NetApp Verified Architecture

FlexPod Express with VMware vSphere 6.0U2, NetApp E-Series, and Cisco UCS Mini

NVA Design and Deployment

Arvind Ramakrishnan, NetApp
January 2017 | NVA-0032 | Version 1.0

Reviewed by

CISCO

NetApp®

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Program Summary

The FlexPod® Express solution portfolio is designed to cater to small and midsized businesses by providing them a data center solution starting at a lower price point and with a wide variety of features that is inherited from FlexPod Datacenter.

This solution introduces the NetApp® E-Series storage controllers to the FlexPod Express portfolio. The entry-level E-series storage systems are chosen to provide a solution with lower TCO, and the compute infrastructure is built using the Cisco UCS Mini systems.

2 Solution Overview

The FlexPod Express with E-Series solution is a suitable platform for running a variety of virtualization hypervisors as well as bare-metal operating systems and enterprise workloads. FlexPod Express delivers not only a baseline configuration, but also the flexibility to be sized and optimized to accommodate many different use cases and requirements. The small, medium, and large FlexPod Express with E-Series configurations are low-cost, standardized infrastructure solutions that are developed to meet the needs of small and midsize businesses. Each configuration provides a standardized base platform capable of running several business-critical applications while providing scalability options to enable the infrastructure to grow with the demands of the business.

Some of the highlights of the FlexPod Express with E-Series solution are as follows:

- Combines all application and data needs into one platform
- Is suitable for small to midsize organizations and for remote and departmental deployments
- Provides easy infrastructure scaling
- Reduces cost and complexity

2.1 Solution Technology

The FlexPod Express configurations described in this document are built using the Cisco UCS Mini chassis for compute and the NetApp E-Series storage systems E2824 for storage. In addition to these components, an existing network infrastructure in the customer’s data center or at the deployment site is used to uplink this solution and to provide additional network resources.

This FlexPod Express solution is classified into two categories: small/starter and all flash. The validation/testing was performed on the small/starter hardware kit; the same approach can be used to build the all-flash configuration.

Figure 1) FlexPod Express architecture diagram.

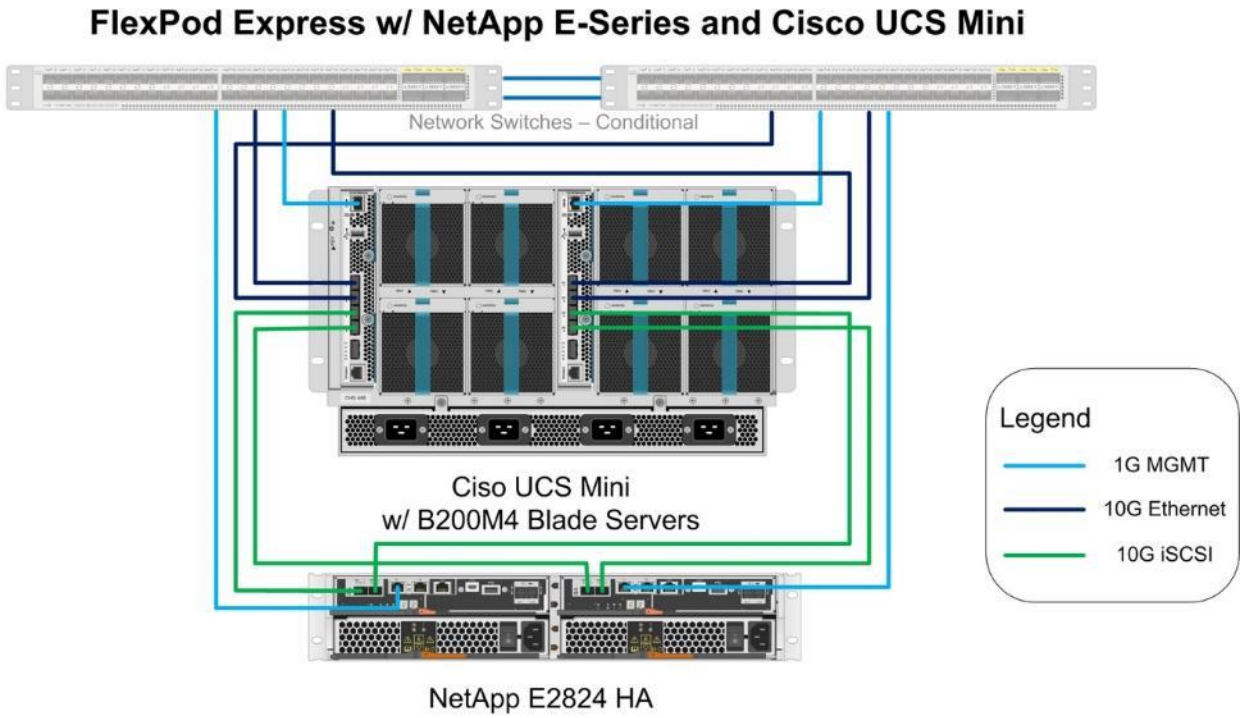


Figure 1 represents the architecture of the FlexPod Express small/starter pack. This architecture can be extended to the all-flash configuration by adding Cisco UCS B200 M4 blade servers and SSD disk drives to the E-Series controllers.

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

Specifically, FlexPod Express is a defined set of hardware and software that serves as an integrated foundation for both virtualized and nonvirtualized solutions. This FlexPod Express architecture includes NetApp E-Series storage, NetApp SANtricity®, Cisco Unified Computing System (Cisco UCS) Mini, and VMware vSphere software. The design is flexible and has a low data center footprint of approximately eight rack units that the computing and storage can easily fit in one data center rack or can be deployed as per the customer's data center design.

One benefit of the FlexPod Express architecture is the ability to customize, or "flex," the environment to suit a customer's requirements. The reference architecture detailed in this document highlights the resiliency, cost benefit, and ease of deployment of an iSCSI-based storage solution.

Figure 1 shows the VMware vSphere built on FlexPod with E-Series components and the connections for a direct-attach configuration with iSCSI-based storage. This design uses:

- Cisco UCS Mini chassis with B-Series B200 M4 servers
- Cisco UCS virtual interface card (VIC) 1340
- NetApp E-Series E2824 storage controllers

The Cisco UCS Mini chassis and the E-Series controllers are direct attached in a highly available design. This infrastructure is deployed to provide iSCSI-booted hosts with block-level access to shared storage datastores.

This solution is designed to cater to greenfield and brownfield environments. In greenfield environments, the organization might consider using a Cisco Nexus 3000 series switch due its lower cost or any other Cisco Nexus model as desired. In existing or brownfield environments, the FlexPod Express solution can be plugged to the existing network/switching infrastructure that is available on site. The solution design does not have any storage traffic traversing the switching infrastructure. The infrastructure is used for Ethernet connectivity to the Cisco UCS and E-Series for ingress and egress traffic.

Note: This FlexPod Express solution does not dictate the Ethernet switching platform in the environment. Non-Cisco switching platforms are not defined in the FlexPod solution portfolio, but when present, third-party switches may provide the functionality to deliver Fibre Channel (FC), iSCSI, or other traffic such as vMotion by providing support for tagged VLANs and a path between fabric interconnects for each VLAN in the solution.

In this deployment, the infrastructure is connected to a pair of Cisco Nexus 9000 switches that are in a vPC configuration. The network configuration required for this solution is described in Appendix: Cisco Nexus 9000 Configuration.

Table 1 lists the hardware components that are essential to build the small and all-flash FlexPod Express configurations.

Table 1) FlexPod Express configurations.

Component	Small/Starter	All Flash
E-Series controller	NetApp E-Series 2824	NetApp E-Series 2824
Disk drive	900GB SAS X 12	800GB SSD X 24
E-Series Express Pack	E2824-0004-EP	E2824-0003-EP
Cisco UCS blade servers	B200 M4 X 2	B200 M4 X 4

NetApp E-Series 2800 Storage Systems

The NetApp E2800 storage system offers all-flash and hybrid configuration options to streamline IT infrastructure and drive down costs. These systems are purpose built to optimize performance for mixed workloads. The E2800 hosts a next-generation controller that is built on Intel processor technology, along with a 12Gb SAS infrastructure that improves IOPS and throughput to help extract value from data and act more quickly.

The E2800 offers an improved user experience with an on-box, web-based interface that is modern, simple, and clean. This intuitive interface simplifies configuration and maintenance while providing enterprise-level storage capabilities to deliver consistent performance, data integrity, and security.

Some of the highlights of the E-Series systems are as follows:

- **Dynamic Disk Pools (DDP).** DDP simplifies the management of traditional RAID groups by distributing data parity information and spare capacity across a pool of drives. DDP enhances data protection by enabling faster drive rebuilds after a failure and protecting against potential data loss if additional drive failures occur. DDP dynamic rebuild technology uses every drive in the pool to rebuild a failed drive, enabling exceptional performance under failure.
- **Price versus performance.** The E-Series systems feature a next-generation entry-level controller that improves IOPS and throughput. Higher performance with solid-state drives (SSDs) enables the E2800 to maximize storage density, requiring fewer disks for better performance. High-performance file systems and data-intensive bandwidth applications benefit from the ability of the E2800 to sustain higher read and write throughput. Database-driven transactional applications benefit from the higher IOPS and low latency of the E2800. The controllers in the E2800 increase performance to a blazing-fast 300,000 IOPS.

- **SSD cache.** The SSD cache feature provides intelligent analytics-based caching capability for read-intensive workloads. Hot data is cached by using higher-performance, lower-latency SSDs in the drive shelves. SSD cache is expandable to up to 5TB per storage system.
- **Modular flexibility.** Flexible configuration options, including all flash as well as hybrid SSD and HDD, enable users to build just one architecture to support a multitiered data model. The E2800 offers multiple form factors and drive technology options to meet customer requirements.
- **Maximum storage density.** The E2800 is designed for capacity-intensive environments that also require efficient data center space, power, and cooling utilization. The system's ultradense, 60-drive, 4U disk shelf provides industry-leading performance and space efficiency to reduce rack space by up to 60%. Its high-efficiency power supplies can lower power and cooling use by up to 40%.
- **Proven data reliability, availability, and serviceability.** The E2800 is based on a field-proven architecture that delivers high reliability and greater than five-9s availability, often exceeding six-9s availability when NetApp best practices are followed. The E2800 is easy to install and to use. It is optimized for performance efficiency, and it fits into most application environments. The E2800 system offers excellent price to performance for small and medium-sized businesses, remote and branch offices, and workgroups within an enterprise.
- **Intuitive management.** NetApp SANtricity software offers a combination of comprehensive features and ease of use. Storage administrators appreciate the extensive configuration flexibility, which allows optimal performance tuning and complete control over data placement. With its dynamic capabilities, SANtricity software supports dynamic expansion, reconfigurations, and maintenance without interrupting storage system I/O. SANtricity Storage Manager gives full control and visibility across your E-Series storage systems. Released with the E2800, SANtricity System Manager is a modern, browser-based, on-box tool that allows users to manage and monitor the E2800 system by using an intuitive web interface.
- **Disk encryption.** To enable comprehensive security for data at rest without sacrificing performance or ease of use, SANtricity encryption combines local key management with drive-level encryption. Because all drives eventually leave the data center through redeployment, retirement, or service, it is reassuring to know that the sensitive data isn't leaving with them. SANtricity also supports FIPS-certified hard drives for security-sensitive customers.

Cisco UCS Mini

Cisco UCS is a next-generation data center platform that unites computing, networking, storage access, and virtualization resources into a cohesive system designed to reduce total cost of ownership (TCO) and increase business agility (Figure 2). The system integrates a low-latency, lossless 10 Gigabit Ethernet unified network fabric with enterprise-class, x86-architecture servers. The system is an integrated, scalable, multichassis platform in which all resources participate in a unified management domain.

The main components of the Cisco UCS are as follows:

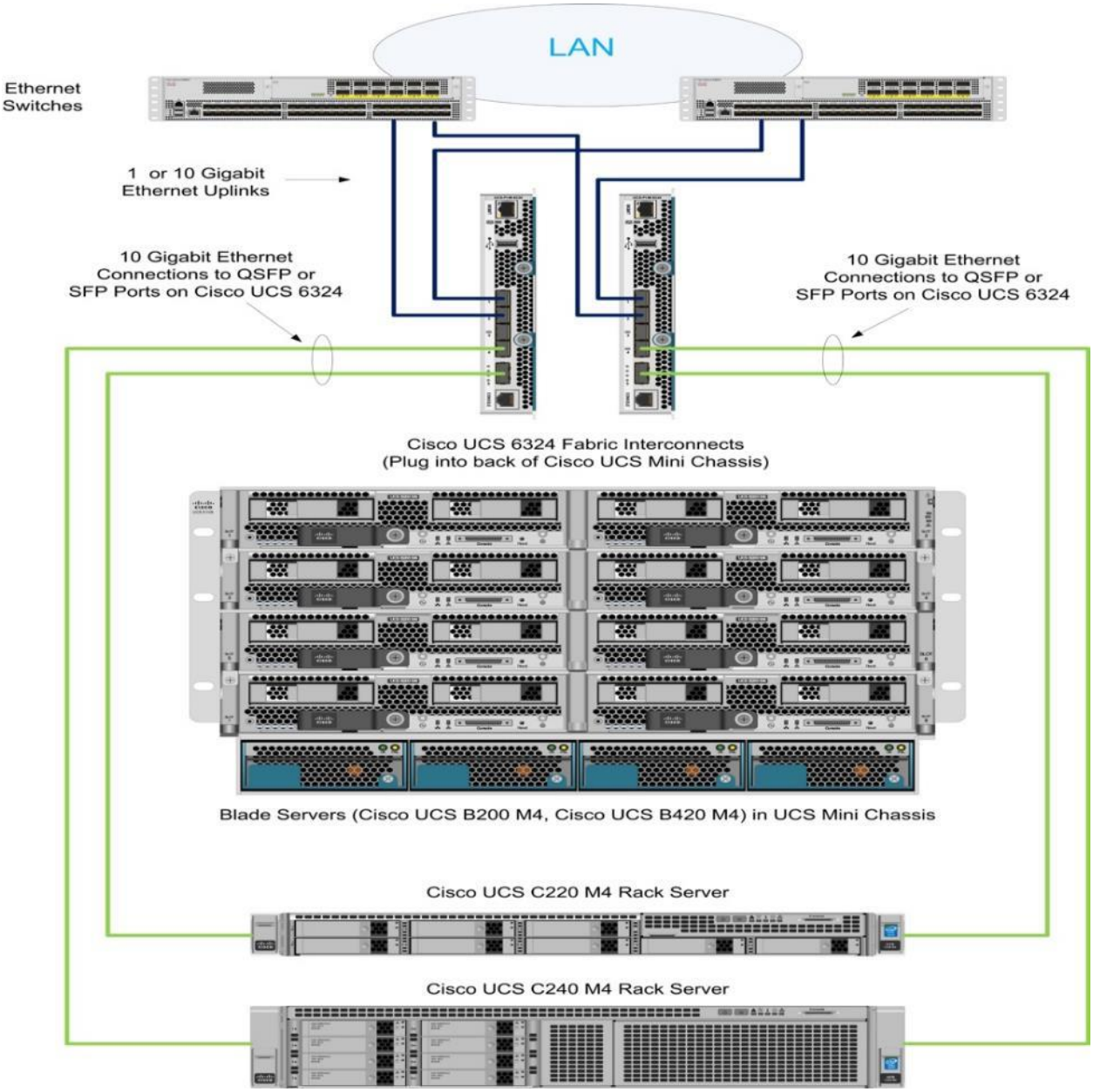
- **Compute**. The system is based on an entirely new class of computing system that incorporates rack mount and blade servers based on Intel processors.
- **Network**. The system is integrated onto a low-latency, lossless, 10Gbps unified network fabric. This network foundation consolidates LANs, SANs, and high-performance computing networks, which are separate networks today. The unified fabric lowers costs by reducing the number of network adapters, switches, and cables and by decreasing the power and cooling requirements.
- **Virtualization**. The system unleashes the full potential of virtualization by enhancing the scalability, performance, and operational control of virtual environments. Cisco security, policy enforcement, and diagnostic features are now extended into virtualized environments to better support changing business and IT requirements.
- **Storage access**. The system provides consolidated access to both SAN storage and network-attached storage (NAS) over the unified fabric. By unifying the storage access, the Cisco Unified Computing System can access storage over Ethernet (NFS or iSCSI), Fibre Channel, and Fibre Channel over Ethernet (FCoE). This provides customers with storage choices and investment

protection. In addition, the server administrators can preassign storage access policies to storage resources for simplified storage connectivity and management, leading to increased productivity.

Cisco UCS fuses access layer networking and servers. This high-performance, next-generation server system provides a data center with a high degree of workload agility and scalability.

The Cisco UCS 6324 fabric interconnect (FI) extends the Cisco UCS architecture into environments with lesser resource requirements. Providing the same unified server and networking capabilities as the full-scale Cisco UCS solution, the Cisco UCS 6324 FI embeds the connectivity within the Cisco UCS 5108 blade server chassis to provide a smaller domain of up to 15 servers (eight blade servers and up to seven direct-connect rack servers).

Figure 2) Cisco UCS: highly cohesive architecture.

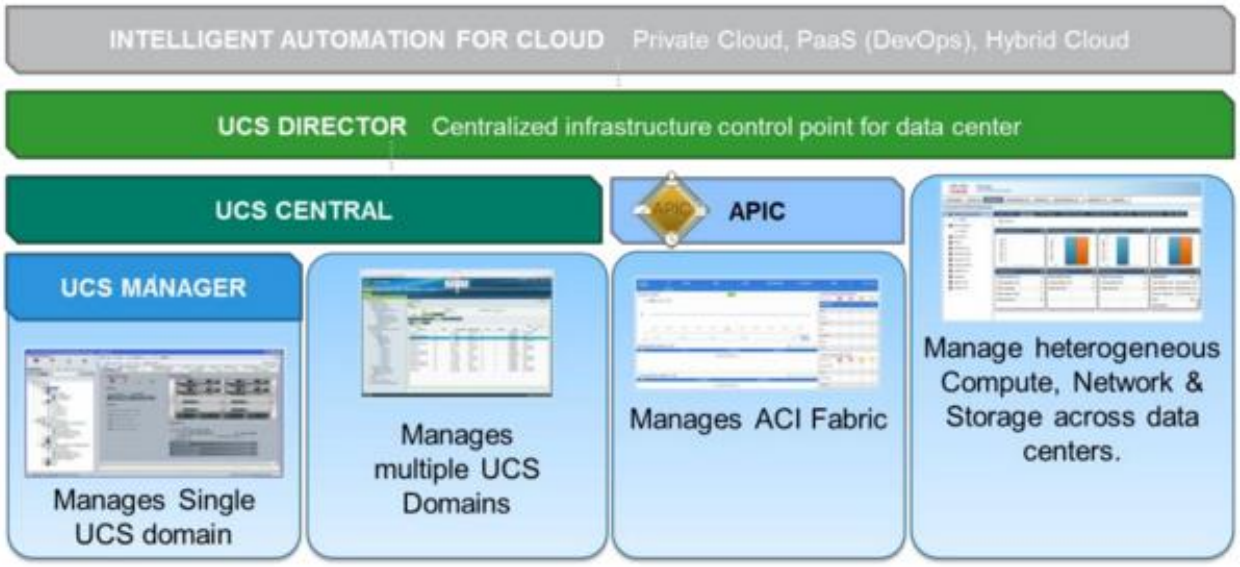


Cisco UCS 6324 Fabric Interconnect Overview

The Cisco UCS 6324 fabric interconnect (Figure 4) provides the management, LAN, and storage connectivity for the Cisco UCS 5108 blade server chassis and direct-connect rack-mount servers. It provides the same full-featured Cisco UCS management capabilities and XML API as the full-scale Cisco UCS solution in addition to integrating with Cisco UCS Central Software and Cisco UCS Director (Figure 3).

From a networking perspective, the Cisco UCS 6324 FI uses a cut-through architecture, supporting deterministic, low-latency, line-rate 10GbE on all ports; switching capacity of up to 500Gbps; and 80Gbps uplink bandwidth for each chassis, independent of packet size and enabled services. Sixteen 10Gbps links connect to the servers, providing a 20Gbps link from each Cisco UCS 6324 Fabric Interconnect to each server. The product family supports Cisco low-latency, lossless 10GbE unified network fabric capabilities, which increase the reliability, efficiency, and scalability of Ethernet networks. The fabric interconnect supports multiple traffic classes over a lossless Ethernet fabric from the blade through the fabric interconnect. Significant TCO savings come from an FCoE-optimized server design in which network interface cards (NICs), host bus adapters (HBAs), cables, and switches can be consolidated.

Figure 3) Cisco UCS management and fabric architecture.



Unified Fabric with FCoE: I/O Consolidation

The Cisco UCS 6324 FI is built to consolidate LAN and storage traffic onto a single unified fabric, eliminating the capital expenditures (capex) and operating expenses (opex) associated with multiple parallel networks, different types of adapter cards, switching infrastructure, and cabling within racks. The unified ports allow the fabric interconnect to support direct connections from Cisco UCS to FC, FCoE, and iSCSI storage devices.

Cisco UCS Manager

The Cisco UCS 6324 FI hosts and runs Cisco UCS Manager in a highly available configuration, enabling the fabric interconnects to fully manage all Cisco UCS elements. The Cisco UCS 6324 fabric interconnects support out-of-band management through a dedicated 10/100/1000Mbps Ethernet management port. Cisco UCS Manager is typically deployed in a clustered active-passive configuration with two Cisco UCS 6324 fabric interconnects connected through the cluster interconnect built into the chassis.

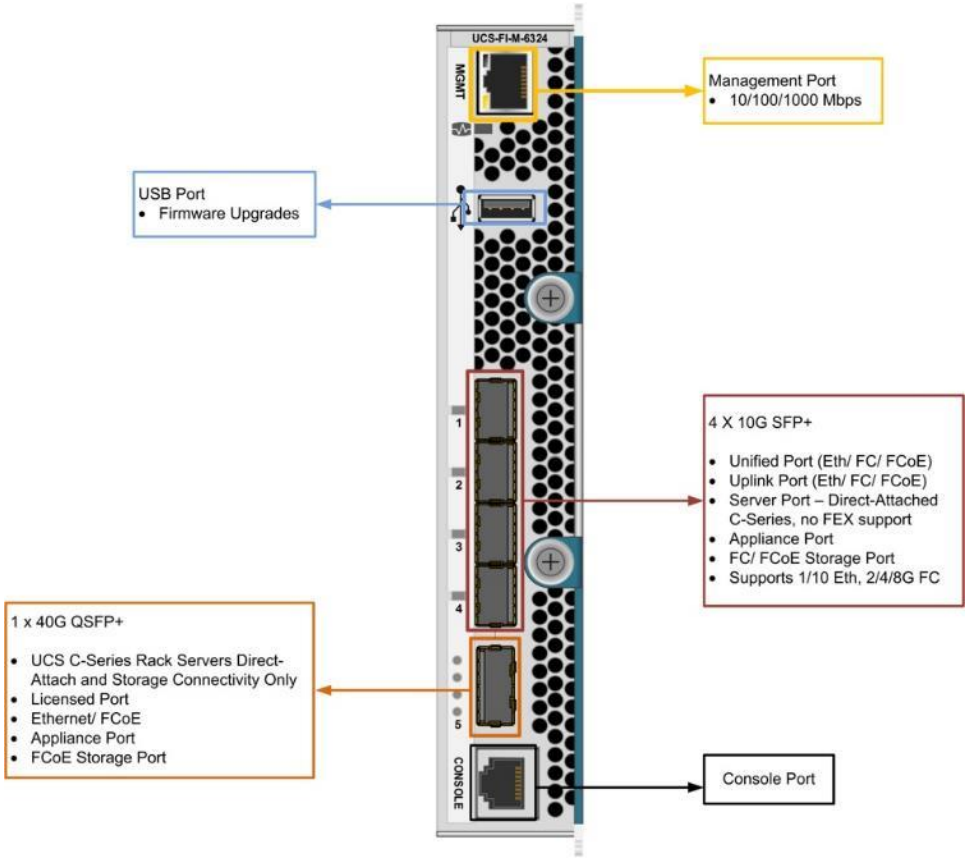
Optimization for Virtualization

For virtualized environments, the Cisco UCS 6324 FI supports Cisco virtualization-aware networking and Cisco Data Center Virtual Machine Fabric Extender (VM-FEX) architecture. Cisco Data Center VM-FEX allows the interconnects to provide policy-based virtual machine (VM) connectivity, with network properties moving with the virtual machine and a consistent operational model for both physical and virtual environments.

Cisco UCS 6324 Fabric Interconnect

The Cisco UCS 6324 FI (Figure 4) is a 10GbE, FCoE, and FC switch offering up to 500Gbps throughput and up to four unified ports and one scalability port.

Figure 4) Cisco UCS 6324 fabric interconnect.



I/O Adapters

The FlexPod with Cisco UCS Mini uses the Cisco UCS VIC for all designs. VIC obviates the need for multiple NICs and HBAs by converging LAN and SAN traffic in a single physical interface. The Cisco VIC delivers 256 virtual interfaces and supports Cisco VM-FEX technology. The Cisco VIC provides I/O policy coherency and visibility to enable true workload mobility in virtualized environments. The Cisco VIC is available in a number of form factors for both Cisco UCS B-Series blades and C-Series rack servers. This wire-once architectural approach and centralized management through the Cisco UCS Manager helps you:

- Simplify cabling
- Reduce points of management
- Lower costs

3 Technology Requirements

This section covers the technology requirements for the FlexPod Express with VMware vSphere 6.0U2, NetApp E-Series, and Cisco UCS Mini solution.

3.1 Hardware and Software Requirements

Table 2 lists the hardware components and their corresponding software versions required to implement the solution.

Table 2) Hardware requirements.

Layer	Hardware	Software	Details
Compute	Cisco UCS Fabric Interconnect FI-6324UP	3.1(1h)	Embedded management
	Cisco UCS B200M4	3.1(1h)	Software bundle release
	Cisco eNIC	2.3.0.10	Ethernet driver for Cisco VIC
	Cisco VIC 1340	4.1(1)	Cisco virtual interface card firmware
Storage	NetApp E2824 with 900GB SAS drives	SANtricity 11.30	Storage operating system version

Table 3 lists the additional software components required to implement the solution.

Table 3) Software requirements.

Software	Version	Details
VMware vSphere ESXi	6.0U2	Host operating system version
VMware vCenter	6.0U2	VMware vCenter Appliance

4 Configuration Guidelines

This document provides details for configuring a fully redundant, highly available configuration for a FlexPod Express unit with NetApp E-Series storage, which uses a pair of controllers in an HA configuration. Controllers are referred to as A and B. The Cisco UCS Mini interconnects are similarly identified. Additionally, this document details the steps for provisioning multiple Cisco UCS hosts, and these are identified sequentially: VM-Host-01, VM-Host-02, and so on. Finally, to indicate that the reader should include information pertinent to your environment in a given step, `<text>` appears as part of the command structure.

This document is intended to enable the reader to fully configure the customer environment. In this process, various steps require the reader to insert customer-specific naming conventions, IP addresses, and VLAN schemes, as well as to record appropriate MAC addresses. Table 4 describes the VLANs necessary for deployment as outlined in this guide.

Table 6 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) Necessary VLANs.

VLAN Name	VLAN Purpose	ID Used in Validating This Document
Mgmt in band	VLAN for in-band management interfaces	3366
Native	VLAN to which untagged frames are assigned	2
iSCSI-A	VLAN for iSCSI traffic for fabric A	3372
iSCSI-B	VLAN for iSCSI traffic for fabric B	3373
vMotion	VLAN designated for the movement of VMs from one physical host to another	3374
VM Traffic	VLAN for VM application traffic	3375

Table 5) VMware virtual machines.

Virtual Machine Description	Host Name
vCenter Server	

Table 6) Configuration variables.

Variable	Description	Customer Implementation Value
<<var_controllerA_mgmt_ip>>	Out-of-band management IP for cluster node 01	
<<var_controllerA_mgmt_mask>>	Out-of-band management network netmask	
<<var_controllerA_mgmt_gateway>>	Out-of-band management network default gateway	
<<var_controllerB_mgmt_ip>>	Out-of-band management IP for cluster node 02	
<<var_controllerB_mgmt_mask>>	Out-of-band management network netmask	
<<var_controllerB_mgmt_gateway>>	Out-of-band management network default gateway	
<<var_array_name>>	Storage array host name	
<<var_password>>	Global default administrative password	
<<var_dns_domain_name>>	DNS domain name	
<<var_nameserver_ip>>	DNS server IPs	
<<var_location>>	Location string for equipment	
<<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_community>>	Storage cluster SNMP v1/v2 community name	
<<var_mailhost>>	Mail server host name	

Variable	Description	Customer Implementation Value
<<var_storage_admin_email>>	Administrator e-mail address	
<<var_nexus_A_hostname>>	Cisco Nexus A host name	
<<var_nexus_A_mgmt0_ip>>	Out-of-band Cisco Nexus A management IP address	
<<var_nexus_A_mgmt0_netmask>>	Out-of-band management network netmask	
<<var_nexus_A_mgmt0_gw>>	Out-of-band management network default gateway	
<<var_nexus_B_hostname>>	Cisco Nexus B host name	
<<var_nexus_B_mgmt0_ip>>	Out-of-band Cisco Nexus B management IP address	
<<var_nexus_B_mgmt0_netmask>>	Out-of-band management network netmask	
<<var_nexus_B_mgmt0_gw>>	Out-of-band management network default gateway	
<<var_ib-mgmt_vlan_id>>	In-band management network VLAN ID	
<<var_native_vlan_id>>	Native VLAN ID	
<<var_oob-mgmt_vlan_id>>	Out-of-band management network VLAN ID	
<<var_vmotion_vlan_id>>	VMware vMotion VLAN ID	
<<var_vm-traffic_vlan_id>>	VM traffic VLAN ID	
<<var_nexus_vpc_domain_id>>	Unique Cisco Nexus switch VPC domain ID	
<<var_iscsi_a_vlan_id>>	Fabric A iSCSI VLAN ID	
<<var_iscsi_b_vlan_id>>	Fabric B iSCSI VLAN ID	
<<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_ucsb_mgmt_ip>>	Cisco UCS FI B out-of-band management IP address	
<<var_vcenter_server_ip>>	vCenter Server IP	
<<var_vm_host_01_A_iscsi>>	iSCSI IP address of VM-Host-01 vNIC iSCSI-A	
<<var_vm_host_02_A_iscsi>>	iSCSI IP address of VM-Host-02	

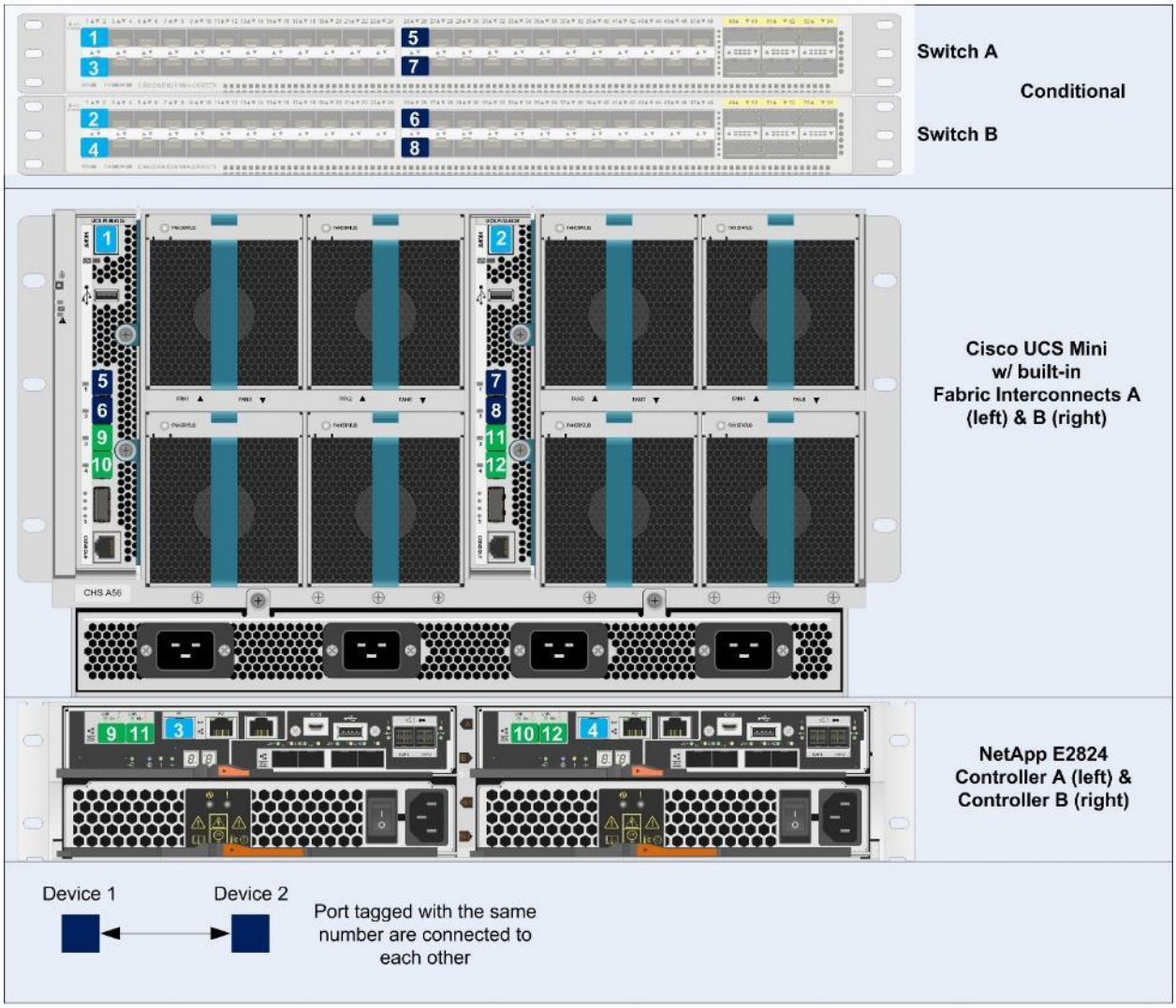
Variable	Description	Customer Implementation Value
	vNIC iSCSI-A	
<<var_controllerA_iscsi_port_1>>	Controller A iSCSI port 1 IP address (fabric A)	
<<var_controllerB_iscsi_port_1>>	Controller B iSCSI port 1 IP address (fabric A)	
<<var_vm_host_01_B_iscsi>>	iSCSI IP address of VM-Host-01 vNIC iSCSI-B	
<<var_vm_host_02_B_iscsi>>	iSCSI IP address of VM-Host-02 vNIC iSCSI-B	
<<var_controllerA_iscsi_port_3>>	Controller A iSCSI port 3 IP address (fabric B)	
<<var_controllerB_iscsi_port_3>>	Controller B iSCSI port 3 IP address (fabric B)	
<<var_iscsi_a_subnet_mask>>	Subnet mask for iSCSI A fabric	
<<var_iscsi_b_subnet_mask>>	Subnet mask for iSCSI B fabric	
<<var_vmhost_infra01_ip>>	VMware ESXi host 01 in-band management IP	
<<var_vmhost_infra02_ip>>	VMware ESXi host 02 in-band management IP	
<<var_vmotion_vlan_id_ip_host-01>>	vMotion VLAN IP address for ESXi host 01	
<<var_vmotion_vlan_id_mask_host-01>>	vMotion VLAN netmask for ESXi host 01	
<<var_vmotion_vlan_id_ip_host-02>>	vMotion VLAN IP address for ESXi host 02	
<<var_vmotion_vlan_id_mask_host-02>>	vMotion VLAN netmask for ESXi host 02	

5 Physical Infrastructure

5.1 FlexPod Express Cabling Using E-Series with 10Gb iSCSI Host Interface Cards and Cisco UCS Mini

Figure 5 shows the cabling diagram for the FlexPod Express configuration.

Figure 5) FlexPod Express cabling diagram.



The information provided in Table 7 through Table 10 corresponds to each connection shown in Figure 5.

Table 7) Cisco UCS fabric interconnect A cabling information.

Local Device	Local Port	Connection	Remote Device	Remote Port	Cabling Code
Cisco UCS fabric interconnect A	Eth 1/1	10GbE	Switch A	Any	5

Local Device	Local Port	Connection	Remote Device	Remote Port	Cabling Code
	Eth 1/2	10GbE	Switch B	Any	6
	Eth 1/3	10GbE	NetApp controller A	0a	9
	Eth 1/4	10GbE	NetApp controller B	0a	10
	MGMT	GbE	Switch A	Any	1

Table 8) Cisco UCS Fabric Interconnect B cabling information.

Local Device	Local Port	Connection	Remote Device	Remote Port	Cabling Code
Cisco UCS fabric interconnect B	Eth 1/1	10GbE	Switch A	Any	7
	Eth 1/2	10GbE	Switch B	Any	8
	Eth 1/3	10GbE	NetApp controller A	0b	11
	Eth 1/4	10GbE	NetApp controller B	0b	12
	MGMT	GbE	Switch B	Any	2

Table 9) NetApp controller A cabling information.

Local Device	Local Port	Connection	Remote Device	Remote Port	Cabling Code
NetApp controller A	Port 1	GbE	Switch A	Any	3
	0a	10GbE	Cisco UCS fabric interconnect A	Eth 1/3	9
	0b	10GbE	Cisco UCS fabric interconnect B	Eth 1/3	11

Table 10) NetApp controller B cabling information.

Local Device	Local Port	Connection	Remote Device	Remote Port	Cabling Code
NetApp controller B	Port 1	GbE	Switch B	Any	4

Local Device	Local Port	Connection	Remote Device	Remote Port	Cabling Code
	0a	10GbE	Cisco UCS fabric interconnect A	Eth 1/4	10
	0b	10GbE	Cisco UCS fabric interconnect B	Eth 1/4	12

6 Deployment Procedures

6.1 Network/Switching Infrastructure

It is recommended to have the network/switching infrastructure ready before configuring the storage and compute infrastructure. This helps to enable a seamless deployment and make sure that interconnectivity between components in the infrastructure is established.

In this deployment, a pair of Cisco Nexus 9000 series switches were used. The essential network configuration required for this solution is described in the appendix of this document.

6.2 NetApp E-Series 2824 Configuration: Part I

E-Series E-2824

Table 11) E-Series E2824 prerequisites.

Requirement	Reference
Before you begin	Handbook
Preparing your site	Site Preparation Guide
Installing a NetApp cabinet	3040 40U Cabinet Installation Guide
Cabling the hardware	Hardware Cabling Guide
Applying power	E2800 System Monitoring Guide

NetApp Hardware Universe

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

- Access the Hardware Universe application to view the System Configuration guides. Click the Platforms tab and select E-Series to view the compatibility between SANtricity software versions and NetApp storage appliances with the desired specifications.
- Alternatively, to compare components by storage appliance, click the Compare Storage Systems tab.

Controllers

This document assumes that the reader workstation has network access to the storage array, either through a direct connection to the storage array management interfaces or through a switched network. A nonrouted connection is required for the initial configuration of the storage array management interfaces.

Perform Initial Configuration of the E2824 System

To launch the System Manager on the E2824 system for the first time, complete the following steps:

1. Connect the management port (port 1) of controller A to the reader workstation.
2. Set the IP address of the reader workstation to 192.168.128.100 with a subnet mask of 255.255.255.0. Leave the gateway and DNS servers blank.
3. Launch a browser and access controller A using IP 192.168.128.101.
4. The SANtricity System Manager setup wizard launches. Click Next.
5. Enter a name for the storage array `<<var_storagearray_name>>` and check if the hardware components are listed correctly. Click Next.
6. Click Next in the Verify Hosts section.
7. Under Select Applications, select VMware (ESXi 5.1 or later) using Virtual Machine File System (VMFS) access. Click Next.
8. Enter a name for the workload `<<var_storage_workload_name>>` and click Next.
9. Choose Yes to accept the recommended pool configuration or No to create one later.

   Note: Disk pools and/or volume groups can be created based on the user's requirement. In this configuration, a disk pool is created.

10. (Optional) Enter a different name for the pool.
11. Click Next.
12. Configure the alerts by providing the mail server details and recipient e-mail address.

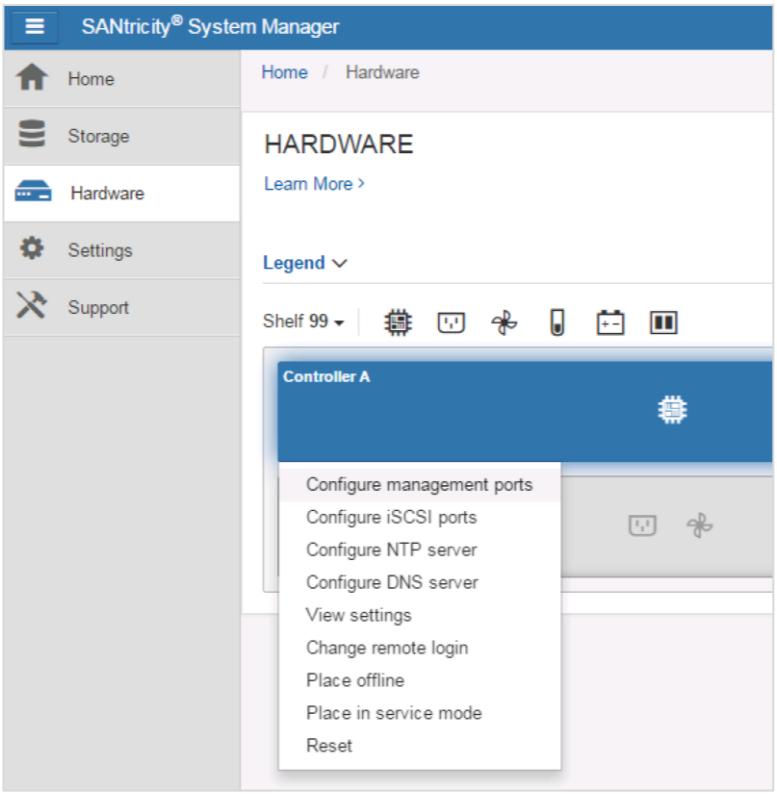
    Note: Select the Do this later option if the necessary information is not available.

13. Enable AutoSupport® by clicking the checkbox. Also, enable AutoSupport OnDemand and Remote Diagnostics if necessary.
14. Review the configuration and click Finish.
15. Click Close.

Configure Management Interfaces on the Controllers

To configure the management interfaces of controllers A and B, complete the following steps:

1. In the left pane, click Hardware. In the right pane, click Show back of shelf.
2. Click Controller A and select Configure management ports from the drop-down menu.



3. Select Port P1 and click Next.
4. Leave the speed and duplex mode set to Auto-negotiate.
5. Clear the Enable IPv6 checkbox and click Next.

   Note: This configuration uses IPv4.

6. If a DHCP source is used, leave the selection set to Automatically obtain configuration from DHCP server. If no DHCP source is used, select Manually specify static configuration and enter the following details:
   - `<<var_controller_A/B_mgmt>>`
   - `<<var_controller_A/B_subnet>>`
   - `<<var_controller_A/B_gateway>>`
7. Click Finish.
8. Click Yes to confirm the network settings.

   Note: Connectivity to the storage array is lost during this process. Reconnect to the storage array using the newly configured management IP address.

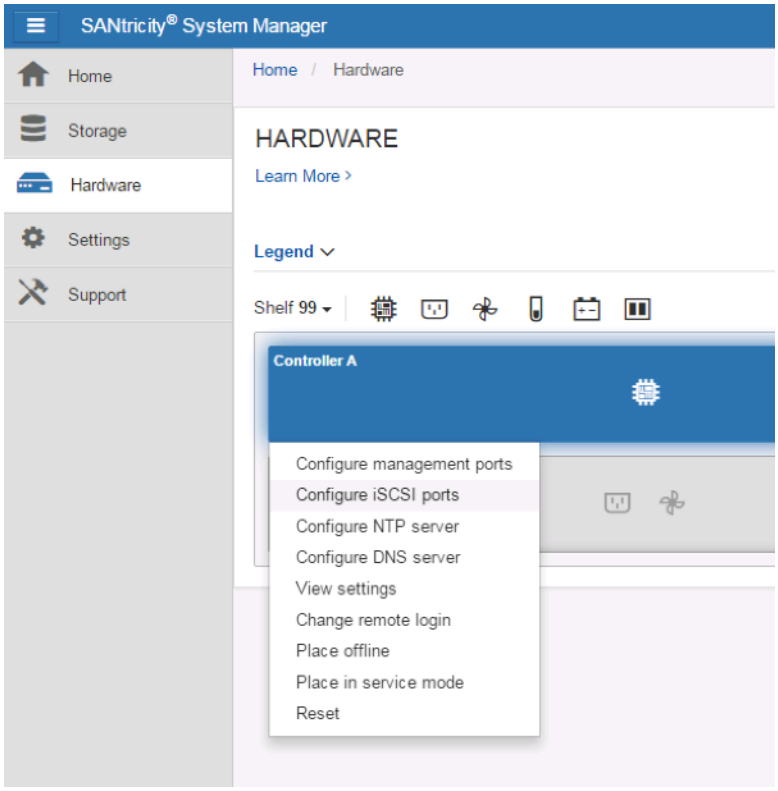
   Note: Change the IP address of the reader workstation to its original configuration.

9. Connect the management ports of controller A and controller B to the network infrastructure.
10. Repeat steps 1 through 7 for configuring the management IP address for controller B.

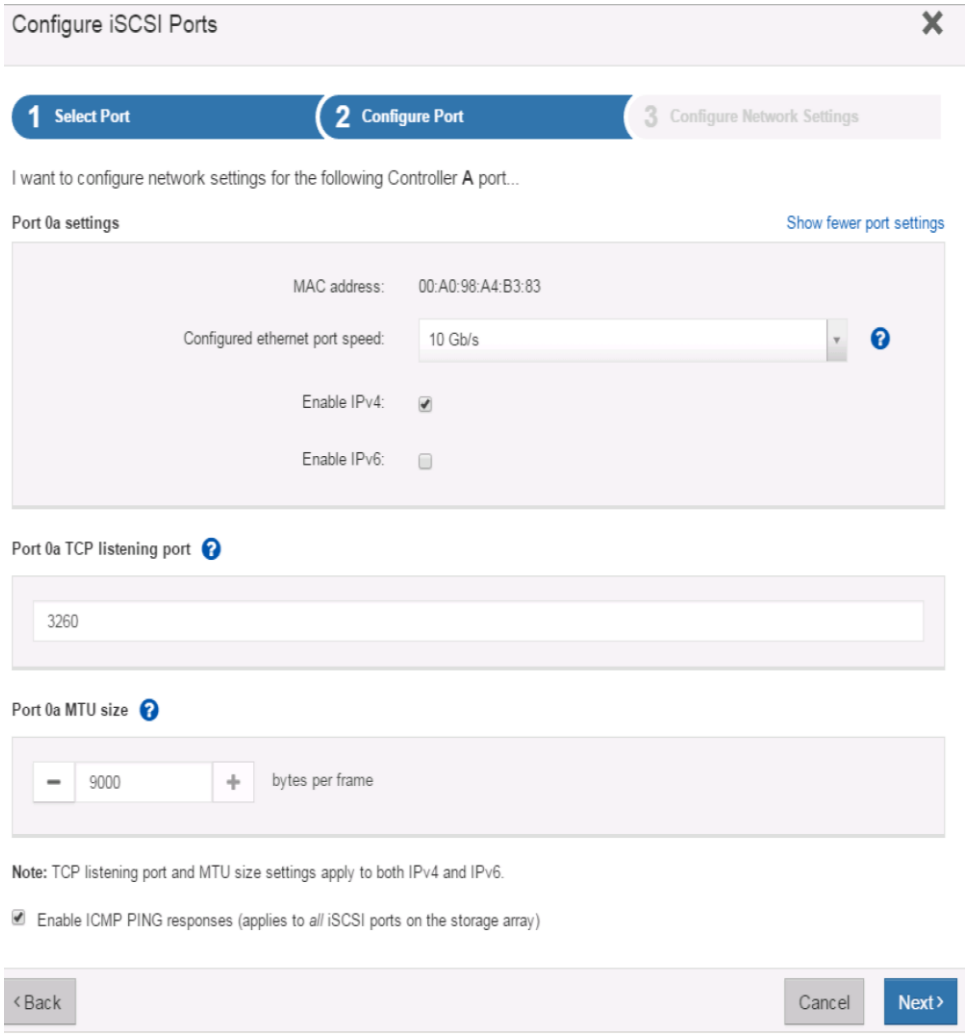
Configure iSCSI Interfaces on the Controllers

To configure the iSCSI interfaces on controller A and controller B, complete the following steps:

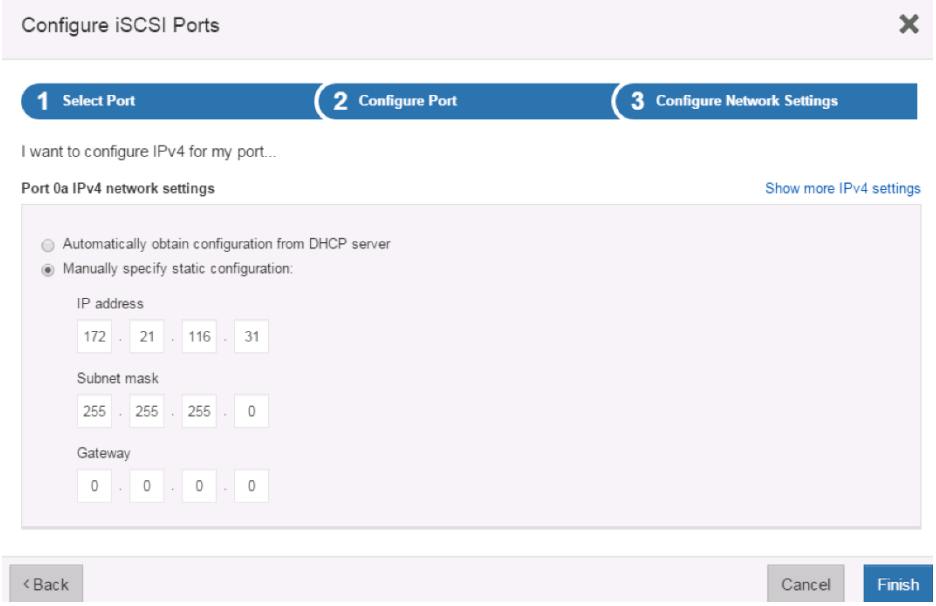
1. In the left pane, click Hardware. In the right pane, click Show back of shelf.
2. Click Controller A and select Configure iSCSI ports from the drop-down menu.



3. Do as follows:
   a. Select Port 0a from the drop-down options and click Next.
   b. Click Show more port settings.
   c. Set the Ethernet port speed to 10Gbps.
   d. Clear the Enable IPv6 option.
   e. Retain the TCP listening port settings at the defaults.
   f. Set the port MTU size to 9000 and click Next.



4. Select the Manually specify the static configuration option. Do as follows:
   a. Enter the iSCSI A VLAN IP address for controller A: `<<var_controller_A_iSCSI_A_IP>>`.
   b. Enter the subnet mask for the iSCSI IP address: `<<var_controller_A_iSCSI_A_netmask>>`.
   c. Click Finish.



5. Click Yes to confirm the iSCSI settings.

   Note: This process takes a couple of minutes to complete.

6. In the left pane, click Hardware. In the right pane, click Show back of shelf.
7. Click Controller A and select Configure iSCSI ports. Do as follows:
   a. Select Port 0b and click Next.
   b. Click Show more port settings.
   c. Set the Ethernet port speed to 10Gbps.
   d. Clear the Enable IPv6 option.
   e. Leave the TCP listening port set to the default.
   f. Set the port MTU size to 9000 and click Next.
8. Select the Manually specify the static configuration option and do as follows:
   a. Enter the iSCSI B VLAN IP address for controller A: `<<var_controller_A_iSCSI_B_IP>>`.
   b. Enter the subnet mask for the iSCSI IP address: `<<var_controller_A_iSCSI_B_netmask>>`.
   c. Click Finish.
9. Click Yes to confirm the iSCSI settings.

   Note: This process takes a couple of minutes to complete.

10. In the left pane, click Hardware. In the right pane, click Show back of shelf.
11. Click Controller B and select Configure iSCSI ports. Do as follows:
    a. Select Port 0a and click Next.
    b. Click Show more port settings.
    c. Set the Ethernet port speed to 10Gbps.
    d. Clear the Enable IPv6 option.
    e. Leave the TCP listening port set to the default.
    f. Set the port MTU size to 9000 and click Next.
12. Select the Manually specify the static configuration option and do as follows:

a. Enter the iSCSI A VLAN IP address for controller B: <<var_controller_B_iSCSI_A_IP>>.
b. Enter the subnet mask for the iSCSI IP address: <<var_controller_B_iSCSI_A_netmask>>.
c. Click Finish.

13. Click Yes to confirm the iSCSI settings.

    Note: This process takes a couple of minutes to complete.

14. In the left pane, click Hardware. In the right pane, click Show back of shelf.
15. Click Controller B and select Configure iSCSI ports. Do as follows:
    a. Select Port 0b from the drop-down options. Click Next.
    b. Click Show more port settings.
    c. Set the Ethernet port speed to 10Gbps.
    d. Clear the Enable IPv6 option.
    e. Leave the TCP listening port set to the default.
    f. Set the port MTU size to 9000.
    g. Click Next.
16. Select the Manually specify the static configuration option and do as follows:
    a. Enter the iSCSI B VLAN IP address for controller B: <<var_controller_B_iSCSI_B_IP>>.
    b. Enter the subnet mask for the iSCSI IP address: <<var_controller_B_iSCSI_B_netmask>>.
    c. Click Finish.
17. Click Yes to confirm the iSCSI settings.

    Note: This process takes a couple of minutes to complete.

Configure NTP Server on the Controllers

To configure NTP settings on the controllers, complete the following steps:

1. In the left pane, click Hardware. In the right pane, click Show back of shelf.
2. Click Controller A and select Configure NTP server.
3. Select the checkbox to enable NTP on controller A.
4. Select the option to manually enter the NTP server address.
5. Enter the primary and backup NTP server addresses <<var_ntp_server_primary>> <<var_ntp_server_secondary>> and click Save.
6. Click Yes to apply the same NTP settings to controller B.

Configure DNS Server on the Controllers

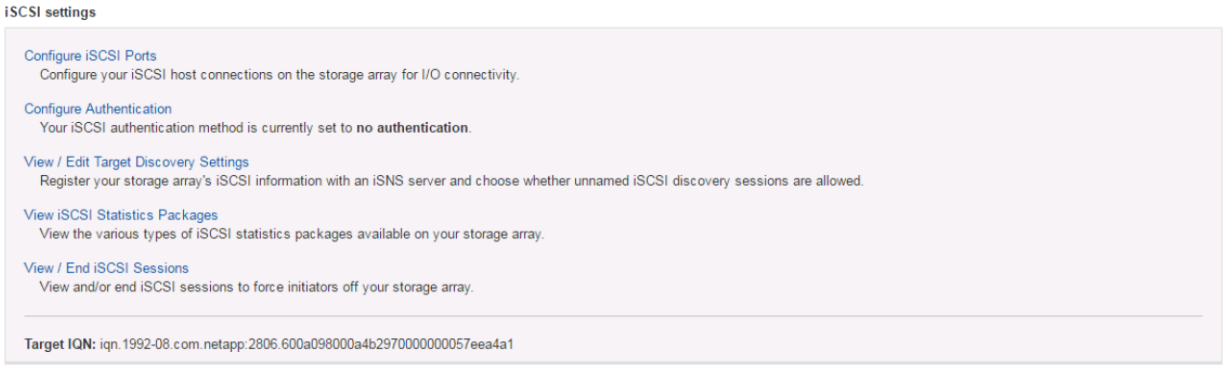
To configure DNS settings on the controllers, complete the following steps:

1. In the left pane, click Hardware. In the right pane, click Show back of shelf.
2. Click Controller A and select Configure DNS server.
3. Select the option to manually specify the DNS server address.
4. Enter the primary and backup DNS server addresses and click Save.
5. Click Yes to apply the same DNS settings to controller B.

Obtain the iSCSI Target Name

The iSCSI target name is used later in this configuration when creating Cisco UCS service profile templates. To obtain the iSCSI target name of the storage, complete the following steps:

1. In the left pane, click Settings.
2. The iSCSI target name is listed under the iSCSI settings section in the right pane.



3. Record the iSCSI target name `<<var_storage_iscsi_target_name>>` for later use.

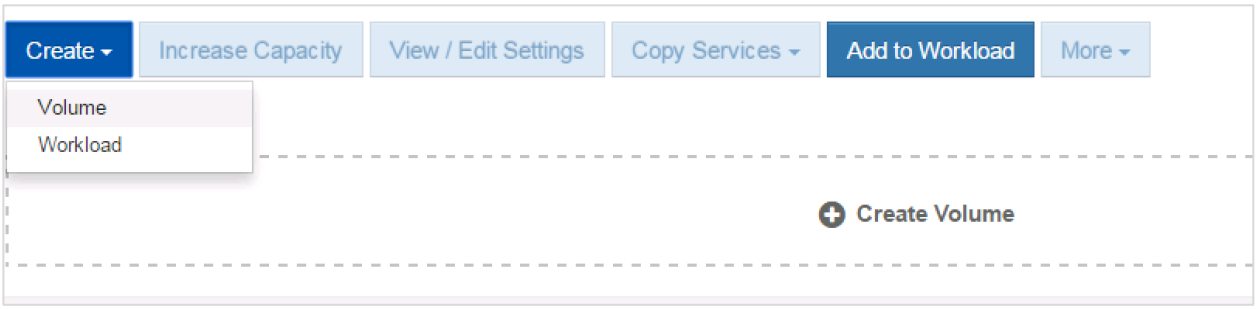
Create Volumes

Volumes are host-accessible units of storage that can be created from disk pools or volume groups. In this deployment, volumes are created from disk pools.

Four volumes are created, of which two serve as boot devices for each host. One volume serves as the infrastructure datastore and one as a VM swap file datastore.

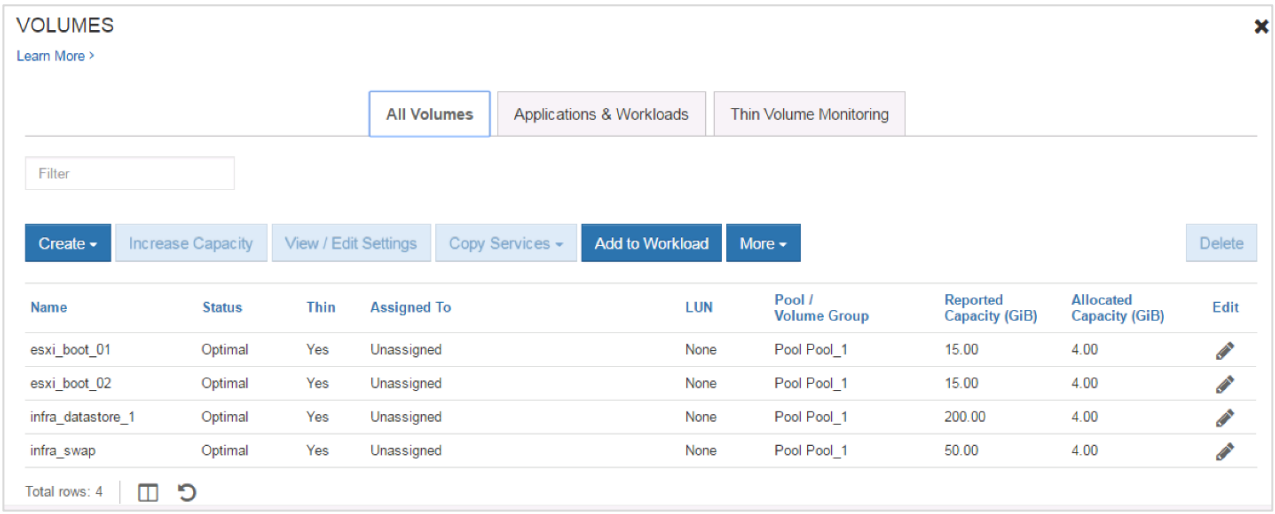
To create the volumes, complete the following steps:

1. In the left pane, click Storage.
2. Click Volumes in the right pane.
3. Click Create and select Volume.



4. Leave the host selection set to Assign Host Later and click Next.
5. From the drop-down options, select the workload created `<<var_storage_workload_name>>` and click Next.
6. Leave the number of VMFS datastores set to 0 and click Skip this step.
7. Click Add new volume.
8. Enter a name for the boot volume of the first ESXi host and its desired capacity.
9. Click the checkbox to enable thin provisioning.

10. Click Add new volume.
11. Enter a name for the boot volume of the second ESXi host and its desired capacity.
12. Click the checkbox to enable thin provisioning.
13. Click Add new volume.
14. Enter a name for the infrastructure volume that hosts all the VMs and its desired capacity.
15. Click the checkbox to enable thin provisioning.
16. Click Add new volume.
17. Enter a name for the infrastructure swap volume that hosts the virtual machine swap files and its desired capacity.
18. Click the checkbox to enable thin provisioning.
19. Click Next.
20. Click Finish.



6.3 Cisco UCS Configuration

FlexPod Express Cisco UCS Base

This section provides detailed procedures for configuring the Cisco UCS 6324 for use in a FlexPod Express environment. The steps are necessary to provision the Cisco UCS B-Series servers and should be followed precisely to avoid improper configuration.

Cisco UCS Fabric Interconnect 6324 A

Cisco UCS uses access layer networking and servers. This high-performance, next-generation server system provides a data center with a high degree of workload agility and scalability.

Cisco UCS Manager 3.1 supports the 6324 FI that integrates the FI with the Cisco UCS chassis and provides an integrated solution for a smaller deployment environment. Cisco UCS Mini simplifies the system management and saves cost for the low-scale deployments.

The first time you access a fabric interconnect in a Cisco UCS domain, a setup wizard prompts you for the following information required to configure the system:

- Installation method (GUI or CLI)
- Setup mode (restore from full system backup or initial setup)
- Admin password

- System configuration type (standalone or cluster configuration)
- System name
- Management port IPv4 address and subnet mask
- Default gateway IPv4 address
- Cisco UCS cluster IPv4 address
- DNS server IPv4 address
- Default domain name

To configure the Cisco UCS for use in a FlexPod Express environment, complete the following steps:

1. Connect to the console port on the first Cisco UCS 6324 FI.

```
Enter the configuration method. (console/gui) ? 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 password? (y/n) [y]: Enter

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

Is this Fabric interconnect part of a cluster(select 'no' for standalone)? (yes/no) [n]: yes

Enter the switch fabric (A/B) []: A

Enter the system name: <<var_ucs_clustername>>

Physical Switch Mgmt0 IP address : <<var_ucsa_mgmt_ip>>

Physical Switch Mgmt0 IPv4 netmask : <<var_ucsa_mgmt_mask>>

IPv4 address of the default gateway : <<var_ucsa_mgmt_gateway>>

Cluster IPv4 address : <<var_ucs_cluster_ip>>

Configure the DNS Server IP address? (yes/no) [n]: y
DNS IP address : <<var_nameserver_ip>>

Configure the default domain name? (yes/no) [n]: y
Default domain name: <<var_domain_name>>

Join centralized management environment (UCS Central)? (yes/no) [n]: no

NOTE: Cluster IP will be configured only after both Fabric Interconnects are initialized. UCSM
will be functional only after peer FI is configured in clustering mode.

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes

Applying configuration. Please wait.
  Configuration file - Ok
```

2. Review the settings displayed on the console. If they are correct, answer `yes` to apply and save the configuration.
3. Wait for the login prompt to verify that the configuration has been saved.

Cisco UCS Fabric Interconnect 6324 B

When you access the secondary FI in a Cisco UCS cluster domain for first time, a setup wizard prompts you for the following information required to configure the system:

- Installation method (GUI or CLI)
- Admin password

- Management port IPv4 address and subnet mask, or IPv6 address and prefix of the peer FI
- Cisco UCS cluster IPv4 address
- Management port IPv4 address of the local FI

To configure the Cisco UCS for use in a FlexPod Express environment, complete the following steps:

1. Connect to the console port on the second Cisco UCS 6324 FI.

```
Enter the configuration method. (console/gui) ? console

Installer has detected the presence of a peer Fabric interconnect. This Fabric interconnect will
be added to the cluster. Continue (y/n) ? y

Enter the admin password of the peer Fabric interconnect:<<var_password>>
Connecting to peer Fabric interconnect... done
Retrieving config from peer Fabric interconnect... done

Peer Fabric interconnect Mgmt0 IPv4 Address: <<var_ucsb_mgmt_ip>>

Peer Fabric interconnect Mgmt0 IPv4 Netmask: <<var_ucsb_mgmt_mask>>
Cluster IPv4 address: <<var_ucs_cluster_address>>

Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv4 Address
Physical Switch Mgmt0 IP address : <<var_ucsb_mgmt_ip>>

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes

Applying configuration. Please wait.
  Configuration file - Ok
```

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

FlexPod Express Cisco UCS on E-Series

Log in to Cisco UCS Manager

To log in to the Cisco UCS environment, complete the following steps:

1. Open a web browser and navigate to the Cisco UCS 6324 FI 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 3.1(1h)

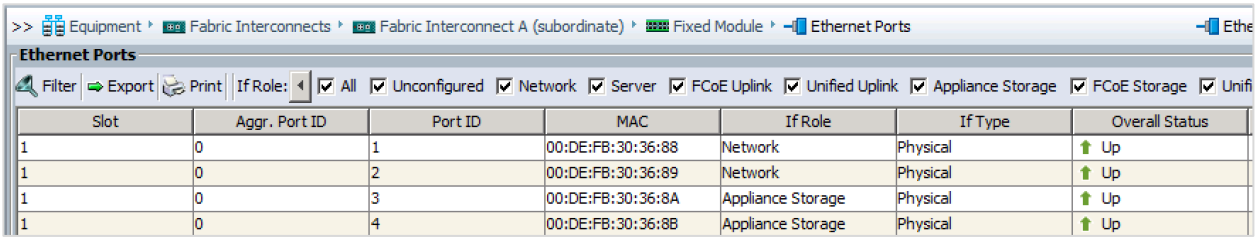
This document assumes the use of Cisco UCS Manager software version 3.1(1h). To upgrade the Cisco UCS Manager software and the Cisco UCS 6324 FI software to version 3.1(1h), refer to Cisco UCS Manager Install and Upgrade Guides.

Enable Server, Uplink, and Storage Ports

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

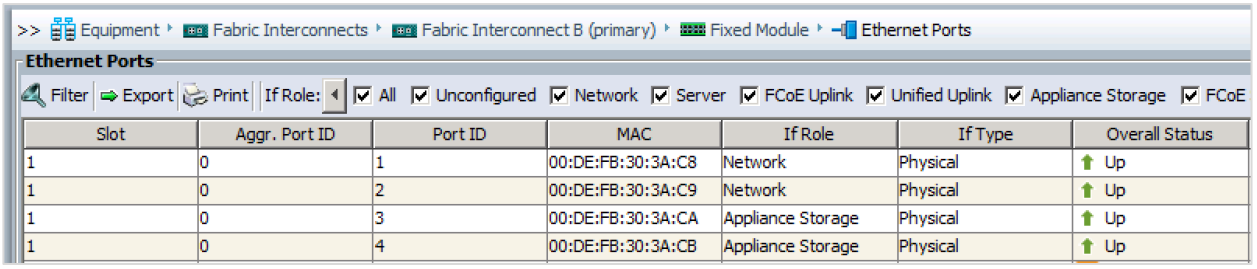
1. In Cisco UCS Manager, click the Equipment tab in the navigation pane.
2. Select Equipment > Fabric Interconnects > Fabric Interconnect A > Fixed Module.
3. Expand Ethernet Ports.
4. Select ports 1 and 2 that are connected to the Cisco Nexus 9000 switches (existing network infrastructure), right-click them, and select Configure as Uplink Port.
5. Click Yes to confirm uplink ports and click OK.

6. Select ports 3 and 4 that are connected to the NetApp E-Series controllers, right-click them, and select Configure as Appliance Port.
7. Click Yes to confirm appliance ports.
8. On the Configure as Appliance Port window, click OK.
9. Click OK to confirm.
10. Under the Ethernet Ports tab, confirm that ports have been configured correctly in the If Role column.



Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status
1	0	1	00:DE:FB:30:36:88	Network	Physical	Up
1	0	2	00:DE:FB:30:36:89	Network	Physical	Up
1	0	3	00:DE:FB:30:36:8A	Appliance Storage	Physical	Up
1	0	4	00:DE:FB:30:36:8B	Appliance Storage	Physical	Up

11. Select Equipment > Fabric Interconnects > Fabric Interconnect B > Fixed Module.
12. Expand Ethernet Ports.
13. Select ports 1 and 2 that are connected to the Cisco Nexus 9000 switches (existing network infrastructure), right-click them, and select Configure as Uplink Port.
14. Click Yes to confirm uplink ports and click OK.
15. Select ports 3 and 4 that are connected to the NetApp E-Series controllers, right-click them, and select Configure as Appliance Port.
16. Click Yes to confirm appliance ports.
17. On the Configure as Appliance Port window, click OK.
18. Click OK to confirm.



Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status
1	0	1	00:DE:FB:30:3A:C8	Network	Physical	Up
1	0	2	00:DE:FB:30:3A:C9	Network	Physical	Up
1	0	3	00:DE:FB:30:3A:CA	Appliance Storage	Physical	Up
1	0	4	00:DE:FB:30:3A:CB	Appliance Storage	Physical	Up

Create Uplink Port Channels to Switching Infrastructure

In this deployment, the uplink port channels are connected to the Cisco Nexus 9000 switches.

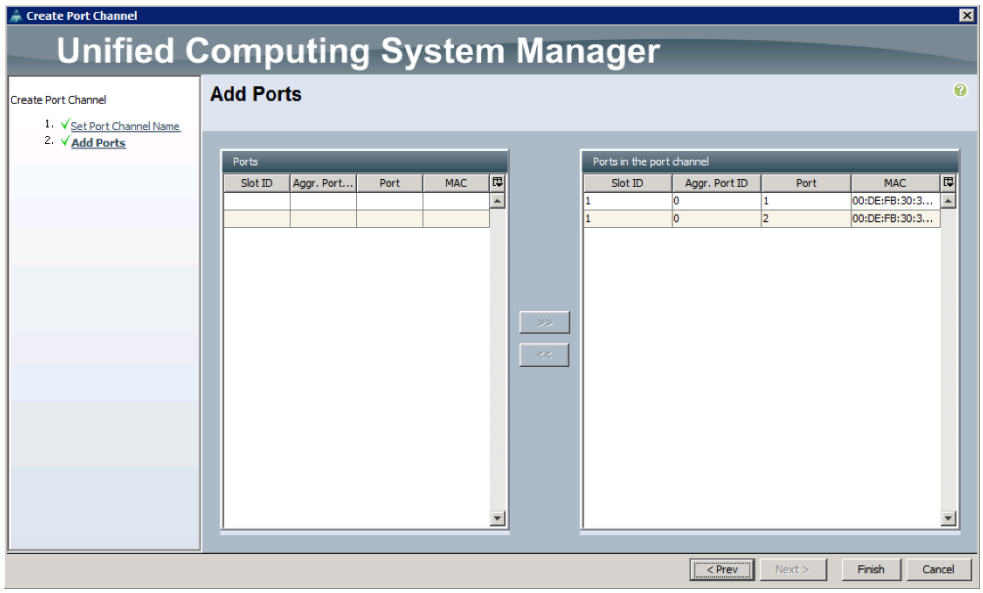
To configure the necessary port channels in the Cisco UCS environment, complete the following steps:

1. In the 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 9000 switches and one from fabric B to both Cisco Nexus 9000 switches. If using standard switches, modify this procedure accordingly. If using 1GbE switches and GLC-T SFPs on the fabric interconnects, the interface speeds of Ethernet ports 1/1 and 1/2 in the fabric interconnects need to be set to 1Gbps.

2. Under LAN > LAN Cloud, expand the fabric A tree.
3. Right-click Port Channels and select Create Port Channel.
4. Enter 13 as the unique ID of the port channel.

5. Enter `vPC-13-N9000` as the name of the port channel and click Next.
6. Select the following ports to be added to the port channel:
   - Slot ID 1 and port 1
   - Slot ID 1 and port 2
7. Click >> to add the ports to the port channel.



8. Click Finish to create the port channel.
9. Click OK.
10. Under Port Channels, select the newly created port channel.
11. The port channel should have an overall status of Up.
12. In the navigation pane, under LAN > LAN Cloud, expand the fabric B tree.
13. Right-click Port Channels and select Create Port Channel.
14. Enter 14 as the unique ID of the port channel.
15. Enter `vPC-14-N9000` as the name of the port channel and click Next.
16. Select the following ports to be added to the port channel:
    - Slot ID 1 and port 1
    - Slot ID 1 and port 2
17. Click >> to add the ports to the port channel.
18. Click Finish to create the port channel.
19. Click OK.
20. Under Port Channels, select the newly created port channel.
21. The port channel should have an overall status of Up.

Create an Organization (Optional)

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

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

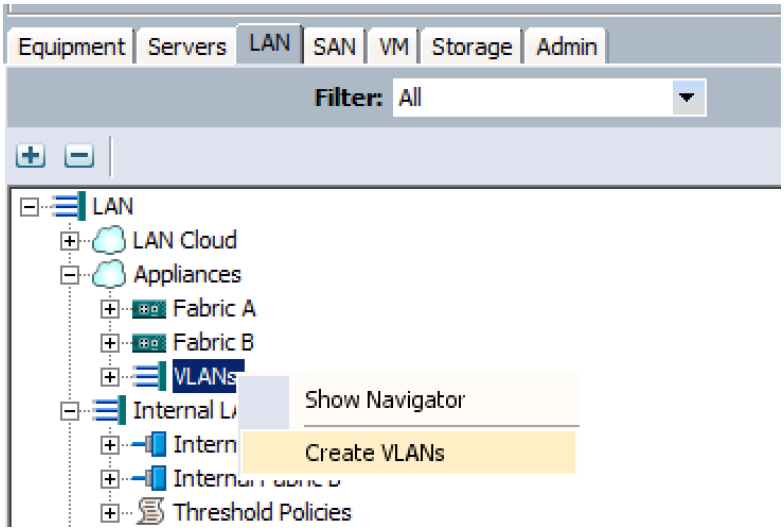
To configure an organization in the Cisco UCS environment, complete the following steps:

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

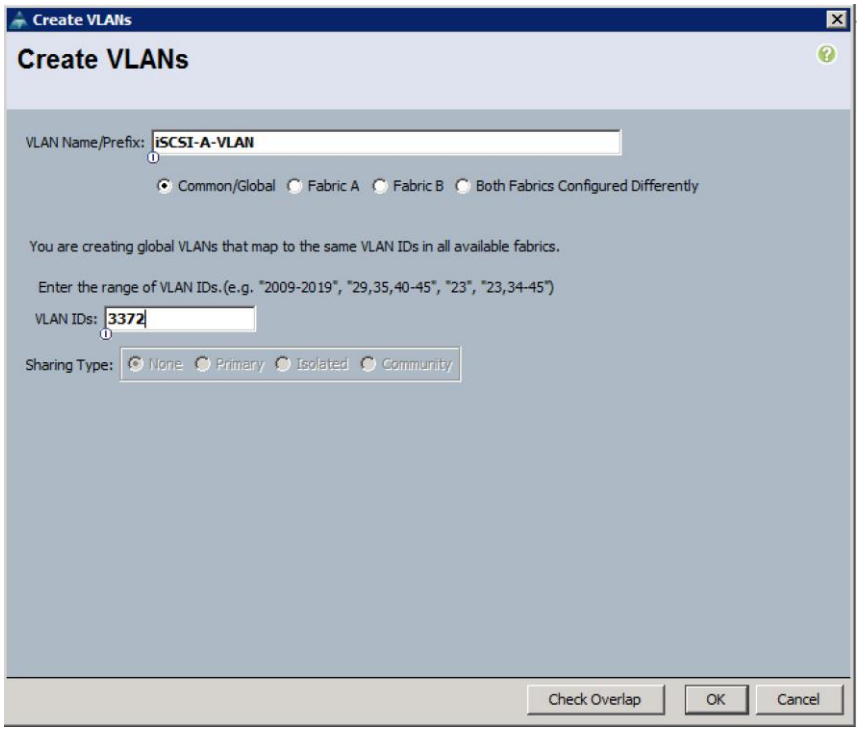
Configure Storage Appliance Ports and Storage VLANs

To configure the storage appliance ports and storage VLANs, complete the following steps:

1. In the Cisco UCS Manager, select the LAN tab.
2. Expand Appliances.
3. Right-click VLANs and select Create VLANs.



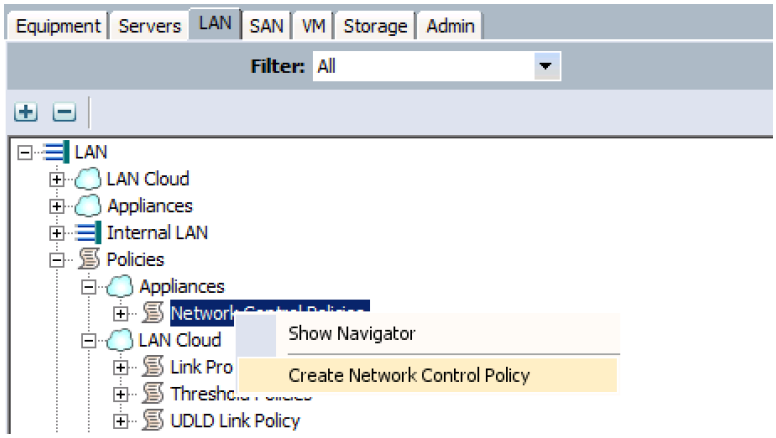
4. Enter `iSCSI-A-VLAN` as the name for the infrastructure iSCSI fabric A VLAN.
5. Leave Common/Global selected.
6. Enter `<<var_iscsi_a_vlan>>` for the VLAN ID.



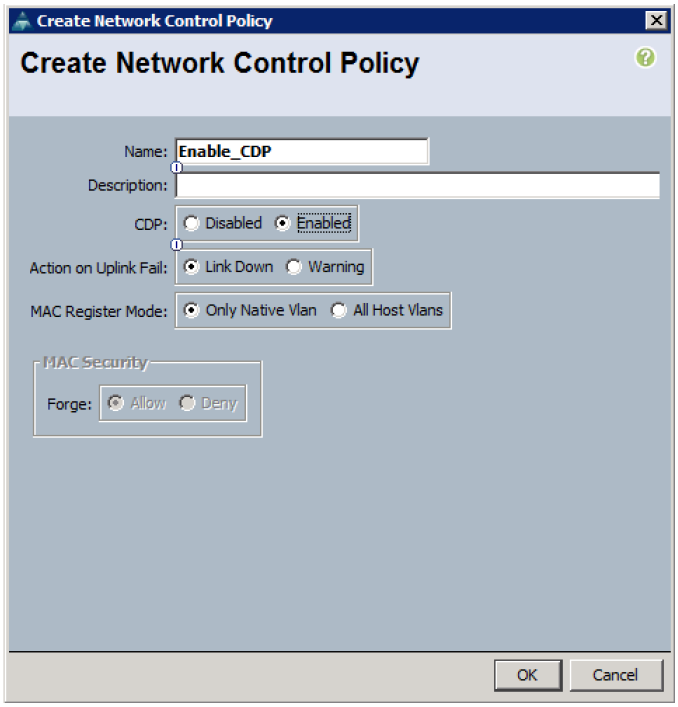
7. Click OK and then click OK again to create the VLAN.
8. Right-click VLANs and select Create VLANs.
9. Enter `iSCSI-B-VLAN` as the name for the infrastructure iSCSI fabric B VLAN.
10. Leave Common/Global selected.
11. Enter `<<var_iscsi_b_vlan_id>>` for the VLAN ID.
12. Click OK and then click OK again to create the VLAN.

Create Network Control Policy for the Appliance

1. In the navigation pane, under LAN > Policies, expand Appliances and right-click Network Control Policies.
2. Select Create Network Control Policy.



3. Name the policy `Enable_CDP` and select Enabled next to CDP.

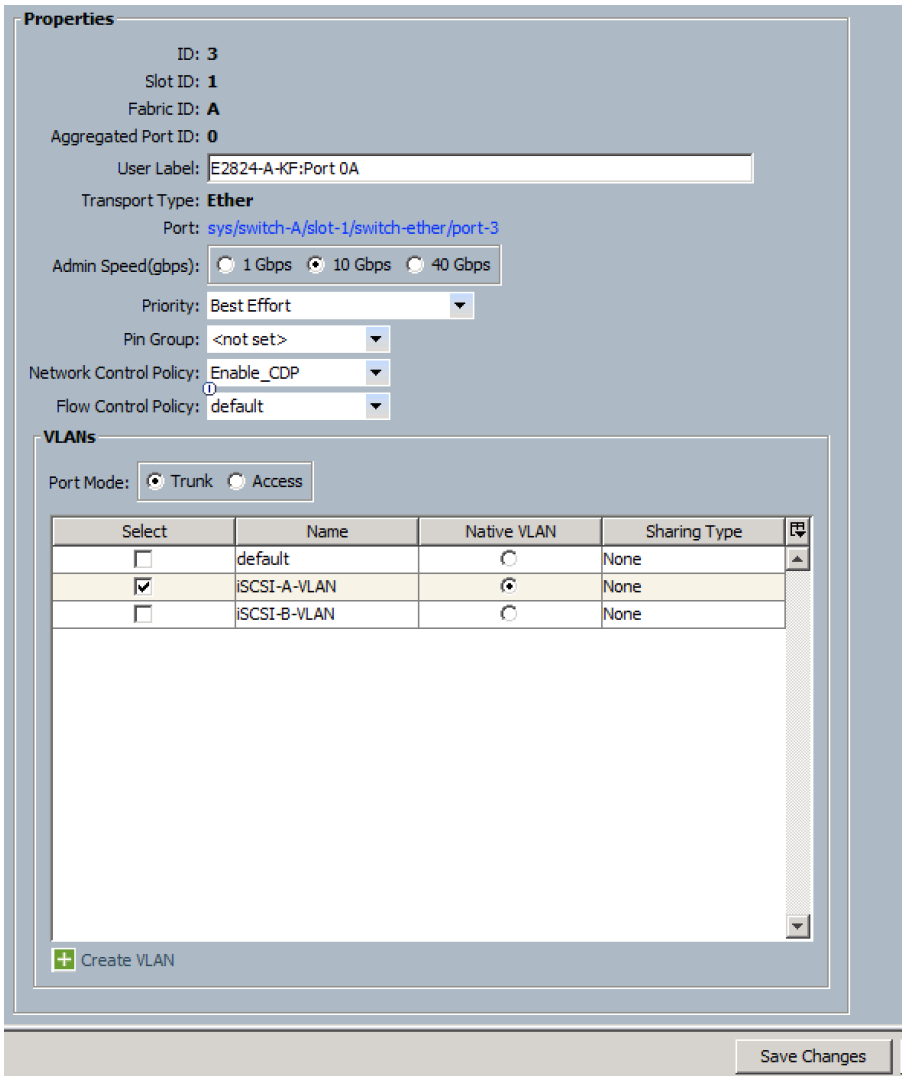


4. Click OK and then click OK again to create the policy.

Configure the Appliance Interfaces

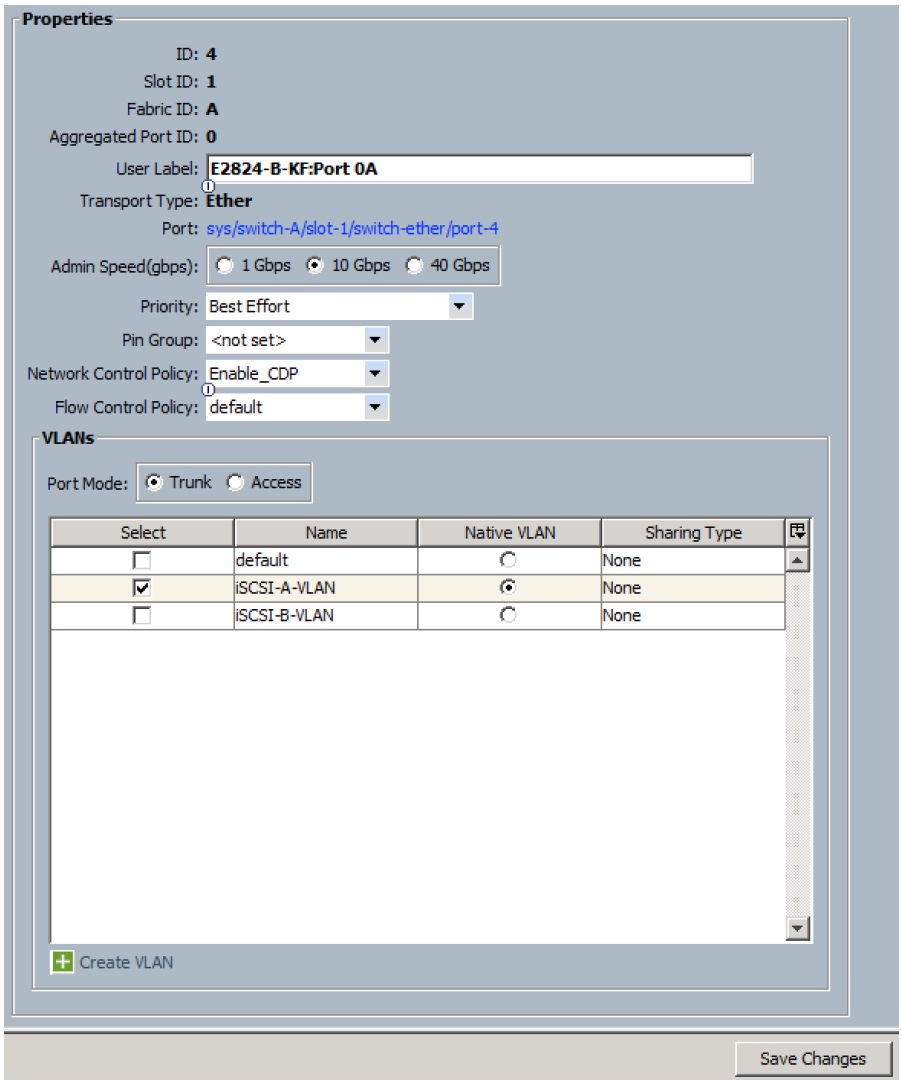
1. In the navigation pane, under LAN > Appliances Cloud, expand the fabric A tree.
2. Expand Interfaces.
3. Select Appliance Interface 1/3.
4. In the User Label field, put in information indicating the storage controller port, such as `<<var_controller_A>>:Port0A`.
5. Click Save Changes and OK.
6. Select the Enable_CDP network control policy and select Save Changes and OK.
7. Under VLANs, select the iSCSI-A-VLAN. Deselect the default VLAN.

   Note: The iSCSI-A-VLAN is automatically set as the native VLAN.



8. Click Save Changes and then click OK.
9. Select Appliance Interface 1/4 under Fabric A.
10. In the User Label field, put in information indicating the storage controller port, such as `<<var_controller_B>>:Port0A`.
11. Click Save Changes and then click OK.
12. Select the Enable_CDP network control policy. Click Save Changes and then click OK.
13. Under VLANs, select the iSCSI-A-VLAN. Deselect the default VLAN.

    Note: The iSCSI-A-VLAN is automatically set as the native VLAN.



14. Click Save Changes and OK.
15. In the navigation pane, under LAN > Appliances Cloud, expand the fabric B tree.
16. Expand Interfaces.
17. Select Appliance Interface 1/3.
18. In the User Label field, enter information indicating the storage controller port, such as `<<var_controller_A>>:Port0B`.
19. Click Save Changes and then click OK.
20. Select the Enable_CDP network control policy and select Save Changes and OK.
21. Under VLANs, select the iSCSI-B-VLAN. Deselect the default VLAN.

    Note: The iSCSI-B-VLAN is automatically set as the native VLAN.
22. Click Save Changes and then click OK.
23. Select Appliance Interface 1/4 under fabric B.
24. In the User Label field, put in information indicating the storage controller port, such as `<<var_controller_B>>:Port0B`.
25. Click Save Changes and then click OK.

26. Select the Enable_CDP network control policy and select Save Changes and then click OK.
27. Under VLANs, select the iSCSI-B-VLAN. Deselect the default VLAN.

    Note: The iSCSI-B-VLAN is automatically set as the native VLAN.

28. Click Save Changes and then 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, in the navigation pane, click the LAN tab.
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.
6. Click Yes.
7. Click OK.

Synchronize Cisco UCS NTP

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

1. In the Cisco UCS Manager, select the Admin tab. In the left pane, expand All and navigate to Time Zone Management > Timezone.
2. Select the appropriate time zone and click Save Changes.
3. Click OK.
4. Select Add NTP server.
5. Enter `<<var_ntp_server_primary>>` and click OK.
6. Click OK to confirm.
7. Select Add NTP server.
8. Enter `<<var_ntp_server_secondary>>` and click OK.
9. Click OK to confirm.

Add Block of IP Addresses for KVM Access

To create a block of IP addresses for server keyboard, video, mouse (KVM) access in the Cisco UCS environment, complete the following steps:

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

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

Acknowledge Cisco UCS Chassis

To acknowledge the Cisco UCS chassis, complete the following steps:

1. In the Cisco UCS Manager, select the Equipment tab in the left pane.
2. Expand Equipment > Chassis and select Chassis 1 (primary).
3. Right-click Chassis 1 and click Acknowledge Chassis.
4. Click Yes.
5. Click OK.

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:

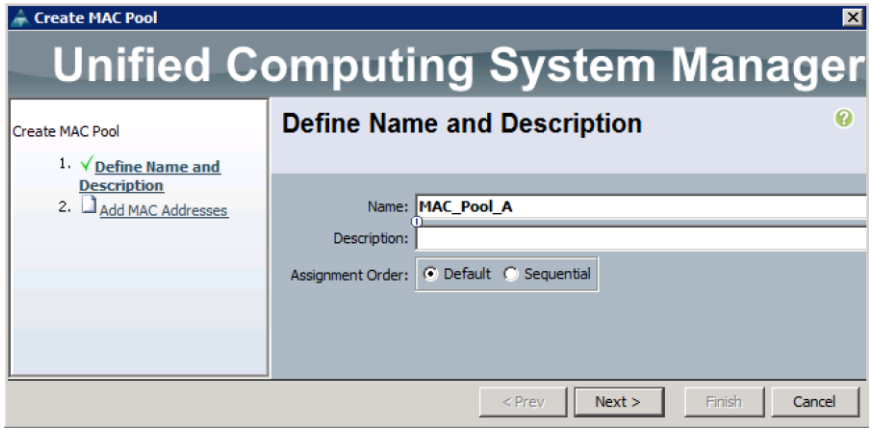
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Host Firmware Packages.
4. Select Create Host Firmware Package.
5. Enter `VM-Host-Infra` as the name of the host firmware package.
6. Leave Simple selected.
7. Select version 3.1(1h)B for the blade package.
8. Click OK to create the host firmware package.
9. Click OK.

Create MAC Address Pools

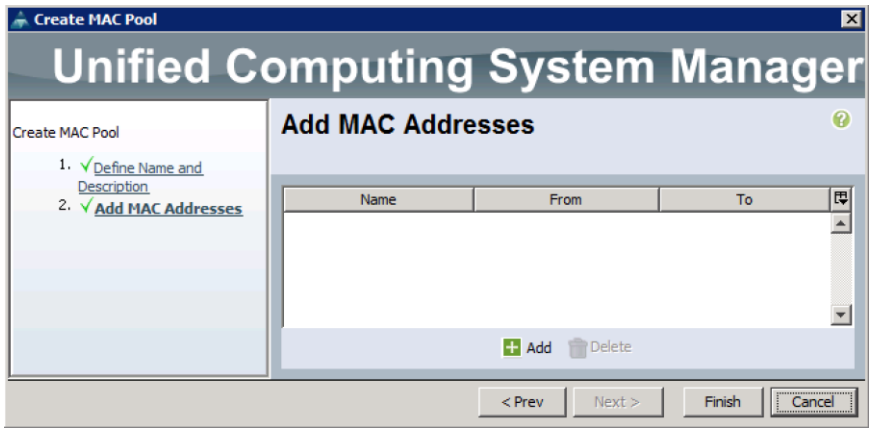
To configure the necessary MAC address pools for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Pools > root.
3. In this procedure, two MAC address pools are created, one for each switching fabric.
4. Right-click MAC Pools under the root organization.
5. Select Create MAC Pool to create the MAC address pool.
6. Enter `MAC_Pool_A` as the name of the MAC pool.
7. Optional: Enter a description for the MAC pool.

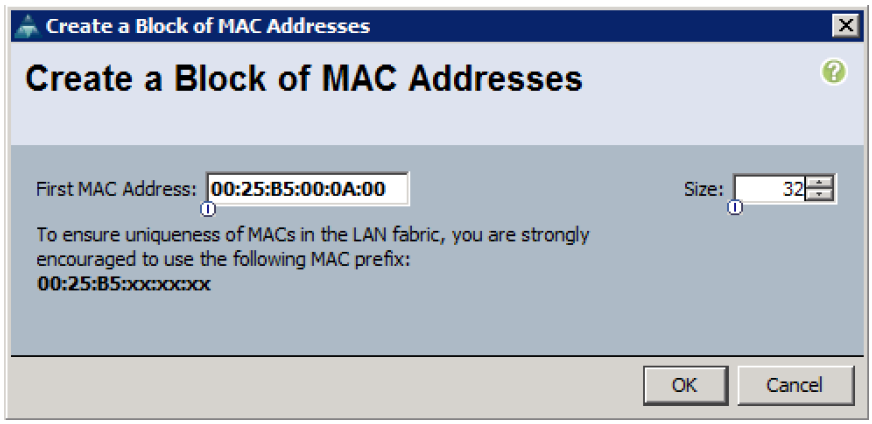
   Note: Retain the assignment order as Default.



8. Click Next.



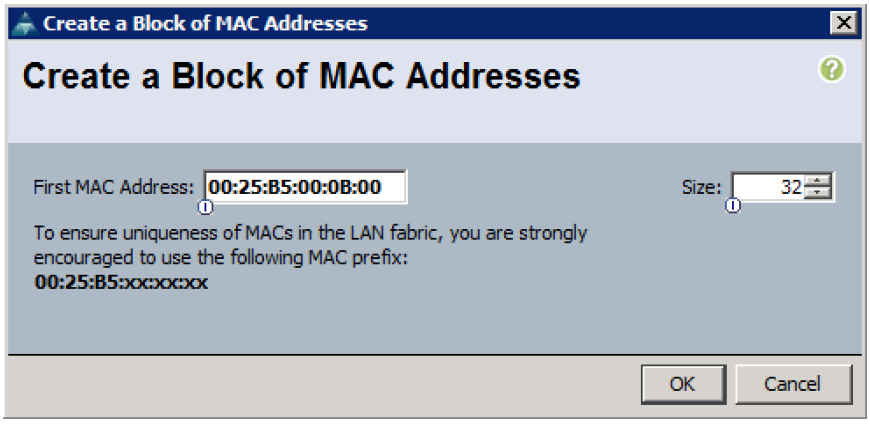
9. Click Add.
10. Specify a starting MAC address.
11. For the FlexPod solution, the recommendation is to place `0A` in the next to last octet of the starting MAC address to identify all the MAC addresses as fabric A addresses.
12. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources.



13. Click OK.

14. Click Finish.
15. In the confirmation message, click OK.
16. Right-click MAC Pools under the root organization.
17. Select Create MAC Pool to create the MAC address pool.
18. Enter `MAC_Pool_B` as the name of the MAC pool.
19. Optional: Enter a description for the MAC pool.

    Note: Keep the assignment order at Default.
20. Click Next.
21. Click Add.
22. Specify a starting MAC address.
23. For the FlexPod solution, the recommendation is to place `0B` in the next to last octet of the starting MAC address to identify all the MAC addresses in this pool as fabric B addresses.
24. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources.

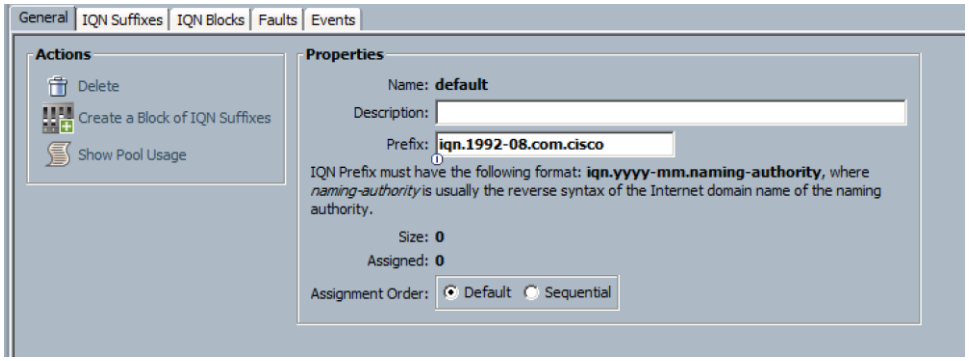


25. Click OK.
26. Click Finish.
27. In the confirmation message, click OK.

Create iSCSI IQN Pool

To enable iSCSI traffic on a service profile, a service profile must have an IQN. IQN pools reduce the effort required to deploy additional service profiles with unique IQNs. To create an IQN pool, use the following procedure:

1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Click Pools > Root > IQN Pools > Pool default.
3. Enter iqn.1992-08.com.cisco as the IQN prefix in the action pane.



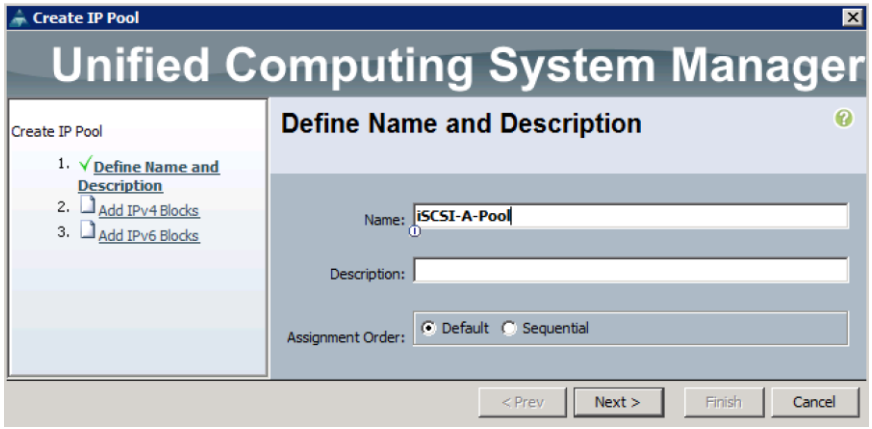
4. Click Save Changes.
5. Click OK to dismiss the notification window.
6. Click the IQN blocks tab.
7. Click the green Add button on the right side of the action pane.
8. Enter `ucs-host` in the suffix field, 0 in the From field, and an appropriate size in the Size field (at least 2).
9. Click OK.
10. Click OK to dismiss the notification message.

Create iSCSI Initiator IP Address Pools

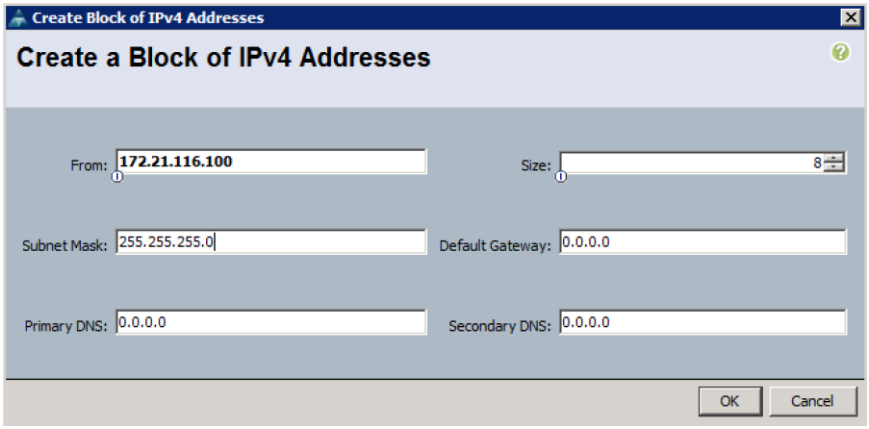
iSCSI initiator IP addresses are assigned from IP address pools. Each iSCSI fabric has its own pool. To create blocks of IP addresses for iSCSI initiators, complete the following steps:

Note: This block of IP addresses should be in the same subnet as the iSCSI target IP addresses assigned to the E-Series storage array 10Gb iSCSI ports.

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Pools > root > IP Pools.
3. Right-click IP Pools and select Create IP Pool.
4. Name the pool `iSCSI-A-POOL` and set the assignment order as Default.



5. Click Next to continue.
6. Click Add.
7. Enter the starting IP address of the block, the number of IP addresses required, and the subnet mask in the appropriate fields.

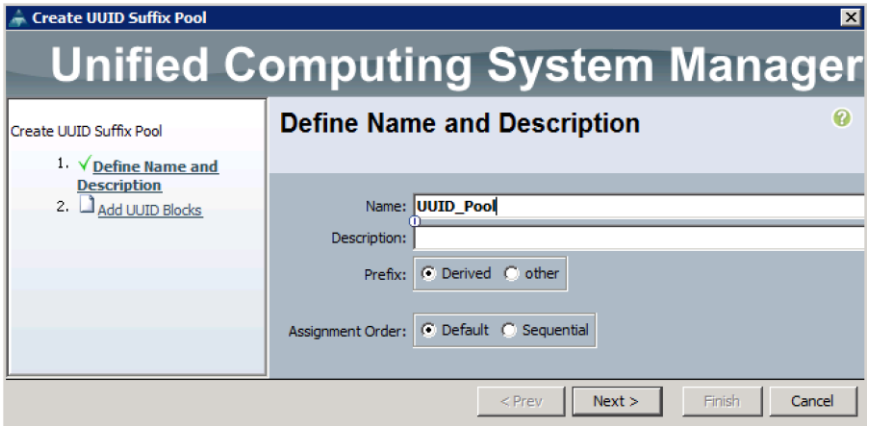


8. Click OK to create the IP block.
9. Click Next to continue.
10. Click Finish to create the IP pool.
11. Click OK to dismiss the notification message.
12. Right-click IP Pools and select Create IP Pool.
13. Name the pool iSCSI-B-POOL and set the assignment order as Default.
14. Click Next to continue.
15. Click Add.
16. Enter the starting IP address of the block, the number of IP addresses required, and the subnet mask in the appropriate fields.
17. Click OK to create the IP block.
18. Click Next to continue.
19. Click Finish to create the IP pool.
20. Click OK to dismiss the notification message.

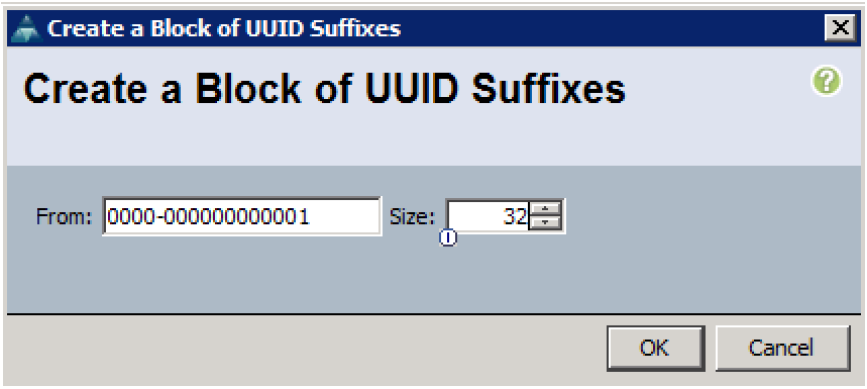
Create UUID Suffix Pool

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 and select Create UUID Suffix Pool.
4. Enter `UUID_Pool` as the name of the UUID suffix pool.
5. Optional: Enter a description for the UUID suffix pool.
6. Keep the prefix at the derived option.
7. Keep the assignment order at Default.



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. 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_Pool` as the name of the server pool.
6. Optional: Enter a description for the server pool.
7. Click Next.
8. Select the two servers that are used for the VMware management cluster and click >> to add them to the `Infra_Pool` server pool.
9. Click Finish.

10. Click OK.

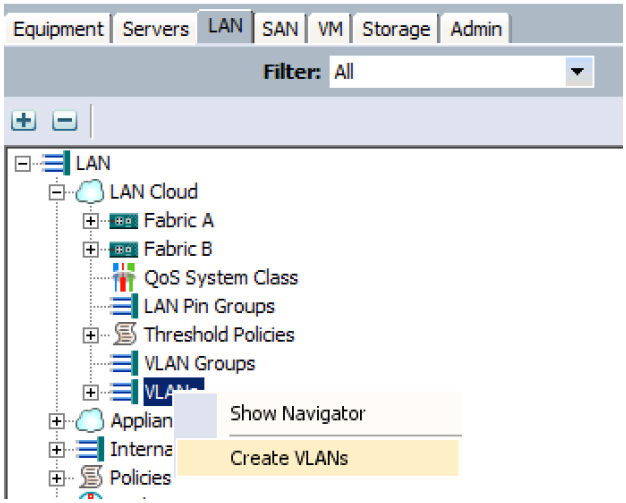
Create VLANs

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

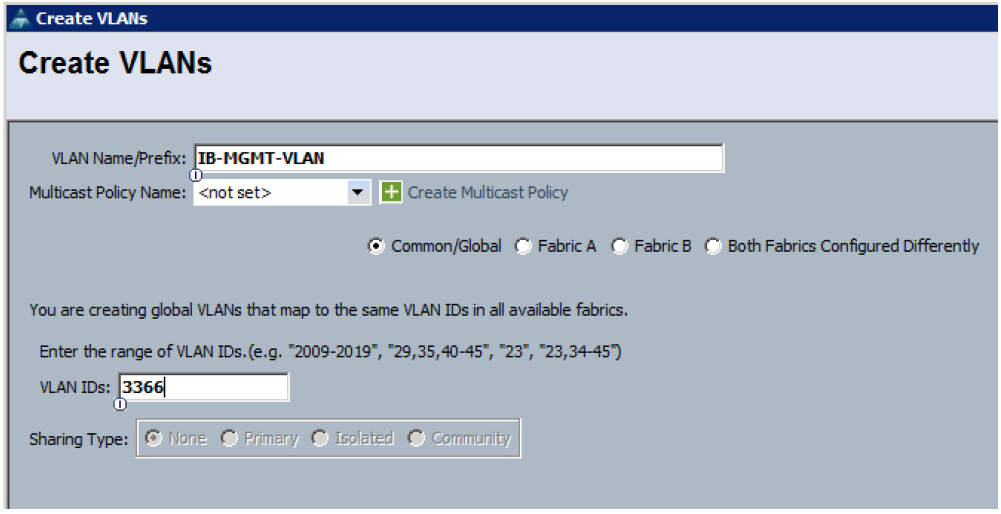
1. In Cisco UCS Manager, click the LAN tab in the navigation pane.

   Note: In this procedure, five VLANs are created.

2. Select LAN > LAN Cloud.
3. Right-click VLANs and select Create VLANs.

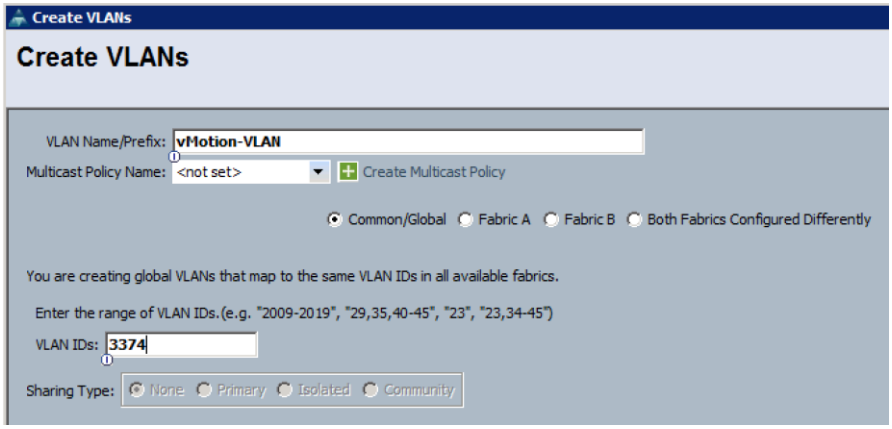


4. Enter `IB-MGMT-VLAN` as the name of the VLAN to be used for management traffic.
5. Keep the Common/Global option selected for the scope of the VLAN.
6. Enter `<<var_ib-mgmt_vlan_id>>` as the ID of the management VLAN.
7. Keep the sharing type as None.

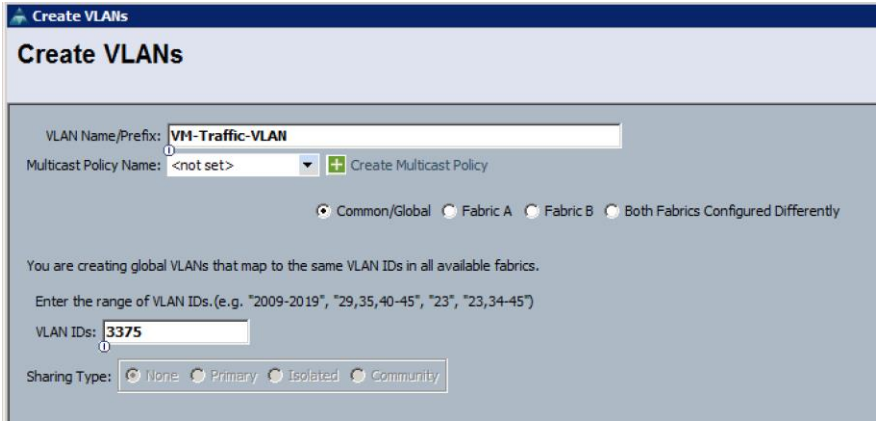


8. Click OK and then click OK again.
9. Right-click VLANs and select Create VLANs.

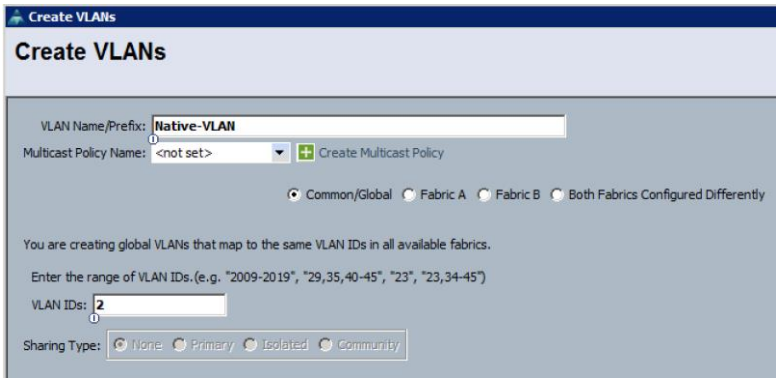
10. Enter `vMotion-VLAN` as the name of the VLAN to be used for vMotion.
11. Keep the Common/Global option selected for the scope of the VLAN.
12. Enter the `<<var_vmotion_vlan_id>>` as the ID of the vMotion VLAN.
13. Keep the sharing type as None.



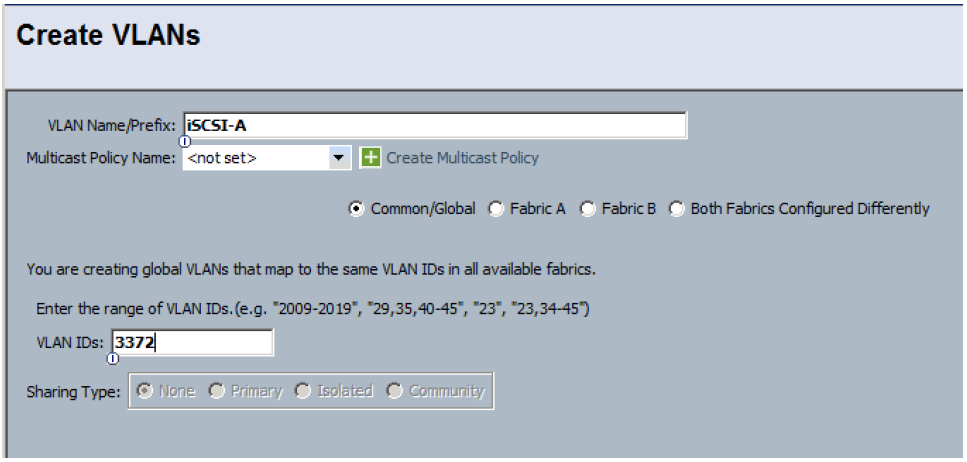
14. Click OK and then click OK again.
15. Right-click VLANs.
16. Select Create VLANs.
17. Enter `VM-Traffic-VLAN` as the name of the VLAN to be used for the VM traffic.
18. Keep the Common/Global option selected for the scope of the VLAN.
19. Enter the `<<var_vm-traffic_vlan>>` for the VM traffic VLAN.
20. Keep the sharing type as None.



21. Click OK and then click OK again.
22. Right-click VLANs and select Create VLANs.
23. Enter `Native-VLAN` as the name of the VLAN to be used as the native VLAN.
24. Keep the Common/Global option selected for the scope of the VLAN.
25. Enter the `<<var_native_vlan_id>>` as the ID of the native VLAN.
26. Keep the sharing type as None.



27. Click OK and then click OK again.
28. Expand the list of VLANs in the navigation pane, right-click the newly created VLAN, and select Set as Native VLAN.
29. Click Yes and then click OK.
30. Right-click VLANs and select Create VLANs.
31. Enter `iSCSI-A` as the name of the VLAN to be used as the iSCSI fabric A VLAN.
32. Keep the Common/Global option selected for the scope of the VLAN.
33. Enter the `<<var_iscsi_a_vlan_id>>` as the ID of the VLAN.
34. Keep the sharing type as None.



35. Click OK and then click OK again.
36. Click Yes and then click OK.
37. Right-click VLANs and select Create VLANs.
38. Enter `iSCSI-B` as the name of the VLAN to be used as the iSCSI fabric B VLAN.
39. Keep the Common/Global option selected for the scope of the VLAN.
40. Enter the `<<var_iscsi_b_vlan_id>>` as the ID of the VLAN.
41. Keep the sharing type as None.

42. Click OK and then click OK again.
43. Click Yes and then click OK.

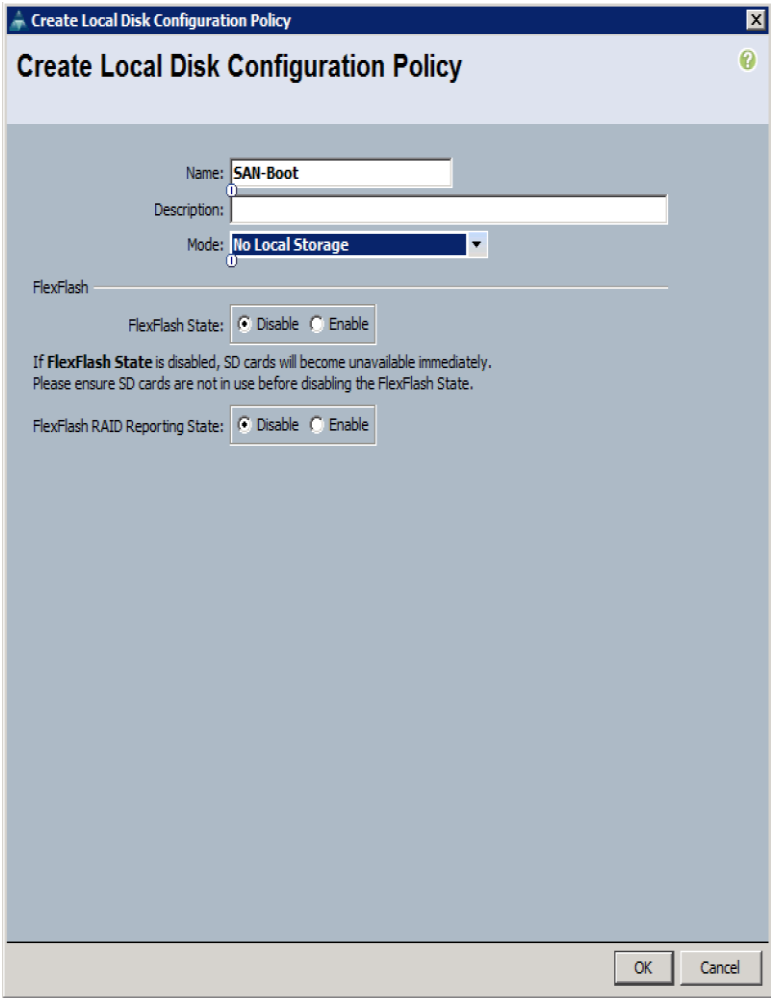
Create Local Disk Configuration Policy (Optional)

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

Note: 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 and select Create Local Disk Configuration Policy.
4. Enter SAN-Boot as the local disk configuration policy name.
5. Change the mode to No Local Storage.
6. Keep the FlexFlash state and FlexFlash RAID reporting state at Disable.

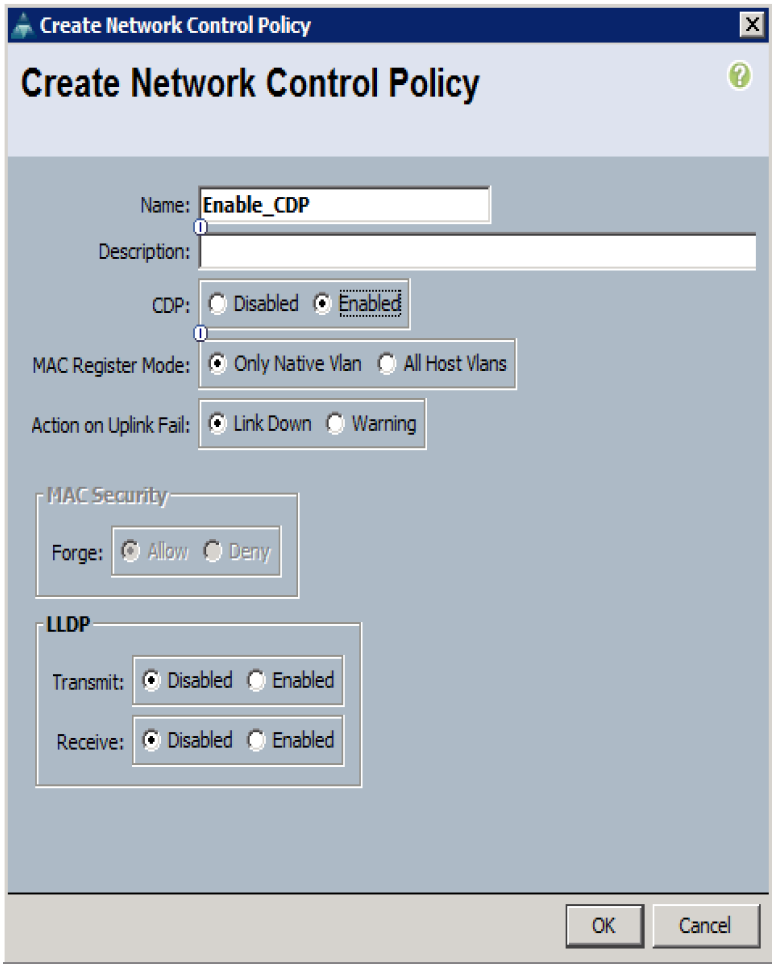


7. Click OK to create the local disk configuration policy.
8. Click OK.

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:

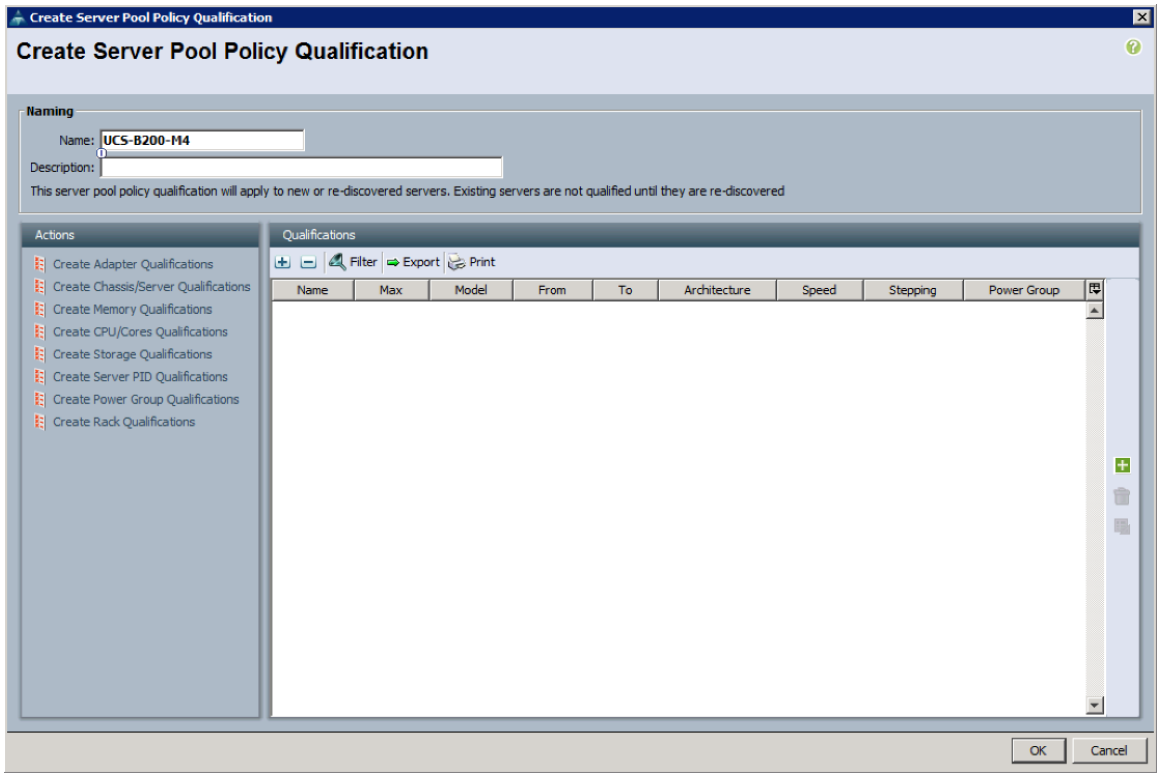
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Power Control Policies and select Create Power Control Policy.
4. Enter `No-Power-Cap` as the power control policy name.
5. Change the power capping setting to No Cap.
6. Click OK to create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

Create Server Pool Qualification Policy (Optional)

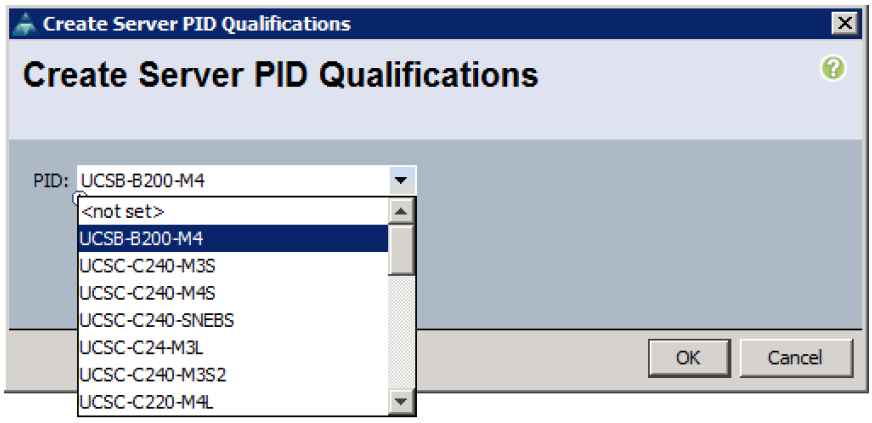
To create an optional server pool qualification policy for the Cisco UCS environment, complete the following steps:

Note: This example creates a policy for a 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-M4` as the name for the policy.



6. In the left pane, under Actions, select Create Server PID Qualifications.
7. From the PID drop-down options, select UCSB-B200-M4.

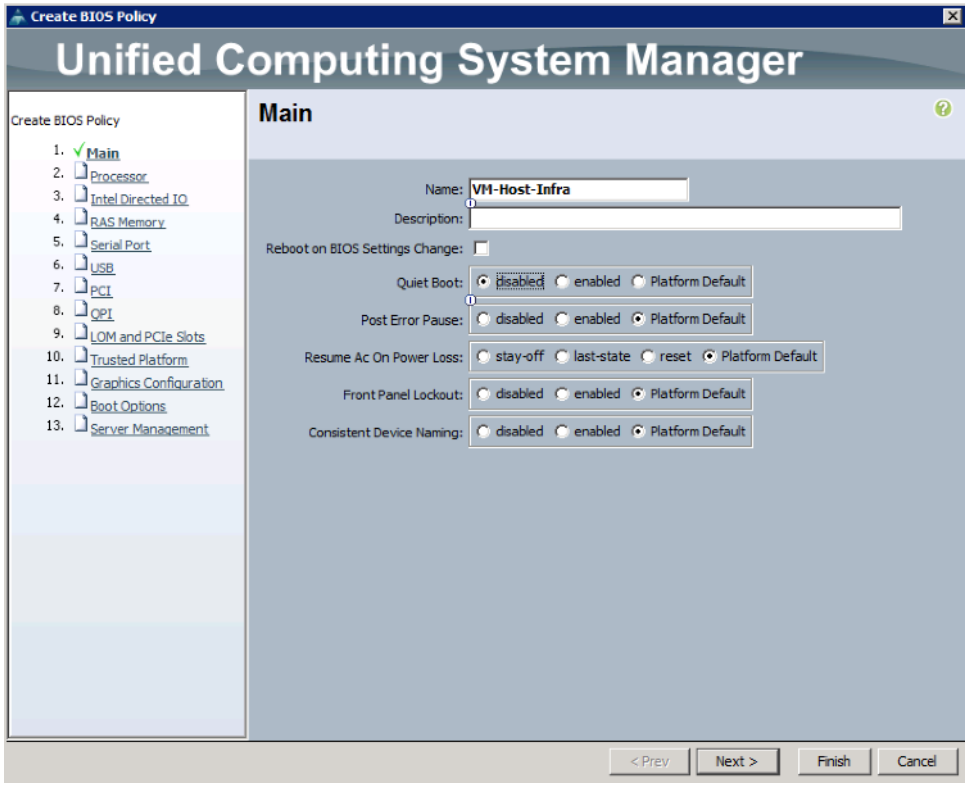


8. Click OK to create the server pool qualification policy.
9. Click OK and then click OK again.

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 and select Create BIOS Policy.
4. Enter `VM-Host-Infra` as the BIOS policy name.
5. Change the quiet boot setting to Disabled.
6. Click Finish to create the BIOS policy.



7. Click OK.

Create vNIC/vHBA Placement Policy for Virtual Machine Hosts

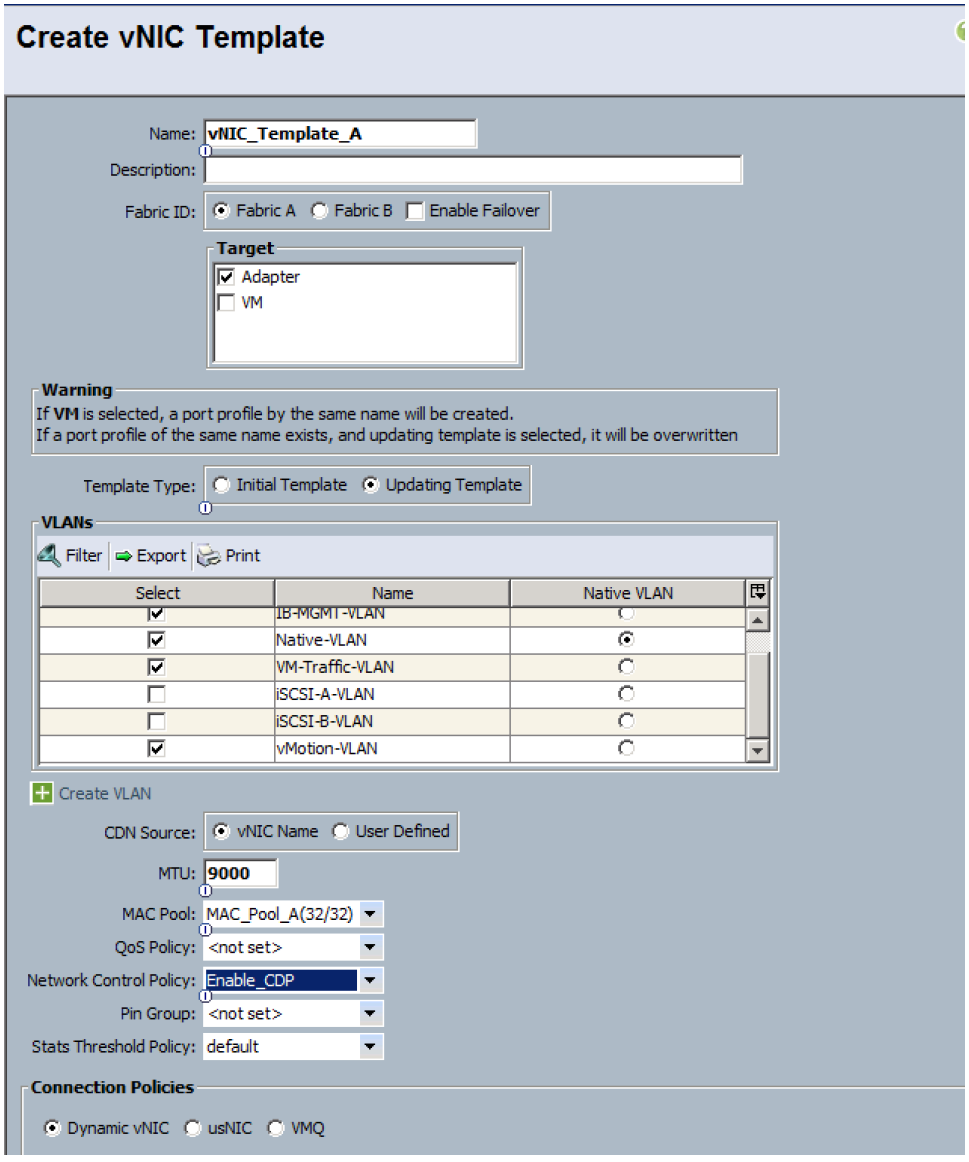
To create a vNIC/vHBA placement policy for the infrastructure hosts, complete the following steps:

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

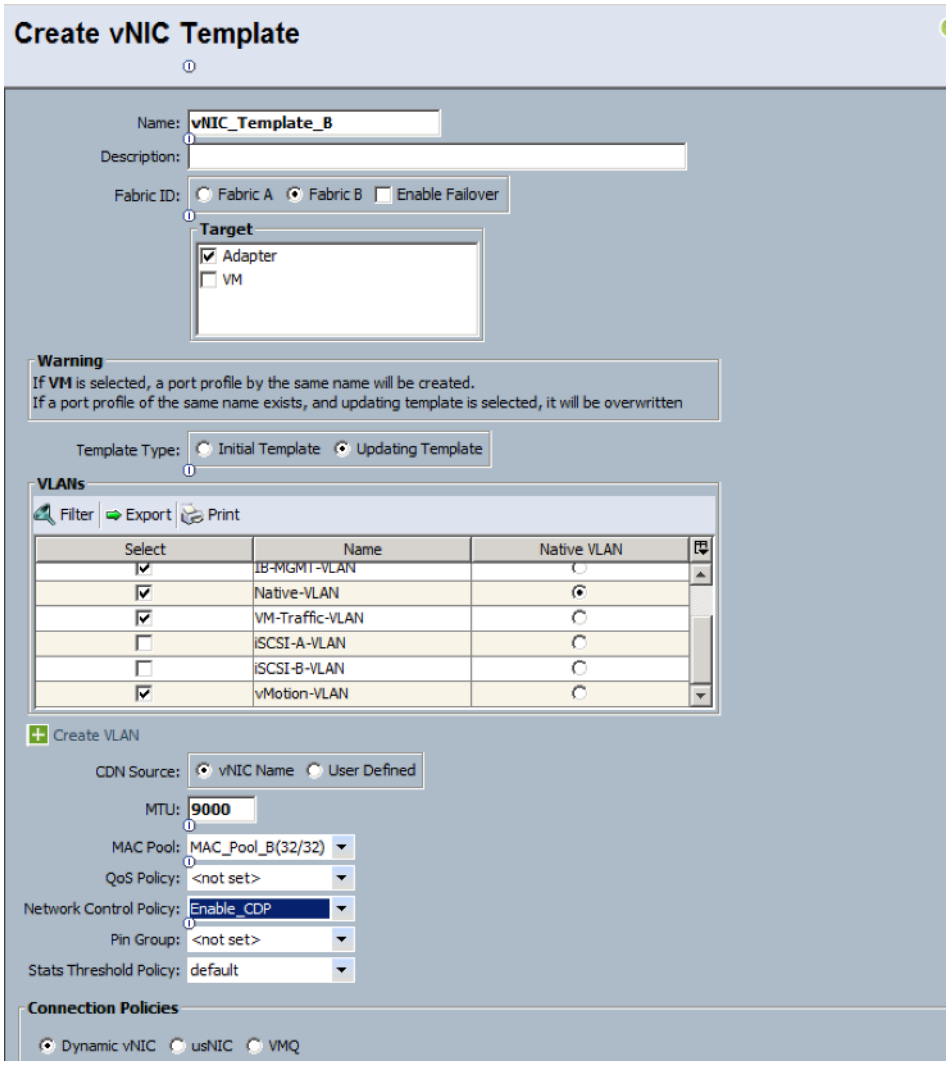
Create vNIC Templates

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

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click vNIC Templates and select Create vNIC Template.
4. Enter `vNIC_Template_A` as the vNIC template name.
5. Keep Fabric A selected.
6. Do not select the Enable Failover checkbox.
7. Under Target, make sure that the VM checkbox is not selected.
8. Select Updating Template as the template type.
9. Under VLANs, select the checkboxes for IB-MGMT-VLAN, Native-VLAN, VM-Traffic-VLAN, and vMotion-VLAN.
10. Set Native-VLAN as the native VLAN.
11. For MTU, enter 9000.
12. From the MAC Pool list, select MAC_Pool_A.
13. From the Network Control Policy list, select Enable_CDP.



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



29. Click OK to create the vNIC template.
30. Click OK.

Create iSCSI vNIC Templates

It is highly recommended that separate iSCSI vNICs be used to support boot from iSCSI in a VMware/Cisco UCS environment. To create multiple iSCSI virtual network interface card (vNIC) templates for the Cisco UCS environment, complete the following steps:

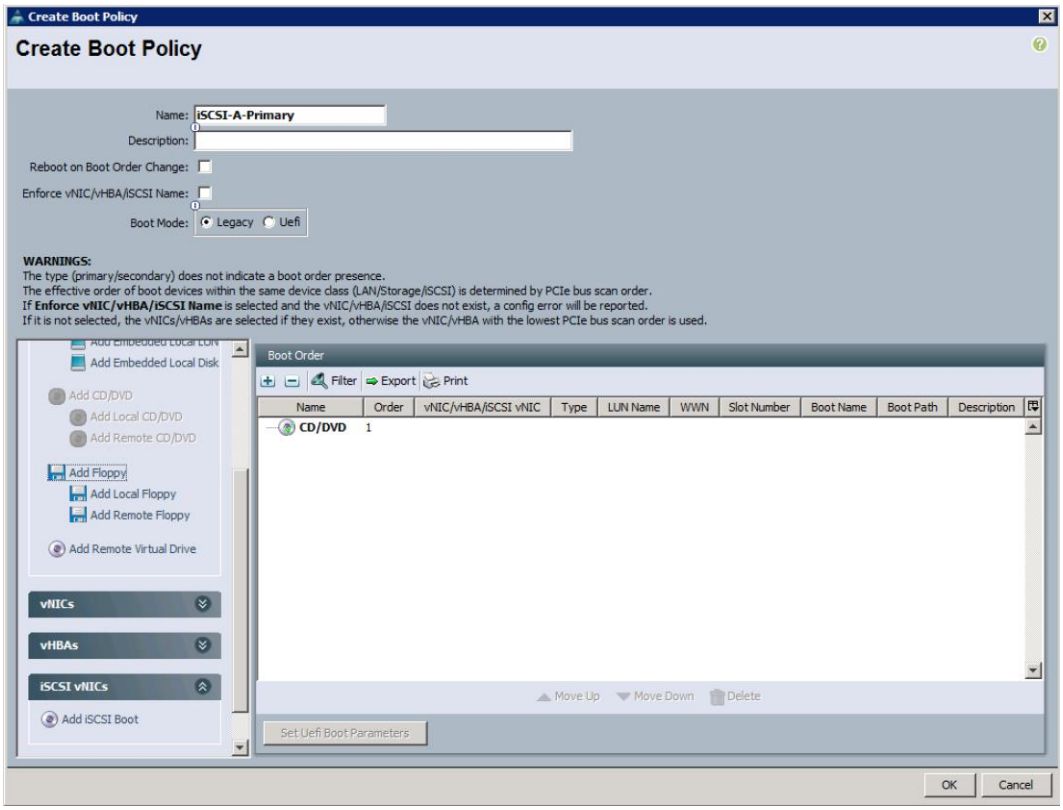
1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click vNIC Templates and select Create vNIC Template.
4. Enter `iSCSI-A` as the vNIC template name.
5. Keep Fabric A selected.
6. Do not select the Enable Failover checkbox.
7. Under Target, make sure that the VM checkbox is not selected.
8. Select Updating Template as the template type.
9. Under VLANs, select the checkbox for the `iSCSI-A` VLAN.
10. Set iSCSI-A as the native VLAN.
11. For MTU, enter 9000.
12. From the MAC Pool list, select MAC_Pool_A.
13. From the Network Control Policy list, select Enable_CDP.
14. Click OK to create the vNIC template.
15. Click OK.
16. In the navigation pane, select the LAN tab.
17. Select Policies > root.
18. Right-click vNIC Templates and select Create vNIC Template.
19. Enter iSCSI-B as the vNIC template name.
20. Select Fabric B.
21. Do not select the Enable Failover checkbox.
22. Under Target, make sure the VM checkbox is not selected.
23. Select Updating Template as the template type.
24. Under VLANs, select the checkboxes for the iSCSI-B VLAN.
25. Set iSCSI-B as the native VLAN.
26. For MTU, enter 9000.
27. From the MAC Pool list, select MAC_Pool_B.
28. From the Network Control Policy list, select Enable_CDP.
29. Click OK to create the vNIC template.
30. Click OK.

Create Boot Policy

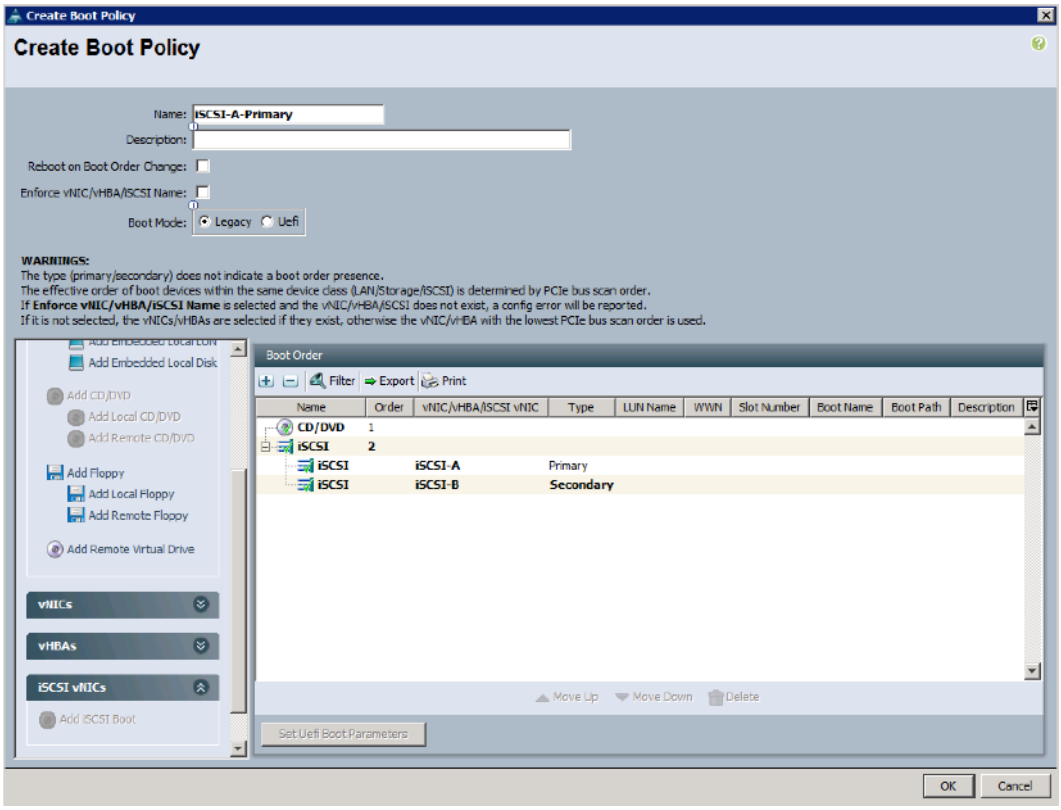
In this procedure, two boot policies are created: one that uses iSCSI fabric A to boot and another that uses fabric B to boot. Two boot policies are used so that boot traffic can be load balanced manually across the two fabrics. Complete the following steps to create boot policies:

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

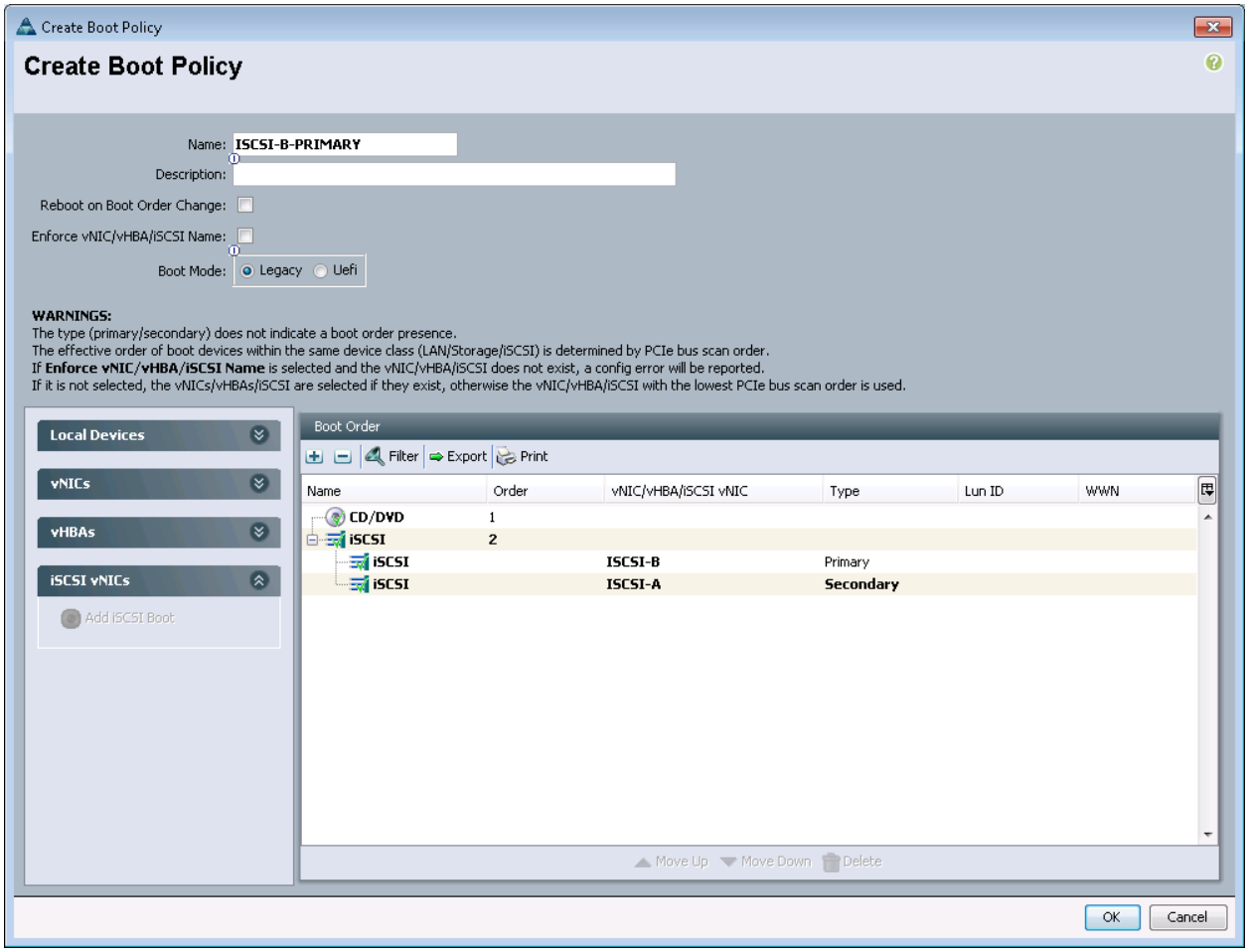
2. Select Servers > Policies > Root.
3. Right-click Boot Policies and select Create Boot Policy.
4. Name the boot policy `iSCSI-A-PRIMARY`.
5. Uncheck the check box beside Enforce vNIC/vHBA/iSCSI Name.
6. Choose the Legacy radio button beside Boot Mode.
7. Expand the Local Devices menu.
8. Select Add CD/DVD.
9. Expand the iSCSI vNICs menu.



10. Select Add iSCSI Boot.
11. Enter `iSCSI-A` as the name.
12. Click OK to add the iSCSI vNIC.
13. Click Add iSCSI Boot.
14. Enter `iSCSI-B` as the name.
15. Click OK to add the iSCSI vNIC.



16. Click OK to save the boot policy.
17. Click OK to dismiss the notification window.
18. Right-click Boot Policies in the left pane and select Create Boot Policy.
19. Name the boot policy `iSCSI-B-PRIMARY`.
20. Clear the Enforce vNIC/vHBA/iSCSI Name checkbox.
21. Select Boot Mode.
22. Expand the Local Devices menu.
23. Select Add CD/DVD.
24. Expand the iSCSI vNICs menu.
25. Select Add iSCSI Boot.
26. Enter iSCSI-B as the name.
27. Click OK to add the iSCSI vNIC.
28. Click Add iSCSI Boot.
29. Enter iSCSI-A as the name.
30. Click OK to add the iSCSI vNIC.



31. Click OK to save the boot policy.
32. Click OK to dismiss the notification window.

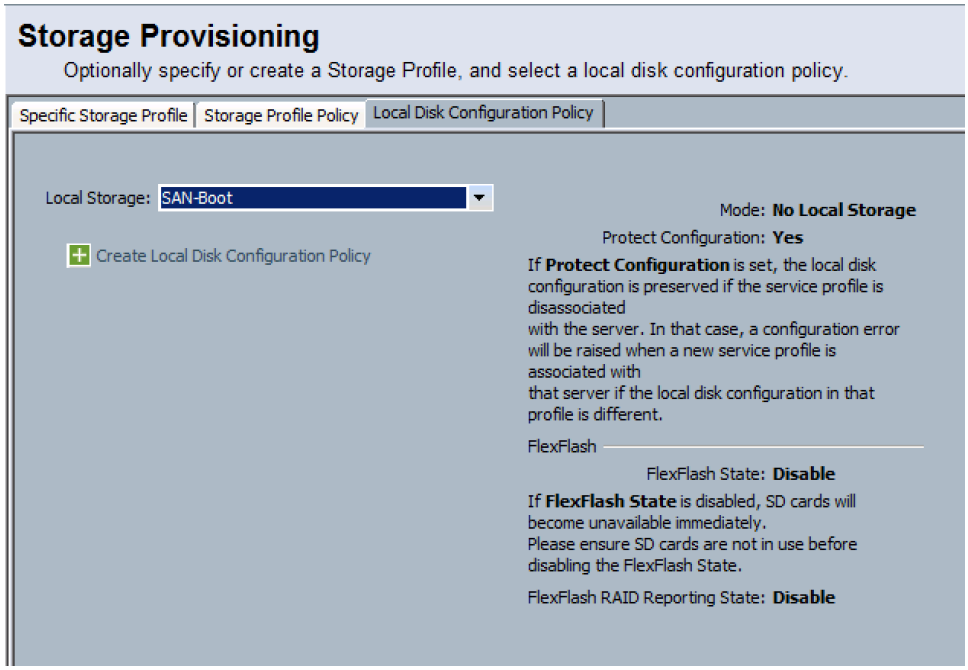
Create Service Profile Template

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

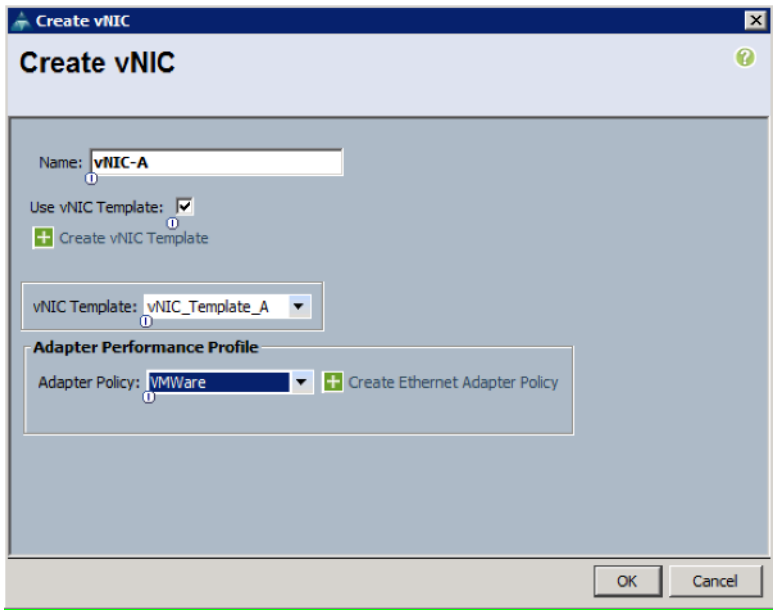
To create service profile templates, complete the following steps:

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

a. Click the Local Disk Configuration Policy tab.
b. From the Local Storage drop-down menu, select SAN-Boot and click Next.



6. Configure the networking options:
   a. Retain 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 and do as follows:
      i. In the Create vNIC dialog box, enter `vNIC-A` as the name of the vNIC.
      ii. Select the Use vNIC Template checkbox.
      iii. From the vNIC Template list, select vNIC_Template_A.
      iv. From the Adapter Policy list, select VMWare.
      v. Click OK to add this vNIC to the template.



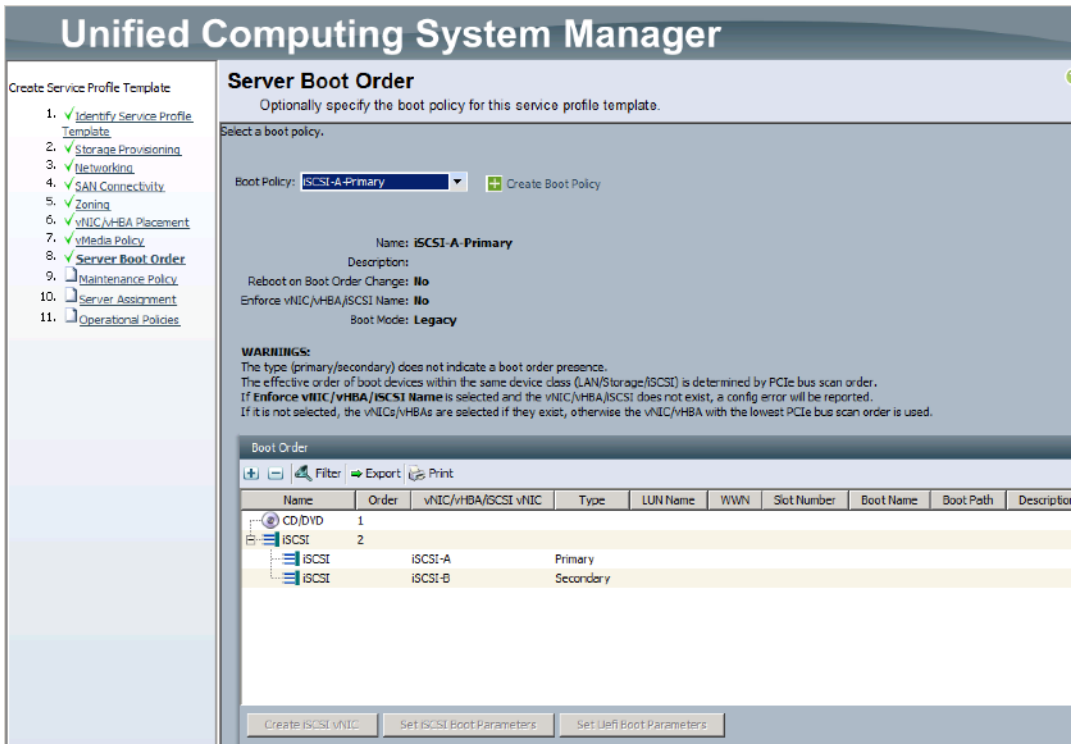
d. In the Networking page of the wizard, click the upper Add button to add another vNIC to the template and do as follows:
    vi. In the Create vNIC box, enter `vNIC-B` as the name of the vNIC.
    vii. Select the Use vNIC Template checkbox.
    viii. From the vNIC Template list, select vNIC_Template_B.
    ix. From the Adapter Policy list, select VMWare.
    x. Click OK to add the vNIC to the template.
e. In the Networking page of the wizard, click the upper Add button to add another vNIC to the template and do as follows:
    i. In the Create vNIC box, enter `iSCSI-A` as the name of the vNIC.
    ii. Select the Use vNIC Template checkbox.
    iii. From the vNIC Template list, select iSCSI-A.
    iv. From the Adapter Policy list, select VMWare.
    v. Click OK to add the vNIC to the template.
f. In the Networking page of the wizard, click the upper Add button to add another vNIC to the template and do as follows:
    i. In the Create vNIC box, enter `iSCSI-B` as the name of the vNIC.
    ii. Select the Use vNIC Template checkbox.
    iii. From the vNIC Template list, select iSCSI-B.
    iv. From the Adapter Policy list, select VMWare.
    v. Click OK to add the vNIC to the template.
g. Review the table in the Networking page to make sure that all vNICs were created.
h. Click Expand the iSCSI vNICs section.
i. Choose the default pool in the iSCSI Initiator Name Assignment field.
j. Click the Add button and do as follows:
    i. Name the iSCSI vNIC iSCSI-A.
    ii. Set the overlay vNIC to iSCSI-A.
    iii. Set the VLAN to iSCSI-A (native).

iv. Click OK.

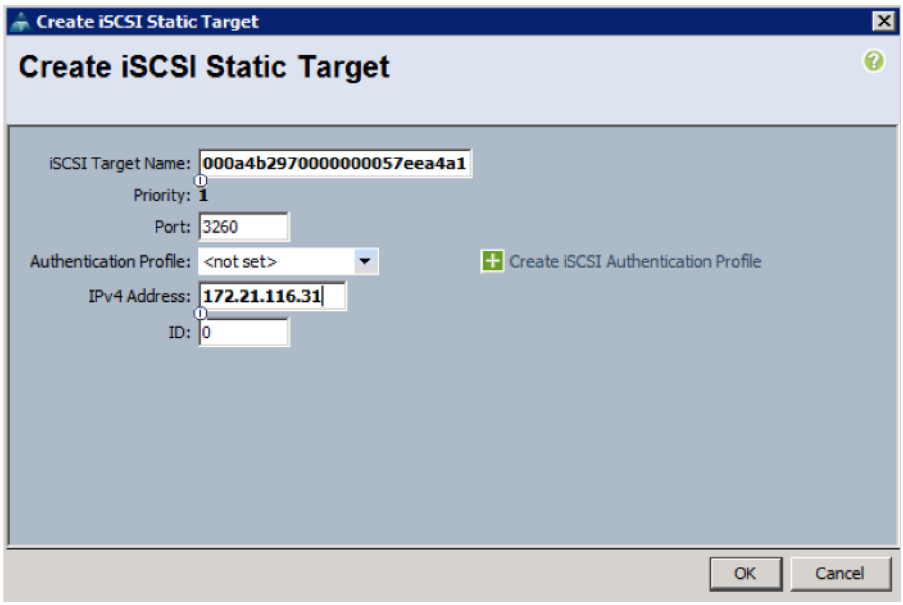
k. Click the Add button and do as follows:
   i. Name the iSCSI vNIC iSCSI-B.
   ii. Set the overlay vNIC to iSCSI-B.
   iii. Set the VLAN to iSCSI-B (native).
   iv. Click OK.

l. Review the settings, then click Next to proceed.

7. Configure the SAN connectivity options:
   a. Select the No vHBAs option because FC/FCoE is not used.
   b. Click Next.
8. Set no zoning options and click Next.
9. Set the vNIC/vHBA placement options.
   a. From 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:
      i. vNIC vNIC-A
      ii. vNIC vNIC-B
      iii. vNIC iSCSI-A
      iv. vNIC iSCSI-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. Click Next on the vMedia Policy screen.
11. Set the server boot order:
   a. From the Boot Policy list, select iSCSI-A-PRIMARY.
   b. Review the table to verify that all boot devices were created and identified. Verify that the boot devices are in the correct boot sequence.



c. Select iSCSI-A.
d. Click Set iSCSI Boot Parameters.
e. Select iSCSI-A-POOL as the initiator IP address policy.
f. Select the iSCSI Static Target Interface option.
g. Click the Add button to add an iSCSI static target:
    i. Set the iSCSI target name to the value gathered from the previous section.
    ii. Set the IP address value to `<<var_controllerA_iscsi_port_0A>>`.
    iii. Set the LUN ID to 0.
    iv. Click OK.



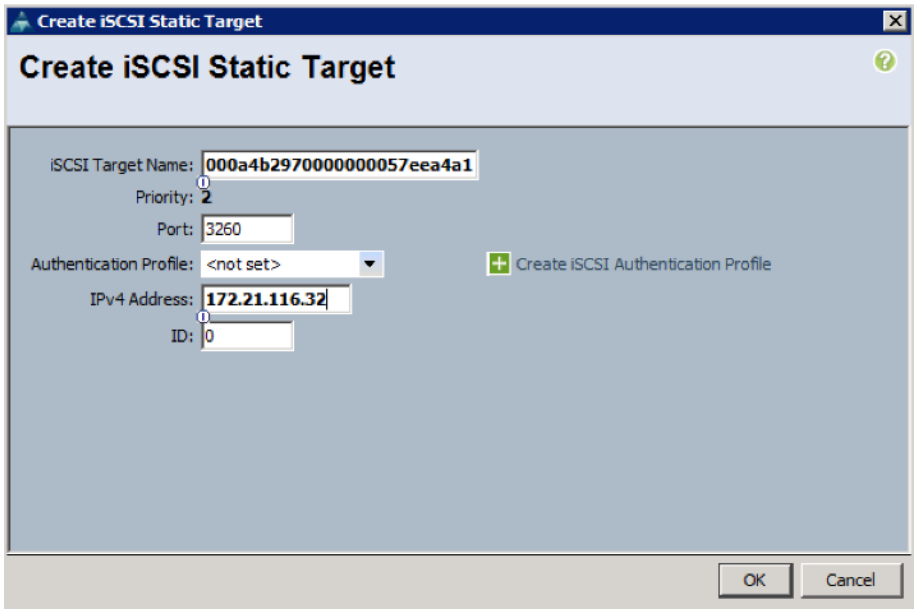
h. Click the Add button to add an iSCSI static target:

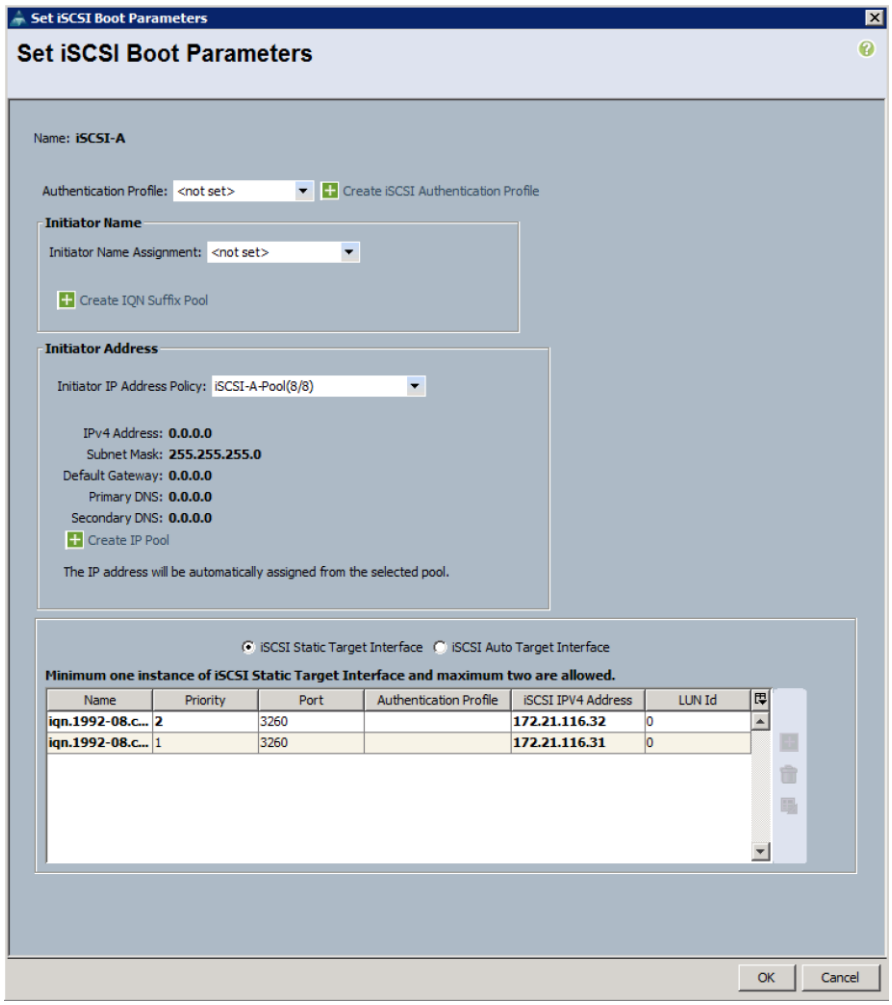
i. Set the iSCSI target name to the value gathered from the previous section.

ii. Set the IP address value to `<<var_controllerB_iscsi_port_0A>>`.

iii. Set the LUN ID to 0.

iv. Click OK.





i. Review the configuration and then click OK.

j. Select iSCSI-B and click Set iSCSI Boot Parameters.

k. Select iSCSI-B-POOL as the initiator IP address policy.

l. Select the iSCSI Static Target Interface option.

m. Click the Add button to add an iSCSI static target:

   i. Set the iSCSI target name to the value gathered from the previous section.

   ii. Set the IP address value to `<<var_controllerA_iscsi_port_2>>`.

   iii. Set the LUN ID to 0.

   iv. Click OK.

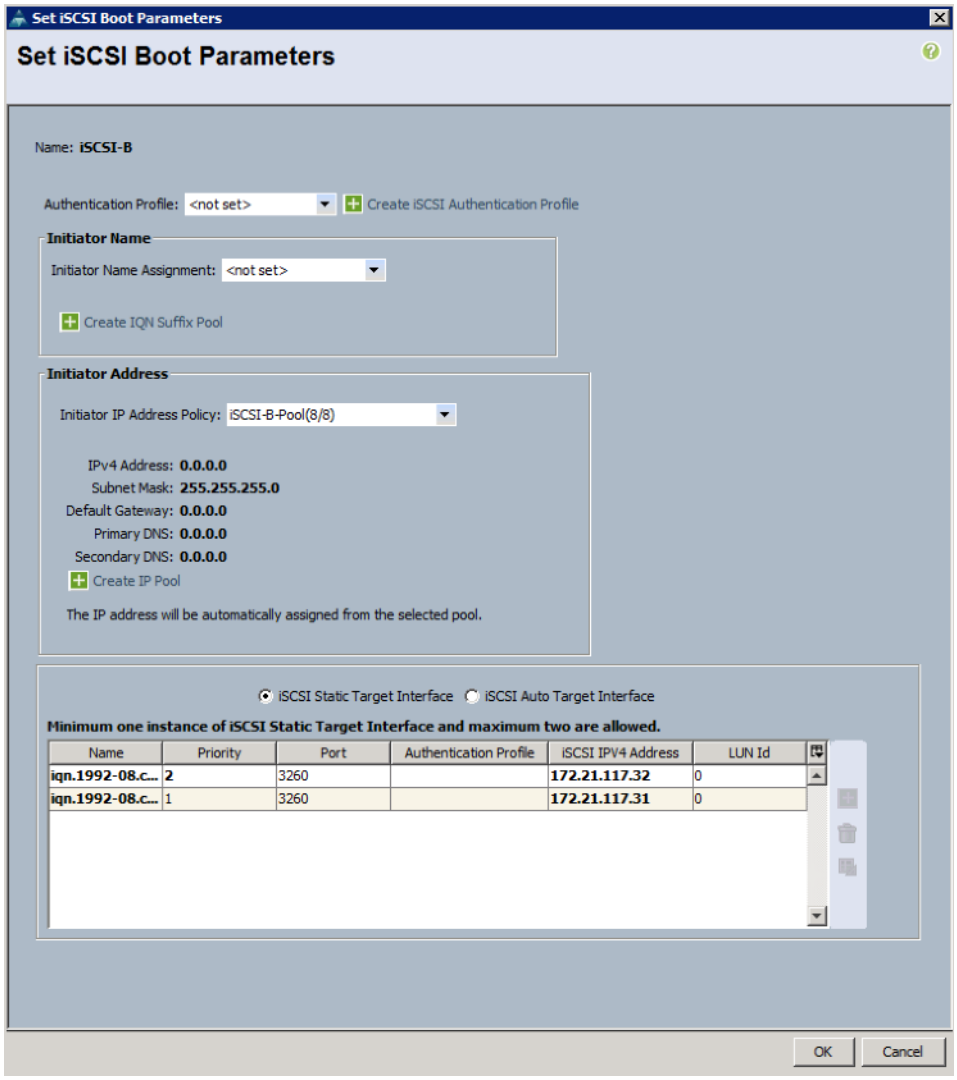
n. Click the Add button to add an iSCSI static target:

   i. Set the iSCSI target name to the value gathered from the previous section.

   ii. Set the IP address value to `<<var_controllerB_iscsi_port_2>>`.

   iii. Set the LUN ID to 0.

   iv. Click OK.



o. Review the configuration and then click OK.

p. Click Next.

12. Add a maintenance policy:
    a. Keep the default setting of not using a policy.
    b. Click Next.
13. Specify the server assignment:
    a. From 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.
14. Add operational policies:
    a. From 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.

15. Click Finish to create the service profile template.
16. Click OK in the confirmation message.
17. Click the Servers tab in the navigation pane.
18. Select Service Profile Templates > root.
19. Right-click the previously created `VM-HOST-iSCSI-A` template.
20. Select Create a Clone.
21. In the dialog box, enter `VM-Host-iSCSI-B` as the name of the clone, select the root Org, and click OK.
22. Click OK.
23. Select the newly cloned service profile template and click the Boot Order tab.
24. Click Modify Boot Policy.
25. From the Boot Policy list, select `iSCSI-B-PRIMARY`.
26. Click OK and then click OK again to close the confirmation window.
27. In the right pane, click the Network tab and then click Modify vNIC/HBA Placement.
28. From the Select Placement drop-down menu, select VM-HOST-INFRA. Expand `vCon 1` and set the vNICs in the following order:
    a. vNIC-A
    b. vNIC-B
    c. iSCSI-B
    d. iSCSI-A
29. Click OK and then click OK again to dismiss the confirmation window.

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-iSCSI-A.
3. Right-click VM-Host-iSCSI-A and select Create Service Profiles from Template.
4. Enter `VM-Host-Infra-0` as the naming prefix.
5. Keep 1 as the suffix starting number.
6. Enter 1 as the number of instances to create.
7. Click OK to create the service profile.
8. Click OK in the confirmation message.
9. Select Service Profile Templates > root > Service Template VM-Host-iSCSI-B.
10. Right-click VM-Host-Infra-Fabric-B and select Create Service Profiles from Template.
11. Enter `VM-Host-Infra-0` as the naming prefix.
12. Enter `2` as the suffix starting number.
13. Enter `1` as the number of instances to create.
14. Click OK to create the service profile.
15. Click OK in the confirmation message.

16. Verify that the service profiles VM-HOST-Infra-01 and VM-HOST-Infra-02 have been created. The service profiles are automatically associated with the servers in their assigned server pools.
17. Optional: Select each newly created service profile and enter the server host name or the FQDN in the User Label field in the General tab. Click Save Changes to map the server host name to the service profile name.

Add More Servers to FlexPod Unit

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

Gather Necessary Information

After the Cisco UCS service profiles have been created, each infrastructure blade in the environment has a unique configuration. To proceed with the FlexPod Express deployment, specific information must be gathered from each Cisco UCS blade and from the NetApp controllers. Insert the required information into Table 12 and Table 13.

Table 12) iSCSI IP addresses for storage array.

Array	iSCSI IP
Controller 1 Port 1	
Controller 1 Port 2	
Controller 2 Port 1	
Controller 2 Port 2	

Table 13) iSCSI IPs for Cisco UCS servers.

Cisco UCS Service Profile Name	iSCSI-A IP	iSCSI-B IP	IQN
VM-HOST-01			
VM-HOST-02			

Note: To gather the iSCSI IQN and iSCSI vNIC IP information, launch the Cisco UCS Manager GUI. In the navigation pane, click the Servers tab. Expand Servers > Service Profiles > root. For each service profile, click the iSCSI vNICs tab in the right pane. The IQN is the initiator name in this window. Click the Boot Order tab. Click each iSCSI vNIC and click Set Boot Parameters. The IP address is located in the Initiator Address section of this window. In Table 13, record the IQN and IP information for each service profile.

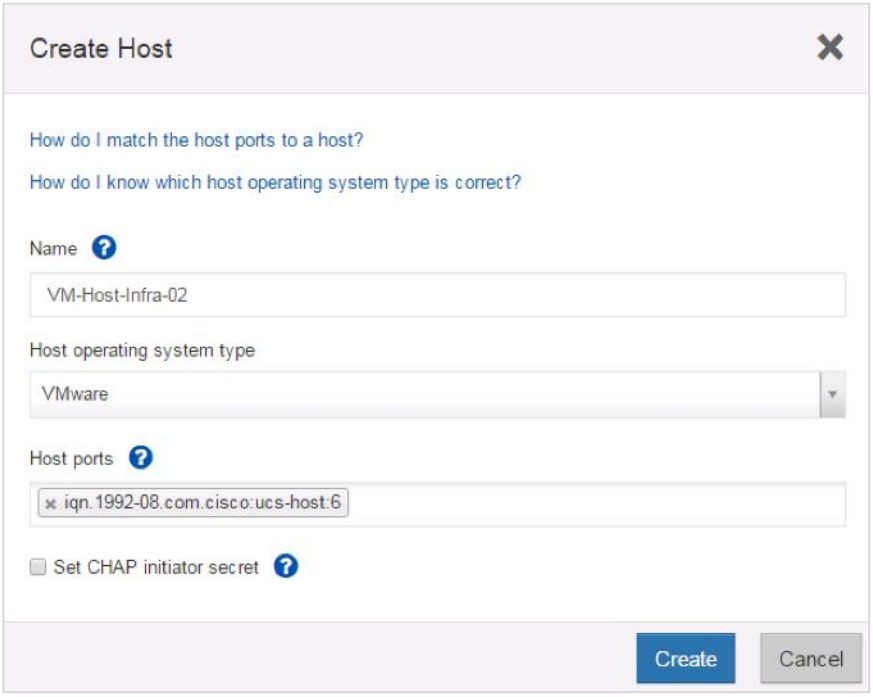
6.4 NetApp E-Series 2824 Configuration: Part II

After the service profiles have been created and their IQNs have been generated, the service profiles can be mapped to the previously created volumes on the E-Series storage array. Complete the following tasks to define iSCSI hosts and groups within SANtricity System Manager and to map hosts to volumes.

Manually Define Hosts in SANtricity

1. Using a web browser, launch the SANtricity System Manager.
2. In the left pane, click Storage. In the right pane, click Hosts.
3. Click Create and select Host from the drop-down menu.
4. Enter the name for the host: `VM-Host-Infra-01`.

5. Select VMware as the host operating system type.
6. In the Host Port field, enter the IQN for service profile VM-Host-Infra-01.
7. Click Create.
8. Repeat steps 3 to 7 for host `VM-Host-Infra-02`.

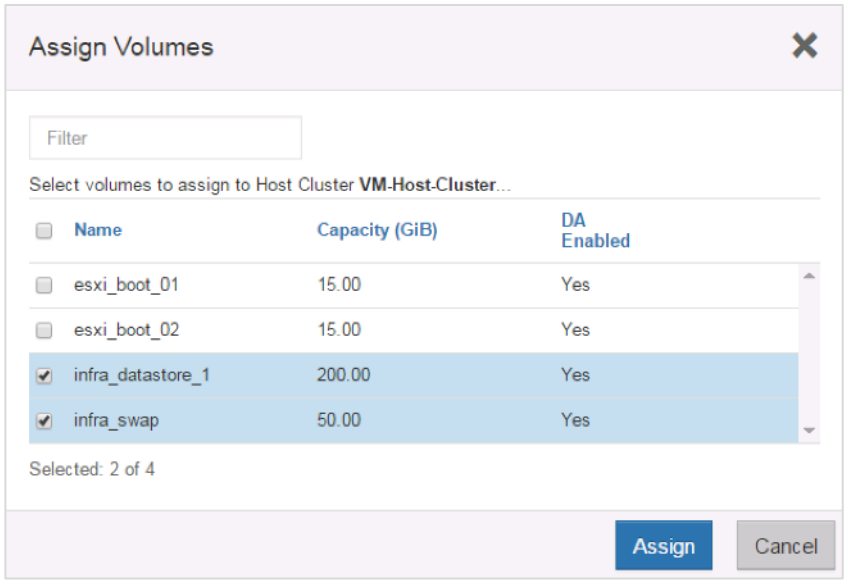


Create a Host Cluster

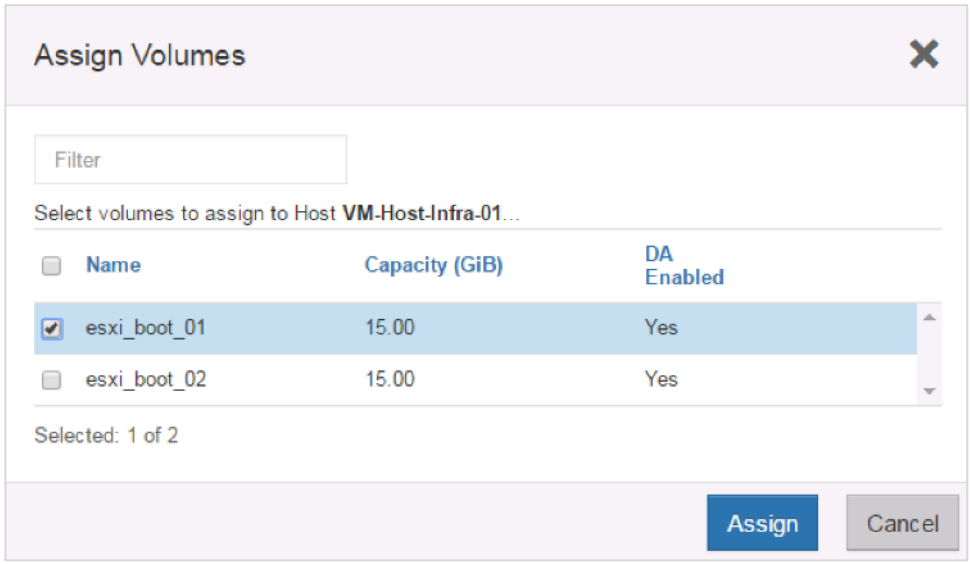
1. In the left pane, click Storage. In the right pane, click Hosts.
2. Click Create and select Host cluster from the drop-down menu.
3. Enter a name for the host cluster: `VM-Host-Cluster`.
4. Select the two hosts: VM-Host-Infra-01 and VM-Host-Infra-02.
5. Click Create.

Assign Volumes to Hosts and Host Cluster

1. In the left pane, click Storage. In the right pane, click Hosts.
2. Select the `VM-Host-Cluster` host cluster and click Assign Volumes.
3. Select infra_datastore_1 and infra_swap.
4. Click Assign.



5. Enter `DISABLE` to confirm the removal of Data Assurance.
6. Click Disable.
7. Select the host `VM-Host-Infra-01` and click Assign Volumes.
8. Select `esxi_boot_01` and click Assign.



9. Enter `DISABLE` to confirm the removal of Data Assurance.
10. Click Disable.
11. Select the host `VM-Host-Infra-02` and click Assign Volumes.
12. Select `esxi_boot_02` and click Assign.
13. Enter `DISABLE` to confirm the removal of Data Assurance.
14. Click Disable.

Modify Boot LUN IDs

1. In the left pane, click Storage. In the right pane, click Volumes.
2. Select the volume esxi_boot_01.
3. Click View/Edit Settings.
4. In the Host section, from the LUN drop-down menu, select 0.
5. Click Save.

6.5 VMware vSphere 6.0 Update 2 Setup

FlexPod Express VMware ESXi 6.0 Update 2 on E-Series

This section provides detailed instructions for installing VMware ESXi 6.0 U2 in a FlexPod Express environment using iSCSI and NetApp E-Series. After the procedures are completed, two iSCSI-booted ESXi hosts are 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 LUNs.

Log in to Cisco UCS Manager

The IP KVM enables the administrator to begin the installation of the operating system 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. 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.
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:

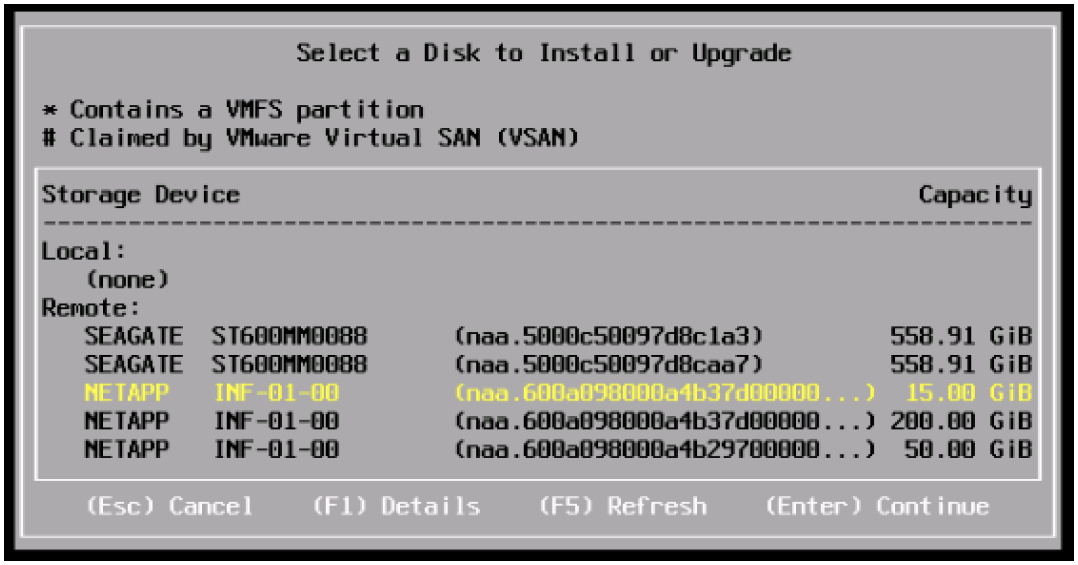
1. In the KVM window, click the Virtual Media tab.
2. If prompted to accept an unencrypted KVM session, accept as necessary.
3. Click Activate Virtual Devices.
4. Click the virtual media menu again and select map CD/DVD.
5. Click browse and browse to the ESXi installed ISO image file and click Open.
6. Click Map device.
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 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 the selected disk will be repartitioned. Press F11 to continue with the installation.
8. From the KVM tab, press Enter to reboot the server.

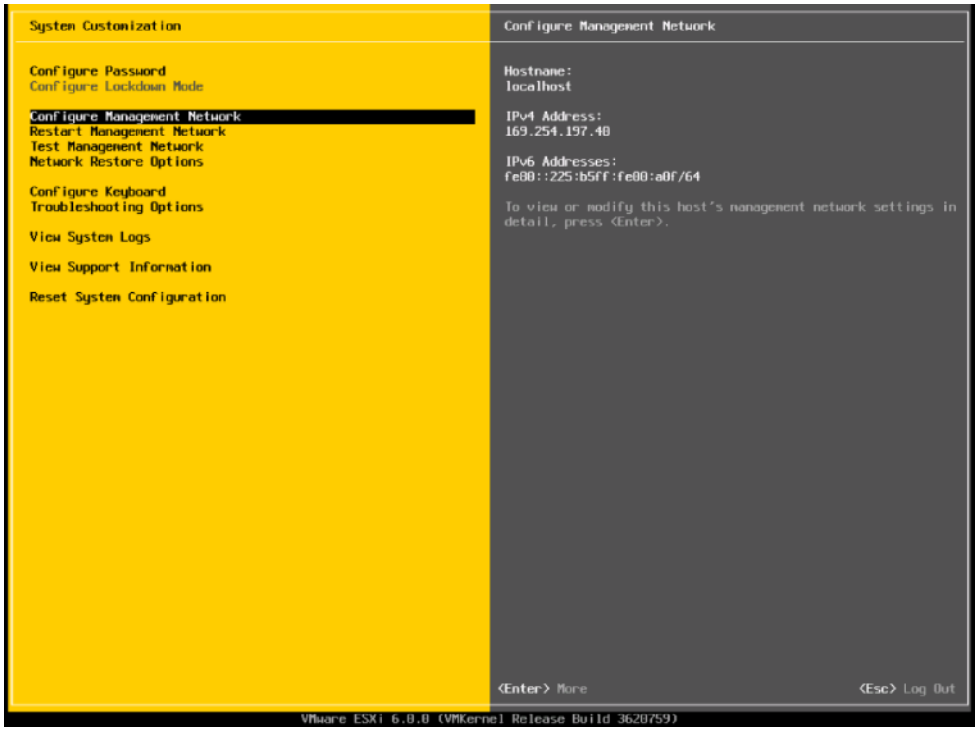
Set Up Management Networking for ESXi Hosts

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:

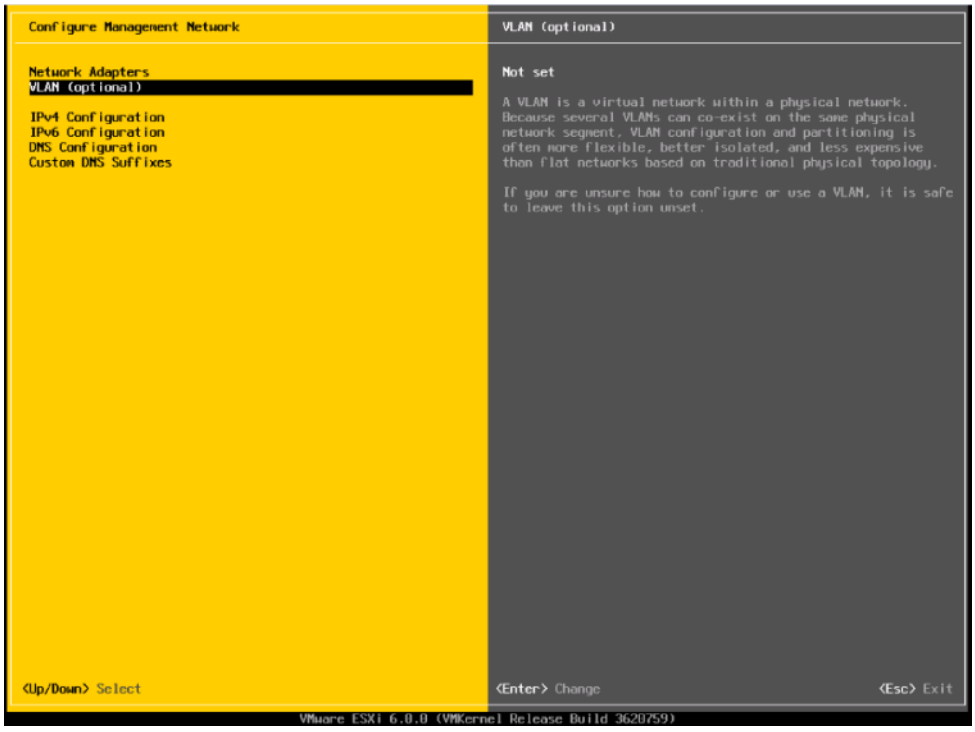
ESXi Host VM-Host-Infra-01

To configure the `VM-Host-Infra-01` ESXi host with access to the management network, complete the following steps:

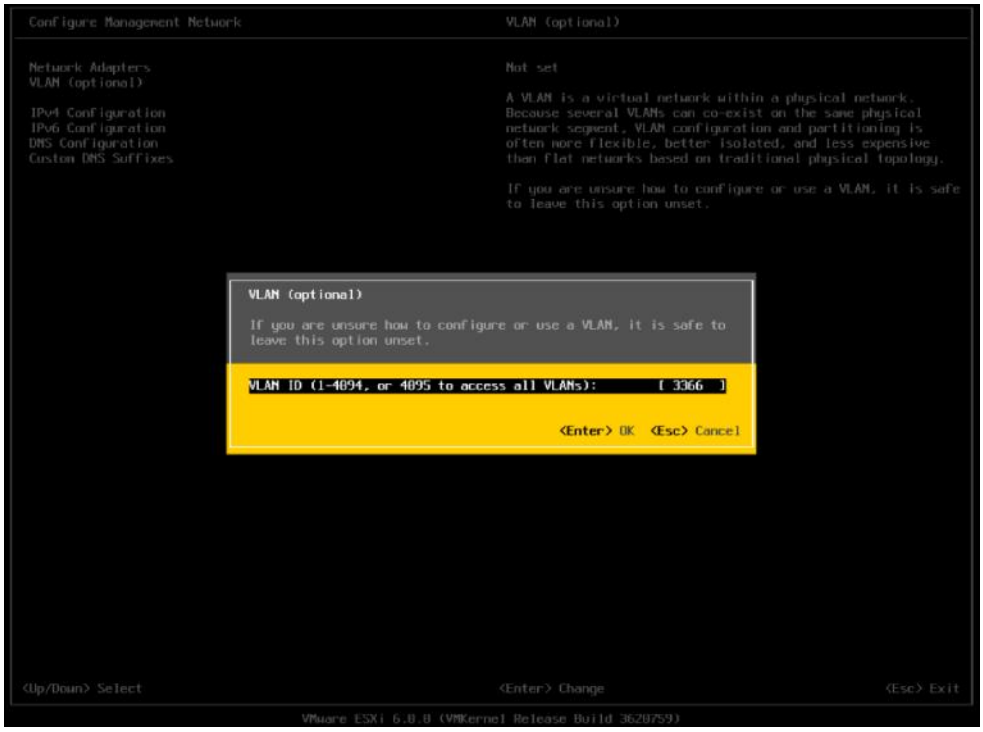
1. After the server has finished rebooting, press F2 to customize the system.
2. Log in as root, enter the corresponding password, and press Enter to log in.
3. Select the Configure the Management Network option and press Enter.



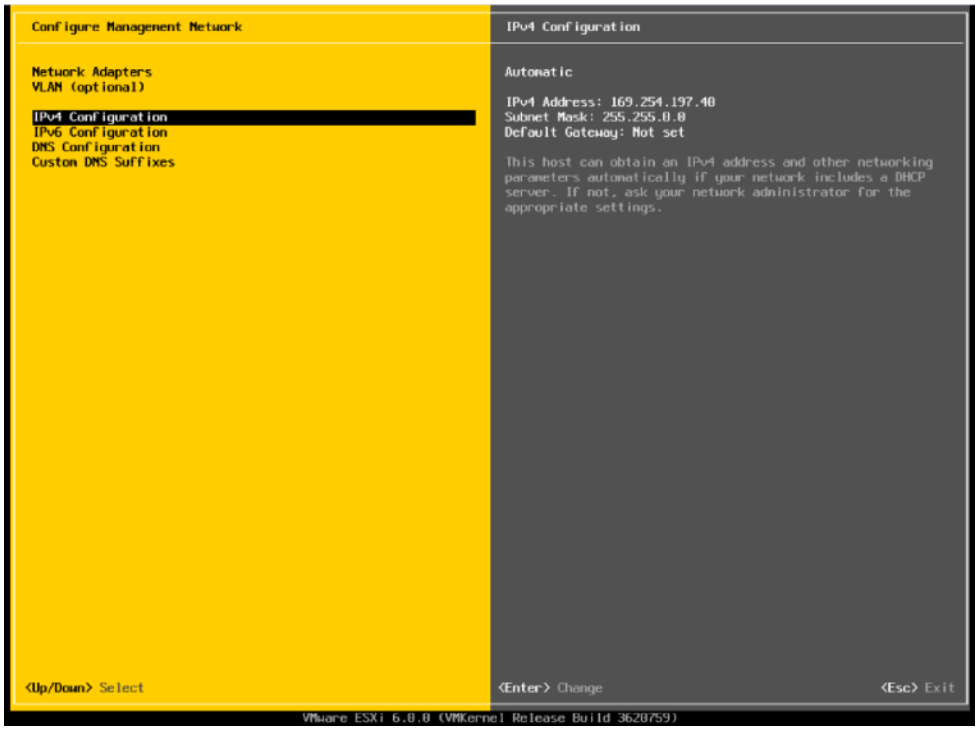
4. Select the VLAN (Optional) option and press Enter.



5. Enter the `<<var_ib-mgmt_vlan_id>>` and press Enter.

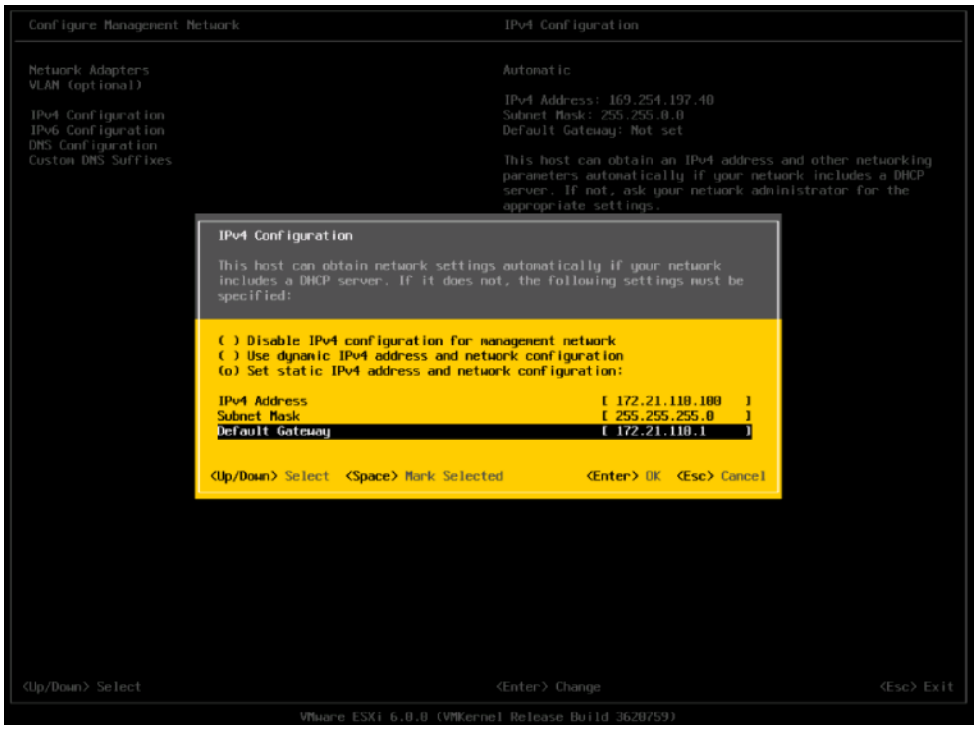


6. From the Configure Management Network menu, select IP Configuration and press Enter.



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.

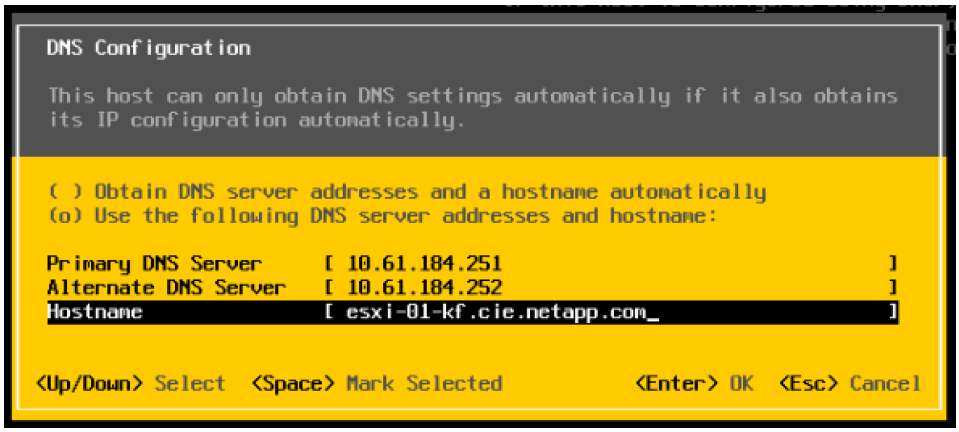
10. Enter the default gateway for the first ESXi host.



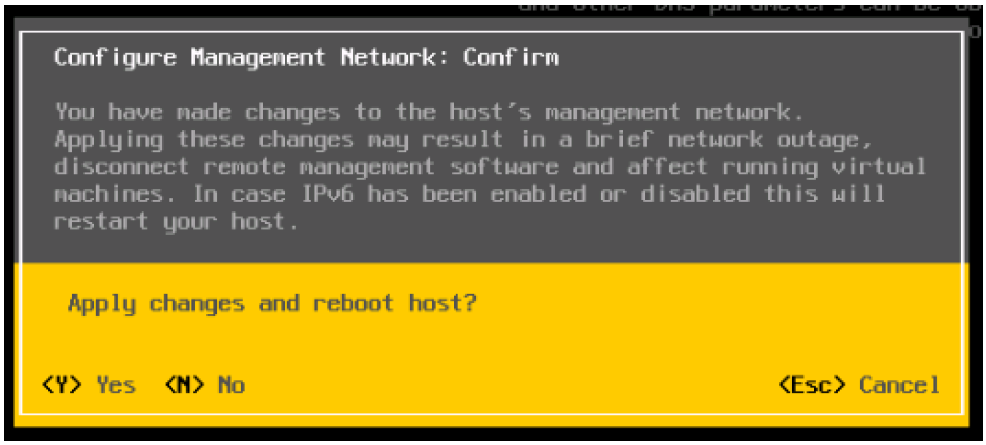
11. Press Enter to accept the changes to the IP configuration.

12. Select the IPv6 Configuration option and press Enter.

13. Using the spacebar, select Disable IPv6 (restart required) and press Enter.
14. Select the DNS Configuration option and press Enter.
15. 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 first ESXi host.

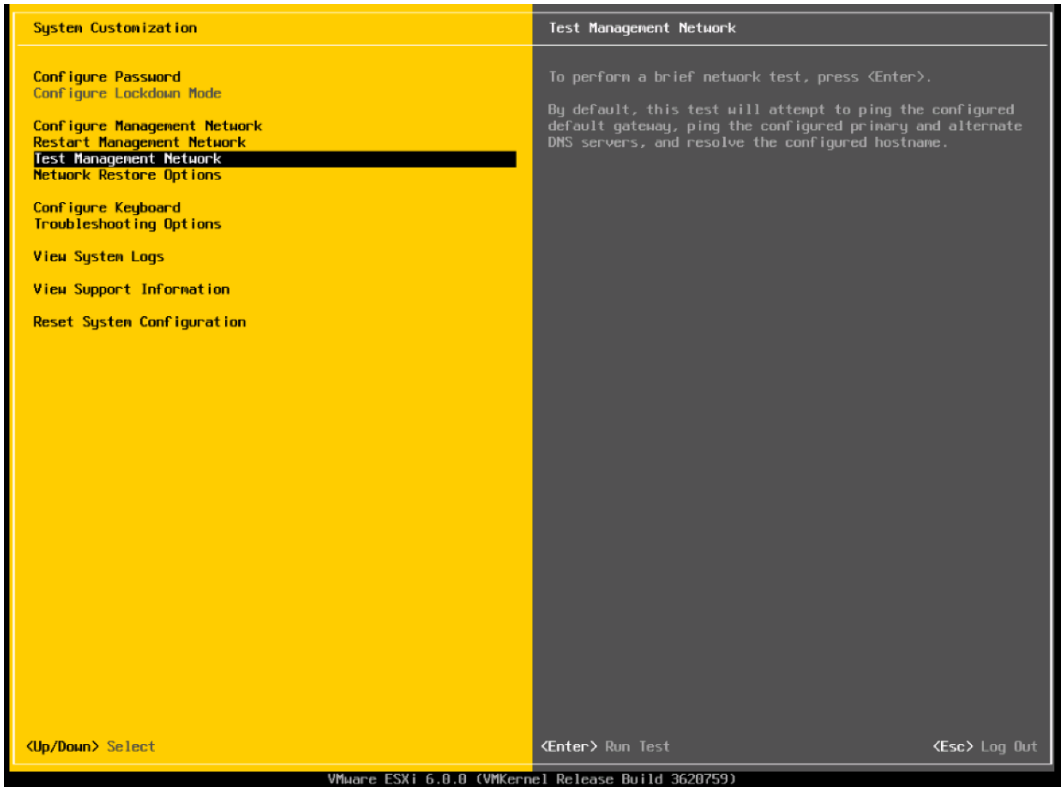


19. Press Enter to accept the changes to the DNS configuration.
20. Press Esc to exit the Configure Management Network submenu.

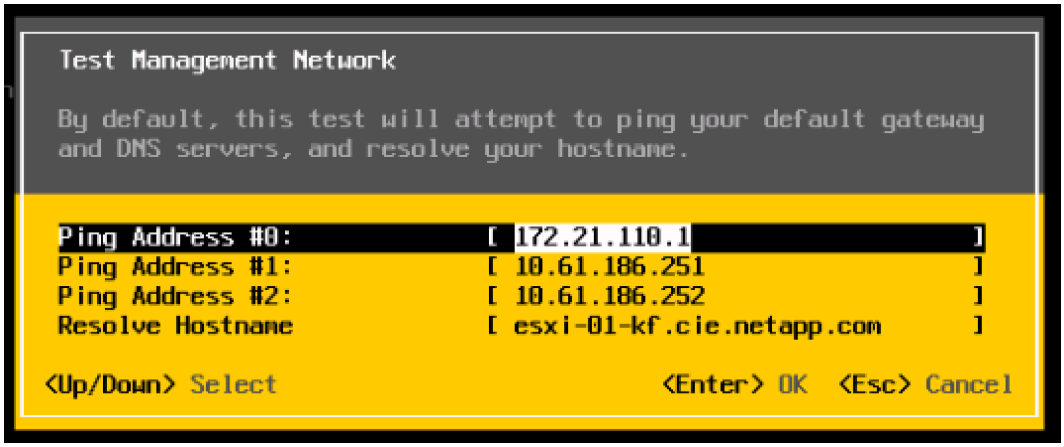


21. Press Y to confirm the changes and return to the main menu.
22. The ESXi host reboots. After reboot, press F2 and log back in as root.

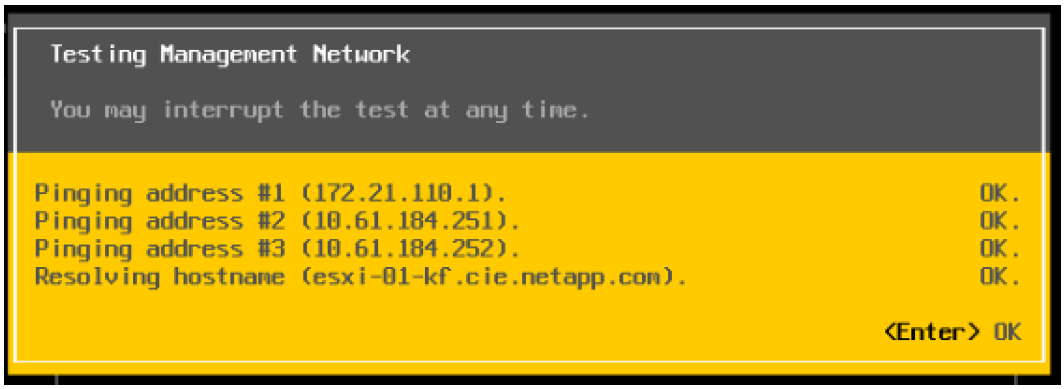
    Note: If the boot process fails due to a device error, click Reset to reboot the server again.



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.
27. Repeat steps 1 to 6 for each additional VM host in the environment. Use the appropriate values for the fields that are specific to each host.

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 CLI.

Note: These applications are downloaded from the VMware website, and Internet access is required on the management workstation.

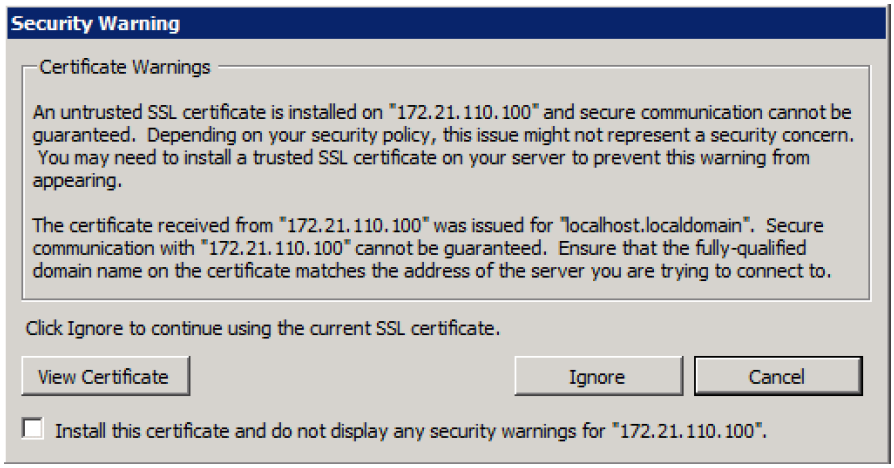
Log in to VMware ESXi Hosts by Using VMware vSphere Client

ESXi Host VM-Host-Infra-01

To log in to the `VM-Host-Infra-01` ESXi host by using the VMware vSphere Client, 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 to which you are trying to connect: `<<var_vm_host_infra_01_ip>>`.
2. Enter `root` for the user name and enter the root password.

3. Click Login to connect.
4. If the Security warning displays, click ignore. Optionally, select the checkbox beside “Install this certificate and do not display any security warnings for…” to avoid this message in the future.



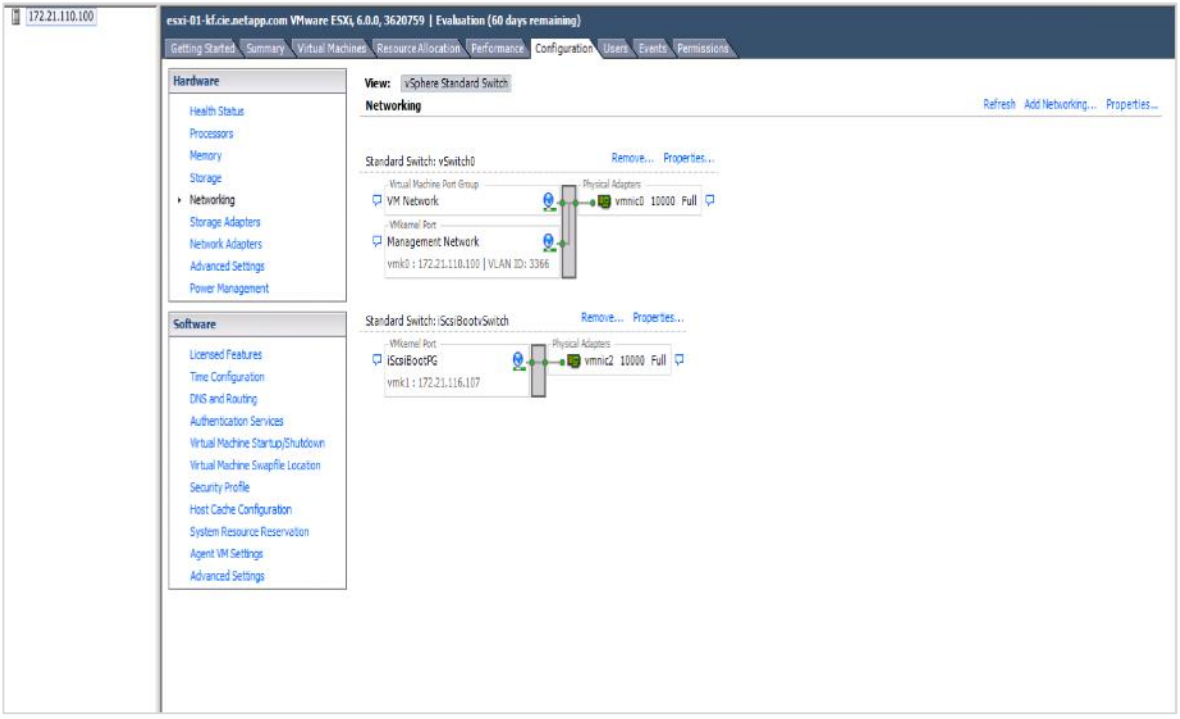
5. Repeat steps 1 through 5 to log in to VM-Host-Infra-02.

Set Up iSCSI Networking for iSCSI Booted Servers

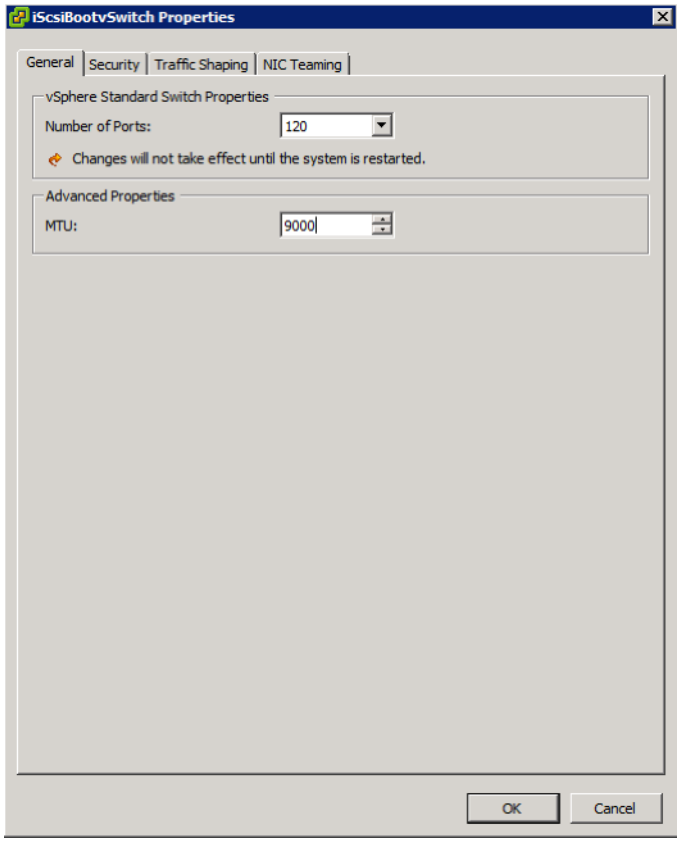
ESXi Hosts VM-Host-Infra-01 and VM-Host-Infra-02

To set up the iSCSI host ports on VM-Host-Infra-01, complete the following steps:

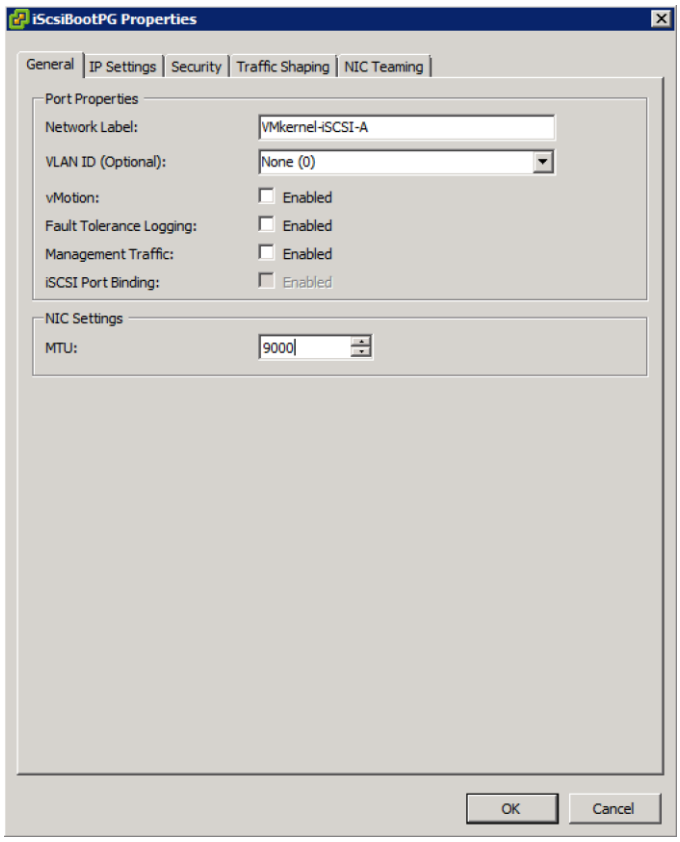
1. Launch the VMware vSphere Client.
2. Connect to the host with the root user ID and password.
3. In the vSphere Client in the right pane, select the configuration tab.
4. In the Hardware pane, select Networking.



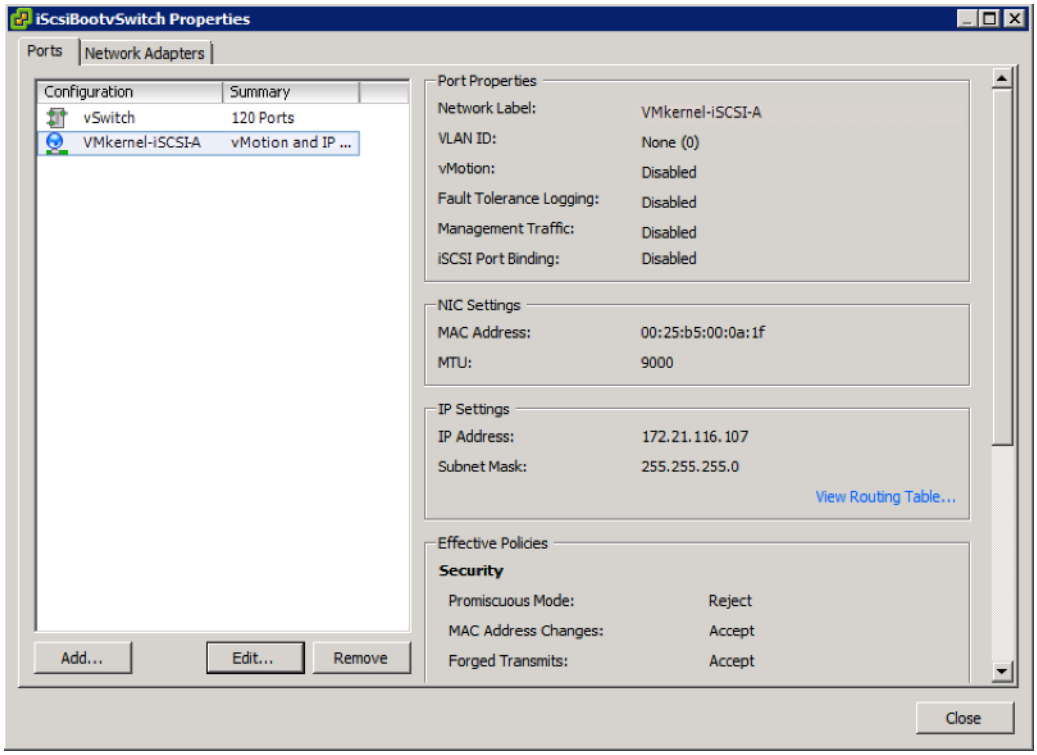
5. Select Properties to the right of the iScsiBootvSwitch.
6. Select the vSwitch configuration and click Edit.
7. Set the MTU to 9000 and click OK.



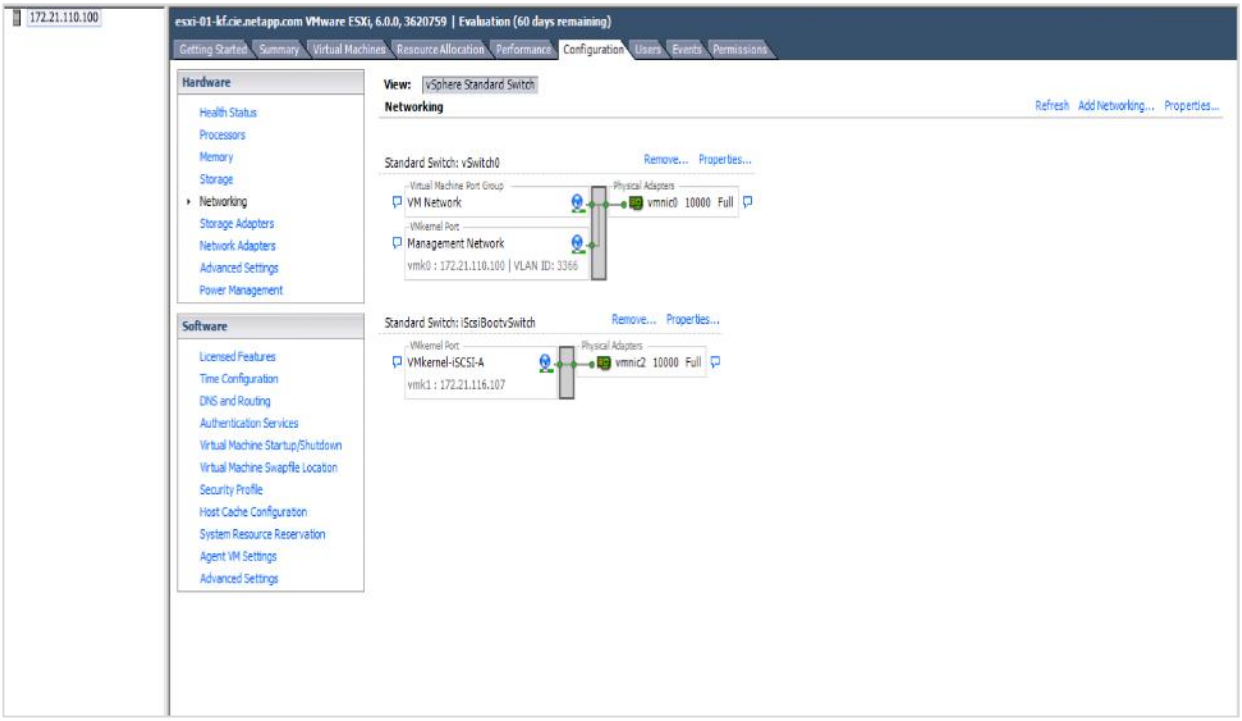
8. Select the iScsiBootPG configuration and click Edit.
9. Change the Network label to VMkernel-iSCSI-A.
10. Set the MTU to 9000.
11. Click OK to accept the change.
12. Do not set a VLAN.



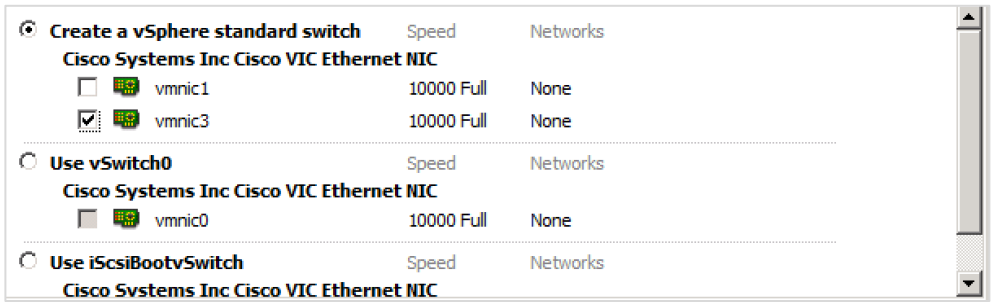
13. Click OK.
14. Click Close to finish the configuration.



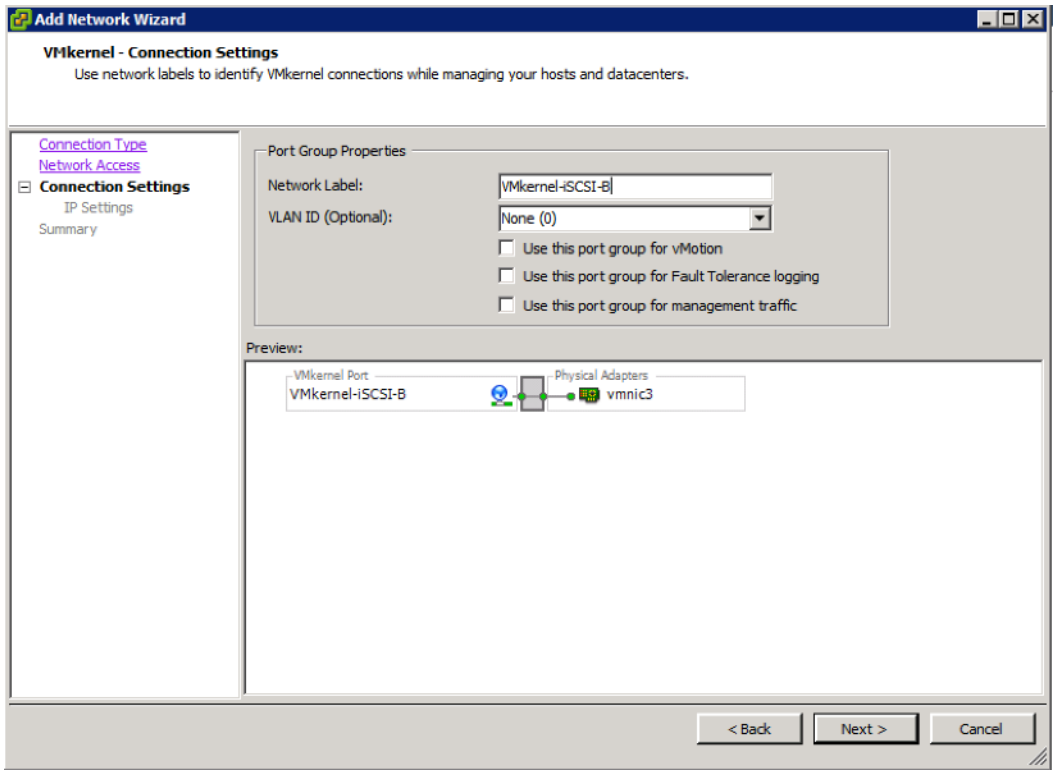
15. On the right, select Add Networking.



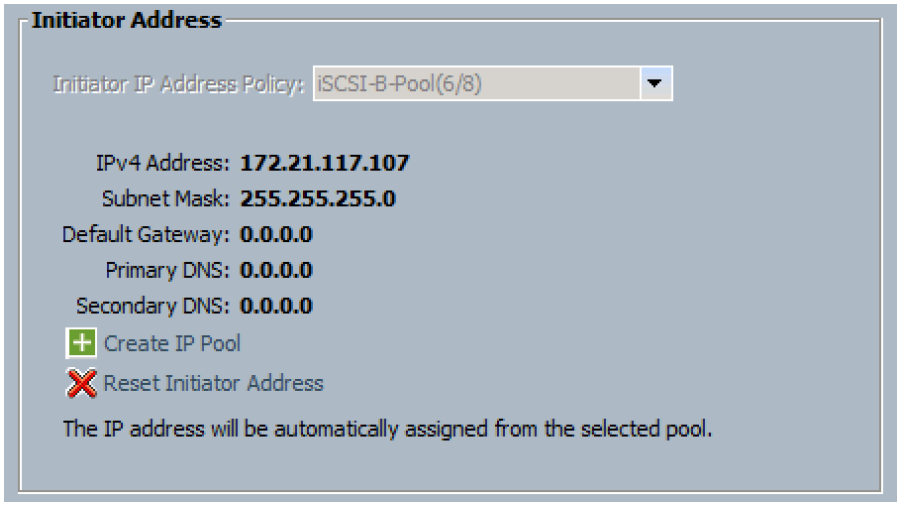
16. Select the VMKernel connection type and click Next.
17. Remove the selection from vmnic1 and select vmnic3.



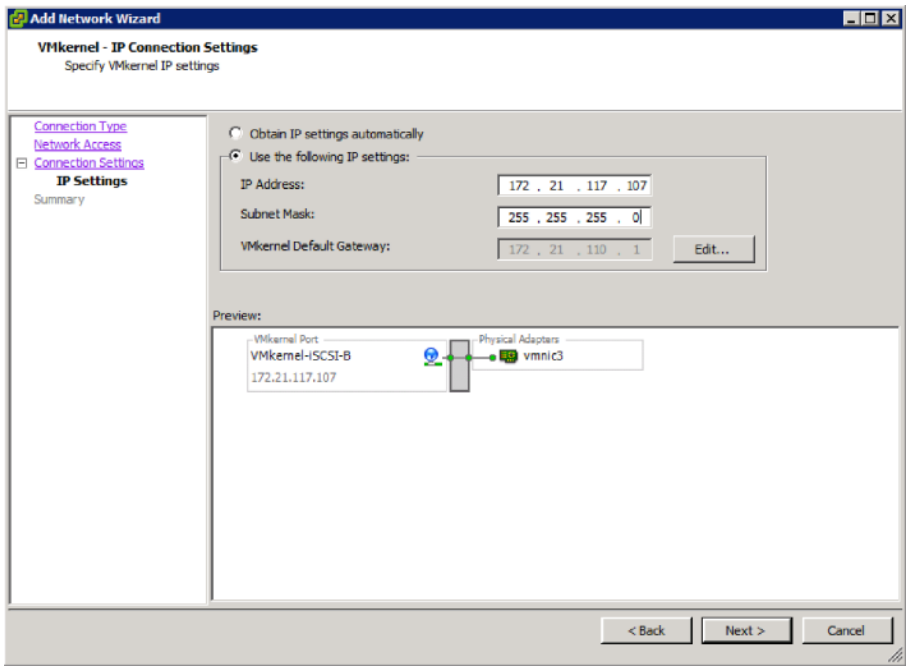
18. Click Next.
19. Set the network label to VMkernel-iSCSI-B. Leave the VLAN ID set to None.
20. Click Next.



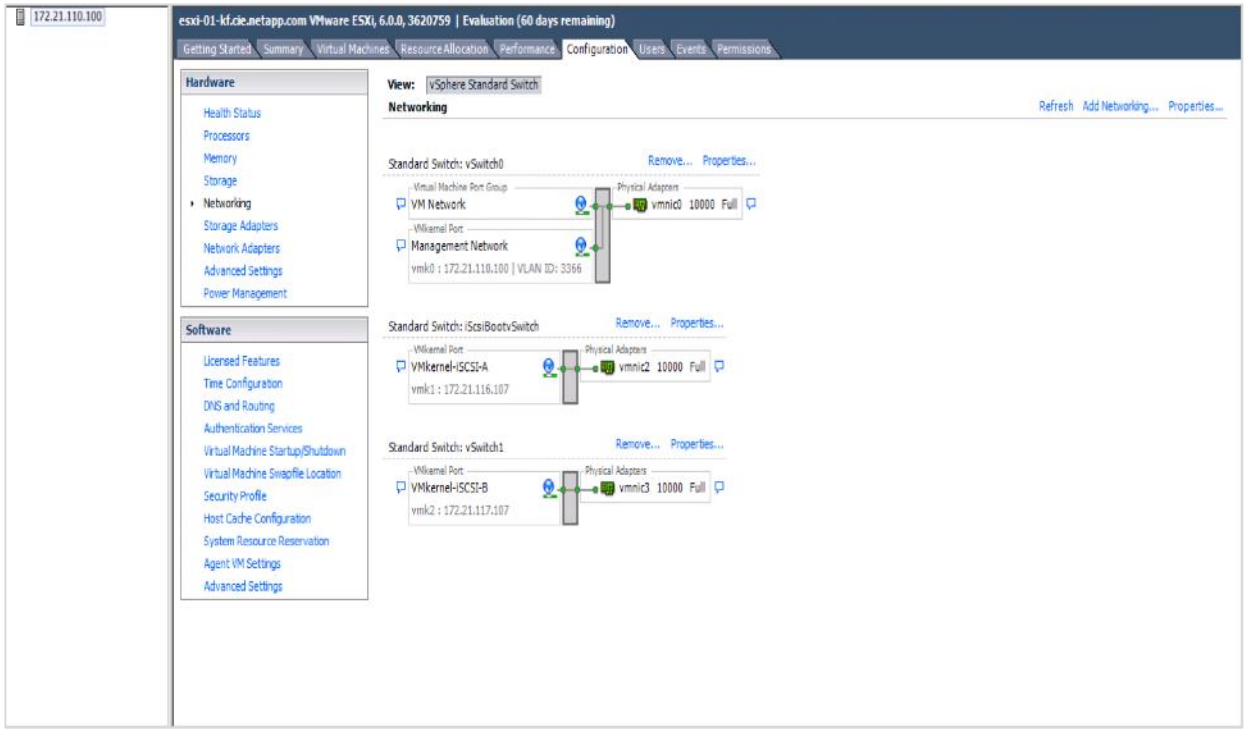
21. Retrieve the VMkernel IP address from Cisco UCS Manager.
22. In Cisco UCS Manager, select the server's service profile. Under the Boot Order tab, expand iSCSI.
23. Select iSCSI-B and click Set iSCSI Boot Parameters. The initiator IP address displays.



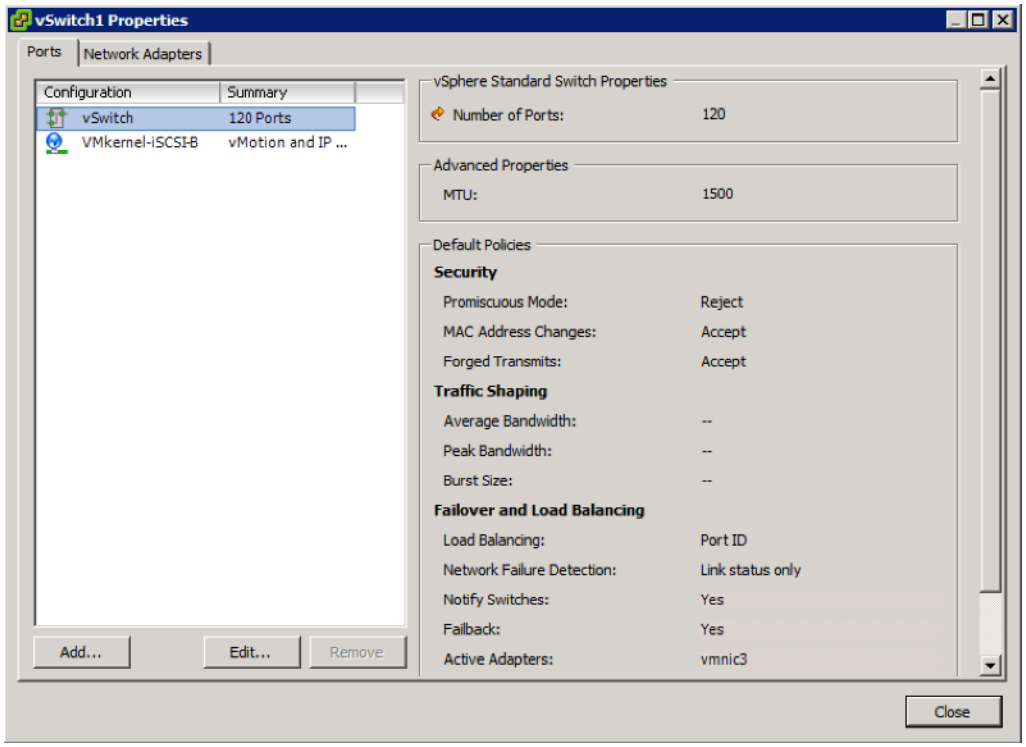
24. In the vSphere Client, enter the IP address and netmask that were obtained from Cisco UCS Manager.



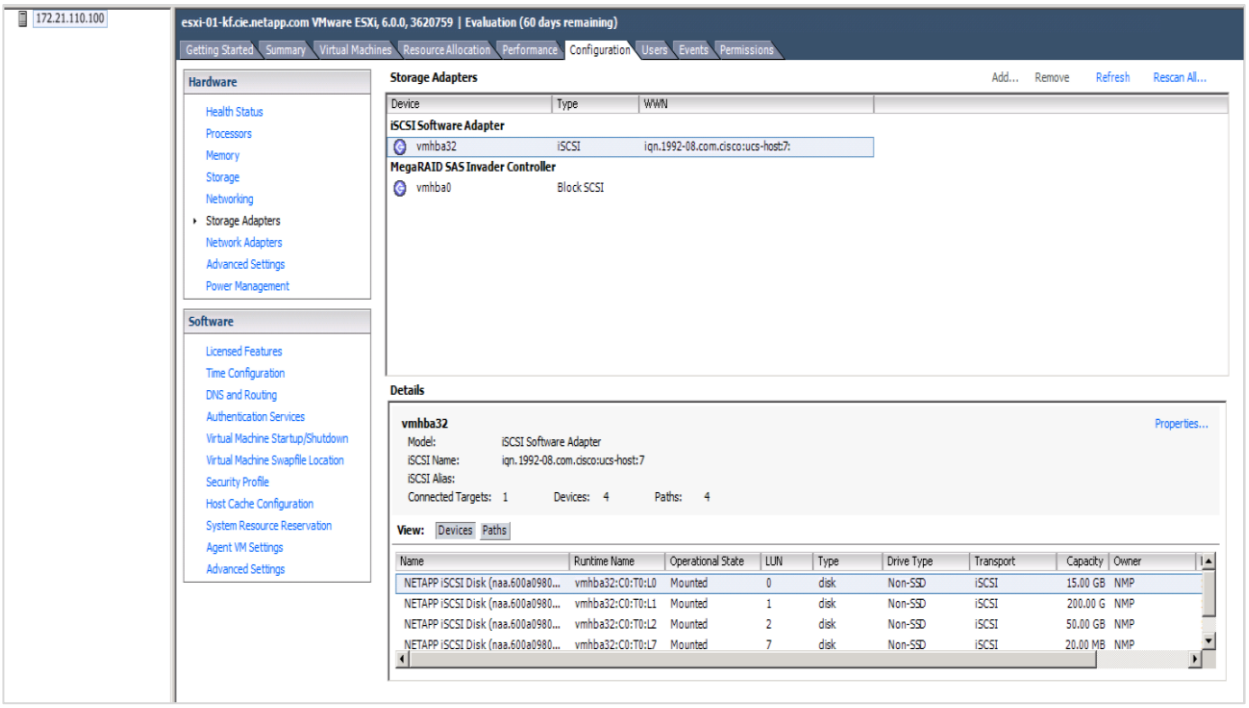
25. Click Next and then Finish to create the vSwitch and VMkernel port.



26. Select Properties to the right of vSwitch1.
27. In the vSwitch1 Properties window, select the vSwitch configuration and click Edit.

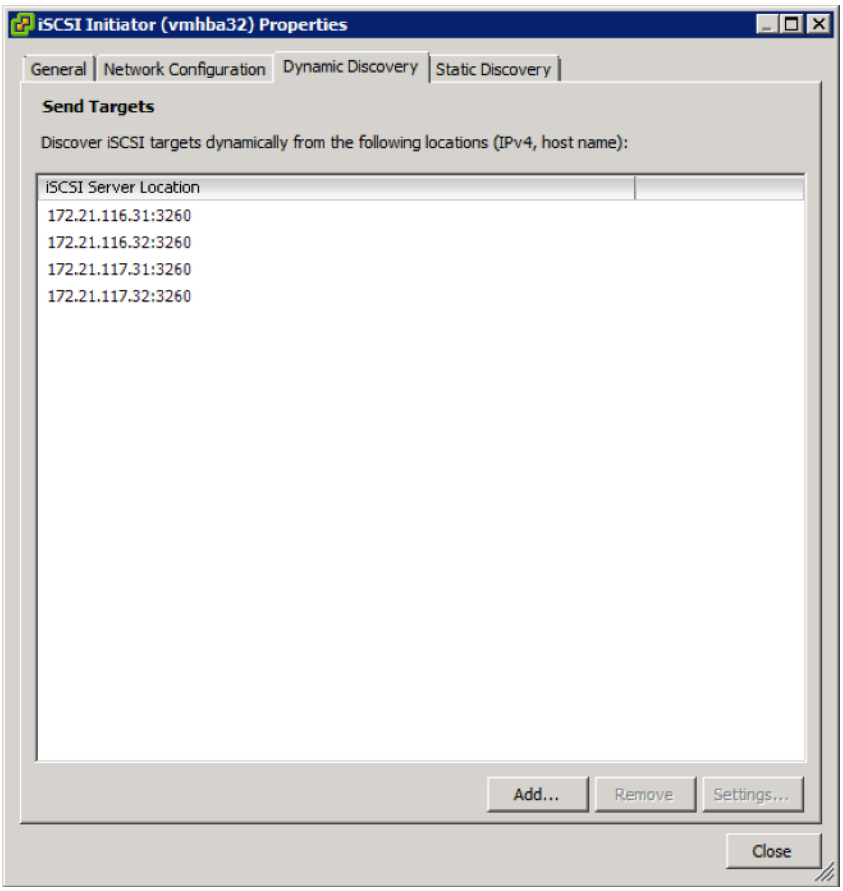


28. Change the MTU to 9000 and click OK.
29. Select the VMkernel-iSCSI-B configuration and click Edit.
30. Change the MTU to 9000 and click OK.
31. Click Close to close the vSwitch1 Properties window.
32. Click Storage Adapters in the Hardware pane.
33. Select the iSCSI software adapter and click Properties.



34. Click the Dynamic Discovery tab.
35. For each storage iSCSI IP address, click Add.
36. Add the iSCSI target IP address. Click OK to add.

Port	IP Address
Port 0A	<<var_controller_A_iSCSI_A_IP>>
	<<var_controller_B_iSCSI_A_IP>>
Port 0B	<<var_controller_A_iSCSI_B_IP>>
	<<var_controller_B_iSCSI_B_IP>>



37. Click Close when complete.
38. Click Yes to rescan the HBA.
39. Repeat steps 1 through 38 for the host `VM-Host-Infra-02`.

Note: If VM-Host-Infra-02 was booted with boot policy iSCSI-B-Primary, then the iScsiBootvSwitch would have been configured on the iSCSI-B network and would host VMkernel-iSCSI-B.

In such case, configure VMkernel-iSCSI-A by obtaining the `VMkernel-iSCSI-A` IP address from the VM-Host-Infra-02 service profile.

Install VMware Drivers for the Cisco VIC

To install VMware VIC drivers on the ESXi hosts VM-Host-Infra-01 and VM-Host-Infra-02, complete the following steps:

Download and extract the following VMware VIC driver to the management workstation: VMware ESXi 6.0 enic 2.3.0.10 NIC Driver for Cisco.

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 the saved location for the downloaded VIC driver and select `ESXi6.0_enic-2.3.0.10-offline_bundle-4303638.zip`.

6. Click Open and Yes to upload the file to datastore1.
7. Make sure the files have been uploaded to both ESXi hosts.
8. From the management workstation, open the VMware vSphere remote CLI that was previously installed.
9. 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>> --thumbprint <host_thumbprint>
software vib update -d /vmfs/volumes/datastore1/ESXi6.0_enic-2.3.0.10-offline_bundle-4303638.zip

esxcli –s <<var_vm_host_infra_02_ip>> -u root –p <<var_password>> --thumbprint
<host_thumbprint>software vib update -d /vmfs/volumes/datastore1/ESXi6.0_enic-2.3.0.10-
offline_bundle-4303638.zip
```

Note: To get the host thumbprint, enter the command without the `--thumbprint` option, then copy and paste the thumbprint into the command.

10. Back in the vSphere Client for each host, right-click the host and select Reboot.
11. Click Yes and OK to reboot the host.
12. Log back in to each host with vSphere Client.

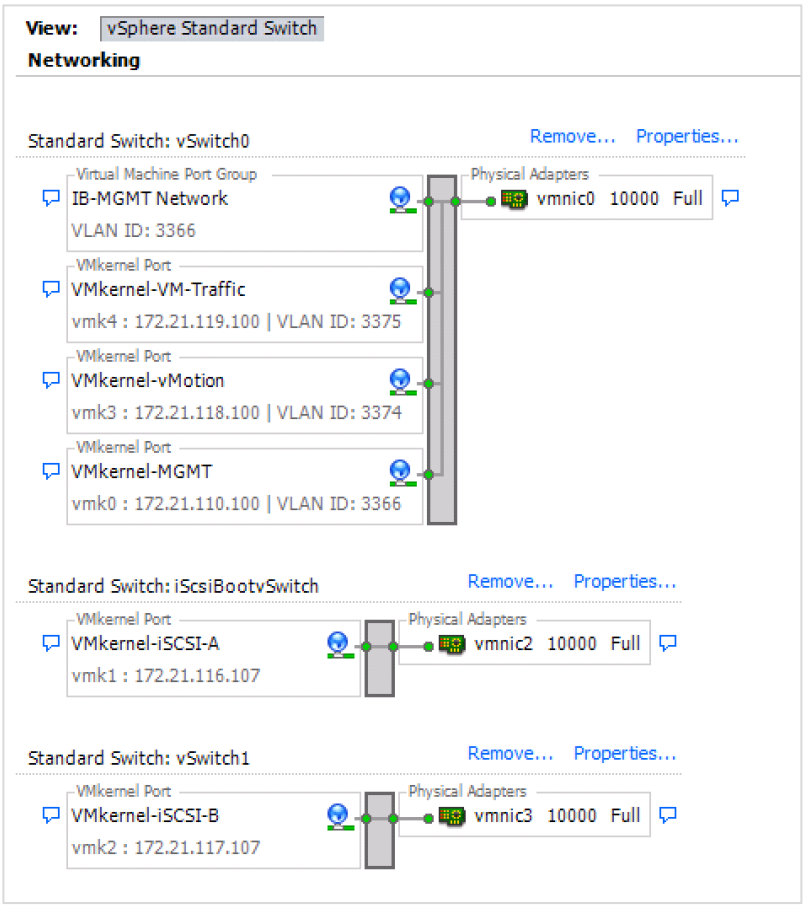
Set Up VMkernel Ports and Virtual Switch

ESXi Host VM-Host-Infra-01

To set up the VMkernel ports and the virtual switches on the VM-Host-Infra-01 ESXi host, 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 to close the properties for vSwitch0.
8. Select the Management Network configuration and click Edit.
9. Change the network label to `VMkernel-MGMT` and select the Management Traffic checkbox.
10. Click OK to finalize the edits for VMkernel-MGMT.
11. Select the VM Network configuration and click Edit.
12. Change the network label to `IB-MGMT Network` and enter `<<var_ib-mgmt_vlan_id>>` in the VLAN ID (Optional) field.
13. Click OK to finalize the edits for IB-MGMT Network.
14. Click Add.
15. Select VMkernel and click Next.
16. Change the network label to `VMkernel-vMotion` and enter `<<var_vmotion_vlan_id>>` in the VLAN ID (Optional) field.
17. Select the checkbox for Use this port group for vMotion.
18. Click Next.
19. Enter the IP address `<<var_vmotion_vlan_ip_host_01>>` and the subnet mask `<<var_vmotion_vlan_ip_mask_host_01>>` for the vMotion VLAN interface for VM-Host-Infra-01.
20. To continue with the vMotion VMkernel creation, click Next.

21. To finalize the creation of the vMotion VMkernel interface, click Finish.
22. Select the `VMkernel-vMotion` configuration and click Edit.
23. Change the MTU to 9000.
24. Click OK to finalize the edits for the VMkernel-vMotion network.
25. Click Add.
26. Select VMkernel and click Next.
27. Change the network label to `VMkernel-VM-Traffic` and enter `<<var_vm-traffic_vlan_id>>` in the VLAN ID (Optional) field.
28. Click Next.
29. Enter the IP address `<<var_vmtraffic_vlan_ip_host_01>>` and the subnet mask `<<var_vmtraffic_vlan_ip_mask_host_01>>` for the VM-Traffic VLAN interface for VM-Host-Infra-01.
30. To continue with the VM-Traffic VMkernel creation, click Next.
31. To finalize the creation of the VM-Traffic VMkernel interface, click Finish.
32. Select the `VMkernel-VM-Traffic` configuration and click Edit.
33. Change the MTU to 9000.
34. Click OK to finalize the edits for the VMkernel-VM-Traffic network.
35. To finalize the ESXi host networking setup, close the dialog box. The networking for the ESXi host should be like the following example.

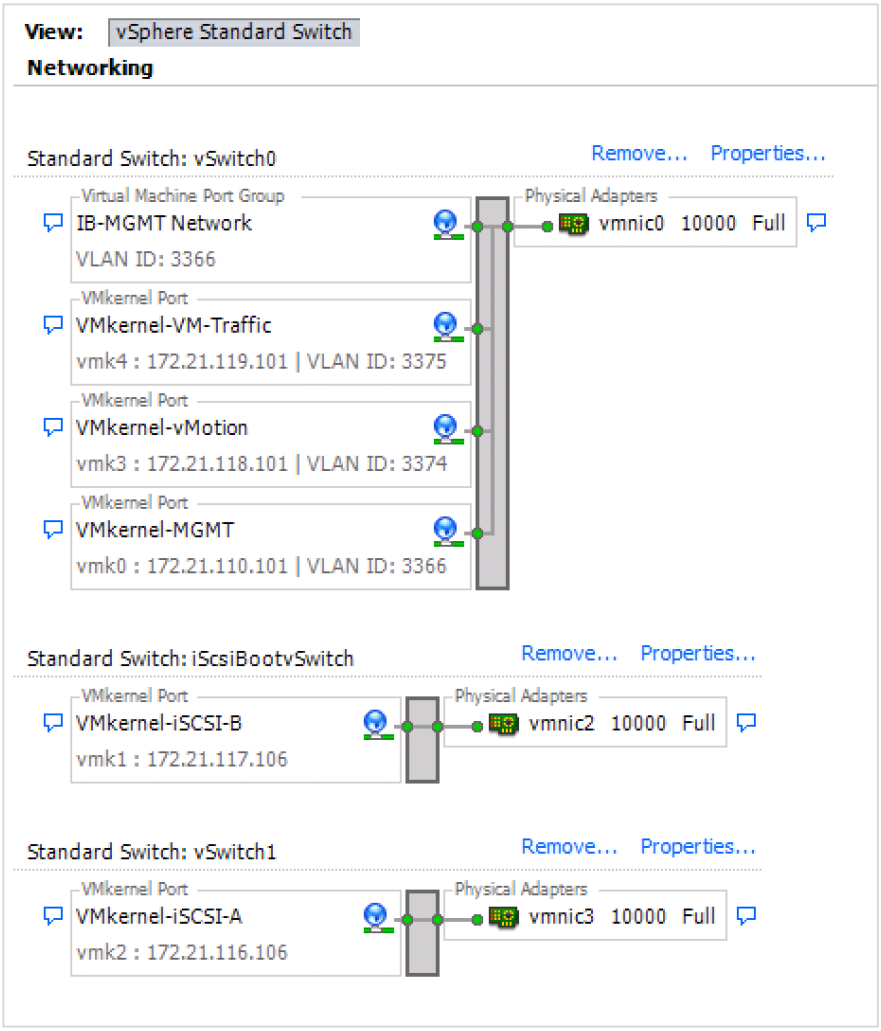


ESXi Host VM-Host-Infra-02

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

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 to close the properties for vSwitch0.
8. Select the Management Network configuration and click Edit.
9. Change the network label to `VMkernel-MGMT` and select the Management Traffic checkbox.
10. Click OK to finalize the edits for VMkernel-MGMT.
11. Select the VM Network configuration and click Edit.
12. Change the network label to `IB-MGMT Network` and enter `<<var_ib-mgmt_vlan_id>>` in the VLAN ID (Optional) field.
13. Click OK to finalize the edits for IB-MGMT network.
14. Click Add.
15. Select VMkernel and click Next.
16. Change the network label to `VMkernel-vMotion` and enter `<<var_vmotion_vlan_id>>` in the VLAN ID (Optional) field.
17. Select the checkbox for Use this port group for vMotion.
18. Click Next.
19. Enter the IP address `<<var_vmotion_vlan_ip_host_02>>` and the subnet mask `<<var_vmotion_vlan_ip_mask_host_02>>` for the vMotion VLAN interface for VM-Host-Infra-02.
20. To continue with the vMotion VMkernel creation, click Next.
21. To finalize the creation of the vMotion VMkernel interface, click Finish.
22. Select the `VMkernel-vMotion` configuration and click Edit.
23. Change the MTU to 9000.
24. Click OK to finalize the edits for the VMkernel-vMotion network.
25. Click Add.
26. Select VMkernel and click Next.
27. Change the network label to `VMkernel-VM-Traffic` and enter `<<var_vm-traffic_vlan_id>>` in the VLAN ID (Optional) field.
28. Click Next.
29. Enter the IP address `<<var_vmtraffic_vlan_ip_host_02>>` and the subnet mask `<<var_vmtraffic_vlan_ip_mask_host_02>>` for the VM-Traffic VLAN interface for VM-Host-Infra-02.
30. To continue with the VM-Traffic VMkernel creation, click Next.
31. To finalize the creation of the VM-Traffic VMkernel interface, click Finish.
32. Select the `VMkernel-VM-Traffic` configuration and click Edit.
33. Change the MTU to 9000.

34. Click OK to finalize the edits for the VMkernel-VM-Traffic network.
35. To finalize the ESXi host networking setup, close the dialog box. The networking for the ESXi host should be like the following example.

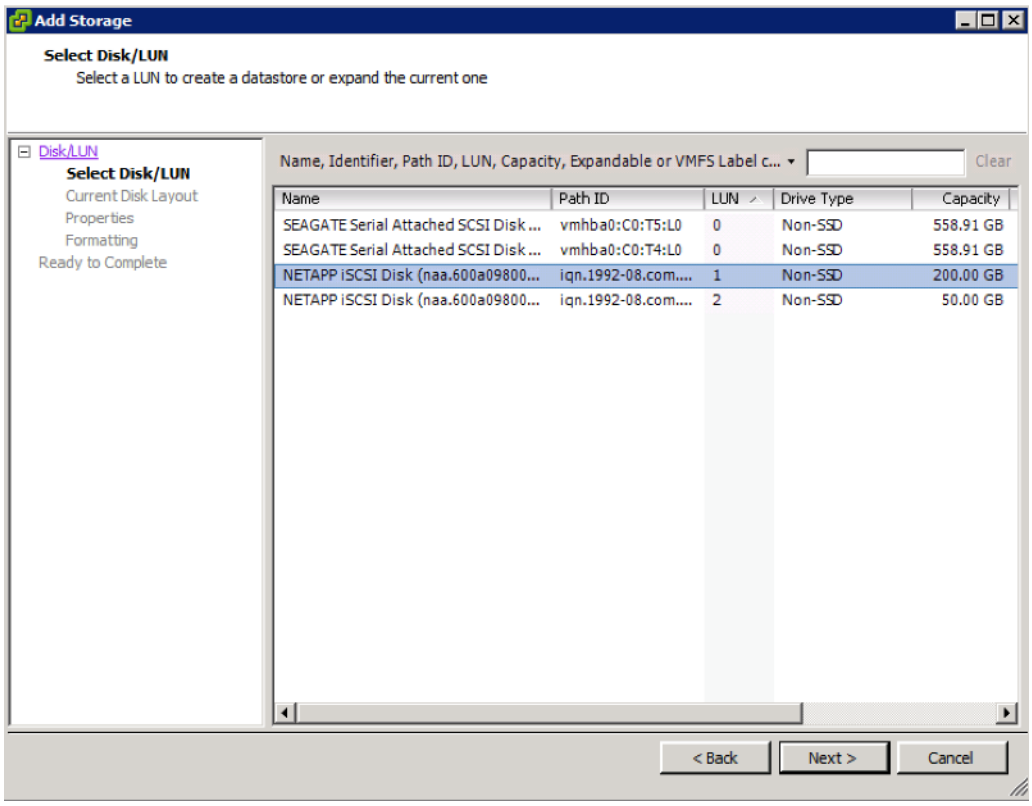


Mount Required Datastores

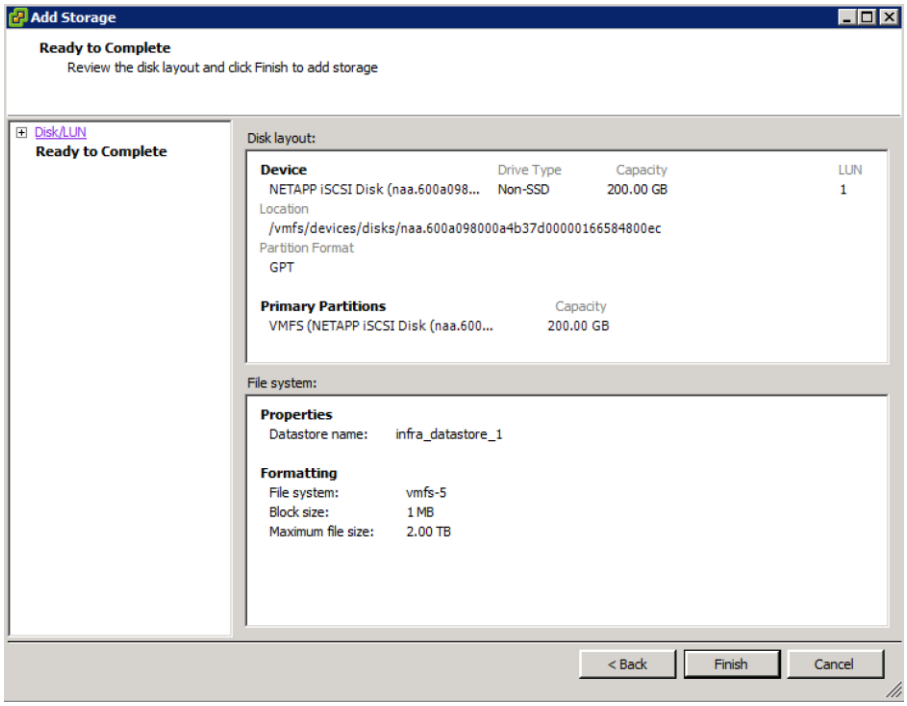
ESXi Host VM-Host-Infra-01

To mount the required datastores, complete the following steps on each ESXi host:

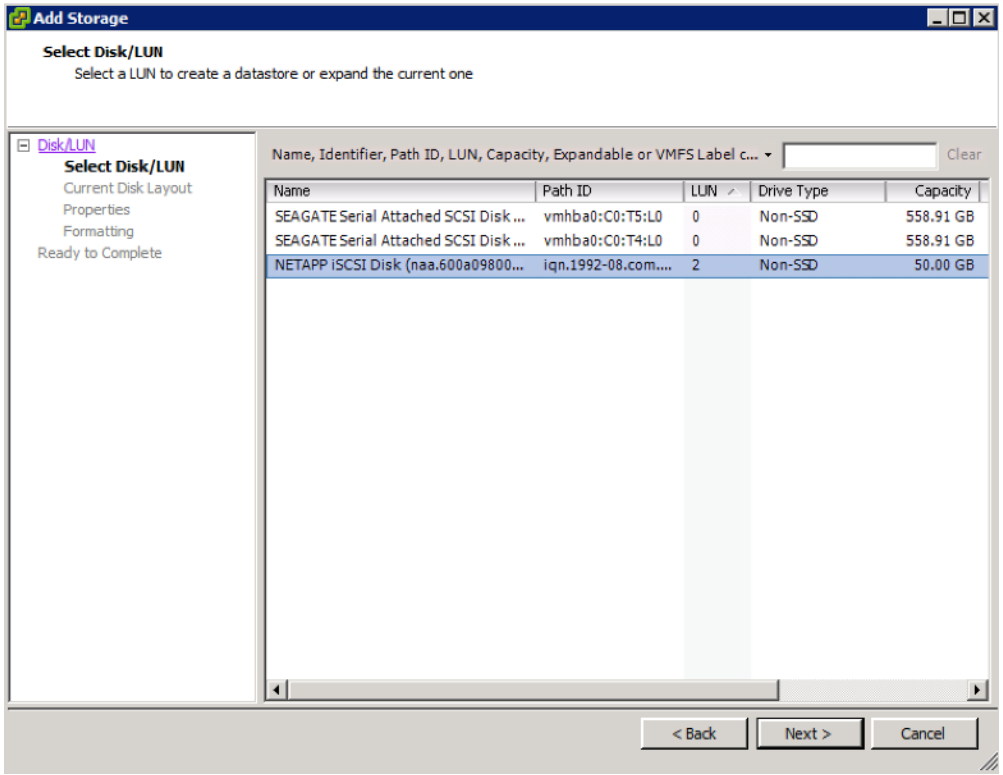
1. From the vSphere Client, select the host in the inventory.
2. Click the Configuration tab.
3. Click Storage in the Hardware pane.
4. From the Datastores area, click Add Storage to open the Add Storage wizard.
5. Select Disk/LUN and click Next.



6. Choose the 200GB LUN and click Next.
7. Review the disk layout and click Next to continue.
8. Enter `infra_datastore_1` as the datastore name.
9. Click Next to continue with the iSCSI datastore creation.
10. Choose the maximum available space and click Next.

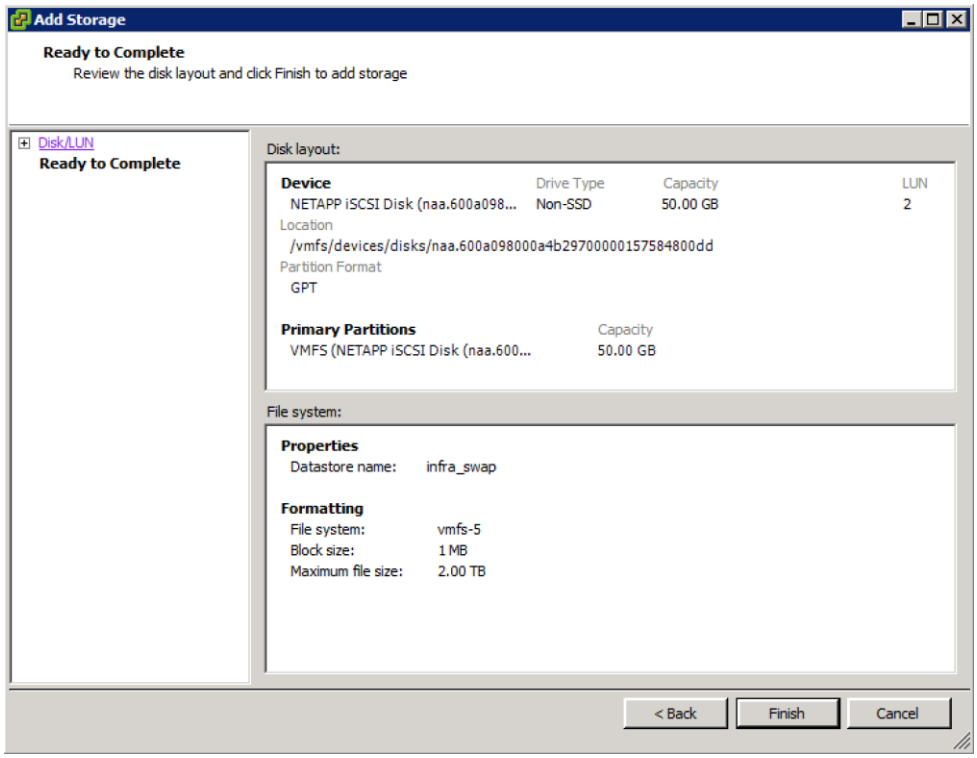


11. Click Finish to create the datastore.
12. From the Datastores area, click Add Storage to open the Add Storage wizard.
13. Select Disk/LUN and click Next.

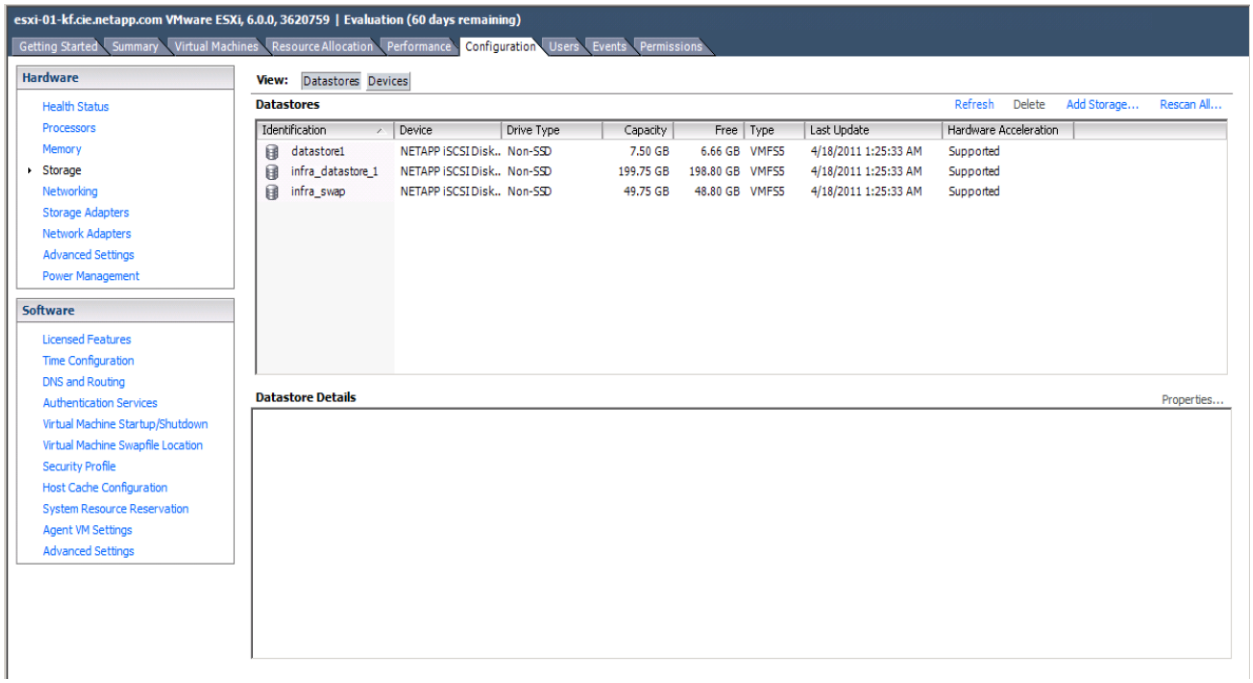


14. Choose the 50GB LUN and click Next.

15. Review the disk layout and click Next to continue.
16. Enter infra_swap as the datastore name and click Next.
17. Choose maximum available space and click Next to continue.



18. Click Finish to finalize the creation of the iSCSI datastore.



ESXi Host VM-Host-Infra-02

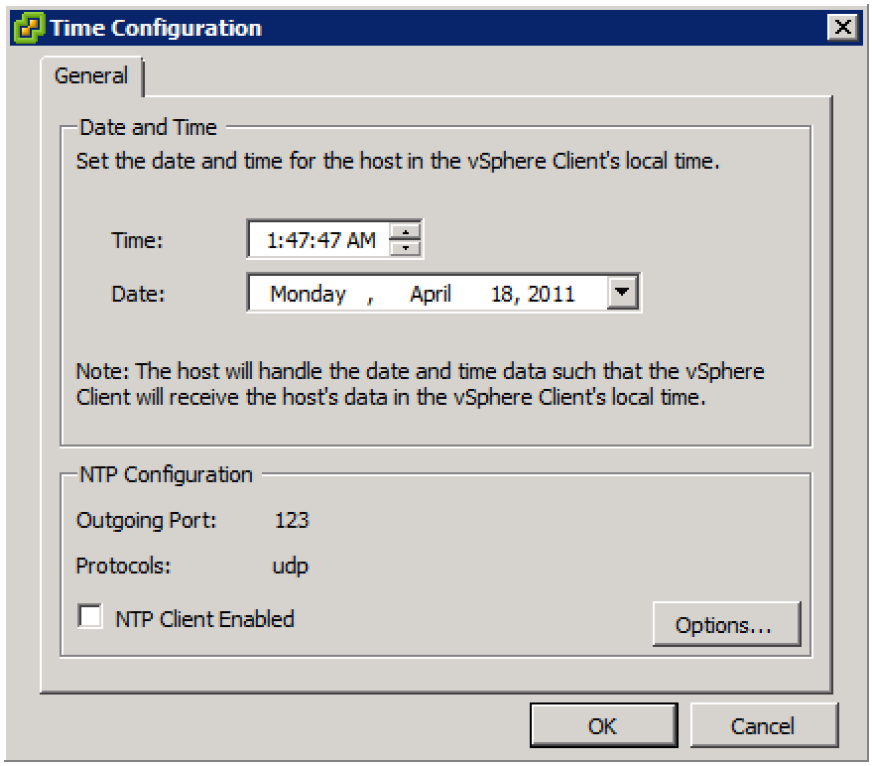
1. From the vSphere Client, select the host in the inventory.
2. Click the Configuration tab.
3. Click Storage in the Hardware pane.
4. Click Rescan All. Click OK.
5. The `infra_datastore_1` and `infra_swap` datastores are mounted automatically.

Configure NTP on ESXi Hosts

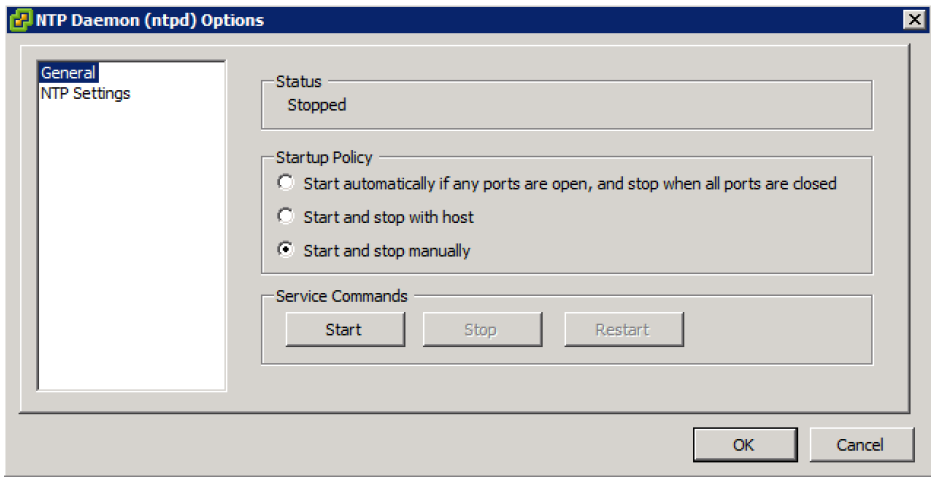
ESXi Hosts VM-Host-Infra-01 and VM-Host-Infra-02

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

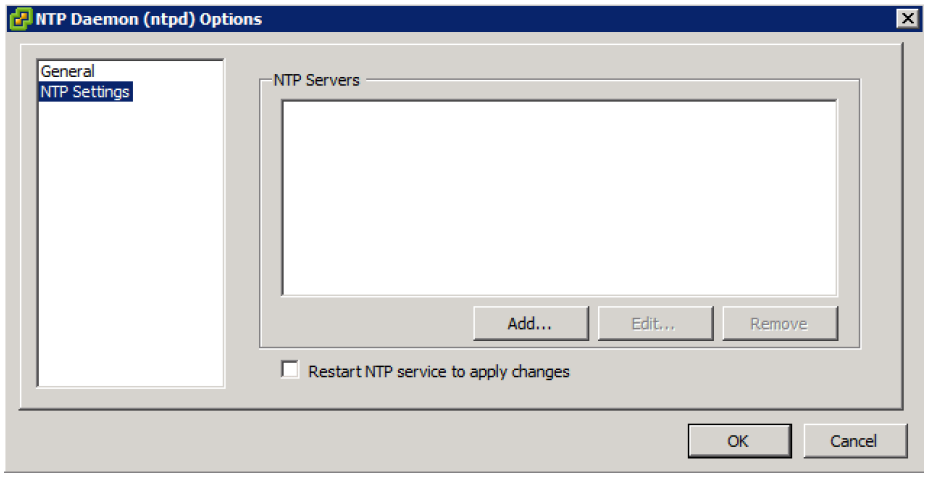
1. From the vSphere Client, select the host in the inventory.
2. Click the Configuration tab to enable configurations.
3. Click Time Configuration in the Software pane.
4. Click Properties at the upper right of the window.



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.



c. In the Add NTP Server dialog box, enter `<<var_ntp_server_primary>>` as the IP address of the primary NTP server and click OK.

d. In the NTP Daemon Options dialog box, select the Restart NTP service to apply changes checkbox and click OK.

7. 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 might vary slightly from the host time.

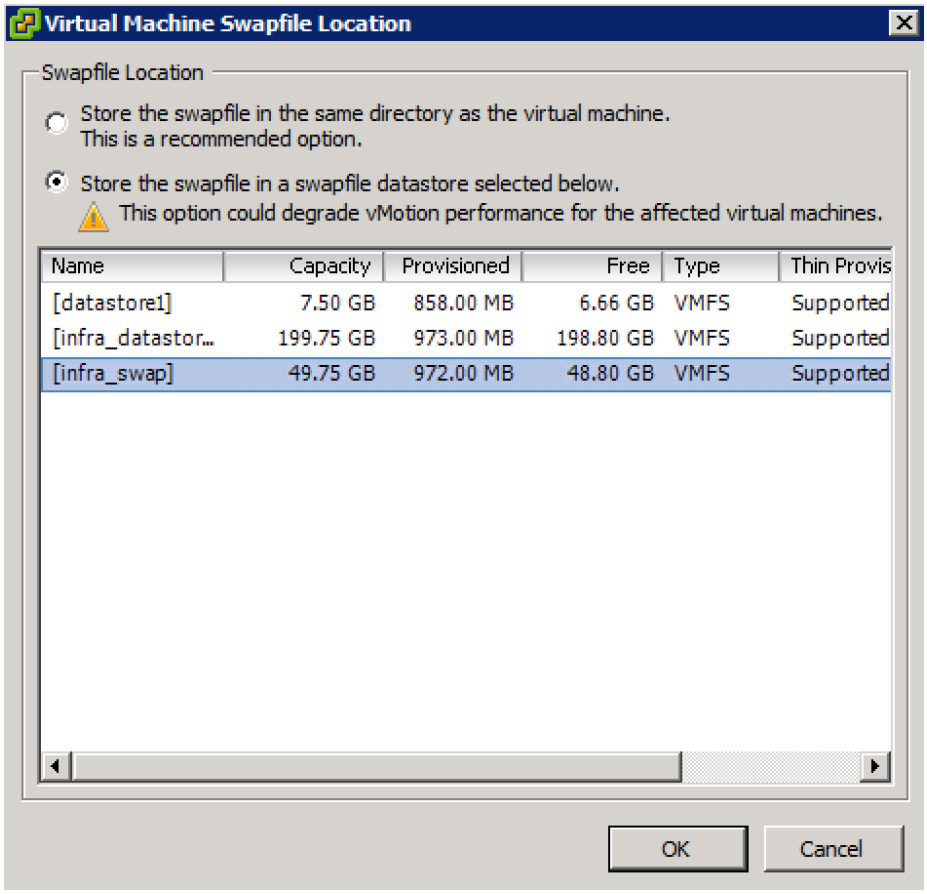
Move VM Swap File Location

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 the vSphere Client, select the host in the inventory.
2. Click the Configuration tab.
3. Click Virtual Machine Swapfile Location in the Software pane.
4. Click Edit at the upper right 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.

FlexPod VMware vCenter 6.0 Update 2

The procedures in the following subsections provide detailed instructions for installing VMware vCenter 6.0U2 in a FlexPod Express environment. After the procedures are completed, a VMware vCenter Server is configured.

Install the Client Integration Plug-In

To install the client integration plug-in, complete the following steps:

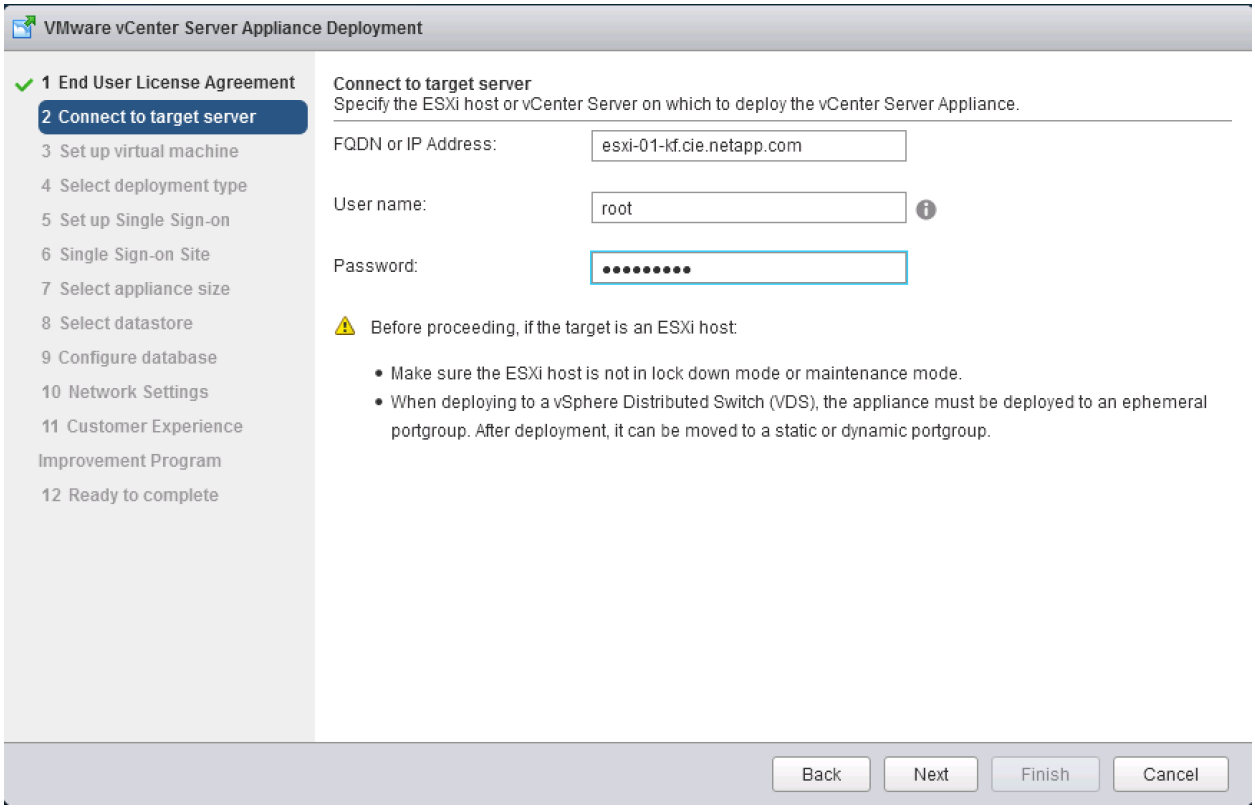
1. Download the .iso installer for the Client Integration Plug-In for vCenter Server Appliance (VCSA).
2. Mount the ISO image to the Windows virtual machine or physical server on which you want to install the Client Integration Plug-In to deploy the VCSA.
3. In the software installer directory, navigate to the `vcsa` directory and double-click VMware-ClientIntegrationPlugin-6.0.0.exe. The Client Integration Plug-In installation wizard appears.
4. On the Welcome page, click Next.
5. Read and accept the terms in the end-user license agreement and click Next.
6. Click Next.
7. Click Install.

8. Click Finish.

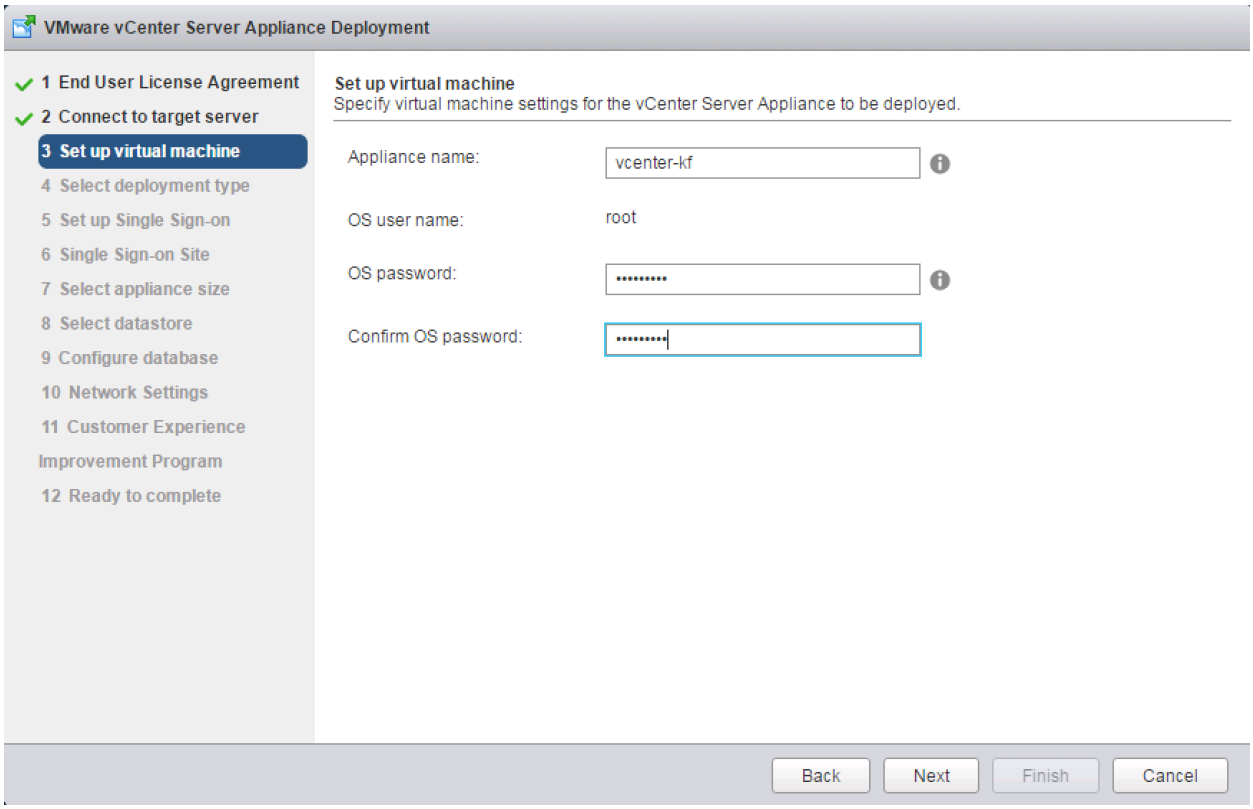
Building the VMware vCenter Server Appliance

To build the VMware vCenter virtual machine, complete the following steps:

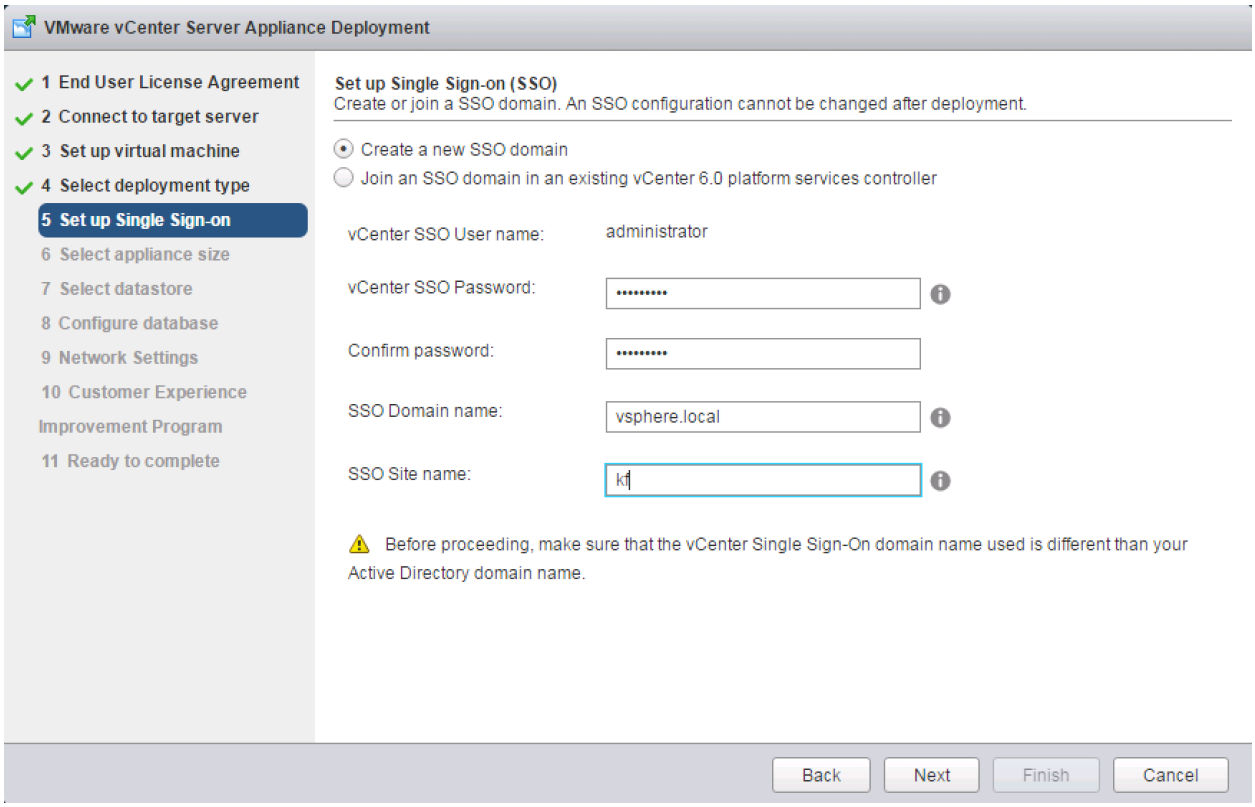
1. In the software installer directory, double-click vcsa-setup.html.
2. Allow the plug-in to run on the browser when prompted.
3. On the Home page, click Install to start the vCenter Server Appliance deployment wizard.
4. Read and accept the license agreement and click Next.
5. In the Connect to target server page, enter the ESXi host name, user name, and password.



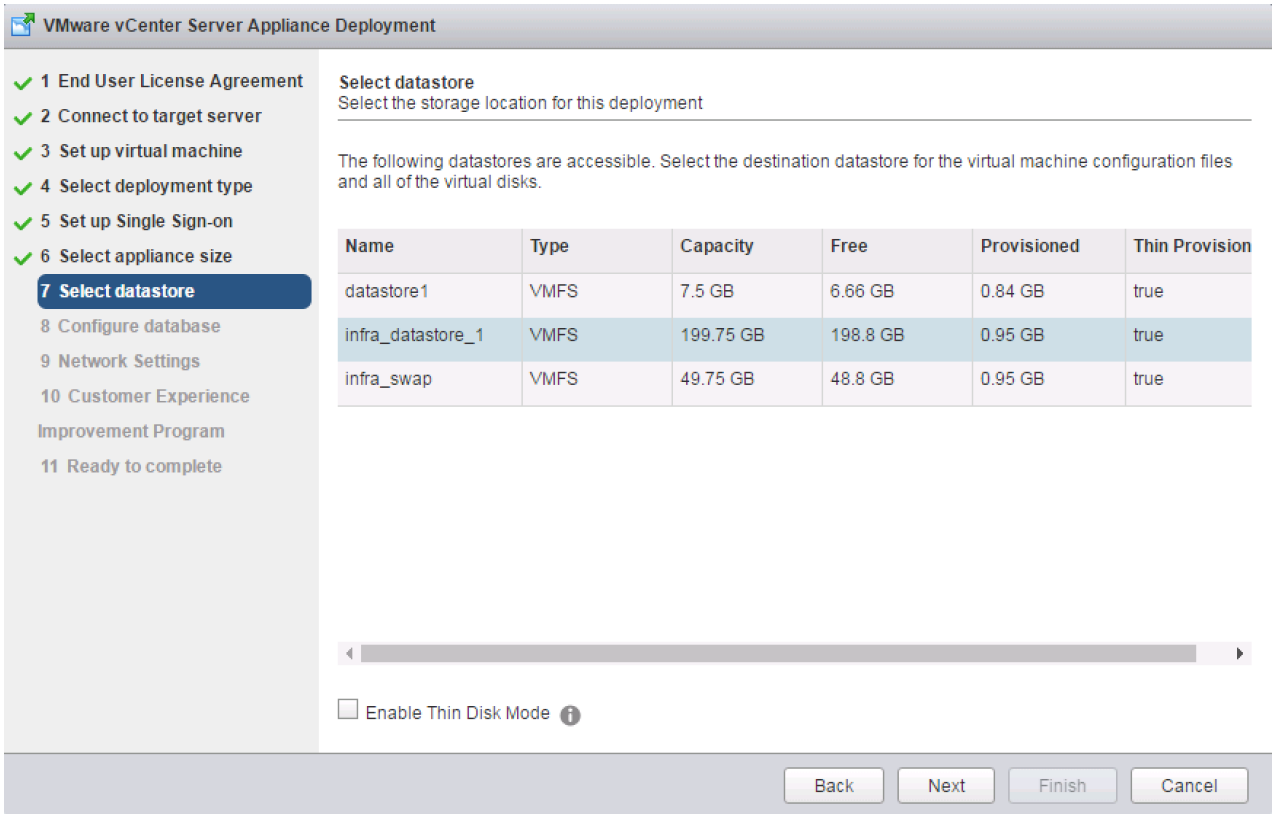
6. Click Yes to accept the certificate.
7. In the Set up virtual machine page, enter the appliance name and password details. Click Next.



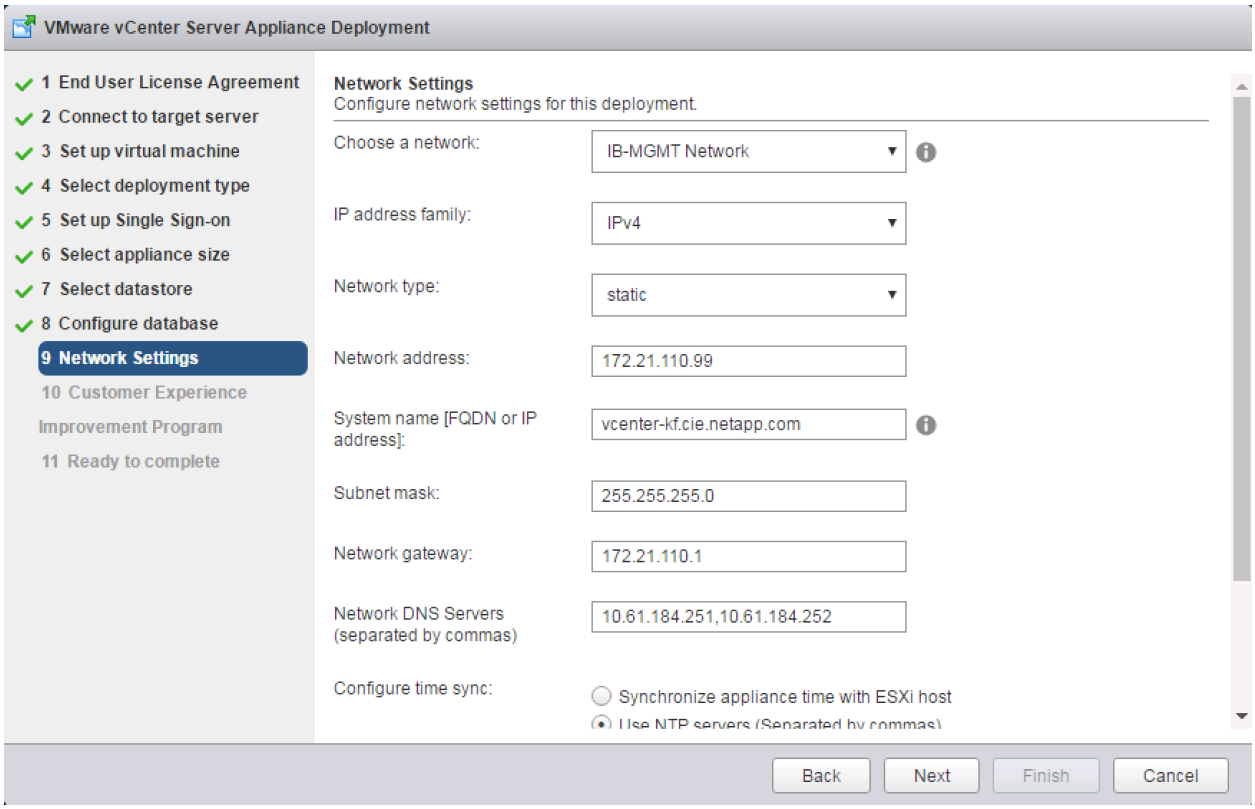
8. In the Select deployment type page, select Install vCenter Server with an embedded Platform Services Controller. Click Next.
9. In the Set up Single Sign-On page, select Create a new SSO domain. Enter the SSO password, domain name, and site name. Click Next.



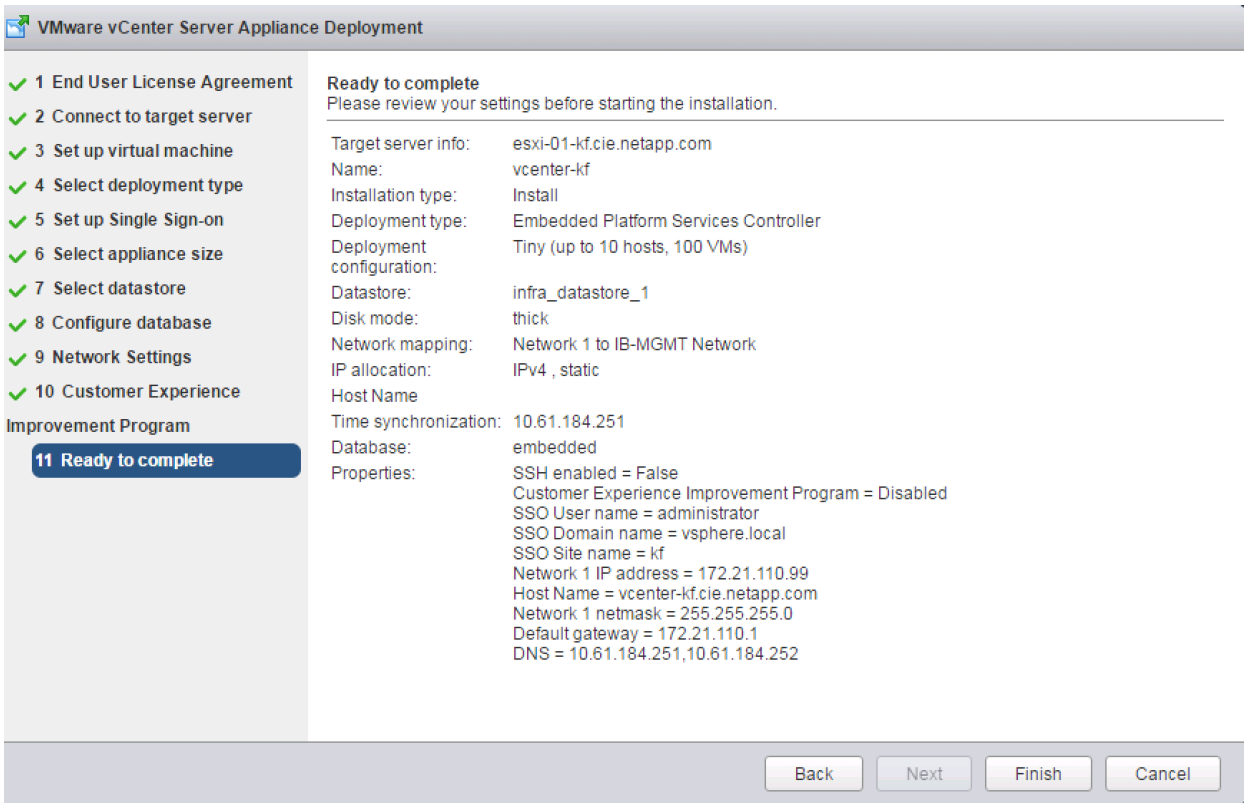
10. In the select appliance size page, set the appliance size: for example, Tiny (up to 10 hosts, 100 VMs). Click Next.
11. In the Select datastore page, choose infra_datastore_1. Click Next.



12. Select embedded database in the Configure database page. Click Next.
13. In the Network Settings page, configure the following settings:
    a. Choose a network: IB-MGMT-Network
    b. IP address family: IPV4
    c. Network type: static
    d. Network address: `<<var_vcenter_ip>>`
    e. System name: `<<var_vcenter_fqdn>>`
    f. Subnet mask: `<<var_vcenter_subnet_mask>>`
    g. Network gateway: `<<var_vcenter_gateway>>`
    h. Network DNS servers: `<<var_dns_server>>`
    i. Configure time sync: Use NTP servers
    j. (Optional). Enable SSH
    k. Click Next.



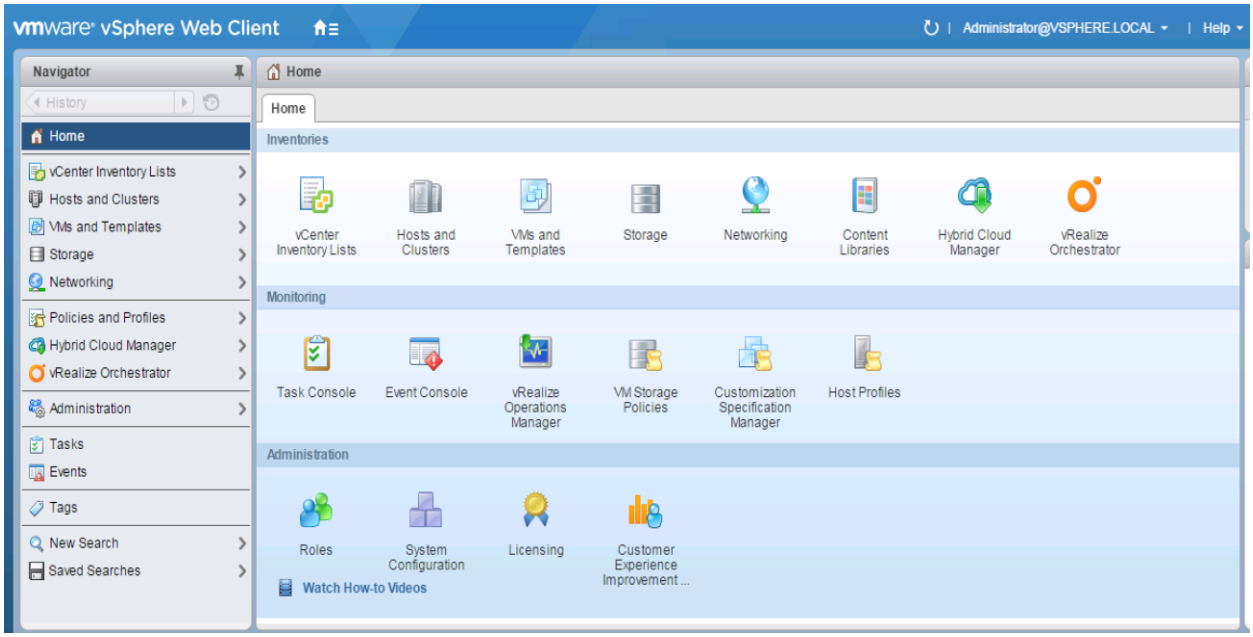
14. Select the checkbox if you want to join the VMware Customer Experience Improvement Program. Click Next.
15. Review the configuration and click Finish.



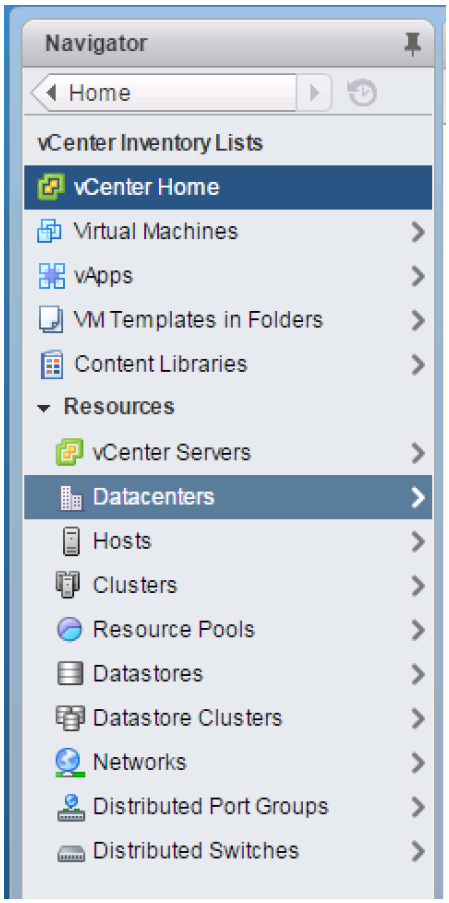
16. The vCenter appliance installation takes a few minutes to complete.
17. Click Close when notified about successful installation.

Setting Up VMware vCenter Server

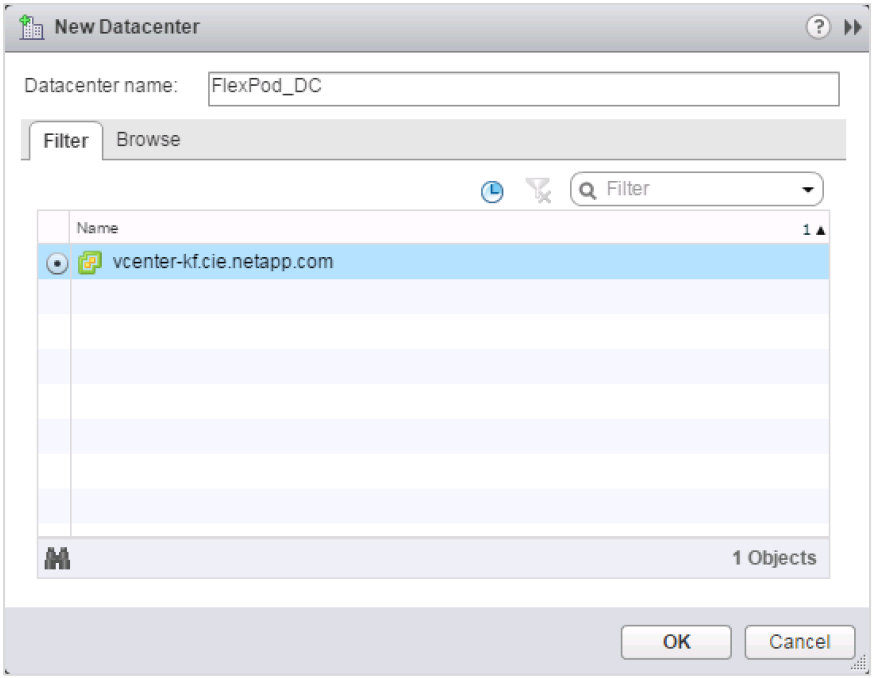
1. Using a web browser, navigate to https://<<var_vcenter_ip>>.
2. Click Log in to vSphere Web Client.
3. Click OK if Launch Application window appears.
4. Log in using Single Sign-On user name and password created during the vCenter installation.



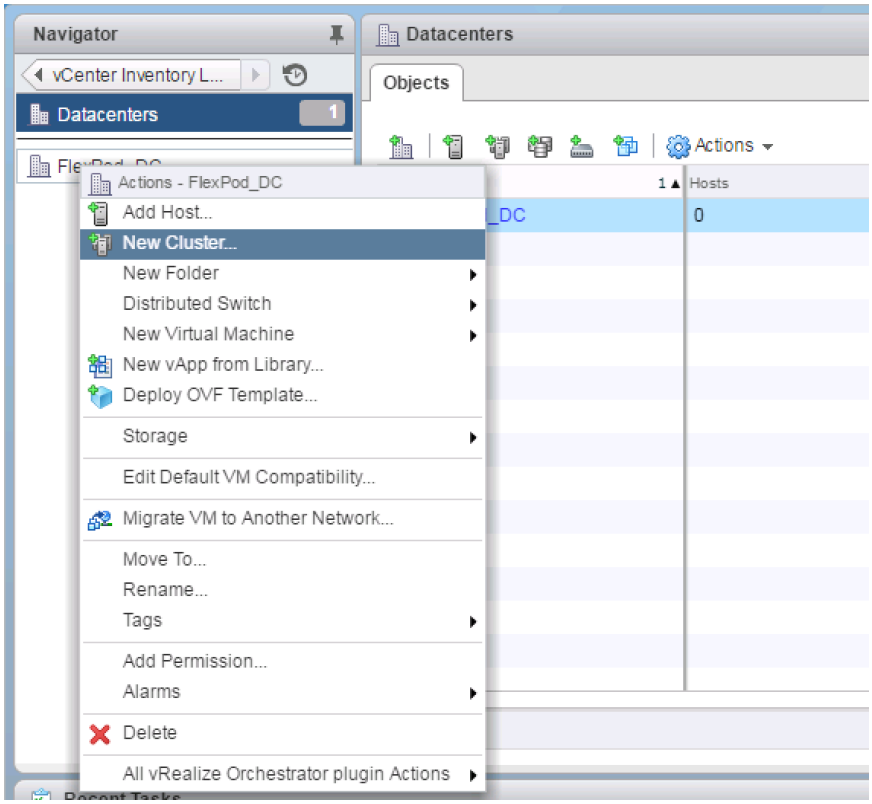
5. Navigate to vCenter Inventory Lists in the left pane.
6. Under Resources, click Datacenters in the left pane.



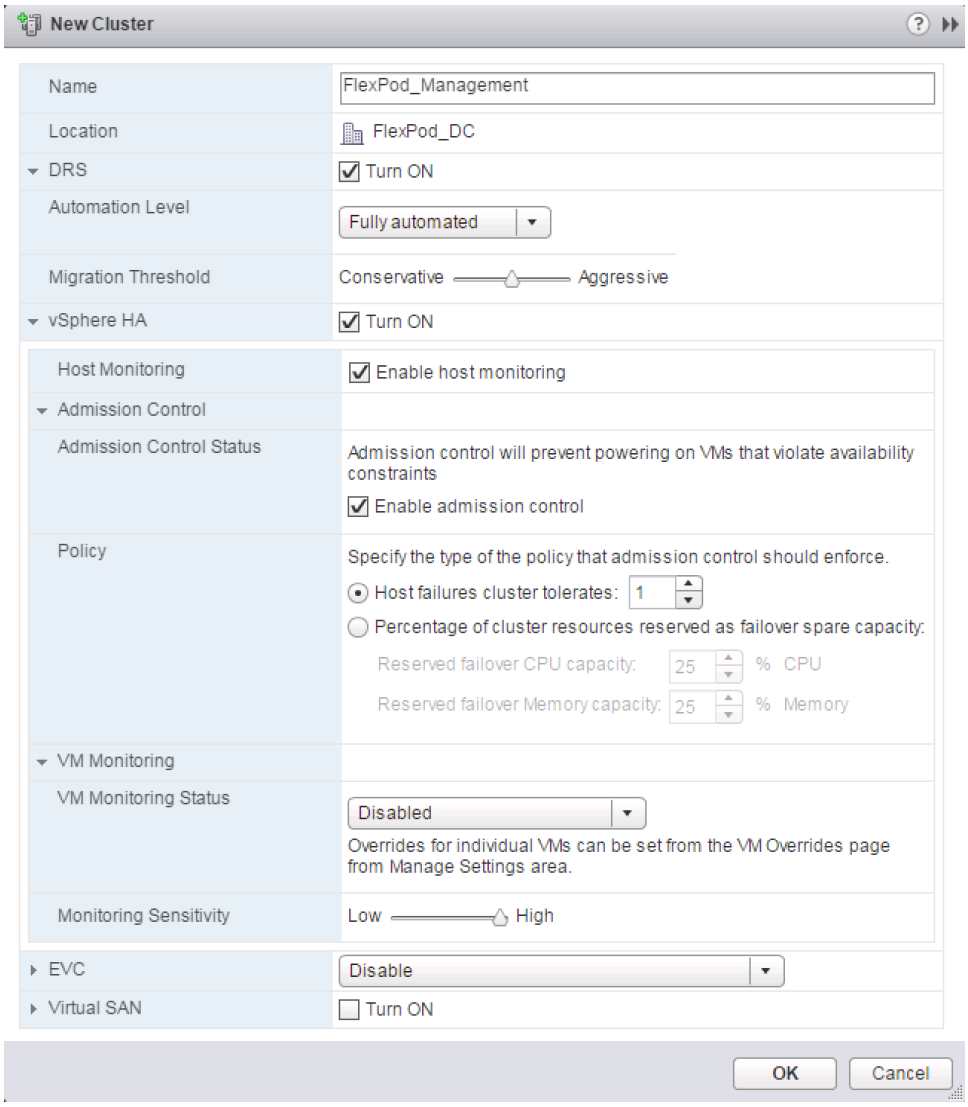
7. To create a data center, click the leftmost icon in the center pane that has a green plus symbol above it.
8. Enter `FlexPod_DC` in the Datacenter name field.
9. Select the vCenter Name/IP option and click OK.



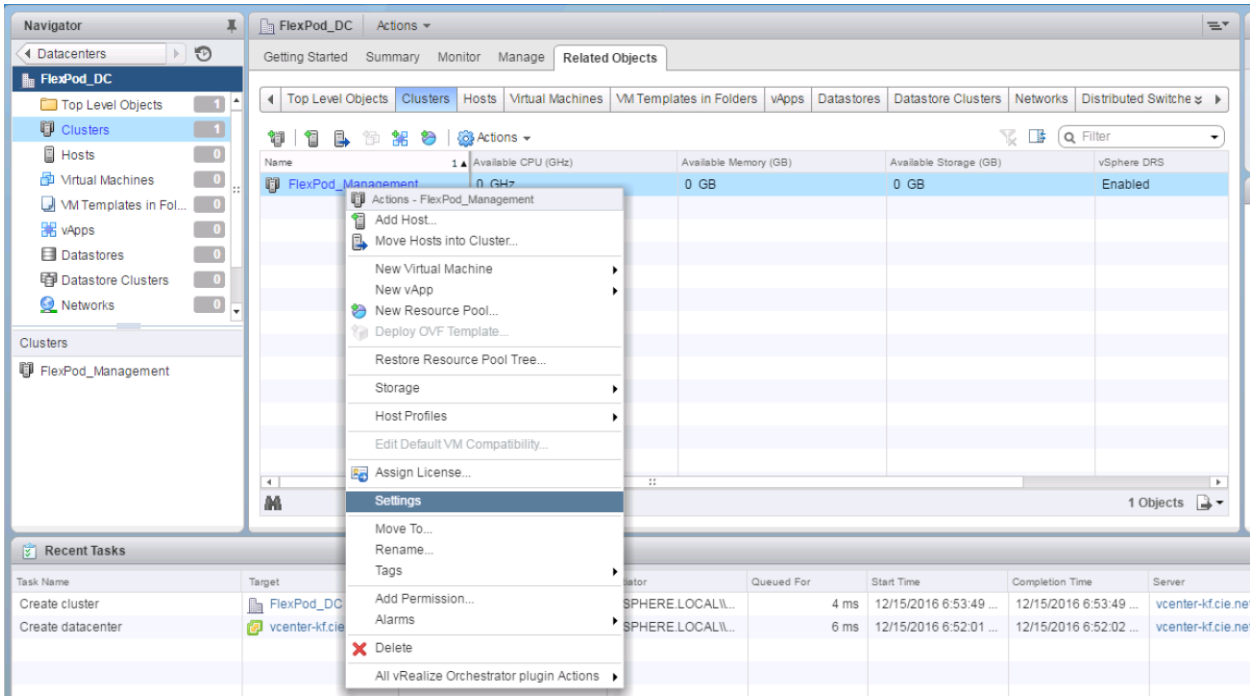
10. Right-click the data center FlexPod_DC in the list in the center pane and select New Cluster.



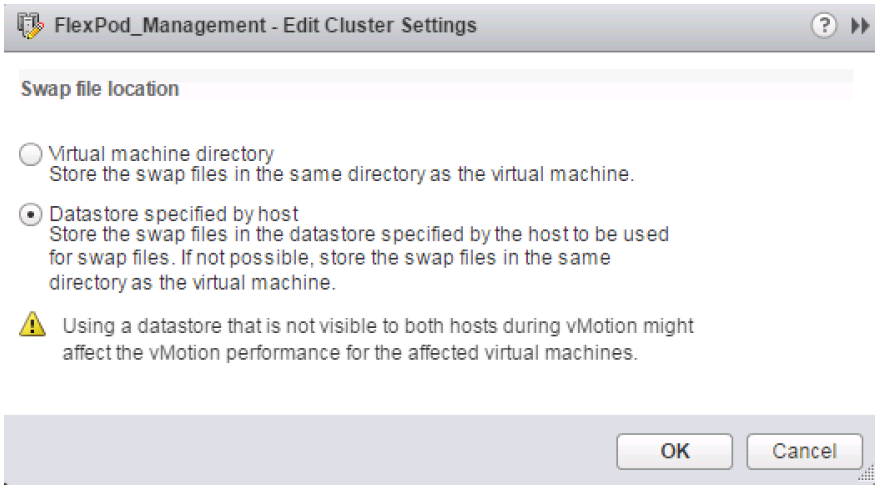
11. Name the cluster FlexPod_Management.
12. Select the DRS checkbox. Retain the default values.
13. Select the vSphere HA checkbox. Retain the default values.



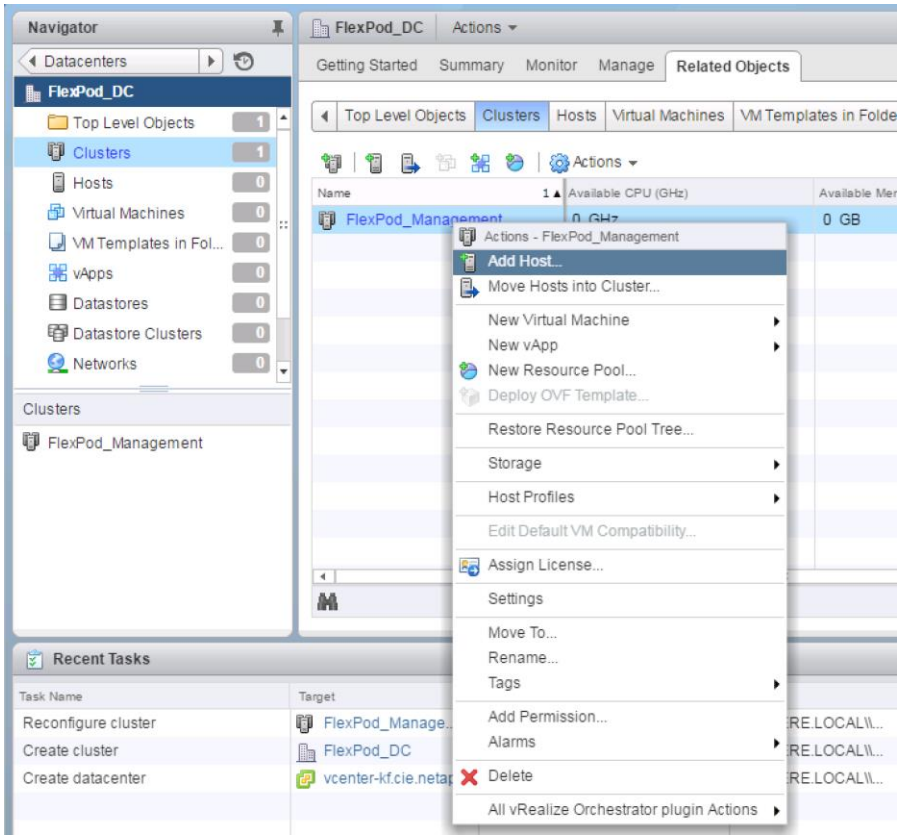
14. Click OK to create the new cluster.
15. In the left pane, double-click the FlexPod_DC.
16. Click Clusters.
17. Click the Related Objects tab in the right pane.
18. Under the Clusters pane, right-click FlexPod_Management and select Settings.



19. Select Configuration > General from the list on the left and select Edit to the right of General.
20. Select Datastore specified by host and click OK.



21. Under the Clusters pane, right-click FlexPod_Management and click Add Host.



22. In the Host field, enter either the IP address or the host name of one of the VMware ESXi hosts. Click Next.
23. Enter root as the user name and the root password. Click Next to continue.
24. Click Yes to accept the certificate.
25. Review the host details and click Next to continue.
26. Assign a license and click Next to continue.
27. Click Next to continue.
28. Click Next to continue.
29. Review the configuration parameters. Then click Finish to add the host.
30. Repeat steps 21 to 30 to add the remaining VMware ESXi hosts to the cluster.

Two VMware ESXi hosts are added to the cluster.

ESXi Dump Collector Setup for iSCSI-Booted Hosts

ESXi hosts booted with iSCSI using the VMware iSCSI software initiator need to be configured to do core dumps to the ESXi Dump Collector that is part of vCenter. The Dump Collector is not enabled by default on the vCenter Appliance. To set up the ESXi Dump Collector, complete the following steps:

1. In the vSphere Client, select Home.
2. In the center pane, click System Configuration.
3. In the left pane, click Services.
4. From the list of services, click VMware vSphere ESXi Dump Collector.
5. From the Actions menu, select Start.

6. From the Actions menu, click Edit Startup Type.
7. Select Automatic.
8. Click OK.
9. On the management workstation, open the VMware vSphere CLI command prompt.
10. Set each iSCSI-booted ESXi host to coredump to the ESXi Dump Collector by running the following commands:

```
esxcli –s <<var_vm_host_infra_01_ip>> -u root –p <<var_password>> --thumbprint <host_thumbprint>
system coredump network set --interface-name vmk0 --server-ipv4 <<var_vcenter_server_ip> --
server-port 6500
```

Note: To get the host thumbprint, enter the command without the `--thumbprint` option, then copy and paste the thumbprint into the command.

```
esxcli –s <<var_vm_host_infra_02_ip>> -u root –p <<var_password>> --thumbprint <host_thumbprint>
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>> --thumbprint <host_thumbprint>
system coredump network set --enable true

esxcli –s <<var_vm_host_infra_02_ip>> -u root –p <<var_password>> --thumbprint <host_thumbprint>
system coredump network set --enable true

esxcli –s <<var_vm_host_infra_01_ip>> -u root –p <<var_password>> --thumbprint <host_thumbprint>
system coredump network check

esxcli –s <<var_vm_host_infra_02_ip>> -u root –p <<var_password>> --thumbprint <host_thumbprint>
system coredump network check
```

Optional: E-Series VMware vCenter Plug-In

The NetApp SANtricity Plug-In for VMware vCenter is a VMware vCenter Server plug-in that provides integrated management of NetApp E-Series and EF-Series storage arrays from within a VMware Web Client session.

This plug-in is only supported on the Windows-based installation of VMware vCenter. It is important to note that this document describes the deployment of the vCenter Appliance and not the Windows variant.

Before you can use the plug-in, the vCenter Server needs to be installed on a Windows operating system.

Appendix: Cisco Nexus 9000 Configuration

The following section provides a detailed procedure for configuring the Cisco Nexus 9000s for use in a FlexPod environment. These steps cover the necessary procedures required to set up a switch from its factory default settings. For greenfield deployments, follow these steps precisely, because failure to do so could result in an improper configuration.

For brownfield deployments, refer to the appropriate sections for guidance on how to configure the necessary network elements.

Physical Connectivity

Follow the physical connectivity guidelines for FlexPod Express as covered in the section “Physical Infrastructure.”

FlexPod Express Cisco Nexus Base

The following procedures describe how to configure the Cisco Nexus switches for use in a base FlexPod Express environment. This procedure assumes the use of Cisco Nexus 9000 7.0(3)I1(1a).

Note: The following procedure includes the setup of NTP distribution on the in-band management VLAN. The `interface-vlan` feature and `ntp` commands are used to set this up. This procedure also assumes the default VRF is used to route the in-band management VLAN.

Set Up Initial Configuration

Cisco Nexus 9372PX A

To set up the initial configuration for the Cisco Nexus A switch on `<<var_nexus_A_hostname>>`, complete the following steps:

1. Configure the switch.

   Note: On initial boot and connection to the serial or console port of the switch, the Cisco NX-OS setup should automatically start and attempt to enter power-on autoprovisioning.

```
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": <<var_password>>
Confirm the password for "admin": <<var_password>>
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]: Enter
Configure read-only SNMP community string (yes/no) [n]: Enter
Configure read-write SNMP community string (yes/no) [n]: Enter
Enter the switch name: <<var_nexus_A_hostname>>
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
Mgmt0 IPv4 address: <<var_nexus_A_mgmt0_ip>>
Mgmt0 IPv4 netmask: <<var_nexus_A_mgmt0_netmask>>
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway: <<var_nexus_A_mgmt0_gw>>
Configure advanced IP options? (yes/no) [n]: Enter
Enable the telnet service? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter

Type of ssh key you would like to generate (dsa/rsa) [rsa]: Enter
Number of rsa key bits <1024-2048> [1024]: Enter
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address: <<var_global_ntp_server_ip>>
Configure default interface layer (L3/L2) [L2]: Enter
Configure default switchport interface state (shut/noshut) [noshut]: shut
Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]: Enter
  Would you like to edit the configuration? (yes/no) [n]: Enter
```

2. Review the configuration summary before enabling the configuration.

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

Cisco Nexus 9372PX B

To set up the initial configuration for the Cisco Nexus B switch on `<<var_nexus_B_hostname>>`, complete the following steps:

1. Configure the switch.

   Note: On initial boot and connection to the serial or console port of the switch, the Cisco NX-OS setup should automatically start and attempt to enter power-on autoprovisioning.

```
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": <<var_password>>
Confirm the password for "admin": <<var_password>>
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]: Enter
Configure read-only SNMP community string (yes/no) [n]: Enter
Configure read-write SNMP community string (yes/no) [n]: Enter
Enter the switch name: <<var_nexus_B_hostname>>
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
```



```
Mgmt0 IPv4 address: <<var_nexus_B_mgmt0_ip>>
Mgmt0 IPv4 netmask: <<var_nexus_B_mgmt0_netmask>>
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway: <<var_nexus_B_mgmt0_gw>>
Configure advanced IP options? (yes/no) [n]: Enter
Enable the telnet service? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter

Type of ssh key you would like to generate (dsa/rsa) [rsa]: Enter
Number of rsa key bits <1024-2048> [1024]: Enter
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address: <<var_global_ntp_server_ip>>
Configure default interface layer (L3/L2) [L2]: Enter
Configure default switchport interface state (shut/noshut) [noshut]: shut
Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]: Enter
Would you like to edit the configuration? (yes/no) [n]: Enter
```

2. Review the configuration summary before enabling the configuration.

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

FlexPod Cisco Nexus Switch Configuration

Enable Licenses

Cisco Nexus 9372PX A and Cisco Nexus 9372PX B

To license the Cisco Nexus switches, complete the following steps:

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

```
config t
feature interface-vlan
feature lacp
feature vpc
feature lldp
```

Set Global Configurations

Cisco Nexus 9372PX A and Cisco Nexus 9372PX B

To set global configurations, complete the following step on both the switches:

1. Run the following commands to set global configurations:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
port-channel load-balance src-dst l4port
ntp server <<var_global_ntp_server_ip>> use-vrf management
ntp master 3
ip route 0.0.0.0/0 <<var_ib-mgmt-vlan_gateway>>
copy run start
```


Create VLANs

Cisco Nexus 9372PX A and Cisco Nexus 9372PX B

To create the necessary VLANs, complete the following step on both the switches:

1. From the global configuration mode, run the following commands:

```
vlan <<var_ib-mgmt_vlan_id>>
name IB-MGMT-VLAN
exit
vlan <<var_native_vlan_id>>
name Native-VLAN
exit
vlan <<var_vmotion_vlan_id>>
name vMotion-VLAN
exit
vlan <<var_vm-traffic_vlan_id>>
name VM-Traffic-VLAN
exit
vlan <<var_iscsi_a_vlan_id>>
name iSCSI-A-VLAN
exit
vlan <<var_iscsi_b_vlan_id>>
name iSCSI-B-VLAN
exit
```

Add NTP Distribution Interface

Cisco Nexus 9372PX A

1. From the global configuration mode, run the following commands:

```
ntp source <<var_switch_a_ntp_ip>>
interface Vlan <<var_ib-mgmt_vlan_id>>
ip address <<var_switch_a_ntp_ip>>/<<var_ib-mgmt_vlan_netmask_length>>
no shutdown
exit
```

Cisco Nexus 9372PX B

1. From the global configuration mode, run the following commands:

```
ntp source <<var_switch_b_ntp_ip>>
interface Vlan <<var_ib-mgmt_vlan_id>>
ip address <<var_switch_b_ntp_ip>>/<<var_ib-mgmt_vlan_netmask_length>>
no shutdown
exit
```

Add Individual Port Descriptions for Troubleshooting

Cisco Nexus 9372PX A

To add individual port descriptions for troubleshooting activity and verification for switch A, complete the following steps:

Note: The following commands are only an example; port numbers and descriptions may vary based on actual connections made in the data center.

1. From the global configuration mode, run the following commands:

```
interface Eth1/1
description <<var_ucs_a>>:Port1
exit
interface Eth1/2
description <<var_ucs_b>>:Port1
```



```
exit
```

2. Similarly, add port descriptions for the remaining connections.

Cisco Nexus 9372PX B

To add individual port descriptions for troubleshooting activity and verification for switch B, complete the following steps:

Note: The following commands are only an example; port numbers and descriptions may vary based on actual connections made in the data center.

1. From the global configuration mode, run the following commands:

```
interface Eth1/1
description <<var_ucs_a>>:Port2
exit
interface Eth1/2
description <<var_ucs_b>>:Port2
exit
```

2. Similarly, add port descriptions for the remaining connections.

Create Port Channels

Cisco Nexus 9372PX A and Cisco Nexus 9372PX B

To create the necessary port channels between devices, complete the following step on both the switches:

Note: The following commands are only an example; port numbers and descriptions may vary based on actual connections made in the data center.

1. From the global configuration mode, run the following commands:

```
interface Po10
description vPC peer-link
exit
interface Eth1/47-48
channel-group 10 mode active
no shutdown
exit

interface Po13
description <<var_ucs_clustername>>-a
exit
interface Eth1/1
channel-group 13 mode active
no shutdown
exit

interface Po14
description <<var_ucs_clustername>>-b
exit
interface Eth1/2
channel-group 14 mode active
no shutdown
exit
copy run start
```


Configure Port Channel Parameters

Cisco Nexus 9372PX A and Cisco Nexus 9372PX B

To configure port channel parameters, complete the following step on both the switches:

Note: The following commands are only an example; the port channel parameters are configured based on the port channels created previously. Actual configurations may differ in the data center.

1. From the global configuration mode, run the following commands:

```
interface Po10
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_vmotion_vlan_id>>, <<var_vm-
traffic_vlan_id>>, <<var_iscsi_a_vlan_id>>, <<var_iscsi_b_vlan_id>>
spanning-tree port type network
exit

interface Po13
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>,<<var_vmotion_vlan_id>>, <<var_vm-
traffic_vlan_id>>,<<var_iscsi_a_vlan_id>>, <<var_iscsi_b_vlan_id>>
spanning-tree port type edge trunk
mtu 9216
exit

interface Po14
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>,<<var_vmotion_vlan_id>>, <<var_vm-
traffic_vlan_id>>, <<var_iscsi_a_vlan_id>>, <<var_iscsi_b_vlan_id>>
spanning-tree port type edge trunk
mtu 9216
exit

copy run start
```

Configure Virtual Port Channels

Cisco Nexus 9372PX A

To configure virtual port channels (vPCs) for switch A, complete the following step:

1. From the global configuration mode, run the following commands:

```
vpc domain <<var_nexus_vpc_domain_id>>
role priority 10
peer-keepalive destination <<var_nexus_B_mgmt0_ip>> source <<var_nexus_A_mgmt0_ip>>
peer-switch
peer-gateway
auto-recovery
delay restore 150
exit

interface Po10
vpc peer-link
exit

interface Po13
vpc 13
exit

interface Po14
vpc 14
exit
```



```
copy run start
```

Cisco Nexus 9372PX B

To configure vPCs for switch B, complete the following step:

1. From the global configuration mode, run the following commands:

```
vpc domain <<var_nexus_vpc_domain_id>>
role priority 20
peer-keepalive destination <<var_nexus_A_mgmt0_ip>> source <<var_nexus_B_mgmt0_ip>>
peer-switch
peer-gateway
auto-recovery
delay restore 150
exit

interface Po10
vpc peer-link
exit

interface Po13
vpc 13
exit

interface Po14
vpc 14
exit

copy run start
```

Conclusion

FlexPod Express is the optimal shared infrastructure foundation for organizations that want to start out with a right-sized, low-cost solution that can ultimately grow with and adapt to their evolving business requirements. Cisco and NetApp have created a platform that is both flexible and scalable for multiple use cases and applications. One common use case is to deploy VMware vSphere as the virtualization solution, as described in this document.

References

This report references the following documents and resources:

- NetApp E-Series Storage System
  http://www.netapp.com/us/products/storage-systems/e2800/index.aspx
- Cisco UCS Mini
  http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-mini/index.html
- Cisco UCS B200 M4 Blade Server
  http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-b200-m4-blade-server/index.html
- VMware vSphere
  http://www.vmware.com/in/products/vsphere.html

Interoperability Matrixes

- VMware and Cisco UCS
  http://www.vmware.com/resources/compatibility/search.php
- NetApp, Cisco UCS, and VMware
  http://support.netapp.com/matrix

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Trademark Information

NVA-0032-0117