



# FlashStack Virtual Server Infrastructure with FibreChannel Storage for VMware vSphere 7.0

Deployment Guide for FlashStack with Cisco UCS 6400 Fabric Interconnects, Cisco UCS M5 Servers, and Pure Storage FlashArray//X R3 Series

Published: January 2021



---

## 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 NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Inter-network 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, Giga-Drive, 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. LD1.

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)

© 2021 Cisco Systems, Inc. All rights reserved.

---

# Contents

Executive Summary .....	4
Solution Overview .....	5
Deployment Hardware and Software .....	8
Network Switch Configuration .....	19
Pure Storage Configuration .....	25
MDS 9132T Configuration .....	35
Cisco UCS Configuration .....	38
MDS Fabric Zoning .....	120
FlashArray Storage Deployment .....	125
vSphere Deployment .....	133
Appendix.....	164
About the Author.....	174
Feedback.....	175

---

## Executive Summary

Cisco Validate Designs 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 7.0, which describes a validated converged infrastructure jointly developed by Cisco and Pure Storage. This solution covers the deployment of a predesigned, best-practice data center architecture with VMware vSphere built on the Cisco Unified Computing System (Cisco 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.

This document describes 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 7.0 hypervisor environment.

### Audience

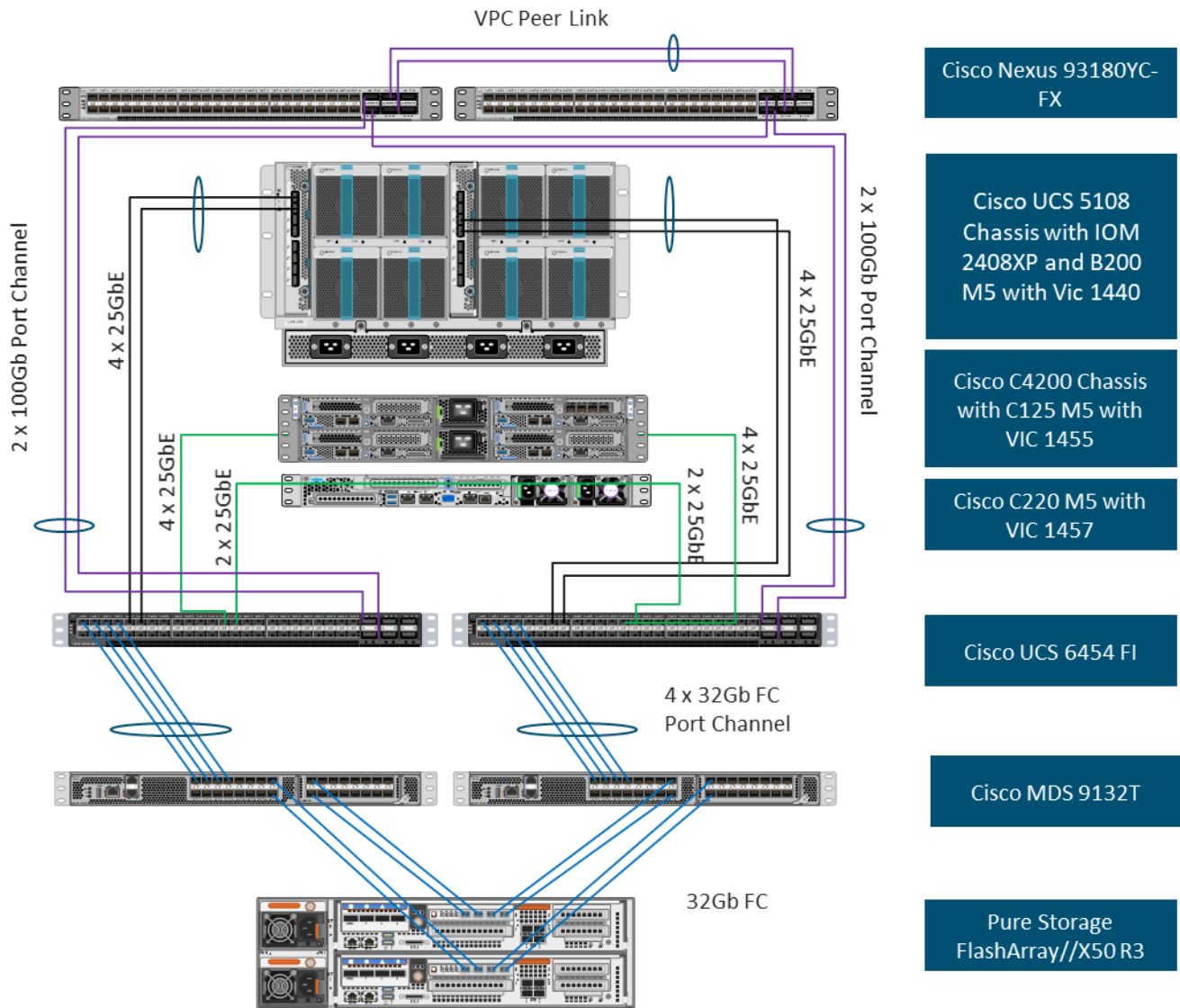
The audience for this document includes, but is not limited to; sales engineers, field consultants, professional services, IT managers, partner engineers, and customers who want to take advantage of an infrastructure built to deliver IT efficiency and enable IT innovation.

### 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//X50 R3. These components are supported by the 1/10/25/40/50/100G capable Cisco Nexus 93180YC-FX switch and 32G FC capable Cisco MDS 9132T to deliver a Virtual Server infrastructure on Cisco UCS C125 M5 Server nodes and Cisco UCS B200 M5 Blade Servers running VMware vSphere 7.0.

The design that will be implemented is discussed in the [FlashStack Virtual Server Infrastructure for VMware vSphere 7.0 Design Guide](#).

Figure 1. FlashStack with Cisco UCS 6454 and Pure Storage FlashArray //50 R3



The reference hardware configuration includes:

- Two Cisco Nexus 93180YC-FX Switches
- Two Cisco MDS 9132T Switches
- Two Cisco UCS 6454 Fabric Interconnects
- Cisco UCS 5108 Chassis with two Cisco UCS 2408 Fabric Extenders
- Four Cisco UCS B200 M5 Blade Servers
- Four Cisco UCS C125 M5 Server Nodes
- One Pure Storage FlashArray//X50 R3

---

The virtual environment this supports is within VMware vSphere 7.0 and includes virtual management and automation components from Cisco and Pure Storage built into the solution, or as optional add-ons.

This document will provide 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

## What's New in this Release?

This FlashStack Datacenter with VMware vSphere 7.0 validated design introduced new hardware and software into the portfolio, enabling 10/25/40/100GbE along with native 32Gb FC via the Cisco MDS Fibre Channel switch or the Cisco Nexus 93180YC-FX switch. This primary design has been updated to include the latest Cisco and Pure Storage hardware and software and has the following new features:

- Support for the Cisco UCS 4.1(2) unified software release, Cisco UCS C125 servers with AMD EPYC 2<sup>nd</sup> Generation Processors, Cisco UCS B200-M5 and C220-M5 servers with 2<sup>nd</sup> Generation Intel Xeon Scalable Processors, and Cisco 1400 Series Virtual Interface Cards (VICs)
- Support for the latest Cisco UCS 6454 and 64108 (supported but not validated) Fabric Interconnects
- Support for the latest Cisco UCS 2408 Fabric Extender
- Support for 32Gb FC SAN Switching in the Cisco Nexus 93180YC-FX switch (appendix)
- Support for Cisco Intersight Software as a Service (SaaS) Management
- Support for the Pure Storage FlashArray//X R3 array
- Support for the latest release of Pure Storage Purity 6
- Validation of VMware vSphere 7.0
- Unified Extensible Firmware Interface (UEFI) Secure Boot of VMware ESXi 7.0
- 25 or 100 Gigabit per second Ethernet Connectivity



## 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 the current supported version information, 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](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](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:
  - Cisco Nex-  
us: [https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/recommended\\_release/b\\_Minimum\\_and\\_Recommended\\_Cisco\\_NX-OS\\_Releases\\_for\\_Cisco\\_Nexus\\_9000\\_Series\\_Switches.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/recommended_release/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](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/b_MDS_NX-OS_Recommended_Releases.html)

If versions differ from the validated versions listed 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	4.1(2a)	Includes Cisco UCS IOM 2408 and Cisco VIC 1400 Series
Network	Cisco Nexus 9000 NX-OS	9.3(5)	
Storage	Pure Storage FlashArray//X50 R3	6.0.2	
	Cisco MDS 9132T	8.4(1a)	
Software	Cisco UCS Manager	4.1(2a)	
	VMware vSphere ESXi Cisco Custom ISO	7.0	



Layer	Device	Image	Comments
	enic Driver for ESXi	1.0.33.0	
	nfnic Driver for ESXi	4.0.0.56	
	VMware vCenter	7.0	

## 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:

```
BB08-93180YC-FX-A (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 external dependencies 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	

VLAN Name	VLAN Purpose	ID Used in Validating this Document	Customer Deployed Value
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	
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)	

Variable Name	Variable Description	Customer Deployed Value
<<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)	
<<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)	

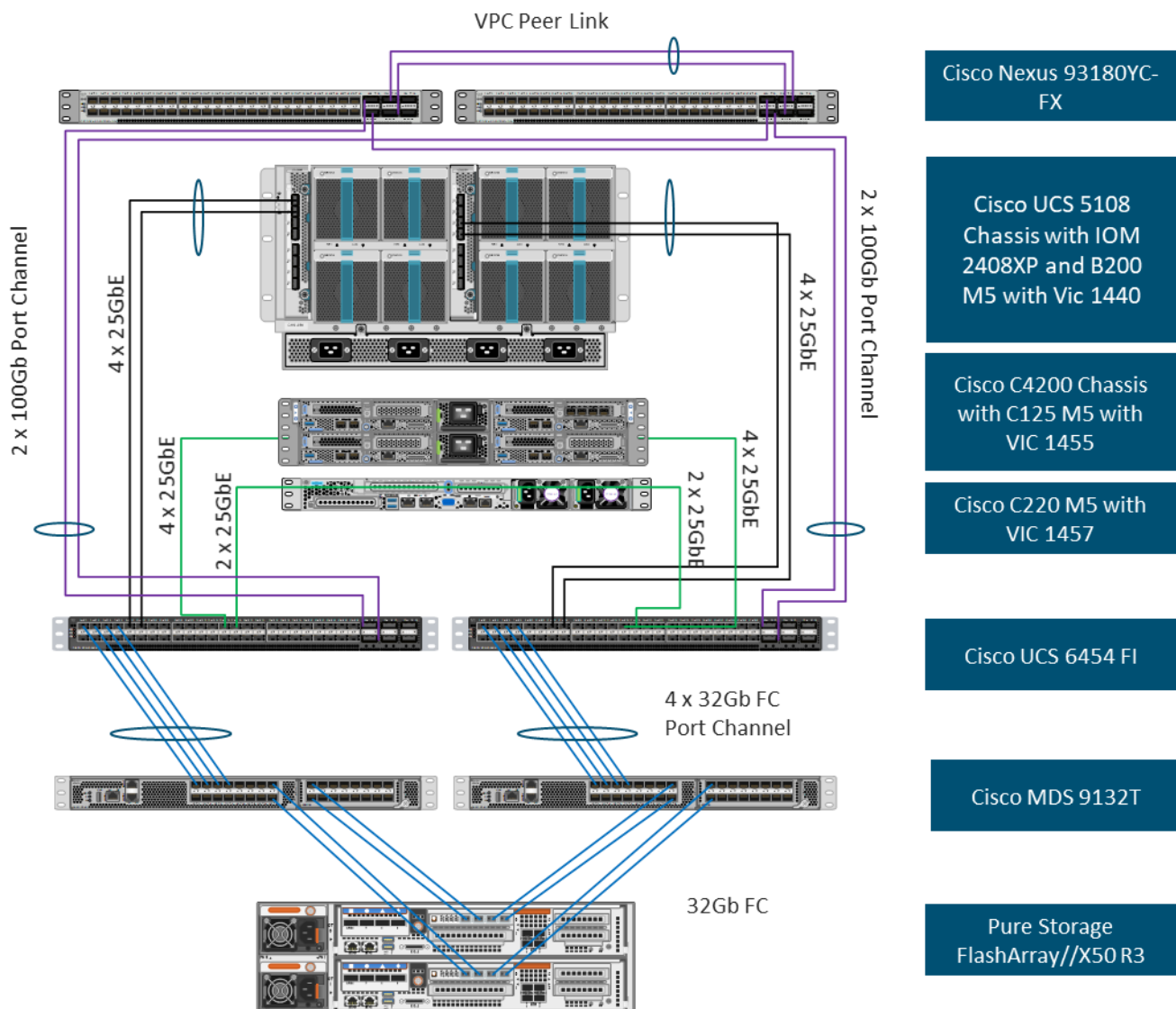
Variable Name	Variable Description	Customer Deployed Value
<<var_mds_A_mgmt_ip>>	Cisco MDS Management IP address (Example: 10.2.164.92)	
<<var_mds_A_hostname>>	Cisco MDS hostname (Example: mds-9132T-A)	
<<var_mds_B_mgmt_ip>>	Cisco MDS Management IP address (Example: 10.2.164.93)	
<<var_mds_B_hostname>>	Cisco MDS hostname (Example: mds-9132T-b)	
<<var_vsan_a_id>>	VSAN used for the A Fabric between the 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 make connectivity clear 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 Cisco Nexus 93180YC-FX 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. FlashStack Cabling in Validated Topology**



**Figure 2** shows fewer connections to the servers in the diagram than are used in the connection table for readability purposes. The connections between the fabric interconnects and the servers are as follows:  
4 connections from the IOM to the respective fabric interconnect

4 connections from the Cisco UCS C420 (1 per server) to each fabric interconnect  
 2 connections from the Cisco UCS C220 to each fabric interconnect

**Table 5.** Cisco Nexus 93180YC-FX-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote port
Cisco Nexus 93180YC-FX-A	Eth 1/49	100Gbe	Cisco UCS 6454-A	Eth 1/49
	Eth 1/50	100Gbe	Cisco UCS 6454-B	Eth 1/49
	Eth 1/51	100Gbe	Cisco Nexus 93180YC-FX-B	Eth 1/51
	Eth 1/52	100Gbe	Cisco Nexus 93180YC-FX-B	Eth 1/52
	Eth 1/53 or Eth 1/47	40Gbe or 100Gbe or 10Gbe or 25 Gbe	Upstream Network Switch	Any
	Eth 1/54 or Eth 1/48	40Gbe or 100Gbe or 10Gbe or 25 Gbe	Upstream Network Switch	Any
	Mgmt0	Gbe	Gbe Management Switch	Any

**Table 6.** Cisco Nexus 93180YC-FX-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote port
Cisco Nexus 93180YC-FX-B	Eth 1/49	100Gbe	Cisco UCS 6454-A	Eth 1/50
	Eth 1/50	100Gbe	Cisco UCS 6454-B	Eth 1/50
	Eth 1/51	100Gbe	Cisco Nexus 93180YC-FX-A	Eth 1/51
	Eth 1/52	100Gbe	Cisco Nexus 93180YC-FX-A	Eth 1/52
	Eth 1/53 or Eth 1/47	40Gbe or 100Gbe or 10Gbe or 25 Gbe	Upstream Network Switch	Any
	Eth 1/54 or Eth 1/48	40Gbe or 100Gbe or 10Gbe or 25 Gbe	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 93180YC-FX-A	Eth 1/49	
	Eth 1/50	100Gbe	Cisco Nexus 93180YC-FX-B	Eth 1/50	
	Eth 1/9	25Gbe	Cisco UCS Chassis 1 2408 FEX A	IOM 1/1	
	Eth 1/10	25Gbe	Cisco UCS Chassis 1 2408 FEX A	IOM 1/2	
	Eth 1/11	25Gbe	Cisco UCS Chassis 1 2408 FEX A	IOM 1/3	
	Eth 1/12	25Gbe	Cisco UCS Chassis 1 2408 FEX A	IOM 1/4	
	Eth 1/17	25Gbe	Cisco UCS C4200 Chassis Server 1	DCE 1	
	Eth 1/18	25Gbe	Cisco UCS C4200 Chassis Server 1	DCE 2	
	Eth 1/19	25Gbe	Cisco UCS C4200 Chassis Server 2	DCE 1	
	Eth 1/20	25Gbe	Cisco UCS C4200 Chassis Server 2	DCE 2	
	Eth 1/21	25Gbe	Cisco UCS C4200 Chassis Server 3	DCE 1	
	Eth 1/22	25Gbe	Cisco UCS C4200 Chassis Server 3	DCE 2	
	Eth 1/23	25Gbe	Cisco UCS C4200 Chassis Server 4	DCE 1	
	Eth 1/24	25Gbe	Cisco UCS C4200 Chassis Server 4	DCE 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



Local Device	Local Port	Connection	Remote Device	Remote port
	Mgmt0	Gbe	Gbe Management Switch	Any

**Table 8. Cisco UCS-6545-B Cabling Information**

Local Device	Local Port	Connection	Remote Device	Remote port
Cisco UCS-6454-B	Eth 1/49	100Gbe	Cisco Nexus 93180YC-FX-A	Eth 1/49
	Eth 1/50	100Gbe	Cisco Nexus 93180YC-FX-B	Eth 1/50
	Eth 1/9	25Gbe	Cisco UCS Chassis 1 2408 FEX B	IOM 1/1
	Eth 1/10	25Gbe	Cisco UCS Chassis 1 2408 FEX B	IOM 1/2
	Eth 1/11	25Gbe	Cisco UCS Chassis 1 2408 FEX B	IOM 1/3
	Eth 1/12	25Gbe	Cisco UCS Chassis 1 2408 FEX B	IOM 1/4
	Eth 1/17	25Gbe	Cisco UCS C4200 Chassis Server 1	DCE 3
	Eth 1/18	25Gbe	Cisco UCS C4200 Chassis Server 1	DCE 4
	Eth 1/19	25Gbe	Cisco UCS C4200 Chassis Server 2	DCE 3
	Eth 1/20	25Gbe	Cisco UCS C4200 Chassis Server 2	DCE 4
	Eth 1/21	25Gbe	Cisco UCS C4200 Chassis Server 3	DCE 3
	Eth 1/22	25Gbe	Cisco UCS C4200 Chassis Server 3	DCE 4
	Eth 1/23	25Gbe	Cisco UCS C4200 Chassis Server 4	DCE 3
	Eth 1/24	25Gbe	Cisco UCS C4200 Chassis Server 4	DCE 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//X50 R3 Controller 1	CT0.FC0
	FC1/16	32Gb FC	FlashArray//X50 R3 Controller 1	CT0.FC2
	FC1/17	32Gb FC	FlashArray//X50 R3 Controller 2	CT1.FC0
	FC1/18	32Gb FC	FlashArray//X50 R3 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//X50 R3 Controller 1	CT0.FC1

Local Device	Local Port	Connection	Remote Device	Remote port
	FC1/16	32Gb FC	FlashArray//X50 R3 Controller 1	CT0.FC3
	FC1/17	32Gb FC	FlashArray//X50 R3 Controller 2	CT1.FC1
	FC1/18	32Gb FC	FlashArray//X50 R3 Controller 2	CT1.FC3
	Mgmt0	Gbe	Gbe Management Switch	Any

**Table 11.** Pure Storage FlashArray//X50 R3 Controller 1 Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote port
FlashArray//X50 R3 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 1/15
	CT0.FC3	32Gb FC	Cisco MDS 9132T-B	FC 1/16
	Eth0	Gbe	Gbe Management Switch	Any

**Table 12.** Pure Storage FlashArray//X50 R3 Controller 2 Cabling Information

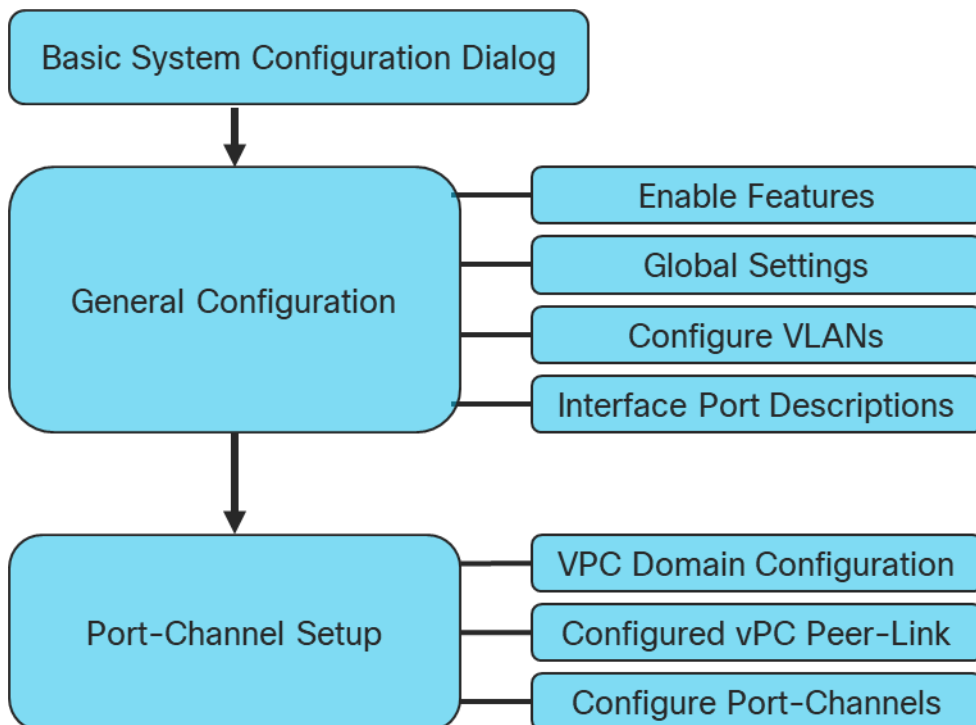
Local Device	Local Port	Connection	Remote Device	Remote port
FlashArray//X50 R3 Controller 2	CT1.FC0	32Gb FC	Cisco MDS 9132T-A	FC 1/17
	CT1.FC1	32Gb FC	Cisco MDS 9132T-B	FC 1/18
	CT1.FC2	32Gb FC	Cisco MDS 9132T-A	FC 1/17
	CT1.FC3	32Gb FC	Cisco MDS 9132T-B	FC 1/18
	Eth0	Gbe	Gbe Management Switch	Any

## 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 you're using Cisco Nexus 93180YC-FX switches running NX-OS 9.3(5). Configuration on a differing model of the Cisco Nexus 9000 series switch should be comparable but may differ slightly with the model and changes in NX-OS release. The Cisco Nexus 93180YC-FX switch and NX-OS 9.3(5) release were used to validate this FlashStack solution, so the steps 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 93180YC-FX 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 93180YC-FX-A

To set up the initial configuration for the Cisco Nexus A switch on <nexus-A-hostname>, follow these steps:



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

```
Abort Power On Auto Provisioning [yes - continue with normal setup, skip - bypass password and basic
configuration, no - continue with Power On Auto Provisioning] (yes/skip/no) [no]: yes
Disabling POAP.....Disabling POAP
poap: Rolling back, please wait... (This may take 5-15 minutes)

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

Do you want to enforce secure password standard (yes/no) [y]: Enter
Enter the password for "admin": <password>
Confirm the password for "admin": <password>
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]: Enter
Configure read-only SNMP community string (yes/no) [n]: Enter
Configure read-write SNMP community string (yes/no) [n]: Enter
Enter the switch name: <nexus-A-hostname>
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
Mgmt0 IPv4 address: <nexus-A-mgmt0-ip>
Mgmt0 IPv4 netmask: <nexus-A-mgmt0-netmask>
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway: <nexus-A-mgmt0-gw>
Configure advanced IP options? (yes/no) [n]: Enter
Enable the telnet service? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter
Type of ssh key you would like to generate (dsa/rsa) [rsa]: Enter
Number of rsa key bits <1024-2048> [1024]: Enter
Configure the ntp server? (yes/no) [n]: Enter
Configure default interface layer (L3/L2) [L2]: Enter
Configure default switchport interface state (shut/noshut) [noshut]: shut
Enter basic FC configurations (yes/no) [n]: n
Configure CoPP system profile (strict/moderate/lenient/dense) [strict]: Enter
Would you like to edit the configuration? (yes/no) [n]: Enter
```

1. Review the configuration summary before enabling the configuration.

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

### Cisco Nexus 93180YC-FX-B

To set up the initial configuration for the Cisco Nexus A switch on <nexus-A-hostname>, follow these steps:



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

```
Abort Power On Auto Provisioning [yes - continue with normal setup, skip - bypass password and basic
configuration, no - continue with Power On Auto Provisioning] (yes/skip/no) [no]: yes
Disabling POAP.....Disabling POAP
poap: Rolling back, please wait... (This may take 5-15 minutes)

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

Do you want to enforce secure password standard (yes/no) [y]: Enter
Enter the password for "admin": <password>
Confirm the password for "admin": <password>
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]: Enter
Configure read-only SNMP community string (yes/no) [n]: Enter
Configure read-write SNMP community string (yes/no) [n]: Enter
Enter the switch name: <nexus-B-hostname>
```

```
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
Mgmt0 IPv4 address: <nexus-B-mgmt0-ip>
Mgmt0 IPv4 netmask: <nexus-B-mgmt0-netmask>
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway: <nexus-B-mgmt0-gw>
Configure advanced IP options? (yes/no) [n]: Enter
Enable the telnet service? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter
Type of ssh key you would like to generate (dsa/rsa) [rsa]: Enter
Number of rsa key bits <1024-2048> [1024]: Enter
Configure the ntp server? (yes/no) [n]: Enter
Configure default interface layer (L3/L2) [L2]: Enter
Configure default switchport interface state (shut/noshut) [noshut]: shut
Enter basic FC configurations (yes/no) [n]: n
Configure CoPP system profile (strict/moderate/lenient/dense) [strict]: Enter
Would you like to edit the configuration? (yes/no) [n]: Enter
```

1. Review the configuration summary before enabling the configuration.

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

## Cisco Nexus Switch Configuration

### Enable Features and Settings

To enable the required features for this deployment, run the following commands on both Cisco Nexus Switches:

```
config t
feature lacp
feature vpc
feature lldp
feature udld
```



The feature interface-valn is an optional requirement if configuring in-band VLAN interfaces.

### Configure Global Settings

To configure global settings for this deployment, run the following commands on both Cisco Nexus Switches:

```
config t
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
port-channel load-balance src-dst l4port
ntp server <global-ntp-server-ip> use-vrf management
ntp master 3
clock timezone <timzezone> <hour-offset> <minute-offset>
clock summer-time <timezone> <start-week> <start-day> <start-month> <start-time> <end-week> <end-day> <end-month> <minute-offset>
ip route 0.0.0.0/0 <<ib-mgmt-vlan-gateway>
copy run start
```



It is important to configure the local time so that logging time alignment and any back up schedules are correct. For more information on configuration of timezone and daylight savings time or summer time please see [<nexus config guide link>](#)

Sample Clock Command for United States Eastern timezone:

---

```
clock timezone EST -5 0
clock summer-time EDT 2 Sunday March 02:00 1 Sunday November 02:00 60
```

---

### Configure VLANs

To configure VLANs for this deployment, run the following commands on both Cisco Nexus Switches:

```
config t
vlan <<var-ib-mgmt-vlanid>>
name IB-MGMT-VLAN
vlan <<var-native-vlan-id>>
name Native-VLAN
vlan <<var-vmote-vlan-id>>
name vMotion-VLAN
vlan <<var-application-vlan-id>>
name VM-Appl-VLAN
```

Continue adding VLANs as appropriate for the environment.

### Add Interface Port Descriptions for Cisco Nexus 93180YC-FX-A

To configure port descriptions for this deployment, run the following commands on both Cisco Nexus Switches:

```
config t
interface Ethernet1/
description Network-Uplink-<<PORT>>
interface Ethernet1/
description Network-Uplink-<<PORT>>
interface Ethernet1/49
description <<var_ucs_clustertype>>-A eth 1/49
interface Ethernet1/50
description <<var_ucs_clustertype>>-B eth 1/49
interface Ethernet1/51
description Peer Link <<nexus-B-hostname>>-Eth1/51
interface Ethernet1/52
description Peer Link <<nexus-B-hostname>>-Eth1/52
```

### Add Interface Port Descriptions for Cisco Nexus 93180YC-FX-B

To configure port descriptions for this deployment, run the following commands on both Cisco Nexus Switches:

```
config t
interface Ethernet1/
description Network-Uplink-<<PORT>>
interface Ethernet1/
description Network-Uplink-<<PORT>>
interface Ethernet1/49
description <<var_ucs_clustertype>>-A eth 1/50
interface Ethernet1/50
description <<var_ucs_clustertype>>-B eth 1/50
interface Ethernet1/51
description Peer Link <<nexus-A-hostname>>-Eth1/51
interface Ethernet1/52
description Peer Link <<nexus-A-hostname>>-Eth1/52
```



---

## Port Channel Setup

### Configure vPC Domain Settings for Cisco Nexus 93180YC-FX-A

The vPC domain will be assigned a unique number from 1-1000 and will handle the vPC settings specified within the switches. For this deployment, vPC domain 10 is used.

```
config t
vpc domain 10
peer-switch
role priority 10
peer-keepalive destination <<vare_nexus_B_mgmt_ip>> source <<var_nexus_A_mgmt_ip>>
delay restore 150
peer-gateway
auto-recovery
ip arp synchronize
```

### Configure vPC Domain Settings for Cisco Nexus 93180YC-FX-B

The vPC domain will be assigned a unique number from 1-1000 and will handle the vPC settings specified within the switches. For this deployment, vPC domain 10 is used.

```
config t
vpc domain 10
peer-switch
role priority 20
peer-keepalive destination <<vare_nexus_A_mgmt_ip>> source <<var_nexus_B_mgmt_ip>>
delay restore 150
peer-gateway
auto-recovery
ip arp synchronize
```

### Configure vpc Peer-Link

On Cisco Nexus 93180YX-FX-A and Cisco Nexus 93180YC-FX-B switches, configure the Port Channel member interfaces that will be part of the vPC Peer Link and then configure the Peer Link.

```
config t
interface eth 1/51-52
switchport mode trunk
switchport trunk native <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib_mgmt_vlan_id>>, <<var_vmotion_vlan_id>>, <var_application_vlan_id>
channel-group 151 mode active
no shut
interface port-channel 151
description BB08-93180YC-FX Peer Link
vpc peer-link
```



The VPC and Port Channel numbers are chosen to indicate the first port in the channel. For example, a port channel starting with port ethernet 1/51 would be labeled as vpc and port-channel 151.

---

### Configure Port-Channel to Fabric Interconnect A

On Cisco Nexus 93180YX-FX-A and Cisco Nexus 93180YC-FX-B switches, configure the Port Channel member interfaces that will be part of the vPC link to Fabric Interconnect A.

```
config t
interface eth 1/49
switchport mode trunk
switchport trunk native <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib_mgmt_vlan_id>>, <<var_vmotion_vlan_id>>, <var_application_vlan_id>
spanning-tree port type edge trunk
channel-group 149 mode active
no shut
interface port-channel 149
description <<var_ucs_clustername>>-A
vpc 149
```

### Configure Port-Channel to Fabric Interconnect B

On Cisco Nexus 93180YX-FX-A and Cisco Nexus 93180YC-FX-B switches, configure the Port Channel member interfaces that will be part of the vPC link to Fabric Interconnect B.

```
config t
interface eth 1/50
switchport mode trunk
switchport trunk native <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib_mgmt_vlan_id>>, <<var_vmotion_vlan_id>>, <var_application_vlan_id>
spanning-tree port type edge trunk
channel-group 150 mode active
no shut
interface port-channel 150
description <<var_ucs_clustername>>-B
vpc 150
```

### Configure Port-Channel to Upstream network

On Cisco Nexus 93180YX-FX-A and Cisco Nexus 93180YC-FX-B switches, configure the Port Channel member interfaces that will be part of the vPC link to the upstream network.

```
config t
interface eth 1/53-54
switchport mode trunk
switchport trunk native <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib_mgmt_vlan_id>>, <<var_vmotion_vlan_id>>, <var_application_vlan_id>
channel-group 153 mode active
no shut
interface port-cahnnel 153
description Uplink
vpc 153
```

## Pure Storage Configuration

### Pure Storage FlashArray//X50 R3 Configuration

#### FlashArray Initial Configuration

The following information 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.

Array Settings	Variable Name
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_controller-1_mgmt_ip >>
Physical IP Address for Management on Controller 1 (CT1):	<<var_controller-2_mgmt_ip>>
Netmask:	<<var_controller-1_mgmt_mask>>
Gateway IP Address:	<<var_controller-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 and Port (For Pure1): (Optional)	
Time Zone:	<<var_timezone>>

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

#### Add an Alert Recipient

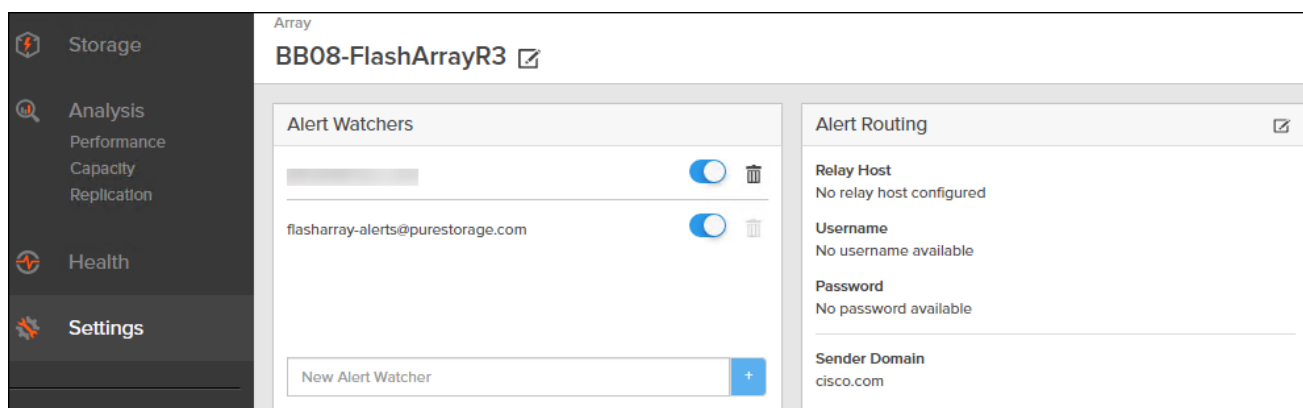
The Alerts sub-view is used to manage the list of addresses to which Purity delivers alert notifications, and the attributes of alert message delivery. You can designate up to 19 alert recipients. The Alert Recipients section displays a list of email addresses that are designated to receive Purity alert 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. Click 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.

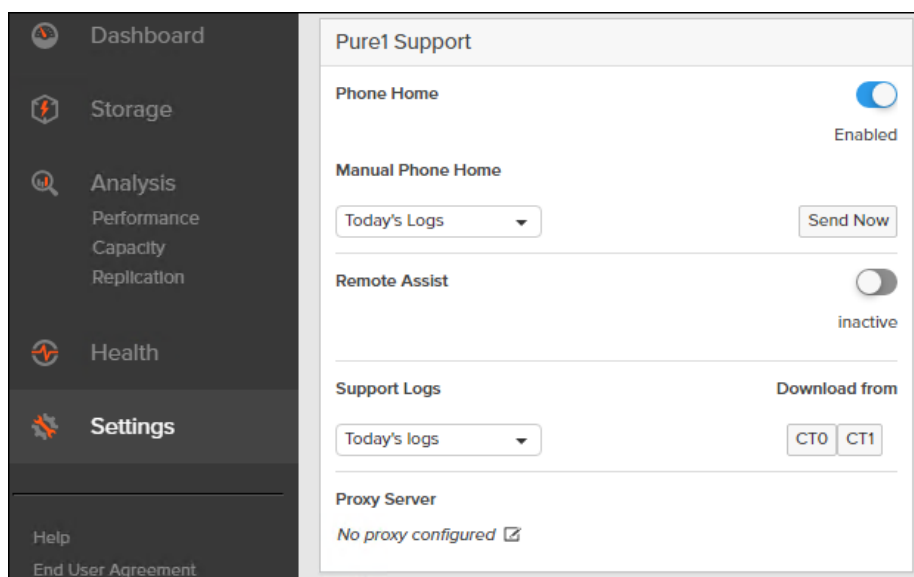
In the Sender Domain section, the sender domain determines how Purity logs are parsed and treated by Pure Storage Support and Escalations. By default, the sender domain is set to the domain name please-configure.me.



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.

## Configure Pure1 Support

The Pure1 Support section manages settings for Phone Home, Remote Assist, and Support Logs.



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. 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.

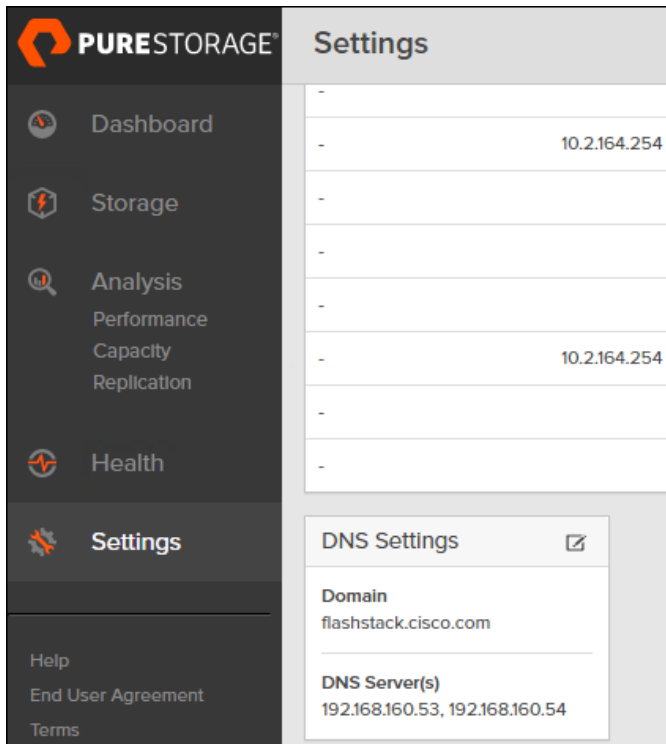
The Remote Assist section displays the remote assist status as "Connected" or "Disconnected". By default, remote assist is disconnected. A connected remote assist status means that a remote assist session has been opened, allowing Pure Storage Support to connect to the array. Disconnect the remote assist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

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.

### Configure DNS Server IP Addresses

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

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



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

The Directory Service 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 management interface. The top navigation bar includes 'System', 'Network', 'Users' (highlighted), and 'Software'. The left sidebar contains 'Dashboard', 'Storage', 'Analysis', 'Performance', 'Capacity', 'Replication', 'Health', and 'Settings'. The main content area is divided into two sections: 'Users' and 'Directory Service'.

The 'Users' section displays a table with the following data:

Name	Role	Type	Public Key	API Token	Lockout Remaining
pureuser	array_admin	local		****	-

The 'Directory Service' section includes a 'Test' button and two expandable panels: 'Configuration' and 'Roles'.

**Configuration:**

Enabled	False
URIs	-
Base DN	-
Bind User	-
Bind Password	-
User Login Attribute	-
User Object Class	-
Check Peer	False
CA Certificate	- Edit

**Roles:**

Name	Group	Group Base
array_admin		
ops_admin		
readonly		
storage_admin		

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.

To configure the Directory Service, follow these steps:

1. Click Settings > Users.
2. Click the icon in the Directory Services panel:
  - a. Enabled: Click 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.



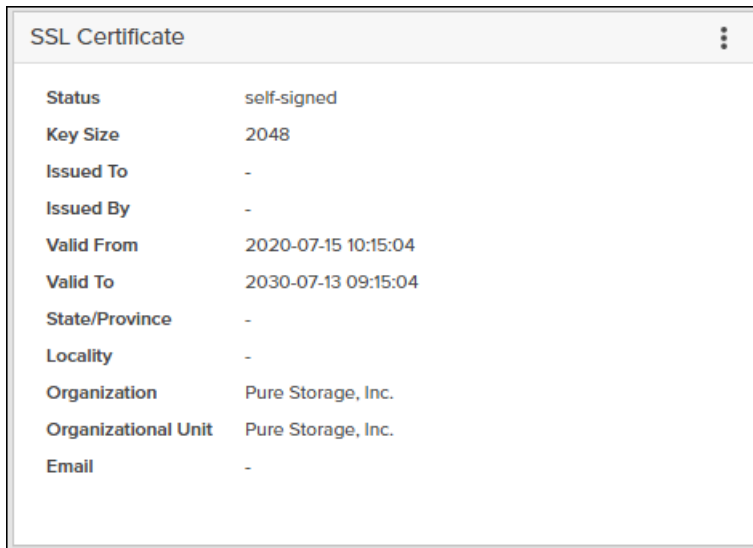
- 
- c. Base DN: Enter the base distinguished name (DN) of the directory service. The Base DN is built from the domain and should consist only of domain components (DCs). For example, for ldap://ad.storage.company.com, the Base DN would be: "DC=storage,DC=company,DC=com".
  - d. Bind User: Username used 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: Click 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

### Self-Signed Certificate

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.



The screenshot shows a window titled "SSL Certificate" with a list of attributes and their values. The attributes are: Status (self-signed), Key Size (2048), Issued To (-), Issued By (-), Valid From (2020-07-15 10:15:04), Valid To (2030-07-13 09:15:04), State/Province (-), Locality (-), Organization (Pure Storage, Inc.), Organizational Unit (Pure Storage, Inc.), and Email (-).

Attribute	Value
Status	self-signed
Key Size	2048
Issued To	-
Issued By	-
Valid From	2020-07-15 10:15:04
Valid To	2030-07-13 09:15:04
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-Signed 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 ×

<b>Country</b>	Two-letter ISO country code
<b>State/Province</b>	State, province, country or region
<b>Locality</b>	Full city name
<b>Organization</b>	Pure Storage, Inc.
<b>Organization Unit</b>	Pure Storage, Inc.
<b>Common Name</b>	FQDN or management IP address of the server
<b>Email</b>	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.

### Import Certificate ✕

**Certificate** Choose File No file chosen

**Private Key** Choose File No file chosen

**Intermediate Certificate (optional)** Choose File No file chosen

**Key Passphrase (optional)**

Cancel
Import

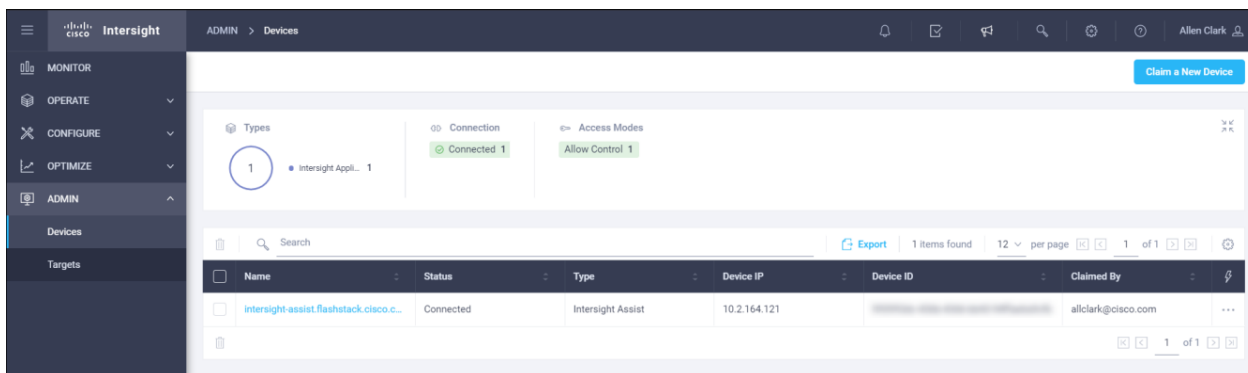
If the certificate is signed with the CSR that was constructed on the current array and you did not change the private key, you do not need to import the key. However, if the CSR was not constructed on the current array or if the private key has changed since you constructed the CSR, you must import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

### Claim FlashArray//X in Intersight (optional)

Claiming a Pure Storage FlashArray or VMware vCenter in Cisco Intersight requires the use of an Intersight Assist virtual machine. Please refer to the following link if there is not already an Intersight Assist system in your environment: [https://www.cisco.com/c/en/us/td/docs/unified\\_computing/Intersight/cisco-intersight-assist-getting-started-guide/m-installing-cisco-intersight-assist.html](https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/cisco-intersight-assist-getting-started-guide/m-installing-cisco-intersight-assist.html)

To claim FlashArray//X in Intersight, follow these steps:

1. Open a browser to Cisco Intersight, <https://intersight.com> and log in to your Intersight account.
2. Click Admin > Devices.



3. Click Claim a New Device and click Claim Through Intersight Assist.

- Set Type to Pure Storage FlashArray.
- Enter FlashArray Hostname/ IP address and credentials.

- Click Claim.

Name	Status	Type	Device IP	Device ID	Claimed By	
10.2.164.102	Connected	Pure Storage FlashArray	10.2.164.102	[REDACTED]	alliclark@cisco.com	...
intersight-assist.flashstack.cisco.c...	Connected	Intersight Assist	10.2.164.121	[REDACTED]	alliclark@cisco.com	...
BB08-FI-6454	Connected	UCS Domain	10.1.164.51, 10.1.164.1... (2)	[REDACTED]	alliclark@cisco.com	...

## MDS 9132T Configuration

The following procedures describe how to configure the Cisco MDS fibre channel switches for use in a base FlashStack environment. This procedure assumes the use of Nexus 9132T switches running NX-OS 8.4(1a) 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.

### 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 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 9132T-A

To set up the initial configuration for the Cisco MDS A switch on <mds\_A\_hostname>, follow these steps:

1. Configure the switch.

```
----- System Admin Account Setup -----
Do you want to enforce secure password standard (yes/no) [y]: Enter
Enter the password for "admin": <password>
Confirm the password for "admin": <password>
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]: Enter
Configure read-only SNMP community string (yes/no) [n]: Enter
Configure read-write SNMP community string (yes/no) [n]: Enter
Enter the switch name: <mds-A-hostname>
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
Mgmt0 IPv4 address: <mds-A-mgmt0-ip>
Mgmt0 IPv4 netmask: <mds-A-mgmt0-netmask>
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway: <<var_oob_gateway>>
Configure advanced IP options? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter
Type of ssh key you would like to generate (dsa/rsa) [rsa]: Enter
Number of rsa key bits <1024-2048> [1024]: Enter
Enable the telnet server: (yes/no) [n]: Enter
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
Configure the ntp server? (yes/no) [n]: Enter
Configure default switchport interface state (shut/noshut) [noshut]: shut
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
Would you like to edit the configuration? (yes/no) [n]: Enter
```

2. Review the configuration summary before enabling the configuration.

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

## Cisco MDS 9132T-B

To set up the initial configuration for the Cisco MDS B switch on <mds\_B\_hostname>, follow these steps:

### 1. Configure the switch.

```
----- System Admin Account Setup -----
Do you want to enforce secure password standard (yes/no) [y]: Enter
Enter the password for "admin": <password>
Confirm the password for "admin": <password>
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]: Enter
Configure read-only SNMP community string (yes/no) [n]: Enter
Configure read-write SNMP community string (yes/no) [n]: Enter
Enter the switch name: <mds-B-hostname>
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
Mgmt0 IPv4 address: <mds-B-mgmt0-ip>
Mgmt0 IPv4 netmask: <mds-B-mgmt0-netmask>
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway: <<var_oob_gateway>>
Configure advanced IP options? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter
Type of ssh key you would like to generate (dsa/rsa) [rsa]: Enter
Number of rsa key bits <1024-2048> [1024]: Enter
Enable the telnet server: (yes/no) [n]: Enter
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
Configure the ntp server? (yes/no) [n]: Enter
Configure default switchport interface state (shut/noshut) [noshut]: shut
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
Would you like to edit the configuration? (yes/no) [n]: Enter
```

### 2. Review the configuration summary before enabling the configuration.

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

## Cisco MDS Switch Configuration

### Enable Features and Settings

To enable the required features for this deployment, run the following commands on both Cisco Nexus Switches:

```
config t
feature npiv
feature fport-channel-trunk
```

### Configure Port Channel for MDS 9132T-A

To configure a port channel on MDS 9132T-A and add the interfaces connecting into the Cisco UCS Fabric Interconnect-A, run the following commands:

```
config t
interface port-channel 100
channel mode active
```



```
switchport rate-mode dedicated
interface fc 1/1-4
port-license acquire
channel-group 100 force
no shutdown
```

### Configure VSAN for MDS 9132T-A

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, by running the following commands:

```
config t
vsan database
vsan <<var_vsan_a_id>>
vsan <<var_vsan_a_id>> name FlashStack-A
vsan <<var_vsan_a_id>> interface fc 1/1-4
vsan <<var_vsan_a_id>> interface fc 1/15-18
vsan <<var_vsan_a_id>> interface po100
zone smart-zoning enable vsan <<var_vsan_a_id>>
```

### Configure Port Channel for MDS 9132T-B

On MDS 9132T-B configure a port channel and add the interfaces connecting into the Cisco UCS Fabric Interconnect-B, by running the following commands:

```
config t
interface port-channel 200
channel mode active
switchport rate-mode dedicated
interface fc 1/1-4
port-license acquire
channel-group 100 force
no shutdown
```

### Configure VSAN for MDS 9132T-B

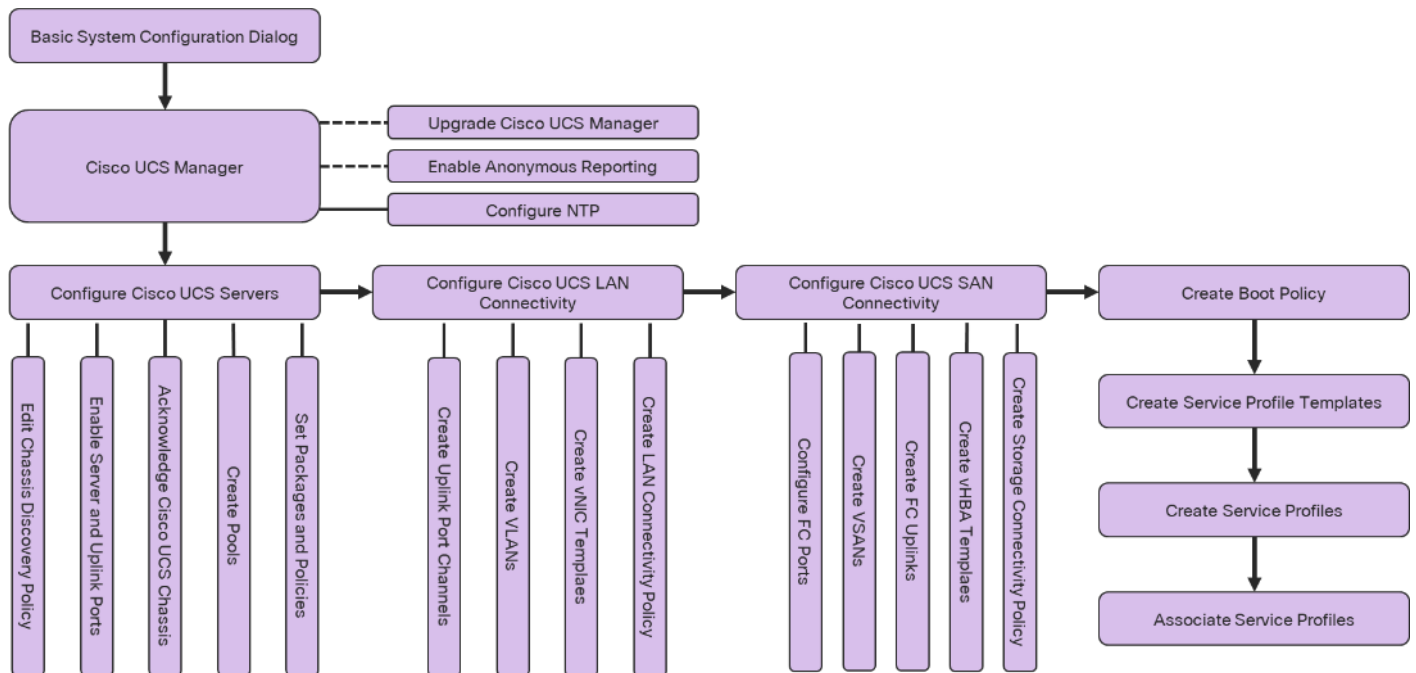
On MDS 9132T B create the VSAN that will be used for connectivity to the Cisco UCS Fabric Interconnect and the Pure Storage FlashArray. Assign this VSAN to the interfaces that will connect to the Pure Storage FlashArray, as well as the interfaces and the Port Channel they create that are connected to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

```
config t
vsan database
vsan <<var_vsan_b_id>>
vsan <<var_vsan_b_id>> name FlashStack-B
vsan <<var_vsan_b_id>> interface fc 1/1-4
vsan <<var_vsan_b_id>> interface fc 1/15-18
vsan <<var_vsan_b_id>> interface po100
zone smart-zoning enable vsan <<var_vsan_b_id>>
```

## Cisco UCS Configuration

The following procedures describe how to configure the Cisco UCS domain for use in a base FlashStack environment. This procedure assumes you're using Cisco UCS Fabric Interconnects running 4.1(2a). Configuration on a differing model of Cisco UCS Fabric Interconnects should be comparable but may differ slightly with the model and changes in the Cisco UCS Manager (Cisco UCSM) release. The Cisco USC 6454 Fabric Interconnects and Cisco UCS Manager 4.1(2a) release were used in validation of this FlashStack solution, so the steps will reflect this model and release.

**Figure 4. Cisco UCS Configuration Workflow**



### Physical Connectivity

The physical cabling should be completed by following the diagram and table references in section [Physical Topology](#).

### 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.

#### Cisco UCS Fabric Interconnect A

To set up the initial configuration for the Cisco Fabric Interconnect A, follow these steps:

1. Configure the Fabric Interconnect:

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

```
Enter the configuration method. (console/gui) ? console
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (y/n) [y]: enter
Enter the password for "admin": <<password>>
Confirm the password for "admin": <<password>>
Is this Fabric interconnect part of a cluster(select 'no' for standalone)? (yes/no) [n]: yes
Enter the switch fabric (A/B) []: A
Enter the system name: <var_ucs_clustername>>
Physical Switch Mgmt0 IP address : <<var_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]: noConfigure
Would you like to edit the configuration? (yes/no) [n]: Enter
```

## 2. Review the configuration summary before enabling the configuration:

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

### Cisco UCS Fabric Interconnect A

To set up the initial configuration for the Cisco Fabric Interconnect A, follow these steps:

#### 1. Configure the Fabric Interconnect:

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

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
Physical Switch Mgmt0 IP address : <<var_ucs_a_mgmt_ip>>
```

## 2. Review the configuration summary before enabling the configuration:

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

### Cisco UCS Manager Configuration

To log into 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 UCS Manager login is prompted, enter admin for the user name and enter the administrative password.
5. Click Login to log into Cisco UCS Manager.

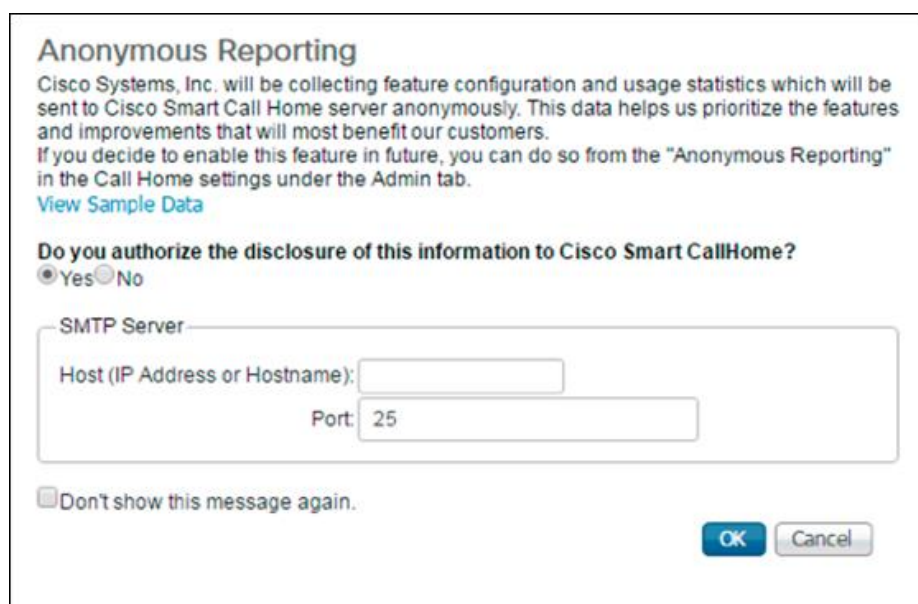
## Upgrade Cisco UCS Manager to Version 4.1(2a)

This document assumes you're using Cisco UCS 4.1(2a). To upgrade the Cisco UCS Manager software and the Cisco UCS Fabric Interconnect software to version 4.1(2a), 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, follow this step:

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



**Anonymous Reporting**

Cisco Systems, Inc. will be collecting feature configuration and usage statistics which will be sent to Cisco Smart Call Home server anonymously. This data helps us prioritize the features and improvements that will most benefit our customers.  
If you decide to enable this feature in future, you can do so from the "Anonymous Reporting" in the Call Home settings under the Admin tab.  
[View Sample Data](#)

**Do you authorize the disclosure of this information to Cisco Smart CallHome?**  
 Yes  No

SMTP Server

Host (IP Address or Hostname):

Port:

Don't show this message again.

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 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 then click OK.

Communication Management / Call Home

General Profiles Call Home Policies System Inventory Anonymous Reporting Events FSM

**Admin**

State :  Off  On

Switch Priority : Debugging

Throttling :  Off  On

**States**

**Contact Information**

Contact :

Phone :

Email :

Address :

**Ids**

Customer ID :

Contract ID :

Site ID :

**Email Addresses**

From :

Reply To :

**SMTP Server**

Host (IP Address or Hostname) :

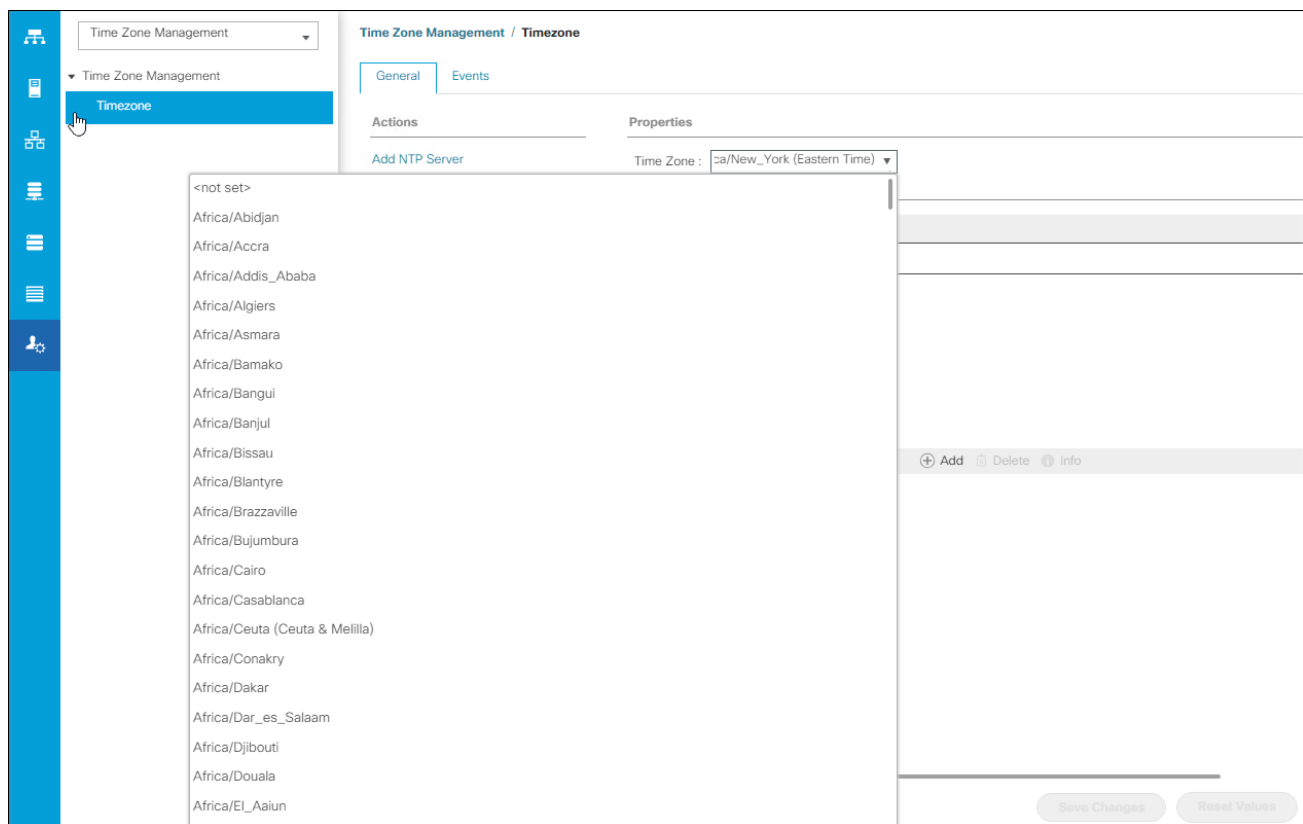
Port :

Save Changes

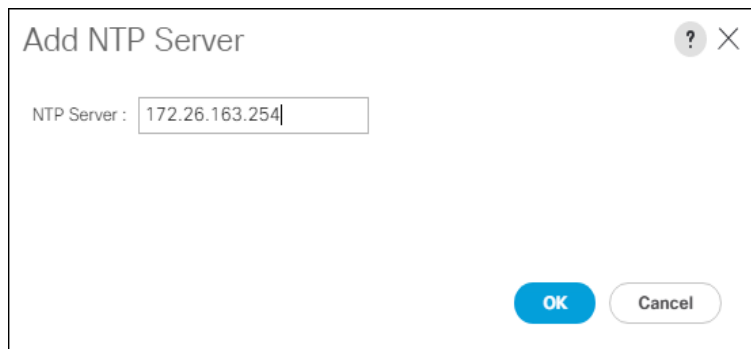
## Configure NTP

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.



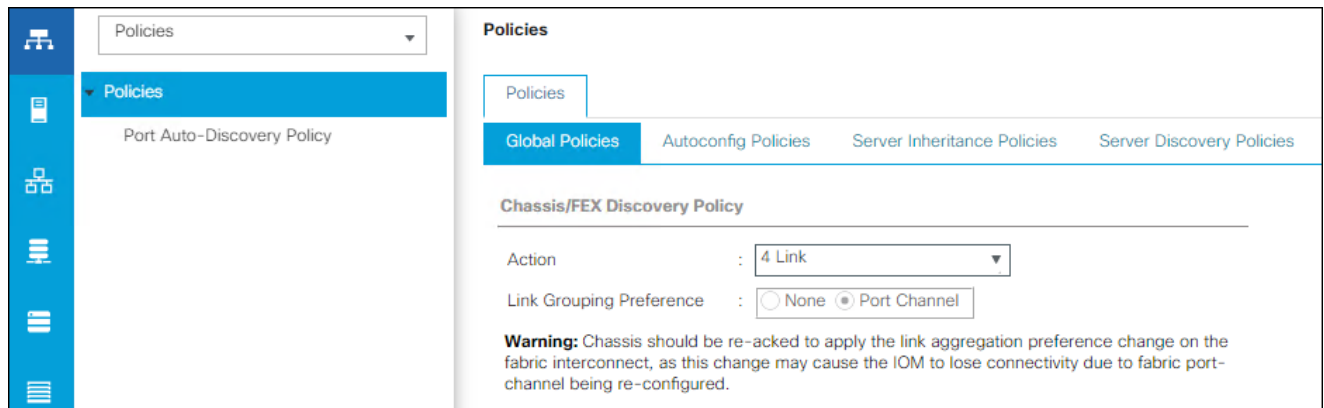
7. Click OK.

## Configure Cisco UCS Servers

### Edit Chassis Discovery Policy

Setting the discovery policy simplifies the addition of 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 from the drop-down list.
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.



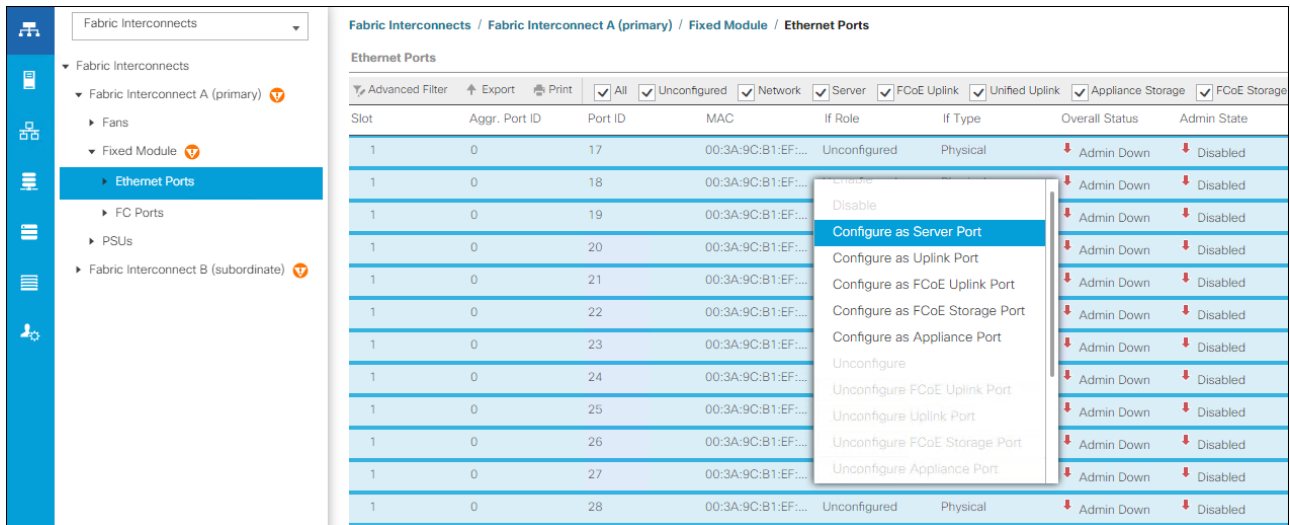
The screenshot shows the Cisco UCS Manager interface. On the left is a navigation pane with a 'Policies' dropdown menu and a list of policy types, including 'Port Auto-Discovery Policy'. The main content area is titled 'Policies' and has tabs for 'Global Policies', 'Autoconfig Policies', 'Server Inheritance Policies', and 'Server Discovery Policies'. The 'Global Policies' tab is active, showing the 'Chassis/FEX Discovery Policy' configuration. The 'Action' is set to '4 Link' and the 'Link Grouping Preference' is set to 'Port Channel' (selected with a radio button). A warning message states: 'Warning: Chassis should be re-acked to apply the link aggregation preference change on the fabric interconnect, as this change may cause the IOM to lose connectivity due to fabric port-channel being re-configured.'

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

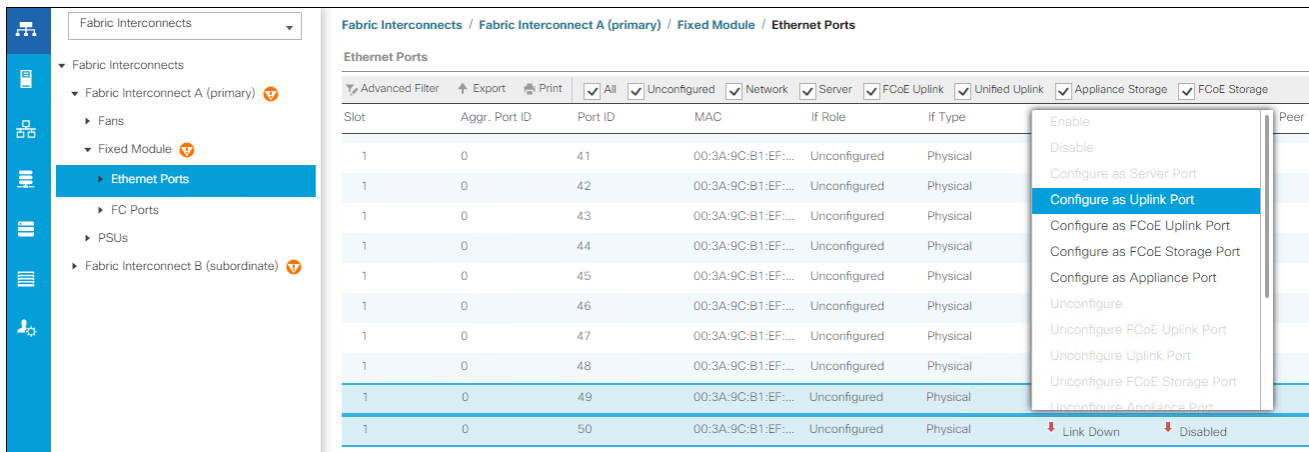
### Enable Server and Uplink Ports

To enable server and uplink ports, follow these steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane.
2. Click Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module.
3. Expand Ethernet Ports.
4. Select the ports that are connected to the 2408, C4200 Servers, and/or C Series Servers , right-click them, and click "Configure as Server Port."



- Click Yes to confirm server ports and click OK.
- Verify that the ports connected to the chassis are now configured as server ports.
- Select ports 49 and 50 that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.



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

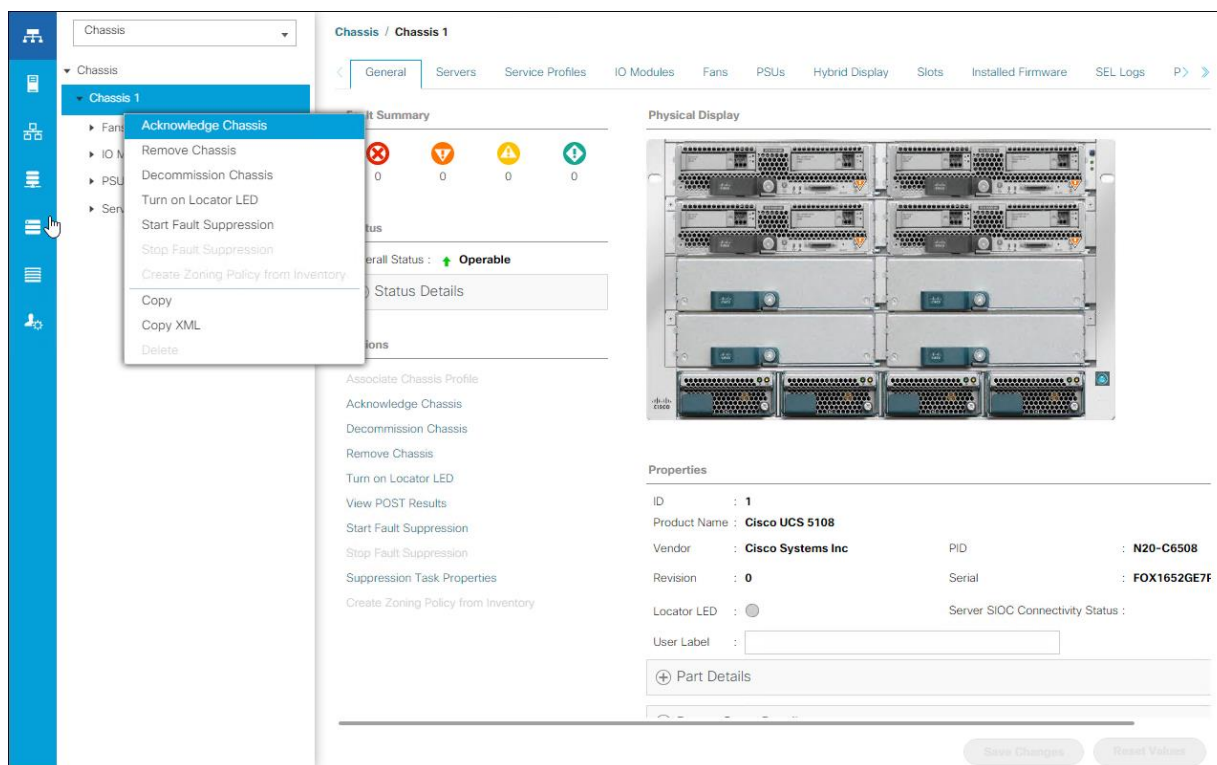


14. Click Yes to confirm the uplink ports and click OK.

### 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 click 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. Click 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. Click Create MAC Pool to create the MAC address pool.
5. Enter MAC\_Pool\_A for the name of the MAC pool.
6. Optional: Enter a description for the MAC pool.
7. Select Sequential for the option for Assignment Order.

**Create MAC Pool** ? X

1 Define Name and Description

2 Add MAC Addresses

Name : MAC\_Pool\_A

Description : FlashStack BB A side mac pool

Assignment Order :  Default  Sequential

< Prev Next > Finish Cancel

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 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 enough to support the available blade or server resources.

---

## Create a Block of MAC Addresses ? ×

First MAC Address :  Size :

To ensure uniqueness of MACs in the LAN fabric, you are strongly encouraged to use the following MAC prefix:  
**00:25:B5:xx:xx:xx**

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 for the name of the MAC pool.

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

1 Define Name and Description

2 Add MAC Addresses

Create MAC Pool

Name : MAC\_Pool\_B

Description : FlashStack BB B side mac pool

Assignment Order :  Default  Sequential

< Prev Next > Finish Cancel

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 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.

Create a Block of MAC Addresses

First MAC Address : 00:25:B5:91:1B:00      Size : 32

To ensure uniqueness of MACs in the LAN fabric, you are strongly encouraged to use the following MAC prefix:  
**00:25:B5:xx:xx:xx**

OK      Cancel

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. Click the SAN tab on the left.
2. Click Pools > root.
3. Right-click WWNN Pools under the root organization.
4. Click 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. Click Sequential for Assignment Order.

Create WWNN Pool

1 Define Name and Description

2 Add WWN Blocks

Name : WWNN\_Pool

Description : FlashStack BB WWNN Pool

Assignment Order :  Default  Sequential

< Prev Next > Finish Cancel

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 6<sup>th</sup> octet was changed from 00 to 01 to represent as identifying information for this being our first Cisco UCS domain.



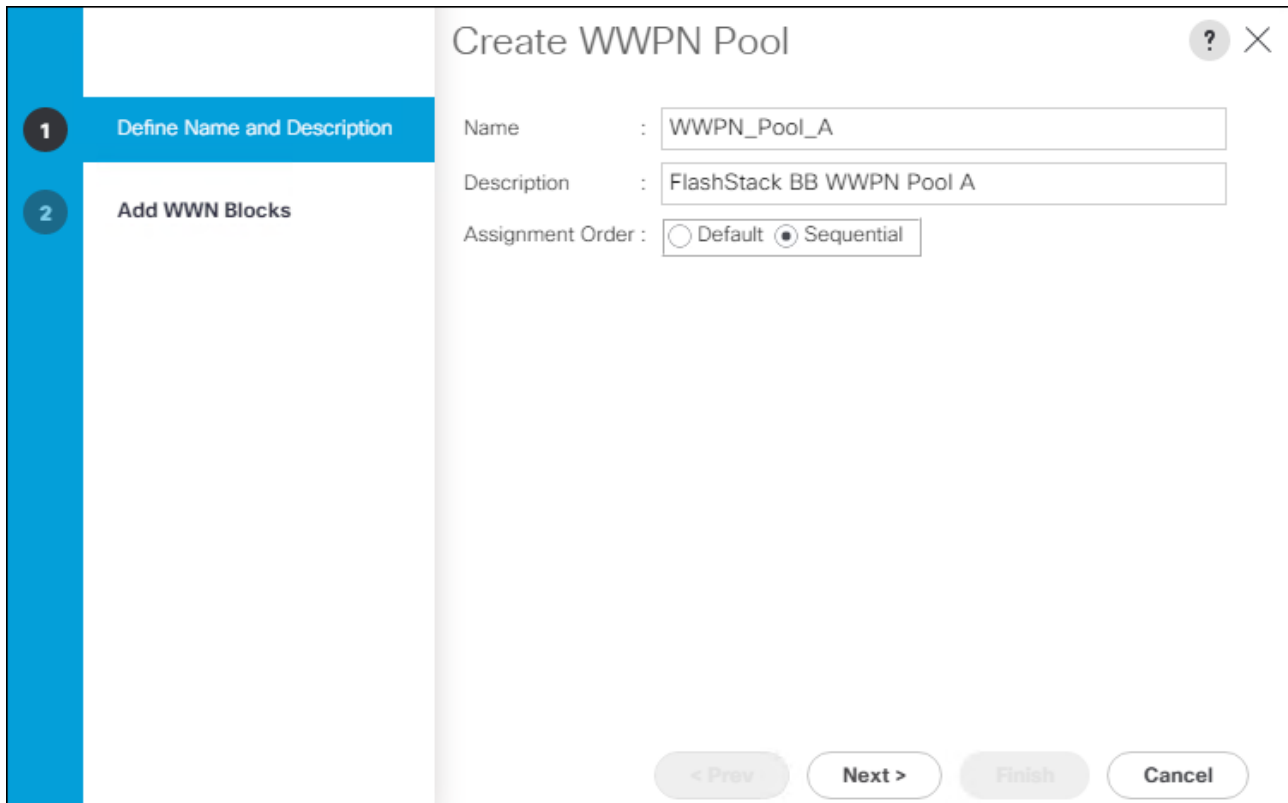
Also, when having multiple Cisco UCS domains sitting in adjacency, it is important that these blocks, the WWNN, WWPN, and MAC hold differing values between each set.

11. Specify a size of the WWNN block enough 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. Click 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. Click Create WWPN Pool to create the WWPN pool.
6. Enter WWPN\_Pool\_A for the name of the WWPN pool.
7. Optional: Enter a description for the WWPN pool.
8. Select Sequential for Assignment Order.



1 Define Name and Description

2 Add WWN Blocks

Create WWPN Pool

Name : WWPN\_Pool\_A

Description : FlashStack BB WWPN Pool A

Assignment Order :  Default  Sequential

< Prev Next > Finish Cancel

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 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 enough to support the available blade or server resources.



---

### Create WWN Block

From :  Size :

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

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

13. Click OK.

14. Click Finish.

15. In the confirmation message, click OK.

16. Right-click WWPN Pools under the root organization.

17. Click Create WWPN Pool to create the WWPN pool.

18. Enter WWPN\_Pool\_B for the name of the WWPN pool.

19. Optional: Enter a description for the WWPN pool.

20. Select Sequential for Assignment Order.

1 Define Name and Description

2 Add WWN Blocks

Create WWPN Pool

Name : WWPN\_Pool\_B

Description : FlashStack BB WWPN Pool B

Assignment Order :  Default  Sequential

< Prev Next > Finish Cancel

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 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.

Create WWN Block

From :  Size :

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

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

OK Cancel

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. Click Pools > root.
3. Right-click UUID Suffix Pools.
4. Click Create UUID Suffix Pool.
5. Enter UUID\_Pool for the name of the UUID suffix pool.

**1** Define Name and Description

**2** Add UUID Blocks

### Create UUID Suffix Pool

Name :

Description :

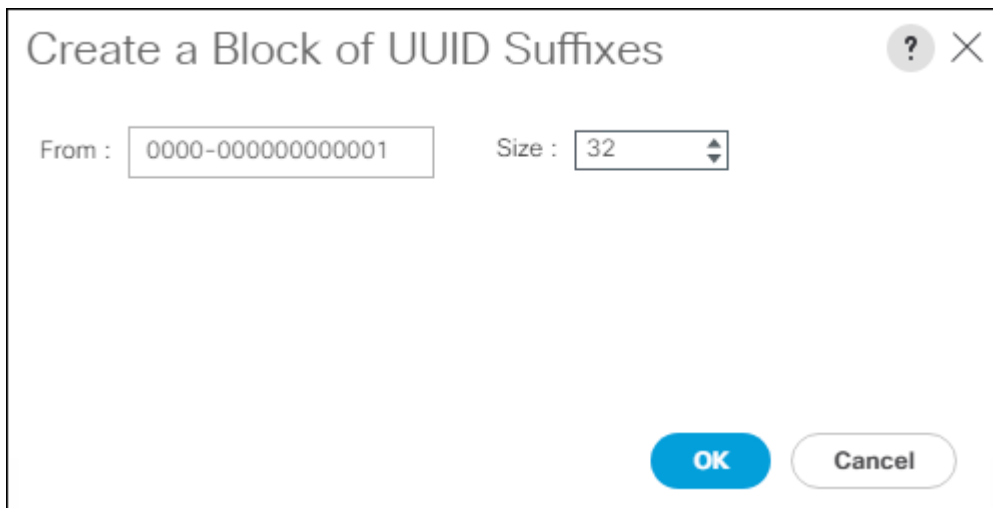
Prefix :  Derived  other

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.

---

Create a Block of UUID Suffixes

From : 0000-000000000001      Size : 32

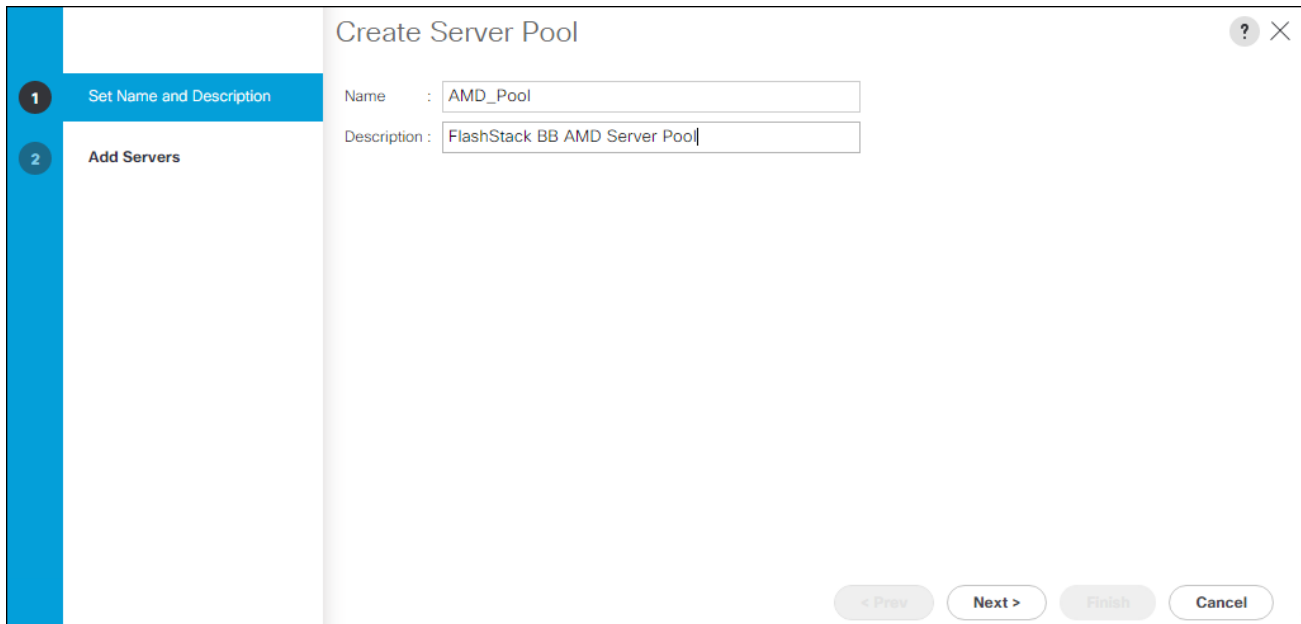
OK      Cancel

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

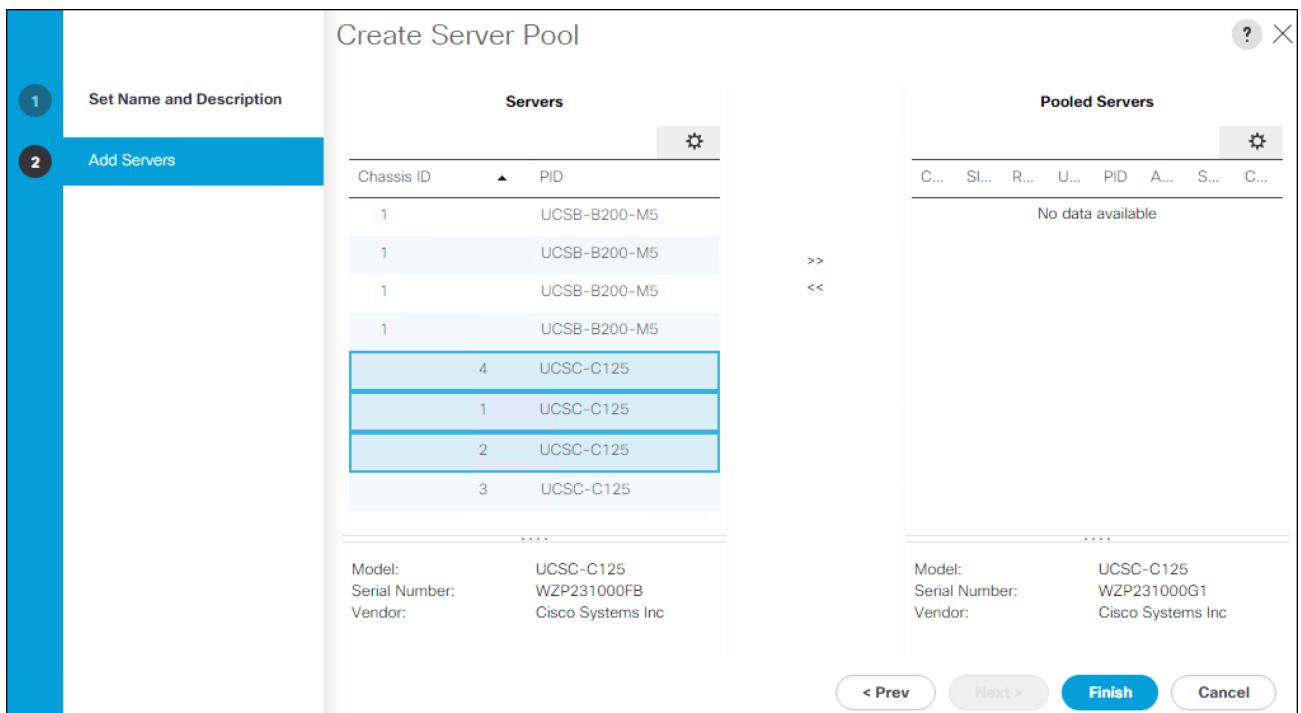
#### **Create Server Pool**

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. Click Pools > root.
3. Right-click Server Pools.
4. Click Create Server Pool.
5. Enter AMD\_Pool for the name of the server pool.



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



9. Click Finish.

10. Click OK



UCS Domains with both AMD and Intel based servers should have separate server pools for each server type.

### 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. Click Pools > root > IP Pools.
3. Right-click IP Pool ext-mgmt and click Create Block of IPv4 Addresses.

**Create Block of IPv4 Addresses**

From :       Size :

Subnet Mask :       Default Gateway :

Primary DNS :       Secondary DNS :

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. Click Policies > root.
3. Expand Host Firmware Packages.
4. Click default.
5. In the Actions pane, click Modify Package Versions.
6. Select the version 4.1(2a)B for the Blade Package, and optionally set version 4.1(2a)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)

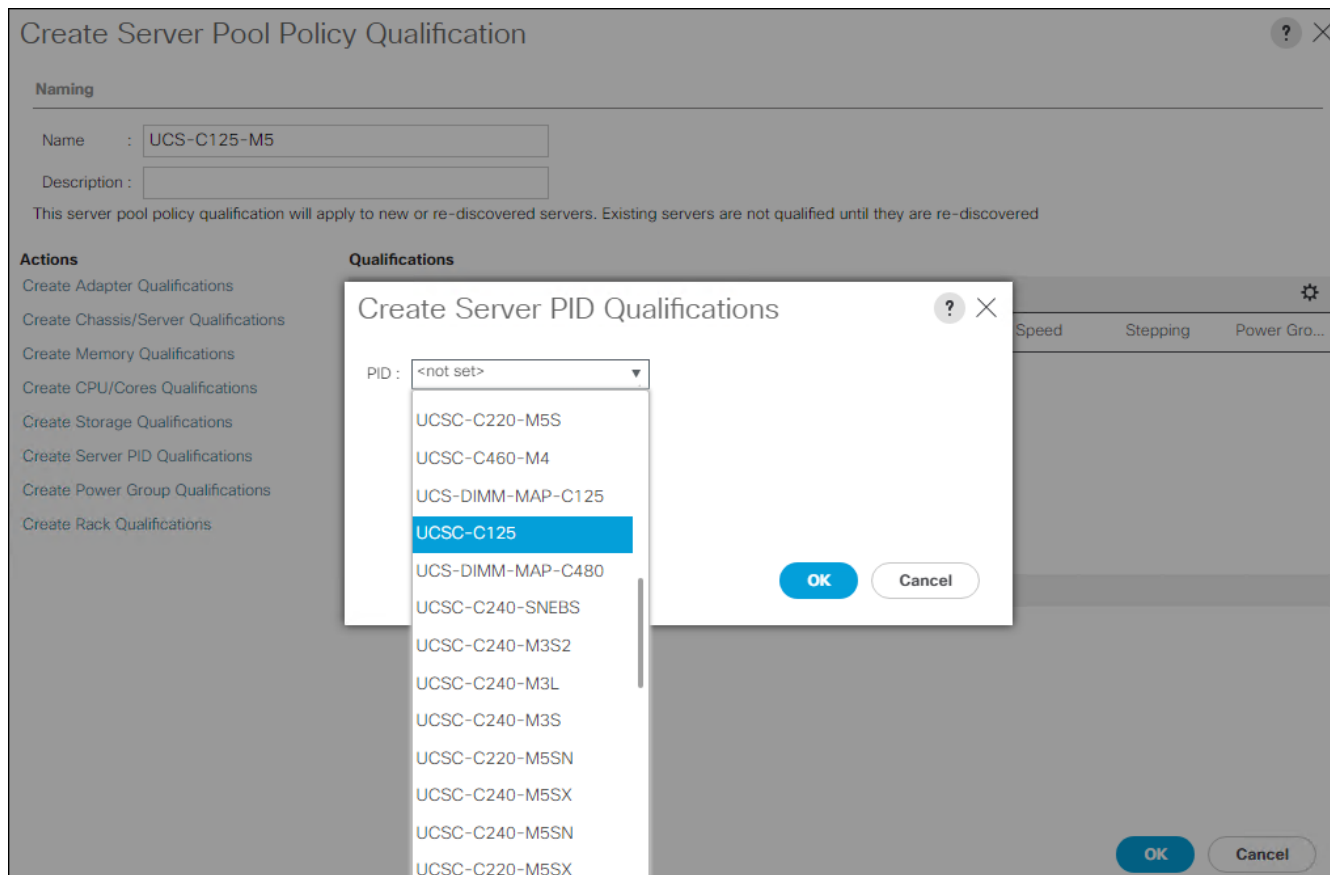
To create an optional server pool qualification policy for the Cisco UCS environment, follow these steps:



This example creates a policy for Cisco UCS C125 M5 servers for a server pool.

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Click Policies > root.
3. Right-click Server Pool Policy Qualifications.
4. Click Create Server Pool Policy Qualification.

5. Name the policy UCS-C125-M5.
6. Click Create Server PID Qualifications.
7. Choose UCSC-125 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.



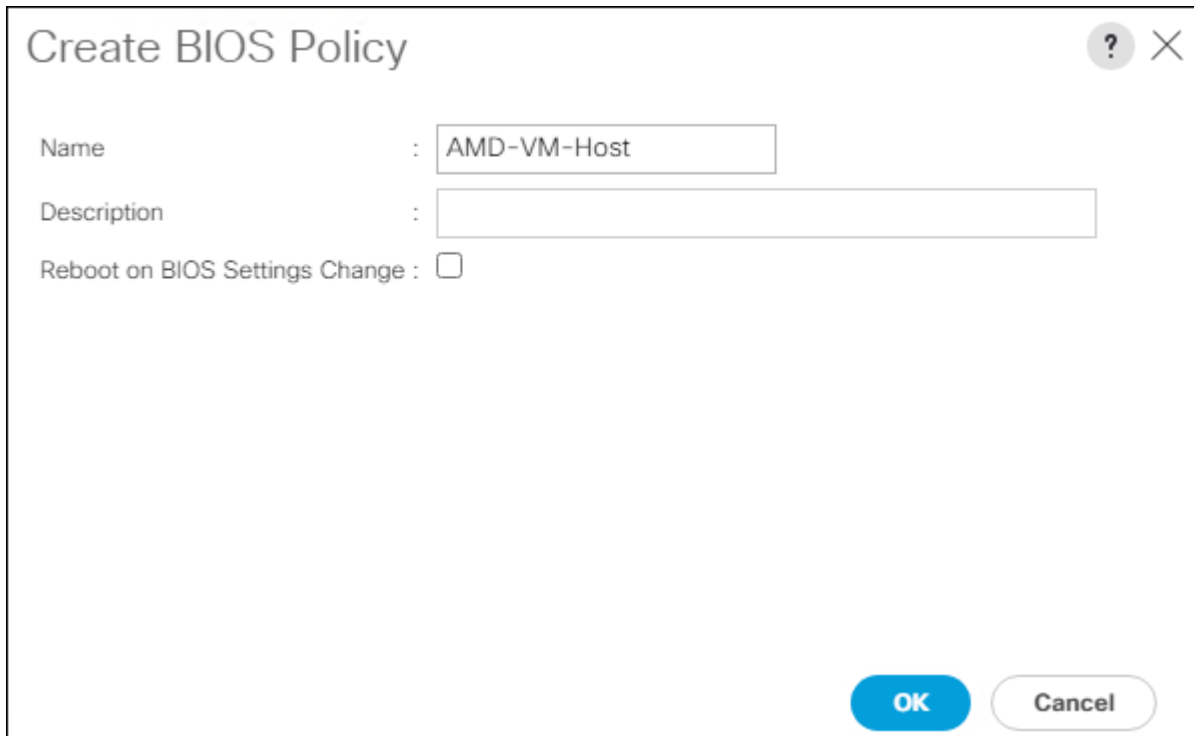
UCS Domains with both AMD and Intel based servers should have separate server pool policy qualifications for each server type.

### 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. Click Policies > root.

3. Right-click BIOS Policies.
4. Click Create BIOS Policy.
5. Enter AMD-VM-Host for the BIOS policy name.



**Create BIOS Policy** ? X

Name : AMD-VM-Host

Description :

Reboot on BIOS Settings Change :

OK Cancel

6. Click the newly created BIOS Policy.
7. Within the Main tab of the Policy:
  - a. Change CDN Control to enabled.
  - b. Change the Quiet Boot setting to disabled.

Policies / root / BIOS Policies / AMD-VM-Host

Main | Advanced | Boot Options | Server Management | Events

**Actions**

Delete  
Show Policy Usage  
Use Global

**Properties**

Name : **AMD-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

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

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

9. Set the following within the Processor tab:

- a. Core Performance Boost -> Auto
- b. Global C-state Control -> Disabled
- c. L1 Stream HW Prefetcher -> Enabled
- d. L2 Stream HW Prefetcher -> Enabled
- e. Determinism Slider -> Power
- f. IOMMU -> Enabled
- g. AMD Memory Interleaving -> Auto
- h. AMD Memory Interleaving Size -> Auto
- i. SMEE -> Enabled
- j. SMT Mode -> Auto
- k. SVM Mode -> Enabled

Policies / root / BIOS Policies / AMD-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 Configuration

Advanced Filter | Export | Print

BIOS Setting	Value
XPT Prefetch	Platform Default
Core Performance Boost	Auto
Downcore control	Platform Default
Global C-state Control	Disabled
L1 Stream HW Prefetcher	Enabled
L2 Stream HW Prefetcher	Enabled
Determinism Slider	Power
IOMMU	Enabled
Bank Group Swap	Platform Default
Chipselect Interleaving	Platform Default
Configurable TDP Control	Platform Default
AMD Memory Interleaving	Auto
AMD Memory Interleaving Size	Auto
SMEE	Enabled
SMT Mode	Auto
SVM Mode	Enabled

10. Click Save Changes.

11. Click OK.



For more information, see [Performance Tuning for Cisco UCS C125 Rack Server Nodes with AMD Processors](#).

### Update Default Maintenance Policies

To update the default Maintenance Policy, follow these steps:

1. In Cisco UCS Manager, click the Servers tab.
2. Click Policies > root.
3. Click Maintenance Policies > default.
4. Change the Reboot Policy to User Ack.
5. (Optional: Click “On Next Boot” to delegate maintenance windows to server owners).

Policies / root / Maintenance Policies / default

General Events

Actions	Properties
Delete	Name : default
Show Policy Usage	Description : <input type="text"/>
Use Global	Owner : Local
	Soft Shutdown Timer : 150 Secs
	Storage Config. Deployment Policy : <input type="radio"/> Immediate <input checked="" type="radio"/> User Ack
	Reboot Policy : <input type="radio"/> Immediate <input checked="" type="radio"/> User Ack <input type="radio"/> Timer Automatic
	<input checked="" type="checkbox"/> On Next Boot (Apply pending changes at next reboot.)

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.
2. Click Policies > root.
3. Right-click Local Disk Config Policies.
4. Click Create Local Disk Configuration Policy.
5. Enter SAN-Boot for 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.
2. Click Policies > root.

3. Right-click Power Control Policies.
4. Click Create Power Control Policy.
5. Enter No-Power-Cap for the power control policy name.
6. Change the power capping setting to No Cap.

**Create Power Control Policy**

Name : No-Power-Cap

Description :

Fan Speed Policy : Any

**Power Capping**

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

No Cap  cap

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

OK Cancel

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. Click Policies > root.
3. Right-click Network Control Policies.



4. Click Create Network Control Policy.
5. Enter Enable\_CDP for the policy name.
6. For CDP, choose the Enabled option.
7. Click OK to create the network control policy.

**Create Network Control Policy**

Name :

Description :

CDP :  Disabled  Enabled

MAC Register Mode :  Only Native Vlan  All Host Vlans

Action on Uplink Fail :  Link Down  Warning

**MAC Security**

Forge :  Allow  Deny

**LLDP**

8. Click OK.

## 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 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. Click Create Port Channel.

5. Enter a unique ID for the port channel, (149 in our example to correspond with the upstream Nexus port channel).
6. With 149 selected, enter PC-149-Nexus for the name of the port channel.

**Create Port Channel**

ID : 149

Name : PC-149-Nexus

< Prev   **Next >**   Finish   Cancel

7. Click Next.
8. Select the following ports to be added to the port channel:
  - a. Slot ID 1 and port 49
  - b. Slot ID 1 and port 50

**Create Port Channel**

Ports			
Slot ID	Aggr. Po...	Port	MAC
1	0	49	00:DE:F...
1	0	50	00:DE:F...

>>

Ports in the port channel			
Slot ID	Aggr. Po...	Port	MAC
No data available			

<<

< Prev   Next >   **Finish**   Cancel

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. Click Create Port Channel.

15. Enter a unique ID for the port channel, (150 in our example to correspond with the upstream Nexus port channel).

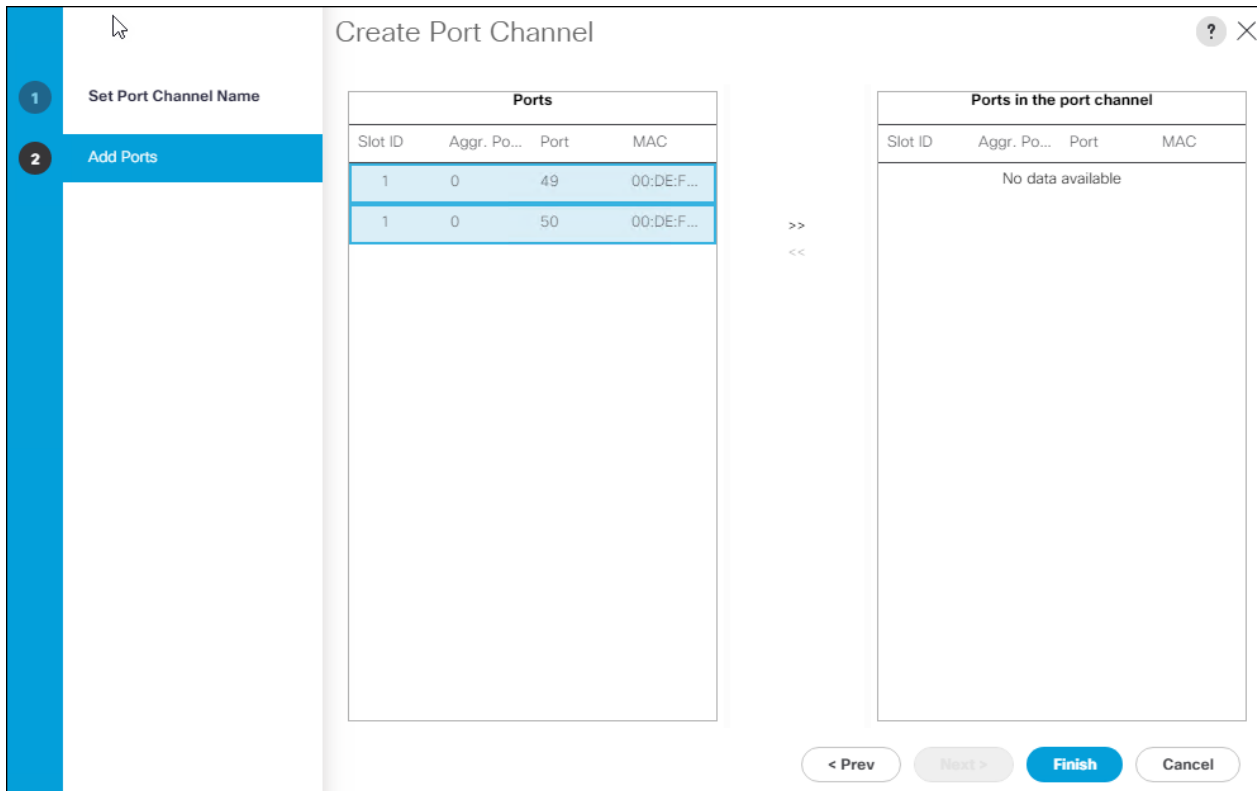
16. With 150 selected, enter PC-150-Nexus for the name of the port channel.

The screenshot shows a 'Create Port Channel' dialog box. On the left, a vertical sidebar contains two steps: '1 Set Port Channel Name' (highlighted in blue) and '2 Add Ports'. The main content area displays 'ID : 150' and 'Name : PC-150-Nexus'. At the bottom right, there are four buttons: '< Prev' (disabled), 'Next >' (disabled), 'Finish' (active/highlighted), and 'Cancel' (disabled). A help icon (?) and a close icon (X) are in the top right corner.

17. Click Next.

18. Select the following ports to be added 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 this procedure, six unique VLANs are created. See [Table 2](#) for a list of VLANs to be created.

2. Click LAN > LAN Cloud.
3. Right-click VLANs.
4. Click Create VLANs.
5. Enter Native-VLAN for the name of the VLAN to be used for 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

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 choose Set as Native VLAN.

**LAN Cloud**

LAN Uplinks | **VLANs** | Server Links | MAC Identity Assignment | IP Identity Assignment | QoS | Global Policies | Faults

All | Dual Mode | Fabric A | Fabric B | VLAN Groups | VP Optimization Sets

Advanced Filter | Export | Print

Name	ID	Fabric ID	Type	Transport	Native	VLAN Sharing
VLAN default ...	1	Dual	Lan	Ether	Yes	None
VLAN Native-...	2	Dual	Lan	Ether	No	None

Add
  Delete
  Info

Show Navigator  
 Set as Native VLAN  
 Set as Not Native VLAN

Details

11. Click Yes and then click OK.
12. Right-click VLANs.
13. Click Create VLANs.
14. Enter IB-Mgmt for 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

[Check Overlap](#) [OK](#) [Cancel](#)

18. Click OK and then click OK again.

19. Right-click VLANs.

20. Click Create VLANs.

21. Enter vMotion for 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.

## Create VLANs

VLAN Name/Prefix : vMotion

Multicast Policy Name : <not set> [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 : 1130

Sharing Type :  None  Primary  Isolated  Community

[Check Overlap](#) [OK](#) [Cancel](#)

25. Click OK and then click OK again.

26. Right-click VLANs.

27. Click Create VLANs.

28. Enter VM-App- for 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.



**Create VLANs**

VLAN Name/Prefix : VM-APP-

Multicast Policy Name : <not set> [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 : 1100-1105

Sharing Type :  None  Primary  Isolated  Community

[Check Overlap](#) [OK](#) [Cancel](#)

31. Click OK and then click OK again.

### Create vNIC Templates

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

#### Create Management vNICs

To create the vNIC\_Mgmt\_A Template, follow these steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Click Policies > root.
3. Right-click vNIC Templates.
4. Click Create vNIC Template.
5. Enter vNIC\_Mgmt\_A for the vNIC template name.
6. Keep Fabric A selected.

7. Click 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 for the Template Type.

### Create vNIC Template

Name : vNIC\_Mgmt\_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

11. Under VLANs, check the boxes for IB-Mgmt and Native-VLAN VLANs.

12. Set Native-VLAN for the native VLAN.

13. Leave vNIC Name selected for the CDN Source.

14. Leave 1500 for the MTU.

15. In the MAC Pool list, choose MAC\_Pool\_A.

16. In the Network Control Policy list, choose Enable\_CDP.

### Create vNIC Template

Select	Name	Native VLAN	VLAN ID
<input type="checkbox"/>	default	<input type="radio"/>	1
<input checked="" type="checkbox"/>	IB-Mgmt	<input type="radio"/>	115
<input checked="" type="checkbox"/>	Native-VLAN	<input checked="" type="radio"/>	2
<input type="checkbox"/>	VM-APP-1100	<input type="radio"/>	1100
<input type="checkbox"/>	VM-APP-1101	<input type="radio"/>	1101
<input type="checkbox"/>	VM-APP-1102	<input type="radio"/>	1102

Create VLAN

CDN Source :  vNIC Name  User Defined

MTU :

MAC Pool :  ▼

QoS Policy :  ▼

Network Control Policy :  ▼

Pin Group :  ▼

Stats Threshold Policy :  ▼

**Connection Policies**

Dynamic vNIC  usNIC  VMQ

usNIC Connection Policy :  ▼

**OK** **Cancel**

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, click the LAN tab.
2. Click Policies > root.
3. Right-click vNIC Templates.
4. Click Create vNIC Template.
5. Enter vNIC\_Mgmt\_B for the vNIC template name.
6. Click Fabric B.

- Click Secondary Template for Redundancy Type.
- For the Peer Redundancy Template drop-down, click 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.

---

- Under Target, make sure the VM checkbox is not selected.

### Create vNIC Template

Name : vNIC\_Mgmt\_B

Description :

Fabric ID :  Fabric A  Fabric B  Enable Failover

**Redundancy**

Redundancy Type :  No Redundancy  Primary Template  Secondary Template

Peer Redundancy Template : vNIC\_Mgmt\_A ▼

**Target**

Adapter

VM

**Warning**

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

Template Type :  Initial Template  Updating Template

- In the MAC Pool list, click MAC\_Pool\_B.

### Create vNIC Template

SELECT	NAME	INDICATE VLAN	VLAN ID
<input type="checkbox"/>	default	<input type="radio"/>	1
<input type="checkbox"/>	IB-Mgmt	<input type="radio"/>	115
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>	2
<input type="checkbox"/>	VM-APP-1100	<input type="radio"/>	1100
<input type="checkbox"/>	VM-APP-1101	<input type="radio"/>	1101
<input type="checkbox"/>	VM-APP-1102	<input type="radio"/>	1102

Create VLAN

CDN Source :  vNIC Name  User Defined

MTU :

MAC Pool :  ▼

QoS Policy :  ▼

Network Control Policy :  ▼

Pin Group :  ▼

Stats Threshold Policy :  ▼

**Connection Policies**

Dynamic vNIC  usNIC  VMQ

usNIC Connection Policy :  ▼

**OK** **Cancel**

11. Click OK to create the vNIC template.

12. Click OK.

#### Create Data vNICs

To create the vNIC\_Data\_A Template, follow these steps:

1. In Cisco UCS Manager, click the LAN tab.
2. Click Policies > root.
3. Right-click vNIC Templates.
4. Click Create vNIC Template.
5. Enter vNIC\_Data\_A for 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 for the Template Type.

### 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"/>	...	<input type="radio"/>	...

11. Under VLANs, check the boxes vMotion, Apps, and Native-VLAN.
12. Set Native-VLAN for the native VLAN.
13. For MTU, enter 9000.
14. In the MAC Pool list, click MAC\_Pool\_A.

15. In the Network Control Policy list, choose Enable\_CDP.

Select	Name	Native VLAN	VLAN ID
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>	2
<input checked="" type="checkbox"/>	VM-APP-1100	<input type="radio"/>	1100
<input checked="" type="checkbox"/>	VM-APP-1101	<input type="radio"/>	1101
<input checked="" type="checkbox"/>	VM-APP-1102	<input type="radio"/>	1102
<input checked="" type="checkbox"/>	vMotion	<input type="radio"/>	1130

Create VLAN

CDN Source :  vNIC Name  User Defined

MTU :

MAC Pool :

QoS Policy :

Network Control Policy :

Pin Group :

Stats Threshold Policy :

**Connection Policies**

Dynamic vNIC  usNIC  VMQ

usNIC Connection Policy :

**OK** **Cancel**

16. Click OK to create the vNIC template.

17. Click OK.

For the vNIC\_Data\_B Template, follow these steps:

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

5. Enter vNIC\_Data\_B for the vNIC template name.
6. Click Fabric B.
7. Select Secondary Template for Redundancy Type.
8. For the Peer Redundancy Template drop-down, click vNIC\_Data\_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"/>	...	<input type="radio"/>	...

10. In the MAC Pool list, click MAC\_Pool\_B.



## Create vNIC Template

SELECT	NAME	INDICATE VLAN	VLAN ID
<input type="checkbox"/>	default	<input type="radio"/>	1
<input type="checkbox"/>	IB-Mgmt	<input type="radio"/>	115
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>	2
<input type="checkbox"/>	VM-APP-1100	<input type="radio"/>	1100
<input type="checkbox"/>	VM-APP-1101	<input type="radio"/>	1101
<input type="checkbox"/>	VM-APP-1102	<input type="radio"/>	1102

Create VLAN

CDN Source :  vNIC Name  User Defined

MTU :

MAC Pool :

QoS Policy :

Network Control Policy :

Pin Group :

Stats Threshold Policy :

**Connection Policies**

Dynamic vNIC  usNIC  VMQ

usNIC Connection Policy :

**OK** **Cancel**

11. Click OK to create the vNIC template.

12. Click OK.

### Create LAN Connectivity Policy

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

13. In Cisco UCS Manager, click LAN.

14. Click LAN > Policies > root.

15. Right-click LAN Connectivity Policies.

16. Click Create LAN Connectivity Policy.

17. Enter FC-LAN-Policy for the name of the policy.

Create LAN Connectivity Policy

Name :

Description :

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

Name	MAC Address	Native VLAN
No data available		

[-] Delete [+ Add] [Modify]

+ Add iSCSI vNICs

OK Cancel

18. Click the upper Add button to add a vNIC.

19. In the Create vNIC dialog box, enter 00-Mgmt-A for 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.

20. Check the box for Use vNIC Template.

21. In the vNIC Template list, choose 00-Mgmt-A.

22. In the Adapter Policy list, click VMWare.

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

Create vNIC

Name : 00-Mgmt-A

Use vNIC Template :

Redundancy Pair :

vNIC Template : vNIC\_Mgmt\_A

Peer Name :

Create vNIC Template

---

Adapter Performance Profile

Adapter Policy : VMWare

Create Ethernet Adapter Policy

OK Cancel

24. Click the upper Add button to add another vNIC to the policy.
25. In the Create vNIC box, enter 01-Mgmt-B for the name of the vNIC.
26. Check the box for Use vNIC Template.
27. In the vNIC Template list, click 01-Mgmt-B.
28. In the Adapter Policy list, click VMWare.

Create vNIC

Name : 01-Mgmt-B

Use vNIC Template :

Redundancy Pair :

vNIC Template : vNIC\_Mgmt\_B ▼

Peer Name :

Create vNIC Template

---

**Adapter Performance Profile**

Adapter Policy : VMWare ▼

Create Ethernet Adapter Policy

OK Cancel

29. Click OK to add the vNIC to the policy.
30. Click the upper Add button to add a vNIC.
31. In the Create vNIC dialog box, enter 02-Data-A for the name of the vNIC.
32. Check the box for Use vNIC Template.
33. In the vNIC Template list, click vNIC\_Data\_A.
34. In the Adapter Policy list, click VMWare.
35. Click OK to add this vNIC to the policy.

**Create vNIC**

Name :

Use vNIC Template :

Redundancy Pair :

Peer Name :

vNIC Template :

[Create vNIC Template](#)

---

**Adapter Performance Profile**

Adapter Policy :

[Create Ethernet Adapter Policy](#)

**OK** **Cancel**

36. Click Add to add a vNIC to the policy.
37. In the Create vNIC dialog box, enter 03-Data-B for the name of the vNIC.
38. Check the box for Use vNIC Template.
39. In the vNIC Template list, click vNIC\_Data\_B.
40. In the Adapter Policy list, click VMWare.

**Create vNIC**

Name : 03\_Data\_B

Use vNIC Template :

Redundancy Pair :

vNIC Template : vNIC\_Data\_B ▼

Peer Name :

Create vNIC Template

---

**Adapter Performance Profile**

Adapter Policy : VMWare ▼

Create Ethernet Adapter Policy

OK Cancel

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

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

### Configure FC SAN Connectivity

This section details the Fibre Channel configuration steps that will enable you to provision the volumes for FlashStack that are 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.

- Click Equipment > Fabric Interconnects > Fabric Interconnect A (primary).
- Click Configure Unified Ports.
- 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.
- Within the Configured Fixed Ports pop-up window move the gray slider bar from the left to the right to choose 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

- Click OK to continue.
- Click Equipment > Fabric Interconnects > Fabric Interconnect B (primary).
- Click Configure Unified Ports.
- 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.
- Within the Configured Fixed Ports pop-up window move the gray slider bar from the left to the right to choose either 4 or 8 ports to be set as FC Uplinks.
- Click OK to continue.



---

The Fabric Interconnects will reboot, reconnect to 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. Click SAN > SAN Cloud.
3. Right-click VSANs.
4. Click Create VSAN.
5. Enter VSAN\_A for the name of the VSAN to be used for Fabric A.
6. Leave Disabled selected for FC Zoning.
7. Click 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 ? ×

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

Enter the VSAN ID that maps to this VSAN. Enter the VLAN ID that maps to this VSAN.

VSAN ID :  FCoE VLAN :

9. Click OK and then click OK again.
10. Under SAN Cloud, right-click VSANs.
11. Click Create VSAN.
12. Enter VSAN\_B for the name of the VSAN to be used for Fabric B.
13. Leave Disabled selected for FC Zoning.
14. Click 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 ? ×

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

Enter the VSAN ID that maps to this VSAN. Enter the VLAN ID that maps to this VSAN.

VSAN ID :  FCoE VLAN :

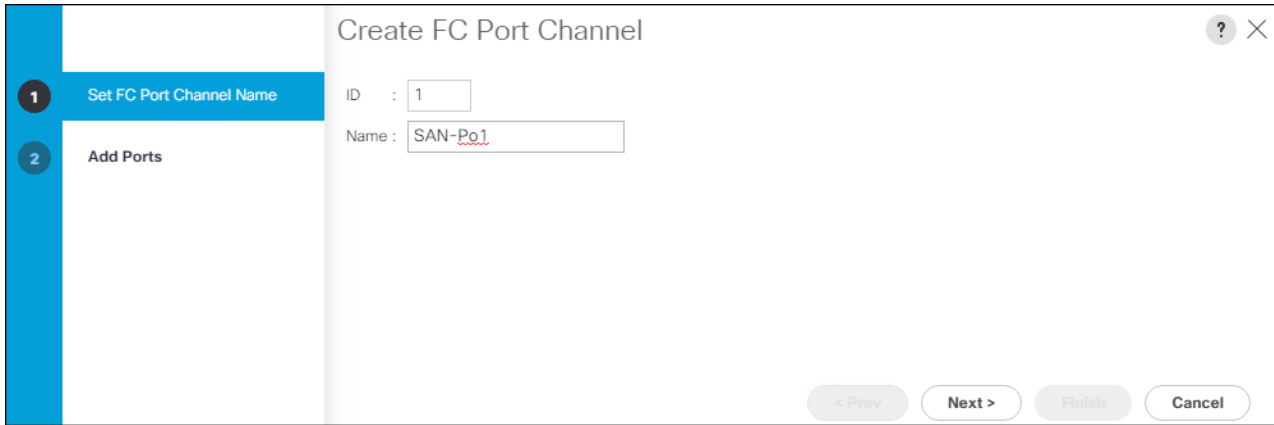
16. Click OK and then click OK again.

### Create FC Port Channels

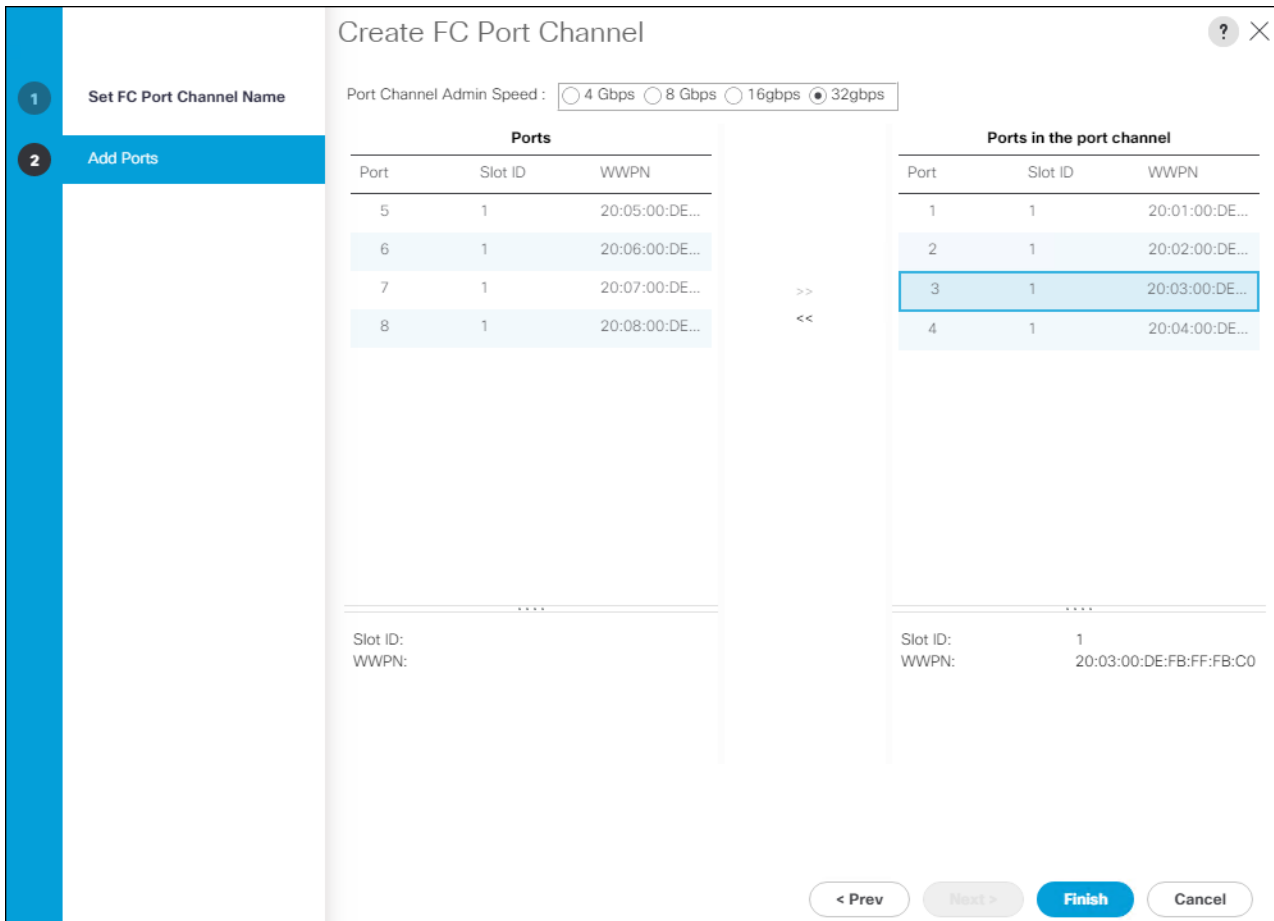
To configure the necessary port channels for the Cisco UCS environment, follow these steps:

#### Fabric A

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



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

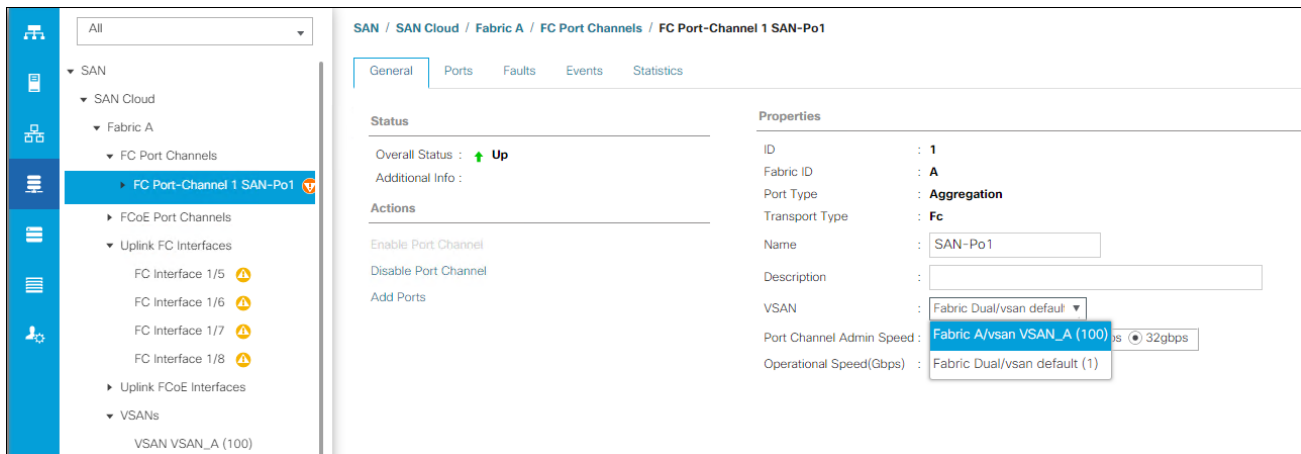


6. Click Finish.

7. Click OK.

8. Click the newly created Port-Channel.

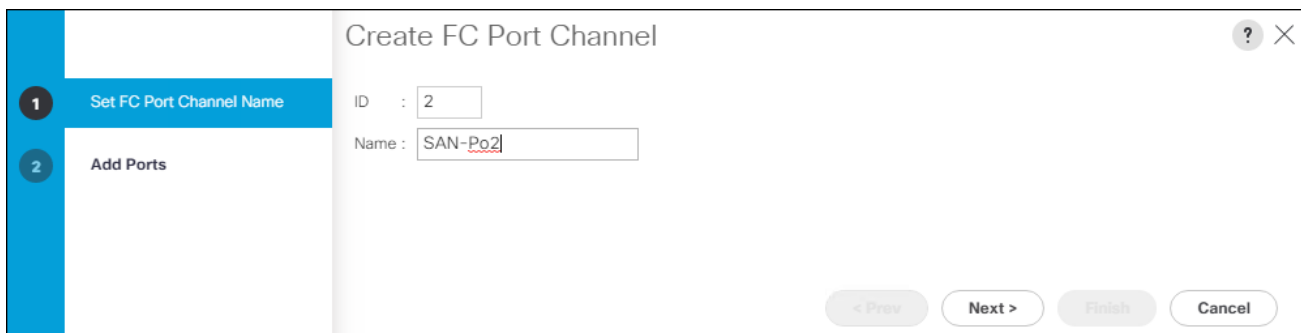
9. From the VSAN drop-down list for Port-Channel SAN-Po1, choose VSAN\_A(100).



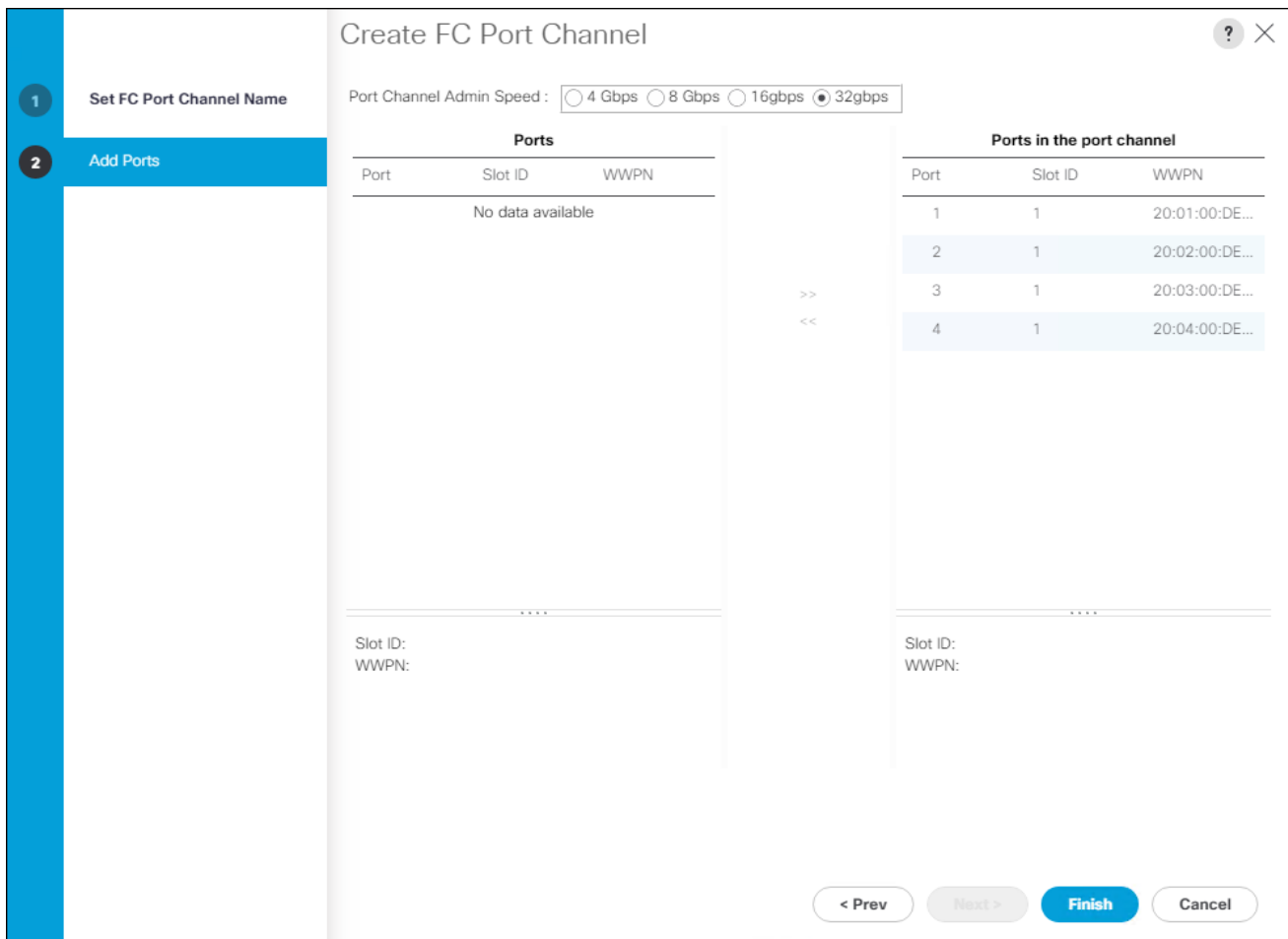
10. Click Save Changes and then click OK.

### Fabric B

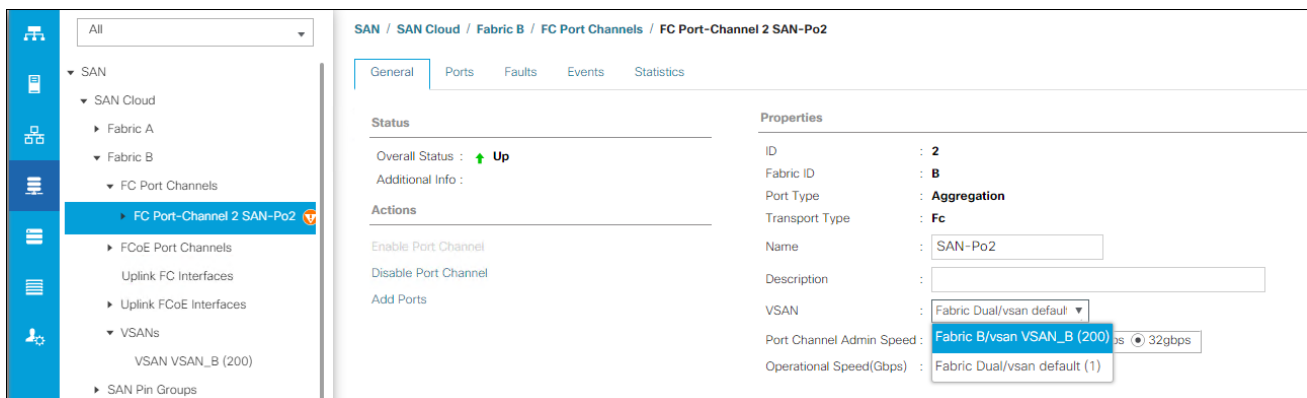
1. In the navigation pane under SAN > SAN Cloud expand the Fabric B tree.
2. Right-click FC Port Channels.
3. Click Create Port Channel.
4. Enter 2 for the ID and SAN-Po2 for the Port Channel name.



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



6. Click Finish.
7. Click OK.
8. Click the newly created Port-Channel.
9. Under the VSAN drop-down for Port-Channel SAN-Po2, choose VSAN\_B(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.
2. Click Policies > root.
3. Right-click vHBA Templates.
4. Click Create vHBA Template.
5. Enter vHBA\_Template\_A for the vHBA template name.
6. Keep Fabric A selected.
7. Leave Redundancy Type as No Redundancy.
8. Click VSAN\_A.
9. Leave Initial Template for the Template Type.
10. Click WWPN\_Pool\_A for the WWPN Pool.
11. Click OK to create the vHBA template.

## Create vHBA Template

Name : vHBA\_Template\_A

Description :

Fabric ID :  A  B

**Redundancy**

---

Redundancy Type :  No Redundancy  Primary Template  Secondary Template

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

Template Type :  Initial Template  Updating Template

Max Data Field Size : 2048

WWPN Pool : WWPN\_Pool\_A(32/32)

QoS Policy : <not set>

Pin Group : <not set>

Stats Threshold Policy : default

**OK** **Cancel**

12. Click OK.
13. Right-click vHBA Templates.
14. Click Create vHBA Template.
15. Enter vHBA\_Template\_B for the vHBA template name.
16. Click Fabric B.
17. Leave Redundancy Type as No Redundancy.
18. Click VSAN\_B.
19. Leave Initial Template for the Template Type.
20. Click WWPN\_Pool\_B for the WWPN Pool.
21. Click OK to create the vHBA template.

## Create vHBA Template

Name : vHBA\_Template\_B

Description :

Fabric ID :  A  B

**Redundancy**

Redundancy Type :  No Redundancy  Primary Template  Secondary Template

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

Template Type :  Initial Template  Updating Template

Max Data Field Size : 2048

WWPN Pool : WWPN\_Pool\_B(32/32)

QoS Policy : <not set>

Pin Group : <not set>

Stats Threshold Policy : default

**OK** **Cancel**

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. Click SAN > Policies > root.
3. Right-click SAN Connectivity Policies.
4. Click Create SAN Connectivity Policy.
5. Enter Infra\_SAN\_Policy for the name of the policy.
6. Select the previously created WWNN\_Pool for the WWNN Assignment.
7. Click Add to add a vHBA.



8. In the Create vHBA dialog box, enter Fabric\_A for the name of the vHBA.
9. Check the box for Use vHBA Template.
10. Leave Redundancy Pair unselected.
11. In the vHBA Template list, choose vHBA\_Template\_A.

**Create vHBA** [?] [X]

Name :

Use vHBA Template :

Redundancy Pair :

Peer Name :

vHBA Template :  [Create vHBA Template](#)

---

**Adapter Performance Profile**

Adapter Policy :  [Create Fibre Channel Adapter Policy](#)

**OK** **Cancel**

12. In the Adapter Policy list, choose VMWare.
13. Click OK.
14. Click Add to add a second vHBA.
15. In the Create vHBA dialog box, enter Fabric\_B for the name of the vHBA.
16. Check the box for Use vHBA Template.
17. Leave Redundancy Pair unselected.

18. In the vHBA Template list, choose vHBA\_Template\_B.

Create vHBA

Name : Fabric\_B

Use vHBA Template :

Redundancy Pair :

Peer Name :

vHBA Template : vHBA\_Template\_B ▼

Adapter Performance Profile

Adapter Policy : VMWare ▼

Create vHBA Template

Create Fibre Channel Adapter Policy

OK Cancel

19. In the Adapter Policy list, choose 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

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 are 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.

**Health** Search  ! 2 x 7

Hardware Alerts Connections Apps

Host Connections All Paths 1-8 of 8 < > ⋮

Host  Paths # WWN # IQN

Array Ports ⋮

Port	Name	Speed	Failover	Port	Name	Speed	Failover
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	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	-	-	-

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 listed in the table below, these appear as the first ports of each controller.

	Port Name	Target Role	Example WWPN	Customer WWPN
FlashArray//X Controller 0	CT0.FC0	Primary	52:4A:93:7C:2B:9B:9F:00	
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 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.
2. Click Policies > root.
3. Right-click Boot Policies.
4. Click Create Boot Policy.
5. Enter Boot-FC-A for the name of the boot policy.
6. Optional: Enter a description for the boot policy.
7. Set boot Mode to Uefi.



**Do not check the box for Reboot on Boot Order Change.**

---

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

**Add SAN Boot** ? X

vHBA :

Type :  Primary  Secondary  Any

**OK** **Cancel**

12. Click OK to add the SAN boot initiator.
13. From the vHBA drop-down list, choose Add SAN Boot Target.
14. Enter 1 for the value for Boot Target LUN.
15. Enter the WWPN for CT0.FC0.
16. Choose Primary for the SAN boot target type.

**Add SAN Boot Target** ? X

Boot Target LUN :

Boot Target WWPN :

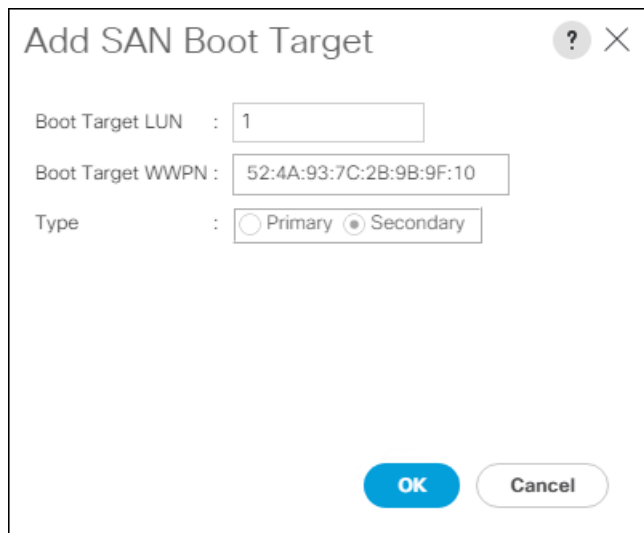
Type :  Primary  Secondary

**OK** **Cancel**

17. Click OK to add the SAN boot target.
18. From the vHBA drop-down list, choose Add SAN Boot Target.

19. Enter 1 for the value for Boot Target LUN.

20. Enter the WWPN for CT1.FC0.



Add SAN Boot Target

Boot Target LUN : 1

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

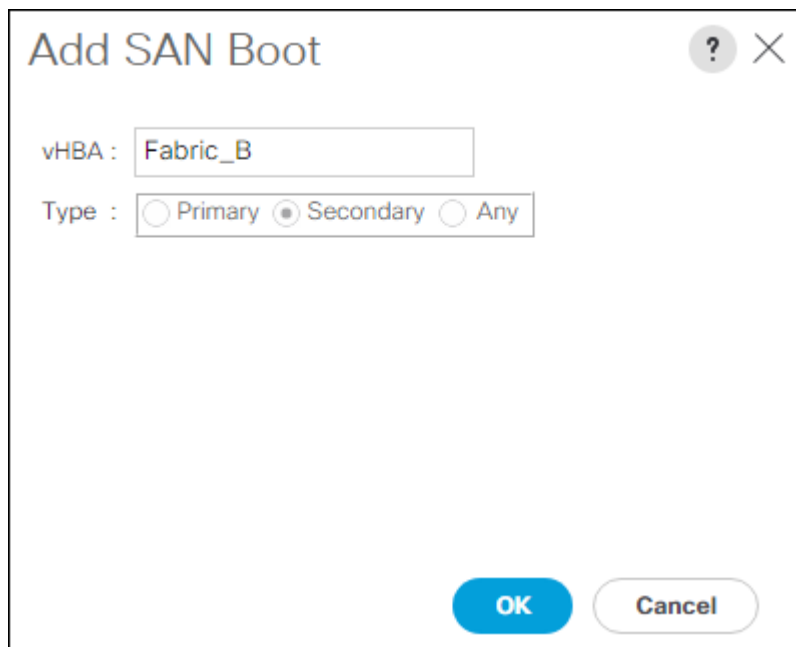
Type :  Primary  Secondary

OK Cancel

21. Click OK to add the SAN boot target.

22. From the vHBA drop-down list, choose Add SAN Boot.

23. In the Add SAN Boot dialog box, enter Fabric\_B in the vHBA box.



Add SAN Boot

vHBA : Fabric\_B

Type :  Primary  Secondary  Any

OK Cancel

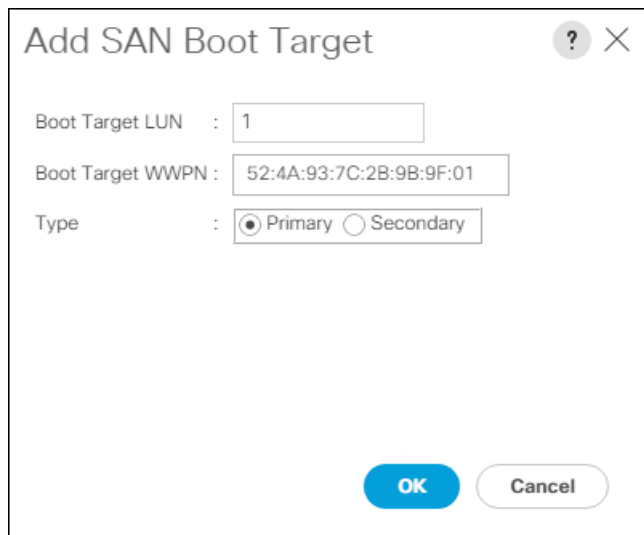
24. Click OK to add the SAN boot initiator.

25. From the vHBA drop-down list, choose Add SAN Boot Target.

26. Enter 1 for the value for Boot Target LUN.

27. Enter the WWPN for CT0.FC1.

28. Choose Primary for the SAN boot target type.



Add SAN Boot Target

Boot Target LUN : 1

Boot Target WWPN : 52:4A:93:7C:2B:9B:9F:01

Type :  Primary  Secondary

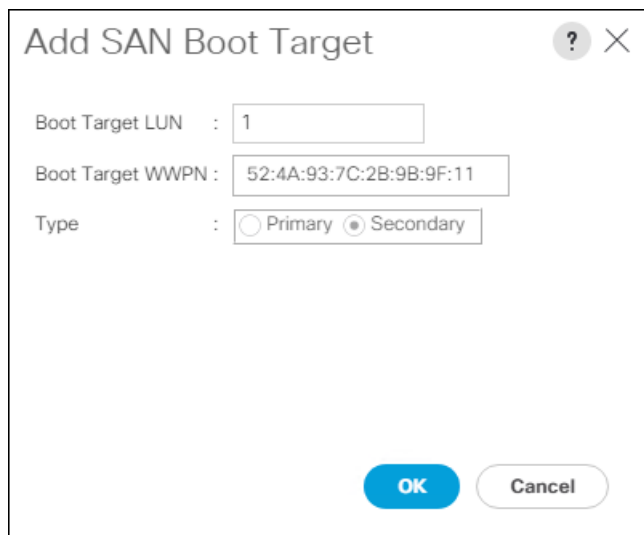
OK Cancel

29. Click OK to add the SAN boot target.

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

31. Enter 1 for the value for Boot Target LUN.

32. Enter the WWPN for CT1.FC1.



Add SAN Boot Target

Boot Target LUN : 1

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

Type :  Primary  Secondary

OK Cancel

33. Click OK to add the SAN boot target.



34. Expand CIMC Mounted Media and click Add CIMC Mounted CD/DVD.

**Create Boot Policy**

Name :

Description :

Reboot on Boot Order Change :

Enforce vNIC/vHBA/iSCSI Name :

Boot Mode :  Legacy  Uefi

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

**Boot Order**

Name	Order	vNIC/v...	Type	LUN N...	WWN	Slot N...	Boot N...	Boot P...	Descri...
SAN Target ...	1		Primary	1	52:4A:...				
SAN Target ...	1		Secon...	1	52:4A:...				
SAN Secondary		Fabric...	Secon...						
SAN Target ...	1		Primary	1	52:4A:...				
SAN Target ...	1		Secon...	1	52:4A:...				
CIMC Mounted C...	2								

↑ Move Up ↓ Move Down Delete

Set Uefi Boot Parameters

OK Cancel

35. 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.
2. Click Service Profile Templates > root.
3. Right-click root.
4. Click Create Service Profile Template to open the Create Service Profile Template wizard.

5. Enter VM-AMD-Host-FC-A for the name of the service profile template. This service profile template is configured to boot from FlashArray//X50 R3 controller 1 on fabric A.
6. Click Updating Template.
7. Under UUID, select UUID\_Pool for the UUID pool.

The screenshot shows a web-based wizard titled "Create Service Profile Template". On the left is a vertical navigation menu with 11 steps, where step 1, "Identify Service Profile Template", is highlighted. The main content area contains the following fields and instructions:

- Name:** A text input field containing "VM-AMD-Host-FC-A". Below it, text reads: "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:** Radio buttons for "Initial Template" and "Updating Template", with "Updating Template" selected.
- UUID:** A dropdown menu labeled "UUID Assignment:" with "UUID\_Pool(32/32)" selected. Below it, text reads: "The UUID will be assigned from the selected pool. The available/total UUIDs are displayed after the pool name."
- Description:** A text area with the instruction: "Optionally enter a description for the profile. The description can contain information about when and where the service profile should be used." The text area is currently empty.

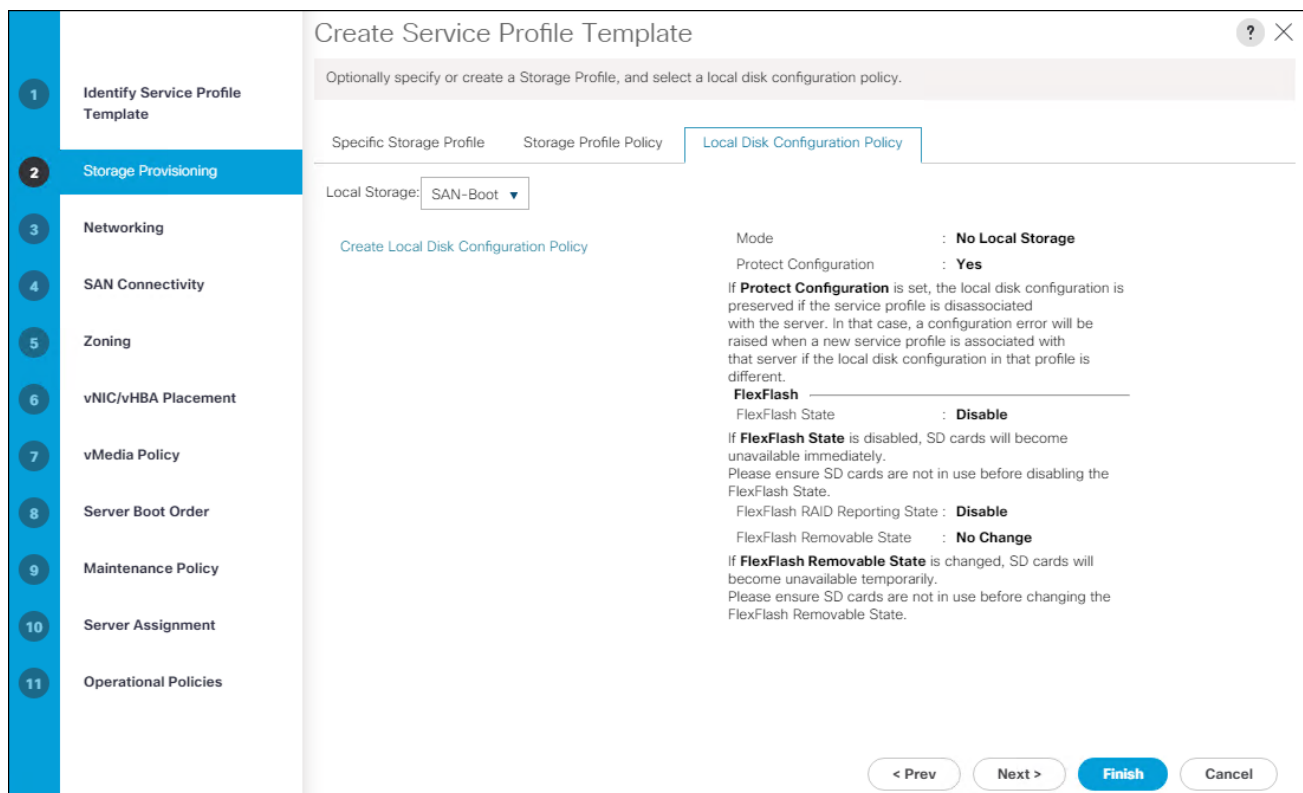
At the bottom right, there are four buttons: "< Prev", "Next >", "Finish" (highlighted in blue), and "Cancel".

8. Click Next.

### Configure Storage Provisioning

To configure the storage provisioning, follow these steps:

1. Click the 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. Choose the "Use Connectivity Policy" option to configure the LAN connectivity.
3. Click FC-LAN-Policy from the LAN Connectivity Policy drop-down list.

**Create Service Profile Template**

Optionally specify LAN configuration information.

Dynamic vNIC Connection Policy:

[Create Dynamic vNIC Connection Policy](#)

---

How would you like to configure LAN connectivity?

Simple
  Expert
  No vNICs
  Use Connectivity Policy

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

Initiator Name

Initiator Name Assignment:

[Create IQN Suffix Pool](#)

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

< Prev    Next >    **Finish**    Cancel

4. Click Next.

### Configure SAN Connectivity Options

To configure the SAN connectivity options, follow these steps:

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

**Create Service Profile Template** ? X

Optionally specify disk policies and SAN configuration information.

How would you like to configure SAN connectivity?

Simple  Expert  No vHBAs  Use Connectivity Policy

SAN Connectivity Policy :  [Create SAN Connectivity Policy](#)

< Prev   Next >   **Finish**   Cancel

### Configure Zoning Options

1. Leave Zoning configuration unspecified and click Next.

### Configure vNIC/HBA Placement

1. From the Select Placement drop-down 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. Click Boot-FC-A for Boot Policy.

**Create Service Profile Template**

Optionally specify the boot policy for this service profile template.

Select a boot policy.

Boot Policy:  [Create Boot Policy](#)

Name : **Boot-FC-A**  
 Description :  
 Reboot on Boot Order Change : **No**  
 Enforce vNIC/vHBA/iSCSI Name : **Yes**  
 Boot Mode : **Uefi**  
 Boot Security : **No**

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

**Boot Order**

+ - Advanced Filter Export Print

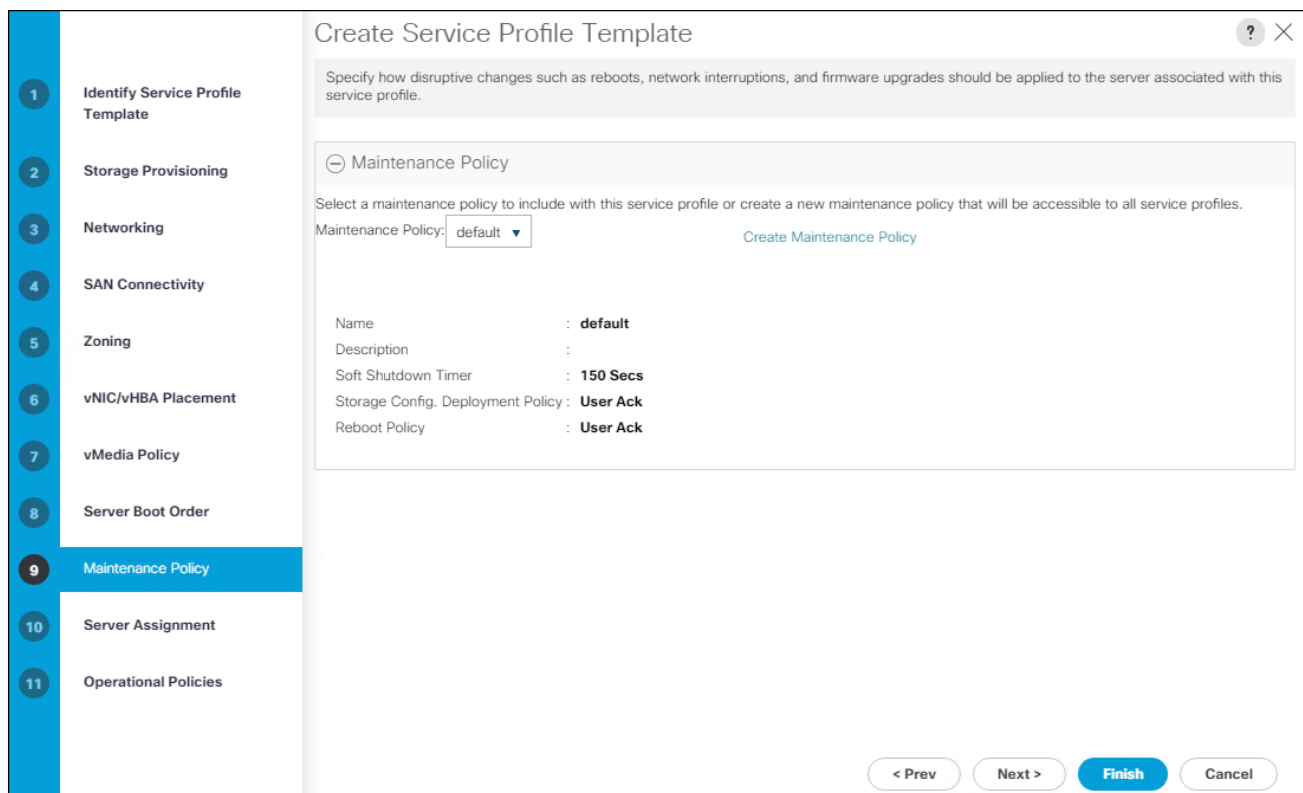
Name	Order	vNIC/vHB...	Type	LUN Name	WWN	Slot Num...	Boot Name	Boot Path	Description
Remot...	1								
San	2								

< Prev    Next >    **Finish**    Cancel

2. Click Next to continue to the next section.

### Configure Maintenance Policy

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 AMD\_Pool
2. Optional: Select a Server Pool Qualification policy.
3. Select Down for the power state to be applied when the profile is associated with the server.
4. Optional: Select “UCS-C125-M5” 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 AMD-VM-Host.
2. Expand Power Control Policy Configuration and select No-Power-Cap in the Power Control Policy list.



**Create Service Profile Template**

Optionally specify information that affects how the system operates.

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

+ External IPMI/Redfish Management Configuration

+ Management IP Address

+ Monitoring Configuration (Thresholds)

⊖ Power Control Policy Configuration  
Power control policy determines power allocation for a server in a given power group.  
Power Control Policy :  [Create Power Control Policy](#)

+ Scrub Policy

+ KVM Management Policy

+ Graphics Card Policy

< Prev   Next >   **Finish**   Cancel

3. Click Finish to create the service profile template.

4. Click OK in the confirmation message.

## Create Service Profiles

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

1. Connect to the UCS 6454 Fabric Interconnect UCS Manager, click the Servers tab in the navigation pane.
2. Click Service Profile Templates > root > Service Template VM-Host-FC-A.
3. Right-click VM-AMD-Host-FC-A and select Create Service Profiles from Template.
4. Enter VM-AMD-Host-FC- for the service profile prefix.
5. Leave 1 as “Name Suffix Starting Number.”
6. Leave 2 for the “Number of Instances.”
7. Click OK to create the service profiles.

## Create Service Profiles From Template ? X

Naming Prefix :

Name Suffix Starting Number :

Number of Instances :

OK
Cancel

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

### Claim UCS Domain in Intersight

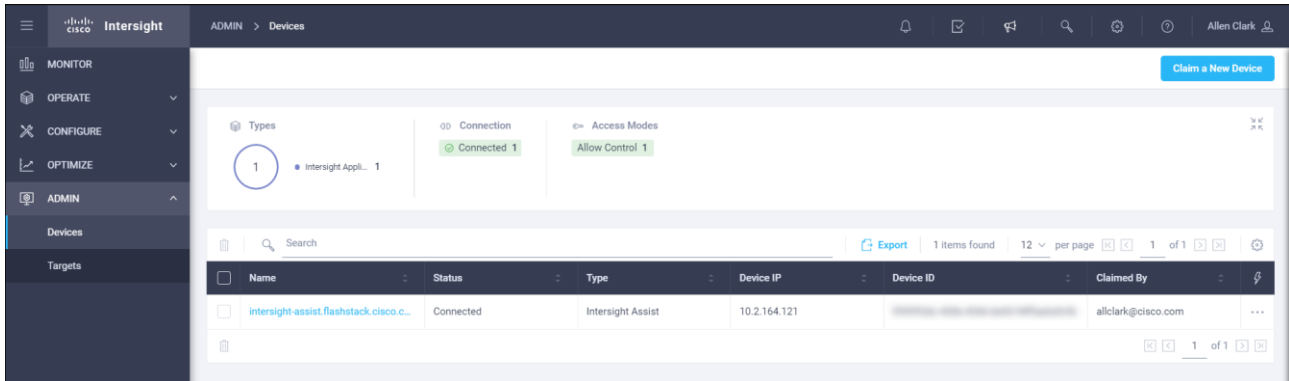
To claim a UCS domain in Intersight, follow these steps:

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

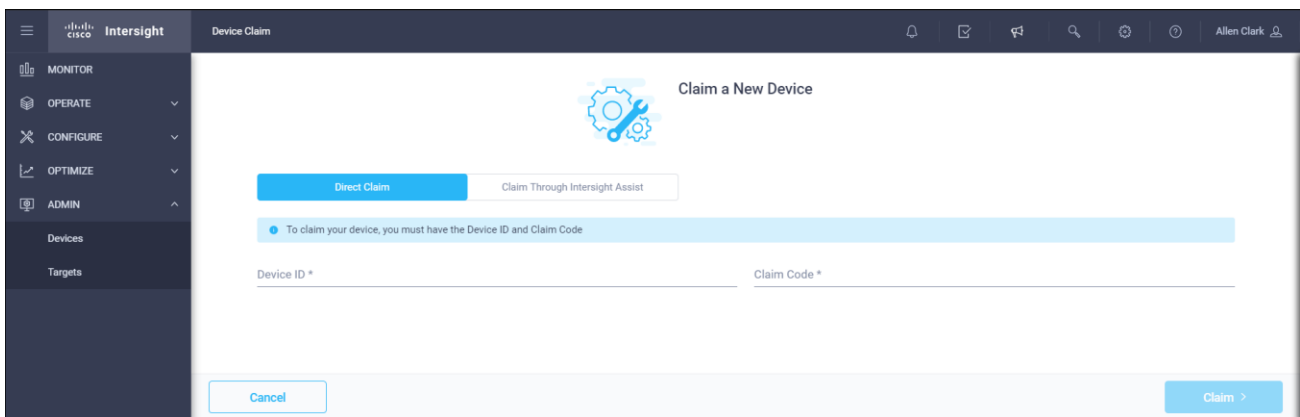
The screenshot displays the 'Device Connector' interface in Cisco Intersight. At the top, there's a navigation menu with 'Device Connector' selected. The main content area shows a status of 'Not Claimed' with a yellow warning banner. Below this, a diagram illustrates the connection path: Device Connector (represented by a monitor icon) connects to the Internet (represented by a globe icon), which then connects to Intersight (represented by a cloud icon). A yellow triangle with an exclamation mark is placed between the Internet and Intersight icons, indicating a connection issue. To the right of the diagram, the 'Device ID' is 'FD023450Q4C&FD023450Q8B' and the 'Claim Code' is 'F84CA25659F9'. The page also includes 'Settings' and 'Refresh' buttons. At the bottom, there's a version number '1.0.9-3286'.

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

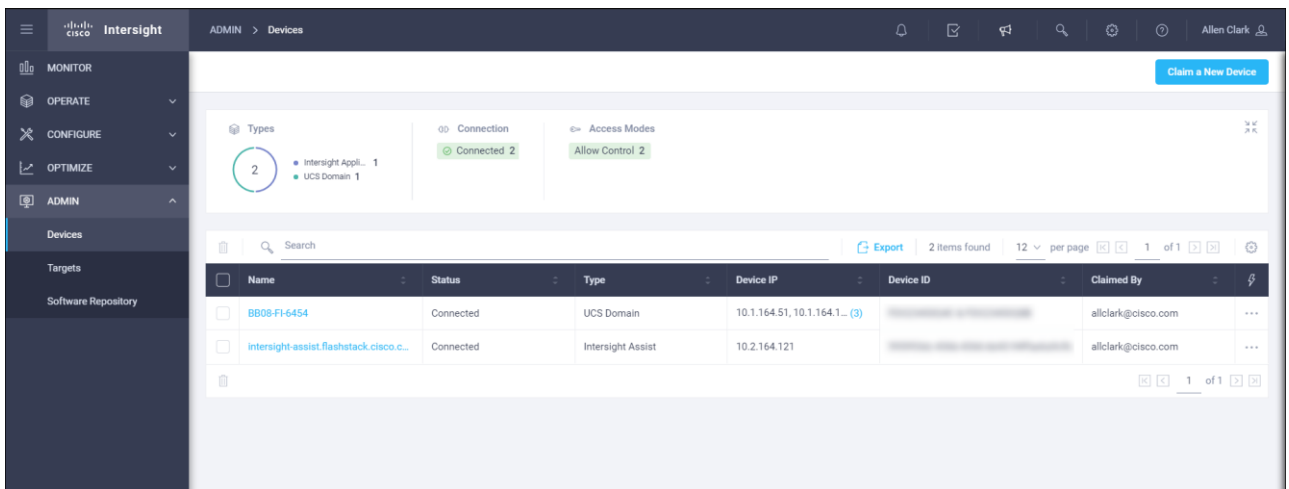
6. Click Admin > Devices.



7. Click Claim a New Device and enter your Device ID and Claim Code under the Direct Claim option.

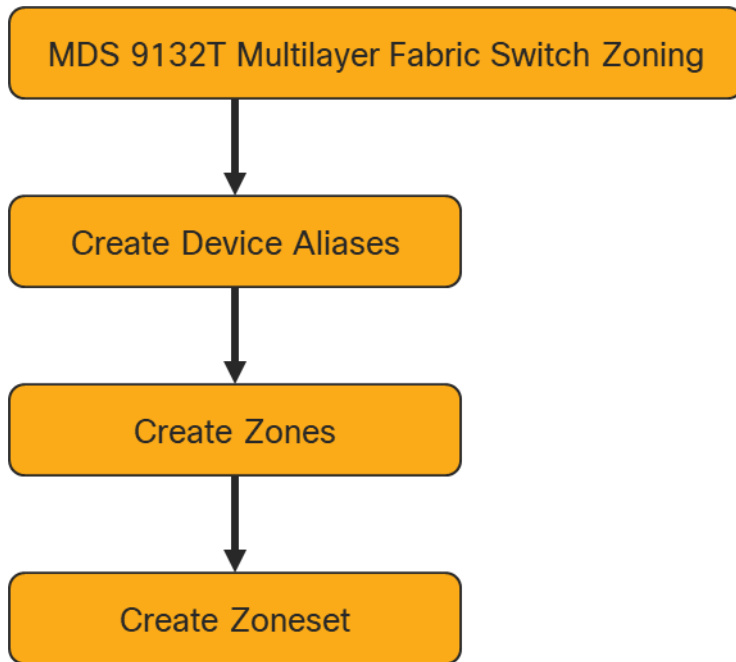


8. Click Claim.



## MDS Fabric Zoning

This section continues the configuration process of the Cisco MDS 9148S 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 will be:

```
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:10	52:4a:93:7c:2b:9b:9f:10
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

2. Match these values to their sources from the Purity command line output gained from a ssh connection to the FlashArray using the pureuser account:

```
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	-	-	-

3. Match these values 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-AMD-Host...

General Storage Network iSCSI vNICs vMedia Policy Boot Order Virtual Machines FC Zones Policies Server Details CIMC Sessions F>

Storage Profiles Local Disk Configuration Policy vHBAs vHBA Initiator Groups

Reset WWNN Address 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 Place...	Actual Placem...	Admin Host Port	Actual Host Port
vHBA Fabri...	20:00:00:25:B5:01:0A:00	1	5	A	Any	1	ANY	NONE
vHBA Fabri...	20:00:00:25:B5:01:0B:00	2	6	B	Any	1	ANY	NONE

4. Record the values to be used for zoning and host mapping:

	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-AMD-Host-FC-01-A	Port-Channel 100	20:00:00:25:b5:01:0a:00	
VM-AMD-Host-FC-02-A	Port-Channel 100	20:00:00:25:b5:01:0a:01	

5. Create device alias database entries for each of the PWWNs mapping them to their human readable source names on MDS-9132T-A:

```
conf t
device-alias database
device-alias name FlashArray-CT0FC0 pwn 52:4A:93:7C:2B:9B:9F:00
device-alias name FlashArray-CT1FC0 pwn 52:4A:93:7C:2B:9B:9F:10
device-alias name FlashArray-CT0FC2 pwn 52:4A:93:7C:2B:9B:9F:02
device-alias name FlashArray-CT1FC2 pwn 52:4A:93:7C:2B:9B:9F:12
device-alias name VM-Host-FC-01-A pwn 20:00:00:25:b5:01:0a:00
device-alias name VM-Host-FC-02-A pwn 20:00:00:25:b5:01:0a:01
device-alias commit
```

6. 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-B this will be:

```
show flogi database
```

INTERFACE	VSAN	FCID	PORT NAME	NODE NAME
fc1/15	200	0xa00000	52:4a:93:7c:2b:9b:9f:01	52:4a:93:7c:2b:9b:9f:01
fc1/16	200	0xa00020	52:4a:93:7c:2b:9b:9f:11	52:4a:93:7c:2b:9b:9f:11
fc1/17	200	0xa00040	52:4a:93:7c:2b:9b:9f:03	52:4a:93:7c:2b:9b:9f:03
fc1/18	200	0xa00040	52:4a:93:7c:2b:9b:9f:13	52:4a:93:7c:2b:9b:9f:13
port-channel200	200	0xa00060	24:01:00:de:fb:ff:fb:c0	20:64:00:de:fb:ff:fb:c1
port-channel200	200	0xa00061	20:00:00:25:b5:01:0b:00	20:00:00:25:b5:01:00:00
port-channel200	200	0xa00062	20:00:00:25:b5:01:0b:01	20:00:00:25:b5:01:00:01

7. Record the values to be used for zoning and host mapping:

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	
6454-B	Port-Channel 100	24:01:00:de:fb:ff:fb:c0	
VM-AMD-Host-FC-01-B	Port-Channel 100	20:00:00:25:b5:01:0b:00	
VM-AMD-Host-FC-02-B	Port-Channel 100	20:00:00:25:b5:01:0b:01	

8. Create device alias database entries for each of the PWWNs mapping them to their human readable source names on MDS-9132T-B:

```
conf t
device-alias database
device-alias name FlashArray-CT0FC1 pwn 52:4A:93:7C:2B:9B:9F:01
device-alias name FlashArray-CT1FC1 pwn 52:4A:93:7C:2B:9B:9F:11
device-alias name FlashArray-CT0FC3 pwn 52:4A:93:7C:2B:9B:9F:03
device-alias name FlashArray-CT1FC3 pwn 52:4A:93:7C:2B:9B:9F:13
device-alias name VM-Host-FC-01-B pwn 20:00:00:25:b5:01:0b:00
device-alias name VM-Host-FC-02-B pwn 20:00:00:25:b5:01:0b:01
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-AMD-Host-FC-01 on MDS A

```
conf t
zone name VM-Host-FC-01-A vsan 100
member device-alias VM-Host-FC-01-A init
member device-alias FlashArray-CT0FC0 target
member device-alias FlashArray-CT0FC2 target
member device-alias FlashArray-CT1FC0 target
member device-alias FlashArray-CT1FC2 target
```

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

```
conf t
zone name VM-Host-FC-02-A vsan 100
member device-alias VM-Host-FC-02-A init
member device-alias FlashArray-CT0FC0 target
member device-alias FlashArray-CT0FC2 target
member device-alias FlashArray-CT1FC0 target
member device-alias FlashArray-CT1FC2 target
```

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

```
conf t
zone name VM-Host-FC-01-B vsan 200
member device-alias VM-Host-FC-01-B init
member device-alias FlashArray-CT0FC1 target
member device-alias FlashArray-CT0FC3 target
member device-alias FlashArray-CT1FC1 target
member device-alias FlashArray-CT1FC3 target
```

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

```
conf t
zone name VM-Host-FC-02-B vsan 200
member device-alias VM-Host-FC-02-B init
member device-alias FlashArray-CT0FC1 target
member device-alias FlashArray-CT0FC3 target
member device-alias FlashArray-CT1FC1 target
member device-alias FlashArray-CT1FC3 target
```

## Create and Activate Zoneset

Add the zones to a zoneset on each MDS switch:

### Zoneset for MDS A

```
conf t
zoneset name FlashStack-Zoneset-A vsan 100
member VM-Host-FC-01-A
member VM-Host-FC-02-A
zoneset activate name FlashStack-Zoneset-A vsan 100
zone commit vsan 100
copy run start
```

---

## Zoneset for MDS B

```
conf t
zoneset name FlashStack-Zoneset-B vsan 200
member VM-Host-FC-01-A
member VM-Host-FC-02-A
zoneset activate name FlashStack-Zoneset-B vsan 200
zone commit vsan 200
copy run start
```



## FlashArray Storage Deployment

The Pure Storage FlashArray//X is accessible to the FlashStack.

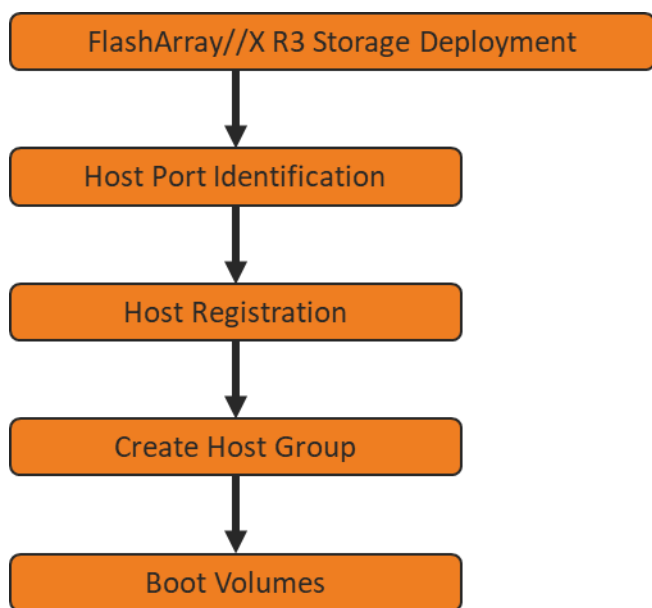


No storage has been deployed at this point in the process.

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 Plugin has later been registered with the vCenter.



### Host Port Identification

FC Boot LUNs will be mapped by the FlashArray//X using the assigned Initiator PWWN to the provisioned service profiles. This information can be found within the service profile.

### Host Registration

To create a host, follow these steps:

1. Selection Configure -> Orchestration.
2. Click New Storage Host.

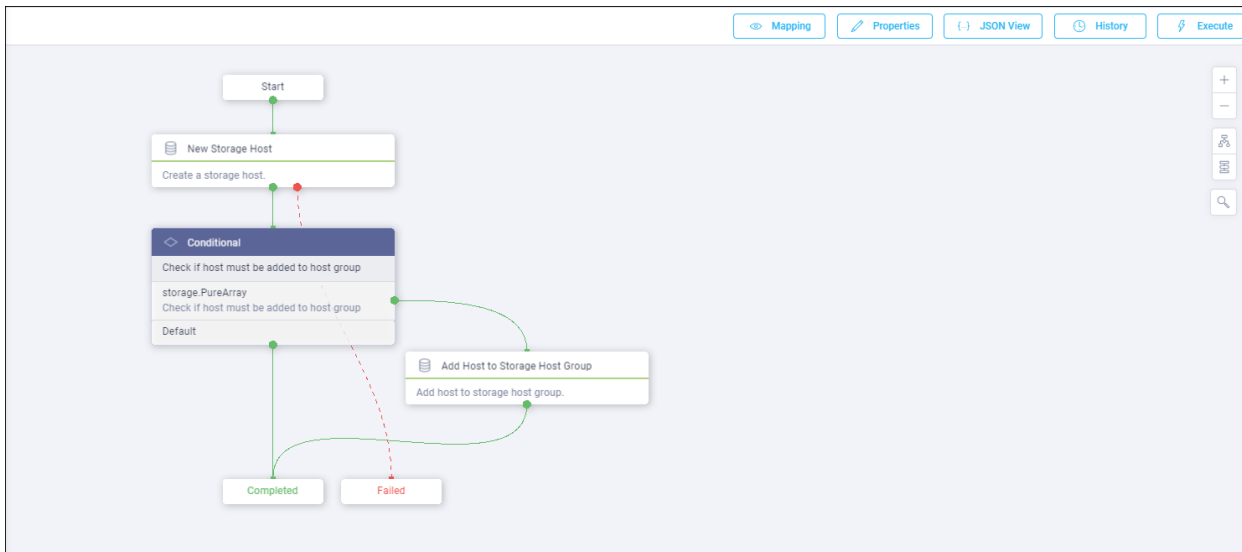
Intersight CONFIGURE > Orchestration

Workflows Data Types

9 items found 10 per page 1 of 1

Name	Description	Default Version	Executions	Last Execution Status	Validation Infor
Update VMFS Datastore	Expand a datastore on hypervisor manager by extending the backing storage volume to specified capacity, and then gro...		2 1		
Update Storage Host	Update the storage host details. If the inputs for a task are provided then the task is run, else it is skipped.		1 0		
Remove VMFS Datastore	Remove VMFS datastore and remove the backing volume from the storage device.		3 0		
Remove Storage Host ...	Remove storage host group. If hosts are provided as input, the workflow will remove the hosts from the host group.		1 0		
Remove Storage Host	Remove storage host. If host group name is provided as input, the workflow will also remove the host from the host gro...		1 1		
New VMFS Datastore	Create a storage volume and build VMFS datastore on the volume.		3 1		
New Virtual Machine	Create a new virtual machine on the hypervisor from an OVA or OVF file. Datastore, Host/Cluster, and Image URL fields ...		1 0		
New Storage Host Group	Create a new storage host group. If hosts are provided as inputs, the workflow will add the hosts to the host group.		1 1		
New Storage Host	Create a new storage host. If host group is provided as input, then the host will be added to the host group.		1 2		

3. Click Execute.



4. Click the appropriate Organization (default by default).

5. Click the appropriate Pure Storage device.

6. Enter the name of the Host name and WWNs for host VM-AMD-Host-FC-01.

## Enter Workflow Input - New Storage Host



Organization \*

FlashStack-BB



Workflow Instance Name

New Storage Host



Storage Device \*

BB08-FlashArrayR3 Pure Storage



Host Group



Host \*

VM-AMD-Host-FC-01



WWNs

20:00:00:25:b5:01:0A:00



WWNs

20:00:00:25:b5:01:0B:00



IQNs



Cancel

Execute

7. Click Execute.
8. Repeat steps 2-7 for all host.

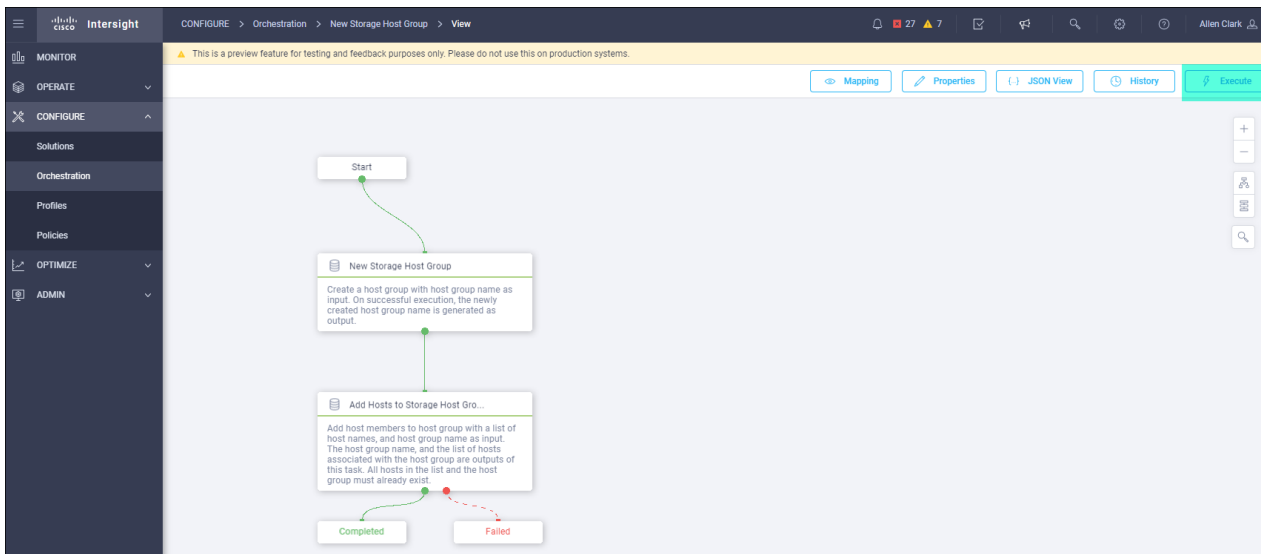
## Create Host Group

To create a host group, follow these steps:

1. Selection Configure -> Orchestration.
2. Click New Storage Host Group.

Name	Description	Default Version	Executions	Last Execution Status	Validation Infor
Update VMFS Datastore	Expand a datastore on hypervisor manager by extending the backing storage volume to specified capacity, and then gro...	2	1		
Update Storage Host	Update the storage host details. If the inputs for a task are provided then the task is run, else it is skipped.	1	0		
Remove VMFS Datastore	Remove VMFS datastore and remove the backing volume from the storage device.	3	0		
Remove Storage Host ...	Remove storage host group. If hosts are provided as input, the workflow will remove the hosts from the host group.	1	0		
Remove Storage Host	Remove storage host. If host group name is provided as input, the workflow will also remove the host from the host gro...	1	1		
New VMFS Datastore	Create a storage volume and build VMFS datastore on the volume.	3	1		
New Virtual Machine	Create a new virtual machine on the hypervisor from an OVA or OVF file. Datastore, Host/Cluster, and image URL fields ...	1	0		
New Storage Host Group	Create a new storage host group. If hosts are provided as inputs, the workflow will add the hosts to the host group.	1	1		
New Storage Host	Create a new storage host. If host group is provided as input, then the host will be added to the host group.	1	2		

3. Click Execute.



4. Select the appropriate Organization (default by default).
5. Select the appropriate Pure Storage device.

6. Enter the name of the Host Group and of the Hosts created during Host Registration. VM-AMD-Host-FC-01 and VM-AMD-Host-FC-02 are the host used in this deployment.

### Enter Workflow Input - New Storage Host Group ×

Organization \*  
FlashStack-BB ▼ ⊙

---

Workflow Instance Name  
New Storage Host Group ⊙

---

Storage Device \*  
10.2.164.102 Pure Storage ▼ ⊙

---

Host Group \*  
VM-AMD-Host-Group ⊙

---

Hosts  
VM-AMD-Host-FC-01 🗑️

---

Hosts  
VM-AMD-Host-FC-02 🗑️ +

Cancel Execute

7. Click Execute.

#### 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. Click Storage > Volumes.
2. Click the + icon in the Volumes Panel.

A pop-up will appear to create a volume on the FlashArray.

### Create Volume

**Container** /

**Name** Letters, Numbers, -

**Provisioned Size** Numbers G

**Bandwidth Limit** Numbers MB/s

Create Multiple... Cancel Create

- 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** VM-AMD-Host-FC-Boot-#

**Provisioned Size** 20 G

**Start Number** 1

**Count** 2

**Number of Digits** 2

QoS Configuration (Optional) v

Create Single... Cancel Create

- Click Create to provision the volumes to be used as FC boot LUNs.
- 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.

The screenshot shows the Pure Storage management console interface. On the left is a dark sidebar with navigation options: Dashboard, Storage, Analysis (Performance, Capacity, Replication), Health, Settings, Help, End User Agreement, Terms, and Log Out. The main content area is titled 'Storage' and has tabs for Array, Hosts, Volumes, Protection Groups, and Pods. The 'Hosts' tab is selected, showing a breadcrumb path: Hosts > VM-AMD-Host-FC-01. Below this is a summary table:

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

Below the table are two sections: 'Connected Volumes' and 'Protection Groups'. Both sections show '0 of 0' items and a gear icon dropdown menu. The 'Connected Volumes' dropdown menu is open, showing the following options:

- Connect..
- Disconnect...
- Download CSV

- From the gear icon drop-down list, select Connect Volumes.

Connect Volumes to Host

Existing Volumes

[Empty]

1-2 of 2 < >

VM-AMD-Host-FC-Boot-01

VM-AMD-Host-FC-Boot-02 ● 1

Selected Volumes

1 selected Clear all

VM-AMD-Host-FC-Boot-01 x

LUN 1

Cancel Connect



LUN ID 1 should be used for the boot .

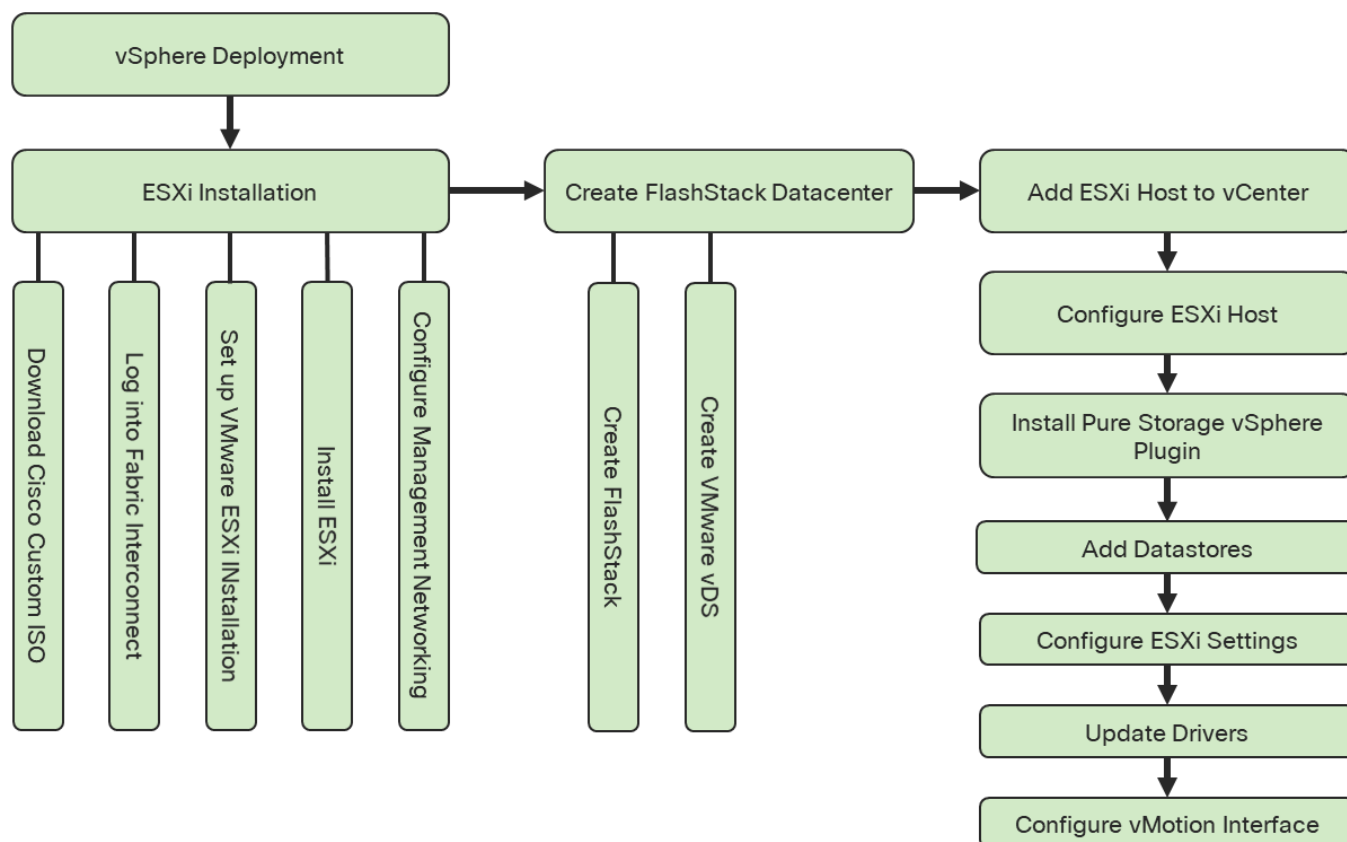
7. Select the volume that has been provisioned for the host, set the LUN ID for the volume, click the + next to the volume, and click Confirm to proceed. Repeat steps 1-7 to connecting volumes for each of the host/volume pairs configured.



## vSphere Deployment

### ESXi Installation

This section provides detailed instructions to install VMware ESXi 7.0 in a FlashStack environment. After the process is 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 7.0

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. If the Cisco Custom Image was not downloaded earlier, download it by following these steps:



You will need a user id and password on [vmware.com](https://www.vmware.com) to download this software.

1. Click the following link: [Cisco Custom ISO for UCS 4.1.2a](#)
2. 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 in to 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. Choose 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 click 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.

---

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

1. In the KVM window, click Virtual Media icon .
2. Click Activate Virtual Devices.
3. Click Virtual Media again and click 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. Choose 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. Click the LUN that was previously set up as the installation disk for ESXi and press Enter to continue with the installation.
  5. Click the appropriate keyboard layout and press Enter.
  6. Enter and confirm the root password and press Enter.
  7. The installer issues a warning that the selected disk will be repartitioned. Press F11 to continue with the installation.
  8. From the KVM window, press Enter to reboot the server.

### **Set Up Management Networking for ESXi Hosts**

Adding a management network to 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:

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.
3. Click Troubleshooting Options.
4. Enable ESXi shell.
5. Enable SSH.
6. Hit Esc to exit.
7. Click the Configure the Management Network option and press Enter.
8. Click the Network Adapters option and leave vmnic0 selected, then arrow down to vmnic1 and press space to select vmnic1 as well and press Enter.
9. Click the VLAN (Optional) option and press Enter.
10. Enter the <<var\_ib\_mgmt\_vlan\_id>> and press Enter.
11. From the Configure Management Network menu, select IPv4 Configuration and press Enter.
12. Choose the Set Static IP Address and Network Configuration option by using the space bar.
13. Enter <<var\_vm\_host\_FC\_01\_ip>> for the IPv4 Address for managing the first ESXi host.
14. Enter <<var\_ib\_mgmt\_vlan\_netmask\_length>> for the Subnet Mask for the first ESXi host.
15. Enter <<var\_ib\_mgmt\_gateway>> for the Default Gateway for the first ESXi host.
16. Press Enter to accept the changes to the IPv4 configuration.
17. Choose the DNS Configuration option and press Enter.



---

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

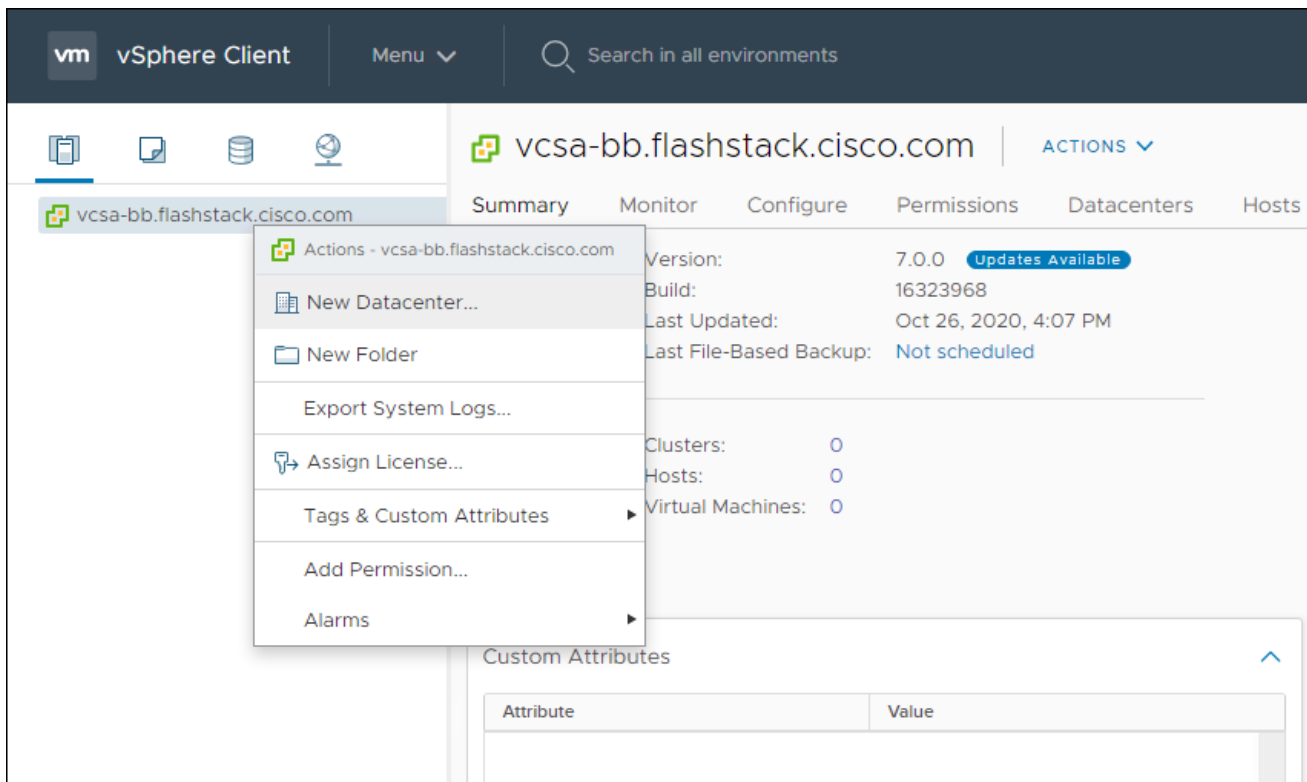
---

18. Enter the IP address of <<var\_nameserver\_ip>> for the Primary DNS Server.
19. Optional: Enter the IP address of the Secondary DNS Server.
20. Enter the fully qualified domain name (FQDN) for the first ESXi host.
21. Press Enter to accept the changes to the DNS configuration.
22. Press Esc to exit the Configure Management Network submenu.
23. Press Y to confirm the changes and return to the main menu.
24. The ESXi host reboots. After reboot, press F2 and log back in as root.
25. Choose Test Management Network to verify that the management network is set up correctly and press Enter.
26. Press Enter to run the test.
27. Press Enter to exit the window, and press Esc to log out of the VMware console.
28. Repeat steps in Set Up VMware ESXi Installation, Install ESXi, and Set UP Management Networking for ESXi Host for additional hosts provisioned, using appropriate values.

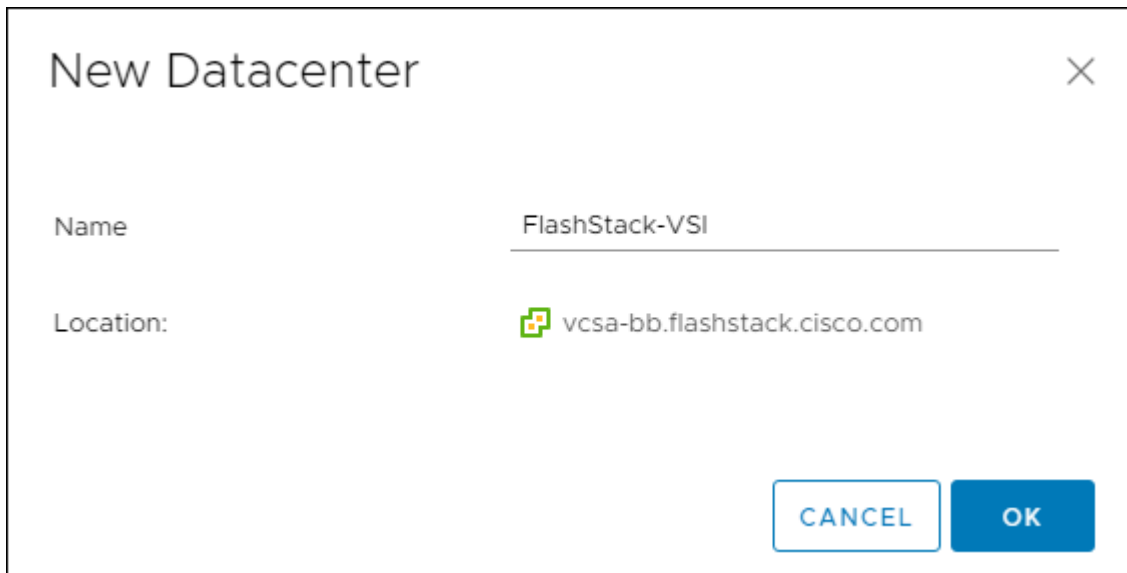
## Create FlashStack Datacenter

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

1. Connect to the vSphere Web Client and click Hosts and Clusters or click the Hosts and Clusters icon from the Home center window.
2. Right-click the vCenter icon and select New Datacenter... from the drop-down list.



3. Enter a Datacenter name and click OK.



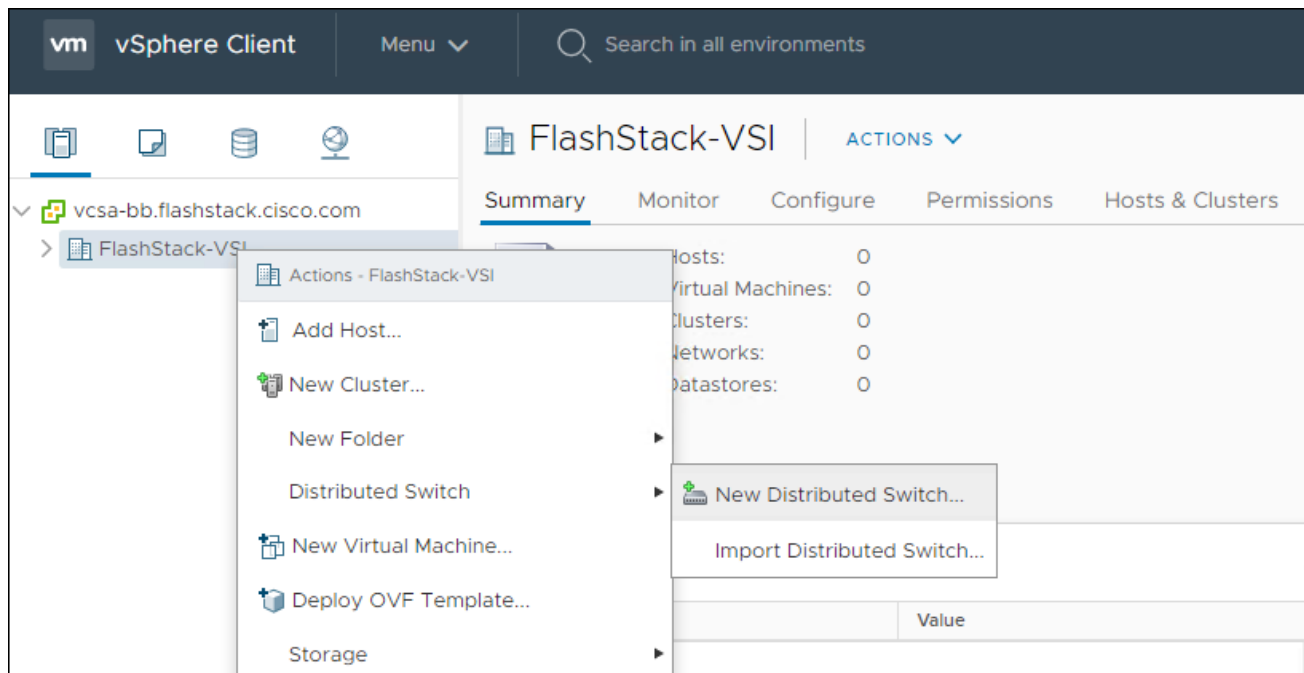
### Create VMware vDS for vMotion and Application Traffic

The VMware vDS setup consists of one vDS that are vMotion and Application traffic.

#### FlashStack vDS

To configure the VMware vDS, follow these steps:

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



3. Provide the Distributed Switch a descriptive name and click Next.
4. Make sure Distributed switch: 7.0.0 is selected and click Next.
5. 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 VM-Traffic 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.

## New Distributed Switch

✓ 1 Name and location

✓ 2 Select version

✓ 3 Configure settings



4 Ready to complete

### Ready to complete

Review your settings selections before finishing the wizard.

Name	FlashStack-vDS
Version	7.0.0
Number of uplinks	2
Network I/O Control	Enabled
Default port group	VM-Traffic

### Suggested next actions

-  New Distributed Port Group
-  Add and Manage Hosts

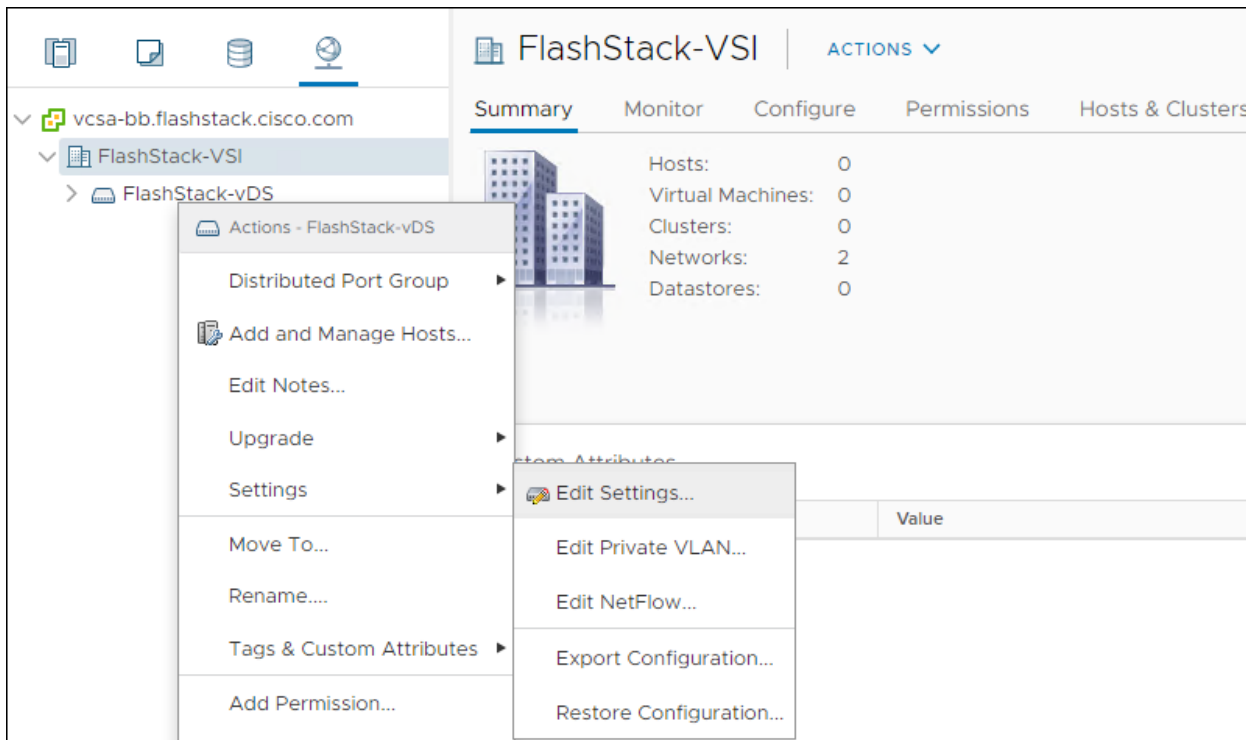
 These actions will be available in the Actions menu of the new distributed switch.

CANCEL

BACK

FINISH

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



The screenshot shows the vSphere interface for a FlashStack-VSI. The left pane shows the hierarchy: vcsa-bb.flashstack.cisco.com > FlashStack-VSI > FlashStack-vDS. The main pane shows the Summary tab with the following statistics:

Hosts:	0
Virtual Machines:	0
Clusters:	0
Networks:	2
Datastores:	0

The context menu for FlashStack-vDS is open, showing the following options:

- Actions - FlashStack-vDS
  - Distributed Port Group
  - Add and Manage Hosts...
  - Edit Notes...
  - Upgrade
  - Settings
    - Edit Settings...
    - Edit Private VLAN...
    - Edit NetFlow...
  - Tags & Custom Attributes
  - Add Permission...

8. Change the MTU to 9000. The Discovery Protocol can optionally be changed to Link Layer Discovery Protocol and the Operation to Both. Click OK.

### FlashStack-vDS - Edit Settings

---

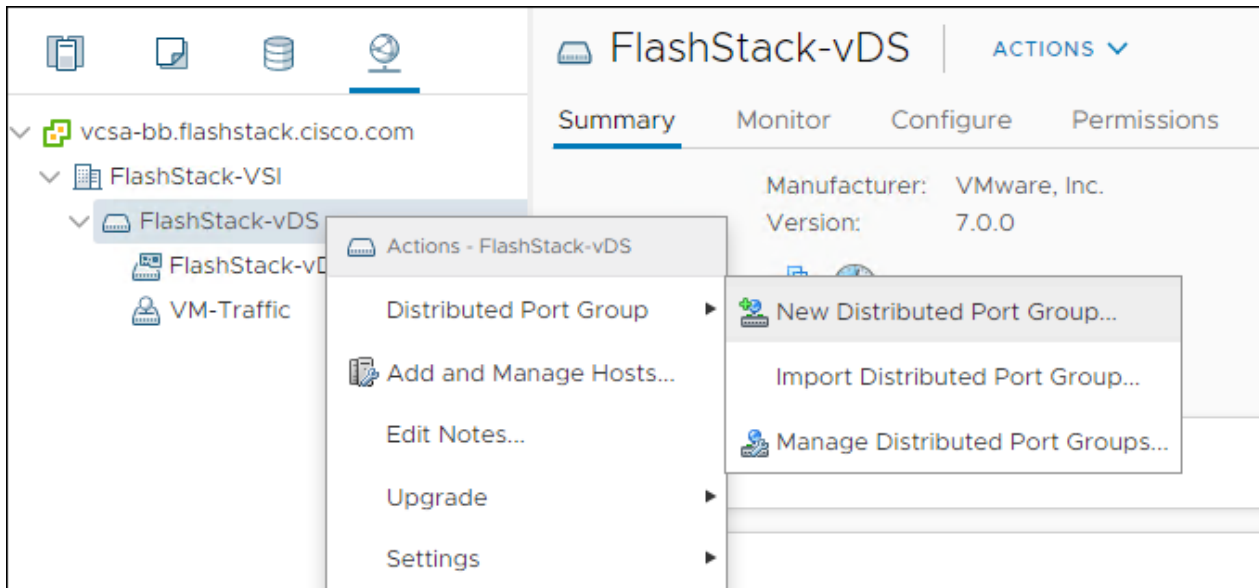
**General**

**Advanced**

MTU (Bytes)	9000
Multicast filtering mode	IGMP/MLD snooping
Discovery protocol	
Type	Link Layer Discovery Protocol
Operation	Both
Administrator contact	
Name	
Other details	

9. Expand the FlashStack VSI datacenter and the newly created vDS.
10. Right-click the VM-Traffic Distributed Port Group, and click Edit Settings...
11. Click VLAN, change the VLAN type from None to VLAN, and enter in the appropriate VLAN number for the VM-Traffic network.
12. Click OK to save the changes.
13. Right-click and select Distributed Port Group -> New Distributed Port Group...





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

15. 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.

### New Distributed Port Group

1 Name and location  
 2 **Configure settings**  
 3 Security  
 4 Traffic shaping  
 5 Teaming and failover  
 6 Monitoring  
 7 Miscellaneous  
 8 Ready to complete

Configure settings  
Set general properties of the new port group.

Port binding	Static binding	▼
Port allocation	Elastic	▼ ⓘ
Number of ports	8	
Network resource pool	(default) ▼	
VLAN		
VLAN type	VLAN	▼
VLAN ID	1130	

Advanced

Customize default policies configuration

CANCEL

16. Click Next.

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

18. Within the Teaming and failover section move Uplink 1 to the Standby uplinks section.



The movement of Uplink 1 to standby is guiding vMotion traffic to stay within the B side fabric contained within Uplink 2 to prevent unnecessary traffic hops up into the Cisco Nexus switch to traverse between Fabric Interconnects.

### New Distributed Port Group

- ✓ 1 Name and location
- ✓ 2 Configure settings
- ✓ 3 Security
- ✓ 4 Traffic shaping
- 5 Teaming and failover**
- 6 Monitoring
- 7 Miscellaneous
- 8 Ready to complete

#### Teaming and failover

Controls load balancing, network failure detection, switches notification, fallback, and uplink failover order.

Load balancing	Route based on originating virtual port
Network failure detection	Link status only
Notify switches	Yes
Fallback	Yes

#### Failover order ⓘ

↑ ↓

Active uplinks
Uplink 2
Standby uplinks
Uplink 1
Unused uplinks

CANCEL BACK NEXT

19. Click Next.

20. Click Next Past Monitoring, Miscellaneous, and Edit additional settings sections.

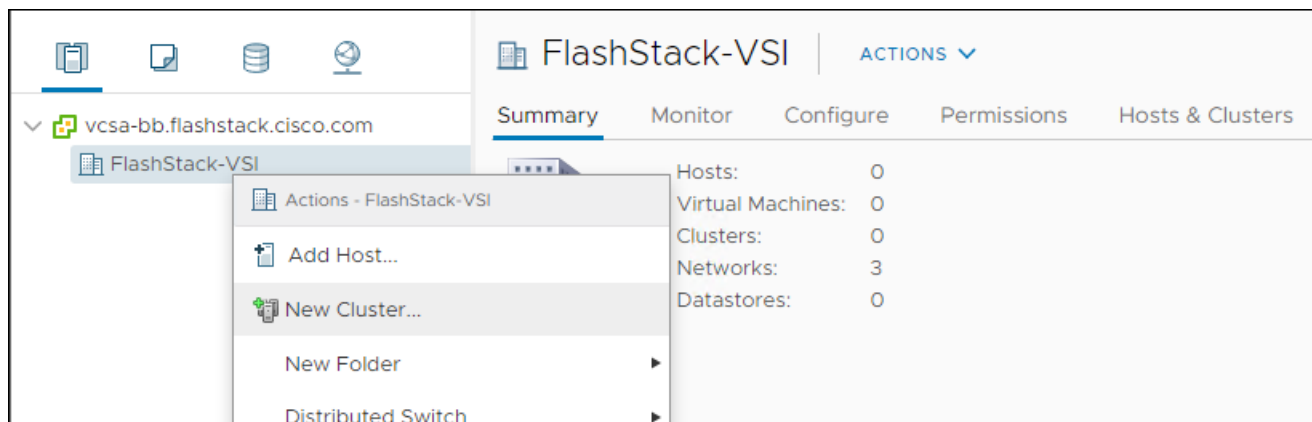
21. Review the Ready to complete section.

22. Click Finish to create the Distributed Port Group.

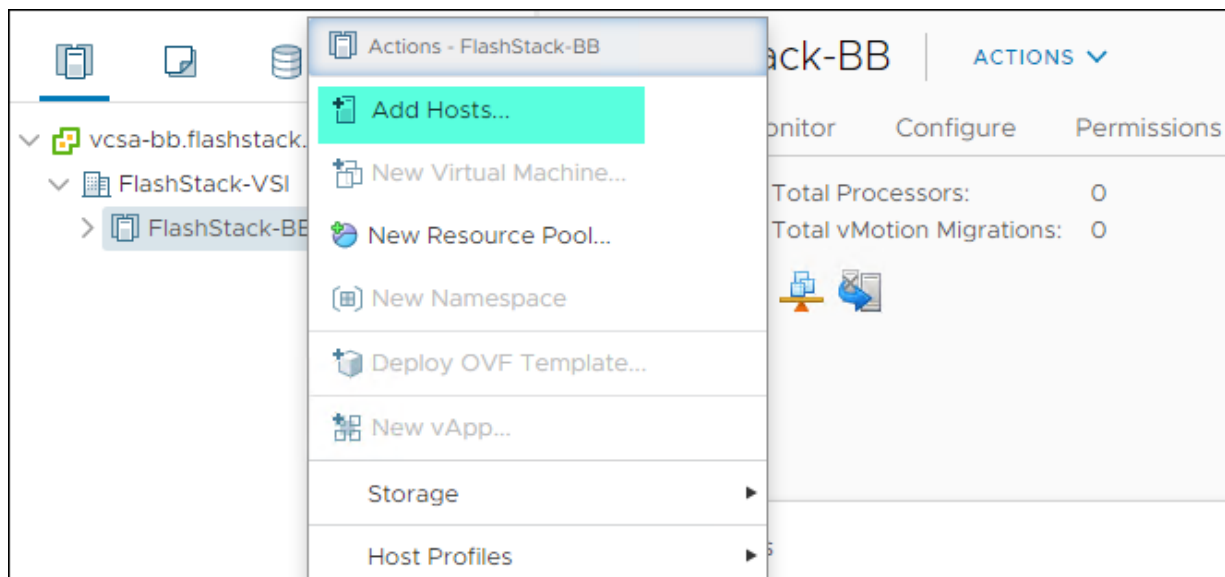
### Add the VMware ESXi Hosts Using the VMware vSphere Web Client

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 list.



2. Enter a name for the new cluster, enable vSphere DRS and vSphere HA, leaving all other options with defaults.
3. Click OK to create the cluster.
4. Right-click the newly created cluster and from the drop-down list select the Add Host.



5. Enter the IP or FQDN, User Name, and password of the ESXi hosts and click Next.

Add hosts
×

1 Add hosts

2 Host summary

3 Ready to complete

### Add new and existing hosts to your cluster

New hosts (2) Existing hosts (0 from 0)

Use the same credentials for all hosts

10.1.164.110	root	.....	×
10.1.164.111	root	.....	×
IP address or FQDN	Username	Password	

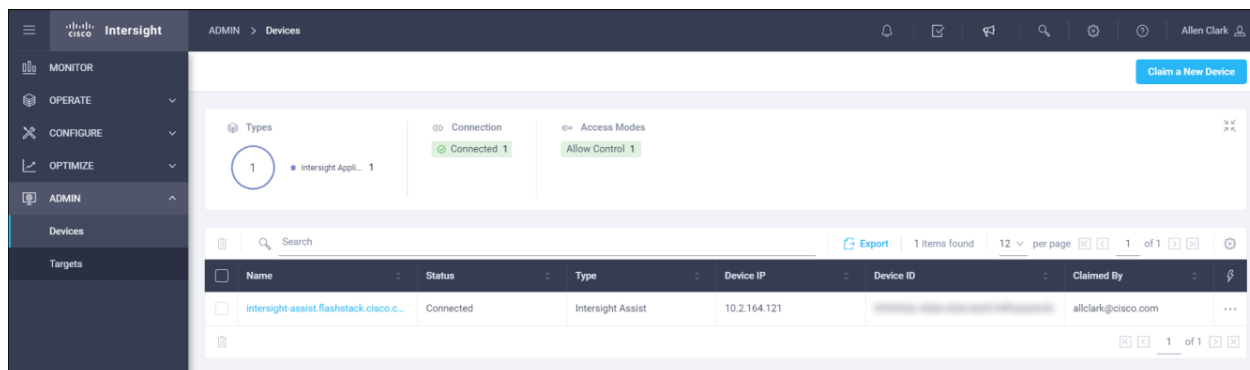
CANCEL NEXT

6. Click Yes in the Security Alert pop-up to confirm the host's certificate.
7. Click Next past the Host summary dialogue.
8. 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.
9. Leave lockdown mode Disabled within the Lockdown mode dialogue window and click Next.
10. Skip past the Resource pool dialogue by clicking Next.
11. Click Next to confirm the Summary dialogue and add the ESXi host to the cluster.

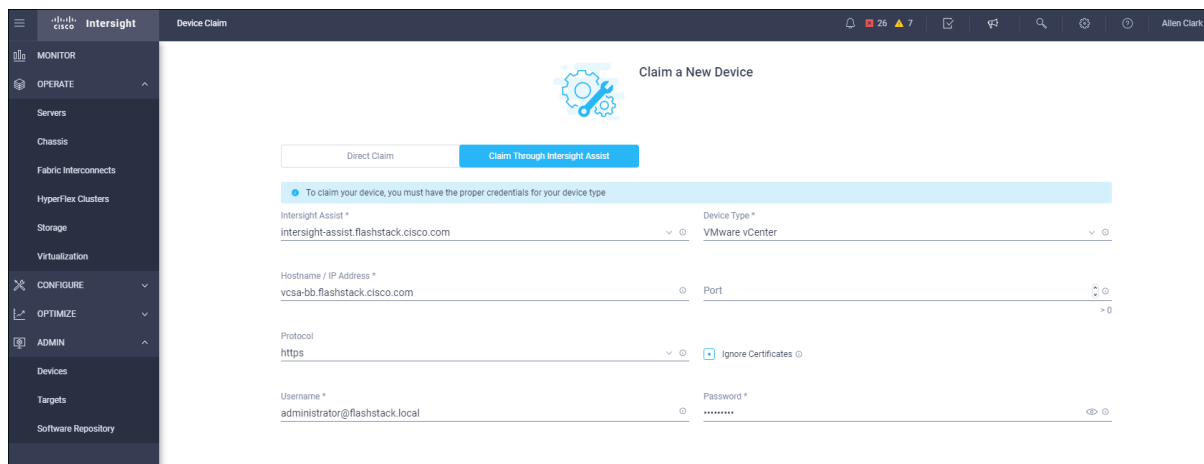
### Claim vCenter in Intersight

To claim vCenter in Intersight, follow these steps:

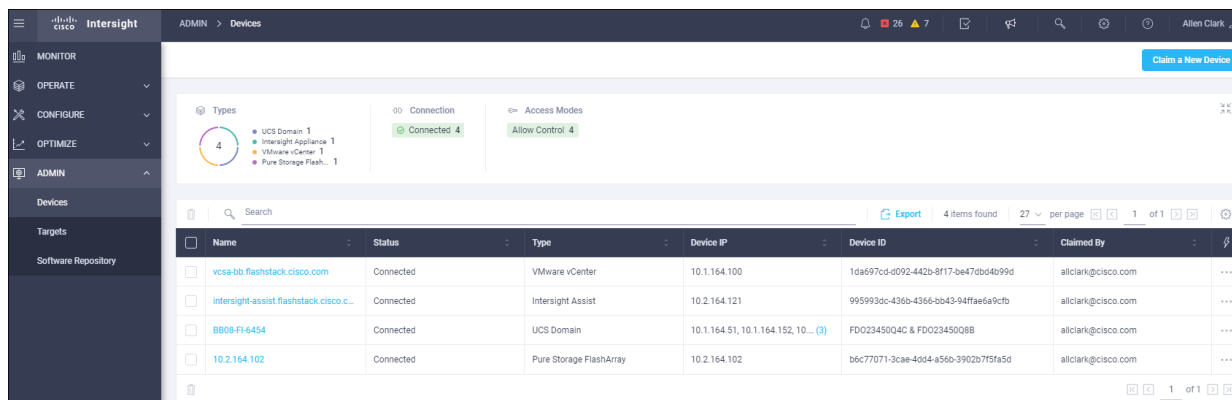
1. Open a browser and go to Cisco Intersight <https://intersight.com> and log into your Intersight account
2. Click Admin > Devices.



3. Click Claim a New Device and select Claim Through Intersight Assist.
4. Set Type to VMware vCenter.
5. Enter vCenter Hostname/ IP address and credentials.



6. Click Claim.



Name	Status	Type	Device IP	Device ID	Claimed By
vcse-bb.flashstack.cisco.com	Connected	VMware vCenter	10.1.164.100	1de6970d-0092-442b-8f17-be470b04b99d	allclark@cisico.com
intersight-assist.flashstack.cisco.c...	Connected	Intersight Assist	10.2.164.121	995993c-436b-4366-bb43-94ffae6a9cfc	allclark@cisico.com
BB08-FI-6454	Connected	UCS Domain	10.1.164.51, 10.1.164.152, 10... (3)	FD02345004c & FD023450088	allclark@cisico.com
10.2.164.102	Connected	Pure Storage FlashArray	10.2.164.102	b6c77071-3cae-40d4-a56b-3902b75fa50	allclark@cisico.com

## Create VMFS Swap Datastore

To create a vmfs 6 datastore to place swap using Intersight Orchestration, follow these steps:



Creating vVol datastores is explained in section [Pure Storage vSphere Client Plugin](#).

1. Selection Configure -> Orchestration.
2. Click New VMFS Datastore.

Interight

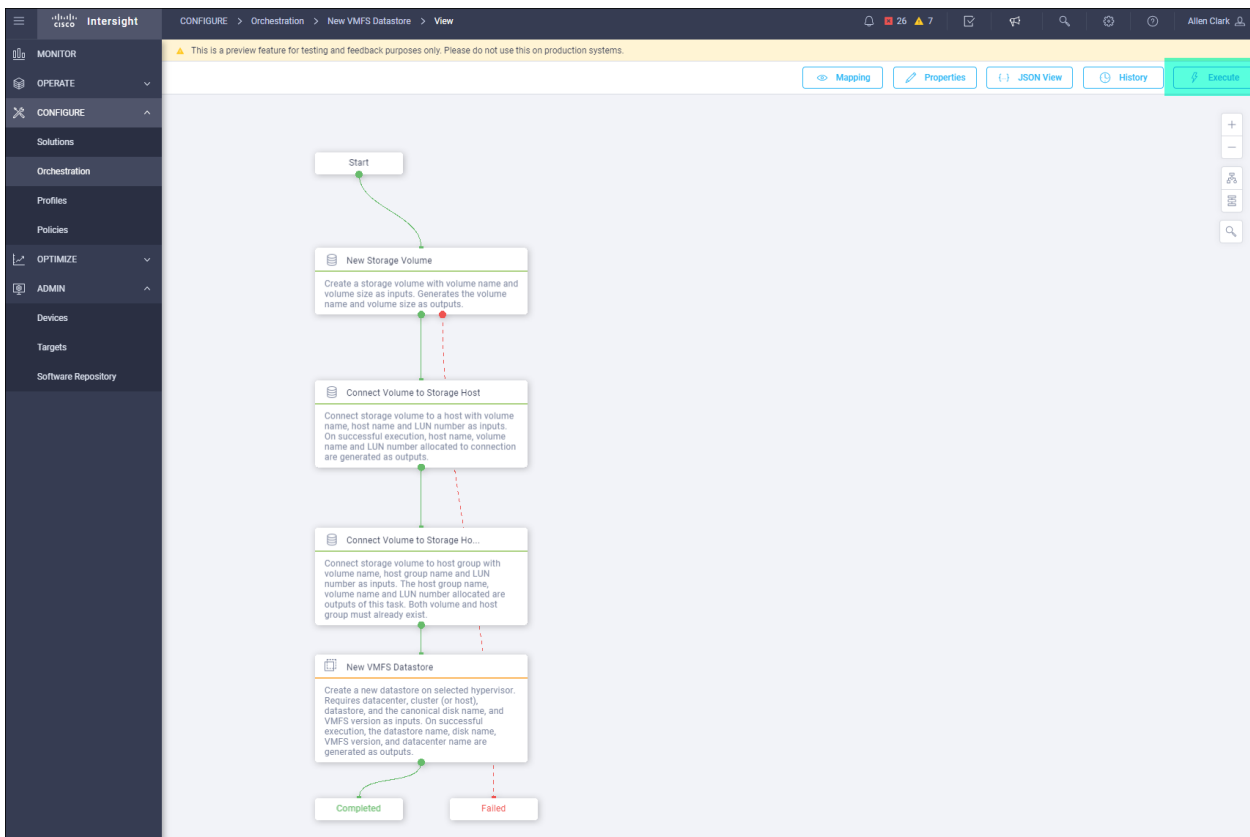
CONFIGURE > Orchestration

Workflows Data Types

9 items found | 10 per page | 1 of 1

Name	Description	Default Version	Executions	Last Execution Status	Validation Infor
<input type="checkbox"/> Update VMFS Datastore	Expand a datastore on hypervisor manager by extending the backing storage volume to specified capacity, and then gro...		2 1	<span style="color: red;">❌</span>	<span style="color: green;">✅</span>
<input type="checkbox"/> Update Storage Host	Update the storage host details. If the inputs for a task are provided then the task is run, else it is skipped.		1 0	<span style="color: green;">✅</span>	<span style="color: green;">✅</span>
<input type="checkbox"/> Remove VMFS Datastore	Remove VMFS datastore and remove the backing volume from the storage device.		3 0	<span style="color: green;">✅</span>	<span style="color: green;">✅</span>
<input type="checkbox"/> Remove Storage Host ...	Remove storage host group. If hosts are provided as input, the workflow will remove the hosts from the host group.		1 0	<span style="color: green;">✅</span>	<span style="color: green;">✅</span>
<input type="checkbox"/> Remove Storage Host ...	Remove storage host. If host group name is provided as input, the workflow will also remove the host from the host gro...		1 1	<span style="color: green;">✅</span>	<span style="color: green;">✅</span>
<input type="checkbox"/> New VMFS Datastore	Create a storage volume and build VMFS datastore on the volume.		3 1	<span style="color: green;">✅</span>	<span style="color: green;">✅</span>
<input type="checkbox"/> New Virtual Machine	Create a new virtual machine on the hypervisor from an OVA or OVF file. Datastore, Host/Cluster, and Image URL, fields ...		1 0	<span style="color: green;">✅</span>	<span style="color: green;">✅</span>
<input type="checkbox"/> New Storage Host Group	Create a new storage host group. If hosts are provided as inputs, the workflow will add the hosts to the host group.		1 1	<span style="color: green;">✅</span>	<span style="color: green;">✅</span>
<input type="checkbox"/> New Storage Host	Create a new storage host. If host group is provided as input, then the host will be added to the host group.		1 2	<span style="color: green;">✅</span>	<span style="color: green;">✅</span>

### 3. Click Execute.



4. Select the appropriate Organization (default by default).
5. Select the appropriate Pure Storage device.
6. Enter the name of the Volume that will appear on the Pure Storage Array: ESXi-Swap.
7. Enter Volume size and units.

8. Choose Storage Host Group: VM-AMD-Host-Group.
9. Choose an unused LUN Number.
10. Choose the appropriate Hypervisor Manager and Datacenter.
11. Enter the name of the Datastore that will appear in vSphere.
12. Choose VMFS Version VMFS-6.

### Enter Workflow Input - New VMFS Datastore ✕

---

Volume \*  
ESXI-Swap ⊙

Volume Capacity  
Volume Size \*  
1 ⊙

Volume Unit \*  
TiB ⌵ ⊙

Storage Host ⌵ ⊙

Storage Host Group  
VM-AMD-Host-Group ⌵ ⊙

LUN Number  
3 ⌵ ⊙  
0 - 16384

Hypervisor Manager \*  
vcsa-bb.flashstack.cisco.com VMware ⌵ ⊙

Datacenter \*  
FlashStack-VSI ⌵ ⊙

Cluster  
FlashStack-BB ⌵ ⊙

Host ⌵ ⊙

Datastore \*  
ESXI-Swap ⊙

VMFS Version \*  
VMFS-6 ⌵ ⊙

Cancel Execute

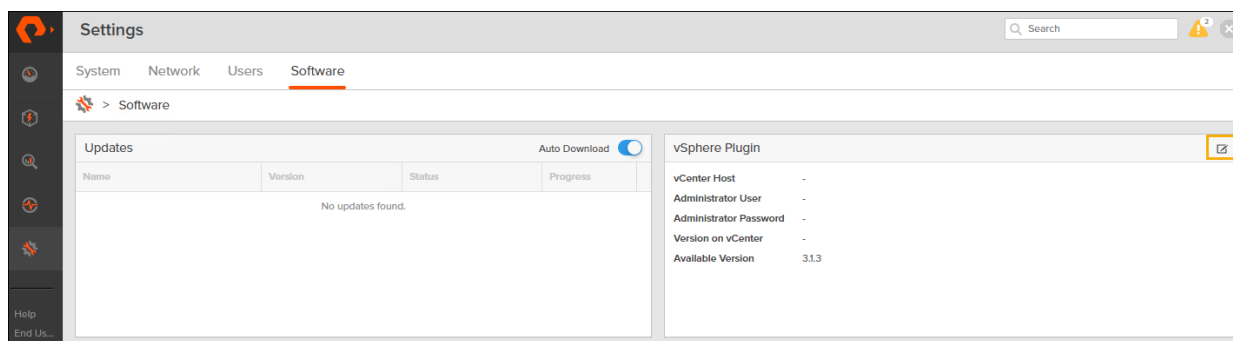
13. Click Execute

### Pure Storage vSphere Client Plugin

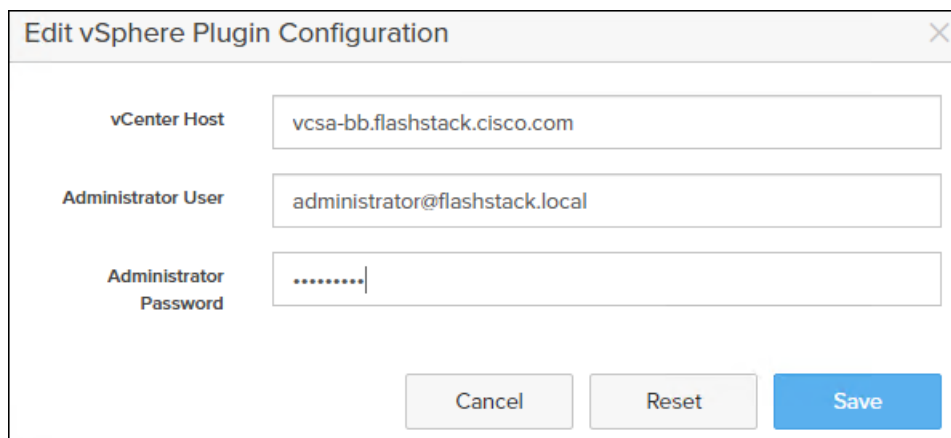
The Pure Storage vSphere Client Plugin will be accessible through the vSphere Client after registration through the Pure Storage Web Portal.

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

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



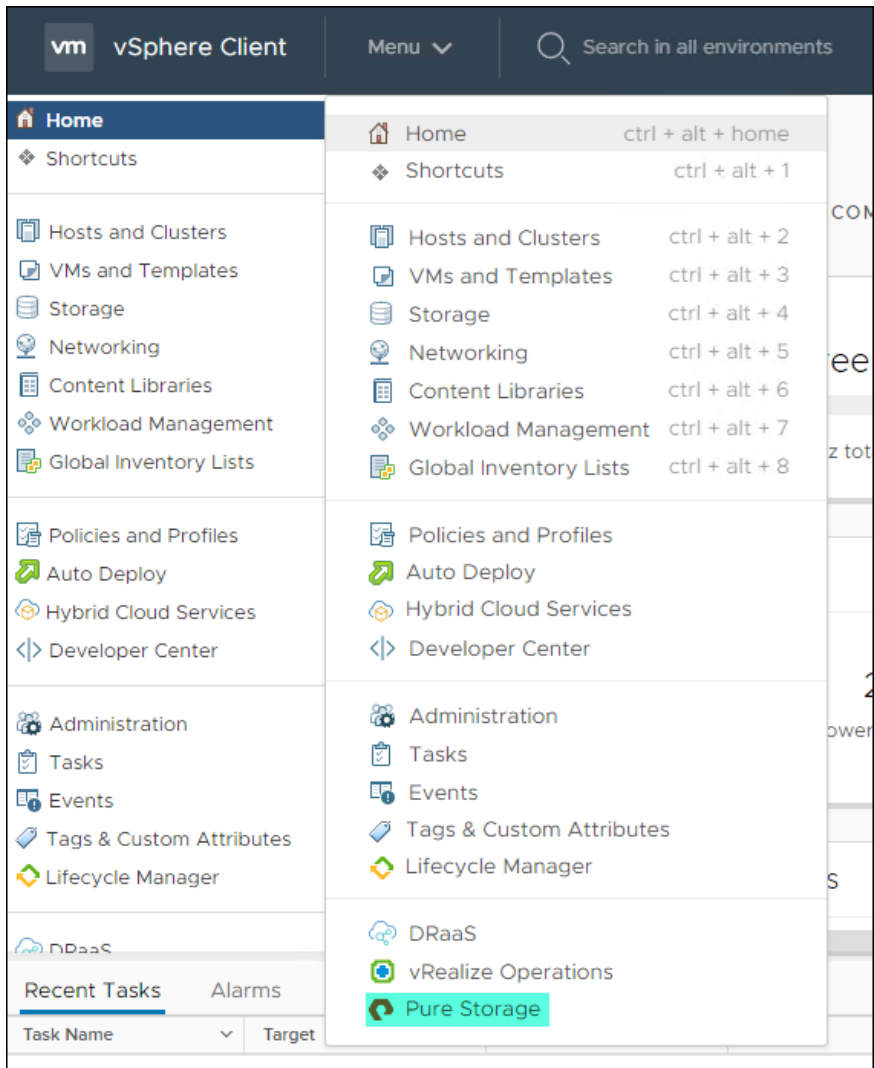
3. Enter the vCenter information and click Save.



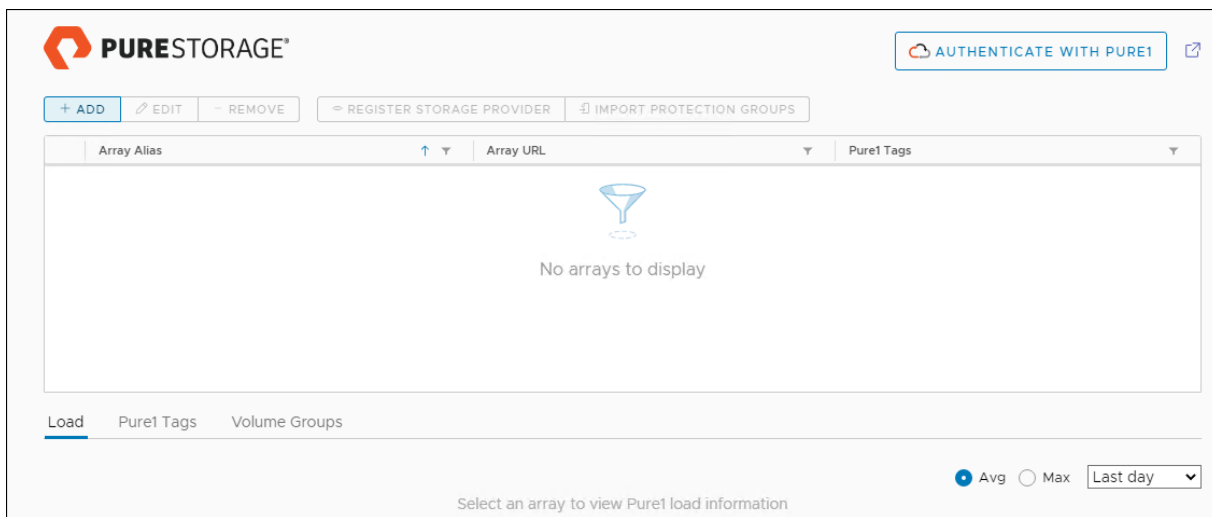
4. After the discovery completes. Click install.

5. In vCenter, click Pure Storage.






6. Click Authenticate with Pure1.



7. Input your Pure1 JWT (link).

## Authenticate with Pure1 ✕

 Authenticate with Pure1 to enable streamlined fleet registration and additional performance data for your Pure Storage arrays and datastores

Pure1 JWT ⓘ \*

```
FeE/YSvCm9OH/MRIRKQCx82VDLM8PFK1HdAes
R1kxxFtXlhUuhoeDJKTJy1hqR5IXdhxB3GdUiNBF0h
kh38FKmJYaexABFSial4CMI4LTSfkrhoA
```

8. Click Authenticate.

9. Click Add.

10. Click Import Arrays from Pure1 and input the Username and Password.

### Add Array ✕

Add a Single Array 🔄 Import Arrays from Pure1

Use the same credentials for all arrays

	Array Alias	Online	Array URL	Username	Password
<input type="checkbox"/>	BB08-FlashArrayR3	📶	10.2.164.102	pureuser	*****
<input type="checkbox"/>		🔴		Username	Password

1 - 2 of 2 arrays

DONE
ADD

11. Click Done
12. Select the newly added array.
13. Click Register Storage Provider.

+ ADD
 ✎ EDIT
 - REMOVE
 ➤ REGISTER STORAGE PROVIDER
 📄 IMPORT PROTECTION GROUPS

	Array Alias	Array URL
<input checked="" type="radio"/>	BB08-FlashArray-R3	https://10.2.164.100

14. Enter Username and Password.

Register Storage Provider

Registering the storage provider requires a valid username and password.

Username \* pureuser

Password \* .....

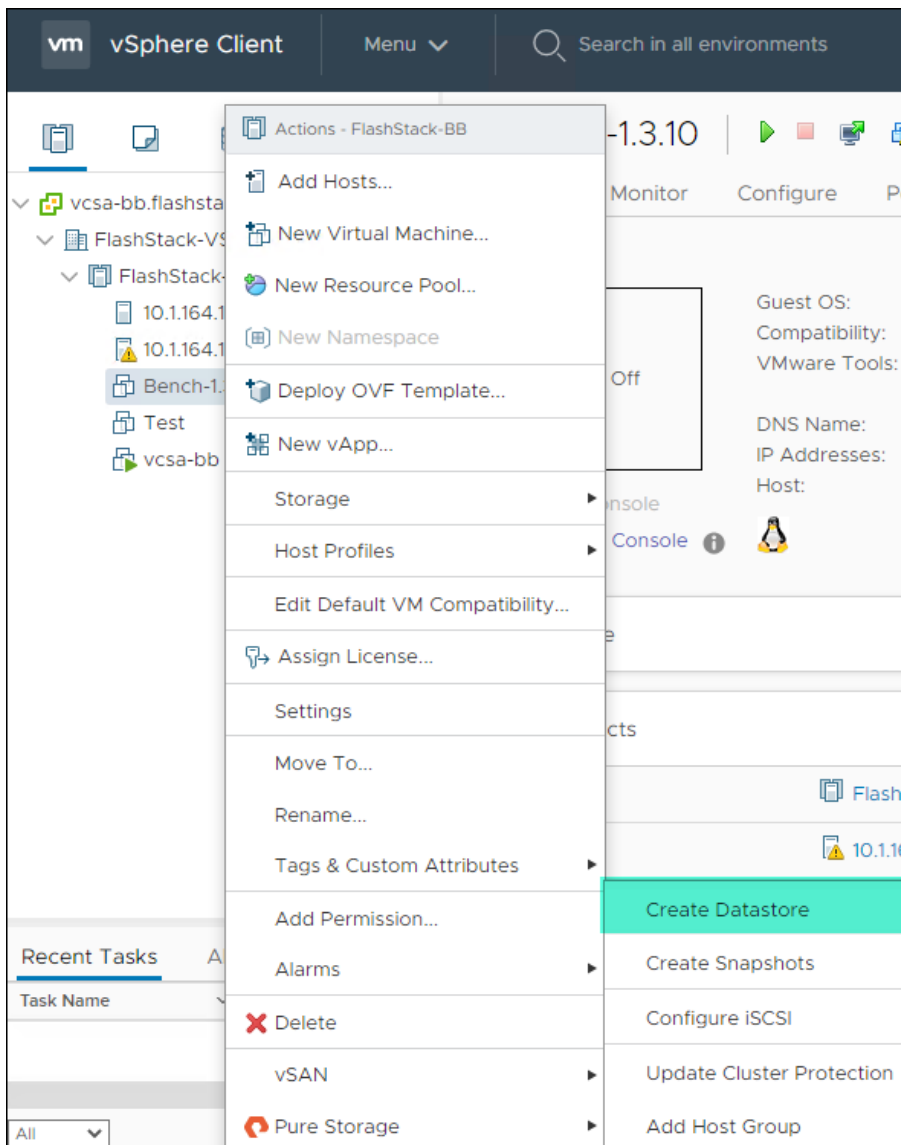
CANCEL REGISTER

15. Click Register.

### Create vVol Datastore

To create a vVol datastore, follow these steps:

1. In vCenter, click Host and Clusters.
2. Right-click the FlashStack Cluster and click Pure Storage -> Create Datastore.



3. Click vVol.

The screenshot shows a 'Create Datastore' wizard window. On the left is a vertical navigation pane with five steps: 1 Type, 2 Name and Size, 3 Compute Resource, 4 Storage, and 5 Ready to Complete. Step 1 is selected. The main area is titled 'Type' and contains two radio button options: 'VMFS' (unselected) and 'vVol' (selected). Below 'VMFS' is the text 'Create a VMFS datastore and corresponding array volume.' Below 'vVol' is the text 'Create a Virtual Volumes datastore on an array storage container.' At the bottom right are 'CANCEL' and 'NEXT' buttons.

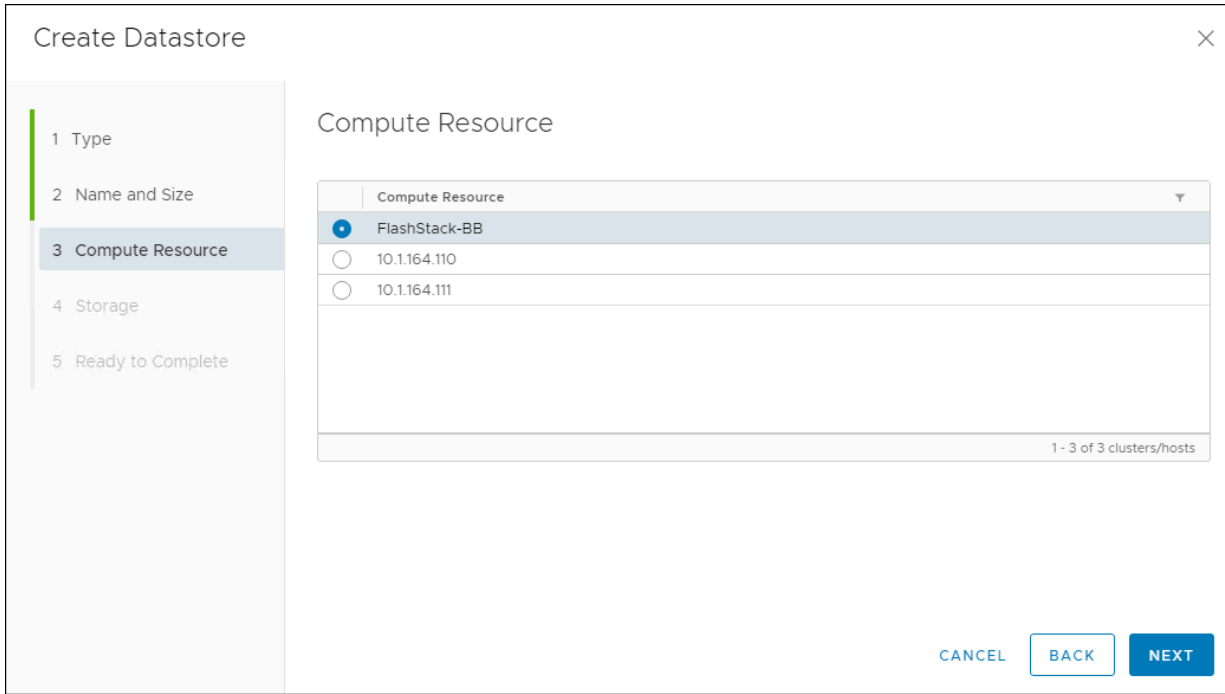
4. Click Next.

5. Enter a Datastore Name.

The screenshot shows the 'Create Datastore' wizard at Step 2: Name and Size. The navigation pane on the left now highlights Step 2. The main area is titled 'Name and Size' and features a 'Datastore Name:' label followed by a text input field containing 'FlashStack-VSI-vVol'. Below the input field is the text 'FlashArray Virtual Volume Datastores are automatically created using the maximum size.' At the bottom right are 'CANCEL', 'BACK', and 'NEXT' buttons.

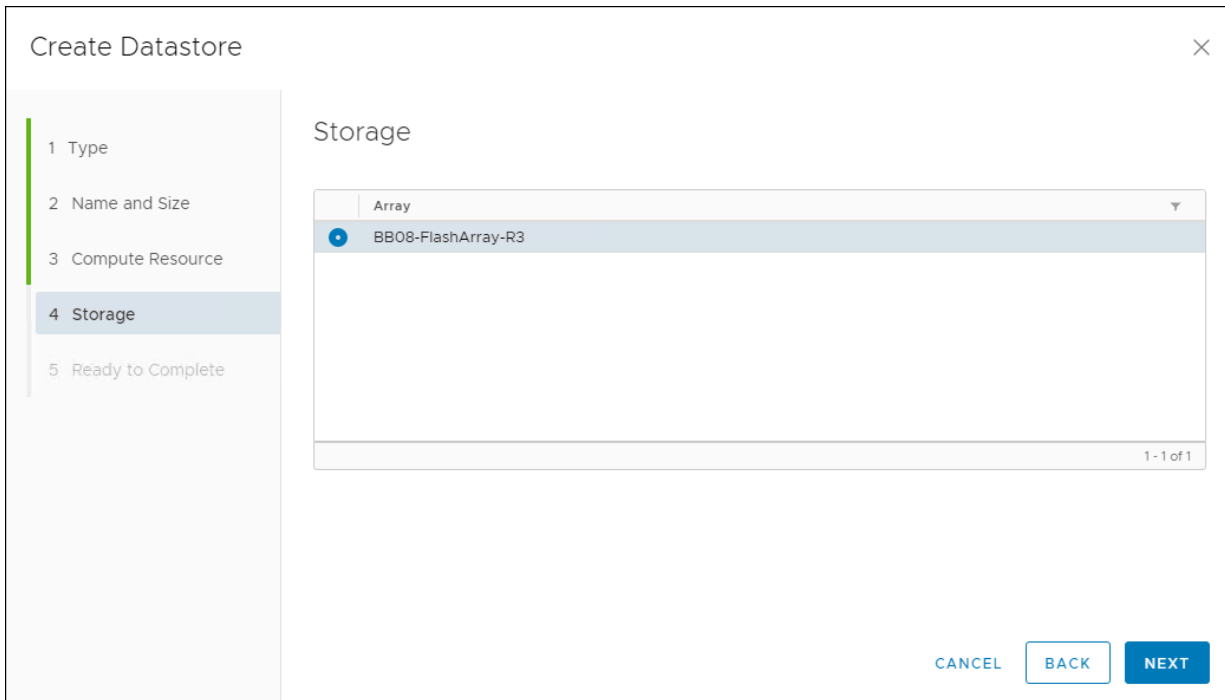
6. Click Next.

7. Choose the Cluster under Compute Resources.



8. Click Next.

9. Click the Registered FlashArray.



10. Click Next.

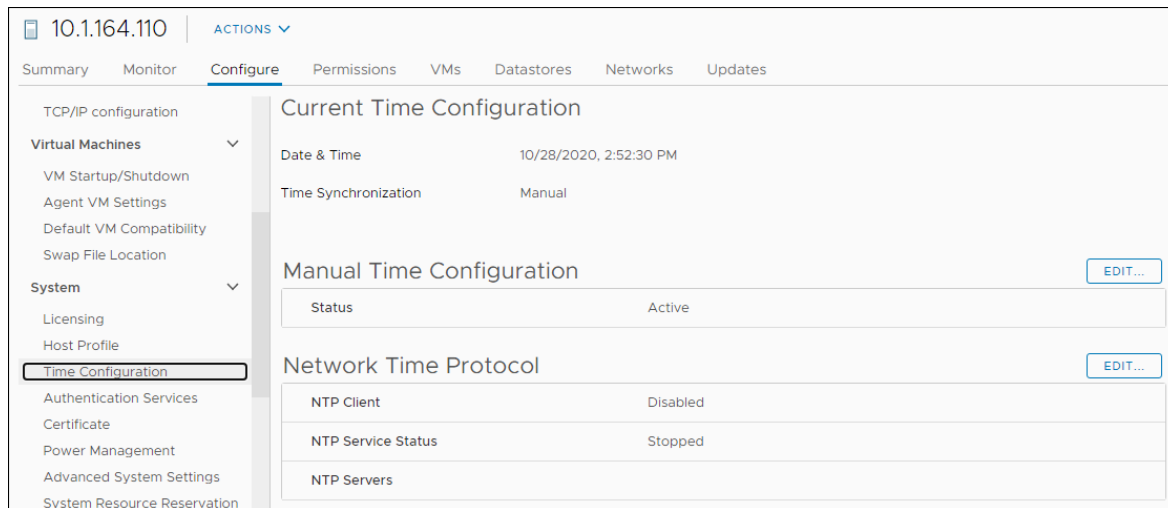
11. Review the information and click Finish.

## Configure ESXi Settings

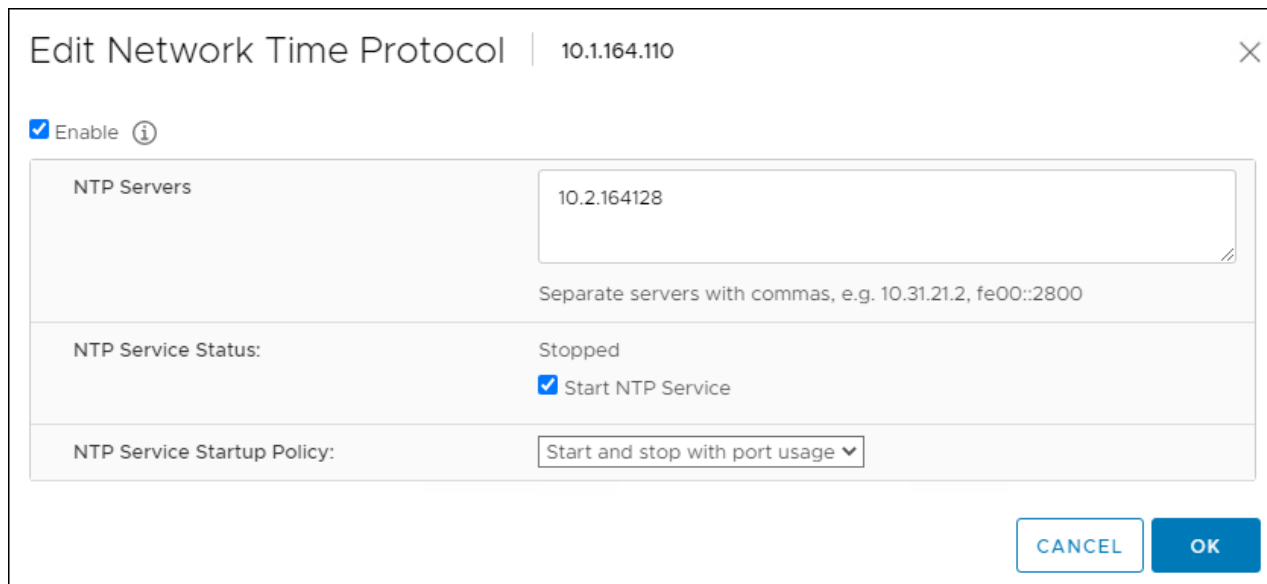
A couple of base settings are needed for stability of the vSphere environment, as well as an optional enablement of SSH connectivity to each host for the updating of drivers.

To configure ESXi settings, follow these steps:

1. Select the first ESXi host to configure with standard settings.
2. Click the Configure tab and select Time Configuration within the options and click Edit for Network Time Protocol.

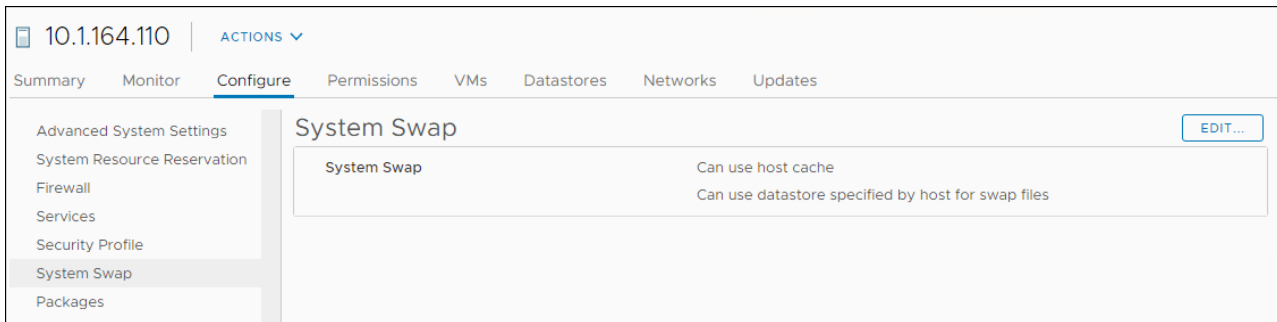


3. Check Enable, enter <<var\_oob\_ntp>> for the NTP Servers, select Start and stop with port usage for NTP Service Startup Policy, and click Start within NTP Service Status. Click OK to submit the changes.



4. Click System Swap in the System section within the Configure tab and click Edit.



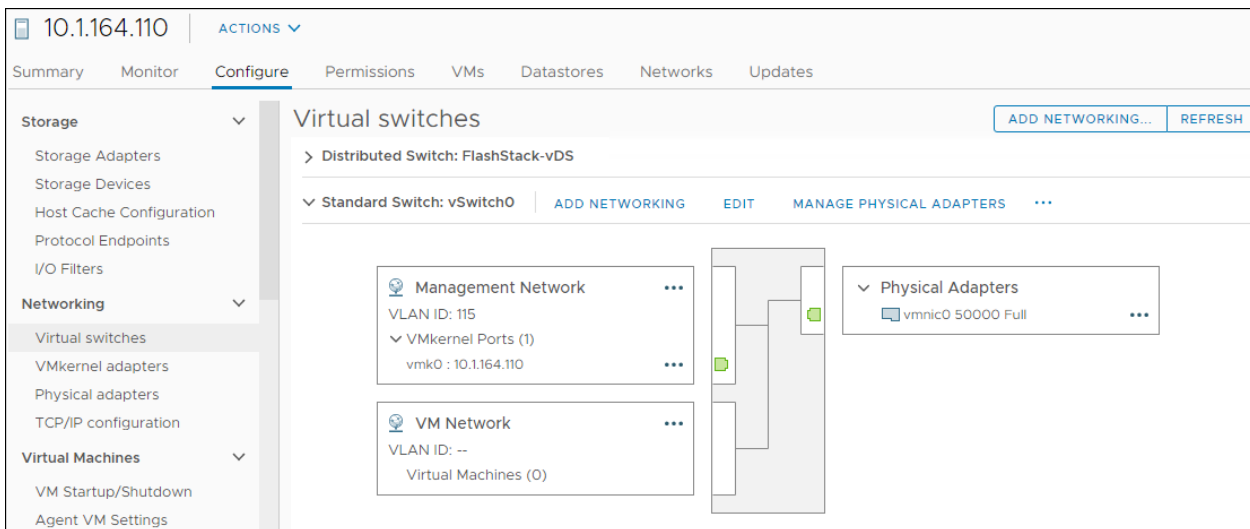


5. Select Can use datastore specified by host for swap files.
6. Repeat steps 1-5 on each ESXi host being added into the cluster.

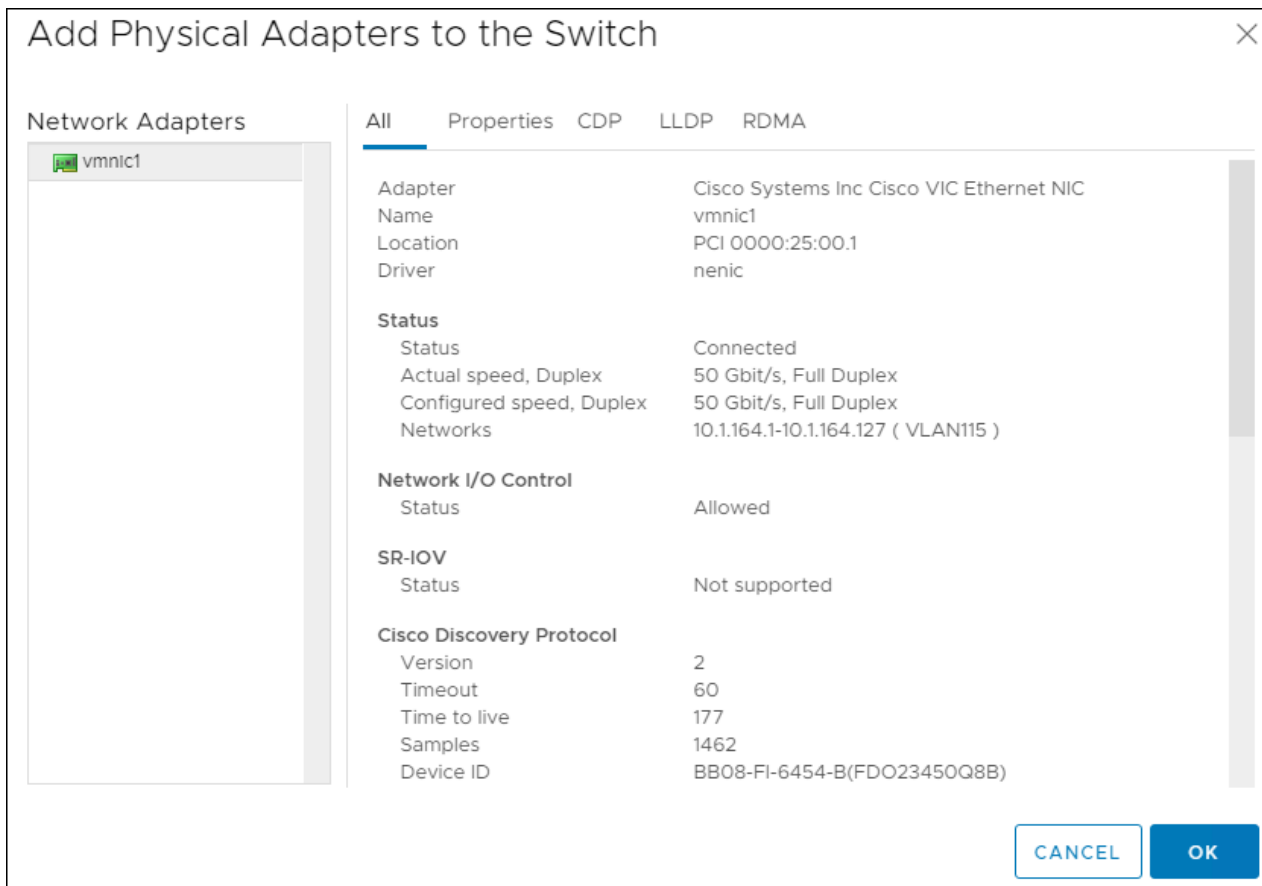
### Configure vSwitch0

To configure vSwitch0, follow these steps:

1. From the Hosts and Clusters, choose the first host and click the Configure tab for that host.
2. Click Virtual Switches under the Networking section
3. Click Manage Physical Adapters for Standard Switch: vSwitch0



4. Click the green + sign under Assigned adapters.
5. Click vmnic1 and click OK.

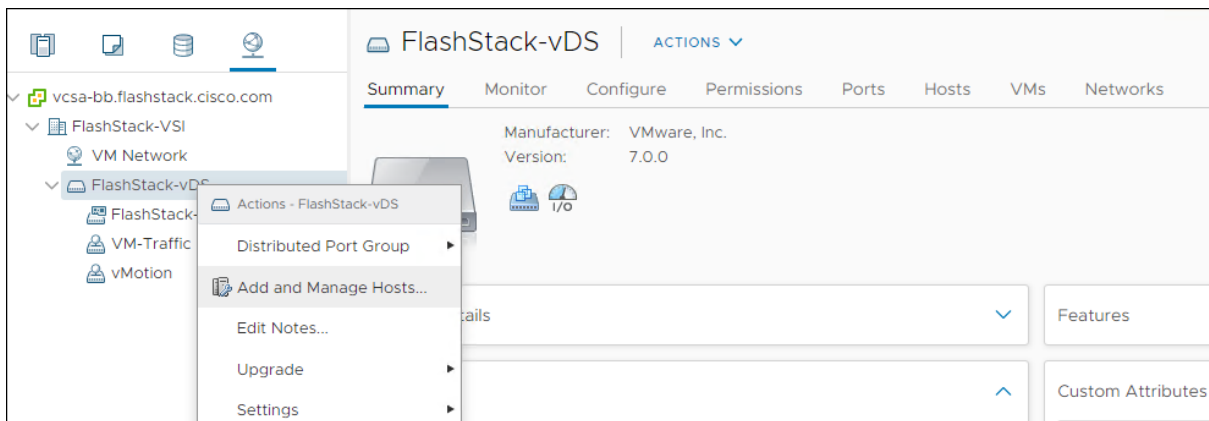


6. Confirmed that vmnic0 and vmnic1 are listed as Active adapters and click OK.

### Add the ESXi hosts to the vDS

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

1. From the Networking tab of the Navigator window, right-click the FlashStack-vDS vDS and click Add and Manage Hosts...



2. Leave Add hosts selected and click Next.

## FlashStack-vDS - Add and Manage Hosts

### 1 Select task

### 2 Select hosts

### 3 Manage physical adapters

### 4 Manage VMkernel adapt...

### 5 Migrate VM networking

### 6 Ready to complete

### Select task

Select a task to perform on this distributed switch.

Add hosts

Add new hosts to this distributed switch.

Manage host networking

Manage networking of hosts attached to this distributed switch.

Remove hosts

Remove hosts from this distributed switch.

CANCEL

BACK

NEXT

3. Click the green + icon next to New hosts...
4. In the Select new hosts pop-up that appears, select the hosts to be added, and click OK to begin joining them to the vDS.
5. Click Next.
6. Choose vmnic2 on each host and click Assign uplink. Choose Uplink 1 and click OK. Choose vmnic3 on each host and click Assign uplink. Choose Uplink 2 and click OK. If more than one host is being connected to the vDS, use the Apply this uplink assignment to the rest of the hosts checkbox.



It is important to assign the uplinks as shown below. This allows the port groups to be pinned to the appropriate Cisco UCS fabric.





## FlashStack-vDS - Add and Manage Hosts

- ✓ 1 Select task
- ✓ 2 Select hosts
- 3 Manage physical adapters**
- 4 Manage VMkernel adapt...
- 5 Migrate VM networking
- 6 Ready to complete

### Manage physical adapters

Add or remove physical network adapters to this distributed switch.

 Assign uplink  Unassign adapter  View settings

Host/Physical Network Adapters	In Use by Switch	Uplink	Uplink Port Group
10.1.164.110			
On this switch			
 vmnic2 (Assigned)	--	Uplink 1	FlashStack-vDS-...
 vmnic3 (Assigned)	--	Uplink 2	FlashStack-vDS-...
On other switches/unclaimed			
 vmnic0	vSwitch0	--	--
 vmnic1	--	--	--

CANCEL

BACK

NEXT

7. Click Next.
8. Do not migrate any VMkernel ports and click Next.
9. Do not migrate any VM ports and click Next.
10. Click Finish to complete adding the ESXi host(s) to the vDS

### 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, choose the first host and click the Configure tab for that host.
2. Choose the VMkernel adapters option within the Networking section of Configure.

10.1.164.110 | ACTIONS ▾

Summary Monitor **Configure** Permissions VMs Datastores Networks Updates

**Storage** ▾

- Storage Adapters
- Storage Devices
- Host Cache Configuration
- Protocol Endpoints
- I/O Filters

**Networking** ▾

- Virtual switches
- VMkernel adapters**
- Physical adapters
- TCP/IP configuration

**VMkernel adapters**

Add Networking... Refresh Edit... Remove

Device	Network Label	Switch	IP Address	TCP/IP Stack	vMotion
vmk0	Management N...	vSwitch0	10.1.164.110	Default	Disabled

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

10.1.164.110 - Add Networking

✓ 1 Select connection type

**2 Select target device**

3 Port properties

4 IPv4 settings

5 Ready to complete

**Select target device**  
Select a target device for the new connection.

**Select an existing network**

vMotion **BROWSE ...**

**Select an existing standard switch**

BROWSE ...

**New standard switch**

MTU (Bytes) 1500

CANCEL **BACK** **NEXT**

- Click Next.
- Choose the vMotion from the Available services and click Next.

## 10.1.164.110 - Add Networking

✓ 1 Select connection type

✓ 2 Select target device

**3 Port properties**

4 IPv4 settings

5 Ready to complete

### Port properties

Specify VMkernel port settings.

### VMkernel port settings

Network label

IP settings

MTU

TCP/IP stack

### Available services

Enabled services

- vMotion
- Provisioning
- Fault Tolerance logging
- Management
- vSphere Replication
- vSphere Replication NFC
- vSAN

CANCEL

BACK

NEXT

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

## 10.1.164.110 - Add Networking

✓ 1 Select connection type

✓ 2 Select target device

✓ 3 Port properties

**4 IPv4 settings**

5 Ready to complete

### IPv4 settings

Specify VMkernel IPv4 settings.

Obtain IPv4 settings automatically

Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway  Override default gateway for this adapter

DNS server addresses

CANCEL

BACK

NEXT

10. Click Next.

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

12. Optionally, create two more vMotion VMkernel NICs to increase the speed of multiple simultaneous vMotions on this solution's 50GE vNICs.

13. Repeat steps 1-12 to create vMotion VMkernel adapters for each additional ESXi host.

## Appendix

### FlashStack with Cisco Nexus 93180YC-FX SAN Switching Configuration

#### FlashStack Cisco Nexus Switch Base Configuration

The following procedures describe how to configure the Cisco Nexus switches for use in a base FlashStack environment using the Cisco Nexus 93180YC-FX switches for both LAN and SAN switching. This procedure assumes you're using Cisco Nexus 9000 9.3(5), which is the Cisco suggested Nexus switch release at the time of this validation.

#### Set Up Initial Configuration in Cisco Nexus 93180YC-FX A

To set up the initial configuration for the Cisco Nexus A switch on <nexus-A-hostname>, follow these steps:

1. Configure the switch.



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

```
Abort Power On Auto Provisioning [yes - continue with normal setup, skip - bypass password and basic
configuration, no - continue with Power On Auto Provisioning] (yes/skip/no) [no]: yes
Disabling POAP.....Disabling POAP
poap: Rolling back, please wait... (This may take 5-15 minutes)

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

Do you want to enforce secure password standard (yes/no) [y]: Enter
Enter the password for "admin": <password>
Confirm the password for "admin": <password>
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]: Enter
Configure read-only SNMP community string (yes/no) [n]: Enter
Configure read-write SNMP community string (yes/no) [n]: Enter
Enter the switch name: <nexus-A-hostname>
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
Mgmt0 IPv4 address: <nexus-A-mgmt0-ip>
Mgmt0 IPv4 netmask: <nexus-A-mgmt0-netmask>
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway: <nexus-A-mgmt0-gw>
Configure advanced IP options? (yes/no) [n]: Enter
Enable the telnet service? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter
Type of ssh key you would like to generate (dsa/rsa) [rsa]: Enter
Number of rsa key bits <1024-2048> [1024]: Enter
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address: <global-ntp-server-ip>
Configure default interface layer (L3/L2) [L2]: Enter
Configure default switchport interface state (shut/noshut) [noshut]: shut
Enter basic FC configurations (yes/no) [n]: y
Configure default physical FC switchport interface state (shut/noshut) [shut]: Enter
Configure default switchport trunk mode (on/off/auto) [on]: auto
Configure default zone policy (permit/deny) [deny]: Enter
Enable full zoneset distribution? (yes/no) [n]: y
Configure CoPP system profile (strict/moderate/lenient/dense) [strict]: Enter
Would you like to edit the configuration? (yes/no) [n]: Enter
```

2. Review the configuration summary before enabling the configuration.



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

## Set Up Initial Configuration in Cisco Nexus 93180YC-FX B

To set up the initial configuration for the Cisco Nexus B switch on <nexus-B-hostname>, follow these steps:

1. Configure the switch.



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

```
Abort Power On Auto Provisioning [yes - continue with normal setup, skip - bypass password and basic
configuration, no - continue with Power On Auto Provisioning] (yes/skip/no) [no]: yes
Disabling POAP.....Disabling POAP
poap: Rolling back, please wait... (This may take 5-15 minutes)
```

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

```
Do you want to enforce secure password standard (yes/no) [y]: Enter
Enter the password for "admin": <password>
Confirm the password for "admin": <password>
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]: Enter
Configure read-only SNMP community string (yes/no) [n]: Enter
Configure read-write SNMP community string (yes/no) [n]: Enter
Enter the switch name: <nexus-B-hostname>
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
Mgmt0 IPv4 address: <nexus-B-mgmt0-ip>
Mgmt0 IPv4 netmask: <nexus-B-mgmt0-netmask>
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway: <nexus-B-mgmt0-gw>
Configure advanced IP options? (yes/no) [n]: Enter
Enable the telnet service? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter
Type of ssh key you would like to generate (dsa/rsa) [rsa]: Enter
Number of rsa key bits <1024-2048> [1024]: Enter
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address: <global-ntp-server-ip>
Configure default interface layer (L3/L2) [L2]: Enter
Configure default switchport interface state (shut/noshut) [noshut]: shut
Enter basic FC configurations (yes/no) [n]: y
Configure default physical FC switchport interface state (shut/noshut) [shut]: Enter
Configure default switchport trunk mode (on/off/auto) [on]: auto
Configure default zone policy (permit/deny) [deny]: Enter
Enable full zoneset distribution? (yes/no) [n]: y
Configure CoPP system profile (strict/moderate/lenient/dense) [strict]: Enter
Would you like to edit the configuration? (yes/no) [n]: Enter
```

2. Review the configuration summary before enabling the configuration.

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

## Enable Features in Cisco Nexus 93180YC-FX A and B

SAN switching requires both the SAN\_ENTERPRISE\_PKG and FC\_PORT\_ACTIVATION\_PKG licenses. Please ensure these licenses are installed on each Cisco Nexus 93180YC-FX switch. To enable the appropriate features on the Cisco Nexus switches, follow these steps:

1. Log in as admin.

2. Because basic FC configurations were entered in the setup script, feature-set fcoe has been automatically installed and enabled. Run the following commands:

```
config t
feature npiv
feature fport-channel-trunk
feature udd
feature interface-vlan
feature lacp
feature vpc
feature lldp
```

### Perform TCAM Carving and Configure Unified Ports in Cisco Nexus 93180YC-FX A and B

SAN switching requires TCAM carving for lossless fibre channel no-drop support. Also, unified ports need to be converted to fc ports. To perform TCAM carving on the Cisco Nexus switches and to convert ports 1-16 to fc, follow these steps:

1. Run the following commands:

```
hardware access-list tcam region ing-racl 1536
hardware access-list tcam region ing-ifacl 256
hardware access-list tcam region ing-redirect 256
slot 1
port 1-16 type fc
copy running-config startup-config
reload
This command will reboot the system. (y/n)? [n] y
```

2. After the switch reboots, log back in as admin. Run the following commands:

```
show hardware access-list tcam region | i i ing-racl
show hardware access-list tcam region | i i ifacl
show hardware access-list tcam region | i i ing-redirect
show int status
```

### Set System-Wide QoS Configurations in Cisco Nexus 93180YC-FX A and B

To set system-wide QoS configurations for FCoE for no-drop traffic support, follow this step on both switches:

1. Run the following commands to set global configurations:

```
config t
system qos
service-policy type queuing input default-fcoe-in-que-policy
service-policy type queuing output default-fcoe-8q-out-policy
service-policy type network-qos default-fcoe-8q-nq-policy
copy run start
```

### Configure VLANs

To configure VLANs for this deployment, run the following commands on both Cisco Nexus Switches:

```
config t
vlan <<var-ib-mgmt-vlanid>>
name IB-MGMT-VLAN
vlan <<var-native-vlan-id>>
name Native-VLAN
vlan <<var-vmote-vlan-id>>
```

```
name vMotion-VLAN
vlan <<var-application-vlan-id>>
name VM-App1-VLAN
```

Continue adding VLANs as appropriate for the environment.

### Add Interface Port Descriptions for Cisco Nexus 93180YC-FX-A

To configure port descriptions for this deployment, run the following commands on both Cisco Nexus Switches:

```
config t
interface Ethernet1/
description Network-Uplink-<<PORT>>
interface Ethernet1/
description Network-Uplink-<<PORT>>
interface Ethernet1/49
description <<var_ucs_clustername>>-A eth 1/49
interface Ethernet1/50
description <<var_ucs_clustername>>-B eth 1/49
interface Ethernet1/51
description Peer Link <<nexus-B-hostname>>-Eth1/51
interface Ethernet1/52
description Peer Link <<nexus-B-hostname>>-Eth1/52
```

### Add Interface Port Descriptions for Cisco Nexus 93180YC-FX-B

To configure port descriptions for this deployment, run the following commands on both Cisco Nexus Switches:

```
config t
interface Ethernet1/
description Network-Uplink-<<PORT>>
interface Ethernet1/
description Network-Uplink-<<PORT>>
interface Ethernet1/49
description <<var_ucs_clustername>>-A eth 1/50
interface Ethernet1/50
description <<var_ucs_clustername>>-B eth 1/50
interface Ethernet1/51
description Peer Link <<nexus-A-hostname>>-Eth1/51
interface Ethernet1/52
description Peer Link <<nexus-A-hostname>>-Eth1/52
```

## Port Channel Setup

### Configure vPC Domain Settings for Cisco Nexus 93180YC-FX-A

The vPC domain will be assigned a unique number from 1-1000 and will handle the vPC settings specified within the switches. For this deployment, vPC domain 10 is used.

```
config t
vpc domain 10
peer-switch
role priority 10
peer-keepalive destination <<vare_nexus_B_mgmt_ip>> source <<var_nexus_A_mgmt_ip>>
delay restore 150
peer-gateway
auto-recovery
ip arp synchronize
```

---

### Configure vPC Domain Settings for Cisco Nexus 93180YC-FX-B

The vPC domain will be assigned a unique number from 1-1000 and will handle the vPC settings specified within the switches. For this deployment, vPC domain 10 is used.

```
config t
vpc domain 10
peer-switch
role priority 20
peer-keepalive destination <<var_nexus_A_mgmt_ip>> source <<var_nexus_B_mgmt_ip>>
delay restore 150
peer-gateway
auto-recovery
ip arp synchronize
```

### Configure vPC Peer-Link

On Cisco Nexus 93180YX-FX-A and Cisco Nexus 93180YC-FX-B switches, configure the Port Channel member interfaces that will be part of the vPC Peer Link and then configure the Peer Link.

```
config t
interface eth 1/51-52
switchport mode trunk
switchport trunk native <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib_mgmt_vlan_id>>, <<var_vmotion_vlan_id>>, <var_application_vlan_id>
channel-group 151 mode active
no shut
interface port-channel 151
description BB08-93180YC-FX Peer Link
vpc peer-link
```



vPC and Port Channel numbers are chosen to indicate the first port in the channel. For example, a port channel starting with port ethernet 1/51 would be labeled as vpc and port-channel 151.

---

### Configure Port-Channel to Fabric Interconnect A

On Cisco Nexus 93180YX-FX-A and Cisco Nexus 93180YC-FX-B switches, configure the Port Channel member interfaces that will be part of the vPC link to Fabric Interconnect A.

```
config t
interface eth 1/49
switchport mode trunk
switchport trunk native <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib_mgmt_vlan_id>>, <<var_vmotion_vlan_id>>, <var_application_vlan_id>
channel-group 149 mode active
no shut
interface port-channel 149
description <<var_ucs_clustername>>-A
vpc 149
```

### Configure Port-Channel to Fabric Interconnect B

On Cisco Nexus 93180YX-FX-A and Cisco Nexus 93180YC-FX-B switches, configure the Port Channel member interfaces that will be part of the vPC link to Fabric Interconnect B.

```
config t
interface eth 1/50
switchport mode trunk
switchport trunk native <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib_mgmt_vlan_id>>, <<var_vmotion_vlan_id>>, <var_application_vlan_id>
channel-group 150 mode active
no shut
interface port-channel 150
description <<var_ucs_clustername>>-B
vpc 150
```

### Configure Port-Channel to Upstream Network

On Cisco Nexus 93180YX-FX-A and Cisco Nexus 93180YC-FX-B switches, configure the Port Channel member interfaces that will be part of the vPC link to the upstream network.

```
config t
interface eth 1/53-54
switchport mode trunk
switchport trunk native <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib_mgmt_vlan_id>>, <<var_vmotion_vlan_id>>, <var_application_vlan_id>
channel-group 153 mode active
no shut
interface port-cahnnel 153
description Uplink
vpc 153
```

### Configure Fibre Channel Ports in Cisco Nexus 93180YC-FX A

To configure individual ports and port-channels for switch A, follow this step:

From the global configuration mode, run the following commands:

```
interface fc1/1
switchport description <<var_flasharray_hostname>>-CT0:FC0
port-license acquire
switchport speed 32000
switchport trunk mode off
no shutdown
exit

interface fc1/2
switchport description <<var_flasharray_hostname>>-CT1:FC0
port-license acquire
switchport speed 32000
switchport trunk mode off
no shutdown
exit

interface fc1/5
switchport description <ucs-clustername>-a:1/3
port-license acquire
channel-group 15
no shutdown
exit

interface fc1/6
switchport description <ucs-clustername>-a:1/4
port-license acquire
channel-group 15
no shutdown
exit
```

```
interface san-port-channel15
channel mode active
switchport trunk allowed vsan <vsan-a-id>
switchport description <ucs-clustername>-a
switchport speed 32000
no shutdown
exit
```



If VSAN trunking is not being used between the Cisco UCS Fabric Interconnects and the MDS switches, do not enter “switchport trunk allowed vsan <vsan-a-id>” for interface port-channel15. The default setting of switchport trunk mode auto is being used for the port channel.

### Configure Fibre Channel Ports in Cisco Nexus 93180YC-FX B

To configure individual ports and port-channels for switch B, follow this step:

From the global configuration mode, run the following commands:

```
interface fc1/1
switchport description <<var_flasharray_hostname>>-CT0:FC1
port-license acquire
switchport speed 32000
switchport trunk mode off
no shutdown
exit

interface fc1/2
switchport description <<<var_flasharray_hostname>>-CT1:FC1
port-license acquire
switchport speed 32000
switchport trunk mode off
no shutdown
exit

interface fc1/5
switchport description <ucs-clustername>-b:1/3
port-license acquire
channel-group 15
no shutdown
exit

interface fc1/6
switchport description <ucs-clustername>-b:1/4
port-license acquire
channel-group 15
no shutdown
exit

interface san-port-channel15
channel mode active
switchport trunk allowed vsan <vsan-b-id>
switchport description <ucs-clustername>-b
switchport speed 32000
no shutdown
exit
```



If VSAN trunking is not being used between the Cisco UCS Fabric Interconnects and the Cisco Nexus switches, do not enter “switchport trunk allowed vsan <vsan-b-id>” for interface port-channel15. The default setting of switchport trunk mode auto is being used for the port channel.

---

## Create VSANs in Cisco Nexus 93180YC-FX A

To create the necessary VSANs for fabric A and add ports to them, follow these steps:

From the global configuration mode, run the following commands:

```
vsan database
vsan <<var_vsan_a_id>>
vsan <<var_vsan_a_id>> name FlashStack-A
vsan <<var_vsan_a_id>> interface fc 1/1-2
vsan <<var_vsan_a_id>> interface fc 1/5-6
vsan <<var_vsan_a_id>> interface po15
```

## Create VSANs in Cisco Nexus 93180YC-FX B

To create the necessary VSANs for fabric B and add ports to them, follow these steps:

From the global configuration mode, run the following commands:

```
vsan database
vsan <<var_vsan_b_id>>
vsan <<var_vsan_b_id>> name FlashStack-B
vsan <<var_vsan_b_id>> interface fc 1/1-2
vsan <<var_vsan_b_id>> interface fc 1/5-6
vsan <<var_vsan_a_id>> interface po15
```

## Switch Testing Commands

The following commands can be used to check for correct switch configuration:



Some of these commands need to run after further configuration of the FlashStack components are complete to see complete results.

---

```
show run
show vpc
show port-channel summary
show ntp peer-status
show cdp neighbors
show lldp neighbors
show run int
show int
show udld neighbors
show int status
show int brief
show flogi database
```

## Cisco Nexus 93180YC-FX Zoning

This section explains how to configure Device Aliases, Zoning, and Zonesets in the Cisco Nexus 93180YC-FX switches for use in a FlashStack environment. Follow the steps precisely because failure to do so could result in an improper configuration.

### Create Device Aliases in Cisco Nexus 93180YC-FX A

To create device aliases for Fabric A that will be used to create zones, follow these steps:

Log in as admin and from the global configuration mode, run the following commands:

```
conf t
device-alias database
device-alias name FlashArray-CT0FC0 pwnn 52:4A:93:7C:2B:9B:9F:00
device-alias name FlashArray-CT1FC0 pwnn 52:4A:93:7C:2B:9B:9F:10
device-alias name VM-Host-FC-01-A pwnn 20:00:00:25:b5:01:0a:00
device-alias name VM-Host-FC-02-A pwnn 20:00:00:25:b5:01:0a:01
device-alias commit
show device-alias database
```

### Create Device Aliases in Cisco Nexus 93180YC-FX B

To create device aliases for Fabric B that will be used to create zones, follow these steps:

Log in as admin and from the global configuration mode, run the following commands:

```
conf t
device-alias database
device-alias name FlashArray-CT0FC1 pwnn 52:4A:93:7C:2B:9B:9F:01
device-alias name FlashArray-CT1FC1 pwnn 52:4A:93:7C:2B:9B:9F:11
device-alias name VM-Host-FC-01-B pwnn 20:00:00:25:b5:01:0b:00
device-alias name VM-Host-FC-02-B pwnn 20:00:00:25:b5:01:0b:01
device-alias commit
show device-alias database
```

### Create Zones and Zoneset in Cisco Nexus 93180YC-FX A

To create the required zones and zoneset on Fabric A, run the following commands:

```
conf t

zone name VM-Host-FC-01-A vsan 100
member device-alias VM-Host-FC-01-A
member device-alias FlashArray-CT0FC0
member device-alias FlashArray-CT1FC0
exit

zone name VM-Host-FC-02-A vsan 100
member device-alias VM-Host-FC-02-A
member device-alias FlashArray-CT0FC0
member device-alias FlashArray-CT1FC0
exit

zoneset name FlashStack-Zoneset-A vsan 100
member VM-Host-FC-01-A
member VM-Host-FC-02-A
zoneset activate name FlashStack-Zoneset-A vsan 100
zone commit vsan 100
copy run start
```



Since Smart Zoning is not currently supported with Cisco Nexus 93180YC-FX, single-initiator, multiple-target zones are being used for each host.

### Create Zones and Zoneset in Cisco Nexus 93180YC-FX B

To create the required zones and zoneset on Fabric B, run the following commands:

```
conf t

zone name VM-Host-FC-01-B vsan 200
member device-alias VM-Host-FC-01-B
member device-alias FlashArray-CT0FC1
```



---

```
member device-alias FlashArray-CT1FC1
exit

zone name VM-Host-FC-02-B vsan 200
member device-alias VM-Host-FC-02-B
member device-alias FlashArray-CT0FC1
member device-alias FlashArray-CT1FC1
exit

zoneset name FlashStack-Zoneset-B vsan 200
member VM-Host-FC-01-B
member VM-Host-FC-02-B
zoneset activate name FlashStack-Zoneset-B vsan 200
zone commit vsan 200
copy run start
```

---

## About the Author

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 author would like to thank:

- John George, Technical Marketing Engineer, Cisco Systems, Inc.
- Craig Waters, Solutions Architecture and Product Management, Pure Storage, Inc.

---

## Feedback

For comments and suggestions about this guide and related guides, join the discussion on [Cisco Community](https://cs.co/en-cvds) at <https://cs.co/en-cvds>.

---

**Americas Headquarters**

Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**

Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**

Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned 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. (1110R)