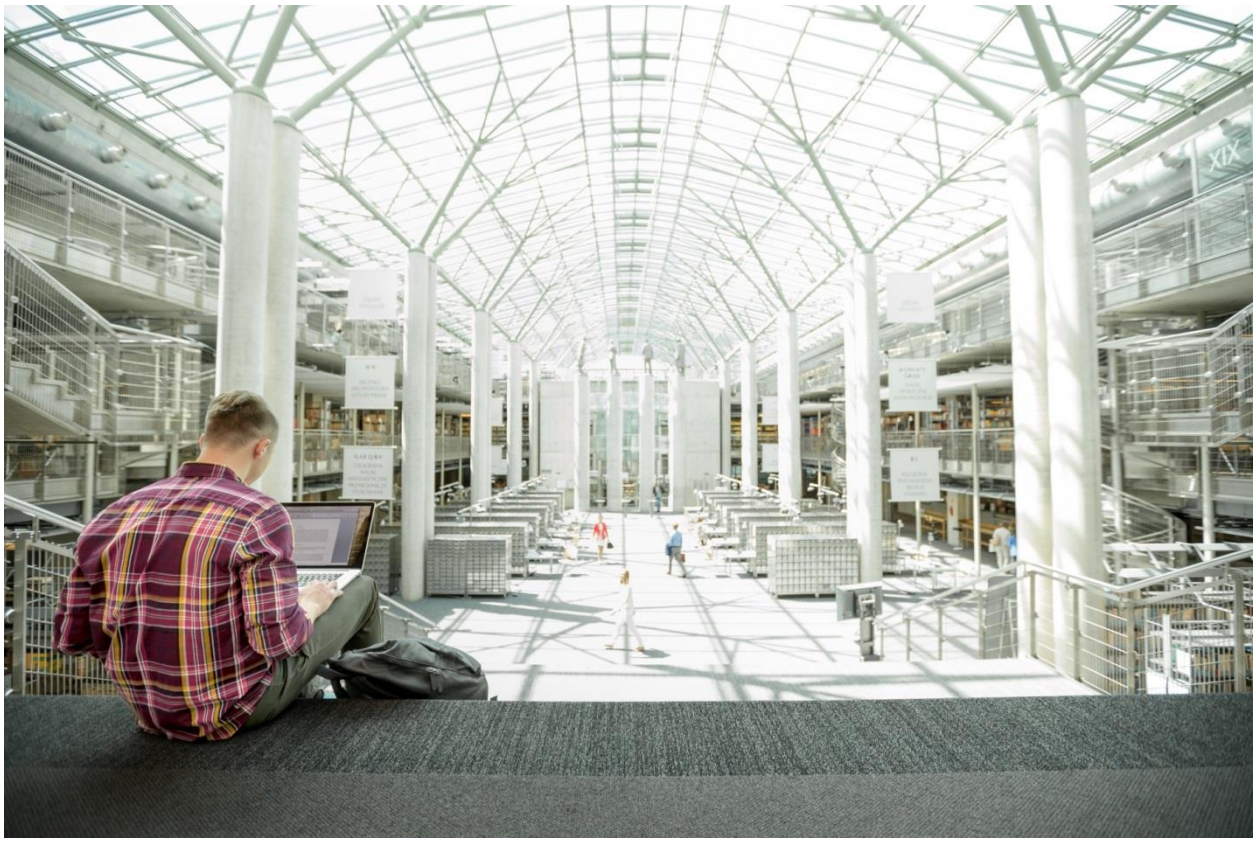


VersaStack with Cisco UCS Mini and IBM Storwize v5000 IP-Based Storage

Deployment Guide for VersaStack using IBM Storwize V5000, Cisco UCS Mini with VMware vSphere 5.5 Update 2 and IP-Based Storage

Last Updated: February 5, 2016

CISCO VALIDATED DESIGN

About Cisco Validated Designs

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

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

Table of Contents

Executive Summary

This deployment guide provides step by step instructions in order to deploy a VersaStack™ system consisting of IBM® V5000 storage and Cisco UCS® Mini infrastructure for a successful VMware deployment using iSCSI SAN for storage connectivity. As an example, this solution could be deployed in a remote branch office location or as a small to midsize solution in the data center. For the VersaStack solution design guidance that best suits your requirements, please refer to the design zone information provided for VersaStack later in this document.

In today's rapid paced IT environment there are many challenges including:

- Increased OPEX. In a recent poll, 73 percent of all IT spending was used just to keep the current data center running
- Rapid storage growth has become more and more difficult to manage and costly
- Existing compute and storage are under utilized
- IT groups are challenged to meet SLA's, dealing with complex troubleshooting
- IT groups are inundated with time consuming data migrations to manage growth and change

In order to solve these issues and increase efficiency, IT departments are moving to converged infrastructure solutions. These solutions offer many benefits, some of them include the integration testing of storage, compute and network completed along with well documented deployment procedures. Converged infrastructure also offers increased feature sets and premium support with Cisco as a single point of contact. Cisco and IBM have teamed up to bring the best network, compute and storage within a single solution named VersaStack. VersaStack offers customers versatility and simplicity, great performance, along with reliability. VersaStack has entry level, midsize, and large enterprise flash solutions to cover multiple data center requirements and assists in reducing the learning curve for administrators. A brief list of the VersaStack benefits that solve the challenges previously noted include:

- Cisco Unified Computing System Manger providing simplified management for compute and network through a consolidated management tool
- Cisco USC Service Profiles designed to vastly reduce deployment time and provide consistency in the data center
- Cisco Fabric Interconnects to reduce infrastructure costs and simplify networking
- IBM Thin-provisioning to reduce the storage footprint and storage costs
- IBM Easy Tier to automate optimizing performance while lowering storage costs by automatically placing infrequently accessed data on less expensive disk, and highly accessed data on faster tiers thereby reducing costly migrations
- IBM V5000 Storwize Simplified Storage Management designed to simplify day-to-day storage tasks

VersaStack offers customers the ability to reduce OPEX while helping administrators meet their SLA’s. This is accomplished by simplifying many of the day-to-day IT tasks, as well as consolidating and automating needs.

VersaStack for Data Center Overview

Introduction

The current data center trend, driven by the need to better utilize available resources, is towards virtualization on shared infrastructure. Higher levels of efficiency can be realized on integrated platforms due to the pooling of compute, network and storage resources, brought together by a pre-validated process. Validation eliminates compatibility issues and presents a platform with reliable features that can be deployed in an agile manner. This industry trend and the validation approach used to cater to it, has resulted in enterprise customers moving away from silo architectures. VersaStack serves as the foundation for a variety of workloads, enabling efficient architectural designs that can be deployed quickly and with confidence.

Audience

This document describes the architecture and deployment procedures of an infrastructure composed of Cisco®, IBM®, and VMware® virtualization that use IBM Storwize V5000 block protocols. The intended audience for this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineering, and customers who want to deploy the core VersaStack architecture with IBM Storwize V5000.

Solution Design

Architecture

The VersaStack architecture is highly modular or "Pod-like". There are sufficient architectural flexibilities and design options to scale as required with investment protection. The platform can be scaled up (adding resources to existing VersaStack units) and/or out (adding more VersaStack units).

Specifically, this VersaStack offering is a defined set of hardware and software that serves as an integrated foundation for both virtualized and non-virtualized solutions. VMware vSphere® built on VersaStack includes IBM Storwize V5000, Cisco networking, the Cisco Unified Computing System™ (Cisco UCS®), and VMware vSphere software in a single package. The design is flexible enough that the networking, computing, and storage can fit in one data center half rack or be deployed according to a customer's data center design. Port density enables the networking components to accommodate multiple configurations.

One benefit of the VersaStack architecture is the ability to meet any customer's capacity or performance needs in a cost effective manner. A storage system capable of serving multiple protocols across a single interface allows for customer choice and investment protection because it is a wire-once architecture.

This architecture references relevant criteria pertaining to resiliency, cost benefit, and ease of deployment of all components including IBM Storwize® V5000 storage.

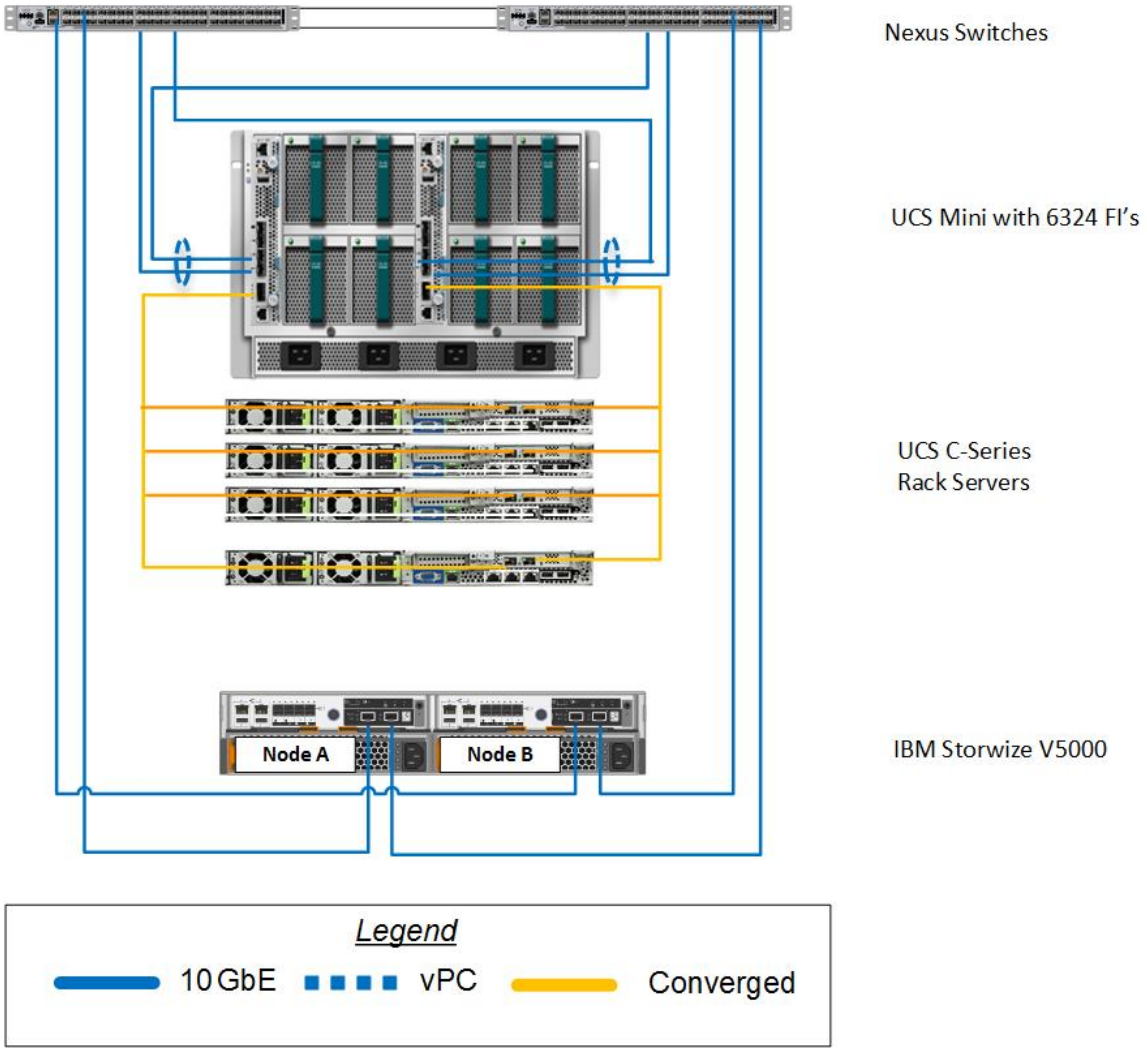
The architecture for this solution shown below uses two sets of hardware resources:

1. Common Infrastructure services on redundant and self-contained hardware
2. VersaStack Pod

The common infrastructure services include Active Directory, DNS, DHCP, vCenter, Nexus 1000v virtual supervisor module (VSM) and any other shared service. These components are considered core infrastructure as they provide necessary data-center wide services where the VersaStack Pod resides. Since these services are integral to the deployment and operation of the platform, there is a need to adhere to best practices in their design and implementation. This includes such features as high-availability, appropriate RAID setup and performance and scalability considerations given such services may need to be extended to multiple Pods. At a customer's site, depending on whether this is a new data center, there may not be a need to build this infrastructure piece.

The figure below illustrates the VMware vSphere built on VersaStack components and the network connections for a configuration with IBM Storwize® V5000 Storage. This design uses the Cisco Nexus® 9372, and Cisco UCS B-Series with the Cisco UCS virtual interface card (VIC) and the IBM Storwize® V5000 storage controllers connected in a highly available design using Cisco Virtual Port Channels (vPCs). This infrastructure is deployed to provide iSCSI-booted hosts with block-level access to shared storage datastores. UCS C-Series rack servers can be used as well.

Figure 1 VersaStack Cabling Overview



The reference hardware configuration includes:

- Two Cisco Nexus 9396 or 9372 switches
- Two Cisco UCS 6324UP Fabric Interconnects
- Support for 4 Cisco UCS C-Series servers without any additional networking components
- Support for 8 Cisco UCS B-Series servers without any additional blade server chassis
- One IBM Storwize V5000 control enclosures and one IBM Storwize V5000 expansion enclosure per control enclosure.
- Support for up to 960 disk capacity attached to two control enclosures and can store up to 1.92 PB per system and 3.84 PB with two-way clustered systems

For server virtualization, the deployment includes VMware vSphere. Although this is the base design, each of the components can be scaled easily to support specific business requirements by duplicating pods. Additional disk shelves can be deployed to improve I/O capability and throughput, and special hardware or software features can be added to introduce new features.

This document guides you through the low-level steps for deploying the base architecture. These procedures cover everything from physical cabling to network, compute and storage device configurations.

For Information regarding the design of VersaStack, please reference the Design guide at:

http://www.cisco.com/c/en/us/solutions/enterprise/data-center-designs-cloud-computing/versastack-designs.html

Software Revisions

The table below details the software revisions used for validating various components of the Cisco Nexus 9000 based VersaStack architecture. To validate your enic version run the "ethtool -i vmnic0" through the command line of the ESX host. For more information regarding supported configurations, please reference the following Interoperability links:

IBM:

http://www-03.ibm.com/systems/support/storage/ssic/interoperability.wss

Cisco:

http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html

Table 1 Hardware/ Software Versions

Layer	Device	Version or Release	Details
Compute	Cisco UCS fabric interconnect	3.0(2d)	Embedded management
	Cisco UCS C 220 M3/M4	3.0(2d)	Software bundle release
	Cisco UCS B 200 M3/ M4	3.0(2d)	Software bundle release
	Cisco eNIC	2.1.2.69	Ethernet driver for Cisco VIC
	Cisco fNIC	1.6.0.16	FCoE driver for Cisco VIC
Network	Cisco Nexus 9372PX	6.1(2)I3(4b)	Operating system version
Storage	IBM Storwize V5000	7.4.0.6	Software version
Software	Cisco UCS hosts	VMware vSphere	Operating system version

		ESXi™ 5.5u2	
	VMware vCenter™	5.5u2	VM (1 each): VMware vCenter
	Cisco Nexus 1000v	5.2(1)SV3(1.4)	Software version
	Virtual Switch Update Manager (VSUM)	1.5	Virtual Switch Deployment Software

Configuration Guidelines

This document provides details on configuring a fully redundant, highly available VersaStack unit with IBM Storwize V5000 storage. Therefore, reference is made at each step to the component being configured as either A or B. For example, Node-A through Node-B are used to identify the IBM storage controllers that are provisioned with this document, and Cisco Nexus A and Cisco Nexus B identify the pair of Cisco Nexus switches that are configured. The Cisco UCS fabric Interconnects are similarly configured. Additionally, this document details the steps for provisioning multiple Cisco UCS hosts, and these are identified sequentially: VM-Host-Infra-01, VM-Host-Infra-02, and so on. Finally, to indicate that you should include information pertinent to your environment in a given step, <text> appears as part of the command structure. See the following example for the network port vlan create command:

Usage:

```
network port vlan create ?

   [-node] <nodename>                    Node

   { [-vlan-name] {<netport>|<ifgrp>}   VLAN Name

   |  -port {<netport>|<ifgrp>}         Associated Network Port

[-vlan-id] <integer> }               Network Switch VLAN Identifier
```

Example:

```
network port vlan –node <node01> -vlan-name i0a-<vlan id
```

This document is intended to enable you to fully configure the VersaStack Pod in the environment. Various steps require you to insert customer-specific naming conventions, IP addresses, and VLAN schemes, as well as to record appropriate MAC addresses.

VLAN Topology

The tables in this section describe the VLANs, example IP ranges, and the virtual machines (VMs) necessary for deployment. The networking architecture can be unique to each environment. Since the design of this deployment is a POD, the architecture in this document leverages private networks and only the in-band management VLAN traffic routes through the Cisco 9k switches. Other management traffic is routed through a separate Out of Band Management switch. The architecture can vary based on the deployment objectives. An NFS VLAN is included in this document to allow connectivity to any existing NFS datastores for migration of virtual machines, if required.

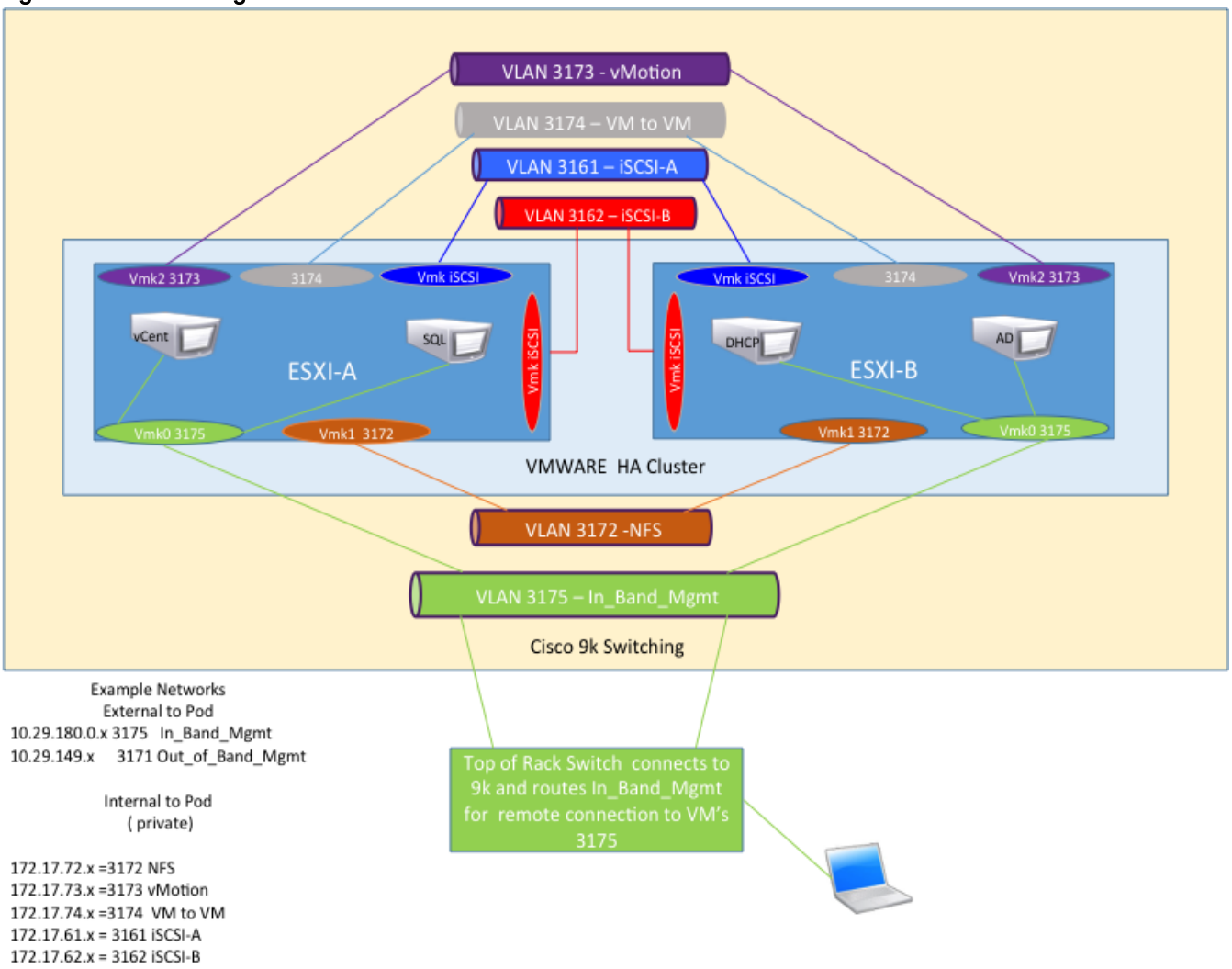
Table 2 VLANS

VLAN Name	VLAN Purpose	ID Used in Validating This Document
Native	VLAN to which untagged frames are assigned	2
Mgmt out of band	VLAN for out-of-band management interfaces	3171
NFS	VLAN for NFS traffic	3172
vMotion	VLAN designated for the movement of VMs from one physical host to another	3173
VM Traffic	VLAN for VM application traffic	3174
Mgmt in band	VLAN for in-band management interfaces	3175
iSCSI-A	VLAN for iSCSI-A	3161
iSCSI-B	VLAN for iSCSI-B	3162

Table 3 Example IP Addresses

VLAN Name	IP addresses range examples	ID Used in Validating This Document
Native	0	2
Mgmt out of band	10.29.149.170 -185 (separate switch outside the 9k)	3171
NFS	172.17.72.10-20 (private, does not route out)	3172
IP-Pool ext-Mgmt (FI KVM IP pool)	10.29.149.186 -225 (separate switch outside the 9k)	3171
vMotion	172.17.73.10-20 (private, does not route out)	3173
VM Traffic	172.17.74.10-20 (private, does not route out)	3174
Mgmt in band	10.29.180.50-100 (routes out through the 9k)	3175
iSCSI-A	172.17.61.10-200 (private, does not route out) 10.29.161.10-200 (IP range used in the document)	3161
iSCSI-B	172.17.62.10-200 (private, does not route out) 10.29.162.10-200 (IP range used in the document)	3162

Figure 2 VLAN Logical View



UCS Central

This document provides the basic installation steps for a single UCS instance. When managing more than a single instance (or domain), it is recommended one deploy UCS Central Software in order to manage across local or globally distributed data centers. Please refer to the UCS Central Software web site to learn more about how UCS Central can assist in more efficiently managing your environment.

Virtual Machines

This document assumes that the following infrastructure machines exist or are created during the installation.

Table 4 Machine List

Virtual Machine Description	Host Name
Active Directory	
vCenter Server (vCSA)	
DHCP Server	

Configuration Variables

Table 5 lists the customer implementation values for the variables which should be identified prior to starting the installation procedure.

Table 5 Customer Variables

Variable	Description	Customer Implementation Value
<<var_node01_mgmt_ip>>	Out-of-band management IP for cluster node 01	
<<var_node01_mgmt_mask>>	Out-of-band management network netmask	
<<var_node01_mgmt_gateway>>	Out-of-band management network default gateway	
<<var_node02_mgmt_ip>>	Out-of-band management IP for cluster node 02	
<<var_node02_mgmt_mask>>	Out-of-band management network netmask	
<<var_node02_mgmt_gateway>>	Out-of-band management network default gateway	
<<var_cluster_mgmt_ip>>	Out-of-band management IP for cluster	
<<var_cluster_mgmt_mask>>	Out-of-band management network netmask	
<<var_cluster_mgmt_gateway>>	Out-of-band management network default gateway	
<<var_password>>	Global default administrative password	
<<var_dns_domain_name>>	DNS domain name	
<<var_nameserver_ip>>	DNS server IP(s)	
<<var_timezone>>	VersaStack time zone (for example, America/New_York)	
<<var_global_ntp_server_ip>>	NTP server IP address	
<<var_email_contact>>	Administrator e-mail address	
<<var_admin_phone>>	Local contact number for support	
<<var_mailhost_ip>>	Mail server host IP	
<<var_country_code>>	Two-letter country code	
<<var_state>>	State or province name	
<<var_city>>	City name	
<<var_org>>	Organization or company name	
<<var_unit>>	Organizational unit name	
<<var_street_address>>,	Street address for support information	
<<var_contact_name>>	Name of contact for support	
<<var_admin>>	Secondary Admin account for	

Variable	Description	Customer Implementation Value
	storage login	
<<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_nfs_vlan_id>>	NFS VLAN ID	
<<var_vmotion_vlan_id>>	VMware vMotion® VLAN ID	
<<var_vm-traffic_vlan_id>>	VM traffic VLAN ID	
<<var_iscsi-a_vlan_id>>	iSCSI-A VLAN ID	
<<var_iscsi-b_vlan_id>>	iSCSI-B VLAN ID	
<<var_nexus_vpc_domain_id>>	Unique Cisco Nexus switch VPC domain 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_cimc_mask>>	Out-of-band management network netmask	
<<var_cimc_gateway>>	Out-of-band management network default gateway	
<<var_vsm_domain_id>>	Unique Cisco Nexus 1000v virtual supervisor module (VSM)	

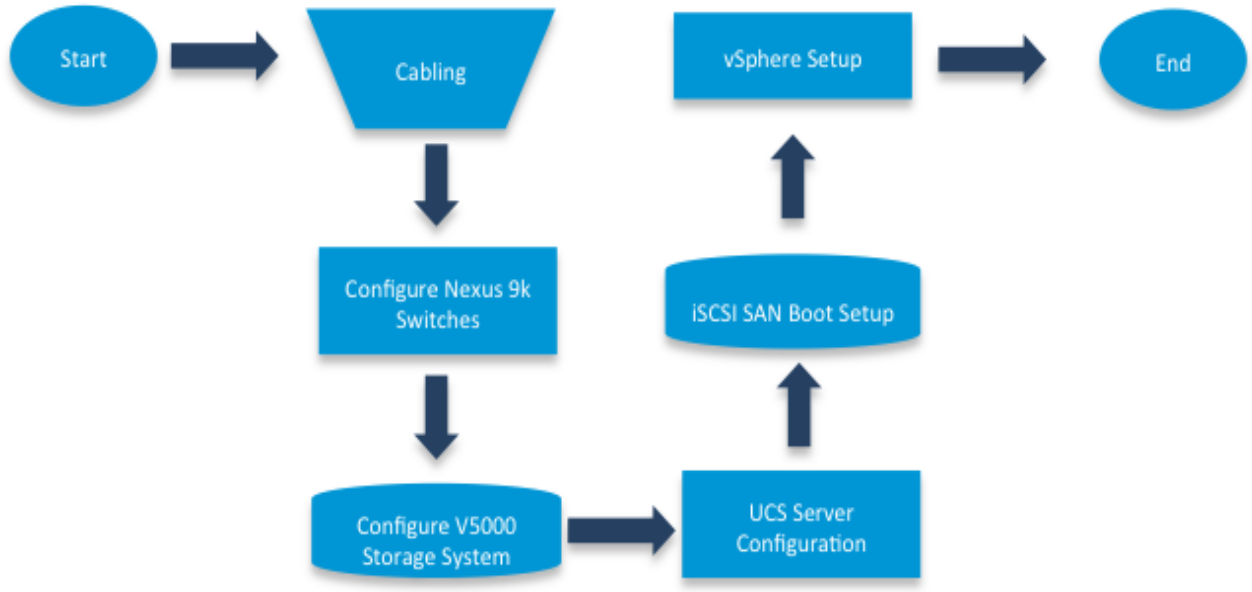
Variable	Description	Customer Implementation Value
	domain ID	
<<var_vsm_mgmt_ip>>	Cisco Nexus 1000v VSM management IP address	
<<var_vsm_updatemgr_mgmt_ip>>	Virtual Switch Update Manager IP address	
<<var_vsm_mgmt_mask>>	In-band management network netmask	
<<var_vsm_mgmt_gateway>>	In-band management network default gateway	
<<var_vsm_hostname>>	Cisco Nexus 1000v VSM host name	
<<var_ftp_server>>	IP address for FTP server	
<<var_node01_iscsi_Eth3_mask>>	Subnet Mask of node 01 iSCSI Eth3	
<<var_node01_iscsi_Eth3_ip>>	IP of node 01 iSCSI Eth3	
<<var_node01_iscsi_Eth4_mask>>	Subnet Mask of node 01 iSCSI Eth4	
<<var_node01_iscsi_Eth4_ip>>	IP of node 01 iSCSI Eth4	
<<var_node02_iscsi_Eth3_mask>>	Subnet Mask of node 02 iSCSI Eth3	
<<var_node02_iscsi_Eth3_ip>>	IP of node 02 iSCSI Eth3	
<<var_node02_iscsi_Eth4_mask>>	Subnet Mask of node 02 iSCSI Eth4	
<<var_node02_iscsi_Eth4_ip>>	IP of node 02 iSCSI Eth4	
<<var_In-band_mgmtblock_net>>	Block of IP addresses for KVM access for UCS	
<<var_vmhost_infra_01_ip>>	VMware ESXi host 01 in-band Mgmt IP	
<<var_vmhost_infra_01_2nd_ip>>	VMware ESXi host 01 secondary in-band Mgmt IP	
<<var_nfs_vlan_id_ip_host-01>>	NFS VLAN IP address for ESXi host 01	
<<var_nfs_vlan_id_mask_host-01>>	NFS VLAN netmask for ESXi host 01	
<<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	

The last 6 variables should be repeated for all ESXi hosts.

VersaStack Cabling

Figure 3 illustrates the VersaStack build process.

Figure 3 VersaStack Build Process



VersaStack Cabling

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

The tables in this section contain details for the prescribed and supported configuration of the IBM Storwize V5000 running 7.4.0.6.

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

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

It is possible to order IBM Storwize V5000 systems in a different configuration from what is presented in the tables in this section. Before starting, be sure that the configuration matches the descriptions in the tables and diagrams in this section.

Figure 4 illustrates the cabling diagrams for VersaStack configurations using the Cisco Nexus 9000 and IBM Storwize V5000. For SAS cabling information, the V5000 control enclosure and expansion enclosure should be connected according to the cabling guide at the following URL:

www.ibm.com/support/knowledgecenter/STHGUJ_7.4.0/com.ibm.storwize.v5000.740.doc/v3500_qisascables_b4jtyu.html?cp=STHGUJ%2F0-3-1-2&lang=en

Figure 4 VersaStack Wiring Diagram

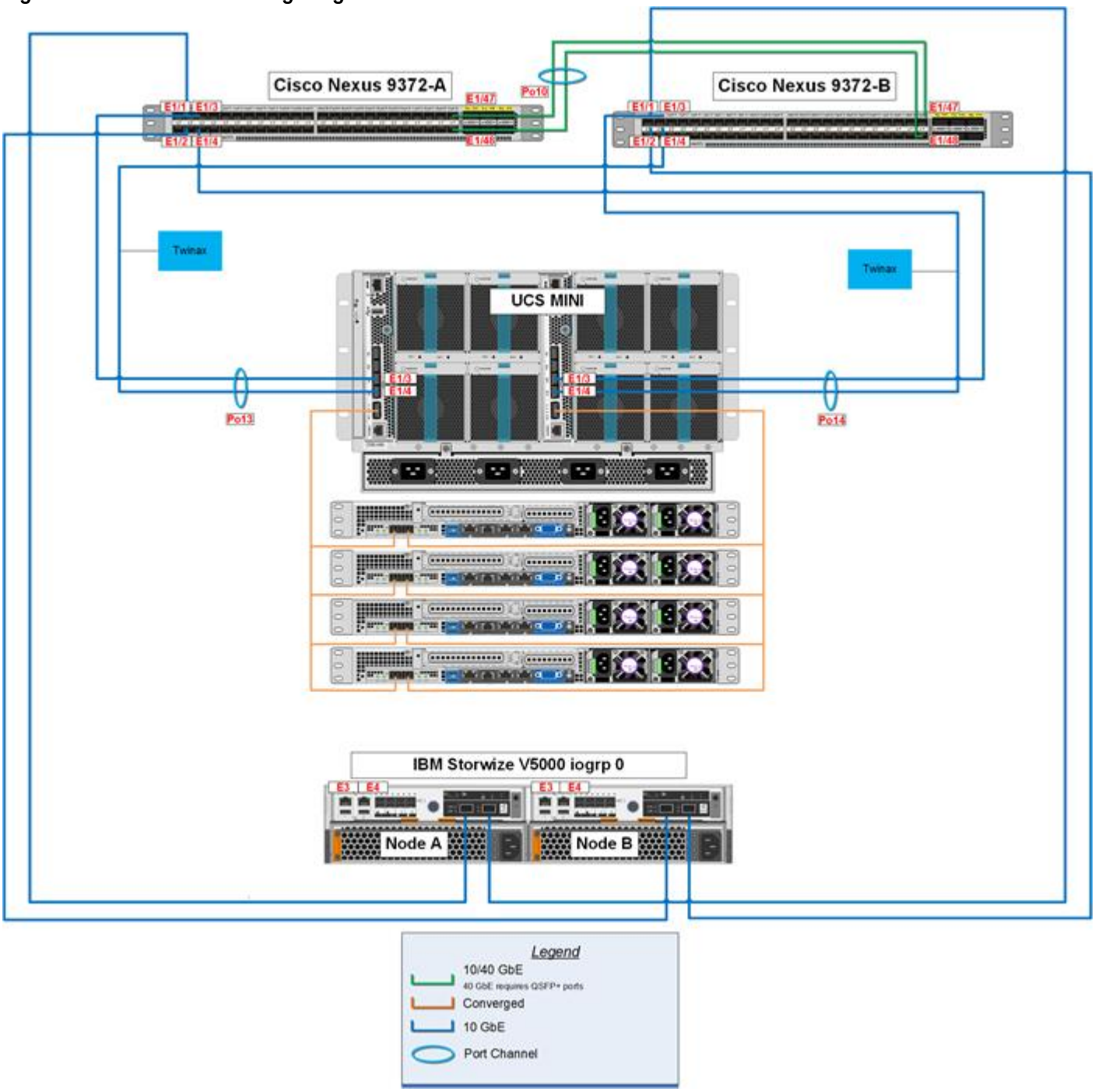
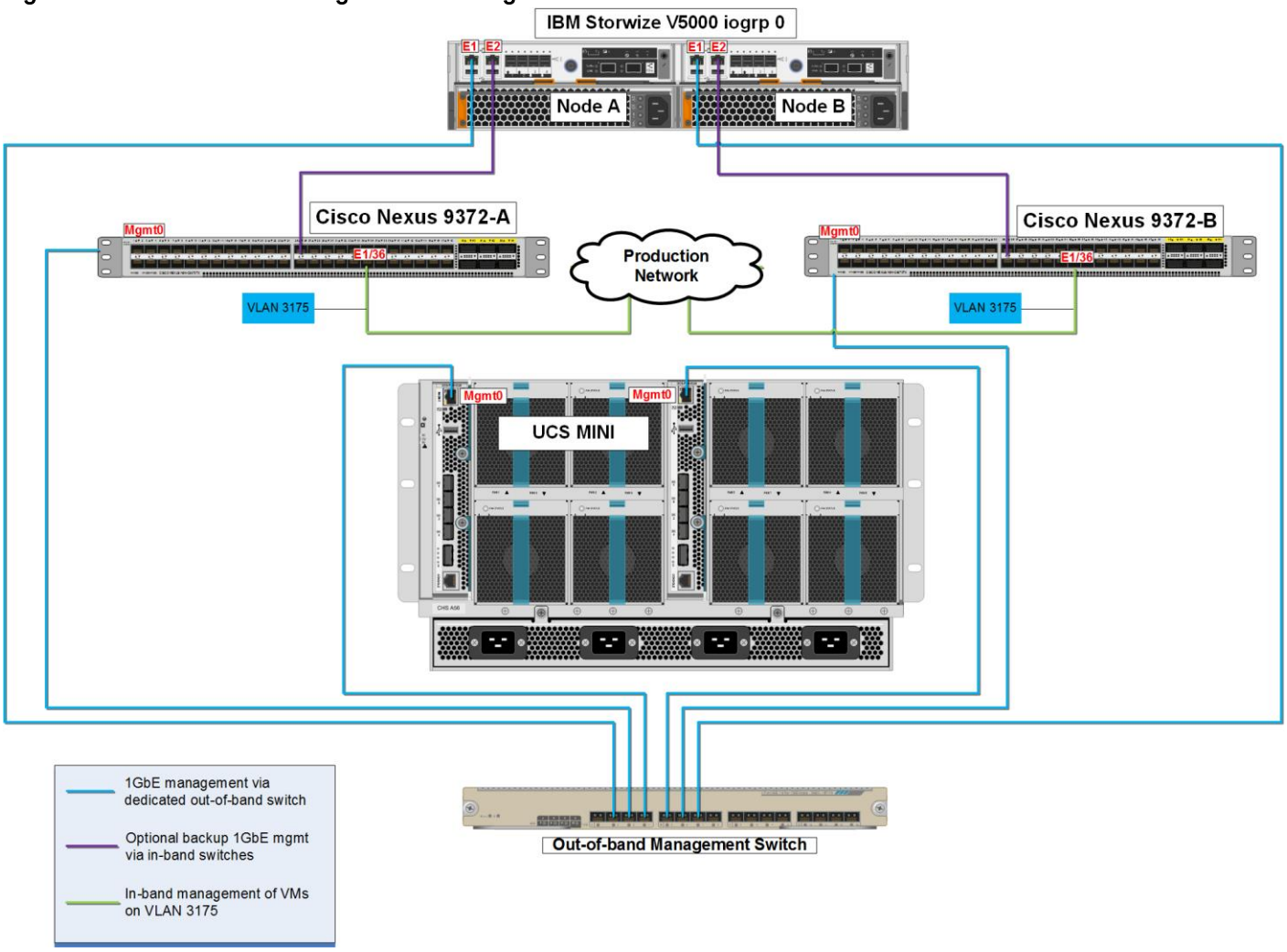


Figure 5 shows the Management cabling. The V5000's have redundant management connections. One path is through the dedicated out-of-band management switch, and the secondary path is through the in-band management path going up through the 9k to the production network.

Figure 5 VersaStack Management Cabling



The tables below provide the details of the connections in use.

Table 6 Cisco Nexus 9000-A cabling information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 9000-A	Eth1/1	10GbE	IBM V5000 Node-A	Eth3
	Eth 1/2	10GbE	IBM V5000 Node-B	Eth3
	Eth1/3	10GbE	Cisco UCS fabric interconnect-A	Eth1/3
	Eth1/4	10GbE	Cisco UCS fabric interconnect-B	Eth1/3
	Eth1/47*	10GbE	Cisco Nexus 9000-B	Eth1/47
	Eth1/48*	10GbE	Cisco Nexus 9000-B	Eth1/48
	Eth1/36	GbE	GbE management switch	Any

* The ports can be replaced with E1/49 and E1/50 for 40G connectivity

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

Table 7 Cisco Nexus 9000-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 9000-B	Eth 1/1	10GbE	IBM V5000 Node-A	Eth4
	Eth 1/2	10GbE	IBM V5000 Node-B	Eth4
	Eth1/3	10GbE	Cisco UCS fabric interconnect-A	Eth1/4
	Eth1/4	10GbE	Cisco UCS fabric interconnect-B	Eth1/4
	Eth1/47*	10GbE	Cisco Nexus 9000-A	Eth1/47
	Eth1/48*	10GbE	Cisco Nexus 9000-A	Eth1/48
	Eth1/36	GbE	GbE management switch	Any

* The ports can be replaced with E1/49 and E1/50 for 40G connectivity

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

Table 8 IBM Storwize V5000 Controller Node-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
IBM Storwize V5000 Controller, Node-A	E1	GbE	GbE management switch	Any
	E2 (optional)	GbE	Cisco Nexus 9000-A	Any
	E3	10GbE	Cisco Nexus 9000-A	Eth1/1
	E4	10GbE	Cisco Nexus 9000-B	Eth1/1

Table 9 IBM Storwize V5000 Controller Node-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
IBM Storwize V5000 Controller, Node-B	E1	GbE	GbE management switch	Any
	E2 (optional)	GbE	Cisco Nexus 9000-B	Any
	E3	10GbE	Cisco Nexus 9000-A	Eth1/2
	E4	10GbE	Cisco Nexus 9000-B	Eth1/2

Table 10 Cisco UCS Fabric Interconnect A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect-A	Mgmt0	GbE	GbE management switch	Any
	Eth1/3	10GbE	Cisco Nexus 9000-A	Eth 1/3
	Eth1/4	10GbE	Cisco Nexus 9000-B	Eth 1/3
	Scalability 1	10GbE	C220 M4	1227 VIC port 1

Table 11 Cisco UCS Fabric Interconnect B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect-B	Mgmt0	GbE	GbE management switch	Any
	Eth1/3	10GbE	Cisco Nexus 9000-A	Eth 1/4
	Eth1/4	10GbE	Cisco Nexus 9000-B	Eth 1/4
	Scalability 1	10GbE	C220 M4	1227 VIC port 2

VersaStack Deployment

Cisco Nexus 9000 Initial Configuration Setup

The steps provide in this section details for the initial Cisco Nexus 9000 Switch setup. In this case we are connected using a Cisco 2901 Terminal Server that is connected via the console port on the switch.

Figure 6 Console port on the Cisco Nexus 9000 Switch

Cisco Nexus A

To set up the initial configuration for the first Cisco Nexus switch complete the following steps:

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

```
Abort Auto Provisioning and continue with normal setup ?(yes/no)[n]: y

         ---- System Admin Account Setup ----

Do you want to enforce secure password standard (yes/no) [y]:

    Enter the password for "admin":

  Confirm the password for "admin":

         ---- Basic System Configuration Dialog VDC: 1 ----

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

Please register Cisco Nexus9000 Family devices promptly with your supplier. Failure
to register may affect response times for initial service calls. Nexus9000 devices
must be registered to receive entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip the remaining
dialogs.

Would you like to enter the basic configuration dialog (yes/no): y

  Create another login account (yes/no) [n]: n

  Configure read-only SNMP community string (yes/no) [n]:

  Configure read-write SNMP community string (yes/no) [n]:

  Enter the switch name : <<var_nexus_A_hostname>>

  Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:
```

```
  Mgmt0 IPv4 address : <<var_nexus_A_mgmt0_ip>>
  Mgmt0 IPv4 netmask : <<var_nexus_A_mgmt0_netmask>>
  Configure the default gateway? (yes/no) [y]:
  IPv4 address of the default gateway : <<var_nexus_A_mgmt0_gw>>
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]:
     Type of ssh key you would like to generate (dsa/rsa) [rsa]:
     Number of rsa key bits <1024-2048> [1024]: 2048
   Configure the ntp server? (yes/no) [n]: y
     NTP server IPv4 address : <<var_global_ntp_server_ip>>
  Configure default interface layer (L3/L2) [L2]:
   Configure default switchport interface state (shut/noshut) [noshut]:
   Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]:
The following configuration will be applied:
   password strength-check
switchname <<var_nexus_A_hostname>>
vrf context management
  ip route 0.0.0.0/0 <<var_nexus_A_mgmt0_gw>>
exit
  no feature telnet
ssh key rsa 2048 force
  feature ssh
ntp server <<var_global_ntp_server_ip>>
system default switchport
  no system default switchport shutdown
  copp profile strict
interface mgmt0 ip address <<var_nexus_A_mgmt0_ip>><var_nexus_A_mgmt0_netmask>> no
shutdown
Would you like to edit the configuration? (yes/no) [n]:
Use this configuration and save it? (yes/no) [y]:
[########################################] 100% Copy complete.
```

Cisco Nexus B

To set up the initial configuration for the second Cisco Nexus switch complete the following steps:

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

```
Abort Auto Provisioning and continue with normal setup ?(yes/no)[n]: y

         ---- System Admin Account Setup ----

Do you want to enforce secure password standard (yes/no) [y]:

    Enter the password for "admin":

  Confirm the password for "admin":

         ---- Basic System Configuration Dialog VDC: 1 ---This setup utility will
guide you through the basic configuration of the system. Setup configures only
enough connectivity for management of the system.

Please register Cisco Nexus9000 Family devices promptly with your supplier. Failure
to register may affect response times for initial service calls. Nexus9000 devices
must be registered to receive entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip the re-
maining dialogs.

Would you like to enter the basic configuration dialog (yes/no): y

  Create another login account (yes/no) [n]: n

  Configure read-only SNMP community string (yes/no) [n]:

  Configure read-write SNMP community string (yes/no) [n]:

  Enter the switch name : <<var_nexus_B_hostname>>

  Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:

    Mgmt0 IPv4 address : <<var_nexus_B_mgmt0_ip>>

    Mgmt0 IPv4 netmask : <<var_nexus_B_mgmt0_netmask>>

Configure the default gateway? (yes/no) [y]:

    IPv4 address of the default gateway : <<var_nexus_B_mgmt0_gw>>

  Configure advanced IP options? (yes/no) [n]:

  Enable the telnet service? (yes/no) [n]:

  Enable the ssh service? (yes/no) [y]:

    Type of ssh key you would like to generate (dsa/rsa) [rsa]:

    Number of rsa key bits <1024-2048> [1024]: 2048

  Configure the ntp server? (yes/no) [n]: y

    NTP server IPv4 address : <<var_global_ntp_server_ip>>

  Configure default interface layer (L3/L2) [L2]:
```

```
Configure default switchport interface state (shut/noshut) [noshut]:

Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]:

The following configuration will be applied:

password strength-check

switchname <<var_nexus_B_hostname>>

vrf context management

ip route 0.0.0.0/0 <<var_nexus_B_mgmt0_gw>>

exit

 no feature telnet

ssh key rsa 2048 force

 feature ssh

ntp server <<var_global_ntp_server_ip>>

system default switchport

 no system default switchport shutdown

 copp profile strict

interface mgmt0 ip address <<var_nexus_B_mgmt0_ip>><<var_nexus_B_mgmt0_netmask>> no
shutdown

Would you like to edit the configuration? (yes/no) [n]:

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

[########################################] 100% Copy complete.
```

Enable Appropriate Cisco Nexus 9000 Features and Settings

Cisco Nexus 9000 A and Cisco Nexus 9000 B

The following commands enable the IP switching feature and set default spanning tree behaviors:

1. On each Nexus 9000, enter the configuration mode:

   ```
   config terminal
   ```

2. Use the following commands to enable the necessary features:

   ```
   feature udld

   feature lacp

   feature vpc
   ```

3. Configure the spanning tree and save the running configuration to start-up:

   ```
   spanning-tree port type network default

   spanning-tree port type edge bpduguard default
   ```

```
spanning-tree port type edge bpdufilter default
copy run start
```

Create VLANs for VersaStack Traffic

Cisco Nexus 9000 A and Cisco Nexus 9000 B

To create the necessary virtual local area networks (VLANs), complete the following step on both switches:

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

```
vlan <<var_ib-mgmt_vlan_id>>
name IB-MGMT-VLAN
vlan <<var_native_vlan_id>>
name Native-VLAN
vlan <<var_nfs_vlan_id>>
name NFS-VLAN
vlan <<var_vmotion_vlan_id>>
name vMotion-VLAN
vlan <<var_vm_traffic_vlan_id>>
name VM-Traffic-VLAN
vlan <<var_iscsi-a_vlan_id>>
name iSCSI-A-VLAN
vlan <<var_iscsi-b_vlan_id>>
name iSCSI-B-VLAN
exit
copy run start
```

Configure Virtual Port Channel Domain

Cisco Nexus 9000 A

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

1. From the global configuration mode, create a new vPC domain:

```
vpc domain <<var_nexus_vpc_domain_id>>
```

2. Make the Nexus 9000A the primary vPC peer by defining a low priority value:

```
 role priority 10
```

3. Use the management interfaces on the supervisors of the Nexus 9000s to establish a keepalive link:

```
peer-keepalive destination <<var_nexus_B_mgmt0_ip>>  source
<<var_nexus_A_mgmt0_ip>>
```

4. Enable the following features for this vPC domain:

```
peer-switch

delay restore 150

peer-gateway

ip arp synchronize

auto-recovery

copy run start
```

Cisco Nexus 9000 B

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

1. From the global configuration mode, create a new vPC domain:

```
vpc domain <<var_nexus_vpc_domain_id>>
```

2. Make the Nexus 9000A the primary vPC peer by defining a low priority value:

```
 role priority 20
```

3. Use the management interfaces on the supervisors of the Nexus 9000s to establish a keepalive link:

```
peer-keepalive destination <<var_nexus_A_mgmt0_ip>> source
<<var_nexus_B_mgmt0_ip>>
```

4. Enable the following features for this vPC domain:

```
peer-switch

delay restore 150

peer-gateway

ip arp synchronize

auto-recovery

copy run start
```

Configure Network Interfaces for the VPC Peer Links

Cisco Nexus 9000 A

1. Define a port description for the interfaces connecting to VPC Peer <var_nexus_B_hostname>>.

```
interface Eth1/47

description VPC Peer <<var_nexus_B_hostname>>:1/47

interface Eth1/48

description VPC Peer <<var_nexus_B_hostname>>:1/48
```

2. Apply a port channel to both VPC Peer links and bring up the interfaces.

```
interface Eth1/47,Eth1/48

channel-group 10  mode active

no shutdown
```

3. Define a description for the port-channel connecting to <<var_nexus_B_hostname>>.

```
interface Po10

description vPC peer-link
```

4. Make the port-channel a switchport, and configure a trunk to allow in-band management, NFS, VM traffic, iSCSI traffic and the native VLAN.

```
switchport

switchport mode trunk

switchport trunk native vlan <<var_native_vlan_id>>

switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>,
<<var_nfs_vlan_id>>,<<var_vmotion_vlan_id>>, <<var_vm_traffic_vlan_id>>,
<<var_iscsi-a_vlan_id>>, <<var_iscsi-b_vlan_id>>
```

5. Make this port-channel the VPC peer link and bring it up.

```
vpc peer-link

no shutdown

copy run start
```

Cisco Nexus 9000 B

1. Define a port description for the interfaces connecting to VPC Peer <var_nexus_A_hostname>>.

```
interface Eth1/47

description VPC Peer <<var_nexus_A_hostname>>:1/47

interface  Eth1/48

description VPC Peer <<var_nexus_A_hostname>>:1/48
```

2. Apply a port channel to both VPC Peer links and bring up the interfaces.

```
interface Eth1/47,Eth1/48

channel-group 10 mode active

no shutdown
```

3. Define a description for the port-channel connecting to <<var_nexus_A_hostname>>.

```
interface Po10

description vPC peer-link
```

4. Make the port-channel a switchport, and configure a trunk to allow in-band management, NFS, VM traffic, iSCSI traffic and the native VLAN.

```
switchport

switchport mode trunk

switchport trunk native vlan <<var_native_vlan_id>>

switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_nfs_vlan_id>>,

<<var_vmotion_vlan_id>>, <<var_vm_traffic_vlan_id>>, <<var_iscsi-a_vlan_id>>,
<<var_iscsi-b_vlan_id>>
```

5. Make this port-channel the VPC peer link and bring it up.

```
vpc peer-link

no shutdown

copy run start
```

Configure Network Interfaces to Cisco UCS Fabric Interconnect

Cisco Nexus 9000 A

1. Define a description for the port-channel connecting to <<var_ucs_clustername>>-A.

```
interface Po13

description <<var_ucs_clustername>>-A
```

2. Make the port-channel a switchport, and configure a trunk to allow in-band management, NFS, VM traffic, iSCSI traffic and the native VLANs.

```
switchport

switchport mode trunk

switchport trunk native vlan <<var_native_vlan_id>>

switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>,
<<var_nfs_vlan_id>>,<<var_vmotion_vlan_id>>, <<var_vm_traffic_vlan_id>>,
<<var_iscsi-a_vlan_id>>, <<var_iscsi-b_vlan_id>>
```

3. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

4. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

5. Make this a VPC port-channel and bring it up.

```
vpc 13

no shutdown
```

6. Define a port description for the interface connecting to <<var_ucs_clustername>>-A.

```
interface Eth1/3

description <<var_ucs_clustername>>-A:1/3
```

7. Apply it to a port channel and bring up the interface.

```
channel-group 13 force mode active

no shutdown
```

8. Define a description for the port-channel connecting to <<var_ucs_clustername>>-B

```
interface Po14

description <<var_ucs_clustername>>-B
```

9. Make the port-channel a switchport, and configure a trunk to allow InBand management, NFS, iSCSI and VM traffic VLANs and the native VLAN.

```
switchport

switchport mode trunk

switchport trunk native vlan <<var_native_vlan_id>>

switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_nfs_vlan_id>>,
<<var_vmotion_vlan_id>>, <<var_vm_traffic_vlan_id>>, <<var_iscsi-a_vlan_id>>,
<<var_iscsi-b_vlan_id>>
```

10. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

11. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

12. Make this a VPC port-channel and bring it up.

```
vpc 14

no shutdown
```

13. Define a port description for the interface connecting to <<var_ucs_clustername>>-B

```
interface Eth1/4

description <<var_ucs_clustername>>-B:1/3
```

14. Apply it to a port channel and bring up the interface.

```
channel-group 14 force  mode active

no shutdown

copy run start
```

Configure Network Interfaces to Cisco UCS Fabric Interconnect

Cisco Nexus 9000 B

1. Define a description for the port-channel connecting to <<var_ucs_clustername>>-A

```
interface Po13

description <<var_ucs_clustername>>-A
```

2. Make the port-channel a switchport, and configure a trunk to allow in-band management, NFS, VM traffic, and the native VLANs.

```
switchport

switchport mode trunk

switchport trunk native vlan <<var_native_vlan_id>>

switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_nfs_vlan_id>>,
<<var_vmotion_vlan_id>>, <<var_vm_traffic_vlan_id>>
```

3. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

4. Set the MTU to 9216 to support jumbo frames.

```
mtu 9216
```

5. Make this a VPC port-channel and bring it up.

```
vpc 13

no shutdown
```

6. Define a port description for the interface connecting to <<var_ucs_clustername>>-A

```
interface Eth1/3

description <<var_ucs_clustername>>-A:1/4
```

7. Apply it to a port channel and bring up the interface.

```
channel-group 13 force mode active

no shutdown
```

8. Define a description for the port-channel connecting to <<var_ucs_clustername>>-A

```
interface Po14

description <<var_ucs_clustername>>-B
```

9. Make the port-channel a switchport, and configure a trunk to allow InBand management, NFS, iSCSI and VM traffic VLANs and the native VLAN.

```
switchport

switchport mode trunk
```

```
switchport trunk native vlan <<var_native_vlan_id>>

switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_nfs_vlan_id>>,
<<var_vmotion_vlan_id>>, <<var_vm_traffic_vlan_id>>, <<var_iscsi-a_vlan_id>>,
<<var_iscsi-b_vlan_id>>
```

10. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

11. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

12. Make this a VPC port-channel and bring it up.

```
vpc 14

no shutdown
```

13. Define a port description for the interface connecting to <<var_ucs_clustername>>-A

```
interface Eth1/4

description <<var_ucs_clustername>>-B:1/4
```

14. Apply it to a port channel and bring up the interface.

```
channel-group 14 force  mode active

no shutdown

copy run start
```

Configure Network Interfaces connected to IBM V5000 iSCSI ports

Cisco Nexus 9000 A

1. Define a description for the Ethernet port connecting to <<var_V5000_n1:Eth3>>

```
interface Ethernet1/1
```

description <<var_V5000_n1:Eth3>>

2. Make the Interface an access port, and configure the switchport access VLAN.

```
switchport mode access

switchport access vlan <<var_iscsi-a_vlan_id>>
```

3. Make the interface spanning normal.

spanning-tree port type normal

4. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

no shutdown

copy run start

5. Define a description for the Ethernet port connecting to <<var_V5000_n2:Eth3>>

```
interface Ethernet1/2
```

description <<var_V5000_n2:Eth3>>

6. Make the Interface an access port, and configure the switchport access VLAN.

```
switchport mode access
switchport access vlan <<var_iscsi-a_vlan_id>>
```

7. Make the interface spanning normal.

spanning-tree port type normal

8. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

no shutdown

copy run start

Cisco Nexus 9000 B

1. Define a description for the Ethernet port connecting to <<var_V5000_n1:Eth4>>

```
interface Ethernet1/1
```

description <<var_V5000_n1:Eth4>>

2. Make the Interface an access port, and configure the switchport access VLAN.

```
switchport mode access
switchport access vlan <<var_iscsi-b_vlan_id>>
```

3. Make the interface spanning normal.

spanning-tree port type normal

4. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

no shutdown

copy run start

5. Define a description for the Ethernet port connecting to <<var_V5000_n2:Eth3>>

```
interface Ethernet1/2
```

description <<var_V5000_n2:Eth4>>

6. Make the Interface an access port, and configure the switchport access VLAN.

```
switchport mode access
switchport access vlan <<var_iscsi-b_vlan_id>>
```

7. Make the interface spanning normal.

spanning-tree port type normal

8. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

no shutdown

copy run start

Management Plane Access for Servers and Virtual Machines

There are multiple ways to configure the switch to uplink to your separate management switch. There are two examples shown below. These examples are provide to help show methods how the configuration could be setup, however, since networking configurations can vary, it is recommended that you consult your local network personal for the optimal configuration. In the first example provided in this section, a single switch is top of rack and the Cisco Nexus 9000 series switches are both connected to it through its ports 36. The Cisco 9k switches use a 1 gig SFP to convert the connected to Cat-5 copper connecting to the top of rack switch, however, connection types can vary. The 9k's are configured with the interface-vlan option and each 9k switch has a unique IP for its VLAN. The traffic required to route from the 9k is the in-band management traffic, so use the VLAN 3175 and set the port to access mode. The top of rack switch also has its ports set to access mode. The second example shows how to leverage port channel, which maximizes upstream connectivity. In the second example, the top of rack switch must have the port channel configured for the port connected from the downstream switch.

Cisco Nexus 9000 A and B Using Interface VLAN Example 1

On the Nexus A switch, type the following commands. Notice the VLAN IP is different on each switch.

Cisco Nexus 9000 A

```
int Eth1/36
description IB-management-access
switchport mode access
spanning-tree port type network
switchport access vlan <<var_ib-mgmt_vlan_id>>
no shut
feature interface-vlan
```

```
int Vlan <<var_ib-mgmt_vlan_id>>
ip address <<var_switch_A_inband_mgmt_ip_address>>/<<var_inband_mgmt_netmask>>
no shut
ip route 0.0.0.0/0 <<var_inband_mgmt_gateway>>
copy run start
```

Cisco Nexus 9000 B

```
int Eth1/36
description Ib-management-access
switchport mode access
spanning-tree port type network
switchport access vlan <<var_ib-mgmt_vlan_id>>
no shut
feature interface-vlan
int Vlan <<var_ib-mgmt_vlan_id>>
ip address <<var_switch_B_inband_mgmt_ip_address>>/<<var_inband_mgmt_netmask>>
no shut
ip route 0.0.0.0/0 <<var_inband_mgmt_gateway>>
copy run start
```

Cisco Nexus 9000 A and B using Port Channel Example 2

To enable management access across the IP switching environment leveraging port channel in config mode run the following commands:

1. Define a description for the port-channel connecting to management switch.

   ```
   interface po9
   description IB-MGMT
   ```

2. Configure the port as an access VLAN carrying the InBand management VLAN traffic.

   ```
   switchport
   switchport mode access
   switchport access vlan <<var_ib-mgmt_vlan_id>>
   ```

3. Make the port channel and associated interfaces normal spanning tree ports.

   ```
    spanning-tree port type normal
   ```

4. Make this a VPC port-channel and bring it up.

   ```
   vpc 9
   ```

```
no shutdown
```

5. Define a port description for the interface connecting to the management plane.

```
interface Eth1/36
description IB-MGMT-SWITCH_uplink
```

6. Apply it to a port channel and bring up the interface.

```
channel-group 9 force mode active
no shutdown
```

7. Save the running configuration to start-up in both Nexus 9000 series switches and run commands to look at port and port channel.

```
Copy run start
sh int eth1/36 br
sh port-channel summary
```

Storage Configuration

There is a two stage setup for the IBM Storwize V5000. A USB key and IBM setup software will be used for initial configuration and IP assignment, and the web interface will be used to complete the configuration.

Required planning is essential to maximize performance and lower operating cost by leveraging the features of VersaStack. We have completed our planning for this test configuration. The IBM Easy Tier is leveraged to automatically move frequently accessed “hot” data to SSD disk. Easy tier will be leveraged with three tiers with the first tier being fast SSD, a middle tier of 10k or 15k RPM enterprise SAS drives, and the third tier consisting of larger capacity slower 7200 RPM drives known as Nearline. Rarely accessed data also known as “cold” data is moved to the third Nearline tier automatically. Moving cold data off the SAS and SSD disks to Nearline disk reduces storage operating costs while improving performance for the other tiers. Money saved leveraging the less expensive Nearline storage will be used to offset the cost of faster SSD disks. While mirroring will not be deployed in this document, it is available for fault tolerance.

Secure Web Access to the IBM Storwize V5000 Service and Management GUI

Browser access to all system and service IPs is automatically configured to connect securely using HTTPS and SSL. Attempts to connect through HTTP will get redirected to HTTPS.

The system generates its own self-signed SSL certificate. Upon first connection to the system, your browser may present a security exception because it does not trust the signer; you should allow the connection to proceed.

Prerequisites

You will need a USB key to run the setup for the IBM Storwize V5000 as well as the setup software from IBM. This is provided with the original shipment but can be downloaded and copied to a blank USB drive as well.

IBM Storwize V5000 Initial Configuration

Complete the following steps for the V5000 setup. Steps 1 and 2 can be skipped if you are already in possession of the USB key with the Initialization Tool installed:

1. Download the System Initialization software from IBM Storwize V5000 support web site.

You will need your IBM login account to download software.

   a. Go to http://www.ibm.com/storage/support/storwize/v5000

   b. Select the IBM Storwize V5000 Code level applicable to this initial setup

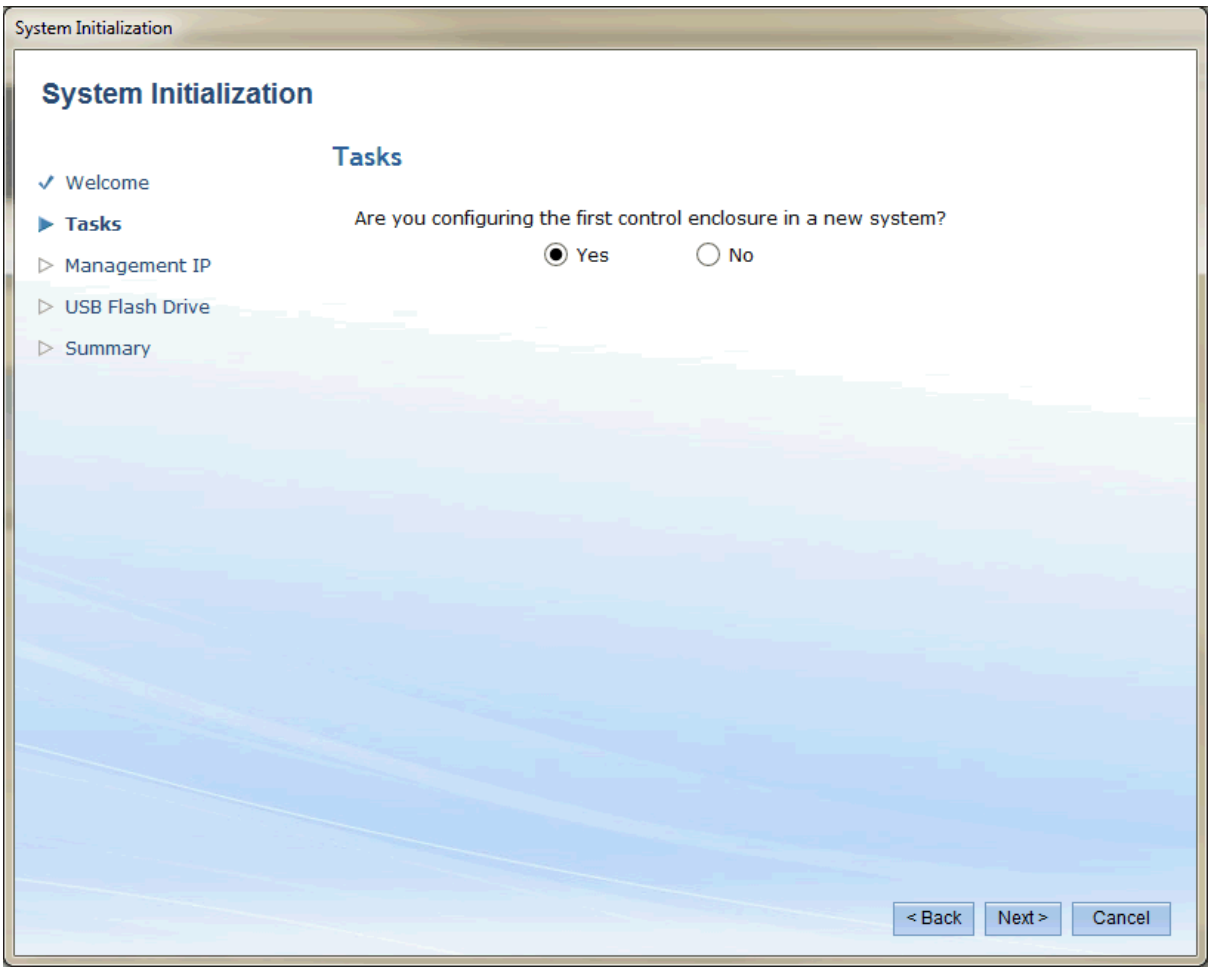
   c. Scroll down and select the hyper link for IBM Storwize V5000 Initialization Tool

2. Extract the contents of the zip archive file to the root directory of any USB key formatted with a FAT32, ext2 or ext3 file system.

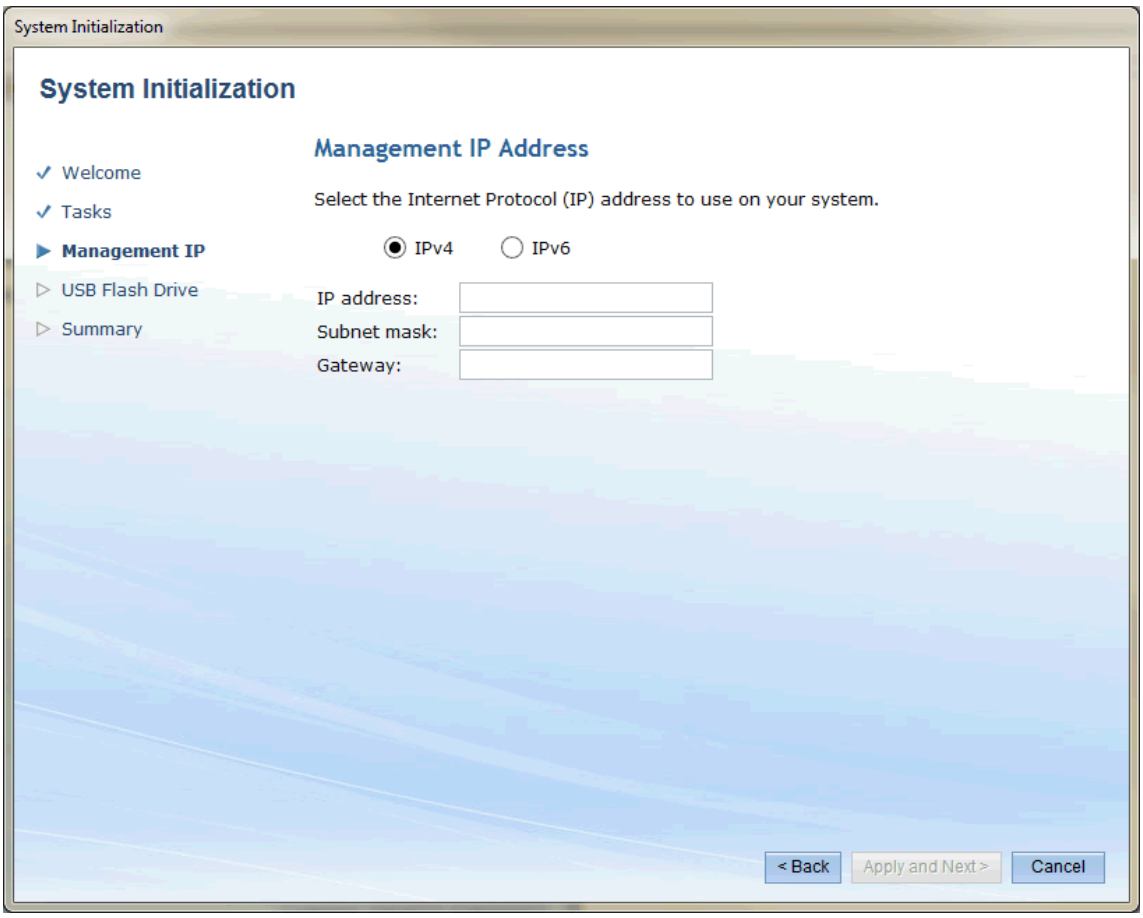
3. Run the System Initialization tool from the USB key. For Windows clients run the InitTool.bat located in the root directory of the USB key. For MAC, Red Hat & Ubuntu run the InitTool.sh located in the root directory of the USB key.

4. This wizard will be used to configure a new system. Click ‘Next’ to continue.

5. Select ‘Yes’ to ‘Are you configuring the first control enclosure in a new system?’ and Click ‘Next’.

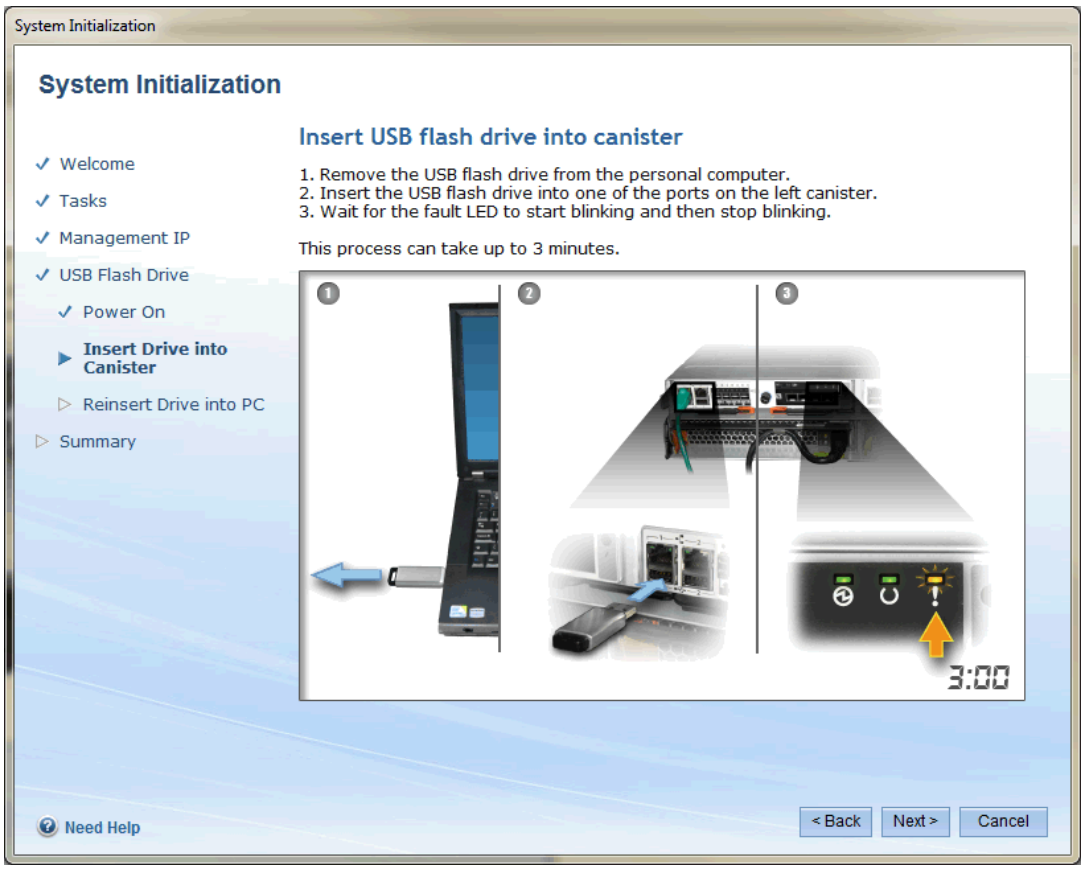


6. Input the IP address for your V5000 Cluster as well as the required subnet mask and gateway. Click on ‘Apply and Next’

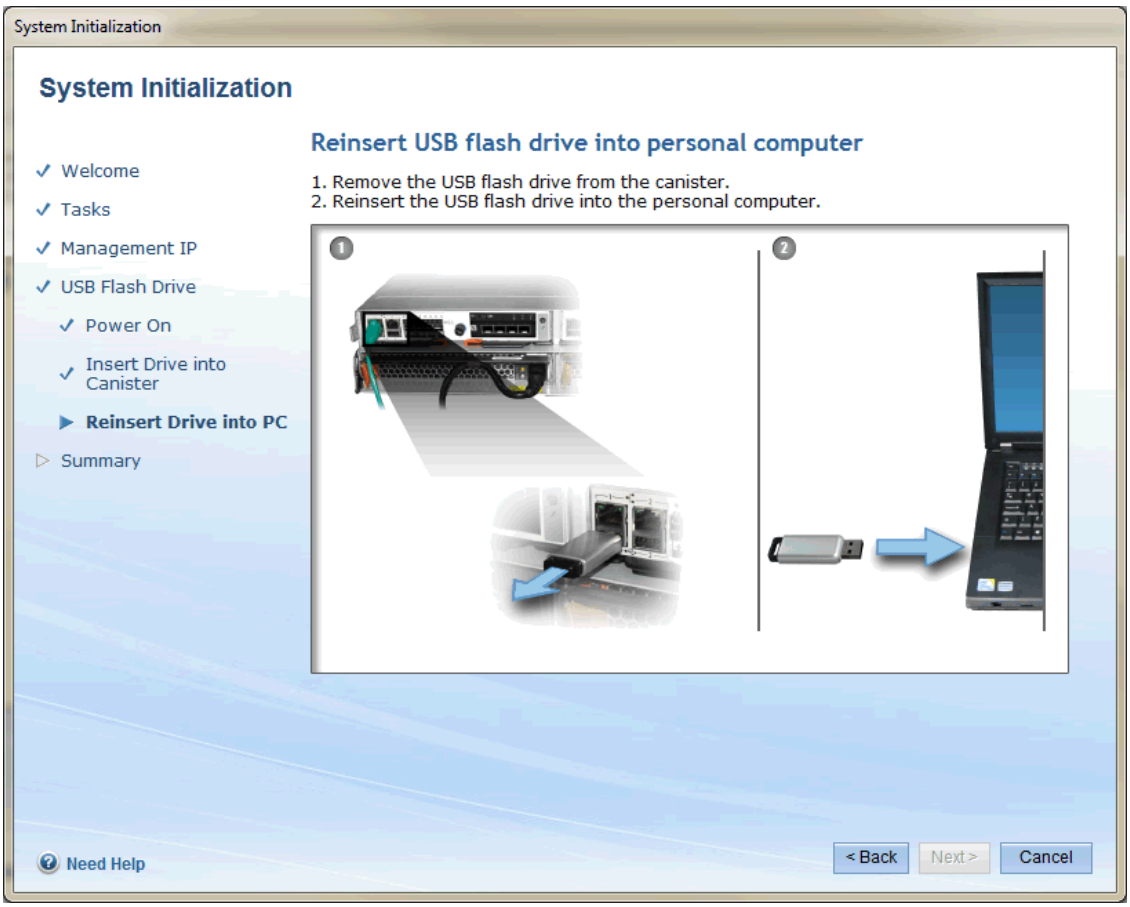


7. Plug in both power cables into the power supply units of the V5000 and wait for the status LED to blink. This process can take up to 10 minutes. Click Next.

8. Remove the USB key from your computer and insert into one of the USB ports on the left canister. Wait for the fault LED to start blinking and then stop blinking. This process can take up to 3 minutes.



9. Remove the USB key from the canister and reinsert into your personal computer. Alternatively, you can input the IP assigned to the V5000 in your browser to connect and complete the setup procedure.



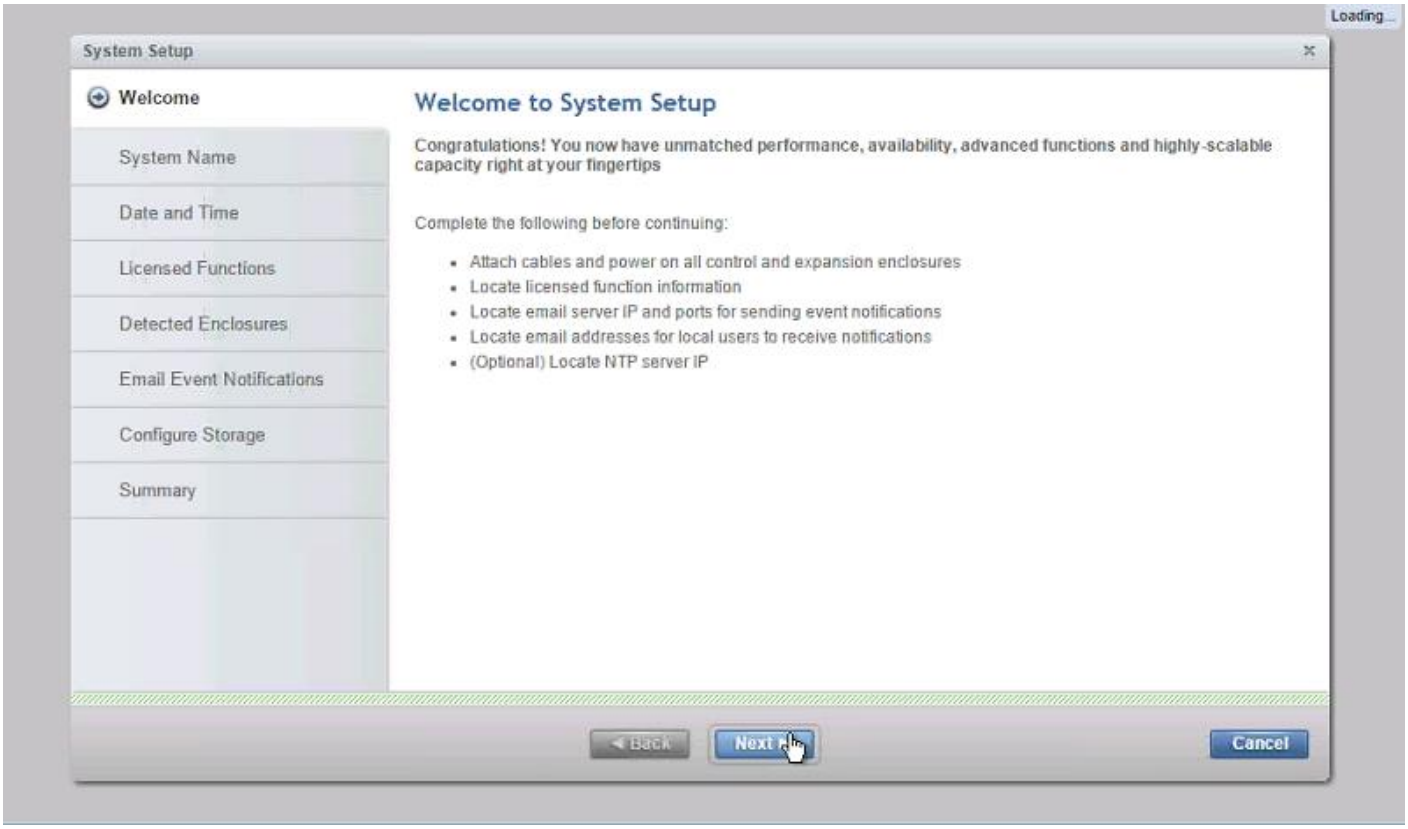
IBM Storwize V5000 Setup

1. Read and accept the license agreement.

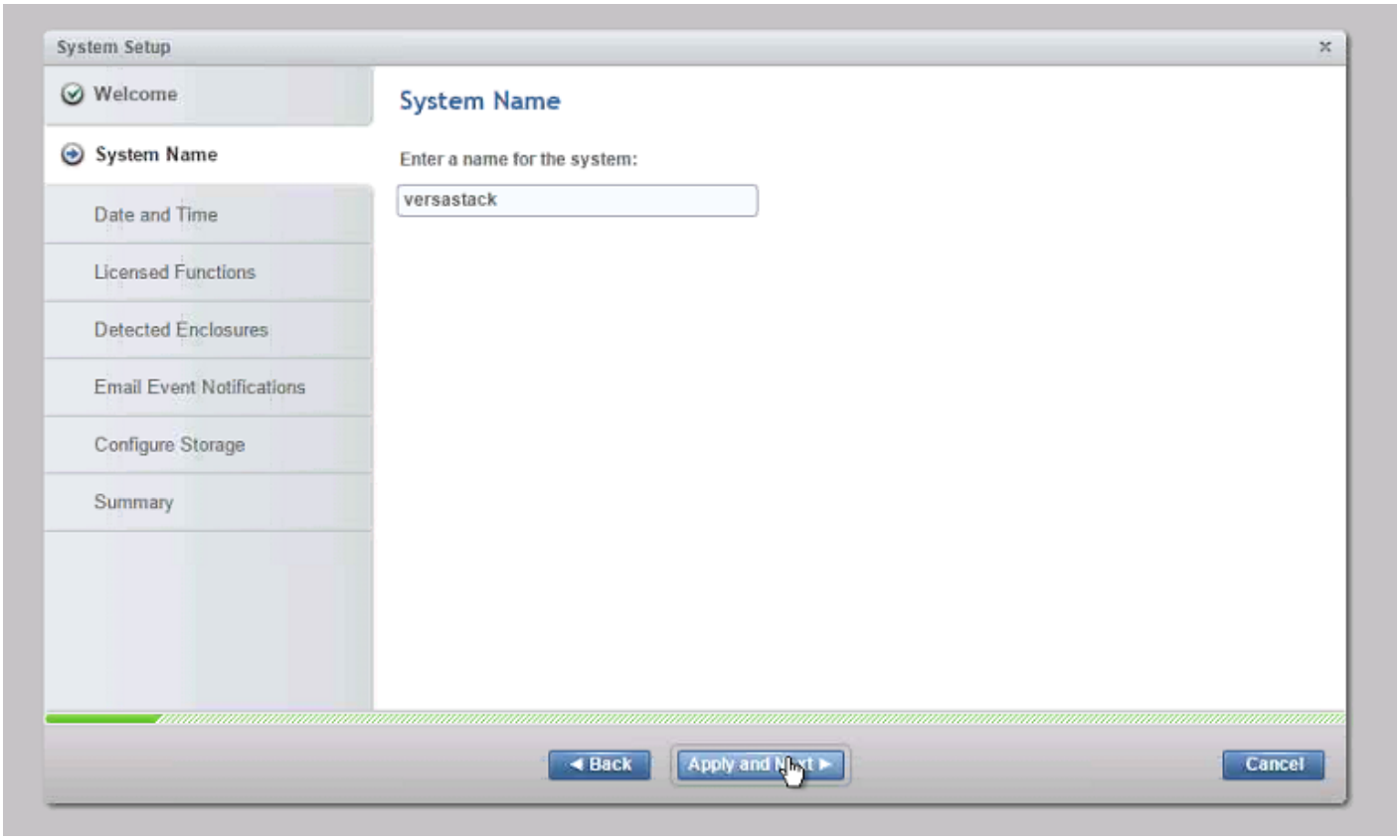
2. Login as superuser with password as password.

3. Change the password for superuser, and then click Log In.

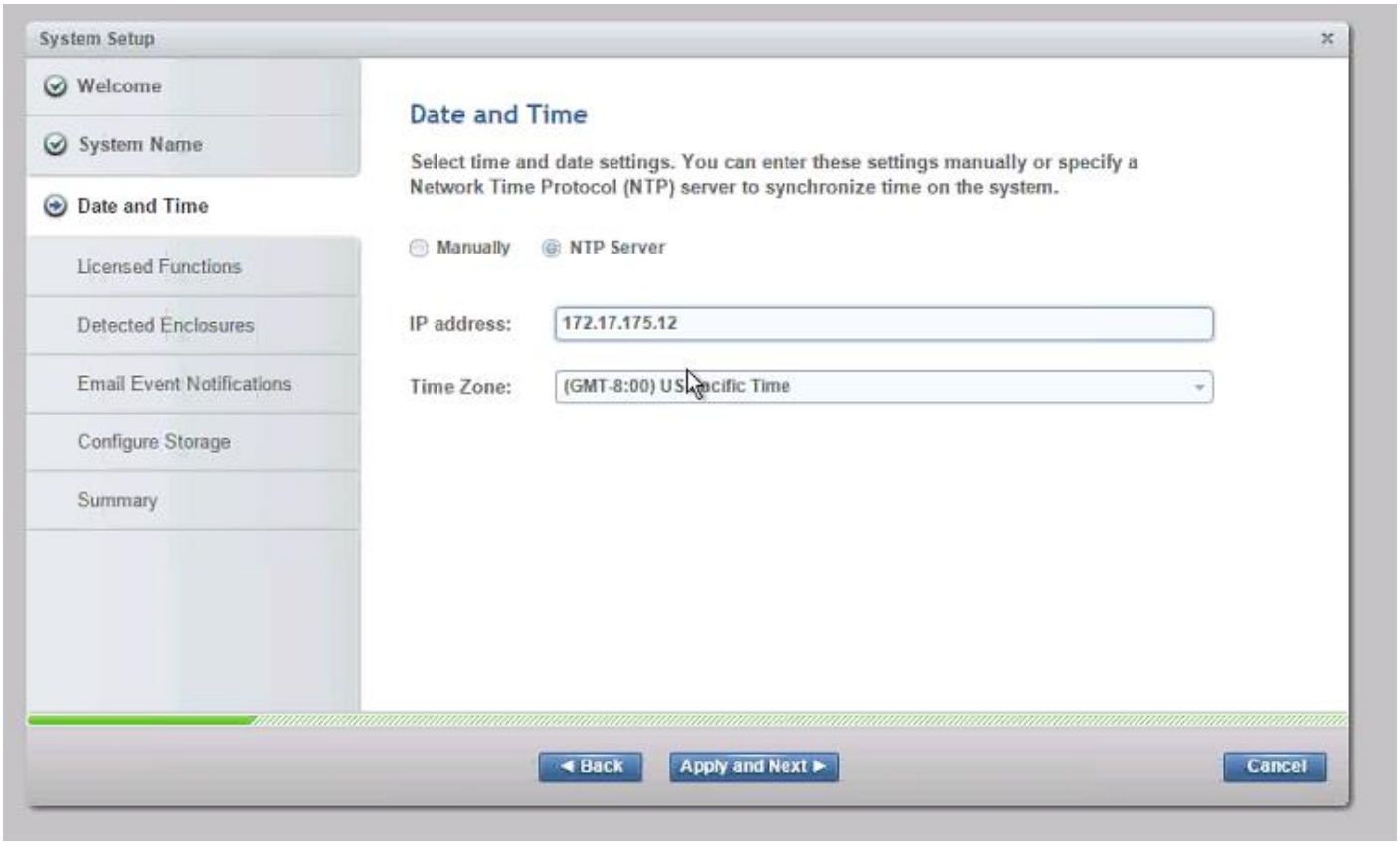
4. On the welcome to system setup screen click ‘Next’.



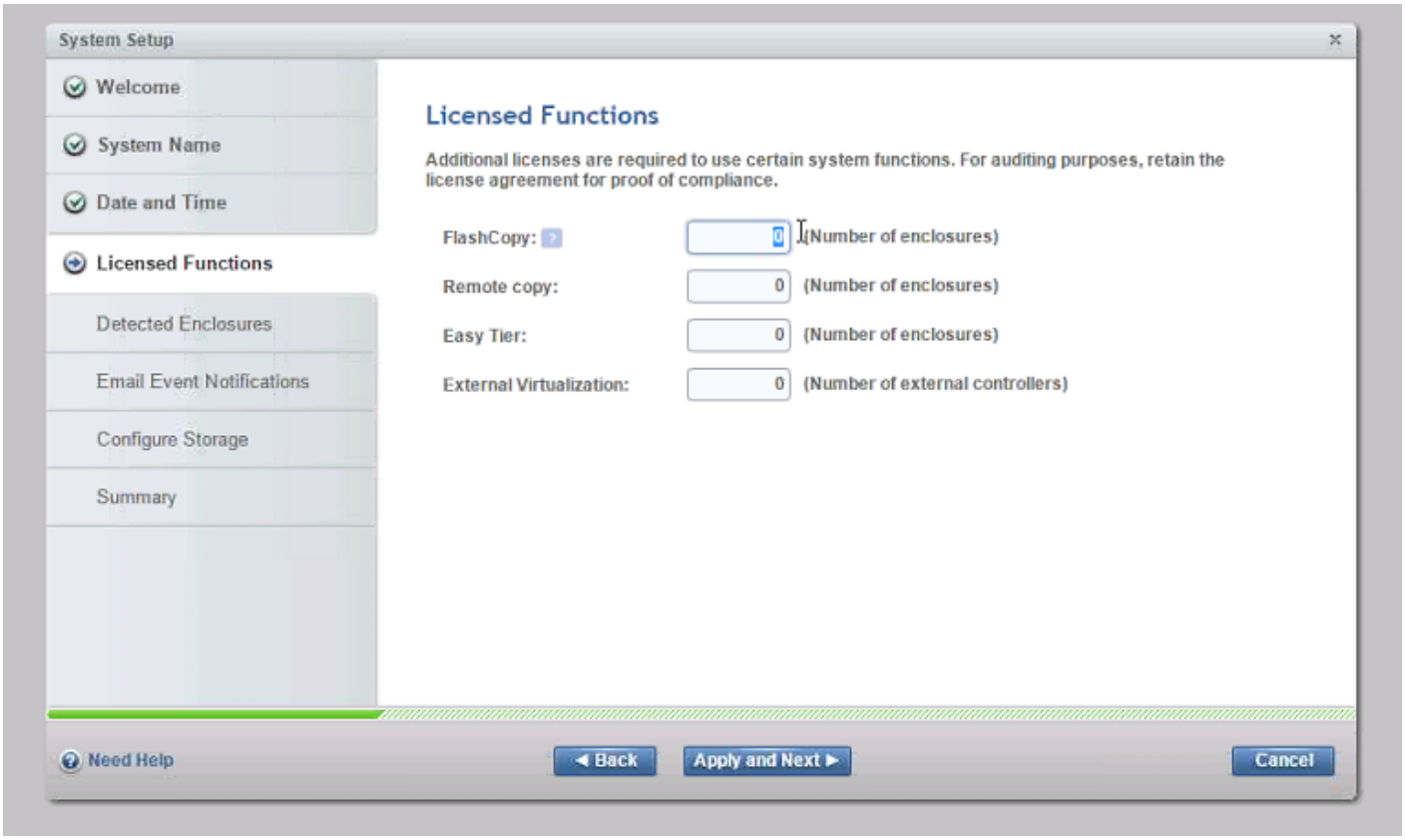
5. Enter the System Name and Click ‘Apply’ and click ‘Next’ to proceed.



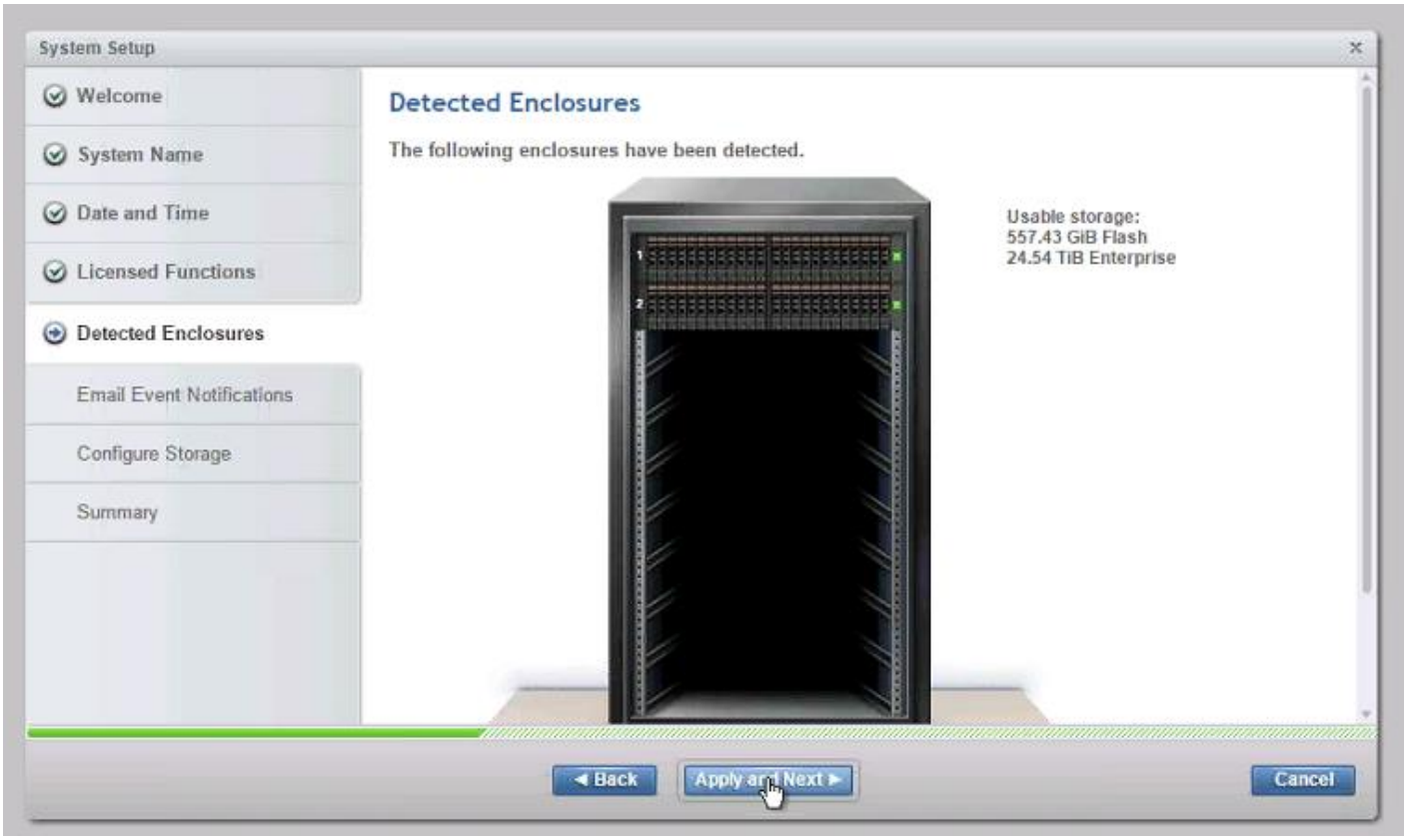
6. Select NTP Server and enter the address of the server then select ‘Apply’ and click ‘Next’, then click ‘Close’.



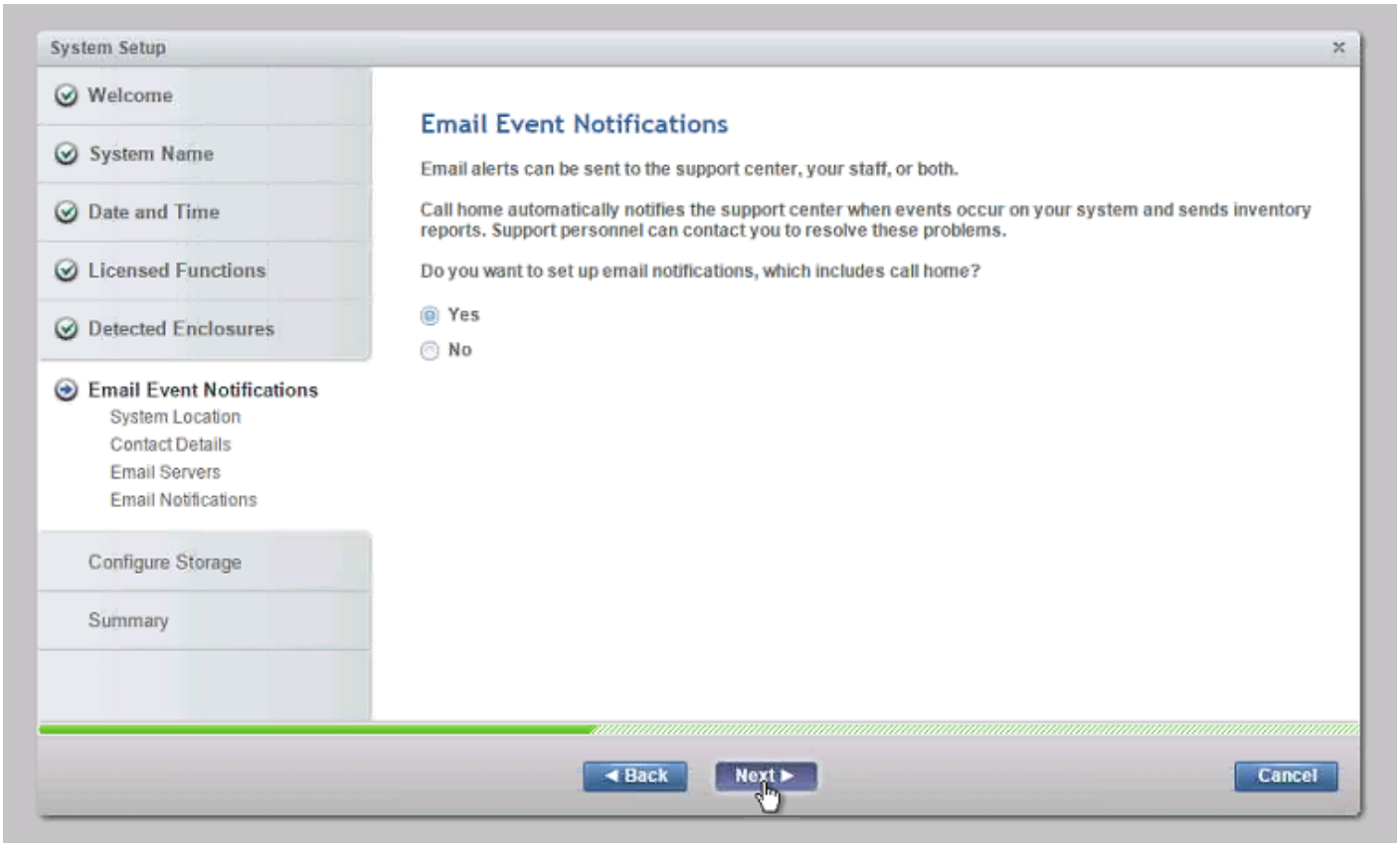
7. Enter the number of licenses for each feature and click ‘Apply’ and click ‘Next’, and then click ‘Close’.



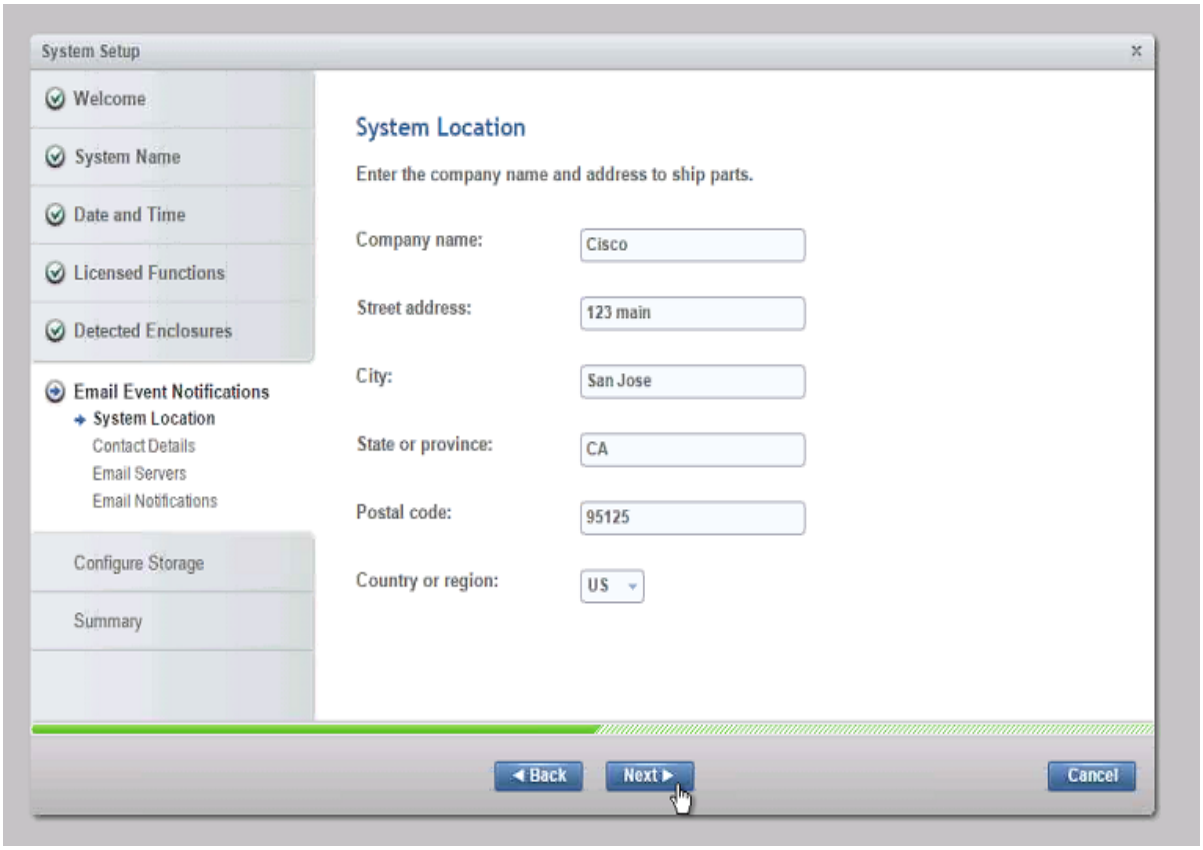
8. Validate the Detected Enclosures and click Apply and click Next, then click Close.



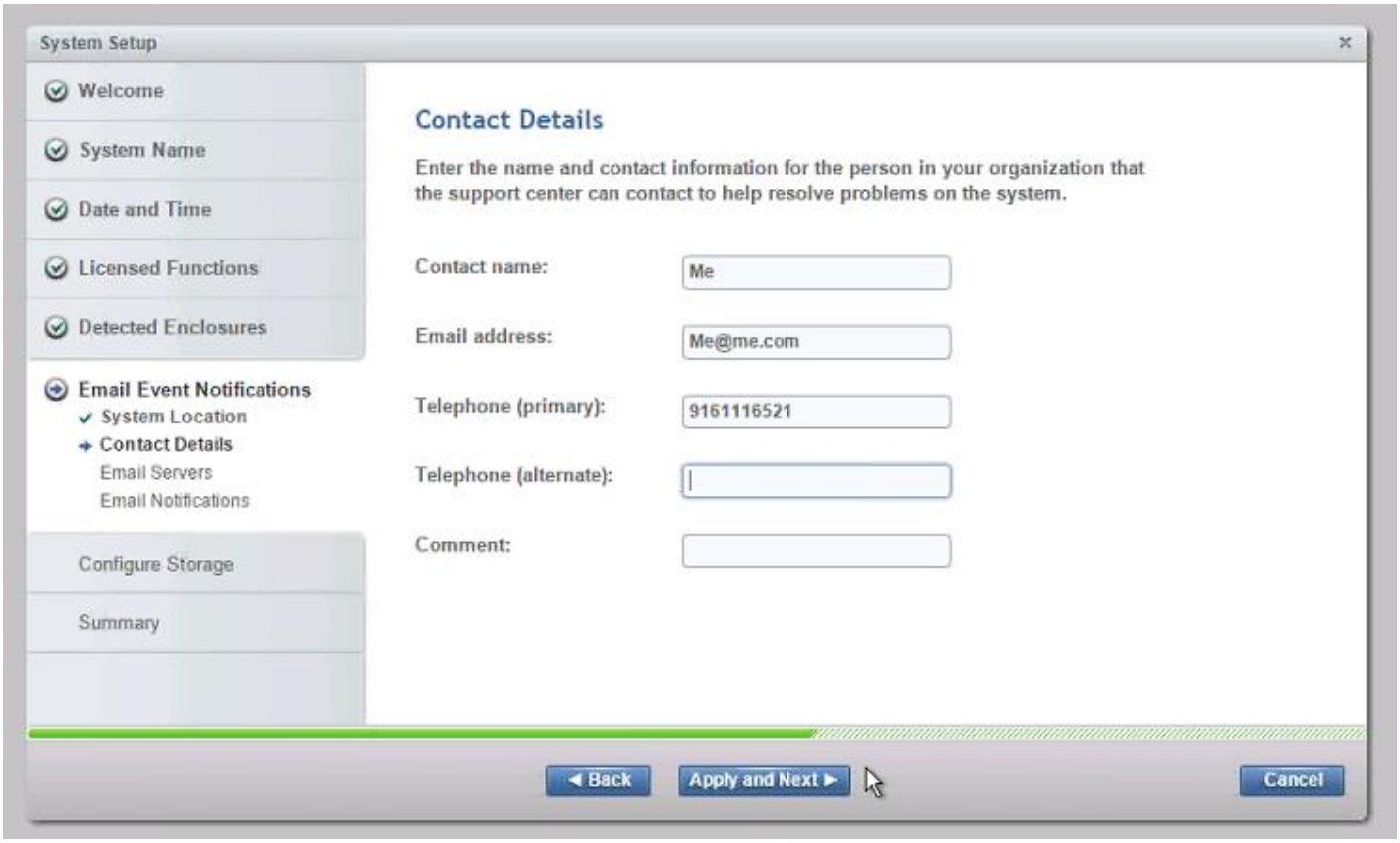
9. Click ‘Yes’ for Email Event Notification and click ‘Next’.



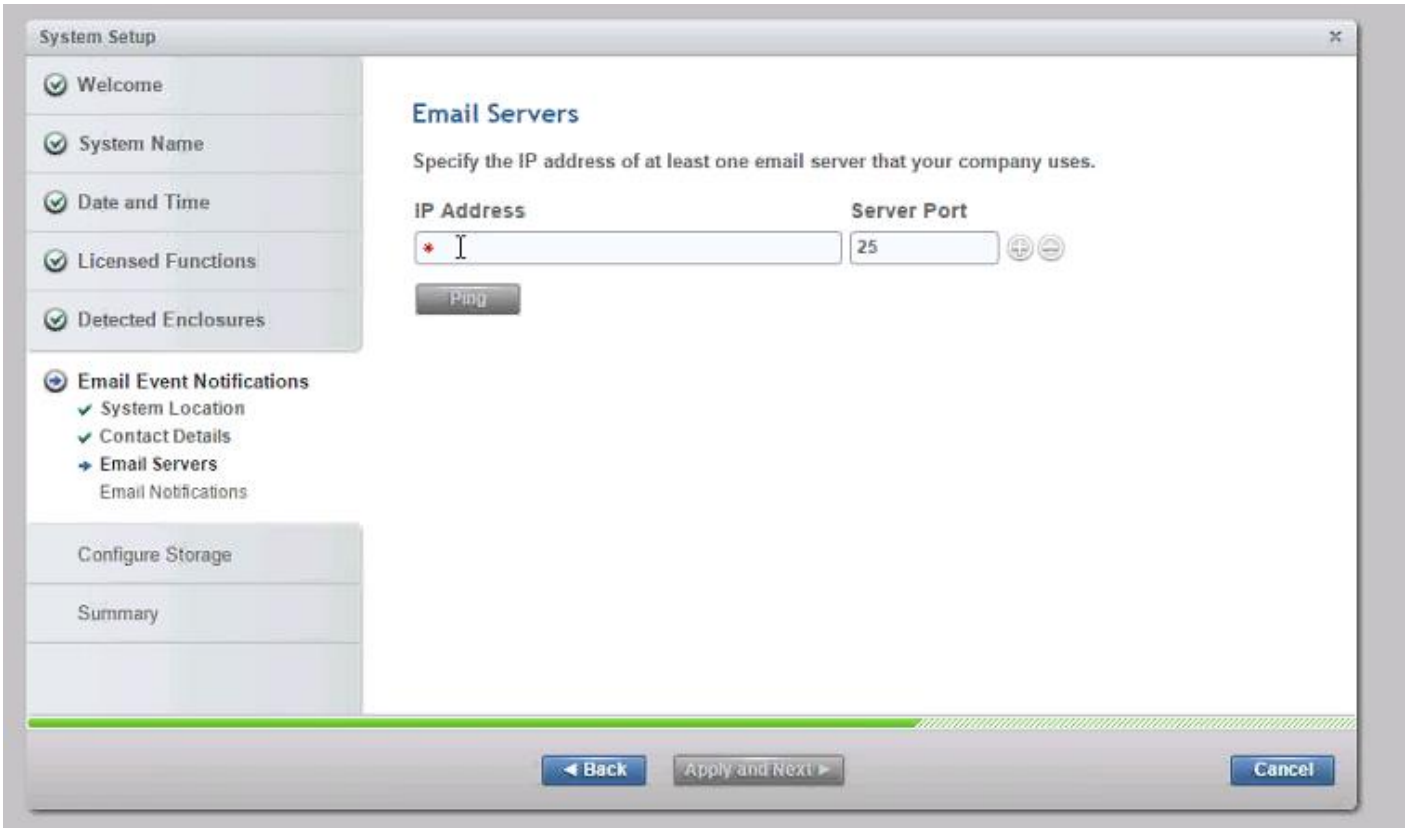
10. Fill out system location and contact details `<<var_org>> <<var_street_address>>, <<var_city>> <<var_state>> <<var_zip>> <<var_country_code>>`, then click ‘Next’.



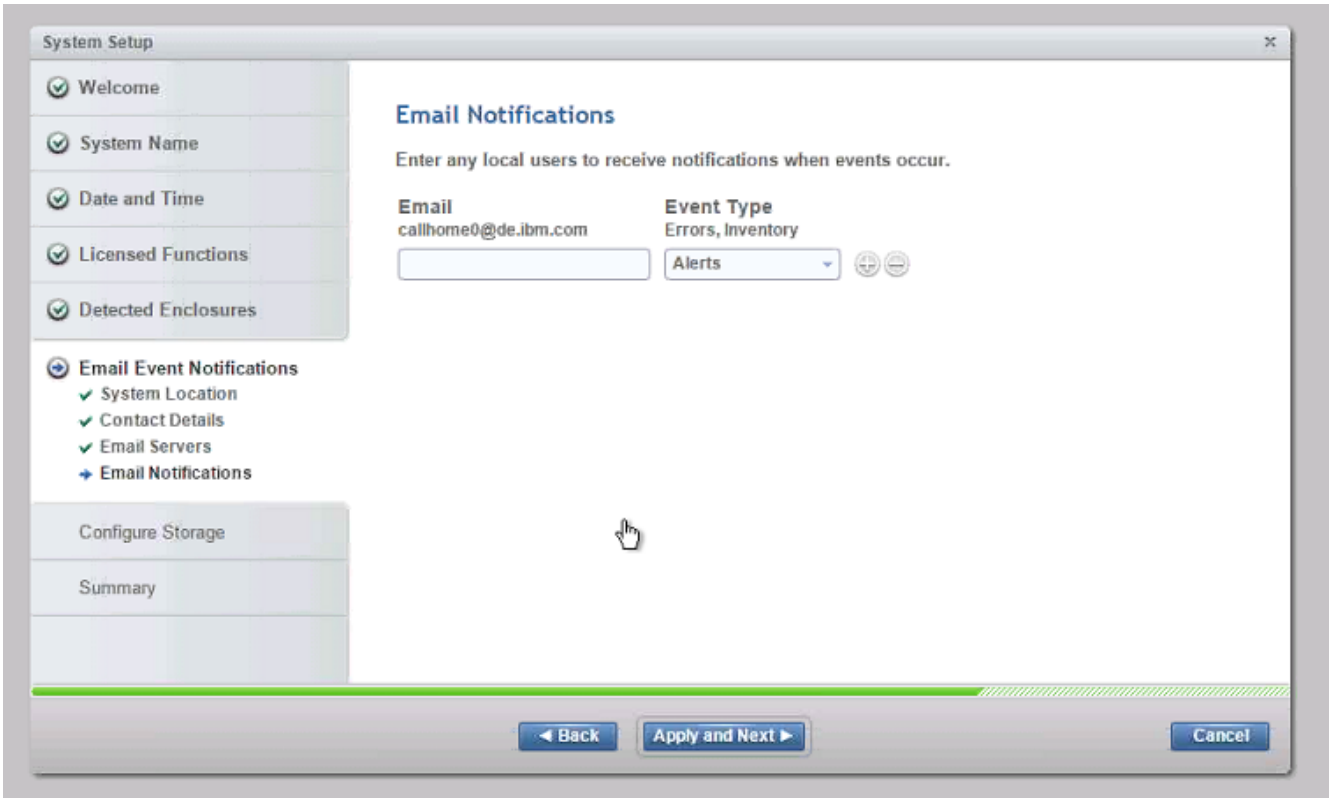
11. Insert Contact Details `<<var_contact_name>> <<var_email_contact>><<var_admin_phone>><<var_city>>` then click Apply and click ‘Next’ and click ‘Close’.



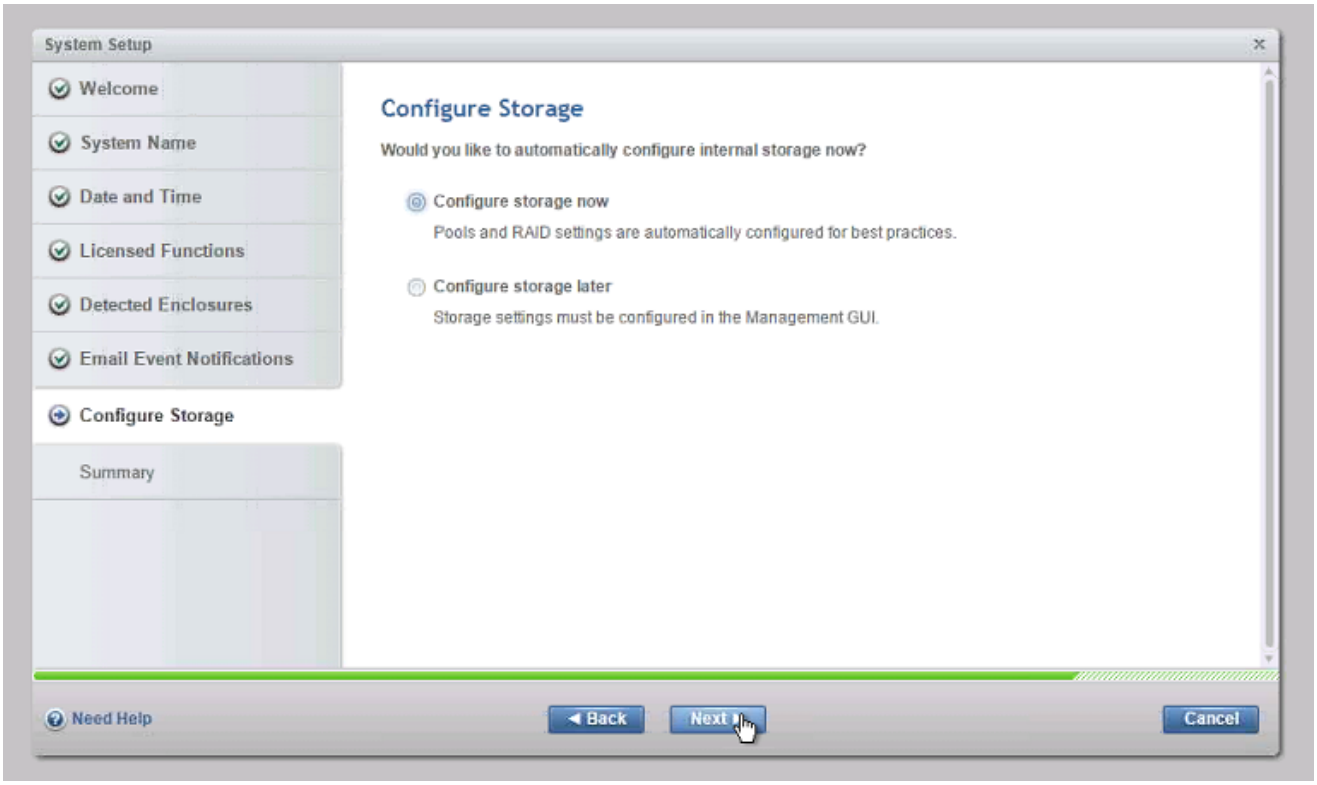
12. Input the email server IP address `<<var_mailhost_ip>>` and change the port if necessary, then click ‘Apply’ and click ‘Next’, then click ‘Close’.



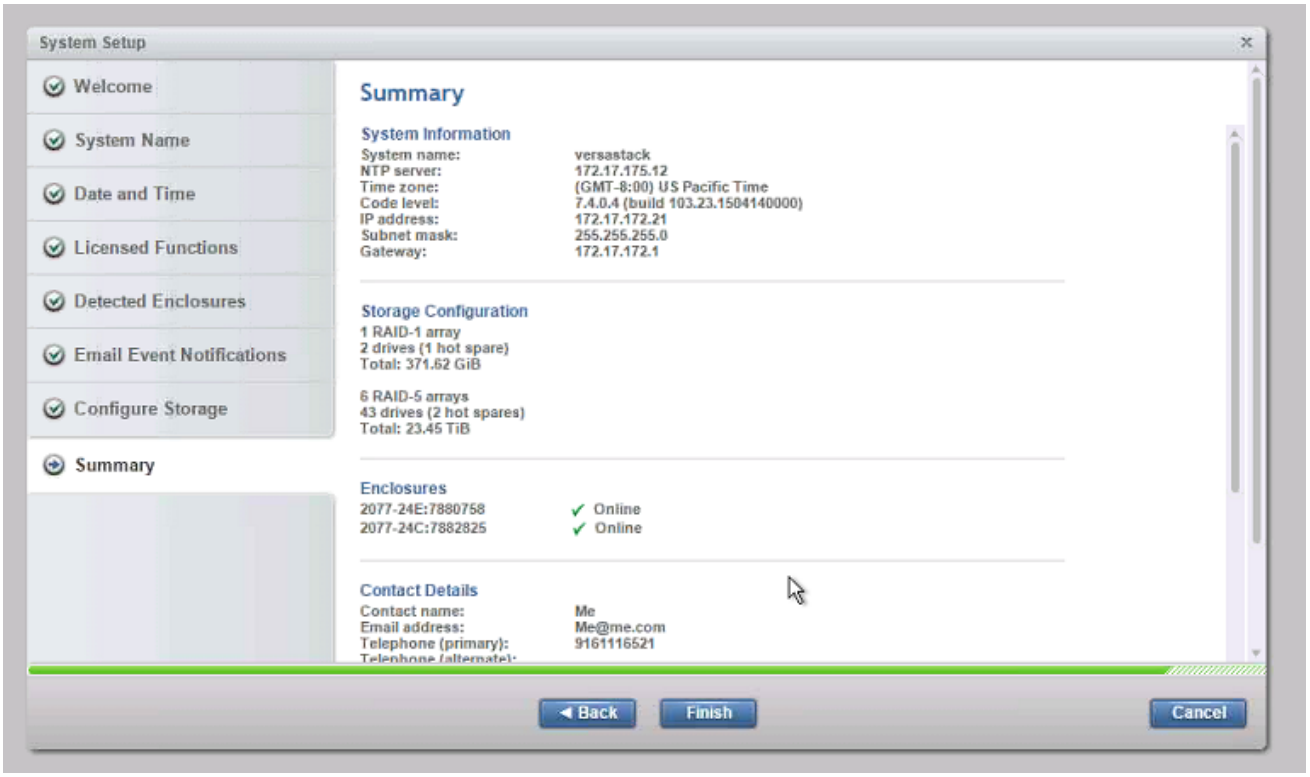
13. Enter the email addresses for all administrators that should be notified when issues occur as well and any other parties that need info or inventory `<<var_email_contact>>`. Click ‘Apply’ and click ‘Next’ then click ‘Close’.



14. Select configure storage now, and click ‘Next’.



15. Review the Summary screen and click finish, then close



16. Click Cancel to the add hosts popup as they will be added later in this document.

17. In the left side menu, hover over each of the icons to become familiar with the GUI options.

18. Select the Setting icon and choose Network.

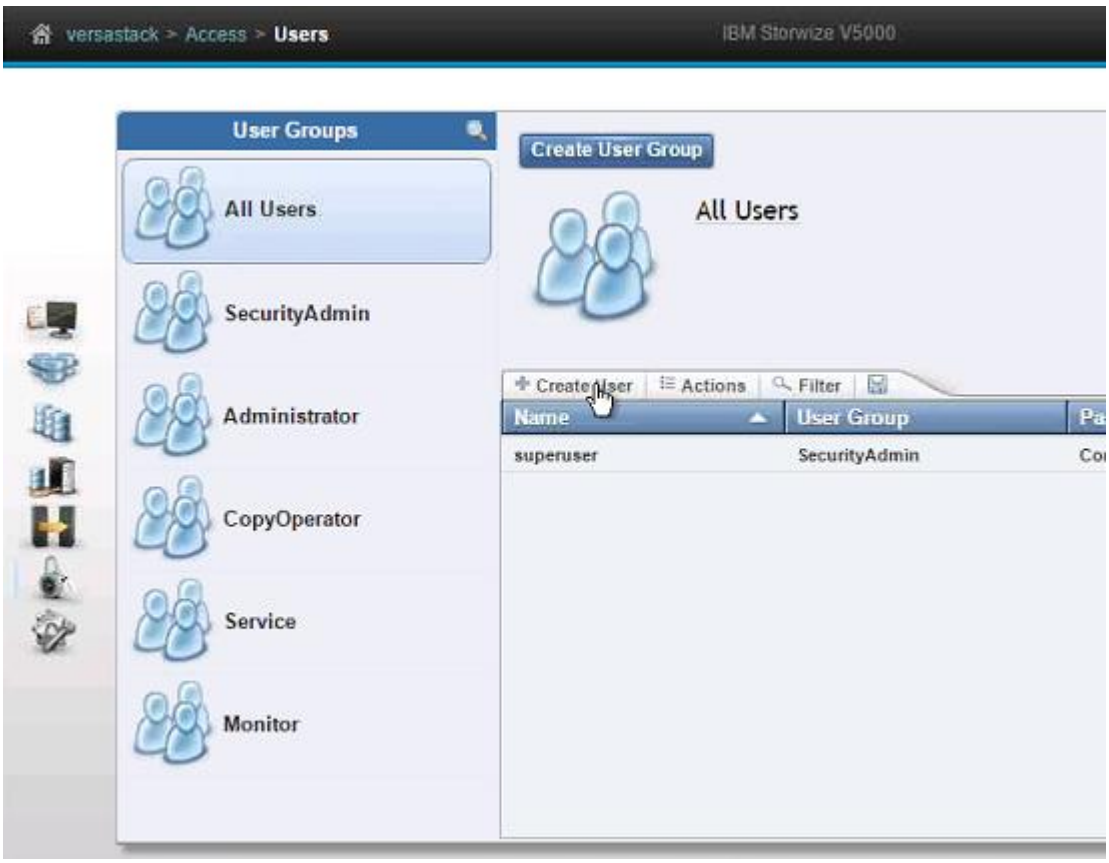
19. On the Network screen, highlight the Management IP Addresses section. Then click the number 1 interface on the left had side to bring up the Ethernet port IP menu. Change the IP address if necessary and click OK. If you are applying change to the interface you are connected to, the application will prompt you to close so it can redirect you to the new IP interface you have chosen.

20. While still on the Network screen, in the dropdown for Node Canister, switch selection to right for interface 1. Change the IP address if necessary and click OK

21. Repeat this process for interface 2 for Node Canisters left and right if you have cabled those interfaces as well.

22. Click the lock Access icon in the left pane and select Users to access the Users screen

23. Select Create User

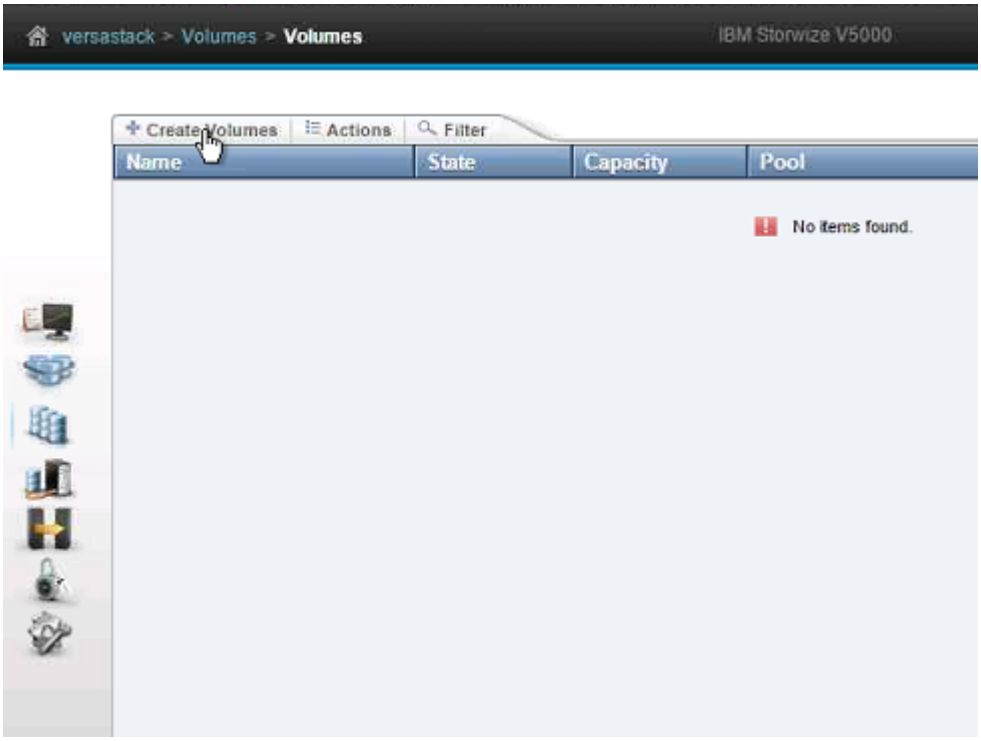


24. Enter and new name for an alternative admin account. Leave Security Admin default, and input the new password then click Create. Optionally, If you have generated an SSH Public Key on an Unix server via the command `"ssh-keygen -t rsa"` and copied that public key file to an accessible location, you can choose to associate it for this user via the Choose File button.

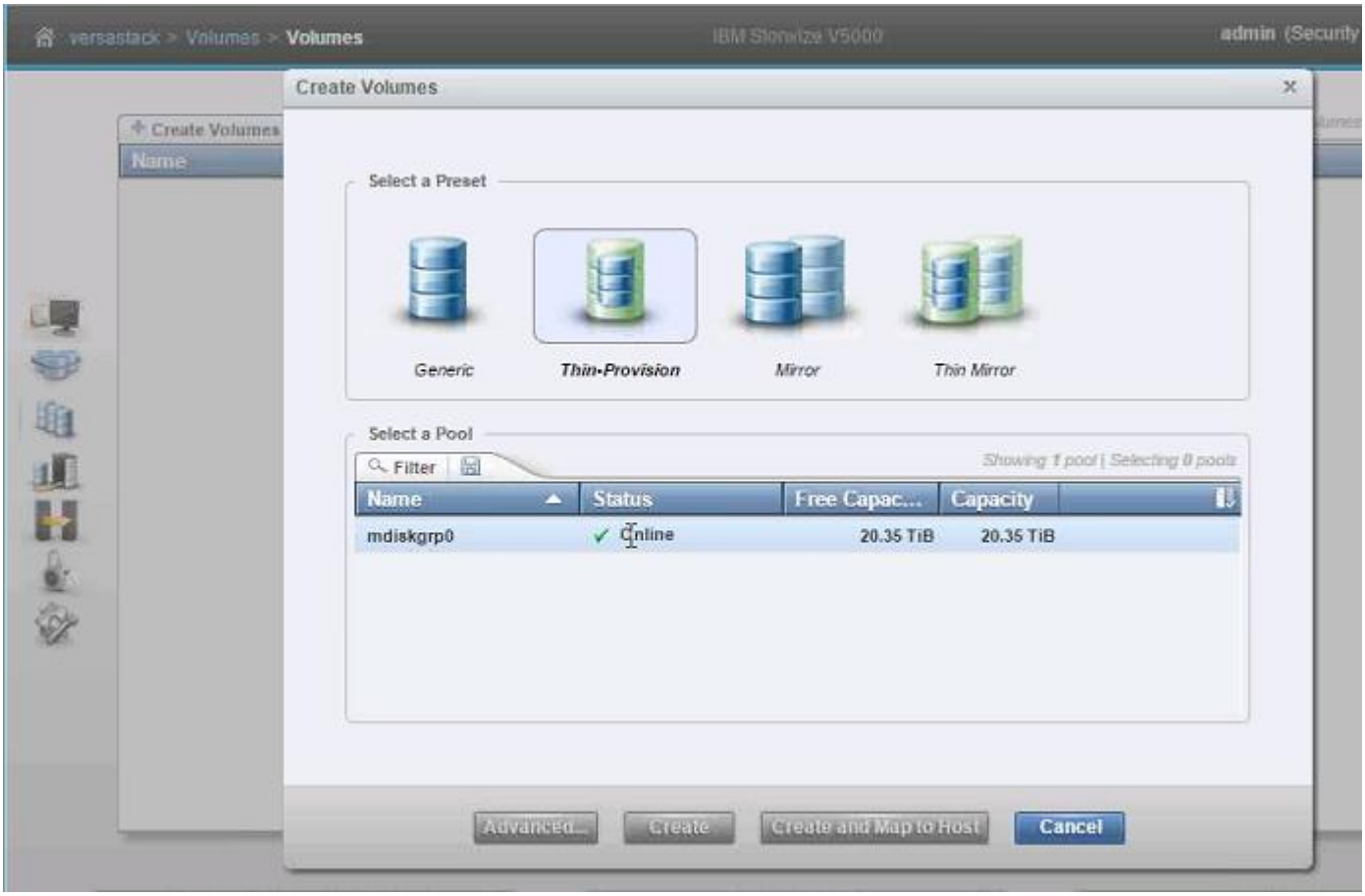
25. Logout the superuser account and log back in as the new account you created.

26. Click Cancel if you are prompted to add host or volumes, and select the Pools icon one the left screen and select Volumes.

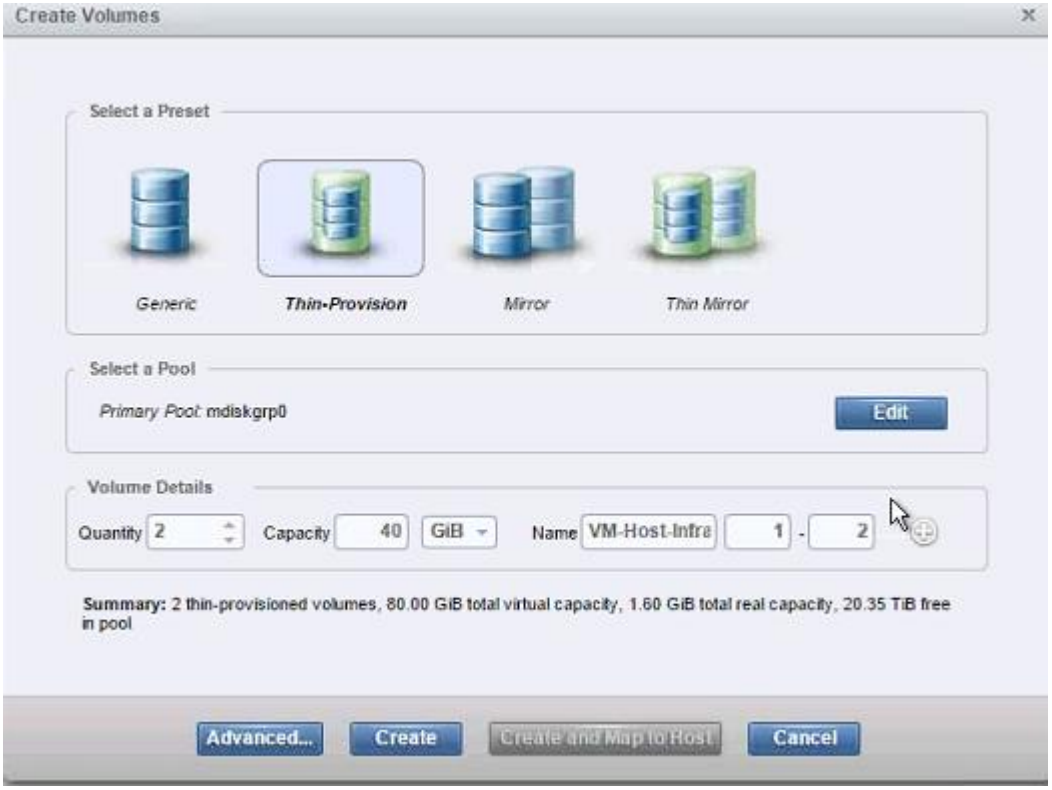
27. Click the Create Volumes selection.



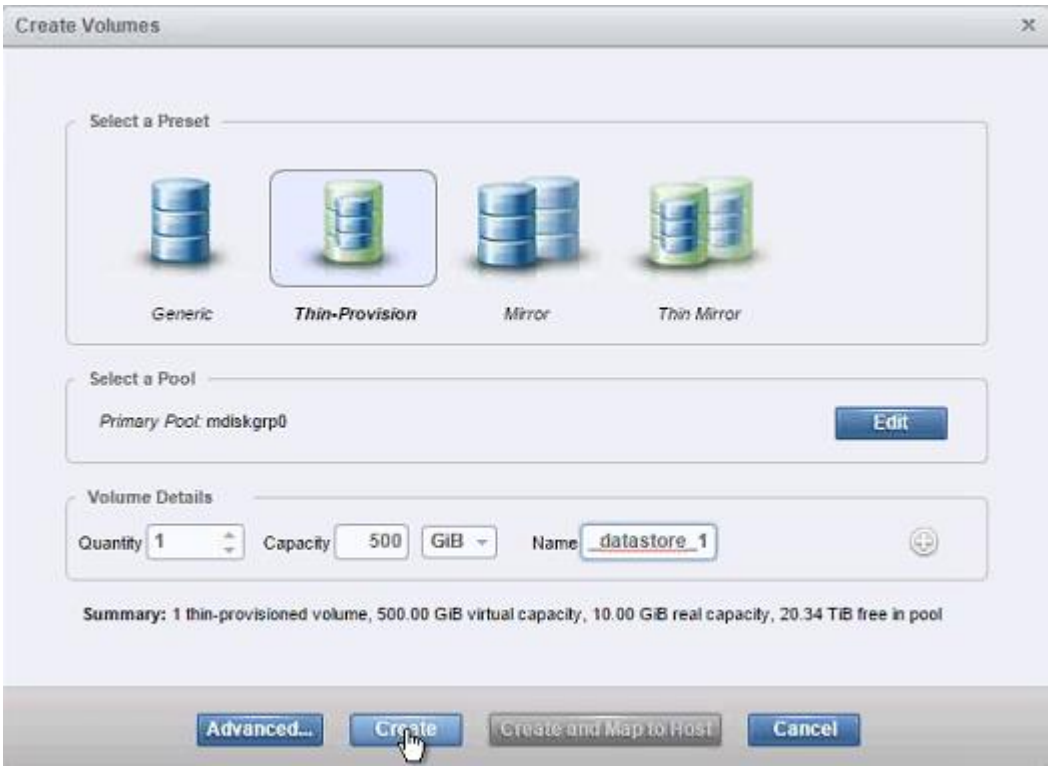
28. Select a preset that you want for the ESXi boot volume and select the Pool for the first control enclosure.



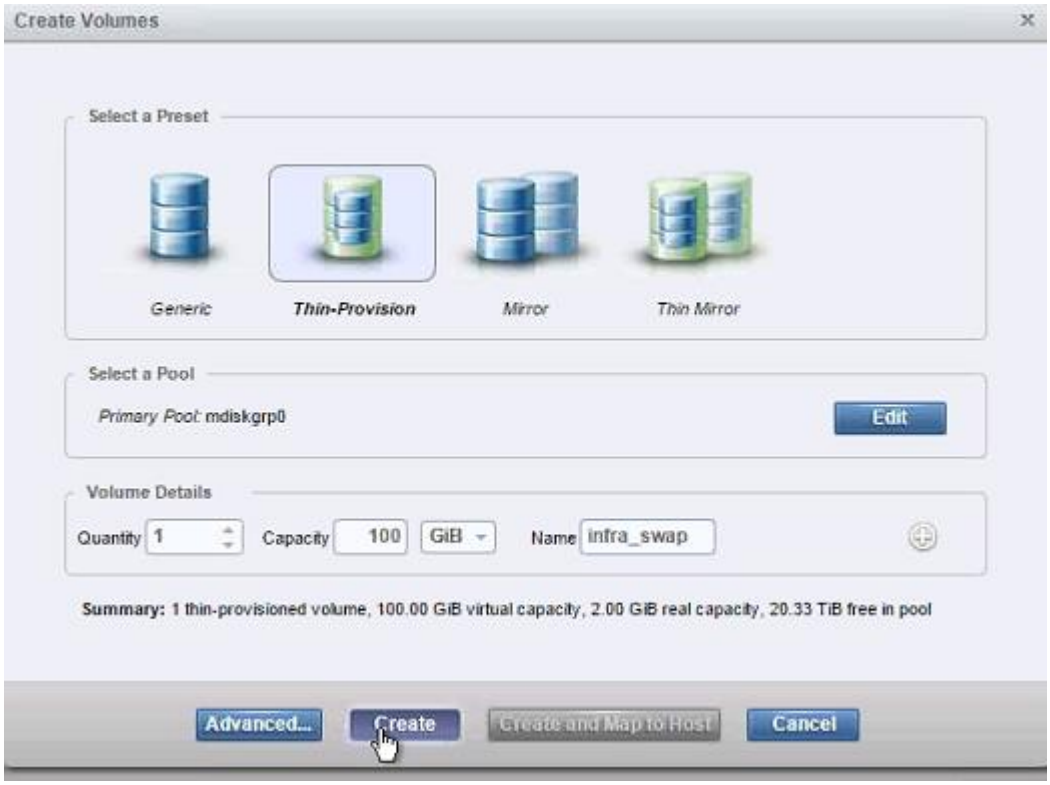
29. Input quantity 2, capacity 40GB, and name `VM-Host-Infra-0`. In addition, change the starting ID to 1. Click ‘Create’, and then click ‘Close’.



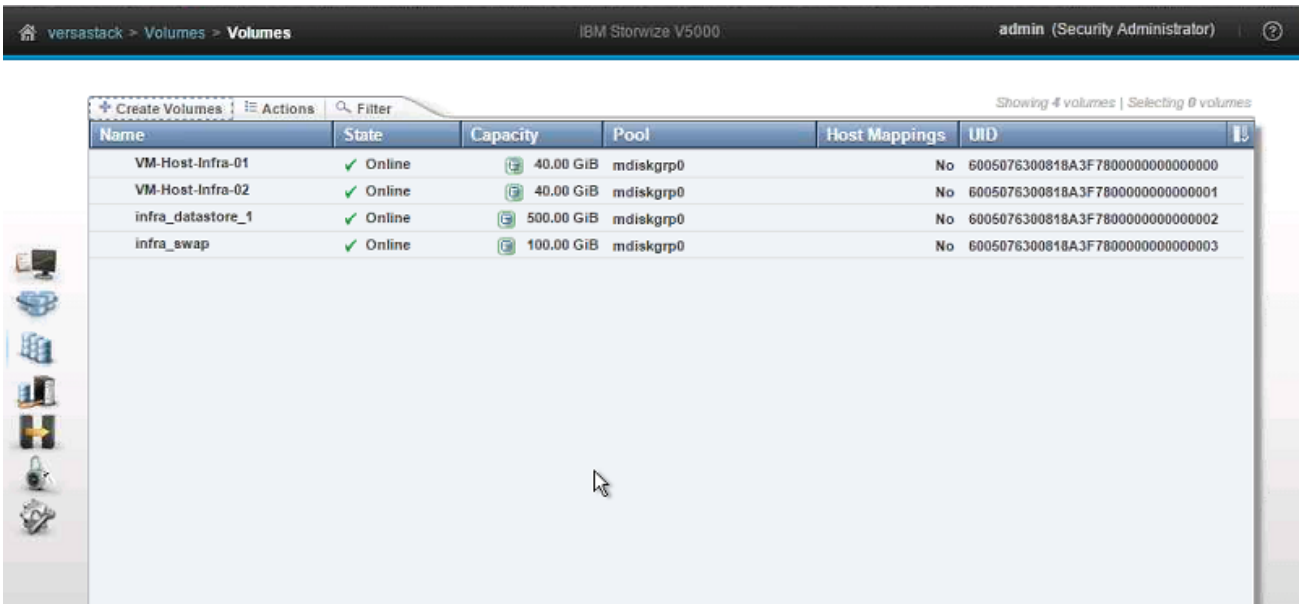
30. Click ‘Create Volume’ again and select the disk preset, and the Pool for the first enclosure. Enter quantity 1, capacity 500GB, and name `infra_datastore_1`. Click ‘Create’, and then click ‘Close’.



31. Click create volume again and select the disk preset, and the Pool for the first enclosure. Enter quantity 1, capacity 100GB, and name `infra_swap`. Click ‘Create’, and then click ‘Close’.

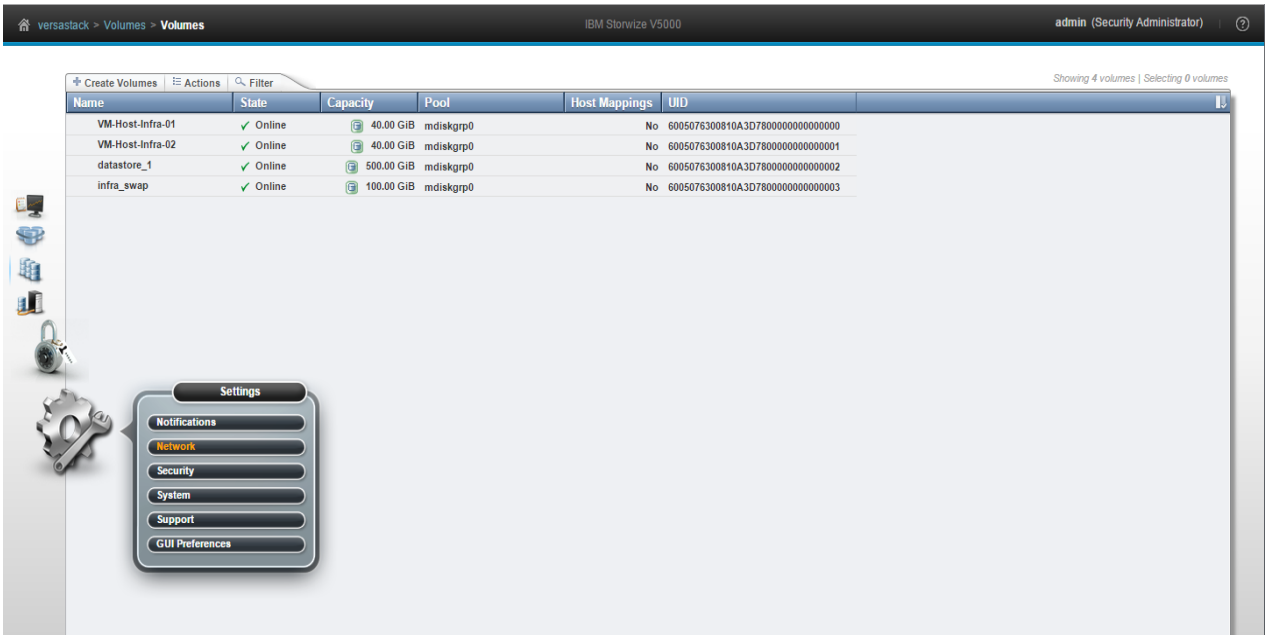


32. Validate the volumes created.

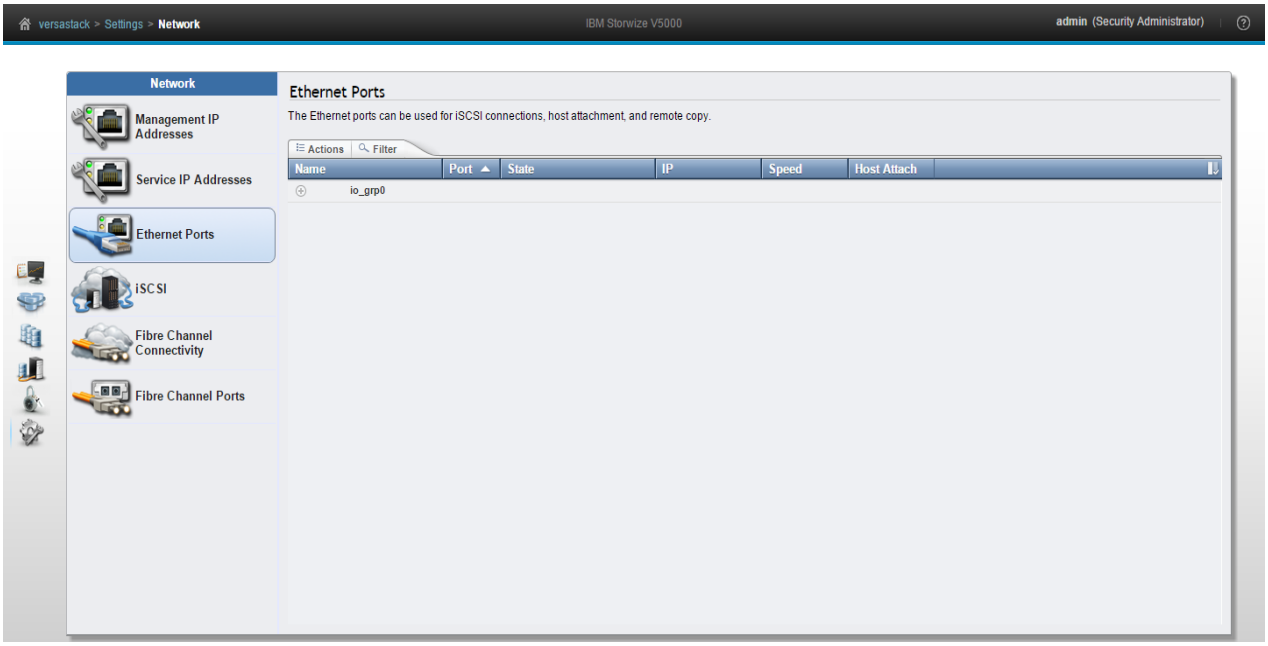


33. Configuring IBM Storwize V5000 for iSCSI host connectivity.

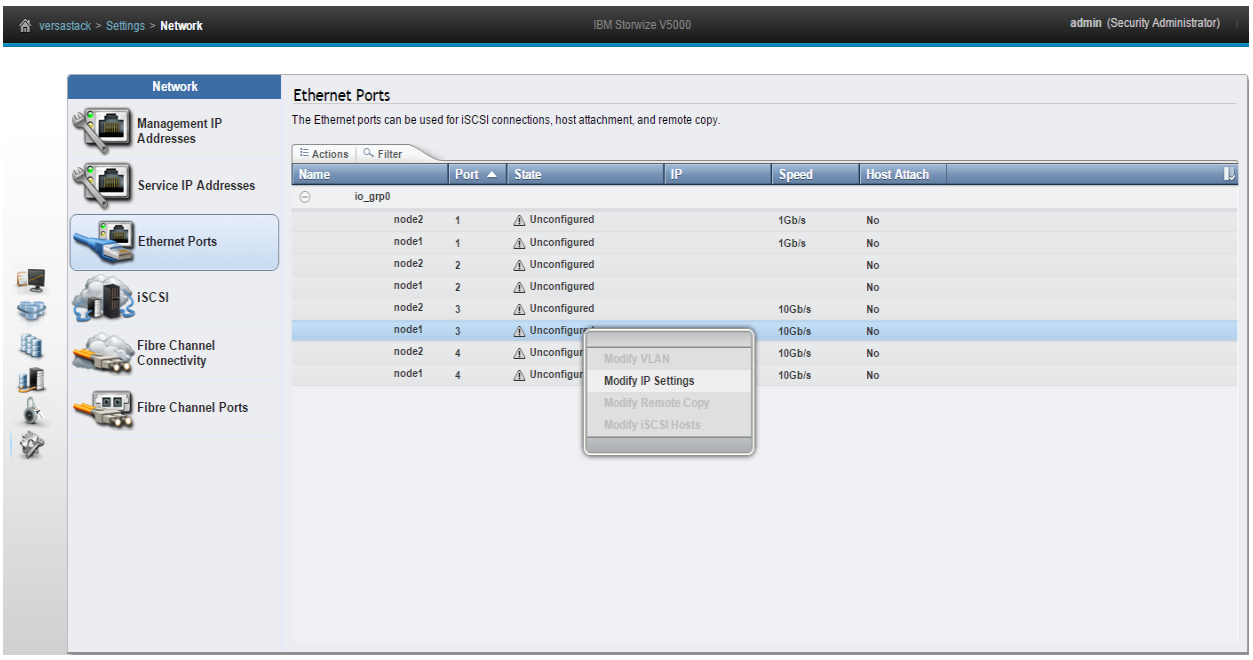
34. Go to Settings > Network.



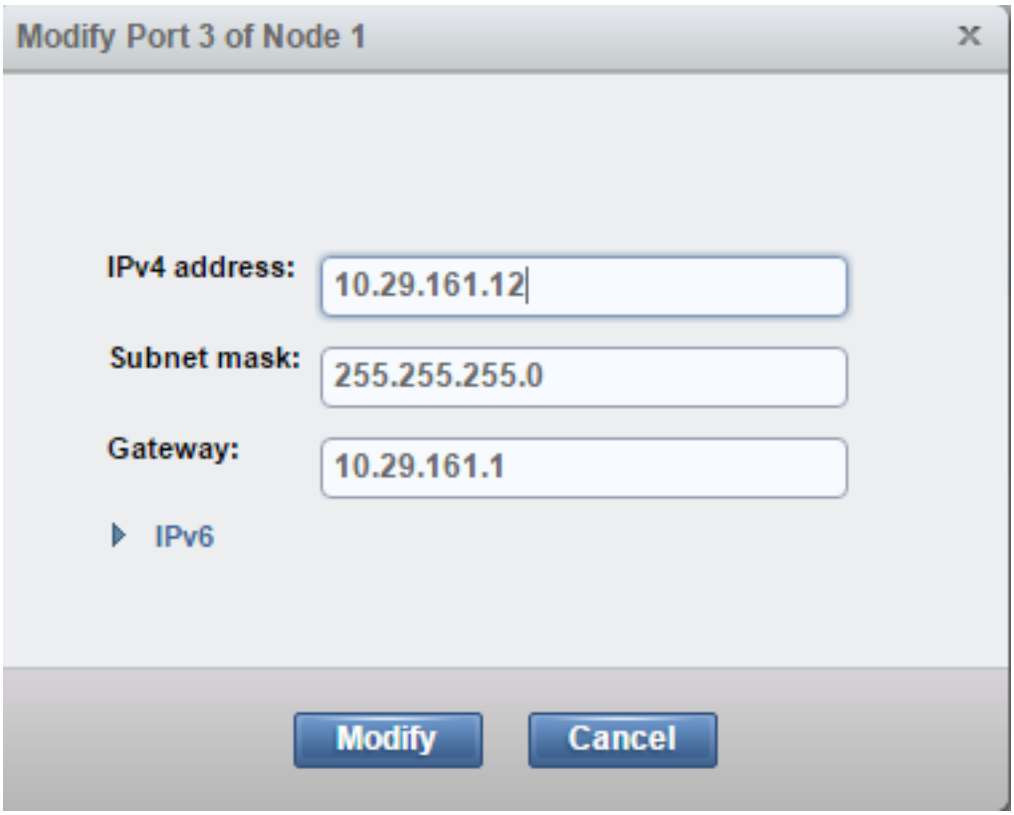
35. Select Ethernet Ports and the Ethernet port configuration view displays



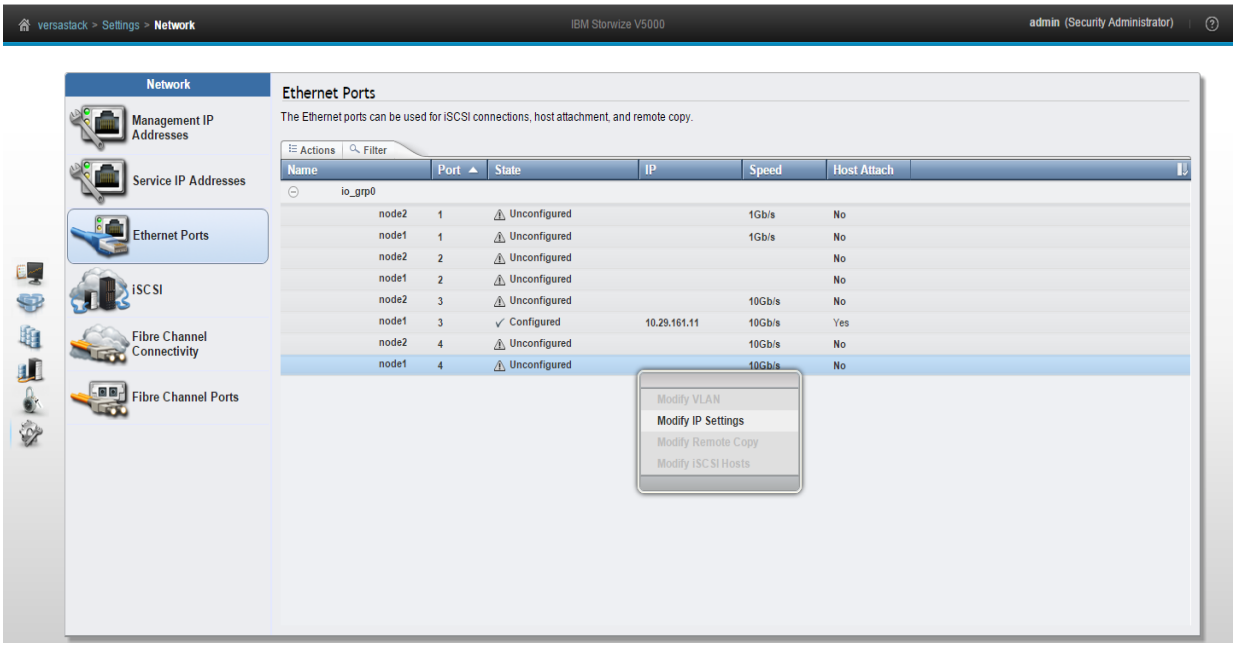
36. To configure an IP address on a node port, expand the I/O group, right-click the desired port and click Modify IP Settings



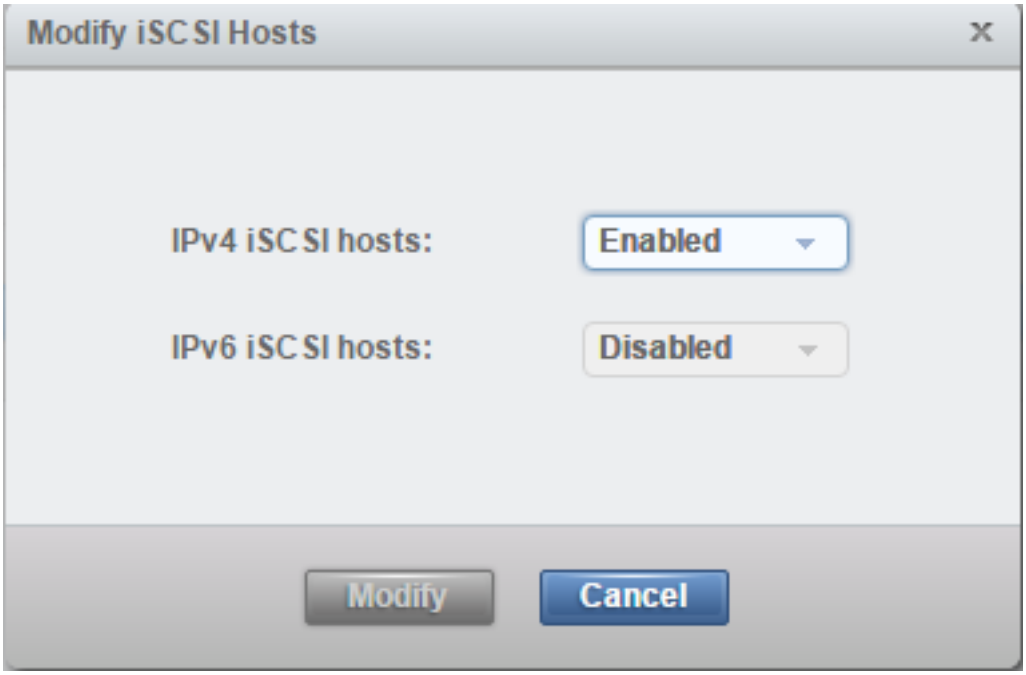
37. Configure IP address, subnet mask and gateway. It is important to make sure that these exist in the same subnet as the host IP addresses, and that the chosen address is not already in use. Click ‘Modify’ to confirm.



38. The port should now be listed as Configured.



39. If Host Attach coloum does not display yes, Right-click the configured port again. This time, the options that were previously greyed out should now be available. To confirm that the port is enabled for iSCSI, click Modify iSCSI Hosts. The window shown in Figure 4-52 displays. If the port is not enabled, do so using the drop-down box and click Modify to confirm.



40. Repeat the foregoing steps for all ports that need to be configured.

    Node 1, Port 3 & 4

    Node 2, Port 3 & 4

41. Input the IP address in a table for later use.

Table 12 IP Address Reference Table

Source	Switch/ Port	Variable	IP Address
Eth3_NodeA-fabricA	Switch A Eth1/1	<<var_node01_iscsi_Eth3_ip>>	10.29.161.11
Eth4_NodeA-fabricB	Switch B Eth1/1	<<var_node01_iscsi_Eth4_ip>>	10.29.162.11
Eth3_NodeB-fabricA	Switch A Eth1/2	<<var_node02_iscsi_Eth3_ip>>	10.29.161.12
Eth4_NodeB-fabricB	Switch B Eth1/2	<<var_node02_iscsi_Eth4_ip>>	10.29.162.12

Server Configuration

VersaStack Cisco UCS Initial Setup

Perform Initial Setup of Cisco UCS 6324 Fabric Interconnect for VersaStack Environments

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

Cisco UCS Fabric Interface 6324 A

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

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

```
Enter the configuration method: console

Enter the setup mode; setup newly or restore from backup.(setup/restore)?
Setup

You have chosen to setup a new fabric interconnect? Continue? (y/n): y

Enforce strong passwords? (y/n) [y]: y

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

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

Is this fabric interconnect part of a cluster (select 'no' for standalone)?

(yes/no) [n]: y

Which switch fabric (A|B): A

Enter the system name: <<var_ucs_clustername>>
```

```
Physical switch Mgmt0 IPv4 address: <<var_ucsa_mgmt_ip>>

Physical switch Mgmt0 IPv4 netmask: <<var_ucsa_mgmt_mask>>

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

Cluster IPv4 address: <<var_ucs_cluster_ip>>

Configure DNS Server IPv4 address? (yes/no) [no]: y

DNS IPv4 address: <<var_nameserver_ip>>

Configure the default domain name? y

Default domain name: <<var_dns_domain_name>>

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

2. Review the settings printed to the console. If they are correct, answer yes to apply and save the configuration

3. Wait for the login prompt to make sure that the configuration has been saved prior to proceeding to step 4

Cisco UCS Fabric Interconnect 6324 B

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

1. Power on the second module and connect to the console port on the second Cisco UCS 6324 fabric interconnect.

```
Enter the configuration method: console

Installer has detected the presence of a peer Fabric interconnect. This Fabric
interconnect will be added to the cluster.  Do you want to continue {y|n}? y

Enter the admin password for the peer fabric interconnect: <<var_password>>

Physical switch Mgmt0 IPv4 address: <<var_ucsb_mgmt_ip>>

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

VersaStack Cisco UCS Configuration

Log in to Cisco UCS Manager

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

1. Open a web browser and navigate to the Cisco UCS 6324 Fabric Interconnect cluster address.

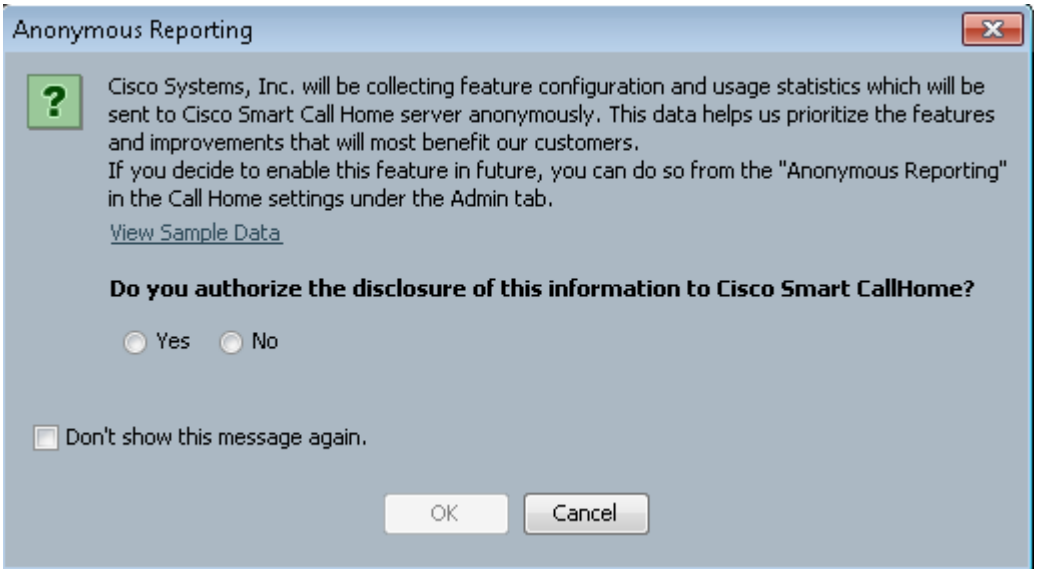
2. Select the Java or HTML Launch UCS Manager option. In this document, we will use the Java option.

3. If prompted to accept security certificates, accept as necessary.

4. When prompted, enter admin as the user name and enter the administrative password. `<<var_password>>`

5. Click Login to log in to Cisco UCS Manager.

6. Enter the information for the Anonymous Reporting if desired and click OK.



Upgrade Cisco UCS Manager Software to Version 3.0(2d)

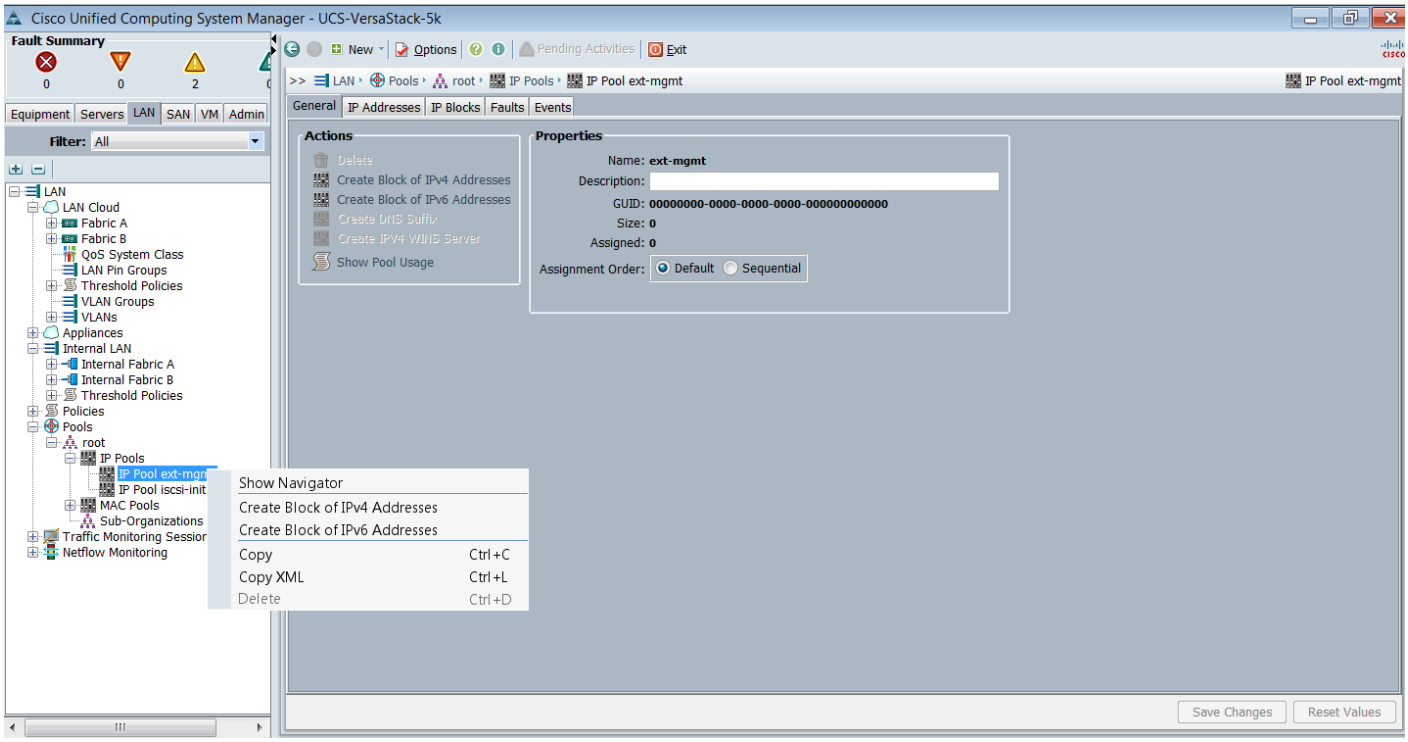
This document assumes the use of Cisco UCS Manager Software version 3.0(2d). To upgrade the Cisco UCS Manager software and the UCS 6324 Fabric Interconnect software to version 3.0(2d), refer to Cisco UCS Manager Install and Upgrade Guides.

Add Block of IP Addresses for Out-of-band 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:

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

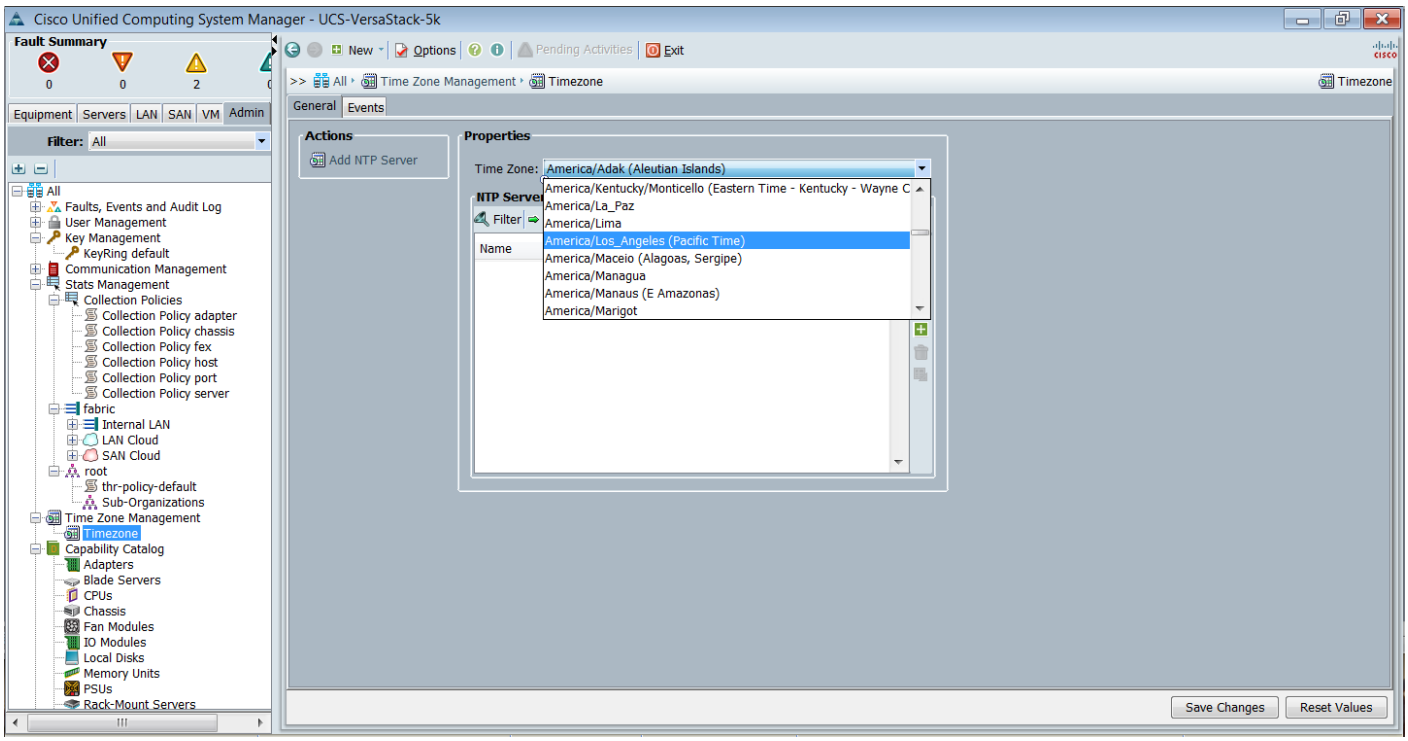
1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Pools > root > IP Pools > IP Pool ext-mgmt.
3. In the Actions pane, select Create Block of IP Addresses.
4. Enter the starting IP address of the block and the number of IP addresses required, and the subnet and gateway information.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



Synchronize Cisco UCS to NTP

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

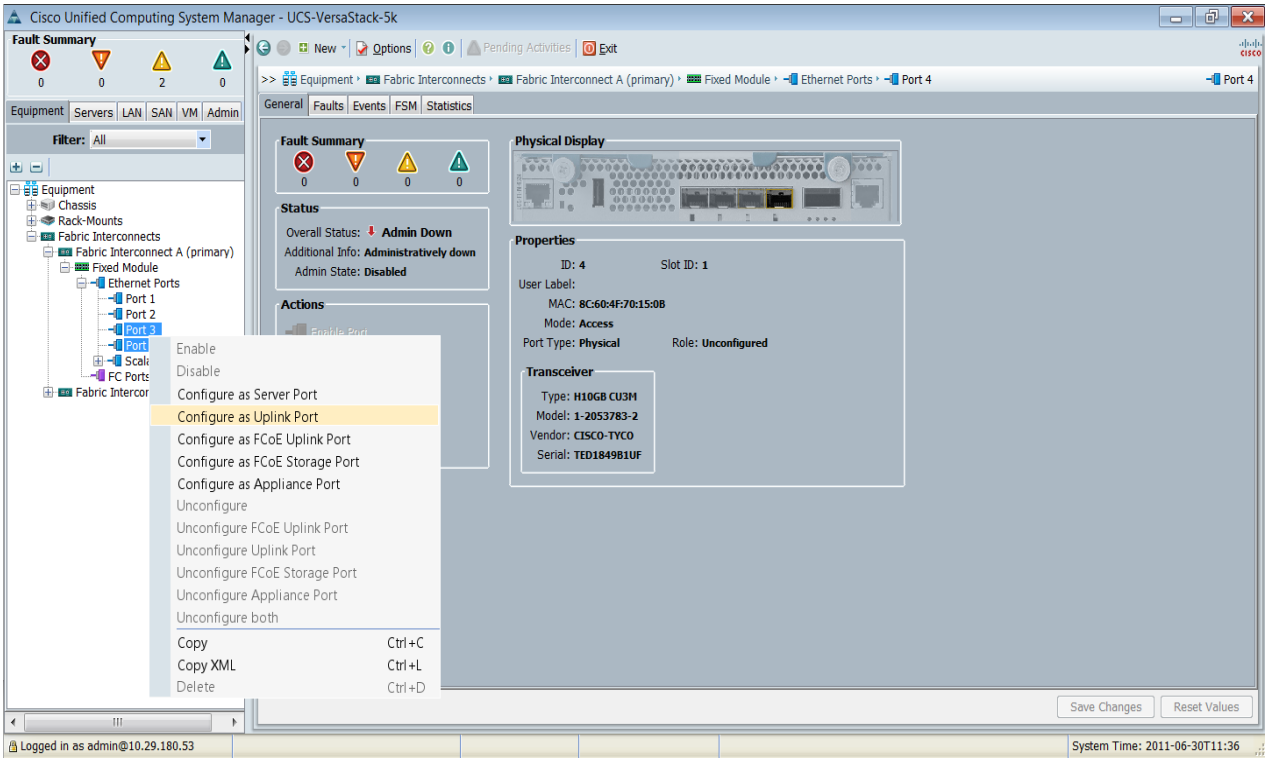
1. In Cisco UCS Manager, click the Admin tab in the navigation pane.
2. Select All > Timezone Management.
3. In the Properties pane, select the appropriate time zone in the Timezone menu.
4. Click Save Changes, and then click OK.
5. Click Add NTP Server.
6. Enter `<<var_global_ntp_server_ip>>` and click OK.
7. Click OK.



Enable Uplink Ports

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

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



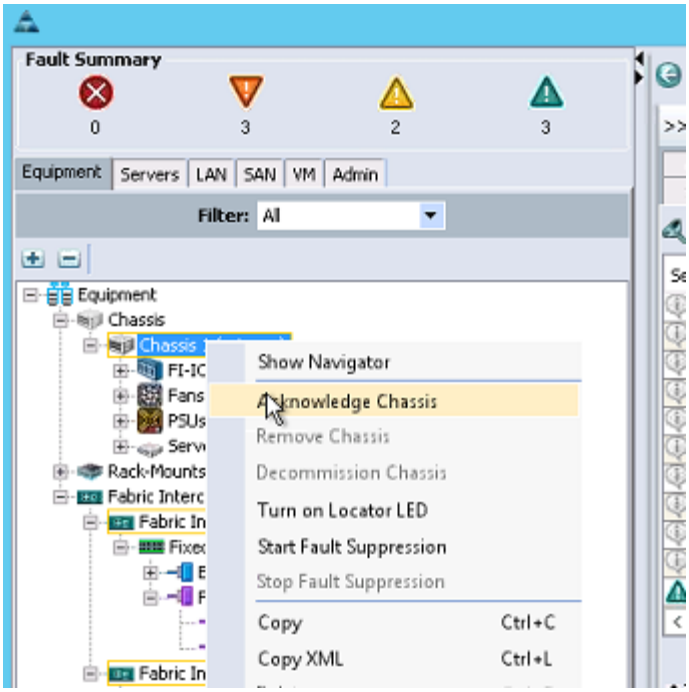
5. Click Yes to confirm uplink ports and click OK.
6. In the left pane, navigate to Fabric Interconnect A and select Fixed Module.
7. In the right pane, navigate to the Ethernet Ports tab. Confirm that ports have been configured correctly in the IfRole column.
8. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.
9. Expand Ethernet Ports.
10. Select ports 3 and 4 that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.
11. Click Yes to confirm the uplink ports and click OK.
12. In the left pane, navigate to Fabric Interconnect A and select Fixed Module.
13. In the right pane, navigate to the Ethernet Ports tab. Confirm that ports have been configured correctly.

Scalability port 5 will need to be selected to verify any C series server ports.

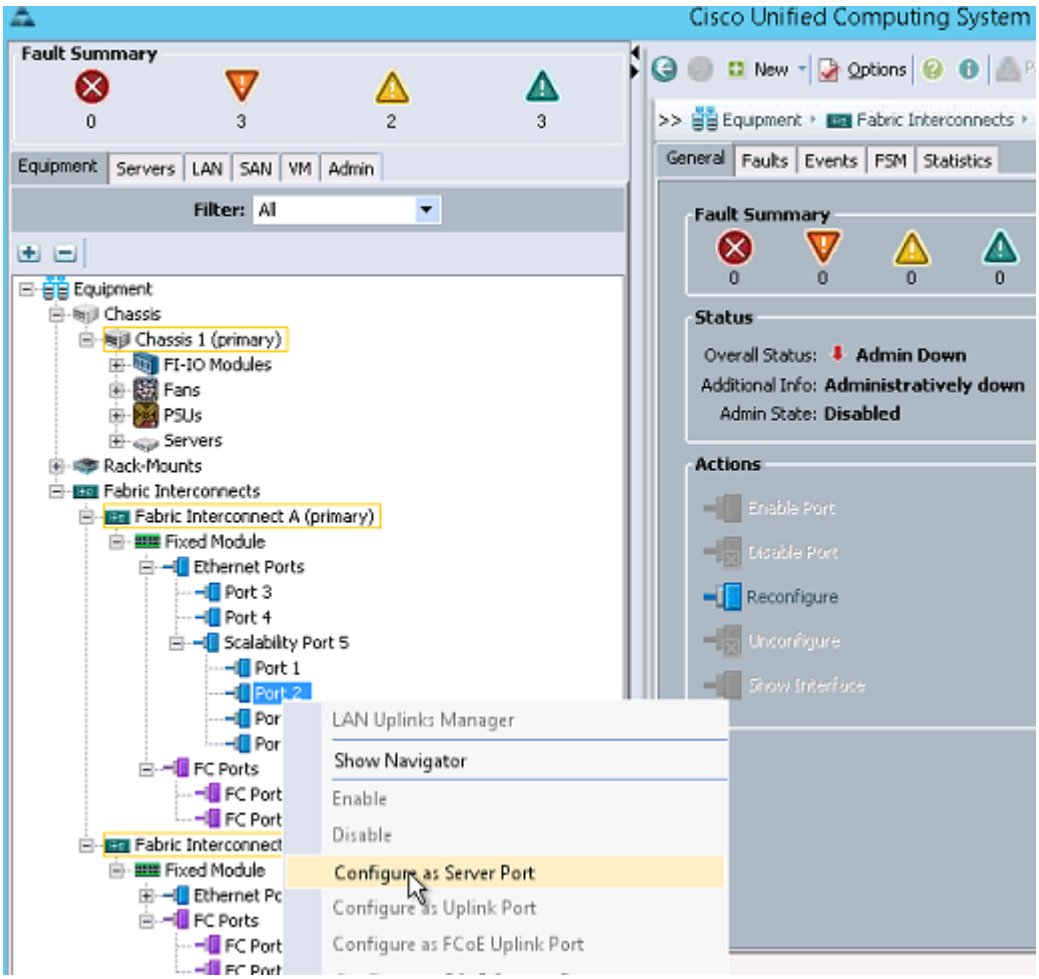
Acknowledge Cisco UCS Chassis and configure Scalability ports

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

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



4. If you have rack servers installed, expand the Fabric Interconnects.
5. Expand Fabric Interconnect A, then Fixed Module.
6. Expand Ethernet ports.
7. Expand Scalability ports and select the port that is connected to the rack server.
8. Right-click to configure the port as a server port and make sure it is enabled.



9. Repeat this process for each port connected to rack servers for Fabric A, then repeat for the Fabric Interconnect B Scalability ports.

Configure Uplink Port Channels to Cisco Nexus Switches

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

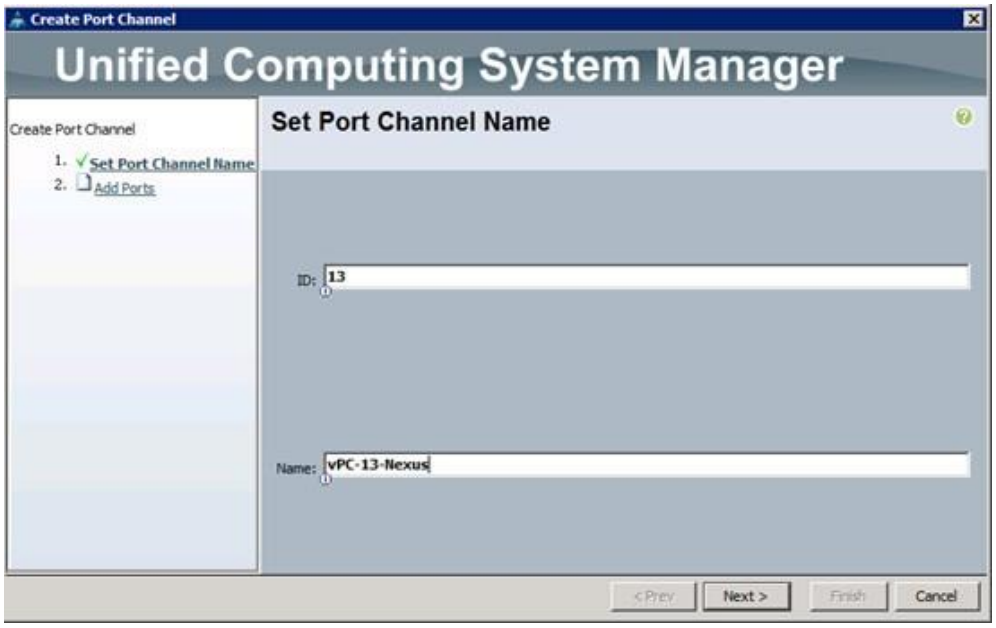
1. In Cisco UCS Manager, click the LAN tab in the navigation pane.

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

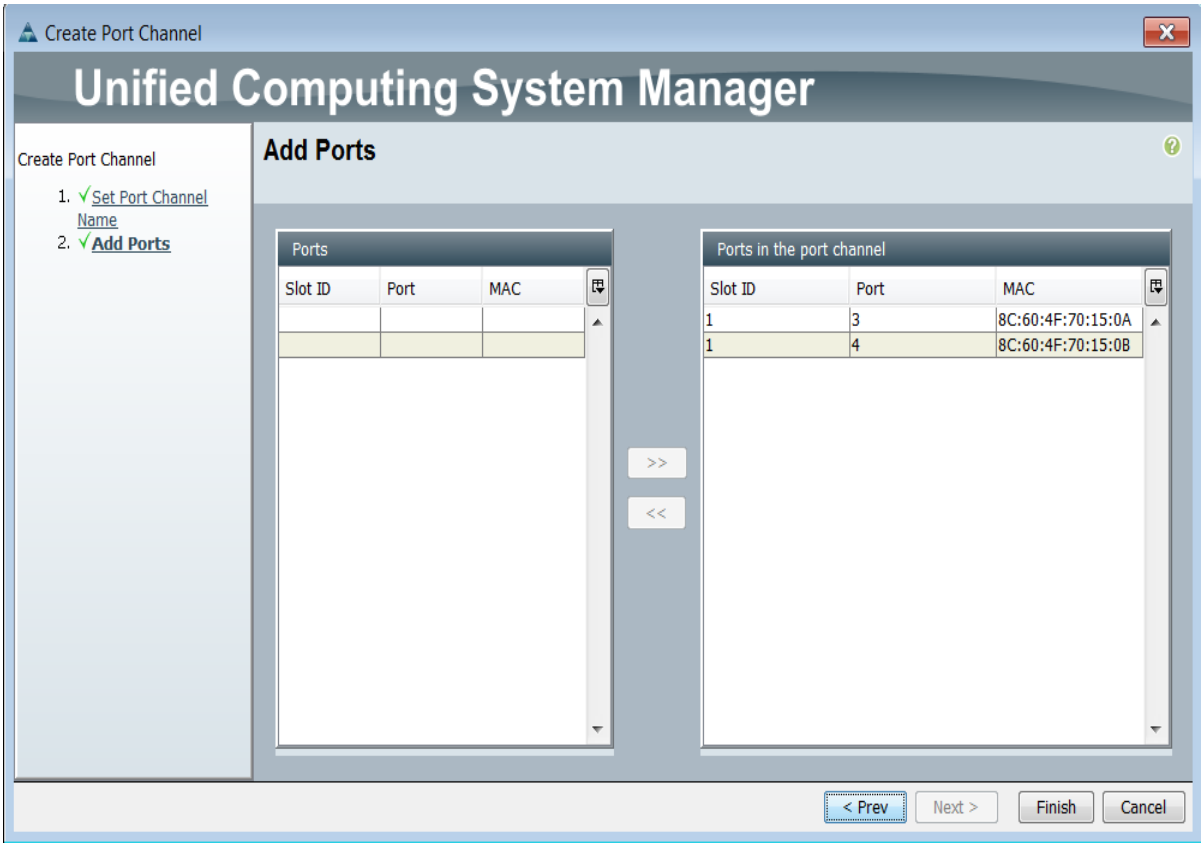
---

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

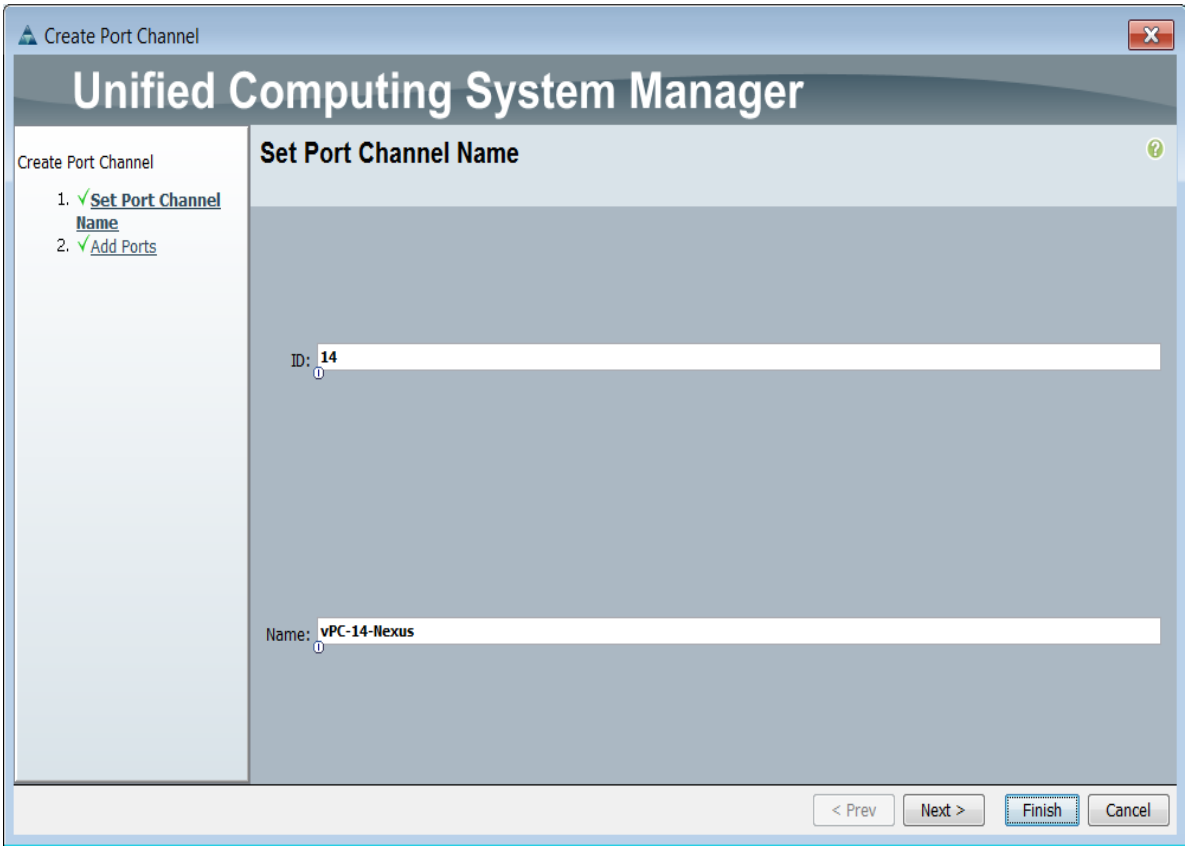
7. Click Next.



8. Select the following ports to be added to the port channel:
   - Slot ID 1 and port 3
   - Slot ID 1 and port 4
9. Click >> to add the ports to the port channel.



10. Click Finish to create the port channel.
11. Click OK.
12. In the navigation pane, under LAN > LAN Cloud, expand the fabric B tree.
13. Right-click Port Channels.
14. Select Create Port Channel.
15. Enter 14 as the unique ID of the port channel.
16. Enter `vPC-14-Nexus` as the name of the port channel.



17. Click Next.
18. Select the following ports to be added to the port channel:
    - Slot ID 1 and port 3
    - Slot ID 1 and port 4
19. Click >> to add the ports to the port channel.
20. Click Finish to create the port channel.
21. Click OK.

Create MAC Address Pools

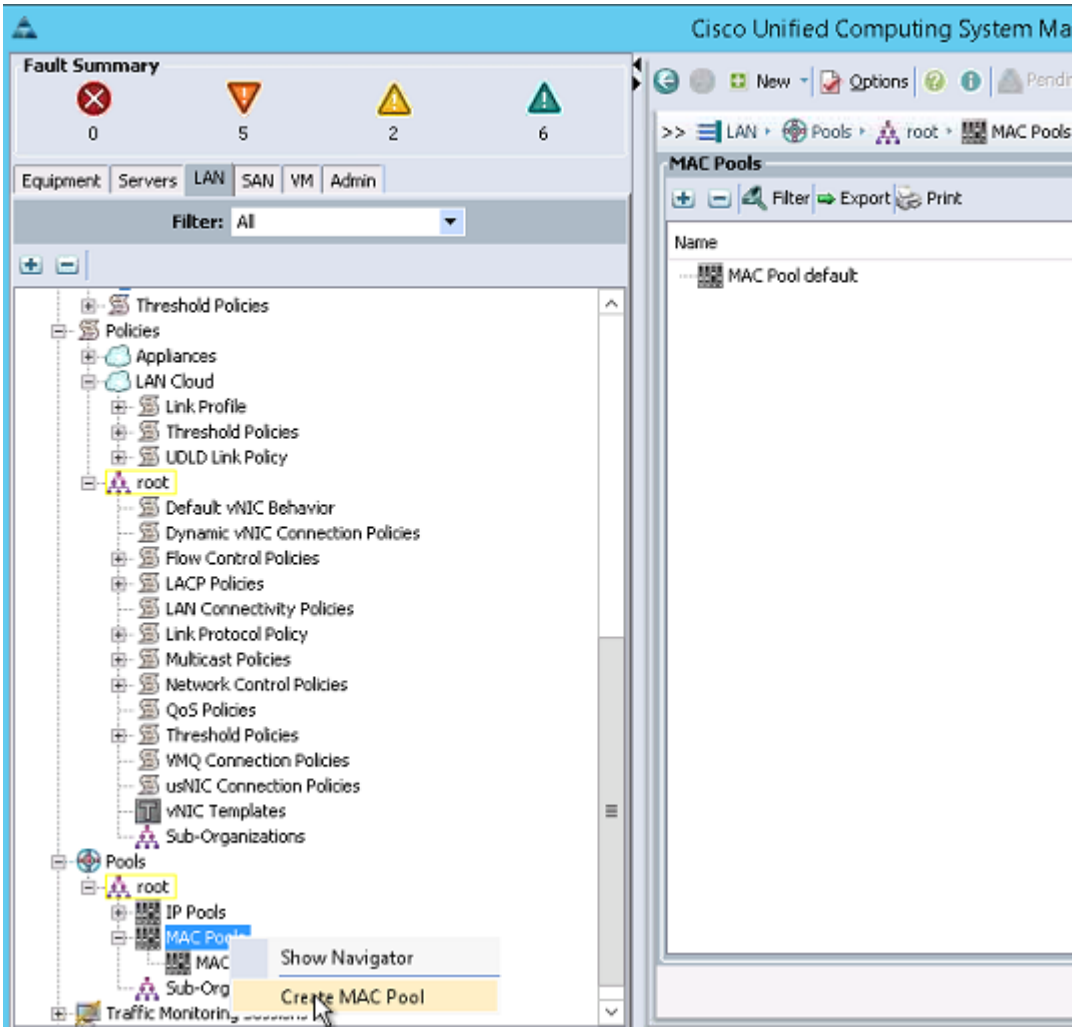
To configure the necessary MAC address pools for the Cisco UCS environment, complete the following steps:

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

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

3. Right-click MAC Pools under the root organization.

4. Select Create MAC Pool to create the MAC address pool.



5. Enter `MAC_Pool_A` as the name of the MAC pool.

6. Optional: Enter a description for the MAC pool.

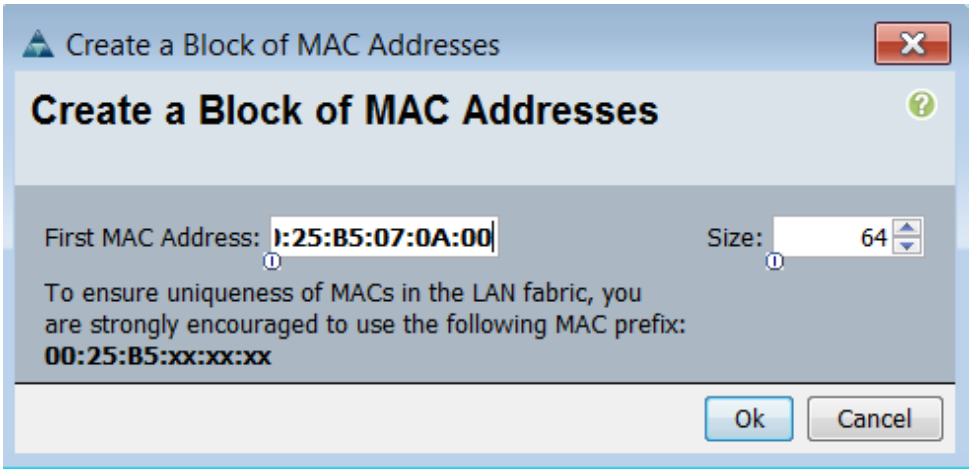
7. Click Next.

8. Click Add.

9. Specify a starting MAC address.

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

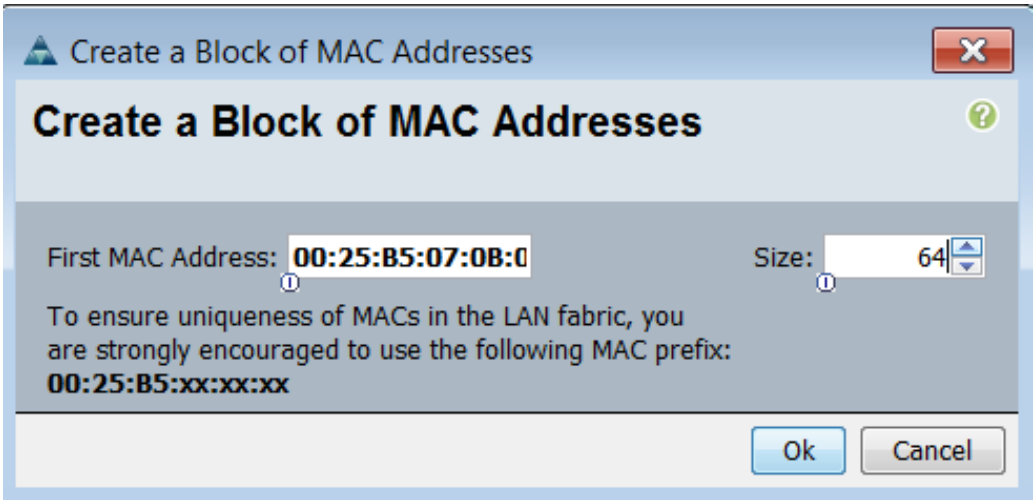
10. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources.



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

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

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

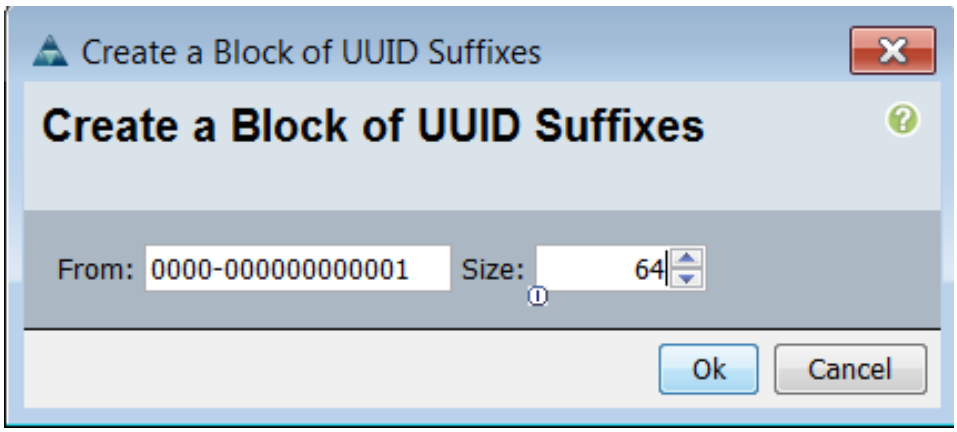


22. Click OK.
23. Click Finish.
24. In the confirmation message, click OK.

Create UUID Suffix Pool

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

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

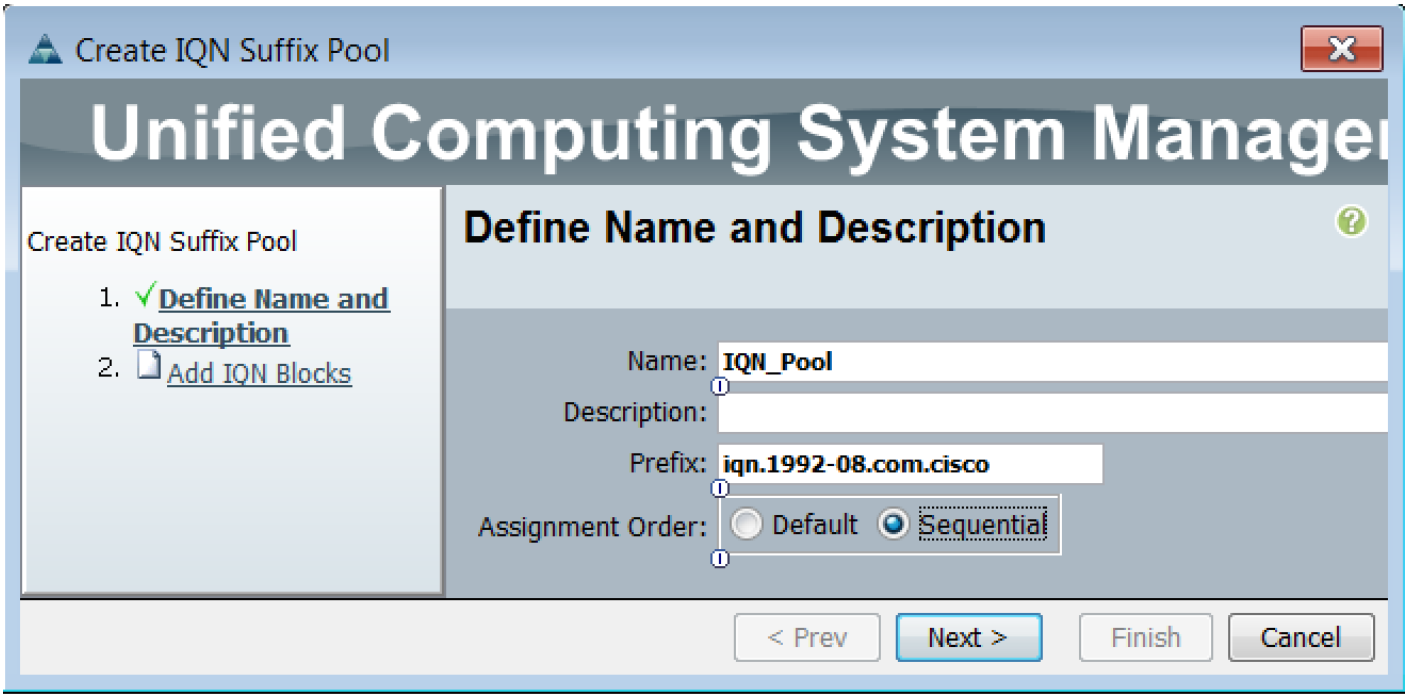


12. Click OK.
13. Click Finish.
14. Click OK.

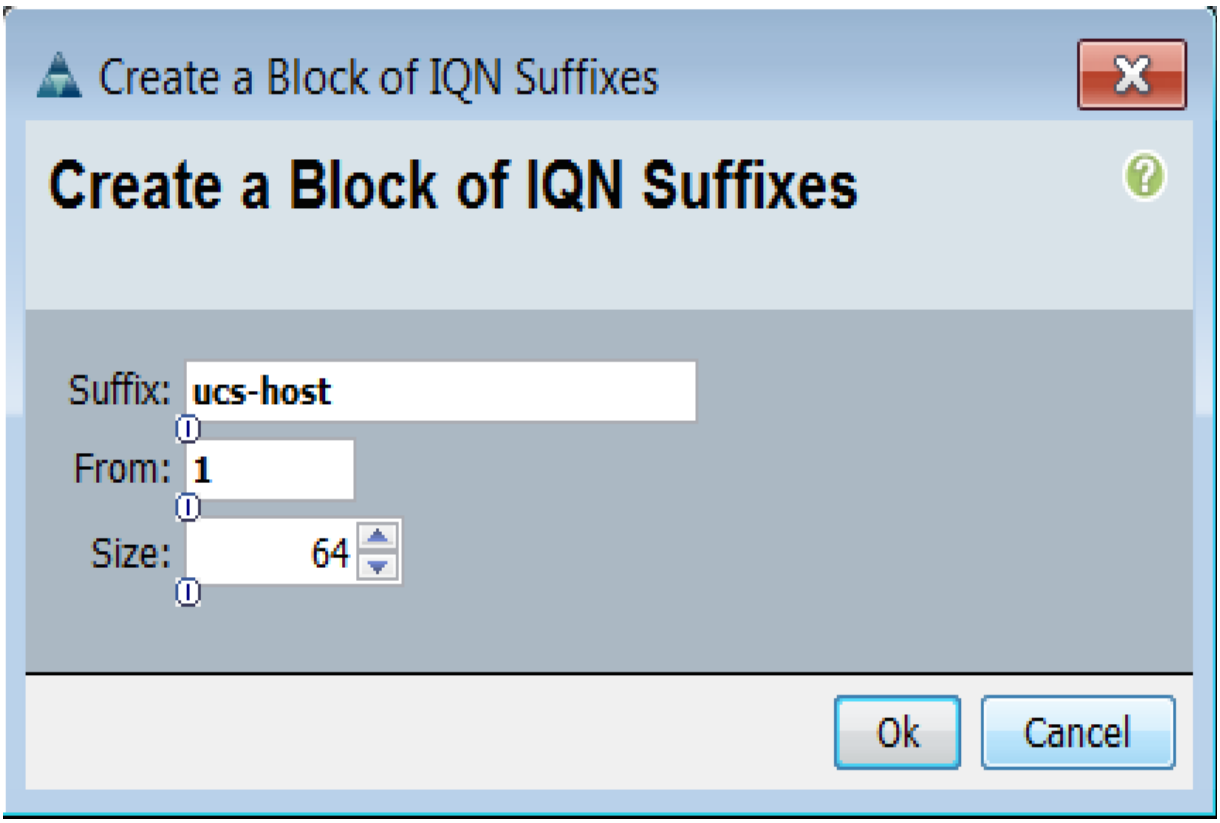
Create iSCSI IQN Pool

To configure the necessary IQN pool for the local site Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Expand Pools > root.
3. Right-click IQN Pools.
4. Select Create IQN Suffix Pool.
5. Enter `IQN_Pool` as the name for IQN pool.
6. Optional: Add a description for the IQN pool.
7. Enter `iqn.1992-08.com.cisco` as the Prefix.
8. Select Sequential for the Assignment Order.



9. Click Next.
10. Click Add to add a block of IQNs.
11. Enter `ucs-host` for the Suffix.
12. Enter 1 for From.
13. Enter a size appropriate to your environment.

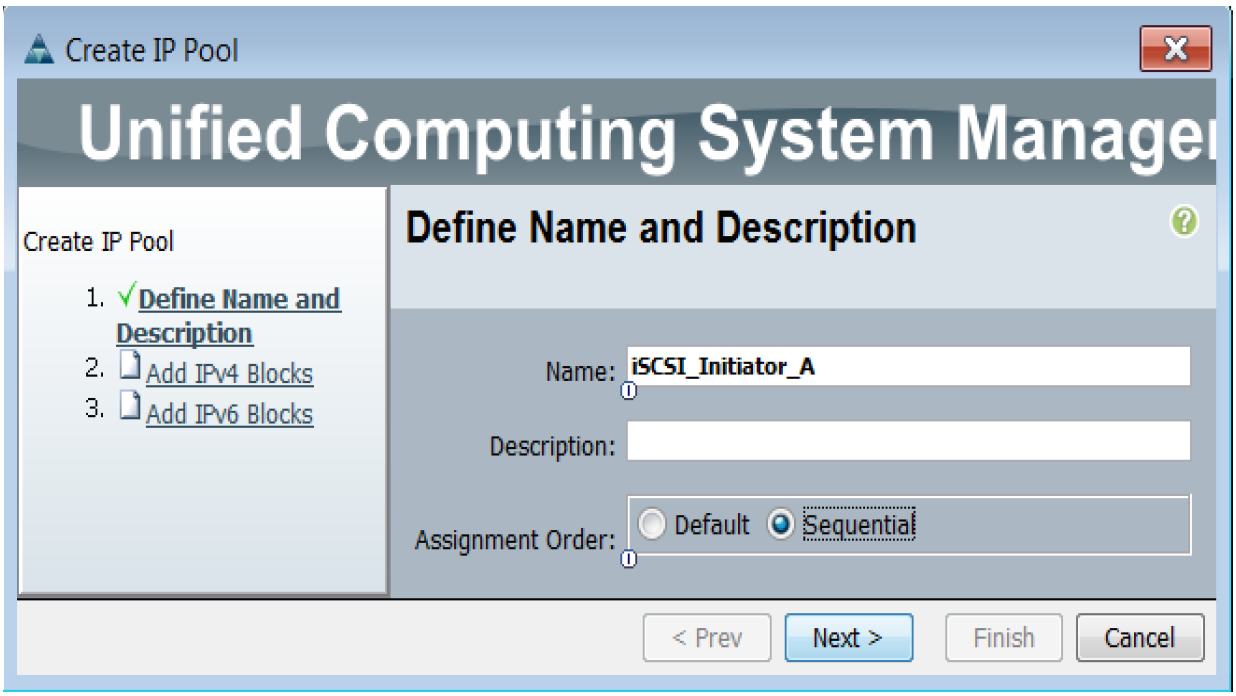


14. Click OK.
15. Click Finish.
16. Click OK.

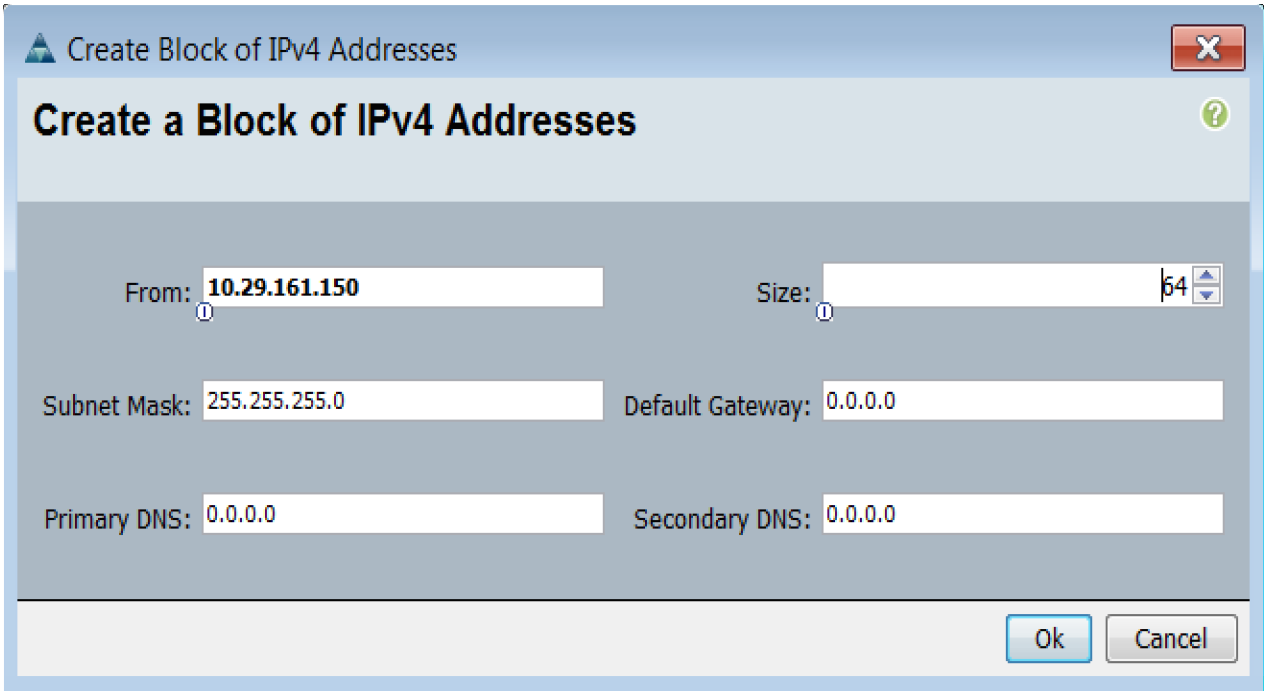
Create iSCSI Initiator IP Address Pools

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

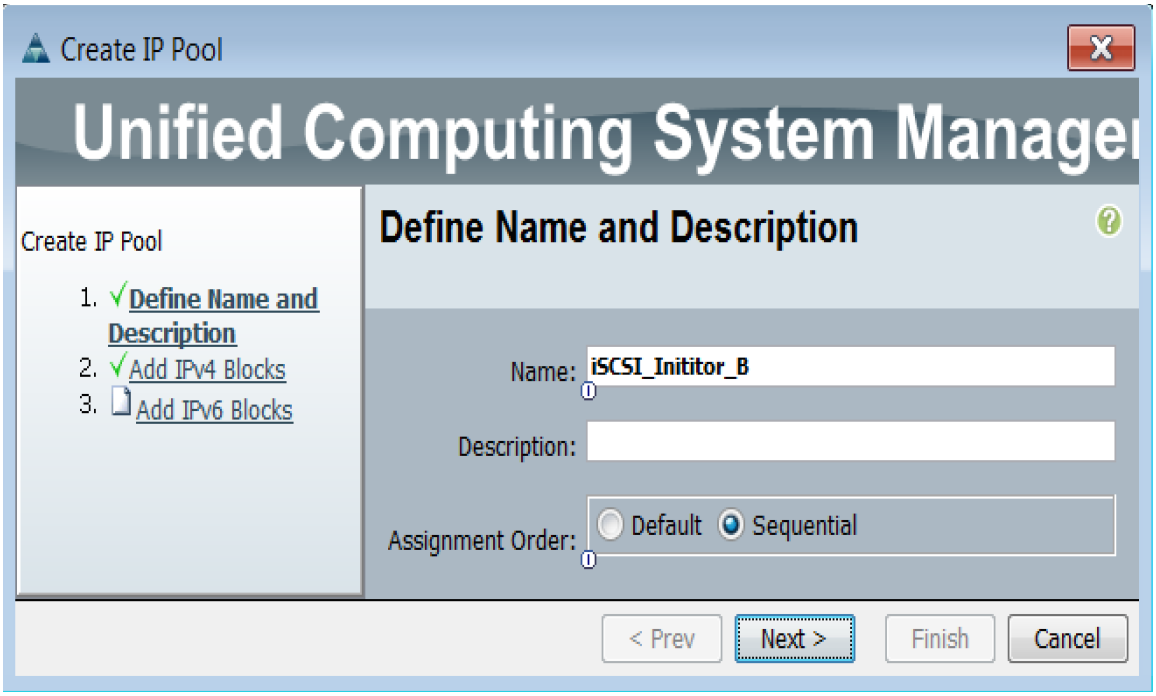
1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Expand Pools > root.
3. Right-click IP Pools.
4. Select Create IP Pool.
5. Enter `iSCSI_Initiator_A` as the name for the IP pool.
6. Optional: Add a description for the IP pool.
7. Select Sequential for the Assignment Order.



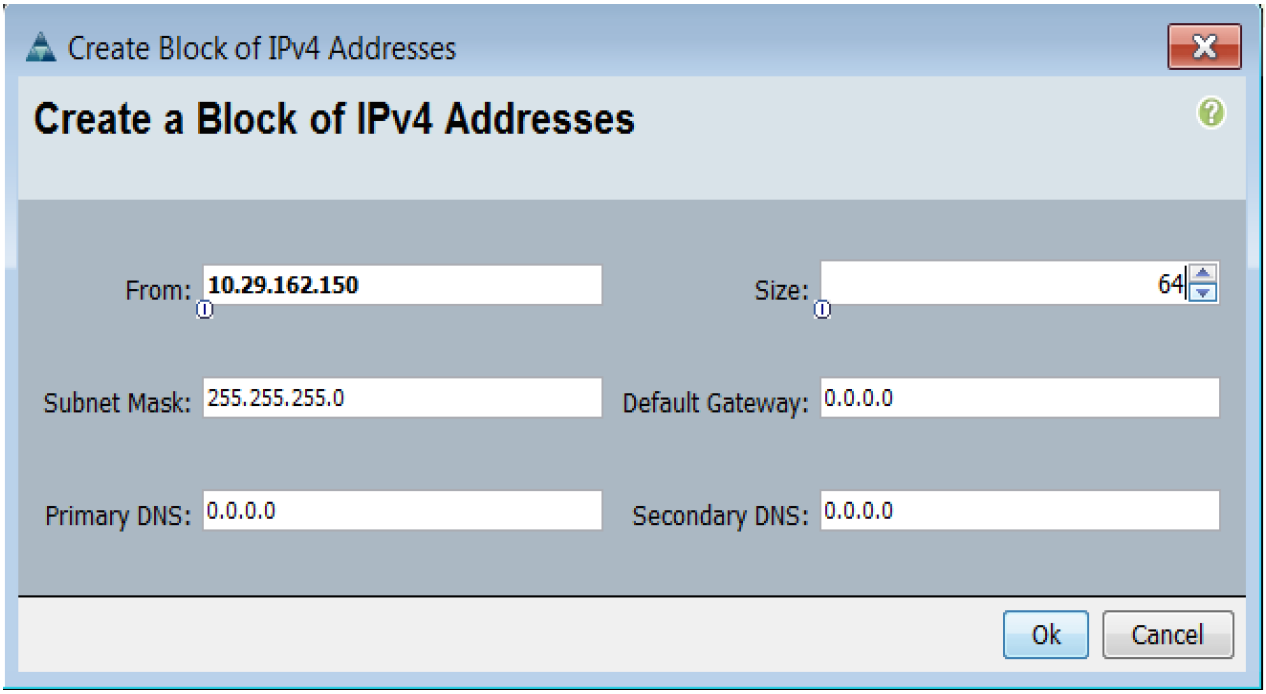
8. Click Next.
9. Click Add to add a Block of IPs.
10. Enter a starting IP address in the subnet from the site iSCSI A VLAN.
11. Enter a size appropriate to your environment.
12. Enter the appropriate subnet mask.



13. Click OK.
14. Click Next, then Finish.
15. Click OK.
16. Right-Click IP Pools.
17. Select Create IP Pool.
18. Enter `iSCSI_Initiator_B` as the name for IP pool.
19. Optional: Add a description for the IP pool.
20. Select Sequential for the Assignment Order.



21. Click Next.
22. Click Add to add a Block of IPs.
23. Enter a starting IP address in the subnet from the site iSCSI A VLAN.
24. Enter a size appropriate to your environment.
25. Enter the appropriate subnet mask.



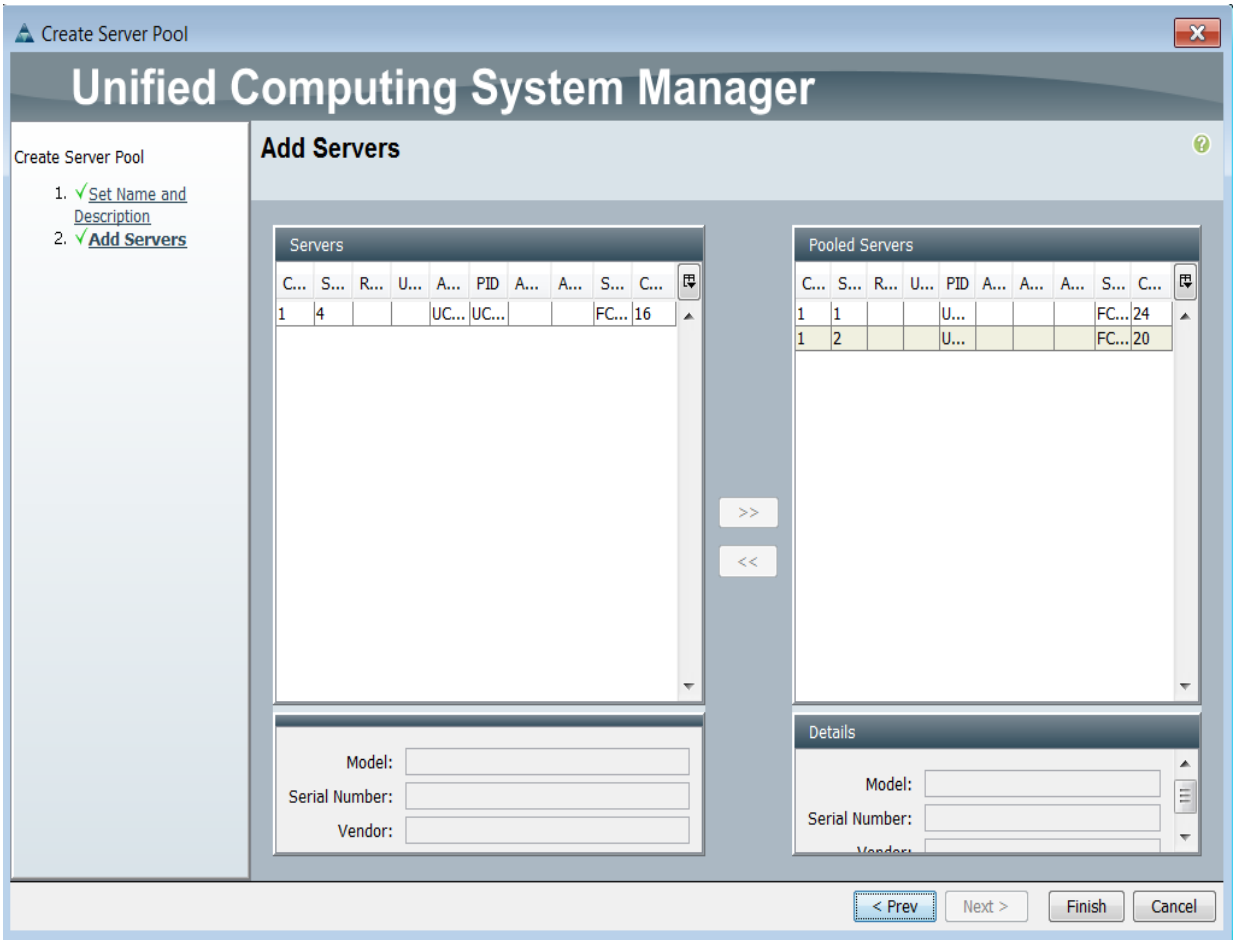
26. Click OK.
27. Click Next, then Finish.
28. Click OK.

Create Server Pool

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

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

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

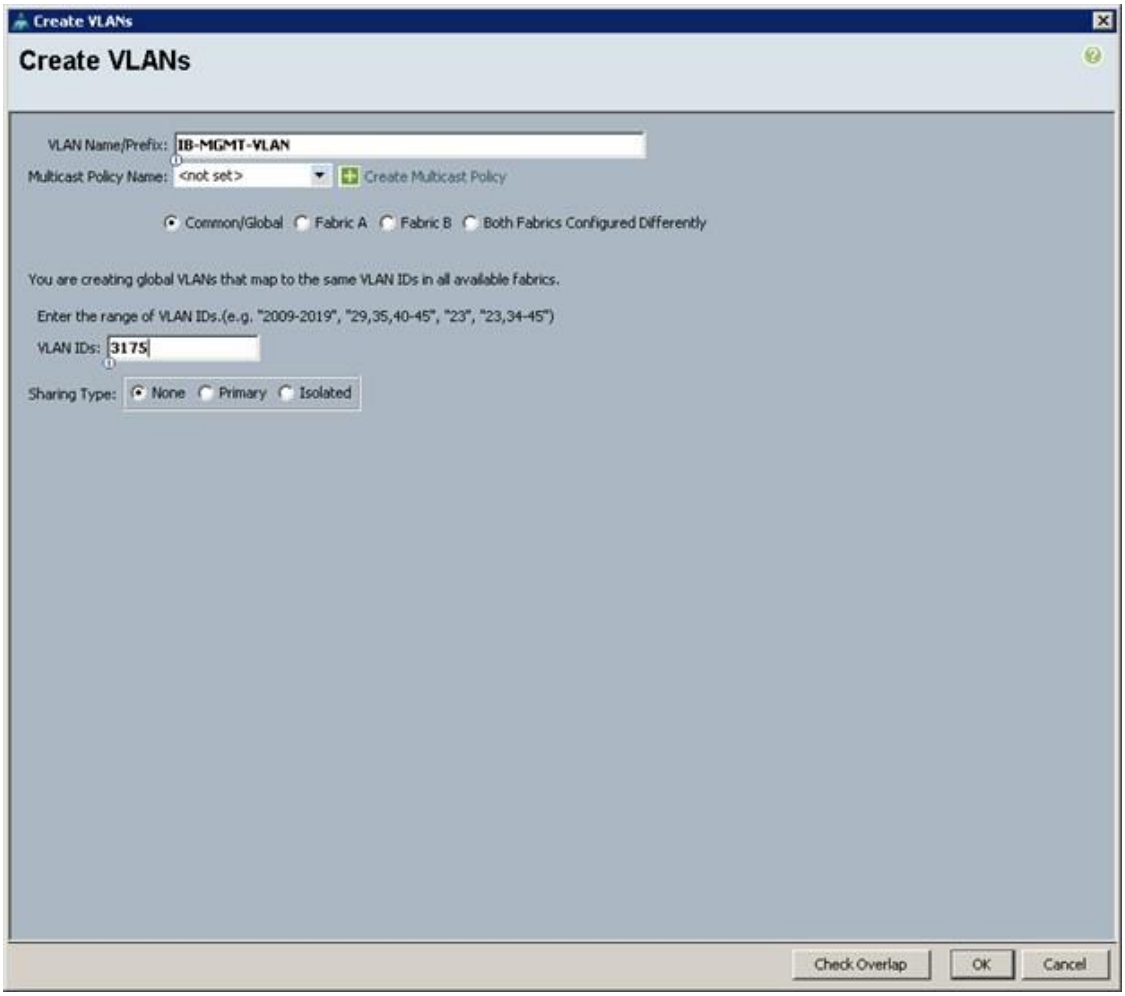
1. In Cisco UCS Manager, click the LAN tab in the navigation pane.

In this procedure, five VLANs are created.

---

2. Select LAN > LAN Cloud.
3. Right-click VLANs.
4. Select Create VLANs
5. Enter `IB-MGMT-VLAN` as the name of the VLAN to be used for management traffic.
6. Keep the Common/Global option selected for the scope of the VLAN.

7. Enter `<<var_ib-mgmt_vlan_id>>` as the ID of the management VLAN.
8. Keep the Sharing Type as None.
9. Click OK and then click OK again.



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

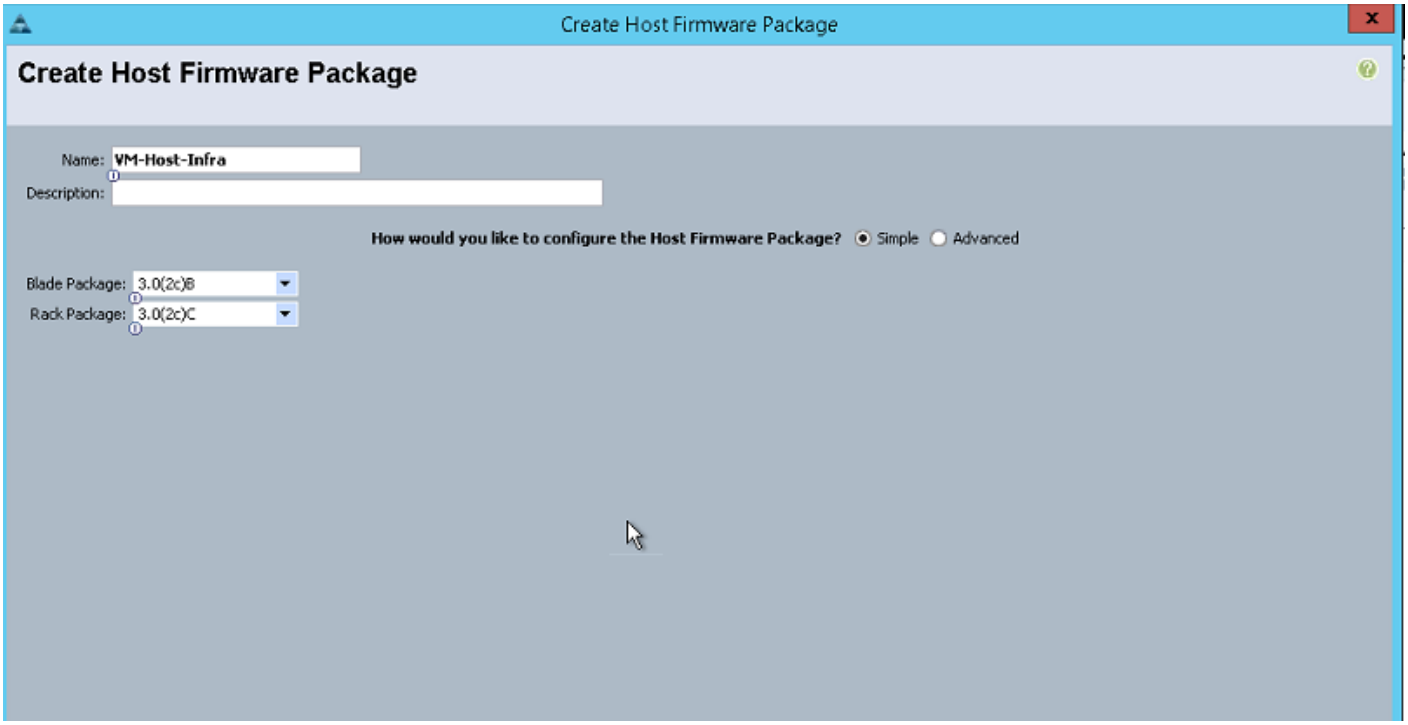
19. Enter `vMotion-VLAN` as the name of the VLAN to be used for vMotion.
20. Keep the Common/Global option selected for the scope of the VLAN.
21. Enter the `<<var_vmotion_vlan_id>>` as the ID of the vMotion VLAN.
22. Keep the Sharing Type as None.
23. Click OK, and then click OK again.
24. Right-click VLANs.
25. Select Create VLANs
26. Enter `VM-Traffic-VLAN` as the name of the VLAN to be used for the VM traffic.
27. Keep the Common/Global option selected for the scope of the VLAN.
28. Enter the `<<var_vm-traffic_vlan_id>>` for the VM Traffic VLAN.
29. Keep the Sharing Type as None.
30. Click OK, and then click OK again.
31. Right-click VLANs.
32. Select Create VLANs
33. Enter `Native-VLAN` as the name of the VLAN to be used as the native VLAN.
34. Keep the Common/Global option selected for the scope of the VLAN.
35. Enter the `<<var_native_vlan_id>>` as the ID of the native VLAN.
36. Keep the Sharing Type as None.
37. Click OK and then click OK again.
38. Expand the list of VLANs in the navigation pane, right-click the newly created Native-VLAN and select Set as Native VLAN.
39. Click Yes, and then click OK.
40. Right-click VLANs.
41. Select Create VLANs
42. Enter `iSCSI-A-VLAN` as the name of the VLAN to be used for iSCSI fabric A.
43. Keep the Common/Global option selected for the scope of the VLAN.
44. Enter the <<var_iscsi-a_vlan_id>> as the ID of iSCSI Fabric A VLAN.

45. Keep the Sharing Type as None.
46. Click OK and then click OK again.
47. Right-click VLANs.
48. Select Create VLANs
49. Enter `iSCSI-B-VLAN` as the name of the VLAN to be used for iSCSI fabric A.
50. Keep the Common/Global option selected for the scope of the VLAN.
51. Enter the `<<var_iscsi-b_vlan_id>>` as the ID of iSCSI Fabric B VLAN.
52. Keep the Sharing Type as None.
53. Click OK and then click OK again.

Create Host Firmware Package

Firmware management policies allow the administrator to select the corresponding packages for a given server con-figuration. These policies often include packages for adapter, BIOS, board controller, FC adapters, host bus adapter (HBA) option ROM, and storage controller properties. To create a firmware management policy for a given server configuration in the Cisco UCS environment, complete the following steps:

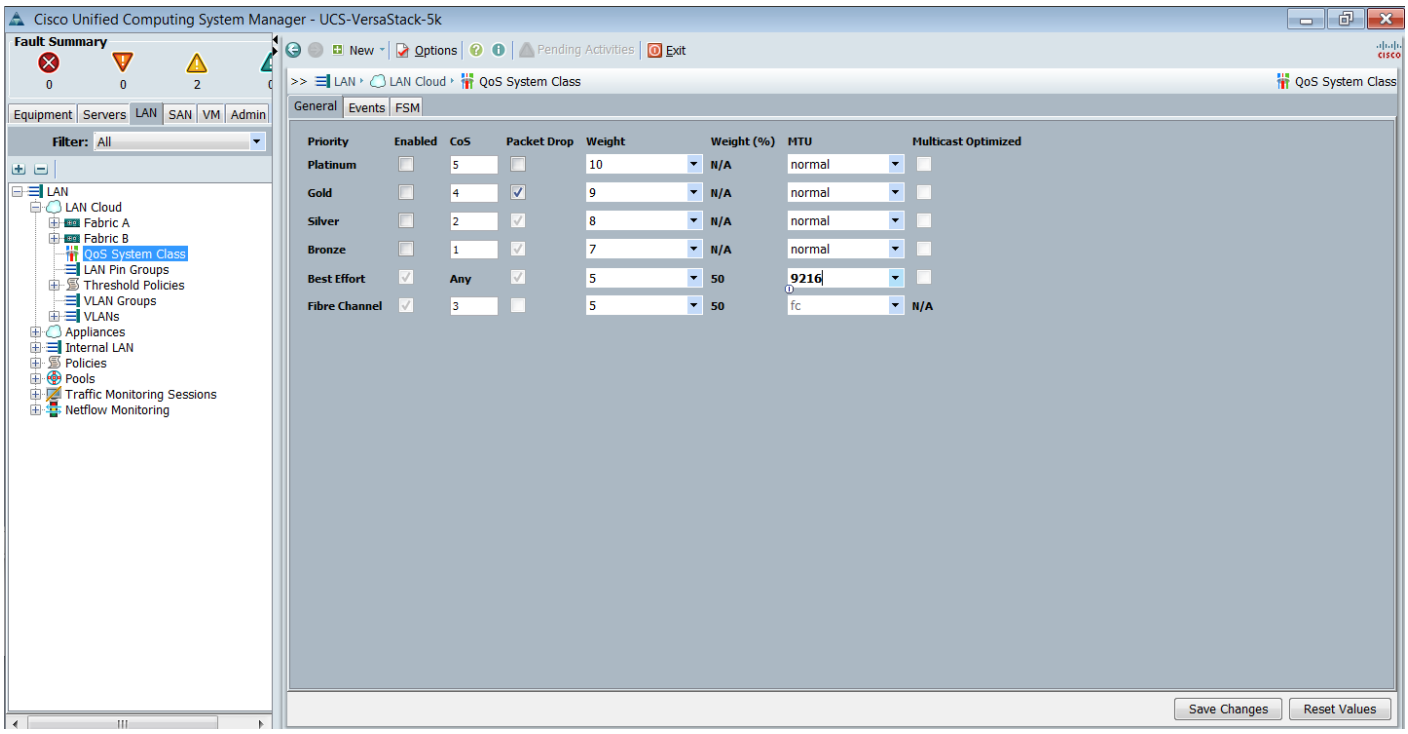
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Host Firmware Packages.
4. Select Create Host Firmware Package
5. Enter `VM-Host-Infra` as the name of the host firmware package.
6. Leave Simple selected.
7. Select the version 3.0(2d) for both the Blade and Rack Packages.
8. Click OK to create the host firmware package.
9. Click OK.



Set Jumbo Frames in Cisco UCS Fabric

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

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



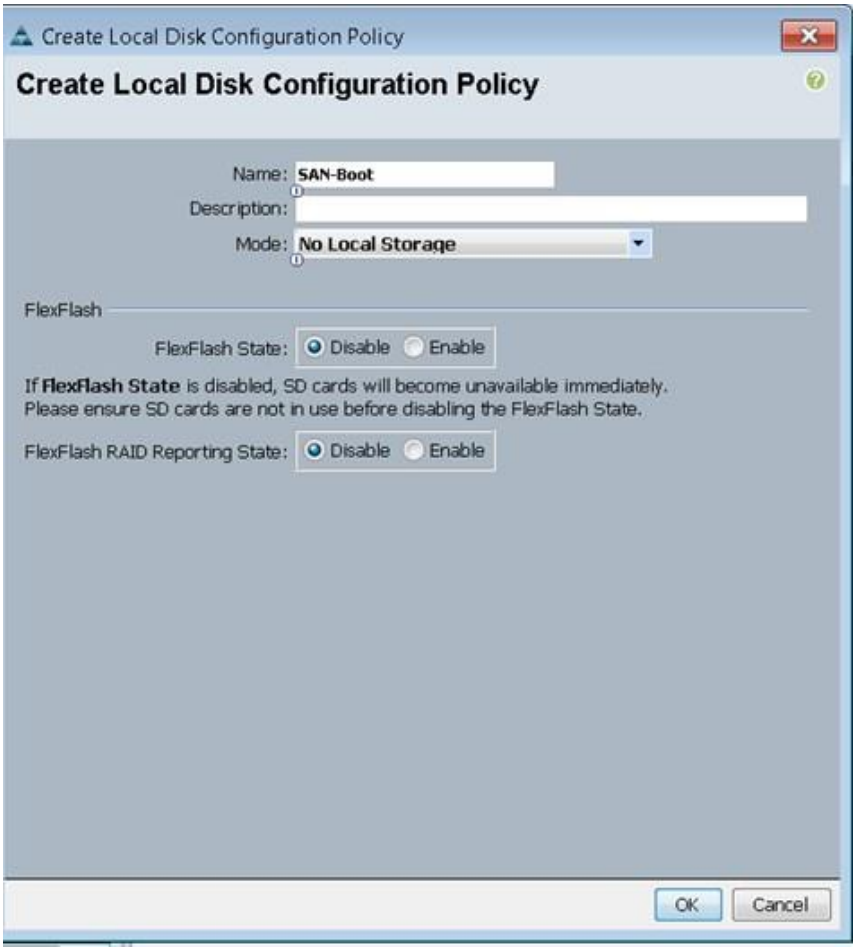
Create Local Disk Configuration Policy (Optional)

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

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

To create a local disk configuration policy, complete the following steps:

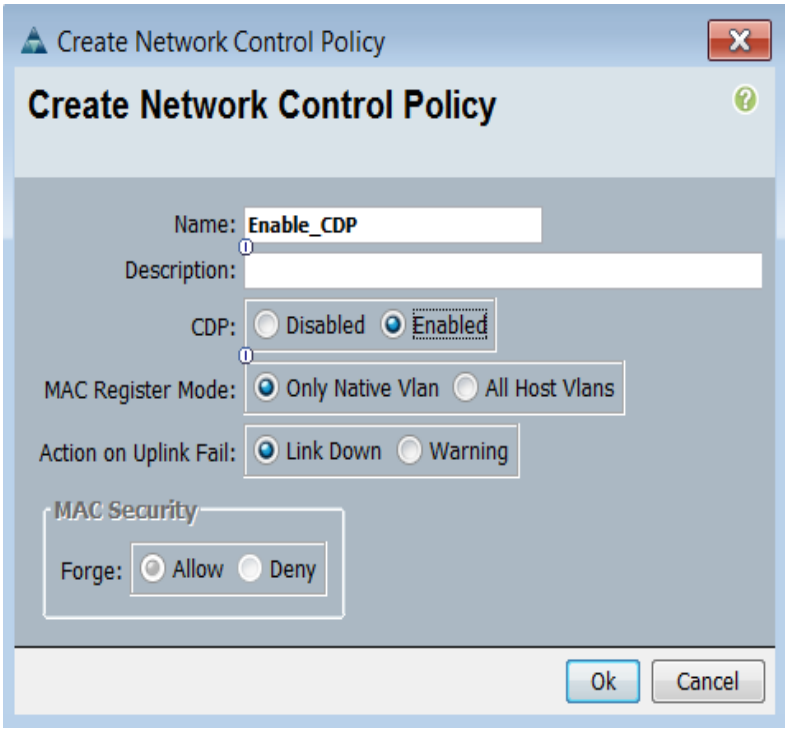
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Local Disk Config Policies.
4. Select Create Local Disk Configuration Policy.
5. Enter `SAN-Boot` as the local disk configuration policy name.
6. Change the mode to No Local Storage.
7. Click OK to create the local disk configuration policy.
8. Click OK.



Create Network Control Policy for Cisco Discovery Protocol

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

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click Network Control Policies.
4. Select Create Network Control Policy
5. Enter `Enable_CDP` as the policy name.
6. For CDP, select the Enabled option.
7. Click OK to create the network control policy.

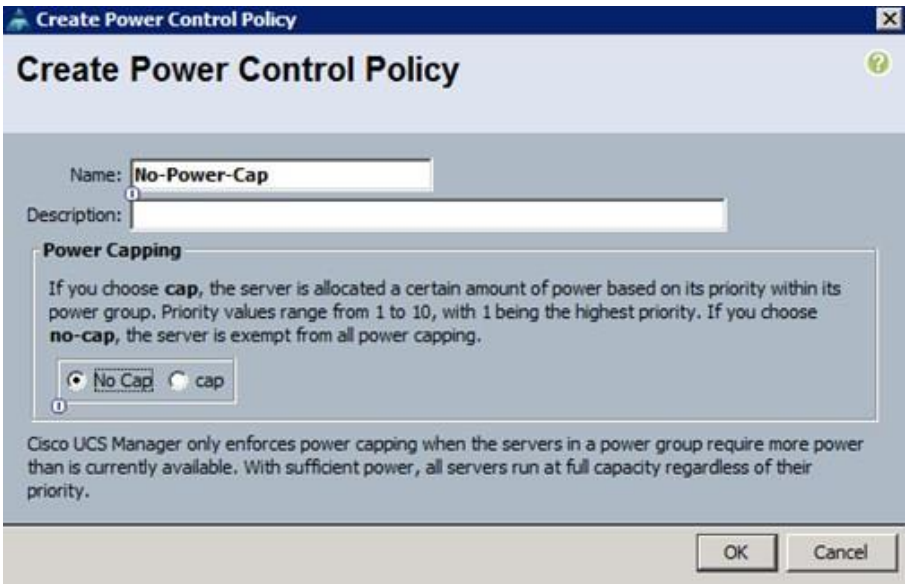


8. Click OK.

Create Power Control Policy

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

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



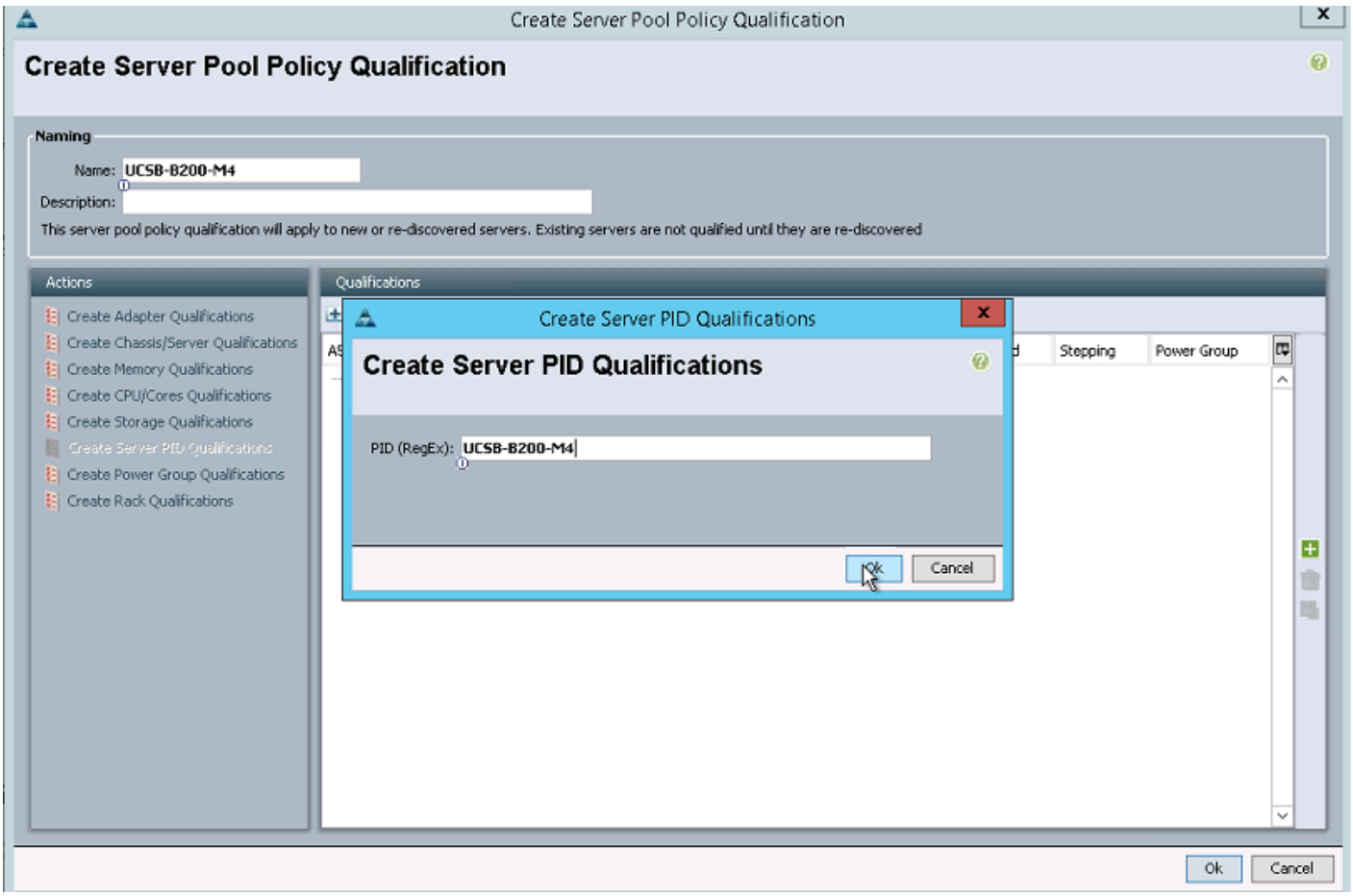
Create Server Pool Qualification Policy (Optional)

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

This example creates a policy for a Cisco UCS B200-M4 server.

---

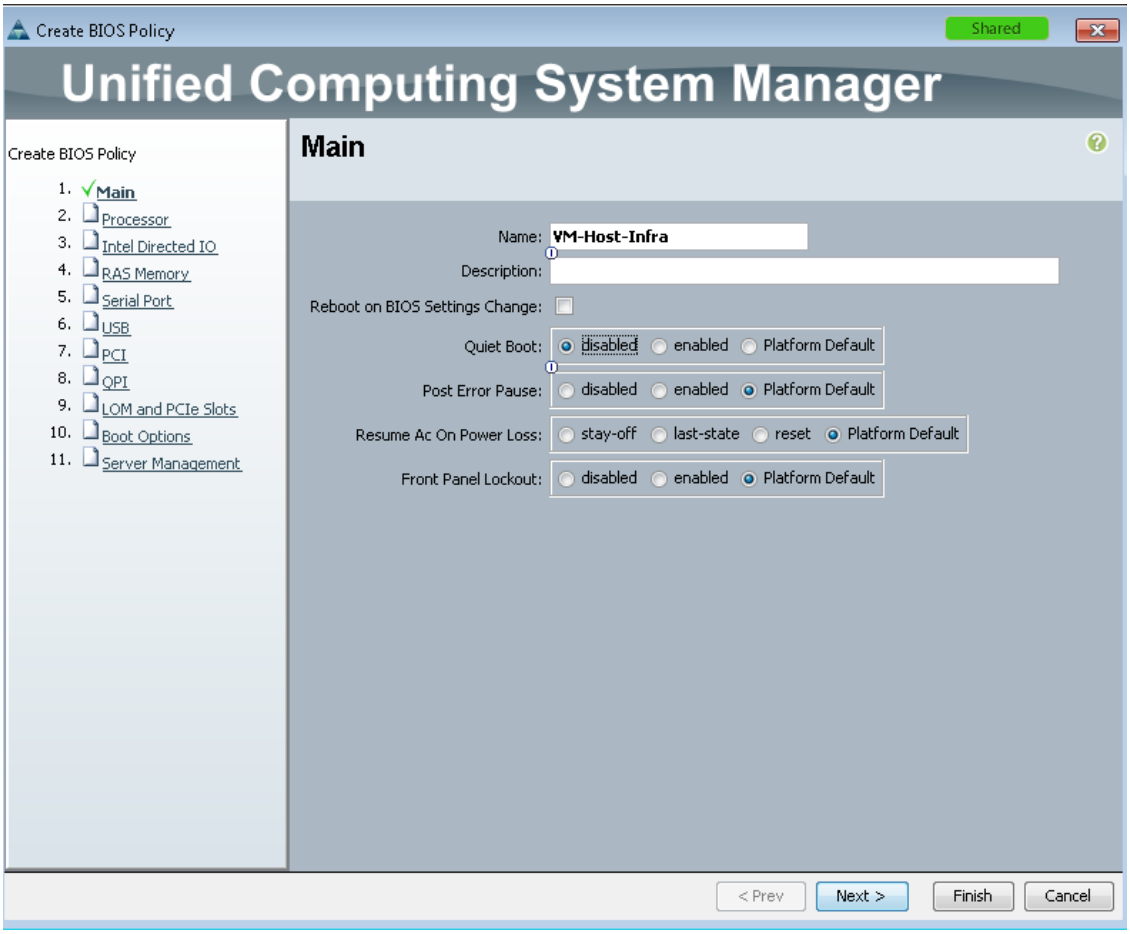
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Server Pool Policy Qualifications.
4. Select Create Server Pool Policy Qualification
5. Enter `UCSB-B200-M4` as the name for the policy.
6. Select Create Server PID Qualifications.
7. Enter `UCSB-B200-M4` as the PID.
8. Click OK to create the server pool qualification policy.
9. Click OK, and then click OK again.



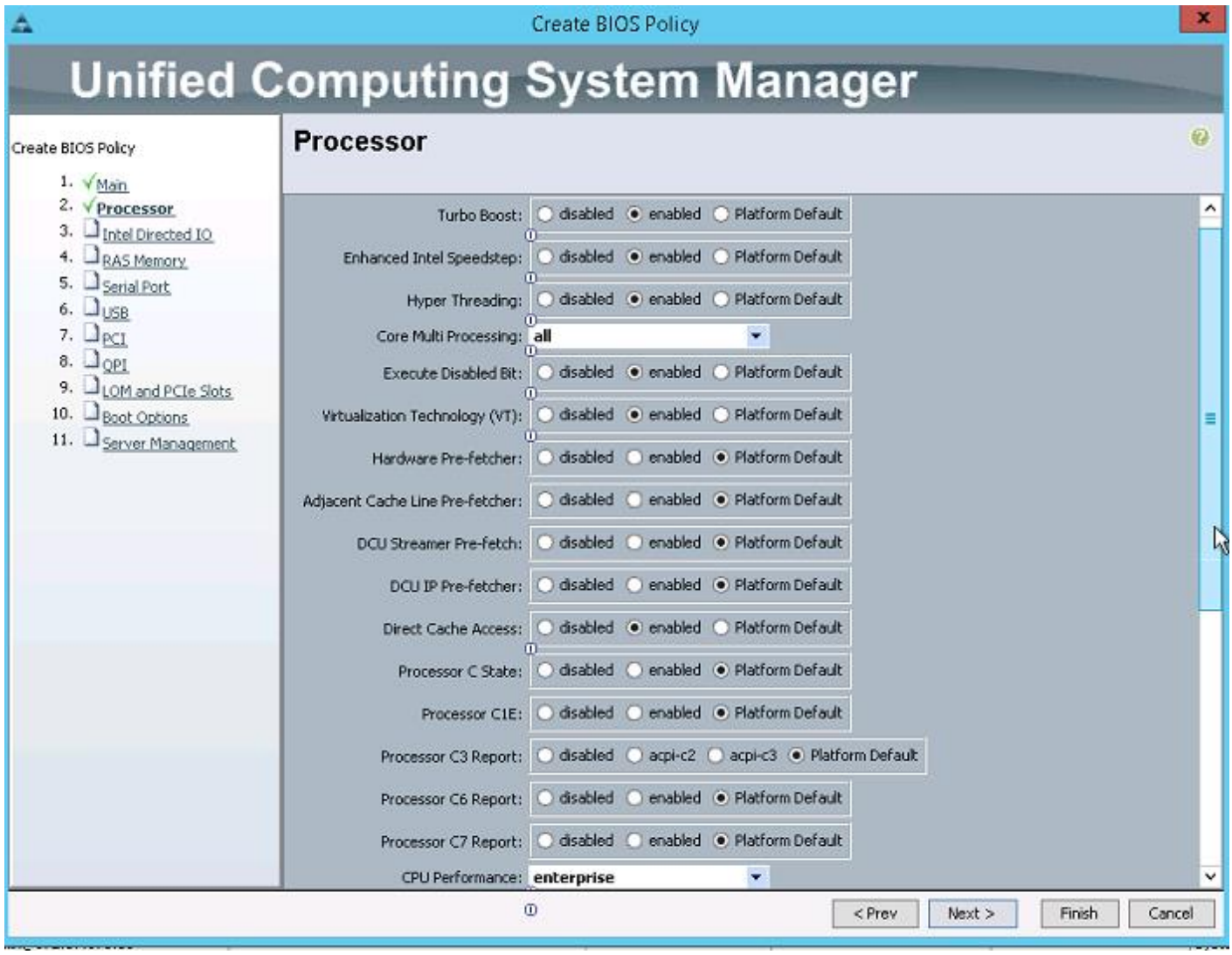
Create Server BIOS Policy

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

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

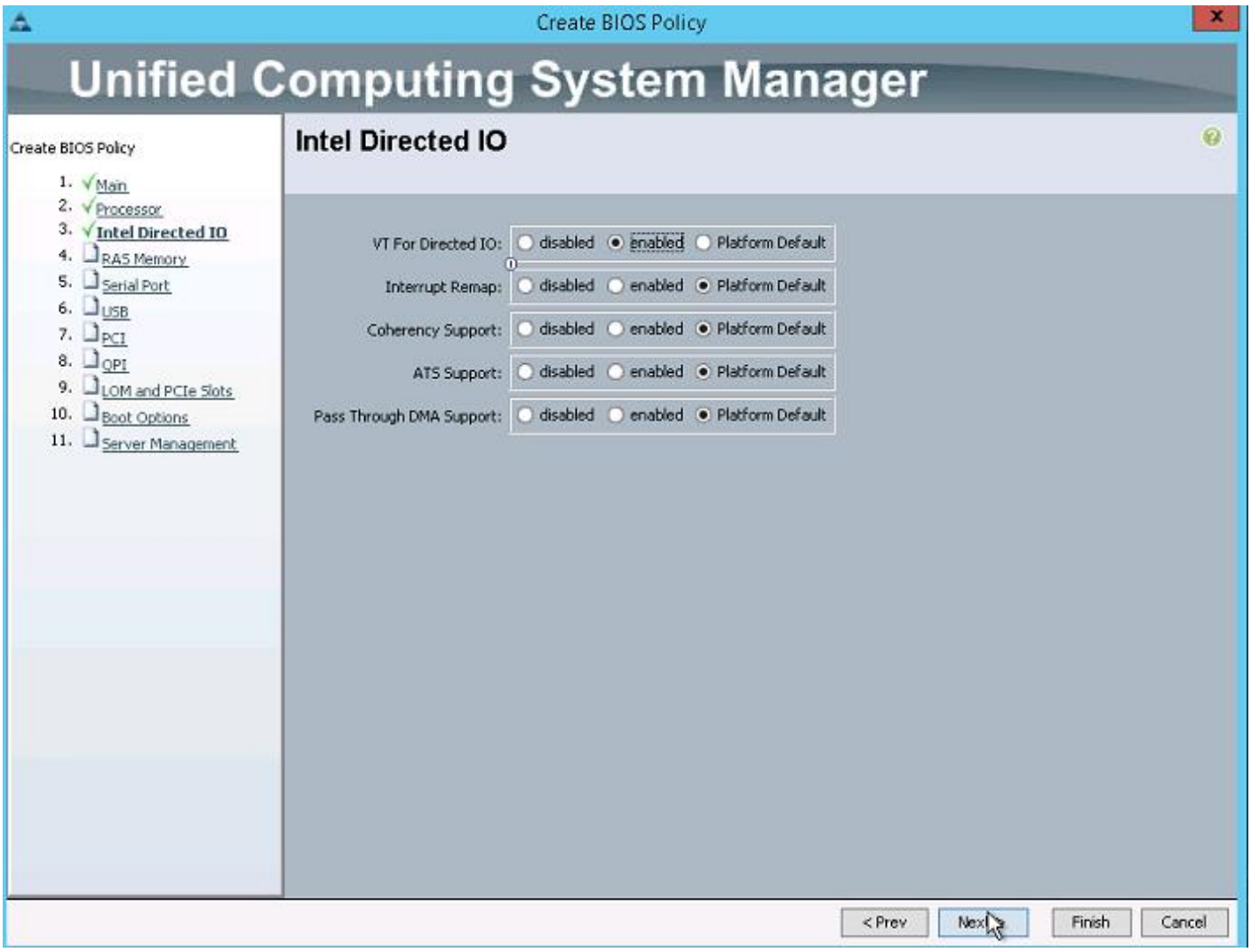


8. Change Turbo Boost to Enabled.
9. Change Enhanced Intel Speedstep to Enabled.
10. Change Hyper Threading to Enabled.
11. Change Core Multi Processing to all.
12. Change Execution Disabled Bit to Enabled.
13. Change Virtualization Technology (VT) to Enabled.
14. Change Direct Cache Access to Enabled.
15. Change CPU Performance to Enterprise.

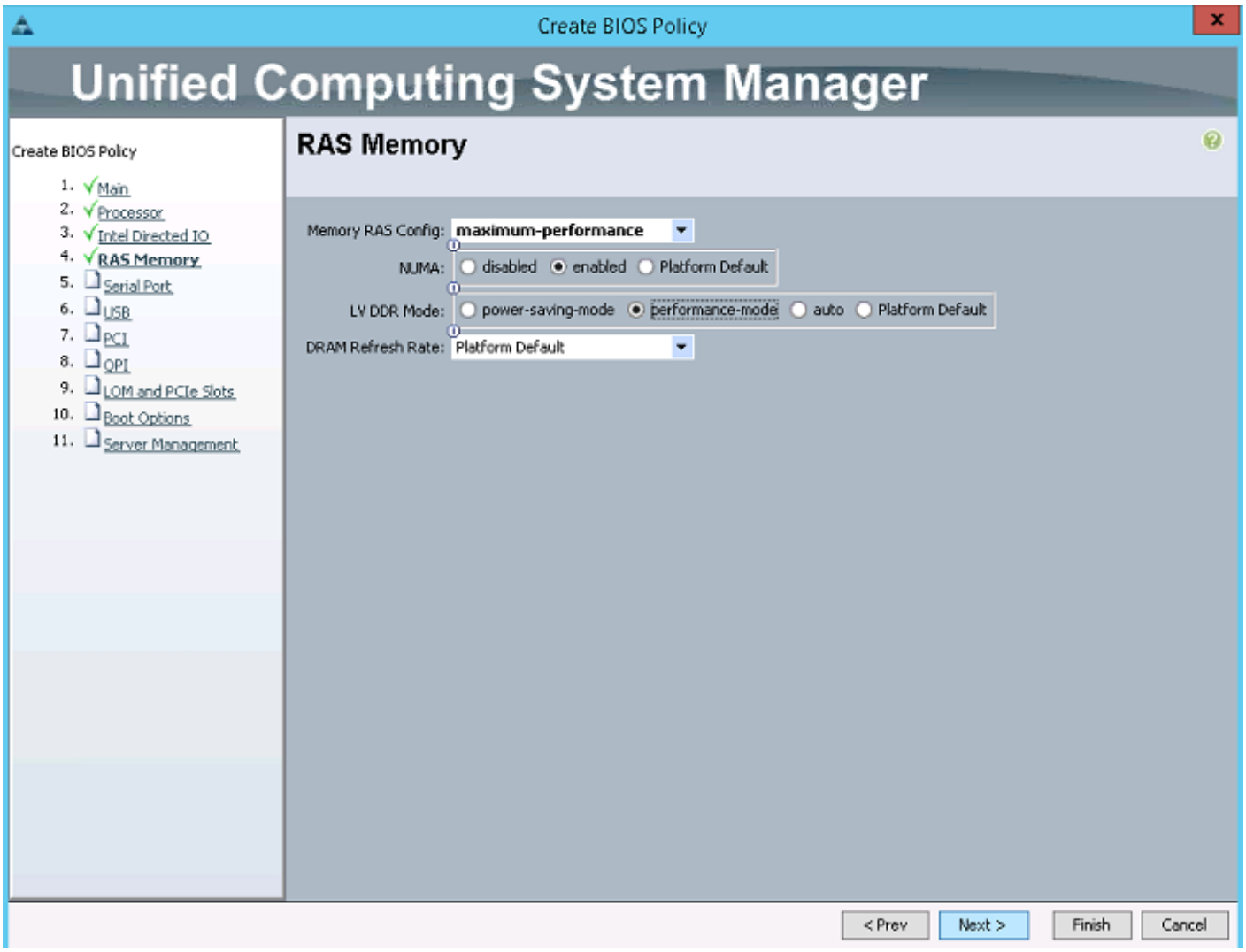


16. Click next to go the Intel Directed IO Screen.

17. Change the VT for Direct IO to Enabled.



18. Click next to go the RaS Memory screen.
19. Change the Memory RAS Config to maximum performance.
20. Change NUMA to Enabled.
21. Change LV DDR Mode to performance-mode.

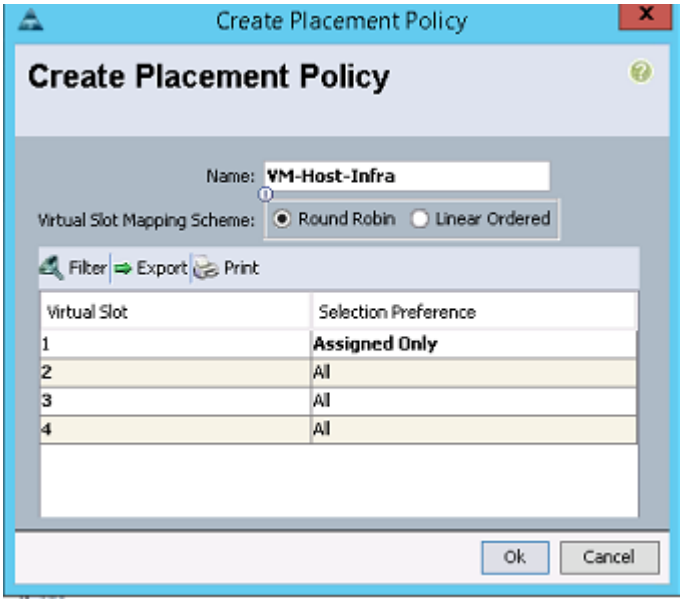


22. Click Finish to create the BIOS policy.
23. Click OK.

Create vNIC/vHBA Placement Policy for Virtual Machine Infrastructure Hosts

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

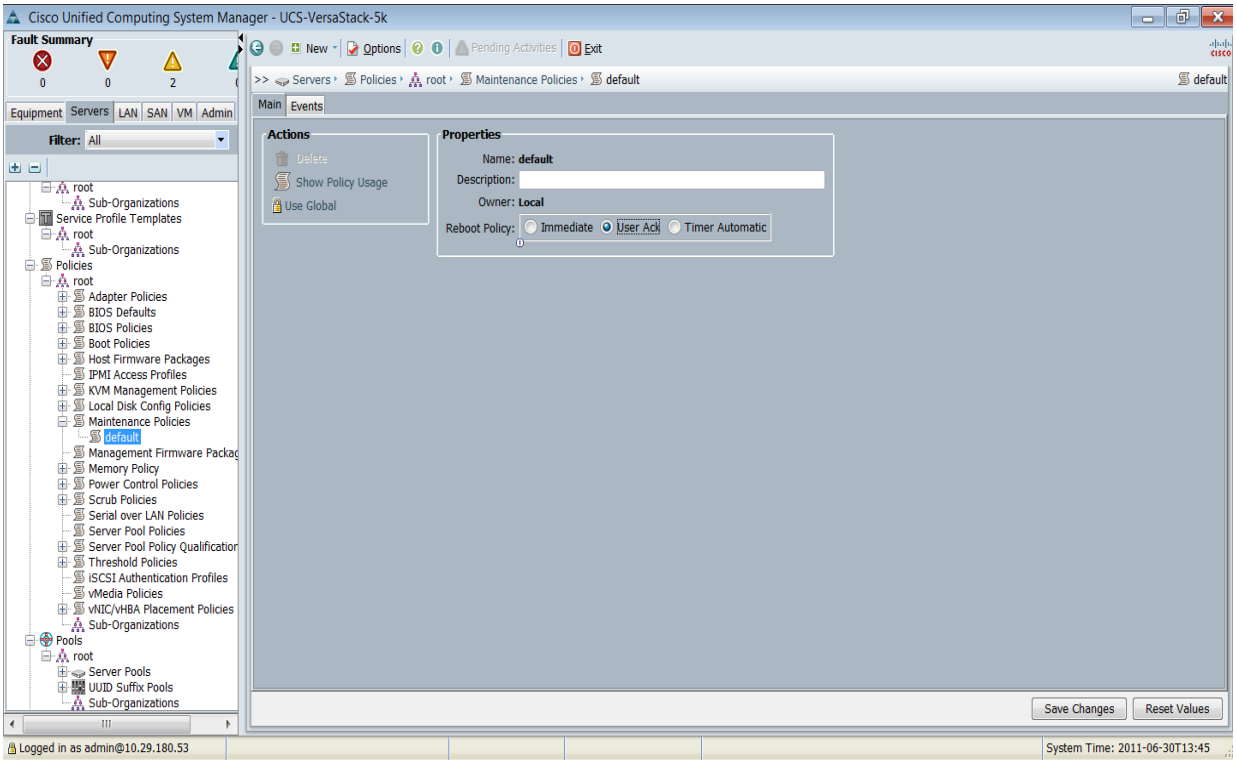
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click vNIC/vHBA Placement Policies.
4. Select Create Placement Policy.
5. Enter `VM-Host-Infra` as the name of the placement policy.
6. Click 1 and select Assigned Only.
7. Click OK and then click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



Update Default Maintenance Policy

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

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Select Maintenance Policies > default
4. Change the Reboot Policy to User Ack.
5. Click Save Changes.
6. Click OK to accept the change.



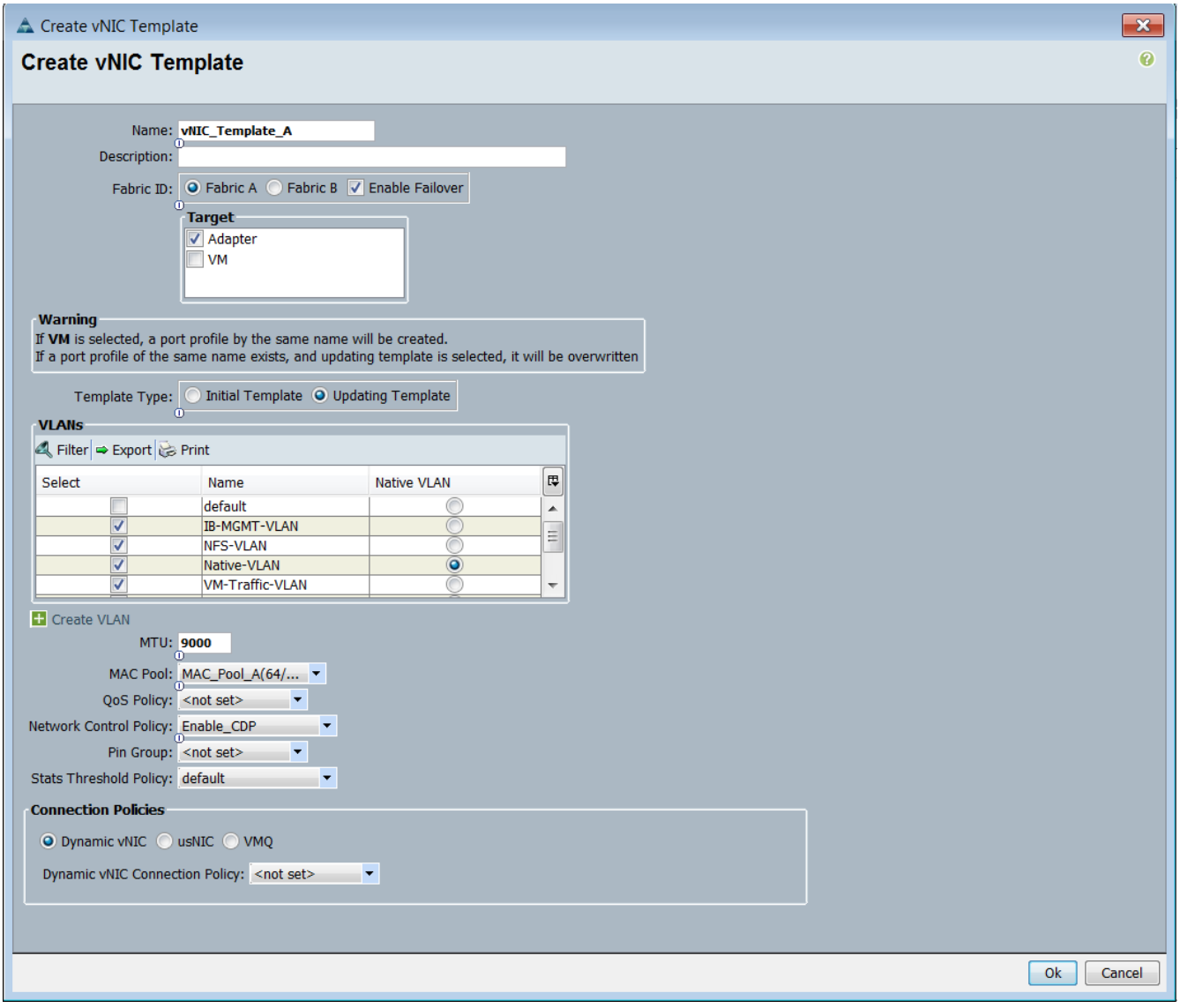
Create vNIC Templates

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

The "Enable Failover " option is used for the vNICs in these steps as default, however , if deploying the optional N1kV virtual switch, the "Enable Failover " options for the vNICs should remain unchecked.

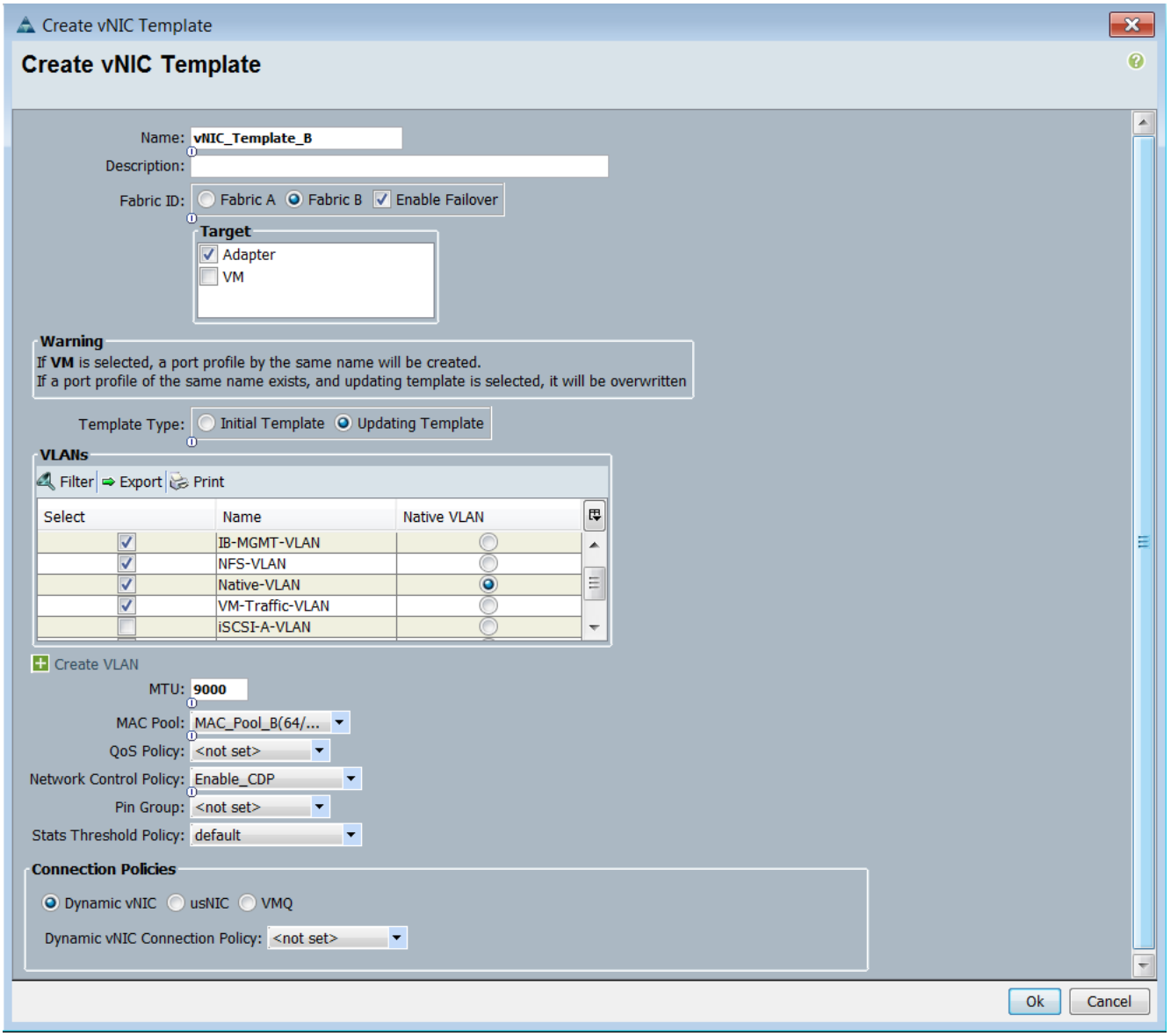
1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter `vNIC_Template_A` as the vNIC template name.
6. Keep Fabric A selected.
7. Select the Enable Failover checkbox.
8. Under Target, make sure that the VM checkbox is not selected.
9. Select Updating Template as the Template Type.

10. Under VLANs, select the checkboxes for `IB-MGMT-VLAN`, `NFS-VLAN`, `Native-VLAN`, `VM-Traffic-VLAN`, and `vMotion-VLAN`.
11. Set Native-VLAN as the native VLAN.
12. For MTU, enter 9000.
13. In the MAC Pool list, select `MAC_Pool_A`.
14. In the Network Control Policy list, select Enable_CDP.
15. Click OK to create the vNIC template.
16. Click OK.



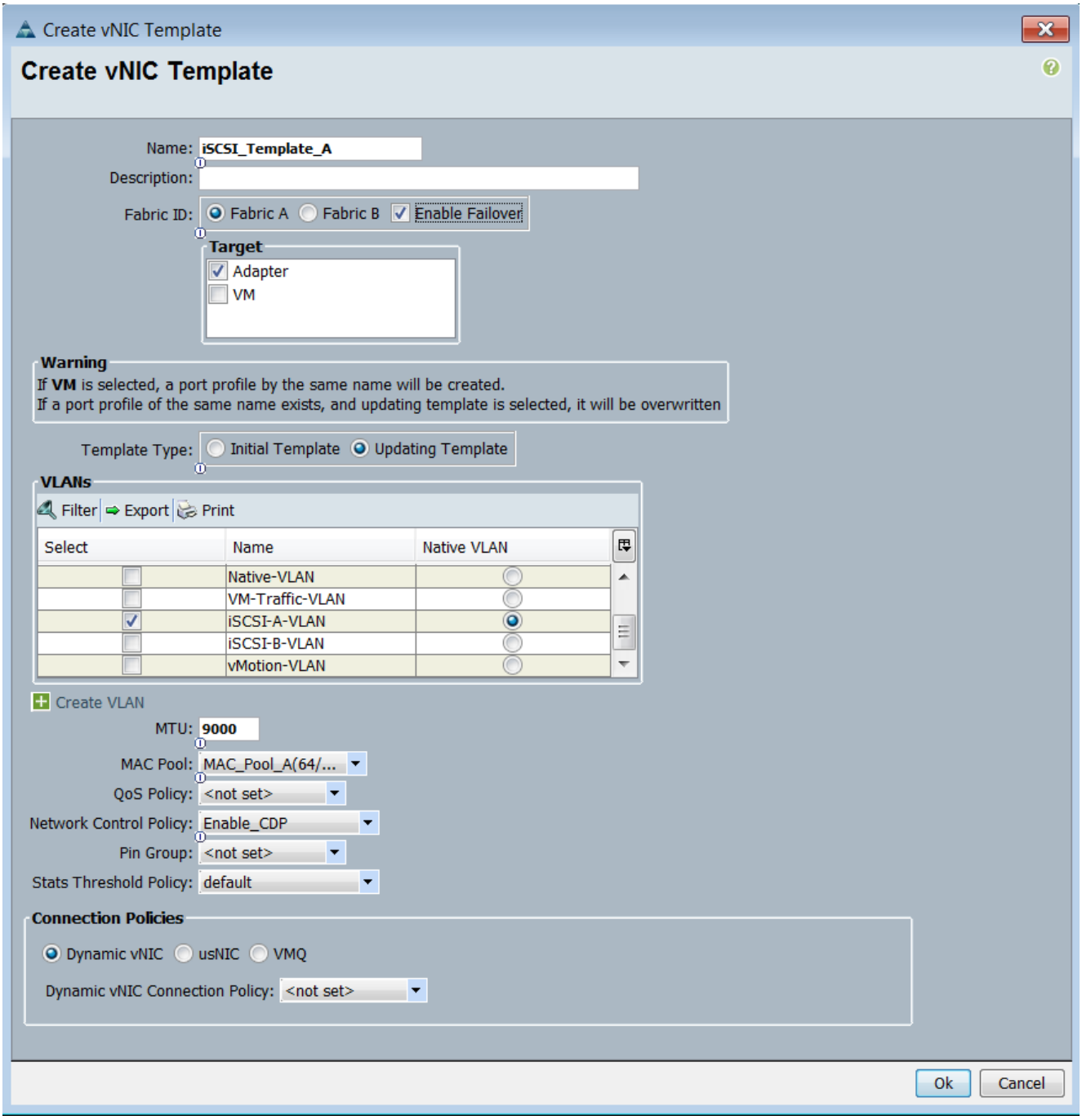
17. In the navigation pane, select the LAN tab.
18. Select Policies > root.

19. Right-click vNIC Templates.
20. Select Create vNIC Template.
21. Enter `vNIC_Template_B` as the vNIC template name.
22. Select Fabric B.
23. Select the Enable Failover checkbox.
24. Select Updating Template as the template type.
25. Under VLANs, select the checkboxes for `IB-MGMT-VLAN`, `NFS-VLAN`, `Native-VLAN`, `VM-Traffic-VLAN`, and `vMotion-VLAN`.
26. Set Native-VLAN as the native VLAN.
27. For MTU, enter 9000.
28. In the MAC Pool list, select `MAC_Pool_B`.
29. In the Network Control Policy list, select `Enable_CDP`.
30. Click OK to create the vNIC template.
31. Click OK.



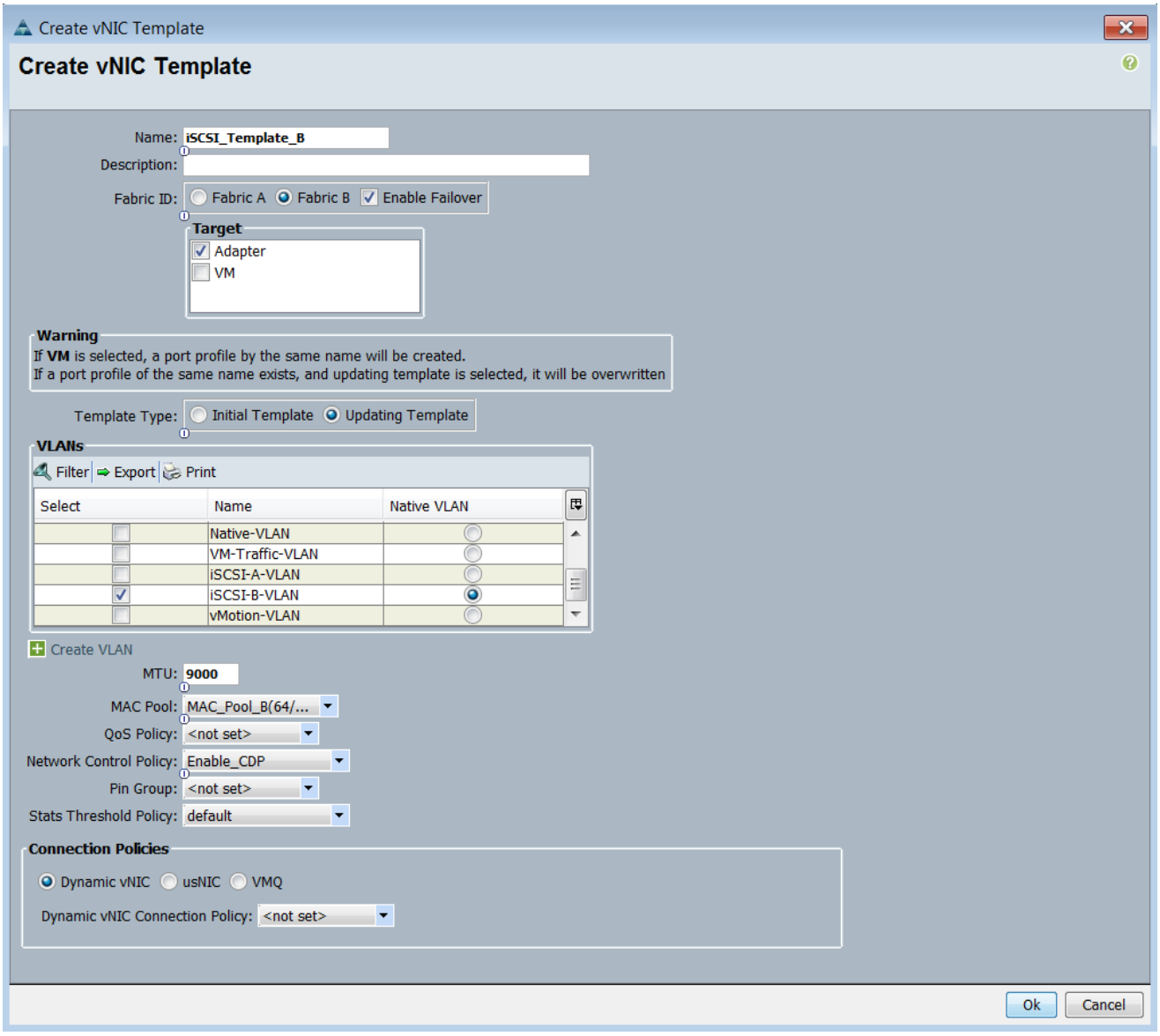
32. In the navigation pane, select the LAN tab.
33. Select Policies > root.
34. Right-click vNIC Templates.
35. Select Create vNIC Template.
36. Enter `iSCSI_Template_A` as the vNIC template name.
37. Keep Fabric A selected.
38. Select the Enable Failover checkbox.
39. Under Target, make sure that the VM checkbox is not selected.
40. Select Updating Template as the Template Type.

41. Under VLANs, select the checkboxes for `iSCSI-A-VLAN`
42. Set `iSCSI-A-VLAN` as the native VLAN.
43. For MTU, enter 9000.
44. In the MAC Pool list, select `MAC_Pool_A`.
45. In the Network Control Policy list, select `Enable_CDP`.
46. Click OK to create the vNIC template.
47. Click OK.



48. In the navigation pane, select the LAN tab.
49. Select Policies > root.
50. Right-click vNIC Templates.
51. Select Create vNIC Template.
52. Enter `iSCSI_Template_B` as the vNIC template name.
53. Select Fabric B.

54. Select the Enable Failover checkbox.
55. Select Updating Template as the template type.
56. Under VLANs, select the `iSCSI-B-VLAN`.
57. Set iSCSI-B-VLAN as the native VLAN.
58. For MTU, enter 9000.
59. In the MAC Pool list, select `MAC_Pool_B`.
60. In the Network Control Policy list, select `Enable_CDP`.
61. Click OK to create the vNIC template.
62. Click OK.



Create Boot Policy

This procedure applies to a Cisco UCS environment in which two 10GbE iSCSI interfaces are on cluster node 1 (Eth3 and Eth4) and two 10GbE iSCSI interfaces are on cluster node 2 (Eth3 and Eth4). Also, it is assumed that the Eth3 interfaces are connected to Fabric A (Cisco Nexus 9372 Switch A) and the Eth4 interfaces are connected to Fabric B (Cisco Nexus 9372 Switch B).

Two boot policies are configured in this procedure. The first policy configures the primary target to be node1, Eth3. And the second policy configures the primary target to be node1, Eth4. Though not absolutely necessary to have two boot policies, having two options helps spread the load across the fabrics.

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

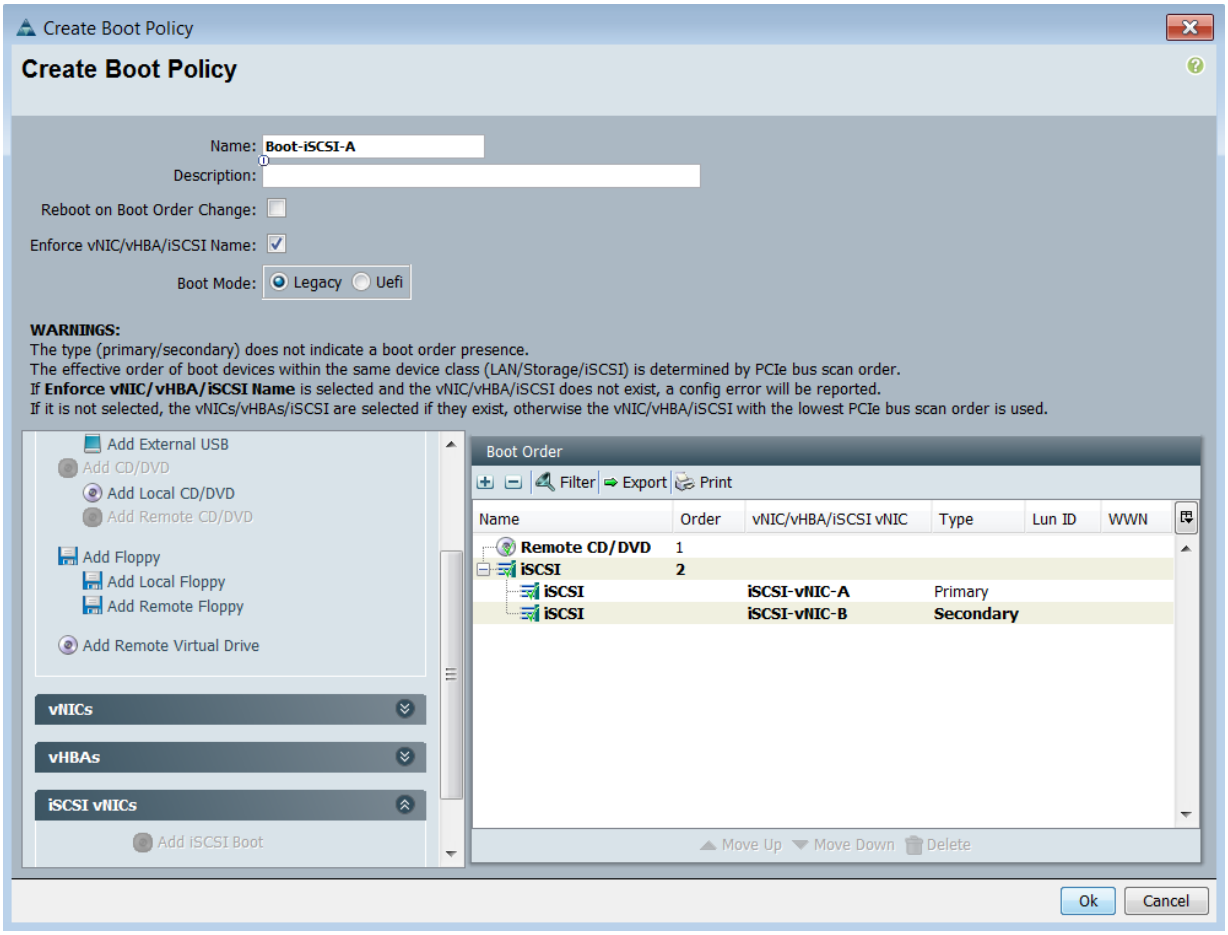
1. In Cisco UCS Manager, in the navigation pane, click the Servers tab.
2. Expand Policies > root.
3. Right-click Boot Policies.
4. Select Create Boot Policy.
5. Enter Boot-iSCSI-A as the name for the boot policy.
6. Optional: Enter a description for the boot policy.

Do not select the Reboot on Boot Order Change checkbox.

7. Expand the Local Devices drop-down menu, select Add `Remote CD/DVD`.
8. Expand the iSCSI vNICs drop-down menu and select Add iSCSI Boot.
9. In the Add iSCSI Boot dialog box, enter `iSCSI-vNIC-A` in the iSCSI vNIC field.

10. Click OK to add the iSCSI boot initiator.
11. From the iSCSI vNICs drop-down menu, select Add iSCSI Boot.
12. Enter `iSCSI-vNIC-B` as the iSCSI vNIC.

13. Click OK to add the iSCSI boot initiator.



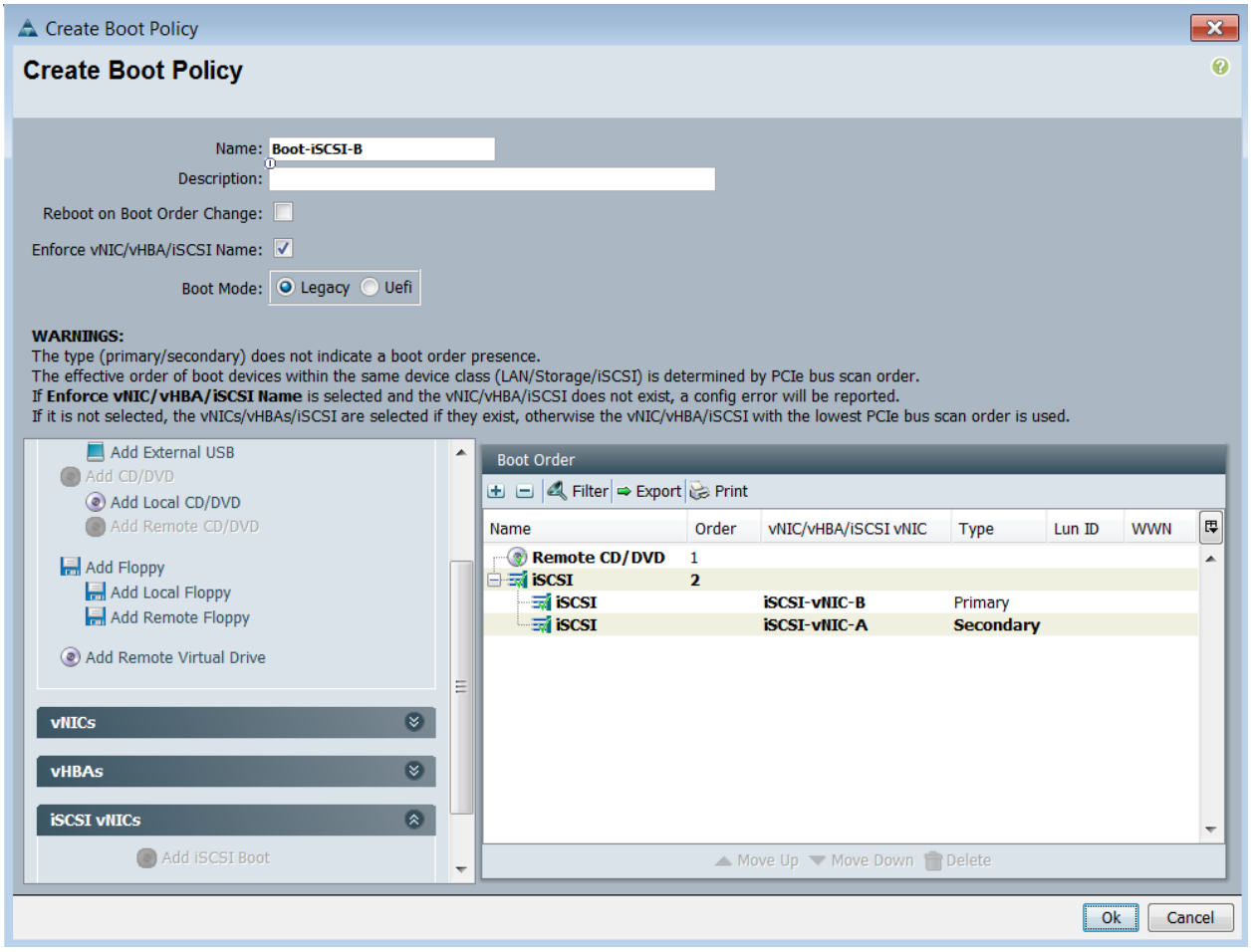
14. Click OK, then click OK again to create the boot policy.
15. Right-click Boot Policies again
16. Select Create Boot Policy.
17. Enter Boot-iSCSI-B as the name for the boot policy.
18. Optional: Enter a description for the boot policy.

Do not select the Reboot on Boot Order Change checkbox.

19. Expand the Local Devices drop-down menu, select Add `Remote CD/DVD`.
20. Expand the iSCSI vNICs drop-down menu and select Add iSCSI Boot.
21. In the Add iSCSI Boot dialog box, enter `iSCSI-vNIC-B` in the iSCSI vNIC field.

22. Click OK to add the iSCSI boot initiator.
23. From the iSCSI vNICs drop-down menu, select Add iSCSI Boot.
24. Enter `iSCSI-vNIC-A` as the iSCSI vNIC.

25. Click OK to add the iSCSI boot initiator.



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

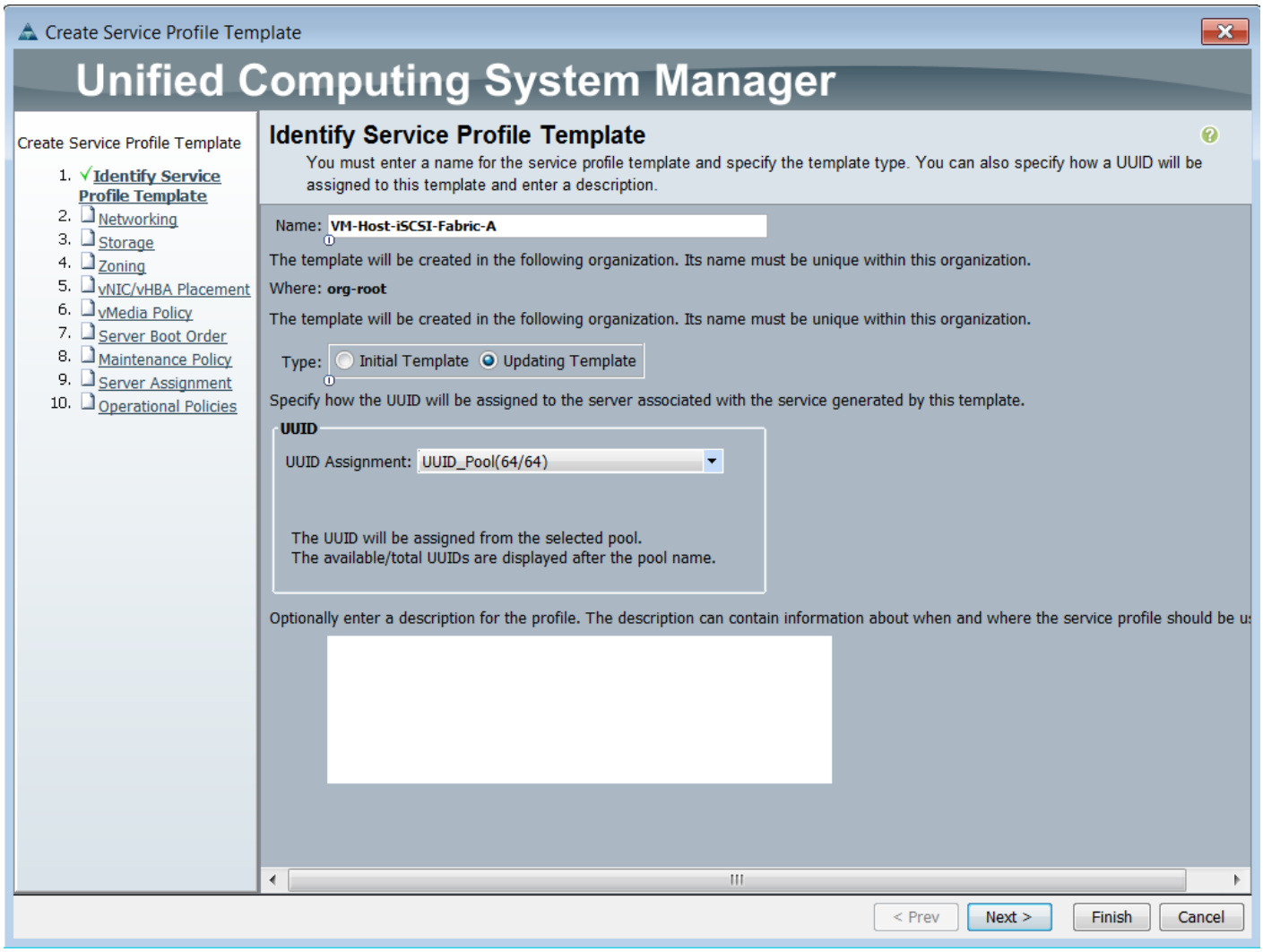
Create iSCSI Boot Service Profile Template

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. Only one service profile template can be used for all the hosts to be booted from Fabric A and the second service profile template is optional.

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

1. In Cisco UCS Manager, in the navigation pane, click the Servers tab.
2. Select Service Profile Templates > root.
3. Right-click root.
4. Select Create Service Profile Template to open the Create Service Profile Template wizard.
5. Identify the Service Profile Template:
   a. Enter `VM-Host-iSCSI-Fabric-A` as the name for the service profile template. This service profile template is configured to boot from Node 1 on Fabric A.
   b. Select the Updating Template option.

c. Under UUID, select `UUID_Pool` as the UUID pool.

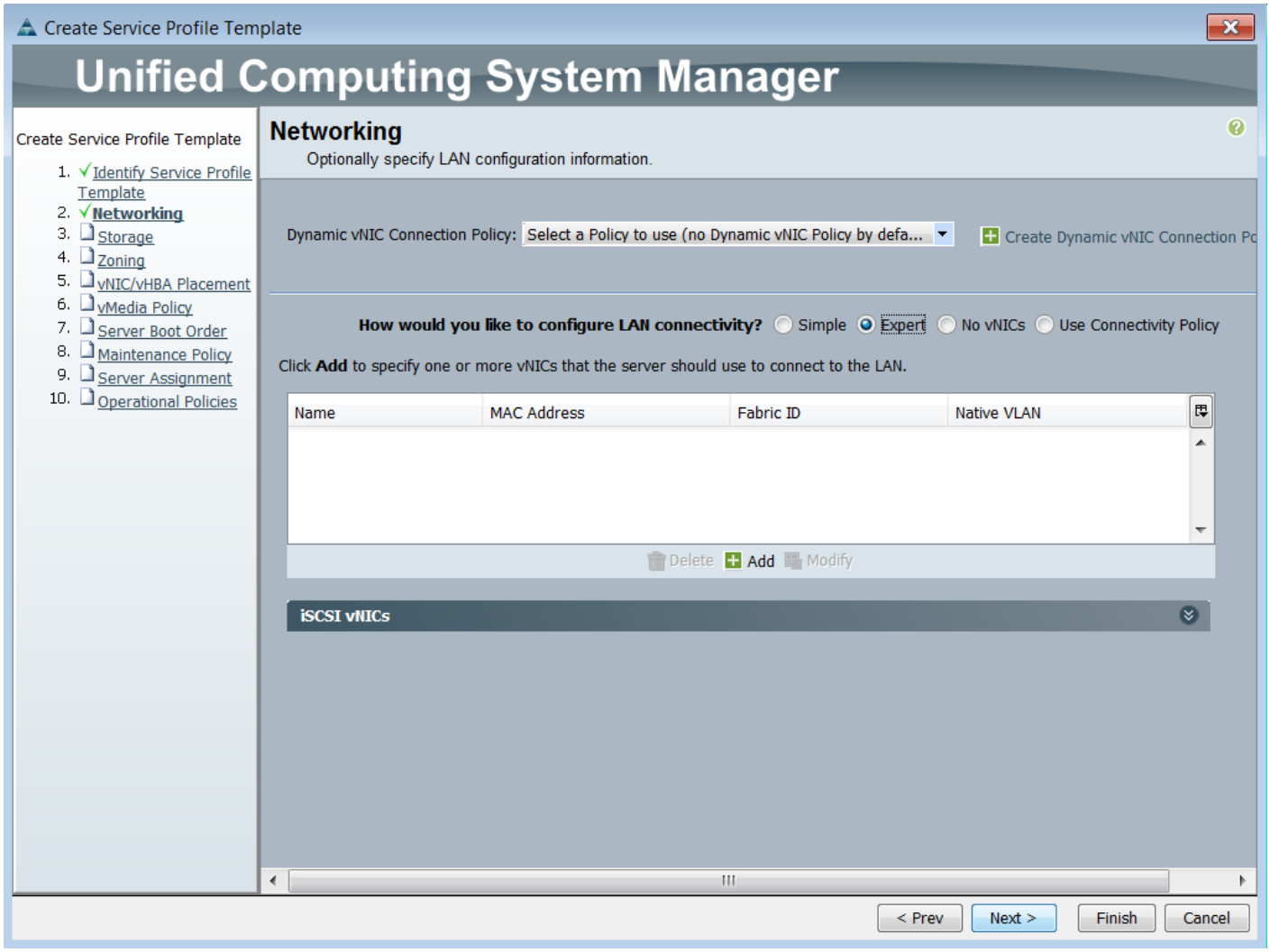


d. Click Next.

6. Configure the Networking options:

a. Retain the default setting for Dynamic vNIC Connection Policy.

b. Select the Expert option to configure the LAN connectivity.



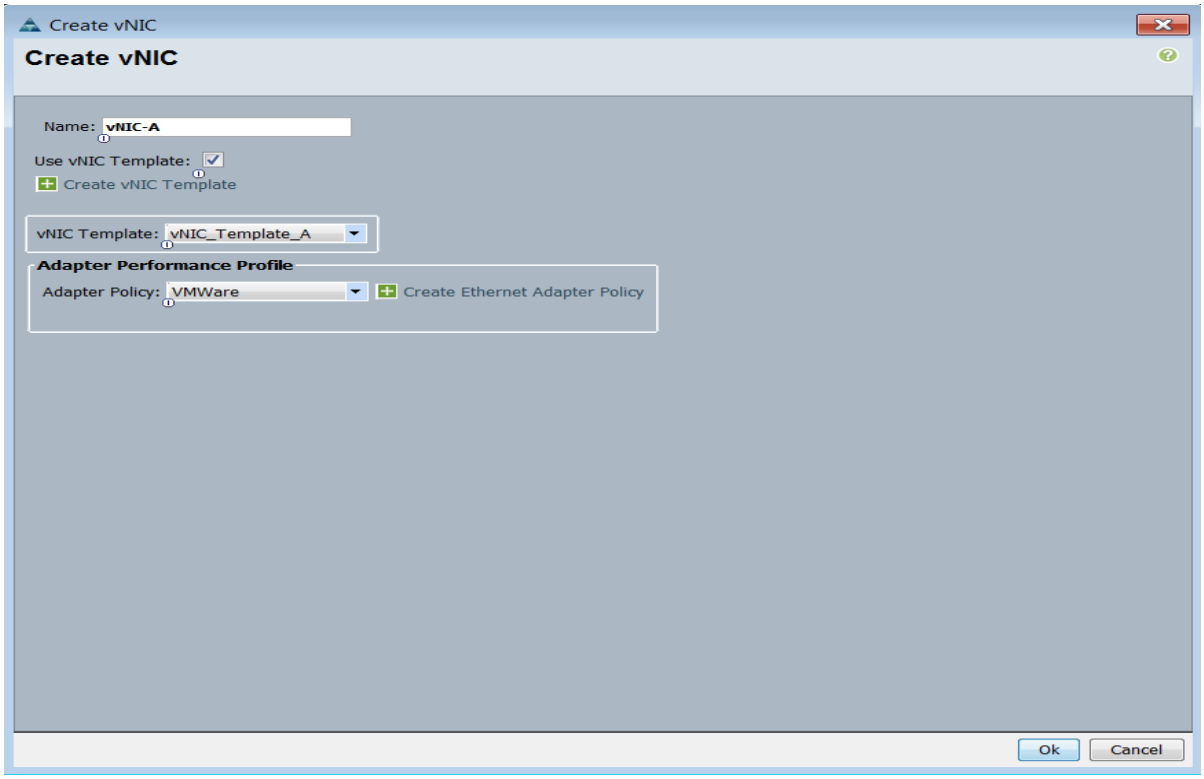
c. Click the upper Add button to add a vNIC to the template.

d. In the Create vNIC dialog box, enter `vNIC-A` as the name for the vNIC.

e. Select the Use vNIC Template checkbox.

f. In the vNIC Template list, select `vNIC_Template_A`.

g. In the Adapter Policy list, select VMWare.



h. Click OK to add this vNIC to the template.

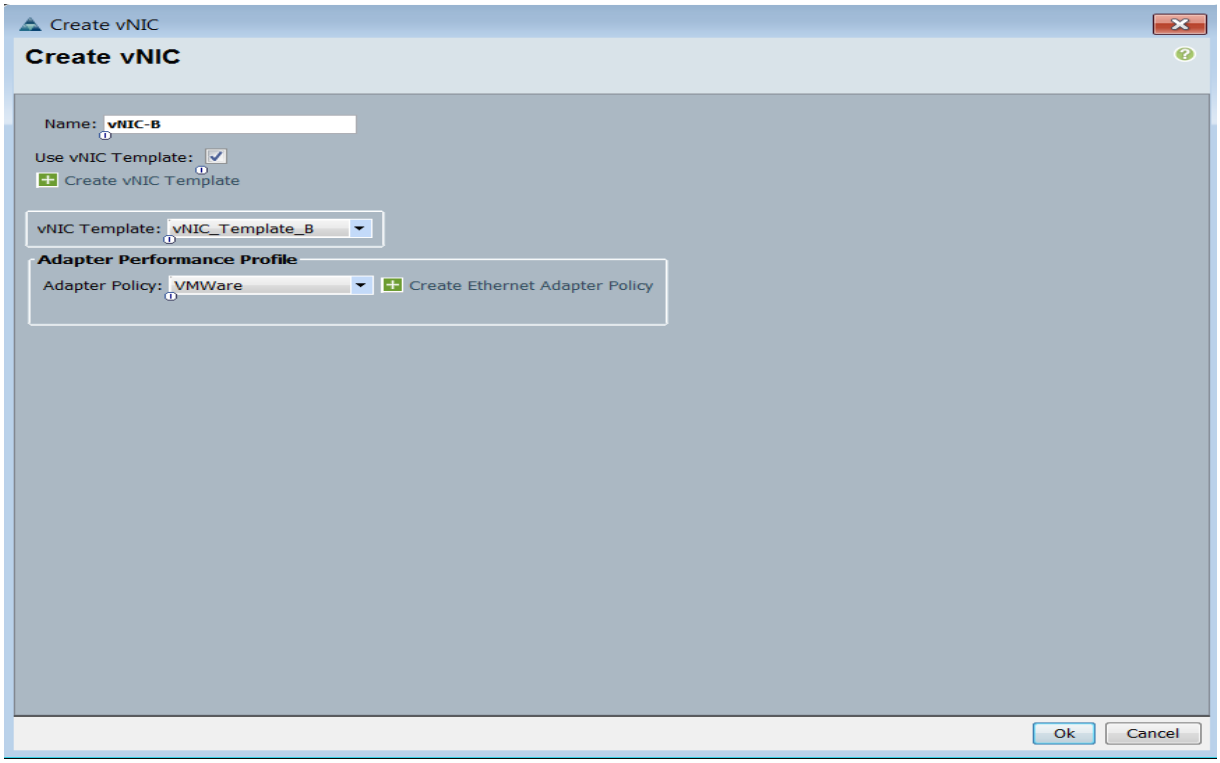
i. On the Networking page of the wizard, click the upper Add button to add another vNIC to the template.

j. In the Create vNIC box, enter `vNIC-B` as the name for vNIC.

k. Select the Use vNIC Template checkbox.

l. In the vNIC Template list, select `vNIC_Template_B`.

m. In the Adapter Policy list, select VMWare.



n. Click OK to add the vNIC to the template.

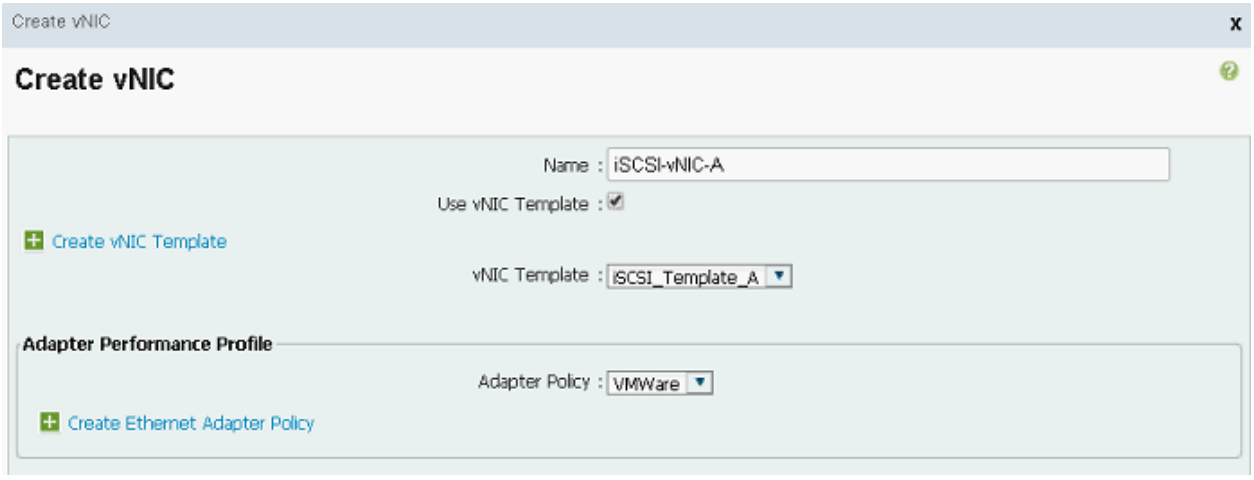
o. Click the upper Add button to add a vNIC to the template.

p. In the Create vNIC dialog box, enter `iSCSI-vNIC-A` as the name for vNIC.

q. Select the Use vNIC Template checkbox.

r. In the vNIC Template list, select `iSCSI_Template_A`.

s. In the Adapter Policy list, select VMWare.



t. Click OK to add this vNIC to the template.

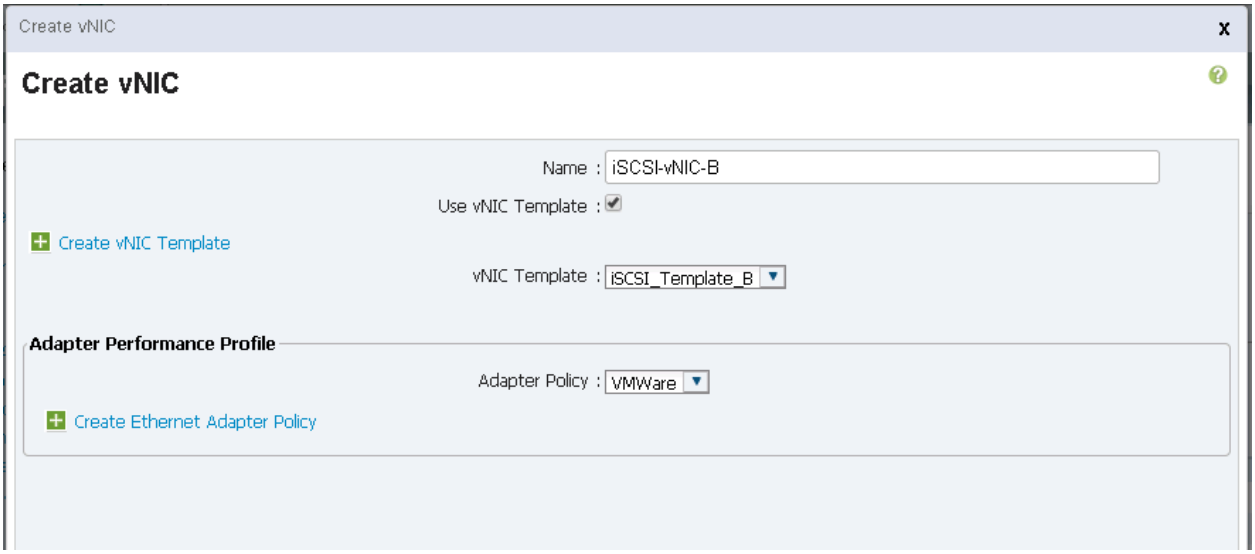
u. On the Networking page of the wizard, click the upper Add button to add another vNIC to the template.

v. In the Create vNIC box, enter `vNIC-B` as the name for vNIC.

w. Select the Use vNIC Template checkbox.

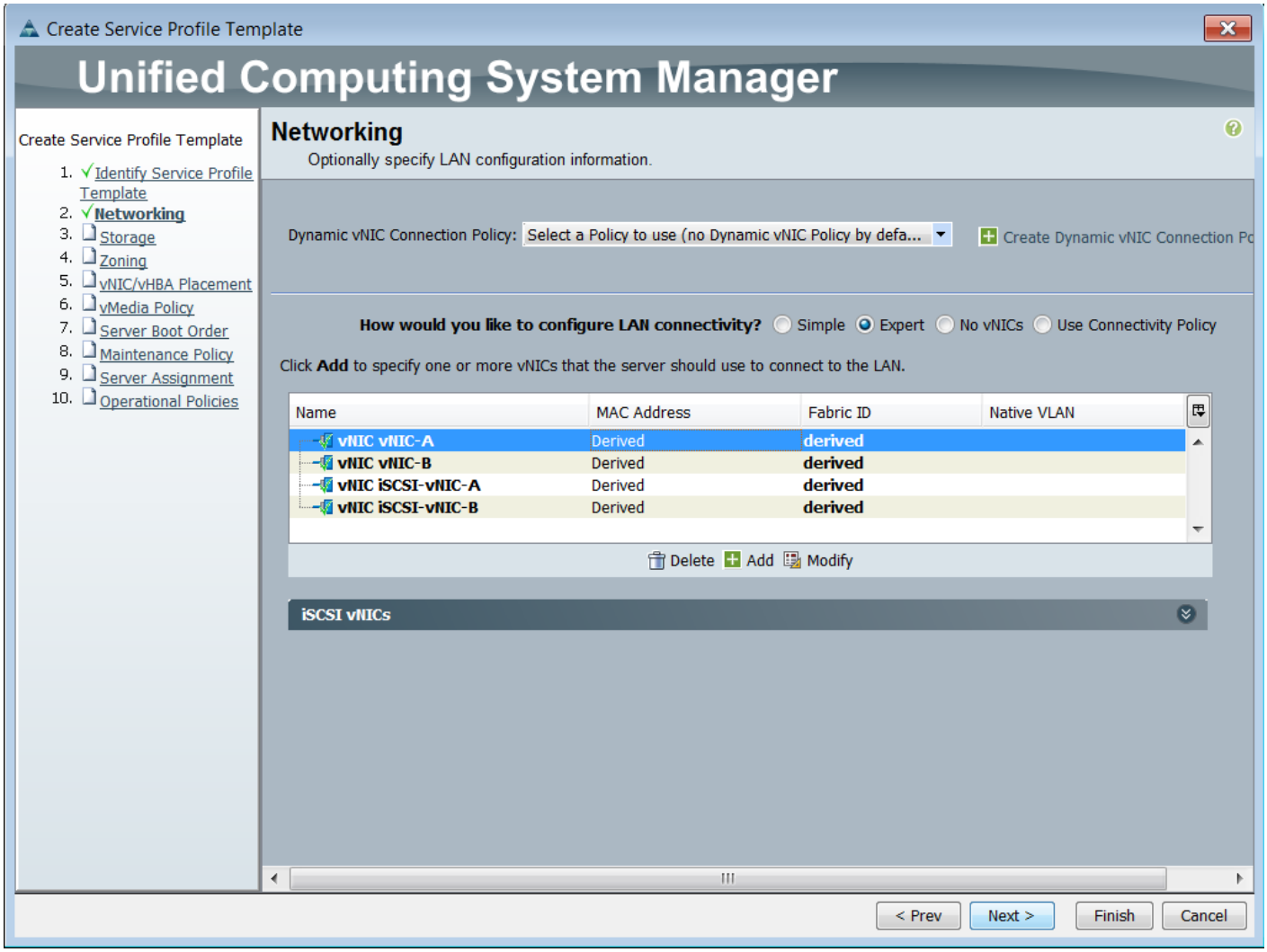
x. In the vNIC Template list, select `iSCSI_Template_B`.

y. In the Adapter Policy list, select VMWare.

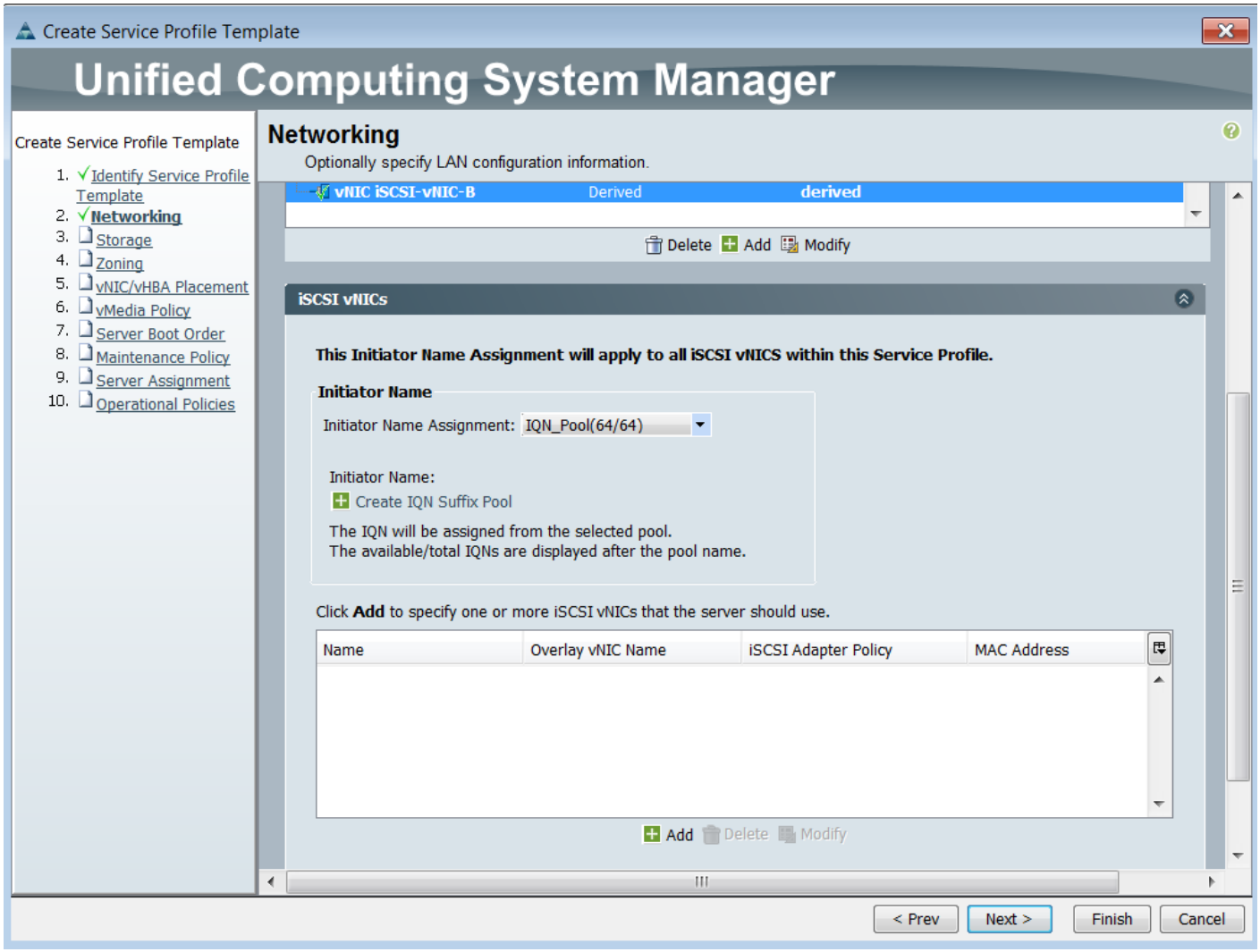


z. Click OK to add the vNIC to the template.

aa. Review the table in the Networking page to confirm that all four vNICs were created.



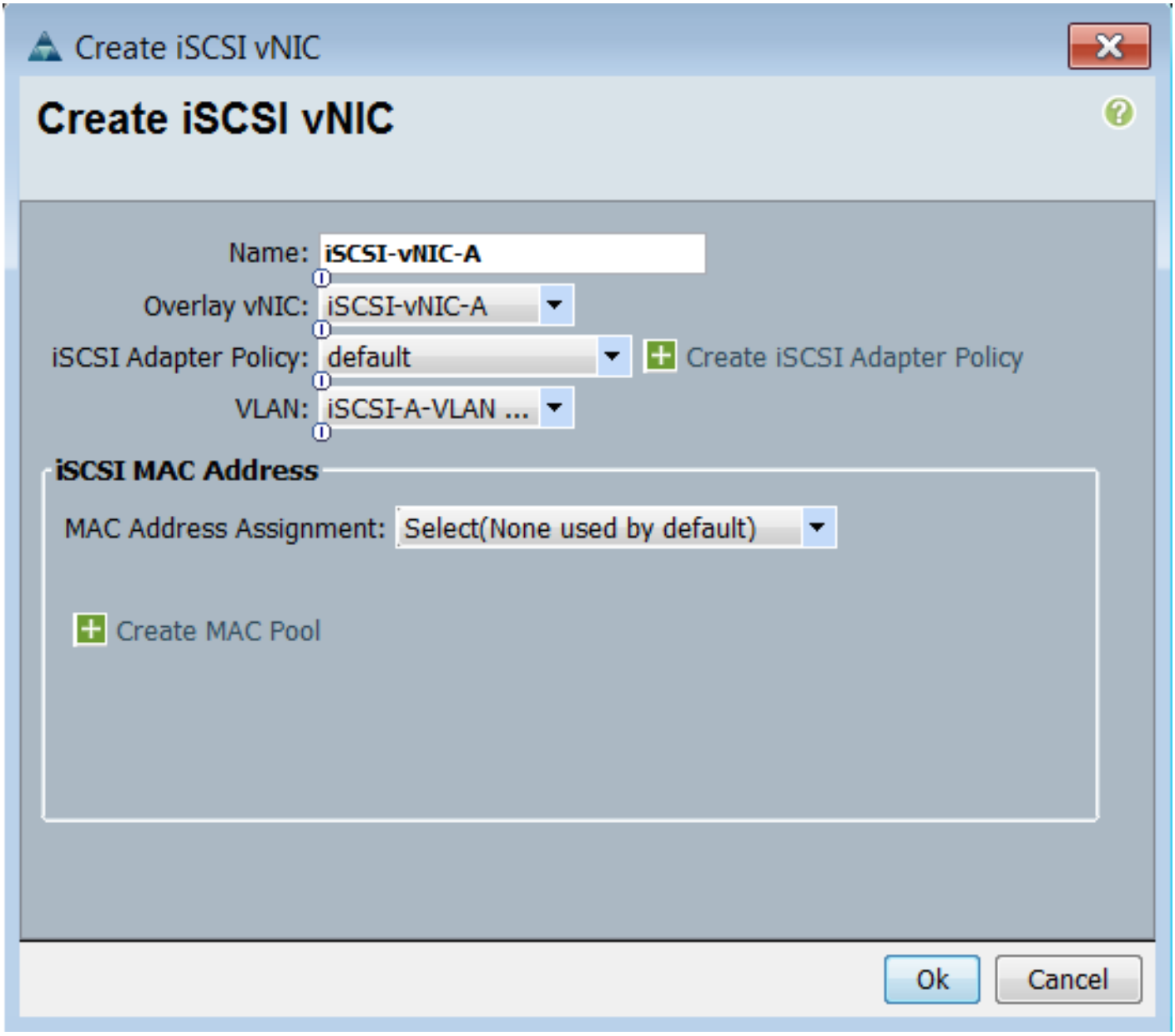
bb. Expand the iSCSI vNICs section and select `IQN_Pool` for the Initiator Name Assignment.



cc. Click the lower Add button to create an iSCSI vNIC.

dd. Name the iSCSI vNIC `iSCSI-vNIC-A`.

ee. Select the `iSCSI-vNIC-A` Overlay vNIC, the default iSCSI Adapter Policy, and the `iSCSI-A-VLAN` VLAN. Do not select a MAC Address Assignment.

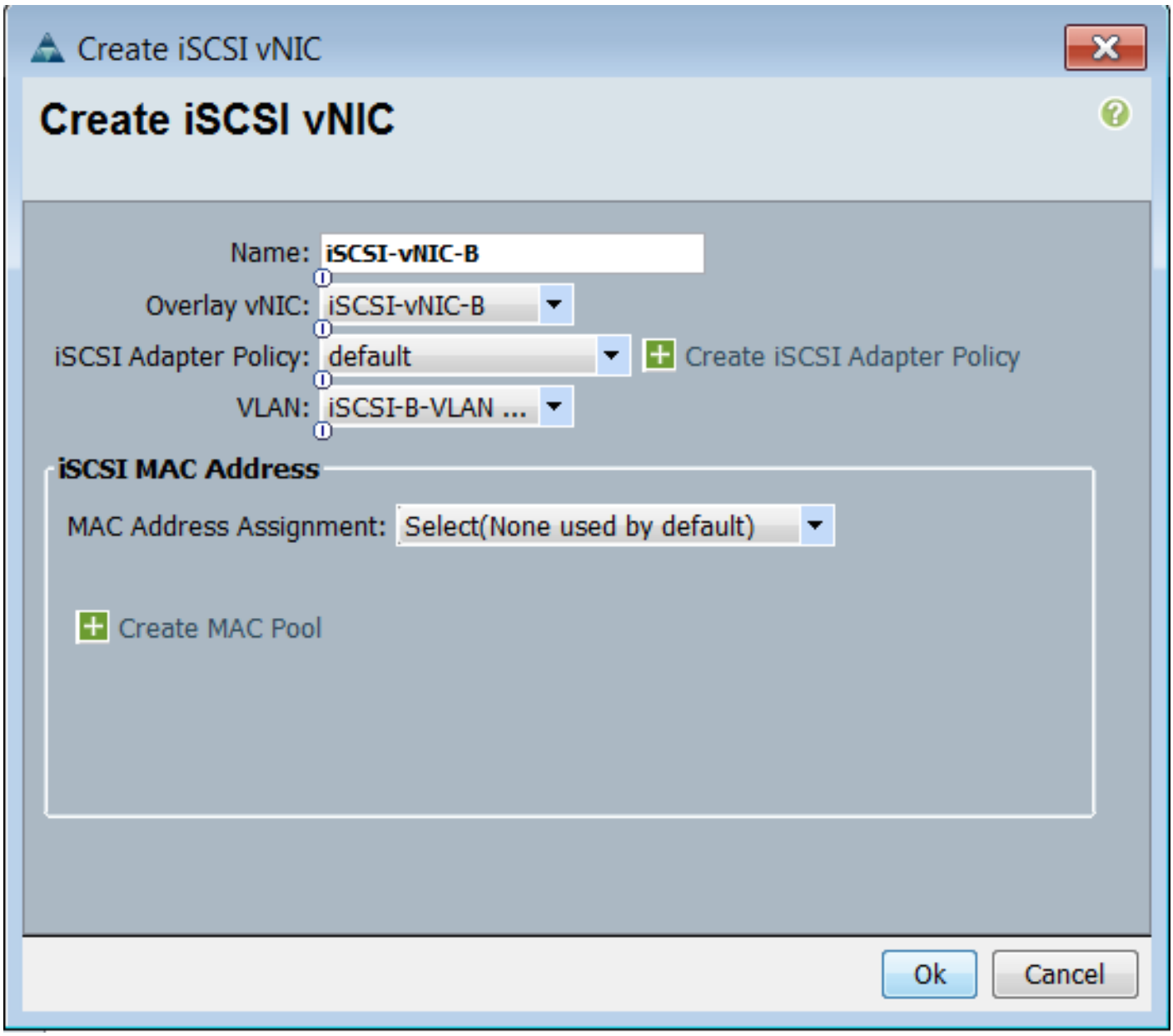


ff. Click OK to create the iSCSI vNIC.

gg. Click the lower Add button to create an iSCSI vNIC.

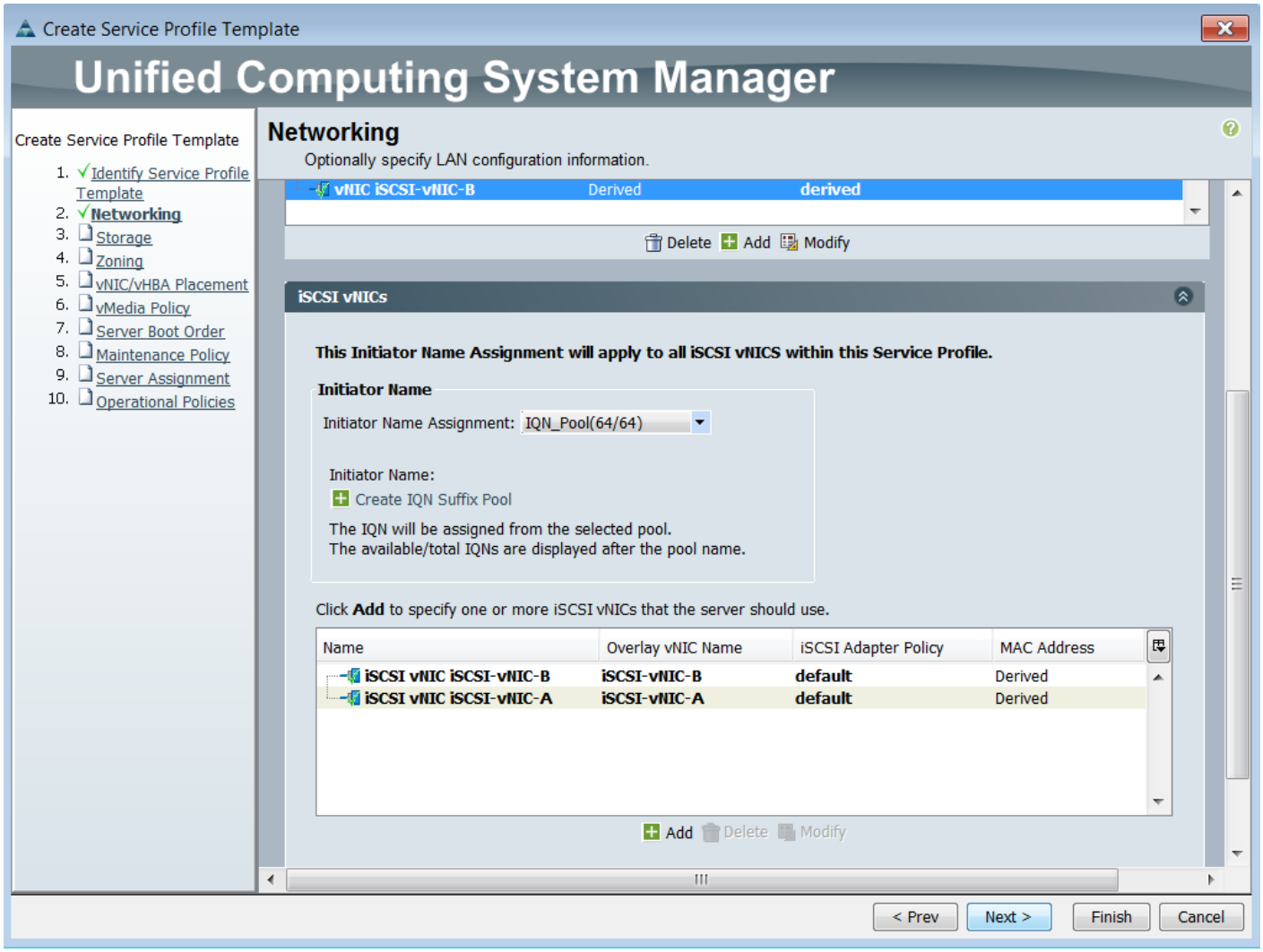
hh. Name the iSCSI vNIC `iSCSI-vNIC-B`.

ii. Select the iSCSI-vNIC-B Overlay vNIC, the default iSCSI Adapter Policy, and the `iSCSI-B-VLAN` VLAN. Do not select a MAC Address Assignment.



jj. Click OK to create the iSCSI vNIC.

kk. Review the table in the Networking page to confirm that both iSCSI vNICs were created.



ll. Click Next.

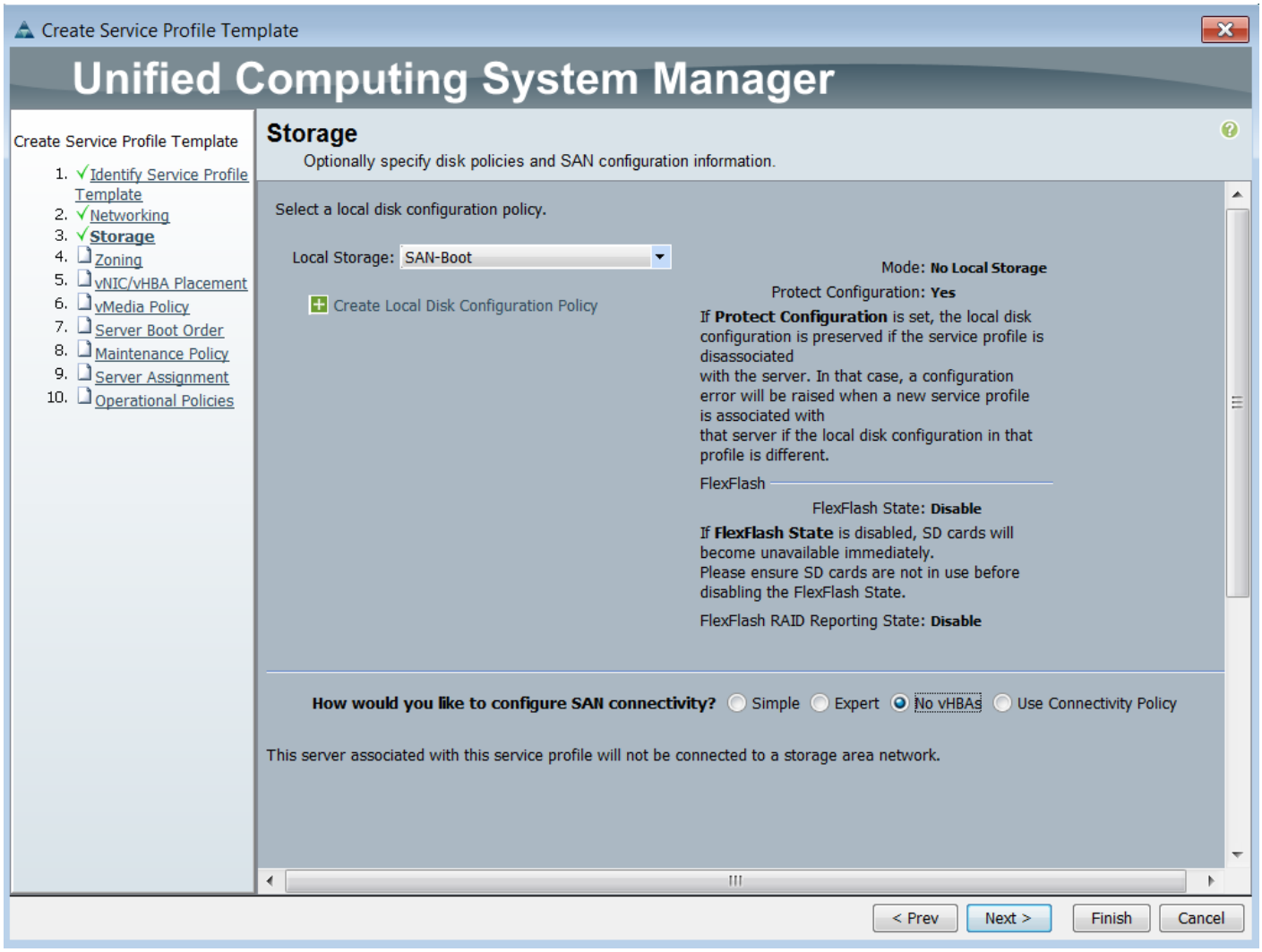
7. Configure the Storage options:

   a. Select a local disk configuration policy:

      — If the server in question has local disks, select default in the Local Storage list.

      — If the server in question does not have local disks, select `SAN-Boot`.

   b. Select the No vHBAs option to configure the SAN connectivity.



a. Click Next.

8. Set up Zoning.

a. Click Next

9. Set the vNIC/vHBA placement options.

a. In the Select Placement list, select the `VM-Host` placement policy.

b. Select vCon1 and assign the vHBAs/vNICs to the virtual network interfaces policy in the following order:

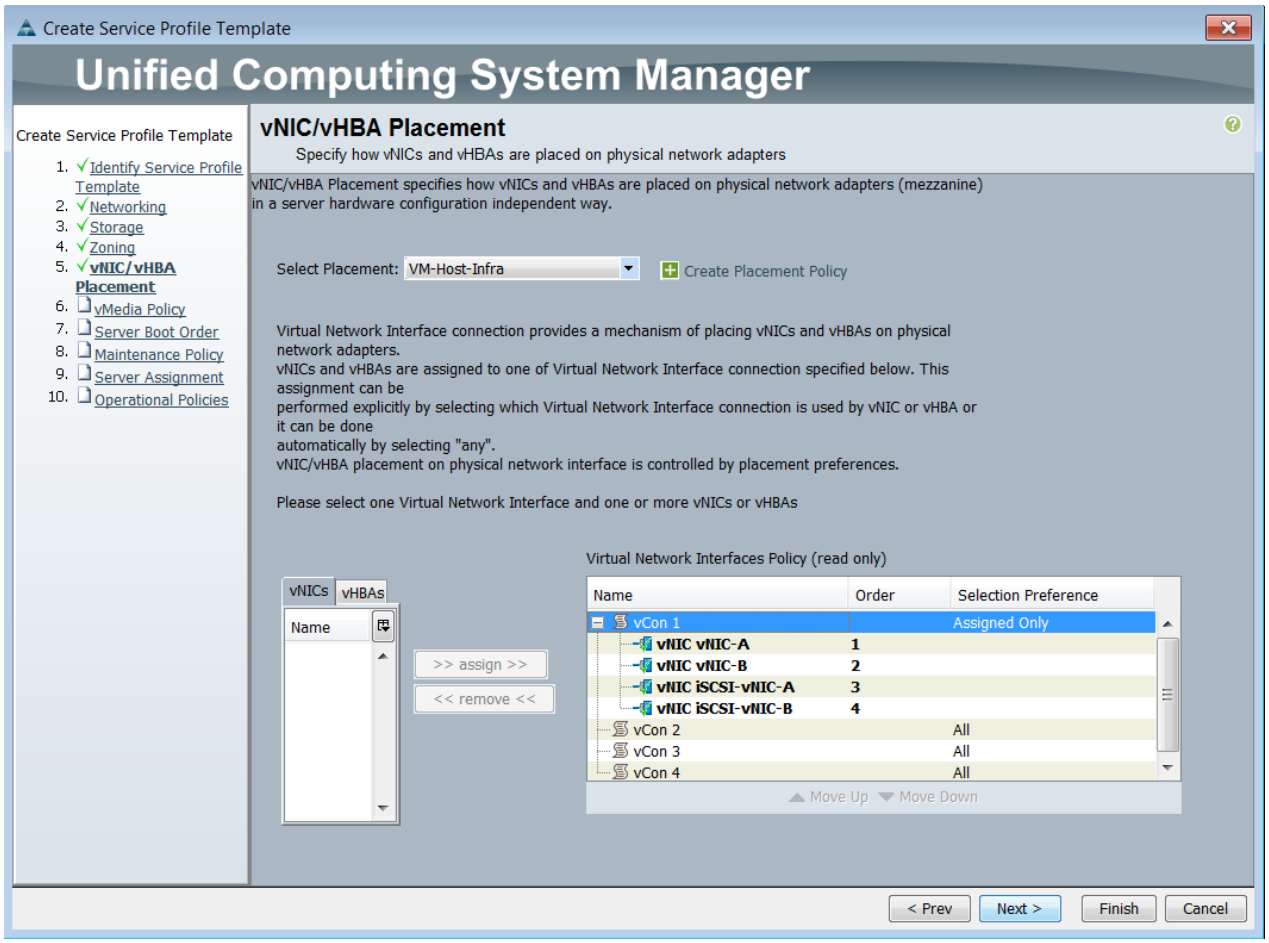
— `vNIC-A`

— `vNIC-B`

— `iSCSI-vNIC-A`

— `iSCSI-vNIC-B`

c. Review the table to verify that all of the vNICs were assigned to the policy in the appropriate order.



d. Click Next

10. vMedia Policy

a. Click next to use the default policy.

11. Set the Server Boot Order:

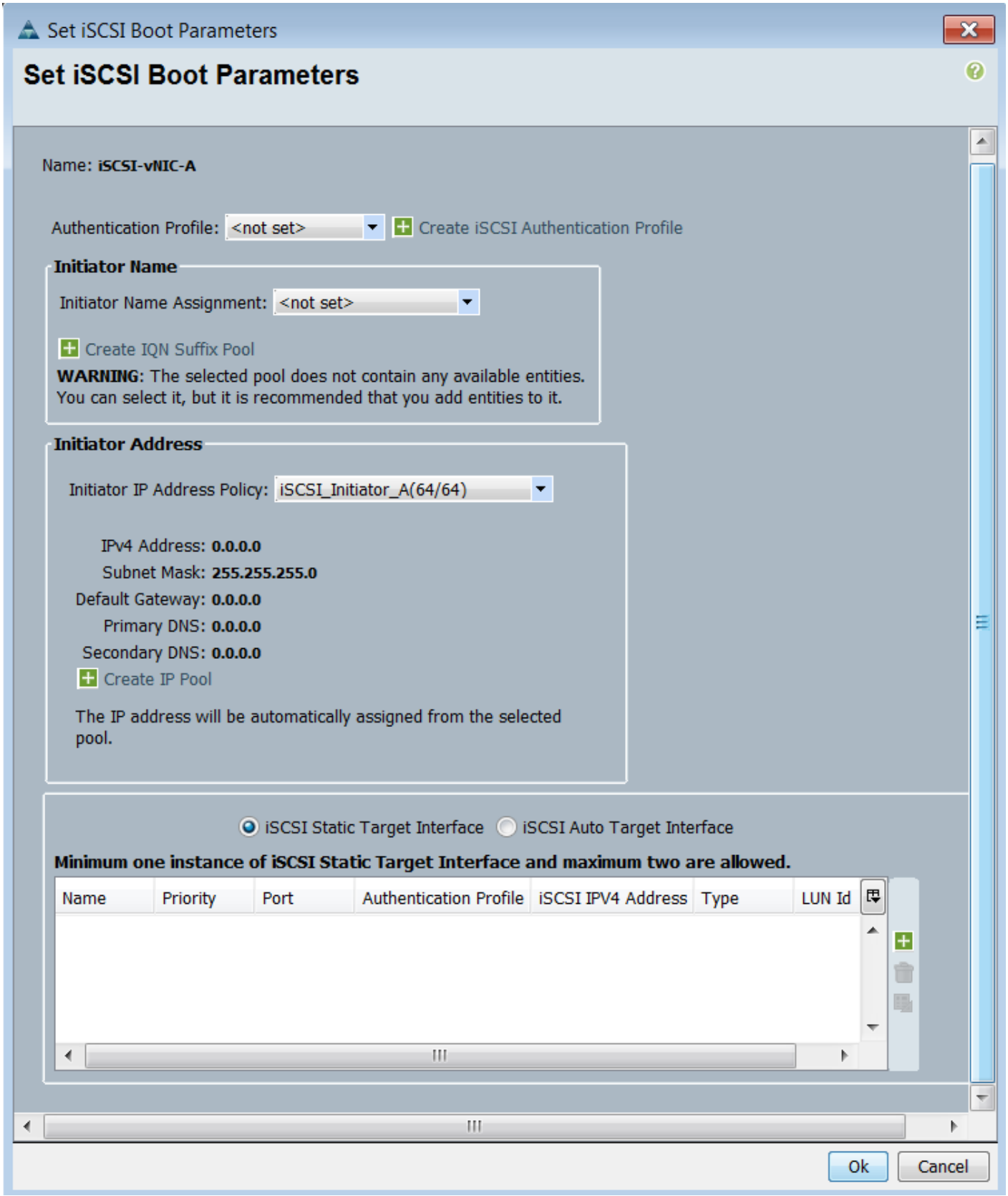
a. In the Boot Policy list, select `Boot-iSCSI-A`.

b. Expand the iSCSI in the lower window.

c. Select `iSCSI-vNIC-A`.

d. Click Set iSCSI boot parameters.

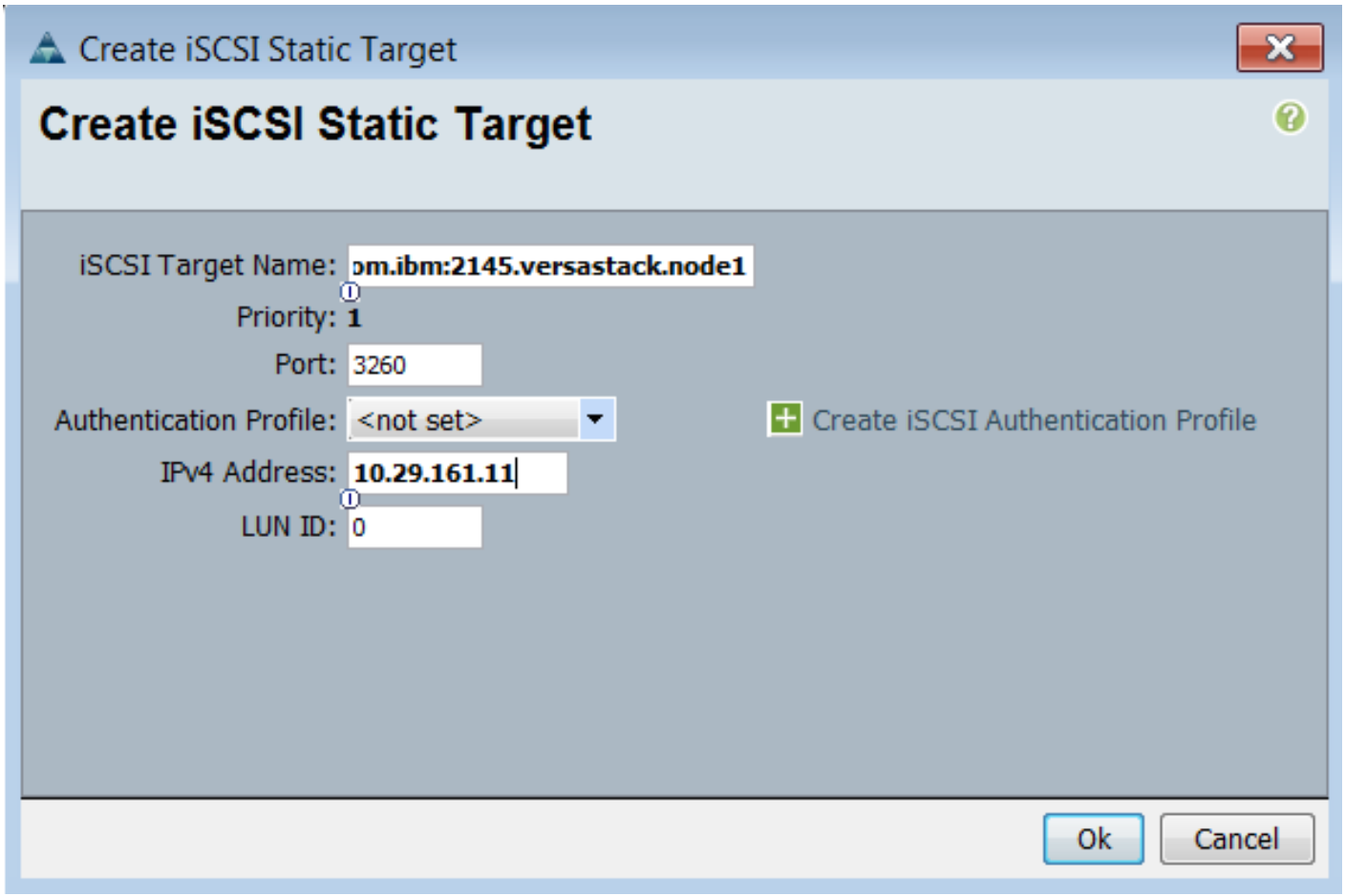
e. Set Initiator IP Address Policy to `iSCSI_initiator_A`.



f. Select iSCSI Static Target interface.

g. Click Add to add a static target.

h. Enter the IQN of V5000 node1 and the IP address of node1:`Eth3` in the static target window.

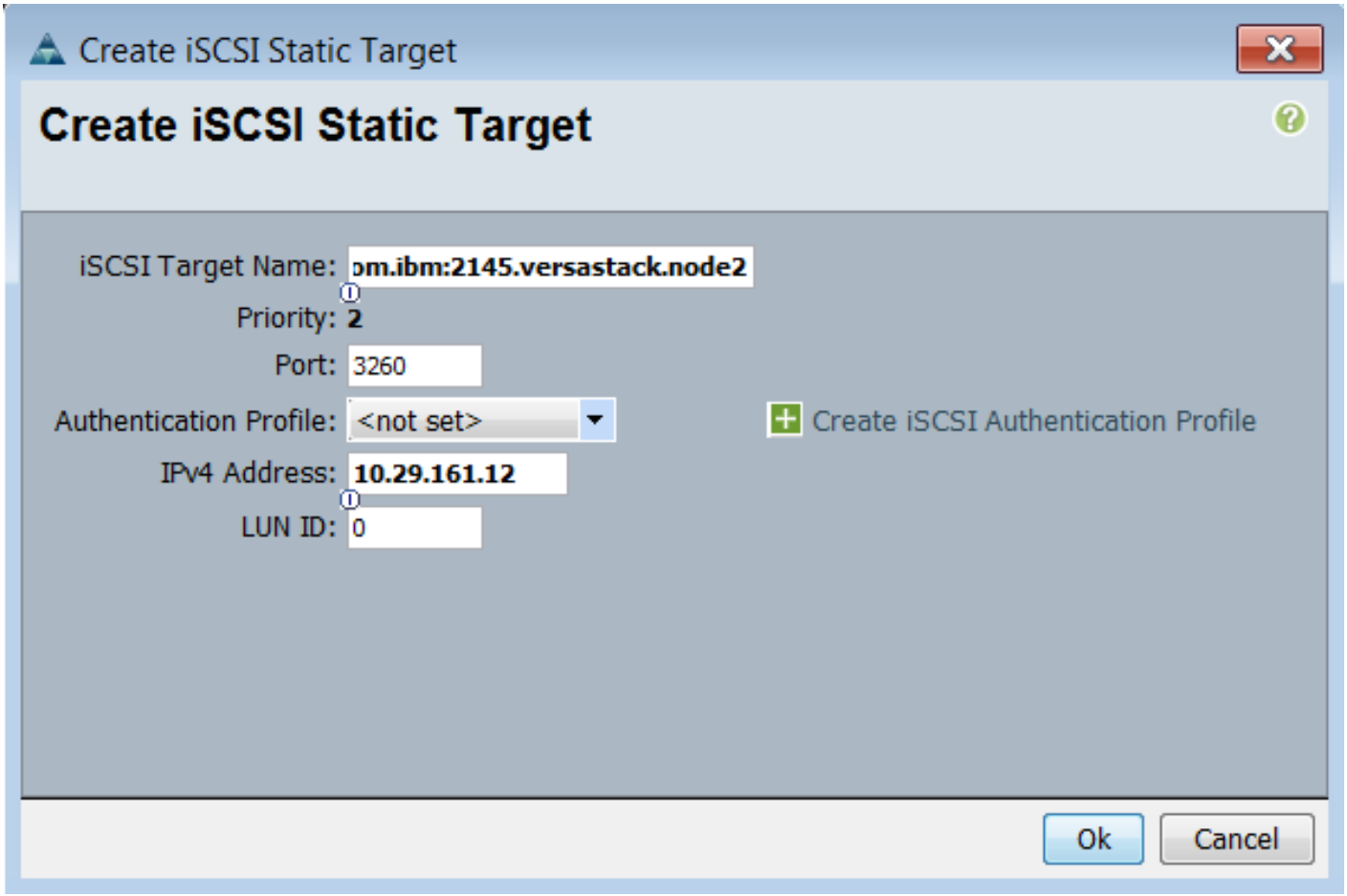


i. Click OK.

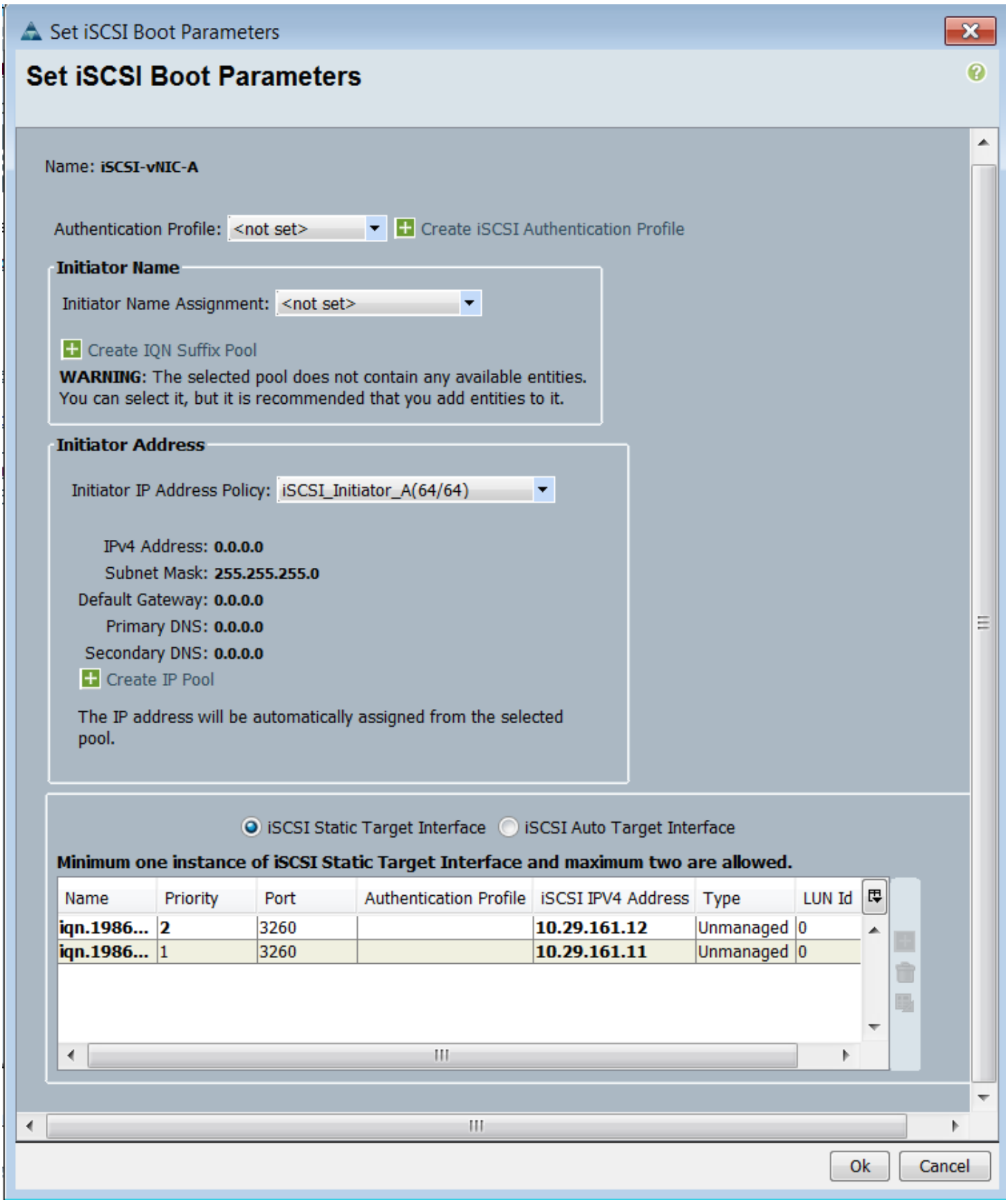
j. Click Add to add a static target.

k. Enter the IQN of V5000 node2 and the IP address of `node2:Eth3` in the static target window.

The V5000 node IQN can be obtained by logging into storewize gui and selecting Settings, Network, iSCSI.


Create iSCSI Static Target
Create iSCSI Static Target
iSCSI Target Name: om.ibm:2145.versastack.node2
Priority: 2
Port: 3260
Authentication Profile: <not set>
Create iSCSI Authentication Profile
IPv4 Address: 10.29.161.12
LUN ID: 0
Ok
Cancel

l. Click OK.



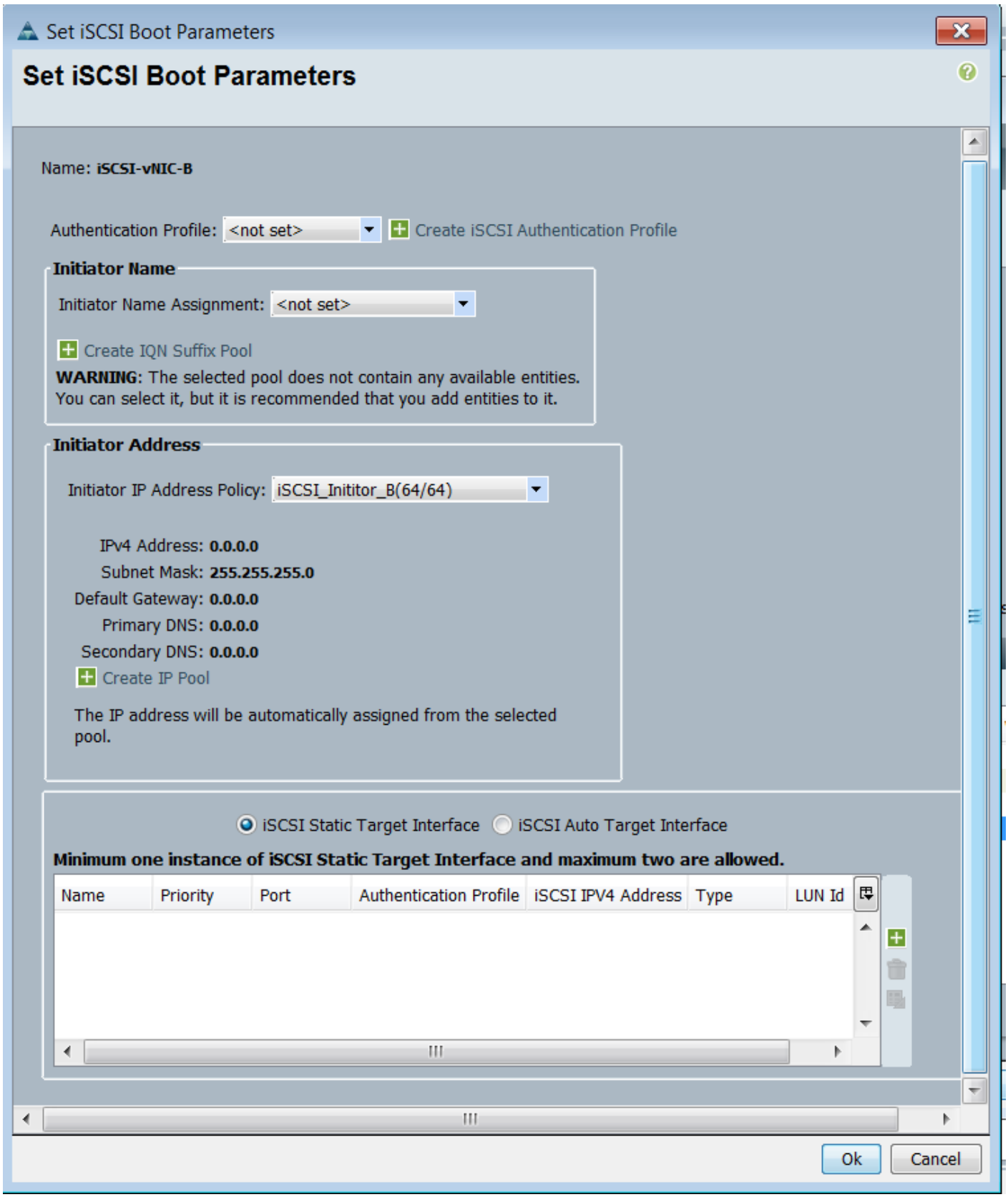
m. Review the table to verify that all of the iSCSI targets were created as identified.

n. Click OK.

o. In the iSCSI boot order, select `iSCSI-vNIC-B`.

p. Click Set iSCSI boot parameters.

q. Set Initiator IP Address Policy to `iSCSI_initiator_B`.

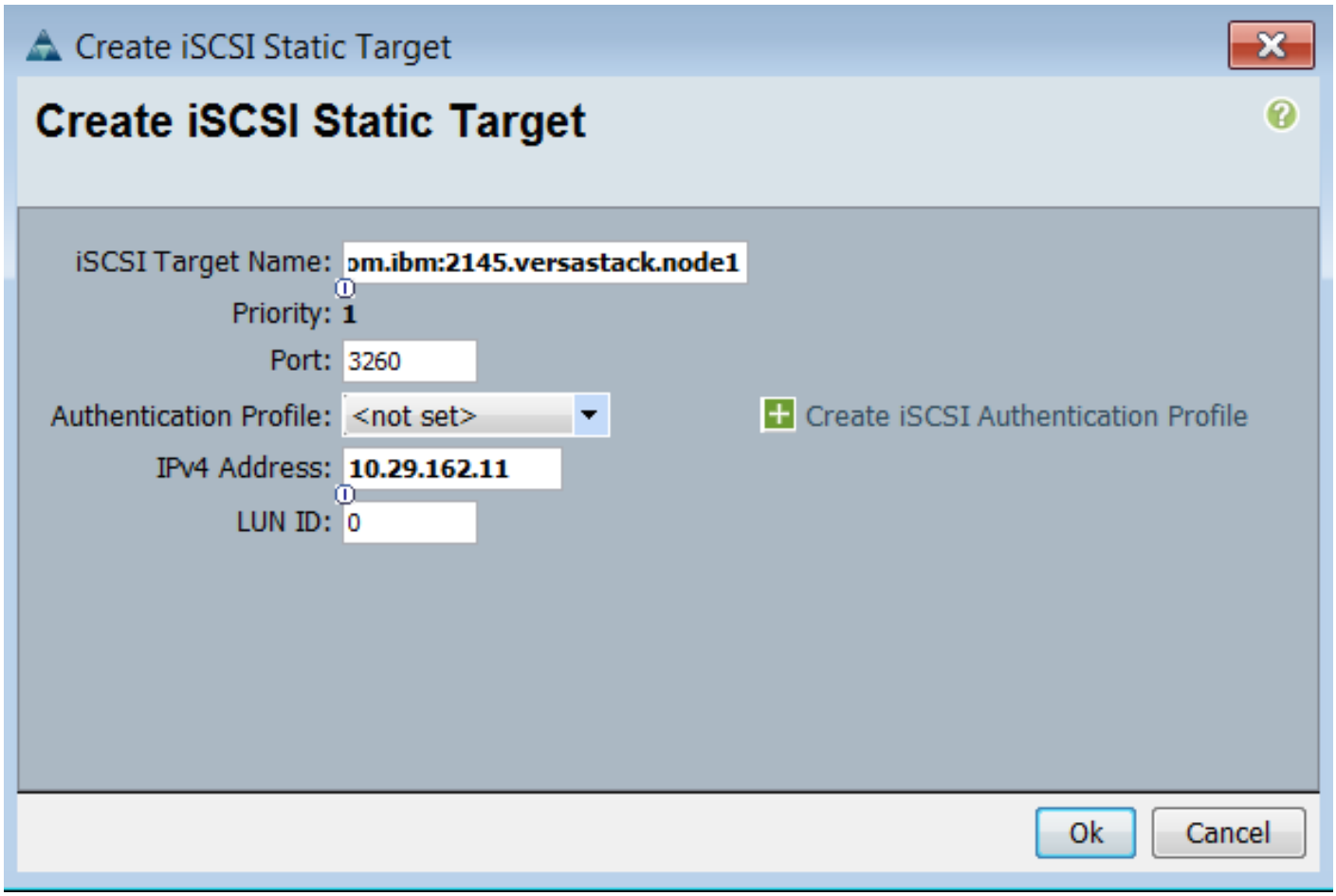


r. Select iSCSI Static Target interface.

s. Click Add to add a static target.

t. Enter the IQN of the V5000 node1 and the IP address of `node1:Eth4` in the static target window.

The V5000 node IQN can be obtained by logging into storewize gui and selecting Settings, Network, iSCSI.



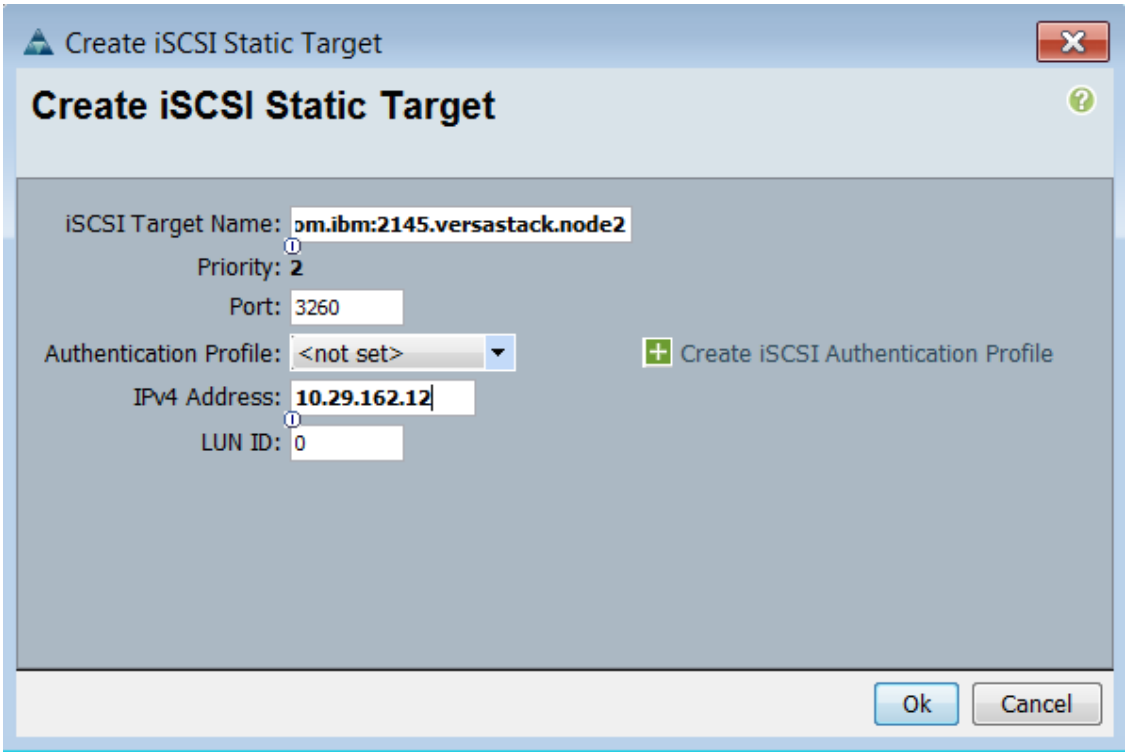
u. Click OK.

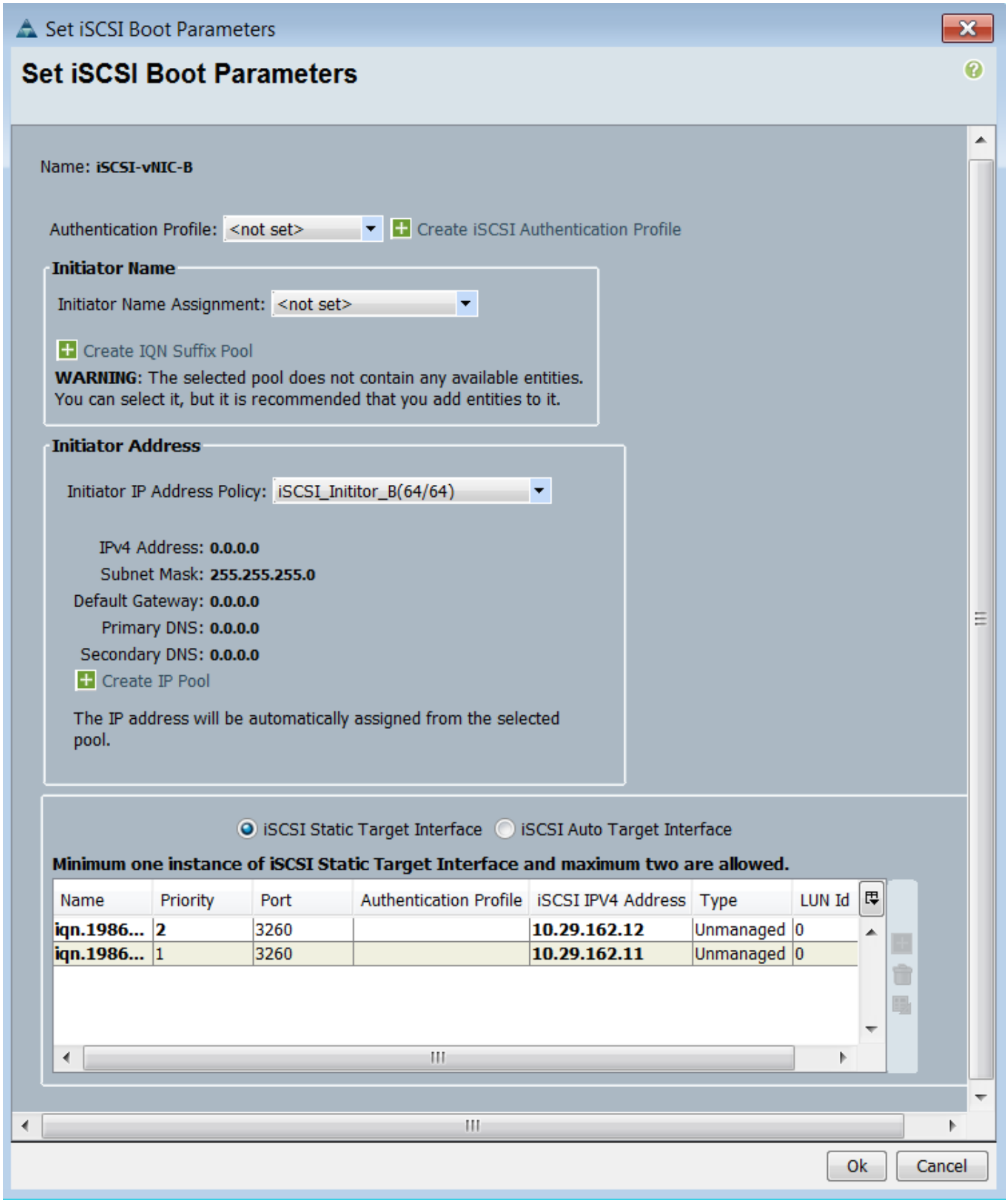
v. Click Add to add a static target.

w. Enter the IQN of the V5000 node2 and the IP address of `node2:Eth4` in the static target window.

The V5000 node IQN can be obtained by logging into storewize gui and selecting Settings, Network, iSCSI.

x. Click OK.


Create iSCSI Static Target
Create iSCSI Static Target
iSCSI Target Name: om.ibm:2145.versastack.node2
Priority: 2
Port: 3260
Authentication Profile: <not set>
Create iSCSI Authentication Profile
IPv4 Address: 10.29.162.12
LUN ID: 0
Ok
Cancel

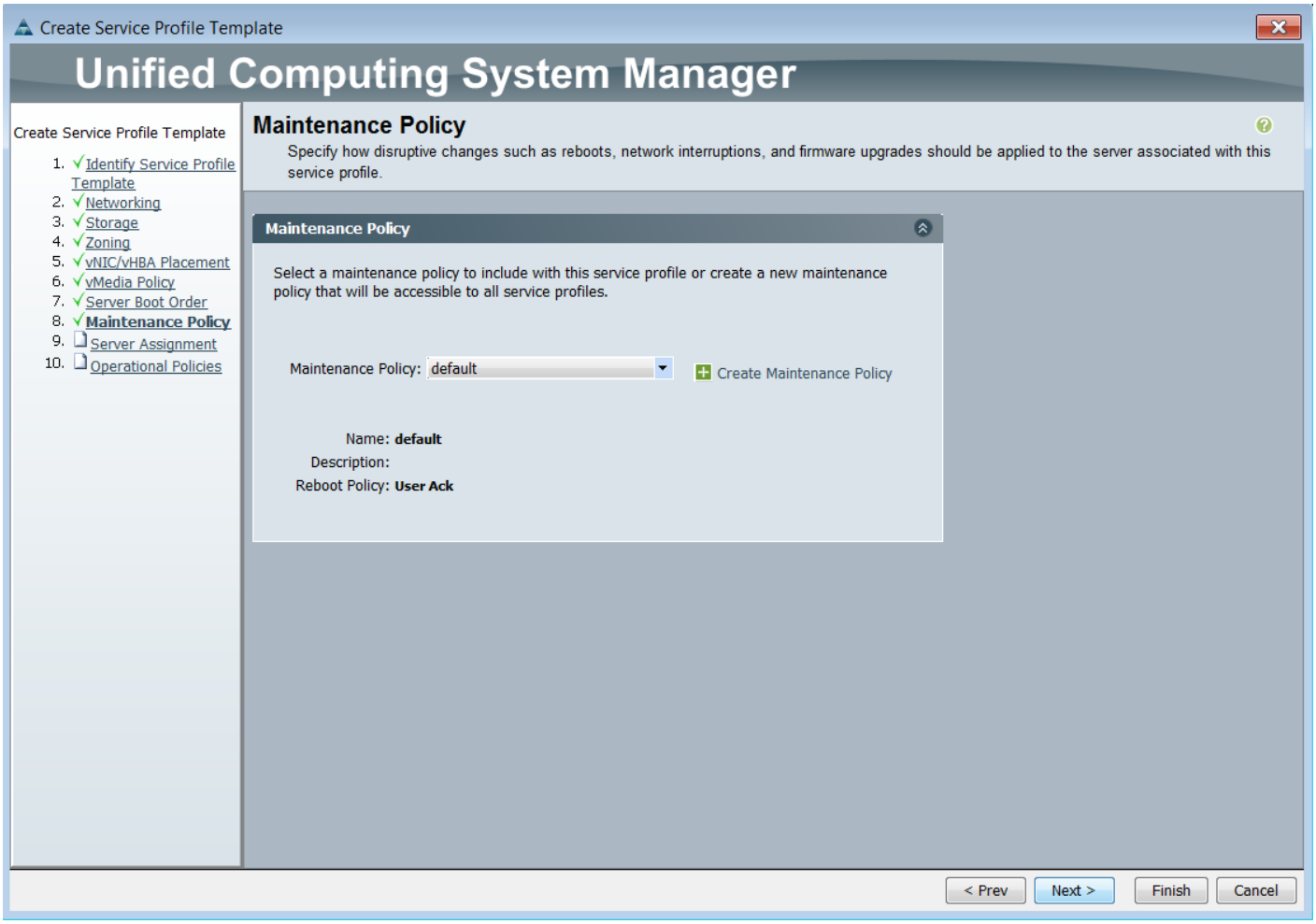


y. Review the table to verify that all of the iSCSI targets were created as identified.

z. Click OK, then Click Next.

12. Add a Maintenance Policy:

a. Select the default maintenance policy.



b. Click Next.

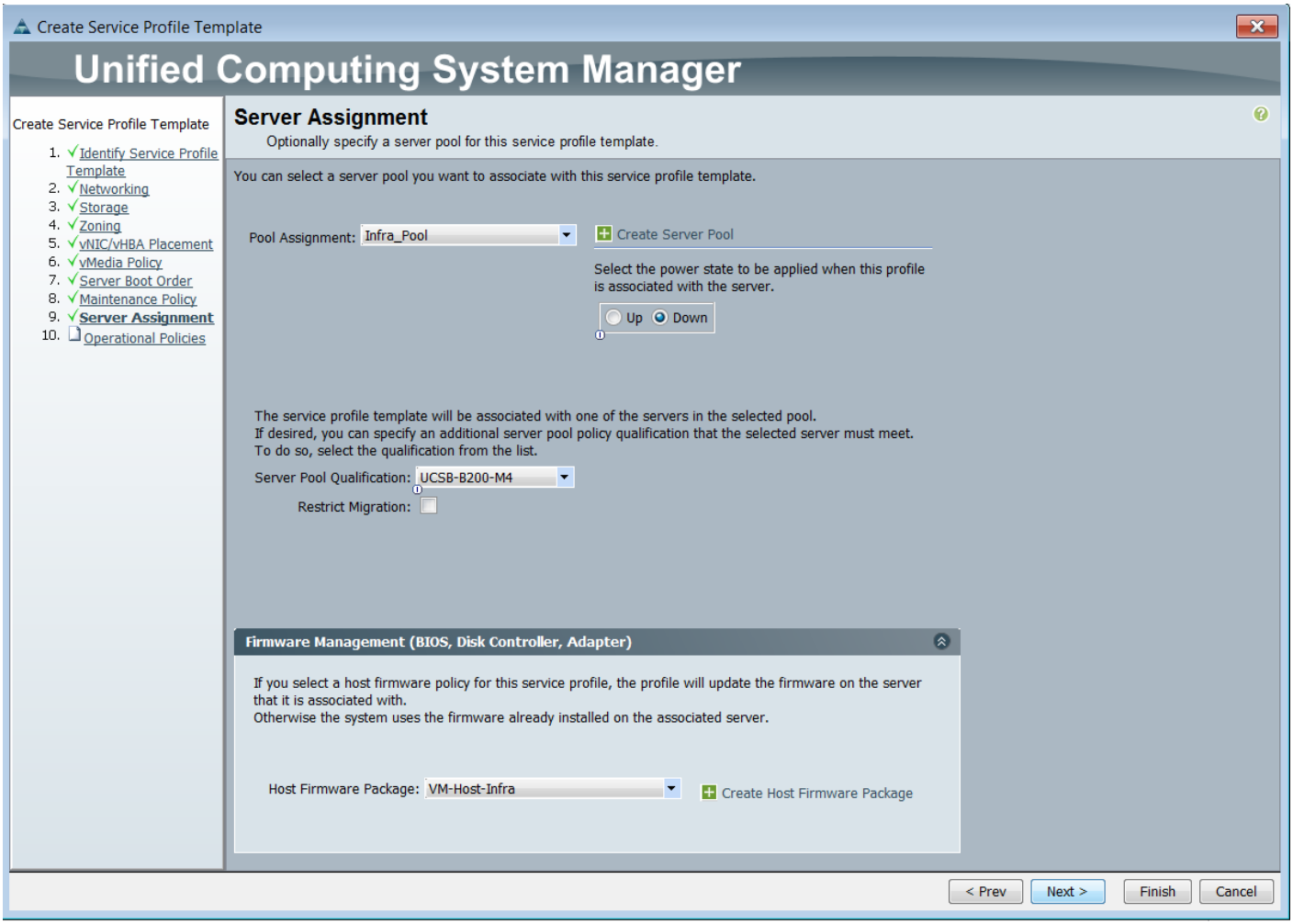
13. Specify the Server Assignment:

a. In the Pool Assignment list, select `Infra_Pool`.

b. Optional: Select a Server Pool Qualification policy.

c. Select Down as the power state to be applied when the profile is associated with the server.

d. Expand Firmware Management and select `VM-Host` from the Host Firmware list.

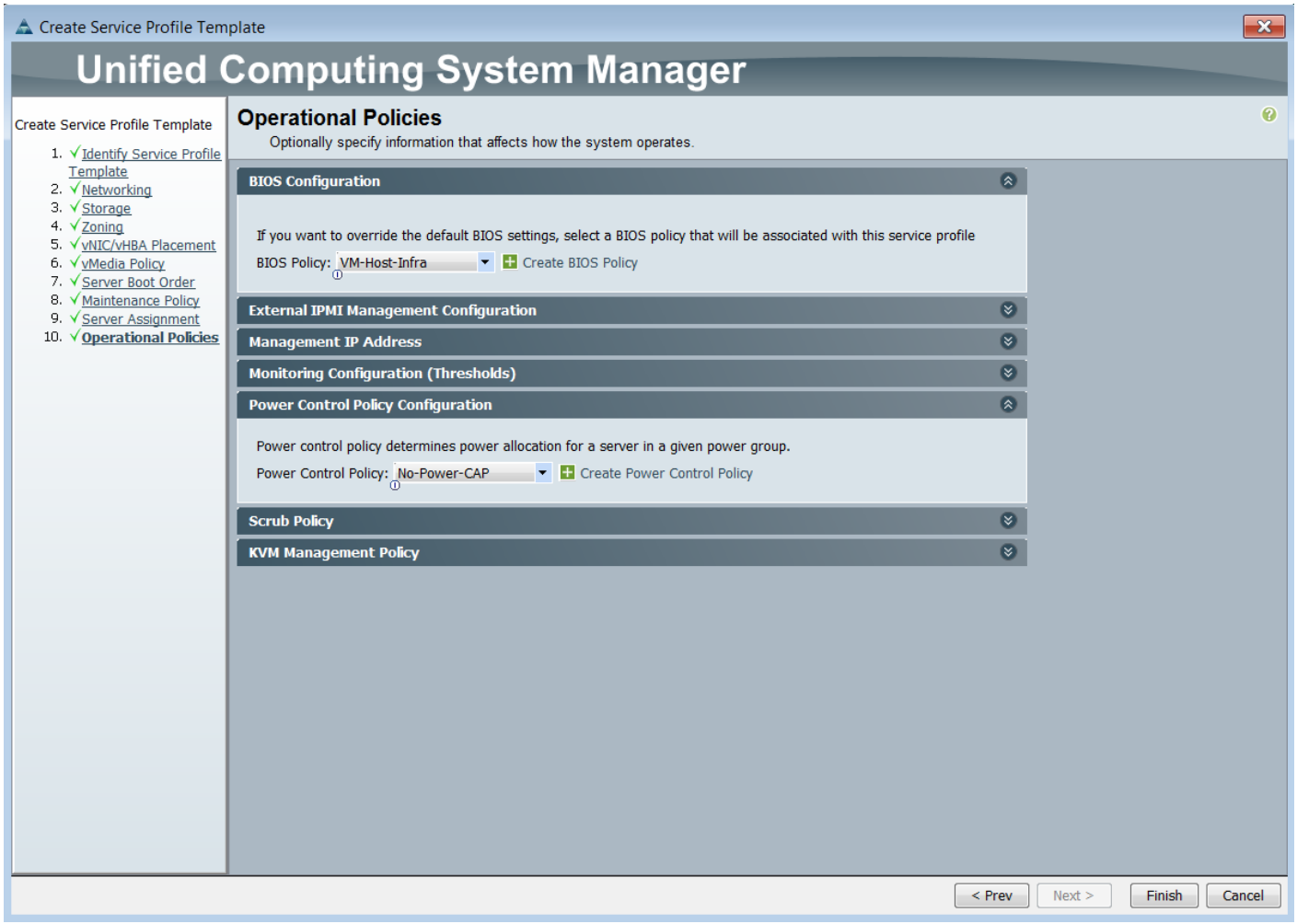


e. Click Next.

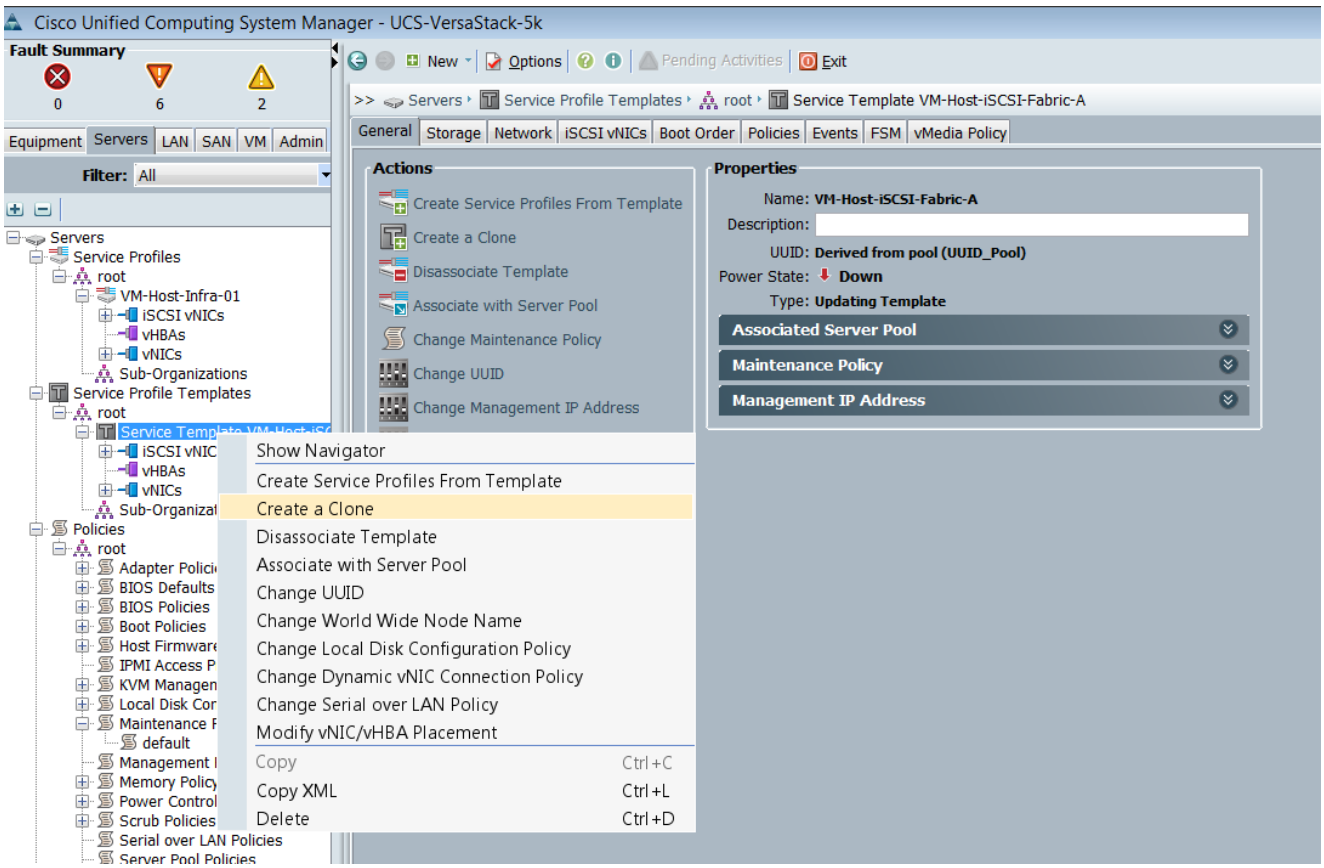
14. Add Operational Policies:

a. In the BIOS Policy list, select `VM-Host`.

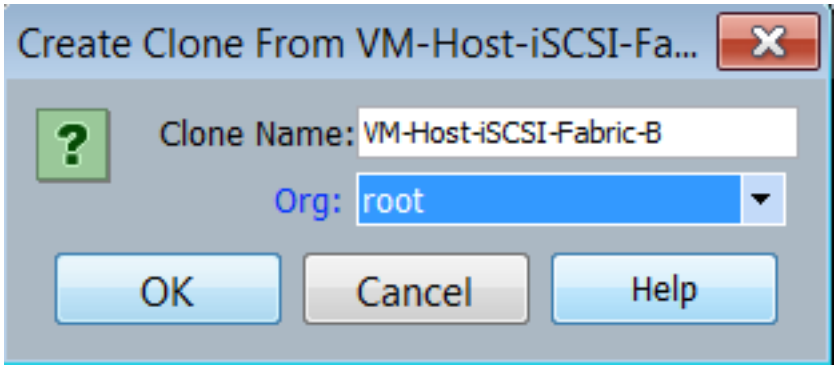
b. Expand Power Control Policy Configuration and select `No-Power-Cap` in the Power Control Policy list.



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. Choose Service Profile Templates > root.
19. Right-click the previously created `VM-Host-Infra-Fabric-A` template.
20. Choose Create a Clone.



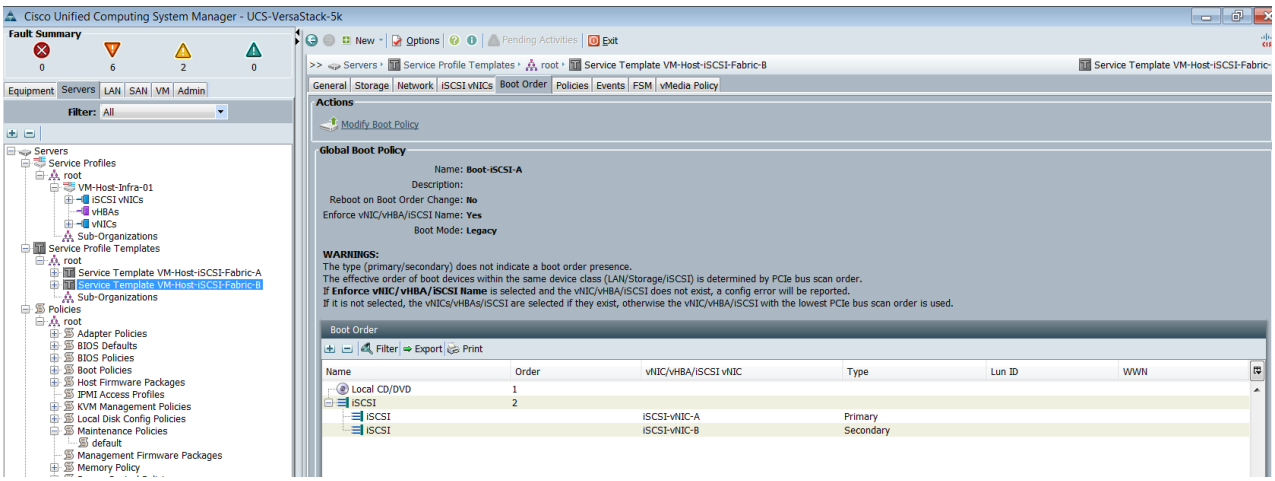
21. In the dialog box, enter VM-Host-Infra-Fabric-B as the name of the clone, choose the root Org, and click OK.



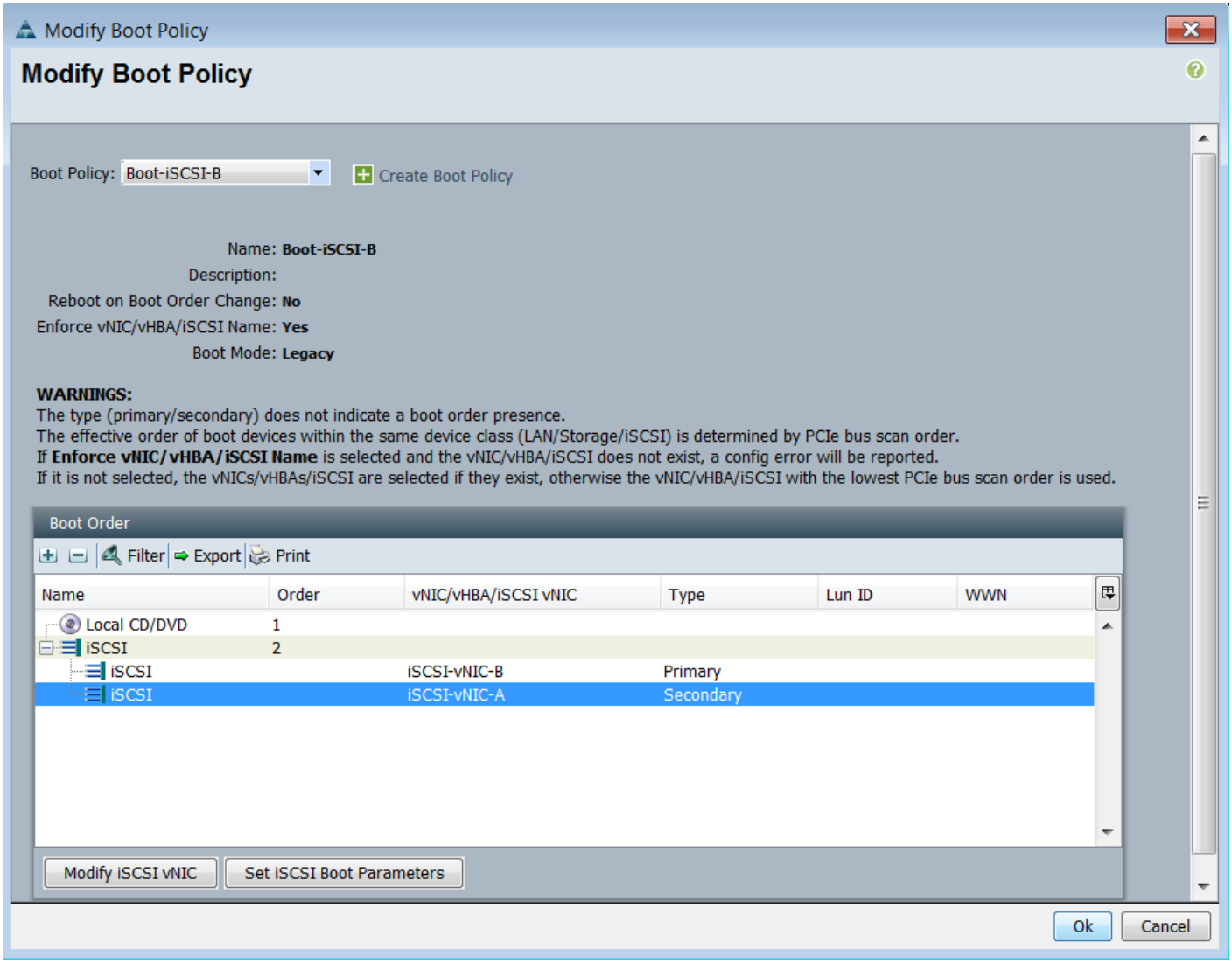
22. Click OK.

23. Choose the newly cloned service profile template and click the Boot Order tab.

24. Click Modify Boot Policy.

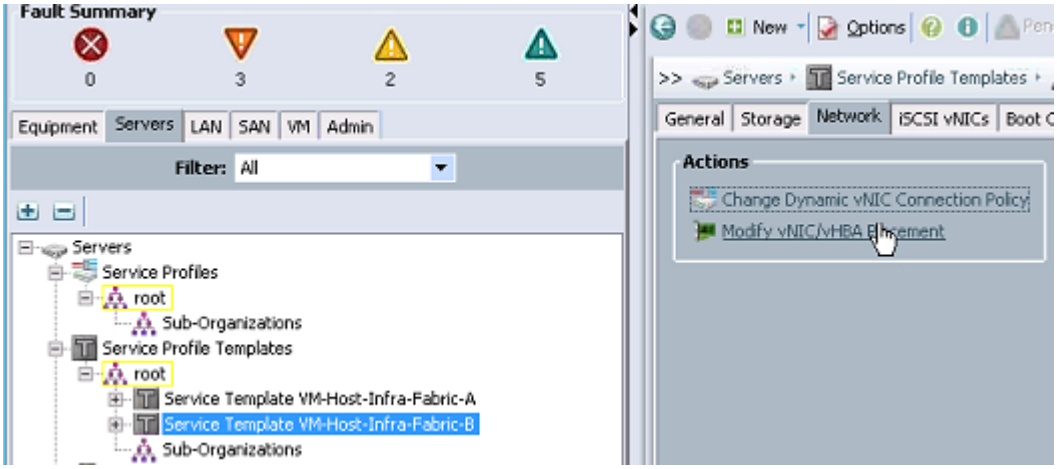


25. In the Boot Policy list, choose `Boot-Fabric-B`.



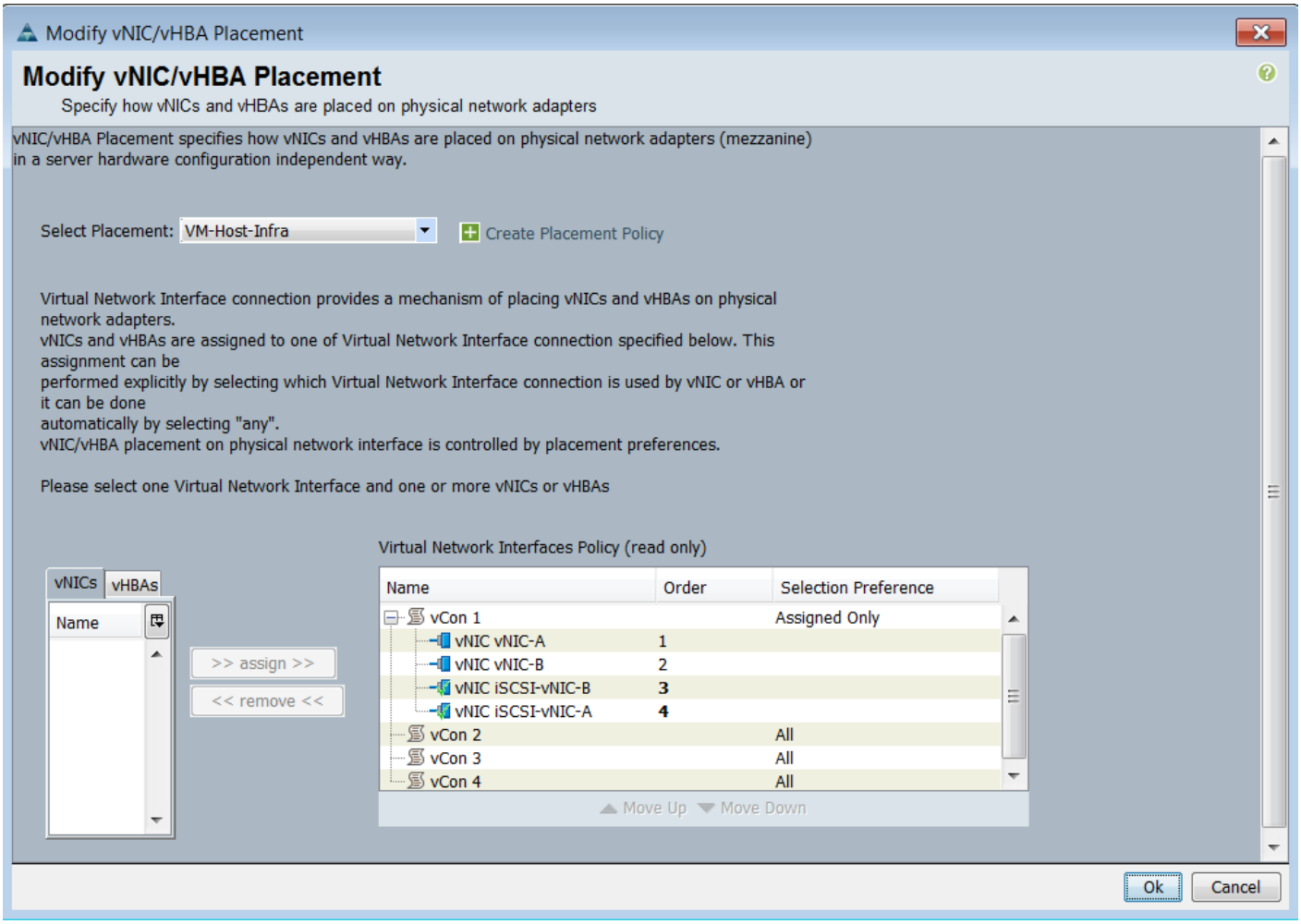
26. Click OK and then click OK again.

27. In the right pane, click the Network tab and then click Modify vNIC/HBA Placement.



28. Select VM-Host-Infra and Expand vCon 1 and move vNIC iSCSI-vNIC-B ahead of vNIC iSCSI-vNIC-A in the placement order.

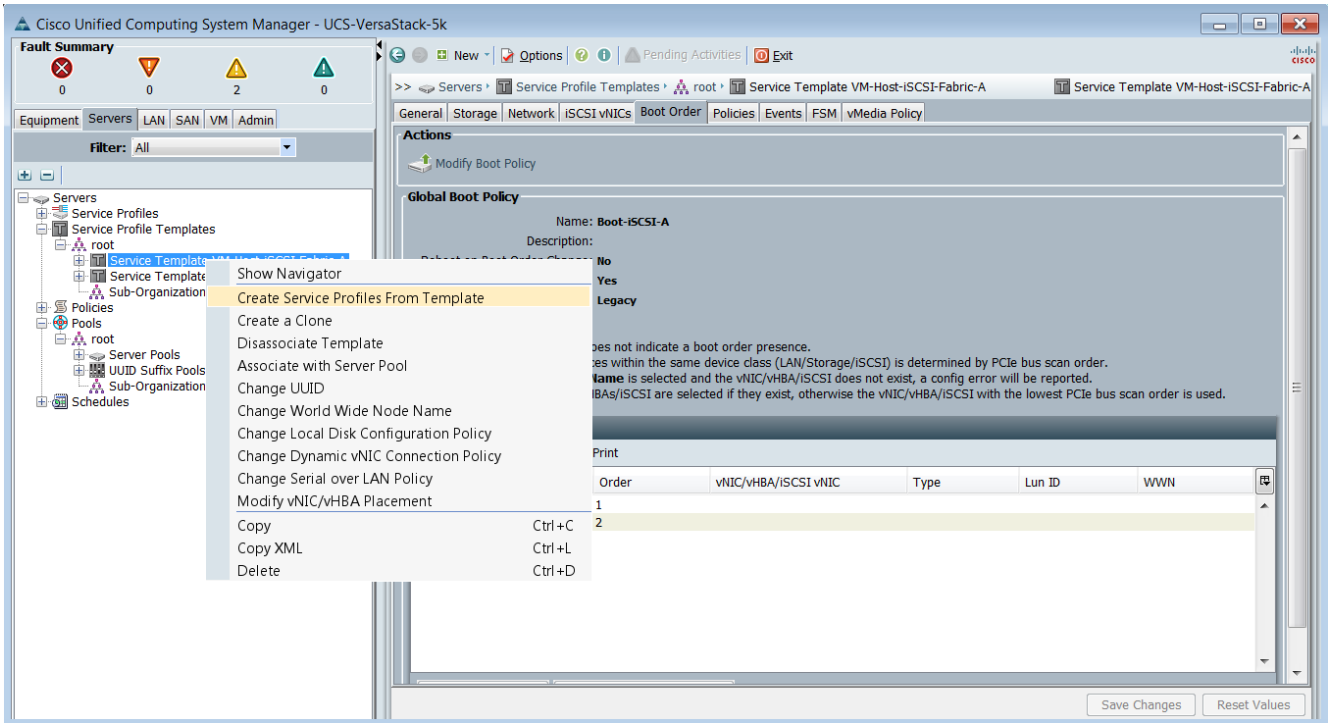
29. Click OK and then click OK again.



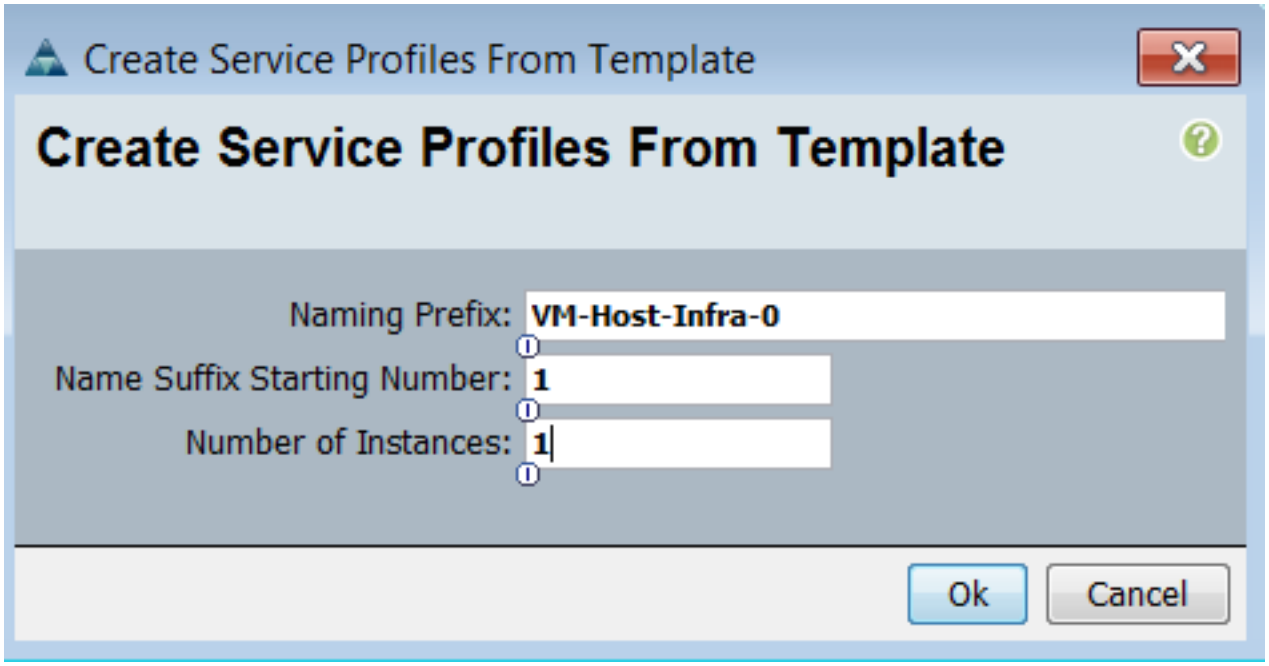
Create Service Profiles

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-Fabric-A`.
3. Right-click `VM-Host-Infra-Fabric-A` and select Create Service Profiles from Template.

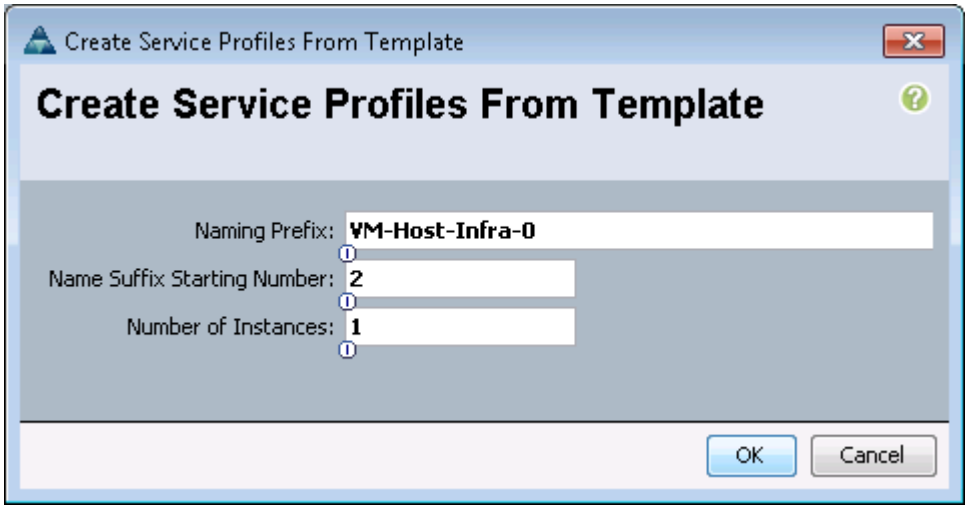


4. Enter `VM-Host-Infra-0` as the Naming Prefix.
5. Enter 1 as the Suffix Starting Number.
6. Enter `1` as the Number of Instances to create.



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-Fabric-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. In the confirmation message, click OK.

Backup the Cisco UCS Manager Configuration

It is recommended that you backup your Cisco UCS Configuration. Please refer to the link below for additional information:

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/gui/config/guide/2-2/b_UCSM_GUI_Configuration_Guide_2_2/b_UCSM_GUI_Configuration_Guide_2_2_chapter_0101010.html

Add More Servers to VersaStack Unit

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

Gather Necessary Information

After the Cisco UCS service profiles have been created, each infrastructure blade in the environment will have a unique configuration. To proceed with the VersaStack deployment, specific information must be gathered from each Cisco UCS blade and from the Storwize V5000 controllers. Insert the required information into Table 13 .

Table 13 iSCSI IQNs and IPs for each ESXi Host

Cisco UCS Service Profile Name	iSCSI IQN	iSCSI-vNIC-A IP	iSCSI-vNIC-B IP
VM-Host-Infra-01			
VM-Host-Infra-02			

To gather the iSCSI IQN information, launch the Cisco UCS Manager GUI. In the navigation pane, click the Servers tab. Expand Servers > Service Profiles > root. Click each service profile then click the iSCSI vNICs tab in the right pane. The iSCSI Initiator Name is the host's iSCSI IQN. To get the iSCSI vNIC IP addresses, click the Boot Order tab. Expand iSCSI in the list below and select an iSCSI vNIC. At the bottom of the page, select Set iSCSI Boot Parameters. The IP address is shown in this window

Storage LUN Mapping

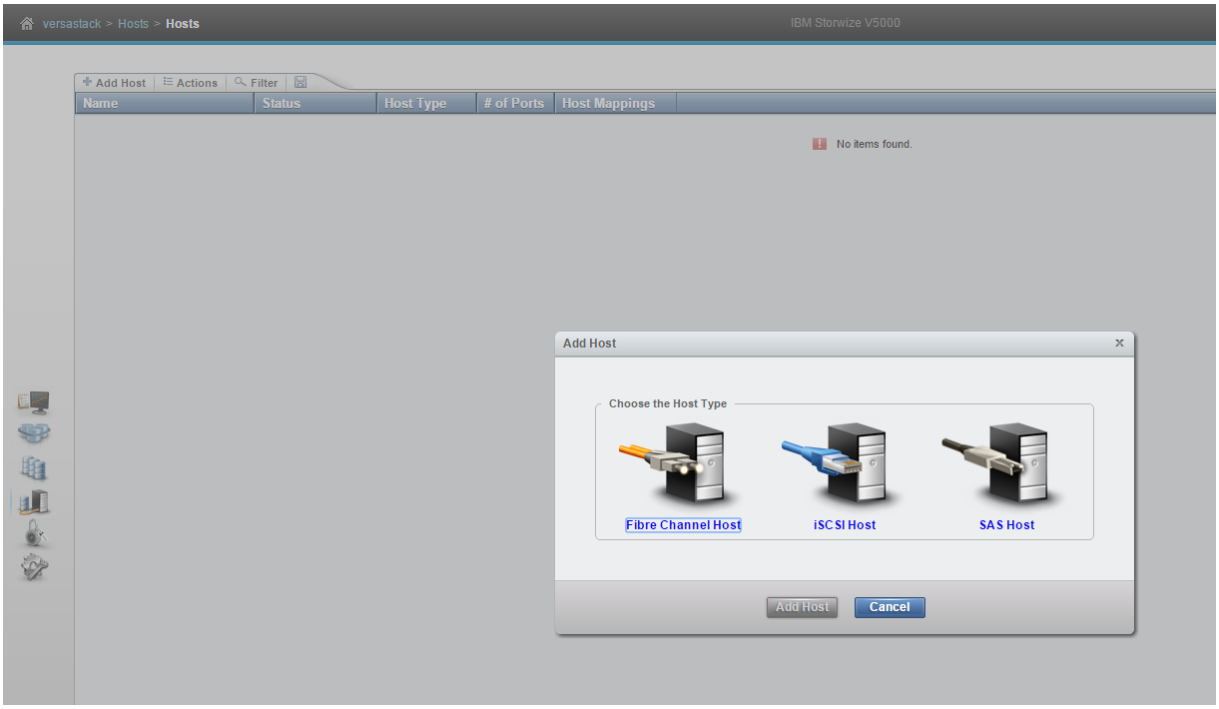
In this section, you will add the host mappings for the host profiles created through the Cisco UCS Manager to the IBM Storwize V5000 storage, connecting to the boot LUNs, and doing the initial ESXi install.

Adding Hosts and Mapping the Boot Volumes on the IBM Storwize V5000

1. Open the Storwize V5000 management GUI by navigating to `<<var_cluster_mgmt_ip>>`and log in with your superuser or admin account.

2. In the left pane click Host icon, and click the Hosts menu item.

3. Click Add Host in the upper left menu to bring up the Host wizard. Select the iSCSI Host option.

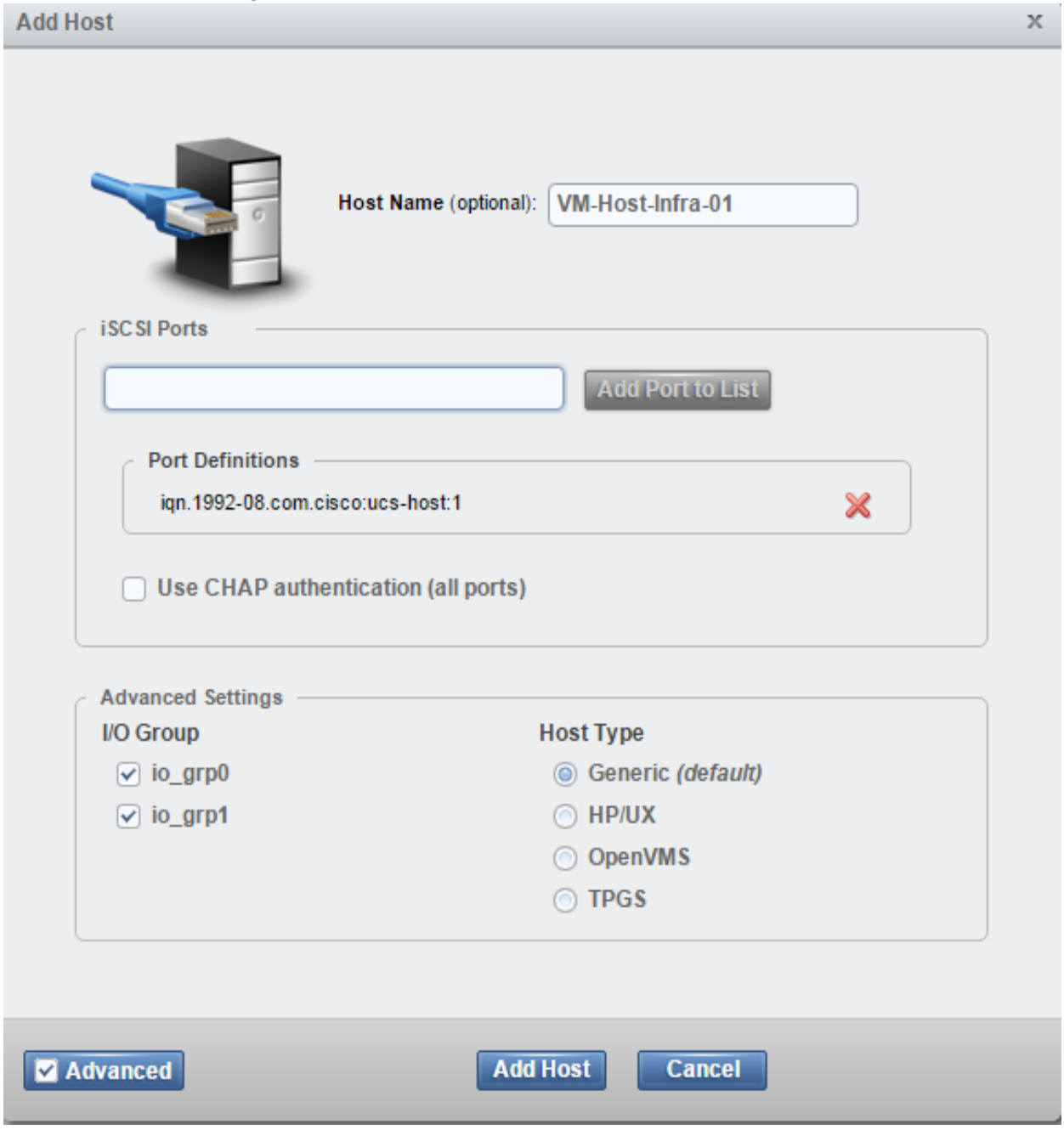


4. Input Host Name `VM-Host-Infra-01`.

5. For iSCSI Ports input the initiator name `<<var_iqn_VM-Host-infra-01-a>>` and click Add Port to List ,

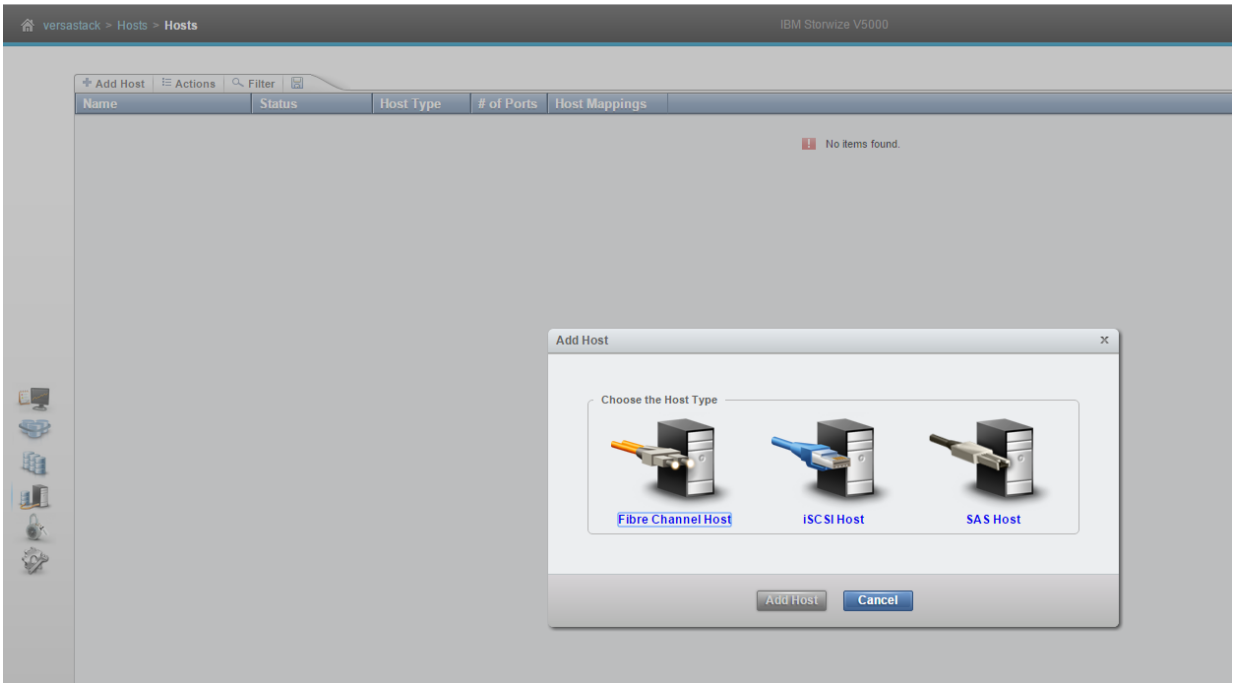
6. Click Close.

7. Leave Advanced Settings as default and click Add Host, then click Close.

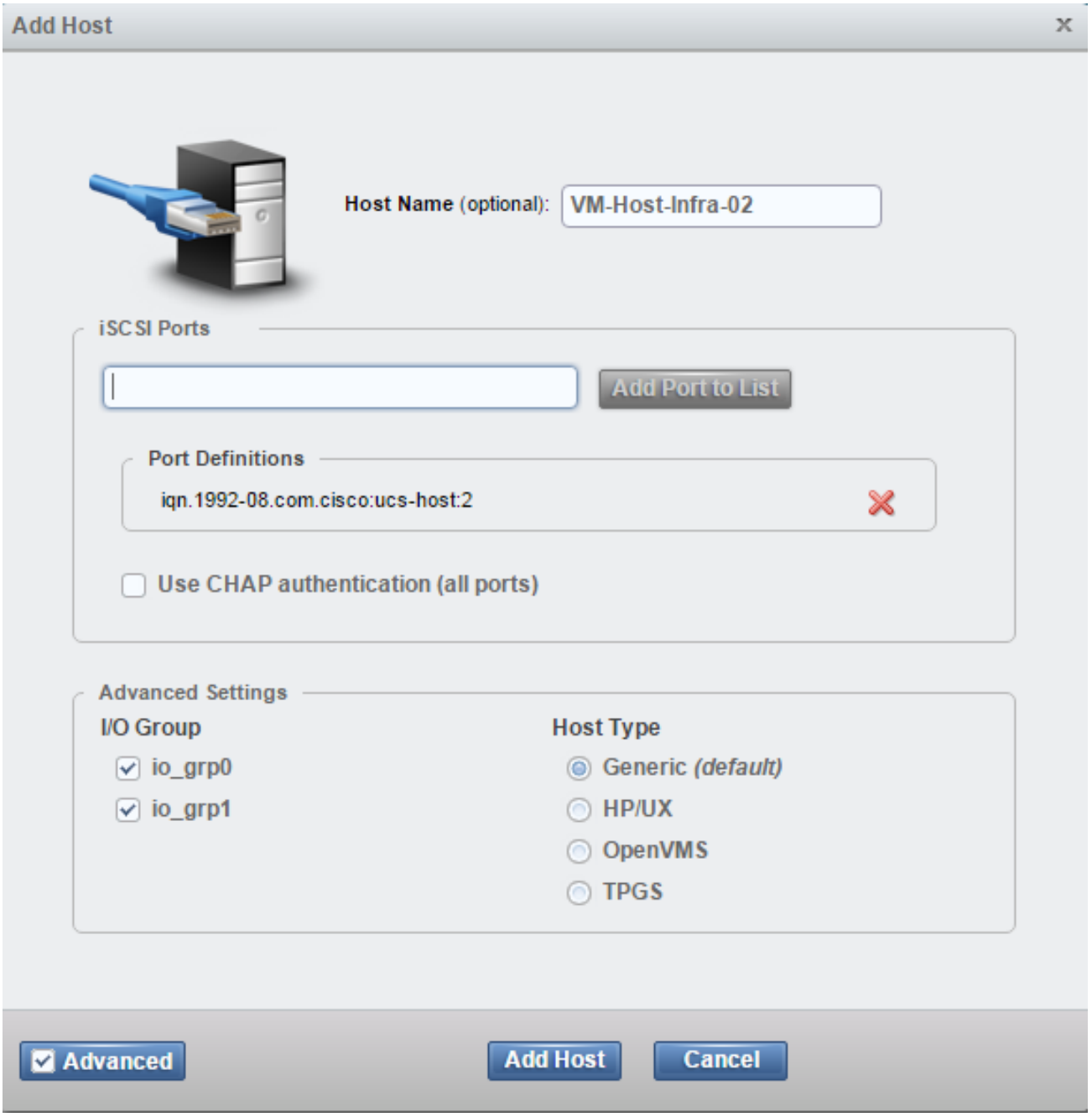


8. Click Add Host to create the second host.

9. Select the iSCSI Host option..

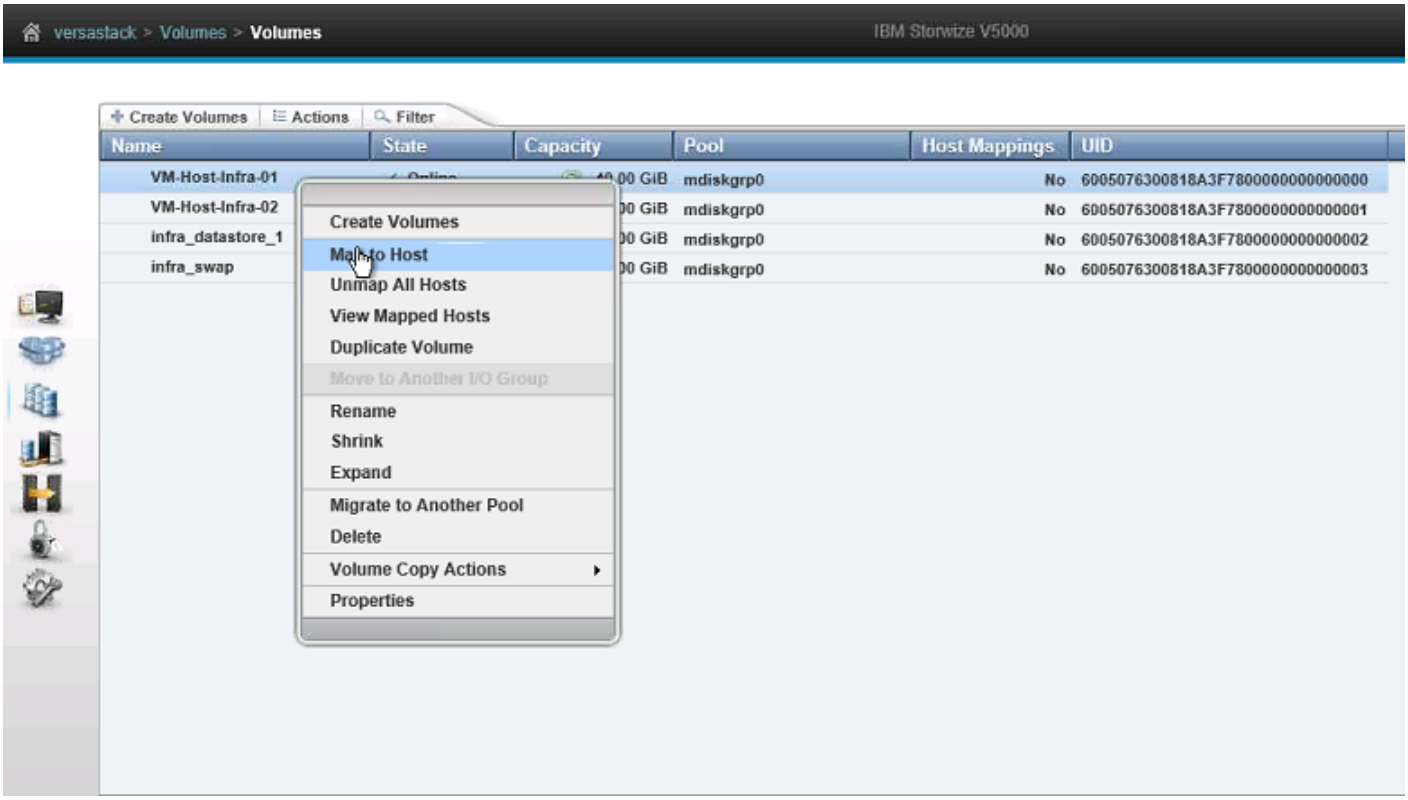


10. Input Host Name VM-Host-Infra-02.
11. For iSCSI Ports input the initiator name `<<var_iqn_VM-Host-infra-02-a>>` and click Add Port to List ,
12. Click Close.
13. Leave Advanced Settings as default and click Add Host, then click Close.

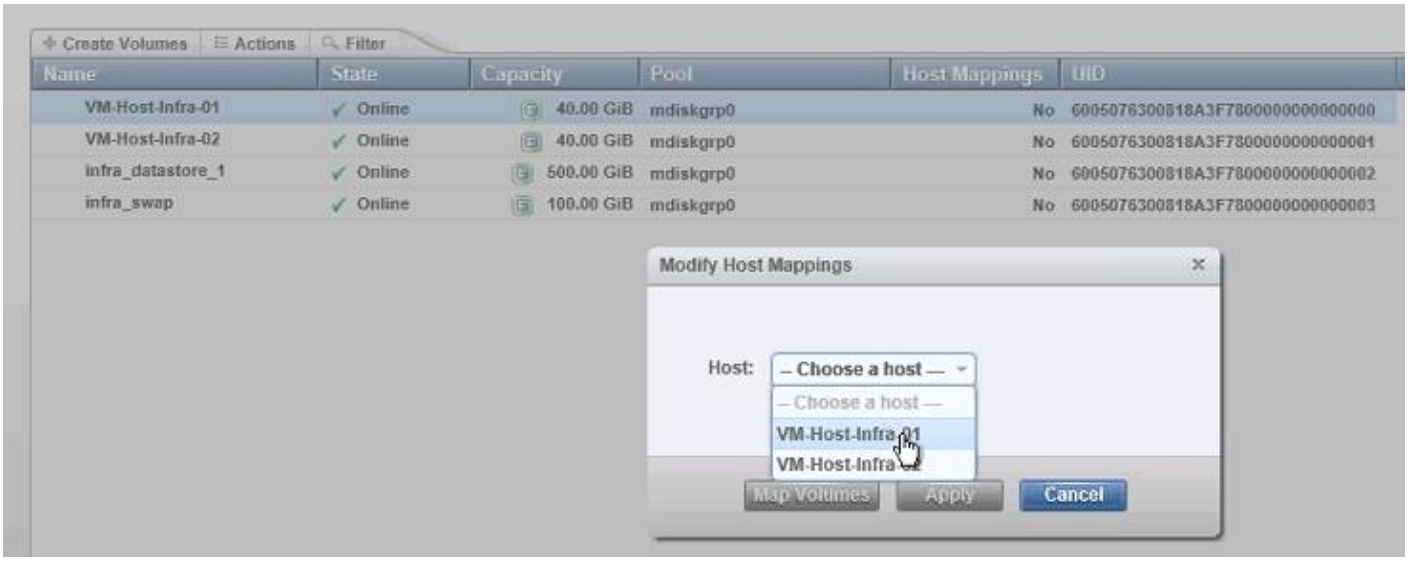


14. Click the Volumes icon in the left pane, then click the volumes menu item to display the created volumes.

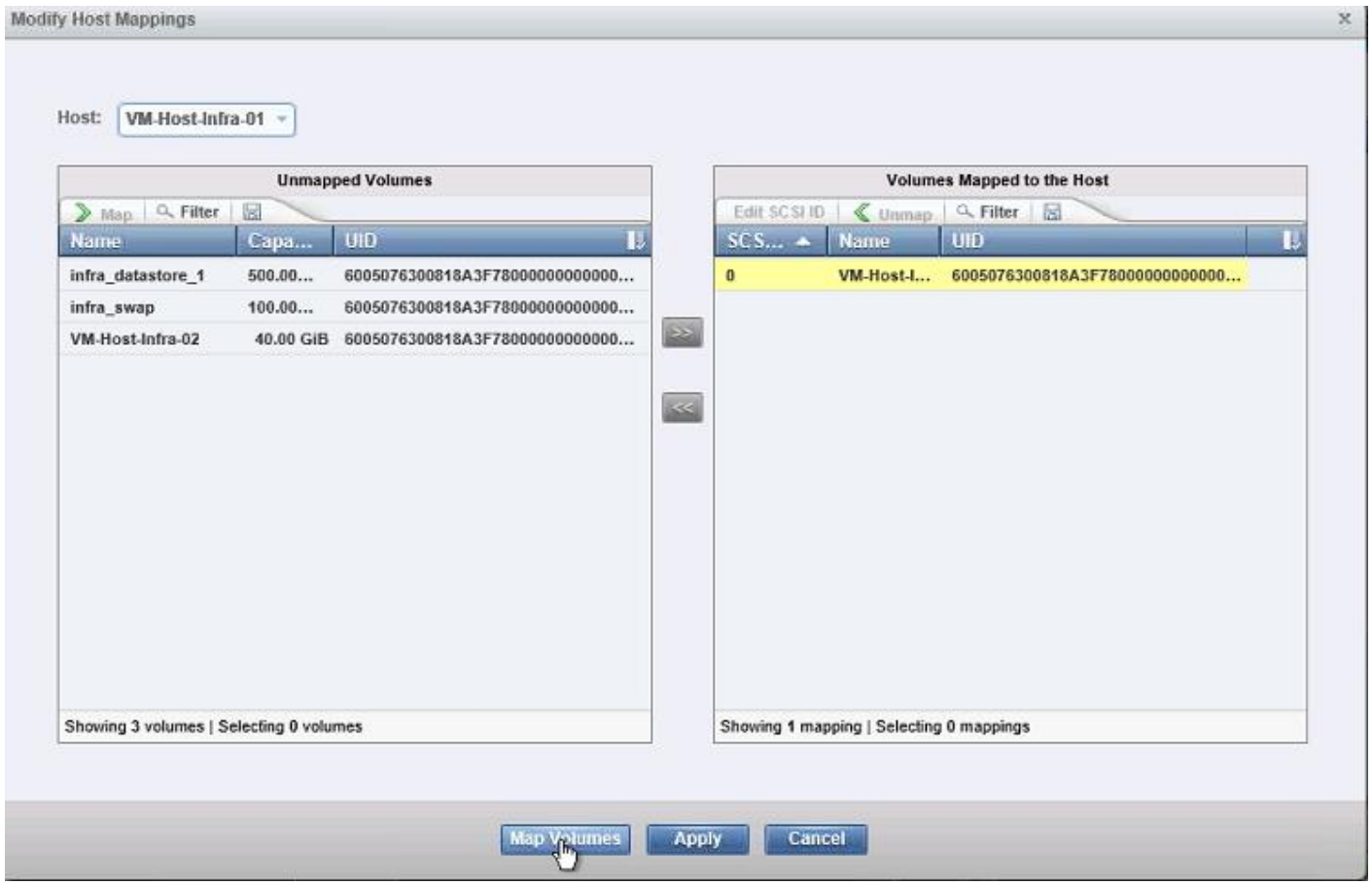
15. Right-click the volume `VM-Host-Infra-01` and select Map to Host.



16. In the drop-down, leave ALL I/O Groups enabled, and select `VM-Host-Infra-01`.

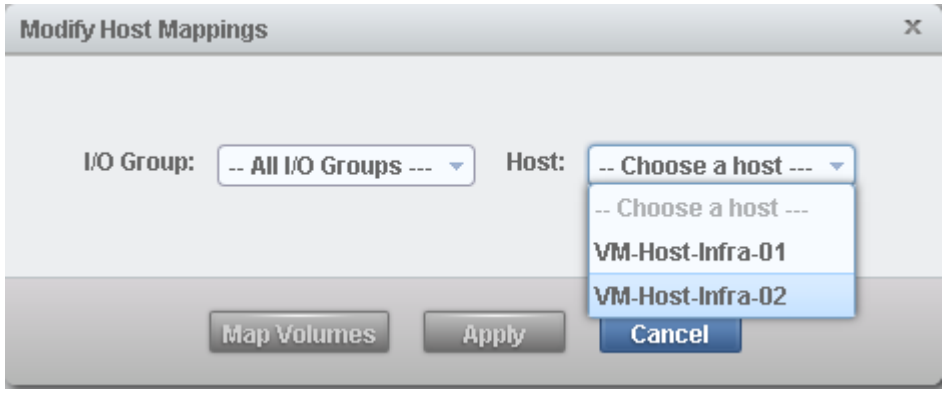


17. Select Map Volumes then click Close.

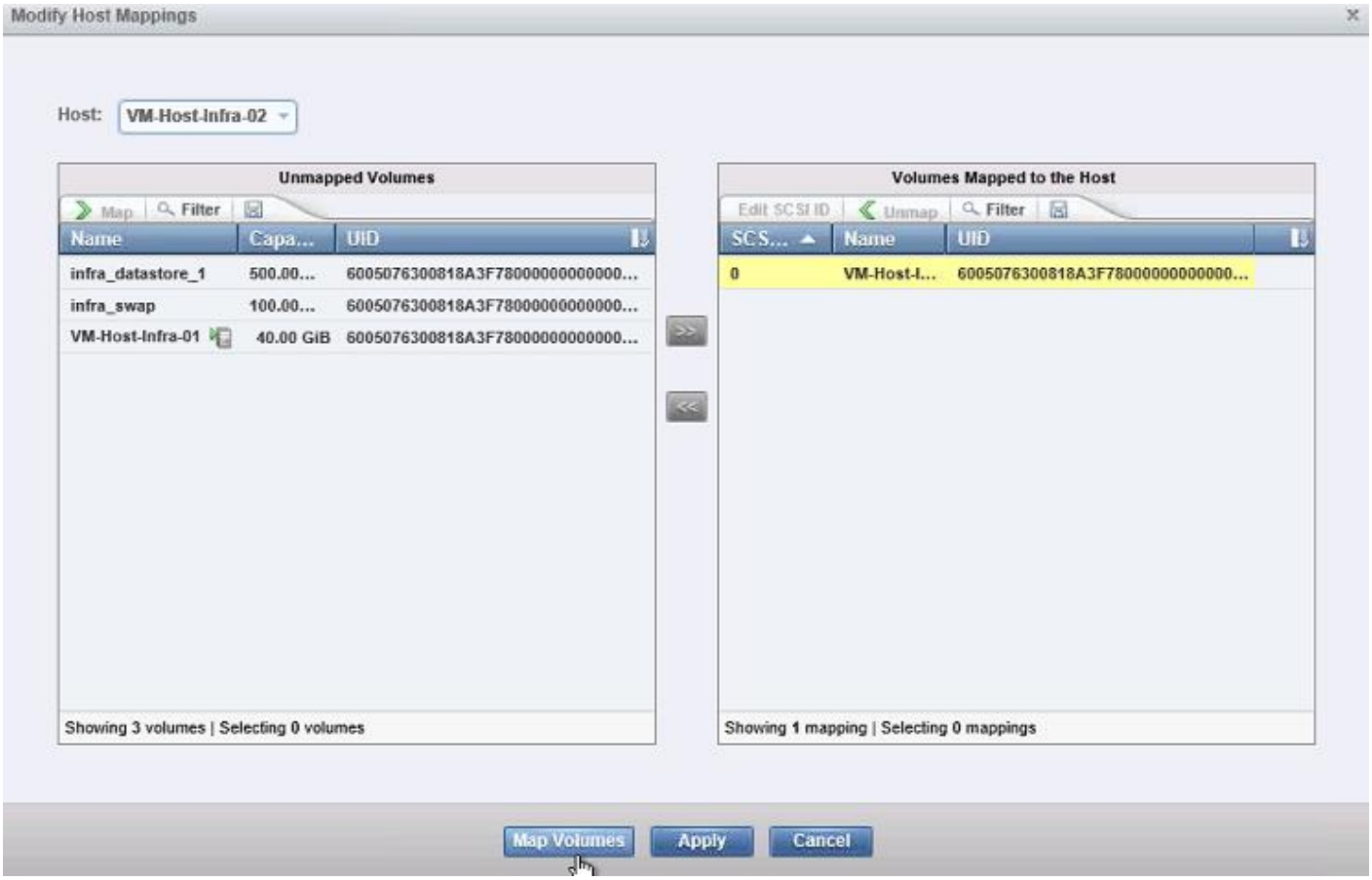


18. Right-click the volume `VM-Host-Infra-02` and click Map to host.

19. In the drop-down, leave ALL I/O Groups enabled, and select `VM-Host-Infra-02`.



20. Select Map Volumes, and then click Close.



ESX and vSphere Installation and Setup

VersaStack VMware ESXi 5.5 Update 2 SAN Boot Installation

This section provides detailed instructions for installing VMware ESXi 5.5 Update 2 in a VersaStack environment. After the procedures are completed, two San-booted ESXi hosts will be provisioned. These deployment procedures are customized to include the environment variables.

Several methods exist for installing ESXi in a VMware environment. These procedures focus on how to use the built-in Keyboard, Video, Mouse (KVM) console and virtual media features in Cisco UCS Manager to map remote installation media to individual servers and connect to their boot logical unit numbers (LUNs). In this Method, use the Cisco Custom ESXi 5.5 U2 GA ISO file which is downloaded from the URL below. This is required for this procedure as it contains custom Cisco drivers and thereby reduces installation steps.

To download the Custom ESX ISO:

1. Open a web browser and click on the custom image

https://my.vmware.com/web/vmware/details?downloadGroup=OEM-ESXI55U2-CISCO&productId=353

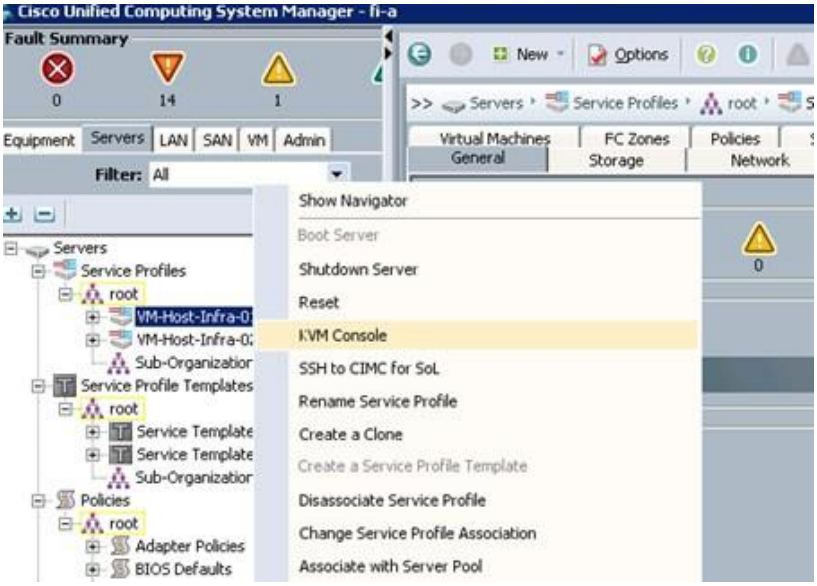
Log in to Cisco UCS 6200 Fabric Interconnect

Cisco UCS Manager

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

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

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



6. Select Servers > Service Profiles > root > VM-Host-Infra-02.
7. Right-click `VM-Host-Infra-02` and select KVM Console Actions > KVM Console.

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 Virtual Media.
2. Click Activate Virtual Devices, select Accept this Session, then Apply.

3. Select Virtual Media, Map CD/DVD, then browse to the ESXi installer ISO image file and click Open.
4. Select the Map Device to map the newly added image.

5. Select Reset, then Ok and allow a power cycle and click the KVM tab to monitor the server boot.
6. As an alternate method if the server is powered on, first shutdown the server, then 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 boot, the machine detects the presence of the ESXi installation media. Select the ESXi installer from the menu that is displayed.
2. After the installer is finished loading, press Enter to continue with the installation.
3. Read and accept the end-user license agreement (EULA). Press F11 to accept and continue.
4. Select the IBM LUN that was previously set up as the installation disk for ESXi and press Enter to continue with the installation.
5. Select the appropriate keyboard layout and press Enter.
6. Enter and confirm the root password and press Enter.
7. The installer issues a warning that existing partitions will be removed from the volume. Press F11 to continue with the installation.
8. After the installation is completes, hitting Enter will reboot the server. The ISO is automatically unmapped

Set Up Management Networking for ESXi Hosts

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

ESXi Host VM-Host-Infra-01

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

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

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

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

25. Press Esc to log out of the VMware console.

ESXi Host VM-Host-Infra-02

To configure the `VM-Host-Infra-02 ESXi` host with access to the management network, complete the following steps:

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

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

15. Enter the IP address of the primary DNS server.
16. Optional: Enter the IP address of the secondary DNS server.
17. Enter the FQDN for the second ESXi host.
18. Press Enter to accept the changes to the DNS configuration.
19. Press Esc to exit the Configure Management Network submenu.
20. Press Y to confirm the changes and restart the host.
21. The ESXi host reboots. After reboot, press F2 and log back in as root.

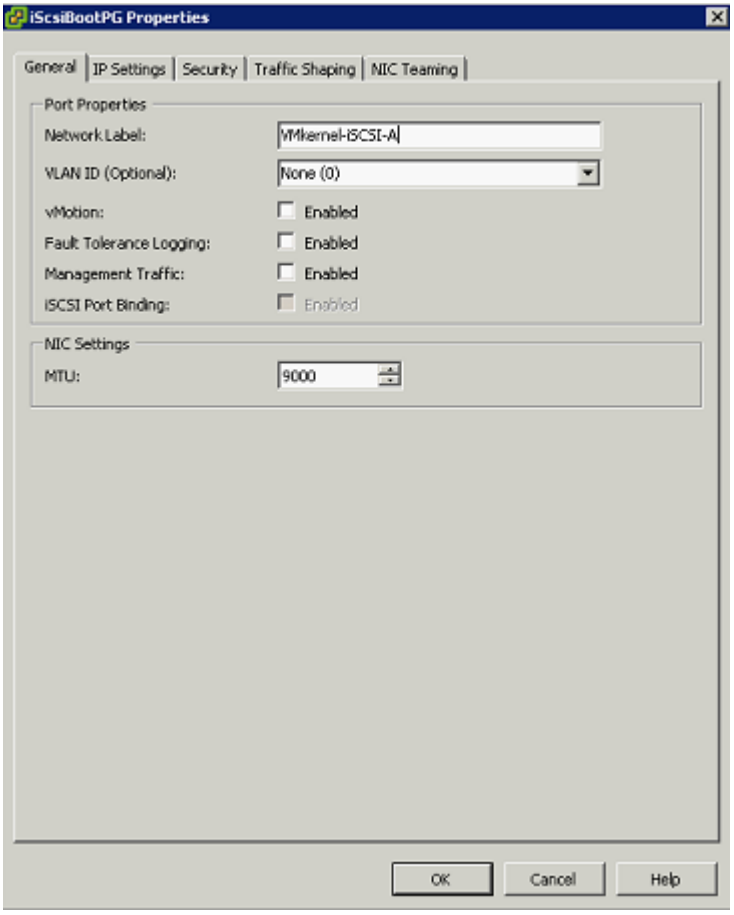
22. Select Test Management Network to verify that the management network is set up correctly and press Enter.
23. Press Enter to run the test.
24. Press Enter to exit the window.
25. Press Esc to log out of the VMware console.

Setup iSCSI Networking for iSCSI Booted Servers

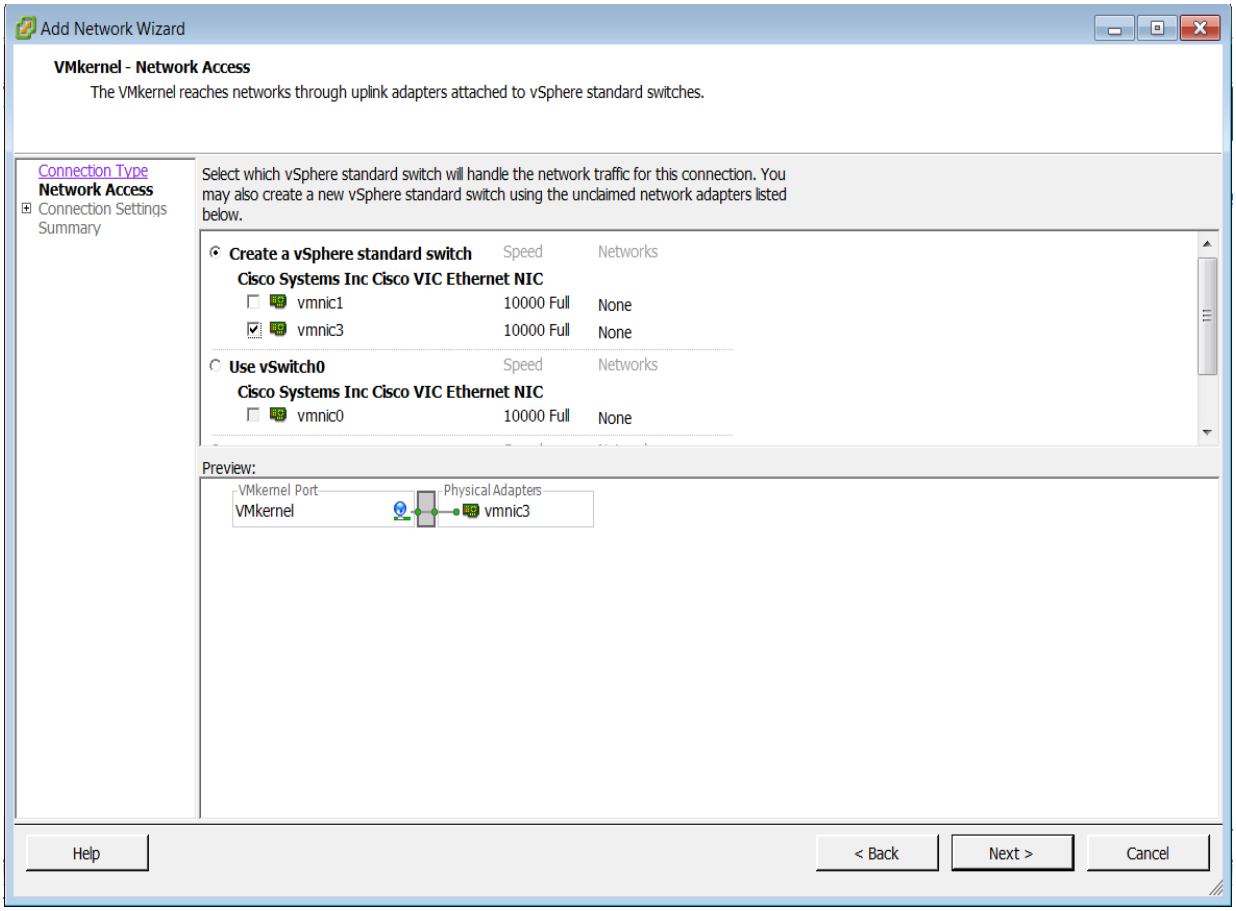
ESXi Host VM-Host-Infra-01

For hosts booting from Fabric A:

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. To the right of the iScsBootvSwitch, select Properties.
6. Select the vSwitch configuration and click Edit.
7. Change the MTU to 9000 and click OK.
8. Select the iScsBootPG configuration and click Edit.
9. Change the Network label to `VMKernel-iSCSI-A`.
10. Change the MTU to 9000.
11. Do not set a VLAN.

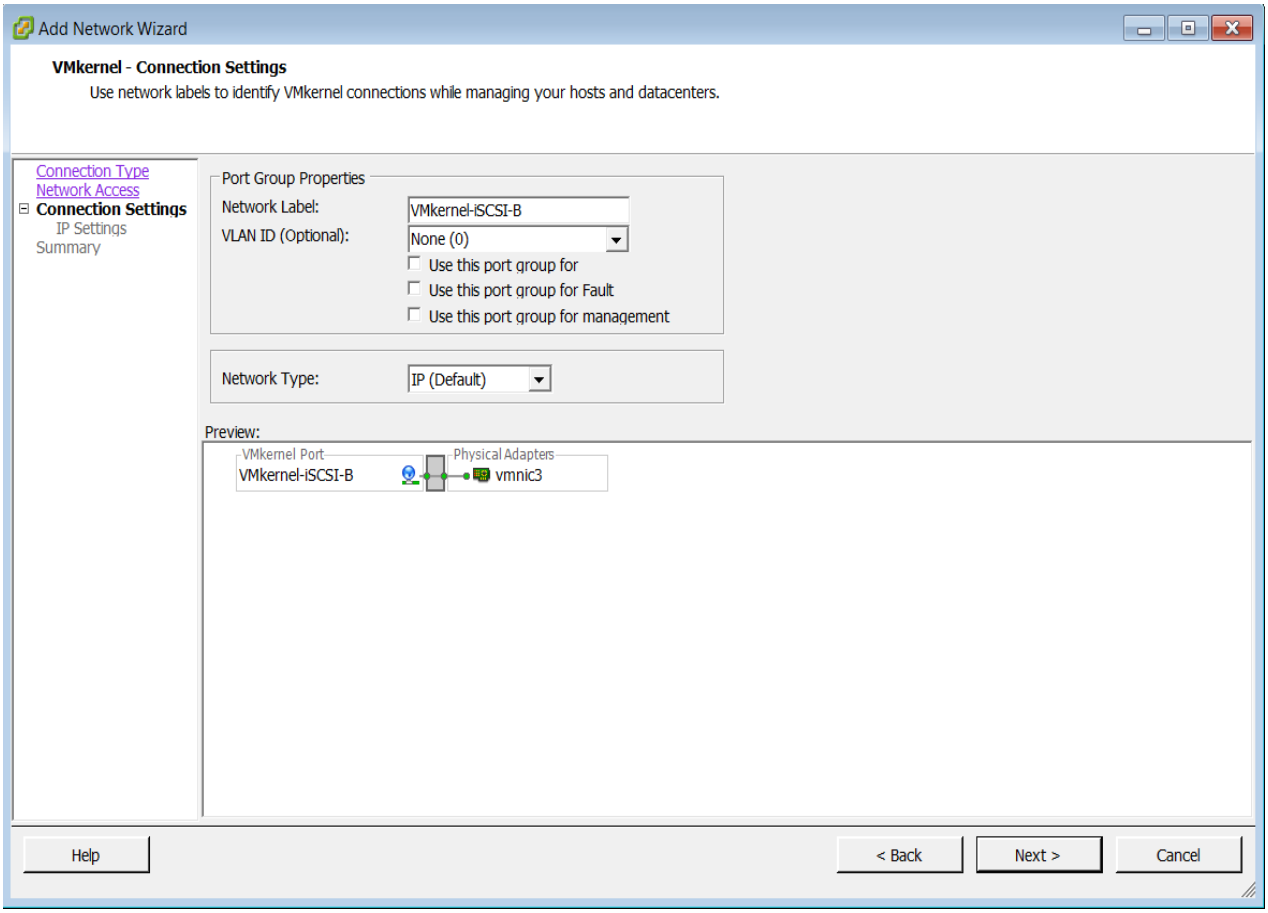


12. Click OK.
13. Click Close to close the iScsiBootvSwitch Properties window.
14. On the right, select Add Networking.
15. Select the VMkernel Connection Type and click Next.
16. Remove the selection from vmnic1 and select vmnic3.



17. Click Next.

18. Set the Network Label to `VMkernel-iSCSI-B`. Leave the VLAN ID set to None.

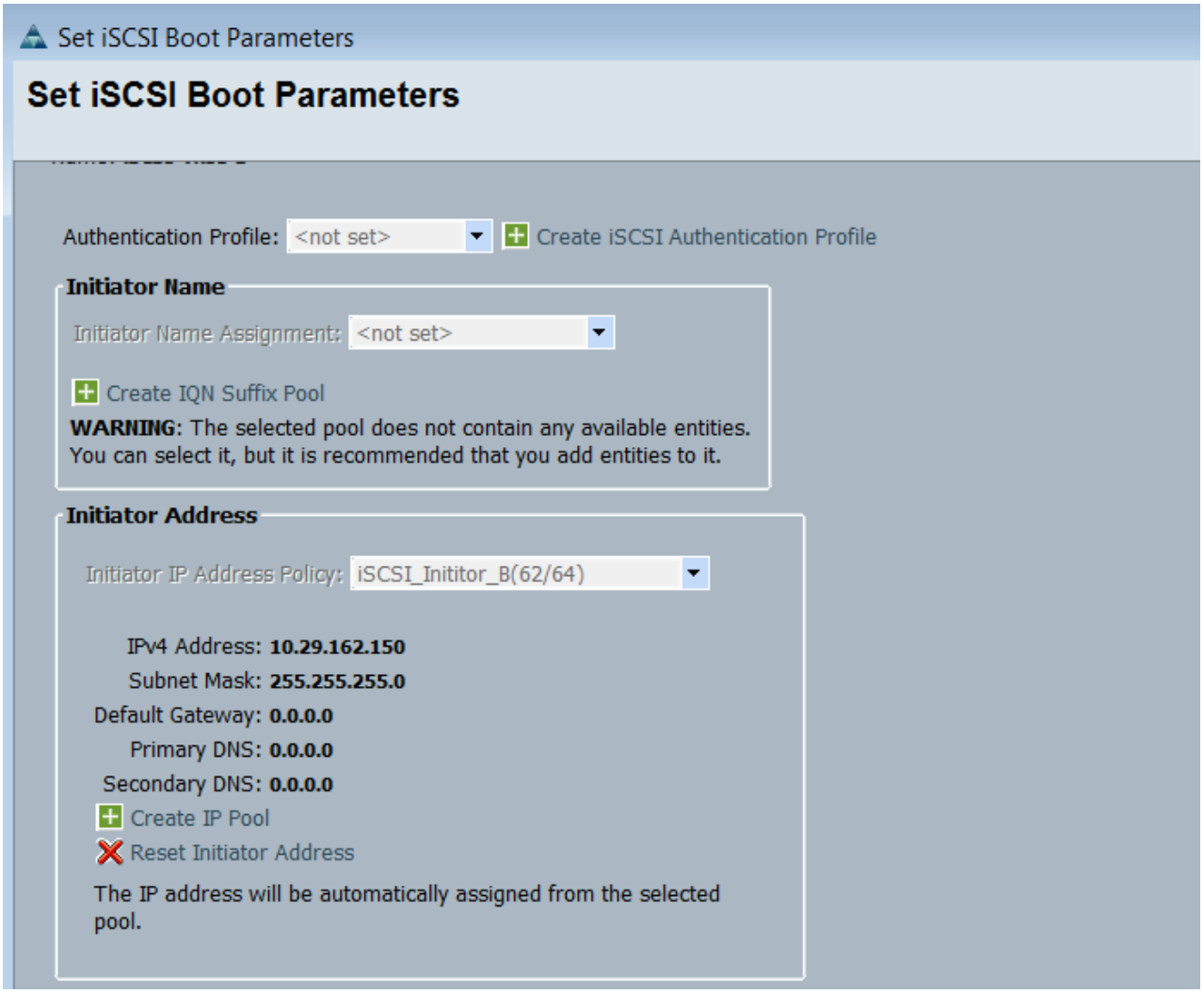


19. Click Next.

20. Retrieve the VMkernel IP address from Cisco UCS Manager.

21. In Cisco UCS Manager, select the Server's Service Profile and under the Boot Order tab expand iSCSI.

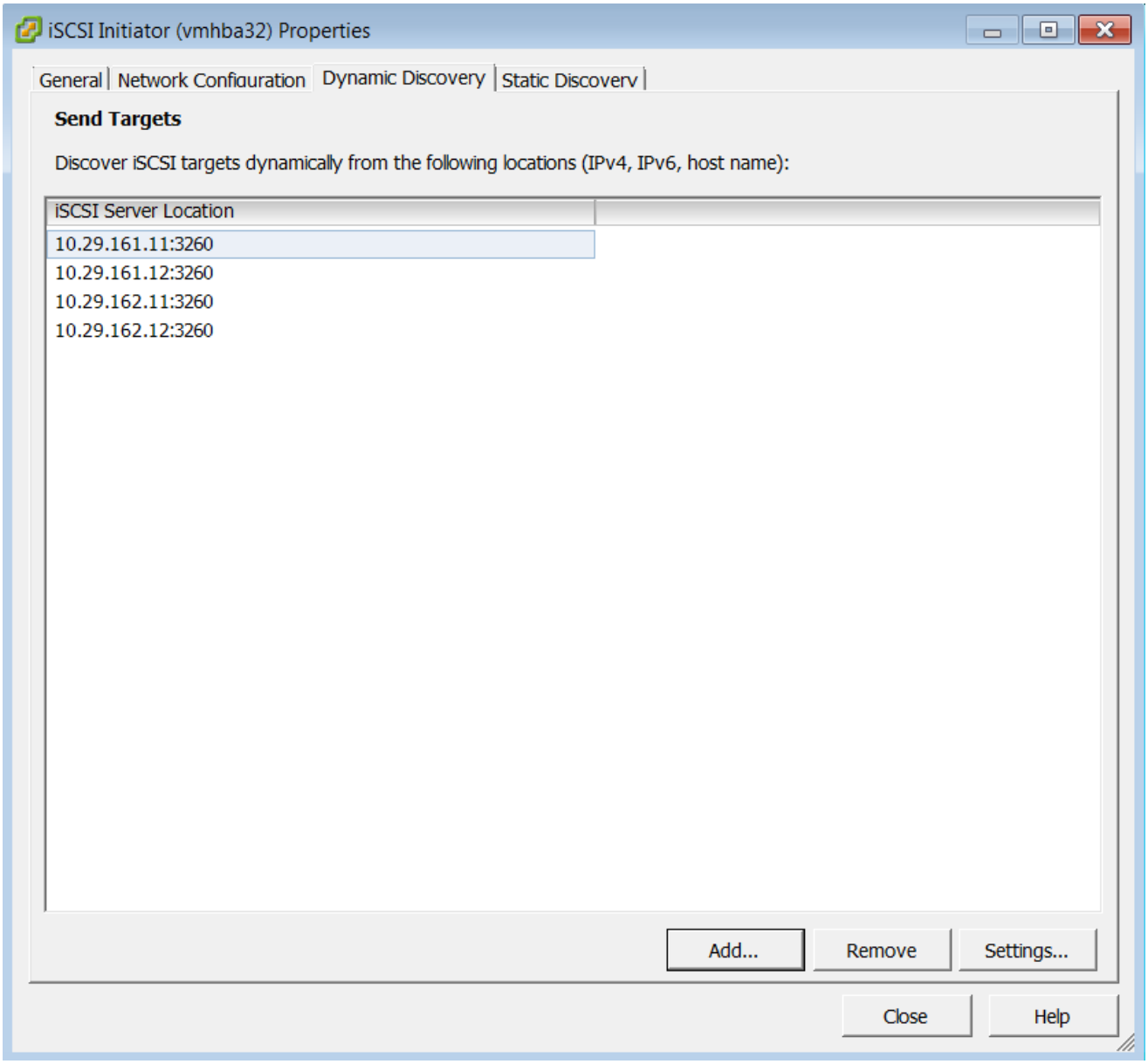
22. Select iSCSI-vNIC-B and click Set iSCSI Boot Parameters. The initiator IP Address appears.



23. In the vSphere client enter the IP Address and net mask you just retrieved from Cisco UCS Manager.
24. Click Next and Finish to create the vSwitch and VMkernel port.
25. Select Properties to the right of vSwitch1.
26. In the vSwitch1 Properties window, select the vSwitch configuration and click Edit.
27. Change the MTU to 9000 and click OK.
28. Select the VMkernel-iSCSI-B configuration and click Edit.
29. Change the MTU to 9000 and click OK.
30. Click Close to close the vSwitch1 Properties window.
31. Click Storage Adapters in the Hardware pane.
32. Select the iSCSI Software Adapter and click Properties.
33. Select the Dynamic Discovery tab and click Add.

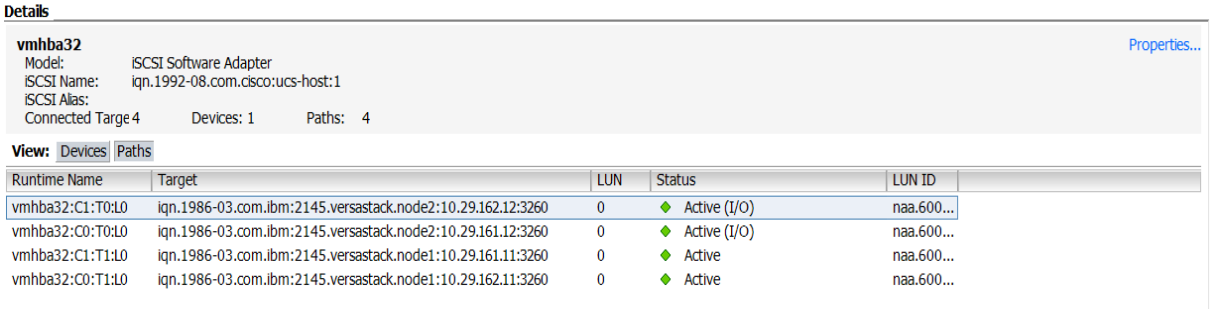
34. Enter the IP address of node1:Eth3.

35. Repeat putting in the IP addresses of node1:Eth4, node2:Eth3 and node2:Eth3.



36. Click Close and then click yes to rescan the host bus adapter.

37. You should now see 4 connected paths in the Details pane.



ESXi Host VM-Host-Infra-02

For hosts booting from Fabric B:

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. To the right of the iScsBootvSwitch, select Properties.
6. Select the vSwitch configuration and click Edit.
7. Change the MTU to 9000 and click OK.
8. Select the iScsBootPG configuration and click Edit.
9. Change the Network label to `VMKernel-iSCSI-B`.
10. Change the MTU to 9000.
11. Do not set a VLAN.
12. Click OK.
13. Click Close to close the iScsiBootvSwitch Properties window.
14. On the right, select Add Networking.
15. Select the VMkernel Connection Type and click Next.
16. Remove the selection from vmnic1 and select vmnic3.
17. Click Next.
18. Set the Network Label to `VMkernel-iSCSI-A`. Leave the VLAN ID set to None.
19. Click Next.
20. Retrieve the VMkernel IP address from Cisco UCS Manager.

21. In Cisco UCS Manager, select the Server's Service Profile and under the Boot Order tab expand iSCSI.
22. Select iSCSI-vNIC-A and click Set iSCSI Boot Parameters. The initiator IP Address appears.
23. In the vSphere client enter the IP Address and net mask you just retrieved from Cisco UCS Manager.
24. Click Next and Finish to create the vSwitch and VMkernel port.
25. Select Properties to the right of vSwitch1.
26. In the vSwitch1 Properties window, select the vSwitch configuration and click Edit.
27. Change the MTU to 9000 and click OK.
28. Select the VMkernel-iSCSI-A configuration and click Edit.
29. Change the MTU to 9000 and click OK.
30. Click Close to close the vSwitch1 Properties window.
31. Click Storage Adapters in the Hardware pane.
32. Select the iSCSI Software Adapter and click Properties.
33. Select the Dynamic Discovery tab and click Add.
34. Enter the IP address of node1:Eth3.
35. Repeat putting in the IP addresses of node1:Eth4, node2:Eth3 and node2:Eth3.
36. Click Close and then Click yes to rescan the host bus adapter.
37. You should now see 4 connected paths in the Details.

vSphere Setup and ESXi Configuration

In this section, you will set up the VSphere environment using Windows 2008 and SQL server. The Virtual machines used in this procedure are installed on a local Datastore on VersaStack for any Greenfield deployments, however these could be installed on a different ESXi clustered system or physical hardware if desired. This procedure will use the volumes previously created for VMFS Datastores.

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 the vSphere Client

3. Click the following link https://my.vmware.com/web/vmware/details?productId=396&downloadGroup=VCLI55U2
4. Select your OS and Click Download.
5. Save it to destination folder.
6. Run the VMware-vSphere-CLI-xxxx.exe.
7. Click Next.
8. Accept the terms for the license and click Next.
9. Click Next on the Destination Folder screen.
10. Click install and Finish.

ESXi Host VM-Host-Infra-01

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

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

ESXi Host VM-Host-Infra-02

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

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

Install VMware Drivers for the Cisco Virtual Interface Card (VIC)

Follow the below steps to install VMware VIC Drivers on the ESXi host VM-Host-Infra-01 and VM-Host-Infra-02

1. Download and extract the following VMware VIC Drivers to the Management workstation -

   fnic Driver version 1.6.0.16

   enic Driver version 2.2.2.69

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

1. From each vSphere Client, select the host in the inventory.
2. Click the Summary tab to view the environment summary.
3. From Resources > Storage, right-click datastore1 and select Browse Datastore.
4. Click the fourth button and select Upload File.
5. Navigate to the saved location for the downloaded VIC drivers and select fnic_driver_1.6.0.16-offline_bundle-2574267.zip.
6. Click Open and Yes to upload the file to datastore1.
7. Click the fourth button and select Upload File.
8. Navigate to the saved location for the downloaded VIC drivers and select enic-2.1.2.69-offline_bundle-2581703.zip.
9. Click Open and Yes to upload the file to datastore1.
10. Make sure the files have been uploaded to both ESXi hosts.
11. From the management workstation, open the VMware vSphere Remote CLI that was previously installed.
12. At the command prompt, run the following commands to account for each host:

```
esxcli –s <<var_vm_host_infra_01_ip>> -u root –p <<var_password>> software vib update --depot /vmfs/volumes/datastore1/fnic_driver_1.6.0.16-offline_bundle-2574267.zip

esxcli –s <<var_vm_host_infra_02_ip>> -u root –p <<var_password>> software vib update --depot /vmfs/volumes/datastore1/fnic_driver_1.6.0.16-offline_bundle-2574267.zip

esxcli –s <<var_vm_host_infra_01_ip>> -u root –p <<var_password>> software vib update --depot /vmfs/volumes/datastore1/enic-2.1.2.69-offline_bundle-2581703.zip

esxcli –s <<var_vm_host_infra_02_ip>> -u root –p <<var_password>> software vib update --depot /vmfs/volumes/datastore1/enic-2.1.2.69-offline_bundle-2581703.zip
```

13. Back in the vSphere Client for each host, right-click the host and select Reboot.
14. Click Yes and OK to reboot the host.
15. Log back into each host with vSphere Client.

Set Up VMkernel Ports and Virtual Switch

ESXi Host VM-Host-Infra-01

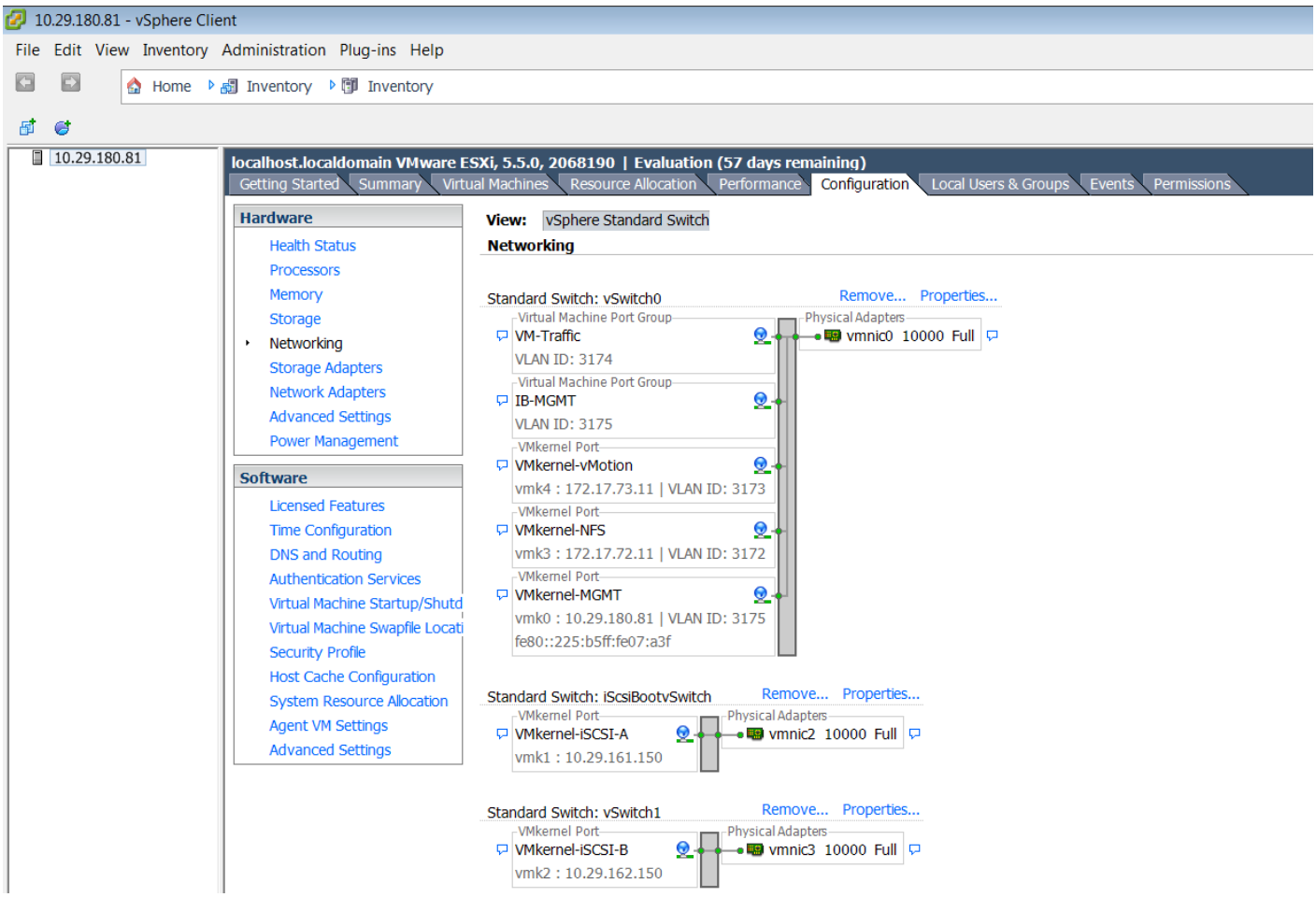
Repeat the steps in this section for all the ESXi Hosts

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

1. From each vSphere Client, select the host in the inventory.
2. Click the Configuration tab.
3. Click Networking in the Hardware pane.
4. Click Properties on the right side of vSwitch0.
5. Select the 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 Management Network.
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 VM Network.
14. Click Add to add a network element.
15. Select VMkernel and click Next.
16. Change the network label to VMkernel-NFS and enter `<<var_nfs_vlan_id>>` in the VLAN ID (Optional) field.
17. Click Next to continue with the NFS VMkernel creation.
18. Enter the IP address `<<var_nfs_vlan_id_ip_host-01>>` and the subnet mask `<<var_nfs_vlan_id_mask_host01>>` for the NFS VLAN interface for VM-Host-Infra-01.
19. Click Next to continue with the NFS VMkernel creation.
20. Click Finish to finalize the creation of the NFS VMkernel interface.

21. Select the VMkernel-NFS configuration and click Edit.
22. Change the MTU to 9000.
23. Click OK to finalize the edits for the VMkernel-NFS network.
24. Click Add to add a network element.
25. Select VMkernel and click Next.
26. Change the network label to VMkernel-vMotion and enter `<<var_vmotion_vlan_id>>` in the VLAN ID (Optional) field.
27. Select the Use This Port Group for vMotion checkbox.
28. Click Next to continue with the vMotion VMkernel creation.
29. Enter the IP address `<<var_vmotion_vlan_id_ip_host-01>>` and the subnet mask `<<var_vmotion_vlan_id_mask_host-01>>` for the vMotion VLAN interface for VM-Host-Infra-01.
30. Click Next to continue with the vMotion VMkernel creation.
31. Click Finish to finalize the creation of the vMotion VMkernel interface.
32. Select the VMkernel-vMotion configuration and click Edit.
33. Change the MTU to 9000.
34. Click OK to finalize the edits for the VMkernel-vMotion network.
35. Click add and select Virtual Machine Network, then click Next.
36. Change the network label to VM-Traffic and enter `<<var_vmtraffic_vlan_id>>` in the VLAN ID (Optional) field
37. Click next, click finish to complete the creation of the VM-traffic network.
38. Close the dialog box to finalize the ESXi host networking setup.

This procedure uses 1 physical adapter (vmnic0) assigned to the vSphere Standard Switch (vSwitch0). If you plan to implement the 1000V Distributed Switch later in this document, this is sufficient. If your environment will be using the vSphere Standard Switch, you must assign another physical adapter to the switch. Click the properties of Vswitch0 on the configuration networking tab, click the Network Adapters tab, Click Add, select vmnic1, click Next, click Next, click Finish, and then click Close.



Map Required VMFS Datastores

Map the VMFS Datastores to the First ESXi Host

The second Host will be mapped when the cluster is created.

1. Log in to the IBM Storwize V5000 management GUI.
2. Select the volumes icon on the left side screen and click the Volumes menu item.
3. Right-click the infra_datastore_1 volume and click map to host
4. Choose host VM-Host-Infra-1, leave All I/O Groups selected then click map volumes , then close
5. Right-click the infra_swap volume and click map to host
6. Choose host VM-Host-Infra-1, leave All I/O Groups selected then click map volumes, then close

ESXi Hosts VM-Host-Infra-01

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

1. From the vSphere Client, select the host VM-Host-Infra-01 in the inventory.
2. Click the Configuration tab to enable configurations.
3. Click Storage in the Hardware pane.
4. From the Datastore area, click Add Storage to open the Add Storage wizard.
5. Select Disk/Lun and click Next.
6. Select the 500GB Datastore lun and click Next.
7. Accept default VMFS setting and click Next.
8. Click next for the disk layout.
9. Enter infra_datastore_1 as the datastore name.
10. Click Next to retain maximum available space.
11. Click finish.
12. Click Add Storage to open the Add Storage wizard.
13. Select Disk/Lun and click Next.
14. Select the 100GB swap lun and click Next.
15. Accept default VMFS setting and click Next.
16. Click next for the disk layout.
17. Enter infra_swap as the datastore name.
18. Click Next to retain maximum available space.
19. Click Finish.

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

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

1. From each vSphere Client, select the host in the inventory.
2. Click the Configuration tab to enable configurations.
3. Click Time Configuration in the Software pane.
4. Click Properties at the upper right side of the window.
5. At the bottom of the Time Configuration dialog box, click Options.
6. In the NTP Daemon Options dialog box, complete the following steps:

a. Click General in the left pane, select Start, and stop with host.

b. Click NTP Settings in the left pane and click Add.

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

8. In the NTP Daemon Options dialog box, select the Restart NTP Service to Apply Changes checkbox and click OK.

9. In the Time Configuration dialog box, complete the following steps:

a. Select the NTP Client Enabled checkbox and click OK.

b. Verify that the clock is now set to approximately the correct time.

VersaStack VMware vCenter Server Appliance 5.5 Update 2

The procedures in the following subsections provide detailed instructions for installing VMware vCenter 5.5 Update 2 appliance in a VersaStack environment. These deployment procedures are customized to include the environment variables.

To install the VMware vCenter 5.5 Update 2 Appliance in the configuration outlined, an accessible Windows Active Directory® (AD) Domain is necessary. If an existing AD Domain is not available, an AD virtual machine, or AD pair, can be set up in this VersaStack environment. Please refer to the Appendix for more information about AD setup.

Build and Set Up VMware vCenter Virtual Machine

Build VMware vCenter VM

To build the VMware vCenter VM, complete the following steps:

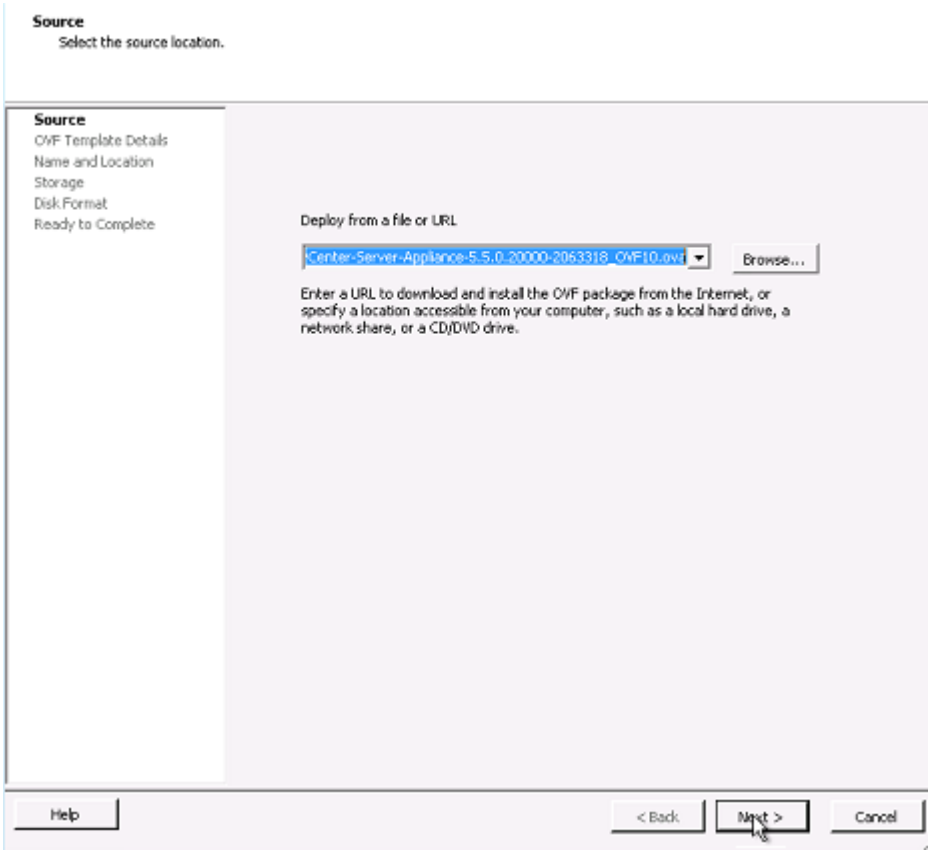
1. From the vSphere 5 download page on the VMware Web site, download the `.OVA` file for the vCenter Server appliance onto your system.

2. Open the vSphere client, and enter `<<var_vm_host_infra_01_ip>>` in the IP address/hostname field.

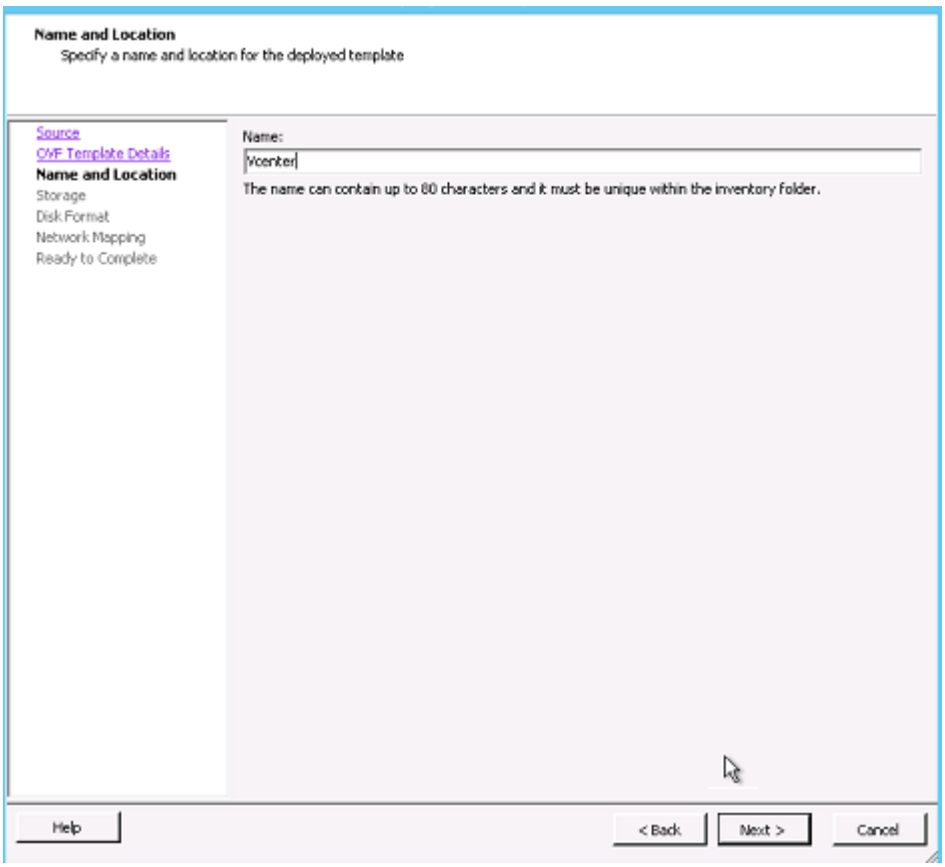
3. Enter root as the user name and the root password in the password field to Login

4. From the vSphere Client interface, click File > Deploy OVF Template

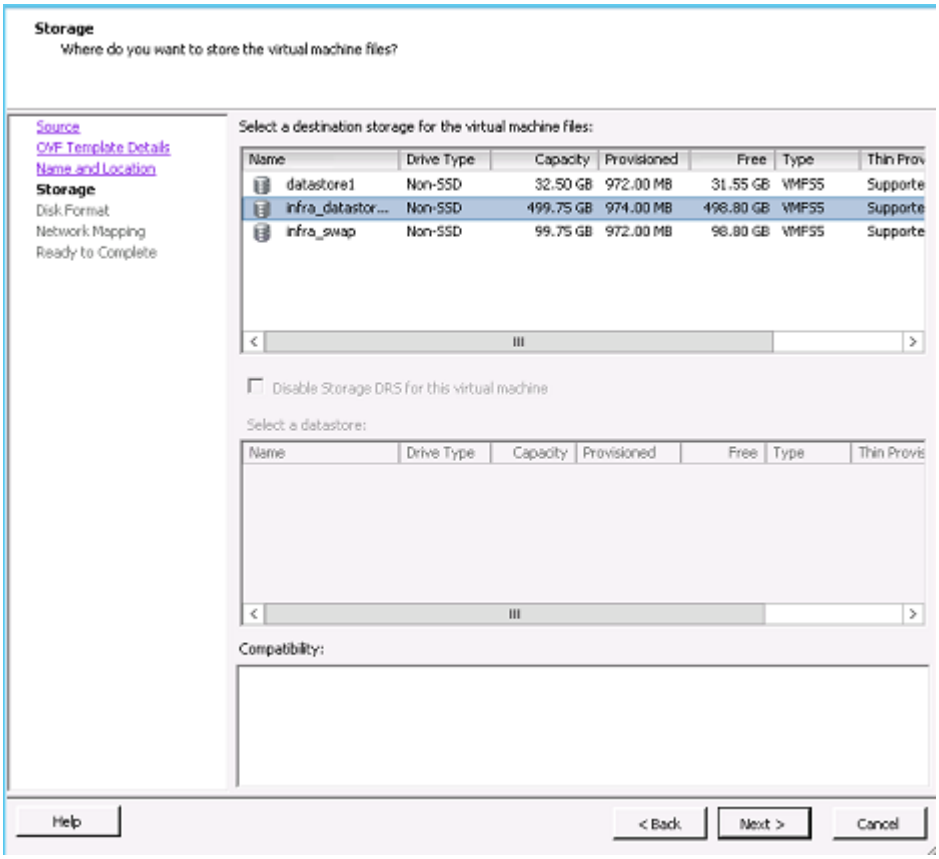
5. Browse to the OVA file.



6. Click Next to continue the installation.
7. Click Next on the details screen
8. Provide a name for the vCenter VM, then click Next to continue

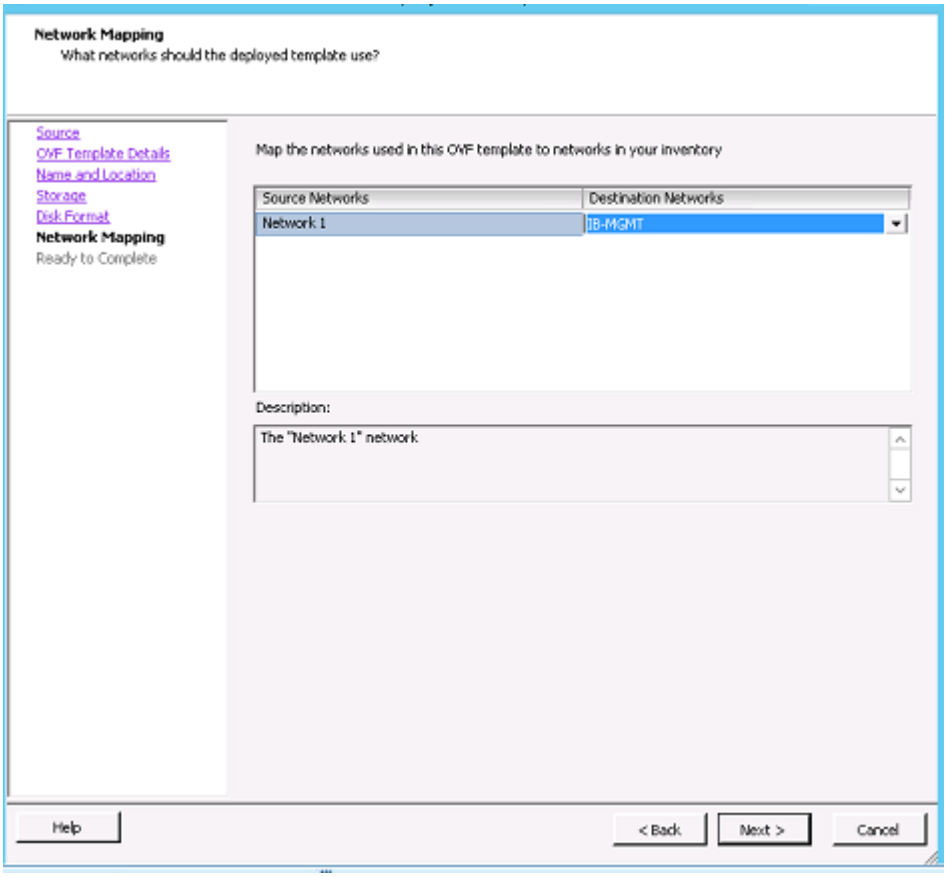


9. Select `infra_datastore_1` as the location for the vCenter VM virtual disks, then click Next to continue.

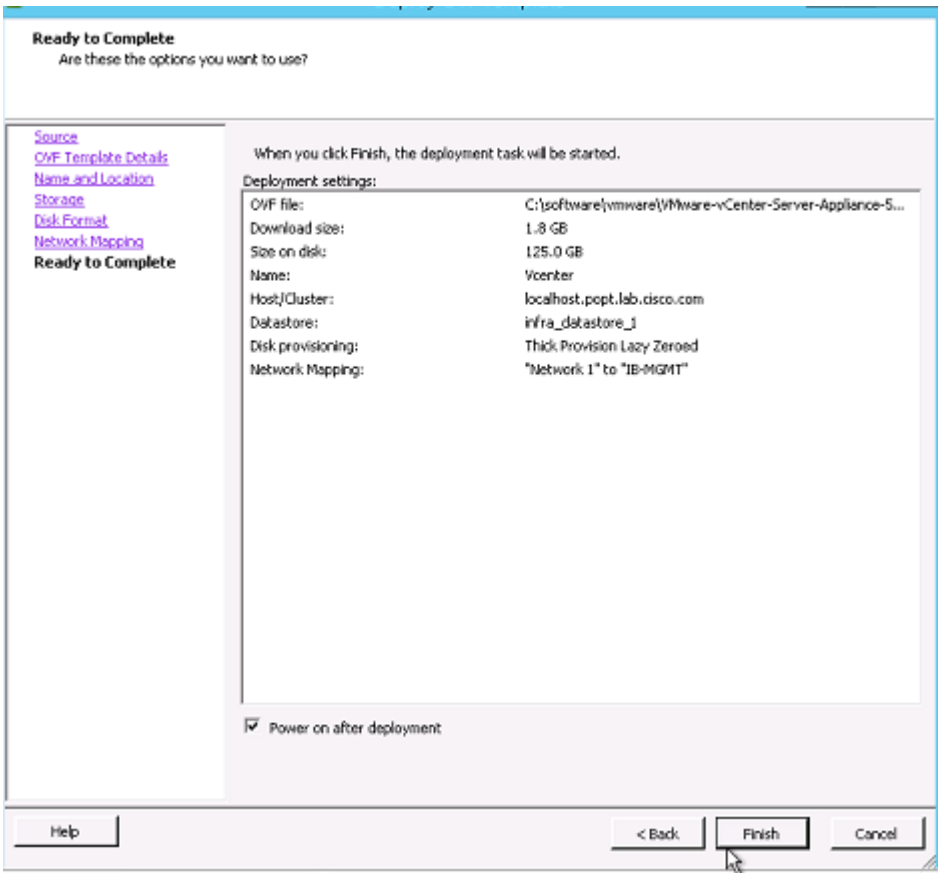


10. Review the disk format selection and click Next to continue.

11. For the network mapping screen make sure the `IB-MGMT` network is selected.



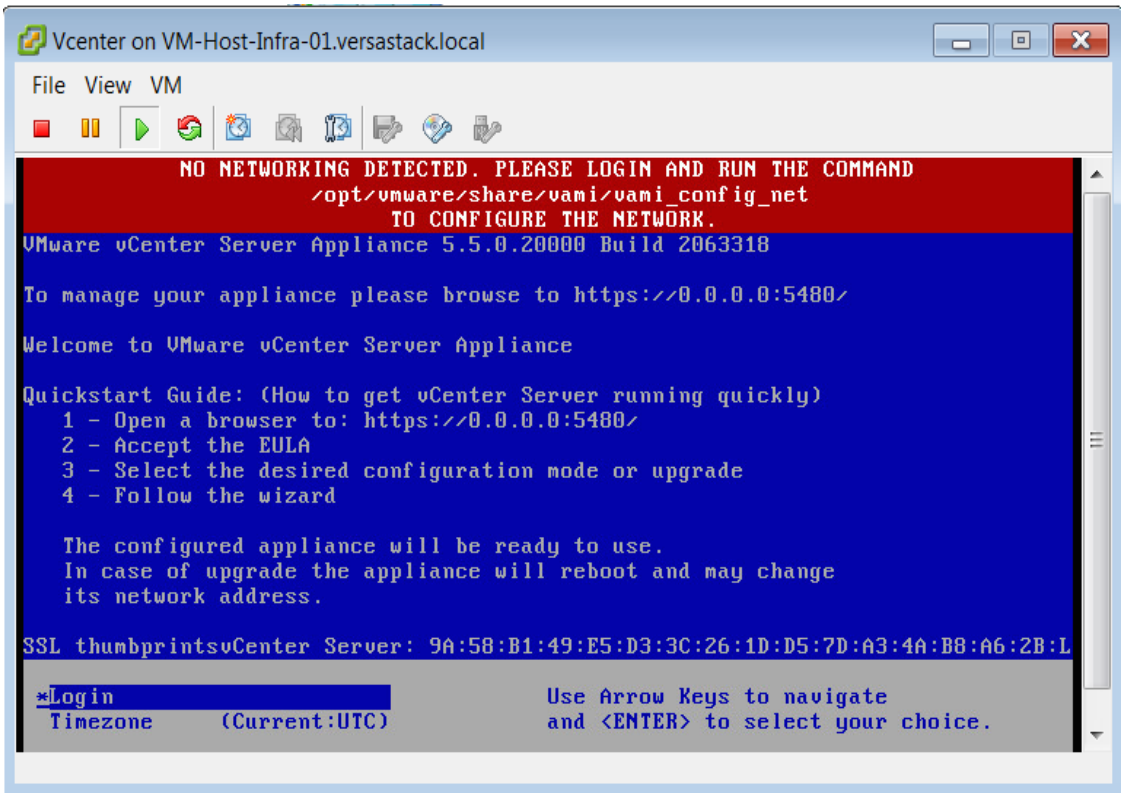
12. Select power on after deployment and click Finish.



13. After the installation has been completed, click the plus symbol to the left of the host IP address in the left pane of the vSphere Client window.

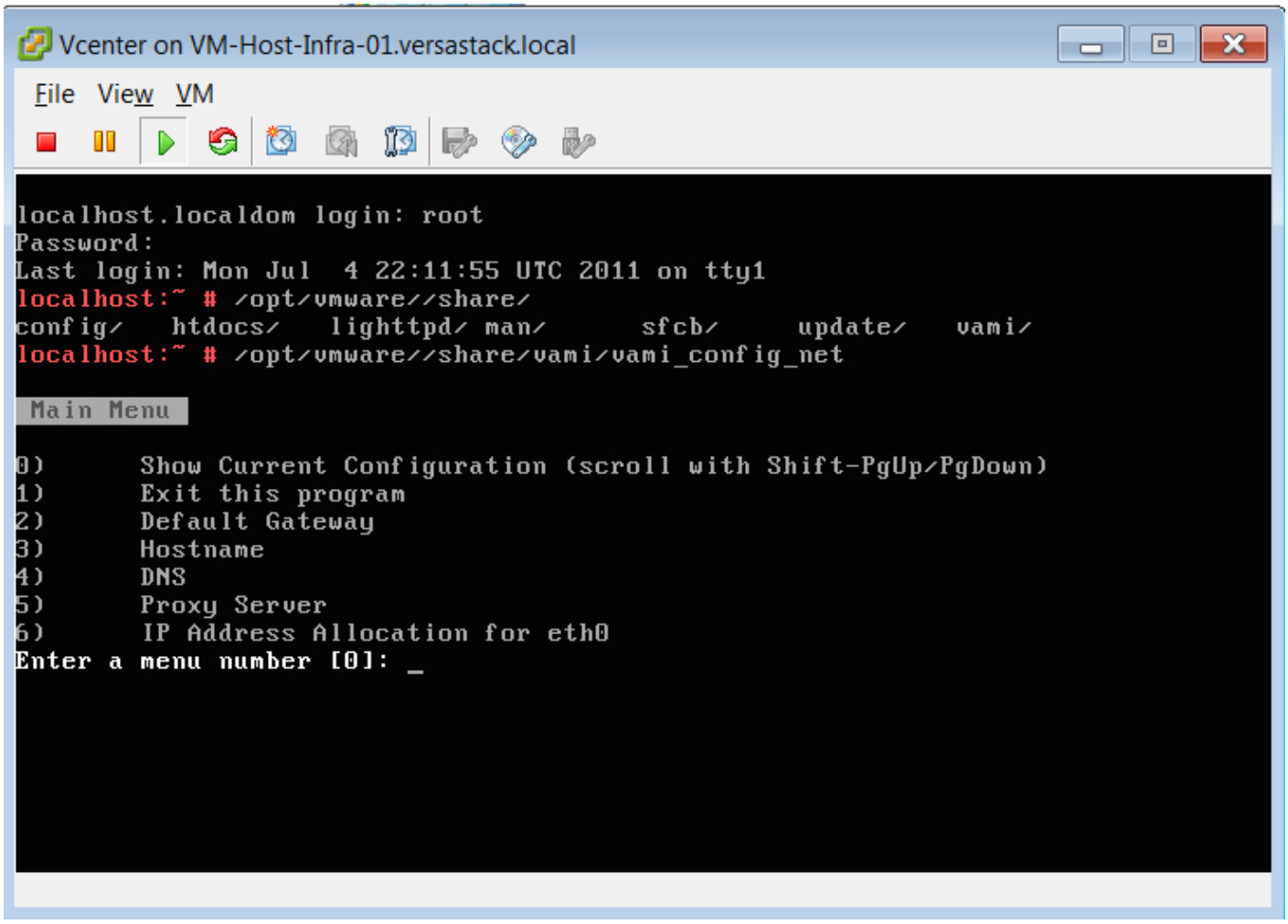
14. Right-click the vCenter VM and click Open Console to open a console view.

15. Once the machine has booted, it may have a DHCP address, but we will manually configure settings. Hit Enter to Login locally to set the proper configuration.

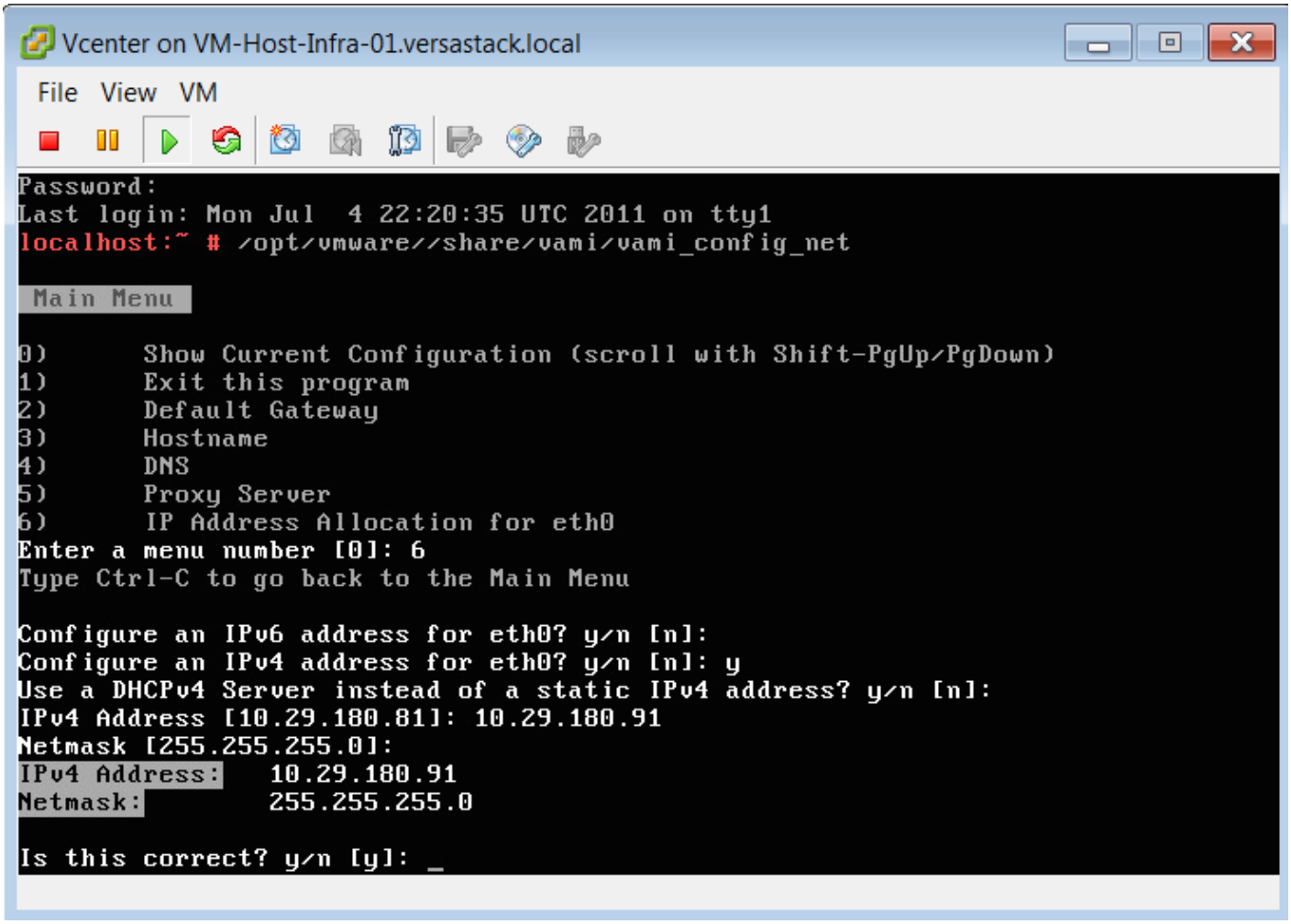


16. Login as root with `vmware` as the password and press Enter.

17. From the prompt, type `/opt/vmware/share/vami/vami_config_net` and press Enter.

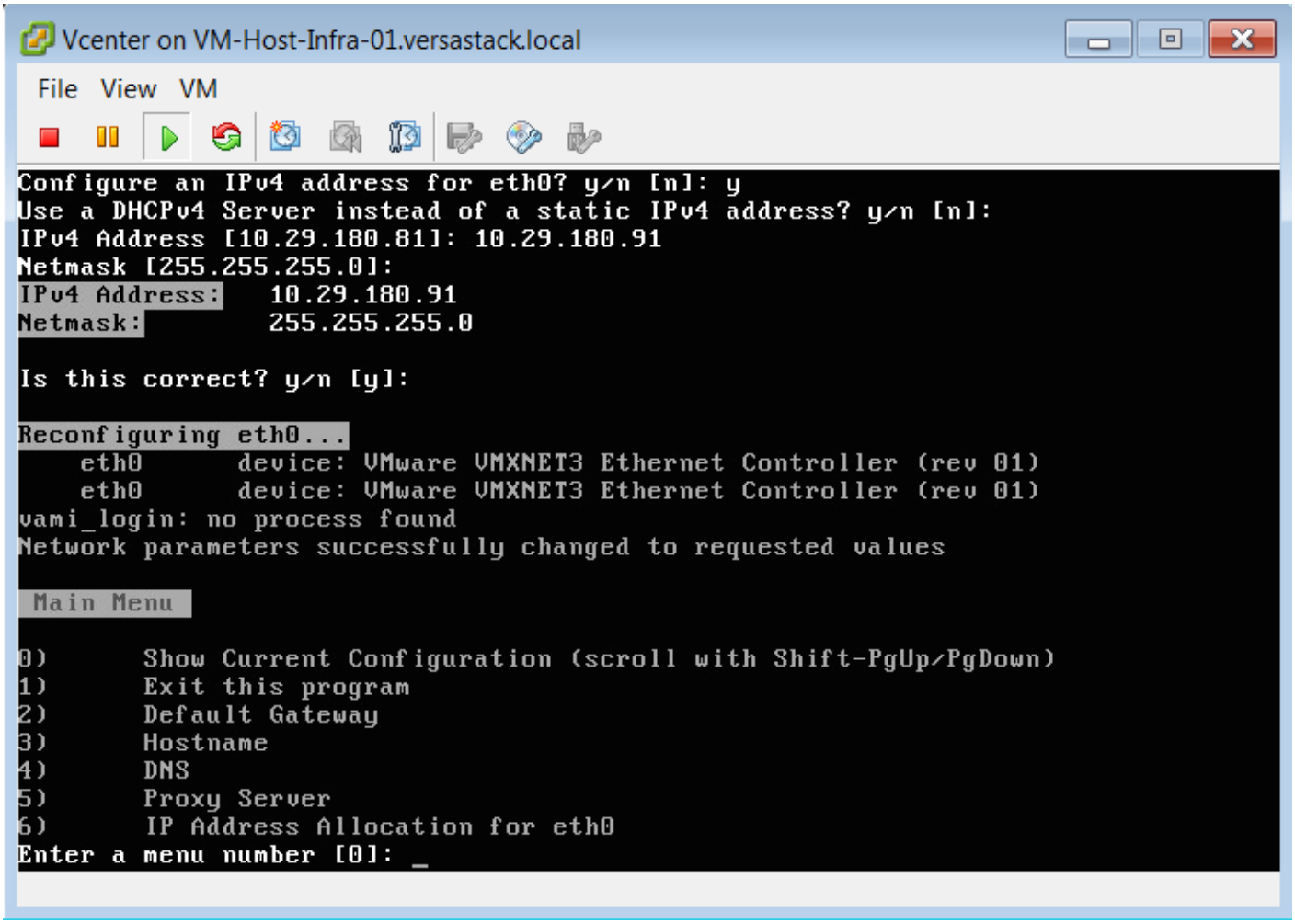


18. To configure the IP address for the vCenter server, type 6 and press Enter.
19. To disable IPv6, type n and press Enter.
20. To choose to configure an IPv4 address, type y and press Enter.
21. To use a static address instead of a DHCP address, type n and press Enter.
22. Type `<<var_vcenter_ip_address>>` and press Enter.
23. Type `<<var_vcenter_netmask>>` and press Enter.

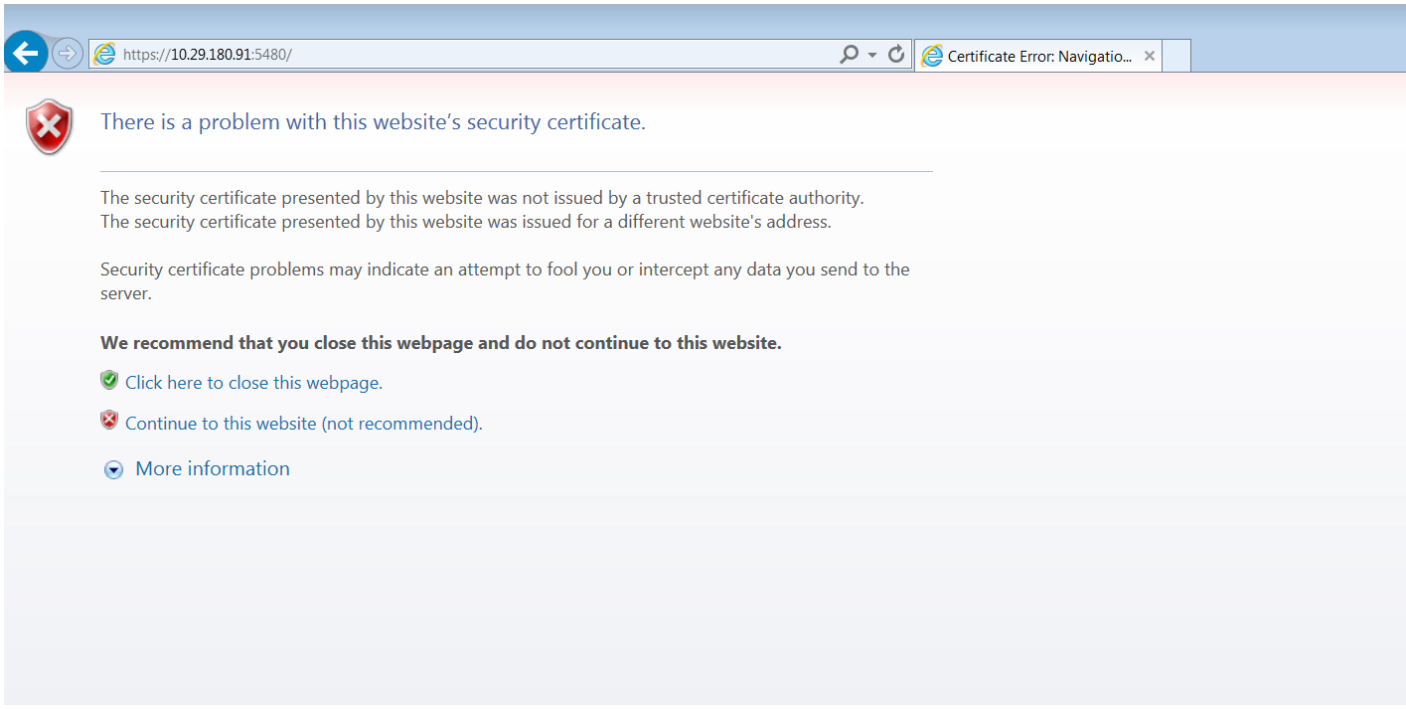


24. Review the IP address and subnet mask. Type y and press Enter to complete the configuration

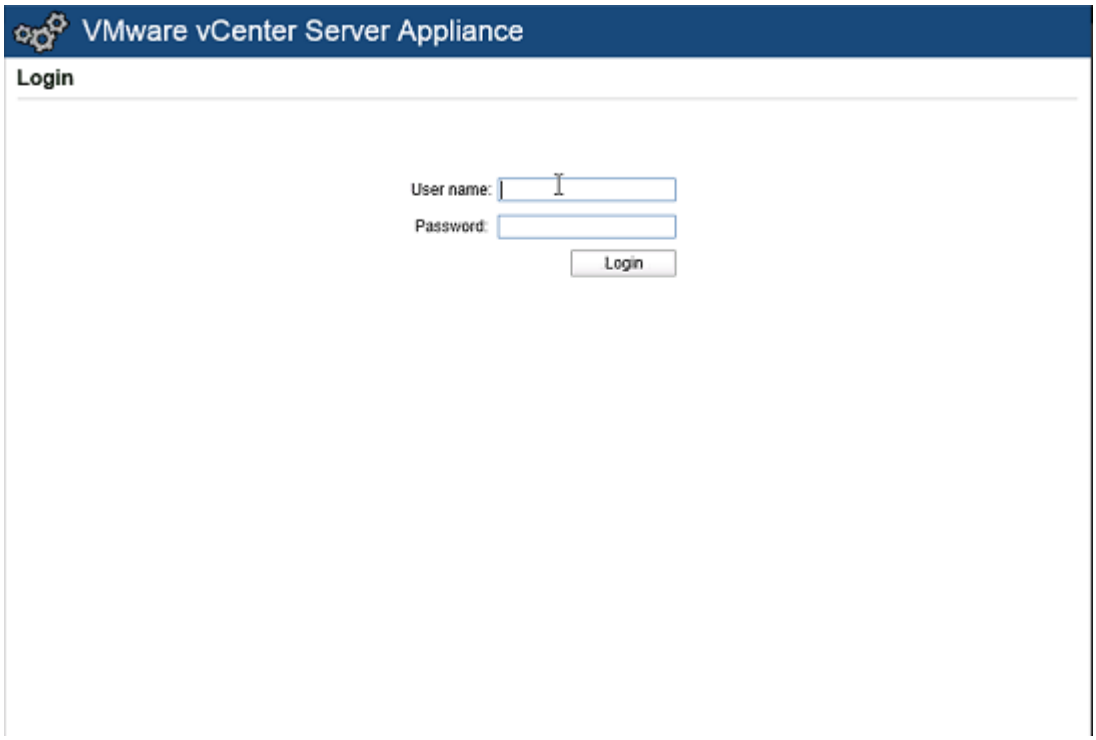
25. Type 3 and press Enter to enter the Hostname of the vCenter Server. It is important to enter the FQDN for the hostname in order for active directory setup to succeed.



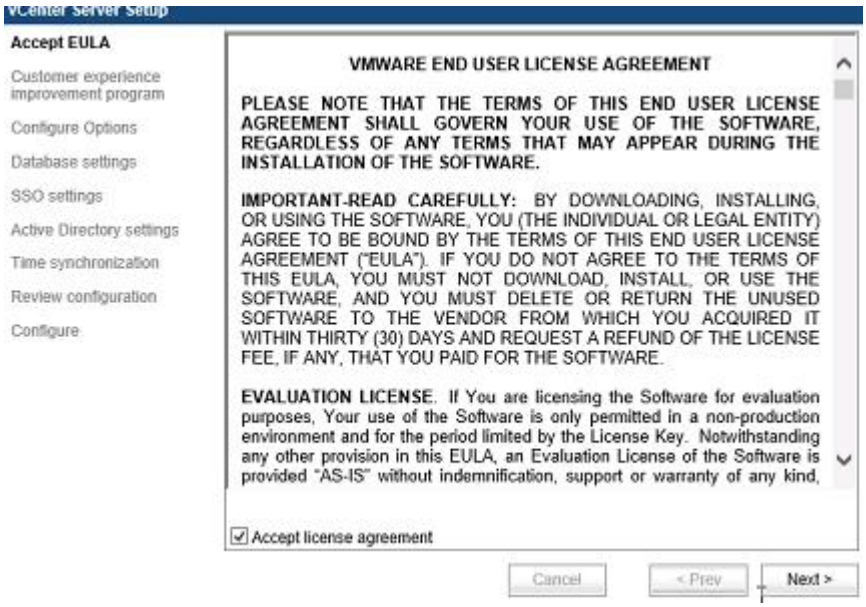
26. Type `2` and press Enter to configure the default gateway IP address.
27. Type `4` and press Enter to configure the DNS information for the vCenter server.
28. Type `<<var_DNS_1_IP>>` and press Enter.
29. Type `<<var_DNS_2_IP>>` and press Enter to accept the configuration changes.
30. Type `1` and press Enter to exit the configuration dialogue.
31. Type `exit` and press Enter to log out of the prompt.
32. Follow the instructions on the welcome screen to open a browser window to the URL shown and click continue to web site. You may need to bypass the security warning.



33. Enter the User name root and vmware for the password. Click Login.

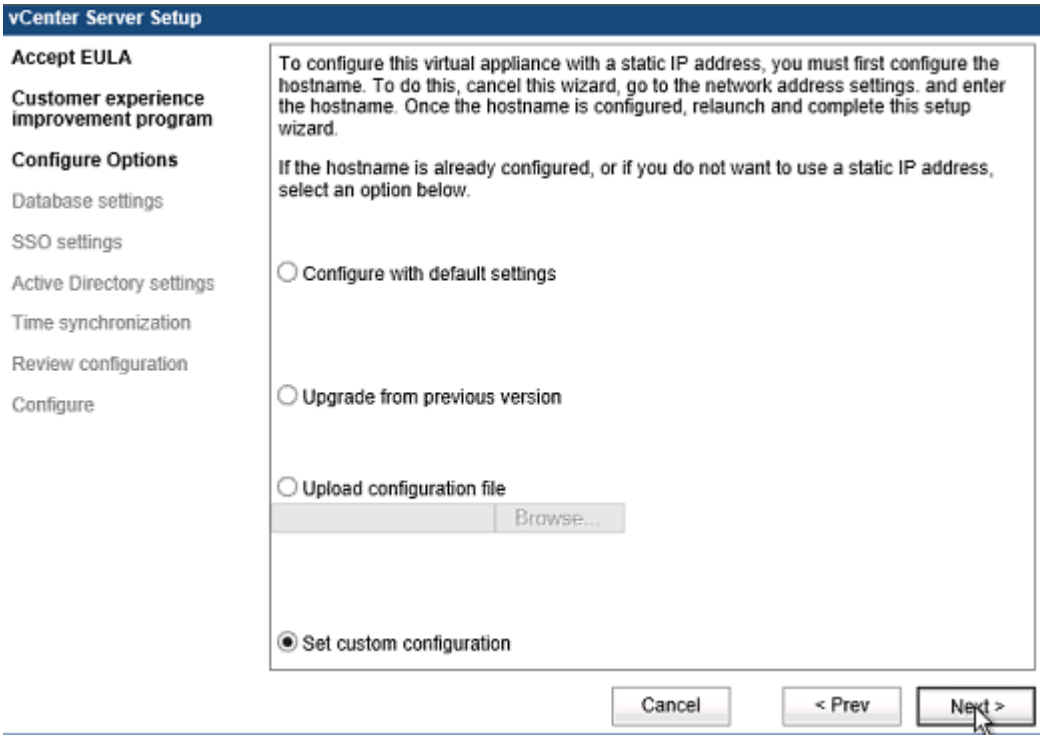


34. Select the Accept license agreement checkbox, click Next to continue.

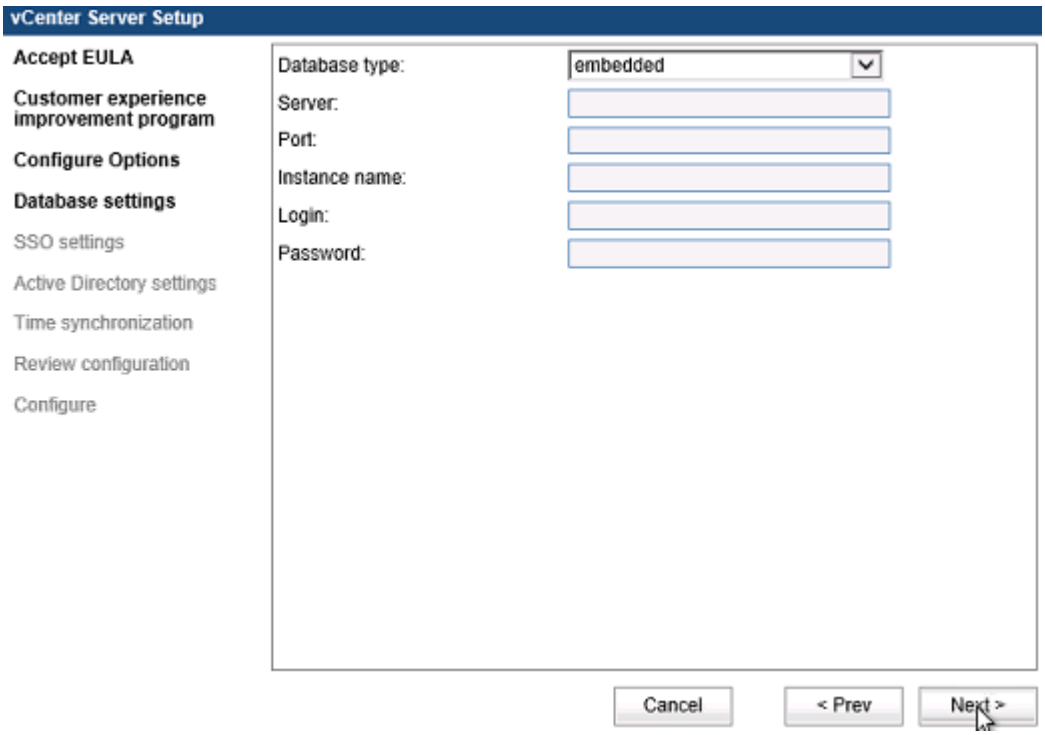


35. Click Next on the Customer Experience Improvement Program screen.

36. Select the Set custom configuration option then click Next to continue.

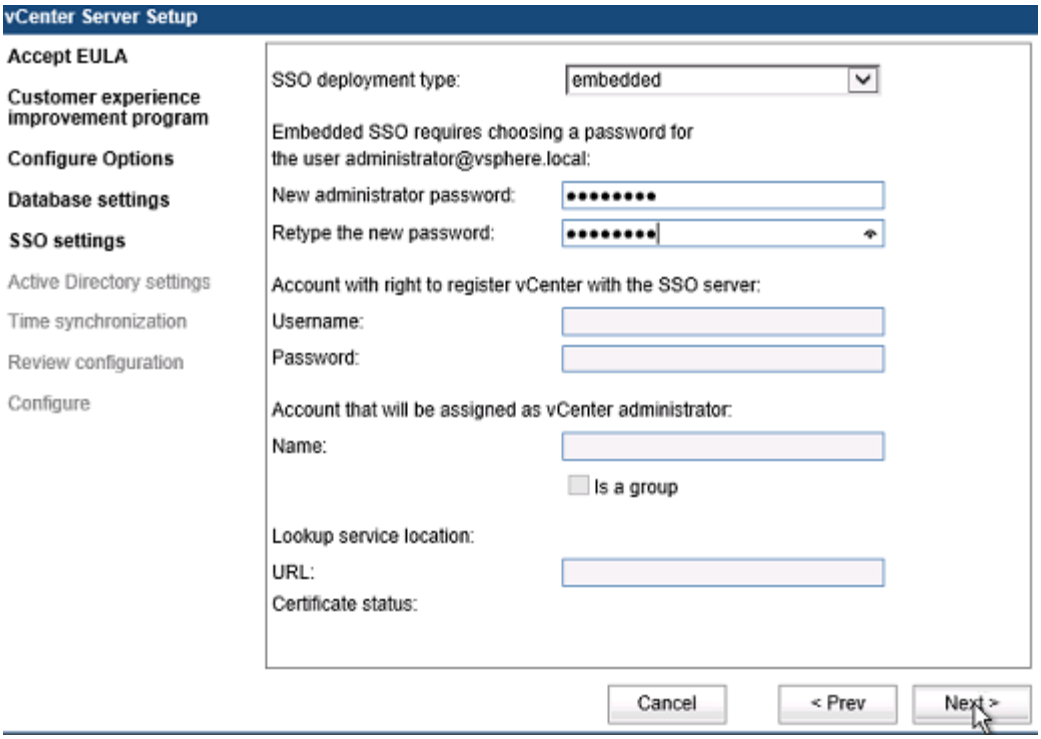


37. Click Next to accept an embedded database.



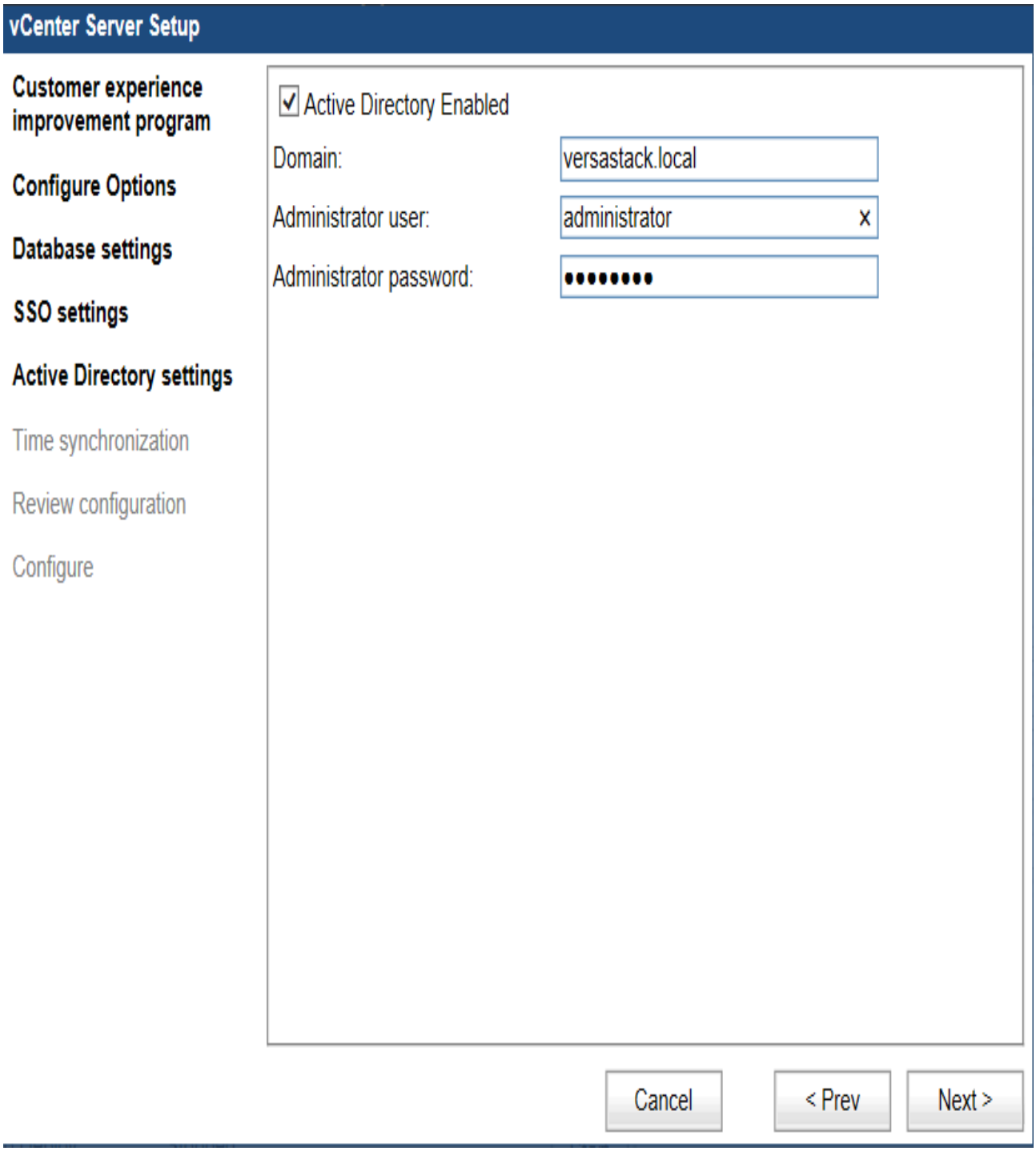
An Oracle database can alternatively be used and is recommended for vCenter installations supporting 1000 or more hosts

38. Enter the password in the password field; click Next to accept an embedded SSO deployment.

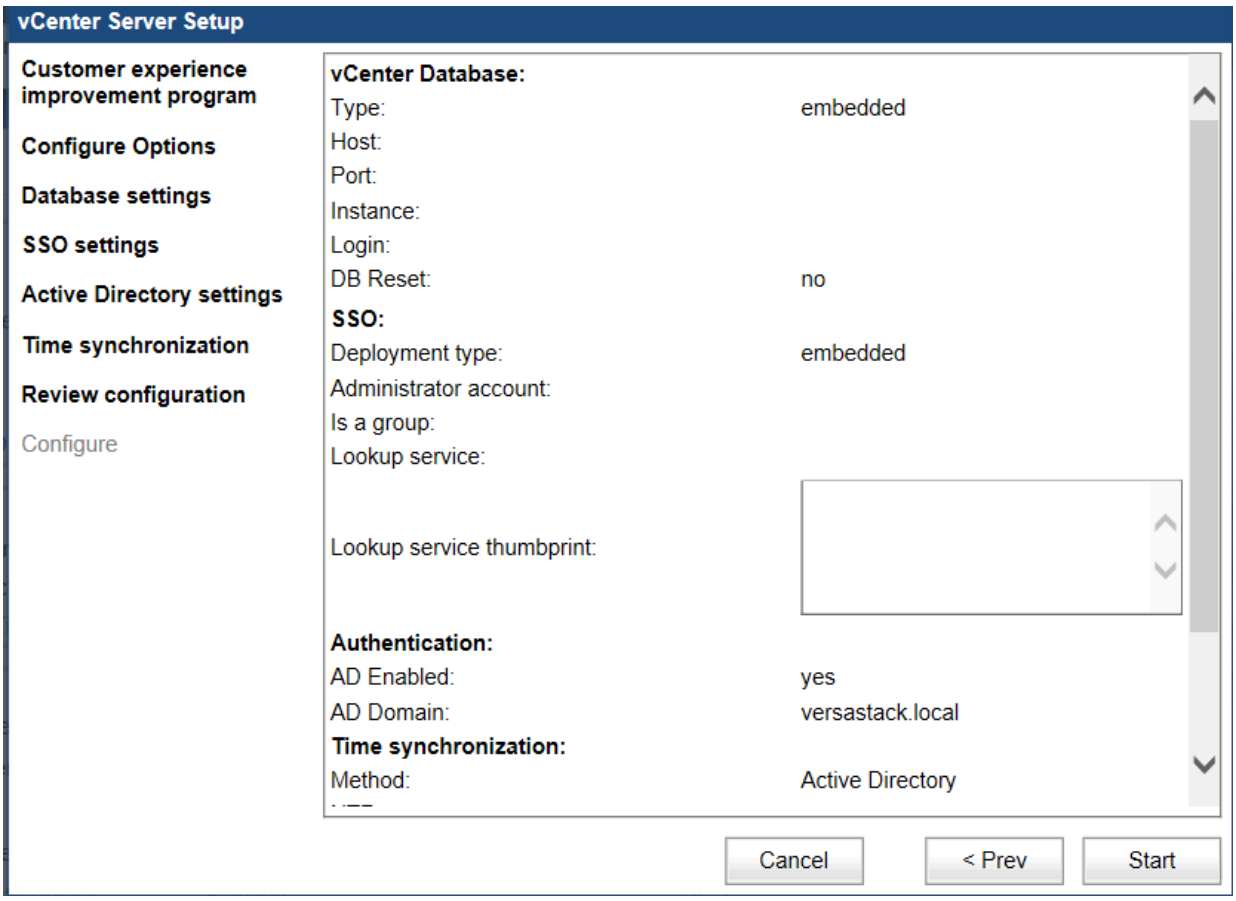


39. Select the Active Directory Enabled checkbox to configure Active Directory based user permissions.

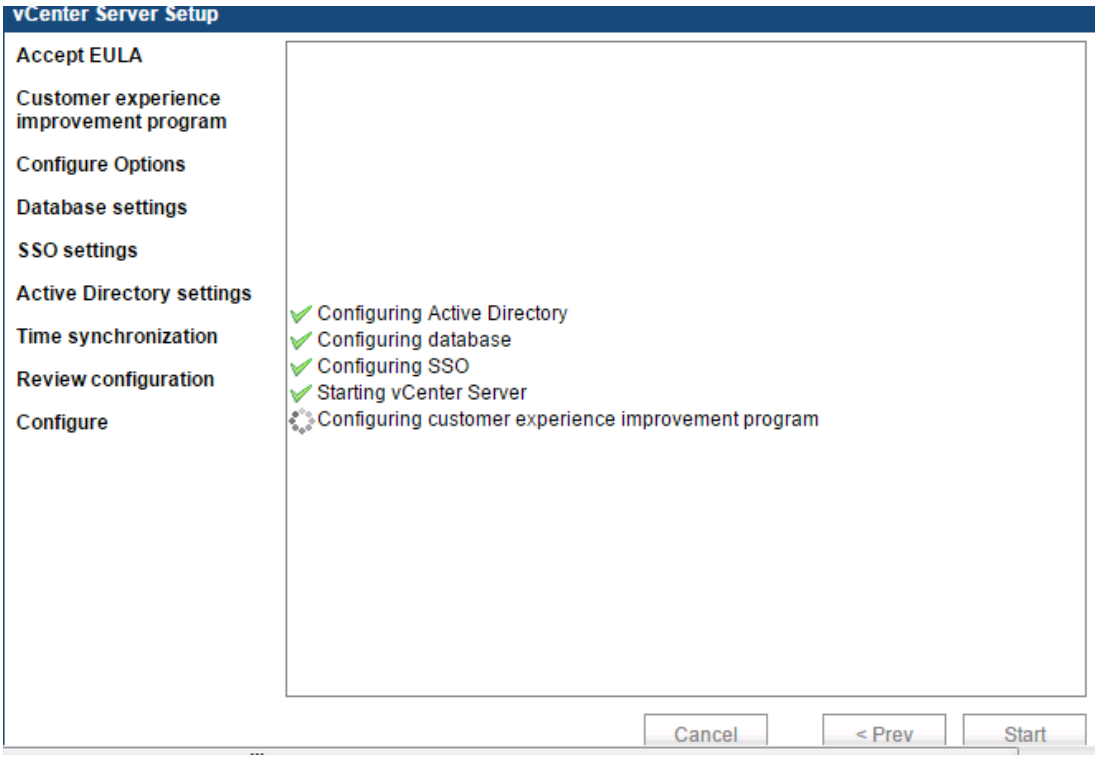
40. Enter the FQDN for the Active directory domain such as popt.lab.cisco.com, administrator user name, and administrator password in the fields then click Next to continue.



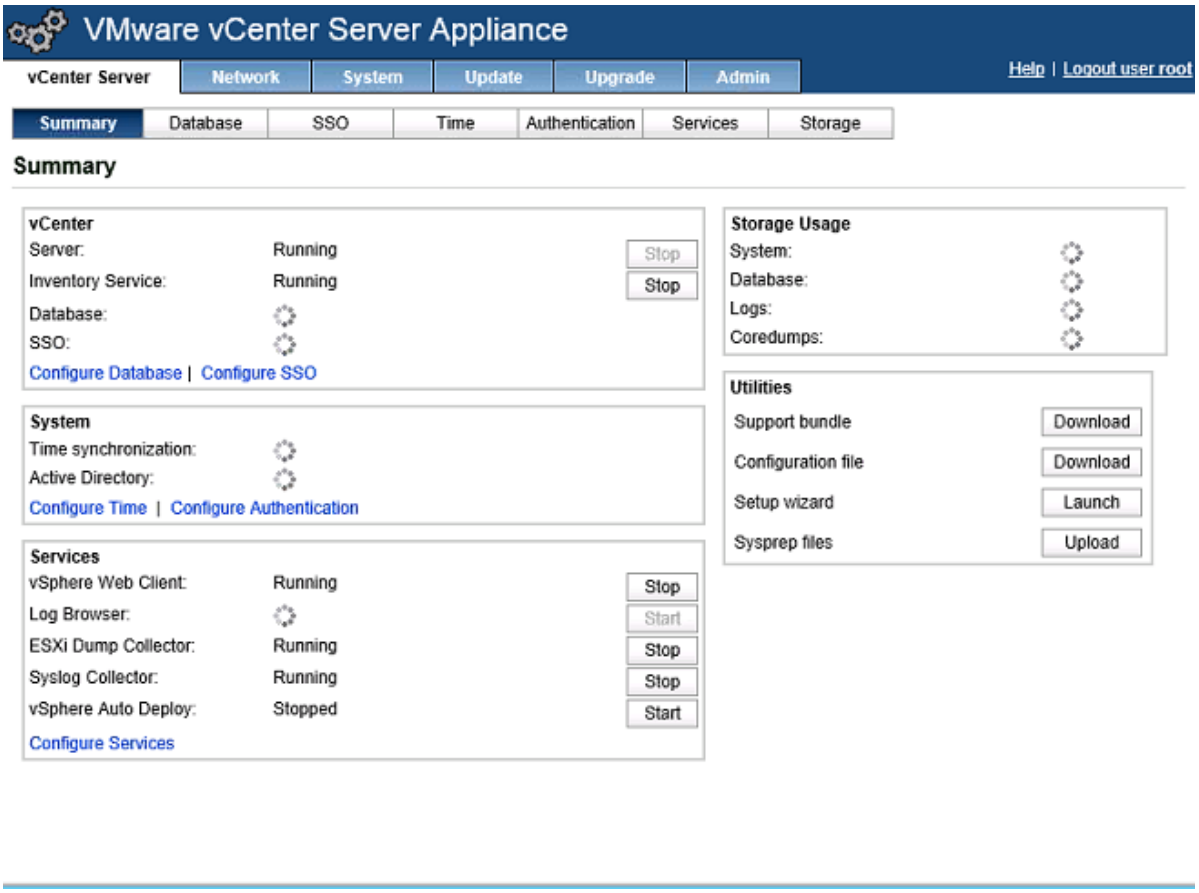
41. Review the configuration settings and click Start to complete the configuration.



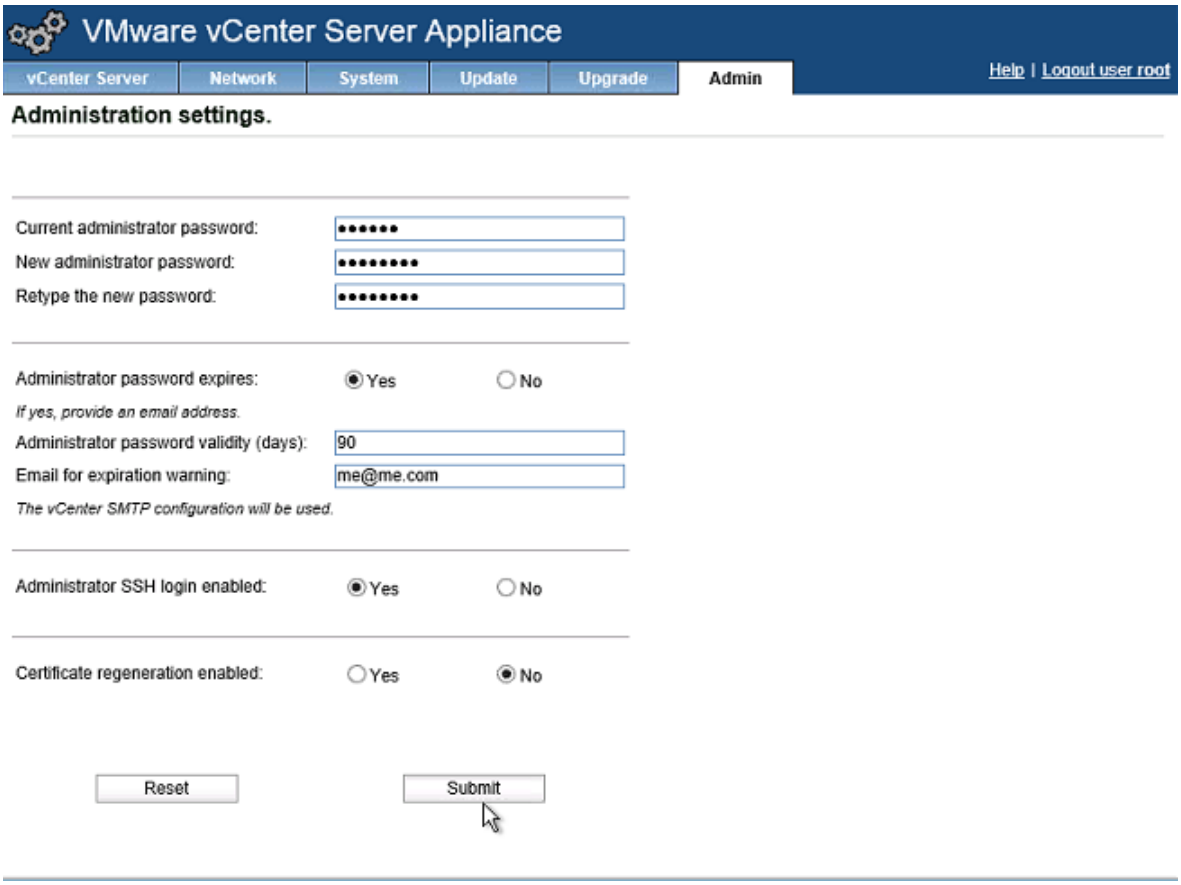
42. The vCenter server will create all of the necessary configurations and database structures specified in the preceding sections include SSO. Click Close.



43. Review the summary screen.



44. Click the admin Tab. Change the root user password and validate SSH login, password expiry settings and email setting then click Submit.



45. Logout user root after the configuration has completed.

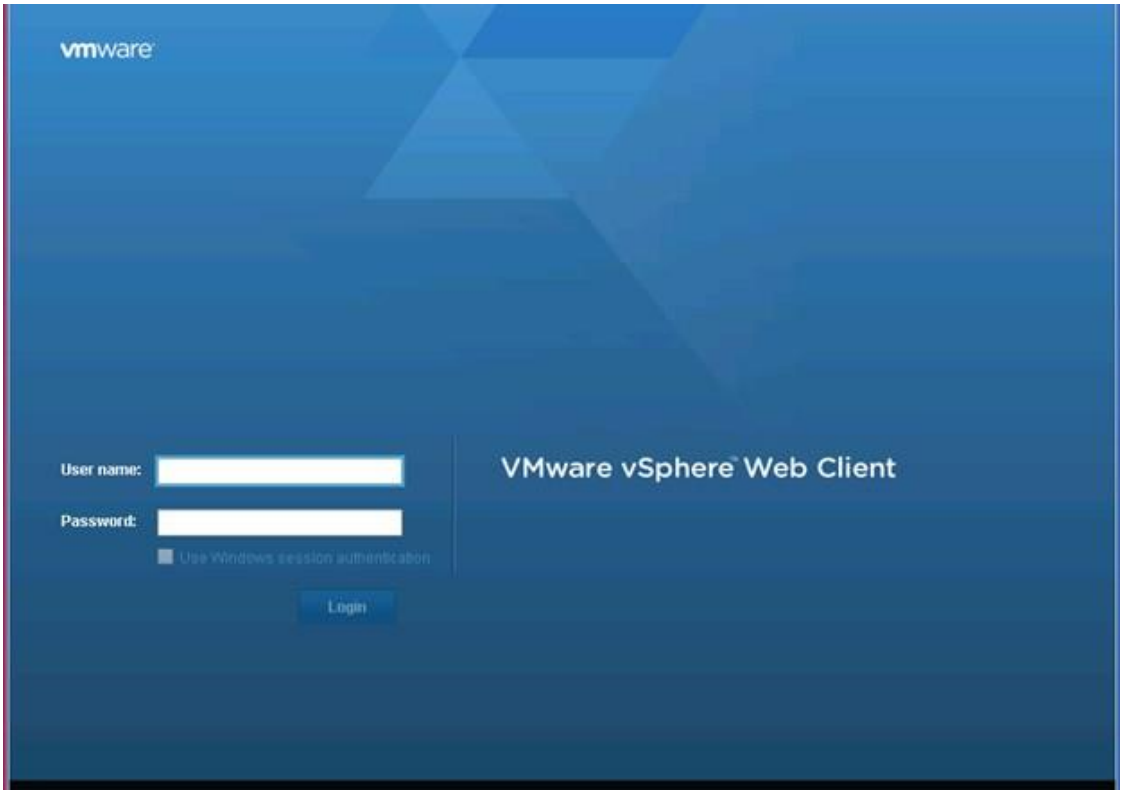
Log into the vSphere Web Client

To set up the Vmware environment log into the vSphere web client. You may need to install Adobe Flash for your browser.

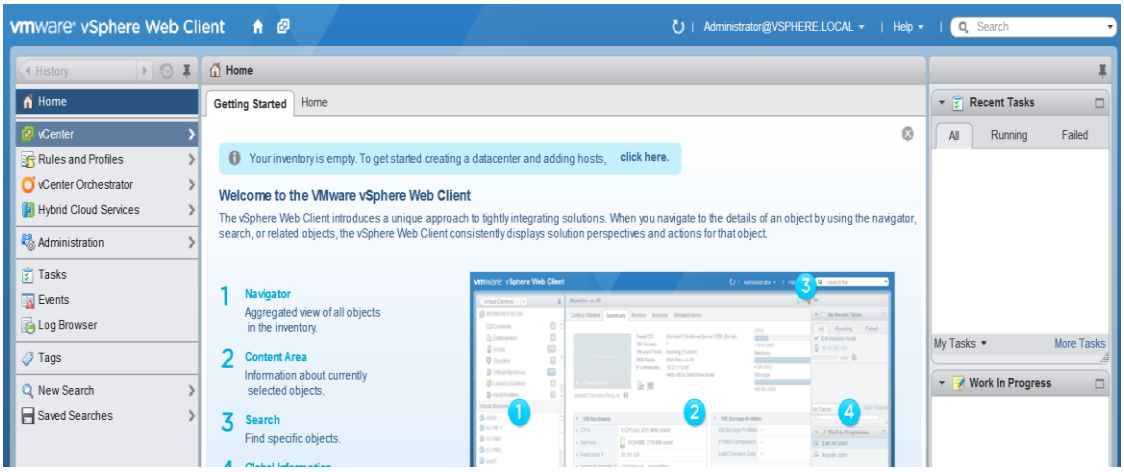
1. Using a web browser, navigate to https://<<var vcenter ip>>.
2. Click the link labeled Log in to vSphere Web Client.

3. If prompted, run the VMWare Remote Console Plug-in.

4. Log in using the root user name and password

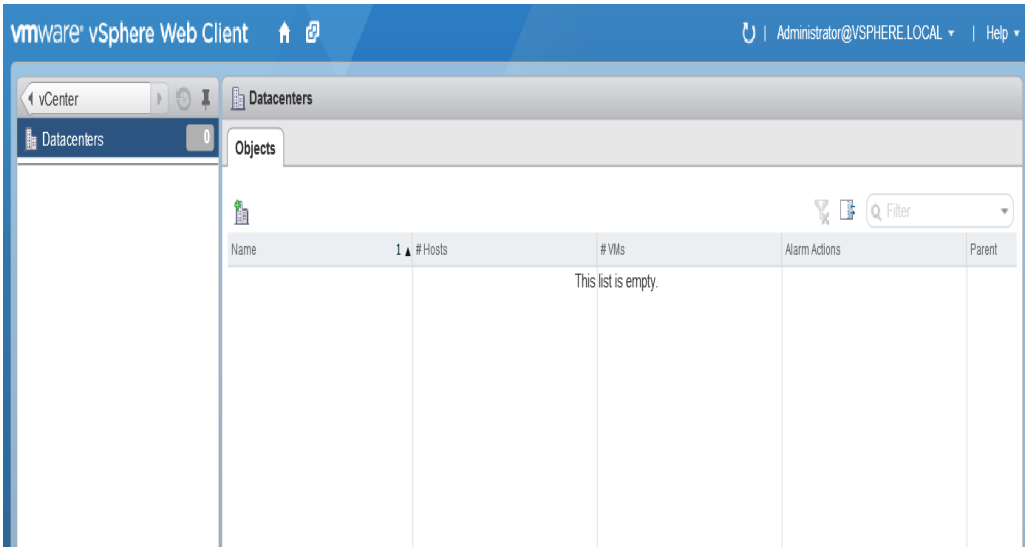


5. Click the vCenter link on the left panel.

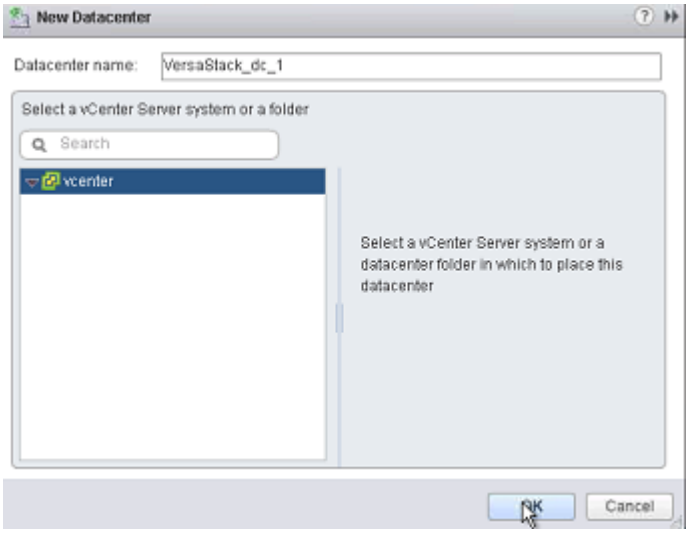


6. Click the Datacenters link on the left panel.

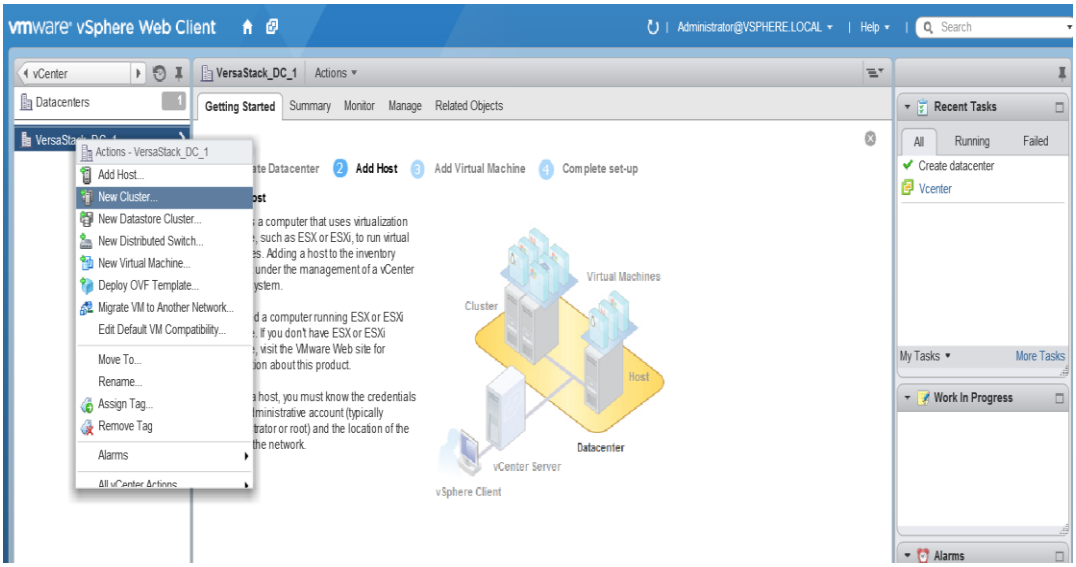
7. To create a Datacenter, click the icon in the center pane which has the green plus symbol above it.



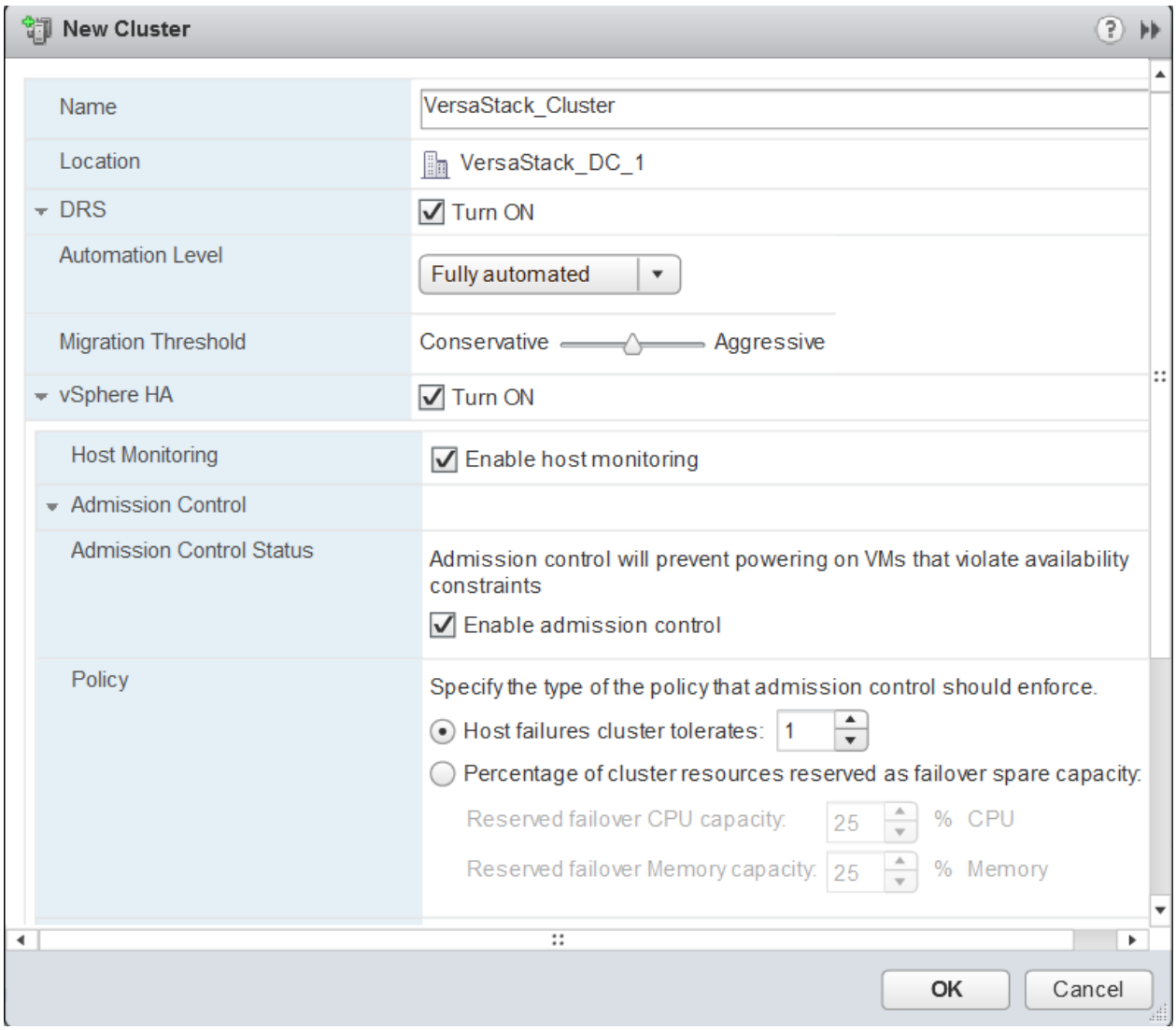
8. Type `VersaStack_DC_1` as the Datacenter name.
9. Click the vCenter server available in the list. Click OK to continue.



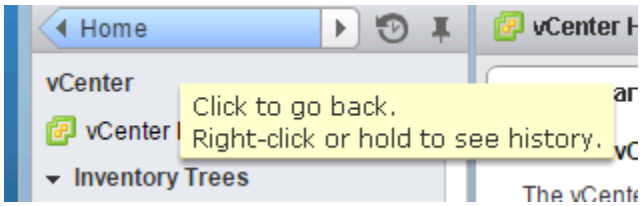
10. Right-click Datacenters > VersaStack_DC_1 in the list in the center pane, then click New Cluster.



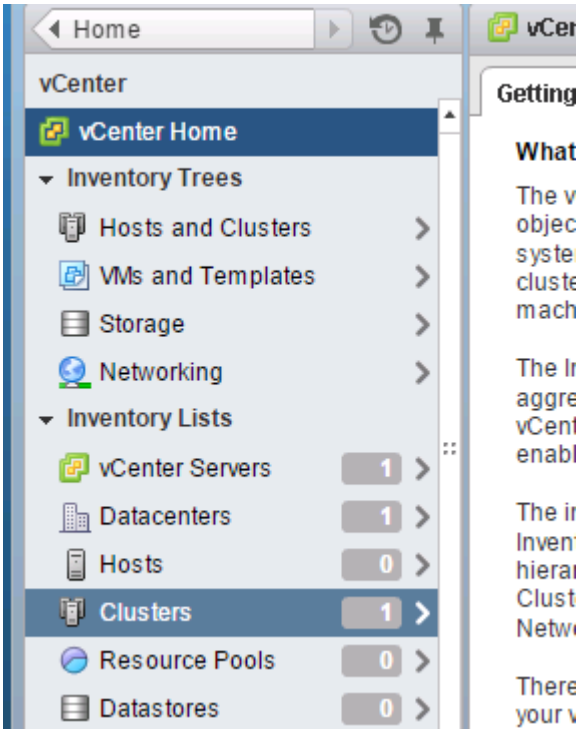
11. Name the cluster `VersaStack_Cluster`.
12. Select DRS Turn ON. Retain the default values.
13. Select vSphere HA Turn ON. Retain the default values.
14. Click OK to create the new cluster.



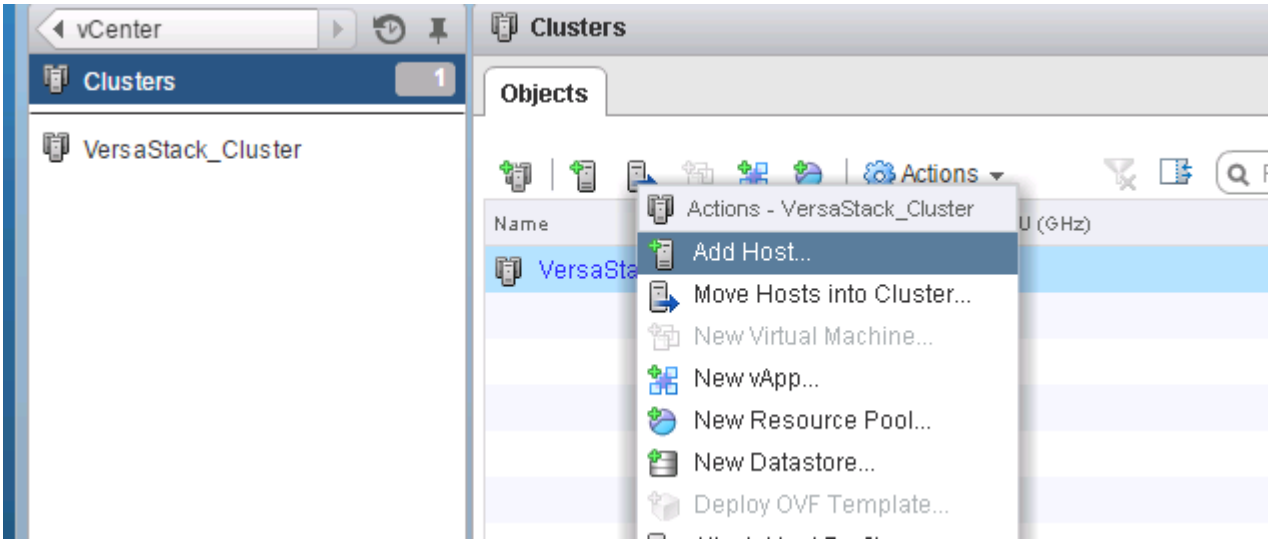
15. Return to the vCenter home screen via the top left button



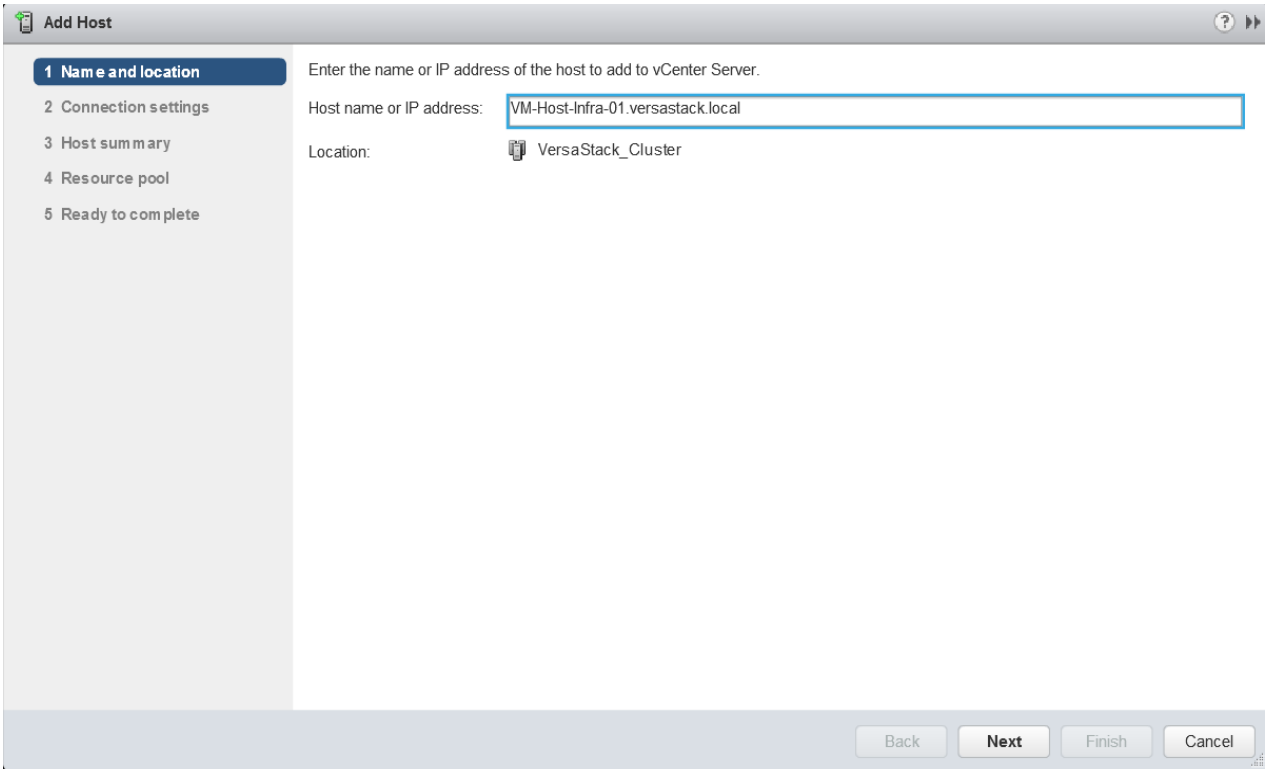
16. Click vCenter, then Clusters



17. Right click the VersaStack_Cluster in the center pane and click Add Host.

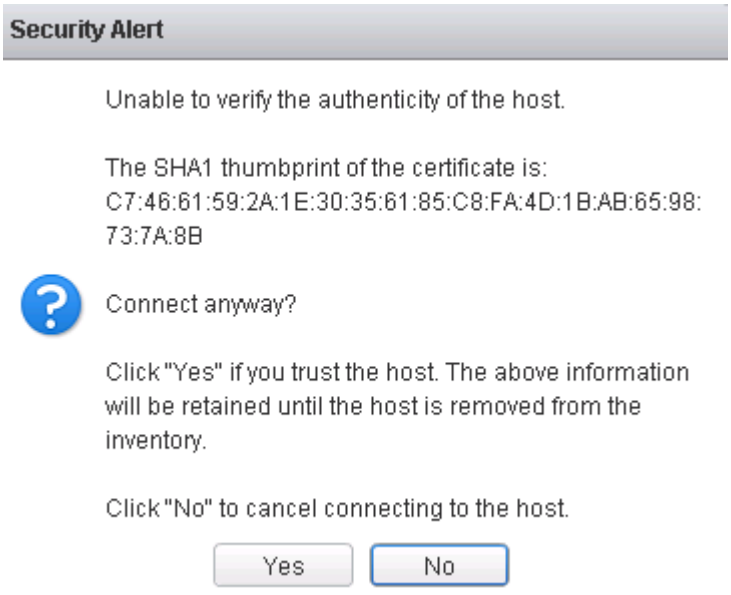


18. Type `<<var_esx_host_1_ip>>` or hostname and click Next.



19. Type `root` as the user name and `<<var_esx_host_password>>` as the password. Click Next to Continue.

20. Click Yes to accept the certificate.



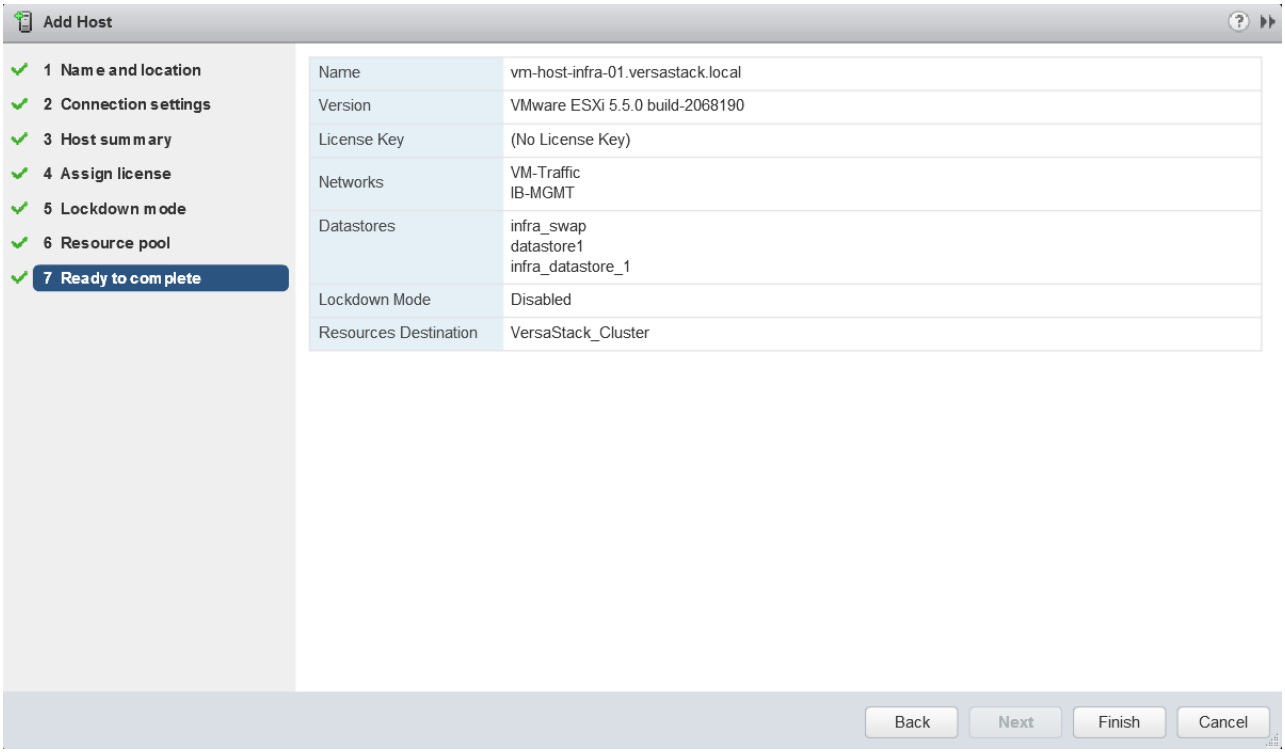
21. Review the host details, and click Next to continue.

22. Assign a license, and click Next to continue.

23. Click Next to continue past lockdown mode.

24. Click Next to continue past the resource pool screen.

25. Review the configuration parameters then click Finish to add the host.



26. Repeat the add cluster host procedure to add VM-Host-Infra-02.

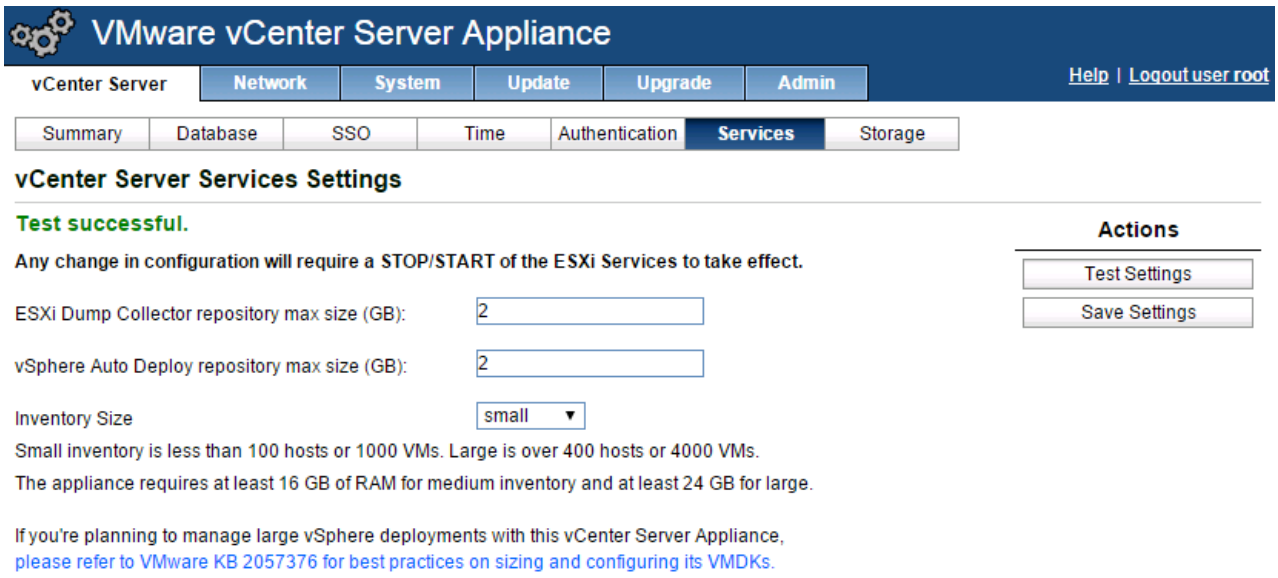
ESXi Dump Collector Setup

In this procedure it is required to have the VMware vSphere CLI 5.5 downloaded and installed as a prerequisite on our windows management host. You will need a registered VMware.com account to download the CLI software. You can refer to the VMware KB2002954 article for more information about configuration of the dump collector.

1. In Open a web browser, and connect to https://vCenterServerVirtualApplianceHostnameOrIP:5480/.

2. Log in using the root account

3. Click the Services tab and validate settings via the Test Settings button.

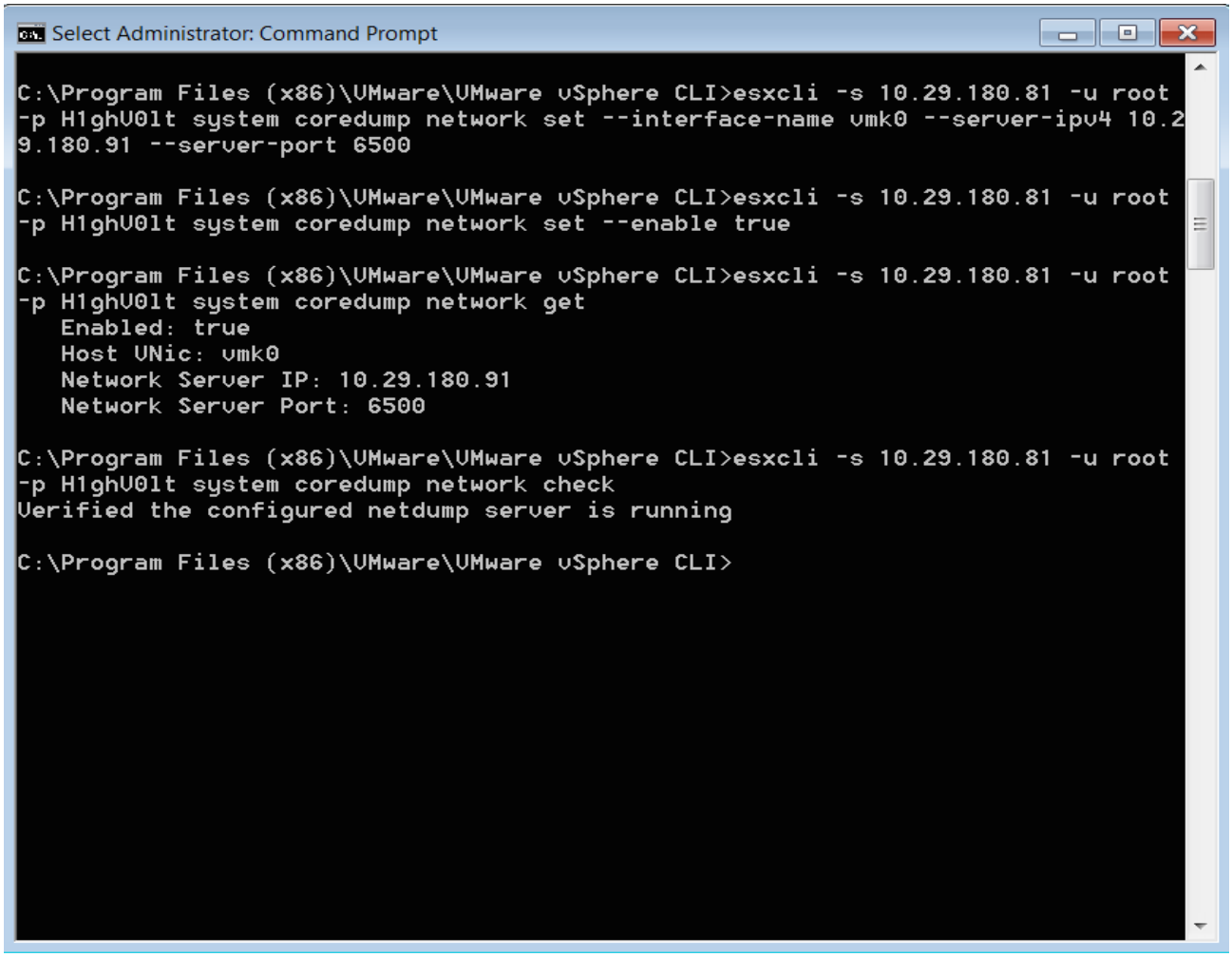


4. Back on the Management Workstation, open the VMware vSphere CLI command prompt.

5. Set each ESXi Host to core dump to the ESXi Dump Collector by running the following commands:

Make sure to type these commands since sometimes the hyphens do not cut and paste correctly (or you can do a find and paste with the hyphens).

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

esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>> system
coredump network set --interface-name vmk0 --server-ipv4
<<var_vcenter_server_ip> --server-port 6500

esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> system
coredump network set --enable true

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

esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> system
coredump network get

esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>> system
coredump network get


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

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



Map the Datastores on the IBM Storwize V5000 Second Host After Enabling the Cluster

1. Open the web client to the Storwize V5000.

2. Click the volumes button in the left pane and select volume to open the volumes screen.
3. Right-click the volume infra_datastore_1 and select map to host.
4. Choose host VM-Host-Infra-02, and leave All I/O Groups default and select Map Volumes.
5. Click Map All volumes on the warning popup click close.
6. Right-click the volume infra_swap and leave All I/O Groups default and select map to host.
7. Choose host VM-Host-Infra-02 and select Map Volumes.
8. Click Map All volumes on the warning popup click Close.
9. In vSphere in the left pane right-click the VersaStack cluster, and click rescan for datastores.

At this point of the install, there is a warning for no network management redundancy. If you plan to add the optional Cisco 1000v virtual switch, that will remedy the issue. If you are not installing the 1000v, you should add the second Cisco network adapter to the VMware standard switch to each ESX hosts. This can be completed via the vSphere client for each host by clicking on the configuration tab, and in the hard-ware pane, click Networking, click the properties of vSwitch0. From the Network adapters tab, click Add and select the unclaimed adapter vmnic1, and click Next, then click Next again and then click Finish, then Close.

Move VM Swap File Location

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

To move the VM swap file location, complete the following steps on each ESXi host:

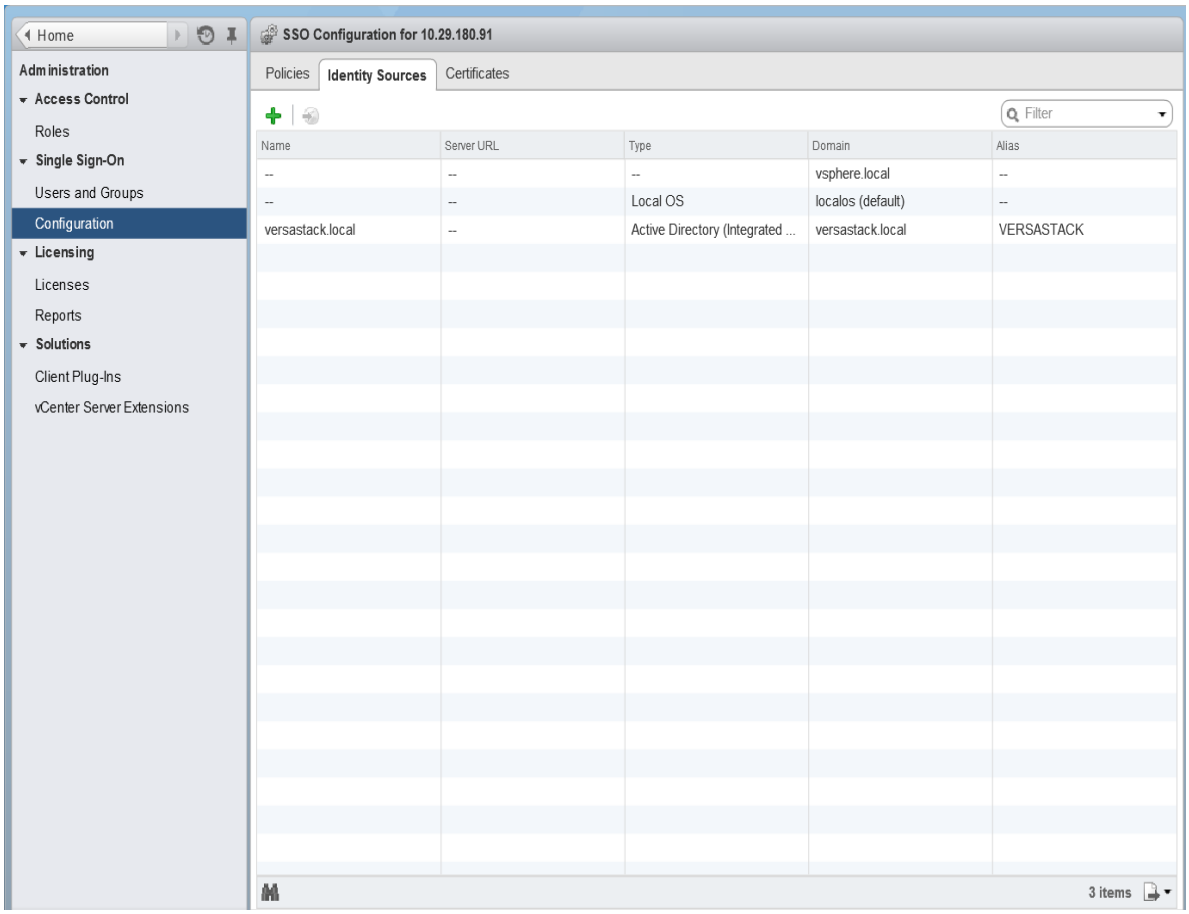
1. From each vSphere Client, select the host in the inventory.
2. Click the Configuration tab to enable configurations.
3. Click Virtual Machine Swapfile Location in the Software pane.
4. Click Edit at the upper right side of the window.
5. Select Store the swapfile in a swapfile datastore selected below.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

At this point of the installation you might want to shut down your compute environment and take a clean snapshot for your IBM volumes.

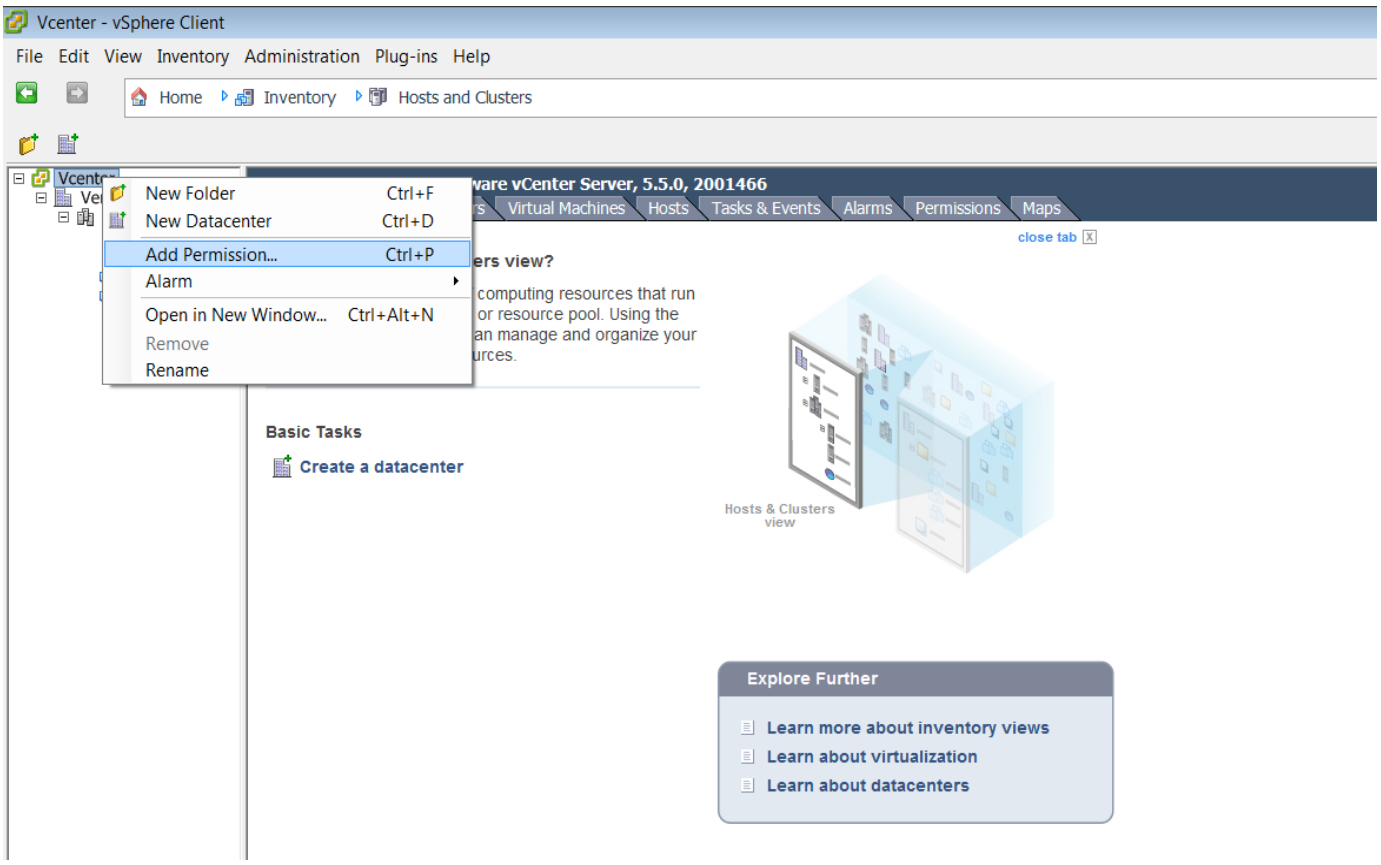
Optional: Add Domain Account Permissions

In this section, you will add a user to provide admin and login permissions in the vSphere client

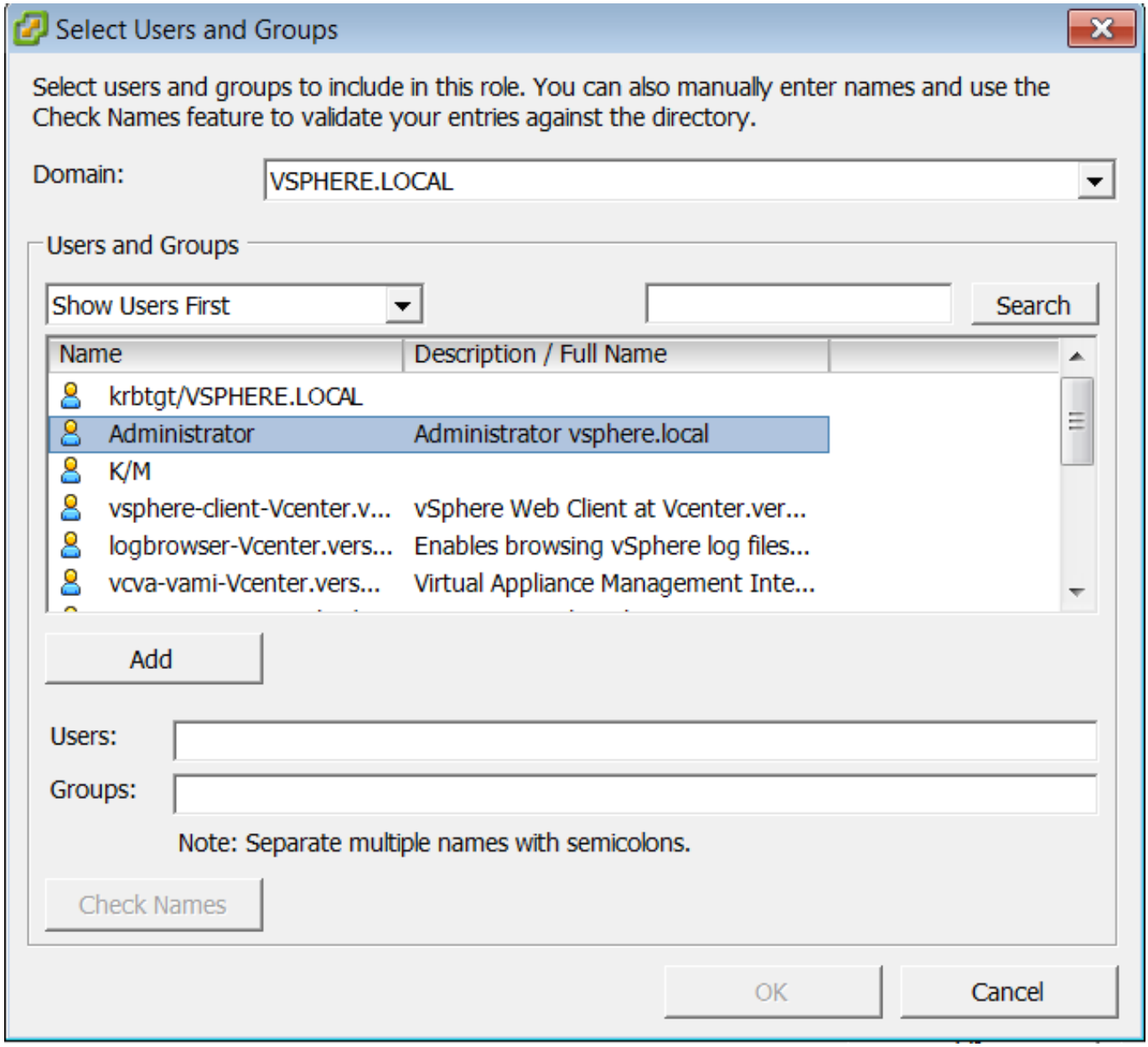
1. In the vSphere web client login as administrator@vsphere.local and navigate to the administration pane, then click configuration to make sure you have the correct identity sources added such as the proper active directory domain. You can use the green plus sign to add identity sources.



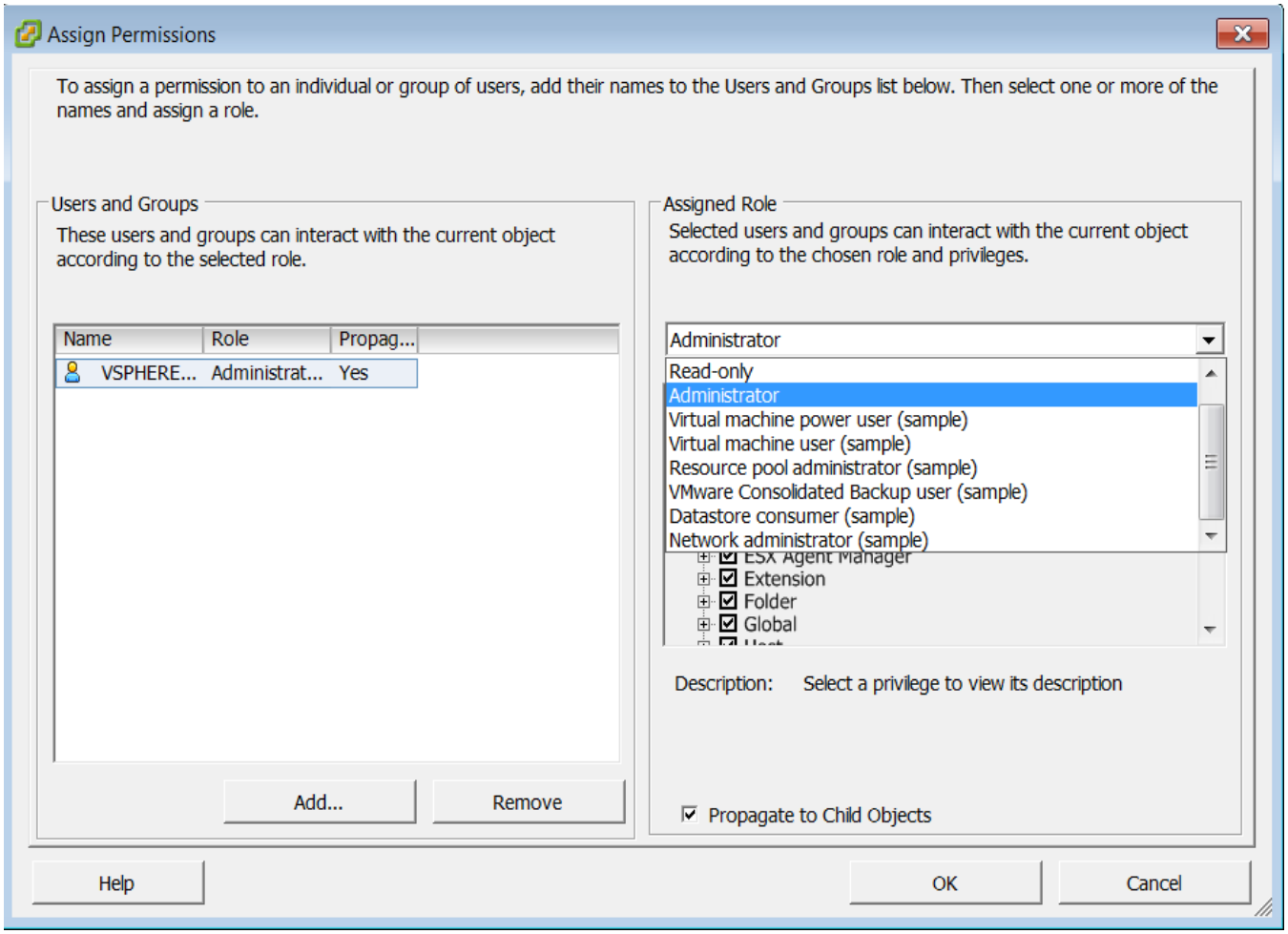
2. Logging into the vSphere thick client as administrator@vsphere.local and right-click the appropriate level for permissions and click Add Permissions.



3. Select Add.
4. Select the domain.
5. Highlight a user and click Add, then click OK.



6. Change the assigned role to the correct group, and click OK.



7. Log off as administrator and back in as that domain user.

Set Up the Optional Cisco Nexus 1000V Switch Using Cisco Switch Update Manager

Cisco Nexus 1000V

The Cisco Nexus 1000V is a distributed virtual switch solution that is fully integrated within the VMware virtual infrastructure, including VMware vCenter, for the virtualization administrator. This solution offloads the configuration of the virtual switch and port groups to the network administrator to enforce a consistent data center network policy. The Cisco Nexus 1000V is compatible with any upstream physical access layer switch that is compliant with Ethernet standard, Cisco Nexus switches, and switches from other network vendors. The Cisco Nexus 1000V is compatible with any server hardware that is listed in the VMware Hardware Compatibility List (HCL).

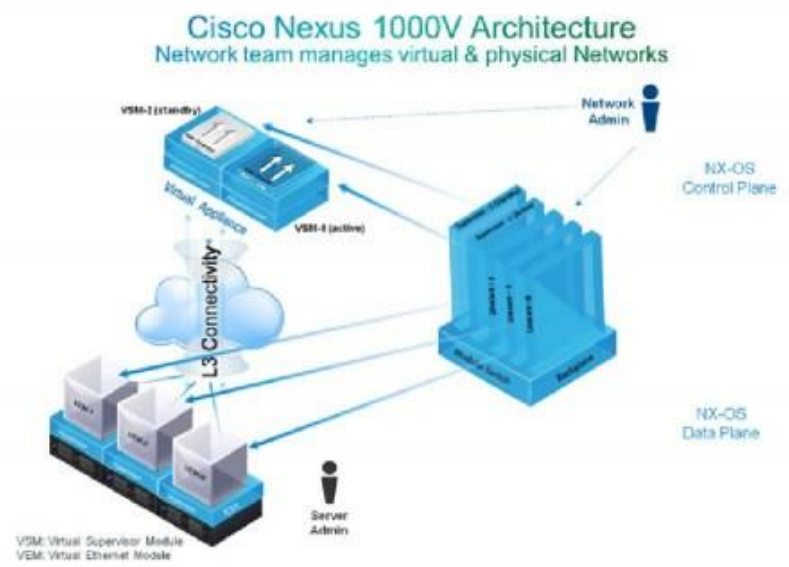
The Cisco Nexus 1000V has the following components:

- Virtual Supervisor Module (VSM)—The control plane of the switch and a VM that runs Cisco NX-OS.
- Virtual Ethernet Module (VEM)—A virtual line card that is embedded in each VMware vSphere (ESXi) host. The VEM is partly inside the kernel of the hypervisor and partly in a user-world process, called the VEM Agent.

Cisco Nexus 1000V Architecture

Figure 7 illustrates the Cisco Nexus 1000V architecture.

Figure 7 Cisco Nexus 1000V Architecture



Layer 3 control mode is the preferred method of communication between the VSM and the VEMs. In Layer 3 control mode, the VEMs can be in a different subnet than the VSM and from each other. Active and standby VSM control ports should be Layer 2 adjacent. These ports are used to communicate the HA protocol between the active and standby VSMs. Each VEM needs a designated VMkernel NIC interface that is attached to the VEM that communicates with the VSM. This interface, which is called the Layer 3 Control vmknic, must have a system port profile applied to it (see System Port Profiles and System VLANs), so the VEM can enable it before contacting the VSM.

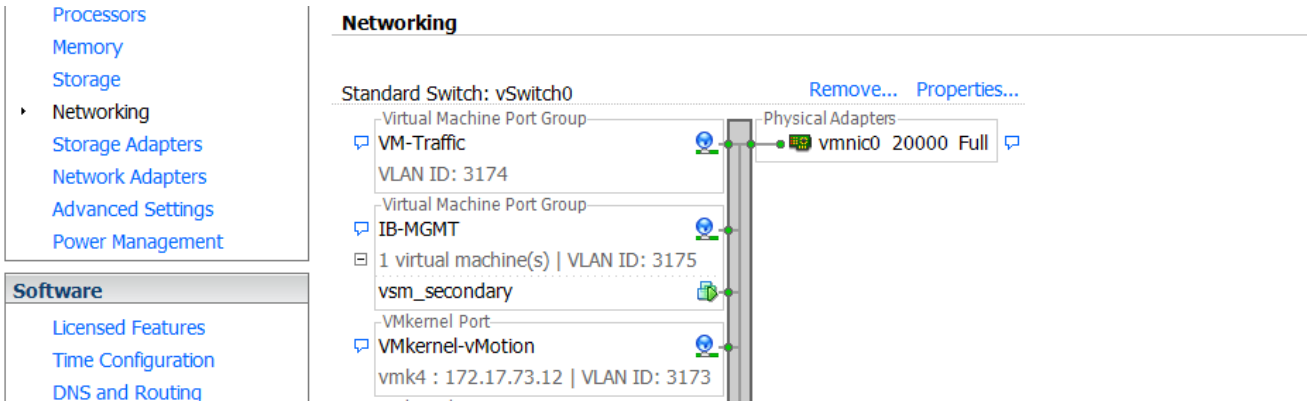
Installation Process

To create network redundancy for the migration, create a temporary VMkernel.

ESXi Host VM-Host-Infra-01

Repeat the steps 1-11 in this section for all the ESXi Hosts.

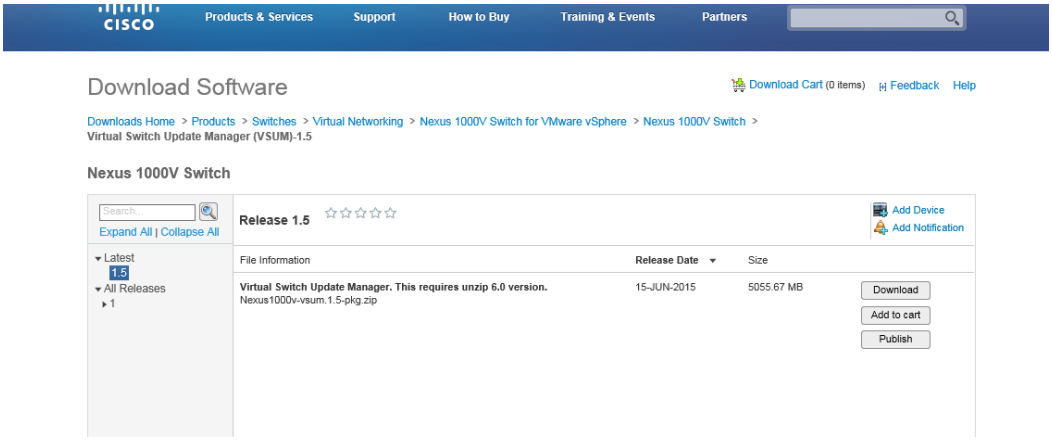
1. From each vSphere Client, select the host in the inventory.
2. Click the Configuration tab.
3. Click Networking in the Hardware then Properties



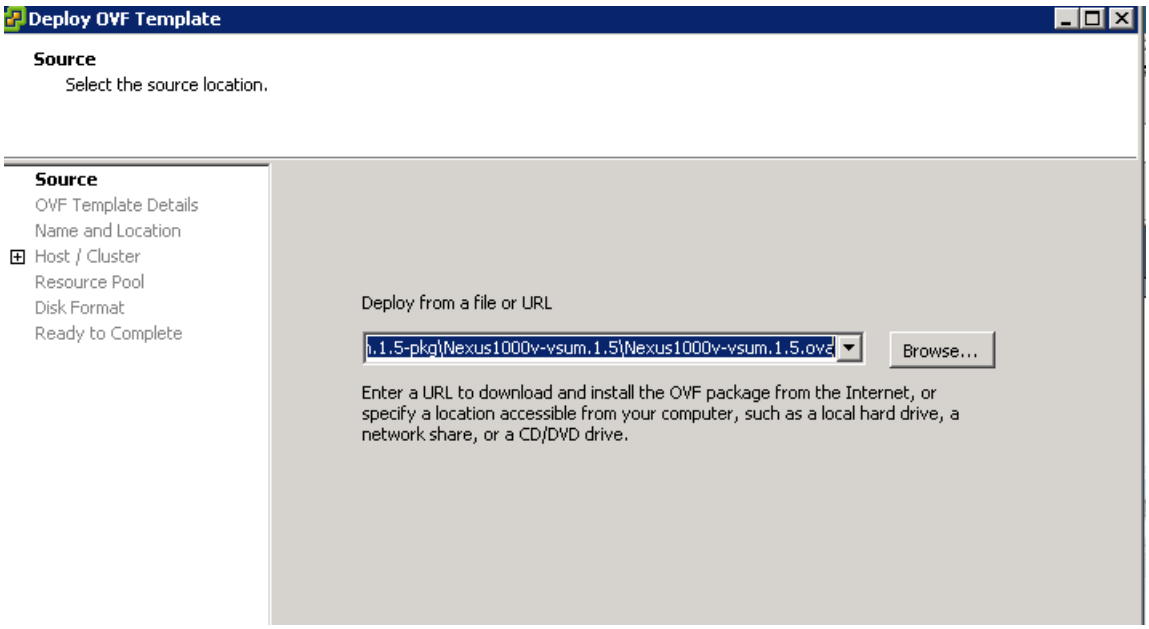
4. Click Add
5. Select VMkernel and click Next.
6. Change the network label to VMkernel-MGMT-2 and enter `<<var_ib-mgmt_vlan_id>>` in the VLAN ID (Optional) field.
7. Select Use this port group for management traffic
8. Click Next to continue with the VMkernel creation.
9. Enter the IP address `<<var_vmhost_infra_01_2nd_ip>>` and the subnet mask for the VLAN interface for VM-Host-Infra-01.
10. Click Next to continue with the VMkernel creation.
11. Click Finish to finalize the creation of the new VMkernel interface

Deploy the OVF Template for the Cisco Nexus 1000 Virtual Switch Update Manager

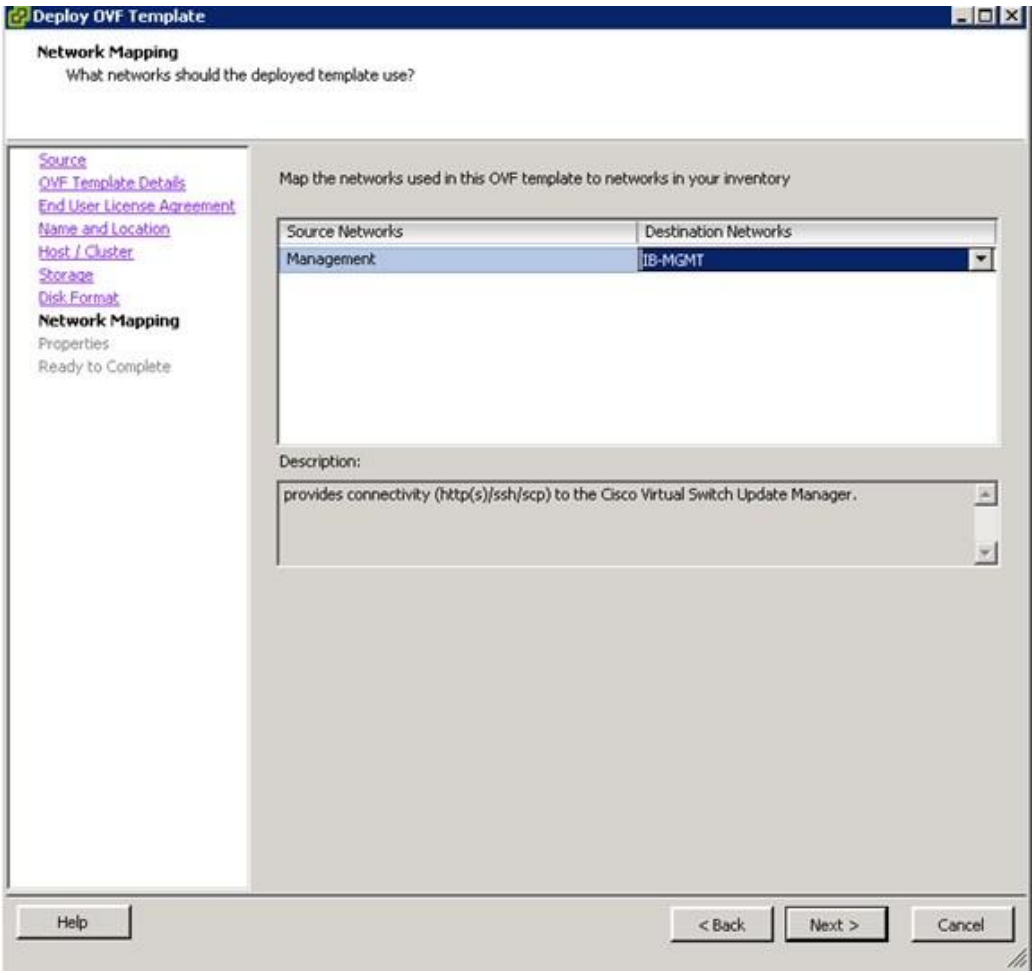
1. Log in and Download the Cisco Nexus 1000V installation software from www.cisco.com.



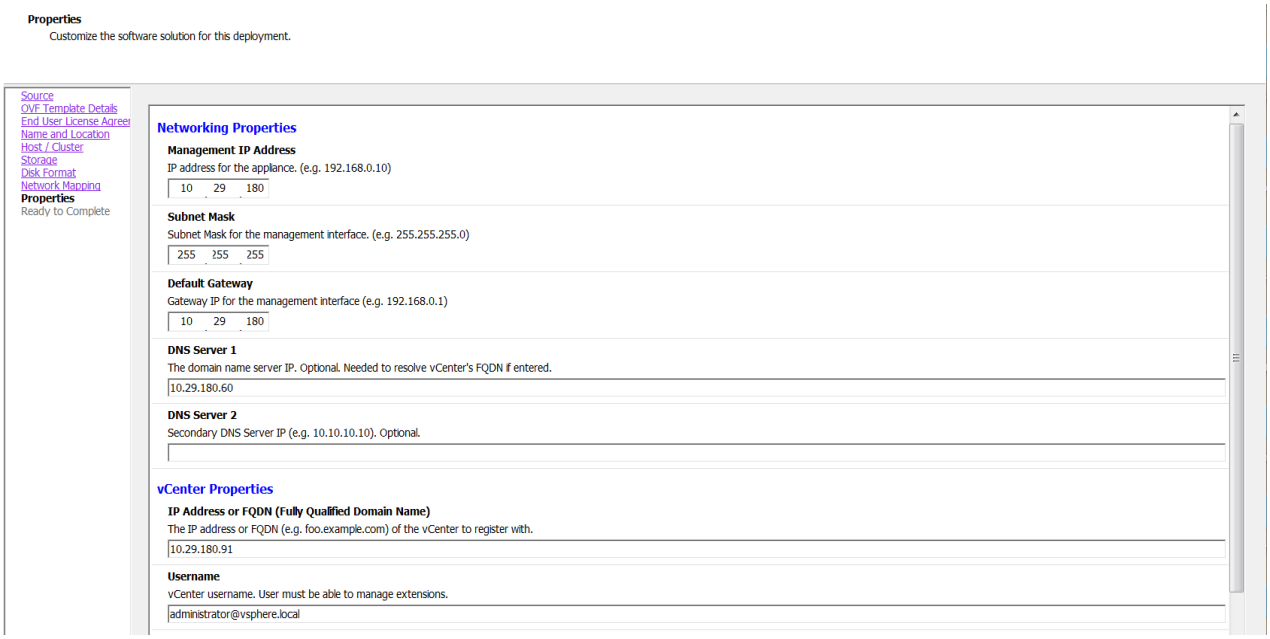
2. Unzip the package contents and validate you can view the ova file.
3. From the vSphere client, click File, Deploy OVF Template and browse to the unzipped ova file.



4. Click Next, then click Next again.
5. Review the license agreement. Click Next.
6. Click Next on the Name and Location screen.
7. Select `infra_datastore_1` as the Datastore and click Next.
8. Choose a disk format and click Next.
9. For Network Mapping make sure you have Management Mapped to `IB-Mgmt` and click Next.

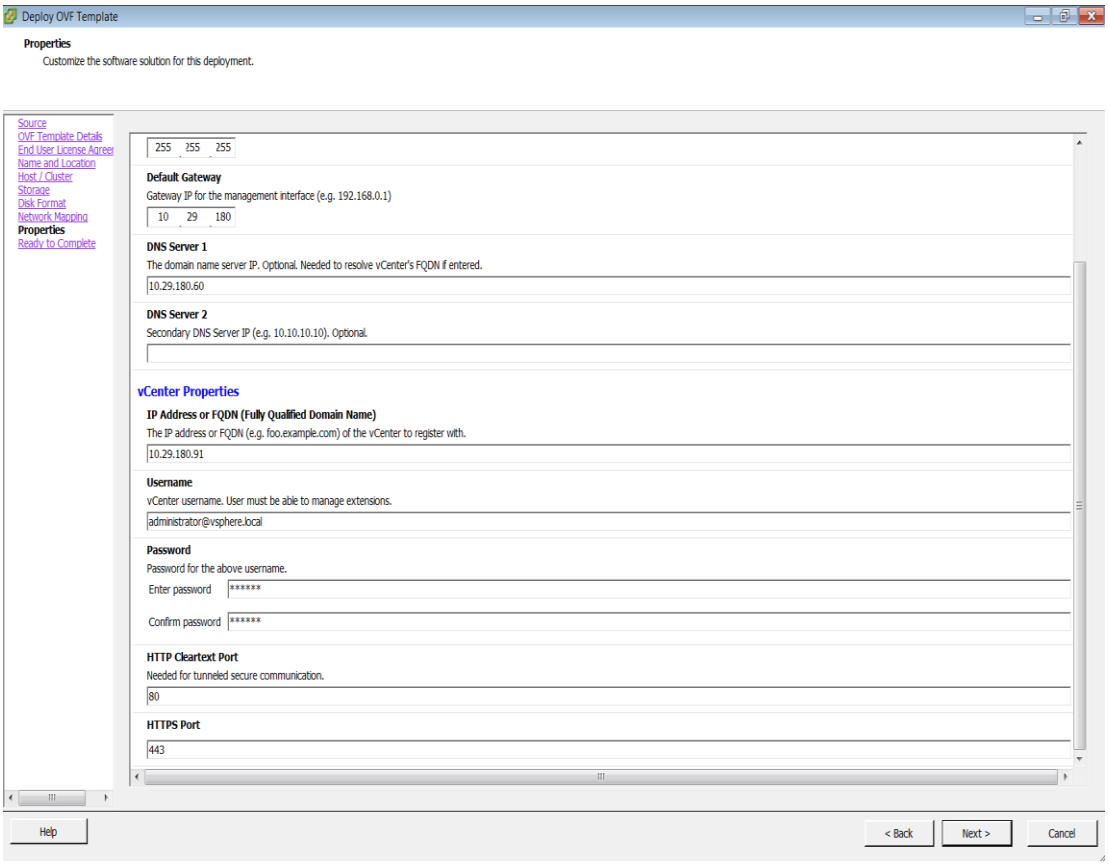


10. On the Properties screen, input `<<var_vsm_updatemgr_mgmt_ip>> <<var_vsm_mgmt_mask>> <<var_vsm_mgmt_gateway>> <<var_nameserver_ip>>.`

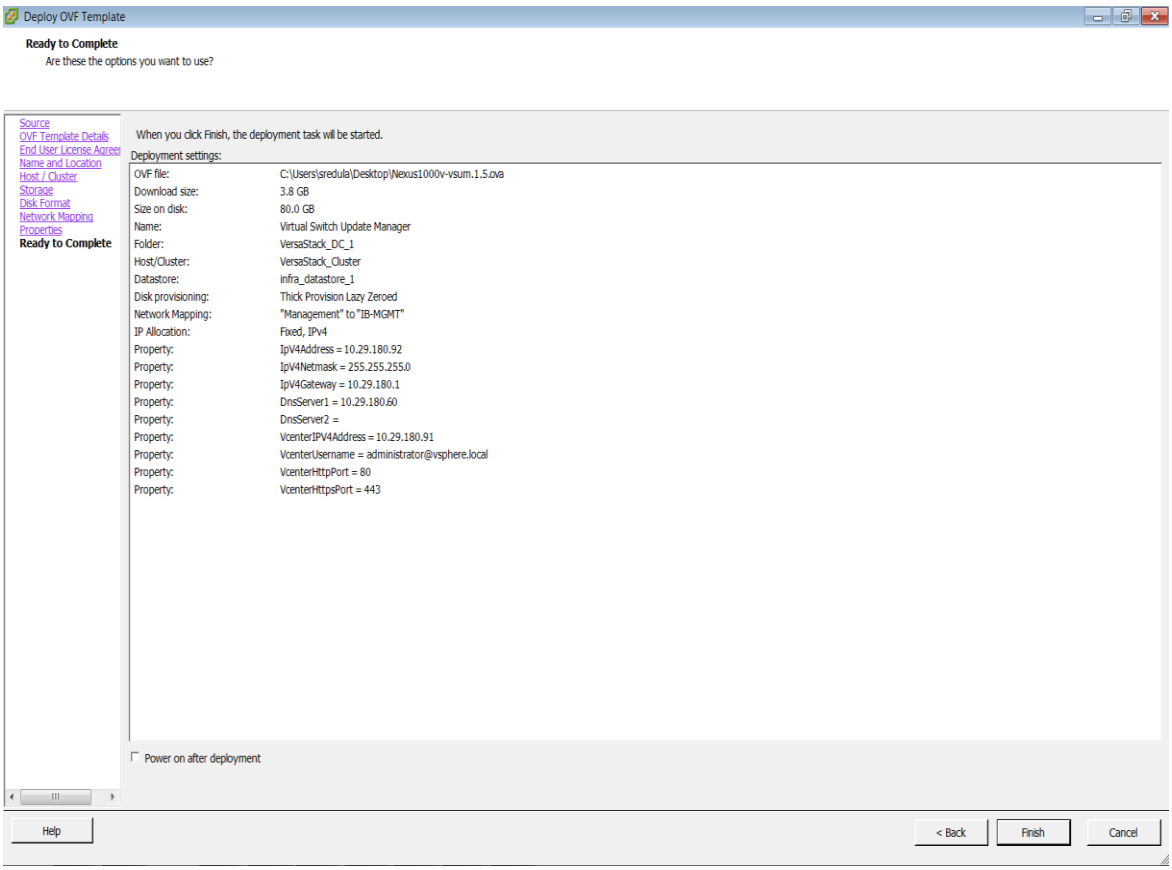


11. Enter the vCenter IP and login information. For domain accounts, use the Administrator@Vsphere.local login format and do not use domainname\user account format.

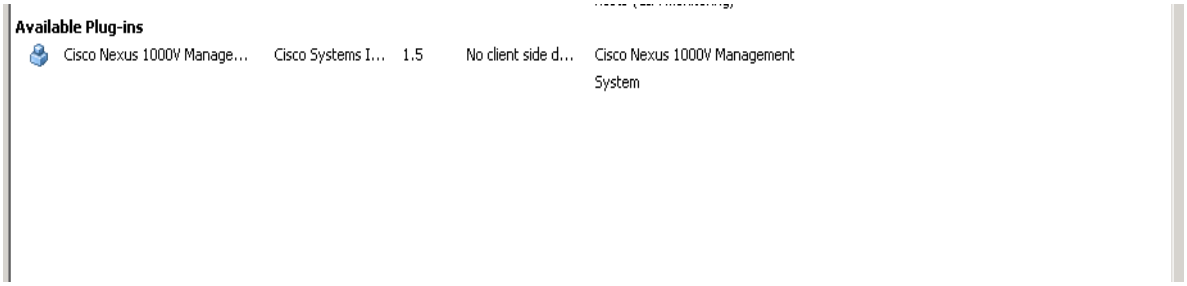
12. Accept default ports, and click Next.



13. Review the summary screen, click Power on after deployment and click Finish.



14. After the VM boots in a few minute the Plugin is registered. Validate the plugin in the vSphere client by clicking Plug-ins, then Manage plug-ins in the top menu bar and look under Available Plug-ins.



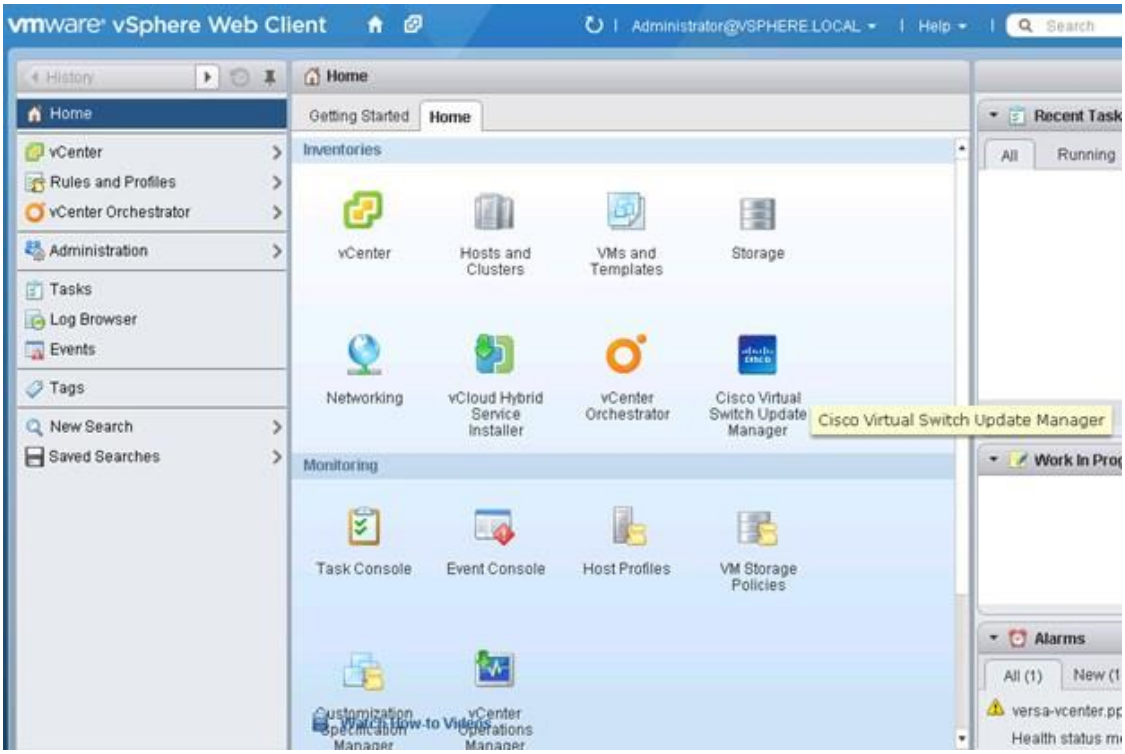
Install the VSM through the Cisco Virtual Switch Update Manager

The VSUM will deploy the VSM primary and secondary to the ESXi hosts through the GUI install. You will have a VSM prmary running on 1 ESXi host and a secondary running on the other ESXi host. Both of these are installed at them same time through the host selection. Complete the following steps to deploy the VSM

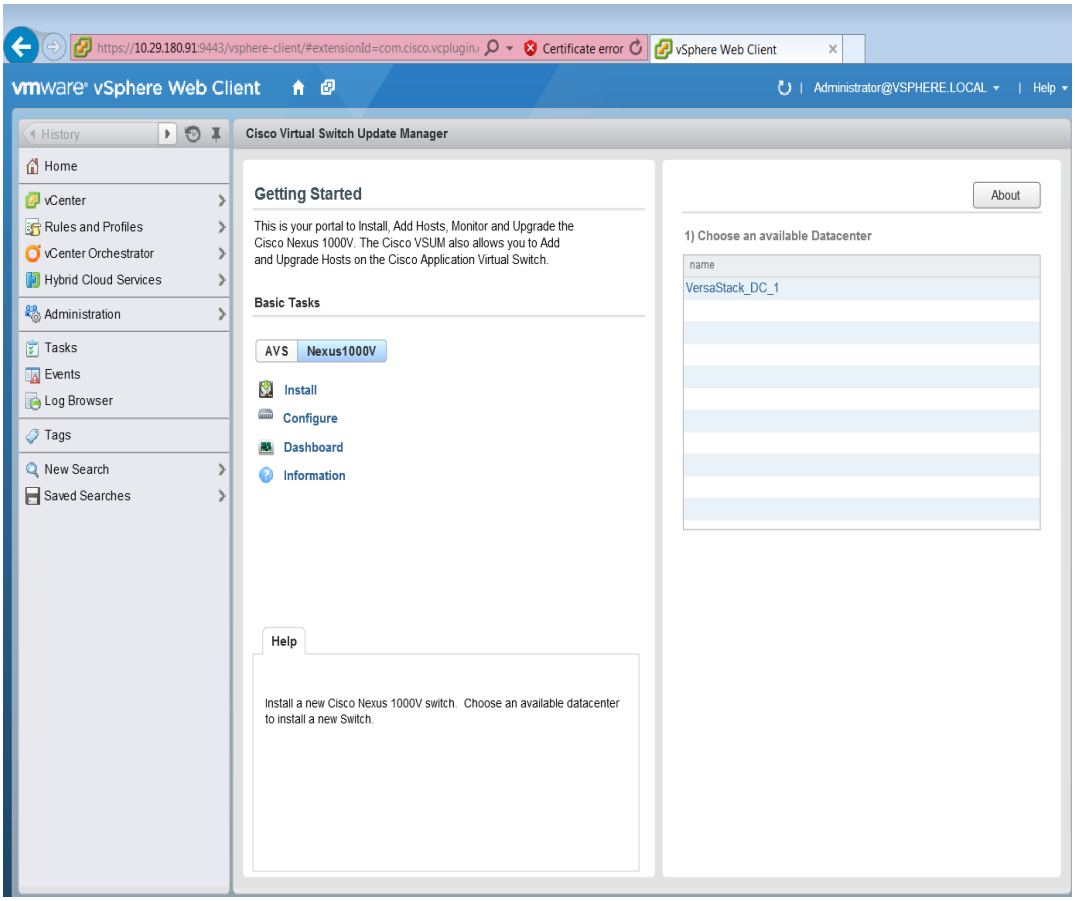
On the machine where you will run the browser for the VMware vSphere Web Client, you should have installed Adobe Flash as well the Client Integration plugin for the web client. The plug-in can be downloaded from the lower left corner of the web client login page.

1. Launch the vSphere Web client interface `https://<<Vcenter_host_ip>>:9443/vsphere-client` and login.

2. Select the home tab and click Cisco Virtual Switch Update Manager.

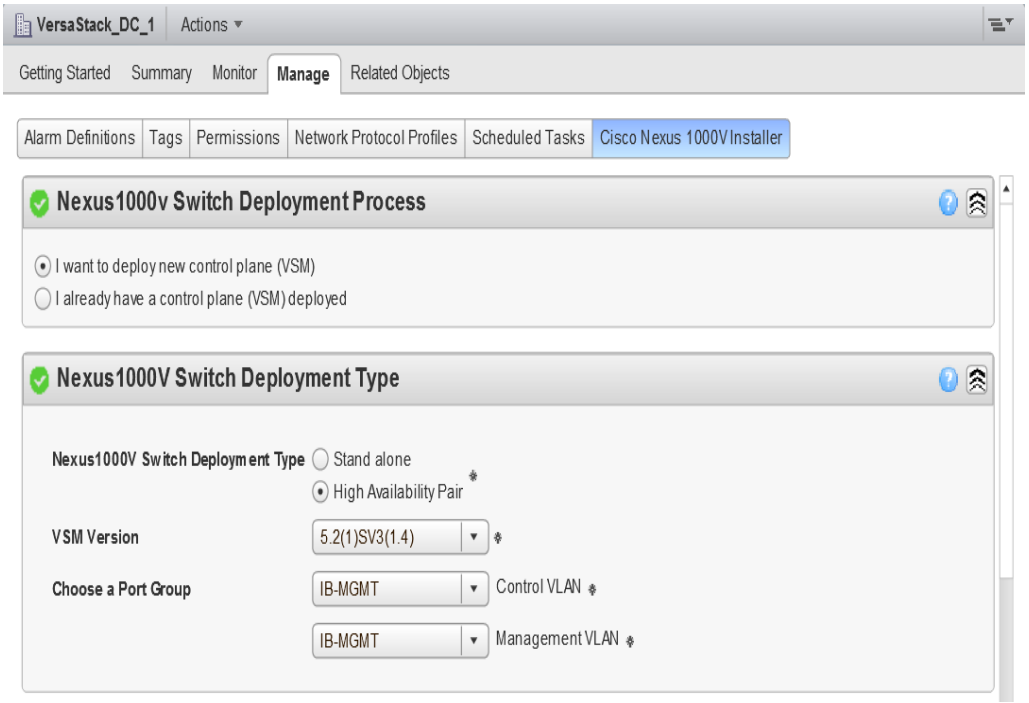


3. Click the Nexus 1000V button then click Install.

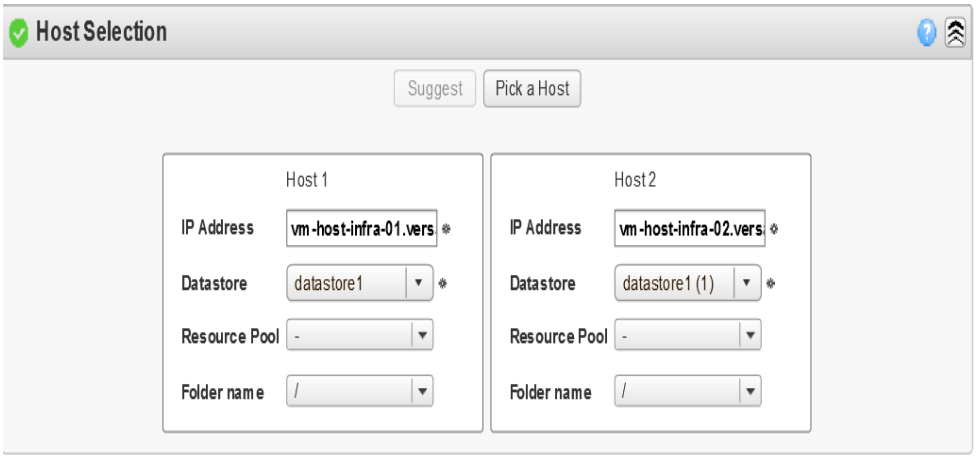


4. Click the VersaStack Datacenter in the right pane of the screen.

5. Keep the default for deploy new VSM and High Availability Pair. Select IB-Mgmt for the control and Management VLAN.

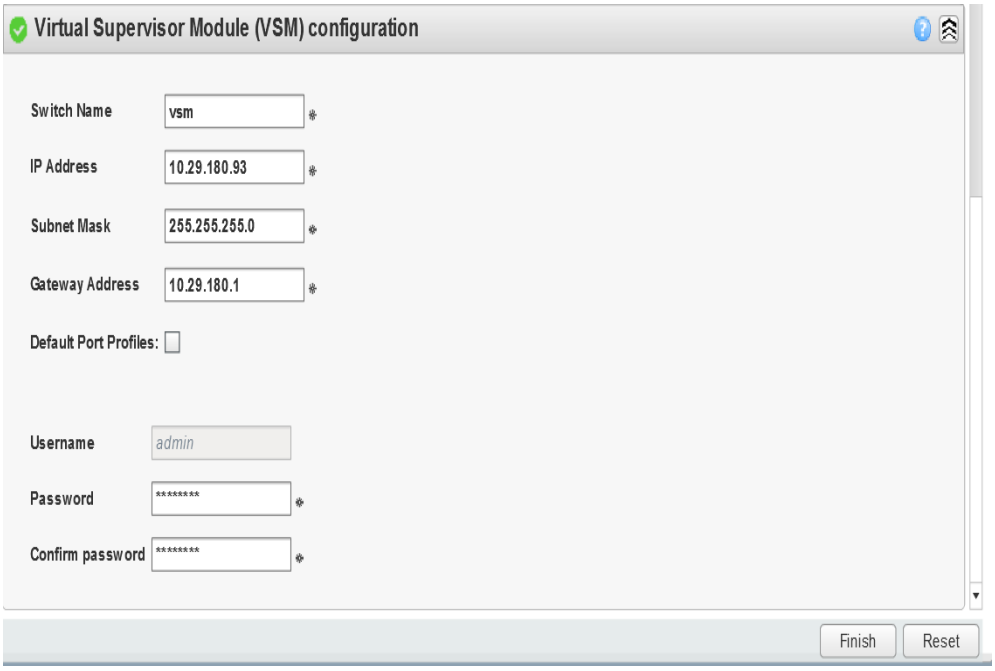


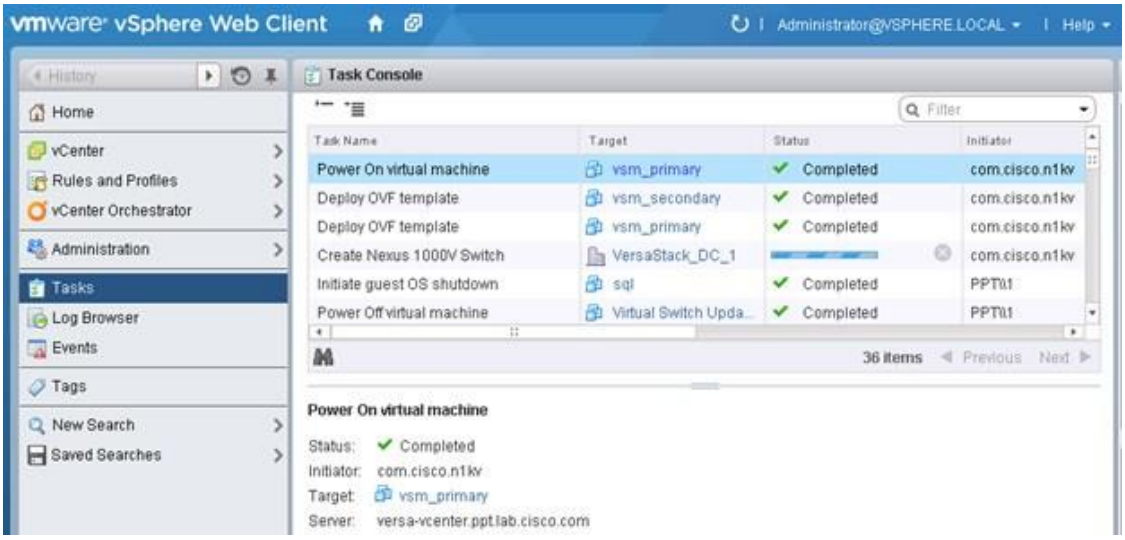
6. For the Host Selection, click the Suggest button and choose the Datastores.



7. Enter a domain ID for the switch configuration section.

8. Enter the following information for the VSM configuration `<<var_vsm_hostname>>` `<<var_vsm_mgmt_ip>>`, `<<var_vsm_mgmt_mask>>` `<<var_vsm_mgmt_gateway>>` `<<var_password>>`, then click Finish. You can launch a second VSphere Client to monitor the progress. Click Tasks in the left pane. It will take a few minutes to complete.





Perform Base Configuration of the Primary VSM

To perform the base configuration of the primary VSM, complete the following steps:

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

```
config t
ntp server <<var_global_ntp_server_ip>> use-vrf management
vlan <<var_ib-mgmt_vlan_id>>
name IB-MGMT-VLAN
vlan <<var_nfs_vlan_id>>
name NFS-VLAN
vlan <<var_vmotion_vlan_id>>
name vMotion-VLAN
vlan <<var_vm-traffic_vlan_id>>
name VM-Traffic-VLAN
vlan <<var_native_vlan_id>>
name Native-VLAN
exit
port-profile type ethernet system-uplink
vmware port-group
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_nfs_vlan_id>>,
```

```
<<var_vmotion_vlan_id>>, <<var_vm-traffic_vlan_id>>

channel-group auto mode on mac-pinning

no shutdown

system vlan <<var_ib-mgmt_vlan_id>>, <<var_nfs_vlan_id>>,
<<var_vmotion_vlan_id>>, <<var_vm-traffic_vlan_id>>

system mtu 9000

state enabled

exit


port-profile type vethernet IB-MGMT-VLAN

vmware port-group

switchport mode access

switchport access vlan <<var_ib-mgmt_vlan_id>>

no shutdown

system vlan <<var_ib-mgmt_vlan_id>>

state enabled

exit

port-profile type vethernet NFS-VLAN

vmware port-group

switchport mode access

switchport access vlan <<var_nfs_vlan_id>>

no shutdown

system vlan <<var_nfs_vlan_id>>

state enabled

exit

port-profile type vethernet vMotion-VLAN

vmware port-group

switchport mode access

switchport access vlan <<var_vmotion_vlan_id>>

no shutdown

system vlan <<var_vmotion_vlan_id>>

state enabled

exit

port-profile type vethernet VM-Traffic-VLAN
```

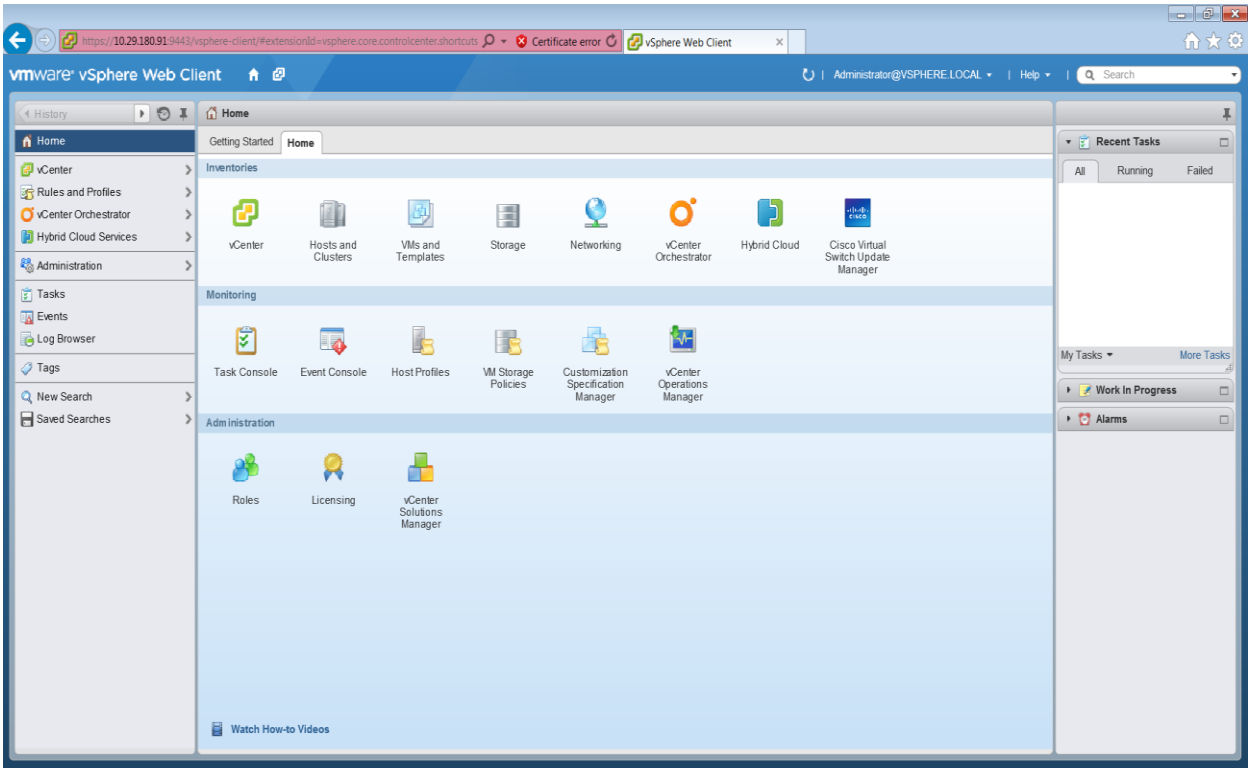
```
vmware port-group
switchport mode access
switchport access vlan <<var_vm-traffic_vlan_id>>
no shutdown
system vlan <<var_vm-traffic_vlan_id>>
state enabled
exit
port-profile type vethernet n1kv-L3
capability l3control
vmware port-group
switchport mode access
switchport access vlan <<var_ib-mgmt_vlan_id>>
no shutdown
system vlan <<var_ib-mgmt_vlan_id>>
state enabled
exit

copy run start
```

Migrate Networking Components for ESXi Hosts to Cisco Nexus 1000V

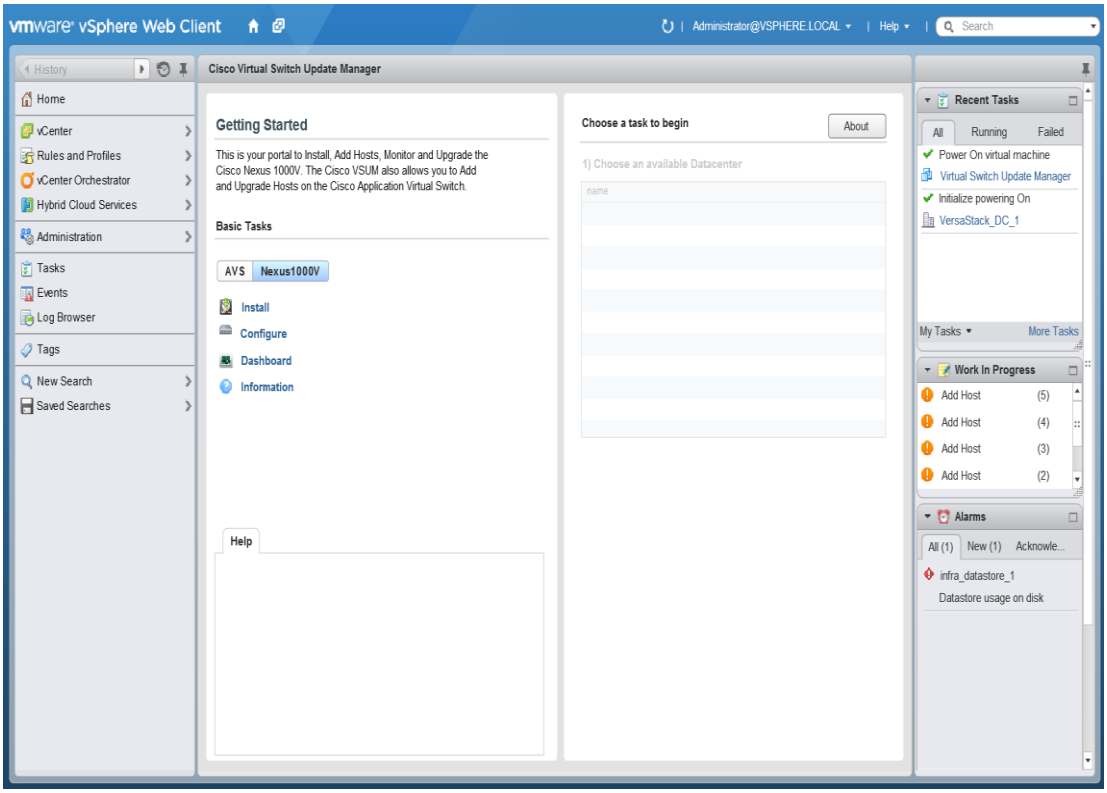
vSphere Client Connect to vCenter

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

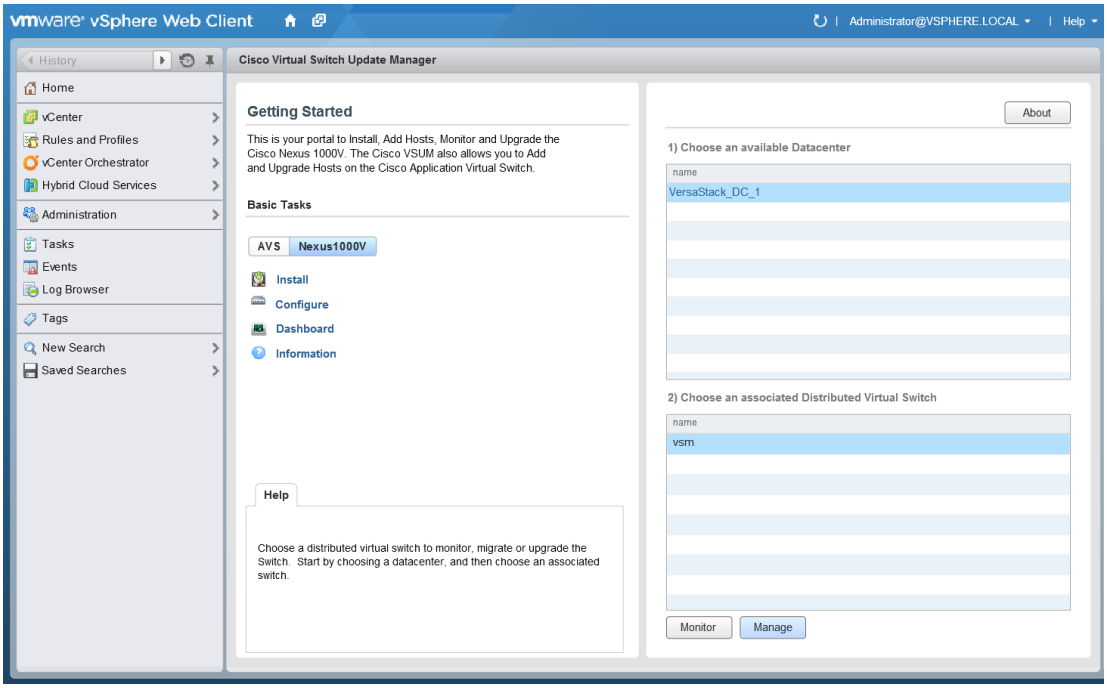
1. In the vSphere web client, click the Home tab and click the Cisco Virtual Switch Update Manager.



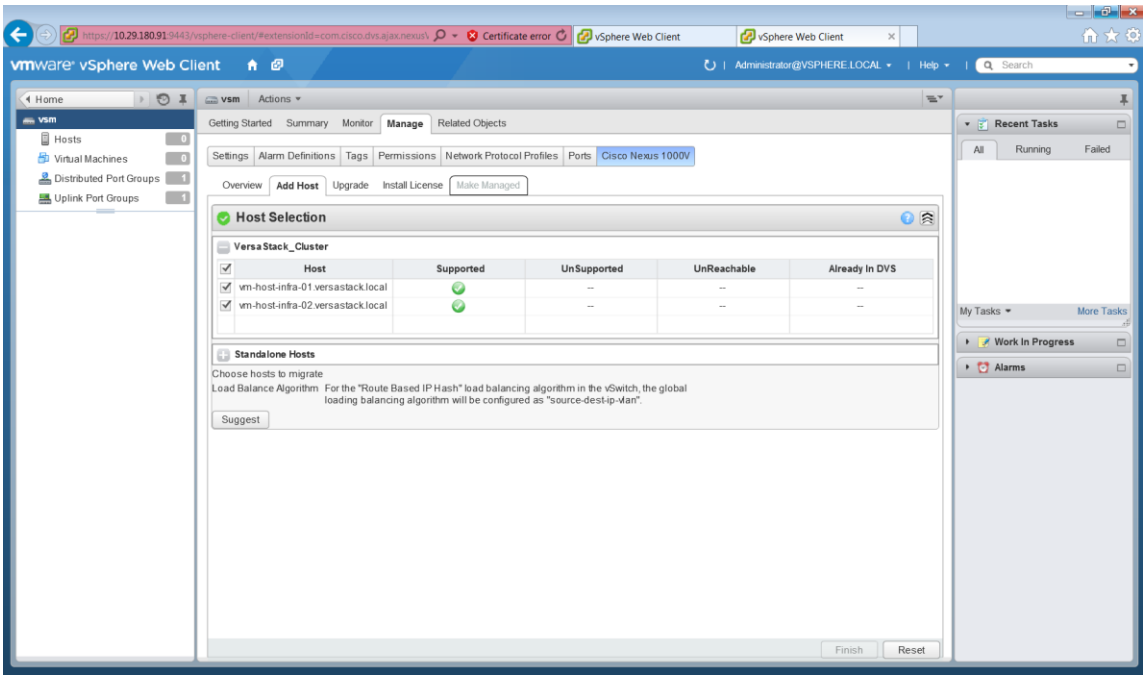
2. Click the Nexus 1000v and click Configure.



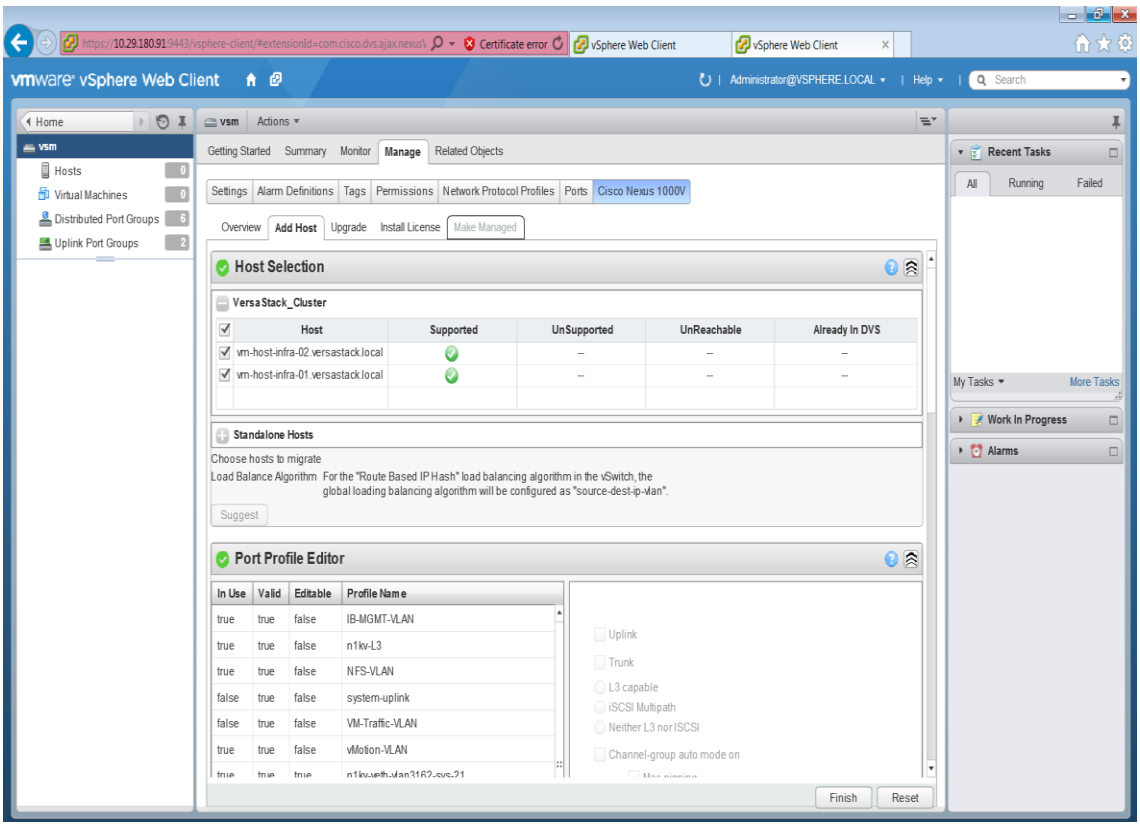
3. Click the Datacenter, then click Distributed Virtual Switch and select manage.



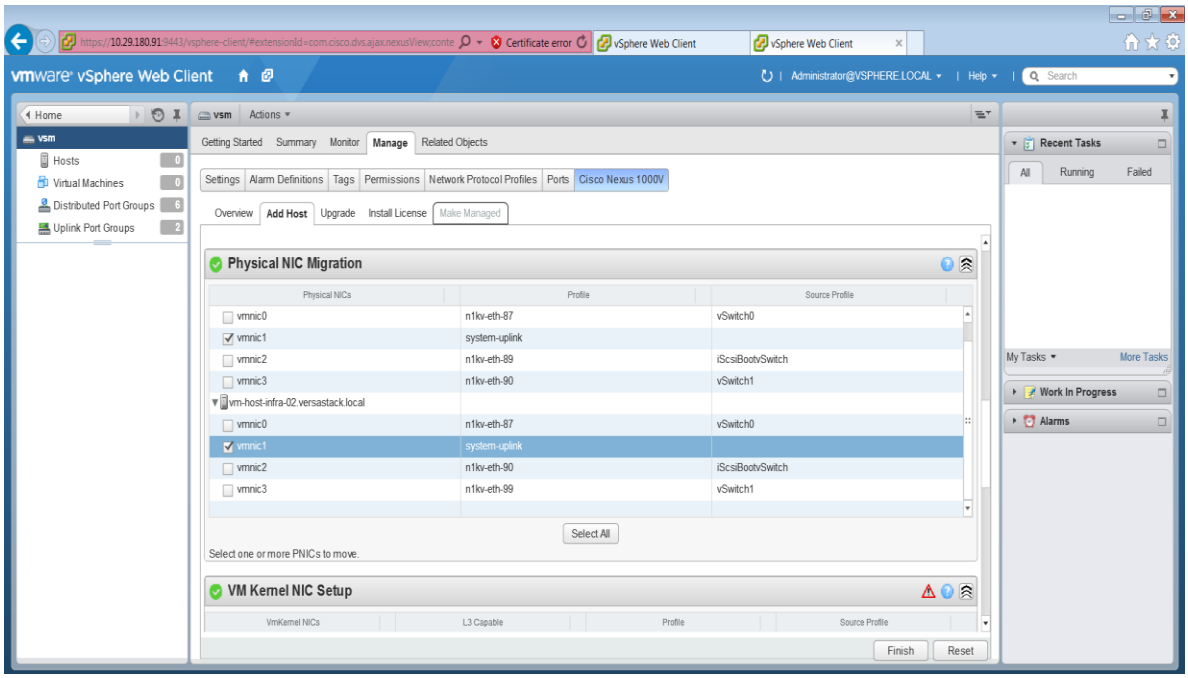
4. Click the Add Host tab then select the plus sign next to `Versastack_Cluster`, then click the top check box to both Hosts.



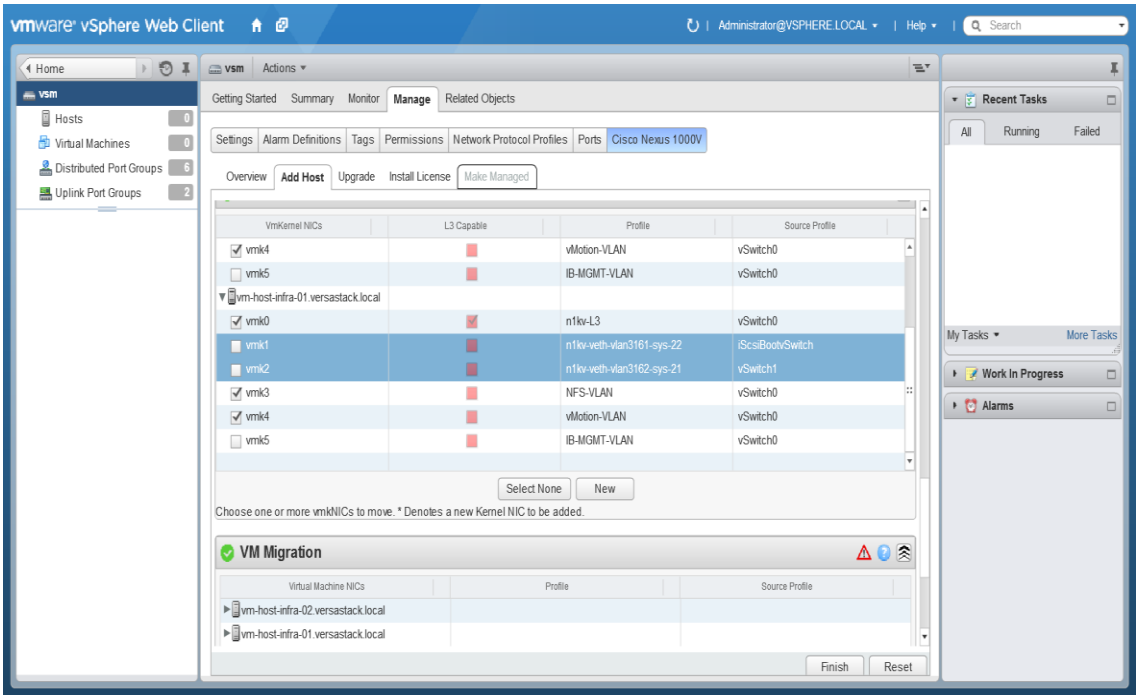
5. Click Suggest.



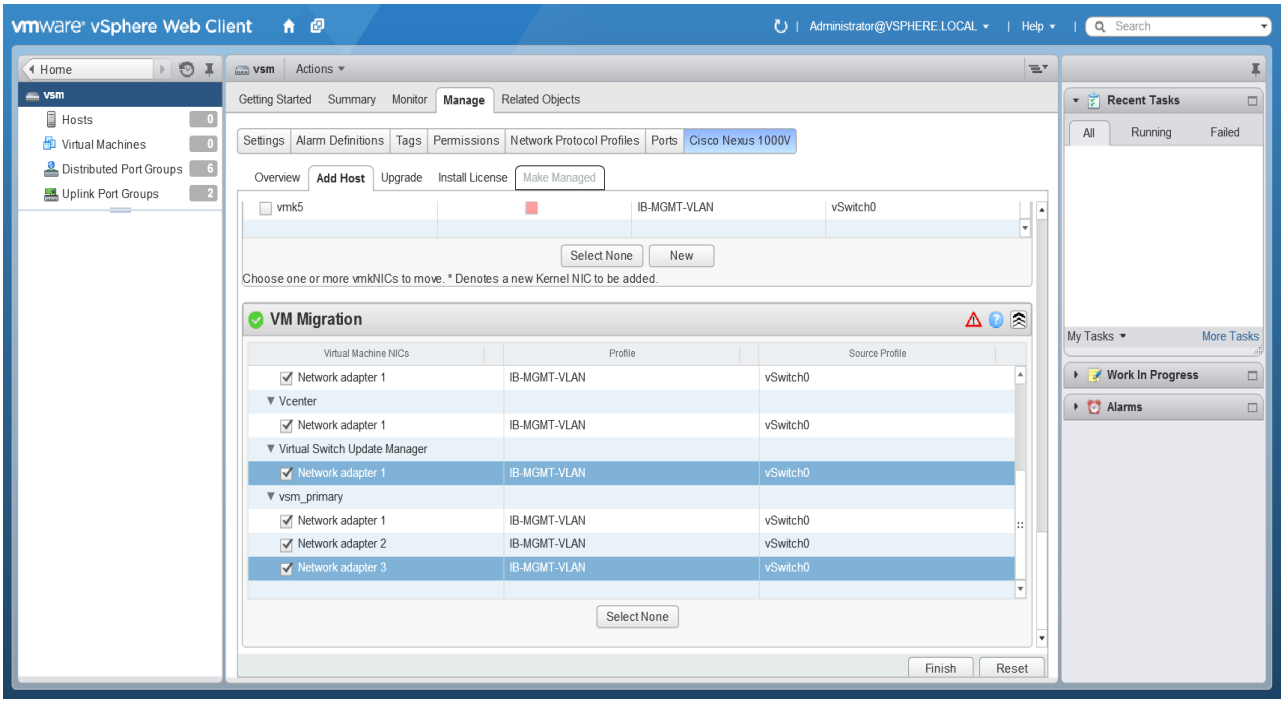
6. Select the Physical NIC Migration, and select the Unused Nic `vmnic1` for migration. Select system uplink in the middle pane. Deselect `vmnic0`. Repeat for the 2nd host



7. For the VM Kernel NIC Setup, deselect `vmk1`, `vmk2` used for iSCSI and vmk3, which is the temporary management kernel we created for this migration.

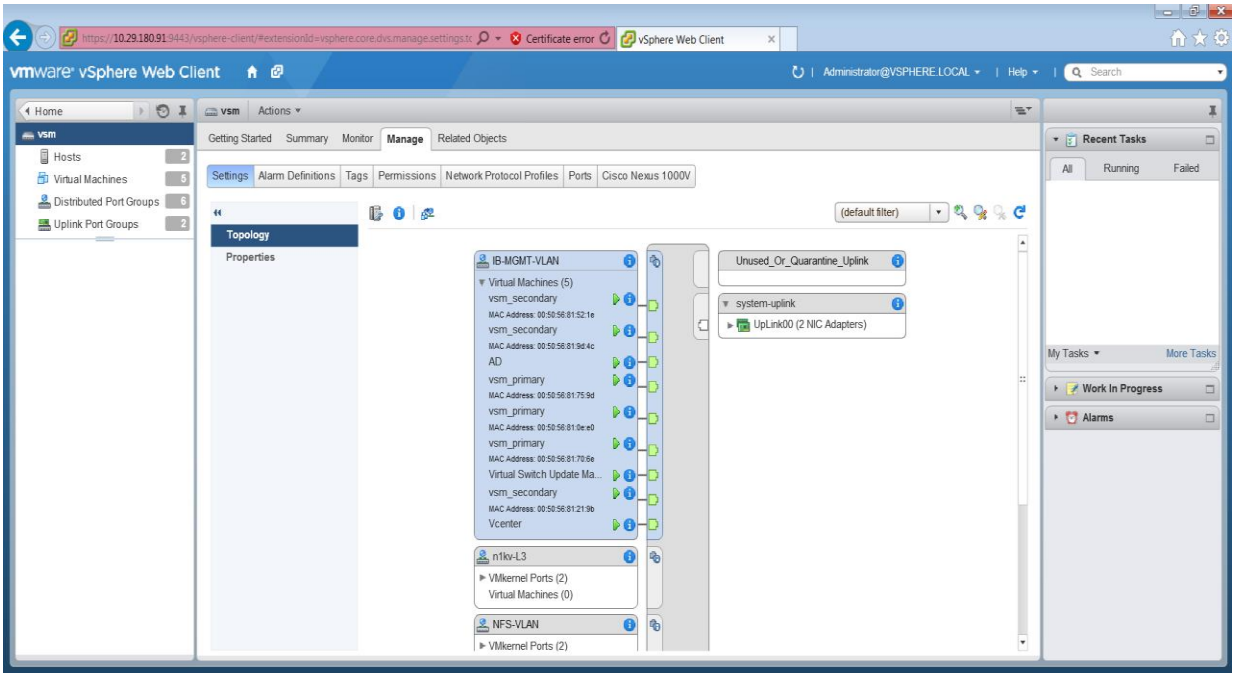


8. For VM migration click the button next to the virtual machine to expand the target profile and chose the correct profile that should be `IB-MGMT-VLAN`. Repeat this for each Virtual Machine.



9. Click Finish.

10. When the migration completes, click Settings then click Topology and expand the virtual machines to view the network connections.



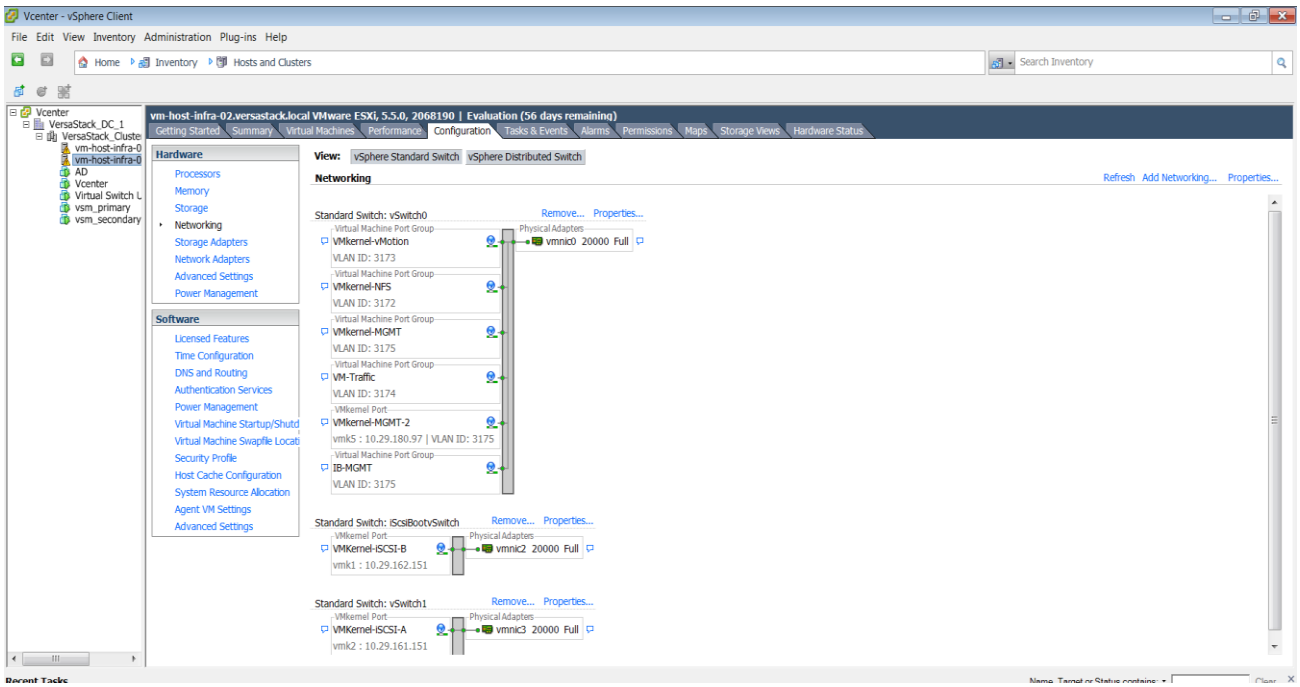
Remove the Networking Standard Switch Components for ESXi Hosts

In this section, the unused standard switch components will be removed and the second VIC will be assigned.

ESXi Host VM-Host-Infra-01

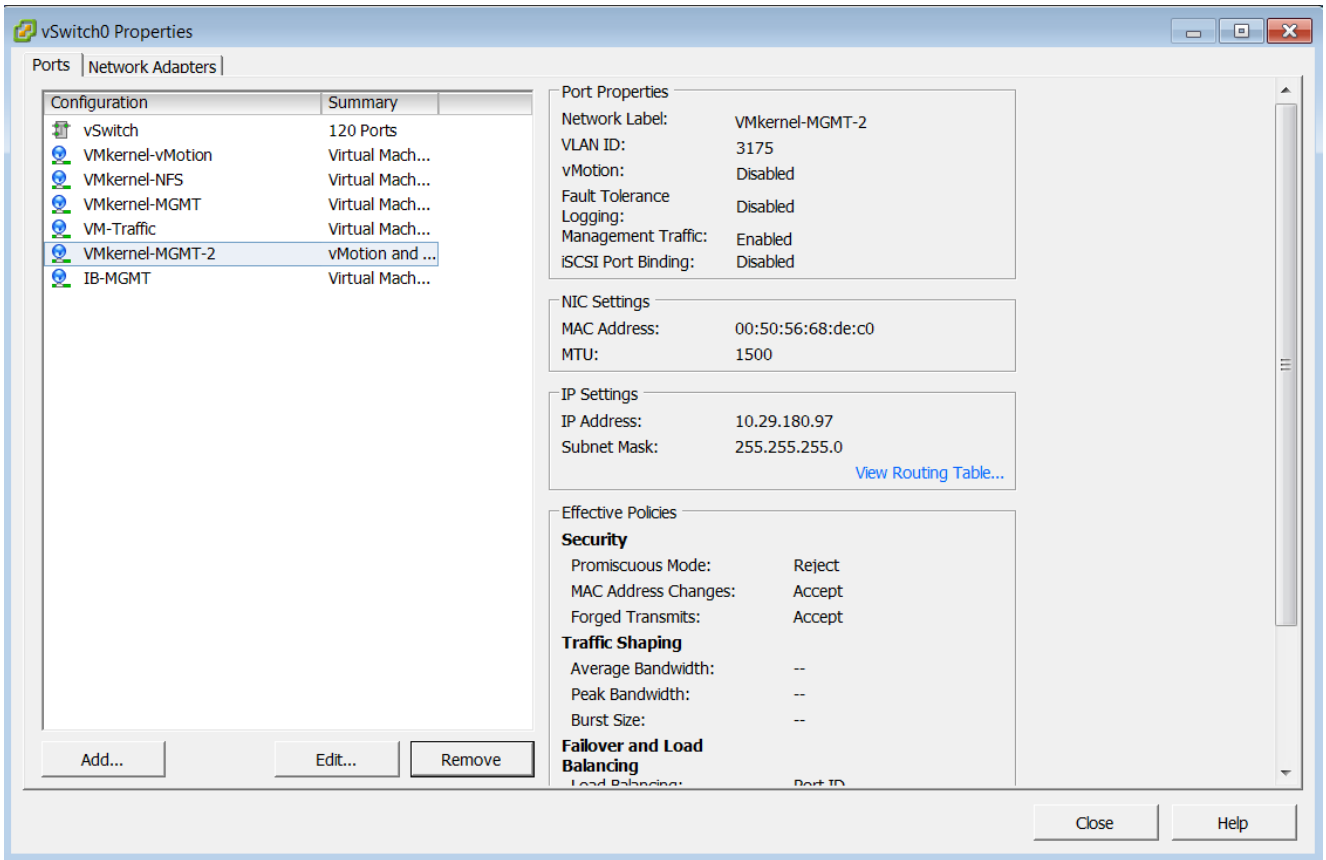
Repeat the steps in this section for all the ESXi Hosts.

1. From vSphere Client, select each host in the inventory.
2. Click the Configuration tab.
3. Click Networking.
4. Select the VSphere Standard switch, and then click Properties.



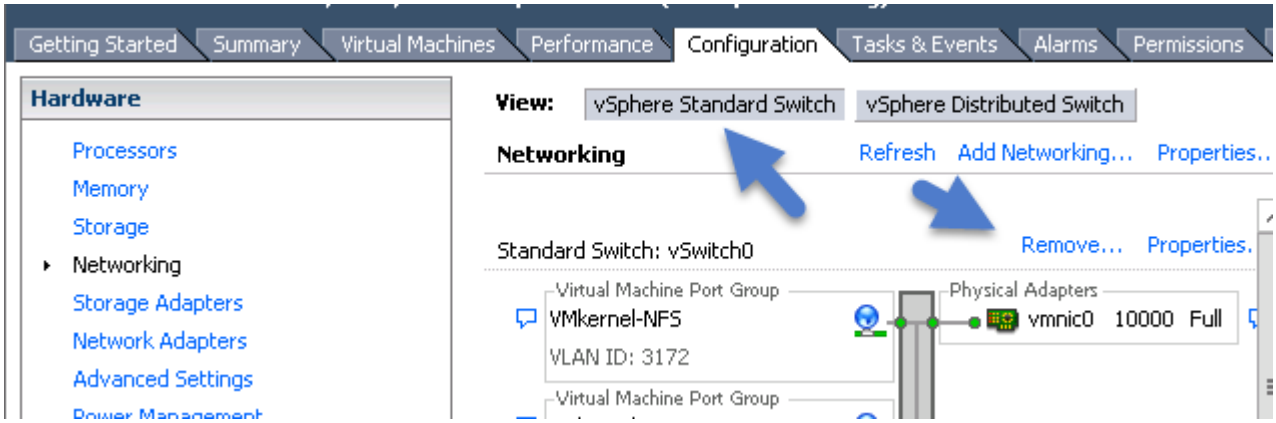
5. Click the temporary network `VMkernel-MGMT-2` created for the migration and click Remove.

6. Click Yes, then click Yes again.



7. Click Close.

8. Validate you still are focused on the VSphere standard switch `vSwitch0` and click Remove to remove this switch.



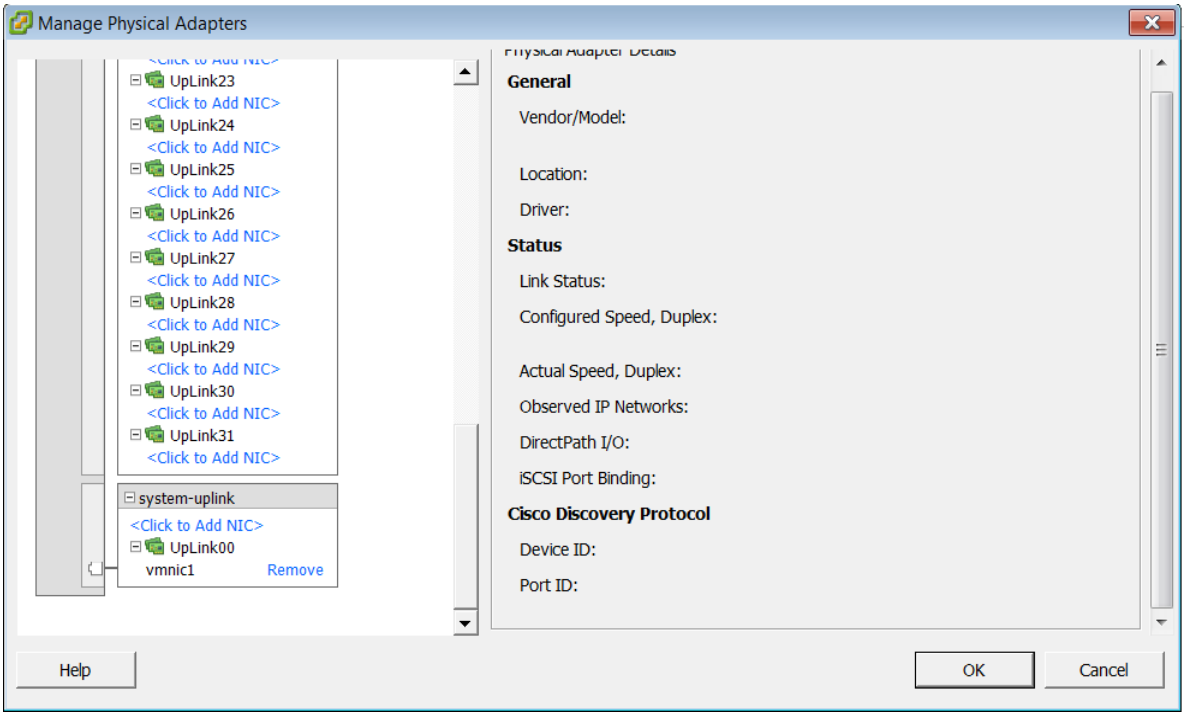
9. Click Yes to the warning popup.

10. After vSwitch0 has disappeared from the screen, click vSphere Distributed Switch at the top next to View.

11. Click Manage Physical Adapters.

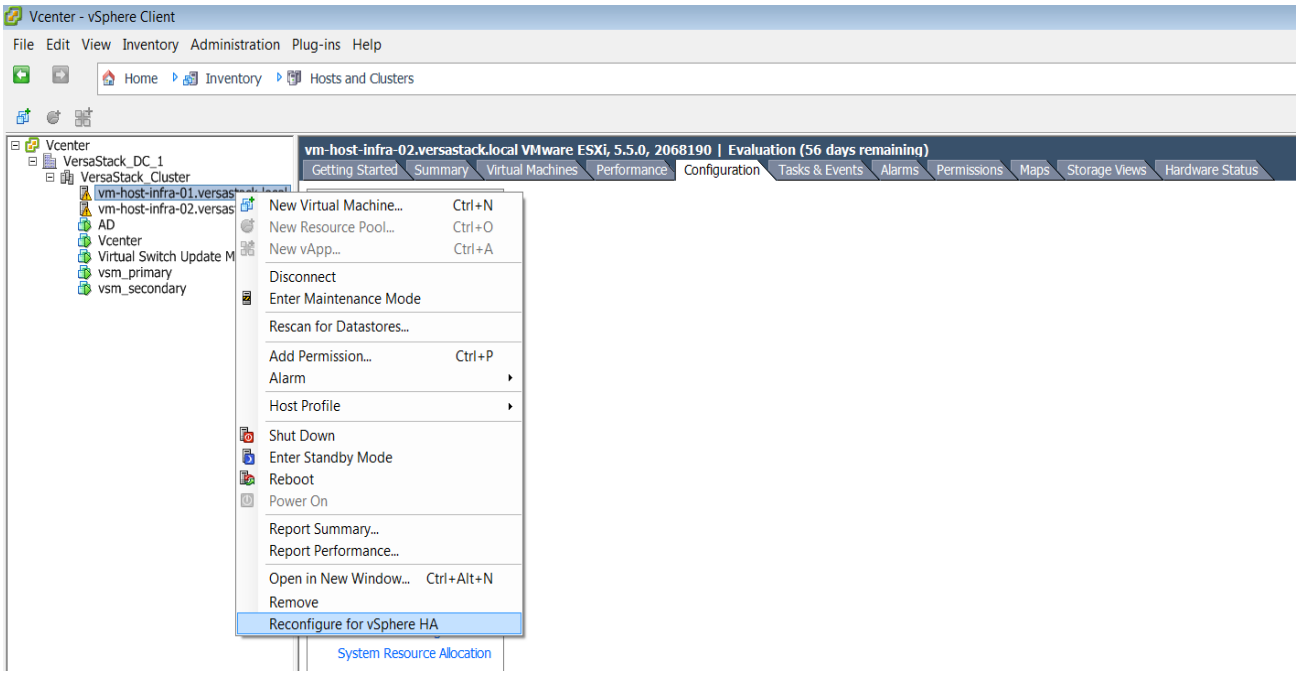
12. Scroll down to the system-uplink box and click Add NIC.

13. Choose `vmnic0` and click OK, then click OK again.



14. Validate there are no warnings for the ESX nodes. From each vSphere Client, select the Hosts and Clusters in the inventory section, click the Summary tab.

15. If there are warnings, right-click each node and click Reconfigure for vSphere HA.



Remove the Redundancy for the NIC in Cisco UCS Manager

While creating the ESXi vNIC template settings, the default was to enable hardware failover on the vNIC. When you have deployed the N1kV that setting is no longer required and should be disabled.

1. Launch UCS Manager and click the LAN tab.
2. Click Policies, root, vNIC templates.
3. Click `vNic_Template_A`, and on the General Tab uncheck enable failover.
4. Click Save Changes, then Yes, then ok.
5. Repeat action for `vNic_Template_B`.

Reboot the ESXi hosts to implement the change.

For more information about the 1000v switch, including how to update the software after installation, please visit the web site: http://www.cisco.com/c/en/us/products/switches/nexus-1000v-switch-vmware-vsphere/index.html

Backup Management and other Software

IBM Solutions

IBM is well known for management software. Added value to this solution can be obtained by installing IBM's Storage Management Console for VMware vCenter. Please visit the IBM website to obtain the latest version at http://www.ibm.com/us/en/.

For details about IBM backup and disaster recovery solutions, please refer to: http://www-03.ibm.com/systems/storage/solutions/backup-and-disaster-recovery/

Bill of Materials

Bill of Materials for VersaStack

Part Number	Product Description	Quantity Required
IBM Storwize V5000 Components		
2077-24C	IBM Storwize V5000 SFF Control	1
5305	5m Fiber Cable (LC)	8
9730	Power Cord - PDU connection	1
AGBS	Shipping and Handling NC	1
AC83	200GB 2.5 Inch Flash Drive	3
AC60	600GB 10K 2.5 Inch HDD	21
5639-CT7	IBM Storwize Family Software V5000 Controller V7.4	1
5639-CTA	Storwize Family Software V5000 Controller Maint (Reg/Ren): 1 Yr	1
2077-24E	IBM Storwize V5000 SFF Expansion	1
9730	Power Cord - PDU connection	1
ACTA	0.6m 12Gb SAS Cable(mSAS HD)	2
AGBT	Shipping and Handling 24F	1
AC60	600GB 10K 2.5 Inch HDD	24
5639-XT7	IBM Storwize Family Software V5000 Expansion	1
5639-XTA	Storwize Family Software V5000 Expansion Maint (Reg/Ren): 1 Yr	1
AC01 (AC06 MES)	10Gb iSCSI-FCoE Ports	2

Part Number	Product Description	Quantity Required
Cisco Nexus 9300 Switching Components		
N9K-C9372PX	Nexus 9300 with 48p 10G SFP+ and 6p 40G QSFP+	2
N3K-C3064-ACC-KIT	Nexus 9300 Accessory Kit	2
NXA-FAN-30CFM-F	Nexus 2K/3K/9K Single Fan, port side exhaust airflow	8
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	4
N9K-PAC-650W-B	Nexus 9300 650W AC PS, Port-side Exhaust	4
N9KDK9-612I3.1	Nexus 9500 or 9300 Base NX-OS Software Rel 6.1(2)I3(1)	2

Part Number	Product Description	Quantity Required
Cisco UCS Mini Chassis and FI		
UCS-SPL-MINI	UCS SP Select 5108 AC2 Chassis w/FI6324, UCS Central license	1
CAB-L520P-C19-US	NEMA L5-20 to IEC-C19 6ft US	4
UCS-CTR-LIC	UCS Central Per UCS Domain License (Physical)	1
N01-UAC1	Single phase AC power module for UCS 5108	1
N20-CAK	Accessory kit for UCS 5108 Blade Server Chassis	1

Part Number	Product Description	Quantity Required
N20-CBLKB1	Blade slot blanking panel for UCS 5108/single slot	8
N20-FAN5	Fan module for UCS 5108	8
N20-FW013	UCS Blade Server Chassis FW Package 3.0	1
UCSB-5108-PKG-HW	UCS 5108 Packaging for chassis with half width blades.	1
UCSB-PSU-2500ACDV	2500W Platinum AC Hot Plug Power Supply - DV	4
UCS-FI-M-6324	UCS 6324 In-Chassis FI with 4 UP, 1x40G Exp Port, 16 10Gb do	2
N10-MGT013	UCS Manager 3.0 for 6324	2

Part Number	Product Description	Quantity Required
Smart Play bundle Example for B200M4 blade (single server)		
UCS-SPL-B200M4-B1	UCS SP Select B200M4 Basic1 w/2xE52609 v3,4x16GB,VIC1340	1
CON-SNT-SPLB24B1	SNTC-8X5XNBD,UCS B200 M4 Smart Play SPL Server	1
UCS-CPU-E52609D	1.90 GHz E5-2609 v3/85W 6C/15MB Cache/DDR4 1600MHz	4
UCS-MR-1X162RU-A	16GB DDR4-2133-MHz	2

Part Number	Product Description	Quantity Required
	RDIMM/PC4-17000/dual rank/x4/1.2v	
UCSB-MLOM-40G-03	Cisco UCS VIC 1340 modular LOM for blade servers	1
UCSB-HS-EP-M4-F	CPU Heat Sink for UCS B200 M4/B420 M4 (Front)	1
UCSB-HS-EP-M4-R	CPU Heat Sink for UCS B200 M4/B420 M4 (Rear)	1

Part Number	Product Description	Quantity Required
Cisco UCS Rack Servers (2)		
UCSC-C220-M4S	UCS C220 M4 SFF w/o CPU, mem, HD, PCIe, PSU, rail kit	2
UCS-CPU-E52640D	2.60 GHz E5-2640 v3/90W 8C/20MB Cache/DDR4 1866MHz	4
UCS-MR-1X162RU-A	16GB DDR4-2133-MHz RDIMM/PC4-17000/dual rank/x4/1.2v	16
UCSC-MLOM-CSC-02	Cisco UCS VIC1227 VIC MLOM - Dual Port 10Gb SFP+	2
UCSC-CMAF-M4	Reversible CMA for C220 M4 friction & ball bearing rail kits	2
UCSC-RAILF-M4	Friction Rail Kit for C220 M4 rack servers	2
UCS-SD-32G-S	32GB SD Card for UCS servers	4
UCSC-PSU1-770W	770W AC Hot-Plug Power Supply for 1U C-Series Rack	4

Part Number	Product Description	Quantity Required
	Server	
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	4
N20-BBLKD	UCS 2.5 inch HDD blanking panel	16
UCSC-HS-C220M4	Heat sink for UCS C220 M4 rack servers	4
UCSC-MLOM-BLK	MLOM Blanking Panel	2

Appendix

Build Windows Active Directory Server VM(s)

ESXi Host VM-Host-Infra-01

To build an Active Directory Server virtual machine (VM) for the VM-Host-Infra-01 ESXi host, complete the following steps:

1. Log in to the host by using the VMware vSphere Client.
2. In the vSphere Client, select the host in the inventory pane.
3. Right-click the host and select New Virtual Machine.
4. Select Custom and click Next.
5. Enter a name for the VM. Click Next.
6. Select infra_datastore_1. Click Next.
7. Select Virtual Machine Version: 10. Click Next.
8. Verify that the Windows option and the Microsoft Windows Server 2008 R2 (64-bit) version are selected. Click Next.
9. Select two virtual sockets and one core per virtual socket. Click Next.
10. Select 4GB of memory. Click Next.
11. Select one network interface card (NIC).
12. For NIC 1, select the IB-MGMT Network option and the VMXNET 3 adapter. Click Next.
13. Keep the LSI Logic SAS option for the SCSI controller selected. Click Next.
14. Keep the Create a New Virtual Disk option selected. Click Next.
15. Make the disk size at least 60GB. Click Next.
16. Click Next.
17. Select the checkbox for Edit the Virtual Machine Settings Before Completion. Click Continue.
18. Click the Options tab.
19. Select Boot Options.
20. Select the Force BIOS Setup checkbox.

21. Click Finish.
22. From the left pane, expand the host field by clicking the plus sign (+).
23. Right-click the newly created AD Server VM and click Open Console.
24. Click the third button (green right arrow) to power on the VM.
25. Click the ninth button (CD with a wrench) to map the Windows Server 2008 R2 SP1 ISO, and then select Connect to ISO Image on Local Disk.
26. Navigate to the Windows Server 2008 R2 SP1 ISO, select it, and click Open.
27. Click in the BIOS Setup Utility window and use the right arrow key to navigate to the Boot menu. Use the down arrow key to select CD-ROM Drive. Press the plus (+) key twice to move CD-ROM Drive to the top of the list. Press F10 and Enter to save the selection and exit the BIOS Setup Utility.
28. The Windows Installer boots. Select the appropriate language, time and currency format, and keyboard. Click Next.
29. Click Install now.
30. Make sure that the Windows Server 2008 R2 Standard (Full Installation) option is selected. Click Next.
31. Read and accept the license terms and click Next.
32. Select Custom (Advanced). Make sure that Disk 0 Unallocated Space is selected. Click Next to allow the Windows installation to complete.
33. After the Windows installation is complete and the VM has rebooted, click OK to set the Administrator password.
34. Enter and confirm the Administrator password and click the blue arrow to log in. Click OK to confirm the password change.
35. After logging in to the VM desktop, from the VM console window, select the VM menu. Under Guest, select Install/Upgrade VMware Tools. Click OK.
36. If prompted to eject the Windows installation media before running the setup for the VMware tools, click OK, then click OK.
37. In the dialog box, select Run setup64.exe.
38. In the VMware Tools installer window, click Next.
39. Make sure that Typical is selected and click Next.
40. Click Install. 41. Click Finish.
41. Click Yes to restart the VM.

42. After the reboot is complete, select the VM menu. Under Guest, select Send Ctrl+Alt+Del. Then enter the password to log in to the VM.

43. Set the time zone for the VM, IP address, gateway, and host name.

A reboot is required.

44. If necessary, activate Windows.

45. Download and install all required Windows updates.

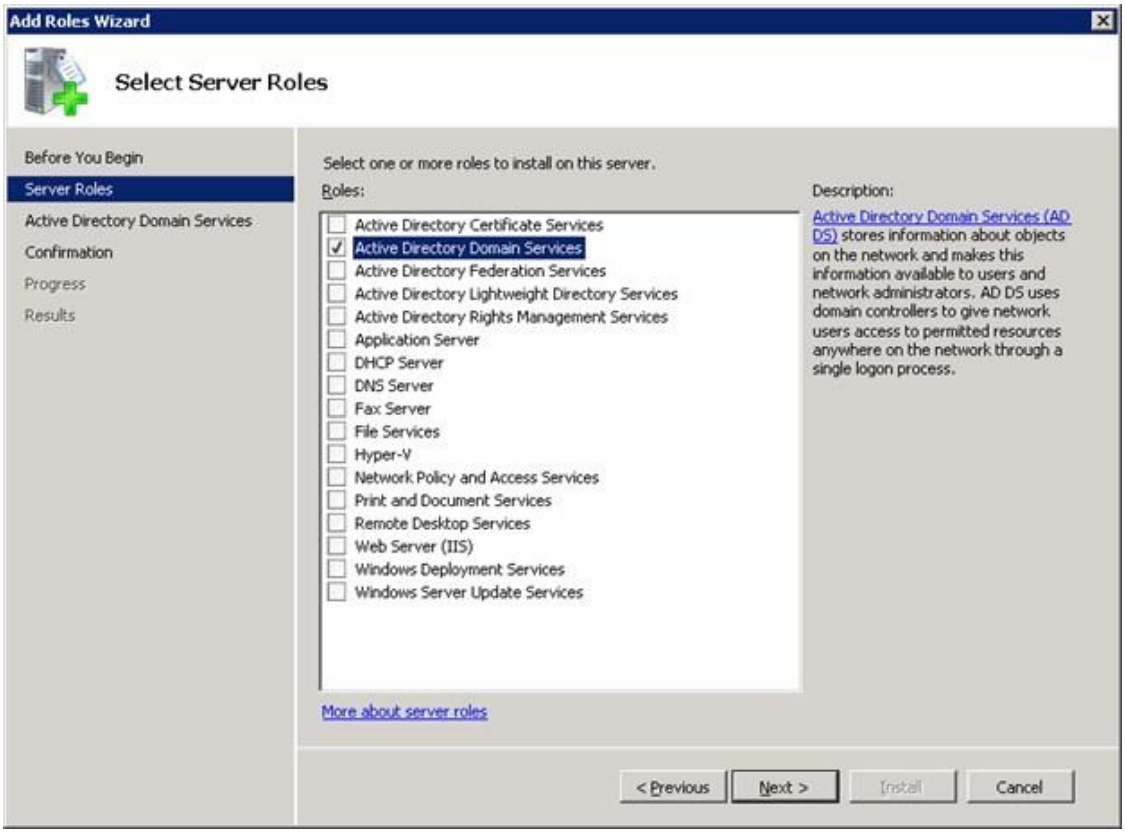
This process requires several reboots.

46. Open Server Manager.

47. On the left, click Roles, the select Add Roles on the right.

48. Click Next.

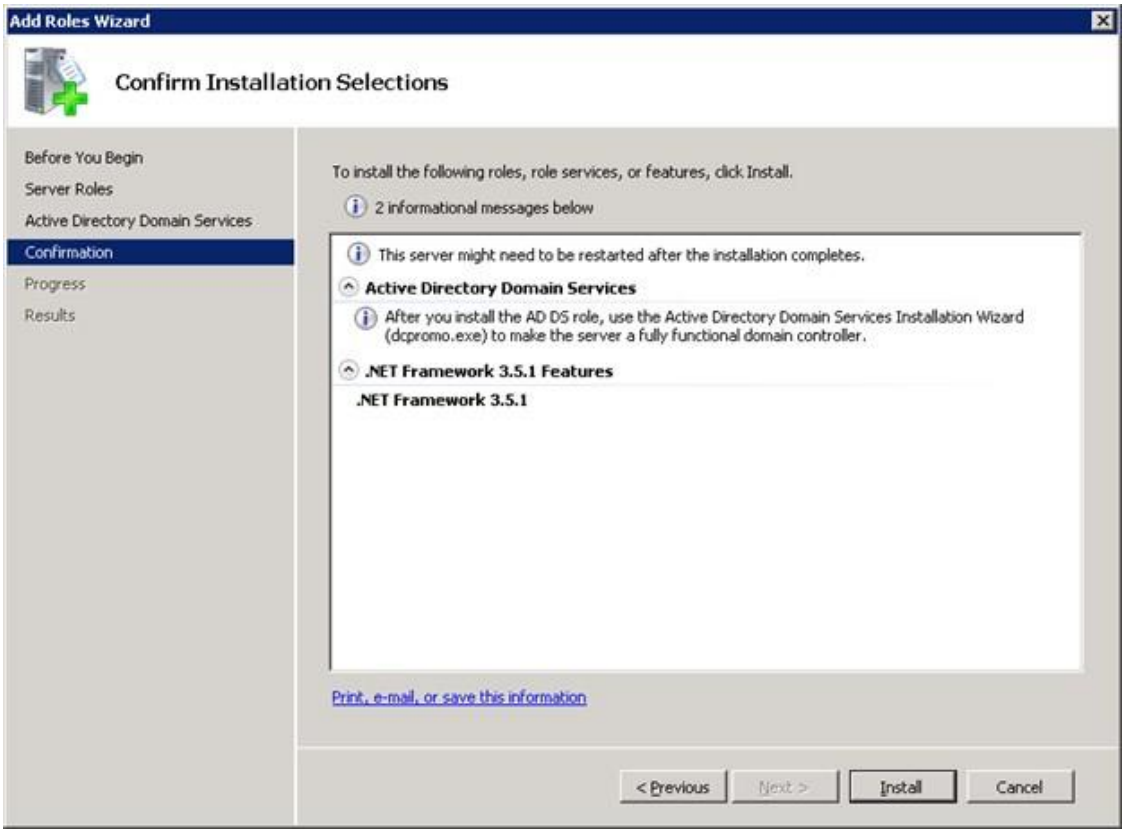
49. In the list, select the checkbox next to Active Directory Domain Services. 51. In the popup, click Add Required Features to add .NET Framework 3.5.1.

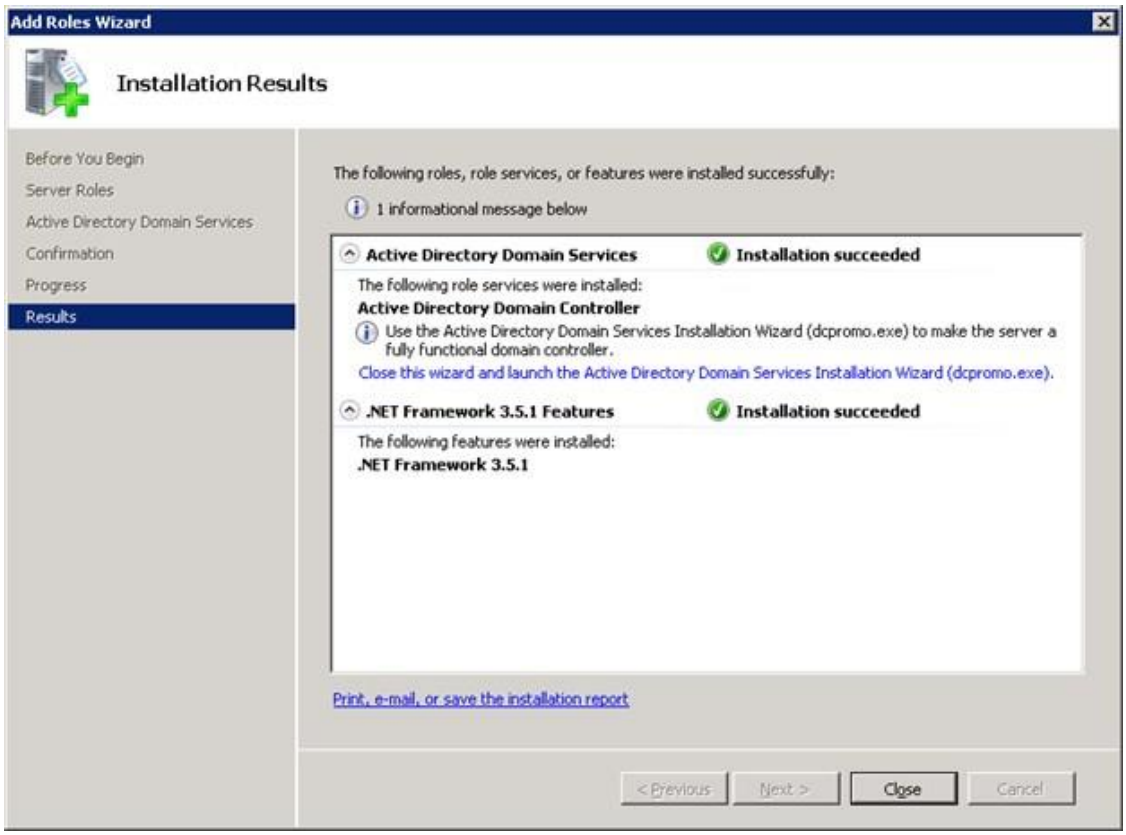


50. Click Next.

51. Click Next.

52. Click Install.



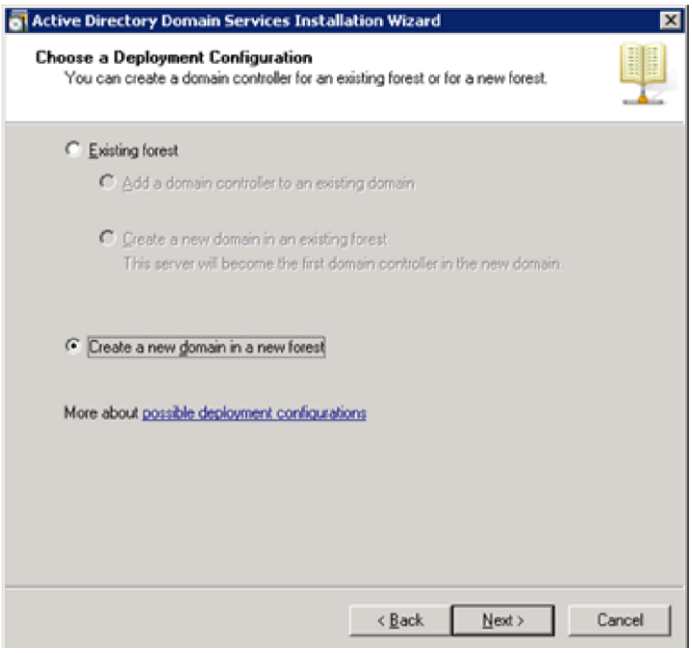


53. In the middle of the window, click Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe).

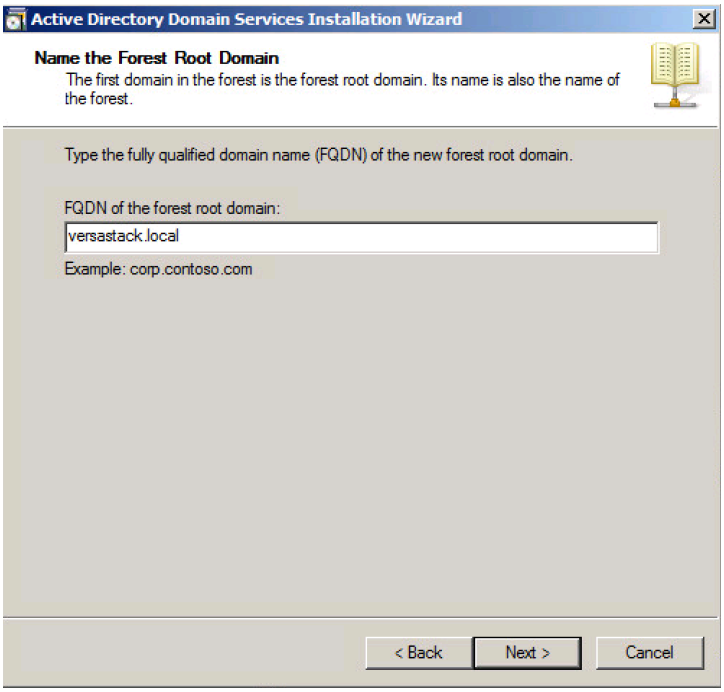
54. In the Active Directory Domain Services Installation Wizard, click Next.

55. Click Next.

56. Select "Create a new domain in a new forest" and click Next.

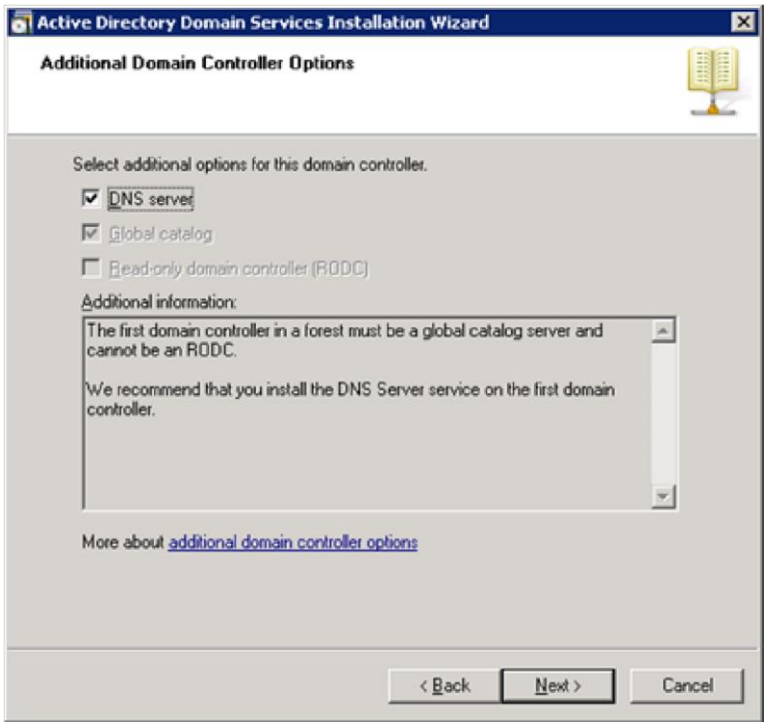


57. Type the FQDN of the Windows domain for this VersaStack and click Next.



58. Select the appropriate forest functional level and click Next.

59. Keep DNS server selected and click Next.



60. If one or more DNS servers exist that this domain can resolve from, select Yes to create a DNS delegation. If this AD server is being created on an isolated network, select No, to not create a DNS delegation. The remaining steps in this procedure assume a DNS delegation is not created. Click Next.

61. Click Next to accept the default locations for database and log files.

62. Enter and confirm `<<var_password>>` for the Directory Services Restore Mode Administrator Password. Click Next.

63. Review the Summary information and click Next. Active Directory Domain Services will install.

64. Click Finish.

65. Click Restart Now to restart the AD Server.

66. After the machine has rebooted, log in as the domain Administrator.

67. Open the DNS Manager by clicking Start > Administrative Tools > DNS.

68. Optional: Add Reverse Lookup Zones for your IP address ranges.

69. Expand the Server and Forward Lookup Zones. Select the zone for the domain. Right-click and select New Host (A or AAAA). Populate the DNS Server with Host Records for all components in the VersaStack.

70. Optional: Build a second AD server VM. Add this server to the newly created Windows Domain and activate Windows. Install Active Directory Domain Services on this machine. Launch dcpromo.exe at

the end of this installation. Choose to add a domain controller to a domain in an existing forest. Add this domain controller to the domain created earlier. Complete the installation of this second domain controller. After vCenter Server is installed, affinity rules can be created to keep the two AD servers running on different hosts.

Cisco Nexus 9000 Example Configurations

Cisco Nexus 9000 A

```
sh runn

!Command: show running-config
!Time: Fri Oct 23 17:58:26 2015

version 6.1(2)I3(4b)
switchname VersaStack5k_9k_A
vdc VersaStack5k_9k_A id 1
  allocate interface Ethernet1/1-54
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 512
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

feature telnet
cfs eth distribute
feature udld
feature interface-vlan
feature lacp
feature vpc

no password strength-check
```

```
username admin password 5 $1$aEhPgXYN$oob3ytHhNVWCN0M7lnL4G.  role network-
admin

ip domain-lookup

no service unsupported-transceiver

copp profile strict

snmp-server user admin network-admin auth md5
0xa21083b369a8dd2c6c6673fac417652d priv 0xa21083b369a8dd2c6c6673fac417652d
localizedkey

rmon event 1 log trap public description FATAL(1) owner PMON@FATAL

rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL

rmon event 3 log trap public description ERROR(3) owner PMON@ERROR

rmon event 4 log trap public description WARNING(4) owner PMON@WARNING

rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO


vlan 1-2,3161-3162,3172-3175

vlan 2

  name Native-VLAN

vlan 3161

  name iSCSI-A-VLAN

vlan 3162

  name iSCSI-B-VLAN

vlan 3172

  name NFS-VLAN

vlan 3173

  name vMotion-VLAN

vlan 3174

  name VM-Traffic-VLAN

vlan 3175

  name IB-MGMT-VLAN


spanning-tree port type edge bpduguard default

spanning-tree port type edge bpdufilter default

spanning-tree port type network default

vrf context management

  ip route 0.0.0.0/0 10.29.180.1
```

```
vpc domain 10
  peer-switch
  role priority 10
  peer-keepalive destination 10.29.180.52 source 10.29.180.51
  delay restore 150
  peer-gateway
  auto-recovery
  ip arp synchronize


interface Vlan1

interface Vlan3175
  no shutdown
  no ip redirects
  ip address 10.29.180.99/24
  no ipv6 redirects

interface port-channel10
  description vPC peer-link
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3161-3162,3172-3175
  spanning-tree port type network
  vpc peer-link

interface port-channel13
  description UCS_VersaStack_5k-A
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3161-3162,3172-3175
  spanning-tree port type edge trunk
  mtu 9216
```

```
  vpc 13

interface port-channel14
  description UCS_VersaStack_5k-B
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3161-3162,3172-3175
  spanning-tree port type edge trunk
  mtu 9216
  vpc 14

interface Ethernet1/1
  description V5000_Node1_E3_iSCSI
  switchport access vlan 3161
  spanning-tree port type normal
  speed 10000
  mtu 9216

interface Ethernet1/2
  description V5000_Node2_E3_iSCSI
  switchport access vlan 3161
  spanning-tree port type normal
  speed 10000
  mtu 9216

interface Ethernet1/3
  description UCS_VersaStack_5k-A:1/3
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3161-3162,3172-3175
  mtu 9216
  channel-group 13 mode active
```

```
interface Ethernet1/4
  description UCS_VersaStack_5k-B:1/3
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3161-3162,3172-3175
  mtu 9216
  channel-group 14 mode active

interface Ethernet1/5

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17
```

```
interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface Ethernet1/33
```

```
interface Ethernet1/34

interface Ethernet1/35

interface Ethernet1/36
  description IB-management-access
  switchport access vlan 3175
  spanning-tree port type network

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40

interface Ethernet1/41

interface Ethernet1/42

interface Ethernet1/43

interface Ethernet1/44

interface Ethernet1/45

interface Ethernet1/46

interface Ethernet1/47
  description VPC Peer VersaStack5k_9k_B:1/47
  switchport mode trunk
  switchport trunk native vlan 2
```

```
  switchport trunk allowed vlan 3161-3162,3172-3175
  channel-group 10 mode active

interface Ethernet1/48
  description VPC Peer VersaStack5k_9k_B:1/48
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3161-3162,3172-3175
  channel-group 10 mode active

interface Ethernet1/49

interface Ethernet1/50

interface Ethernet1/51

interface Ethernet1/52

interface Ethernet1/53

interface Ethernet1/54

interface mgmt0
  vrf member management
  ip address 10.29.180.51/24
line console
line vty
boot nxos bootflash:/n9000-dk9.6.1.2.I3.4b.bin
```

Cisco Nexus 9000 B

```
sh runn
```

```
!Command: show running-config
!Time: Fri Oct 23 17:57:27 2015

version 6.1(2)I3(4b)
switchname VersaStack5k_9k_B
vdc VersaStack5k_9k_B id 1
  allocate interface Ethernet1/1-54
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 512
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

feature telnet
cfs eth distribute
feature udld
feature interface-vlan
feature lacp
feature vpc

no password strength-check
username admin password 5 $1$Qi9pTwWv$/FR8rmAxCodsX92Z.NErf.  role network-
admin
ip domain-lookup
no service unsupported-transceiver
copp profile strict
snmp-server user admin network-admin auth md5
0x4d6994e49b563879120697a8255e41df priv 0x4d6994e49b563879120697a8255e41df
localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
```

```
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO

vlan 1-2,3161-3162,3172-3175
vlan 2
  name Native-VLAN
vlan 3161
  name iSCSI-A-VLAN
vlan 3162
  name iSCSI-B-VLAN
vlan 3172
  name NFS-VLAN
vlan 3173
  name vMotion-VLAN
vlan 3174
  name VM-Traffic-VLAN
vlan 3175
  name IB-MGMT-VLAN

spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
spanning-tree port type network default
vrf context management
  ip route 0.0.0.0/0 10.29.180.1
vpc domain 10
  peer-switch
  role priority 20
  peer-keepalive destination 10.29.180.51 source 10.29.180.52
  delay restore 150
  peer-gateway
  auto-recovery
  ip arp synchronize
```

```
interface Vlan1

interface Vlan3175
  no shutdown
  no ip redirects
  ip address 10.29.180.100/24
  no ipv6 redirects

interface port-channel10
  description vPC peer-link
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3161-3162,3172-3175
  spanning-tree port type network
  vpc peer-link

interface port-channel13
  description UCS_VersaStack_5k-A
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3161-3162,3172-3175
  spanning-tree port type edge trunk
  mtu 9216
  vpc 13

interface port-channel14
  description UCS_VersaStack_5k-B
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3161-3162,3172-3175
  spanning-tree port type edge trunk
  mtu 9216
  vpc 14
```

```
interface Ethernet1/1
  description V5000_Node1_E4_iSCSI
  switchport access vlan 3162
  spanning-tree port type normal
  speed 10000
  mtu 9216

interface Ethernet1/2
  description V5000_Node2_E4_iSCSI
  switchport access vlan 3162
  spanning-tree port type normal
  speed 10000
  mtu 9216

interface Ethernet1/3
  description UCS_VersaStack_5k-A:1/4
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3161-3162,3172-3175
  mtu 9216
  channel-group 13 mode active

interface Ethernet1/4
  description UCS_VersaStack_5k-B:1/4
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3161-3162,3172-3175
  mtu 9216
  channel-group 14 mode active

interface Ethernet1/5
```

```
interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22
```

```
interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface Ethernet1/33

interface Ethernet1/34

interface Ethernet1/35

interface Ethernet1/36
  description IB-management-access
  switchport access vlan 3175
  spanning-tree port type network

interface Ethernet1/37
```

```
interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40

interface Ethernet1/41

interface Ethernet1/42

interface Ethernet1/43

interface Ethernet1/44

interface Ethernet1/45

interface Ethernet1/46

interface Ethernet1/47
  description VPC Peer VersaStack5k_9k_A:1/47
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3161-3162,3172-3175
  channel-group 10 mode active

interface Ethernet1/48
  description VPC Peer VersaStack5k_9k_A:1/48
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3161-3162,3172-3175
  channel-group 10 mode active
```

```
interface Ethernet1/49

interface Ethernet1/50

interface Ethernet1/51

interface Ethernet1/52

interface Ethernet1/53

interface Ethernet1/54

interface mgmt0
  vrf member management
  ip address 10.29.180.52/24
line console
line vty
boot nxos bootflash:/n9000-dk9.6.1.2.I3.4b.bin
```

About the Authors

Sreenivasa Edula, Technical Marketing Engineer, UCS Data Center Solutions Engineering, Cisco Systems, Inc.

Sreeni has over 17 years of experience in Information Systems with expertise across Cisco Data Center technology portfolio, including DC architecture design, virtualization, compute, network, storage and cloud computing.

Adam Reid, Test Specialist, Systems and Technology Group, IBM

Adam has more than 15 years of Computer Engineering experience. Focused more recently on IBM's Storwize Storage Systems, he's been deeply involved with VMware and the testing and configuration of virtualized environments pivotal to the future of software defined storage. Adam has designed and tested validated systems to meet the demands of a wide range of mid-range and enterprise environments.

Acknowledgments

The authors would like to acknowledge the following for their support and contribution to the design, validation and creation of this Cisco Validated Design (CVD):

- Asher Pemberton - Test Specialist, Systems and Technology Group, IBM
- Chris O'Brien - Manager, Technical Marketing Team, Cisco Systems, Inc.
- Jeff Fultz - Technical Marketing Engineer, UCS Data Center Solutions Engineering, Cisco Systems, Inc.