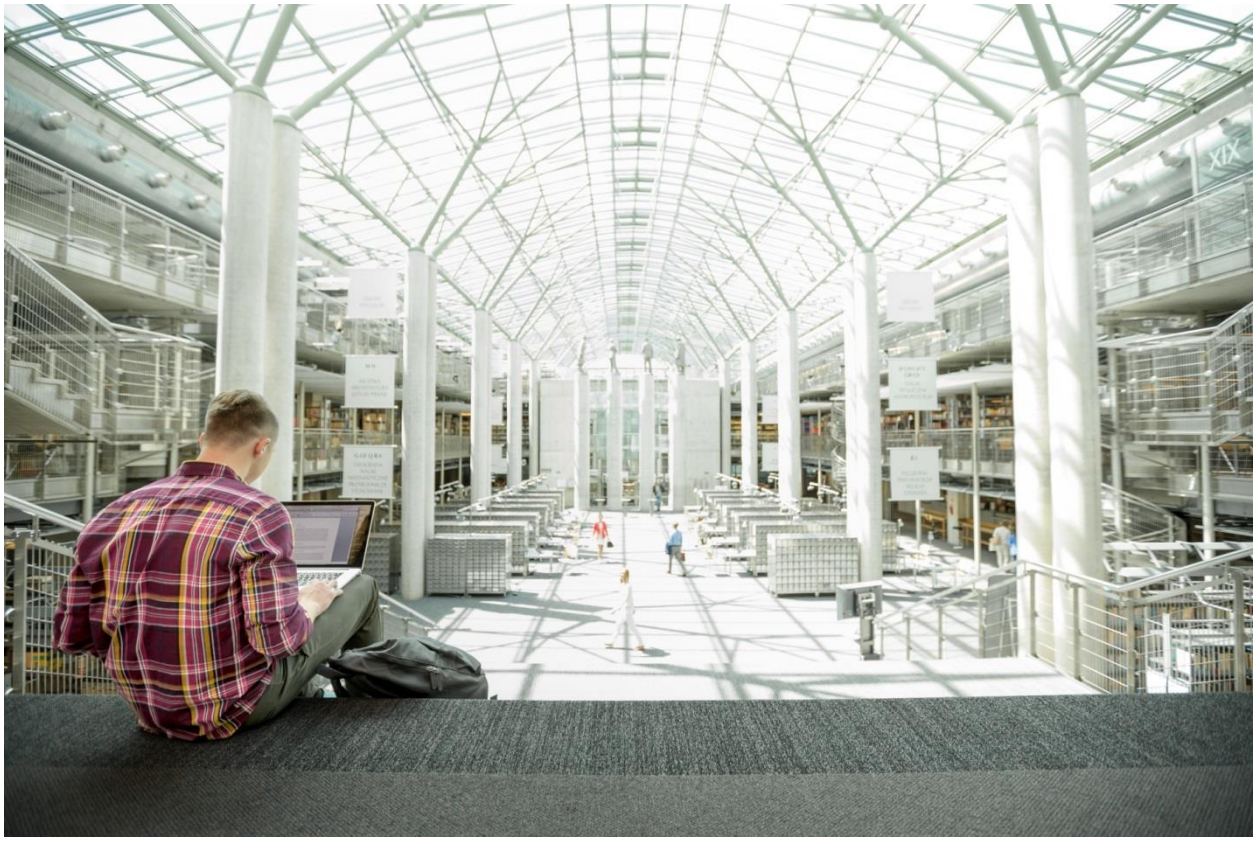


VersaStack for Data Center with All-Flash Storage and VMware vSphere 6.0

Deploying Cisco Unified Computing System 3.1 and IBM FlashSystem V9000 with VMware vSphere 6.0 Update 1a

Last Updated: April 26, 2016

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 V9000 storage and Cisco UCS infrastructure for a successful VMware deployment. As an example, this solution could be deployed by enterprises to support their environments needing extreme performance in the datacenter. For design guidance on which VersaStack solution best suites your requirements, please refer to the design zone information for VersaStack later in this document.

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

- In a recent poll, 73% of all IT spending was used just to keep the current data center running; amounting in increased Opex
- Rapid storage growth resulting in expensive and complex storage management
- Underutilized compute and storage resources
- IT groups are challenged to meet SLA's, dealing with complex troubleshooting
- IT groups are beset with time consuming data migrations to manage growth and change

To overcome these issues and increase efficiency, IT departments are moving towards converged infrastructure solutions. These solutions offer many benefits, some of which are having the integration testing completed along with thoroughly documented deployment procedures. They also offer increased feature sets and premium support with a single point of contact. Cisco and IBM have team up to bring the best networking, compute and storage in a single solution named VersaStack. VersaStack offers customer's versatility, simplicity and great performance along with reliability. In this document we will show how to install an All-Flash VersaStack setup for a VMware infrastructure that is designed to increase IOPS and provide best performance for IO intensive applications. 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 UCS Service Profiles designed to vastly reduce deployment time and provide consistency in the datacenter
- Cisco Fabric Interconnects to reduce infrastructure costs and simplify networking
- IBM Real-time compression to reduce the storage footprint and storage costs
- IBM Data-at-rest Encryption to provide Enterprise reliability
- Optional IBM Easy Tier to automate optimizing performance while lowering storage costs by automatically placing infrequently accessed data on cheaper disks, and highly accessed data on faster tiers thereby reducing costly migrations
- IBM's FlashSystem V9000 Simplified Storage Management designed to simplify day to day storage tasks

VersaStack offers customers the ability to reduce OPEX while at the same time helping meet their SLA's by simplifying many of the day to day IT tasks, as well as consolidating and automating others.

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 FlashSystem V9000 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 FlashSystem V9000.

What's New?

The following design elements distinguish this version of VersaStack from previous models:

- Support for the Cisco UCS 3.1(1e) release and Cisco UCS B200-M4 servers
- Support for the latest release of IBM FlashSystem V9000 software 7.6.0.4
- VMware vSphere 6.0 U1a
- Validation of the Cisco Nexus 9000 switches including an IBM FlashSystem V9000 storage array with 16G Host connectivity
- Validation of Cisco MDS 9148S Switches with 16G ports

For more information on previous VersaStack models, please refer the VersaStack guides at:

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

Solution Design and Architecture

Architecture

The VersaStack architecture is highly modular or "Pod-like". There are sufficient architectural flexibility 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 is a defined set of hardware and software that serves as an integrated foundation for both virtualized and non-virtualized solutions. VersaStack All-Flash includes IBM FlashSystem V9000, Cisco networking, the Cisco Unified Computing System™ (Cisco UCS®), Cisco MDS fiber-channel switches and VMware vSphere software in a single package. The design is flexible enough that the networking, computing, and storage can fit in one data center rack or be deployed according to a customer's data center design. Port density enables the networking components to accommodate multiple configurations.

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

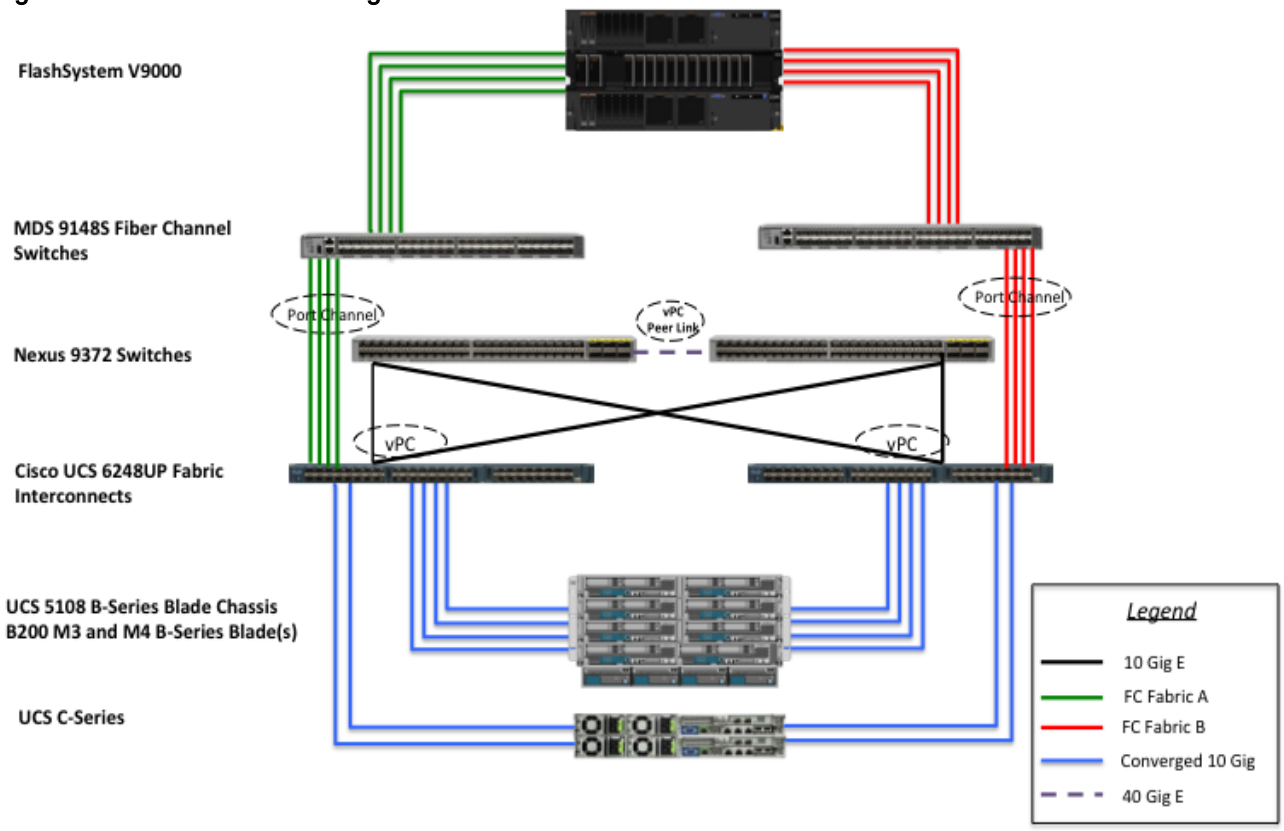
This architecture references relevant criteria pertaining to resiliency, cost benefit, and ease of deployment of all components including IBM FlashSystem V9000 storage.

Figure 1 illustrates the VMware vSphere built on VersaStack components and the network connections for a configuration with IBM FlashSystem V9000 Storage. This design uses the Cisco Nexus® 9372, and Cisco UCS B-Series with the Cisco UCS virtual interface card (VIC) and the IBM FlashSystem V9000 storage controllers connected in a highly available design using Cisco Virtual Port Channels (vPCs). This infrastructure is deployed to provide FC-booted hosts with block-level access to shared storage datastores.

Common infrastructure services such as Active Directory, DNS, DHCP, vCenter, Cisco Nexus 1000v virtual supervisor module (VSM), Cisco UCS Performance Manager etc can be deployed on a redundant and self-contained hardware in a Common Infrastructure Pod along with the VersaStack Pod. 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.

This document details the implementation and deployment of VersaStack Pod and does not cover the implementation of the Common Infrastructure Pod.

Figure 1 VersaStack Cabling Overview



The reference hardware configuration includes:

- Two Cisco Nexus 9396 or 9372 switches
- Two Cisco UCS 6248UP Fabric Interconnects
- Two Cisco MDS 9148S Fibre-Channel switches
- Support for 32 Cisco UCS C-Series servers without any additional networking components
- Support for 8 Cisco UCS B-Series servers without any additional blade server chassis
- Support for up to 160 Cisco UCS C-Series and B-Series servers by way of additional fabric extenders and blade server chassis
- Two IBM FlashSystem V9000 control enclosures and one V9000 Storage enclosure. Support for up to 12 flash modules of the same capacity within storage enclosures.

For server virtualization, the deployment includes VMware vSphere. Although this is the base design, each of the components can be scaled easily to support specific business requirements. For example, more (or different) servers or even blade chassis can be deployed to increase compute capacity, additional V9000 Storage Enclosures to increase capacity, and pairs of V9000 Control Enclosures shelves can be deployed to improve I/O capability and throughput, and special hardware or software features can be added to introduce new features and functionality.

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 detailed 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 command "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 Software Revisions

Layer	Device	Image	Comments
Compute	Cisco UCS Fabric Interconnects 6200 Series Switches	3.1(1e)	Embedded management
	Cisco UCS C 220 M3/M4 Server	3.1(1e)	Software bundle release
	Cisco UCS B 200 M3/ M4 Server	3.1(1e)	Software bundle release
	Cisco ESXi enic driver	2.3.0.7	Ethernet driver for Cisco VIC
	Cisco ESXi fnic driver	1.6.0.25	FCoE driver for Cisco VIC
Network	Cisco Nexus 9372 Switches	6.1(2)I3(5)	Operating system version
	Cisco MDS 9148S Switches	6.2(13b)	FC switch firmware version
Storage	IBM FlashSystem V9000 Storage	7.6.0.4	Software version
Software	VMware vSphere ESXi	6.0 update1a	Software version
	VMware vCenter	6.0	Software version
	Cisco Nexus 1000v Switch	5.2(1)SV3(1.5a)	Software version

Configuration Guidelines

This document provides details on configuring a fully redundant, highly available VersaStack unit with IBM FlashSystem V9000 storage. Therefore, reference is made at each step to the component being configured as either A or B. For example, Controller-A and Controller-B are used to identify the IBM storage controllers that are provisioned within this document and Cisco Nexus A and Cisco Nexus B identifies the pair of Cisco Nexus switches that are configured. The Cisco UCS fabric Interconnects are similarly configured. Additionally, this document details the steps for provisioning multiple Cisco UCS hosts, and these are identified sequentially: VM-Host-Infra-01, VM-Host-Infra-02, and so on. Finally, to indicate that you should include information pertinent to your environment in a given step, <text> appears as part of the command structure.

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, VSAN and VLAN schemes, as well as to record appropriate MAC addresses.

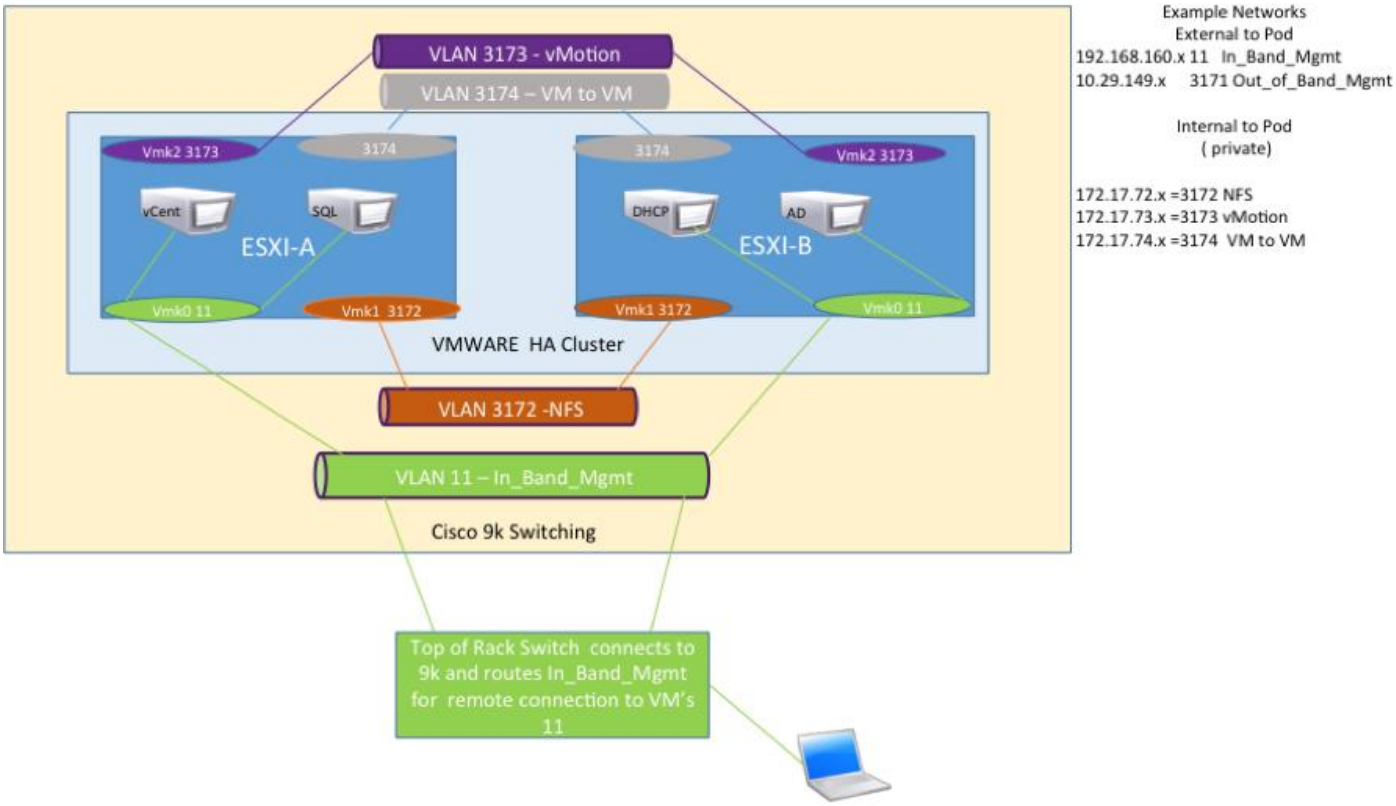
VLAN Topology

Table 2 and Table 3 describe the VLAN and VSAN IDs necessary for deployment as outlined in this guide. The virtual machines (VMs) necessary for deployment are outlined in this guide as well. Networking architectures 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 out through the Cisco Nexus 9000 switches. Other management traffic is routed through a separate Out of Band Management switch; your architecture could vary based on the deployment objectives. An NFS VLAN is included in this document to allow connectivity to any existing NFS data stores for migration of virtual machines if required, however NFS is not validated in the solution and is not supported on IBM FlashSystem V9000.

Table 2 Example IPs

VLAN Name	VLAN Purpose	ID used in this Document
Native	VLAN to which untagged frames are assigned	2
Out of Band Mgmt	VLAN for out-of-band management interfaces	3171
NFS	VLAN for Infrastructure NFS traffic	3172
vMotion	VLAN for VMware vMotion	3173
VM-Traffic	VLAN for Production VM Interfaces	3174
In-Band Mgmt	VLAN for in-band management interfaces	11

Figure 2 VLAN Logical View



Fibre Channel Topology

The SAN infrastructure allows addition of storage enclosures or additional building blocks non-disruptively. A pair of Cisco MDS switches has been used for the fibre channel connectivity providing redundancy. Separate fabrics have been created by utilizing VSAN's on the Cisco MDS switches which provides dedicated hosts or server-side storage area networks (SANs) and a private fabric to support the cluster interconnects.

The logical fabric isolation provides:

- No access for any host or server to the storage enclosure accidentally.
- No congestion to the host or server-side SAN can cause potential performance implications for both the host or server-side SAN and the FlashSystem V9000.

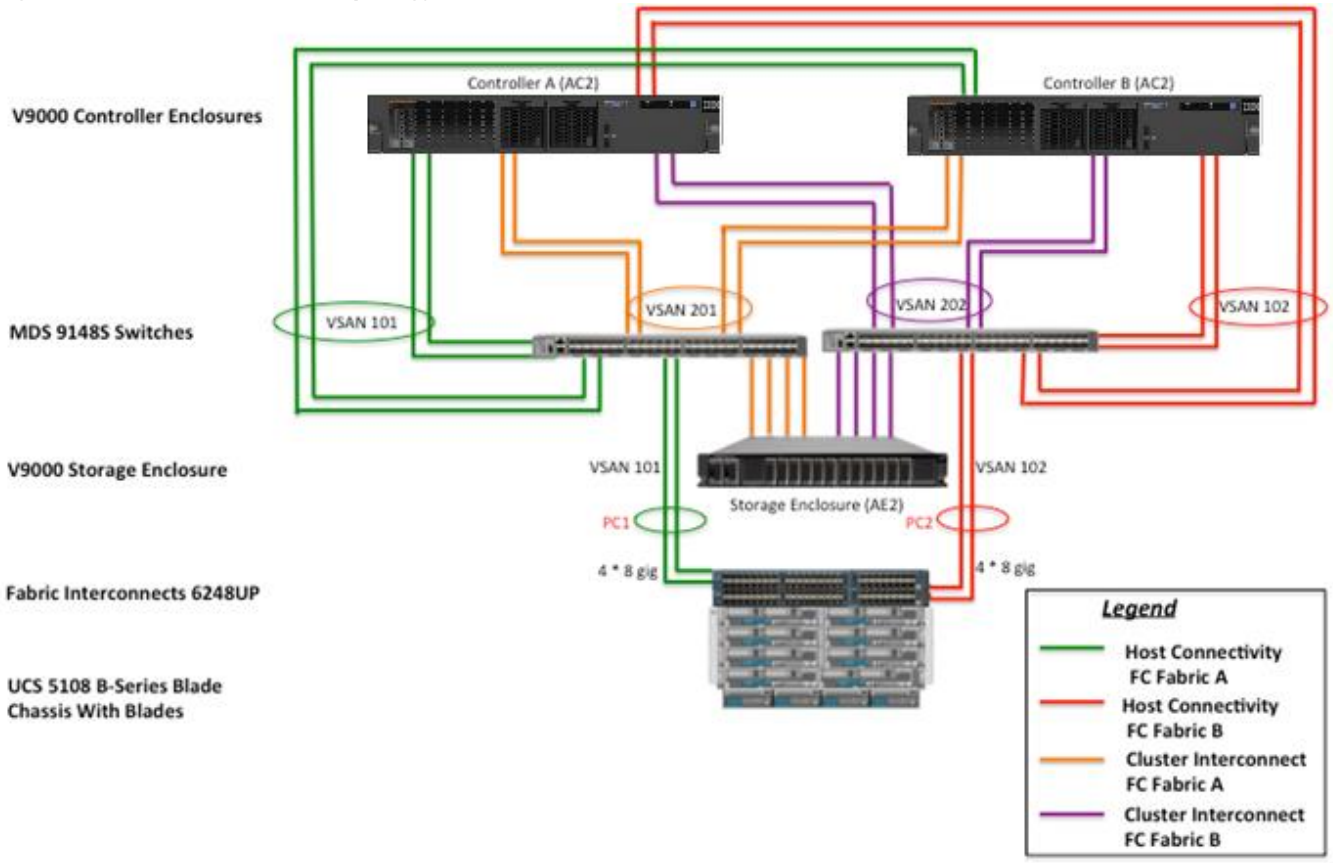
Table 3 describes the VSANs necessary for deployment as outlined in this guide.

Table 3 VSANs for Deployment

VSAN Name	VSAN Purpose	ID Used in Validating This Document
Host-Fabric-A	VSAN for Host connectivity	101

VSAN Name	VSAN Purpose	ID Used in Validating This Document
Host-Fabric-B	VSAN for Host connectivity	102
Cluster-Fabric-A	VSAN for Cluster connectivity	201
Cluster-Fabric-B	VSAN for Cluster connectivity	202

Figure 3 Fibre Channel Topology View



Virtual Machines

This document assumes that the required infrastructure machines exists or are created during the install. For example, some of the machines that would be necessary are listed in the below table.

Table 4 Virtual Machine List

Virtual Machine Description	Host Name
Active Directory	

Virtual Machine Description	Host Name
vCenter Server	
DHCP Server	

Configuration Variables

The following customer implementation values for the variables below should be identified prior to starting the installation procedure.

Table 5 Customer Variables

Variable	Description	Customer Implementation Value
<<var_cont01_mgmt_ip>>	Out-of-band management IP for V9000 Controller 01	
<<var_cont01_mgmt_mask>>	Out-of-band management network netmask	
<<var_cont01_mgmt_gateway>>	Out-of-band management network default gateway	
<<var_cont02_mgmt_ip>>	Out-of-band management IP for V9000 Controller 02	
<<var_cont02_mgmt_mask>>	Out-of-band management network netmask	
<<var_cont02_mgmt_gateway>>	Out-of-band management network default gateway	
<<var_can01_srvc_ip>>	Out-of-band service IP for canister1, Storage Enclosure	
<<var_can02_srvc_ip>>	Out-of-band service IP for canister2, Storage Enclosure	
<<var_can_srvc_mask>>	Out-of-band services management network netmask	
<<var_can_srvc_gateway>>	Out-of-band services management network default gateway	
<<var_cluster_mgmt_ip>>	Out-of-band management IP for V9000 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	

Variable	Description	Customer Implementation Value
<<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 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	

Variable	Description	Customer Implementation Value
<<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_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_ucsb_mgmt_ip>>	Cisco UCS fabric interconnect (FI) B 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_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) 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_MDS_A_hostname>>	Name for the FC Cisco MDS Switch in Fabric A	
<<var_MDS_A_mgmt0_ip>>	Cisco MDS switch Out-of-band management IP address	
<<var_MDS_A_mgmt0_netmask>>	Cisco MDS switch Out-of-band management IP netmask	

Variable	Description	Customer Implementation Value
<<var_MDS_A_mgmt0_gw>>	Cisco MDS switch Out-of-band Cisco Nexus A management IP gateway	
<<var_MDS_B_hostname>>	Name for the FC Cisco MDS Switch in Fabric B	
<<var_MDS_B_mgmt0_ip>>	Cisco MDS switch Out-of-band management IP address	
<<var_MDS_B_mgmt0_netmask>>	Cisco MDS switch Out-of-band management IP netmask	
<<var_MDS_B_mgmt0_gw>>	Cisco MDS switch Out-of-band management IP gateway	
<<var_UTC_offset>>	UTC time offset for your area	
<<var_vsan_a_id>>	VSAN id for Host connectivity on Cisco MDS switch A (101 is used)	
<<var_vsan_B_id>>	VSAN id for Host connectivity on Cisco MDS switch B (102 is used)	
<<var_vsan_a_clus_id>>	VSAN id for V9000 Cluster connectivity on Cisco MDS switch A (201 is used)	
<<var_vsan_B_clus_id>>	VSAN id for V9000 Cluster connectivity on Cisco MDS switch B (202 is used)	
<<var_fabric_a_fcoe_vlan_id>>	Fabric id for Cisco MDS switch A (101 is used)	
<<var_fabric_b_fcoe_vlan_id>>	Fabric id for Cisco MDS switch B (102 is used)	
<<var_In-band_mgmtblock_net>>	Block of IP addresses for KVM access for Cisco UCS	
<<var_vmhost_infra_01_ip>>	VMware ESXi host 01 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 5 variables should be repeated for all ESXi hosts		

The variables below for the Fibre Channel environment are to be collected during the installation phase for subsequent use in this document.

IBM FlashSystem V9000 Storage Controllers are also referred to as AC2 and the Storage Enclosure as AE2, this document refers to the controllers as Controller A (ContA) and Controller B (ContB) and the storage enclosure as (SE).

Following are the IBM FlashSystem V9000 Storage Fibre Channel port naming conventions used on Cisco MDS switches:

- Cont – Storage Controller
- SE- Storage Enclosure
- FE – Front-end, Host connectivity
- BE – Back-end, Cluster communication

Table 6 WWPN Variables

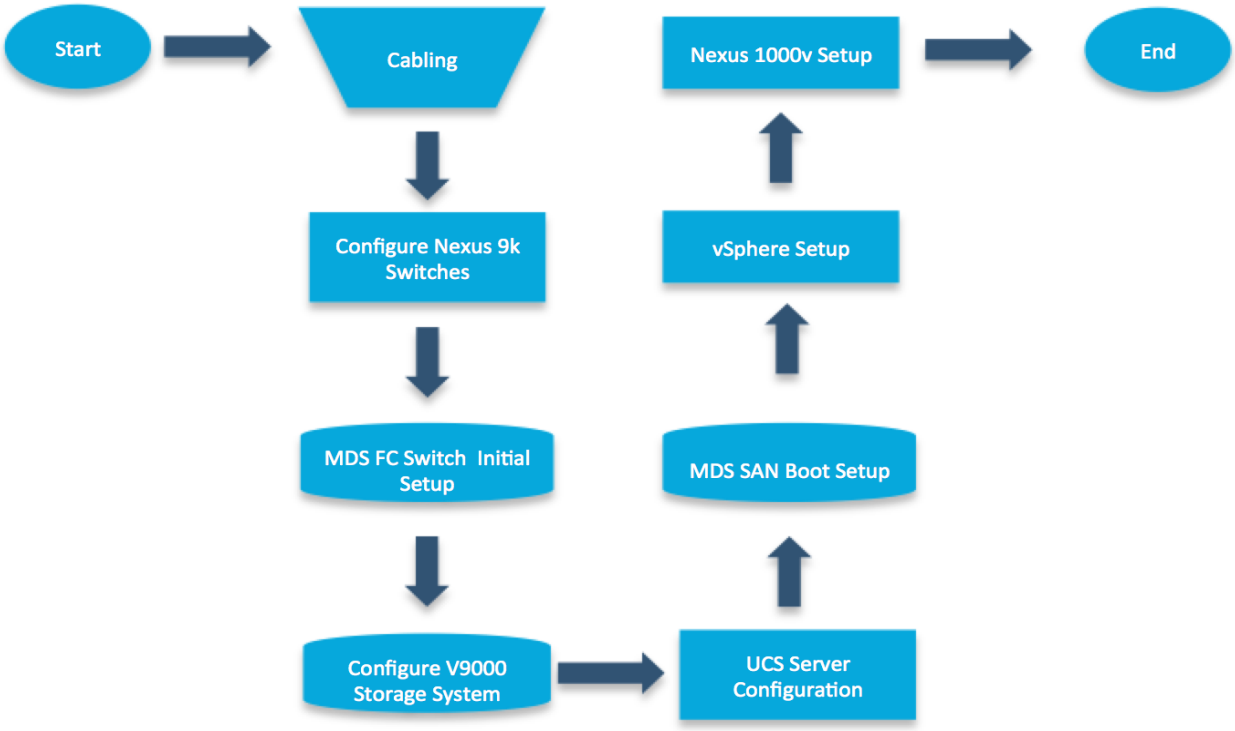
Source	Switch/ Port	Variable	WWPN
FC_SE-BE1-fabricA	Switch A, FC13	<<var_wwpn_FC_SE-BE1-fabricA>>	
FC_SE-BE2-fabricA	Switch A, FC14	<<var_wwpn_FC_SE-BE2-fabricA>>	
FC_SE-BE3-fabricA	Switch A, FC15	<<var_wwpn_FC_SE-BE3-fabricA>>	
FC_SE-BE4-fabricA	Switch A, FC16	<<var_wwpn_FC_SE-BE4-fabricA>>	
FC_SE-BE5-fabricB	Switch B, FC13	<<var_wwpn_FC_SE-BE5-fabricB>>	
FC_SE-BE6-fabricB	Switch B, FC14	<<var_wwpn_FC_SE-BE6-fabricB>>	
FC_SE-BE7-fabricB	Switch B, FC15	<<var_wwpn_FC_SE-BE7-fabricB>>	
FC_SE-BE8-fabricB	Switch B, FC16	<<var_wwpn_FC_SE-BE8-fabricB>>	
FC_ContA-BE1-fabricA	Switch A, FC9	<<var_wwpn_FC_ContA-BE1-fabricA>>	
FC_ContA-BE2-fabricA	Switch A, FC10	<<var_wwpn_FC_ContA-BE2-fabricA>>	
FC_ContB-BE1-fabricA	Switch A, FC11	<<var_wwpn_FC_ContB-BE1-fabricA>>	
FC_ContB-BE2-fabricA	Switch A, FC12	<<var_wwpn_FC_ContB-BE2-fabricA>>	
FC_ContA-BE3-fabricB	Switch B, FC9	<<var_wwpn_FC_ContA-BE3-	

Source	Switch/ Port	Variable	WWPN
		fabricB>>	
FC_ContA-BE4-fabricB	Switch B, FC10	<<var_wwpn_FC_ContA-BE4-fabricB>>	
FC_ContB-BE3-fabricB	Switch B, FC11	<<var_wwpn_FC_ContB-BE3-fabricB>>	
FC_ContB-BE4-fabricB	Switch B, FC12	<<var_wwpn_FC_ContB-BE4-fabricB>>	
FC_ContA-FE1-fabricA	Switch A, FC5	<<var_wwpn_FC_ContA-FE1-fabricA>>	
FC_ContA-FE2-fabricB	Switch B, FC5	<<var_wwpn_FC_ContA-FE2-fabricB>>	
FC_ContA-FE3-fabricA	Switch A, FC6	<<var_wwpn_FC_ContA-FE3-fabricA>>	
FC_ContA-FE4-fabricB	Switch B, FC6	<<var_wwpn_FC_ContA-FE4-fabricB>>	
FC_ContB-FE1-fabricA	Switch A, FC7	<<var_wwpn_FC_ContB-FE1-fabricA>>	
FC_ContB-FE2-fabricB	Switch B, FC7	<<var_wwpn_FC_ContB-FE2-fabricB>>	
FC_ContB-FE3-fabricA	Switch A, FC8	<<var_wwpn_FC_ContB-FE3-fabricA>>	
FC_ContB-FE4-fabricB	Switch B, FC8	<<var_wwpn_FC_ContB-FE4-fabricB>>	

VersaStack Cabling

VersaStack Build Process

Figure 4 VersaStack Build Process Flow Chart



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 FlashSystem V9000 running 7.6.0.4.

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 FlashSystem V9000 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 5 shows the cabling diagrams for VersaStack configurations using the Cisco Nexus 9000 and IBM FlashSystem V9000. For more information about FlashSystem V9000 enclosure cabling information, reference the following URL:

https://www.ibm.com/support/knowledgecenter/STKMQV_7.6.0/com.ibm.storage.vflashsystem9000.7.6.doc/FlashSystem_V9000_welcome.htm?lang=en

Figure 5 VersaStack Wiring

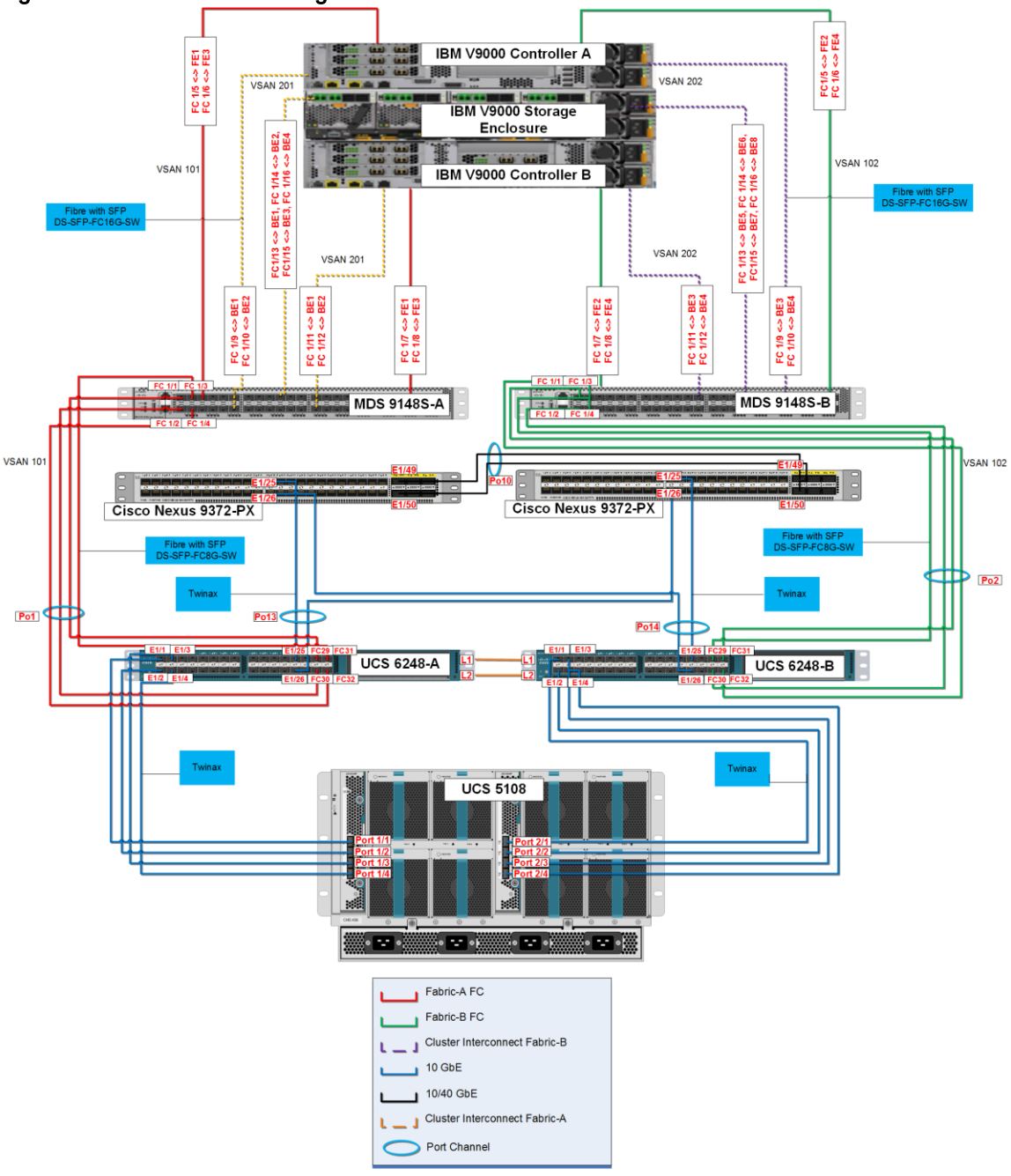
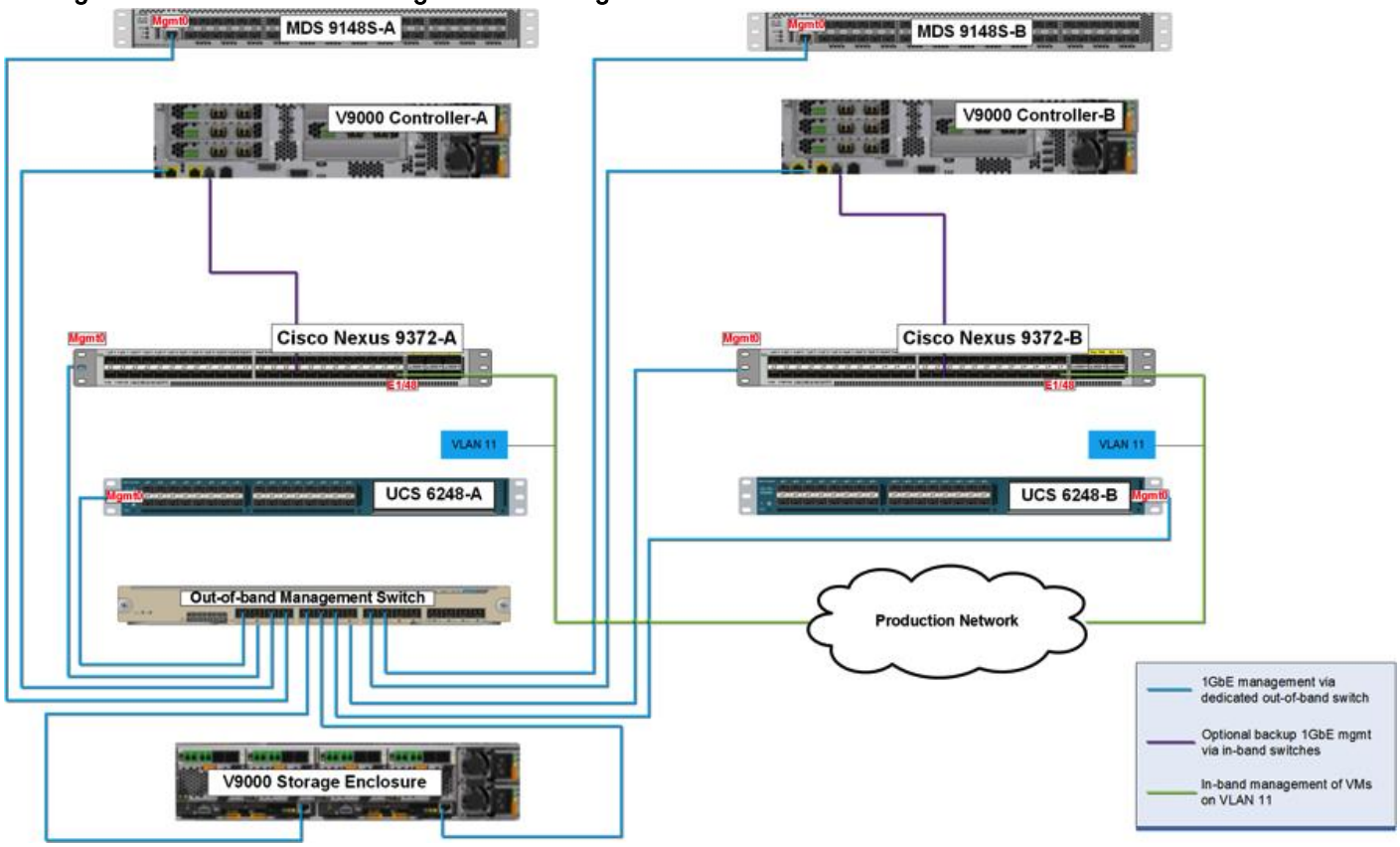


Figure 6 shows the Management cabling. The V9000's have redundant management connections. One path is through the dedicated out-of-band management switch, and the secondary path is through the in-band management path going up through the Cisco Nexus 9000 to the production network.

Figure 6 VersaStack Management Cabling



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

Table 7 Cisco Nexus 9000-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 9000-A	Eth1/25	10GbE	Cisco UCS fabric interconnect-A	Eth1/25
	Eth1/26	10GbE	Cisco UCS fabric interconnect-B	Eth1/26
	Eth1/49	40GbE	Cisco Nexus 9000-B	Eth1/49
	Eth1/50	40GbE	Cisco Nexus 9000-B	Eth1/50
	Eth1/48	GbE	GbE management switch	Any

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

Table 8 Cisco Nexus 9000-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 9000-B	Eth1/25	10GbE	Cisco UCS fabric interconnect-B	Eth1/25
	Eth1/26	10GbE	Cisco UCS fabric interconnect-A	Eth1/26
	Eth1/49	40GbE	Cisco Nexus 9000-A	Eth1/49
	Eth1/50	40GbE	Cisco Nexus 9000-A	Eth1/50
	Eth1/48	GbE	GbE management switch	Any

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

Figure 7 IBM V9000 Storage Day-0 Fibre Cabling Reference

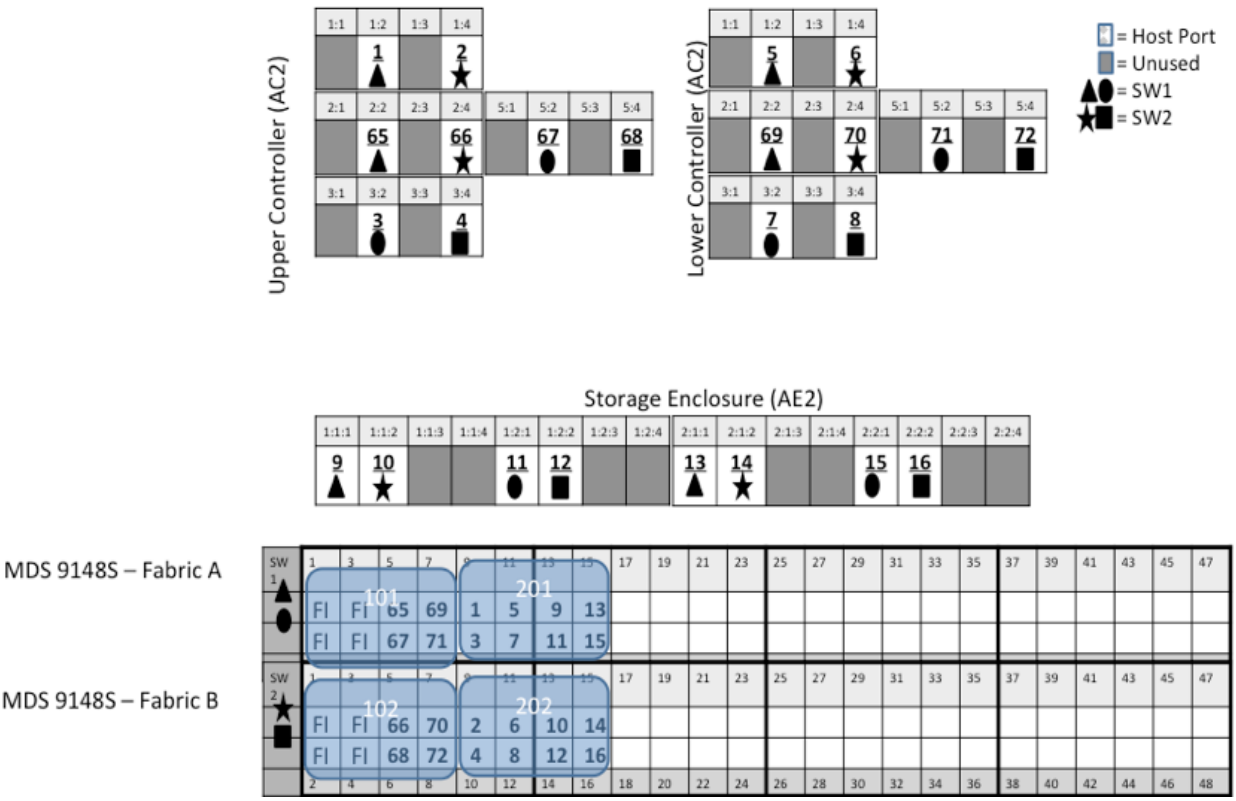


Table 9 Cisco Nexus MDS 9148S-A Cabling Reference to Switch Port Correlation

Port naming on Switch	Switch/ Port	Cabling reference
FC_SE-BE1-fabricA	Switch A, FC13	9
FC_SE-BE2-fabricA	Switch A, FC14	11
FC_SE-BE3-fabricA	Switch A, FC15	13
FC_SE-BE4-fabricA	Switch A, FC16	15
FC_ContA-BE1-fabricA	Switch A, FC9	1
FC_ContA-BE2-fabricA	Switch A, FC10	3
FC_ContB-BE1-fabricA	Switch A, FC11	5
FC_ContB-BE2-fabricA	Switch A, FC12	7
FC_ContA-FE1-fabricA	Switch A, FC5	65
FC_ContA-FE3-fabricA	Switch A, FC6	67
FC_ContB-FE1-fabricA	Switch A, FC7	69
FC_ContB-FE3-fabricA	Switch A, FC8	71

Table 10 Cisco Nexus MDS 9148S-B Cabling Reference Correlation

Port naming on Switch	Switch/ Port	Cabling reference
FC_SE-BE5-fabricB	Switch B, FC13	10
FC_SE-BE6-fabricB	Switch B, FC14	12
FC_SE-BE7-fabricB	Switch B, FC15	14
FC_SE-BE8-fabricB	Switch B, FC16	16
FC_ContA-BE3-fabricB	Switch B, FC9	2
FC_ContA-BE4-fabricB	Switch B, FC10	4
FC_ContB-BE3-fabricB	Switch B, FC11	6
FC_ContB-BE4-fabricB	Switch B, FC12	8
FC_ContA-FE2-fabricB	Switch B, FC5	66
FC_ContA-FE4-fabricB	Switch B, FC6	68
FC_ContB-FE2-fabricB	Switch B, FC7	70
FC_ContB-FE4-fabricB	Switch B, FC8	72

Table 11 IBM FlashSystem V9000 Controller, Cont-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
IBM FlashSystem V9000 Controller, Cont-A	E1	GbE	GbE management switch	Any
	E2 (optional)	GbE	Cisco Nexus 9000-A	Any
	FC1 (Slot2:Port2)	16gbps	Cisco MDS 9148S-A	fc1/5
	FC2 (Slot2:Port4)	16gbps	Cisco MDS 9148S-B	fc1/5
	FC3 (Slot5:Port2)	16gbps	Cisco MDS 9148S-A	fc1/6
	FC4 (Slot5:Port4)	16gbps	Cisco MDS 9148S-B	fc1/6
	FC5 (Slot1:Port2)	16gbps	Cisco MDS 9148S-A	fc1/9

Local Device	Local Port	Connection	Remote Device	Remote Port
	FC6 (Slot1:Port4)	16gbps	Cisco MDS 9148S-A	fc1/10
	FC7 (Slot3:Port2)	16gbps	Cisco MDS 9148S-B	fc1/9
	FC8 (Slot3:Port4)	16gbps	Cisco MDS 9148S-B	fc1/10

Table 12 IBM FlashSystem V9000 Controller, Cont-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
IBM FlashSystem V9000 Controller, Cont-B	E1	GbE	GbE management switch	Any
	E2 (optional)	GbE	Cisco Nexus 9000-B	Any
	FC1 (Slot2:Port2)	16gbps	Cisco MDS 9148S-A	fc1/7
	FC2 (Slot2:Port4)	16gbps	Cisco MDS 9148S-B	fc1/7
	FC3 (Slot5:Port2)	16gbps	Cisco MDS 9148S-A	fc1/8
	FC4 (Slot5:Port4)	16gbps	Cisco MDS 9148S-B	fc1/8
	FC5 (Slot1:Port2)	16gbps	Cisco MDS 9148S-A	fc1/11
	FC6 (Slot1:Port4)	16gbps	Cisco MDS 9148S-A	fc1/12
	FC7 (Slot3:Port2)	16gbps	Cisco MDS 9148S-B	fc1/11
	FC8 (Slot3:Port4)	16gbps	Cisco MDS 9148S-B	fc1/12

Table 13 IBM FlashSystem V9000 Storage Enclosure, SE Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
IBM FlashSystem V9000 Storage Enclosure, SE	E1	GbE	GbE management switch	Any
	E2	GbE	GbE management switch	Any
	FC1	16gbps	Cisco MDS 9148S-A	fc1/13

Local Device	Local Port	Connection	Remote Device	Remote Port
	FC2	16gbps	Cisco MDS 9148S-A	fc1/14
	FC3	16gbps	Cisco MDS 9148S-A	fc1/15
	FC4	16gbps	Cisco MDS 9148S-A	fc1/16
	FC5	16gbps	Cisco MDS 9148S-B	fc1/13
	FC6	16gbps	Cisco MDS 9148S-B	fc1/14
	FC7	16gbps	Cisco MDS 9148S-B	fc1/15
	FC8	16gbps	Cisco MDS 9148S-B	fc1/16

Table 14 Cisco Nexus MDS 9148S-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco MDS 9148S-A	Mgmt0	GbE	GbE management switch	Any
	fc1/1	8gbps	Cisco UCS Fabric Interconnect 6248-A	fc29
	fc1/2	8gbps	Cisco UCS Fabric Interconnect 6248-A	fc30
	fc1/3	8gbps	Cisco UCS Fabric Interconnect 6248-A	fc31
	fc1/4	8gbps	Cisco UCS Fabric Interconnect 6248-A	fc32
	fc1/5	16gbps	IBM controller, ContA-FE1	FC1
	fc1/6	16gbps	IBM controller, ContA-FE3	FC3
	fc1/7	16gbps	IBM controller, ContB-FE1	FC1
	fc1/8	16gbps	IBM controller, ContB-FE3	FC3
	fc1/9	16gbps	IBM controller, ContA-BE1	FC5
	fc1/10	16gbps	IBM controller, ContA-BE2	FC6
	fc1/11	16gbps	IBM controller, ContB-BE1	FC5
	fc1/12	16gbps	IBM controller, ContB-BE2	FC6
	fc1/13	16gbps	IBM Storage Enclosure, SE-BE1	FC1
	fc1/14	16gbps	IBM Storage Enclosure, SE-BE2	FC2
	fc1/15	16gbps	IBM Storage Enclosure, SE-BE3	FC3
	fc1/16	16gbps	IBM Storage Enclosure, SE-BE4	FC4

Table 15 Cisco Nexus MDS 9148S-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco MDS 9148S-B	Mgmt0	GbE	GbE management switch	Any
	fc1/1	8gbps	Cisco UCS Fabric Interconnect 6248-B	fc29
	fc1/2	8gbps	Cisco UCS Fabric Interconnect 6248-B	fc30
	fc1/3	8gbps	Cisco UCS Fabric Interconnect 6248-B	fc31
	fc1/4	8gbps	Cisco UCS Fabric Interconnect 6248-B	fc32
	fc1/5	16gbps	IBM controller, ContA-FE2	FC2
	fc1/6	16gbps	IBM controller, ContA-FE4	FC4
	fc1/7	16gbps	IBM controller, ContB-FE2	FC2
	fc1/8	16gbps	IBM controller, ContB-FE4	FC4
	fc1/9	16gbps	IBM controller, ContA-BE3	FC7
	fc1/10	16gbps	IBM controller, ContA-BE4	FC8
	fc1/11	16gbps	IBM controller, ContB-BE3	FC7
	fc1/12	16gbps	IBM controller, ContB-BE4	FC8
	fc1/13	16gbps	IBM Storage Enclosure, SE-BE5	FC5
	fc1/14	16gbps	IBM Storage Enclosure, SE-BE6	FC6
	fc1/15	16gbps	IBM Storage Enclosure, SE-BE7	FC7
	fc1/16	16gbps	IBM Storage Enclosure, SE-BE8	FC8

Table 16 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
	Eth1/25	10GbE	Cisco Nexus 9000-A	Eth 1/25
	Eth1/26	10GbE	Cisco Nexus 9000-B	Eth 1/26
	Eth1/1	10GbE	Cisco UCS Chassis FEX-A	IOM 1/1
	Eth1/2	10GbE	Cisco UCS Chassis FEX-A	IOM 1/2
	Eth1/3	10GbE	Cisco UCS Chassis FEX-A	IOM 1/3
	Eth1/4	10GbE	Cisco UCS Chassis FEX-A	IOM 1/4
	fc29	8gbps	Cisco MDS 9148S-A	fc1/1

Local Device	Local Port	Connection	Remote Device	Remote Port
	fc30	8gbps	Cisco MDS 9148S-A	fc1/2
	fc31	8gbps	Cisco MDS 9148S-A	fc1/3
	fc32	8gbps	Cisco MDS 9148S-A	fc1/4
	L1	GbE	Cisco UCS fabric interconnect-B	L1
	L2	GbE	Cisco UCS fabric interconnect-B	L2

Table 17 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
	Eth1/25	10GbE	Cisco Nexus 9000-B	Eth 1/25
	Eth1/26	10GbE	Cisco Nexus 9000-A	Eth 1/26
	Eth1/1	10GbE	Cisco UCS Chassis FEX-B	IOM 1/1
	Eth1/2	10GbE	Cisco UCS Chassis FEX-B	IOM 1/2
	Eth1/3	10GbE	Cisco UCS Chassis FEX-B	IOM 1/3
	Eth1/4	10GbE	Cisco UCS Chassis FEX-B	IOM 1/4
	fc29	8gbps	Cisco MDS 9148S-B	fc1/1
	fc30	8gbps	Cisco MDS 9148S-B	fc1/2
	fc31	8gbps	Cisco MDS 9148S-B	fc1/3
	fc32	8gbps	Cisco MDS 9148S-B	fc1/4
	L1	GbE	Cisco UCS fabric interconnect-A	L1
	L2	GbE	Cisco UCS fabric interconnect-A	L2

Cisco UCS C-Series can be connected to the FI directly or using FEX, the system validation included Cisco UCS C-Series directly connected to the Fabric Interconnects.

Table 18 Connectivity with Direct Connect to FI

Local Device	Local Port	Connection	Remote Device	Remote Port

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS C-Series Server 1 with Cisco VIC	Port 0	10GbE	Cisco UCS Fabric Interconnect 6248-A	Port 5
	Port 1	10GbE	Cisco UCS Fabric Interconnect 6248-B	Port 6
Cisco UCS C-Series Server 2 with Cisco VIC	Port 0	10GbE	Cisco UCS Fabric Interconnect 6248-A	Port 7
	Port 1	10GbE	Cisco UCS Fabric Interconnect 6248-B	Port 8

Table 19 Cisco Nexus Rack FEX A Example Connectivity Option

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 2232PP FEX A	Fabric Port 1/1	10GbE	Cisco UCS fabric interconnect A	Port 5
	Fabric Port 1/2	10GbE	Cisco UCS fabric interconnect A	Port 6

Table 20 Cisco Nexus Rack FEX B

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 2232PP FEX B	Fabric Port 1/1	10GbE	Cisco UCS fabric interconnect B	Port 5
	Fabric Port 1/2	10GbE	Cisco UCS fabric interconnect B	Port 6

VersaStack Deployment

Cisco Nexus 9000 Initial Configuration Setup

This section provides the details for the initial Cisco Nexus 9000 Switch setup.

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
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_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 the Appropriate Cisco Nexus 9000 Features and Settings

Cisco Nexus 9000 A and Cisco Nexus 9000 B

To enable IP switching feature and set default spanning tree behaviors, complete the following steps:

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

```
config terminal
```

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

```
feature udld
feature lacp
feature vpc
```

3. Configure 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 IP 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:

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
exit
copy run start
```

Configure Virtual Port Channel Domain

Cisco Nexus 9000 A

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

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

2. Make Cisco 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 Cisco Nexus 9000s to establish a keepalive link:

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

4. Enable 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 Cisco 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 Cisco Nexus 9000s to establish a keepalive link:

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

4. Enable 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 Eth1/49
description VPC Peer <<var_nexus_B_hostname>>:1/47
interface Eth1/50

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 Eth1/49,Eth1/50
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, 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>>,
```

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 Eth1/49
 description VPC Peer <<var_nexus_A_hostname>>:1/47
 interface  Eth1/50
 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 Eth1/49,Eth1/50
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, 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>>,
```

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, 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 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 Eth1/25
description <<var_ucs_clustername>>-A:1/25
```

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, 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>>
```

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 Eth1/26
description <<var_ucs_clustername>>-B:1/26
```

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>>-B

```
interface Po14
description <<var_ucs_clustername>>-B
```

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 be 9216 to support jumbo frames.

```
mtu 9216
```

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

```
vpc 14
no shutdown
```

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

```
interface Eth1/25
description <<var_ucs_clustername>>-B:1/25
```

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

```
channel-group 14 force mode active
no shutdown
```

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

```
interface Po13
description <<var_ucs_clustername>>-A
```

9. Make the port-channel a switchport, and configure a trunk to allow InBand management, NFS, 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>>,
```

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 13
no shutdown
```

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

```
interface Eth1/26
description <<var_ucs_clustername>>-A:1/26
```

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

```
channel-group 13 force  mode active
no shutdown
copy run start
```

Management Plane Access for Servers and Virtual Machines

There are multiple ways to configure the switch to the uplink to your separate management switch. The two examples shown below helps you to know how your configuration could be setup, however since networking configurations can vary, we recommend 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 number 48. The Cisco Nexus 9000-Series switches use a 1 GB SFP to convert the Cat-5 copper cable connected to the top of rack switch; however, note that the connection types can vary. The Cisco Nexus 9000 switches are configured with the interface-VLAN option and each Cisco Nexus 9000 switch has a unique IP for its VLAN. The traffic we wish to route from the Cisco Nexus 9000 is the in-band management traffic, so we will use the VLAN 11 and set the port to access mode. The top of rack switch also has its ports set to access mode. In the second example, the top of rack switch would have port channel configured, and also we show how to leverage port channel, which maximizes upstream connectivity.

Cisco Nexus 9000 A and B using Interface VLAN Example 1

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

Cisco Nexus 9000 A

```
int Eth1/48
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 Eth1/48
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, complete the following steps:

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

```
interface po11
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 11
no shutdown
```

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

```
interface Eth1/48
description IB-MGMT-SWITCH_uplink
```

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

```
channel-group 11 force mode active
no shutdown
```

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

```
Copy run start
sh int eth1/48 br
sh port-channel summary
```

Cisco MDS 9148S Initial Configuration Setup

These steps provide the details of the initial Cisco MDS Fibre Channel Switch setup. We are creating a cluster zone to enable FlashSystem V9000 Controllers (AC2) to Storage Enclosure (AE2) communication.

Cisco MDS A

To set up the initial configuration for the first Cisco MDS switch complete the following step:

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.

On initial boot and connection to the serial or console port of the switch, the Cisco MDS 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 ----

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 MDS 9000 Family devices promptly with your supplier.
Failure to register may affect response times for initial service calls. MDS
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]:

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

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

  Enter the switch name : <<var_MDS_A_hostname>>

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

    Mgmt0 IPv4 address : <<var_MDS_A_mgmt0_ip>>

    Mgmt0 IPv4 netmask : <<var_MDS_A_mgmt0_netmask>>

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

    IPv4 address of the default gateway : <<var_MDS_A_mgmt0_gw>>

    Configure advanced IP options? (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
    Enable the telnet service? (yes/no) [n]:
```

```
Configure congestion/no_credit drop for fc interfaces? (yes/no)[y]:
Enter the type of drop to configure congestion/no_credit drop? (con/no) [c]:

Enter milliseconds in multiples of 10 for congestion-drop for port mode F in
range (<100-500>/default), where default is 500.  [d]:
Congestion-drop for port mode E must be greater than or equal to Congestion-drop
for port mode F. Hence, Congestion drop for port mode E will be set as default.

 Enable the http-server? (yes/no) [y]:

 Configure clock? (yes/no) [n]:

 Configure timezone? (yes/no) [n]: y

Enter timezone config [PST/MST/CST/EST] : <<var_timezone>>

Enter Hrs offset from UTC [-23:+23] : <<var_UTC_offset>>

Enter Minutes offset from UTC [0-59] :

Configure summertime? (yes/no) [n]:

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

NTP server IPv4 address : <<var_global_ntp_server_ip>>
Configure default switchport interface state (shut/noshut) [shut]:

  Configure default switchport trunk mode (on/off/auto) [on]:

  Configure default switchport port mode F (yes/no) [n]:

  Configure default zone policy (permit/deny) [deny]:

  Enable full zoneset distribution? (yes/no) [n]:

  Configure default zone mode (basic/enhanced) [basic]:

The following configuration will be applied:

  password strength-check

 switchname <<var_MDS_A_hostname>>
   interface mgmt0

    ip address <<var_MDS_A_mgmt0_ip>> <<var_MDS_A_mgmt0_netmask>>     no shutdown

ip default-gateway <<var_MDS_A_mgmt0_gw>>

ssh key rsa 2048 force

feature ssh

 no feature telnet   system timeout congestion-drop default mode F   system
timeout congestion-drop default mode E

feature http-server

clock timezone PST 0 0

ntp server <<var_global_ntp_server_ip>>

system default switchport shutdown

system default switchport trunk mode on
```

```
no system default zone default-zone permit

no system default zone distribute full

no system default zone mode enhanced

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

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

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

Cisco MDS B

To set up the initial configuration for the second Cisco MDS switch complete the following step:

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.

On initial boot and connection to the serial or console port of the switch, the Cisco MDS 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 ----

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 MDS 9000 Family devices promptly with your supplier.
Failure to register may affect response times for initial service calls. MDS
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]:

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

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

  Enter the switch name : <<var_MDS_B_hostname>>

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

    Mgmt0 IPv4 address : <<var_MDS_B_mgmt0_ip>>

    Mgmt0 IPv4 netmask : <<var_MDS_B_mgmt0_netmask>>

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

```
    IPv4 address of the default gateway : <<var_MDS_B_mgmt0_gw>>

 Configure advanced IP options? (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

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

  Configure congestion/no_credit drop for fc interfaces? (yes/no)     [y]:

  Enter the type of drop to configure congestion/no_credit drop? (con/no) [c]:

    Enter milliseconds in multiples of 10 for congestion-drop for port mode F
in range (<100-500>/default), where default is 500.  [d]:

Congestion-drop for port mode E must be greater than or equal to     Congestion-
drop for port mode F. Hence, Congestion drop for port     mode E will be set as
default.

  Enable the http-server? (yes/no) [y]:

 Configure clock? (yes/no) [n]:

 Configure timezone? (yes/no) [n]: y

Enter timezone config [PST/MST/CST/EST] : <<var_timezone>>

Enter Hrs offset from UTC [-23:+23] : <<var_UTC_offset>>

Enter Minutes offset from UTC [0-59] :

Configure summertime? (yes/no) [n]:

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

NTP server IPv4 address : <<var_global_ntp_server_ip>>

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

Configure default switchport trunk mode (on/off/auto) [on]:

  Configure default switchport port mode F (yes/no) [n]:

  Configure default zone policy (permit/deny) [deny]:

  Enable full zoneset distribution? (yes/no) [n]:

  Configure default zone mode (basic/enhanced) [basic]:

The following configuration will be applied:

  password strength-check

switchname : <<var_MDS_B_hostname>>

interface mgmt0

  ip address <<var_MDS_B_mgmt0_ip>> <<var_MDS_B_mgmt0_netmask>>

   no shutdown

  ip default-gateway <<var_MDS_B_mgmt0_gw>>
```

```
  ssh key rsa 2048 force
feature ssh
 no feature telnet
 system timeout congestion-drop default mode F
system timeout congestion-drop default mode E
feature http-server  clock timezone PST 0 0
       ntp server <<var_global_ntp_server_ip>>
      system default switchport shutdown
      system default switchport trunk mode on
       no system default zone default-zone permit
       no system default zone distribute full
       no system default zone mode enhanced
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 MDS Features and Settings

Cisco MDS A and B

To enable the feature on both switches, enter the following commands

```
Config
feature npiv
feature fport-channel-trunk
```

Enable VSANs and Create Port Channel and Cluster Zone

Cisco MDS A

1. Create Port Channel that will be uplinked to the fabric interconnect

```
interface port-channel 1
```

2. Create a VSAN for Host Connectivity and assign interfaces to it. Ports assigned to the port channel will also be in this VSAN. Configure the ports up.

```
vsan database
vsan <<var_vsan_a_id>>
vsan <<var_vsan_a_id>>  interface fc1/5-8
vsan <<var_vsan_a_id>>  interface po1
interface fc1/5-8
no shut
```

3. Create a VSAN for Cluster Interconnect and assign interfaces to it.

```
vsan database
vsan <<var_vsan_a_clus_id>>
vsan <<var_vsan_a_clus_id>> interface fc1/8-16
no shut
```

4. Activate the port channel.

The port channel ports will not be connected until the Fabric Interconnect is configured.

```
interface port-channel 1
channel mode active
switchport rate-mode dedicated
```

5. Assign interfaces to the port channel and save the config.

```
interface fc1/1-4
port-license acquire
channel-group 1 force
no shutdown
exit
copy run start
```

You can run a “show int br” to validate the interfaces 1-4 are in the proper VSAN.

6. Run show flogi database to obtain the WWPN’s for the FlashSystem V9000 ports in cluster VSAN. Copy the 8 WWPN’s for the IBM Storwize system to create a zone for the cluster in Step 9.

```
VersaStack-MDS-A# sh flogi database  vsan 201
--------------------------------------------------------------------------------
INTERFACE        VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
fc1/9            201   0x940000  50:05:07:68:0c:11:22:71 50:05:07:68:0c:00:22:71
fc1/10           201   0x940300  50:05:07:68:0c:31:22:71 50:05:07:68:0c:00:22:71
fc1/11           201   0x940100  50:05:07:68:0c:11:22:67 50:05:07:68:0c:00:22:67
fc1/12           201   0x940200  50:05:07:68:0c:31:22:67 50:05:07:68:0c:00:22:67
fc1/13           201   0x940400  50:05:07:60:5e:83:cc:81 50:05:07:60:5e:83:cc:80
fc1/14           201   0x940600  50:05:07:60:5e:83:cc:91 50:05:07:60:5e:83:cc:80
fc1/15           201   0x940500  50:05:07:60:5e:83:cc:a1 50:05:07:60:5e:83:cc:bf
fc1/16           201   0x940700  50:05:07:60:5e:83:cc:b1 50:05:07:60:5e:83:cc:bf

Total number of flogi = 8.
```

7. Input all FlashSystem V9000 Fabric A WWPNs into the variable table below belonging to host and cluster VSANs. Their assigned switch ports identify FlashSystem V9000 Fibre Channel ports.

Table 21 V9000 Fabric A WWPNs

Source	Switch/ Port	Variable	WWPN
FC_SE-BE1-fabricA	Switch A FC13	var_wwpn_FC_SE-BE1-fabricA	50:05:07:60:5e:83:cc:81
FC_SE-BE2-fabricA	Switch A FC14	var_wwpn_FC_SE-BE2-fabricA	50:05:07:60:5e:83:cc:91
FC_SE-BE3-fabricA	Switch A FC15	var_wwpn_FC_SE-BE3-fabricA	50:05:07:60:5e:83:cc:a1

FC_SE-BE4-fabricA	Switch A FC16	var_wwpn_FC_SE-BE4-fabricA	50:05:07:60:5e:83:cc:b1
FC_ContA-BE1-fabricA	Switch A FC9	var_wwpn_FC_ContA-BE1-fabricA	50:05:07:68:0c:11:22:71
FC_ContA-BE2-fabricA	Switch A FC10	var_wwpn_FC_ContA-BE2-fabricA	50:05:07:68:0c:31:22:71
FC_ContB-BE1-fabricA	Switch A FC11	var_wwpn_FC_ContB-BE1-fabricA	50:05:07:68:0c:11:22:67
FC_ContB-BE2-fabricA	Switch A FC12	var_wwpn_FC_ContB-BE2-fabricA	50:05:07:68:0c:31:22:67
FC_ContA-FE1-fabricA	Switch A FC5	var_wwpn_FC_ContA-FE1-fabricA	50:05:07:68:0c:21:22:71
FC_ContA-FE3-fabricA	Switch A FC6	var_wwpn_FC_ContA-FE3-fabricA	50:05:07:68:0c:51:22:71
FC_ContB-FE1-fabricA	Switch A FC7	var_wwpn_FC_ContB-FE1-fabricA	50:05:07:68:0c:21:22:67
FC_ContB-FE3-fabricA	Switch A FC8	var_wwpn_FC_ContB-FE3-fabricA	50:05:07:68:0c:51:22:67

8. Create a device alias database with each PWWN mapping using the port assignments:

```
device-alias database
device-alias name VersaStack-ContA-BE1 pwwn var_wwpn_FC_ContA-BE1-fabricA
device-alias name VersaStack-ContA-BE2 pwwn var_wwpn_FC_ContA-BE2-fabricA
device-alias name VersaStack-ContB-BE1 pwwn var_wwpn_FC_ContB-BE1-fabricA
device-alias name VersaStack-ContB-BE2 pwwn var_wwpn_FC_ContB-BE2-fabricA
device-alias name VersaStack-SE-BE1 pwwn var_wwpn_FC_SE-BE1-fabricA
device-alias name VersaStack-SE-BE2 pwwn var_wwpn_FC_SE-BE2-fabricA
device-alias name VersaStack-SE-BE3 pwwn var_wwpn_FC_SE-BE3-fabricA
device-alias name VersaStack-SE-BE4 pwwn var_wwpn_FC_SE-BE4-fabricA
device-alias name VersaStack-ContA-FE1 pwwn var_wwpn_FC_ContA-FE1-fabricA
device-alias name VersaStack-ContA-FE3 pwwn var_wwpn_FC_ContA-FE3-fabricA
device-alias name VersaStack-ContB-FE1 pwwn var_wwpn_FC_ContB-FE1-fabricA
device-alias name VersaStack-ContB-FE3 pwwn var_wwpn_FC_ContB-FE3-fabricA
device-alias commit
```

9. Create the zone for FlashSystem V9000 Cluster used for controller communication. If adding more FlashSystem V9000 control or storage nodes, you will add the WWPN's to the cluster communication zone used below named VersaStack. Host zones and the cluster zone belong to separate VSAN fabrics.

```
zone name versastack vsan <<var_vsan_a_clus_id>>
member device-alias VersaStack-ContA-BE1
member device-alias VersaStack-ContA-BE2
member device-alias VersaStack-ContB-BE1
member device-alias VersaStack-ContB-BE2
member device-alias VersaStack-SE-BE1
member device-alias VersaStack-SE-BE2
member device-alias VersaStack-SE-BE3
```

```
member device-alias VersaStack-SE-BE4
exit
```

10. Create the zoneset for the VersaStack cluster configuration and add the zone. This gets created in the cluster communication VSAN.

```
zoneset name versastack-cluster vsan <<var_vsan_a_clus_id>>
member versastack
zoneset activate name  versastack-cluster vsan <<var_vsan_a_clus_id>>
sh zoneset active
copy run start
```

Cisco MDS B

1. Create Port Channel that will be uplinked to the fabric interconnect.

```
interface port-channel 2
```

2. Create a VSAN for Host Connectivity and assign interfaces to it. Ports assigned to the port channel will also be in this vsan.

```
vsan  database
vsan <<var_vsan_b_id>>
vsan <<var_vsan_b_id>> interface fc1/5-8
vsan <<var_vsan_b_id>> interface po2
interface fc1/5-8
no shut
```

3. Create a VSAN for Cluster Interconnect and assign interfaces to it.

```
vsan database
vsan <<var_vsan_b_clus_id>>
vsan <<var_vsan_b_clus_id>> interface fc1/8-16
no shut
```

4. Activate the port channel

The port channel ports will not be connected until the Fabric Interconnect is configured.

```
interface port-channel 2
channel mode active
switchport rate-mode dedicated
```

5. Assign interfaces to the port channel and save the config.

```
interface fc1/1-4
port-license acquire
channel-group 2 force
no shutdown
exit
copy run start
```

You can run a “show int br” to validate the interfaces 1-4 are in the proper VSAN.

6. Run show flogi database to obtain the WWPN’s for the FlashSystem V9000 ports in the cluster VSAN. Copy the 8 WWPN’s for the IBM Storewize system to create a zone for the cluster in Step 9.

```
VersaStack-MDS-B# sh flogi database vsan 202
--------------------------------------------------------------------------------
INTERFACE        VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
fc1/9            202   0x7c0700  50:05:07:68:0c:12:22:71 50:05:07:68:0c:00:22:71
fc1/10           202   0x7c0000  50:05:07:68:0c:32:22:71 50:05:07:68:0c:00:22:71
fc1/11           202   0x7c0600  50:05:07:68:0c:12:22:67 50:05:07:68:0c:00:22:67
fc1/12           202   0x7c0100  50:05:07:68:0c:32:22:67 50:05:07:68:0c:00:22:67
fc1/13           202   0x7c0300  50:05:07:60:5e:83:cc:82 50:05:07:60:5e:83:cc:80
fc1/14           202   0x7c0500  50:05:07:60:5e:83:cc:92 50:05:07:60:5e:83:cc:80
fc1/15           202   0x7c0200  50:05:07:60:5e:83:cc:a2 50:05:07:60:5e:83:cc:bf
fc1/16           202   0x7c0400  50:05:07:60:5e:83:cc:b2 50:05:07:60:5e:83:cc:bf

Total number of flogi = 8.
```

7. Input all FlashSystem V9000 fabric B WWPN's into the variable table below belonging to host and cluster VSANs.

Table 22 V9000 Fabric B WWPNs

Source	Switch/ Port	Variable	WWPN
FC_SE-BE5-fabricB	Switch B FC13	var_wwpn_FC_SE-BE5-fabricB	50:05:07:60:5e:83:cc:82
FC_SE-BE6-fabricB	Switch B FC14	var_wwpn_FC_SE-BE6-fabricB	50:05:07:60:5e:83:cc:92
FC_SE-BE7-fabricB	Switch B FC15	var_wwpn_FC_SE-BE7-fabricB	50:05:07:60:5e:83:cc:a2
FC_SE-BE8-fabricB	Switch B FC16	var_wwpn_FC_SE-BE8-fabricB	50:05:07:60:5e:83:cc:b2
FC_ContA-BE3-fabricB	Switch B FC9	var_wwpn_FC_ContA-BE3-fabricB	50:05:07:68:0c:12:22:71
FC_ContA-BE4-fabricB	Switch B FC10	var_wwpn_FC_ContA-BE4-fabricB	50:05:07:68:0c:32:22:71
FC_ContB-BE3-fabricB	Switch B FC11	var_wwpn_FC_ContB-BE3-fabricB	50:05:07:68:0c:12:22:67
FC_ContB-BE4-fabricB	Switch B FC12	var_wwpn_FC_ContB-BE4-fabricB	50:05:07:68:0c:32:22:67
FC_ContA-FE2-fabricB	Switch B FC5	var_wwpn_FC_ContA-FE2-fabricB	50:05:07:68:0c:22:22:71
FC_ContA-FE4-fabricB	Switch B FC6	var_wwpn_FC_ContA-FE4-fabricB	50:05:07:68:0c:52:22:71
FC_ContB-FE2-fabricB	Switch B FC7	var_wwpn_FC_ContB-FE2-fabricB	50:05:07:68:0c:22:22:67
FC_ContB-FE4-fabricB	Switch B FC8	var_wwpn_FC_ContB-FE4-fabricB	50:05:07:68:0c:52:22:67

8. Create a dev alias database for each PWWN using the port assignments:

```
device-alias database
device-alias name VersaStack-ContA-BE3 pwwn var_wwpn_FC_ContA-BE3-fabricB
device-alias name VersaStack-ContA-BE4 pwwn var_wwpn_FC_ContA-BE4-fabricB
device-alias name VersaStack-ContB-BE3 pwwn var_wwpn_FC_ContB-BE3-fabricB
device-alias name VersaStack-ContB-BE4 pwwn var_wwpn_FC_ContB-BE4-fabricB
```

```
device-alias name VersaStack-SE-BE5 pwwn var_wwpn_FC_SE-BE5-fabricB
device-alias name VersaStack-SE-BE6 pwwn var_wwpn_FC_SE-BE6-fabricB
device-alias name VersaStack-SE-BE7 pwwn var_wwpn_FC_SE-BE7-fabricB
device-alias name VersaStack-SE-BE8 pwwn var_wwpn_FC_SE-BE8-fabricB
device-alias name VersaStack-ContA-FE2 pwwn var_wwpn_FC_ContA-FE2-fabricB
device-alias name VersaStack-ContA-FE4 pwwn var_wwpn_FC_ContA-FE4-fabricB
device-alias name VersaStack-ContB-FE2 pwwn var_wwpn_FC_ContB-FE2-fabricB
device-alias name VersaStack-ContB-FE4 pwwn var_wwpn_FC_ContB-FE4-fabricB
device-alias commit
```

9. Create the zone for the FlashSystem V9000 Cluster; used for controller communication .If adding more FlashSystem V9000 control or storage nodes, you will add the WWPN's to the cluster communication zone used below named versastack. Host zones and the cluster zone belong to separate VSAN fabrics

```
zone name versastack vsan <<var_vsan_b_clus_id>>
member device-alias VersaStack-ContB-BE3
member device-alias VersaStack-ContB-BE4
member device-alias VersaStack-ContA-BE3
member device-alias VersaStack-ContA-BE4
member device-alias VersaStack-SE-BE5
member device-alias VersaStack-SE-BE6
member device-alias VersaStack-SE-BE7
member device-alias VersaStack-SE-BE8
exit
```

10. Create the zoneset for the VersaStack cluster configuration and add the zone. This gets created in the cluster communication VSAN.

```
zoneset name versastack-cluster vsan <<var_vsan_b_clus_id>>
member versastack
zoneset activate name  versastack-cluster vsan <<var_vsan_b_clus_id>>
sh zoneset active
copy run start
```

Storage Configuration

This section is about storage configuration. Encryption is used to improve security, and to save cost when disposing of drives. We also leverage IBM Real-time compression to reduce OPEX by reducing our storage footprint. Proper planning can optimize your performance and help reduce operational costs for your VersaStack.

Secure Web Access to the IBM FlashSystem V9000 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

Since we will implement encryption during our setup, we will need the licenses for this feature for both storage controllers. There is no trial license. We will also need three USB keys for our two control

enclosures, installed across both control enclosures to allow us to complete the encryption. The USB keys can be removed from the system after setup and kept in a secure location. Whenever an encryption-enabled V9000 system is powered on, it requires a USB key containing the correct encryption key to be plugged into a control enclosure. As such, it is recommended that one USB key is to remain installed in each system if you plan to allow automatic rebooting of the system should it be shut down for any reason. Alternatively, you would need to re-insert one USB key to reboot.

Three USB Drives Installed in the V9000

IBM FlashSystem V9000 Initial Configuration

If you are connecting multiple control enclosures for scale, the additional nodes will communicate through the Fibre Channel connection for initial discovery. To setup on node A only, complete the following steps:

1. Configure an Ethernet port of a PC/laptop to allow DHCP to configure its IP address and DNS.

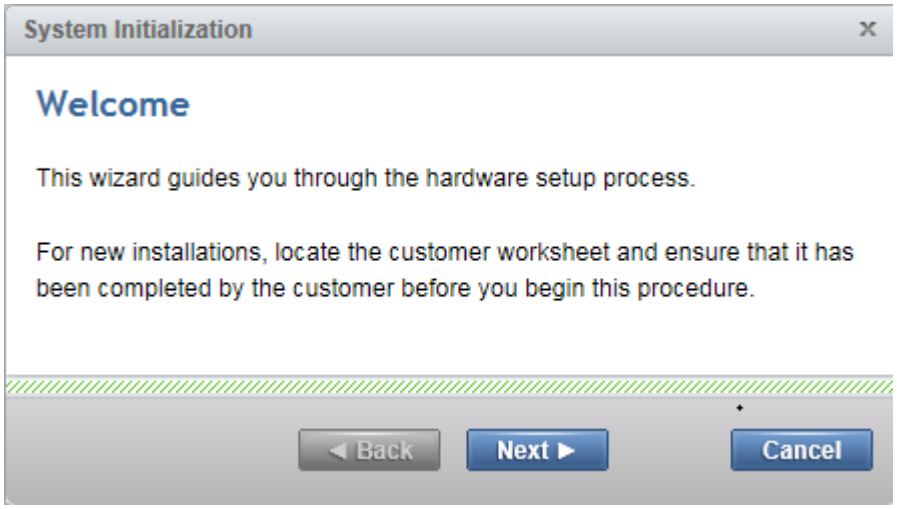
2. Connect an Ethernet cable from the PC/laptop Ethernet port to the Ethernet port labeled "T" on the rear of either node canister in the V9000 control enclosure.

3. A few moments after the connection is made, the node will use DHCP to configure the IP address and DNS settings of the laptop/PC.

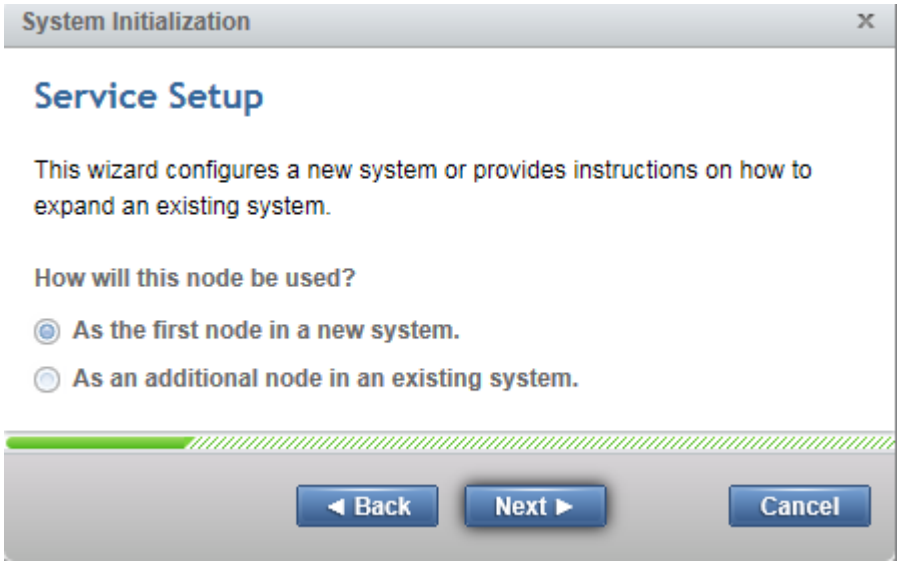
This will likely disconnect you from any other network connections you have on the laptop/PC. If you do not have DHCP on your PC/laptop, you can manually configure it with the following network settings: IPv4 address 192.168.0.2, mask to 255.255.255.0, gateway to 192.168.0.1, and DNS to 192.168.0.1

---

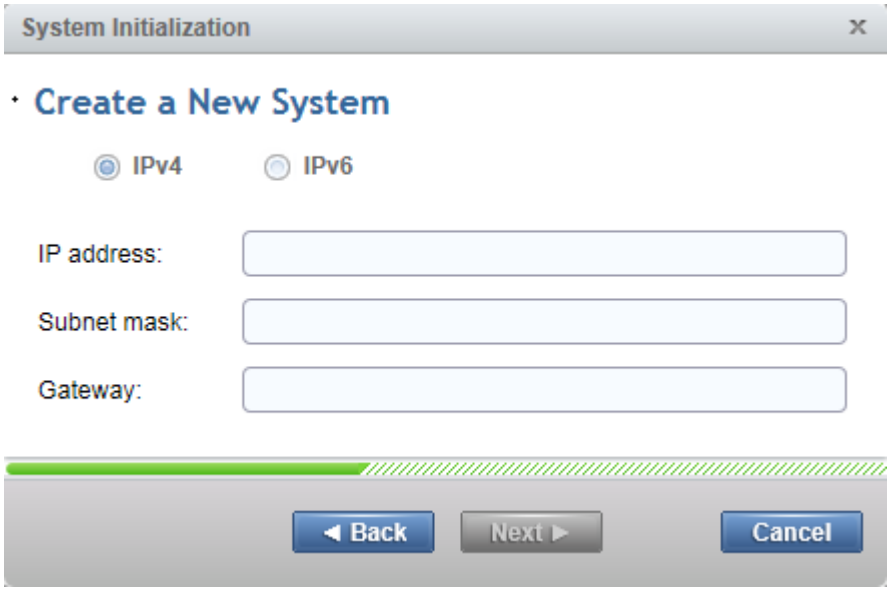
4. Open a browser and go to address https://install, which will direct you to the initialization wizard.



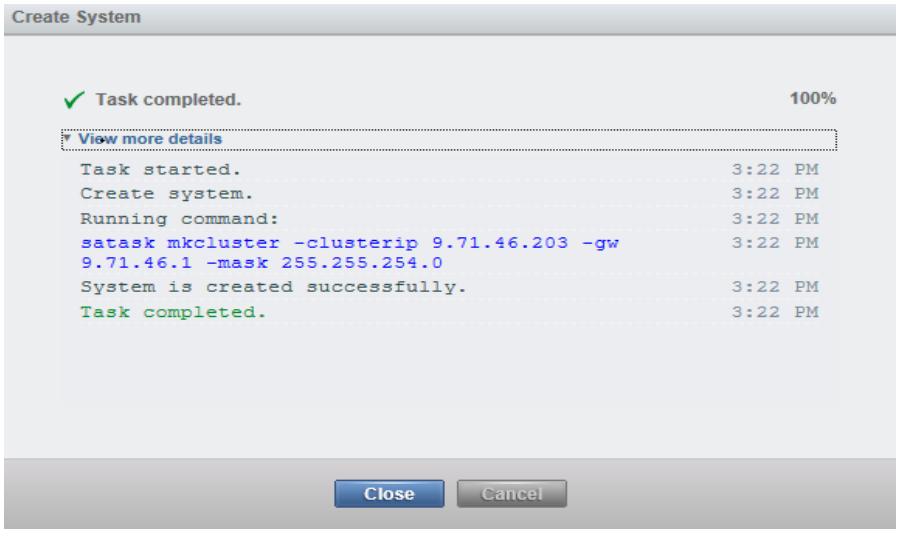
5. When asked how the node will be used, select "As the first node in a new system" and click Next.



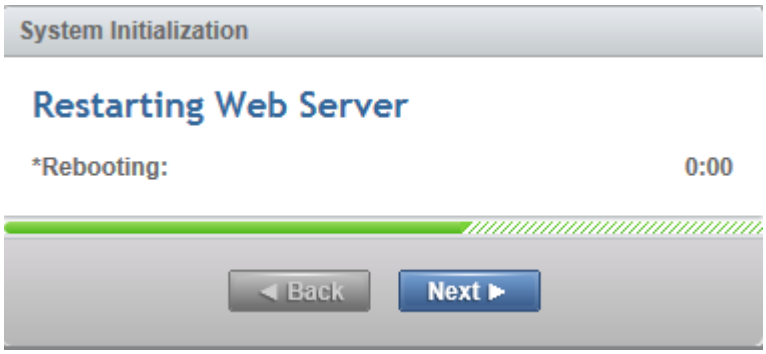
6. Follow the instructions that are presented by the initialization tool to configure the system with a management IP address <<var_cluster_mgmt_ip>>,<<var_cluster_mgmt_mask>> and <<var_cluster_mgmt_gateway>>, then click Next.

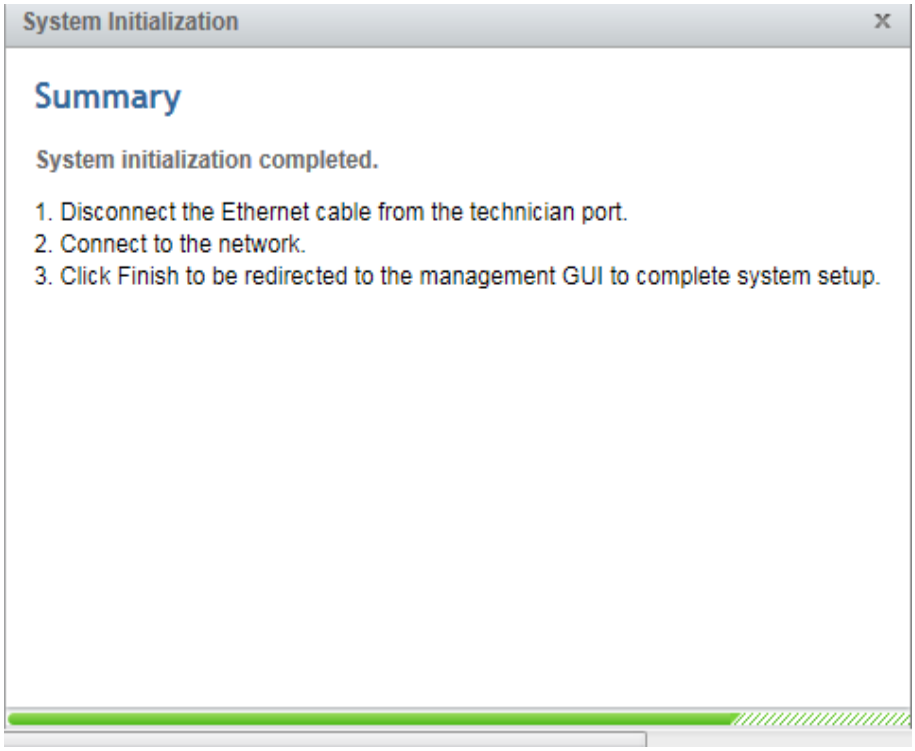


7. Click Close when the task is completed.



8. Click Next.





After you complete the initialization process, disconnect the cable as directed, between the PC/laptop and the technician port, and reconnect to your network with your previous settings. Your browser will be redirected the management GUI, at the IP address you configured.

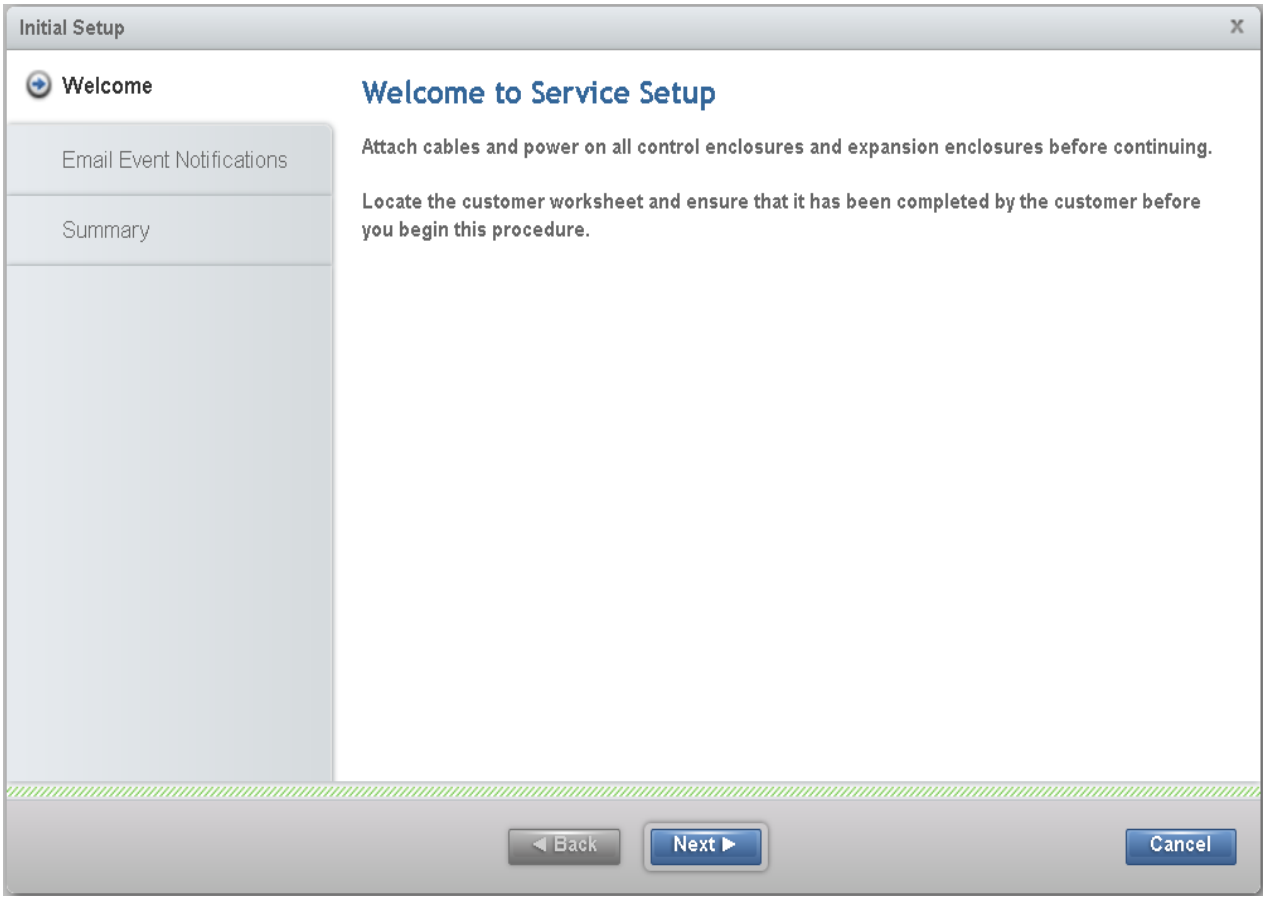
You may have to wait up to five minutes for the management GUI to start up and become accessible.

IBM FlashSystem V9000 SSR Initialization

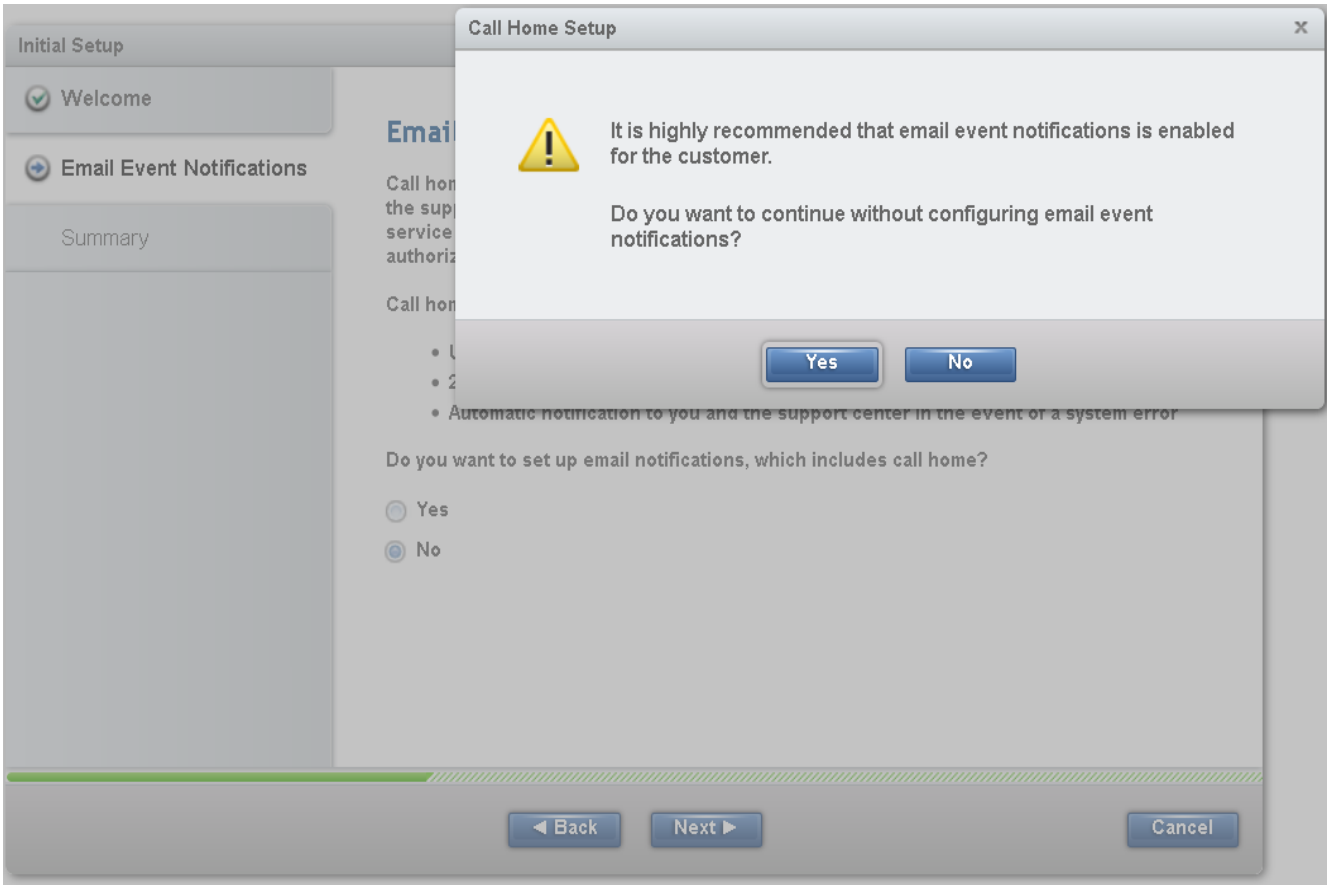
To initialize IBM FlashSystem V9000 SSR, complete the following steps:

1. Use “password” for the Password field and log in.

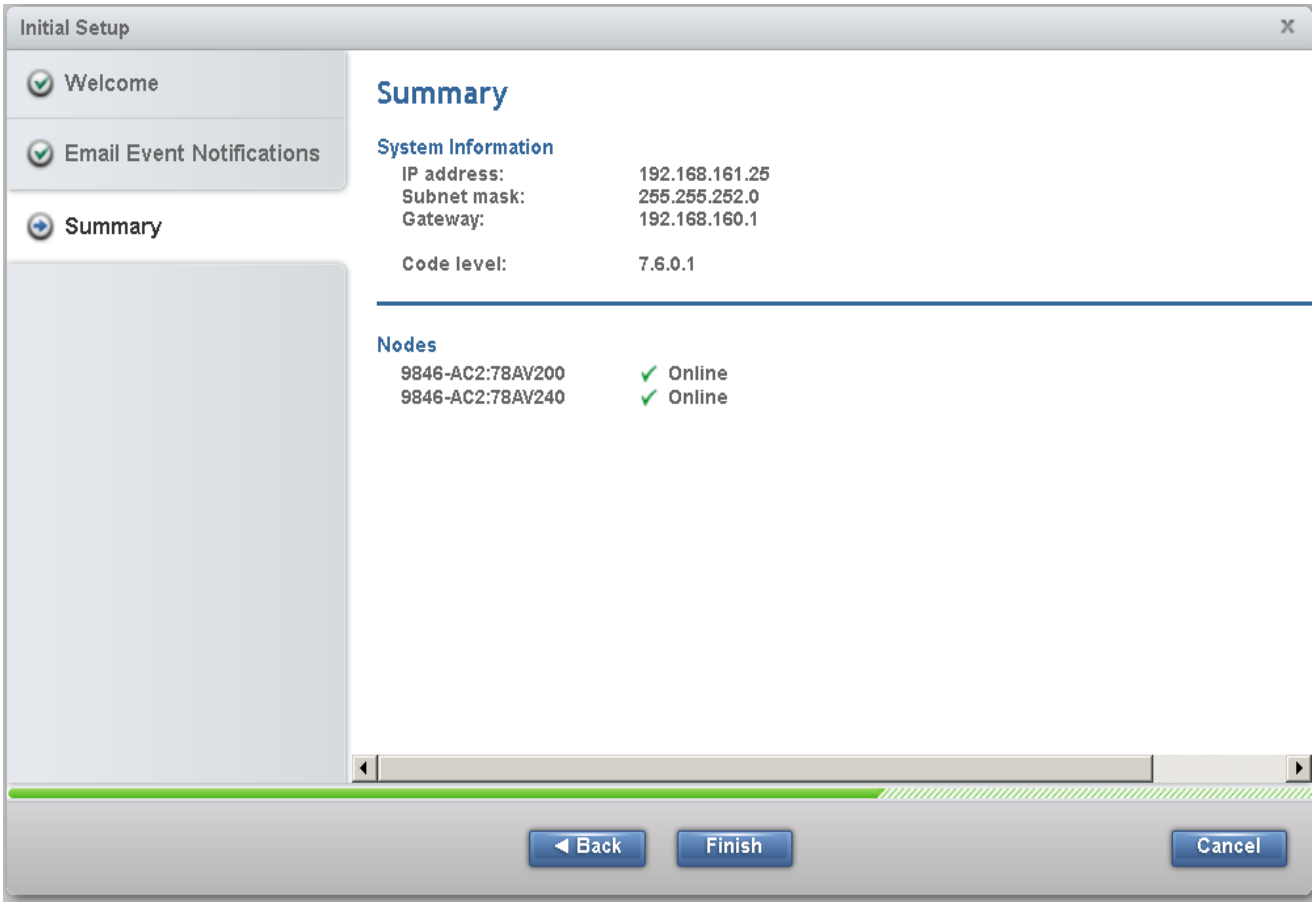
2. Click Next.



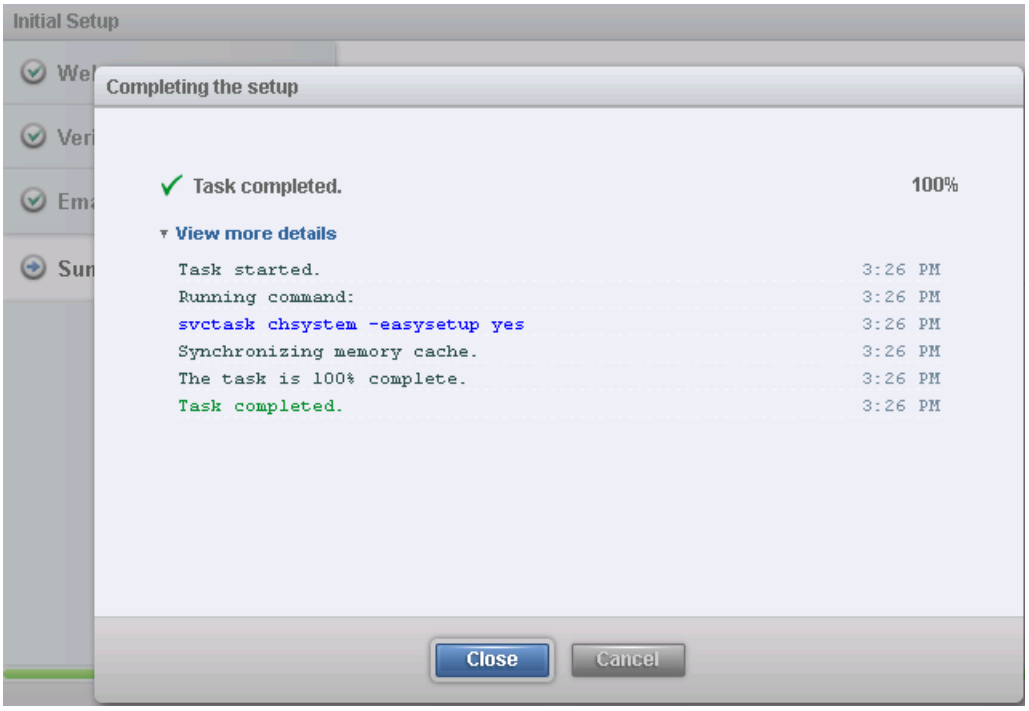
3. During the next wizard the prompt for Call Home information will be presented again, so select No here then Yes on the popup dialog to continue.



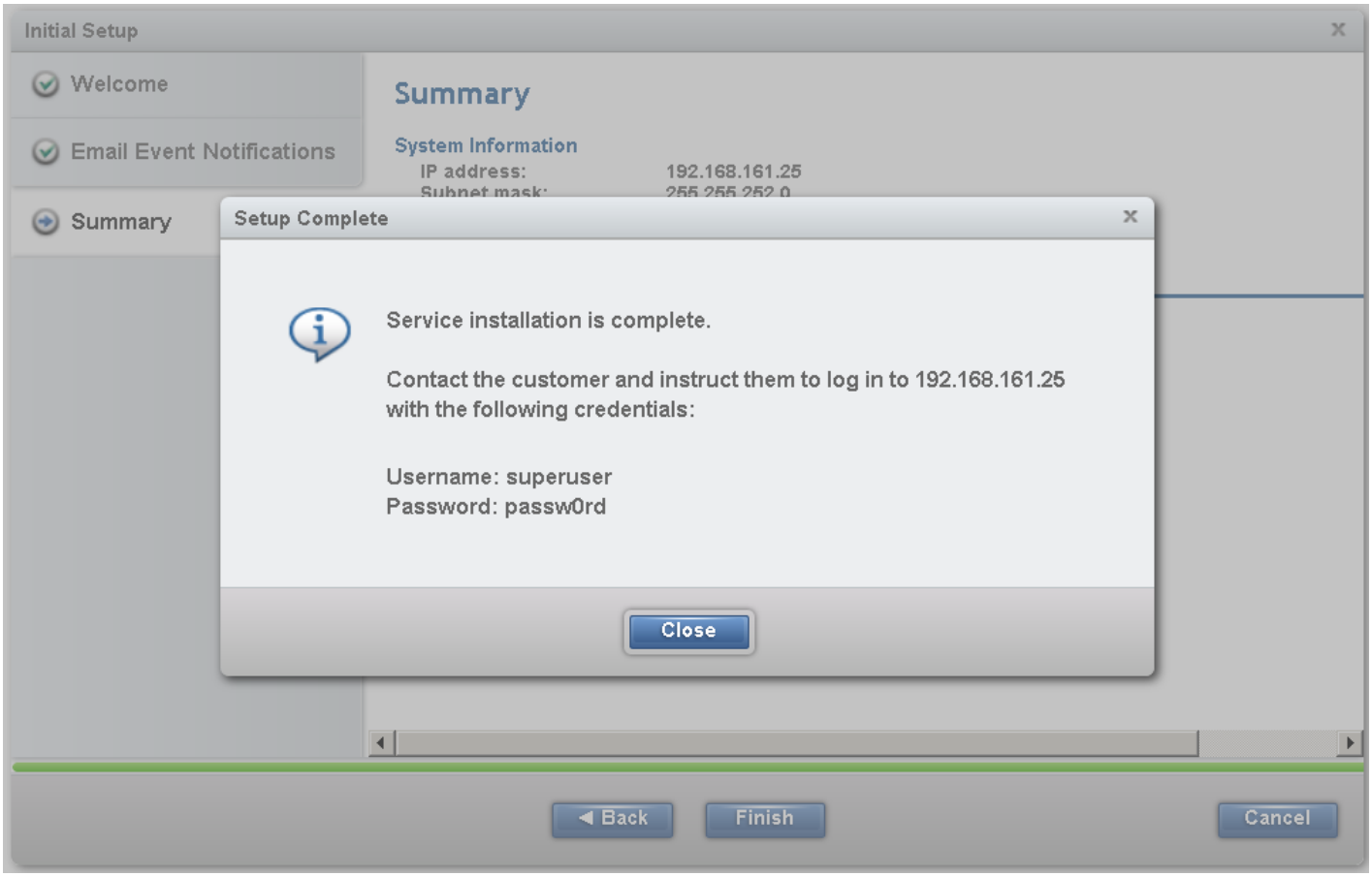
4. Verify the information, click Finish.



5. The task runs briefly (around 20 seconds). Close the dialog to continue.



6. Information panel displays the cluster ipaddress, and default userid and password to proceed to the next wizard with. Click Close to continue.



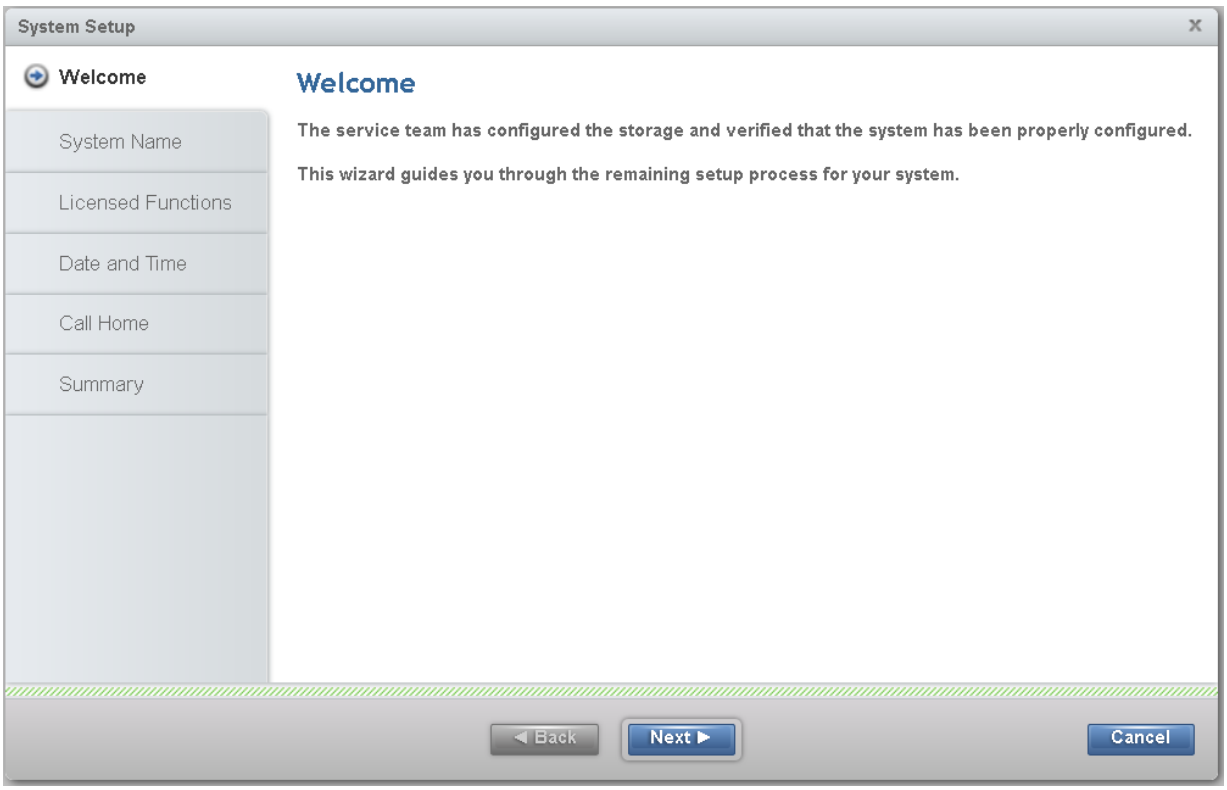
IBM FlashSystem V9000 Initial Configuration Setup

To configure the IBM FlashSystem V9000, complete the following steps:

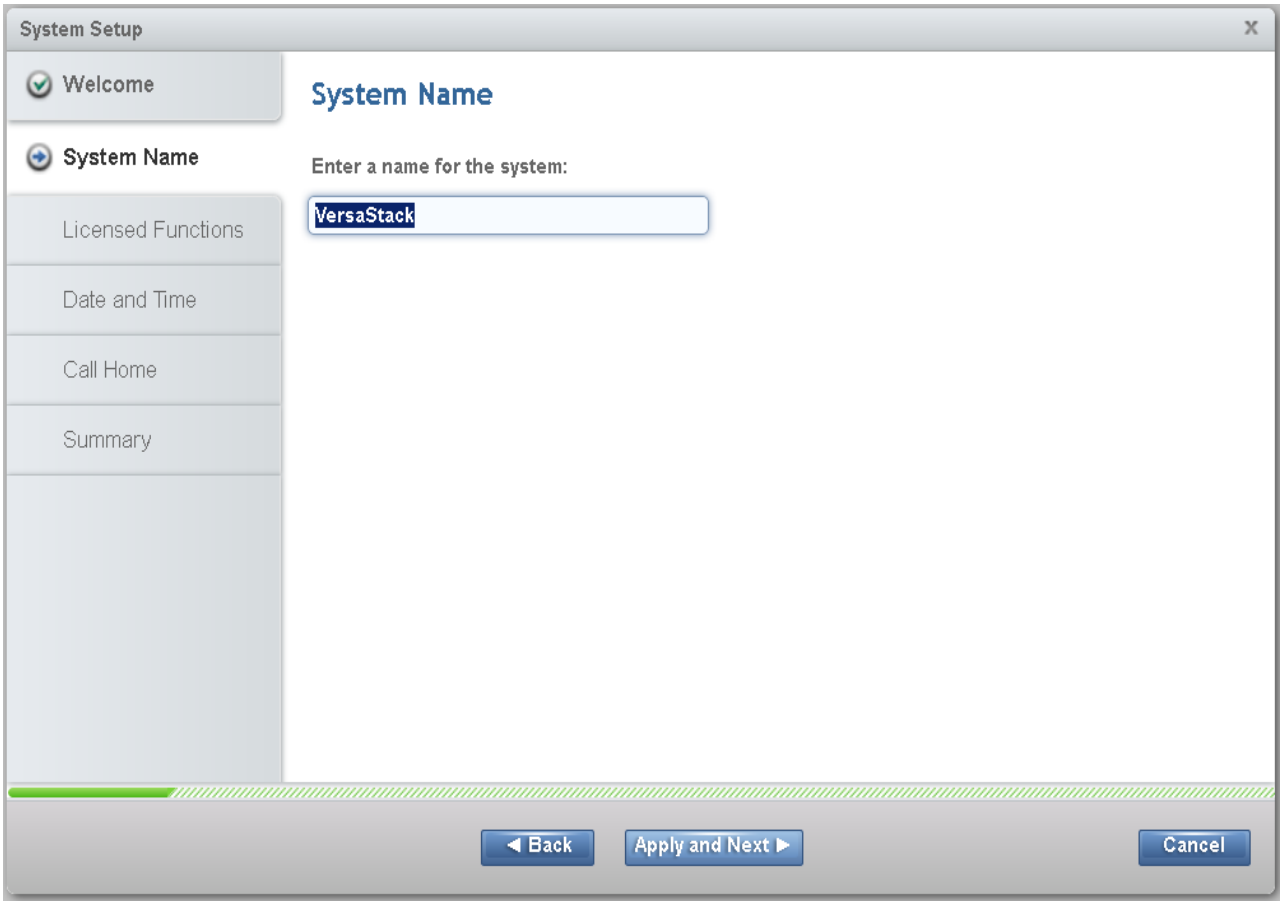
1. Read and accept the license agreement.

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

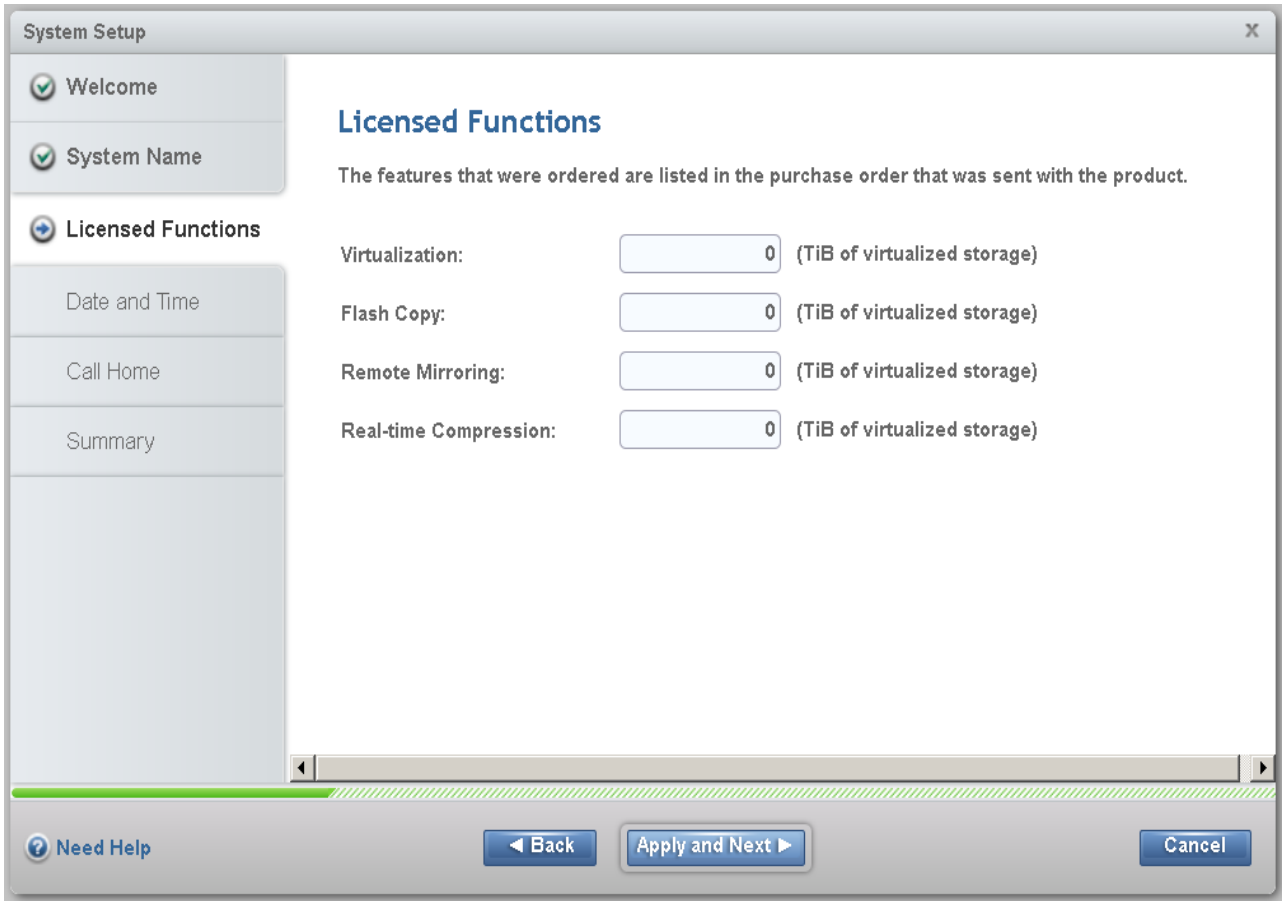
3. In the welcome to system setup screen click Next.



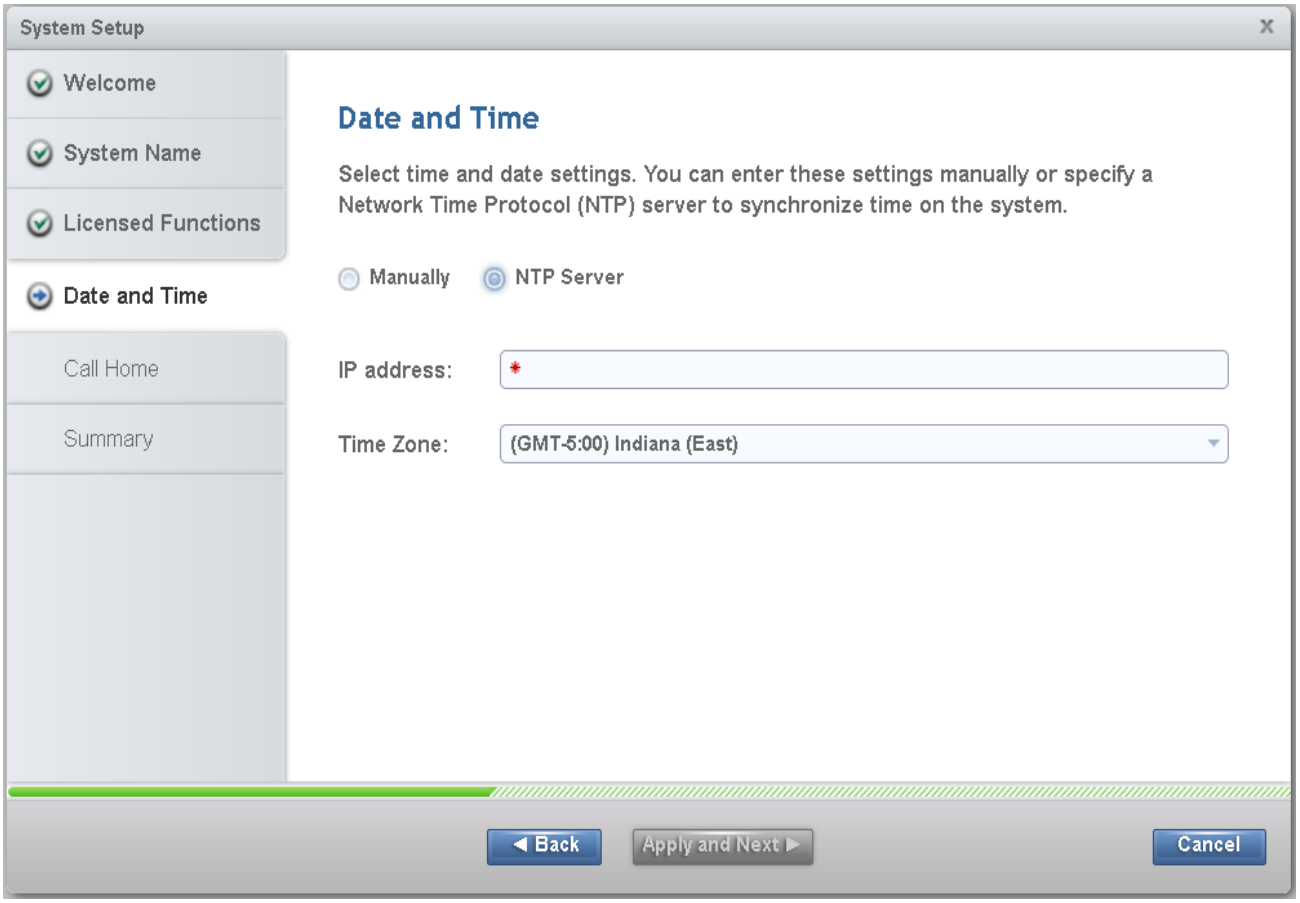
4. Enter the System Name and click Apply and Next to proceed.



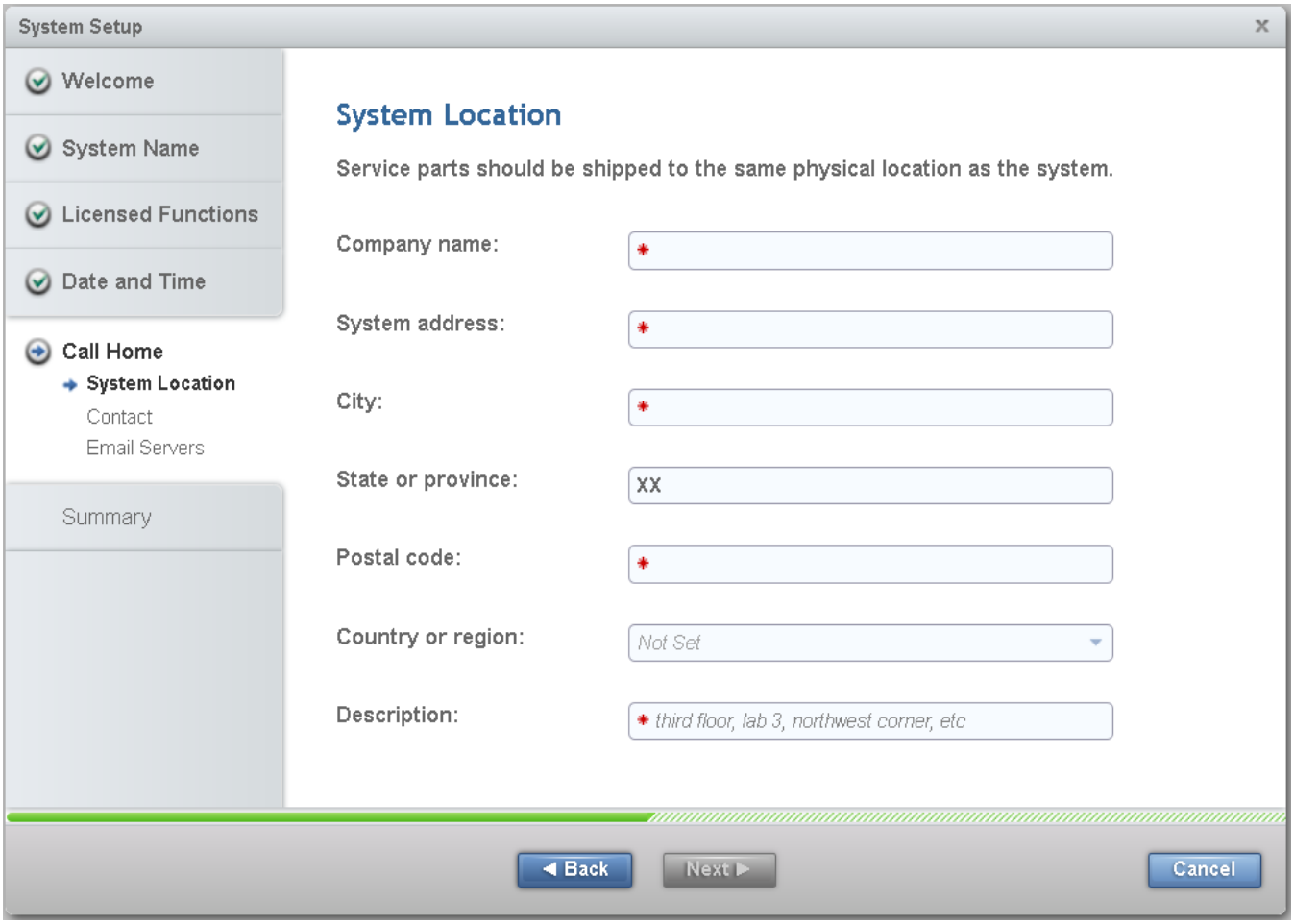
5. Enter the number of licenses and click Apply and Next.



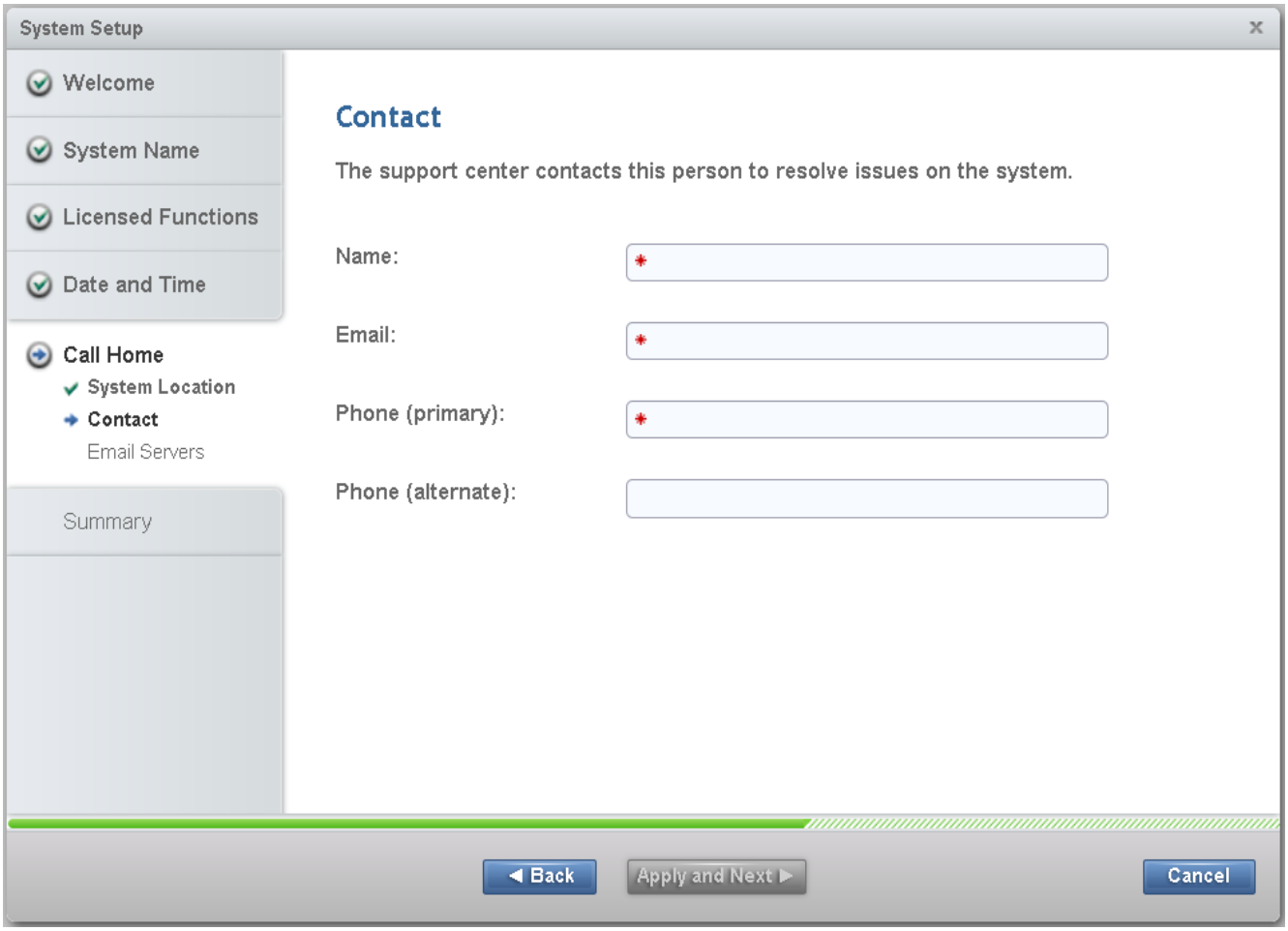
6. Select NTP Server and enter the address of the server then click Apply and Next, then click Close.



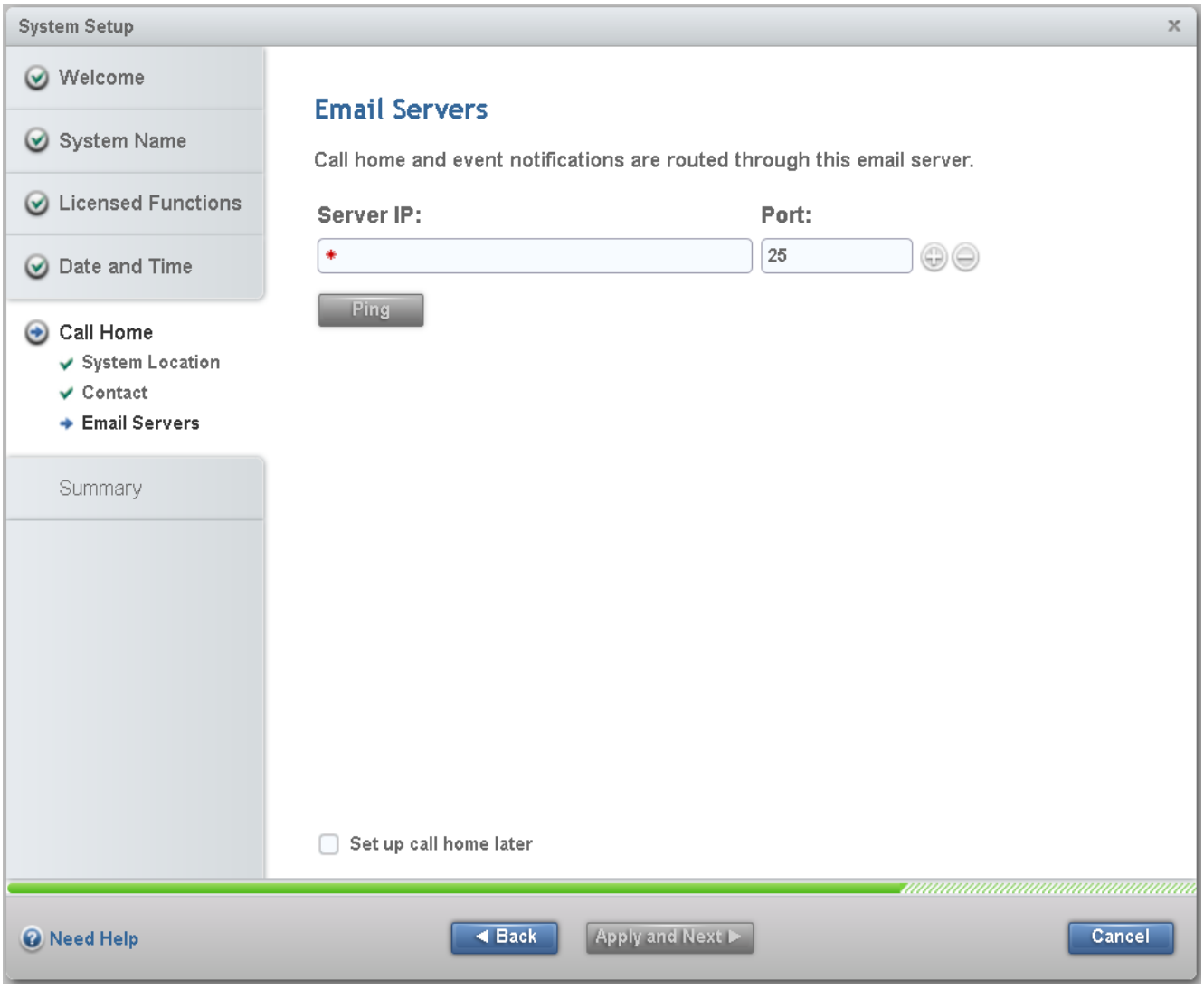
7. Fill out system location and contact details <<var_org>>, <<var_street_address>>, <<var_city>> <<var_state>>, <<var_zip>>, <<var_country_code>> then click Next.



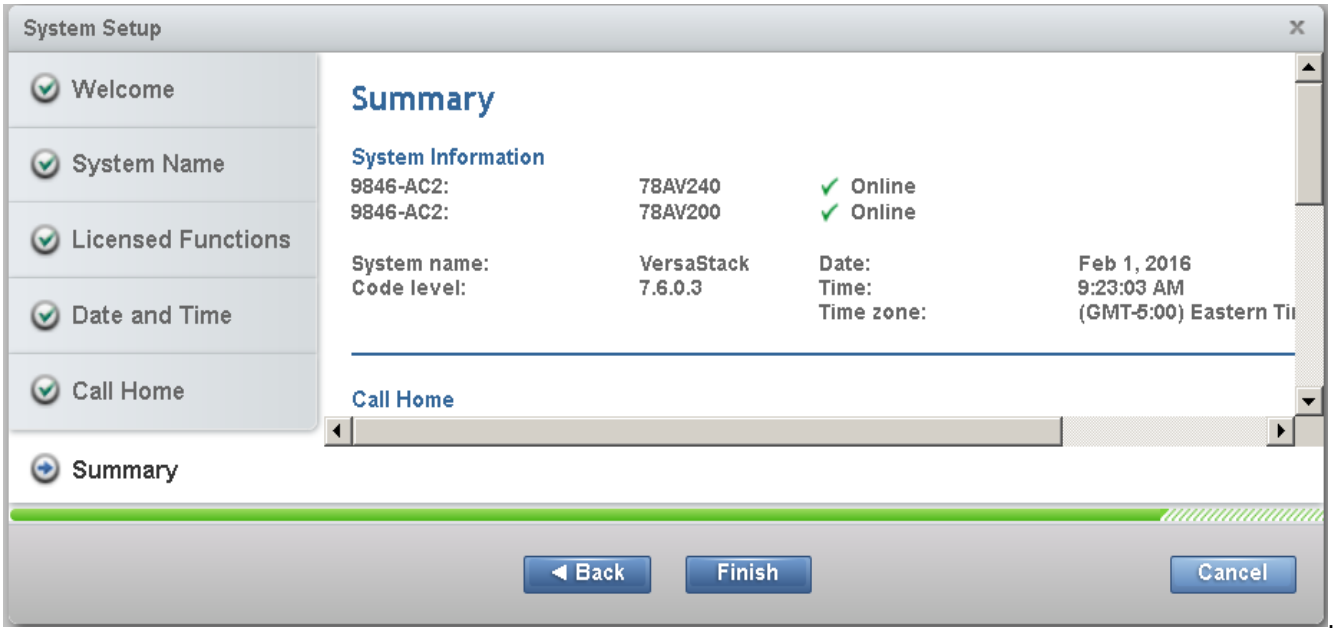
8. Insert Contact Details <<var_contact_name>>, <<var_email_contact>>, <<var_admin_phone>>, <<var_city>> then Click Apply and Next and click Close.

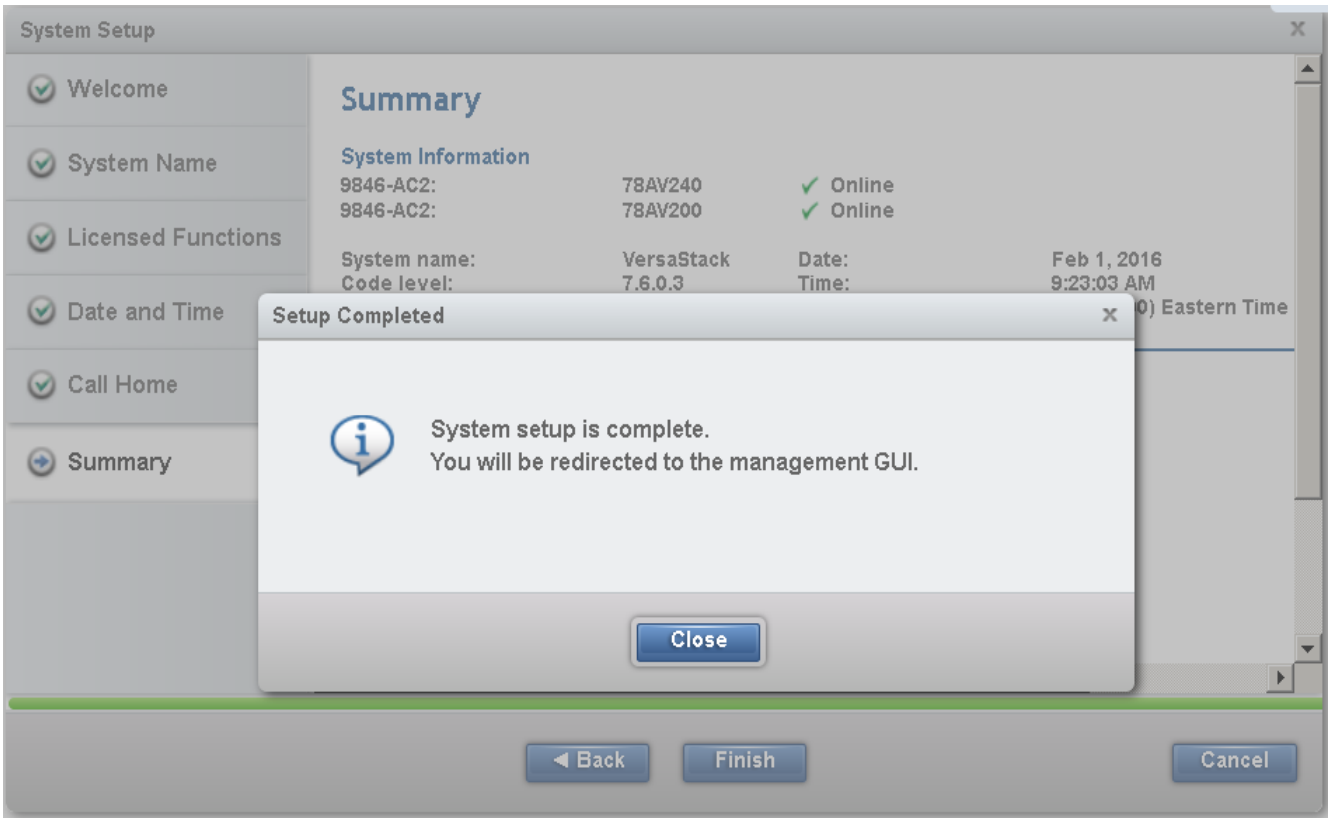


9. Input the email server IP address <<var_mailhost_ip>> and change the port if necessary, then click Apply and Next, then Close.



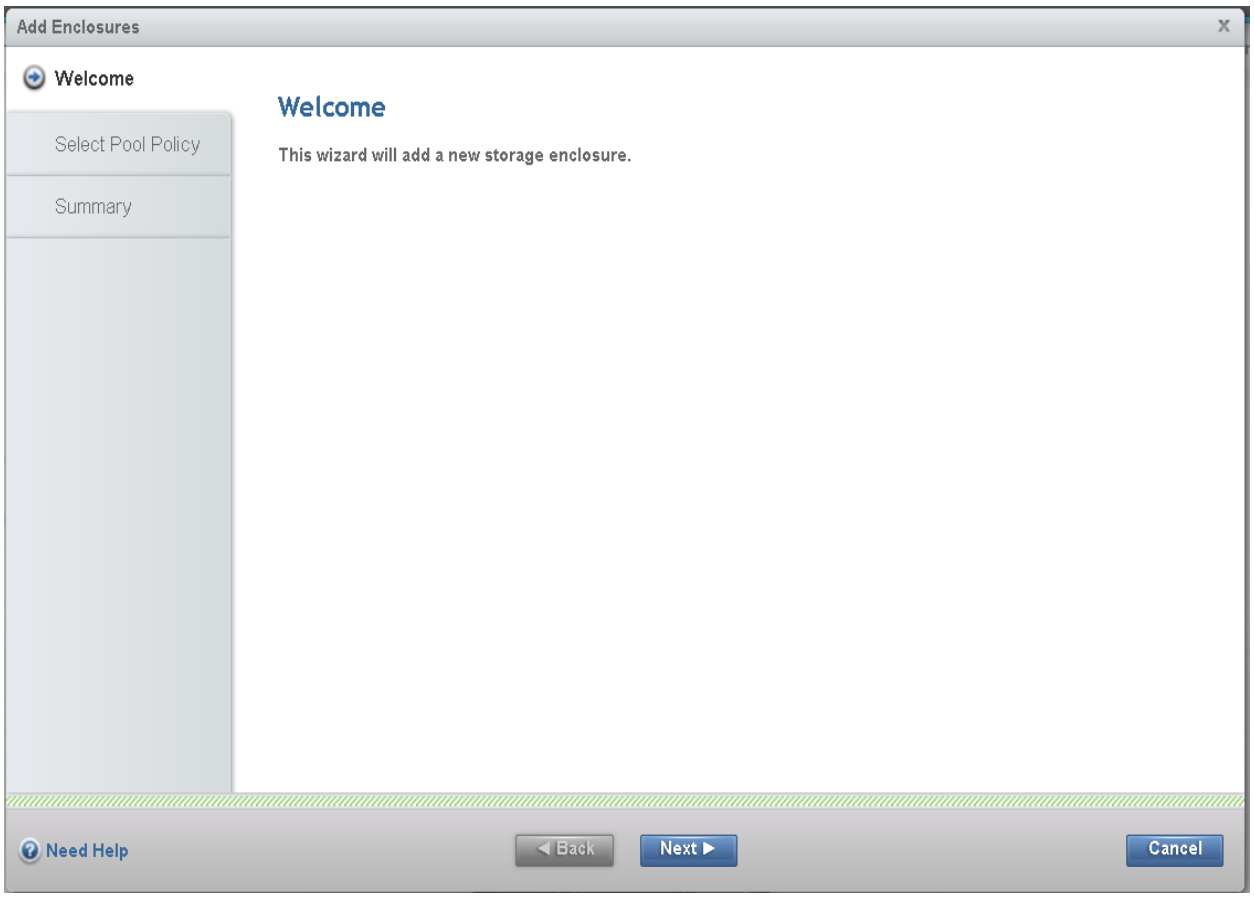
10. Review the Summary screen and Click Finish, then click Close after tasks have completed.

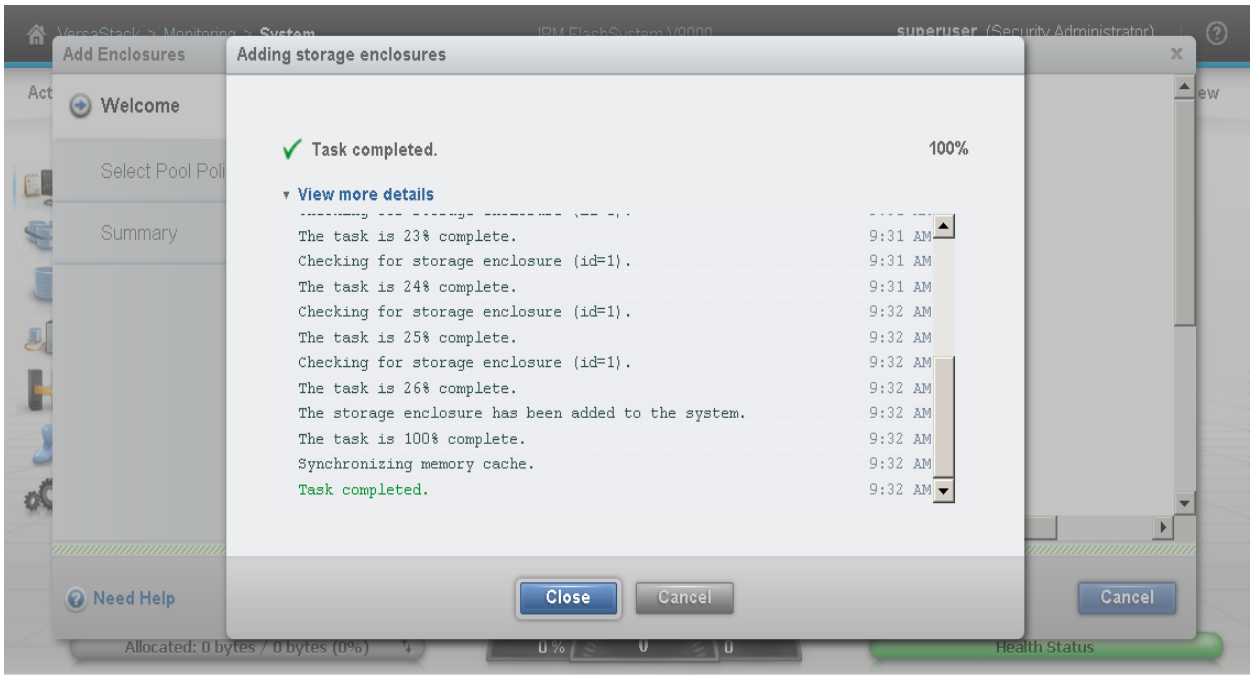




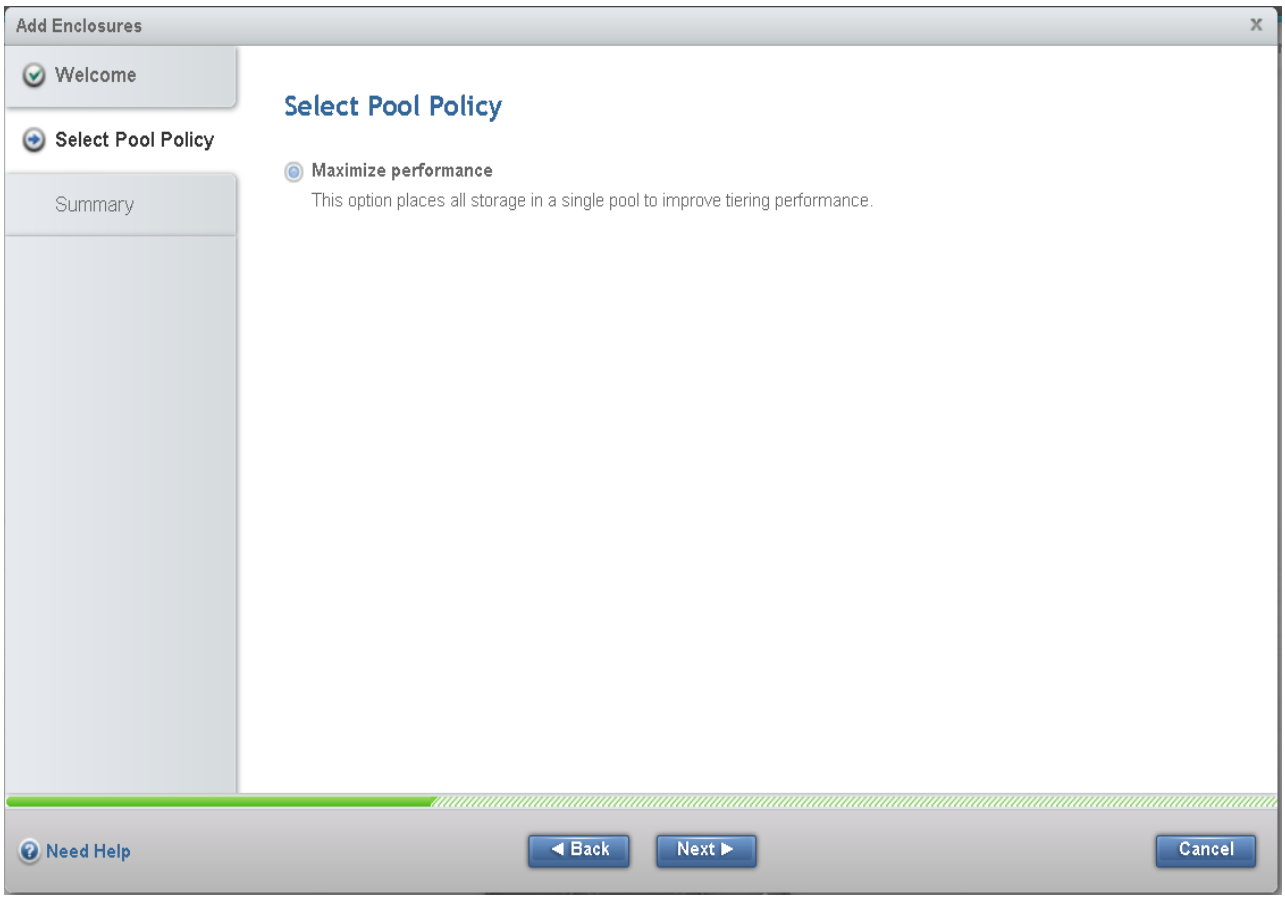
11. On Home screen, click on the enclosure to the right (indicated by the fly over labeled “Click to add additional storage”).

12. Click Next, then Close once the task dialog completes.

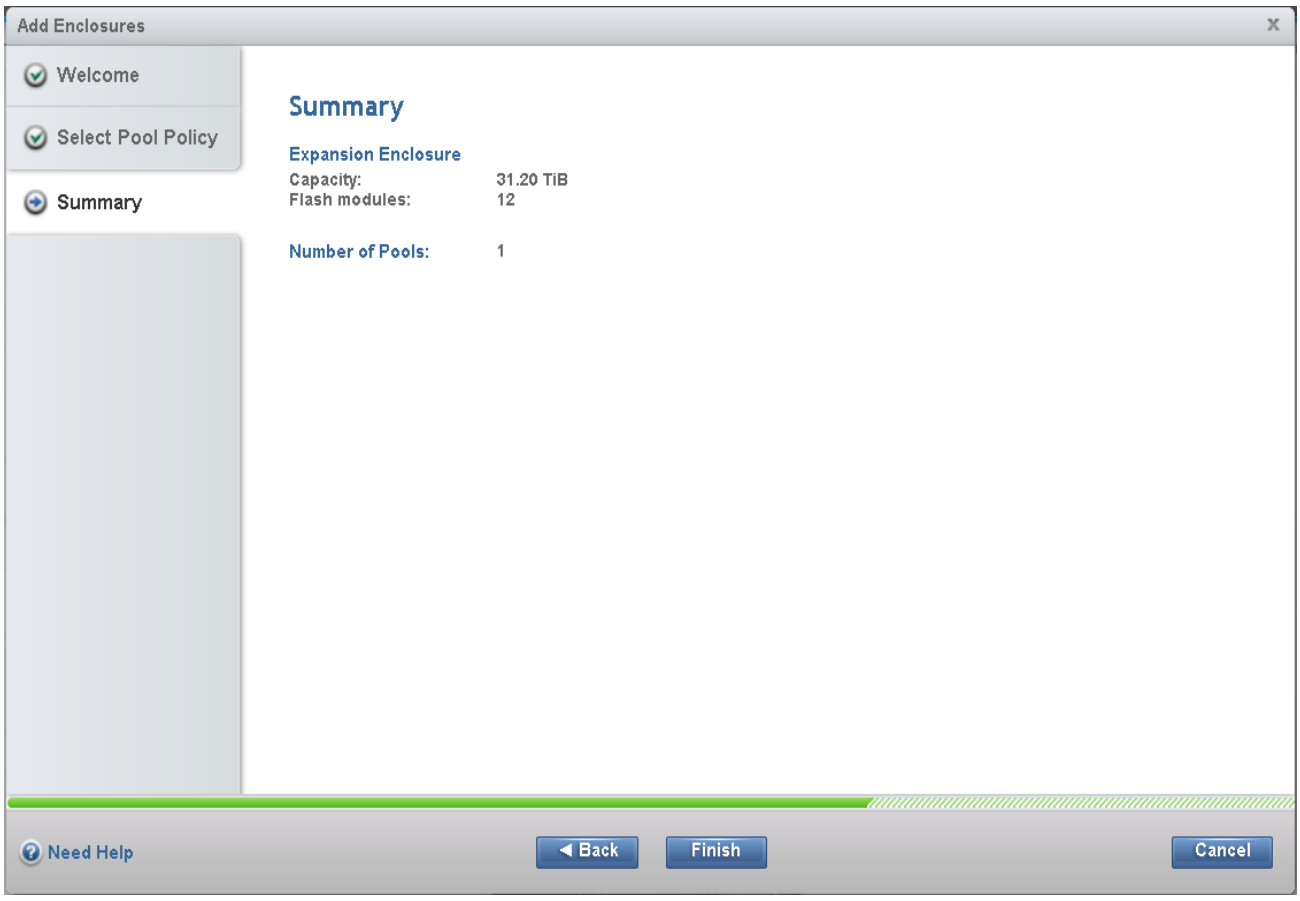


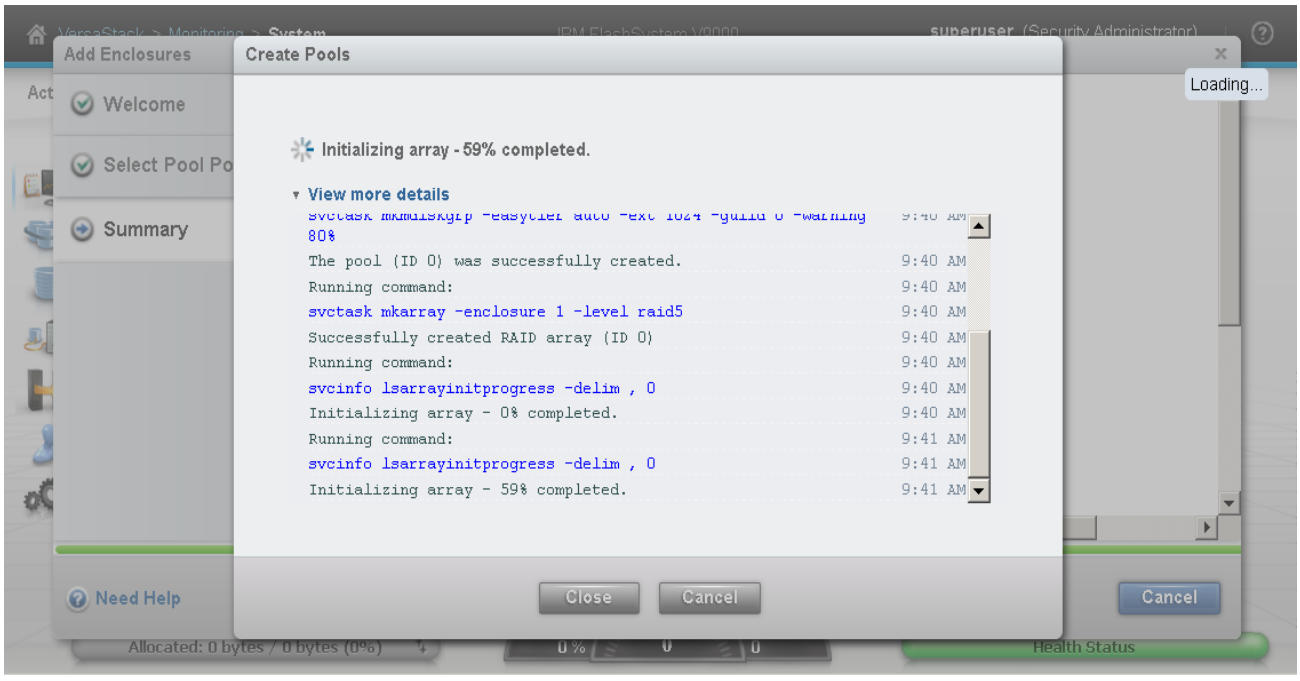


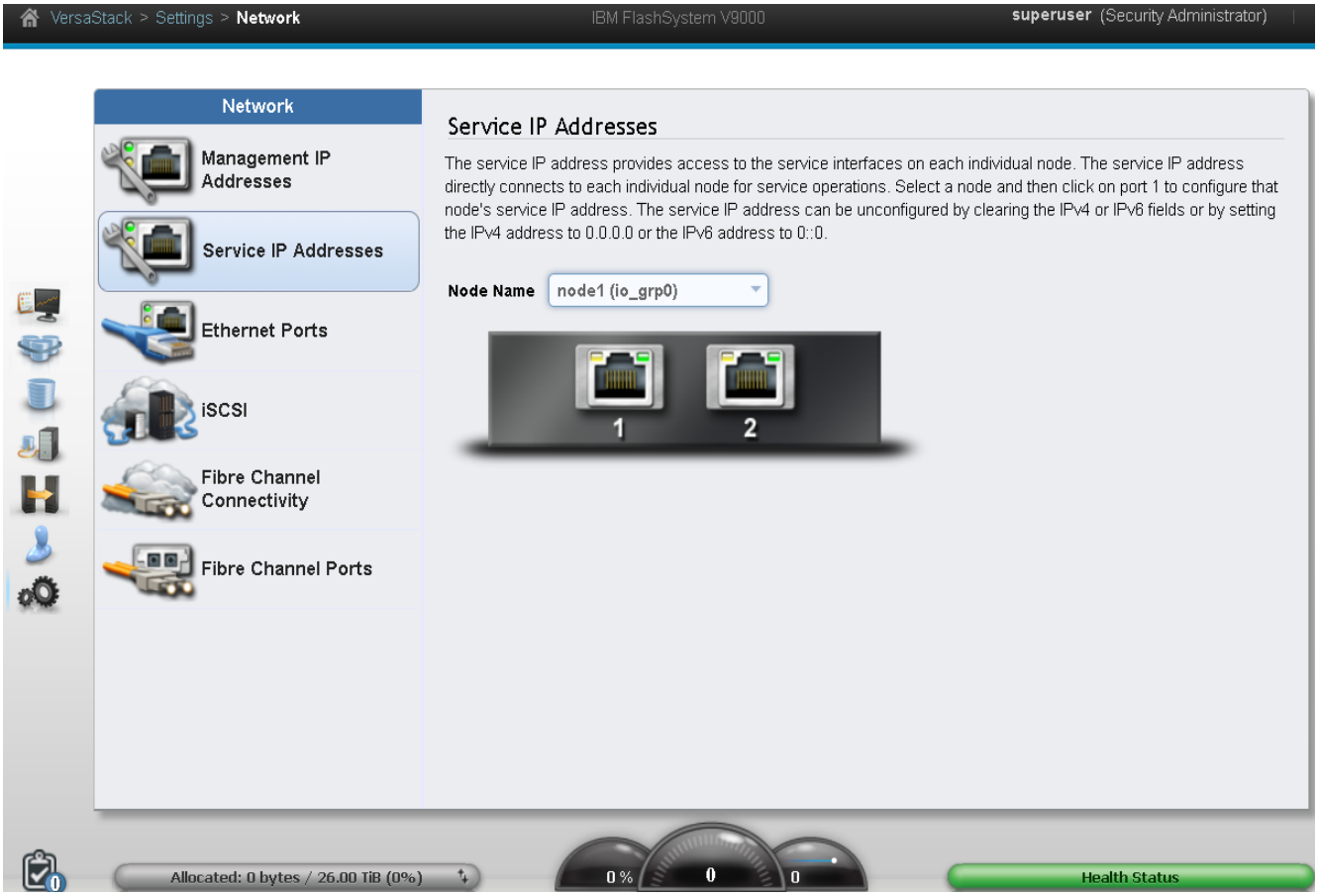
13. Click Next (keeping Pool Policy selection of Maximum Performance).



14. Click Finish, then Close once the task dialog completes.


Add Enclosures
Welcome
Select Pool Policy
Summary
Summary
Expansion Enclosure
Capacity: 31.20 TiB
Flash modules: 12
Number of Pools: 1
Need Help
Back
Finish
Cancel


Add Enclosures
Welcome
Select Pool Po
Summary
Create Pools
Initializing array - 59% completed.
View more details
80%
The pool (ID 0) was successfully created. 9:40 AM
Running command: 9:40 AM
svctask mkarray -enclosure 1 -level raid5 9:40 AM
Successfully created RAID array (ID 0) 9:40 AM
Running command: 9:40 AM
svcinfo lsarrayinitprogress -delim , 0 9:40 AM
Initializing array - 0% completed. 9:40 AM
Running command: 9:41 AM
svcinfo lsarrayinitprogress -delim , 0 9:41 AM
Initializing array - 59% completed. 9:41 AM
Close
Cancel
Loading...
Need Help
Cancel
Allocated: 0 bytes / 0 bytes (0%)
Health Status

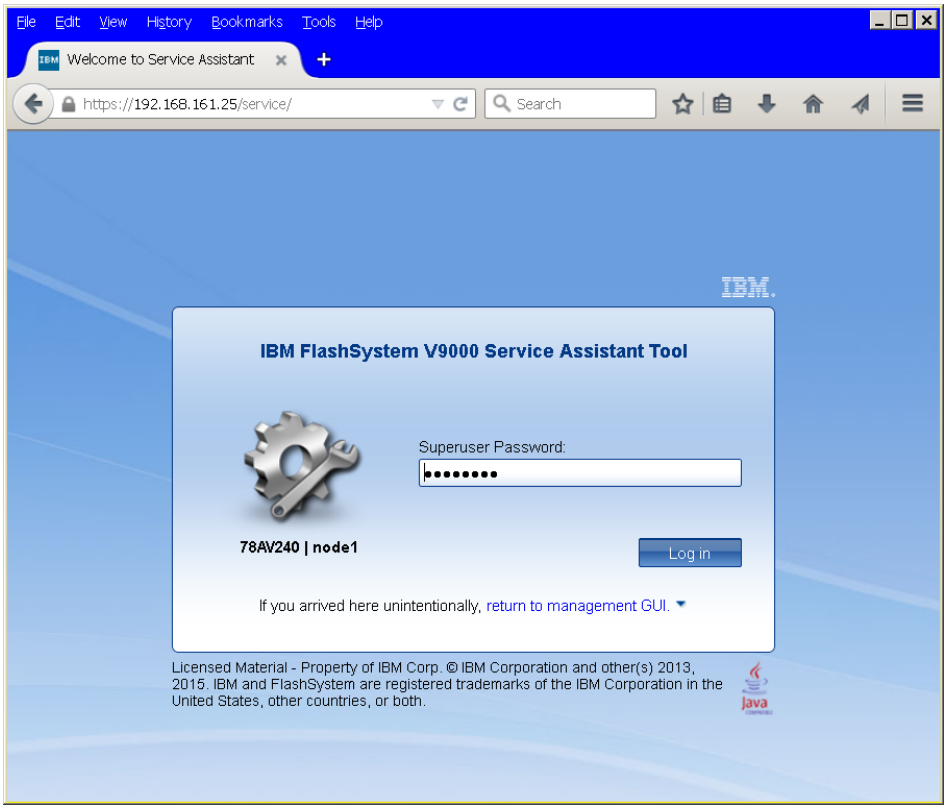


15. Using the lower left Setting navigation, select Network, then highlight the Service IP Addresses section and click interface 1. Change the IP address if necessary and click OK.

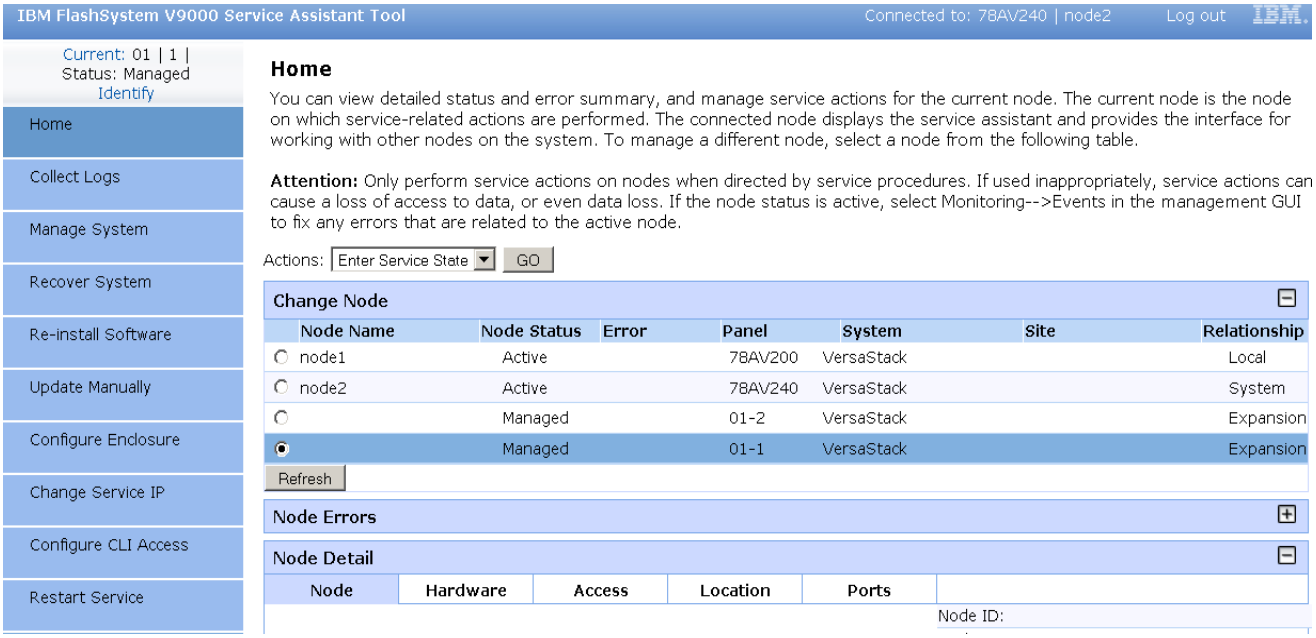
16. Select the Node Name drop-down and select node2.

17. Click node2. Change the IP address if necessary and click OK.

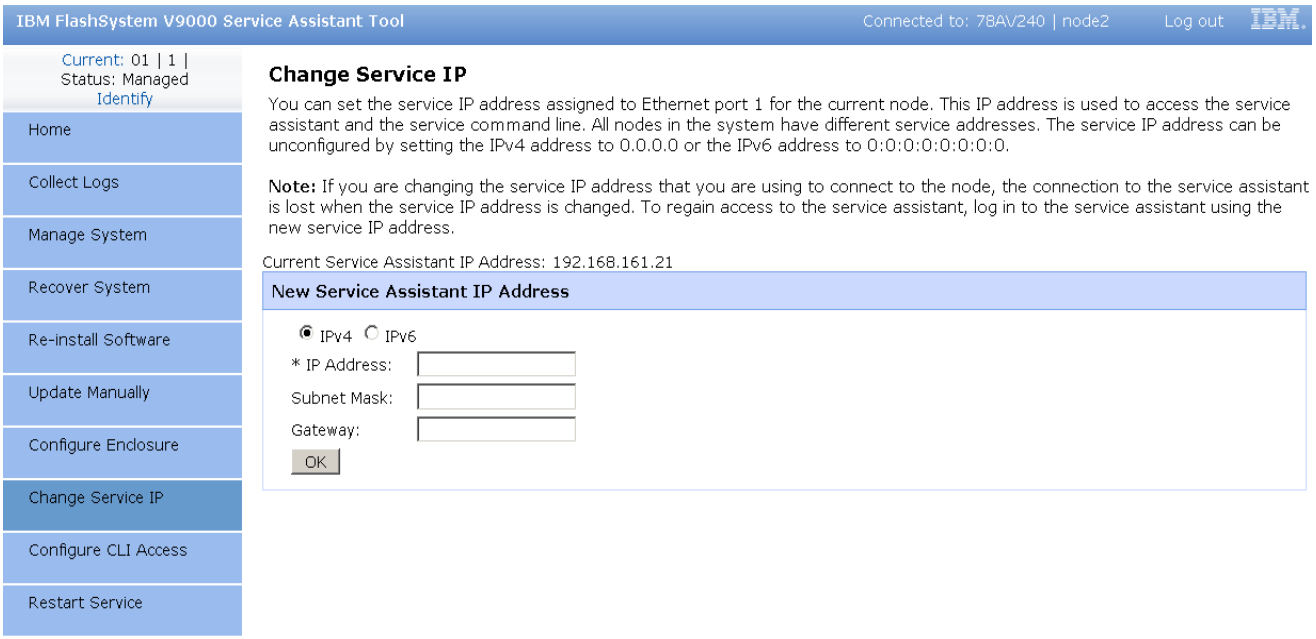
18. Open another browser session to URL, enter the ipaddress of the cluster, followed by /service. (“<<var_cluster_mgmt_ip>>/service”) Enter the superuser password (set on step 4), and click “Log in”.



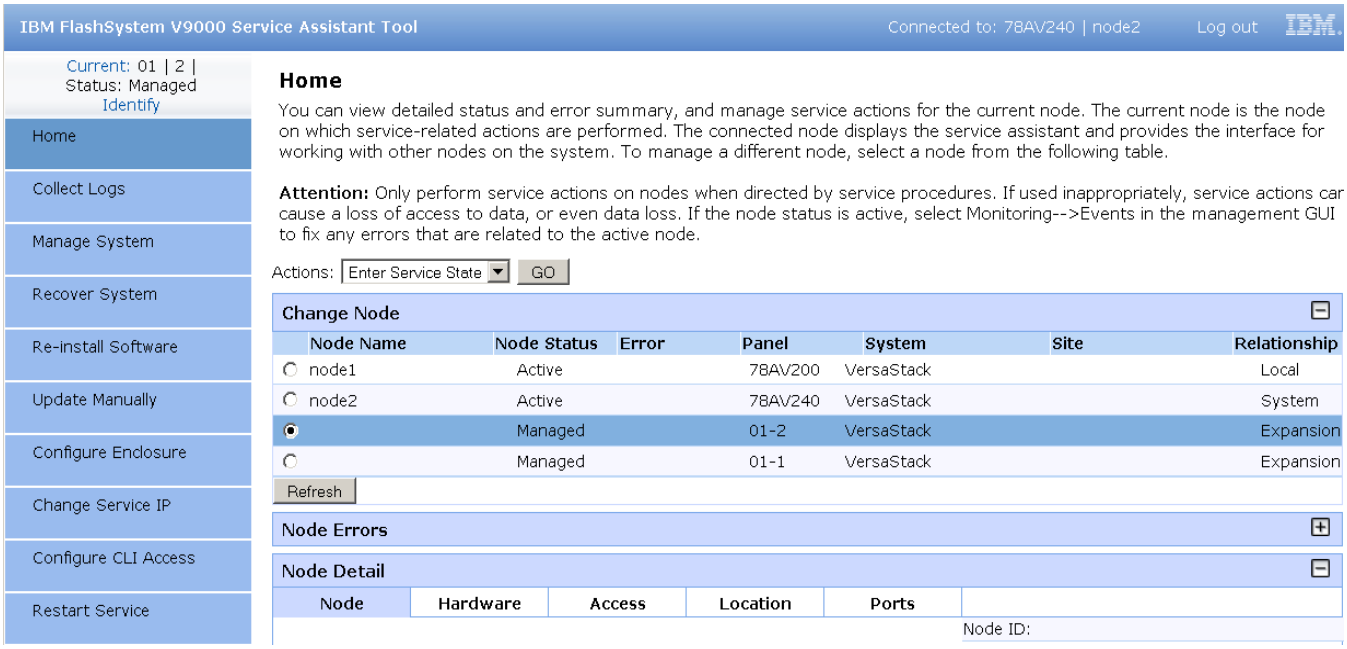
19. Click the radio button on Panel 01-1, then from the left navigation click Change Service IP.



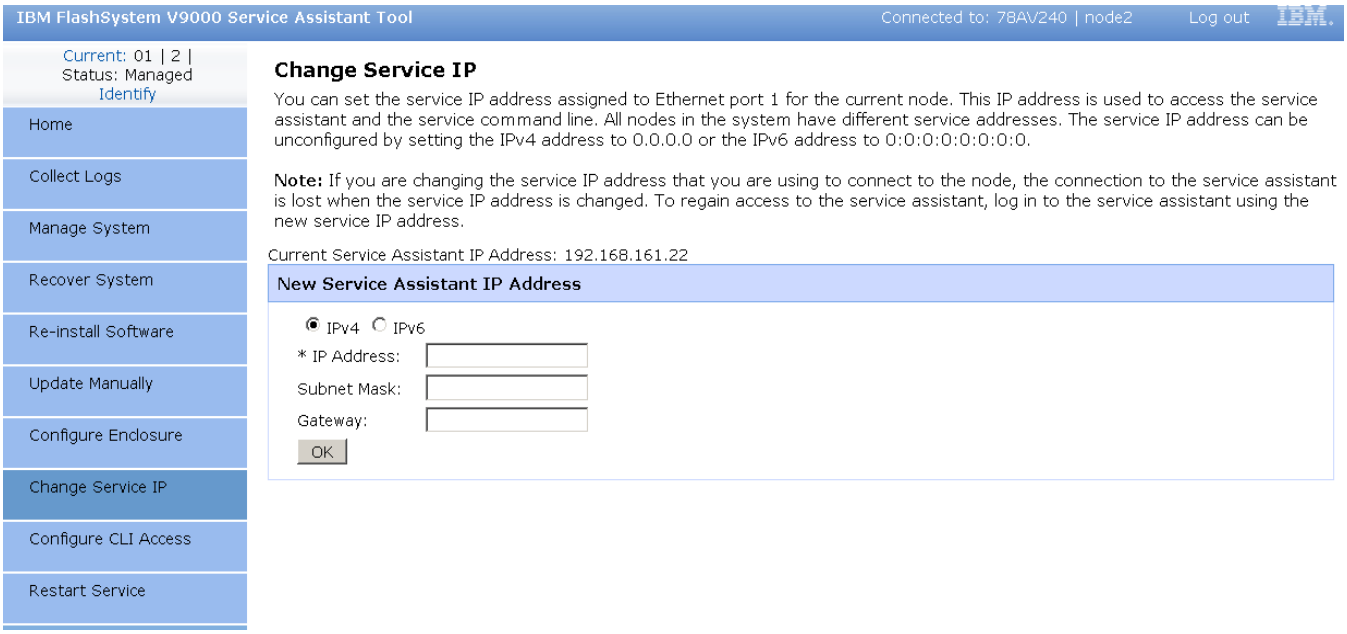
20. Enter <<var_can01_srvc_ip>> for IPAddress, <<var_can_srvc_mask>> for Subnet Mask, <<var_can_srvc_gateway>> for Gateway, then click OK.



21. From left navigation click Home, select the radio button for Panel 01-2, then click Change Service IP.

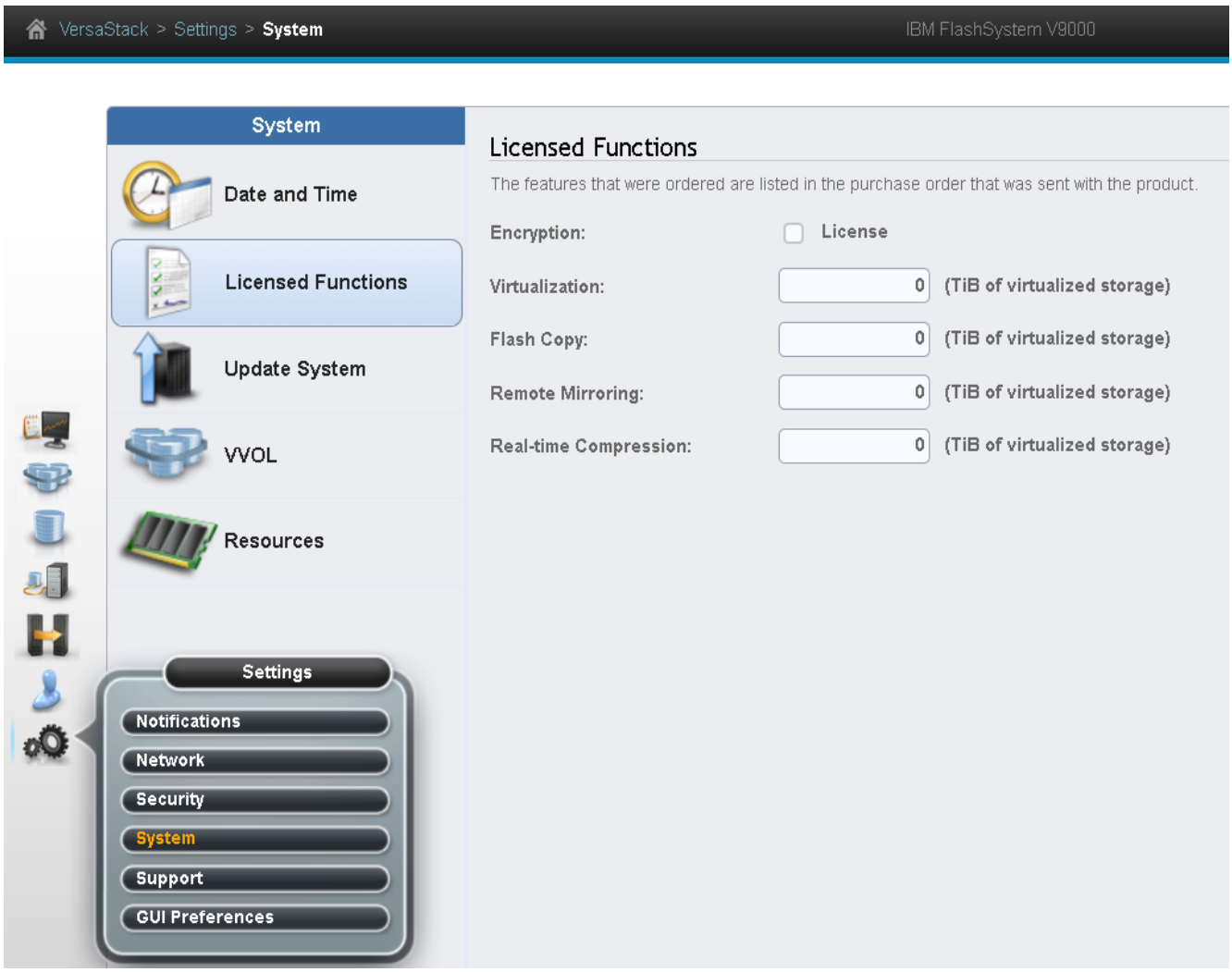


22. Enter <<var_can02_srvc_ip>> for IPAddress, <<var_can_srvc_mask>> for Subnet Mask, <<var_can_srvc_gateway>> for Gateway, then click OK.

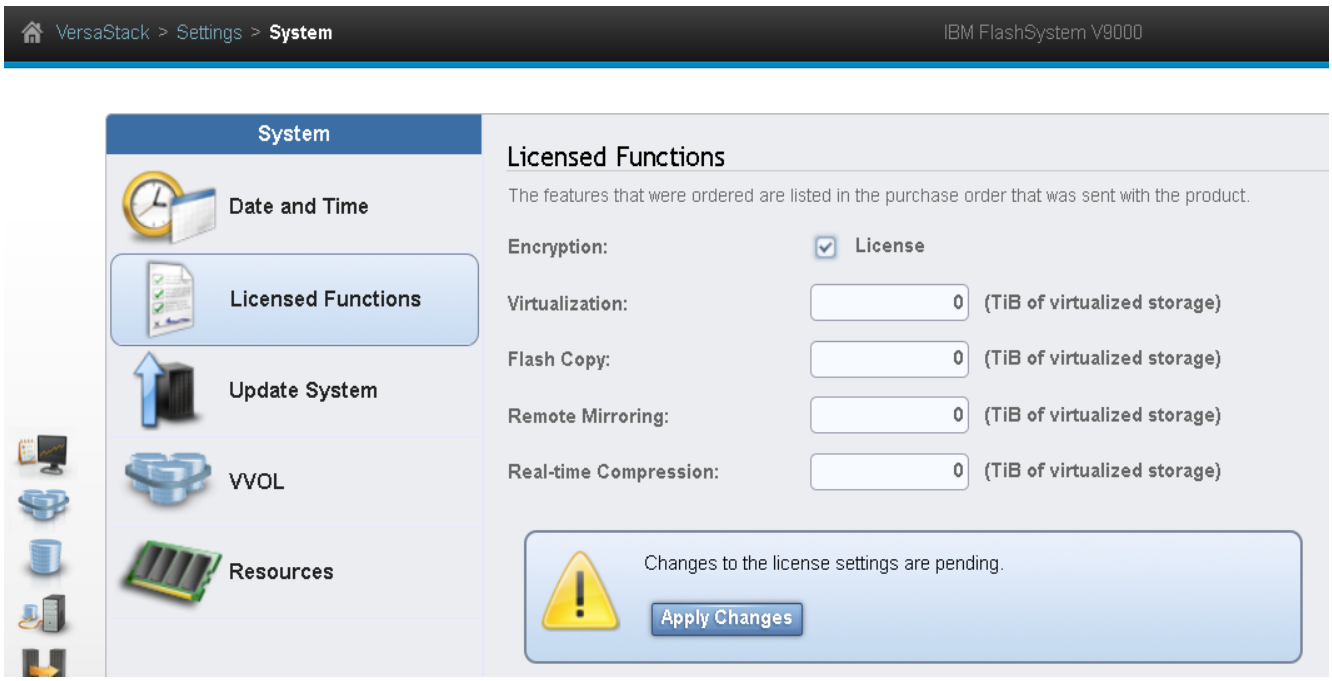


23. Close this browser session and return to the main V9000 GUI browser session.

24. From the Settings icon in the left pane, select System.

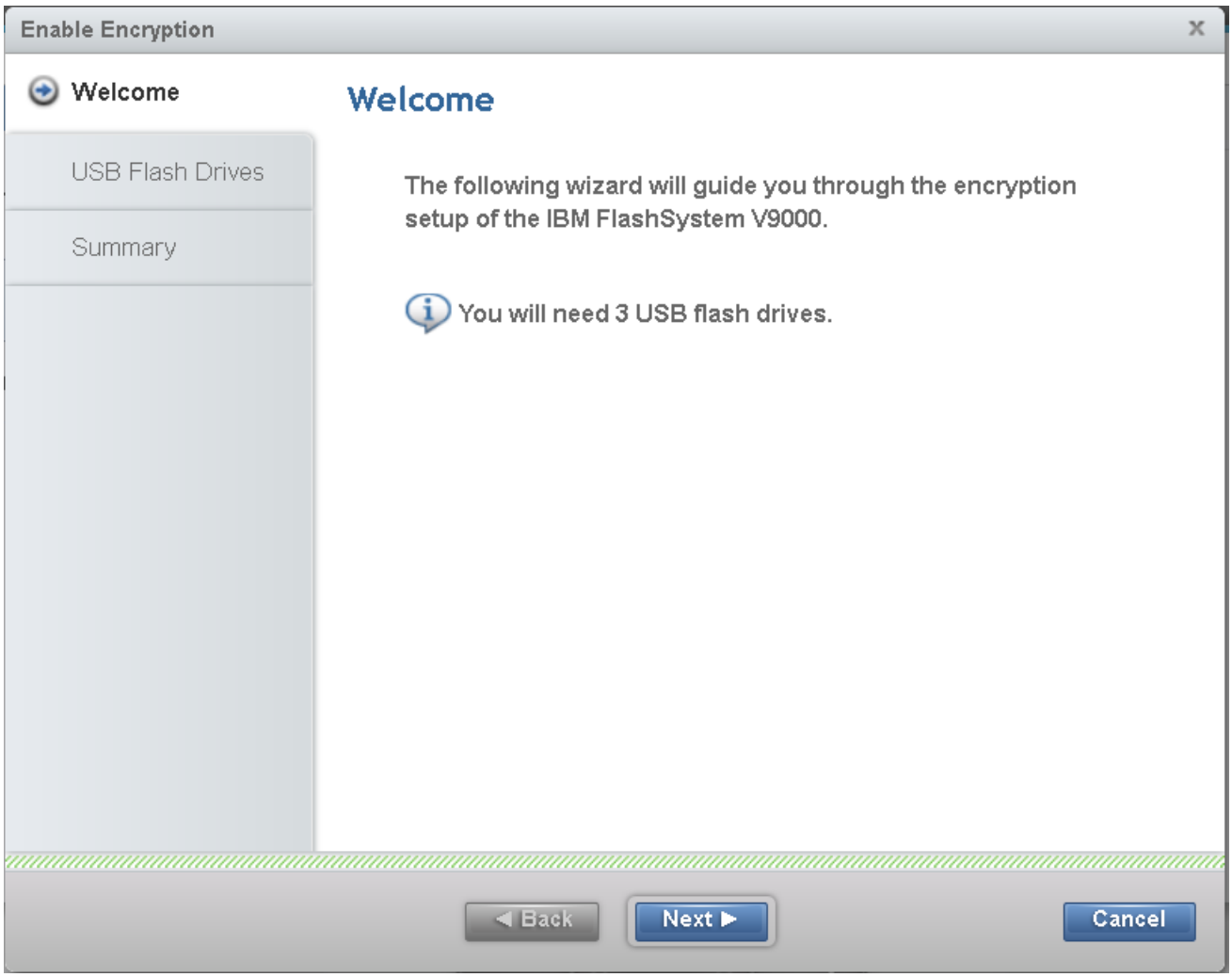


25. Select Licensed Functions, and select the Encryption License (if you have purchased that). Click Apply Changes, and then Close.



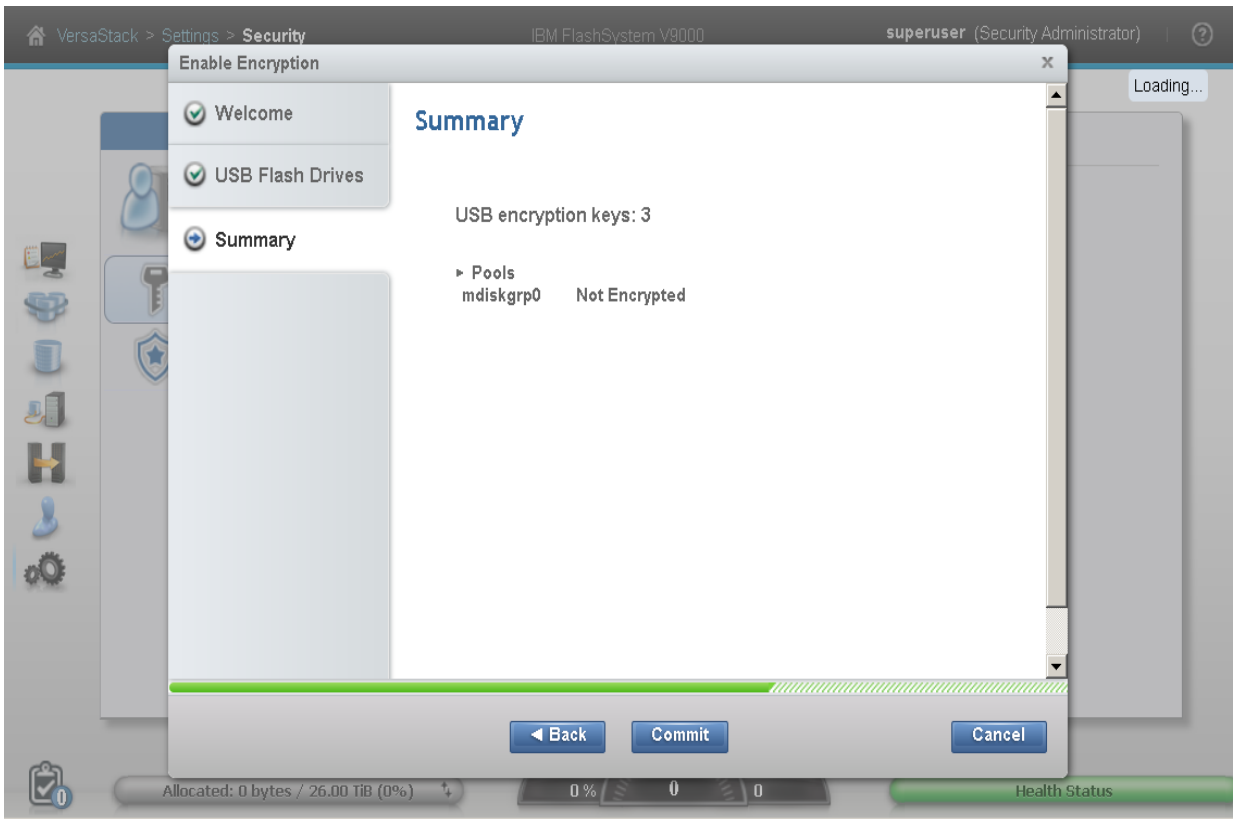
26. From Settings icon in the left pane, select Security then Encryption. Click Enable Encryption.

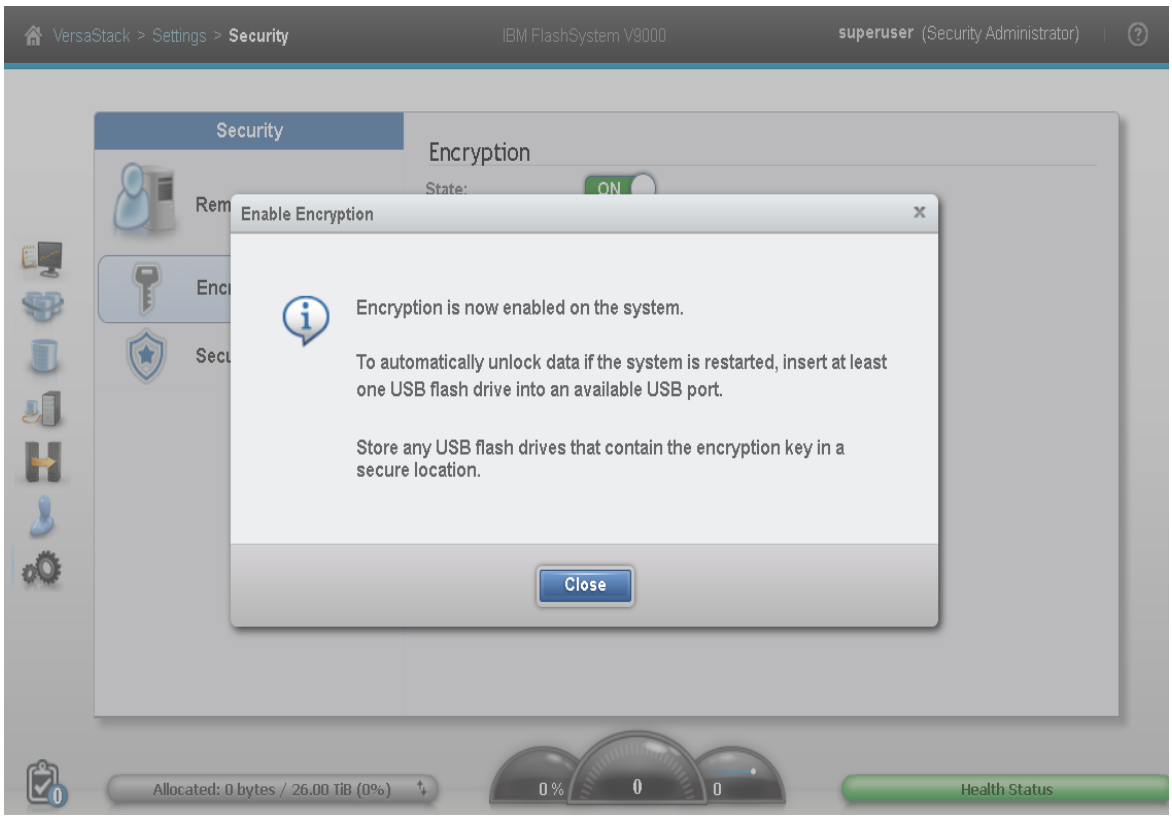
27. In this wizard, click Next


Enable Encryption
Welcome
USB Flash Drives
Summary
Welcome
The following wizard will guide you through the encryption setup of the IBM FlashSystem V9000.
You will need 3 USB flash drives.
Back
Next
Cancel

28. Insert all 3 USB sticks, then click Next. Wait for the Encryption Key updates to complete then click Next.

29. Click Commit to enable Encryption, and then click Close.

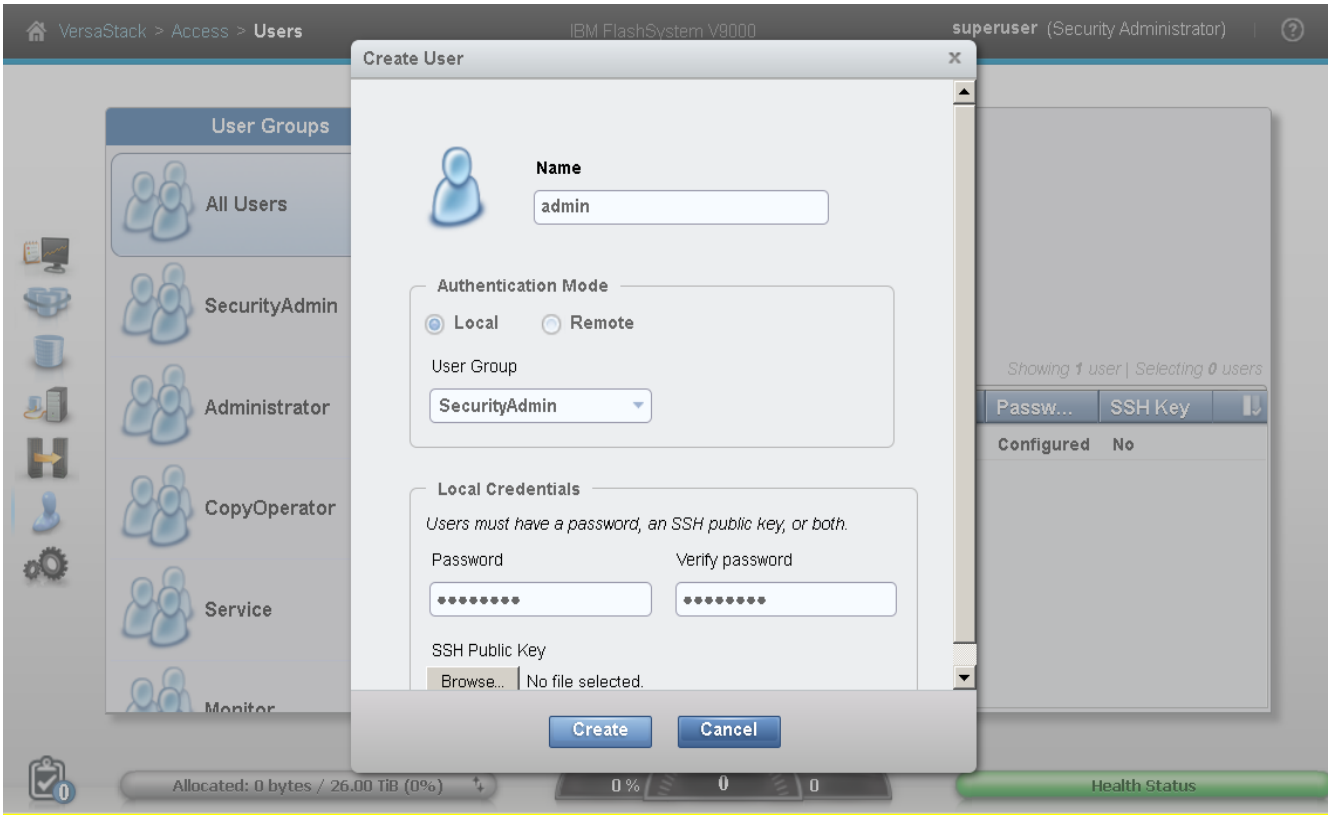




30. Click the User icon in the left pane, and then select Users to access the Users screen.

31. Click Create User.

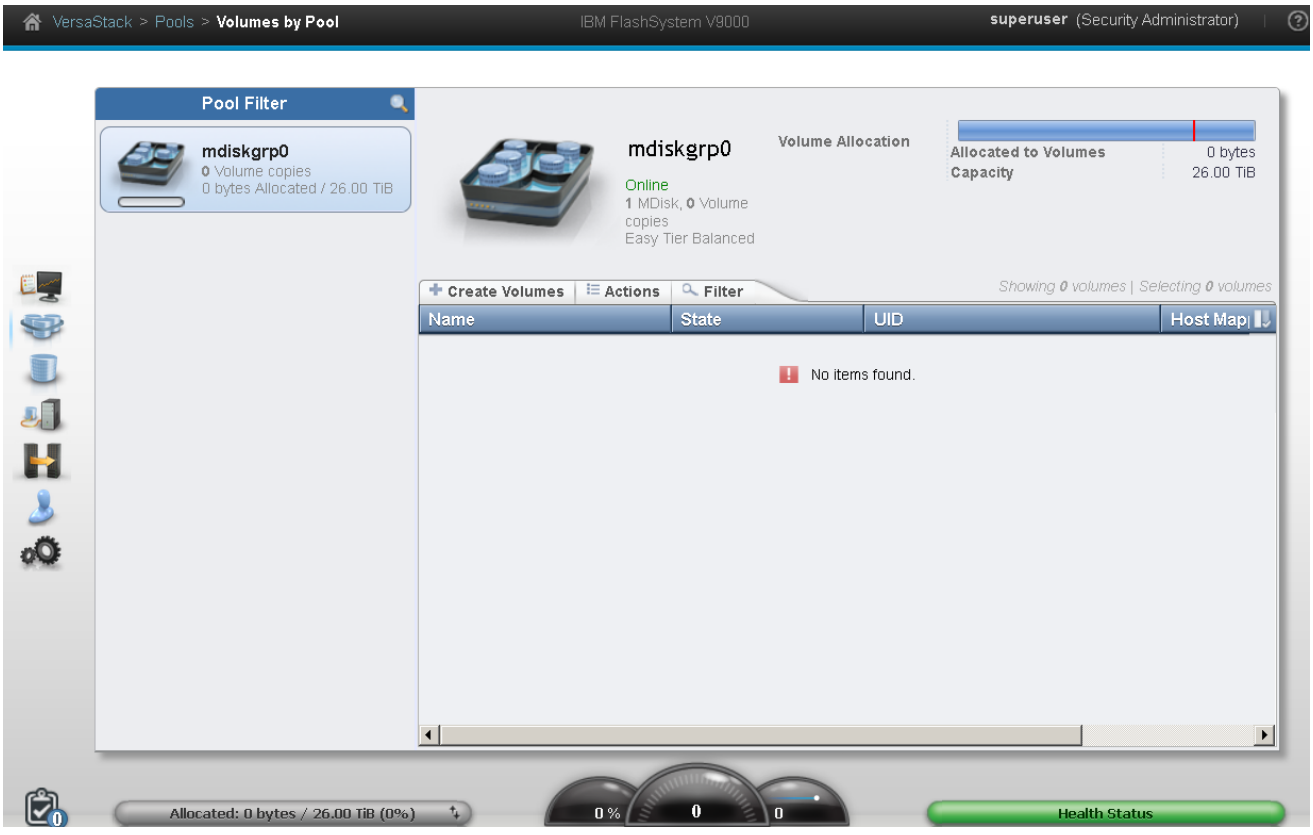
32. Enter and new name for an alternative admin account. Leave Security Admin default, and input the new password then click Create.



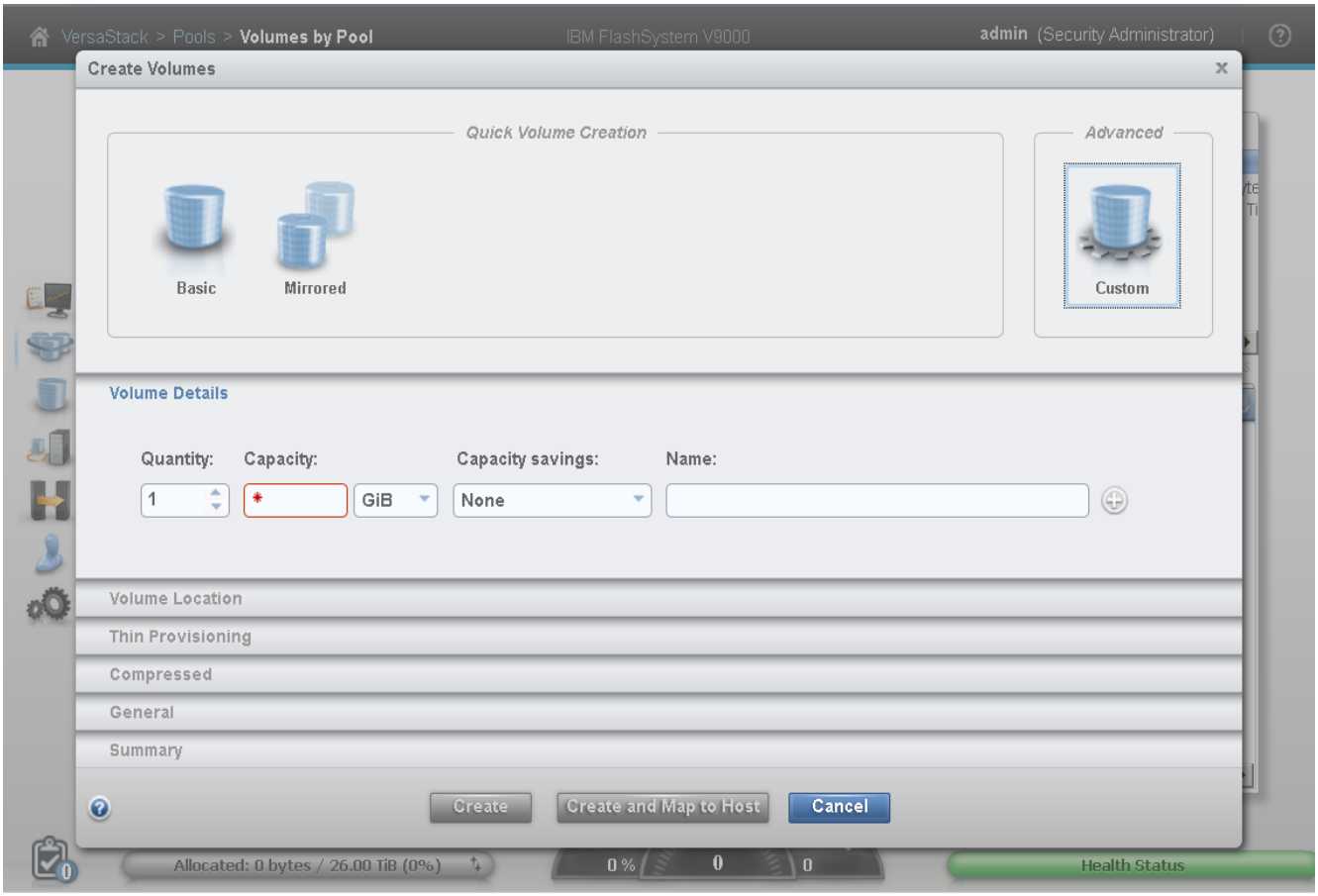
33. Log out the superuser account and log back in as the new account you created.

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

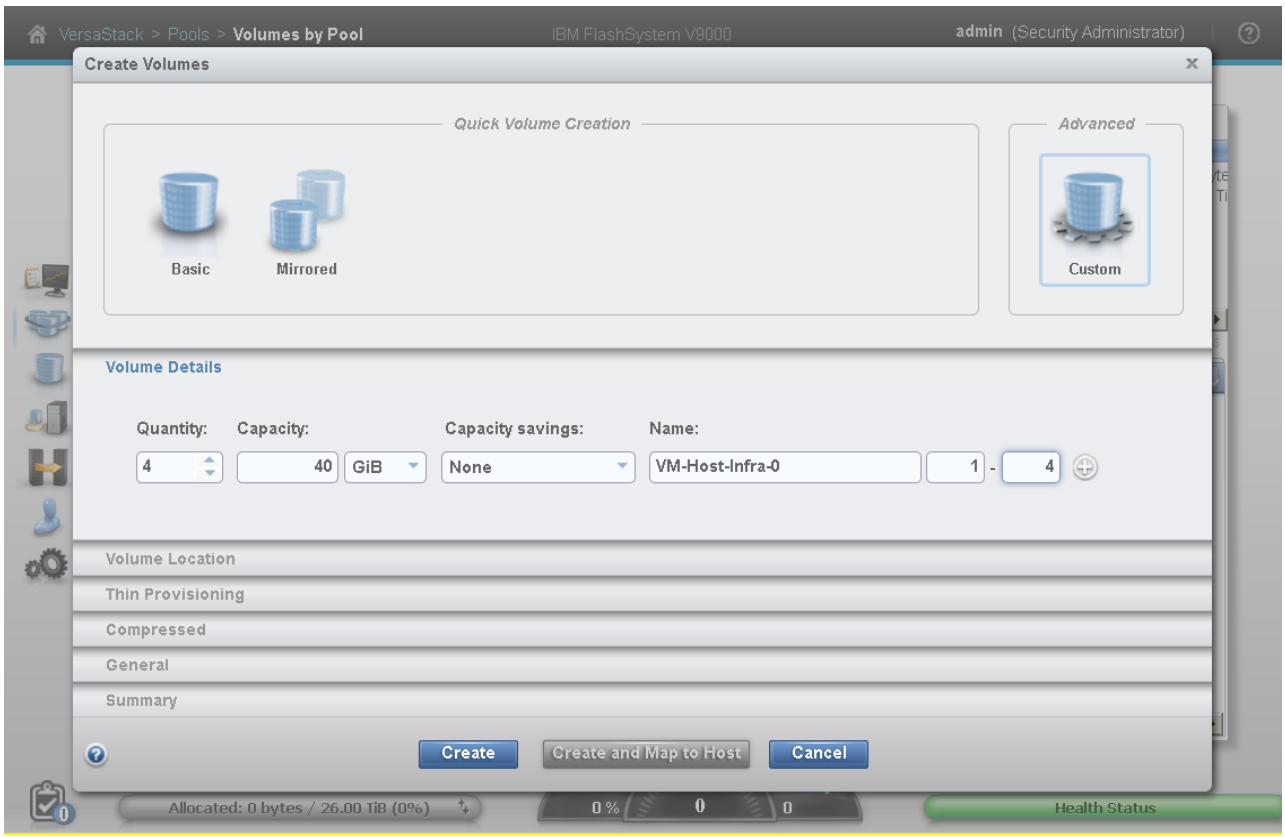
35. Click the Create Volumes tab.

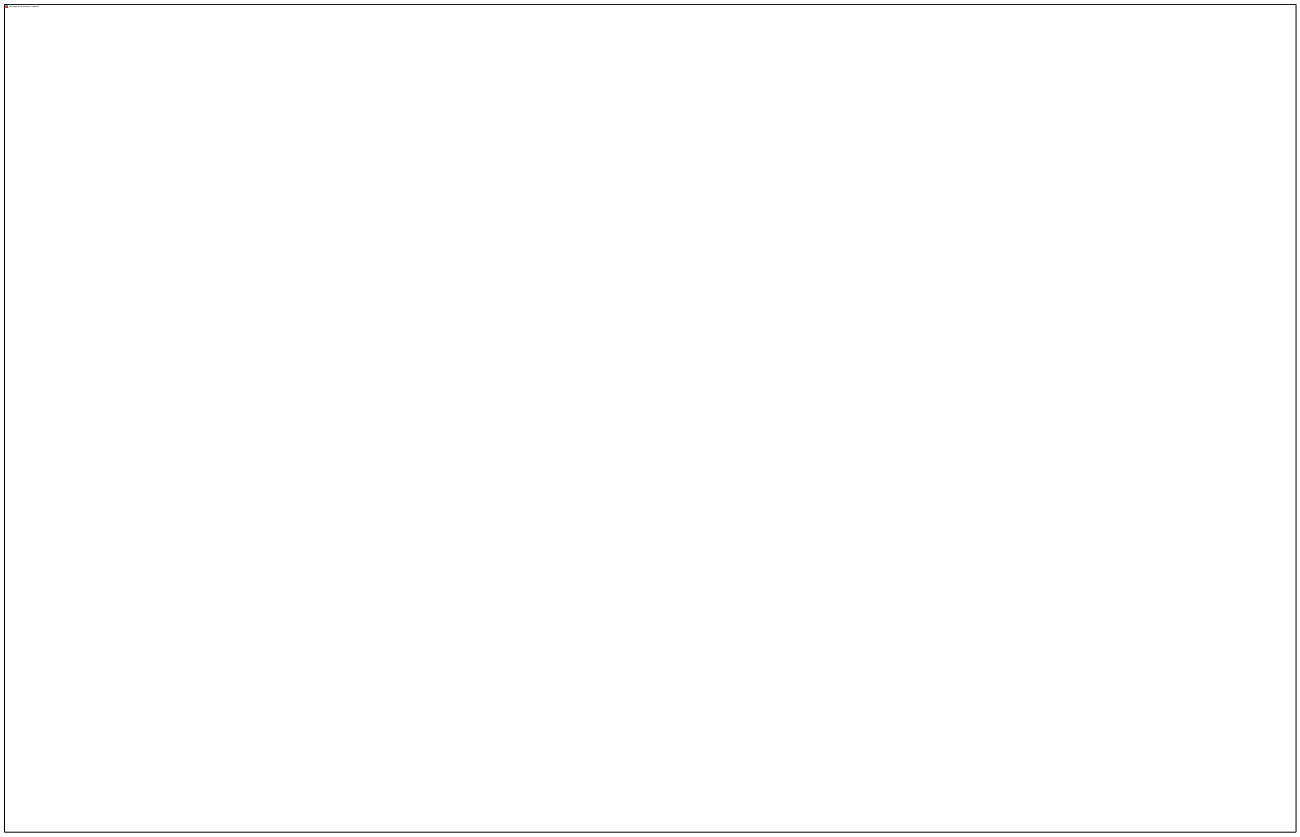


36. Select Custom for the ESXi boot volumes to get to the Volume Details section.

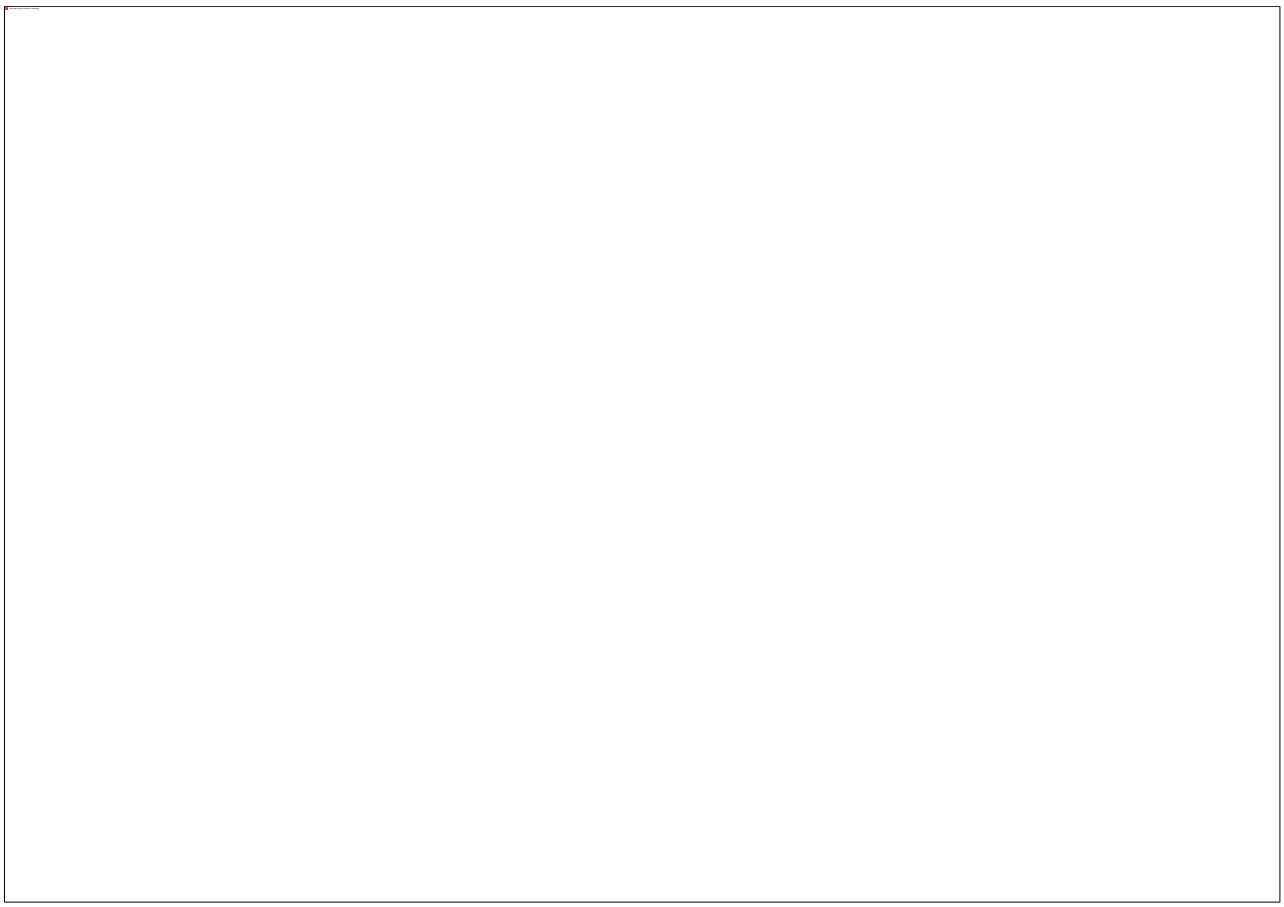


37. Input quantity 4, capacity 40GB, and name VM-Host-Infra-0. And change the starting ID to 1.

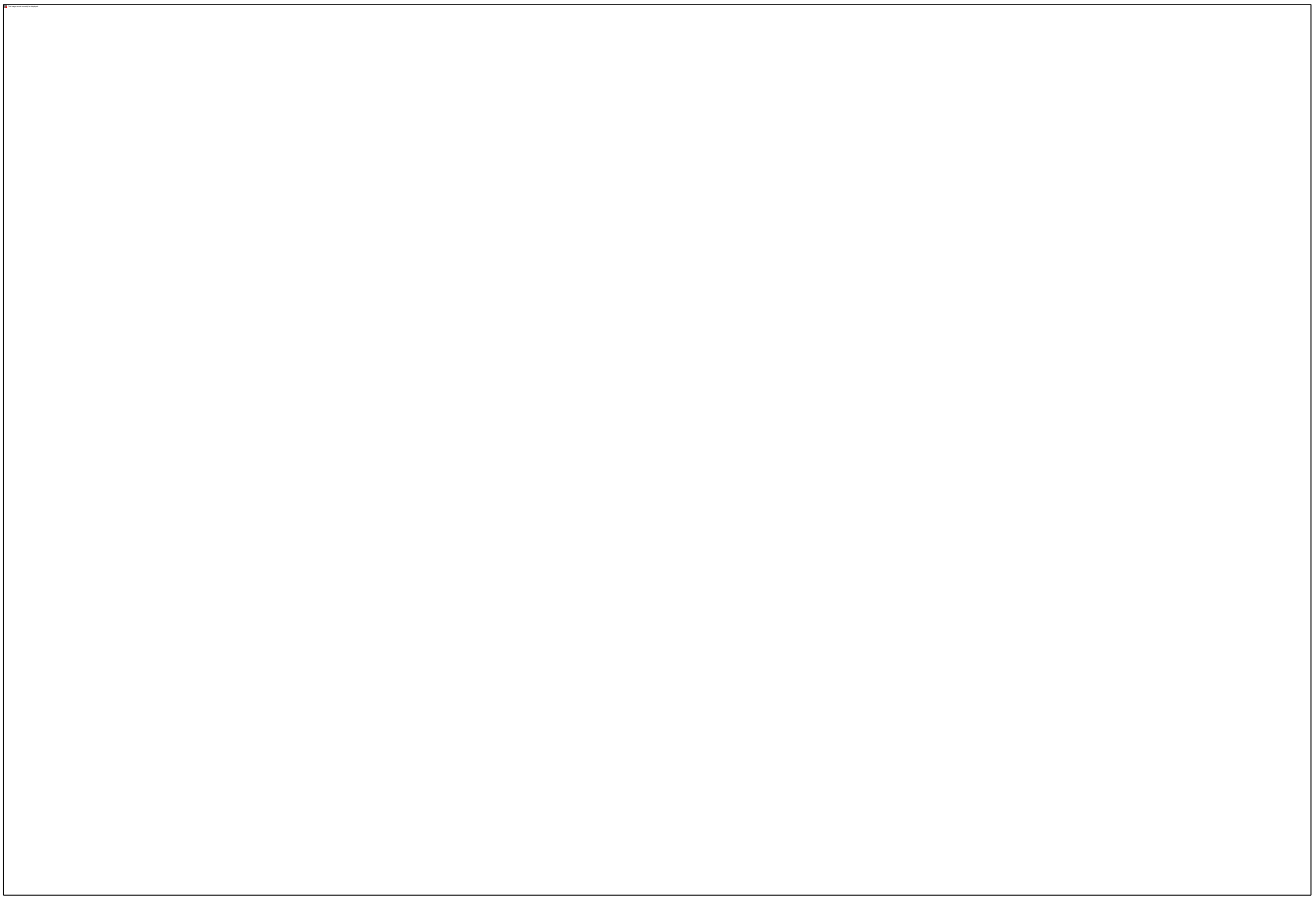


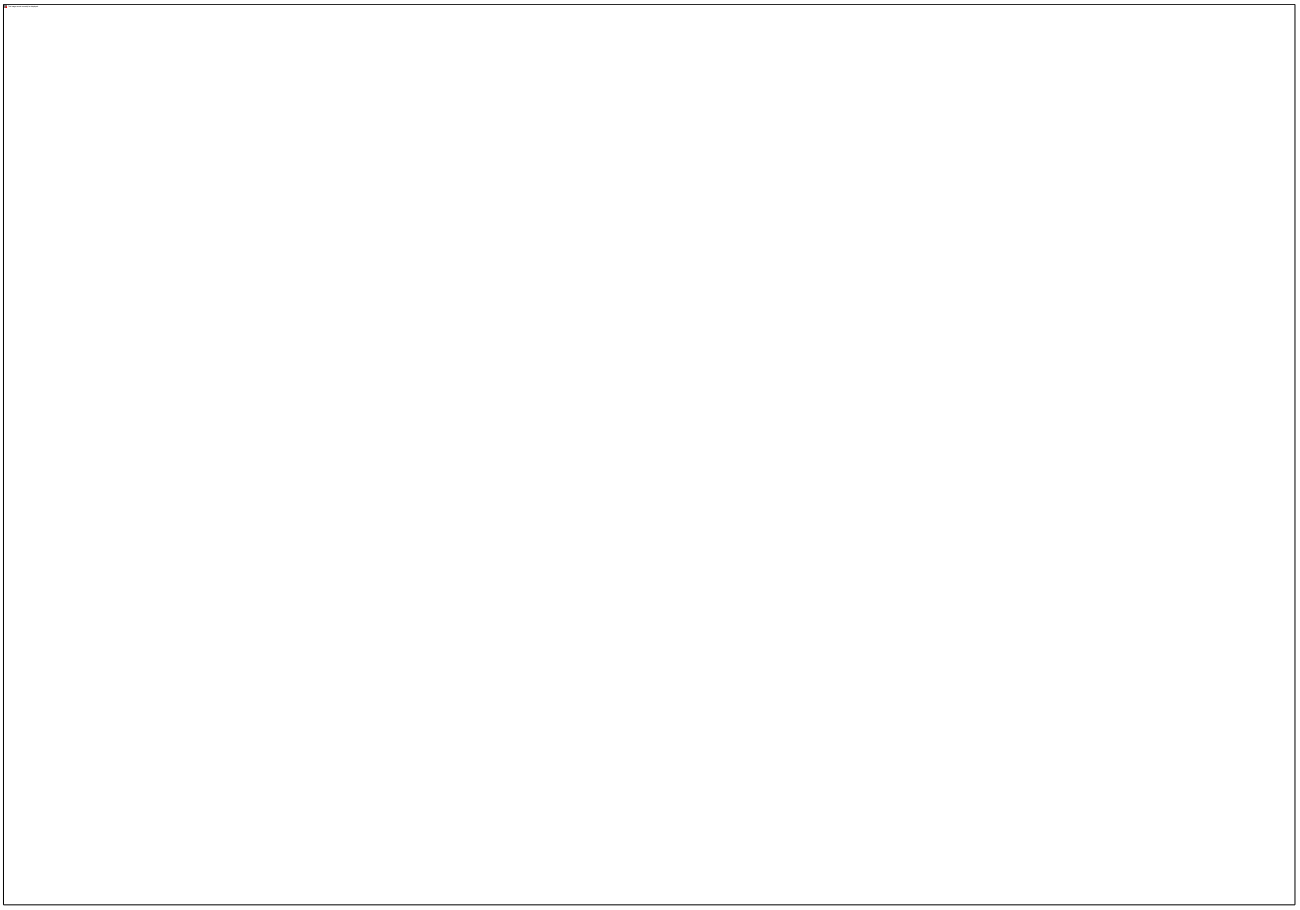


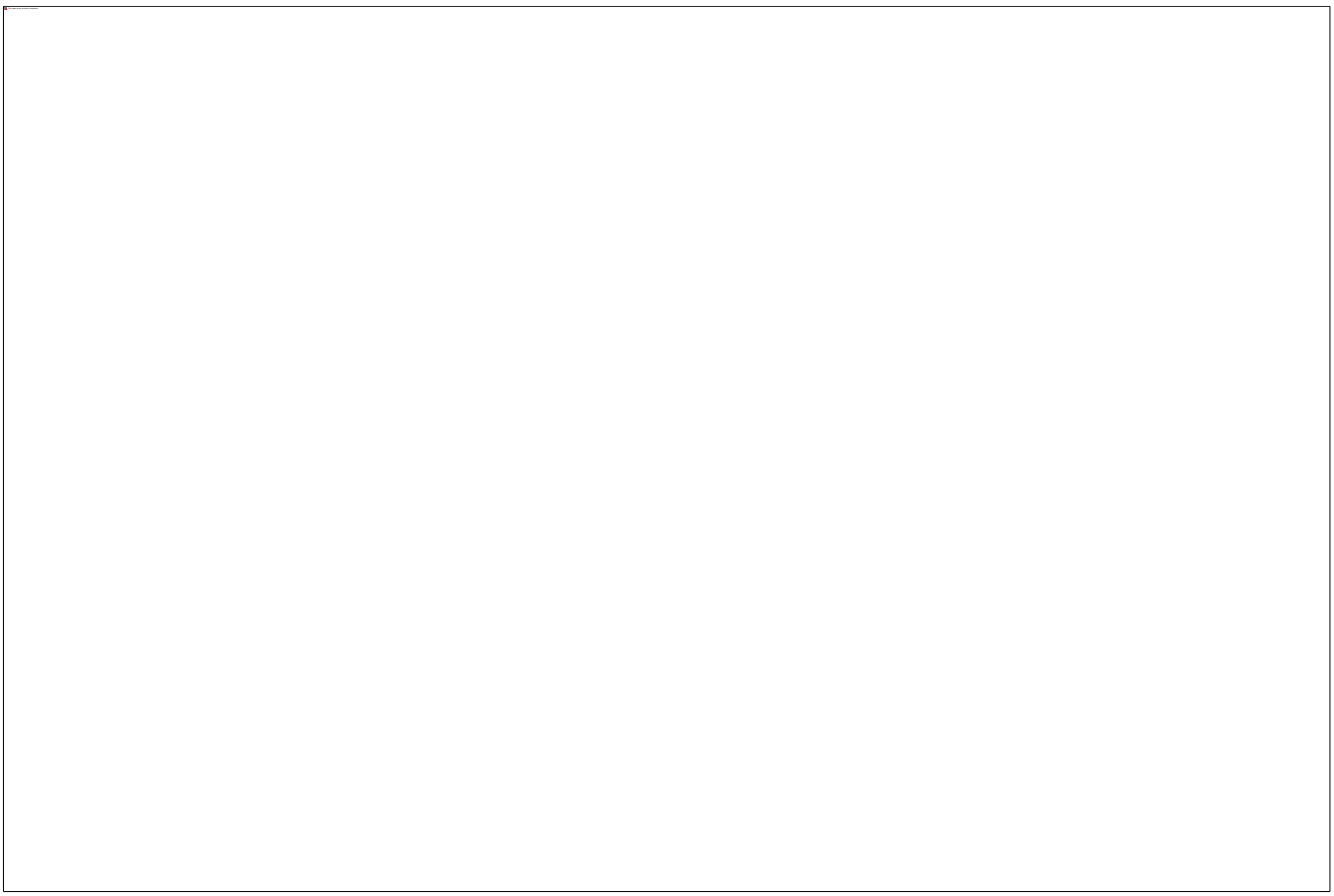
38. Click General section, and deselect the Format volume option, then click Create, then Close.



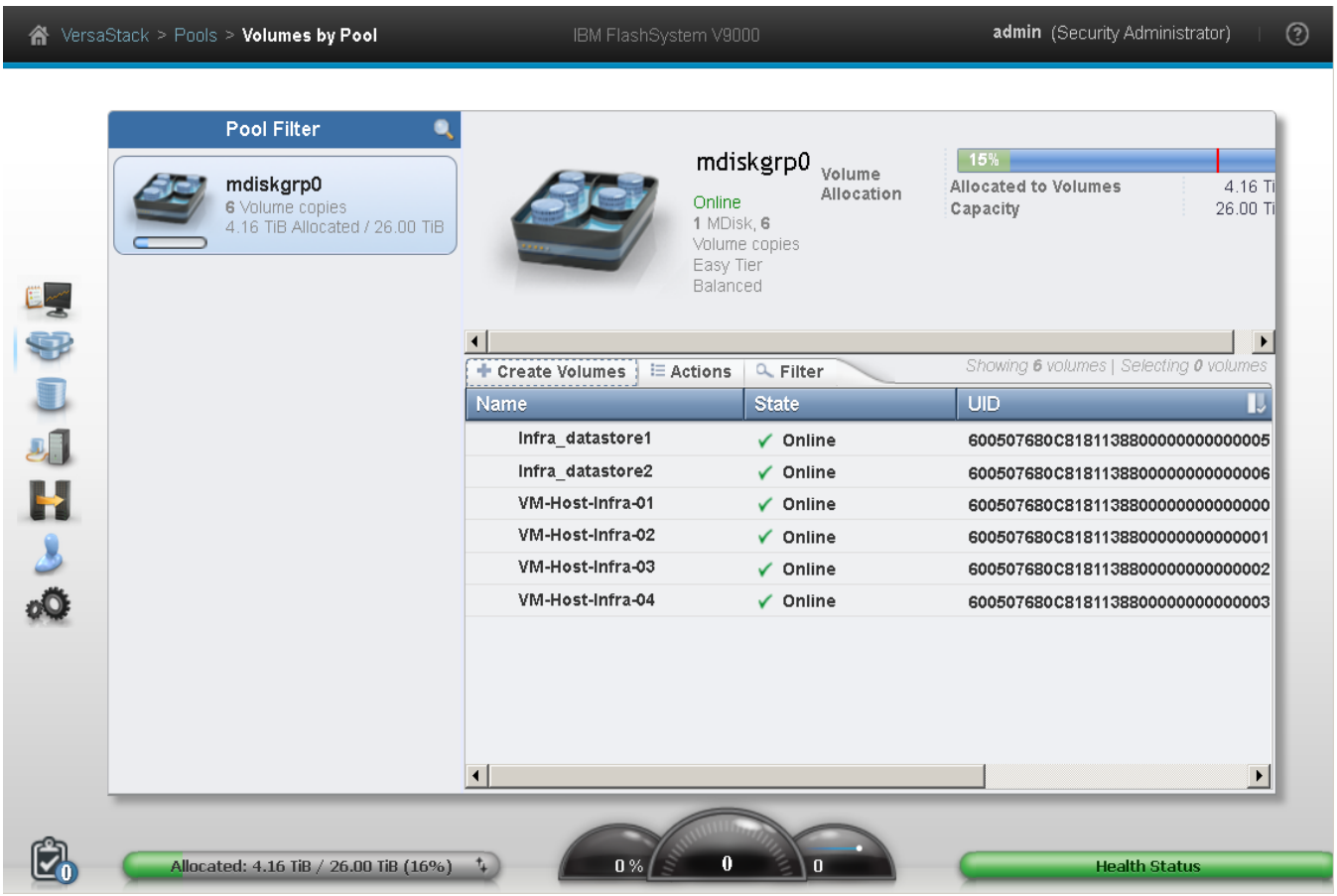
39. Click Create Volumes again and select the Custom preset. Enter quantity 2, capacity 2 TB, and name Infra_datastore. Enter 1 for the starting ID. Similar to above, on the General section deselect Format volume from General section. Click Create, and then Close.

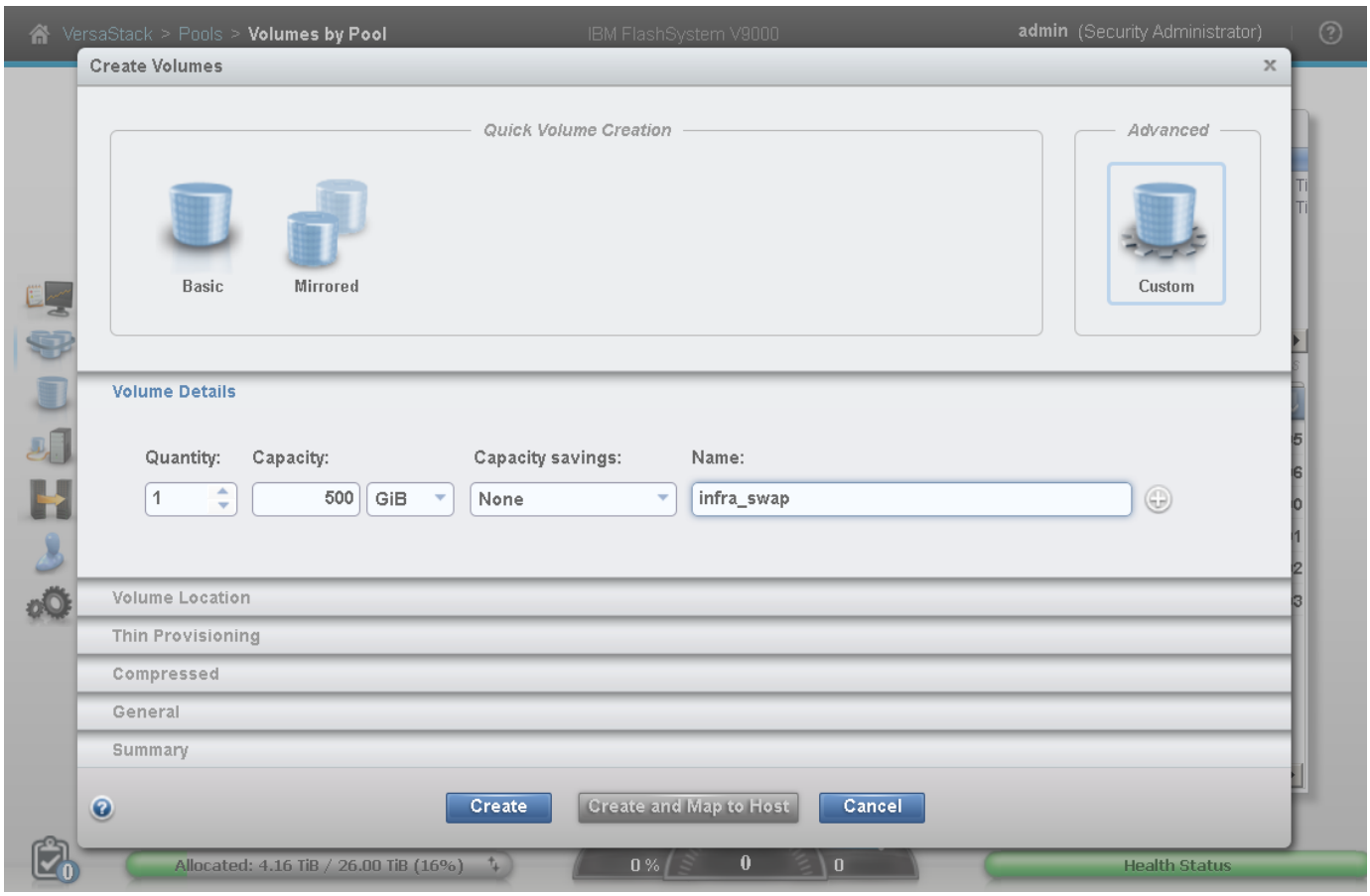


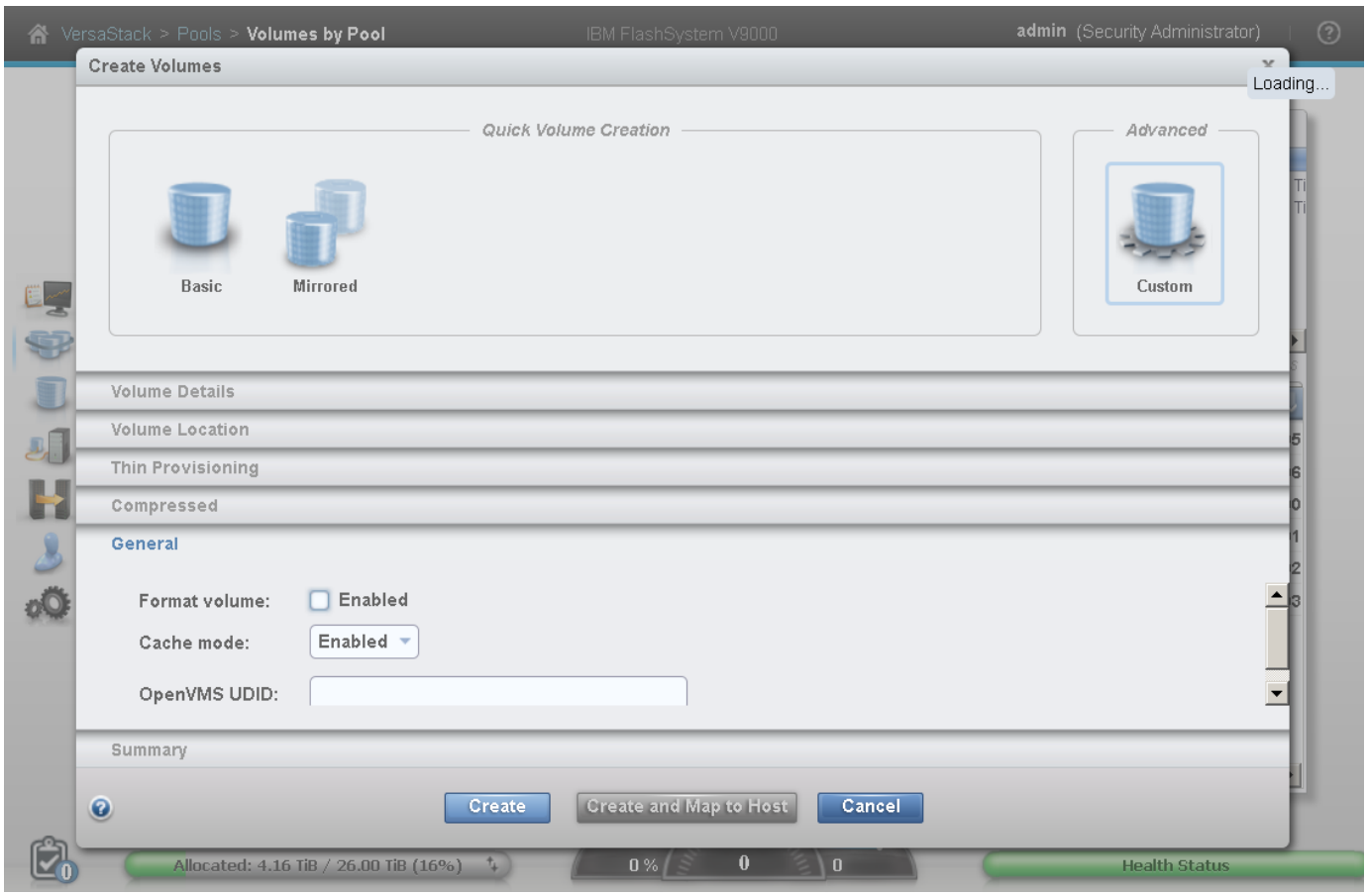




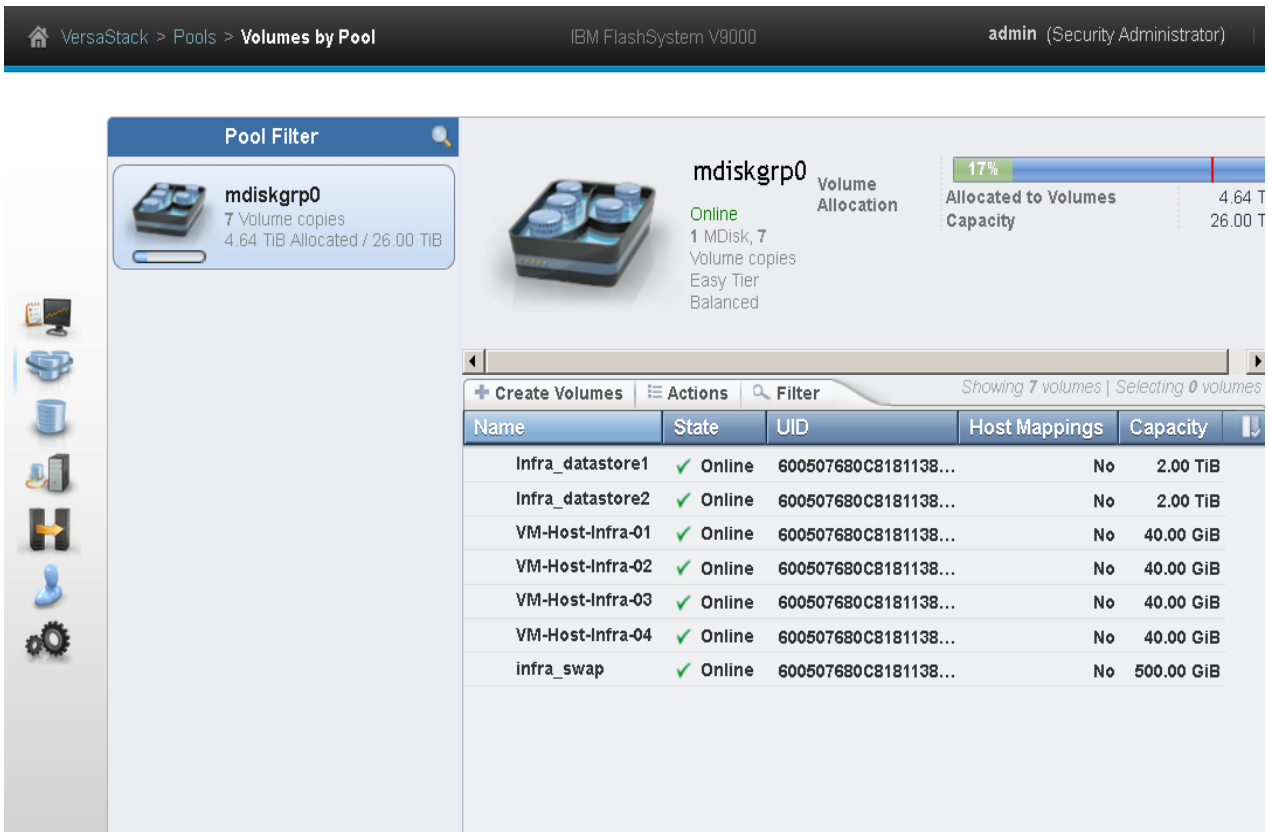
40. Click Create Volumes again and select the Custom volume. Enter quantity 1, capacity 500GB, and name infra_swap. Similar to above, on Volume Location section select mdiskgrp0, and deselect Format volume from General section. Click Create, and then click Close.


VersaStack > Pools > Volumes by Pool
IBM FlashSystem V9000
admin (Security Administrator)
Pool Filter
mdiskgrp0
6 Volume copies
4.16 TiB Allocated / 26.00 TiB
mdiskgrp0
Online
1 MDisk, 6
Volume copies
Easy Tier
Balanced
Volume Allocation
15%
Allocated to Volumes
Capacity
4.16 Ti
26.00 Ti
Create Volumes
Actions
Filter
Showing 6 volumes | Selecting 0 volumes
Name
State
UID
Infra_datastore1 Online 600507680C8181138800000000000005
Infra_datastore2 Online 600507680C8181138800000000000006
VM-Host-Infra-01 Online 600507680C8181138800000000000000
VM-Host-Infra-02 Online 600507680C8181138800000000000001
VM-Host-Infra-03 Online 600507680C8181138800000000000002
VM-Host-Infra-04 Online 600507680C8181138800000000000003
Allocated: 4.16 TiB / 26.00 TiB (16%)
0 %
0
0
Health Status


VersaStack > Pools > Volumes by Pool
IBM FlashSystem V9000
admin (Security Administrator)
Create Volumes
Quick Volume Creation
Basic
Mirrored
Advanced
Custom
Volume Details
Quantity:
Capacity:
Capacity savings:
Name:
1
500
GiB
None
infra_swap
Volume Location
Thin Provisioning
Compressed
General
Summary
Create
Create and Map to Host
Cancel
Allocated: 4.16 TiB / 26.00 TiB (16%)
0 %
0
0
Health Status



41. Validate the volumes created.



Server Configuration

VersaStack Cisco UCS Initial Setup

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

This section provides the detailed procedures for configuring the Cisco Unified Computing System (Cisco UCS) 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 6248 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 6248 fabric interconnect.

```
Enter the configuration method: console

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

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

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

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

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

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

```
(yes/no) [n]: y

Which switch fabric (A|B): A

Enter the system name: <<var_ucs_clustername>>

Physical switch Mgmt0 IPv4 address: <<var_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.

Cisco UCS 6248 B

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

Power on the 2nd module and connect to the console port on the second Cisco UCS 6248 fabric interconnect.

```
Enter the configuration method: console

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

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

Physical switch Mgmt0 IPv4 address: <<var_ucsb_mgmt_ip>>
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no):
y
```

VersaStack Cisco UCS Configuration

Log in to Cisco UCS Manager

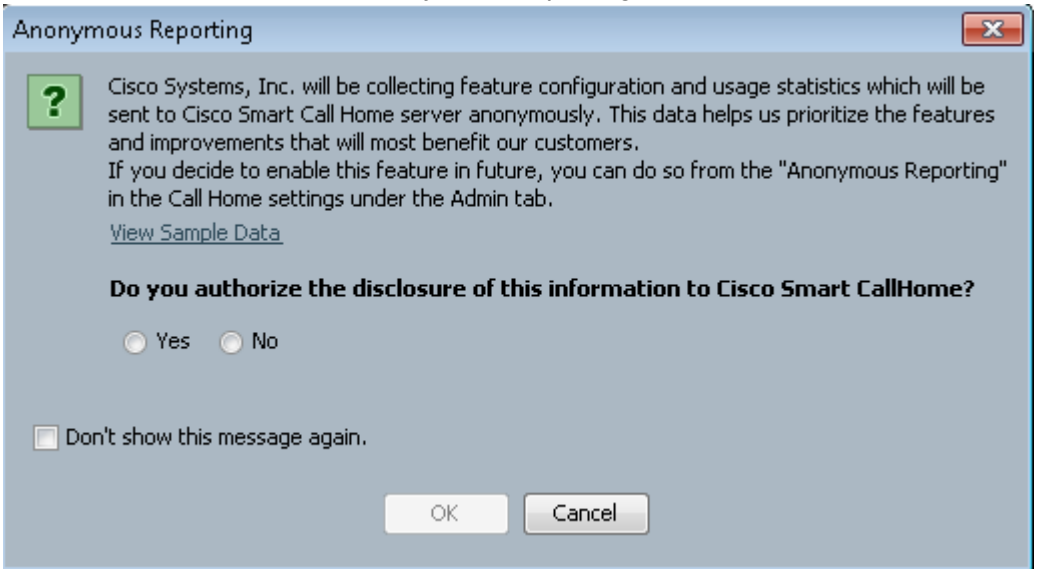
To log in to the Cisco Unified Computing System (UCS) environment, complete the following steps:

1. Open a web browser and navigate to the Cisco UCS 6248 Fabric Interconnect cluster address.
2. Click the Launch Cisco UCS Manager link under HTML.
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 3.1(1e)

This document assumes the use of Cisco UCS Manager Software version 3.1(1e). To upgrade the Cisco UCS Manager software and the Cisco UCS 6248 Fabric Interconnect software to version 3.1(1e), refer to Cisco UCS Manager Install and Upgrade Guides.

Add Block of IP Addresses for KVM Access

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

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

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

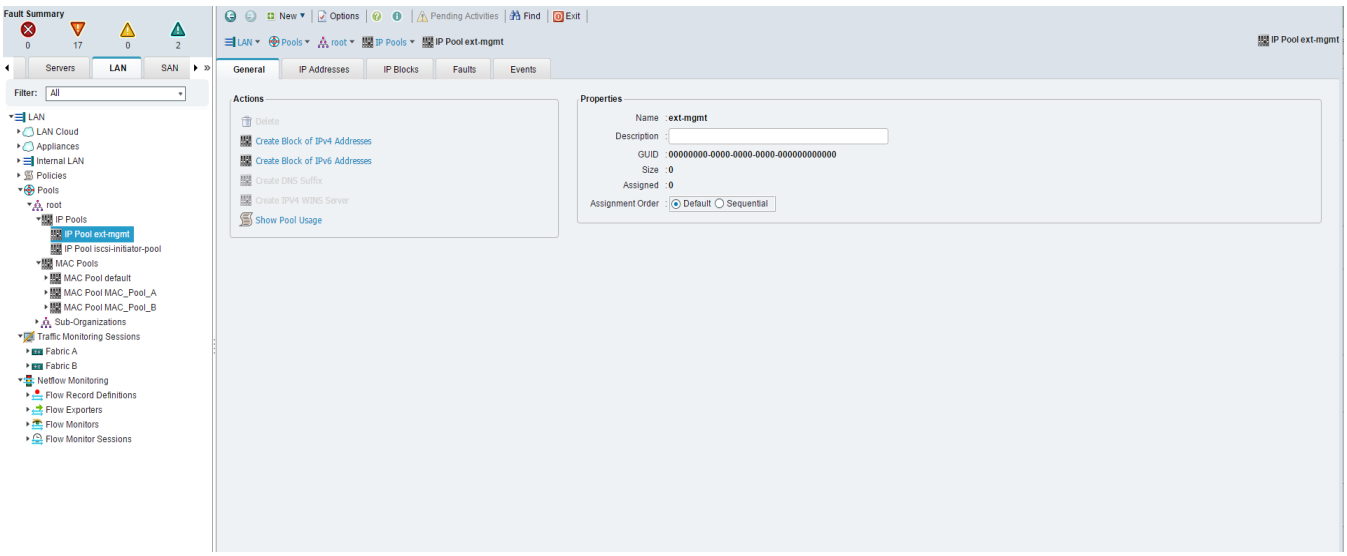
2. Select Pools > root > IP Pools > IP Pool ext-mgmt.

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.

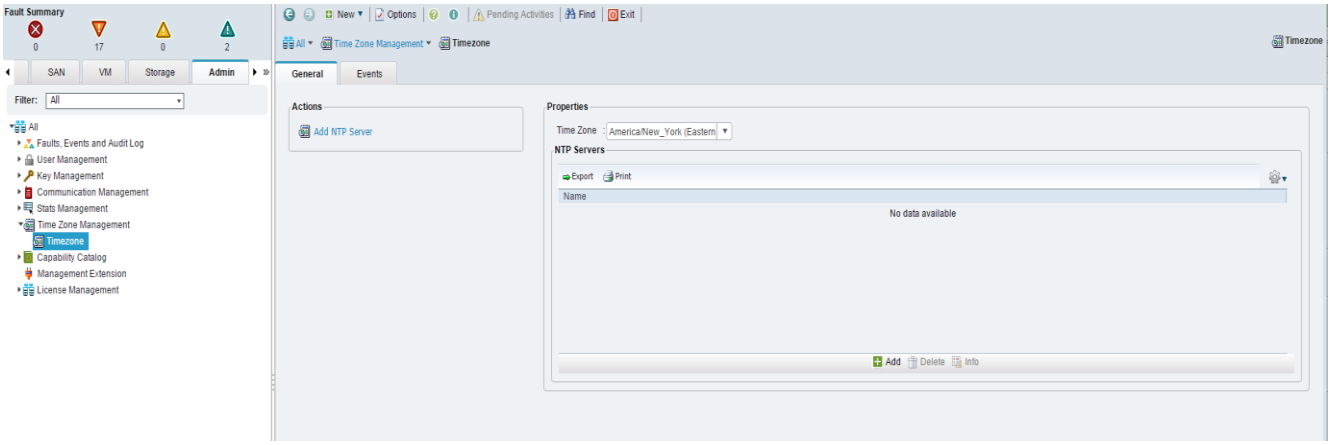
6. Click OK in the confirmation message.



Synchronize Cisco UCS to NTP

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

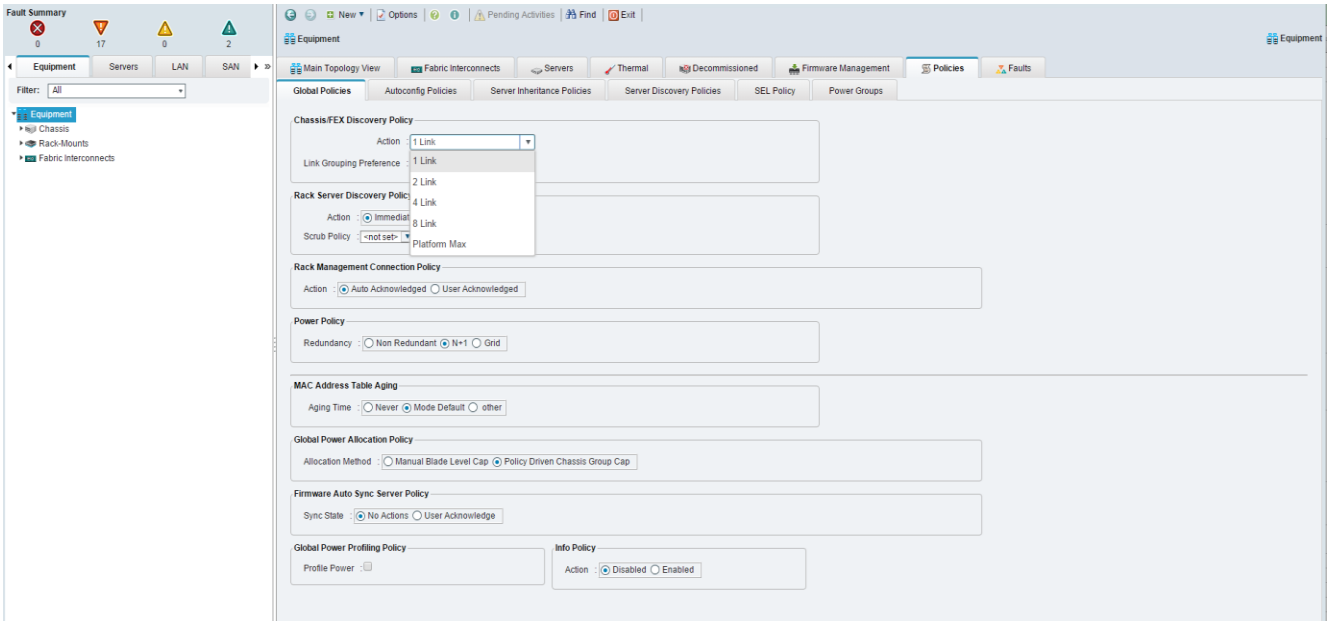
1. In Cisco UCS Manager, click the Admin tab in the navigation pane.
2. Select All > Timezone Management.
3. In the Properties pane, select the appropriate time zone in the Timezone menu.
4. Click Save Changes, and then click OK.
5. Click Add NTP Server.
6. Enter `<<var_global_ntp_server_ip>>` and click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



Edit Chassis Discovery Policy

Setting the discovery policy simplifies the addition of Cisco UCS B-Series Cisco UCS chassis and of additional fabric extenders for further Cisco UCS C-Series connectivity. To modify the chassis discovery policy, complete the following steps:

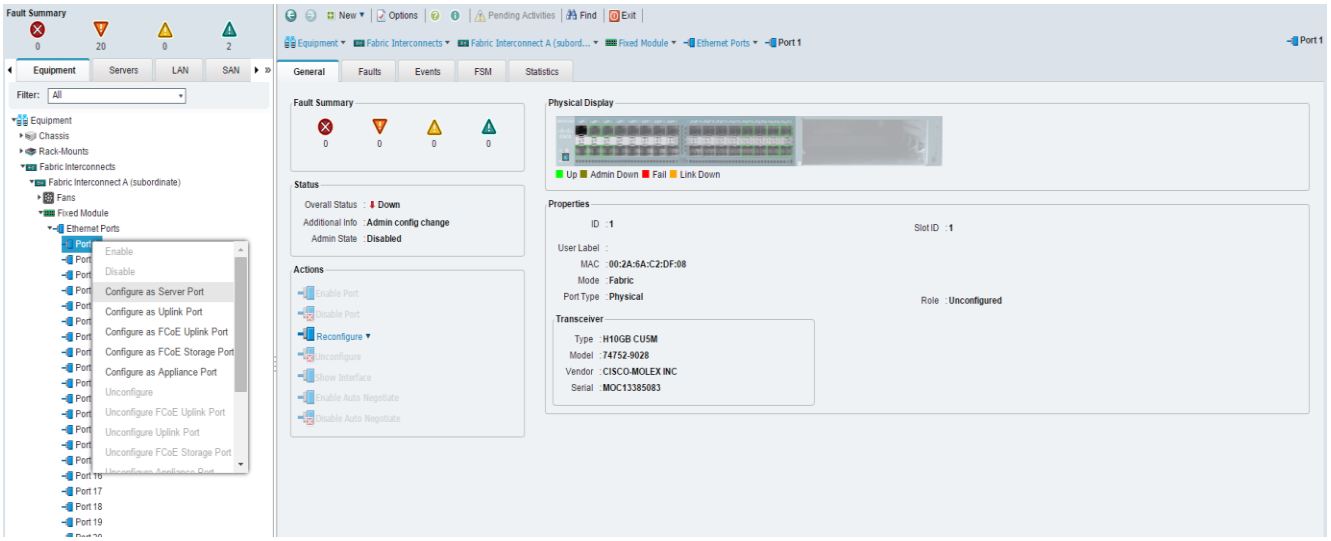
1. In Cisco UCS Manager, click Equipment tab in the navigation pane and select Equipment in the list on the left.
2. In the right pane, click the Policies tab.
3. Under Global Policies, set the Chassis/FEX Discovery Policy to match the number of uplink ports that are cabled between the chassis or fabric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



Enable Server and Uplink Ports

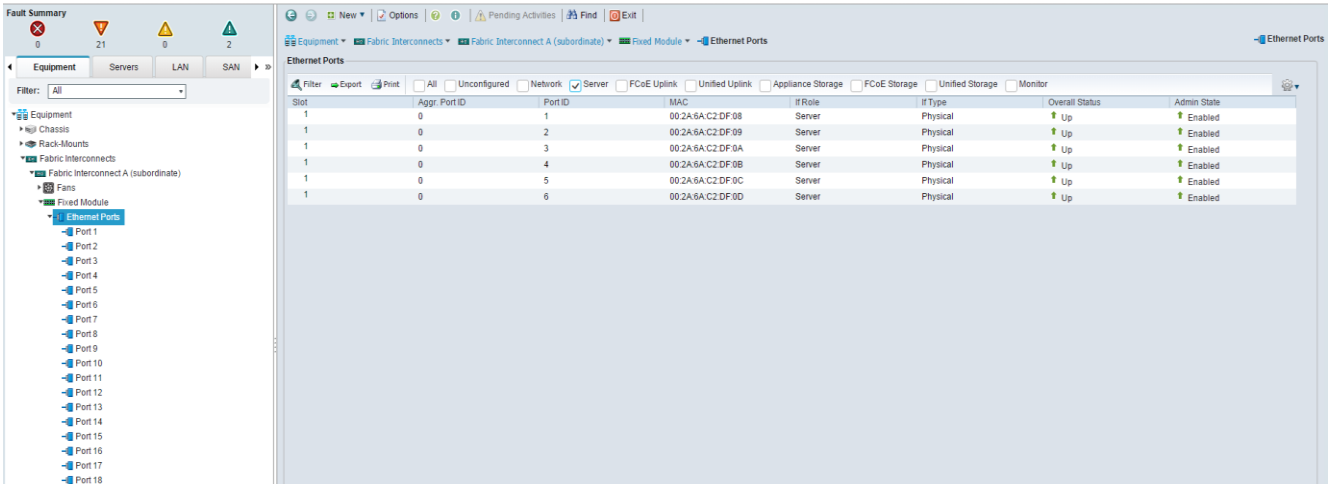
To enable server and uplink ports, complete the following steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane.
2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module.
3. Expand Ethernet Ports.
4. Select the ports that are connected to the chassis and to the Cisco UCS C-Series or the FEX (two per FEX) if used, right-click them, and select Configure as Server Port.



5. Click Yes to confirm server ports and click OK.

6. Verify that the ports connected to the chassis and to the Cisco UCS C-Series are now configured as server ports.



7. Select ports 25 and 26 that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.

8. Click Yes to confirm uplink ports and click OK.

9. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.

10. Expand Ethernet Ports.

11. Select the ports that are connected to the chassis and Cisco UCS C-Series or the FEX (two per FEX) if used, right-click them, and select Configure as Server Port.

12. Click Yes to confirm server ports and click OK.

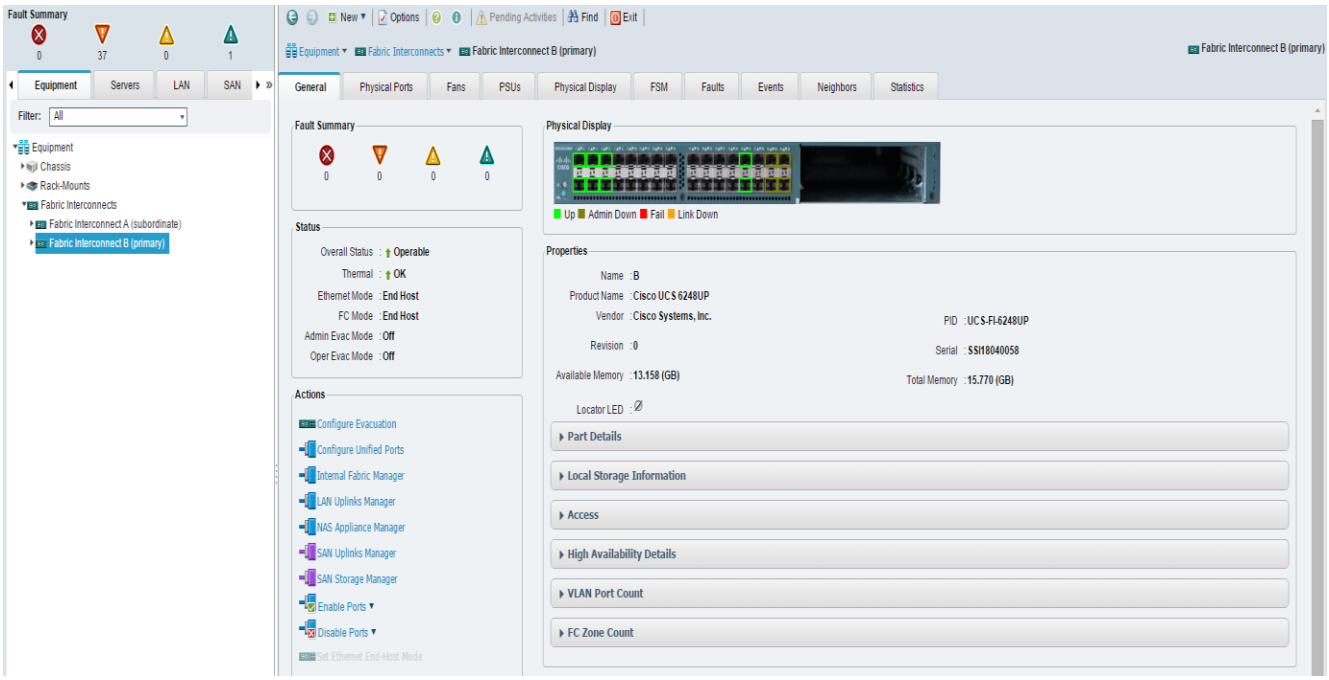
13. Select ports 25 and 26 that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.

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

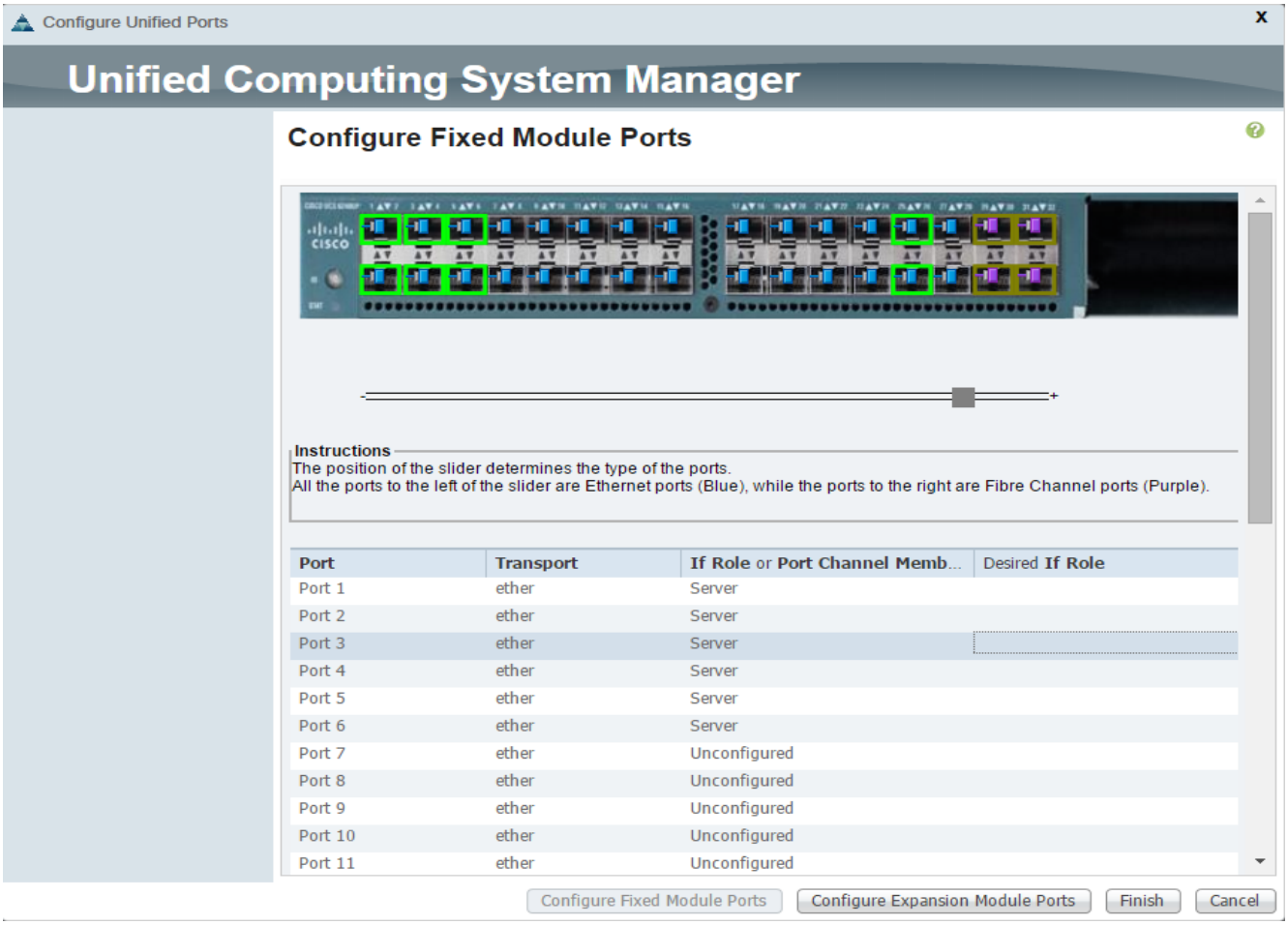
Enable Fibre Channel Ports

To enable FC uplink ports, complete the following steps making sure you first reconfigure the subordinate switch to save time:

1. On the equipment tab, select the Fabric Interconnect B which should be the subordinate FI, and in the Actions pane, select Configure Unified Ports, Click Yes.



2. Slide the lever to change the ports `29-32` to change the ports to Fiber Channel. Click Finish and then Yes to the reboot message. Click OK.



3. When the subordinate has completed reboot, select the Fabric Interconnect A, (primary), and then select Configure Unified Ports, and click Yes.

4. Slide the Bar to the left to select ports `29-32` for FC (purple), click Finish, and say Yes to the reboot message. You will need to re-login to the client after the reboot of the FI completes.

Create VSAN for the Fibre Channel Interfaces

To configure the necessary virtual storage area networks (VSANs) for FC uplinks for the Cisco UCS environment, follow these steps:

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

2. Expand the SAN > SAN Cloud tree. Then fabric A.

3. Right-click VSANs.

4. Choose Create VSAN.

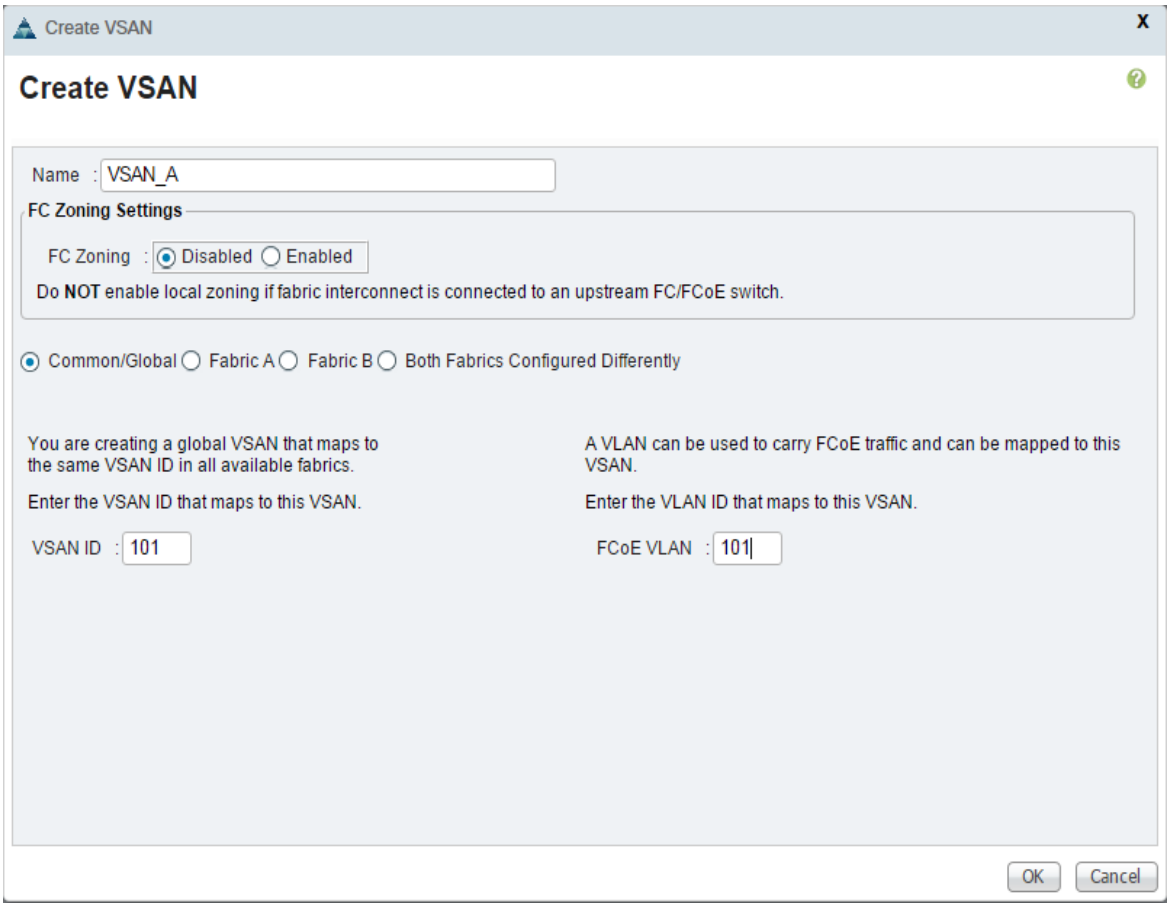
5. Enter `VSAN_A` as the name of the VSAN for fabric A.

6. Keep the Disabled option selected for FC Zoning.

7. Click the Fabric A radio button.

8. Enter `<<var_vsan_a_id>>` as the VSAN ID for fabric A.

9. Enter `<<var_fabric_a_fcoe_vlan_id>>` as the FCoE VLAN ID for fabric A. and click OK, and OK again.



10. On the SAN tab, expand SAN, SAN Cloud, Fabric-B and Right-click VSANs.

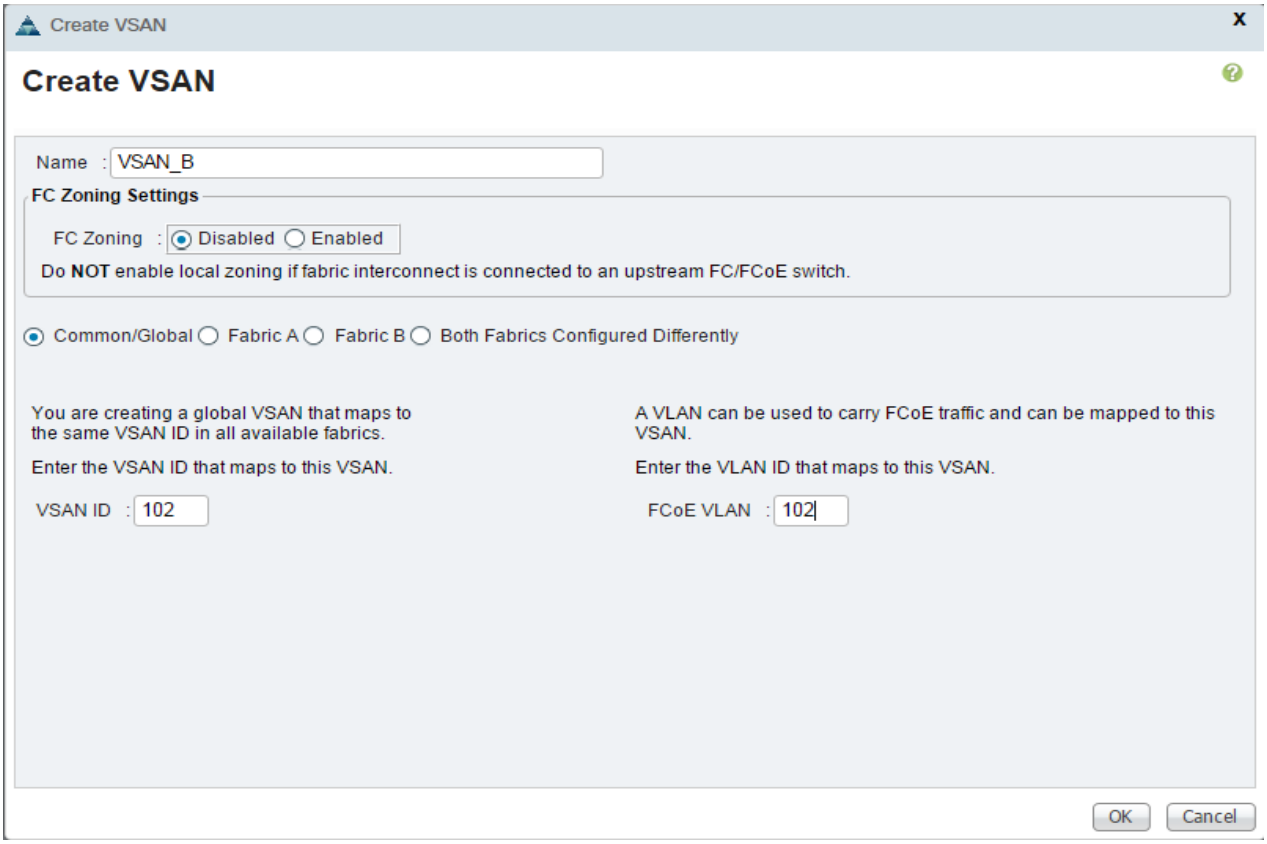
11. Right-click VSANs and choose Create VSAN.

12. Enter `VSAN_B` as the name of the VSAN for Fabric B.

13. Keep the Disabled option selected for FC Zoning.

14. Click Fabric B radio button.

15. Enter `<<var_vsan_b_id>>` as the VSAN ID for fabric B. Enter `<<var_fabric_b_fcoe_vlan_id>>` as the FCoE VLAN ID for fabric B, then click OK and then OK.

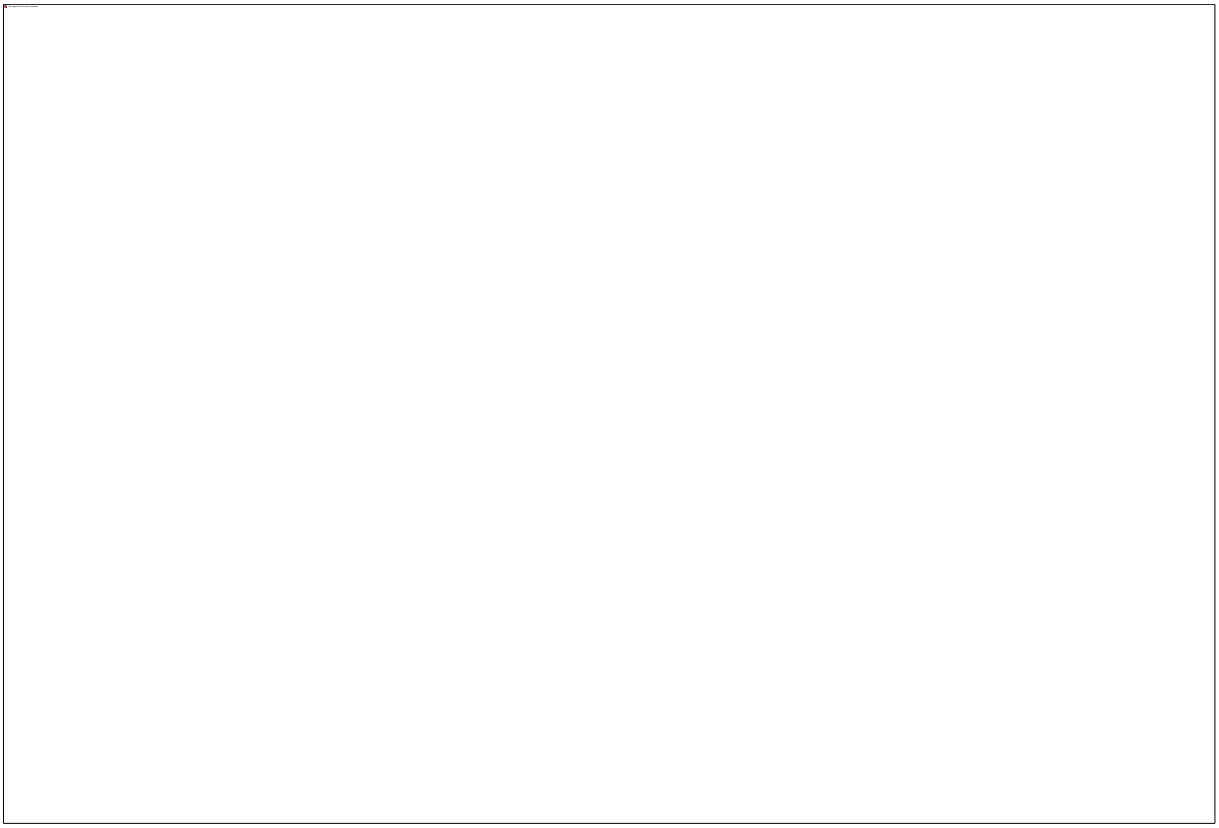


Create Port Channels for the Fibre Channel Interfaces

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

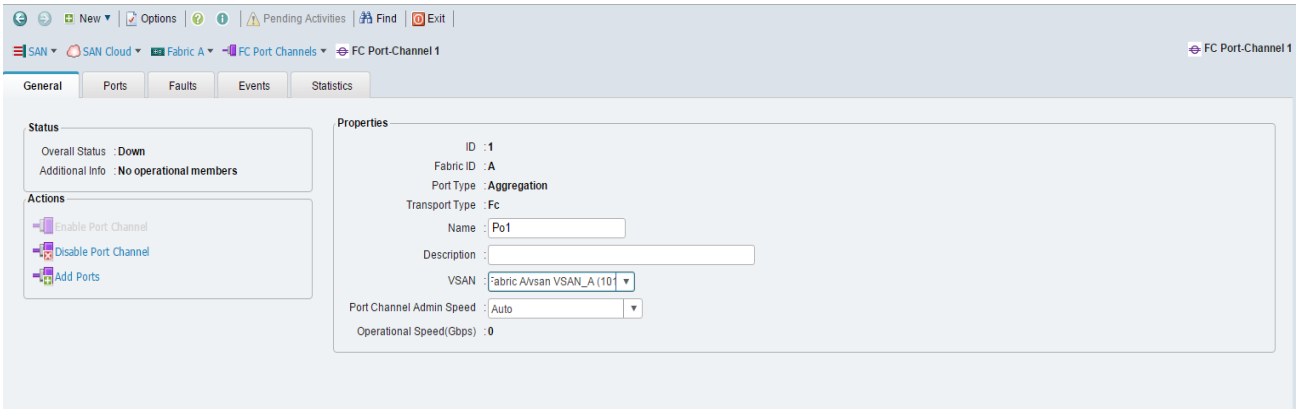
Fabric-A

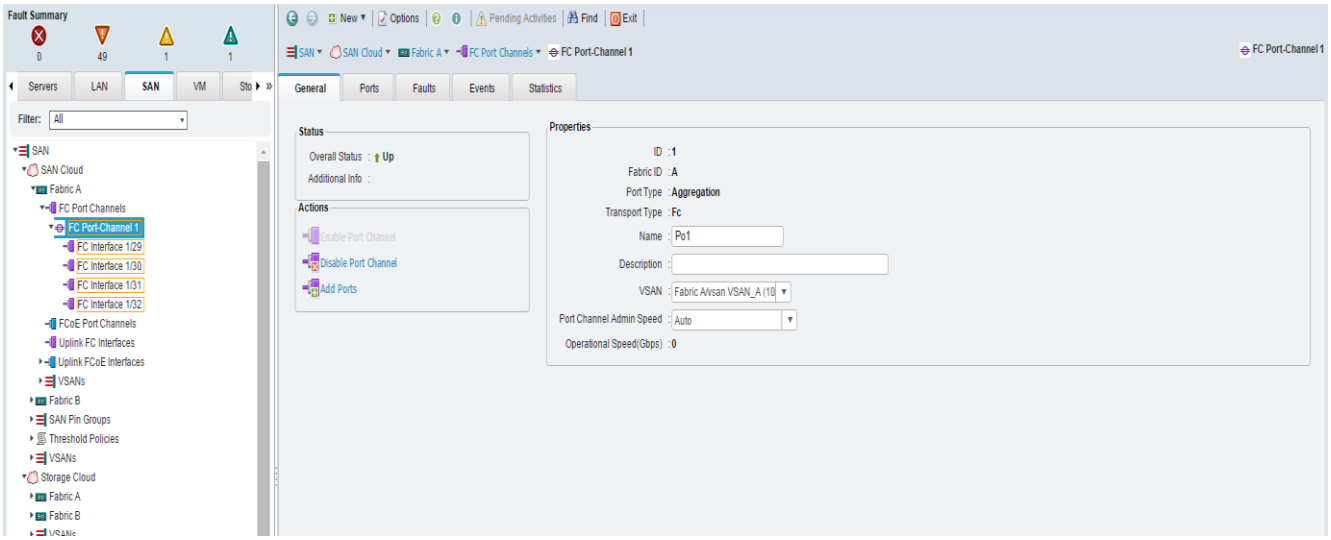
1. In the navigation pane, under SAN > SAN Cloud, expand the Fabric A tree.
2. Right-click FC Port Channels.
3. Choose Create Port Channel.
4. Enter `1` for the port channel ID and `Po1` for the port channel name.
5. Click Next then choose ports `29 and 32` and click >> to add the ports to the port channel. Click Finish.



6. Click OK.

7. Under the VSAN drop-down, select VSAN 101.

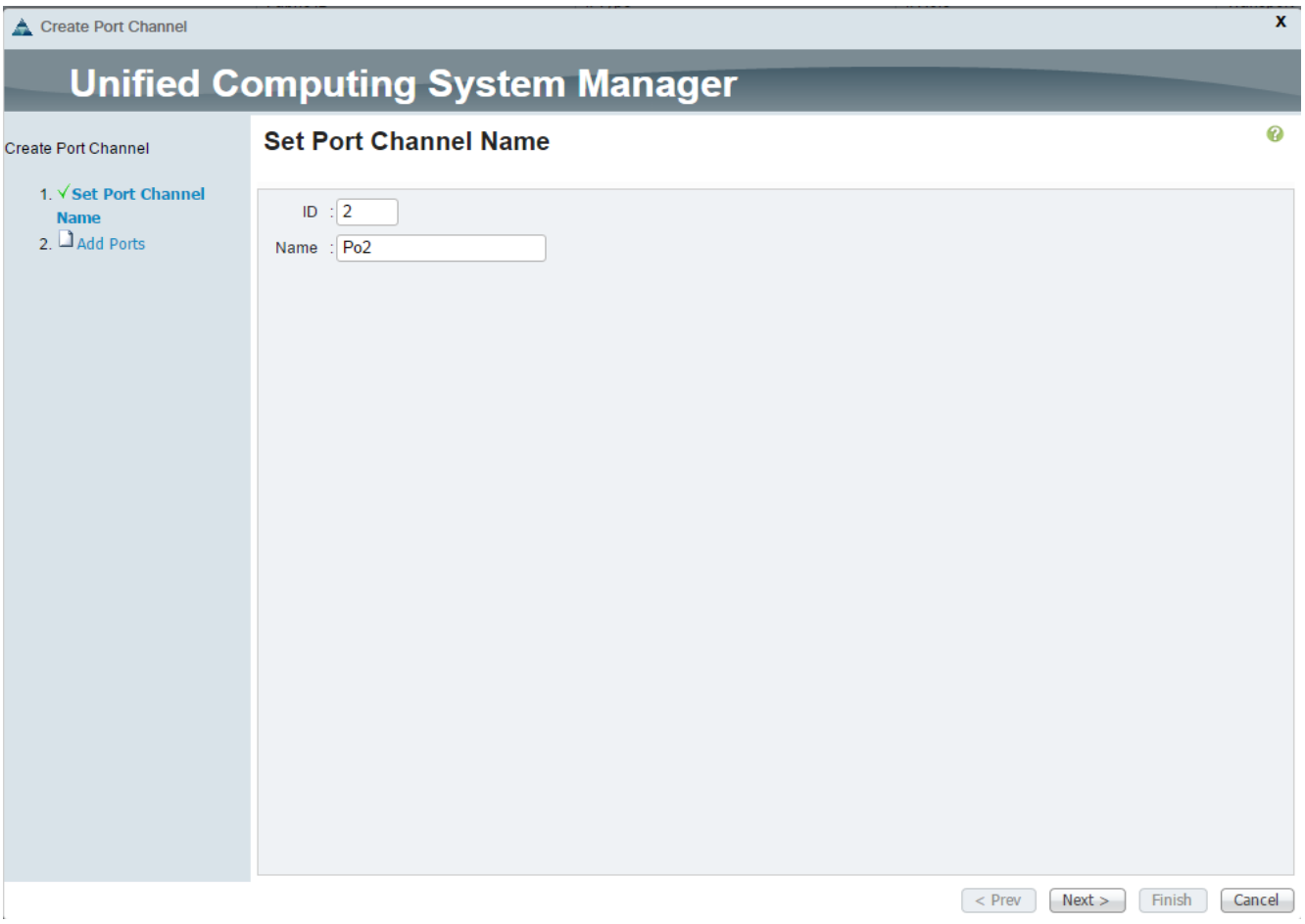




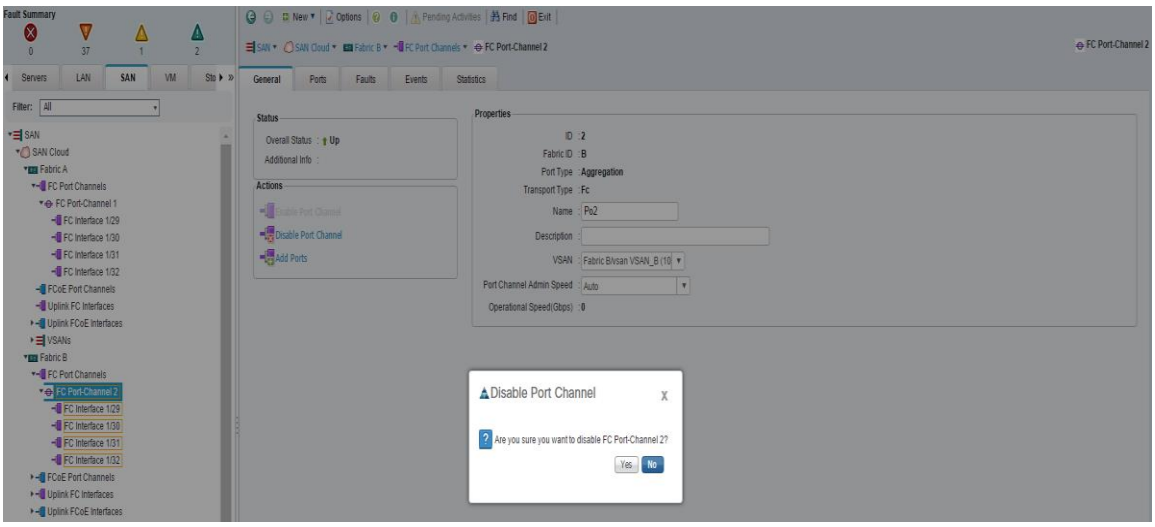
8. Click Save Changes and then click OK.

Fabric-B

1. Click the SAN tab. In the navigation pane, under SAN > SAN Cloud, expand the Fabric B tree.
2. Right-click FC Port Channels.
3. Choose Create Port Channel.
4. Enter `2` for the port channel ID and `Po2` for the port channel name.



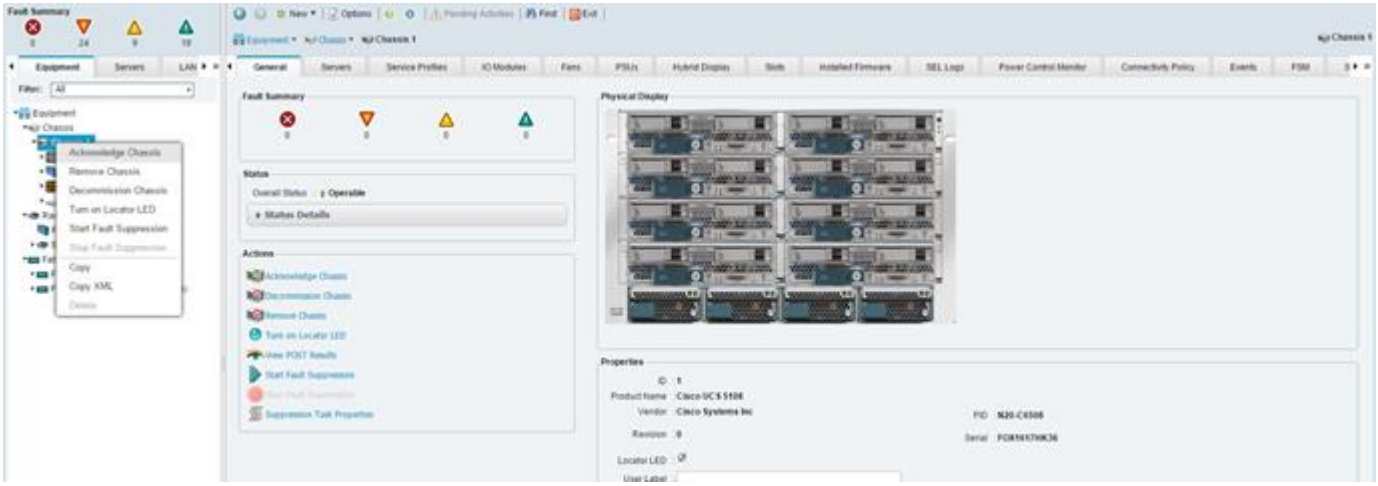
5. Click Next.
6. Choose ports `29-32` and click >> to add the ports to the port channel.
7. Click Finish, Click OK.
8. Under the VSAN drop-down, select `VSAN 102`, click Save Changes, and click OK.
9. To initialize a quick sync of the connections to the Cisco MDS switch, right click the port channel created, and select disable port channel, then re-enable the port channel. Repeat this step for the port channel created for Fabric-A.



Acknowledge Cisco UCS Chassis and Cisco UCS C-Series

To acknowledge all Cisco UCS chassis and C-Series Servers, complete the following steps:

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



4. If C-Series servers are part of the configuration, expand Rack Mounts.
5. Right-click each Server under Rack-Mounts that is listed and select Acknowledge. If FEX is used for the Cisco UCS C-Series servers, acknowledge FEX.

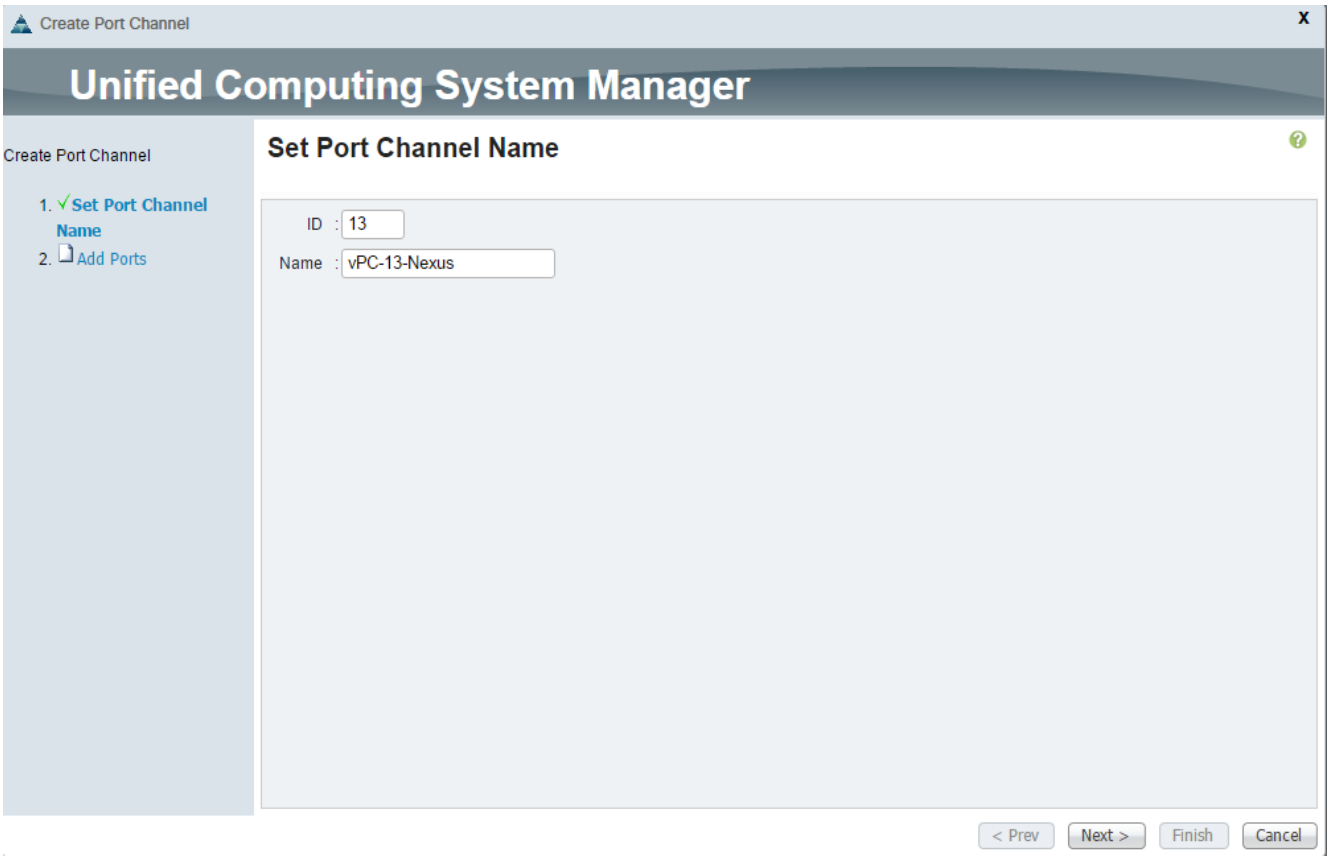
Create Uplink Port Channels to Cisco Nexus Switches

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

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

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.

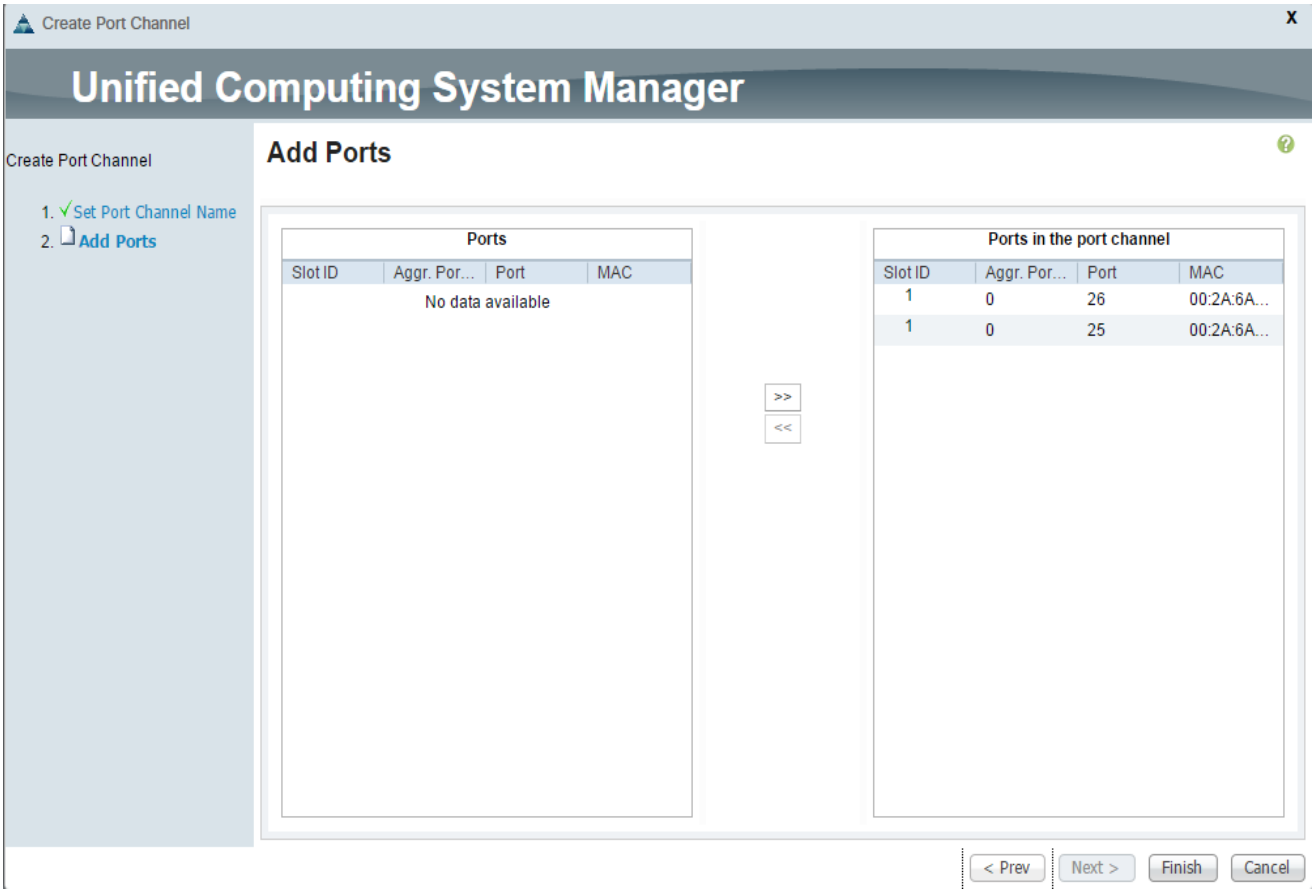


8. Select the following ports to be added to the port channel:

— Slot ID 1 and port 25

— Slot ID 1 and port 26

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 25
    - Slot ID 1 and port 26
19. Click >> to add the ports to the port channel.
20. Click Finish to create the port channel.
21. Click OK.

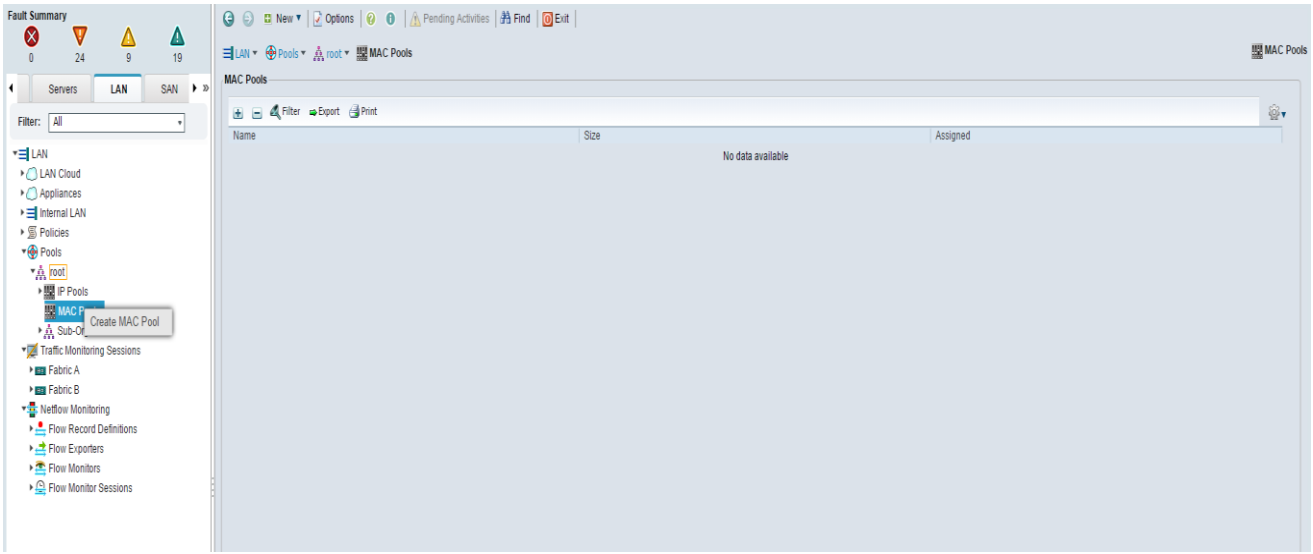
Create MAC Address Pools

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.

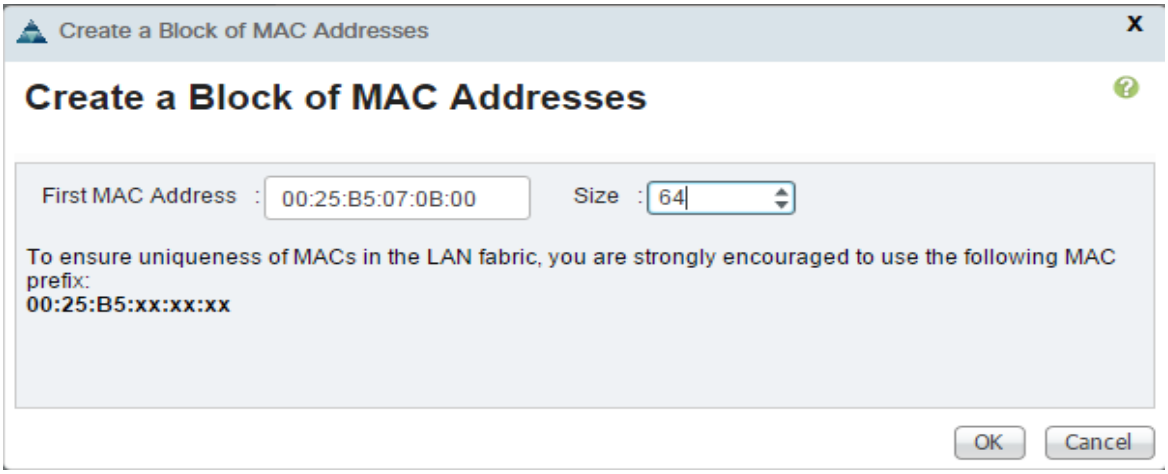
10. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources.

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.



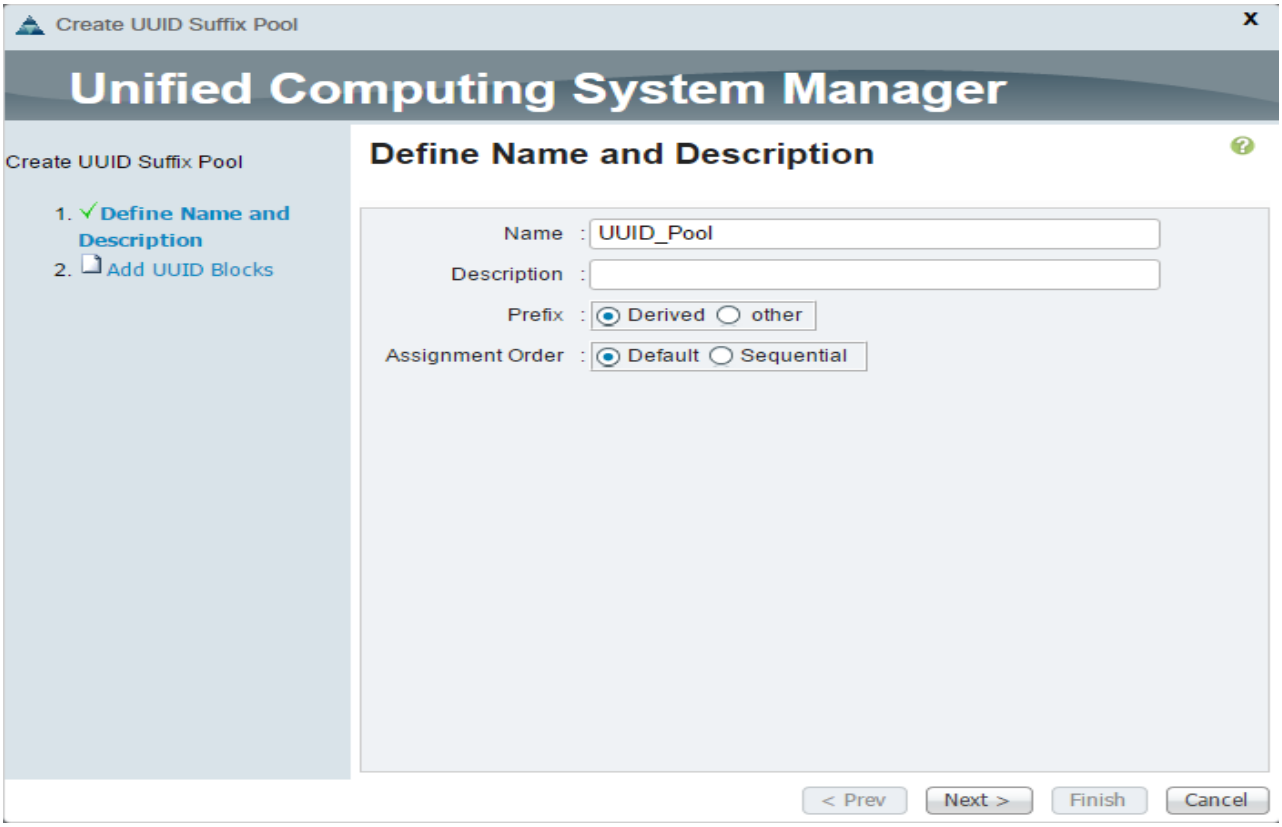
22. Click OK.
23. Click Finish.
24. In the confirmation message, click OK.

Create UUID Suffix Pool

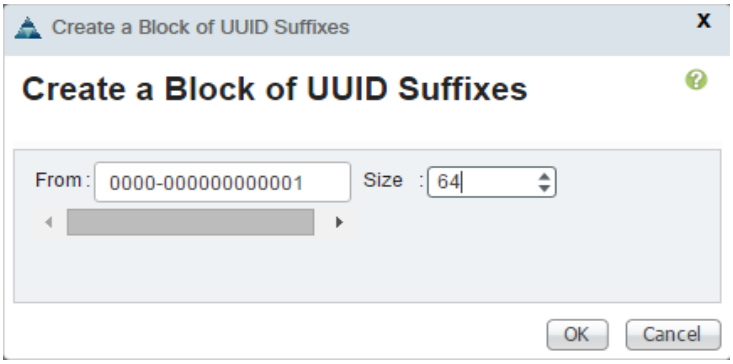
To configure the necessary universally unique identifier (UUID) suffix pool for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click Servers tab in the navigation pane.
2. Select Pools > root.
3. Right-click UUID Suffix Pools.

4. Select Create UUID Suffix Pool
5. Enter `UUID_Pool` as the name of the UUID suffix pool.



6. Optional: Enter a description for the UUID suffix pool.
7. Keep the prefix at the derived option.
8. Click Next.
9. Click Add to add a block of UUIDs.
10. Keep the From field at the default setting.
11. Specify a size for the UUID block that is sufficient to support the available blade or server resources.



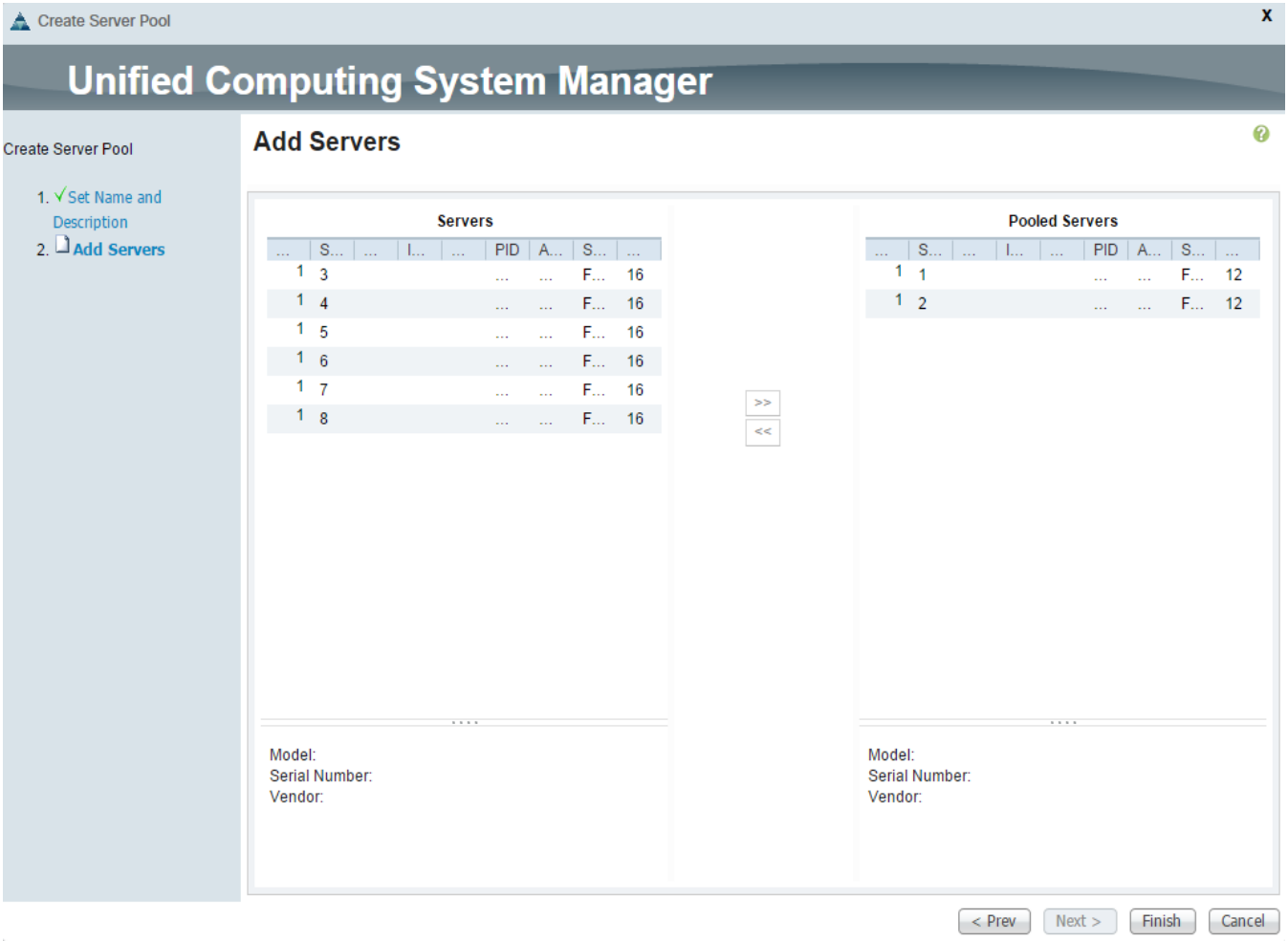
12. Click OK.
13. Click Finish.
14. Click OK.

Create Server Pool

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

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 the 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.

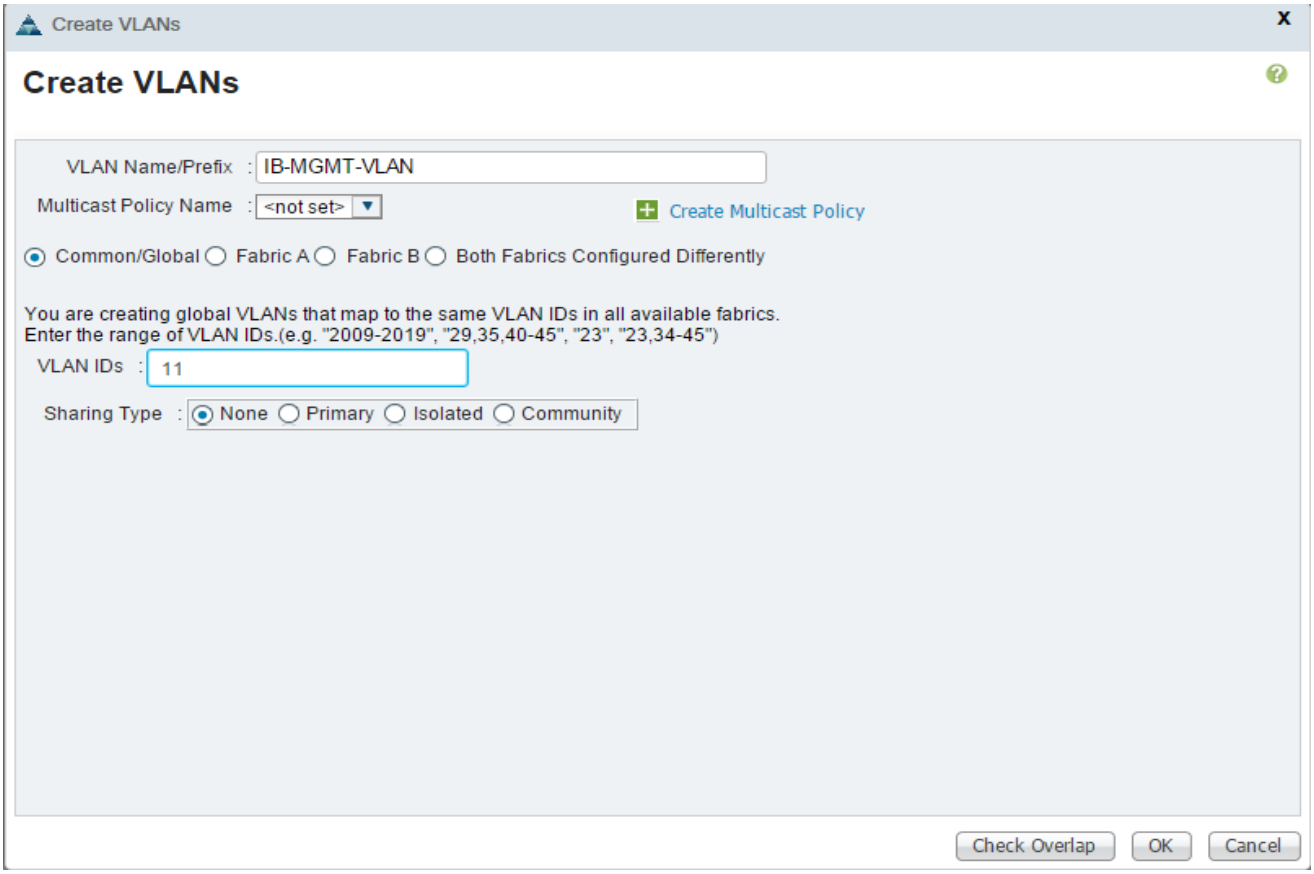
3. Right-click VLANs.

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.

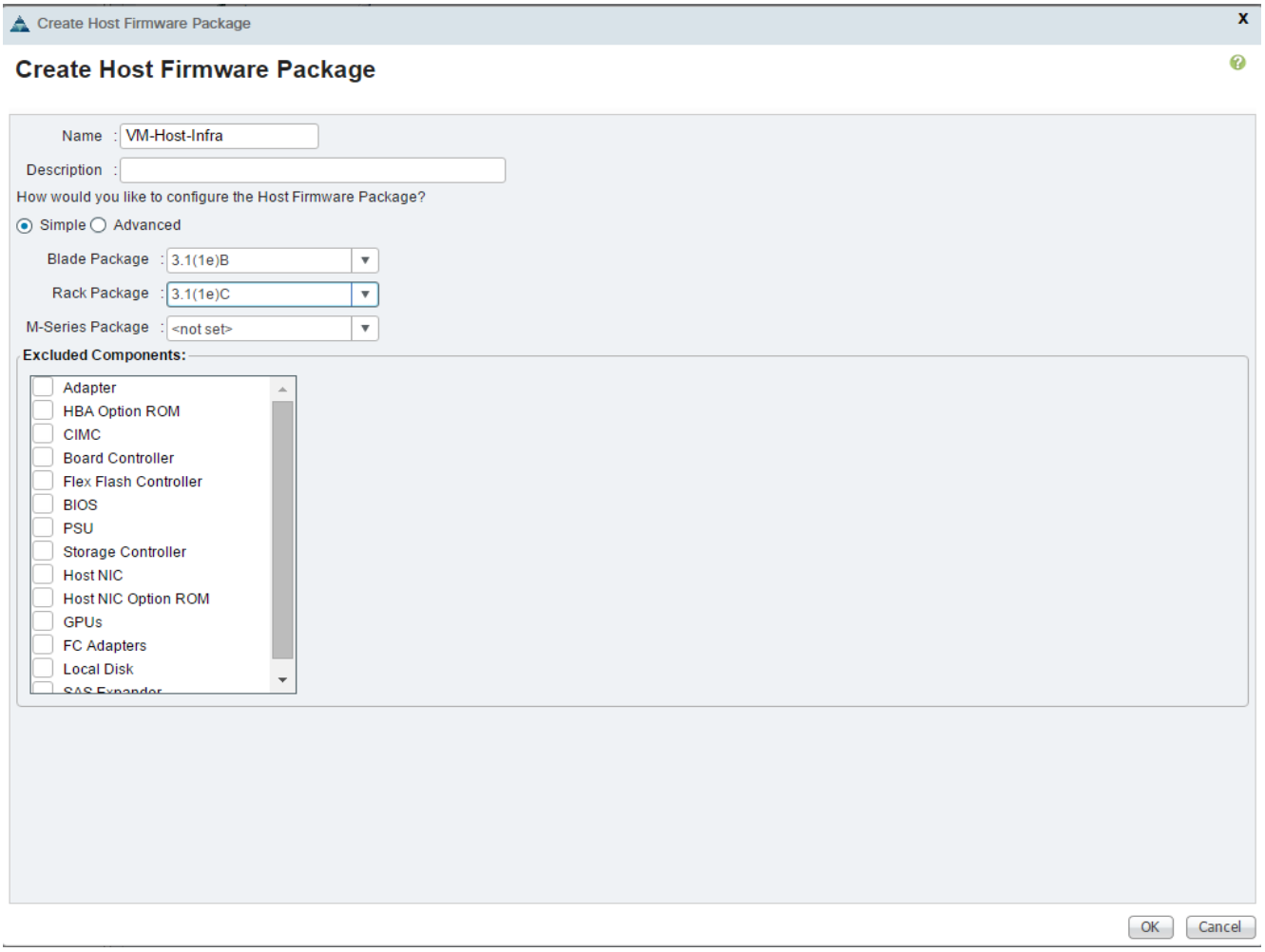
20. Keep the Common/Global option selected for the scope of the VLAN.
21. Enter the `<<var_vmotion_vlan_id>>` as the ID of the vMotion VLAN.
22. Keep the Sharing Type as None.
23. Click OK, and then click OK again.
24. Right-click VLANs.
25. Select Create VLANs
26. Enter VM-Traffic-VLAN as the name of 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.

Create Host Firmware Package

Firmware management policies allow the administrator to select the corresponding packages for a given server configuration. These policies often include packages for adapter, BIOS, board controller, FC adapters, host bus adapter (HBA), 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 3.1(1e) for both the Blade and Rack Packages and also for M-Series Package if M-Series servers are managed.
8. Click OK to create the host firmware package.
9. Click OK.

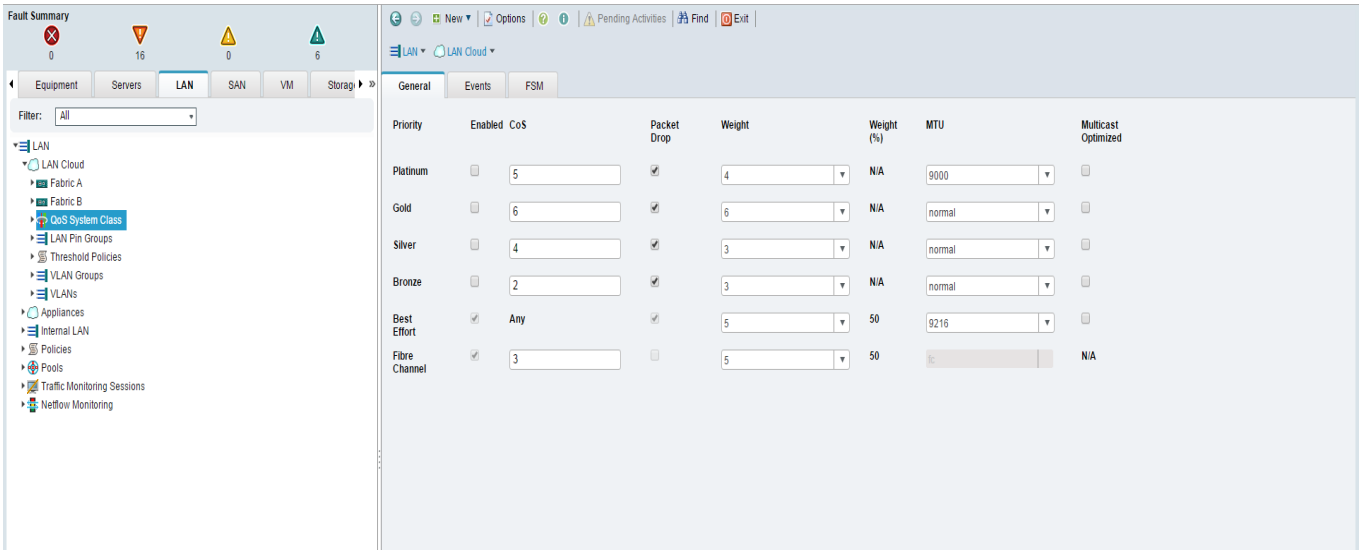


Set Jumbo Frames in Cisco UCS Fabric

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 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



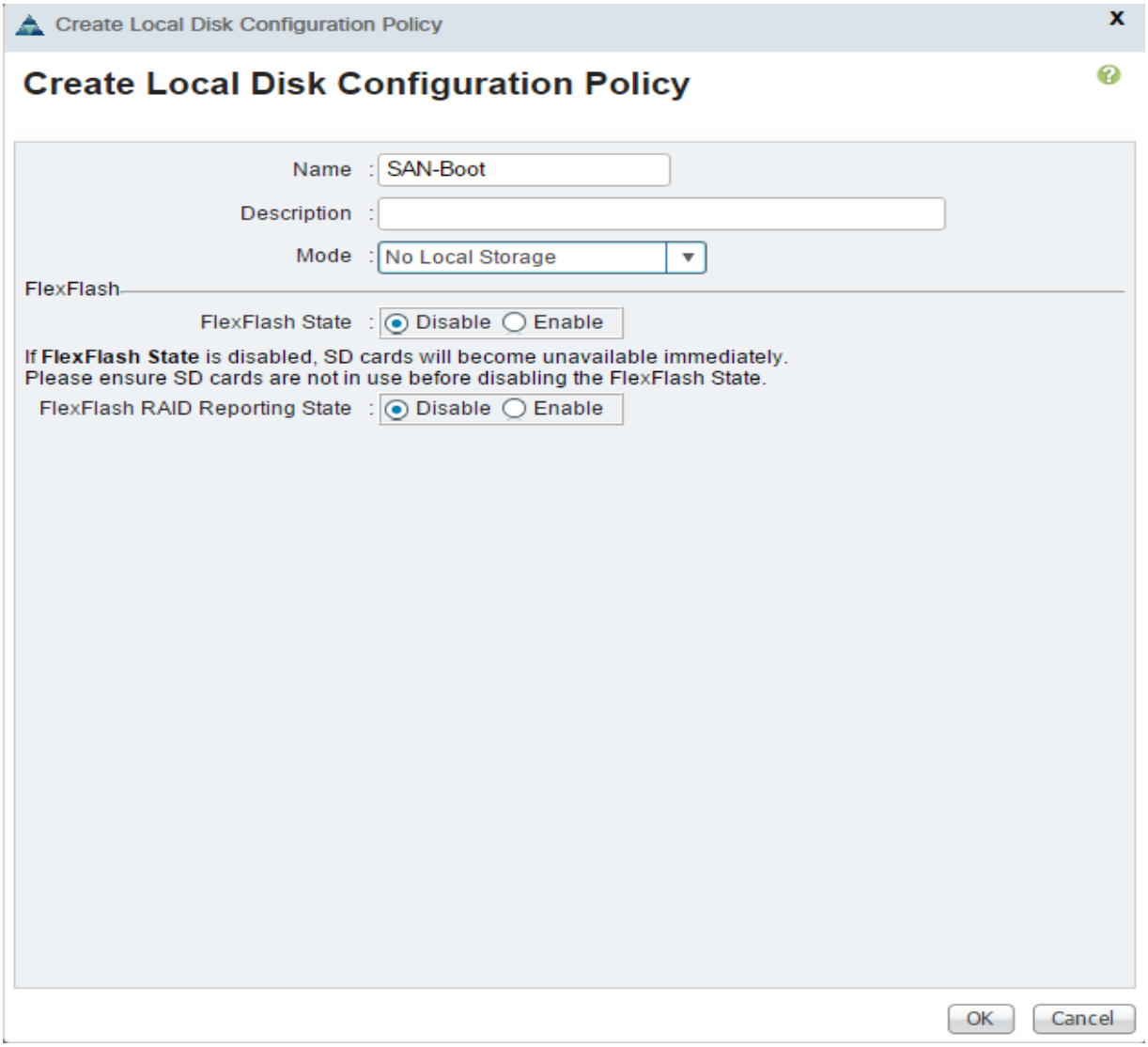
Create Local Disk Configuration Policy (Optional)

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:

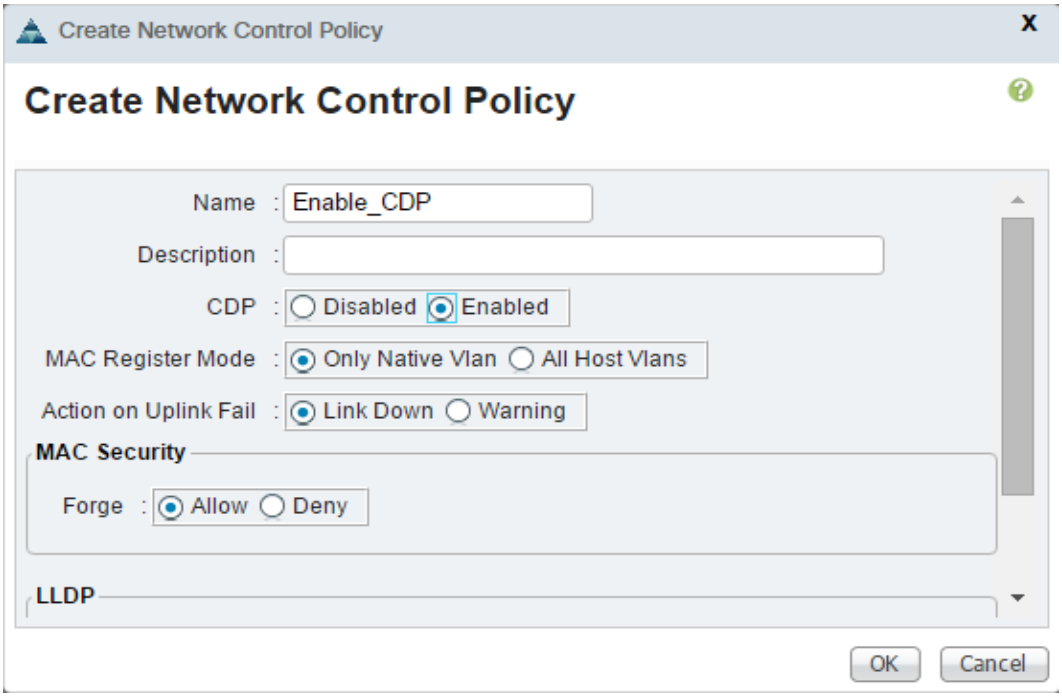
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Local Disk Config Policies.
4. Select Create Local Disk Configuration Policy.
5. Enter `SAN-Boot` as the local disk configuration policy name.
6. Change the mode to No Local Storage.
7. Click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

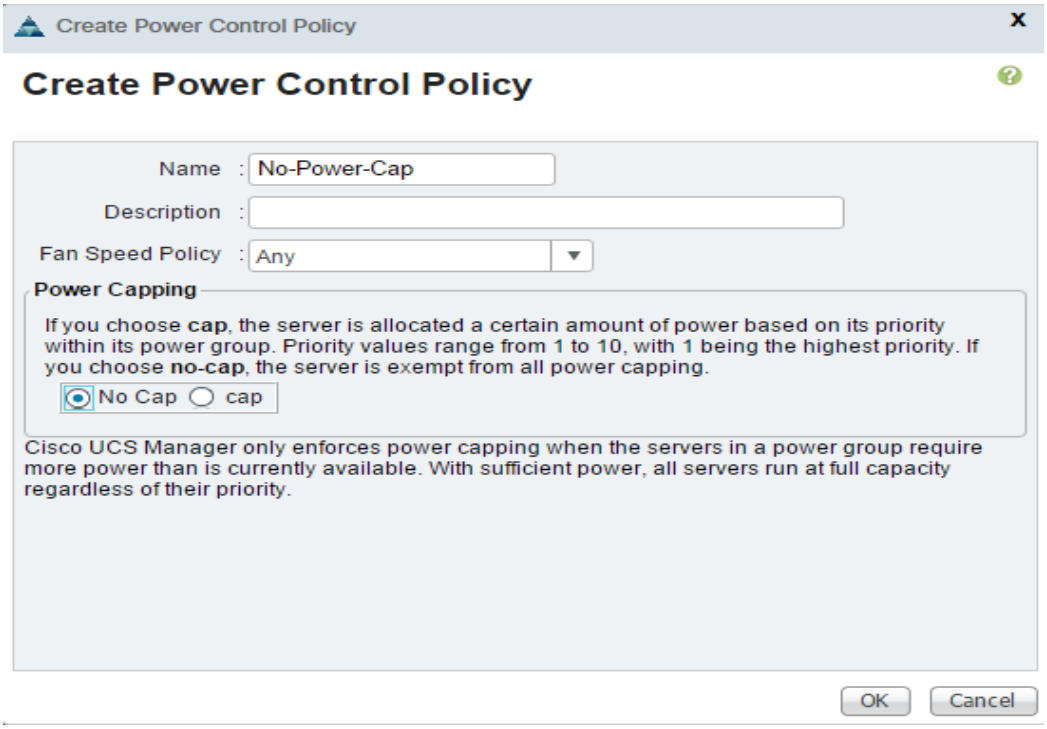


8. Click OK.

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.

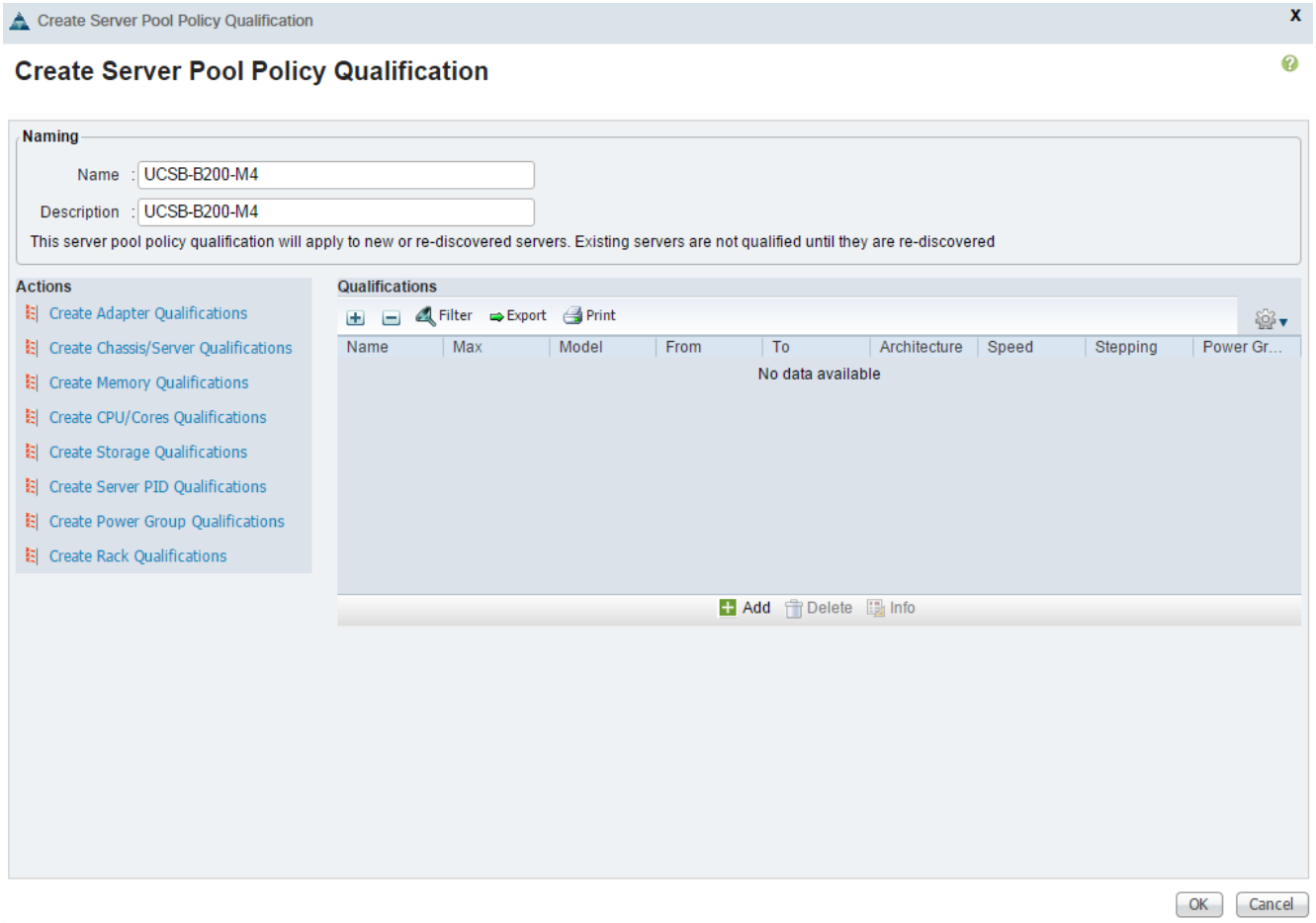


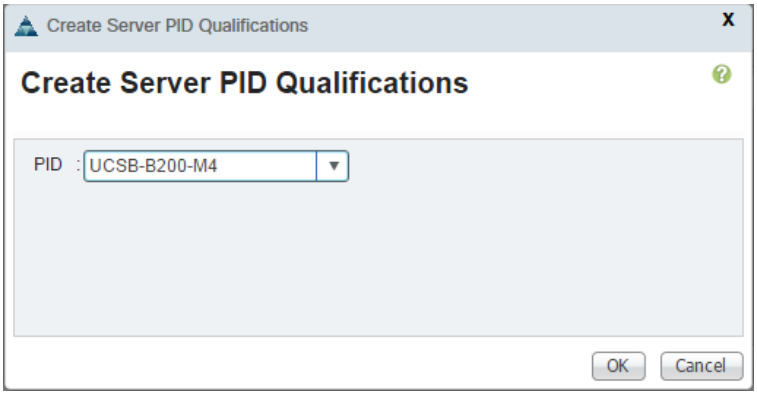
Create Server Pool Qualification Policy (Optional)

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.



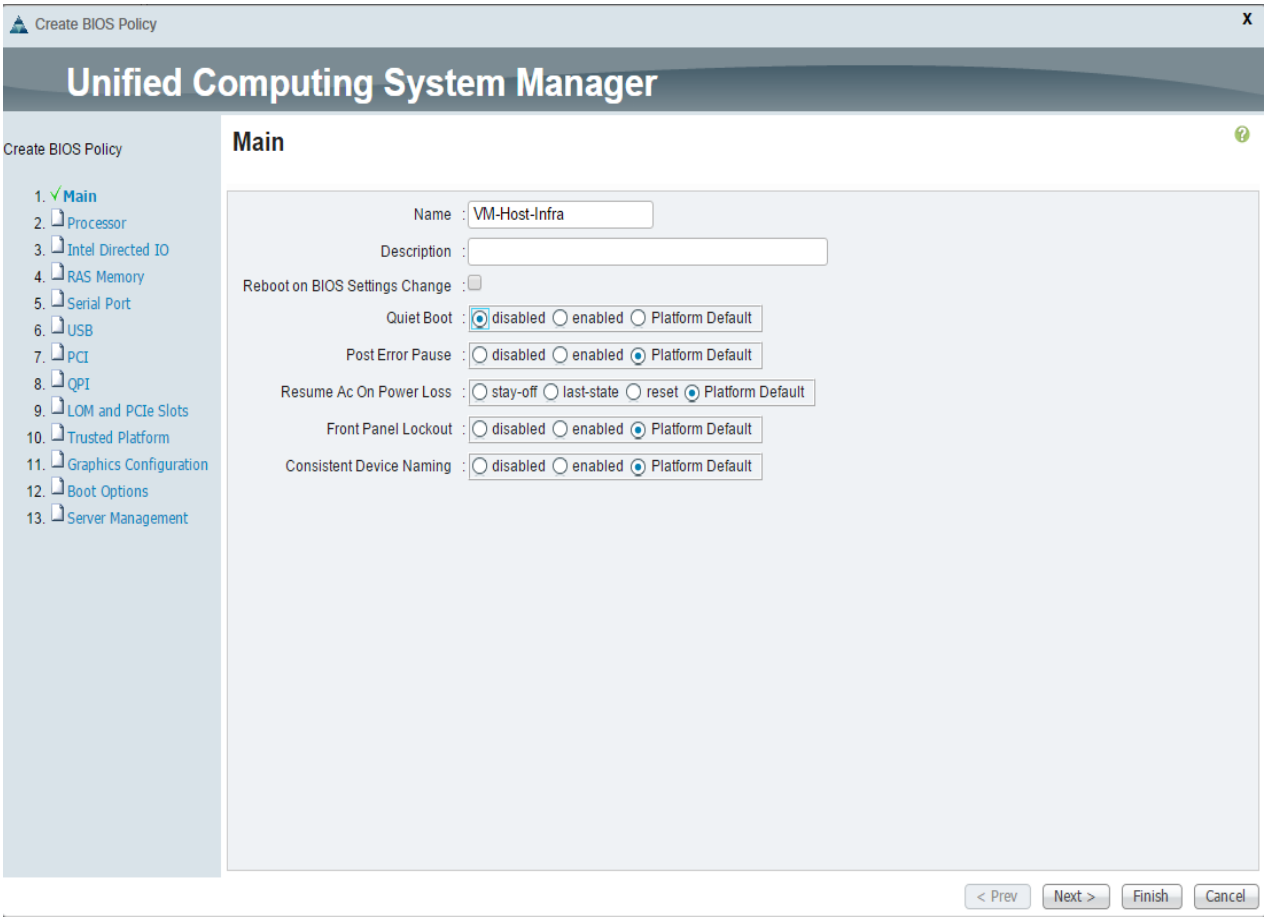


Create Server BIOS Policy

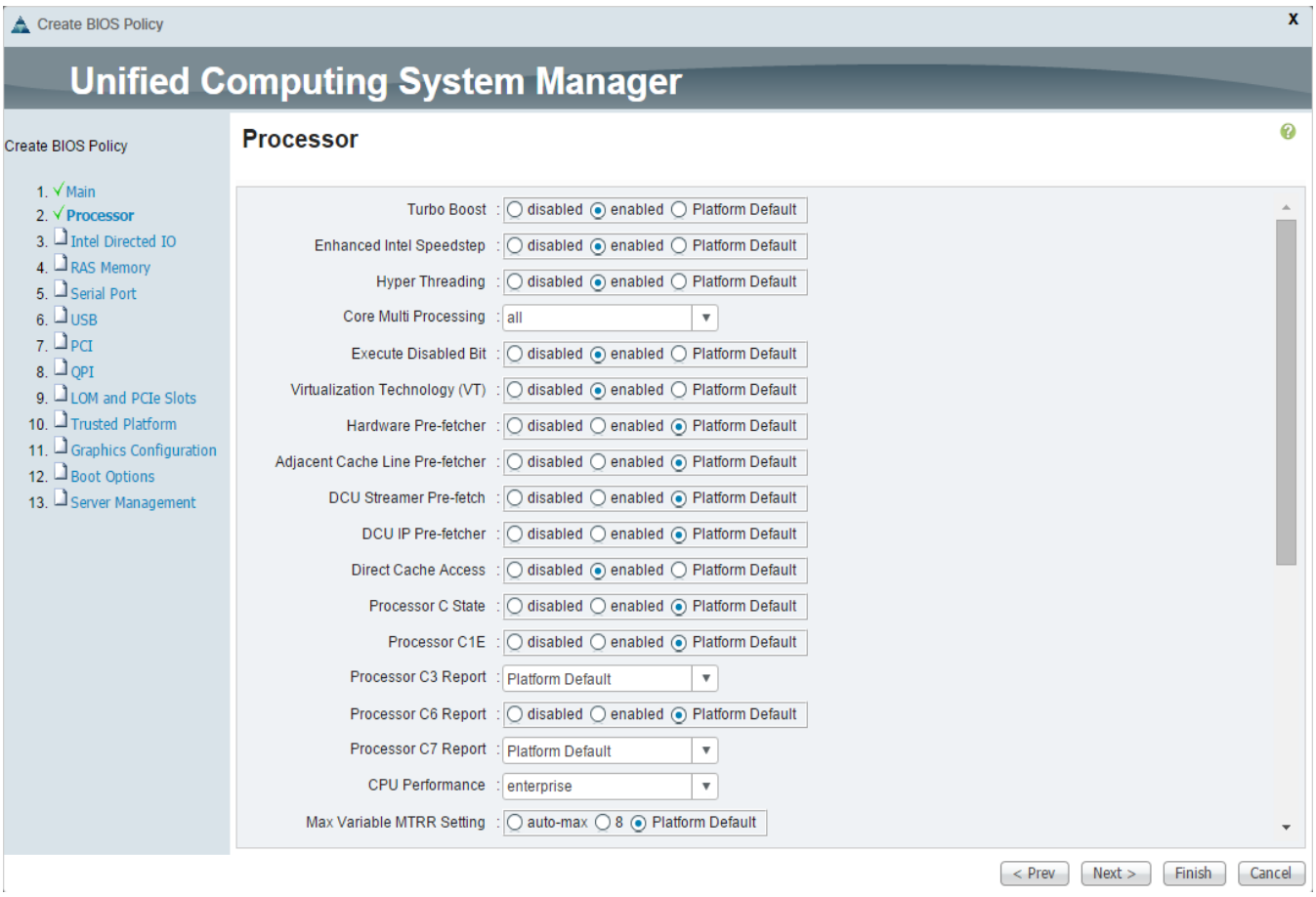
To create a server BIOS policy for the Cisco UCS environment, complete the following steps:

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.

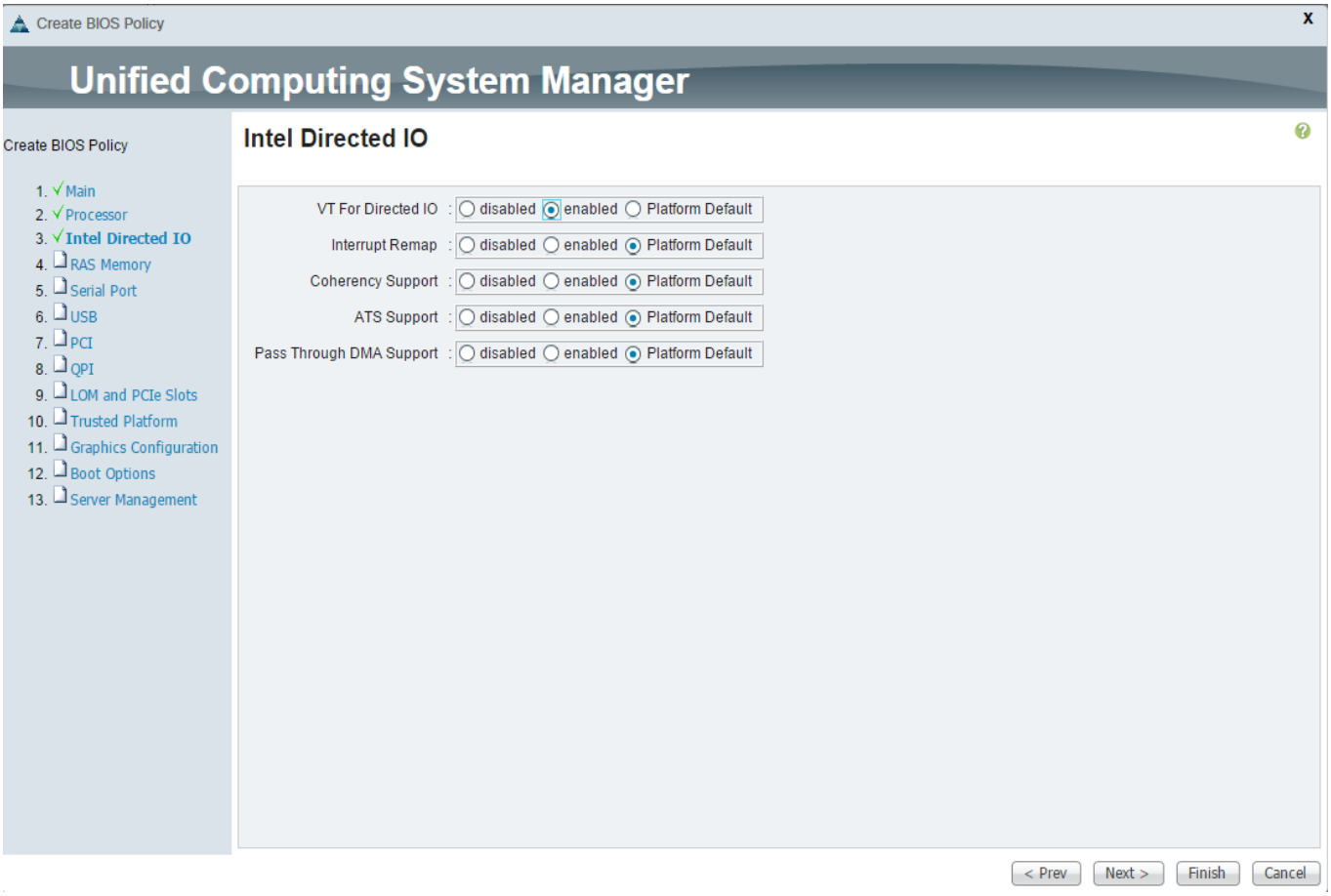


8. Change Turbo Boost to enabled.
9. Change Enhanced Intel Speedstep to enable.
10. Change Hyper Threading to enabled.
11. Change Core Multi Processing to all.
12. Change Execution Disabled Bit to enabled.
13. Change Virtualization Technology (VT) to enabled.
14. Change Direct Cache Access to enabled.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

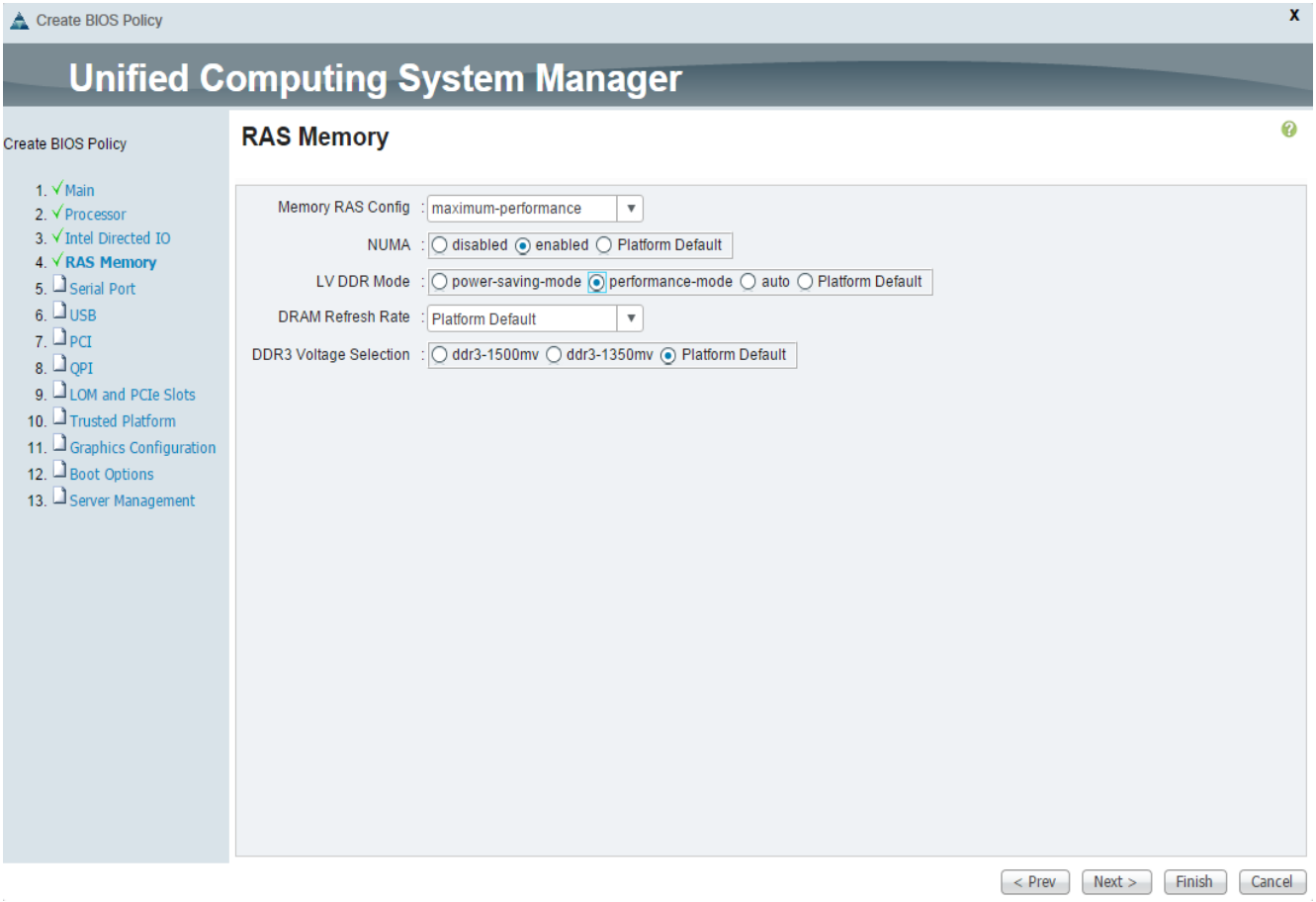


16. Click Next to go the Intel Directed IO Screen.

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.



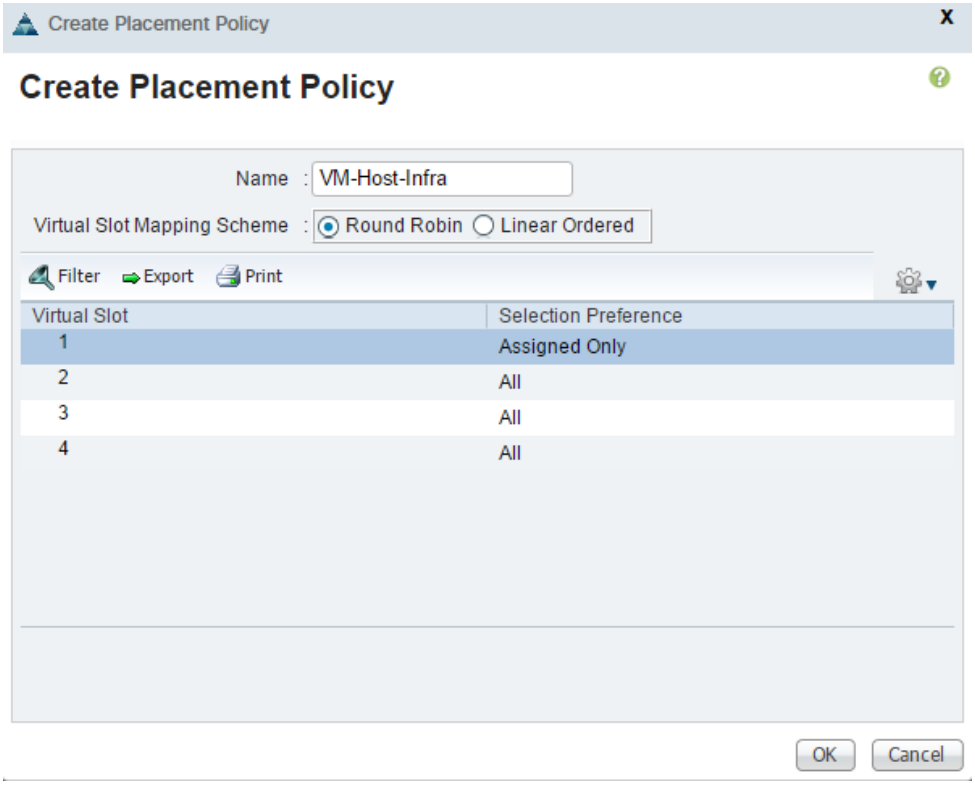
22. Click Finish to create the BIOS policy.

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:

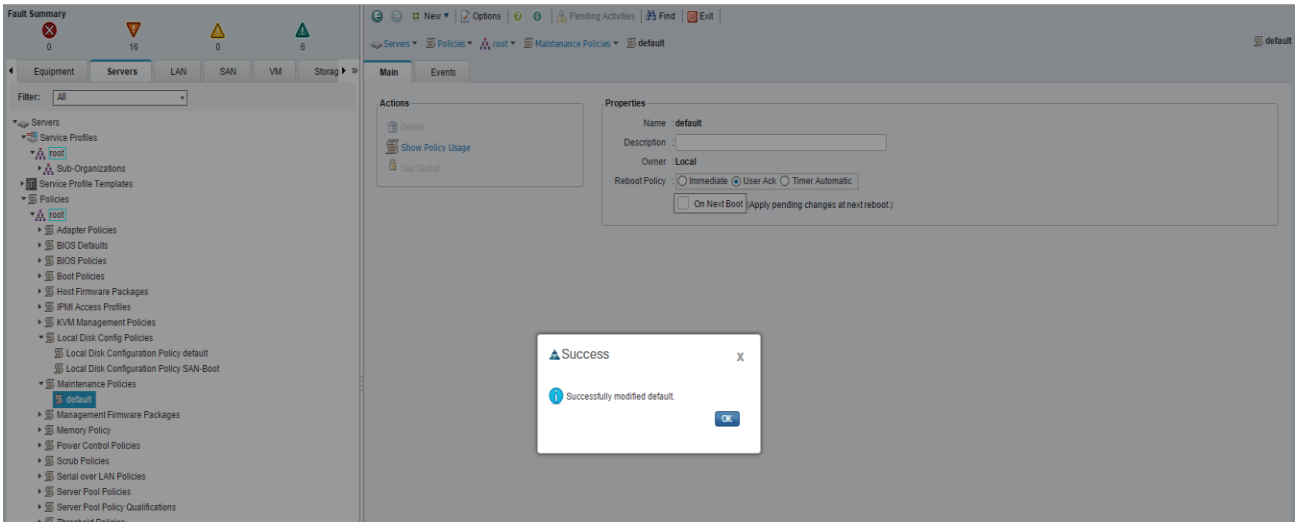
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click vNIC/vHBA Placement Policies.
4. Select Create Placement Policy.
5. Enter `VM-Host-Infra` as the name of the placement policy.
6. Click 1 and select Assigned Only.
7. Click OK and then click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



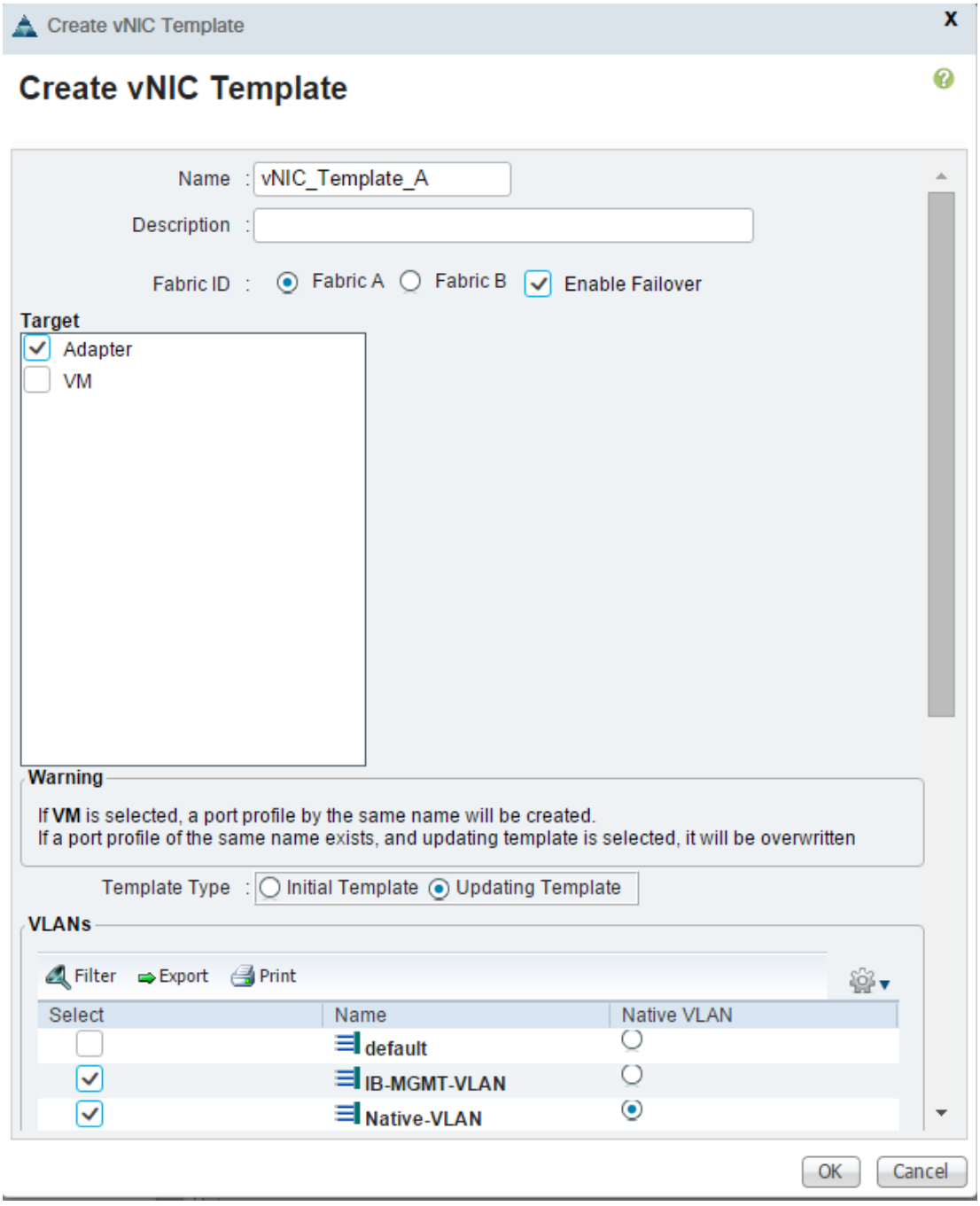
Create vNIC Templates

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. Select Policies > root.
2. Right-click vNIC Templates.
3. Select Create vNIC Template.
4. Enter `vNIC_Template_A` as the vNIC template name.
5. Keep `Fabric A` selected.
6. Select the Enable Failover checkbox.
7. Under Target, make sure that the VM checkbox is not selected.
8. Select Updating Template as the Template Type.
9. Under VLANs, select the checkboxes for `IB-MGMT-VLAN`, `NFS-VLAN`, `Native-VLAN`, `VM-Traffic-VLAN`, and `vMotion-VLAN`.
10. Set `Native-VLAN` as the native VLAN.
11. For MTU, enter `9000`.
12. In the MAC Pool list, select `MAC_Pool_A`.
13. In the Network Control Policy list, select `Enable_CDP`.
14. Click OK to create the vNIC template.

15. Click OK.



16. In the navigation pane, select the LAN tab.

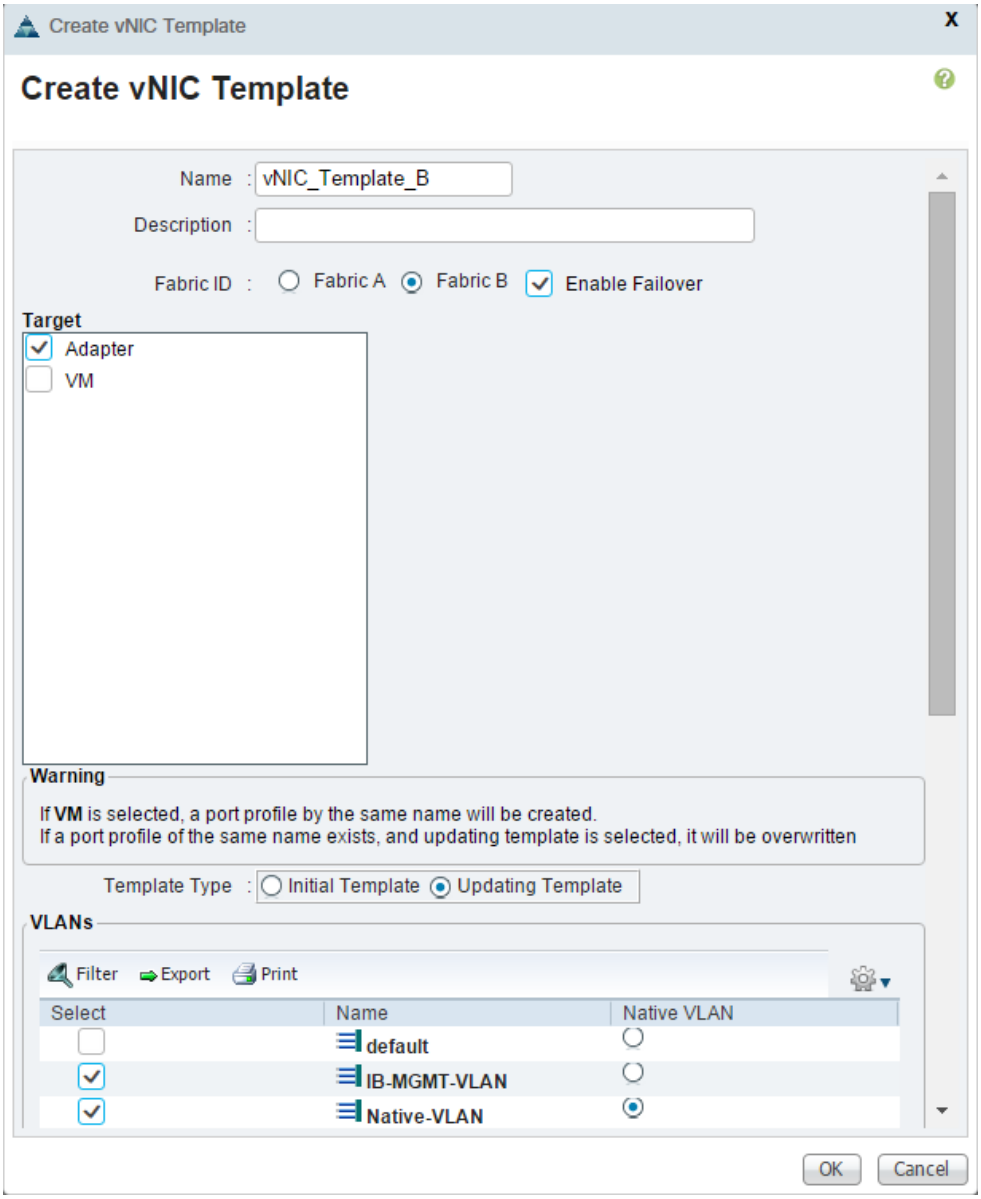
17. Select Policies > root.

18. Right-click vNIC Templates.

19. Select Create vNIC Template

20. Enter `vNIC_Template_B` as the vNIC template name.

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

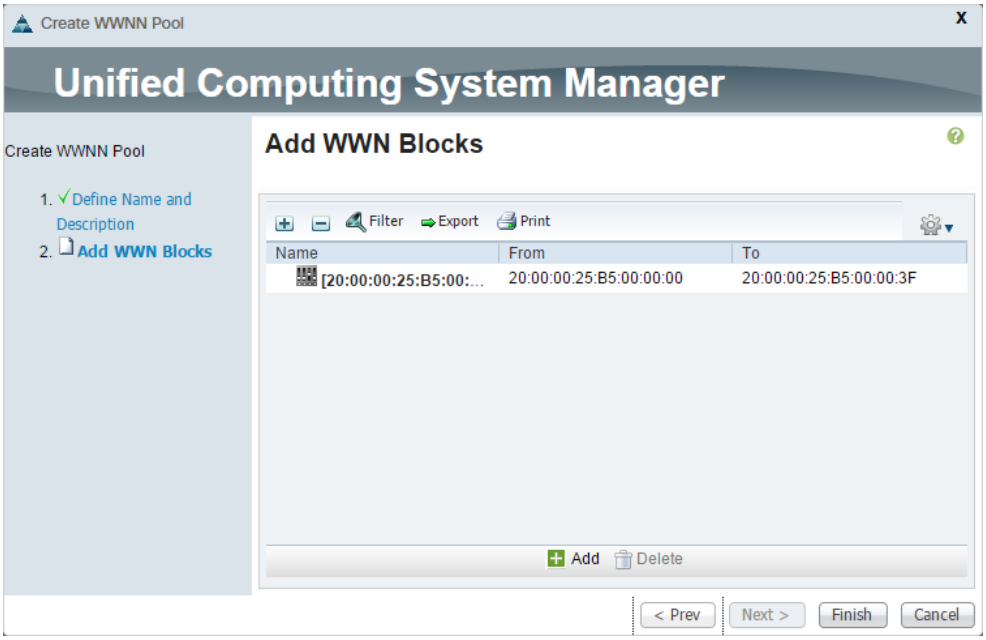


Create WWNN Pools

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

1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Choose Pools > root.
3. Right-click WWNN Pools.
4. Choose Create WWNN Pool.
5. Enter `WWNN_Pool` as the name of the WWNN pool.
6. (Optional) Add a description for the WWNN pool.

7. Click Next.
8. Click Add to add a block of WWNNs.
9. Keep the default block of WWNNs, or specify a base WWNN.
10. Specify a size for the WWNN block that is sufficient to support the available blade or server resources.
11. Click OK.
12. Click Finish.
13. Click OK.



Create WWPN Pools

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

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

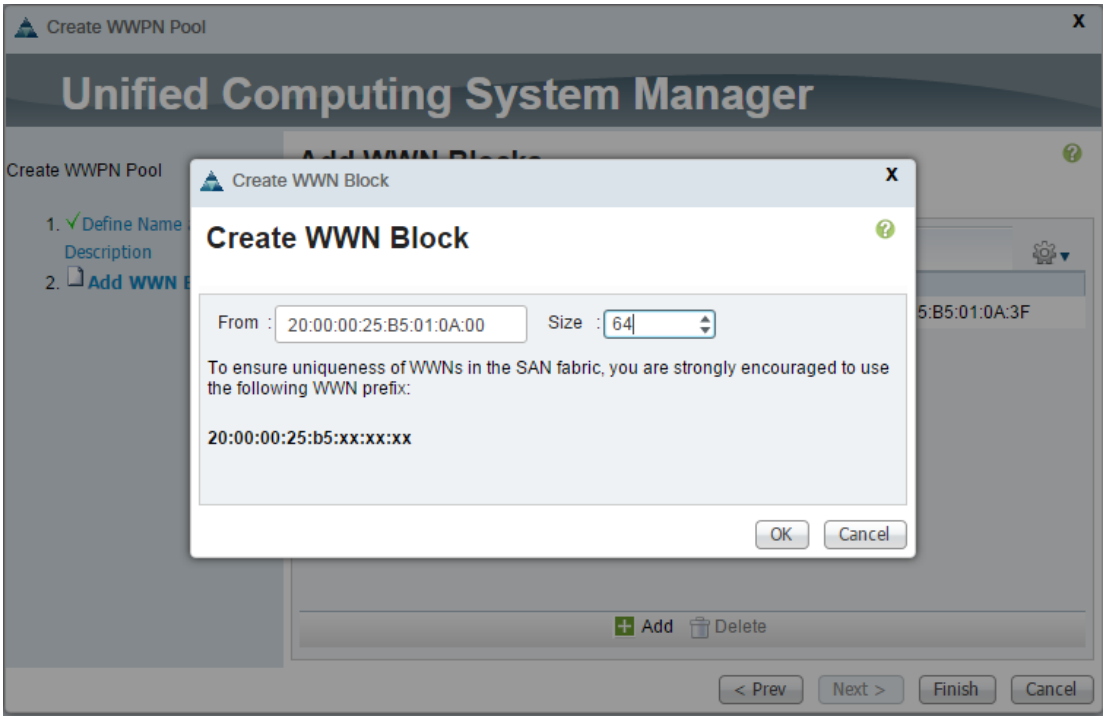
In this procedure, two WWPN pools are create; one for fabric A and one for fabric B.

3. Right-click WWPN Pools.
4. Choose Create WWPN Pool.
5. Enter `WWPN_Pool_A` as the name of the WWPN pool for fabric A.
6. (Optional) Enter a description for this WWPN pool.

7. Click Next.
8. Click Add to add a block of WWPNs.
9. Specify the starting WWPN in the block for fabric A.

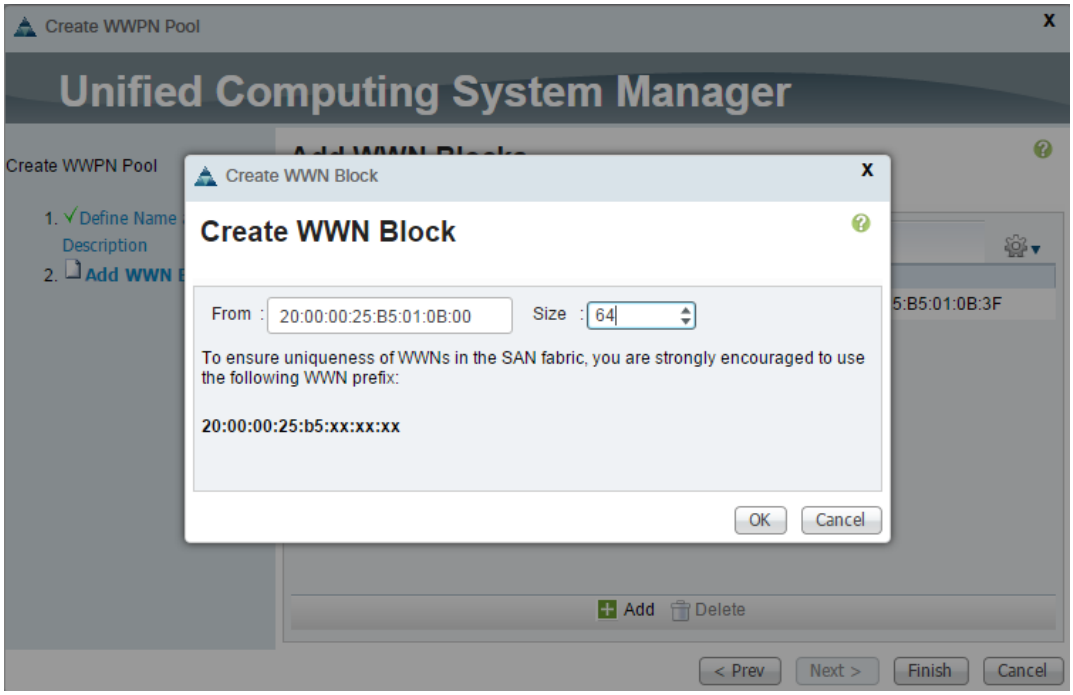
For the VersaStack solution, the recommendation is to place 0A in the next-to-last octet of the starting WWPN to identify all the WWPNs in this pool as Fabric A addresses.

10. Specify a size for the WWPN block that is sufficient to support the available blade or server resources.
11. Click OK.
12. Click Finish to create the WWPN pool.
13. Click OK.



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

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



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

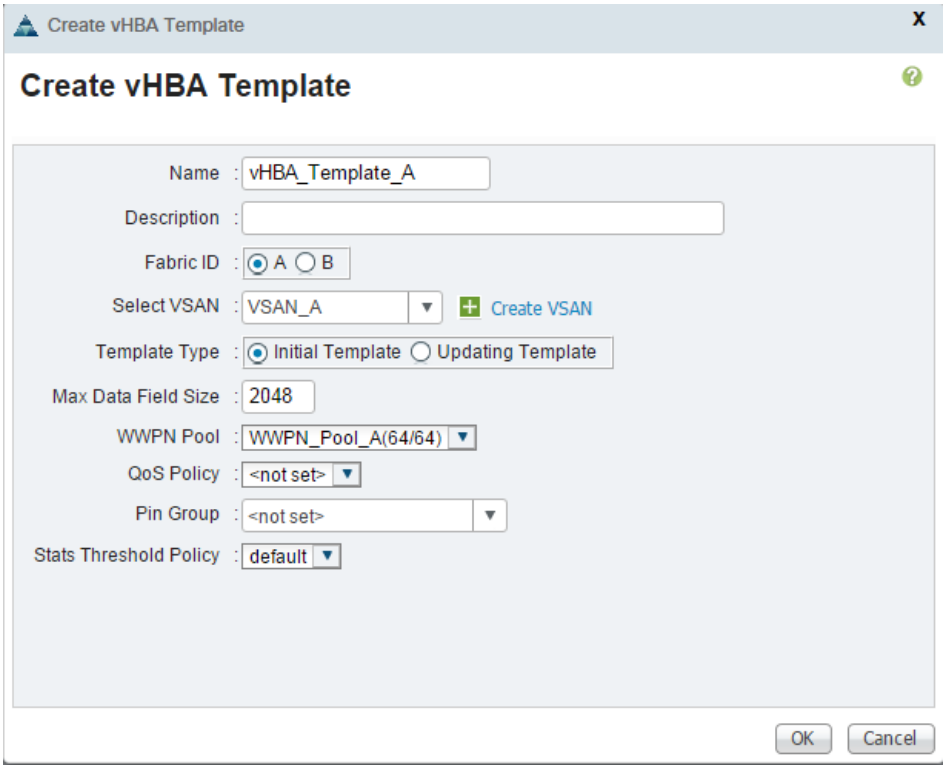
21. Specify a size for the WWPN block that is sufficient to support the available blade or server resources.
22. Click OK.
23. Click Finish.
24. Click OK.

Create vHBA Templates for Fabric A and Fabric B

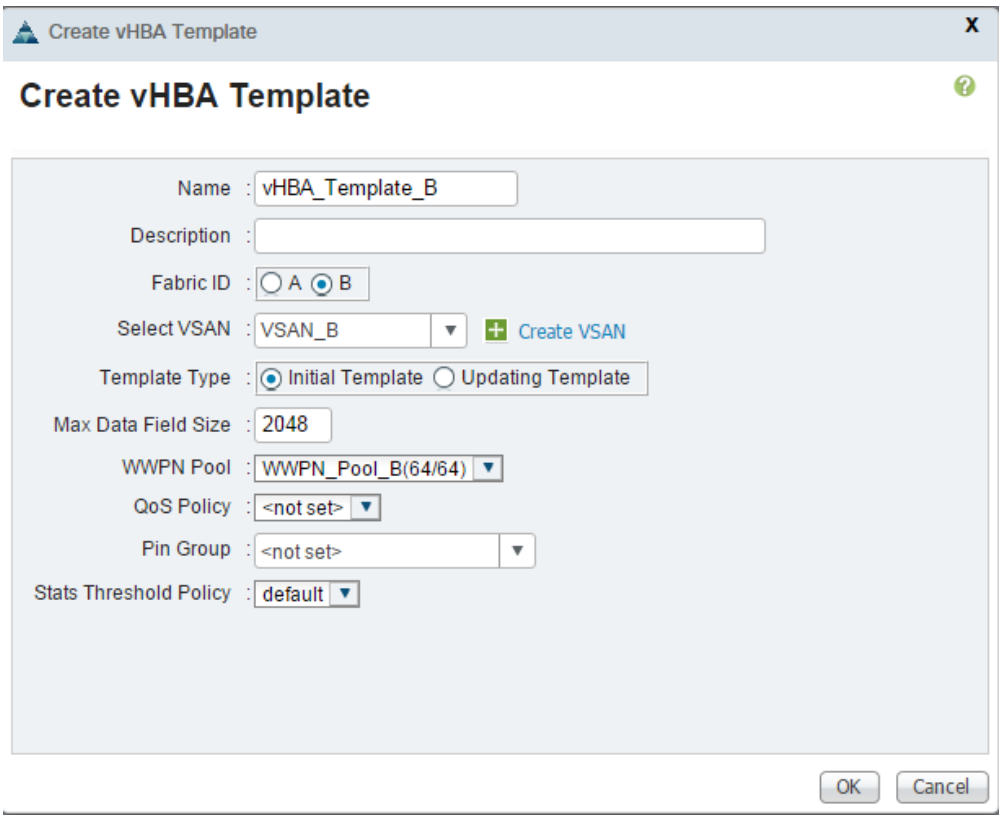
To create multiple virtual host bus adapter (vHBA) templates for the Cisco UCS environment, follow these steps:

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

7. In the Select VSAN list, Choose `VSAN_A`.
8. In the WWPN Pool list, Choose `WWPN_Pool_A`.
9. Click OK to create the vHBA template.
10. Click OK.



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



Create Boot Policies

This procedure applies to a Cisco UCS environment in which two FC interfaces are used on the IBM V9000 cluster Controller 1 and two FC interfaces used on Controller 2 for the Hosts connectivity.

Two boot policies need to be created. The first boot policy will be created to boot from Fabric A and the second to boot from Fabric B. Though not absolutely necessary to have two boot policies, having two options helps spread the load and helps ensure that a total failure does not happen if a disaster occur which may removes an entire fabric.

For this example, the following WWPN values are used for the V9000. Your ports may vary depending on the configuration of your V9000.

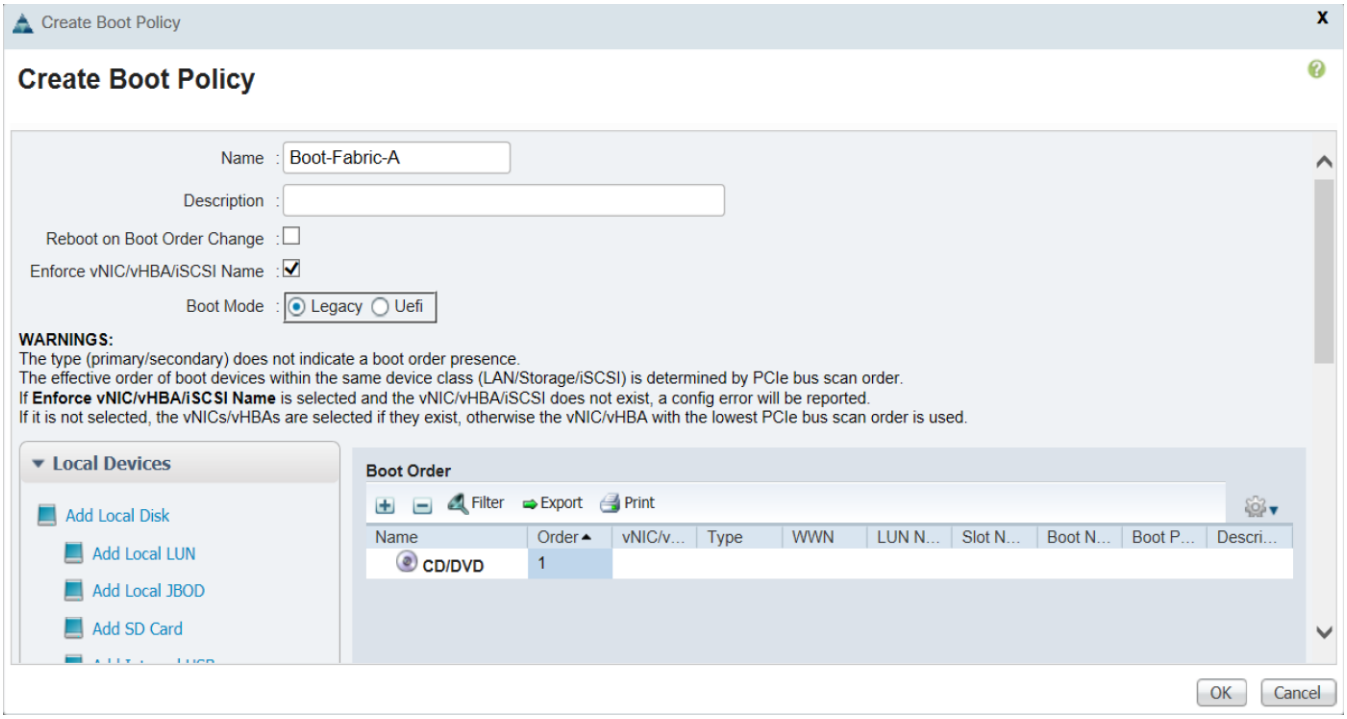
To create boot policies for the Cisco UCS environment, complete the following steps:

Use the WWPN variables that were logged into the storage section of the WWPN table.

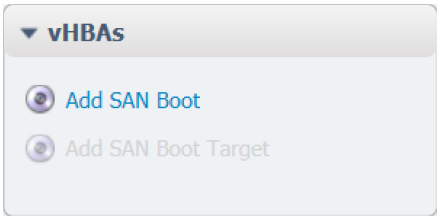
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Choose Policies > root.
3. Right-click Boot Policies.
4. Choose Create Boot Policy.
5. Enter `Boot-Fabric-A` as the name of the boot policy.
6. (Optional) Enter a description for the boot policy.

7. Keep the Reboot on Boot Order Change check box unchecked.

8. Expand the Local Devices drop-down menu and Choose Add `CD/DVD` (you should see local and remote greyed out).



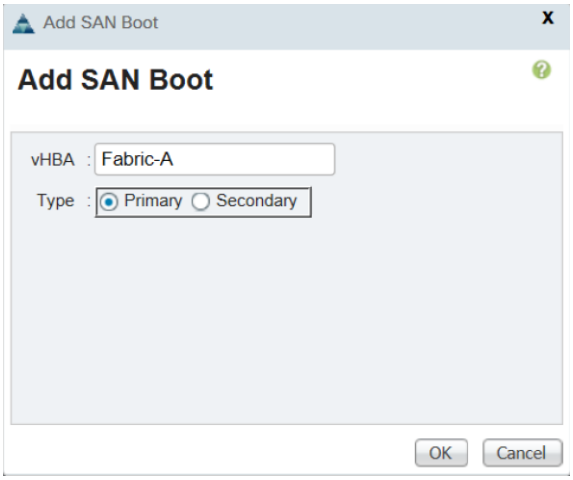
9. Expand the vHBAs drop-down menu and Choose Add SAN Boot.



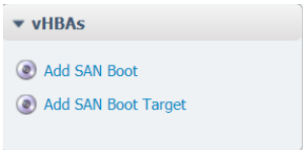
10. In the Add SAN Boot dialog box, enter `Fabric-A` in the vHBA field.

11. Make sure that the Primary radio button is selected as the SAN boot type.

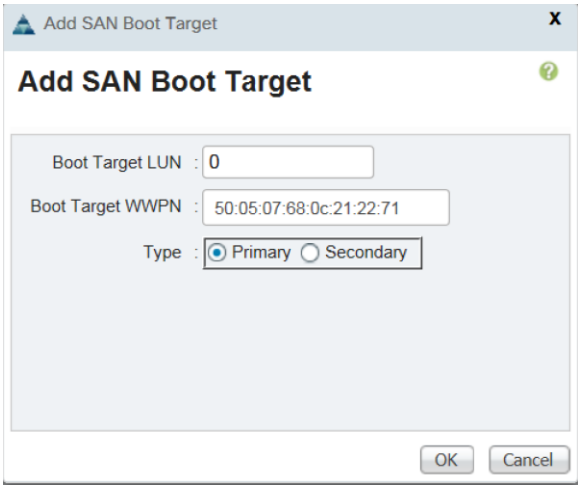
12. Click OK to add the SAN boot initiator.



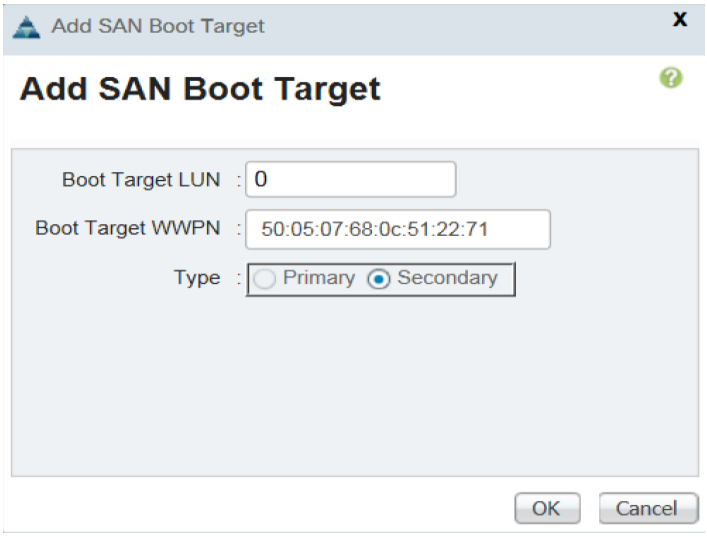
13. From the vHBA drop-down menu, choose Add SAN Boot Target.



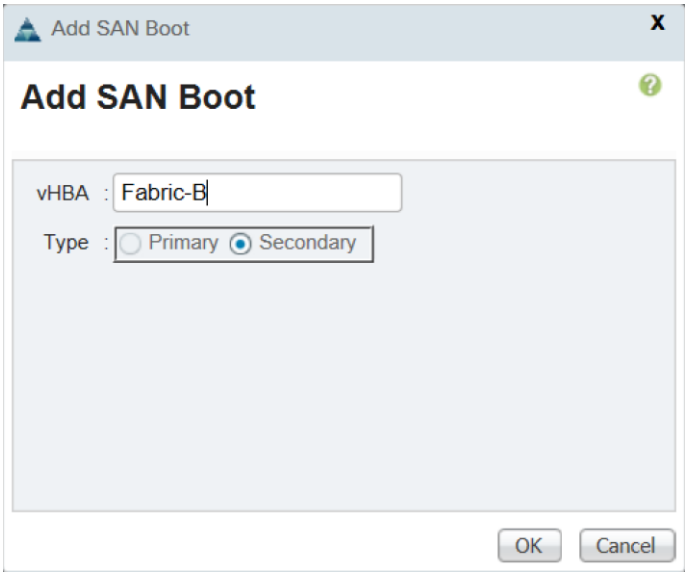
14. Keep 0 as the value for Boot Target LUN.
15. Enter the WWPN for Controller A going to switch A `<<var_wwpn_FC_ContA-FE1-fabricA>>`
16. Keep the Primary radio button selected as the SAN boot target type.
17. Click OK to add the SAN boot target.



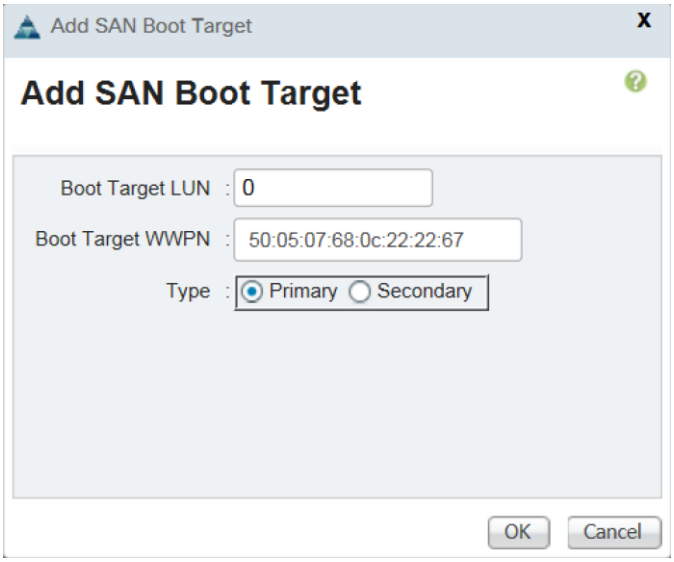
18. From the vHBA drop-down menu, choose Add SAN Boot Target.
19. Keep 0 as the value for Boot Target LUN.
20. Enter the WWPN for Controller A going to switch A `<<var_wwpn_FC_ContA-FE3-fabricA>>`
21. Click OK to add the SAN boot target.



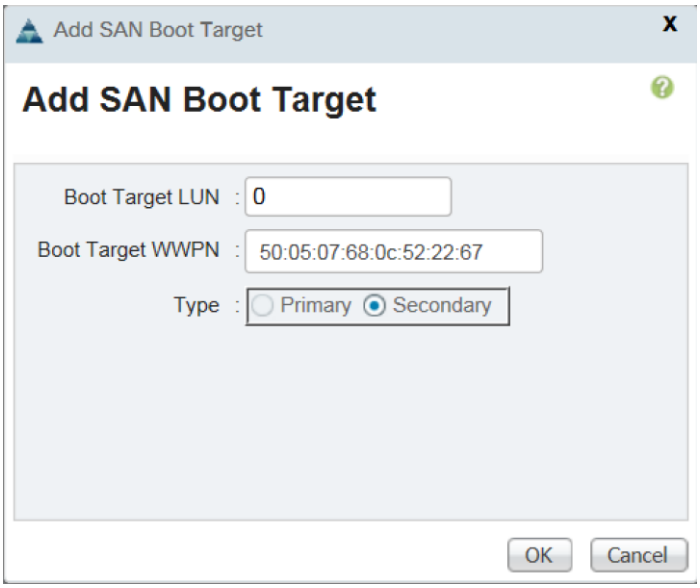
22. From the vHBA drop-down menu, choose Add SAN Boot.
23. In the Add SAN Boot dialog box, enter `Fabric-B` in the vHBA box.
24. The SAN boot type should automatically be set to Secondary
25. Click OK to add the SAN boot initiator.



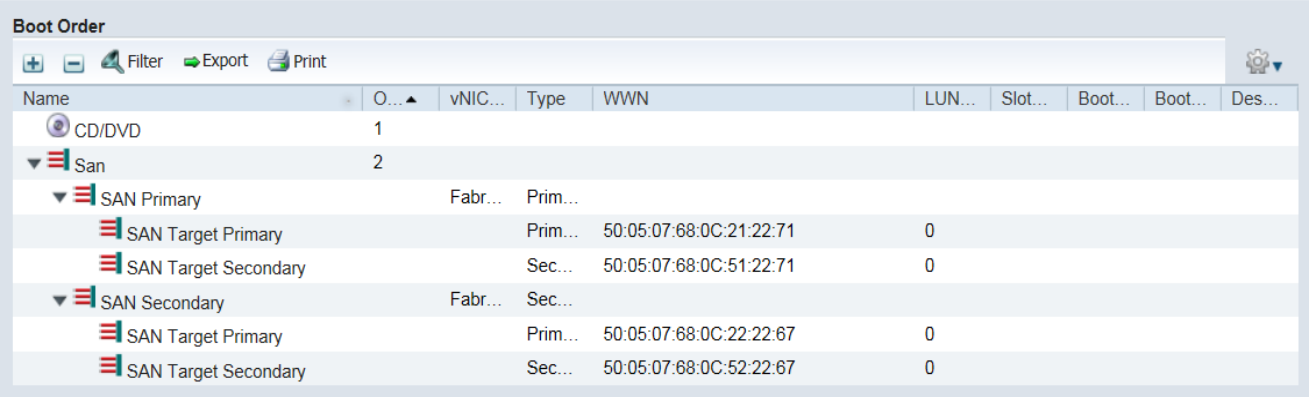
26. From the vHBA drop-down menu, choose Add SAN Boot Target.
27. Keep 0 as the value for Boot Target LUN.
28. Enter the WWPN for Controller B switch B `<<var_wwpn_FC_ContB-FE2-fabricB>>`
29. Keep Primary as the SAN boot target type.
30. Click OK to add the SAN boot target.



31. From the vHBA drop-down menu, choose Add SAN Boot Target.
32. Keep 0 as the value for Boot Target LUN.
33. Enter the WWPN for Controller B going to switch B `<<var_wwpn_FC_ContB-FE4-fabricB>>`
34. Click OK to add the SAN boot target.

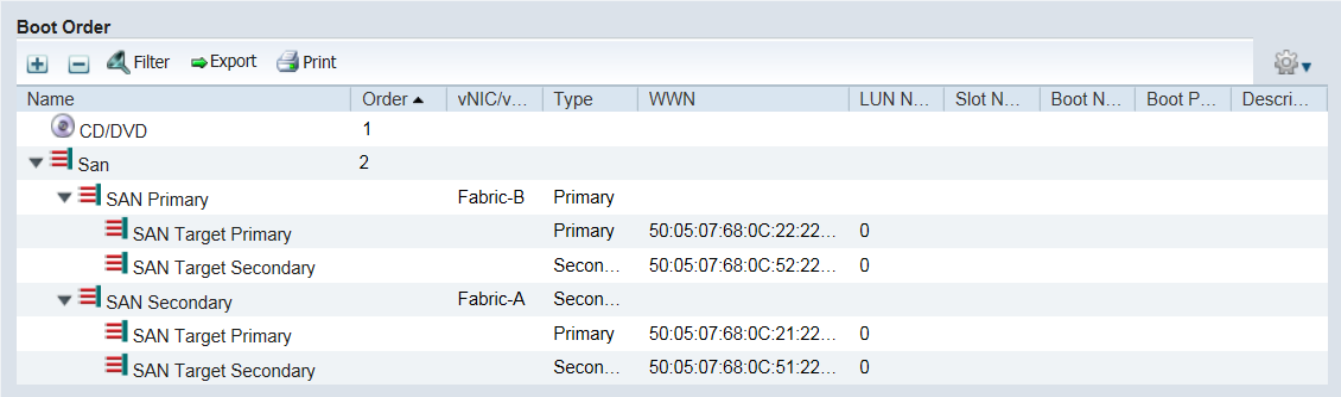


35. Click OK, and then click OK again to create the boot policy.
36. Verify that your configuration looks similar to the screenshot below:



37. Right-click Boot Policies again.
38. Choose Create Boot Policy.
39. Enter `Boot-Fabric-B` as the name of the boot policy.
40. (Optional) Enter a description of the boot policy.
41. Keep the Reboot on Boot Order Change check box unchecked.
42. From the Local Devices drop-down menu choose Add `CD/DVD`.
43. From the vHBA drop-down menu choose Add SAN Boot.
44. In the Add SAN Boot dialog box, enter `Fabric-B` in the vHBA box.
45. Make sure that the Primary radio button is selected as the SAN boot type.
46. Click OK to add the SAN boot initiator.
47. From the vHBA drop-down menu, choose Add SAN Boot Target.
48. Keep 0 as the value for Boot Target LUN.
49. Enter the WWPN for Controller B Switch-B `<< var_wwpn_FC_ContB-FE2-fabricB>>`
50. Keep Primary as the SAN boot target type.
51. Click OK to add the SAN boot target.
52. From the vHBA drop-down menu, choose Add SAN Boot Target.
53. Keep 0 as the value for Boot Target LUN.
54. Enter the WWPN for Controller B Switch-B `<< var_wwpn_FC_ContB-FE4-fabricB>>`
55. Click OK to add the SAN boot target.
56. From the vHBA menu, choose Add SAN Boot.

57. In the Add SAN Boot dialog box, enter Fabric-A in the vHBA box.
58. The SAN boot type should automatically be set to Secondary, and the Type option should be unavailable.
59. Click OK to add the SAN boot initiator.
60. From the vHBA menu, choose Add SAN Boot Target.
61. Keep 0 as the value for Boot Target LUN.
62. Enter the WWPN for Controller A Switch-A `<< var_wwpn_FC_ContA-FE1-fabricA>>`
63. Keep Primary as the SAN boot target type.
64. Click OK to add the SAN boot target.
65. From the vHBA drop-down menu, choose Add SAN Boot Target.
66. Keep 0 as the value for Boot Target LUN.
67. Enter the WWPN for Controller A Switch-A `<< var_wwpn_FC_ContA-FE3-fabricA>>`
68. Click OK to add the SAN boot target.
69. Click OK and then click OK again to create the boot policy.
70. Verify that your configuration looks similar to the screenshot below:



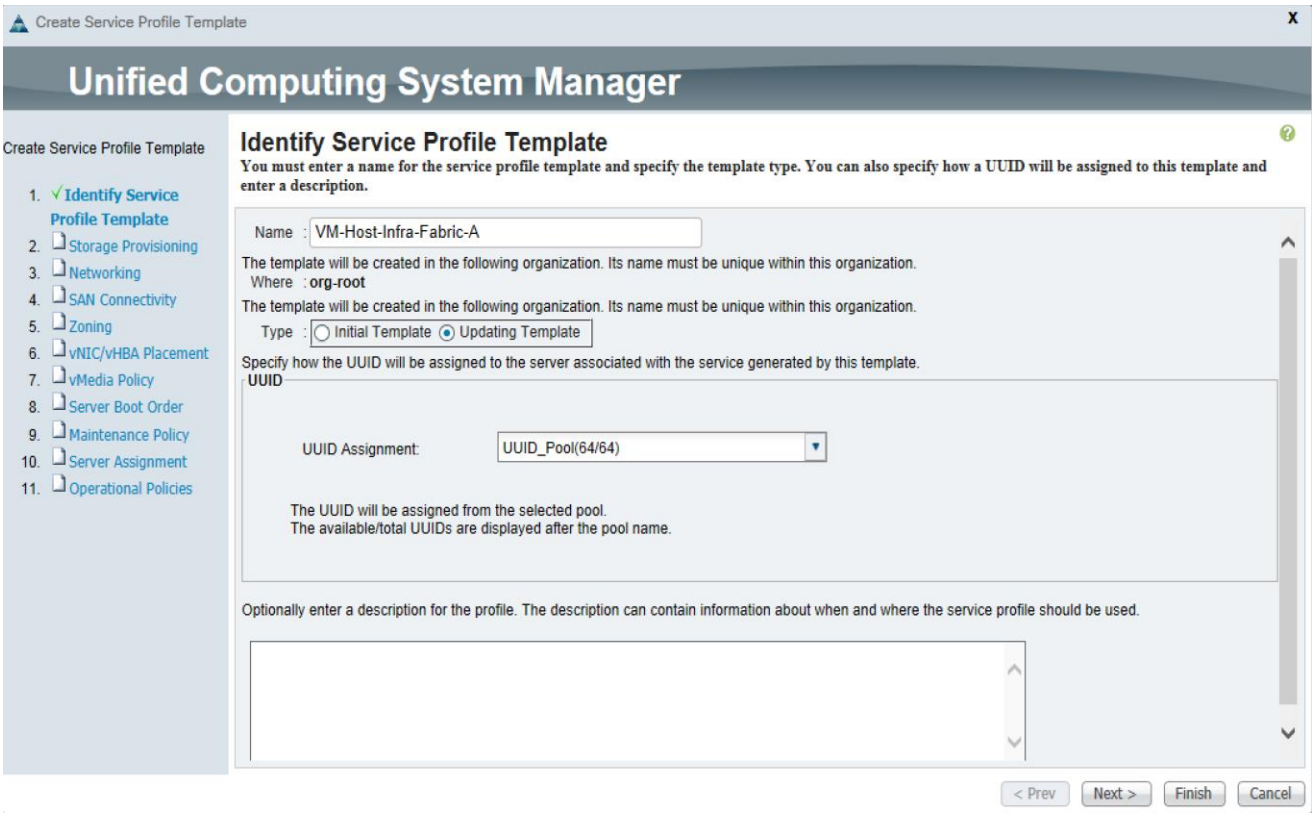
Create Service Profile Templates

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

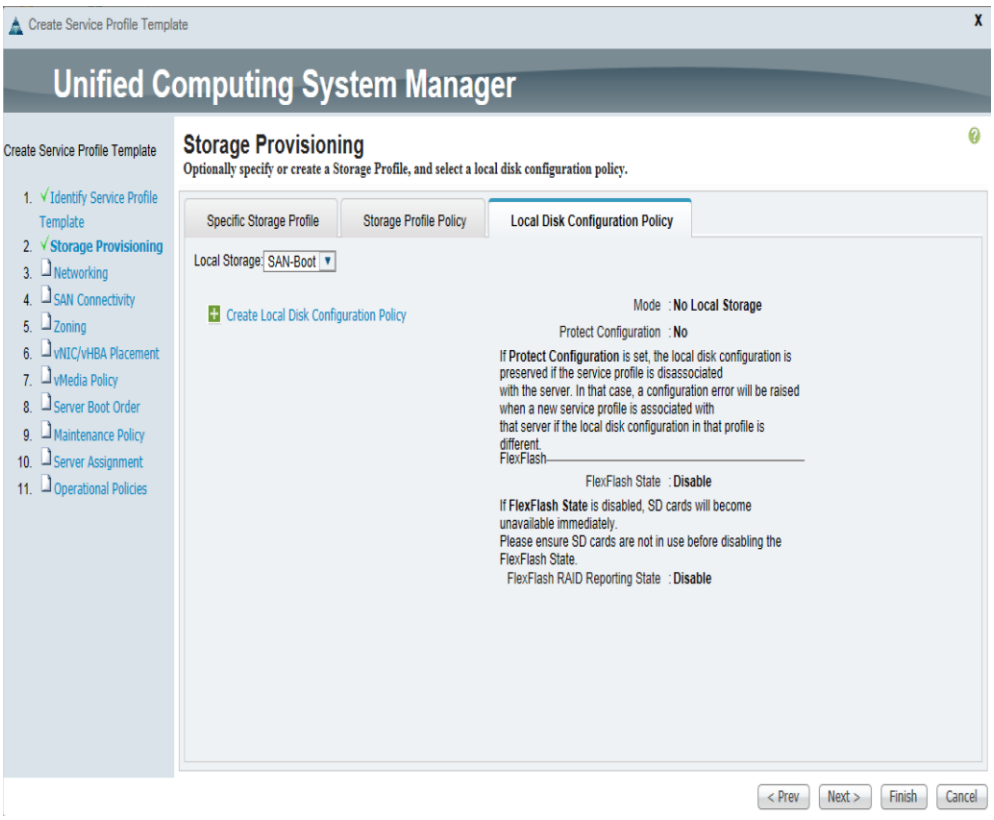
To create service profile templates, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Choose Service Profile Templates > root.
3. Right-click root.

4. Choose Create Service Profile Template to open the Create Service Profile Template wizard.
5. Identify the Service Profile Template:
   a. Enter `VM-Host-Infra-Fabric-A` as the name of the service profile template. This service profile template is configured to boot from node 1 on fabric A.
   b. Click the Updating Template radio button.
   c. Under UUID, choose `UUID_Pool` as the UUID pool.
   d. Click Next.



6. Configure the Storage Provisioning Options:
   a. Choose a local disk configuration policy:
      i. If the server in question has local disks, choose default in the Local Storage list.
      ii. If the server in question does not have local disks, choose SAN-Boot.
      iii. Leave Simple radio button selected as default.

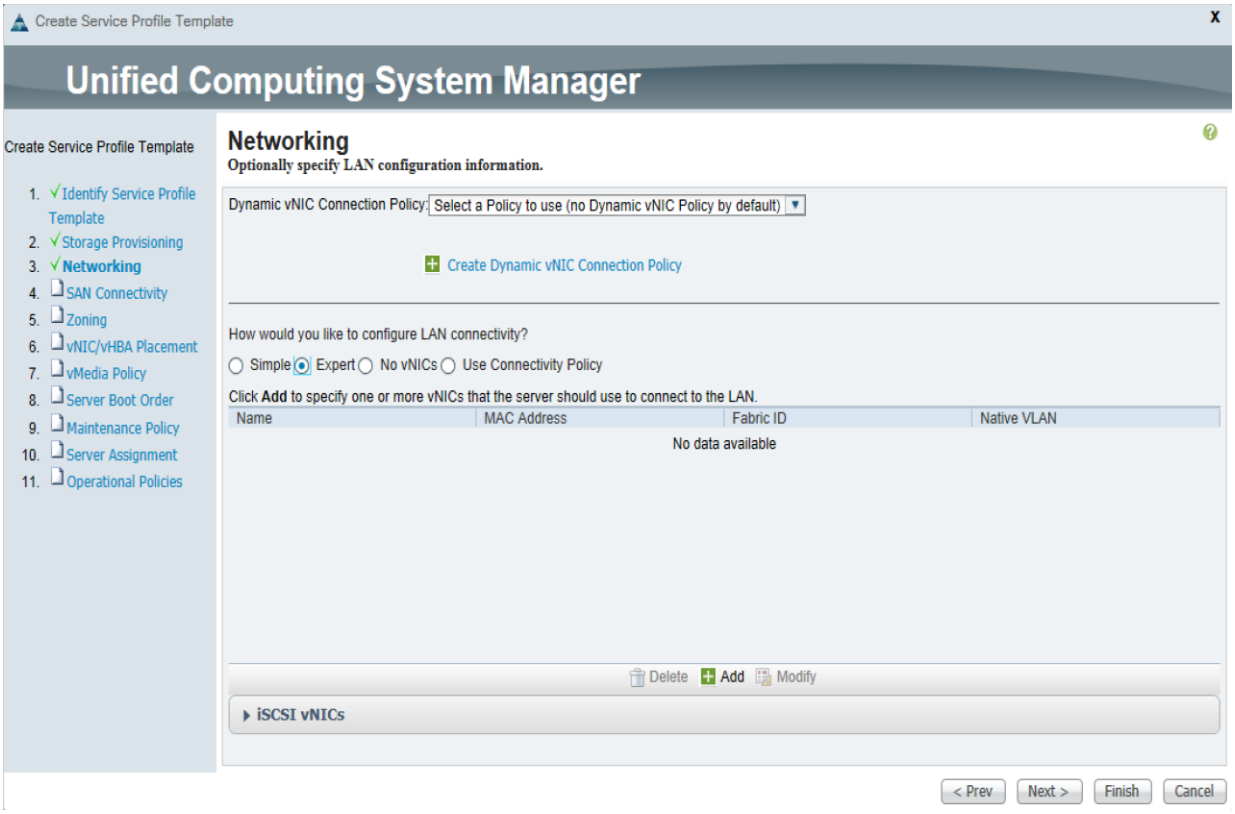


iv. Click Next.

7. Configure the Networking options:

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

   b. Click the Expert radio button to configure the LAN connectivity.



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

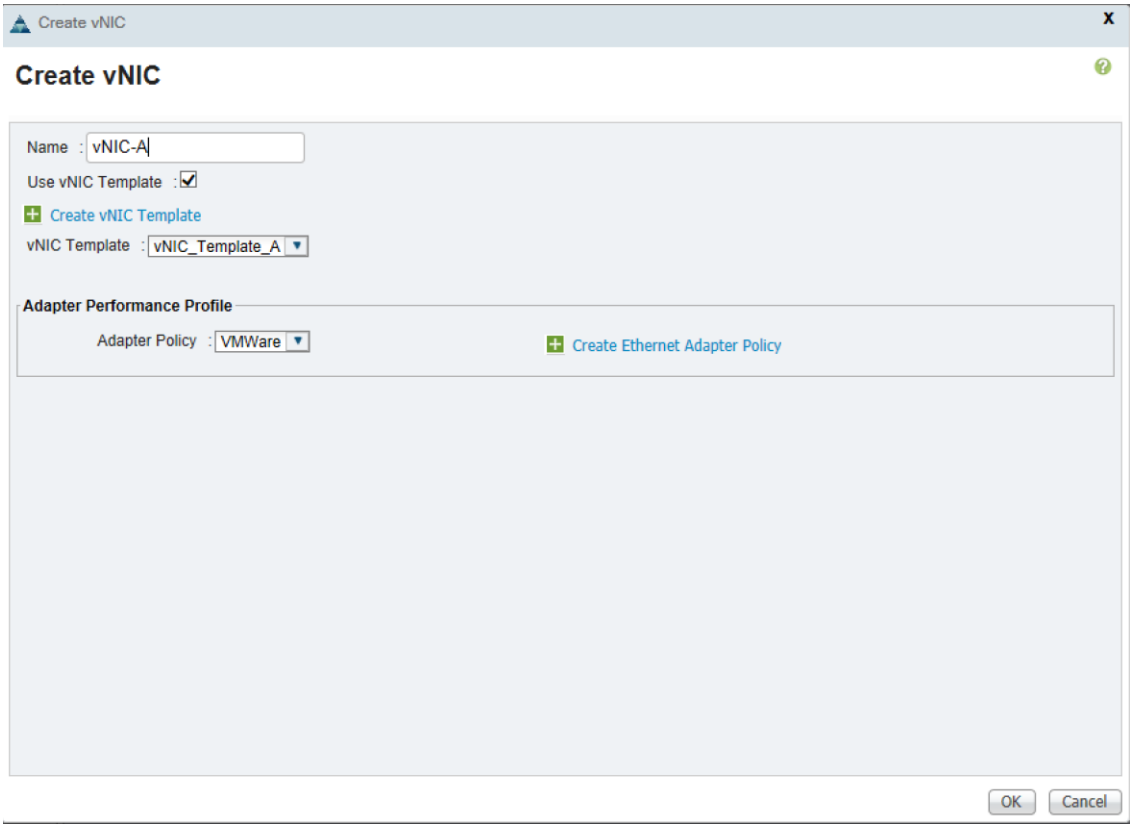
d. In the Create vNIC dialog box, enter `vNIC-A` as the name of the vNIC.

e. Check the Use vNIC Template check box.

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

g. In the Adapter Policy list, choose VMWare.

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



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

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

k. Check the Use vNIC Template check box.

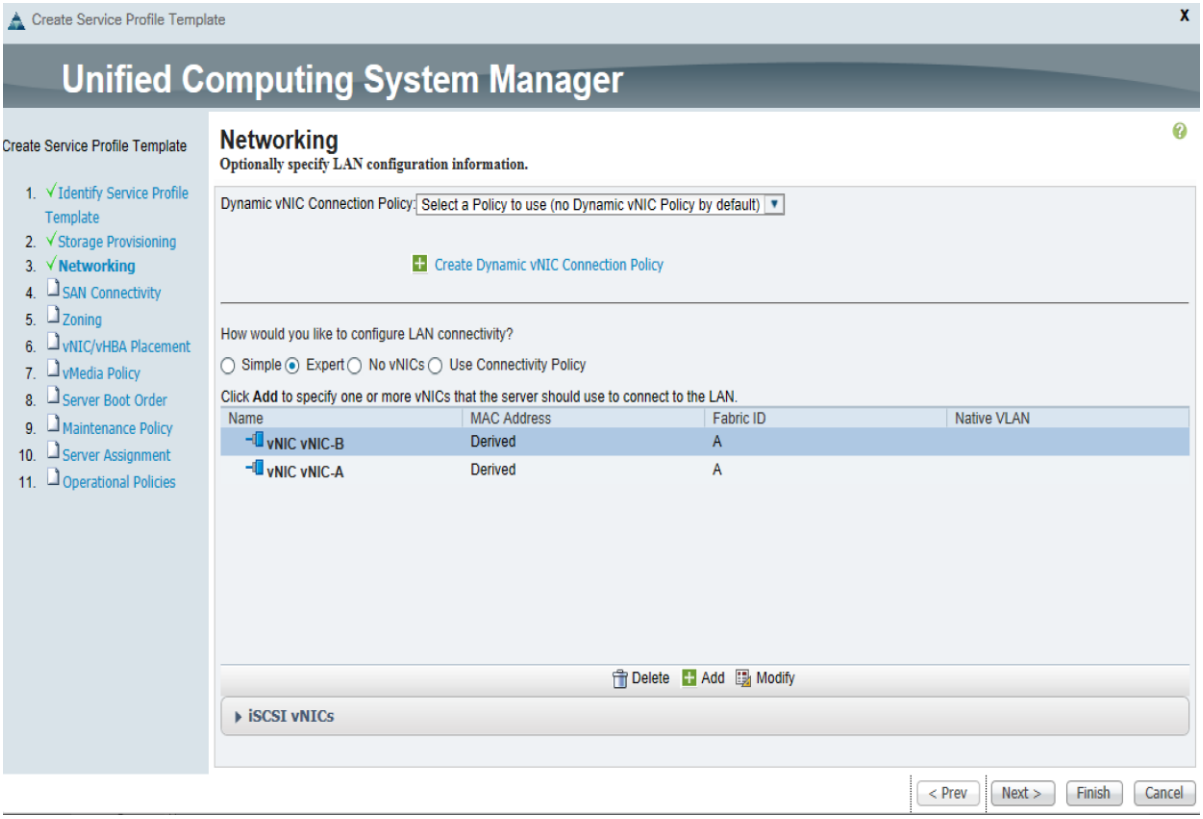
l. In the vNIC Template list, choose `vNIC_Template_B`.

m. In the Adapter Policy list, choose VMWare.

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

o. Review the table in the Networking page to make sure that both vNICs were created.

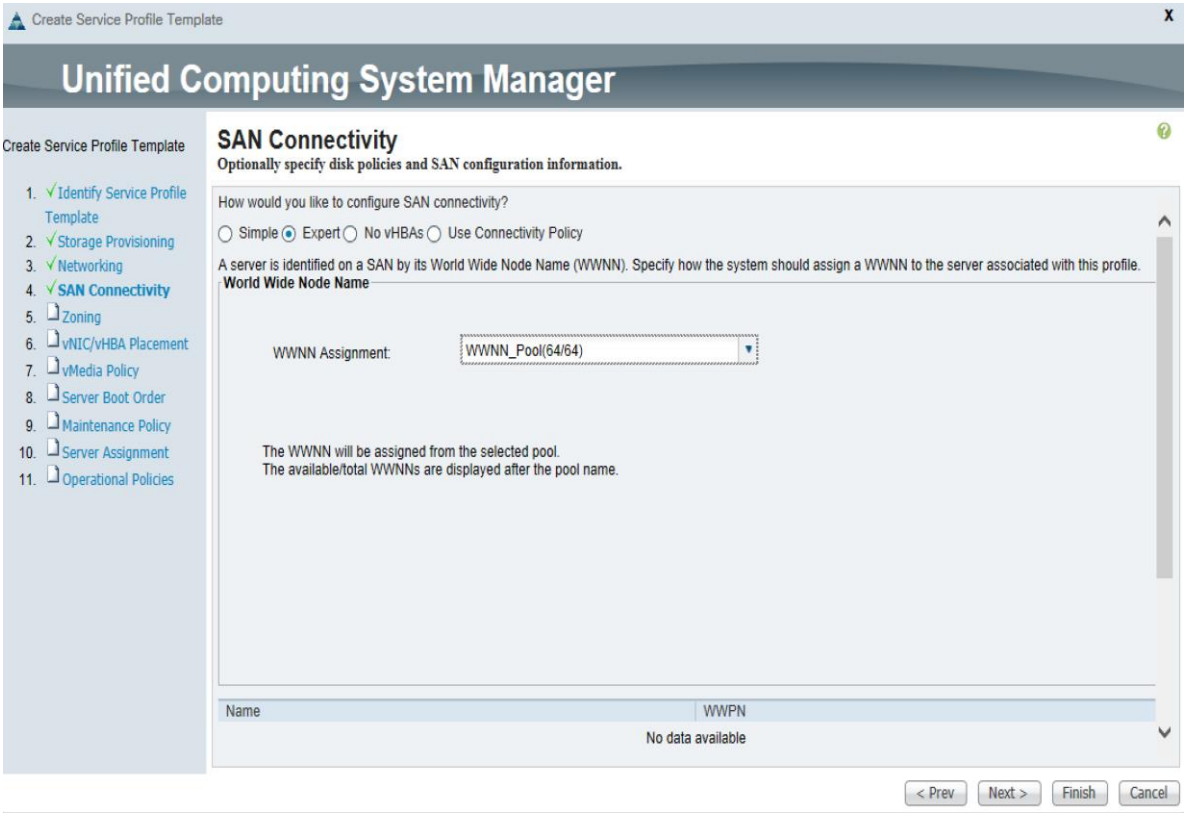
p. Click Next.



8. Configure the SAN Connectivity options:

   a. Click the Expert radio button to configure the SAN connectivity.

   b. In the WWNN Assignment list, choose `WWNN_Pool`.



c. Click Add at the bottom of the page to add a vHBA to the template.

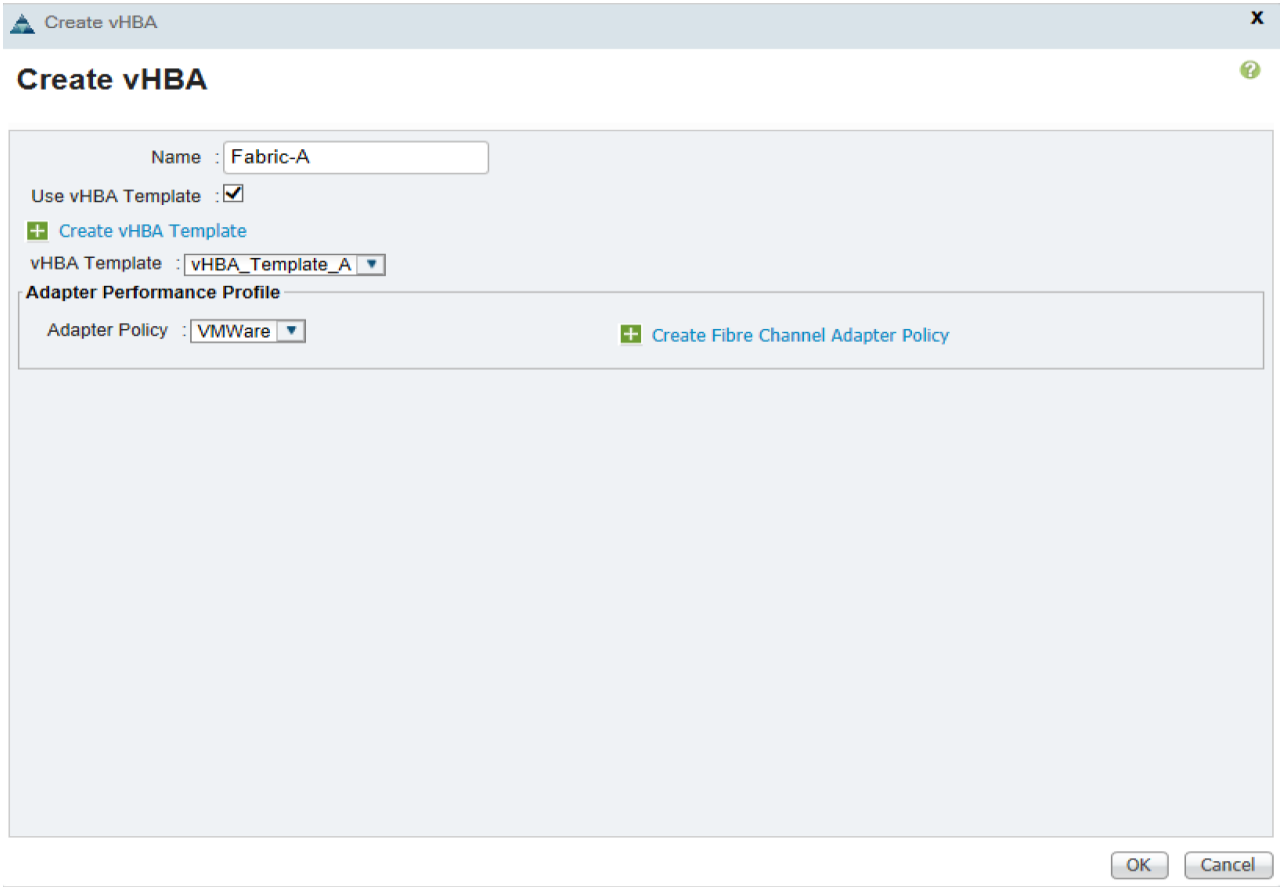
d. In the Create vHBA dialog box, enter `Fabric-A` as the name of the vHBA.

e. Check the Use vHBA Template check box.

f. In the vHBA Template list, choose `vHBA_Template_A`.

g. In the Adapter Policy list, choose VMware.

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



i. On the SAN Connectivity page of the wizard, click Add at the bottom of the page to add another vHBA to the template.

j. In the Create vHBA dialog box, enter `Fabric-B` as the name of the vHBA.

k. Check the check box for Use HBA Template.

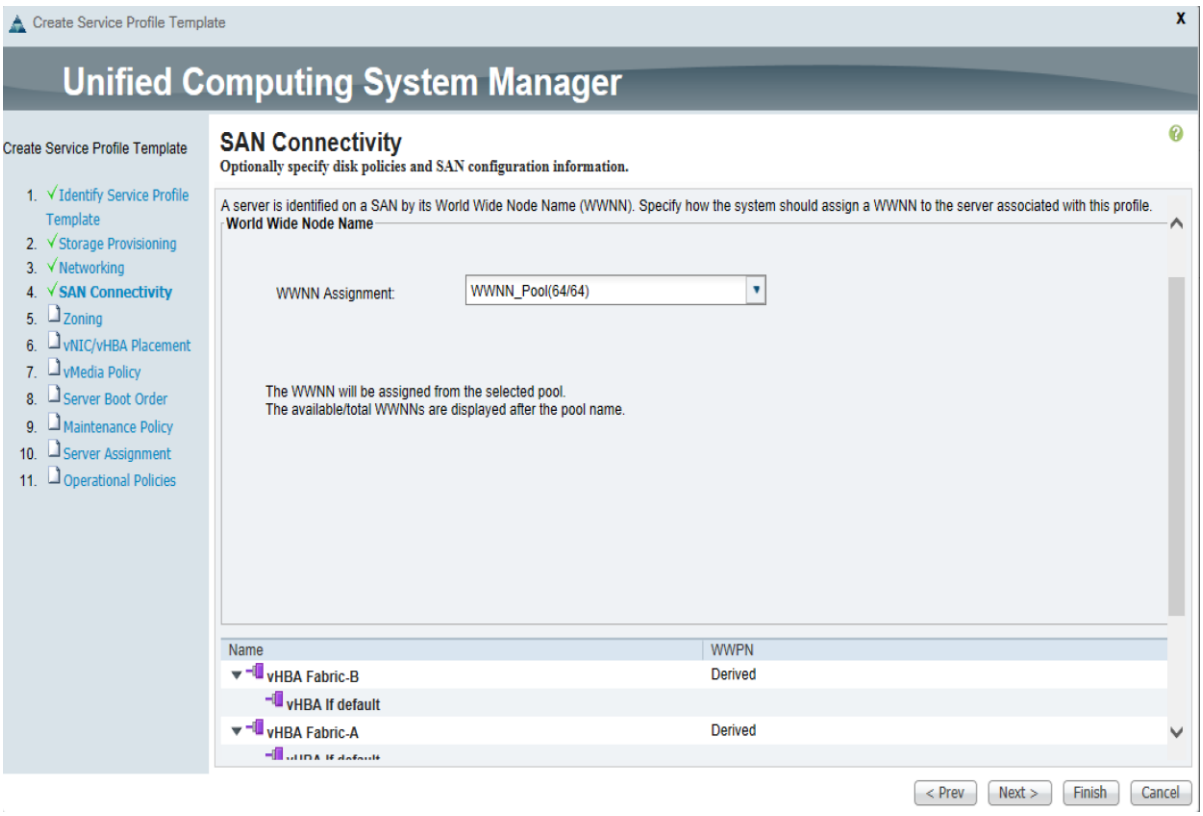
l. In the vHBA Template list, choose `vHBA_Template_B`.

m. In the Adapter Policy list, choose VMware.

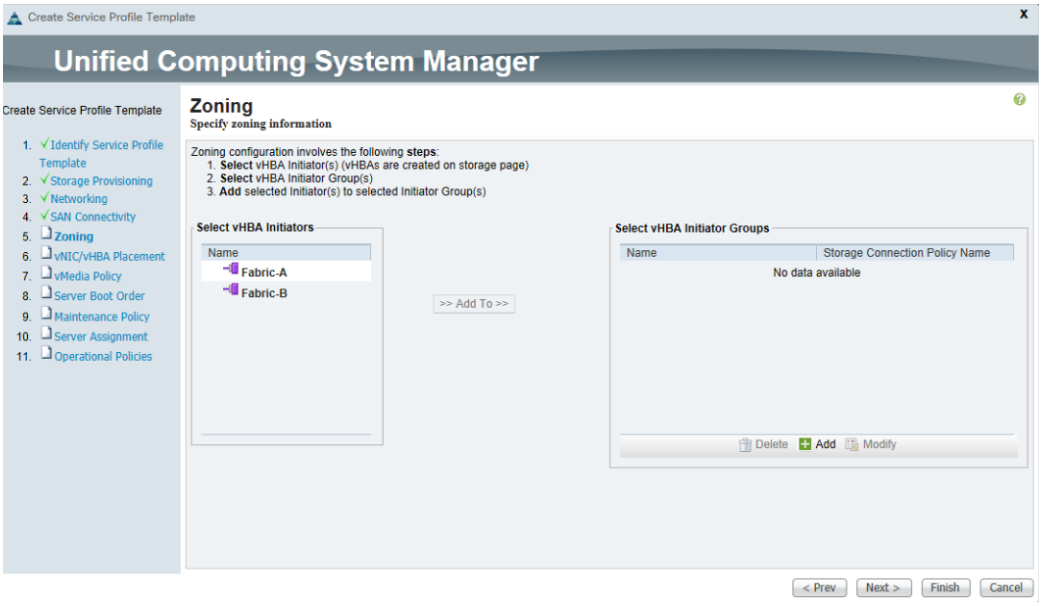
n. Click OK to add the vHBA to the template.

o. Review the table in the SAN Connectivity page to verify that both A and B vHBAs were created.

p. Click Next.



q. Set no Zoning options and click Next.



r. Set the vNIC/vHBA placement options.

s. In the Select Placement list, choose the `VM-Host-Infra` placement policy.

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

a. vHBA Fabric-A

b. vHBA Fabric-B

c. vNIC-A

d. vNIC-B

10. Review the table to verify that all vNICs and vHBAs were assigned to the policy in the appropriate order.

11. Click Next.

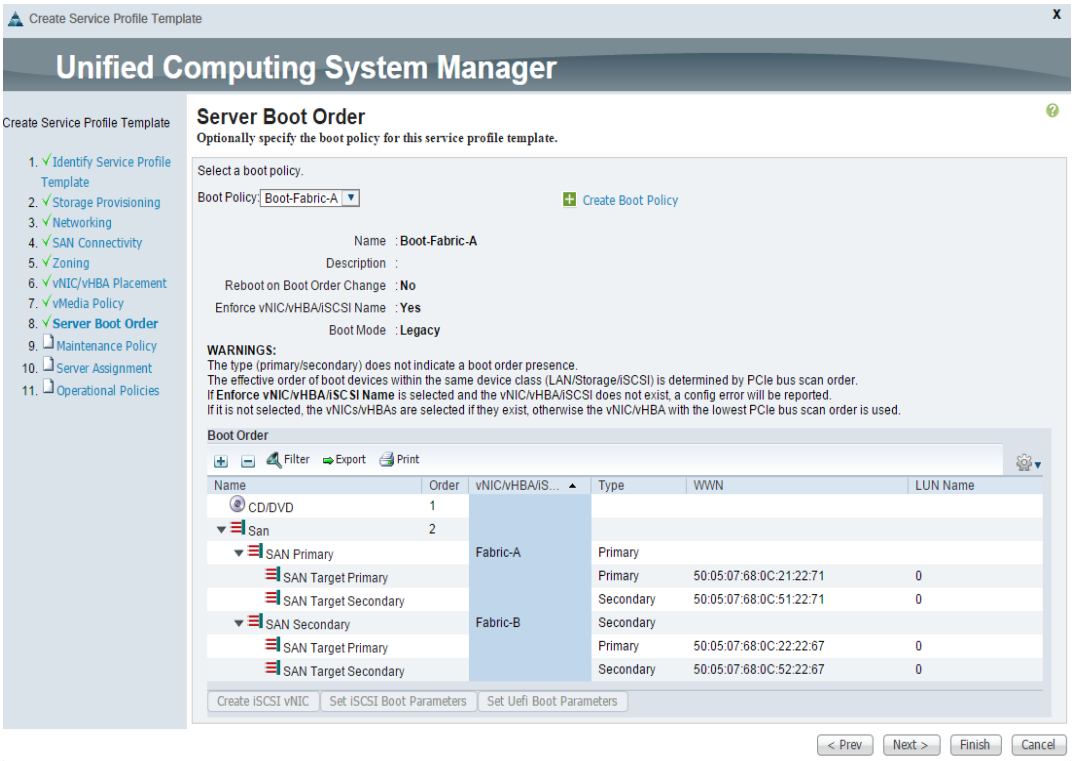
12. Click Next to bypass the vMedia policy screen.

13. Set the Server Boot Order:

    a. In the Boot Policy list, choose Boot-Fabric-A.

    b. Review the table to verify that all boot devices were created and identified. Verify that the boot devices are in the correct boot sequence.

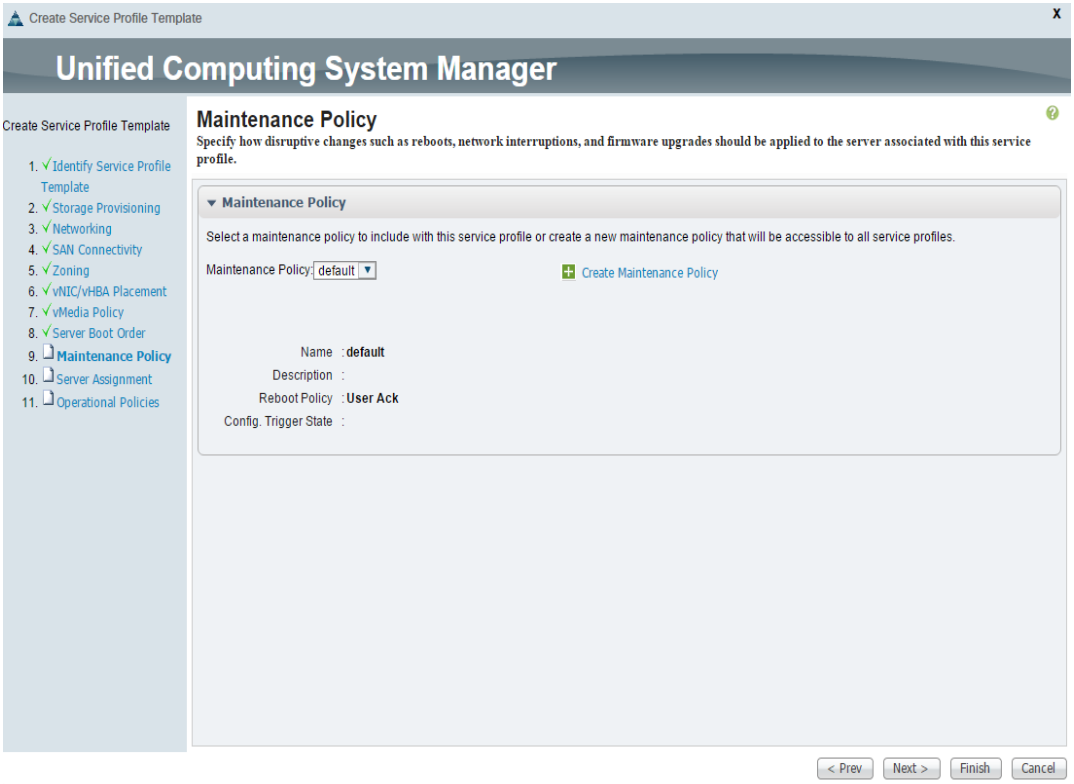
    c. Click Next.



14. Add a Maintenance Policy:

    a. Choose the Default Maintenance Policy.

    b. Click Next.



15. Specify the Server Assignment:

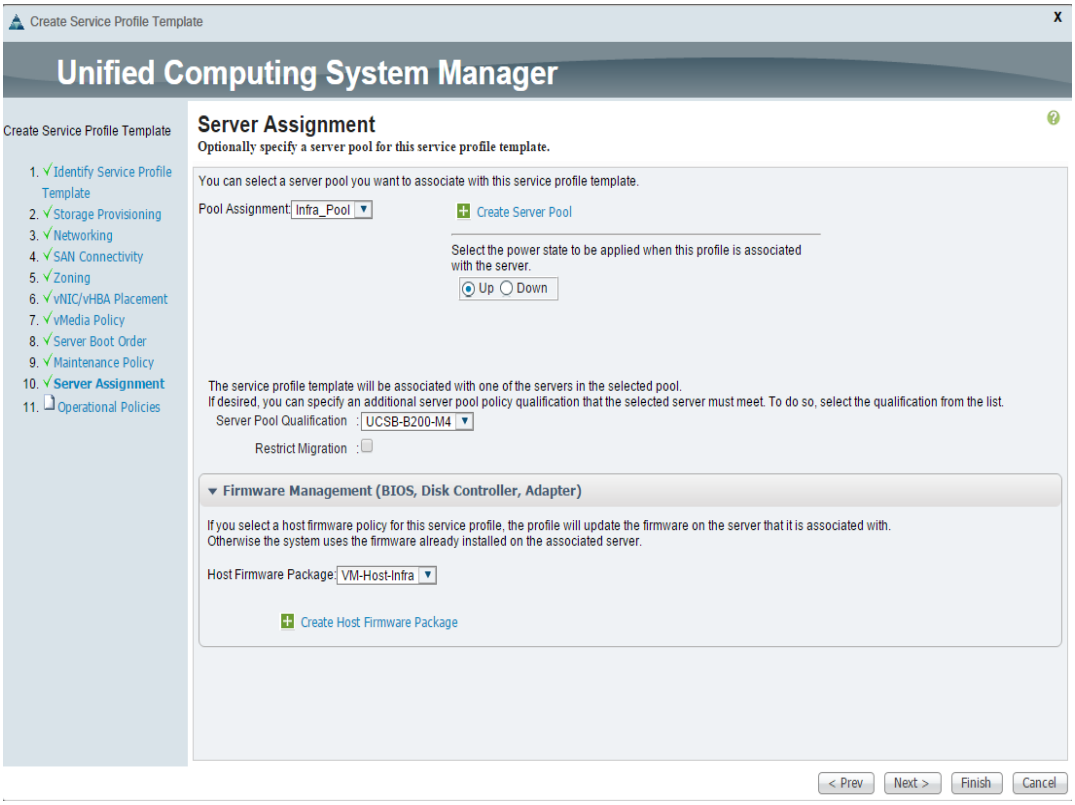
    a. In the Pool Assignment list, choose `Infra_Pool`.

    b. (Optional) Choose a Server Pool Qualification policy.

    c. Choose Up as the power state to be applied when the profile is associated with the server.

    d. Expand Firmware Management at the bottom of the page and choose `VM-Host-Infra` from the Host. Firmware list.

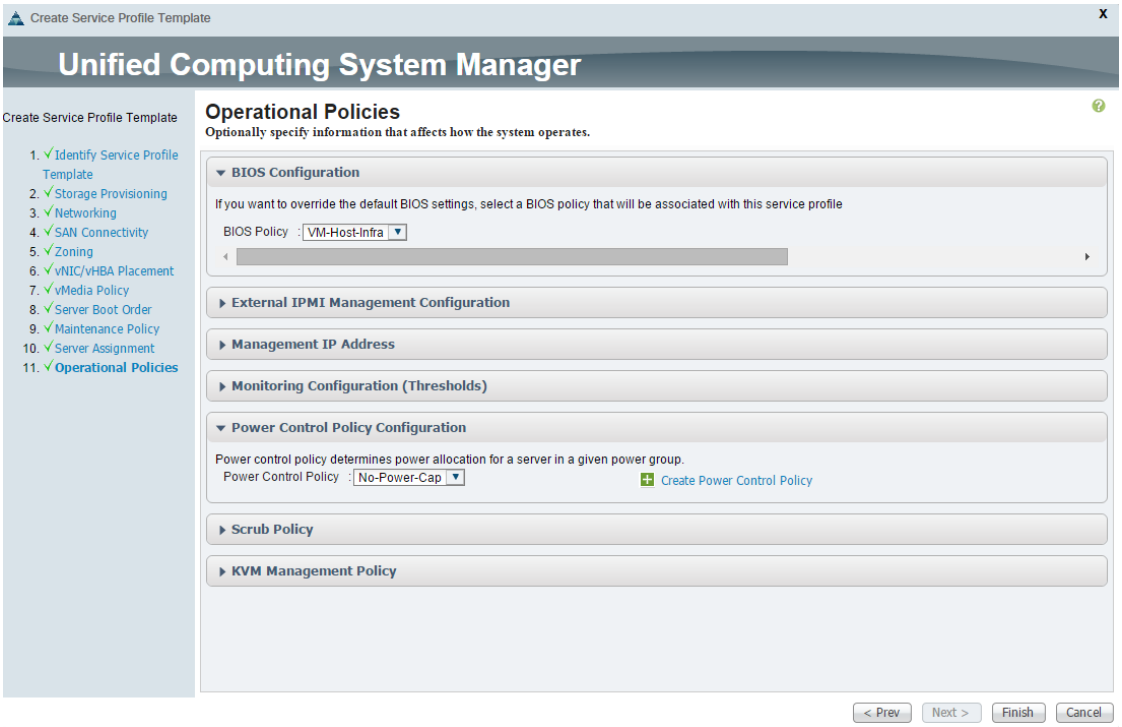
    e. Click Next.



16. Add Operational Policies:

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

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



c. Click Finish to create the service profile template.

d. Click OK in the confirmation message.

e. Click the Servers tab in the navigation pane.

f. Choose Service Profile Templates > root.

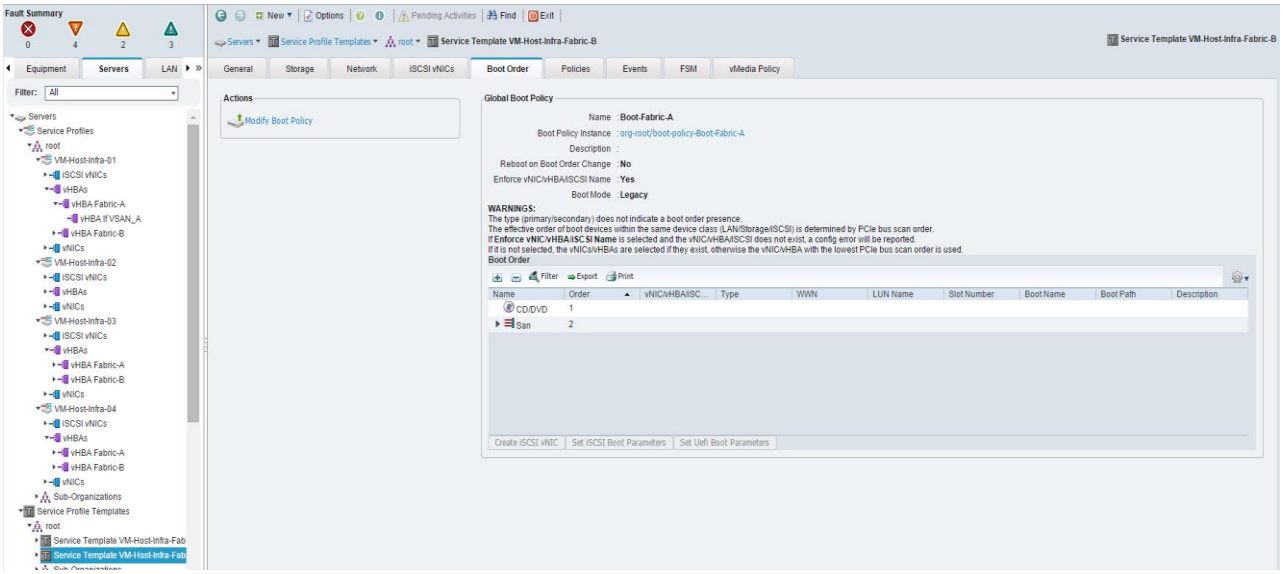
g. Right-click the previously created `VM-Host-Infra-Fabric-A` template.

h. Choose Create a Clone.

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

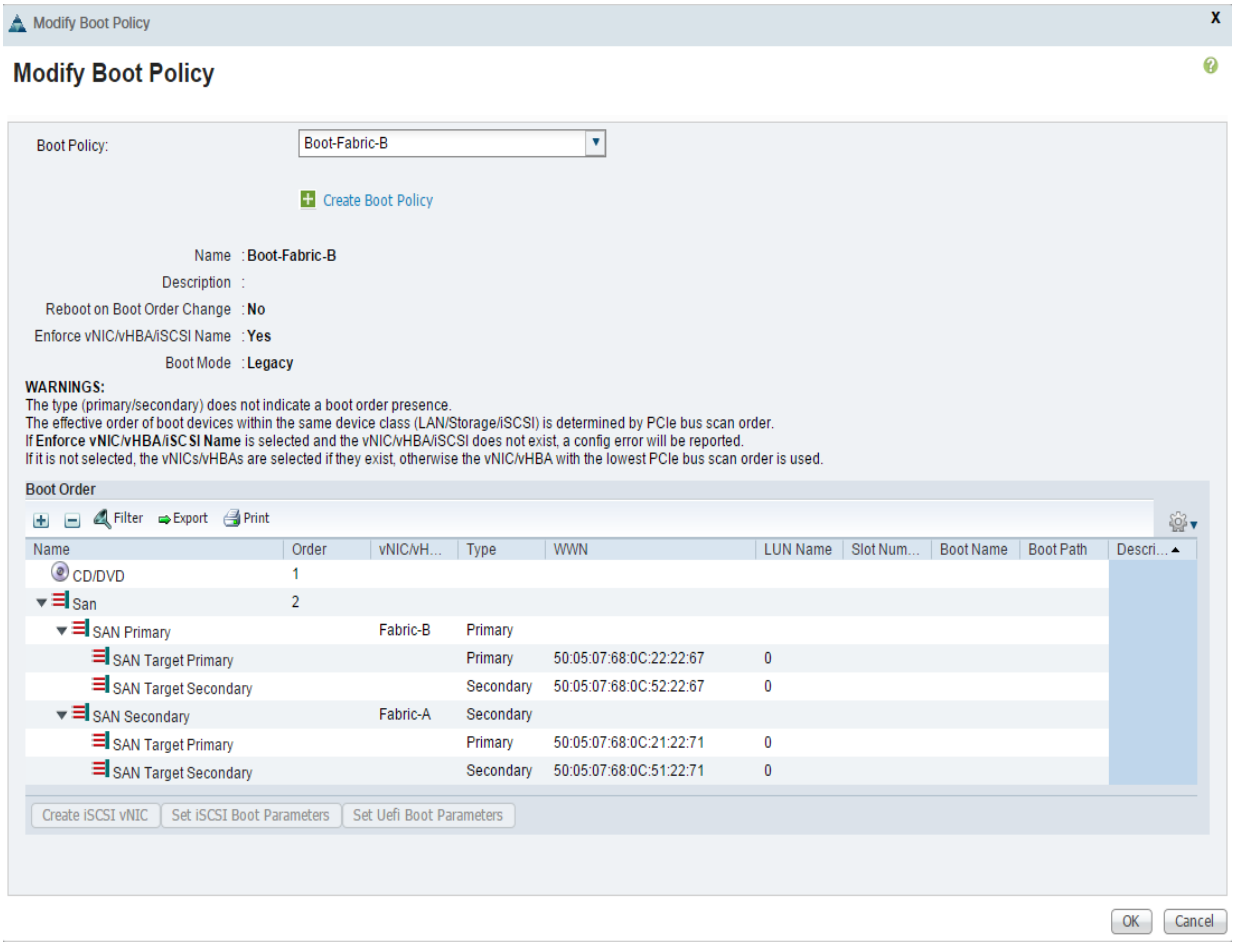
j. Click OK.

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



l. Click Modify Boot Policy.

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

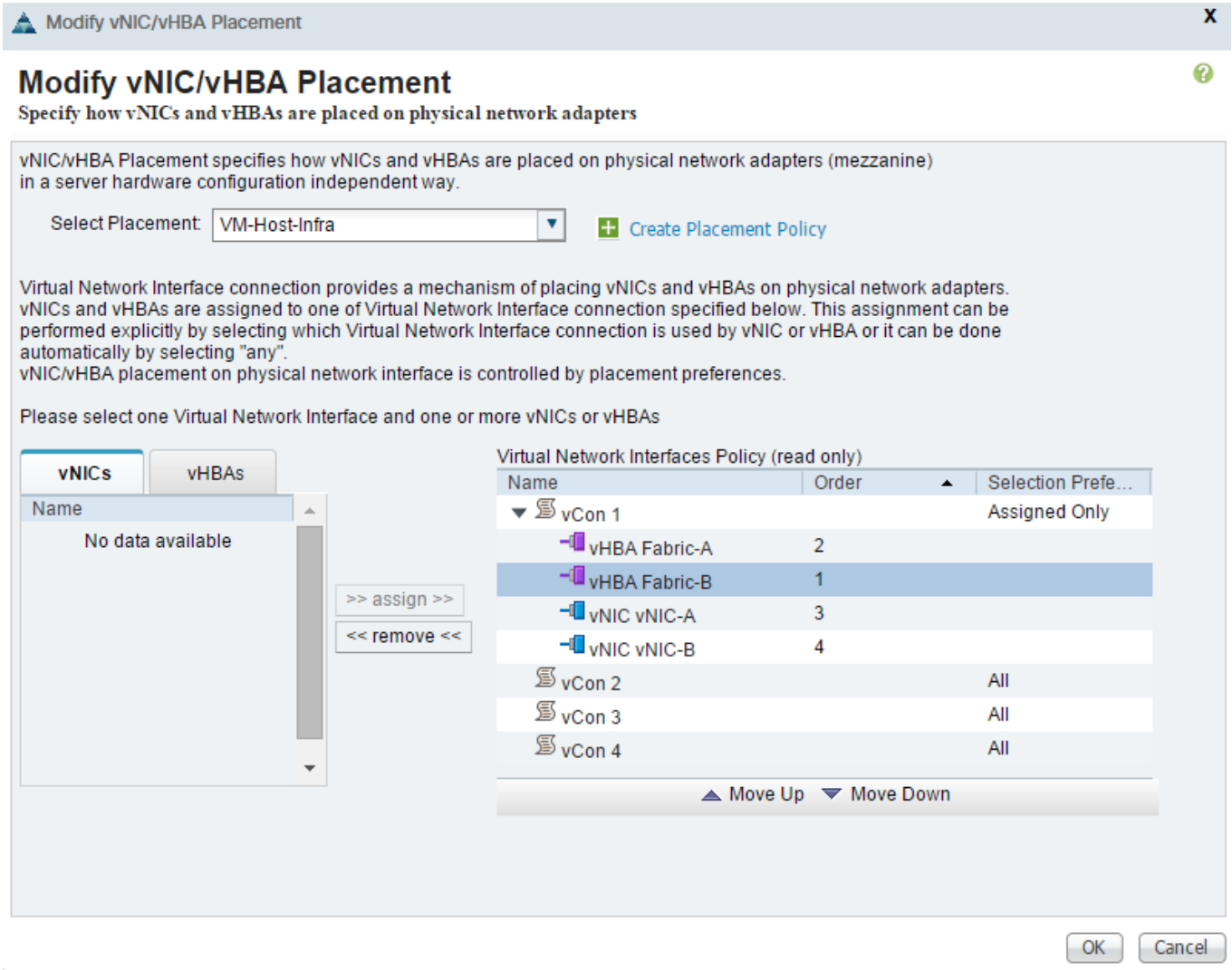


n. Click OK and then click OK again.

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

p. Select VM-Host-Infra and Expand `vCon 1` and move `vHBA Fabric-B` ahead of `vHBA Fabric-A` in the placement order.

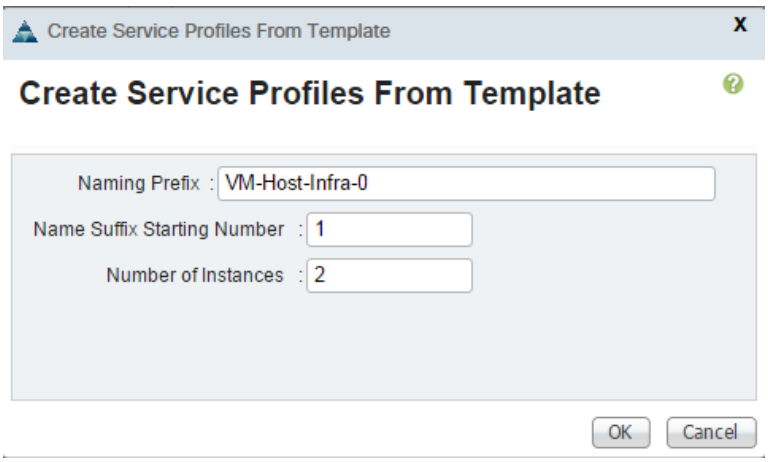
q. Click OK and then click OK again.



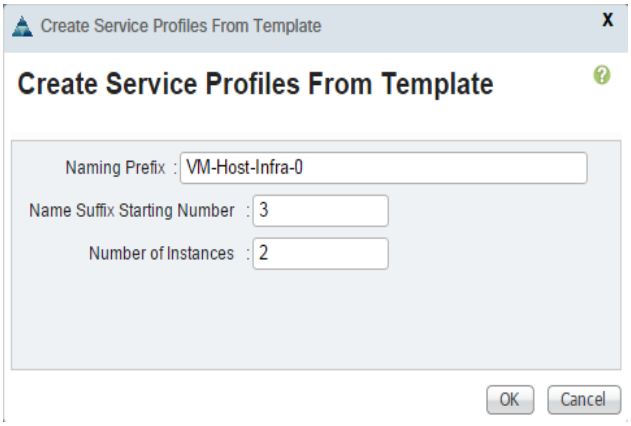
Create Service Profiles

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. Choose Service Profile Templates > root > Service Template `VM-Host-Infra-Fabric-A`.
3. Right-click `VM-Host-Infra-Fabric-A` and choose Create Service Profiles from Template.
4. Enter `VM-Host-Infra-0` as the service profile prefix.
5. Enter 1 as the Name Suffix Staring Number.
6. Enter 2 as the Number of Instances.
7. Click OK to create the service profile.



8. Click OK in the confirmation message.
9. Choose Service Profile Templates > root > Service Template `VM-Host-Infra-Fabric-B`.
10. Right-click `VM-Host-Infra-Fabric-B` and choose Create Service Profiles from Template.
11. Enter `VM-Host-Infra-0` as the service profile prefix.
12. Enter 3 as the Name Suffix Staring Number.
13. Enter 2 as the Number of Instances
14. Click OK to create the service profile.



15. Click OK in the confirmation message.
16. Verify that the service profiles `VM-Host-Infra-01, VM-Host-Infra-02, VM-Host-Infra-03` and `VM-Host-Infra-04` have been created. The service profiles are automatically associated with the servers in their assigned server pools.
17. (Optional) Choose each newly created service profile and enter the server host name or the FQDN in the User Label field in the General tab. Click Save Changes to map the server host name to the service profile name.

Backup the Cisco UCS Manager Configuration

It is recommended 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/ucs-manager/GUI-User-Guides/Admin-Management/3-1/b_Cisco_UCS_Admin_Mgmt_Guide_3_1/b_Cisco_UCS_Admin_Mgmt_Guide_3_1_chapter_01001.html

Adding Servers

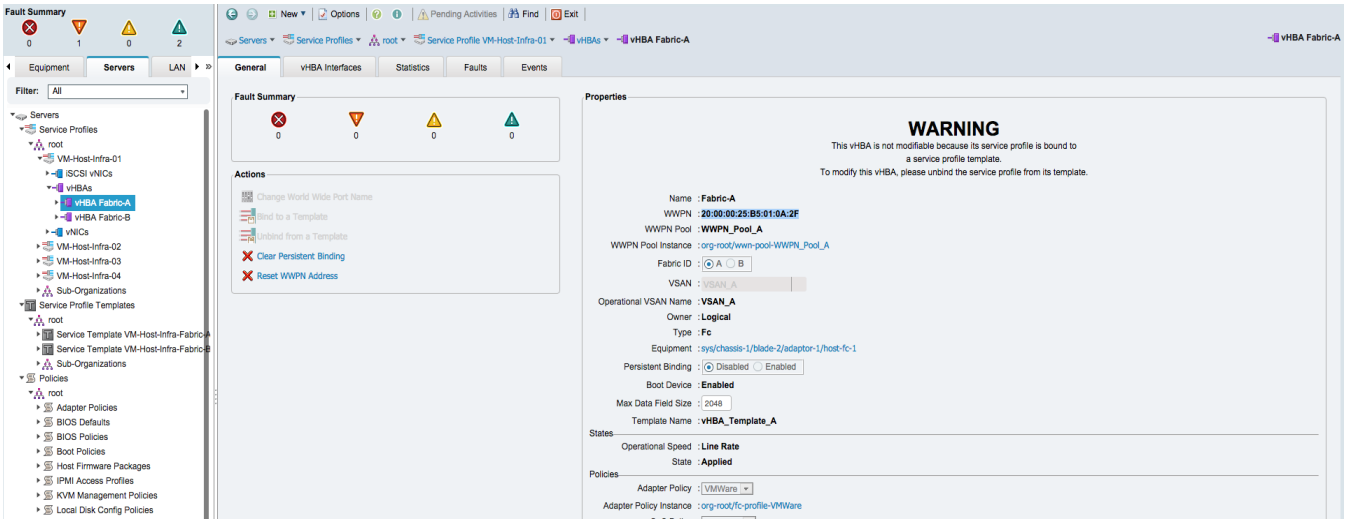
Additional server pools, service profile templates, and service profiles can be created in the respective organizations to add more servers to the Pod unit. All other pools and policies are at the root level and can be shared among the organizations.

Gather Necessary WWPN 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 SAN-BOOT deployment, specific information must be gathered from each Cisco UCS blade and from the IBM controllers. Complete the following steps:

1. To gather the vHBA WWPN information, launch the Cisco UCS Manager GUI. In the navigation pane, click the Servers tab. Expand Servers > Service Profiles > root. Select each of the service profiles and expand to see the vHBAs.

2. Click vHBA Fabric-A, in the General tab highlight and right-click the WWPN and click Copy.



3. Record the WWPN information that is displayed for both the Fabric A vHBA and the Fabric B vHBA for each service profile into the WWPN variable in Table 23 .

Table 23 WWPN Variables

VM-Host-Infra-01-A	Switch A	var_wwpn_VM-Host-Infra-01-A	20:00:00:25:b5:01:0a:2f
VM-Host-Infra-01-B	Switch B	var_wwpn_VM-Host-Infra-01-B	20:00:00:25:b5:01:0b:2f

VM-Host-Infra-02-A	Switch A	var_wwpn_VM-Host-Infra-02-A	20:00:00:25:b5:01:0a:3f
VM-Host-Infra-02-B	Switch B	var_wwpn_VM-Host-Infra-02-B	20:00:00:25:b5:01:0b:3f
VM-Host-Infra-03-A	Switch A	var_wwpn_VM-Host-Infra-03-A	20:00:00:25:b5:01:0a:0f
VM-Host-Infra-03-B	Switch B	var_wwpn_VM-Host-Infra-03-B	20:00:00:25:b5:01:0b:0f
VM-Host-Infra-04-A	Switch A	var_wwpn_VM-Host-Infra-04-A	20:00:00:25:b5:01:0a:1f
VM-Host-Infra-04-B	Switch B	var_wwpn_VM-Host-Infra-04-B	20:00:00:25:b5:01:0b:1f

Cisco MDS 9148S Compute SAN Zoning

The steps below are for configuring zoning for the WWPN's from the server and the FlashSystem V9000. We are using the WWPN information collected in the previous steps. There are 4 zones created for servers in VSAN 101 on Switch A and 4 zones created in VSAN 102 on Switch B. Host zones and the cluster zone belongs to separate VSAN fabrics.

Cisco MDS - A Switch

1. Log in to the Cisco MDS switch and complete the following steps to create the WWPN aliases:

```
config

Enter configuration commands, one per line.  End with CNTL/Z.

device-alias database
device-alias name VM-Host-Infra-01-A pwwn var_wwpn_VM-Host-Infra-01-A
device-alias name VM-Host-Infra-02-A pwwn var_wwpn_VM-Host-Infra-02-A
device-alias name VM-Host-Infra-03-A pwwn var_wwpn_VM-Host-Infra-03-A
device-alias name VM-Host-Infra-04-A pwwn var_wwpn_VM-Host-Infra-04-A
device-alias commit
```

2. Create the zones and add device-alias members for the 4 blades.

```
zone name  VM-Host-Infra-01-A vsan 101
member device-alias  VM-Host-Infra-01-A
member device-alias VersaStack-ContA-FE1
member device-alias VersaStack-ContA-FE3
member device-alias VersaStack-ContB-FE1
member device-alias VersaStack-ContB-FE3


zone name  VM-Host-Infra-02-A vsan 101
member device-alias  VM-Host-Infra-02-A
member device-alias VersaStack-ContA-FE1
member device-alias VersaStack-ContA-FE3
```

```
member device-alias VersaStack-ContB-FE1
member device-alias VersaStack-ContB-FE3


zone name  VM-Host-Infra-03-A vsan 101
member device-alias  VM-Host-Infra-032-A
member device-alias VersaStack-ContA-FE1
member device-alias VersaStack-ContA-FE3
member device-alias VersaStack-ContB-FE1
member device-alias VersaStack-ContB-FE3


zone name  VM-Host-Infra-04-A vsan 101
member device-alias  VM-Host-Infra-042-A
member device-alias VersaStack-ContA-FE1
member device-alias VersaStack-ContA-FE3
member device-alias VersaStack-ContB-FE1
member device-alias VersaStack-ContB-FE3
exit
```

3. Add zones to zoneset.

```
zoneset name versastackzoneset vsan 101
member VM-Host-Infra-01-A
member VM-Host-Infra-02-A
member VM-Host-Infra-03-A
member VM-Host-Infra-04-A
exit
```

4. Activate the zoneset.

```
zoneset activate  name versastackzoneset vsan 101
```

Validate all the HBA's are logged into the Cisco MDS switch. The V9000 and the Cisco servers should be powered on. To start the Cisco server's from Cisco UCS Manager, select the server tab, then click Servers→Service→Profiles→root, and then right click service profile, For example, `VM-Host-Infra-01` then select boot server.

5. Validate all powered on systems HBA's are logged into the switch through the show zoneset command.

```
sh zoneset active
```

```
VersaStack-MDS-A# sh zoneset active vsan 101
zoneset name versastackzoneset vsan 101
  zone name VM-Host-Infra-01-A vsan 101
  * fcid 0x670003 [pwwn 20:00:00:25:b5:01:0a:2f] [VM-Host-Infra-01-A]
  * fcid 0x670200 [pwwn 50:05:07:68:0c:21:22:71] [VersaStack-ContA-FE1]
  * fcid 0x670400 [pwwn 50:05:07:68:0c:51:22:71] [VersaStack-ContA-FE3]
  * fcid 0x670100 [pwwn 50:05:07:68:0c:21:22:67] [VersaStack-ContB-FE1]
  * fcid 0x670300 [pwwn 50:05:07:68:0c:51:22:67] [VersaStack-ContB-FE3]

  zone name VM-Host-Infra-02-A vsan 101
  * fcid 0x670004 [pwwn 20:00:00:25:b5:01:0a:3f] [VM-Host-Infra-02-A]
  * fcid 0x670200 [pwwn 50:05:07:68:0c:21:22:71] [VersaStack-ContA-FE1]
  * fcid 0x670400 [pwwn 50:05:07:68:0c:51:22:71] [VersaStack-ContA-FE3]
  * fcid 0x670100 [pwwn 50:05:07:68:0c:21:22:67] [VersaStack-ContB-FE1]
  * fcid 0x670300 [pwwn 50:05:07:68:0c:51:22:67] [VersaStack-ContB-FE3]

  zone name VM-Host-Infra-03-A vsan 101
  * fcid 0x670200 [pwwn 50:05:07:68:0c:21:22:71] [VersaStack-ContA-FE1]
  * fcid 0x670400 [pwwn 50:05:07:68:0c:51:22:71] [VersaStack-ContA-FE3]
  * fcid 0x670100 [pwwn 50:05:07:68:0c:21:22:67] [VersaStack-ContB-FE1]
  * fcid 0x670300 [pwwn 50:05:07:68:0c:51:22:67] [VersaStack-ContB-FE3]
  * fcid 0x670001 [pwwn 20:00:00:25:b5:01:0a:0f] [VM-Host-Infra-03-A]

  zone name VM-Host-Infra-04-A vsan 101
  * fcid 0x670200 [pwwn 50:05:07:68:0c:21:22:71] [VersaStack-ContA-FE1]
  * fcid 0x670400 [pwwn 50:05:07:68:0c:51:22:71] [VersaStack-ContA-FE3]
  * fcid 0x670100 [pwwn 50:05:07:68:0c:21:22:67] [VersaStack-ContB-FE1]
  * fcid 0x670300 [pwwn 50:05:07:68:0c:51:22:67] [VersaStack-ContB-FE3]
  * fcid 0x670002 [pwwn 20:00:00:25:b5:01:0a:1f] [VM-Host-Infra-04-A]
```

6. Save the configuration.

```
copy run start
```

Cisco MDS - B Switch

1. Log in to the Cisco MDS switch and complete the following steps to create the WWPN aliases:

```
config

Enter configuration commands, one per line.  End with CNTL/Z.

device-alias database
device-alias name VM-Host-Infra-01-B pwwn var_wwpn_VM-Host-Infra-01-B
device-alias name VM-Host-Infra-02-B pwwn var_wwpn_VM-Host-Infra-02-B
device-alias name VM-Host-Infra-03-B pwwn var_wwpn_VM-Host-Infra-03-B
device-alias name VM-Host-Infra-04-B pwwn var_wwpn_VM-Host-Infra-04-B
device-alias commit
```

2. Create the zones and add device-alias members for the 4 servers.

```
zone name  VM-Host-Infra-01-B vsan 102
member device-alias  VM-Host-Infra-01-B
member device-alias VersaStack-ContA-FE2
member device-alias VersaStack-ContA-FE4
member device-alias VersaStack-ContB-FE2
member device-alias VersaStack-ContB-FE4
exit
```

```
zone name  VM-Host-Infra-02-B vsan 102
member device-alias  VM-Host-Infra-02-B
member device-alias VersaStack-ContA-FE2
member device-alias VersaStack-ContA-FE4
member device-alias VersaStack-ContB-FE2
member device-alias VersaStack-ContB-FE4
exit

zone name  VM-Host-Infra-03-B vsan 102
member device-alias  VM-Host-Infra-03-B
member device-alias VersaStack-ContA-FE2
member device-alias VersaStack-ContA-FE4
member device-alias VersaStack-ContB-FE2
member device-alias VersaStack-ContB-FE4
exit

zone name  VM-Host-Infra-04-B vsan 102
member device-alias  VM-Host-Infra-04-B
member device-alias VersaStack-ContA-FE2
member device-alias VersaStack-ContA-FE4
member device-alias VersaStack-ContB-FE2
member device-alias VersaStack-ContB-FE4
exit
```

3. Add zones to zoneset.

```
zoneset name versastackzoneset vsan 102
member VM-Host-Infra-01-B
member VM-Host-Infra-02-B
member VM-Host-Infra-03-B
member VM-Host-Infra-04-B
```

4. Activate the zoneset.

```
zoneset activate  name versastackzoneset vsan 102
```

Validate all the HBA's are logged into the Cisco MDS switch. The V9000 and the Cisco servers should be powered on. To start the Cisco server's from Cisco UCS Manager, select the server tab, then click Servers→Service→Profiles→root, and right click service profile, For example, `VM-Host-Infra-01` then select boot server.

5. Validate the all powered on systems HBA's are logged into the switch.

```
sh zoneset active
```

```
VersaStack-MDS-B# sh zoneset active vsan 102
zoneset name versastackzoneset vsan 102
  zone name VM-Host-Infra-01-B vsan 102
  * fcid 0xa50203 [pwwn 20:00:00:25:b5:01:0b:2f] [VM-Host-Infra-01-B]
  * fcid 0xa50000 [pwwn 50:05:07:68:0c:22:22:71] [VersaStack-ContA-FE2]
  * fcid 0xa50400 [pwwn 50:05:07:68:0c:52:22:71] [VersaStack-ContA-FE4]
  * fcid 0xa50100 [pwwn 50:05:07:68:0c:22:22:67] [VersaStack-ContB-FE2]
  * fcid 0xa50300 [pwwn 50:05:07:68:0c:52:22:67] [VersaStack-ContB-FE4]

  zone name VM-Host-Infra-02-B vsan 102
  * fcid 0xa50204 [pwwn 20:00:00:25:b5:01:0b:3f] [VM-Host-Infra-02-B]
  * fcid 0xa50000 [pwwn 50:05:07:68:0c:22:22:71] [VersaStack-ContA-FE2]
  * fcid 0xa50400 [pwwn 50:05:07:68:0c:52:22:71] [VersaStack-ContA-FE4]
  * fcid 0xa50100 [pwwn 50:05:07:68:0c:22:22:67] [VersaStack-ContB-FE2]
  * fcid 0xa50300 [pwwn 50:05:07:68:0c:52:22:67] [VersaStack-ContB-FE4]

  zone name VM-Host-Infra-03-B vsan 102
  * fcid 0xa50201 [pwwn 20:00:00:25:b5:01:0b:0f] [VM-Host-Infra-03-B]
  * fcid 0xa50000 [pwwn 50:05:07:68:0c:22:22:71] [VersaStack-ContA-FE2]
  * fcid 0xa50400 [pwwn 50:05:07:68:0c:52:22:71] [VersaStack-ContA-FE4]
  * fcid 0xa50100 [pwwn 50:05:07:68:0c:22:22:67] [VersaStack-ContB-FE2]
  * fcid 0xa50300 [pwwn 50:05:07:68:0c:52:22:67] [VersaStack-ContB-FE4]

  zone name VM-Host-Infra-04-B vsan 102
  * fcid 0xa50202 [pwwn 20:00:00:25:b5:01:0b:1f] [VM-Host-Infra-04-B]
  * fcid 0xa50000 [pwwn 50:05:07:68:0c:22:22:71] [VersaStack-ContA-FE2]
  * fcid 0xa50400 [pwwn 50:05:07:68:0c:52:22:71] [VersaStack-ContA-FE4]
  * fcid 0xa50100 [pwwn 50:05:07:68:0c:22:22:67] [VersaStack-ContB-FE2]
  * fcid 0xa50300 [pwwn 50:05:07:68:0c:52:22:67] [VersaStack-ContB-FE4]
```

6. Save the configuration.

   ```
   copy run start
   ```

Storage LUN Mapping

In this section we will be adding the host mappings for the host profiles created through Cisco UCS Manager to the V9000 storage, connecting to the boot LUNs, and doing the initial ESXi install. The WWPN's for the hosts will be required to complete this section.

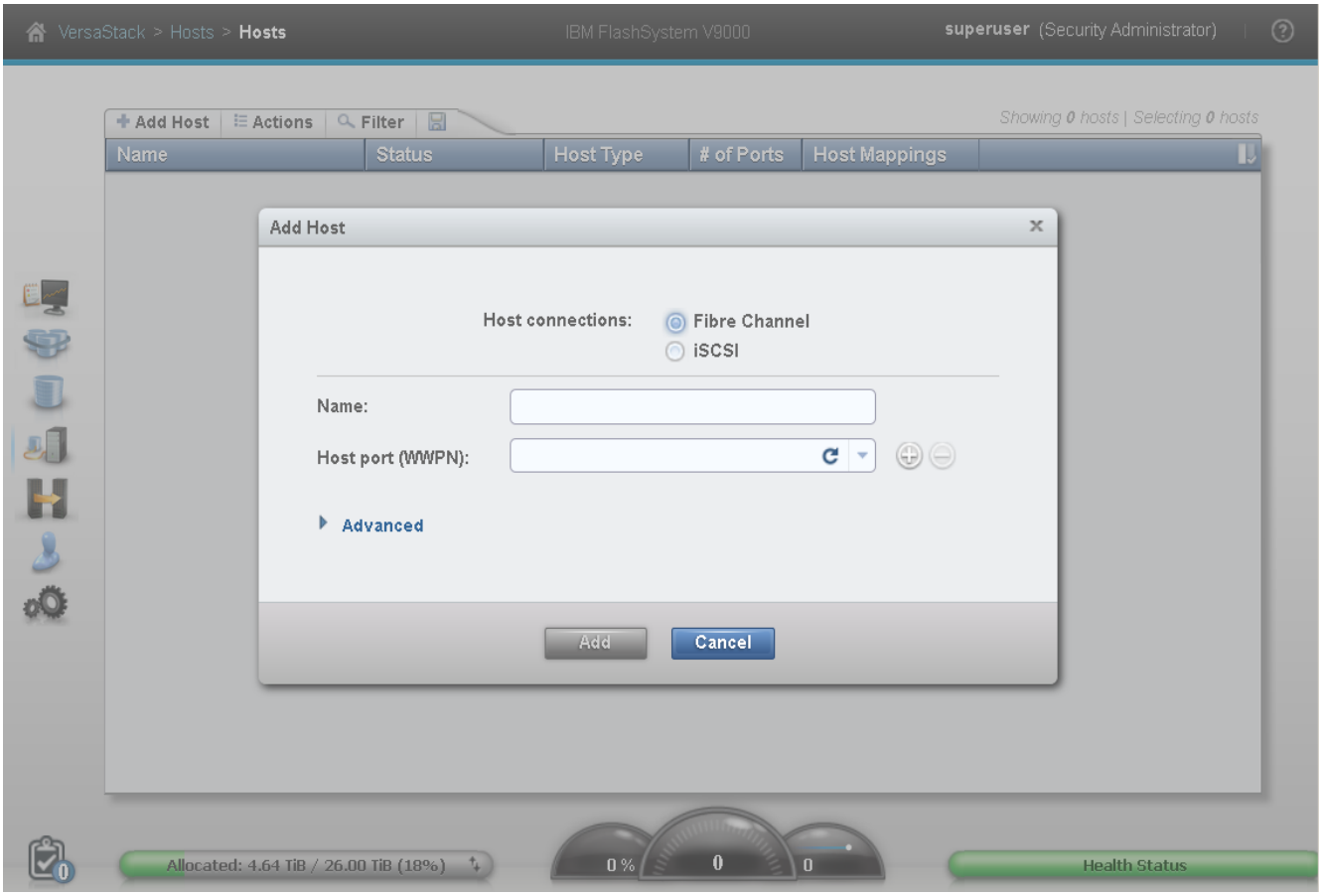
Adding Hosts and Mapping the Boot Volumes on the IBM FlashSystem V9000

To add hosts and map the boot volumes, complete the following steps:

1. Open the FlashSystem V9000 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 Hosts menu item.

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



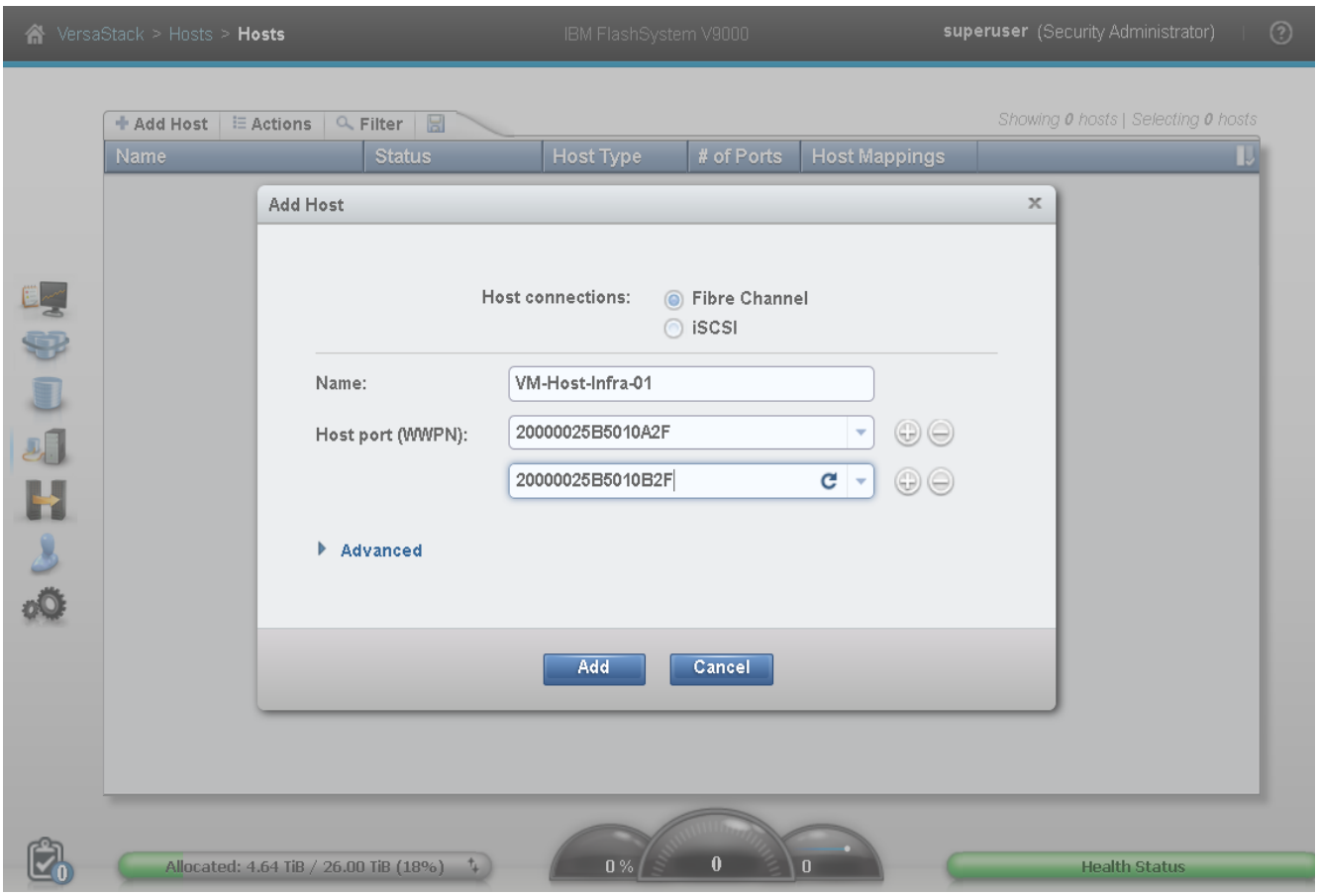
4. Input Host Name `VM-Host-Infra-01`.

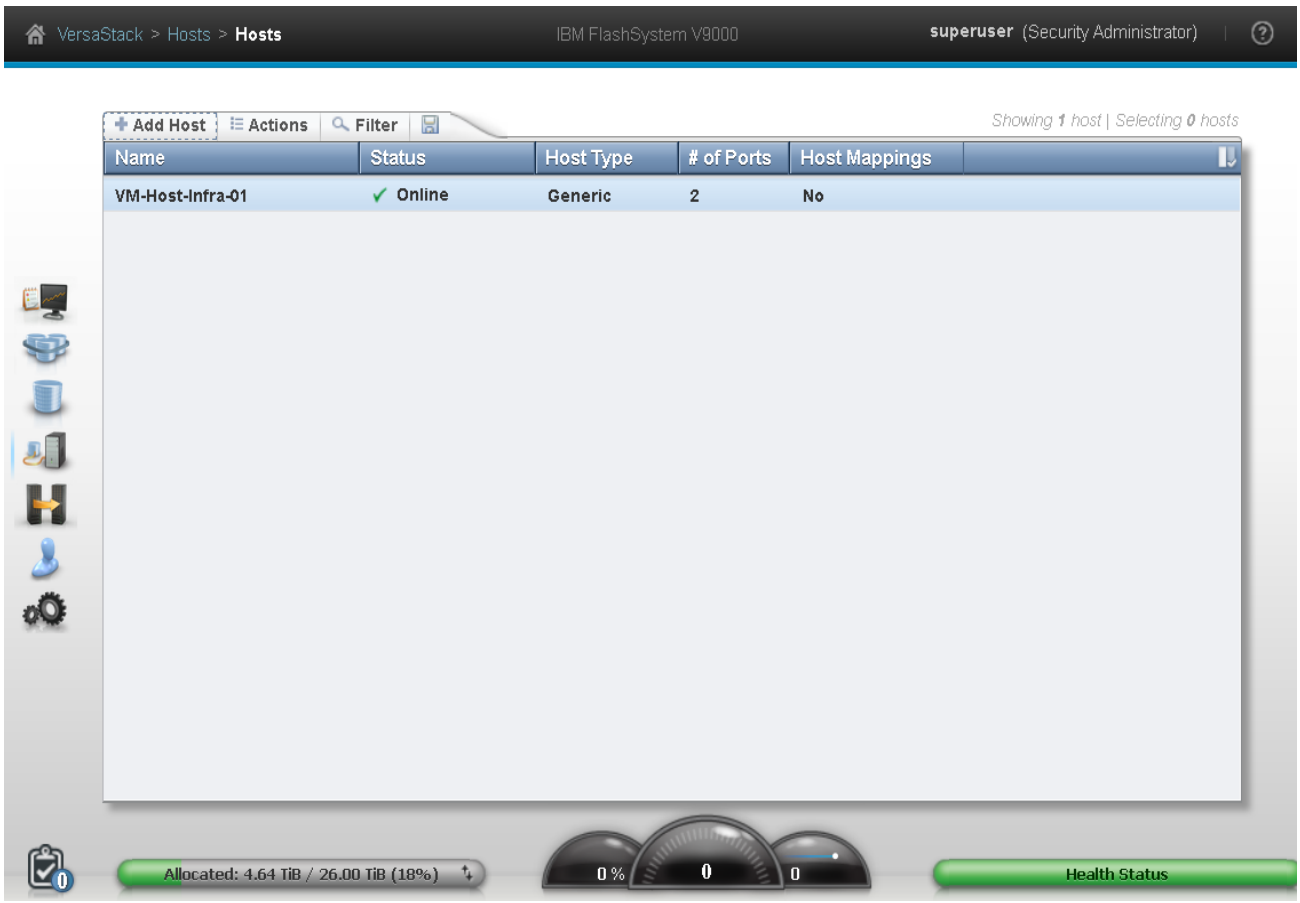
5. For Fibre Channel Ports open the drop-down menu and select or input the WWPN's for the A path vHBA's, `<<var_wwpn_VM-Host-infra-01-a>>`, and click Add Port to List.

6. Click the drop-down menu again, and select or Input the host B port, `<<wwpn_VM-Host-infra-01-b>>`, and click Add Port to List.

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

If the Hosts are powered on and zoned correctly they will appear in the selection drop-down or if you type in the WWPN, you should green check marks for each WWPNs.

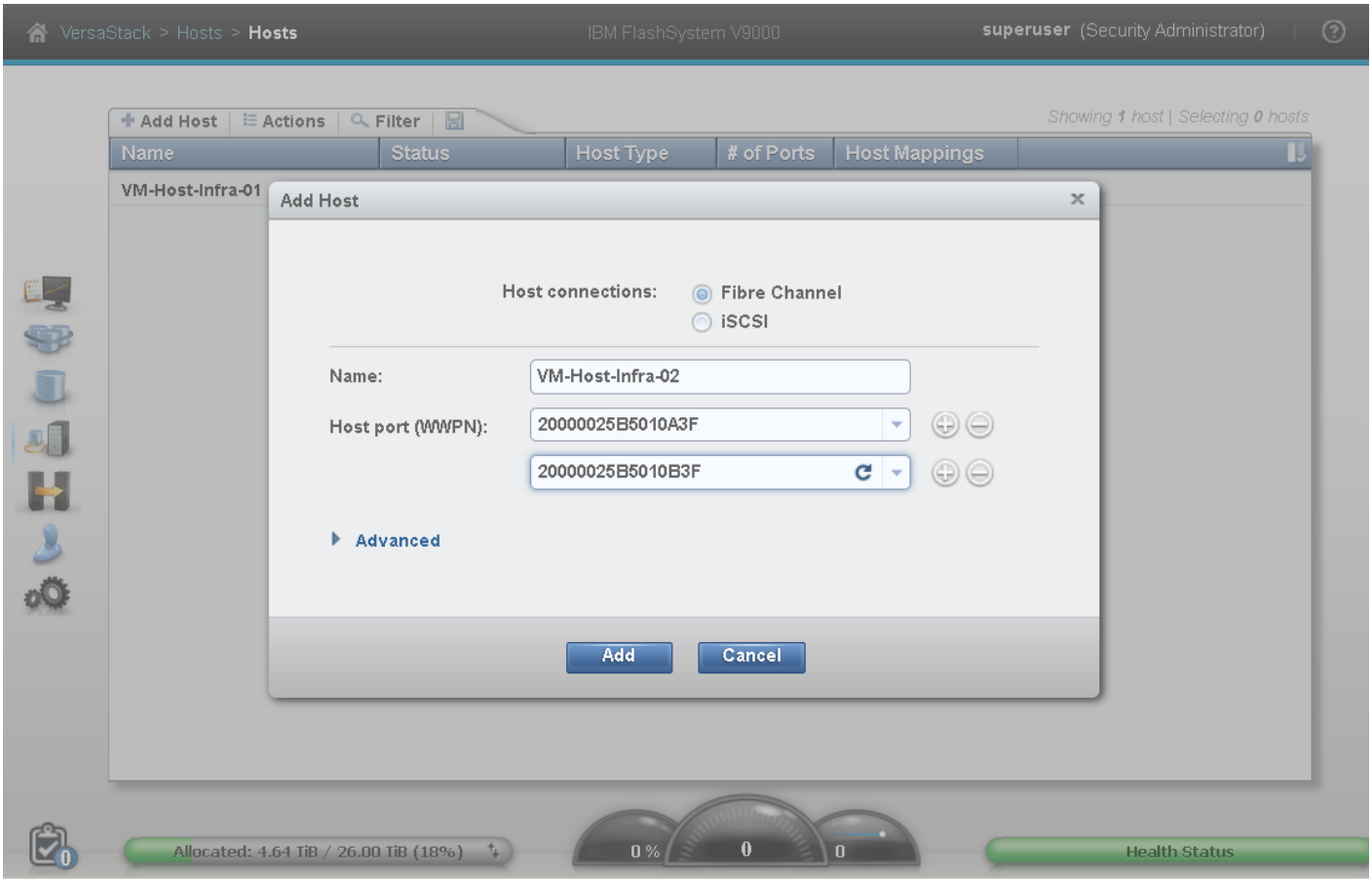

VersaStack > Hosts > Hosts
IBM FlashSystem V9000
superuser (Security Administrator)
Add Host
Actions
Filter
Showing 0 hosts | Selecting 0 hosts
Name
Status
Host Type
# of Ports
Host Mappings
Add Host
Host connections:
Fibre Channel
iSCSI
Name:
VM-Host-Infra-01
Host port (WWPN):
20000025B5010A2F
20000025B5010B2F
Advanced
Add
Cancel
Allocated: 4.64 TiB / 26.00 TiB (18%)
0 %
0
0
Health Status



8. Click Add Host to create the 2nd host, select Fibre Channel, and input `VM-Host-Infra-02` for Host Name.

9. For Fibre Channel Ports open the drop-down menu and select the WWPN's for the A path vHBA's, `<<var_wwpn_VM-Host-infra-02-a>>`, and click Add Port to List.

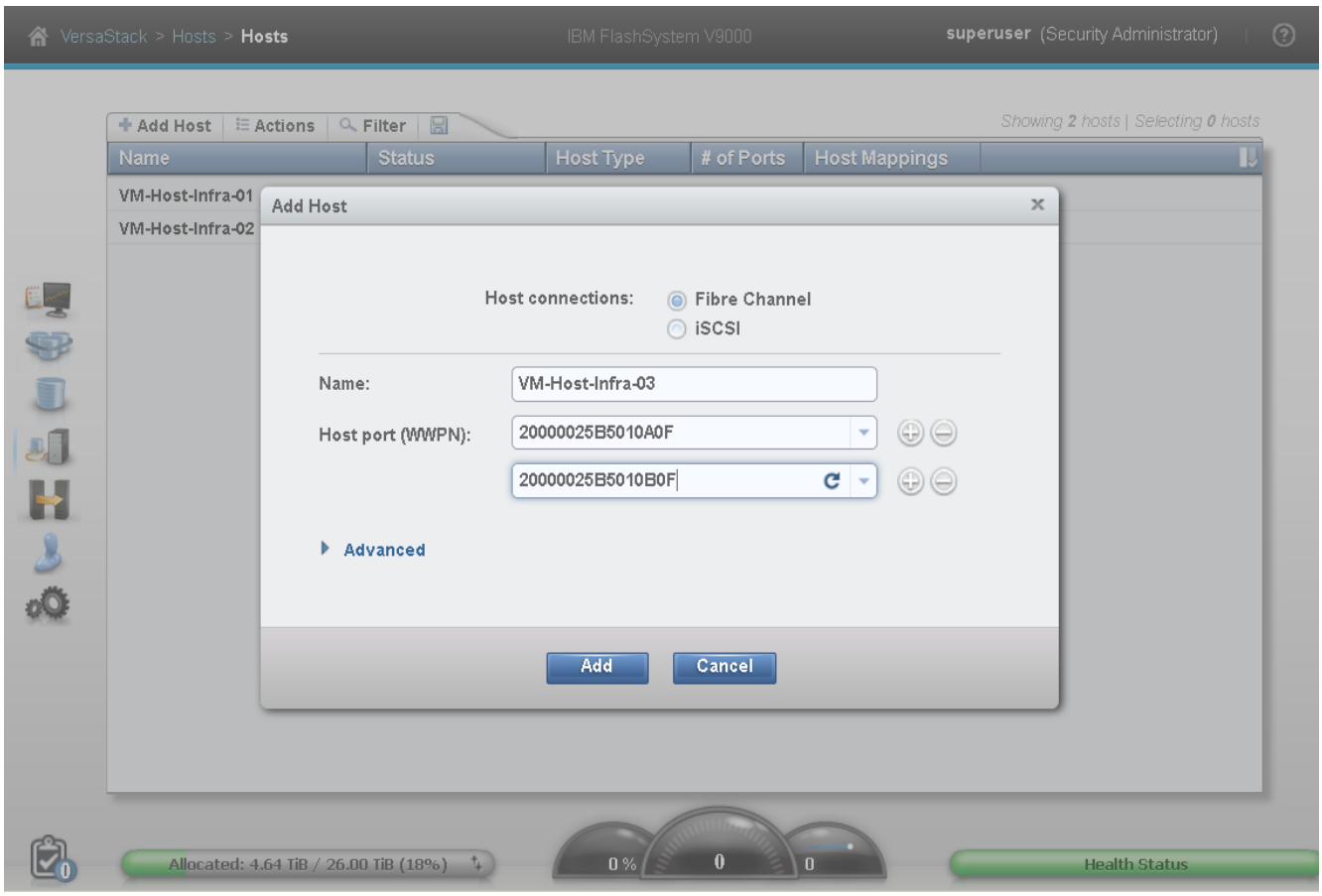
10. Select the B port by selecting the var for the B path, `<<wwpn_VM-Host-infra-02-b>>`, and click Add Port to List. Leave the Advanced Settings as default and click Add Host, then click Close.



11. Click Add Host to create the 3rd host, select Fibre Channel, and input `VM-Host-Infra-03` for Host Name.

12. For Fibre Channel Ports open the drop-down menu and select the WWPN's for the A path vHBA's, `<<var_wwpn_VM-Host-infra-03-a>>`, and click Add Port to List.

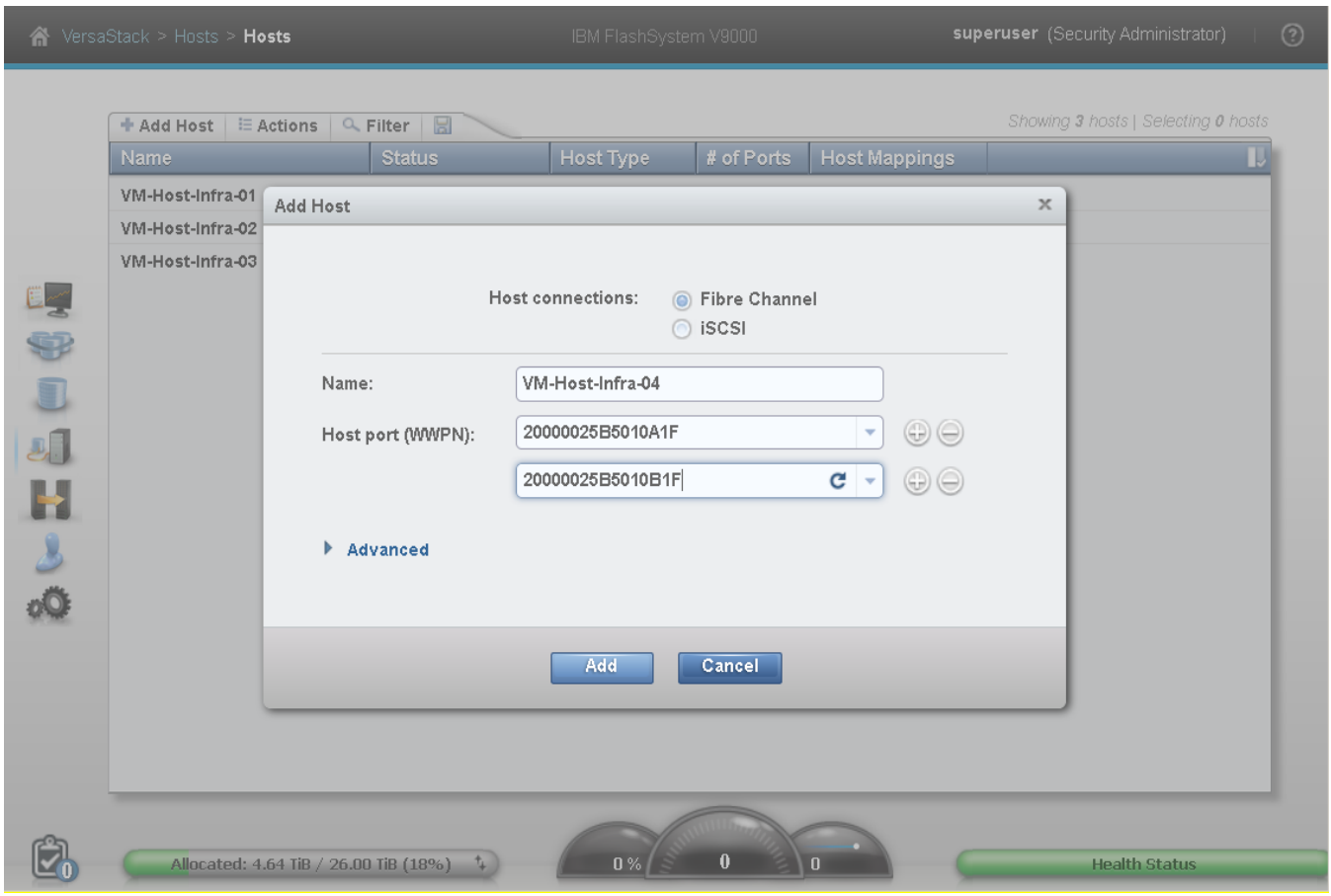
13. Select the B port by selecting the var for the B path, `<<wwpn_VM-Host-infra-03-b>>`, and click Add Port to List. Leave the Advanced Settings as default and click Add Host, then click Close.



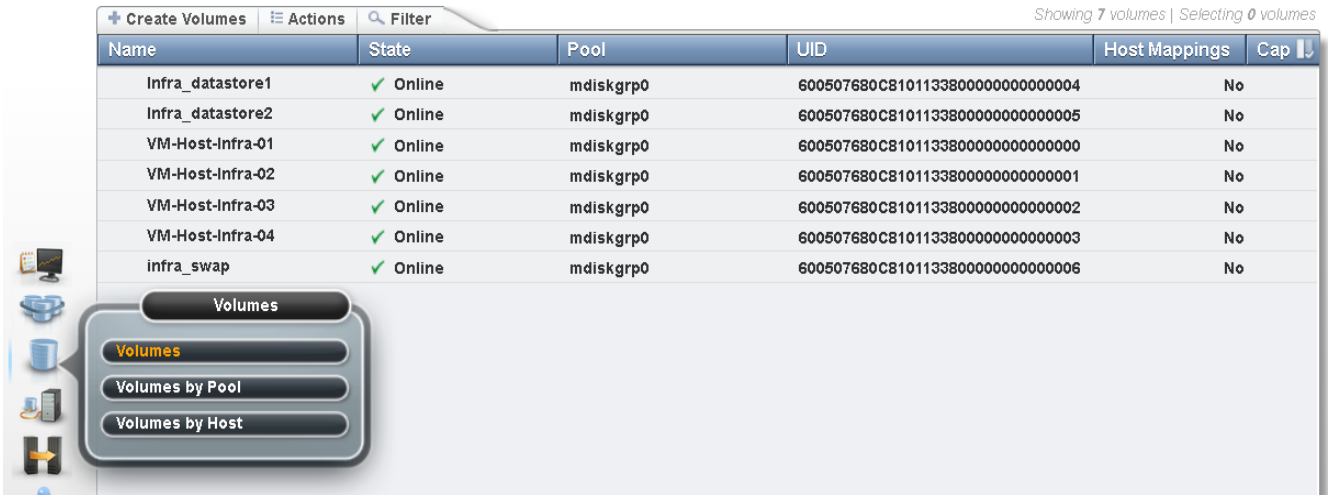
14. Click Add Host to create the 4th host, select Fibre Channel, and input `VM-Host-Infra-04` for Host Name.

15. For Fibre Channel Ports open the drop-down menu and select the WWPN's for the A path vHBAs, `<<var_wwpn_VM-Host-infra-04-a>>`, and click Add Port to List.

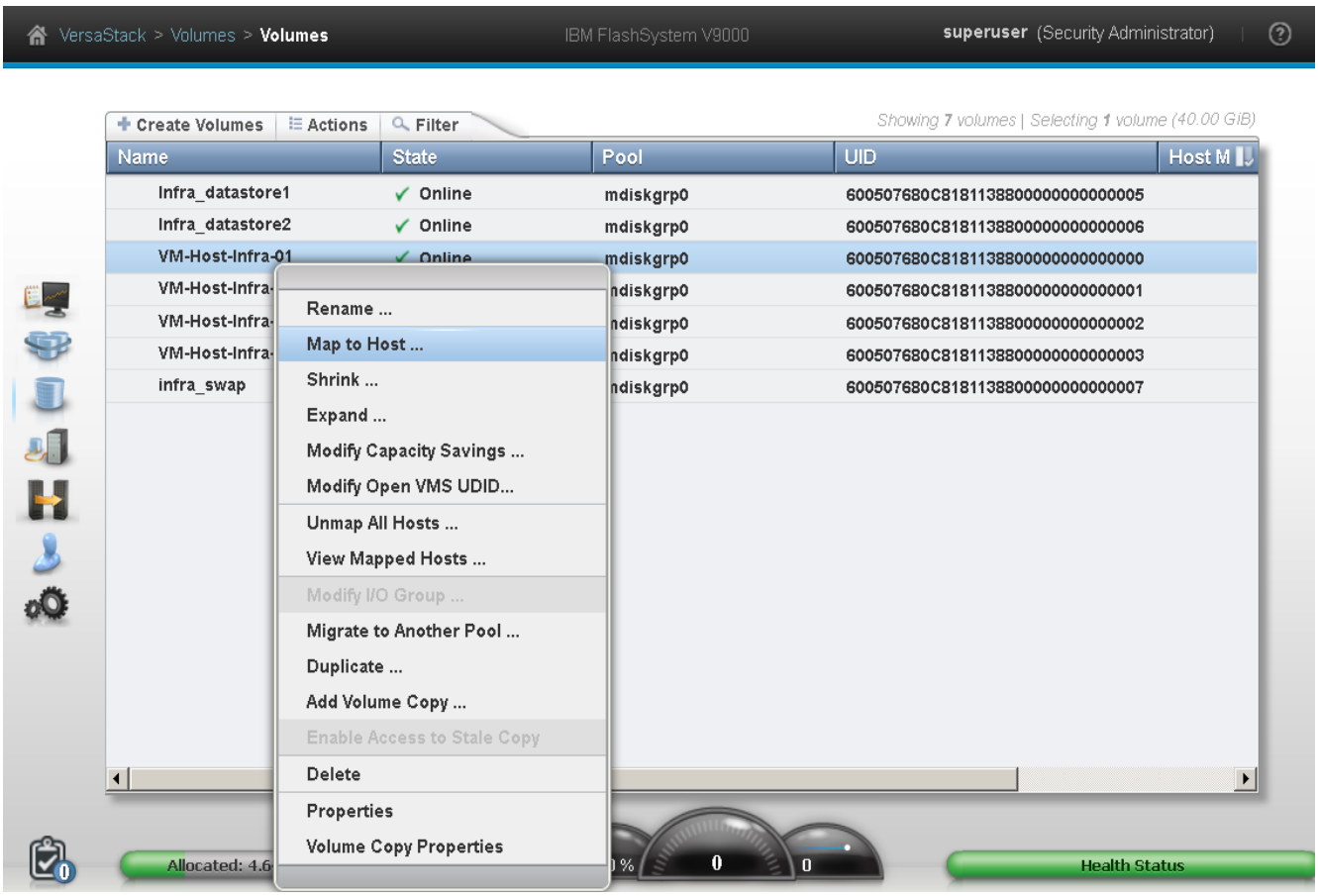
16. Select the B port by selecting the var for the B path, `<<wwpn_VM-Host-infra-04-b>>`, and click Add Port to List. Leave the Advanced Settings as default and click Add Host, then click Close.



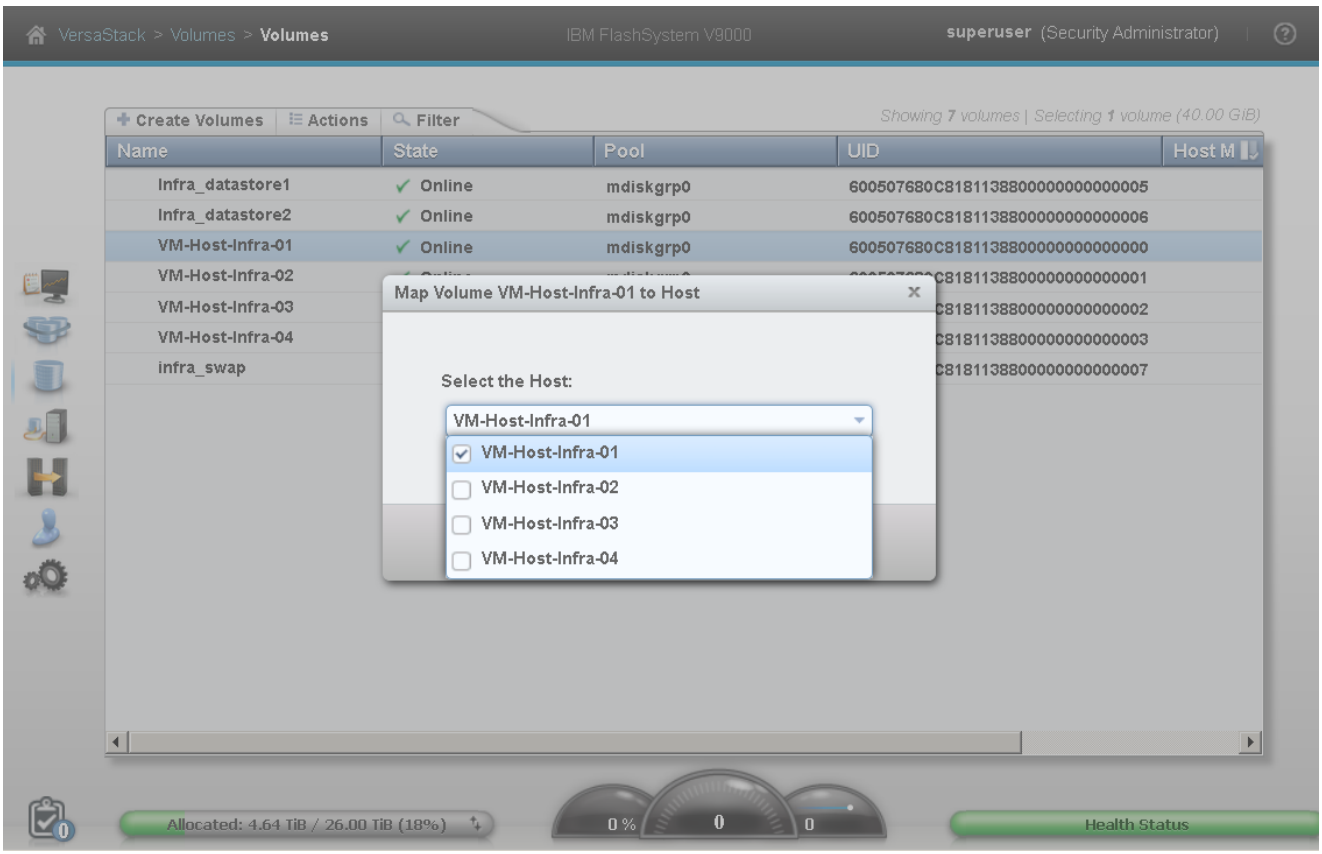
17. Click the Volumes icon in the left pane, then click the volumes menu item to display the created volumes.



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

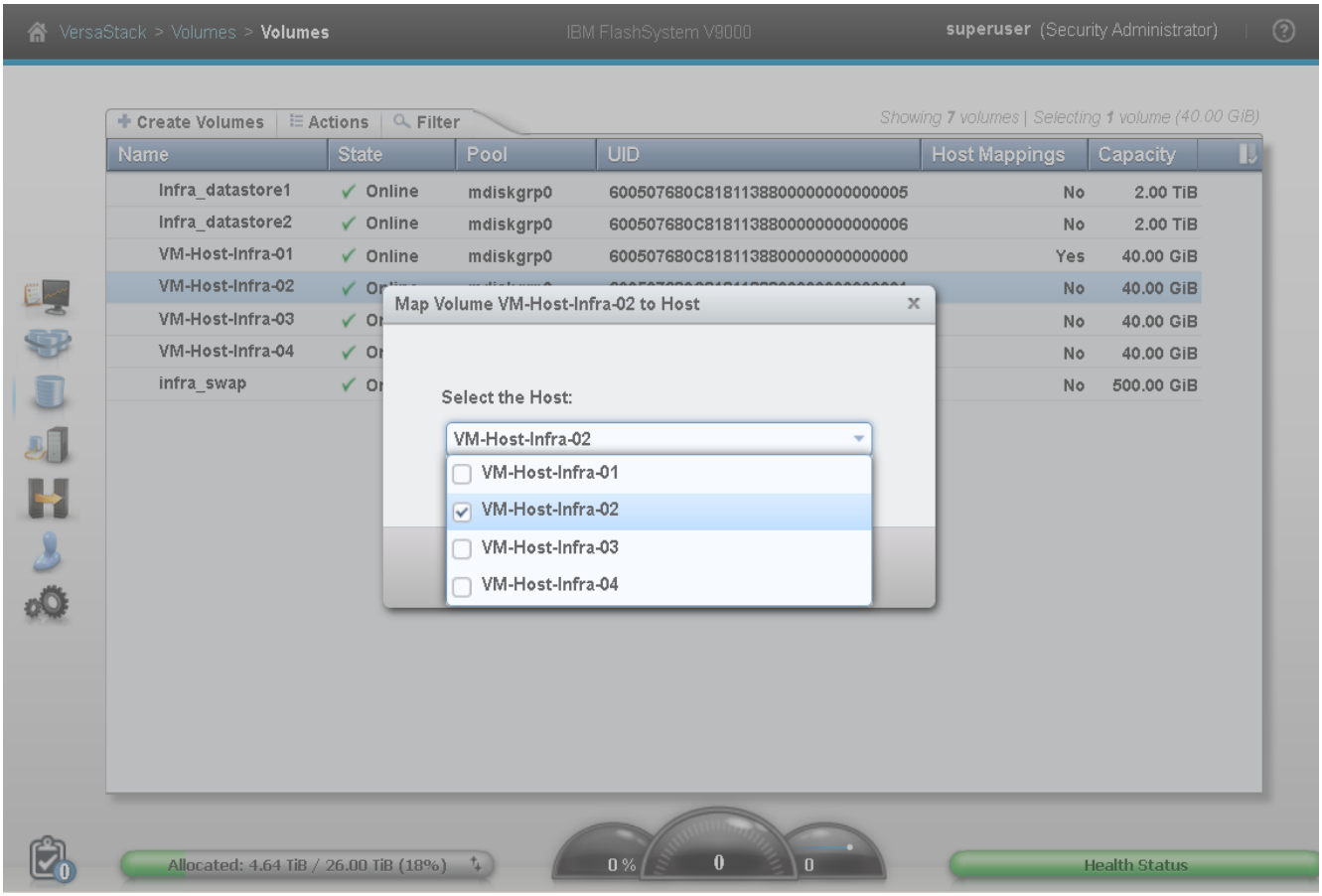


19. In the drop-down select `VM-Host-Infra-01`.



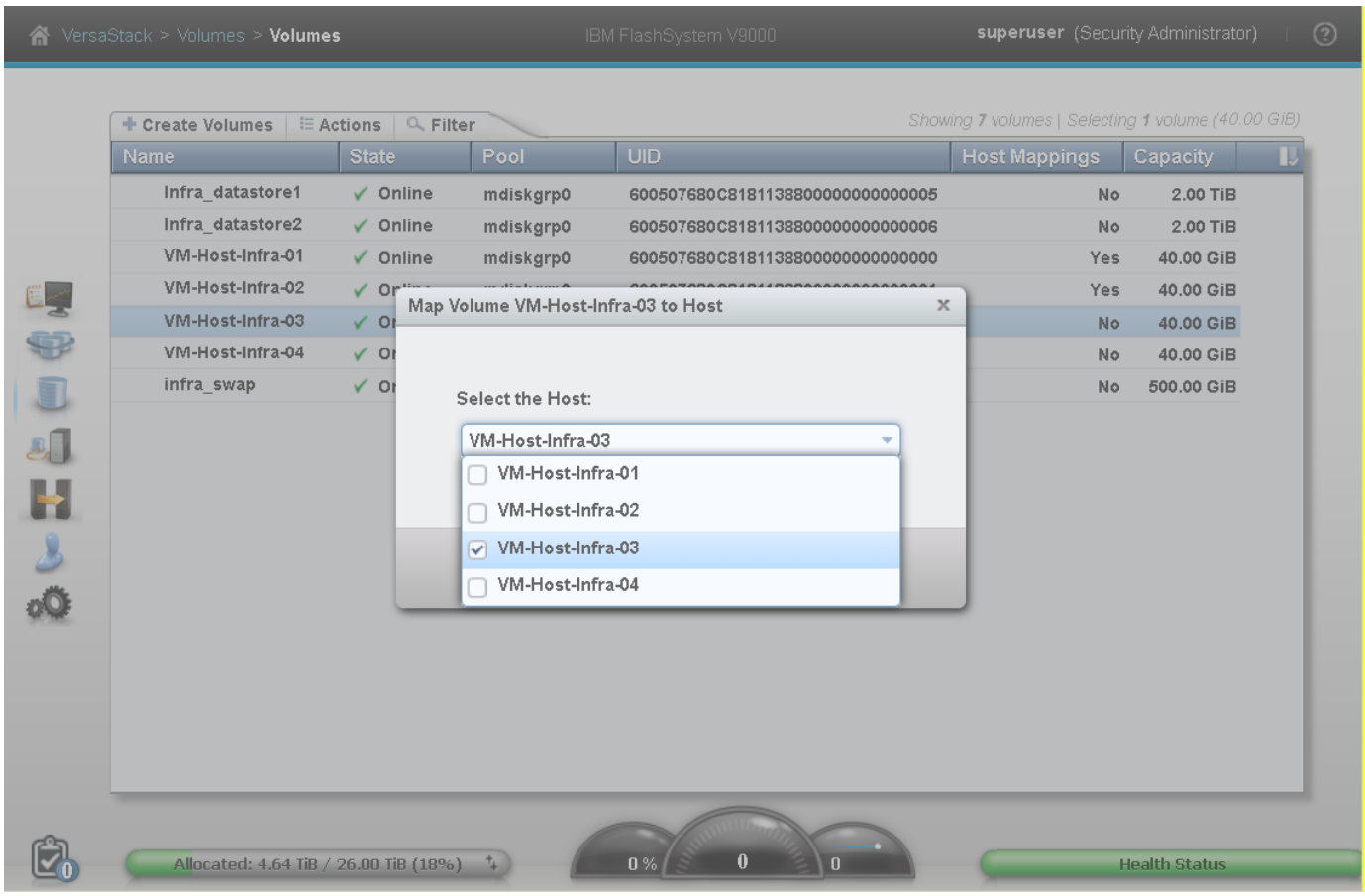
20. Select Map Volumes then click Close.

21. Right-click the volume `VM-Host-Infra-02` and click Map to host. In the drop-down select `VM-Host-Infra-02`.



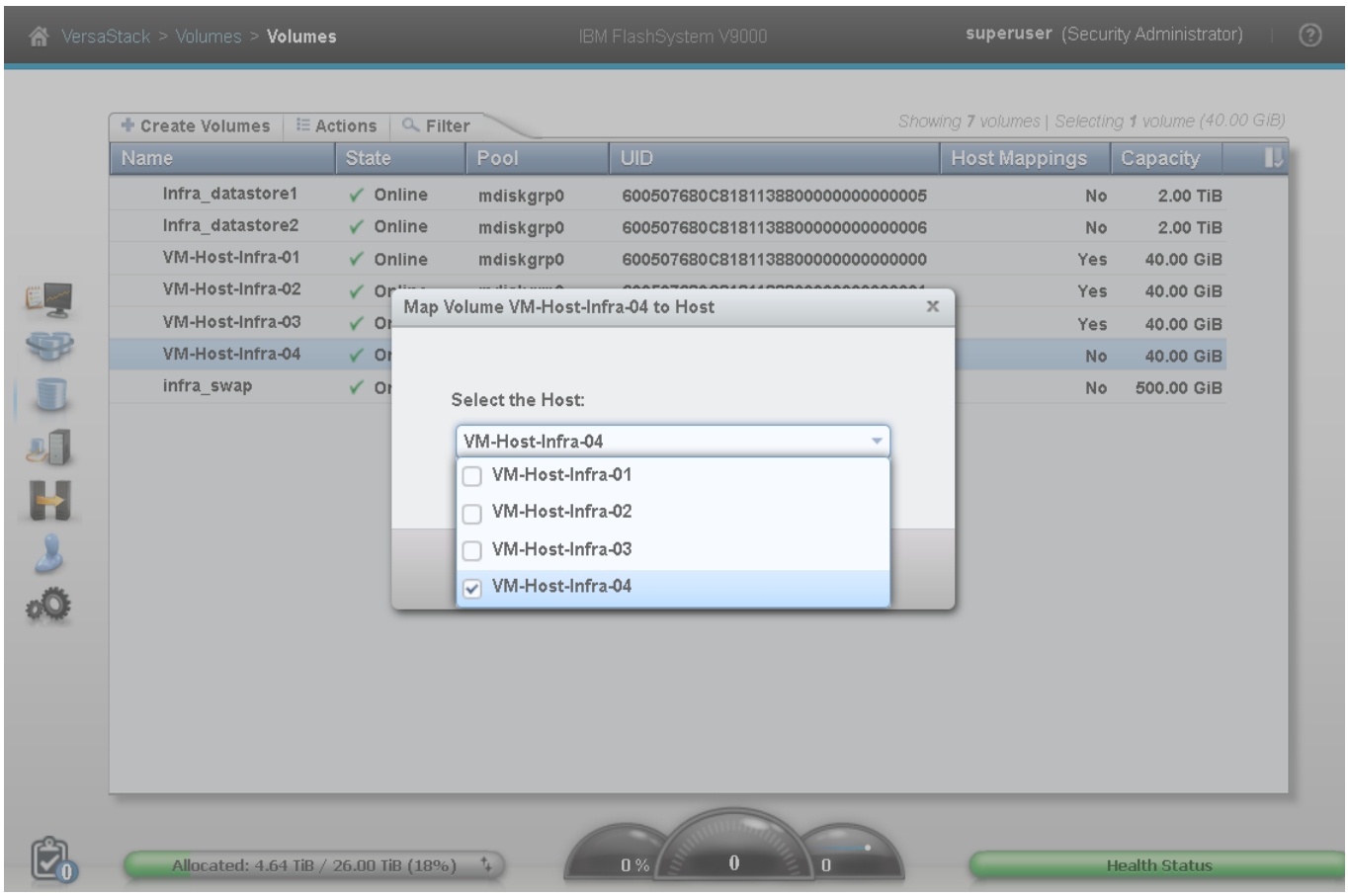
22. Click Map, and then click Close.

23. Right-click the volume `VM-Host-Infra-03` and click Map to host. In the drop-down select `VM-Host-Infra-03`.



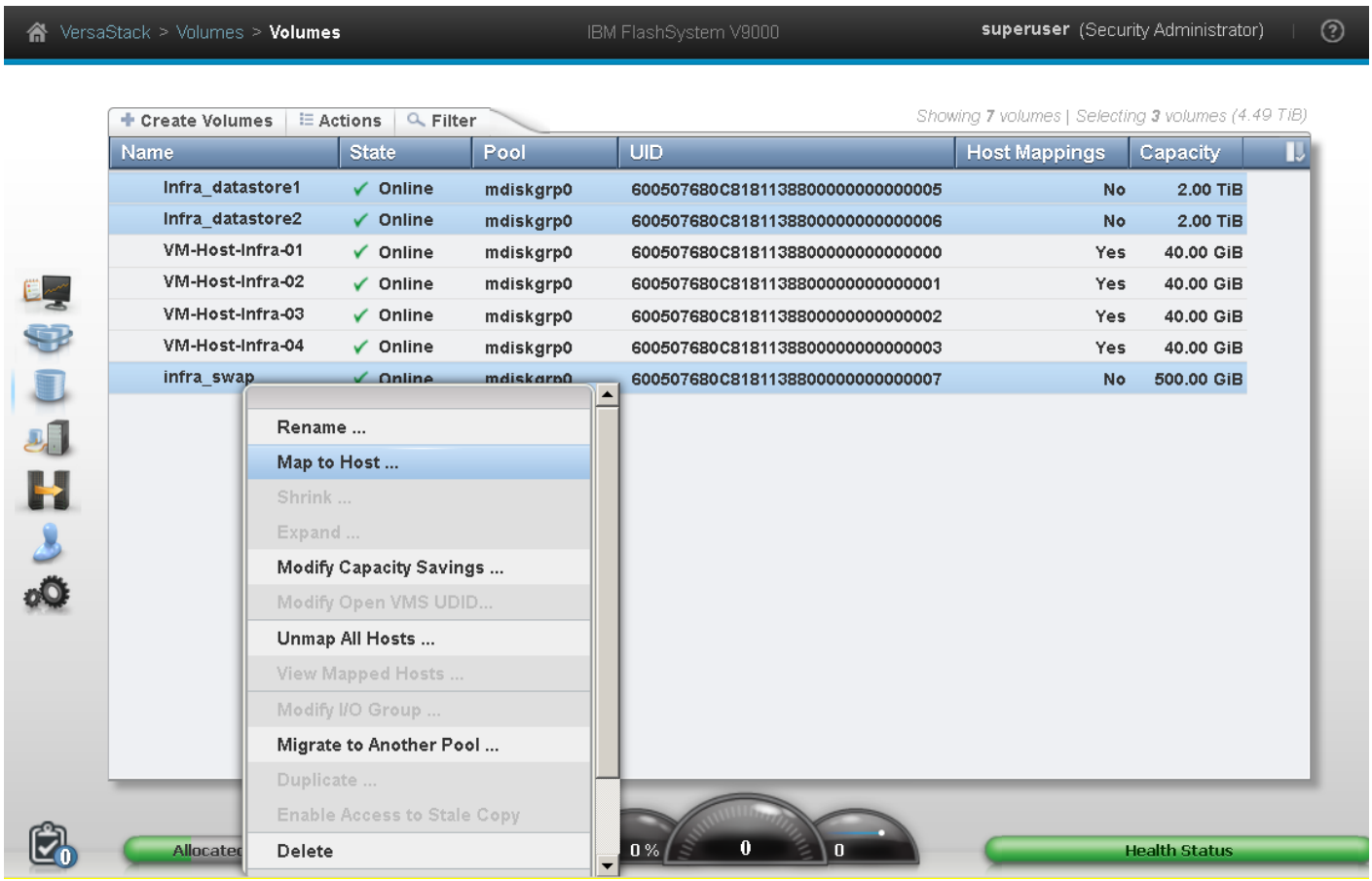
24. Click Map, and then click Close.

25. Right-click the volume `VM-Host-Infra-04` and click Map to host. In the drop-down select `VM-Host-Infra-04`.



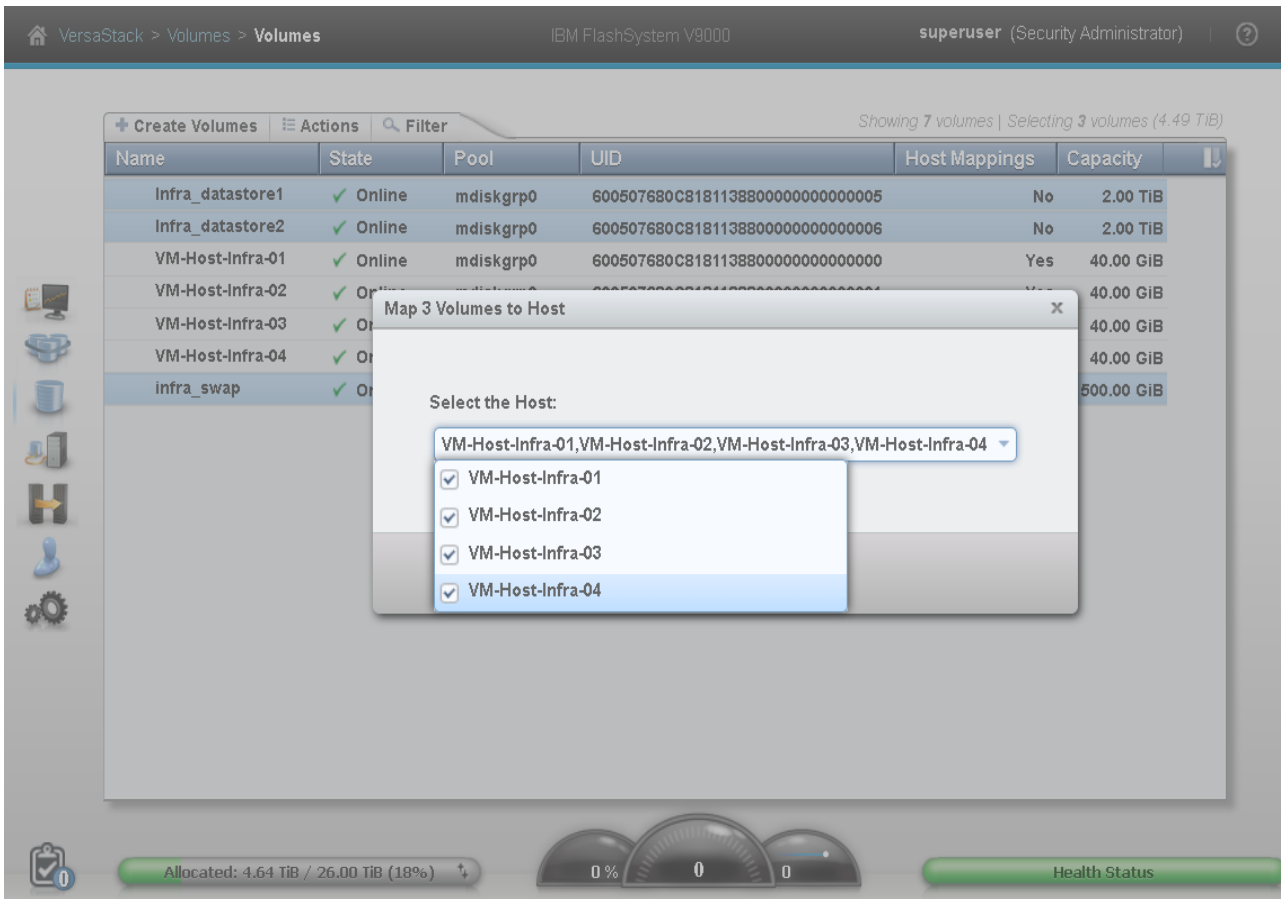
26. Click Map, and then click Close.

27. Holding down Control key on keyboard, left mouse click `Infra_datastore1`, `Infra_datastore2`, and `infra_swap`, then Right-click infra_swap, and click Map to Host.



28. Select all four hosts: `VM-Host-Infra-01, VM-Host-Infra-02, VM-Host-Infra-03, VM-Host-Infra-4.`

29. Click Map, and then click Close.



ESX and vSphere Installation and Setup

VersaStack VMware ESXi 6.0 Update 1a SAN Boot Installation

This section provides detailed instructions for installing VMware ESXi 6.0 Update 1a in a VersaStack environment. After the procedures are completed, four 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, we are using the Cisco Custom ESXi 6.0 U1a 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.

This ESXi 6.0 Cisco custom image includes updates for the fnic and enic drivers. The versions that are part of this image are: enic: 2.1.2.71; fnic: 1.6.0.17a

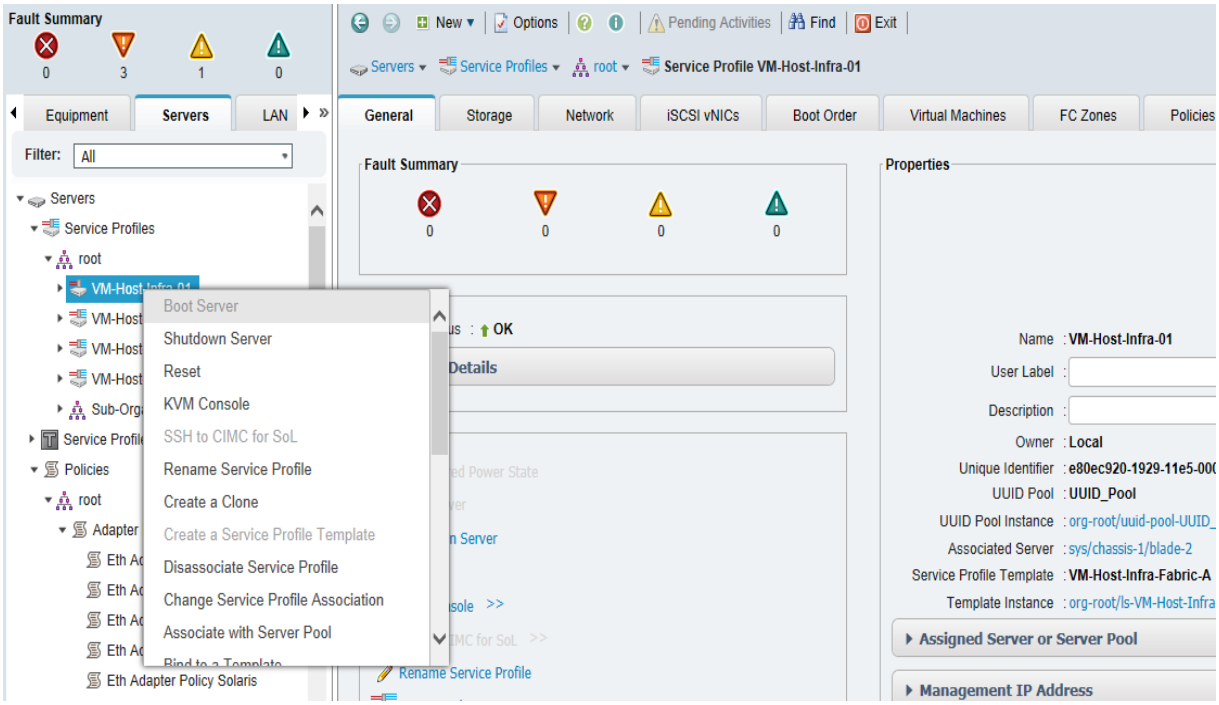
https://my.vmware.com/web/vmware/details?downloadGroup=OEM-ESXI60U1A-CISCO&productId=491

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.

1. Login to Cisco UCSM using a web browser – use the Cisco FI cluster IP address and admin username and password to log in.
2. Download the Cisco Custom ISO for ESXi from the VMware website.
3. Open a web browser and enter the IP address for the Cisco UCS cluster address. This step launches the Cisco UCS Manager application.
4. Log in to Cisco UCS Manager by using the admin user name and password.
5. From the main menu, click Servers tab.
6. Select Servers > Service Profiles > root > `VM-Host-Infra-01`.
7. Right-click `VM-Host-Infra-01` and select KVM Console Actions > KVM Console.
8. Repeat these steps for other servers.

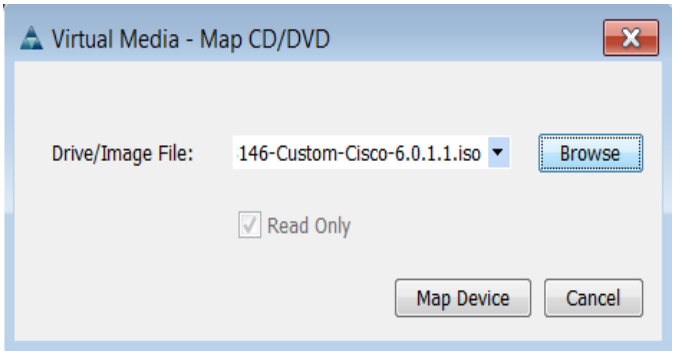


VMware ESXi Installation

ESXi Hosts VM-Host-Infra-01, VM-Host-Infra-02, VM-Host-Infra-03, and VM-Host-Infra-04

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 Map Device to map the newly added image.



5. Select Reset, then Ok and allow a power cycle and click 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, and then click OK again.

Install ESXi

ESXi Hosts VM-Host-Infra-01,VM-Host-Infra-02,VM-Host-Infra-03 and VM-Host-Infra-04

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 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.
26. Repeat the above procedure to configure `VM-Host-Infra-02`, `VM-Host-Infra-03` and `VM-Host-Infra-04` ESXi hosts.

vSphere Setup and ESXi configuration

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?downloadGroup=VCLI600&productId=491
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 then Finish.

These applications are downloaded from the VMware website and Internet.

Log in to VMware ESXi Hosts Using VMware vSphere Client

ESXi Host VM-Host-Infra-01

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

1. Open the recently downloaded VMware vSphere Client and enter the IP address of `VM-Host-Infra-01` as the host you are trying to connect to: `<<var_vm_host_infra_01_ip>>`.

2. Enter root for the user name.
3. Enter the root password.
4. Click Login to connect.

ESXi Host VM-Host-Infra-02

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

1. Open the recently downloaded VMware vSphere Client and enter the IP address of `VM-Host-Infra-02` as the host you are trying to connect to: `<<var_vm_host_infra_02_ip>>`.
2. Enter root for the user name.
3. Enter the root password.
4. Click Login to connect.
5. Login to VM-Host-Infra-03 and VM-Host-Infra-04 as per the above procedure.

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, VM-Host-Infra-02, VM-Host-Infra-03, VM-Host-Infra-04

Download and extract the following VMware VIC Drivers to the Management workstation:

- fnic Driver version 1.6.0.25
- enic Driver version 2.3.0.7

ESXi Hosts VM-Host-Infra-01, VM-Host-Infra-02, VM-Host-Infra-03 and VM-Host-Infra-04

1. From each vSphere Client, select the host in the inventory.
2. Click 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_1.6.0.25-offline_bundle-3741467.zip`.
6. Click Open, and then 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 `ESXi60-enic-2.3.0.7-offline_bundle-3642661.zip`.
9. Click Open, and then Yes to upload the file to datastore1.

10. Make sure the files have been uploaded to all 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:

Starting with vSphere 6.0, ESXCLI checks whether a trust relationship exists between the machine where you run the ESXCLI command and the ESXi host. An error results if the trust relationship does not exist. To get the host thumbprint, type the command without the --thumbprint option, then copy and paste the thumbprint into the command.

```
esxcli –s <<var_vm_host_infra_01_ip>> -u root –p <<var_password>> --thumbprint
<host_thumbprint> software vib update -d /vmfs/volumes/datastore1/
fnic_driver_1.6.0.25-offline_bundle-3741467.zip

esxcli –s <<var_vm_host_infra_02_ip>> -u root –p <<var_password>> -- thumbprint
<host_thumbprint> software vib update -d /vmfs/volumes/datastore1/
fnic_driver_1.6.0.25-offline_bundle-3741467.zip

esxcli –s <<var_vm_host_infra_03_ip>> -u root –p <<var_password>> --thumbprint
<host_thumbprint> software vib update -d /vmfs/volumes/datastore1/
fnic_driver_1.6.0.25-offline_bundle-3741467.zip

esxcli –s <<var_vm_host_infra_04_ip>> -u root –p <<var_password>> -- thumbprint
<host_thumbprint> software vib update -d /vmfs/volumes/datastore1/
fnic_driver_1.6.0.25-offline_bundle-3741467.zip

esxcli –s <<var_vm_host_infra_01_ip>> -u root –p <<var_password>> -- thumbprint
<host_thumbprint> software vib update -d /vmfs/volumes/datastore1/ ESXi60-enic-
2.3.0.7-offline_bundle-3642661.zip

esxcli –s <<var_vm_host_infra_02_ip>> -u root –p <<var_password>> -- thumbprint
<host_thumbprint> software vib update -d /vmfs/volumes/datastore1/ ESXi60-enic-
2.3.0.7-offline_bundle-3642661.zip

esxcli –s <<var_vm_host_infra_03_ip>> -u root –p <<var_password>> -- thumbprint
<host_thumbprint> software vib update -d /vmfs/volumes/datastore1/ ESXi60-enic-
2.3.0.7-offline_bundle-3642661.zip

esxcli –s <<var_vm_host_infra_04_ip>> -u root –p <<var_password>> -- thumbprint
<host_thumbprint> software vib update -d /vmfs/volumes/datastore1/ ESXi60-enic-
2.3.0.7-offline_bundle-3642661.zip
```

13. Back in the vSphere Client for each host, right-click the host and select Reboot.

14. Click Yes, and then OK to reboot the host.

Set Up VMkernel Ports and Virtual Switch

ESXi Host VM-Host-Infra-01

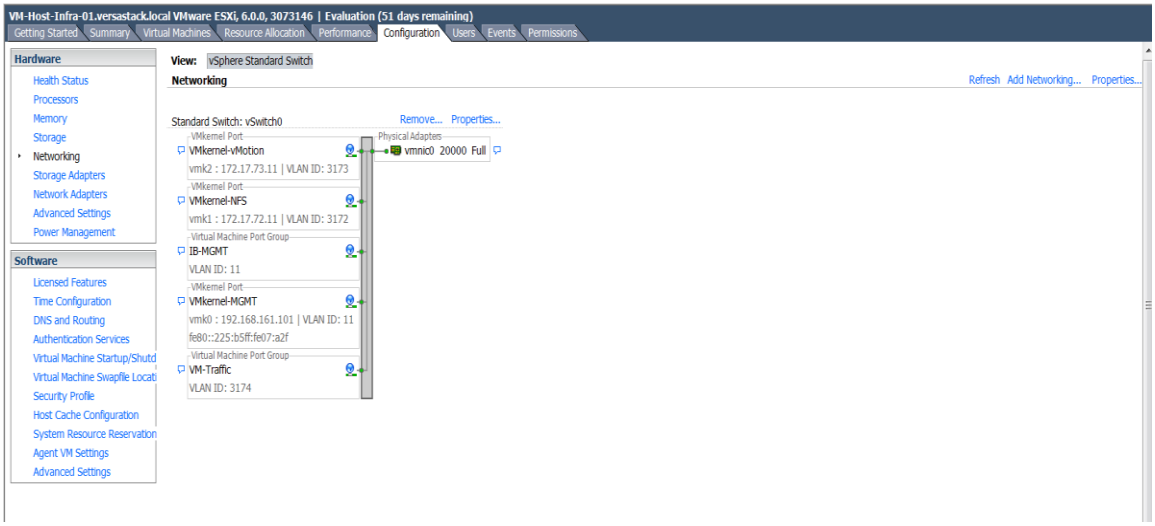
Repeat the steps in this section for all the ESXi Hosts.

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

1. From vSphere Client, select the host in the inventory.
2. Click 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 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 then 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 then 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, and then 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 click Close.



Mount Required VMFS Datastores

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 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 first 2TB 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. Select the other 2TB Datastore LUN and click Next.
13. Accept default VMFS setting and click Next.
14. Click Next for the disk layout.
15. Enter `infra_datastore_2` as the datastore name.
16. Click Next to retain maximum available space.

17. Click Finish.
18. Click Add Storage to open the Add Storage wizard.
19. Select Disk/LUN and click Next.
20. Select the 500GB swap LUN and click Next.
21. Accept default VMFS setting and click Next.
22. Click Next for the disk layout.
23. Enter `infra_swap` as the datastore name.
24. Click Next to retain maximum available space.
25. Click Finish.

Configure NTP on ESXi Hosts

ESXi Hosts VM-Host-Infra-01, VM-Host-Infra-02, VM-Host-Infra-03 and VM-Host-Infra-04

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 Configuration tab to enable configurations.
3. Click Time Configuration in the Software pane.
4. Click Properties at the upper right side of the window.
5. At the bottom of the Time Configuration dialog box, click Options.
6. In the NTP Daemon Options dialog box, complete the following steps:
    a. Click General in the left pane and select Start and stop with host.
    b. Click NTP Settings in the left pane and click Add.
    c. In the Add NTP Server dialog box, enter `<<var_global_ntp_server_ip>>` as the IP address of the NTP server and click OK.
    d. In the NTP Daemon Options dialog box, select the Restart NTP Service to Apply Changes check-box and click OK.
7. In the Time Configuration dialog box, complete the following steps:
    a. Select NTP Client Enabled checkbox and click OK.
    b. Verify that the clock is now set to approximately the correct time.

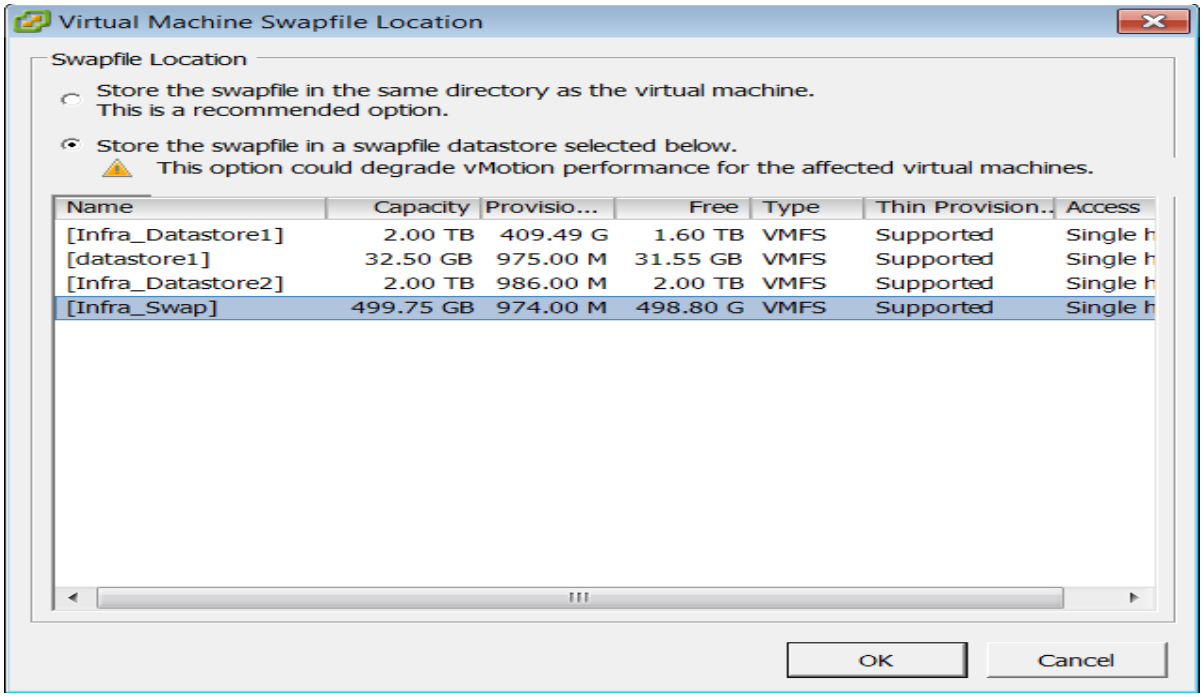
The NTP server time may vary slightly from the host time.

Move VM Swap File Location

ESXi Hosts VM-Host-Infra-01, VM-Host-Infra-02, VM-Host-Infra-03 and VM-Host-Infra-04

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

1. From the vSphere Client, select the host in the inventory.
2. To enable configurations, click Configuration tab.
3. Click Virtual Machine Swapfile Location in the Software pane.
4. Click Edit at the upper-right side of the window.
5. Select “Store the swapfile in a swapfile datastore selected below”
6. Select the <Infra_Swap> datastore in which to house the swap files.



7. Click OK to finalize moving the swap file location.

VersaStack VMware vCenter 6.0

The procedures in the following subsections provide detailed instructions to install VMware vCenter 6.0 appliance in a VersaStack environment. These deployment procedures are customized to include the environment variables.

Build and Setup VMware vCenter 6.0

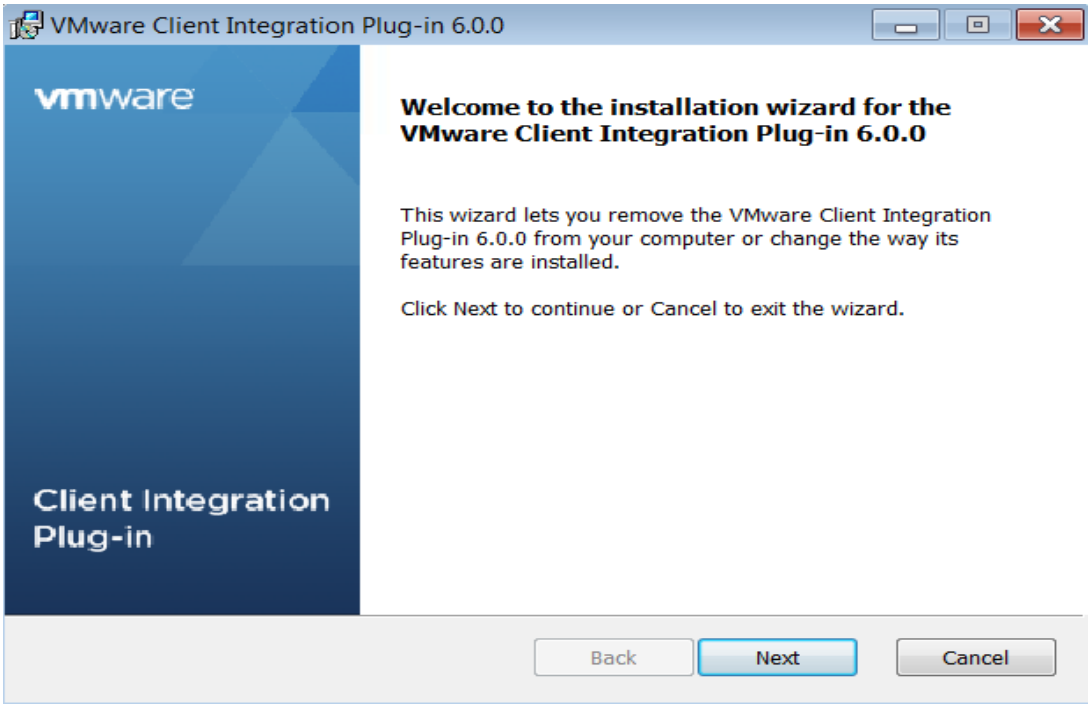
The procedures in the following subsections provide detailed instructions for installing the VMware vCenter 6.0 Server Appliance in an environment. After the procedures are completed, a VMware vCenter Server will be configured.

Installing/upgrading VMware vCenter Server Appliance (VCSA) in 6.0 is significantly different from other releases and uses an ISO file. Please refer to Knowledge Base 2110730 article for details installing VCSA 6.0.

Install the Client Integration Plug-In

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

1. Download the .iso installer for the vCenter Server Appliance and Client Integration Plug-in.
2. Mount the ISO image to the Windows virtual machine or physical server on which you want to install the Client Integration Plug-In to deploy the vCenter Server Appliance.
3. In the software installer directory, navigate to the vcsa directory and double-click VMware-ClientIntegrationPlugin-6.0.0.exe. The Client Integration Plug-in installation wizard appears.

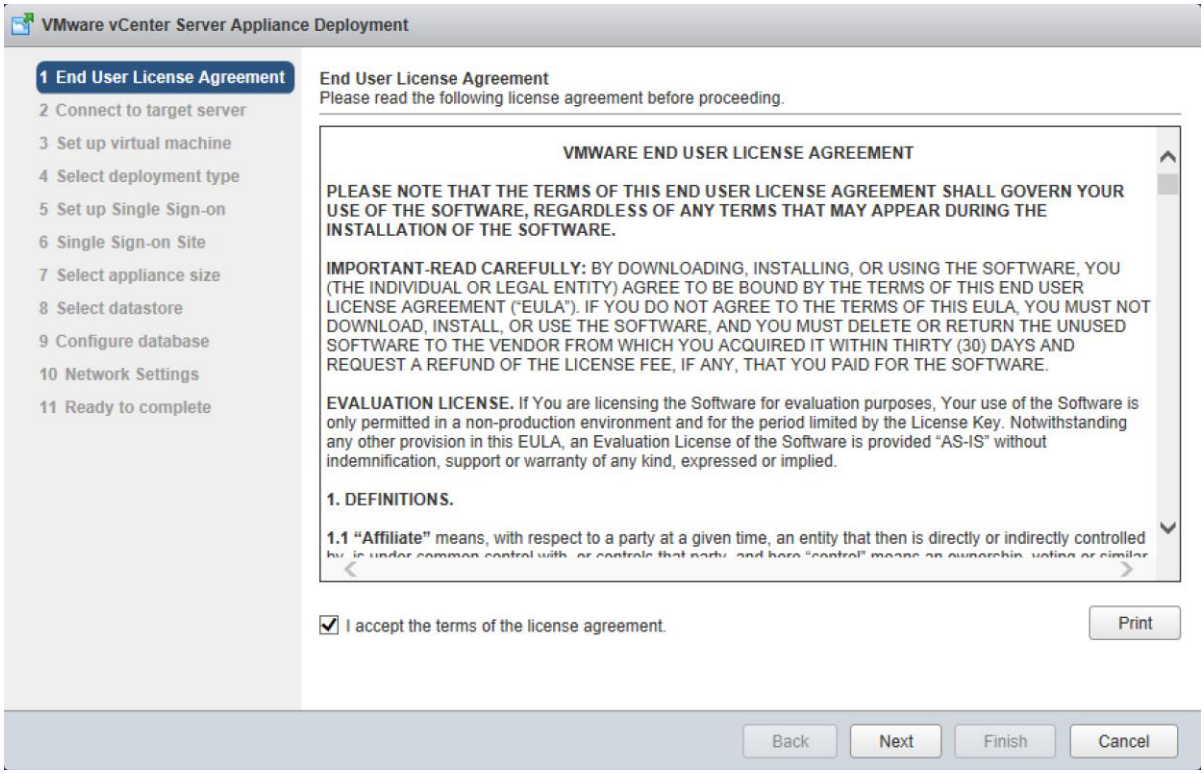


4. On the Welcome page, click Next.
5. Read and accept the terms in the End-User License Agreement and click Next.
6. Click Next.
7. Click Install.

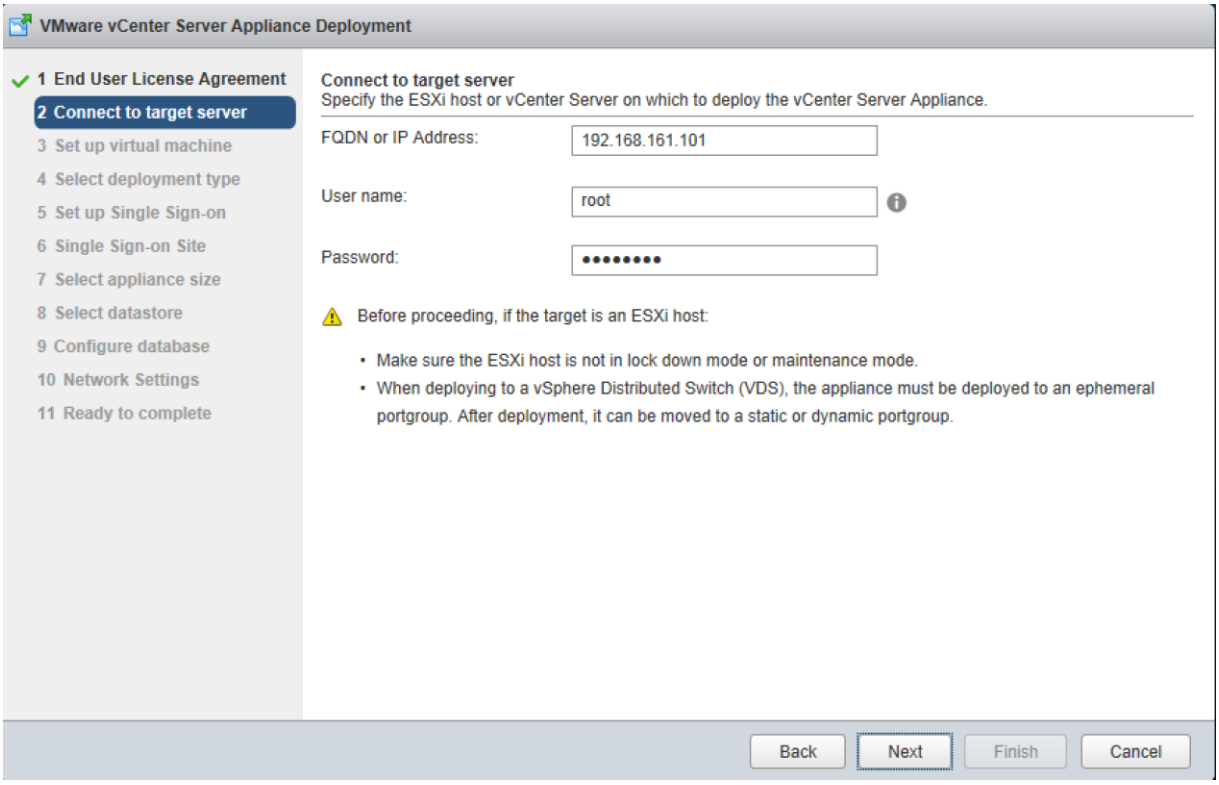
Building the VMware vCenter Server Appliance

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

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

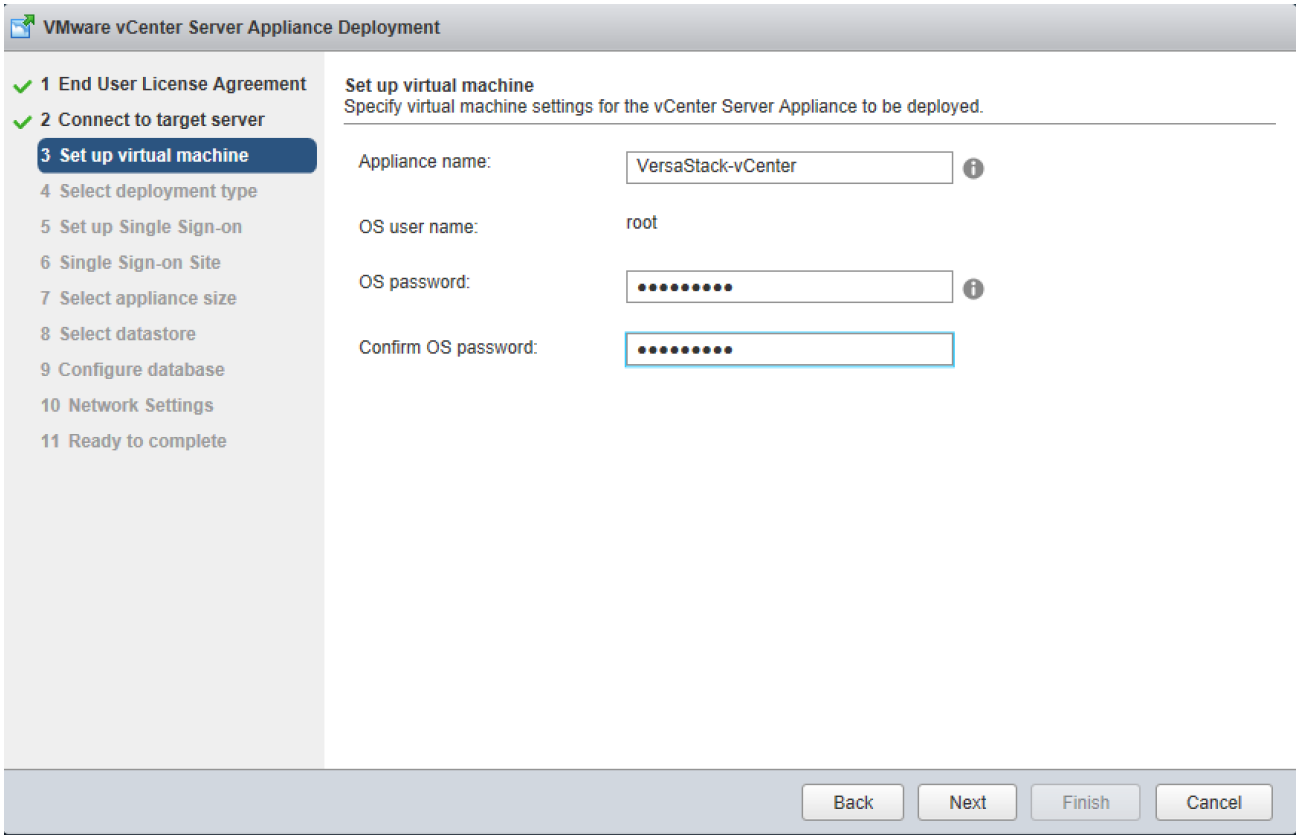


5. On the "Connect to target server" page, enter the ESXi host name, User name and Password.

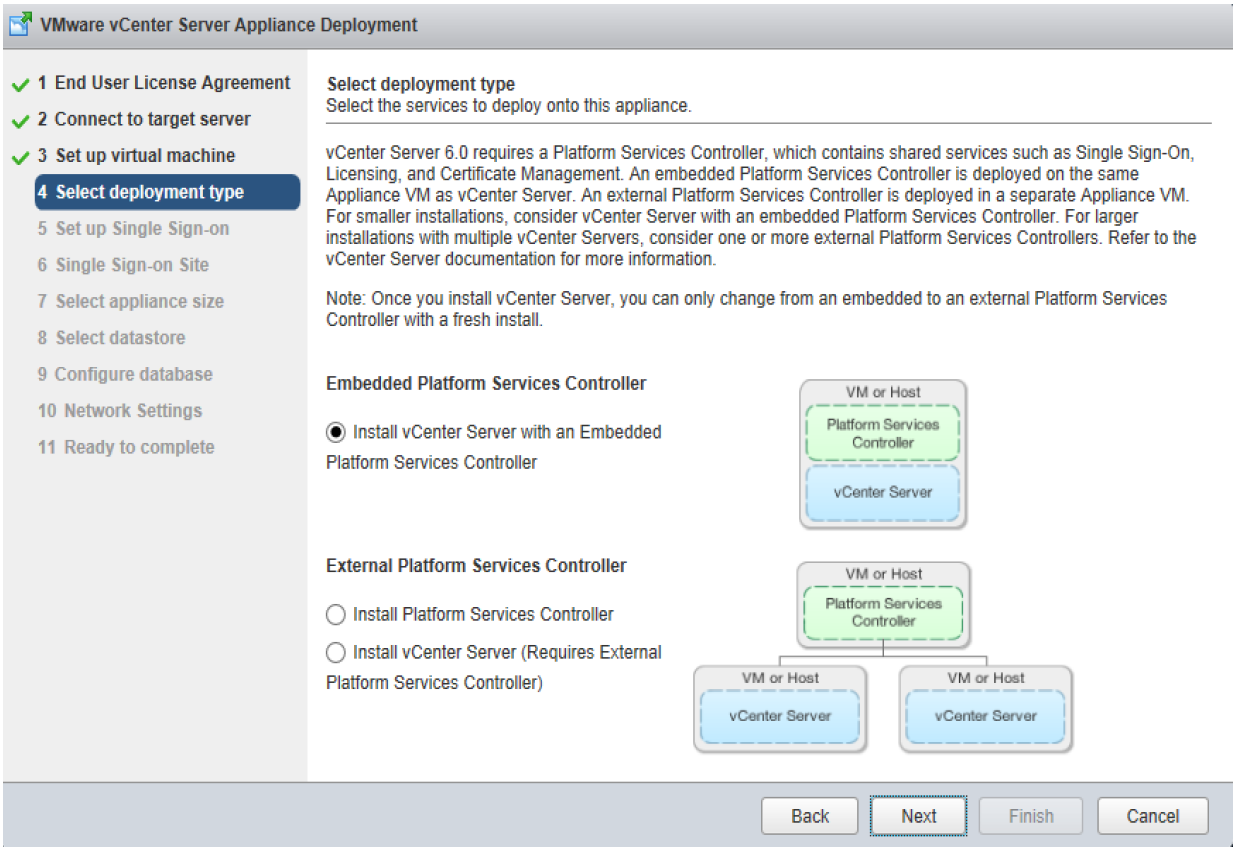


6. Click Yes to accept the certificate.

7. On the Set up virtual machine screen, enter the vCenter Server Appliance name, set the password for the root user, and click Next.

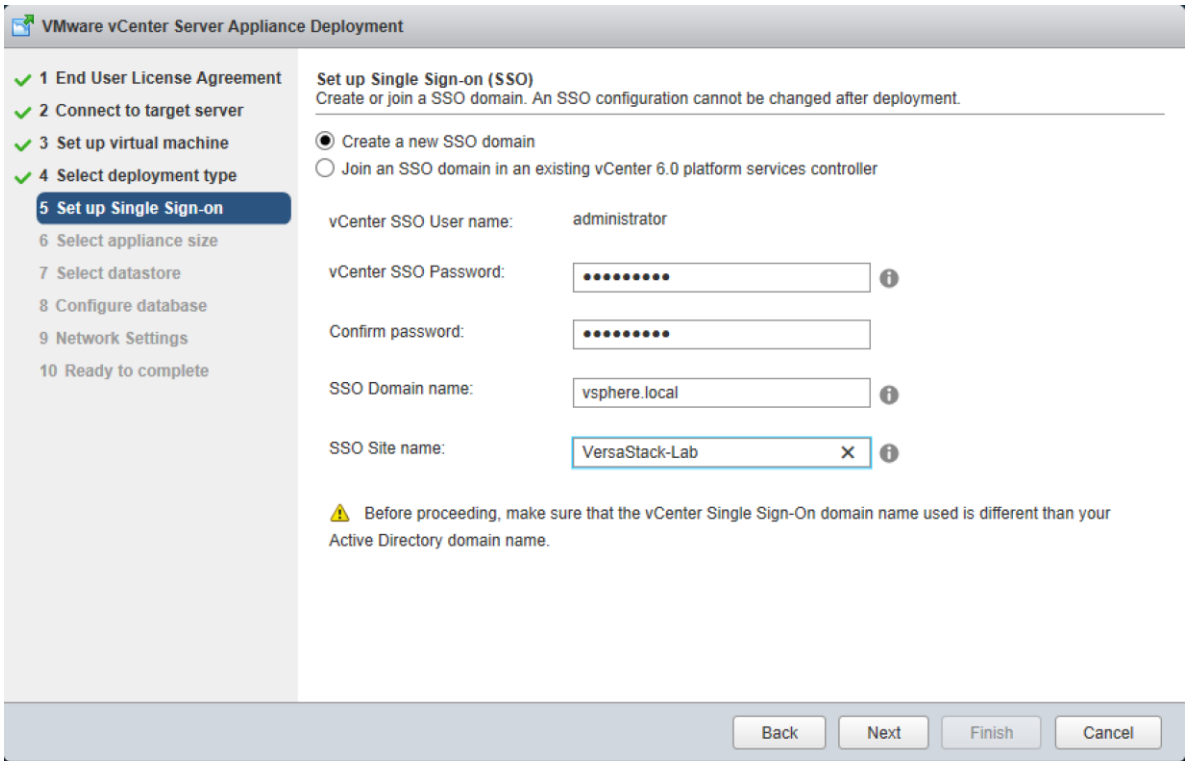


8. In the Select deployment type screen, select Install vCenter Server with an embedded Platform Services Controller and click Next.

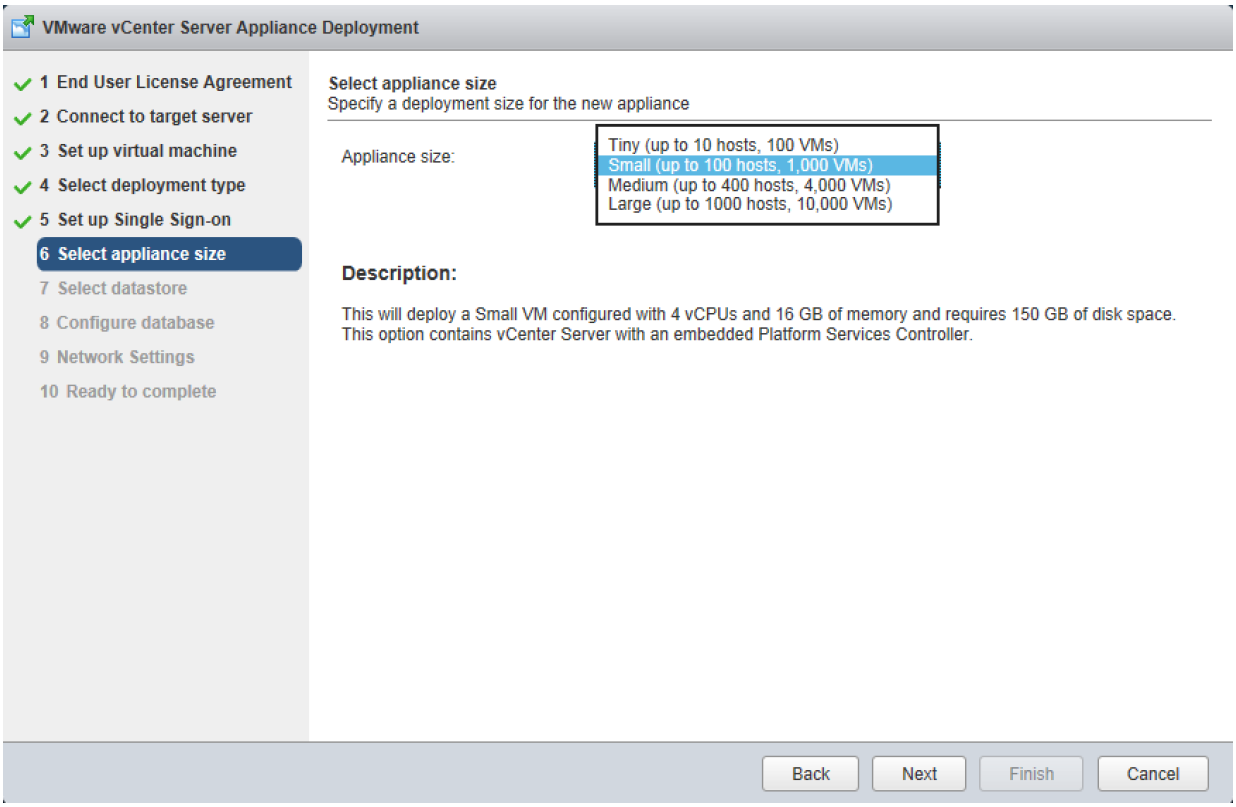


9. In the “Set up Single Sign-On” page, select “Create a new SSO domain.”

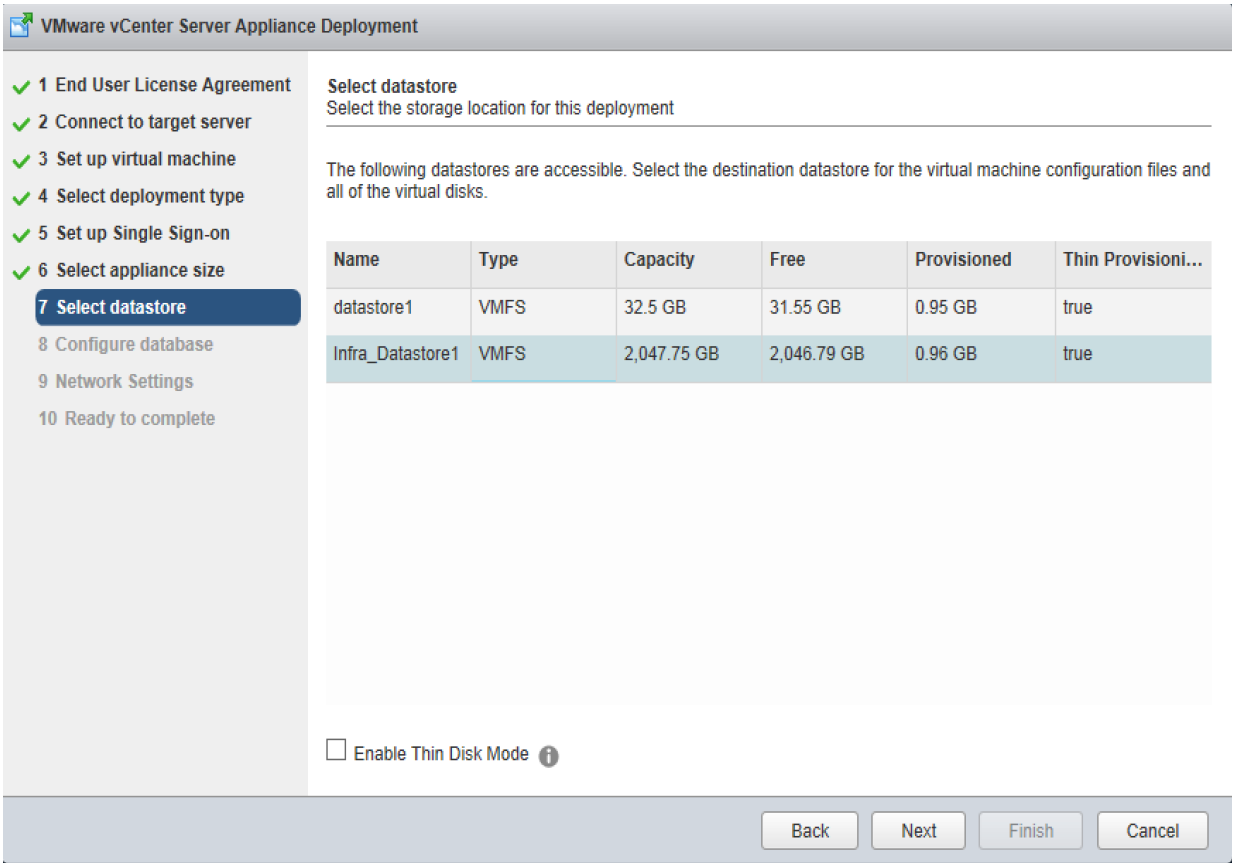
10. Enter the SSO password, Domain name and Site name, Click Next.



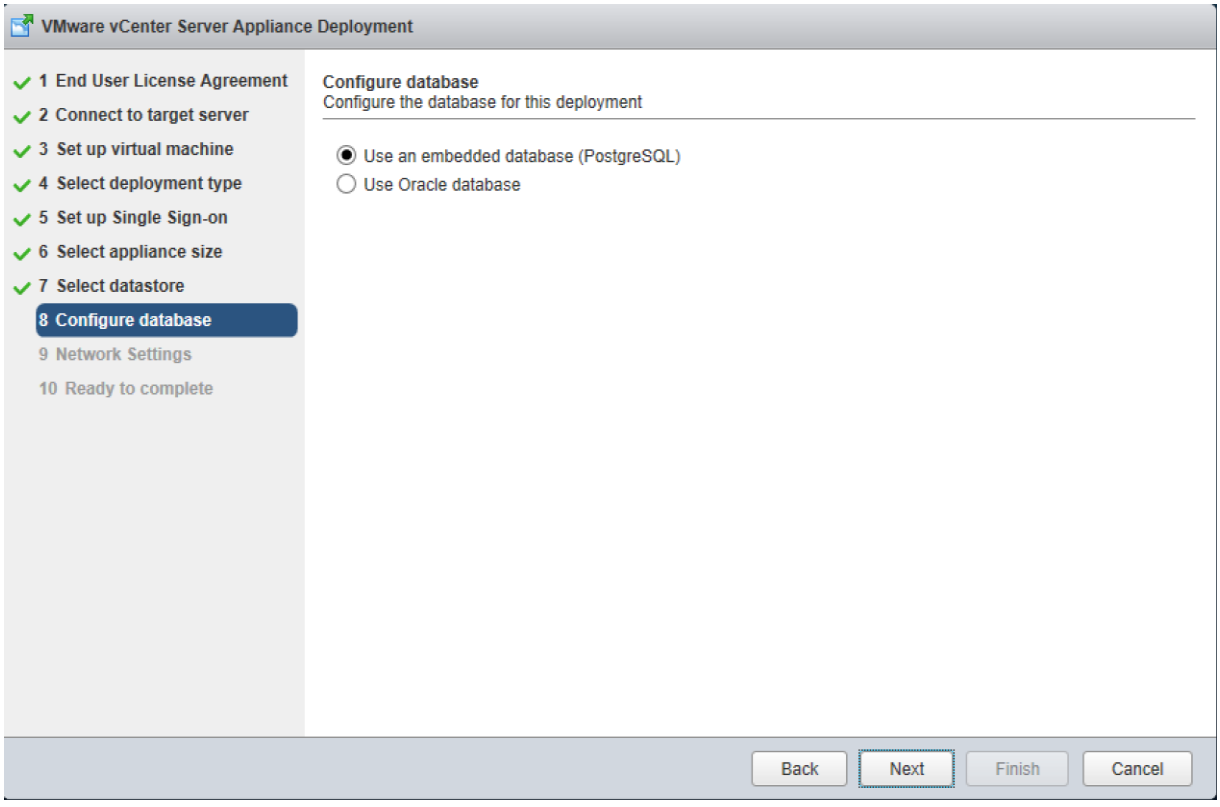
11. In the Select appliance size screen, select the size that matches your deployment, and click Next.



12. In the Select data store screen, select the location for the VM configuration and virtual disks should be stored (`Infra_Datastore1`), and click Next.



13. Select embedded database in the “Configure database” page. Click Next.



14. In the “Network Settings” page, configure the below settings:

    a. Choose a Network: MGMT-Network

    b. IP address family: IPV4

    c. Network type: static

    d. Network address: <<var_vcenter_ip>>

    e. System name: <<var_vcenter_fqdn>>

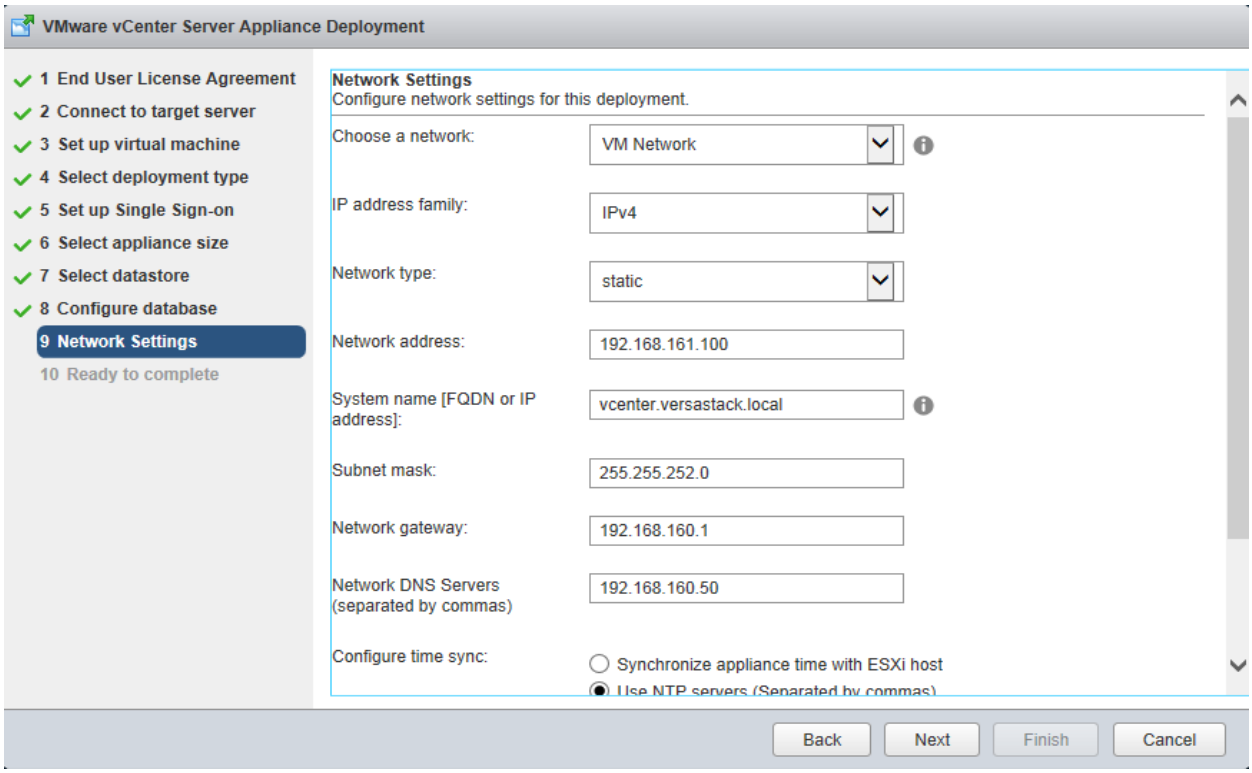
    f. Subnet mask: <<var_vcenter_subnet_mask>>

    g. Network gateway: <<var_vcenter_gateway>>

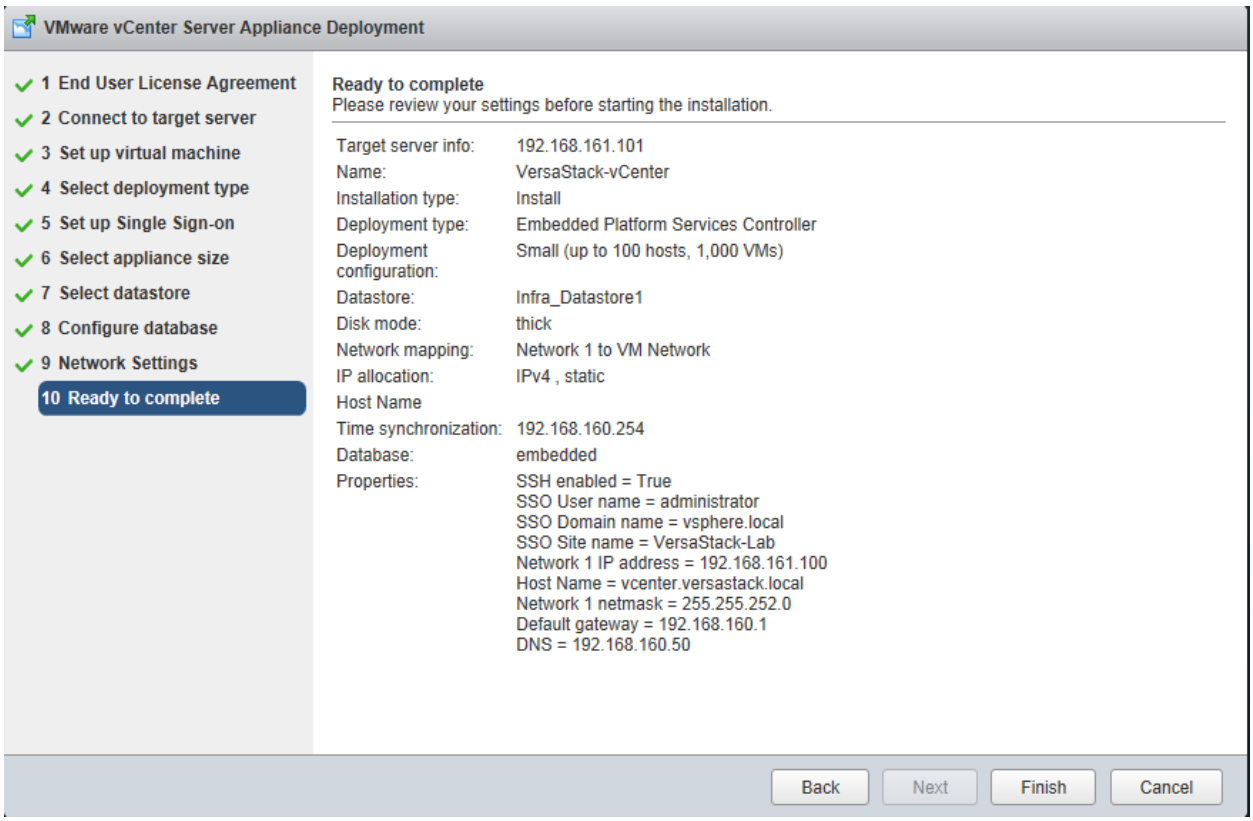
    h. Network DNS Servers: <<var_dns_server>>

    i. Configure time sync: Use NTP servers

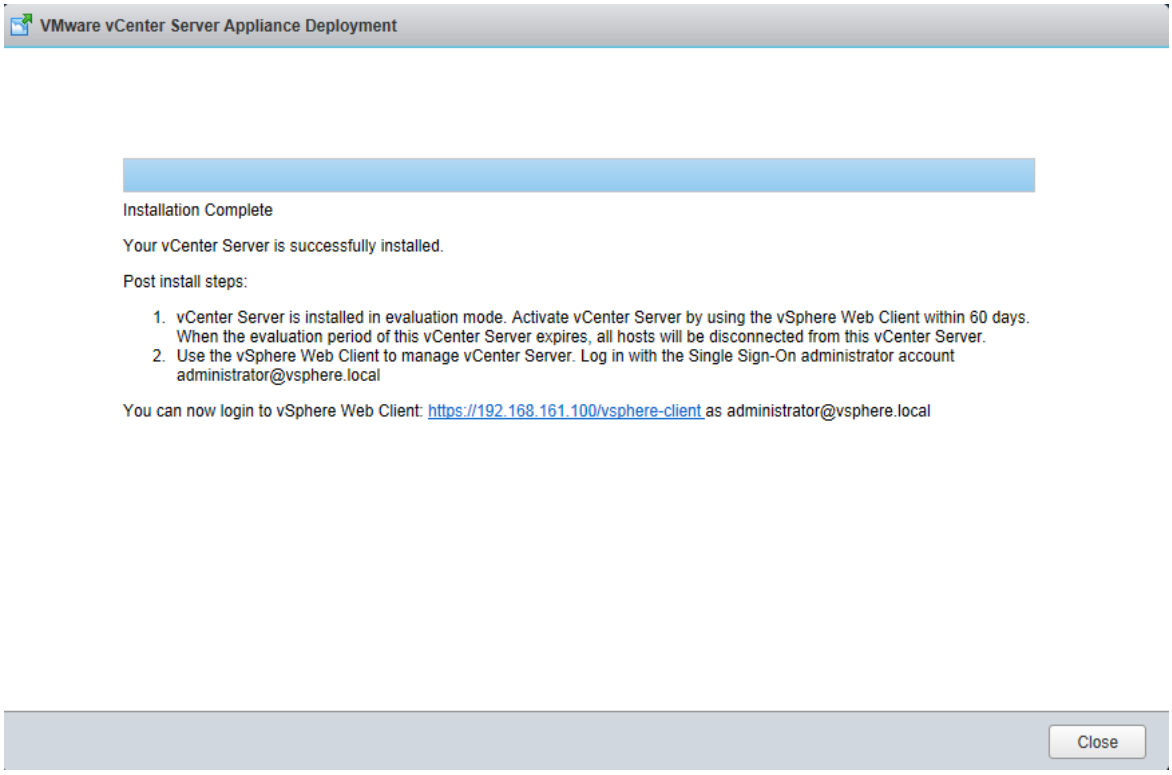
    j. (Optional). Enable SSH



15. In the Ready to complete screen, review the deployment settings for the vCenter Server Appliance, and click Finish to complete the deployment process.



16. The vCenter appliance installation will take few minutes to complete.

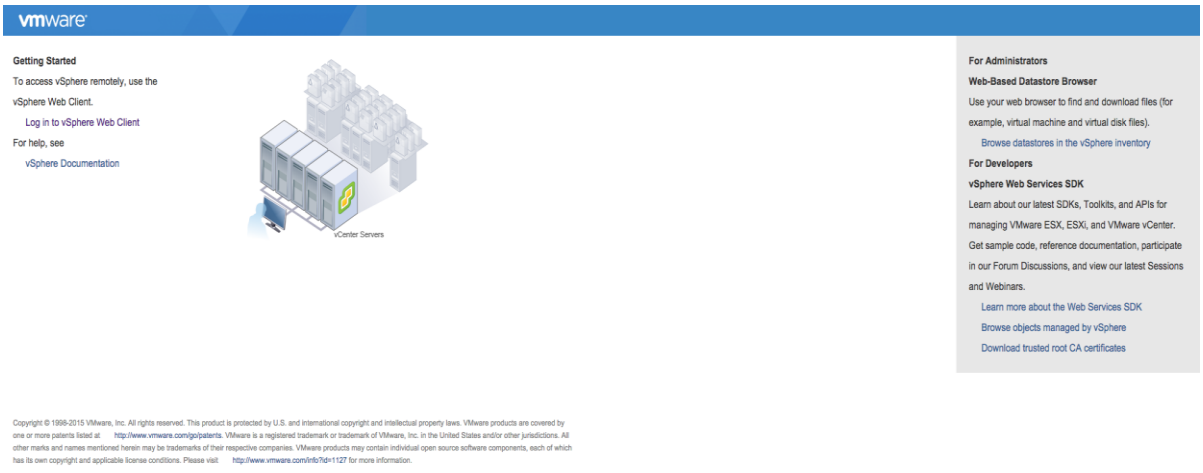


Setup vCenter Server

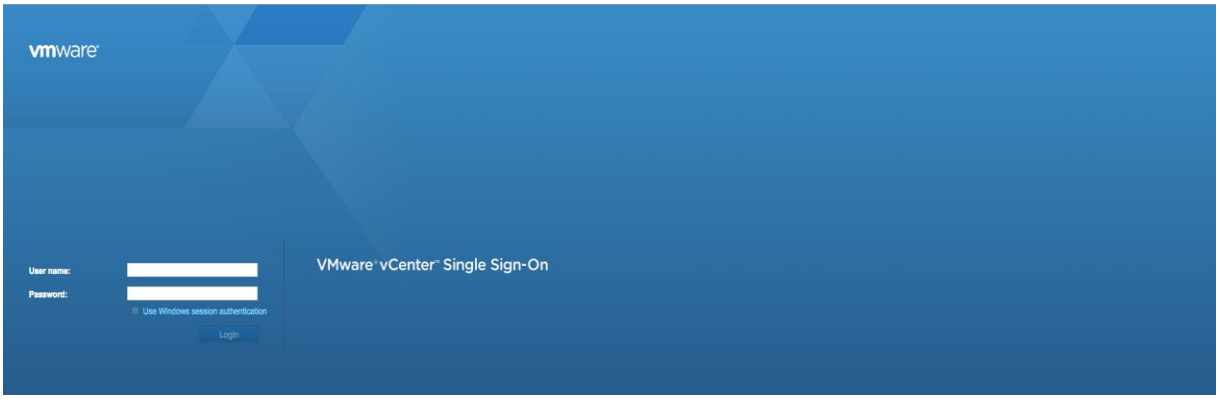
vCenter Server Appliance

To set up the VMware environment, log into the vCenter Server web client.

1. Using a web browser, navigate to vSphere. Click the link labeled Log in to vSphere Web Client.



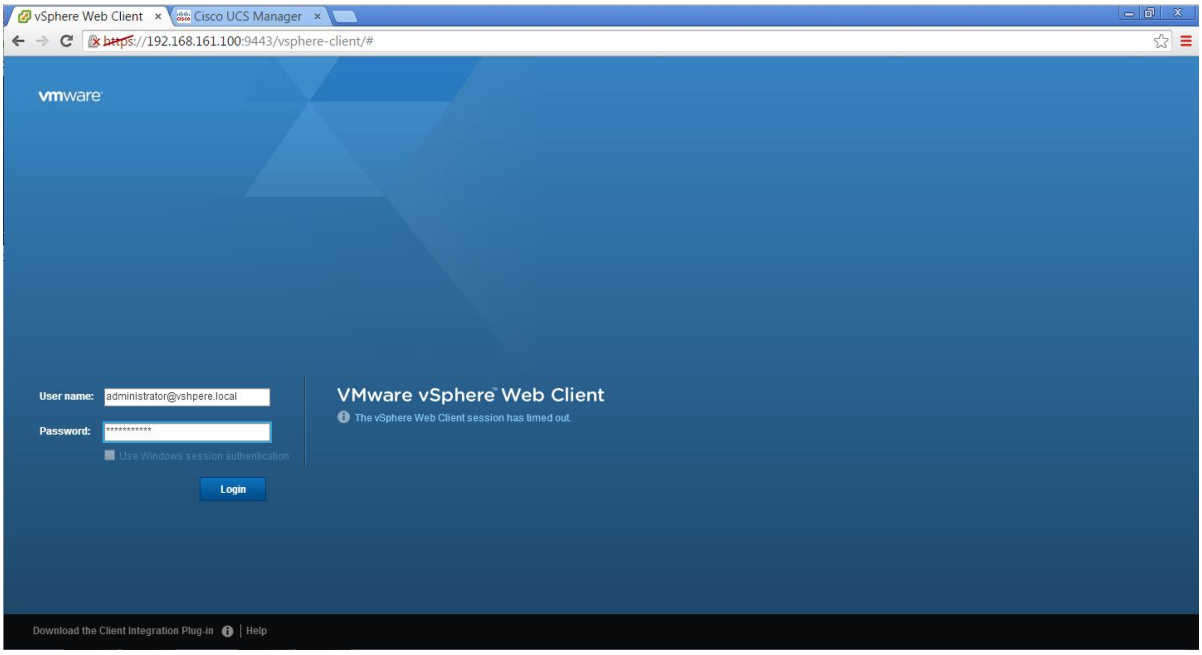
2. If prompted, run the VMWare Remote Console Plug-in.
3. Log in using the root user name and password



4. Click Run.
5. Click Next.
6. Accept the license terms and Click Next.
7. Click Next on Destination Folder window.
8. Click Install.
9. Click Finish.

10. Using a web browser, navigate to https:// <<var_vcenter_server_ip>>:9443/vsphere-client/#

11. In the user name type in administrator@vsphere.local and Password your <<password>.

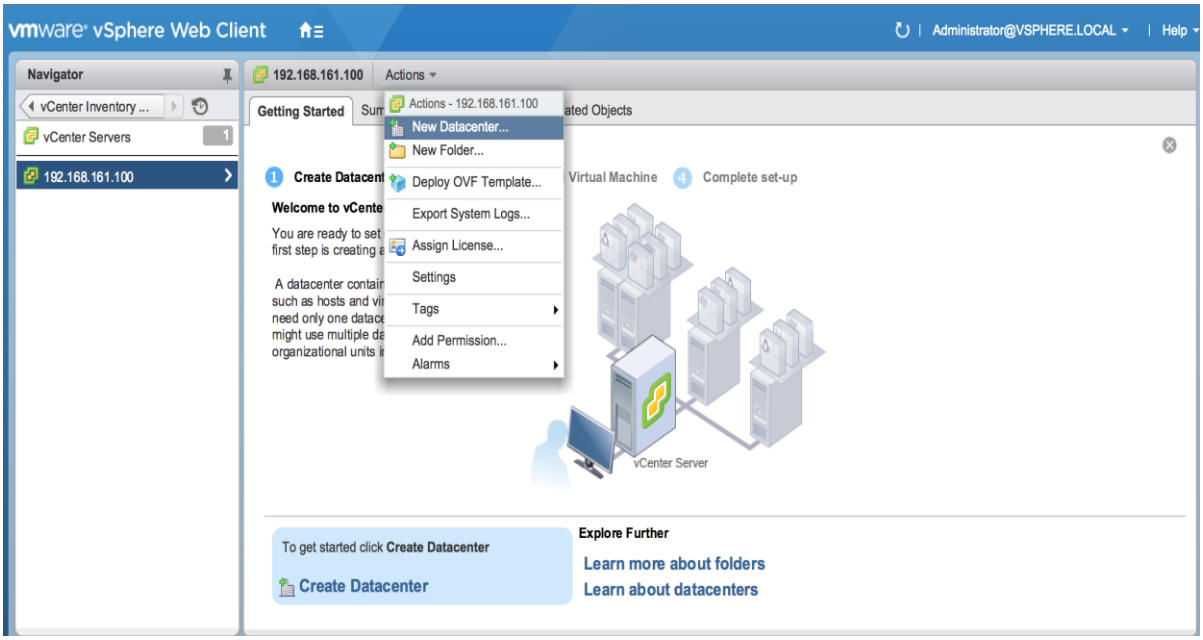


12. Click Login.

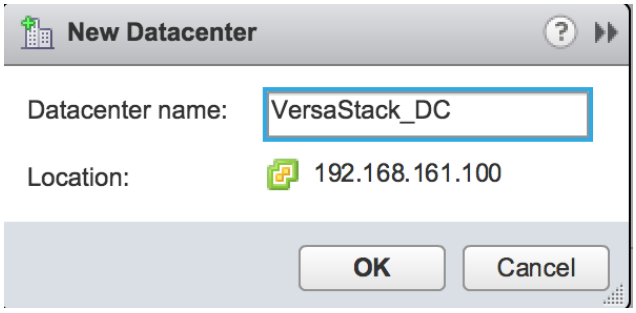
Setup vCenter Server with a Datacenter, Cluster, DRS and HA

To setup the vCenter Server, complete the following steps:

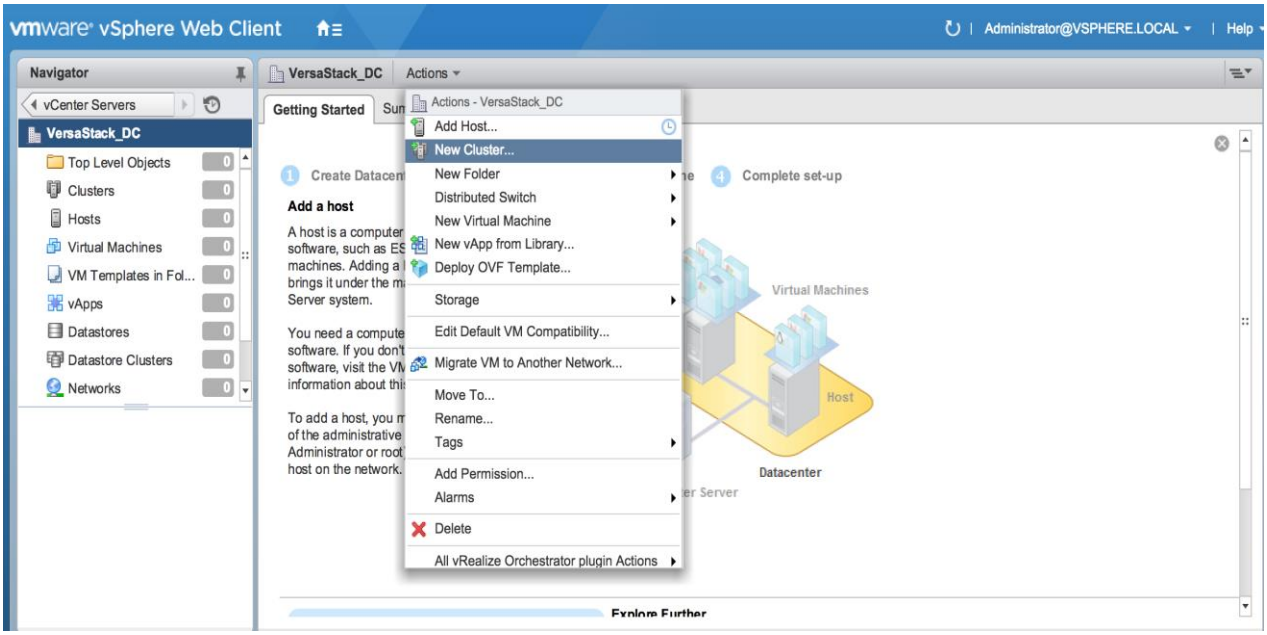
1. In the vSphere Web Client, navigate to the vCenter Inventory Lists > Resources > vCenter Servers.
2. Select the vCenter instance (192.168.161.100).
3. Go to Actions in the toolbar and select New Datacenter from the drop-down.



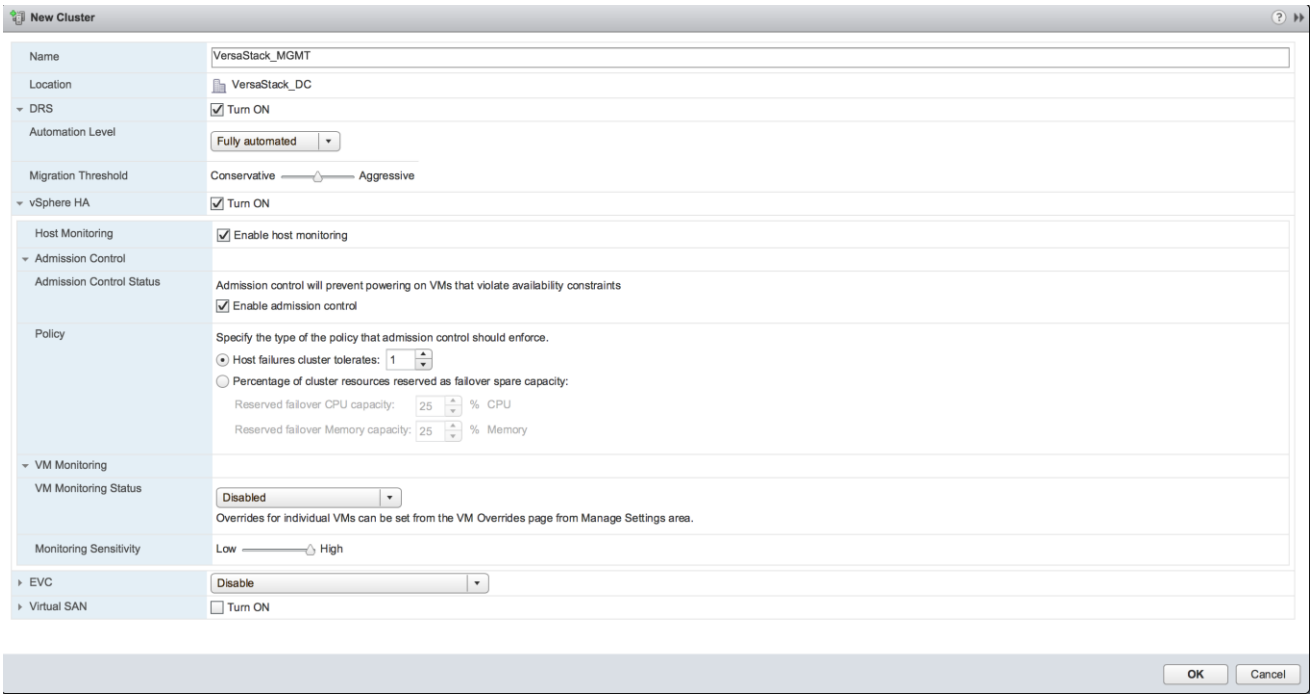
4. Rename the datacenter and click OK.



5. Go to Actions in the toolbar and select New Cluster from the drop-down.



6. In the New Cluster window, provide a cluster name, enable DRS, vSphere HA and Host monitoring.



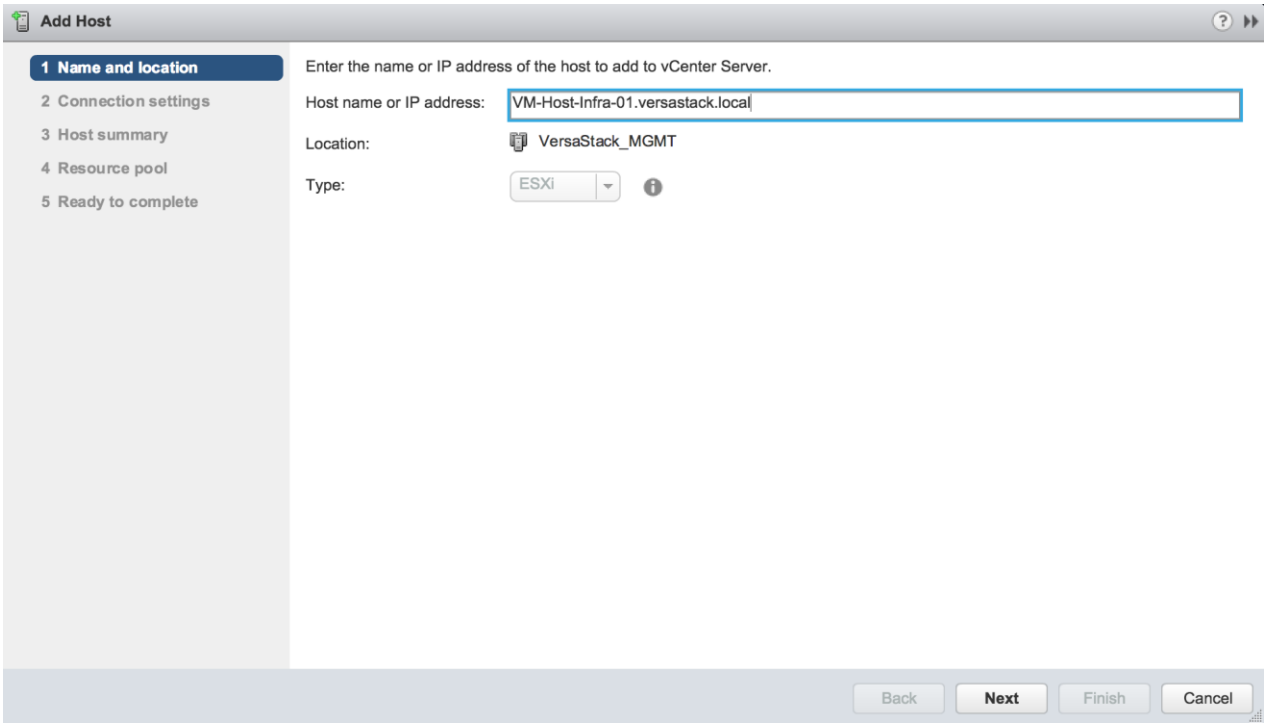
7. Click OK.

Important: If mixing Cisco UCS B or C-Series M2, M3 or M4 servers within a vCenter cluster, it is necessary to enable VMware Enhanced vMotion Compatibility (EVC) mode. For more information about setting up EVC mode, refer to Enhanced vMotion Compatibility (EVC) Processor Support.

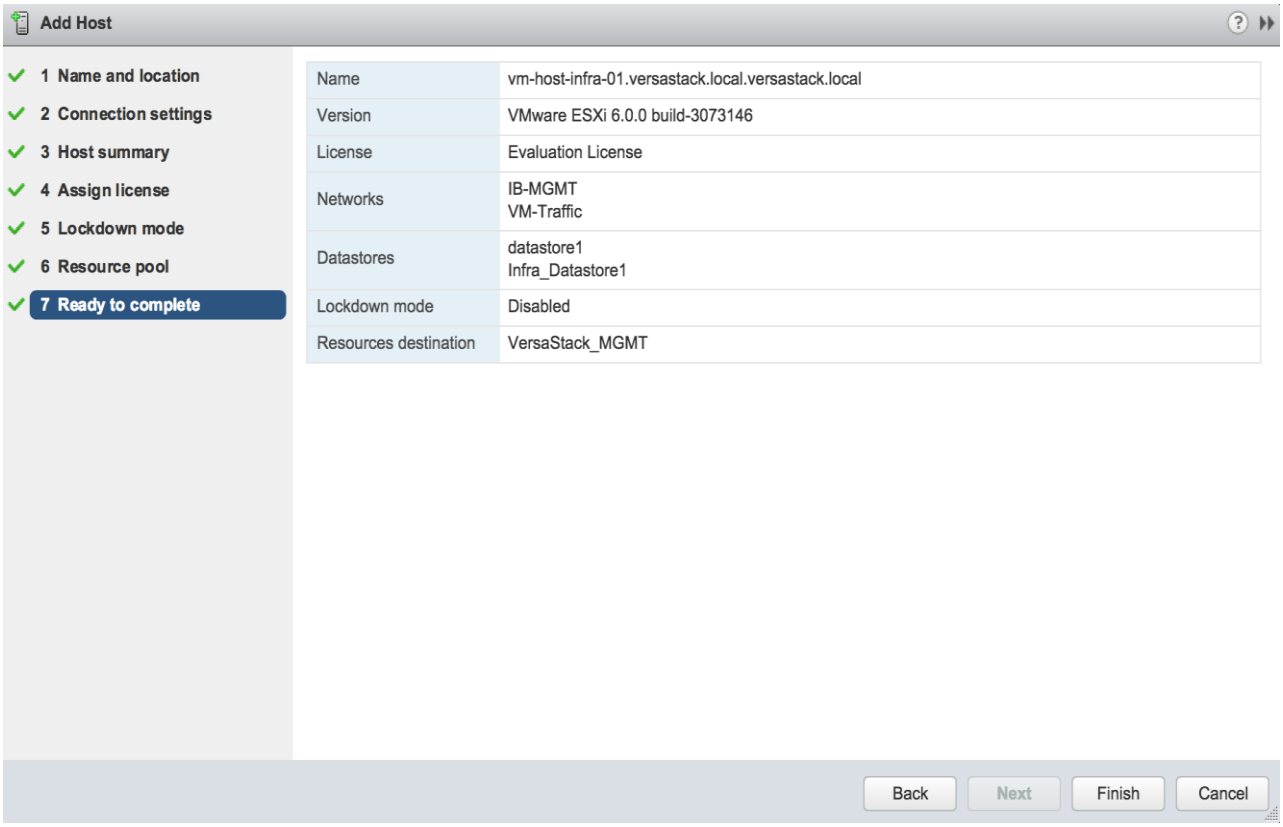
Add Host to Cluster

To add hosts to the Cluster, complete the following steps:

1. Select the newly created cluster in the left pane.
2. Go to Actions in the menu bar and select Add Host from the pull-down menu.
3. In the Add Host window, in the Name and Location screen, provide the IP address or FQDN of the host.



4. In the Connection settings screen, provide the root access credentials for the host.
5. Click Yes to accept the certificate.
6. In the Host summary screen, review the information and click Next.
7. Assign a license key to the host Click Next.
8. (Optional) In the Lockdown Mode screen, to enable/disable remote access for the administrator account after vCenter Server takes control of this host and click Next.
9. In the Resource pool screen, click Next.
10. In the Ready to complete screen, review the summary and click Finish.



11. Repeat this procedure to add other Hosts to the cluster.

12. In vSphere in the left pane right click the cluster `VersaStack_MGMT`, and click Rescan for datastores.

At this point of the install, there is a warning for no network management redundancy. The optional Cisco 1000v virtual switch shown later is this document will remedy that issue. If you are not installing 1000v, you should add the second Cisco network adapter to the VMware standard switch to each ESX hosts by clicking on the configuration tab, and in the hardware 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.

ESXi Dump Collector Setup

ESXi hosts need to be configured to do core dumps to the ESXi Dump Collector that is part of vCenter. The Dump Collector is not enabled by default on the vCenter Appliance. To setup the ESXi Dump Collector, complete the following steps:

1. In the vSphere web client, select Home.
2. In the center pane, click System Configuration.
3. In the left hand pane, under Services, click VMware vSphere ESXi Dump Collector.
4. In the Actions menu, choose Start.
5. In the Actions menu, click Edit Startup Type.

6. Select Automatic.
7. Click OK.
8. On the Management Workstation, open the VMware vSphere CLI command prompt.
9. Set each SAN-booted ESXi Host to coredump to the ESXi Dump Collector by running the following commands, repeat the commands for ESXi hosts 3 and 4:

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

To get the host thumbprint, type the command without the --thumbprint option, then copy and paste the thumbprint into the command.

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

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

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

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

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

Setup 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).

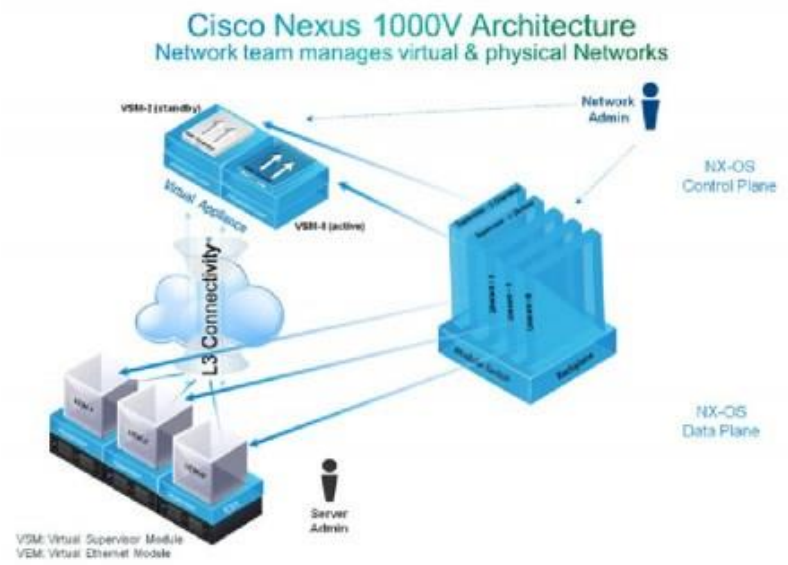
The Cisco Nexus 1000V has the following components:

- 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 8 illustrates the Cisco Nexus 1000V architecture.

Figure 8 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.

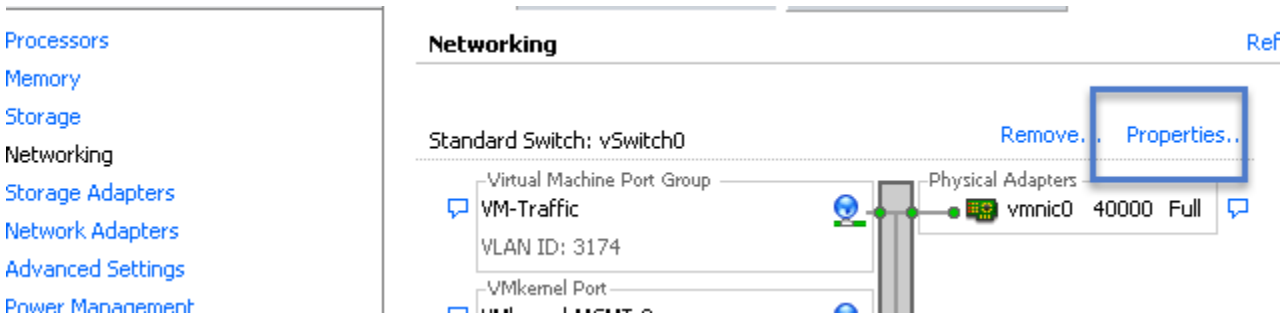
Installation Process

To create network redundancy for the migration, create a temporary VMkernel, and complete the following steps:

ESXi Host VM-Host-Infra-01

Repeat steps 1-11 in this section for all 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.

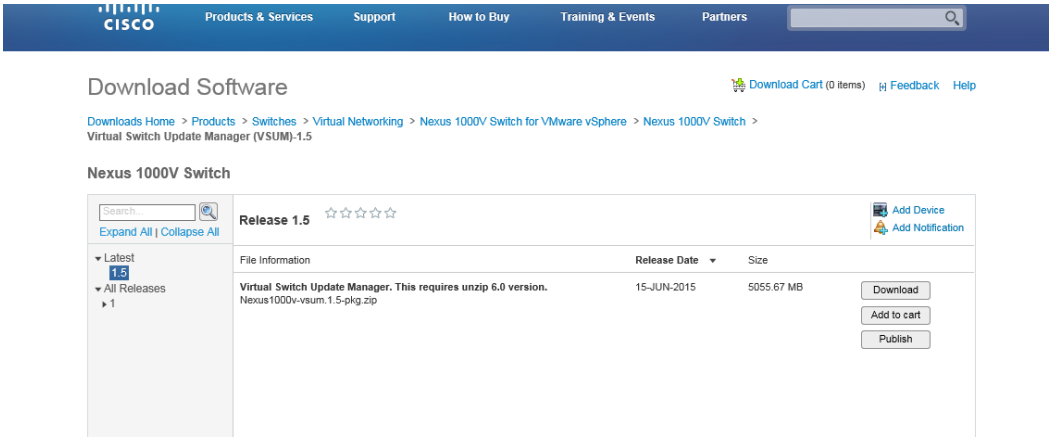


4. Click Add
5. Select VMkernel and click Next.
6. Change the network label to `VMkernel-MGMT-2` and enter `<<var_ib-mgmt_vlan_id>>` in the VLAN ID (Optional) field.
7. Select Use this port group for management traffic
8. Click Next to continue with the VMkernel creation.
9. Enter the IP address `<<var_vmhost_infra_01_2nd_ip>>` 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

To deploy the OVF template, complete the following the steps:

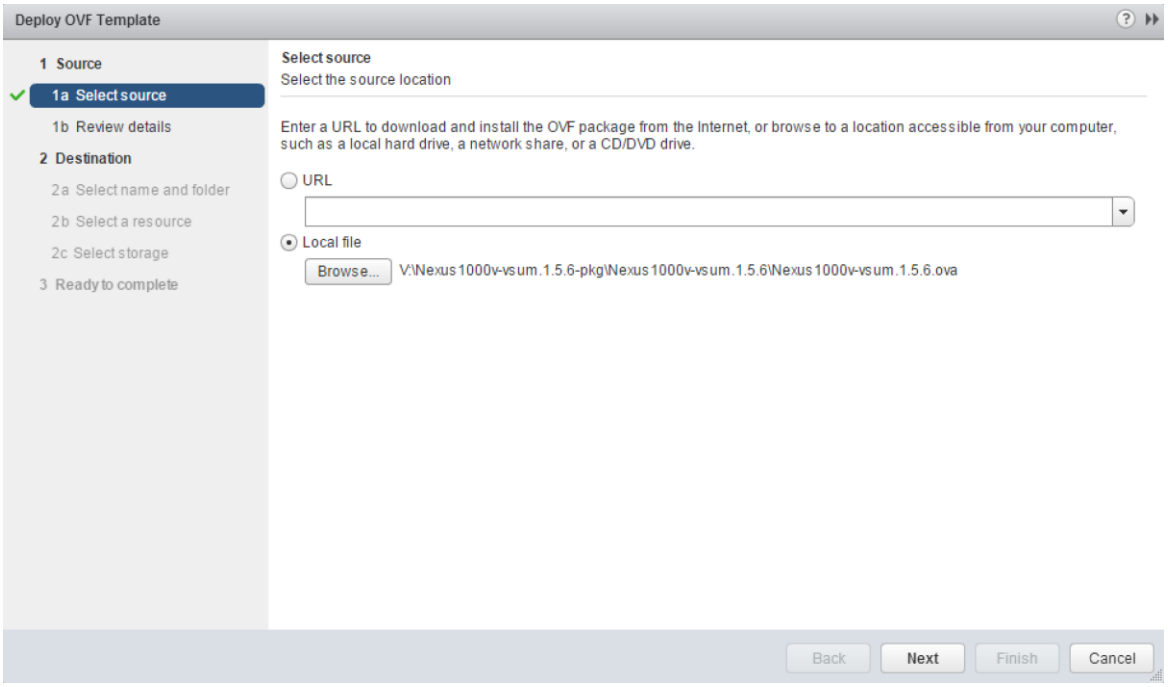
1. Log in and Download the Cisco Nexus 1000V installation software from www.cisco.com.



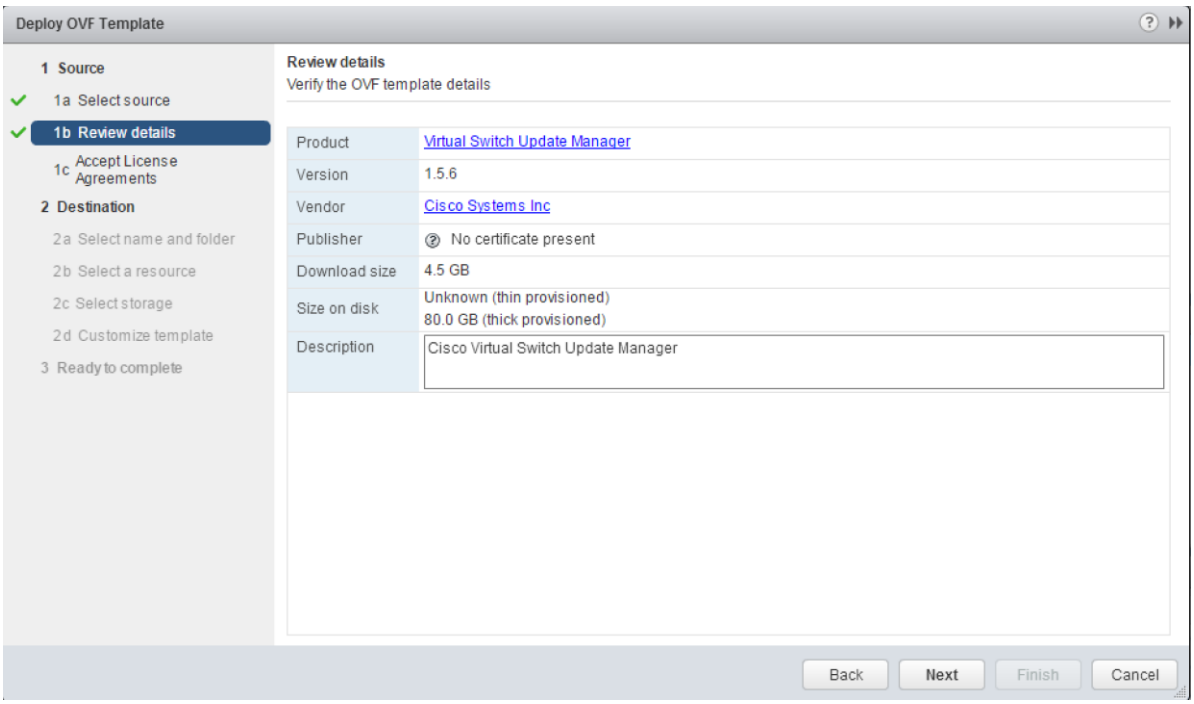
2. Unzip the package contents and validate you can view the ova file.
3. From the vSphere client, click File, Deploy OVF Template and browse to the unzipped ova file.

4. From the vSphere Web Client, Select Hosts and Clusters > Actions > Deploy OVF Template.

5. Specify the source location as Local File and browse to the OVA file location.



6. Click Next, then click Next again.



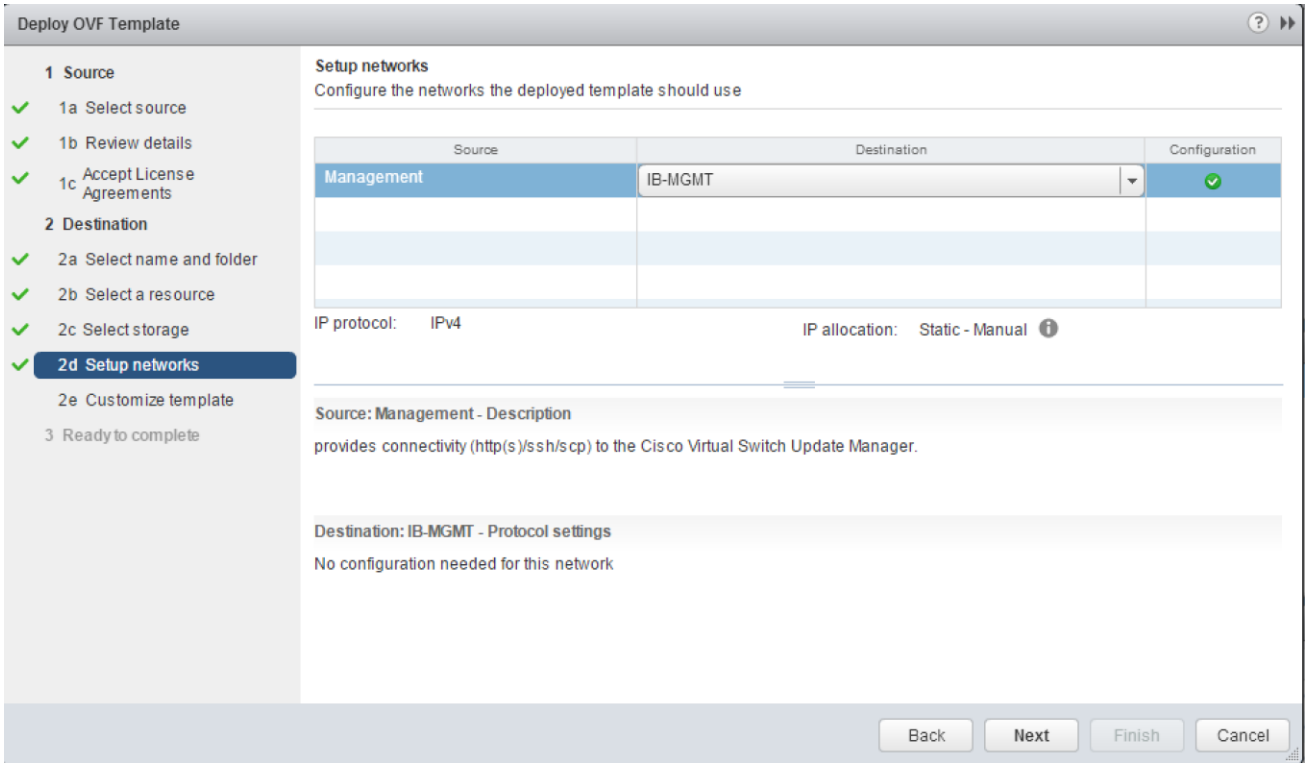
7. Review the license agreement. Accept and Click Next.

8. Click Next on the Select name and folder screen.

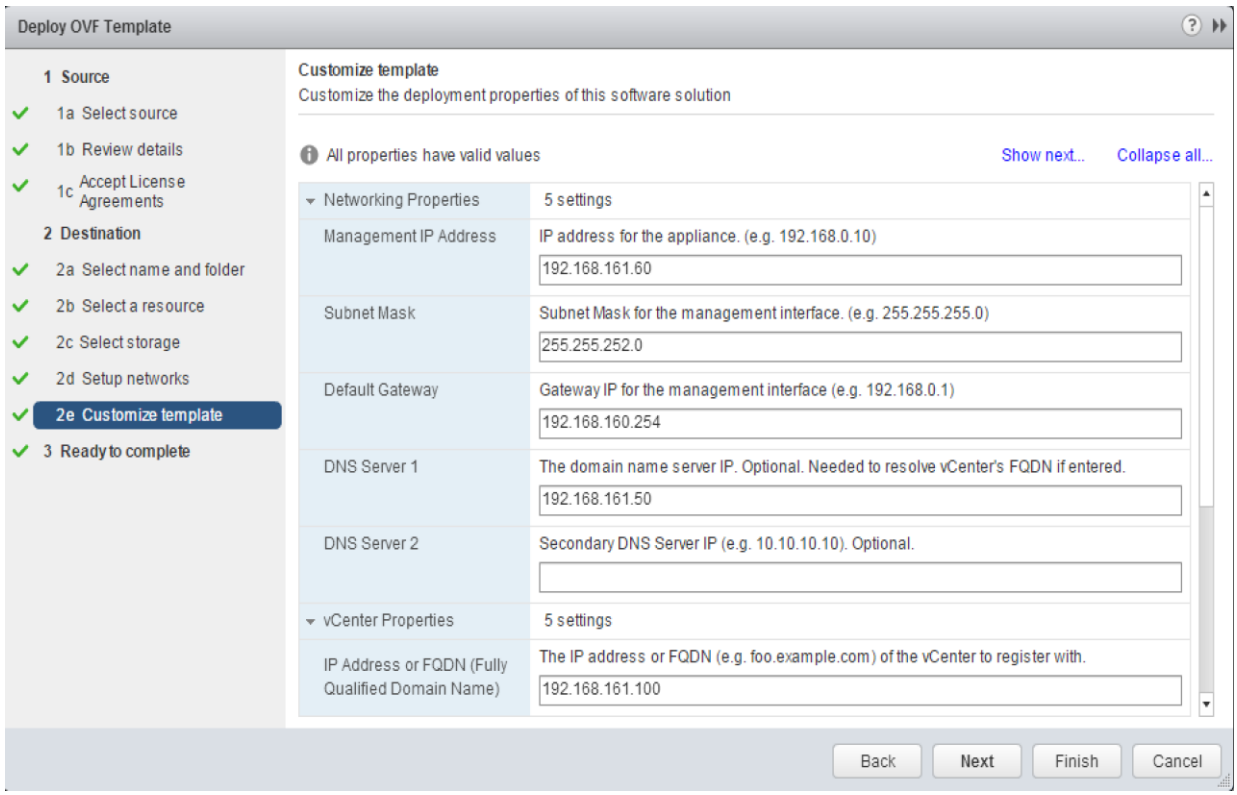
9. Select `VersaStack_MGMT` cluster on the Select a resource screen.

10. Select `infra_datastore_1` as the Datastore and click Next, leave the other options as default.

11. Make sure you have Management Mapped to `IB-Mgmt` in the Setup networks screen and click Next.

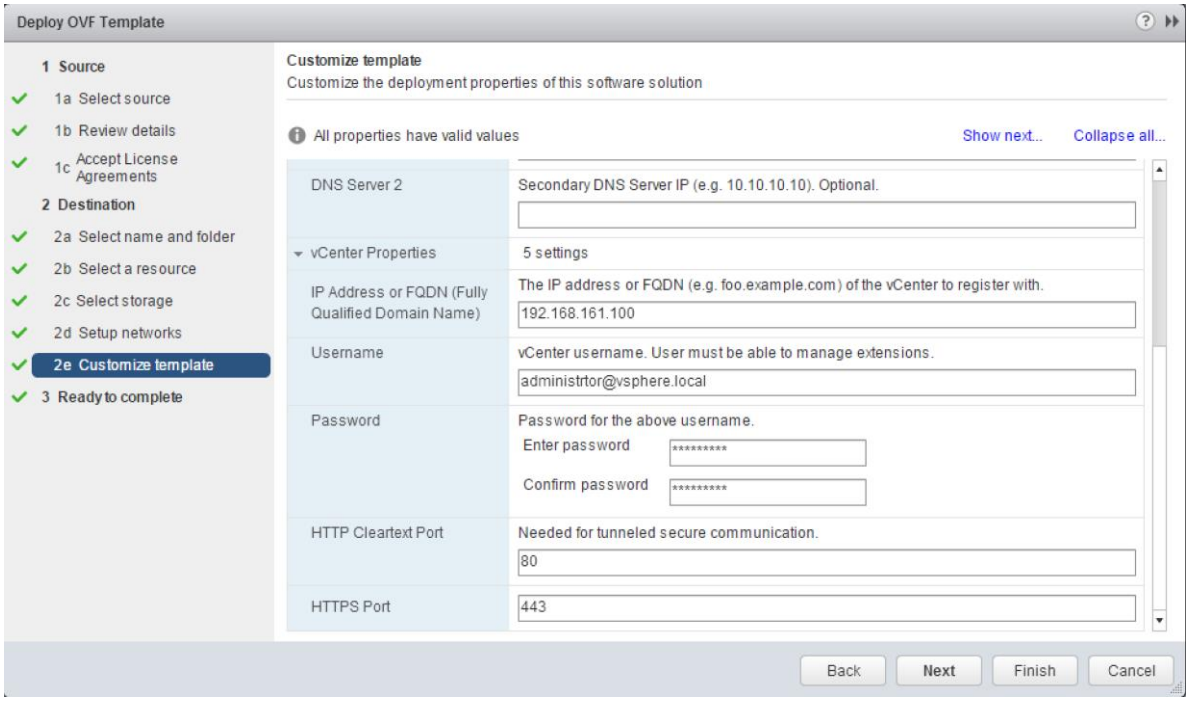


12. On the Properties screen, input `<<var_vsm_updatemgr_mgmt_ip>>, <<var_vsm_mgmt_mask>> <<var_vsm_mgmt_gateway>>, <<var_nameserver_ip>>.`

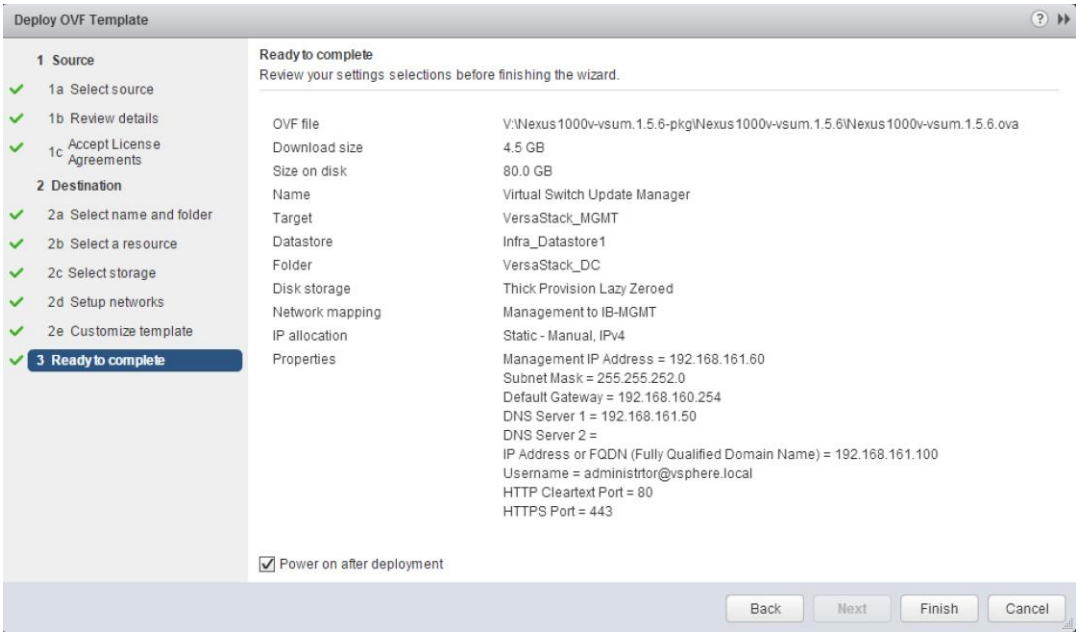


13. Enter the vCenter IP and login information. For domain accounts, use the Administrator@Vsphere.local login format and do not use domainname\user account format.

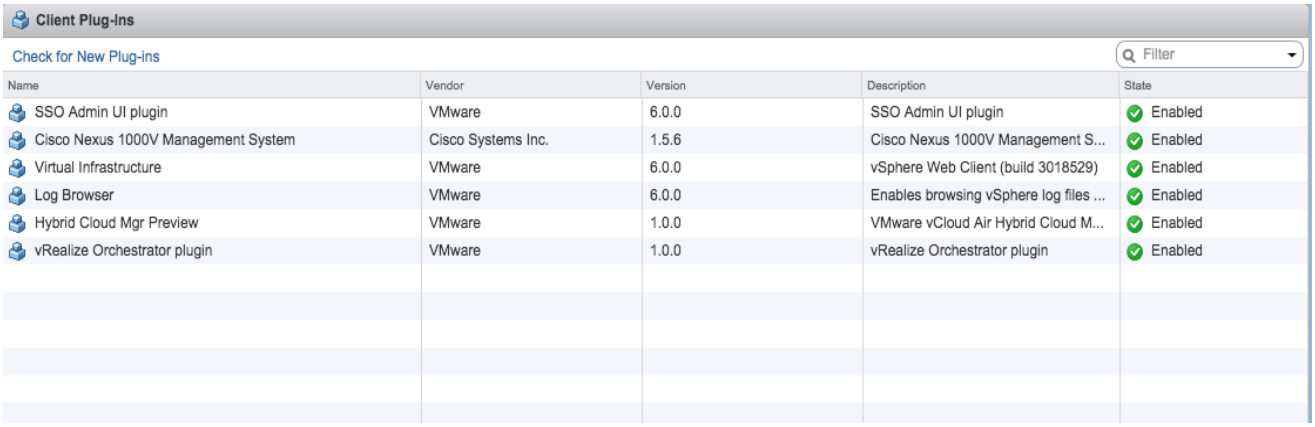
14. Accept default ports, and click Next.



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



16. After the VM boots in a few minute the Plugin is registered. Validate the plugin in the vSphere web client by clicking Client Plug-ins from the Administration window in Navigator pane.



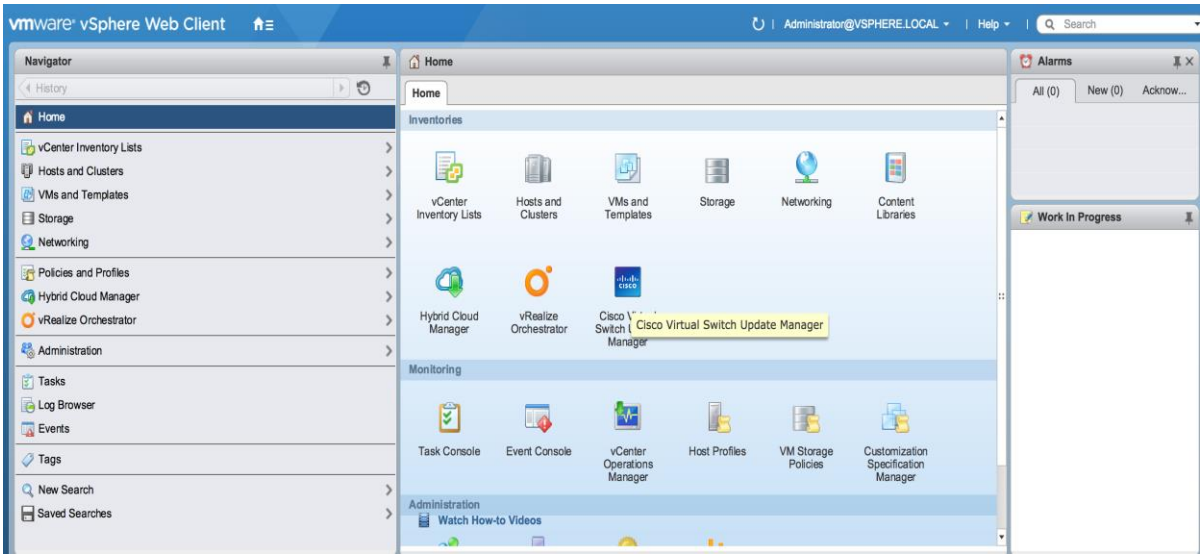
Install the VSM through the Cisco Virtual Switch Update Manager

The VSUM will deploy the VSM primary and secondary to the ESXi hosts through the GUI install. You will have a VSM primary 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:

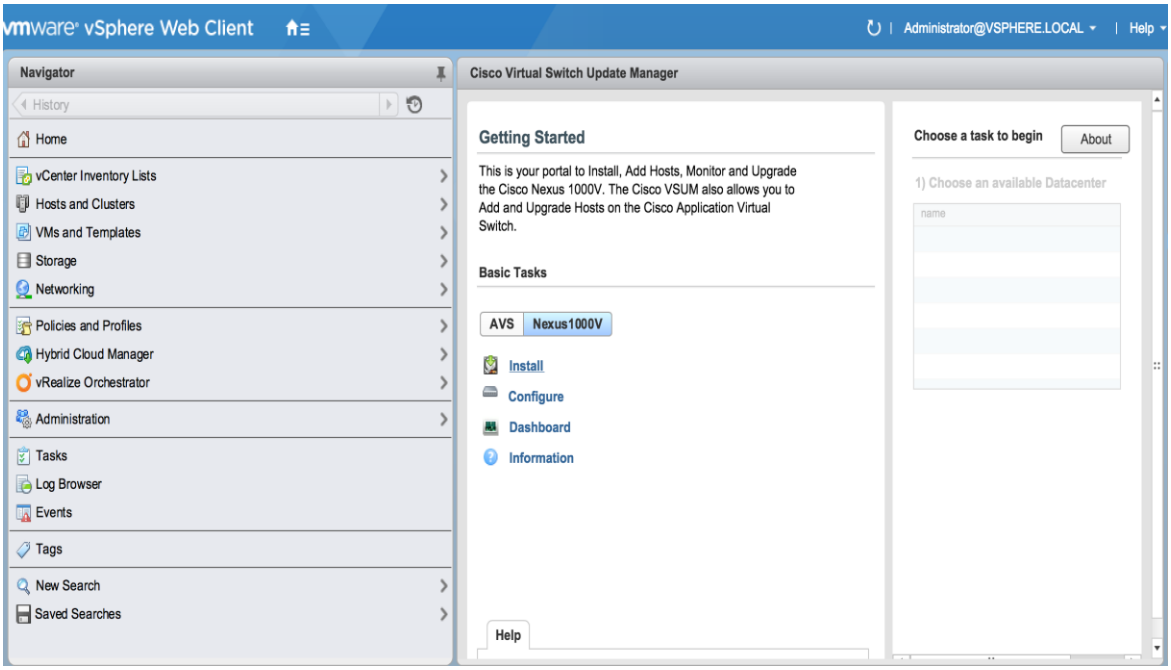
On the machine where you will run the browser for the VMware vSphere Web Client, you should have installed Adobe Flash as well the Client Integration plugin for the web client. The plug-in can be downloaded from the lower left corner of the web client login page.

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

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

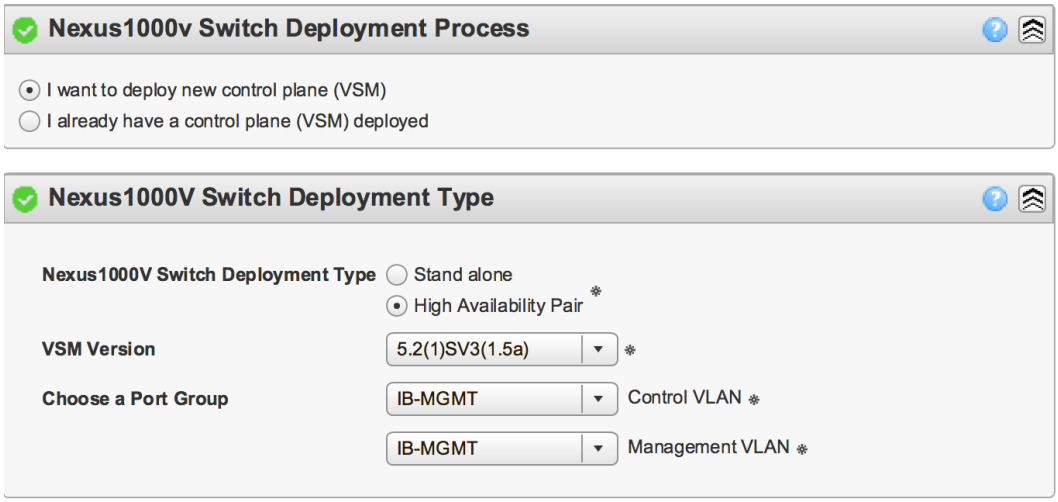


3. Click Cisco Nexus 1000V button then click Install.

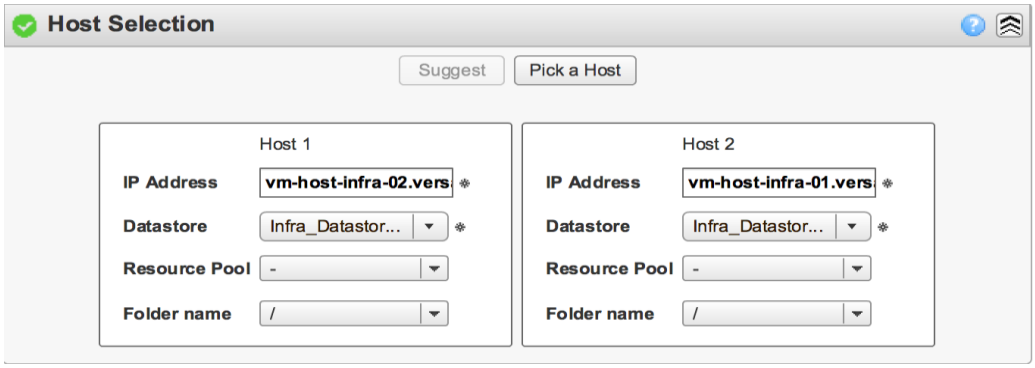


4. Click the `VersaStack_DC` datacenter in the right screen.

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

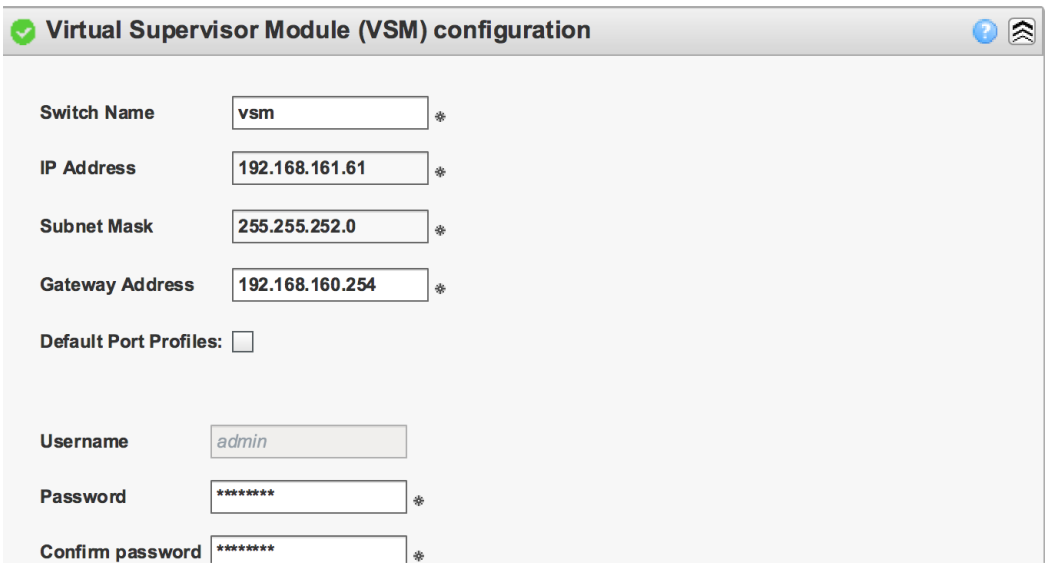


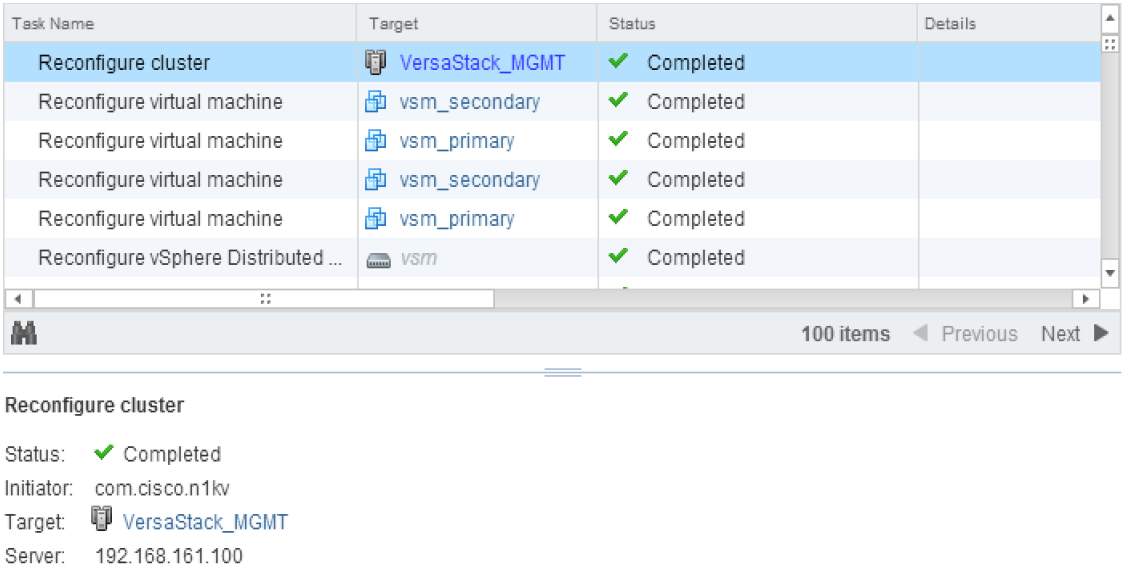
6. For the Host Selection, click the Suggest button and choose the Datastores.



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 step:

Use an SSH client, log in to the primary Cisco Nexus 1000V VSM as admin.

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
```

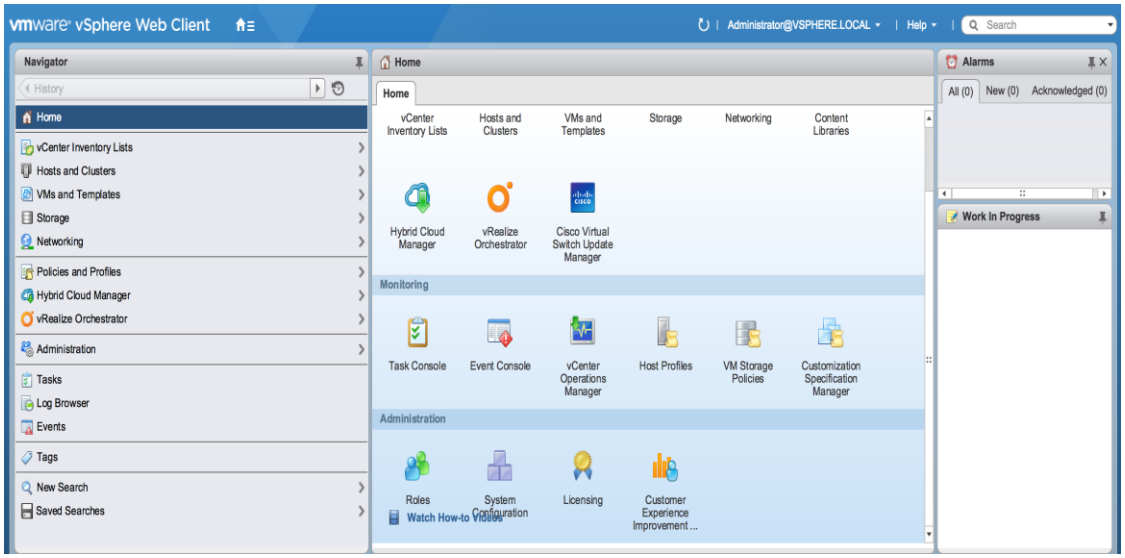
```
switchport access vlan <<var_ib-mgmt_vlan_id>>
no shutdown
system vlan <<var_ib-mgmt_vlan_id>>
state enabled
exit

copy run start
```

Migrate Networking Components for ESXi Hosts to Cisco Nexus 1000V

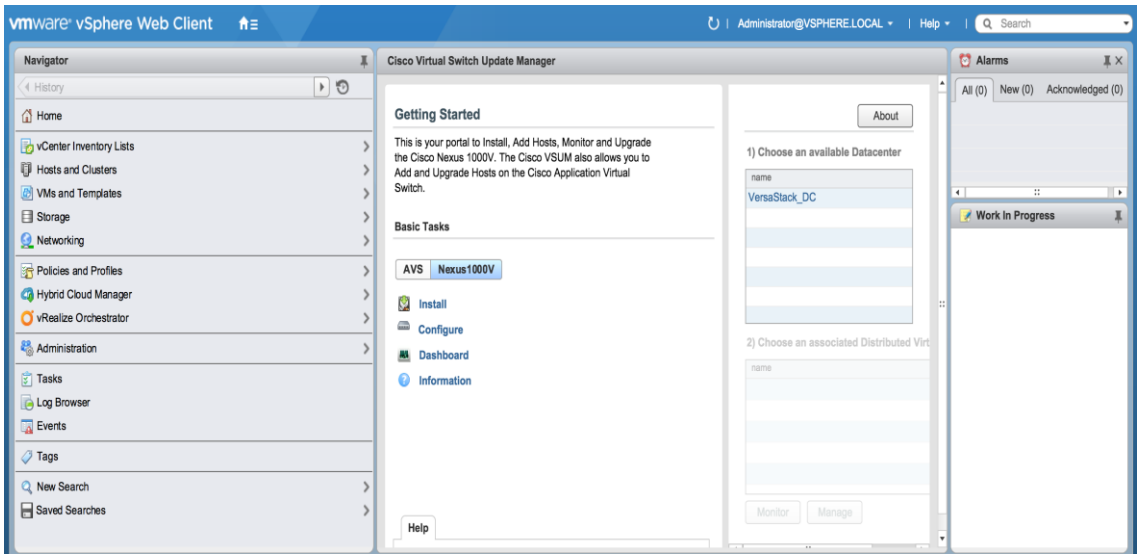
vSphere Client Connect to vCenter

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

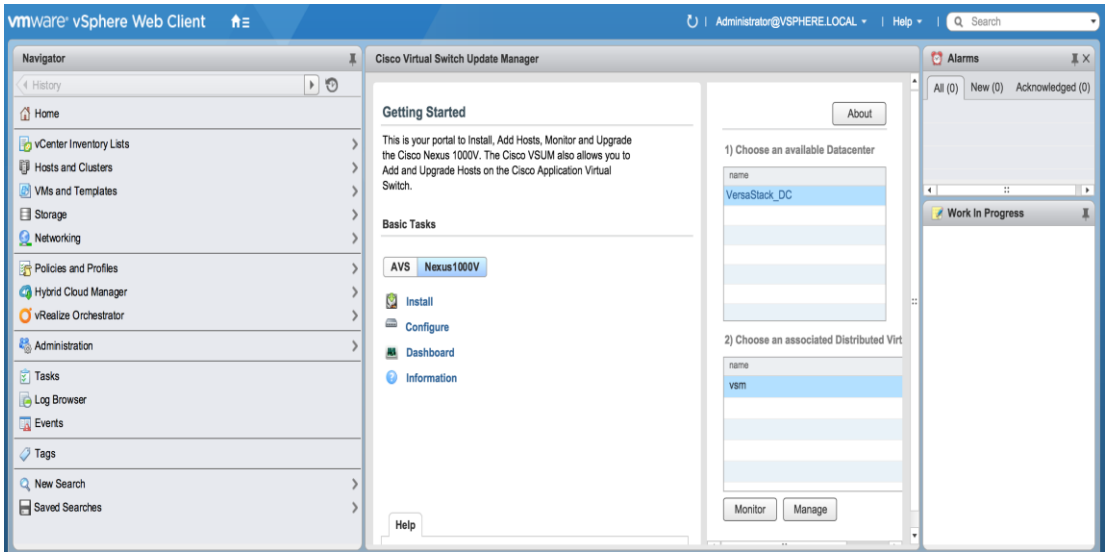
1. In the vSphere web client, click the Home tab and click the Cisco Virtual Switch Update Manager.



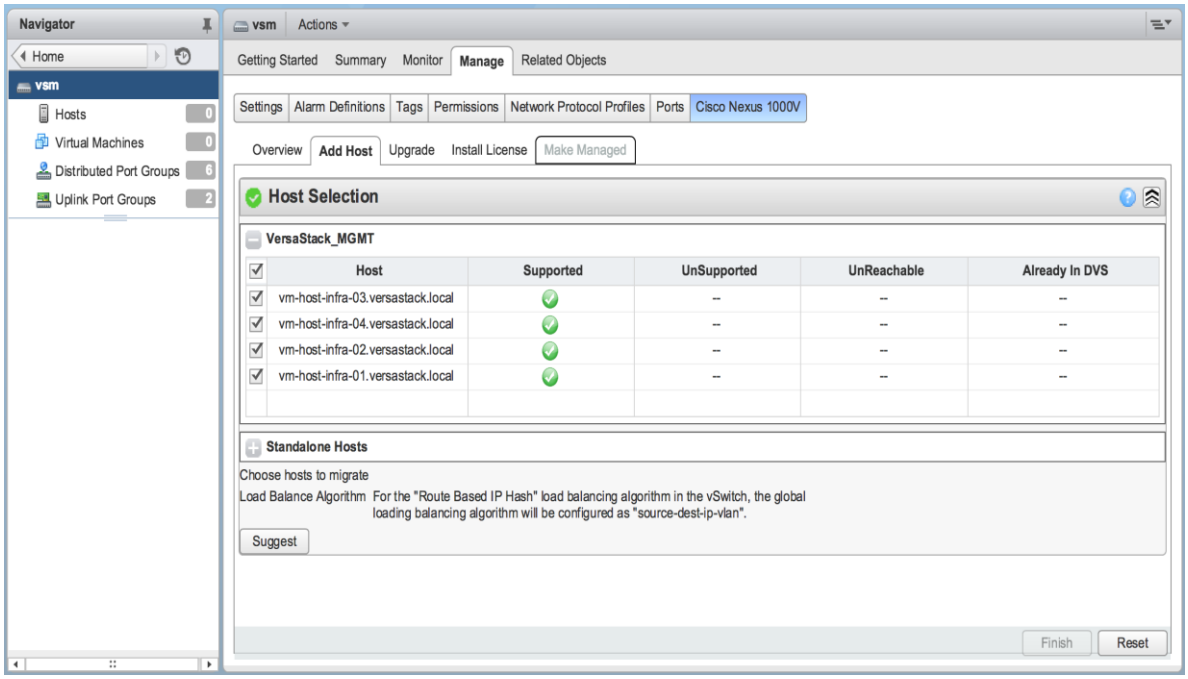
2. Click the Cisco Nexus 1000v and click Configure.



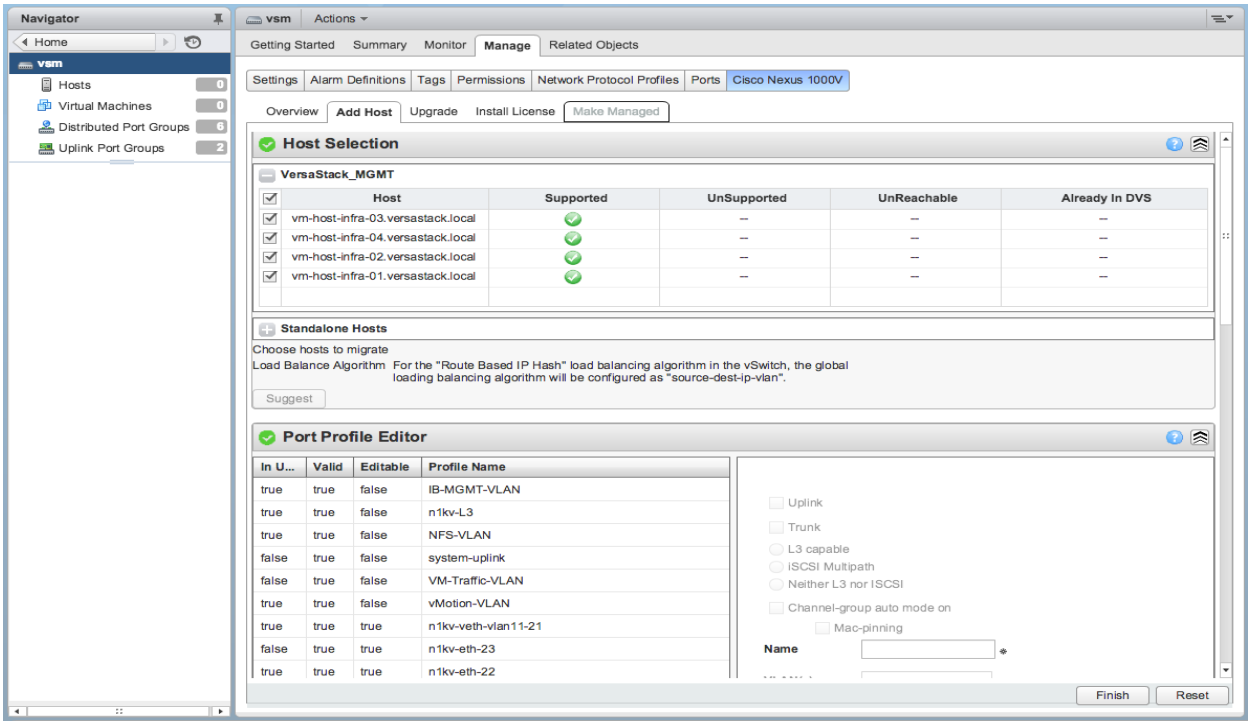
3. Click Datacenter, then click Distributed Virtual Switch and select Manage.



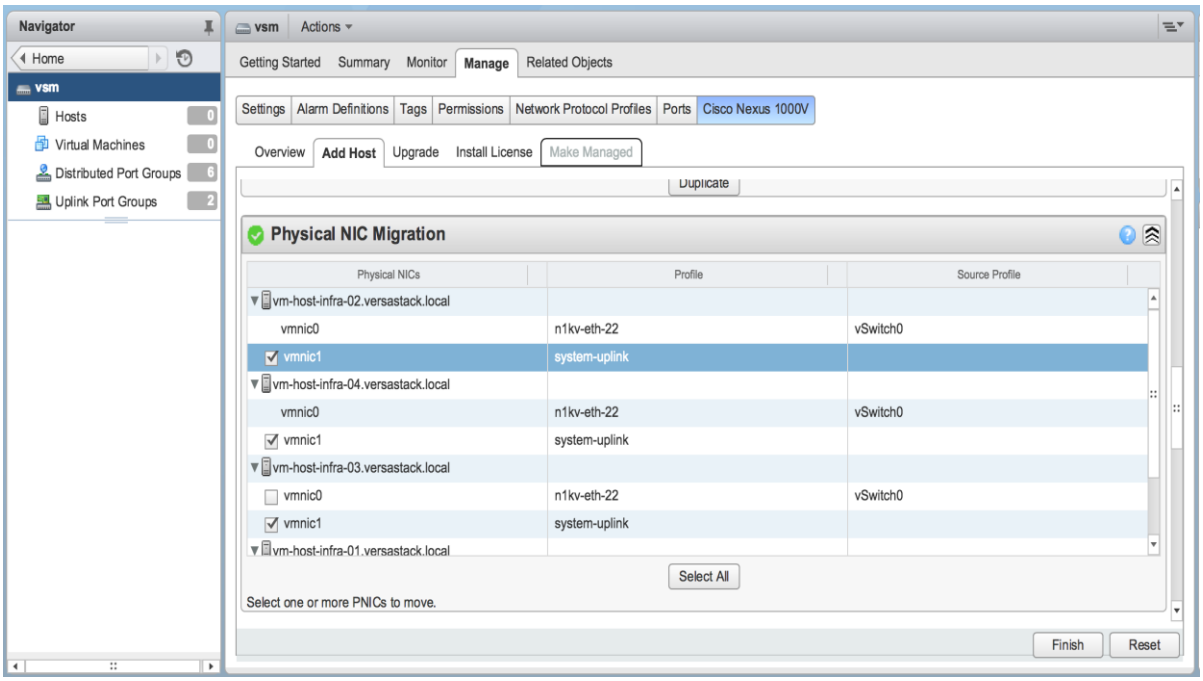
4. Click Add Host tab then select the plus sign next to `VersaStack_MGMT`, then click the top check box to all Hosts.



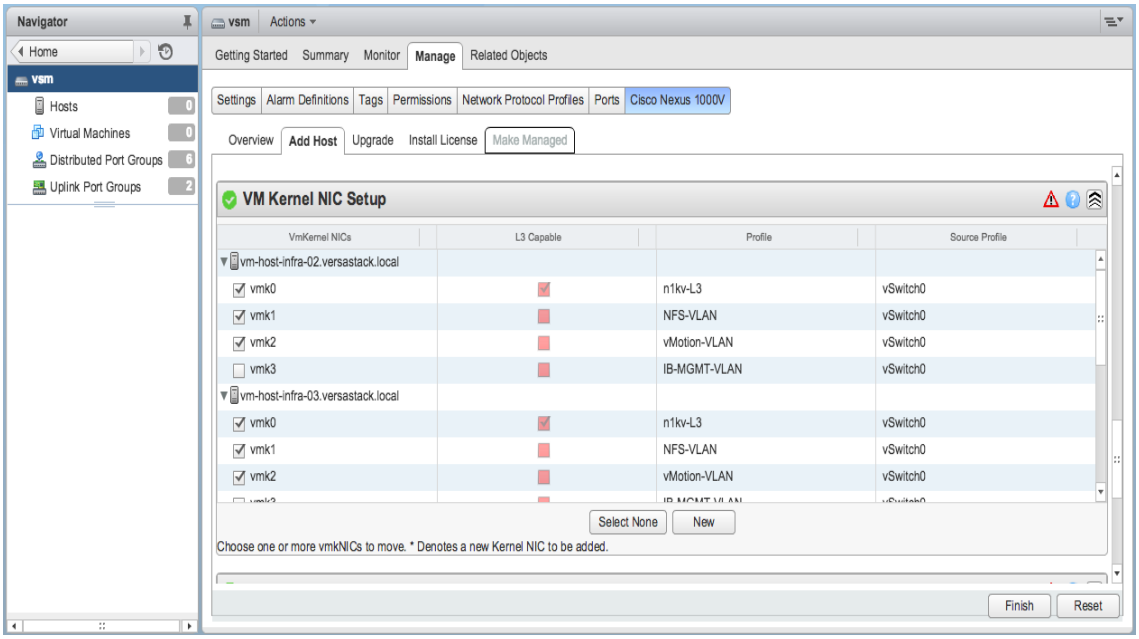
5. Click Suggest.



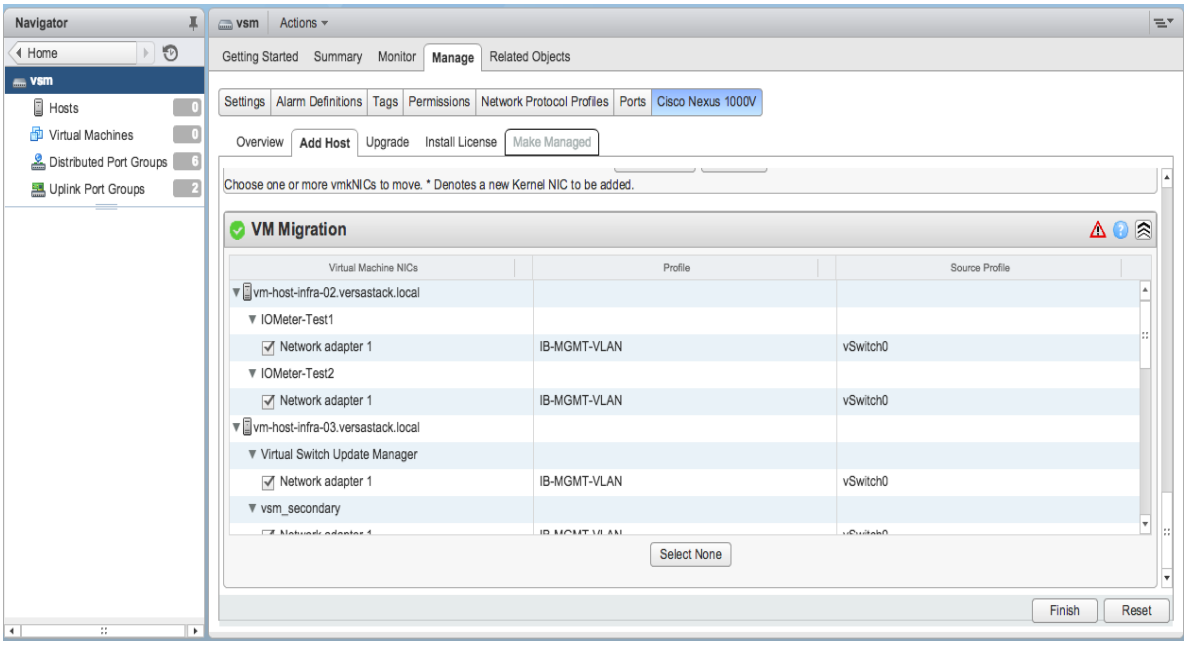
6. Select the Physical NIC Migration, and select the Unused NIC `vmnic1` for migration. Select system uplink in the middle pane.



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

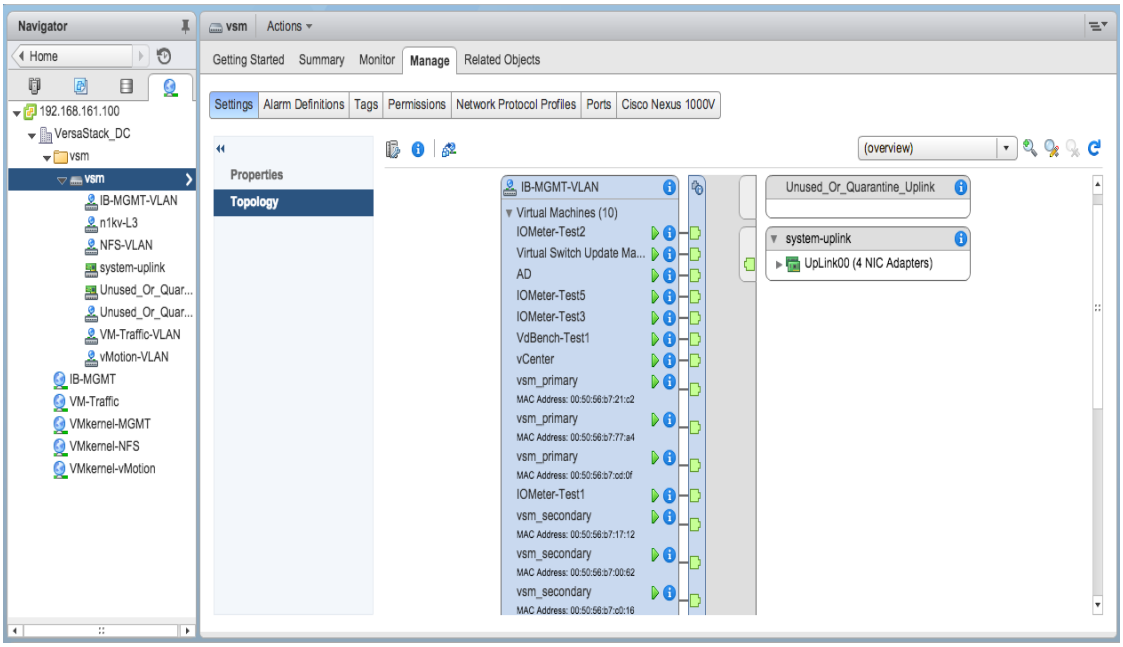


8. For VM migration click button next to the virtual machine to expand the target profile and chose the correct profile, which should be `IB-MGMT-VLAN`. Repeat this for each Virtual Machine.



9. Click Finish.

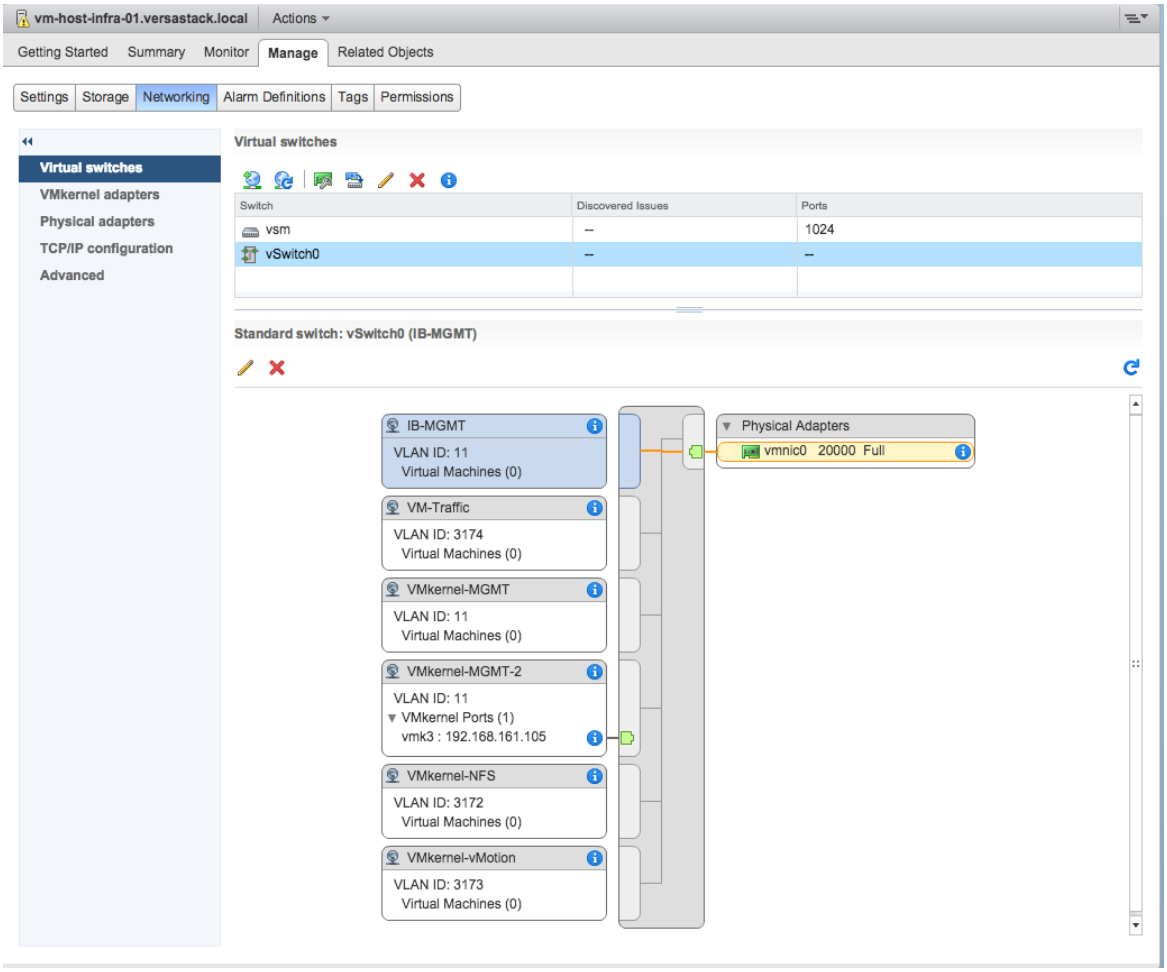
10. When the migration completes, click Settings then click Topology and expand the virtual machines to view the network connections.



Migrate ESXi Host Redundant Network Ports to Cisco Nexus 1000V

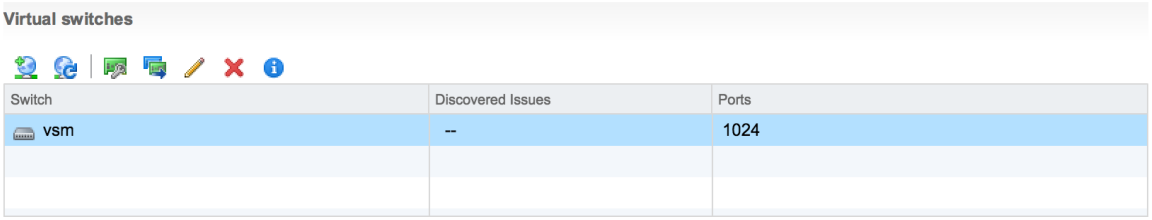
To migrate the ESXi host redundant network ports, complete the following steps:

1. In the VMware vSphere Web Client window, select Home > Hosts and Clusters.
2. On the left expand the Datacenter and cluster, and select the first VMware ESXi host.
3. In the center pane, select the Manage tab, and then select Networking.
4. Select `vSwitch0`. All of the port groups on vSwitch0 should be empty. Click the x mark in red under Virtual switches to delete `vSwitch0`.



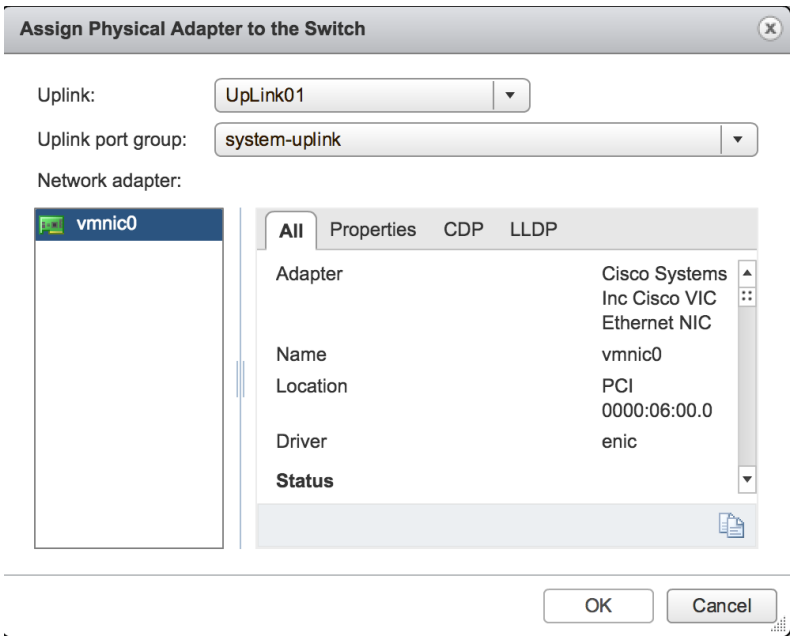
5. Click Yes to remove `vSwitch0`. It may be necessary to refresh the Web Client to see the deletion.

6. The Cisco Nexus 1000V VSM should now be the only virtual switch. Select it and select the third icon above it under Virtual switches (Manage the physical network adapters connected to the selected switch).



7. Click the plus mark in green to add an adapter.

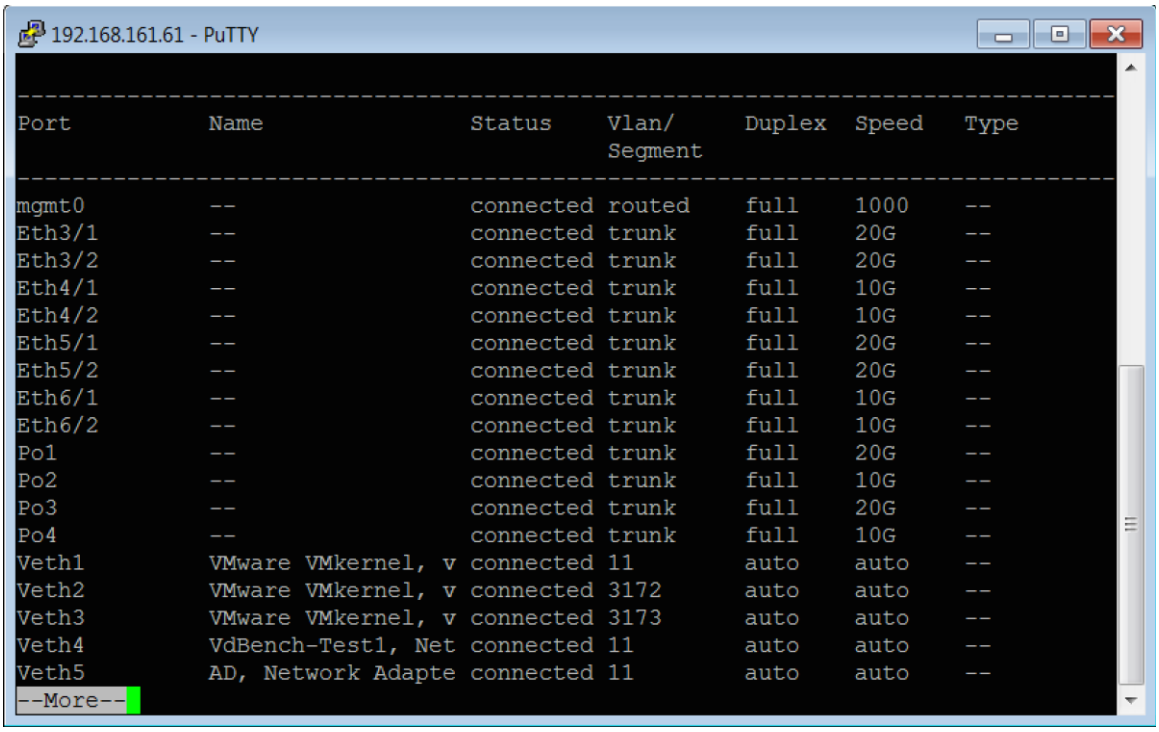
8. For `UpLink01`, select the system-uplink port group and make sure `vmnic0` is the Network adapter. Click OK.



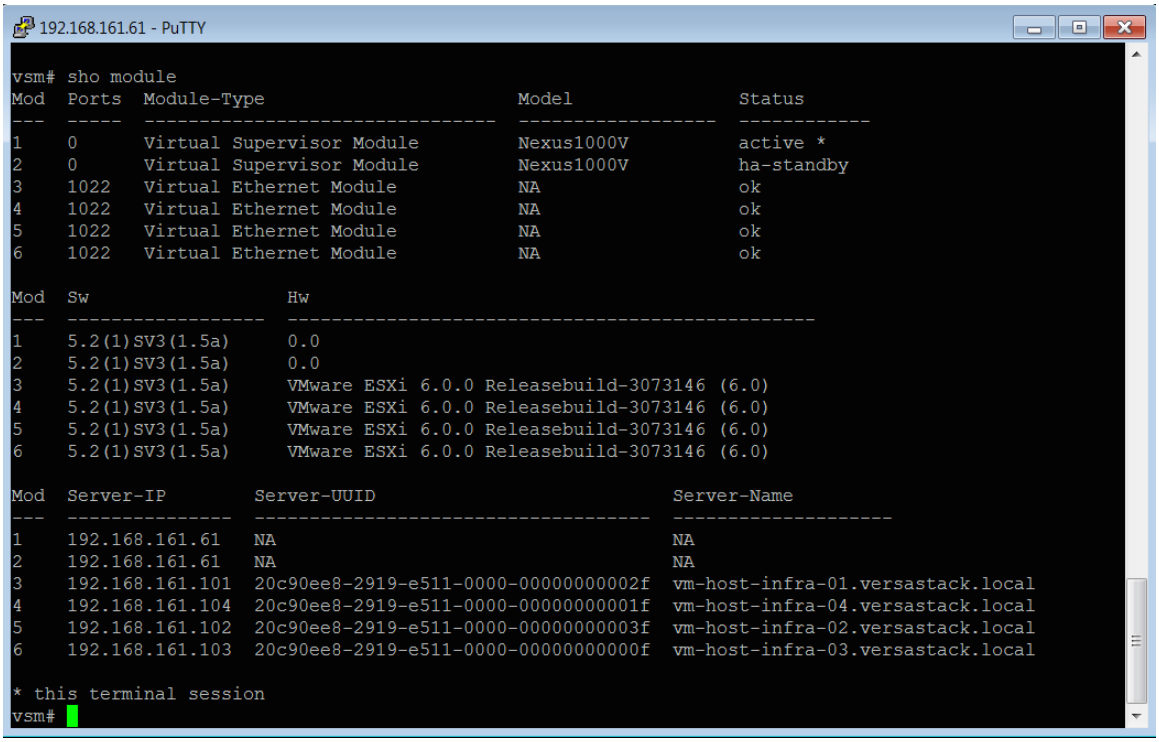
9. Click OK to complete adding the Uplink. It may be necessary to refresh the Web Client to see the addition.

10. Repeat this procedure for the second ESXi host.

11. From the SSH client that is connected to the Cisco Nexus 1000V, run show interface status to verify that all interfaces and port channels have been correctly configured.



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



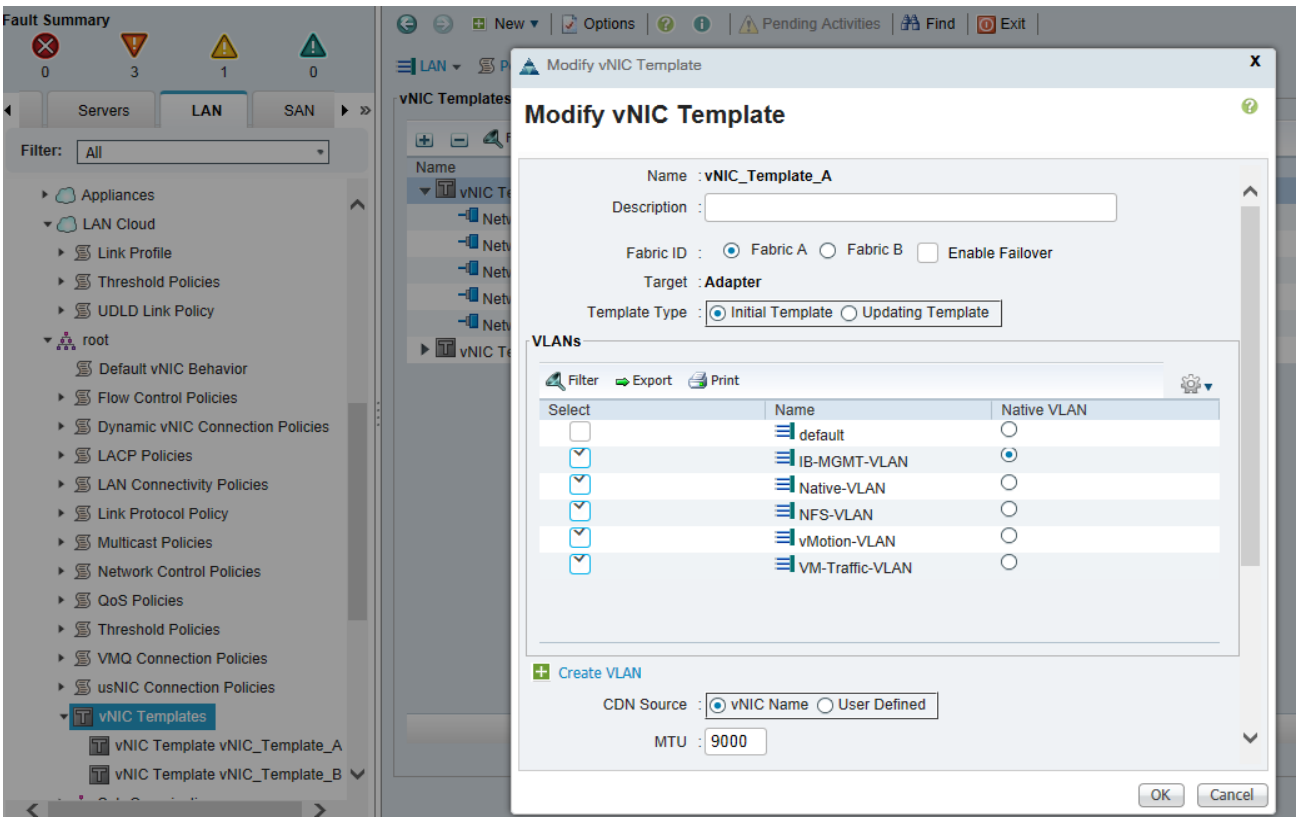
13. Run copy run start.

Remove the Redundancy for the NIC in Cisco UCS Manager

While creating the ESXi vNIC template settings, the default is to enable hardware failover on the vNIC. When you have deployed the N1kV, that setting is no longer required and should be disabled. To remove the redundancy, complete the following steps:

1. Launch Cisco UCS Manager and click LAN tab.
2. Click Policies, root, vNIC templates.
3. Click vNIC_Template_A, and uncheck Enable Failover.
4. Click Save Changes, and 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

This Bill of Materials for the VersaStack is for reference only including major components and may or may not include components such as cables, SFPs, etc.

Bill of Materials for VersaStack

Part Number	Product Description	Quantity Required
IBM FlashSystem V9000		
9846/9848-AC2	FlashSystem V9000 Control Enclosure	2
9846/9848-AE2	FlashSystem V9000 Storage Enclosure	1
AF1P	2m Fiber Cable (LC)	24
AH11	16Gb FC Adapter	8
AF19	16Gb Flash Enclosure Optics (4 pack)	2
AHA1	Compression Accelerator	4
5641-RB7	IBM FlashSystem V9000 Software V7	1
AF25	5.7 TB MicroLatency Flash Module	12

Part Number	Product Description	Quantity Required
Cisco Nexus 9300 Switching Components		
N9K-C9372PX	Cisco Nexus 9300 with 48p 10G SFP+ and 6p 40G QSFP+	2
N3K-C3064-ACC-KIT	Cisco Nexus 9300 Accessory Kit	2

Part Number	Product Description	Quantity Required
NXA-FAN-30CFM-F	Cisco 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
Cisoc N9K-PAC-650W-B	Cisco Nexus 9300 650W AC PS, Port-side Exhaust	4

Part Number	Product Description	Quantity Required
Cisco MDS FC Switch		
DS-C9148S-12PK9	Cisco MDS 9148S 16G FC switch, w/ 12 active ports	2
DS-9148S-KIT-CSCO	Cisco MDS 9148S Accessory Kit for Cisco	2
M9148S-PL12	Cisco MDS 9148S 16G FC 12-port upgrade license	2
DS-SFP-FC8G-SW	8 Gbps Fibre Channel SW SFP+, LC	8
DS-SFP-FC16G-SW	16 Gbps Fibre Channel SW SFP+, LC	24

CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	4

Part Number	Product Description	Quantity Required
Cisco UCS Unified Computing System		
Cisco UCSB-5108-AC2	Cisco UCS 5108 Blade Server AC2 Chassis, 0 PSU/8 fans/0 FEX	1
Cisco UCS-IOM-2208XP	Cisco UCS 2208XP I/O Module (8 External, 32 Internal 10Gb Ports)	2
Cisco UCSB-5108-PKG-HW	Cisco UCS 5108 Packaging for chassis with half width blades.	1
N20-CBLKP	Power supply unit blanking panel for Cisco UCS 5108	1
N01-UAC1	Single phase AC power module for Cisco UCS 5108	1
N20-FAN5	Fan module for Cisco UCS 5108	8
N20-CBLKB1	Blade slot blanking panel for Cisco UCS 5108/single slot	4

Part Number	Product Description	Quantity Required
N20-CAK	Accessory kit for Cisco UCS 5108 Blade Server Chassis	1
Cisco UCSB-B200-M4	Cisco UCS B200 M4 w/o CPU, mem, drive bays, HDD, mezz	4
Cisco UCS-CPU-E52650D	2.30 GHz E5-2650 v3/105W 10C/25MB Cache/DDR4 2133MHz	8
Cisco UCS-MR-1X162RU-A	16GB DDR4-2133-MHz RDIMM/PC4-17000/dual rank/x4/1.2v	32
Cisco UCSB-MLOM-PT-01	Cisco UCS Port Expander Card (mezz) for VIC	4
Cisco UCSB-MLOM-40G-03	Cisco UCS VIC 1340 modular LOM for blade servers	4
Cisco UCSB-HS-EP-M4-F	CPU Heat Sink for Cisco UCS B200 M4 Socket 1 (Front)	4
Cisco UCSB-HS-EP-M4-R	CPU Heat Sink for Cisco UCS B200 M4 Socket 2 (Rear)	4

Part Number	Product Description	Quantity Required
Cisco UCSB-LSTOR-BK	FlexStorage blanking panels w/o controller, w/o drive bays	8
Cisco UCSB-PSU-2500ACDV	2500W Platinum AC Hot Plug Power Supply - DV	4
CAB-C19-CBN	Cabinet Jumper Power Cord, 0 VAC 16A, C20-C19 Connectors	4

Part Number	Product Description	Quantity Required
Cisco UCS UCS-FI-6248UP Fabric Interconnect		
Cisco UCS-FI-6248UP	Cisco UCS 6248UP 1RU Fabric Int/No PSU/32 UP/ 12p LIC	2
Cisco UCS-ACC-6248UP	Cisco UCS 6248UP Chassis Accessory Kit	2
Cisco UCS-PSU-6248UP-AC	Cisco UCS 6248UP Power Supply/100-240VAC	4
Cisco UCS-BLKE-6200	Cisco UCS 6200 Series Expansion Module Blank	2
Cisco UCS-FAN-6248UP	Cisco UCS 6248UP Fan Module	4
Cisco UCS-FI-DL2	Cisco UCS 6248 Layer 2	2

Part Number	Product Description	Quantity Required
	Daughter Card	
CAB-9K12A-NA	Power Cord, 1VAC 13A NEMA 5-15 Plug, North America	4

Part Number	Product Description	Quantity Required
Cisco FEX		
N2K-C2232PF	Cisco Nexus 2232PP with 16 FET, choice of airflow/power	2
NXA-AIRFLOW-SLV	Cisco Nexus Airflow Extension Sleeve	2
N2K-F10G-F10G	N2K Uplink option FET-10G to FET-10G	2
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	4
FET-10G	10G Line Extender for FEX	32
N2232PP-FA-BUN	Standard airflow pack: N2K-C2232PP-10GE, 2AC PS, 1Fan	1

Part Number	Product Description	Quantity Required
Cisco UCS Rack Servers		
Cisco UCSC-C220-M4S	Cisco UCS C220 M4 SFF w/o CPU, mem, HD,	2

Part Number	Product Description	Quantity Required
	PCIe, PSU, rail kit	
Cisco UCS-CPU-E52640D	2.60 GHz E5-2640 v3/90W 8C/20MB Cache/DDR4 1866MHz	4
Cisco UCS-MR-1X162RU-A	16GB DDR4-2133-MHz RDIMM/PC4-17000/dual rank/x4/1.2v	16
Cisco UCSC-MLOM-CSC-02	Cisco UCS VIC1227 VIC MLOM - Dual Port 10Gb SFP+	2
Cisco UCSC-CMAF-M4	Reversible CMA for C220 M4 friction & ball bearing rail kits	2
Cisco UCSC-RAILF-M4	Friction Rail Kit for C220 M4 rack servers	2
Cisco UCS-SD-32G-S	32GB SD Card for UCS servers	4
Cisco UCSC-PSU1-770W	770W AC Hot-Plug Power Supply for 1U C-Series Rack Server	4
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	4
N20-BBLKD	Cisco UCS 2.5 inch HDD blanking panel	16
Cisco UCSC-HS-C220M4	Heat sink for Cisco UCS C220 M4 rack servers	4
Cisco UCSC-MLOM-BLK	MLOM Blanking Panel	2

This Bill of Materials is using the Cisco 1300 series VIC for blade servers. The Cisco 1200 VIC series can be substituted for the 1300 series VIC. Please consult with the IBM and Cisco compatibility guides for the latest hardware supported.

Appendix

Cisco Nexus 9000 Example Configurations

Cisco Nexus 9000 A

```
VersaStack_nexus9k_A# sh runn
!Command: show running-config
!Time: Mon Apr 11 19:07:04 2016
version 6.1(2)I3(5)
switchname VersaStack_nexus9k_A
vdc VersaStack_nexus9k_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 511
  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
cfs eth distribute
feature udld
feature lacp
feature vpc
logging level vpc 5
logging level aaa 5
logging level cdp 6
logging level monitor 6
logging level otm 5
logging level radius 5
logging level spanning-tree 6
username admin password 5 $1$cKpcGJCk$L13EI7E/kT7yugetZGc4z1  role network-admin
ssh key rsa 2048
ip domain-lookup
```

```
no service unsupported-transceiver

copp profile strict

snmp-server user admin network-admin auth md5 0x2727a9ca03efa8aac32b8a529849f2ad
priv 0x2727a9ca03efa8aac32b8a529849f2ad localizedkey

snmp-server host 192.168.161.67 traps version 2c public udp-port 2162

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

ntp server 192.168.160.254

vlan 1-2,11,3172-3174

vlan 2

  name Native-VLAN

vlan 11

  name IB-MGMT-VLAN

vlan 3172

  name NFS-VLAN

vlan 3173

  name vMotion-VLAN

vlan 3174

  name VM-Traffic-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 0.0.0.0/0 192.168.160.1

hardware qos ns-buffer-profile mesh

vpc domain 10

  peer-switch

  role priority 10

  peer-keepalive destination 192.168.161.12 source 192.168.161.11

  delay restore 150

  peer-gateway
```

```
  auto-recovery
  ip arp synchronize
interface port-channel10
  description vPC peer-link
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 11,3172-3174
  spanning-tree port type network
  vpc peer-link
interface port-channel11
  description IB-MGMT
  switchport mode trunk
  switchport access vlan 11
  switchport trunk allowed vlan 11
  spanning-tree port type network
  vpc 11
interface port-channel13
  description UCS-VersaStack-Flash-A
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 11,3172-3174
  spanning-tree port type edge trunk
  mtu 9216
  vpc 13
interface port-channel14
  description UCS-VersaStack-Flash-B
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 11,3172-3174
  spanning-tree port type edge trunk
  mtu 9216
  vpc 14
```

```
interface Ethernet1/1
interface Ethernet1/2
interface Ethernet1/3
interface Ethernet1/4
interface Ethernet1/5
interface Ethernet1/6
interface Ethernet1/7
interface Ethernet1/8
interface Ethernet1/9
interface Ethernet1/10
interface Ethernet1/11
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
  description UCS-VersaStack-Flash-A:1/25
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 11,3172-3174
  mtu 9216
  channel-group 13 mode active

interface Ethernet1/26
```

```
  description UCS-VersaStack-Flash-B:1/26
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 11,3172-3174
  mtu 9216
  channel-group 14 mode active
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
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
interface Ethernet1/48
  description IB-MGMT-SWITCH_uplink
  switchport mode trunk
  switchport access vlan 11
  switchport trunk allowed vlan 11
  channel-group 11 mode active
```

```
interface Ethernet1/49
  description VPC Peer VersaStack_nexus9k_B:1/49
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 11,3172-3174
  channel-group 10 mode active
interface Ethernet1/50
  description VPC Peer VersaStack_nexus9k_B:1/50
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 11,3172-3174
  channel-group 10 mode active
interface Ethernet1/51
interface Ethernet1/52
interface Ethernet1/53
interface Ethernet1/54
interface mgmt0
  vrf member management
  ip address 192.168.161.11/22
line console
line vty
boot nxos bootflash:/n9000-dk9.6.1.2.I3.5.bin
logging logfile messages 6
VersaStack_nexus9k_A# exit
```

Cisco Nexus 9000 B

```
VersaStack_nexus9k_B# sh runn
!Command: show running-config
!Time: Mon Apr 11 19:02:08 2016
version 6.1(2)I3(5)
switchname VersaStack_nexus9k_B
vdc VersaStack_nexus9k_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 511
  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
cfs eth distribute
feature udld
feature lacp
feature vpc
logging level vpc 5
logging level aaa 5
logging level cdp 6
logging level monitor 6
logging level otm 5
logging level radius 5
logging level spanning-tree 6
username admin password 5 $1$lcR9IS65$9aVGBC4Hxva9j45ss3lE91  role network-admin
ssh key rsa 2048
ip domain-lookup
no service unsupported-transceiver
copp profile strict
snmp-server user admin network-admin auth md5 0xb559c5eb732b5743e31f14e5dfeeb86a
priv 0xb559c5eb732b5743e31f14e5dfeeb86a localizedkey
snmp-server host 192.168.161.67 traps version 2c public udp-port 2162
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
ntp server 192.168.160.254
vlan 1-2,11,3172-3174
```

```
vlan 2
  name Native-VLAN
vlan 11
  name IB-MGMT-VLAN
vlan 3172
  name NFS-VLAN
vlan 3173
  name vMotion-VLAN
vlan 3174
  name VM-Traffic-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 0.0.0.0/0 192.168.160.254
hardware qos ns-buffer-profile mesh
vpc domain 10
  peer-switch
  role priority 20
  peer-keepalive destination 192.168.161.11 source 192.168.161.12
  delay restore 150
  peer-gateway
  ip arp synchronize
interface port-channel10
  description vPC peer-link
  switchport mode trunk
  switchport trunk allowed vlan 11,3172-3174
  spanning-tree port type network
  vpc peer-link
interface port-channel11
  description IB-MGMT
  switchport mode trunk
  switchport access vlan 11
```

```
  switchport trunk allowed vlan 11
  spanning-tree port type network
  vpc 11
interface port-channel13
  description UCS-VersaStack-Flash-A
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 11,3172-3174
  spanning-tree port type edge trunk
  mtu 9216
  vpc 13

interface port-channel14
  description UCS-VersaStack-B
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 11,3172-3174
  spanning-tree port type edge trunk
  mtu 9216
  vpc 14
interface Ethernet1/1
interface Ethernet1/2
interface Ethernet1/3
interface Ethernet1/4
interface Ethernet1/5
interface Ethernet1/6
interface Ethernet1/7
interface Ethernet1/8
interface Ethernet1/9
interface Ethernet1/10
interface Ethernet1/11
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
  description UCS-VersaStack-Flash-B:1/25
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 11,3172-3174
  mtu 9216
  channel-group 14 mode active
interface Ethernet1/26
  description UCS-VersaStack-Flash-A:1/26
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 11,3172-3174
  mtu 9216
  channel-group 13 mode active
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-MGMT-SWITCH_uplink
  switchport access vlan 11
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
interface Ethernet1/48
  switchport mode trunk
  switchport access vlan 11
  switchport trunk allowed vlan 11
  channel-group 11 mode active
interface Ethernet1/49
  description VPC Peer VersaStack_nexus9k_A:1/49
  switchport mode trunk
  switchport trunk allowed vlan 11,3172-3174
  channel-group 10 mode active
interface Ethernet1/50
  description VPC Peer VersaStack_nexus9k_A:1/50
  switchport mode trunk
  switchport trunk allowed vlan 11,3172-3174
  channel-group 10 mode active
interface Ethernet1/51
```

```
interface Ethernet1/52
interface Ethernet1/53
interface Ethernet1/54
interface mgmt0
  vrf member management
  ip address 192.168.161.12/22
line console
line vty
boot nxos bootflash:/n9000-dk9.6.1.2.I3.5.bin
logging logfile messages 6
VersaStack_nexus9k_B# exit
```

Cisco MDS Example Configurations

Cisco MDS 9148S A

```
VersaStack-MDS-A#
!Command: show running-config
!Time: Mon Apr 11 13:40:19 2016
version 6.2(13b)
power redundancy-mode redundant
feature npiv
feature fport-channel-trunk
role name default-role
  description This is a system defined role and applies to all users.
  rule 5 permit show feature environment
  rule 4 permit show feature hardware
  rule 3 permit show feature module
  rule 2 permit show feature snmp
  rule 1 permit show feature system
username admin password 5 $1$sKRMPQYi$/NAdDEi2J44GW9n9cQhY40  role network-admin
ssh key rsa 2048
ip domain-lookup
ip host VersaStack-MDS-A  192.168.161.15
aaa group server radius radius
```

```
snmp-server user admin network-admin auth md5 0x6f53059324fc0a02a20aca0a0e62a0a4
priv 0x6f53059324fc0a02a20aca0a0e62a0a4 localizedkey

snmp-server host 192.168.161.67 traps version 2c public udp-port 2162

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

ntp server 192.168.160.254

vsan database

  vsan 101

  vsan 201

device-alias database

  device-alias name VersaStack-SE-BE1 pwwn 50:05:07:60:5e:83:cc:81

  device-alias name VersaStack-SE-BE2 pwwn 50:05:07:60:5e:83:cc:91

  device-alias name VersaStack-SE-BE3 pwwn 50:05:07:60:5e:83:cc:a1

  device-alias name VersaStack-SE-BE4 pwwn 50:05:07:60:5e:83:cc:b1

  device-alias name VM-Host-Infra-01-A pwwn 20:00:00:25:b5:01:0a:2f

  device-alias name VM-Host-Infra-02-A pwwn 20:00:00:25:b5:01:0a:3f

  device-alias name VM-Host-Infra-03-A pwwn 20:00:00:25:b5:01:0a:0f

  device-alias name VM-Host-Infra-04-A pwwn 20:00:00:25:b5:01:0a:1f

  device-alias name VersaStack-ContA-BE1 pwwn 50:05:07:68:0c:11:22:71

  device-alias name VersaStack-ContA-BE2 pwwn 50:05:07:68:0c:31:22:71

  device-alias name VersaStack-ContA-FE1 pwwn 50:05:07:68:0c:21:22:71

  device-alias name VersaStack-ContA-FE3 pwwn 50:05:07:68:0c:51:22:71

  device-alias name VersaStack-ContB-BE1 pwwn 50:05:07:68:0c:11:22:67

  device-alias name VersaStack-ContB-BE2 pwwn 50:05:07:68:0c:31:22:67

  device-alias name VersaStack-ContB-FE1 pwwn 50:05:07:68:0c:21:22:67

  device-alias name VersaStack-ContB-FE3 pwwn 50:05:07:68:0c:51:22:67


device-alias commit

fcdomain fcid database

  vsan 101 wwn 24:01:00:2a:6a:c2:df:00 fcid 0x670000 dynamic

  vsan 101 wwn 20:00:00:25:b5:01:0a:0f fcid 0x670001 dynamic
```

```
!              [VM-Host-Infra-03-A]
  vsan 101 wwn 20:00:00:25:b5:01:0a:1f fcid 0x670002 dynamic
!              [VM-Host-Infra-04-A]
  vsan 101 wwn 20:00:00:25:b5:01:0a:2f fcid 0x670003 dynamic
!              [VM-Host-Infra-01-A]
  vsan 101 wwn 20:00:00:25:b5:01:0a:3f fcid 0x670004 dynamic
!              [VM-Host-Infra-02-A]
  vsan 101 wwn 50:05:07:68:0c:21:22:67 fcid 0x670100 dynamic
!              [VersaStack-ContB-FE1]
  vsan 101 wwn 50:05:07:68:0c:21:22:71 fcid 0x670200 dynamic
!              [VersaStack-ContA-FE1]
  vsan 201 wwn 50:05:07:68:0c:11:22:71 fcid 0x940000 dynamic
!              [VersaStack-ContA-BE1]
  vsan 101 wwn 50:05:07:68:0c:51:22:67 fcid 0x670300 dynamic
!              [VersaStack-ContB-FE3]
  vsan 201 wwn 50:05:07:68:0c:11:22:67 fcid 0x940100 dynamic
!              [VersaStack-ContB-BE1]
  vsan 101 wwn 50:05:07:68:0c:51:22:71 fcid 0x670400 dynamic
!              [VersaStack-ContA-FE3]
  vsan 201 wwn 50:05:07:68:0c:31:22:67 fcid 0x940200 dynamic
!              [VersaStack-ContB-BE2]
  vsan 201 wwn 50:05:07:68:0c:31:22:71 fcid 0x940300 dynamic
!              [VersaStack-ContA-BE2]
  vsan 201 wwn 50:05:07:60:5e:83:cc:81 fcid 0x940400 dynamic
!              [VersaStack-SE-BE1]
  vsan 201 wwn 50:05:07:60:5e:83:cc:a1 fcid 0x940500 dynamic
!              [VersaStack-SE-BE3]
  vsan 201 wwn 50:05:07:60:5e:83:cc:91 fcid 0x940600 dynamic
!              [VersaStack-SE-BE2]
  vsan 201 wwn 50:05:07:60:5e:83:cc:b1 fcid 0x940700 dynamic
!              [VersaStack-SE-BE4]
interface mgmt0
  ip address 192.168.161.15 255.255.252.0
```

```
interface port-channel1
  channel mode active
  switchport rate-mode dedicated
vsan database
  vsan 101 interface port-channel1
  vsan 101 interface fc1/5
  vsan 101 interface fc1/6
  vsan 101 interface fc1/7
  vsan 101 interface fc1/8
  vsan 201 interface fc1/9
  vsan 201 interface fc1/10
  vsan 201 interface fc1/11
  vsan 201 interface fc1/12
  vsan 201 interface fc1/13
  vsan 201 interface fc1/14
  vsan 201 interface fc1/15
  vsan 201 interface fc1/16
  vsan 201 interface fc1/17
  vsan 201 interface fc1/18
  vsan 201 interface fc1/19
  vsan 201 interface fc1/20
clock timezone EST -5 30
switchname VersaStack-MDS-A
line console
line vty
boot kickstart bootflash:/m9100-s5ek9-kickstart-mz.6.2.13b.bin
boot system bootflash:/m9100-s5ek9-mz.6.2.13b.bin
interface fc1/1
interface fc1/2
interface fc1/3
interface fc1/4
interface fc1/5
```

```
interface fc1/6
interface fc1/7
interface fc1/8
interface fc1/9
interface fc1/10
interface fc1/11
interface fc1/12
interface fc1/13
interface fc1/14
interface fc1/15
interface fc1/16
interface fc1/17
interface fc1/18
interface fc1/19
interface fc1/20
interface fc1/21
interface fc1/22
interface fc1/23
interface fc1/24
interface fc1/25
interface fc1/26
interface fc1/27
interface fc1/28
interface fc1/29
interface fc1/30
interface fc1/31
interface fc1/32
interface fc1/33
interface fc1/34
interface fc1/35
interface fc1/36
interface fc1/37
interface fc1/38
```

```
interface fc1/39
interface fc1/40
interface fc1/41
interface fc1/42
interface fc1/43
interface fc1/44
interface fc1/45
interface fc1/46
interface fc1/47
interface fc1/48
interface fc1/1
interface fc1/2
interface fc1/3
interface fc1/4
zoneset distribute full vsan 101
!Active Zone Database Section for vsan 101
zone name VM-Host-Infra-01-A vsan 101
    member pwwn 20:00:00:25:b5:01:0a:2f
!               [VM-Host-Infra-01-A]
    member pwwn 50:05:07:68:0c:21:22:71
!               [VersaStack-ContA-FE1]
    member pwwn 50:05:07:68:0c:51:22:71
!               [VersaStack-ContA-FE3]
    member pwwn 50:05:07:68:0c:21:22:67
!               [VersaStack-ContB-FE1]
    member pwwn 50:05:07:68:0c:51:22:67
!               [VersaStack-ContB-FE3]

zone name VM-Host-Infra-02-A vsan 101
    member pwwn 20:00:00:25:b5:01:0a:3f
!               [VM-Host-Infra-02-A]
    member pwwn 50:05:07:68:0c:21:22:71
!               [VersaStack-ContA-FE1]
```

```
    member pwwn 50:05:07:68:0c:51:22:71
!               [VersaStack-ContA-FE3]
    member pwwn 50:05:07:68:0c:21:22:67
!               [VersaStack-ContB-FE1]
    member pwwn 50:05:07:68:0c:51:22:67
!               [VersaStack-ContB-FE3]

zone name VM-Host-Infra-03-A vsan 101
    member pwwn 50:05:07:68:0c:21:22:71
!               [VersaStack-ContA-FE1]
    member pwwn 50:05:07:68:0c:51:22:71
!               [VersaStack-ContA-FE3]
    member pwwn 50:05:07:68:0c:21:22:67
!               [VersaStack-ContB-FE1]
    member pwwn 50:05:07:68:0c:51:22:67
!               [VersaStack-ContB-FE3]
    member pwwn 20:00:00:25:b5:01:0a:0f
!               [VM-Host-Infra-03-A]

zone name VM-Host-Infra-04-A vsan 101
    member pwwn 50:05:07:68:0c:21:22:71
!               [VersaStack-ContA-FE1]
    member pwwn 50:05:07:68:0c:51:22:71
!               [VersaStack-ContA-FE3]
    member pwwn 50:05:07:68:0c:21:22:67
!               [VersaStack-ContB-FE1]
    member pwwn 50:05:07:68:0c:51:22:67
!               [VersaStack-ContB-FE3]
    member pwwn 20:00:00:25:b5:01:0a:1f
!               [VM-Host-Infra-04-A]

zoneset name versastackzoneset vsan 101
    member VM-Host-Infra-01-A
```

```
    member VM-Host-Infra-02-A
    member VM-Host-Infra-03-A
    member VM-Host-Infra-04-A

zoneset activate name versastackzoneset vsan 101
do clear zone database vsan 101
!Full Zone Database Section for vsan 101
zone name VM-Host-Infra-01-A vsan 101
    member pwwn 20:00:00:25:b5:01:0a:2f
!               [VM-Host-Infra-01-A]
    member pwwn 50:05:07:68:0c:21:22:71
!               [VersaStack-ContA-FE1]
    member pwwn 50:05:07:68:0c:51:22:71
!               [VersaStack-ContA-FE3]
    member pwwn 50:05:07:68:0c:21:22:67
!               [VersaStack-ContB-FE1]
    member pwwn 50:05:07:68:0c:51:22:67
!               [VersaStack-ContB-FE3]

zone name VM-Host-Infra-02-A vsan 101
    member pwwn 20:00:00:25:b5:01:0a:3f
!               [VM-Host-Infra-02-A]
    member pwwn 50:05:07:68:0c:21:22:71
!               [VersaStack-ContA-FE1]
    member pwwn 50:05:07:68:0c:51:22:71
!               [VersaStack-ContA-FE3]
    member pwwn 50:05:07:68:0c:21:22:67
!               [VersaStack-ContB-FE1]
    member pwwn 50:05:07:68:0c:51:22:67
!               [VersaStack-ContB-FE3]

zone name VM-Host-Infra-03-A vsan 101
    member pwwn 50:05:07:68:0c:21:22:71
```

```
!               [VersaStack-ContA-FE1]
    member pwwn 50:05:07:68:0c:51:22:71
!               [VersaStack-ContA-FE3]
    member pwwn 50:05:07:68:0c:21:22:67
!               [VersaStack-ContB-FE1]
    member pwwn 50:05:07:68:0c:51:22:67
!               [VersaStack-ContB-FE3]
    member pwwn 20:00:00:25:b5:01:0a:0f
!               [VM-Host-Infra-03-A]

zone name VM-Host-Infra-04-A vsan 101
    member pwwn 50:05:07:68:0c:21:22:71
!               [VersaStack-ContA-FE1]
    member pwwn 50:05:07:68:0c:51:22:71
!               [VersaStack-ContA-FE3]
    member pwwn 50:05:07:68:0c:21:22:67
!               [VersaStack-ContB-FE1]
    member pwwn 50:05:07:68:0c:51:22:67
!               [VersaStack-ContB-FE3]
    member pwwn 20:00:00:25:b5:01:0a:1f
!               [VM-Host-Infra-04-A]

zoneset name versastackzoneset vsan 101
    member VM-Host-Infra-01-A
    member VM-Host-Infra-02-A
    member VM-Host-Infra-03-A
    member VM-Host-Infra-04-A

!Active Zone Database Section for vsan 201
zone name versastack vsan 201
    member pwwn 50:05:07:68:0c:11:22:71
!               [VersaStack-ContA-BE1]
    member pwwn 50:05:07:68:0c:31:22:71
```

```
!               [VersaStack-ContA-BE2]
    member pwwn 50:05:07:68:0c:11:22:67
!               [VersaStack-ContB-BE1]
    member pwwn 50:05:07:68:0c:31:22:67
!               [VersaStack-ContB-BE2]
    member pwwn 50:05:07:60:5e:83:cc:81
!               [VersaStack-SE-BE1]
    member pwwn 50:05:07:60:5e:83:cc:91
!               [VersaStack-SE-BE2]
    member pwwn 50:05:07:60:5e:83:cc:a1
!               [VersaStack-SE-BE3]
    member pwwn 50:05:07:60:5e:83:cc:b1
!               [VersaStack-SE-BE4]

zoneset name versastack-cluster vsan 201
    member versastack

zoneset activate name versastack-cluster vsan 201
do clear zone database vsan 201
!Full Zone Database Section for vsan 201
zone name versastack vsan 201
    member pwwn 50:05:07:68:0c:11:22:71
!               [VersaStack-ContA-BE1]
    member pwwn 50:05:07:68:0c:31:22:71
!               [VersaStack-ContA-BE2]
    member pwwn 50:05:07:68:0c:11:22:67
!               [VersaStack-ContB-BE1]
    member pwwn 50:05:07:68:0c:31:22:67
!               [VersaStack-ContB-BE2]
    member pwwn 50:05:07:60:5e:83:cc:81
!               [VersaStack-SE-BE1]
    member pwwn 50:05:07:60:5e:83:cc:91
!               [VersaStack-SE-BE2]
```

```
    member pwwn 50:05:07:60:5e:83:cc:a1
!               [VersaStack-SE-BE3]
    member pwwn 50:05:07:60:5e:83:cc:b1
!               [VersaStack-SE-BE4]

zoneset name versastack-cluster vsan 201
    member versastack

interface fc1/1
  port-license acquire
  channel-group 1 force
  no shutdown
interface fc1/2
  port-license acquire
  channel-group 1 force
  no shutdown
interface fc1/3
  port-license acquire
  channel-group 1 force
  no shutdown
interface fc1/4
  port-license acquire
  channel-group 1 force
  no shutdown
interface fc1/5
  switchport trunk mode off
  port-license acquire
  no shutdown

interface fc1/6
  switchport trunk mode off
  port-license acquire
  no shutdown
```

```
interface fc1/7
  switchport trunk mode off
  port-license acquire
  no shutdown
interface fc1/8
  switchport trunk mode off
  port-license acquire
  no shutdown
interface fc1/9
  switchport trunk mode off
  port-license acquire
  no shutdown
interface fc1/10
  switchport trunk mode off
  port-license acquire
  no shutdown
interface fc1/11
  switchport trunk mode off
  port-license acquire
  no shutdown
interface fc1/12
  switchport trunk mode off
  port-license acquire
  no shutdown
interface fc1/13
  switchport trunk mode off
  port-license acquire
  no shutdown

interface fc1/14
  switchport trunk mode off
  port-license acquire
  no shutdown
```

```
interface fc1/15
  switchport trunk mode off
  port-license acquire
  no shutdown
interface fc1/16
  switchport trunk mode off
  port-license acquire
  no shutdown
interface fc1/17
  port-license acquire
  no shutdown
interface fc1/18
  port-license acquire
  no shutdown
interface fc1/19
  port-license acquire
  no shutdown
interface fc1/20
  port-license acquire
  no shutdown
interface fc1/21
  port-license acquire
interface fc1/22
  port-license acquire
interface fc1/23
  port-license acquire
interface fc1/24
  port-license acquire

interface fc1/25
  port-license acquire
interface fc1/26
  port-license acquire
```

```
interface fc1/27
  port-license acquire
interface fc1/28
  port-license acquire
interface fc1/29
  port-license acquire
interface fc1/30
  port-license acquire
interface fc1/31
  port-license acquire
interface fc1/32
  port-license acquire
interface fc1/33
  port-license acquire
interface fc1/34
  port-license acquire
interface fc1/35
  port-license acquire
interface fc1/36
  port-license acquire
interface fc1/37
  port-license acquire
interface fc1/38
  port-license acquire
interface fc1/39
  port-license acquire
interface fc1/40
  port-license acquire

interface fc1/41
  port-license acquire
interface fc1/42
  port-license acquire
```

```
interface fc1/43
  port-license acquire
interface fc1/44
  port-license acquire
interface fc1/45
  port-license acquire
interface fc1/46
  port-license acquire
interface fc1/47
  port-license acquire
interface fc1/48
  port-license acquire
ip default-gateway 192.168.160.1
VersaStack-MDS-A# exit
```

Cisco MDS 9148S B

```
VersaStack-MDS-B# sh runn
!Command: show running-config
!Time: Mon Apr 11 13:36:57 2016
version 6.2(13b)
power redundancy-mode redundant
feature npiv
feature fport-channel-trunk
role name default-role
  description This is a system defined role and applies to all users.
  rule 5 permit show feature environment
  rule 4 permit show feature hardware
  rule 3 permit show feature module
  rule 2 permit show feature snmp
  rule 1 permit show feature system
username admin password 5 $1$yq9x2ZVf$e.61ttAhQoB2hortQJhmU1  role network-admin
ssh key rsa 2048
ip domain-lookup
```

```
ip host VersaStack-MDS-B  192.168.161.16

aaa group server radius radius

snmp-server user admin network-admin auth md5 0x574860bd3b13b5ab5f7652b55cc19206
priv 0x574860bd3b13b5ab5f7652b55cc19206 localizedkey

snmp-server host 192.168.161.67 traps version 2c public udp-port 2162

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

ntp server 192.168.160.254

vsan database

  vsan 102

  vsan 202

device-alias database

  device-alias name VersaStack-SE-BE5 pwwn 50:05:07:60:5e:83:cc:82

  device-alias name VersaStack-SE-BE6 pwwn 50:05:07:60:5e:83:cc:92

  device-alias name VersaStack-SE-BE7 pwwn 50:05:07:60:5e:83:cc:a2

  device-alias name VersaStack-SE-BE8 pwwn 50:05:07:60:5e:83:cc:b2

  device-alias name VM-Host-Infra-01-B pwwn 20:00:00:25:b5:01:0b:2f

  device-alias name VM-Host-Infra-02-B pwwn 20:00:00:25:b5:01:0b:3f

  device-alias name VM-Host-Infra-03-B pwwn 20:00:00:25:b5:01:0b:0f

  device-alias name VM-Host-Infra-04-B pwwn 20:00:00:25:b5:01:0b:1f

  device-alias name VersaStack-ContA-BE3 pwwn 50:05:07:68:0c:12:22:71

  device-alias name VersaStack-ContA-BE4 pwwn 50:05:07:68:0c:32:22:71

  device-alias name VersaStack-ContA-FE2 pwwn 50:05:07:68:0c:22:22:71

  device-alias name VersaStack-ContA-FE4 pwwn 50:05:07:68:0c:52:22:71

  device-alias name VersaStack-ContB-BE3 pwwn 50:05:07:68:0c:12:22:67

  device-alias name VersaStack-ContB-BE4 pwwn 50:05:07:68:0c:32:22:67

  device-alias name VersaStack-ContB-FE2 pwwn 50:05:07:68:0c:22:22:67

  device-alias name VersaStack-ContB-FE4 pwwn 50:05:07:68:0c:52:22:67


device-alias commit
```

```
fcdomain fcid database
  vsan 102 wwn 50:05:07:68:0c:22:22:71 fcid 0xa50000 dynamic
!              [VersaStack-ContA-FE2]
  vsan 102 wwn 50:05:07:68:0c:22:22:67 fcid 0xa50100 dynamic
!              [VersaStack-ContB-FE2]
  vsan 102 wwn 24:02:00:2a:6a:c2:de:c0 fcid 0xa50200 dynamic
  vsan 102 wwn 20:00:00:25:b5:01:0b:0f fcid 0xa50201 dynamic
!              [VM-Host-Infra-03-B]
  vsan 102 wwn 20:00:00:25:b5:01:0b:1f fcid 0xa50202 dynamic
!              [VM-Host-Infra-04-B]
  vsan 102 wwn 20:00:00:25:b5:01:0b:2f fcid 0xa50203 dynamic
!              [VM-Host-Infra-01-B]
  vsan 102 wwn 20:00:00:25:b5:01:0b:3f fcid 0xa50204 dynamic
!              [VM-Host-Infra-02-B]
  vsan 102 wwn 50:05:07:68:0c:52:22:67 fcid 0xa50300 dynamic
!              [VersaStack-ContB-FE4]
  vsan 102 wwn 50:05:07:68:0c:52:22:71 fcid 0xa50400 dynamic
!              [VersaStack-ContA-FE4]
  vsan 202 wwn 50:05:07:68:0c:32:22:71 fcid 0x7c0000 dynamic
!              [VersaStack-ContA-BE4]
  vsan 202 wwn 50:05:07:68:0c:32:22:67 fcid 0x7c0100 dynamic
!              [VersaStack-ContB-BE4]
  vsan 202 wwn 50:05:07:60:5e:83:cc:a2 fcid 0x7c0200 dynamic
!              [VersaStack-SE-BE7]
  vsan 202 wwn 50:05:07:60:5e:83:cc:82 fcid 0x7c0300 dynamic
!              [VersaStack-SE-BE5]
  vsan 202 wwn 50:05:07:60:5e:83:cc:b2 fcid 0x7c0400 dynamic
!              [VersaStack-SE-BE8]
  vsan 202 wwn 50:05:07:60:5e:83:cc:92 fcid 0x7c0500 dynamic
!              [VersaStack-SE-BE6]
  vsan 202 wwn 50:05:07:68:0c:12:22:67 fcid 0x7c0600 dynamic
!              [VersaStack-ContB-BE3]
  vsan 202 wwn 50:05:07:68:0c:12:22:71 fcid 0x7c0700 dynamic
```

```
!              [VersaStack-ContA-BE3]


interface mgmt0
  ip address 192.168.161.16 255.255.252.0

interface port-channel2
  channel mode active
  switchport rate-mode dedicated
vsan database
  vsan 102 interface port-channel2
  vsan 102 interface fc1/5
  vsan 102 interface fc1/6
  vsan 102 interface fc1/7
  vsan 102 interface fc1/8
  vsan 202 interface fc1/9
  vsan 202 interface fc1/10
  vsan 202 interface fc1/11
  vsan 202 interface fc1/12
  vsan 202 interface fc1/13
  vsan 202 interface fc1/14
  vsan 202 interface fc1/15
  vsan 202 interface fc1/16
  vsan 202 interface fc1/17
  vsan 202 interface fc1/18
  vsan 202 interface fc1/19
  vsan 202 interface fc1/20
clock timezone EST -5 30
switchname VersaStack-MDS-B
line console
line vty
boot kickstart bootflash:/m9100-s5ek9-kickstart-mz.6.2.13b.bin
boot system bootflash:/m9100-s5ek9-mz.6.2.13b.bin
```

```
interface fc1/1
interface fc1/2
interface fc1/3
interface fc1/4
interface fc1/5
interface fc1/6
interface fc1/7
interface fc1/8
interface fc1/9
interface fc1/10
interface fc1/11
interface fc1/12
interface fc1/13
interface fc1/14
interface fc1/15
interface fc1/16
interface fc1/17
interface fc1/18
interface fc1/19
interface fc1/20
interface fc1/21
interface fc1/22
interface fc1/23
interface fc1/24
interface fc1/25
interface fc1/26
interface fc1/27
interface fc1/28
interface fc1/29
interface fc1/30
interface fc1/31
interface fc1/32
interface fc1/33
```

```
interface fc1/34
interface fc1/35
interface fc1/36
interface fc1/37
interface fc1/38
interface fc1/39
interface fc1/40
interface fc1/41
interface fc1/42
interface fc1/43
interface fc1/44
interface fc1/45
interface fc1/46
interface fc1/47
interface fc1/48
interface fc1/1
interface fc1/2
interface fc1/3
interface fc1/4
!Active Zone Database Section for vsan 102
zone name VM-Host-Infra-01-B vsan 102
    member pwwn 20:00:00:25:b5:01:0b:2f
!               [VM-Host-Infra-01-B]
    member pwwn 50:05:07:68:0c:22:22:71
!               [VersaStack-ContA-FE2]
    member pwwn 50:05:07:68:0c:52:22:71
!               [VersaStack-ContA-FE4]
    member pwwn 50:05:07:68:0c:22:22:67
!               [VersaStack-ContB-FE2]
    member pwwn 50:05:07:68:0c:52:22:67
!               [VersaStack-ContB-FE4]

zone name VM-Host-Infra-02-B vsan 102
```

```
    member pwwn 20:00:00:25:b5:01:0b:3f
!               [VM-Host-Infra-02-B]
    member pwwn 50:05:07:68:0c:22:22:71
!               [VersaStack-ContA-FE2]
    member pwwn 50:05:07:68:0c:52:22:71
!               [VersaStack-ContA-FE4]
    member pwwn 50:05:07:68:0c:22:22:67
!               [VersaStack-ContB-FE2]
    member pwwn 50:05:07:68:0c:52:22:67
!               [VersaStack-ContB-FE4]

zone name VM-Host-Infra-03-B vsan 102
    member pwwn 20:00:00:25:b5:01:0b:0f
!               [VM-Host-Infra-03-B]
    member pwwn 50:05:07:68:0c:22:22:71
!               [VersaStack-ContA-FE2]
    member pwwn 50:05:07:68:0c:52:22:71
!               [VersaStack-ContA-FE4]
    member pwwn 50:05:07:68:0c:22:22:67
!               [VersaStack-ContB-FE2]
    member pwwn 50:05:07:68:0c:52:22:67
!               [VersaStack-ContB-FE4]

zone name VM-Host-Infra-04-B vsan 102
    member pwwn 20:00:00:25:b5:01:0b:1f
!               [VM-Host-Infra-04-B]
    member pwwn 50:05:07:68:0c:22:22:71
!               [VersaStack-ContA-FE2]
    member pwwn 50:05:07:68:0c:52:22:71
!               [VersaStack-ContA-FE4]
    member pwwn 50:05:07:68:0c:22:22:67
!               [VersaStack-ContB-FE2]
    member pwwn 50:05:07:68:0c:52:22:67
```

```
!               [VersaStack-ContB-FE4]

zoneset name versastackzoneset vsan 102
    member VM-Host-Infra-01-B
    member VM-Host-Infra-02-B
    member VM-Host-Infra-03-B
    member VM-Host-Infra-04-B

zoneset activate name versastackzoneset vsan 102
do clear zone database vsan 102
!Full Zone Database Section for vsan 102
zone name VM-Host-Infra-01-B vsan 102
    member pwwn 20:00:00:25:b5:01:0b:2f
!               [VM-Host-Infra-01-B]
    member pwwn 50:05:07:68:0c:22:22:71
!               [VersaStack-ContA-FE2]
    member pwwn 50:05:07:68:0c:52:22:71
!               [VersaStack-ContA-FE4]
    member pwwn 50:05:07:68:0c:22:22:67
!               [VersaStack-ContB-FE2]
    member pwwn 50:05:07:68:0c:52:22:67
!               [VersaStack-ContB-FE4]

zone name VM-Host-Infra-02-B vsan 102
    member pwwn 20:00:00:25:b5:01:0b:3f
!               [VM-Host-Infra-02-B]
    member pwwn 50:05:07:68:0c:22:22:71
!               [VersaStack-ContA-FE2]
    member pwwn 50:05:07:68:0c:52:22:71
!               [VersaStack-ContA-FE4]
    member pwwn 50:05:07:68:0c:22:22:67
!               [VersaStack-ContB-FE2]
    member pwwn 50:05:07:68:0c:52:22:67
```

```
!               [VersaStack-ContB-FE4]

zone name VM-Host-Infra-03-B vsan 102
    member pwwn 20:00:00:25:b5:01:0b:0f
!               [VM-Host-Infra-03-B]
    member pwwn 50:05:07:68:0c:22:22:71
!               [VersaStack-ContA-FE2]
    member pwwn 50:05:07:68:0c:52:22:71
!               [VersaStack-ContA-FE4]
    member pwwn 50:05:07:68:0c:22:22:67
!               [VersaStack-ContB-FE2]
    member pwwn 50:05:07:68:0c:52:22:67
!               [VersaStack-ContB-FE4]

zone name VM-Host-Infra-04-B vsan 102
    member pwwn 20:00:00:25:b5:01:0b:1f
!               [VM-Host-Infra-04-B]
    member pwwn 50:05:07:68:0c:22:22:71
!               [VersaStack-ContA-FE2]
    member pwwn 50:05:07:68:0c:52:22:71
!               [VersaStack-ContA-FE4]
    member pwwn 50:05:07:68:0c:22:22:67
!               [VersaStack-ContB-FE2]
    member pwwn 50:05:07:68:0c:52:22:67
!               [VersaStack-ContB-FE4]

zoneset name versastackzoneset vsan 102
    member VM-Host-Infra-01-B
    member VM-Host-Infra-02-B
    member VM-Host-Infra-03-B
    member VM-Host-Infra-04-B

!Active Zone Database Section for vsan 202
```

```
zone name versastack vsan 202
    member pwwn 50:05:07:68:0c:12:22:67
!               [VersaStack-ContB-BE3]
    member pwwn 50:05:07:68:0c:32:22:67
!               [VersaStack-ContB-BE4]
    member pwwn 50:05:07:68:0c:12:22:71
!               [VersaStack-ContA-BE3]
    member pwwn 50:05:07:68:0c:32:22:71
!               [VersaStack-ContA-BE4]
    member pwwn 50:05:07:60:5e:83:cc:82
!               [VersaStack-SE-BE5]
    member pwwn 50:05:07:60:5e:83:cc:92
!               [VersaStack-SE-BE6]
    member pwwn 50:05:07:60:5e:83:cc:a2
!               [VersaStack-SE-BE7]
    member pwwn 50:05:07:60:5e:83:cc:b2
!               [VersaStack-SE-BE8]

zoneset name versastack-cluster vsan 202
    member versastack

zoneset activate name versastack-cluster vsan 202
do clear zone database vsan 202
!Full Zone Database Section for vsan 202
zone name versastack vsan 202
    member pwwn 50:05:07:68:0c:12:22:67
!               [VersaStack-ContB-BE3]
    member pwwn 50:05:07:68:0c:32:22:67
!               [VersaStack-ContB-BE4]
    member pwwn 50:05:07:68:0c:12:22:71
!               [VersaStack-ContA-BE3]
    member pwwn 50:05:07:68:0c:32:22:71
!               [VersaStack-ContA-BE4]
```

```
    member pwwn 50:05:07:60:5e:83:cc:82
!               [VersaStack-SE-BE5]
    member pwwn 50:05:07:60:5e:83:cc:92
!               [VersaStack-SE-BE6]
    member pwwn 50:05:07:60:5e:83:cc:a2
!               [VersaStack-SE-BE7]
    member pwwn 50:05:07:60:5e:83:cc:b2
!               [VersaStack-SE-BE8]

zoneset name versastack-cluster vsan 202
    member versastack

interface fc1/1
  port-license acquire
  channel-group 2 force
  no shutdown
interface fc1/2
  port-license acquire
  channel-group 2 force
  no shutdown
interface fc1/3
  port-license acquire
  channel-group 2 force
  no shutdown
interface fc1/4
  port-license acquire
  channel-group 2 force
  no shutdown
interface fc1/5
  switchport trunk mode off
  port-license acquire
  no shutdown
interface fc1/6
```

```
    switchport trunk mode off
    port-license acquire
    no shutdown
  interface fc1/7
    switchport trunk mode off
    port-license acquire
    no shutdown
  interface fc1/8
    switchport trunk mode off
    port-license acquire
    no shutdown
  interface fc1/9
    switchport trunk mode off
    port-license acquire
    no shutdown
  interface fc1/10
    switchport trunk mode off
    port-license acquire
    no shutdown
  interface fc1/11
    switchport trunk mode off
    port-license acquire
    no shutdown
  interface fc1/12
    switchport trunk mode off
    port-license acquire
    no shutdown

  interface fc1/13
    switchport trunk mode off
    port-license acquire
    no shutdown
  interface fc1/14
```

```
    switchport trunk mode off
    port-license acquire
    no shutdown
interface fc1/15
    switchport trunk mode off
    port-license acquire
    no shutdown
interface fc1/16
    switchport trunk mode off
    port-license acquire
    no shutdown
interface fc1/17
    port-license acquire
    no shutdown
interface fc1/18
    port-license acquire
    no shutdown
interface fc1/19
    port-license acquire
    no shutdown
interface fc1/20
    port-license acquire
    no shutdown
interface fc1/21
    port-license acquire
interface fc1/22
    port-license acquire
interface fc1/23
    port-license acquire
interface fc1/24
    port-license acquire
interface fc1/25
    port-license acquire
```

```
interface fc1/26
  port-license acquire
interface fc1/27
  port-license acquire
interface fc1/28
  port-license acquire
interface fc1/29
  port-license acquire
interface fc1/30
  port-license acquire
interface fc1/31
  port-license acquire
interface fc1/32
  port-license acquire
interface fc1/33
  port-license acquire
interface fc1/34
  port-license acquire
interface fc1/35
  port-license acquire
interface fc1/36
  port-license acquire
interface fc1/37
  port-license acquire
interface fc1/38
  port-license acquire

interface fc1/39
  port-license acquire
interface fc1/40
  port-license acquire
interface fc1/41
  port-license acquire
```

```
interface fc1/42
  port-license acquire
interface fc1/43
  port-license acquire
interface fc1/44
  port-license acquire
interface fc1/45
  port-license acquire
interface fc1/46
  port-license acquire
interface fc1/47
  port-license acquire
interface fc1/48
  port-license acquire
ip default-gateway 192.168.160.1
VersaStack-MDS-B# exit
```

About the Authors

Sreenivasa Edula, Technical Marketing Engineer, Cisco 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.

Dave Gimpl, Senior Technical Staff Member, IBM Systems

Dave has over 25 years of engineering experience in IBMs Systems group, and is the Chief Architect of the FlashSystem V9000 and has been involved in the development of the FlashSystem product range from its inception.