

FlashStack Virtual Server Infrastructure with Fibre Channel Storage for VMware vSphere 6.7 U1

Deployment Guide for Fibre Channel using FlashStack with
Cisco UCS 6400 Fabric Interconnect and Pure Storage
FlashArray//X Series

Last Updated: December 23, 2019



About the Cisco Validated Design Program

The Cisco Validated Design (CVD) program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information, go to:

<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 NON-INFRINGEMENT 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 Unified Computing System (Cisco UCS), Cisco UCS B-Series Blade Servers, Cisco UCS C-Series Rack Servers, Cisco UCS S-Series Storage Servers, Cisco UCS Manager, Cisco UCS Management Software, Cisco Unified Fabric, Cisco Application Centric Infrastructure, Cisco Nexus 9000 Series, Cisco Nexus 7000 Series, Cisco Prime Data Center Network Manager, Cisco NX-OS Software, Cisco MDS Series, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, 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)

© 2019 Cisco Systems, Inc. All rights reserved.

Table of Contents

Executive Summary	6
Solution Overview	7
Introduction.....	7
Audience	7
Purpose of this Document.....	7
Solution Summary	7
Deployment Hardware and Software.....	10
Software Revisions	10
Configuration Guidelines	11
Physical Topology	14
Network Switch Configuration.....	20
Network Configuration	20
Physical Connectivity.....	20
Cisco Nexus Basic System Configuration Dialog.....	20
Cisco Nexus Switch Configuration	23
Storage Configuration	28
Pure Storage FlashArray//X70 R2 Configuration	28
FlashArray Initial Configuration.....	28
Add an Alert Recipient.....	29
Configure Pure1 Support	30
Configure the Domain Name System (DNS) Server IP Addresses.....	32
Directory Service Sub-view	33
SSL Certificate Sub-view.....	35
CA-Sign Certificate	35
MDS Fabric Configuration	38
Physical Connectivity.....	38
Cisco MDS Basic System Configuration Dialog	38
Cisco MDS Configuration	41
Compute Configuration.....	44
Cisco UCS Compute Configuration	44
Physical Connectivity.....	44
Cisco UCS Basic System Configuration Dialog.....	44
Cisco UCS Manager Configuration	46
Upgrade Cisco UCS Manager to Version 4.0(2b).....	46
Enable Anonymous Reporting	46

Configure Cisco UCS Call Home.....	47
Configure NTP.....	48
Configure Cisco UCS Servers	50
Edit Chassis Discovery Policy	50
Enable Server and Uplink Ports.....	50
Acknowledge Cisco UCS Chassis.....	52
Create Pools	53
Set Packages and Policies	67
Configure Cisco UCS LAN Connectivity	80
Create Uplink Port Channels	80
Create VLANs.....	83
Create vNIC Templates.....	86
Create LAN Connectivity Policy.....	100
Configure FC SAN Connectivity	108
Create Boot Policy.....	120
Create Service Profile Templates	126
Create Service Profiles.....	135
Claim in Intersight	135
MDS Fabric Zoning	138
Create Device Aliases	138
MDS Zoning	142
Create and Activate Zoneset	143
FlashArray Storage Deployment	144
Host Port Identification	144
Host Registration	144
Create Host Group.....	147
Private Boot Volumes for Each ESXi Host	149
Configure Storage Policy Based Management.....	151
VMware vSphere Deployment	153
ESXi Installation.....	153
Download Cisco Custom Image for ESXi 6.7 U1	153
Log into Cisco UCS 6454 Fabric Interconnect	154
Set Up VMware ESXi Installation	154
Install ESXi.....	154
Set Up Management Networking for ESXi Hosts.....	155
Create FlashStack Datacenter	156
Create VMware vDS for Infrastructure and Application Traffic	157

Add the VMware ESXi Hosts Using the VMware vSphere Web Client	164
Pure Storage vSphere Web Client Plugin	168
Import Protection Group as VM Storage Policy	171
Add Datastores	172
Configure ESXi Settings	175
Install VMware Driver for the Cisco Virtual Interface Card (VIC)	179
Add the ESXi Hosts to the vDS	180
Create vMotion VMkernel adapters	192
Appendix.....	197
Sample Switch Configuration.....	197
About the Authors.....	203
Acknowledgements	203

Executive Summary

Cisco Validated Designs (CVDs) consist of systems and solutions that are designed, tested, and documented to facilitate and improve customer deployments. These designs incorporate a wide range of technologies and products into a portfolio of solutions that have been developed to address the business needs of our customers.

This document details the design in the FlashStack Virtual Server Infrastructure Design Guide for VMware vSphere 6.7 U1, which describes a validated converged infrastructure jointly developed by Cisco and Pure Storage. This solution explains the deployment of a predesigned, best-practice data center architecture with VMware vSphere built on the Cisco Unified Computing System (UCS), the Cisco Nexus® 9000 family of switches, Cisco MDS 9000 family of Fibre Channel switches, and Pure Storage FlashArray//X all flash storage configured for Fibre Channel based storage access.

When deployed, the architecture presents a robust infrastructure viable for a wide range of application workloads implemented as a virtual server infrastructure.

Solution Overview

Introduction

In the current industry there is a trend for pre-engineered solutions which standardize the data center infrastructure, offering the business operational efficiencies, agility and scale to address cloud, bimodal IT and their business. Their challenge is complexity, diverse application support, efficiency and risk; all these are met by FlashStack with:

- Reduced complexity and automatable infrastructure and easily deployed resources
- Robust components capable of supporting high performance and high bandwidth virtualized applications
- Efficiency through optimization of network bandwidth and in-line storage compression with de-duplication
- Risk reduction at each level of the design with resiliency built into each touch point throughout

Cisco and Pure Storage have partnered to deliver this Cisco Validated Design, which uses best of breed storage, server and network components to serve as the foundation for virtualized workloads, enabling efficient architectural designs that can be quickly and confidently deployed.

In this document we will describe a reference architecture detailing a Virtual Server Infrastructure composed of Cisco Nexus switches, Cisco UCS Compute, Cisco MDS Multilayer Fabric Switches and a Pure Storage FlashArray//X delivering a VMware vSphere 6.7 U1 hypervisor environment.

Audience

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

Purpose of this Document

This document details a step-by-step configuration and implementation guide for FlashStack, centered around the Cisco UCS 6454 Fabric Interconnect and the Pure Storage FlashArray//X70 R2. These components are supported by the 100G capable Cisco Nexus 9336C-FX2 switch and 32G FC capable Cisco MDS 9132T to deliver a Virtual Server infrastructure on Cisco UCS B200 M5 Blade Servers and Cisco UCS C220 M5 Rack Servers running VMware vSphere 6.7 U1.

The design that will be implemented is discussed in the [FlashStack Virtual Server Infrastructure for VMware vSphere 6.7 Update 1 Design Guide](#).

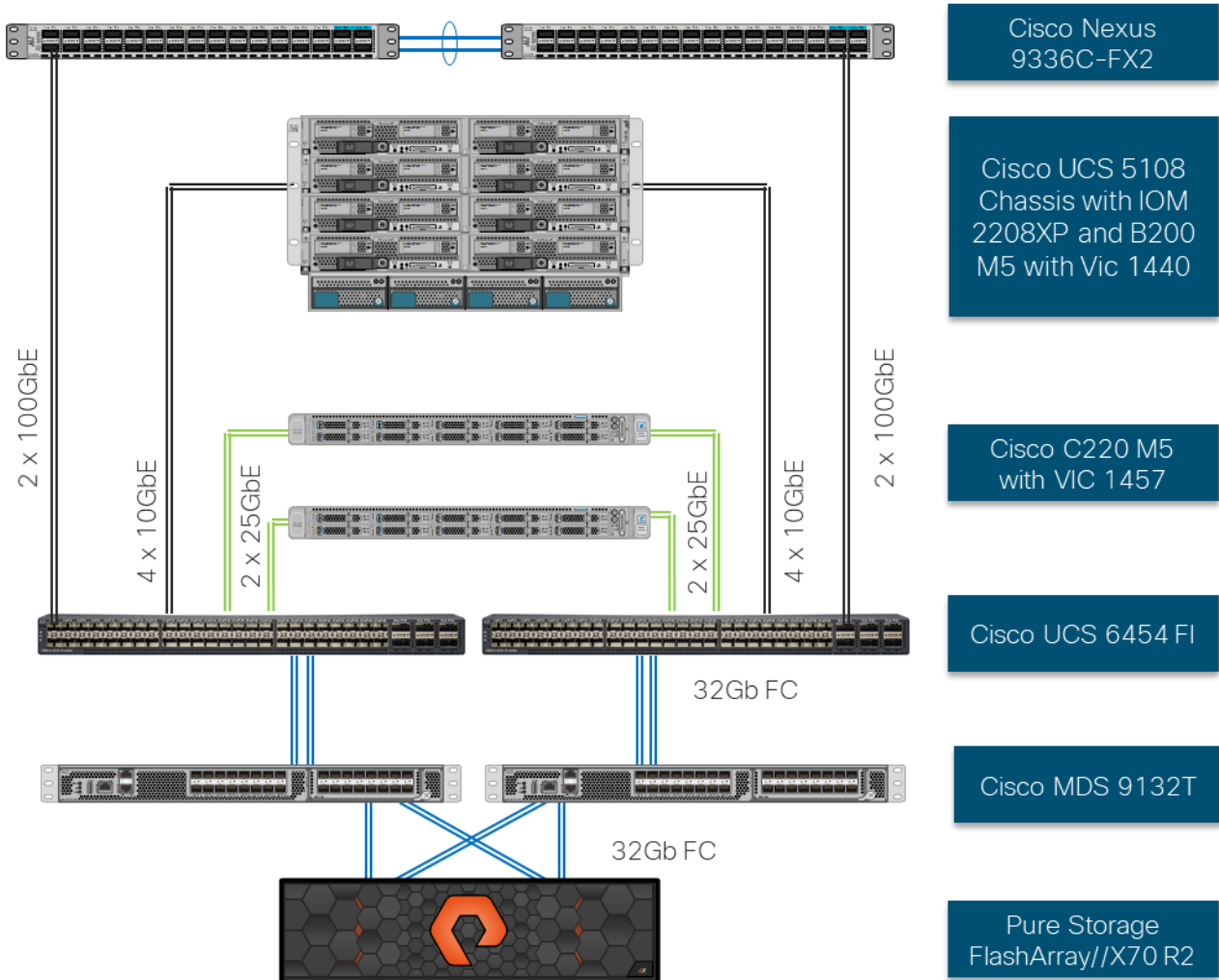
Solution Summary

The FlashStack Virtual Server Infrastructure is a validated reference architecture, collaborated on by Cisco and Pure Storage, built to serve enterprise data centers. The solution is built to deliver a VMware vSphere based environment, leveraging the Cisco Unified Computing System (Cisco UCS), Cisco Nexus switches, Cisco MDS switches, and Pure Storage FlashArray.

The architecture brings together a simple, wire once solution that is SAN booted from FC and is highly resilient at each layer of the design. This creates an infrastructure that is ideal for a variety of virtual application deployments that can reliably scale when growth is needed.

Figure 1 illustrates the base physical architecture used in FlashStack Virtual Server Infrastructure.

Figure 1 FlashStack with Cisco UCS 6454 and Pure Storage FlashArray //70 R2



The reference hardware configuration includes:

- Two Cisco Nexus 9336C-FX2 Switches
- Two Cisco MDS 9132T Switches
- Two Cisco UCS 6454 Fabric Interconnects
- Cisco UCS 5108 Chassis with two Cisco UCS 2308 Fabric Extenders
- Two Cisco UCS B200 M5 Blade Servers
- Four Cisco UCS C220 M5 Rack Servers

- One Pure Storage FlashArray//X70 R2

The virtual environment this supports is within VMware vSphere 6.7 U1 and includes virtual management and automation components from Cisco and Pure Storage built into the solution, or as optional add-ons.

This document provides a low-level example of steps to deploy this base architecture that may need some adjustments depending on the customer environment. These steps include physical cabling, network, storage, compute, and virtual device configurations.

Deployment Hardware and Software

Software Revisions

Table 1 lists the software versions for hardware and virtual components used in this solution. Each of these versions have been used have been certified within interoperability matrixes supported by Cisco, Pure Storage, and VMware. For information about the current supported versions, consult the following sources:

- Cisco UCS Hardware and Software Interoperability
Tool: <http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html>
- Pure Storage Interoperability(note, this interoperability list will require a support login form Pure): https://support.purestorage.com/FlashArray/Getting_Started/Compatibility_Matrix
- Pure Storage FlashStack Compatibility Matrix (note, this interoperability list will require a support login from Pure): https://support.purestorage.com/FlashStack/Product_Information/FlashStack_Compatibility_Matrix
- VMware Compatibility Guide: <http://www.vmware.com/resources/compatibility/search.php>
- Additionally, it is also strongly suggested to align FlashStack deployments with the recommended release for the Cisco Nexus 9000 switches used in the architecture:
- Nexus: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/recommended_releases/b_Minimum_and_Recommended_Cisco_NX-OS_Releases_for_Cisco_Nexus_9000_Series_Switches.html
- MDS: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/b_MDS_NX-OS_Recommended_Releases.html

If versions are selected that differ from the validated versions below, it is highly recommended to read the release notes of the selected version to be aware of any changes to features or commands that may have occurred.

Table 1 Software Revisions

Layer	Device	Image	Comments
Compute	Cisco UCS Fabric Interconnects 6400 Series, UCS B-200 M5, UCS C-220 M5	4.0(2b)	Includes Cisco UCS IOM 2208 and Cisco VIC 1400 Series
Network	Cisco Nexus 9000 NX-OS	7.0(3)I7(5)	
Storage	Pure Storage FlashArray//X70 R2	5.1.9	
	Cisco MDS 9132T	8.3(2)	
Software	Cisco UCS Manager	4.0(2b)	
	VMware vSphere ESXi Cisco Custom ISO	6.7 U1	
	VMware vSphere nenic Driver for ESXi	1.0.26.0	
	VMware vCenter	6.7 U1	

Layer	Device	Image	Comments
	Pure Storage vSphere Web Client Plugin	3.1.1	

Configuration Guidelines

This document details the step-by-step configuration of a fully redundant and highly available Virtual Server Infrastructure built on Cisco and Pure Storage components. References are made to which component is being configured with each step, either 01 or 02 or A and B. For example, controller-1 and controller-2 are used to identify the two controllers within the Pure Storage FlashArray//X that are provisioned with this document, and Cisco Nexus A or Cisco Nexus B identifies the pair of Cisco Nexus switches that are configured. The Cisco UCS fabric interconnects are similarly configured. Additionally, this document details the steps for provisioning multiple Cisco UCS hosts, and these examples are identified as: VM-Host-FC-01, VM-Host-FC-02 to represent Fibre Channel booted infrastructure and production hosts deployed to the fabric interconnects in this document. Finally, to indicate that you should include information pertinent to your environment in a given step, <<text>> appears as part of the command structure. See the following example during a configuration step for both Nexus switches:

```
AA12-9336C-A&B (config)# ntp server <<var_oob_ntp>> use-vrf management
```

This document is intended to enable you to fully configure the customer environment. In this process, various steps require you to insert customer-specific naming conventions, IP addresses, and VLAN schemes, as well as to record appropriate MAC addresses. Table 2 lists the VLANs necessary for deployment as outlined in this guide, and Table 3 lists the virtual machines (VMs) necessary for deployment as outlined in this guide.

Table 2 Required VLANs

VLAN Name	VLAN Purpose	ID Used in Validating this Document	Customer Deployed Value
Native	VLAN for untagged frames	2	
Out of Band Mgmt	VLAN for out-of-band management interfaces	15	
In-band Mgmt	VLAN for in-band management interfaces	215	
vMotion	VLAN for vMotion	1130	
VM-App-1301	VLAN for Production VM interfaces	1301	
VM-App-1302	VLAN for Production VM interfaces	1302	
VM-App-1303	VLAN for Production VM interfaces	1303	

Table 3 Infrastructure Servers

Server Description	Server Name Used in Validating This Document	Customer Deployed Value
vCenter Server	Pure-VC	

Server Description	Server Name Used in Validating This Document	Customer Deployed Value
Active Directory	Pure-AD	

Table 4 Configuration Variables

Variable Name	Variable Description	Customer Deployed Value
<<var_nexus_A_hostname>>	Nexus switch A Host name (Example: AA12-9336C-A)	
<<var_nexus_A_mgmt_ip>>	Out-of-band management IP for Nexus switch A (Example: 192.168.164.90)	
<<var_oob_mgmt_mask>>	Out-of-band network mask (Example: 255.255.255.0)	
<<var_oob_gateway>>	Out-of-band network gateway (Example: 192.168.164.254)	
<<var_oob_ntp>>	Out-of-band management network NTP Server (Example: 172.26.163.254)	
<<var_nexus_B_hostname>>	Nexus switch B Host name (Example: AA12-9336C-B)	
<<var_nexus_B_mgmt_ip>>	Out-of-band management IP for Nexus switch B (Example: 162.168.164.91)	
<<var_flasharray_hostname>>	Array Hostname set during setup (Example: flashstack-1)	
<<var_flasharray_vip>>	Virtual IP that will answer for the active management controller (Example: 10.2.164.45)	
<<var_contoller-1_mgmt_ip>>	Out-of-band management IP for FlashArray controller-1 (Example:10.2.164.47)	
<<var_contoller-1_mgmt_mask>>	Out-of-band management network netmask (Example: 255.255.255.0)	
<<var_contoller-1_mgmt_gateway>>	Out-of-band management network default gateway (Example: 192.168.164.254)	
<<var_contoller-2_mgmt_ip>>	Out-of-band management IP for FlashArray controller-2 (Example:10.2.164.49)	
<<var_contoller-2_mgmt_mask>>	Out-of-band management network netmask (Example: 255.255.255.0)	
<<var_ contoller-2_mgmt_gateway>>	Out-of-band management network default gateway (Example: 192.168.164.254)	
<<var_password>>	Administrative password (Example: FI@shSt4x)	

Variable Name	Variable Description	Customer Deployed Value
<<var_dns_domain_name>>	DNS domain name (Example: flashstack.cisco.com)	
<<var_nameserver_ip>>	DNS server IP(s) (Example: 10.1.164.9)	
<<var_smtp_ip>>	Email Relay Server IP Address or FQDN (Example: smtp.flashstack.cisco.com)	
<<var_smtp_domain_name>>	Email Domain Name (Example: flashstack.cisco.com)	
<<var_timezone>>	FlashStack time zone (Example: America/New_York)	
<<var_oob_mgmt_vlan_id>>	Out-of-band management network VLAN ID (Example: 15)	
<<var_ib_mgmt_vlan_id>>	In-band management network VLAN ID (Example: 215)	
<<var_ib_mgmt_vlan_netmask_length>>	Length of IB-MGMT-VLAN Netmask (Example: /24)	
<<var_ib_gateway_ip>>	In-band management network VLAN ID (Example: 10.2.164.254)	
<<var_vmotion_vlan_id>>	vMotion network VLAN ID (Example: 1130)	
<<var_vmotion_vlan_netmask_length>>	Length of vMotion VLAN Netmask (Example: /24)	
<<var_native_vlan_id>>	Native network VLAN ID (Example: 2)	
<<var_app_vlan_id>>	Example Application network VLAN ID (Example: 1301)	
<<var_snmp_contact>>	Administrator e-mail address (Example: admin@flashstack.cisco.com)	
<<var_snmp_location>>	Cluster location string (Example: RTP9-AA12)	
<<var_mds_A_mgmt_ip>>	Cisco MDS Management IP address (Example: 10.2.164.92)	
<<var_mds_A_hostname>>	Cisco MDS hostname (Example: mds-9132T-A)	
<<var_mds_B_mgmt_ip>>	Cisco MDS Management IP address (Example: 10.2.164.93)	
<<var_mds_B_hostname>>	Cisco MDS hostname (Example: mds-9132T-b)	
<<var_vsan_a_id>>	VSAN used for the A Fabric between the	

Variable Name	Variable Description	Customer Deployed Value
	FlashArray/MDS/FI (Example: 100)	
<<var_vsan_b_id>>	VSAN used for the B Fabric between the FlashArray/MDS/FI (Example: 200)	
<<var_ucs_clustername>>	Cisco UCS Manager cluster host name (Example: AA-12-ucs-6454)	
<<var_ucs_a_mgmt_ip>>	Cisco UCS fabric interconnect (FI) A out-of-band management IP address (Example: 10.2.164.51)	
<<var_ucs_mgmt_vip>>	Cisco UCS fabric interconnect (FI) Cluster out-of-band management IP address (Example: 10.2.164.50)	
<<var_ucs_b_mgmt_ip>>	Cisco UCS fabric interconnect (FI) Cluster out-of-band management IP address (Example: 10.2.164.52)	
<<var_vm_host_fc_01_ip>>	VMware ESXi host 01 in-band management IP (Example:10.2.164.73)	
<<var_vm_host_fc_vmotion_01_ip>>	VMware ESXi host 01 vMotion IP (Example: 192.168.130.73)	
<<var_vm_host_fc_02_ip>>	VMware ESXi host 02 in-band management IP (Example:10.2.164.74)	
<<var_vm_host_fc_vmotion_02_ip>>	VMware ESXi host 02 vMotion IP (Example: 192.168.130.74)	
<<var_vmotion_subnet_mask>>	vMotion subnet mask (Example: 255.255.255.0)	
<<var_vcenter_server_ip>>	IP address of the vCenter Server (Example: 10.1.164.20)	

Physical Topology

This section details a cabling example for a FlashStack environment. To explain the connectivity in this example, the tables include both the local and remote port locations.

This document assumes that out-of-band management ports are plugged into an existing management infrastructure at the deployment site. The upstream network from the Nexus 9336C-FX2 switches is out of scope of this document, with only the assumption that these switches will connect to the upstream switch or switches with a vPC.

Figure 2 shows the cabling configuration used in this FlashStack design.

Figure 2 FlashStack Cabling in the Validate Topology

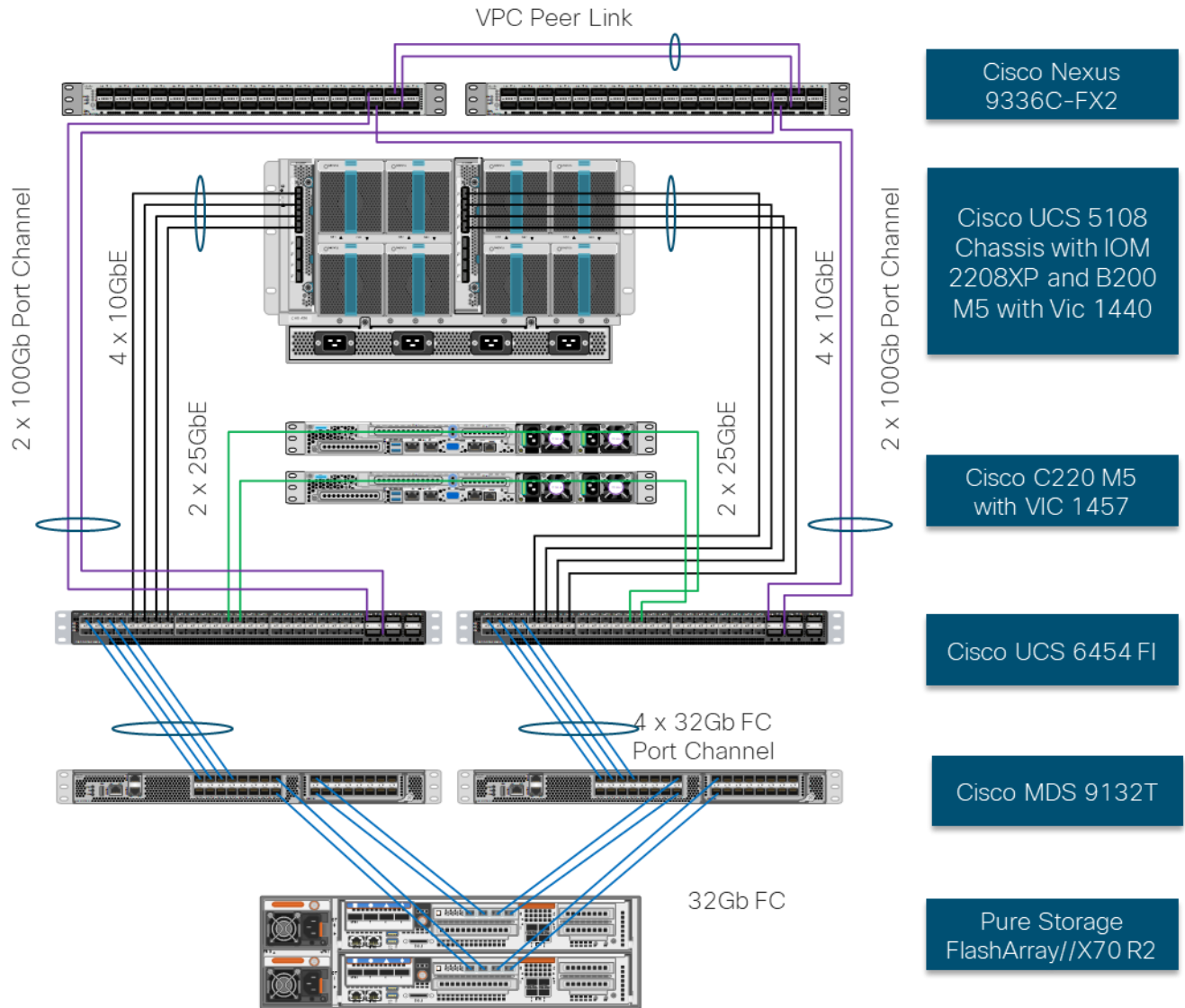


Table 5 Cisco Nexus 9336C-FX2-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote port
Cisco Nexus 9336C-FX2-A	Eth 1/31	100Gbe	Cisco UCS 6454-A	Eth 1/49
	Eth 1/32	100Gbe	Cisco UCS 6454-B	Eth 1/49
	Eth 1/33	100Gbe	Cisco Nexus 9336C-FX2-B	Eth 1/33
	Eth 1/34	100Gbe	Cisco Nexus 9336C-FX2-B	Eth 1/33
	Eth 1/35	10Gbe or 40Gbe or 100Gbe	Upstream Network Switch	Any

Local Device	Local Port	Connection	Remote Device	Remote port
	Eth 1/36	10Gbe or 40Gbe or 100Gbe	Upstream Network Switch	Any
	Mgmt0	Gbe	Gbe Management Switch	Any

Table 6 Cisco Nexus 9336C-FX2-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote port
Cisco Nexus 9336C-FX2-B	Eth 1/31	100Gbe	Cisco UCS 6454-A	Eth 1/50
	Eth 1/32	100Gbe	Cisco UCS 6454-B	Eth 1/50
	Eth 1/33	100Gbe	Cisco Nexus 9336C-FX2-A	Eth 1/33
	Eth 1/34	100Gbe	Cisco Nexus 9336C-FX2-A	Eth 1/33
	Eth 1/35	10Gbe or 40Gbe or 100Gbe	Upstream Network Switch	Any
	Eth 1/36	10Gbe or 40Gbe or 100Gbe	Upstream Network Switch	Any
	Mgmt0	Gbe	Gbe Management Switch	Any

Table 7 Cisco UCS-6545-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote port
Cisco UCS-6454-A	Eth 1/49	100Gbe	Cisco Nexus 9336C-FX2-A	Eth 1/31
	Eth 1/50	100Gbe	Cisco Nexus 9336C-FX2-B	Eth 1/31
	Eth 1/9	10Gbe	Cisco UCS Chassis 1 2208 FEX A	IOM 1/1
	Eth 1/10	10Gbe	Cisco UCS Chassis 1 2208 FEX A	IOM 1/2
	Eth 1/11	10Gbe	Cisco UCS Chassis 1 2208 FEX A	IOM 1/3
	Eth 1/12	10Gbe	Cisco UCS Chassis 1 2208 FEX A	IOM 1/4
	Eth 1/17	25Gbe	Cisco UCS C220-01	Eth 1
	Eth 1/18	25Gbe	Cisco UCS C220-01	Eth 2

Local Device	Local Port	Connection	Remote Device	Remote port
	Eth 1/19	25Gbe	Cisco UCS C220-02	Eth 1
	Eth 1/20	25Gbe	Cisco UCS C220-02	Eth 2
	FC1/1	32G FC	Cisco MDS 9132T-A	FC1/1
	FC1/2	32G FC	Cisco MDS 9132T-A	FC1/2
	FC1/3	32G FC	Cisco MDS 9132T-A	FC1/3
	FC1/4	32G FC	Cisco MDS 9132T-A	FC1/4
	Mgmt0	Gbe	Gbe Management Switch	Any

Table 8 Cisco UCS-6454-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote port
Cisco UCS-6454-B	Eth 1/49	100Gbe	Cisco Nexus 9336C-FX2-A	Eth 1/32
	Eth 1/50	100Gbe	Cisco Nexus 9336C-FX2-B	Eth 1/32
	Eth 1/9	10Gbe	Cisco UCS Chassis 1 2208 FEX B	IOM 1/1
	Eth 1/10	10Gbe	Cisco UCS Chassis 1 2208 FEX B	IOM 1/2
	Eth 1/11	10Gbe	Cisco UCS Chassis 1 2208 FEX B	IOM 1/3
	Eth 1/12	10Gbe	Cisco UCS Chassis 1 2208 FEX B	IOM 1/4
	Eth 1/17	25Gbe	Cisco UCS C220-01	Eth 3
	Eth 1/18	25Gbe	Cisco UCS C220-01	Eth 4
	Eth 1/19	25Gbe	Cisco UCS C220-02	Eth 3
	Eth 1/20	25Gbe	Cisco UCS C220-02	Eth 4
	FC1/1	32G FC	Cisco MDS 9132T-B	FC1/1
	FC1/2	32G FC	Cisco MDS 9132T-B	FC1/2

Local Device	Local Port	Connection	Remote Device	Remote port
	FC1/3	32G FC	Cisco MDS 9132T-B	FC1/3
	FC1/4	32G FC	Cisco MDS 9132T-B	FC1/4
	Mgmt0	Gbe	Gbe Management Switch	Any

Table 9 Cisco MDS-9132T-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote port
Cisco MDS-9132T-A	FC1/1	32Gb FC	Cisco UCS 6454-A	FC1/1
	FC1/2	32Gb FC	Cisco UCS 6454-A	FC1/2
	FC 1/3	32Gb FC	Cisco UCS 6454-A	FC1/3
	FC 1/4	32Gb FC	Cisco UCS 6454-A	FC1/4
	FC1/15	32Gb FC	FlashArray//X70 R2 Controller 1	CT0.FC0
	FC1/16	32Gb FC	FlashArray//X70 R2 Controller 1	CT0.FC2
	FC1/17	32Gb FC	FlashArray//X70 R2 Controller 2	CT1.FC0
	FC1/18	32Gb FC	FlashArray//X70 R2 Controller 2	CT1.FC2
	Mgmt0	Gbe	Gbe Management Switch	Any

Table 10 Cisco MDS-9132T-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote port
Cisco MDS-9132T-B	FC1/1	32Gb FC	Cisco UCS 6454-B	FC1/1
	FC1/2	32Gb FC	Cisco UCS 6454-B	FC1/2
	FC 1/3	32Gb FC	Cisco UCS 6454-B	FC1/3
	FC 1/4	32Gb FC	Cisco UCS 6454-B	FC1/4
	FC1/15	32Gb FC	FlashArray//X70 R2 Controller 1	CT0.FC1
	FC1/16	32Gb FC	FlashArray//X70 R2 Controller 1	CT0.FC3

Local Device	Local Port	Connection	Remote Device	Remote port
	FC1/17	32Gb FC	FlashArray//X70 R2 Controller 2	CT1.FC1
	FC1/18	32Gb FC	FlashArray//X70 R2 Controller 2	CT1.FC3
	Mgmt0	Gbe	Gbe Management Switch	Any

Table 11 Pure Storage FlashArray//X70 R2 Controller 1 Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote port
FlashArray//X70 R2 Controller 1	CT0.FC0	32Gb FC	Cisco MDS 9132T-A	FC 1/15
	CT0.FC1	32Gb FC	Cisco MDS 9132T-B	FC 1/15
	CT0.FC2	32Gb FC	Cisco MDS 9132T-A	FC 1/16
	CT0.FC3	32Gb FC	Cisco MDS 9132T-B	FC 1/16
	Eth0	Gbe	Gbe Management Switch	Any

Table 12 Pure Storage FlashArray//X70 R2 Controller 2 Cabling Information

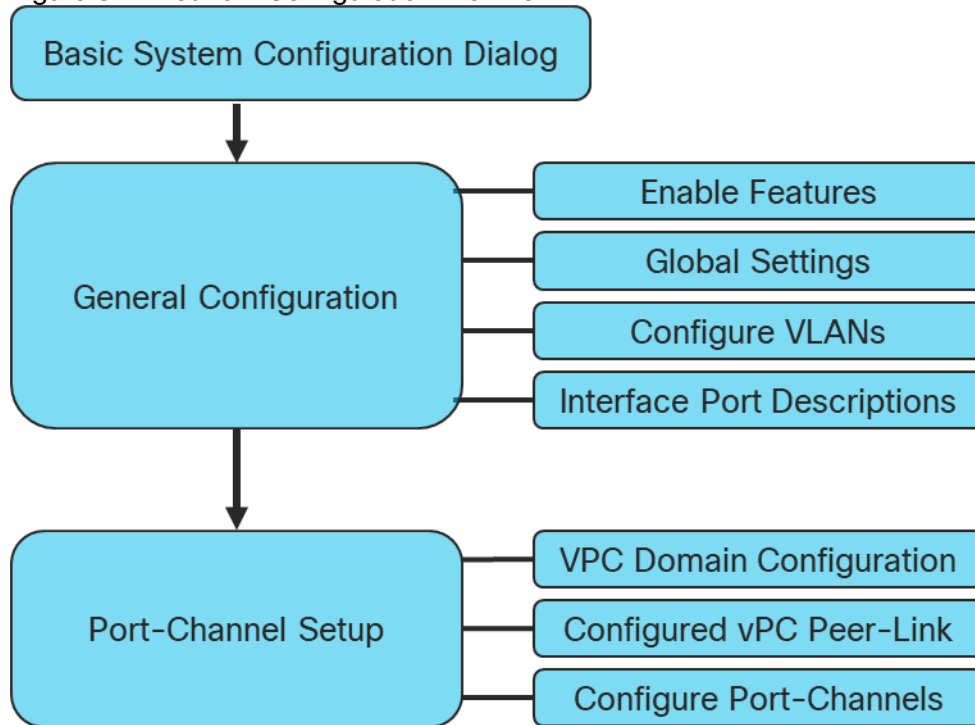
Local Device	Local Port	Connection	Remote Device	Remote port
FlashArray//X70 R2 Controller 2	CT1.FC0	32Gb FC	Cisco MDS 9132T-A	FC 1/17
	CT1.FC1	32Gb FC	Cisco MDS 9132T-B	FC 1/17
	CT1.FC2	32Gb FC	Cisco MDS 9132T-A	FC 1/18
	CT1.FC3	32Gb FC	Cisco MDS 9132T-B	FC 1/18
	Eth0	Gbe	Gbe Management Switch	Any

Network Switch Configuration

Network Configuration

The following procedures describe how to configure the Cisco Nexus switches for use in a base FlashStack environment. This procedure assumes the use of Nexus 9336C-FX2 switches running 7.0(3)I7(5). Configuration on a differing model of Nexus 9000 series switch should be comparable but may differ slightly with model and changes in NX-OS release. The Cisco Nexus 9336C-FX2 switch and NX-OS 7.0(3)I7(5) release were used in validation of this FlashStack solution, so the instructions will reflect this model and release.

Figure 3 Network Configuration Workflow



Physical Connectivity

Physical cabling should be completed by following the diagram and table references in the previous section referenced as FlashStack Cabling.

Cisco Nexus Basic System Configuration Dialog

This section provides detailed instructions for the configuration of the Cisco Nexus 9336C-FX2 switches used in this FlashStack solution. Some changes may be appropriate for a customer’s environment, but care should be taken when stepping outside of these instructions as it may lead to an improper configuration.

Cisco Nexus Basic System Configuration Dialog

```

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]: yes

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): yes

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

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

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

Enter the switch name : <<var_nexus_A_hostname>>

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

Mgmt0 IPv4 address : <<var_nexus_A_mgmt_ip>>

Mgmt0 IPv4 netmask : <<var_oob_mgmt_mask>>

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

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

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

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

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

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

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

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

NTP server IPv4 address : <<var_oob_ntp>>

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

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

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

The following configuration will be applied:

```
password strength-check
switchname AA12-9336C-A
vrf context management
ip route 0.0.0.0/0 192.168.164.254
exit
```



```

no feature telnet

ssh key rsa 2048 force

feature ssh

ntp server 172.26.163.254

system default switchport

no system default switchport shutdown

copp profile strict

interface mgmt0

ip address 192.168.164.90 255.255.252.0

no shutdown

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

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

```

Cisco Nexus Switch Configuration

Enable Features and Settings

To enable IP switching features, run the following commands on each Cisco Nexus:

```

AA12-9336C-A&B (config)# feature lacp

AA12-9336C-A&B (config)# feature vpc

AA12-9336C-A&B (config)# feature interface-vlan

```



The feature interface-vlan is an optional requirement if configuring an In-Band VLAN interface to redistribute NTP. Layer-3 routing is possible with Nexus switches after setting this feature but is not covered in this architecture.

Additionally, configure spanning tree and save the running configuration to start-up:

```

AA12-9336C-A&B (config)# spanning-tree port type network default

AA12-9336C-A&B (config)# spanning-tree port type edge bpduguard default

AA12-9336C-A&B (config)# spanning-tree port type edge bpdufilter default

```

Configure Global Settings

Run the following commands on both switches to set global configurations:

```

AA12-9336C-A&B (config)# port-channel load-balance src-dst l4port

AA12-9336C-A&B (config)# ip route 0.0.0.0/0 <<var_ib-mgmt-vlan_gateway>>

AA12-9336C-A&B (config)# ntp server <<var_oob_ntp>> use-vrf management

```

```
AA12-9336C-A&B (config)# ntp master 3
```

Configure VLANs

Run the following commands on both switches to create VLANs:

```
AA12-9336C-A&B (config)# vlan <<var_ib-mgmt_vlan_id>>
AA12-9336C-A&B (config-vlan)# name IB-MGMT-VLAN
AA12-9336C-A&B (config-vlan)# vlan <<var_native_vlan_id>>
AA12-9336C-A&B (config-vlan)# name Native-VLAN
AA12-9336C-A&B (config-vlan)# vlan <<var_vmotion_vlan_id>>
AA12-9336C-A&B (config-vlan)# name vMotion-VLAN
AA12-9336C-A&B (config-vlan)# vlan <<var_application_vlan_id>>
AA12-9336C-A&B (config-vlan)# name VM-App1-VLAN
```

Continue adding VLANs as appropriate to the customer's environment.

Add Interface Port Descriptions

To add individual port descriptions for troubleshooting activity and verification for switch A, enter the following commands from the global configuration mode:

```
AA12-9336C-A(config-if)# interface Ethernet1/31
AA12-9336C-A(config-if)# description AA12-UCS-6454-A-Eth1/53
AA12-9336C-A(config-if)# interface Ethernet1/32
AA12-9336C-A(config-if)# description AA12-UCS-6454-B-Eth1/53
AA12-9336C-A(config-if)# interface Ethernet1/33
AA12-9336C-A(config-if)# description AA12-9336C-B-Eth1/33 Peer Link
AA12-9336C-A(config-if)# interface Ethernet1/34
AA12-9336C-A(config-if)# description AA12-9336C-B-Eth1/34 Peer Link
AA12-9336C-A(config-if)# interface Ethernet1/35
AA12-9336C-A(config-if)# description Network-Uplink-A
AA12-9336C-A(config-if)# interface Ethernet1/36
AA12-9336C-A(config-if)# description Network-Uplink-B
```

To add individual port descriptions for troubleshooting activity and verification for switch B, enter the following commands from the global configuration mode:

```
AA12-9336C-B(config-if)# interface Ethernet1/31
AA12-9336C-B(config-if)# description AA12-UCS-6454-A-Eth1/54
AA12-9336C-B(config-if)# interface Ethernet1/32
AA12-9336C-B(config-if)# description AA12-UCS-6454-B-Eth1/54
AA12-9336C-B(config-if)# interface Ethernet1/33
```

```

AA12-9336C-B(config-if)# description AA12-9336C-A-Eth1/33 Peer Link
AA12-9336C-B(config-if)# interface Ethernet1/34
AA12-9336C-B(config-if)# description AA12-9336C-A-Eth1/34 Peer Link
AA12-9336C-B(config-if)# interface Ethernet1/35
AA12-9336C-B(config-if)# description Network-Uplink-A
AA12-9336C-B(config-if)# interface Ethernet1/36
AA12-9336C-B(config-if)# description Network-Uplink-B

```

Configure vPC Domain Settings

The vPC domain will be assigned a unique number from 1-1000 and will handle the vPC settings specified within the switches. To set the vPC domain configuration on 9336C-A, run the following commands:

```

AA12-9336C-A(config)# vpc domain 10
AA12-9336C-A(config-vpc-domain)# peer-switch
AA12-9336C-A(config-vpc-domain)# role priority 10
AA12-9336C-A(config-vpc-domain)# peer-keepalive
destination <<var_nexus_B_mgmt_ip>> source <<var_nexus_A_mgmt_ip>>
AA12-9336C-A(config-vpc-domain)# delay restore 150
AA12-9336C-A(config-vpc-domain)# peer-gateway
AA12-9336C-A(config-vpc-domain)# auto-recovery
AA12-9336C-A(config-vpc-domain)# ip arp synchronize

```

To set the vPC domain configuration on 9336C-B, run the following commands:

```

AA12-9336C-B(config)# vpc domain 10
AA12-9336C-B(config-vpc-domain)# peer-switch
AA12-9336C-B(config-vpc-domain)# role priority 20
AA12-9336C-B(config-vpc-domain)# peer-keepalive
destination <<var_nexus_A_mgmt_ip>> source <<var_nexus_B_mgmt_ip>>
AA12-9336C-B(config-vpc-domain)# delay restore 150
AA12-9336C-B(config-vpc-domain)# peer-gateway
AA12-9336C-B(config-vpc-domain)# auto-recovery
AA12-9336C-B(config-vpc-domain)# ip arp synchronize

```

Configure vPC Peer-Link

On each switch, configure the Port Channel member interfaces that will be part of the vPC Peer Link and configure the vPC Peer Link:

```

AA12-9336C-A&B (config)# int eth 1/33-34
AA12-9336C-A&B (config-if-range)# switchport mode trunk
AA12-9336C-A&B (config-if-range)# switchport trunk native vlan 2

```

```

AA12-9336C-A&B (config-if-range)# switchport trunk allowed vlan 215,1110,1120,1130,1301-1303
AA12-9336C-A&B (config-if-range)# channel-group 133 mode active
AA12-9336C-A&B (config-if-range)# no shut
AA12-9336C-A&B (config-if-range)# int port-channel 133
AA12-9336C-A&B (config-if)# description AA12-9336C Peer Link
AA12-9336C-A&B (config-if)# vpc peer-link

```

Configure Port-Channels

On each switch, configure the Port Channel member interfaces and the vPC Port Channels to the Cisco UCS Fabric Interconnect and the upstream network switches:

Nexus Connection vPC to UCS Fabric Interconnect A

```

AA12-9336C-A&B (config)# int eth 1/31
AA12-9336C-A&B (config-if)# switchport mode trunk
AA12-9336C-A&B (config-if)# switchport trunk native vlan 2
AA12-9336C-A&B (config-if)# switchport trunk allowed vlan 215,1110,1120,1130,1301-1303
AA12-9336C-A&B (config-if)# channel-group 131 mode active
AA12-9336C-A&B (config-if)# no shut
AA12-9336C-A&B (config-if)# int port-channel 131
AA12-9336C-A&B (config-if)# description AA12-UCS-6454-A
AA12-9336C-A&B (config-if)# vpc 131

```

Nexus Connection vPC to UCS Fabric Interconnect B

```

AA12-9336C-A&B (config)# int eth 1/32
AA12-9336C-A&B (config-if)# switchport mode trunk
AA12-9336C-A&B (config-if)# switchport trunk native vlan 2
AA12-9336C-A&B (config-if)# switchport trunk allowed vlan 215,1110,1120,1130,1301-1303
AA12-9336C-A&B (config-if)# channel-group 132 mode active
AA12-9336C-A&B (config-if)# no shut
AA12-9336C-A&B (config-if)# int port-channel 132
AA12-9336C-A&B (config-if)# description AA12-UCS-6454-B
AA12-9336C-A&B (config-if)# vpc 132

```

Nexus Connection vPC to Upstream Network

```

AA12-9336C-A&B (config)# int eth 1/35-36
AA12-9336C-A&B (config-if-range)# switchport mode trunk
AA12-9336C-A&B (config-if-range)# switchport trunk native vlan 2
AA12-9336C-A&B (config-if-range)# switchport trunk allowed vlan 215,1110,1120,1130,1301-1303
AA12-9336C-A&B (config-if-range)# channel-group 135 mode active

```

```
AA12-9336C-A&B (config-if-range)# no shut
AA12-9336C-A&B (config-if-range)# int port-channel 135
AA12-9336C-A&B (config-if)# description Uplink
AA12-9336C-A&B (config-if)# vpc 135
```

Storage Configuration

Pure Storage FlashArray//X70 R2 Configuration

FlashArray Initial Configuration

The information in Table 13 should be gathered to enable the installation and configuration of the FlashArray. An official representative of Pure Storage will help rack and configure the new installation of the FlashArray.

Table 13 FlashArray Setup Information

Global Array Settings Heading Title	
Array Name (Hostname for Pure Array):	<<var_flasharray_hostname>>
Virtual IP Address for Management:	<<var_flasharray_vip>>
Physical IP Address for Management on Controller 0 (CT0):	<<var_contoller-1_mgmt_ip>>
Physical IP Address for Management on Controller 1 (CT1):	<<var_contoller-2_mgmt_ip>>
Netmask:	<<var_contoller-1_mgmt_mask>>
Gateway IP Address:	<<var_contoller-1_mgmt_gateway>>
DNS Server IP Address(es):	<<var_nameserver_ip>>
DNS Domain Suffix: (Optional)	<<var_dns_domain_name>>
NTP Server IP Address or FQDN:	<<var_oob_ntp>>
Email Relay Server (SMTP Gateway IP address or FQDN): (Optional)	<<var_smtp_ip>>
Email Domain Name:	<<var_smtp_domain_name>>
Alert Email Recipients Address(es): (Optional)	
HTTP Proxy Server ad Port (For Pure1): (Optional)	
Time Zone:	<<var_timezone>>

When the FlashArray has completed initial configuration, it is important to configure the Cloud Assist phone-home connection to provide the best pro-active support experience possible. Furthermore, this will enable the analytics functionalities provided by Pure1.

Add an Alert Recipient

The Alerts sub-view is used to manage the list of addresses to which Purity delivers alert notifications, and the attributes of alert message delivery. The Alert Recipients section displays a list of email addresses that are designated to receive Purity alert messages. Up to 20 alert recipients can be designated.



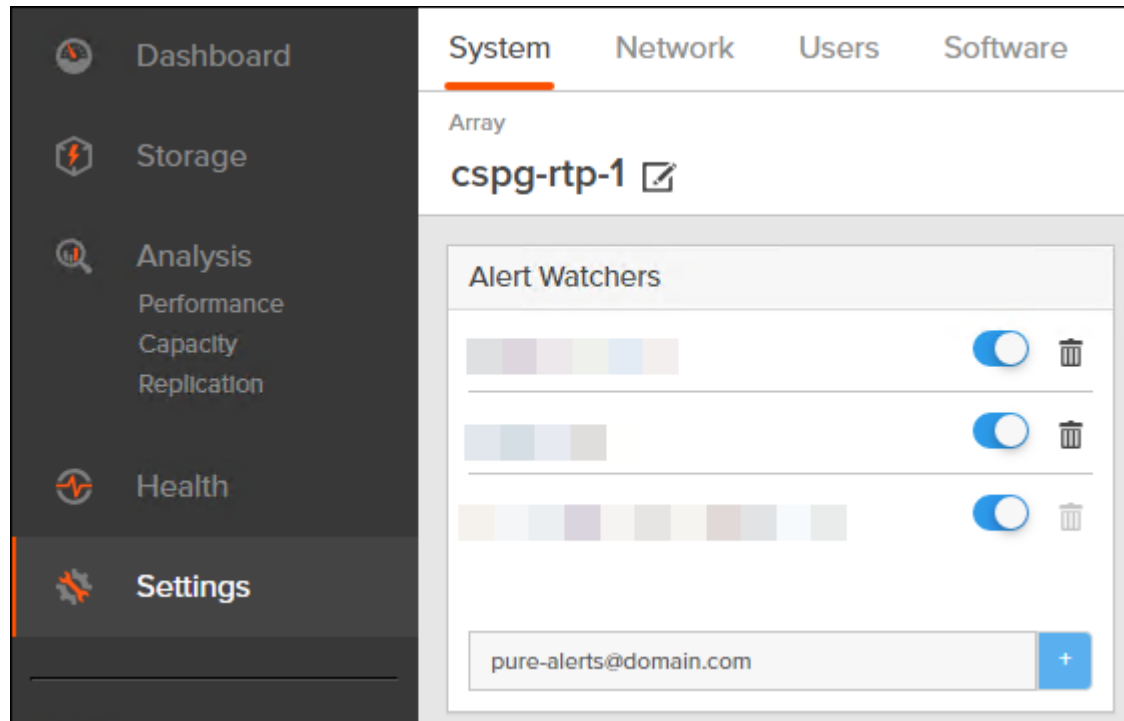
The list includes the built-in flasharray-alerts@purestorage.com address, which cannot be deleted.

The email address that Purity uses to send alert messages includes the sender domain name and is comprised of the following components:

<Array_Name>-<Controller_Name>@<Sender_Domain_Name>.com

To add an alert recipient, follow these steps:


1. Select Settings
2. In the Alert Watchers section, enter the email address of the alert recipient and click the + icon.



The Relay Host section displays the hostname or IP address of an SMTP relay host, if one is configured for the array. If you specify a relay host, Purity routes the email messages via the relay (mail forwarding) address rather than sending them directly to the alert recipient addresses.

In the Sender Domain section, the sender domain determines how Purity logs are parsed and treated by Pure Storage Support and Escalations. By default, the sender domain is set to the domain name please-configure.me.

It is crucial that you set the sender domain to the correct domain name. If the array is not a Pure Storage test array, set the sender domain to the actual customer domain name. For example, mycompany.com.

Alert Routing 

Relay Host
No relay host configured

Username
No username available

Password
No password available

Sender Domain
cisco.com

Configure Pure1 Support

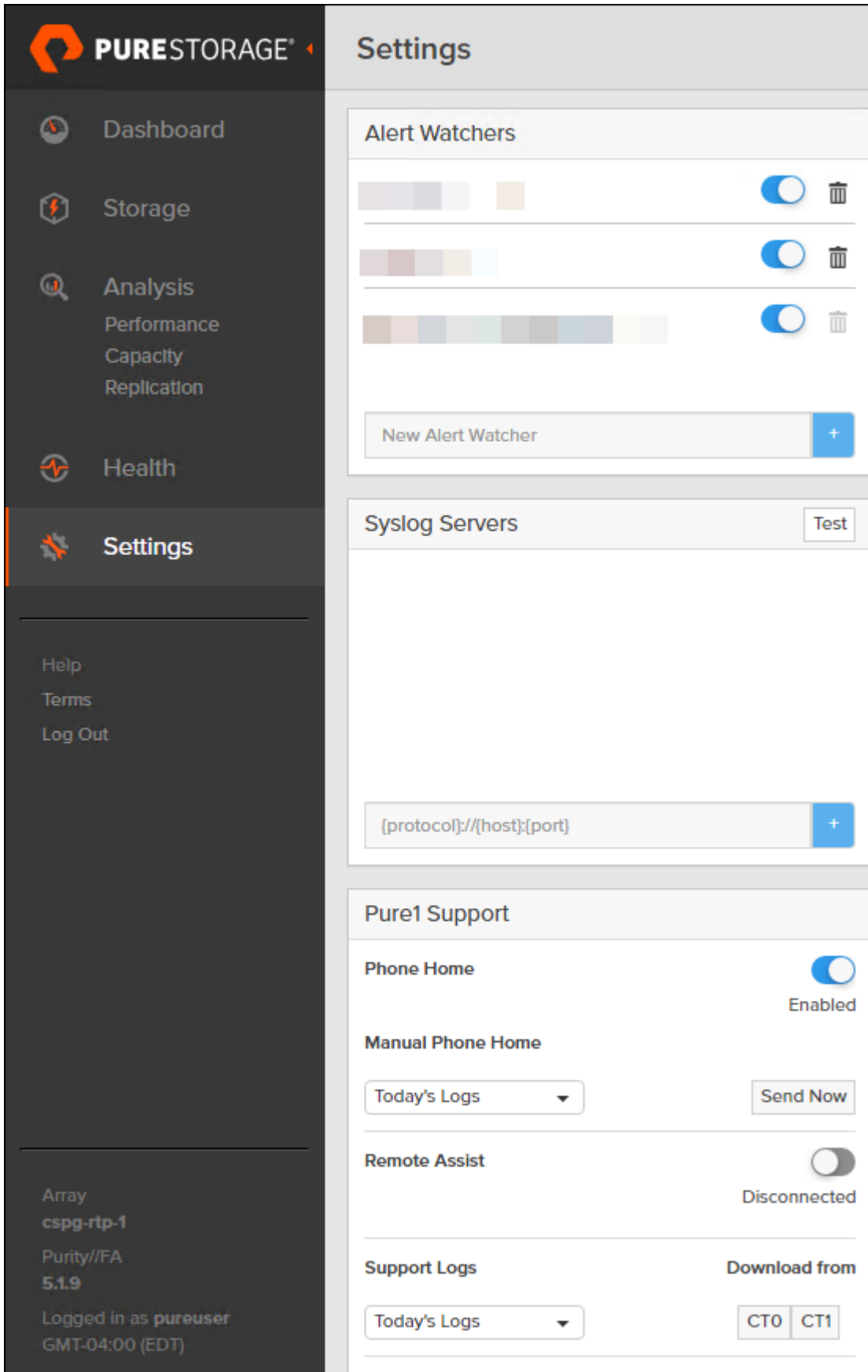
The Pure1 Support section manages the phone home facility. The phone home facility provides a secure direct link between the array and the Pure Storage Technical Support web site. The link is used to transmit log contents and alert messages to the Pure Storage Support team so that when diagnosis or remedial action is required, complete recent history about array performance and significant events is available.

The Remote Assist section displays the remote assist status as "Connected" or "Disconnected." By default, remote assist is disconnected. A connected remote assist status means that a remote assist session has been opened, allowing Pure Storage Support to connect to the array. Disconnect the remote assist session to close the session.

By default, the phone home facility is enabled. If the phone home facility is enabled to send information automatically, Purity transmits log and alert information directly to Pure Storage Support via a secure network connection. Log contents are transmitted hourly and stored at the support web site, enabling detection of array performance and error rate trends. Alerts are reported immediately when they occur so that timely action can be taken.

Phone home logs can also be sent to Pure Storage Technical support on demand, with options including Today's Logs, Yesterday's Logs, or All Log History.

The Support Logs section allows you to download the Purity log contents of the specified controller to the current administrative workstation. Purity continuously logs a variety of array activities, including performance summaries, hardware and operating status reports, and administrative actions.



PURESTORAGE

Settings

Dashboard

Storage

Analysis
Performance
Capacity
Replication

Health

Settings

Help

Terms

Log Out

Array
cspg-rtp-1

Purity//FA
5.1.9

Logged in as pureuser
GMT-04:00 (EDT)

Alert Watchers

[Color bars]

[Color bars]

[Color bars]

New Alert Watcher

Syslog Servers

[protocol]://[host]:[port]

Pure1 Support

Phone Home Enabled

Manual Phone Home

Today's Logs

Remote Assist Disconnected

Support Logs **Download from**

Today's Logs

Configure the Domain Name System (DNS) Server IP Addresses

To configure the DNS server IP addresses, follow these steps:

1. Select Settings > Network.
2. In the DNS section, hover over the domain name and click the pencil icon. The Edit DNS dialog box appears.

The screenshot shows the Pure Storage Settings interface. The left sidebar contains navigation options: Dashboard, Storage, Analysis (Performance, Capacity, Replication), Health, Settings (highlighted), Help, Terms, and Log Out. The main content area is titled 'Settings' and has tabs for System, Network (selected), Users, and Software. Under the Network tab, there is a 'Subnets & Interfaces' table and a 'DNS Settings' dialog box.

Subnet	VLAN	Gateway
-		192.168.101.253
-		192.168.102.253
-		10.2.164.254
-		10.2.164.254
-		10.10.164.254
-		10.10.164.254
-		
-		

DNS Settings ✎

Domain
flashstack.cisco.com

DNS Server(s)
10.1.164.9

3. Complete the following fields:

- a. Domain: Specify the domain suffix to be appended by the array when doing DNS lookups.
- b. NS#: Specify up to three DNS server IP addresses for Purity to use to resolve hostnames to IP addresses. Enter one IP address in each DNS# field. Purity queries the DNS servers in the order that the IP addresses are listed.

4. Click Save.

Directory Service Sub-view

The Directory Service sub-view manages the integration of FlashArray with an existing directory service. When the Directory Service sub-view is configured and enabled, the FlashArray leverages a directory service to perform user account and permission level searches. Configuring directory services is OPTIONAL.

The screenshot shows the FlashArray web interface with the 'Users' tab selected. The 'Users' panel displays a table with the following data:

Name	Role	Type	Public Key	API Token
pureuser	array_admin	local	****	****
root		local		****

Below the table is the 'Directory Service' configuration panel, which includes the following settings:


- Enabled: False
- URI: -
- Base DN: -
- Bind User: -
- Bind Password: -
- Group Base: -
- Array Admin Group: -
- Storage Admin Group: -
- Read-only Group: -
- Check Peer: False
- CA Certificate: - Edit

The FlashArray is delivered with a single local user, named pureuser, with array-wide (Array Admin) permissions.

To support multiple FlashArray users, integrate the array with a directory service, such as Microsoft Active Directory or OpenLDAP.

Role-based access control is achieved by configuring groups in the directory that correspond to the following permission groups (roles) on the array:

- Read Only Group. Read Only users have read-only privilege to run commands that convey the state of the array. Read Only users cannot alter the state of the array.
- Storage Admin Group. Storage Admin users have all the privileges of Read Only users, plus the ability to run commands related to storage operations, such as administering volumes, hosts, and host groups. Storage Admin users cannot perform operations that deal with global and system configurations.
- Array Admin Group. Array Admin users have all the privileges of Storage Admin users, plus the ability to perform array-wide changes. In other words, Array Admin users can perform all FlashArray operations.

1. Select Settings > Users.
2. Select the  icon in the Directory Services panel:
 - a. Enabled: Select the check box to leverage the directory service to perform user account and permission level searches.
 - b. URI: Enter the comma-separated list of up to 30 URIs of the directory servers. The URI must include a URL scheme (ldap, or ldaps for LDAP over SSL), the hostname, and the domain. You can optionally specify a port. For example, ldap://ad.company.com configures the directory service with the hostname "ad" in the domain "company.com" while specifying the unencrypted LDAP protocol.

- c. Base DN: Enter the base distinguished name (DN) of the directory service. The Base DN is built from the domain and should consist only of domain components (DCs). For example, for `ldap://ad.storage.company.com`, the Base DN would be: `"DC=storage,DC=company,DC=com"`
 - d. Bind User: Username used to bind to and query the directory. For Active Directory, enter the username - often referred to as `sAMAccountName` or User Logon Name - of the account that is used to perform directory lookups. The username cannot contain the characters `" [] ; | = + * ? < > / \` and cannot exceed 20 characters in length. For OpenLDAP, enter the full DN of the user. For example, `"CN=John,OU=Users,DC=example,DC=com"`.
 - e. Bind Password: Enter the password for the bind user account.
 - f. Group Base: Enter the organizational unit (OU) to the configured groups in the directory tree. The Group Base consists of OUs that, when combined with the base DN attribute and the configured group CNs, complete the full Distinguished Name of each groups. The group base should specify `"OU="` for each OU and multiple OUs should be separated by commas. The order of OUs should get larger in scope from left to right. In the following example, `SANManagers` contains the sub-organizational unit `PureGroups`: `"OU=PureGroups,OU=SANManagers"`.
 - g. Array Admin Group: Common Name (CN) of the directory service group containing administrators with full privileges to manage the FlashArray. Array Admin Group administrators have the same privileges as `pureuser`. The name should be the Common Name of the group without the `"CN="` specifier. If the configured groups are not in the same OU, also specify the OU. For example, `"pureadmins,OU=PureStorage"`, where `pureadmins` is the common name of the directory service group.
 - h. Storage Admin Group: Common Name (CN) of the configured directory service group containing administrators with storage related privileges on the FlashArray. The name should be the Common Name of the group without the `"CN="` specifier. If the configured groups are not in the same OU, also specify the OU. For example, `"pureusers,OU=PureStorage"`, where `pureusers` is the common name of the directory service group.
 - i. Read Only Group: Common Name (CN) of the configured directory service group containing users with read-only privileges on the FlashArray. The name should be the Common Name of the group without the `"CN="` specifier. If the configured groups are not in the same OU, also specify the OU. For example, `"purereadonly,OU=PureStorage"`, where `purereadonly` is the common name of the directory service group.
 - j. Check Peer: Select the check box to validate the authenticity of the directory servers using the CA Certificate. If you enable Check Peer, you must provide a CA Certificate.
 - k. CA Certificate: Enter the certificate of the issuing certificate authority. Only one certificate can be configured at a time, so the same certificate authority should be the issuer of all directory server certificates. The certificate must be PEM formatted (Base64 encoded) and include the `"-----BEGIN CERTIFICATE-----"` and `"-----END CERTIFICATE-----"` lines. The certificate cannot exceed 3000 characters in total length.
3. Click Save.
 4. Click Test to test the configuration settings. The LDAP Test Results pop-up window appears. Green squares represent successful checks. Red squares represent failed checks.

SSL Certificate Sub-view

Purity creates a self-signed certificate and private key when you start the system for the first time. The SSL Certificate sub-view allows you to view and change certificate attributes, create a new self-signed certificate, construct certificate signing requests, import certificates and private keys, and export certificates.

Creating a self-signed certificate replaces the current certificate. When you create a self-signed certificate, include any attribute changes, specify the validity period of the new certificate, and optionally generate a new private key.

SSL Certificate	
Status	self-signed
Key Size	2048
Issued To	
Issued By	
Valid From	2018-04-03 16:05:40
Valid To	2028-03-31 15:05:40
State/Province	
Locality	
Organization	Pure Storage, Inc.
Organizational Unit	Pure Storage, Inc.
Email	

When you create the self-signed certificate, you can generate a private key and specify a different key size. If you do not generate a private key, the new certificate uses the existing key.

You can change the validity period of the new self-signed certificate. By default, self-signed certificates are valid for 3650 days

CA-Sign Certificate

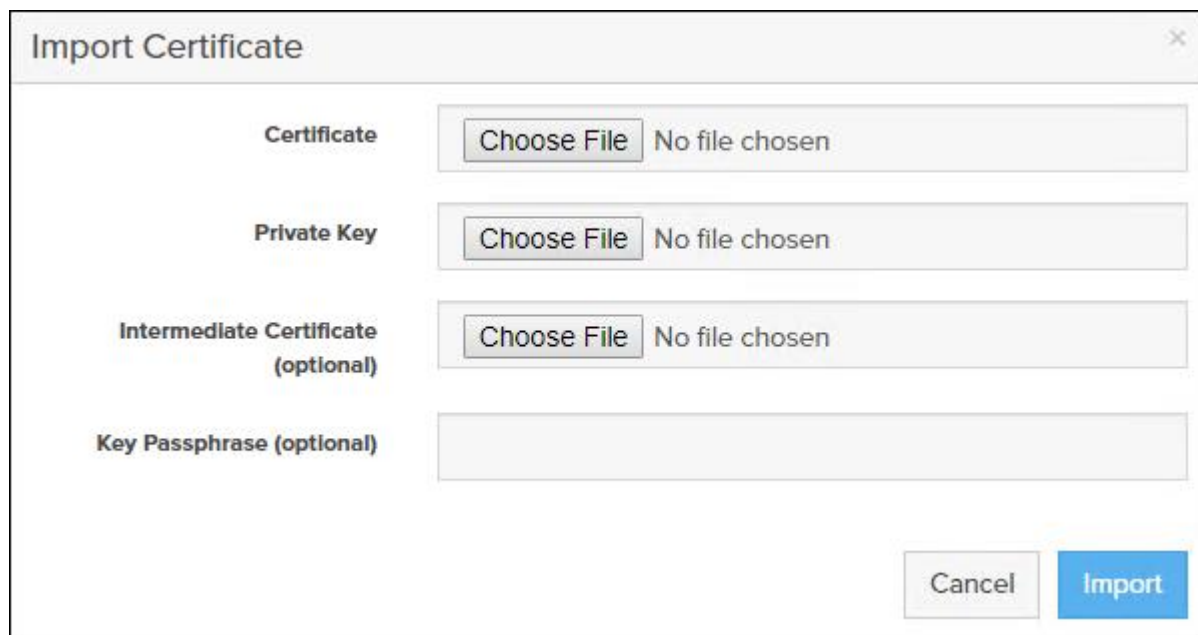
Certificate authorities (CA) are third party entities outside the organization that issue certificates. To obtain a CA certificate, you must first construct a certificate signing request (CSR) on the array.

Construct Certificate Signing Request ×

Country	<input style="width: 80%;" type="text" value="Two-letter ISO country code"/>
State/Province	<input style="width: 80%;" type="text" value="State, province, country or region"/>
Locality	<input style="width: 80%;" type="text" value="Full city name"/>
Organization	<input style="width: 80%;" type="text" value="Pure Storage, Inc."/>
Organization Unit	<input style="width: 80%;" type="text" value="Pure Storage, Inc."/>
Common Name	<input style="width: 80%;" type="text" value="FQDN or management IP address of the server"/>
Email	<input style="width: 80%;" type="text" value="Email address"/>

The CSR represents a block of encrypted data specific to your organization. You can change the certificate attributes when you construct the CSR; otherwise, Purity will reuse the attributes of the current certificate (self-signed or imported) to construct the new one. Note that the certificate attribute changes will only be visible after you import the signed certificate from the CA.

Send the CSR to a certificate authority for signing. The certificate authority returns the SSL certificate for you to import. Verify that the signed certificate is PEM formatted (Base64 encoded), includes the "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines, and does not exceed 3000 characters in total length. When you import the certificate, also import the intermediate certificate if it is not bundled with the CA certificate.



The image shows a dialog box titled "Import Certificate" with a close button (X) in the top right corner. It contains four input fields:

- Certificate:** A file selection field with a "Choose File" button and the text "No file chosen".
- Private Key:** A file selection field with a "Choose File" button and the text "No file chosen".
- Intermediate Certificate (optional):** A file selection field with a "Choose File" button and the text "No file chosen".
- Key Passphrase (optional):** A text input field.

At the bottom right of the dialog, there are two buttons: "Cancel" and "Import".

If the certificate is signed with the CSR that was constructed on the current array and you did not change the private key, you do not need to import the key. However, if the CSR was not constructed on the current array or if the private key has changed since you constructed the CSR, you must import the private key. If the private key is encrypted, also specify the passphrase.

MDS Fabric Configuration

This section provides detailed instructions for the configuration of the Cisco MDS 9132T Multilayer Fabric Switches used in this FlashStack solution. Some changes may be appropriate for a customer's environment, but use caution; if you don't follow the instructions as written it may lead to an improper configuration.

Physical Connectivity

Physical cabling should be completed by following the diagram and table references in the previous section referenced as FlashStack Cabling.

Cisco MDS Basic System Configuration Dialog

This section provides detailed instructions for the configuration of the Cisco MDS 9132T switches used in this FlashStack solution. Some changes may be appropriate for a customer's environment, but care should be taken when stepping outside of these instructions as it may lead to an improper configuration.

Cisco MDS Basic System Configuration Dialog

Set up the initial configuration for the Cisco MDS A switch on <<var_mds_A_hostname>>, by following the dialogue steps:

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

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

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

```
----- Basic System Configuration Dialog -----
```

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

```
Please register Cisco MDS 9000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. MDS devices must be registered to receive entitled
support services.
```

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

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

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

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

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

Enter the switch name : <<var_mds_A_mgmt_hostname>>

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

Mgmt0 IPv4 address : <<var_mds_A_mgmt_ip>>

Mgmt0 IPv4 netmask : <<var_oob_mgmt_mask>>

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

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

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

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

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

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

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

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

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

Enter milliseconds in multiples of 10 for congestion-drop for logical-type edge in range (<200-500>/default), where default is 500. [d]: 500

Congestion-drop for logical-type core must be greater than or equal to Congestion-drop for logical-type edge. Hence, Congestion drop for logical-type core will be set as default.

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

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

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

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

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

NTP server IPv4 address : <<var_oob_ntp>>

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

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

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

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

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

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

The following configuration will be applied:

```
password strength-check
switchname MDS-9132T-A
interface mgmt0
  ip address 10.2.164.92 255.255.255.0
  no shutdown
ip default-gateway 10.2.164.254
ssh key rsa 1024 force
feature ssh
no feature telnet
system timeout congestion-drop 500 logical-type edge
system timeout congestion-drop default logical-type core
feature http-server
ntp server 172.26.163.254
system default switchport shutdown
system default switchport trunk mode on
no system default zone default-zone permit
system default zone distribute full
system default zone mode enhanced
```

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

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

Set up the initial configuration for the Cisco MDS B switch on <<var_mds_B_hostname>>, by running through the same steps followed in the configuration, making the appropriate substitutions for <<var_mds_B_hostname>> and <<var_mds_B_mgmt_ip>>.

Cisco MDS Configuration

Enable Features and Settings

```
mds-9132T-a&b(config)# feature npiv
mds-9132T-a&b(config)# feature fport-channel-trunk
```

Create VSAN and Interfaces

On MDS 9132T A create the VSAN that will be used for connectivity to the Cisco UCS Fabric Interconnect and the Pure Storage FlashArray. Assign this VSAN to the interfaces that will connect to the Pure Storage FlashArray, as well as the interfaces and the Port Channel they create that are connected to the Cisco UCS Fabric Interconnect:

```

mds-9132T-a(config)# vsan database
mds-9132T-a(config-vsan-db)# vsan <<var_vsan_a_id>>

mds-9132T-a(config-vsan-db)# vsan <<var_vsan_a_id>> name Fabric-A

mds-9132T-a(config-vsan-db)# exit

mds-9132T-a(config)# zone smart-zoning enable vsan <<var_vsan_a_id>>

mds-9132T-a(config)# vsan database
mds-9132T-a(config-vsan-db)# vsan <<var_vsan_a_id>> interface fc1/1-4

mds-9132T-a(config-vsan-db)# vsan <<var_vsan_a_id>> interface fc1/15-18
mds-9132T-a(config-vsan-db)# vsan <<var_vsan_a_id>> interface po1

mds-9132T-a(config-vsan-db)# exit

mds-9132T-a(config)# int fc1/1-4
mds-9132T-a(config-if)# no shut

mds-9132T-a(config)# int fc1/15-18
mds-9132T-a(config-if)# no shut

mds-9132T-a(config-if)# exit

```

Repeat these commands on MDS 9132T B using the Fabric B appropriate VSAN ID:

```

mds-9132T-b(config)# vsan database
mds-9132T-b(config-vsan-db)# vsan <<var_vsan_b_id>>

mds-9132T-b(config-vsan-db)# vsan <<var_vsan_b_id>> name Fabric-B

mds-9132T-b(config-vsan-db)# exit

mds-9132T-b(config)# zone smart-zoning enable vsan <<var_vsan_b_id>>

mds-9132T-b(config)# vsan database
mds-9132T-b(config-vsan-db)# vsan <<var_vsan_b_id>> interface fc1/1-4

mds-9132T-b(config-vsan-db)# vsan <<var_vsan_b_id>> interface fc1/15-18
mds-9132T-b(config-vsan-db)# vsan <<var_vsan_b_id>> interface po2

mds-9132T-b(config-vsan-db)# exit

mds-9132T-b(config)# int fc1/1-4
mds-9132T-b(config-if)# no shut

mds-9132T-b(config)# int fc1/15-18
mds-9132T-b(config-if)# no shut

mds-9132T-b(config-if)# exit

```

Configure the MDS 9132T A Port Channel and add the interfaces connecting into the Cisco UCS Fabric Interconnect into it:

```
mds-9132T-a(config)# interface port-channel 1
mds-9132T-a(config-if)# channel mode active
mds-9132T-a(config-if)# switchport rate-mode dedicated

mds-9132T-a(config-if)# interface fc1/1-4
mds-9132T-a(config-if)# port-license acquire
mds-9132T-a(config-if)# channel-group 1 force
mds-9132T-a(config-if)# no shutdown
```

Repeat these commands on MDS 9132T B using the Fabric B appropriate Port Channel:

```
mds-9132T-b(config)# interface port-channel 2
mds-9132T-b(config-if)# channel mode active
mds-9132T-b(config-if)# switchport rate-mode dedicated

mds-9132T-b(config-if)# interface fc1/1-4
mds-9132T-b(config-if)# port-license acquire
mds-9132T-b(config-if)# channel-group 2 force
mds-9132T-b(config-if)# no shutdown
```



Save all configuration on both MDS Switches.

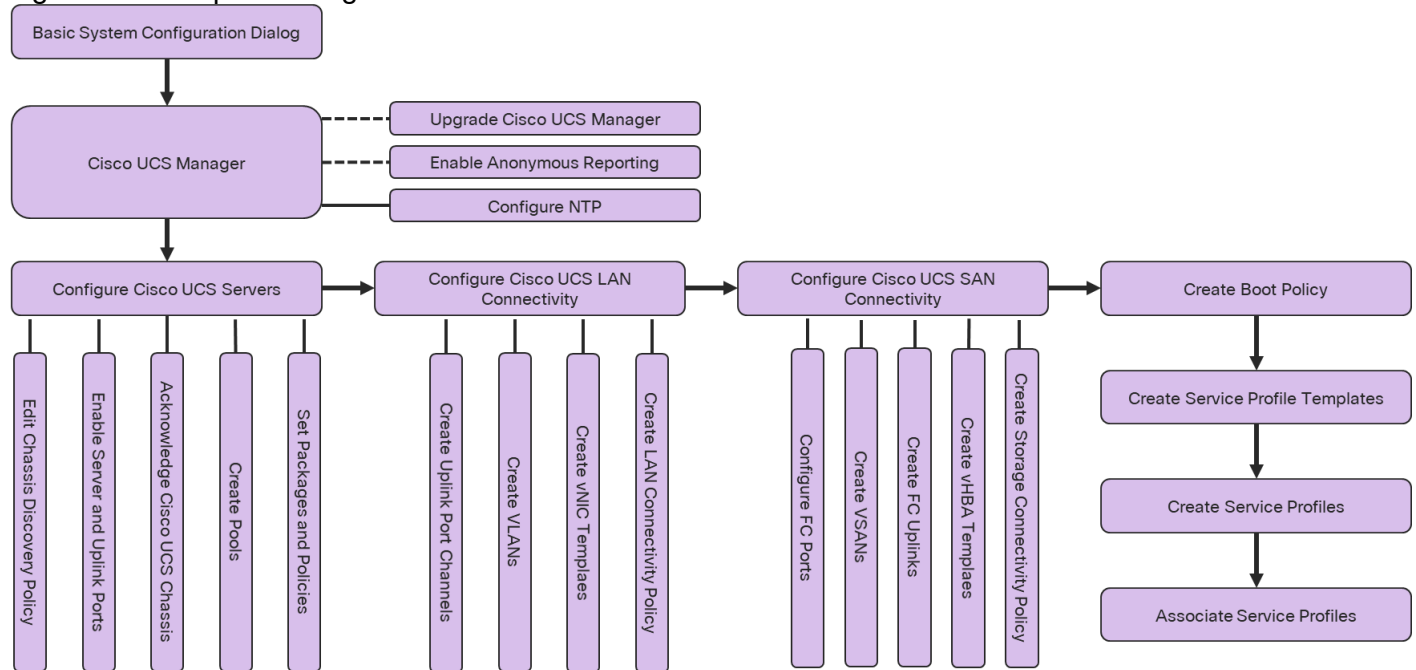
```
mds-9132T-a&b (config-if)# copy running-config startup-config
```

Compute Configuration

Cisco UCS Compute Configuration

The following procedures describe how to configure the Cisco UCS domain for use in a base FlashStack environment. This procedure assumes the use of UCS Fabric Interconnects running 4.0(2b). Configuration on a differing model of UCS Fabric Interconnects should be comparable but may differ slightly with model and changes in the Cisco UCS Manager (UCSM) release. The Cisco USC 6454 Fabric Interconnects and Cisco UCS Manger 4.0(2b) release were used in validation of this FlashStack solution, so steps will reflect this model and release.

Figure 4 Compute Configuration Workflow



Physical Connectivity

Physical cabling should be completed by following the diagram and table references in the previous section referenced as FlashStack Cabling.

Cisco UCS Basic System Configuration Dialog

This section provides detailed instructions for the configuration of the Cisco UCS 6454 Fabric Interconnects used in this FlashStack solution. Some changes may be appropriate for a customer’s environment, but care should be taken when stepping outside of these instructions as it may lead to an improper configuration.

To start on the configuration of the Fabric Interconnect A, connect to the console of the fabric interconnect and step through the Basic System Configuration Dialogue:

```

UCSM image signature verification successful

---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
    
```


the system. Only minimal configuration including IP connectivity to the Fabric interconnect and its clustering mode is performed through these steps.

Type Ctrl-C at any time to abort configuration and reboot system. To back track or make modifications to already entered values, complete input till end of section and answer no when prompted to apply configuration.

```

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

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

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

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

Enter the password for "admin":
Confirm the password for "admin":

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

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

Enter the system name: <var_ucs_clustername>>

Physical Switch Mgmt0 IP address : <<var_ucs_a_mgmt_ip>>

Physical Switch Mgmt0 IPv4 netmask : <<var_oob_mgmt_mask>>

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

Cluster IPv4 address : <<var_ucs_mgmt_vip>

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

    DNS IP address : <<var_nameserver_ip>>

Configure the default domain name? (yes/no) [n]: yes

    Default domain name : <<var_dns_domain_name>>

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

Following configurations will be applied:

    Switch Fabric=A
    System Name=AA12-UCS-6454
    Enforced Strong Password=yes
    Physical Switch Mgmt0 IP Address=10.2.164.51
    Physical Switch Mgmt0 IP Netmask=255.255.255.0
    Default Gateway=10.2.164.254
    Ipv6 value=0
    DNS Server=10.1.164.9
    Domain Name=flashstack.cisco.com

    Cluster Enabled=yes
    Cluster IP Address=10.2.164.50
    NOTE: Cluster IP will be configured only after both Fabric Interconnects are initialized.
          UCSM will be functional only after peer FI is configured in clustering mode.

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

```

Continue the configuration on the console of the Fabric Interconnect B:

---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of the system. Only minimal configuration including IP connectivity to

the Fabric interconnect and its clustering mode is performed through these steps.

Type Ctrl-C at any time to abort configuration and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.

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

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

Enter the admin password of the peer Fabric interconnect:
Connecting to peer Fabric interconnect... done
Retrieving config from peer Fabric interconnect... done
Peer Fabric interconnect Mgmt0 IPv4 Address: 10.2.164.51
Peer Fabric interconnect Mgmt0 IPv4 Netmask: 255.255.255.0
Cluster IPv4 address : 10.2.164.50

Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv4 Address

Physical Switch Mgmt0 IP address : <<var_ucs_b_mgmt_ip>>

Local fabric interconnect model(UCS-FI-6454)
Peer fabric interconnect is compatible with the local fabric interconnect. Continuing with the installer...

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

Cisco UCS Manager Configuration

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

1. Open a web browser and navigate to the Cisco UCS fabric interconnect cluster address.
2. Click the Launch UCS Manager link within the opening page.
3. If prompted to accept security certificates, accept as necessary.
4. When the Cisco UCS Manager login is prompted, enter admin as the user name and enter the administrative password.
5. Click Login to log into Cisco UCS Manager.

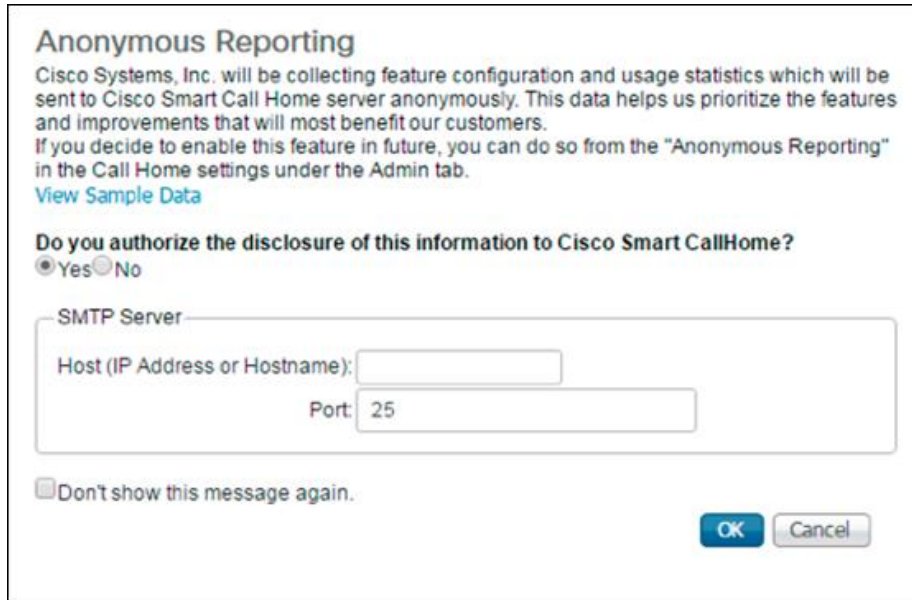
Upgrade Cisco UCS Manager to Version 4.0(2b)

This document assumes the use of Cisco UCS 4.0(2b). To upgrade the Cisco UCS Manager (UCSM) software and the Cisco UCS Fabric Interconnect software to version 4.0(2b), refer to [Cisco UCS Manager Install and Upgrade Guides](#).

Enable Anonymous Reporting

During the first connection to the Cisco UCS Manager GUI, a pop-up window will appear to allow for the configuration of Anonymous Reporting to Cisco on use to help with future development. To create anonymous reporting, complete the following step:

1. In the Anonymous Reporting window, select whether to send anonymous data to Cisco for improving future products, and provide the appropriate SMTP server gateway information if configuring:

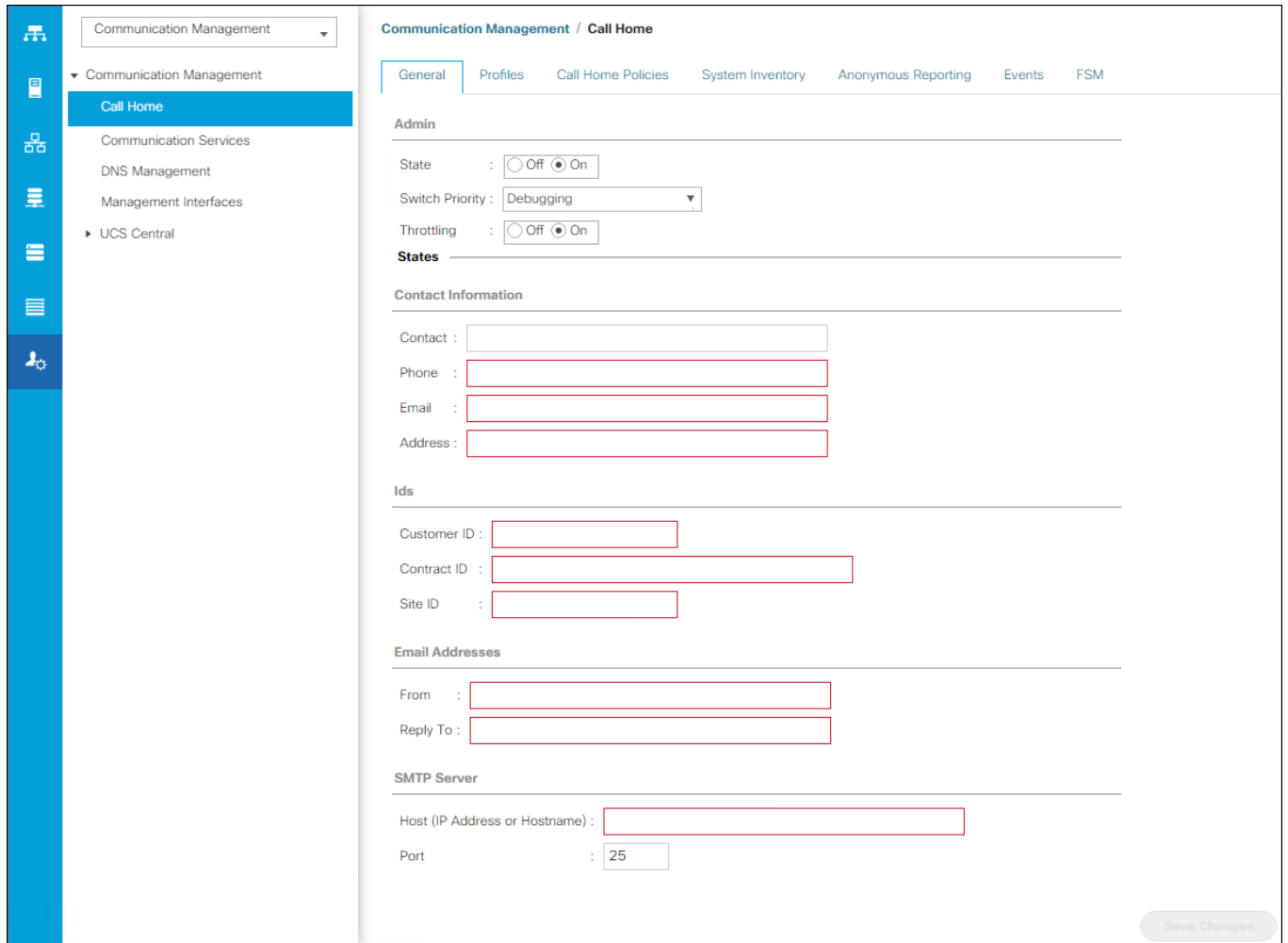


2. If you want to enable or disable Anonymous Reporting at a later date, it can be found within Cisco UCS Manager under: Admin -> Communication Management -> Call Home, which has a tab on the far right for Anonymous Reporting.

Configure Cisco UCS Call Home

During the first connection to the Cisco UCS Manager GUI, a pop-up window will appear to allow for the configuration of Anonymous Reporting to Cisco on use to help with future development. To create anonymous reporting, follow these steps:

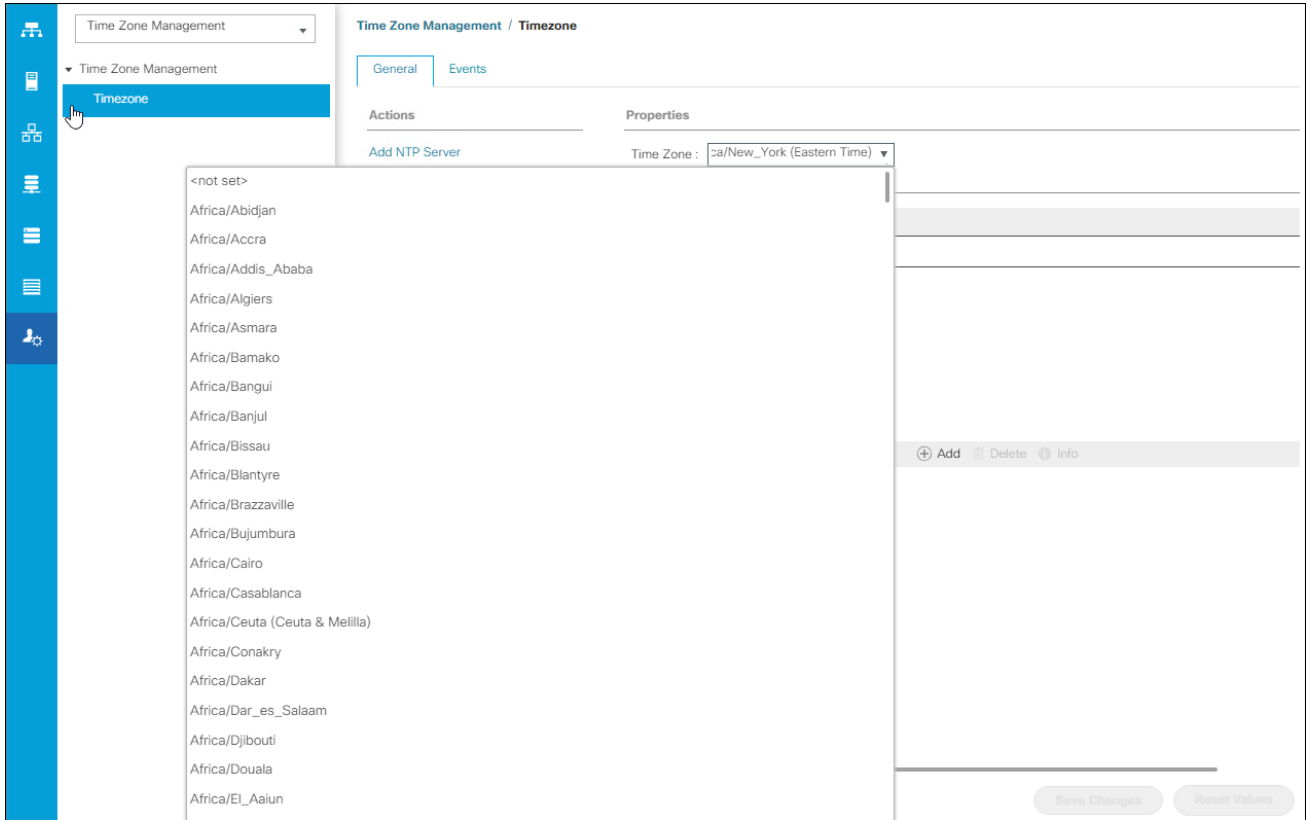
1. In Cisco UCS Manager, click the Admin tab in the navigation pane.
2. Expand Communication Management and click Call Home
3. Change State to On.
4. Fill in the fields according to your preferences and click Save Changes and OK



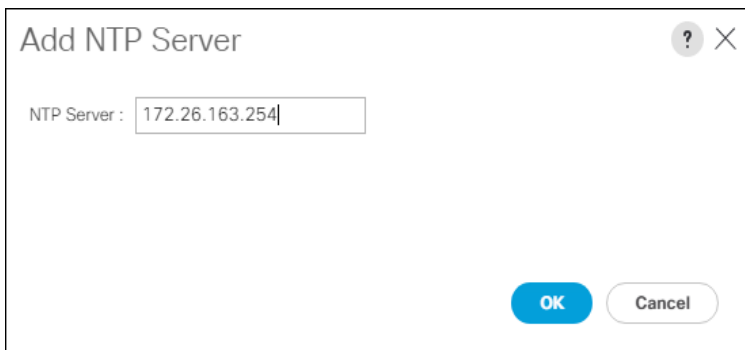
Configure NTP

To synchronize the Cisco UCS environment to the NTP server, follow these steps:

1. In Cisco UCS Manager, click the Admin tab in the navigation pane.
2. Expand Timezone Management and click Timezone.



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_oob_ntp>> and click OK.



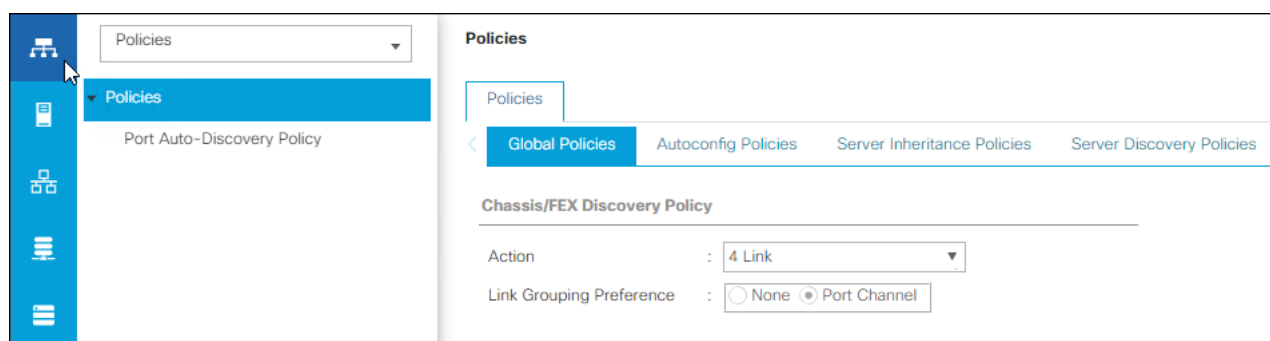
7. Click OK.

Configure Cisco UCS Servers

Edit Chassis Discovery Policy

Setting the discovery policy simplifies the addition of the Cisco UCS B-Series chassis. To modify the chassis discovery policy, follow these steps:

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

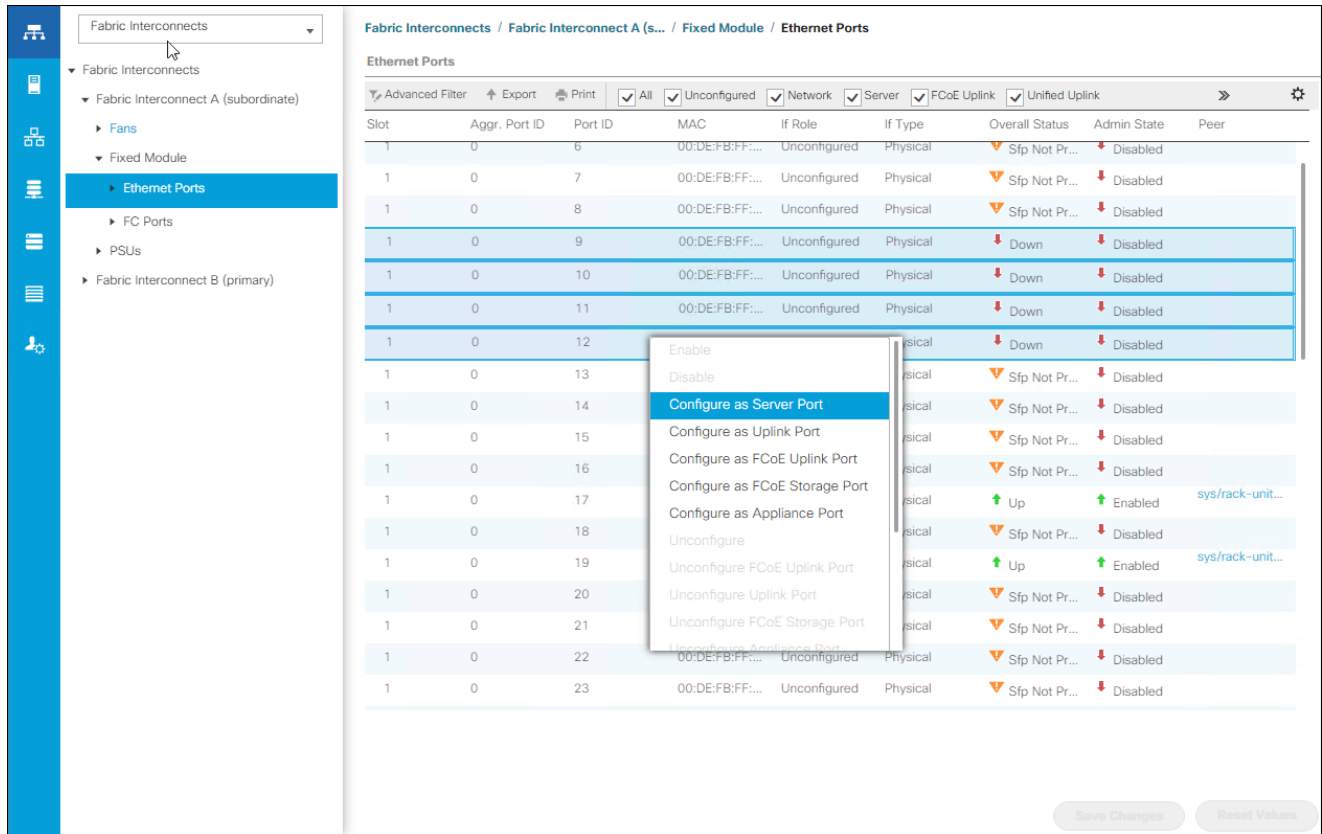


4. Leave other settings alone or change if appropriate to your environment.
5. Click Save Changes.
6. Click OK.

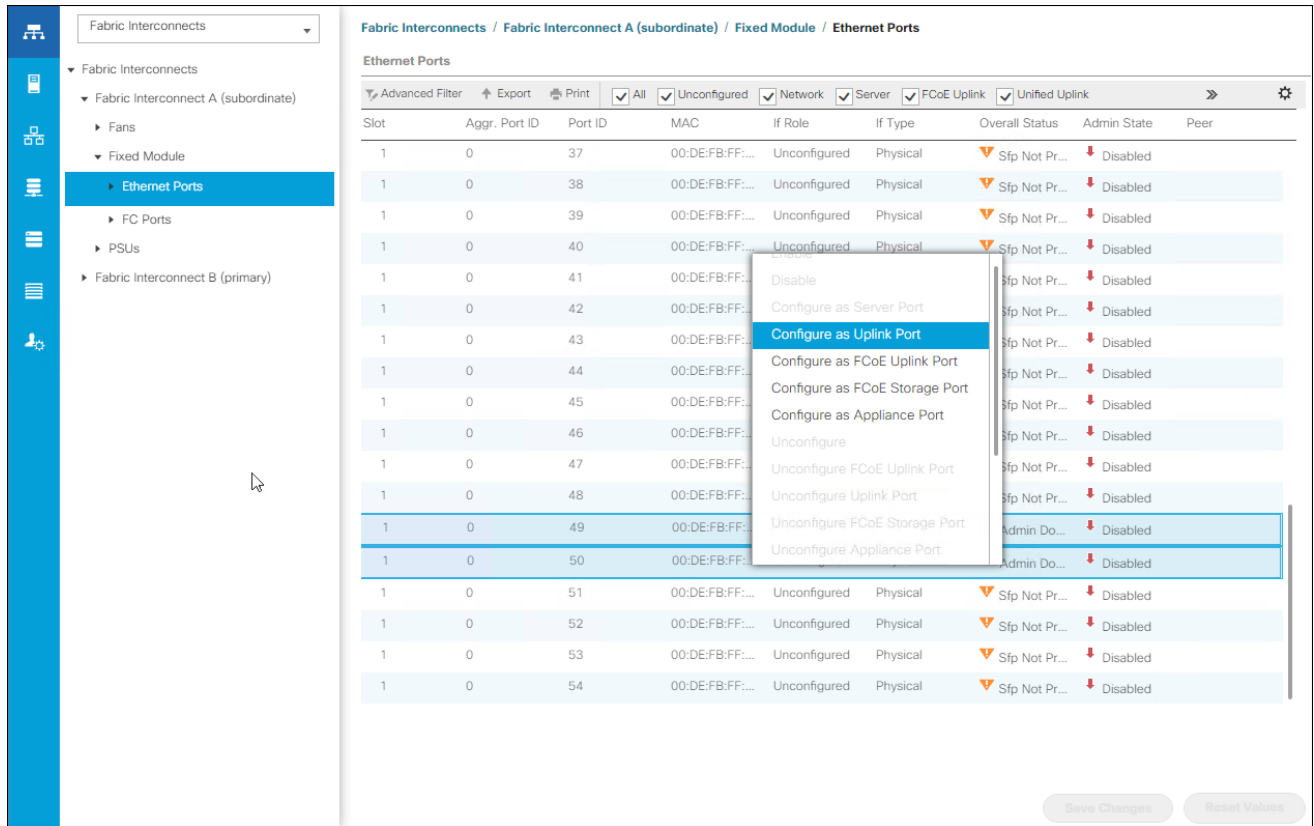
Enable Server and Uplink Ports

To enable server and uplink ports, follow these steps:

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



5. Click Yes to confirm server ports and click OK.
6. Verify that the ports connected to the chassis are now configured as server ports.
7. Select ports 39 and 40 that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.

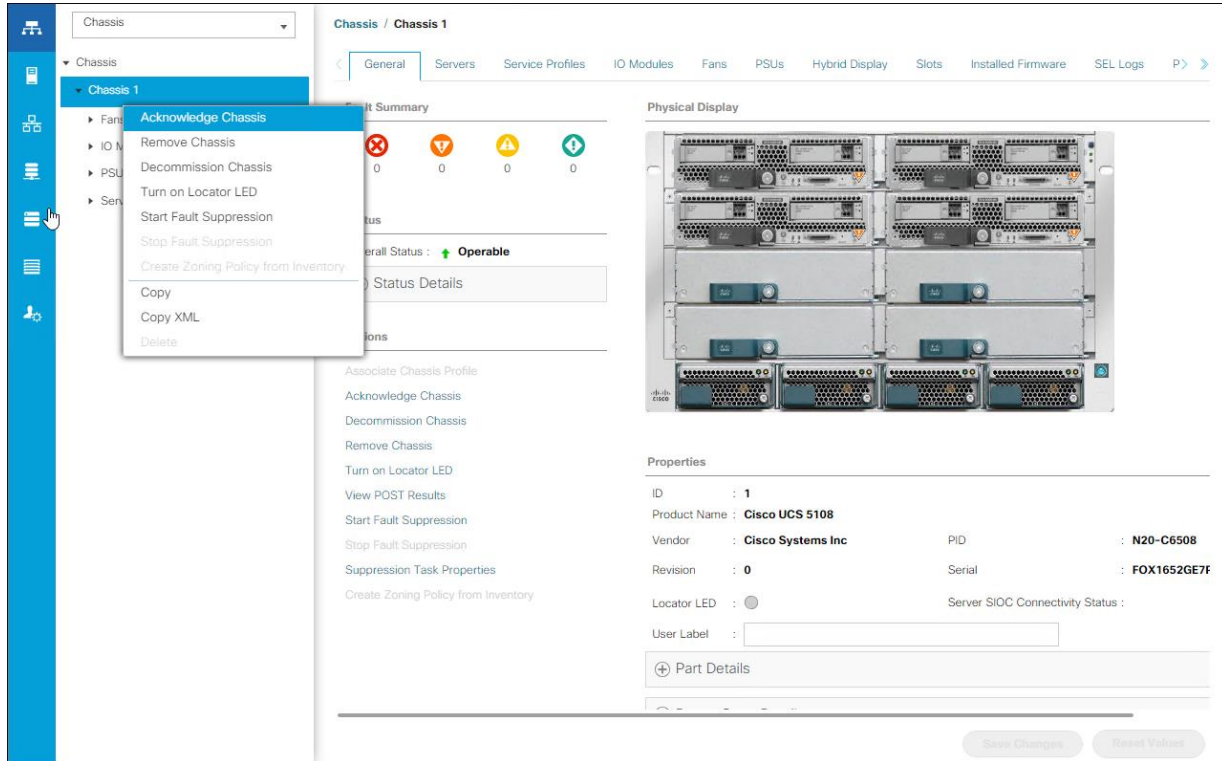


8. Click Yes to confirm uplink ports and click OK.
9. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.
10. Expand Ethernet Ports.
11. Select the ports that are connected to the chassis, right-click them and select Configure as Server Port.
12. Click Yes to confirm server ports and click OK.
13. Select ports 39 and 40 that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.
14. Click Yes to confirm the uplink ports and click OK

Acknowledge Cisco UCS Chassis

To acknowledge all Cisco UCS chassis, follow these steps:

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



4. Click Yes and then click OK to complete acknowledging the chassis.

Create Pools

Create MAC Address Pools

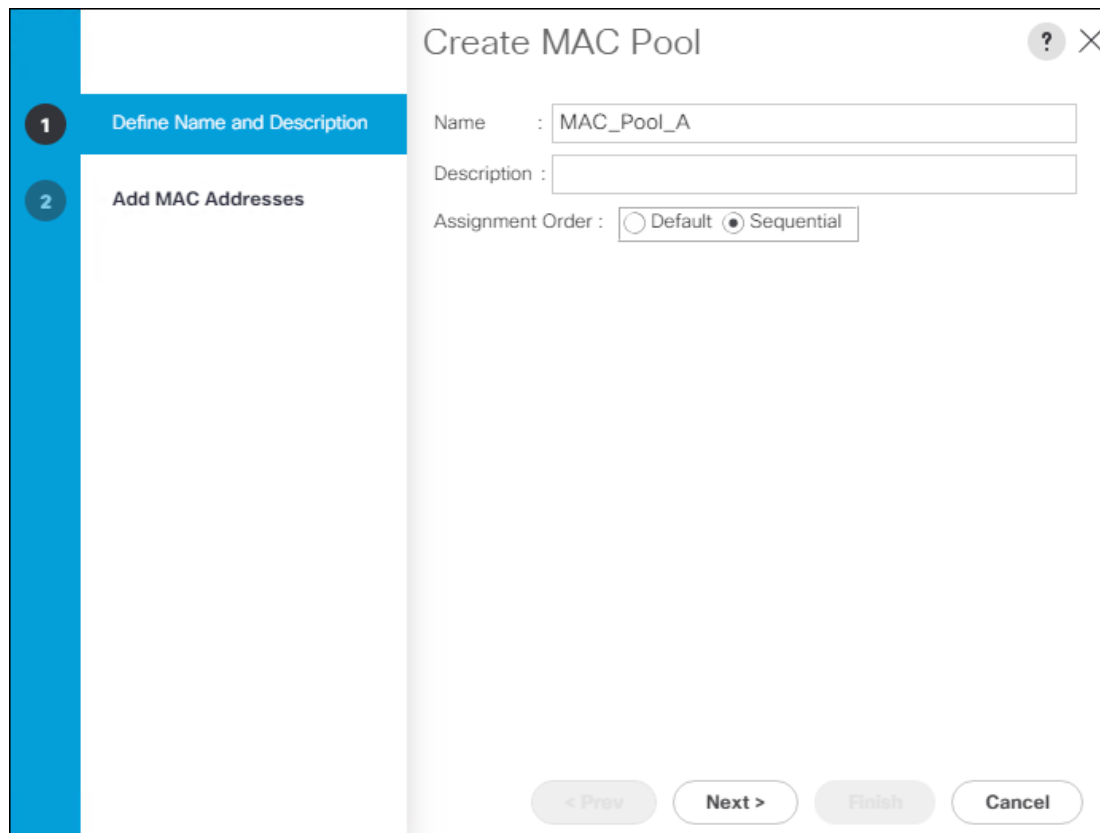
To configure the necessary MAC address pools for the Cisco UCS environment, follow these steps:

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. Select Sequential as the option for Assignment Order.



8. Click Next.

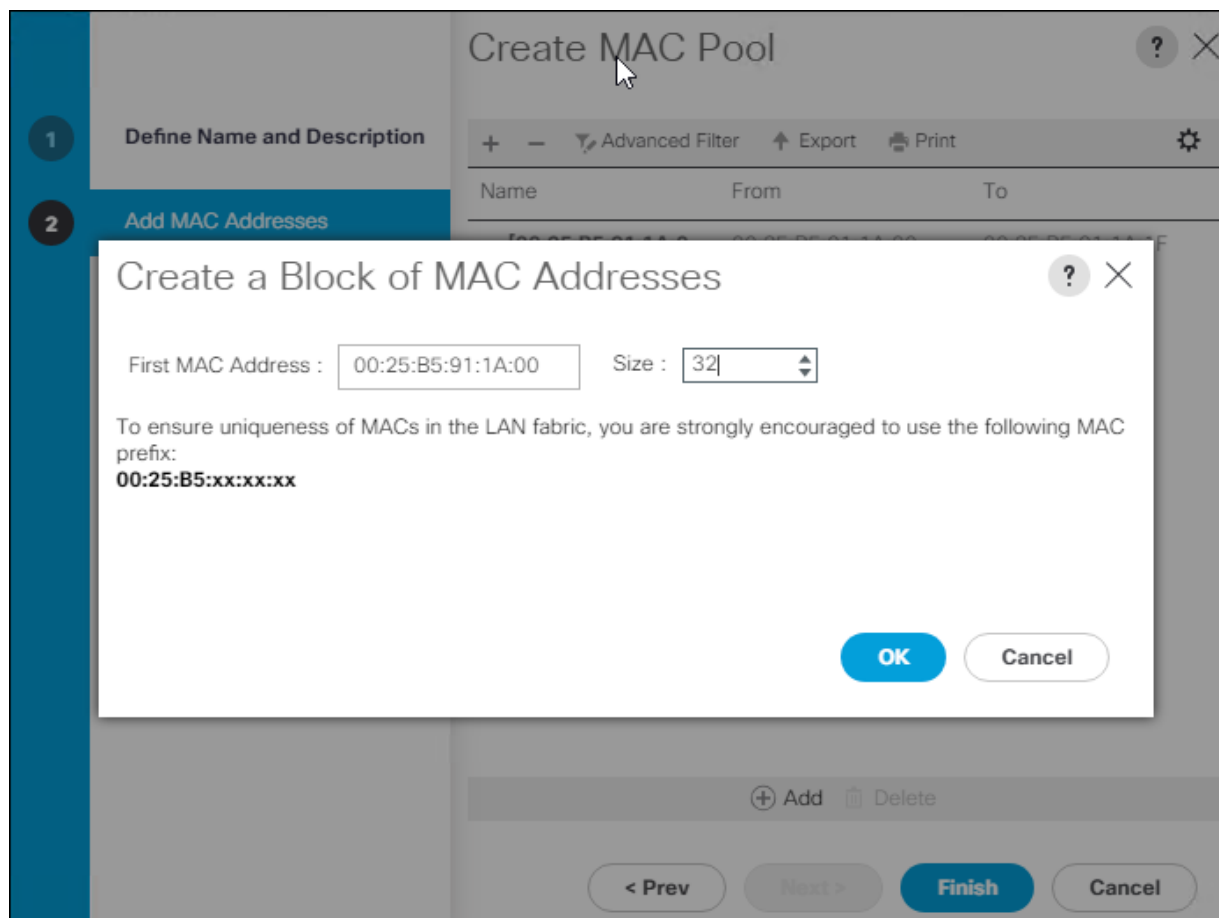
9. Click Add.

10. Specify a starting MAC address.



For Cisco UCS deployments, 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. In our example, we have carried forward the of also embedding the extra building, floor and Cisco UCS domain number information giving us 00:25:B5:91:1A:00 as our first MAC address.

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



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

19. Click Next.

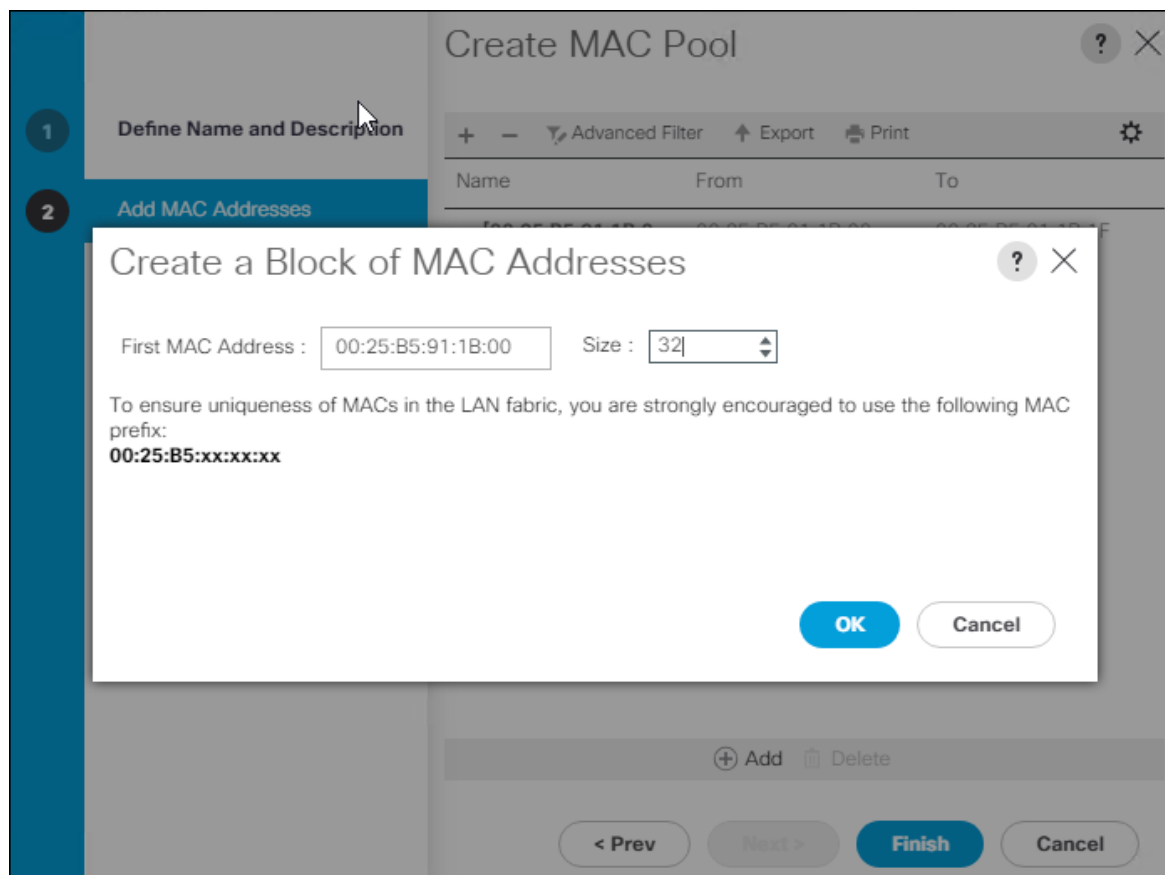
20. Click Add.

21. Specify a starting MAC address.



For Cisco UCS deployments, the recommendation is to place 0B in the next-to-last octet of the starting MAC address to identify all of the MAC addresses as fabric B addresses. In our example, we have carried forward the of also embedding the extra building, floor and Cisco UCS domain number information giving us 00:25:B5:91:1B:00 as our first MAC address.

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



23. Click OK.

24. Click Finish.


25. In the confirmation message, click OK.


Create WWNN Pool

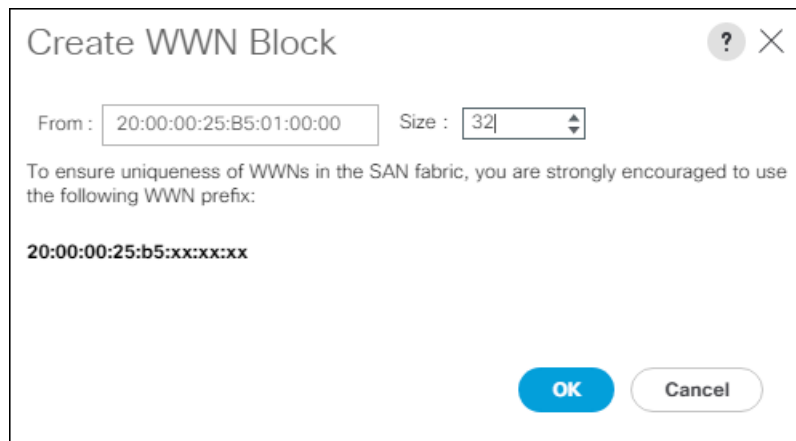
To configure the necessary WWNN pool for the Cisco UCS environment, follow these steps on Cisco UCS Manager:

1. Select the SAN tab.
2. Select Pools > root.
3. Right-click WWNN Pools under the root organization.
4. Select Create WWNN Pool to create the WWNN pool.
5. Enter WWNN_Pool for the name of the WWNN pool.
6. Optional: Enter a description for the WWNN pool.
7. Select Sequential for Assignment Order.

8. Click Next.
9. Click Add.
10. Modify the From field as necessary for the UCS Environment.

 Modifications of the WWN block, as well as the WWPN and MAC Addresses, can convey identifying information for the Cisco UCS domain. Within the From field in our example, the 6th octet was changed from 00 to 01 to represent as identifying information for this being our first Cisco UCS domain.

 Also, when having multiple Cisco UCS domains sitting in adjacency, it is important that these blocks, the WWNN, WWPN, and MAC hold differing values between each set.



11. Specify a size of the WWNN block sufficient to support the available server resources.
12. Click OK.
13. Click Finish to create the WWNN Pool.
14. Click OK.

Create WWPN Pools


To configure the necessary WWPN pools for the Cisco UCS environment, follow these steps:

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

9. Click Next.

10. Click Add.

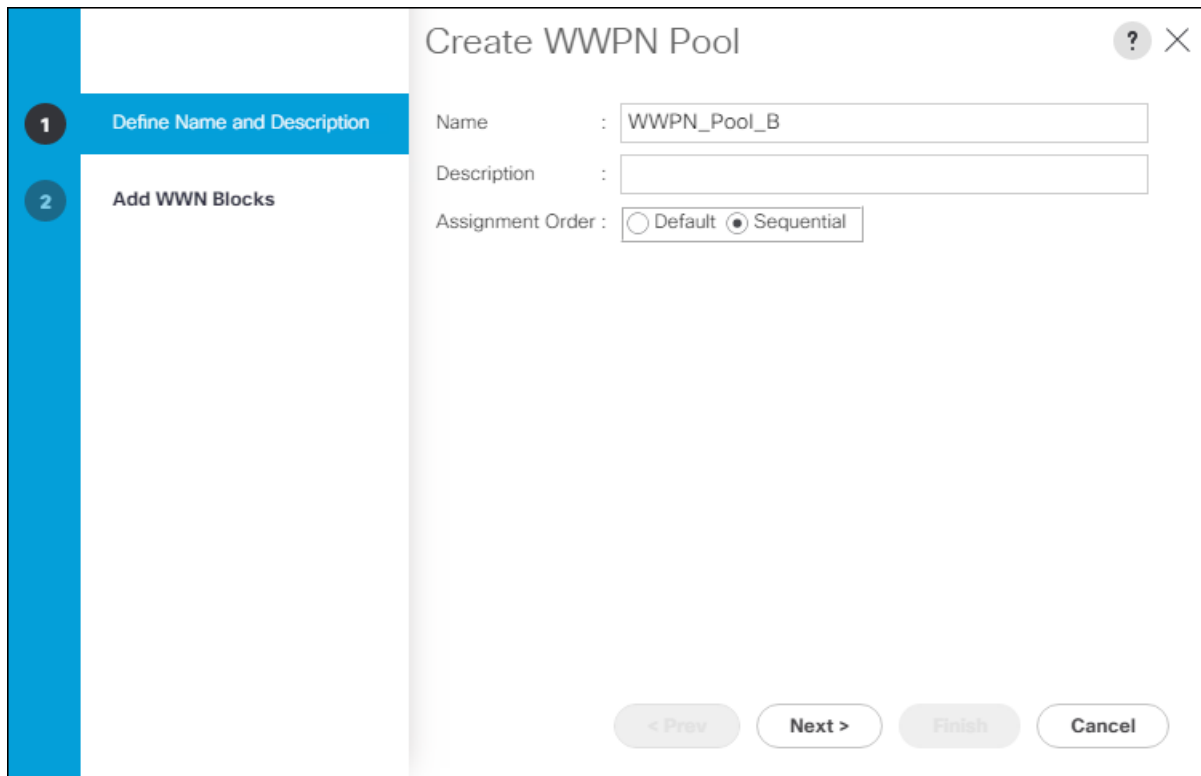
11. Specify a starting WWPN

 For the FlashStack solution, the recommendation is to place 0A in the next-to-last octet of the starting WWPN to identify all of the WWPNs as fabric A addresses. Merging this with the pattern we used for the WWNN we see a WWPN block starting with 20:00:00:25:B5:01:0A:00.


12. Specify a size for the WWPN pool that is sufficient to support the available blade or server resources.

13. Click OK.

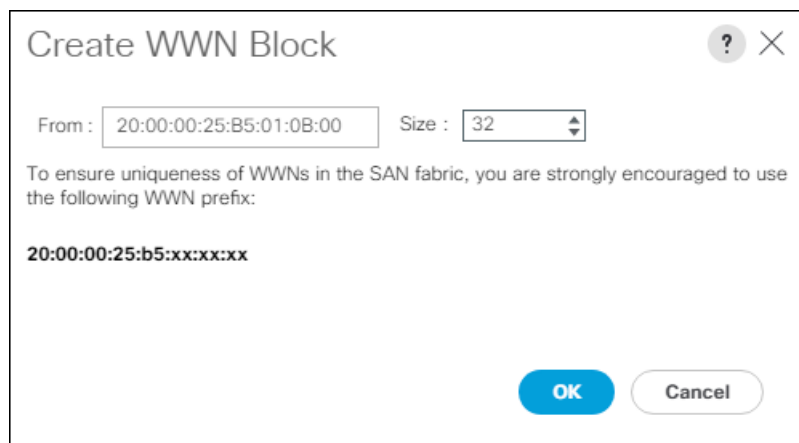
14. Click Finish.
15. In the confirmation message, click OK.
16. Right-click WWPN Pools under the root organization.
17. Select Create WWPN Pool to create the WWPN pool.
18. Enter WWPN_Pool_B as the name of the WWPN pool.
19. Optional: Enter a description for the WWPN pool.
20. Select Sequential for Assignment Order.



21. Click Next.
22. Click Add.
23. Specify a starting WWPN.

 For the FlashStack solution, the recommendation is to place 0B in the next-to-last octet of the starting WWPN to identify all of the WWPNs as fabric A addresses. Merging this with the pattern we used for the WWNN we see a WWPN block starting with 20:00:00:25:B5:01:0B:00.

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



25. Click OK.

26. Click Finish.

27. In the confirmation message, click OK.

Create UUID Suffix Pool

To configure the necessary universally unique identifier (UUID) suffix pool for the Cisco UCS environment, follow these 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.

1 Define Name and Description

2 Add UUID Blocks

Create UUID Suffix Pool

Name :

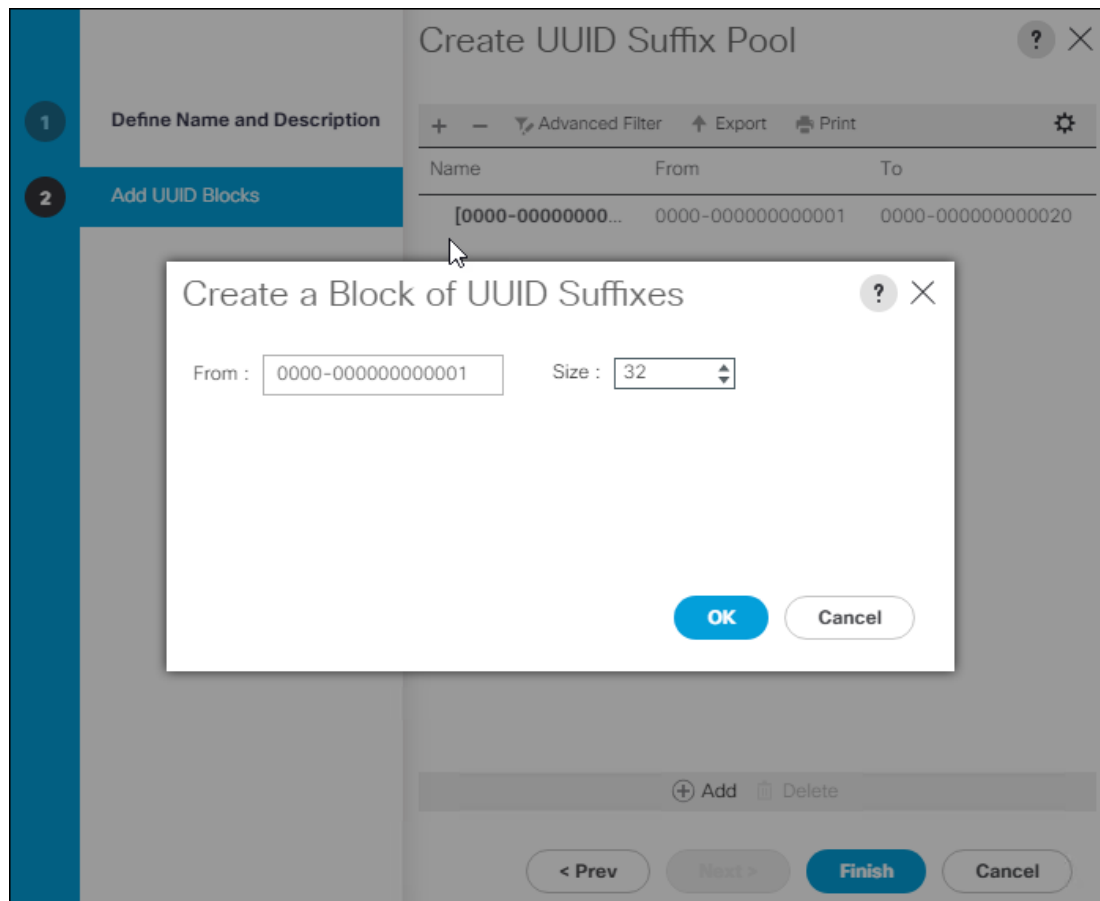
Description :

Prefix : Derived other

Assignment Order : Default Sequential

< Prev Next > Finish Cancel

6. Optional: Enter a description for the UUID suffix pool.
7. Keep the prefix at the derived option.
8. Select Sequential for the Assignment Order.
9. Click Next.
10. Click Add to add a block of UUIDs.



11. Keep the From: field at the default setting.
12. Specify a size for the UUID block that is sufficient to support the available blade or server resources.
13. Click OK.
14. Click Finish.
15. Click OK.

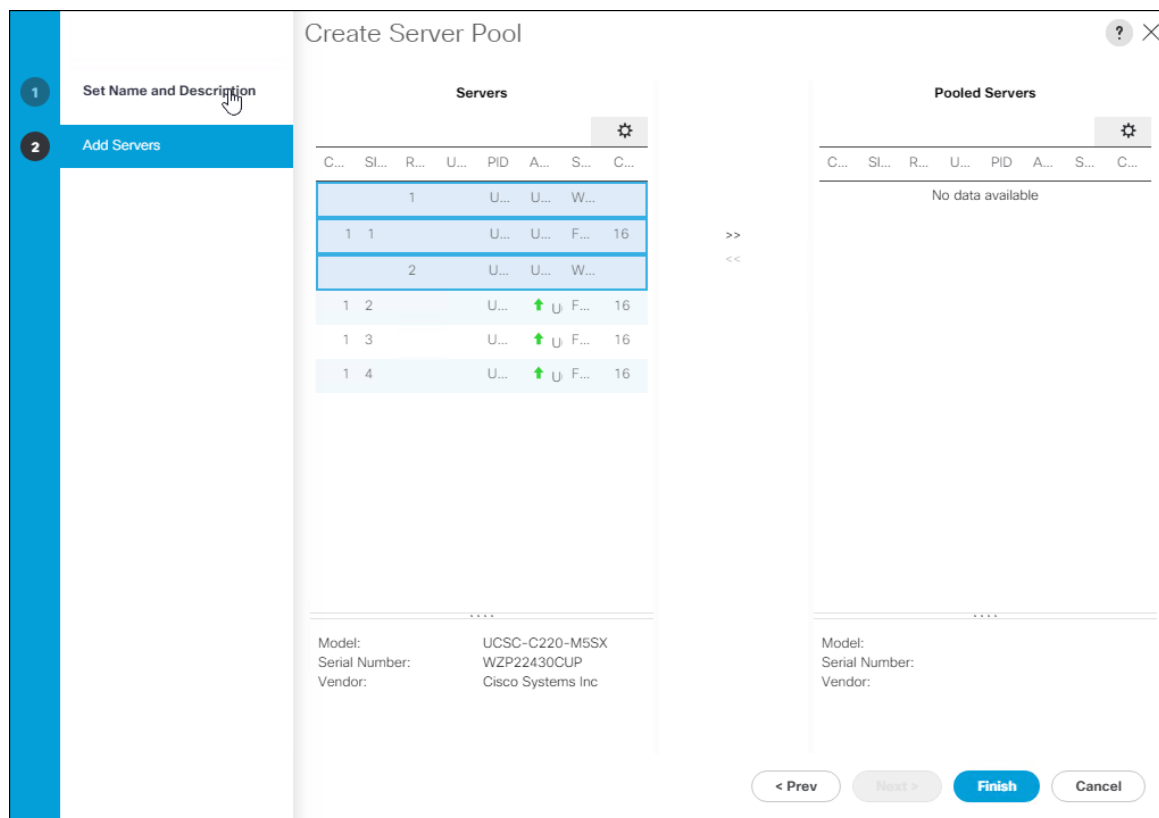
Create Server Pool

To configure the necessary server pool for the Cisco UCS environment, follow these steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Pools > root.
3. Right-click Server Pools.
4. Select Create Server Pool.
5. Enter Infra_Pool as the name of the server pool.

The screenshot shows a 'Create Server Pool' dialog box. The title bar includes a question mark icon and a close button. A vertical sidebar on the left contains two steps: '1 Set Name and Description' (highlighted in blue) and '2 Add Servers'. The main content area has two input fields: 'Name : Infra_Pool' and 'Description :'. At the bottom right, there are four buttons: '< Prev', 'Next >', 'Finish', and 'Cancel'.

6. Optional: Enter a description for the server pool.
7. Click Next.
8. Select two (or more) servers to be used for the VMware management cluster and click >> to add them to the Infra_Pool server pool.



9. Click Finish.

10. Click OK

Create IP Pool for KVM Access

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

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

Create Block of IPv4 Addresses [?] [X]

From : 10.2.164.70 Size : 16

Subnet Mask : 255.255.255.0 Default Gateway : 10.2.164.254

Primary DNS : 10.1.164.9 Secondary DNS : 0.0.0.0

[OK] [Cancel]

4. Enter the starting IP address of the block and the number of IP addresses required, and the subnet and gateway information.
5. Click OK to create the block of IPs.
6. Click OK.

Set Packages and Policies

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, follow these steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Expand Host Firmware Packages.
4. Select default.
5. In the Actions pane, select Modify Package Versions.
6. Select the version 4.0(2b)B for the Blade Package, and optionally set version 4.0(2b)C for the Rack Package.
7. Leave Excluded Components with only Local Disk selected.

Modify Package Versions ✕

Blade Package :

Rack Package :

Service Pack :

The images from Service Pack will take precedence over the images from Blade or Rack Package

Excluded Components:

Adapter
 BIOS
 Board Controller
 CIMC
 FC Adapters
 Flex Flash Controller
 GPUs
 HBA Option ROM
 Host NIC
 Host NIC Option ROM
 Local Disk
 NVME Mswitch Firmware
 PSU
 Pci Switch Firmware

8. Click OK to modify the host firmware package.

Create Server Pool Qualification Policy (Optional)

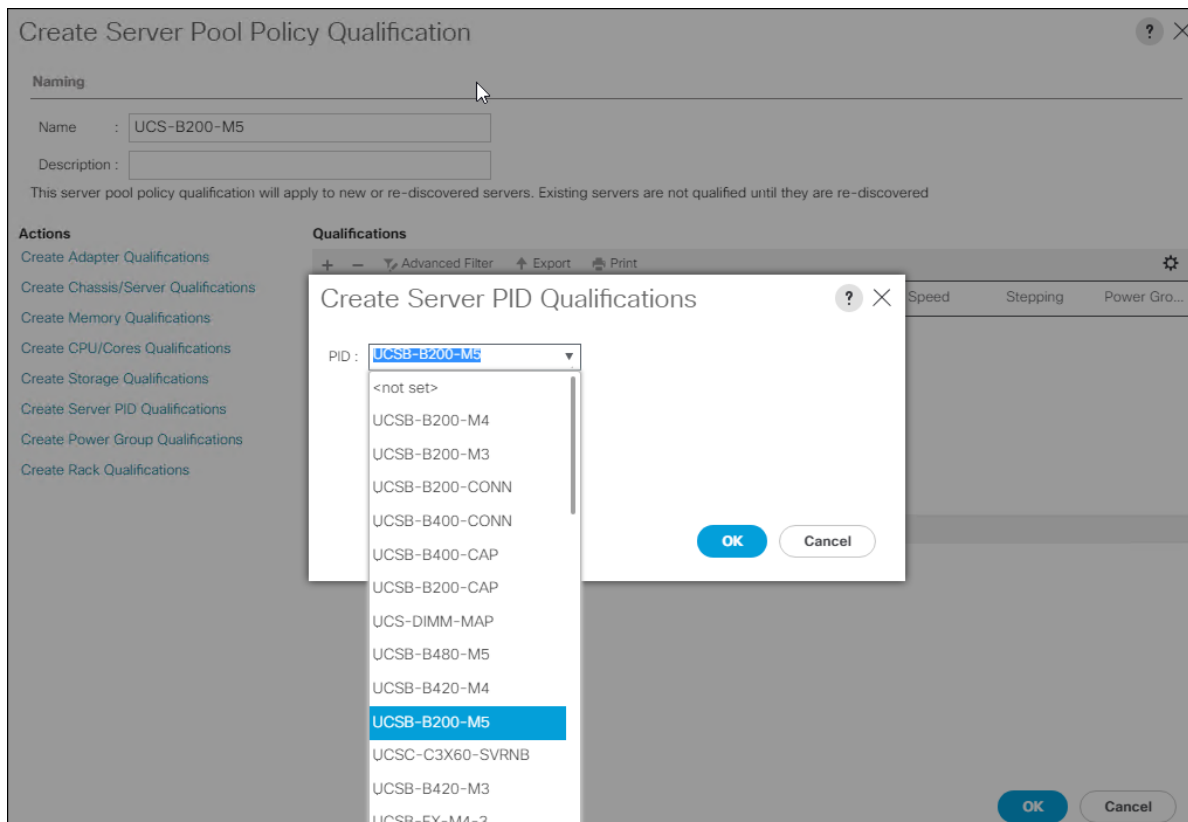
To create an optional server pool qualification policy for the Cisco UCS environment, follow these steps:



This example creates a policy for Cisco UCS B200 M5 servers for a server pool.

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. Name the policy UCS-B200M5.
6. Select Create Server PID Qualifications.
7. Select UCS-B200-M5 from the PID drop-down list.



8. Click OK.
9. Optionally select additional qualifications to refine server selection parameters for the server pool.
10. Click OK to create the policy then OK for the confirmation.

Create vMedia Policy for VMware ESXi 6.7 U1 Install Boot (Optional)

A separate HTTP web server is required to automate the availability of the ESXi image to each Service Profile on first power on. The creation of this web server is not covered in this document but can be any existing web server capable of serving files via HTTP that are accessible on the OOB network that the ESXi image can be placed upon.

Place the Cisco Custom Image VMware ESXi 6.7 U1 ISO on the HTTP server and follow these steps to create a vMedia Policy:

1. In Cisco UCS Manager, select Servers.
2. Select Policies > root.
3. Right-click vMedia Policies.

4. Select Create vMedia Policy.
5. Name the policy ESXi-6.7U1-HTTP.
6. Enter "Mounts ISO for ESXi 6.7 U1" in the Description field.
7. Click Add.
8. Name the mount ESXi-6.7U1-HTTP.
9. Select the CDD Device Type.
10. Select the HTTP Protocol.
11. Enter the IP Address of the web server.



Since DNS server IPs are not required in the KVM IP earlier, it is may be necessary to enter the IP of the web server instead of the hostname.

12. Leave "None" selected for Image Name Variable.
13. Enter VMware_ESXi_6.7.0_10302608_Custom_Cisco_6.7.1.1 as the Remote File name.
14. Enter the web server path to the ISO file in the Remote Path field.

Create vMedia Mount [?] [X]

Name : ESXi-6.7U1 HTTP

Description :

Device Type : CDD HDD

Protocol : NFS CIFS HTTP HTTPS

Hostname/IP Address : 192.1.164.165

Image Name Variable : None Service Profile Name

Remote File : VMware_ESXi_6.7.0_10302608_Custom_Cisco_6.7

Remote Path : /srv/repo/VMware/

Username :

Password :

Remap on Eject :

OK Cancel

15. Click OK to create the vMedia Mount.

16. Click OK then OK again to complete creating the vMedia Policy.



For any new servers added to the Cisco UCS environment the vMedia service profile template can be used to install the ESXi host. On first boot the host will boot into the ESXi installer. After ESXi is installed, the vMedia will not be referenced as long as the boot disk is accessible.

Create Server BIOS Policy

To create a server BIOS policy for the Cisco UCS environment, follow these steps:

1. In Cisco UCS Manager, click Servers .
2. Select Policies > root.
3. Right-click BIOS Policies.
4. Select Create BIOS Policy.
5. Enter VM-Host as the BIOS policy name.

Create BIOS Policy ? X

Name : VM-Host

Description :

Reboot on BIOS Settings Change :

OK Cancel

6. Select and right click the newly created BIOS Policy.
7. Within the Main tab of the Policy:
8. Change CDN Control to enabled.
9. Change the Quiet Boot setting to disabled.

Policies / root / BIOS Policies / VM-Host

Main | **Advanced** | Boot Options | Server Management | Events

Actions

Delete

Show Policy Usage

Use Global

Properties

Name : **VM-Host**

Description :

Owner : **Local**

Reboot on BIOS Settings Change :

Advanced Filter | Export | Print |

BIOS Setting	Value
CDN Control	Enabled
Front panel lockout	Platform Default
POST error pause	Platform Default
Quiet Boot	Disabled
Resume on AC power loss	Platform Default

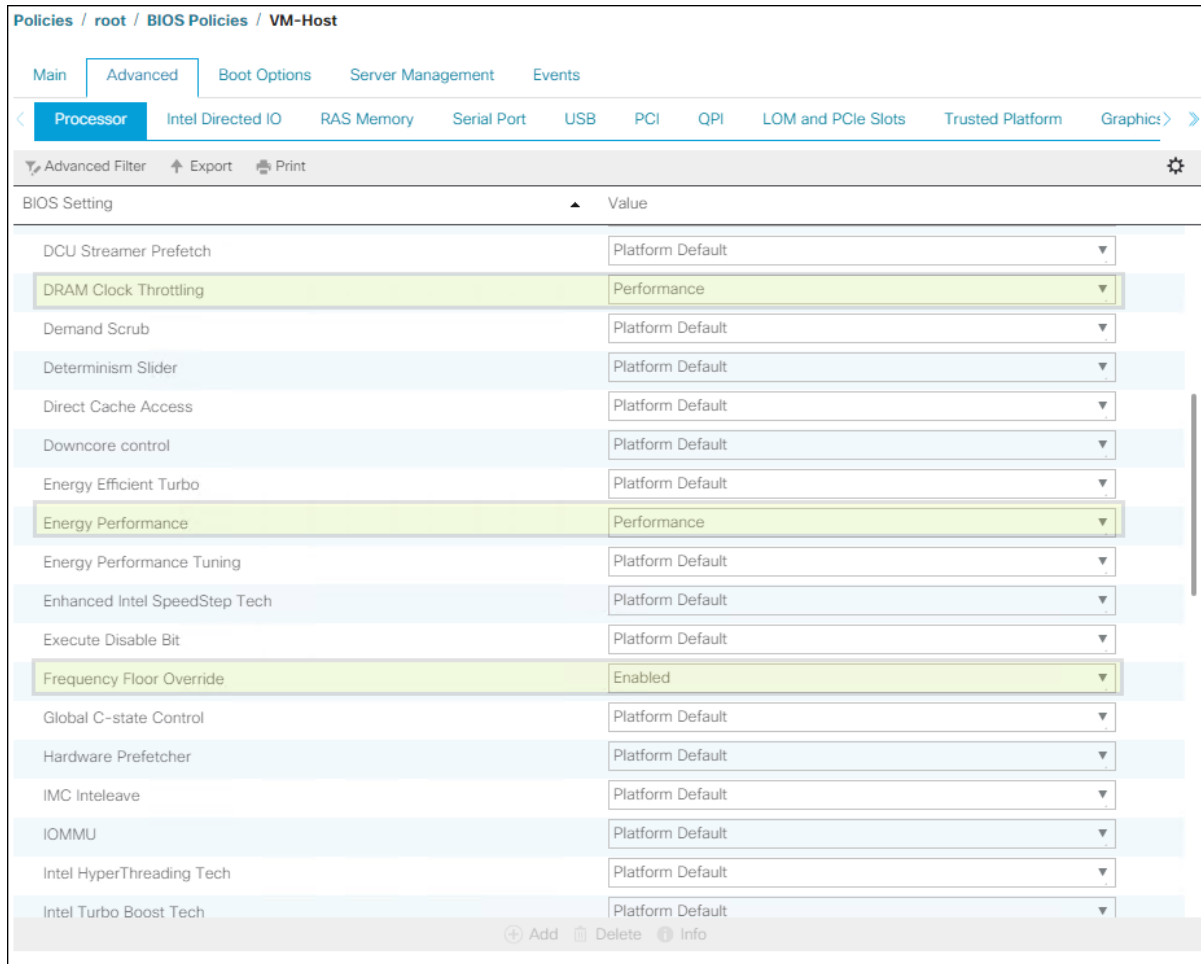
Add Delete Info

Save Changes | Reset Values

10. Click the Advanced tab, leaving the Processor tab selected within the Advanced tab.

11. Set the following within the Processor tab:

- a. DRAM Clock Throttling -> Performance
- b. Frequency Floor Override -> Enabled
- c. Energy Performance -> Performance



12. Scroll down to the remaining Processor options and select:

- a. Processor C State -> Disabled
- b. Processor C1E -> disabled
- c. Processor C3 Report -> disabled
- d. Processor C6 Report -> disabled
- e. Processor C7 Report -> disabled

Policies / root / BIOS Policies / VM-Host

Main | **Advanced** | Boot Options | Server Management | Events

Processor | Intel Directed IO | RAS Memory | Serial Port | USB | PCI | QPI | LOM and PCIe Slots | Trusted Platform | Graphics >

Advanced Filter | Export | Print

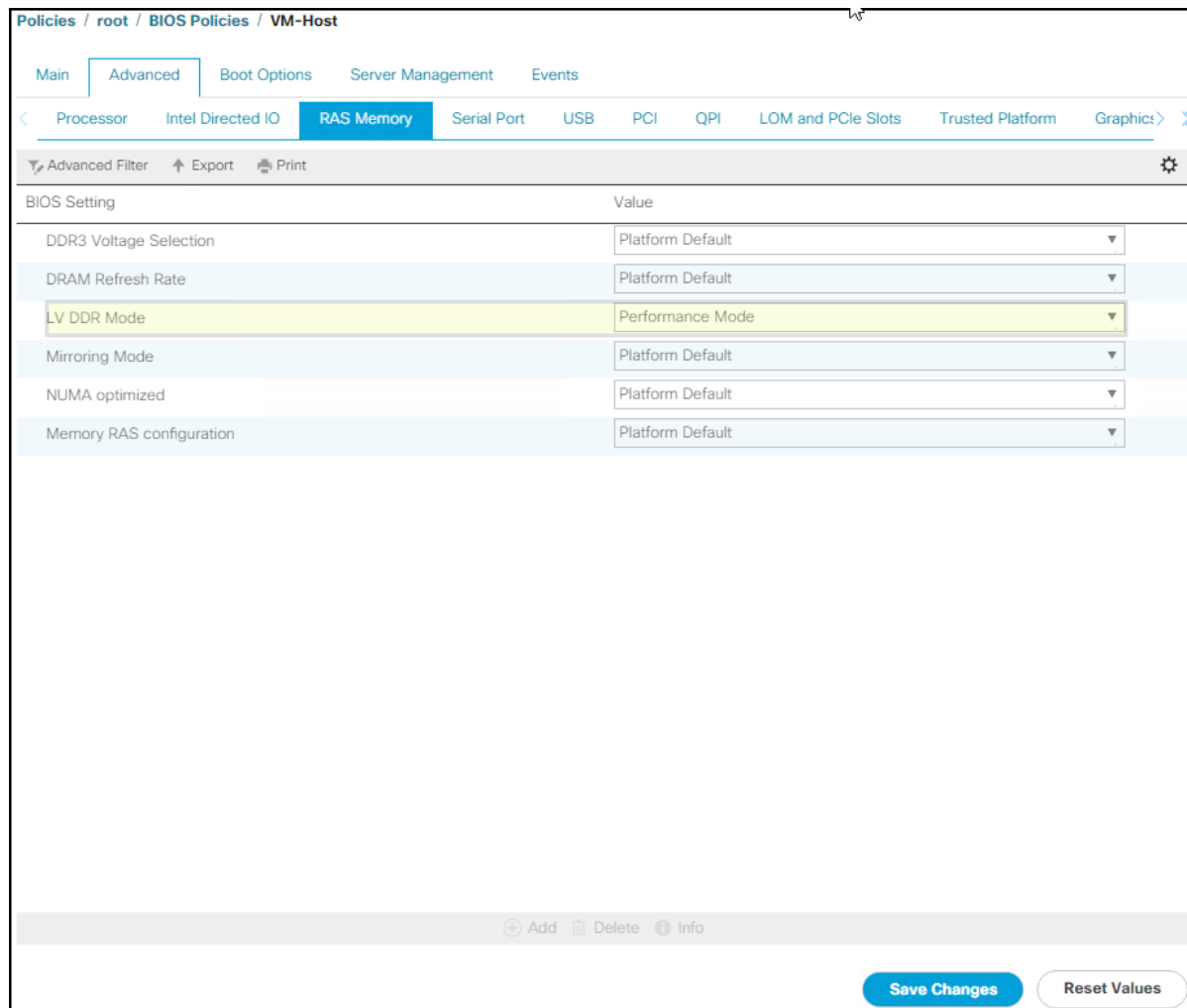
BIOS Setting	Value
Package C State Limit	Platform Default
Patrol Scrub	Platform Default
Power Technology	Platform Default
Processor C State	Disabled
Processor C1E	Disabled
Processor C3 Report	Disabled
Processor C6 Report	Disabled
Processor C7 Report	Disabled
Processor CMCI	Platform Default
ProcessorEppProfile	Platform Default
Rank Interleaving	Platform Default
SMEE	Platform Default
SMT Mode	Platform Default
SVM Mode	Platform Default
Sub NUMA Clustering	Platform Default
UPI Prefetch	Platform Default
Workload Configuration	Platform Default
XPT Prefetch	Platform Default

+ Add | Delete | Info

Save Changes | Reset Values

13. Click the RAS Memory tab and select:

- a. LV DDR Mode -> performance-mode



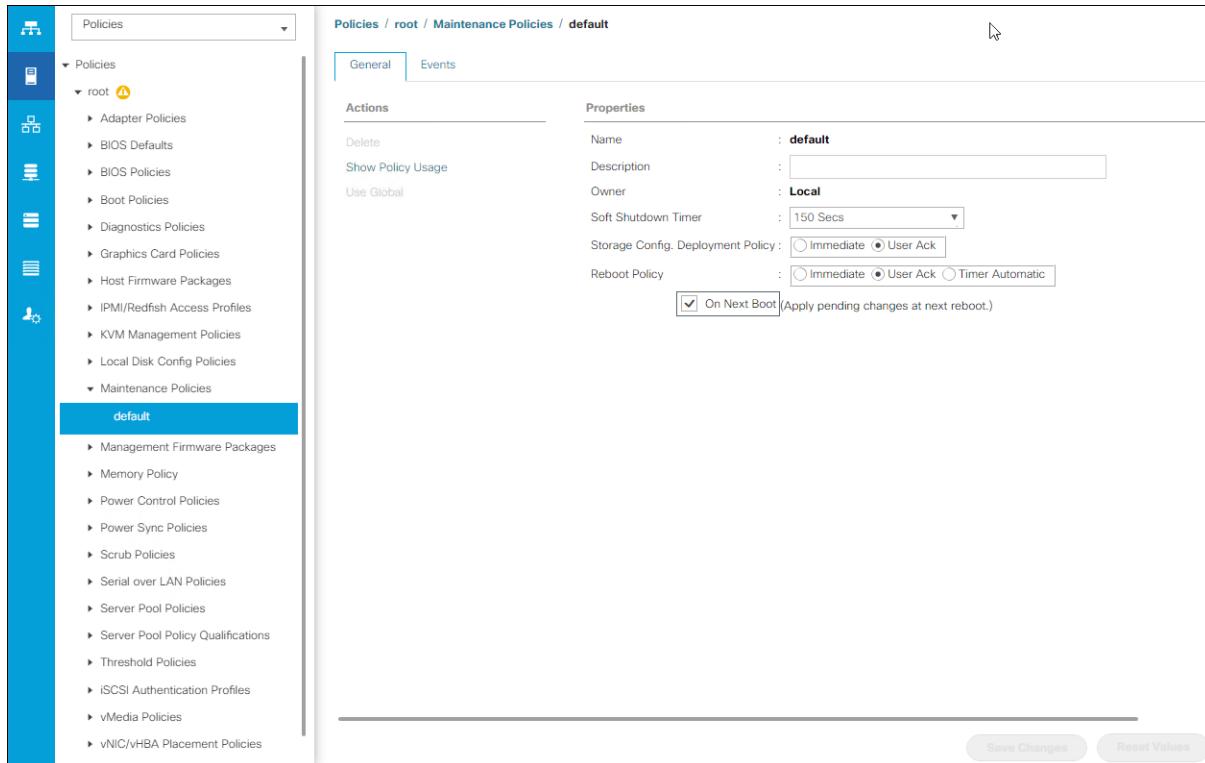
14. Click Save Changes.

15. Click OK.

Update Default Maintenance Policy

To update the default Maintenance Policy, follow these 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. (Optional: Click "On Next Boot" to delegate maintenance windows to server owners).



6. Click Save Changes.
7. Click OK to accept the change.

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, follow these 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.

Create Local Disk Configuration Policy ? X

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

FlexFlash Removable State : Yes No No Change

If **FlexFlash Removable State** is changed, SD cards will become unavailable temporarily.
Please ensure SD cards are not in use before changing the FlexFlash Removable State.

8. Click OK.

Create Power Control Policy

To create a power control policy for the Cisco UCS environment, follow these 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.

Create Power Control Policy ? X

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.

7. Click OK to create the power control policy.
8. Click OK.

Create Network Control Policy for Cisco Discovery Protocol

To create a network control policy that enables Cisco Discovery Protocol (CDP) on virtual network ports, follow these 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 [?] [X]

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.

Configure Cisco UCS LAN Connectivity

Create Uplink Port Channels

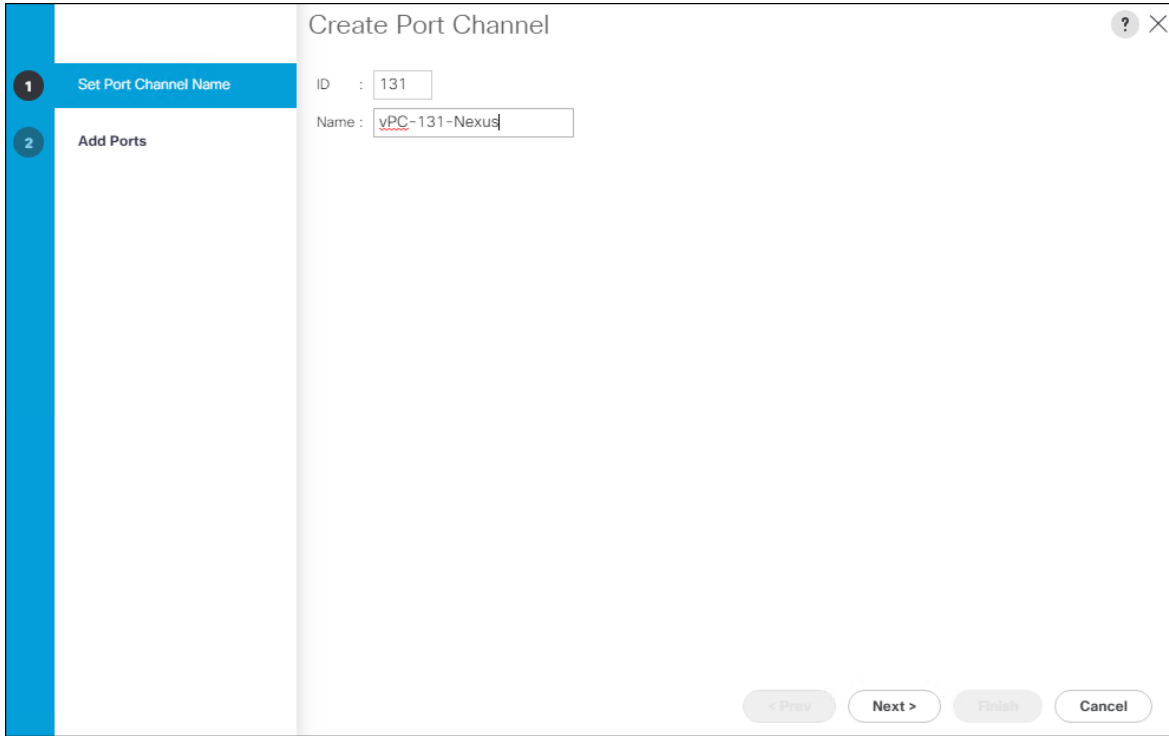
To configure the necessary port channels out of the Cisco UCS environment, follow these steps:

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.

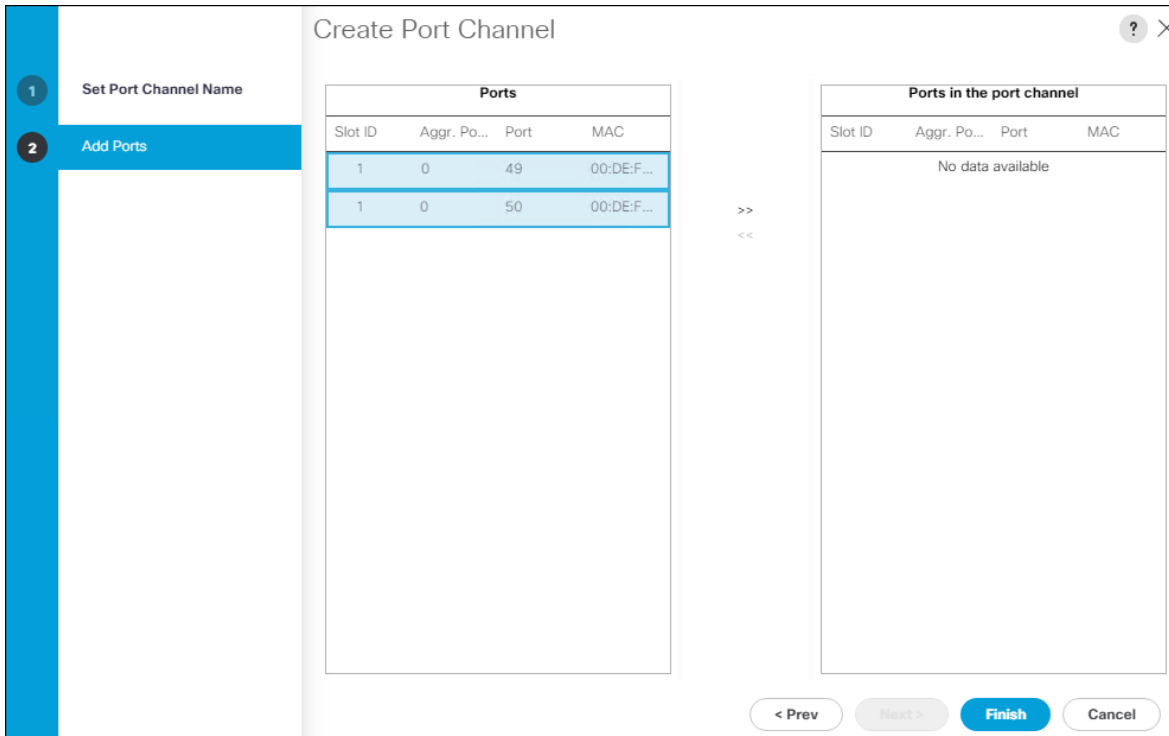
2. Under LAN > LAN Cloud, expand the Fabric A tree.
3. Right-click Port Channels.
4. Select Create Port Channel.
5. Enter a unique ID for the port channel, (131 in our example to correspond with the upstream Nexus port channel).
6. With 131 selected, enter vPC-131-Nexus as the name of the port channel.



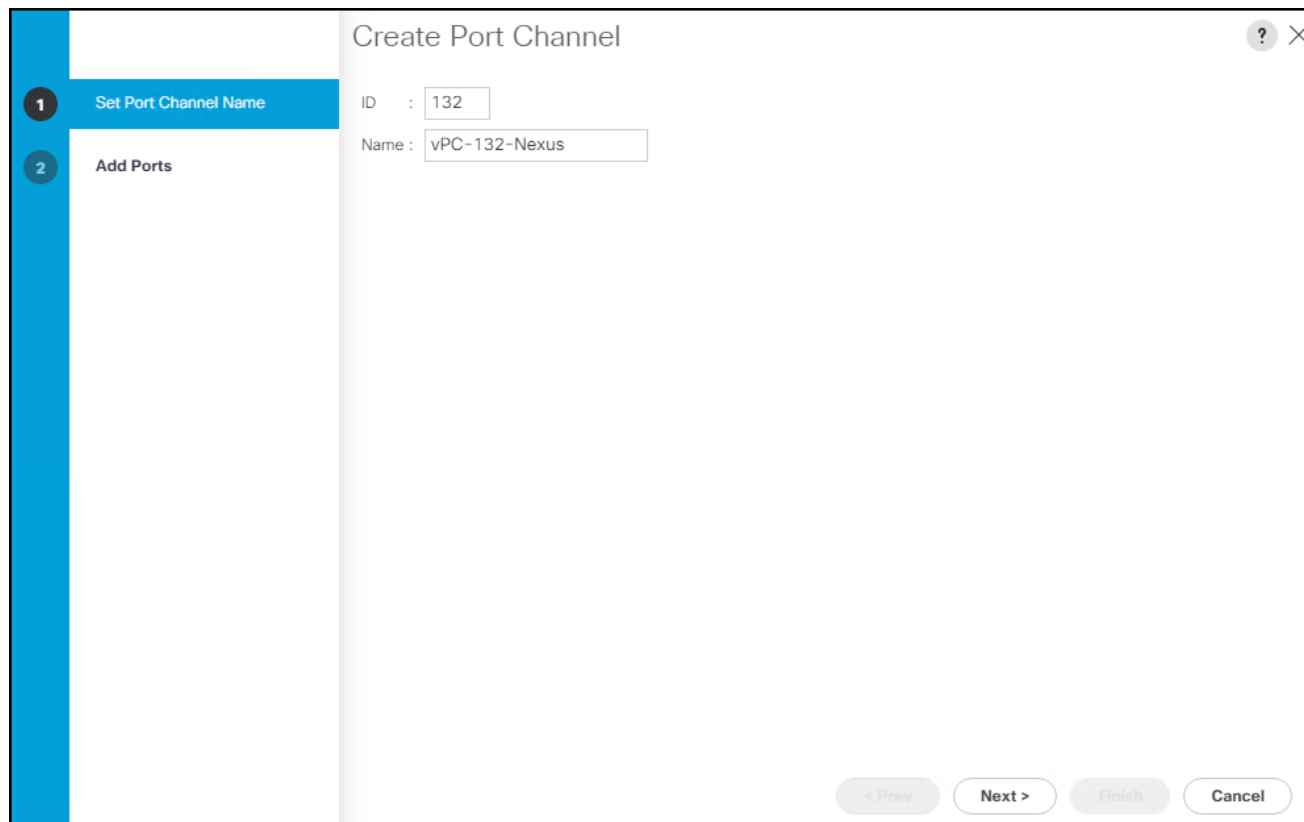
7. Click Next.

8. Select the following ports to add to the port channel:

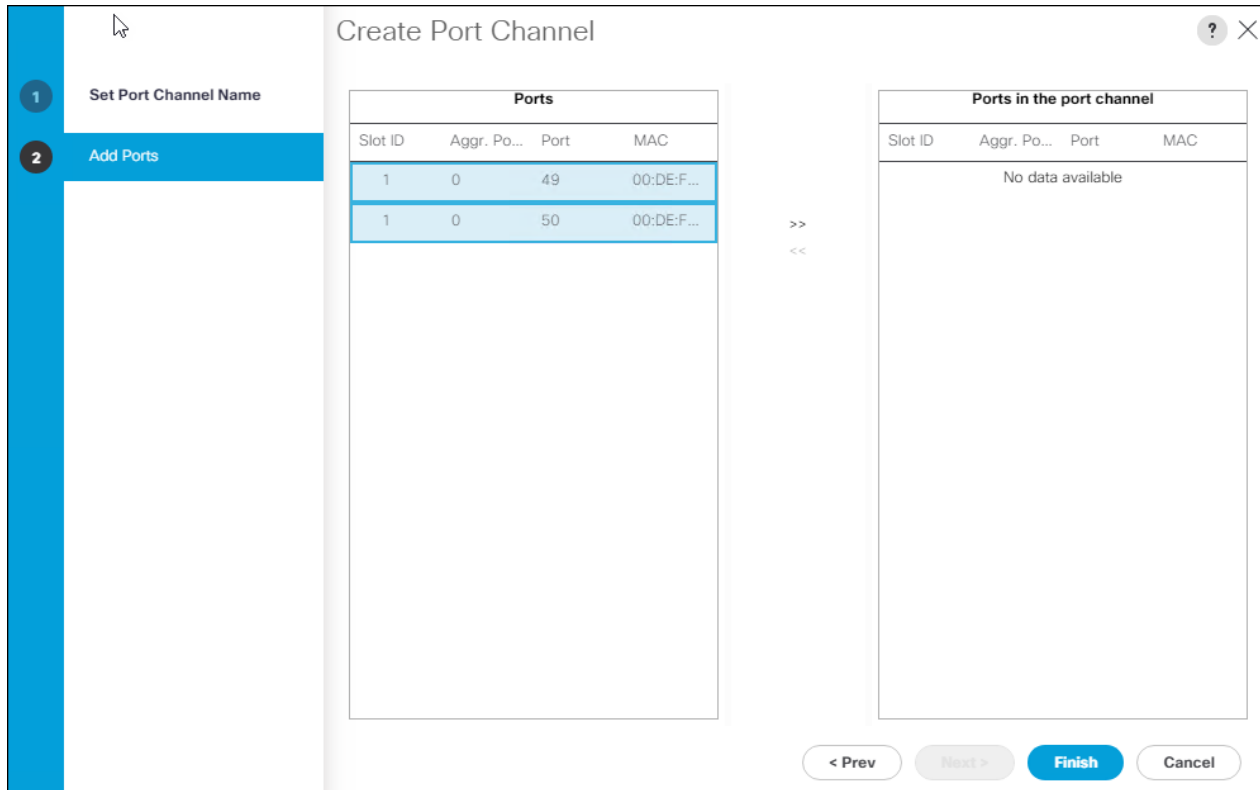
- a. Slot ID 1 and port 49
- b. Slot ID 1 and port 50



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 a unique ID for the port channel, (132 in our example to correspond with the upstream Nexus port channel).
16. With 132 selected, enter vPC-132-Nexus as the name of the port channel.



17. Click Next.
18. Select the following ports to add to the port channel:
 - a. Slot ID 1 and port 49
 - b. Slot ID 1 and port 50



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


20. Click Finish to create the port channel.

21. Click OK.

Create VLANs

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

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

 **In this procedure, six unique VLANs are created. See Table 2 for a list of VLANs to be created.**

2. Select LAN > LAN Cloud.

3. Right-click VLANs.

4. Select Create VLANs.

5. Enter Native-VLAN as the name of the VLAN to be used as the native VLAN.

6. Keep the Common/Global option selected for the scope of the VLAN.

7. Enter the native VLAN ID.

8. Keep the Sharing Type as None.

Create VLANs [?] [X]

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

9. Click OK and then click OK again.

10. Expand the list of VLANs in the navigation pane, right-click the newly created Native-VLAN and select Set as Native VLAN.

11. Click Yes and then click OK.

12. Right-click VLANs.

13. Select Create VLANs

14. Enter **IB-Mgmt** as the name of the VLAN to be used for management traffic.

15. Keep the Common/Global option selected for the scope of the VLAN.

16. Enter the In-Band management VLAN ID.

17. Keep the Sharing Type as None.

Create VLANs [?] [X]

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

18. Click OK and then click OK again.

19. Right-click VLANs.

20. Select Create VLANs.

21. Enter **vMotion** as the name of the VLAN to be used for vMotion.

22. Keep the Common/Global option selected for the scope of the VLAN.

23. Enter the vMotion VLAN ID.

24. Keep the Sharing Type as None.

25. Click OK and then click OK again.
26. Right-click VLANs.
27. Select Create VLANs.
28. Enter VM-App- as the prefix of the VLANs to be used for VM Traffic.
29. Keep the Common/Global option selected for the scope of the VLAN.
30. Enter the VM-Traffic VLAN ID range.
31. Keep the Sharing Type as None.

Create vNIC Templates

To create the multiple virtual network interface card (vNIC) templates for the Cisco UCS environment, follow the steps in this section.

Create Management vNICs

For the vNIC_Mgmt_A Template, follow these steps:

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. Select Primary Template for the Redundancy Type.
8. Leave Peer Redundancy Template as <not set>



Redundancy Type and specification of Redundancy Template are configuration options to later allow changes to the Primary Template to automatically adjust onto the Secondary Template.

9. Under Target, make sure that the VM checkbox is not selected.
10. Select Updating Template as the Template Type.
11. 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

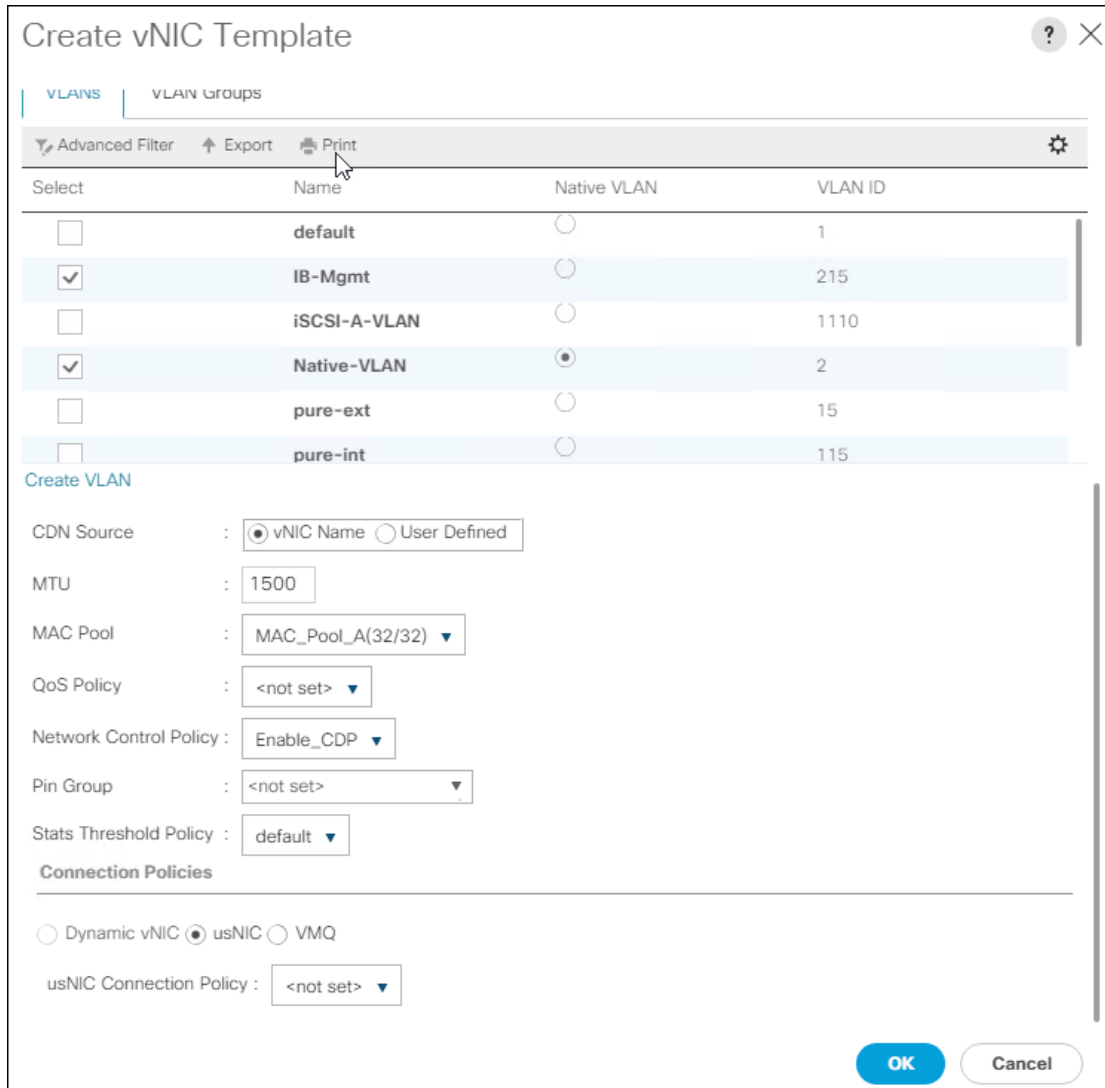
Template Type : Initial Template Updating Template

VLANs VLAN Groups

Advanced Filter Export Print ⚙

Select	Name	Native VLAN	VLAN ID
<input checked="" type="checkbox"/>	IB-Mgmt	<input type="radio"/>	215
<input type="checkbox"/>	iSCSI-A-VLAN	<input type="radio"/>	1110
<input checked="" type="checkbox"/>	Native-VLAN	<input checked="" type="radio"/>	2

12. Set Native-VLAN as the native VLAN.
13. Leave vNIC Name selected for the CDN Source.
14. Leave 1500 for the MTU.
15. In the MAC Pool list, select MAC_Pool_A.
16. In the Network Control Policy list, select Enable_CDP.



17. Click OK to create the vNIC template.

18. Click OK.

For the vNIC_Mgmt_B Template, follow these steps:

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. Select Secondary Template for Redundancy Type.

8. For the Peer Redundancy Template drop-down list, select vNIC_Mgmt_A.

With Peer Redundancy Template selected, Failover specification, Template Type, VLANs, CDN Source, MTU, and Network Control Policy are all pulled from the Primary Template.

9. 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 :

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

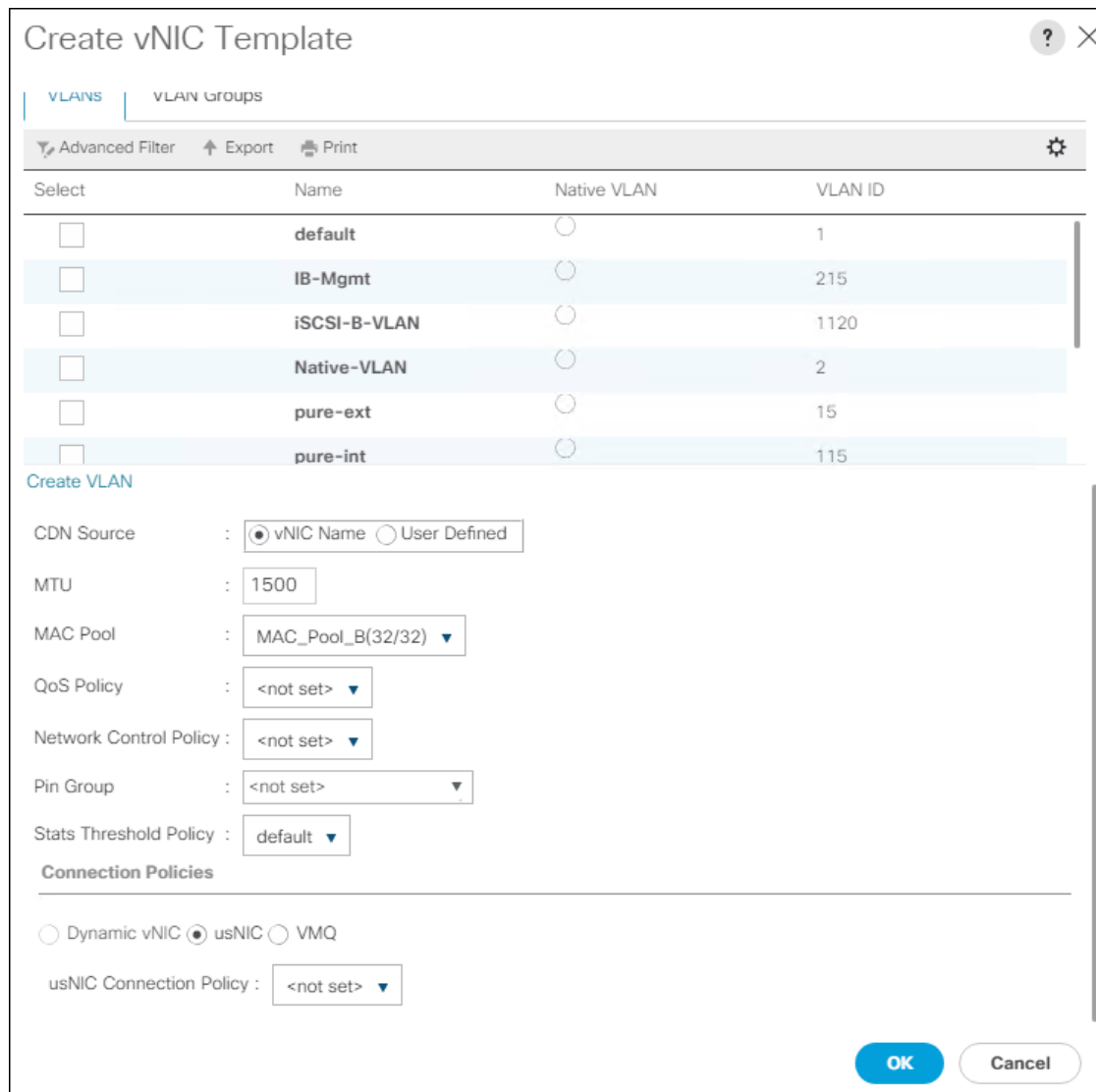
Template Type : Initial Template Updating Template

VLANs | VLAN Groups

Advanced Filter | Export | Print ⚙

Select	Name	Native VLAN	VLAN ID
<input type="checkbox"/>	default	<input type="radio"/>	1
<input type="checkbox"/>	IB-Mgmt	<input type="radio"/>	215
<input type="checkbox"/>	iSCSI-B-VLAN	<input type="radio"/>	1120
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>	?

10. In the MAC Pool list, select MAC_Pool_B.



11. Click OK to create the vNIC template.

12. Click OK.

Create vMotion vNICs

For the vNIC_vMotion_A Template, follow these steps:

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. Select Primary Template for the Redundancy Type.
8. Leave Peer Redundancy Template as <not set>
9. Under Target, make sure that the VM checkbox is not selected.
10. Select Updating Template as the Template Type.

Create vNIC Template

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

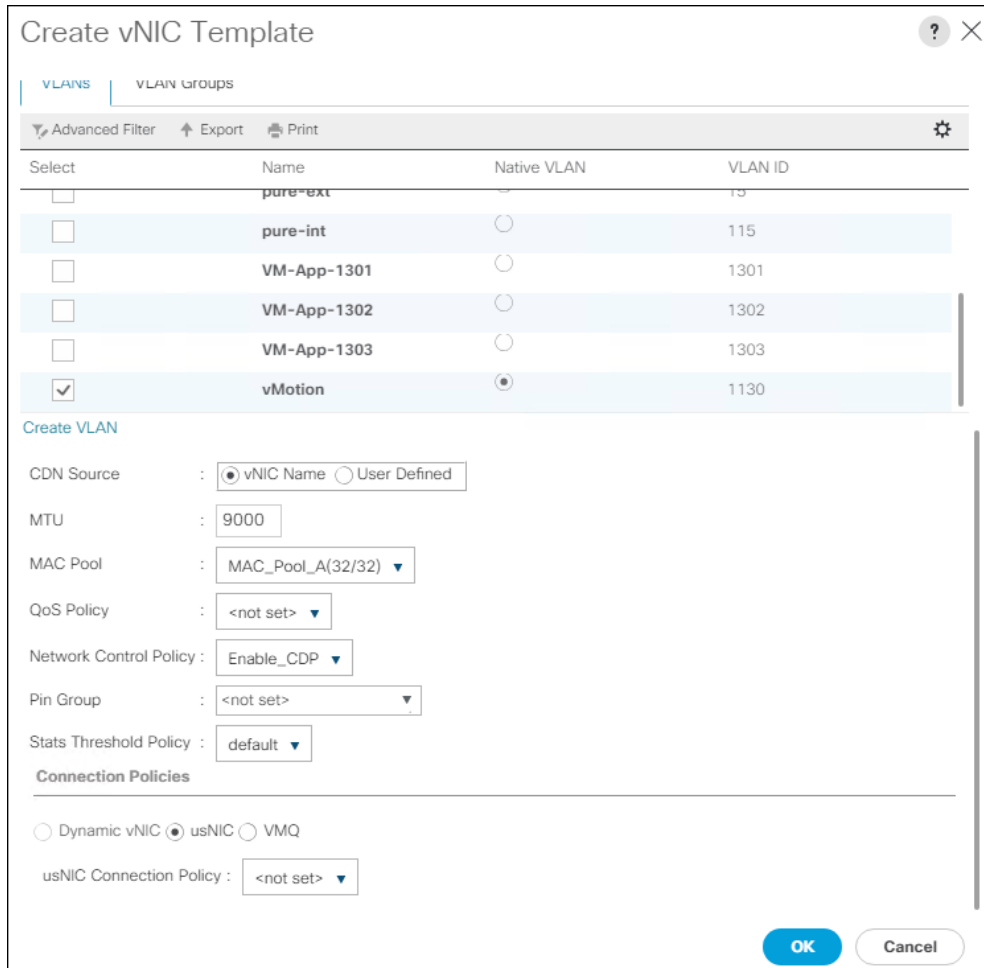
Template Type : Initial Template Updating Template

VLANs | VLAN Groups

Advanced Filter | Export | Print

Select	Name	Native VLAN	VLAN ID
<input type="checkbox"/>	default	<input type="radio"/>	1
<input type="checkbox"/>	IB-Mgmt	<input type="radio"/>	215
<input type="checkbox"/>	iSCSI-A-VLAN	<input type="radio"/>	1110
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>	2

11. Under VLANs, select the checkboxes vMotion and Native-VLAN.
12. Set vMotion as the native VLAN.
13. For MTU, enter 9000.
14. In the MAC Pool list, select MAC_Pool_A.
15. In the Network Control Policy list, select Enable_CDP.



16. Click OK to create the vNIC template.

17. Click OK.

For the vNIC_vMotion_B Template, follow these steps:

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. Select Secondary Template for Redundancy Type.
8. For the Peer Redundancy Template drop-down, select vNIC_vMotion_A.



With Peer Redundancy Template selected, MAC Pool will be the main configuration option left for this vNIC template.

9. 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 :

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

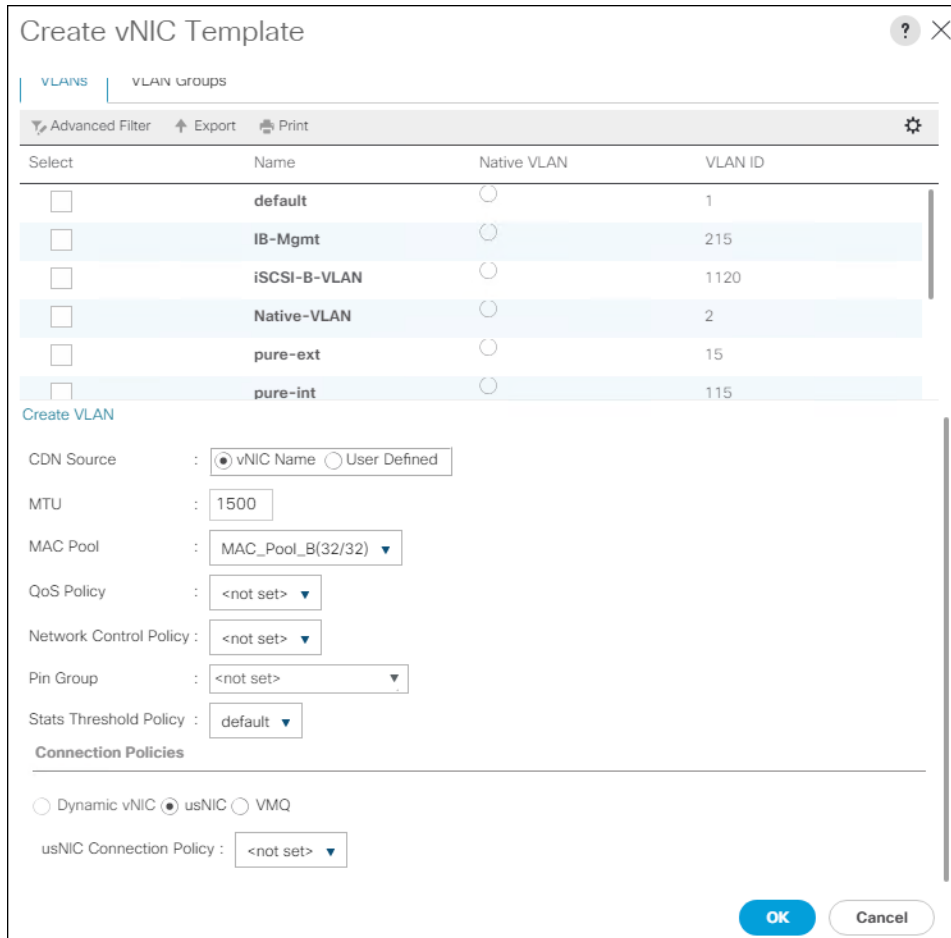
Template Type : Initial Template Updating Template

VLANs | VLAN Groups

Advanced Filter | Export | Print ⚙️

Select	Name	Native VLAN	VLAN ID
<input type="checkbox"/>	default	<input type="radio"/>	1
<input type="checkbox"/>	IB-Mgmt	<input type="radio"/>	215
<input type="checkbox"/>	iSCSI-B-VLAN	<input type="radio"/>	1120
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>	2

10. In the MAC Pool list, select MAC_Pool_B.



11. Click OK to create the vNIC template.

12. Click OK.

Create Application vNICs

For the vNIC_App_A Template, follow these steps:

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_App_A as the vNIC template name.
6. Keep Fabric A selected.
7. Optional: 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. Set default as the native VLAN.

Create vNIC Template

Name : vNIC_APP_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

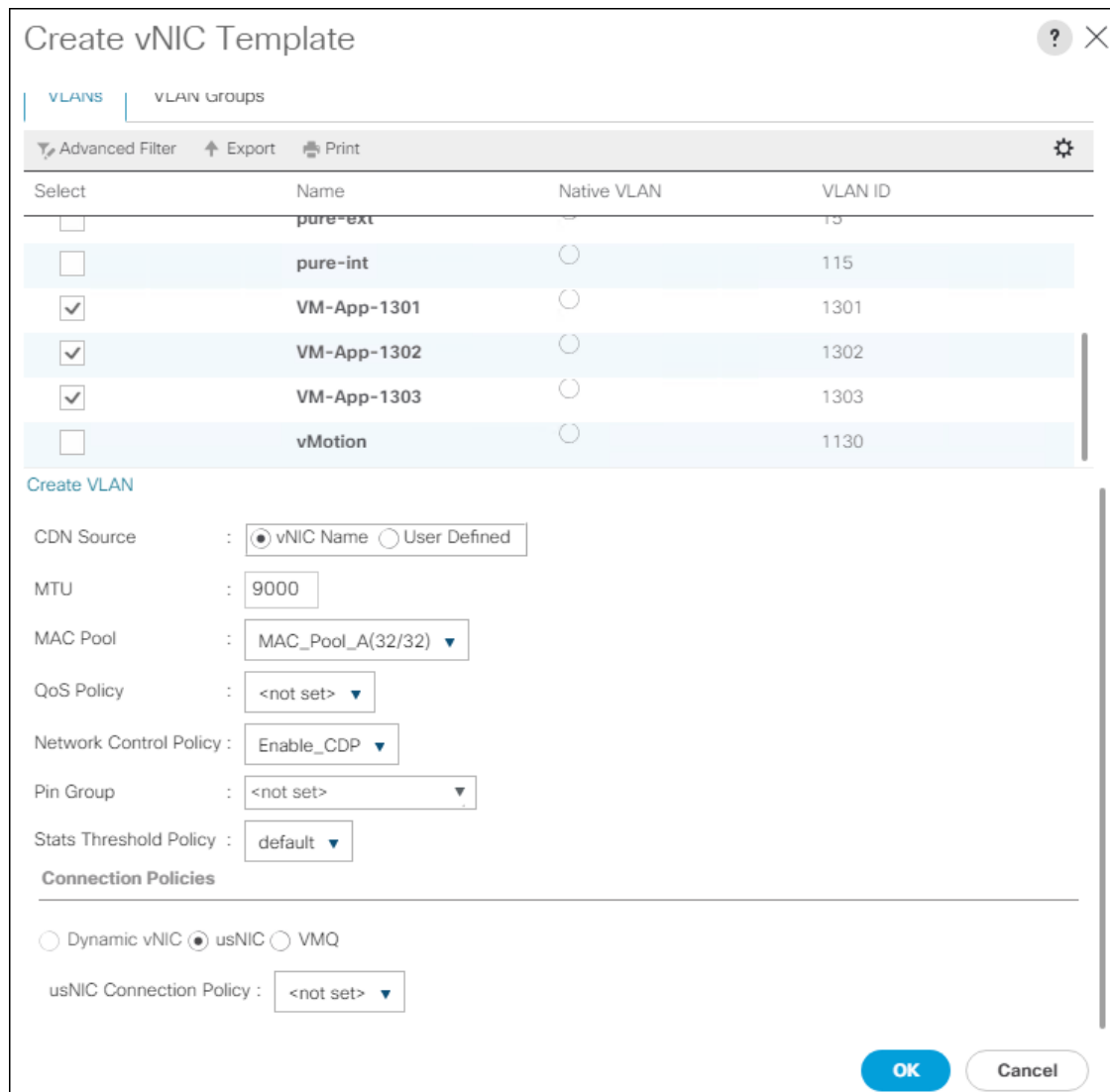
Template Type : Initial Template Updating Template

VLANs | VLAN Groups

Advanced Filter | Export | Print

Select	Name	Native VLAN	VLAN ID
<input checked="" type="checkbox"/>	default	<input checked="" type="radio"/>	1
<input type="checkbox"/>	IB-Mgmt	<input type="radio"/>	215
<input type="checkbox"/>	iSCSI-A-VLAN	<input type="radio"/>	1110
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>	2

13. Under VLANs, select the checkboxes for any application or production VLANs that should be delivered to the ESXi hosts.
14. For MTU, enter 9000.
15. In the MAC Pool list, select MAC_Pool_A.
16. In the Network Control Policy list, select Enable_CDP.



17. Click OK to create the vNIC template.

18. Click OK.

For the vNIC_App_B Templates, follow these steps:

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_App_B as the vNIC template name.
6. Select Fabric B.

7. Select Secondary Template for Redundancy Type.
8. For the Peer Redundancy Template drop-down, select vNIC_App_A.

 **With Peer Redundancy Template selected, MAC Pool will be the main configuration option left for this vNIC template.**

9. 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 :

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 | VLAN Groups

Advanced Filter | Export | Print ⚙

Select	Name	Native VLAN	VLAN ID
<input type="checkbox"/>	default	<input type="radio"/>	1
<input type="checkbox"/>	IB-Mgmt	<input type="radio"/>	215
<input type="checkbox"/>	iSCSI-B-VLAN	<input type="radio"/>	1120
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>	?

10. In the MAC Pool list, select MAC_Pool_B.

Create vNIC Template

VLANS | VLAN Groups

Advanced Filter | Export | Print

Select	Name	Native VLAN	VLAN ID
<input type="checkbox"/>	pure-ext	<input type="radio"/>	15
<input type="checkbox"/>	pure-int	<input type="radio"/>	115
<input type="checkbox"/>	VM-App-1301	<input type="radio"/>	1301
<input type="checkbox"/>	VM-App-1302	<input type="radio"/>	1302
<input type="checkbox"/>	VM-App-1303	<input type="radio"/>	1303
<input type="checkbox"/>	vMotion	<input type="radio"/>	1130

Create VLAN

CDN Source : vNIC Name User Defined

MTU : 1500

MAC Pool : MAC_Pool_B(32/32) ▼

QoS Policy : <not set> ▼

Network Control Policy : <not set> ▼

Pin Group : <not set> ▼

Stats Threshold Policy : default ▼

Connection Policies

Dynamic vNIC usNIC VMQ

usNIC Connection Policy : <not set> ▼

OK Cancel

11. Click OK to create the vNIC template.

12. Click OK.

Create VLANs ? X

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

13. Click OK and then click OK again.

14. Repeat as needed for any additional VLANs created on the upstream Nexus switches.

Create LAN Connectivity Policy

To configure the necessary FC Infrastructure LAN Connectivity Policy, follow these steps:

1. In Cisco UCS Manager, click LAN .
2. Select LAN > Policies > root.
3. Right-click LAN Connectivity Policies.
4. Select Create LAN Connectivity Policy.
5. Enter `FC-LAN-Policy` as the name of the policy.

Create LAN Connectivity Policy ? X

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
No data available		

🗑 Delete
➕ Add
ⓘ Modify

➕
Add iSCSI vNICs

OK
Cancel

6. Click the upper Add button to add a vNIC.
7. In the Create vNIC dialog box, enter 00-Mgmt-A as the name of the vNIC.



The numeric prefix of “00-“ and subsequent increments on the later vNICs are used in the vNIC naming to force the device ordering through Consistent Device Naming (CDN). Without this, some operating systems might not respect the device ordering that is set within Cisco UCS.

8. Select the Use vNIC Template checkbox.
9. In the vNIC Template list, select 00-Mgmt-A.
10. In the Adapter Policy list, select VMWare.
11. Click OK to add this vNIC to the policy.

Create vNIC [?] [X]

Name :

Use vNIC Template :

Redundancy Pair :

Peer Name :

vNIC Template : [Create vNIC Template](#)

Adapter Performance Profile

Adapter Policy : [Create Ethernet Adapter 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 01-Mgmt-B.
16. In the Adapter Policy list, select VMWare.

Create vNIC

Name :

Use vNIC Template :

Redundancy Pair :

vNIC Template :

Peer Name :

Adapter Performance Profile

Adapter Policy :

Buttons:

17. Click OK to add the vNIC to the policy.
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 :

vNIC Template :

Peer Name :

[Create vNIC Template](#)

Adapter Performance Profile

Adapter Policy :

[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 ? X

Name :

Use vNIC Template :

Redundancy Pair : Peer Name :

vNIC Template : [Create vNIC Template](#)

Adapter Performance Profile

Adapter Policy : [Create Ethernet Adapter Policy](#)

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

Create vNIC ? X

Name :

Use vNIC Template :

Redundancy Pair :

Peer Name :

vNIC Template :

[Create vNIC Template](#)

Adapter Performance Profile

Adapter Policy :

[Create Ethernet Adapter Policy](#)

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

37. In the Create vNIC dialog box, enter **05-App-B** as the name of the vNIC.

38. Select the Use vNIC Template checkbox.

39. In the vNIC Template list, select vNIC_App_B.

40. In the Adapter Policy list, select VMWare.

Create vNIC

Name :

Use vNIC Template :

Redundancy Pair :

Peer Name :

vNIC Template :

[Create vNIC Template](#)

Adapter Performance Profile

Adapter Policy :

[Create Ethernet Adapter Policy](#)

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

Create LAN Connectivity Policy ? X

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-App-B	Derived	
vNIC 04-App-A	Derived	
vNIC 03-vMotion-B	Derived	
vNIC 02-vMotion-A	Derived	
vNIC 01-Mgmt-B	Derived	
vNIC 00-Mgmt-A	Derived	

🗑 Delete ➕ Add ℹ Modify

➕ Add iSCSI vNICs

OK
Cancel

42. Click OK again to create the LAN Connectivity Policy.

Configure FC SAN Connectivity

These Fibre Channel configuration steps will enable the FlashStack for provisioning of volumes to be used as datastores by the FlashStack vSphere hosts, and the creation of UCS Service Profiles that will be configured to boot from Fibre Channel LUNs.

Configure Unified Ports


The Cisco UCS 6454 Fabric Interconnects will have a slider mechanism within the Cisco UCS Manager GUI interface that will control the first 8 ports starting from the first port, and configured in increments of the first 4 or 8 of the unified ports.

To enable the fibre channel ports, follow these steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane.
2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary)

3. Select Configure Unified Ports.
4. Click Yes on the pop-up window warning that changes to the fixed module will require a reboot of the fabric interconnect and changes to the expansion module will require a reboot of that module.
5. Within the Configured Fixed Ports pop-up window move the gray slider bar from the left to the right to select either 4 or 8 ports to be set as FC Uplinks.

Configure Unified Ports ? X



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	FC Uplink
Port 4	ether	Ethernet Uplink	FC Uplink
Port 5	ether	Unconfigured	FC Uplink
Port 6	ether	Unconfigured	FC Uplink
Port 7	ether	Unconfigured	FC Uplink
Port 8	ether	Unconfigured	FC Uplink

■ Up
 ■ Admin Down
 ■ Fail
 ■ Link Down

OK
Cancel

6. Click OK to continue
7. Select Equipment > Fabric Interconnects > Fabric Interconnect B (primary)
8. Select Configure Unified Ports.
9. Click Yes on the pop-up window warning that changes to the fixed module will require a reboot of the fabric interconnect and changes to the expansion module will require a reboot of that module.
10. Within the Configured Fixed Ports pop-up window move the gray slider bar from the left to the right to select either 4 or 8 ports to be set as FC Uplinks.
11. Click OK to continue

The Fabric Interconnects will reboot and reconnect to Cisco UCS Manager after they are back up.

Create VSANs

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

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



In this procedure two VSANs are created.

2. Select SAN > SAN Cloud.
3. Right-click VSANs.
4. Select Create VSAN.
5. Enter `VSAN_A` as the name of the VSAN to be used for Fabric A.
6. Leave Disabled selected for FC Zoning.
7. Select Fabric A.
8. Enter a unique VSAN ID and a corresponding FCoE VLAN ID.



It is recommended use the same ID for both parameters and to use something other than 1.

Create 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 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 :

9. Click OK and then click OK again.
10. Under SAN Cloud, right-click VSANs.
11. Select Create VSAN.
12. Enter **VSAN_B** as the name of the VSAN to be used for Fabric B.
13. Leave Disabled selected for FC Zoning.
14. Select Fabric B.
15. Enter a unique VSAN ID and a corresponding FCoE VLAN ID. It is recommended use the same ID for both parameters and to use something other than 1.

Create 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 :

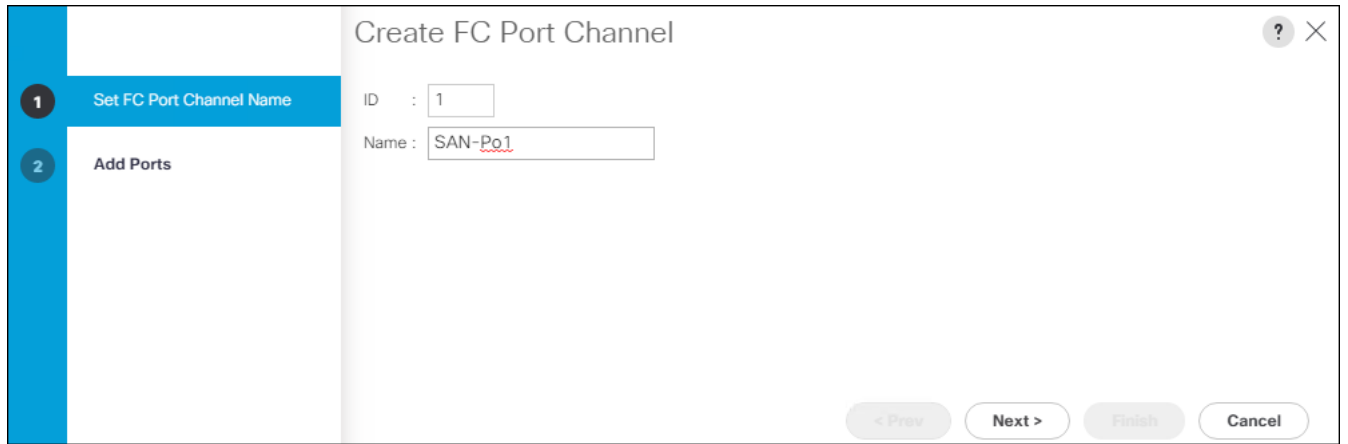
16. Click OK and then click OK again.

Create FC Port Channels

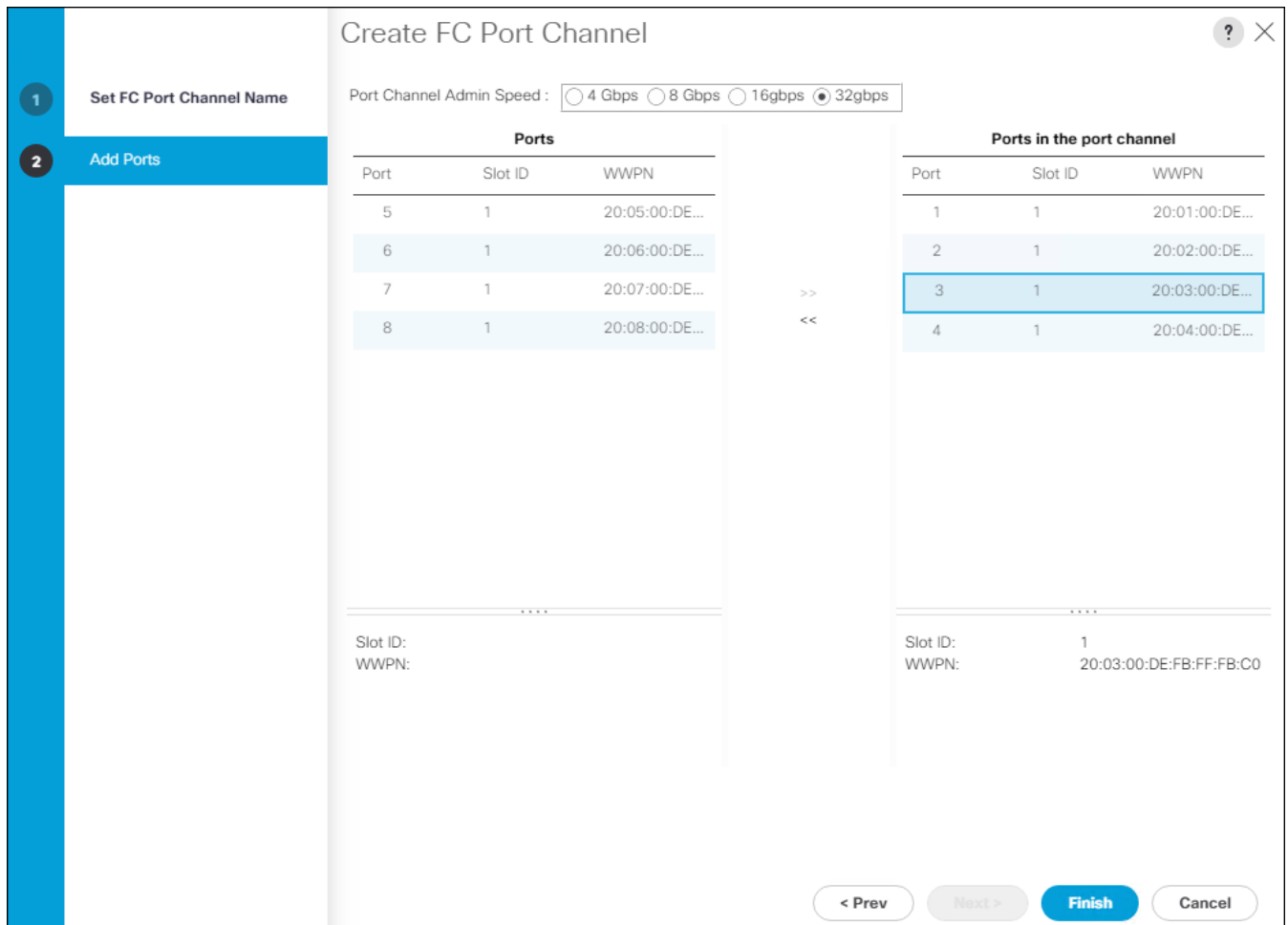
To configure the necessary port channels for the Cisco UCS environment, follow these steps:

Fabric A

1. In the navigation pane under SAN > SAN Cloud expand the Fabric A tree.
2. Right-click FC Port Channels.
3. Select Create FC Port Channel.
4. Enter 1 for the ID and SAN-Po1 for the Port Channel name.



5. Click Next then choose appropriate ports and click >> to add the ports to the port channel.

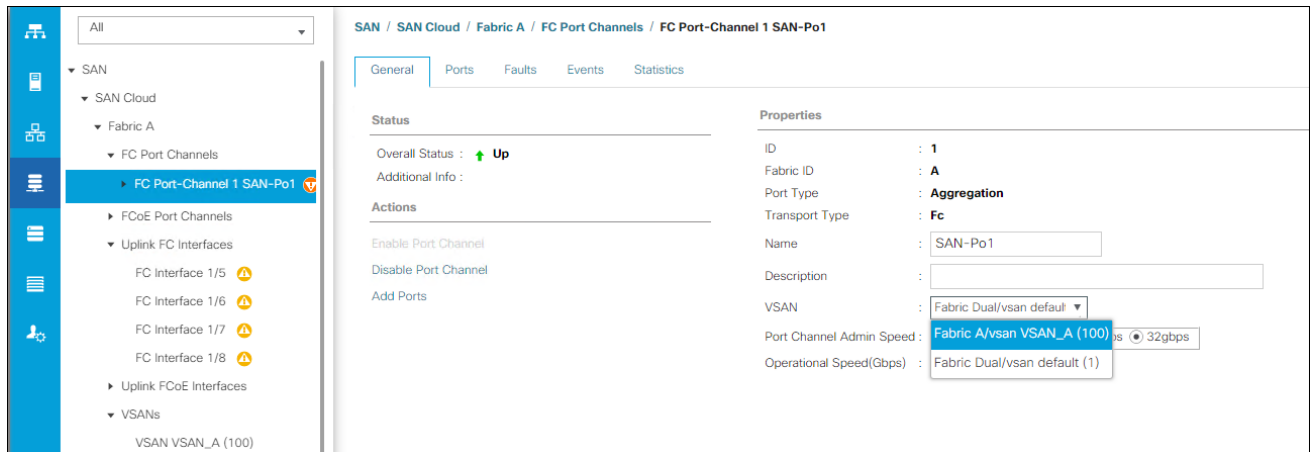


6. Click Finish.

7. Click OK.

8. Select the newly created Port-Channel.

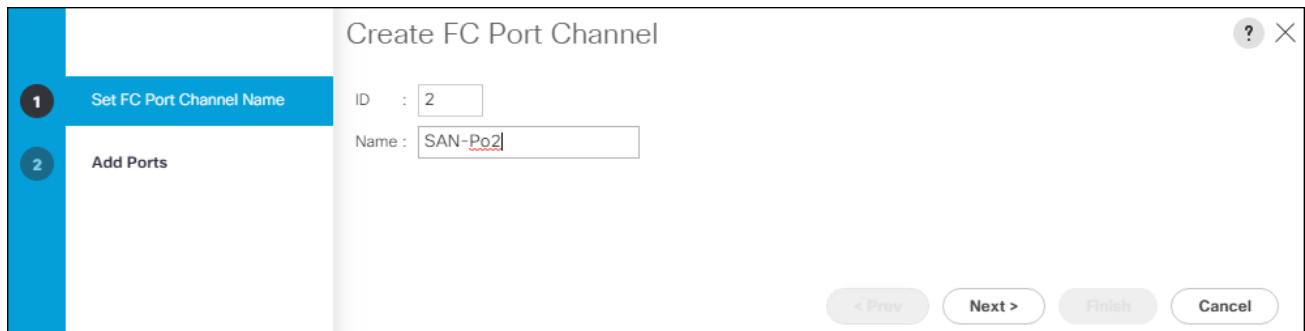
9. Under the VSAN drop-down for Port-Channel SAN-Po1, select **VSAN_A 100**



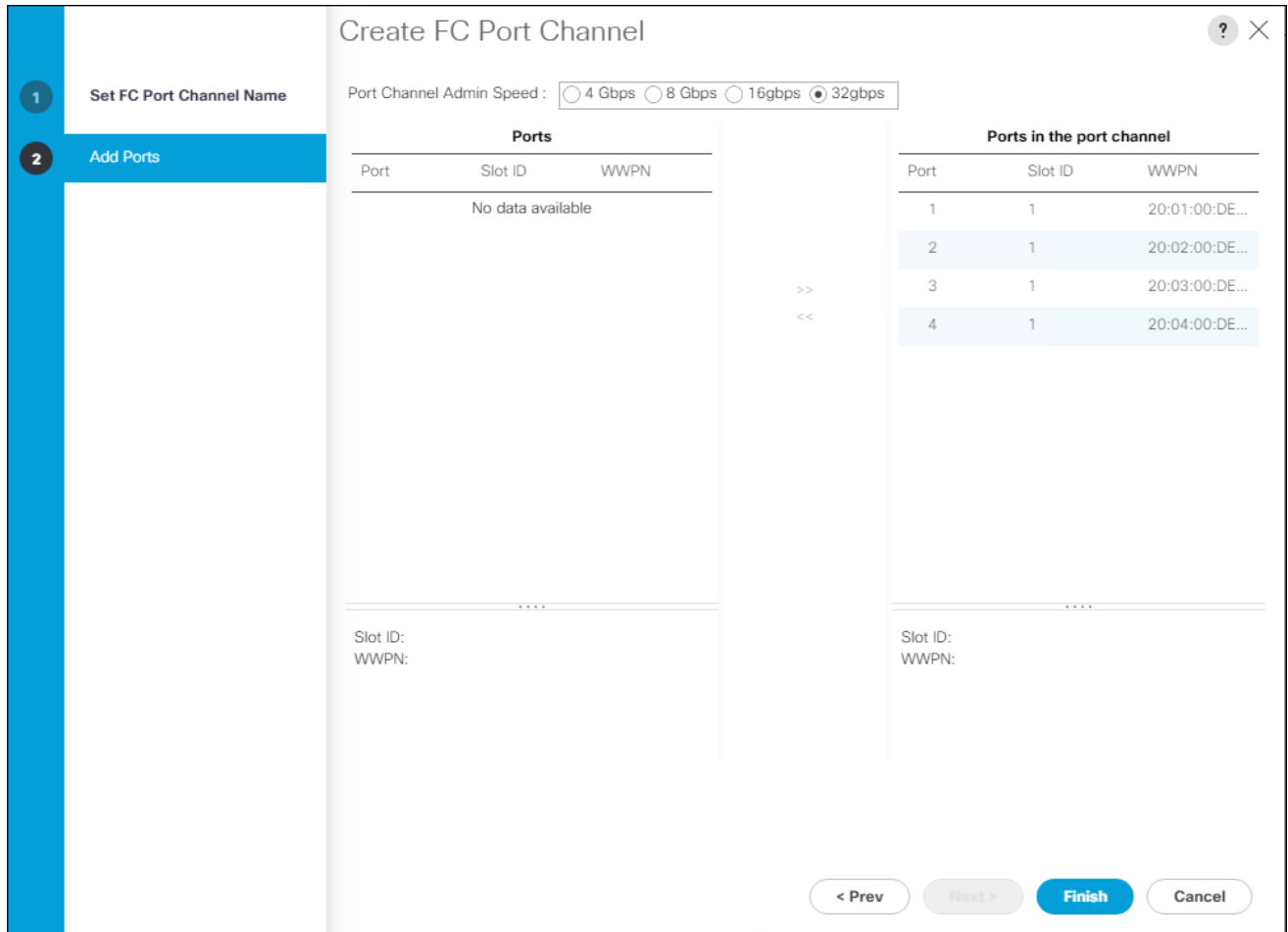
10. Click Save Changes and then click OK.

Fabric B

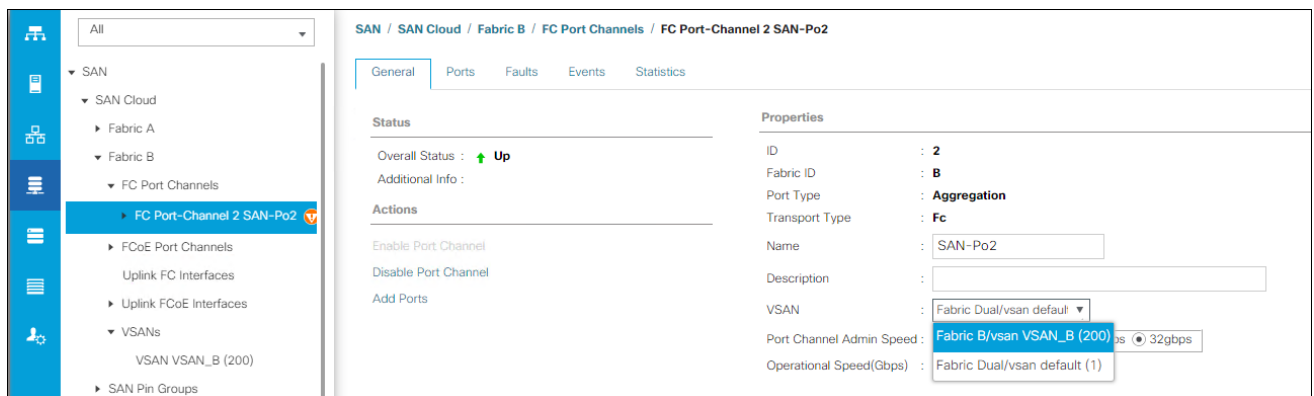
1. In the navigation pane under SAN > SAN Cloud expand the Fabric B tree.
2. Right-click FC Port Channels.
3. Select Create Port Channel.
4. Enter 2 for the ID and SAN-Po2 for the Port Channel name.



5. Click Next then choose the appropriate ports and click >> to add the ports to the port channel.



6. Click Finish.
7. Click OK.
8. Select the newly created Port-Channel.
9. From the VSAN drop-down list for Port-Channel SAN-Po2, select VSAN_A 200.



10. Click Save Changes and then click OK.

Create vHBA Templates

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

1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Select Policies > root.
3. Right-click vHBA Templates.
4. Select Create vHBA Template.
5. Enter `vHBA_Template_A` as the vHBA template name.
6. Keep Fabric A selected.
7. Leave Redundancy Type as No Redundancy.
8. Select `VSAN_A`.
9. Leave Initial Template as the Template Type.
10. Select `WWPN_Pool_A` as the WWPN Pool.
11. Click OK to create the vHBA template.

Create vHBA Template
?
✕

Name :

Description :

Fabric ID : A B

Redundancy

Redundancy Type : No Redundancy Primary Template Secondary Template

Select VSAN : [Create VSAN](#)

Template Type : Initial Template Updating Template

Max Data Field Size :

WWPN Pool : ▼

QoS Policy : ▼

Pin Group : ▼

Stats Threshold Policy : ▼

12. Click OK.
13. Right-click vHBA Templates.
14. Select Create vHBA Template.
15. Enter `vHBA_Template_B` as the vHBA template name.
16. Select Fabric B.
17. Leave Redundancy Type as No Redundancy.
18. Select VSAN_B.
19. Leave Initial Template as the Template Type.
20. Select WWPN_Pool_B as the WWPN Pool.
21. Click OK to create the vHBA template.

Create vHBA Template ? X

Name :

Description :

Fabric ID : A B

Redundancy

Redundancy Type : No Redundancy Primary Template Secondary Template

Select VSAN : [Create VSAN](#)

Template Type : Initial Template Updating Template

Max Data Field Size :

WWPN Pool :

QoS Policy :

Pin Group :

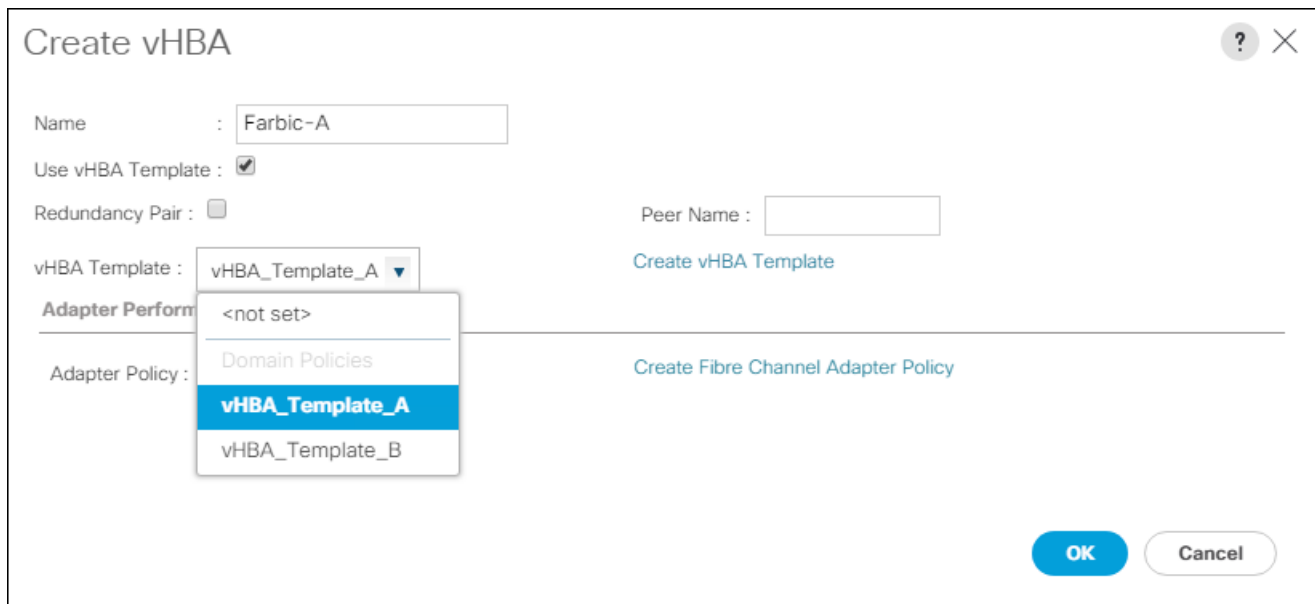
Stats Threshold Policy :

22. Click OK.

Create SAN Connectivity Policy

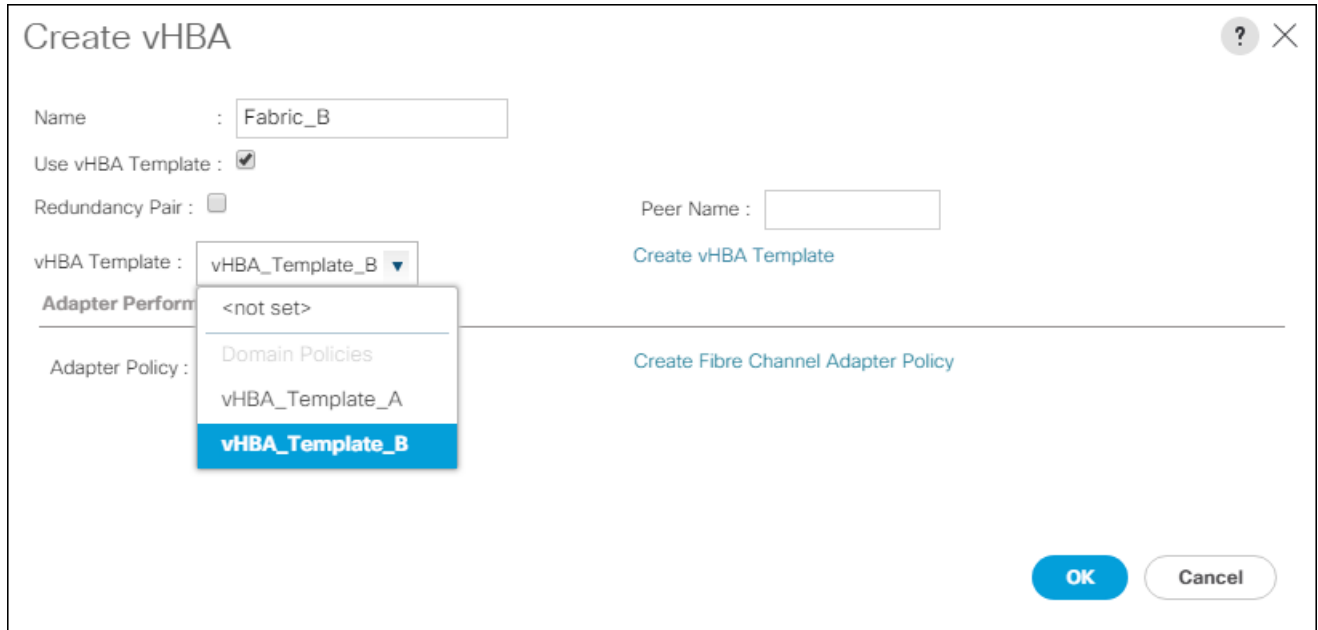
To configure the necessary Infrastructure SAN Connectivity Policy, follow these steps:

1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Select SAN > Policies > root.
3. Right-click SAN Connectivity Policies.
4. Select Create SAN Connectivity Policy.
5. Enter Infra-SAN-Policy as the name of the policy.
6. Select the previously created WWNN_Pool for the WWNN Assignment.
7. Click the Add button at the bottom to add a vHBA.
8. In the Create vHBA dialog box, enter **Fabric-A** as the name of the vHBA.
9. Select the Use vHBA Template checkbox.
10. Leave Redundancy Pair unselected.
11. In the vHBA Template list, select vHBA_Template_A.



12. In the Adapter Policy list, select VMWare.
13. Click OK.
14. Click the Add button at the bottom to add a second vHBA.
15. In the Create vHBA dialog box, enter Fabric-B as the name of the vHBA.

- 16. Select the Use vHBA Template checkbox.
- 17. Leave Redundancy Pair unselected.
- 18. In the vHBA Template list, select vHBA_Template_B.



- 19. In the Adapter Policy list, select VMWare.
- 20. Click OK.

Create SAN Connectivity Policy ? X

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 Fabric-A	Derived

🗑 Delete ➕ Add ⓘ Modify

OK
Cancel

21. Click OK to create the SAN Connectivity Policy.

22. Click OK to confirm creation.

Create Boot Policy

This procedure will define the Primary and Secondary Boot Targets for each Fabric side (A/B). These will be the WWNs that need to be collected from the first adapter of each controller on the Pure Storage FlashArray that are visible from the Connections tab under the Health section of the FlashArray Web GUI.

The screenshot shows the 'Health' section with the 'Connections' tab selected. Below the navigation tabs, there's a 'Host Connections' section with a search bar and a dropdown for 'All Paths'. The main table, 'Array Ports', has the following data:

Port	Name	Speed	Fallover	Port	Name	Speed	Fallover
CT0.FC0	52:4A:93:7C:2B:9B:9F:00	0		CT1.FC0	52:4A:93:7C:2B:9B:9F:10	0	
CT0.FC1	52:4A:93:7C:2B:9B:9F:01	0		CT1.FC1	52:4A:93:7C:2B:9B:9F:11	0	
CT0.FC2	52:4A:93:7C:2B:9B:9F:02	32 Gb/s		CT1.FC2	52:4A:93:7C:2B:9B:9F:12	32 Gb/s	
CT0.FC3	52:4A:93:7C:2B:9B:9F:03	32 Gb/s		CT1.FC3	52:4A:93:7C:2B:9B:9F:13	32 Gb/s	
CT0.FC8	52:4A:93:7C:2B:9B:9F:08	0		CT1.FC8	52:4A:93:7C:2B:9B:9F:16	0	
CT0.FC9	52:4A:93:7C:2B:9B:9F:09	0		CT1.FC9	52:4A:93:7C:2B:9B:9F:17	0	

As an alternative to the GUI, connect to the FlashArray//X via ssh using the pureuser account and find the WWNs using the pureport list command:

```

pureuser@cspg-rtp-1> pureport list
Name      WWN          Portal      IQN          Fallover
CT0.FC0   52:4A:93:7C:2B:9B:9F:00 - - -
CT0.FC1   52:4A:93:7C:2B:9B:9F:01 - - -
CT0.FC2   52:4A:93:7C:2B:9B:9F:02 - - -
CT0.FC3   52:4A:93:7C:2B:9B:9F:03 - - -
CT0.FC8   52:4A:93:7C:2B:9B:9F:08 - - -
CT0.FC9   52:4A:93:7C:2B:9B:9F:09 - - -
CT1.FC0   52:4A:93:7C:2B:9B:9F:10 - - -
CT1.FC1   52:4A:93:7C:2B:9B:9F:11 - - -
CT1.FC2   52:4A:93:7C:2B:9B:9F:12 - - -
CT1.FC3   52:4A:93:7C:2B:9B:9F:13 - - -
CT1.FC8   52:4A:93:7C:2B:9B:9F:16 - - -
CT1.FC9   52:4A:93:7C:2B:9B:9F:17 - - -
    
```

Find the FC0 adapters for each controller from within the System view and record the values to be used for Primary and Secondary Targets. In the example lab environment, these appear as the first ports on the right side of each controller shown.

	Port Name	Target Role	Example WWPN	Customer WWPN
FlashArray//X Controller 0	CT0.FC0	Primary	52:4A:93:7C:2B:9B:9F:00	

	Port Name	Target Role	Example WWPN	Customer WWPN
FlashArray//X Controller 1	CT1.FC0	Secondary	52:4A:93:7C:2B:9B:9F:10	

Within the same System view, find the FC1 adapters for each controller and record the values to be used for Primary and Secondary Targets. In the example lab environment, these appear as the second ports on the right side of each controller shown.

	Port Name	Target Role	Example WWPN	Customer WWPN
FlashArray//X Controller 0	CT0.FC1	Primary	52:4A:93:7C:2B:9B:9F:01	
FlashArray//X Controller 1	CT1.FC1	Secondary	52:4A:93:7C:2B:9B:9F:11	

To create boot policies for the Cisco UCS environment, follow these steps:

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



Do not select the Reboot on Boot Order Change checkbox.

7. Expand the Local Devices drop-down menu and select Add Remote CD/DVD.
8. Expand the vHBAs drop-down menu and select Add SAN Boot.
9. In the Add SAN Boot dialog box, enter Fabric-A in the vHBA field.
10. Confirm that Primary is selected for the Type option.

Add SAN Boot ? X

vHBA :

Type : Primary Secondary Any

11. Click OK to add the SAN boot initiator.
12. From the vHBA drop-down menu, select Add SAN Boot Target.
13. Enter 1 as the value for Boot Target LUN.
14. Enter the WWPN for CT0.FC0 recorded in Table 14.
15. Select Primary for the SAN boot target type.

Add SAN Boot Target ? X

Boot Target LUN : 1

Boot Target WWPN : 52:4A:93:7C:2B:9B:9F:00

Type : Primary Secondary

OK Cancel

16. Click OK to add the SAN boot target.
17. From the vHBA drop-down menu, select Add SAN Boot Target.
18. Enter 1 as the value for Boot Target LUN.
19. Enter the WWPN for CT1.FC0 recorded in Table 14.

Add SAN Boot Target ? X

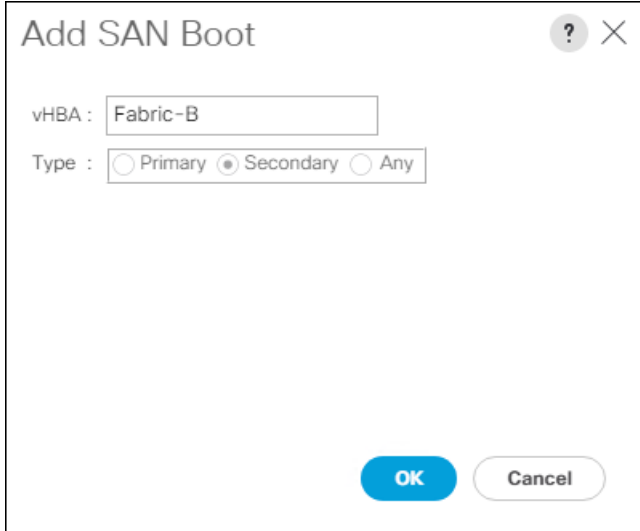
Boot Target LUN : 1

Boot Target WWPN : 52:4A:93:7C:2B:9B:9F:10

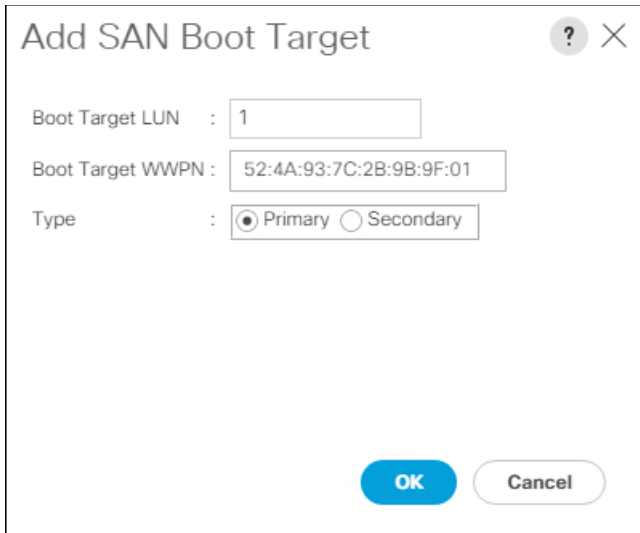
Type : Primary Secondary

OK Cancel

- 20. Click OK to add the SAN boot target.
- 21. From the vHBA drop-down menu, select Add SAN Boot.
- 22. In the Add SAN Boot dialog box, enter Fabric-B in the vHBA box.



- 23. Click OK to add the SAN boot initiator.
- 24. From the vHBA drop-down menu, select Add SAN Boot Target.
- 25. Enter 1 as the value for Boot Target LUN.
- 26. Enter the WWPN for CT0.FC1 recorded in Table 14.
- 27. Select Primary for the SAN boot target type.



- 28. Click OK to add the SAN boot target.

29. From the vHBA drop-down list, select Add SAN Boot Target.

30. Enter 1 as the value for Boot Target LUN.

31. Enter the WWPN for CT1.FC1 recorded in Table 15.

Add SAN Boot Target ? X

Boot Target LUN : 1

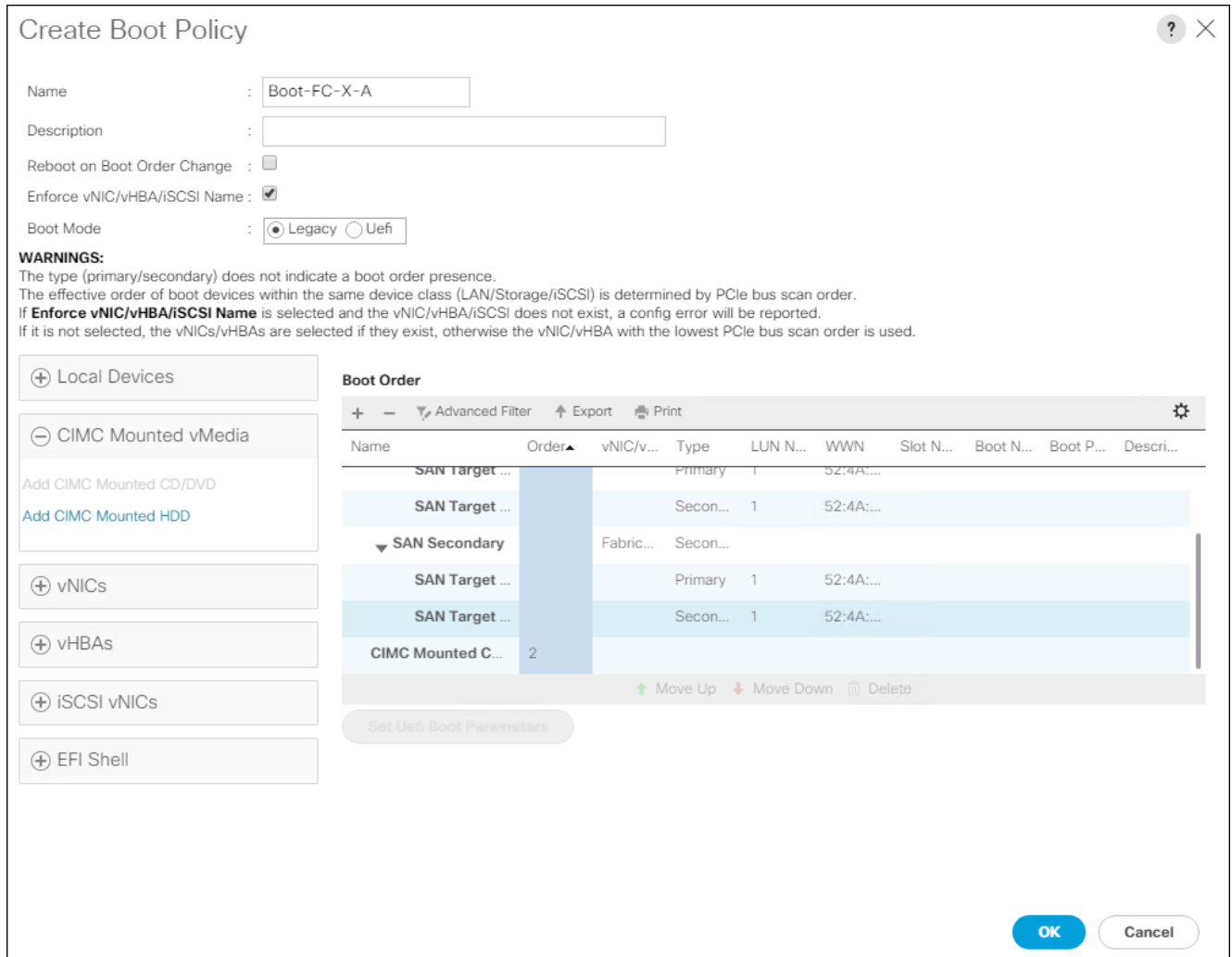
Boot Target WWPN : 52:4A:93:7C:2B:9B:9F:11

Type : Primary Secondary

OK Cancel

32. Click OK to add the SAN boot target.

33. Expand CIMC Mounted Media and select Add CIMC Mounted CD/DVD.



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

Create Service Profile Templates

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

To create the service profile template, follow these 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-FC-A as the name of the service profile template. This service profile template is configured to boot from FlashArray//X70 R2 controller 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.

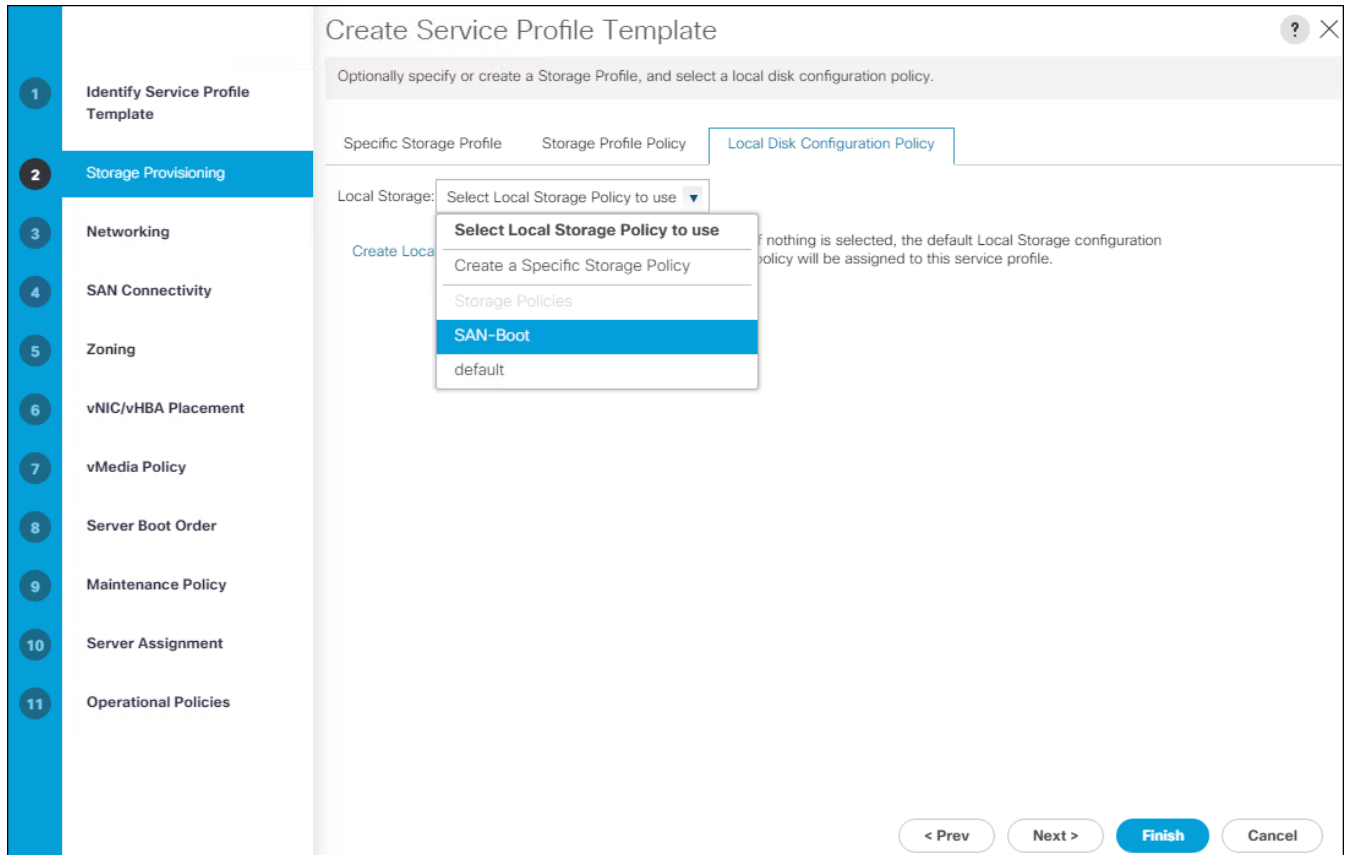
Optionally enter a description for the profile. The description can contain information about when and where the service profile should be used.

8. Click Next.

Configure Storage Provisioning

To configure storage provisioning, follow these steps:

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



3. Click Next.

Configure Networking Options

To configure the network options, follow these steps:

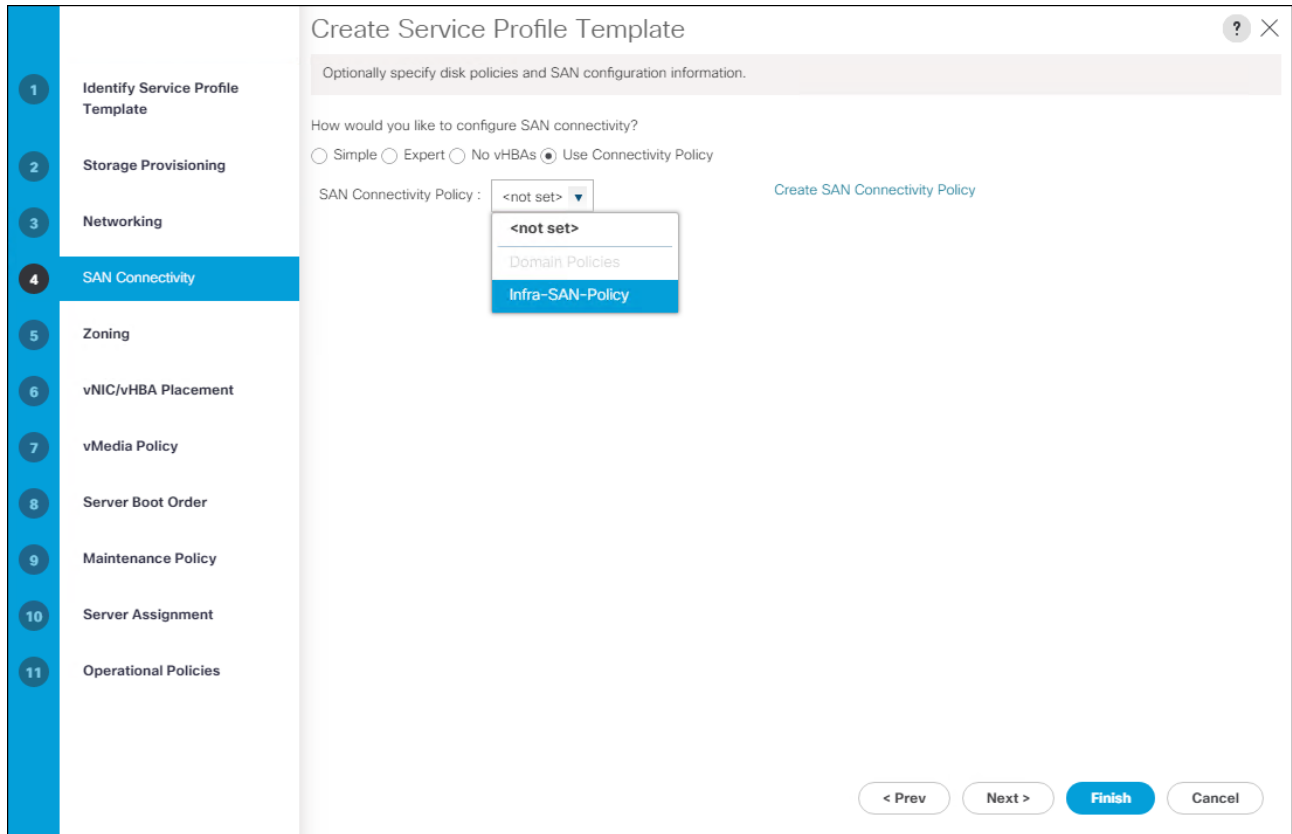
1. Keep the default setting for Dynamic vNIC Connection Policy.
2. Select the "Use Connectivity Policy" option to configure the LAN connectivity.
3. Select FC-LAN-Policy from the LAN Connectivity Policy drop-down list.

4. Click Next.

Configure SAN Connectivity Options

To configure the SAN connectivity options, follow these steps:

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



Configure Zoning Options

1. Leave Zoning configuration unspecified and click Next.

Configure vNIC/HBA Placement

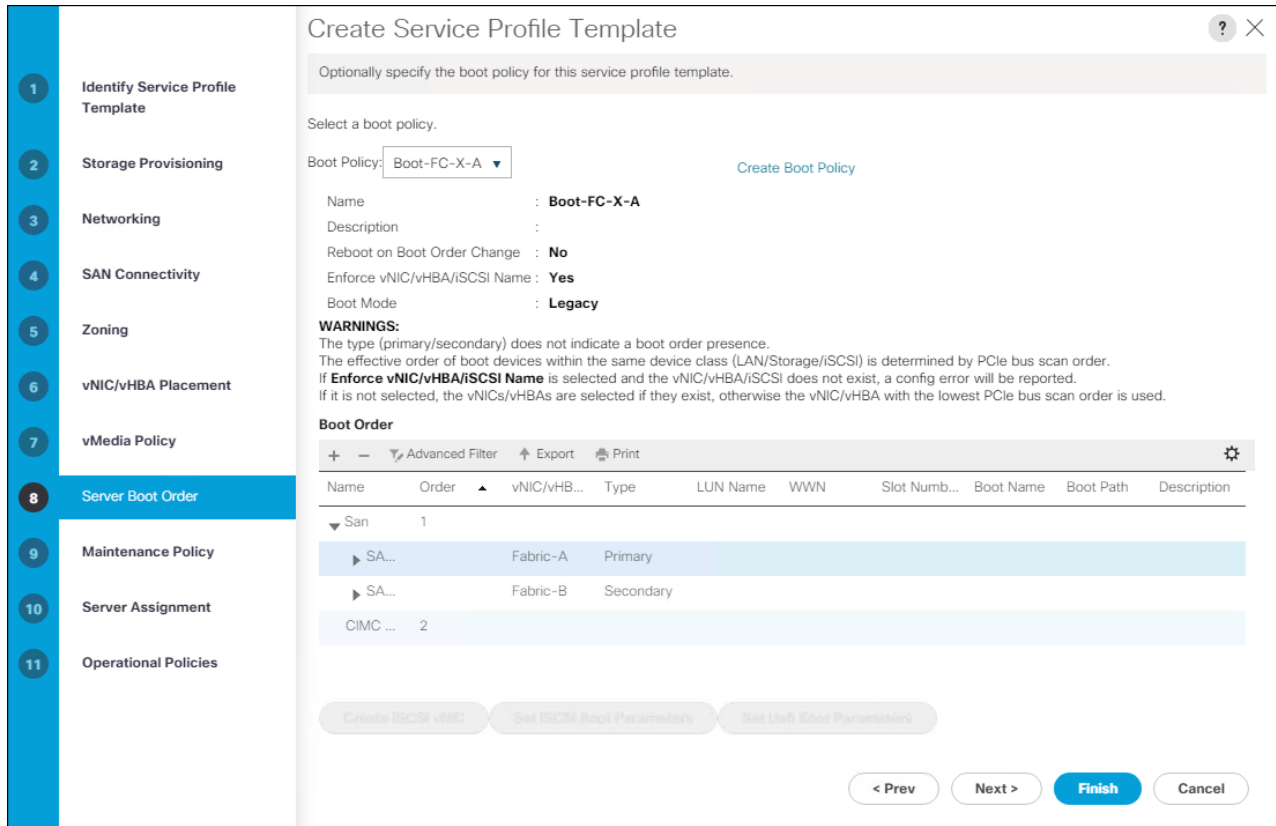
1. In the “Select Placement” list, leave the placement policy as “Let System Perform Placement”.
2. Click Next.

Configure vMedia Policy

1. Do not select a vMedia Policy.
2. Click Next.

Configure Server Boot Order

1. Select **Boot-FC-X-A** for Boot Policy.

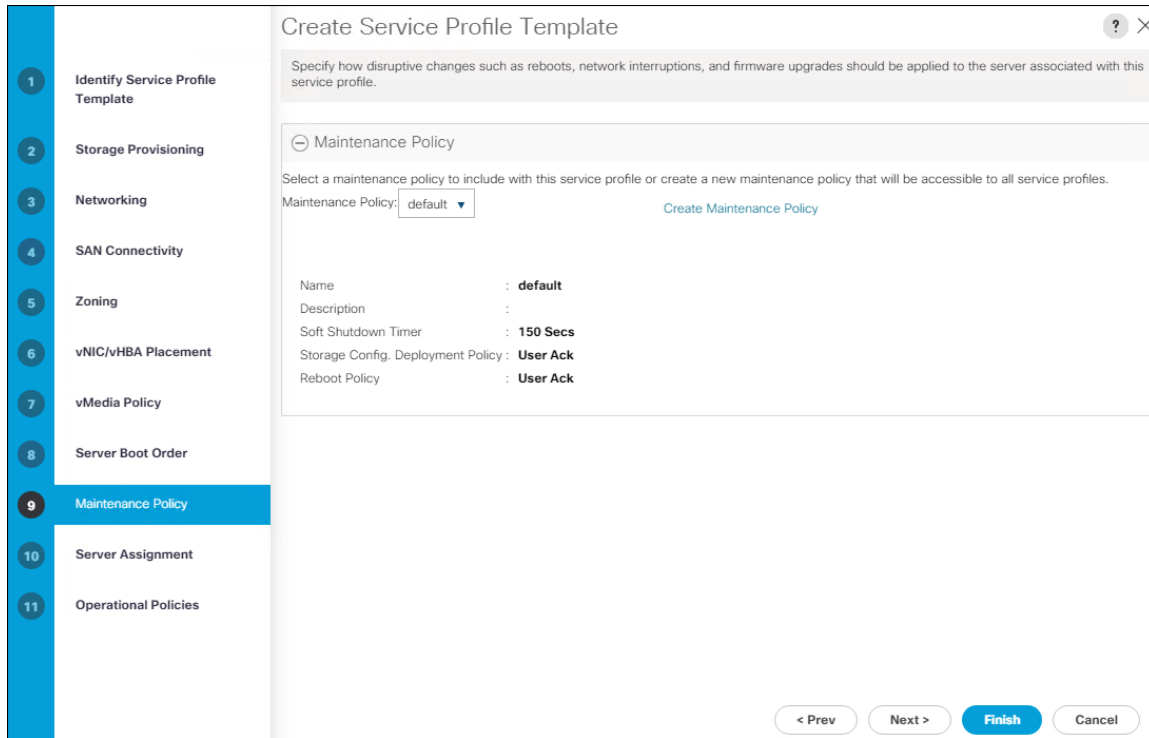


2. Click Next to continue to the next section.

Configure Maintenance Policy

To configure the maintenance policy, follow these steps:

1. Change the Maintenance Policy to default.

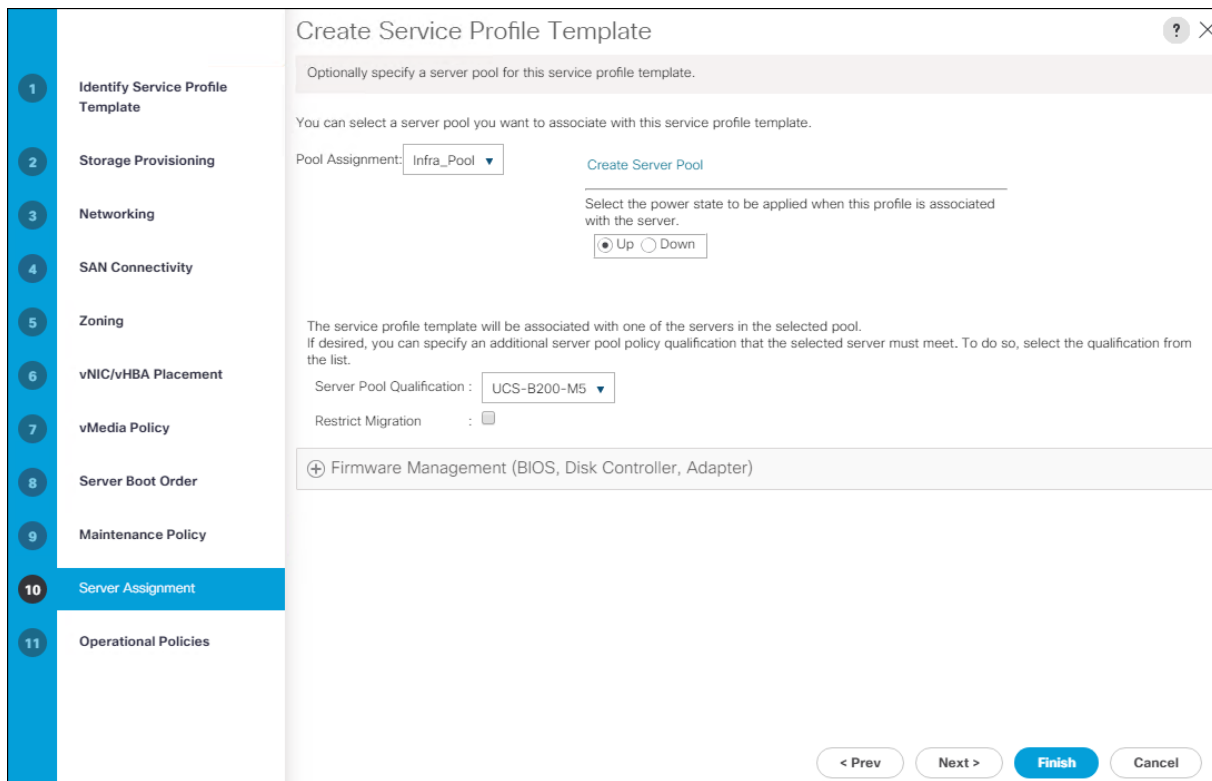


2. Click Next.

Configure Server Assignment

To configure server assignment, follow these steps:

1. In the Pool Assignment list, select `Infra_Pool1`.
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. Optional: Select “UCS-B200M5” 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.

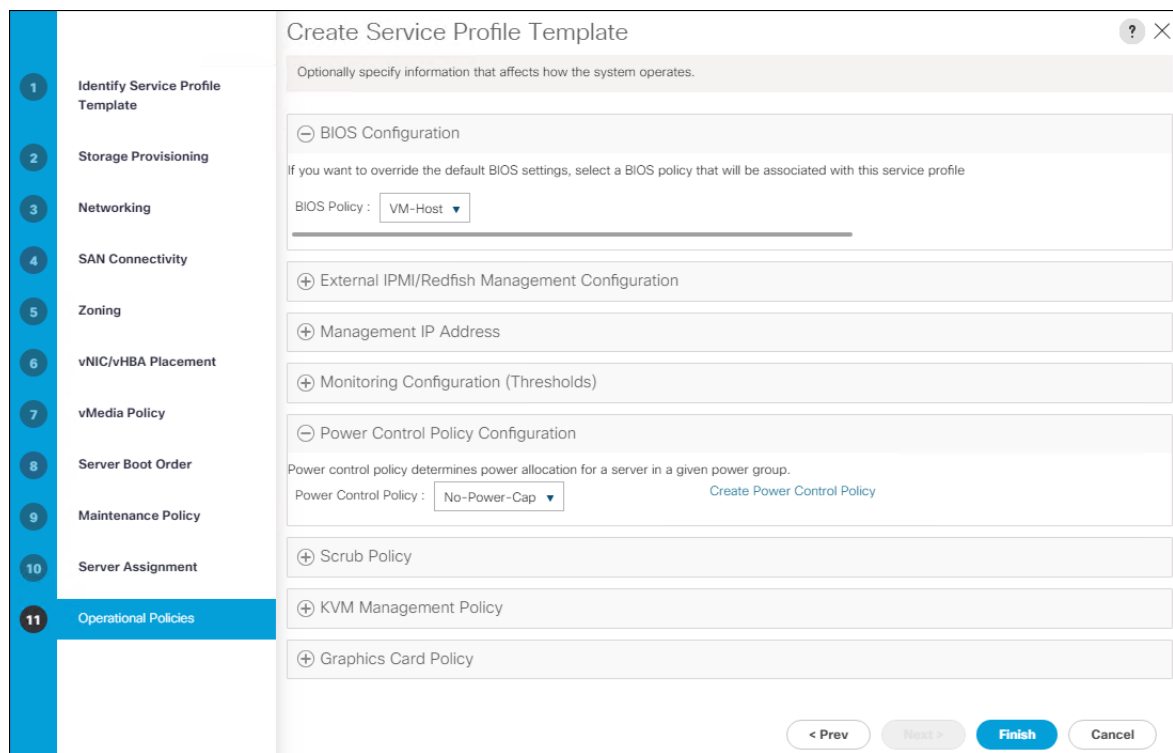


6. Click Next.

Configure Operational Policies

To configure the operational policies, follow these steps:

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



3. Click Finish to create the service profile template.

4. Click OK in the confirmation message.

Create vMedia Service Profile Template

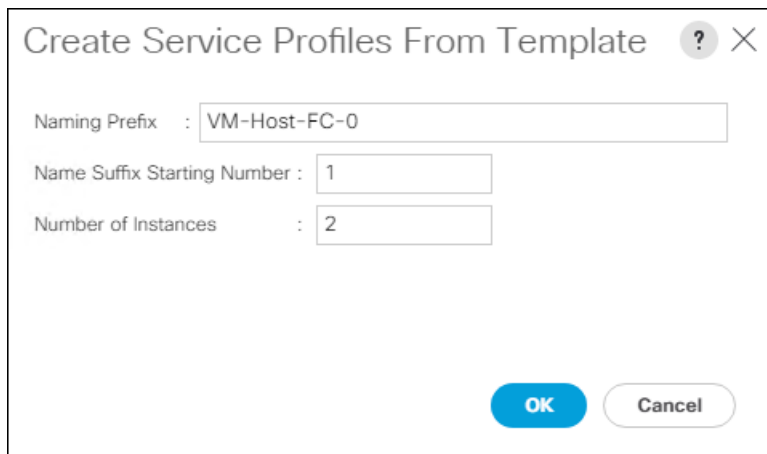
If the optional ESXi 6.7 U1 vMedia Policy is being used, a clone of the created service profile template will be made to reference this vMedia Policy. The clone of the service profile template will have the vMedia Policy configured for it, and service profiles created from it, will be unbound and re-associated to the original service profile template after ESXi installation. To create a clone of the VM-Host-FC-A service profile template, and associate the vMedia Policy to it, follow these steps:

1. Connect to UCS Manager, click Servers.
2. Select Service Profile Templates > root > Service Template VM-Host-FC-A.
3. Right-click Service Template VM-Host-FC-A and select Create a Clone.
4. Name the clone VM-Host-FC-A-vM and click OK.
5. Select Service Template VM-Host-FC-A-vM.
6. In the right pane, select the vMedia Policy tab.
7. Under Actions, select Modify vMedia Policy.
8. From the drop-down list, select the ESXi-6.7U1-HTTP vMedia Policy.
9. Click OK then click OK again to complete modifying the Service Profile Template.

Create Service Profiles

To create service profiles from the service profile template, follow these steps:

1. Connect to the UCS 6454 Fabric Interconnect UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Service Template VM-Host-FC-A.
3. Right-click **VM-Host-FC-A** and select Create Service Profiles from Template.
4. Enter **VM-Host-FC-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.



The screenshot shows a dialog box titled "Create Service Profiles From Template". It has a title bar with a question mark icon and a close button (X). The dialog contains three input fields:

- Naming Prefix : VM-Host-FC-0
- Name Suffix Starting Number : 1
- Number of Instances : 2

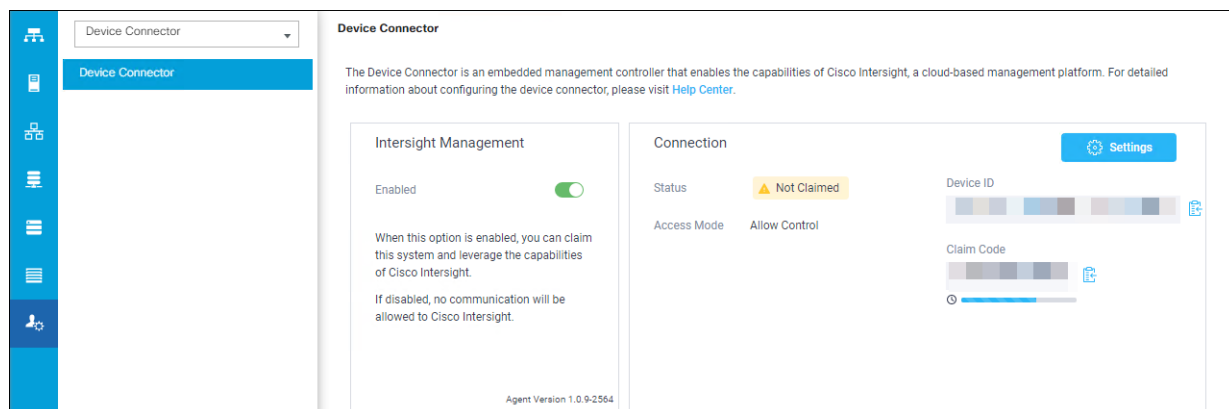
At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (white with a grey border).

8. Click OK in the confirmation message to provision two FlashStack Service Profiles.
9. When VMware ESXi 6.5 U1 has been installed on the hosts, the host Service Profiles can be unbound from the VM-Host-FC-A-vM and rebound to the VM-Host-FC-A Service Profile Template to remove the vMedia mapping from the host, to prevent issues at boot time if the HTTP source for the ESXi ISO is somehow not available.

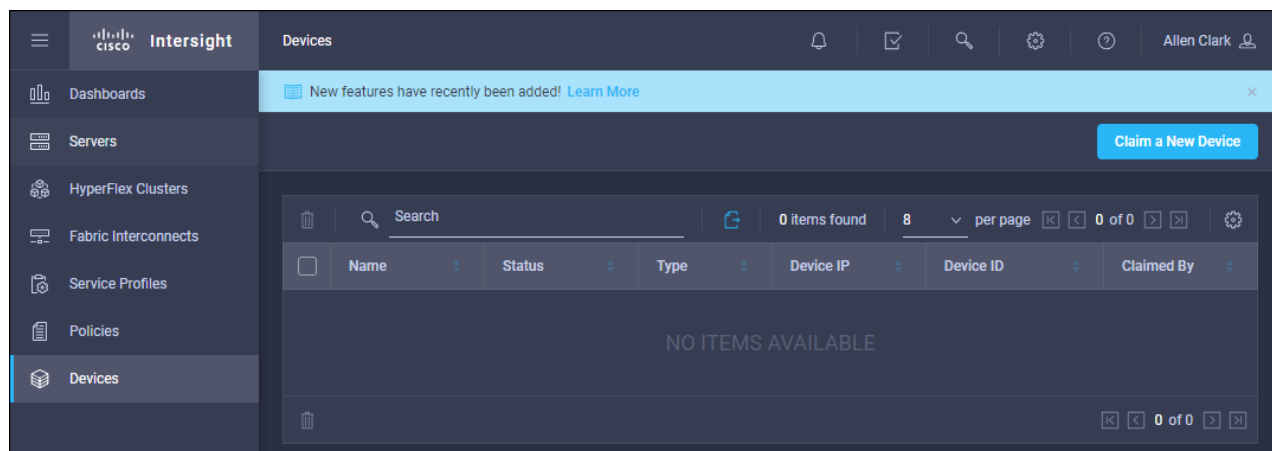
Claim in Intersight

To claim the UCS 6454 Domain in Intersight, follow these steps:

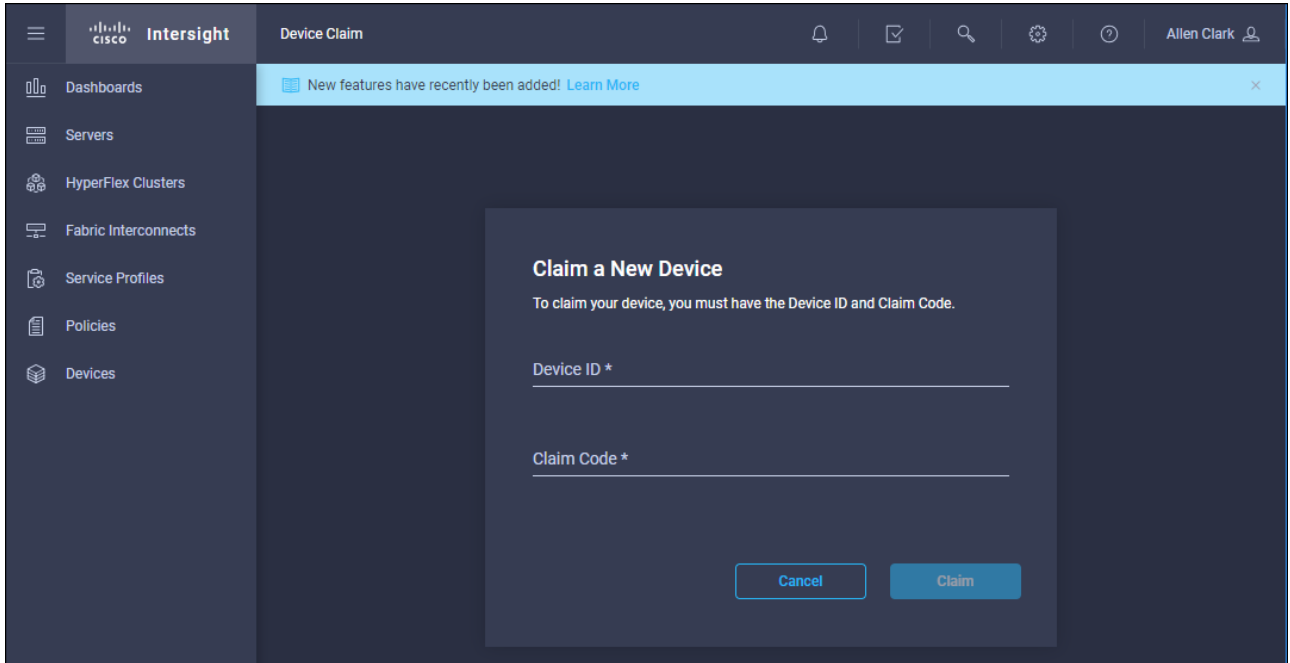
1. Connect to the UCS 6454 Fabric Interconnect UCS Manager, click the Admin tab in the navigation pane.
2. Select Device Connector.
3. Set Intersight Management to Enabled.
4. Copy the Device ID and Claim Code.



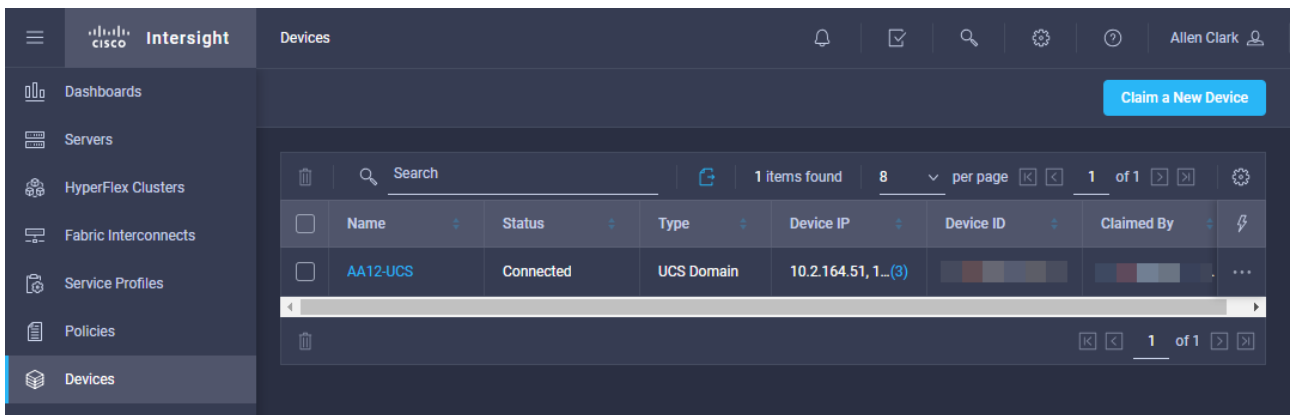
5. Open a browser to Cisco Intersight, <https://intersight.com> and log in to your Intersight account.
6. Select Devices.



7. Click Claim a New Device and enter your Device ID and Claim Code.

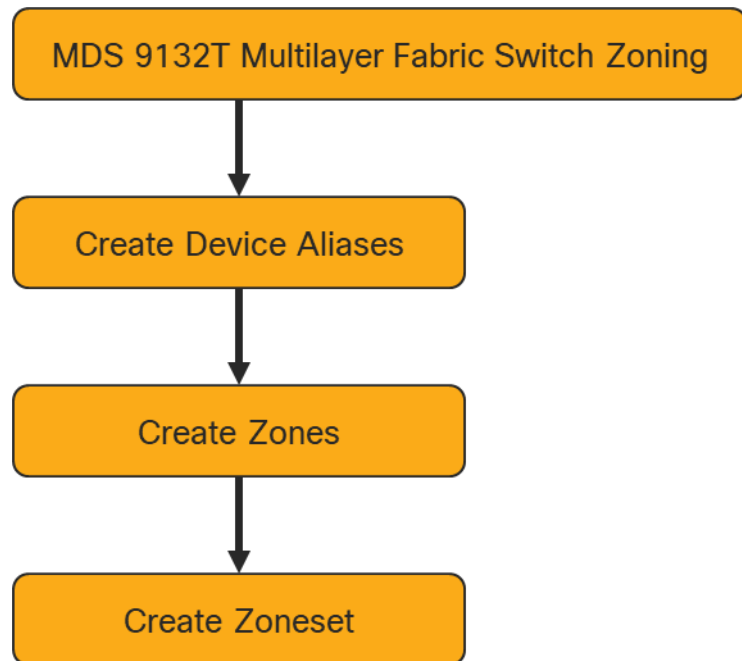


8. Click Claim.



MDS Fabric Zoning

This section continues the configuration of the Cisco MDS 9132T Multilayer Fabric Switches now that resources are attached, to provide zoning for supported devices.



Create Device Aliases

To create device aliases, follow these steps:

1. Gather the WWPN of the FlashArray adapters using the `show flogi database` command on each switch and create a spreadsheet to reference when creating device aliases on each MDS. For MDS 9132T-A this is:

```
MDS-9132T-A# show flogi database
```

INTERFACE	VSAN	FCID	PORT NAME	NODE NAME
fc1/15	100	0xb00000	52:4a:93:7c:2b:9b:9f:00	52:4a:93:7c:2b:9b:9f:00
fc1/16	100	0xb00020	52:4a:93:7c:2b:9b:9f:00	52:4a:93:7c:2b:9b:9f:00
fc1/17	100	0xb00040	52:4a:93:7c:2b:9b:9f:02	52:4a:93:7c:2b:9b:9f:02
fc1/18	100	0xb00040	52:4a:93:7c:2b:9b:9f:12	52:4a:93:7c:2b:9b:9f:12
port-channel100	100	0xb00060	24:01:00:de:fb:ff:fb:c0	20:64:00:de:fb:ff:fb:c1
port-channel100	100	0xb00061	20:00:00:25:b5:01:0a:00	20:00:00:25:b5:01:00:00
port-channel100	100	0xb00062	20:00:00:25:b5:01:0a:01	20:00:00:25:b5:01:00:01

- Match the values from the individual interfaces to the Purity command line output gained from a ssh connection to the FlashArray using the pureuser account:

```

pureuser@cspg-rtp-1> pureport list
Name      WWN          Portal      IQN          Failover
CT0.FC0   52:4A:93:7C:2B:9B:9F:00 -            -            -
CT0.FC1   52:4A:93:7C:2B:9B:9F:01 -            -            -
CT0.FC2   52:4A:93:7C:2B:9B:9F:02 -            -            -
CT0.FC3   52:4A:93:7C:2B:9B:9F:03 -            -            -
CT0.FC8   52:4A:93:7C:2B:9B:9F:08 -            -            -
CT0.FC9   52:4A:93:7C:2B:9B:9F:09 -            -            -
CT1.FC0   52:4A:93:7C:2B:9B:9F:10 -            -            -
CT1.FC1   52:4A:93:7C:2B:9B:9F:11 -            -            -
CT1.FC2   52:4A:93:7C:2B:9B:9F:12 -            -            -
CT1.FC3   52:4A:93:7C:2B:9B:9F:13 -            -            -
CT1.FC8   52:4A:93:7C:2B:9B:9F:16 -            -            -
CT1.FC9   52:4A:93:7C:2B:9B:9F:17 -            -            -
    
```

- Match the values from the port-channel to the UCS Service Profile vHBA listing for each host found within Servers -> Service Profiles -> <Service Profile of Source Host> -> Storage -> vHBAs.

Servers / Service Profiles / root / Service Profile VM-Host-FC-01

General | **Storage** | Network | iSCSI vNICs | vMedia Policy | Boot Order | Virtual Machines | FC Zones | Policies | Server Details | CIMC Sessions | FSM | VIF Paths | Faults | Events

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

Actions

- Change World Wide Node Name
- Modify vNIC/vHBA Placement
- Reset WWNN Address

World Wide Node Name

World Wide Node Name : **20:00:00:25:B5:01:00:00**
 WWNN Pool : **WWNN_Pool**
 WWNN Pool Instance : **org-root/wwn-pool-WWNN_Pool**

Local Disk Configuration Policy

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

SAN Connectivity Policy

SAN Connectivity Policy : **Infra-SAN-Policy**
 SAN Connectivity Policy Instance : **org-root/san-conn-pol-Infra-SAN-Policy**
 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 Order	Actual Order	Fabric ID	Desired Placement	Actual Placement	Admin Host Port	Actual Ho
vHBA Fabric-A	20:00:00:25:B5:01:0A:00	1	7	A	Any	1	ANY	NONE
vHBA Fabric-B	20:00:00:25:B5:01:08:00	2	8	B	Any	1	ANY	NONE

Source	Switch/Port	WWPN/PWWN	Customer WWPN/PWWN
--------	-------------	-----------	--------------------

Source	Switch/Port	WWPN/PWWN	Customer WWPN/PWWN
FlashArray-CT0FC0	MDS A fc 1/15	52:4A:93:7C:2B:9B:9F:00	
FlashArray-CT1FC0	MDS A fc 1/16	52:4A:93:7C:2B:9B:9F:02	
FlashArray-CT0FC2	MDS A fc 1/17	52:4A:93:7C:2B:9B:9F:10	
FlashArray-CT1FC2	MDS A fc 1/18	52:4A:93:7C:2B:9B:9F:12	
6454-A	Port-Channel 100	24:01:00:de:fb:ff:fb:c0	
VM-Host-FC-01-A	Port-Channel 100	20:00:00:25:b5:01:0a:00	
VM-Host-FC-02-A	Port-Channel 100	20:00:00:25:b5:01:0a:01	

4. Create device alias database entries for each of the PWWNs mapping them to their human readable source names:

```

MDS-9132T-A# conf t
MDS-9132T-A(config)# device-alias database
MDS-9132T-A(config-device-alias-db)# device-alias name FlashArray-CT0FC0 pwwn 52:4A:93:7C:2B:9B:9F:00
MDS-9132T-A(config-device-alias-db)# device-alias name FlashArray-CT1FC0 pwwn 52:4A:93:7C:2B:9B:9F:10
MDS-9132T-A(config-device-alias-db)# device-alias name FlashArray-CT0FC2 pwwn 52:4A:93:7C:2B:9B:9F:02
MDS-9132T-A(config-device-alias-db)# device-alias name FlashArray-CT1FC2 pwwn 52:4A:93:7C:2B:9B:9F:12
MDS-9132T-A(config-device-alias-db)# device-alias name VM-Host-FC-01-A pwwn 20:00:00:25:b5:01:0a:00
MDS-9132T-A(config-device-alias-db)# device-alias name VM-Host-FC-02-A pwwn 20:00:00:25:b5:01:0a:01
MDS-9132T-A(config-device-alias-db)#device-alias commit

```

5. Repeat steps 1-4 on MDS 9132T-B, starting with gathering the flogi database information:


```

MDS-9132T-B# show flogi database
-----
INTERFACE                VSAN      FCID      PORT NAME                NODE NAME
-----
fc1/15                    200      0xa50000  52:4a:93:7c:2b:9b:9f:01  52:4a:93:7c:2b:9b:9f:01
fc1/16                    200      0xa50020  52:4a:93:7c:2b:9b:9f:11  52:4a:93:7c:2b:9b:9f:11
fc1/17                    200      0xa50030  52:4a:93:7c:2b:9b:9f:03  52:4a:93:7c:2b:9b:9f:03
fc1/18                    200      0xa50040  52:4a:93:7c:2b:9b:9f:13  52:4a:93:7c:2b:9b:9f:13
port-channel100          200      0xa50060  24:02:00:de:fb:ff:f3:80  20:c8:00:de:fb:ff:f3:81
port-channel100          200      0xa50061  20:00:00:25:b5:01:0b:00  20:00:00:25:b5:01:00:00
port-channel100          200      0xa50062  20:00:00:25:b5:01:0b:01  20:00:00:25:b5:01:00:01
    
```

Source	Switch/Port	WWPN/PWWN	Customer WWPN/PWWN
FlashArray-CT0FC1	MDS A fc 1/15	52:4A:93:7C:2B:9B:9F:01	
FlashArray-CT1FC1	MDS A fc 1/16	52:4A:93:7C:2B:9B:9F:03	
FlashArray-CT0FC3	MDS A fc 1/17	52:4A:93:7C:2B:9B:9F:11	
FlashArray-CT1FC3	MDS A fc 1/18	52:4A:93:7C:2B:9B:9F:13	
VM-Host-FC-01-B	Port-Channel 100	24:02:00:de:fb:ff:f3:80	
VM-Host-FC-02-B	Port-Channel 100	20:00:00:25:b5:01:0b:00	
VM-Host-FC-02-B	Port-Channel 100	20:00:00:25:b5:01:0b:01	

alias database entries for each of the PWWNs mapping them to their human readable source names:

```

MDS-9132T-B# conf t
MDS-9132T-B(config)# device-alias database
MDS-9132T-B(config-device-alias-db)# device-alias name FlashArray-CT0FC1 pwwn 52:4A:93:7C:2B:9B:9F:01
MDS-9132T-B(config-device-alias-db)# device-alias name FlashArray-CT1FC1 pwwn 52:4A:93:7C:2B:9B:9F:11
MDS-9132T-B(config-device-alias-db)# device-alias name FlashArray-CT0FC3 pwwn 52:4A:93:7C:2B:9B:9F:03
MDS-9132T-B(config-device-alias-db)# device-alias name FlashArray-CT1FC3 pwwn 52:4A:93:7C:2B:9B:9F:13
MDS-9132T-B(config-device-alias-db)# device-alias name VM-Host-FC-01-B pwwn 20:00:00:25:b5:01:0B:00
MDS-9132T-B(config-device-alias-db)# device-alias name VM-Host-FC-02-B pwwn 20:00:00:25:b5:01:0B:01
MDS-9132T-B(config-device-alias-db)#device-alias commit
    
```

MDS Zoning

Create zones for each host using the device aliases created in the previous step, specifying init and target roles to optimize zone traffic:

Zone for UCS VM-Host-FC-01 on MDS A

```
MDS-9132T-A(config)# zone name VM-Host-FC-01-A vsan 100
MDS-9132T-A(config-zone)# member device-alias VM-Host-FC-01-A init
MDS-9132T-A(config-zone)# member device-alias FlashArray-CT0FC0 target
MDS-9132T-A(config-zone)# member device-alias FlashArray-CT0FC2 target
MDS-9132T-A(config-zone)# member device-alias FlashArray-CT1FC0 target
MDS-9132T-A(config-zone)# member device-alias FlashArray-CT1FC2 target
```

Zone for UCS VM-Host-FC-02 on MDS A

```
MDS-9132T-A(config-zone)# zone name VM-Host-FC-02-A vsan 100
MDS-9132T-A(config-zone)# member device-alias VM-Host-FC-02-A init
MDS-9132T-A(config-zone)# member device-alias FlashArray-CT0FC0 target
MDS-9132T-A(config-zone)# member device-alias FlashArray-CT0FC2 target
MDS-9132T-A(config-zone)# member device-alias FlashArray-CT1FC0 target
MDS-9132T-A(config-zone)# member device-alias FlashArray-CT1FC2 target
```

Zone for UCS VM-Host-FC-01 on MDS B

```
MDS-9132T-B(config)# zone name VM-Host-FC-01-B vsan 200
MDS-9132T-B(config-zone)# member device-alias VM-Host-FC-01-B init
MDS-9132T-B(config-zone)# member device-alias FlashArray-CT0FC1 target
MDS-9132T-B(config-zone)# member device-alias FlashArray-CT0FC3 target
MDS-9132T-B(config-zone)# member device-alias FlashArray-CT1FC1 target
MDS-9132T-B(config-zone)# member device-alias FlashArray-CT1FC3 target
```

Zone for UCS VM-Host-FC-02 on MDS B

```
MDS-9132T-B(config)# zone name VM-Host-FC-02-B vsan 200
MDS-9132T-B(config-zone)# member device-alias VM-Host-FC-02-B init
MDS-9132T-B(config-zone)# member device-alias FlashArray-CT0FC1 target
MDS-9132T-B(config-zone)# member device-alias FlashArray-CT0FC3 target
MDS-9132T-B(config-zone)# member device-alias FlashArray-CT1FC1 target
MDS-9132T-B(config-zone)# member device-alias FlashArray-CT1FC3 target
```

Create and Activate Zoneset

Add the zones to a zoneset on each MDS switch:

zoneset for MDS A

```
MDS-9132T-A(config-zone)# zoneset name flashstack-zoneset vsan 100
MDS-9132T-A config-zoneset)# member VM-Host-FC-01-A
MDS-9132T-A(config-zoneset)# member VM-Host-FC-02-A
```

zoneset for MDS B

```
MDS-9132T-B(config-zone)# zoneset name flashstack-zoneset vsan 200
MDS-9132T-B(config-zoneset)# member VM-Host-FC-01-B
MDS-9132T-B(config-zoneset)# member VM-Host-FC-02-B
```

Activate the zonesets and save the configuration:

zoneset for MDS A

```
mds-9148s-a(config-zoneset)# zoneset activate name flashstack-zoneset vsan 101
mds-9148s-a(config)# copy run start
```

zoneset for MDS B

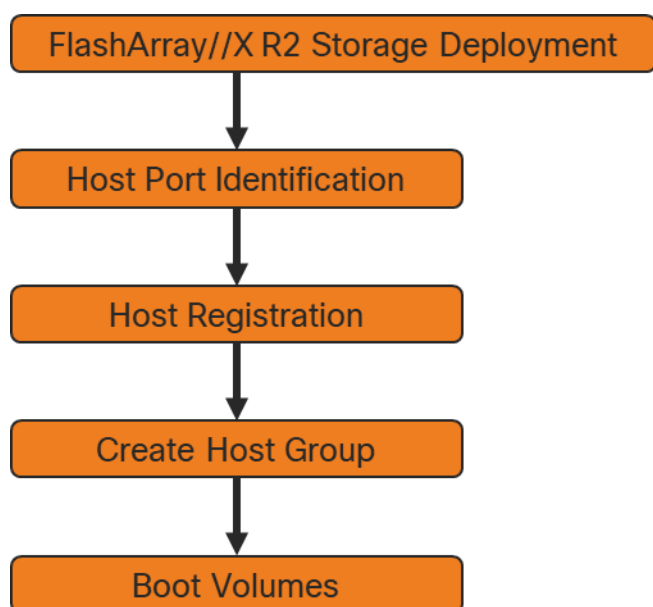
```
mds-9148s-b(config-zoneset)# zoneset activate name flashstack-zoneset vsan 102
mds-9148s-b(config)# copy run start
```

FlashArray Storage Deployment

The Pure Storage FlashArray//X is accessible to the FlashStack, but no storage has been deployed at this point. The storage to be deployed will include:

- ESXi FC Boot LUNs
- VMFS Datastores
- VVol Data Stores

The FC Boot LUNs will need to be setup from the Pure Storage Web Portal, and the VMFS datastores will be directly provisioned from the vSphere Web Client after the Pure Storage vSphere Web Client Plug-in has later been registered with the vCenter.



Host Port Identification

FC Boot LUNs is mapped by the FlashArray//X using the assigned Initiator PWWN to the provisioned service profiles.

Host Registration

For Host registration, follow these steps in the Pure Storage Web Portal:

1. Select Storage > Hosts
2. Select the + icon in the Hosts Panel
3. After clicking the Create Host (+) option, a pop-up will appear to create an individual host entry on the FlashArray

Create Host

Name

- To create more than one host entry, click the Create Multiple... option, filling in the Name, Start Number, Count, and Number of Digits, with a “#” appearing in the name where an iterating number will appear:

Create Multiple Hosts

Name

Start Number

Count

Number of Digits

- Click Create to add the hosts.
- For each host created, select the host.
- In the Host view, select Configure WWNs... from the Host Ports menu.

PURE STORAGE Storage

Array **Hosts** Volumes Protection Groups Pods

> Hosts > VM-Host-FC-1

Size	Data Reduction	Volumes	Snapshots	Shared	System	Total
0	1.0 to 1	0.00	0.00	-	-	0.00

Connected Volumes 0 of 0 < > ⋮

Name ▲

Shared LUN

No volumes found.

Protection Groups 0 of 0 < > ⋮

Name ▲

No protection groups found.

Host Ports ⋮

Port

No ports found.

- Configure WWNs...
- Configure IQNs...
- Remove...

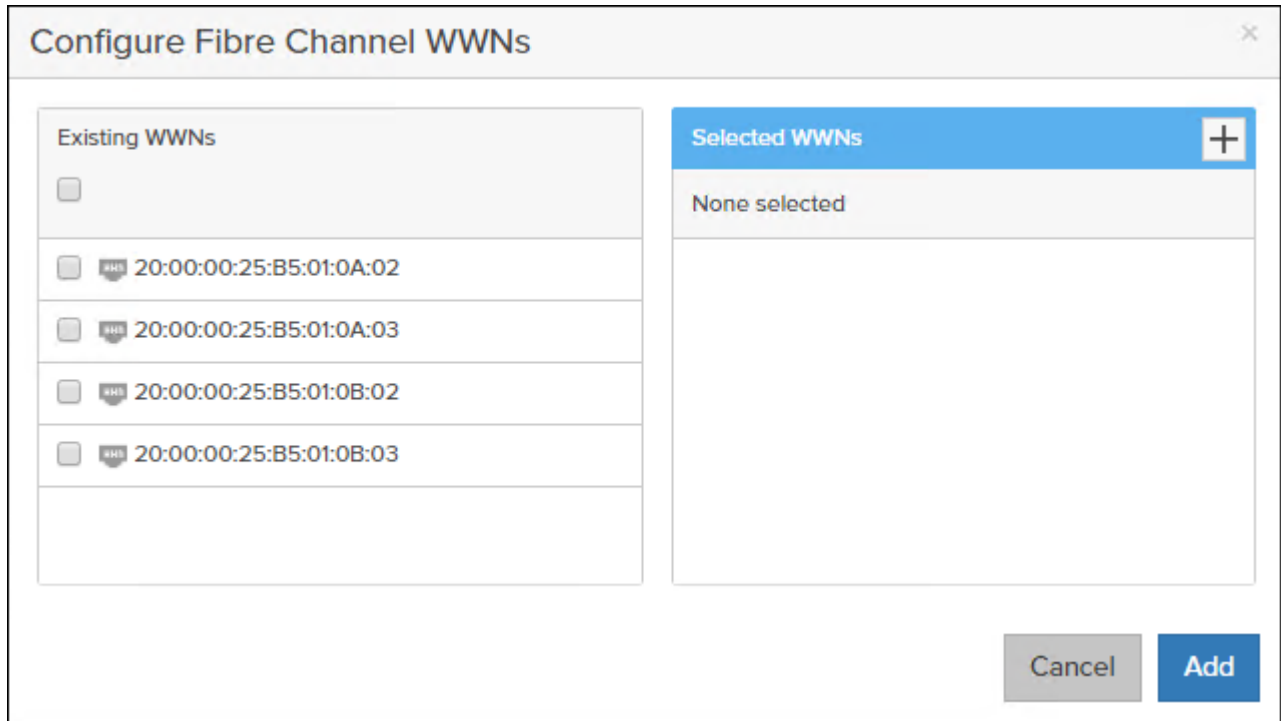
Details ⋮

CHAP Credentials

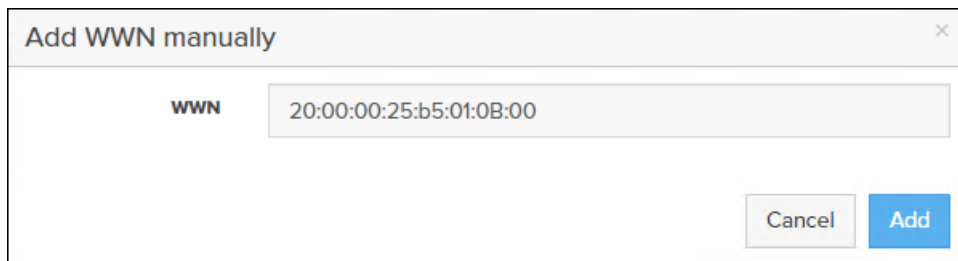
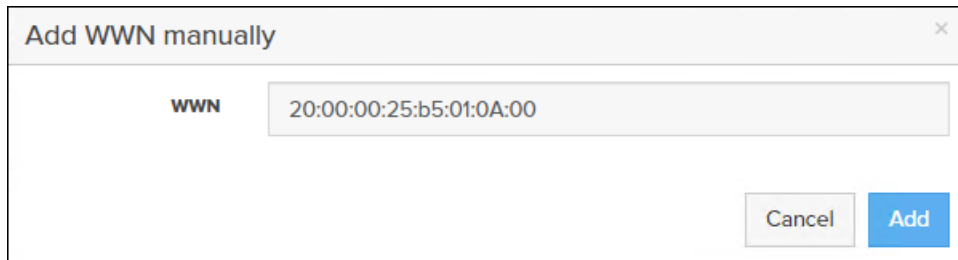
Personality

Preferred Arrays

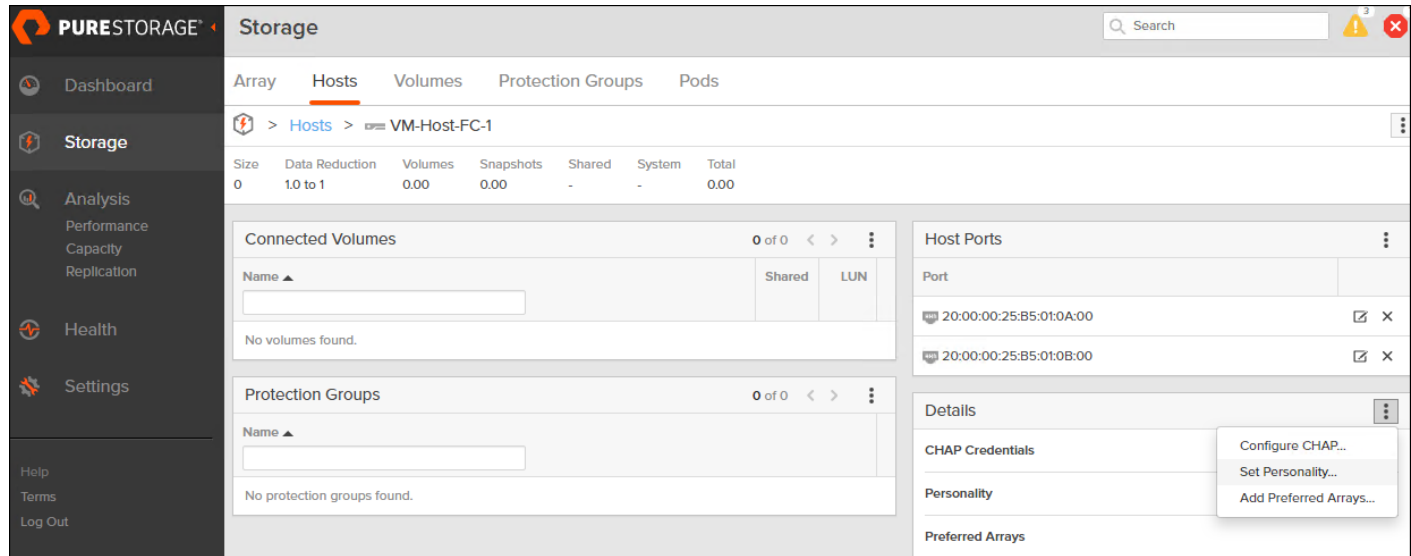
- 8. A pop-up will appear for Configure Fibre Channel WWNs <host being configured>. Within this pop-up, select the appropriate Existing WWNs from the discovered list.



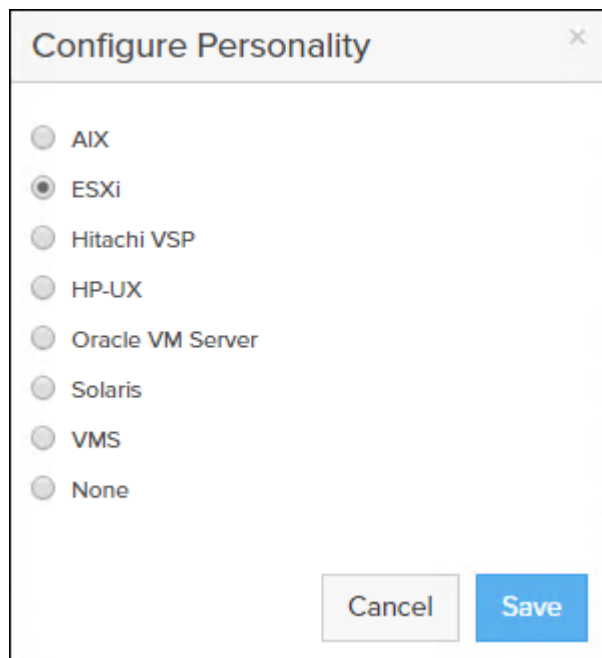
- 9. Or you may enter the WWN manually by Selecting the +.



- 10. After entering the PWWN/WWPN, click Add to add the Host Ports.
- 11. Select Set Personality... in the Details menu.



12. Select ESXi and click Save.



13. Repeat steps 1-12 for each host created.

Create Host Group

Host Groups allow the Administrator to map Volumes to a group of hosts at once with the same LUN ID. To create a Host Group, follow these steps in the Pure Storage Web Portal:

1. Select Storage > Hosts.
2. Select the + icon in the Host Groups Panel.
3. A pop-up will appear to create a host group on the FlashArray.

Create Host Group

Name

4. Provide a name for the group and click Create.
5. Select the group in the Host Groups Panel.
6. In the Host Group view, select Add... from the Member Hosts menu.

The screenshot shows the Pure Storage console interface. The main content area is titled 'Production' under the 'Hosts' tab. A table at the top shows summary statistics: Size (0), Data Reduction (1.0 to 1), Volumes (0.00), Snapshots (0.00), Shared (-), System (-), and Total (0.00). Below this are three sections: 'Member Hosts', 'Connected Volumes', and 'Protection Groups', all of which are currently empty. A context menu is open over the 'Member Hosts' section, showing options: 'Add...', 'Remove...', and 'Download CSV'.

7. Select the host to be part of the host group.

Add Hosts to Host Group

Existing Hosts

FSV-Upgrade-ESXi-03

VM-Host-FC-1

VM-Host-FC-2

Selected Hosts

2 selected Clear all

VM-Host-FC-1 ✕

VM-Host-FC-2 ✕

8. Click Add.

Private Boot Volumes for Each ESXi Host

To create private boot volumes for each ESXi Host, follow these steps in the Pure Storage Web Portal:

1. Select Storage > Volumes.
2. Select the + icon in the Volumes Panel.
3. A pop-up will appear to create a volume on the FlashArray.

The screenshot shows a 'Create Volume' dialog box with the following fields and options:

- Container:** /
- Name:** Letters, Numbers, -
- Provisioned Size:** Numbers (unit: G)
- Bandwidth Limit:** Numbers (unit: MB/s)

Buttons at the bottom: Create Multiple..., Cancel, Create

4. To create more than one volume, click the Create Multiple... option, filling in the Name, Provisioned Size, Starting Number, Count, and Number of Digits, with a “#” appearing in the name where an iterating number will appear.

Create Multiple Volumes ✕

Container

Name

Provisioned Size G

Bandwidth Limit MB/s

Start Number

Count

Number of Digits

5. Click Create to provision the volumes to be used as FC boot LUNs.
6. Go back to the Hosts section under the Storage tab. Click one of the hosts and select the gear icon drop-down list within the Connected Volumes tab within that host.

Storage

Array
Hosts
Volumes
Protection Groups
Pods

⚡ > Hosts > 📄 Production > 🖨️ VM-Host-FC-1

Size	Data Reduction	Volumes	Snapshots	Shared	System	Total
0	1.0 to 1	0.00	0.00	-	-	0.00

Connected Volumes

Name ▲

No volumes found.

0 of 0
<
>
⋮

Connect..
Disconnect..
Download CSV

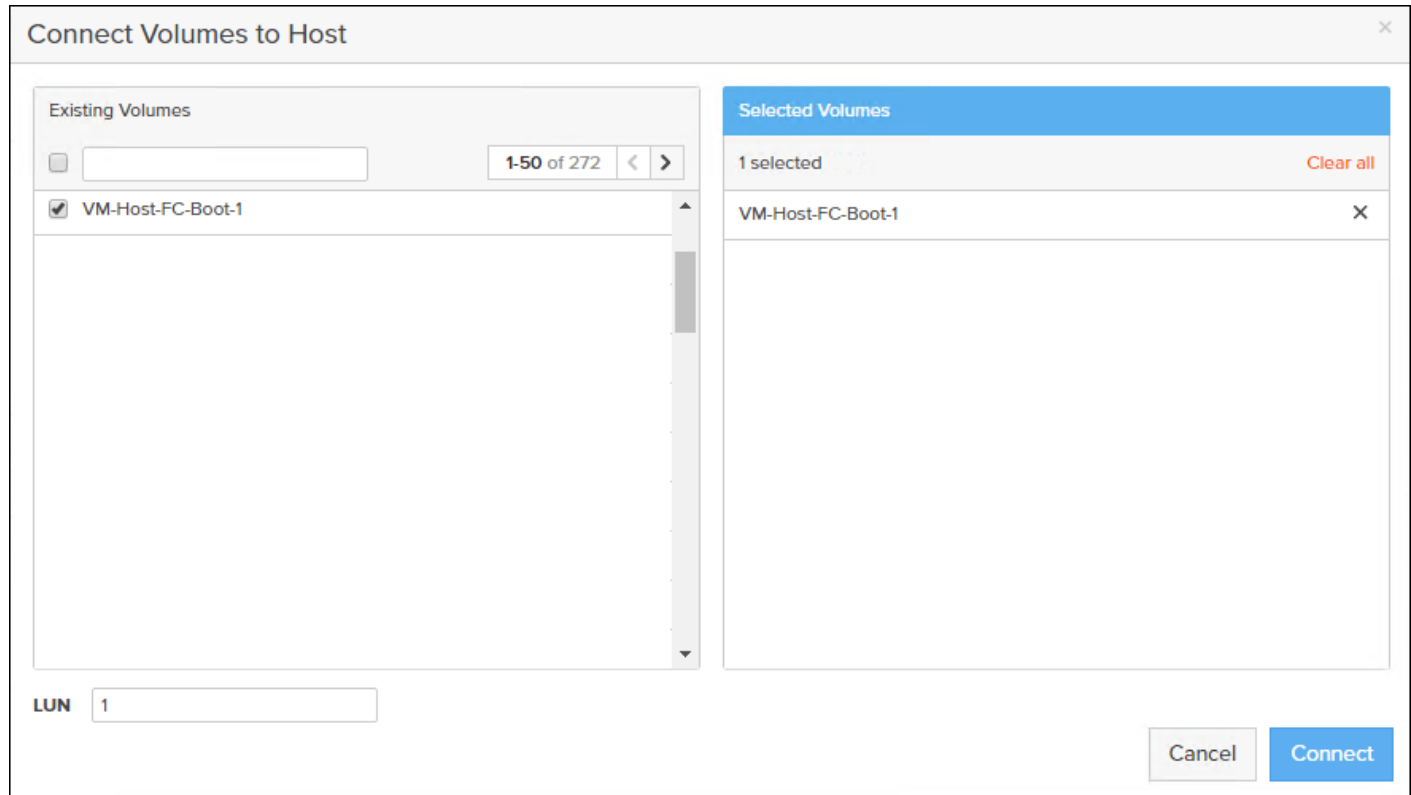
Protection Groups

Name ▲

No protection groups found.

0 of 0
<
>
⋮

7. From the drop-down list of the gear icon, select Connect Volumes, and a pop-up will appear.



LUN ID 1 should be used for the boot.

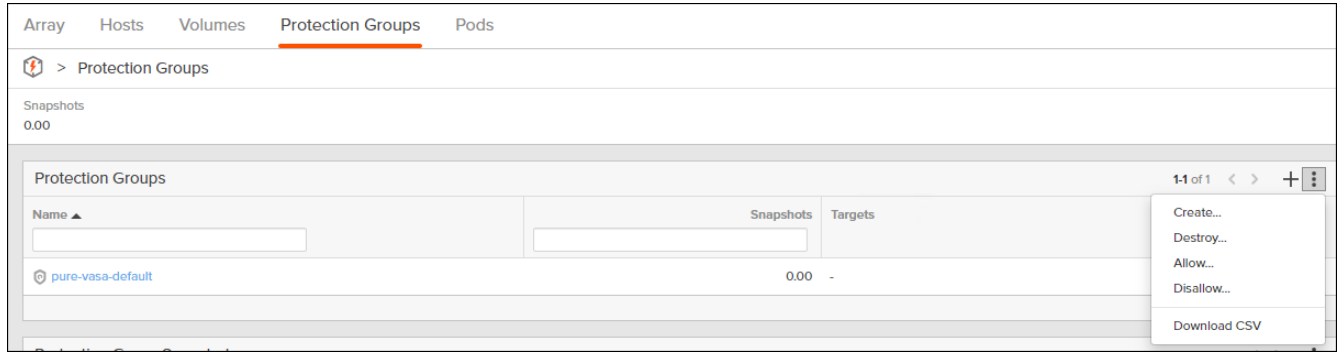
8. Select the volume that has been provisioned for the host, set the LUN ID for the volume, click the + next to the volume, and select Confirm to proceed. Repeat steps 1–7 to connect volumes for each of the host/volume pairs configured.

Configure Storage Policy Based Management

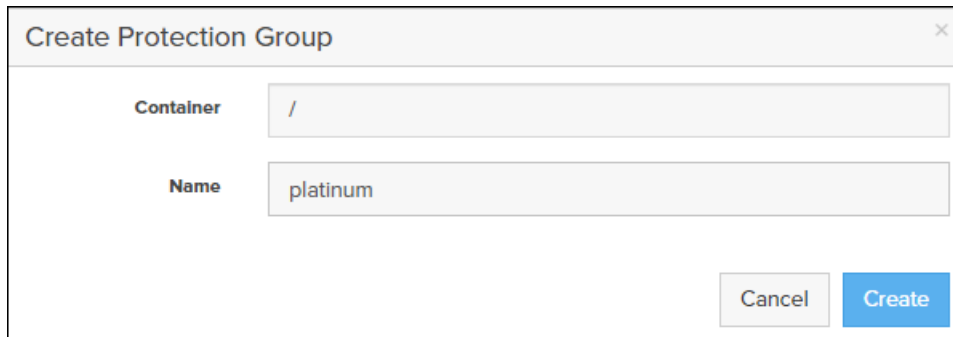
vSphere can communicate to the array via VASA provider to find out what features it supports and allow the vSphere administrator to assign, change, or remove functionality on a VVol on demand and via policies. Below is an example of how to configure a Protection group that will provide hourly snapshots that will be retained for 1 day, with 4 snapshots per day retained for 7 days. These policies should be configured based on application snapshot need.

To configure Storage Policy Based Management, follow these steps:

1. In the Pure Storage Web Portal select Storage > Protection Groups.
2. Select Create... from the Protection Groups menu.

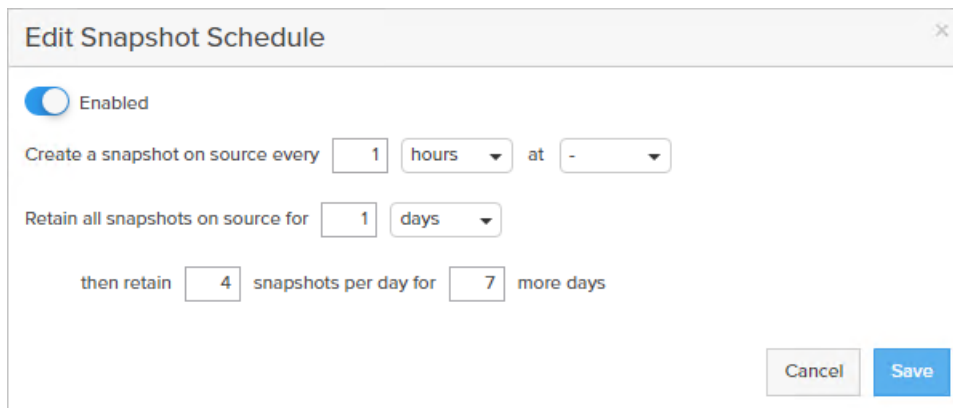


3. Enter a name.



4. Select the protection group.

5. Edit the Snapshot Schedule based on your operational requirements.

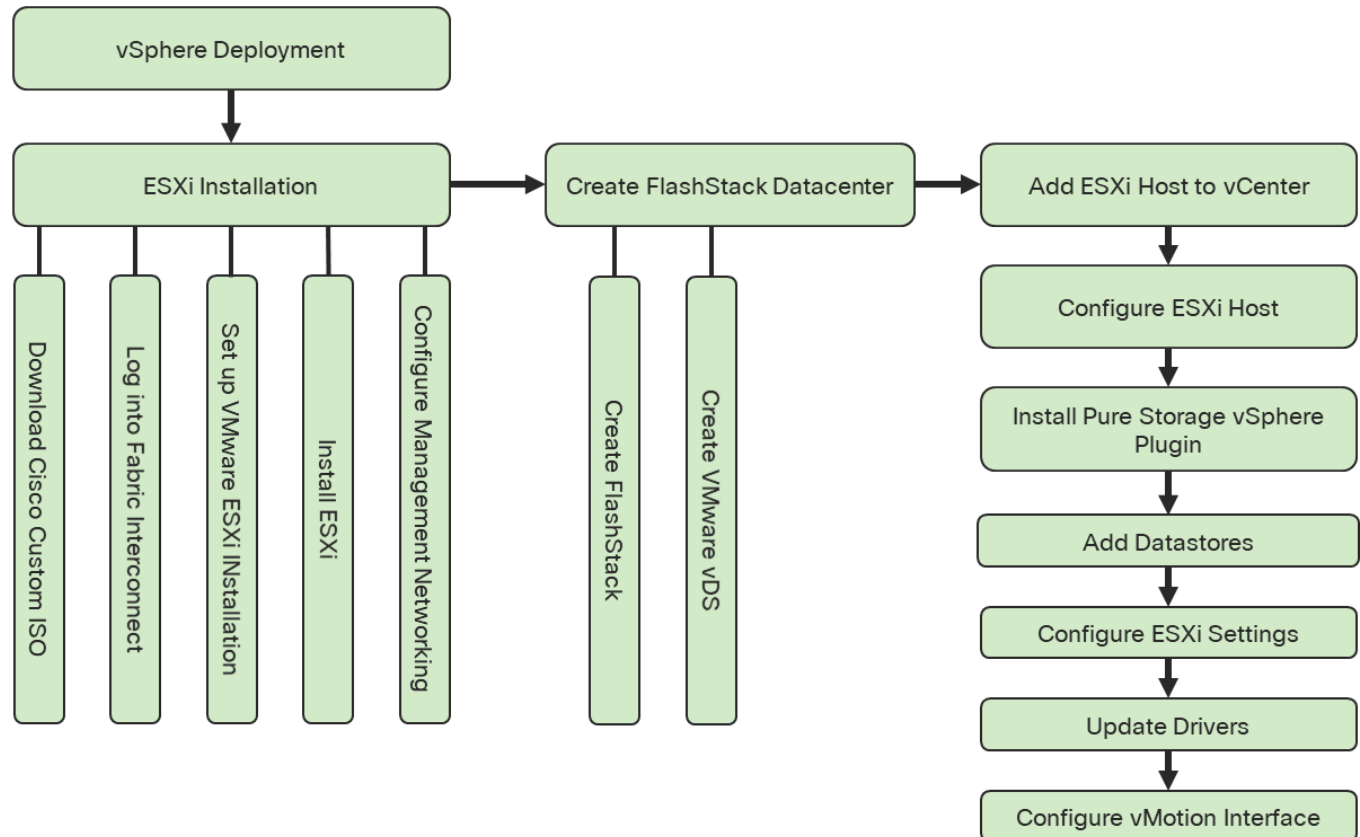


6. Click Save.

VMware vSphere Deployment

ESXi Installation

This section provides detailed instructions to install VMware ESXi 6.7 U1 in a FlashStack environment. After the procedures are completed, the FC SAN booted ESXi hosts will be configured.



Several methods exist for installing ESXi in a VMware environment. These procedures focus on how to use the built-in keyboard, video, mouse (KVM) console and virtual media features in Cisco UCS Manager to map remote installation media to individual servers and connect to their boot logical unit numbers (LUNs).

Download Cisco Custom Image for ESXi 6.7 U1

The VMware Cisco Custom Image will be needed for use during installation by manual access to the Cisco UCS KVM vMedia, or through a vMedia Policy covered in a previous subsection. If the Cisco Custom Image was not downloaded during the vMedia Policy setup, download it now by following these steps:

1. Click the following link: <https://my.vmware.com/web/vmware/details?downloadGroup=OEM-ESXI67U1-CISCO&productId=859>
2. You will need a user id and password on vmware.com to download this software.
3. Download the .iso file.

Log into Cisco UCS 6454 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 into the Cisco UCS environment to run the IP KVM.

To log into the Cisco UCS environment, follow these steps:


1. Open a web browser to `https:// <var_ucs_mgmt_vip>`
2. Select the Launch UCS Manager Section in the HTML section to pull up the UCSM HTML5 GUI.
3. Enter admin for the Username, and provide the password used during setup.
4. Within the UCSM select Servers -> Service Profiles and pick the first host provisioned as VM-Host-FC-01.
5. Click the KVM Console option within Actions and accept the KVM server certificate in the new window or browser tab that is spawned for the KVM session.
6. Click the link within the new window or browser tab to load the KVM client application.

Set Up VMware ESXi Installation



Skip this step if you are using vMedia policies. ISO file will already be connected to KVM.

To prepare the server for the OS installation, follow these steps on each ESXi host:

1. In the KVM window, click Virtual Media icon  in the upper right of the screen.
2. Click Activate Virtual Devices
3. Click Virtual Media again and select Map CD/DVD.
4. Browse to the ESXi installer ISO image file and click Open.
5. Click Map Device.
6. Click the KVM tab to monitor the server boot.
7. Boot the server by selecting Boot Server and clicking OK, then click OK again.

Install ESXi

To install VMware ESXi to the FC bootable LUN of the hosts, follow these steps on each host:

1. On reboot, the machine detects the presence of the ESXi installation media. Select the ESXi installer from the boot menu that is displayed.
2. After the installer is finished loading, press Enter to continue with the installation.
3. Read and accept the end-user license agreement (EULA). Press F11 to accept and continue.

4. Select the LUN that was previously set up as the installation disk for ESXi and press Enter to continue with the installation.
5. Select the appropriate keyboard layout and press Enter.
6. Enter and confirm the root password and press Enter.
7. The installer issues a warning that the selected disk will be repartitioned. Press F11 to continue with the installation.
8. After the installation is complete, if using locally mapped Virtual Media, click the Virtual Media tab and clear the P mark next to the ESXi installation media. Click Yes.
9. From the KVM window, press Enter to reboot the server.

Set Up Management Networking for ESXi Hosts

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

To configure the ESXi host with access to the management network, follow these steps:

1. After the server has finished rebooting, press F2 to customize the system.
2. Log in as root, enter the corresponding password, and press Enter to log in.
3. Select the Configure the Management Network option and press Enter.
4. Select Network Adapters option leave vmnic0 selected, arrow down to vmnic1 and press space to select vmnic1 as well and press Enter.
5. Select the VLAN (Optional) option and press Enter.
6. Enter the <<var_ib_mgmt_vlan_id>> and press Enter.
7. From the Configure Management Network menu, select IPv4 Configuration and press Enter.
8. Select the Set Static IP Address and Network Configuration option by using the space bar.
9. Enter <<var_vm_host_FC_01_ip>> for the IPv4 Address for managing the first ESXi host.
10. Enter <<var_ib_mgmt_vlan_netmask_length>> for the Subnet Mask for the first ESXi host.
11. Enter <<var_ib_mgmt_gateway>> for the Default Gateway for the first ESXi host.
12. Press Enter to accept the changes to the IPv4 configuration.
13. Select the DNS Configuration option and press Enter.



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

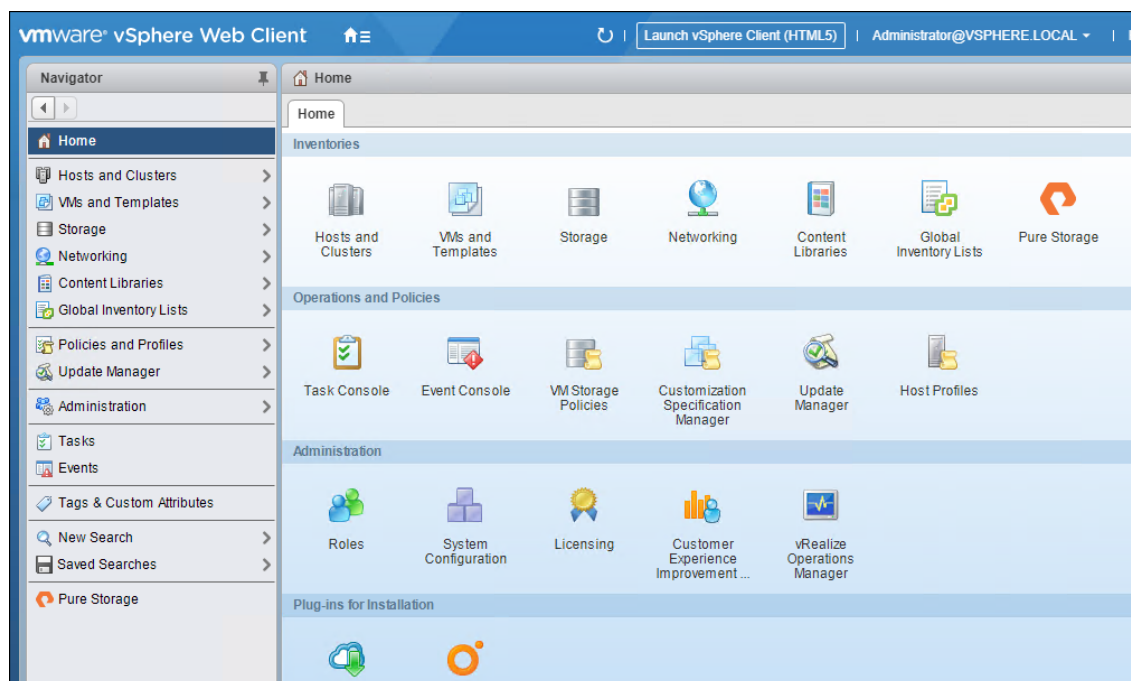
14. Enter the IP address of <<var_nameserver_ip>> for the Primary DNS Server.

15. Optional: Enter the IP address of the Secondary DNS Server.
16. Enter the fully qualified domain name (FQDN) for the first ESXi host.
17. Press Enter to accept the changes to the DNS configuration.
18. Select the IPv6 Configuration option and press Enter.
19. Using the spacebar, select Disable IPv6 (restart required) and press Enter.
20. Press Esc to exit the Configure Management Network submenu.
21. Press Y to confirm the changes and return to the main menu.
22. The ESXi host reboots. After reboot, press F2 and log back in as root.
23. Select Test Management Network to verify that the management network is set up correctly and press Enter.
24. Press Enter to run the test.
25. Press Enter to exit the window, and press Esc to log out of the VMware console.
26. Repeat the steps in Set Up VMware ESXi Installation, Install ESXi, and Set UP Management Networking for ESXi Host for additional hosts provisioned, using appropriate values.

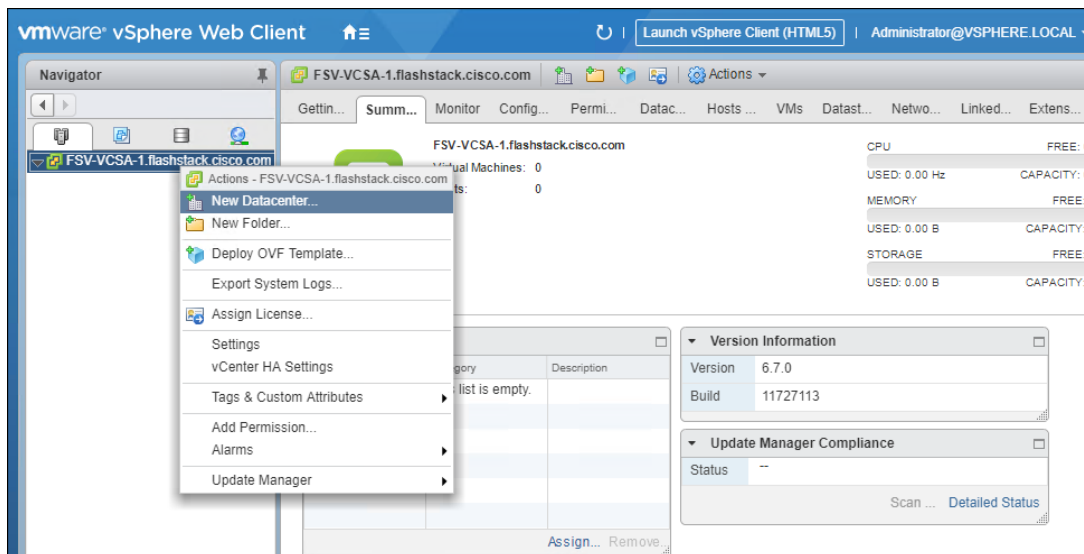
Create FlashStack Datacenter

If a new Datacenter is needed for the FlashStack, follow these steps on the vCenter:

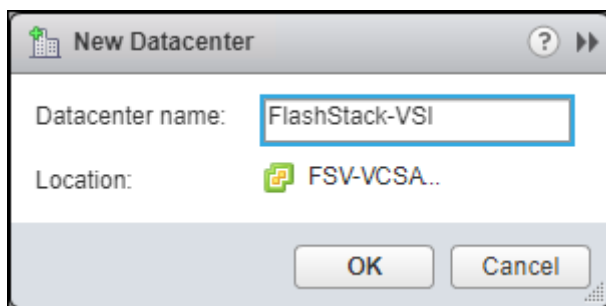
1. Connect to the vSphere Web Client and click Hosts and Clusters from the left side Navigator window or the Hosts and Clusters icon from the Home center window.



2. From Hosts and Clusters:
3. Right-click the vCenter icon and select New Datacenter... from the drop-down list.



4. From the New Datacenter pop-up dialogue enter in a Datacenter name and click OK.



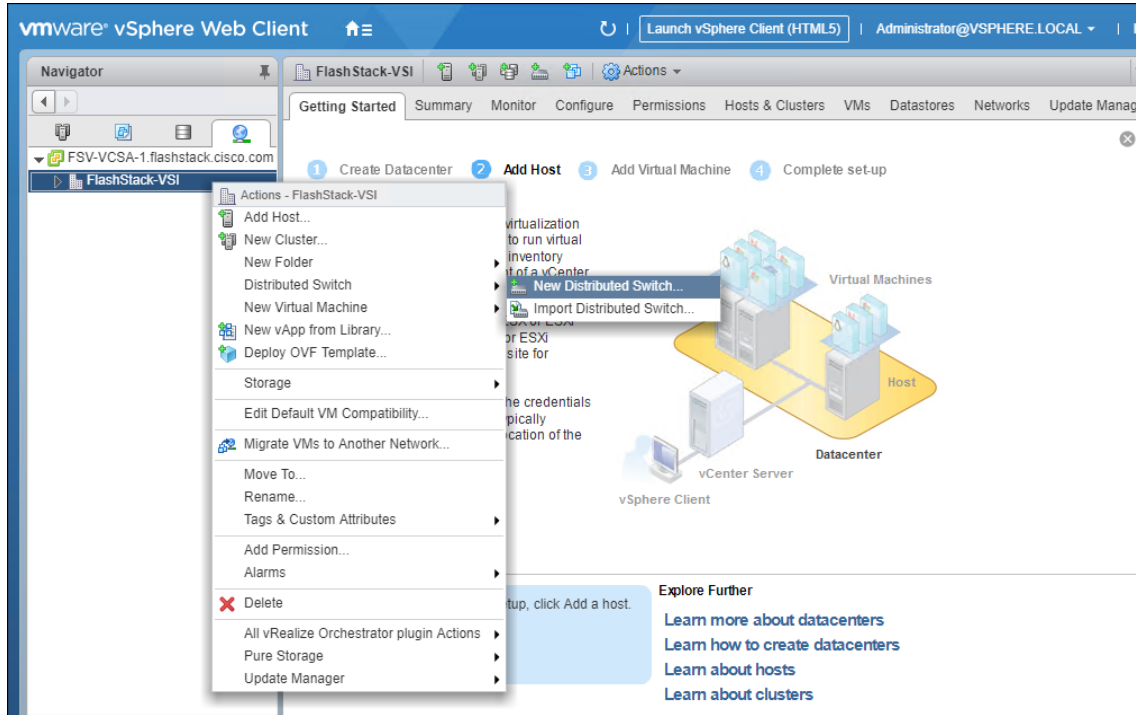
Create VMware vDS for Infrastructure and Application Traffic

The VMware vDS setup will consist of two vDS that are separated for Infrastructure use versus Application traffic.

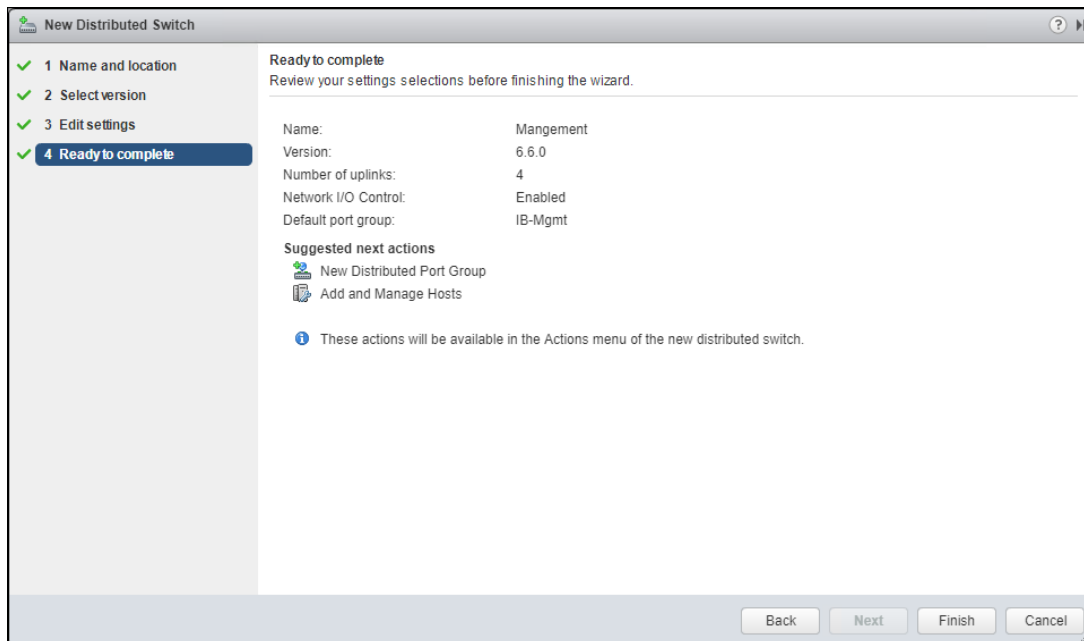
FlashStack Infrastructure vDS

To configure the first VMware vDS, follow these steps:

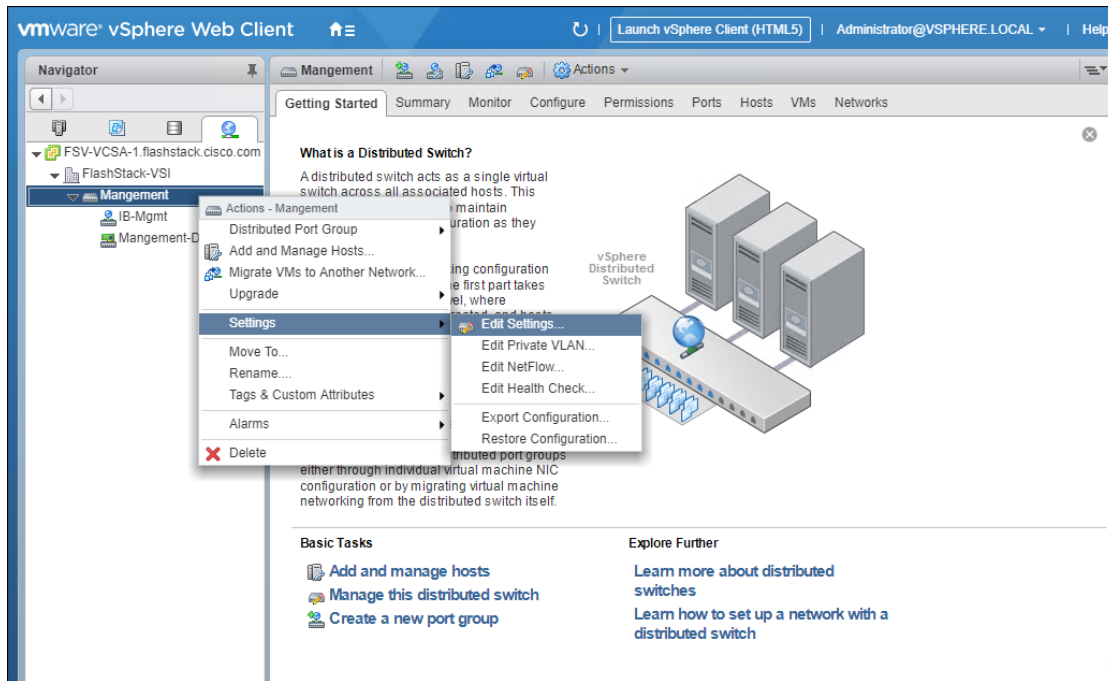
1. Connect to the vSphere Web Client and click Networking from the left side Navigator window or the Networking icon from the Home center window.
2. Right-click the FlashStack-VSI datacenter and select Distributed Switch > New Distributed Switch...



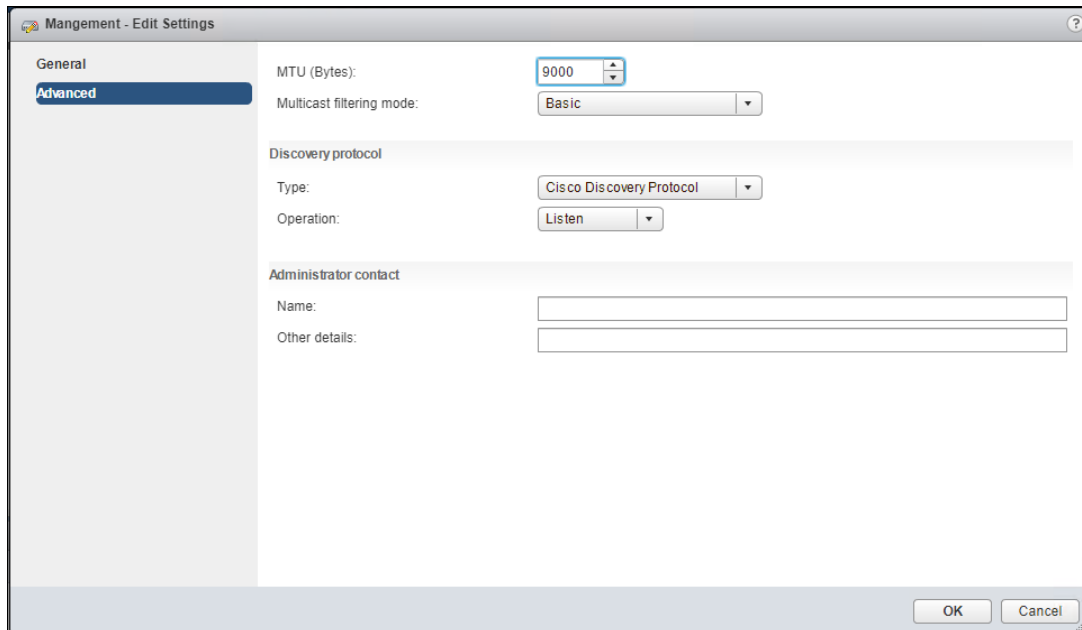
3. Give the Distributed Switch a descriptive name and click Next.
4. Make sure Distributed switch: 6.6.0 is selected and click Next.
5. Leave the Number of uplinks at 4. If VMware Network I/O Control is to be used for Quality of Service, leave Network I/O Control Enabled. Otherwise, Disable Network I/O Control. Enter IB-Mgmt for the name of the default Port group to be created. Click Next.
6. Review the information and click Finish to complete creating the vDS.



7. Right-click the newly created vDS , and select Settings -> Edit Settings...



8. Click the Advanced option side of the Edit Settings window and adjust the MTU from 1500 to 9000.



9. Click OK to save the changes.

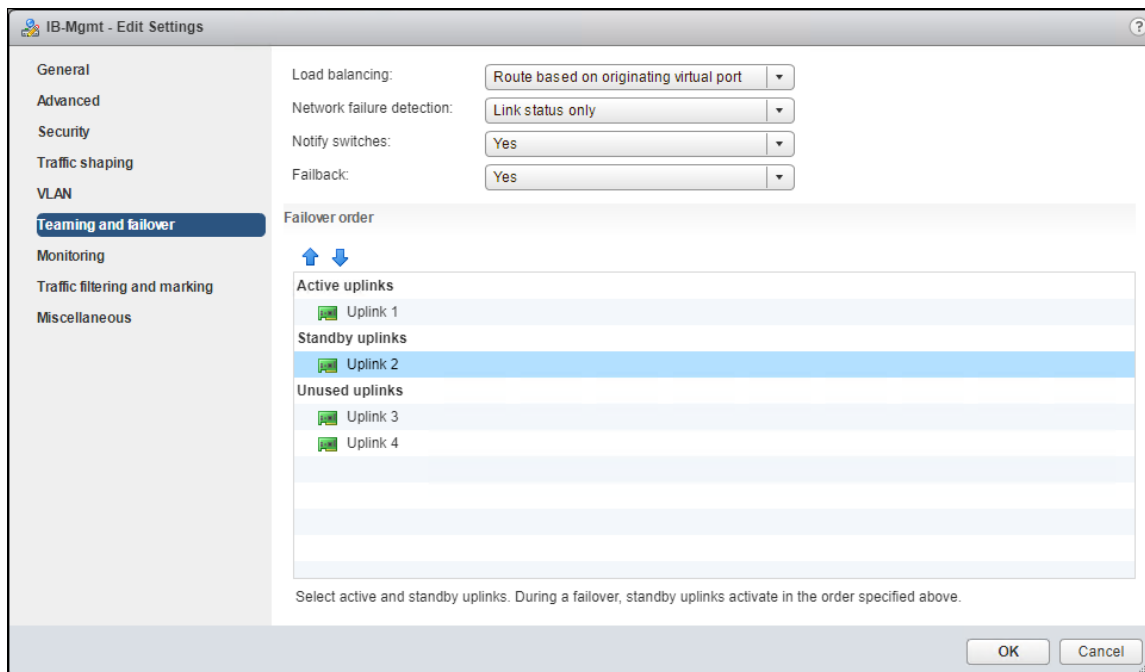
10. Expand the FlashStack VSI data center and the newly created vDS.

11. Right-click the IB-Mgmt Distributed Port Group, and select Edit Settings...

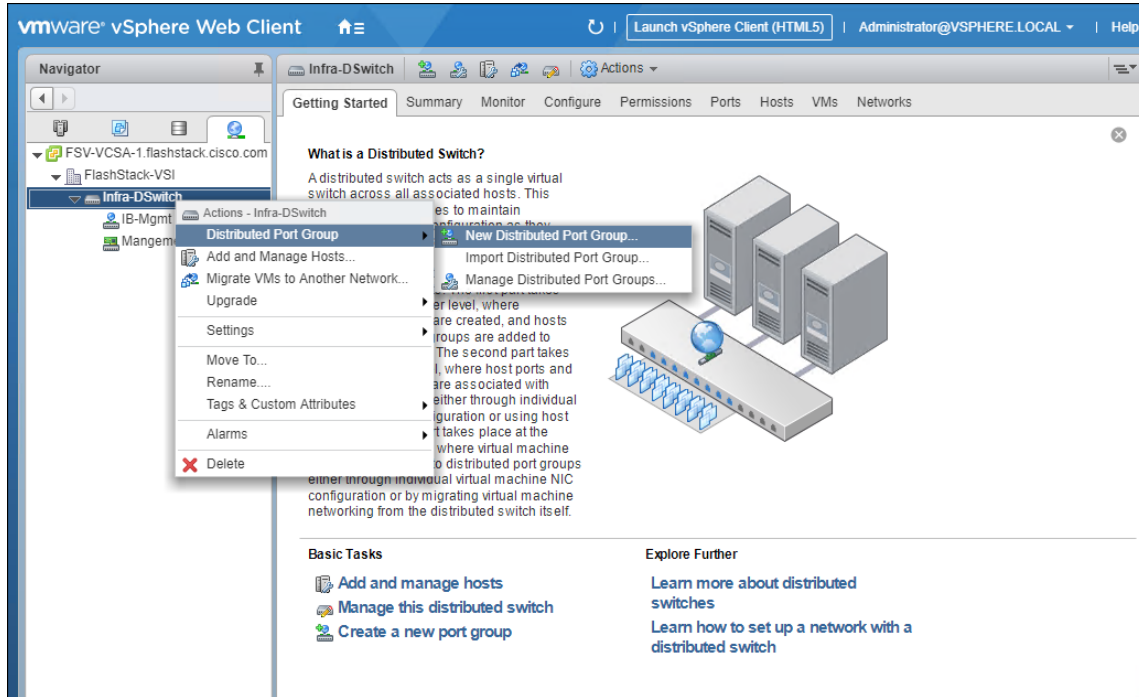
12. Click VLAN, changing VLAN type from None to VLAN, and enter in the appropriate VLAN number for the IB-Mgmt network.
13. Click the Teaming and Failover and move the Uplinks 3 and 4 to the Unused uplinks state and move the Uplink 2 to the Standby uplinks state.



The movement of Uplink 2 to standby is guiding Management traffic to stay within the A side fabric contained within Uplink 1 to prevent unnecessary traffic hops up into the Nexus switch to traverse between fabrics. Uplinks 3 and 4 are set as unused as these are the vMotion vNICs and will be used by the other Distributed Port Group in this vDS.

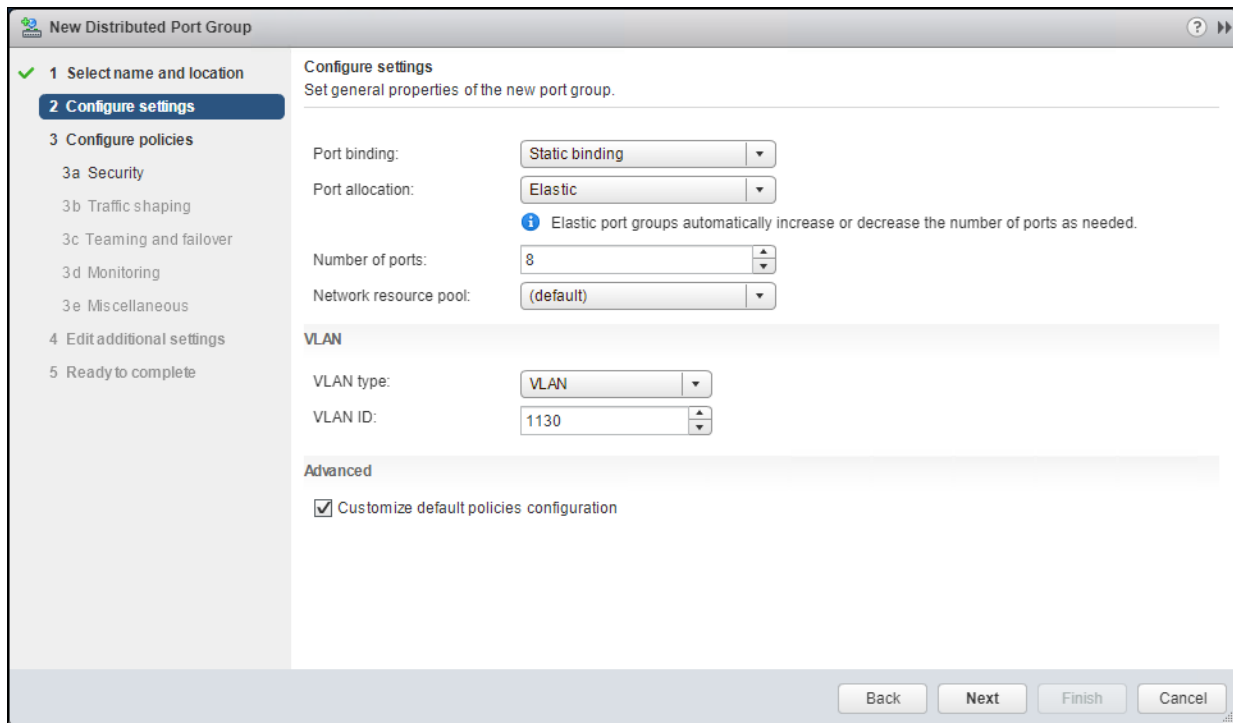


14. Click OK to save the changes.
15. Right-click the infrastructure vDS (Infra-DSwitch), and select Distributed Port Group -> New Distributed Port Group...



16. Name the new Port Group vMotion and click Next.

17. Change the VLAN type from None to VLAN, select the VLAN ID appropriate for your vMotion traffic, and select the Customize default policies configuration check box under the Advanced section.



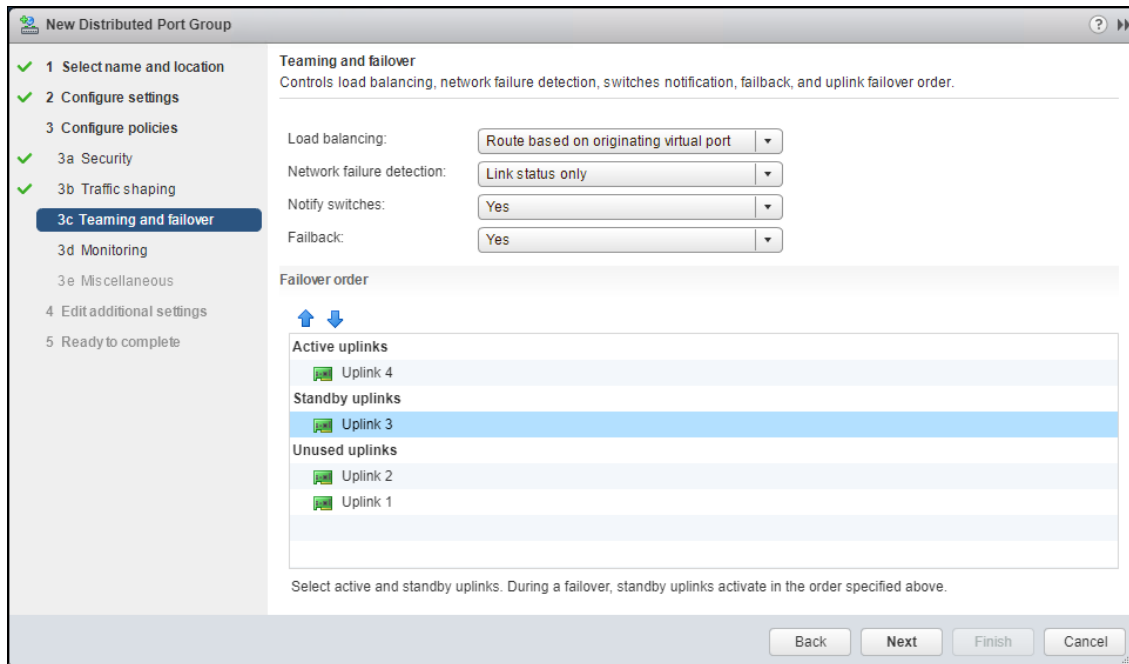
18. Click Next.

19. Click Next through the Security and Traffic Shaping sections.

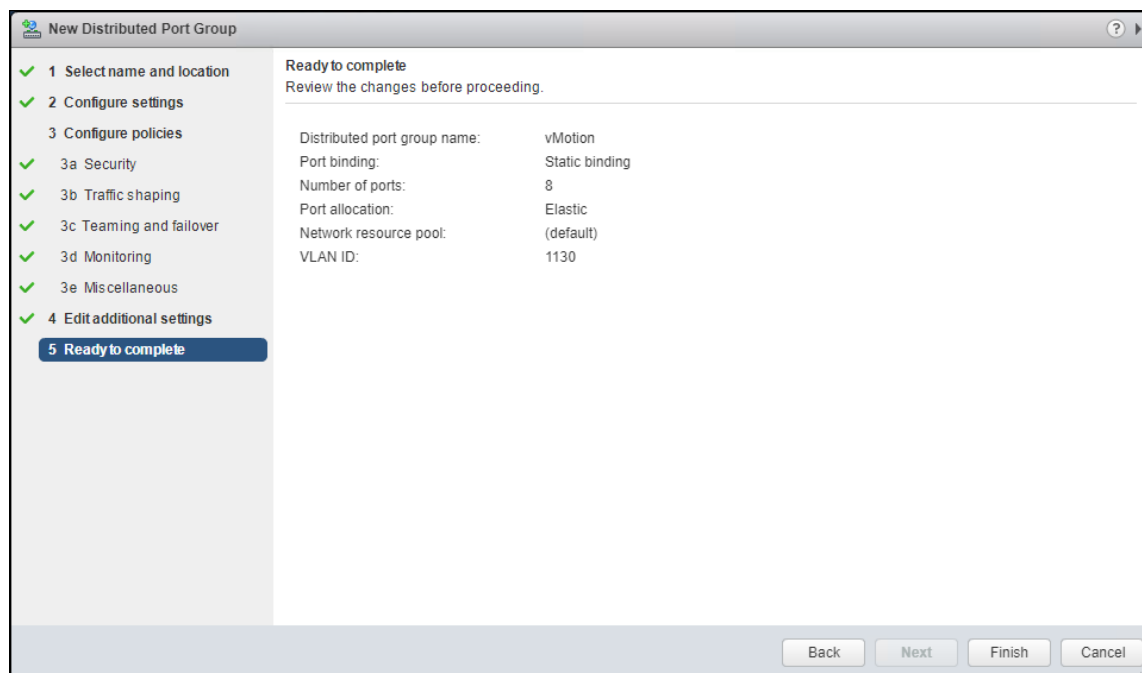
20. Within the Teaming and failover section, move Uplinks 1 & 2 to the Unused uplinks section, and move Uplink 3 to the Standby uplinks section.



Teaming for the vMotion Distributed Port Group will be a mirror of teaming on the Infrastructure Distributed Port group. Uplinks 1 and 2 are unused because they are used by the Infrastructure Distributed Port group, and Uplink 3 will be moved to standby to guide vMotion traffic to stay within the B side fabric contained within Uplink 4.



21. Click Next
22. Click Next Past Monitoring, Miscellaneous, and Edit additional settings sections.
23. Review the Ready to complete section.

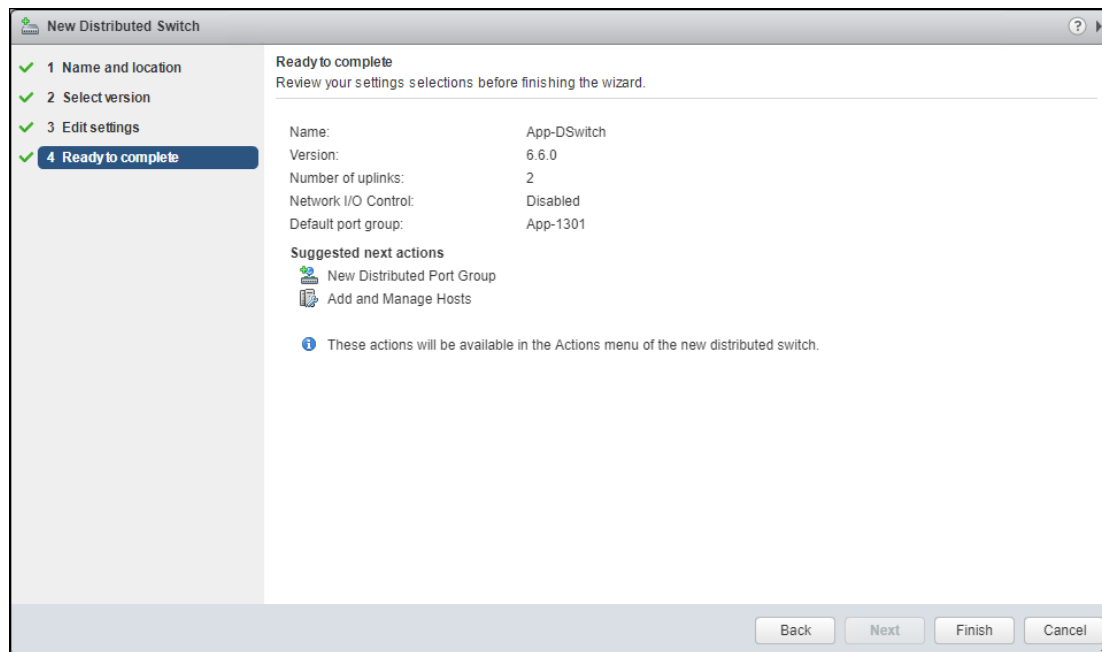


24. Click Finish to create the Distributed Port Group.

FlashStack Application vDS

To configure the second VMware vDS, follow these steps:

1. Right-click the FlashStack-VSI Datacenter and select Distributed Switch -> New Distributed Switch... to create the Application vDS.
2. Provide a name for the vDS (App-DSwitch), and click Next.
3. Make sure Distributed switch: 6.6.0 is selected and click Next.
4. Change the Number of uplinks to 2. If VMware Network I/O Control is to be used for Quality of Service, leave Network I/O Control Enabled. Otherwise, Disable Network I/O Control. Enter App-1301 for the name of the default Port group to be created. Click Next.
5. Review the information and click Finish to complete creating the vDS.



6. Right-click the newly created App-DSwitch vDS, and select Settings -> Edit Settings...
7. Click the Advanced option for the Edit Settings window and change the MTU from 1500 to 9000.
8. Click OK to save the changes.
9. Right-click the App-1301 Distributed Port Group, and select Edit Settings...
10. Click VLAN, changing VLAN type from None to VLAN, and enter in the appropriate VLAN number for the first application network.



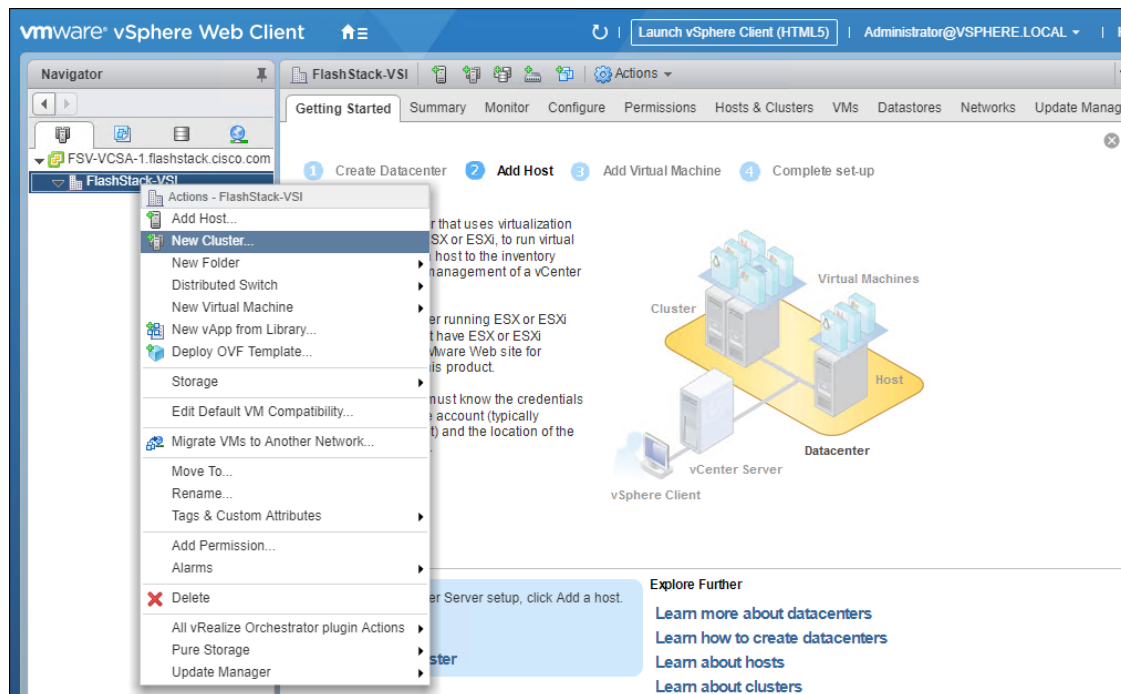
The application Distributed Port Groups will not need to adjust their NIC Teaming as they will be Active/Active within the two vNICs uplinks associated to the App-DSwitch, using the default VMware Route based on originating virtual port load balancing algorithm.

11. Click OK to save the changes.
12. Right-Click the App-DSwitch, selecting Distributed Port Group -> New Distributed Port Group... for any additional application networks to be created, setting the appropriate VLAN for each new Distributed Port Group.

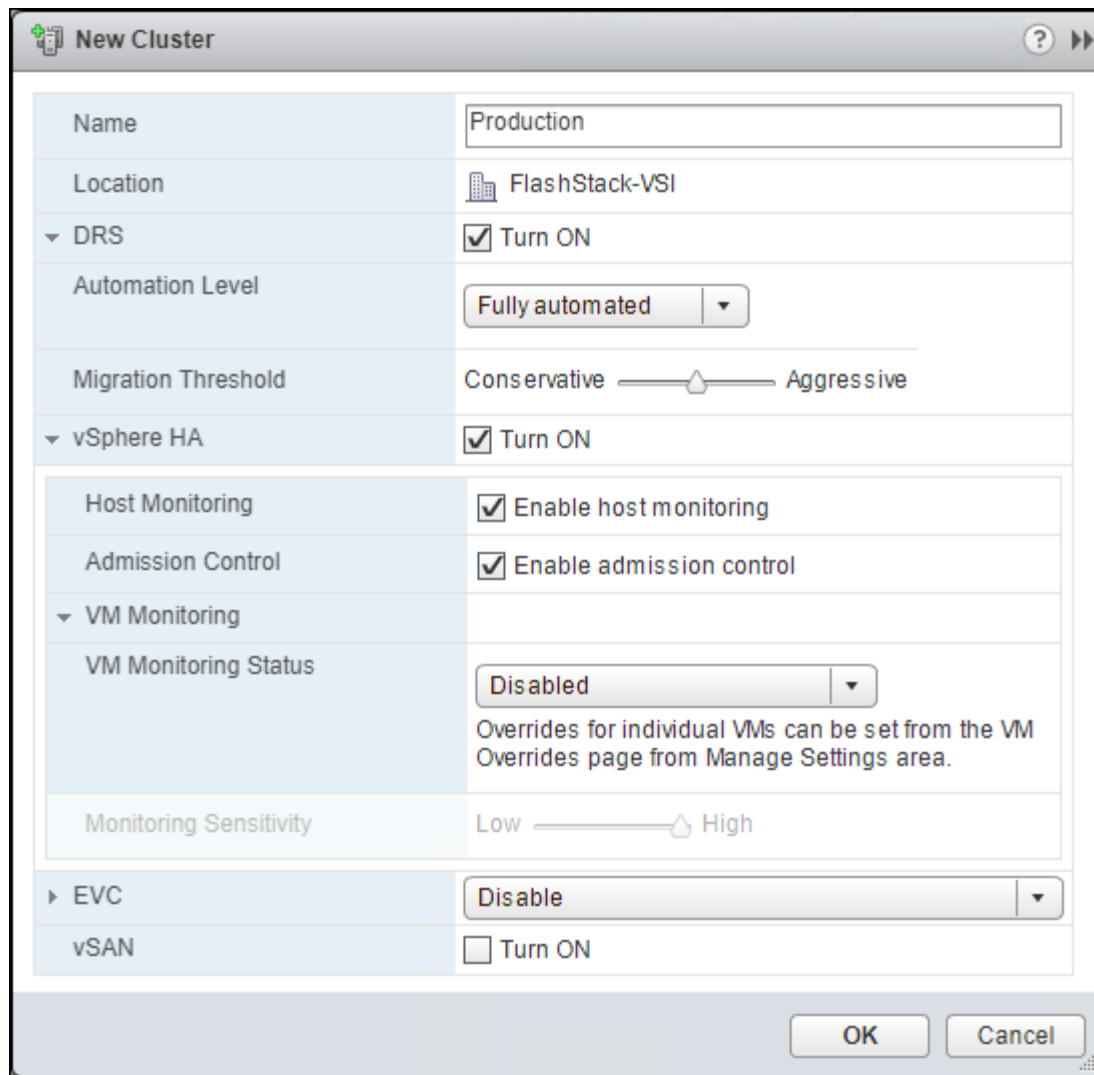
Add the VMware ESXi Hosts Using the VMware vSphere Web Client

To add the VMware ESXi Hosts using the VMware vSphere Web Client, follow these steps:

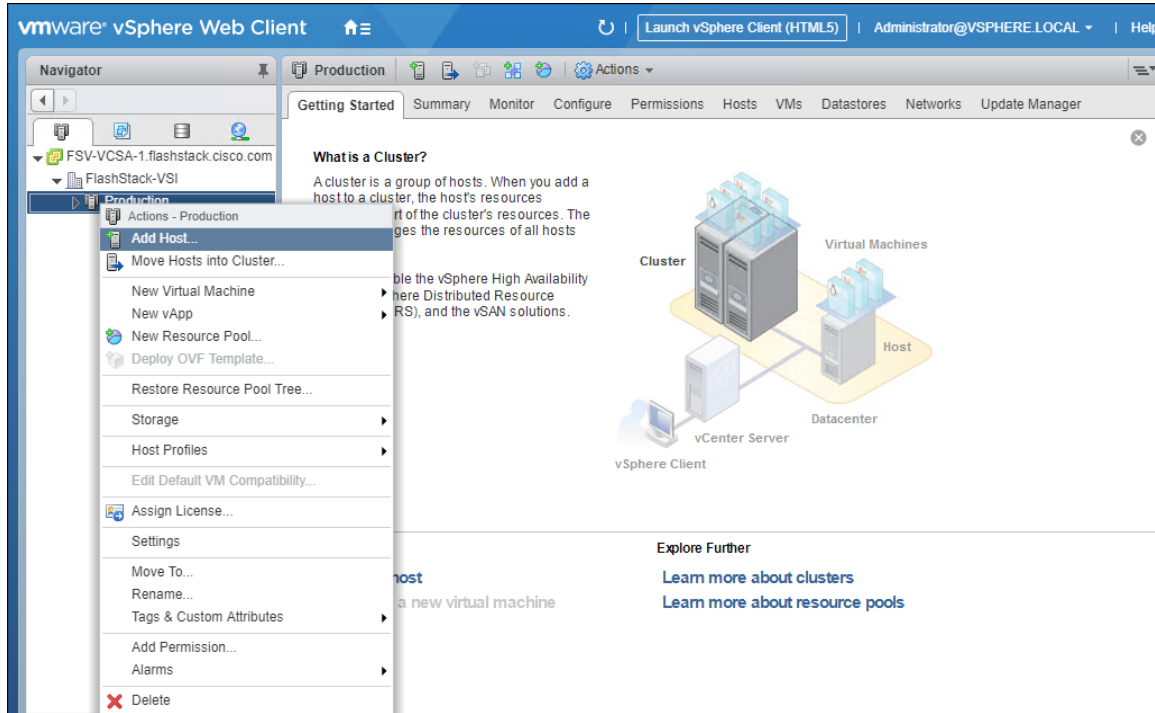
1. From the Hosts and Clusters tab, right-click the new or existing Datacenter within the Navigation window and select New Cluster... from the drop-down options.



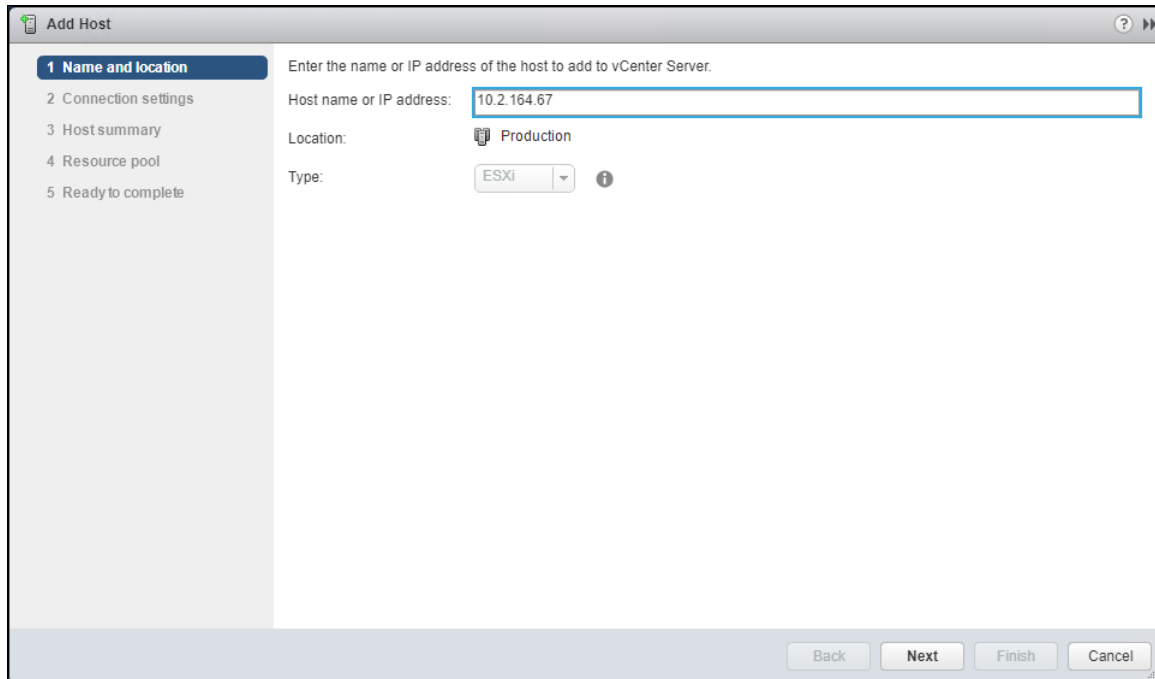
2. Enter a name for the new cluster, select the DRS and HA checkmark boxes, leaving all other options with defaults.



3. Click OK to create the cluster.
4. Right-click the newly created cluster and select Add Host..



5. Enter the IP or FQDN of the first ESXi host and click Next.

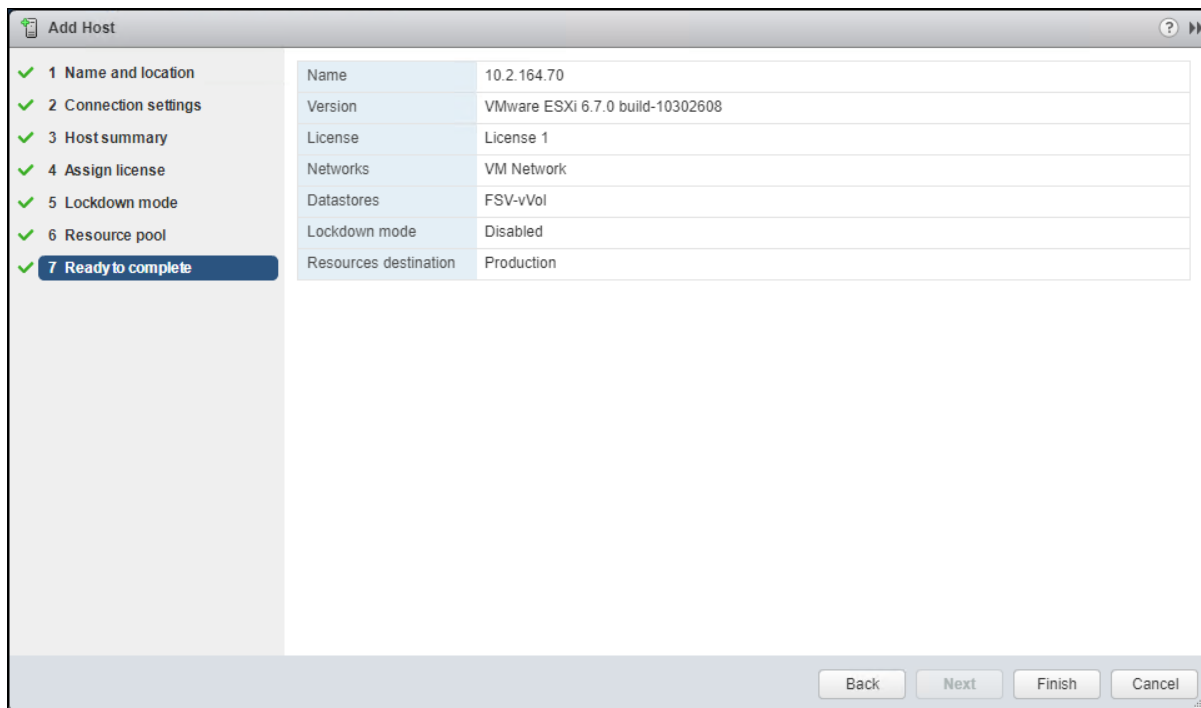


6. Enter root for the User Name, provide the password set during initial setup and click Next.

7. Click Yes in the Security Alert pop-up to confirm the host's certificate.

8. Click Next past the Host summary dialogue.

9. Provide a license by clicking the green + icon under the License title, select an existing license, or skip past the Assign license dialogue by clicking Next.
10. Leave lockdown mode Disabled within the Lockdown mode dialogue window and click Next.
11. Skip past the Resource pool dialogue by clicking Next.
12. Confirm the Summary dialogue and add the ESXi host to the cluster by clicking Next.



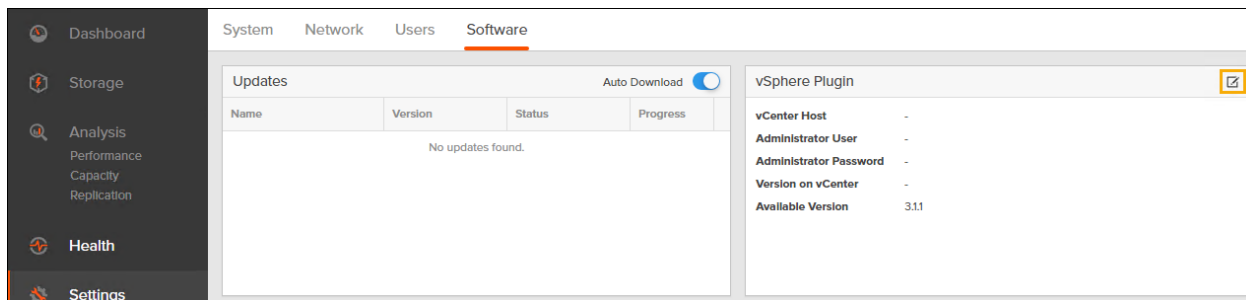
13. Repeat steps 4-12 for each ESXi host to be added to the cluster.

Pure Storage vSphere Web Client Plugin

The Pure Storage vSphere Web Client Plugin will be accessible through the vSphere Web Client after registration through the Pure Storage Web Portal.

To access the Pure Storage vSphere Web Client Plugin, follow these steps:

1. Go to Settings > Software
2. Select the edit icon in the vSphere Plugin panel



3. Enter the vCenter information in the pop-up window and click Save.

Edit vSphere Plugin Configuration

vCenter Host 10.164.20

Administrator User administrator@vsphere.local

Administrator Password

Cancel Reset Save

4. After the discovery completes. Click Install.

vSphere Plugin

vCenter Host 10.164.20

Administrator User administrator@vsphere.local

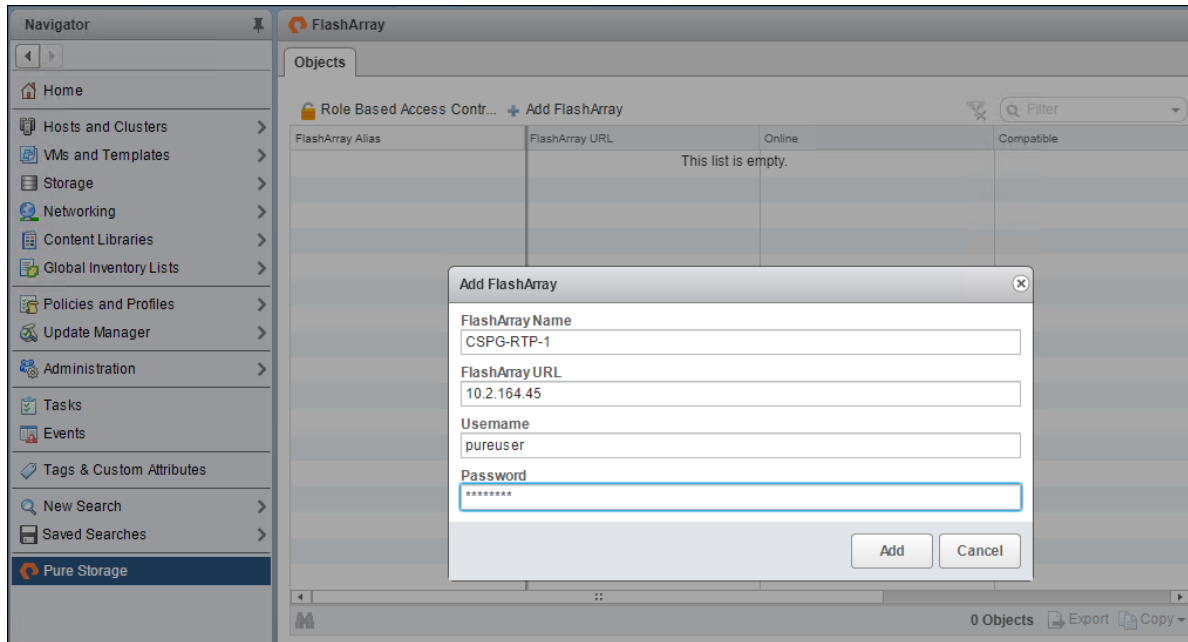
Administrator Password ****

Version on vCenter -

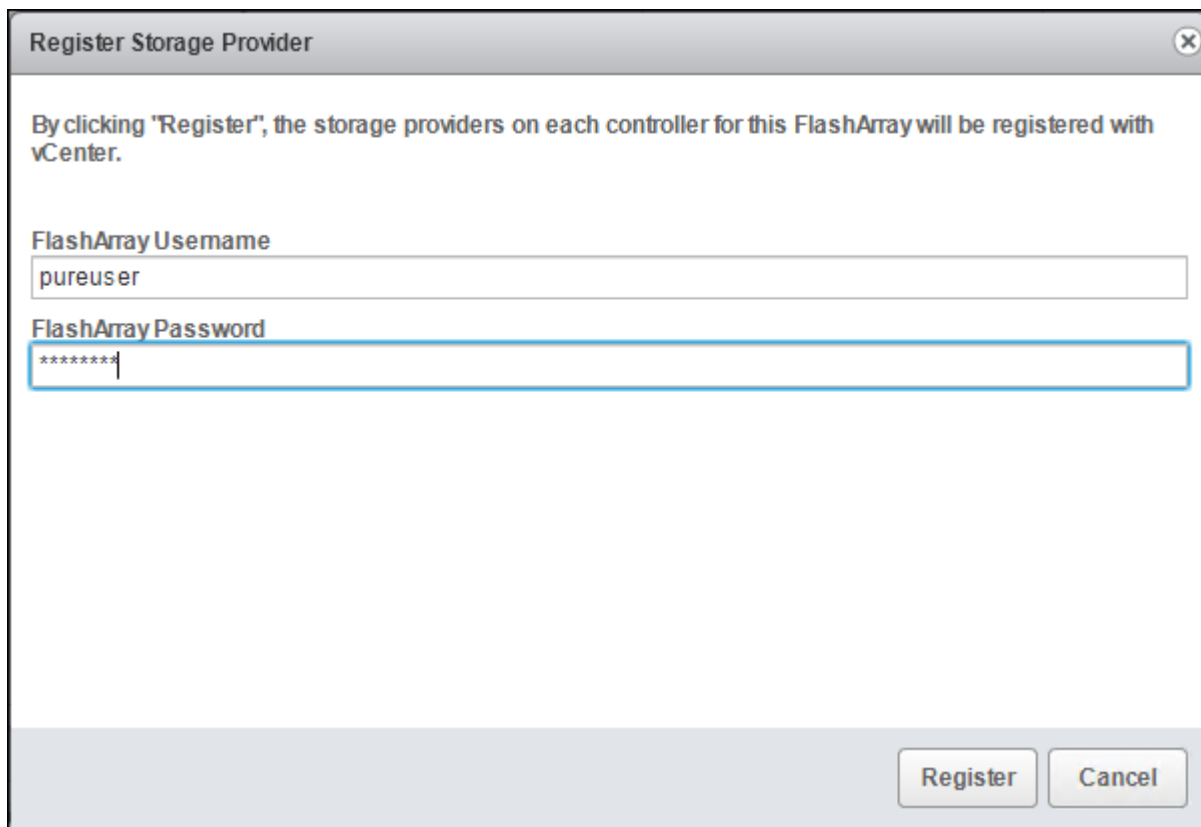
Available Version 3.1.1

Install

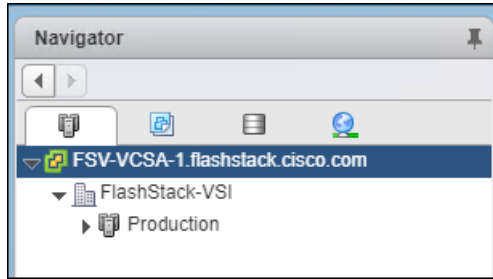
5. In vCenter, register the FlashArray to the plugin by navigating to Home and selecting the Pure Storage Plugin. Then select Add FlashArray



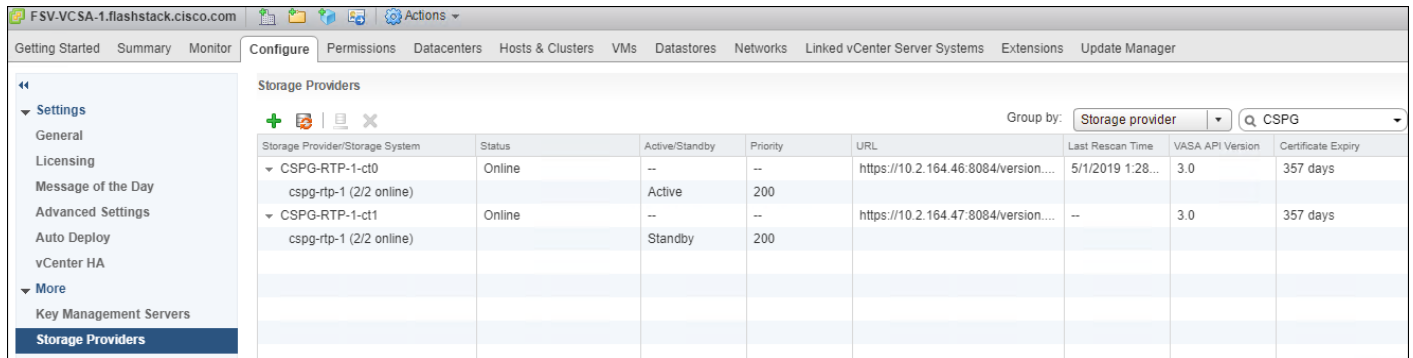
6. Add the FlashArray as a Storage Provider by clicking the 'Register Storage Provider' (🗄️) icon and providing the login information for the FlashArray.



7. Verify that the FlashArray is registered correctly as a storage provider.
8. Select Host and Cluster, Select the vCenter Server.



9. Select Configure > Storage Providers.
10. Filter on the name.

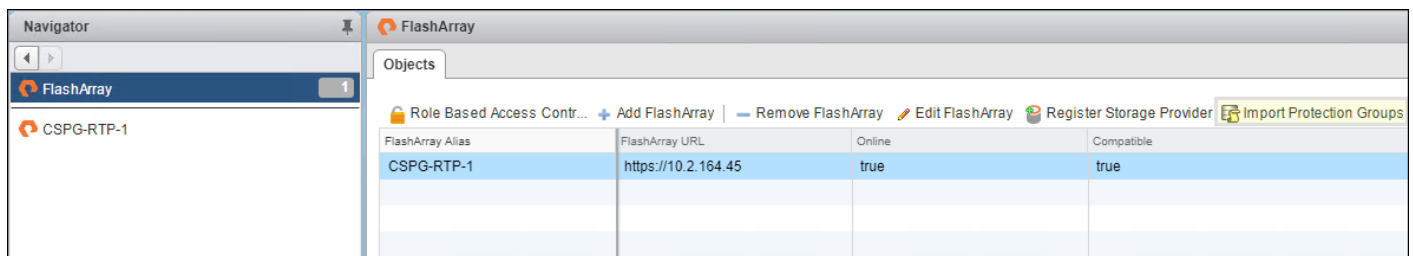


11. Verify that one controller is Active and the other is Standby.

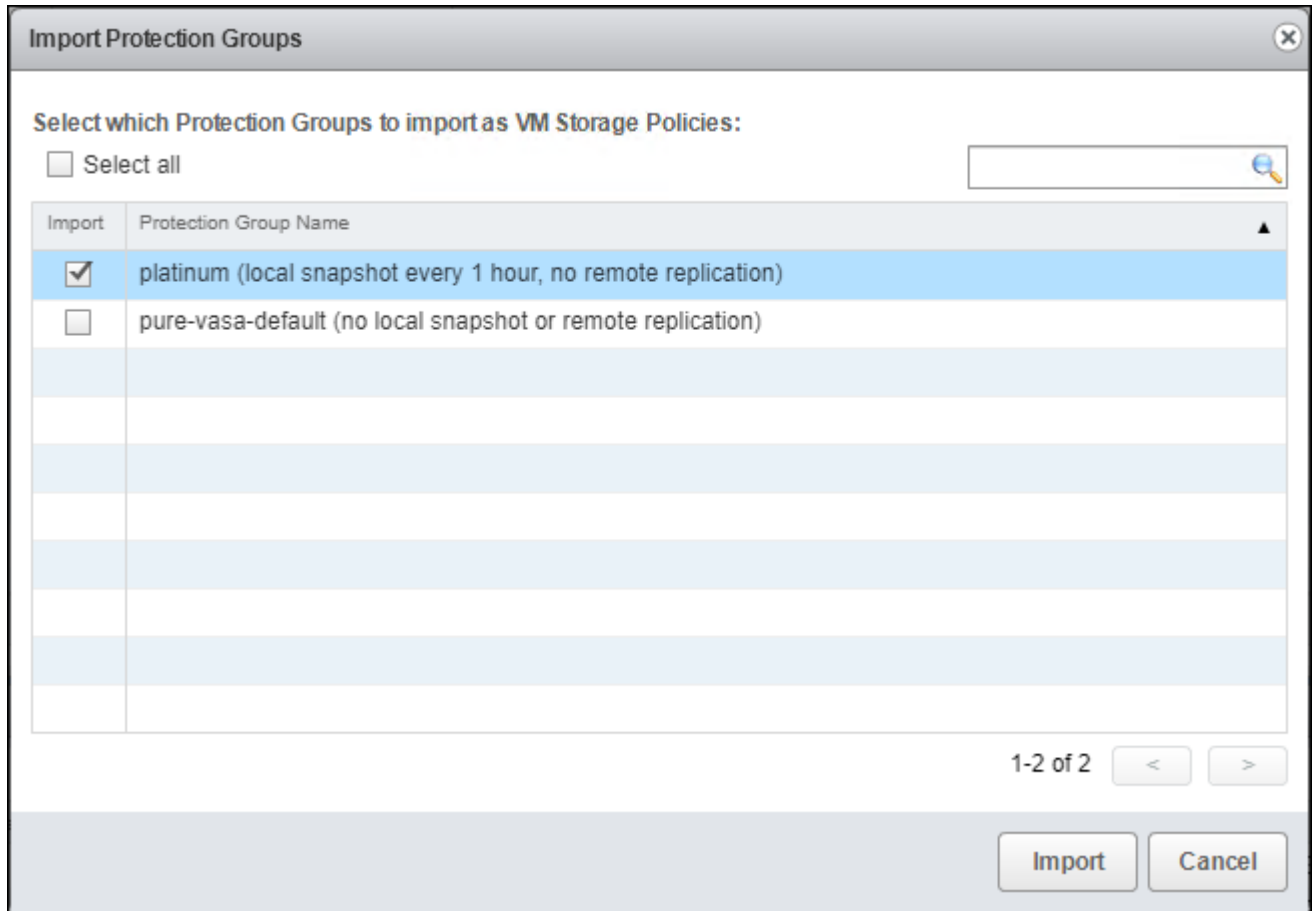
Import Protection Group as VM Storage Policy

To import the FlashArray Protection Group settings as VM Storage Policies, follow these steps:

1. From the vSphere Web Client home screen Select the Pure Storage Plugin.
2. Select Import Protection Groups.



3. Select the local snapshot Protection Group that was created during the “Configure Storage Policy Based Management” step and click Import.



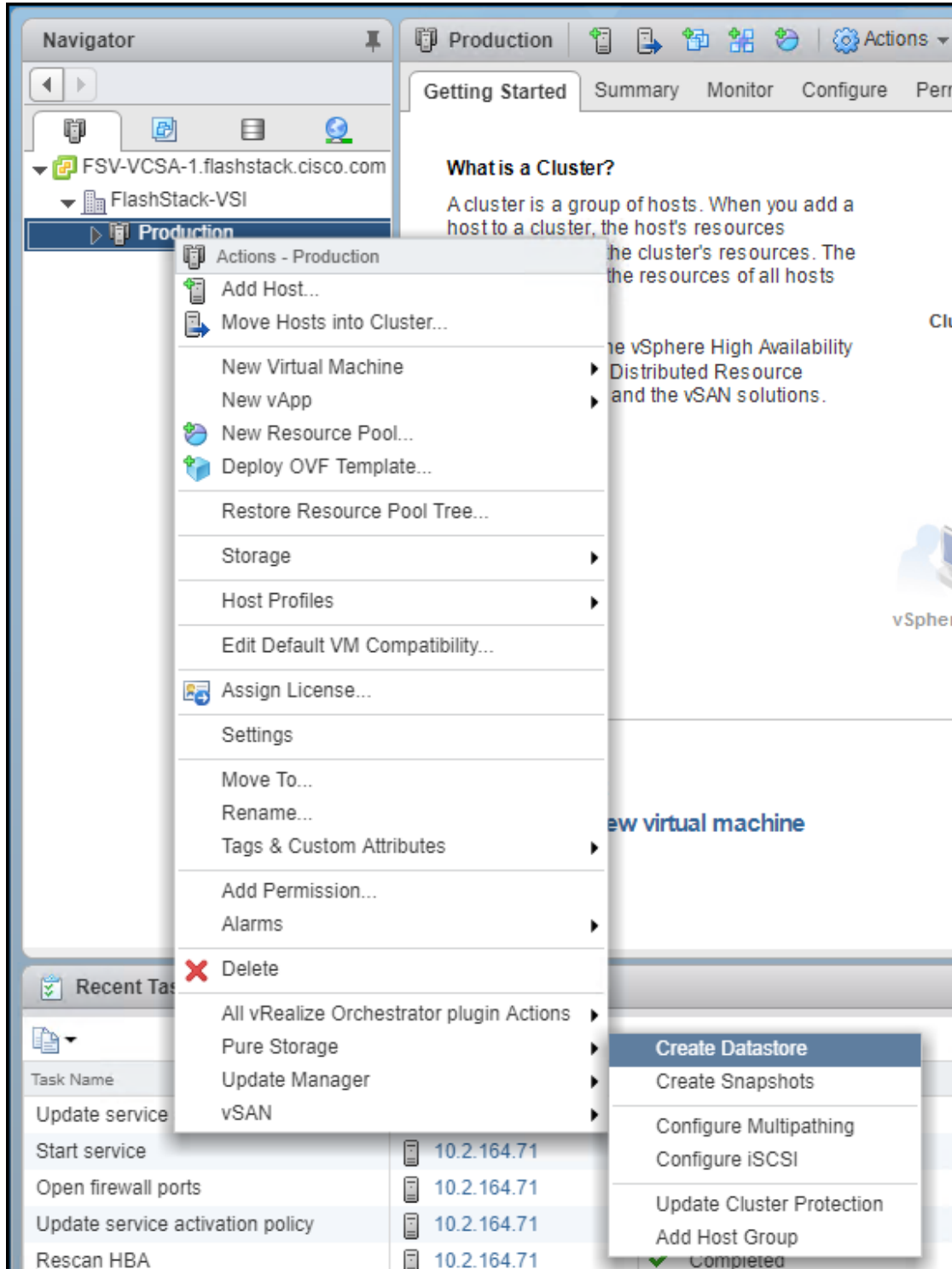
Add Datastores

This section details the steps to add VMFS to place swap and driver files and a VVol datastore to place VMs on the FlashArray//X R2.



A dedicated swapfile location will not provide a performance increase over the existing all flash datastores created from the FlashArray//X R2 but can be useful to have these files in a separate location to have them excluded from snapshots and backups.

1. Right-click the cluster and select the Pure Storage -> Create Datastore option from the drop-down list.



2. Select Datastore type VMFS, provide a Datastore Name, Datastore size, Cluster, and Select VMFS 6.

Create Datastore

Datastore Type

VMFS
 Wol

Datastore Name

ESXi-Swap

Datastore Size

1 TB

VMFS Options

VMFS 5
 VMFS 6

Select Pure Storage Array

CSPG-RTP-1

Select Host / Cluster

Production

1-1 of 1

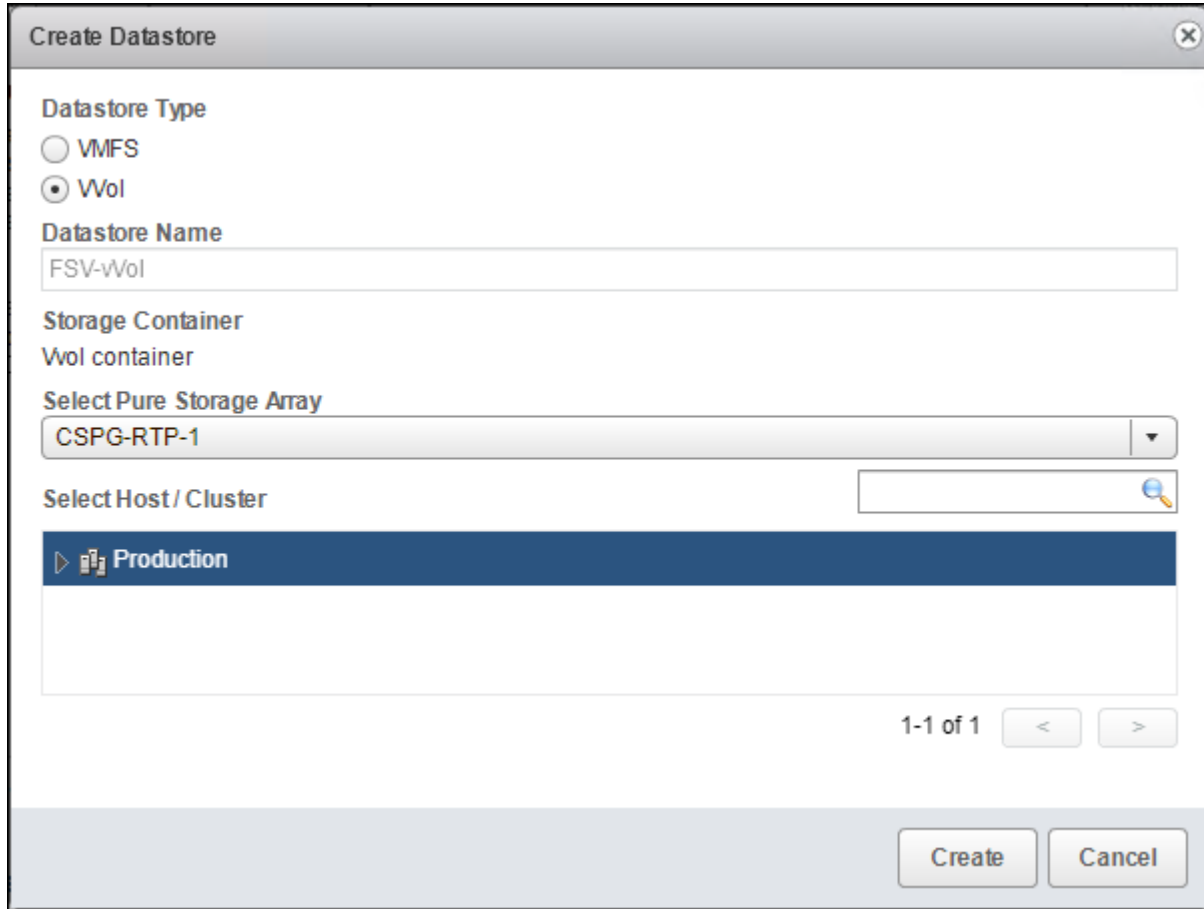
Pure Storage Protection Group (optional)

Joined

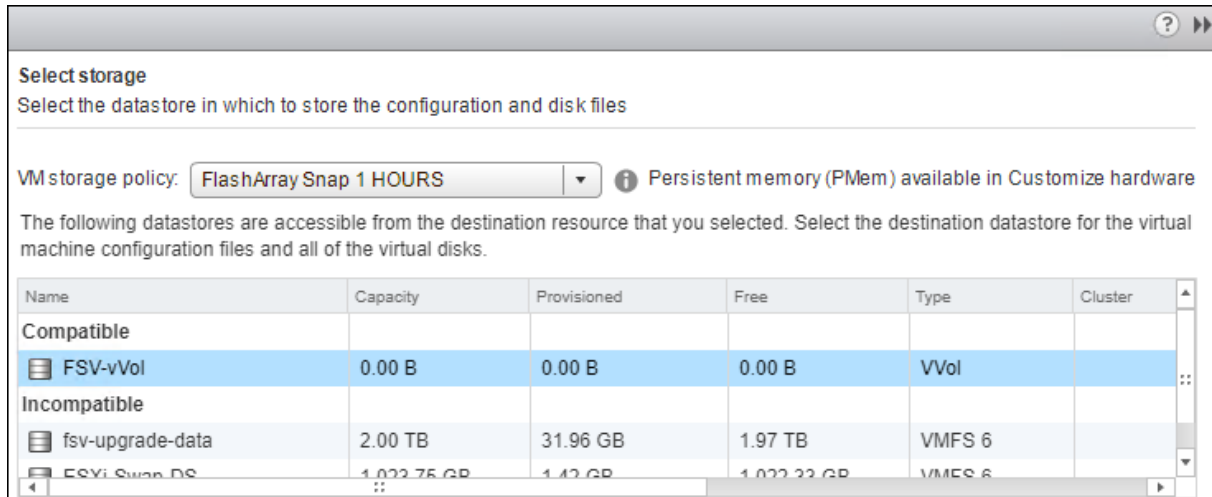
Joined	Protection Group Name

Create Cancel

3. Right-click the cluster and select the Pure Storage -> Create Datastore option from the drop-down list to create a second datastore.
4. Select Datastore Type WVol and click Create to finish.



You will now be able to select the VM storage policy when creating or migrating Virtual Machines.

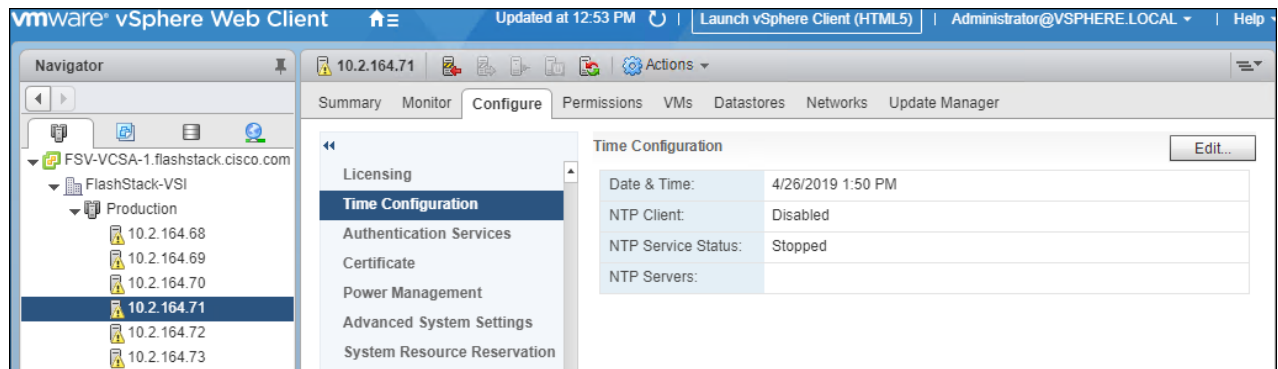


Configure ESXi Settings

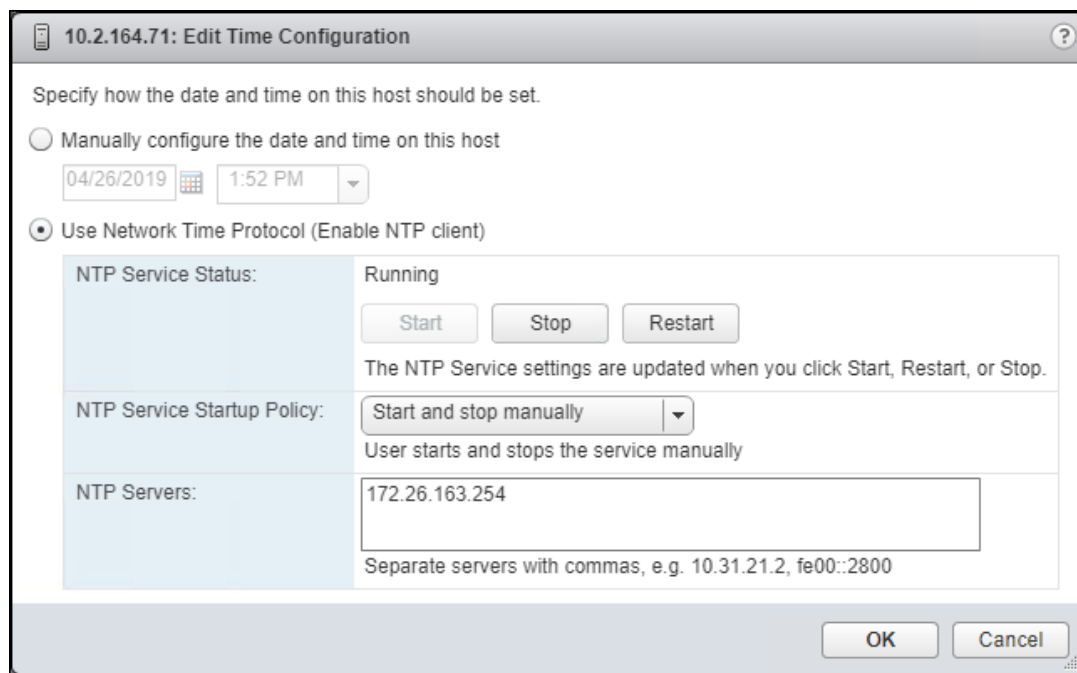
Base settings are needed for the stability of the vSphere environment, as well as optional enablement of SSH connectivity to each host for the updating of drivers.

To configure ESXi settings, follow these steps:


1. Select the first ESXi host to configure with standard settings.
2. Select the Configure tab and select Time Configuration within the options under System and click Edit within Time Configuration.



3. Select Use Network Time Protocol (Enable NTP client), enter <<var_oob_ntp>> for the NTP Servers, select Start and stop with port usage for NTP Service Startup Policy, and click Start within NTP Service Status. Click OK to submit the changes.



4. (Optional) Click Security Profile within the Configure tab under the System section for the host.

 Security Profile settings of ESXi Shell and SSH are enabled for the potential update of the nenic driver later. These steps are unnecessary if using VMware Update Manager and these drivers are being handled by being included into a configured baseline. If SSH is enabled for updates, it is recommended to later disable this service if it is considered a security risk in the environment.

The screenshot shows the VMware vSphere configuration interface. The 'Configure' tab is active, and the 'Security Profile' is selected in the left-hand navigation pane. The main content area is divided into two sections: 'Services' and 'Firewall'.

Services Section:

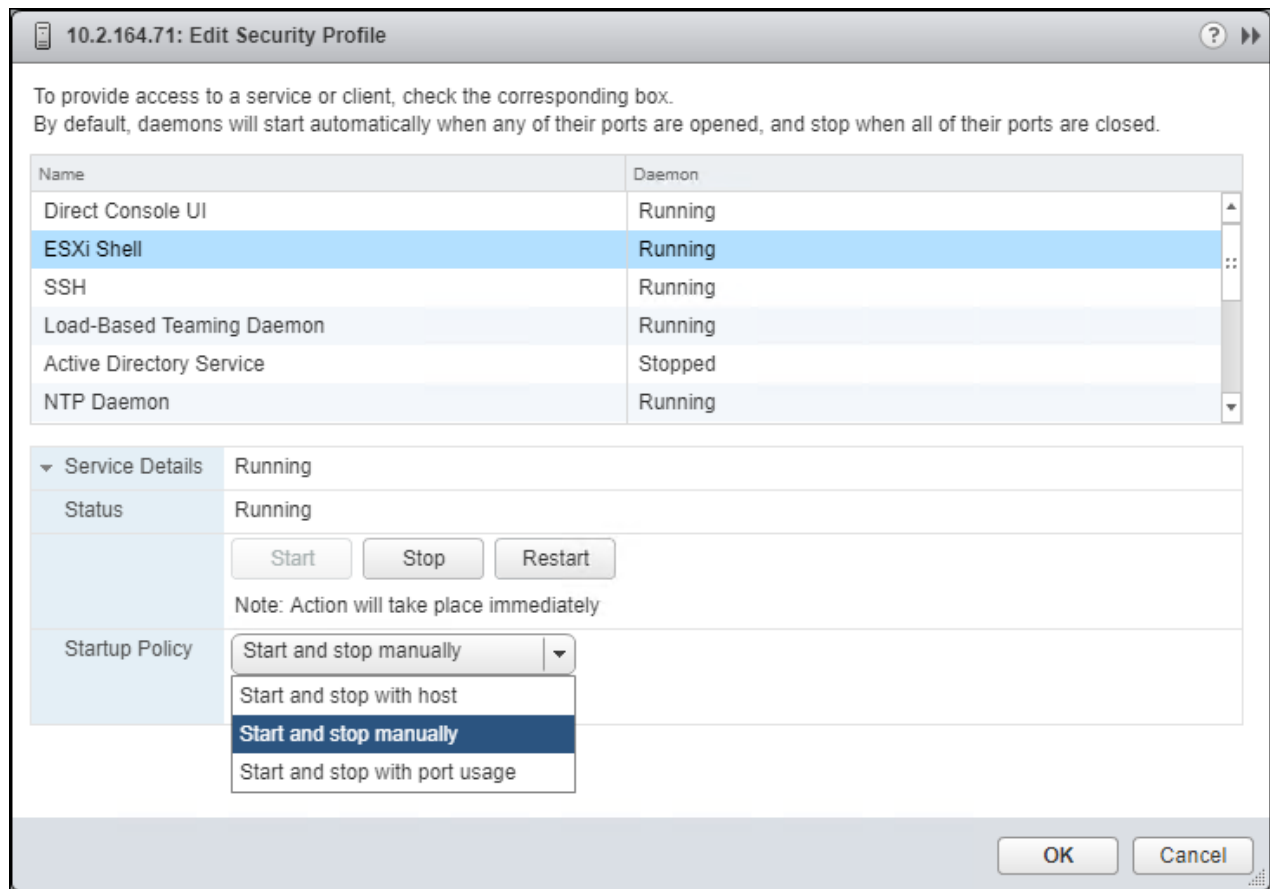
Name	Daemon
Direct Console UI	Running
ESXi Shell	Running
SSH	Running
Load-Based Teaming Daemon	Running
Active Directory Service	Stopped
NTP Daemon	Running
PC/SC Smart Card Daemon	Stopped
CIM Server	Stopped
SNMP Server	Stopped
Syslog Server	Running
vSphere High Availability Agent	Running
VMware vCenter Agent	Running
X.Org Server	Stopped

Firewall Section:

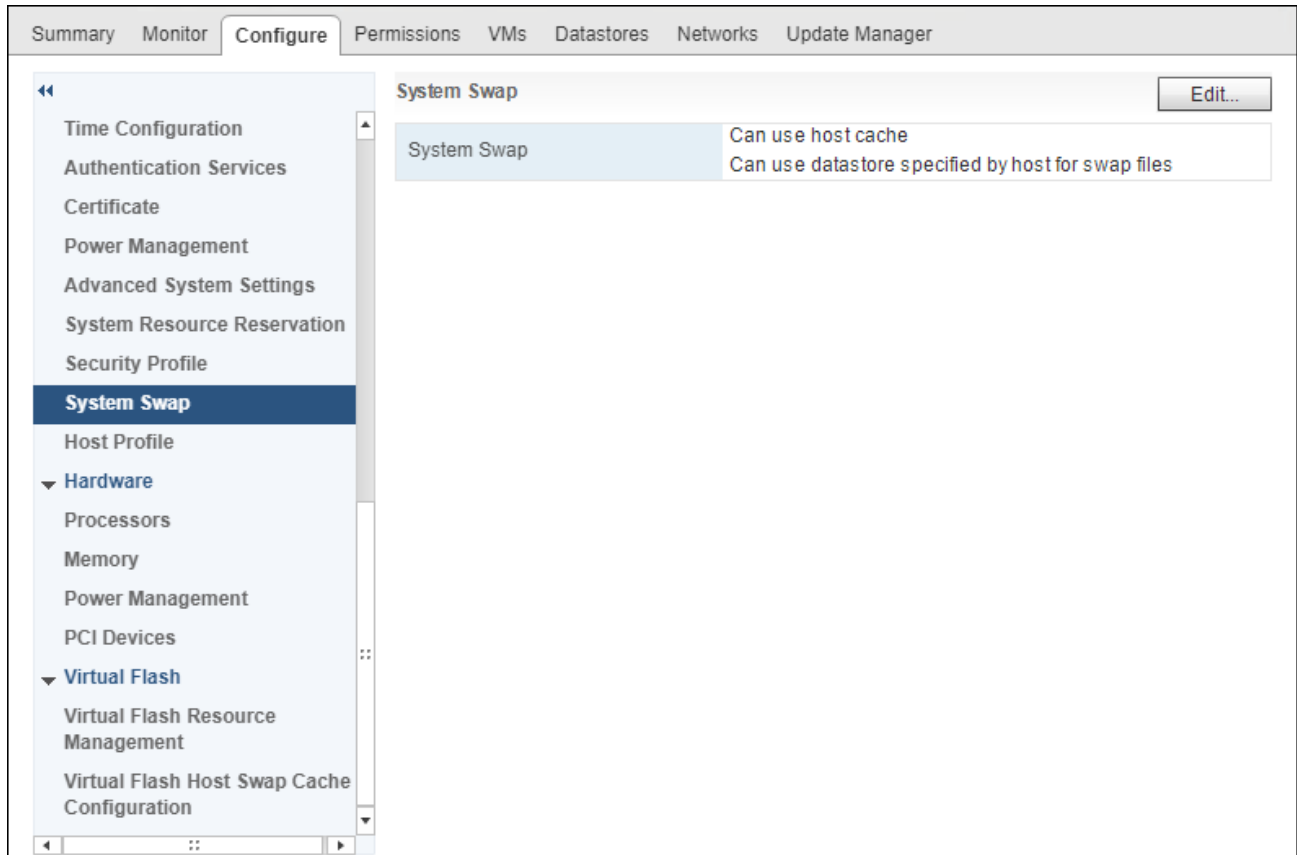
The Firewall section is expanded to show 'Incoming Connections'.

Service	Port	Protocol	Action
CIM Server	5988	TCP	All
CIM Secure Server	5989	TCP	All
CIM SLP	427	UDP,TCP	All

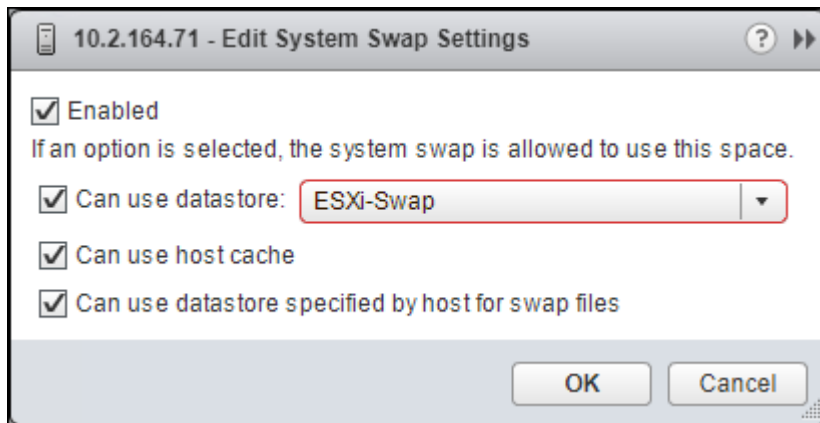
5. Scroll down to the Services section within Security Profile and click Edit.



6. Select the ESXi Shell entry, change the Startup Policy to Start and stop with port usage, and click Start. Repeat these steps for the SSH entry. Click OK.



7. If an optional ESXi swap datastore was configured earlier, click System Swap the System section within the Configure tab and click Edit.



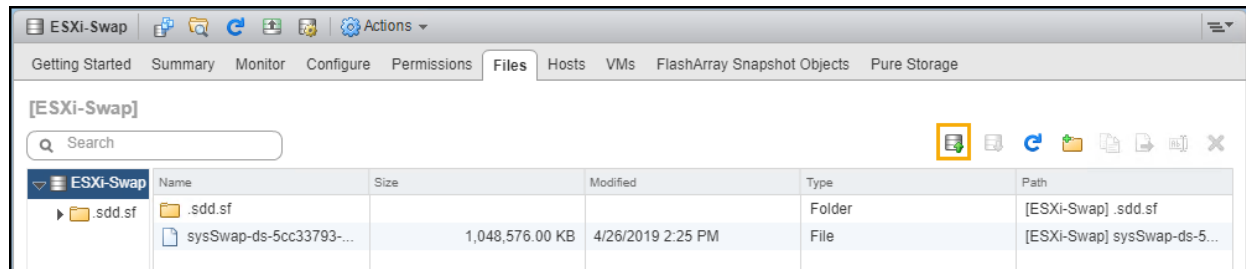
8. Checkmark the Can use datastore option, and from the drop-down list select the ESXi swap datastore that was configured. Click OK.
9. Repeat steps 1-8 on each ESXi host being added into the cluster.

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

The Cisco Custom Image for VMware vSphere 6.7 U1 comes with the currently specified nenic 1.0.25.0 for Ethernet traffic from the ESXi host, an upgrade is recommended. For the most recent versions, please refer

to [Cisco UCS HW and SW Availability Interoperability Matrix](#). If a more recent driver is made available that is appropriate for VMware vSphere 6.7 U1, to update the drivers, follow these steps:

1. Download and extract either driver bundle (example nenic Driver version 1.0.26.0) to the system the vSphere Web Client is running from.
2. Within the vSphere Web Client, select one of the datastores common to all the hosts.



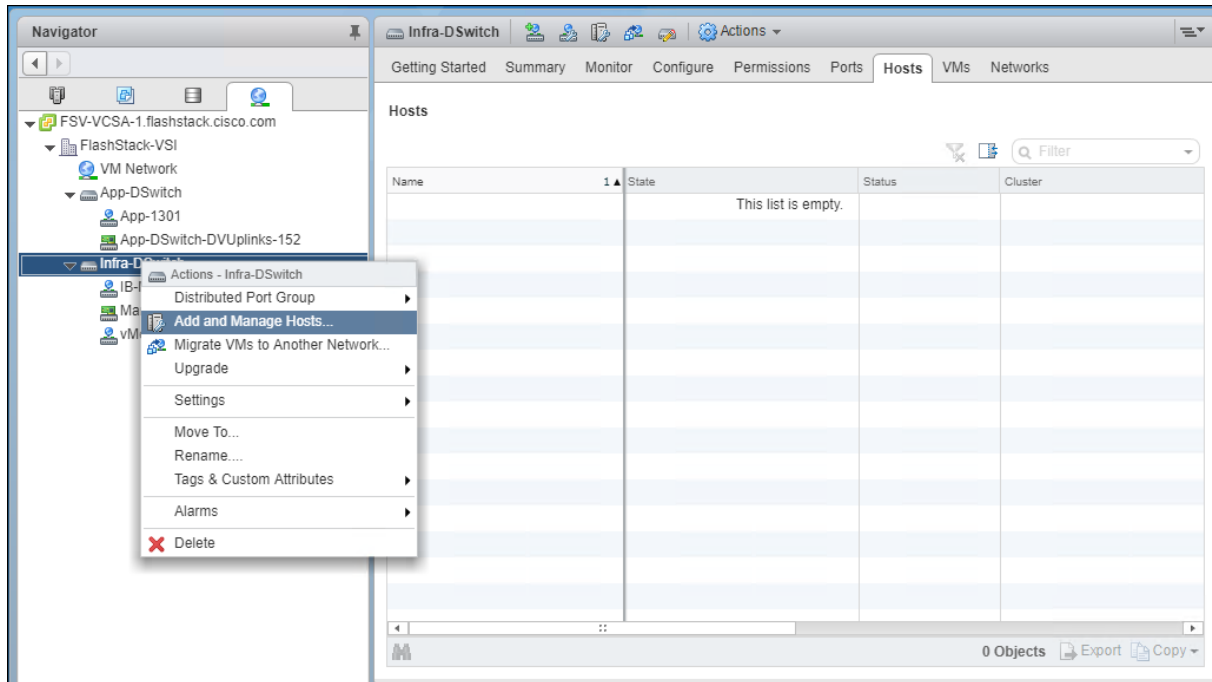
3. Click the Upload a file to the Datastore button.
4. Select and upload the offline_bundle (VMW-ESX-6.7.0-nenic-1.0.26.0-offline_bundle-10825029.zip) from each of the extracted driver downloads.
5. Place all hosts in Maintenance mode requiring update.
6. Connect to each ESXi host through ssh from a shell connection or putty terminal.
7. Login as root with the root password.
8. Run the following command (substituting the appropriate datastore directory if needed) on each host:


```
esxcli software vib update -d /vmfs/volumes/ESXi-Swap/VMW-ESX-6.7.0-nenic-1.0.26.0-offline_bundle-10825029.zip
```
9. Reboot each host by typing reboot from the SSH connection after the command has run.
10. Log into the Host Client on each host once reboot is complete.

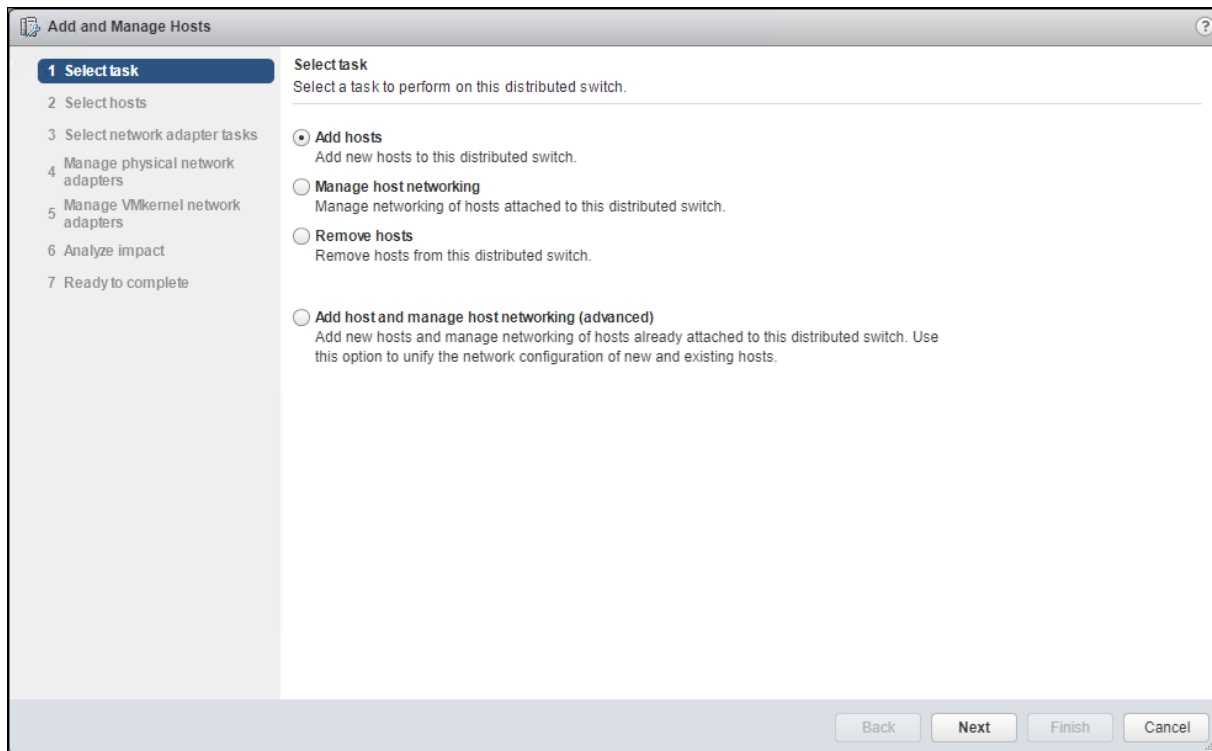
Add the ESXi Hosts to the vDS

To Add the ESXi Hosts to each vDS, follow these steps:

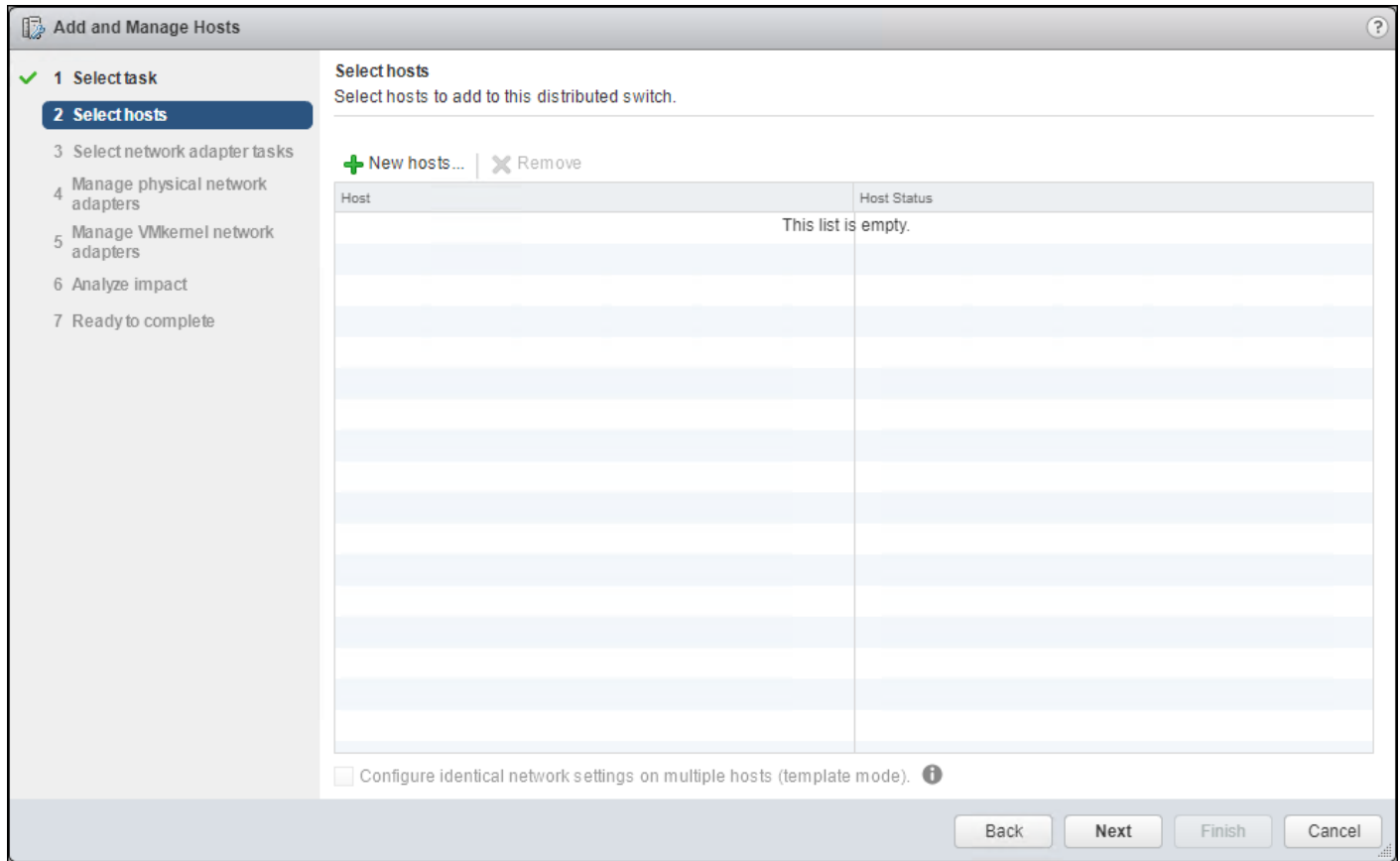
1. Within the Networking tab of the Navigator window, right-click the Infra-DSwitch vDS and select Add and Manage Hosts...



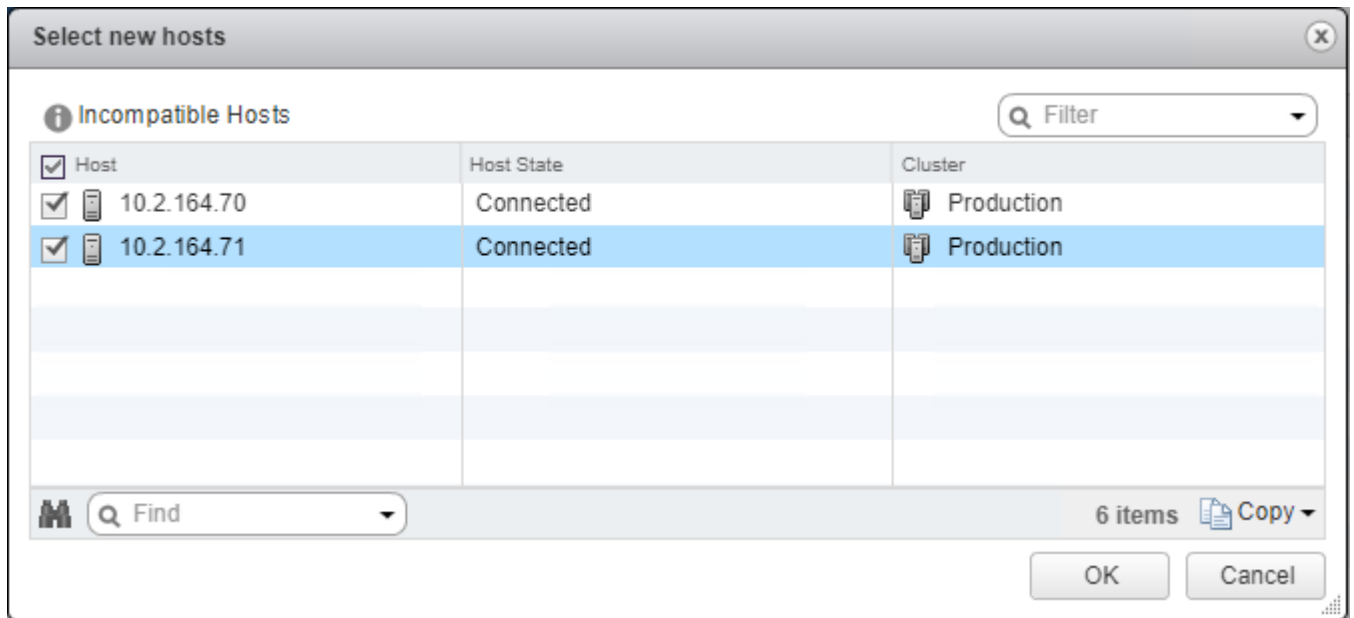
2. Leave Add hosts selected and click Next.



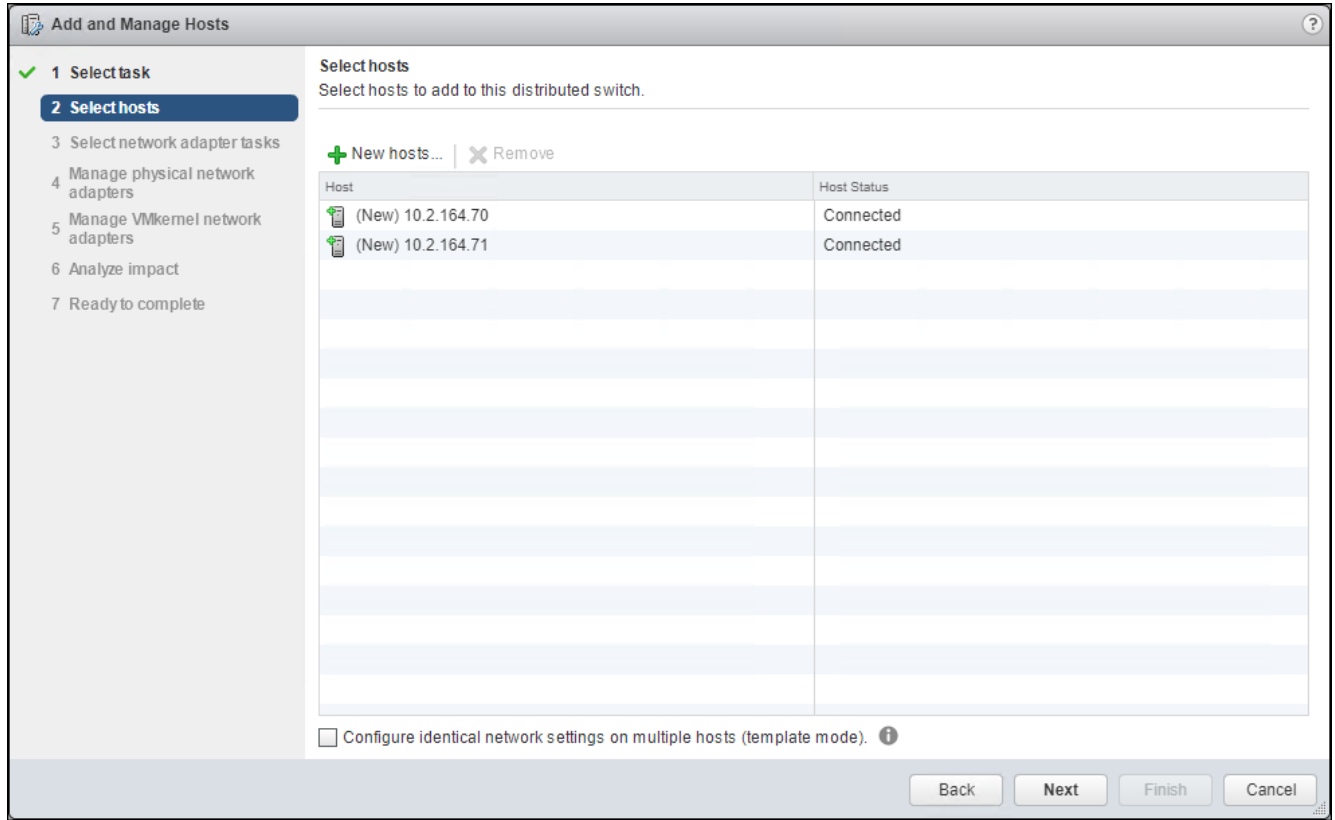
3. Click the green + icon next to New hosts...



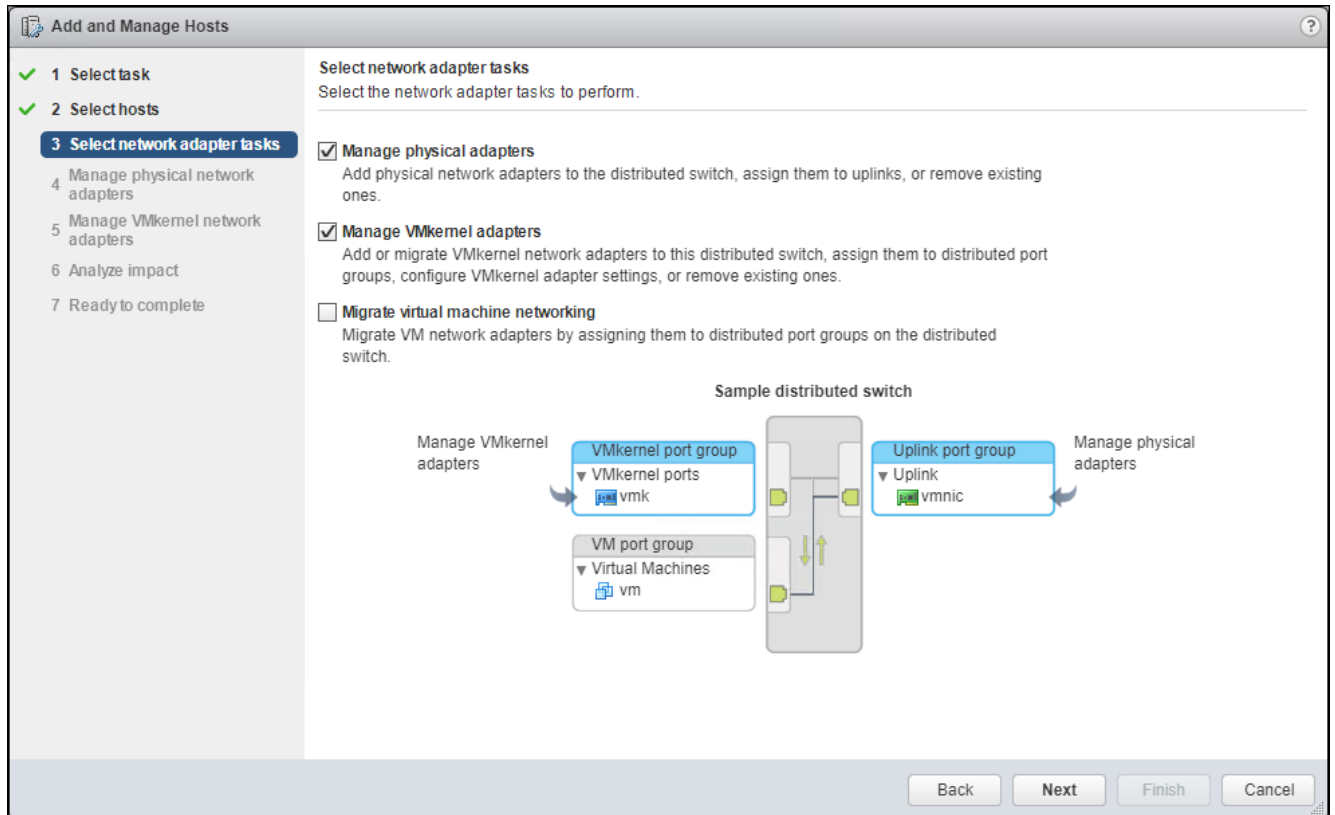
- In the Select new hosts pop-up that appears, select the hosts to be added, and click OK to begin joining them to the vDS.



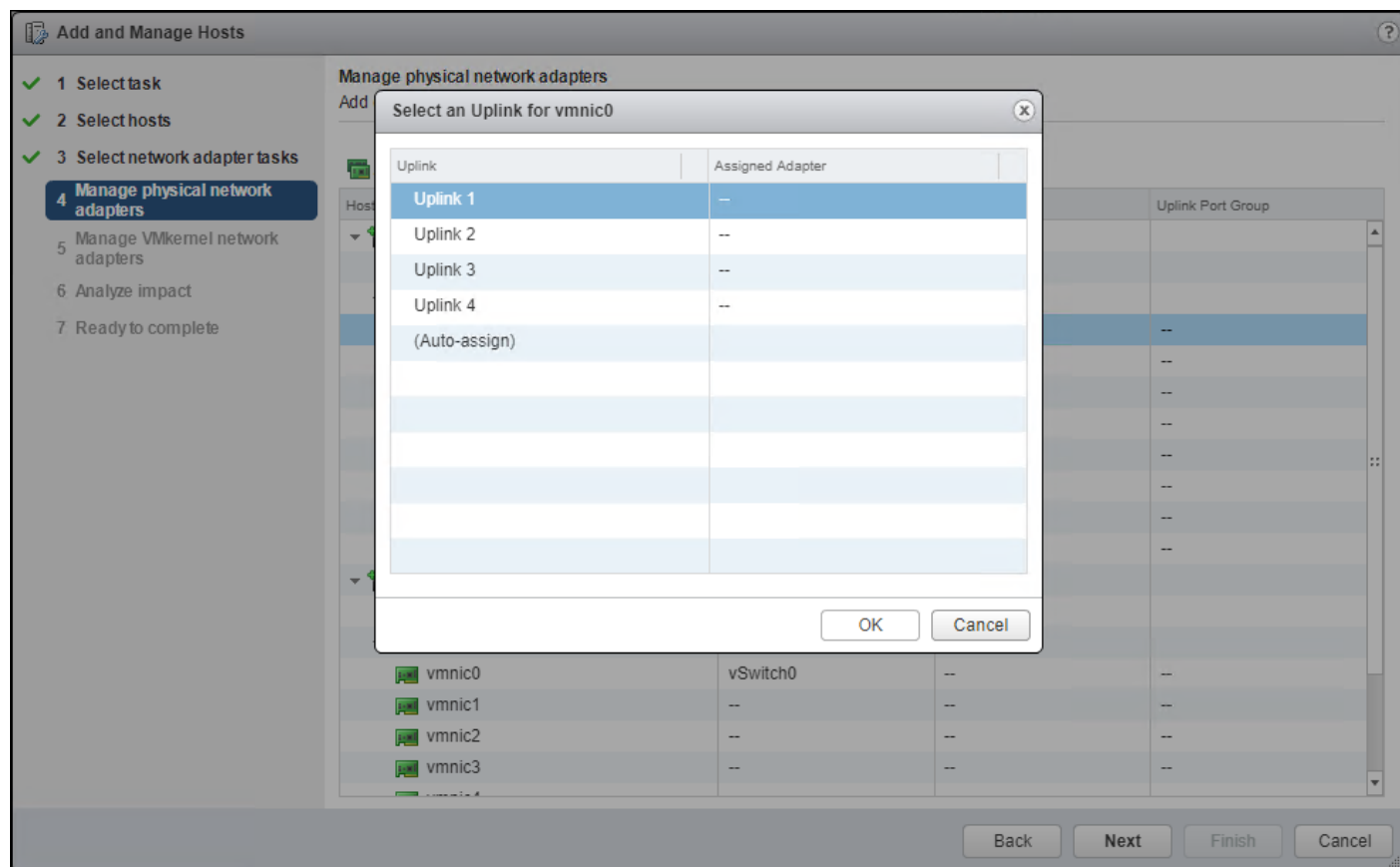
- Click Next.



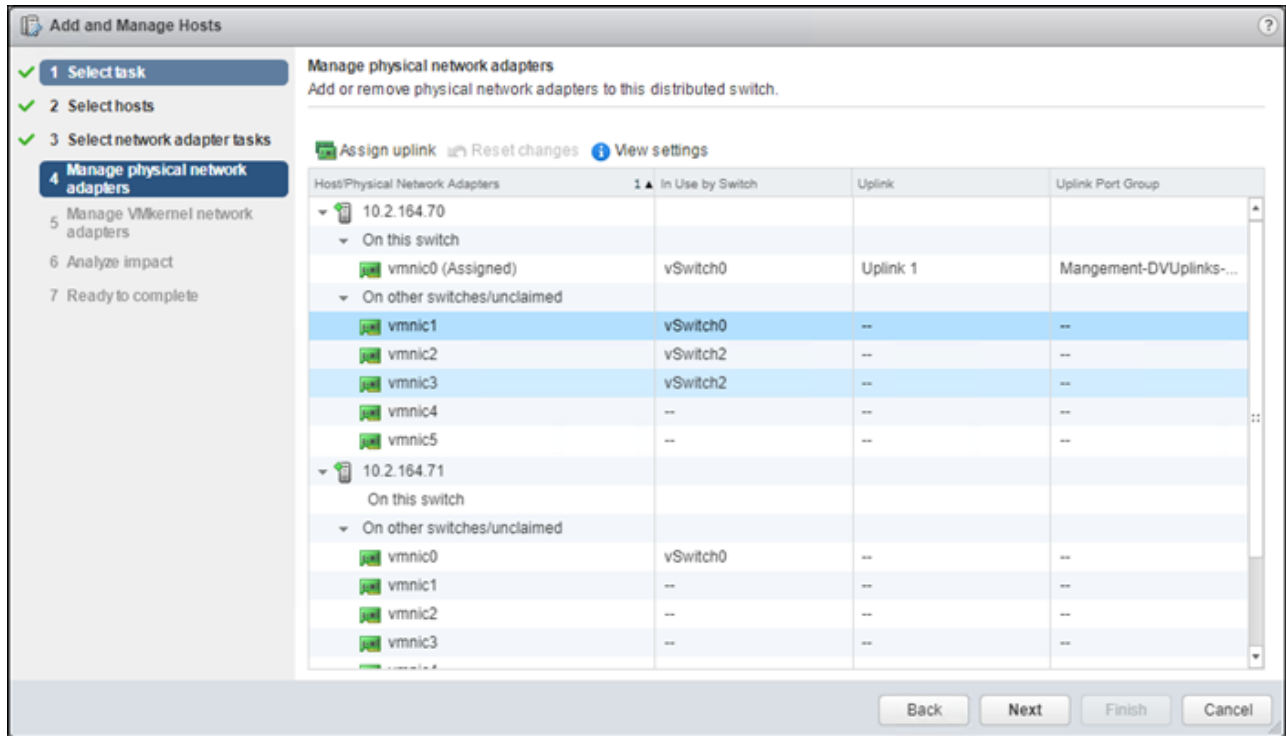
6. Leave Manage physical adapters and Manage VMkernel adapters both selected and click Next.



7. Select vmnic0 from the Host/Physical Network Adapters column and click the Assign uplink option.

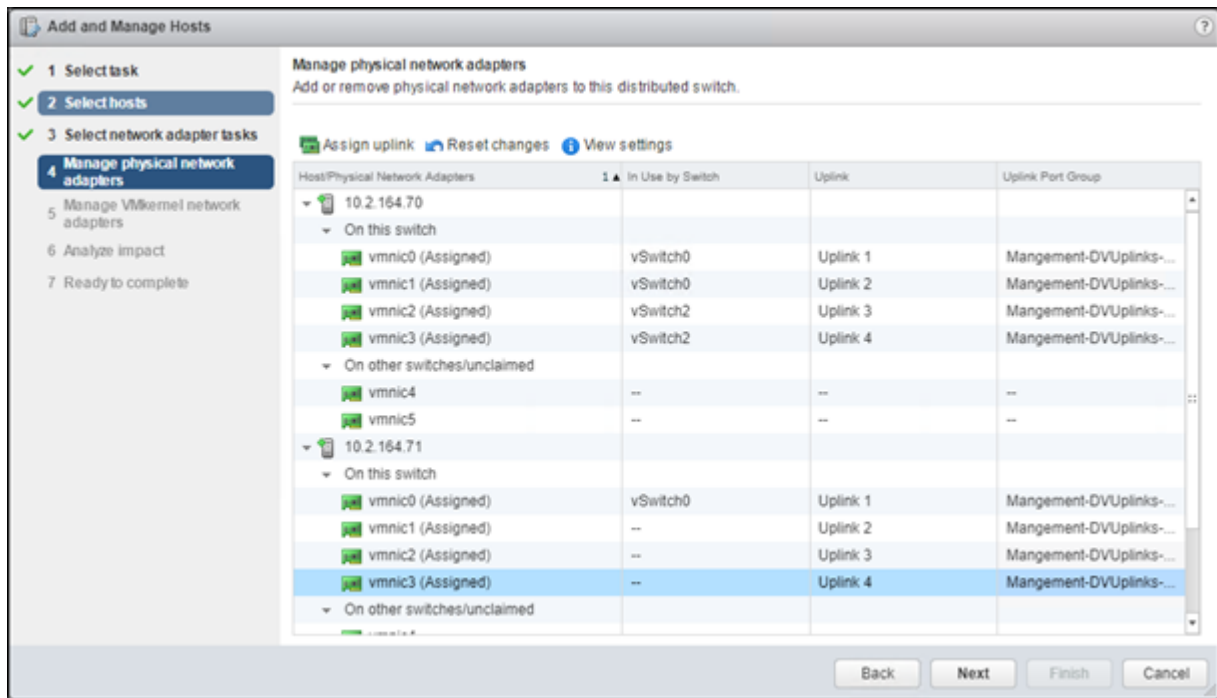


8. Leave Uplink 1 selected and click OK.

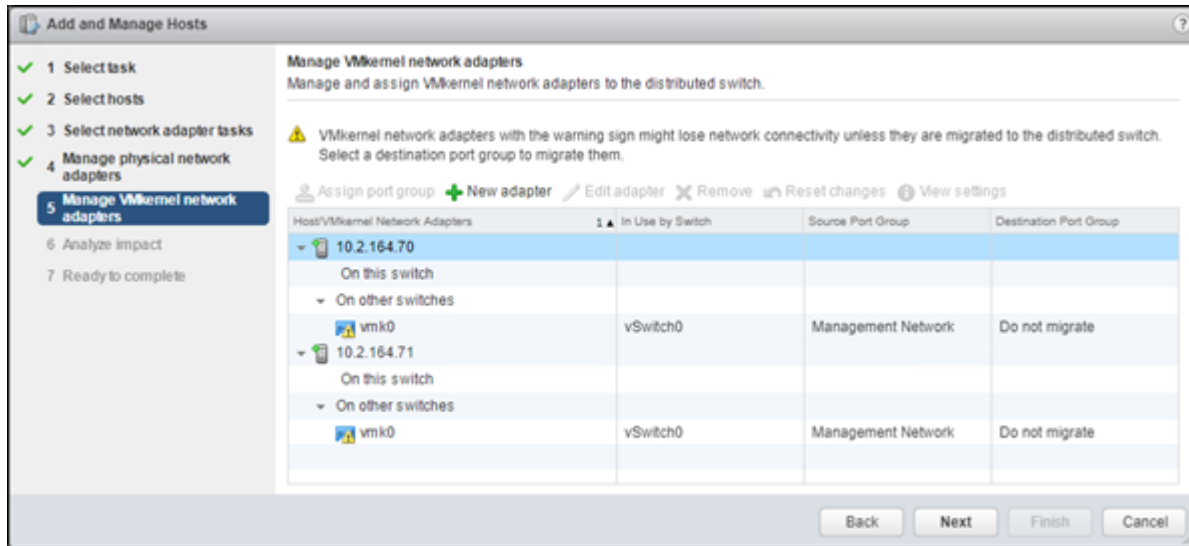


9. Repeat this step for vmnic1-3, assigning them to uplinks 2-4 in corresponding sequence.

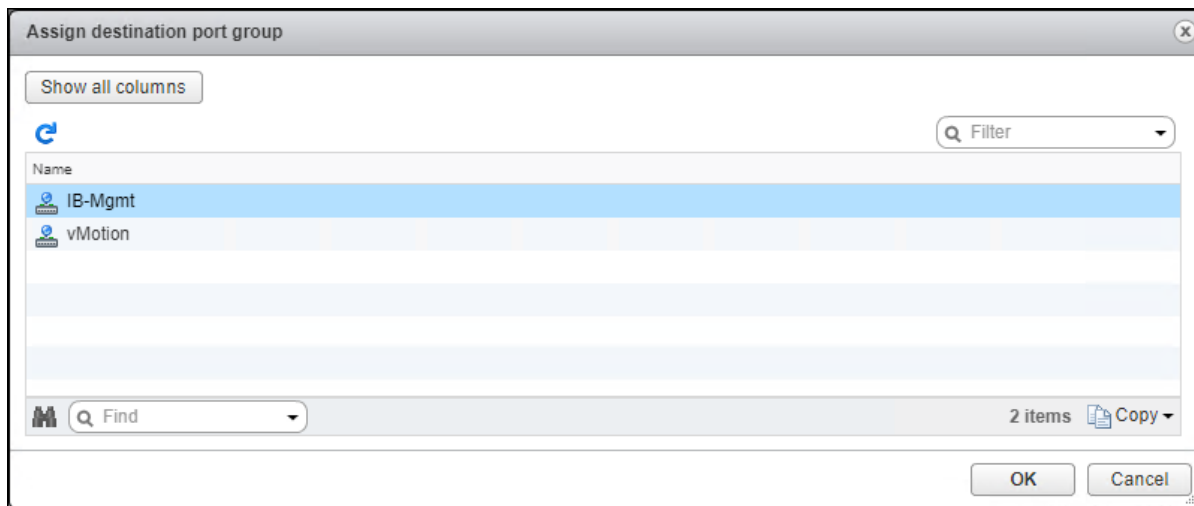
10. Repeat these assignments for all additional ESXi hosts being configured.



11. Click Next.

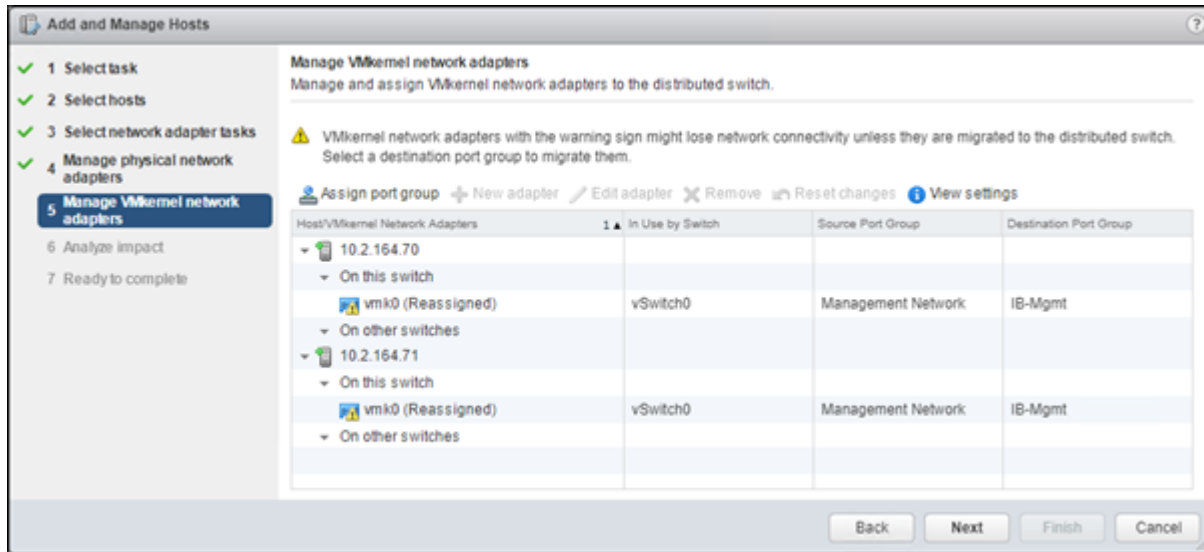


12. Select the vmk0 of the first host and click the Assign port group option.



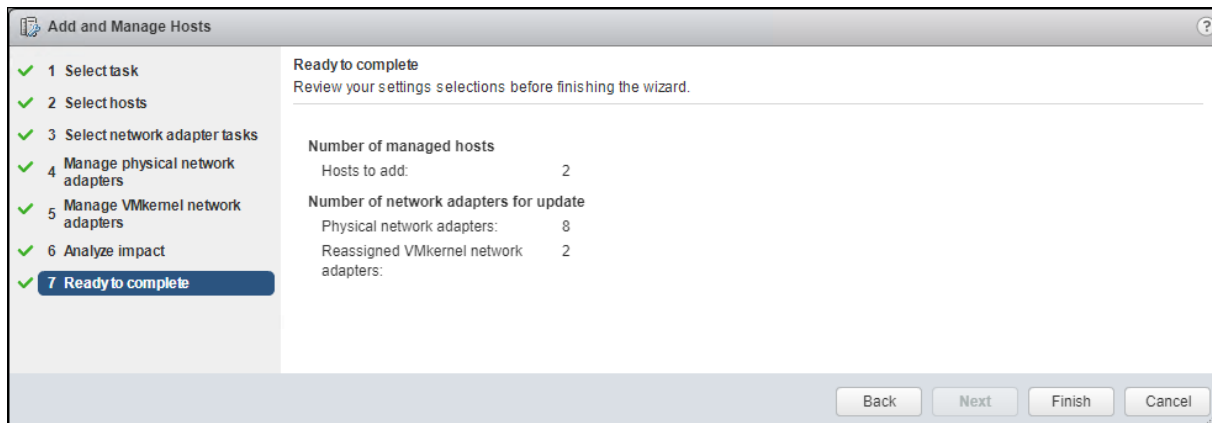
13. Select the IB-Mgmt destination port group and click OK.

14. Repeat this step for all additional hosts being configured.



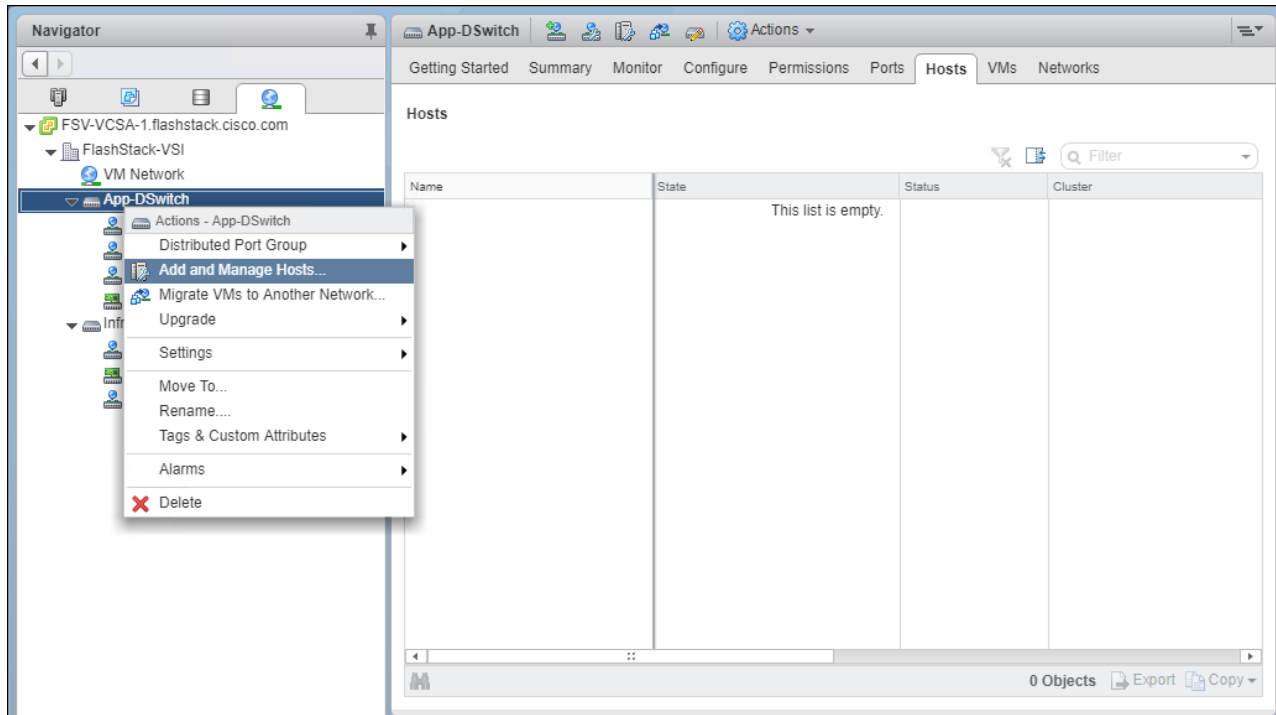
15. Click Next.

16. Click Next past Analyze impact.

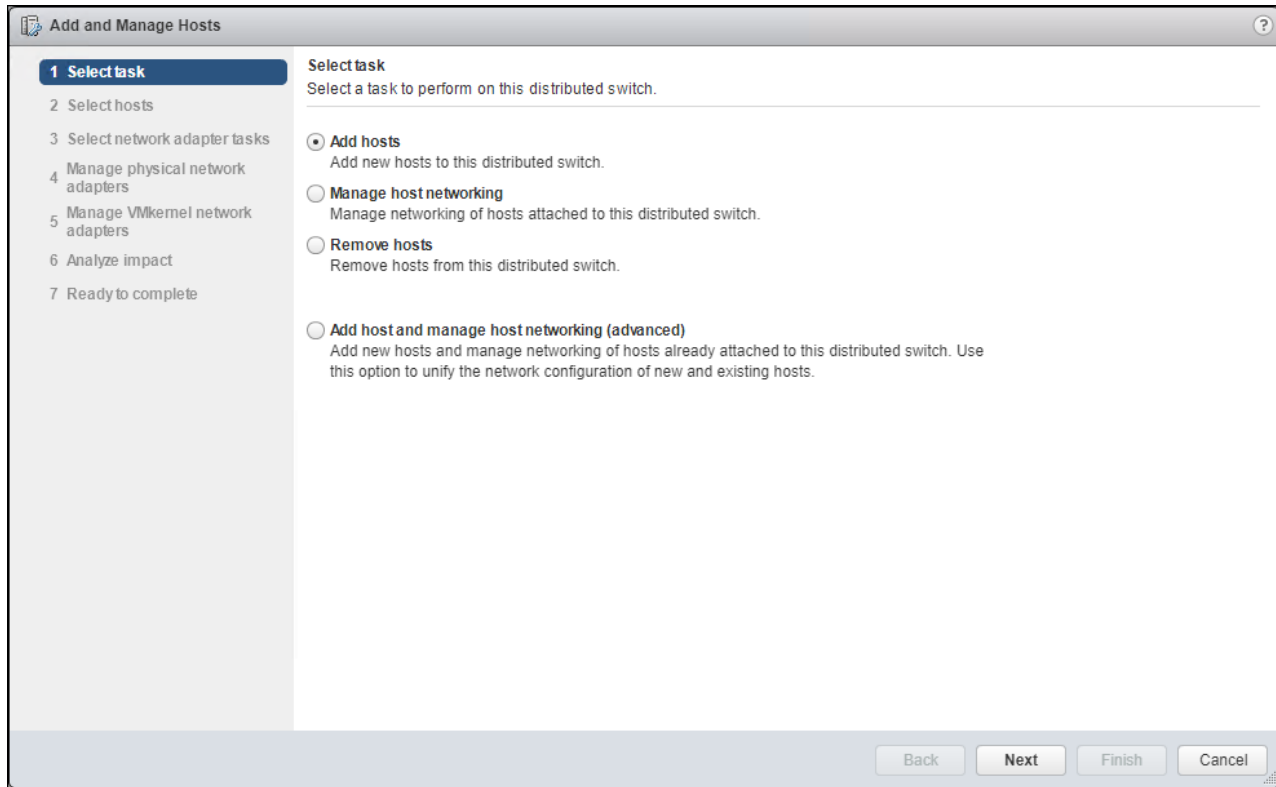


17. Review the settings and click Finish to apply.

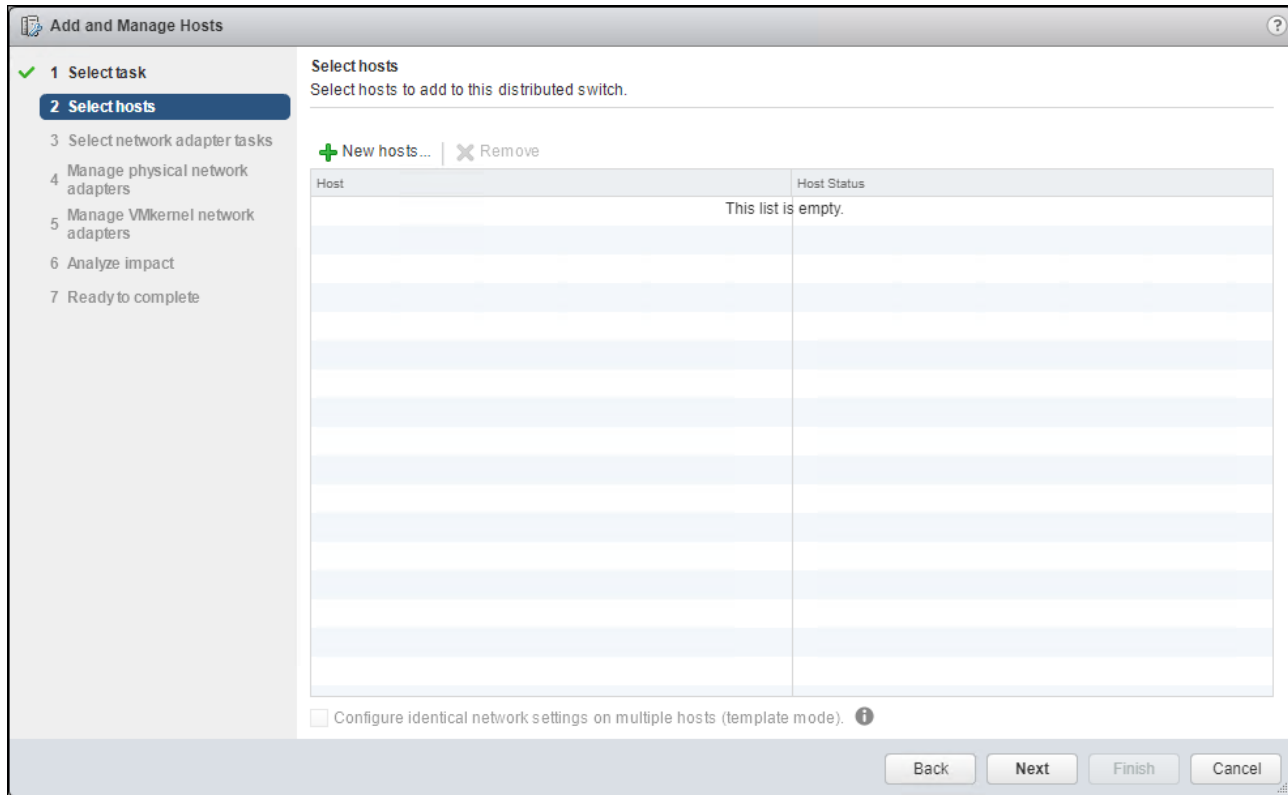
18. Within the Networking tab of the Navigator window, right-click the App-DSwitch vDS and select Add and Manage Hosts...



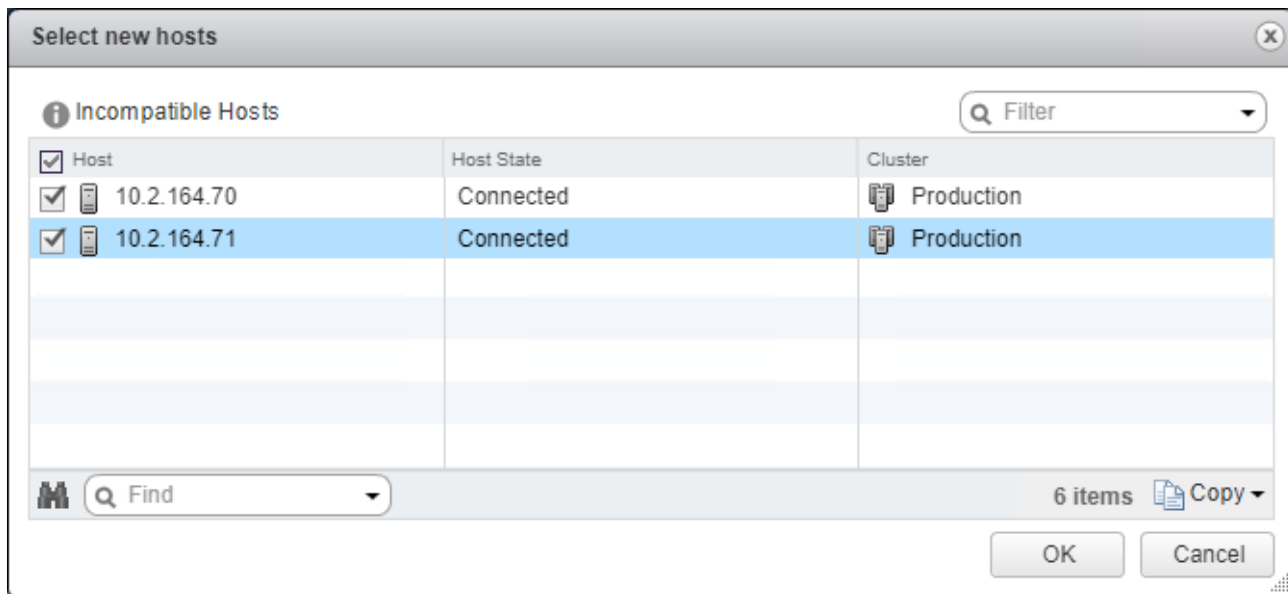
19. Leave Add hosts selected and click Next.



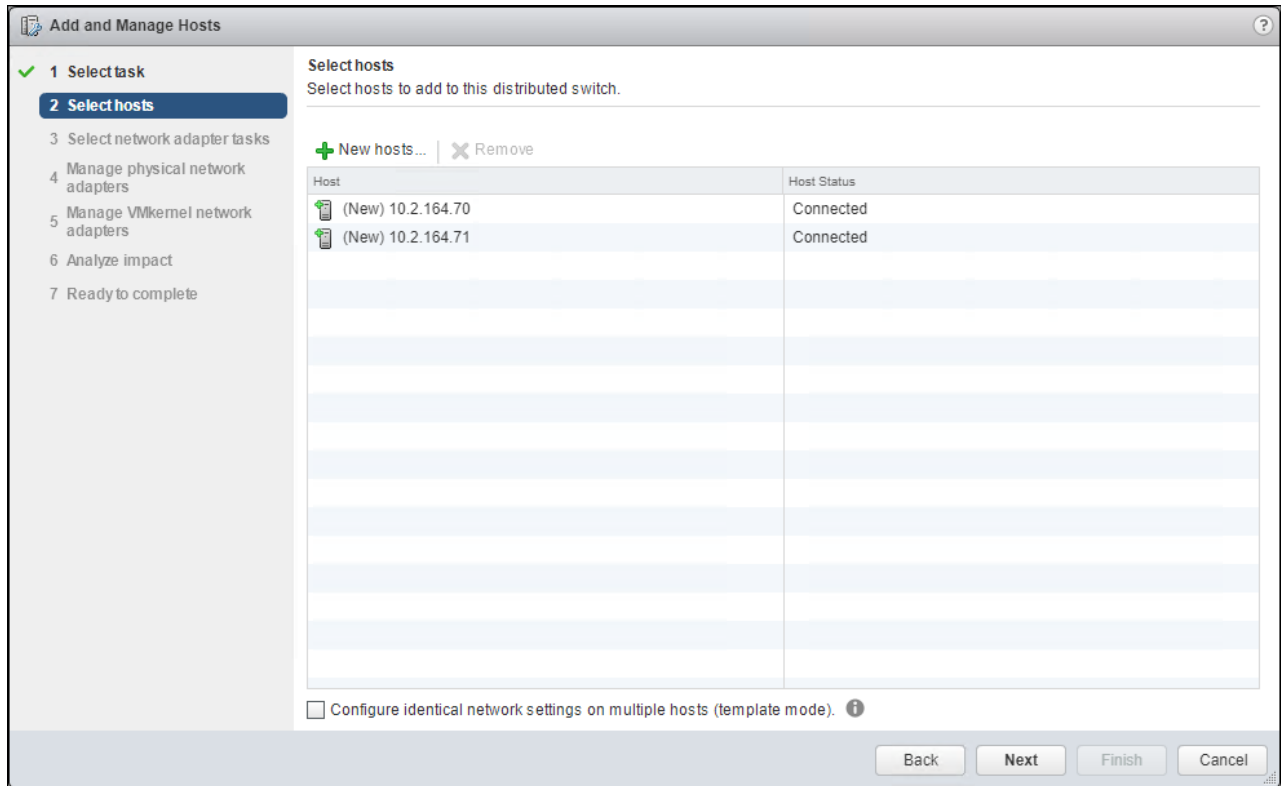
20. Click the green + icon next to New hosts...



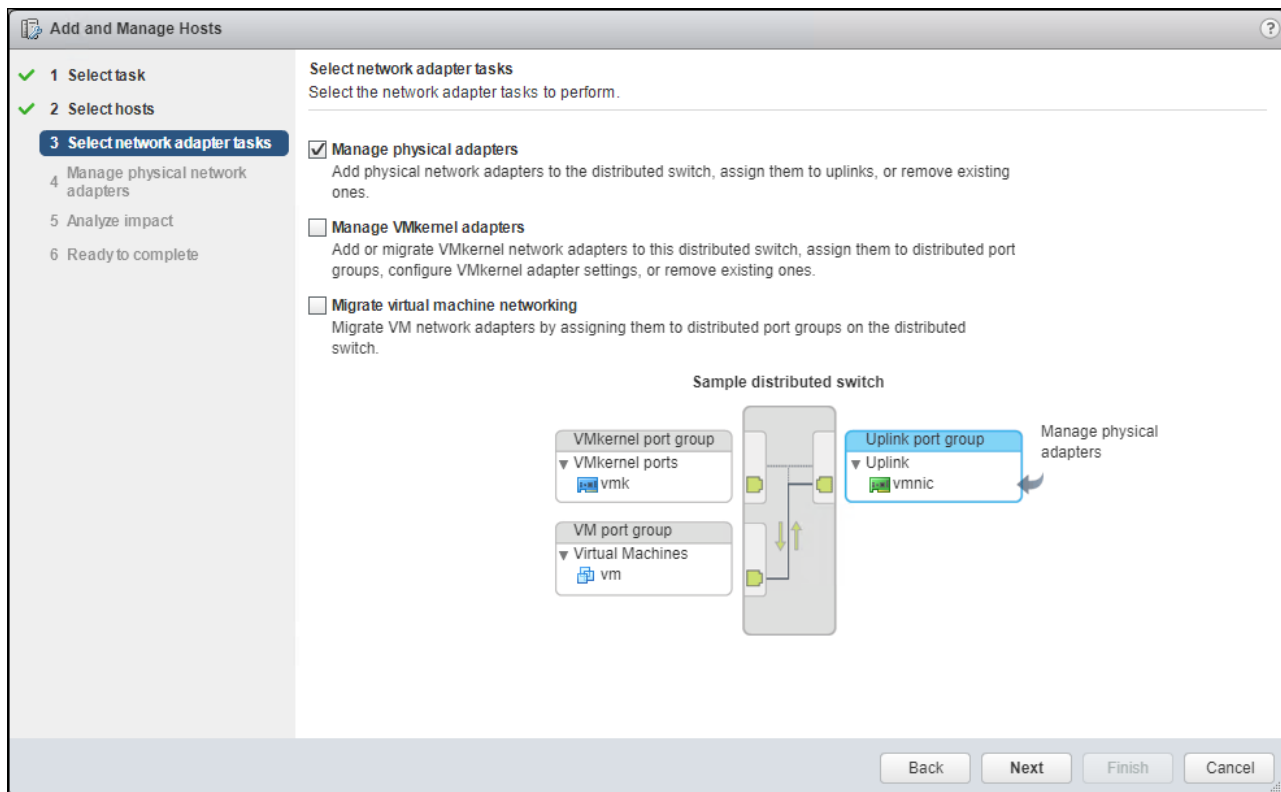
21. In the Select new hosts pop-up that appears, select the hosts to be added, and click OK to begin joining them to the vDS.



22. Click Next.

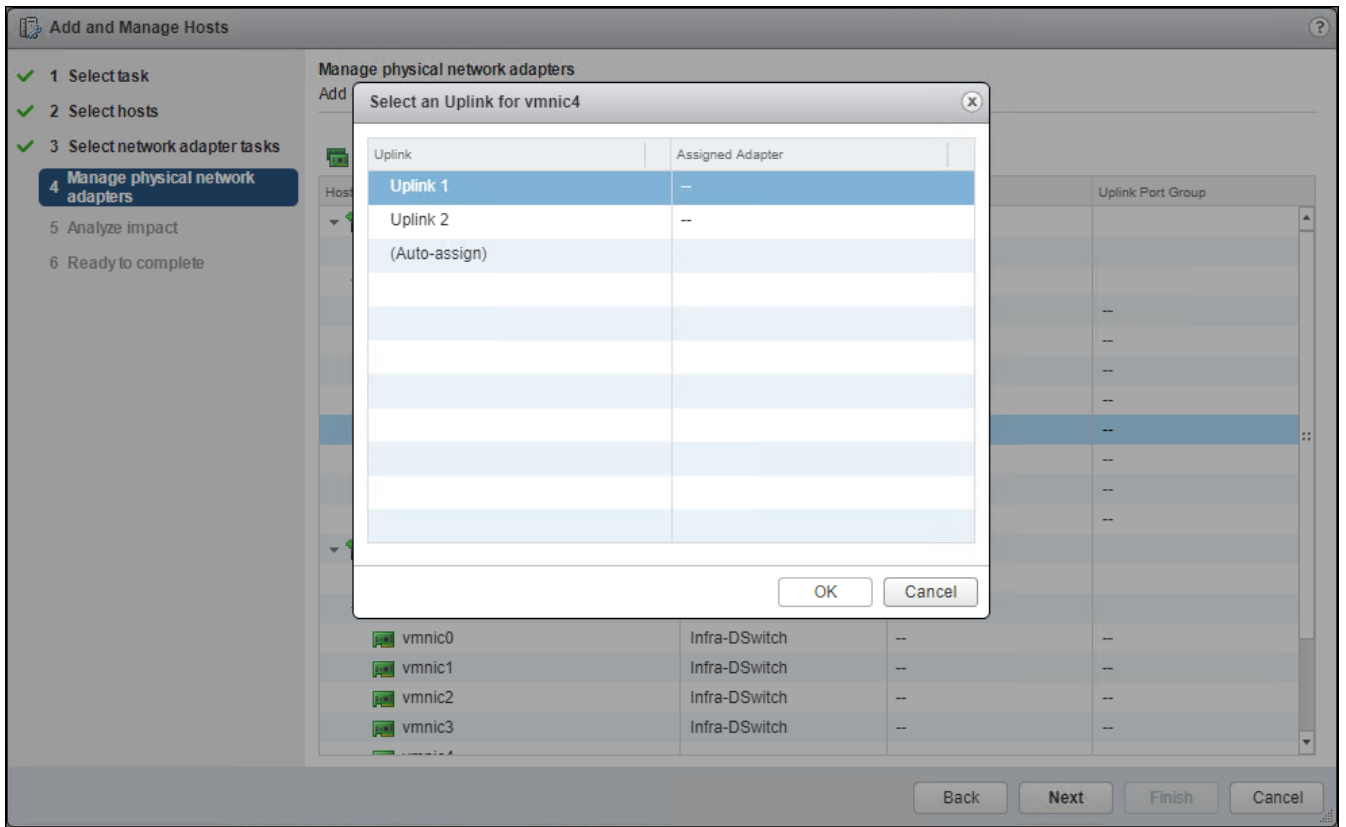


23. Leave Manage physical adapters selected and unselect Manage VMkernel adapters.

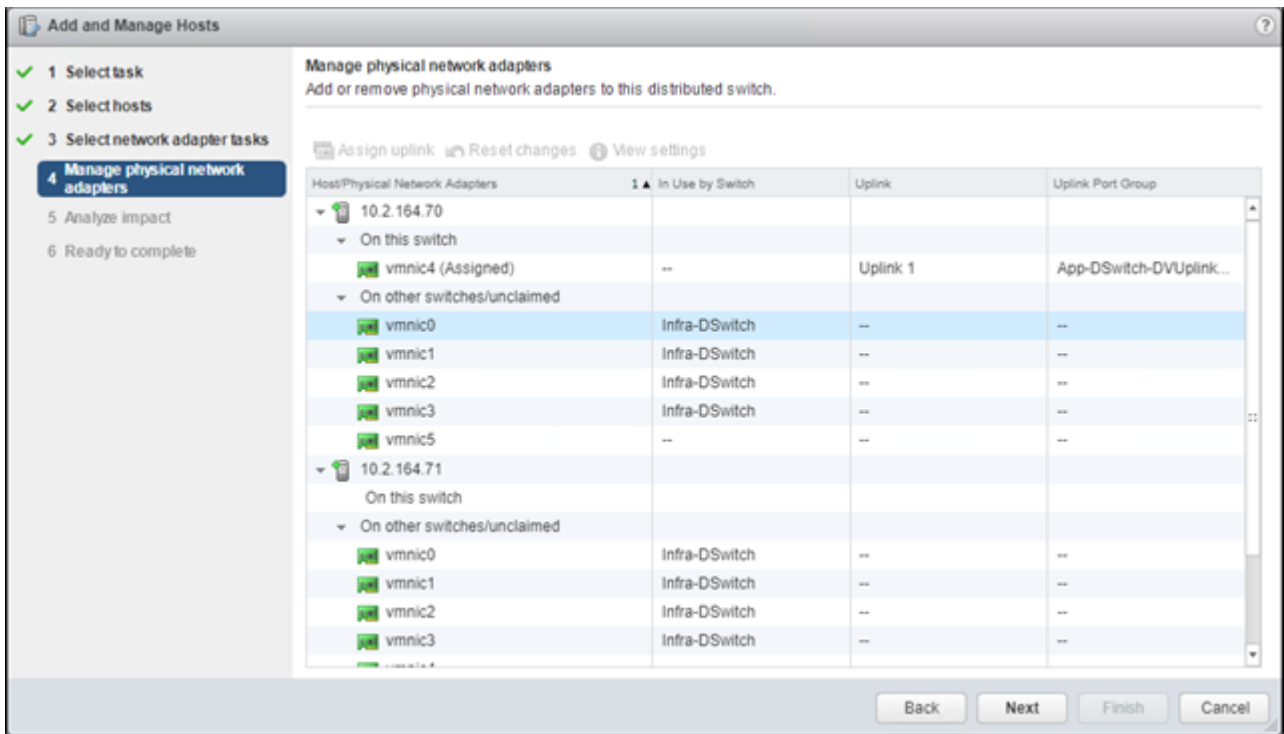


24. Click Next.

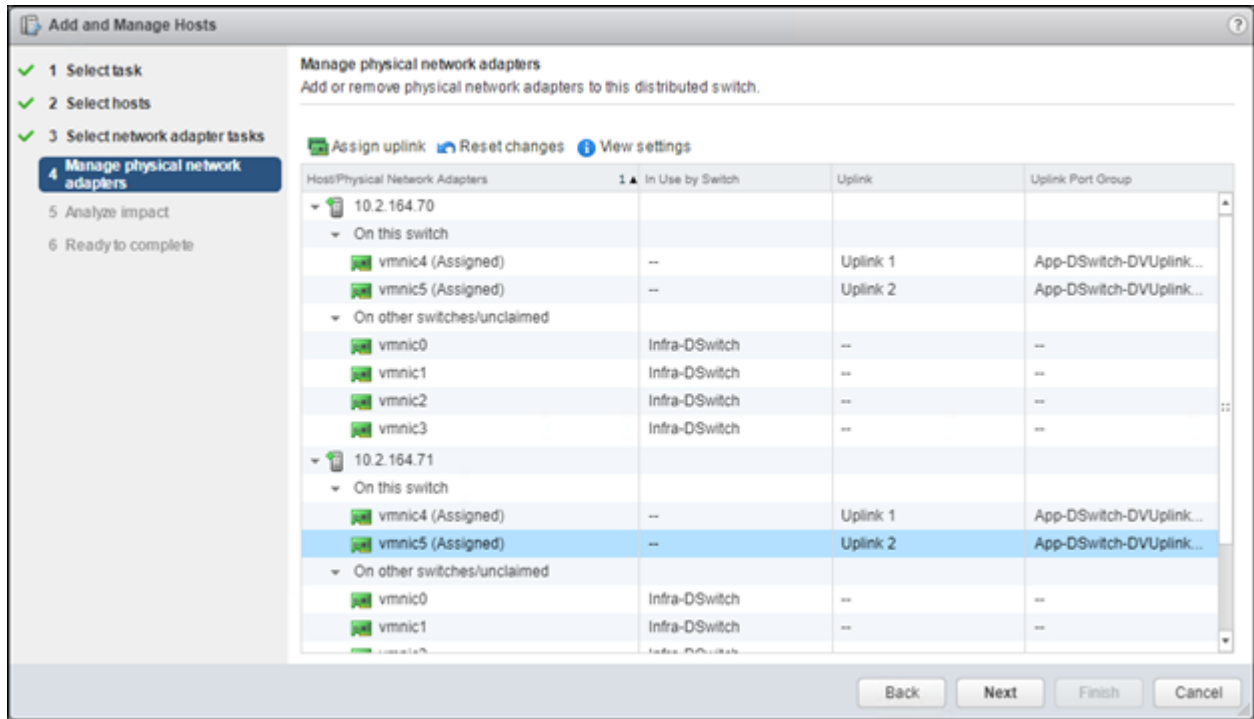
25. Select vmnic4 from the Host/Physical Network Adapters column and click the Assign uplink option.



26. Leave Uplink 1 selected and click OK.

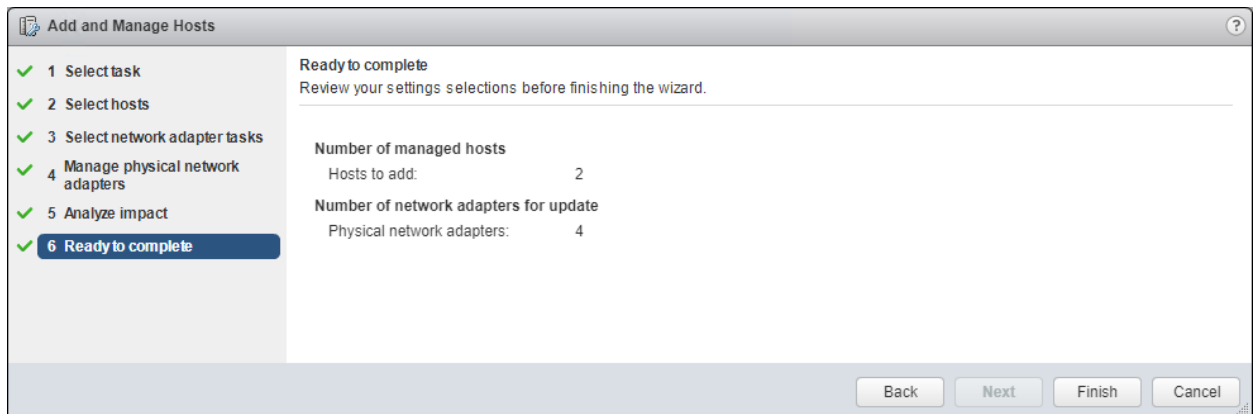


27. Repeat this step for vmnic5, assigning it to uplink 2, then perform these same steps for vmnic4 and vmnic5 for all remaining ESXi hosts to be configured.



28. Click Next.

29. Click Next past Analyze impact.

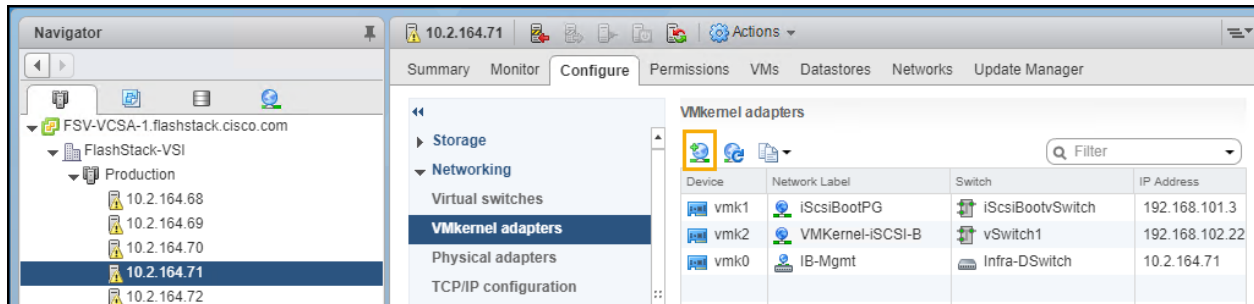


30. Review the settings and click Finish to apply.

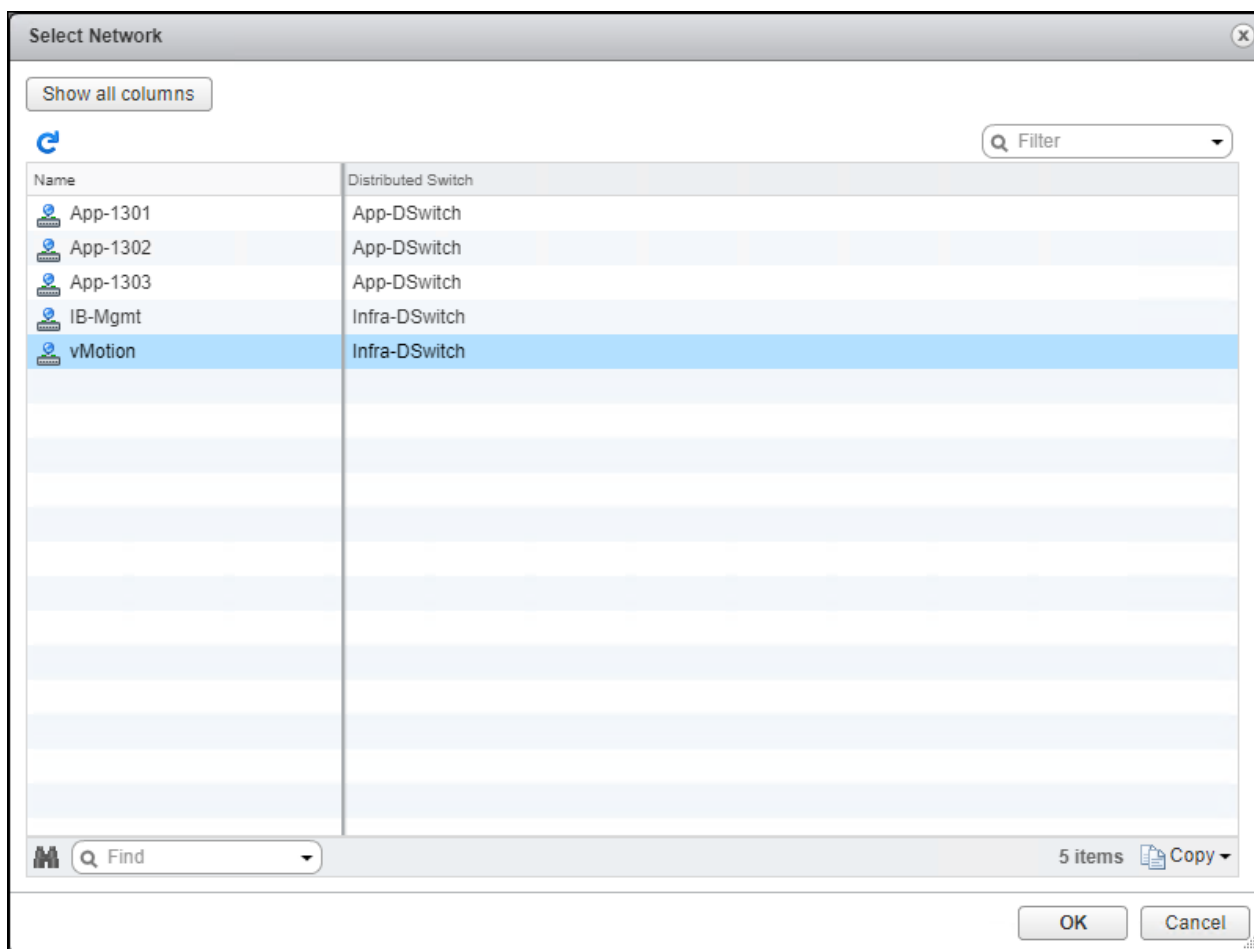
Create vMotion VMkernel adapters

A vMotion VMkernel adapter will be created for FlashStack infrastructure to keep vMotion traffic independent of management traffic. To create the vMotion VMkernel adapters, follow these steps:

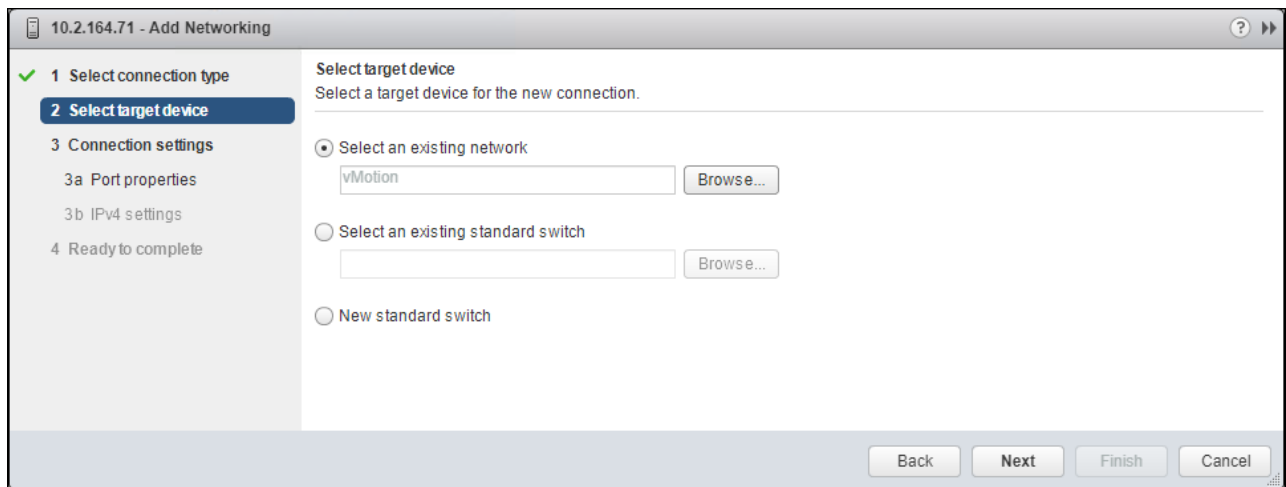
1. From the Hosts and Clusters, drill down to the first host and select the Configure tab for that host.
2. Select the VMkernel adapters option within the Networking section of Configure.



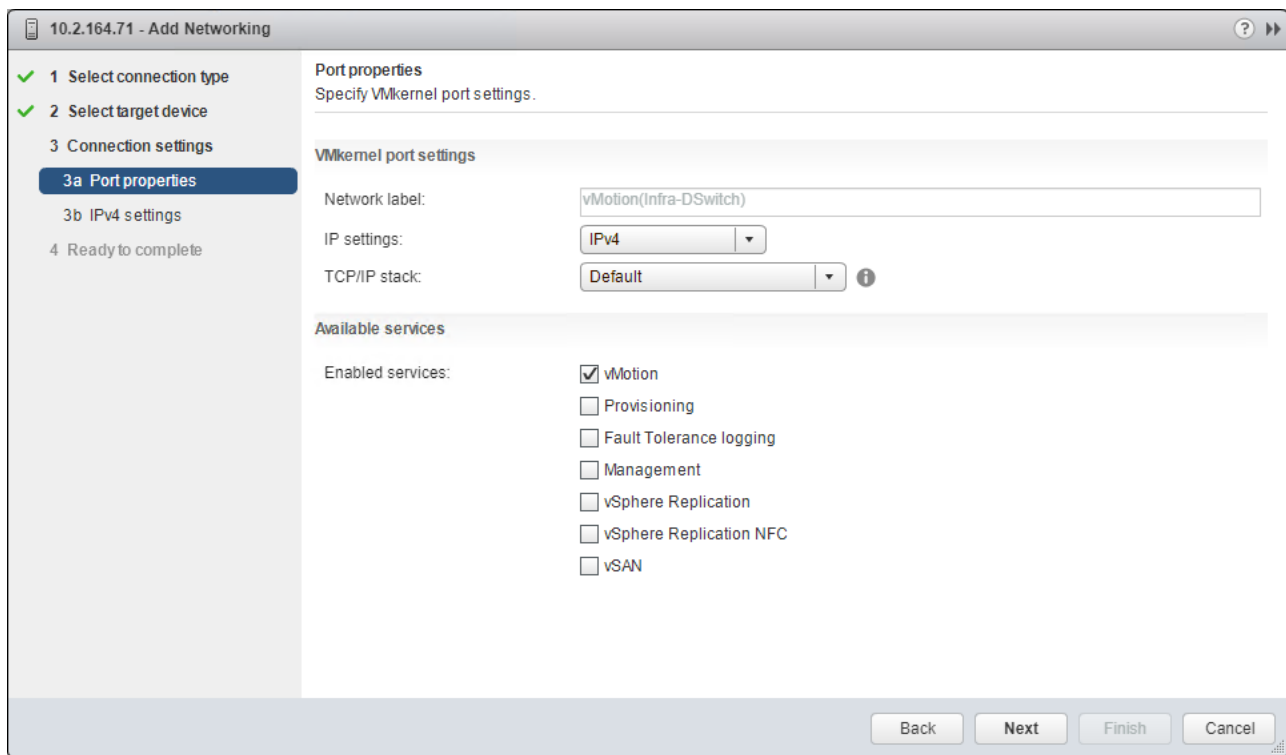
3. Click the first icon under VMkernel adapters to Add host networking.
4. Leave the connection type selected as VMkernel Network Adapter and click Next.
5. Select Browse with Select an existing network selected.



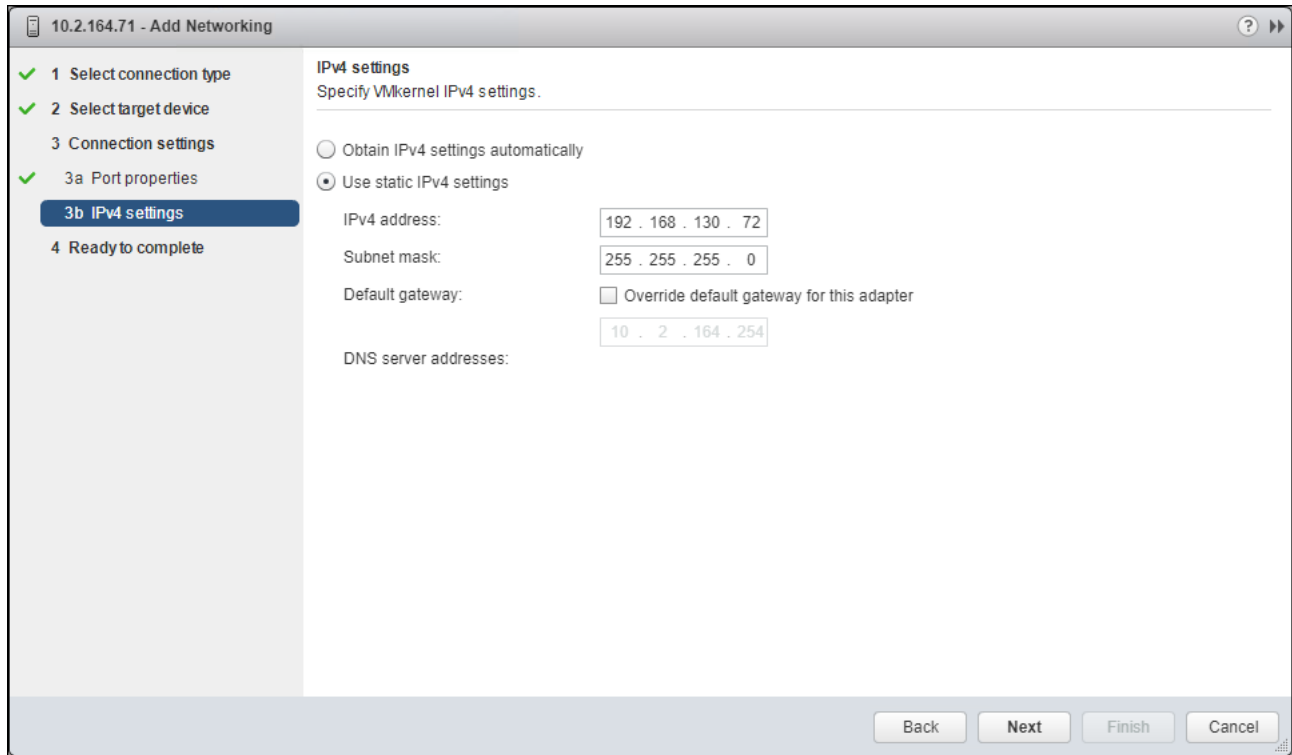
6. Pick the vMotion network from the list shown and click OK.



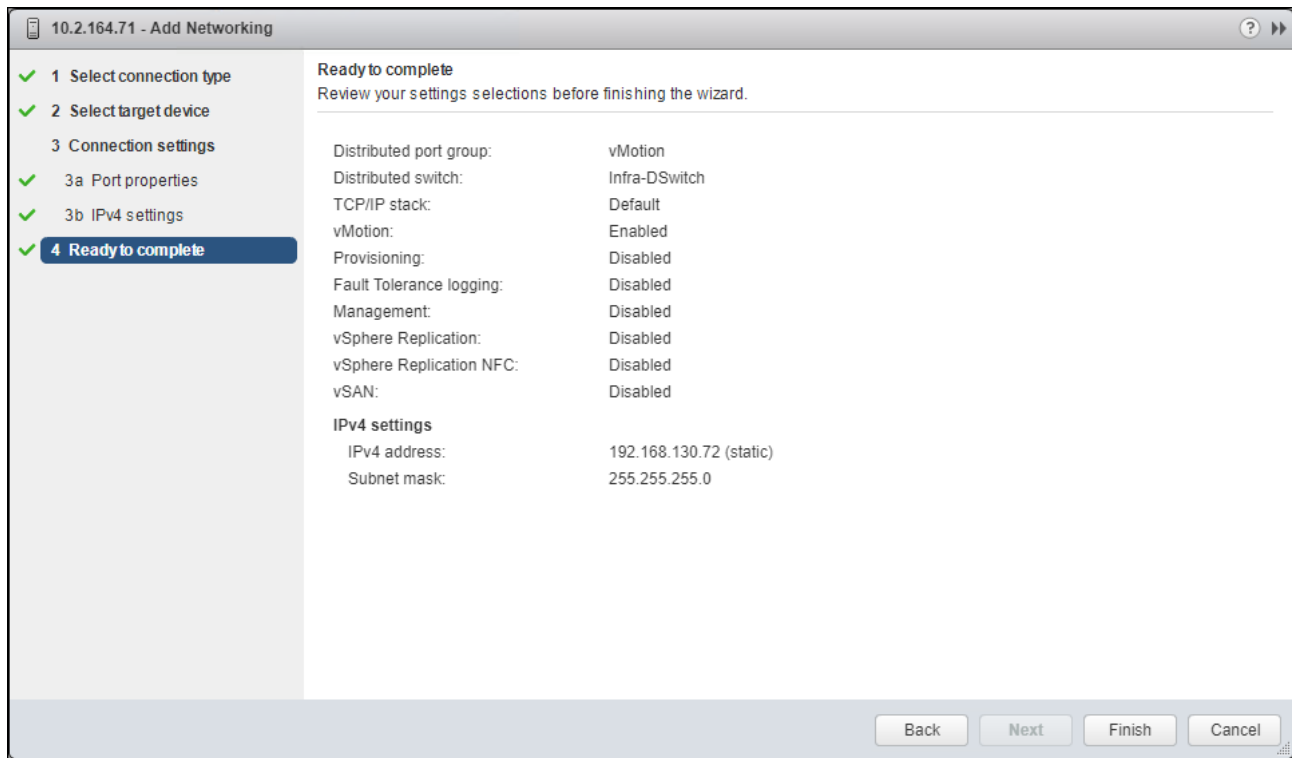
7. Click Next.



8. Select the vMotion from the Available services and click Next.

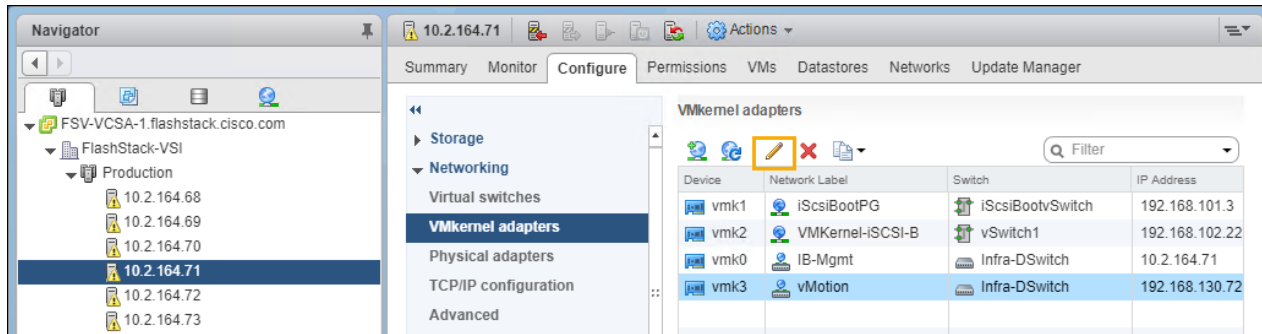


9. Provide an IP address and subnet mask within the vMotion network. Click Next.



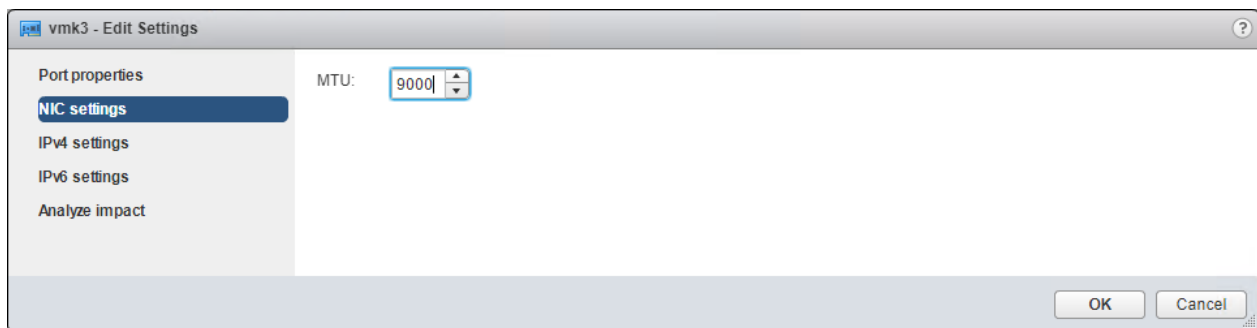
10. Review the settings and click Finish to create the VMkernel adapter.

11. Select the newly created vMotion VMkernel adapter.



12. Click the pencil icon to Edit settings for the VMkernel adapter.

13. Select the NIC Settings option and change the MTU from 1500 to 9000.



14. Click OK to save the changes.

15. Repeat steps 1-14 to create and adjust vMotion VMkernel adapters for each additional ESXi host.

Appendix

Sample Switch Configuration

```
switchname AA12-9336C-A
vdc AA12-9336C-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

cfs eth distribute
feature interface-vlan
feature lacp
feature vpc
feature lldp

ssh key rsa 2048
ip domain-lookup
system default switchport
copp profile strict
rmon event 1 description FATAL(1) owner PMON@FATAL
rmon event 2 description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 description ERROR(3) owner PMON@ERROR
rmon event 4 description WARNING(4) owner PMON@WARNING
rmon event 5 description INFORMATION(5) owner PMON@INFO
ntp server 172.26.163.254 use-vrf default

vlan 1,15,215,1130,1301-1303
```

```
vlan 15
  name pure-oob
vlan 215
  name Management
vlan 1130
  name vMotion
vlan 1301
  name VM-Apps-1
vlan 1302
  name VM-Apps-2
vlan 1303
  name VM-Apps-3

vrf context management
  ip route 0.0.0.0/0 10.2.164.254
vpc domain 10
  peer-keepalive destination 10.2.164.91

interface port-channel136
  switchport mode trunk
  switchport trunk allowed vlan 15,215,1130,1301-1303
  mtu 9216
  vpc 136

interface port-channel133
  switchport mode trunk
  spanning-tree port type network
  vpc peer-link

interface port-channel129
```

```
switchport mode trunk
switchport trunk allowed vlan 215, 1130,1301-1303
spanning-tree port type edge trunk
mtu 9216
vpc 129
```

```
interface port-channel130
switchport mode trunk
switchport trunk allowed vlan 215,1130,1301-1303
spanning-tree port type edge trunk
mtu 9216
vpc 130
```

```
interface Ethernet1/1
```

```
interface Ethernet1/2
```

```
interface Ethernet1/3
```

```
interface Ethernet1/4
```

```
interface Ethernet1/5
```

```
interface Ethernet1/6
```

```
interface Ethernet1/7
```

```
interface Ethernet1/8
```

```
interface Ethernet1/9
```

```
interface Ethernet1/10
```

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

```
interface Ethernet1/27
```

```
interface Ethernet1/28
```

```
interface Ethernet1/29
```

```
description FSV-UCS-FI-A
```

```
switchport mode trunk
```

```
switchport trunk allowed vlan 215,1130,1301-1303
```

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

```
mtu 9216
```

```
channel-group 129 mode active
```

```
interface Ethernet1/30
```

```
description FSV-UCS-FI-B
```

```
switchport mode trunk
```

```
switchport trunk allowed vlan 215,1130,1301-1303
```

```
mtu 9216
```

```
channel-group 130 mode active
```

```
interface Ethernet1/31
```

```
interface Ethernet1/32
```

```
interface Ethernet1/33
```

```
switchport mode trunk
```

```
channel-group 133 mode active
```

```
interface Ethernet1/34
```

```
switchport mode trunk
```

```
channel-group 133 mode active
```

```
interface Ethernet1/35
```

```
interface Ethernet1/36
```

```
    switchport mode trunk
```

```
    switchport trunk allowed vlan 15,115,215,1130,1301-1303
```

```
    mtu 9216
```

```
    channel-group 136 mode active
```

```
interface mgmt0
```

```
    vrf member management
```

```
    ip address 10.2.164.90/24
```

```
line console
```

```
line vty
```

```
no system default switchport shutdown
```

About the Authors

Allen Clark, Technical Marketing Engineer, Cisco Systems, Inc.

Allen Clark has over 15 years of experience working with enterprise storage and data center technologies. As a member of various organizations within Cisco, Allen has worked with hundreds of customers on implementation and support of compute and storage products. Allen holds a bachelor's degree in Computer Science from North Carolina State University and is a dual Cisco Certified Internetwork Expert (CCIE 39519, Storage Networking and Data Center)

Acknowledgements

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

- Ramesh Isaac, Technical Marketing Engineer, Cisco Systems, Inc.
- Haseeb Niazi, Technical Marketing Engineer, Cisco Systems, Inc.
- Craig Waters, Solutions Architecture / Product Management, Pure Storage Inc.
- Alex Carver, Solutions Architecture, Pure Storage Inc.