

# VersaStack with Cisco UCS Mini and IBM Storwize V5000 Gen2, Direct Attached SAN Storage

Deployment Guide for VersaStack using IBM Storwize V5000 2nd Generation, Cisco UCS Mini with VMware vSphere 6.0 Update 2 and Direct Attached SAN Storage

**Last Updated:** February 27, 2017



# 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>

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

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

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

© 2017 Cisco Systems, Inc. All rights reserved.

# Table of Contents

Executive Summary .....	7
VersaStack for Data Center Overview .....	9
Introduction .....	9
Audience .....	9
Purpose of this document .....	9
Solution Design and Architecture .....	10
Architecture .....	10
Physical Topology.....	10
Software Revisions .....	12
Configuration Guidelines .....	12
Cisco UCS Central .....	13
Virtual Machines .....	13
Configuration Variables.....	14
VersaStack Cabling.....	18
VersaStack Cabling.....	18
Network Configuration .....	22
Cisco Nexus 9000 Initial Configuration Setup .....	22
Cisco Nexus A.....	22
Cisco Nexus B .....	24
Enable Appropriate Cisco Nexus 9000 Features and Settings.....	25
Cisco Nexus 9000 A and Cisco Nexus 9000 B.....	25
Create VLANs for VersaStack IP Traffic .....	26
Cisco Nexus 9000 A and Cisco Nexus 9000 B.....	26
Configure Virtual Port Channel Domain .....	26
Cisco Nexus 9000 A .....	26
Cisco Nexus 9000 B .....	27
Configure Network Interfaces for the vPC Peer Links.....	27
Cisco Nexus 9000 A .....	28
Cisco Nexus 9000 B .....	28
Configure Network Interfaces to Cisco UCS Fabric Interconnect.....	29
Cisco Nexus 9000 A .....	29
Cisco Nexus 9000 B .....	31
Management Plane Access for Servers and Virtual Machines .....	32

Cisco Nexus 9000 A and B Using Interface VLAN Example 1 .....	33
Cisco Nexus 9000 A and B using Port Channel Example 2 .....	34
Storage Configuration .....	35
IBM Storwize V5030 .....	35
Prerequisites .....	35
IBM Storwize V5000 Initial Configuration .....	35
IBM Storwize V5000 GUI Setup .....	39
Cisco UCS Compute Configuration .....	60
VersaStack Cisco UCS Initial Setup .....	60
Cisco UCS Fabric Interconnect 6324 A .....	60
Cisco UCS Fabric Interconnect 6324 B .....	61
VersaStack Cisco UCS Base Setup .....	61
Log in to Cisco UCS Manager .....	61
Upgrade Cisco UCS Manager Software to Version 3.1(2c) .....	62
Add Block of IP Addresses for Out-of-band KVM Access .....	62
Synchronize Cisco UCS to NTP .....	63
Configure UCS Servers .....	64
Edit Chassis Discovery Policy .....	64
Extending Cisco UCS Mini .....	65
Acknowledge Cisco UCS Chassis .....	65
Enable Uplink Ports .....	66
Create UUID Suffix Pool .....	67
Create Server Pool .....	68
Create Host Firmware Package .....	69
Create Local Disk Configuration Policy (Optional) .....	70
Create Power Control Policy .....	71
Create Server Pool Qualification Policy (Optional) .....	72
Create Server BIOS Policy .....	73
Create vNIC/vHBA Placement Policy for Virtual Machine Infrastructure Hosts .....	77
Update Default Maintenance Policy .....	78
Configure UCS SAN Connectivity .....	79
Configure Unified Ports .....	79
Configure Fabric Interconnects in FC Switching Mode .....	80
Create VSAN for the Fibre Channel Interfaces .....	81
Configure the FC Ports as Storage Ports .....	83

Create WWNN Pools.....	85
Create WWPN Pools.....	86
Create vHBA Templates for Fabric A and Fabric B.....	89
Create the Storage Connection Policy Fabric-A.....	90
Create the Storage Connection Policy Fabric-B.....	93
Create a SAN Connectivity Policy .....	94
Create Boot Policies .....	98
Configure UCS LAN Connectivity.....	105
Configure Uplink Port Channels to Cisco Nexus Switches.....	105
Create MAC Address Pools .....	107
Create VLANs.....	110
Set Jumbo Frames in Cisco UCS Fabric.....	112
Create Network Control Policy for Cisco Discovery Protocol.....	113
Create vNIC Templates.....	114
Create LAN Connectivity Policy .....	130
Create Service Profile Template .....	138
Create Service Profiles .....	148
Storage LUN Mapping .....	150
Adding Hosts and Mapping Volumes on the IBM Storwize V5000.....	150
VMware vSphere Installation and Setup.....	156
VersaStack VMware ESXi 6.0 Update 2 SAN Boot Installation.....	156
Log in to Cisco UCS 6324 Fabric Interconnect.....	156
VMware ESXi Installation .....	157
Install ESXi on the Servers .....	158
Set Up Management Networking for ESXi Hosts .....	158
Log in to VMware ESXi Hosts Using VMware vSphere Client .....	161
Install VMware Drivers for the Cisco Virtual Interface Card (VIC).....	162
Map Required VMFS Datastores .....	163
Configure NTP on ESXi Hosts .....	164
Move VM Swap File Location.....	165
VersaStack VMware vCenter 6.0U2 .....	166
Install the Client Integration Plug-In .....	166
Building the VMware vCenter Server Appliance.....	167
Set Up vCenter Server.....	176
Set Up vCenter Server with a Datacenter, Cluster, DRS and HA .....	178

Configure ESXi Networking .....	183
Create a VMware vDS for Application and Production networks .....	192
Add the ESXi Hosts to the vDS .....	199
Appendix .....	211
Cisco Nexus 9000 Example Configurations .....	211
Cisco Nexus 9000 A .....	211
Cisco Nexus 9000 B .....	219
About the Authors .....	228
Acknowledgements .....	228



## Executive Summary

---

This deployment guide provides step-by-step instructions to deploy a VersaStack system consisting of IBM V5030 storage and Cisco UCS Mini infrastructure for a successful VMware deployment with Direct Attached Fibre Channel Storage Connectivity. For example, this solution could be deployed in a remote branch office location or as a small to midsize solution in the datacenter. For design guidance for which VersaStack solution best suites your requirements, please refer to the Design Zone for information about VersaStack later in this document.

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

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

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

- Cisco Unified Computing System Manger providing simplified management for compute and network through a consolidated management tool
- Cisco 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 Thin-provisioning to reduce the storage footprint and storage costs
- IBM Easy Tier to automate optimizing performance while lowering storage costs by automatically placing infrequently accessed data on less expensive disks, and highly accessed data on faster tiers thereby reducing costly migrations
- **IBM's V5000 Storwize Simplified Storage Management** designed to simplify day to day storage tasks

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



# VersaStack for Data Center Overview

---

## Introduction

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

This document describes the architecture and deployment procedures of an infrastructure composed of Cisco®, IBM®, and VMware® virtualization that uses IBM Storwize V5030 with Fibre Channel storage directly attached to the Cisco UCS Mini.

## Audience

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

## Purpose of this document

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

- Validation of the Cisco UCS Mini with Cisco Nexus 9000 switches and IBM Storwize V5000 2nd Generation storage array
- Support for the Cisco UCS 3.1(2c) release
- Cisco UCS Mini with Secondary Chassis support
- Support for release 7.7.1.3 of IBM® Spectrum Virtualize™

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

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

## Solution Design and Architecture

---

### Architecture

VersaStack with Cisco UCS Mini and V5000 2nd Generation architecture aligns with the converged infrastructure configurations and best practices as identified in the previous VersaStack releases. The system includes hardware and software compatibility support between all components and aligns to the configuration best practices for each of these components. All the core hardware components and software releases are listed and supported on both the Cisco compatibility list:

[http://www.cisco.com/en/US/products/ps10477/prod\\_technical\\_reference\\_list.html](http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html)

and IBM Interoperability Matrix:

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

The system supports high availability at network, compute and storage layers such that no single point of failure exists in the design. The system utilizes 10 Gbps Ethernet jumbo-frame based connectivity combined with port aggregation technologies such as virtual port-channels (VPC) for non-blocking LAN traffic forwarding. A dual SAN 8Gbps environment enabled by the Cisco 6324 fabric Interconnects provides redundant storage access from compute devices to the storage controllers.

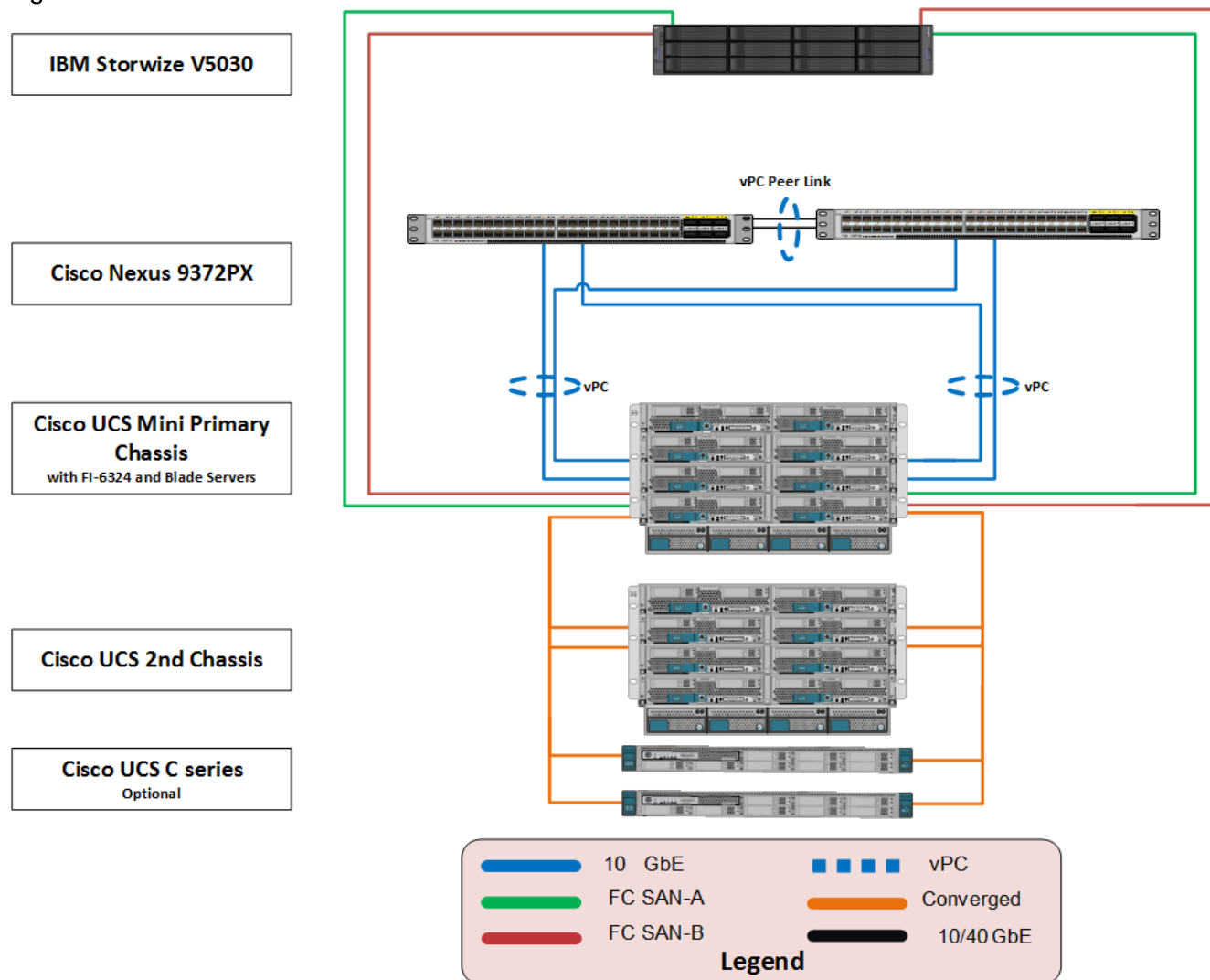
### Physical Topology

VersaStack Direct Attached SAN storage design provides a high redundancy, high-performance solution for the deployment of virtualized data center architecture. This solution design leverages Direct Attached Fibre Channel storage connectivity for compute enabling a simple, flexible and cost-effective solution.

This VersaStack design utilizes Cisco UCS Mini platform with Cisco B200 M4 half-width blades and Cisco UCS C220 M4 rack mount servers connected and managed through Cisco UCS 6324 Fabric Interconnects and the integrated UCS manager. These high performance servers are configured as stateless compute nodes where ESXi 6.0 U2 hypervisor is loaded using Fibre Channel SAN boot. The boot disks to store ESXi hypervisor image and configuration along with the block datastores to host application Virtual Machines (VMs) are provisioned on the IBM Storwize V5030 storage. The Cisco Unified Computing System and Cisco Nexus 9000 platforms support active port channeling using 802.3ad standard Link Aggregation Control Protocol (LACP). Port channeling is a link aggregation technique offering link fault tolerance and traffic distribution (load balancing) for improved aggregate bandwidth across member ports.

Each Cisco UCS Fabric Interconnect is connected to both the Cisco Nexus 9372 switches using virtual port-channel (vPC) enabled 10GbE uplinks for a total aggregate bandwidth of 20Gbps. The Cisco UCS Mini can be extended by connecting a second Cisco UCS Chassis with eight blades and with two Cisco UCS rack-mount servers using the 40GbE Enhanced Quad SFP (QSFP+) ports available on the Cisco UCS 6324 Fabric Interconnects.

Figure 1 VersaStack Architecture



The reference architecture covered in this document leverages the following:

- Two Cisco Nexus 9372PX switches
- Two Cisco UCS 6324 Fabric Interconnects
- Support for 2 Cisco UCS C-Series servers without any additional networking components
- Support for up to 16 Cisco UCS B-Series servers without any additional blade server chassis
- IBM Storwize V5000 Support for 16 Gb FC, 12 Gb SAS, 10 Gb iSCSI/FCoE, and 1 Gb iSCSI for additional I/O connectivity
- Support for 504 drives per system with an attachment of 20 Storwize V5000 expansion enclosures and 1,008 drives with a two-way clustered configuration

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.

## Software Revisions

Table 1 outlines the hardware and software versions used for the solution validation. It is important to note that Cisco, IBM, and VMware have interoperability matrices that should be referenced to determine support for any specific implementation of VersaStack. Please refer to the following links for more information:

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	Version or Release	Details
Compute	Cisco UCS fabric interconnect	3.1(2c)	Embedded management
	Cisco UCS C 220 M3/M4	3.1(2c)	Software bundle release
	Cisco UCS B 200 M3/ M4	3.1(2c)	Software bundle release
	Cisco eNIC	2.3.0.10	Ethernet driver for Cisco VIC
	Cisco fNIC	1.6.0.28	FCoE driver for Cisco VIC
Network	Cisco Nexus 9372PX	7.0(3)I2(4)	Operating system version
Storage	IBM Storwize V5030	7.7.1.3	Software version
Software	VMware vSphere	ESXi™ 6.0u2	Operating system version
	VMware vCenter™	6.0u2	VMware vCenter Appliance
	Cisco Nexus 1000v (Optional)	5.2(1)SV3(2.1)	Software version
	Virtual Switch Update Manager (VSUM)  (Only if installing Cisco Nexus 1000V)	2.0	Virtual Switch Deployment Software

## Configuration Guidelines

This document provides the details for configuring a fully redundant, highly available infrastructure. Therefore, reference is made to which component is being configured with each step, either 01 or 02 or

A and B. For example, the Cisco UCS Fabric Interconnects are identified as FI-A or FI-B. This document is intended to enable you to fully configure the customer environment and during this process, various steps require you to insert customer-specific naming conventions, IP addresses, and VLAN schemes, as well as to record appropriate MAC addresses.

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

Table 2 Necessary VLANs

VLAN Name	VLAN Purpose	ID Used in Validating This Document
Native	VLAN to which untagged frames are assigned	2
Mgmt out of band	VLAN for out-of-band management interfaces	3172
vMotion	VLAN designated for the movement of VMs from one physical host to another	3173
VM Traffic	VLAN for VM application traffic	3174
Mgmt in band	VLAN for in-band management interfaces	11

Table 3 Necessary VSANs

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

## Cisco UCS Central

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

## Virtual Machines

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

Table 4 Machine List

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

## Configuration Variables

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

Table 5 Customer Variables

Variable	Description	Customer Implementation Value
<<var_node01_mgmt_ip>>	Out-of-band management IP for V5000 node 01	
<<var_node01_mgmt_mask>>	Out-of-band management network netmask	
<<var_node01_mgmt_gateway>>	Out-of-band management network default gateway	
<<var_node02_mgmt_ip>>	Out-of-band management IP for V5000 node 02	
<<var_node02_mgmt_mask>>	Out-of-band management network netmask	
<<var_node02_mgmt_gateway>>	Out-of-band management network default gateway	
<<var_cluster_mgmt_ip>>	Out-of-band management IP for V5000 cluster	
<<var_cluster_mgmt_mask>>	Out-of-band management network netmask	
<<var_cluster_mgmt_gateway>>	Out-of-band management network default gateway	
<<var_password>>	Global default administrative password	
<<var_dns_domain_name>>	DNS domain name	
<<var_nameserver_ip>>	DNS server IP(s)	
<<var_timezone>>	VersaStack time zone (for example, America/New_York)	
<<var_global_ntp_server_ip>>	NTP server IP address	
<<var_email_contact>>	Administrator e-mail address	
<<var_admin_phone>>	Local contact number for support	
<<var_mailhost_ip>>	Mail server host IP	

Variable	Description	Customer Implementation Value
<<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	
<<var_native_vlan_id>>	Native 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_ucs_mgmt_mask>>	Out-of-band management network netmask	
<<var_ucs_mgmt_gateway>>	Out-of-band management network default gateway	

Variable	Description	Customer Implementation Value
<<var_ucs_cluster_ip>>	Cisco UCS Manager cluster IP address	
<<var_ucsb_mgmt_ip>>	Cisco UCS Fabric Interconnect (FI) B out-of-band management IP address	
<<var_cimc_mask>>	Out-of-band management network netmask	
<<var_cimc_gateway>>	Out-of-band management network default gateway	
<<var_ftp_server>>	IP address for FTP server	
<<var_UTC_offset>>	UTC time offset for your area	
<<var_vsan_a_id>>	VSAN id for FC fabric A ( 101 is used )	
<<var_vsan_b_id>>	VSAN id for FC fabric B ( 102 is used )	
<<var_fabric_a_fcoe_vlan_id>>	Fabric id for Fcoe A ( 101 is used )	
<<var_fabric_b_fcoe_vlan_id>>	Fabric id for Fcoe B ( 102 is used )	
<<var_In-band_mgmtblock_net>>	Block of IP addresses for KVM access for UCS	
<<var_vmhost_infra_01_ip>>	VMware ESXi host 01 in-band Mgmt IP	
<<var_vmotion_vlan_id_ip_host-01>>	vMotion VLAN IP address for ESXi host 01	
<<var_vmotion_vlan_id_mask_host-01>>	vMotion VLAN netmask for ESXi host 01	
<<var_vmhost_infra_02_ip>>	VMware ESXi host 02 in-band Mgmt IP	
<<var_vmotion_vlan_id_ip_host-02>>	vMotion VLAN IP address for ESXi host 02	
<<var_vmotion_vlan_id_mask_host-02>>	vMotion VLAN netmask for ESXi host 02	

Table 6 lists the Fibre Channel environment and these variables need to be collected during the installation phase for subsequent use in this document.

Table 6 WWPN Variables

Source	Switch/ Port	Variable	WWPN
FC_NodeA-fabricA	Switch A FC3	<<var_wwpn_FC_NodeA-fabricA>>	
FC_NodeA-fabricB	Switch B FC3	<<var_wwpn_FC_NodeA-fabricB>>	

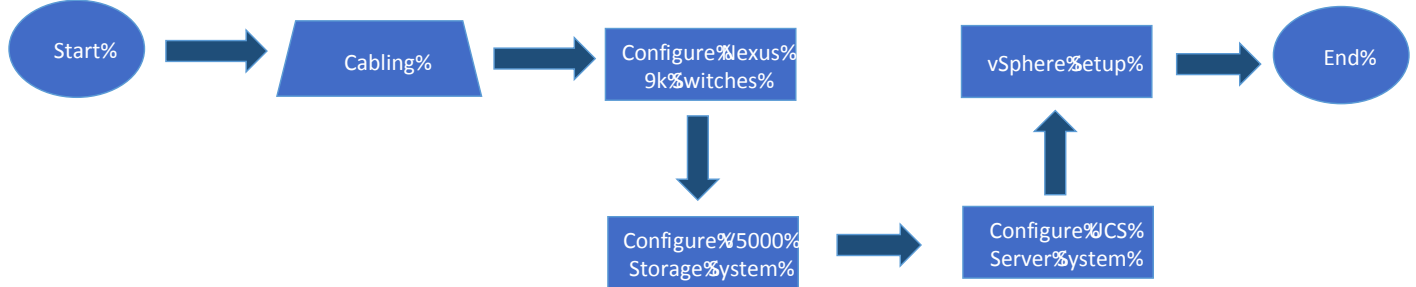


Source	Switch/ Port	Variable	WWPN
FC_NodeB-fabricA	Switch A FC4	<<var_wwpn_FC_NodeB-fabricA>>	
FC_NodeB-fabricB	Switch B FC4	<<var_wwpn_FC_NodeB-fabricB>>	
VM-Host-infra-01-A	Switch A	<<var_wwpn_VM-Host-Infra-01-A>>	
VM-Host-infra-01-B	Switch B	<<var_wwpn_VM-Host-Infra-01-B>>	
VM-Host-infra-02-A	Switch A	<<var_wwpn_VM-Host-Infra-02-A>>	
VM-Host-infra-02-B	Switch B	<<var_wwpn_VM-Host-Infra-02-B>>	

## VersaStack Cabling

Figure 2 illustrates the VersaStack build process

**Figure 2 VersaStack Build Process**



## VersaStack Cabling

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

The tables in this section contain details for the prescribed and supported configuration of the IBM Storwize V5030 running 7.7.1.3.

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



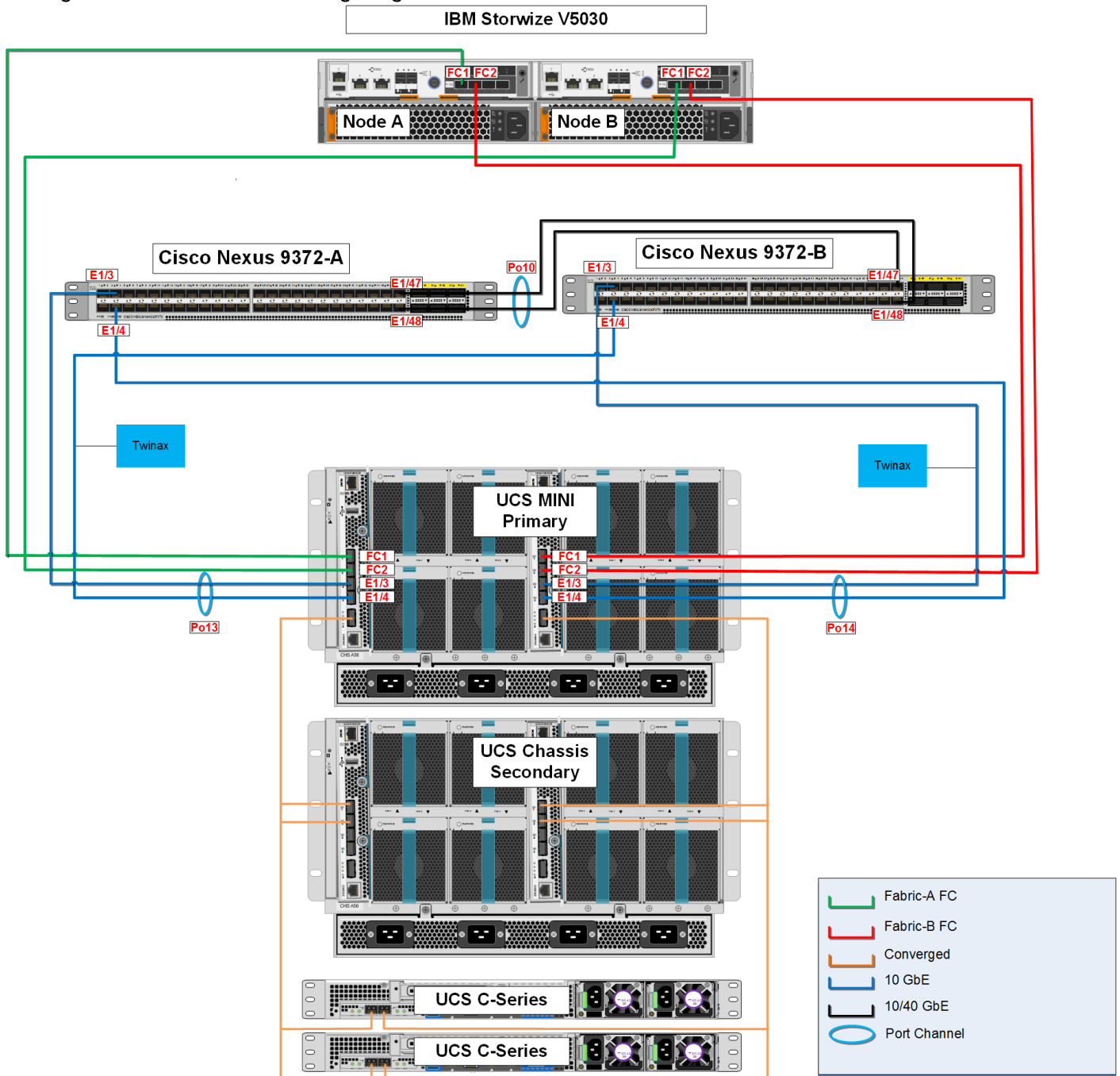
Be sure to follow the cabling directions in this section. Failure to do so will result in changes to the deployment procedures that follow because specific port locations are mentioned.

It is possible to order IBM Storwize V5030 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 3 illustrates the cabling diagrams for VersaStack configurations using the Cisco Nexus 9000 and IBM Storwize V5030. For SAS cabling information, the V5000 control enclosure and expansion enclosure should be connected according to the cabling guide at the following URL:

[http://www.ibm.com/support/knowledgecenter/STHGuj\\_7.4.0/com.ibm.storwize.v5000.740.doc/v3500\\_qisascables\\_b4jtyu.html?cp=STHGuj&lang=en](http://www.ibm.com/support/knowledgecenter/STHGuj_7.4.0/com.ibm.storwize.v5000.740.doc/v3500_qisascables_b4jtyu.html?cp=STHGuj&lang=en)

Figure 3 VersaStack Cabling Diagram



The tables below provide the details of 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	Eth1/3	10GbE	Cisco UCS fabric interconnect-A	Eth1/3

Local Device	Local Port	Connection	Remote Device	Remote Port
	Eth1/4	10GbE	Cisco UCS fabric interconnect-B	Eth1/4
	Eth1/47 *	40GbE	Cisco Nexus 9000-B	Eth1/47
	Eth1/48 *	40GbE	Cisco Nexus 9000-B	Eth1/48
	Eth1/36	10GbE	Management switch	Any

\* 40 GbE ports can be used in lieu of the 10GbE ports.

Table 8 Cisco Nexus 9000-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 9000-B	Eth1/3	10GbE	Cisco UCS fabric interconnect-B	Eth1/3
	Eth1/4	10GbE	Cisco UCS fabric interconnect-A	Eth1/4
	Eth1/47 *	10GbE	Cisco Nexus 9000-A	Eth1/47
	Eth1/48 *	10GbE	Cisco Nexus 9000-A	Eth1/48
	Eth1/36	10GbE	Management switch	Any

\* 40 GbE ports can be used in lieu of the 10GbE ports.

Table 9 IBM Storwize V5030 Controller Node-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
IBM Storwize V5030 Controller, Node-A	E1	GbE	Management switch	Any
	E2 (optional)	GbE	Management switch	Any
	FC1	8gbps	Cisco UCS fabric interconnect -A	FC1/1
	FC2	8gbps	Cisco UCS fabric interconnect -B	FC1/1

Table 10 IBM Storwize V5030 Controller Node-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
IBM Storwize V5030 Controller, Node-B	E1	GbE	Management switch	Any
	E2 (optional)	GbE	Management switch	Any

Local Device	Local Port	Connection	Remote Device	Remote Port
	FC1	8gbps	Cisco UCS fabric interconnect -A	FC1/2
	FC2	8gbps	Cisco UCS fabric interconnect -B	FC1/2

Table 11 Cisco UCS Fabric Interconnect A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect-A	Mgmt0	GbE	Management switch	Any
	FC1/1	8gbps	V5000 Node-A	FC1/1
	FC1/2	8gbps	V5000 Node-B	FC1/1
	Eth1/3	10GbE	Cisco Nexus 9000-A	Eth 1/3
	Eth1/4	10GbE	Cisco Nexus 9000-B	Eth 1/4
	Scalability 1	40 GbE	2 <sup>nd</sup> UCS Chassis	IOM 2208XP
		UCS C220 M4	1340 VIC port 1	

Table 12 Cisco UCS Fabric Interconnect B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect-B	Mgmt0	GbE	Management switch	Any
	FC1/1	8gbps	V5000 Node-A	FC1/2
	FC1/2	8gbps	V5000 Node-B	FC1/2
	Eth1/3	10GbE	Cisco Nexus 9000-B	Eth 1/3
	Eth1/4	10GbE	Cisco Nexus 9000-A	Eth 1/4
	Scalability 1	40 GbE	2 <sup>nd</sup> UCS Chassis	IOM 2208XP
		UCS C220 M4	1340 VIC port 2	

## Network Configuration

---

### Cisco Nexus 9000 Initial Configuration Setup

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



#### Cisco Nexus A

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



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

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

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

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

```
Enter the password for "admin":
```

```
Confirm the password for "admin":
```

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

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

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

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

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

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

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

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

```
Enter the switch name : <<var_nexus_A_hostname>>
```

```

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

```

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

## Cisco Nexus B

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



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

---

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

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

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

```
Enter the password for "admin":
```

```
Confirm the password for "admin":
```

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

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

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

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

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

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

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

```
Enter the switch name : <<var_nexus_B_hostname>>
```

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

```
Mgmt0 IPv4 address : <<var_nexus_B_mgmt0_ip>>
```

```
Mgmt0 IPv4 netmask : <<var_nexus_B_mgmt0_netmask>>
```

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

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

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

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

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

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

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



```

Configure the ntp server? (yes/no) [n]: y
  NTP server IPv4 address : <<var_global_ntp_server_ip>>
Configure default interface layer (L3/L2) [L2]:
Configure default switchport interface state (shut/noshut) [noshut]:
Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]:
The following configuration will be applied:
password strength-check
switchname <<var_nexus_B_hostname>>
vrf context management
ip route 0.0.0.0/0 <<var_nexus_B_mgmt0_gw>>
exit
  no feature telnet
ssh keyrsa 2048 force
  feature ssh
ntp server <<var_global_ntp_server_ip>>
system default switchport
  no system default switchport shutdown
  copp profile strict
interface mgmt0 ip address <<var_nexus_B_mgmt0_ip>><<var_nexus_B_mgmt0_netmask>>
no shutdown
Would you like to edit the configuration? (yes/no) [n]:
Use this configuration and save it? (yes/no) [y]:
[#####] 100% Copy complete.

```

## Enable Appropriate Cisco Nexus 9000 Features and Settings

### Cisco Nexus 9000 A and Cisco Nexus 9000 B

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

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

```
config terminal
```

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

```
feature lacp
```

```
feature vpc
feature interface-vlan
```

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

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

## Create VLANs for VersaStack 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:

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

```
vlan <<var_ib-mgmt_vlan_id>>
name IB-MGMT-VLAN
vlan <<var_native_vlan_id>>
name Native-VLAN
vlan <<var_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

To configure vPC domain for switch A, complete the following steps:

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

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

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

```
role priority 10
```

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

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

4. Enable the following features for this vPC domain:

```
peer-switch
delay restore 150
peer-gateway
ip arp synchronize
auto-recovery
copy run start
```

## Cisco Nexus 9000 B

To configure the vPC domain for switch B, complete the following steps:

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

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

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

```
role priority 20
```

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

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

4. Enable the following features for this vPC domain:

```
peer-switch
delay restore 150
peer-gateway
ip arp synchronize
auto-recovery
copy run start
```

## Configure Network Interfaces for the vPC Peer Links

To configure the network interfaces for the vPC Peer links, complete the following steps:

## Cisco Nexus 9000 A

1. Define a port description for the interfaces connecting to vPC Peer <<var\_nexus\_B\_hostname>>.

```
interface Eth1/47
description VPC Peer <<var_nexus_B_hostname>>:1/47
interface Eth1/48
description VPC Peer <<var_nexus_B_hostname>>:1/48
```

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

```
interface Eth1/47,Eth1/48
channel-group 10 mode active
no shutdown
```

3. Define a description for the port-channel connecting to <<var\_nexus\_B\_hostname>>.

```
interface Po10
description vPC peer-link
```

4. Make the port-channel a switchport, and configure a trunk to allow in-band management, VM traffic, vMotion 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_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 Eth1/47
description VPC Peer <<var_nexus_A_hostname>>:1/47
interface Eth1/48
description VPC Peer <<var_nexus_A_hostname>>:1/48
```

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

```
interface Eth1/47,Eth1/48
channel-group 10 mode active
no shutdown
```

3. Define a description for the port-channel connecting to <<var\_nexus\_A\_hostname>>.

```
interface Po10
description vPC peer-link
```

4. Make the port-channel a switchport, and configure a trunk to allow in-band management, VM traffic, vMotion 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_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, VM traffic, vMotion 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_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 Eth1/3
```

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

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

```
channel-group 13 force mode active
```

```
no shutdown
```

8. Define a description for the port-channel connecting to <<var\_ucs\_clustername>>-B.

```
interface Po14
```

```
description <<var_ucs_clustername>>-B
```

9. Make the port-channel a switchport, and configure a trunk to allow in-band management, VM traffic, vMotion 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_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 Eth1/4
description <<var_ucs_clustername>>-B:1/4
```

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

```
channel-group 14 force mode active
no shutdown
copy run start
```

## 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, VM traffic, vMotion 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_vmotion_vlan_id>>, <<var_vm_traffic_vlan_id>>
```

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

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

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

```
mtu 9216
```

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

```
vpc 14
no shutdown
```

6. Define a port description for the interface connecting to <<var\_ucs\_clustername>>-B.

```
interface Eth1/3
description <<var_ucs_clustername>>-B:1/3
```

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

```
channel-group 14 force mode active
```

```
no shutdown
```

- Define a description for the port-channel connecting to <<var\_ucs\_clustername>>-A.

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

- Make the port-channel a switchport, and configure a trunk to allow in-band management, VM traffic, vMotion 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_vmotion_vlan_id>>, <<var_vm_traffic_vlan_id>>,
```

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

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

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

```
mtu 9216
```

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

```
vpc 13
no shutdown
```

- Define a port description for the interface connecting to <<var\_ucs\_clustername>>-A.

```
interface Eth1/4
description <<var_ucs_clustername>>-A:1/4
```

- 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 uplinks to your separate management switch. There are two examples shown below. These examples are provided to help show the methods about how the configuration could be setup, however, since networking configurations can vary, it is recommended that you consult your local network personnel for the optimal configuration. In the first example provided in this section, a single switch is top of rack and the Cisco Nexus 9000 series switches are both connected to it through its ports 36. The Cisco 9k switches use a 1 gig SFP to convert the



connected to Cat-5 copper connecting to the top of rack switch, however, connection types can vary. **The 9k's are configured with the interface-vlan option** and each 9k switch has a unique IP for its VLAN. The traffic required to route from the 9k is the in-band management traffic, so use the VLAN 11 and set the port to access mode. The top of rack switch also has its ports set to access mode. The second example shows how to leverage port channel, which maximizes upstream connectivity. In the second example, the top of rack switch must have the port channel configured for the port connected from the downstream switch.

## Cisco Nexus 9000 A and B Using Interface VLAN Example 1

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

### Cisco Nexus 9000 A

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

### Cisco Nexus 9000 B

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

```
ip route 0.0.0.0/0 <<var_inband_mgmt_gateway>>
copy run start
```

## Cisco Nexus 9000 A and B using Port Channel Example 2

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

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

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

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

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

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

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

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

```
vpc 9
no shutdown
```

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

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

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

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

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

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

## Storage Configuration

---

### IBM Storwize V5030

Configuring the IBM Storwize V5000 Second Generation is a two-stage setup. The technician port (T) will be used for the initial configuration and IP assignment, and the management GUI will be used to complete the configuration. For a more in-depth look at installing the IBM Storwize V5000 Second Generation hardware, please refer to the excellent Redbook publication: Implementing the IBM Storwize V5000 Gen2.

#### Prerequisites

Begin this procedure only after the physical installation of the IBM Storwize V5000 has been completed. The computer used to initialize the IBM Storwize V5000 must have an Ethernet cable connecting the personal computer to the technician to the IBM Storwize V5000 as well as a supported browser installed. At the time of writing, the following browsers or later are supported with the management GUI; Firefox 32, Internet Explorer 10 and Google Chrome 37. 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. On the 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.



**Attention:** Do not connect the technician port to a switch. If a switch is detected, the technician port connection might shut down, causing a 746 node error.

---

### IBM Storwize V5000 Initial Configuration

The initialization procedure must be run after your system has been racked, cabled, and powered on. To complete this process, you will need access to your powered on V5000 system, the USB flash drive that was shipped with your system, the network credentials of your system, and a personal computer.

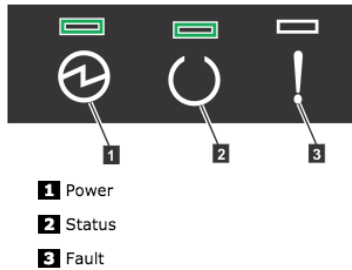
1. Power on the IBM Storwize V5000 control enclosure. Use the supplied power cords to connect both power supply units. The enclosure does not have power switches.



If you have expansion enclosures, you must power these on before powering on the control enclosure.

---

2. From the rear of the control enclosure, check the LEDs on each node canister. The canister is ready with no critical errors when Power is illuminated, Status is flashing, and Fault is off. See the figure below for reference.



3. Configure an Ethernet port, on the computer used to connect to the control enclosure, to enable Dynamic Host Configuration Protocol (DHCP) configuration of its IP address and DNS settings.
4. If you do not have DHCP, you must manually configure the personal computer. Specify the static IPv4 address 192.168.0.2, subnet mask 255.255.255.0, gateway 192.168.0.1, and DNS 192.168.0.1.
5. Locate the Ethernet port that is labelled T on the rear of the IBM Storwize V5000 node canister. On IBM Storwize V5010 and Storwize V5020 systems, the second on-board 1 Gbps Ethernet port is initially used as the technician port. For the IBM Storwize V5030 system, there is a dedicated technician port. Refer to the appropriate figures below that show the location of the technician port ( T ) on each model.

Figure 4 IBM Storwize V5010



Figure 5 IBM Storwize V5020



Figure 6 IBM Storwize V5030



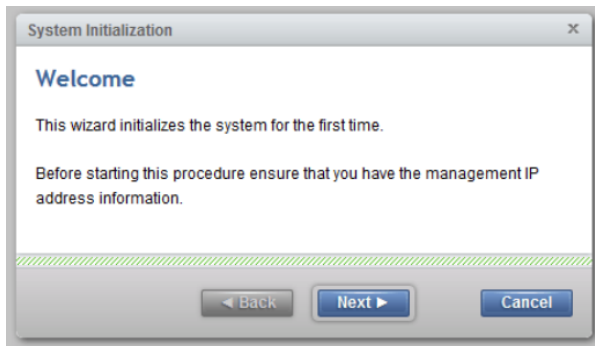
6. Connect an Ethernet cable between the port of the computer that is configured in step 3 and the technician port. After the connection is made, the system will automatically configure the IP and DNS settings for the personal computer if DHCP is available. If it is not available, the system will use the values you provided.

7. After the Ethernet port of the personal computer is connected, open a supported browser and browse to address `http://install`. (If you do not have DHCP, open a supported browser and go to the following static IP address `192.168.0.1`). The browser is automatically directed to the initialization tool.

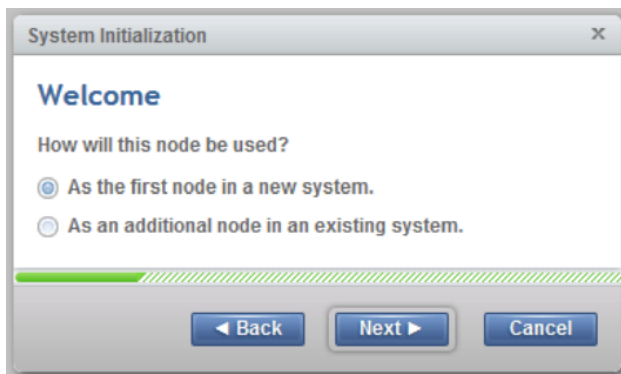


If you experience a problem when you try to connect due to a change in system states, wait 5 - 10 seconds and then try again.

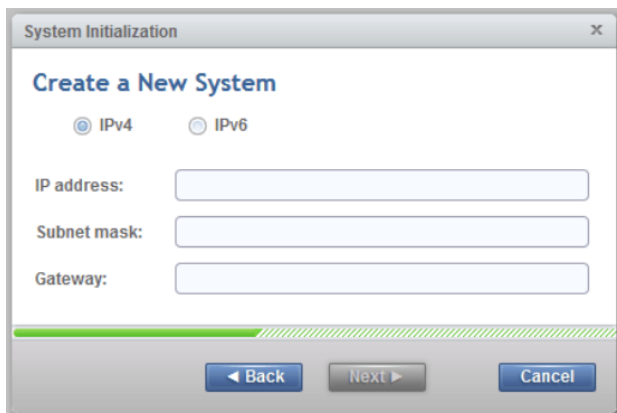
---



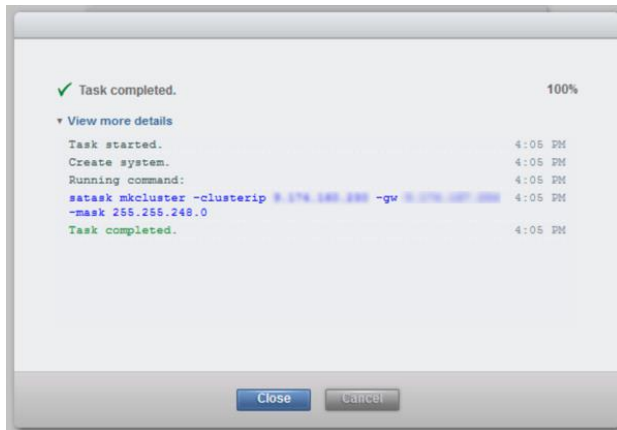
8. Click Next on the System Initialization welcome message.



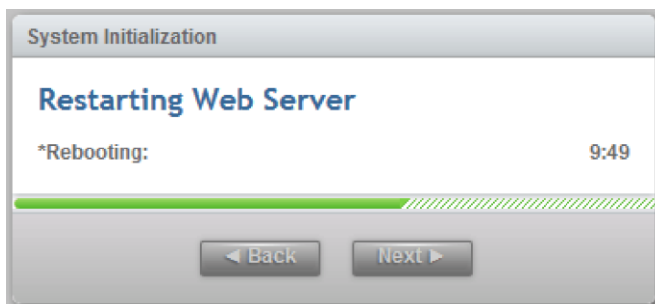
9. Click Next to continue with As the first node in a new system.



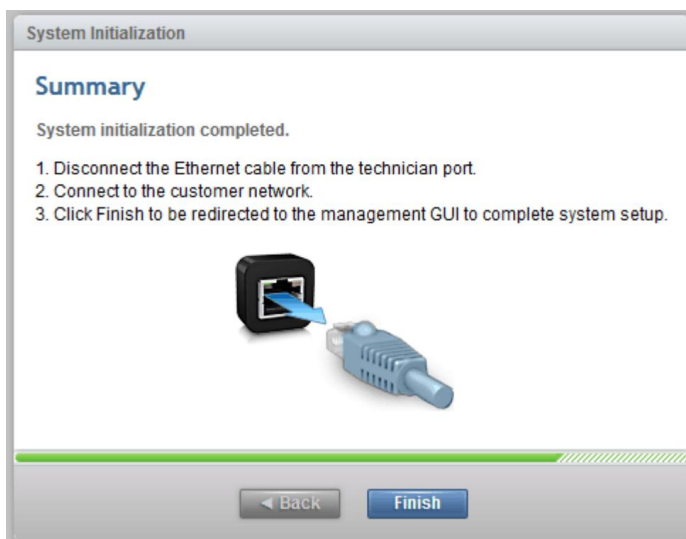
10. Complete all of the fields with the networking details for managing the system. This will be referred to as the System or Cluster IP address. Click Next.



11. The setup task completes and you are provided a view of the generated *safask* CLI command as show above. Click Close. The storage enclosure will now reboot.



12. The system takes approximately 10 minutes to reboot and reconfigure the Web Server. After this time, click Next to proceed to the final step.



13. After you complete the initialization process, disconnect the cable between the computer and the technician port, as instructed above. Re-establish the connection to the customer network

and click Finish to be redirected to the management address that you provided to configure the system initially.

## IBM Storwize V5000 GUI Setup

After completing the initial tasks above, we are ready to launch the management GUI, and configure the IBM Storwize V5000 system.



e-Learning modules introduce the IBM Storwize V5000 management interface and provide an overview of the system setup tasks, including configuring the system, migrating and configuring storage, creating hosts, creating and mapping volumes, and configuring email notifications. You can find e-Learning modules here: [Getting Started](#)

To setup IBM Storwize V5000, complete the following steps:

1. Log in to the management GUI using the previously configured cluster IP address <<var\_cluster\_mgmt\_ip>>.



2. Read and accept the license agreement. Click Accept.

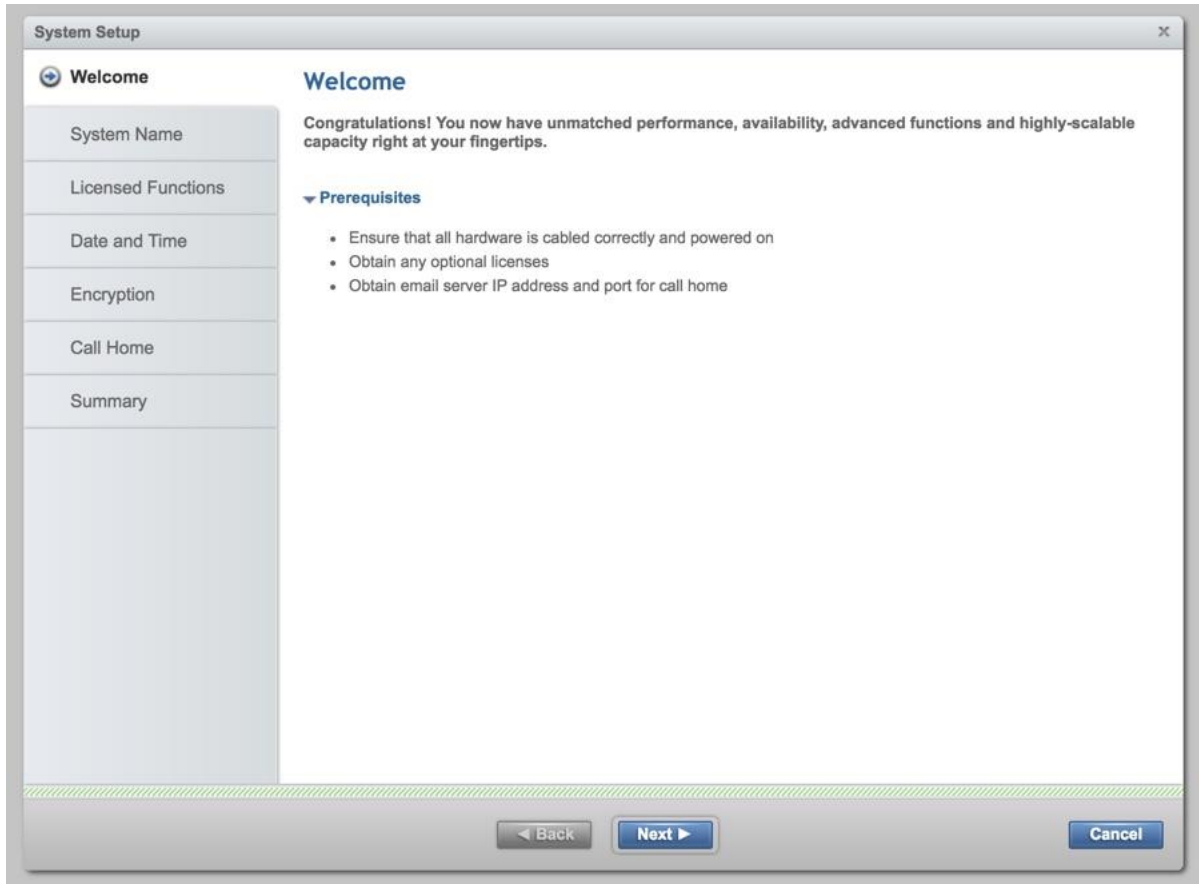


3. Login as superuser with the password of passw0rd. Click Log In.

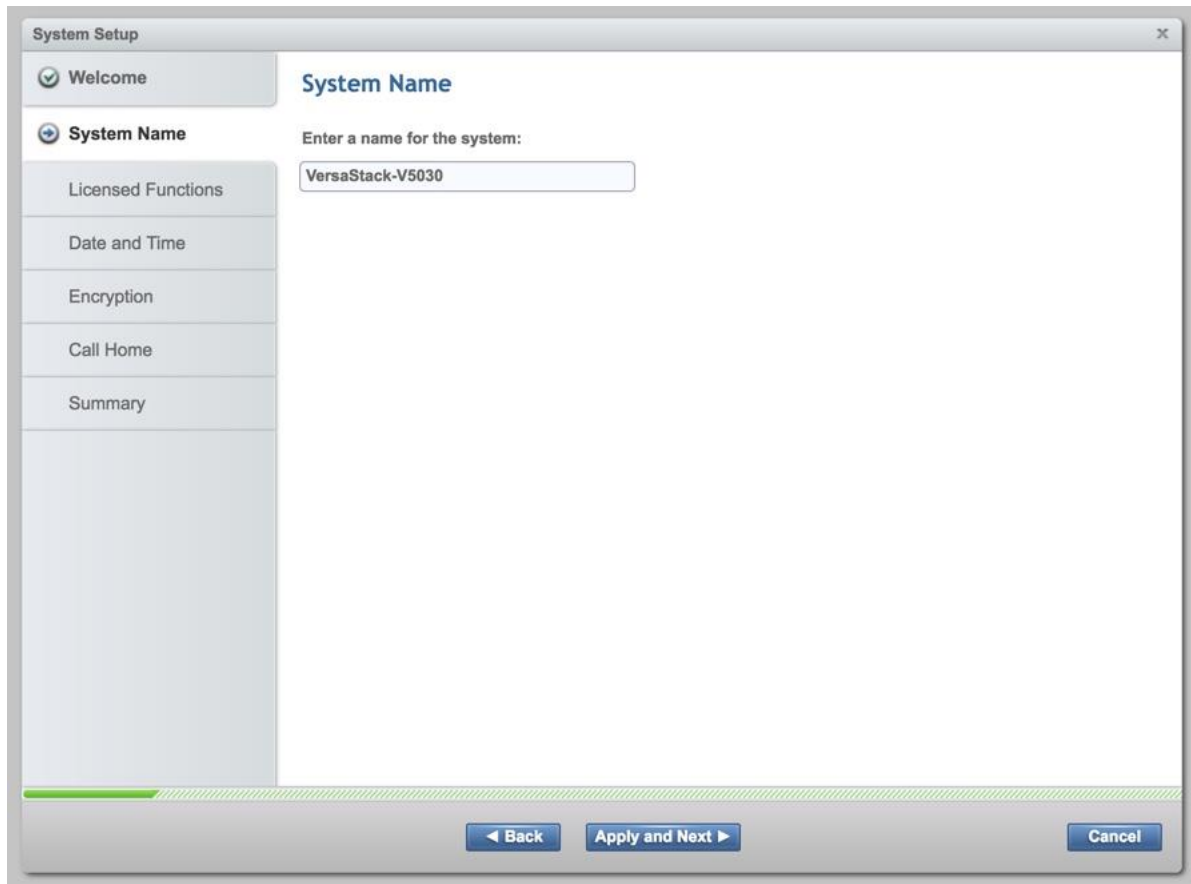


4. You will be prompted to change the password for superuser. Make a note of the password and then click Log In.





5. On the Welcome to System Setup screen click Next.



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

The screenshot shows a 'System Setup' window with a sidebar on the left containing the following options: Welcome, System Name, Licensed Functions (selected), Date and Time, Encryption, Call Home, and Summary. The main area is titled 'Licensed Functions' and contains the following text: 'Additional licenses are required to use certain system functions. For auditing purposes, retain the license agreement for proof of compliance.' Below this text are four rows of configuration options, each with a text label, a numeric input field, and a label 'Number of enclosures':

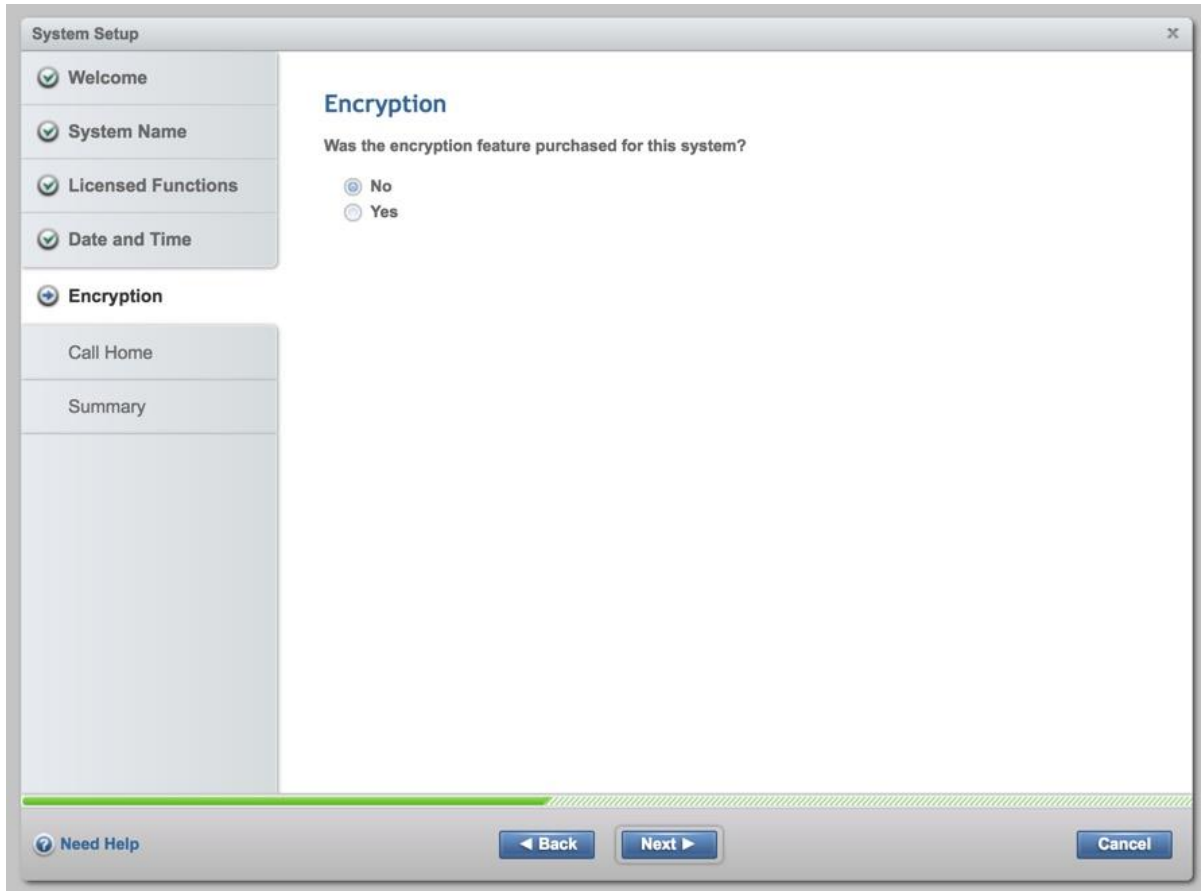
Function	Value	Label
FlashCopy:	1	Number of enclosures
Remote Mirroring:	0	Number of enclosures
Easy Tier:	1	Number of enclosures
External Virtualization:	0	Number of enclosures

At the bottom of the window, there are three buttons: 'Need Help', 'Back', and 'Apply and Next', followed by a 'Cancel' button on the right.

7. Select the license that was purchased, and enter the number of enclosures that will be used for FlashCopy, Remote Mirroring, Easy Tier, and External Virtualization. Click Apply and Next to proceed.

The screenshot shows a 'System Setup' window with a sidebar on the left containing the following menu items: Welcome, System Name, Licensed Functions, Date and Time (selected), Encryption, Call Home, and Summary. The main content area is titled 'Date and Time' and includes the following text: 'Select time and date settings. You can enter these settings manually or specify a Network Time Protocol (NTP) server to synchronize time on the system.' Below this text are two radio buttons: 'Manually' (unselected) and 'NTP Server' (selected). There are two input fields: 'IP address:' with a red asterisk icon and an empty text box, and 'Time Zone:' with a dropdown menu showing '(GMT) Dublin, Edinburgh, London, Lisbon'. At the bottom of the window are three buttons: 'Back', 'Apply and Next', and 'Cancel'.

8. Configure the date and time settings, inputting NTP server details `<<var_global_ntp_server_ip>>` if you have one. Click Apply and Next to proceed.



9. If you have purchased the Encryption feature and wish to enable it, do so here. Click Next to proceed.



It is highly recommended that you configure email event notifications, which automatically notify IBM support centers when problems occur.

---

The screenshot shows a 'System Setup' dialog box with a sidebar on the left and a main content area. The sidebar contains a list of steps: 'Welcome', 'System Name', 'Licensed Functions', 'Date and Time', 'Encryption', 'Call Home', 'System Location', 'Contact', and 'Email Servers'. The 'System Location' step is currently selected and expanded. The main content area is titled 'System Location' and contains a note: 'Service parts should be shipped to the same physical location as the system.' Below this note are several input fields: 'Company name' (text box with 'IBM UK'), 'System address' (text box with 'Hursley Park'), 'City' (text box with 'Winchester'), 'State or province' (text box with 'XX'), 'Postal code' (text box with 'SO21 2JN'), 'Country or region' (dropdown menu with 'United Kingdom'), and 'Comment' (text box with 'Hursley Labs'). At the bottom of the dialog box are three buttons: 'Back', 'Next', and 'Cancel'.

**System Setup**

- ✓ Welcome
- ✓ System Name
- ✓ Licensed Functions
- ✓ Date and Time
- ✓ Encryption
- Call Home
  - System Location
  - Contact
  - Email Servers
- Summary

### System Location

Service parts should be shipped to the same physical location as the system.

Company name:

System address:

City:

State or province:

Postal code:

Country or region:

Comment:

◀ Back   Next ▶   Cancel

10. Enter the complete company name and address details <<var\_org>> <<var\_street\_address>>, <<var\_city>> <<var\_state>> <<var\_zip>> <<var\_country\_code>>, then click Next.

**System Setup** [x]

- ✓ Welcome
- ✓ System Name
- ✓ Licensed Functions
- ✓ Date and Time
- ✓ Encryption
- **Call Home**
  - ✓ System Location
  - **Contact**
  - Email Servers

Summary

### Contact

The support center contacts this person to resolve issues on the system.

Name:

Email:

Phone (primary):

Phone (alternate):

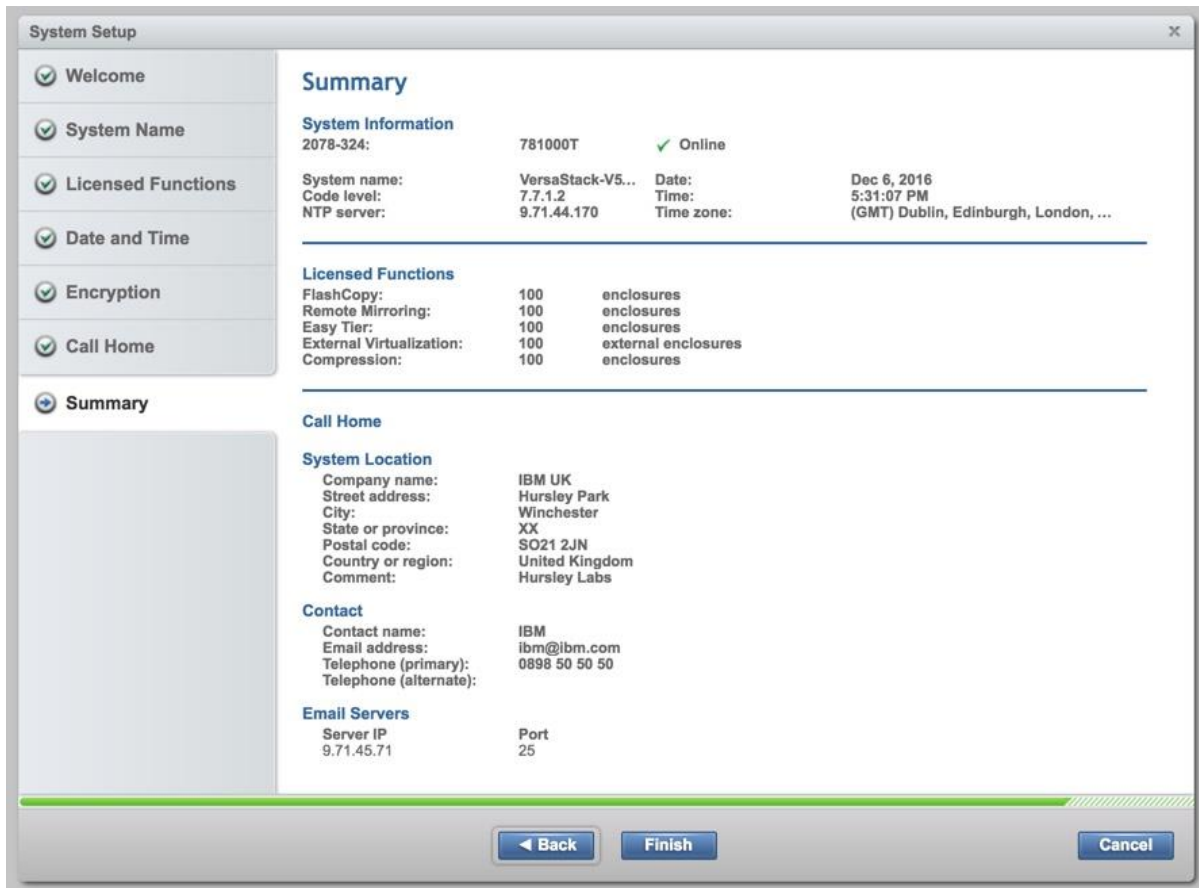
◀ Back    Apply and Next ▶    Cancel

11. Enter the information for the person at your company whom the support centres should contact <<var\_contact\_name>> <<var\_email\_contact>> <<var\_admin\_phone>>. click Apply and Next.

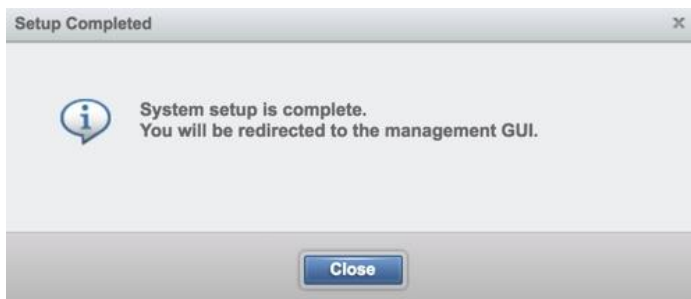
The screenshot shows a 'System Setup' window with a sidebar on the left and a main configuration area on the right. The sidebar contains a list of setup steps: Welcome, System Name, Licensed Functions, Date and Time, Encryption, Call Home, and Summary. Under 'Call Home', 'System Location' and 'Contact' are checked, and 'Email Servers' is selected with a right-pointing arrow. The main area is titled 'Email Servers' and contains the text: 'Call home and event notifications are routed through this email server.' Below this, there are two input fields: 'Server IP:' with the value '9.71.45.71' and a green checkmark, and 'Port:' with the value '25' and increment/decrement buttons. A 'Ping' button is located below the IP field. At the bottom of the main area, there is a checkbox labeled 'Set up call home later'. The bottom of the window features a 'Need Help' link, 'Back' and 'Apply and Next' buttons, and a 'Cancel' button.

12. Enter the IP address `<<var_mailhost_ip>>` and server port for one or more of the email servers that you are providing for the Call Home email notification. Click Apply and Next.





13. Review the final summary page, and click Finish to complete the System Setup wizard.



14. Setup Complete. Click Close.



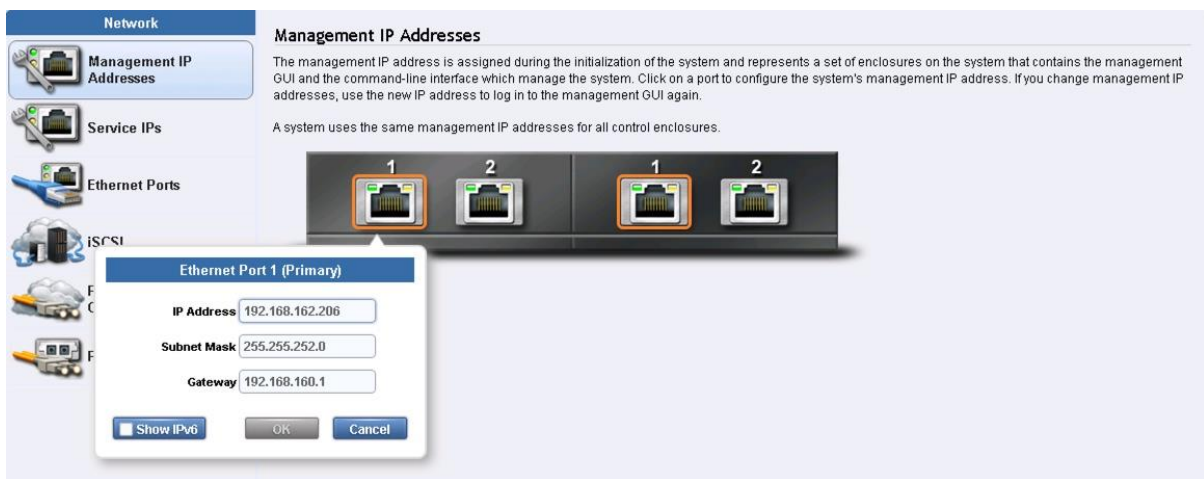
15. You will now presented with the System view of your IBM Storwize V5000, as depicted above.



16. In the left side menu, hover over each of the icons on the Navigation Dock to become familiar with the options.



17. Select the Setting icon from the Navigation Dock and choose Network.



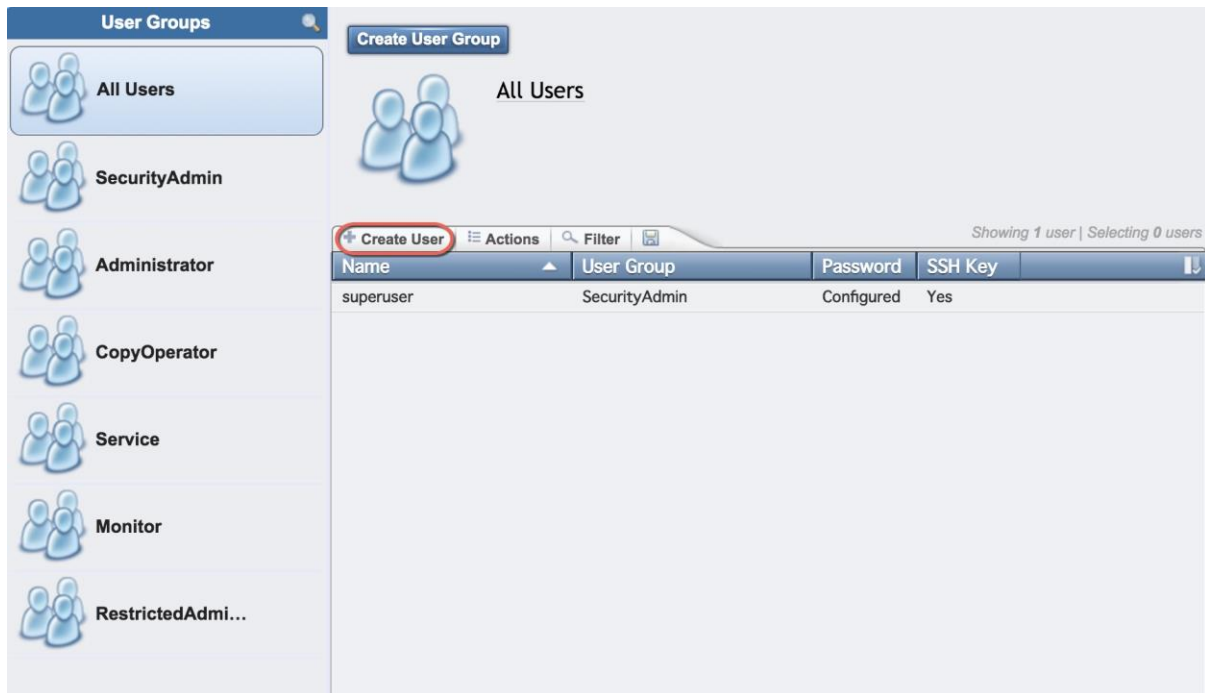
18. On the Network screen, highlight the Management IP Addresses section. Then click the number 1 interface on the left-hand side to bring up the Ethernet port IP menu. Change the IP address if necessary and click OK. If you are applying changes to the interface you are currently connected to, the application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



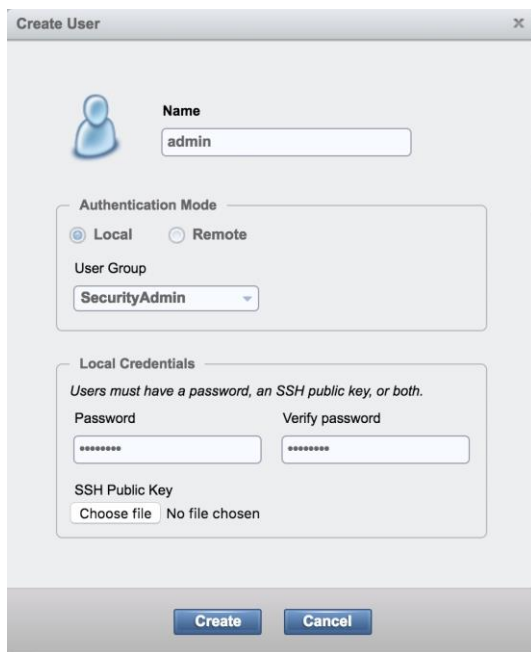
19. While still on the Network screen, select 1) 'Service IP Addresses' from the list on the left and 2) Node Canister 'left' then 3) change the IP address for port 1, click OK.
20. Repeat this process for port 1 on Node Canisters right (and port 2 left/right if you have cabled those ports)



21. Click the Access icon from the Navigation Dock on the left and select Users to access the Users screen.



22. Select Create User.



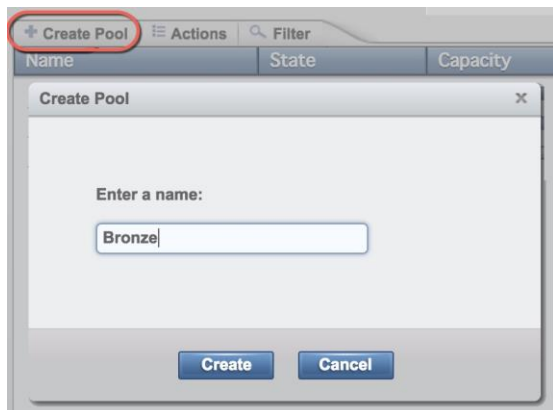
23. Enter a new name for an alternative admin account. Leave the 'SecurityAdmin' default as the User Group, and input the new password, then click Create. Optionally, if you have generated an SSH Public Key on a Unix server through the command "ssh-keygen -t rsa" and copied that public key file to an accessible location, you can choose to associate it for this user through the Choose File button.



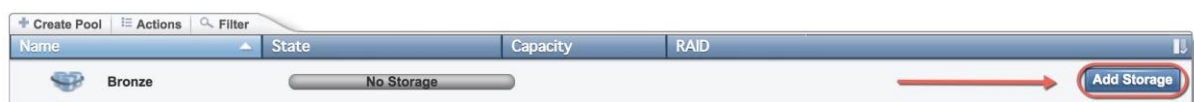
24. Logout from the superuser account and log back in as the new account you created.



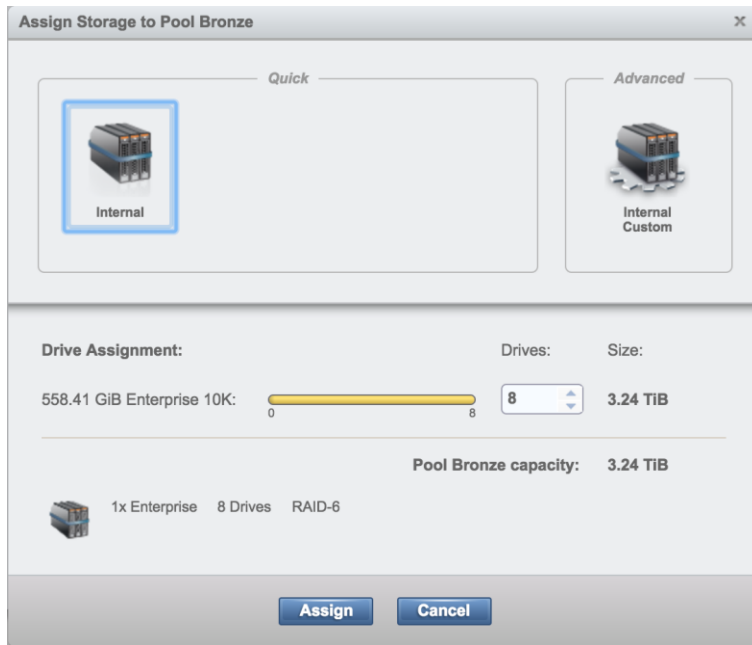
25. Select Pools from the Navigation Dock and select MDisk by Pools.



26. Click Create Pool, and enter the name of the new storage pool. Click Create.



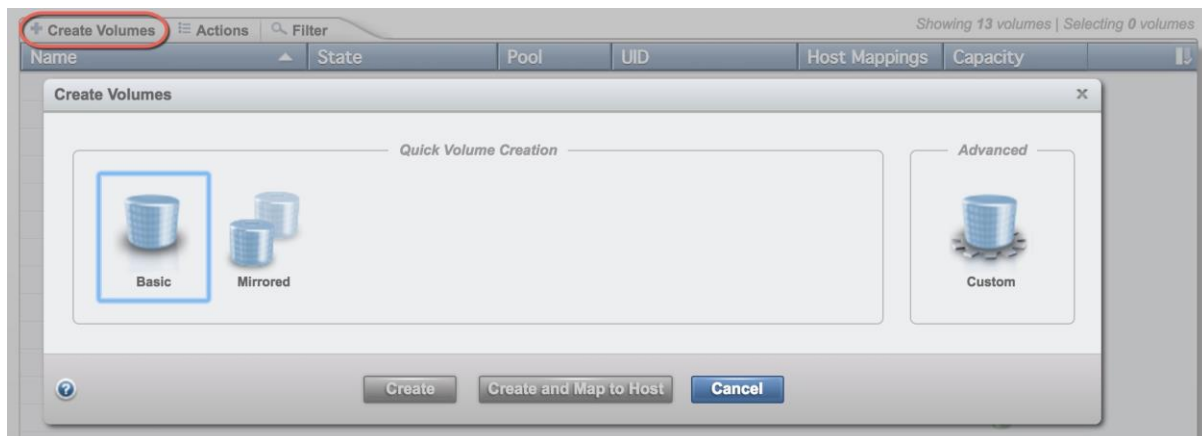
27. Select 'Add Storage'.



28. Select Internal, review the drive assignments and then select Assign. Depending on your configuration, you may want to use 'Internal Custom' to manually create tired storage pools, grouping together disk by capabilities.



29. Select Volumes from the Navigation Dock and then select Volumes.




30. Click Create Volumes.


**Create Volumes** ✕

---

*Quick Volume Creation*




Basic



Mirrored

*Advanced*




Custom

---

**Pool:** Bronze Total 3.24 TiB

**Quantity:** 2 **Capacity:** 40 **GiB** **Capacity savings:** Thin-provisioned **Name:** VM-Host-Infra-0 1 - 2 ⊕

**I/O group:** Automatic



**Summary**  
**2 volumes**  
**Volume range: VM-Host-Infra-01-VM-Host-Infra-02**  
**2 volumes in pool Bronze**  
**Caching I/O group: Automatic**  
**Accessible I/O group: Automatic**  
**Total real capacity: 1.60 GiB**  
**Total virtual capacity: 80.00 GiB**

Create
Create and Map to Host
Cancel

31. Select a pre-set that you want for the ESXi boot volume. Select the storage pool you've just created, and select I/O group Automatic. Input quantity 2, capacity 40GB, desired capacity savings and name VM-Host-Infra-0. Additionally, change the starting ID to 1. Click Create and then click Close.



**Create Volumes**

Quick Volume Creation

Basic Mirrored

Advanced

Custom

Pool: **Bronze** Total 3.24 TiB

Quantity: **1** Capacity: **500 GiB** Capacity savings: **Thin-provisioned** Name: **infra\_datastore\_1**

I/O group: **Automatic**

**Summary**

1 volume  
Volume name: infra\_datastore\_1

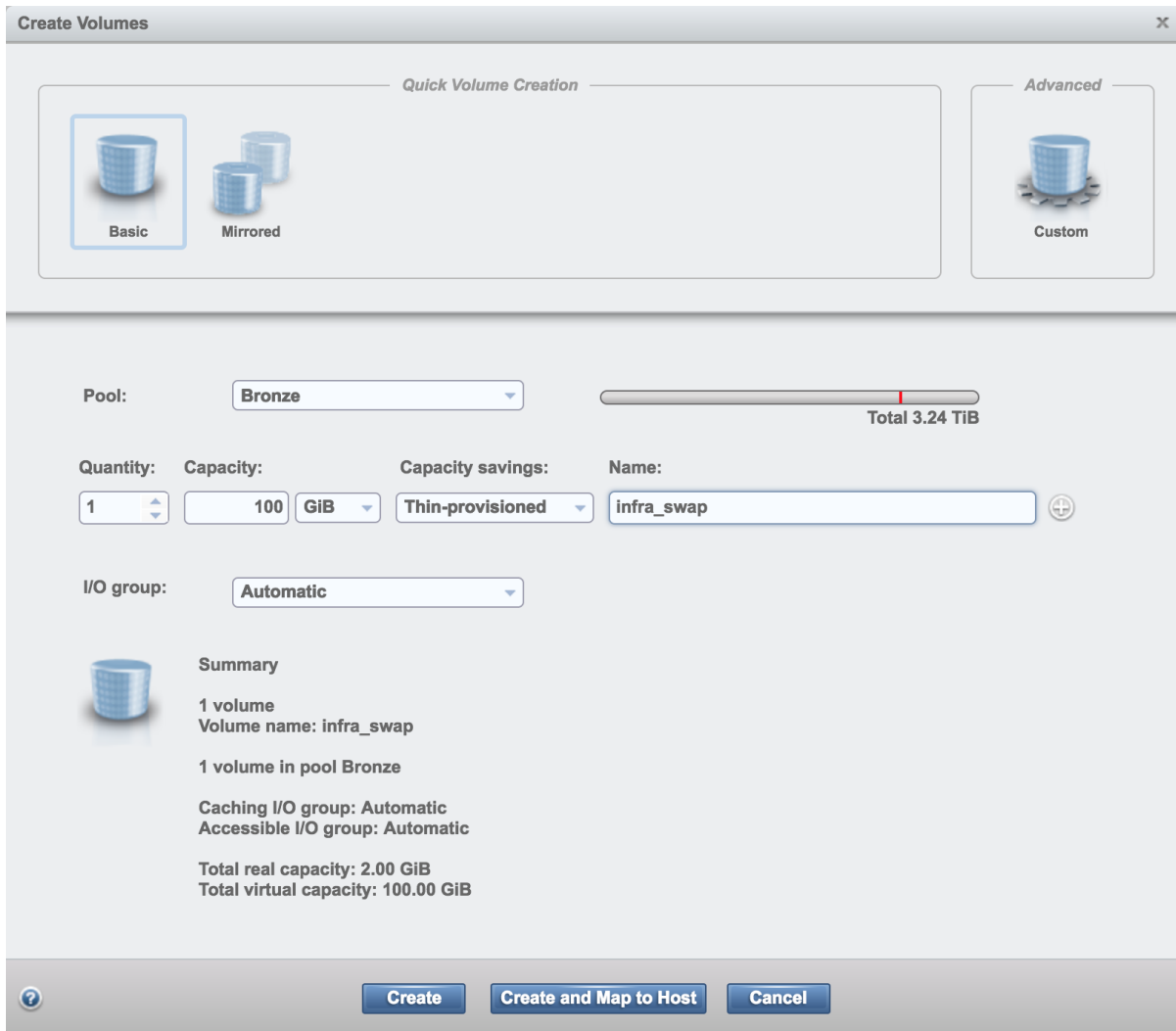
1 volume in pool Bronze

Caching I/O group: Automatic  
Accessible I/O group: Automatic

Total real capacity: 10.00 GiB  
Total virtual capacity: 500.00 GiB

**Create** **Create and Map to Host** **Cancel**

32. Click Create, to create volume again, select the storage pool, capacity savings and I/O group. Enter quantity 1, capacity 500GB, and name infra\_datastore\_1. Click Create and then click Close.



33. Click Create, to create volume again, select the storage pool, capacity savings and I/O group. Enter quantity 1, capacity 100GB, and name infra\_swap. Click Create and then click Close.

Name	State	Capacity	Pool	Host Mappings	UUID
VM-Host-Infra-01	✓ Online	40.00 GiB	mdiskgrp0	No	6005076300818A3F7800000000000000
VM-Host-Infra-02	✓ Online	40.00 GiB	mdiskgrp0	No	6005076300818A3F7800000000000001
infra_datastore_1	✓ Online	500.00 GiB	mdiskgrp0	No	6005076300818A3F7800000000000002
infra_swap	✓ Online	100.00 GiB	mdiskgrp0	No	6005076300818A3F7800000000000003

34. Validate the volumes created.



35. To Collect the WWPN for LUN mapping, select Settings from the Navigation Dock, then Network.



36. Select the Fibre Channel Ports in the Network column and then expand the FC port 1 ID 1 to display the WWPN ID's for Nodes 1 and 2. Input the WWPN ID's in a table for later use. Repeat this step for FC port 2 ID 2 Nodes 1 and 2.

Table 13 IBM V5030 – WWPN Information

Source	Switch/ Port	Variable	WWPN
FC_NodeA-fabricA	Fabric Interconnect A FC1	var_wwpn_FC_NodeA-fabricA	
FC_NodeA-fabricB	Fabric Interconnect B FC2	var_wwpn_FC_NodeA-fabricB	
FC_NodeB-fabricA	Fabric Interconnect A FC1	var_wwpn_FC_NodeB-fabricA	
FC_NodeB-fabricB	Fabric Interconnect B FC2	var_wwpn_FC_NodeB-fabricB	

## Cisco UCS Compute Configuration

---

### VersaStack Cisco UCS Initial Setup

This section provides 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 Fabric Interconnect 6324 A

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

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

```

Enter the configuration method: console

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

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

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

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

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

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

(yes/no) [n]: y

Which switch fabric (A|B): A

Enter the system name: <<var_ucs_clustertype>>

Physical switch Mgmt0 IPv4 address: <<var_ucsa_mgmt_ip>>

Physical switch Mgmt0 IPv4 netmask: <<var_ucsa_mgmt_mask>>

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

Cluster IPv4 address: <<var_ucs_cluster_ip>>

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

DNS IPv4 address: <<var_nameserver_ip>>

Configure the default domain name? y

Default domain name: <<var_dns_domain_name>>

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

```

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

## Cisco UCS Fabric Interconnect 6324 B

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

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

```
Enter the configuration method: console
```

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

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

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

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

## VersaStack Cisco UCS Base Setup

### Log in to Cisco UCS Manager

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

1. Open a web browser and navigate to the Cisco UCS 6324 Fabric Interconnect cluster address.
2. Select the HTML Launch UCS Manager option. In this document, we will use the HTML option.
3. If prompted to accept security certificates, accept as necessary.
4. When prompted, enter admin as the user name and enter the administrative password.  
<<var\_password>>
5. Click Login to log in to Cisco UCS Manager.
6. Enter the information for the Anonymous Reporting if desired and click OK.

## Anonymous Reporting

Cisco Systems, Inc. will be collecting feature configuration and usage statistics which will be sent to Cisco Smart Call Home server anonymously. This data helps us prioritize the features and improvements that will most benefit our customers.

If you decide to enable this feature in future, you can do so from the " Anonymous Reporting" in the Call Home settings under the Admin tab.

[View Sample Data](#)

**Do you authorize the disclosure of this information to Cisco Smart CallHome?**

Yes  No

Don't show this message again.

OK

Cancel

## Upgrade Cisco UCS Manager Software to Version 3.1(2c)

This document assumes the use of Cisco UCS Manager Software version 3.1(2c). To upgrade the Cisco UCS Manager software and the Cisco UCS 6324 Fabric Interconnect software to version 3.1(2c), refer to the Cisco UCS Manager Install and Upgrade Guides.

## Add Block of IP Addresses for Out-of-band KVM Access

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



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

---

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Pools > root > IP Pools > IP Pool ext-mgmt.
3. In the Actions pane, select Create Block of IPv4 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.

The screenshot shows the Cisco UCS Manager interface. On the left is a navigation pane with categories: Equipment, Servers, LAN, SAN, and VM. Under Servers, the path is: All > Pools > root > IP Pools > IP Pool ext-mgmt. The main content area is titled "LAN / Pools / root / IP Pools / IP Pool ext-mgmt" and has tabs for General, IP Addresses, IP Blocks, Faults, and Events. The "General" tab is active, showing "Actions" (Delete, Create Block of IPv4 Addresses, Create Block of IPv6 Addresses, Create DNS Suffix, Create IPv4 WINS Server, Show Pool Usage) and "Properties" (Name: ext-mgmt, Description: [empty], GUID: 00000000-0000-0000-0000-000000000000, Size: 15, Assigned: 13, Assignment Order: Default [selected] / Sequential).

## 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.

The screenshot shows the Cisco UCS Manager interface for Timezone Management. The navigation pane shows: All > Time Zone Management > Timezone. The main content area is titled "All / Time Zone Management / Timezone" and has tabs for General and Events. The "General" tab is active, showing "Actions" (Add NTP Server) and "Properties" (Time Zone: [ca/New\_York (Eastern Time)]). Below the properties is a table for "NTP Servers" with columns for Name and a "No data available" message. At the bottom, there are buttons for Add, Delete, and Info.

## Configure UCS Servers

### Edit Chassis Discovery Policy

Setting the discovery policy simplifies the extension of Cisco UCS Mini chassis. To modify the chassis discovery policy, complete the following steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane and select Equipment in the list on the left under the pulldown.
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 Primary chassis to the Secondary Chassis.
4. Set the Rack Server Discovery Policy to Immediate.

**Equipment**

Main Topology View Fabric Interconnects Servers Thermal Decommissioned Firmware Management **Policies** Faults

Global Policies Autoconfig Policies Server Inheritance Policies Server Discovery Policies SEL Policy Power Groups

---

**Chassis/FEX Discovery Policy**

Action : 2 Link ▾

Link Grouping Preference :  None  Port Channel

Multicast Hardware Hash :  Disabled  Enabled

---

**Rack Server Discovery Policy**

Action :  Immediate  User Acknowledged

Scrub Policy : <not set> ▾

---

**Rack Management Connection Policy**

Action :  Auto Acknowledged  User Acknowledged

---

**Power Policy**

Redundancy :  Non Redundant  N+1  Grid

---

**MAC Address Table Aging**

[Save Changes](#) [Reset Values](#)

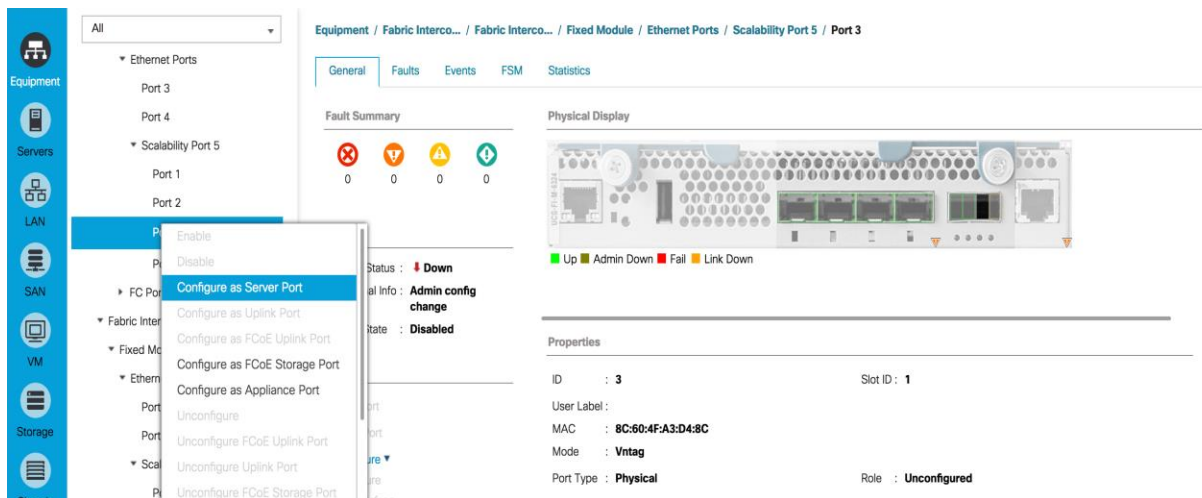
5. Leave other settings alone or change if appropriate to your environment.
6. Click Save Changes.
7. Click OK.



## Extending Cisco UCS Mini

To extend Cisco UCS Mini with a second Cisco UCS Chassis and to attach the Cisco UCS C-Series Rack Servers, complete the following steps:

1. Connect the second Cisco UCS 5108 chassis to the existing single-chassis Cisco UCS6324 series fabric interconnect configuration through the scalability port.
2. Connect two ports from each 6324 Fabric Interconnect to the second Chassis IOM modules.
3. The other two remaining ports can be connected to attach C-Series Rack mountable servers.
4. Expand Fabric Interconnect A, then Fixed Module.
5. Expand the Ethernet ports.
6. Expand Scalability ports and select the ports that are connected to the second Cisco UCS Chassis and rack servers.
7. Right-click to configure the ports as server ports and make sure the ports are enabled.



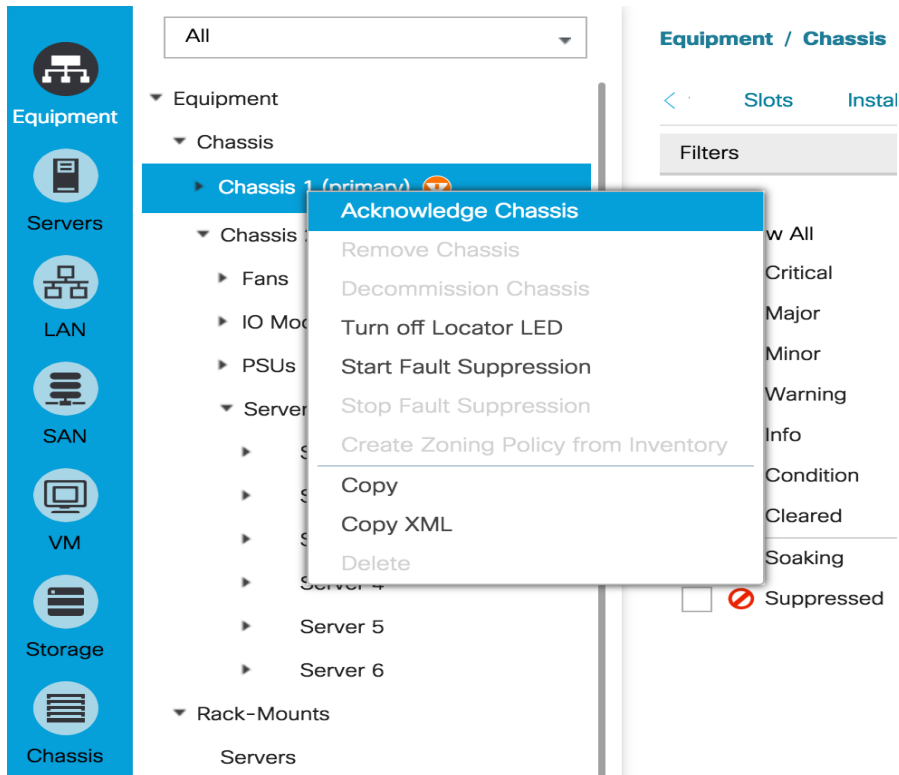
8. Repeat this process for each port connected to Fabric Interconnect A, then repeat for the Fabric Interconnect B Scalability ports
9. Configure the server ports and wait for the second chassis and Rack Servers to be discovered.

## Acknowledge Cisco UCS Chassis

To acknowledge all Cisco UCS chassis, 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.

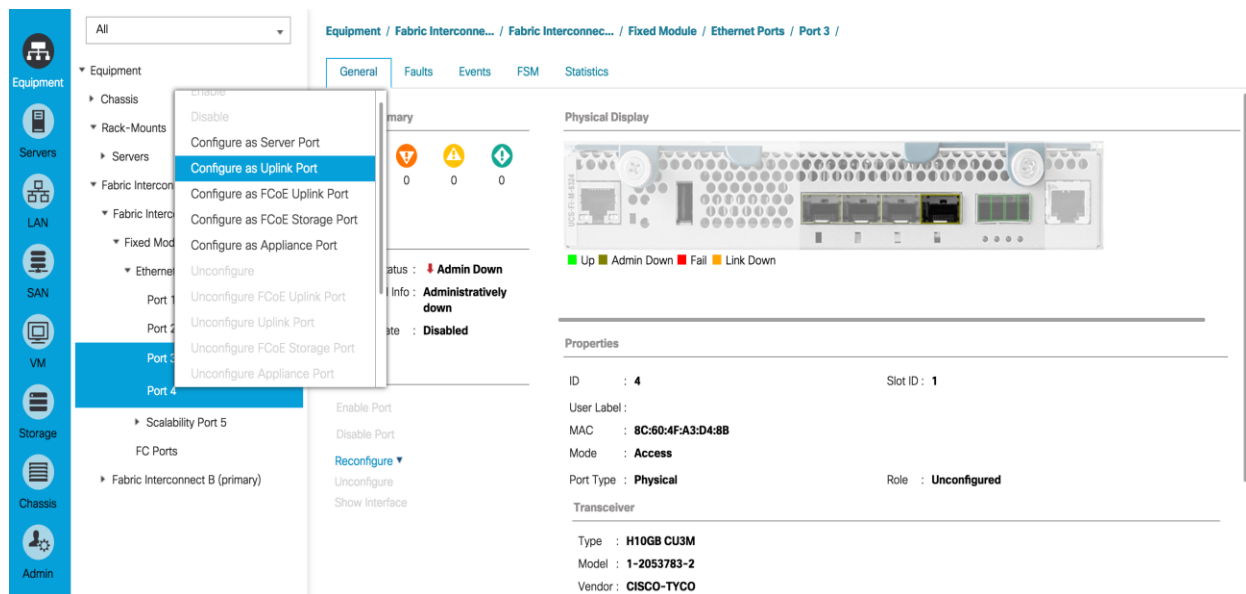
- Right-click the chassis both Primary and Extended Secondary and select Acknowledge Chassis, click Yes, then click OK.



## Enable Uplink Ports

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

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



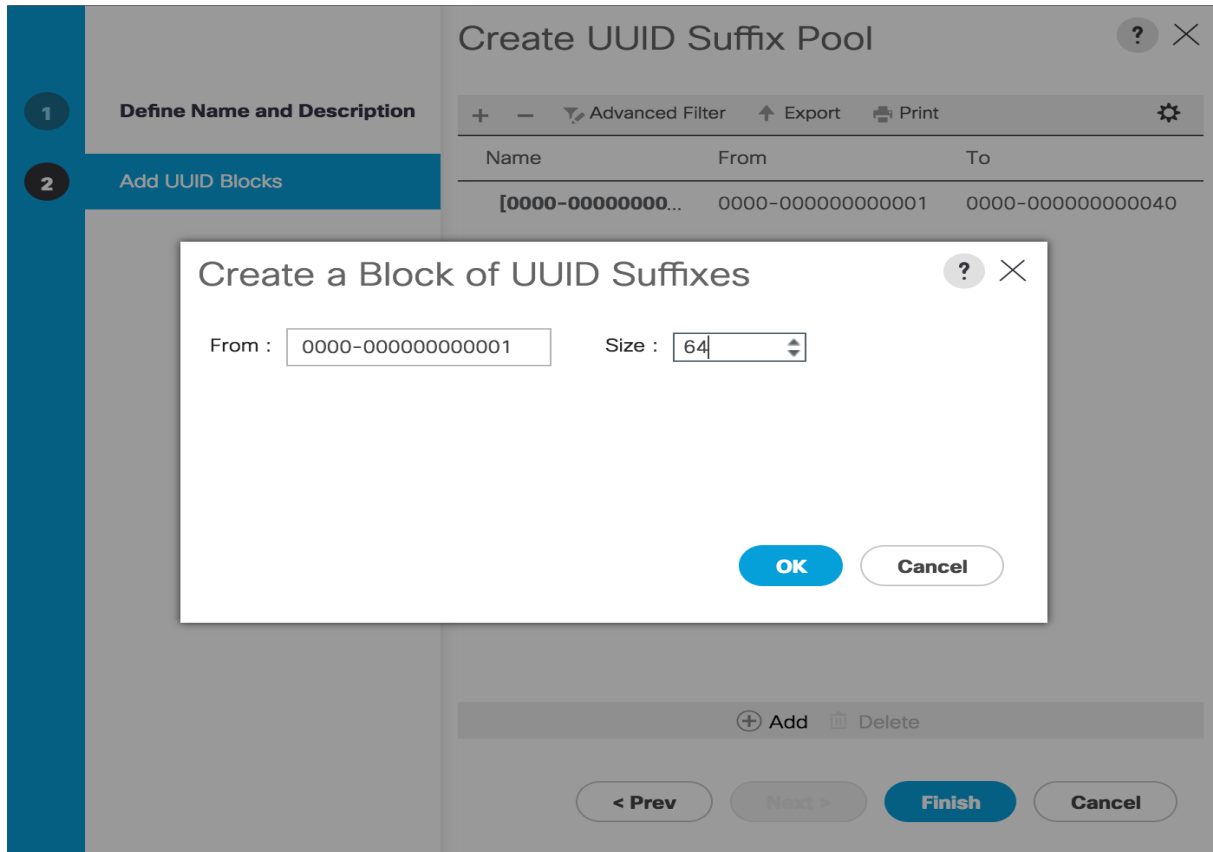
5. Click Yes to confirm uplink ports and click OK.
6. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.
7. Expand Ethernet Ports.
8. Select ports 3 and 4 that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.
9. Click Yes to confirm the uplink ports and click OK.

## Create UUID Suffix Pool

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

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Pools > root.
3. Right-click UUID Suffix Pools.
4. Select Create UUID Suffix Pool
5. Enter UUID\_Pool as the name of the UUID suffix pool.
6. Optional: Enter a description for the UUID suffix pool.
7. Keep the prefix at the derived option.
8. Click Next.

9. Click Add to add a block of UUIDs.
10. Keep the From field at the default setting.
11. Specify a size for the UUID block that is sufficient to support the available blade or server resources.



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

## Create Server Pool

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



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

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

4. Select Create Server Pool.
5. Enter Infra\_Pool as the name of the server pool.
6. Optional: Enter a description for the server pool.
7. Click Next.
8. Select two (or more) servers to be used for the VMware Cluster and click >> to add them to the Infra\_Pool server pool.
9. Click Finish.
10. Click OK.

**1** Set Name and Description

**2** Add Servers

### Create Server Pool

**Servers**

Chassis ...	...	...	...	...	...	...
2	1	...	...	...	...	...
2	2	...	...	...	...	...
2	3	...	...	...	...	...
2	4	...	...	...	...	...
2	5	...	...	...	...	...
2	6	...	...	...	...	...
1	3	...	...	...	...	8
1	5	...	...	...	...	...
1	6	...	...	...	...	...
1	7	...	...	...	...	...

Model:  
Serial Number:  
Vendor:

**Pooled Servers**

...	Sl...	R...	U...	PID	A...	S...	C...
1	2		U...	U...	FL...		28
1	1		U...	U...	FL...		28

Model:  
Serial Number:  
Vendor:

< Prev   Next >   **Finish**   Cancel

## Create Host Firmware Package

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

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

3. Right-click Host Firmware Packages.
4. Select Create Host Firmware Package
5. Enter VM-Host-Infra as the name of the host firmware package.
6. Leave Simple selected.
7. Select the version 3.1(2c) for both the Blade and Rack Packages.
8. Leave Excluded Components with only Local Disk selected.
9. Click OK to create the host firmware package.
10. Click OK.

**Create Host Firmware Package** ? X

Name :

Description :

How would you like to configure the Host Firmware Package?

Simple  Advanced

Blade Package :  ▼

Rack Package :  ▼

**Excluded Components:**

- Adapter
- Host NIC Option ROM
- CIMC
- Board Controller
- Flex Flash Controller
- BIOS
- PSU
- SAS Expander
- Storage Controller Onboard Device
- Storage Device Bridge
- GPUs
- FC Adapters
- Local Disk
- HBA Device ROM

### 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 Local Disk Configuration Policy

Name :

Description :

Mode :

---

FlexFlash

FlexFlash State :  Disable  Enable

If **FlexFlash State** is disabled, SD cards will become unavailable immediately.  
Please ensure SD cards are not in use before disabling the FlexFlash State.

FlexFlash RAID Reporting State :  Disable  Enable

## 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 Power Control Policy



Name :

Description :

Fan Speed Policy :

### Power Capping

If you choose **cap**, the server is allocated a certain amount of power based on its priority within its power group. Priority values range from 1 to 10, with 1 being the highest priority. If you choose **no-cap**, the server is exempt from all power capping.

No Cap  cap

Cisco UCS Manager only enforces power capping when the servers in a power group require more power than is currently available. With sufficient power, all servers run at full capacity regardless of their priority.

OK

Cancel

## Create Server Pool Qualification Policy (Optional)

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

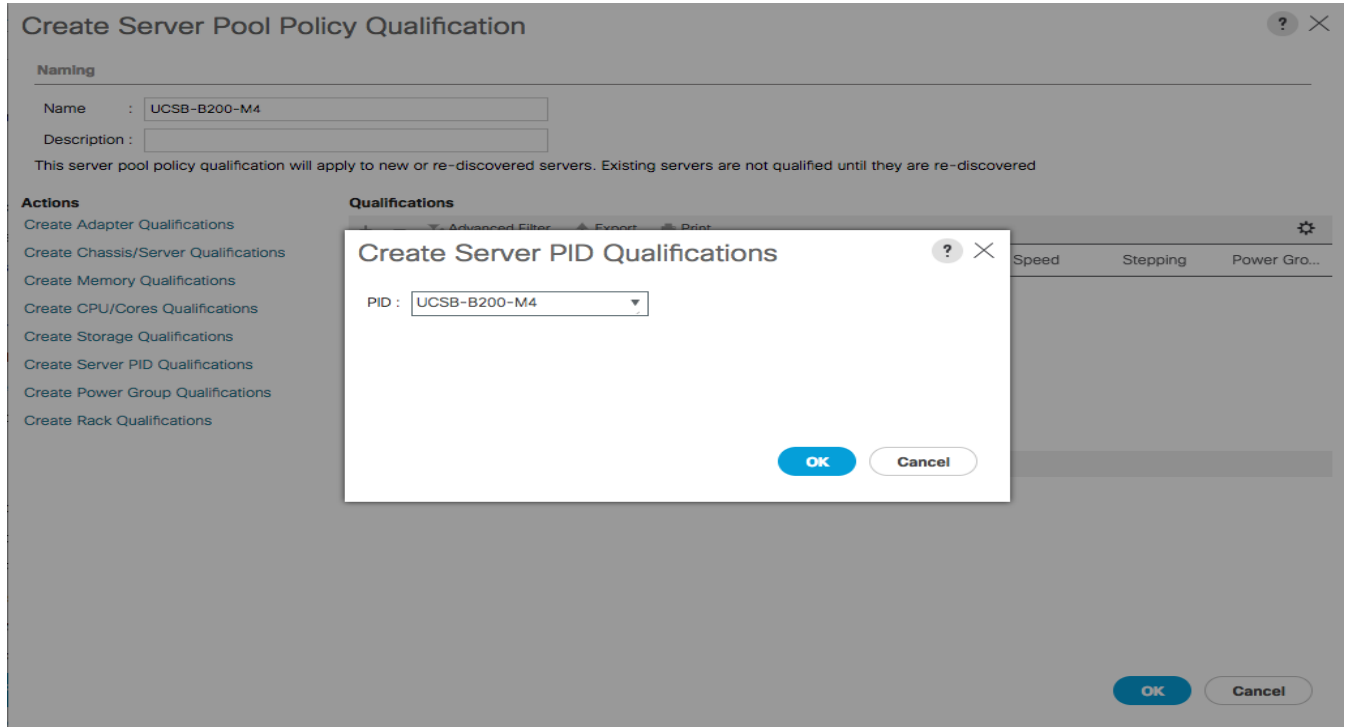


This example creates a policy for a Cisco UCS B200-M4 server.

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.

**Create BIOS Policy**

Name : VM-Host-Infra

Description :

Reboot on BIOS Settings Change :

Quiet Boot :  disabled  enabled  Platform Default

Post Error Pause :  disabled  enabled  Platform Default

Resume Ac On Power Loss :  stay-off  last-state  reset  Platform Default

Front Panel Lockout :  disabled  enabled  Platform Default

Consistent Device Naming :  disabled  enabled  Platform Default

< Prev   Next >   **Finish**   Cancel

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

**Create BIOS Policy**

1 Main

2 **Processor**

3 Intel Directed IO

4 RAS Memory

5 Serial Port

6 USB

7 PCI

8 QPI

9 LOM and PCIe Slots

10 Trusted Platform

11 Graphics Configuration

12 Boot Options

13 Server Management

Turbo Boost :  disabled  enabled  Platform Default

Enhanced Intel Speedstep :  disabled  enabled  Platform Default

Hyper Threading :  disabled  enabled  Platform Default

Core Multi Processing : all

Execute Disabled Bit :  disabled  enabled  Platform Default

Virtualization Technology (VT) :  disabled  enabled  Platform Default

Hardware Pre-fetcher :  disabled  enabled  Platform Default

Adjacent Cache Line Pre-fetcher :  disabled  enabled  Platform Default

DCU Streamer Pre-fetch :  disabled  enabled  Platform Default

DCU IP Pre-fetcher :  disabled  enabled  Platform Default

Direct Cache Access :  disabled  enabled  auto  Platform Default

Processor C State :  disabled  enabled  Platform Default

Processor C1E :  disabled  enabled  Platform Default

Processor C3 Report : Platform Default

Processor C6 Report :  disabled  enabled  Platform Default

Processor C7 Report : Platform Default

Processor CMCI :  enabled  disabled  Platform Default

CPU Performance : Platform Default

Max Variable MTRR Setting :  auto-max  8  Platform Default

< Prev Next > Finish Cancel

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

17. Change the VT for Direct IO to Enabled.

**Create BIOS Policy** ? X

VT For Directed IO :  disabled  enabled  Platform Default

Interrupt Remap :  disabled  enabled  Platform Default

Coherency Support :  disabled  enabled  Platform Default

ATS Support :  disabled  enabled  Platform Default

Pass Through DMA Support :  disabled  enabled  Platform Default

< Prev Next > Finish Cancel

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.

**Create BIOS Policy** ? X

Memory RAS Config :

NUMA :  disabled  enabled  Platform Default

LV DDR Mode :  power-saving-mode  performance-mode  auto  Platform Default

DRAM Refresh Rate :

DDR3 Voltage Selection :  ddr3-1500mv  ddr3-1350mv  Platform Default

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.

## Create Placement Policy ? X

Name :

Virtual Slot Mapping Scheme :  Round Robin  Linear Ordered

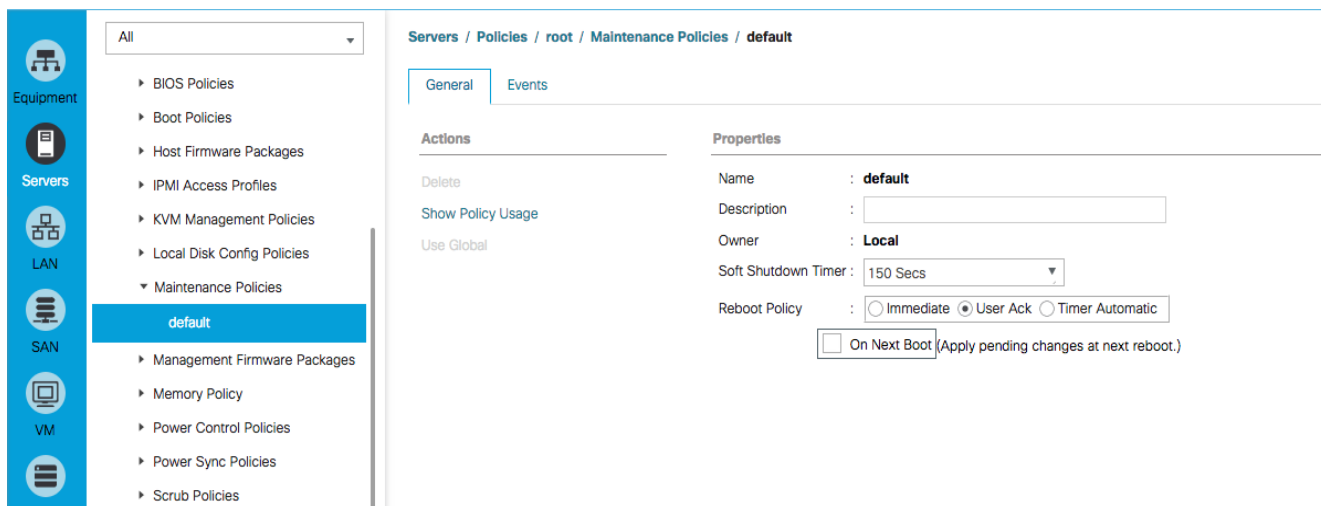
Advanced Filter

Virtual Slot	Selection Preference
1	Assigned Only
2	All
3	All
4	All

### 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.

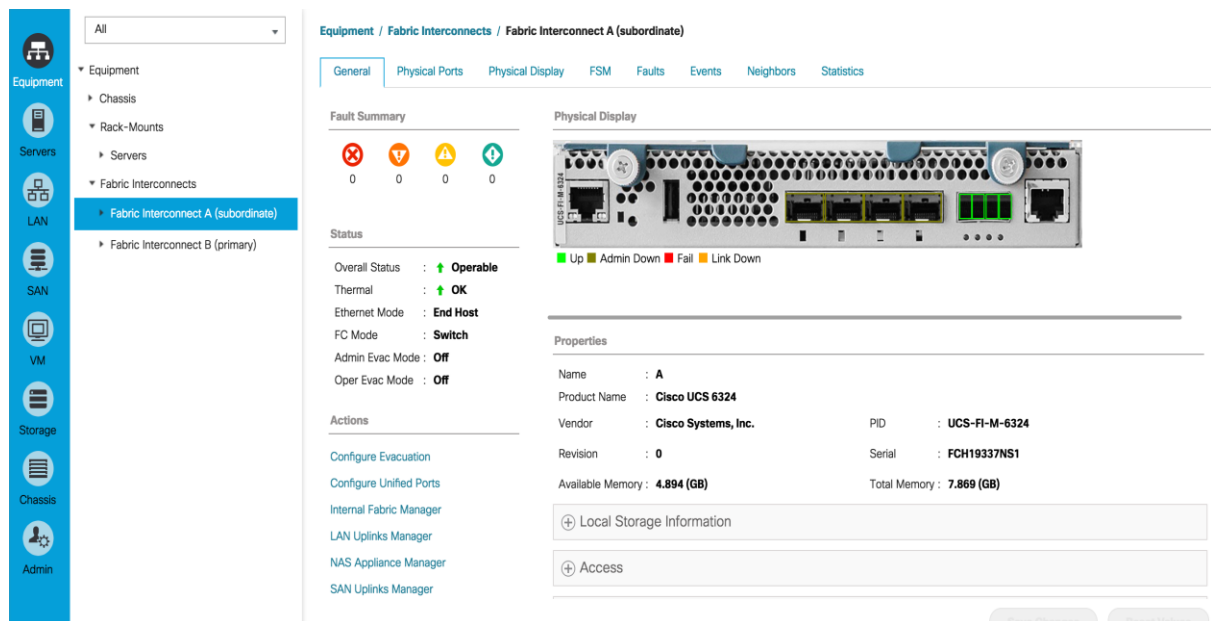


## Configure UCS SAN Connectivity

### Configure Unified Ports

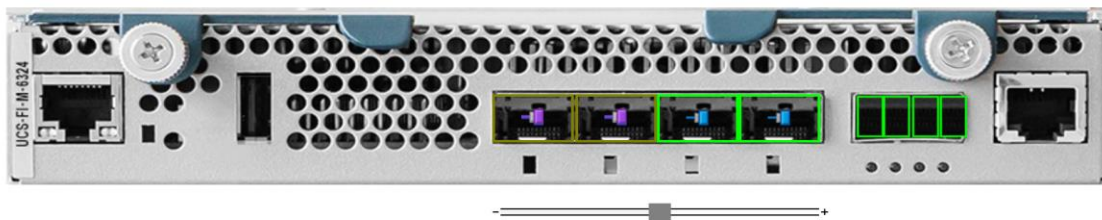
Complete the following steps making sure you first reconfigure on the subordinate switch to save time:

1. On the equipment tab, select the Fabric Interconnect A or B which is the subordinate FI at this time, and in the Actions pane, select Configure Unified Ports, and then click Yes.



2. Slide the lever to change the ports 1-2 to change the ports to Fibre Channel. Click Finish then click Yes to the reboot message. Click OK.

## Configure Unified Ports



## Instructions

The position of the slider determines the type of the ports.

All the ports to the left of the slider are Fibre Channel ports (Purple), while the ports to the right are Ethernet ports (Blue).

Port	Transport	If Role or Port Channel Membership	Desired If Role
Port 1	ether	Unconfigured	FC Uplink
Port 2	ether	Unconfigured	FC Uplink
Port 3	ether	Ethernet Uplink	
Port 4	ether	Ethernet Uplink	

■ Up
 ■ Admin Down
 ■ Fail
 ■ Link Down



- When the subordinate has completed reboot, select the Primary Fabric Interconnect (A or B), then select Configure Unified Ports, and click Yes.
- Slide the Bar to the left to select ports 1-2 for FC (purple), click Finish, and click Yes to the re-boot message. You will need to re-login to the client after the reboot of the FI completes

## Configure Fabric Interconnects in FC Switching Mode

FC Switching mode requires the Fabric Interconnects to reboot. The reboot will take place automatically. When the Fabric Interconnects complete the reboot process, a new management session must be established to continue with management and configuration.

To configure fabric interconnects in FC Switching Mode, complete the following steps:

- Navigate to the Equipment tab in the left pane and expand the Fabric Interconnects object.
- Select Fabric Interconnect A, in the left pane, General tab, and click Set FC Switching Mode in the left pane.
- Click yes, then OK. Reconnect after the restart.



The screenshot displays the Cisco UCS Manager interface. On the left, a navigation pane shows a tree structure with 'Fabric Interconnect A (primary)' selected. The main content area is titled 'Equipment / Fabric Interconnects / Fabric Interconnect A (primary)'. It features several tabs: 'General', 'Physical Ports', 'Physical Display', 'FSM', 'Faults', 'Events', 'Neighbors', and 'Statistics'. The 'General' tab is active, showing a list of actions on the left and hardware details on the right. The hardware details include Product Name (Cisco UCS 6324), Vendor (Cisco Systems, Inc.), PID (UCS-FI-M-6324), Revision (0), Serial (FCH19337NS1), Available Memory (4.824 GB), and Total Memory (7.869 GB). Below this, there are expandable sections for Local Storage Information, Access, High Availability Details, VLAN Port Count, and FC Zone Count. A 'Firmware' section at the bottom lists Boot-loader Version (v1.022.0), Kernel Version (5.0(3)N2(3.12c)), System Version (5.0(3)N2(3.12c)), Package Version (3.1(2c)A), and Startup Kernel Version (5.0(3)N2(3.12c)).

## Create VSAN for the Fibre Channel Interfaces

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

1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Expand the SAN > Storage Cloud tree.
3. Right-click VSANs.
4. Choose Create Storage VSAN.
5. Enter VSAN\_A as the name of the VSAN for fabric A.
6. Select the Enabled option 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 click OK again.

## Create Storage VSAN ? ✕

Name :

**FC Zoning Settings**

---

FC Zoning :  Disabled  Enabled

Do **NOT** enable local zoning if fabric interconnect is connected to an upstream FC/FCoE switch.

Common/Global  Fabric A  Fabric B  Both Fabrics Configured Differently

You are creating a local VSAN in fabric A that maps to a VSAN ID that exists only in fabric A.

Enter the VSAN ID that maps to this VSAN.

VSAN ID :

A VLAN can be used to carry FCoE traffic and can be mapped to this VSAN.

Enter the VLAN ID that maps to this VSAN.

FCoE VLAN :

10. Right-click VSANs again and choose Create Storage VSAN.

11. Enter VSAN\_B as the name of the VSAN for fabric B.

12. Keep the Enabled option selected for FC Zoning.

13. Click the Fabric B radio button.

14. 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, click OK and then click OK again.

## Create Storage VSAN ? X

Name :

**FC Zoning Settings**

---

FC Zoning :  Disabled  Enabled

Do **NOT** enable local zoning if fabric interconnect is connected to an upstream FC/FCoE switch.

Common/Global
  Fabric A
  Fabric B
  Both Fabrics Configured Differently

You are creating a local VSAN in fabric B that maps to a VSAN ID that exists only in fabric B.

Enter the VSAN ID that maps to this VSAN.

VSAN ID :

A VLAN can be used to carry FCoE traffic and can be mapped to this VSAN.

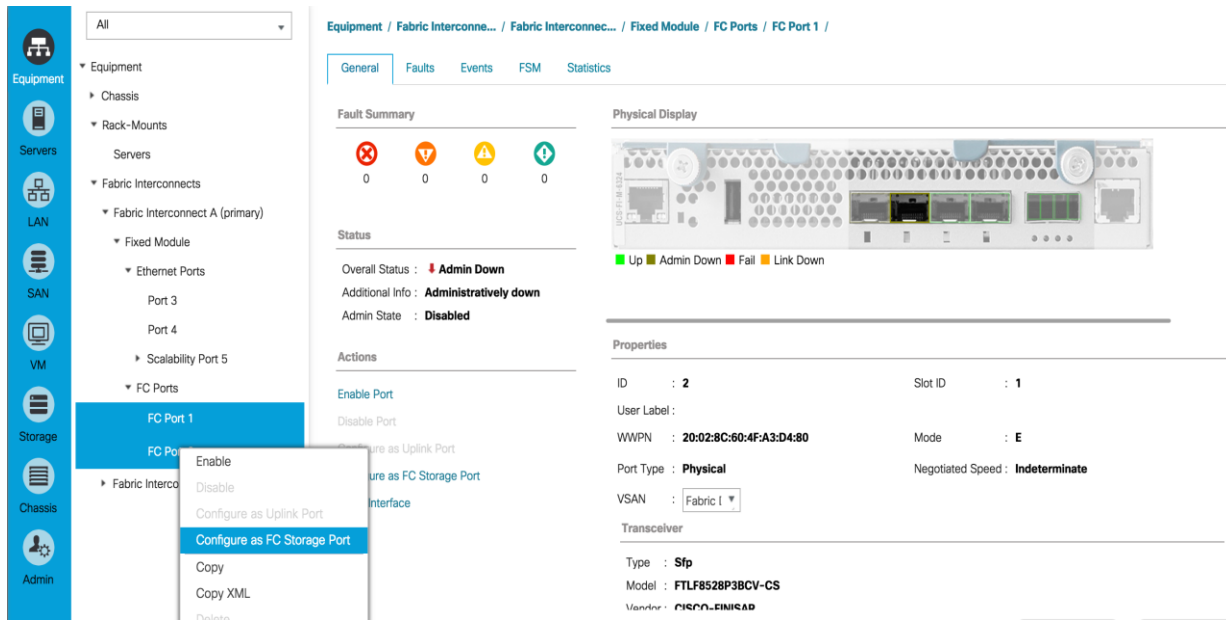
Enter the VLAN ID that maps to this VSAN.

FCoE VLAN :

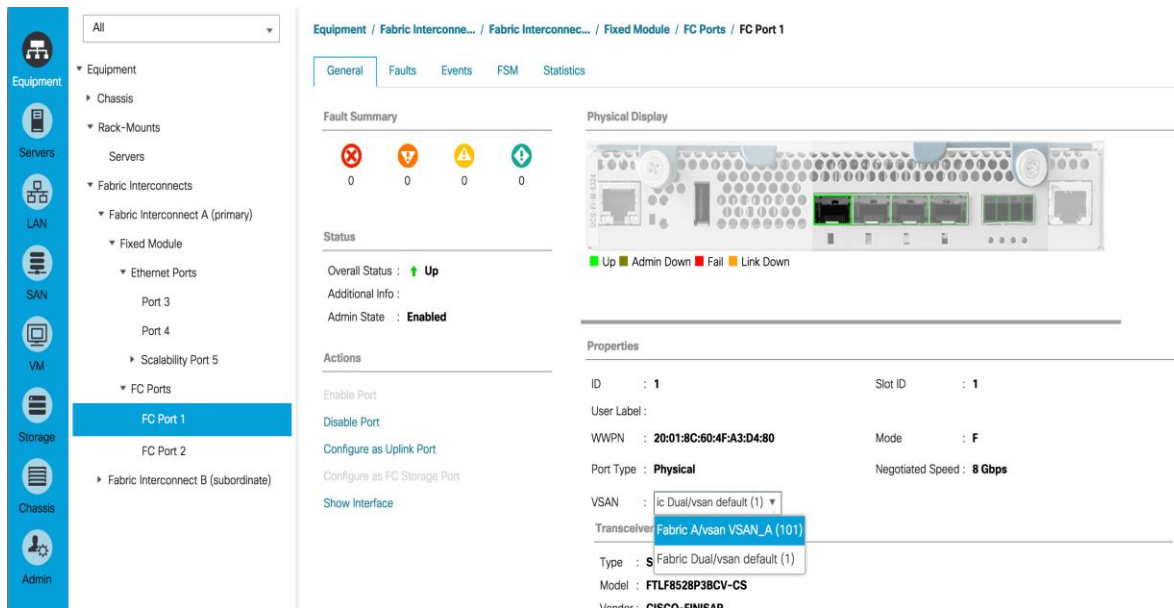
## Configure the FC Ports as Storage Ports

To configure FC Storage Ports complete the following steps:

1. Select the Equipment tab on the top left of the window.
2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module.
3. Expand the FC Ports object.
4. Select FC ports 1 and 2 that are connected to the IBM storage array.
5. Right-click and select configure as FC Storage Port.
6. Click Yes, then click OK.



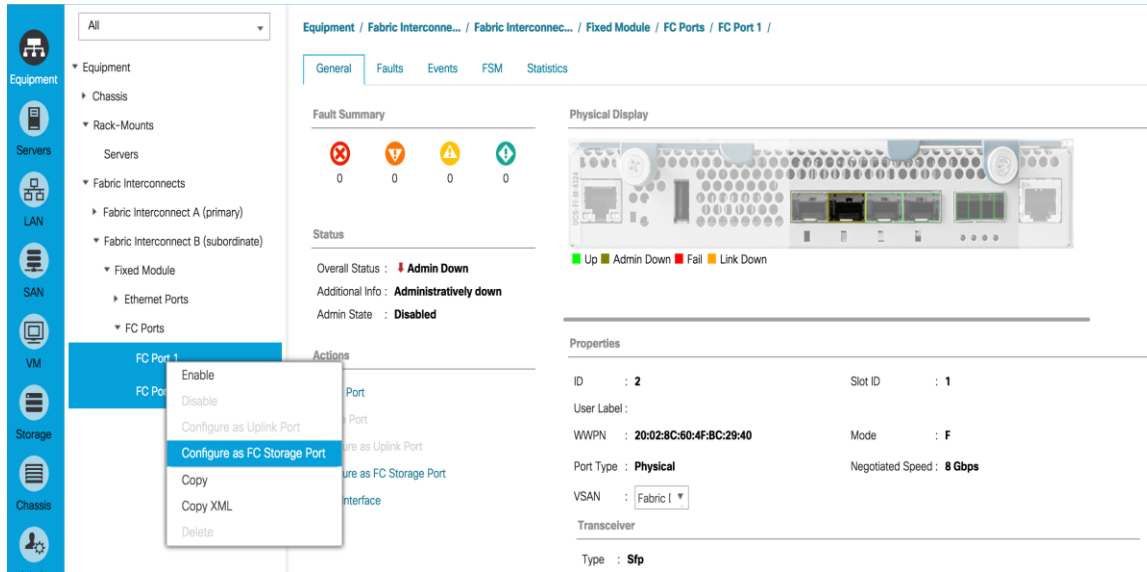
- Assign the VSAN\_A you created to FC1 and FC2 storage ports on general tab and click Save changes, then click OK.



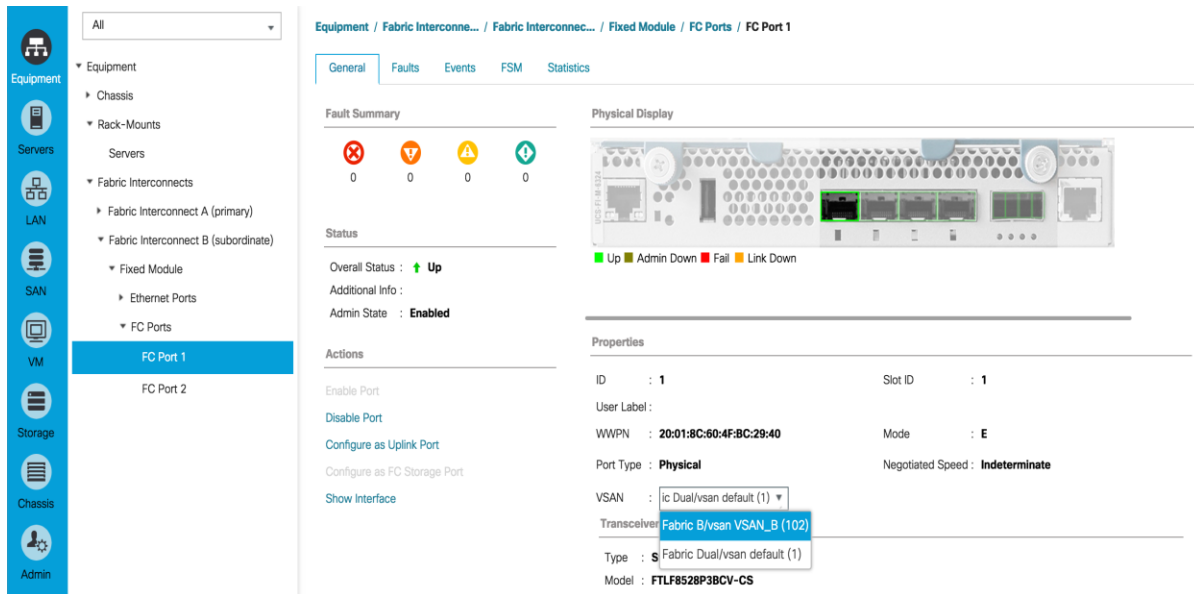
- Select Equipment > Fabric Interconnects > Fabric Interconnect B > Fixed Module.
- Expand the FC Ports object.
- Select FC ports 1 and 2 that are connected to the IBM storage array.

11. Right-click and select configure as FC Storage Port.

12. Click Yes, then click OK.



13. Assign the VSAN\_B you created to FC1 and FC2 the storage ports on general tab and click Save changes, then click OK.

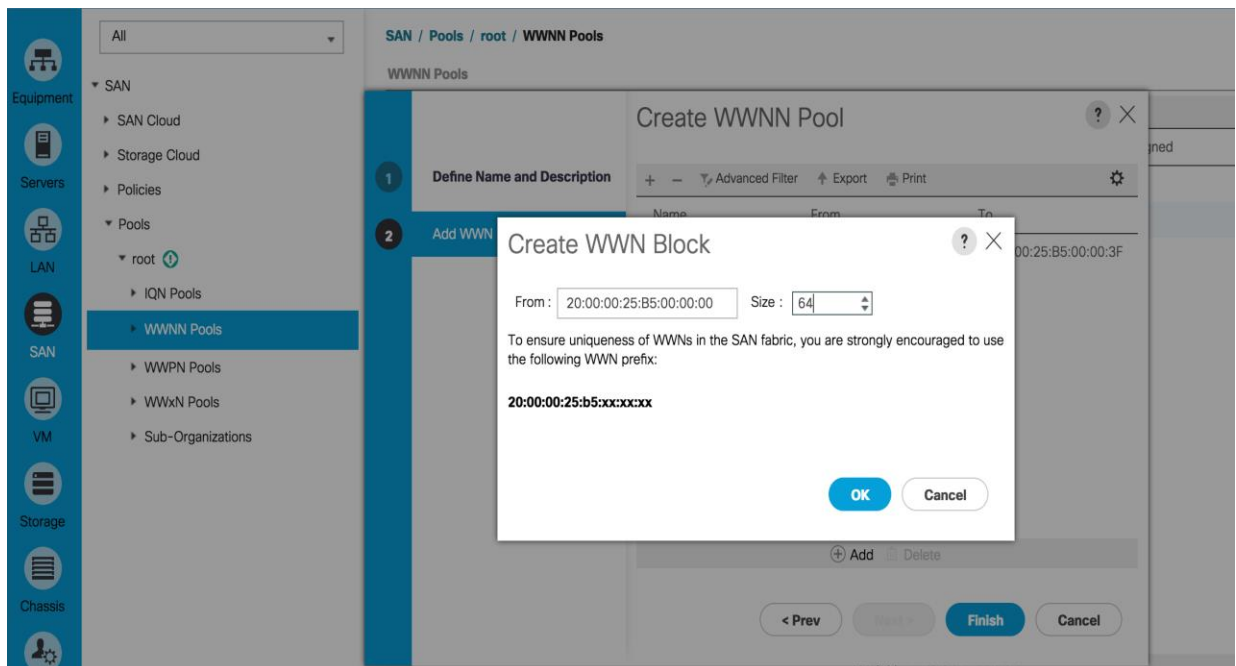


## Create WWNN Pools

To configure the necessary World Wide Node Name (WWNN) 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.
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 created: one for fabric A and one for fabric B.

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

The screenshot shows the Cisco UCS Manager interface. On the left is a navigation pane with categories like Equipment, Servers, LAN, SAN, VM, Storage, and Chassis. The 'SAN' category is expanded, showing 'SAN Cloud', 'Storage Cloud', 'Policies', and 'Pools'. Under 'Pools', 'root' is selected, and 'WWPN Pools' is highlighted. A 'Create WWPN Pool' dialog box is open in the foreground. It has a blue header and a white body. The first step, '1 Define Name and Description', is active. It contains three input fields: 'Name' (filled with 'WWPN\_Pool\_A'), 'Description' (empty), and 'Assignment Order' (radio buttons for 'Default' and 'Sequential', with 'Default' selected). At the bottom of the dialog are four buttons: '< Prev', 'Next >', 'Finish', and 'Cancel'. The 'Next >' button is highlighted in blue. The second step, '2 Add WWN Blocks', is visible but not yet active.

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.

## Create WWN Block ? X

From :  Size :

To ensure uniqueness of WWNs in the SAN fabric, you are strongly encouraged to use the following WWN prefix:

**20:00:00:25:b5:xx:xx:xx**

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.

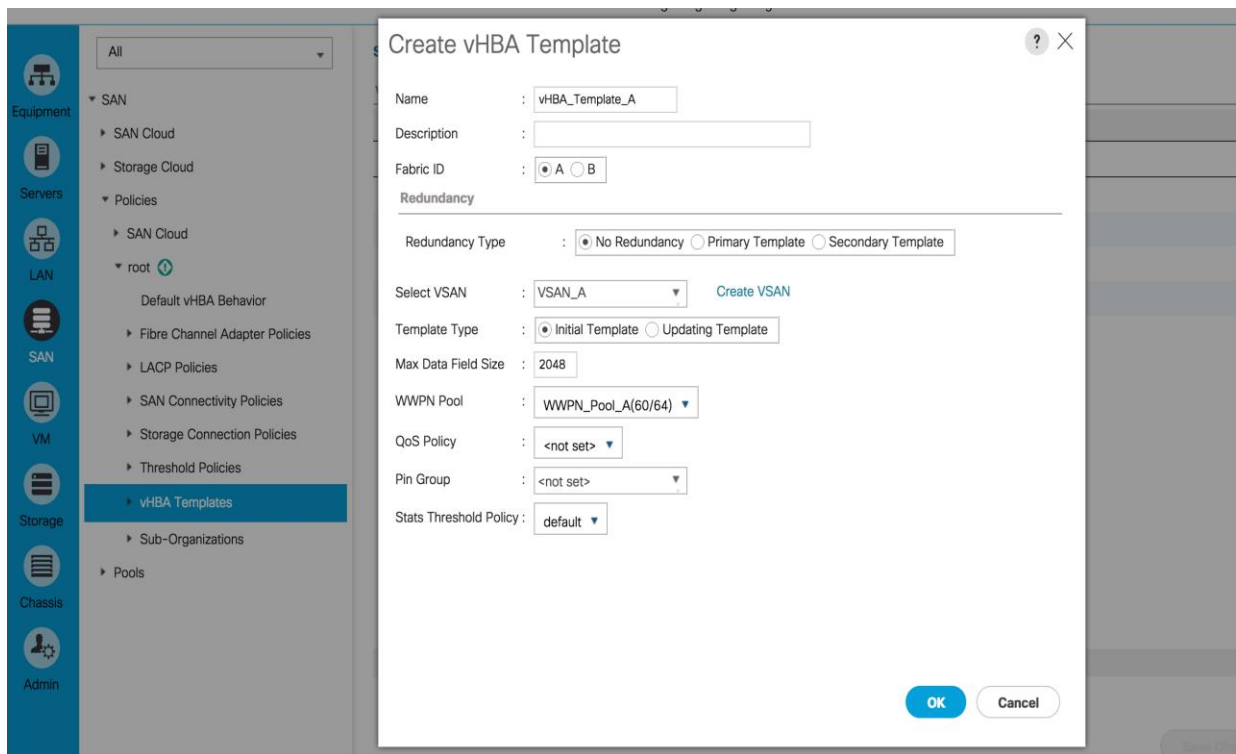
24. Click OK.



## Create vHBA Templates for Fabric A and Fabric B

To create multiple virtual host bus adapter (vHBA) templates for the Cisco UCS environment, complete the following 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 vHBA Template



Name : vHBA\_Template\_B

Description :

Fabric ID :  A  B

---

**Redundancy**

Redundancy Type :  No Redundancy  Primary Template  Secondary Template

Select VSAN : VSAN\_B [Create VSAN](#)

Template Type :  Initial Template  Updating Template

Max Data Field Size : 2048

WWPN Pool : WWPN\_Pool\_B(64/64)

QoS Policy : <not set>

Pin Group : <not set>

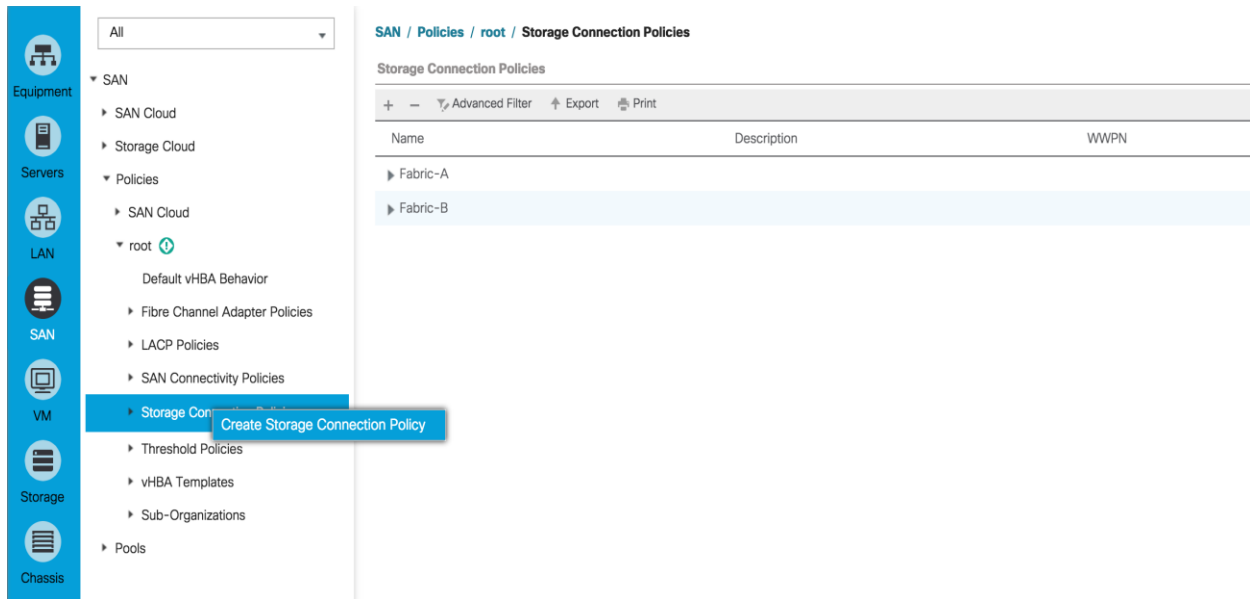
Stats Threshold Policy : default



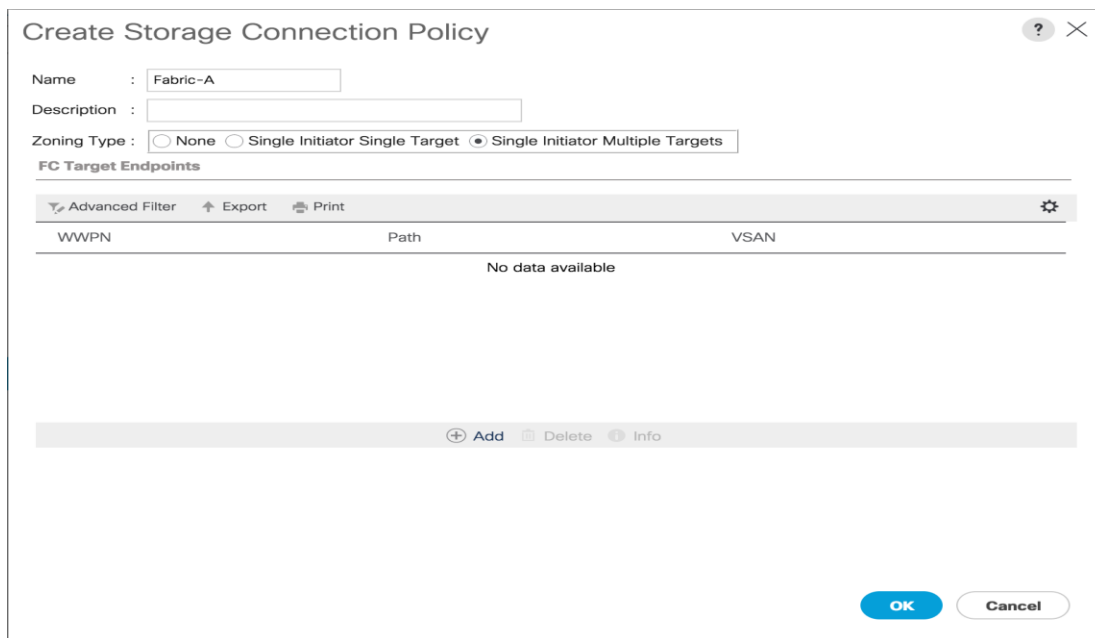
### Create the Storage Connection Policy Fabric-A

To create the Storage Connection Policy Fabric-A, complete the following steps:

1. Select the SAN tab at the top left of the window.
2. Go to Policies > root.
3. Right-click Storage Connection Policies.
4. Select Create Storage Connection Policy.



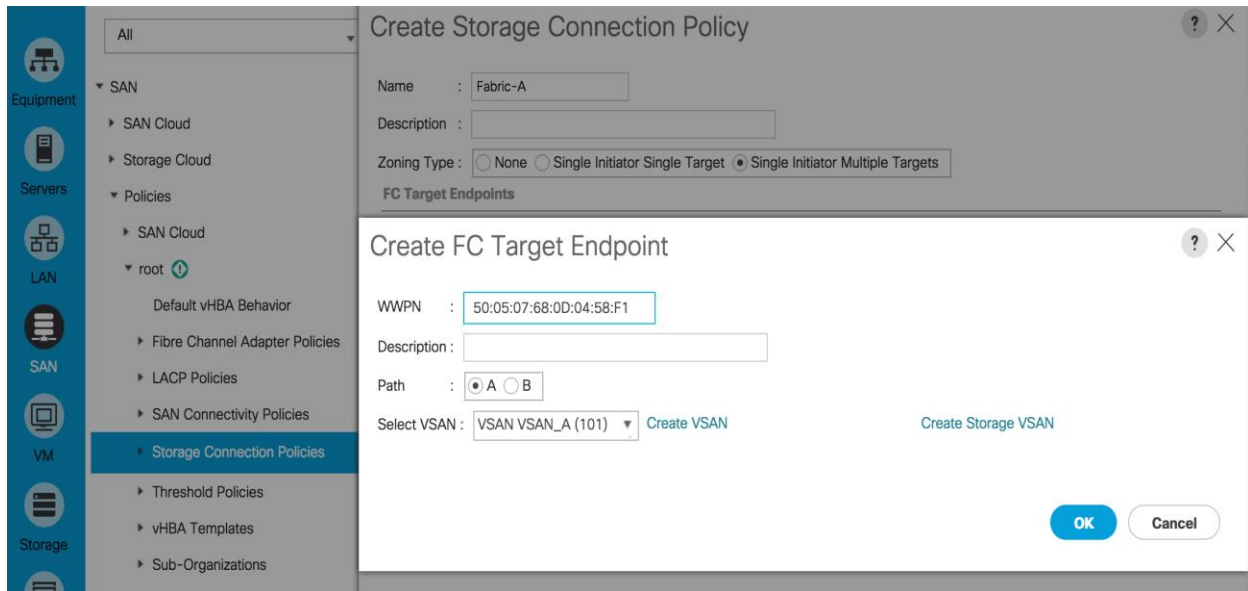
5. Enter Storage Connection Policy name Fabric-A.
6. Select the Zoning Type Single Initiator Multiple Targets.
7. Click Add to add the FC Target Endpoint.



8. Enter the WWPN for Node 1 Fabric A <<var\_wwpn\_Node1-switch-A>>.
9. Select Path A.

10. Select VSAN VSAN\_A.

11. Click OK to create the FC Target Endpoint.



12. Click the Add button to add the FC Target Endpoint.

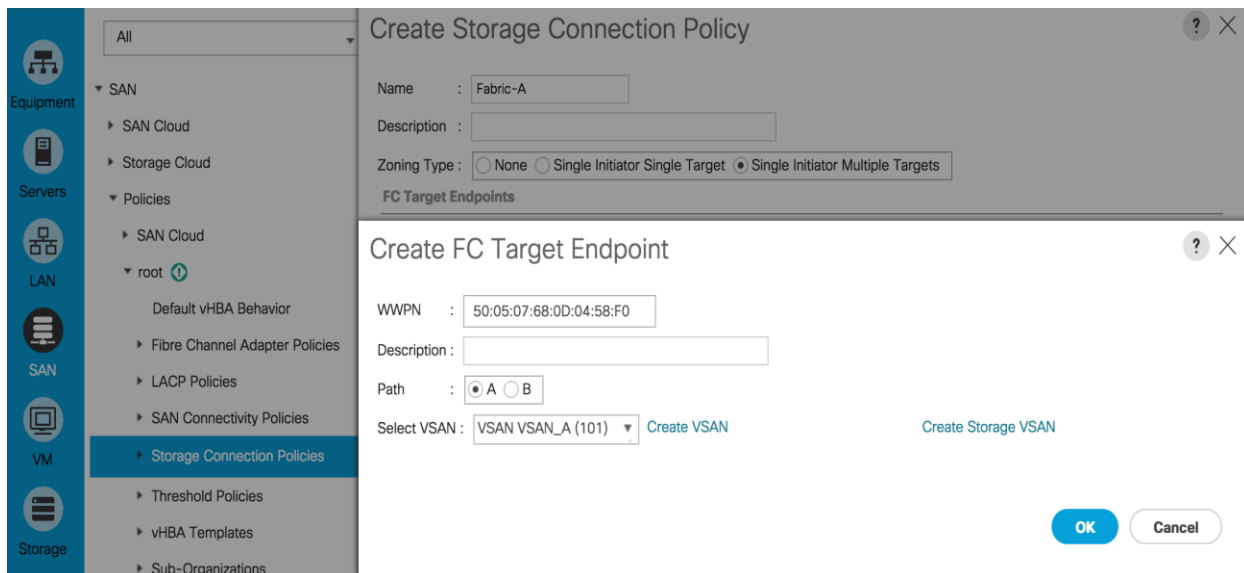
13. Enter the WWPN for Node 2 Fabric A <<var\_wwpn\_Node2-switch-A>>.

14. Select Path A.

15. Select VSAN VSAN\_A.

16. Click OK to create the FC Target Endpoint.

17. Click OK to create the storage connection policy.



## Create the Storage Connection Policy Fabric-B

To create the Storage Connection Policy Fabric-B, complete the following steps:

1. Select the SAN tab at the top left of the window.
2. Go to Policies > root .
3. Right-click Storage Connection Policies.
4. Select Create Storage Connection Policy.
5. Enter Storage Connection Policy name. Fabric-B.
6. Select the Zoning Type Single Initiator Multiple Targets.
7. Enter the WWPN for Node 1 Fabric B <<var\_wwpn\_Node1-Switch-B>>.
8. Select Path B.
9. Select VSAN VSAN\_B.
10. Click OK to create the FC Target Endpoint.
11. Click the Add button to add the FC Target Endpoint.
12. Enter the WWPN for Node 2 Fabric B<<var\_wwpn\_Node2-switch-B>>.
13. Select Path B.
14. Select VSAN VSAN\_B.
15. Click OK to create the FC Target Endpoint.

- Click OK to create the storage connection policy.

## Create a SAN Connectivity Policy

To create a SAN Connectivity Policy that will be leveraged for automated Fibre Channel zone creation on the Fabric interconnect, complete the following steps:

- Select the SAN tab at the top left of the window.
- Go to Policies > root.
- Right-click the SAN Connectivity Policies, and click Create SAN Connectivity Policy.

The screenshot displays the Cisco UCS management console interface. On the left, a blue sidebar contains navigation icons for Equipment, Servers, LAN, SAN, VM, Storage, and Chassis. The 'SAN' icon is selected. The main content area shows a breadcrumb path: **SAN / Policies / root / SAN Connectivity Policies**. Below this, there is a section titled **SAN Connectivity Policies** with options for 'Advanced Filter', 'Export', and 'Print'. A table lists existing policies: 'Dual-Fabric' and 'Test-FCOE'. A context menu is overlaid on the 'SAN Connectivity Policies' folder, with the option 'Create SAN Connectivity Policy' highlighted in blue.

- Input name Dual-Fabric.
- Select WWNN\_Pool for WWNN Assignment.
- Click Add.

## Create SAN Connectivity Policy



A server is identified on a SAN by its World Wide Node Name (WWNN). Specify how the system should assign a WWNN to the server associated with this profile.

### World Wide Node Name

WWNN Assignment:

[Create WWNN Pool](#)

The WWNN will be assigned from the selected pool.  
The available/total WWNNs are displayed after the pool name.

Name	WWPN
No data available	

[Delete](#) [Add](#) [Modify](#)

**OK** **Cancel**

7. Enter Name Fabric-A.
8. Click Use vHBA-template.
9. Select vHBA\_Template\_A.
10. Select Adapter Policy VMware.

## Create vHBA



Name :

Use vHBA Template :

Redundancy Pair :

Peer Name :

vHBA Template :

[Create vHBA Template](#)

### Adapter Performance Profile

Adapter Policy :

[Create Fibre Channel Adapter Policy](#)

- <not set>
- Domain Policies
- Linux
- Solaris
- VMWare**
- Windows
- WindowsBoot
- default

**OK** **Cancel**

11. Click OK.
12. Click the Add button again to add another vHBA.
13. Enter Name Fabric-B.
14. Select Use vHBA Template.
15. Select vHBA-Template-B.
16. Select Adapter Policy VMware.
17. Click OK to complete the policy creation.
18. Click OK.

## Create SAN Connectivity Policy



Name :

Description :

A server is identified on a SAN by its World Wide Node Name (WWNN). Specify how the system should assign a WWNN to the server associated with this profile.

### World Wide Node Name

WWNN Assignment:

[Create WWNN Pool](#)

The WWNN will be assigned from the selected pool.  
The available/total WWNNs are displayed after the pool name.

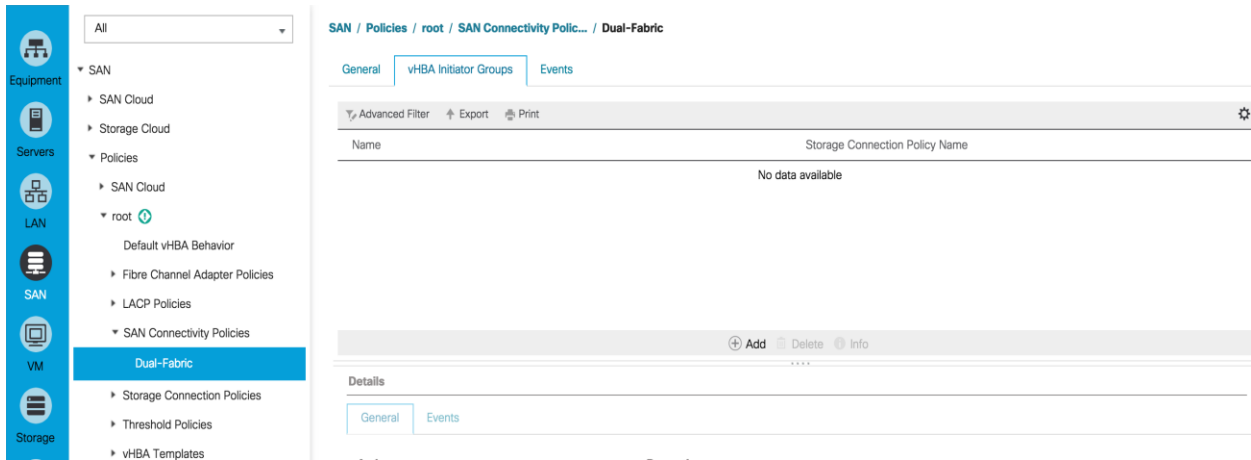
Name	WWPN
▼ vHBA Fabric-B	Derived
vHBA If default	
▼ vHBA Fabric-A	Derived
vHBA If default	

OK

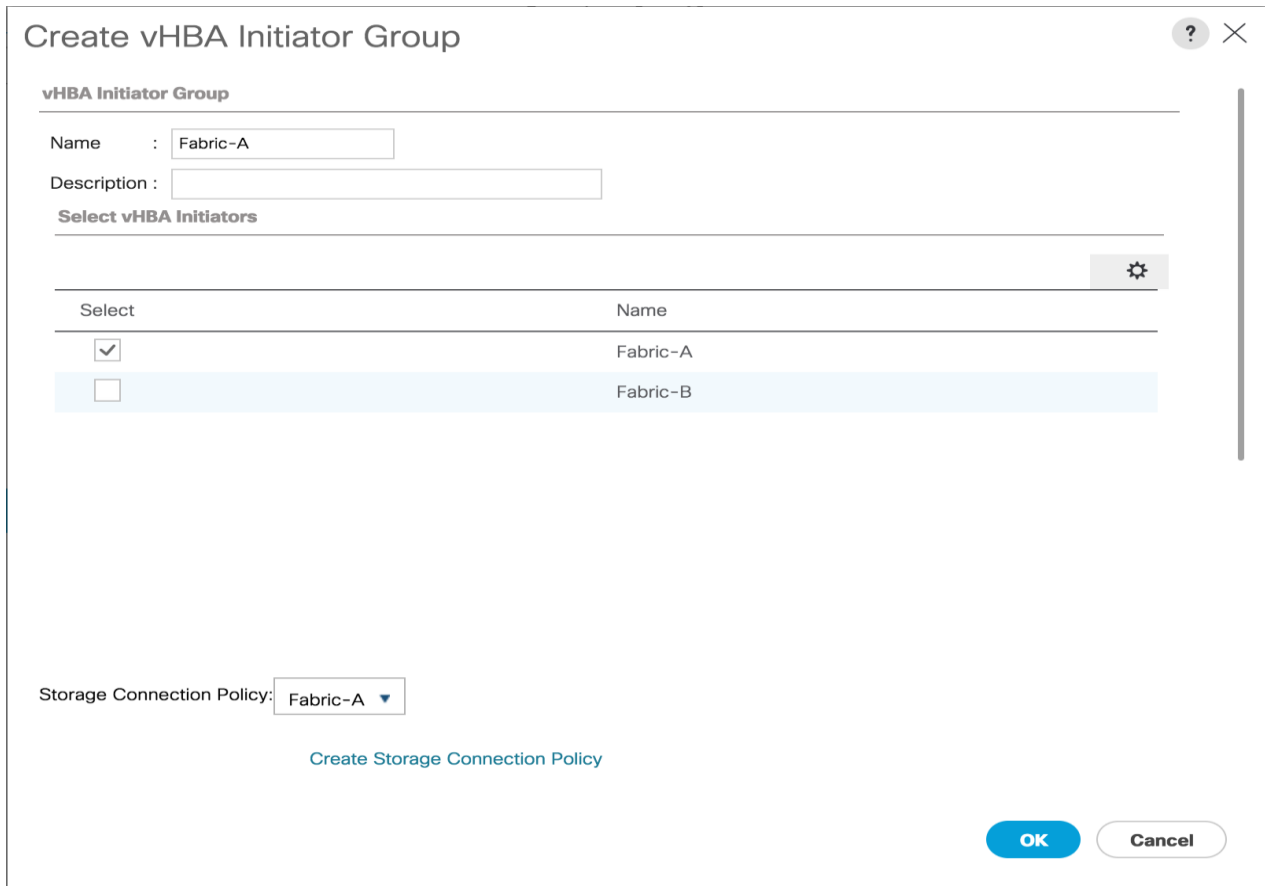
Cancel

19. Expand the San Connectivity Policies and click the Dual-Fabric policy.
20. In the right screen, click the HBA initiator groups tab.
21. Click Add.

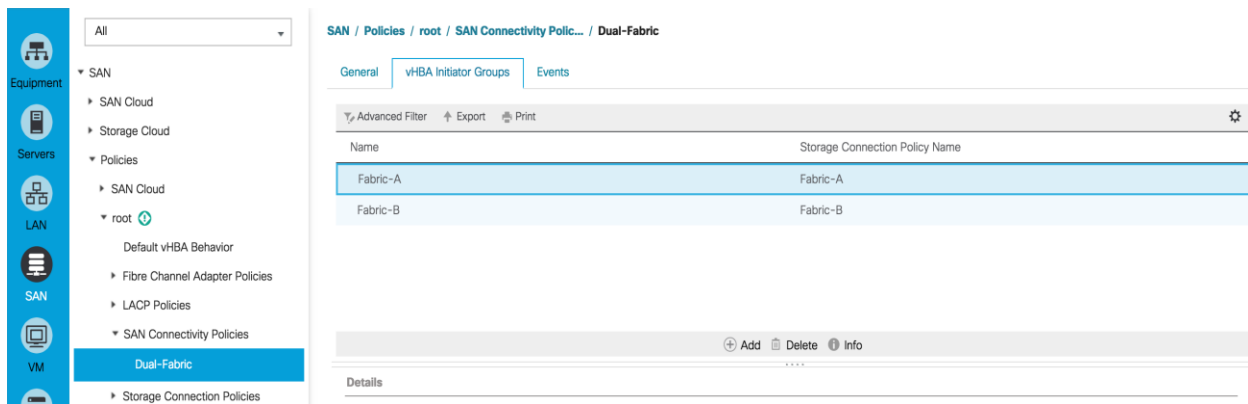




22. Enter Fabric-A for the Name.
23. Click the Fabric-A select box.
24. For Storage Connection Policy, select Fabric-A.



25. Click OK, then click OK again.
26. Click the Add button to add another vHBA Initiator Group.
27. For the Name input Fabric-B.
28. Select the checkbox Fabric-B.
29. For Storage Connection Policy, select Fabric-B.
30. Click OK, then click OK again.



## Create Boot Policies

This procedure applies to a Cisco UCS environment in which two FC interfaces are used on the IBM Storwize V5030 Node 1 and two FC interfaces are used on Node 2. This procedure captures a single boot policy, which defines Fabric-A as the primary fabric. Customer can choose to create a second boot policy that can use Fabric-B as primary fabric to spread the boot-from-san traffic load on both the nodes in case of disaster recovery.

WWPN information from the IBM v5030 is required to complete this section. This information can be found by logging into the IBM Storwize GUI and hovering the mouse over the FC ports as shown in the figure below, the same information has been captured as part of the procedure in Table 13. The information can be recorded in Table 14.

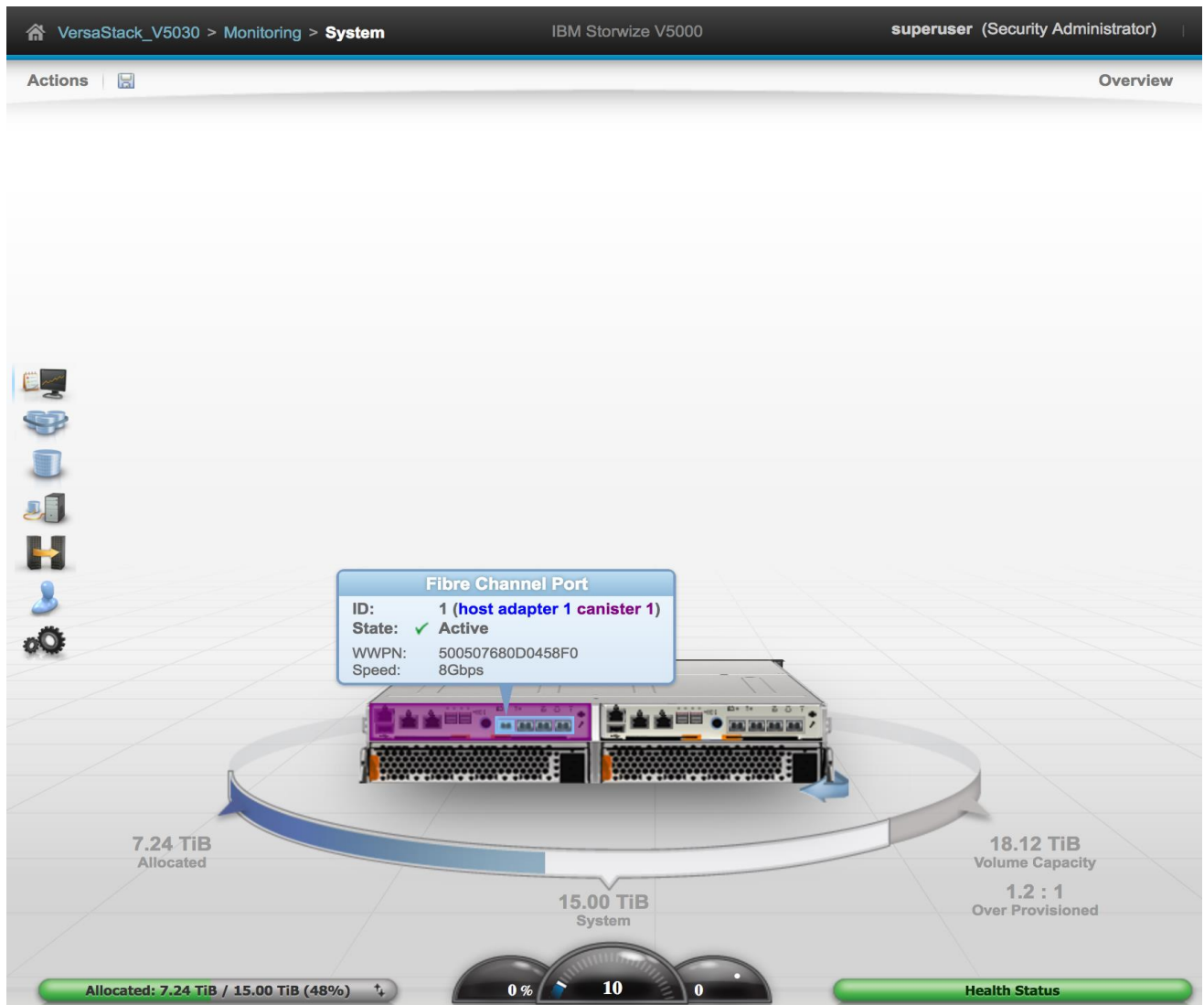


Table 14 IBM V5030 – WWPN Information

Node	Port ID	WWPN	Variable
Node 1	1		WWPN-Node-1-Fabric-A
Node 1	2		WWPN-Node-1-Fabric-B
Node 2	1		WWPN-Node-2-Fabric-A
Node 2	2		WWPN-Node-2-Fabric-B

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



You will use the WWPN variables that were logged in 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).

### Create Boot Policy ? X

Name :

Description :

Reboot on Boot Order Change :

Enforce vNIC/vHBA/iSCSI Name :

Boot Mode :  Legacy  Uefi

**WARNINGS:**  
 The type (primary/secondary) does not indicate a boot order presence.  
 The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.  
 If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.  
 If it is not selected, the vNICs/vHBAs are selected if they exist, otherwise the vNIC/vHBA with the lowest PCIe bus scan order is used.

Local Devices

Add Local Disk

- Add Local LUN
- Add Local JBOD
- Add SD Card
- Add Internal USB
- Add External USB
- Add Embedded Local LUN
- Add Embedded Local Disk

Add CD/DVD

- Add Local CD/DVD
- Add Remote CD/DVD

Add Floppy

- Add Local Floppy
- Add Remote Floppy

Add Remote Virtual Drive

**Boot Order**

Name	Or...	vNIC/...	Type	WWN	LUN N...	Slot N...	Boot ...	Boot ...	Descri...
CD/DVD	1								

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.

## Add SAN Boot



vHBA :

Type :  Primary  Secondary  Any



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 Node 1 connected to UCS Fabric Interconnect A << var\_wwpn\_FC\_NodeA-fabricA >>
16. Keep the Primary radio button selected as the SAN boot target type.
17. Click OK to add the SAN boot target.

## Add SAN Boot Target



Boot Target LUN :

Boot Target WWPN :

Type :  Primary  Secondary

OK

Cancel

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 Node 2 connected to UCS Fabric Interconnect A <<  
var\_wwpn\_FC\_NodeB-fabricA >>

21. Click OK to add the SAN boot target.

## Add SAN Boot Target



Boot Target LUN :

Boot Target WWPN :

Type :  Primary  Secondary

OK

Cancel

22. From the vHBA drop-down menu, choose Add SAN Boot.
23. In the Add SAN Boot dialog box, enter Fabric-B in the vHBA box.
24. The SAN boot type should automatically be set to Secondary.
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 Node 2 connected to UCS Fabric Interconnect B << var\_wwpn\_FC\_NodeB-fabricB >>
29. Keep Primary as the SAN boot target type.
30. Click OK to add the SAN boot target.

## Add SAN Boot Target



Boot Target LUN :

Boot Target WWPN :

Type :  Primary  Secondary

OK

Cancel

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 Node 1 connected to UCS Fabric Interconnect B << var\_wwpn\_FC\_NodeA-fabricB >>
34. Click OK to add the SAN boot target.

## Add SAN Boot Target



Boot Target LUN :

Boot Target WWPN :

Type :  Primary  Secondary

**OK**

**Cancel**

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



## Create Boot Policy



Name :

Description :

Reboot on Boot Order Change :

Enforce vNIC/vHBA/iSCSI Name :

Boot Mode :  Legacy  Uefi

**WARNINGS:**

The type (primary/secondary) does not indicate a boot order presence.

The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.

If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.

If it is not selected, the vNICs/vHBAs are selected if they exist, otherwise the vNIC/vHBA with the lowest PCIe bus scan order is used.

**Boot Order**

Name	vNIC/v...	Type	WWN	...	...	...	...
▼ SAN Primary		Fabric-A	Primary				
SAN Target Primary			Primary	50:05:07:68:0D:04:58:F0	0		
SAN Target Secondary			Secondary	50:05:07:68:0D:08:58:F0	0		
▼ SAN Secondary		Fabric-B	Secondary				
SAN Target Primary			Primary	50:05:07:68:0D:04:58:F1	0		
SAN Target Secondary			Secondary	50:05:07:68:0D:08:58:F1	0		

OK

Cancel

## Configure UCS LAN Connectivity

## Configure Uplink Port Channels to Cisco Nexus Switches

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

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



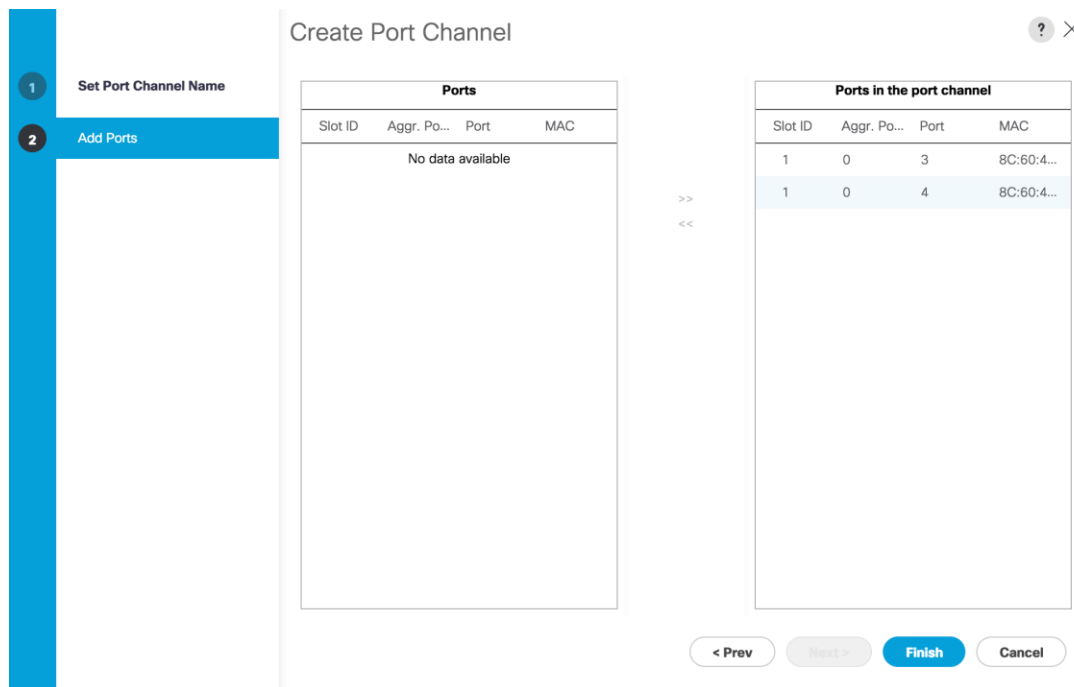
In this procedure, two port channels are created: one from fabric A to both Cisco Nexus switches and one from fabric B to both Cisco Nexus switches.

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

5. Enter 13 as the unique ID of the port channel.
6. Enter vPC-13-Nexus as the name of the port channel.
7. Click Next.

The screenshot shows the 'Create Port Channel' configuration window. The title bar includes a help icon (?) and a close icon (X). The left sidebar has two steps: '1 Set Port Channel Name' (highlighted) and '2 Add Ports'. The main configuration area shows 'ID : 13' and 'Name : vPC-13-Nexus'. At the bottom right, there are four buttons: '< Prev', 'Next >', 'Finish', and 'Cancel'.

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



12. In the navigation pane, under LAN > LAN Cloud, expand the fabric B tree.

13. Right-click Port Channels.

14. Select Create Port Channel.

15. Enter 14 as the unique ID of the port channel.

16. Enter vPC-14-Nexus as the name of the port channel.

17. Click Next.

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

- Slot ID 1 and port 3
- Slot ID 1 and port 4

19. Click >> to add the ports to the port channel.

20. Click Finish to create the port channel.

21. Click OK.

## Create MAC Address Pools

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

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

2. Select Pools > root.



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

3. Right-click MAC Pools under the root organization.
4. Select Create MAC Pool to create the MAC address pool.
5. Enter MAC\_Pool\_A as the name of the MAC pool.
6. Optional: Enter a description for the MAC pool.
7. Click Next.

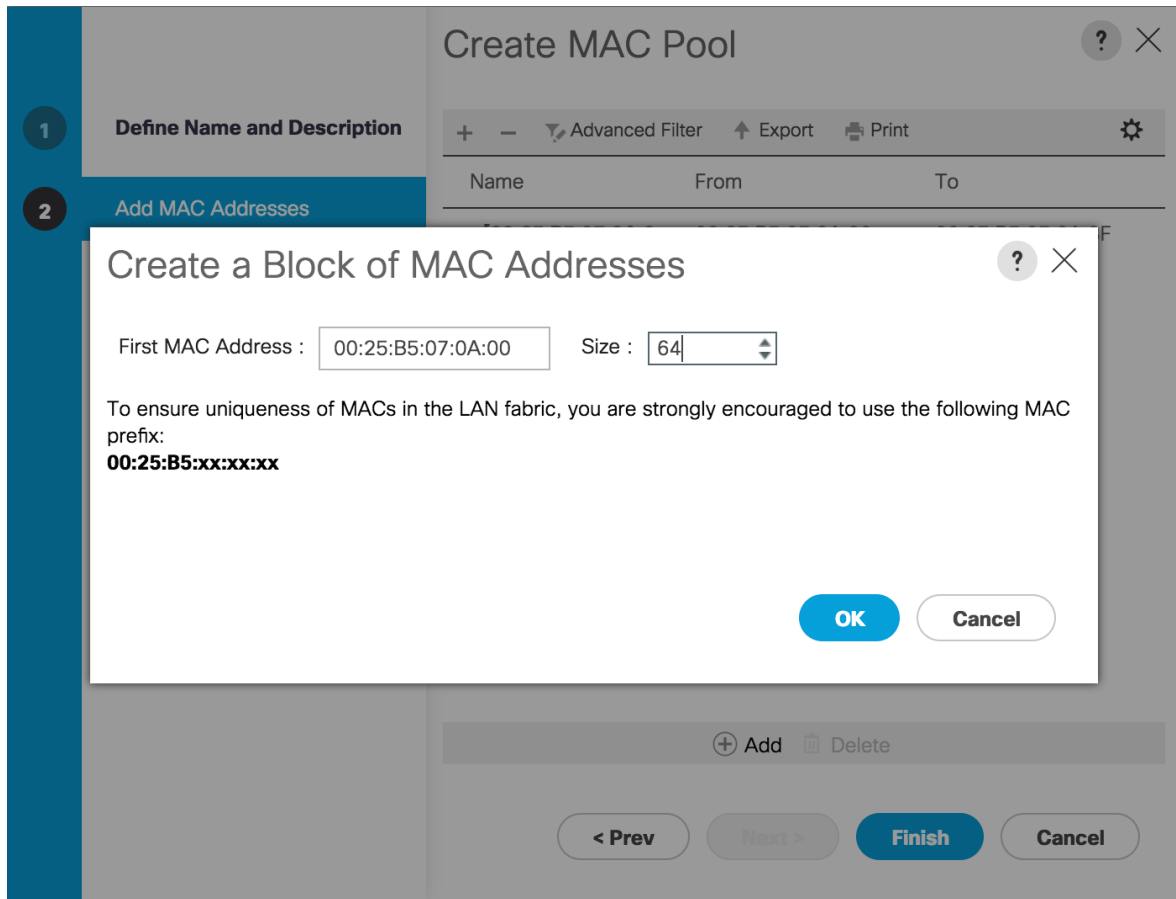
The screenshot shows the Cisco UCS configuration interface. On the left is a navigation tree with categories like Equipment, Servers, LAN, SAN, VM, Storage, Chassis, and Admin. The 'LAN' category is expanded, and 'MAC Pools' is selected. The main area shows the 'Create MAC Pool' dialog box. The dialog has a breadcrumb 'LAN / Pools / root / MAC Pools'. It has two steps: '1 Define Name and Description' and '2 Add MAC Addresses'. The 'Name' field is filled with 'MAC\_Pool\_A'. The 'Description' field is empty. The 'Assignment Order' is set to 'Default' (radio button selected). At the bottom, there are buttons for '< Prev', 'Next >', 'Finish', and 'Cancel'. The 'Next >' button is highlighted in blue.

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.

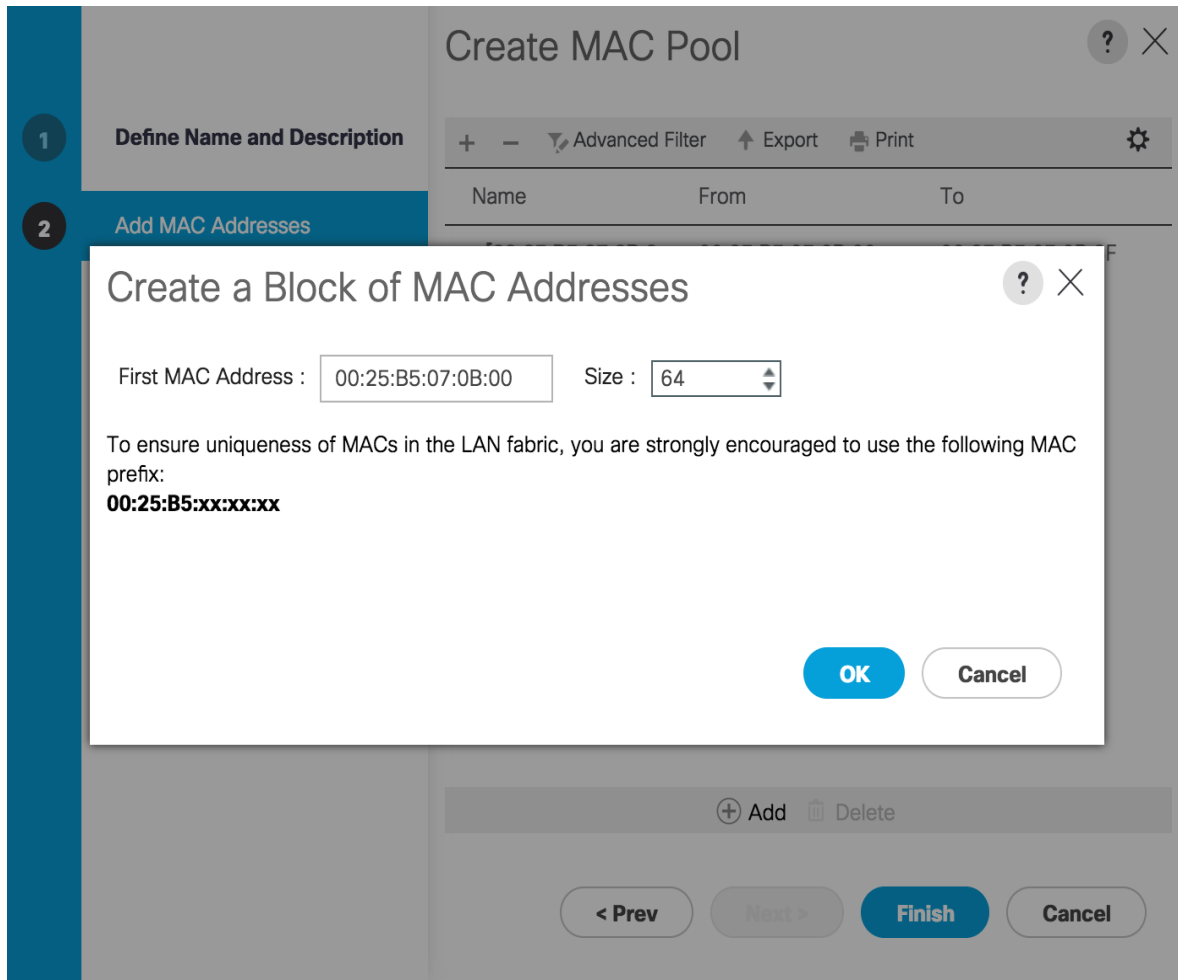


11. Click OK.
12. Click Finish.
13. In the confirmation message, click OK.
14. Right-click MAC Pools under the root organization.
15. Select Create MAC Pool to create the MAC address pool.
16. Enter MAC\_Pool\_B as the name of the MAC pool.
17. Optional: Enter a description for the MAC pool.
18. Click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

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



- Click OK.
- Click Finish.
- In the confirmation message, click OK.

## Create VLANs

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

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



In this procedure, five VLANs are created.

---

- 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.

### Create VLANs ? ×

VLAN Name/Prefix :

Multicast Policy Name :  [Create Multicast Policy](#)

Common/Global
  Fabric A
  Fabric B
  Both Fabrics Configured Differently

You are creating global VLANs that map to the same VLAN IDs in all available fabrics.  
 Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")

VLAN IDs :

Sharing Type :  None  Primary  Isolated  Community

Check Overlap

OK

Cancel

10. Right-click VLANs.
11. Select Create VLANs
12. Enter vMotion-VLAN as the name of the VLAN to be used for vMotion.
13. Keep the Common/Global option selected for the scope of the VLAN.
14. Enter the <<var\_vmotion\_vlan\_id>> as the ID of the vMotion 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 VM-Traffic-VLAN as the name of the VLAN to be used for the VM traffic.
20. Keep the Common/Global option selected for the scope of the VLAN.
21. Enter the <<var\_vm-traffic\_vlan\_id>> for the VM Traffic 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 Native-VLAN as the name of the VLAN to be used as the native VLAN.
27. Keep the Common/Global option selected for the scope of the VLAN.
28. Enter the <<var\_native\_vlan\_id>> as the ID of the native VLAN.
29. Keep the Sharing Type as None.
30. Click OK and then click OK again.
31. Expand the list of VLANs in the navigation pane, right-click the newly created Native-VLAN and select Set as Native VLAN.
32. Click Yes, and then click OK.

## Set Jumbo Frames in Cisco UCS Fabric

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

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



LAN / LAN Cloud / QoS System Class

General Events FSM

Priority	Enabled	CoS	Packet Drop	Weight	Weight (%)	MTU	Multicast Optimized
Platinum	<input type="checkbox"/>	5	<input type="checkbox"/>	10	N/A	normal	<input type="checkbox"/>
Gold	<input type="checkbox"/>	4	<input checked="" type="checkbox"/>	9	N/A	normal	<input type="checkbox"/>
Silver	<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	8	N/A	normal	<input type="checkbox"/>
Bronze	<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	7	N/A	normal	<input type="checkbox"/>
Best Effort	<input checked="" type="checkbox"/>	Any	<input checked="" type="checkbox"/>	5	50	9216	<input type="checkbox"/>
Fibre Channel	<input checked="" type="checkbox"/>	3	<input type="checkbox"/>	5	50	fc	N/A

## 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.

**Create Network Control Policy**

Name :

Description :

CDP :  Disabled  Enabled

MAC Register Mode :  Only Native Vlan  All Host Vlans

Action on Uplink Fail :  Link Down  Warning

**MAC Security**

Forge :  Allow  Deny

**LLDP**

8. Click OK.

## Create vNIC Templates

To create multiple virtual network interface card (vNIC) templates for the Cisco UCS environment, complete the following steps. A total of 6 vNIC Templates will be created.

### Create Management vNICs

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter vNIC\_Mgmt\_A as the vNIC template name.
6. Keep Fabric A selected.
7. Do not select the Enable Failover checkbox.
8. Select Primary Template for the Redundancy Type.
9. Leave Peer Redundancy Template as <not set>
10. Under Target, make sure that the VM checkbox is not selected.
11. Select Updating Template as the Template Type.

12. Under VLANs, select the checkboxes for IB-MGMT and Native-VLAN VLANs.

## Create vNIC Template ? X

Name :

Description :

Fabric ID :  Fabric A  Fabric B  Enable Failover

**Redundancy**

---

Redundancy Type :  No Redundancy  Primary Template  Secondary Template

Peer Redundancy Template :

**Target**

Adapter  
 VM

**Warning**

---

If **VM** is selected, a port profile by the same name will be created.  
 If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type :  Initial Template  Updating Template

**VLANs**

Advanced Filter Export Print ⚙️

Select	Name	Native VLAN
<input type="checkbox"/>	<b>default</b>	<input type="radio"/>
<input checked="" type="checkbox"/>	<b>IB-MGMT-VLAN</b>	<input type="radio"/>
<input checked="" type="checkbox"/>	<b>Native-VLAN</b>	<input checked="" type="radio"/>

13. Set Native-VLAN as the native VLAN.

14. Leave vNIC Name selected for the CDN Source.

15. Leave 1500 for the MTU.

16. In the MAC Pool list, select MAC\_Pool\_A.

17. In the Network Control Policy list, select Enable\_CDP.

## Create vNIC Template



<input type="checkbox"/>	default	<input type="radio"/>
<input checked="" type="checkbox"/>	IB-MGMT-VLAN	<input type="radio"/>
<input checked="" type="checkbox"/>	Native-VLAN	<input checked="" type="radio"/>
<input type="checkbox"/>	VM-Traffic-VLAN	<input type="radio"/>
<input type="checkbox"/>	vMotion-VLAN	<input type="radio"/>

CDN Source :  vNIC Name  User Defined

MTU : 1500

MAC Pool : MAC\_Pool\_A(32/32) ▼

QoS Policy : <not set> ▼

Network Control Policy : Enable\_CDP ▼

Pin Group : <not set> ▼

Stats Threshold Policy : default ▼

#### Connection Policies

Dynamic vNIC  usNIC  VMQ

Dynamic vNIC Connection Policy : <not set> ▼

OK

Cancel

18. Click OK to create the vNIC template.

19. Click OK.

Follow these similar steps for the vNIC\_Mgmt\_B Template:

1. In the navigation pane, select the LAN tab.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template
5. Enter vNIC\_Mgmt\_B as the vNIC template name.

6. Select Fabric B.
7. Do not select the Enable Failover checkbox.
8. Select Secondary Template for Redundancy Type.
9. For the Peer Redundancy Template pulldown, select vNIC\_Mgmt\_A.
10. Under Target, make sure the VM checkbox is not selected.
11. Select Updating Template as the template type.
12. Under VLANs, select the checkboxes for IB-MGMT and Native-VLAN VLANs.

## Create vNIC Template



Name : vNIC\_Mgmt\_B

Description :

Fabric ID :  Fabric A  Fabric B  Enable Failover

### Redundancy

Redundancy Type :  No Redundancy  Primary Template  Secondary Template

Peer Redundancy Template : vNIC\_Mgmt\_A ▼

### Target

Adapter

VM

### Warning

If **VM** is selected, a port profile by the same name will be created.  
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type :  Initial Template  Updating Template

### VLANs

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input checked="" type="checkbox"/>	IB-MGMT-VLAN	<input type="radio"/>
<input checked="" type="checkbox"/>	Native-VLAN	<input checked="" type="radio"/>

OK

Cancel

13. Set default as the native VLAN.
14. Leave vNIC Name selected for the CDN Source.
15. Leave 1500 for the MTU.
16. In the MAC Pool list, select MAC\_Pool\_B.
17. In the Network Control Policy list, select Enable\_CDP.

## Create vNIC Template



### VLANs

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input checked="" type="checkbox"/>	IB-MGMT-VLAN	<input type="radio"/>
<input checked="" type="checkbox"/>	Native-VLAN	<input checked="" type="radio"/>
<input type="checkbox"/>	VM-Traffic-VLAN	<input type="radio"/>
<input type="checkbox"/>	vMotion-VLAN	<input type="radio"/>

CDN Source :  vNIC Name  User Defined

MTU :

MAC Pool :  ▼

QoS Policy :  ▼

Network Control Policy :  ▼

Pin Group :  ▼

Stats Threshold Policy :  ▼

### Connection Policies

Dynamic vNIC  usNIC  VMQ

Dynamic vNIC Connection Policy :  ▼

OK

Cancel

18. Click OK to create the vNIC template.

19. Click OK.

#### Create vMotion vNICs

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter vNIC\_vMotion\_A as the vNIC template name.
6. Keep Fabric A selected.
7. Do not select the Enable Failover checkbox.
8. Select Primary Template for the Redundancy Type.
9. Leave Peer Redundancy Template as <not set>
10. Under Target, make sure that the VM checkbox is not selected.
11. Select Updating Template as the Template Type.
12. Under VLANs, select the checkboxes vMotion as the only VLAN.

## Create vNIC Template



Name : vNIC\_vMotion\_A

Description :

Fabric ID :  Fabric A  Fabric B  Enable Failover

### Redundancy

Redundancy Type :  No Redundancy  Primary Template  Secondary Template

Peer Redundancy Template : <not set> ▼

### Target

Adapter

VM

### Warning

If **VM** is selected, a port profile by the same name will be created.  
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type :  Initial Template  Updating Template

### VLANs

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	IB-MGMT-VLAN	<input type="radio"/>
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>

OK

Cancel

- Set vMotion as the native VLAN.
- For MTU, enter 9000.
- In the MAC Pool list, select MAC\_Pool\_A.
- In the Network Control Policy list, select Enable\_CDP.



## Create vNIC Template



### VLANs

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	IB-MGMT-VLAN	<input type="radio"/>
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>
<input type="checkbox"/>	VM-Traffic-VLAN	<input type="radio"/>
<input checked="" type="checkbox"/>	vMotion-VLAN	<input checked="" type="radio"/>

CDN Source :  vNIC Name  User Defined

MTU :

MAC Pool :

QoS Policy :

Network Control Policy :

Pin Group :

Stats Threshold Policy :

### Connection Policies

Dynamic vNIC  usNIC  VMQ

Dynamic vNIC Connection Policy :

OK

Cancel

17. Click OK to create the vNIC template.

18. Click OK.

Follow these similar steps for the vNIC\_vMotion\_B Template:

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

5. Enter vNIC\_vMotion\_B as the vNIC template name.
6. Select Fabric B.
7. Do not select the Enable Failover checkbox.
8. Select Secondary Template for Redundancy Type.
9. For the Peer Redundancy Template pulldown, select vNIC\_vMotion\_A.
10. Under Target, make sure the VM checkbox is not selected.
11. Select Updating Template as the template type.
12. Under VLANs, select the **checkbox for the** vMotion VLAN.

## Create vNIC Template



Name : vNIC\_vMotion\_B

Description :

Fabric ID :  Fabric A  Fabric B  Enable Failover

### Redundancy

Redundancy Type :  No Redundancy  Primary Template  Secondary Template

Peer Redundancy Template : <not set>

### Target

Adapter  
 VM

<not set>  
 Domain Policies  
 vNIC\_Mgmt\_A  
**vNIC\_vMotion\_A**

### Warning

If **VM** is selected, a port profile by the same name will be created.  
 If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type :  Initial Template  Updating Template

### VLANs

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	IB-MGMT-VLAN	<input type="radio"/>
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>
<input type="checkbox"/>		<input type="radio"/>

OK

Cancel

13. Select vNIC Name for the CDN Source.
14. For MTU, enter 9000.
15. In the MAC Pool list, select MAC\_Pool\_B.
16. In the Network Control Policy list, select Enable\_CDP.

## Create vNIC Template



### VLANs

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	IB-MGMT-VLAN	<input type="radio"/>
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>
<input type="checkbox"/>	VM-Traffic-VLAN	<input type="radio"/>
<input checked="" type="checkbox"/>	vMotion-VLAN	<input checked="" type="radio"/>

CDN Source :  vNIC Name  User Defined

MTU :

MAC Pool :

QoS Policy :

Network Control Policy :

Pin Group :

Stats Threshold Policy :

### Connection Policies

Dynamic vNIC  usNIC  VMQ

Dynamic vNIC Connection Policy :

OK

Cancel

17. Click OK to create the vNIC template.

18. Click OK.

### Create VM Traffic vNICs

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

4. Select Create vNIC Template.
5. Enter vNIC\_VM\_A as the vNIC template name.
6. Keep Fabric A selected.
7. Do not select the Enable Failover checkbox.
8. Select Primary Template for the Redundancy Type.
9. Leave Peer Redundancy Template as <not set>
10. Under Target, make sure that the VM checkbox is not selected.
11. Select Updating Template as the Template Type.
12. Under VLANs, select the checkboxes for any application or production VLANs that should be delivered to the ESXi hosts.

## Create vNIC Template



Name : vNIC\_VM\_A

Description :

Fabric ID :  Fabric A  Fabric B  Enable Failover

**Redundancy**

Redundancy Type :  No Redundancy  Primary Template  Secondary Template

Peer Redundancy Template : <not set>

**Target**

- Adapter
- VM

**Warning**

If **VM** is selected, a port profile by the same name will be created.  
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type :  Initial Template  Updating Template

**VLANs**

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	IB-MGMT-VLAN	<input type="radio"/>
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>

OK

Cancel

- For MTU, enter 9000.
- In the MAC Pool list, select MAC\_Pool\_A.
- In the Network Control Policy list, select Enable\_CDP.

## Create vNIC Template



## VLANs

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	IB-MGMT-VLAN	<input type="radio"/>
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>
<input checked="" type="checkbox"/>	VM-Traffic-VLAN	<input type="radio"/>
<input type="checkbox"/>	vMotion-VLAN	<input type="radio"/>

CDN Source :  vNIC Name  User Defined

MTU :

MAC Pool :

QoS Policy :

Network Control Policy :

Pin Group :

Stats Threshold Policy :

## Connection Policies

Dynamic vNIC  usNIC  VMQ

Dynamic vNIC Connection Policy :

OK

Cancel

16. Click OK to create the vNIC template.

17. Click OK.

Follow these similar steps for the vNIC\_VM\_B Template:

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

5. Enter vNIC\_VM\_B as the vNIC template name.
6. Select Fabric B.
7. Do not select the Enable Failover checkbox.
8. Select Secondary Template for Redundancy Type.
9. For the Peer Redundancy Template pulldown, select vNIC\_VM\_A.
10. Under Target, make sure the VM checkbox is not selected.

## Create vNIC Template ? X

Name :

Description :

Fabric ID :  Fabric A  Fabric B  Enable Failover

**Redundancy**

Redundancy Type :  No Redundancy  Primary Template  Secondary Template

Peer Redundancy Template : 

- <not set>
- Domain Policies
- vNIC\_Mgmt\_A
- vNIC\_VM\_A
- vNIC\_vMotion\_A

**Target**

Adapter

VM

**Warning**

If **VM** is selected, a port profile by the same name will be created.  
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type :  Initial Template  Updating Template

**VLANs**

Advanced Filter ↑ Export Print ⚙

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	IB-MGMT-VLAN	<input type="radio"/>
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>

11. Select Updating Template as the template type.



12. Under VLANs, select the same checkboxes for the application or production VLANs selected for the vNIC\_App\_A vNIC Template.
13. Set default as the native VLAN.
14. Select vNIC Name for the CDN Source.
15. For MTU, enter 9000.
16. In the MAC Pool list, select MAC\_Pool\_B.
17. In the Network Control Policy list, select Enable\_CDP.

## Create vNIC Template



### VLANs

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	IB-MGMT-VLAN	<input type="radio"/>
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>
<input checked="" type="checkbox"/>	VM-Traffic-VLAN	<input type="radio"/>
<input type="checkbox"/>	vMotion-VLAN	<input type="radio"/>

CDN Source :  vNIC Name  User Defined

MTU :

MAC Pool :

QoS Policy :

Network Control Policy :

Pin Group :

Stats Threshold Policy :

### Connection Policies

Dynamic vNIC  usNIC  VMQ

Dynamic vNIC Connection Policy :

OK

Cancel

18. Click OK to create the vNIC template.

19. Click OK.

## Create LAN Connectivity Policy

To configure the necessary Infrastructure LAN Connectivity Policy, complete the following steps:

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

3. Right-click LAN Connectivity Policies.
4. Select Create LAN Connectivity Policy.
5. Enter Infra-LAN-Policy as the name of the policy.
6. Click the Add button to add a vNIC.
7. In the Create vNIC dialog box, enter 00-Mgmt-A as the name of the vNIC.
8. Select the Use vNIC Template checkbox.
9. In the vNIC Template list, select vNIC\_Mgmt\_A.
10. In the Adapter Policy list, select VMWare.

## Create vNIC

Name : Use vNIC Template : Redundancy Pair : Peer Name : vNIC Template : [Create vNIC Template](#)

Adapter Perform

Adapter Policy

&lt;not set&gt;

Domain Policies

vNIC\_Mgmt\_A

vNIC\_Mgmt\_B

vNIC\_VM\_A

vNIC\_VM\_B

vNIC\_vMotion\_A

vNIC\_vMotion\_B

[Create Ethernet Adapter Policy](#)

OK

Cancel

11. Click OK to add this vNIC to the policy.
12. Click the upper Add button to add another vNIC to the policy.
13. In the Create vNIC box, enter 01-Mgmt-B as the name of the vNIC.
14. Select the Use vNIC Template checkbox.
15. In the vNIC Template list, select vNIC\_Mgmt\_B.
16. In the Adapter Policy list, select VMWare.
17. Click OK to add the vNIC to the policy.

## Create vNIC

Name : Use vNIC Template : Redundancy Pair : Peer Name : vNIC Template : [Create vNIC Template](#)

Adapter Perform

Adapter Policy

&lt;not set&gt;

Domain Policies

vNIC\_Mgmt\_A

vNIC\_Mgmt\_B

vNIC\_VM\_A

vNIC\_VM\_B

vNIC\_vMotion\_A

vNIC\_vMotion\_B

[Create Ethernet Adapter Policy](#)

OK

Cancel

18. Click the upper Add button to add a vNIC.
19. In the Create vNIC dialog box, enter 02-vMotion-A as the name of the vNIC.
20. Select the Use vNIC Template checkbox.
21. In the vNIC Template list, select vNIC\_vMotion\_A.
22. In the Adapter Policy list, select VMWare.

23. Click OK to add this vNIC to the policy.

## Create vNIC



Name :

Use vNIC Template :

Redundancy Pair :

Peer Name :

vNIC Template :

[Create vNIC Template](#)

**Adapter Perform**

Adapter Policy

- <not set>
- Domain Policies
- vNIC\_Mgmt\_A
- vNIC\_Mgmt\_B
- vNIC\_VM\_A
- vNIC\_VM\_B
- vNIC\_vMotion\_A**
- vNIC\_vMotion\_B

[Create Ethernet Adapter Policy](#)

OK

Cancel

24. Click the upper Add button to add a vNIC to the policy.

25. In the Create vNIC dialog box, enter 03-vMotion-B as the name of the vNIC.

26. Select the Use vNIC Template checkbox.

27. In the vNIC Template list, select vNIC\_vMotion\_B.

28. In the Adapter Policy list, select VMWare.

## Create vNIC



Name : 03-vMotion-B

Use vNIC Template : Redundancy Pair : Peer Name : 

vNIC Template : &lt;not set&gt;

Create vNIC Template

Adapter Perform

Adapter Policy

&lt;not set&gt;

Domain Policies

vNIC\_Mgmt\_A

vNIC\_Mgmt\_B

vNIC\_VM\_A

vNIC\_VM\_B

vNIC\_vMotion\_A

vNIC\_vMotion\_B

Create Ethernet Adapter Policy

OK

Cancel

20. Click OK to add this vNIC to the policy.
29. Click the upper Add button to add a vNIC.
30. In the Create vNIC dialog box, enter 04-VM-A as the name of the vNIC.
31. Select the Use vNIC Template checkbox.
32. In the vNIC Template list, select vNIC\_VM\_A.
33. In the Adapter Policy list, select VMWare.
34. Click OK to add this vNIC to the policy.

### Create vNIC ? X

Name :

Use vNIC Template :

Redundancy Pair :

Peer Name :

vNIC Template : <not set> Create vNIC Template

---

Adapter Policy

Adapter Policy

<not set>

- Domain Policies
- vNIC\_Mgmt\_A
- vNIC\_Mgmt\_B
- vNIC\_VM\_A**
- vNIC\_VM\_B
- vNIC\_vMotion\_A
- vNIC\_vMotion\_B

Create Ethernet Adapter Policy

OK Cancel

35. Click the upper Add button to add a vNIC to the policy.
36. In the Create vNIC dialog box, enter 05-VM-B as the name of the vNIC.
37. Select the Use vNIC Template checkbox.
38. In the vNIC Template list, select vNIC\_VM\_B.
39. In the Adapter Policy list, select VMWare.



## Create vNIC



Name :

Use vNIC Template :

Redundancy Pair :

Peer Name :

vNIC Template :

[Create vNIC Template](#)

**Adapter Perform**

Adapter Policy

- <not set>
- Domain Policies
- vNIC\_Mgmt\_A
- vNIC\_Mgmt\_B
- vNIC\_VM\_A
- vNIC\_VM\_B**
- vNIC\_vMotion\_A
- vNIC\_vMotion\_B

[Create Ethernet Adapter Policy](#)

40. Click OK to add this vNIC to the policy.

## Create LAN Connectivity Policy



Name :

Description :

Click **Add** to specify one or more vNICs that the server should use to connect to the LAN.

Name	MAC Address	Native VLAN
vNIC 05-VM-B	Derived	
vNIC 04-VM-A	Derived	
vNIC 03-vMotion-B	Derived	
vNIC 02-vMotion-A	Derived	
vNIC 01-Mgmt-B	Derived	
vNIC 00-Mgmt-A	Derived	

OK

Cancel

41. Click OK to create the LAN Connectivity Policy.

42. Click OK.

## Create Service Profile Template

In this procedure, a service profile template is created to use FC Fabric A as primary boot path.

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

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root.
3. Right-click root.
4. Select Create Service Profile Template to open the Create Service Profile Template wizard.

5. Enter VM-Host-Infra-Fabric-A as the name of the service profile template. This service profile template is configured to boot from IBM Storwize V5030 Node 1 on fabric A.
6. Select the “Updating Template” option.
7. Under UUID, select UUID\_Pool as the UUID pool.

**Create Service Profile Template** ? X

You must enter a name for the service profile template and specify the template type. You can also specify how a UUID will be assigned to this template and enter a description.

Name :

The template will be created in the following organization. Its name must be unique within this organization.  
Where : **org-root**

The template will be created in the following organization. Its name must be unique within this organization.  
Type :  Initial Template  Updating Template

Specify how the UUID will be assigned to the server associated with the service generated by this template.  
UUID

UUID Assignment:

The UUID will be assigned from the selected pool.  
The available/total UUIDs are displayed after the pool name.

Optionally enter a description for the profile. The description can contain information about when and where the service profile should be used.

8. Click Next.

## Configure Storage Provisioning

1. If you have servers with no physical disks, click on the Local Disk Configuration Policy tab and select the SAN-Boot Local Storage Policy. Otherwise, select the default Local Storage Policy.

**Create Service Profile Template**

Optionally specify or create a Storage Profile, and select a local disk configuration policy.

Specific Storage Profile    Storage Profile Policy    **Local Disk Configuration Policy**

Local Storage: **SAN-Boot** ▼

Create Local Storage Policy

- Select Local Storage Policy to use
- Create a Specific Storage Policy
- Storage Policies
- SAN-Boot**
- Test
- default

Mode : **No Local Storage**

Protect Configuration : **Yes**

If **Protect Configuration** is set, the local disk configuration is preserved if the service profile is disassociated with the server. In that case, a configuration error will be raised when a new service profile is associated with that server if the local disk configuration in that profile is different.

FlexFlash

FlexFlash State : **Disable**

If **FlexFlash State** is disabled, SD cards will become unavailable immediately. Please ensure SD cards are not in use before disabling the FlexFlash State.

FlexFlash RAID Reporting State : **Disable**

< Prev    Next >    **Finish**    Cancel

2. Click Next.

### Configure Networking Options

1. Keep the default setting for Dynamic vNIC Connection Policy.
2. Select the “Use Connectivity Policy” option to configure the LAN connectivity.
3. Select Infra-LAN-Policy from the LAN Connectivity Policy pull-down.

**Create Service Profile Template** ? ×

Optionally specify LAN configuration information.

Dynamic vNIC Connection Policy:  ▼

[Create Dynamic vNIC Connection Policy](#)

---

How would you like to configure LAN connectivity?

Simple  Expert  No vNICs  Use Connectivity Policy

LAN Connectivity Policy :  ▼ [Create LAN Connectivity Policy](#)

Initiator Name

Initiator Name Assignment  ▼

▼

[Create IQN Suffix Pool](#)

**WARNING:** The selected pool does not contain any available entities. You can select it, but it is recommended that you add entities to it.

[< Prev](#) [Next >](#) [Finish](#) [Cancel](#)

4. Click Next.

## Configure Storage Options

1. Select the Use Connectivity Policy option for the “How would you like to configure SAN connectivity?” field.
2. Pick the Dual-Fabric option from the SAN Connectivity Policy pull-down.

**Create Service Profile Template** ? X

Optionally specify disk policies and SAN configuration information.

How would you like to configure SAN connectivity?

Simple
  Expert
  No vHBAs
  Use Connectivity Policy

SAN Connectivity Policy : Dual-Fabric ▼ Create SAN Connectivity Policy

<not set>

Domain Policies

Dual-Fabric

< Prev
Next >
Finish
Cancel

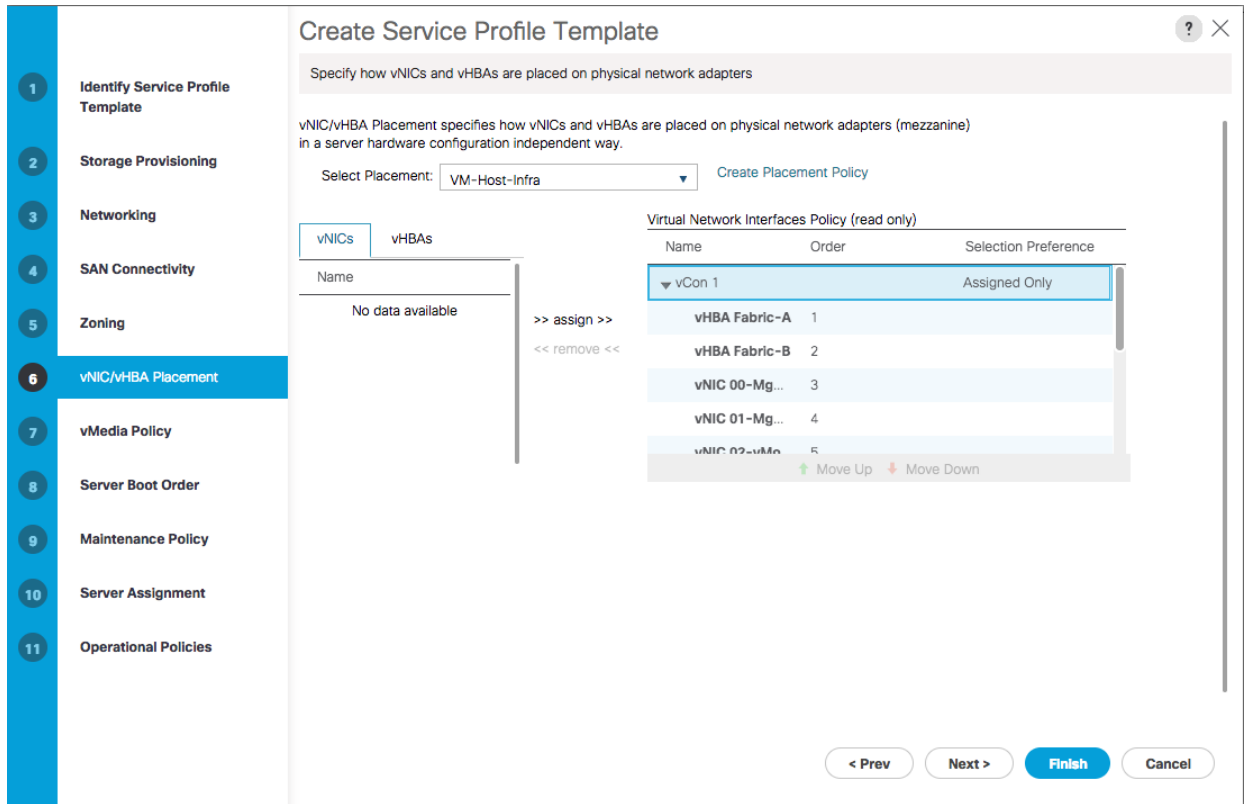
3. Click Next.

4. Click Next on the Zoning Options page.

### Configure vNIC/HBA Placement

1. In the **“Select Placement”** list, leave the placement policy as **“Let System Perform Placement”**.
2. Set the vNIC/vHBA placement options.
  - a. In the Select Placement list, choose the VM-Host-Infra placement policy.
  - b. Choose vCon1 and assign the vHBAs/vNICs to the virtual network interfaces policy in the following order:
    - vHBA Fabric-A
    - vHBA Fabric-B
    - vNIC 00-Mgmt-A
    - vNIC 01-Mgmt-B
    - vNIC 02-vMotion-A

- vNIC 03-vMotion-B
  - vNIC 04-VM-A
  - vNIC 05-VM-B
- c. Review the table to verify that all vNICs and vHBAs were assigned to the policy in the appropriate order.
3. Click Next.



### Configure vMedia Policy

1. Do not configure a vMedia Policy.
2. Click next.

**1 Identify Service Profile Template**

**2 Storage Provisioning**

**3 Networking**

**4 SAN Connectivity**

**5 Zoning**

**6 vNIC/vHBA Placement**

**7 vMedia Policy**

**8 Server Boot Order**

**9 Maintenance Policy**

**10 Server Assignment**

**11 Operational Policies**

### Create Service Profile Template

Optionally specify the Scriptable vMedia policy for this service profile template.

vMedia Policy:

[Create vMedia Policy](#)

The default boot policy will be used for this service profile.

< Prev   Next >   **Finish**   Cancel

3. Click Next.

### Configure Server Boot Order

1. Select Boot-Fabric-A for Boot Policy.



**Create Service Profile Template**

Optionally specify the boot policy for this service profile template.

Select a boot policy.

Boot Policy: **Boot-fabric-A** [Create Boot Policy](#)

Name : **Boot-fabric-A**  
 Description :  
 Reboot on Boot Order Change : **No**  
 Enforce vNIC/vHBA/iSCSI Name : **Yes**  
 Boot Mode : **Legacy**

**WARNINGS:**  
 The type (primary/secondary) does not indicate a boot order presence.  
 The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.  
 If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.  
 If it is not selected, the vNICs/vHBAs are selected if they exist, otherwise the vNIC/vHBA with the lowest PCIe bus scan order is used.

**Boot Order**

Name	Order	vNIC/vHB...	Type	WWN	LUN Name	Slot Numb...	Boot Name	Boot Path	Description
CD/DVD	1								
▶ San	2								

[Create iSCSI vNIC](#) [Set iSCSI Boot Parameters](#) [Set UEFI Boot Parameters](#)

[< Prev](#) [Next >](#) **Finish** [Cancel](#)

2. Click Next to continue to the next section.

## Configure Maintenance Policy

1. Change the Maintenance Policy to default.

**Create Service Profile Template**

Specify how disruptive changes such as reboots, network interruptions, and firmware upgrades should be applied to the server associated with this service profile.

⊖ Maintenance Policy

Select a maintenance policy to include with this service profile or create a new maintenance policy that will be accessible to all service profiles.

Maintenance Policy: Select (no policy used by default) ▾ [Create Maintenance Policy](#)

**Select (no policy used by default)**

Domain Policies

**default**

No maintenance policy is selected by default.  
The service profile will immediately reboot when disruptive changes are applied.

< Prev   Next >   **Finish**   Cancel

2. Click Next.

## Configure Server Assignment

To configure server assignment, complete the following steps:

1. In the Pool Assignment list, select Infra\_Pool.
2. Optional: Select a Server Pool Qualification policy.
3. Select Down as the power state to be applied when the profile is associated with the server.
4. **Select “UCSB-B200-M4” for the Server Pool Qualification.**
5. Firmware Management at the bottom of the page can be left alone as it will use default from the Host Firmware list.

**1 Identify Service Profile Template**

**2 Storage Provisioning**

**3 Networking**

**4 SAN Connectivity**

**5 Zoning**

**6 vNIC/vHBA Placement**

**7 vMedia Policy**

**8 Server Boot Order**

**9 Maintenance Policy**

**10 Server Assignment**

**11 Operational Policies**

### Create Service Profile Template

Optionally specify a server pool for this service profile template.

You can select a server pool you want to associate with this service profile template.

Pool Assignment:  [Create Server Pool](#)

Select the power state to be applied when this profile is associated with the server.

Up  Down

The service profile template will be associated with one of the servers in the selected pool. If desired, you can specify an additional server pool policy qualification that the selected server must meet. To do so, select the qualification from the list.

Server Pool Qualification :

Restrict Migration :

[< Prev](#) [Next >](#) [Finish](#) [Cancel](#)

6. Click Next.

## Configure Operational Policies

To configure the operational policies, complete the following steps:

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

**Create Service Profile Template** ? X

Optionally specify information that affects how the system operates.

BIOS Configuration

If you want to override the default BIOS settings, select a BIOS policy that will be associated with this service profile

BIOS Policy : VM-Host-Infra ▼

External IPMI Management Configuration

Management IP Address

Monitoring Configuration (Thresholds)

Power Control Policy Configuration

Power control policy determines power allocation for a server in a given power group.

Power Control Policy : default ▼ [Create Power Control Policy](#)

Scrub Policy

KVM Management

<not set>  
Domain Policies  
**No-Power-Cap**  
default

< Prev   Next >   **Finish**   Cancel

3. Click Finish to create the service profile template.
4. Click OK in the confirmation message.

## Create Service Profiles

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

1. Connect to the UCS 6324 Fabric Interconnect UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Service Template VM-Host-Prod-Fabric-A.
3. Right-click VM-Host-Infra-Fabric-A and select Create Service Profiles from Template.
4. Enter VM-Host-Infra-0 as the service profile prefix.
5. Leave 1 as **“Name Suffix Starting Number.”**
6. Leave 2 as the **“Number of Instances.”**
7. Click OK to create the service profiles.

Create Service Profiles From Template ? X  
 Naming Prefix : VM-Host-Infra-0  
 Name Suffix Starting Number : 1  
 Number of Instances : 2  
 OK Cancel

8. Click OK in the confirmation message to provision two VersaStack Service Profiles.

### Backup the Cisco UCS Manager Configuration

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

[http://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/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](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. 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. Insert the required information in the table below.

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. Click each service profile and click Storage and select vHBAs from the panel right side.

Servers / Service Profiles / root / Service Profile VM-Host-Infra...

General Storage Network iSCSI vNICs Boot Order Virtual Machines FC Zones Policies Server Details CIMC Sessions FSM VIF P&E

Storage Profiles Local Disk Configuration Policy **vHBAs** vHBA Initiator Groups

Local Disk Policy : **SAN-Boot**  
 Local Disk Policy Instance : org-root/local-disk-config-SAN-Boot

**SAN Connectivity Policy**

SAN Connectivity Policy : Dual-Fabric  
 SAN Connectivity Policy Instance : org-root/san-conn-pol-Dual-Fabric  
 Create SAN Connectivity Policy

**No Configuration Change of vNICs/vHBAs/iSCSI vNICs is allowed due to connectivity policy.**

vHBAs

Advanced Filter Export Print

Name	WWPN	Desired Or...	Actual Order	Fabric ID	Desired Place...	Actual Placem...	Admin Host Port	Actual Host Port
vHBA Fabri...	20:00:00:25:B5:01:0A:2F	1	4	A	1	1	ANY	1
vHBA Fabri...	20:00:00:25:B5:01:0B:2F	2	8	B	1	1	ANY	2

- 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 table provided.

Table 15 ESXi Hosts – WWPN Information

Source	Switch/ Port	Variable	WWPN
VM-Host-infra-01-A	Switch A	var_wwpn_VM-Host-Infra-01-A	
VM-Host-infra-01-B	Switch B	var_wwpn_VM-Host-Infra-01-B	
VM-Host-infra-02-A	Switch A	var_wwpn_VM-Host-Infra-02-A	
VM-Host-infra-02-B	Switch B	var_wwpn_VM-Host-Infra-02-B	

## Storage LUN Mapping

In this section, you will add the LUN mappings for the host profiles created through the Cisco UCS Manager to the V5000 storage, connecting to the boot LUNs and datastore LUNs. The WWPN's for the hosts will be required to complete this section.

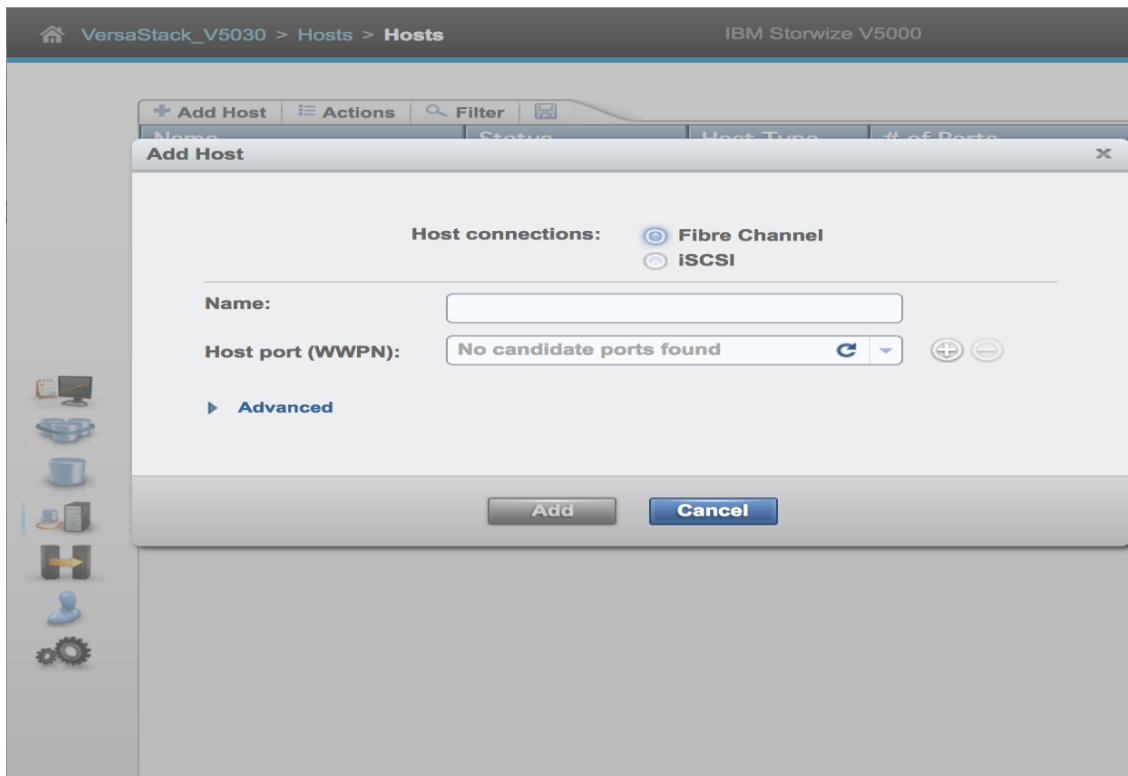
### Adding Hosts and Mapping Volumes on the IBM Storwize V5000

To add Hosts and Mapping Volumes on the IBM Storwize V5000, complete the following steps:

- Open the Storwize V5000 management GUI by navigating to <<var\_cluster\_mgmt\_ip>> and log in with your superuser or admin account.
- From the Navigation Dock, click the Host icon, and click the Hosts menu item.



3. Click Add Host in the upper left menu to bring up the Host wizard. Select the Fibre Channel Host 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 Fabric-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 **WWPN's for the Fabric-B** path, <<wwpn\_VM-Host-infra-01-b>>, and click add port to list.
7. Leave Advanced Settings as default (as below) 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 will see green check marks for each WWPN's.

**Add Host**
X

**Host connections:**     **Fibre Channel**  
 **iSCSI**

---

**Name:**

**Host port (WWPN):**  ⊕ ⊖

⊕ ⊖

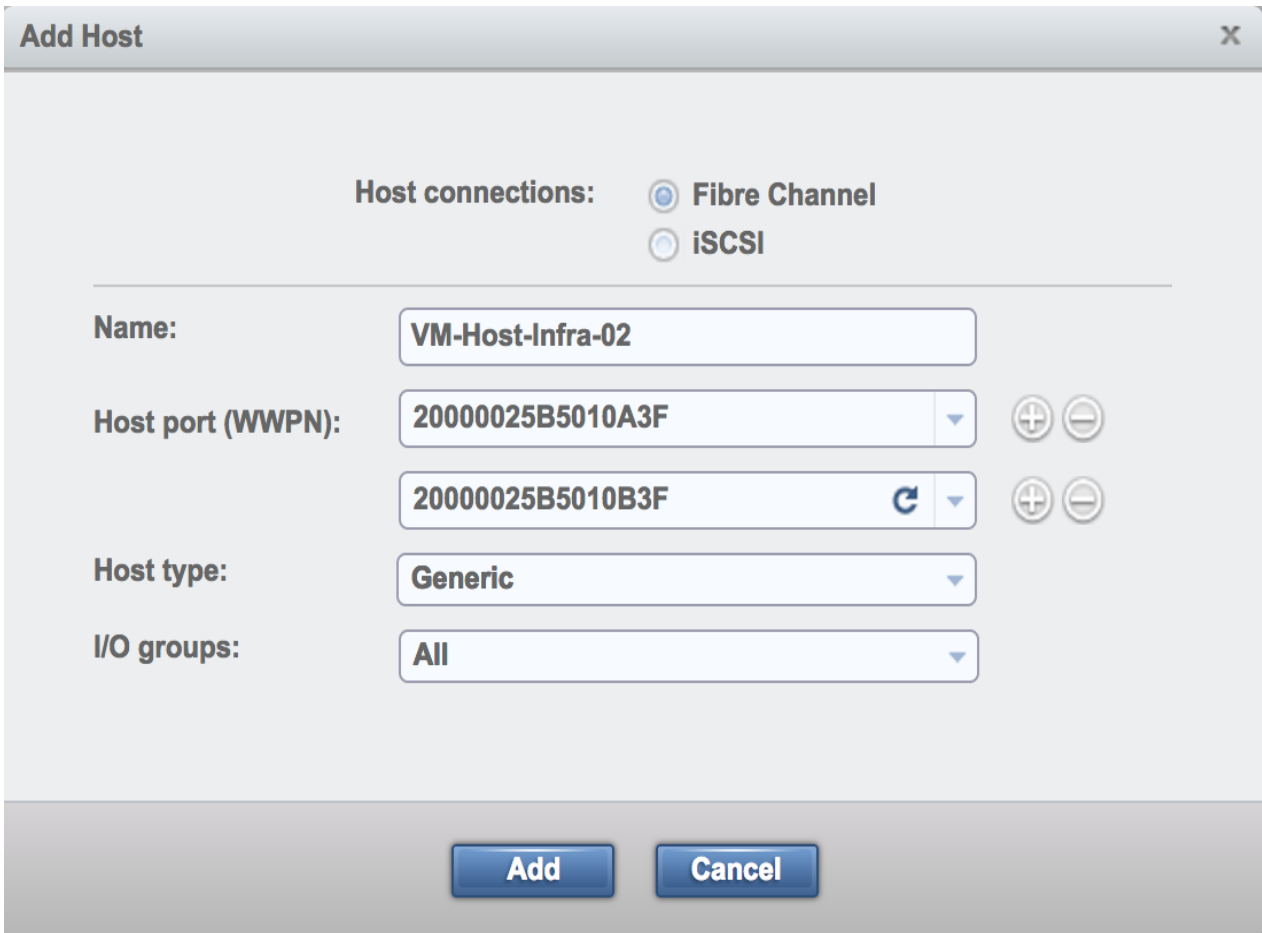
**Host type:**

**I/O groups:**

8. Click Add Host to create the second host.
9. Select the Fibre Channel Host option.
10. For Host Name input VM-Host-Infra-02.
11. For Fibre Channel Ports open the drop-down menu and select the WWPN's for the Fabric-A path vHBA's, <<var\_wwpn\_VM-Host-infra-02-a>>, and click Add Port to List.



12. Select the B port by selecting the var for the Fabric-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.



**Add Host**

Host connections:  Fibre Channel  
 iSCSI

Name: VM-Host-Infra-02

Host port (WWPN): 20000025B5010A3F  
20000025B5010B3F

Host type: Generic

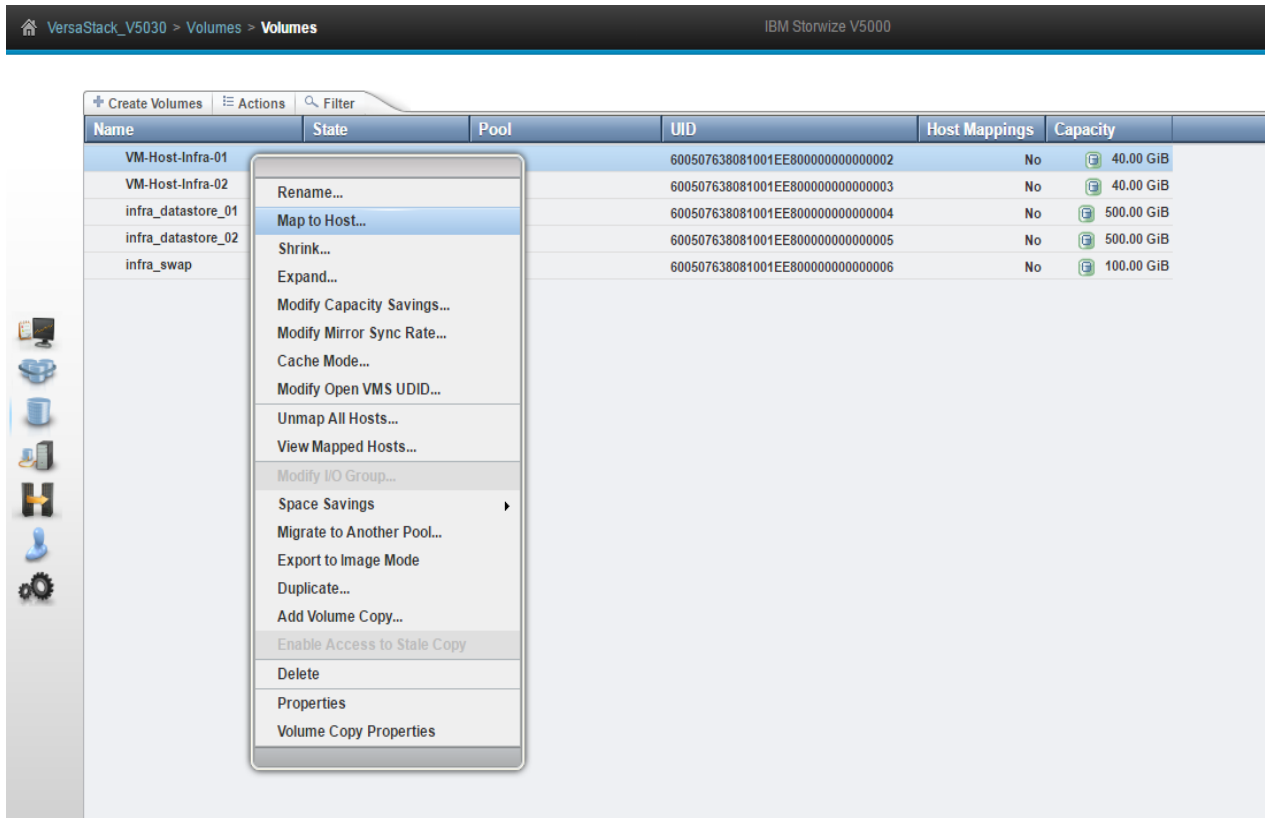
I/O groups: All

Add Cancel

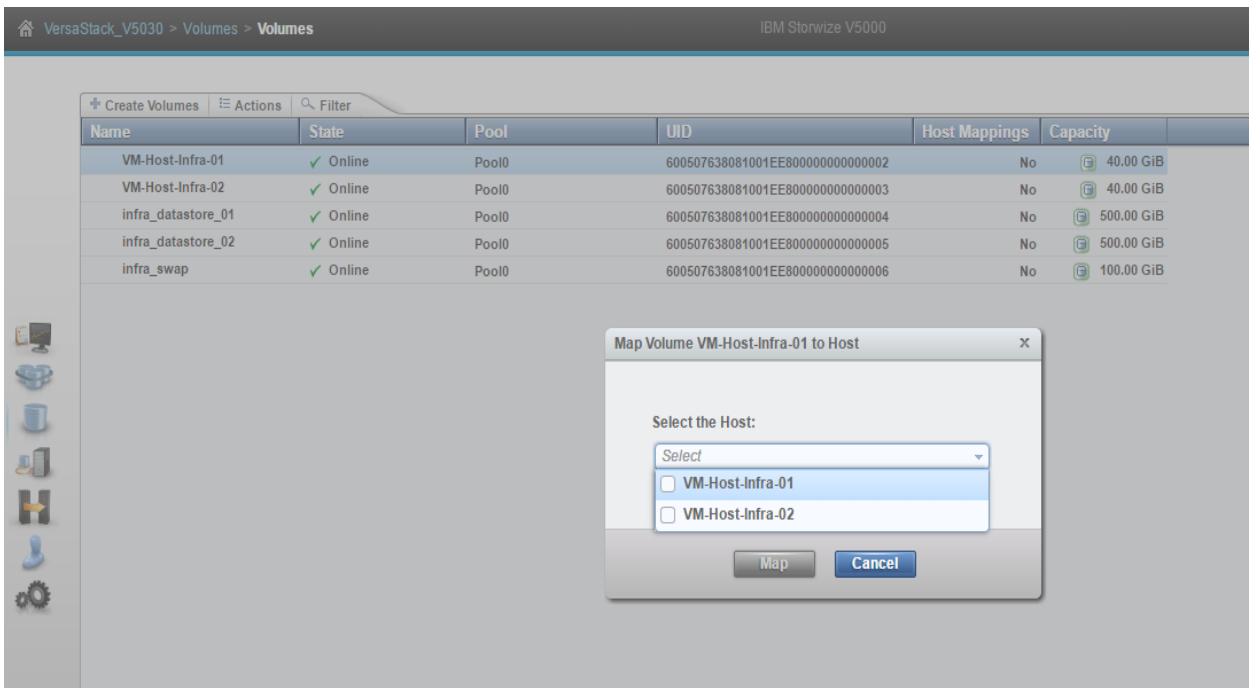
13. Click the Volumes icon from the Navigation Dock, then click the volumes menu item to display the created volumes.



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



15. In the drop-down, select VM-Host-Infra-01.



16. Click Map and then click Close on the *Modify Mappings* dialogue box.

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

18. In the drop-down, select VM-Host-Infra-02.

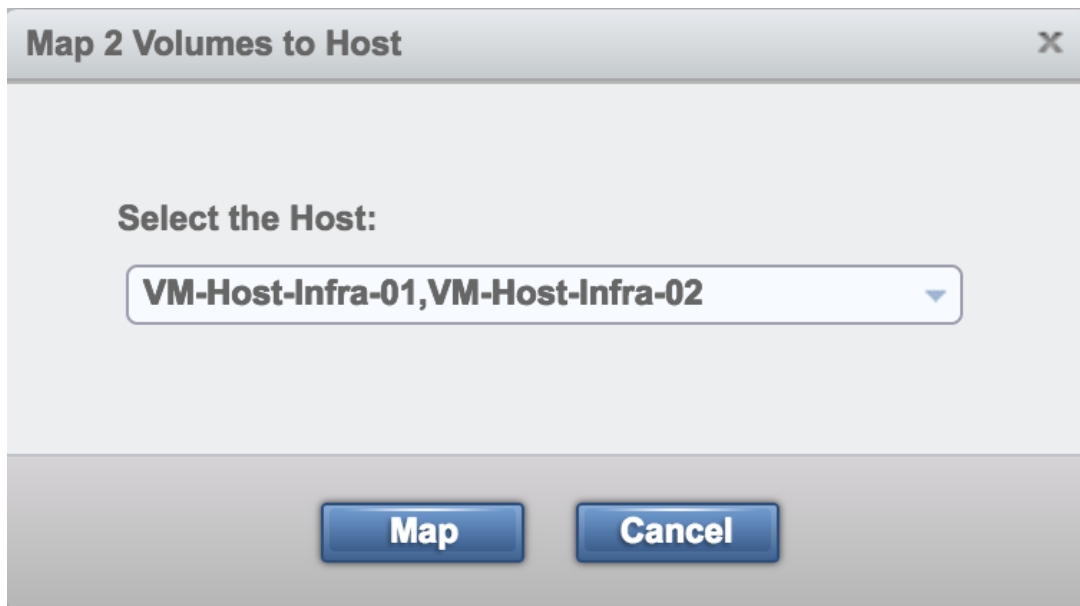


19. Click Map and then click Close on the *Modify Mappings* dialogue box

20. Map the volumes infra\_datastore\_1 and infra\_swap to the ESXi servers following the steps specified above.

21. Right-click while the volumes infra\_datastore\_1 and infra\_swap are selected.

22. In the drop-down, select VM-Host-Infra-01 and VM-Host-Infra-02.



## VMware vSphere Installation and Setup

---

### VersaStack VMware ESXi 6.0 Update 2 SAN Boot Installation

This section provides detailed instructions for installing VMware ESXi 6.0 Update 2 in a VersaStack environment. After the procedures are completed, two SAN-booted ESXi hosts will be provisioned. These deployment procedures are customized to include the environment variables.



Several methods exist for installing ESXi in a VMware environment. These procedures focus on how to use the built-in Keyboard, Video, Mouse (KVM) console and virtual media features in Cisco UCS Manager to map remote installation media to individual servers and connect to their boot logical unit numbers (LUNs). In this method, use the Cisco Custom ESXi 6.0 U2 GA ISO file which is downloaded from the URL below. This is required for this procedure as it contains custom Cisco drivers and thereby reduces installation steps.

---

To download the Custom ESX ISO:

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

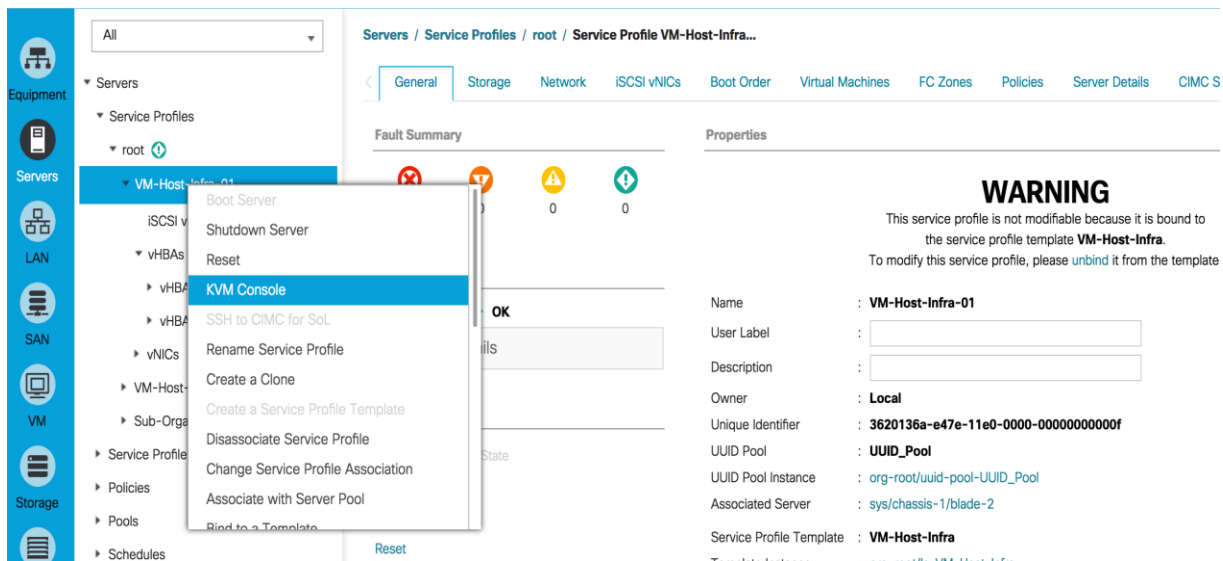
<https://my.vmware.com/web/vmware/details?downloadGroup=OEM-ESXI60U2-CISCO&productId=491>

### Log in to Cisco UCS 6324 Fabric Interconnect

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

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

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



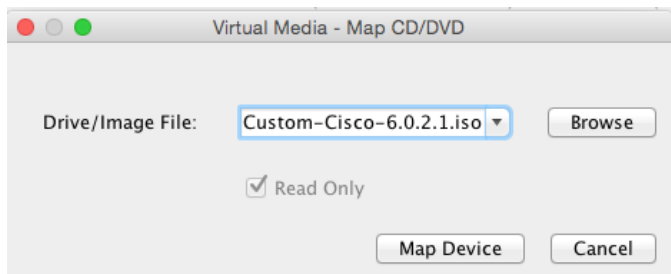
6. Select Servers > Service Profiles > root > VM-Host-Infra-02.
7. Right-click VM-Host-Infra-02 and select KVM Console Actions > KVM Console.

## VMware ESXi Installation

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

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

1. In the KVM window, click Virtual Media.
2. Click Activate Virtual Devices, select Accept this Session, then Apply.
3. Select Virtual Media, Map CD/DVD, then browse to the ESXi installer ISO image file and click Open.
4. Select the Map Device to map the newly added image.



5. Select Reset, then Ok and allow a power cycle and click the KVM tab to monitor the server boot.
6. As an alternate method; if the server is powered on, first shutdown the server, then boot the server by selecting Boot Server and clicking OK, then click OK again.

## Install ESXi on the Servers

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

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

1. On boot, the machine detects the presence of the ESXi installation media. Select the ESXi installer from the menu that is displayed.
2. After the installer is finished loading, press Enter to continue with the installation.
3. Read and accept the end-user license agreement (EULA). Press F11 to accept and continue.
4. Select the IBM LUN that was previously set up as the installation disk for ESXi and press Enter to continue with the installation.
5. Select the appropriate keyboard layout and press Enter.
6. Enter and confirm the root password and press Enter.
7. The installer issues a warning that existing partitions will be removed from the volume. Press F11 to continue with the installation.
8. After the installation is completed, 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 in the following section.

### ESXi Host VM-Host-Infra-01

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

1. After the server has finished rebooting, press F2 to customize the system.
2. Log in as root and enter the corresponding password.
3. Select the Configure the Management Network option and press Enter.
4. Select the VLAN (Optional) option and press Enter.
5. Enter the <<var\_ib-mgmt\_vlan\_id>> and press Enter.
6. From the Configure Management Network menu, select IP Configuration and press Enter.
7. Select the Set Static IP Address and Network Configuration option by using the space bar.

8. Enter the IP address for managing the first ESXi host: <<var\_vm\_host\_infra\_01\_ip>>.
9. Enter the subnet mask for the first ESXi host.
10. Enter the default gateway for the first ESXi host.
11. Press Enter to accept the changes to the IP configuration.
12. Select the IPv6 Configuration option and press Enter.
13. Using the spacebar, unselect Enable IPv6 (restart required) and press Enter.
14. Select the DNS Configuration option and press Enter.



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

---

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

### ESXi Host VM-Host-Infra-02

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

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

4. Select the VLAN (Optional) option and press Enter.
5. Enter the <<var\_ib-mgmt\_vlan\_id>> and press Enter.
6. From the Configure Management Network menu, select IP Configuration and press Enter.
7. Select the Set Static IP Address and Network Configuration option by using the space bar.
8. Enter the IP address for managing the second ESXi host: <<var\_vm\_host\_infra\_02\_ip>>.
9. Enter the subnet mask for the second ESXi host.
10. Enter the default gateway for the second ESXi host.
11. Press Enter to accept the changes to the IP configuration.
12. Select the IPv6 Configuration option and press Enter.
13. Using the spacebar, unselect Enable IPv6 (restart required) and press Enter.
14. Select the DNS Configuration option and press Enter.



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

---

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

### [Download VMware vSphere Client](#)

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 for Windows.

### Download VMware vSphere CLI

To download the VMware Remote CLI, complete the following steps:

1. Click the following link:  
<https://my.vmware.com/web/vmware/details?downloadGroup=VCLI60U2&productId=491>
2. Select your OS and Click Download.
3. Save it to destination folder.
4. Run the VMware-vSphere-CLI-xxxx.exe.
5. Click Next.
6. Accept the terms for the license and click Next.
7. Click Next on the Destination Folder screen.
8. Click install and Finish.

### Log in to VMware ESXi Hosts Using VMware vSphere Client

#### ESXi Host VM-Host-Infra-01

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

1. Open the recently downloaded VMware vSphere Client and enter the IP address of VM-Host-Infra-01 as the host you are trying to connect to: <<var\_vm\_host\_infra\_01\_ip>>.
2. Enter root for the user name.
3. Enter the root password.
4. Click Login to connect.

#### ESXi Host VM-Host-Infra-02

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

1. Open the recently downloaded VMware vSphere Client and enter the IP address of VM-Host-Infra-02 as the host you are trying to connect to: <<var\_vm\_host\_infra\_02\_ip>>.

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

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

The Cisco Custom Image for VMware vSphere 6.0 U2 comes with fnic 1.6.0.26 and enic 2.3.0.7 drivers that are older than the recommended drivers stated in the [Cisco UCS HW and SW Availability Interoperability Matrix](#) at the time of this document's publishing.

For the appropriate drivers, download and extract the following VMware VIC Drivers to the system the vSphere Web Client is being run from:

fnic Driver version 1.6.0.28  
enic Driver version 2.3.0.10

To install VMware VIC Drivers on ALL the ESXi hosts, complete the following steps:

1. From each vSphere Client, select the host in the inventory.
2. Click the Summary tab to view the environment summary.
3. From Resources > Storage, right-click datastore1 and select Browse Datastore.
4. Click the fourth button and select Upload File.
5. Navigate to the saved location for the downloaded VIC drivers and select fnic\_driver\_1.6.0.28-offline\_bundle-4179603.zip.
6. Click Open and Yes to upload the file to datastore1.
7. Click the fourth button and select Upload File.
8. Navigate to the saved location for the downloaded VIC drivers and select ESXi6.0\_enic-2.3.0.10-offline\_bundle-4303638.
9. Click Open and Yes to upload the file to datastore1.
10. Make sure the files have been uploaded to both ESXi hosts.
11. In the ESXi host vSphere Client, select the Configuration tab.
12. In the Software pane, select Security Profile.
13. To the right of Services, click Properties.
14. Select SSH and click Options at the bottom right.
15. Click Start and OK.



---

The step above does not enable SSH service and the service will not be restarted when ESXi host reboots.

---

16. Click OK to close the window.
17. Ensure SSH is started on each host.
18. From the management workstation, start an ssh session to each ESXi host. Login as root with the root password.
19. At the command prompt, run the following commands to account for each host:

```
esxcli software vib update -d /vmfs/volumes/datastore1/fnic_driver_1.6.0.28-offline_bundle-4179603.zip
```

```
esxcli software vib update -d /vmfs/volumes/datastore1/ESXi6.0_enic-2.3.0.10-offline_bundle-4303638
```

```
reboot
```

20. After each host has rebooted, log back into each host with vSphere Client.

## Map Required VMFS Datastores

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

1. From the vSphere Client, select the host VM-Host-Infra-01 in the inventory.
2. Click the Configuration tab.
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. Verifying by using the size of the datastore LUN, select the LUN configured for VM hosting and click Next.
7. Accept default VMFS setting and click Next.
8. Click Next for the disk layout.
9. Enter infra\_datastore\_1 as the datastore name.
10. Click Next to retain maximum available space.
11. Click finish.
12. Click Add Storage to open the Add Storage wizard.

13. Select the second LUN configured for swap file location and click Next.
14. Accept default VMFS setting and click Next.
15. Click Next for the disk layout.
16. Enter infra\_swap as the datastore name.
17. Click Next to retain maximum available space.
18. Click Finish.
19. The storage configuration should look similar to figure shown below.
20. Repeat these steps on all the ESXi hosts

Datastores								Refresh
Identification	Device	Drive Type	Capacity	Free	Type	Last Update	Hardware Ac	
datastore1	IBM Fibre Channel...	Non-SSD	2.50 GB	1.92 GB	VMFS5	2/22/2016 3:21:54 PM	Supported	
infra-datastore-1	IBM Fibre Channel...	Non-SSD	499.75 GB	498.80 GB	VMFS5	2/22/2016 5:58:55 PM	Supported	
infra-swap	IBM Fibre Channel...	Non-SSD	99.75 GB	98.80 GB	VMFS5	2/22/2016 3:21:54 PM	Supported	

## Configure NTP on ESXi Hosts

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

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

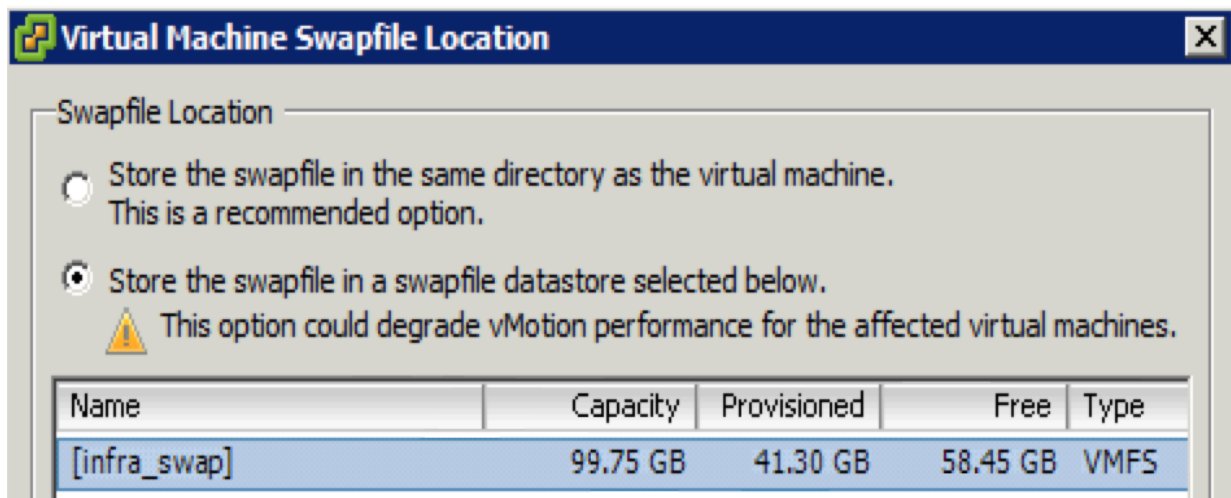
1. From each vSphere Client, select the host in the inventory.
2. Click the Configuration tab.
3. Click Time Configuration in the Software pane.
4. Click Properties at the upper right side of the window.
5. At the bottom of the Time Configuration dialog box, click NTP Client Enabled.
6. At the bottom of the Time Configuration dialog box, click Options.
7. In the NTP Daemon Options (ntpd) dialog box, complete the following steps:
8. Click General in the left pane, select Start, and stop with host.
9. Click NTP Settings in the left pane and click Add.

10. In the Add NTP Server dialog box, enter <<var\_global\_ntp\_server\_ip>> as the IP address of the NTP server and click OK.
11. In the NTP Daemon Options dialog box, select the Restart NTP Service to Apply Changes checkbox and click OK.
12. Click OK.
13. In the Time Configuration dialog box, verify that the clock is now set to approximately the correct time.

## Move VM Swap File Location

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

1. From the vSphere Client, select the host in the inventory.
2. Click the Configuration tab.
3. Click Virtual Machine Swapfile Location in the Software pane.
4. Click Edit at the upper-right side of the window.
5. **Select “Store the swapfile in a swapfile datastore selected below.”**
6. Select the infra\_swap datastore to house the swap files.
7. Click OK to finalize the swap file location.



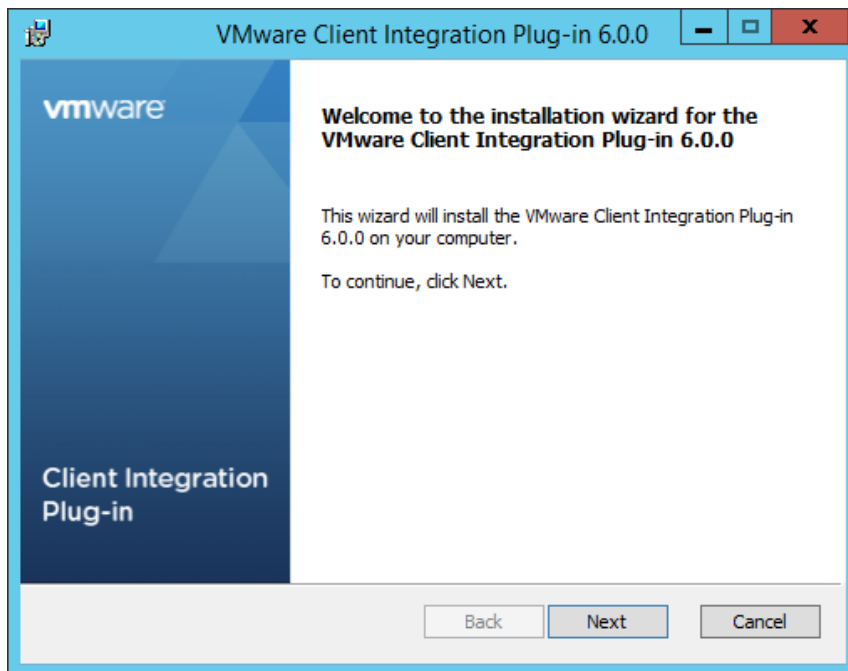
## VersaStack VMware vCenter 6.0U2

The procedures in the following subsections provide detailed instructions to install VMware vCenter 6.0U2 Server Appliance in a VersaStack environment. After the procedures are completed, a VMware vCenter Server will be configured.

### Install the Client Integration Plug-In

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

1. Download the .iso installer for the version 6.0U2 vCenter Server Appliance and Client Integration Plug-in.
2. Mount the ISO image on the management station.
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.

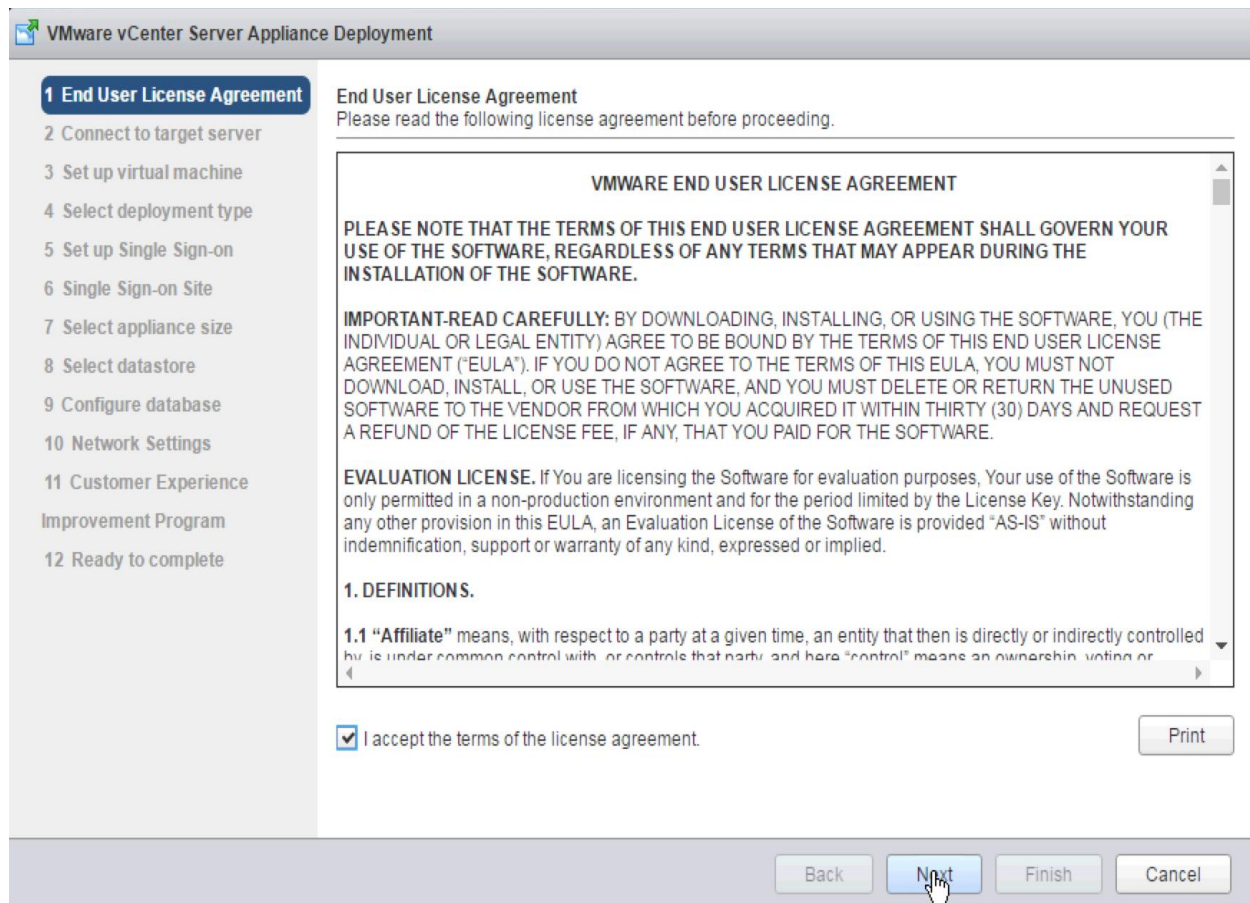


4. On the Welcome page, click Next.
5. Read and accept the terms in the End-User License Agreement and click Next.
6. Click Next.
7. Click Install.

## Building the VMware vCenter Server Appliance

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

1. In the iso top-level 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.

The screenshot shows the 'Connect to target server' step of the VMware vCenter Server Appliance Deployment wizard. The left sidebar lists 12 steps, with step 2, 'Connect to target server', highlighted in blue. The main area contains the following fields and instructions:

- Connect to target server**  
Specify the ESXi host or vCenter Server on which to deploy the vCenter Server Appliance.
- FQDN or IP Address:**
- User name:**  ⓘ
- Password:**

⚠ Before proceeding, if the target is an ESXi host:

- Make sure the ESXi host is not in lock down mode or maintenance mode.
- When deploying to a vSphere Distributed Switch (VDS), the appliance must be deployed to an ephemeral portgroup. After deployment, it can be moved to a static or dynamic portgroup.

At the bottom right, there are four buttons: Back, Next, Finish, and Cancel.

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.



The screenshot shows the VMware vCenter Server Appliance Deployment wizard. The title bar reads "VMware vCenter Server Appliance Deployment". On the left, a navigation pane lists 12 steps: 1 End User License Agreement, 2 Connect to target server, 3 Set up virtual machine (highlighted), 4 Select deployment type, 5 Set up Single Sign-on, 6 Single Sign-on Site, 7 Select appliance size, 8 Select datastore, 9 Configure database, 10 Network Settings, 11 Customer Experience Improvement Program, and 12 Ready to complete. The main area is titled "Set up virtual machine" with the instruction "Specify virtual machine settings for the vCenter Server Appliance to be deployed." Below this, there are four input fields: "Appliance name:" with the value "vCenter" and an information icon; "OS user name:" with the value "root"; "OS password:" with a masked password "....." and an information icon; and "Confirm OS password:" with a masked password ".....". At the bottom right, there are four buttons: "Back", "Next", "Finish", and "Cancel".

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

**VMware vCenter Server Appliance Deployment**

1 End User License Agreement  
 2 Connect to target server  
 3 Set up virtual machine  
 4 **Select deployment type**  
 5 Set up Single Sign-on  
 6 Single Sign-on Site  
 7 Select appliance size  
 8 Select datastore  
 9 Configure database  
 10 Network Settings  
 11 Ready to complete

**Select deployment type**  
Select the services to deploy onto this appliance.

vCenter Server 6.0 requires a Platform Services Controller, which contains shared services such as Single Sign-On, Licensing, and Certificate Management. An embedded Platform Services Controller is deployed on the same Appliance VM as vCenter Server. An external Platform Services Controller is deployed in a separate Appliance VM. For smaller installations, consider vCenter Server with an embedded Platform Services Controller. For larger installations with multiple vCenter Servers, consider one or more external Platform Services Controllers. Refer to the vCenter Server documentation for more information.

Note: Once you install vCenter Server, you can only change from an embedded to an external Platform Services Controller with a fresh install.

**Embedded Platform Services Controller**

Install vCenter Server with an Embedded Platform Services Controller

**External Platform Services Controller**

Install Platform Services Controller  
 Install vCenter Server (Requires External Platform Services Controller)

Back Next Finish Cancel

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.

**VMware vCenter Server Appliance Deployment**

- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- ✓ 4 Select deployment type
- 5 Set up Single Sign-on**
- 6 Select appliance size
- 7 Select datastore
- 8 Configure database
- 9 Network Settings
- 10 Customer Experience Improvement Program
- 11 Ready to complete

**Set up Single Sign-on (SSO)**  
Create or join a SSO domain. An SSO configuration cannot be changed after deployment.

Create a new SSO domain  
 Join an SSO domain in an existing vCenter 6.0 platform services controller

vCenter SSO User name: administrator

vCenter SSO Password:  ⓘ

Confirm password:

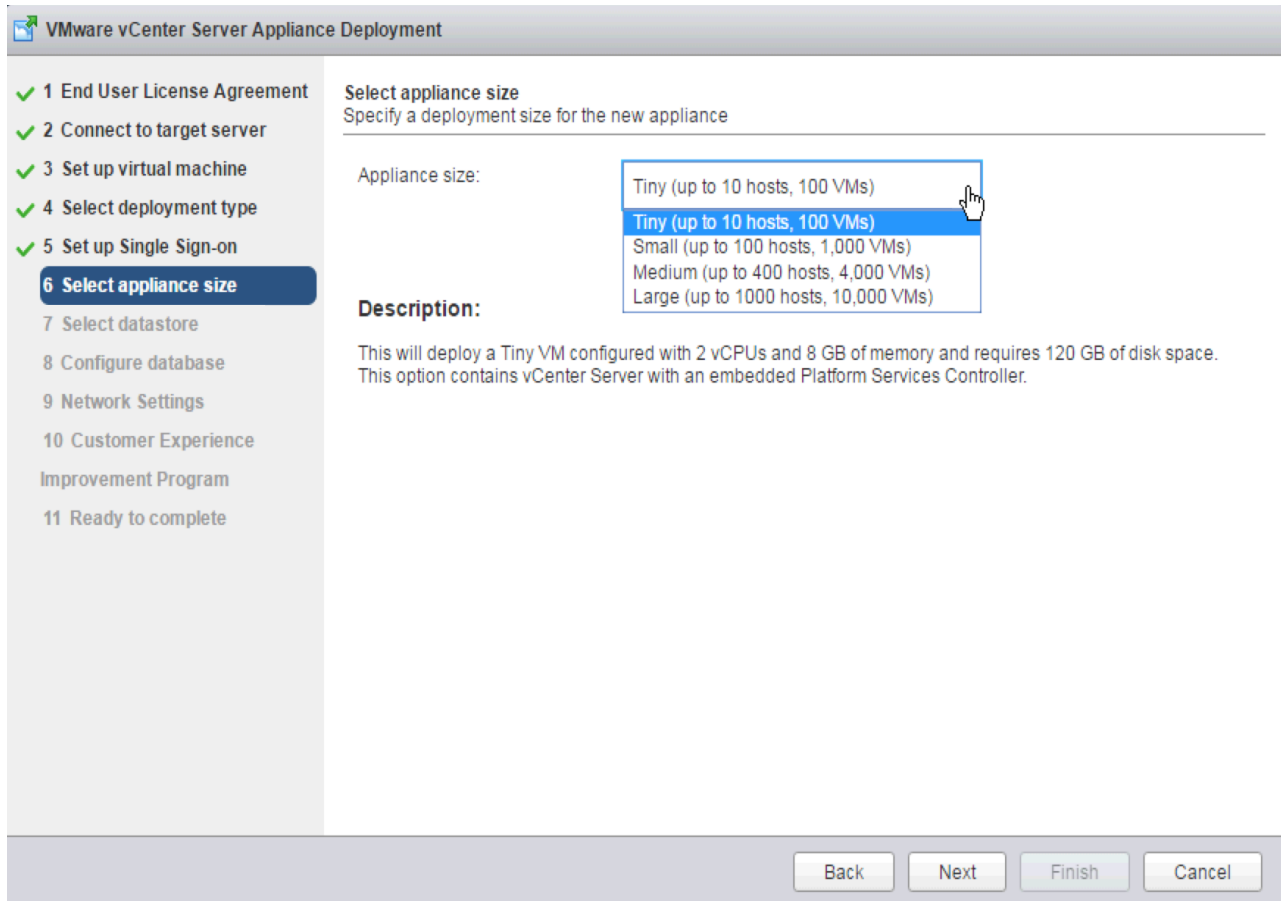
SSO Domain name:  ⓘ

SSO Site name:  ⓘ

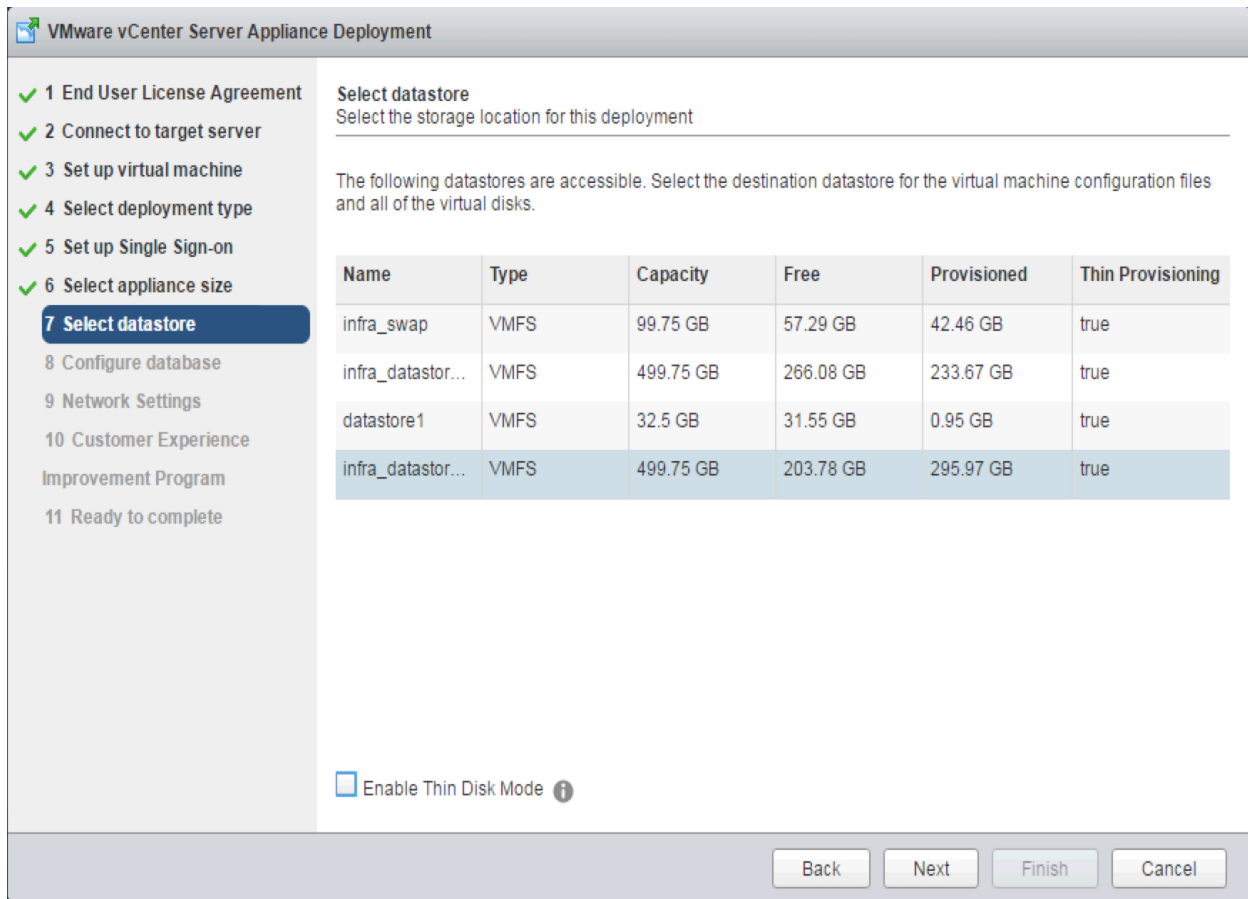
⚠ Before proceeding, make sure that the vCenter Single Sign-On domain name used is different than your Active Directory domain name.

Back Next Finish Cancel

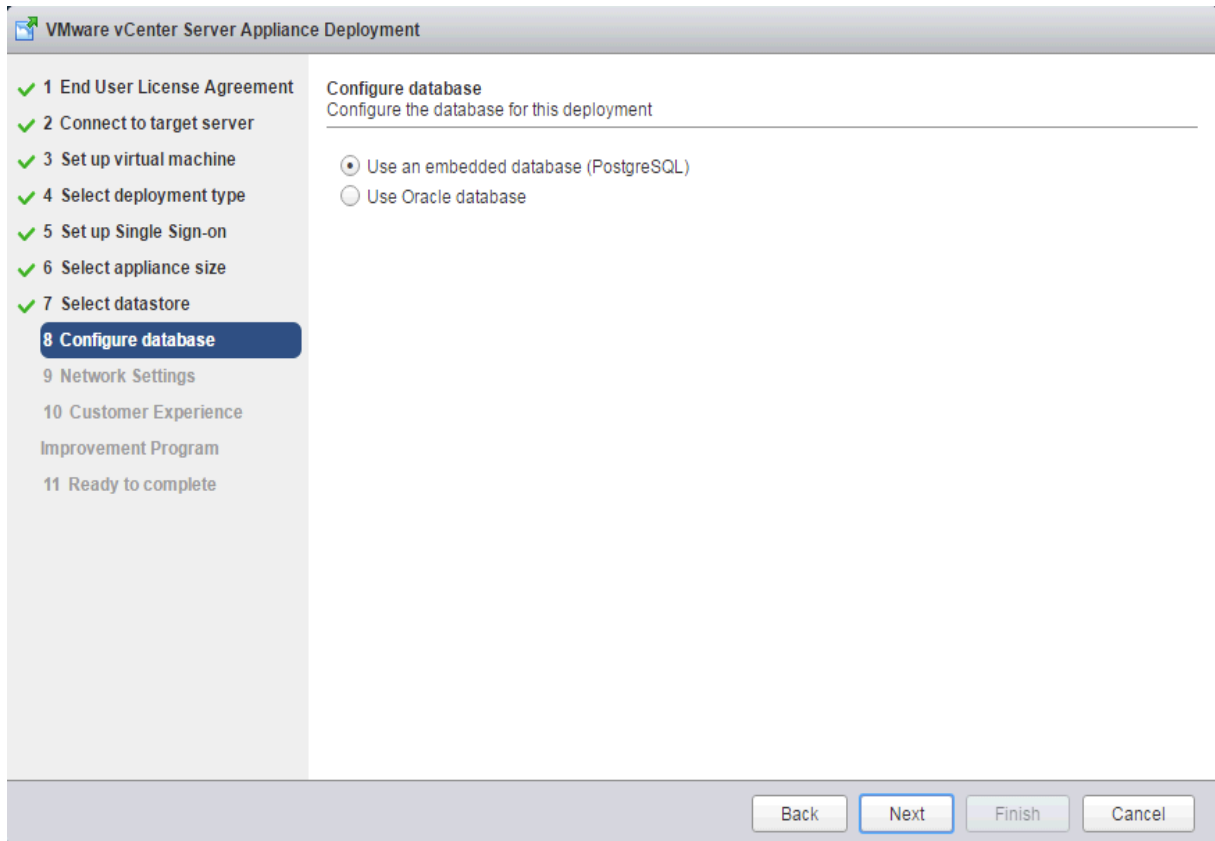
11. In the Select appliance size screen, select the size that matches your deployment, and click Next.



12. In the Select datastore screen, select the location for the VM configuration and virtual disks should be stored (infra\_datastore\_1), and click Next.



13. Select embedded database in the "Configure database" page. Click Next.



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

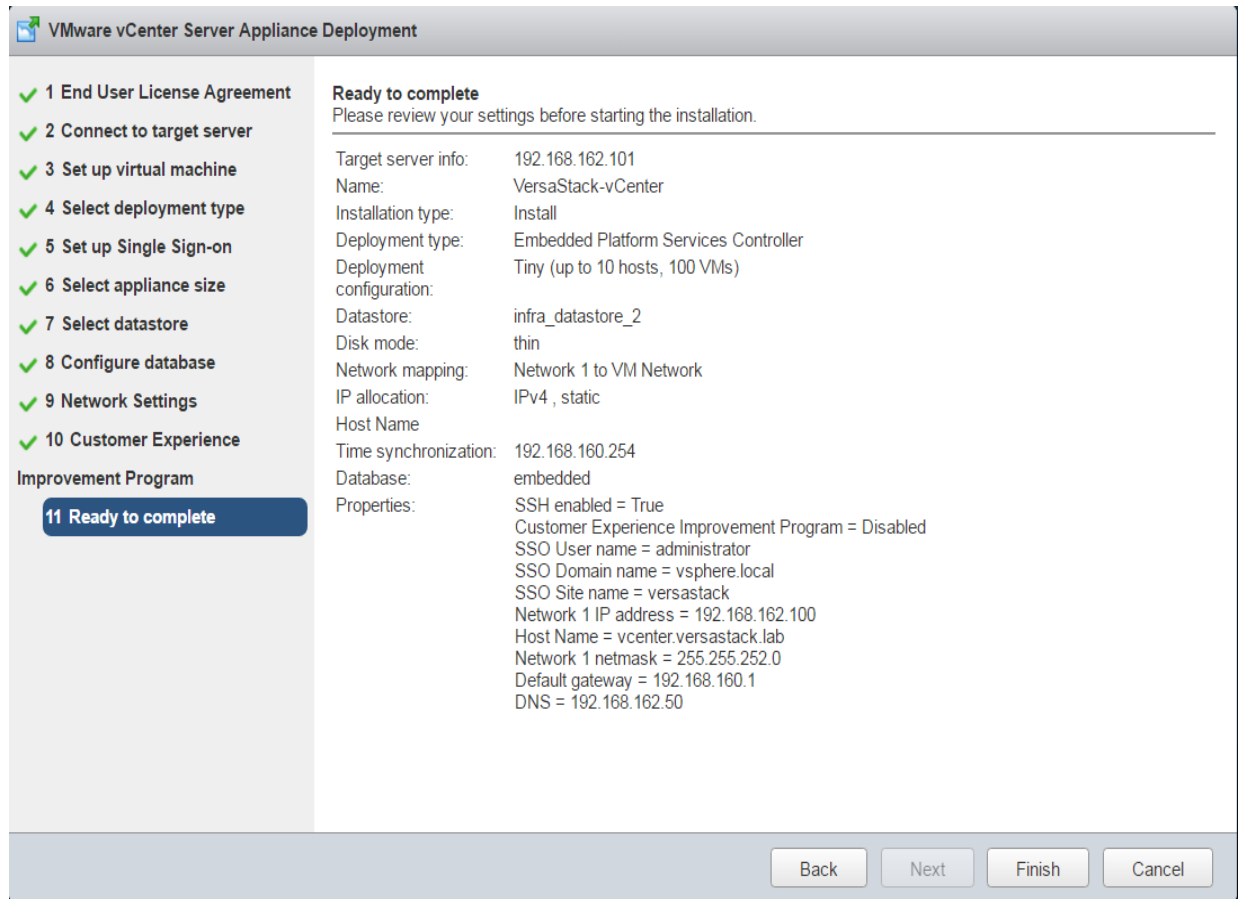
- a. Choose a Network: IB-MGMT
- b. IP address family: IPV4
- c. Network type: static
- d. Network address: <<var\_vcenter\_ip>>
- e. System name: <<var\_vcenter\_fqdn>>
- f. Subnet mask: <<var\_vcenter\_subnet\_mask>>
- g. Network gateway: <<var\_vcenter\_gateway>>
- h. Network DNS Servers: <<var\_dns\_server>>
- i. Configure time sync: Use NTP servers

The screenshot shows the 'VMware vCenter Server Appliance Deployment' wizard. On the left, a progress list shows steps 1 through 11. Step 9, 'Network Settings', is currently selected and highlighted in blue. The main area is titled 'Network Settings' and contains the following fields and options:

- Choose a network:** A dropdown menu with 'VM Network' selected.
- IP address family:** A dropdown menu with 'IPv4' selected.
- Network type:** A dropdown menu with 'static' selected.
- Network address:** A text input field containing '192.168.162.100'.
- System name [FQDN or IP address]:** A text input field containing 'vcenter.versastack.lab'.
- Subnet mask:** A text input field containing '255.255.252.0'.
- Network gateway:** A text input field containing '192.168.160.1'.
- Network DNS Servers (separated by commas):** A text input field containing '192.168.162.50'.
- Configure time sync:** Two radio button options: 'Synchronize appliance time with ESXi host' (unselected) and 'Use NTP servers (Separated by commas)' (selected).

At the bottom of the wizard, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

15. Make appropriate choice for Joining VMware customer experience improvement program. Click Next.
16. In the Ready to complete screen, review the deployment settings for the vCenter Server Appliance, and click Finish to complete the deployment process.



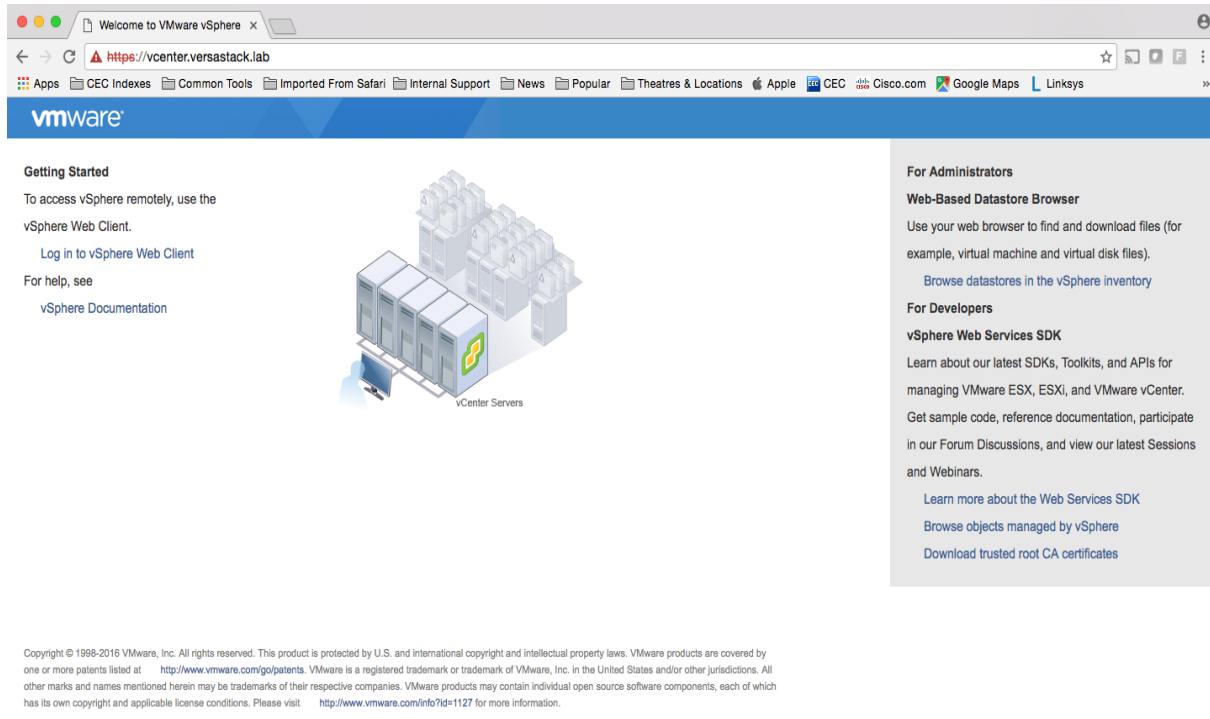
17. The vCenter appliance installation will take few minutes to complete.

## Set Up vCenter Server

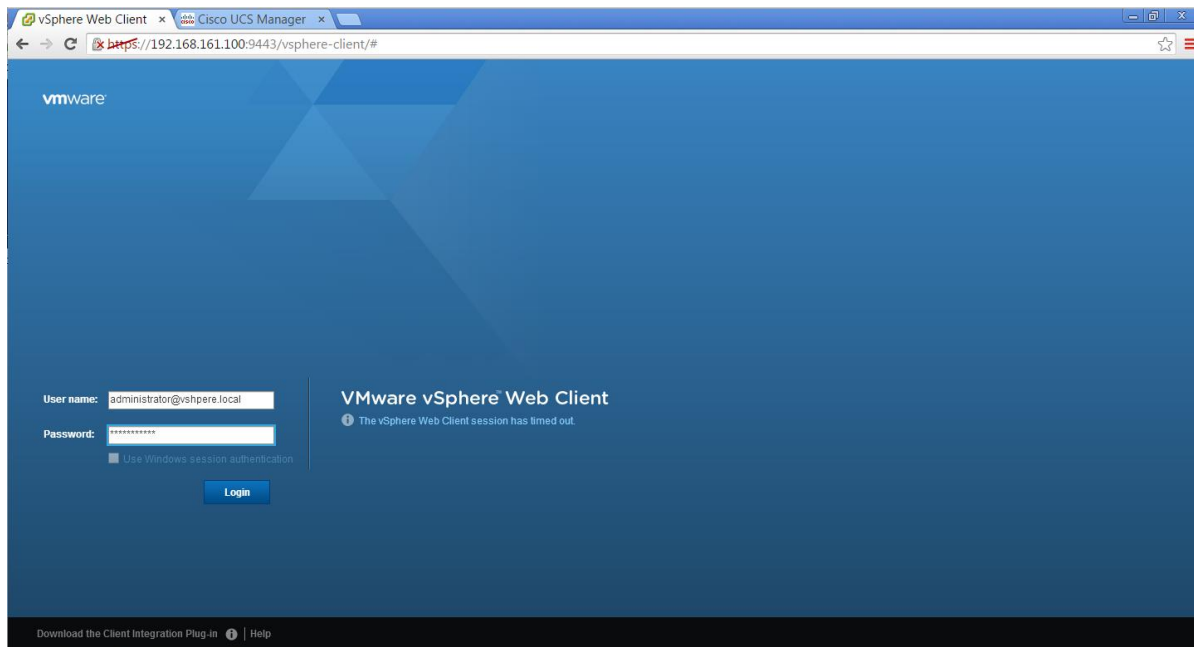
To set up the VMware environment, log into the vCenter Server web client, and complete the following steps:

1. Using a web browser, navigate to [https://<<var\\_vcenter\\_ip/FQDN>>](https://<<var_vcenter_ip/FQDN>>)
2. Click the link labeled Log in to vSphere Web Client.





3. If prompted, run the VMWare Remote Console Plug-in.
4. Log in as root, with the root password entered above in the vCenter installation.

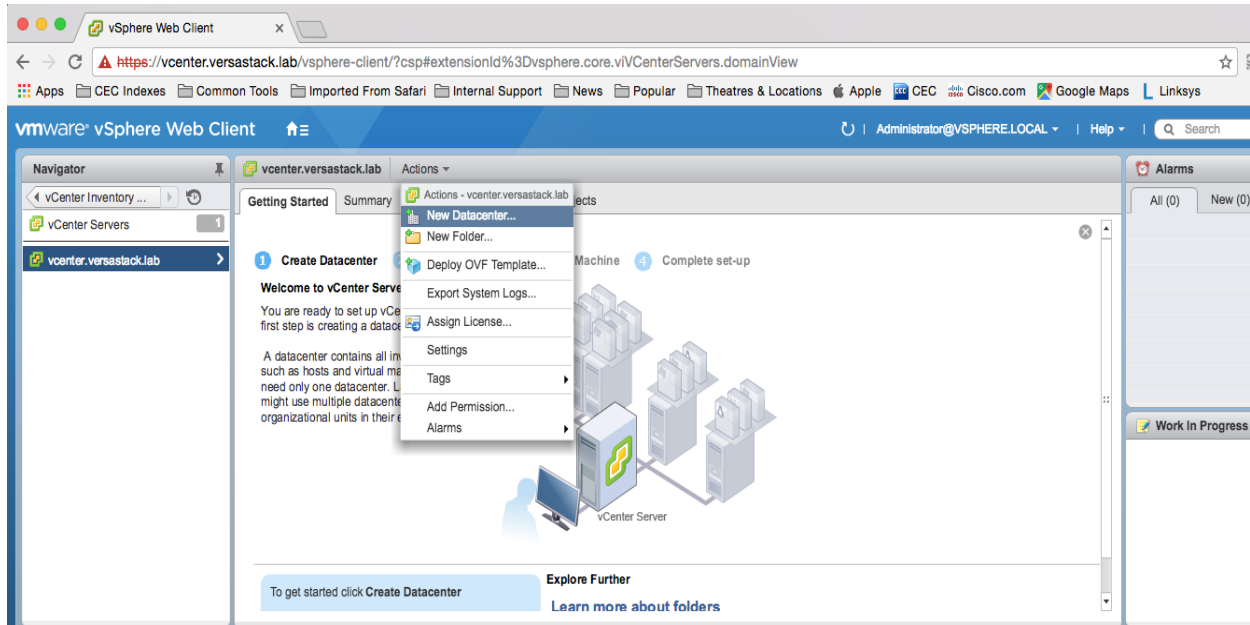


5. Click Login.

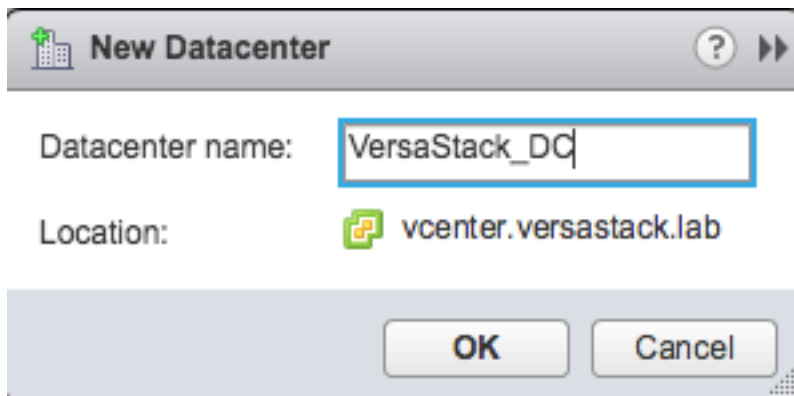
## Set Up vCenter Server with a Datacenter, Cluster, DRS and HA

To setup the vCenter Server, complete the following steps:

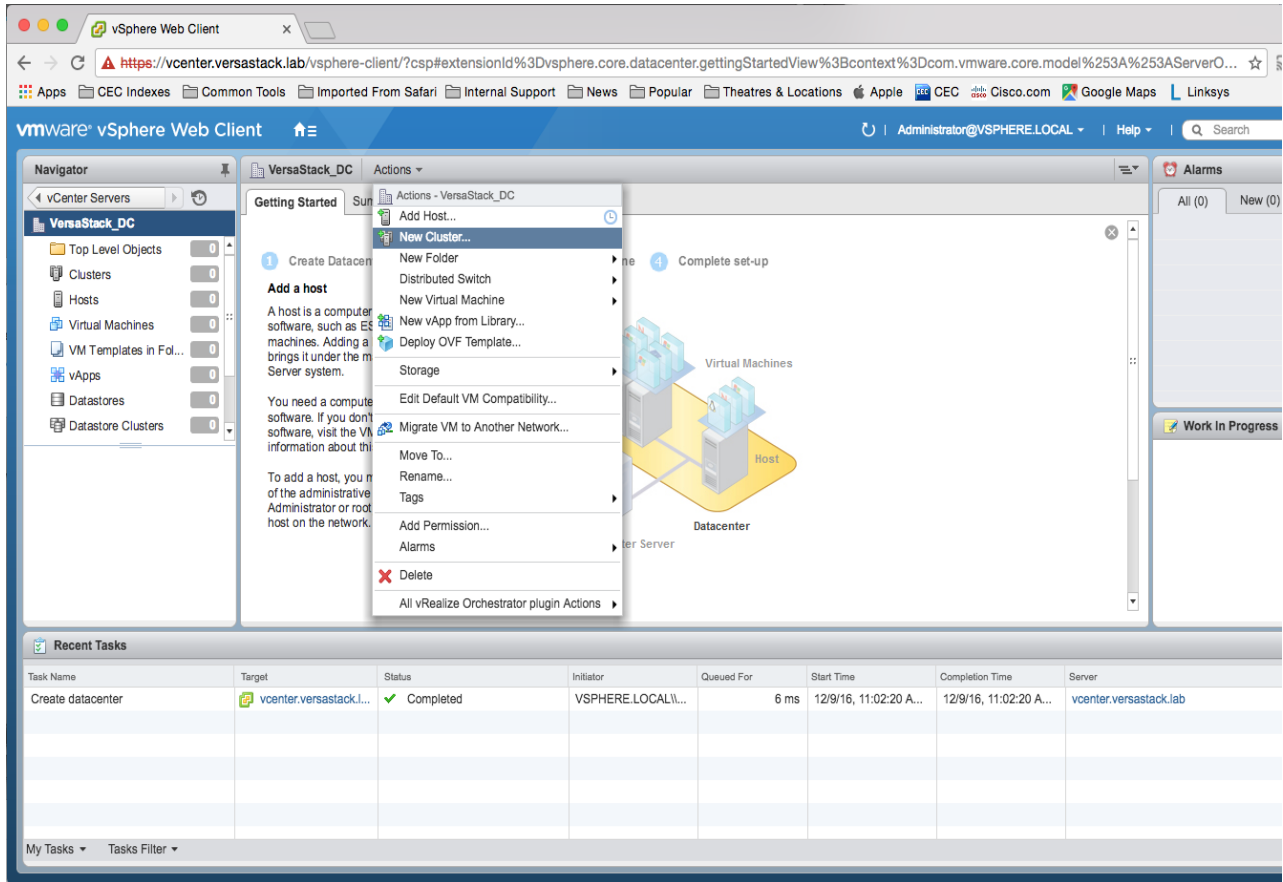
1. In the vSphere Web Client, navigate to the vCenter Inventory Lists > Resources > vCenter Servers.
2. Select the vCenter instance (vcenter.versastack.lab).
3. Go to Actions in the toolbar and select New Datacenter from the drop-down menu.



4. Rename the datacenter and click OK.



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



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

New Cluster	
Name	VersaStack_MGMT
Location	VersaStack_DC
DRS	<input checked="" type="checkbox"/> Turn ON
Automation Level	Fully automated
Migration Threshold	Conservative ——— Aggressive
vSphere HA	<input checked="" type="checkbox"/> Turn ON
Host Monitoring	<input checked="" type="checkbox"/> Enable host monitoring
Admission Control	
Admission Control Status	Admission control will prevent powering on VMs that violate availability constraints <input checked="" type="checkbox"/> Enable admission control
Policy	Specify the type of the policy that admission control should enforce. <input checked="" type="radio"/> Host failures cluster tolerates: 1 <input type="radio"/> Percentage of cluster resources reserved as failover spare capacity: Reserved failover CPU capacity: 25 % CPU Reserved failover Memory capacity: 25 % Memory
VM Monitoring	
VM Monitoring Status	Disabled Overrides for individual VMs can be set from the VM Overrides page from Manage Settings area.
Monitoring Sensitivity	Low ——— High
EVC	Disable
Virtual SAN	<input type="checkbox"/> Turn ON

OK Cancel

7. Click OK.

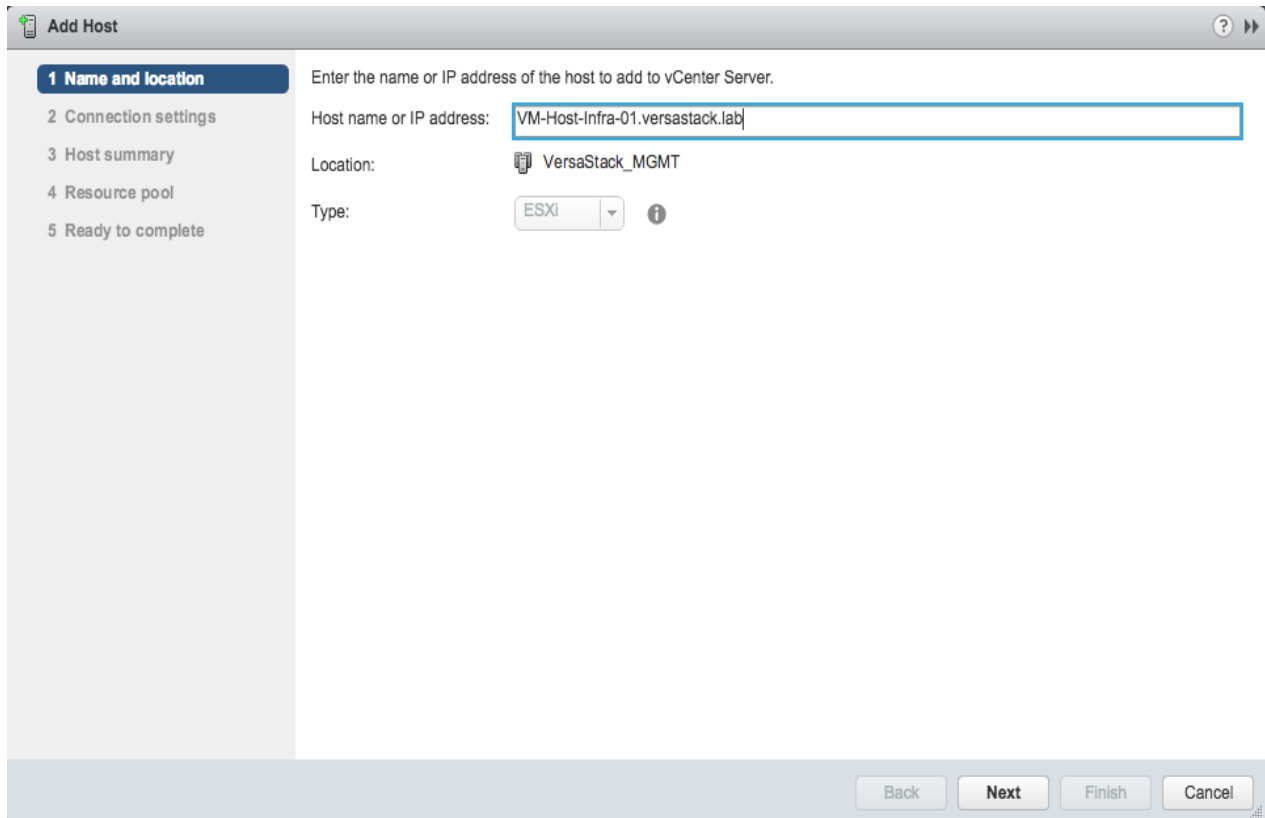


**Important:** If mixing Cisco UCS B or C-Series M2, M3 or M4 servers within a vCenter cluster, it is necessary to enable VMware Enhanced vMotion Compatibility (EVC) mode. For more information about setting up EVC mode, refer to [Enhanced vMotion Compatibility \(EVC\) Processor Support](#).

## Add Hosts 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.

**Add Host**

1 Name and location

**2 Connection settings**

3 Host summary

4 Resource pool

5 Ready to complete

Enter the administrative account information for the host. The vSphere Web Client will use this information to connect to the host and establish a permanent account for its operations.

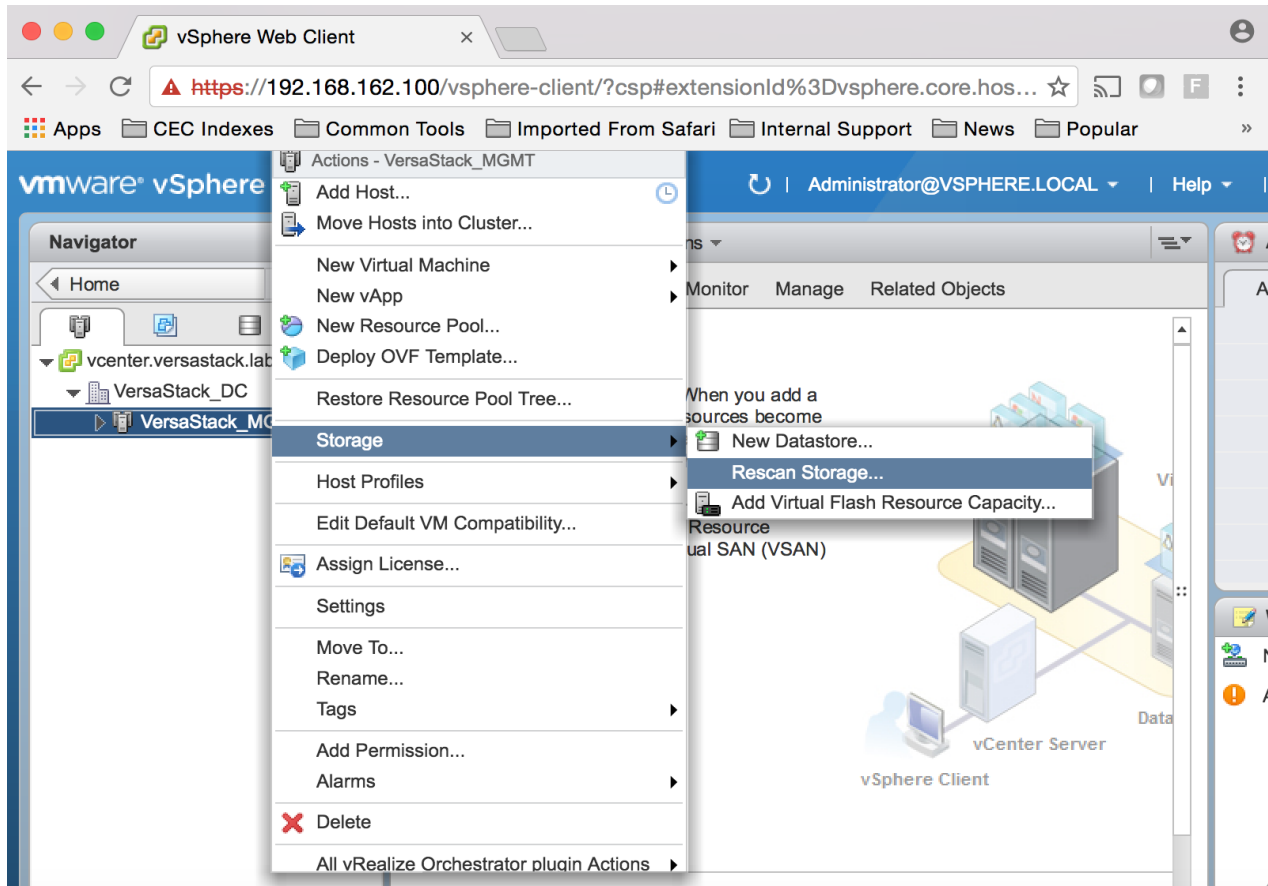
User name:

Password:

Back Next Finish Cancel

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

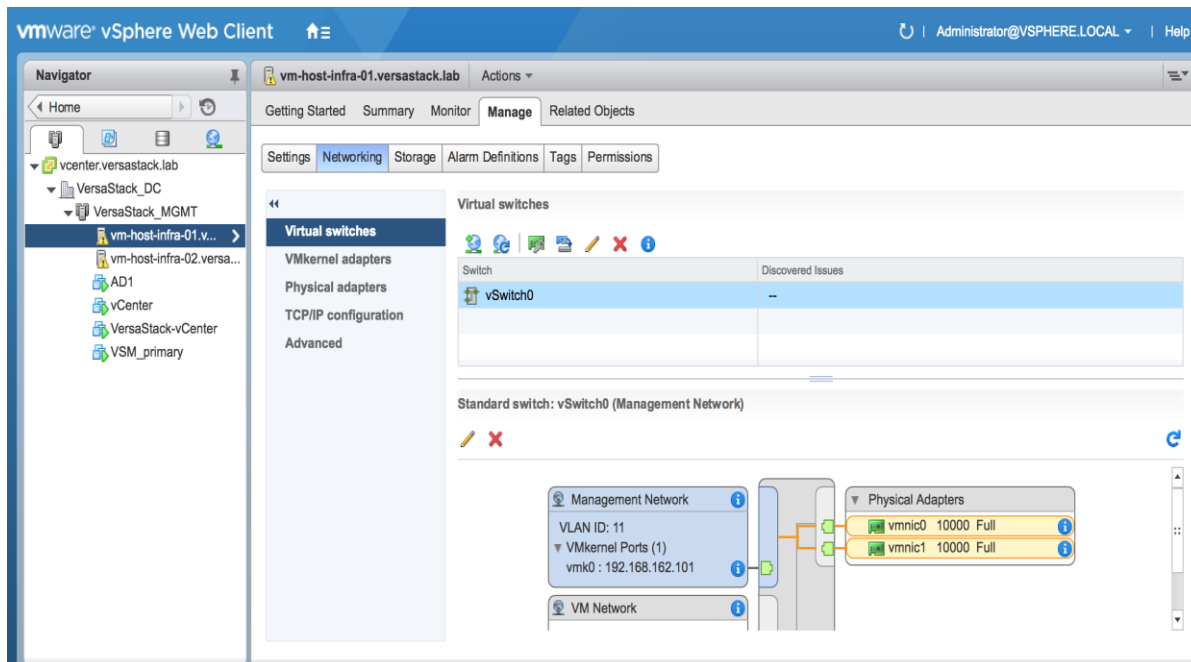
12. In vSphere in the left pane right-click the cluster VersaStack\_MGMT, and click Rescan Storage.



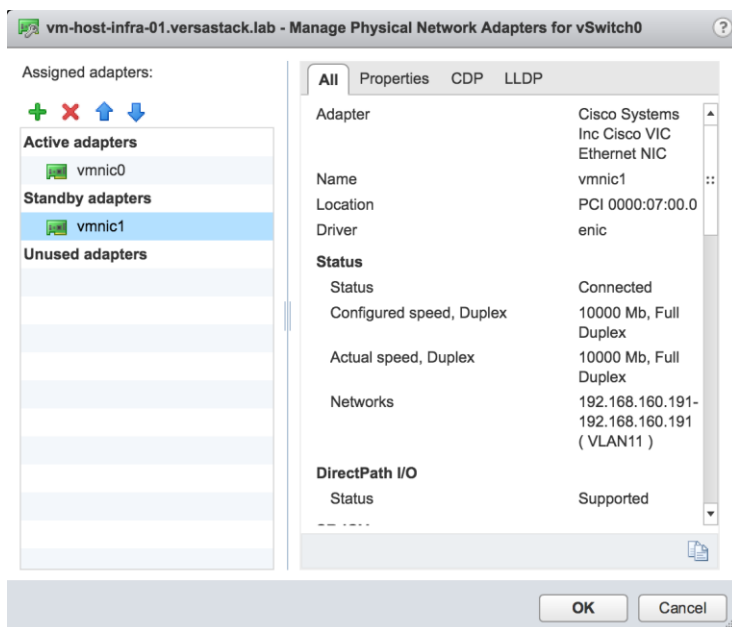
## Configure ESXi Networking

To configure the ESXi networking, complete the following steps:

1. Select the ESXi host installed VM-Host-Infra-01 from within the newly create cluster, click the Manage tab within that host and Networking within the Manage tab.



2. With vSwitch0 selected, click the third icon (a green adapter card with a wrench) over from the left under Virtual switches to produce a Manage Physical Network Adapters for vSwitch0 pop-up window.

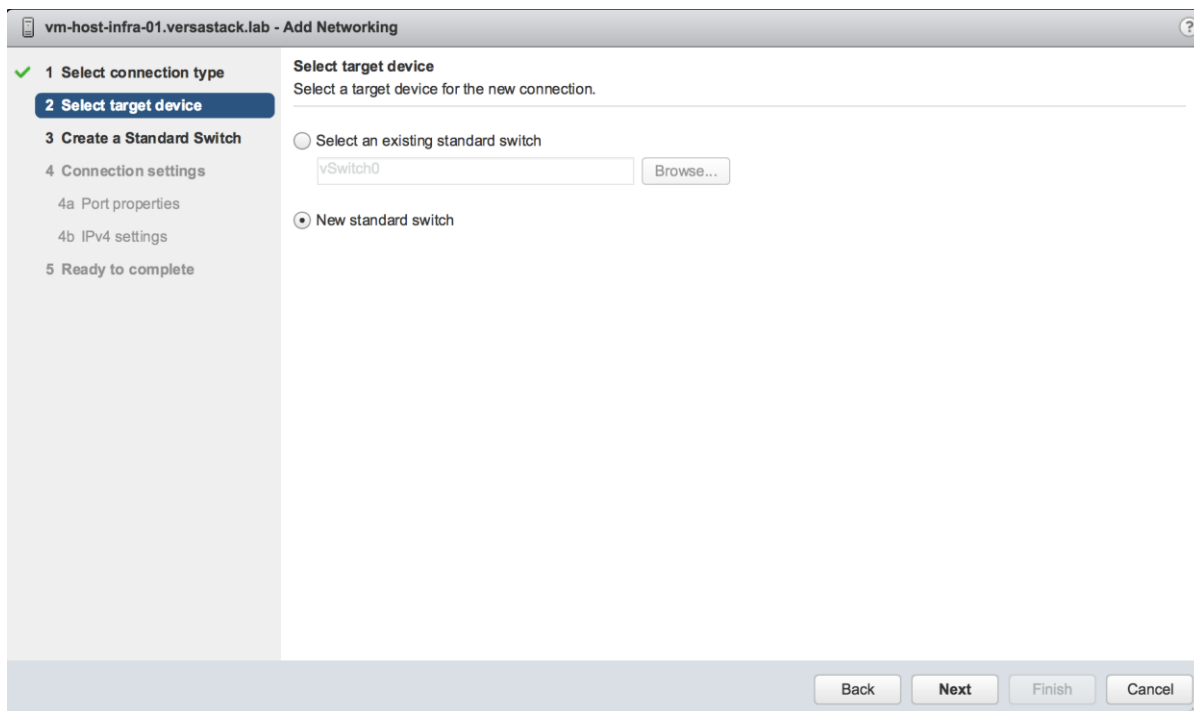


3. Select vmnic1 within the Standby adapters and click on the blue up arrow under Assigned adapters to move vmnic1 from the Standby adapters to the Active adapters.
4. Click OK to commit the change.
5. Still within the Manage tab under Networking -> Virtual switches, click the far left icon under Virtual switches to Add host networking.

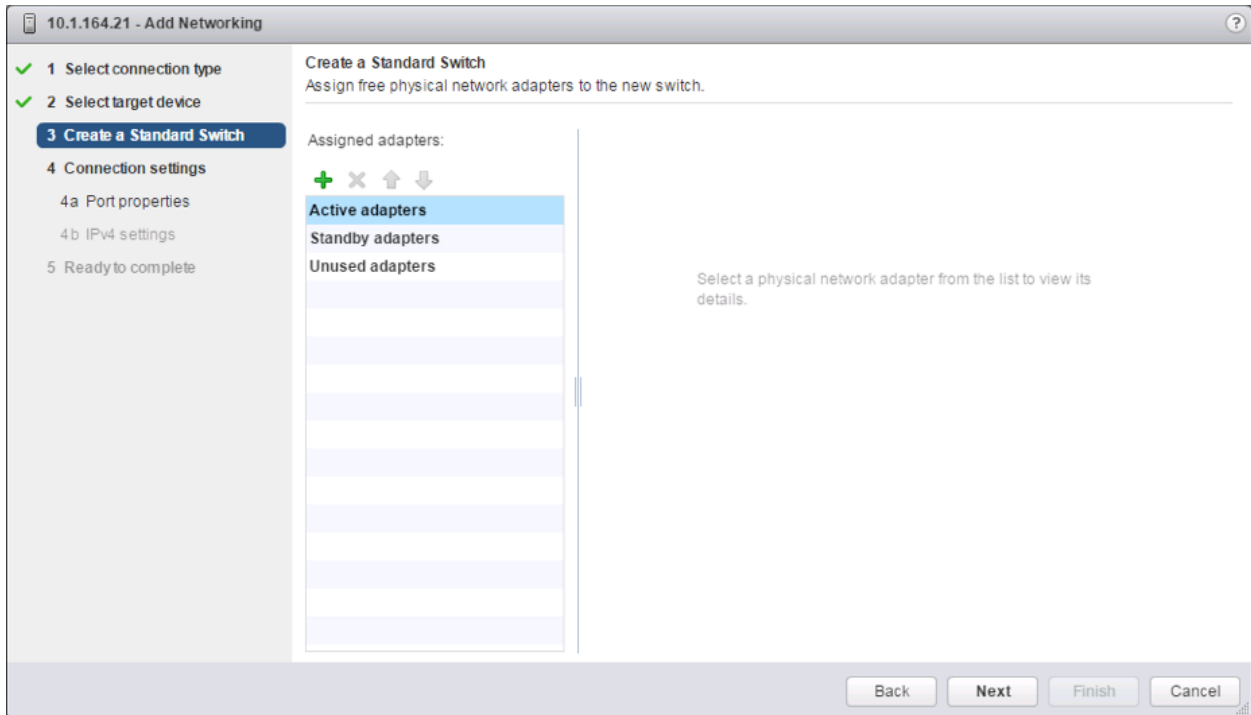




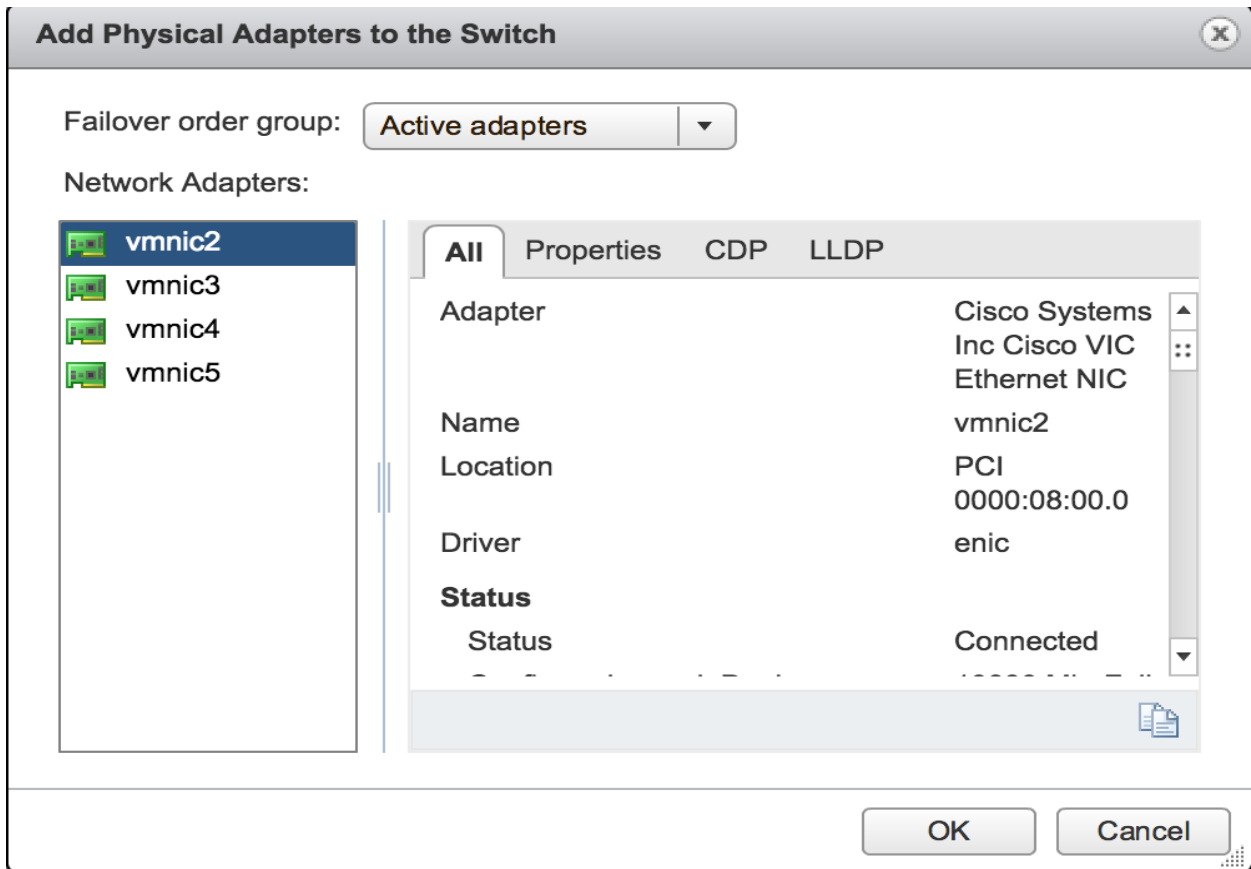
6. Leave VMkernel Network Adapter selected within Select connection type of the Add Networking pop-up window that is generated, and click Next.



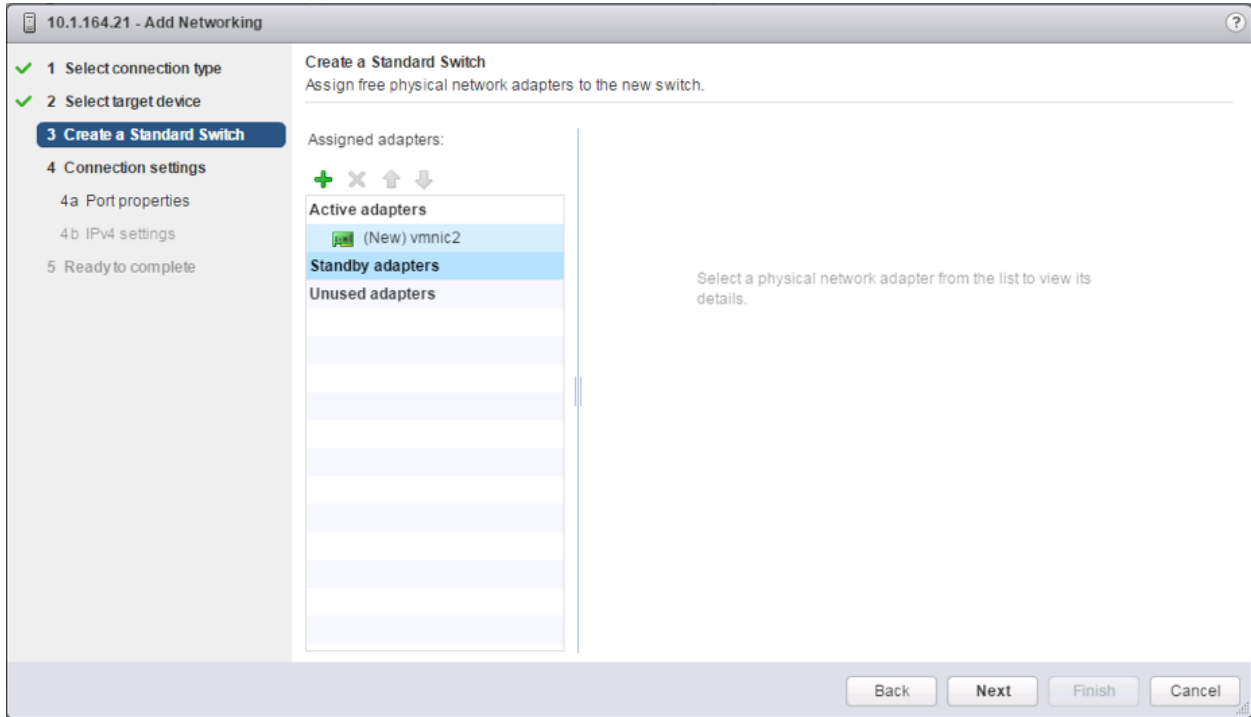
7. Within Select target device, click the New standard switch option, and click Next.



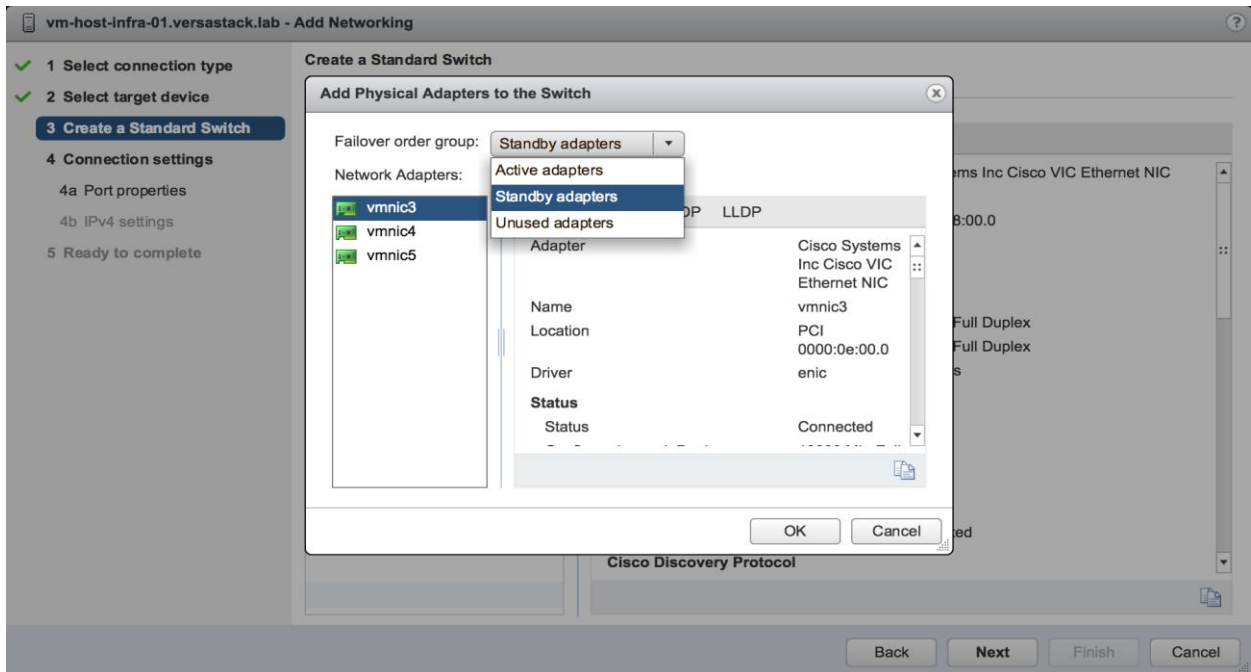
8. Within the Create Standard Switch dialogue press the green + icon below Assigned adapters.



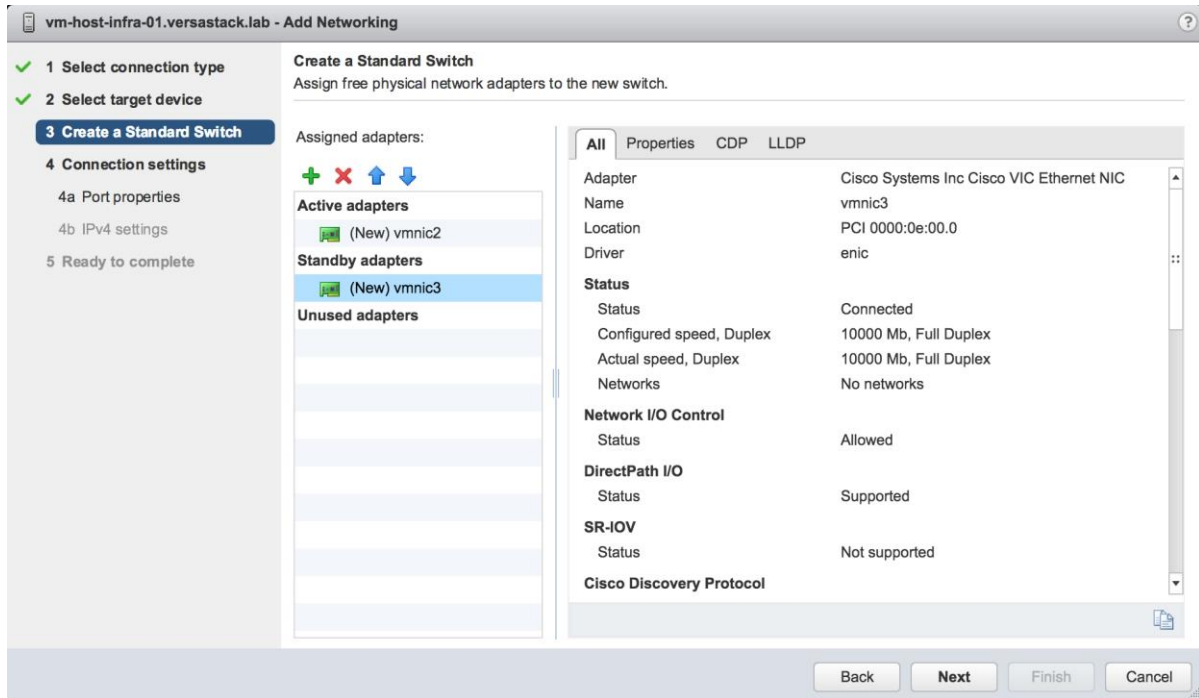
9. Select vmnic2 within the Network Adapters, and click OK.



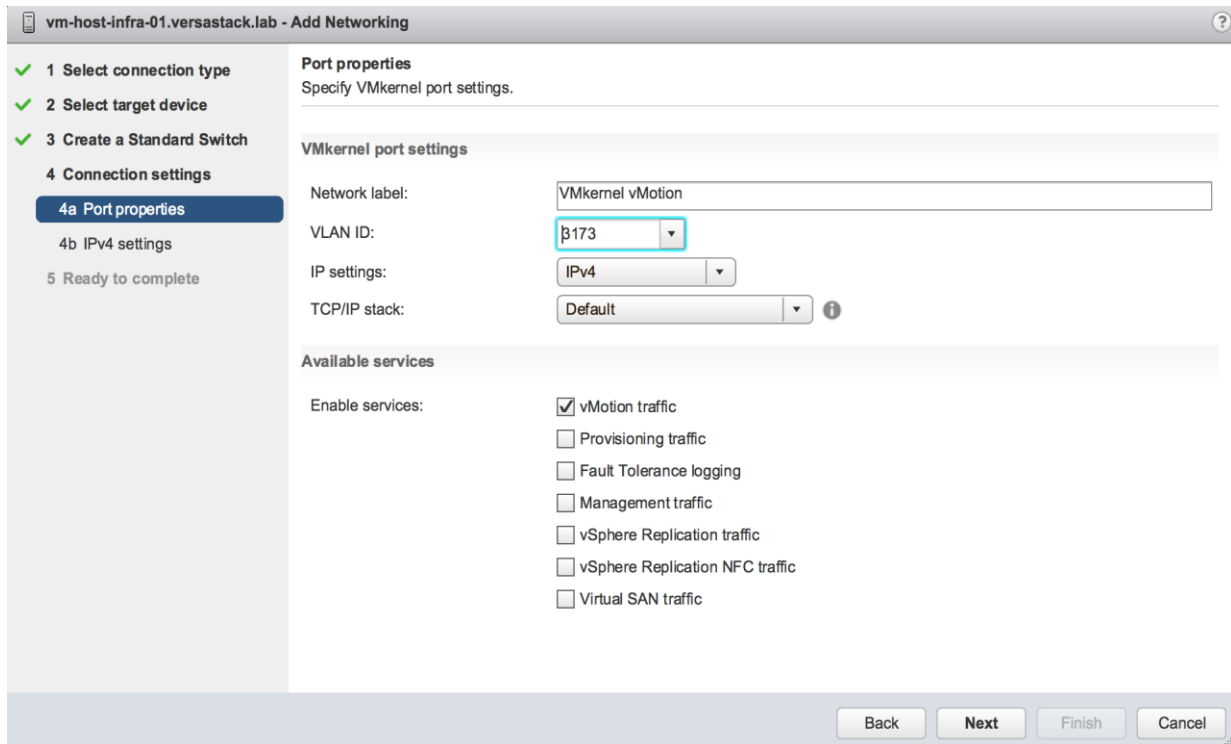
10. While still in the Create a Standard Switch dialogue, click the green + icon one more time.



11. Select vmnic3, and from the Failover order group pulldown, select Standby adapters. Click OK.



12. Click Next.



13. Within Port properties under Connection settings, set the Network label to be VMkernel vMotion, set the VLAN ID to the value for <<var\_vmotion\_vlan\_id>>, and checkmark vMotion traffic under Available services. Click Next.

vm-host-infra-01.versastack.lab - Add Networking

- ✓ 1 Select connection type
- ✓ 2 Select target device
- ✓ 3 Create a Standard Switch
- 4 Connection settings
  - ✓ 4a Port properties
  - 4b IPv4 settings
- 5 Ready to complete

**IPv4 settings**  
Specify VMkernel IPv4 settings.

Obtain IPv4 settings automatically  
 Use static IPv4 settings

IPv4 address: 172 . 17 . 73 . 11  
 Subnet mask: 255 . 255 . 255 . 0  
 Default gateway for IPv4: 192.168.160.1  
 DNS server addresses: 192.168.162.50

Back Next Finish Cancel

14. Enter `<<var_vm_host_infra_vmotion_01_ip>>` in the field for IPv4 address, and `<<var_vmotion_subnet_mask>>` for the Subnet mask. Click Next.

vm-host-infra-01.versastack.lab - Add Networking

- ✓ 1 Select connection type
- ✓ 2 Select target device
- ✓ 3 Create a Standard Switch
- 4 Connection settings
  - ✓ 4a Port properties
  - ✓ 4b IPv4 settings
  - 5 Ready to complete

**Ready to complete**  
Review your settings selections before finishing the wizard.

New standard switch: vSwitch1  
 Assigned adapters: vmnic3, vmnic2  
 New port group: VMkernel vMotion  
 VLAN ID: 3173  
 TCP/IP stack: Default  
 vMotion traffic: Enabled  
 Provisioning traffic: Disabled  
 Fault Tolerance logging: Disabled  
 Management traffic: Disabled  
 vSphere Replication traffic: Disabled  
 vSphere Replication NFC traffic: Disabled  
 Virtual SAN traffic: Disabled

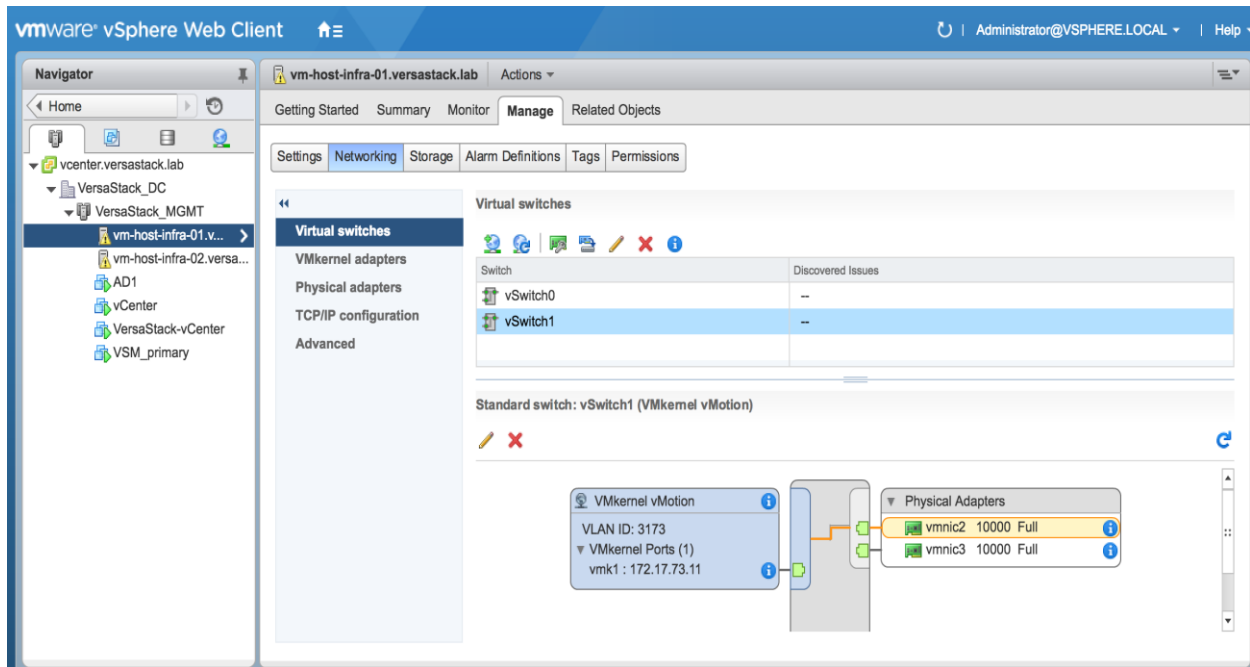
**IPv4 settings**

IPv4 address: 172.17.73.11 (static)  
 Subnet mask: 255.255.255.0

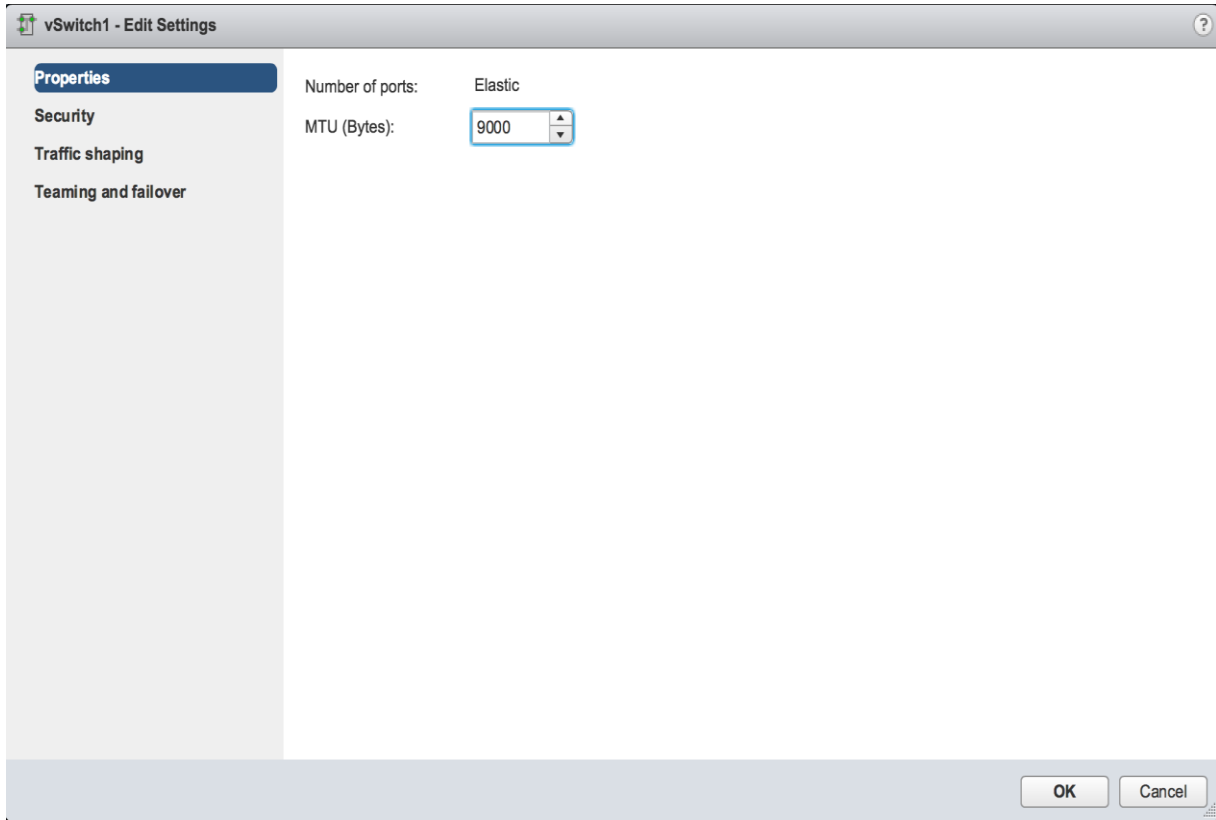
Back Next Finish Cancel

15. Confirm the values shown on the Ready to complete summary page, and click Finish to create the vSwitch and VMkernel for vMotion.

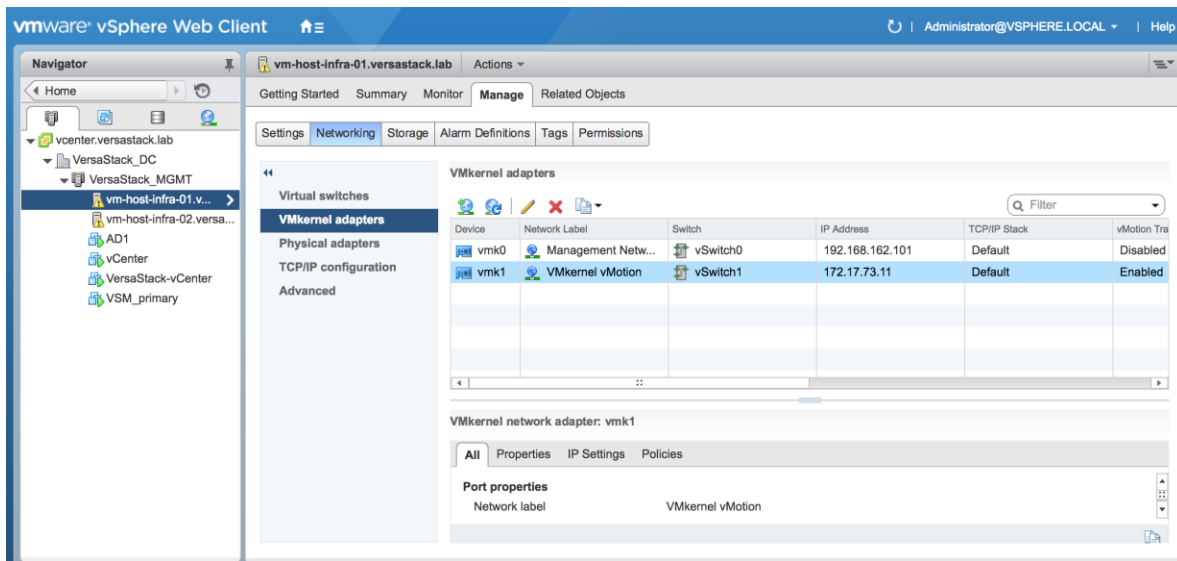
16. Still within the Manage tab for the host, under Networking -> Virtual switches, make sure that vSwitch1 is selected, and click on the pencil icon under the Virtual Switches title to edit the vSwitch properties to adjust the MTU for the vMotion vSwitch.



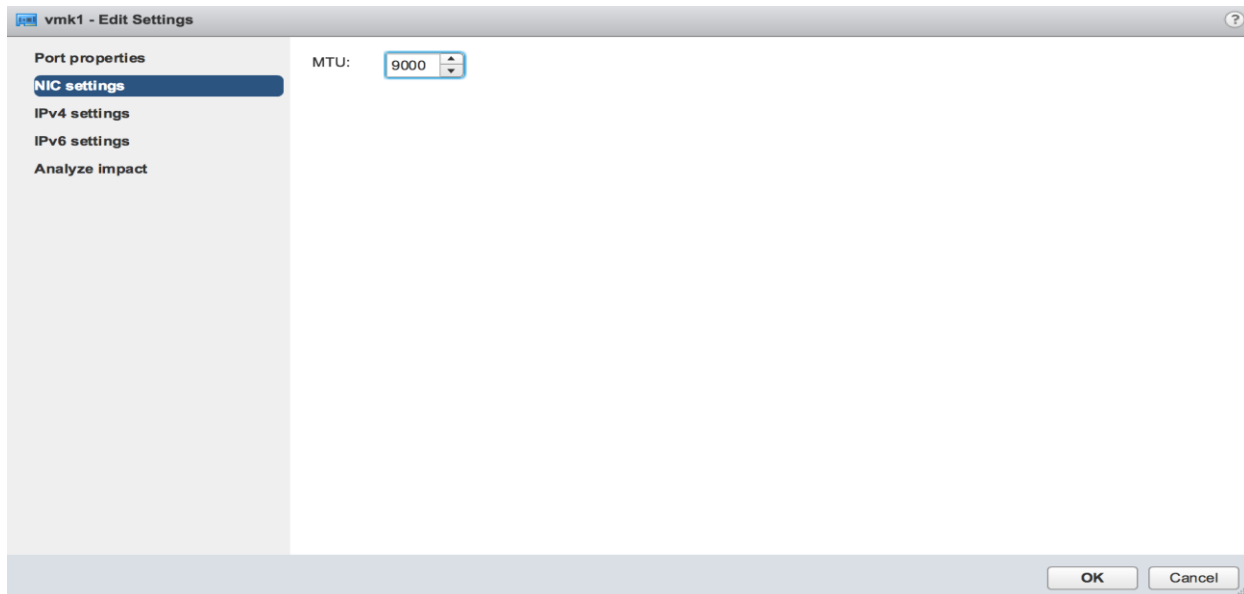
17. Enter 9000 in the Properties dialogue for the vSwitch1 - Edit Settings pop-up that appears. Click OK to apply the change.



18. Click the VMkernel adapters within Manage -> Networking for the host, and with the VMkernel for vMotion (vmk1) selected, click the pencil icon to edit the VMkernel settings.



19. Click the NIC settings in the vmk1 - Edit Settings pop-up window that appears, and enter 9000 for the MTU value to use for the VMkernel. Click OK to apply the change.

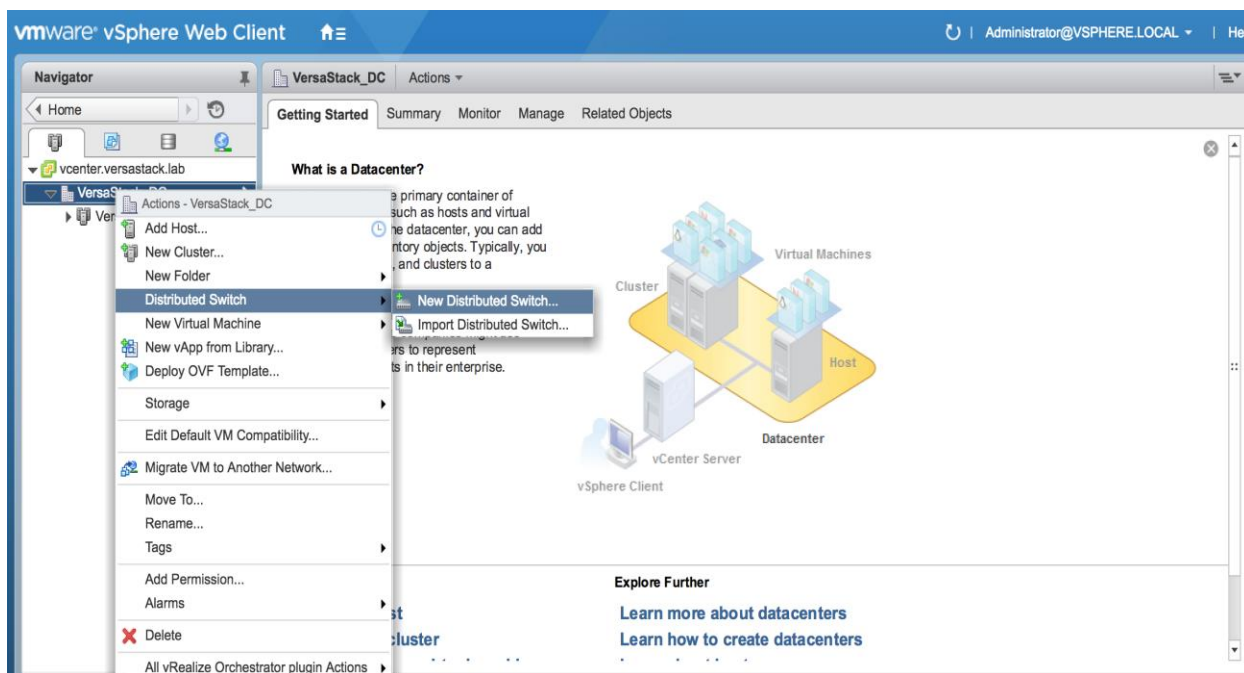


20. Repeat these steps for each host being added to the cluster, changing the vMotion VMkernel IP to an appropriate unique value for each host.

### Create a VMware vDS for Application and Production networks

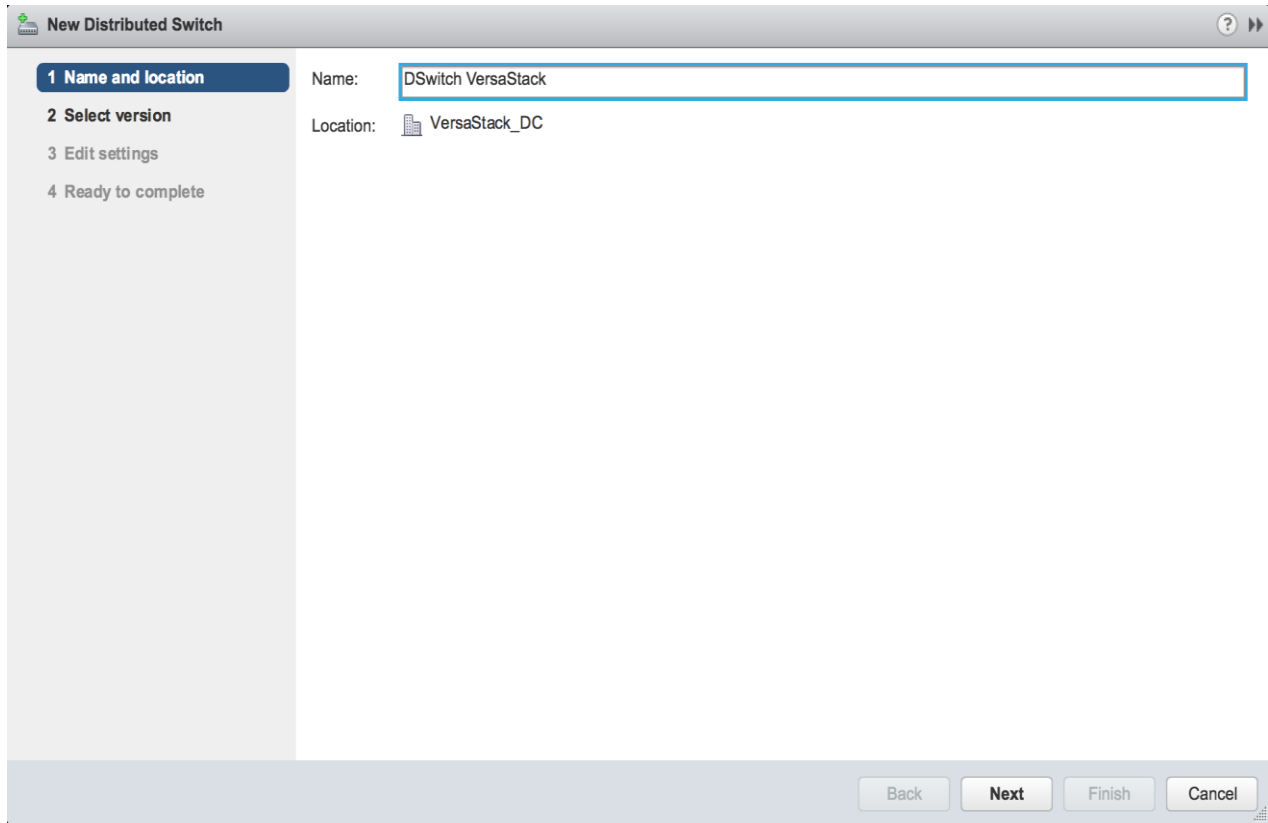
Production networks will be configured on a VMware vDS to allow additional configuration, as well as consistency between hosts. To configure the VMware vDS, click the right-most icon within the Navigation window, and complete the following steps:

1. Right-click the Datacenter (VersaStack\_DC in the example picture), select from the pulldown Distributed Switch -> New Distributed Switch.

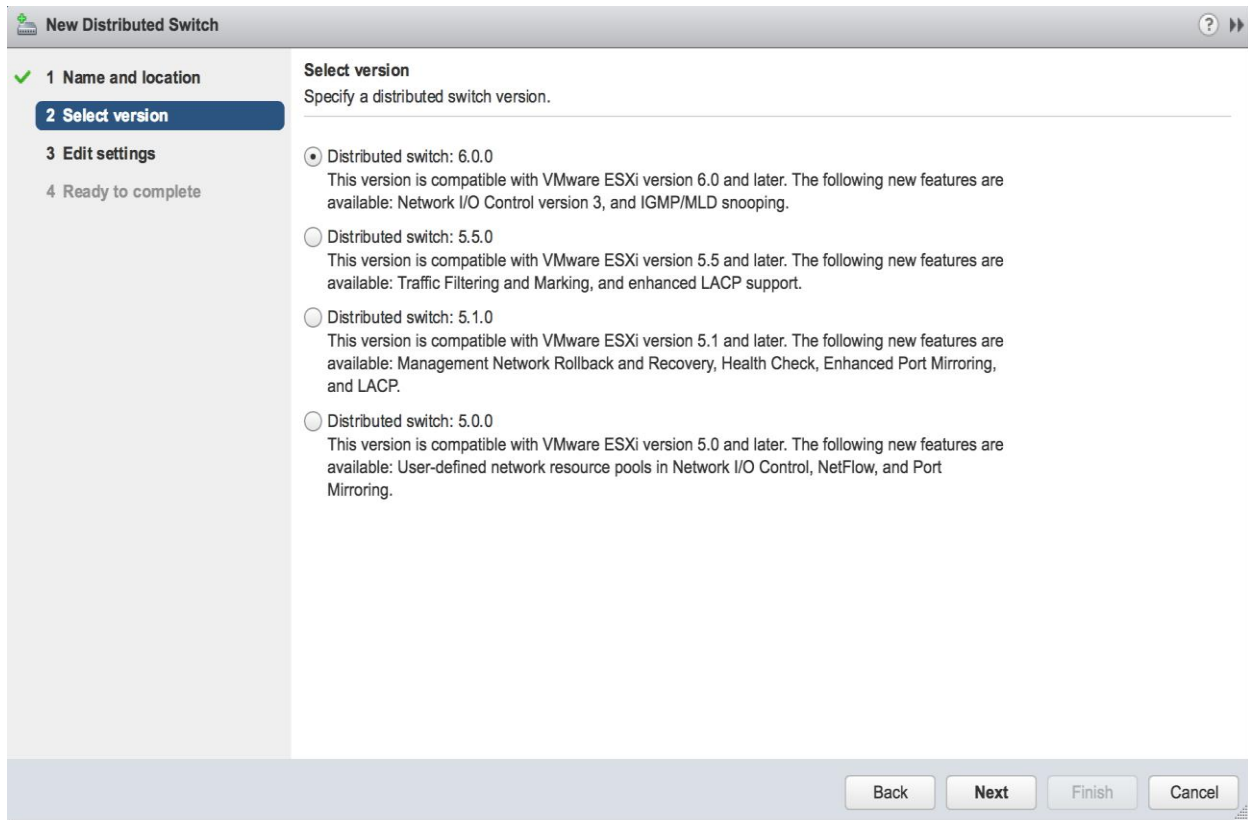




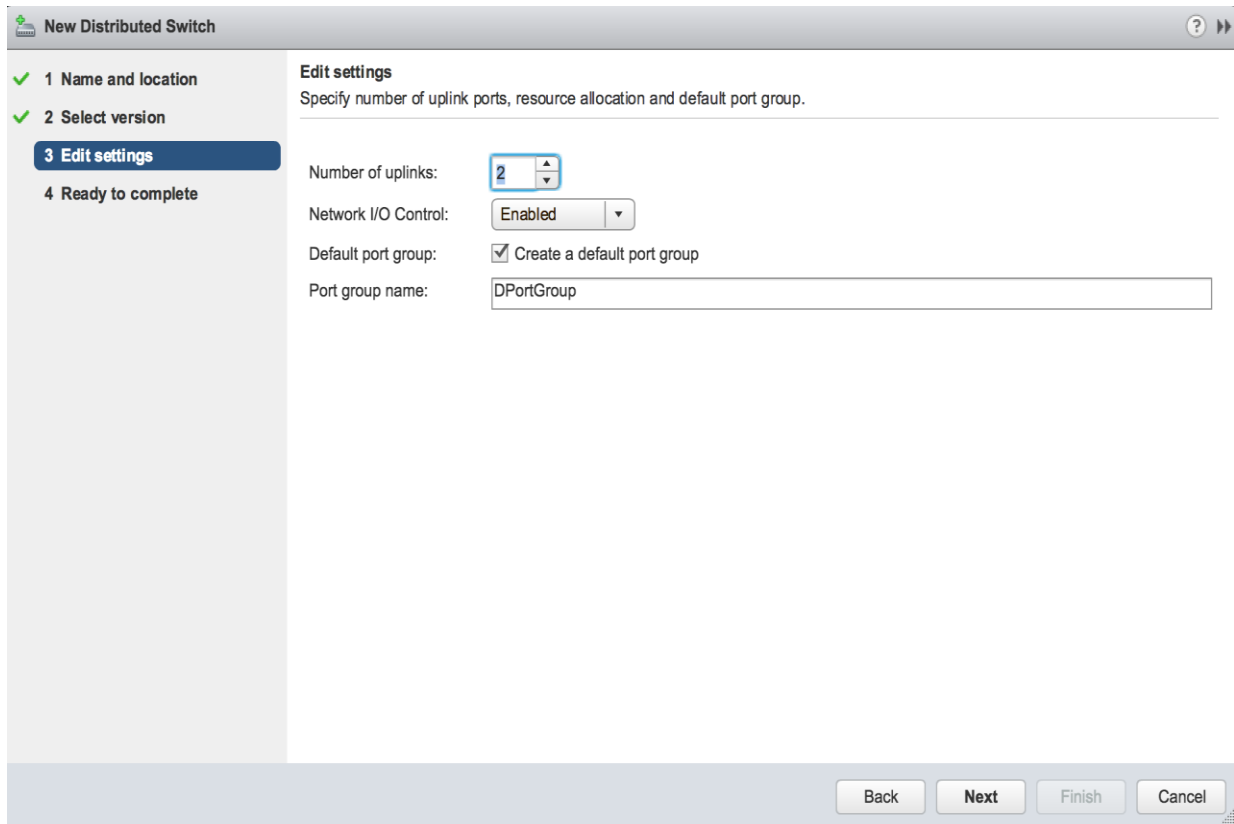
2. Provide a relevant name for the Name field, and click Next.



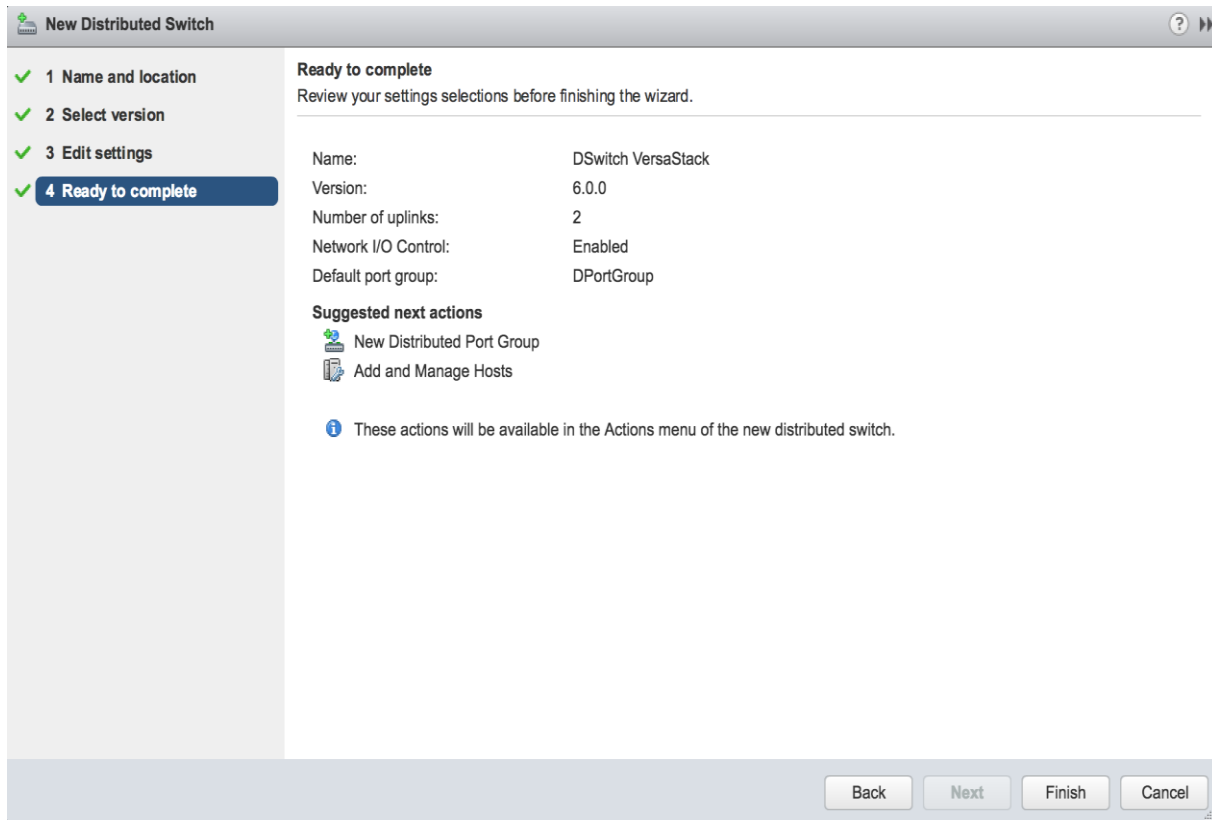
3. Leave the version selected as Distributed switch: 6.0.0, and click Next.



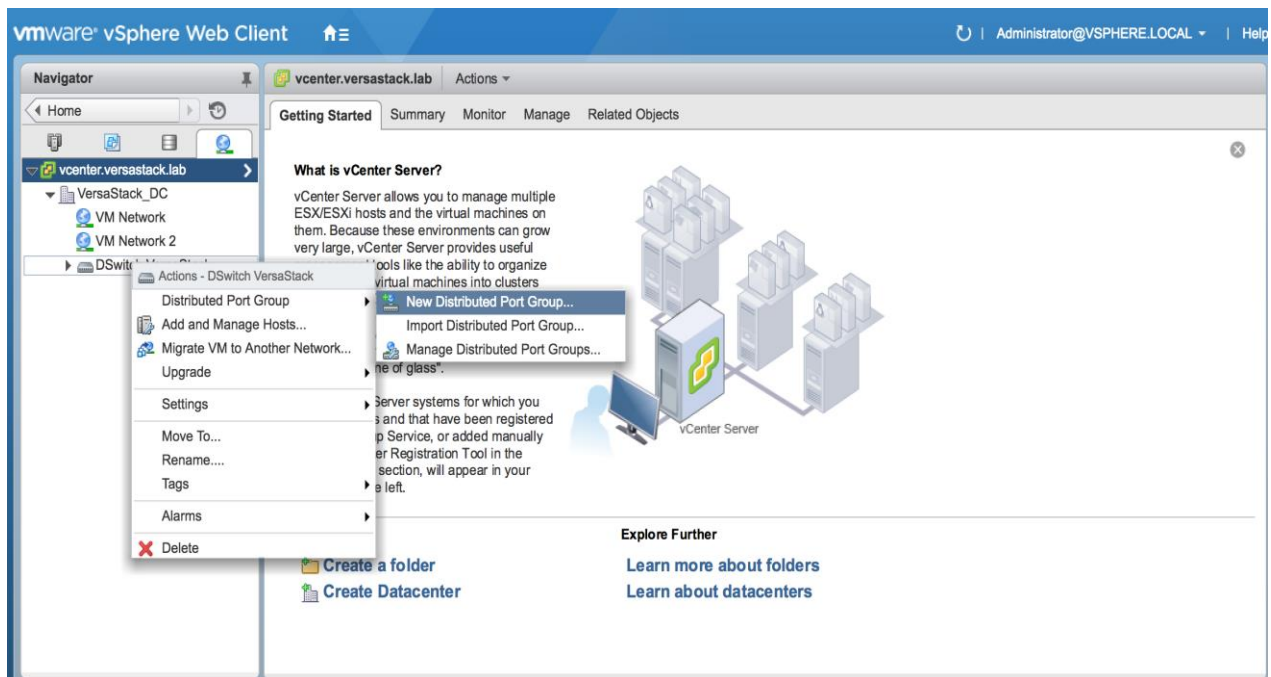
4. Change the Number of uplinks from 4 to 2, and click Next.



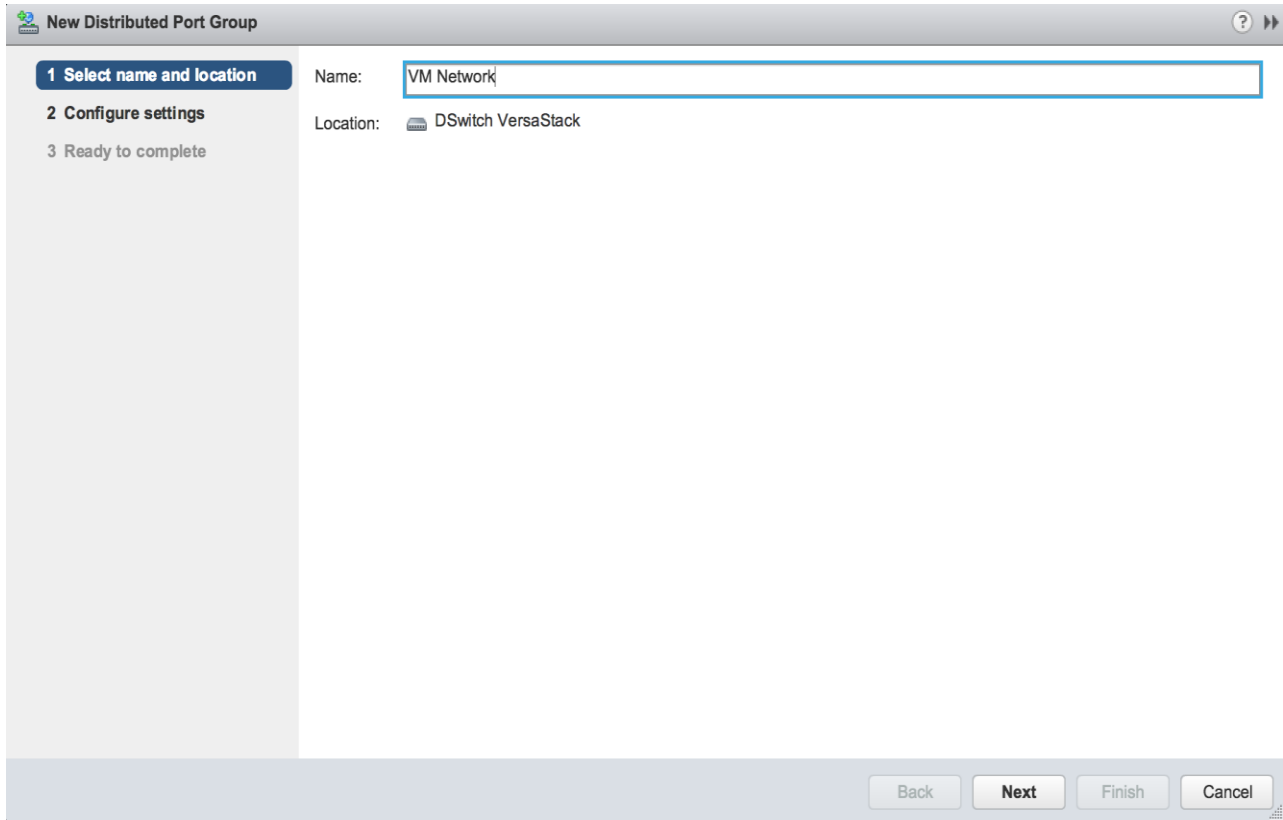
5. Review the summary in the Ready to complete page and click Finish to create the vDS.



- Finding the vDS showing up as DSwitch VersaStack under the Network icon of the Navigator pane, right-click the vDS and select Distributed Port Group -> **New Distributed Port Group...**



7. Enter an appropriate name into the Name field for application/production networks that will be carried on the vDS, and click Next.



8. Select VLAN from the VLAN type pull-down, and enter the appropriate VLAN number into the VLAN ID field. Click Next.

**New Distributed Port Group**

1 Select name and location  
2 **Configure settings**  
3 Ready to complete

**Configure settings**  
Set general properties of the new port group.

Port binding: Static binding

Port allocation: Elastic

Number of ports: 8

Network resource pool: (default)

**VLAN**

VLAN type: VLAN

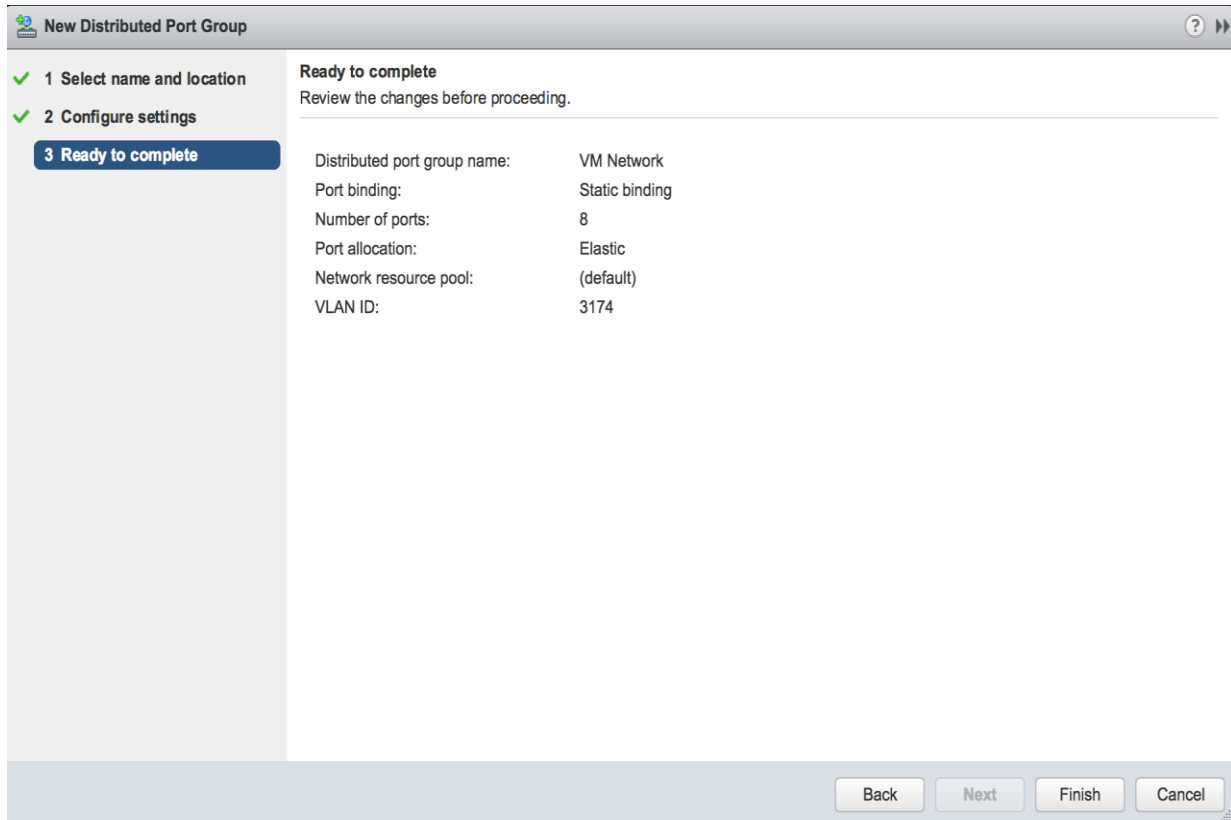
VLAN ID: 3174

**Advanced**

Customize default policies configuration

Back Next Finish Cancel

9. Confirm the summary shown on the Ready to complete page, and click Finish to create the distributed port group.

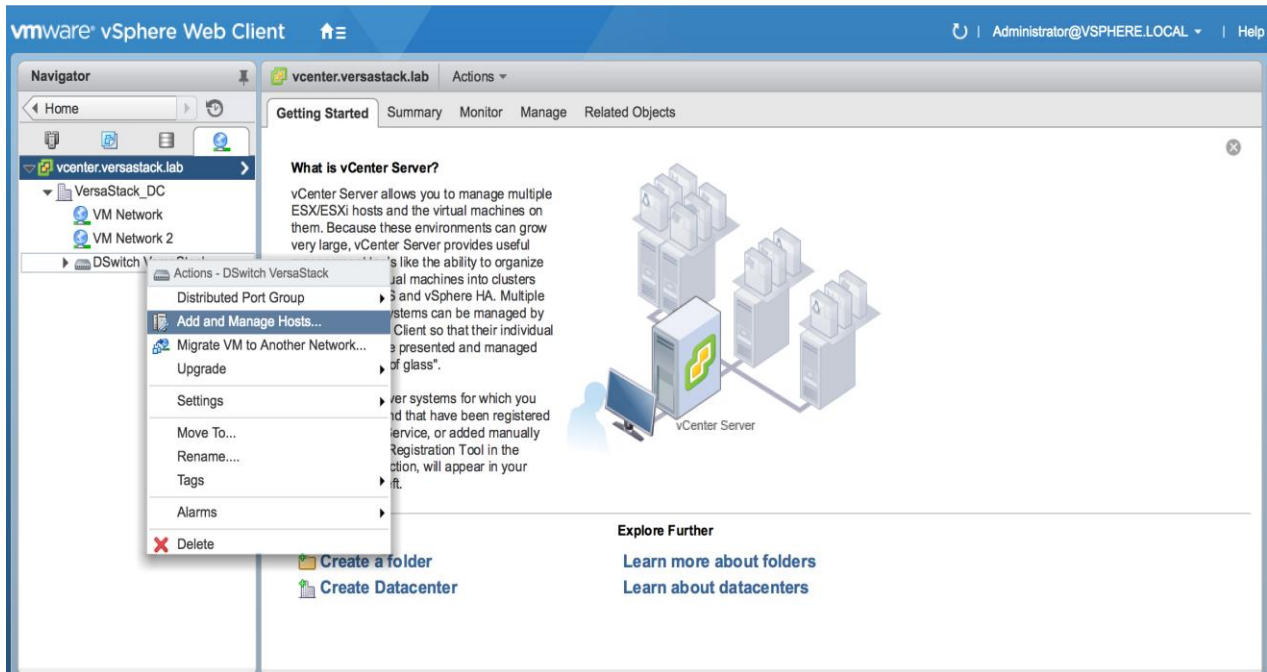


## Add the ESXi Hosts to the vDS

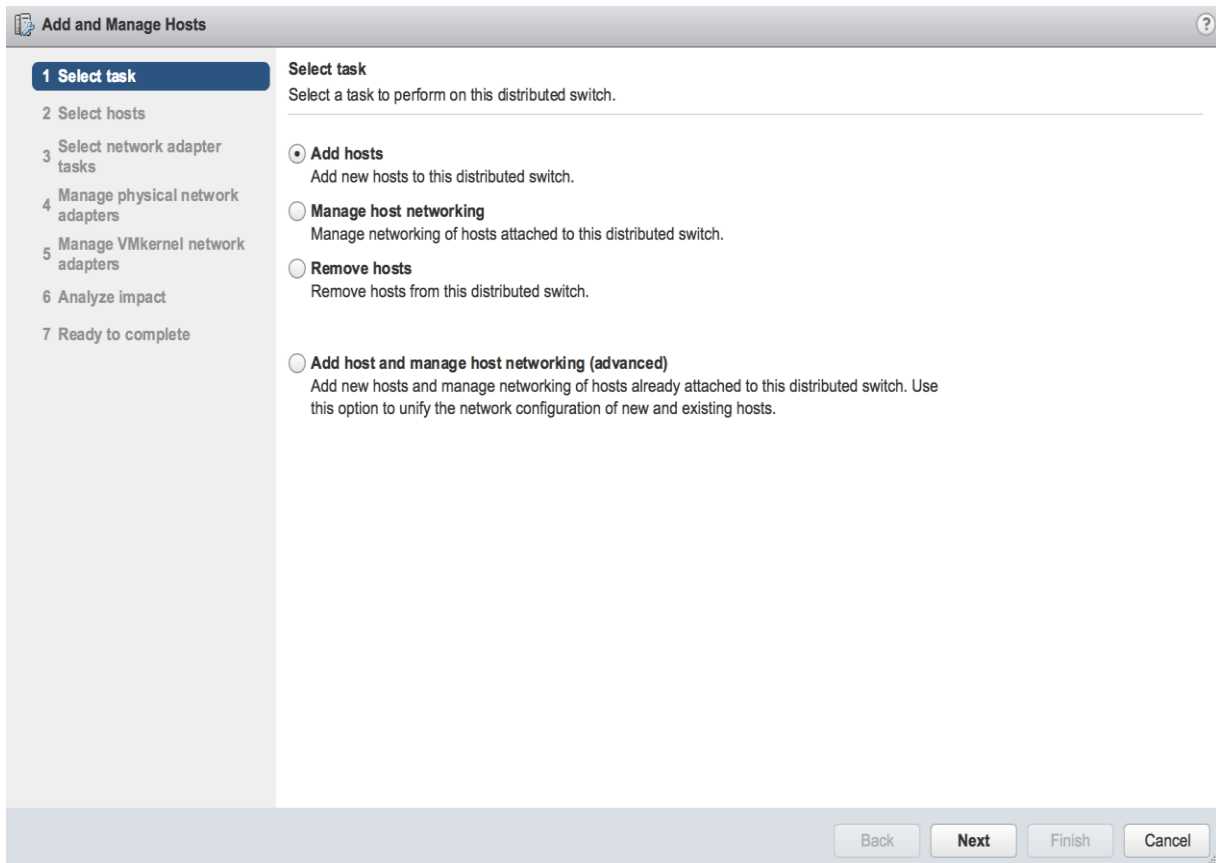
With the vDS and the distributed port groups created within the vDS in place, the ESXi hosts will be added to the vDS.

To add the ESXi Hosts to the vDS, complete the following steps:

1. Within the Networking sub-tab of Hosts and Clusters of the Navigator window, right-click the vDS and select **Add and Manage Hosts...**

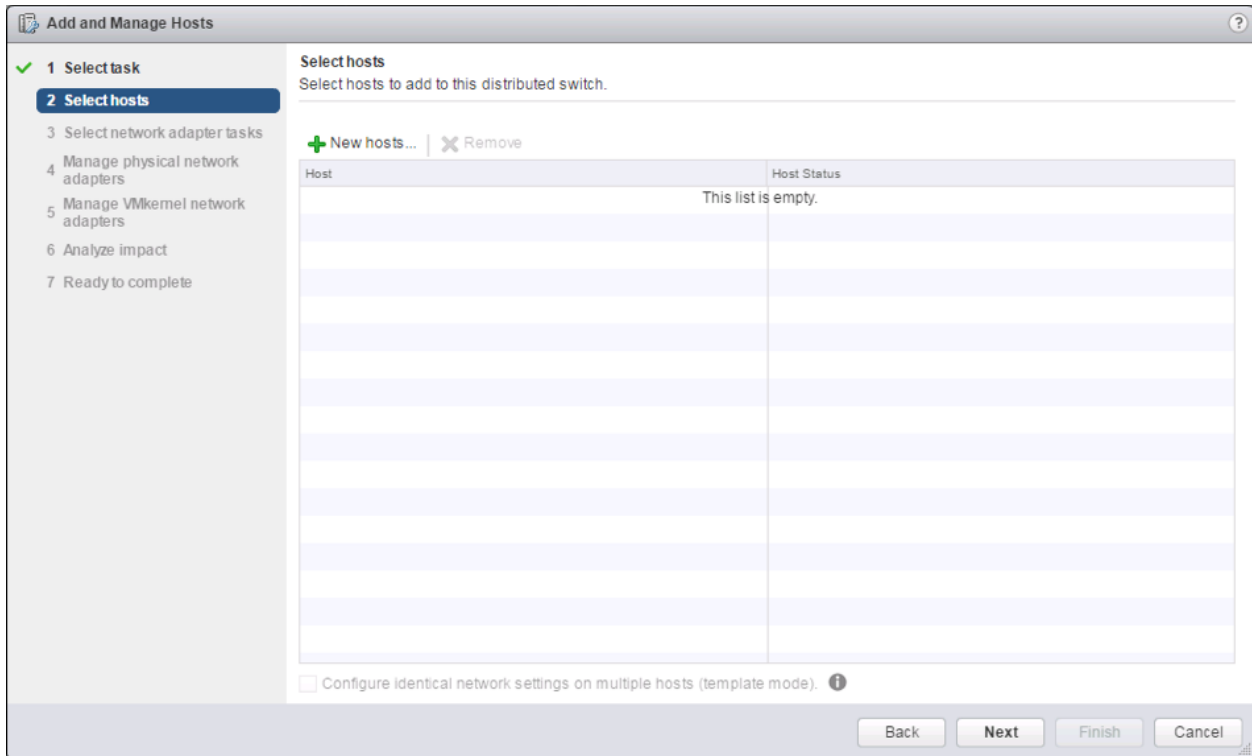


2. Leave Add hosts selected and click Next.

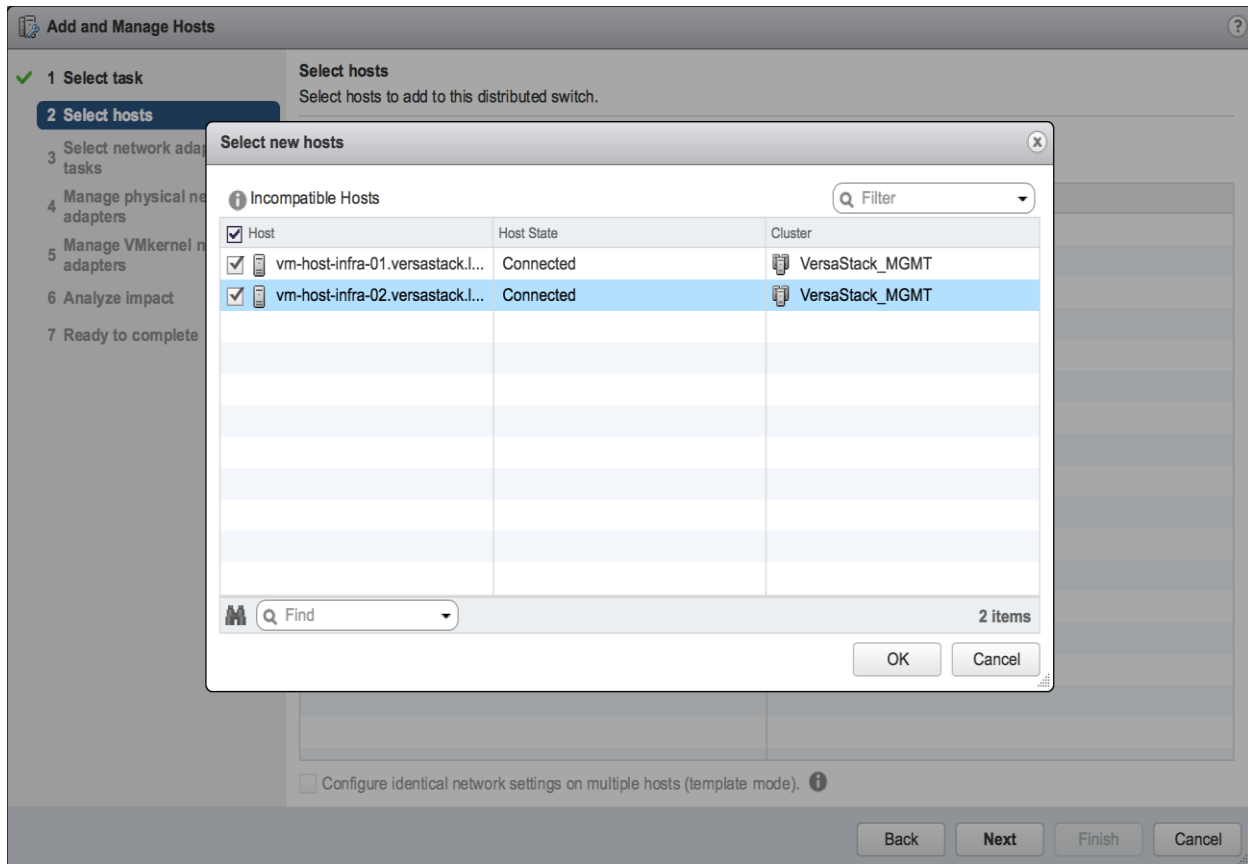




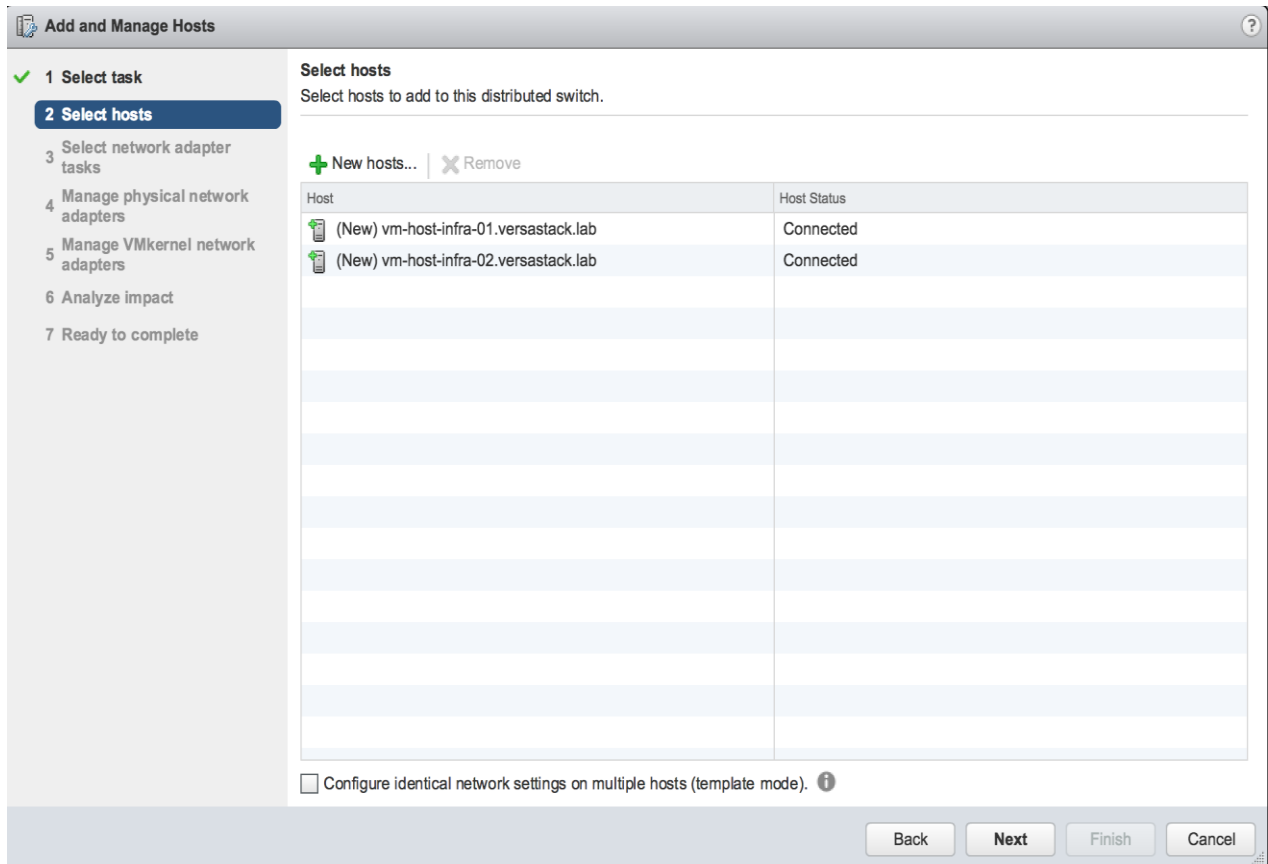
3. Click the green + icon next to New hosts...



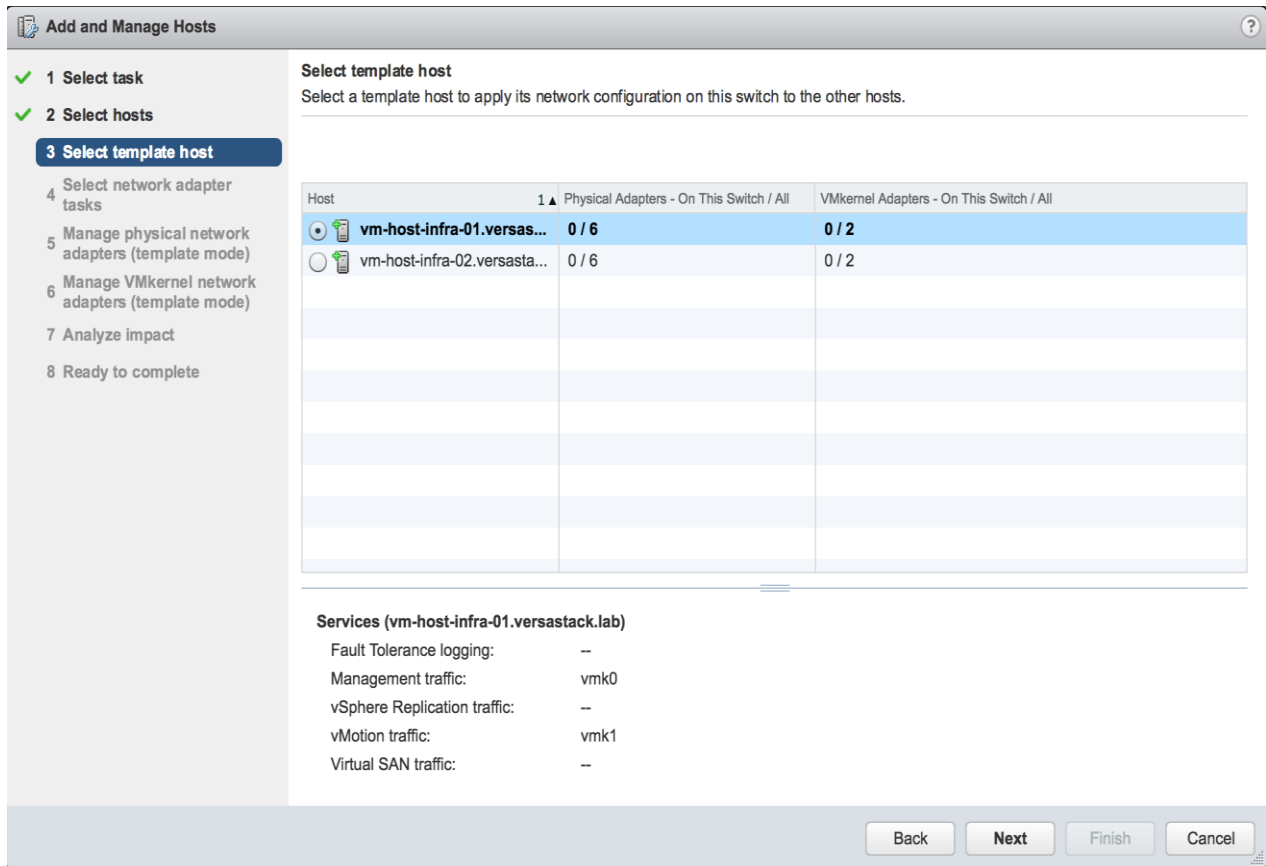
4. In the Select new hosts pop-up that appears, select the hosts to be added, and click OK to begin joining them to the vDS.



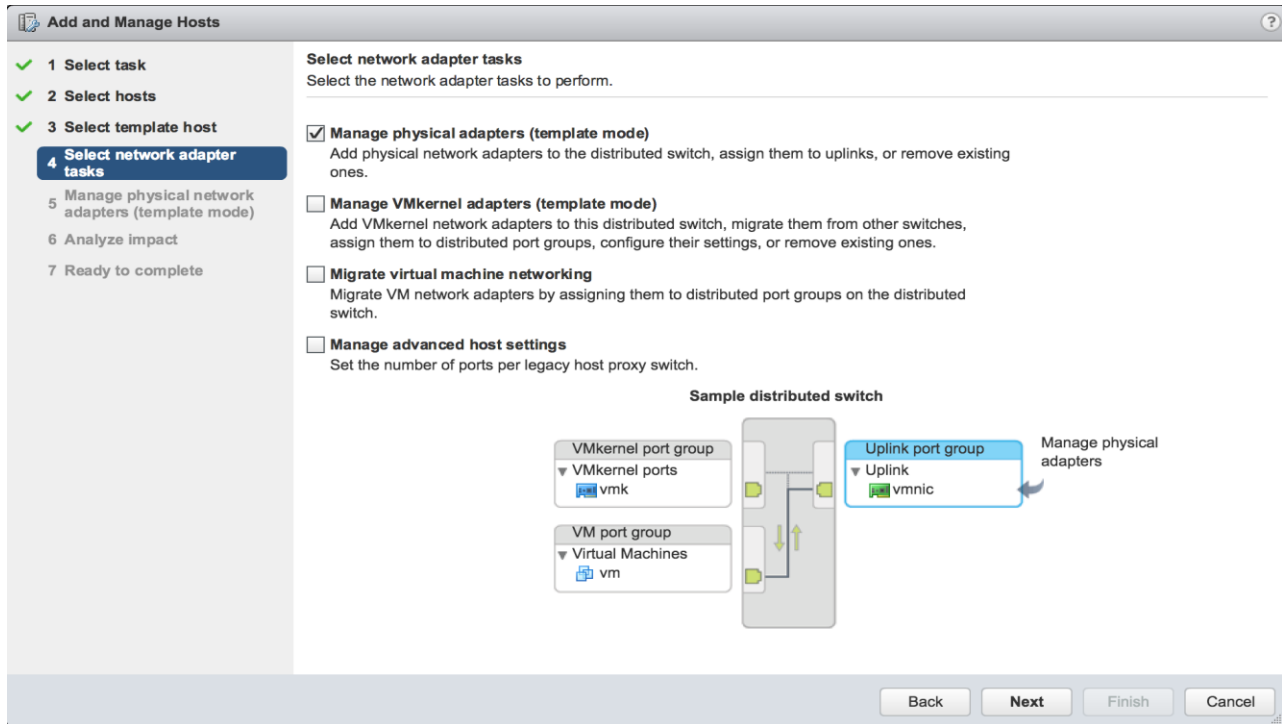
5. Click the Configure identical network settings on multiple hosts (template mode) checkbox near the bottom of the window, and click Next.



6. Select the first host to be the template host, and click Next.



7. Unselect Manage VMkernel adapters (template mode) if it is selected, and click Next.



- For each vmnic (vmnic4 and vmnic5) to be assigned from the Host/Physical Network Adapters column, select the vmnic and click the Assign uplink.

**Add and Manage Hosts**

- ✓ 1 Select task
- ✓ 2 Select hosts
- ✓ 3 Select template host
- ✓ 4 Select network adapter tasks
- 5 Manage physical network adapters (template mode)**
- 6 Analyze impact
- 7 Ready to complete

**Manage physical network adapters (template mode)**  
 Add or remove physical network adapters to this distributed switch.

1 Configure or review physical network adapter assignments for the template host in this switch.

Assign uplink Reset changes View settings

Host/Physical Network Adapters	1 ▲ In Use by Switch	Uplink	Uplink Port Group
vmnic0	vSwitch0	--	--
vmnic1	vSwitch0	--	--
vmnic2	vSwitch1	--	--
vmnic3	vSwitch1	--	--
vmnic4	--	--	--
vmnic5	--	--	--

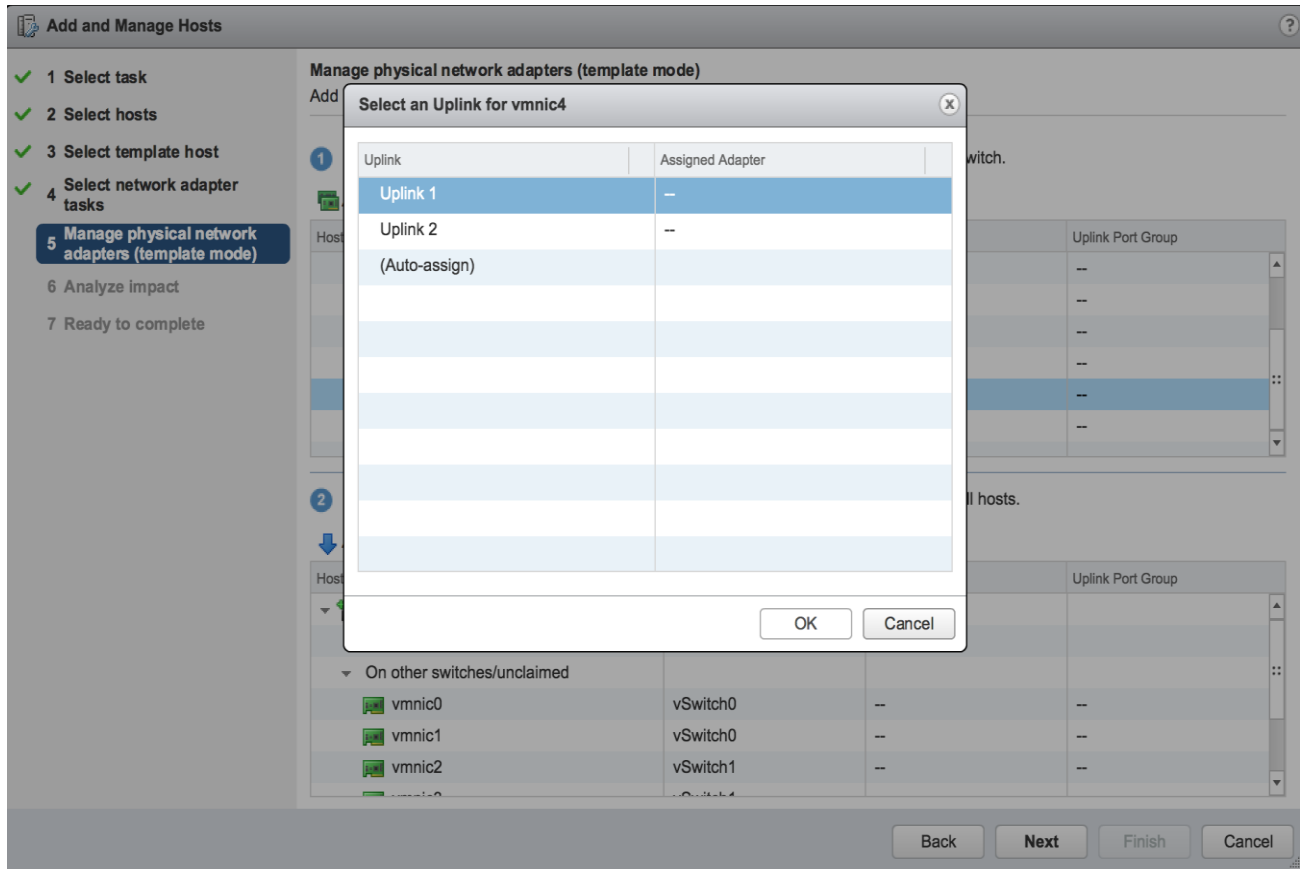
2 Apply the physical network adapter assignments on this switch for the template host to all hosts.

Apply to all Reset all View settings

Host/Physical Network Adapters	1 ▲ In Use by Switch	Uplink	Uplink Port Group
vm-host-infra-02.versastack.lab			
On this switch			
On other switches/unclaimed			
vmnic0	vSwitch0	--	--
vmnic1	vSwitch0	--	--
vmnic2	vSwitch1	--	--

Back Next Finish Cancel

9. Assign the first to Uplink 1 and assign the second to Uplink 2.



10. With both vmnics assigned, click Apply to all within the second part of this page, click OK in the Host Settings Not Applied pop-up that will appear, and click Next.

**Add and Manage Hosts**

- ✓ 1 Select task
- ✓ 2 Select hosts
- ✓ 3 Select template host
- ✓ 4 Select network adapter tasks
- 5 Manage physical network adapters (template mode)**
- 6 Analyze impact
- 7 Ready to complete

**Manage physical network adapters (template mode)**  
Add or remove physical network adapters to this distributed switch.

1 Configure or review physical network adapter assignments for the template host in this switch.

Assign uplink Reset changes View settings

Host/Physical Network Adapters	In Use by Switch	Uplink	Uplink Port Group
<b>vmnic5 (Assigned)</b>	--	Uplink 2	DSwitch VersaSta-DVU...
▼ On other switches/unclaimed			
vmnic0	vSwitch0	--	--
vmnic1	vSwitch0	--	--
vmnic2	vSwitch1	--	--
vmnic3	vSwitch1	--	--

2 Apply the physical network adapter assignments on this switch for the template host to all hosts.

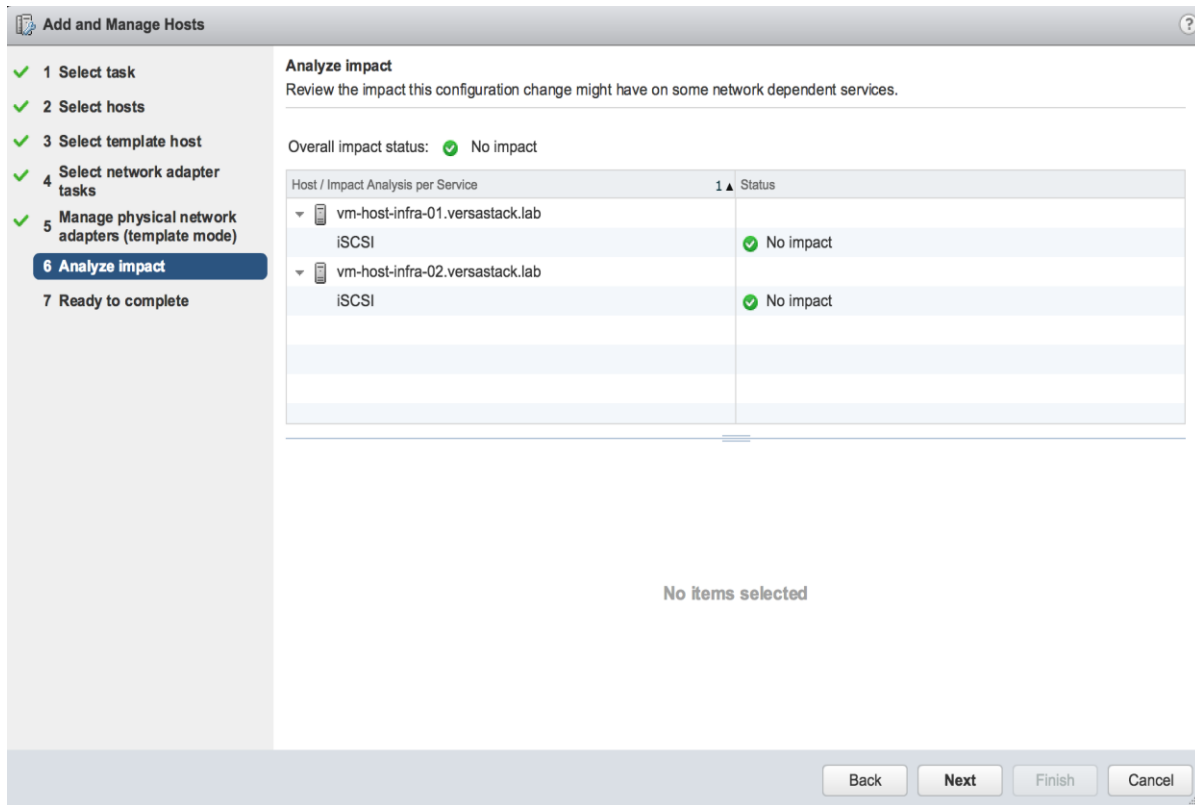
Apply to all Reset all View settings

Host/Physical Network Adapters	In Use by Switch	Uplink	Uplink Port Group
▼ vm-host-infra-02.versastack.lab			
▼ On this switch			
vmnic4 (Assigned)	--	Uplink 1	DSwitch VersaSta-DVU...
vmnic5 (Assigned)	--	Uplink 2	DSwitch VersaSta-DVU...
▼ On other switches/unclaimed			
vmnic0	vSwitch0	--	--

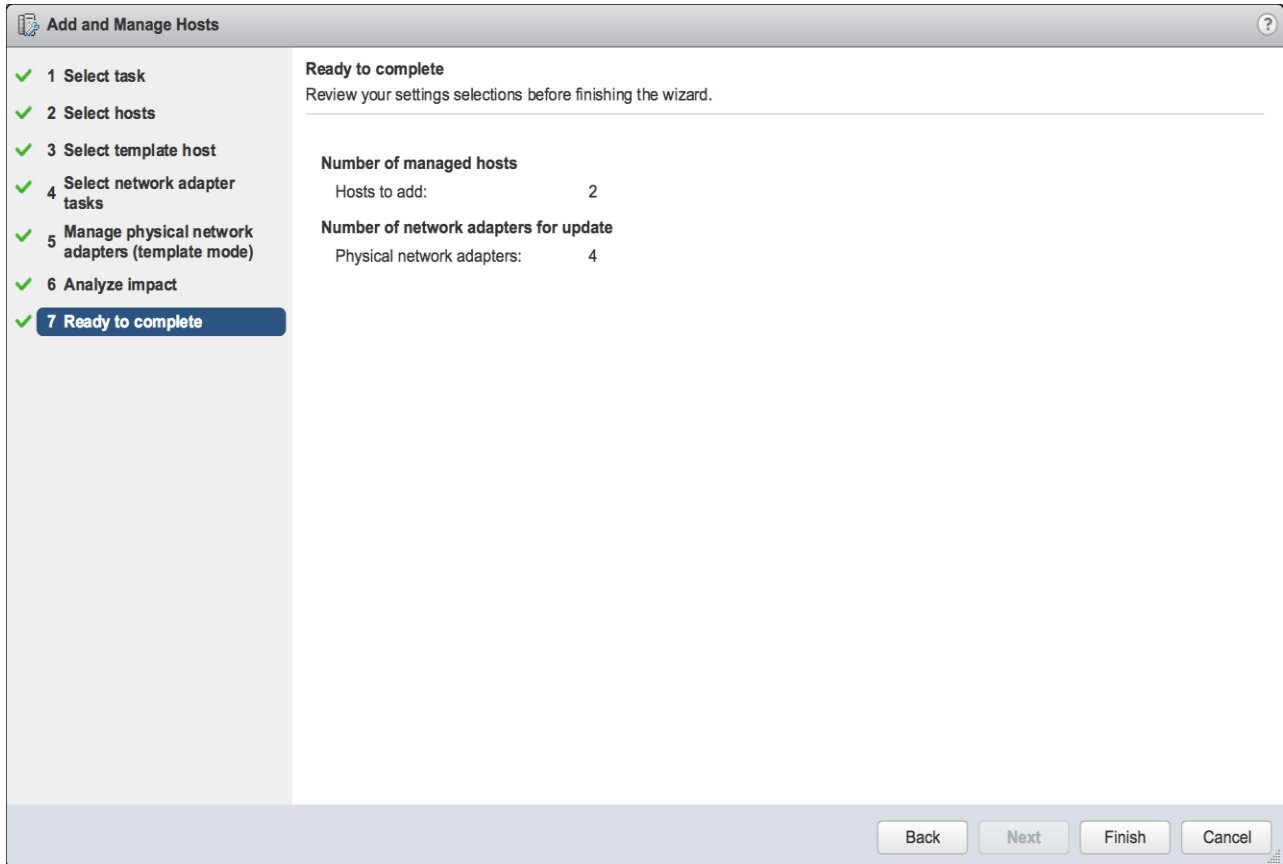
Back Next Finish Cancel

11. Proceed past the Analyze impact screen if no issues appear.





12. Review the Ready to complete summary and click Finish to add the hosts to the vDS.



## Appendix

---

### Cisco Nexus 9000 Example Configurations

#### Cisco Nexus 9000 A

```
VersaStack_V5030_Mini-A# sh running-config
```

```
!Command: show running-config
```

```
!Time: Thu Jan 5 15:13:19 2017
```

```
version 7.0(3)I2(4)
```

```
switchname VersaStack_V5030_Mini-A
```

```
vdc VersaStack_V5030_Mini-A id 1
```

```
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
```

```
feature telnet
```

```
cfs eth distribute
```

```
feature lacp
```

```
feature vpc
```

```
username admin password 5 $1$xqcEGkDT$/lpogNkFXi8RTWhgAuSnD1 role network-admin
```

```
ssh key rsa 2048
```

```
ip domain-lookup
```

copp profile strict

snmp-server user admin network-admin auth md5 0xc00b2a99699a8d5f64bd04c45092197d priv  
0xc00b2a99699a8d5f64bd04c45092197d localizedkey

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

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

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

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

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

ntp server 192.168.160.254

vlan 1-2,11,3173-3174

vlan 2

name Native-VLAN

vlan 11

name IB-MGMT-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

vpc domain 10

peer-switch

role priority 10

peer-keepalive destination 192.168.162.202 source 192.168.162.201

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 11,3173-3174

spanning-tree port type network

vpc peer-link

interface port-channel13

description VersaStack\_UCS-Mini-A

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan 11,3173-3174

spanning-tree port type edge trunk

mtu 9216

vpc 13

interface port-channel14

description VersaStack\_UCS-Mini-B

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan 11,3173-3174

spanning-tree port type edge trunk

```
mtu 9216
```

```
vpc 14
```

```
interface port-channel15
```

```
description IB-MGMT
```

```
switchport mode trunk
```

```
switchport access vlan 11
```

```
switchport trunk allowed vlan 11
```

```
spanning-tree port type network
```

```
vpc 15
```

```
interface Ethernet1/1
```

```
interface Ethernet1/2
```

```
interface Ethernet1/3
```

```
description VersaStack_UCS-Mini-A:1/3
```

```
switchport mode trunk
```

```
switchport trunk native vlan 2
```

```
switchport trunk allowed vlan 11,3173-3174
```

```
mtu 9216
```

```
channel-group 13 mode active
```

```
interface Ethernet1/4
```

```
description VersaStack_UCS-Mini-B:1/4
```

```
switchport mode trunk
```

```
switchport trunk native vlan 2
```

```
switchport trunk allowed vlan 11,3173-3174
```

```
mtu 9216
```

```
channel-group 14 mode active
```

interface Ethernet1/5

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface Ethernet1/33



interface Ethernet1/34

interface Ethernet1/35

interface Ethernet1/36

description IB-MGMT-SWITCH\_uplink

switchport mode trunk

switchport access vlan 11

switchport trunk allowed vlan 11

channel-group 15 mode active

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40

interface Ethernet1/41

interface Ethernet1/42

interface Ethernet1/43

interface Ethernet1/44

interface Ethernet1/45

interface Ethernet1/46

interface Ethernet1/47

description VPC Peer VersaStack-V5030\_9k\_B:1/47

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan 11,3173-3174

channel-group 10 mode active

interface Ethernet1/48

description VPC Peer VersaStack-V5030\_9k\_B:1/48

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan 11,3173-3174

channel-group 10 mode active

interface Ethernet1/49

interface Ethernet1/50

interface Ethernet1/51

interface Ethernet1/52

interface Ethernet1/53

interface Ethernet1/54

```
interface mgmt0
  vrf member management
  ip address 192.168.162.201/22

line console

line vty
  session-limit 16

boot nxos bootflash:/nxos.7.0.3.I2.4.bin
```

```
VersaStack_V5030_Mini-A# exit
```

## Cisco Nexus 9000 B

```
VersaStack_V5030_Mini-B# sh running-config
```

```
!Command: show running-config
```

```
!Time: Thu Jan 5 15:12:02 2017
```

```
version 7.0(3)I2(4)
switchname VersaStack_V5030_Mini-B
vdc VersaStack_V5030_Mini-B id 1

  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
```

feature telnet

cfs eth distribute

feature lacp

feature vpc

username admin password 5 \$1\$9MAlmrSw\$7LR4R1BI06fIWSbkgI6KM/ role network-admin

ssh key rsa 2048

ip domain-lookup

copp profile strict

snmp-server user admin network-admin auth md5 0xca1d453021a34c63cd343709533f6187 priv  
0xca1d453021a34c63cd343709533f6187 localizedkey

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

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

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

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

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

ntp server 192.168.160.254

vlan 1-2,11,3173-3174

vlan 2

name Native-VLAN

vlan 11

name IB-MGMT-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
vpc domain 10
  peer-switch
  role priority 10
  peer-keepalive destination 192.168.162.201 source 192.168.162.202
  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 11,3173-3174
  spanning-tree port type network
  vpc peer-link
```

```
interface port-channel13
  description VersaStack_UCS-Mini-A
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 11,3173-3174
  spanning-tree port type edge trunk
```

mtu 9216

vpc 13

interface port-channel14

description VersaStack\_UCS-Mini-B

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan 11,3173-3174

spanning-tree port type edge trunk

mtu 9216

vpc 14

interface port-channel15

description IB-MGMT

switchport mode trunk

switchport access vlan 11

switchport trunk allowed vlan 11

spanning-tree port type network

vpc 15

interface Ethernet1/1

interface Ethernet1/2

interface Ethernet1/3

description VersaStack\_UCS-Mini-B:1/3

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan 11,3173-3174

```
mtu 9216  
channel-group 14 mode active
```

```
interface Ethernet1/4  
description VersaStack_UCS-Mini-A:1/4  
switchport mode trunk  
switchport trunk native vlan 2  
switchport trunk allowed vlan 11,3173-3174  
mtu 9216  
channel-group 13 mode active
```

```
interface Ethernet1/5
```

```
interface Ethernet1/6
```

```
interface Ethernet1/7
```

```
interface Ethernet1/8
```

```
interface Ethernet1/9
```

```
interface Ethernet1/10
```

```
interface Ethernet1/11
```

```
interface Ethernet1/12
```

```
interface Ethernet1/13
```

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28



interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface Ethernet1/33

interface Ethernet1/34

interface Ethernet1/35

interface Ethernet1/36

description IB-MGMT-SWITCH\_uplink

switchport mode trunk

switchport access vlan 11

switchport trunk allowed vlan 11

channel-group 15 mode active

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40

interface Ethernet1/41

interface Ethernet1/42

interface Ethernet1/43

interface Ethernet1/44

interface Ethernet1/45

interface Ethernet1/46

interface Ethernet1/47

description VPC Peer VersaStack-V5030\_9k\_A:1/47

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan 11,3173-3174

channel-group 10 mode active

interface Ethernet1/48

description VPC Peer VersaStack-V5030\_9k\_A:1/48

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan 11,3173-3174

channel-group 10 mode active

interface Ethernet1/49

```
interface Ethernet1/50
```

```
interface Ethernet1/51
```

```
interface Ethernet1/52
```

```
interface Ethernet1/53
```

```
interface Ethernet1/54
```

```
interface mgmt0
```

```
  vrf member management
```

```
  ip address 192.168.162.202/22
```

```
line console
```

```
line vty
```

```
  session-limit 16
```

```
boot nxos bootflash:/nxos.7.0.3.I2.4.bin
```

```
VersaStack_V5030_Mini-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.

Adam Reid - Test Specialist, Systems & Technology Group, IBM

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

## Acknowledgements

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

- Haseeb Niazi, Technical Marketing Engineer, Cisco Systems, Inc.