDENTITY

Specify the EPG Identity

Name:	Web						
Description:	optional						
Tags:	<input type="text"/>						
enter tags separated by comma							
QoS class:	Unspecified						
Custom QoS:	select or type to pre-provision						
Bridge Domain:	bd-Internal						
Monitoring Policy:	default						
Associated Domain Profiles (VMs or bare metals):							
<table border="1"> <thead> <tr> <th>Domain Profile</th> <th>Deployment Immediacy</th> <th>Resolution Immediacy</th> </tr> </thead> <tbody> <tr> <td>VMM Domain - A01-VC</td> <td>Immediate</td> <td>Immediate</td> </tr> </tbody> </table>		Domain Profile	Deployment Immediacy	Resolution Immediacy	VMM Domain - A01-VC	Immediate	Immediate
Domain Profile	Deployment Immediacy	Resolution Immediacy					
VMM Domain - A01-VC	Immediate	Immediate					
Statically Link with Leaves/Paths: <input type="checkbox"/>							

< PREVIOUS OK CANCEL

15. Click UPDATE.
16. Click OK.
17. Click SUBMIT to finish creating Application Profile.
18. Expand the newly created EPG Web and click Subnets.



19. Click Action and select Create EPG Subnet.

The screenshot shows a table titled 'Subnets' with the following columns: IP, SCOPE, and SUBNET CONTROL. A message at the bottom says 'No items have been found. Select Actions to create a new item.' On the right, there is an 'ACTIONS' dropdown menu with two options: 'Create EPG Subnet' (highlighted with a blue border) and 'Delete'.

20. Enter 10.10.1.254/24 for the Default Gateway IP. This IP address is the gateway that all the Web VMs will use.
21. Change scope to only Shared Subnet.

The screenshot shows the 'CREATE EPG SUBNET' dialog with the following fields:

- Specify the Subnet Identity**
- Default Gateway IP:** 10.10.1.254/24 (Address) 255.255.255.0 (Mask)
- Scope:** Shared Subnet, Public Subnet, Private Subnet
- Description:** optional
- Subnet Control:** Querier IP
- L3 Out for Route Profile:** select or type to pre-provision
- Route Profile:** select value

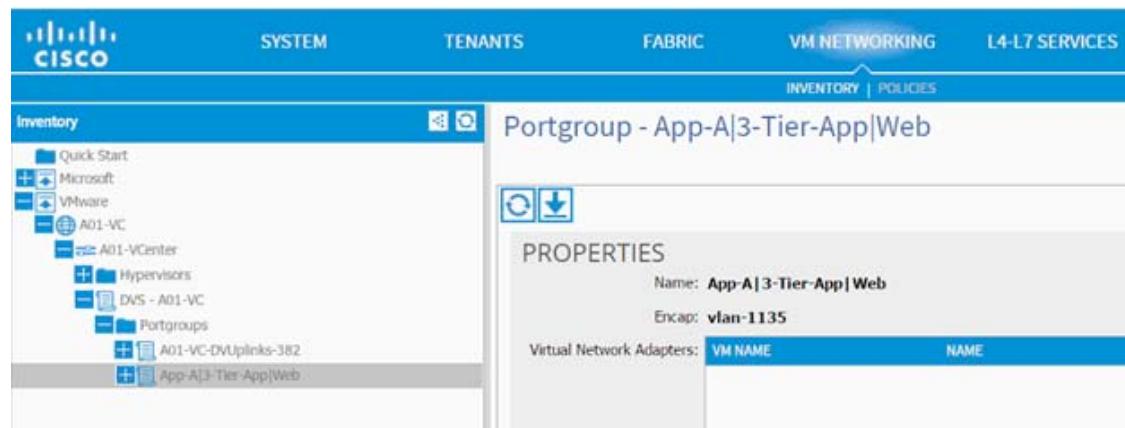
At the bottom are 'SUBMIT' and 'CANCEL' buttons.

22. Click Submit.

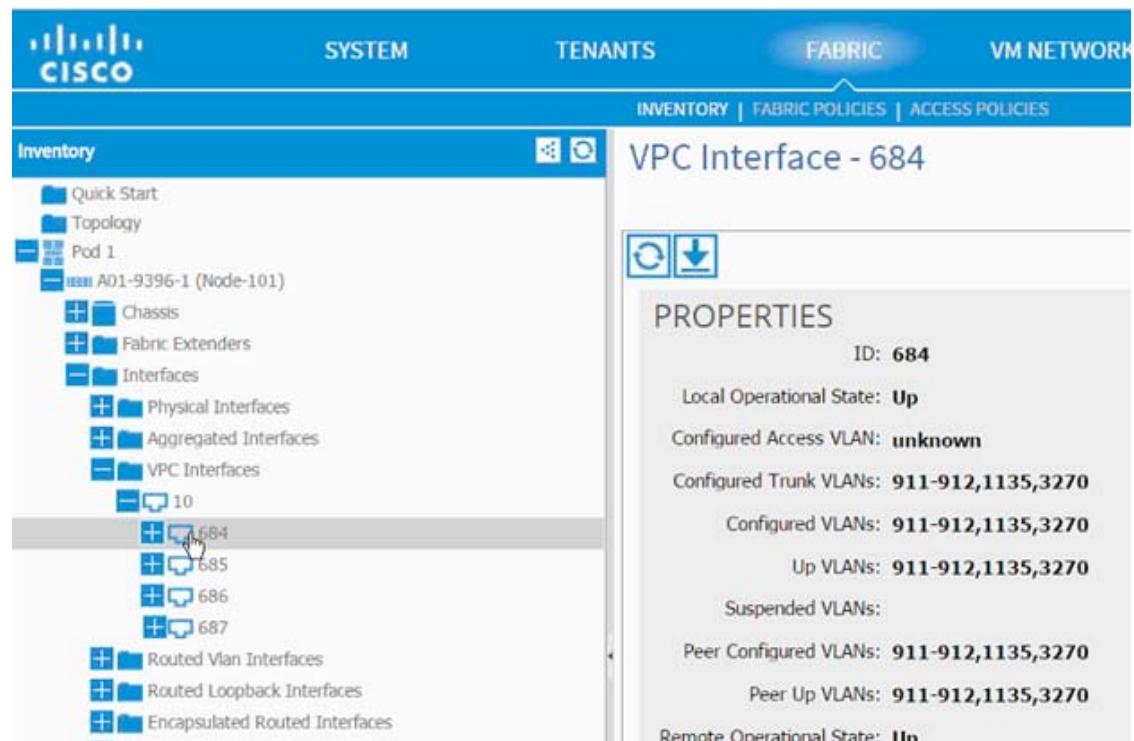
Port-Group Deployment Validation

When an EPG is tied to a VMM domain, a port-group gets created on the VDS so that the application admin can deploy a virtual machine and make it part of the application tier just defined. A dynamic VLAN is associated with this newly created EPG/port-group. To validate the configuration complete the following steps:

1. Browse to the VM NETWORKING and on the left menu bar, drill down to VDS to list the port-groups. VLAN 1135 from the pre-defined range 1101-1200 was assigned to the newly created port-group



2. Browse to FABRIC and in the left menu bar, expand the Leaf, Interface, vPC Interfaces, and domain 10. Click the vPC associated with UCS Fabric Interconnect
3. VLAN 1135 should have been added to the vPC VLANs.



4. Log into the vCenter and browse to the VDS. Right-click the newly added port-group and click Teaming and Failover.
5. Validate Load balancing method is Route based on originating virtual port (VMware default).



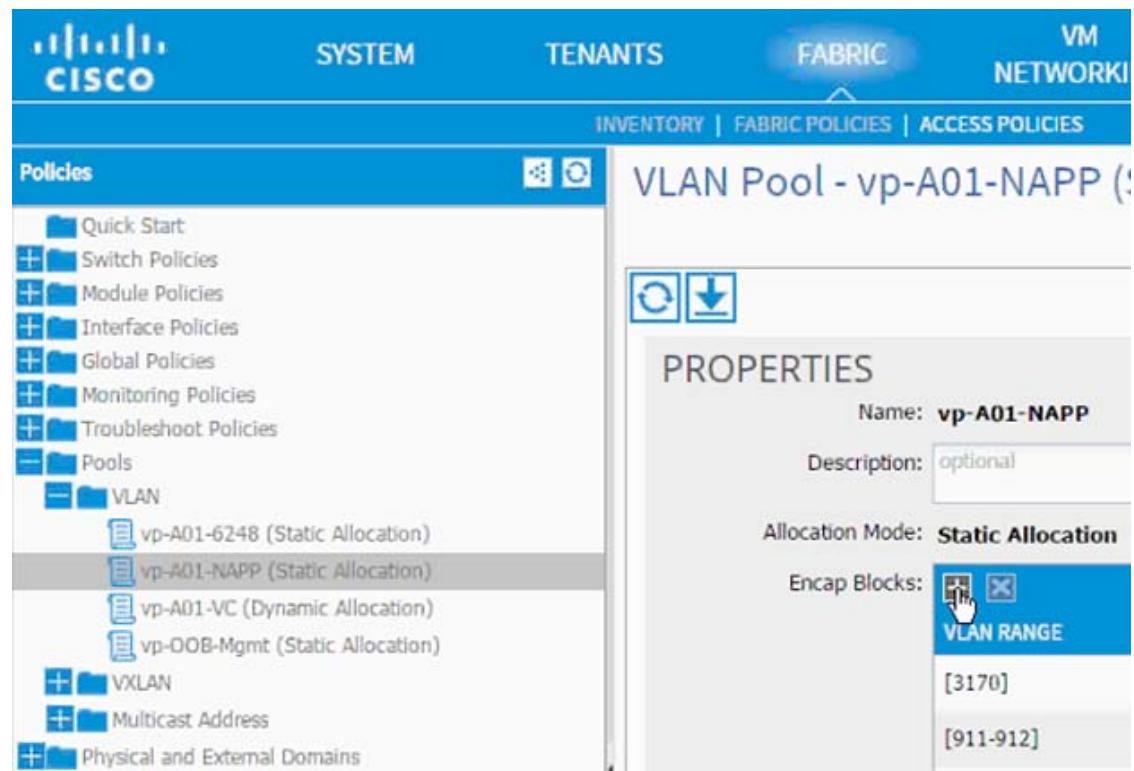
6. Validate the VLAN assigned is 1135.



Modifying the Storage (NetApp) Physical Domain VLANs

The physical domain associated with NetApp storage was initially configured for infrastructure iSCSI and NFS VLANs. In this step, NFS and iSCSI VLANs associated with App-A SVM will be added to the physical domain

1. Select Fabric and Access Policies from the top menu.
2. Expand Pools and then VLAN.
3. Click the pool name associated with the NetApp controllers (vp-A01-NetApp in this example) and click + to add another Encap Block.

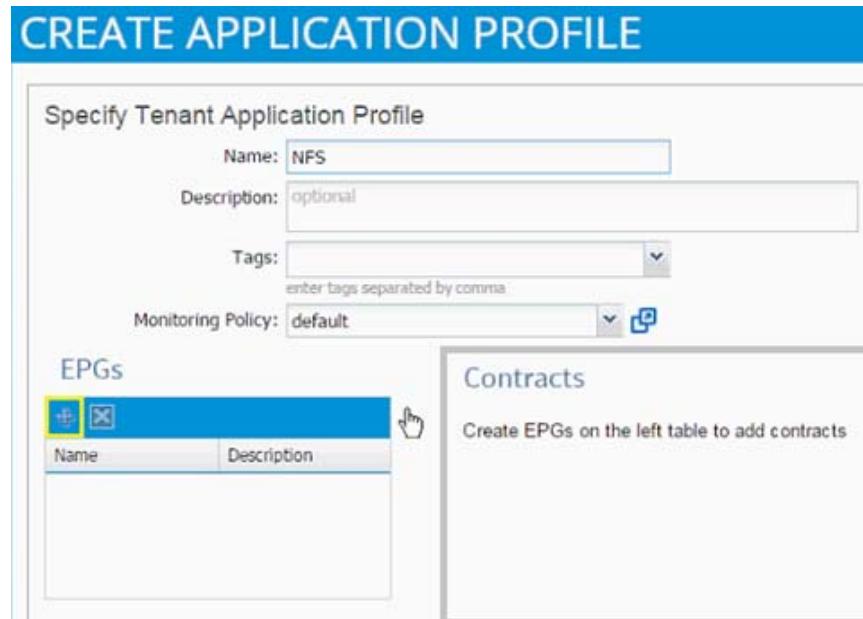


4. Enter <>var_nfs_vlan_tenant<> (3180 to 3180 in this example) as the range of VLANs for Tenant NFS.
5. (Optional) Add the range of VLANs for iSCSI-a and iSCSI-b, if configuring the tenant for iSCSI access.
6. Click Submit.

NFS - Application Profile Creation

In this section, an application profile to setup NFS connectivity between the ESXi servers and the Application specific SVM will be created. An NFS datastore will then be mounted to host application specific virtual machines.

1. Select Tenant and App-A tenant from the top menu.
2. Expand Tenant App-A in the left menu bar.
3. Right-click Application Profile and click Create Application Profile.
4. In the CREATE APPLICATION PROFILE dialog box, enter NFS as the Name.
5. From the drop-down list, select default for Monitoring Policy.
6. Click + next to EPG to add an EPG.



7. In the CREATE APPLICATION EPG dialog box, enter vmk-nfs as the Name.
8. From the drop-down list, select bd-Internal as the Bridge Domain.
9. From the drop-down list, select default for Monitoring Policy.
10. Click OK.
11. Click + next to Associated Domain Profiles (VMs or Bare metals).
12. From the drop-down list, select the VMM domain previously defined.
13. Select Immediate for Deployment Immediacy.
14. Select Immediate for Resolution Immediacy.

CREATE APPLICATION EPG

STEP 1 > IDENTITY

1. IDENTITY

Specify the EPG Identity

Name:	vmk-nfs						
Description:	optional						
Tags:	<input type="text"/> enter tags separated by comma						
QoS class:	Unspecified						
Custom QoS:	select or type to pre-provision						
Bridge Domain:	bd-Internal						
Monitoring Policy:	default						
Associated Domain Profiles (VMs or bare metals):	<table border="1"> <thead> <tr> <th>Domain Profile</th> <th>Deployment Immediacy</th> <th>Resolution Immediacy</th> </tr> </thead> <tbody> <tr> <td>VMM Domain - A01-VC</td> <td>Immediate</td> <td>Immediate</td> </tr> </tbody> </table>	Domain Profile	Deployment Immediacy	Resolution Immediacy	VMM Domain - A01-VC	Immediate	Immediate
Domain Profile	Deployment Immediacy	Resolution Immediacy					
VMM Domain - A01-VC	Immediate	Immediate					
Statically Link with Leaves/Paths:	<input type="checkbox"/>						

< PREVIOUS **OK** **CANCEL**

15. Click UPDATE.
16. Click OK.
17. Click + next to EPG to add another EPG.
18. In the CREATE APPLICATION EPG dialog box, enter lif-nfs as the Name.
19. From the drop-down list, select bd-internal as the Bridge Domain.
20. From the drop-down list, select default for Monitoring Policy.

CREATE APPLICATION EPG

STEP 1 > IDENTITY

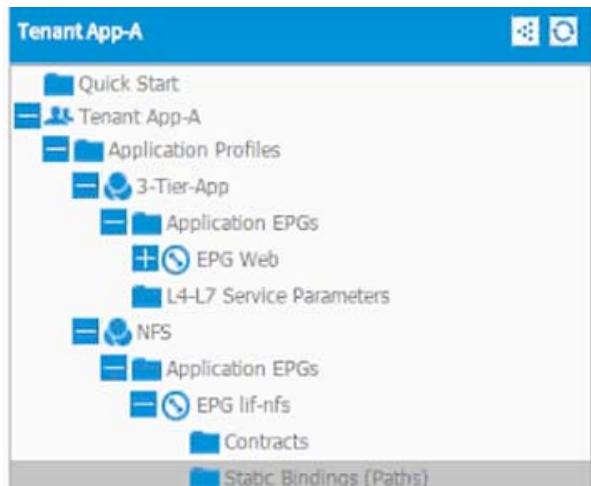
1. IDENTITY

Specify the EPG Identity

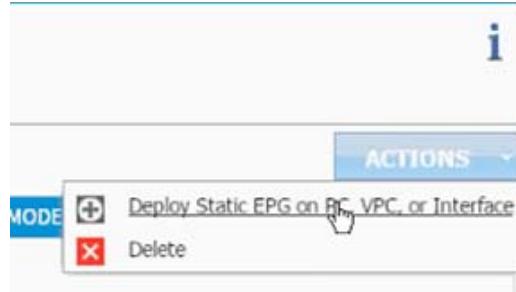
Name:	lif-nfs						
Description:	optional						
Tags:	<input type="text"/>						
enter tags separated by comma							
QoS class:	Unspecified						
Custom QoS:	select or type to pre-provision						
Bridge Domain:	bd-Internal						
Monitoring Policy:	default						
Associated Domain Profiles (VMs or bare metals):	<input type="button" value="+"/> <input type="button" value="X"/> <table border="1"> <thead> <tr> <th>Domain Profile</th> <th>Deployment Immediacy</th> <th>Resolution Immediacy</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Domain Profile	Deployment Immediacy	Resolution Immediacy			
Domain Profile	Deployment Immediacy	Resolution Immediacy					
<input type="checkbox"/> Statically Link with Leaves/Paths:							

< PREVIOUS **OK** **CANCEL**

21. Click OK.
22. Click SUBMIT to finish creating Application Profile.
23. Expand the newly created NFS Application profile from the menu bar on the left.
24. Expand NFS, expand Application EPGs and expand EPG lif-nfs.
25. Click Static Bindings (Paths).



26. Click Action.
27. Click Deploy Static EPG on PC, vPC, or Interface.



28. In the DEPLOY STATIC EPG ON PC, VPC OR INTERFACE dialog box, select Virtual Port Channel as the Path Type.
29. From the drop-down list Path, select NetApp Controller 1.

DEPLOY STATIC EPG ON PC, VPC, OR I... i x

Select PC, VPC, or Interface

Path Type: Port
 Direct Port Channel
 Virtual Port Channel

Path: !

Encap: topology/pod-1/protpaths-101-102/pathep-[pg-A01-6248-1]
topology/pod-1/protpaths-101-102/pathep-[pg-A01-6248-2]
topology/pod-1/protpaths-101-102/pathep-[pg-A02-NAPP-1]
topology/pod-1/protpaths-101-102/pathep-[pg-A02-NAPP-2]
802.1P Tag

Deployment Immediacy:

Mode:

SUBMIT **CANCEL**

30. Enter `vlan-<App-A-NFS LIF VLAN>` for Encap; VLAN 3180 is the NFS VLAN on NetApp Controller in the screenshot below.
31. Change Deployment Immediacy to Immediate.

DEPLOY STATIC EPG ON PC, VPC, OR I... i X

Select PC, VPC, or Interface

Path Type: Port
 Direct Port Channel
 Virtual Port Channel

Path: ▼ ✚

Encap:
 For example, vlan-1

Deployment Immediacy: Immediate
 On Demand

Mode: Tagged
 Untagged
 802.1P Tag

SUBMIT CANCEL

32. Click Submit.
33. Repeat these steps for mapping NetApp Controller 2 path.

The screenshot shows the Cisco ACI Tenant App-A interface. The left sidebar lists Tenant App-A components: Quick Start, Tenant App-A, Application Profiles (3-Tier-App, NFS), Application EPGs (EPG lif-nfs, Contracts), and Static Bindings (Paths). The main panel displays "Static Bindings (Paths)" for "Node: Nodes-101-102". It shows two entries:

PATH	ENCAP	DEPLOYMENT
Node-101-102/pg-A02-NAPP-1	vlan-3180	Immediate
Node-101-102/pg-A02-NAPP-2	vlan-3180	Immediate

34. Click Contracts under the EPG lif-nfs.
35. Click Action and select Add Provided Contract.
36. From the ADD PROVIDED CONTRACT dialog box, select Create Contract under Contract.

ADD PROVIDED CONTRACT

Select a contract

Contract: !

QoS:

[Create Contract](#)

SUBMIT **CANCEL**

37. Enter Allow-NFS as Name in the CREATE CONTRACT dialog box.
38. Click + next to Subjects to add a new contract subject.
39. In the CREATE CONTRACT SUBJECT dialog box, enter Allow-All as the Name.
40. Click + under Filter Chain to add a new filter.

CREATE CONTRACT SUBJECT

Specify Identity Of Subject

Name:

Description:

Reverse Filter Ports:

Apply Both Directions:

Filter Chain

FILTERS

Name

L4-L7 SERVICE GRAPH

Service Graph:

PRIORITY

QoS:

OK **CANCEL**

41. From the FILTERS drop-down list and click +.

CREATE CONTRACT SUBJECT

Specify Identity Of Subject

Name:	Allow-NFS
Description:	optional
Reverse Filter Ports:	<input checked="" type="checkbox"/>
Apply Both Directions:	<input checked="" type="checkbox"/>

Filter Chain

FILTERS

NAME		TENANT
Tenant: common		
arp	common	
default	common	
est	common	
icmp	common	

L4-L7 SERVICE GRAPH
Service Graph: select an option

PRIORITY
QoS:

OK CANCEL

42. In the CREATE FILTER dialog box, enter Allow-All as the Name. In this example, allow all the traffic for this contract.
43. Click + to add a filter.

CREATE FILTER

Specify the Filter Identity

Name:	Allow-All		
Description:	optional		
Entries:	+ X		
Name	EtherType	ARP Flag	IP Protocol

44. Enter Allow-All as the name of the filter.
45. From drop-down list, select IP as Ethertype.

CREATE FILTER

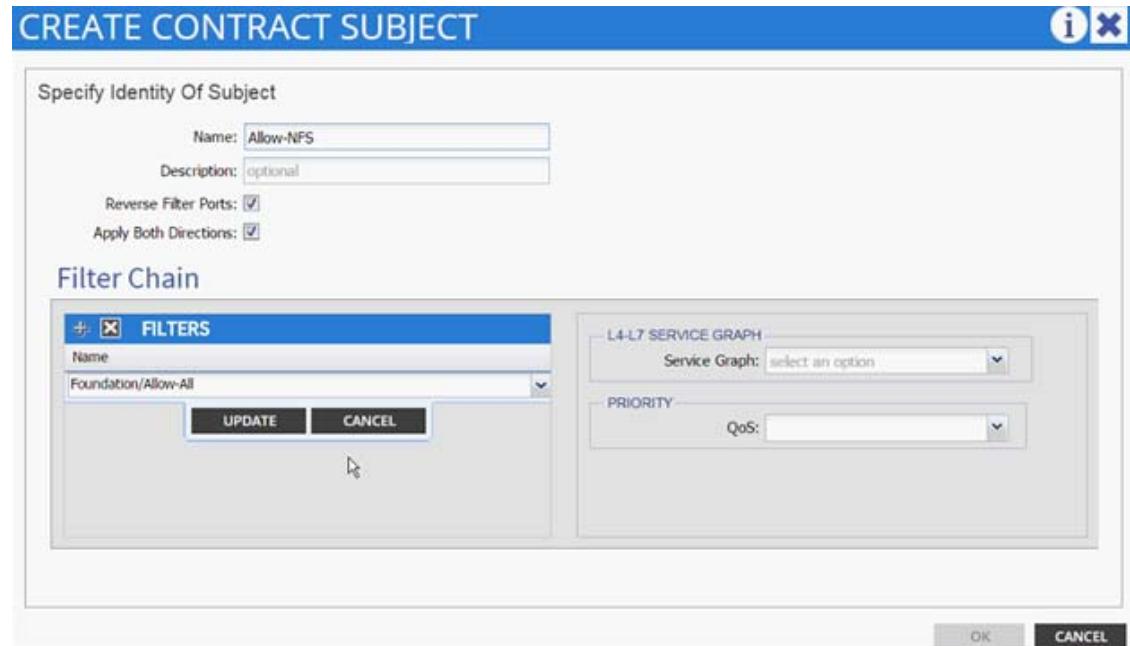
Specify the Filter Identity

Name:	Allow-All						
Description:	optional						
Entries:	+ X						
Name	EtherType	ARP Flag	IP Protocol	Allow Fragment	Source Port / Range	Destination Port / Range	TCP Session Rules
Allow-All	IP	Unspecified	Unspecified	<input type="checkbox"/>	From: <input type="text"/> To: <input type="text"/>	From: <input type="text"/> To: <input type="text"/>	From: <input type="text"/> To: <input type="text"/>

UPDATE CANCEL

46. Click Update.

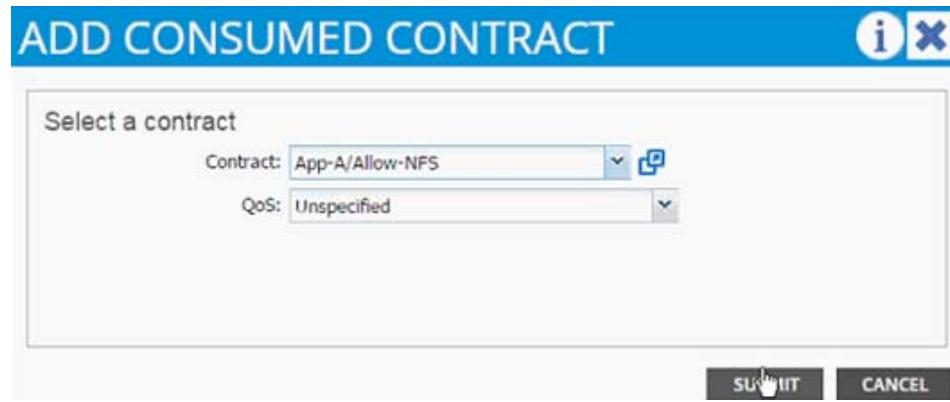
47. Click SUBMIT to create the filter.
48. Click UPDATE to add the newly created filter to the filter chain.



49. Click OK to finish creating the Contract Subject.
50. Click SUBMIT.
51. Click SUBMIT again to finish adding a provided contract.
52. Verify the Provided Contract appears under the Contracts.

TENANT NAME	CONTRACT NAME	CONTRACT TYPE	PROVIDED / CONSUMED
App-A	Allow-NFS	Contract	Provided

53. Expand EPG vmk-nfs.
54. Click Contracts.
55. Click ACTIONS and select Add Consumed Contract.
56. In the ADD CONSUMED CONTRACT dialog box, from the drop-down list select App-A/Allow-NFS contract.



57. Click Submit.

iSCSI Application Profile Creation (Optional)

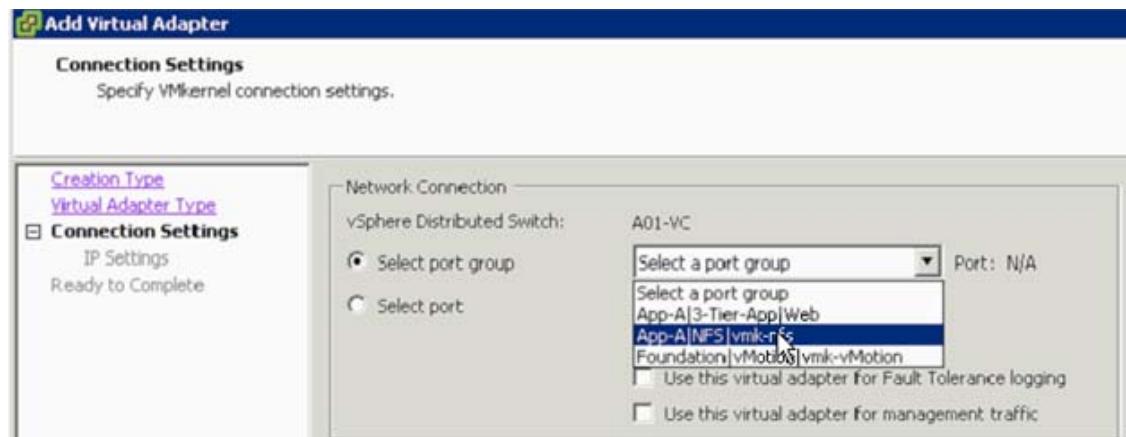
If an application requires access to block-based storage using iSCSI, steps from previous sections can be repeated to accomplish the following:

- Define two Bridge Domains - "bd-iSCSI-a" and "bd-iSCSI-b"
- Define an Application Profile called "iSCSI"
- Define four EPGs called "lif-iSCSI-a", "lif-iSCSI-b", "vmk-iSCSI-a" and "vmk-iSCSI-b"
- Use separate bridge domains for iSCSI-a and iSCSI-b EPGs
- Attach the vmk specific EPGs to the VMM domain
- Attach the LIF specific EPGs to static VLAN path mappings
- Define the contracts to enable communication between iSCSI-a and iSCSI-b vmk and lif EPGs
- Define VMkernel ports on the VMware vDS for iSCSI-a and iSCSI-b.
- Add the storage SVM targets in the VMware iSCSI software initiator.

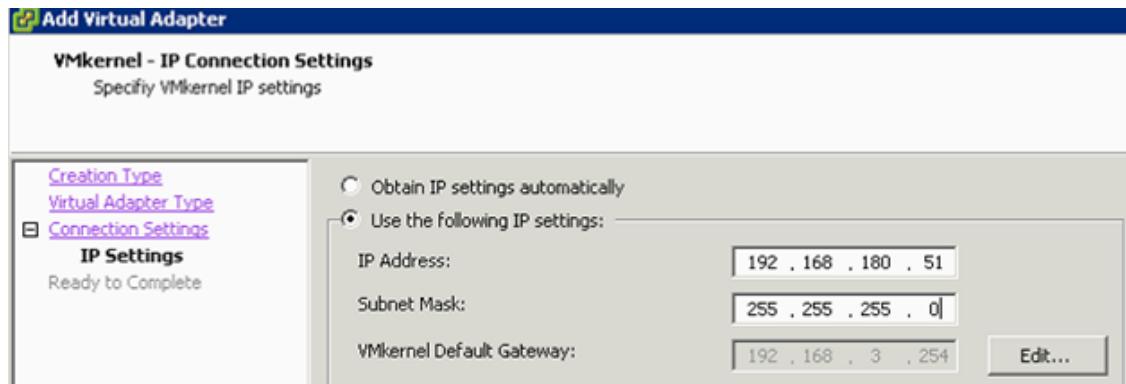
Defining NFS VMkernel Port and Mounting the Datastore

In the previous section, the NFS communication between the Application SVM and ESXi servers was set up. In this section, a VMkernel port will be defined on ESXi servers and NFS datastore will be mounted to host application specific virtual machines.

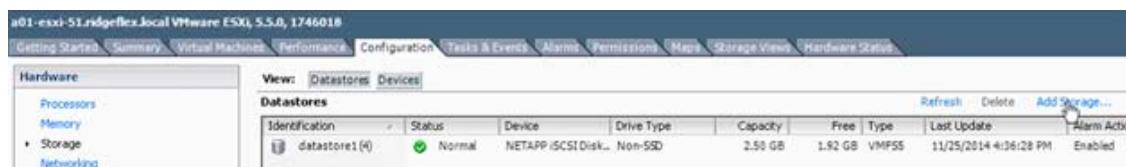
1. Select ESXi server in the vSphere Client. Click Configuration and then Networking.
2. Click vSphere Distributed Switch.
3. Click Manage Virtual Adapters.
4. Click Add to add VMkernel Port.
5. Select New virtual adapter. Click Next.
6. Click Next.
7. Select App-A|NFS|vnk-nfs from the drop-down list for Select port group.



8. Click Next.
9. Enter the NFS VMkernel Port IP address in the same subnet as the NetApp LIF defined earlier.

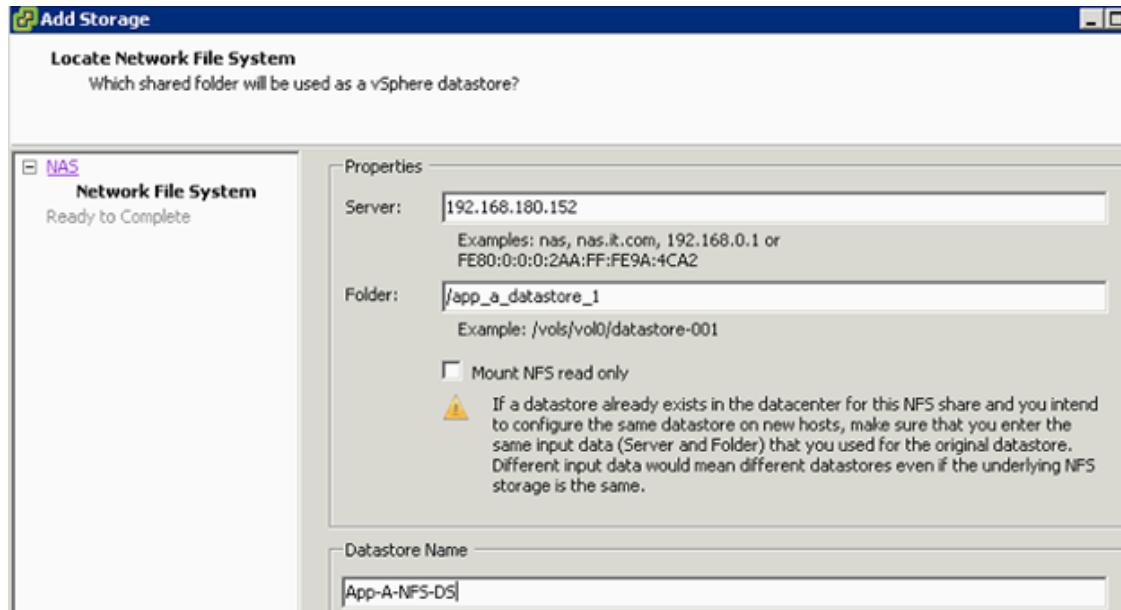


10. Click Next.
11. Click Finish.
12. Click the newly created vmk port and click Edit.
13. Set the MTU to 9000.
14. Click OK.
15. Click Close to finish setting up the VMkernel port.
16. Click Storage under Settings.
17. Click Add Storage.



18. Select Network File System.
19. Click Next.

20. Provide the SVM LIF address, path and datastore name for the predefined NFS datastore.



21. Click Next.
22. Verify information and click Finish.

Defining EPGs for Additional Application Tiers (Optional)

In the previous section, an application profile "3-Tier-App" was defined and an EPG "Web" was deployed. For defining EPGs for additional tiers of the application complete the following steps:

1. Expand Application Profiles for Tenant App-A.
2. Right-click 3-Tier-App and select Create Application EPG.
3. Provide the name of the Application Tier EPG (App in this example).
4. From the drop-down list, select bd-Internal as the Bridge Domain.
5. Select Monitoring Policy as default.
6. Click + to add Associated Domain Profiles (VMs or bare metals) and select vCenter domain.
7. Change Deployment Immediacy and Resolution Immediacy to Immediate.
8. Click Update.

CREATE APPLICATION EPG

STEP 1 > IDENTITY

1. IDENTITY

Specify the EPG Identity

Name:	App						
Description:	optional						
Tags:	enter tags separated by comma						
QoS class:	Unspecified						
Custom QoS:	select or type to pre-provision						
Bridge Domain:	bd-Internal						
Monitoring Policy:	default						
Associated Domain Profiles (VMs or bare metals):	<table border="1"> <tr> <th>Domain Profile</th> <th>Deployment Immediacy</th> <th>Resolution Immediacy</th> </tr> <tr> <td>VMM Domain - A01-VC</td> <td>Immediate</td> <td>Immediate</td> </tr> </table>	Domain Profile	Deployment Immediacy	Resolution Immediacy	VMM Domain - A01-VC	Immediate	Immediate
Domain Profile	Deployment Immediacy	Resolution Immediacy					
VMM Domain - A01-VC	Immediate	Immediate					
Statically Link with Leaves/Paths:	<input type="checkbox"/>						

ACTIONS

< PREVIOUS FINISH CANCEL

9. Click Finish.
10. Expand the newly created EPG App and click Subnets.
11. Click Action and select Create EPG Subnet.

Subnets

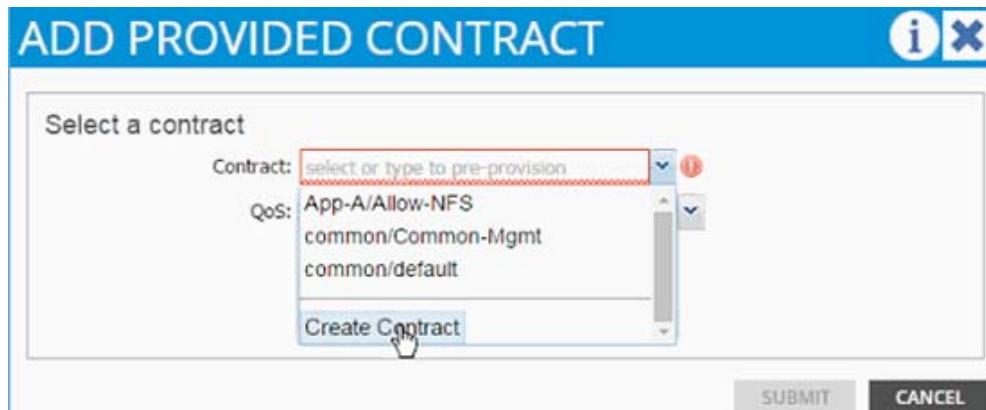
IP	SCOPE	SUBNET CONTROL	ACTIONS
No items have been found. Select Actions to create a new item.			

12. Enter 10.10.2.254/24 for the Default Gateway IP. This IP address is the gateway that all the App VMs will use; adjust this subnet according to your implementation.
13. Change the scope to only Shared Subnet.
14. Click Finish.
15. Repeat these steps for additional EPG (application tier) definitions.

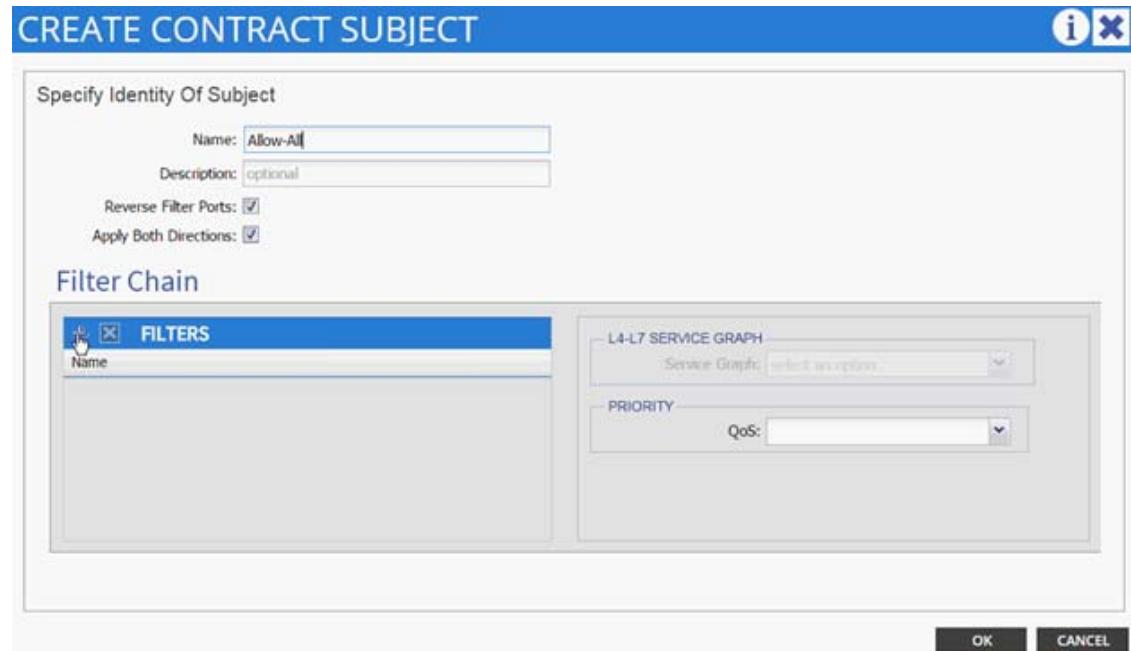
Enabling Communication Between Application Tiers

If an application tier needs to communicate to another application tier, a contract needs to be provided by one EPG and consumed by the other. In this example, the previously defined "App" EPG will provide a contract and "Web" EPG will consume the contract. The ports on which the two application tiers can be limited in the contract subject but for this example, all communication will be allowed between the two tiers.

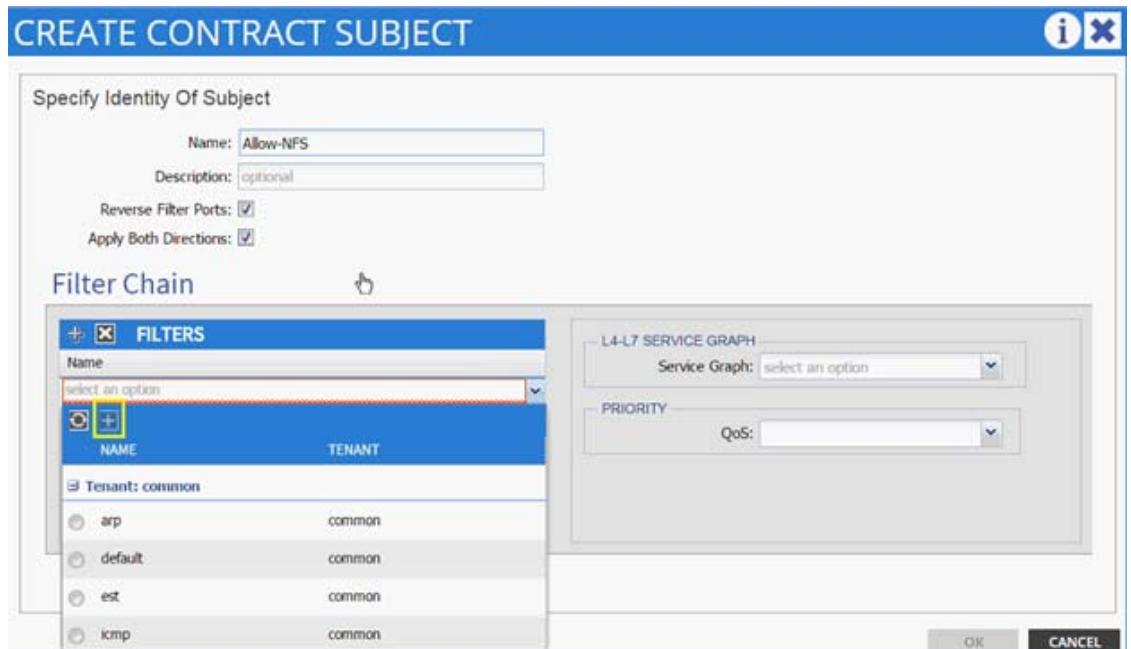
1. Expand the Application Profile 3-Tier-App, Application EPGs, and EPG App.
2. Click Contracts under the EPG App.
3. Click Action and select Add Provided Contract.
4. From the ADD PROVIDED CONTRACT dialog box, select Create Contract under Contract.



5. Enter Allow-App-Web as Name in the CREATE CONTRACT dialog box.
6. Click + next to Subjects to add a new contract subject.
7. In the CREATE CONTRACT SUBJECT dialog box, enter Allow-All as the Name.
8. Click + under Filter Chain to add a new filter.



9. From the FILTERS drop-down list click +.



10. In the CREATE FILTER dialog box, enter Allow-All as the Name. In this example, allow all the traffic for this contract.
11. Click + to add a filter.

CREATE FILTER

Specify the Filter Identity

Name:	Allow-All		
Description:	optional		
Entries:	[+] [X]		
Name	EtherType	ARP Flag	IP Protocol

12. Enter Allow-All as the name of the filter.
13. From drop-down list, select IP as EtherType.

CREATE FILTER

Specify the Filter Identity

Name:	Allow-All						
Description:	optional						
Entries:	[+] [X]						
Name	EtherType	ARP Flag	IP Protocol	Allow Fragment	Source Port / Range	Destination Port / Range	TOP Session Rules
Allow-All	IP	Unspecified	Unspecified	<input type="checkbox"/>	From _____ To _____	From _____ To _____	Unspecified

14. Click Update.
15. Click SUBMIT to create the filter.
16. Click UPDATE to add the newly created filter to the filter chain.

CREATE CONTRACT SUBJECT

Specify Identity Of Subject

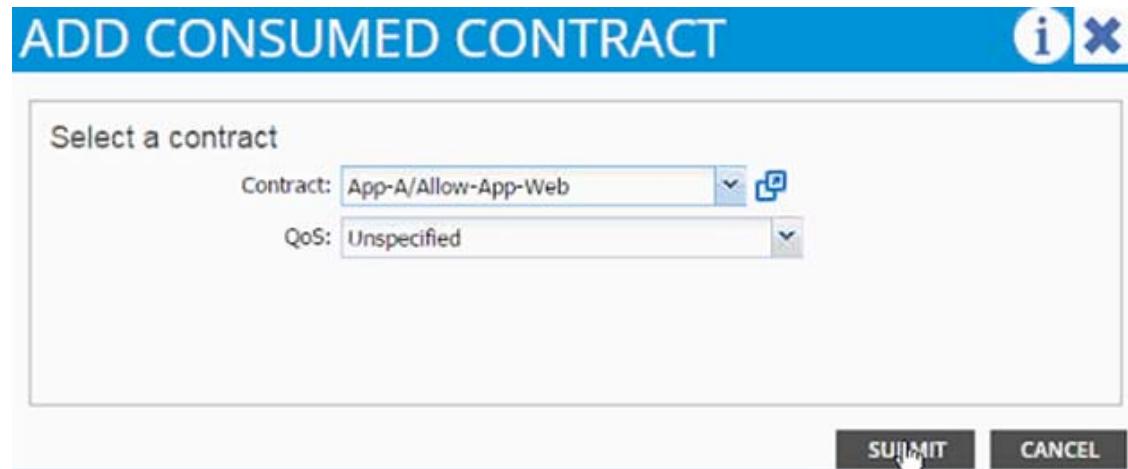
Name:	Allow-All
Description:	optional
Reverse Filter Ports:	<input checked="" type="checkbox"/>
Apply Both Directions:	<input checked="" type="checkbox"/>

Filter Chain

FILTERS
Name
App-A/Allow-All

17. Click OK to finish creating the Contract Subject.
18. Click SUBMIT.
19. Click SUBMIT again to finish adding a provided contract.
20. Expand EPG Web.
21. Click Contracts in the left menu.

22. Click ACTIONS and select Add Consumed Contract.
23. In the ADD CONSUMED CONTRACT dialog box, from the drop-down list select App-A/Allow-App-Web contract.

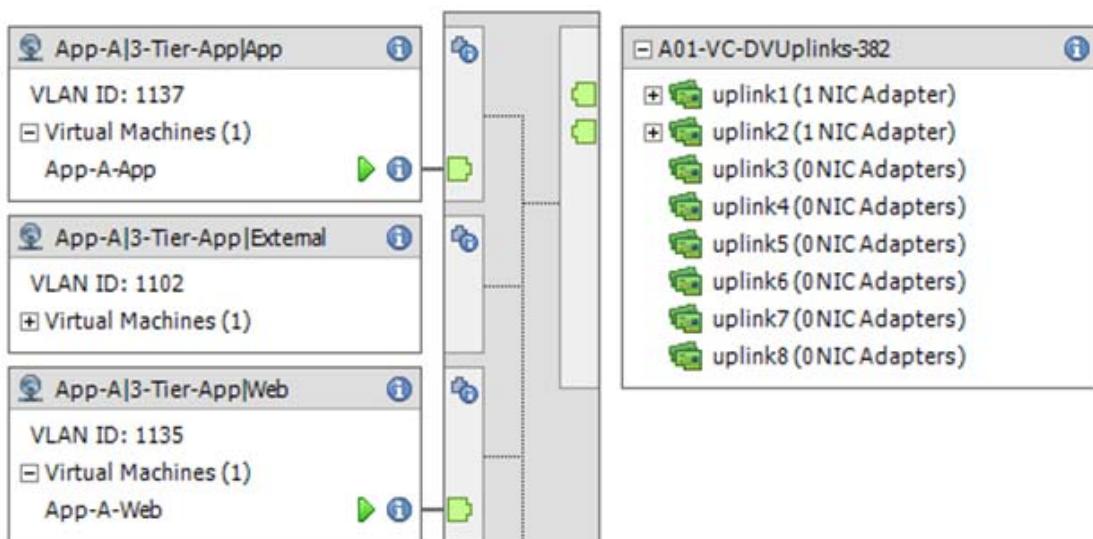


24. Click Submit.

Deploying Virtual Machines

After completing the configuration process, application related virtual machines can be deployed using vSphere client. VMware distributed switched managed using APIC will show port-groups for the Application EPGs defined in previous steps. The Web-tier VMs will be deployed and connected to the port-group labeled "App-a|3-Tier-App-Web". VM related to other application tiers will be deployed in their respective port-groups. The resulting VDS configuration for an ESXi host will look like [Figure 5](#). As the name suggests, App-A-Web is the web-VM while App-A-App is the application virtual machine.

Figure 5 ESXi - VDS Deployment Example for Application Virutal Machines



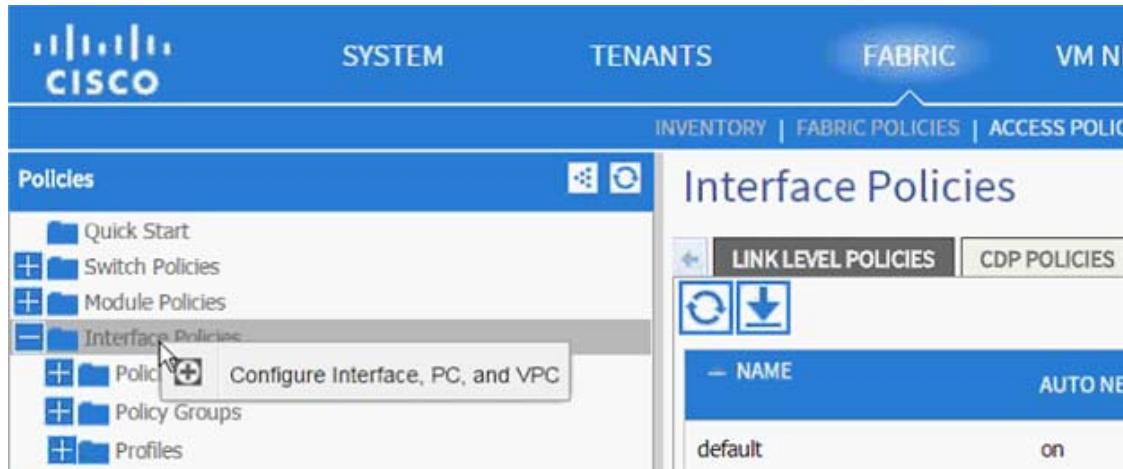
Cisco ACI - Accessing Common Services

This section provides a detailed procedure for configuring access to common services such as AD, DNS and in some cases vCenter. The leaf switches in the ACI fabric connect to an existing management switch where common service servers or virtual machines are connected using a dedicated LAN segment (VLAN 3177 in this case). This management segment is then mapped to an EPG in the common tenant using static VLAN mappings. In ACI, any contracts defined and provided in the common tenant can be consumed in any all other tenants and this makes common tenant an ideal candidate to host the common services management EPGs.

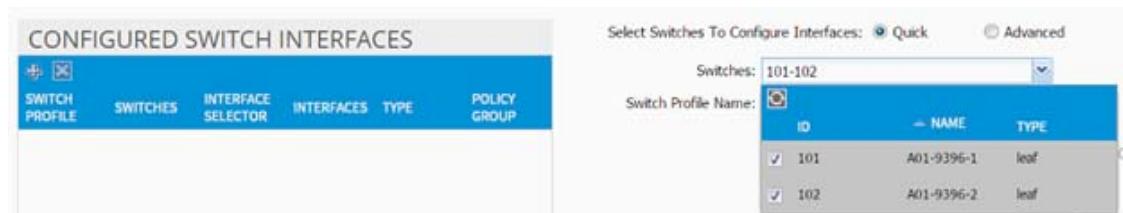
Configuring ACI for Management Switch

A vPC for management switch will be created using the interface creation wizard.

1. From the main menu, click FABRIC and select Access Policies.
2. Right-click Interface Policies and select Configure interface, PC and vPC.



3. In the dialog box, click + under the CONFIGURED SWITCH INTERFACES.
4. From the Switches drop-down list select both leaves.



5. Enter <sp-OOB-Mgmt> as the Switch Profile Name. OOB-Mgmt is the host name for management switch.
6. Click + to add interfaces.
7. Select the vPC radio button to configure vPC.
8. Enter 1/21 under Interfaces. This is the port on both switches where existing management switch is connected.

9. Enter <ifs- OOB-Mgmt> as the Interface Selector Name.
10. From the vPC Policy Group drop-down list and click Create vPC Interface Policy Group. A new dialog box will appear.
11. Enter <pg- OOB-Mgmt> as the name of the vPC INTERFACE POLICY GROUP in the dialog box.
12. From the Link Level Policy drop-down list, select Create Link Level Policy.
13. In the CREATE LINK LEVEL POLICY, enter 1_GE as the Name.
14. Select 1 Gbps as the Speed.
15. Click Submit.

CREATE LINK LEVEL POLICY

Specify the Physical Interface Policy Identity

Name:

Description:

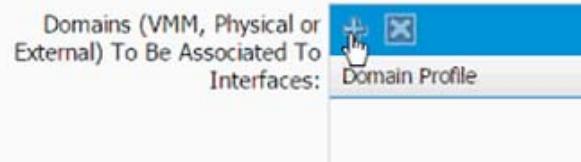
Auto Negotiation: off on

Speed: 40 Gbps
 1 Gbps
 10 Gbps
 100 Mbps

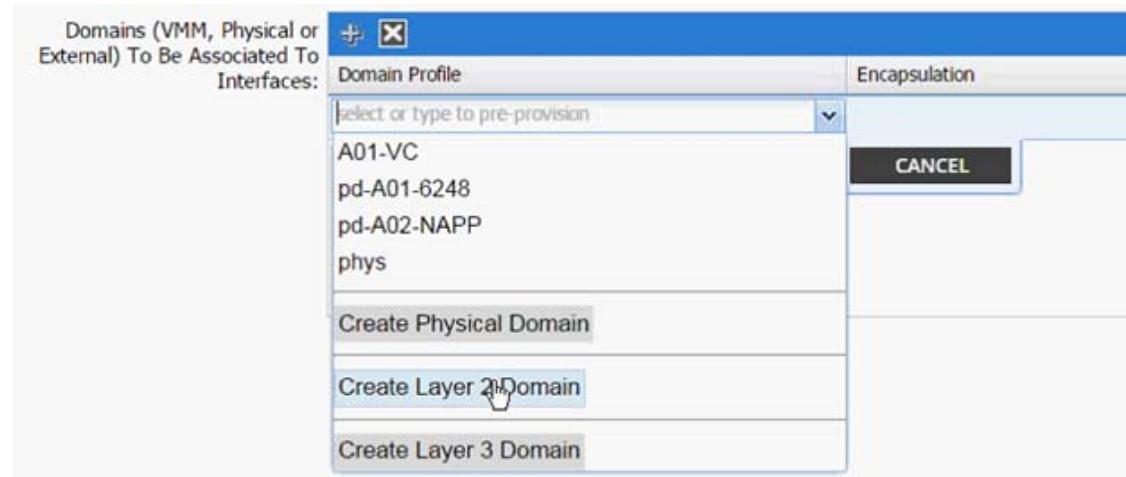
Link debounce interval (msec):

SUBMIT **CANCEL**

16. Select CDP_Enabled as CDP Policy.
17. Select LLDP_Disabled as LLDP Policy.
18. Select default as STP Interface Policy.
19. Select LACP_ACTIVE as LACP Policy.
20. Select default as Monitoring Policy.
21. From the Attached Entity Profile drop-down list and click Create Attachable Access Entity Profile. A new dialog box will appear
22. Enter <aep-OOB-Mgmt> as the Name.
23. Click + to add Domain.



24. In the added domain, from the drop-down list select Create Layer 2 Domain.



25. In the Create Layer 2 Domain dialog box, enter <L2-OOB-Mgmt> as Name.
26. From the VLAN Pool drop-down list select Create VLAN Pool.

CREATE LAYER 2 DOMAIN

Specify the Layer 2 Domain

Name:	L2-OOB-Mgmt
VLAN Pool:	select an option
vp-A01-6248 vp-A01-NAPP vp-A01-VC Create VLAN Pool	

SUBMIT **CANCEL**

27. In the Create VLAN Pool dialog box, enter <vp-OOB-Mgmt> as Name.
28. Select Allocation Mode > Static Allocation.
29. Click + next to Encap Block.
30. In the CREATE RANGES dialog box, enter the two iSCSI VLANs and the NFS VLAN.



In the screenshot below, 3177 is the management VLAN utilized for common services segment.

CREATE RANGES

Specify the Encap Block Range

Type: **VLAN**

Range: **3177** - **3177**

From To

OK **CANCEL**

31. Click OK.

CREATE VLAN POOL

Specify the Pool identity

Name: **vp-OOB-Mgmt**

Description: optional

Allocation Mode: Dynamic Allocation
 Static Allocation

Encap Blocks: **+ X**

VLAN Range
[3177]

SUBMIT **CANCEL**

32. Click SUBMIT to finish VLAN pool creation.
33. Click SUBMIT to finish Layer 2 Domain creation.

CREATE LAYER 2 DOMAIN

Specify the Layer 2 Domain

Name:	L2-OOB-Mgmt
VLAN Pool:	vp-OOB-Mgmt

SUBMIT **CANCEL**

34. Click UPDATE to finish adding Layer 2 domain to AEP.

CREATE ATTACHABLE ACCESS ENTITY PROFILE

Specify the name, domains and infrastructure encaps

Name:	aep-OOB-Mgmt
Description:	optional
Enable Infrastructure VLAN:	<input type="checkbox"/>
Domains (VMM, Physical or External) To Be Associated To Interfaces:	<input type="button" value="+"/> <input checked="" type="checkbox"/> Domain Profile Encapsulation L2 External Domain - L2-OOB-Mgmt from:vlan-3177 to:vlan-3177

35. Click SUBMIT to finish adding AEP.
 36. Click SUBMIT to finish creating vPC Interface Policy Group.

Specify the Policy Group identity

Name:	pg-OOB-Mgmt				
Description:	optional				
Link Level Policy:	1_GE				
CDP Policy:	CDP_Enable				
LLDP Policy:	LLDP_Disabled				
STP Interface Policy:	default				
LACP Policy:	LACP_Active				
Monitoring Policy:	default				
Override Policy Group:	<input type="button" value="+"/> <input type="button" value="X"/>				
<table border="1"> <thead> <tr> <th>Name</th> <th>LACP Member Policy</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table>		Name	LACP Member Policy		
Name	LACP Member Policy				
Attached Entity Profile:	aep-OOB-Mgmt				

SUBMIT **CANCEL**

37. On the Configure Interface, PC, vPC screen, click SAVE.

Select Switches To Configure Interfaces: Quick Advanced

Switches:	101-102
Switch Profile Name:	DOB-Mgmt
Interface Type:	<input checked="" type="radio"/> Individual <input type="radio"/> PC <input type="radio"/> VPC
Interfaces:	1/21 Select interfaces by typing, e.g. 1/17-18 or use the mouse to click on the switch image below.
Color:	<input type="color"/>
Interface Selector Name:	ifs-OOB-Mgmt
VPC Policy Group:	pg-OOB-Mgmt

SAVE **CANCEL**

Switch (Access Port Fabric Port). Only the access ports can be selected.

38. Click SAVE.
39. Click SUBMIT to finish.

Configuring the Management Switch

This section details the management switch configuration. The Management switch connects to both Leaf switches using port Gig 0/37 and Gig 0/38. These ports form a LACP port-channel Po1.

```

interface Port-channel1
  description *** To ACI Fabric for Common Segment Connectivity ***
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 3177
  switchport mode trunk
end
!
interface GigabitEthernet0/37
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 3177
  switchport mode trunk
  channel-group 1 mode active
end
!
interface GigabitEthernet0/38
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 3177
  switchport mode trunk
  channel-group 1 mode active
end
!
MGMTSW# show etherchannel summary
Flags: D - down      P - in port-channel
      I - stand-alone S - suspended
      H - Hot-standby (LACP only)
      R - Layer3      S - Layer2
      U - in use       f - failed to allocate aggregator
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol     Ports
-----+-----+-----+
-----+
1      Po1 (SU)      LACP        Gi0/37 (P)   Gi0/38 (P)

```

Configuring Common Tenant

An EPG and a contract are configured in the common tenant. This contract will be consumed in all the application tenants, which require access to common services.

Common Management - Application Profile Creation

1. Select Tenant and common tenant from the top menu.

2. Expand Tenant common in the left menu bar.
3. Right-click Application Profile and click Create Application Profile.
4. In the CREATE APPLICATION PROFILE dialog box, enter Management for the Name.
5. From the drop-down list, select default for Monitoring Policy.
6. Click + next to EPG to add an EPG.

CREATE APPLICATION PROFILE

Specify Tenant Application Profile

Name:	Management
Description:	optional
Tags:	<input type="text"/> enter tags separated by comma
Monitoring Policy:	default <input type="button" value=""/>

EPGs

Name	Description

Contracts

Create EPGs on the left table to add contracts

7. In the CREATE APPLICATION EPG dialog box, enter Mgmt_Access for the Name.
8. From the drop-down list, select Create Bridge Domain as the Bridge Domain.
9. In the CREATE BRIDGE DOMAIN dialog box, use bd-Internal as the Name of the bridge domain.
10. From the drop-down list next to Network, select Create Private Network.

CREATE BRIDGE DOMAIN

Specify Bridge Domain for the Network

Name:	bd-Internal
Description:	optional
Network:	<input type="text"/> select or type to pre-provision
Forwarding:	default
Config BD MAC Address:	Create Private Network
IGMP Snoop Policy:	<input type="text"/> select or type to pre-provision

11. In the CREATE PRIVATE NETWORK dialog box, enter Common-Mgmt for the Name.

CREATE PRIVATE NETWORK

Specify Tenant Network

Name:

Policy enforcement: Enforced
 Unenforced

Description:

BGP Timers:

OSPF Timers:

Monitoring Policy:

 **SUBMIT** **CANCEL**

12. Click SUBMIT.
13. From the Forwarding drop-down list select Custom.
14. Check the boxes to enable Flooding and Unicast Routing.
15. Select default for IGMP Snoop Policy.

CREATE BRIDGE DOMAIN

Specify Bridge Domain for the Network

Network:

Forwarding:

L2 Unknown Unicast: Flood Hardware Proxy

Unknown Multicast Flooding: Flood Optimized Flood

ARP Flooding: Enabled

Unicast Routing: Enabled

Config BD MAC Address:

IGMP Snoop Policy:

Associated L3 Outs:

16. Click SUBMIT to finish bridge domain creation.
17. From the CREATE APPLICATION EPG dialog box, select the newly created bridge domain.

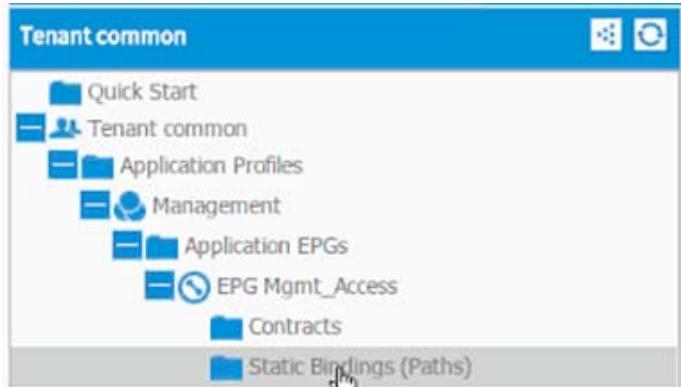
STEP 1 > IDENTITY

Specify the EPG Identity

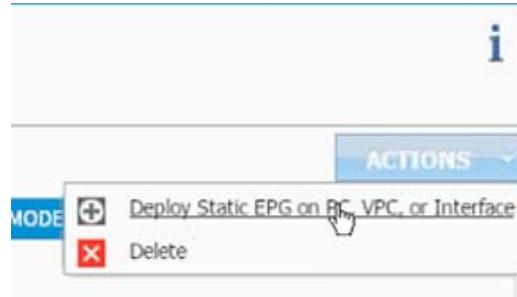
Name:	Mgmt_Access
Description:	optional
Tags:	<input type="text"/>
enter tags separated by comma	
QoS class:	Unspecified
Custom QoS:	<input type="text"/> select or type to pre-provision
Bridge Domain:	bd-Internal
Monitoring Policy:	bd-Internal default

Associated Domains Profiles (VMs or

18. From the drop-down list, select default for Monitoring Policy.
19. Click OK to finish EPG creation.
20. Click SUBMIT to finish creating Application Profile.
21. Expand the newly created Management Application profile from the menu bar on the left.
22. Expand Management, expand Application EPGs and expand EPG Mgmt_Access.
23. Click Static Bindings (Paths).



24. Click Actions.
25. Click Deploy Static EPG on PC, vPC, or Interface.



26. In the DEPLOY STATIC EPG ON PC, vPC OR INTERFACE dialog box, select Virtual Port Channel as the Path Type.
27. From the Path drop-down list, select OUT OF BAND management switch VPC.

DEPLOY STATIC EPG ON PC, VPC, OR I... i X

Select PC, VPC, or Interface

Path Type: Port
 Direct Port Channel
 Virtual Port Channel

Path: !

Encap:

Deployment Immediacy:

Mode:

SUBMIT CANCEL

28. Enter `vlan-< common_mgmt_segment>` for Encap; VLAN 3177 is the common management segment VLAN in the screenshot below.
29. Change Deployment Immediacy to Immediate.

DEPLOY STATIC EPG ON PC, VPC, OR I... i X

Select PC, VPC, or Interface

Path Type: Port
 Direct Port Channel
 Virtual Port Channel

Path: topology/pod-1/protpaths-101-102/pathep-[pg] i X

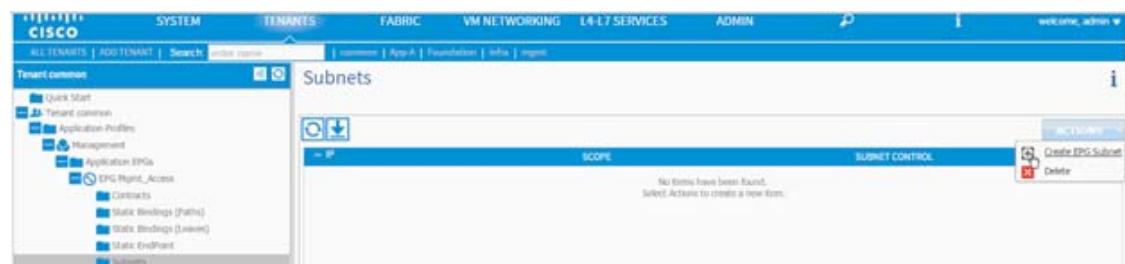
Encap: vlan-3177
 For example, vlan-1

Deployment Immediacy: Immediate
 On Demand

Mode: Tagged
 Untagged
 802.1P Tag

SUBMIT CANCEL

30. Click SUBMIT.
31. On the left menu bar, click Subnet.
32. From the ACTIONS menu, select Create EPG Subnet.



33. In the CREATE EPG SUBNET dialog box, enter 192.168.3.253/24 for the Default Gateway IP. The Mask field should be auto populated with 255.255.255.0
34. From the scope, only select Shared Subnet.

CREATE EPG SUBNET

Specify the Subnet Identity

Default Gateway IP:	192.168.3.253/24	Mask:	255.255.255.0
Address			
Scope:	<input checked="" type="checkbox"/> Shared Subnet <input type="checkbox"/> Public Subnet <input type="checkbox"/> Private Subnet		
Description:	optional		
Subnet Control:	<input type="checkbox"/> Querier IP		
L3 Out for Route Profile:	select or type to pre-provision		
Route Profile:	select value		

35. Click SUBMIT.
36. Click Contracts under the EPG Mgmt_Access.
37. Click Action and select Add Provided Contract.

38. From the ADD PROVIDED CONTRACT dialog box, select Create Contract under Contract.

ADD PROVIDED CONTRACT

Select a contract

Contract:	select or type to pre-provision
QoS:	common/default
<input type="button" value="Create Contract"/>	

ACTIONS

- Add Consumed Contract
- Add Consumed Contract Interface
- Add Toobar Contract
- Add Provider Contract
- Delete

SUBMIT CANCEL

39. Enter Common-Mgmt as Name in the CREATE CONTRACT dialog box.
40. Change the Scope to global from the drop-down list.
41. Click + next to Subjects to add a new contract subject.
42. In the CREATE CONTRACT SUBJECT dialog box, enter Allow-All as the Name.
43. Click + under Filter Chain to add a new filter.

CREATE CONTRACT SUBJECT

Specify Identity Of Subject

Name:	Allow-All
Description:	optional
Reverse Filter Ports:	<input checked="" type="checkbox"/>
Apply Both Directions:	<input checked="" type="checkbox"/>

Filter Chain

FILTERS	
Name	
<input style="width: 100%; height: 100%;" type="button" value="+"/>	

L4-L7 SERVICE GRAPH	Service Graph: <input type="button" value="select an option"/>
PRIORITY	<input type="button" value="QoS:"/>

OK **CANCEL**

44. From the FILTERS drop-down list click +.
45. In the CREATE FILTER dialog box, enter Allow-All as the Name. In this example, allow all the traffic for this contract.
46. Click + to add a filter.

CREATE FILTER

Specify the Filter Identity

Name:	Allow-All								
Description:	optional								
Entries:	<input style="width: 20px; height: 20px;" type="button" value="+"/>								
<table border="1" style="width: 100%;"> <thead> <tr> <th>Name</th> <th>EtherType</th> <th>ARP Flag</th> <th>IP Protocol</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>		Name	EtherType	ARP Flag	IP Protocol				
Name	EtherType	ARP Flag	IP Protocol						

47. Enter Allow-All as the name of the filter.
48. From the drop-down list, select IP as EtherType.

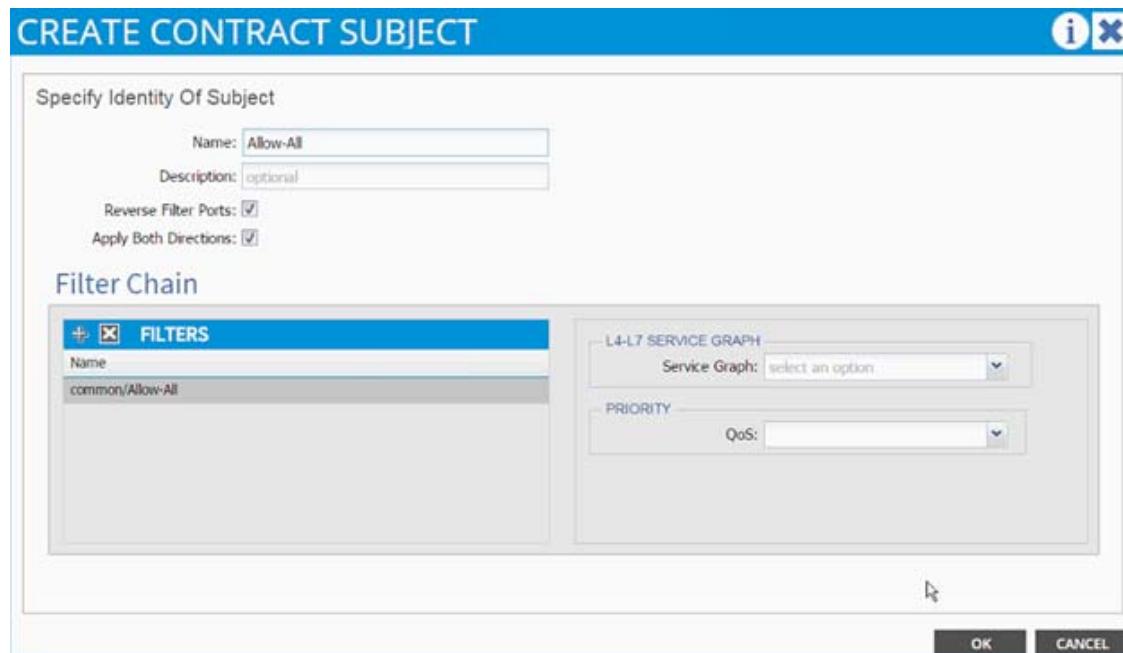
CREATE FILTER

Specify the Filter Identity

Name:	Allow-All																
Description:	optional																
Entries:	<input style="width: 20px; height: 20px;" type="button" value="+"/>																
<table border="1" style="width: 100%;"> <thead> <tr> <th>Name</th> <th>EtherType</th> <th>ARP Flag</th> <th>IP Protocol</th> <th>Allow Fragment</th> <th>Source Port / Range</th> <th>Destination Port / Range</th> <th>TCP Session Rules</th> </tr> </thead> <tbody> <tr> <td>Allow-All</td> <td>IP</td> <td>Unspecified</td> <td>Unspecified</td> <td><input type="checkbox"/></td> <td>From <input type="button" value="Unspecified"/> To <input type="button" value="Unspecified"/></td> <td>From <input type="button" value="Unspecified"/> To <input type="button" value="Unspecified"/></td> <td>Unspecified</td> </tr> </tbody> </table>		Name	EtherType	ARP Flag	IP Protocol	Allow Fragment	Source Port / Range	Destination Port / Range	TCP Session Rules	Allow-All	IP	Unspecified	Unspecified	<input type="checkbox"/>	From <input type="button" value="Unspecified"/> To <input type="button" value="Unspecified"/>	From <input type="button" value="Unspecified"/> To <input type="button" value="Unspecified"/>	Unspecified
Name	EtherType	ARP Flag	IP Protocol	Allow Fragment	Source Port / Range	Destination Port / Range	TCP Session Rules										
Allow-All	IP	Unspecified	Unspecified	<input type="checkbox"/>	From <input type="button" value="Unspecified"/> To <input type="button" value="Unspecified"/>	From <input type="button" value="Unspecified"/> To <input type="button" value="Unspecified"/>	Unspecified										

UPDATE **CANCEL**

49. Click Update.
50. Click SUBMIT to create the filter.
51. Click UPDATE to add the newly created filter to the filter chain.



52. Click OK to finish creating the Contract Subject.

CREATE CONTRACT

Specify Identity Of Contract

Name:	Common-Mgmt
Scope:	global
QoS Class:	Unspecified
Description:	optional

Subjects:

Name	Description
Allow-All	

SUBMIT **CANCEL**

53. Click SUBMIT.
54. Click SUBMIT again to finish adding a provided contract.
55. To validate access to the EPG gateway just added, ping 192.168.3.253 from a common services virtual machine. The virtual machine should be able to ping the address.

Consuming the Common Contract in Application EPGs

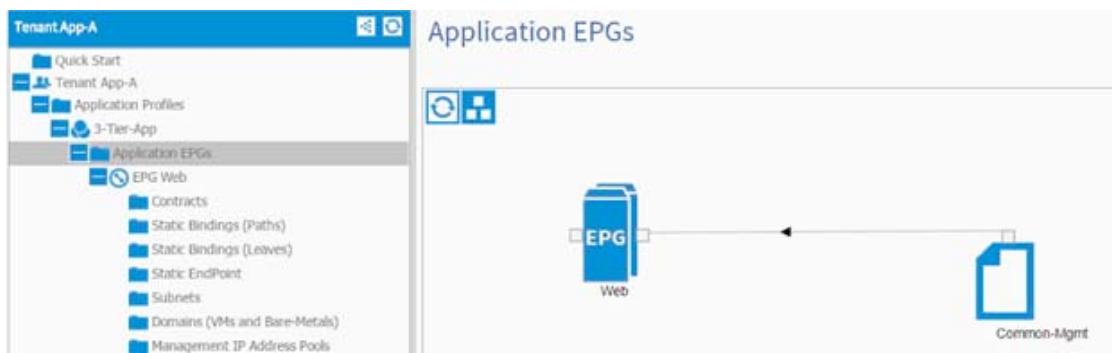
1. Select Tenant and App-A tenant from the top menu.
2. Expand Tenant App-A in the left menu bar.
3. Expand the Application Profiles, 3-Tier-App, Application EPGs, and EPG Web.
4. Click Contracts.
5. Click ACTIONS and select Add Consumed Contract.



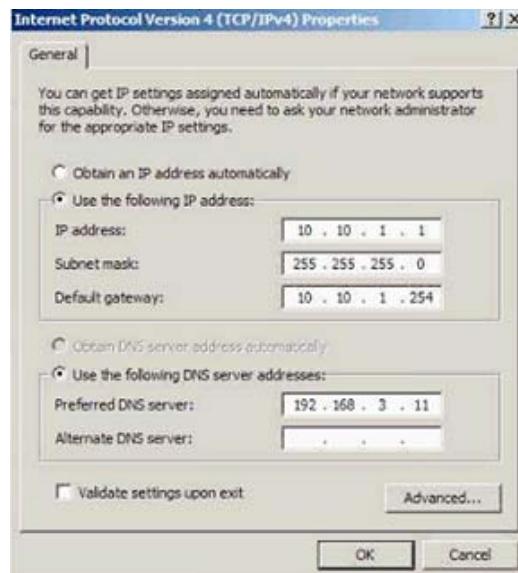
6. In the ADD CONSUMED CONTRACT dialog box, from the drop-down list select Common/Common-Mgmt contract.



7. Click SUBMIT.
8. To validate the contract definition, click Application EPGs under Application Profile NFS in the left menu bar.



9. Repeat these steps for all the application tiers that need access to the common services.
10. For a Web virtual machine with shown Network Parameters, communication to the 192.168.3.0 subnet should be established and ping should work from 10.1.1.1 to 192.168.3.11



**Note**

Make sure the common services virtual machines either use 192.168.3.253 as their default gateway or have a persistent route added for the 10.10.1.0/24 subnet with the gateway set as 192.168.3.253.

Cisco ACI - Accessing SVM Management Interface from Application Virtual Machines (Optional)

When configuring NetApp SnapManager and SnapDrive, access to SVM management LIF is required. This configuration can be enabled on a per tenant (per application) basis. A new application profile called "SVM-Access" is defined under the application tenant (App-A) and an EPG (svm-mgmt) is statically mapped to SVM management LIF VLAN. Access to the "svm-mgmt" from various application tiers (EPGs) is then enabled using contracts. The contracts are provided by the EPG "svm-mgmt" and consumed by the application EPGs such as "Web" and "App" as defined in the previous sections

SVM-Access - Application Profile Creation

In this section, a bridge domain is created and an Application Profile to setup SVM management interface connectivity between the application virtual machines the SVM management LIF. Since all the LIFs sharing the same uplink port-channel share the same MAC address, a unique bridge domain is required for SVM access.

1. Select Tenant and App-A tenant from the top menu.
2. Expand Tenant App-A in the left menu bar.
3. Expand Networking, right-click Bridge Domains and select Create Bridge Domain.
4. Use bd-svm-mgmt as Name of the bridge domain.
5. Select App-A from the drop-down list as the Network.
6. Select Custom from the drop-down list for Forwarding and enable Flood and ARP Flooding.
7. Select default as the IGMP Snoop Policy.

CREATE BRIDGE DOMAIN

Specify Bridge Domain for the Network

Name:

Description: optional

Network:

Forwarding: Custom

L2 Unknown Unicast: Flood Hardware Proxy

Unknown Multicast Flooding: Flood Optimized Flood

ARP Flooding: Enabled

Unicast Routing: Enabled

Config BD MAC Address:

IGMP Snoop Policy:

Associated L3 Outs:

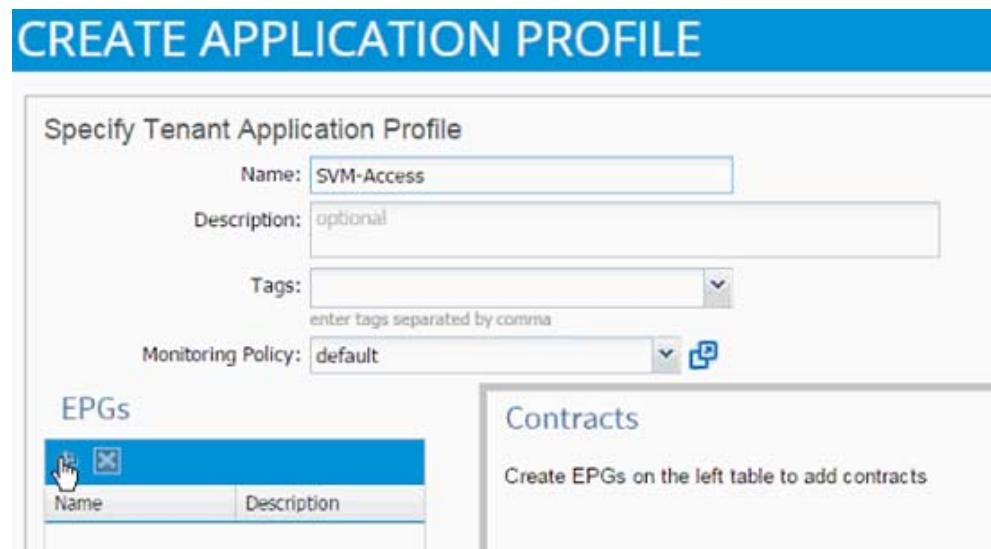
L3 Out for Route Profile:

Route Profile:

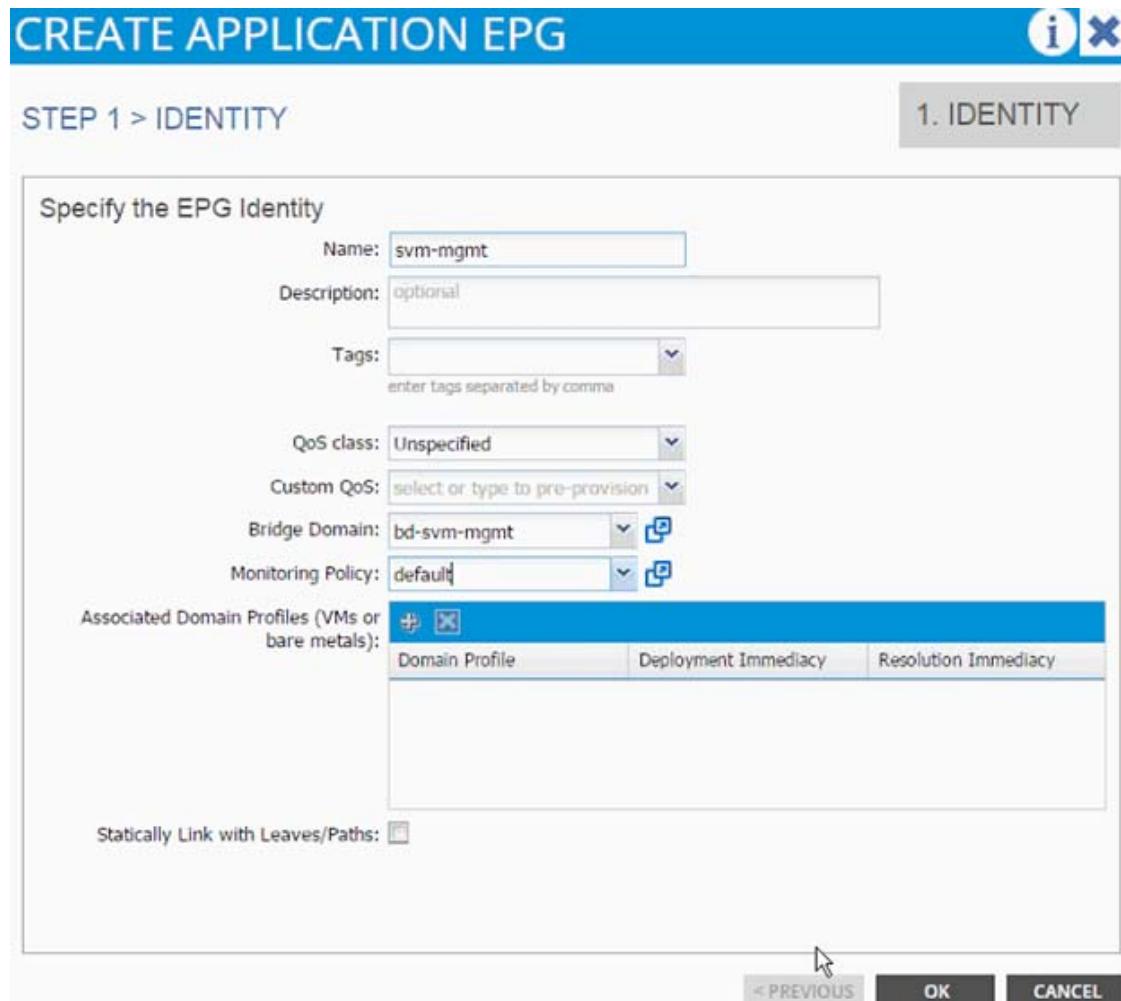
Monitoring Policy:

Subnets:

8. Click SUBMIT.
9. In the menu on the left, right-click Application Profile and click Create Application Profile.
10. In the CREATE APPLICATION PROFILE dialog box, enter SVM-Access as the Name.
11. From the drop-down list, select default for Monitoring Policy.
12. Click + next to EPG to add an EPG.



13. In the CREATE APPLICATION EPG dialog box, enter svm-mgmt as the Name.
14. From the drop-down list, select bd-svm-mgmt as the Bridge Domain.
15. From the drop-down list, select default for Monitoring Policy.



Modifying the Physical Domain

The physical domain associated with NetApp storage needs to be modified and the SVM Management LIF VLAN associated with App-A SVM needs to be added to the physical domain. To do so, complete the following steps:

1. Select Fabric and Access Policies from the top menu.
2. Expand Pools and then VLAN.
3. Click the pool name associated with NetApp controllers (vp-A01-NetApp in this example) and click + to add another Encap Block.
4. Enter a range of 3181 to 3181 for SVM Management LIF VLAN
5. Click SUBMIT.

EPG and Contract Configuration

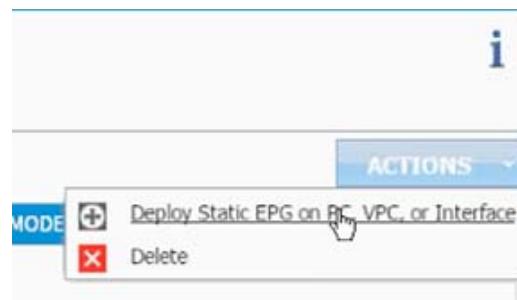
To configure EPG and the contract, complete the following steps:

1. Select Tenant and then App-A from the top menu.

2. Expand the newly created SVM-Access Application profile from the menu bar on the left.
3. Expand SVM-Access, expand Application EPGs and expand EPG svm-mgmt.
4. Click Static Bindings (Paths).



5. Click Actions.
6. Click Deploy Static EPG on PC, vPC, or Interface.



7. In the DEPLOY STATIC EPG ON PC, vPC OR INTERFACE dialog box, select Virtual Port Channel as the Path Type.
8. From the Path drop-down list, select NetApp Controller 1.

DEPLOY STATIC EPG ON PC, VPC, OR I...

Select PC, VPC, or Interface

Path Type: Port
 Direct Port Channel
 Virtual Port Channel

Path:  

Encap:

Deployment Immediacy:

Mode:

topology/pod-1/protpaths-101-102/pathep-[pg-A01-6248-1]
 topology/pod-1/protpaths-101-102/pathep-[pg-A01-6248-2]
 topology/pod-1/protpaths-101-102/pathep-[pg-A02-NAPP-1] 
 topology/pod-1/protpaths-101-102/pathep-[pg-A02-NAPP-2]
 802.1P Tag

SUBMIT **CANCEL**

9. Enter `vlan-<App-A-SVM-MGMT LIF VLAN>` for "Encap; VLAN 3181 is the Mgmt VLAN on NetApp Controller in the screenshot below.
10. Change Deployment Immediacy to Immediate.

DEPLOY STATIC EPG ON PC, VPC, OR I...

Select PC, VPC, or Interface

Path Type: Port
 Direct Port Channel
 Virtual Port Channel

Path:  

Encap:
For example, vlan-1

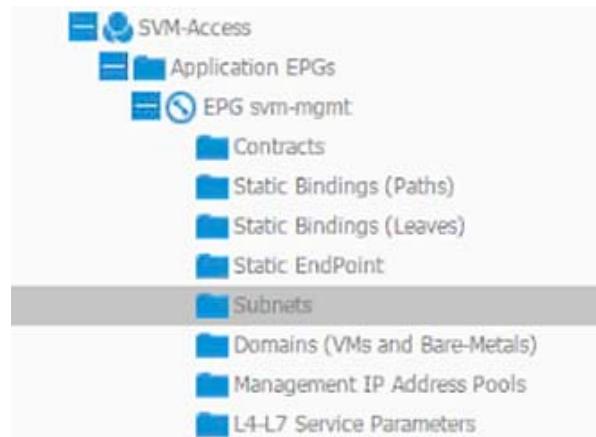
Deployment Immediacy: Immediate
 On Demand

Mode: Tagged
 Untagged
 802.1P Tag

SUBMIT **CANCEL**

11. Click Submit.
12. Repeat these steps for mapping NetApp Controller 2 path.
13. Click Subnet under the EPG svm-mgmt.

14. Click Contracts under the EPG svm-mgmt.



15. Click Actions and select Create EPG Subnet.



16. Enter 192.168.181.254/24 for the Default Gateway IP. This IP address is the gateway that SVM management LIF will use.
 17. Change scope to Private Subnet.

CREATE EPG SUBNET

Specify the Subnet Identity

Default Gateway IP: Address Mask:

Scope: Shared Subnet
 Public Subnet
 Private Subnet

Description:

Subnet Control: Querier IP

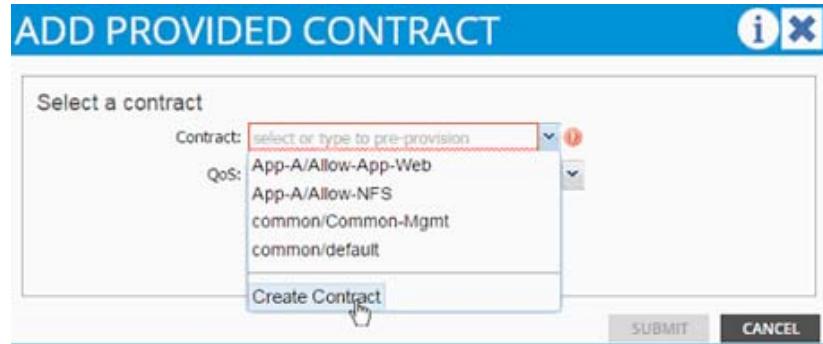
L3 Out for Route Profile:

Route Profile:

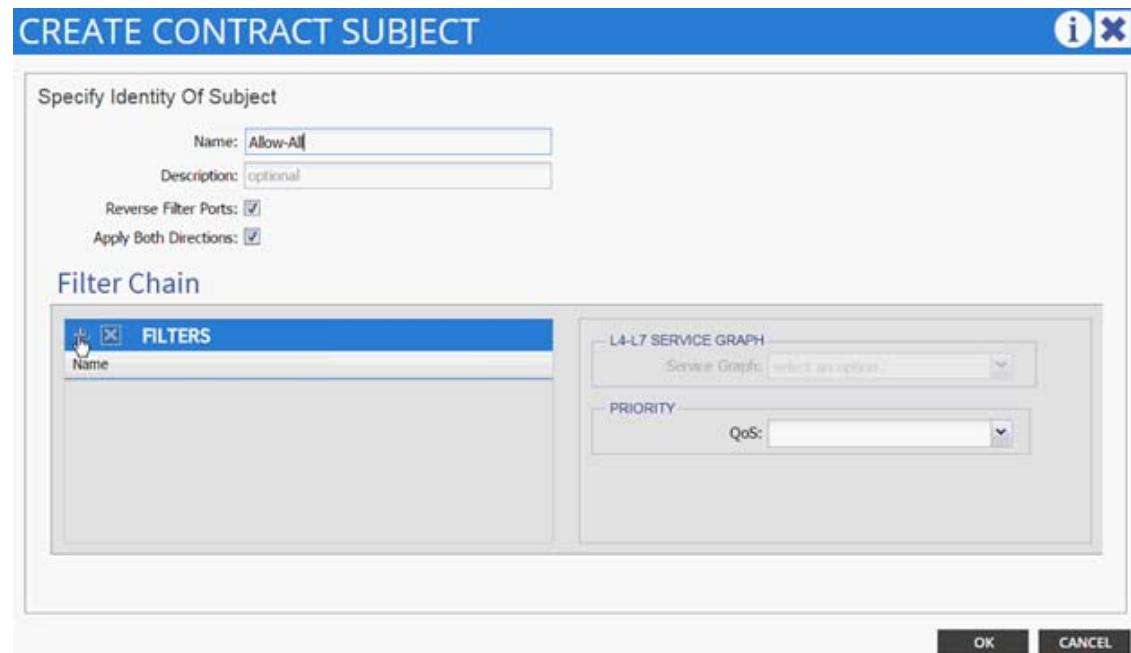
SUBMIT **CANCEL**

18. Click SUBMIT.
 19. Click Action and select Add Provided Contract.

20. From the ADD PROVIDED CONTRACT dialog box, select Create Contract under Contract.



21. Enter Allow-SVM-Acces as Name in the CREATE CONTRACT dialog box.
22. Click + next to Subjects to add a new contract subject.
23. In the CREATE CONTRACT SUBJECT dialog box, enter Allow-All as the Name.
24. Click + under Filter Chain to add a new filter.



25. From the FILTERS drop-down list select the Allow-All filter under Tenant App-A.

NAME	TENANT
Tenant: App-A	
Allow-All	App-A
Tenant: common	
Allow-All	common
arp	common
default	common
est	common
icmp	common

26. Click UPDATE to add the newly created filter to the filter chain.
27. Click OK to finish creating the Contract Subject.
28. Click SUBMIT.
29. Click SUBMIT again to finish adding a provided contract.

Consuming the SVM Management Contract in an Application Tier (Web)

To consume the SVM management contract, complete the following steps:

1. Expand Application Profile 3-Tier-App.
2. Expand Application EPGs.
3. Expand EPG Web.
4. Click Contracts.
5. Click ACTIONS and select Add Consumed Contract.
6. In the ADD CONSUMED CONTRACT dialog box, from the drop-down menu select App-A/Allow-SVM-Access contract (previously defined).
7. Click SUBMIT.

Cisco ACI - Connectivity to Existing Infrastructure

This section provides the detailed procedure for a tenant (App-A) to existing CiscoNexus 7000 core routers using sub-interfaces and VRF aware OSPF. The following are some of the highlights of this connectivity:

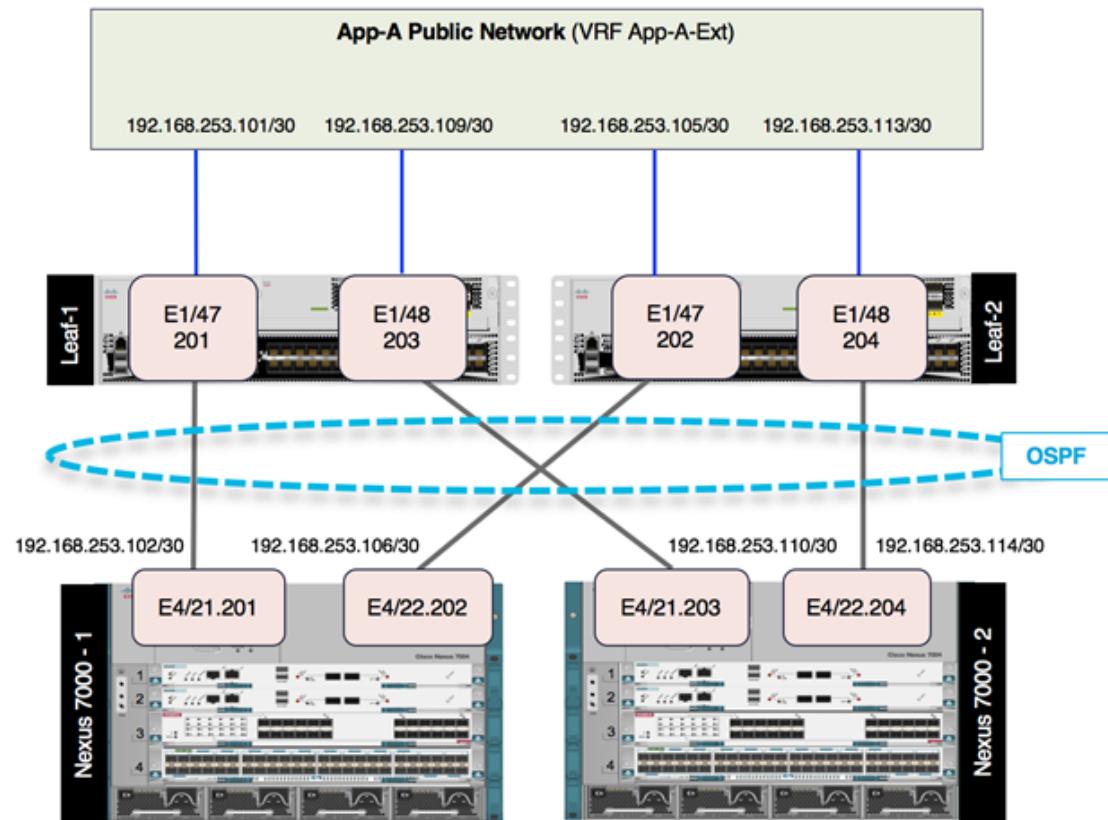
- A new bridge domain and associated private network is configured in ACI for external connectivity
- The Web VM is configured with two interfaces - one to connect to an EPG attached to inside bridge domain (bd-internal) and another to connect to an EPG on the external bridge domain (bd-external)
- Each of the two Cisco Nexus 7000s is connected to each of Cisco Nexus 9000 leaf
- Sub-interfaces are configured and used for external connectivity

- Cisco Nexus 9000 is configured to run per-VRF OSPF - Cisco Nexus 7000 does not use VRFs
- Cisco Nexus 7000 is configured to originate and send a default route to Cisco Nexus 9000 leaves

Figure 6 illustrates the VLANs and networks used for this connectivity.

When using service graphs (load balancer), the Web VM does not need two separate interfaces

Figure 6 *ACI - Layer-3 Connectivity Details*



Configuring the Cisco Nexus 7000 for ACI connectivity (Sample)

```
Cisco Nexus 7000-1

feature ospf
!
router ospf 10
  router-id 192.168.254.3
  area 0.0.0.10 nssa no-summary default-information-originate
no-redistribution
!
interface Vlan100
  no shutdown
  mtu 9216
  no ip redirects
  ip address 192.168.253.253/30
  no ipv6 redirects
```

```

        ip ospf mtu-ignore
        ip router ospf 10 area 0.0.0.0
    !
    interface Ethernet4/21.201
        encapsulation dot1q 201
        ip address 192.168.253.102/30
        ip ospf mtu-ignore
        ip router ospf 10 area 0.0.0.10
        no shutdown
    !
    interface Ethernet4/22.202
        encapsulation dot1q 202
        ip address 192.168.253.106/30
        ip ospf cost 5
        ip ospf mtu-ignore
        ip router ospf 10 area 0.0.0.10
        no shutdown
    !
Cisco Nexus 7000-2

feature ospf
!
router ospf 10
    router-id 192.168.254.4
    area 0.0.0.10 nssa no-summary default-information-originate
no-redistribution
!
interface Vlan100
    no shutdown
    mtu 9216
    no ip redirects
    ip address 192.168.253.254/30
    no ipv6 redirects
    ip ospf mtu-ignore
    ip router ospf 10 area 0.0.0.0
!
interface Ethernet4/21.203
    encapsulation dot1q 203
    ip address 192.168.253.110/30
    ip ospf cost 20
    ip ospf mtu-ignore
    ip router ospf 10 area 0.0.0.10
    no shutdown
!
interface Ethernet4/22.204
    encapsulation dot1q 204
    ip address 192.168.253.114/30
    ip ospf cost 30
    ip ospf mtu-ignore
    ip router ospf 10 area 0.0.0.10
    no shutdown
!
```

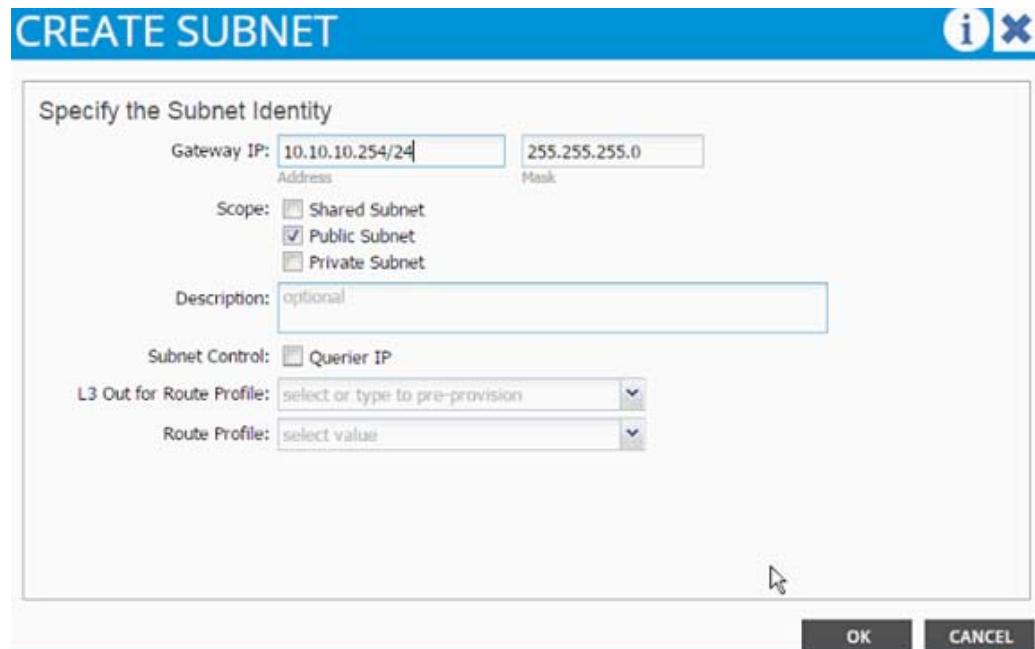
Configuring ACI for External Routed Domain

To configure ACI for an external routed domain, complete the following steps:

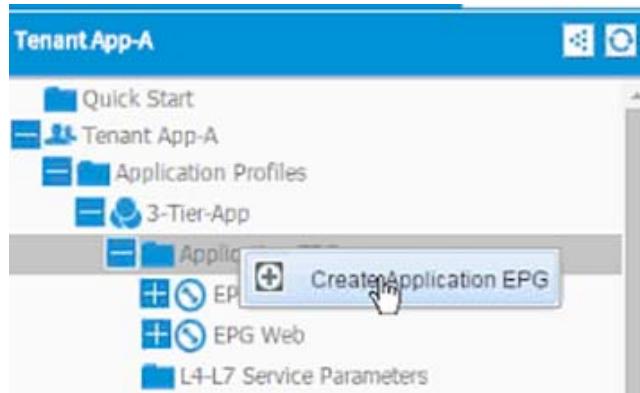
1. Select Tenant and App-A tenant from the top menu.
2. Expand Tenant App-A in the left menu bar.
3. Expand Networking, right-click Bridge Domains and select Create Bridge Domain.
4. Use bd-external as Name of the bridge domain.
5. From the Network drop-down list, select Create Private Network.
6. In the CREATE PRIVATE NETWORK dialog box, enter App-A-Ext for the Name.

The screenshot shows the 'CREATE PRIVATE NETWORK' dialog box. The 'Name' field is filled with 'App-A-Ext'. The 'Policy enforcement' section has two radio buttons: 'Enforced' (selected) and 'Unenforced'. The 'Description' field contains the word 'optional'. Below these are three dropdown menus labeled 'BGP Timers', 'OSPF Timers', and 'Monitoring Policy', each with the placeholder text 'select or type to pre-provision'. At the bottom of the dialog are two buttons: 'SUBMIT' and 'CANCEL'.

7. Click SUBMIT.
8. Select default as the IGMP Snoop Policy.
9. Click + next to Subnets to add a subnet.
10. Provide the gateway address of the subnet which will communicate to the external world.
11. Set Scope as Public.



12. Click OK.
13. Click SUBMIT.
14. Expand the Application Profile 3-Tier-App on the left and right-click Application EPGs and click Create Application EPG.



15. In the CREATE APPLICATION EPG dialog box, enter External as the Name.
16. From the drop-down list, select bd-External as the Bridge Domain.
17. From the drop-down list, select default for Monitoring Policy.
18. Click OK.
19. Click + next to Associated Domain Profiles (VMs or Bare metals).
20. From the drop-down list, select the VMM domain previously defined.
21. Select Immediate for Deployment Immediacy.
22. Select Immediate for Resolution Immediacy.

CREATE APPLICATION EPG

STEP 1 > IDENTITY

1. IDENTITY

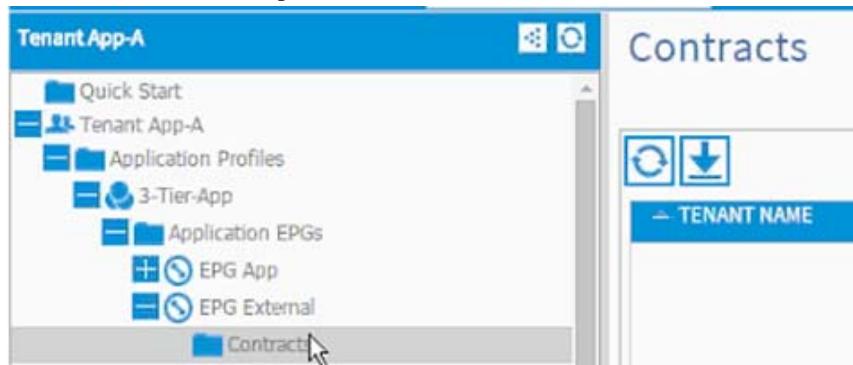
Specify the EPG Identity

Name:	External								
Description:	optional								
Tags:	enter tags separated by comma								
QoS class:	Unspecified								
Custom QoS:	select or type to pre-provision								
Bridge Domain:	bd-External								
Monitoring Policy:	select or type to pre-provision								
Associated Domain Profiles (VMs or bare metals):	<table border="1"> <tr> <td>+</td> <td>X</td> </tr> <tr> <td>Domain Profile</td> <td>Deployment Immediacy</td> <td>Resolution Immediacy</td> </tr> <tr> <td>VMM Domain - A01-VC</td> <td>Immediate</td> <td>Immediate</td> </tr> </table>	+	X	Domain Profile	Deployment Immediacy	Resolution Immediacy	VMM Domain - A01-VC	Immediate	Immediate
+	X								
Domain Profile	Deployment Immediacy	Resolution Immediacy							
VMM Domain - A01-VC	Immediate	Immediate							
Statically Link with Leaves/Paths: <input type="checkbox"/>									

< PREVIOUS **FINISH** **CANCEL**

23. Click Finish.

24. From the left list, expand the EPG External and click Contracts.



25. Click Action and select Add Provided Contract.

26. From the ADD PROVIDED CONTRACT dialog box, select Create Contract under Contract.

ADD PROVIDED CONTRACT

Select a contract

Contract: !

QoS:

- App-A/Allow-App-Web
- App-A/Allow-NFS
- common/Common-Mgmt
- common/default

Create Contract

SUBMIT **CANCEL**

27. Enter Allow-External as Name in the CREATE CONTRACT dialog box.
28. Change the Scope to Tenant.
29. Click + next to Subjects to add a new contract subject.
30. In the CREATE CONTRACT SUBJECT dialog box, enter Allow-All as the Name.
31. Click + under Filter Chain to add a new filter.

CREATE CONTRACT SUBJECT

Specify Identity Of Subject

Name:

Description:

Reverse Filter Ports:

Apply Both Directions:

Filter Chain

FILTERS

Allow-All

L4-L7 SERVICE GRAPH

Service Graph:

PRIORITY

QoS:

OK **CANCEL**

32. From the FILTERS drop-down list select Allow-All filter under Tenant App-A.

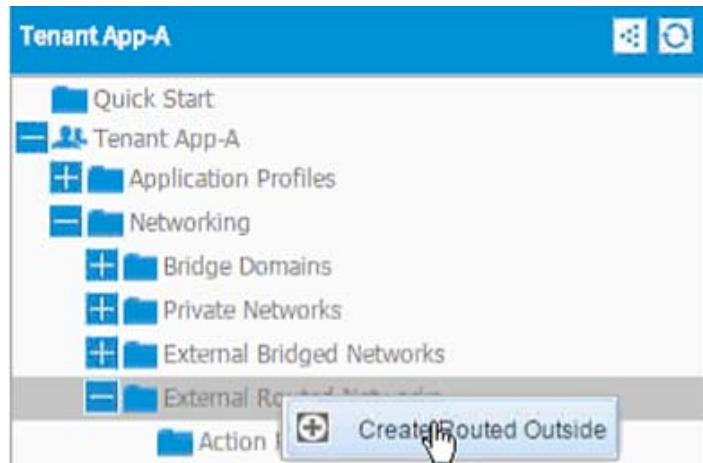
NAME	TENANT
 Tenant: App-A	
Allow-All	App-A
 Tenant: common	
Allow-All	common
arp	common
default	common
est	common
icmp	common

33. Click UPDATE to add the newly created filter to the filter chain.
34. Click OK to finish creating the Contract Subject.
35. Click SUBMIT.
36. Click SUBMIT again to finish adding a provided contract.

Adding External Routed Domain

To add external routed domains, complete the following steps:

1. Select Tenants and App-A from the top menu.
2. Expand Tenant App-A in the left menu.
3. Expand Networking and External Routed Networks.
4. Right-click External Routed Networks and select Create Routed Outside.



5. In the CREATE ROUTED OUTSIDE dialog box, enter App-A-L3-Out as the Name.
6. Click the check mark next to OSPF.
7. Enter 0.0.0.10 as the OSPF Area ID.

8. Select App-A-Ext from the drop-down list as the Private Network.
9. Click + next to Nodes and Interfaces Protocol Profiles.

CREATE ROUTED OUTSIDE

STEP 1 > IDENTITY 1. IDENTITY 2. EXTERNAL EPG NETWORKS

Define the Routed Outside

Name:	App-A-L3-Out	BGP	<input checked="" type="checkbox"/> OSPF
Description:	optional	OSPF Area ID: 0.0.0.10	
Tags:	enter tags separated by comma		
Private Network:	App-A-Ext	<input type="button" value=""/>	
External Routed Domain:	select an option		

NODES AND INTERFACES PROTOCOL PROFILES

+ <input type="button" value=""/>	Name	Description	DSCP	Nodes
-----------------------------------	------	-------------	------	-------

10. In the CREATE NODE PROFILE dialog box, enter Node_101 as the Name.
11. Click + to add Nodes.

CREATE NODE PROFILE

Specify the Node Profile

Name:	Node_101			
Description:	optional			
DSCP:	<input type="button" value=""/>			
Nodes:	<input type="button" value="+"/> <input type="button" value="X"/> <table border="1"> <tr> <td>Node ID</td> <td>Router ID</td> <td>Static Routes</td> </tr> </table>	Node ID	Router ID	Static Routes
Node ID	Router ID	Static Routes		

12. In the SELECT NODE dialog box, select the first Cisco Nexus 9000 switch (Node-101).

SELECT NODE

Select Node and Configure Static Routes

Node ID:

Router ID:

Static Routes



IP Address

A01-9396-1 (Node-101)

A01-9396-2 (Node-102)

- Provide a loopback address to be used for the tenant private network.

SELECT NODE



Select Node and Configure Static Routes

Node ID:

Router ID:

Static Routes



IP Address

Next Hop IP

- Click OK.
- Click + to add OSPF Interface Profile.

CREATE NODE PROFILE

Specify the Node Profile

Name:	Node_101
Description:	optional

DSCP:

Nodes:

Node ID	Router ID	Static Routes
topology/pod-1/node-101	192.168.254.101	

OSPF INTERFACE PROFILES

Name	Description	Interfaces
New		

16. In the CREATE INTERFACE PROFILE dialog box, use a descriptive name; Node101_Int_Profile in this example provides information about interface policy for Node 101.
17. From the OSPF Policy drop-down list list select Create OSPF Interface Policy.
18. In the CREATE OSPF INTERFACE POLICY dialog box, provide a descriptive name.
19. Check MTU ignore and Advertise Subnet.

CREATE OSPF INTERFACE POLICY

Define OSPF Interface Policy

Name:	To-7K
Description:	optional
Network Type:	<input type="radio"/> Broadcast <input checked="" type="radio"/> Unspecified <input type="radio"/> Point-to-point
Priority:	1
Cost of Interface:	
Interface Controls:	<input checked="" type="checkbox"/> MTU Ignore <input type="checkbox"/> Passive Participation <input checked="" type="checkbox"/> Advertise Subnet
Hello Interval (sec):	10
Dead Interval (sec):	40
Retransmit Interval (sec):	5
Transmit Delay (sec):	1

SUBMIT **CANCEL**

20. Click SUBMIT.
21. Under INTERFACES, select ROUTED SUB-INTERFACE and click + to add a new sub-interface.

INTERFACES					
<input checked="" type="checkbox"/> ROUTED SUB-INTERFACES ROUTED INTERFACES SVI ROUTED SUB-INTERFACE					
Path	Encap	IP Address	MAC Address	MTU (bytes)	Target DSCP

22. In the SELECT ROUTED SUB-INTERFACE dialog box, select the Cisco Nexus 9000-1 interface connected to Nexus 7000-1 (Eth 1/47).
23. In the Encap enter vlan-201.
24. Provide the IP address 192.168.253.101/30.
25. Set MTU to 1500.

SELECT ROUTED SUB-INTERFACE

Specify the Interface

Path:	topology/pod-1/paths-101/pathep-[eth1/47]	▼
Encap:	vlan-201	For example, vlan-1
IP Address:	192.168.253.101/30	255.255.255.252 Mask
MAC Address:	00:22:BD:F8:19:FF	
MTU (bytes):	1500	
Target DSCP:	▲ ▼	

OK **CANCEL**

26. Click OK.
27. Repeat steps 21-25 to add a second interface profile with appropriate sub-interfaces. The OSPF Policy created in steps 18-20 can be re-used (select from the drop-down list) for the interface profiles.

ROUTED SUB-INTERFACES					
Path	Encap	IP Address	MAC Address	MTU (bytes)	Target DSCP
Node-101/eth1/47	vlan-201	192.168.253.101/30	00:22:BD:F8:19:FF	1500	Unspecified
Node-101/eth1/48	vlan-203	192.168.253.109/30	00:22:BD:F8:19:FF	1500	Unspecified

28. Click OK.
29. Click + next to Nodes and Interfaces Protocol Profiles.

CREATE ROUTED OUTSIDE

STEP 1 > IDENTITY 1. IDENTITY 2. EXTERNAL EPG NETWORKS

Define the Routed Outside

Name: <input type="text" value="App-A-L3-Out"/>	<input type="checkbox"/> BGP	<input checked="" type="checkbox"/> OSPF
Description: <input type="text" value="optional"/>	OSPF Area ID: <input type="text" value="0.0.0.10"/>	
Tags: <input type="text" value=""/>	enter tags separated by comma	
Private Network: <input type="text" value="App-A-Ext"/>	<input type="button" value=""/>	
External Routed Domain: <input type="text" value="select an option"/>	<input type="button" value=""/>	

NODES AND INTERFACES PROTOCOL PROFILES

<input type="button" value="+"/>	<input type="button" value="X"/>	Name	Description	DSCP	Nodes
----------------------------------	----------------------------------	------	-------------	------	-------

30. In the CREATE NODE PROFILE dialog box, enter Node_102 as the Name.
31. Click + to add Nodes.

CREATE NODE PROFILE

Specify the Node Profile

Name: <input type="text" value="Node_102"/>			
Description: <input type="text" value="optional"/>			
DSCP: <input type="text" value=""/>			
Nodes:			
<input type="button" value="+"/> <input type="button" value="X"/>	Node ID	Router ID	Static Routes

32. In the SELECT NODE dialog box, select second Cisco Nexus 9000 switch (Node-102).

SELECT NODE

Select Node and Configure Static Routes

Node ID: <input type="text" value="select a node"/>	<input type="button" value=""/>
Router ID: <input type="text" value=""/>	<input type="button" value=""/>
Static Routes	
<input type="button" value="+"/> <input type="button" value="X"/>	IP Address

A01-9396-1 (Node-101)
A01-9396-2 (Node-102)

33. Provide a loopback address to be used for the tenant private network.



34. Click OK.
35. Click + to add OSPF INTERFACE PROFILE.
36. In the CREATE INTERFACE PROFILE dialog box, use a descriptive name; Node102_Int_Profile in this example provides information about interface policy for Node 101.
37. From the OSPF Policy drop-down list select the previously created OSPF policy.
38. Click SUBMIT.
39. Under INTERFACES, select ROUTED SUB-INTERFACE and click + to add a new sub-interface.



40. In the SELECT ROUTED SUB-INTERFACE dialog box, select the Cisco Nexus 9000-2 interface connected to Cisco Nexus 7000-1 (Eth 1/47).
41. In the Encap enter vlan-202.
42. Provide the IP address.
43. Set MTU to 1500.
44. Click OK.
45. Repeat these steps to add second interface profiles with appropriate sub-interfaces.
46. Click OK.

CREATE ROUTED OUTSIDE

STEP 1 > IDENTITY 1. IDENTITY 2. EXTERNAL EPG NETWORKS

Define the Routed Outside

Name:	App-A-L3-Out	BGP	<input checked="" type="checkbox"/> OSPF
Description:	optional	OSPF Area ID: 0.0.0.10	
Tags:	enter tags separated by comma		
Private Network:	App-A-Ext	<input type="button" value=""/>	
External Routed Domain:	select an option	<input type="button" value=""/>	

NODES AND INTERFACES PROTOCOL PROFILES

Name	Description	DSCP	Nodes
Node_102		Unspecified	topology/pod-1/node-102
Node_101		Unspecified	topology/pod-1/node-101

< PREVIOUS NEXT > CANCEL

47. Click Next.
48. Click + to add EXTERNAL EPG NETWORKS.

STEP 2 > EXTERNAL EPG NETWORKS 1. IDENTITY 2. EXTERNAL EPG NETWORKS

Configure External EPG Networks

Create Route Profiles:

EXTERNAL EPG NETWORKS

Name	QoS Class	Description	Subnet
------	-----------	-------------	--------

49. In the CREATE EXTERNAL NETWORK dialog box, enter Ext-Default as the Name.
50. Click + next to SUBNET to add remote subnet that will be accessed from the ACI fabric

CREATE EXTERNAL NETWORK

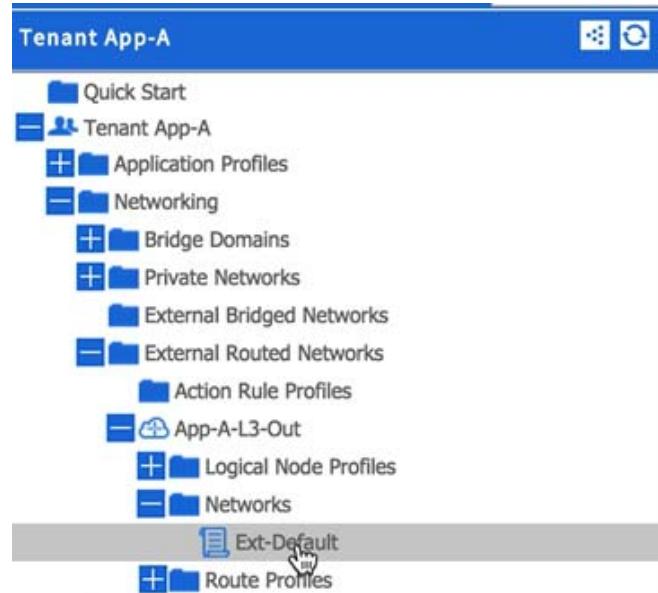
Define an External Network

Name:	Ext-Default
Tags:	<input type="text"/>
enter tags separated by comma	
QoS class:	Unspecified
Description:	optional

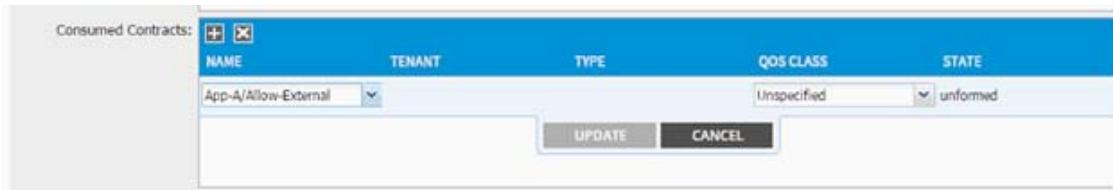
SUBNET

Address	Mask

51. In the CREATE SUBNET dialog box, enter 0.0.0.0/0 as the remote subnet to be accessed.
52. Click OK.
53. Click OK.
54. Click Finish.
55. Expand the App-A-L3-Out routed network and click the newly created network Ext-Default.



56. Click + next to Consumed Contracts.
57. From the drop-down list, select App-A/Allow-External contract.



58. Click UPDATE.
59. Click SUBMIT.
60. Expand Bridge Domains.
61. Click bd-External and click + next to Associated L3 Outs.
62. From the drop-down list, select the newly created routed domain App-A/App-A-L3-Out.

ALL TENANTS | ADD TENANT | Search: enter name
common | App-A | Foundation | Infra | mgmt

SYSTEM
TENANTS
FABRIC
VM NETWORKING
L4-L7 SERVICES
ADMIN

Quick Start
+
Tenant App-A
+
Application Profiles
+
Networking
+
Bridge Domains
+
bd-App-A-Internal
+
DHCP Relay Labels
+
L4-L7 Service Parameters
+
Subnets
+
bd-External
+
bd-Iscsi-a
+
bd-Iscsi-b
+
bd-svm-mgmt
+
Private Networks
+
External Bridged Networks
+
External Routed Networks
+
Action Rule Profiles
+
App-A-L3-Out
+
Logical Node Profiles
+
Networks
+
Ext-Default
+
Route Profiles
+
Protocol Policies
+
Security Policies

Bridge Domain - bd-External

100

PROPERTIES

Network: App-A-Ext

Custom MAC Address: 00:22:BD:F8:19:FF

L2 Unknown Unicast: Flood
 Hardware Proxy

Unknown Multicast Flooding: Flood
 Optimized Flood

ARP Flooding:
Unicast Routing:

IGMP Snoop Policy: default

End Point Retention Policy: default

Associated L3 Outs:

— L3 OUT

select or type to pre-provision

App-A/App-A-L3-Out

common/default

63. Click UPDATE.
64. Click SUBMIT.

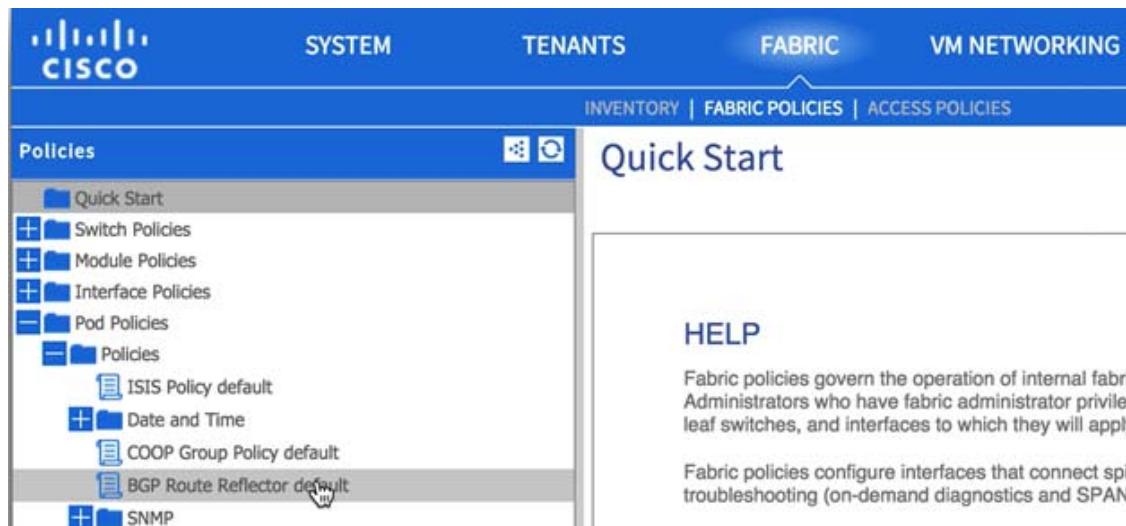
At this time, the network, 10.10.10.0/24, marked public under bridge domain "bd-External" should be seen in the Cisco Nexus 7000 routing table and Cisco Nexus 9000 should be learning the OSPF routes including default route from Cisco Nexus 7000. The provider and consumed contracts should enable communication from a virtual machine connected to "External" EPG (port-group) and any subnet on the external network.

Configuring Multi-Protocol BGP on Spines

Within the ACI fabric, Multiprotocol BGP (MP-BGP) is implemented between leaf and spine switches to propagate external routes within the ACI fabric. The BGP route reflector technology is deployed in order to support a large number of leaf switches within a single fabric. All of the leaf and spine switches are in one single BGP autonomous system (AS). When the border leaf learns the external routes, it can then redistribute the external routes of a given VRF to an MP-BGP address family VPN version 4 (or VPN version 6 when IPv6 routing is supported in ACI). With address family VPN version 4, MP-BGP maintains a separate BGP routing table for each VRF. Within MP-BGP, the border leaf advertises routes to a spine switch, which is a BGP route reflector.

MP-BGP is not enabled by default in the ACI fabric. For the deployment scenario where ACI fabric is used as L2 fabric or there is no need for L3 outside connection, MP-BGP is not required. To enable MP-BGP, configure BGP policy on the APIC to specify the BGP ASN and specify spine nodes as BGP route reflectors.

1. Select Fabric and Fabric Policies from the top menu.
2. Expand Pod Policies and Policies in the left menu bar.
3. Click BGP Route Reflector default.



4. Enter an Autonomous System Number (100 in this example).
5. Click + to select spines (one after the other) as Route Reflector Nodes.

The screenshot shows two main windows from the Cisco ACI interface:

- Left Window (Policies View):** A sidebar menu under the "Policies" tab. The "BGP Route Reflector default" policy is selected and highlighted in grey.
- Right Window (Properties View):** A detailed view of the selected policy. It includes fields for Name (default), Description (optional), Autonomous System Number (100), and Route Reflector Nodes (NODE ID).

Bottom Window (Create Route Reflector Node Policy EP):

Header: CREATE ROUTE REFLECTOR NODE POLICY EP i x

Form Fields:

- Spine Node: 1
- Description: 201

Buttons: SUBMIT CANCEL

6. Click SUBMIT.
7. Right-click Policy Groups and select Create POD Policy Group.



8. Enter a descriptive name for Pod1 policy.
9. From the drop-down list BGP Route Reflector Policy, select default.

**Note**

The policy group allows users to combine multiple policies, such as BGP policy, Integrated System to Integrated System (IS-IS) routing protocol policy, co-operative (COOP) policy, and others, to a policy group and apply it to the POD. In this example, the policy is being utilized to only make changes to BGP.

CREATE POD POLICY GROUP

Specify the Policy Group Properties

Name:	pod1_policygrp
Description:	Enable BGP Route Reflector
Date Time Policy:	select or type to pre-provision
ISIS Policy:	select or type to pre-provision
COOP Group Policy:	select or type to pre-provision
BGP Route Reflector Policy:	default <input checked="" type="button"/>
Communication Policy:	select or type to pre-provision
SNMP Policy:	select or type to pre-provision

SUBMIT CANCEL

10. Click SUBMIT.
11. Click default from Policy Groups.
12. From the drop-down list Fabric Policy Group, select the recently created Pod policy (pod1_policygrp in this example).

The screenshot shows the Cisco ACI Policy Selector interface. The top navigation bar includes links for SYSTEM, TENANTS, FABRIC, VM NETWORKING, L4-L7 SERVICES, and ADMIN. The FABRIC tab is selected. Below the navigation is a sub-navigation bar with INVENTORY, FABRIC POLICIES (which is selected), and ACCESS POLICIES. On the left, a sidebar titled 'Policies' lists categories like Quick Start, Switch Policies, Module Policies, Interface Policies, Pod Policies, Policies, and Global Policies. Under Pod Policies, 'Pod Selector - default' is expanded, showing sub-options for ISIS Policy default, Date and Time, COOP Group Policy default, BGP Route Reflector default, SNMP, Communication, Policy Groups, and a newly created entry 'pod1_policygrp'. The main panel displays the 'Pod Selector - default' properties. The 'Name' field is set to 'default' and the 'Description' field is 'optional'. The 'Type' is set to 'ALL'. In the 'Fabric Policy Group' dropdown, 'pod1_policygrp' is selected. A button labeled 'Create POD Policy Group' is visible at the bottom of the dropdown menu.

13. Click Submit.

FlexPod Management Tool Setup

NetApp Virtual Storage Console (VSC) 5.0 Deployment Procedure

This section describes the deployment procedures for the NetApp Virtual Storage Console (VSC).

VSC 5.0 Preinstallation Considerations

The following licenses are required for VSC on storage systems that run clustered Data ONTAP 8.2.3:

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

Install VSC 5.0

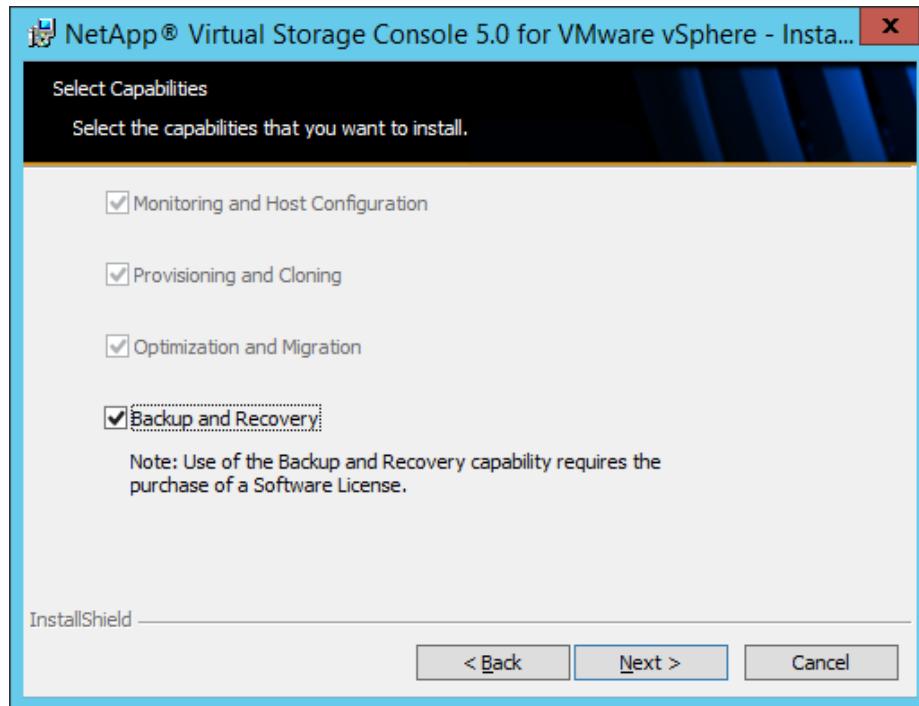
To install the VSC 5.0 software, complete the following steps:

1. Build a VSC virtual machine with Windows Server 2012 R2, 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.
2. Bring up the VM, install VMware Tools, assign IP addresses, and join the machine to the Active Directory domain.
3. Activate Adobe Flash Player in Windows Server 2012 R2 by installing Desktop Experience under the User Interfaces and Infrastructure Feature on the VM.
4. Install all Windows updates on the VM.
5. Log in to the VSC VM as FlexPod admin user.
6. Download the x64 version of the [Virtual Storage Console 5.0](#) from the NetApp Support site.
7. From the VMware Console, right-click the file downloaded in step 3 and select Run As Administrator.
8. On the Installation wizard Welcome page, click Next.
9. Select the checkbox to accept the message, click Next.
10. Select the backup and recovery capability. Click Next.

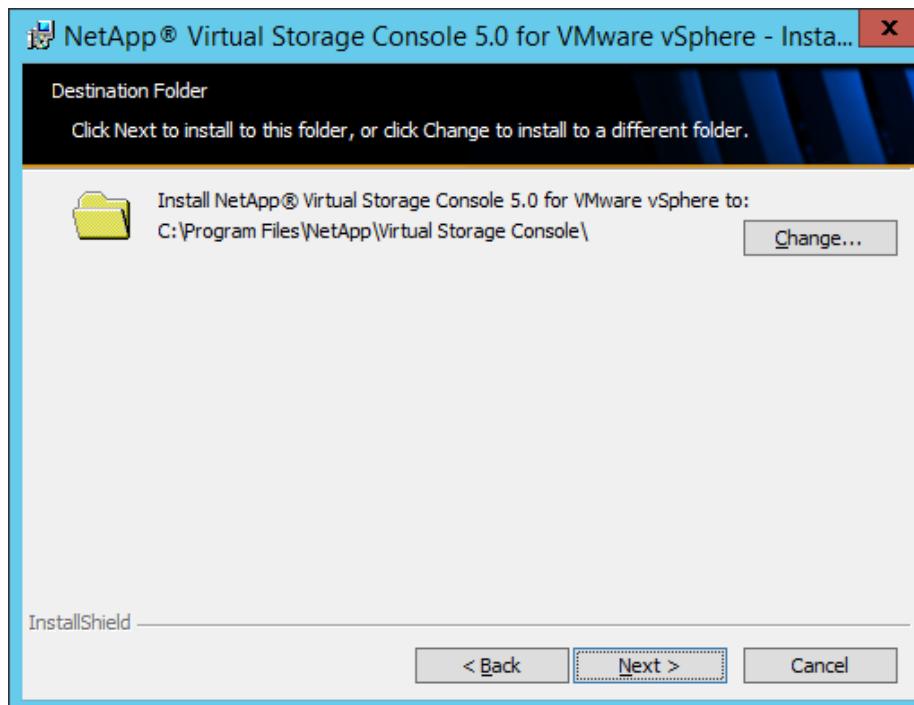


Note

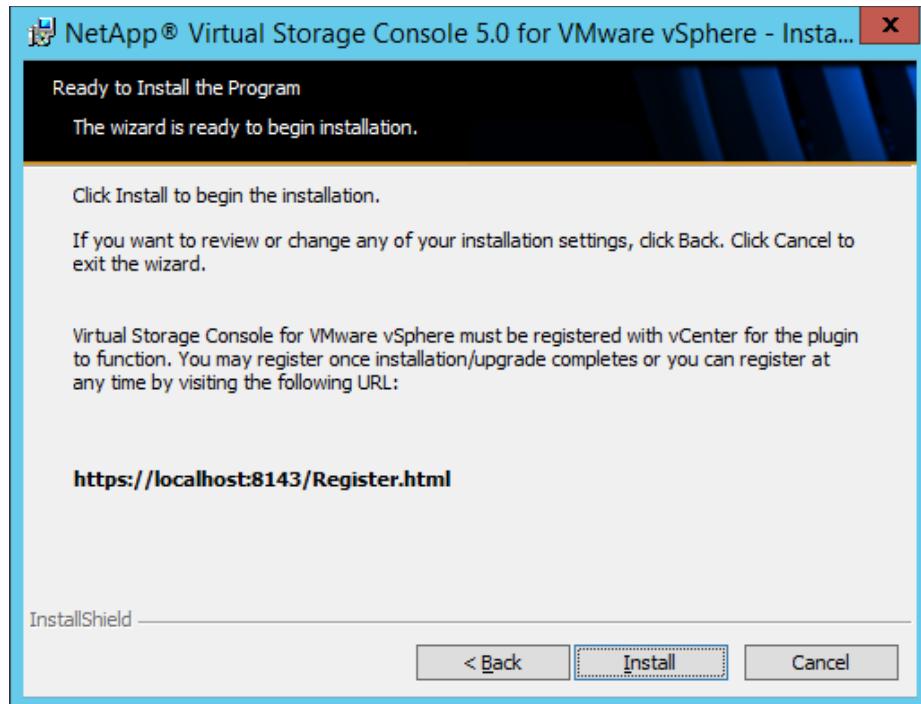
The backup and recovery capability requires an additional license.



11. Click Next to accept the default installation location.



12. Click Install.



13. Click Finish.



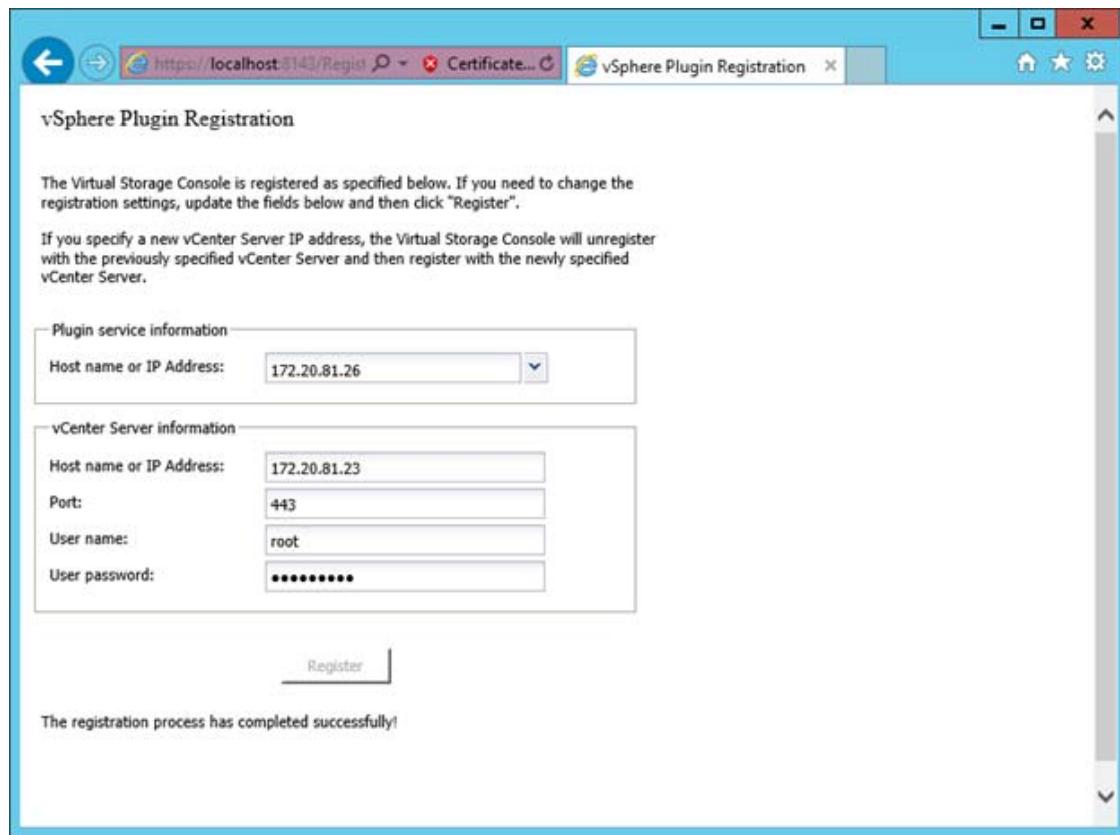
Note If the installation fails giving out an error Incorrect function or VSC service not started, run the following command from the command prompt and start the Virtual Storage Console service manually.

```
"C:\Program Files\NetApp\Virtual Storage Console\bin\vsc" ssl setup  
-generate-passwords
```

Register VSC with vCenter Server

To register the VSC with the vCenter Server, complete the following steps:

1. A browser window with the registration URL opens automatically when the installation phase is complete. If the URL does not open automatically, open <https://localhost:8143/Register.html> in Internet Explorer.
2. Click Continue to this website (not recommended).
3. In the Plug-in Service Information section, select 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 or root), and user password for the vCenter Server. Click Register to complete the registration.



- Upon successful registration, the storage controllers are discovered automatically.

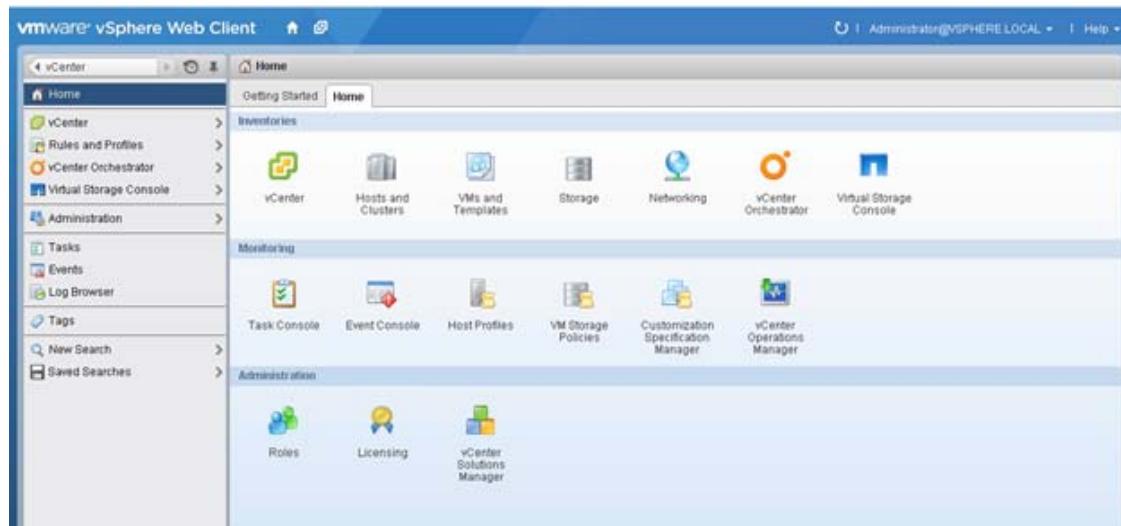


Note Storage discovery process will take some time.

Discover and Add Storage Resources

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

- Using the vSphere web client, log in to the vCenter Server as FlexPod admin user or root. If the vSphere web client was previously opened, close it and then reopen it.
- In the Home screen, click the Home tab and click Virtual Storage Console.

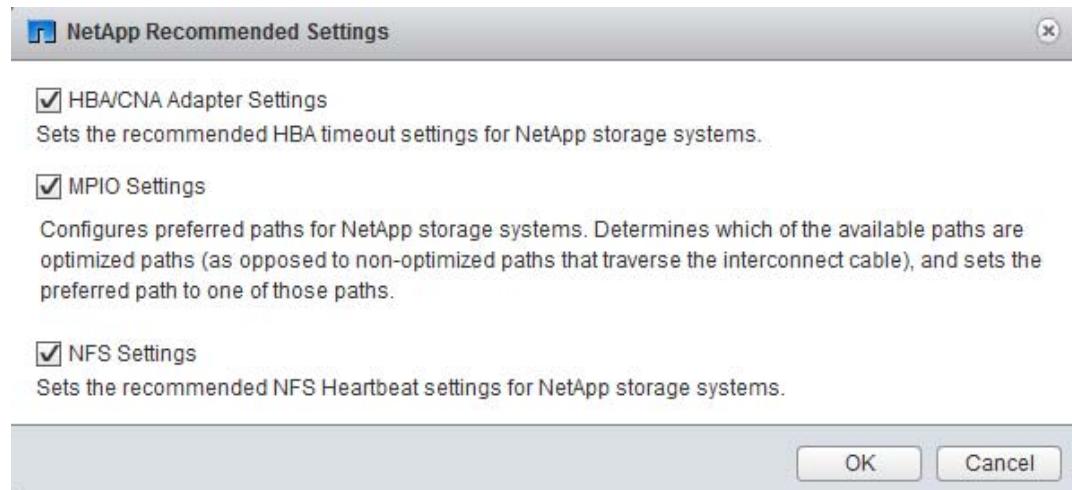


3. Click the Storage Systems. Under Objects tab, click Actions > Modify.
4. In the IP Address/Hostname field, enter the storage cluster management IP. Enter admin for the user name, and the admin password for password. Confirm that Use SSL to connect to this storage system is selected. Click OK.
5. Click OK to accept the controller privileges.

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, complete the following steps:

1. From the Home screen, click on vCenter > Hosts and Clusters. For each ESXi host, right-click and select NetApp VSC > Set Recommended Values for these hosts.

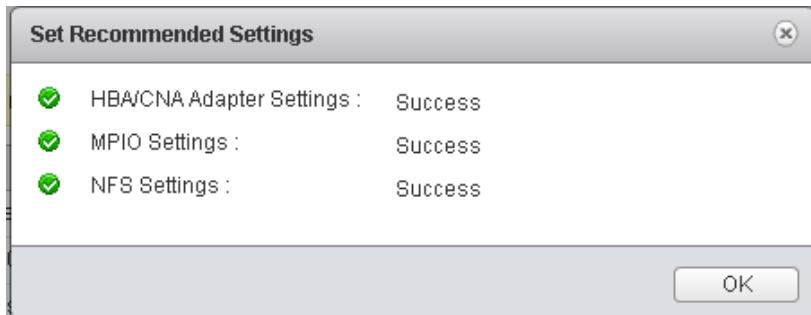


2. Check the settings that are to be applied to the selected vSphere hosts. Click OK to apply the settings.



Note 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).

3. Click OK.



VSC 5.0 Backup and Recovery

Prerequisites to Use 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 confirm that the storage systems that contain the datastores and virtual machines for which you are creating backups have valid storage credentials.

If you plan to leverage the SnapMirror update option, add all the destination storage systems with valid storage credentials.

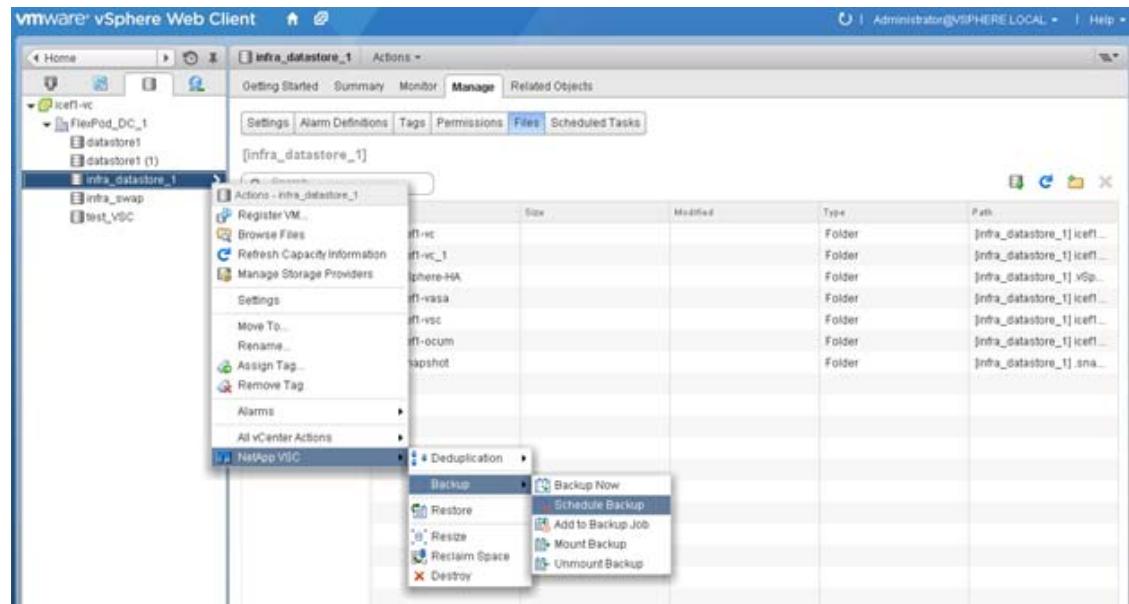
Backup and Recovery Configuration

The following steps detail the procedure to configure a backup job for a datastore.

1. From Home screen, select the Home tab and click Storage.
2. Right-click the datastore which you need to take backup. Select NetApp VSC > Backup > Schedule Backup.



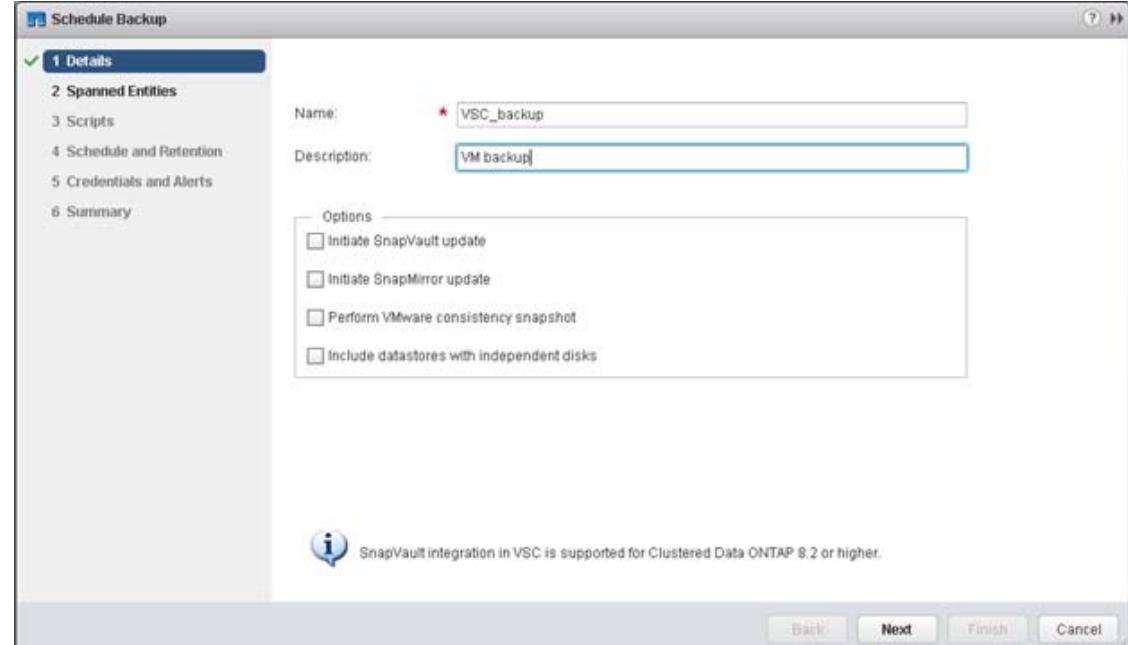
Note If you prefer one time backup, then choose Backup Now instead of Schedule Backup.



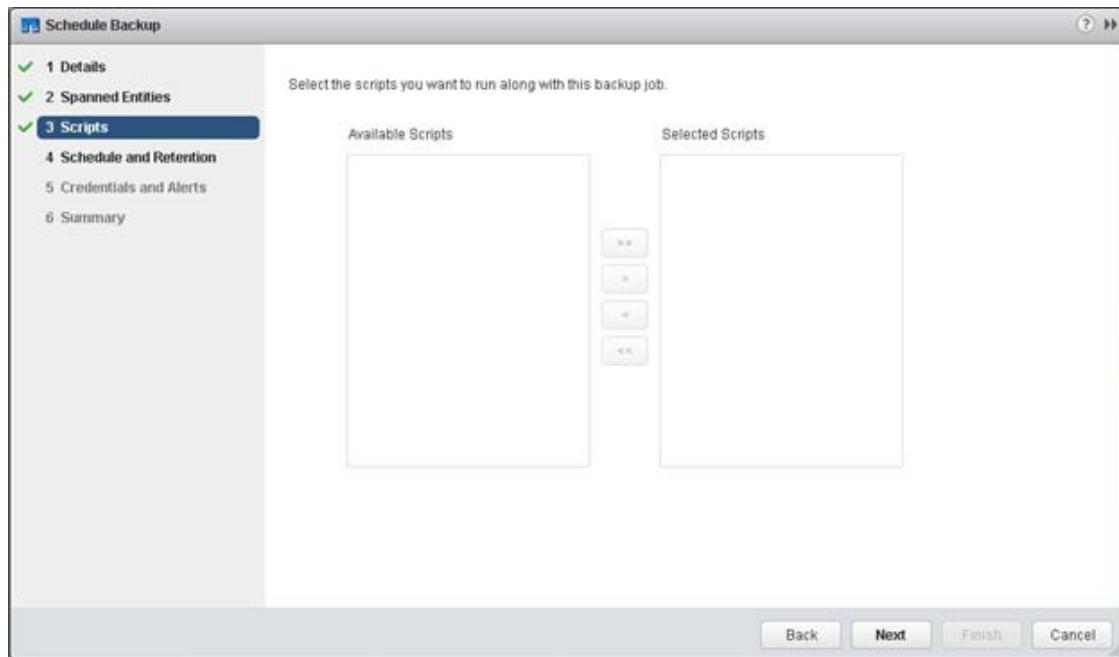
- Type a backup job name and description.



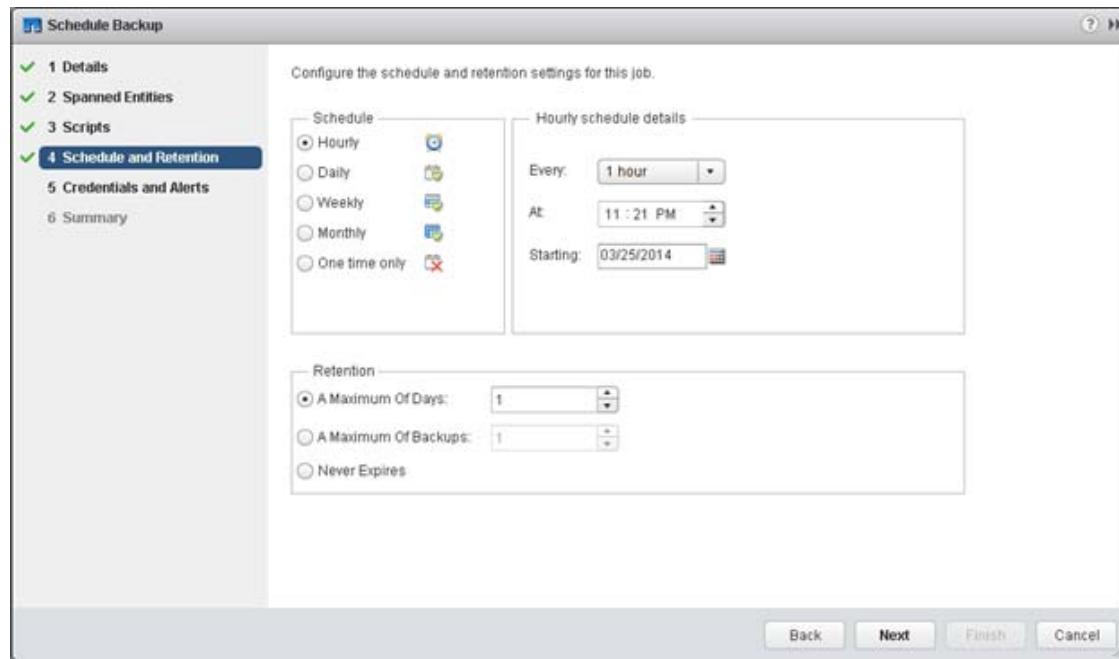
If you want to create a VMware snapshot for each backup, select Perform VMware consistency snapshot in the options pane.



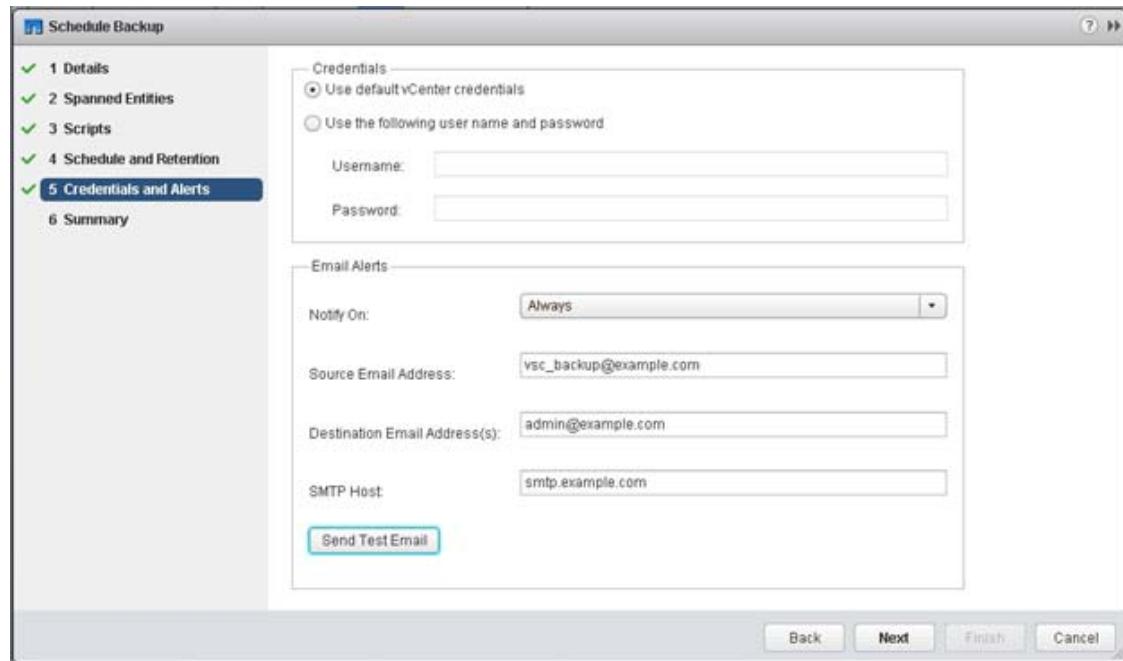
- Click Next.
- Click Next.
- Select one or more backup scripts if available and click Next.



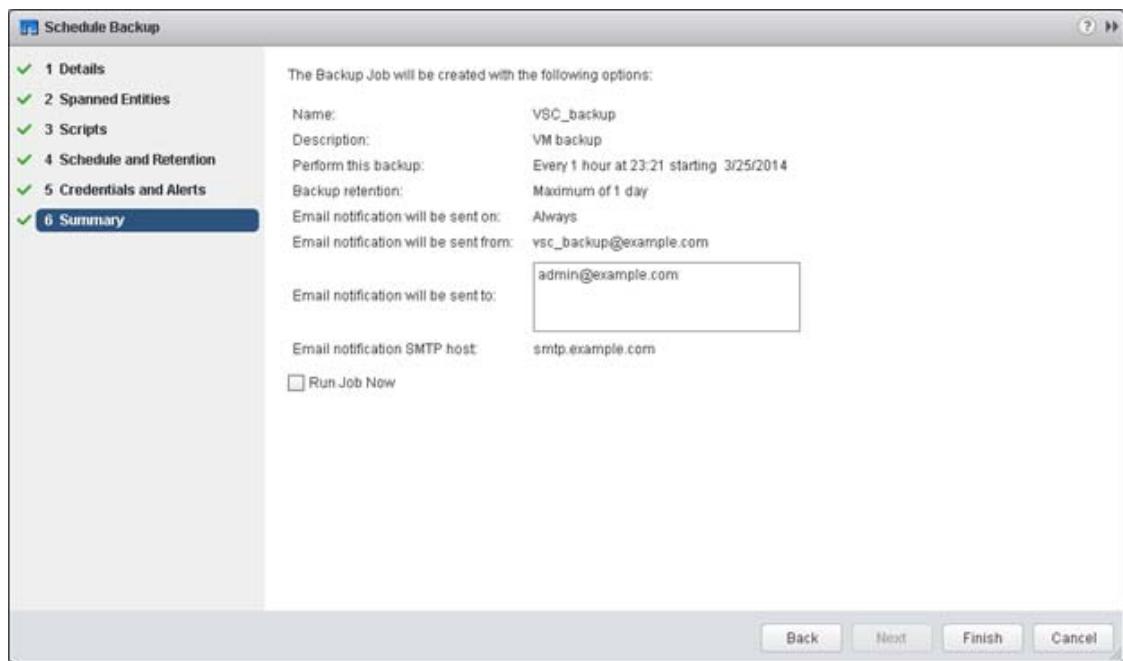
7. Select the hourly, daily, weekly, or monthly schedule that you want for this backup job and click Next.



8. Use the default vCenter credentials or type the user name and password for the vCenter Server and click Next.
9. Specify backup retention details as per requirements. Enter an e-mail address for receiving email alerts. You can add multiple email addresses by using semicolons to separate e-mail addresses. Click Next.



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



11. Click OK.



12. On the storage cluster interface, automatic Snapshot copies of the volume can be disabled by entering the following command:

```
volume modify -volume infra_datastore_1 -snapshot-policy none
```

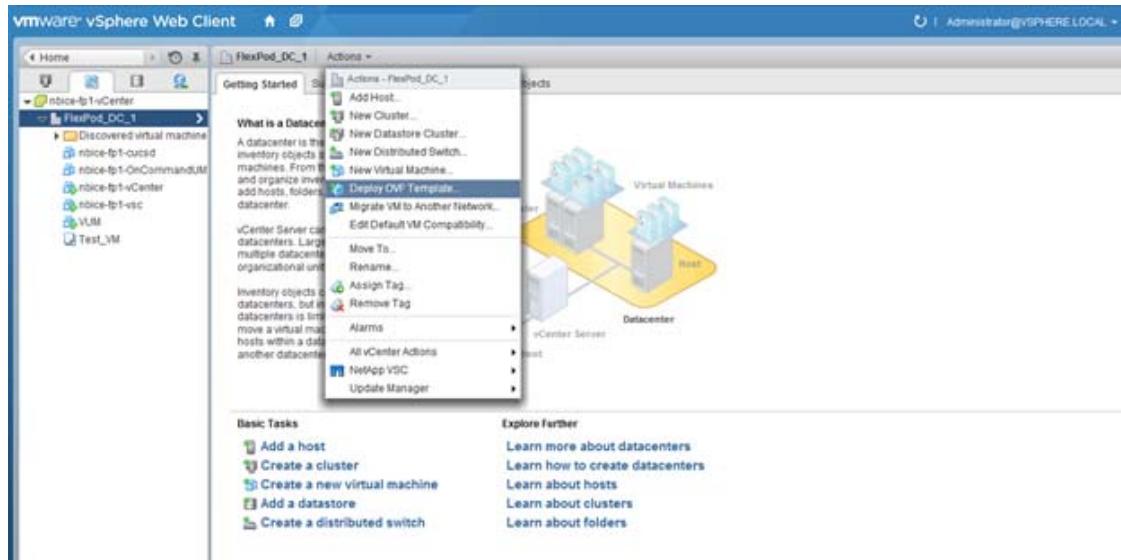
13. Also, to delete any existing automatic Snapshot copies that have been created on the volume, enter the following command:

```
volume snapshot show -volume infra_datastore_1
volume snapshot delete -volume infra_datastore_1 <snapshot name>
```

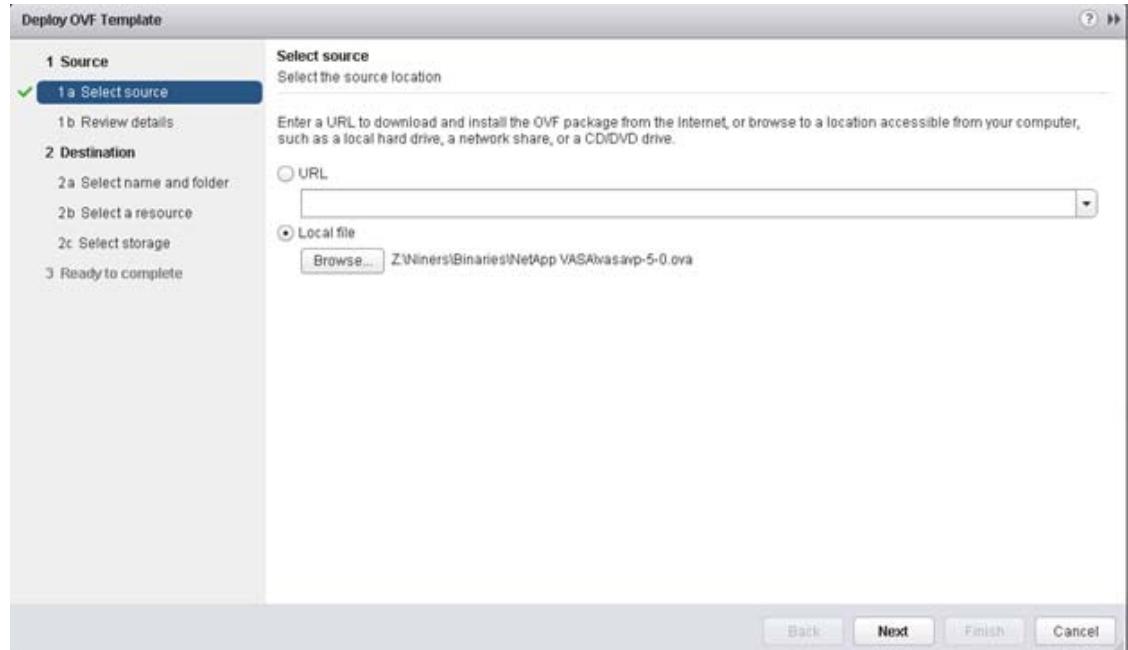
NetApp VASA Provider for Clustered Data ONTAP Deployment Procedure

VASA Provider for clustered Data ONTAP uses VMware VASA (vSphere APIs for Storage Awareness) to provide better storage management. By providing information about storage used by Virtual Storage Console for VMware vSphere to the vCenter Server, VASA Provider enables you to make more intelligent virtual machine provisioning decisions and allows the vCenter Server to warn you when certain storage conditions may affect your VMware environment. Virtual Storage Console for VMware vSphere is the management console for VASA Provider. To install the NetApp VASA provider, complete the following steps:

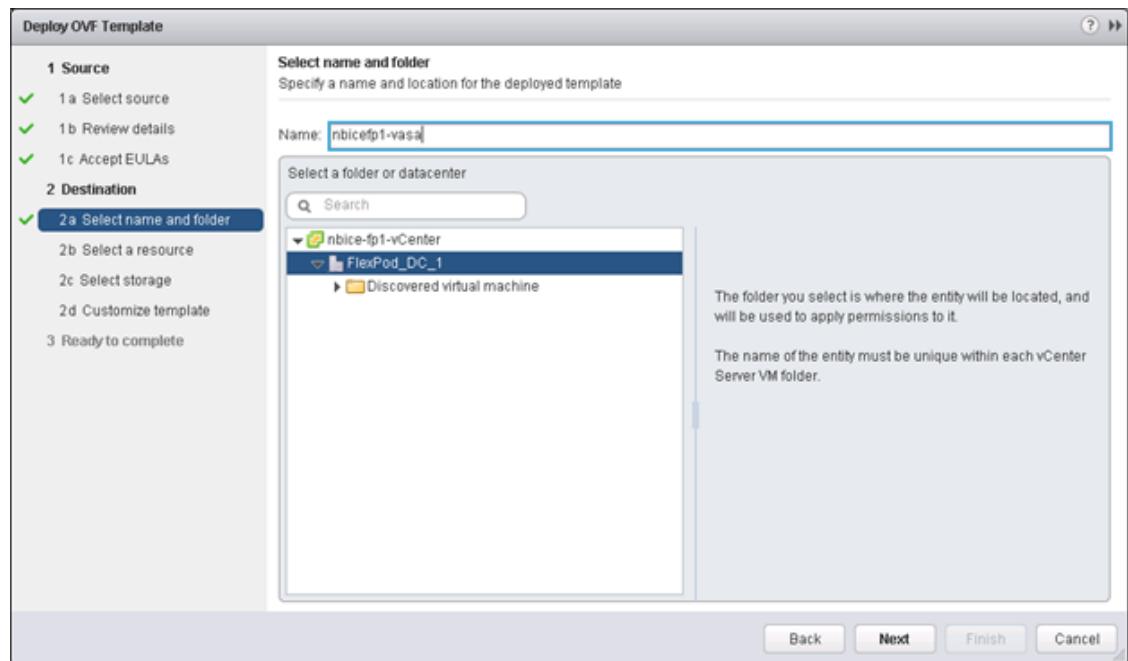
1. Download the VASA provider from NetApp support site.
2. Log into the vSphere Web Client. Go to vCenter > VMs and Templates
3. At the top of the center pane, click Actions > Deploy OVF Template.



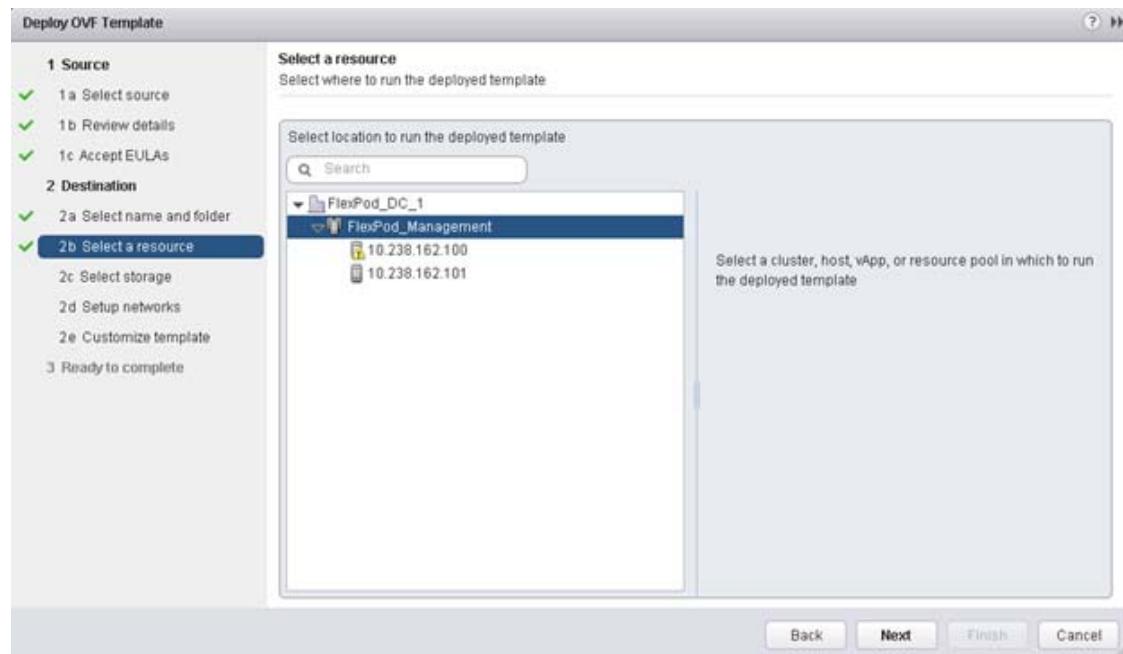
- Browse the .ova file that was downloaded locally. Click Open to select the file.



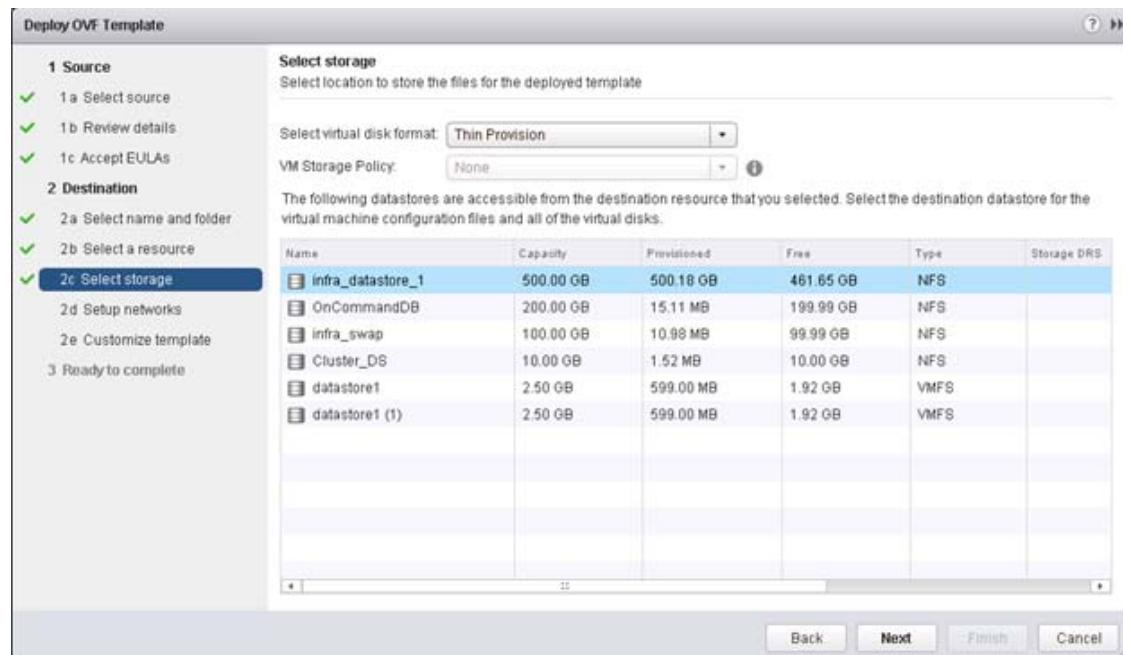
- Click Next to proceed with the selected file.
- Click Next.
- Read the EULA, then click the Accept button to accept the agreement. Click Next to continue.
- Enter the name of the VM and select the FlexPod_DC_1 folder to hold the virtual machine. Click Next to continue.



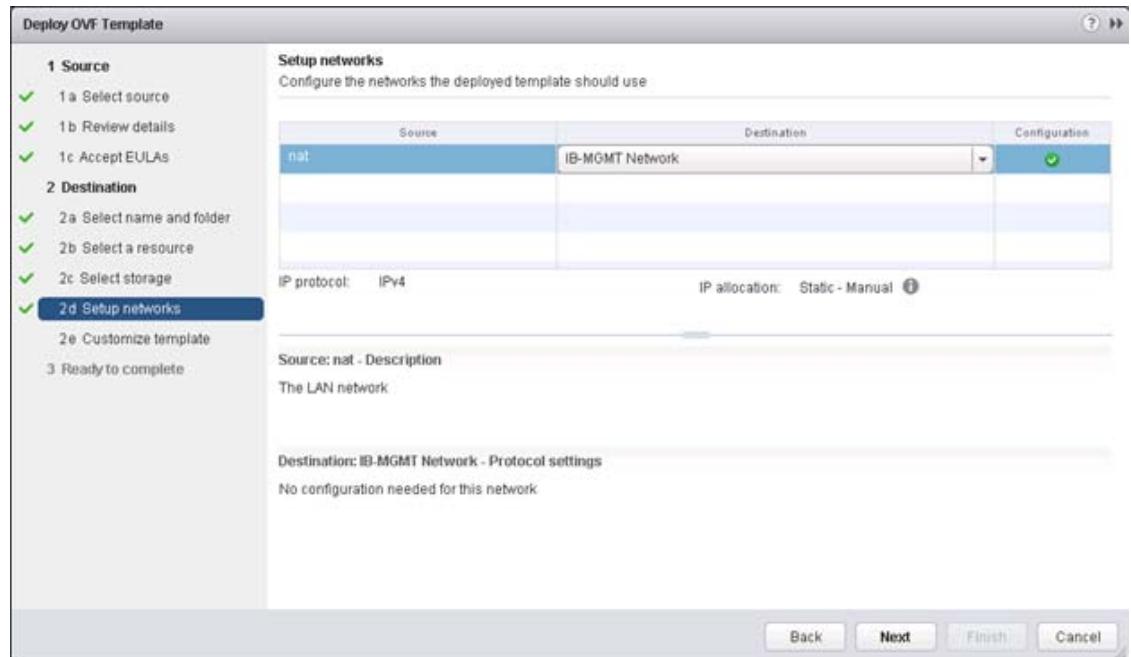
- Select FlexPod_Management within the FlexPod_DC_1 Datacenter as the destination compute resource pool to host the VM. Click Next to continue.



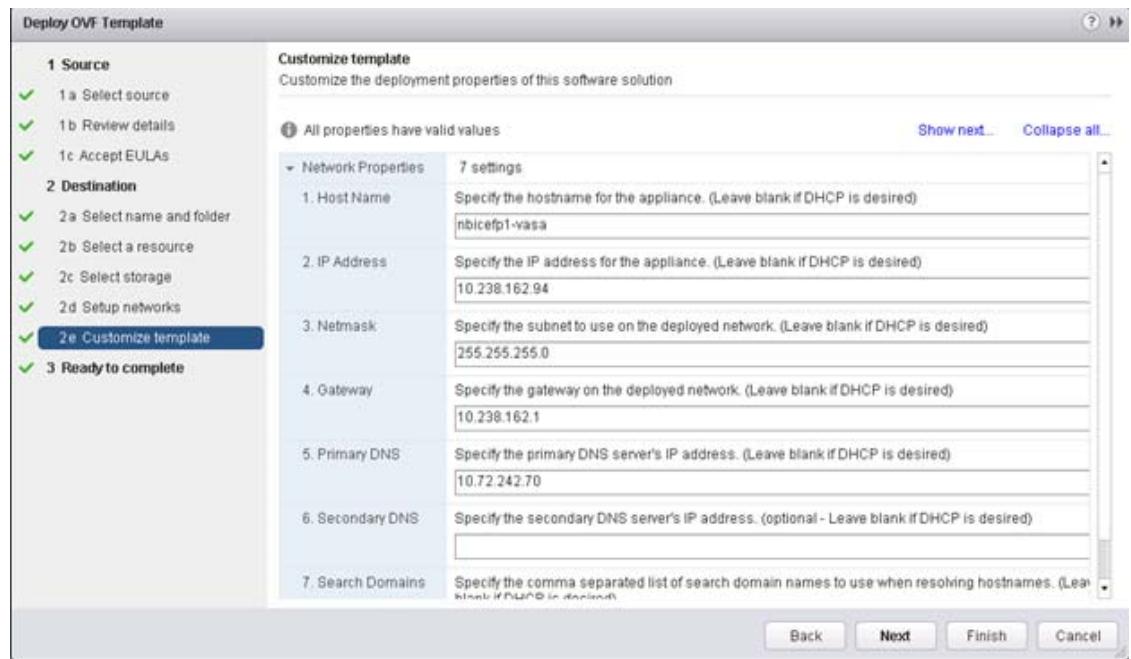
- Select infra_datastore_1 as the storage target for the VM and select Thin Provision as the Virtual disk format. Click Next to continue.



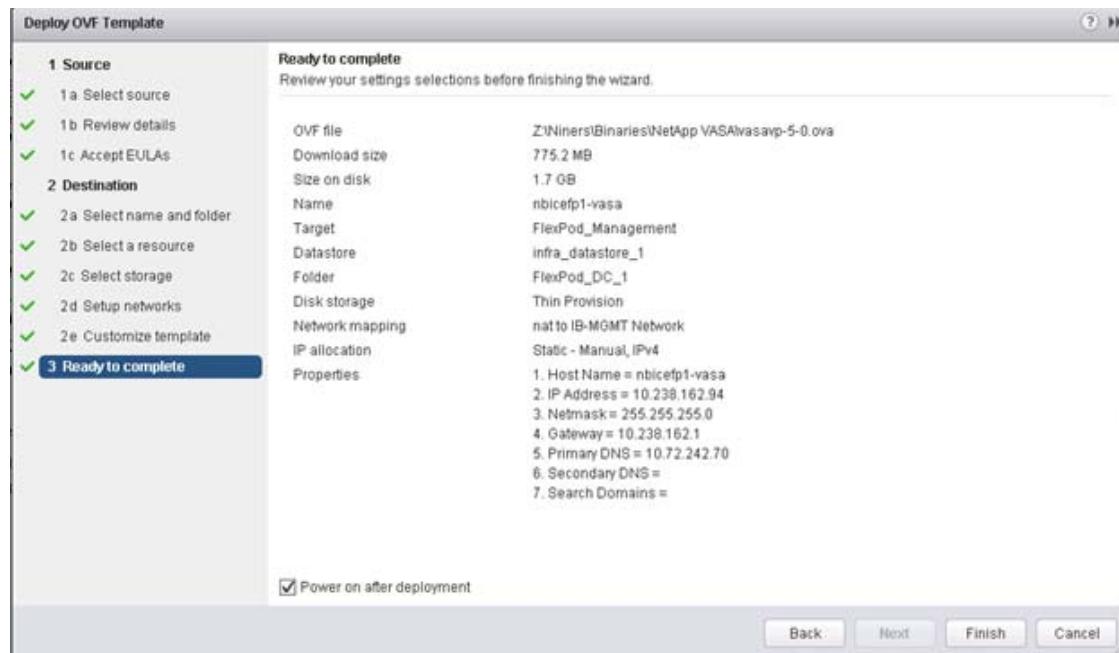
- Select IB-MGMT Network as the destination network to the nat source network. Click Next.



12. Fill out the details for the Host Name, IP Address, NetworkMask, gateway, Primary DNS, and Secondary DNS. Click Next to continue.



13. Select Power on after deployment and click Finish.



14. Right-click the VASA VM and click Open Console. VASA Provider installation will prompt for installing the VMware tools.

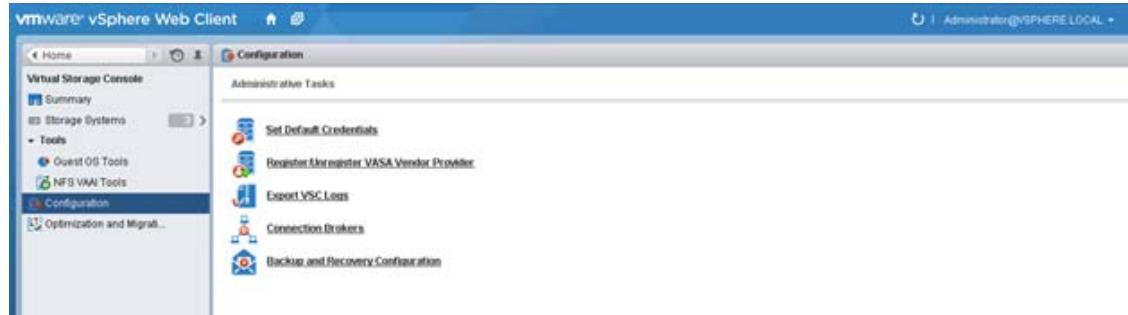


15. In the web client, click on the VASA VM. Click Summary tab.
 16. Click Install VMware Tools and switch back to VASA VM console window.
 17. In the VASA VM console, press Enter to continue the VASA provider installation.
 18. Switch back to web client. Right-click VASA VM and select Edit Settings. Set CD/DVD device type to Client Device.
 19. Switch back to VASA VM console window and press Enter to reboot the VM.
 20. Upon reboot, the VASA appliance will prompt for Maint and vpserver passwords. Type the new passwords accordingly.

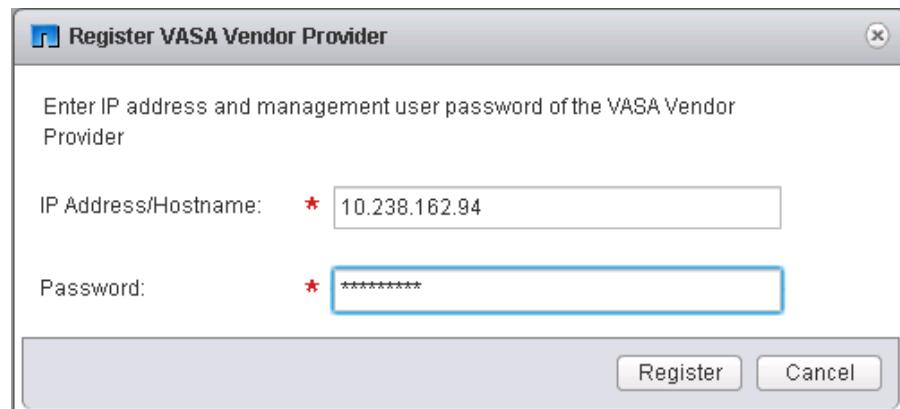
Registering VASA Provider for Clustered Data ONTAP with VSC

1. Log in to the web client. Click Virtual Storage Console.

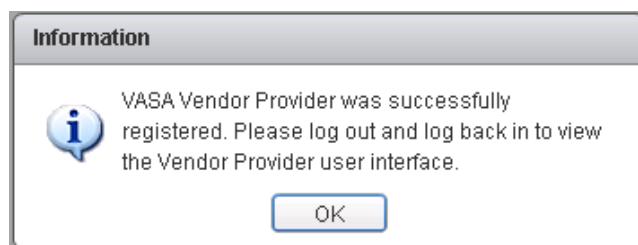
- Click Configuration. Click Register/Unregister VASA Vendor Provider.



- Enter the IP Address and Password for the VASA VM. Click Register.



- Log out of the web client and log back in to view the Vendor Provider user interface.



OnCommand Unified Manager 6.1

OnCommand Unified Manager OVF Deployment

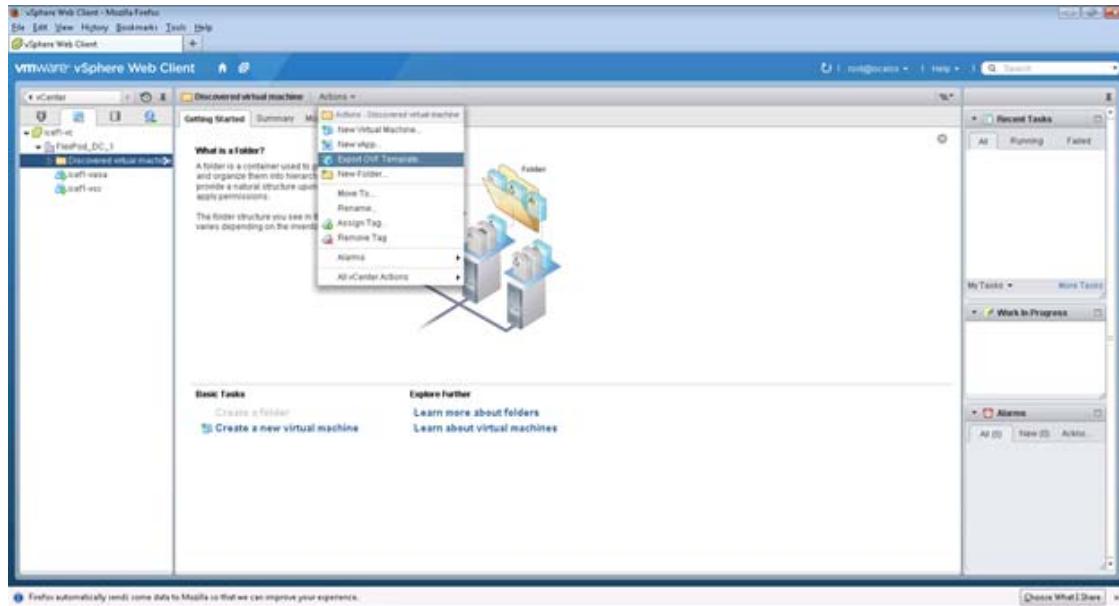
To install the OnCommand Unified Manager, complete the following steps:

- Download and review the [OnCommand Unified Manager for Clustered Data ONTAP 6.1 Installation and Setup Guide](#).

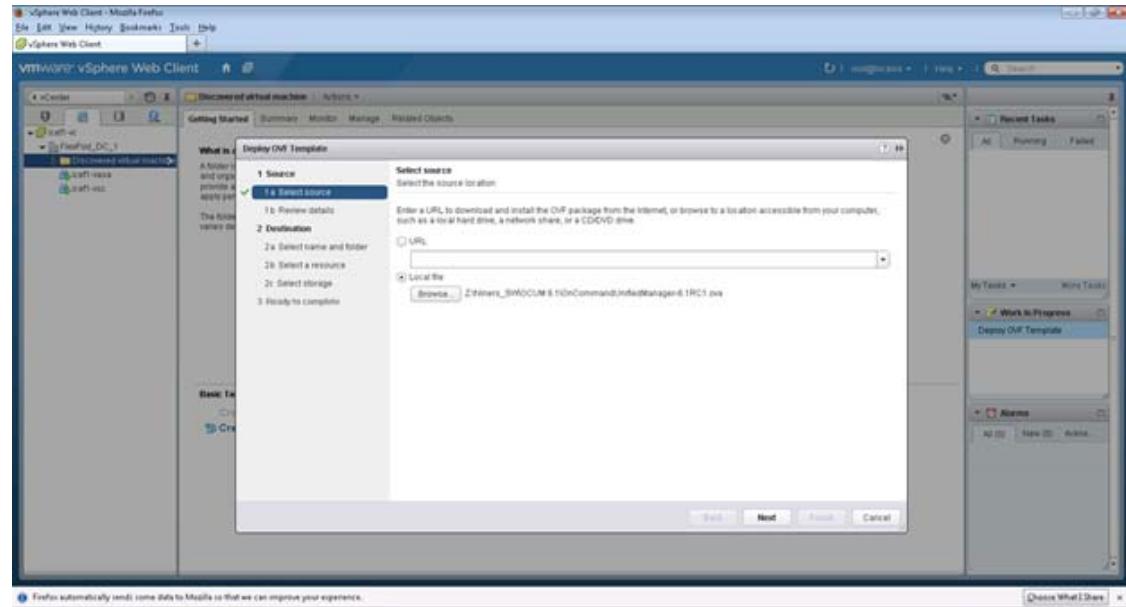


Note VMware High Availability for the Unified Manager virtual appliance is not supported. The virtual appliance can be deployed on a VMware server that is a member of a VMware high availability environment, but utilizing the VMware High Availability functionality is not supported.

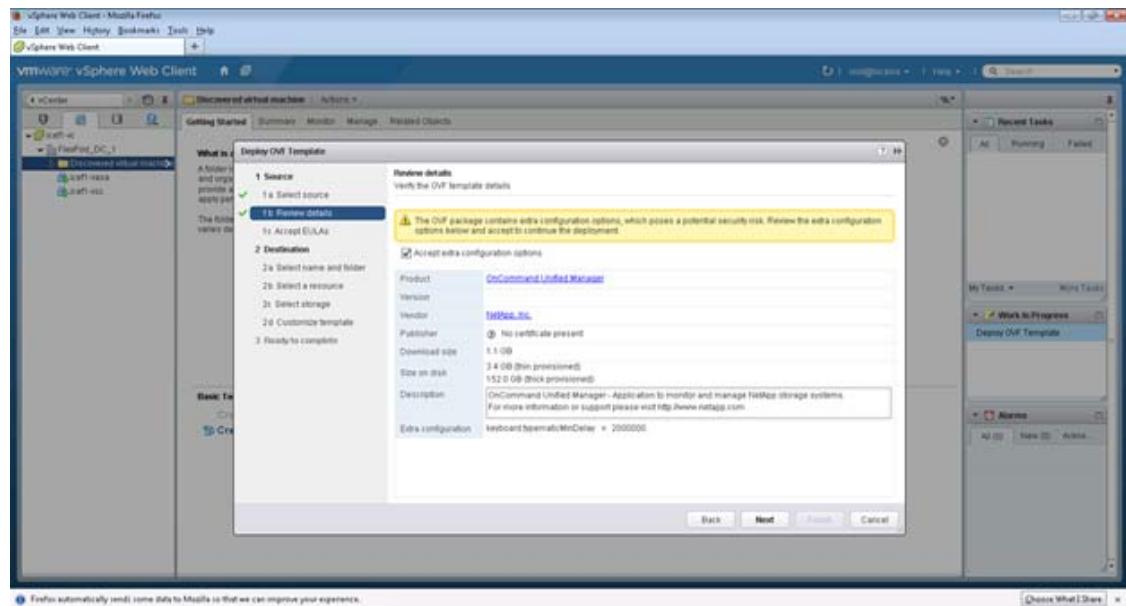
- If deployment fails when using an high-availability-enabled environment due to insufficient resources, modify the following default VMware settings.
 - Decrease the VM resources CPU and memory settings.
 - Decrease the vSphere HA Admission Control Policy to use less than the default percentage of CPU and memory.
 - Modify the Cluster Features Virtual Machine Options by disabling the VM Restart Priority and leaving the Host Isolation Response powered on.
- 2. Download the OnCommand Unified Manager (OnCommandUnifiedManager-6.1.ova), from http://support.netapp.com/NOW/download/software/oncommand_cdot/6.1/
- 3. Log in to the vSphere Web Client. Go to vCenter > VMs and Templates.



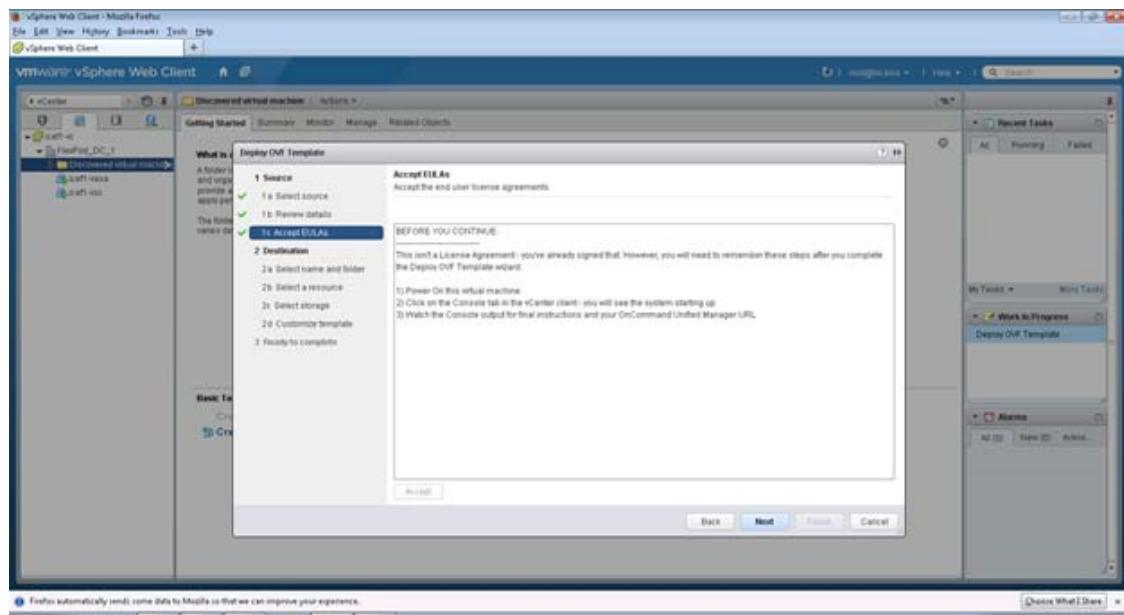
4. At the top of the center pane, click Actions > Deploy OVF Template.
5. Browse the .ova file that was downloaded locally. Click Open to select the file.



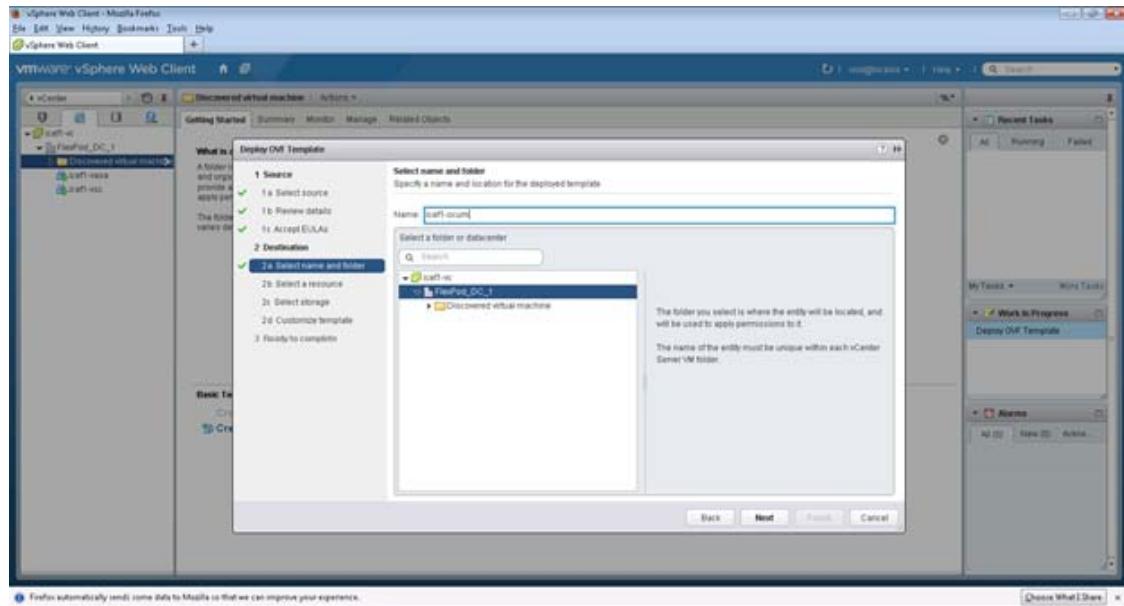
- Click Next to proceed with the selected file.



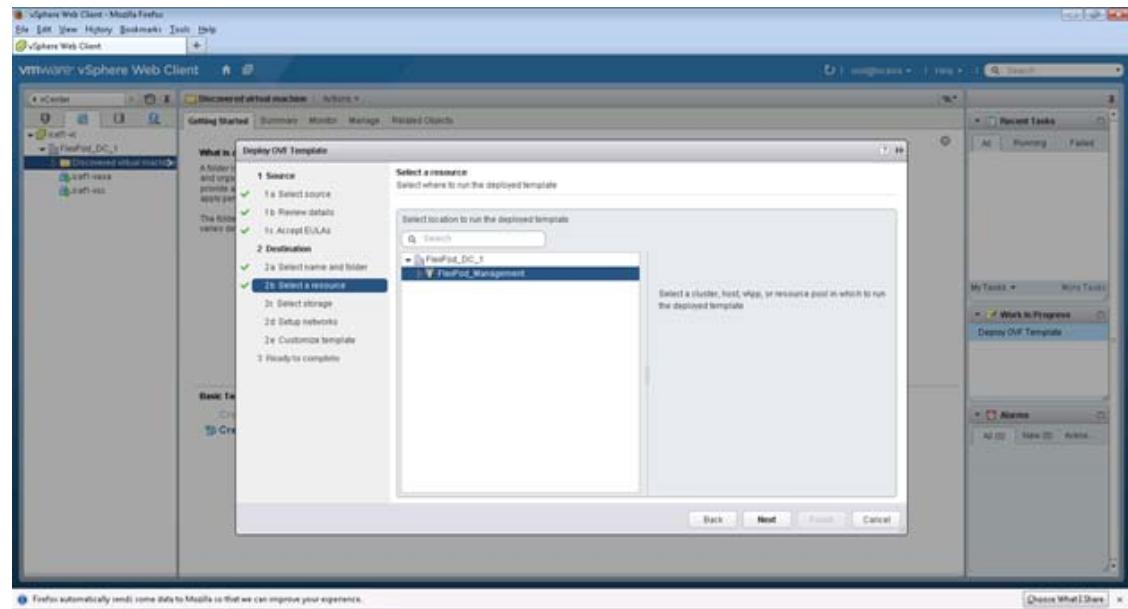
- Click the checkbox to accept the additional configuration options and click Next.



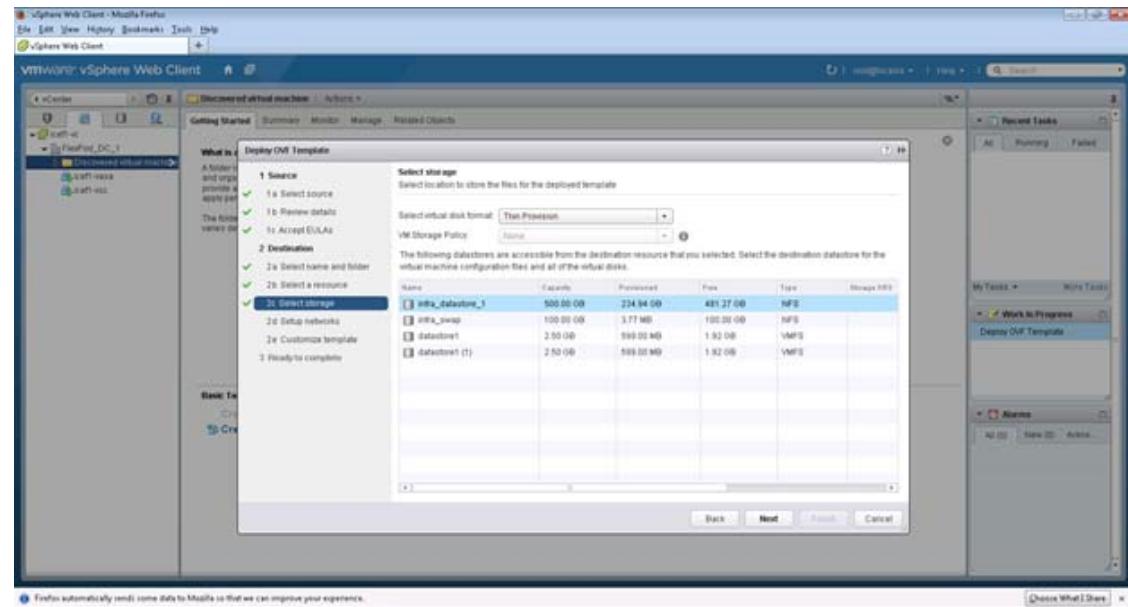
8. Read the EULA, then click the Accept button to accept the agreement. Click Next to continue.



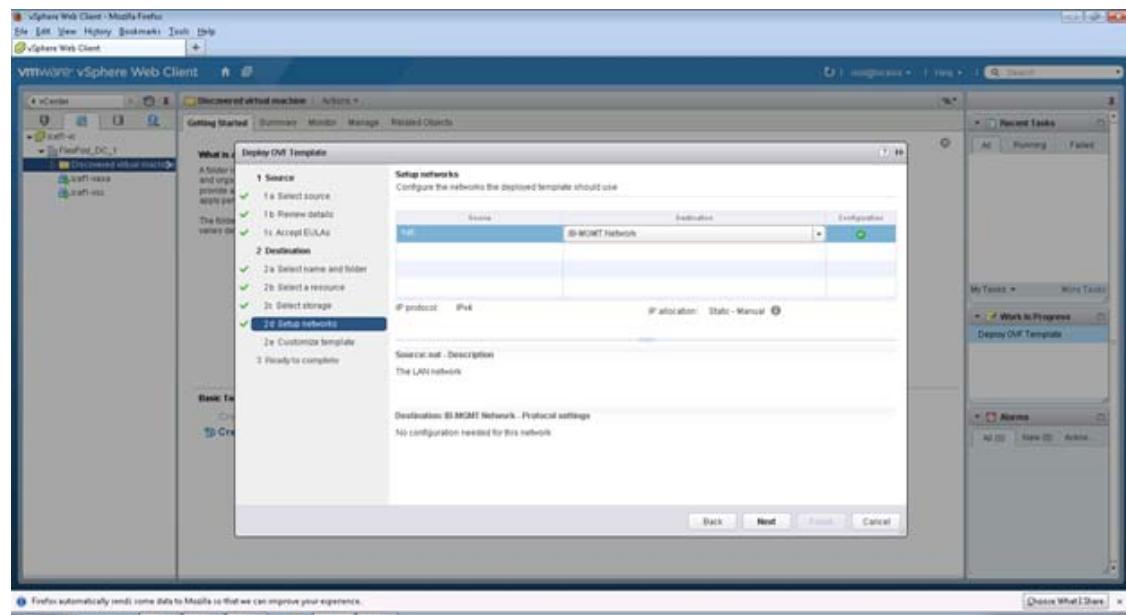
9. Enter the name of the VM and select the FlexPod_DC_1 folder to hold the VM. Click Next to continue.



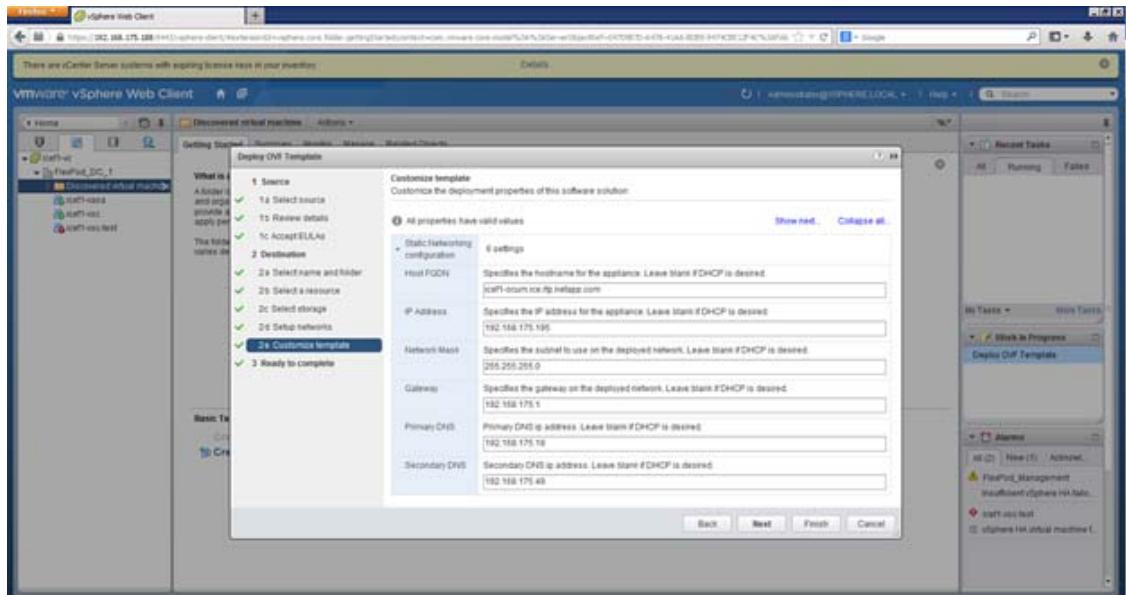
10. Select FlexPod_Management within the FlexPod_DC_1 datacenter as the destination compute resource pool to host the VM. Click Next to continue.



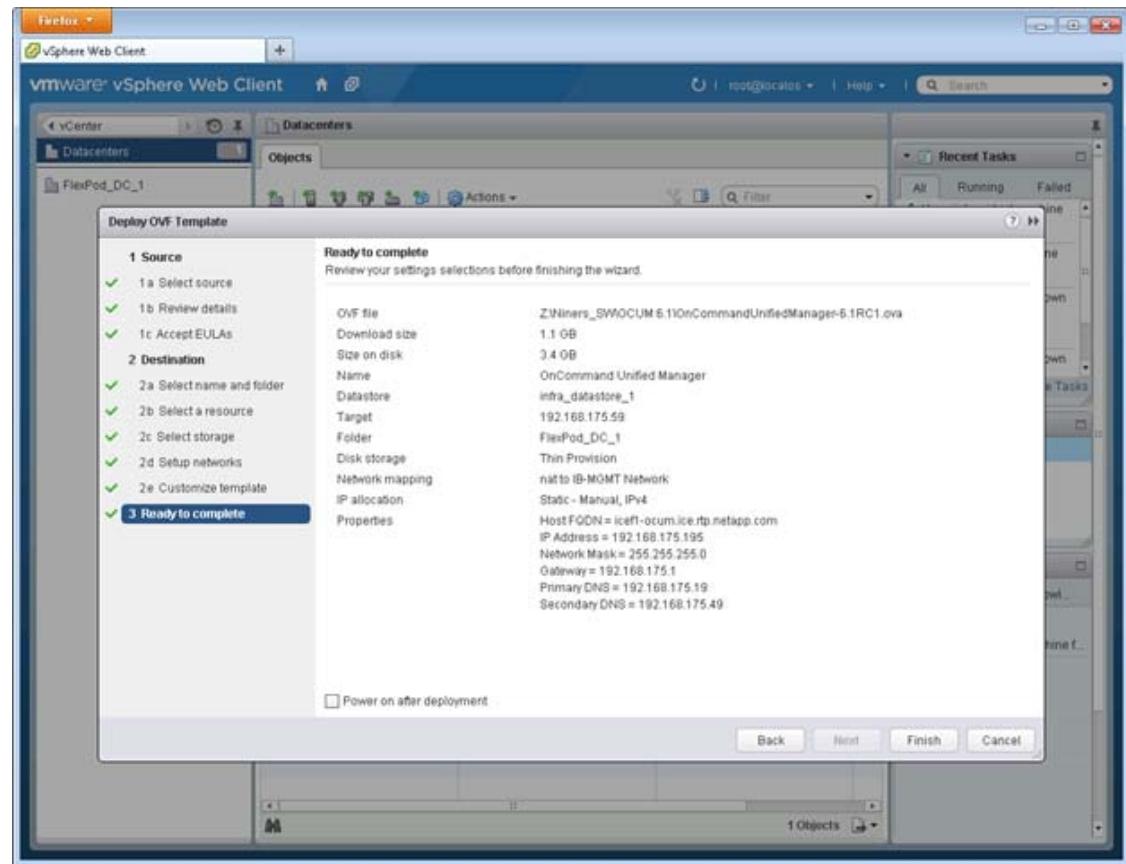
11. Select **infra_datastore_1** as the storage target for the VM and select **Thin Provision** as the Virtual disk format. Click Next to continue.



12. Select **IB-MGMT Network** as the destination network to the nat source network. Click Next.



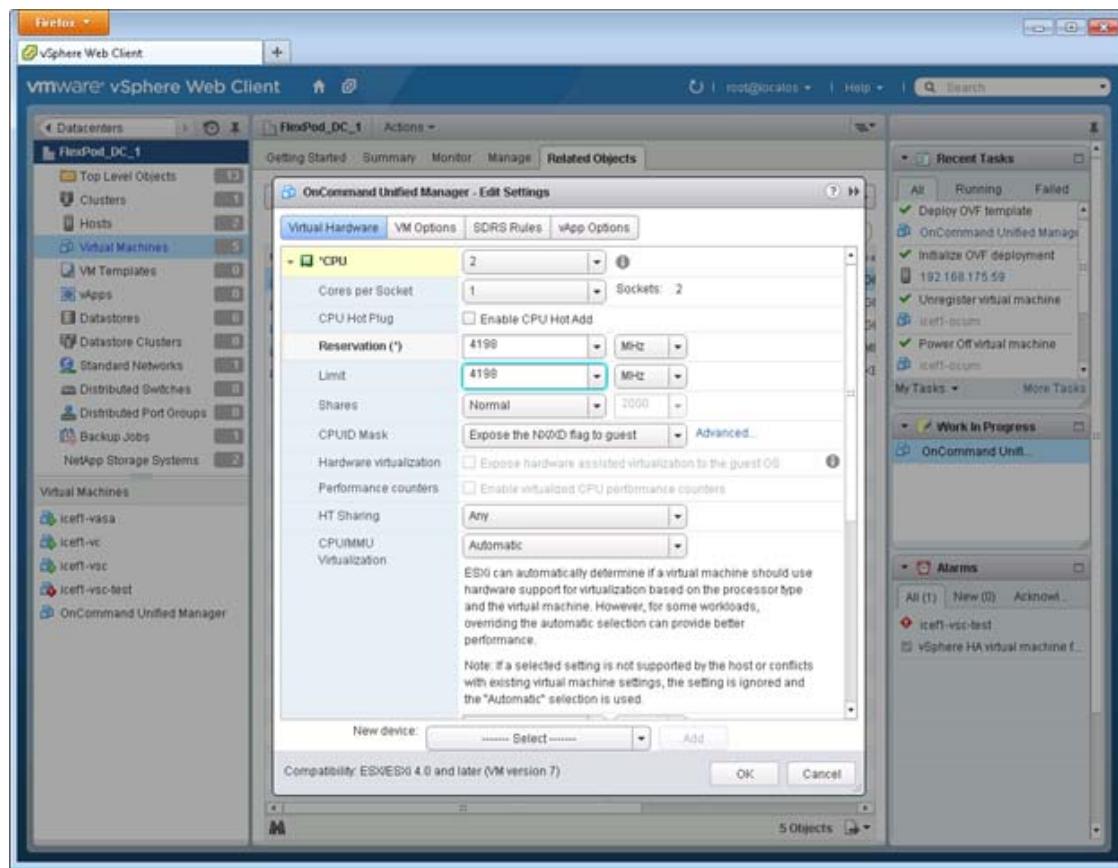
13. Fill out the details for the Host Name, IP Address, Networkmask, Gateway, Primary DNS, and Secondary DNS. Click Next to continue.



14. Uncheck the Power on after deployment checkbox.
15. Review the configuration details. Click Finish to begin deploying the VM with the provided configuration details:
 - On the left pane click Virtual machines. Right-click the newly created virtual machine and select Edit Settings.
 - Click the CPU tab to expand the CPU options.
 - Set the number of CPUs to match the number of CPUs present in the host.
 - Set the Reservation and Limit (MHz values) by following the below calculation -(Number of CPUs) X (Processor speed of the CPUs in the host)

For example, if a host has 2 CPUs operating at a speed of 2099MHz, then the reservation and limit would be set to 4198.

The amount of memory can be set to 8 GB. Use the [OnCommand Unified Manager Installation and Setup Guide](#) for guidance on these settings.



16. Click OK to accept the changes.
17. Right-click the VM in the left-hand pane. Click Power On.

OnCommand Unified Manager Basic Setup

1. Right-click the VM in the left-hand pane. Click Open Console.
2. Set up OnCommand Unified Manager by answering the following questions in the console window:

Geographic area: <<Enter your geographic location>>

Time zone: <<Select the city or region corresponding to your time zone>>

These commands complete the network configuration checks SSL certificate generation for HTTPS and start the OnCommand Unified Manager services.

3. To Create a Maintenance User account, run the following commands:

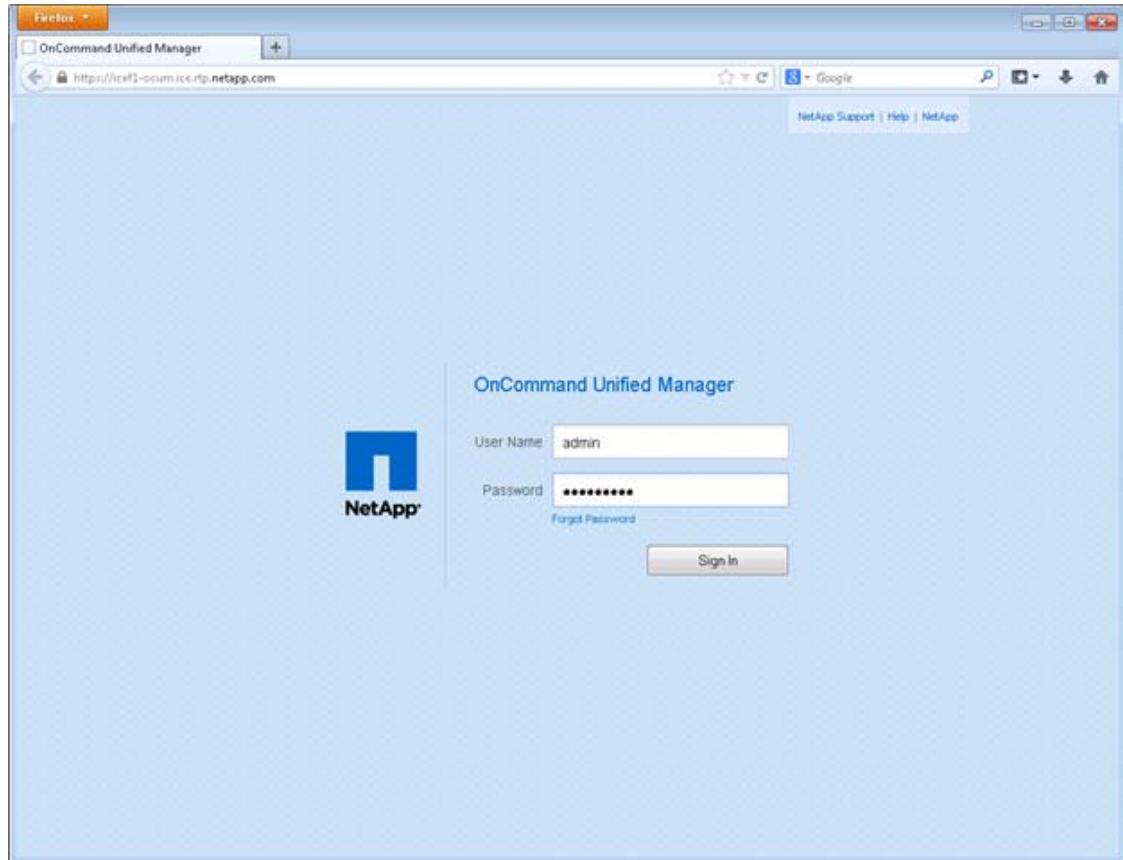


Note The maintenance user manages and maintains the settings on the OnCommand Unified Manager virtual appliance.

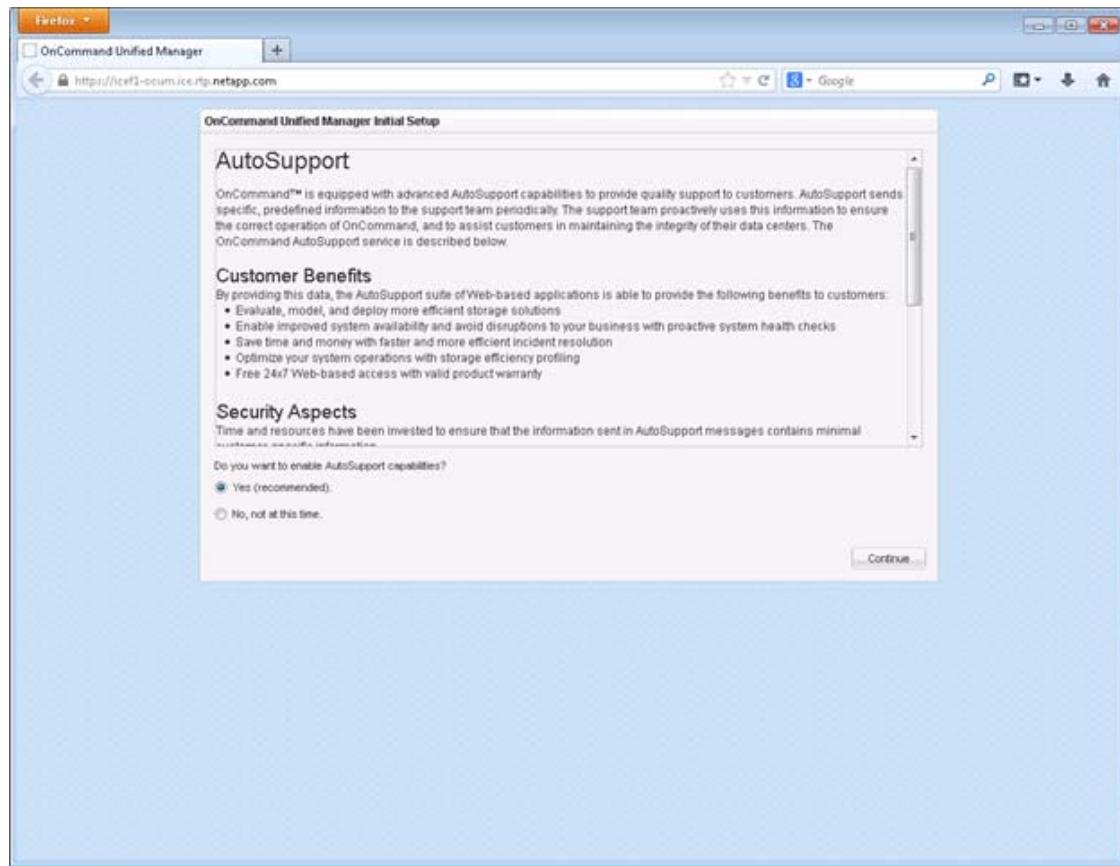
```
Username : admin
Enter new UNIX password: <<var_password>>
Retype new UNIX password: <<var_password>>
```

OnCommand Unified Manager Initial Setup

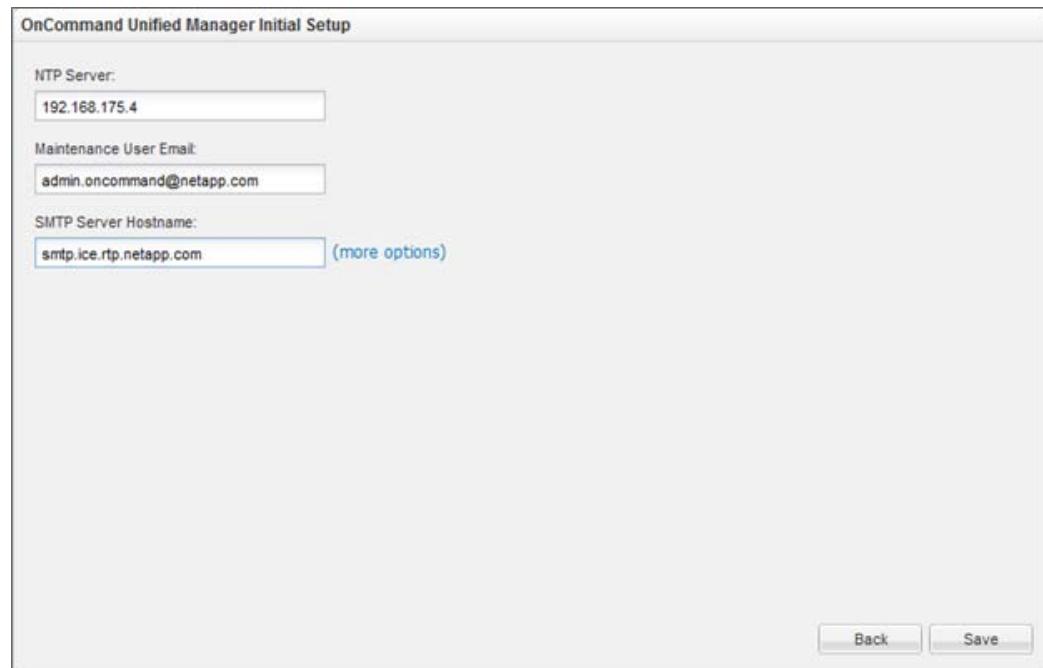
1. Using a web browser navigate to the OnCommand Unified Manager using URL: https://<<var_oncommand_server_ip>>.



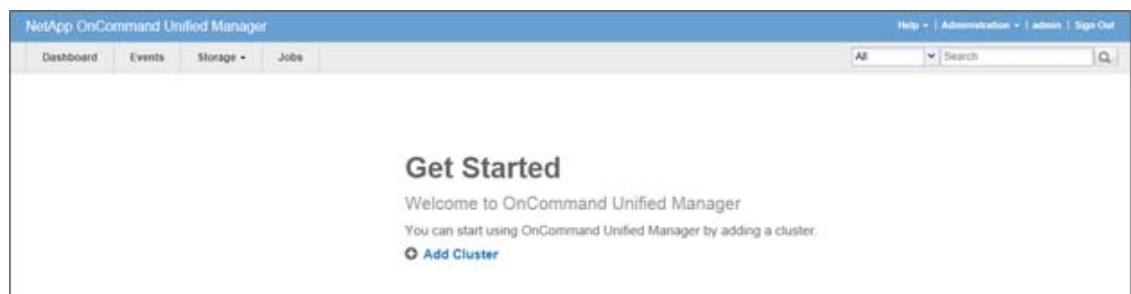
2. Log in using the Maintenance User account credentials.
3. Select Yes option to enable AutoSupport capabilities.



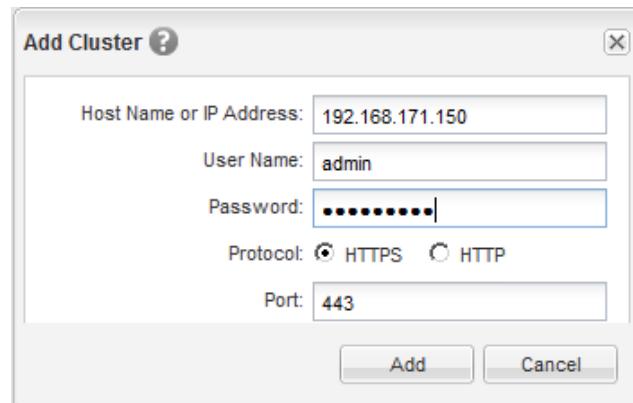
4. Click Continue.
5. Provide the NTP Server IP address <<var_global_ntp_server_ip>>
6. Provide the Maintenance User Email <<var_storage_admin_email>>
7. Provide the SMTP Server Hostname.



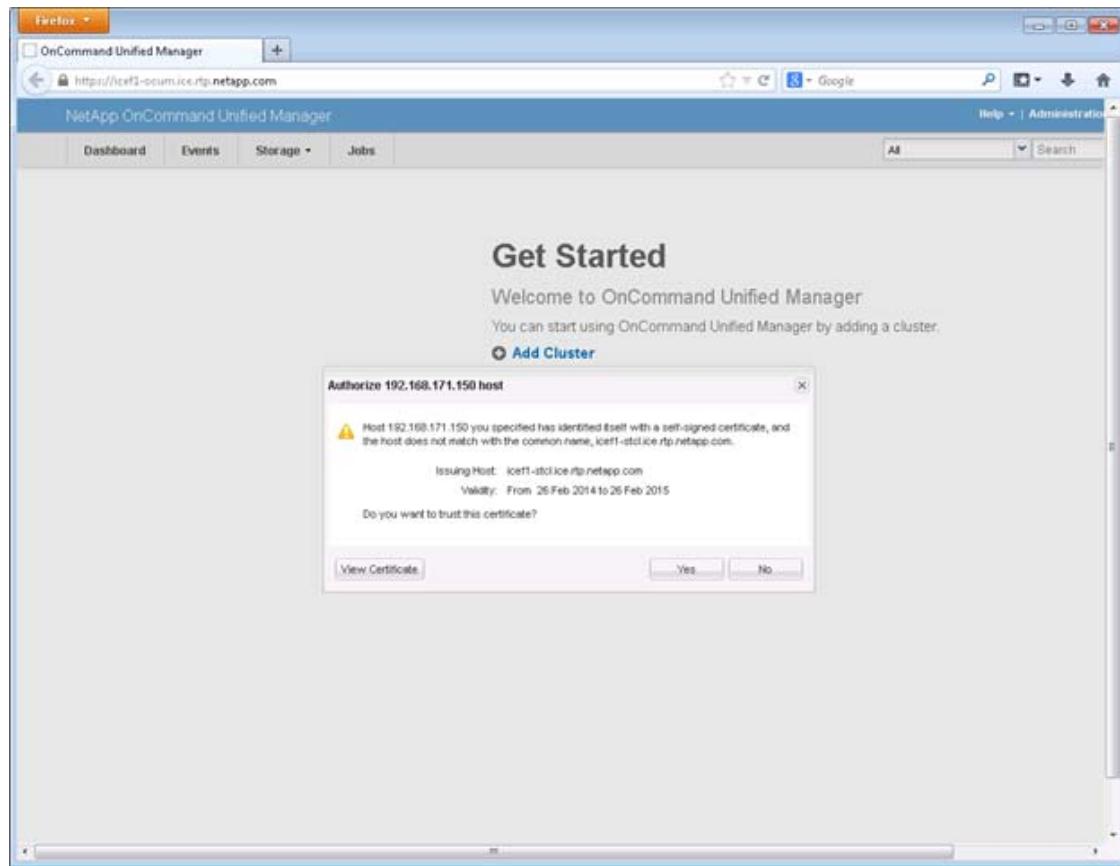
8. Click Save.
9. Click Add Cluster



10. Provide the Cluster Management IP address, User Name, Password, Protocol, and Port.



11. Click Add.



12. Click Yes to trust the certificate from the controller.



Note

The Cluster Add operation might take a couple of minutes.

13. After the cluster is added it can be accessed by clicking on the Storage tab and selecting Clusters.

NetApp NFS Plug-In 1.0.21 for VMware VAAI

Enable VMware vStorage for NFS in Clustered Data ONTAP

To enable VMware vStorage for NFS in clustered Data ONTAP, complete the following steps:

- From an SSH session to the storage cluster management address, log in with the admin user name and password.
- Enable vStorage on the Vserver.

```
vserver nfs modify -vserver Infra_Vserver -vstorage enabled
```

- Verify that the export policy rules are set up correctly.

```
vserver export-policy rule show -vserver Infra_Vserver
```

Sample output:

Vserver	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
<hr/>					
<hr/>					
Infra_Vserver	default	1	nfs	192.168.170.59	sys
Infra_Vserver	default	2	nfs	192.168.170.58	sys
2 entries were displayed.					

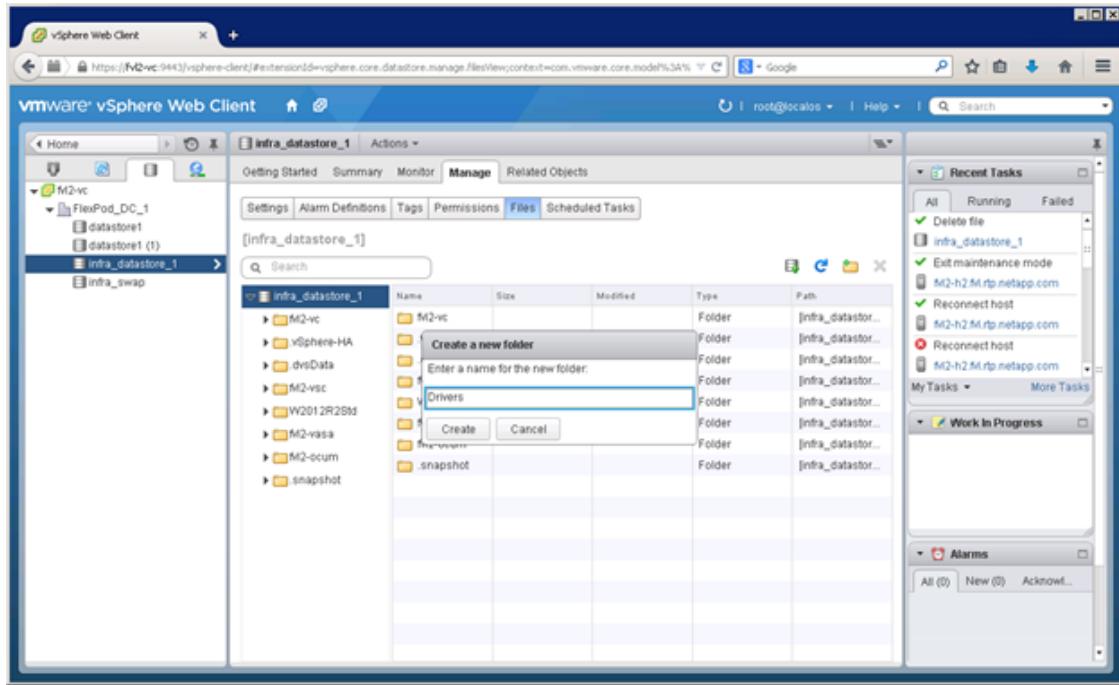
- The access protocol for the FlexPod policy name should be NFS. If the access protocol is not "nfs" for a given rule index, run the following command to set NFS as the access protocol:

```
vserver export-policy rule modify -vserver Infra_Vserver -policyname default -ruleindex <>var_rule_index<> -protocol nfs
```

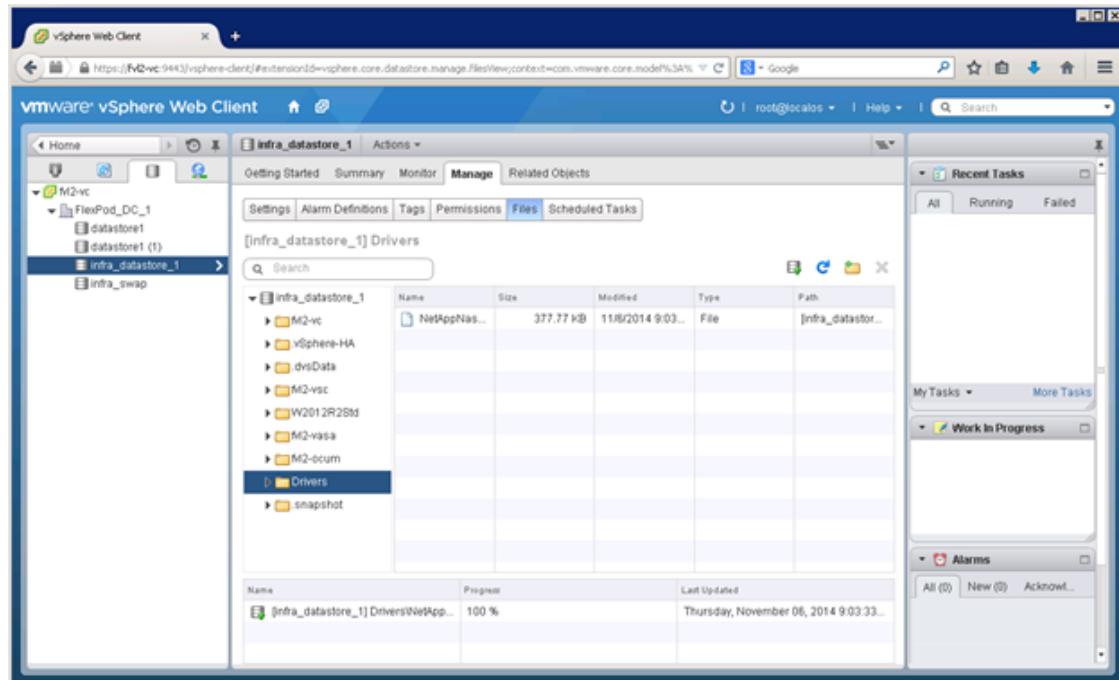
Install NetApp NFS Plug-In for VMware VAAI

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

- From the management workstation, go to the [Software Downloads page](#) in the NetApp Support site.
- Scroll down to locate the NetApp NFS Plug-in for VMware VAAI, select the ESXi platform, and click Go.
- Download the .vib file of the most recent plug-in version.
- In the vSphere Web Client, from the Home page, select Storage, and then expand the vCenter and DataCenter on the left and select the `infra_datastore_1` datastore.
- In the center pane, click the icon to Create a New Folder. Name the folder `Drivers` and click Create.



6. On the left side of the center pane, select the Drivers folder. Click the icon to Upload a File.
7. Browse to the location of the NetAppNasPlugin.v21.vib file, select it, and click Open to upload it to the Drivers folder.



8. Open the VMware vSphere CLI command prompt, and type the following commands:

```

esxcli -s <>var_vm_host_infra_01_ip>> -u root -p <>var_password>> software
vib install -v
/vmfs/volumes/infra_datastore_1/Drivers/NetAppNasPlugin.v21.zip
esxcli -s <>var_vm_host_infra_02_ip>> -u root -p <>var_password>> software
vib install -v
/vmfs/volumes/infra_datastore_1/Drivers/NetAppNasPlugin.v21.zip

```

```

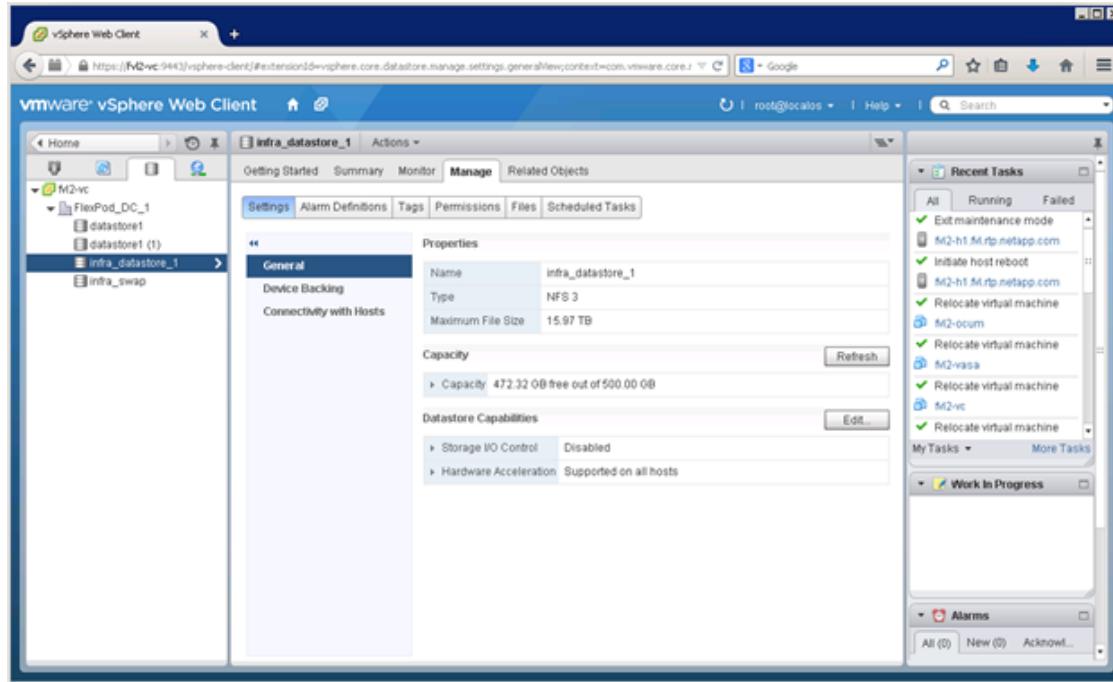
C:\Command Prompt
C:\Program Files (<x86>)\\VMware\\vSphere CLI>
C:\Program Files (<x86>)\\VMware\\vSphere CLI>
C:\Program Files (<x86>)\\VMware\\vSphere CLI>esxcli -s 172.20.81.11 -u root
-p NetApp!23 software vib install -v /vmfs/volumes/infra_datastore_1/Drivers/Net
AppNasPlugin.v21.vib
Installation Result
Message: The update completed successfully, but the system needs to be rebooted for the changes to be effective.
Reboot Required: true
VIBs Installed: NetApp_bootbank_NetAppNasPlugin_1.0-21
VIBs Removed:
VIBs Skipped:

C:\Program Files (<x86>)\\VMware\\vSphere CLI>esxcli -s 172.20.81.12 -u root
-p NetApp!23 software vib install -v /vmfs/volumes/infra_datastore_1/Drivers/Net
AppNasPlugin.v21.vib
Installation Result
Message: The update completed successfully, but the system needs to be rebooted for the changes to be effective.
Reboot Required: true
VIBs Installed: NetApp_bootbank_NetAppNasPlugin_1.0-21
VIBs Removed:
VIBs Skipped:

C:\Program Files (<x86>)\\VMware\\vSphere CLI>_

```

9. One at a time, put each ESXi host into Maintenance Mode, reboot the host, then Exit Maintenance Mode. It may be necessary to manually migrate VMs to the other host to allow the host to enter Maintenance Mode.
10. When the reboots have completed, in the vSphere Web Client from the Home page, click Storage, then select the infra_datastore_1 datastore. Select Settings under the Manage tab in the center pane. Hardware Acceleration should now show Supported on all hosts as shown below. All NFS datastores should now support Hardware Acceleration.



Appendix A - Building a Windows Active Directory Server VM

For detailed guidance deploying a Windows Active Directory server, refer to one of the following documents:

- Windows 2012R2 <http://technet.microsoft.com/en-us/library/jj574166.aspx>
- Windows 2008R2 [http://technet.microsoft.com/en-us/library/cc755059\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc755059(v=ws.10).aspx)

Appendix B - Deploying Application-Centric Infrastructure Layer 4 to Layer 7 Services

Cisco ACI is a policy driven framework which optimizes application delivery. Applications consist of server end points and network services. The relationship between these elements and their requirements forms an application-centric network policy. Through Cisco APIC automation application-centric network policies are managed and dynamically provisioned to simplify and accelerate application deployments on the fabric. Network services such as load balancers and firewalls can be readily consumed by the application end points as the APIC controlled fabric directs traffic to the appropriate services. This is the data center network agility application teams have been demanding to reduce deployment from days or weeks to minutes.

L4-L7 service integration is achieved by using service specific Device Packages. These Device Packages are imported into the Cisco APIC which are used to define, configure, and monitor a network service device such as a firewall, SSL offload, load balancer, context switch, SSL termination device, or intrusion prevention system (IPS). Device packages contain descriptions of the functional capability and settings along with interfaces and network connectivity information for each function.


Note

The Cisco APIC is an open platform enabling a broad ecosystem and opportunity for industry interoperability with Cisco ACI. Numerous Device Packages associated with various vendors are available and can be found at:

<http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/solution-overview-c22-732445.html>

An L4-L7 network service device is deployed in the fabric by adding it to a service graph which essentially identifies the set of network or service functions that are provided by the device to the application. The service graph is inserted between source and destination EPGs by a contract. The service device itself can be configured through the Cisco APIC or optionally through the devices traditional GUI or CLI. The level of APIC control is dependent on the functionality defined in the Device Package device scripts.


Note

Firewalls and load balancers are not a core component of the FlexPod solution but since most of the application deployments are incomplete without security and load distribution, Firewall and Load balancer designs are covered as part of the infrastructure deployment.

The remainder of this section details the deployment of L4-L7 services.

Import Device Package

Use the Import a Device Package wizard to import a device package for a function that you want to manage with APIC.

1. From the main menu bar click L4-L7 Services.
2. Click Packages" on the sub-menu.
3. Click Import a Device Package in the working pane.
4. Click Browse. Provide the device package file (zipped format) by browsing to the device package file location.
5. Click Submit.

IMPORT DEVICE PACKAGE

File Name: **BROWSE...**

SUBMIT **CLOSE**

6. Confirm Device Package; click L4-L7 Service Device Types in the left navigation pane. All imported packages are listed in the work pane.

The screenshot shows the ACI interface with the following details:

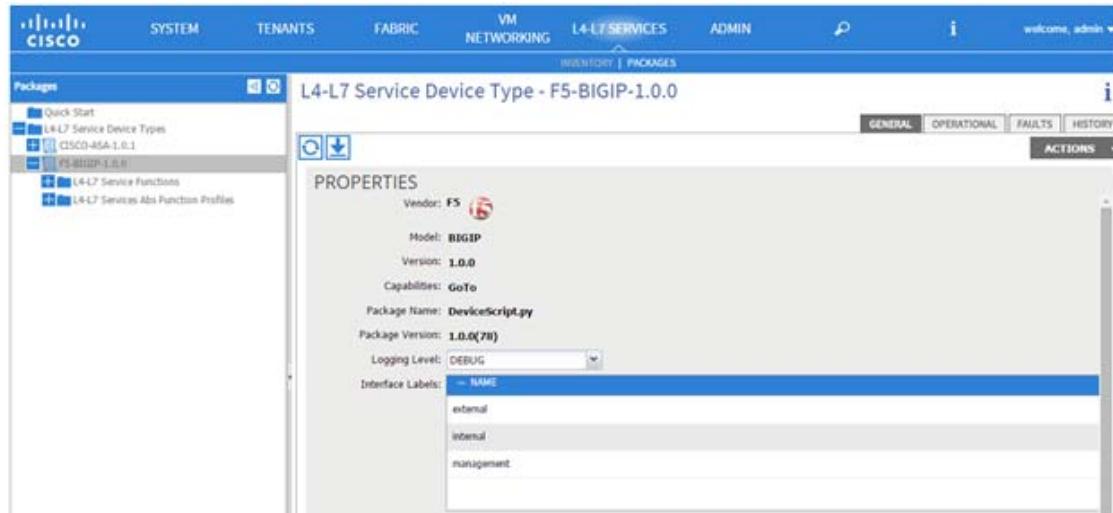
- Top Navigation:** SYSTEM, TENANTS, FABRIC, VM NETWORKING, L4-L7 SERVICES, ADMIN, welcome, admin ▾
- Left Sidebar:** Packages (selected), Quick Start, L4-L7 Service Device Types
- Central Content:** L4-L7 Service Device Types

VENDOR	MODEL	VERSION	FUNCTIONS
CISCO	ASA	1.0.1	Firewall
F5	BIGIP	1.0.0	Microsoft-SharePoint, Virtual-Server

L4-L7 Service Device Example

The Device Package defines the logical properties and functions available on the L4-L7 service. [Figure 7](#) captures the characteristics of an F5 Big-IP Application Delivery Controller (ADC). The vendor and model information is detailed as well as the capability of the device as a "GoTo" or "GoThrough" (not shown). This capability indicates if a packet is explicitly destined to the service or transparently processed by the device. Interface labels define the interfaces on the device that will be referenced to create service graphs.

Figure 7 Device Package Example



Configuring Connectivity to a Device Cluster

The following is required to begin configuration of the F5 device cluster via APIC.

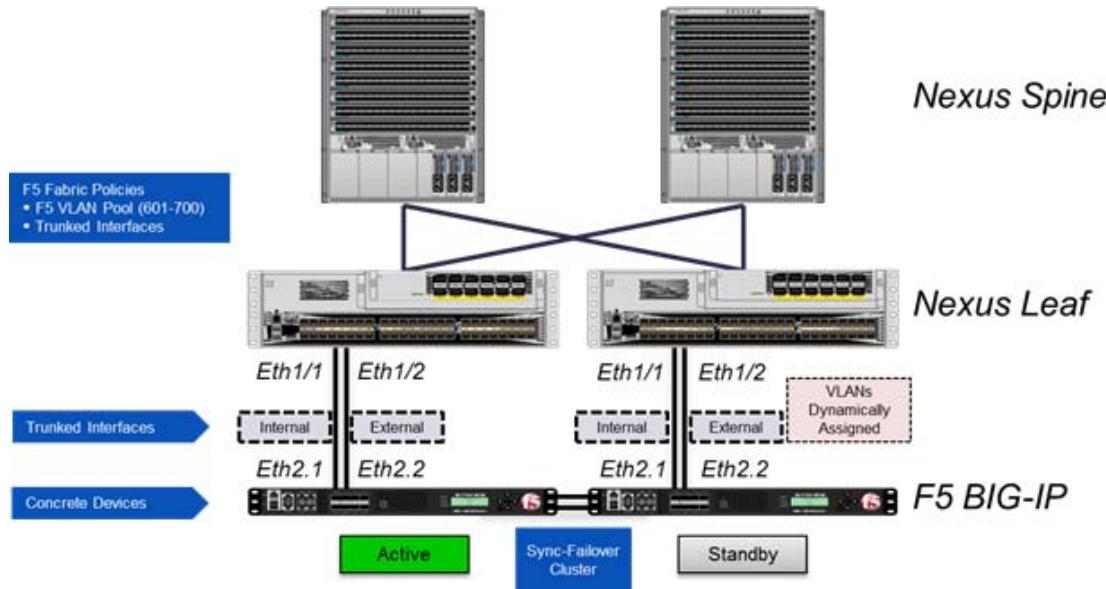
- The BIG-IP system must be cabled to a leaf switch and powered on (if using an appliance) or started in a VMware environment (if using a Virtual Edition).
- A management IP address and it must be accessible by the APIC environment.
- Access to an administrator-level account on the BIG-IP system.

The minimum requirements for the F5 BIG-IP implementation with Cisco ACI are:

- Cisco APIC v1.0(1e) and Switch software 11.0(1b)
- BIG-IP version 11.4.1 or later, running as a standalone BIG-IP system or in a BIG-IP cluster. This can be a physical appliance or a BIG-IP Virtual Edition (VE)
- F5 BIG-IP Device Package v1.0.0 for Cisco APIC v1.0(1e)

The internal and external interfaces on the BIG-IP system are connected to leaf nodes in the ACI architecture. Items such as web servers, database engines, and application tiers are also connected to leaf nodes. Spine nodes handle the routing between the BIG-IP system and the various other end points necessary to deliver an application service.

The management port of the BIG-IP system is connected out-of-band to a switch outside of the ACI architecture (not shown in the diagram) to provide management access. [Figure 8](#) details the physical connections between the BIG-IP system and the leaf nodes. The interface details are critical during the concrete device deployment.

Figure 8 Example Connectivity of F5 Big-IP Device Cluster

Configuring a Device Cluster (Logical Device)

A device cluster (also known as a logical device) is one or more concrete devices that act as a single L4-L7 device. A concrete device has concrete interfaces that are mapped or added to the logical interfaces of the device cluster (logical device) when associated. The device cluster is defined within a tenant and can be exported to support multiple context (VRFs or tenants) depending on the capabilities of the specific service device package.



Note This appendix assumes that the tenant constructs (bridge domains, application profiles, EPGs, contracts etc.) have already been created based on the best practices documented above.

To centralize the deployment of shared services a "Service Tenant" was created to host multiple device clusters (logical devices) and their associated concrete devices. From this central service tenant the logical device cluster can be exported to other tenants on the fabric requiring the service functionality.

The Create Device Cluster wizard needs to be completed to create a device cluster in the APIC GUI. The following captures the deployment of an F5 BIG-IP service within the "Service Tenant" tenant.

1. From the Quick Start work pane click Configure a device cluster. The Create Device Cluster form appears. All red flagged fields are required.

CREATE DEVICE CLUSTER

STEP 1 > CLUSTER 1. CLUSTER 2. DEVICES 3. PARAMETERS

Please enter cluster info below.

Name:	<input type="text"/>	!
Device Package:	<input type="text" value="select an option"/>	!
Context Aware:	<input checked="" type="radio"/> Multiple <input type="radio"/> Single	
Function Type:	<input checked="" type="radio"/> GoThrough <input type="radio"/> GoTo	
Device Type:	<input checked="" type="radio"/> PHYSICAL <input type="radio"/> VIRTUAL	
Physical Domain:	<input type="text" value="select an option"/>	!

Cluster Management Interface

EPG:	<input type="text" value="select an option"/>	!
Virtual IP Address:	<input type="text"/>	!
Port:	<input type="text"/>	!
Username:	<input type="text"/>	!
Password:	<input type="text"/>	!
Confirm Password:	<input type="text"/>	!

Logical Interfaces

Name	Type

[< PREVIOUS](#) [NEXT >](#) [CANCEL](#)

1. Complete the form.



Note The Device Package field is a drop down that contains all device packages currently imported into the APIC. The Physical Domain must already be defined in the Fabric - Access Policies - Physical and External Domains. This essentially identifies the dynamic VLAN pool with service devices. The default username and password for the F5 BIG-IP devices are admin/admin using port 443 for secure communications.

CREATE DEVICE CLUSTER

STEP 1 > CLUSTER 1. CLUSTER 2. DEVICES 3. PARAMETERS

Please enter cluster info below.

Name:	FS
Device Package:	F5-BIGIP-1.0.0
Context Aware:	<input checked="" type="radio"/> Multiple <input type="radio"/> Single
Function Type:	<input checked="" type="radio"/> GoThrough <input type="radio"/> GoTo
Device Type:	<input checked="" type="radio"/> PHYSICAL <input type="radio"/> VIRTUAL
Physical Domain:	pd-A08-F5

Cluster Management Interface

EPG:	select an option
Virtual IP Address:	172.26.163.106
Port:	443
Username:	admin
Password:	*****
Confirm Password:	*****

Logical Interfaces

+		X	
Name	Type		

< PREVIOUS NEXT > CANCEL

- Click + to add Logical Interface. The Name field is an arbitrary value.

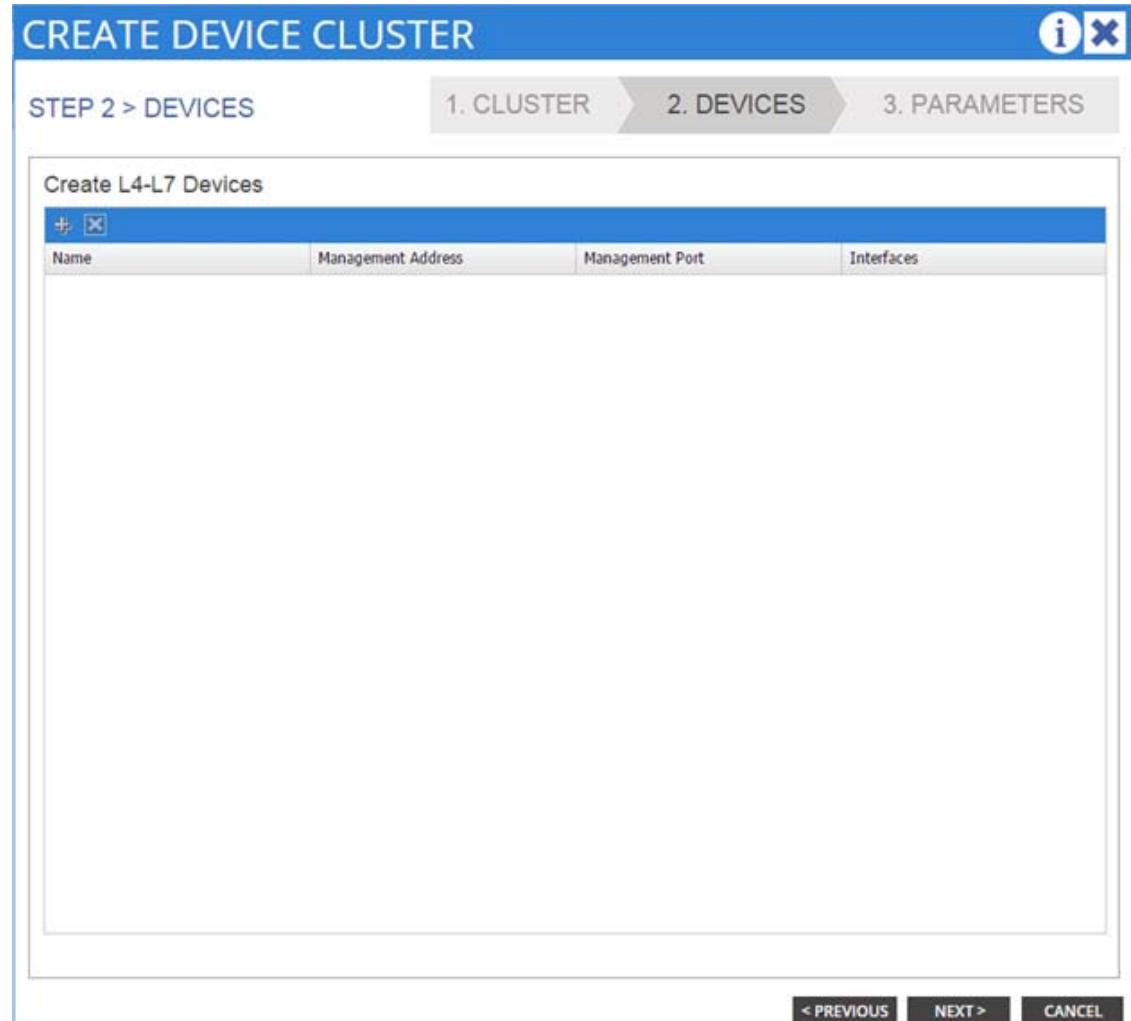
Logical Interfaces

+		X
Name	Type	
internal	internal	
external	external	
		UPDATE
		internal management

- Click Next. The Create Device Cluster STEP 2 > Devices form appears.

Configuring a Concrete Device

At this point the creation of concrete devices occurs within the same wizard.



4. Click + to create/define an L4-L7 device. The Create Concrete Device STEP 1 > Device form appears. All red flagged fields are required.

**Note**

It is strongly suggested to provide a context label as that maybe referenced during service graph instantiation.

CREATE CONCRETE DEVICE

i X

STEP 1 > DEVICE 1. DEVICE 2. PARAMETERS

Please enter device info below.

Name: ⓘ

Context Label:

Management Interface

IP Address: ⓘ

Port: ⓘ

Username: ⓘ

Password: ⓘ

Confirm Password: ⓘ

Interfaces

Name	Path	Logical Interface

< PREVIOUS NEXT > CANCEL

CREATE CONCRETE DEVICE

STEP 1 > DEVICE

1. DEVICE **2. PARAMETERS**

Please enter device info below.

Name: Context Label:

Management Interface

IP Address:
Port:
Username:
Password:
Confirm Password:

Interfaces

Name	Path	Logical Interface

< PREVIOUS **NEXT >** CANCEL

5. Click + to add interfaces.

CREATE CONCRETE DEVICE

STEP 1 > DEVICE 1. DEVICE 2. PARAMETERS

Please enter device info below.

Name:	bigip1
Context Label:	ADC1

Management Interface

IP Address:	172.26.163.106
Port:	443
Username:	admin
Password:	*****
Confirm Password:	*****

Interfaces

Name	Path	Logical Interface
2_1	Node-301/eth1/1	external
2_2	Node-301/eth1/2	internal

Note

The use of an "_" underscore to define the interfaces on the BIG-IP system. Be sure to replace the traditional ":" period of the F5 interface identifier.

Note

The logical interfaces that must be defined are dependent on the specific Device Package. This example is built using an F5 service package.

Note

The parameters in this field are dependent on the specific Device Package. This example is built using an F5 service package.

6. The Name field is arbitrary and the Path value is dependent on the physical connectivity of the device.

Note The use of an "_" underscore to define the interfaces on the BIG-IP system. Be sure to replace the traditional ":" period of the F5 interface identifier.

7. Click update for each interface.

Note The logical interfaces that must be defined are dependent on the specific Device Package. This example is built using an F5 service package.

8. Click Next to proceed. The Create Concrete Device STEP 2 > Parameters form appears

Note The parameters in this field are dependent on the specific Device Package. This example is built using an F5 service package.

CREATE CONCRETE DEVICE

STEP 2 > PARAMETERS

1. DEVICE 2. PARAMETERS

Please enter value for device folder and parameters.

FOLDER/PARAM	NAME	VALUE
+ DeviceInterface		
+ DeviceRoute		
+ HighAvailability		
+ HostConfig		

< PREVIOUS OK CANCEL

- The Parameters form requires that you double-click the FOLDER/PARAM field to enter name value pairs. If you intend to complete a specific field within a folder you must provide a name for the folder as shown in the example below. The "HighAvailability" folder requires a name entry to complete the remaining parameters with the folder. Click Update upon completion.

- The screenshot below illustrates parameter name value pair entries. The name value is arbitrary. Click Update upon completion.



Note Not all folder and parameter values are required. Please check the documentation regarding the specific device package being implemented.

- Complete the folder and parameter values entry. The screenshot below captures the required entries to deploy a BIG-IP HA Sync-Failover group.

CREATE CONCRETE DEVICE

STEP 2 > PARAMETERS

1. DEVICE 2. PARAMETERS

Please enter value for device folder and parameters.

FOLDER/PARAM	NAME	VALUE
<input type="checkbox"/> DeviceInterface		
<input type="checkbox"/> DeviceRoute		
<input checked="" type="checkbox"/> HighAvailability - HA	HA	
<input checked="" type="checkbox"/> Interface - interface	interface	1_1
<input checked="" type="checkbox"/> SelfIPAddress - selfip	selfip	5.5.5.1
<input checked="" type="checkbox"/> SelfIPNetmask - selfmask	selfmask	255.255.255.0
<input checked="" type="checkbox"/> VLAN - vlan	vlan	20
<input type="checkbox"/> HostConfig - HostConfig	HostConfig	
<input type="checkbox"/> DNSServerPrimary		
<input type="checkbox"/> DNSServerSecondary		
<input checked="" type="checkbox"/> HostName - Hostname	Hostname	bigip1.acidc.local
<input checked="" type="checkbox"/> NTPServer - ntp	ntp	172.26.163.254
<input type="checkbox"/> SyslogServer		

< PREVIOUS OK CANCEL

12. Click OK. The concrete device configuration is summarized in the window.
13. Click + in the Create L4-L7 Devices pane to add another device. [Figure 9](#) through [Figure 12](#) capture the definition of the second device in the F5 BIG-IP deployment. This is the exact same workflow as the previously defined workflow.

Figure 9 Create L4-L7 Devices



Figure 10 Example of second F5 Concrete Device

CREATE CONCRETE DEVICE

STEP 1 > DEVICE 1. DEVICE 2. PARAMETERS

Please enter device info below.

Name: bigip2
Context Label: ADC2

Management Interface

IP Address: 172.26.163.107
Port: 443
Username: admin
Password: *****
Confirm Password: *****

Interfaces

Name	Path	Logical Interface
2_1	Node-302/eth1/1	internal
2_2	Node-302/eth1/2	external

< PREVIOUS NEXT > CANCEL

Figure 11 Completed Example Parameter Form using F5 BIG-IP Device Package for Second Concrete Device

CREATE CONCRETE DEVICE

STEP 2 > PARAMETERS

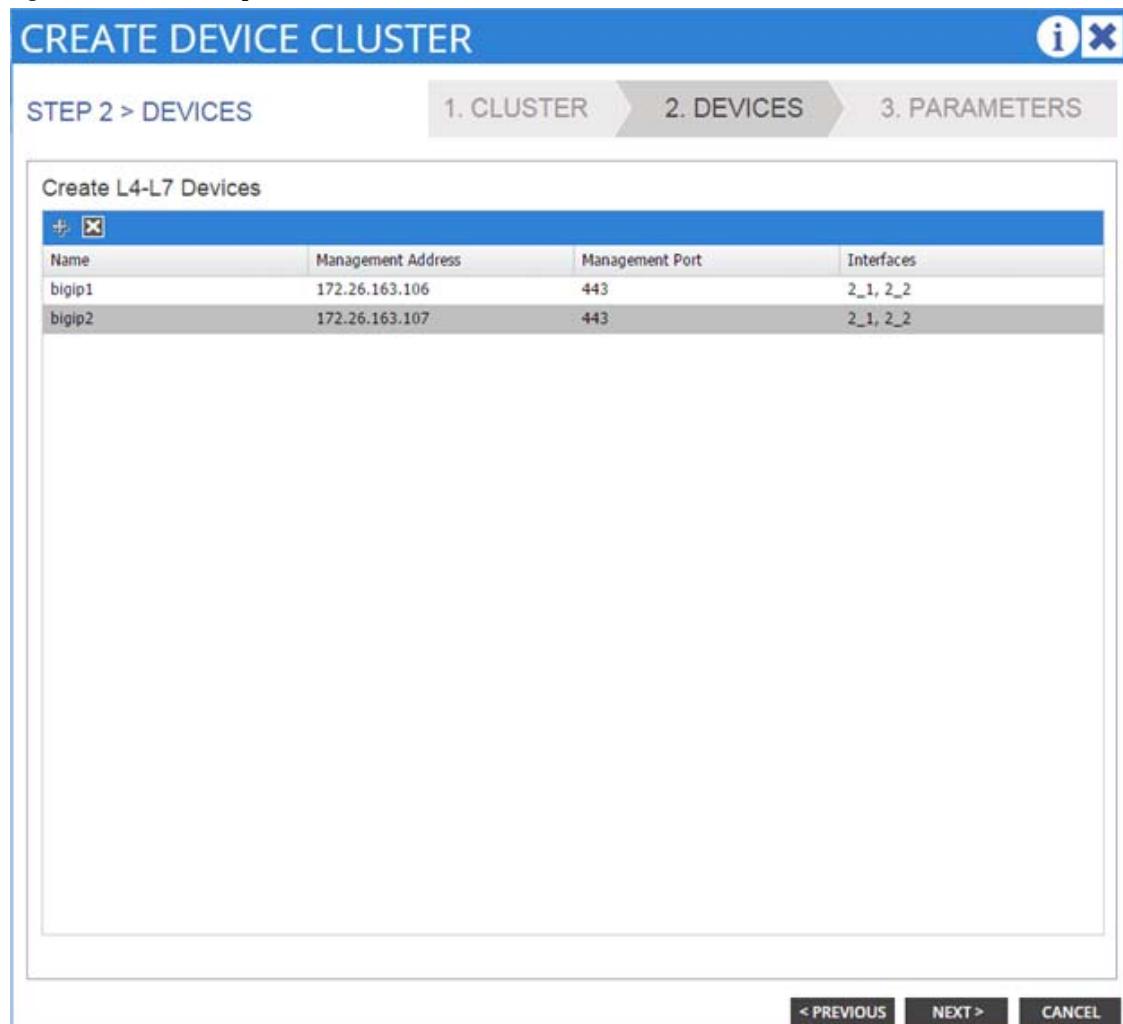
1. DEVICE 2. PARAMETERS

Please enter value for device folder and parameters.

FOLDER/PARAM	NAME	VALUE
<input type="checkbox"/> DeviceInterface		
<input type="checkbox"/> DeviceRoute		
<input checked="" type="checkbox"/> HighAvailability - HA	HA	
<input checked="" type="checkbox"/> Interface - Interface	interface	1_1
<input checked="" type="checkbox"/> SelfIPAddress - selfip	selfip	5.5.5.2
<input checked="" type="checkbox"/> SelfIPNetmask - selfmask	selfmask	255.255.255.0
<input checked="" type="checkbox"/> VLAN - vlan	vlan	20
<input type="checkbox"/> HostConfig - HostConfig	HostConfig	
<input type="checkbox"/> DNSServerPrimary		
<input type="checkbox"/> DNSServerSecondary		
<input checked="" type="checkbox"/> HostName - Hostname	Hostname	bigip2.acdc.local
<input checked="" type="checkbox"/> NTPServer - ntp	ntp	172.26.163.254
<input type="checkbox"/> SyslogServer		

< PREVIOUS OK CANCEL

Figure 12 Completed L4-L7 Devices



14. Click Finish.



Verifying L4-L7 Device Cluster on APIC

In the tenant where the device cluster resides expand the "L4-L7 Services" folder in the left navigation pane and expand the "Device Clusters" folder. The name given the device cluster should appear as a folder. Expanding the device cluster instance should reveal a number of concrete devices and logical interfaces.

[Figure 13](#) illustrate an F5 logical device cluster with two concrete BIG-IP devices defined as "bigip1" and "bigip2". The device cluster uses two logical interfaces namely "external" and "internal" that are defined on each concrete device.

Figure 13 Logical Device Cluster

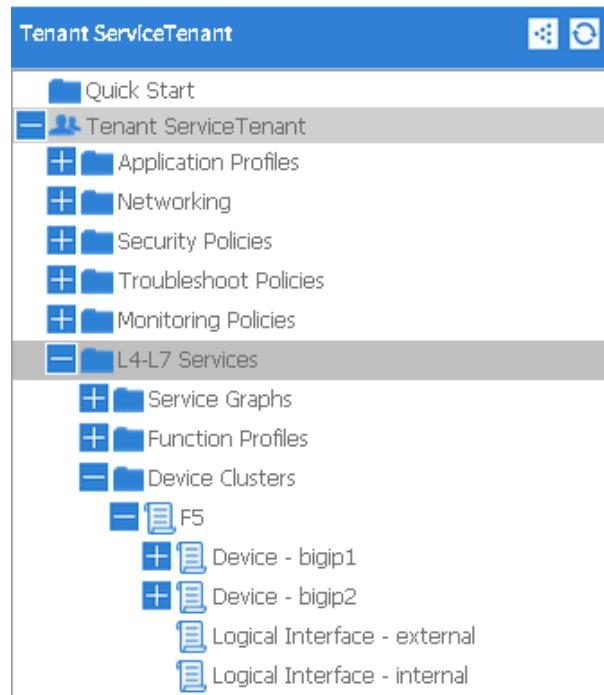


Figure 14 Device Cluster Deployment Example

The screenshot shows a web-based management interface for a device cluster named 'F5'. The top navigation bar includes tabs for POLICY, OPERATIONAL, FAULTS, and HISTORY, along with an ACTIONS button.

PROPERTY:

- Name: F5
- Device Package: F5-BIGIP-1.0.0
- Context Aware: Multiple Single
- Function Type: GoThrough GoTo
- Device Type: PHYSICAL
- Physical Domain: pd-A08-F5
- Device State: stable
- Config Issues:

CLUSTER MANAGEMENT INTERFACE:

- EPG: select or type to pre-pop
- Virtual IP Address: 172.26.163.106
- Port: 443
- Username: admin
- Password: *****
- Confirm Password: *****

LOGICAL INTERFACES:

NAME	TYPE	CONCRETE INTERFACES
external	external	bigip1/[2_2], bigip2/[2_2]
internal	internal	bigip1/[2_1], bigip2/[2_1]

DEVICES:

NAME	MANAGEMENT ADDRESS	MANAGEMENT PORT	INTERFACES
bigip1	172.26.163.106	443	2_1, 2_2
bigip2	172.26.163.107	443	2_1, 2_2

The "POLICY" tab under each concrete device will indicate the state of the configuration, health as well as reflect the management and physical interface properties.

Concrete Device - Device - bigip1

PROPERTIES

Name: bigip1
Configuration State: stable
Context Label: ADC1
Management Address: 172.26.163.106
Management Port: 443
Mapped Host Address: 0.0.0.0
Username: admin
Password:
Confirm Password:
Interfaces:

NAME	PATH	LOGICAL INTERFACE
2_1	Node-301/eth1/1	internal
2_2	Node-301/eth1/2	external

The "OPERATIONAL" tab reflects the entries made in the parameter form wizard. In this example, the F5 HA configuration and host information.

Concrete Device - Device - bigip1

PARAMETERS

META FOLDER/PARAM KEY	FOLDER/PARAM INSTANCE NAME	VALUE
HighAvailability	HA	
Interface	interface	1_1
SelfIPAddress	selfip	5.5.5.1
SelfIPNetmask	selfmask	255.255.255.0
VLAN	vlan	20
HostConfig	Hostconfig	
HostName	hostname	bigip1.acdc.local
NTPServer	ntp	172.26.163.254

The Logical Interfaces for the device cluster should be checked to confirm the physical interfaces on the device have been dedicated to the logical service and reflect a "formed" state.

Logical Interface -- external

PROPERTIES

Name: external
Type: F5-BIGIP-1.0.0/external
Concrete Interfaces:

DEVICE	INTERFACE	STATE
bigip1	[2_2]	formed
bigip2	[2_2]	formed



Verifying L4-L7 Device Cluster on F5 BIG-IP

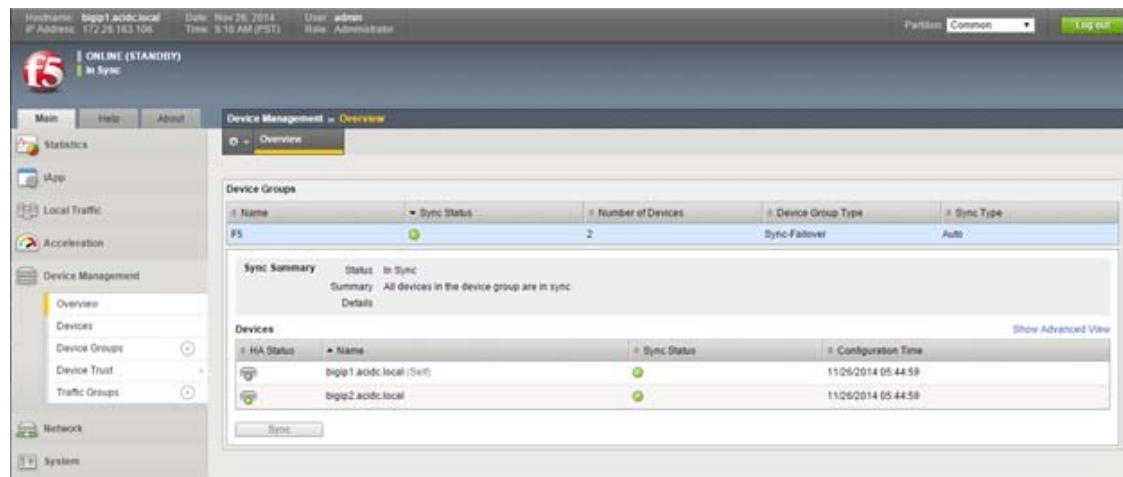
The F5 BIG-IP platforms are deployed in an HA pair as endpoints to the ACI fabric. After logging into the GUI of one or both F5 platforms you can immediately determine if integration was successful. Please refer to [Figure 15](#). The upper left hand corner of the BIG-IP GUI will display the hostname assigned by APIC and the management IP address defined as a pre-requisite. In addition, the date and time should align to your NTP server again defined via APIC. The state of the BIG-IP device (ACTIVE or STANDBY) and its SYNC status relative to the device group point to the success of the implementation.

Using the left navigation click "Device Management". The "Overview" panel will indicate the state of the cluster and the two concrete devices defined with Cisco APIC. In this example, there are two "In Sync" F5 BIG-IP appliances.

Figure 15 BIG-IP Example - Device Overview Page Active Unit

HA Status	Name	Sync Status	Configuration Time
Active	bigip1.acid.local	Sync	11/26/2014 05:44:59
Standby	bigip2.acid.local (Standby)	Sync	11/26/2014 05:44:59

Figure 16 the Standby unit's state.

Figure 16 BIG-IP Example - Device Overview Page Standby Unit

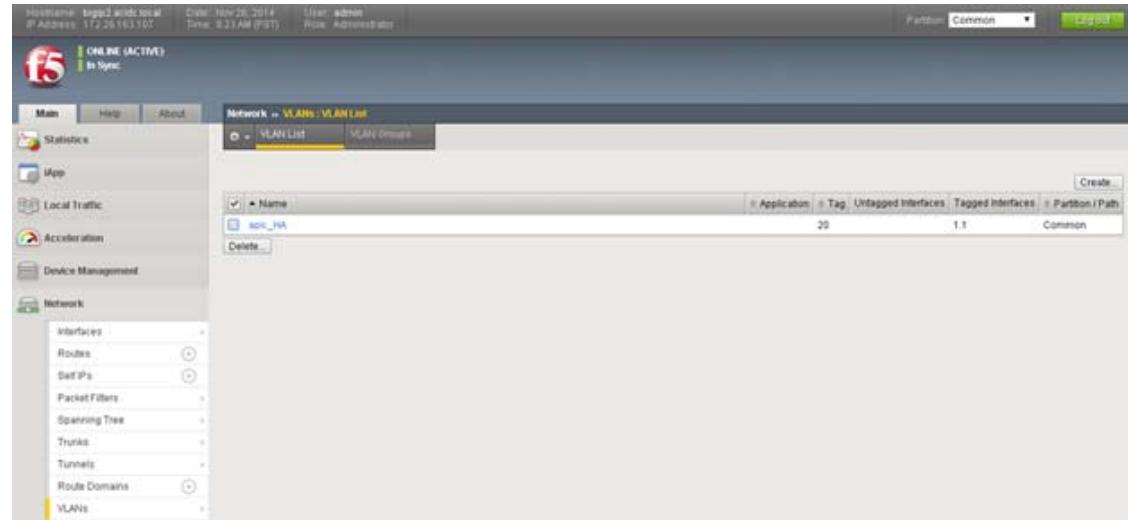
If further validation of the deployment is required there are a number of screens in the GUI that reflect the parameters sent via the APIC concrete device deployment.

The following checks can be made and will reflect the variables entered in the APIC:

1. From the Main navigation menu click Network and then click Self IPs to confirm HA IP address assignment.



2. From the Main navigation menu click Network and then click VLANs to confirm HA VLAN assignment.



Exporting a Device Clusters

Device clusters can be exported to enable sharing of device clusters among tenants. This means if a service device is dedicated to a tenant, you should perform the previous logical and concrete device configuration steps within the tenant context using the service. Exporting the device cluster service is not necessary. If a service device is shared across multiple tenants, you should configure the following in the management (mgmt.) tenant or common service tenant and then export it to the desired tenant.



Note The previous sections assumed the use of a common "Service Tenant" to house shared services.

To share a device cluster from the "Service Tenant" with another tenant, complete the following steps:

- From the Service Tenant in the left navigation pane expand L4-L7 Services.
- In the left navigation pane click Device Clusters.
- In the Device Clusters work pane click Actions.
- Select Export Device Cluster.

CLUSTER NAME	CONTEXT AWARE	FUNCTION TYPE	VENDOR	MGMT IP
FS	Multiple	GoTo	F5	172.26.163.106



Note In the figure above, the F5 cluster device supports multiple contexts meaning this service can be exported to multiple ACI tenants.

The Export Device Cluster form appears.

EXPORT DEVICE CLUSTER

Choose a device cluster and a tenant to export

Device Cluster: select an option

Tenant: select a tenant

Description:

SUBMIT CANCEL

5. Select the device cluster
6. Select the tenant. This is the tenant who will "import" the service.
7. Optionally provide a description of the device cluster service.
8. Click Submit upon completion of the form

The following screenshots capture the export of an F5 BIG-IP device cluster to a tenant. This service may be exported to multiple tenants allowing the central definition of the device cluster and associated concrete devices within the "Service Tenant" and partitioning of the F5 device to support multiple tenants or applications in the ACI fabric.

EXPORT DEVICE CLUSTER

Choose a device cluster and a tenant to export

Device Cluster: select an option

Tenant: F5

Description: Create Device Cluster

SUBMIT CANCEL

EXPORT DEVICE CLUSTER

Choose a device cluster and a tenant to export

Device Cluster: F5

Tenant: !

Description: Exchange
Foundation
infra
mgmt
mztest
SharePoint

SUBMIT **CANCEL**

EXPORT DEVICE CLUSTER

Choose a device cluster and a tenant to export

Device Cluster: F5

Tenant: SharePoint

Description: Application Network Services

SUBMIT **CANCEL**

Verify the Export of a Device Cluster

The F5 BIG-IP services are made readily available to any tenant in the data center through the abstraction offered by the fabric and in particular the export feature. [Figure 17](#) shows the successful exportation of the F5 service to the "SharePoint" tenant. [Figure 18](#) is a screen shot captured from the SharePoint Tenant showing the successful importation of the F5 BIG-IP device cluster. At this point the "SharePoint" tenant can deploy service graphs with F5 based functions abstracted from the concrete implementation defined centrally in the "Service Tenant".

Figure 17 Example of Exported Device Cluster

Device Clusters

CLUSTER NAME	CONTEXT AWARE	FUNCTION TYPE	VENDOR	MGMT IP	ACTIONS
F5	Multiple	GoTo	F5	172.26.163.106	

Figure 18 Example of Imported Device Cluster

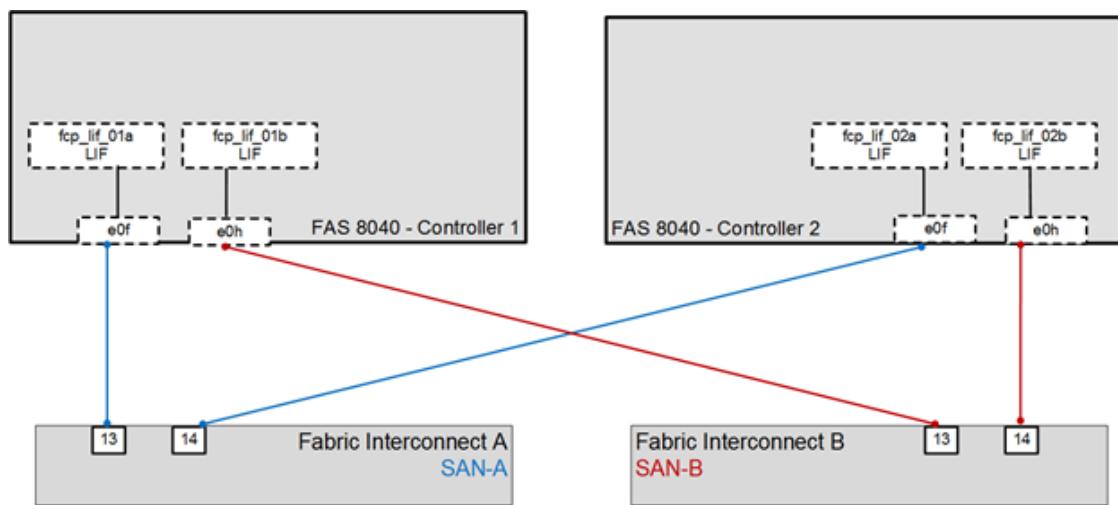
References

[Cisco APIC Layer 4 to Layer 7 Services Deployment Guide](#)

Appendix C - Deploying Direct Connect FCoE

This section details the additional configuration to setup FCoE Boot using direct connection between FAS 8040 and UCS FI. The FCoE boot configuration can be used in addition to or instead of iSCSI Boot. In this appendix, FCoE boot is configured and enabled to coexist with the iSCSI boot option. Customers can choose to replace the appropriate iSCSI specific sections of the main deployment guide with the FCoE sections in this appendix.

To support FCoE direct attached storage, the following additional physical connectivity is required, as illustrated in [Figure 19](#):

Figure 19 FCoE Direct Attached Storage

Storage Configuration

FCP Service in Clustered Data ONTAP

1. Create the FCP service on each Vserver. This command also starts the FCP service and sets World Wide Nodename (WWNN) of the Vserver.

```
fcp create -vserver Infra_Vserver
fcp show
```

Create LUNs in Clustered Data ONTAP

1. Create two boot LUNS: VM-Host-Infra-01 and VM-Host-Infra-02.

```
lun create -vserver Infra_Vserver -volume esxi_boot -lun VM-Host-Infra-01
-size 10GB -ostype vmware -space-reserve disabled
lun create -vserver Infra_Vserver -volume esxi_boot -lun VM-Host-Infra-02
-size 10GB -ostype vmware -space-reserve disabled
```

FCoE LIF in Clustered Data ONTAP

1. Create FCoE logical interfaces (LIFs).

```
network interface create -vserver Infra_Vserver -lif fcp_lif01a -role data
-data-protocol fcp -home-node <<var_node01>> -home-port 0f -status-admin up

network interface create -vserver Infra_Vserver -lif fcp_lif01b -role data
-data-protocol fcp -home-node <<var_node01>> -home-port 0h -status-admin up

network interface create -vserver Infra_Vserver -lif fcp_lif02a -role data
-data-protocol fcp -home-node <<var_node02>> -home-port 0f -status-admin up

network interface create -vserver Infra_Vserver -lif fcp_lif02b -role data
-data-protocol fcp -home-node <<var_node02>> -home-port 0h -status-admin up

network interface show -vserver Infra_Vserver
```

Place Cisco UCS Fabric Interconnects in Fiber Channel Switching Mode

To use FCoE Appliance Ports, the CiscoUCS Fabric Interconnects must be placed in Fiber Channel Switching Mode. Complete the following steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane.
2. Expand Fabric Interconnects and select Fabric Interconnect B.



Note

This next step will reboot both Cisco UCS Fabric Interconnects. If any servers are running on this system, they should be shut down before this step is executed.

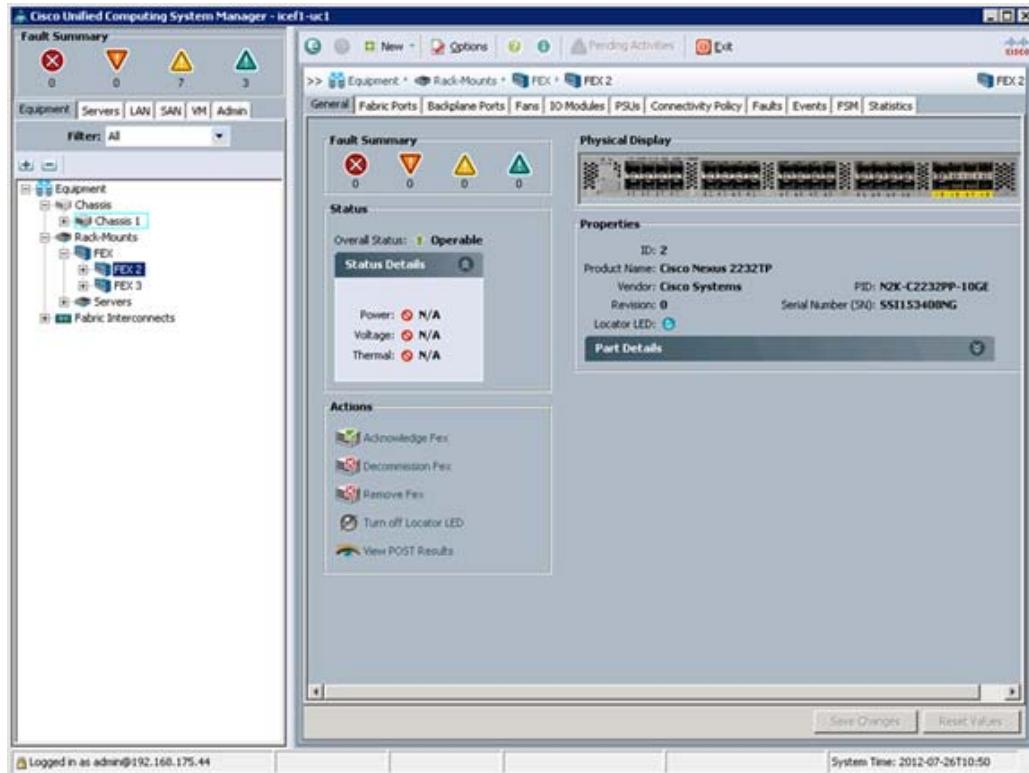
3. In the Actions pane, select Set FC Switching Mode. Click Yes. Click OK.
4. After the Fabric Interconnects have rebooted, log back into UCS Manager.
5. Expand Fabric Interconnects and select Fabric Interconnects.

- For each Fabric Interconnect, verify under Status that the FC Mode is now Switch.

Enable FCoE Storage Ports

To enable FCoE ports, complete the following steps:

- In Cisco UCS Manager, click the Equipment tab in the navigation pane.
- Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module.
- Expand Ethernet Ports.
- Select ports 13 and 14 that are connected to the FCoE ports on the storage controllers, right-click them, and select Configure as FCoE Storage Port. Click Yes to confirm.
- Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.
- Expand Ethernet Ports.
- Select ports 13 and 14 that are connected to the FCoE ports on the storage controllers, right-click them, and select Configure as FCoE Storage Port. Click Yes to confirm.



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

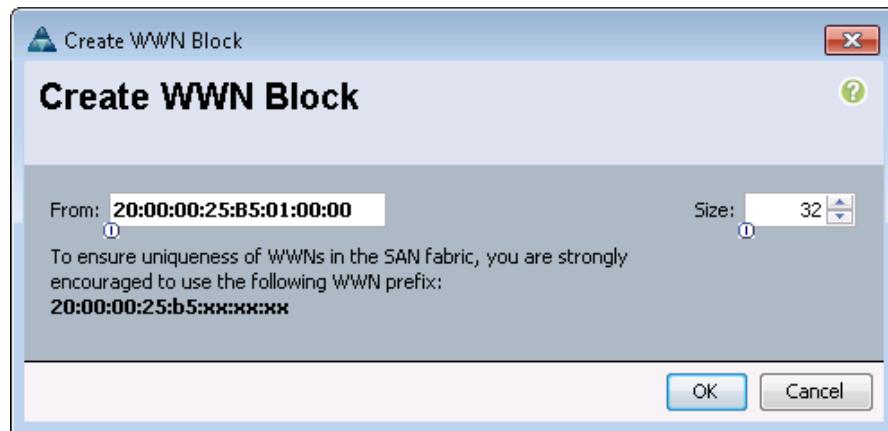
Create a WWNN Pool for FCoE Boot

To configure the necessary WWNN pool for the Cisco UCS environment, complete the following steps.

Cisco UCS Manager

- Select the SAN tab on the left.

2. Select Pools > root.
3. Right-click WWNN Pools under the root organization.
4. Select Create WWNN Pool to create the WWNN pool.
5. Enter WWNN_Pool for the name of the WWNN pool.
6. Optional: Enter a description for the WWNN pool.
7. Select Sequential for Assignment Order.
8. Click Next.
9. Click Add.
10. Modify the From field as necessary for this UCS Environment.
11. Specify a size of the WWNN block sufficient to support the available server resources.
12. Click OK.



13. Click Finish.
14. In the message box that displays, click OK.

Create WWPN Pools

To configure the necessary WWPN pools for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Select Pools > root.



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

3. Right-click WWPN Pools under the root organization.
4. Select Create WWPN Pool to create the WWPN pool.
5. Enter WWPN_Pool_A as the name of the WWPN pool.
6. Optional: Enter a description for the WWPN pool.
7. Select Sequential for Assignment Order.
8. Click Next.

9. Click Add.
10. Specify a starting WWPN.



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

11. Specify a size for the WWPN pool that is sufficient to support the available blade or server resources.

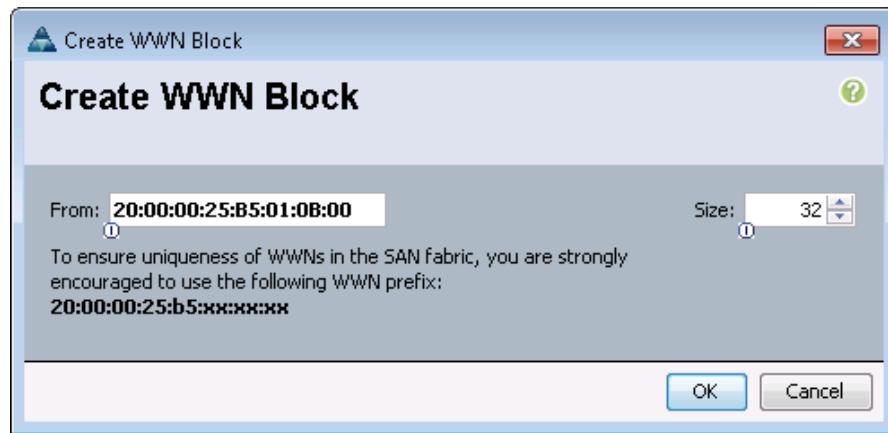


12. Click OK.
13. Click Finish.
14. In the confirmation message, click OK.
15. Right-click WWPN Pools under the root organization.
16. Select Create WWPN Pool to create the WWPN pool.
17. Enter WWPN_Pool_B as the name of the WWPN pool.
18. Optional: Enter a description for the WWPN pool.
19. Select Sequential for Assignment Order.
20. Click Next.
21. Click Add.
22. Specify a starting WWPN.



Note For the FlexPod solution, it is recommended 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.

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



24. Click OK.
25. Click Finish.
26. In the confirmation message, click OK.

Create Server Pool

To configure specific server pool for servers supporting FCoE boot, complete the following steps:



Note 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. Select Pools > root.
3. Right-click Server Pools.
4. Select Create Server Pool.
5. Enter `Infra_FCoE_Pool` as the name of the server pool.
6. Optional: Enter a description for the server pool.
7. Click Next.
8. Select two (or more) servers to be used for the VMware management cluster and click `>>` to add them to the `Infra_FCoE_Pool` server pool.
9. Click Finish.
10. Click OK.

Assign VSANs to FCoE Storage Ports

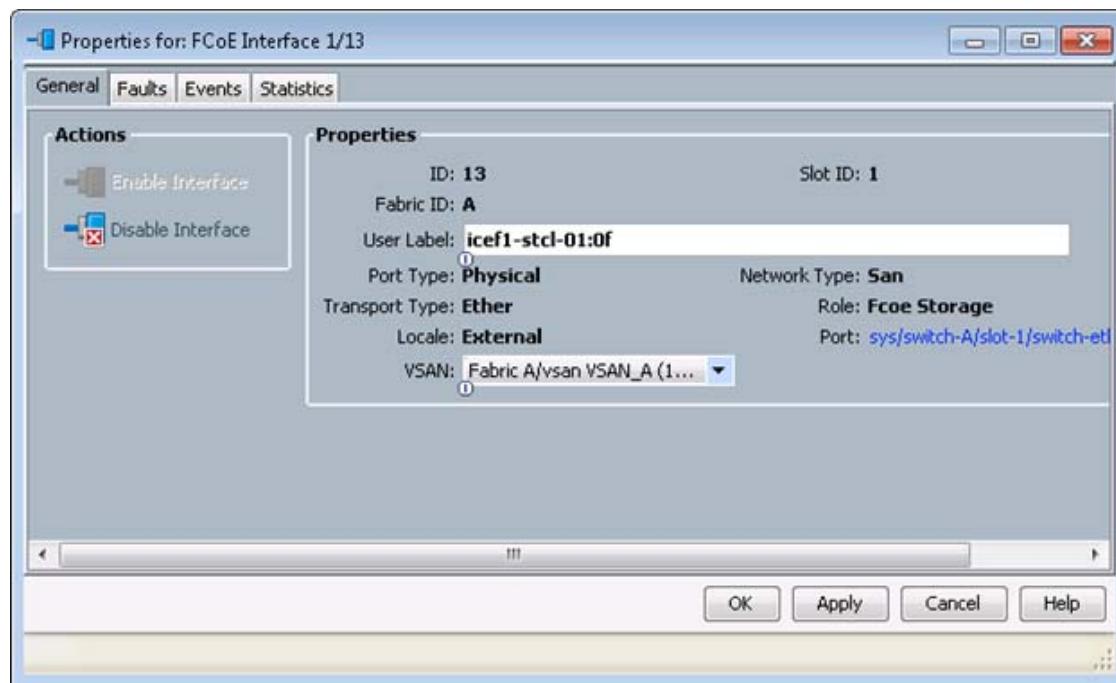
To assign the necessary virtual storage area networks (VSANs) to the FCoE Storage Ports for the Cisco UCS environment, complete the following steps:

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



Note In this procedure, two VSANs are created.

2. Select SAN > Storage Cloud.
3. Expand Fabric A and Storage FCoE Interfaces.
4. Right-click FCoE Interface 1/13 and select Storage FCoE.
5. Set the User Label to the storage controller name and port that this interface is connected to.
6. Select VSAN_A as the VSAN.
7. Click OK.



Create VSANs

To configure the necessary virtual storage area networks (VSANs) for the Cisco UCS environment, complete the following steps:

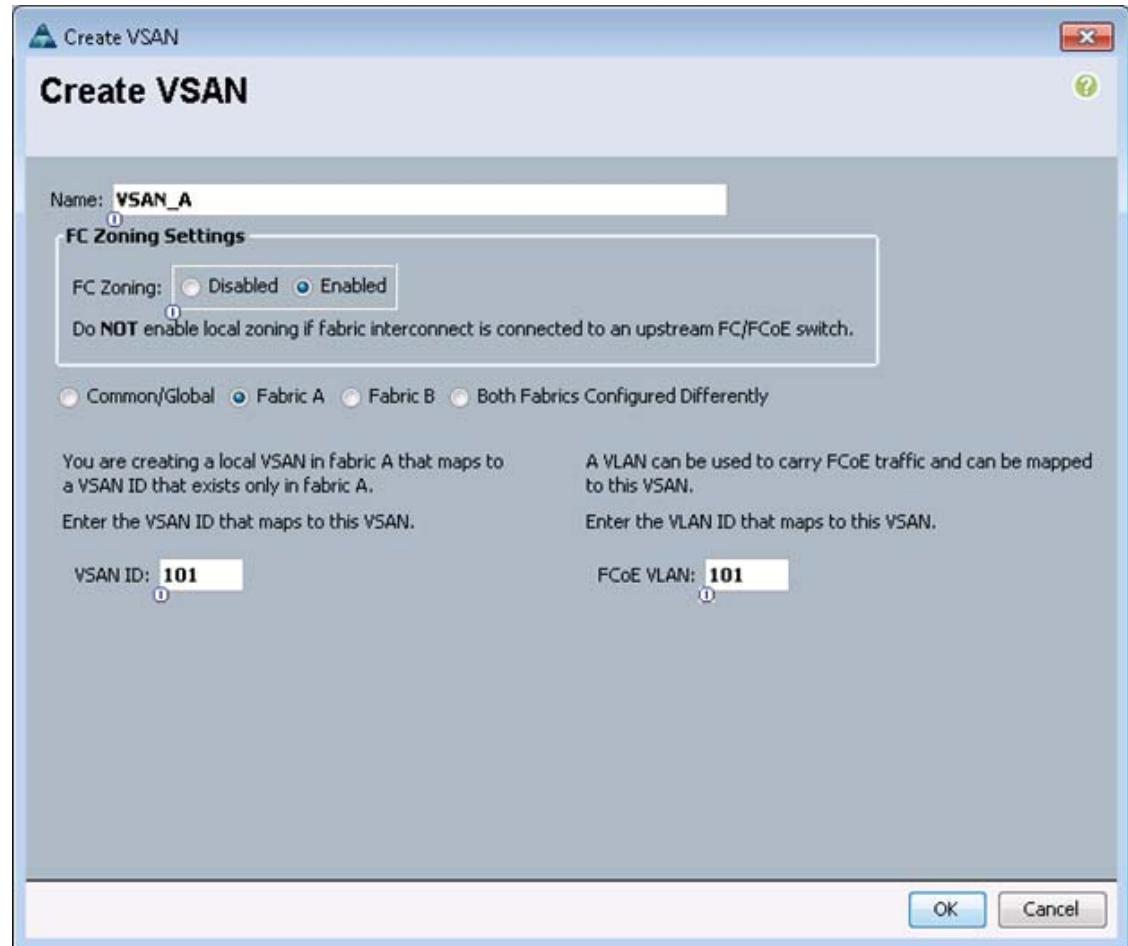
1. In Cisco UCS Manager, click the SAN tab in the navigation pane.



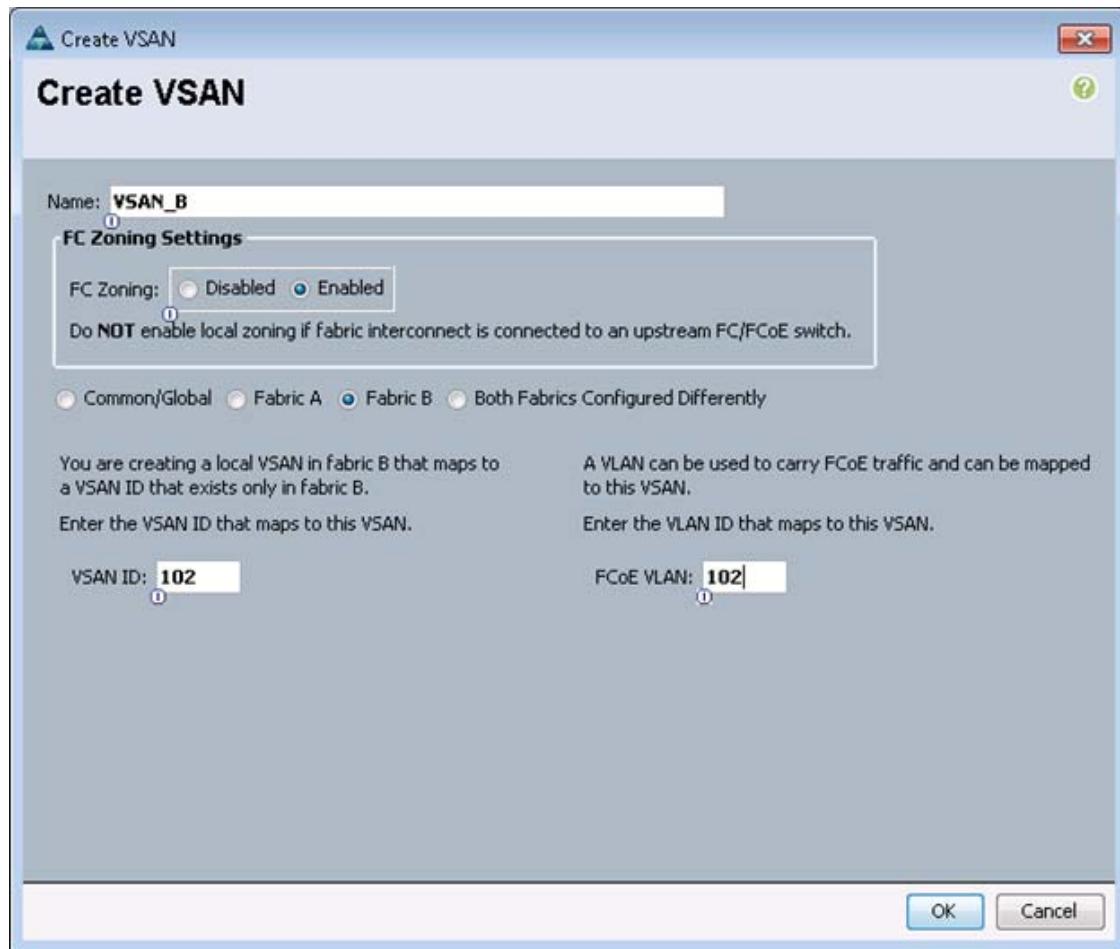
Note In this procedure, two VSANs are created.

2. Select SAN > SAN Cloud.
3. Right-click VSANs.
4. Select Create VSAN.
5. Enter VSAN_A as the name of the VSAN to be used for Fabric A
6. Select Enabled for FC Zoning.
7. Select Fabric A.
8. Enter a unique VSAN ID and a corresponding FCoE VLAN ID. It is recommended use the same ID for both parameters and to use something other than 1.

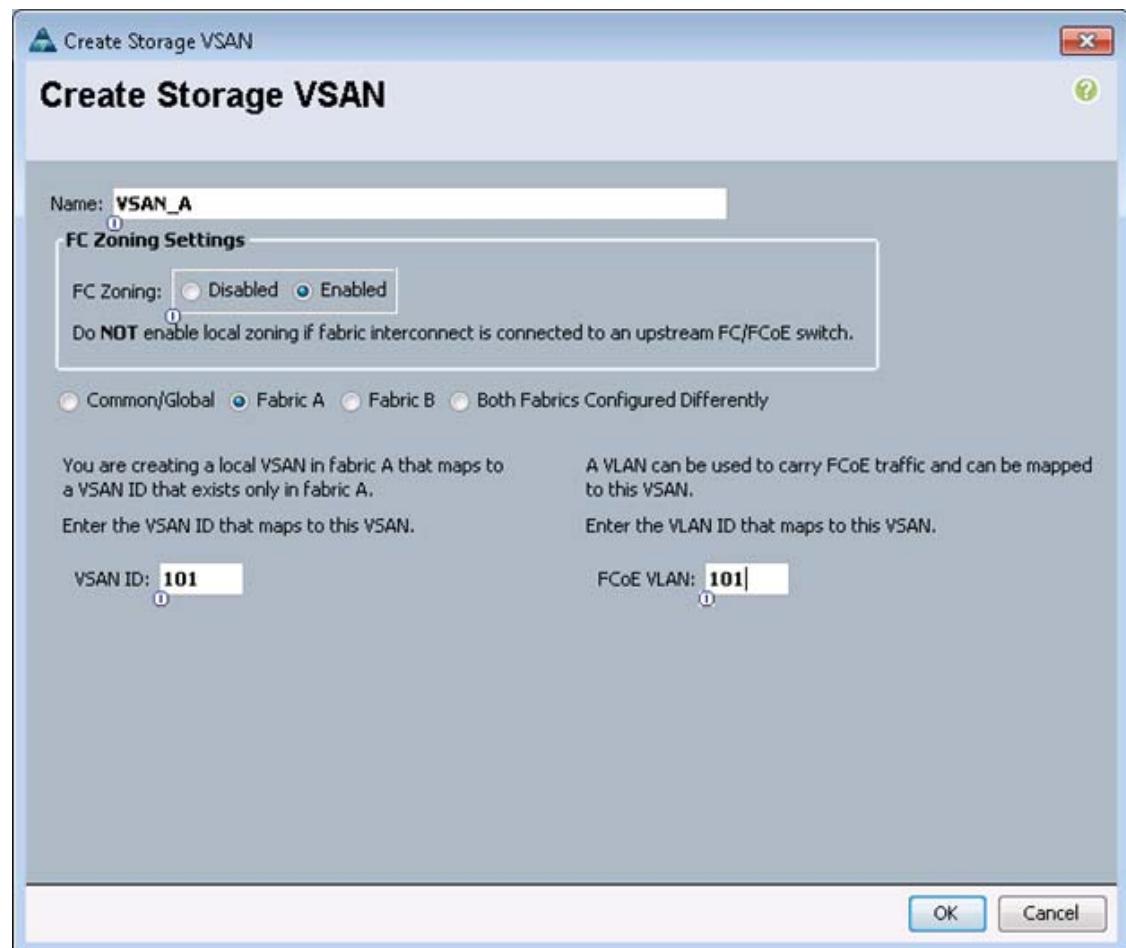
9. Click OK, and then click OK again.



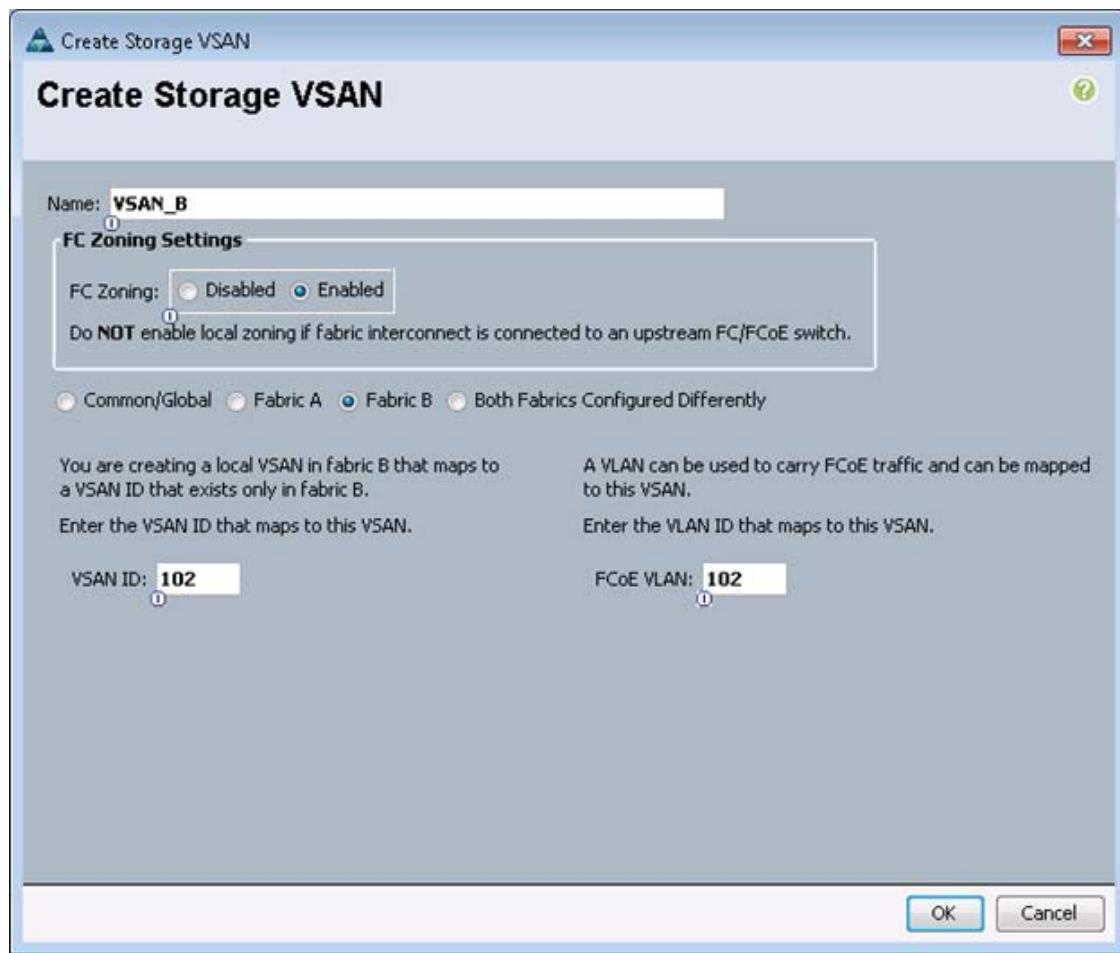
10. Under SAN Cloud, right-click VSANs.
11. Select Create VSAN.
12. Enter VSAN_B as the name of the VSAN to be used for Fabric B.
13. Select Enabled for FC Zoning.
14. Select Fabric B.
15. Enter a unique VSAN ID and a corresponding FCoE VLAN ID. It is recommended to use the same ID for both parameters and to use something other than 1.
16. Click OK, and then click OK again.



17. Under Storage Cloud, right-click VSANs.
18. Select Create Storage VSAN.
19. Enter VSAN_A as the name of the VSAN to be used for Fabric A.
20. Select Enabled for FC Zoning.
21. Select Fabric A.
22. Enter the same unique VSAN ID and corresponding FCoE VLAN ID that you entered for Fabric A above.
23. Click OK, and then click OK again.



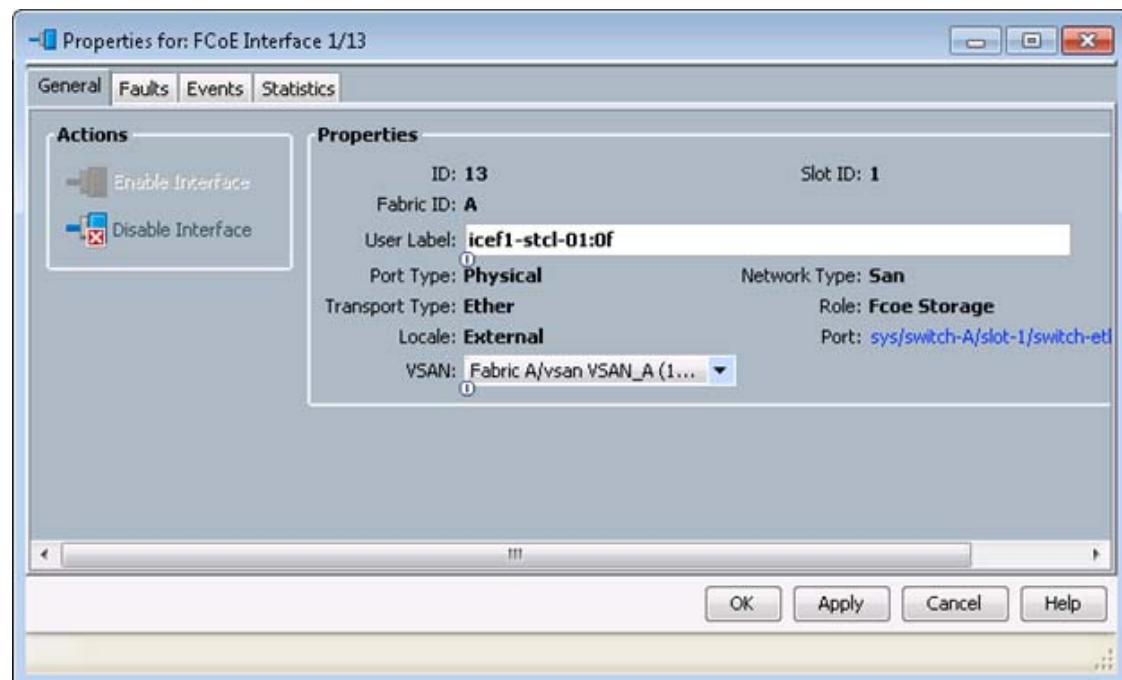
24. Under Storage Cloud, right-click VSANs.
25. Select Create Storage VSAN.
26. Enter VSAN_B as the name of the VSAN to be used for Fabric B.
27. Select Enabled for FC Zoning.
28. Select Fabric B.
29. Enter the same unique VSAN ID and corresponding FCoE VLAN ID that you entered for Fabric B above.
30. Click OK, and then click OK again.



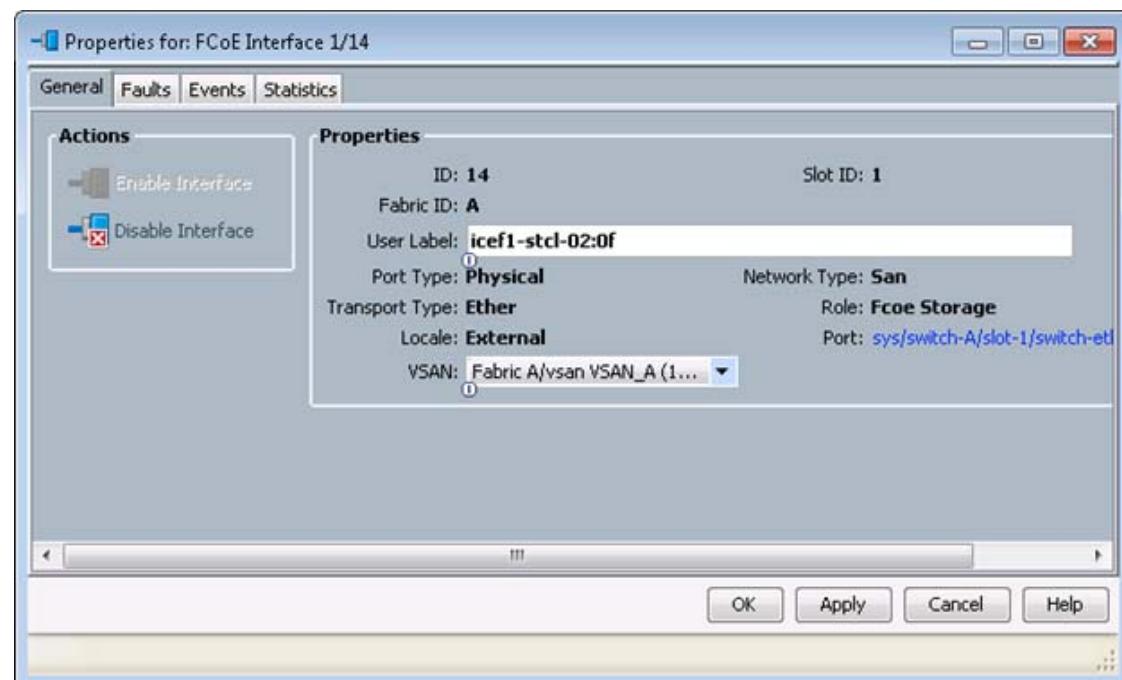
Assign VSANs to FCoE Storage Ports

To assign the necessary virtual storage area networks (VSANs) to the FCoE Storage Ports for the Cisco UCS environment, complete the following steps:

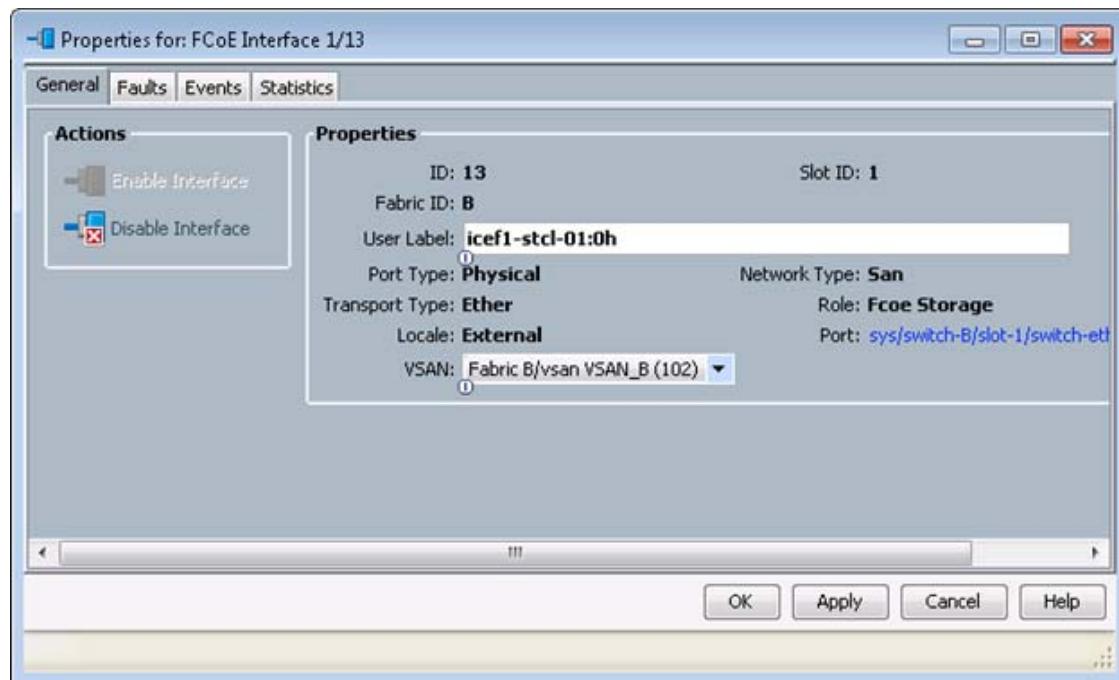
1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Select SAN > Storage Cloud.
3. Expand Fabric A and Storage FCoE Interfaces.
4. Right-click FCoE Interface 1/13 and select Storage FCoE Interface.
5. Set the User Label to the storage controller name and port that this interface is connected to.
6. Select VSAN_A as the VSAN.
7. Click OK.



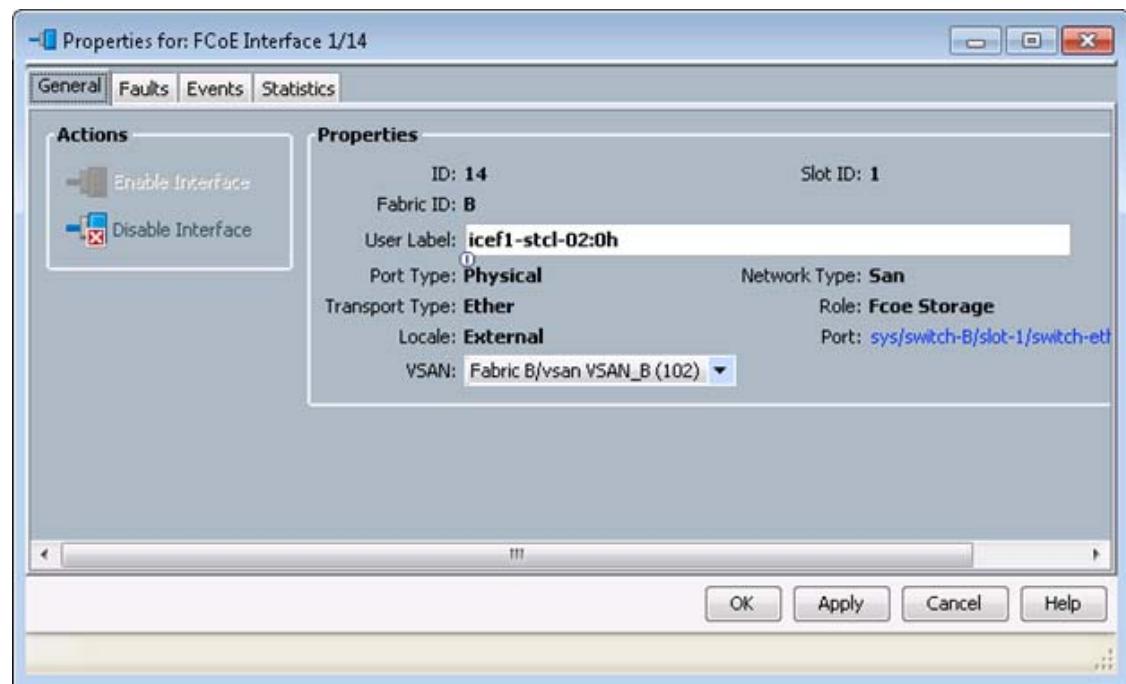
8. Expand Fabric A and Storage FCoE Interfaces.
9. Right-click FCoE Interface 1/14 and select Storage FCoE.
10. Set the User Label to the storage controller name and port that this interface is connected to.
11. Select VSAN_A as the VSAN.
12. Click OK.



13. Expand Fabric B and Storage FCoE Interfaces.
14. Right-click FCoE Interface 1/13 and select Storage FCoE.
15. Set the User Label to the storage controller name and port that this interface is connected to.
16. Select VSAN_B as the VSAN.
17. Click OK.



18. Expand Fabric B and Storage FCoE Interfaces.
19. Right-click FCoE Interface 1/14 and select Storage FCoE Interface.
20. Set the User Label to the storage controller name and port that this interface is connected to.
21. Select VSAN_B as the VSAN.
22. Click OK.



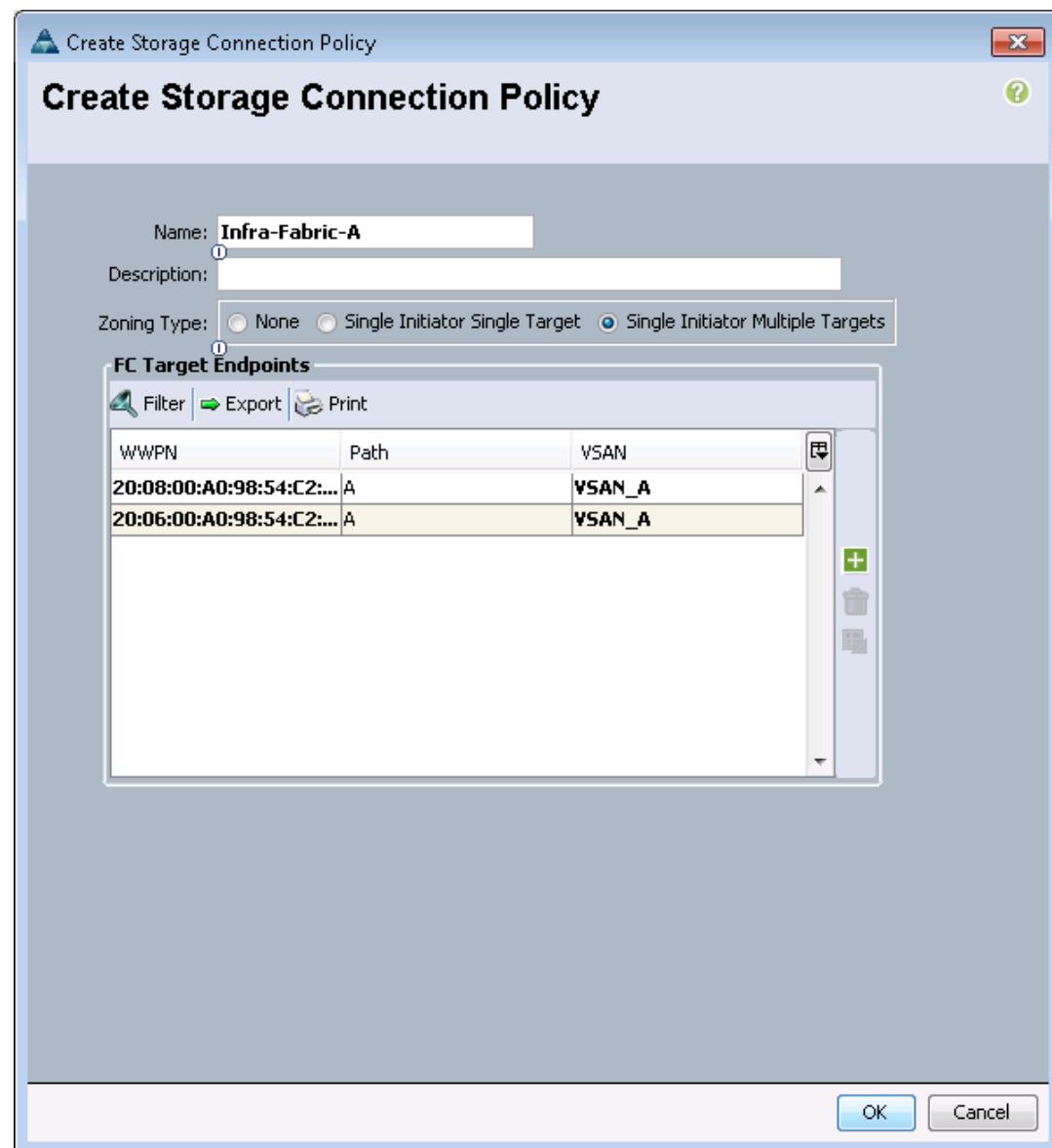
Create Storage Connection Policies for FCoE Zoning

To create Storage Connection Policies for the FCoE Zoning, complete the following steps:

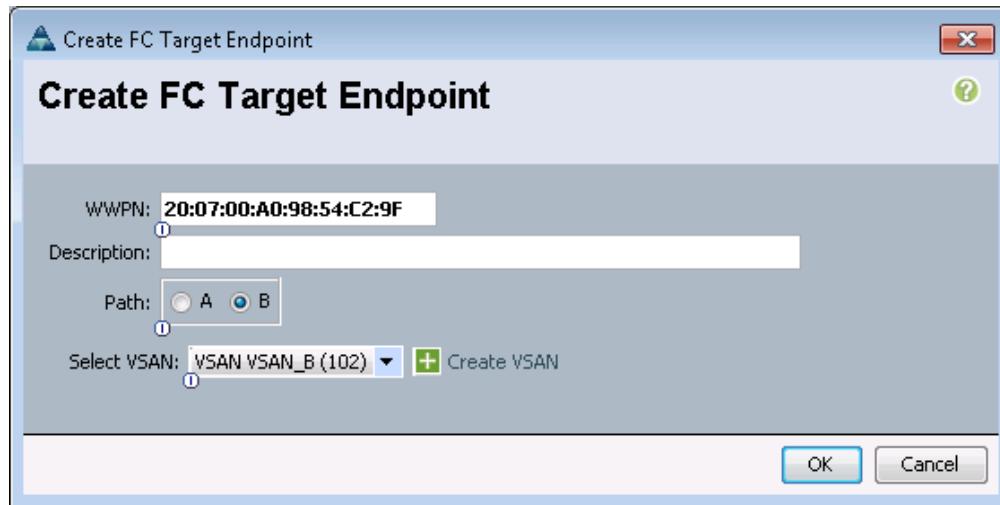
1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click Storage Connection Policies.
4. Select Create Storage Connection Policy.
5. Enter **Infra-Fabric-A** as the name of the policy.
6. Select the Single Initiator Multiple Targets Zoning Type.
7. Click the Plus Sign on the right to add a zoning target.
8. Enter the WWPN for **fcp_lif01a** from the storage cluster. This WWPN can be obtained by logging into the storage cluster CLI and entering the `network interface show -vserver Infra_Vserver` command.
9. Select Path A and VSAN_A.



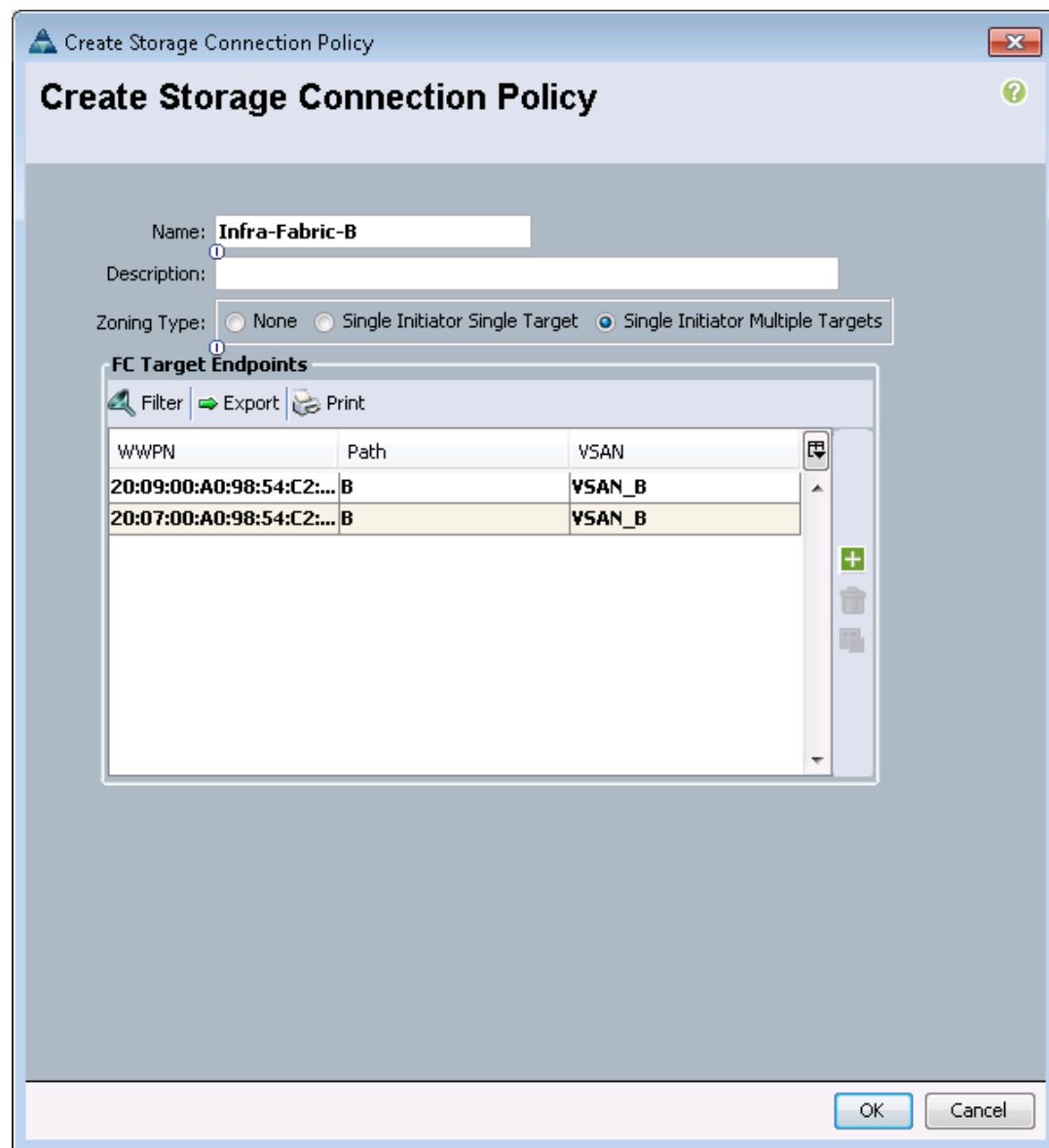
10. Click OK.
11. Click the Plus Sign on the right to add a second zoning target.
12. Enter the WWPN for `fcp_lif02a` from the storage cluster. This WWPN can be obtained by logging into the storage cluster CLI and entering the `network interface show -vserver Infra_Vserver` command.
13. Select Path A and VSAN_A.
14. Click OK, and then click OK again.



15. Right-click Storage Connection Policies.
16. Select Create Storage Connection Policy
17. Enter Infra-Fabric-B as the name of the policy.
18. Select the Single Initiator Multiple Targets Zoning Type.
19. Click the Plus Sign on the right to add a zoning target.
20. Enter the WWPN for fcp_lif01b from the storage cluster. This WWPN can be obtained by logging into the storage cluster CLI and entering the network interface show -vserver Infra_Vserver command.
21. Select Path B and VSAN_B.



22. Click OK.
23. Click the Plus Sign on the right to add a second zoning target.
24. Enter the WWPN for `fcp_lif02b` from the storage cluster. This WWPN can be obtained by logging into the storage cluster CLI and entering the `network interface show -vserver Infra_Vserver` command.
25. Select Path B and VSAN_B.
26. Click OK, and then click OK again.

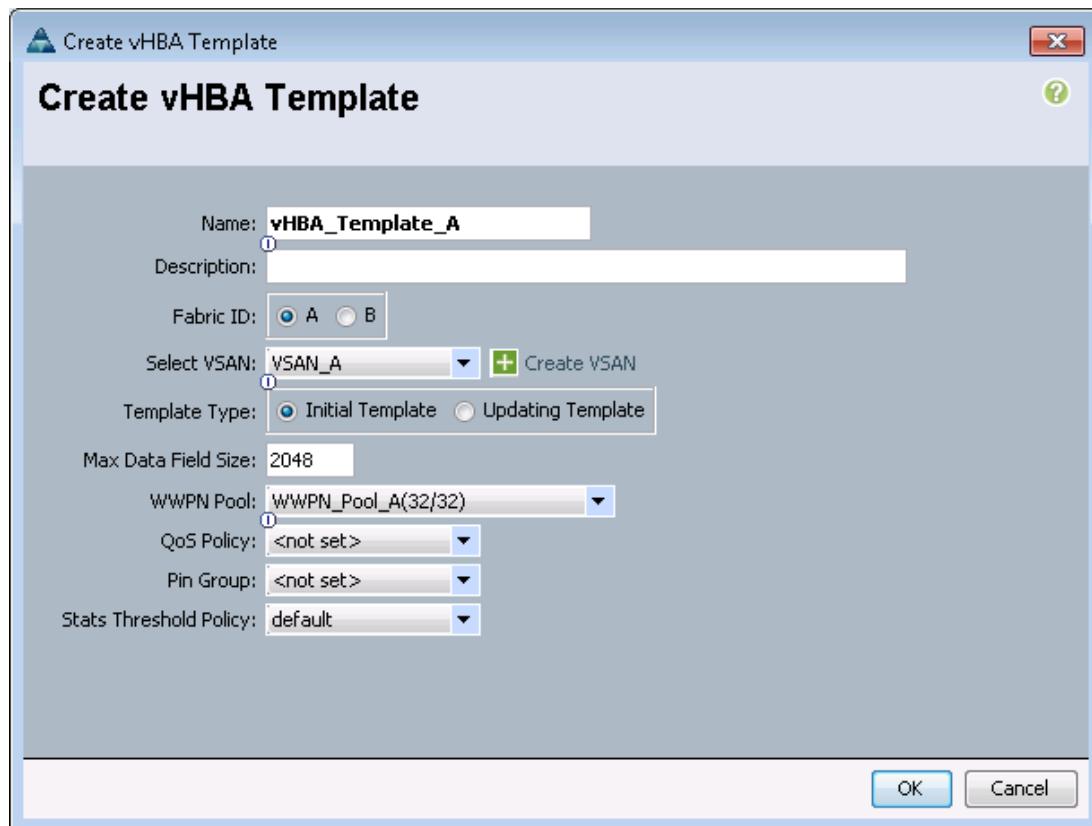


Create vHBA Templates

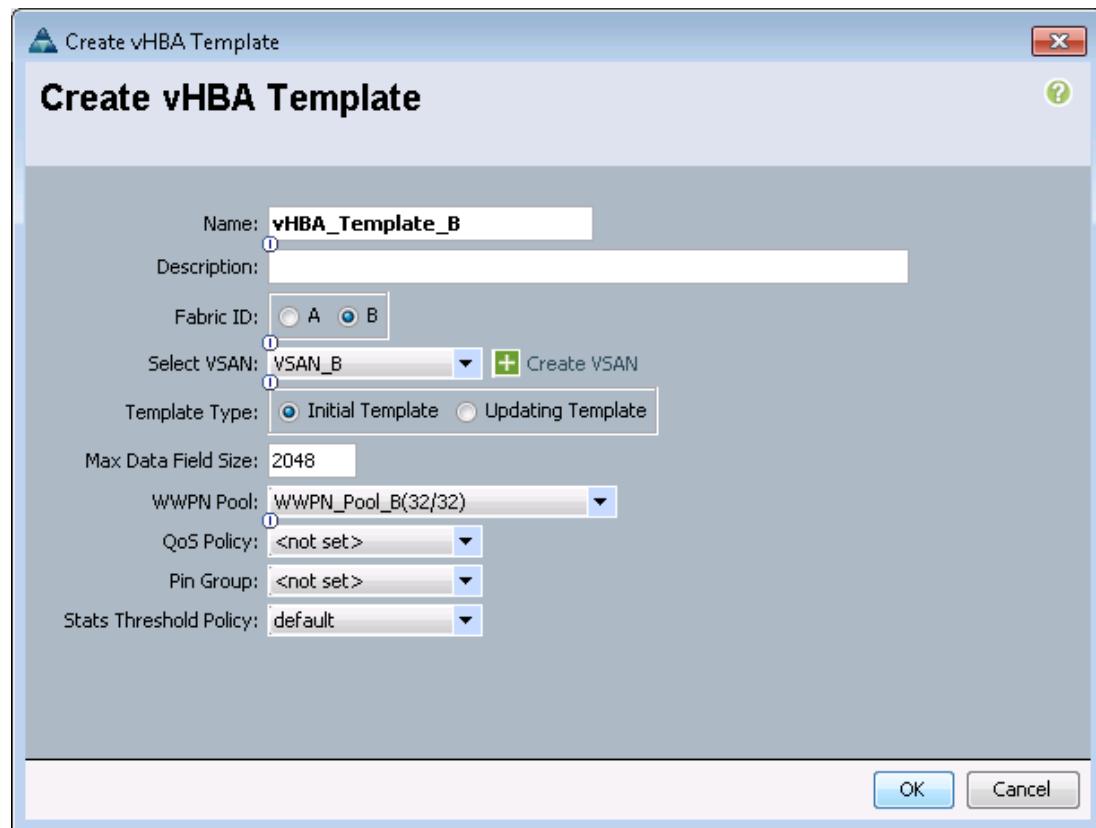
To create the necessary virtual host bus adapter (vHBA) templates for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click vHBA Templates.
4. Select Create vHBA Template.
5. Enter vHBA_Template_A as the vHBA template name.
6. Keep Fabric A selected.
7. Select VSAN_A.

8. Leave Initial Template as the Template Type.
9. Select WWPN_Pool_A as the WWPN Pool.
10. Click OK to create the vHBA template.
11. Click OK.



12. Right-click vHBA Templates.
13. Select Create vHBA Template.
14. Enter vHBA_Template_B as the vHBA template name.
15. Select Fabric B as the Fabric ID.
16. Select VSAN_B.
17. Leave Initial Template as the Template Type.
18. Select WWPN_Pool_B as the WWPN Pool.
19. Click OK to create the vHBA template.
20. Click OK.



Create Boot Policies

This procedure applies to a Cisco UCS environment in which two FCoE logical interfaces (LIFs) are on cluster node 1 (`fcp_lif01a` and `fcp_lif01b`) and two FCoE LIFs are on cluster node 2 (`fcp_lif02a` and `fcp_lif02b`). Also, it is assumed that the A LIFs are connected to Fabric A (Cisco UCS 6248UP A) and the B LIFs are connected to Fabric B (Cisco UCS 6248UP B).

Two boot policies are configured in this procedure. The first policy configures the primary target to be `fcp_lif01a` and the second boot policy configures the primary target to be `fcp_lif01b`.

To create boot policies for the Cisco UCS environment, complete the following steps:

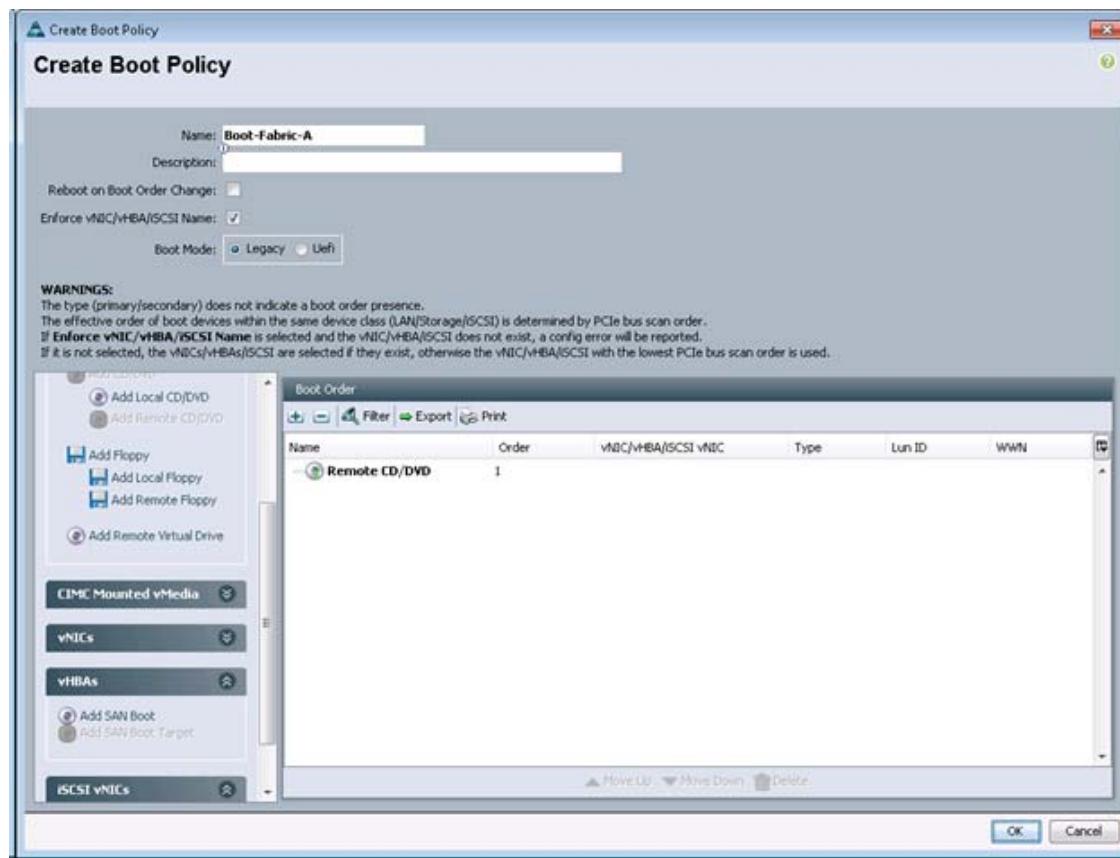
1. In Cisco UCS Manager, in the navigation pane, click the Servers tab.
2. Select Policies > root.
3. Right-click Boot Policies.
4. Select Create Boot Policy.
5. Enter `Boot-Fabric-A` as the name for the boot policy.
6. Optional: Enter a description for the boot policy.



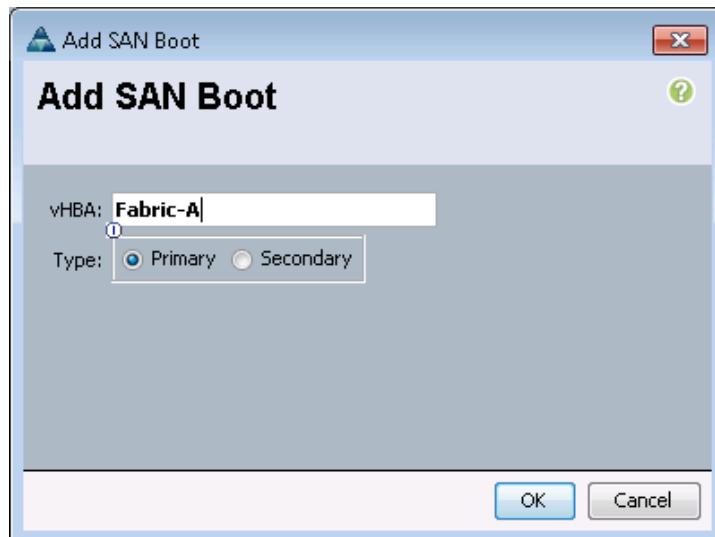
Note

Do not select the Reboot on Boot Order Change checkbox.

7. Expand the Local Devices drop-down list, select Add Remote CD/DVD.



8. Expand the vHBAs drop-down list and select Add SAN Boot.
9. In the Add SAN Boot dialog box, enter Fabric-A in the vHBA field.
10. Confirm that Primary is selected for the Type option.



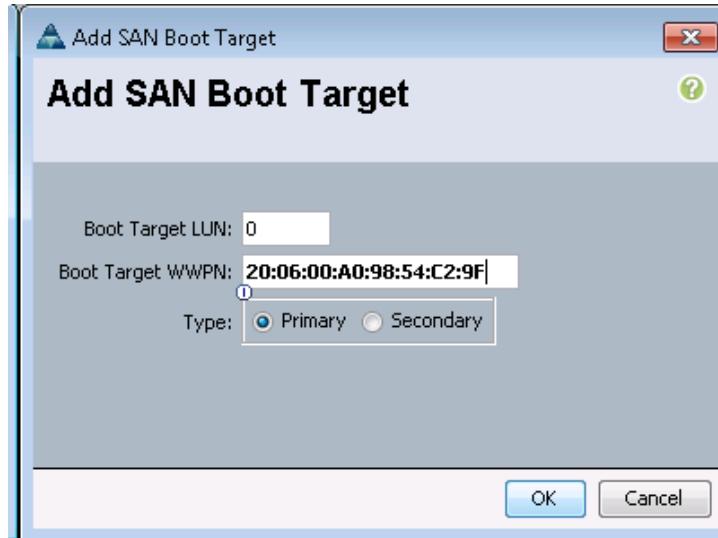
11. Click OK to add the SAN boot initiator.
12. From the vHBA drop-down list, select Add SAN Boot Target.

13. Keep 0 as the value for Boot Target LUN.
14. Enter the WWPN for fcp_lif01a.



Note To obtain this information, log in to the storage cluster and run the network interface show command.

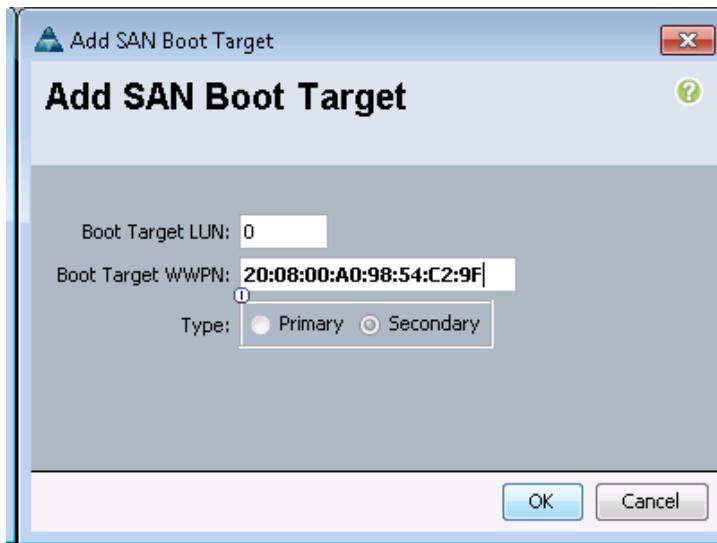
15. Select Primary for the SAN boot target type.



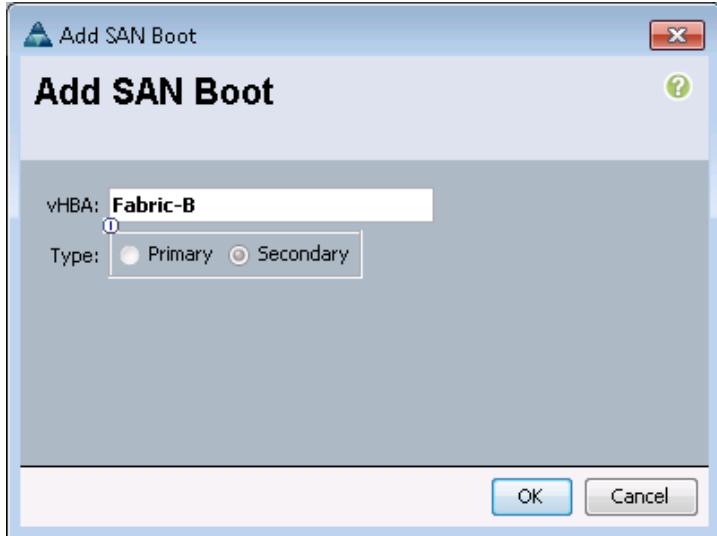
16. Click OK to add the SAN boot target.
17. From the vHBA drop-down list, select Add SAN Boot Target.
18. Enter 0 as the value for Boot Target LUN.
19. Enter the WWPN for fcp_lif02a.



Note To obtain this information, log in to the storage cluster and run the network interface show command.



20. Click OK to add the SAN boot target.
21. From the vHBA drop-down list, select Add SAN Boot.
22. In the Add SAN Boot dialog box, enter Fabric-B in the vHBA box.
23. The SAN boot type should automatically be set to Secondary, and the Type option should be unavailable.

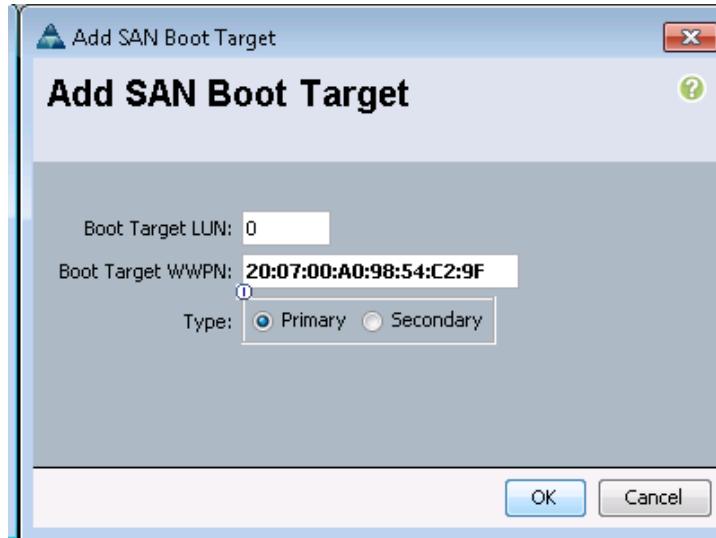


24. Click OK to add the SAN boot initiator.
25. From the vHBA drop-down list, select Add SAN Boot Target.
26. Keep 0 as the value for Boot Target LUN.
27. Enter the WWPN for fcp_lif01b.



Note To obtain this information, log in to the storage cluster and run the network interface show command.

28. Select Primary for the SAN boot target type.

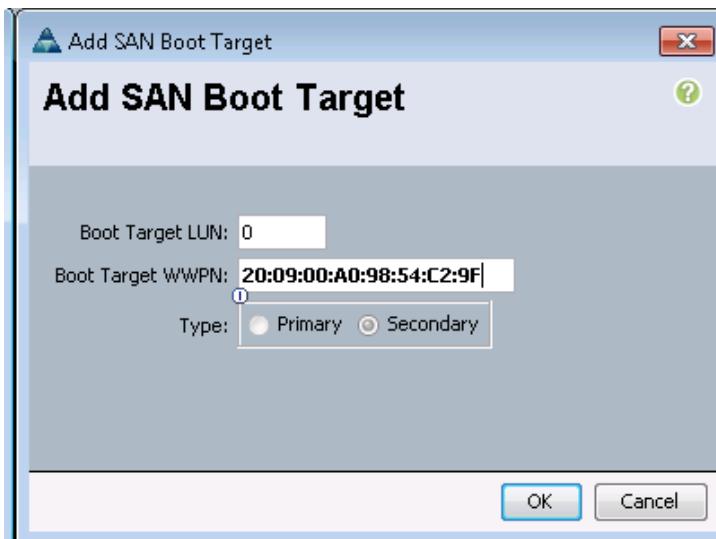


29. Click OK to add the SAN boot target.
30. From the vHBA drop-down list, select Add SAN Boot Target.
31. Keep 0 as the value for Boot Target LUN.
32. Enter the WWPN for fcp_lif02b.

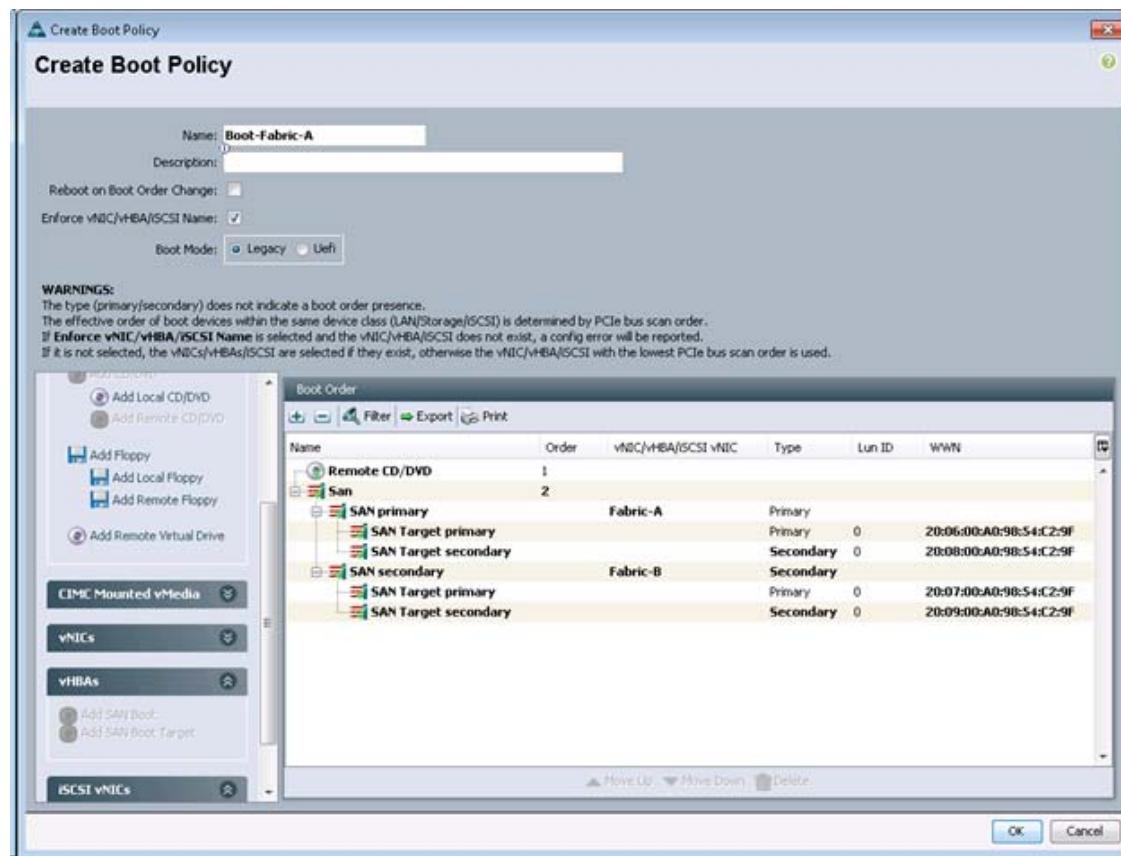


Note

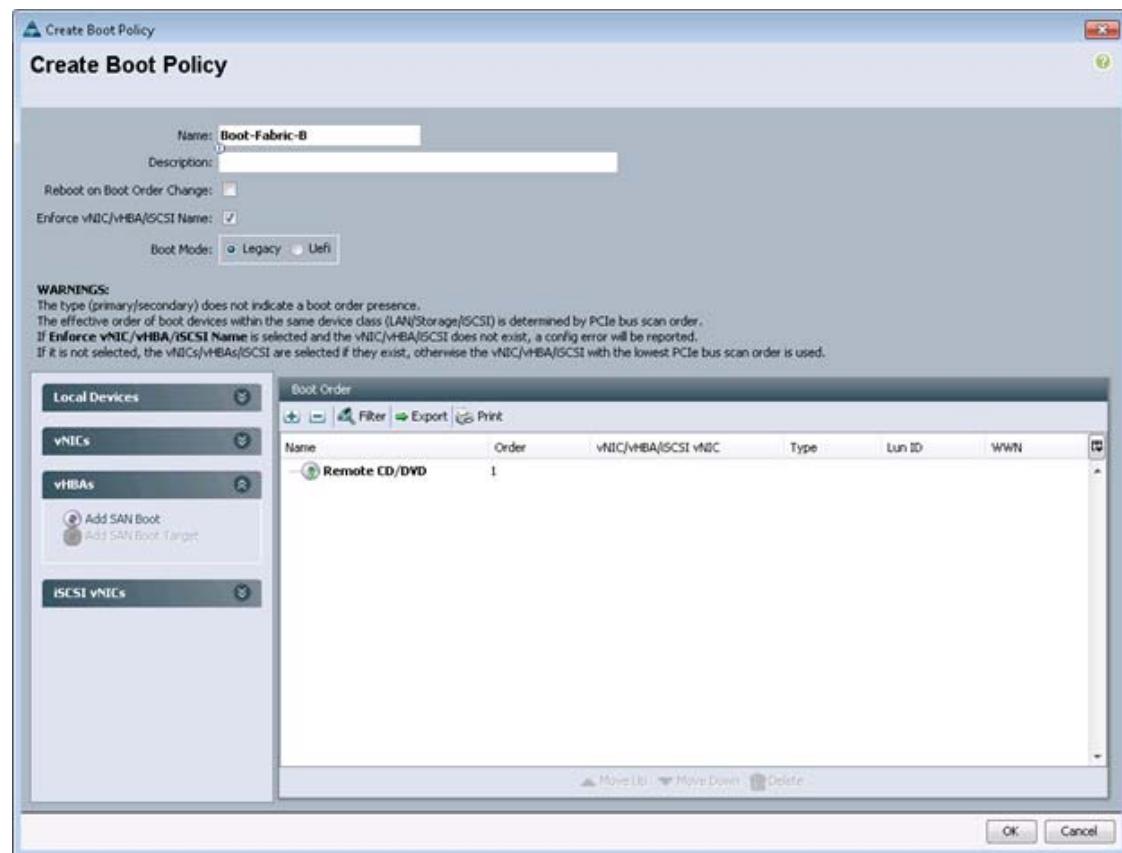
To obtain this information, log in to the storage cluster and run the `network interface show` command.



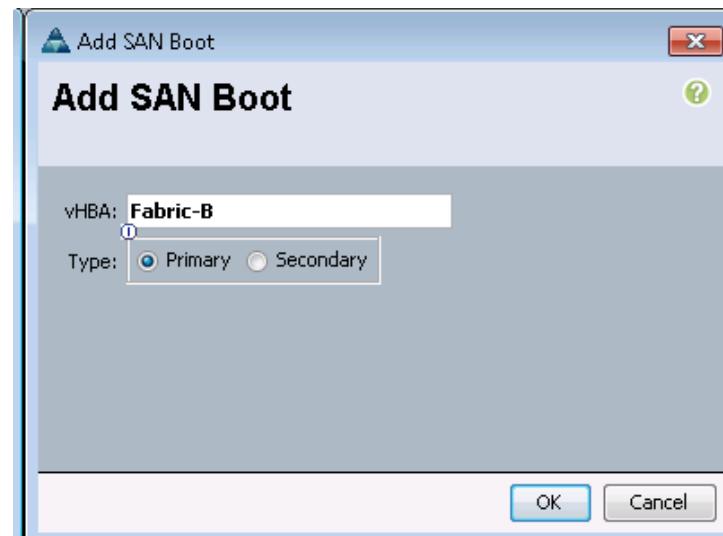
33. Click OK to add the SAN boot target.



34. Click OK, then click OK again to create the boot policy.
35. Right-click Boot Policies again.
36. Select Create Boot Policy.
37. Enter Boot - Fabric - B as the name for the boot policy.
38. Optional: Enter a description of the boot policy.
39. Do not select the Reboot on Boot Order Change option.
40. From the Local Devices drop-down list, select Add Remote CD/DVD.



41. From the vHBA drop-down list, select Add SAN Boot.
42. In the Add SAN Boot dialog box, enter Fabric-B in the vHBA box.
43. Confirm that Primary option is selected for the SAN boot type.



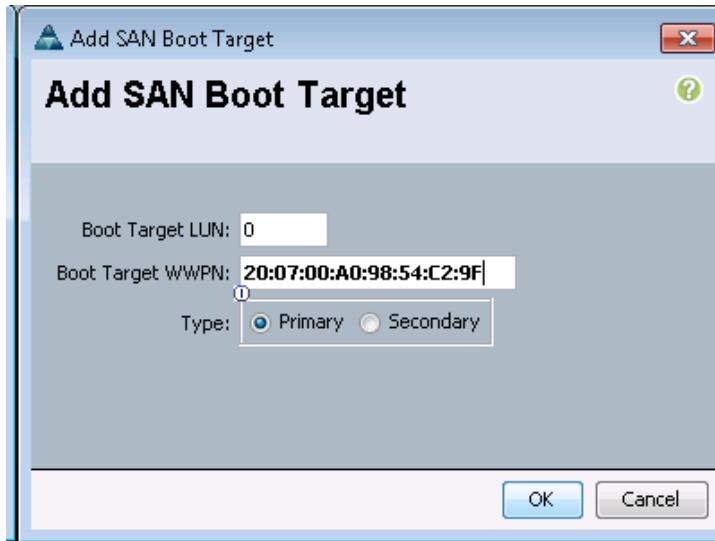
44. Click OK to add the SAN boot initiator.
45. From the vHBA drop-down list, select Add SAN Boot Target.

46. Enter 0 as the value for Boot Target LUN.
47. Enter the WWPN for fcp_lif01b.



Note To obtain this information, log in to the storage cluster and run the `network interface show` command.

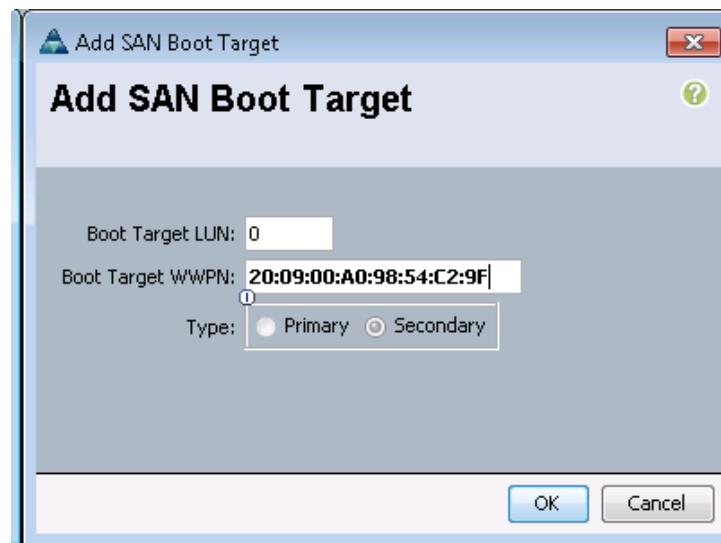
48. Select Primary option for the SAN boot target type.



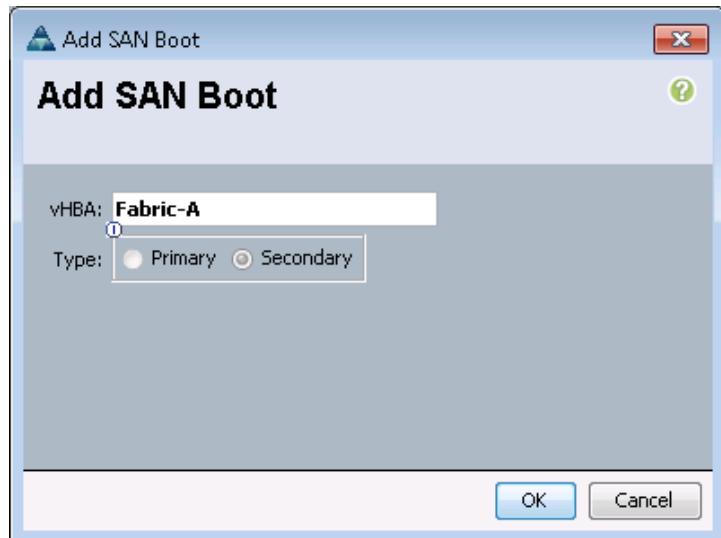
49. Click OK to add the SAN boot target.
50. From the vHBA drop-down list, select Add SAN Boot Target.
51. Enter 0 as the value for Boot Target LUN.
52. Enter the WWPN for fcp_lif02b.



Note To obtain this information, log in to the storage cluster and run the `network interface show` command.



53. Click OK to add the SAN boot target.
54. From the vHBA menu, select Add SAN Boot.
55. In the Add SAN Boot dialog box, enter Fabric-A in the vHBA box.
56. The SAN boot type should automatically be set to Secondary, and the Type option should be unavailable.

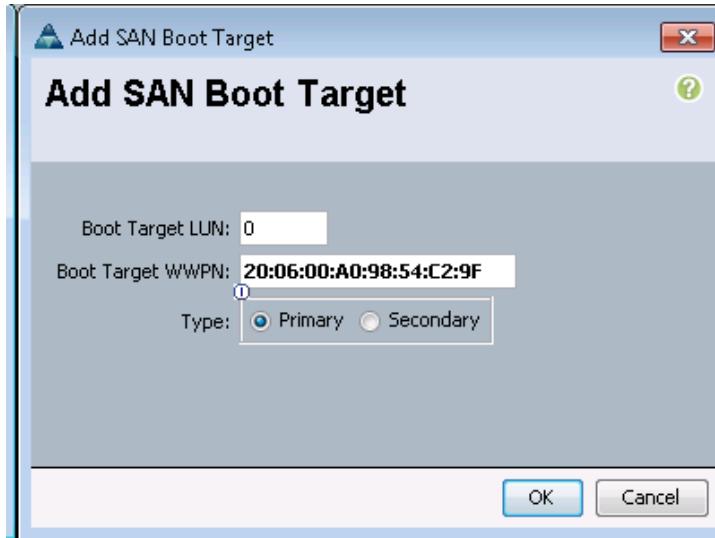


57. Click OK to add the SAN boot initiator.
58. From the vHBA menu, select Add SAN Boot Target.
59. Enter 0 as the value for Boot Target LUN.
60. Enter the WWPN for fcp_lif01a.

**Note**

To obtain this information, log in to the storage cluster and run the `network interface show` command.

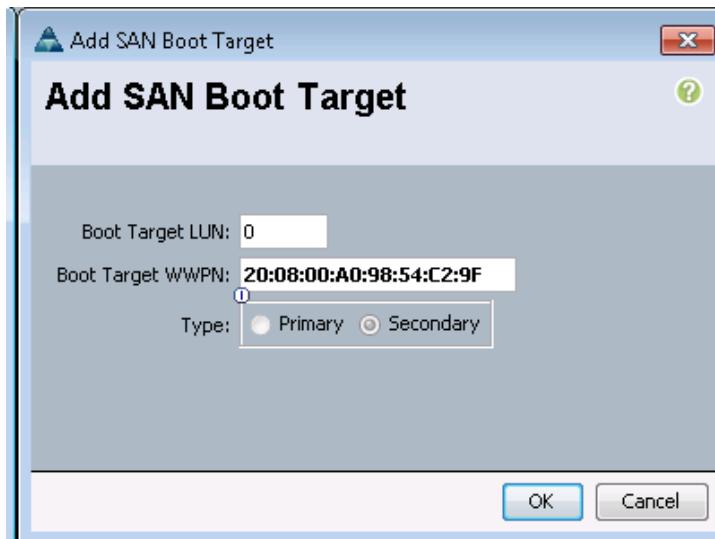
61. Select the Primary option for the SAN boot target type.



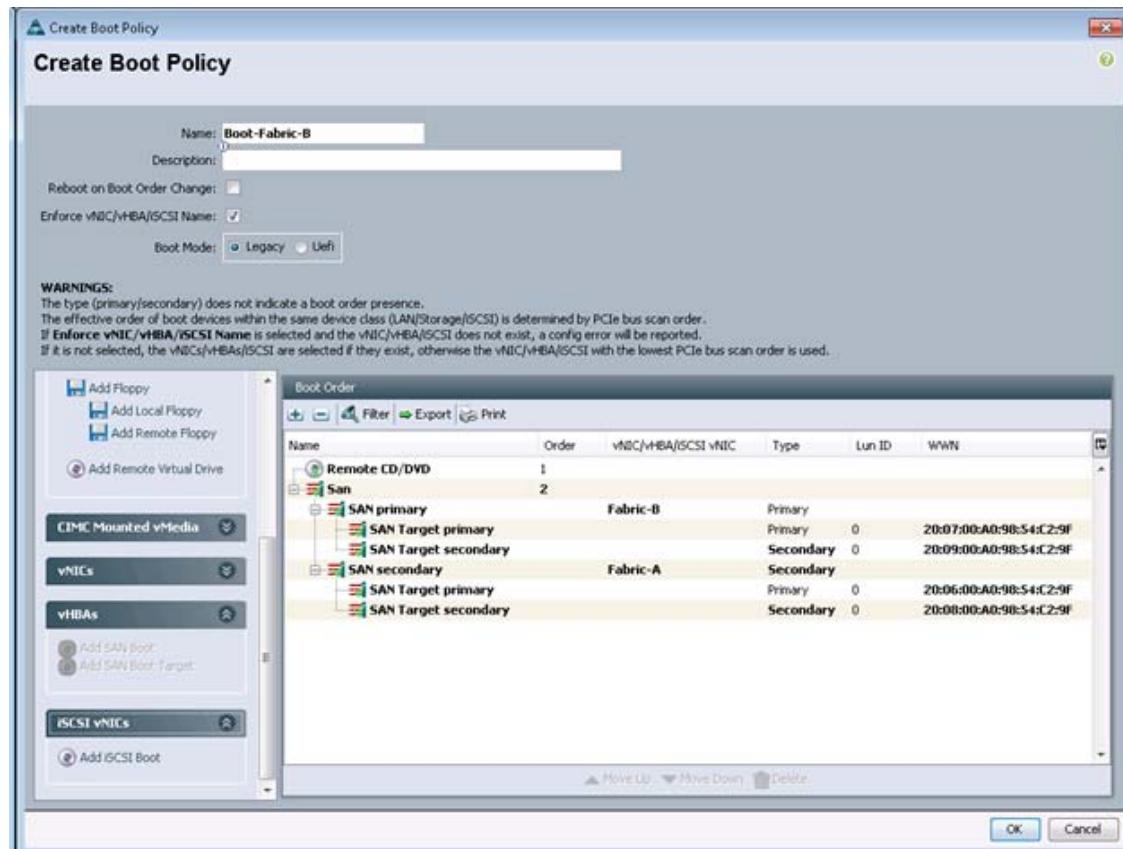
62. Click OK to add the SAN boot target.
 63. From the vHBA drop-down list, select Add SAN Boot Target.
 64. Enter 0 as the value for Boot Target LUN.
 65. Enter the WWPN for fcp_lif02a.



Note To obtain this information, log in to the storage cluster and run the network interface show command.



66. Click OK to add the SAN boot target.



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

Create Service Profile Templates

In this procedure, one service profile template is created for fabric A boot.

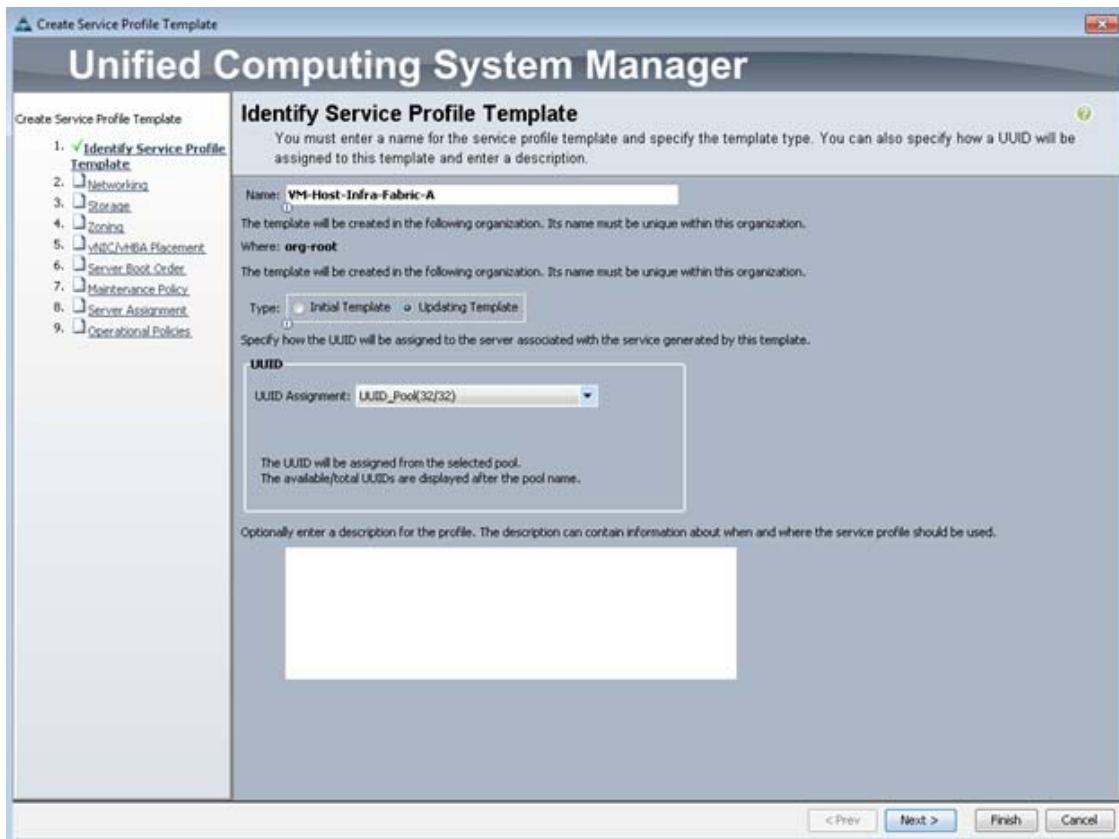
To create the service profile template, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root.
3. Right-click root.
4. Select 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.

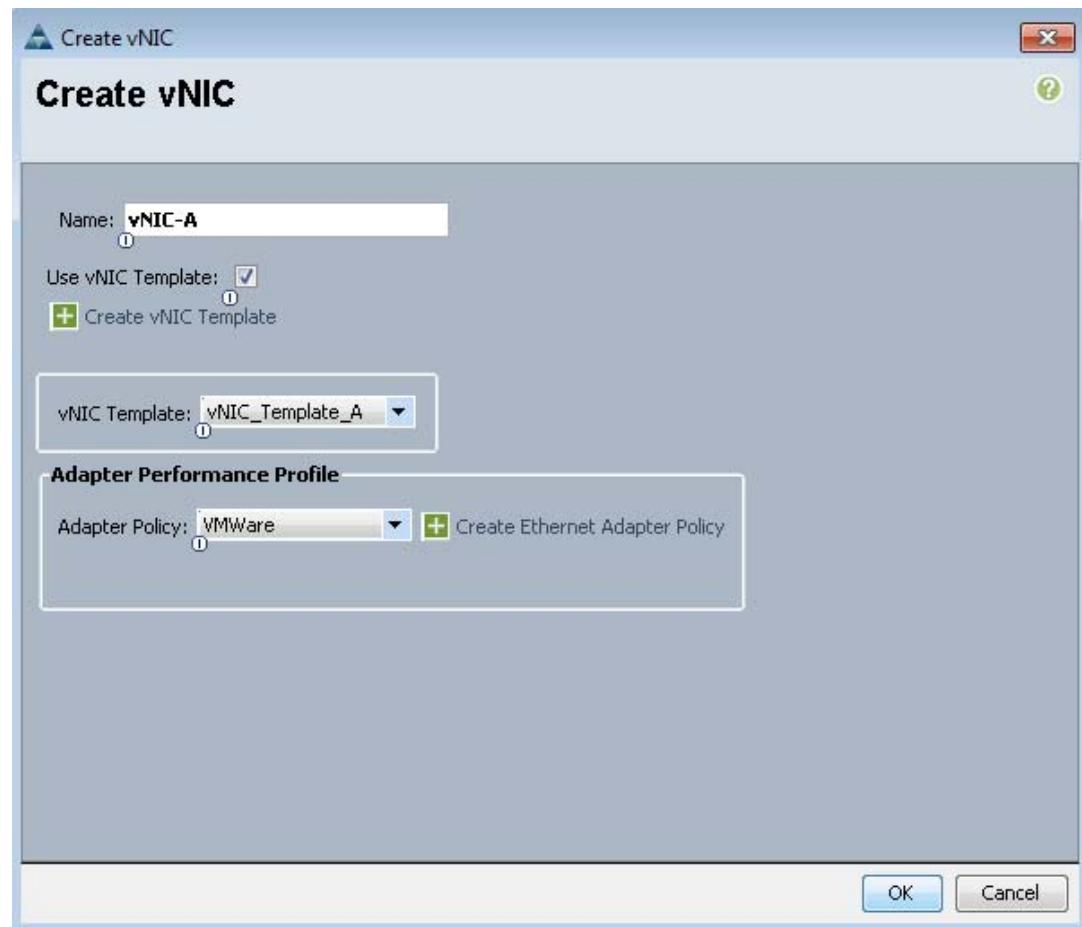


Note If this name has already been utilized for the Infrastructure hosts utilizing iSCSI boot, please choose a different name or append "fcoe" to this template name.

- b. Select the "Updating Template" option.
- c. Under UUID, select UUID_Pool as the UUID pool.
- d. Click Next.



6. To configure the networking options, 6 vNIC interfaces will be added for Infrastructure ESXi hosts:
7. Keep the default setting for Dynamic vNIC Connection Policy.
8. Select the "Expert" option to configure the LAN connectivity.
9. Click the upper Add button to add a vNIC to the template.
10. In the Create vNIC dialog box, enter vNIC-A as the name of the vNIC.
11. Select the Use vNIC Template checkbox.
12. In the vNIC Template list, select vNIC_Template_A.
13. In the Adapter Policy list, select VMWare.
14. Click OK to add this vNIC to the template.



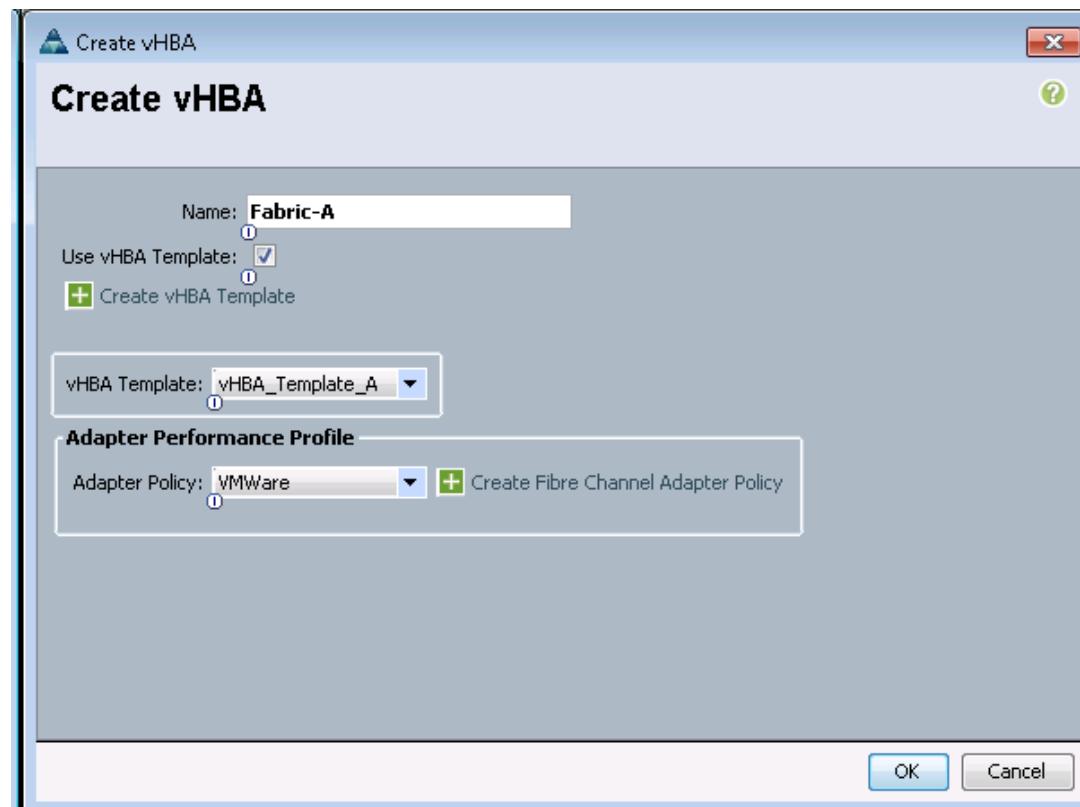
15. On the Networking page of the wizard, click the upper Add button to add another vNIC to the template.
16. In the Create vNIC box, enter vNIC-B as the name of the vNIC.
17. Select the Use vNIC Template checkbox.
18. In the vNIC Template list, select vNIC_Template_B.
19. In the Adapter Policy list, select VMWare.
20. Click OK to add the vNIC to the template.
21. On the Networking page of the wizard, click the upper Add button to add another vNIC to the template.
22. In the Create vNIC box, enter OOB-A as the name of the vNIC.
23. Select the Use vNIC Template checkbox.
24. In the vNIC Template list, select OOB-A.
25. In the Adapter Policy list, select VMWare.
26. Click OK to add the vNIC to the template.
27. On the Networking page of the wizard, click the upper Add button to add another vNIC to the template.
28. In the Create vNIC box, enter OOB-B as the name of the vNIC.

29. Select the Use vNIC Template checkbox.
30. In the vNIC Template list, select OOB-B.
31. In the Adapter Policy list, select VMWare.
32. Click OK to add the vNIC to the template.

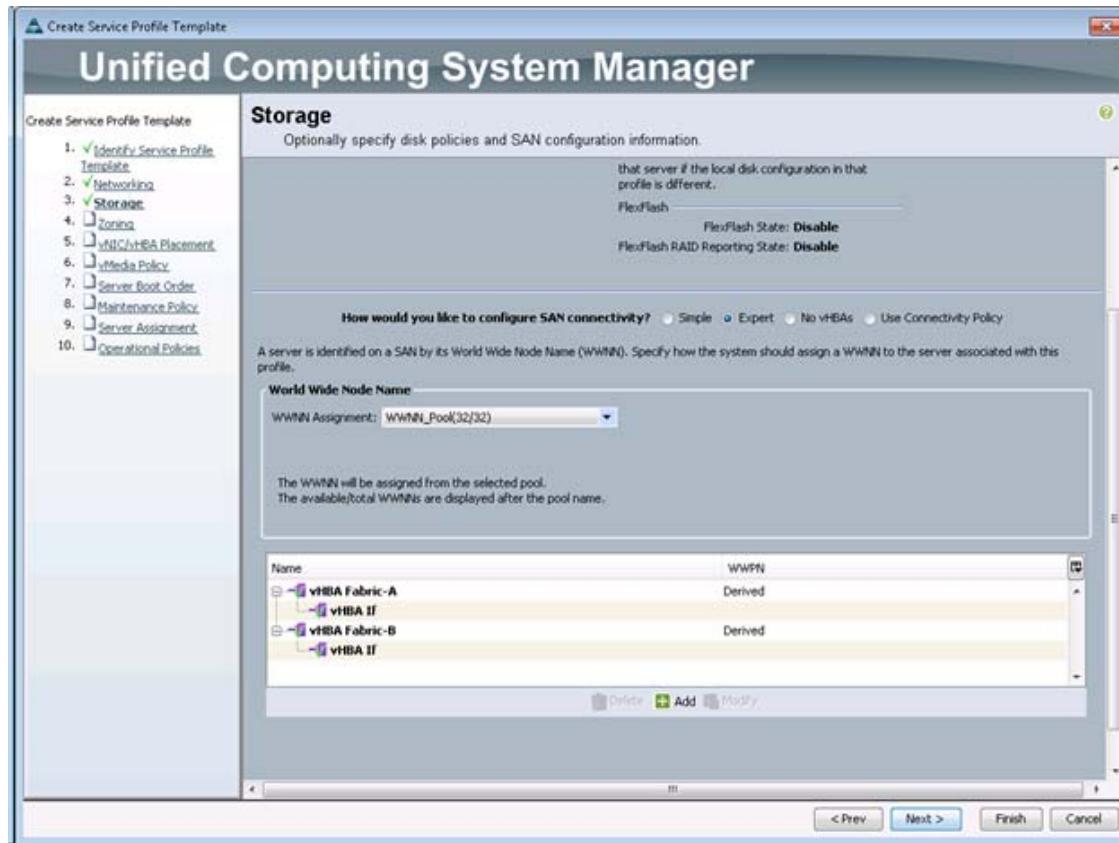


Note The next two vNIC interfaces are only needed for Infrastructure ESXi Hosts. These interfaces enable NFS access using NFS specific vSwitch and static EPG mapping. ESXi servers not hosting infrastructure VMs, use VDS for NFS access to application specific SVMs.

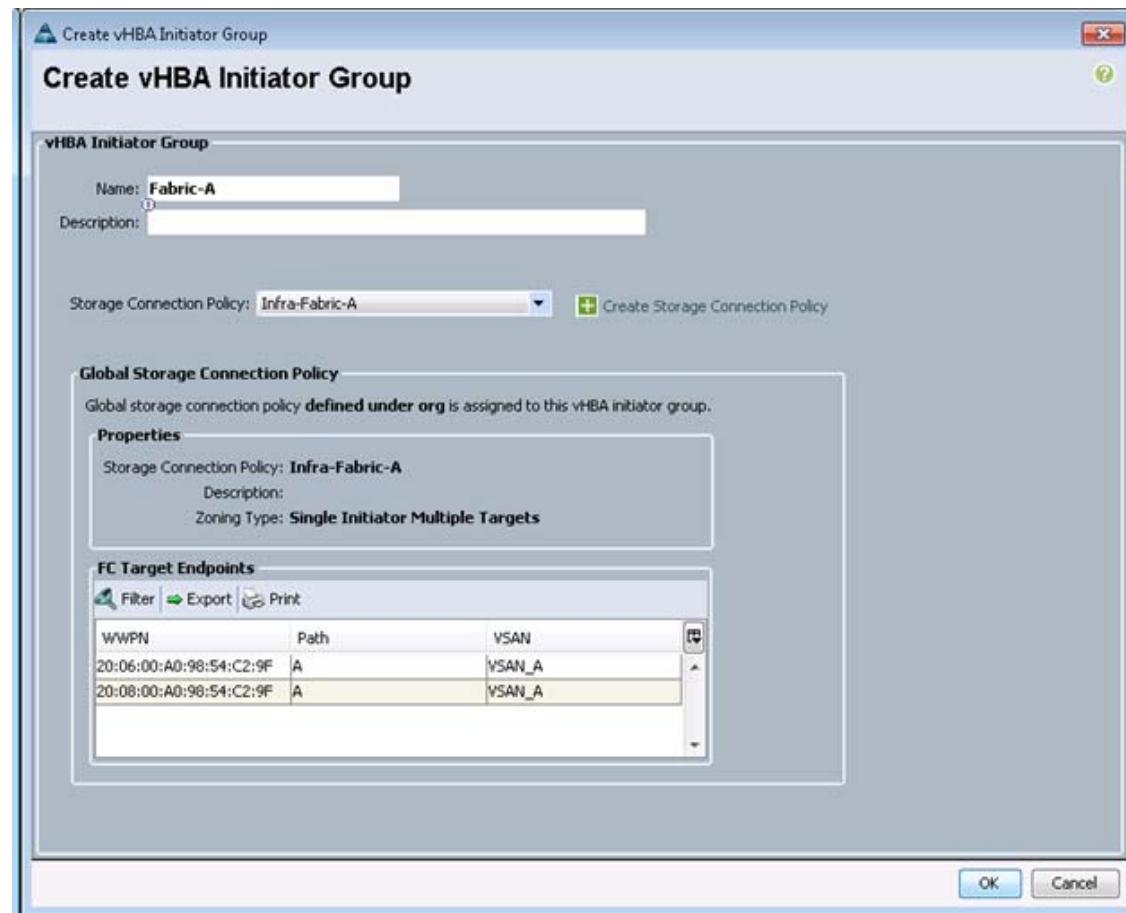
33. On the Networking page of the wizard, click the upper Add button to add another vNIC to the template.
34. In the Create vNIC box, enter NFS-A as the name of the vNIC.
35. Select the Use vNIC Template checkbox.
36. In the vNIC Template list, select Infra_NFS_A.
37. In the Adapter Policy list, select VMWare.
38. Click OK to add the vNIC to the template.
39. On the Networking page of the wizard, click the upper Add button to add another vNIC to the template.
40. In the Create vNIC box, enter NFS-B as the name of the vNIC.
41. Select the Use vNIC Template checkbox.
42. In the vNIC Template list, select Infra_NFS_B.
43. In the Adapter Policy list, select VMWare.
44. Click OK to add the vNIC to the template.
45. Verify 6 vNIC interfaces are present.
46. Review the table in the Networking page to make sure that all vNICs were created.
47. Click Next.
48. Configure the storage options:
 - a. Select a local disk configuration policy:
 - If the server in question has local disks, select default in the Local Storage list.
 - If the server in question does not have local disks, select SAN-Boot.
 - b. Select the Expert option for the “How would you like to configure SAN connectivity?” field.
 - c. Select WWNN_Pool for the WWNN Assignment.
 - d. Click the Add button to add a vHBA.
 - e. Enter Fabric-A as the vHBA name and select the checkbox for Use vHBA Template.
 - f. Select the vHBA_Template_A vHBA Template and the VMWare Adapter Policy.



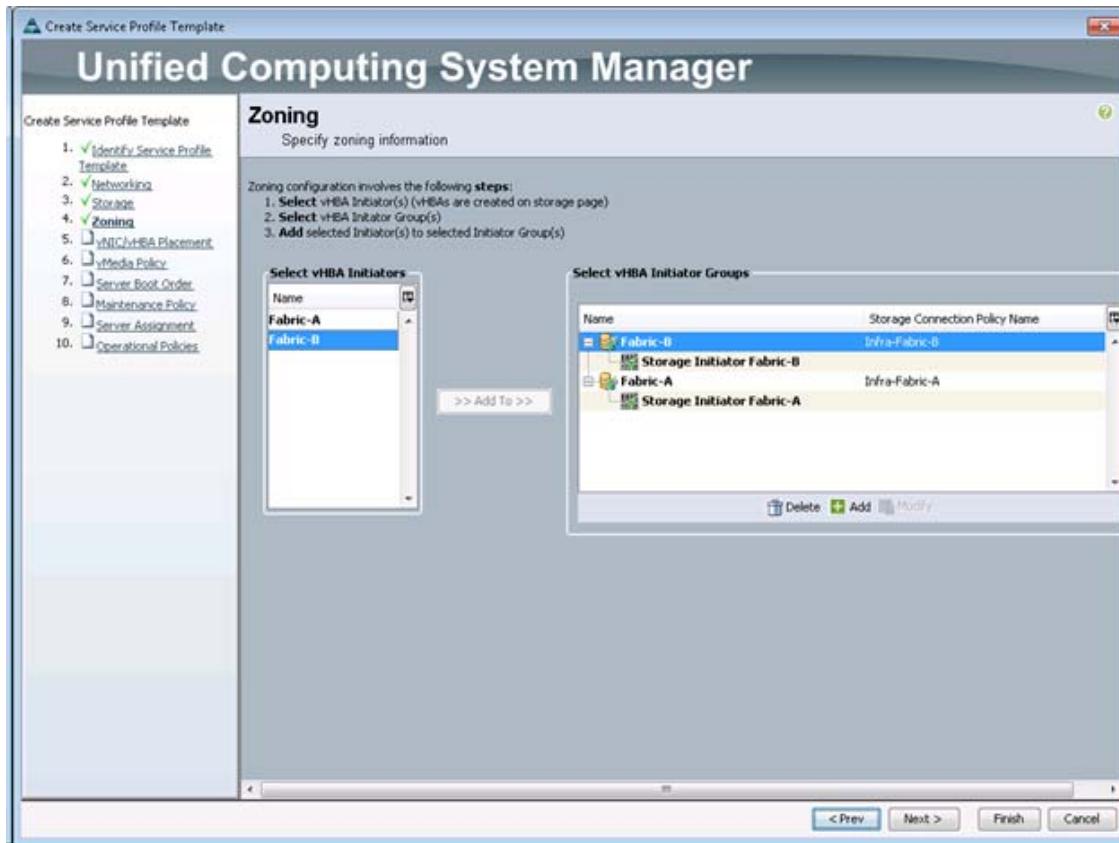
49. Click OK to add the vHBA.
50. Click the Add button to add a vHBA.
51. Enter Fabric-B as the vHBA name and select the checkbox for Use vHBA Template.
52. Select the vHBA_Template_B vHBA Template and the VMWare Adapter Policy.
53. Click OK to add the vHBA.
54. Click Next.



55. In the Zoning window, click the Add button.
56. Name the vHBA Initiator Group, Fabric-A and select the Infra-Fabric-A Storage Connection Policy.



57. Click OK to add the vHBA Initiator Group.
58. In the Zoning window, click the Add button.
59. Name the vHBA Initiator Group, Fabric-B and select the Infra-Fabric-B Storage Connection Policy.
60. Click OK to add the vHBA Initiator Group.
61. In the Zoning window, select Fabric A in the list of vHBA Initiators and Fabric-A in the list of vHBA Initiator Groups.
62. Click the >> Add To >> button.
63. In the Zoning window, select Fabric B in the list of vHBA Initiators and Fabric-B in the list of vHBA Initiator Groups.
64. Click the >> Add To >> button.



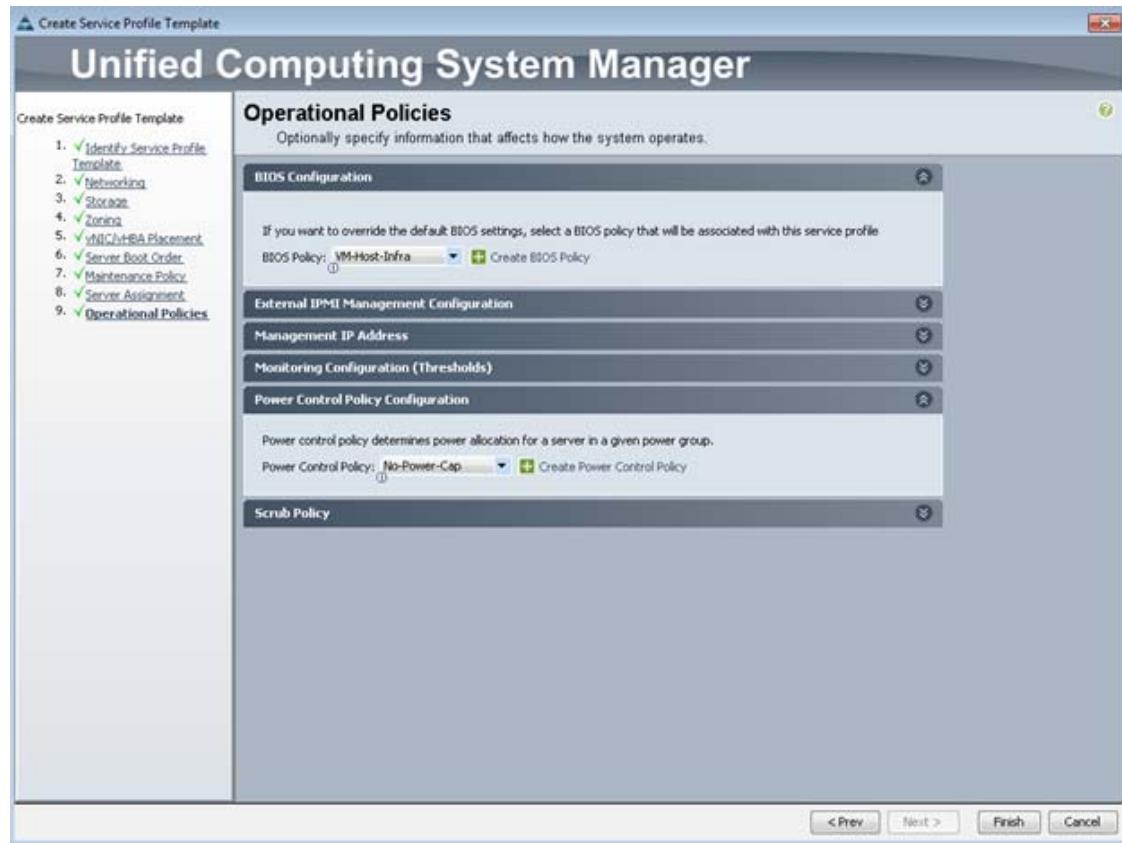
65. Click Next.
66. Set the vNIC/vHBA placement options.
 - a. In the “Select Placement” list, select the VM-Host-Infra placement policy.
 - b. Select vCon1 and assign the vHBAs/vNICs to the virtual network interfaces policy in the following order:
 - vNIC-A
 - vNIC-B
 - OOB-A
 - OOB-B
 - NFS-A
 - NFS-B
 - vHBA Fabric-A
 - vHBA Fabric-B
 - c. Review the table to verify that all vNICs and vHBAs were assigned to the policy in the appropriate order.
 - d. Click Next.
67. Set the server boot order:
68. Select Boot-Fabric-A for Boot Policy.



69. Review the table to make sure that all boot devices were created and identified. Verify that the boot devices are in the correct boot sequence.
70. Click Next to continue to the next section.
71. Add a maintenance policy:
 - a. Select the default Maintenance Policy.
 - b. Click Next.



72. Specify the server assignment:
 - a. In the Pool Assignment list, select Infra_Pool.
 - b. Optional: Select a Server Pool Qualification policy.
 - c. Select Down as the power state to be applied when the profile is associated with the server.
 - d. Expand Firmware Management at the bottom of the page and select VM-Host-Infra from the Host Firmware list.
 - e. Click Next.
73. Add operational policies:
 - a. In the BIOS Policy list, select VM-Host-Infra.
 - b. Expand Power Control Policy Configuration and select No-Power-Cap in the Power Control Policy list.

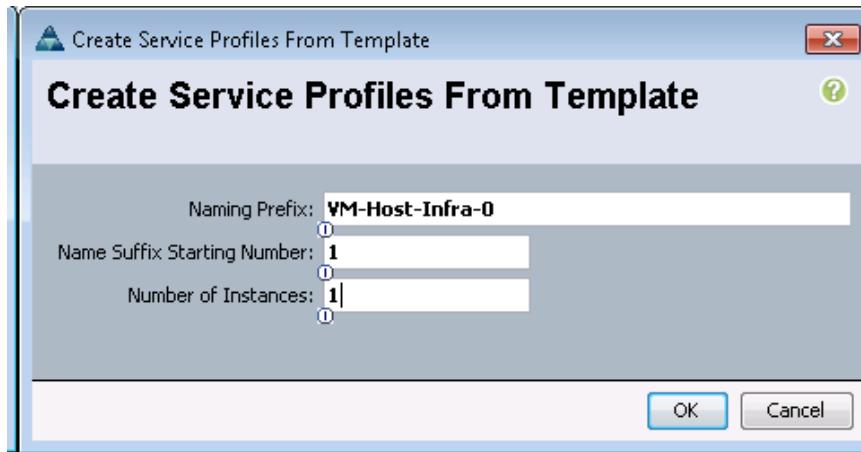


74. Click Finish to create the service profile template.
75. Click OK in the confirmation message.

Create Service Profiles

To create service profiles from the service profile template, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Service Template VM-Host-Infra-Fabric-A.
3. Right-click VM-Host-Infra-Fabric-A and select Create Service Profiles from Template.
4. Enter VM-Host-Infra-0 as the service profile prefix.
5. Enter 1 as Name Suffix Starting Number.
6. Enter 1 as the Number of Instances.
7. Click OK to create the service profile.



- Click OK in the confirmation message.

Storage Part 2

Clustered Data ONTAP SAN Boot Storage Setup

Create Igroups

- From the cluster management node SSH connection, enter the following:

```
igroup create -vserver Infra_Vserver -igroup VM-Host-Infra-01 -protocol fcp
-ostype vmware -initiator <<var_vm_host_infra_01_A_wwpn>>,
<<var_vm_host_infra_01_B_wwpn>>
igroup create -vserver Infra_Vserver -igroup VM-Host-Infra-02 -protocol fcp
-ostype vmware -initiator <<var_vm_host_infra_02_A_wwpn>>,
<<var_vm_host_infra_02_B_wwpn>>
igroup create -vserver Infra_Vserver -igroup MGMT-Hosts -protocol fcp
-ostype vmware -initiator <<var_vm_host_infra_01_A_wwpn>>,
<<var_vm_host_infra_01_B_wwpn>>, <<var_vm_host_infra_02_A_wwpn>>,
<<var_vm_host_infra_02_B_wwpn>>
```



Note To view the three igroups just recently created, enter igrup show.

Map Boot LUNs to Igroups

- From the cluster management SSH connection, enter the following:

```
lun map -vserver Infra_Vserver -volume esxi_boot -lun VM-Host-Infra-01
-igroup VM-Host-Infra-01 -lun-id 0
lun map -vserver Infra_Vserver -volume esxi_boot -lun VM-Host-Infra-02
-igroup VM-Host-Infra-02 -lun-id 0
```

Appendix D - Deploying VMware vSphere 5.1 Update 1

FlexPod VMware ESXi 5.1 Update 1 FCoE on Clustered Data ONTAP

This section provides detailed instructions for installing VMware ESXi 5.1 Update 1 in a FlexPod environment. After the procedures are completed, two FCoE-booted ESXi hosts will be provisioned. These deployment procedures are customized to include the environment variables.



- Note** 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 iSCSI 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 Cisco UCS environment to run the IP KVM.

To log in to the Cisco UCS environment, complete the following 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. Select Servers > Service Profiles > root > VM-Host-Infra-01.
5. Right-click VM-Host-Infra-01 and select KVM Console.
6. Select Servers > Service Profiles > root > VM-Host-Infra-02.
7. Right-click VM-Host-Infra-02 and select 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, complete the following steps on each ESXi host:

1. In the KVM window, click the Virtual Media menu option and select Activate Virtual Devices.
2. Click the Virtual Media menu option and select Map CD/DVD.
3. Click Browse.
4. Browse to the ESXi installer ISO image file and click Open.
5. Click Map Device to map the newly added image.
6. Boot the server by selecting Boot Server and clicking 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, complete the following steps on each host:

1. On reboot, the machine detects the presence of the ESXi installation media. Select 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. Select the NetApp LUN that was previously set up as the installation disk for ESXi and press Enter to continue with the installation.
5. Select 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, clear the Mapped checkbox (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, complete the following 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, complete the following 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. Select the Configure the Management Network option and press Enter.
4. Select 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, select IP Configuration and press Enter.
7. Select 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. Select the IPv6 Configuration option and press Enter.
13. Using the spacebar, unselect Enable IPv6 (restart required) and press Enter.
14. Select 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 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. Select 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, complete the following 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. Select the Configure the Management Network option and press Enter.
4. Select 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, select IP Configuration and press Enter.
7. Select 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. Select the IPv6 Configuration option and press Enter.
13. Using the spacebar, unselect Enable IPv6 (restart required) and press Enter.
14. Select 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. Select 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, complete the following 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.
3. These applications are downloaded from the VMware website and Internet access is required on the management workstation.

Log in to VMware ESXi Hosts 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, complete the following 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, complete the following 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.
4. Click Login to connect.

Install VMware ESXi Patches

To install VMware ESXi patches on the ESXi host VM-Host-Infra-01 and VM-Host-Infra-02, complete the following steps:

1. Download the following VMware ESXi patches to the Management workstation -
 - EP 02 - Express Patch 02
 - EP 04 - Express Patch 04

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

1. From each vSphere Client, select the host in the inventory.
2. Click the Summary tab to view the environment summary.
3. From Resources > Storage, right-click datastore1 and select Browse Datastore.
4. Click the fourth button and select Upload File.
5. Navigate to the saved location for the downloaded patches and select ESXi550-201404001.zip.
6. Click Open to upload the file to datastore1.
7. Click the fourth button and select Upload File.
8. Navigate to the saved location for the downloaded patches and select ESXi550-201406001.zip.
9. Click Open to upload the file to datastore1.
10. Right click on the ESXi host and select Enter Maintenance Mode, Click Yes.
11. From the management workstation, open the VMware vSphere Remote CLI that was previously installed.
12. At the command prompt, run the following commands to account for each host

```
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> software
vib update -d /vmfs/volumes/datastore1/ESXi550-201404001.zip
esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>> software
vib update -d /vmfs/volumes/datastore1/ESXi550-201404001.zip
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> software
vib update -d /vmfs/volumes/datastore1/ESXi550-201406001.zip
esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>> software
vib update -d /vmfs/volumes/datastore1/ESXi550-201406001.zip
```

Download Updated Cisco VIC enic and fnic Drivers

To download the Cisco virtual interface card (VIC) enic driver, complete the following steps:



Note The enic version used in this configuration is 2.1.2.50. The fnic version used in this configuration is 1.6.0.10.

1. Open a Web browser on the management workstation and navigate to:
<https://my.vmware.com/web/vmware/details?downloadGroup=DT-ESXI55-CISCO-ENIC-21250&productId=353>.
2. Download the enic_driver_2.1.2.50_esx55-1906033.zip driver bundle
3. Open the enic driver bundle. This bundle includes the VMware driver bundle which will be uploaded to ESXi hosts.
 enic-2.1.2.50_esx55-offline_bundle-1906033.zip
4. Save the location of this driver bundle for uploading to ESXi in the next section.
5. Open a Web browser on the management workstation and navigate to:
<https://my.vmware.com/web/vmware/details?downloadGroup=DT-ESXI55-CISCO-FNIC-16010&productId=353>.
6. Download the fnic_driver_1.6.0.10_esx55-1897613.zip driver bundle
7. Open the fnic driver bundle. This bundle includes the VMware driver bundle which will be uploaded to ESXi hosts.
 fnic_driver-1.6.0.10_esx55-offline_bundle-1897613.zip
8. Save the location of this driver bundle for uploading to ESXi in the next section.

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 driver for the Cisco VIC, complete the following steps for the hosts on each vSphere Client:

1. From each vSphere Client, select the host in the inventory.
2. Click the Summary tab to view the environment summary.
3. From Resources > Storage, right-click **datastore1** and select **Browse Datastore**.
4. Click the fourth button and select **Upload File**.
5. Navigate to the saved location for the downloaded enic driver version and select **enic-2.1.2.50_esx55-offline_bundle-1906033.zip**.
6. Click **Open** to open the file.
7. Click **Yes** to upload the **.zip** file to **datastore1**.
8. Click the fourth button and select **Upload File**.
9. Navigate to the saved location for the downloaded fnic driver version and select **fnic_driver-1.6.0.10_esx55-offline_bundle-1897613.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 -d
/vmfs/volumes/datastore1/enic-2.1.2.50_esx55-offline_bundle-1906033.zip
esxcli -s <><var_vm_host_infra_01_ip>> -u root -p <><var_password>> software
vib install -d
/vmfs/volumes/datastore1/fnic_driver_1.6.0.10_esx55-offline_bundle-1897613.z
ip
esxcli -s <><var_vm_host_infra_02_ip>> -u root -p <><var_password>> software
vib install -d
/vmfs/volumes/datastore1/enic-2.1.2.50_esx55-offline_bundle-1906033.zip
esxcli -s <><var_vm_host_infra_02_ip>> -u root -p <><var_password>> software
vib install -d
/vmfs/volumes/datastore1/fnic_driver_1.6.0.10_esx55-offline_bundle-1897613.z
ip
```

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

```
C:\Program Files (<x86>)\VMware\VMware vSphere CLI>esxcli -s 192.168.175.58 -u roo
t -p NetApp!23 software vib install -d /vmfs/volumes/datastore1/enic-2.1.2.50_es
x55-offline_bundle-1906033.zip
Installation Result
Message: The update completed successfully, but the system needs to be rebooted for the changes to be effective.
Reboot Required: true
VIBs Installed: Cisco_bootbank_net-enic_2.1.2.50-10EM.550.0.0.1331820
VIBs Removed: VMware_bootbank_net-enic_1.4.2.15a-1vmw.550.0.0.1331820
VIBs Skipped:

C:\Program Files (<x86>)\VMware\VMware vSphere CLI>esxcli -s 192.168.175.58 -u roo
t -p NetApp!23 software vib install -d /vmfs/volumes/datastore1/fnic_driver_1.6.
0.10_esx55-offline_bundle-1897613.zip
Installation Result
Message: The update completed successfully, but the system needs to be rebooted for the changes to be effective.
Reboot Required: true
VIBs Installed: cisco_bootbank_scsi-fnic_1.6.0.10-10EM.550.0.0.1331820
VIBs Removed: VMware_bootbank_scsi-fnic_1.5.0.4-1vmw.550.0.0.1331820
VIBs Skipped:

C:\Program Files (<x86>)\VMware\VMware vSphere CLI>
```

Set Up VMkernel Ports and Virtual Switch

ESXi Host VM-Host-Infra-01

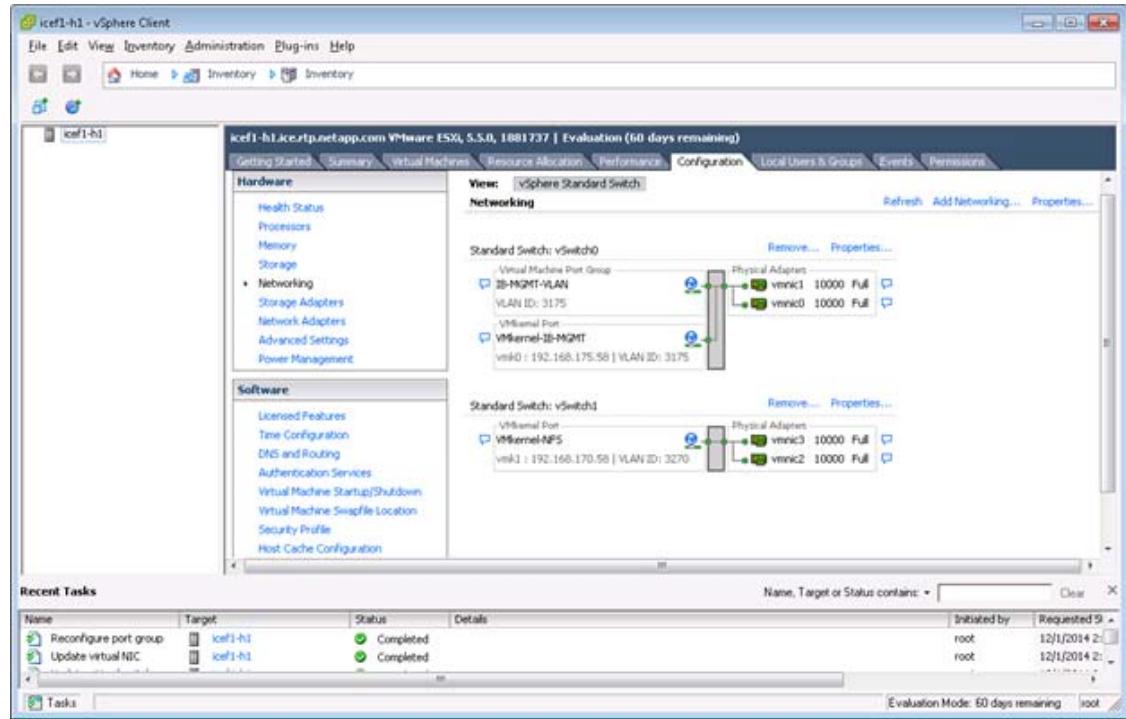


Note Repeat the steps in this section for all the ESXi Hosts.

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

1. From each vSphere Client, select 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. Select the Network Adapters tab.
6. Click Add and select the checkbox next to vmnic1. Click Next.
7. Click Next.
8. Click Finish.
9. Select the Ports tab.
10. Select the Management Network configuration and click Edit.
11. Change the network label to VMkernel-IB-MGMT and select the Management Traffic checkbox.
12. Click OK to finalize the edits for Management Network.
13. Select the VM Network configuration and click Edit.
14. Change the network label to IB-MGMT-VLAN and enter <<var_ib_mgmt_vlan_id>> in the VLAN ID (Optional) field.
15. Click OK to finalize the edits for VM Network.
16. Click Close to close vSwitch0 Properties.
17. Click Add Networking to add a vSwitch.
18. Select VMkernel and click Next.
19. Leave Create a vSphere standard switch selected and select the checkboxes for vmnic2 and vmnic3. Click Next.
20. Change the network label to VMkernel-NFS and enter <<var_server_nfs_vlan_id>> in the VLAN ID (Optional) field.
21. Click Next to continue with the NFS VMkernel creation.
22. Enter the IP address <<var_nfs_vlan_ip_host_01>> and the subnet mask <<var_nfs_vlan_ip_mask_host_01>> for the NFS VLAN interface for VM-Host-Infra-01.
23. Click Next to continue with the NFS VMkernel creation.
24. Click Finish to finalize the creation of the NFS VMkernel interface.
25. Click Properties on the right side of vSwitch1.
26. Select the vSwitch configuration and click Edit.
27. From the General tab, change the MTU to 9000.
28. Click OK to close the properties for vSwitch1.
29. Select the VMkernel-NFS configuration and click Edit.
30. Change the MTU to 9000.
31. Click OK to finalize the edits for the VMkernel-NFS network.
32. Click Add to add a network element.

33. Click Close to close vSwitch1 Properties.
34. The networking for the ESXi host should be similar to the following example:



Mount Required Datastores

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

To mount the required datastores, complete the following steps on each ESXi host:

1. From each vSphere Client, select 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. Select Network File System and click Next.
6. The wizard prompts for the location of the NFS export. Enter <<var_nfs_lif02_ip>> as the IP address for nfs_lif02.
7. Enter /infra_datastore_1 as the path for the NFS export.
8. Make sure that the Mount NFS read only checkbox is NOT selected.
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. Select Network File System and click Next.

14. The wizard prompts for the location of the NFS export. Enter <<var_nfs_lif01_ip>> as the IP address for nfs_lif01.
15. Enter /infra_swap as the path for the NFS export.
16. Make sure that the Mount NFS read only checkbox is NOT selected.
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, complete the following steps on each host:

1. From each vSphere Client, select 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, complete the following steps:
 - a. Click General in the left pane and select 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, select the Restart NTP Service to Apply Changes checkbox and click OK.
9. In the Time Configuration dialog box, complete the following steps:
 - a. Select the NTP Client Enabled checkbox and click OK.
 - b. Verify that the clock is now set to approximately the correct time.



Note 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, complete the following steps on each ESXi host:

1. From each vSphere Client, select 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. Select 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.