cisco.



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

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

Last Updated: December 23, 2019



About the Cisco Validated Design Program

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

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

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

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

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

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

© 2019 Cisco Systems, Inc. All rights reserved.

Table of Contents

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

Configure Cisco UCS Call Home	
Configure NTP	
Configure Cisco UCS Servers	
Edit Chassis Discovery Policy	
Enable Server and Uplink Ports	
Acknowledge Cisco UCS Chassis	
Create Pools	
Set Packages and Policies	
Configure Cisco UCS LAN Connectivity	
Create Uplink Port Channels	
Create VLANS	
Create vNIC Templates	
Create LAN Connectivity Policy	
Configure FC SAN Connectivity	
Create Boot Policy	
Create Service Profile Templates	
Create Service Profiles	
Claim in Intersight	
MDS Fabric Zoning	
Create Device Aliases	
MDS Zoning	
Create and Activate Zoneset	
FlashArray Storage Deployment	
Host Port Identification	
Host Registration	
Create Host Group	
Private Boot Volumes for Each ESXi Host	
Configure Storage Policy Based Management	
VMware vSphere Deployment	
ESXi Installation	
Download Cisco Custom Image for ESXi 6.7 U1	
Log into Cisco UCS 6454 Fabric Interconnect	
Set Up VMware ESXi Installation	
Install ESXi	
Set Up Management Networking for ESXi Hosts	
Create FlashStack Datacenter	
Create VMware vDS for Infrastructure and Application Traffic	

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



Executive Summary

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

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

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

Solution Overview

Introduction

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

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

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

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

Audience

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

Purpose of this Document

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

The design that will be implemented is discussed in the <u>FlashStack Virtual Server Infrastructure for VMware</u><u>vSphere 6.7 Update 1 Design Guide</u>.

Solution Summary

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

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

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



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

The reference hardware configuration includes:

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

• One Pure Storage FlashArray//X70 R2

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

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

Deployment Hardware and Software

Software Revisions

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

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

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

Layer	Device Image		Comments
Compute	Cisco UCS Fabric Interconnects 6400 Series, UCS B-200 M5, UCS C-220 M5	4.0(2b)	Includes Cisco UCS IOM 2208 and Cisco VIC 1400 Series
Network	Cisco Nexus 9000 NX-OS	7.0(3)17(5)	
Storage	Pure Storage FlashArray//X70 R2	5.1.9	
	Cisco MDS 9132T	8.3(2)	
Software	Cisco UCS Manager	4.0(2b)	
	VMware vSphere ESXi Cisco Custom ISO	6.7 U1	
	VMware vSphere nenic Driver for ESXi	1.0.26.0	
	VMware vCenter	6.7 U1	

Table 1 Software Revisions

Layer	Device	Image	Comments
	Pure Storage vSphere Web Client Plugin	3.1.1	

Configuration Guidelines

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

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

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

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

Table 2 Required VLANs

Table 3 Infrastructure Servers

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

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

Table 4 Configuration Variables

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

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

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

Physical Topology

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

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

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



Figure 2 FlashStack Cabling in the Validate Topology

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

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

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

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

Local Device	Local Port	Connection	Remote Device	Remote port
Cisco Nexus 9336C- EX2-B	Eth 1/31	100Gbe	Cisco UCS 6454-A	Eth 1/50
	Eth 1/32	100Gbe	Cisco UCS 6454-B	Eth 1/50
	Eth 1/33	100Gbe	Cisco Nexus 9336C- FX2-A	Eth 1/33
	Eth 1/34	100Gbe	Cisco Nexus 9336C- FX2-A	Eth 1/33
	Eth 1/35	10Gbe or 40Gbe or 100Gbe	Upstream Network Switch	Any
	Eth 1/36	10Gbe or 40Gbe or 100Gbe	Upstream Network Switch	Any
	Mgmt0	Gbe	Gbe Management Switch	Any

Table 7 Cisco UCS-6545-A Cabling Information

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

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

Table 8 Cisco UCS-6545-B Cabling Information

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

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

Table 9 Cisco MDS-9132T-A Cabling Information

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

Table 10 Cisco MDS-9132T-B Cabling Information

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

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

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

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

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

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

Network Switch Configuration

Network Configuration

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



Physical Connectivity

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

Cisco Nexus Basic System Configuration Dialog

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

Cisco Nexus Basic System Configuration Dialog

Abort Auto Provisioning and continue with normal setup $\ensuremath{(yes/no)[n]: y}$

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

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

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

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

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

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

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

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

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

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

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

Enter the switch name : <<var_nexus_A_hostname>>

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

Mgmt0 IPv4 address : <<var_nexus_A_mgmt_ip>>

Mgmt0 IPv4 netmask : <<var oob mgmt mask>>

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

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

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

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

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

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

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

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

NTP server IPv4 address : <<var_oob_ntp>>

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

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

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

The following configuration will be applied:

password strength-check

switchname AA12-9336C-A

vrf context management

ip route 0.0.0.0/0 192.168.164.254

exit

no feature telnet ssh key rsa 2048 force feature ssh ntp server 172.26.163.254 system default switchport no system default switchport shutdown copp profile strict interface mgmt0 ip address 192.168.164.90 255.255.252.0 no shutdown Would you like to edit the configuration? (yes/no) [n]: no

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

Cisco Nexus Switch Configuration

Enable Features and Settings

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

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

٨

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

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

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

Configure Global Settings

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

AA12-9336C-A&B (config) # port-channel load-balance src-dst l4port AA12-9336C-A&B (config) # ip route 0.0.0.0/0 <**var_ib-mgmt-vlan_gateway>>** AA12-9336C-A&B (config) # ntp server <**var_oob_ntp>>** use-vrf management AA12-9336C-A&B (config) # ntp master 3

Configure VLANs

Run the following commands on both switches to create VLANs:

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

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

Add Interface Port Descriptions

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

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

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

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

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

Configure vPC Domain Settings

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

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

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

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

Configure vPC Peer-Link

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

AA12-9336C-A&B (config)# int eth 1/33-34 AA12-9336C-A&B (config-if-range)# switchport mode trunk AA12-9336C-A&B (config-if-range)# switchport trunk native vlan 2 AA12-9336C-A&B (config-if-range) # switchport trunk allowed vlan 215,1110,1120,1130,1301-1303 AA12-9336C-A&B (config-if-range) # channel-group 133 mode active AA12-9336C-A&B (config-if-range) # no shut AA12-9336C-A&B (config-if-range) # int port-channel 133 AA12-9336C-A&B (config-if) # description AA12-9336C Peer Link AA12-9336C-A&B (config-if) # vpc peer-link

Configure Port-Channels

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

Nexus Connection vPC to UCS Fabric Interconnect A

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

Nexus Connection vPC to UCS Fabric Interconnect B

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

Nexus Connection vPC to Upstream Network

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

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

Storage Configuration

Pure Storage FlashArray//X70 R2 Configuration

FlashArray Initial Configuration

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

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

Table 13 FlashArray Setup Information

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

Add an Alert Recipient

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

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

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

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

To add an alert recipient, follow these steps:

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

۲	Dashboard	System	Network	Users	Software
۲	Storage	Array cspg-rt	p-1 ⊡		
	Analysis Performance Capacity Replication	Alert Wa	tchers		
✤	Health				
*	Settings				
		pure-alei	rts@domain.com		+

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

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

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

Alert Routing	2
Relay Host No relay host configured	
Username No username available	
Password No password available	
Sender Domain cisco.com	

Configure Pure1 Support

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

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

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

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

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

	• Settings	
Oashboard	Alert Watchers	
🤨 Storage		(
Analysis		(
Performance Capacity Replication		
🛞 Health	New Alert Watcher	•
settings	Syslog Servers	Test
Help Terms Log Out	{protocol]://{host]:{port}	t
	Pure1 Support	
	Phone Home	Enabled
	Manual Phone Home	
	Today's Logs 🗸	Send Now
Array cspg-rtp-1	- Remote Assist	Disconnected
Purity//FA 5.1.9	Support Logs	Download from
Logged in as pureuser GMT-04:00 (EDT)	Today's Logs 🔹	CT0 CT1

Configure the Domain Name System (DNS) Server IP Addresses

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

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

P	PURESTORAGE [®] 4	Settings	
۹	Dashboard	System Network Users Software	
۲	Storage	Subnets & Interfaces	
Q	Analysis Performance Capacity Replication	Subnet VLAN	Gateway 192.168.101.253 192.168.102.253
÷	Health	•	10.2.164.254
\$	Settings	-	10.10.164.254
Help		- - -	10.10.164.254
Log O	, but	DNS Settings	ß
		Domain flashstack.cisco.com DNS Server(s) 10.1.164.9	

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

4. Click Save.

Directory Service Sub-view

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

۹	Dashboard	System	Network	Users	Software					
۲	Storage	Users							1-2 o	f2 < > 🚦
~		Name 🔺			Role	١	Туре	Public Key	API Token	
Щ,	Analysis Performance	pureuser			array_admin	ŀ	ocal		••••	:
	Capacity	root				ŀ	ocal		****	:
	Replication	Directory	Sonvico							Text D
€	Health	Directory	Service							lest 🛛
		Enabled	False				Array Admin Group	-		
*	Settings	URI					Storage Admin Group	-		
		Base DN	-				Read-only Group	-		
		Bind User	-				Check Peer	False		
Help		Bind Passw	rord -				CA Certificate	- Edit		
Terms	5	Group Base	- é							
Log C	Dut									

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 uses cannot alter the state of the array.
- Storage Admin Group. Storage Admin users have all the privileges of Read Only users, plus the ability to run commands related to storage operations, such as administering volumes, hosts, and host groups. Storage Admin users cannot perform operations that deal with global and system configurations.
- Array Admin Group. Array Admin users have all the privileges of Storage Admin users, plus the ability to perform array-wide changes. In other words, Array Admin users can perform all FlashArray operations.
- 1. Select Settings > Users.
- 2. Select the 🗹 icon in the Directory Services panel:
 - a. Enabled: Select the check box to leverage the directory service to perform user account and permission level searches.
 - URI: Enter the comma-separated list of up to 30 URIs of the directory servers. The URI must include a URL scheme (Idap, or Idaps for LDAP over SSL), the hostname, and the domain. You can optionally specify a port. For example, Idap://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 Idap://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.
- Read Only Group: Common Name (CN) of the configured directory service group containing users with read-only privileges on the FlashArray. The name should be the Common Name of the group without the "CN=" specifier. If the configured groups are not in the same OU, also specify the OU. For example, " purereadonly,OU=PureStorage", where purereadonly is the common name of the directory service group.
- j. Check Peer: Select the check box to validate the authenticity of the directory servers using the CA Certificate. If you enable Check Peer, you must provide a CA Certificate.
- k. CA Certificate: Enter the certificate of the issuing certificate authority. Only one certificate can be configured at a time, so the same certificate authority should be the issuer of all directory server certificates. The certificate must be PEM formatted (Base64 encoded) and include the "----BEGIN CERTIFICATE-----" and "----END CERTIFICATE-----" lines. The certificate cannot exceed 3000 characters in total length.
- 3. Click Save.
- 4. Click Test to test the configuration settings. The LDAP Test Results pop-up window appears. Green squares represent successful checks. Red squares represent failed checks.

SSL Certificate Sub-view

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

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

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

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

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

CA-Sign Certificate

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

Construct Certificate Signing Request ×			
Country	Two-letter ISO country code		
State/Province	State, province, country or region		
Locality	Full city name		
Organization	Pure Storage, Inc.		
Organization Unit	Pure Storage, Inc.		
Common Name	FQDN or management IP address of the server		
Email	Email address		
	Cancel Create		

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.
Choose File No file chosen
Choose File No file chosen
Choose File No file chosen
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.

MDS Fabric Configuration

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

Physical Connectivity

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

Cisco MDS Basic System Configuration Dialog

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

Cisco MDS Basic System Configuration Dialog

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

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

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

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

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

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

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

38

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

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

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

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

Enter the switch name : <<var mds A mgmt hostname>>

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

Mgmt0 IPv4 address : <<var mds A mgmt ip>>

Mgmt0 IPv4 netmask : <<var oob mgmt mask>>

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

IPv4 address of the default gateway : <<var oob gateway>>

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

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

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

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

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

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

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

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

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

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

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

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

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

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

NTP server IPv4 address : <<var oob ntp>>

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

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

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

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

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

```
Configure default zone mode (basic/enhanced) [basic]: enhanced
The following configuration will be applied:
 password strength-check
  switchname MDS-9132T-A
  interface mgmt0
    ip address 10.2.164.92 255.255.255.0
    no shutdown
  ip default-gateway 10.2.164.254
  ssh key rsa 1024 force
  feature ssh
  no feature telnet
  system timeout congestion-drop 500 logical-type edge
  system timeout congestion-drop default logical-type core
  feature http-server
  ntp server 172.26.163.254
  system default switchport shutdown
  system default switchport trunk mode on
  no system default zone default-zone permit
  system default zone distribute full
  system default zone mode enhanced
```

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

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

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

Cisco MDS Configuration

```
Enable Features and Settings
```

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

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

Create VSAN and Interfaces

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

mds-9132T-a(config) # vsan database mds-9132T-a(config-vsan-db) # vsan <<var vsan a id>> mds-9132T-a(config-vsan-db)# vsan <<var vsan a id>> name Fabric-A mds-9132T-a(config-vsan-db)# exit mds-9132T-a(config) # zone smart-zoning enable vsan <<var vsan a id>> mds-9132T-a(config) # vsan database mds-9132T-a(config-vsan-db)# vsan <<var vsan a id>> interface fc1/1-4 mds-9132T-a(config-vsan-db) # vsan <<var vsan a id>> interface fc1/15-18 mds-9132T-a(config-vsan-db) # vsan <<var vsan a id>> interface po1 mds-9132T-a(config-vsan-db)# exit mds-9132T-a(config) # int fc1/1-4 mds-9132T-a(config-if) # no shut mds-9132T-a(config) # int fc1/15-18 mds-9132T-a(config-if) # no shut mds-9132T-a(config-if) # exit Repeat these commands on MDS 9132T B using the Fabric B appropriate VSAN ID: mds-9132T-b(config) # vsan database mds-9132T-b(config-vsan-db)# vsan <<var vsan b id>> mds-9132T-b(config-vsan-db)# vsan <<var vsan b id>> name Fabric-B mds-9132T-b(config-vsan-db)# exit mds-9132T-b(config)# zone smart-zoning enable vsan <<var vsan b id>> mds-9132T-b(config) # vsan database mds-9132T-b(config-vsan-db) # vsan <<var vsan b id>> interface fc1/1-4 mds-9132T-b(config-vsan-db) # vsan <<var vsan b id>> interface fc1/15-18 mds-9132T-b(config-vsan-db)# vsan <<var vsan b id>> interface po2 mds-9132T-b(config-vsan-db) # exit mds-9132T-b(config) # int fc1/1-4 mds-9132T-b(config-if) # no shut mds-9132T-b(config) # int fc1/15-18 mds-9132T-b(config-if) # no shut mds-9132T-b(config-if) # exit

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

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

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

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

Save all configuration on both MDS Switches.

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

Compute Configuration

Cisco UCS Compute Configuration

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



```
Figure 4 Compute Configuration Workflow
```

Physical Connectivity

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

Cisco UCS Basic System Configuration Dialog

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

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

```
UCSM image signature verification successful
---- Basic System Configuration Dialog ----
This setup utility will guide you through the basic configuration of
```

the system. Only minimal configuration including IP connectivity to the Fabric interconnect and its clustering mode is performed through these steps. Type Ctrl-C at any time to abort configuration and reboot system. To back track or make modifications to already entered values, complete input till end of section and answer no when prompted to apply configuration. Enter the configuration method. (console/gui) ? console Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup You have chosen to setup a new Fabric interconnect. Continue? (y/n): yEnforce strong password? (y/n) [y]: y Enter the password for "admin": Confirm the password for "admin": Is this Fabric interconnect part of a cluster(select 'no' for standalone)? (yes/no) [n]: yes Enter the switch fabric (A/B) []: A Enter the system name: <var ucs clustername>> Physical Switch Mgmt0 IP address : <<var ucs a mgmt ip>> Physical Switch Mgmt0 IPv4 netmask : <<var oob mgmt mask>> IPv4 address of the default gateway : <<var oob gateway>> Cluster IPv4 address : <<var ucs mgmt vip> Configure the DNS Server IP address? (yes/no) [n]: yes DNS IP address : <<var nameserver ip>> Configure the default domain name? (yes/no) [n]: yes Default domain name : <<var dns domain name>> Join centralized management environment (UCS Central)? (yes/no) [n]: no Following configurations will be applied: Switch Fabric=A System Name=AA12-UCS-6454 Enforced Strong Password=yes Physical Switch Mgmt0 IP Address=10.2.164.51 Physical Switch Mgmt0 IP Netmask=255.255.255.0 Default Gateway=10.2.164.254 Ipv6 value=0 DNS Server=10.1.164.9 Domain Name=flashstack.cisco.com Cluster Enabled=yes Cluster IP Address=10.2.164.50 NOTE: Cluster IP will be configured only after both Fabric Interconnects are initialized. UCSM will be functional only after peer FI is configured in clustering mode. Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no):yes

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

---- Basic System Configuration Dialog ----This setup utility will guide you through the basic configuration of the system. Only minimal configuration including IP connectivity to

```
the Fabric interconnect and its clustering mode is performed through these steps.
  Type Ctrl-C at any time to abort configuration and reboot system.
  To back track or make modifications to already entered values,
  complete input till end of section and answer no when prompted
  to apply configuration.
  Enter the configuration method. (console/qui) ? console
  Installer has detected the presence of a peer Fabric interconnect. This Fabric interconnect will be
added to the cluster. Continue (y/n) ? y
  Enter the admin password of the peer Fabric interconnect:
    Connecting to peer Fabric interconnect... done
   Retrieving config from peer Fabric interconnect... done
   Peer Fabric interconnect Mgmt0 IPv4 Address: 10.2.164.51
    Peer Fabric interconnect Mgmt0 IPv4 Netmask: 255.255.255.0
   Cluster IPv4 address
                                  : 10.2.164.50
    Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv4 Address
  Physical Switch Mgmt0 IP address : <<var_ucs_b_mgmt_ip>>
  Local fabric interconnect model(UCS-FI-6454)
  Peer fabric interconnect is compatible with the local fabric interconnect. Continuing with the install-
er...
```

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

Cisco UCS Manager Configuration

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

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

Upgrade Cisco UCS Manager to Version 4.0(2b)

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

Enable Anonymous Reporting

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

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

Cisco Systems, Inc. will be collectin sent to Cisco Smart Call Home sen and improvements that will most be if you decide to enable this feature in the Call Home settings under the View Sample Data Do you authorize the disclosure of @Yes No SMTP Server	ng feature conf ver anonymous enefit our custo in future, you c a Admin tab.	iguration and i sly. This data h mers. can do so from tion to Cisco s	usage statistics which will be lelps us prioritize the features the "Anonymous Reporting" Smart CallHome?
Host (IP Address or Hostname):			
Port:	25		
Don't show this message again.			OK Cancel

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

Configure Cisco UCS Call Home

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

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

Æ	Communication Management	Communication Management / Call Home	
	 Communication Management 	General Profiles Call Home Policies System Inventory Anonymous Reporting Events FSM	
	Call Home	Admin	
윪	Communication Services	Admin	
	DNS Management	State : Off On	
	Management Interfaces	Switch Priority : Debugging	
-	 UCS Central 	Throttling : Off On	
_		States	
		Contact Information	
		Contact :	
20		Phone :	
		Email :	
		Address ·	
		lds	
		Customer ID :	
		Contract ID :	
		Site ID :	
		Email Addresses	
		From :	
		Reply To :	
		SMTP Server	
		Host (IP Address or Hostname) :	
		Port : 25	

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.

æ	Time Zone Management	Time Zone Management / Time	zone
8	▼ Time Zone Management	General Events	
	Timezone	Actions	Properties
56		Add NTP Server	Time Zone : za/New_York (Eastern Time) V
.	<not set=""></not>		
	Africa/Abidjan		
	Africa/Accra		
	Africa/Addis_Ababa		
	Africa/Algiers		
20	Africa/Asmara		
	Africa/Bamako		
	Africa/Bangui		
	Africa/Banjul		
	Africa/Bissau		🕀 Add 前 Delete 🌒 Info
	Africa/Blantyre		
	Africa/Brazzaville		
	Africa/Bujumbura		
	Africa/Cairo		
	Africa/Casablanca		
	Africa/Ceuta (Ceuta 8	& Melilla)	
	Africa/Conakry		
	Africa/Dakar		
	Africa/Dar_es_Salaar	n	
	Africa/Djibouti		
	Africa/Douala		
	Africa/EI_Aaiun		Save Changes Reset Values

- 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.

Add NTP Server	? ×
NTP Server : 172.26.163.254]
	OK Cancel

7. Click OK.

Configure Cisco UCS Servers

Edit Chassis Discovery Policy

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

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

Æ	Policies 👻	Policies	
	 Policies 	Policies	
-	Port Auto-Discovery Policy	Global Policies Autoconfig Policies Server Inheritance Policies Server Discovery Policies	5
格		Chassis/FEX Discovery Policy	
		Action : 4 Link	
=		Link Grouping Preference : None Port Channel	

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

Enable Server and Uplink Ports

To enable server and uplink ports, follow these steps:

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

Æ	Fabric Interconnects Fabric Interconnect / Fabric Interconnect A (s / Fixed Module / Ethernet Ports Ethernet Ports										
=	Fabric Interconnects Fabric Interconnect A (subordinate)	Ty Advanced Filte	er 🛧 Export	🖶 Print 🔽 All	✓ Unconfigured	Vetwork VS	erver 🗸 FCoE Up	link 🗸 Unified Upl	link	>>	¢
0	► Fans	Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status	Admin State	Peer	
88	▼ Fixed Module	1	0	6	00:DE:FB:FF:	Unconfigured	Physical	V Sfp Not Pr	Disabled		
=	Ethernet Ports	1	0	7	00:DE:FB:FF:	Unconfigured	Physical	V Sfp Not Pr	Disabled		
	FC Ports	1	0	8	00:DE:FB:FF:	Unconfigured	Physical	🔻 Sfp Not Pr	Disabled		
	▶ PSUs	1	0	9	00:DE:FB:FF:	Unconfigured	Physical	Down	Disabled		
_	 Fabric Interconnect B (primary) 	1	0	10	00:DE:FB:FF:	Unconfigured	Physical	Down	Disabled		
		1	0	11	00:DE:FB:FF:	Unconfigured	Physical	Down	Disabled		
20		1	0	12	Enable		vsical	Down	Disabled		
		1	0	13			/sical	V Sfp Not Pr	Disabled		
		1	0	14	Configure as Se	ver Port	/sical	V Sfp Not Pr	Disabled		
		1	0	15	Configure as Up	ink Port	/sical	V Sfp Not Pr	Disabled		
		1	0	16	Configure as FC	oE Uplink Port	/sical	V Sfp Not Pr	Disabled		
		1	0	17	Configure as FC	oE Storage Port	/sical	🕈 Up	Enabled	sys/rack-unit.	***
		1	0	18	Unconfigure	pliance Port	/sical	V Sfp Not Pr	Disabled		
		1	0	19			/sical	🕇 Up	Enabled	sys/rack-unit.	
		1	0	20			/sical	V Sfp Not Pr	Disabled		
		1	0	21			/sical	V Sfp Not Pr	Disabled		
		1	0	22	00:DE:FB:FF:	Unconfigured	Physical	V Sfp Not Pr	Disabled		
		1	0	23	00:DE:FB:FF:	Unconfigured	Physical	V Sfp Not Pr	Disabled		
								5	ave Changes	Reset Val	ues

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

æ	Fabric Interconnects	Fabric Interco	nnects / Fabric	Interconnect A (subordinate) / Fixe	d Module / Ether	rnet Ports				
B	▼ Fabric Interconnects	Ethernet Port	s								
	▼ Fabric Interconnect A (subordinate)	Te Advanced F	ilter 🔶 Export	🖶 Print 🔽 Al	Unconfigured	Vetwork VS	erver VFCoE Up	link 🔽 Unified Upl	ink	>>	₽
묬	 Fans 	Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status	Admin State	Peer	
	▼ Fixed Module	1	0	37	00:DE:FB:FF:	Unconfigured	Physical	V Sfp Not Pr	Disabled		
<u>.</u>	Ethemet Ports	1	0	38	00:DE:FB:FF:	Unconfigured	Physical	V Sfp Not Pr	Disabled		
	► FC Ports	1	0	39	00:DE:FB:FF:	Unconfigured	Physical	V Sfp Not Pr	Disabled		
	► PSUs	1	0	40	00:DE:FB:FF:	Unconfigured	Physical	V Sfp Not Pr	Disabled		
_	 Fabric Interconnect B (primary) 	1	0	41	00:DE:FB:FF:			Sfp Not Pr	Disabled		
		1	0	42	00:DE:FB:FF:			Sfp Not Pr	Disabled		
20		1	0	43	00:DE:FB:FF:	Configure as U	Iplink Port	Sfp Not Pr	Disabled		
		1	0	44	00:DE:FB:FF:	Configure as F	CoE Uplink Port	Sfp Not Pr	Disabled		
		1	0	45	00:DE:FB:FF:	Configure as F	CoE Storage Port	Sfp Not Pr	Disabled		
		1	0	46	00:DE:FB:FF:	Configure as A	ppliance Port	Sfp Not Pr	Disabled		
		1	0	47	00:DE:FB:FF:			Sfp Not Pr	Disabled		
	2	1	0	48	00:DE:FB:FF:			Sfp Not Pr	Disabled		
		1	0	49	00:DE:FB:FF:			Admin Do	Disabled		
		1	0	50	00:DE:FB:FF:			Admin Do	Disabled		
		1	0	51	00:DE:EB:EE:	Linconfigured	Physical	V Cfe Net Dr.	Disabled		
		1	0	52	00-DE-EP-EE-	Unconfigured	Dhueical	• Stp Not Pr	Disabled		
		1	0	52	00.DE.FD.FF.	Unconfigured	Dhusical	Stp Not Pr	Disabled		
			0	55	00.DE.FD.FF	Unconligured	Physical	▼ Stp Not Pr	Disabled		
			U	54	00:DE:FB:FF:	Unconfigured	Physical	♥ Sfp Not Pr	 Disabled 		

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

Acknowledge Cisco UCS Chassis

To acknowledge all Cisco UCS chassis, follow these steps:

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



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

Create Pools

Create MAC Address Pools

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

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

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

- 3. Right-click MAC Pools under the root organization.
- 4. Select Create MAC Pool to create the MAC address pool.
- 5. Enter MAC_Pool_A as the name of the MAC pool.
- 6. Optional: Enter a description for the MAC pool.
- 7. Select Sequential as the option for Assignment Order.

		Create MAC Pool	? ×
1	Define Name and Description	Name : MAC_Pool_A	
2	Add MAC Addresses	Description : Assignment Order : O Default Sequential	
		< Prev Next > Finish Ca	incel

- 8. Click Next.
- 9. Click Add.
- 10. Specify a starting MAC address.

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

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



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

		Create MAC Pool	? ×
0	Define Name and Description	Name : MAC_Pool_B	
2	Add MAC Addresses	Assignment Order : O Default Sequential	
		< Prev Next > Finish C	ancel

- 19. Click Next.
- 20. Click Add.

B

21. Specify a starting MAC address.

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

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

		Create MAC Pool	? ×
	Define Name and Descripsion	+ - 🏹 Advanced Filter 🛧 Export 🚔 Print	¢
2	Add MAC Addresses	Name From To	
	Create a Block of N	AC Addresses ? ×	
	First MAC Address : 00:25:85: To ensure uniqueness of MACs in t prefix: 00:25:85:xx:xx:xx	91:1B:00 Size : 32 he LAN fabric, you are strongly encouraged to use the following MAC OK	
		🕀 Add 👘 Delete	
		< Prev Next > Finish Can	cel

23. Click OK.

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

Create WWNN Pool

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

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

		Create WWNN Pool	? ×
0	Define Name and Description	Name : WWNN_Pool	
2	Add WWN Blocks	Description : Assignment Order : Default Sequential	
		< Prev Next > Finish Ca	ncel

- 8. Click Next.
- 9. Click Add.

0

10. Modify the From field as necessary for the UCS Environment.

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

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

Create WWN Block	? ×
From : 20:00:00:25:85:01:00:00 Size : 32 \$ To ensure uniqueness of WWNs in the SAN fabric, you are strongly encouraged the following WWN prefix:	d to use
20:00:25:b5:xx:xx:xx	
ОК Сапсе	ł

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

Create WWPN Pools

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

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

		Create WWPN Pool	? ×
0	Define Name and Description	Name : WWPN_Pool_A	
2	Add WWN Blocks	Description : Assignment Order : O Default Sequential	
		< Prev Next > Finish Ca	ncel

- 9. Click Next.
- 10. Click Add.
- 11. Specify a starting WWPN

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

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

Create WWN Block	<
From : 20:00:00:25:B5:01:0A:00 Size : 32	
To ensure uniqueness of WWNs in the SAN fabric, you are strongly encouraged to us the following WWN prefix:	e
20:00:00:25:b5:xx:xx	
OK Cancel	

13. Click OK.

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

		Create WWPN Pool	? ×
0	Define Name and Description	Name : WWPN_Pool_B	
2	Add WWN Blocks	Description : Assignment Order : O Default Sequential	
		< Prev Next > Finish Car	ncel

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

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

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



- 25. Click OK.
- 26. Click Finish.
- 27. In the confirmation message, click OK.

Create UUID Suffix Pool

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

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

		Create UUID Suffix Pool	: ×
0	Define Name and Description	Name : UUID_Pool	
2	Add UUID Blocks	Description : Prefix : Other Assignment Order : Default Osequential	
		< Prov Next > Finish Ca	incel

- 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 UUID Suffix Pool ? ×
	Define Name and Description	+ - 🌾 Advanced Filter 🛧 Export 🚔 Print 🏠
2	Add UUID Blocks	Name From To [0000-00000000 0000-0000000001 0000-00000000000000000000000000000000
	Create a Block	k of UUID Suffixes ? X
		⊕ Add
		< Prev Next > Finish Cancel

11. Keep the From: field at the default setting.

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

- 13. Click OK.
- 14. Click Finish.
- 15. Click OK.

Create Server Pool

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

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

		Create Server Pool	? ×
1	Set Name and Description	Name : Infra_Pool	
2	Add Servers	Description :	
		< Prov Next > Finish Ca	ancel

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

		Create Server Pool		? ×
1	Set Name and Description	Servers	Pooled Servers	
2	Add Servers	C Sl R U PID A S 1 U U W	C C Sl R U PID A Sl No data available No Stata available Stata available Stata available	₽ S C
		1 1 U U F 2 U U W	16 >> <<	
		1 2 U ↑ ∪ F 1 3 U ↑ ∪ F 1 4 U ◆ ∪ F	16 16	
		Model: UCSC-C220-M5SX Serial Number: WZP22430CUP Vendor: Cisco Systems Inc	K Model: Serial Number: Vendor:	
			< Prev Next > Finish (Cancel

- 9. Click Finish.
- 10. Click OK

Create IP Pool for KVM Access

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

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

Create Block of IPv4 Addresse	es	? ×
From : 10.2.164.70 Subnet Mask : 255.255.255.0 Primary DNS : 10.1.164.9	Size : 16 Default Gateway : 10.2.164.254 Secondary DNS : 0.0.00	
	ОК Са	ncel

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

Set Packages and Policies

Create Host Firmware Package

Firmware management policies allow the administrator to select the corresponding packages for a given server configuration. These policies often include packages for adapter, BIOS, board controller, FC adapters, host bus adapter (HBA) option ROM, and storage controller properties.

To create a firmware management policy for a given server configuration in the Cisco UCS environment, follow these steps:

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

Modify Package Versions	×
Blade Package : 4.0(2b)B	▼ cedence over the images from Blade or Rack Package
Adapter BIOS Board Controller CIMC FC Adapters FIex Flash Controller GPUs HBA Option ROM Host NIC Host NIC Option ROM V Local Disk NVME Mswitch Firmware PSU Dci Switch Firmware	
	OK Apply Cancel Help

8. Click OK to modify the host firmware package.

Create Server Pool Qualification Policy (Optional)

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

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

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

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

Create Server Pool Polic	cy Qualification	? ×
Naming		
Name : UCS-B200-M5		
Description :		
This server pool policy qualification will ap	ply to new or re-discovered servers. Existing servers are not qualified until they are re-discovered	
Actions	Qualifications	
Create Adapter Qualifications	+ - Ty Advanced Filter 🔶 Export 🖶 Print	≎
Create Chassis/Server Qualifications	Create Server PID Qualifications ? X Speed Stepping	Power Gro
Create Memory Qualifications		
Create CPU/Cores Qualifications	PID: UCSB-B200-MS	
Create Storage Qualifications	<not set=""></not>	
Create Server PiD Qualincations	UCSB-B200-M4	
Create Power Group Qualifications	UCSB-B200-M3	
Create Rack Quanications	UCSB-B200-CONN	
	UCSB-B400-CONN	_
	UCSB-B400-CAP	
	UCSB-B200-CAP	
	UCS-DIMM-MAP	
	UCSB-B480-M5	
	UCSB-B420-M4	
	UCSB-B200-M5	
	LICSC-C3X60-SVRNB	
	UCSB-EV-M4-2	Cancel

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

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

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

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

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

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

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

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

Create vMed	ia Mount	? ×
Name	: ESXI-6.7U1 ATTP	
Description	:	
Device Type	: OCDD HDD	
Protocol		
Hostname/IP Address	: 192.1.164.165	
Image Name Variable	: None Service Profile Name	
Remote File	: VMware_ESXi_6.7.0_10302608_Custom_Cisco_6.7	
Remote Path	: /srv/repo/VMware/	
Username	:	
Password	:	
Remap on Eject	:	
	ОК Са	ncel

15. Click OK to create the vMedia Mount.

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

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

Create Server BIOS Policy

25

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

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

Create BIOS Policy	,			?	\times
Name	:	VM-Host			
Description	:				
Reboot on BIOS Settings Change	:				
			ОК	Cancel	

- 6. Select and right click the newly created BIOS Policy.
- 7. Within the Main tab of the Policy:
- 8. Change CDN Control to enabled.
- 9. Change the Quiet Boot setting to disabled.
| Policies / root / B | IOS Policies / VN | И-Host | | | |
|---------------------|-------------------|------------------------------|-----------------|--------------|------------|
| Main Advan | and Dept Opti | and Conver Management Events | | | |
| Main Advance | Sed Boot Opti | ons Server Management Events | | | |
| Actions | | | | | |
| Delete | | | | | |
| Show Policy Usa | age | | | | |
| | | | | | |
| Properties | | | | | |
| Name | | : VM-Host | | Ls. | |
| Description | | : | | | |
| Owner | | Local | | | |
| Reboot on BIOS | S Settings Change | : | | | |
| | | | | | |
| Te Advanced Filter | r 🛧 Export 🖷 | Print | | | ¢ |
| BIOS Setting | | | Value | | |
| CDN Control | | | Enabled | | ▼. |
| Front panel lo | ckout | | Platform Defaul | lt | V . |
| POST error pa | use | | Platform Defaul | lt | T. |
| Quiet Boot | | | Disabled | | T |
| Resume on AC | C power loss | | Platform Defaul | lt | ¥ |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | 🕀 Add 💼 | | | |
| | | | | | |
| | | | | | |
| | | | | Save Unanges | |

- 10. Click the Advanced tab, leaving the Processor tab selected within the Advanced tab.
- 11. Set the following within the Processor tab:
 - a. DRAM Clock Throttling -> Performance
 - b. Frequency Floor Override -> Enabled
 - c. Energy Performance -> Performance

Main Advanced Boot Options Server Managemen	t Events	PCI	ODI	LOM and DCIa State	Tructod Diatform	Graphics
Processor Intel Directed IO RAS Memory Sena	I PORT USB	PCI	QPI	LOW and PCIE Slots	Trusted Platform	Graphics
, Advanced Filter 🔺 Export 🚔 Print						\$
OS Setting	•	Value				
DCU Streamer Prefetch		Platform De	efault			V
DRAM Clock Throttling		Performanc	e			V .
Demand Scrub		Platform De	efault			V
Determinism Slider		Platform De	efault			₹
Direct Cache Access		Platform De	efault			▼.
Downcore control		Platform De	efault			V
Energy Efficient Turbo		Platform De	efault			V .
Energy Performance		Performanc	e			T
Energy Performance Tuning		Platform De	efault			V .
Enhanced Intel SpeedStep Tech		Platform De	efault			V
Execute Disable Bit		Platform De	efault			V .
Frequency Floor Override		Enabled				Y
Global C-state Control		Platform De	efault			V
Hardware Prefetcher		Platform De	efault			V
IMC Inteleave		Platform De	efault			V
IOMMU		Platform De	efault			V
Intel HyperThreading Tech		Platform De	efault			V .
Intel Turbo Boost Tech		Platform De	efault			v

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

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

Policies / root / BIOS Policies / VM-Host Main Advanced Boot Options Server Management Events		
Processor Intel Directed IO RAS Memory Serial Port USB	PCI QPI LOM and PCIe Slots Trusted Platform	Graphic:>>>
Ty Advanced Filter ↑ Export ♣ Print		\$
BIOS Setting	Value	
Package C State Limit	Platform Default	₹.
Patrol Scrub	Platform Default	₩.
Power Technology	Platform Default	V .
Processor C State	Disabled	Y .
Processor C1E	Disabled	T.
Processor C3 Report	Disabled	T .
Processor C6 Report	Disabled	T
Processor C7 Report	Disabled	Y .
Processor CMCI	Platform Default	₹.
ProcessorEppProfile	Platform Default	₹.
Rank Interleaving	Platform Default	₹.
SMEE	Platform Default	₩.
SMT Mode	Platform Default	<u>.</u>
SVM Mode	Platform Default	₹.
Sub NUMA Clustering	Platform Default	₹.
UPI Prefetch	Platform Default	V .
Workload Configuration	Platform Default	Ψ.
XPT Prefetch	Platform Default	V .
🕀 Add 💼		
	Save Changes R	eset Values

- 13. Click the RAS Memory tab and select:
 - a. LV DDR Mode -> performance-mode

olicies / root / BIOS Policies / VM-Ho	st					6		
Main Advanced Root Options	Server Man	agement E	vente					
Processor Intel Directed IO	RAS Memory	Serial Port	USB	PCI	QPI	LOM and PCIe Slots	Trusted Platform	Graphice>
🏹 Advanced Filter 🔺 Export 🚔 Print								\$
BIOS Setting				Value				
DDR3 Voltage Selection				Platform	Default			₹.
DRAM Refresh Rate				Platform	Default			₹.
LV DDR Mode				Performa	ance Mod	le		V .
Mirroring Mode				Platform	Default			₹.
NUMA optimized				Platform	Default			₹.
Memory RAS configuration				Platform	Default			₹.
		(+) A(id 📋 De					
						_		
						Sa	ve Changes	Reset Values

14. Click Save Changes.

15. Click OK.

Update Default Maintenance Policy

To update the default Maintenance Policy, follow these steps:

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

æ	Policies 👻	Policies / root / Maintenance Policies /	default	l≽
B	▼ Policies	General Events		
_	🕶 root 🙆			
뮮	 Adapter Policies 	Actions	Properties	
	 BIOS Defaults 		Name	default
	 BIOS Policies 	Show Policy Usage	Description	:
	 Boot Policies 	Use Glóbal	Owner	Local
	 Diagnostics Policies 		Soft Shutdown Timer	: 150 Secs 🔻
_	 Graphics Card Policies 		Storage Config. Deployment Policy	ry : Immediate User Ack
	 Host Firmware Packages 		Reboot Policy	: O Immediate O User Ack Timer Automatic
2	► IPMI/Redfish Access Profiles		 On Next Boo 	ot (Apply pending changes at next reboot.)
	 KVM Management Policies 			
	 Local Disk Config Policies 			
	 Maintenance Policies 			
	default			
	 Management Firmware Packages 			
	 Memory Policy 			
	 Power Control Policies 			
	 Power Sync Policies 			
	 Scrub Policies 			
	 Serial over LAN Policies 			
	 Server Pool Policies 			
	 Server Pool Policy Qualifications 			
	 Threshold Policies 			
	 iSCSI Authentication Profiles 			
	 vMedia Policies 			
	 vNIC/vHBA Placement Policies 			Save Changes Reset Values

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

Create Local Disk Configuration Policy (Optional)

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

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

To create a local disk configuration policy, follow these steps:

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

Create Local Disk	Configuration Policy	? ×
Name	: SAN-Boot	
Description	:	
Mode	No Local Storage	
FlexFlash —		
FlexFlash State	: Olisable Enable	
If FlexFlash State is disabled, SD Please ensure SD cards are not in	or cards will become unavailable immediately. In use before disabling the FlexFlash State.	
FlexFlash RAID Reporting State	: O Disable C Enable	
FlexFlash Removable State	: Ves No No Change	
Please ensure SD cards are not in	n use before changing the FlexFlash Removable State.	
	ОК Саг	ncel

8. Click OK.

Create Power Control Policy

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

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

- 4. Select Create Power Control Policy.
- 5. Enter No-Power-Cap as the power control policy name.
- 6. Change the power capping setting to No Cap.

Create Pow	er 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.								
	ОК	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. Select Policies > root.
- 3. Right-click Network Control Policies.
- 4. Select Create Network Control Policy.
- 5. Enter Enable_CDP as the policy name.

- 6. For CDP, select the Enabled option.
- 7. Click OK to create the network control policy.

Create Network Control Policy						
Name : E	Enable_CDP					
Description :						
CDP : (Disabled Enabled					
MAC Register Mode :	Only Native Vlan All Host Vlans					
Action on Uplink Fail :	Link Down Warning					
MAC Security						
Forge : O Allow C	Deny					
LLDP						
	ОК Са	incel				

8. Click OK.

6

Configure Cisco UCS LAN Connectivity

Create Uplink Port Channels

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

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

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

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

		Create Port Channel	? ×
0	Set Port Channel Name	ID : 131	
2	Add Ports	Name : <u>vPC</u> -131-Nexus	
		< Prev Next > Finish Can	cel

7. Click Next.

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

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

		Create	e Port Ch	nannel					? ×
	Set Port Channel Name		F	Ports			Ports in the port cha		
0	Add Ports	Slot ID	Aggr. Po	. Port	MAC		Slot ID	Aggr. Po Port	MAC
•		1	0	49	00:DE:F			No data available	
		1	0	50	00:DE:F	>>			
						<<			
						< Pr	ev	ext > 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. Select Create Port Channel.
- 15. Enter a unique ID for the port channel, (132 in our example to correspond with the upstream Nexus port channel).
- 16. With 132 selected, enter vPC-132-Nexus as the name of the port channel.

		Create Port Channel	? ×
0	Set Port Channel Name	ID : 132	
2	Add Ports	Name : vPC-132-Nexus	
		< Prev Next > Finish Car	ncel

17. Click Next.

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

	A	Create	Create Port Channel						
1	Set Port Channel Name		Р	orts			Ports in the port chann		
2	Add Ports	Slot ID	Aggr. Po	Port	MAC		Slot ID	Aggr. Po Port	MAC
		1	0	49	00:DE:F			No data available	
		1	0	50	00:DE:F	>>			
						<<			
						< Pre	v N	mt > Finish	Cancel

- 19. Click >> to add the ports to the port channel.
- 20. Click Finish to create the port channel.
- 21. Click OK.

Create VLANS

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

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

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

- 2. Select LAN > LAN Cloud.
- 3. Right-click VLANs.
- 4. Select Create VLANs.
- 5. Enter Native-VLAN as the name of the VLAN to be used as the native VLAN.
- 6. Keep the Common/Global option selected for the scope of the VLAN.
- 7. Enter the native VLAN ID.

8. Keep the Sharing Type as None.

Create VLANs	X
VLAN Name/Prefix : Native-VLAN	
Multicast Policy Name : wmm.endoweduction.com 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 : 2	
Sharing Type : None Primary Isolated Community	
Check Overlap OK Cancel	\supset

- 9. Click OK and then click OK again.
- 10. Expand the list of VLANs in the navigation pane, right-click the newly created Native-VLAN and select Set as Native VLAN.
- 11. Click Yes and then click OK.
- 12. Right-click VLANs.
- 13. Select Create VLANs
- 14. Enter IB-Mgmt as the name of the VLAN to be used for management traffic.
- 15. Keep the Common/Global option selected for the scope of the VLAN.
- 16. Enter the In-Band management VLAN ID.
- 17. Keep the Sharing Type as None.

Create VLANs	? ×
VLAN Name/Prefix : IB-Mgmt	
Multicast Policy Name : <pre></pre>	reate Multicast Policy
Common/Global Fabric A Fabric B Both Fabrics Config	red Differently
You are creating global VLANs that map to the same VLAN IDs in all Enter the range of VLAN IDs.(e.g. " 2009-2019" , " 29,35,40-45" , "	vailable fabrics. 3" , " 23,34-45")
VLAN IDs : 215	
Sharing Type : ONONE OPrimary Olsolated OCommunity	
	Check Overlap OK Cancel

- 18. Click OK and then click OK again.
- 19. Right-click VLANs.
- 20. Select Create VLANs.
- 21. Enter vMotion as the name of the VLAN to be used for vMotion.
- 22. Keep the Common/Global option selected for the scope of the VLAN.
- 23. Enter the vMotion VLAN ID.
- 24. Keep the Sharing Type as None.

VLAN Name/Prefix : whotion Multicast Policy Name: Into 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 Community	Create VLANs	? ×
	Create VLANs VLAN Name/Prefix v Multicast Policy Name: <not set=""> 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</not>	? ×
Check Overlap OK Cancel	Check Overlap O	Cancel

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

Create vNIC Templates

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

Create Management vNICs

For the vNIC_Mgmt_A Template, follow these steps:

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

- 3. Right-click vNIC Templates.
- 4. Select Create vNIC Template.
- 5. Enter vNIC_Mgmt_A as the vNIC template name.
- 6. Keep Fabric A selected.
- 7. Select Primary Template for the Redundancy Type.
- 8. Leave Peer Redundancy Template as <not set>

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

- 9. Under Target, make sure that the VM checkbox is not selected.
- 10. Select Updating Template as the Template Type.
- 11. Under VLANs, select the checkboxes for IB-Mgmt and Native-VLAN VLANs.

Create vNIC Ten	nplate🎝		? ×
Name : vi Description :	NIC_Mgmt_A		
Fabric ID : Redundancy	Fabric A	⊖ Fabric B	Enable Failover
Redundancy Type Peer Redundancy Templat	: No Redundancy Prima e: <pre><not set=""> </not></pre>	ary Template 🔿 Secondary	y Template
Adapter Adapter VM Warning If VM is selected, a port pro If a port profile of the same	file by the same name will be cre	ated.	
Template Type : C) Initial Template () Updating Te	mplate	erwritten
Te Advanced Filter 🕈 Expo	rt 🖷 Print		\$
Select	Name	Native VLAN	VLAN ID
~	IB-Mgmt	\odot	215
	iSCSI-A-VLAN	0	1110
\checkmark	Native-VLAN	۲	2
			OK Cancel

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

Create vNIC T	emplate			? ×
VLANS VLAN GR	pups			
🏹 Advanced Filter 🛛 🔶 E	Export 🚔 Print			¢
Select	Name	Native VLAN	VLAN ID	
	default	0	1	
\checkmark	IB-Mgmt	0	215	
	iSCSI-A-VLAN	0	1110	
\checkmark	Native-VLAN	۲	2	, i i i
	pure-ext	0	15	
	pure-int	0	115	
CDN Source : MTU : MAC Pool : QoS Policy : Network Control Policy : Pin Group : Stats Threshold Policy : Connection Policies O Dynamic vNIC (•) us	 i ● vNIC Name ○ User Define i 1500 i MAC_Pool_A(32/32) ▼ i < not set> ▼ i < enot set> ▼ i < enot set> ▼ i < default ▼ 	d		
			ОК	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, select the LAN tab.
- 2. Select Policies > root.
- 3. Right-click vNIC Templates.
- 4. Select Create vNIC Template
- 5. Enter vNIC_Mgmt_B as the vNIC template name.
- 6. Select Fabric B.
- 7. Select Secondary Template for Redundancy Type.

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

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

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

Create vNIC Tem	plate		? ×
Name : VNI Description : Fabric ID : C	C_Mgmt_B	 Fabric B 	Enable Failover
Redundancy		2	
Redundancy Type :	No Redundancy ○ vNIC_Mgmt_A ▼	Primary Template Second	ary Template
Target ✓ Adapter VM			
Warning If VM is selected, a port profile If a port profile of the same na Template Type :	e by the same name will b ime exists, and updating to nitial Template () Updatin	e created. emplate is selected, it will be o ng Template	overwritten
VLANs VLAN Groups			
🏹 Advanced Filter 🛛 🛧 Export	🖶 Print		\$
Select	Name	Native VLAN	VLAN ID
	default	0	1
	IB-Mgmt	0	215
	iSCSI-B-VLAN	0	1120
	Native-VI AN	0	2 OK Cancel

10. In the MAC Pool list, select MAC_Pool_B.

Create vNIC	Template			? ×
VLANS VLAN G	roups			
▼ Advanced Filter ↑	Export 🖶 Print			¢
Select	Name	Native VLAN	VLAN ID	
	default	0	1	
	IB-Mgmt	0	215	
	iSCSI-B-VLAN	0	1120	
	Native-VLAN	0	2	
	pure-ext	0	15	
	pure-int	0	115	
Create VLAN				
CDN Source	: • vNIC Name User [Defined		
MTU	: 1500			
MAC Pool	: MAC_Pool_B(32/32)	,		
QoS Policy	: <not set=""> 🔻</not>			
Network Control Policy	y∶ <not set=""> ▼</not>			
Pin Group	: <not set=""></not>	▼.		
Stats Threshold Policy	: default 🔻			
Connection Policies				
O Dynamic VNIC () I				
usNIC Connection Po	olicy : <not set=""> 🔻</not>			
			ОК	Cancel

- 11. Click OK to create the vNIC template.
- 12. Click OK.

Create vMotion vNICs

For the vNIC_vMotion_A Template, follow these steps:

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

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

Create vNIC	Template		? ×
Name Description	: vNIC_vMotion_A]	
Fabric ID Redundancy	: Fabric A	Fabric B	Enable Failover
Redundancy Type Peer Redundancy Target Adapter VM Warning If VM is selected, a If a port profile of th Template Type VLANS VLAN	: ○ No Redundancy ④ Template : <not set=""> ▼ port profile by the same name will b e same name exists, and updating to : ○ Initial Template ④ Updatin Groups</not>	Primary Template () Second e created. emplate is selected, it will be a ng Template	ary Template
Te Advanced Filter	🕈 Export 🛛 🖶 Print		¢
Select	Name	Native VLAN	VLAN ID
	default	0	1
	IB-Mgmt	0	215
	iSCSI-A-VLAN	0	1110
	Native-VI ∆N	0	2 OK Cancel

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

Te Advanced Filter	🕈 Export 🛛 🖶 Print			\$
Select	Name	Native VLAN	VLAN ID	
	pure-ext	0	15	
	pure-int	0	115	
	VM-App-1301	0	1301	
	VM-App-1302	0	1302	
	VM-App-1303	0	1303	
\checkmark	vMotion	۲	1130	
MAC Pool QoS Policy Network Control Polic Pin Group Stats Threshold Polic	: MAC_Pool_A(32/32) ▼ : <not set=""> ▼ : <not set=""> ▼ : <not set=""> ▼ y : default ▼</not></not></not>			
Connection Policie	s usNIC VMQ			

- 16. Click OK to create the vNIC template.
- 17. Click OK.

For the vNIC_vMotion_B Template, follow these steps:

- 1. In the navigation pane, select the LAN tab.
- 2. Select Policies > root.
- 3. Right-click vNIC Templates.
- 4. Select Create vNIC Template
- 5. Enter vNIC_vMotion_B as the vNIC template name.
- 6. Select Fabric B.
- 7. Select Secondary Template for Redundancy Type.
- 8. For the Peer Redundancy Template drop-down, select vNIC_vMotion_A.

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

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

Create vNIC Terr	plate		? ×
Name : vN Description :	IC_vMotion_B		
Fabric ID : (Redundancy) Fabric A	 Fabric B 	Enable Failover
Redundancy Type	: ON Redundancy O	Primary Template Second	dary Template
Peer Redundancy Template	: vNIC_vMotion_A 🔻		
Target ✓ Adapter VM Warning If VM is selected, a port profile of the same n Template Type : VLANs VLAN Groups	le by the same name will b ame exists, and updating te Initial Template) Updatin	e created. emplate is selected, it will be ig Template	overwritten
🏹 Advanced Filter 🔺 Export	🖶 Print		¢
Select	Name	Native VLAN	VLAN ID
	default	0	1
	IB-Mgmt	0	215
	iSCSI-B-VLAN	0	1120
	Native-VI ΔN	0	2 OK Cancel

10. In the MAC Pool list, select MAC_Pool_B.

Ty Advanced Filter	🕈 Export 🛛 🚔 Print			≎
Select	Name	Native VLAN	VLAN ID	
	default	0	1	
	IB-Mgmt	0	215	
	iSCSI-B-VLAN	0	1120	
	Native-VLAN	0	2	
	pure-ext	0	15	
	pure-int	0	115	
MAC Pool QoS Policy Network Control Polic Pin Group Stats Threshold Policies	: MAC_Pool_B(32/32) ▼ : <not set=""> ▼ : <not set=""> ▼ : <not set=""> ▼ y : y: <not set=""> ▼</not></not></not></not>			
O Dynamic vNIC UsNIC Connection F	usNIC VMQ Policy : <a>Anat set> T			

- 11. Click OK to create the vNIC template.
- 12. Click OK.

Create Application vNICs

For the vNIC_App_A Template, follow these steps:

- 1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
- 2. Select Policies > root.
- 3. Right-click vNIC Templates.
- 4. Select Create vNIC Template.
- 5. Enter vNIC_App_A as the vNIC template name.
- 6. Keep Fabric A selected.
- 7. Optional: select the Enable Failover checkbox.
- 8. Select **Primary Template** for the Redundancy Type.

- 9. Leave Peer Redundancy Template as <not set>
- 10. Under Target, make sure that the VM checkbox is not selected.
- 11. Select Updating Template as the Template Type.
- 12. Set default as the native VLAN.

Create vNIC Template			? ×
Name : VNIC_APP_A Description :			
Fabric ID : Fabric A Redundancy	⊖ Fabric B	Enable Failove	r
Redundancy Type : No Re Peer Redundancy Template : 	dundancy Primary Template Se	econdary Template	
Target ✓ Adapter ✓ VM			
Warning If VM is selected, a port profile by the sar If a port profile of the same name exists,	ne name will be created. and updating template is selected, it w	vill be overwritten	-
Template Type : Initial Template VLANs VLAN Groups	ate Updating Template 		
🏷 Advanced Filter 🔺 Export 🚔 Print			¢
Select Name	Native VLAN	VLAN ID	
✓ default	۲	1	
IB-Mgmt	0	215	
iSCSI-A-	VLAN	1110	
Native-V	LAN	2	
		OK Can	cel

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

Create vNIC Template				? ×
VLAINS VLAIN GROUPS				
🏹 Advanced Filter 🛛 🛧 E	Export 📑 Print			\$
Select	Name	Native VLAN	VLAN ID	
	pure-ext	0	15	
	pure-int	0	115	
\checkmark	VM-App-1301	0	1301	
\checkmark	VM-App-1302	0	1302	
\checkmark	VM-App-1303	0	1303	
	vMotion	0	1130	
Create VLAN				
CDN Source :	● vNIC Name ○ User Defined			
MTU :	9000			
MAC Pool :	MAC_Pool_A(32/32) V			
QoS Policy :	<not set=""> 🔻</not>			
Network Control Policy :	Enable_CDP V			
Pin Group :	<not set=""></not>			
Stats Threshold Policy :	default 🔻			
Connection Policies				
O Dynamic vNIC 🖲 us				
usNIC Connection Poli	icy : <not set=""> 🔻</not>			
			ок	Cancel

17. Click OK to create the vNIC template.

18. Click OK.

For the vNIC_App_B Templates, follow these steps:

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

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



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

Create vNIC Tem	plate		? ×
Name : vNI Description :	C_App_B		
Fabric ID : C) Fabric A	 Fabric B 	Enable Failover
Redundancy Type Peer Redundancy Template	No Redundancy OPrimar	ry Template 💿 Secondar	ry Template
Target ✓ Adapter ✓ VM Warning If VM is selected, a port profil If a port profile of the same na Template Type : □1 VLANs VLAN Groups	e by the same name will be crea ame exists, and updating templat nitial Template () Updating Tem	ted. te is selected, it will be ov	verwritten
🏹 Advanced Filter 🛛 🛧 Export	r Print		\$
Select	Name	Native VLAN	VLAN ID
	default	0	1
	IB-Mgmt	0	215
	iSCSI-B-VLAN	0	1120
	Native-VI AN	0	2 OK Cancel

10. In the MAC Pool list, select MAC_Pool_B.

Te Advanced Filter	🕈 Export 🛛 🖷 Print			¢
Select	Name	Native VLAN	VLAN ID	
	pure-ext		15	
	pure-int	0	115	
	VM-App-1301	0	1301	
	VM-App-1302	0	1302	
	VM-App-1303	0	1303	
	vMotion	0	1130	
Create VLAN				
CDN Source	: • vNIC Name OUser Defin	ed		
MTU	: 1500			
MAC Pool	: MAC_Pool_B(32/32) V			
QoS Policy	: <not set=""> 🔻</not>			
Network Control Polic	cy: <not set=""> ▼</not>			
Pin Group	: <not set=""></not>			
Stats Threshold Polic	y : default 🔻			
Connection Policies	S			
O Dynamic vivic				

11. Click OK to create the vNIC template.

12. Click OK.

Create VLANs	? ×
VLAN Name/Prefix : VM-App-	
Multicast Policy Name : <pre> </pre> <pre> </pre> <pre> </pre> <pre> Create Multicast Policy</pre>	
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 : 1301-1303	
Sharing Type : None Primary Isolated Community	
Check Overlap OK OK	ancel

13. Click OK and then click OK again.

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

Create LAN Connectivity Policy

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

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

Create LAN Connec	ctivity Policy		? ×
Name : EC-LAN-Policy			
Description :			
Click Add to specify one or more vi Name	NICs that the server should use to connect to MAC Address	the LAN. Native VLAN	
	No data avail	able	
	÷	0.11.2	
	Delete (+) Add	Modify	
+ Add ISCSI VINICS			
			OK Cancel

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

7. In the Create vNIC dialog box, enter 00-Mgmt-A as the name of the vNIC.

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

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

Create vNIC	? ×
Name : 00-Mgmt-A	
	Development
Redundancy Pair :	Peer Name :
vNIC Template : vNIC_Mgmt_A 🔻	Create vNIC Template
Adapter Performance Profile	
Adapter Policy : VMWare 🔻	Create Ethernet Adapter Policy
	OK Cancel

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

Create vNIC		? ×
Name : 01-Mgmt-B		
Use vNIC Template : 🗹		
Redundancy Pair :	Peer Name :	
vNIC Template : vNIC_Mgmt_B v	Create vNIC Template	
Adapter Performance Profile		
Adapter Policy : VMWare 🔻	Create Ethernet Adapter Policy	
		OK Cancel

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

Create vNIC		? ×
Name : 02-vMotion-A		
Use vNIC Template : 🗹		
Redundancy Pair :	Peer Name :	
vNIC Template : vNIC_vMotion_A 🔻	Create vNIC Template	
Adapter Performance Profile		
Adapter Policy : VMWare 🔻	Create Ethernet Adapter Policy	
		OK Canaci
		Cancel

- 24. Click the upper Add button to add a vNIC to the policy.
- 25. In the Create vNIC dialog box, enter 03-vMotion-B as the name of the vNIC.
- 26. Select the Use vNIC Template checkbox.
- 27. In the vNIC Template list, select vNIC_vMotion_B.
- 28. In the Adapter Policy list, select VMWare.

Create vNIC		? ×
Name : 03-vMotion-B		
Use vNIC Template : 🕑		
Redundancy Pair : 🔲	Peer Name :	
vNIC Template : vNIC_vMotion_B v	Create vNIC Template	1
Adapter Performance Profile		
Adapter Policy : VMWare 🔻	Create Ethernet Adapter Policy	
		OK Cancel

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

Create vNIC		? ×
Name : 04-App-A Use vNIC Template : 🕑		
Redundancy Pair :	Peer Name :	
vNIC Template : vNIC_APP_A 🔻	Create vNIC Template	
Adapter Performance Profile		
Adapter Policy : VMWare 🔻	Create Ethernet Adapter Policy	
		OK Cancel

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

- 37. In the Create vNIC dialog box, enter 05-App-B as the name of the vNIC.
- 38. Select the Use vNIC Template checkbox.
- 39. In the vNIC Template list, select vNIC_App_B.
- 40. In the Adapter Policy list, select VMWare.

Create vNIC		? ×
Name : 05-App-B		
Redundancy Pair :	Peer Name :	
vNIC Template : vNIC_App_B v	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.

Create LAN Connect	tivity Policy		? ×
Name : FC-LAN-Policy			
Description :			
Click Add to specify one or more vNI	Cs that the server should use to connect to th	e LAN.	
Name	MAC Address	Native VLAN	
vNIC 05-App-B	Derived		
vNIC 04-App-A	Derived		
vNIC 03-vMotion-B	Derived		
vNIC 02-vMotion-A	Derived		
vNIC 01-Mgmt-B	Derived		
vNIC 00-Mamt-A	Derived Delete 🕂 Add () Modify	
Add iSCSI vNICs			
			Cancel
		OR	Cancel

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

Configure FC SAN Connectivity

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

Configure Unified Ports

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

To enable the fibre channel ports, follow these steps:

- 1. In Cisco UCS Manager, click the Equipment tab in the navigation pane.
- 2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary)
- 3. Select Configure Unified Ports.
- 4. Click Yes on the pop-up window warning that changes to the fixed module will require a reboot of the fabric interconnect and changes to the expansion module will require a reboot of that module.
- 5. Within the Configured Fixed Ports pop-up window move the gray slider bar from the left to the right to select either 4 or 8 ports to be set as FC Uplinks.

Configure	Unified Ports		?	X
The position of the	slider determines the type of the p	ports.		
All the ports to the	left of the slider are Fibre Channel	ports (Purple), while the ports to the right are Ethernet	t 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	
	ether	Unconfigured	FC Uplink	
Port 5				
Port 5 Port 6	ether	Unconfigured	FC Uplink	
Port 5 Port 6 Port 7	ether ether	Unconfigured Unconfigured	FC Uplink FC Uplink	

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

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

Create VSANs

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

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



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



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

Create VSAN	? ×
Name : VSAN_A	
FC Zoning : Disabled C Enabled Do NOT enable local zoning if fabric interconnect is connected to an	n upstream FC/FCoE switch.
○ Common/Global Fabric A Fabric B Both Fabrics Configu	ared 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 : 100	FCoE VLAN : 100
	OK Cancel

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

Create VSAN	? ×
Name : VSAN_B	
FC Zoning Settings	
FC Zoning : O Disabled Enabled	
Do NOT enable local zoning if fabric interconnect is connected to	an upstream FC/FCoE switch.
○ Common/Global ○ Eabric A ● Eabric B ○ Both Eabrics Cont	figured 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 : 200	FCoE VLAN : 200
	OK Cancel

16. Click OK and then click OK again.

Create FC Port Channels

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

Fabric A

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

		Create FC Port Channel	? ×
0	Set FC Port Channel Name	ID : 1	
2	Add Ports	Name : SAN-Pol	
		< Prev Next > Finish Car	ncel

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

		Create I	FC Port (Channel				? ×
1	Set FC Port Channel Name	Port Channel	Admin Speed :	4 Gbps 8 Gbps	◯ 16gbps ④ 32gbps			
			Ports	5			Ports in the port	channel
2	Add Ports	Port	Slot ID	WWPN		Port	Slot ID	WWPN
		5	1	20:05:00:DE		1	1	20:01:00:DE
		6	1	20:06:00:DE		2	1	20:02:00:DE
		7	1	20:07:00:DE	>>	3	1	20:03:00:DE
		8	1	20:08:00:DE	<<	4	1	20:04:00:DE
		Slot ID:				Slot ID:	1	3-00-DE-EB-EE-EB-CO
		VVVVFIN.				VVVVFIN.	20.0	5.00.DE.FB.FF.FB.00
					< Prev		Finish	Cancel

- 6. Click Finish.
- 7. Click OK.
- 8. Select the newly created Port-Channel.

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

Æ	All	SAN / SAN Cloud / Fabric A / FC Port Channels / FC Port-Cl	hannel 1 SAN-Po1	
	▼ SAN	General Ports Faults Events Statistics		
暴	 ▼ Fabric A 	Status	Properties	
	✓ FC Port Channels	Overall Status : 🛉 Up	ID	: 1
	FC Port-Channel 1 SAN-Po1 👽	Additional Info :	Fabric ID Port Type	: A
	 FCoE Port Channels 	Actions	Transport Type	: Fc
	 Uplink FC Interfaces 	Enable Port Channel	Name	: SAN-Po1
_	FC Interface 1/5	Disable Port Channel	Description	
-	FC Interface 1/6 0	Add Ports	VSAN	: Fabric Dual/vsan default 🔻
20	FC Interface 1/7 🕚		Port Channel Admin Speed	: Fabric A/vsan VSAN_A (100) s ⊙ 32gbps
	FC Interface 1/8 🕚		Operational Speed(Gbps)	: Fabric Dual/vsan default (1)
	 Uplink FCoE Interfaces 			
	▼ VSANs			
	VSAN VSAN_A (100)			

10. Click Save Changes and then click OK.

Fabric B

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

		Create FC Port Channel ? ×
0	Set FC Port Channel Name	ID : 2
2	Add Ports	Name : SAN-Po2
		< Prev Next > Finish Cancel

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

		Create FC Port C	hannel				? ×
	Set FC Port Channel Name	Port Channel Admin Speed :	◯ 4 Gbps ◯ 8 Gbps	◯ 16gbps ④ 32gbps			
		Ports			1	Ports in the port	channel
2	Add Ports	Port Slot ID	WWPN		Port	Slot ID	WWPN
		No data avai	ilable		1	1	20:01:00:DE
					2	1	20:02:00:DE
				>>	3	1	20:03:00:DE
				<<	4	1	20:04:00:DE
		Slot ID:			Slot ID:		
		WWPN:			WWPN:		
				< Prev	Next	Finish	Cancel

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

Æ	All	SAN / SAN Cloud / Fabric B / FC Port Channels / FC Port-Cl	hannel 2 SAN-Po2	
⊟	▼ SAN	General Ports Faults Events Statistics		
	▼ SAN Cloud			
무	▶ Fabric A	Status	Properties	
	✓ Fabric B	Overall Status : 🛉 Up	ID	: 2
=	▼ EC Port Channels	Additional Info :	Fabric ID	: B
	. TO FOIL ON MINIO	Autor	Port Type	Aggregation
_	FC Port-Channel 2 SAN-Po2	Actions	Transport Type	: Fc
	► FCoE Port Channels	Enable Port Channel	Name	: SAN-Po2
	Uplink FC Interfaces	Disable Port Channel	Description	
	 Uplink FCoE Interfaces 	Add Ports	VSAN	: Fabric Dual/vsan default 🔻
20	▼ VSANs		Port Channel Admin Speed	Fabric B/vsan VSAN_B (200) os 32gbps
	VSAN VSAN_B (200)		Operational Speed(Gbps)	: Fabric Dual/vsan default (1)
	 SAN Pin Groups 			

10. Click Save Changes and then click OK.

Create vHBA Templates

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

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

Create vHBA	Template	? ×
Name Description Fabric ID Redundancy	: vHBA_Template_A :	
Redundancy Type	: No Redundancy Primary Template Secondary Template	
Select VSAN	Create VSAN	
Max Data Field Size	: 2048	
WWPN Pool	: WWPN_Pool_A(32/32) 🔻	
QoS Policy Pin Group	<pre>: <not set=""> ▼</not></pre>	
Stats Threshold Policy	: default 🔻	
	ОК Са	ncel

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

Create vHBA	Template	? ×
Name Description Fabric ID Redundancy	: vHBA_Template_B :	
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=""> 🔻</not>	
Pin Group	: <not set=""></not>	
Stats Threshold Policy	Contraction default 🔻	
	ОК Сал	cel

22. Click OK.

Create SAN Connectivity Policy

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

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

Create vHI	BA	? ×
Name	: Farbic-A	
Redundancy Pair :		Peer Name :
vHBA Template :	vHBA_Template_A 🔻	Create vHBA Template
Adapter Perform	<not set=""></not>	
Adapter Policy :	Domain Policies	Create Fibre Channel Adapter Policy
	vHBA_Template_A	
	vHBA_Template_B	
		OK Cancel

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

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

Create vHE	3A	3	X
Name	: Fabric_B		
Use vHBA Templat	te: 🗹		
Redundancy Pair :		Peer Name :	
vHBA Template :	vHBA_Template_B	Create vHBA Template	
Adapter Perform	<not set=""></not>		
Adapter Policy :	Domain Policies	Create Fibre Channel Adapter Policy	
	vHBA_Template_A		
	vHBA_Template_B		
		OK Cancel	D

19. In the Adapter Policy list, select VMWare.

20. Click OK.

Create SAN Connectiv	ity Policy	? ×
Name : Infra-SAN-Policy		
Description :		
A server is identified on a SAN by its Wor with this profile. World Wide Node Name	ld Wide Node Name (WWNN). Spe	ecify how the system should assign a WWNN to the server associated
WWNN Assignment:	WWNN_Pool(32/32)	•
Create WWNN Pool		
The WWNN will be assigned from The available/total WWNNs are di	the selected pool. splayed after the pool name.	
Name	W	WPN
▶ vHBA Fabric-B	De	erived
▶ vHBA Fabric-A	De	erived
	🗓 Delete 🕂 Add	Modify
		OK Cancel

21. Click OK to create the SAN Connectivity Policy.

22. Click OK to confirm creation.

Create Boot Policy

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

Health							Q s	Search			3 🗙
Hardware A	Alerts Connections Apps										
Host Connection	ons						All Pat	hs	▼ 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	w 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@	Dcspg-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 FCO adapters for each controller from within the System view and record the values to be used for Primary and Secondary Targets. In the example lab environment, these appear as the first ports on the right side of each controller shown.

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

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

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

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

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

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

Do not select the Reboot on Boot Order Change checkbox.

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

Add SAN Boot	? ×
vHBA : Fabric-A	
Type . Primary O Secondary O Ally	
ОК Са	incel

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

Add SAN Boo	ot Target	? ×
Boot Target LUN : Boot Target WWPN :	1 52:4A:93:7C:2B:9B:9F:00	
Туре :	Primary Secondary	
	ОК Са	ancel

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

Add SAN Bo	? ×	
Boot Target LUN :	1	
Boot Target WWPN :	52:4A:93:7C:2B:9B:9F:10	
Type :	OPrimary Secondary	
	ок	Cancel

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

Add SAN Boot	? ×
vHBA : Fabric-B	
Type : Primary Secondary Any	
ОК	Cancel

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

Add SAN Boo	? ×	
Boot Target LUN :	1	
Boot Target WWPN :	52:4A:93:7C:2B:9B:9F:01]
Type :	Primary Secondary	
	ок	Cancel

28. Click OK to add the SAN boot target.

- 29. From the vHBA drop-down list, select Add SAN Boot Target.
- 30. Enter 1 as the value for Boot Target LUN.
- 31. Enter the WWPN for CT1.FC1 recorded in Table 15.

Add SAN Boot Target	? ×
Boot Target LUN : 1	
Boot Target WWPN : 52:4A:93:7C:2B:9B:9F:11	
Type : Primary Secondary	
ОК Са	ancel

- 32. Click OK to add the SAN boot target.
- 33. Expand CIMC Mounted Media and select Add CIMC Mounted CD/DVD.

Create Boot Policy												? ×
Name :	Boot-FC-	-X-A										
Description :												
Reboot on Boot Order Change :												
Enforce vNIC/vHBA/iSCSI Name :												
Boot Mode :	 Legacy 	/ 🔾 Uefi										
WARNINGS: The type (primary/secondary) does The effective order of boot devices If Enforce vNIC/vHBA/iSCSI Name If it is not selected, the vNICs/vHBA	not indicate within the s is selected as are select	a boot order prese ame device class (and the vNIC/vHB/ ted if they exist, oth	ence. LAN/Stor A/iSCSI d erwise th	age/iSCSI loes not ex ne vNIC/vH) is determi kist, a config IBA with the	ned by PCI g error will e lowest PC	le bus scan be reported Cle bus sca	order. d. n order is us	sed.			
(+) Local Devices		Boot Order		A 5								
○ CIMC Mounted vMedia		+ - Ty Adva	anced Filte	Ordor		Tupo		MAANI	Slot N	Root N	Root D	₽
		SAN TE	arget	Oldela	VINIC/V	Primary	LON N	52:4A:	510L N	BOOL N	D001 F	Desch
Add CIMC Mounted CD/DVD		SAN Ta	arget			Secon	1	52:4A:				
Add olivio Modified fibb		🚽 SAN Seco	ondary		Fabric	Secon						1
(+) vNICs		SAN Ta	arget			Primary	1	52:4A:				
		SAN Ta	arget			Secon	1	52:4A:				
⊕ vHBAs		CIMC Mounte	ed C	2								
(+) iSCSI vNICs					1 N	love Up 🚽	Move Do					
⊕ EFI Shell												
											ок	Cancel

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

Create Service Profile Templates

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

To create the service profile template, follow these steps:

- 1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
- 2. Select Service Profile Templates > root.
- 3. Right-click root.
- 4. Select Create Service Profile Template to open the Create Service Profile Template wizard.
- 5. Enter VM-Host-FC-A as the name of the service profile template. This service profile template is configured to boot from FlashArray//X70 R2 controller 1 on fabric A.
- 6. Select the "Updating Template" option.

7. Under UUID, select UUID_Pool as the UUID pool.

		Create Service Profile Template	? ×
0	Identify Service Profile Template	You must enter a name for the service profile template and specify the template type. You can also specify how a UUID will be assigned to template and enter a description.	his
2	Storage Provisioning	Name : VM-Host-FC-A	
3	Networking	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.	
0	SAN Connectivity	Type : Initial Template Updating Template Specify how the UUID will be assigned to the server associated with the service generated by this template.	
5	Zoning	UUID	
6	vNIC/vHBA Placement	UUID Assignment: UUID_Pool(32/32)	
7	vMedia Policy	The UUID will be assigned from the selected pool. The available/total UUIDs are displayed after the pool name.	
8	Server Boot Order	Optionally enter a description for the profile. The description can contain information about when and where the service profile should be use	d.
9	Maintenance Policy		
10	Server Assignment		
11	Operational Policies		
		Next > Finish Car	cel

8. Click Next.

Configure Storage Provisioning

To configure storage provisioning, follow these steps:

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

		Create Service Profile Template	? ×
0	Identify Service Profile	Optionally specify or create a Storage Profile, and select a local disk configuration policy.	
	Template	Specific Storage Profile Storage Profile Policy	
2	Storage Provisioning		
		Local Storage: Select Local Storage Policy to use V	
3	Networking	Create Local Create a Specific Storage Policy to use olicy will be assigned to this service profile.	
4	SAN Connectivity	Storage Policies	
	Tester	SAN-Boot	
5	Zoning	default	
6	vNIC/vHBA Placement		
7	vMedia Policy		
8	Server Boot Order		
9	Maintenance Policy		
10	Server Assignment		
11	Operational Policies		
		< Prev Next > Finish	Cancel

3. Click Next.

Configure Networking Options

To configure the network options, follow these steps:

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

		Create Service Profile Template	? ×
	Identify Service Profile	Optionally specify LAN configuration information.	
	Template	Dynamic vNIC Connection Policy: Select a Policy to use (no Dynamic vNIC Policy by default) +	
2	Storage Provisioning	Create Dynamic vNIC Connection Policy	
3	Networking		
4	SAN Connectivity	How would you like to configure LAN connectivity?	
6	Zoning	LAN Connectivity Policy : FC-LAN-Policy Create LAN Connectivity Policy Initiator Name	
6	vNIC/vHBA Placement	Initiator Name Assignment: <pre></pre> <pr< th=""><th></th></pr<>	
	vMedia Policy	Create IQN Suffix Pool	
8	Server Boot Order	WARNING : The selected pool does not contain any available entities. You can select it, but it is recommended that you add entities to it.	
9	Maintenance Policy		
10	Server Assignment		
11	Operational Policies		
		< Prev Next > Finish Ca	ancel

4. Click Next.

Configure SAN Connectivity Options

To configure the SAN connectivity options, follow these steps:

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

		Create Service Profile Template	? ×
0	Identify Service Profile	Optionally specify disk policies and SAN configuration information.	
	Template	How would you like to configure SAN connectivity?	
2	Storage Provisioning	San Connectivity Policy : Croat sets Create SAN Connectivity Policy	
3	Networking	<not set=""></not>	
4	SAN Connectivity	Domain Policies Infra-SAN-Policy	
5	Zoning		
6	vNIC/vHBA Placement		
0	vMedia Policy		
8	Server Boot Order		
9	Maintenance Policy		
10	Server Assignment		
11	Operational Policies		
		< Prev Next > Finish	Cancel

Configure Zoning Options

1. Leave Zoning configuration unspecified and click Next.

Configure vNIC/HBA Placement

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

Configure vMedia Policy

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

Configure Server Boot Order

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

		Create Service Profile Template	? ×				
	Identify Service Profile	Optionally specify the boot policy for this service profile template.					
	Template	Select a boot policy.					
2	Storage Provisioning	Boot Policy: Boot-FC-X-A V Create Boot Policy					
3	Networking	Name : Boot-FC-X-A Description :					
4	SAN Connectivity	Rebot on Boot Order Change : No Enforce vNIC/vHBA/iSCSI Name : Yes					
5	Zoning	Boot Mode : Legacy WARNINGS: The type (primary/secondary) does not indicate a boot order presence.					
6	vNIC/vHBA Placement	The effective order of boot devices within the same device class (LAN/Storage/NSSI) is determined by PCIe bus scan order. If Enforce vNIC/vHBA/iSSI Mame is selected and the vNIC/vHBA/iSSCI 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.					
	vMedia Policy	Boot Order + - Ty Advanced Filter ↑ Export Print	¢				
8	Server Boot Order	Name Order A vNIC/vHB Type LUN Name WWN Slot Numb Boot Name Boot Path Descrip	ition				
9	Maintenance Policy	San 1 SA Fabric-A Primary					
10	Server Assignment	SA Fabric-B Secondary					
	Operational Balician	CIMC 2					
W	Operational Policies						
		< Prev Next > Finish Can	cel				

2. Click Next to continue to the next section.

Configure Maintenance Policy

To configure the maintenance policy, follow these steps:

1. Change the Maintenance Policy to default.

		Create Service Profile Template ? X				
1	Identify Service Profile Template	Specify how disruptive changes such as reboots, network interruptions, and firmware upgrades should be applied to the server associated with this service profile.				
2	Storage Provisioning	Maintenance Policy				
3	Networking	Select a maintenance policy to include with this service profile or create a new maintenance policy that will be accessible to all service profiles. Maintenance Policy: default Greate Maintenance Policy				
4	SAN Connectivity					
5	Zoning	Name : default Description :				
6	vNIC/vHBA Placement	Soft Shutdown Immer : 150 Secs Storage Config. Deployment Policy : User Ack				
7	vMedia Policy	Reboot Policy : User Ack				
8	Server Boot Order					
9	Maintenance Policy					
10	Server Assignment					
11	Operational Policies					
		< Prev Next > Finish Cancel				

2. Click Next.

Configure Server Assignment

To configure server assignment, follow these steps:

- 1. In the Pool Assignment list, select Infra_Pool.
- 2. Optional: Select a Server Pool Qualification policy.
- 3. Select Down as the power state to be applied when the profile is associated with the server.
- 4. Optional: Select "UCS-B200M5" for the Server Pool Qualification.
- 5. Firmware Management at the bottom of the page can be left alone as it will use default from the Host Firmware list.

		Create Service Profile Template ?	\times					
	Identify Service Profile Template	ptionally specify a server pool for this service profile template.						
2	Storage Provisioning	Pool Assignment: Infra_Pool Create Server Pool						
3	Networking	Select the power state to be applied when this profile is associated with the server.						
4	SAN Connectivity	● Up ◯ Down						
5	Zoning	The service profile template will be associated with one of the servers in the selected pool. If desired, you can specify an additional server pool policy qualification that the selected server must meet. To do so, select the qualification from						
6	vNIC/vHBA Placement	the list. Server Pool Qualification : UCS-B200-M5 ▼						
	vMedia Policy	Restrict Migration :						
8	Server Boot Order	⊕ Firmware Management (BIOS, Disk Controller, Adapter)						
9	Maintenance Policy							
10	Server Assignment							
11	Operational Policies							
		< Prev Next > Finish Cancel)					

6. Click Next.

Configure Operational Policies

To configure the operational policies, follow these steps:

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

		Create Service Profile Template	? ×
1	Identify Service Profile Template	Optionally specify information that affects how the system operates.	
2	Storage Provisioning	BIOS Configuration If you want to override the default BIOS settings, select a BIOS policy that will be associated with this service profile	
3	Networking	BIOS Policy : VM-Host V	
4	SAN Connectivity	External IPMI/Redfish Management Configuration	
5	Zoning	Management IP Address	
6	vNIC/vHBA Placement	Monitoring Configuration (Thresholds)	
7	vMedia Policy	Power Control Policy Configuration	
8	Server Boot Order	Power control policy determines power allocation for a server in a given power group.	
9	Maintenance Policy	Power Control Policy : No-Power-Cap Create Power Control Policy	
10	Server Assignment	① Scrub Policy	
1	Operational Policies	⊕ KVM Management Policy	
		⊕ Graphics Card Policy	
		< Prev Next > Finish Ca	ancel

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

Create vMedia Service Profile Template

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

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

Create Service Profiles

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

- 1. Connect to the UCS 6454 Fabric Interconnect UCS Manager, click the Servers tab in the navigation pane.
- 2. Select Service Profile Templates > root > Service Template VM-Host-FC-A.
- 3. Right-click VM-Host-FC-A and select Create Service Profiles from Template.
- 4. Enter VM-Host-FC-0 as the service profile prefix.
- 5. Leave 1 as "Name Suffix Starting Number."
- 6. Leave 2 as the "Number of Instances."
- 7. Click OK to create the service profiles.

Create Service Pr	ofiles From	Template	? ×
Naming Prefix : VM-Host-	FC-0		
Name Suffix Starting Number :	1		
Number of Instances :	2		
		ОК Са	ncel

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

Claim in Intersight

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

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

æ	Device Connector	Device Connector		
=	Device Connector	The Device Connector is an embedded management or information about configuring the device connector, ple	ntroller that enables the capabilities of Cisco Intersig ase visit Help Center.	ht, a cloud-based management platform. For detailed
器		Intersight Management	Connection	(3) Settings
		Enabled	Status Avot Claimed	Device ID
≡		When this option is enabled, you can claim	Access Mode Allow Control	Claim Code
		of Cisco Intersight.		
3 0		allowed to Cisco Intersight.		0
		Agent Version 1.0.9-2564		

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

≡	cisco Intersight	Devices	다 오 🎧 🔅 🔿 Allen Clark 요
<u>00o</u>	Dashboards	I New features have recently been added! Learn More	×
	Servers		Claim a New Device
669	HyperFlex Clusters		
₽	Fabric Interconnects	iii Q Search	0 items found 8
ā	Service Profiles	Name Status Type	Device IP Device ID Claimed By
1	Policies		
	Devices		
			K < 0 of 0 > >

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



8. Click Claim.

	رابیان Intersight	Devices \square \square \square \square Allen Clark \square
000	Dashboards	Claim a New Device
	Servers	
Q D	HyperFlex Clusters	□ Q Search □ 1 items found 8 ✓ per page ✓ 1 of 1 > ○
	Fabric Interconnects	Name Status Type Device IP Device ID Claimed By ∅
6	Service Profiles	AA12-UCS Connected UCS Domain 10.2.164.51, 1(3)
1	Policies	ش الا ح 1 of1 کا
Ŵ	Devices	

MDS Fabric Zoning

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



Create Device Aliases

To create device aliases, follow these steps:

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

MDS-9132T-A# show flogi database							
INTERFACE	VSAN	FCID	PORT NAME	NODE NAME			
fc1/15	100	0xb00000	52:4a:93:7c:2b:9b:9f:00	52:4a:93:7c:2b:9b:9f:00			
fc1/16	100	0xb00020	52:4a:93:7c:2b:9b:9f:00	52:4a:93:7c:2b:9b:9f:00			
fc1/17	100	0xb00040	52:4a:93:7c:2b:9b:9f:02	52:4a:93:7c:2b:9b:9f:02			
fc1/18	100	0xb00040	52:4a:93:7c:2b:9b:9f:12	52:4a:93:7c:2b:9b:9f:12			
port-channel100	100	0xb00060	24:01:00:de:fb:ff:fb:c0	20:64:00:de:fb:ff:fb:c1			
port-channel100	100	0xb00061	20:00:00:25:b5:01:0a:00	20:00:00:25:b5:01:00:00			
port-channel100	100	0xb00062	20:00:00:25:b5:01:0a:01	20:00:00:25:b5:01:00:01			

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

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

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

Servers / Service Profiles / root / Service Profile	VM-Host-FC-01						
General Storage Network iSCSI vNIC	s vMedia Policy Boot O	rder Virtual Machines	FC Zones Policies	Server Details CIMC Sessio	ns FSM VIF Paths	Faults Events	
Storage Profiles Local Disk Configuration Policy	vHBAs vHBA Initiator	Groups					
Actions	World Wide N	lode Name					
Change World Wide Node Name Modify vNIC/vHBA Placement Reset WWNN Address	World Wide N WWNN Pool WWNN Pool	Node Name : 20:00:00:25:89 : WWNN_Pool Instance : org-root/wwn-	5:01:00:00				
	Local Disk Po Local Disk Po	Local Disk Policy : SAN-Boot Local Disk Policy Instance : org-root/local-disk-config-SAN-Boot					
No Configuration Change of WICE/WIRE/SCSLVNI	SAN Connec SAN Connec SAN Connec Create SAN C	tivity Policy : Infra tivity Policy Instance : org-ro onnectivity Policy	-SAN-Policy 💌 pot/san-conn-pol-Infra-SAN	-Policy			
vHBAs	CS is allowed due to connectiv	ity policy.					
🏹 Advanced Filter 🔶 Export 🚔 Print							
Name WWPN	Desired Order	Actual Order	Fabric ID	Desired Placement	Actual Placement	Admin Host Port	Actual Ho
vHBA Fabric-A 20:00:00:25:B5:01:0	A:00 1	7	A	Any	1	ANY	NONE
vHBA Fabric-B 20:00:00:25:85:01:0	B:00 2	8	В	Any	1	ANY	NONE
Source	Switch/Port		WWPN/PV	VWN	Customer \	WPN/PWWN	

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

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

MDS-9132T-A# conf t

MDS-9132T-A(config)# device-alias database

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

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

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

6	Squrce	Switch/Port	WWPN/PWWN	Customer WWPN/PWWN
0.	FlashArray-CT0FC1 r	MDS A fc 1/15	52:4A:93:7C:2B:9B:9F:01	
	FeashArray-CT1FC1 a	MDS A fc 1/16	52:4A:93:7C:2B:9B:9F:03	
	FilashArray-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	
	60454-B	Port-Channel 100	24:02:00:de:fb:ff:f3:80	
	VM-Host-FC-01-B	Port-Channel 100	20:00:00:25:b5:01:0b:00	
	VM-Host-FC-02-B c	Port-Channel 100	20:00:00:25:b5:01:0b:01	

е

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

MDS-9132T-B# conf t

MDS-9132T-B(config)# device-alias database

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

MDS Zoning

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

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

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

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

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

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

MDS-9132T-B(config) # zone name VM-Host-FC-01-B vsan 200

MDS-9132T-B(config-zone)# member device-alias VM-Host-FC-01-B init MDS-9132T-B(config-zone)# member device-alias FlashArray-CTOFC1 target MDS-9132T-B(config-zone)# member device-alias FlashArray-CTOFC3 target MDS-9132T-B(config-zone)# member device-alias FlashArray-CT1FC1 target MDS-9132T-B(config-zone)# member device-alias FlashArray-CT1FC1 target

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

MDS-9132T-B(config) # zone name VM-Host-FC-02-B vsan 200

MDS-9132T-B(config-zone) # member device-alias VM-Host-FC-02-B init MDS-9132T-B(config-zone) # member device-alias FlashArray-CTOFC1 target MDS-9132T-B(config-zone) # member device-alias FlashArray-CTOFC3 target MDS-9132T-B(config-zone) # member device-alias FlashArray-CT1FC1 target MDS-9132T-B(config-zone) # member device-alias FlashArray-CT1FC1 target

Create and Activate Zoneset

Add the zones to a zoneset on each MDS switch:

zoneset for MDS A

MDS-9132T-A(config-zone) # zoneset name flashstack-zoneset vsan 100

MDS-9132T-A config-zoneset) # member VM-Host-FC-01-A

MDS-9132T-A(config-zoneset) # member VM-Host-FC-02-A

zoneset for MDS B

MDS-9132T-B(config-zone) # zoneset name flashstack-zoneset vsan 200

MDS-9132T-B(config-zoneset) # member VM-Host-FC-01-B

MDS-9132T-B(config-zoneset) # member VM-Host-FC-02-B

Activate the zonesets and save the configuration:

zoneset for MDS A

mds-9148s-a(config-zoneset)# zoneset activate name flashstack-zoneset vsan 101

mds-9148s-a(config) # copy run start

zoneset for MDS B

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

FlashArray Storage Deployment

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

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

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



Host Port Identification

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

Host Registration

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

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

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

Create Multiple Hosts				
Name	VM-Host-FC-#			
Start Number	1			
Count	2			
Number of Digits	1			
Create Single	Cancel Create			

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

Ç	PURESTORAGE" •	Storage		Q Search	
۲	Dashboard	Array Hosts Volumes Protection Groups Pods			
۲	Storage	Size Data Reduction Volumes Snanshots Shared System Total			:
Q		0 1.0 to 1 0.00 0.00 0.00			
	Capacity	Connected Volumes	0 of 0 < >	Host Ports	:
		Name 🔺	Shared LUN	Port	Configure WWNs
Æ	Health			No ports found.	Remove
Ŭ		No volumes found.		Dotails	:
*		Protection Groups	0 of 0 < >		:
		Name 🔺		CHAP Credentials	
Help				Personality	
Terms	5	No protection groups found.		Preferred Arrays	

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

Configure Fibre Channel WWNs		*
Existing WWNs	Selected WWNs	+
	None selected	
20:00:00:25:B5:01:0A:02		
🔲 🐺 20:00:00:25:B5:01:0A:03		
20:00:00:25:B5:01:0B:02		
20:00:00:25:B5:01:0B:03		
	C	ancel Add

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

Add WWN manual	у	×
WWN	20:00:00:25:b5:01:0A:00	
		Cancel Add
Add WWN manual	у	×
WWN	20:00:00:25:b5:01:0B:00	
		Cancel Add

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

0	PURESTORAGE" •	Storage		Q Search	▲ 🛛
۲	Dashboard	Array Hosts Volumes Protection Groups Pods			
۲	Storage	Size Data Reduction Volumes Snapshots Shared System Total			**
Q		0 1.0 to 1 0.00 0.00 0.00			
	Performance Capacity	Connected Volumes o of	0 < > :	Host Ports	:
		Name 🔺 St	nared LUN	Port	
4	Hoalth			20:00:00:25:B5:01:0A:00	N X
•	riedui	No volumes found.		a 20:00:00:25:B5:01:0B:00	× ×
*		Protection Groups 0 of	0 < > :		
		Name 🔺		Details	i
				CHAP Credentials	Configure CHAP
Terms		No protection groups found.		Personality	Add Preferred Arrays
Log C				Preferred Arrays	

12. Select ESXi and click Save.

Configure Person	ality	×
ESXi		
Hitachi VSP		
HP-UX		
Oracle VM Server		
Solaris		
VMS		
None		
	Cancel	Save

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

Create Host Group

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

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

Create Host Group				
Name	Production			
Create Multiple		Cancel	Create	

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

\mathbf{O}	PURESTORAGE* 4	Storage			Q Search	N
٩	Dashboard	Array Hosts Volumes Protection Groups Pods				
۲	Storage	😢 > Hosts > 📴 Production				
Q	Analysis	Size Data Reduction Volumes Snapshots Shared System Total 0 1.0 to 1 0.00 0.00 - - 0.00				
	Performance Capacity	Member Hosts				0 of 0 < >
	Replication	Name 🔺		Interface	Size V	Add Remove
€	Health	No hosts found.				Download CSV
*	Settings	Connected Volumes o of 0 <	> :	Protection Groups		0 of 0 < >
		Name 🔺	LUN	Name 🔺		
Help						
Terms	5	No volumes found.		No protection groups found.		

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

Add Hosts to Host Group		×
Existing Hosts	Selected Hosts	
□ 1-5 of 5 < >	2 selected	Clear all
FSV-Upgrade-ESXI-03	VM-Host-FC-1	×
VM-Host-FC-1	VM-Host-FC-2	×
VM-Host-FC-2		
		Cancel Add

8. Click Add.

Private Boot Volumes for Each ESXi Host

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

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

Create Volume		×
Container	1	
Name	Letters, Numbers, -	
Provisioned Size	Numbers	G 🔹
Bandwidth Limit	Numbers	MB/s 💌
Create Multiple	Cancel	Create

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

Create Multiple Volumes					
Container	1				
Name	VM-Host-FC-Boot-#				
Provisioned Size	20	G	•		
Bandwidth Limit	Numbers	MB/s	•		
Start Number	1				
Count	2				
Number of Digits	1				
Create Single	Cancel	Create	5		

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

0	PURESTORAGE [®] 4	Storage
٩	Dashboard	Array Hosts Volumes Protection Groups Pods
۲	Storage	😢 > Hosts > 📰 Production > 📼 VM-Host-FC-1
Q	Analysis	Size Data Reduction Volumes Snapshots Shared System Total 0 1.0 to 1 0.00 0.00 - - 0.00
	Performance Capacity Replication	Connected Volumes 0 of 0 < > ▮ Name ▲ Connect Disconnect
✤	Health	No volumes found. Download CSV
*	Settings	Protection Groups 0 of 0 < >
	{	Name 🔺
Help Term	5	No protection groups found.

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

Connect Volumes to Host	×
Existing Volumes	Selected Volumes
□ 1-50 of 272 < >	1 selected Clear all
VM-Host-FC-Boot-1	VM-Host-FC-Boot-1 X
_	
LUN 1	
	Cancel Connect

LUN ID 1 should be used for the boot.

2

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

Configure Storage Policy Based Management

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

To configure Storage Policy Based Management, follow these steps:

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

Array Hosts Volumes Protection Groups Po	ods		
Protection Groups			
Snapshots 0.00			
Protection Groups			1-1 of 1 < > +
Name 🔺	Snapshots	Targets	Create Destroy
© pure-vasa-default	0.00	•	Allow Disallow
			Download CSV

3. Enter a name.

Create Protection Group				
Container	1			
Name	platinum			
	Cancel Create			

- 4. Select the protection group.
- 5. Edit the Snapshot Schedule based on your operational requirements.

Edit Snapshot Schedule	×
Enabled	
Create a snapshot on source every 1 hours 🔹 at - 💌	
Retain all snapshots on source for 1 days -	
then retain 4 snapshots per day for 7 more days	
	Chartel Dave
	Cancel Save

6. Click Save.

VMware vSphere Deployment

ESXi Installation

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



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

Download Cisco Custom Image for ESXi 6.7 U1

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

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

Log into Cisco UCS 6454 Fabric Interconnect

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

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

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

Set Up VMware ESXi Installation

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

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

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

Install ESXi

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

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

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

Set Up Management Networking for ESXi Hosts

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

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

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

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

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

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

Create FlashStack Datacenter

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

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



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

vmware [®] vSphere Web	Client ਜ ≘	1	ן י ט	Launo	ch vSphere (Client (HTM	IL5)	Administrator	@VSPHERE.LOCAL -
Navigator	FSV-VCSA-1.flashs	stack.cisco.com	11 🗂 🌍	20	Actions	÷ 🛨			
	Gettin Summ	Monitor Config	Permi I	Datac.	Hosts .	. VMs	Datast	Netwo	Linked Extens
		FSV-VCSA-1.flashs	stack.cisco.com					CPU	FREE: 0
C Actions	- FSV-VCSA-1.flashstack.cisco.ci	om)					USED: 0.00 Hz	CAPACITY: 0
🚹 New D	atacenter	ts: U	,					MEMORY	FREE: (
🛅 New F	older							USED: 0.00 B	CAPACITY: (
🎲 Deploy	OVF Template							STORAGE	FREE: (
Export	System Logs							USED: 0.00 B	CAPACITY: (
Reg Assign	License								
Setting	s				 Versio 	n Informat	tion		
vCente	er HA Settings	gory	Description		Version	6.7.0			
Tags &	Custom Attributes	list is empty.			Build	1172711	3		
Add Pe	ermission						_		<u></u>
Alarms		•			▼ Updat	e Manager	Compli	iance	
Update	Manager	•			Status				
								Scan	Detailed Status
			Assign Remo	ove					

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

1 New Datacenter	?	¥
Datacenter name:	FlashStack-VSI	
Location:	🛃 FSV-VCSA	
	OK Cancel)

Create VMware vDS for Infrastructure and Application Traffic

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

FlashStack Infrastructure vDS

To configure the first VMware vDS, follow these steps:

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

vmware vSphere Web Client	ひ Launch vSphere Client (HTML5) Administrator@VSPHERE.LOCAL - H
Navigator I 📑 Flash Stack-VSI 🕤 🎲 🖗	📴 💁 👘 🎯 Actions 🗸 🗧
Getting Started Summary M Getting Started Summary M FSV-VCSA-1 flashstack cisco com FlashStack-VSI Actions - FlashStack-VSI Actions - FlashStack-VSI Pathod Rest New Folder Distributed Switch New Virtual Machine New Vapp from Library Deploy OVF Template Storage Edit Default VM Compatibility Move To Rename Tags & Custom Attributes Add Permission	onitor Configure Permissions Hosts & Clusters VMs Datastores Networks Update Manage Add Host Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up virtualization Image: Complete set-up Image: Complete set-up Image: Complete set-up virtualization Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up Image: Complete set-up <t< th=""></t<>
Allinis Delete All vRealize Orchestrator plugin Actions Pure Storage Update Manager	tup, click Add a host. Learn more about datacenters Learn how to create datacenters Learn about hosts Learn about clusters

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

Len New Distributed Switch				(€)
 1 Name and location 2 Select version 	Ready to complete Review your settings selections before	e finishing the wizard.		
 2 Select version 3 Edit settings 4 Ready to complete 	Name: Version: Number of uplinks: Network I/O Control: Default port group: Suggested next actions Mew Distributed Port Group Add and Manage Hosts These actions will be available	Mangement 6.6.0 4 Enabled IB-Mgmt	outed switch.	
			Back Next Finish	Cancel

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



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

🔊 Mangement - Edit Settings		(9
General Advanced	MTU (Bytes): Multicast filtering mode:	9000 + Basic +	
	Discovery protocol		
	Type:	Cisco Discovery Protocol	
	Operation.	Listen	
	Administrator contact		
	Name:		
	Other details:		
		OK Cancel)

- 9. Click OK to save the changes.
- 10. Expand the FlashStack VSI data center and the newly created vDS.
- 11. Right-click the IB-Mgmt Distributed Port Group, and select Edit Settings...

- 12. Click VLAN, changing VLAN type from None to VLAN, and enter in the appropriate VLAN number for the IB-Mgmt network.
- 13. Click the Teaming and Failover and move the Uplinks 3 and 4 to the Unused uplinks state and move the Uplink 2 to the Standby uplinks state.
- The movement of Uplink 2 to standby is guiding Management traffic to stay within the A side fabric contained within Uplink 1 to prevent unnecessary traffic hops up into the Nexus switch to traverse between fabrics. Uplinks 3 and 4 are set as unused as these are the vMotion vNICs and will be used by the other Distributed Port Group in this vDS.

🍰 IB-Mgmt - Edit Settings				?
General Advanced	Load balancing:	Route based on originating virtual port		
Security	Network failure detection: Notify switches:	Ves	▼ ▼	
VLAN	Failback:	Yes	•	
Teaming and failover Monitoring				
Traffic filtering and marking Miscellaneous	Active uplinks Uplink 1 Standby uplinks			
	Uplink 2			
	Uplink 3			
	Select active and standby up	links. During a failover, standby uplinks activ	rate in the order specified above.	
			OK Cance	<mark>ا ا</mark>

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

vmware [®] vSphere Web Cli	ent fill Eaunch vSphere Client (HTML5) Administrator@VSPHERE.LOCAL •	Help
Navigator I	👝 Infra-DSwitch 🛛 🔽 🍰 🕼 🐼 🤪 🎯 Actions 🗸	<u>=</u> *
	Getting Started Summary Monitor Configure Permissions Ports Hosts VMs Networks	
		8
→ PSV-VCSA-1.flashstack.cisco.com	What is a Distributed Switch?	
FlashStack-VSI	A distributed switch acts as a single virtual switch across all associated hosts. This	
Re-Mamt Actions - Infr	a-DSwitch es to maintain	
Mangem Distributed	Port Group 🔹 New Distributed Port Group	
Add and Ma	anage Hosts Import Distributed Port Group	
🔂 Migrate VM	Is to Another Network 🍰 Manage Distributed Port Groups	
Upgrade	er level, where	
Settings	roups are added to	
Move To	The second part takes	
Rename	are associated with	
Tags & Cus	stom Attributes either through individual	
Alarms	takes place at the	
× Delete	o distributed port groups	
	einer mrougn individual virtual machine NIC	
	networking from the distributed switch itself.	
	Basic Tasks Explore Further	
	Add and manage hosts Learn more about distributed	
	Manage this distributed switch switches	
	Create a new port group Learn how to set up a network with a distributed switch	

- 16. Name the new Port Group vMotion and click Next.
- 17. Change the VLAN type from None to VLAN, select the VLAN ID appropriate for your vMotion traffic, and select the Customize default policies configuration check box under the Advanced section.

Level 2014 New Distributed Port Group			? ••
 1 Select name and location 2 Configure softings 	Configure settings Set general properties of the	new port group.	
 3 Configure policies 3a Security 3b Traffic shaping 3c Teaming and failover 3d Monitoring 3e Miscellaneous 4 Edit additional settings 5 Ready to complete 	Port binding: Port allocation: Number of ports: Network resource pool: VLAN VLAN type: VLAN ID: Advanced Customize default police	Static binding • Elastic • Blastic port groups automatically increase or decrease the number of ports as needed. 8 • (default) • 1130 • es configuration	
		Back Next Finish Can	cel

18. Click Next.

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

Ø.

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

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

2 New Distributed Port Group		9	*
 New Distributed Port Group 1 Select name and location 2 Configure settings 3 Configure policies 3a Security 3b Traffic shaping 3c Teaming and failover 3d Monitoring 3e Miscellaneous 	Teaming and failover Controls load balancing, netw Load balancing: Network failure detection: Notify switches: Failback: Failover order	Route based on originating virtual port • Link status only • Yes • Yes •	44
 4 Edit additional settings 5 Ready to complete 	Active uplinks Uplink 4 Standby uplinks Unused uplinks Uplink 2 Uplink 1 Select active and standby up	plinks. During a failover, standby uplinks activate in the order specified above.	
		Back Next Finish Cancel	

21. Click Next

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

😤 New Distributed Port Group				(4 (?)
 1 Select name and location 2 Configure settings 	Ready to complete Review the changes before proceed	ling.		
 3 Configure policies 3a Security 3b Traftic shaping 3c Teaming and failover 3d Monitoring 3e Miscellaneous 4 Edit additional settings 5 Ready to complete 	Distributed port group name: Port binding: Number of ports: Port allocation: Network resource pool: VLAN ID:	vMotion Static binding 8 Elastic (default) 1130		
			Back Next Finish	Cancel

24. Click Finish to create the Distributed Port Group.

FlashStack Application vDS

To configure the second VMware vDS, follow these steps:

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

Lange Switch				(€ €				
 1 Name and location 2 Select version 	Ready to complete Review your settings selections befor	Ready to complete Review your settings selections before finishing the wizard.						
 3 Edit settings 4 Ready to complete 	Name: Version: Number of uplinks: Network I/O Control: Default port group: Suggested next actions New Distributed Port Group Add and Manage Hosts These actions will be available	App-DSwitch 6.6.0 2 Disabled App-1301	buted switch.					
			Back	lext Finish Cancel				

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

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

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

Add the VMware ESXi Hosts Using the VMware vSphere Web Client

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

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

vmware [®] vSphere Web Client	ن ا	Launch vSphere Client (HTML5) Administrator@VSPHERE.LOCAL +
Navigator 📕 📑 Flash Stack-V	SI 📋 🎁 🎝 🏠 🟠 🛞 Act	ions 🕶
Getting Started	Summary Monitor Configure P	ermissions Hosts & Clusters VMs Datastores Networks Update Mana
FSV-VCSA-1.flashstack.cisco.com Create Dat FlashStack2VSI Create Dat Actions - FlashStack-VSI	tacenter 💈 Add Host ₃ Add 1	Virtual Machine 🔄 Complete set-up
Add Host New Cluster New Folder Dictinuted Switch	r that uses virtualization SX or ESXI, to run virtual host to the inventory nanagement of a vCenter	Virtual Machines
New Virtual Machine Rew VApp from Library Deploy OVF Template	er running ESX or ESXi t have ESX or ESXi wware Web site for	Cluster
Storage Edit Default VM Compatibility	nust know the credentials	Host
Migrate VMs to Another Network		Datacenter
Move To Rename Tags & Custom Attributes	vSp	here Client
Add Permission Alarms	,	Fundam Sutther
× Delete	er Server setup, click Add a host.	Learn more about datacenters
All vRealize Orchestrator plugin Action Pure Storage Update Manager	s • ster	Learn how to create datacenters Learn about hosts
		Learn about clusters

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

🗊 New Cluster	? »
Name	Production
Location	FlashStack-VSI
▼ DRS	Turn ON
Automation Level	Fully automated 🔹
Migration Threshold	Conservative Aggressive
vSphere HA	Turn ON
Host Monitoring	Enable host monitoring
Admission Control	Enable admission control
✓ VM Monitoring	
VM Monitoring Status	Disabled ▼ Overrides for individual VMs can be set from the VM Overrides page from Manage Settings area.
Monitoring Sensitivity	Low High
▶ EVC	Disable 🔹
VSAN	Turn ON
	OK Cancel

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

vmware vSphere Web Clie	ent † ≣			U	Launch vS	phere Clie	ent (HTN	1L5) Ad	lministrator@	VSPHERE.LOCAL -	Help
Navigator I	Production	1 🖪 1	5 28 8) 🐼 Actio	ons 🔻						≡∗
	Getting Started	Summary	Monitor	Configure	Permissions	Hosts	VMs	Datastores	Networks	Update Manager	
	_										8
- FSV-VCSA-1.flashstack.cisco.com	What is a Clus	ter?									
FlashStack-VSI	A cluster is a g host to a cluste	roup of hosts er, the host's	s. When you resources	u add a	R	1					
Actions - Production	rt	of the cluste	r's resource rces of all h	es. The	2						
Add Host	9							Virtual Mad	chines		
Miove Hosts into Cluster.		e the vSpher	re High Avai	ilability	Cluster			- AN			
New Virtual Machine	► h	ere Distribute	ed Resourc	e				AD	•		
New VApp	• •	S), and the v	SAN SOLULO	ms.				No.			
Depley OVE Templete					2		>	н	lost		
Deploy OVP Template					1		<				
Restore Resource Pool 1	Free					5		-			
Storage	•					ontor Sou	[)atacenter			
Host Profiles	•			,	Sphere Client	ciller aci	IVEI				
Edit Default VM Compati	bility										
Assign License											
Settings					Explore F	urther					
Move To	2	ost			l earn i	more al	out clu	isters			
Rename		new virtu:	al machin		Learn	more at			de		
Tags & Custom Attributes	5 •	TIEW VILLA		-	Leann	nore as	Jouries	ource poc	//3		
Add Permission											
Alarms	•										
X Delete											

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

Tadd Host		(°))							
1 Name and location	Enter the name or IP addre	inter the name or IP address of the host to add to vCenter Server.							
2 Connection settings	Host name or IP address:	10.2.164.67							
3 Hostsummary	Location:	Production							
4 Resource pool	Type:	ESXI -							
5 Ready to complete	.,,								
		Back Next Finish Cancel							

- 6. Enter root for the User Name, provide the password set during initial setup and click Next.
- 7. Click Yes in the Security Alert pop-up to confirm the host's certificate.
- 8. Click Next past the Host summary dialogue.

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

1 Add Host		(* §
 1 Name and location 	Name	10.2.164.70
✓ 2 Connection settings	Version	VMware ESXi 6.7.0 build-10302608
✓ 3 Host summary	License	License 1
✓ 4 Assign license	Networks	VM Network
✓ 5 Lockdown mode	Datastores	FSV-vVol
✓ 6 Resource pool	Lockdown mode	Disabled
7 Ready to complete	Resources destination	Production
		Back Next Finish Cancel

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

Pure Storage vSphere Web Client Plugin

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

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

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

۲		System	Network	Users Softv	/are				
۲		Updates			Auto	Download 🚺	vSphere Plugin		ß
~		Name		Version	Status	Progress	vCenter Host	-	
Q	Analysis			No updates fo	und.		Administrator User	-	
	Performance						Administrator Password	-	
	Capacity						Version on vCenter	-	
							Available Version	3.1.1	
÷	Health								
-	Settings								

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

Edit vSphere Plugi	n Configuration ×
vCenter Host	10.1.164.20
Administrator User	administrator@vsphere.local
Administrator Password	•••••
	Cancel Reset Save

4. After the discovery completes. Click Install.

vSphere Plugin		ß
vCenter Host Administrator User	10.1.164.20 administrator@vsphere.local	
Administrator Password Version on vCenter	-	
Available Version	3.1.1	Install

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

Navigator	🚺 FlashArray				
	Objects				
付 Home					
Hosts and Clusters	Role Based Access Contr	Add FlashArray		×	
WMs and Templates	FlashArray Alias	FlashArray URL	Online This list is empty		Compatible
Storage			nia nacia empty.		
Q Networking		_			
Content Libraries					
Global Inventory Lists					
Policies and Profiles	Add Fla	Add FlashArray X			
🔬 Update Manager	FlashA CSPG	rrayName -RTP-1			_
administration	FlashA	rrayURL			
😴 Tasks	10.2.1	64.45			
I Events	Usema	ime			
Tags & Custom Attributes	- Passw	ord			
Q New Search	-	*			
Saved Searches					
🔁 Pure Storage			Add	Cance	
					•
	M			0 0	bjects 📑 Export 📑 Copy 🗸

6. Add the FlashArray as a Storage Provider by clicking the 'Register Storage Provider' (²²) icon and providing the login information for the FlashArray.

Register Storage Provider	×
By clicking 'Register', the storage providers on each controller for this FlashArray will be registered with vCenter.	
FlashArrayUsemame	
pureuser	
FlashArray Password	
******	ור
	_
Register	

7. Verify that the FlashArray is registered correctly as a storage provider.

8. Select Host and Cluster, Select the vCenter Server.



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

FSV-VCSA-1.flashstack.cisco.com	🚹 🎦 🎲 😼 🎯 Actions 👻							
Getting Started Summary Monitor	Configure Permissions Datacente	rs Hosts & Clusters VMs	Datastores	Networks Linke	d vCenter Server Systems Extensions	Update Manage	er	
	Storage Providers							
✓ Settings	+ 🛃 🗏 🗙				Group by:	Storage provide	er 🔹 Q C	SPG +
General	Storage Provider/Storage System	Status	Active/Standby	Priority	URL	Last Rescan Time	VASA API Version	Certificate Expiry
Licensing		Online			https://10.2.164.46:8084/version	5/1/2019 1:28	3.0	357 days
Message of the Day	cspg-rtp-1 (2/2 online)		Active	200				
Advanced Settings		Online			https://10.2.164.47:8084/version		3.0	357 days
Auto Deploy	cspg-rtp-1 (2/2 online)		Standby	200				
vCenter HA								
✓ More								
Key Management Servers								
Storage Providers								

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

Import Protection Group as VM Storage Policy

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

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

Navigator I	🔿 FlashArray			
	Objects			
👎 FlashArray 📃				
	🔓 Role Based Access Contr 🖣	Add FlashArray 📔 🗕 Remove Flash	nArray 🥜 Edit FlashArray 🖀 Regis	ter Storage Provider 📅 Import Protection Groups
CSPG-RTP-T	FlashArray Alias	FlashArray URL	Online	Compatible
	CSPG-RTP-1	https://10.2.164.45	true	true

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

Import Protection Groups					
Select which Protection Groups to import as VM Storage Policies:		e			
Import	Protection Group Name	*			
	platinum (local snapshot every 1 hour, no remote replication)				
	pure-vasa-default (no local snapshot or remote replication)				
		1-2 of 2 < >			
		Import Cancel			

Add Datastores

么

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

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

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

Navigator	Ŧ	Production	1 📑 🔁 🔠 🍪 🖓 Actions 🗸
		Getting Started	Summary Monitor Configure Per
▼ Production	ashstack.cisco.com VSI Actions - Production Add Host Move Hosts into Clu New Virtual Machin New VApp New Resource Poo Deploy OVF Templa Restore Resource F Storage Host Profiles Edit Default VM Cor	Getting Started What is a Clus A cluster is a g host to a cluster uster e I ate Pool Tree	Summary Monitor Configure Perinter? Inter? Inter? Inter of hosts. When you add a ter, the host's resources. The the resources of all hosts Inter vSphere High Availability Distributed Resource and the vSAN solutions. Note: Solution the vSAN solution the vS
	Assign License Settings Move To Rename Tags & Custom Attr Add Permission Alarms Delete	ibutes	ew virtual machine
Task Name Update service Start service Open firewall ports Update service activ	All vRealize Orches Pure Storage Update Manager vSAN	trator plugin Actions 10.2.164.71 10.2.164.71 10.2.164.71 10.2.164.71	Create Datastore Create Snapshots Configure Multipathing Configure iSCSI Update Cluster Protection Add Host Group

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

Create Datastore		 	(lpha)
Datastore Type VMFS VVol			
Datastore Name ESXi-Swap		 	
Datastore Size			
VMFS Options VMFS 5 VMFS 6			•
Select Pure Storag	je Array		•
▷ II Production	60 T	L	
			1-1 of 1 < >
Pure Storage Prot	ection Group (optional)	Joined	e
Joined Protection	Group Name		•
			Create Cancel

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

Create Datastore	۲
Datastore Type VMFS VVol	
Datastore Name FSV-vVol	
Storage Container Wol container	
Select Pure Storage Array CSPG-RTP-1	•
Select Host / Cluster	e
▷ II Production	
	1-1 of 1 < >
	Create Cancel

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

						? >>
Select storage						
Select the datastore in which	to store the configuration	and disk files				
VM storage policy: FlashArray Snap 1 HOURS				vare rtual		
Name	Capacity	Provisioned	Free	Туре	Cluster	*
Compatible						
FSV-vVol	0.00 B	0.00 B	0.00 B	VVol		::
Incompatible						
fsv-upgrade-data	2.00 TB	31.96 GB	1.97 TB	VMFS 6		
EQVi Quan DQ	1 022 75 GP	1.42 GP	1 022 22 GP	V/MEQ.6		• •

Configure ESXi Settings

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

To configure ESXi settings, follow these steps:

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

VMWare [®] vSphere Web Clie	ent fi ≘ Updated at 1	12:53 PM 🕐 Launch v	Sphere Client (HTML5) Administrator@VSP	PHERE.LOCAL - Help
Navigator I	10.2.164.71 🛃 🔂 🕞 🗋	💽 💮 Actions 👻		≡∗
	Summary Monitor Configure Pe	ermissions VMs Datasto	ores Networks Update Manager	
▼ PSV-VCSA-1.flashstack.cisco.com		Time Configuration		Edit
➡ FlashStack-VSI	Licensing	Date & Time:	4/26/2019 1:50 PM	
➡ I Production	Time Configuration	NTP Client:	Disabled	
10.2.164.68	Authentication Services	NTP Service Status:	Stopped	
10.2.164.69	Certificate	NTT DENNCE Otatus.	Glopped	
10.2.164.70	Power Management	NTP Servers:		
<u>⊼</u> 10.2.164.71	Advanced System Settings			
10.2.164.72	Advanced system settings			
10.2.164.73	System Resource Reservation			

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

	10.2.164.71: Edit Time Configuration ?				
Spe	ecify how the date and time on th	is host should be set.			
\bigcirc	Manually configure the date and time on this host				
ullet	Use Network Time Protocol (Ena	ble NTP client)			
	NTP Service Status:	Start Stop Restart The NTP Service settings are updated when you click Start, Restart, or Stop.			
	NTP Service Startup Policy:	Start and stop manually - User starts and stops the service manually			
	NTP Servers:	172.26.163.254 Separate servers with commas, e.g. 10.31.21.2, fe00::2800			
		OK Cancel			

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

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

Summary Monitor Configure Pe	Permissions VMs	Datastores Networks Update Manager		
	services			
Time Configuration	Name	Daemon		
Authentication Services	Direct Console	UI Running		
Certificate	ESXi Shell	Running		
Power Management	SSH	Running		
Advanced System Settings	Load-Based Te	eaming Daemon Running		
System Resource Reservation	Active Directory	y Service Stopped		
Security Profile	NTP Daemon	Running		
System Swap	PC/SC Smart C	Card Daemon Stopped		
Host Profile	CIM Server	Stopped		
- Hardwaro	SNMP Server	Stopped		
	Syslog Server	Running		
Processors	vSphere High A	Availability Agent Running		
Memory	VMware vCente	ter Agent Running		
Power Management	X.Org Server	Stopped		
PCI Devices ::	i Finance II			
	Firewall	Edit		
Virtual Flash Resource		onnections		
Management	CIM Server	5988 (TCP) All		
Virtual Flash Host Swap Cache Configuration	CIM Secure Se	erver 5989 (TCP) All		
▲ ►	CIM SLP	427 (UDP,TCP) All		

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

10.2.164.71: Edit Security Profile						
To provide access to a service or client, check the corresponding box. By default, daemons will start automatically when any of their ports are opened, and stop when all of their ports are closed.						
Name		Daemon				
Direct Console UI		Running				
ESXi Shell		Running				
SSH		Running				
Load-Based Teaming	ng Daemon	Running				
Active Directory Se	rvice	Stopped				
NTP Daemon		Running	Ŧ			
✓ Service Details Status	Running					
olulus	Start Stop Restart Note: Action will take place immediately					
Startup Policy	Start and stop manually - Start and stop with host					
	Start and stop manually Start and stop with port usage					
		ОК Са	ancel			

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

Summary Monitor Configure	Permis	sions VI	ls	Datastores	Network	s Updat	te Manager	
44	Sj	stem Swa)					Edit
Time Configuration Authentication Services	•	System Swa	ар		C	an use hos an use dat	st cache tastore specified by host for swap file	s
Certificate								
Power Management								
Advanced System Settings								
System Resource Reservation								
Security Profile								
System Swap								
Host Profile								
Processors								
Memory								
Power Management								
PCI Devices								
Virtual Flash Resource Management								
Virtual Flash Host Swap Cache Configuration	•							

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

10.2.164.71 - Edit System Swap Settings	(?) ▶
 Enabled If an option is selected, the system swap is allowed to use this sp Can use datastore: ESXi-Swap Can use host cache Can use datastore specified by host for swap files 	oace.
OK Car	icel

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

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

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

to <u>Cisco UCS HW and SW Availability Interoperability Matrix</u>. If a more recent driver is made available that is appropriate for VMware vSphere 6.7 U1, to update the drivers, follow these steps:

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

ESXi-Swap	Swap 📴 🛱 🔁 🔯 Kations 🗸							
Getting Started	Summary Monitor Configure	Permissions Files Hosts	VMs FlashArray Snapshot	Objects Pure Storage				
[ESXi-Swap] Q Search C M M M M M M M M M M M M M M M M M M								
🤝 📑 ESXi-Swap	Name	Size	Modified	Туре	Path			
▶ 🛅 .sdd.sf	🛅 .sdd.sf			Folder	[ESXi-Swap] .sdd.sf			
	SysSwap-ds-5cc33793	1,048,576.00 KB	4/26/2019 2:25 PM	File	[ESXi-Swap] sysSwap-ds-5			

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

```
esxcli software vib update -d /vmfs/volumes/ESXi-Swap/VMW-ESX-6.7.0-nenic-
1.0.26.0-offline_bundle-10825029.zip
```

- 9. Reboot each host by typing reboot from the SSH connection after the command has run.
- 10. Log into the Host Client on each host once reboot is complete.

Add the ESXi Hosts to the vDS

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

1. Within the Networking tab of the Navigator window, right-click the Infra-DSwitch vDS and select Add and Manage Hosts...
| Navigator I | 📖 Infra-D Switch | n 🙁 🕹 🕼 🕫 | . 🚕 🔯 Ac | ctions 👻 | | | ≡∗ |
|--|------------------|-----------------|------------|---------------------|-------------|----------------------|-------|
| | Getting Started | Summary Monitor | Configure | Permissions Ports | Hosts VMs N | Vetworks | |
| Image: Constraint of the state of | Hosts | | | | ×. | Q Filter | - |
| M Network | Name | 1 🔺 Sta | ate | | Status | Cluster | |
| App-DSwitch | | | | This list is empty. | | | |
| App-DSwitch-DVUplinks-152 | | | | | | | |
| □ Infra-D Antiene Jafes DCuvitab | | | | | | | |
| B-IB-I Distributed Port Group | | | | | | | |
| Ma 🔂 Add and Manage Hosts | | | | | | | |
| 🐣 VM 🙀 Migrate VMs to Another Networ | k | | | | | | |
| Upgrade | • | | | | | | |
| Settings | • | | | | | | |
| Move To
Rename | | | | | | | |
| Tags & Custom Attributes | • | | | | | | |
| Alarms | • | | | | | | |
| × Delete | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | 4 | | | | | | Þ |
| | M | | | | 0 | Objects 📑 Export 😭 C | ору 🕶 |

2. Leave Add hosts selected and click Next.

🕞 Add and Manage Hosts	?
Add and Manage Hosts Select task Select hosts Select network adapter tasks Manage physical network adapters Manage VMkernel network adapters Analyze impact 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. Add host and manage host networking (advanced) Add new hosts and manage networking of hosts already attached to this distributed switch. Use this option to unify the network configuration of new and existing hosts.
	Back Next Finish Cancel

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

B	Add and Manage Hosts		(?
~	1 Select task	Select hosts Select hosts to add to this distributed switch.	
	2 Select hosts		
	3 Select network adapter tasks	🕂 New hosts 🗶 Remove	
	4 Manage physical network adapters	Host	Host Status
	5 Manage VMkernel network adapters	This list is	s empty.
	6 Analyze impact		
	7 Ready to complete		
		Configure identical network settings on multiple bosts (template	mode)
		e eningere reenreer neuron oorange en manple hoots (template	nove, w
			Back Next Finish Cancel

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.

Select new hosts		×
Incompatible Hosts		Q Filter
✓ Host	Host State	Cluster
10.2.164.70	Connected	Production
10.2.164.71	Connected	Production
A Q Find -		6 items 🖺 Copy 🗸
		OK Cancel

5. Click Next.

C	Add and Manage Hosts				
>	1	Selecttask	Select hosts Select hosts to add to this distributed switch.		
	2	Select hosts			
	3	Select network adapter tasks	4 New hosts 🗶 Remove		
	4	Manage physical network adapters	Host	Host Status	
	5	Manage VMkernel network	(New) 10.2.164.70	Connected	
	-	adapters	(New) 10.2.164.71	Connected	
	6	Analyze impact			
	7	Ready to complete			
			Configure identical network settings on multiple hosts (template	e mode). 🚯	
				Back Next Finish Cancel	

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

🕼 Add and Manage Hosts		?
✓ 1 Selecttask	Select network adapter tasks Select the network adapter tasks to perform.	
 2 Select hosts 3 Select network adapter tasks 4 Manage physical network adapters 5 Manage VMkernel network adapters 6 Analyze impact 7 Ready to complete 	Select the network adapter tasks to perform. Manage physical adapters Add physical network adapters to the distributed switch, assign them to uplinks, or remove existing ones. Manage VMkernel adapters Add or migrate VMkernel network adapters to this distributed switch, assign them to distributed port groups, configure VMkernel adapter settings, or remove existing ones. Migrate vtM network adapters by assigning them to distributed port groups on the distributed switch. Sample distributed switch Manage VMkernel adapters VMkernel port group VMkernel ports VMkernel ports V	
	Back Next Finish	Cancel

- 🕼 Add and Manage Hosts ? Manage physical network adapters 1 Select task Add Select an Uplink for vmnic0 x 2 Select hosts 3 Select network adapter tasks Assigned Adapter Uplink 4 Manage physical network adapters Uplink 1 Hos Uplink Port Group 5 Manage VMkernel network adapters Uplink 2 ---* ----Uplink 3 6 Analyze impact Uplink 4 --7 Ready to complete (Auto-assign) -Cancel OK vSwitch0 🗾 vmnic0 💓 vmnic1 vmnic2 vmnic3 Back Next Cancel
- 7. Select vmnic0 from the Host/Physical Network Adapters column and click the Assign uplink option.

8. Leave Uplink 1 selected and click OK.

C	Add and Manage Hosts					?
č	1 Selecttask 2 Selecthosts	Manage physical network adapters Add or remove physical network adap	oters to this distributed switch.			
~	3 Select network adapter tasks	🖬 Assign uplink 🖃 Reset change	🚯 View settings			
	4 adapters	Host/Physical Network Adapters	1 A In Use by Switch	Uplink	Uplink Port Group	
	5 Manage VMkernel network	- 🗑 10.2.164.70				<u>*</u>
	adapters	 On this switch 				
	6 Analyze impact	vmnic0 (Assigned)	vSwitch0	Uplink 1	Mangement-DVU	plinks
	7 Ready to complete	 On other switches/unclaimed 				
		vmnic1	vSwitch0	-		
		vmnic2	vSwitch2			
		vmnic3	vSwitch2			
		vmnic4	-	-		
		vmnic5	-	-		
		On this switch				
		 On other switches/unclaimed 				
		vmnic0	vSwitch0			
		vmnic1	-			
		vmnic2	-	-		
		vmnic3	-			
						٣
				Back	Next Finish	Cancel

- 9. Repeat this step for vmnic1-3, assigning them to uplinks 2-4 in corresponding sequence.
- 10. Repeat these assignments for all additional ESXi hosts being configured.

Add and Manage Hosts				0
 ✓ 1 Selecttask ✓ 2 Select hosts 	Manage physical network adapters Add or remove physical network adap	pters to this distributed switch.		
 3 Select network adapter tasks 	🔤 Assign uplink 🐚 Reset change	es 🚯 View settings		
4 Manage physical network adapters	Host/Physical Network Adapters	1 A In Use by Switch	Uplink	Uplink Port Group
5 Manage VMkernel network				<u>م</u>
adapters	✓ On this switch			
6 Analyze impact	vmnic0 (Assigned)	vSwitch0	Uplink 1	Mangement-DVUplinks
7 Ready to complete	vmnic1 (Assigned)	vSwitch0	Uplink 2	Mangement-DVUplinks
	vmnic2 (Assigned)	vSwitch2	Uplink 3	Mangement-DVUplinks
	vmnic3 (Assigned)	vSwitch2	Uplink 4	Mangement-DVUplinks
	 On other switches/unclaimed 			
	vmnic4			
	vmnic5			-
	- 10.2.164.71			
	✓ On this switch			
	vmnic0 (Assigned)	vSwitch0	Uplink 1	Mangement-DVUplinks
	vmnic1 (Assigned)		Uplink 2	Mangement-DVUplinks
	vmnic2 (Assigned)		Uplink 3	Mangement-DVUplinks
	vmnic3 (Assigned)		Uplink 4	Mangement-DVUplinks
	 On other switches/unclaimed 			
				•
			Back	Next Finish Cancel

11. Click Next.

Add and Manage Hosts								
 ✓ 1 Selecttask ✓ 2 Selecthosts 	Manage VMkernel network adapters Manage and assign VMkernel network adapters to the distributed switch.							
3 Select network adapter tasks 4 Manage physical network adapters	VMkernel network adapters with the warning sign might lose network connectivity unless they are migrated to the distributed switch. Select a destination port group to migrate them.							
5 Manage VMkernel network adapters	Assign port group New adapter Host/Vilkernel Network Adapters	Edit adapter X Remove 1	Changes 🕜 View sett	Destination Port Group				
7 Ready to complete	On this switch							
	vmk0 ▼ 10.2.164.71	vSwitch0	Management Network	Do not migrate				
	On this switch • On other switches							
	Mik0	vSwitch0	Management Network	Do not migrate				
			Back Next	Finish Cancel				

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

Assign destination port group	×
Show all columns	
C	Q Filter
Name	
🚨 IB-Mgmt	
2 vMotion	
A Q Find	2 items 🖺 Copy 🗸
	OK Cancel

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

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

Add and Manage Hosts				(?)		
 ✓ 1 Selecttask ✓ 2 Selecthosts 	Manage VMixemel network adapters Manage and assign VMixemel network adapters to the distributed switch.					
3 Select network adapter tasks 4 Manage physical network adapters	VMkernel network adapters with the warning sign might lose network connectivity unless they are migrated to the distributed switch. Select a destination port group to migrate them.					
5 Manage VMkernel network adapters 6 Analyze impact	Host/Witemel Network Adapters 1 102.156.70 0.01 bis excitch	In Use by Switch	Source Port Group	Destination Port Group		
/ Keady to complete	On this switch my which which	vSwitch0	Management Network	IB-Mgmt		
	 ✓ On this switch ₩ wnk0 (Reassigned) ✓ On other switches 	vSwitch0	Management Network	IB-Mgmt		
			Back Next	Finish Cancel		

- 15. Click Next.
- 16. Click Next past Analyze impact.

🖟 Add and Manage Hosts		?
 1 Select task 2 Select hosts 	Ready to complete Review your settings selections before finishing the wizard.	
✓ 3 Select network adapter tasks	Number of managed hosts	
 4 Manage physical network adapters 	Hosts to add: 2	
 5 Manage VMkernel network adapters 	Number of network adapters for update Physical network adapters: 8	
 6 Analyze impact 7 Ready to complete 	Reassigned VMkernel network 2 adapters:	
	Back Next Finis	h Cancel

- 17. Review the settings and click Finish to apply.
- 18. Within the Networking tab of the Navigator window, right-click the App-DSwitch vDS and select Add and Manage Hosts...

Navigator I	👝 App-D Switch 🛛 😤 🧕 🚺	💤 🧔 🛛 🔯 Actions 👻		=×
	Getting Started Summary Monit	or Configure Permissions Por	ts Hosts VMs N	letworks
♥ ■ Q ▼ PSV-VCSA-1.flashstack.cisco.com	Hosts			
▼ hashStack-VSI			V II	Q Filter
VM Network	Name	State	Status	Cluster
Actions - App-DSwitch		This list is empty.		
Distributed Port Group	•			
🧕 🎼 Add and Manage Hosts				
🔜 🚵 Migrate VMs to Another Network				
🕶 📖 Infr Upgrade	•			
settings	•			
Move To				
Rename				
Tags & Custom Attributes	•			
Alarms	•			
× Delete				
	1 III III		0.0	Objects Export Copy -
	1011		0.	objects and state objects

19. Leave Add hosts selected and click Next.

🚯 Add and Manage Hosts		?
1 Select task 2 Select hosts	Select task Select a task to perform on this distributed switch.	
 Select network adapter tasks Manage physical network adapters Manage VMkernel network adapters Analyze impact Ready to complete 	 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. Add host and manage host networking (advanced) Add new hosts and manage networking of hosts already attached to this distributed switch. Use this option to unify the network configuration of new and existing hosts. 	
	Back Next Finish Can	.cel

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

	Add	and Manage Hosts	?
>	15	electtask	Select hosts Select hosts to add to this distributed switch.
	2 S	elect hosts	
	3 S	ielect network adapter tasks	🕂 New hosts 💥 Remove
	4 ^N a	lanage physical network dapters	Host Host Status
	5 ^N a	lanage VMkernel network dapters	This list is empty.
	6 A	nalyze impact	
	7 R	teady to complete	
			Configure identical network settings on multiple hosts (template mode). 1
			Back Next Finish Cancel

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

Select new hosts		×
Incompatible Hosts		Q Filter
✓ Host	Host State	Cluster
10.2.164.70	Connected	Production
10.2.164.71	Connected	Production
A Find	•	6 items 🕒 Copy 🗸
		OK Cancel

22. Click Next.

	Add and Manage Hosts		(?)
~	1 Select task	Select hosts Select hosts to add to this distributed switch.	
	Select network adapter tasks Manage physical network	♣ New hosts 🗙 Remove	
	4 adapters	Host	Host Status
	5 Manage VMkernel network adapters	 (New) 10.2.164.70 (New) 10.2.164.71 	Connected Connected
	6 Analyze impact		
	7 Ready to complete		
		Configure identical network settings on multiple basts (template	
		Configure identical network settings on multiple hosts (template	emode). 😈
			Back Next Finish Cancel

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

🕼 Add and Manage Hosts	(?)
 1 Select task 2 Select hosts 3 Select network adapter tasks 	Select network adapter tasks Select the network adapter tasks to perform.
4 Manage physical network adapters	Add physical network adapters to the distributed switch, assign them to uplinks, or remove existing ones.
5 Analyze impact 6 Ready to complete	Manage VMkernel adapters Add or migrate VMkernel network adapters to this distributed switch, assign them to distributed port groups, configure VMkernel adapter settings, or remove existing ones.
	Migrate virtual machine networking Migrate VM network adapters by assigning them to distributed port groups on the distributed switch.
	Sample distributed switch
	VMkernel port group VMikernel ports v VMkernel ports vulplink port group v VM port group vmic v Virtual Machines vmic
	Back Next Finish Cancel

24. Click Next.

Add	l and Manage Hosts					(?)
✓ 1 S	elect task	Manage physical network ada Add Select an Uplink for vr	pters nnic4	(x)		
✓ 2 S	elect network adapter tasks	Uplink	Assigned Adapter			
4 <mark>M</mark>	anage physical network dapters	Host Uplink 1	-		Uplink Port Group	
5 A.	nalyze impact	✓ Uplink 2				^
6 R	eady to complete	(Auto-assign)				
					-	
					-	
					-	
					-	
		× 1				
			OK	Cancel		
		vmnic0	Infra-DSwitch		-	
		🗾 vmnic1	Infra-DSwitch	-	-	
		mic2	Infra-DSwitch			
		vmnic3	Infra-DSwitch			
				Pack	Novt Einich	Cancel
				Back	Pinish	Cancer

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

26. Leave Uplink 1 selected and click OK.

Add and Manage Hosts					(?)
 ✓ 1 Selecttask ✓ 2 Selecthosts 	Manage physical network adapters Add or remove physical network ada	pters to this distributed switch.			
 3 Select network adapter tasks 	🐻 Assign uplink 🖃 Reset change	es 👩 View settings			
4 Manage physical network adapters	Host/Physical Network Adapters	1 🛦 In Use by Switch	Uplink	Uplink Port Group	
5 Analyze impact 6 Ready to complete	 On this switch 				
	 vmnic4 (Assigned) On other switches/unclaimed 		Uplink 1	App-DSwitch-DVUp	plink
	vmnic0	Infra-DSwitch	-	-	
	vmnic1	Infra-DSwitch			
	vmnic2	Infra-DSwitch			
	vmnic3	Infra-DSwitch			
	vmnic5	-			
	√ 10.2.164.71				
	On this switch				
	 On other switches/unclaimed 				
	vmnic0	Infra-DSwitch			
	vmnic1	Infra-DSwitch			
	vmnic2	Infra-DSwitch			
	vmnic3	Infra-DSwitch	-		
	and a second a d				•
			Back	Next Einish	Cancel
			Dack	HEAL PHISH	Cancel

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

Add and Manage Hosts				0
 ✓ 1 Selecttask ✓ 2 Selecthosts 	Manage physical network adapters Add or remove physical network adapt	ers to this distributed switch.		
 3 Select network adapter tasks 	🔤 Assign uplink 🕐 Reset changes	1 View settings		
4 Manage physical network adapters	Host/Physical Network Adapters	1 A In Use by Switch	Uplink	Uplink Port Group
5 Analyze impact	- 🕤 10.2.164.70			•
6 Ready to complete	 On this switch 			
o neady to complete	vmnic4 (Assigned)		Uplink 1	App-DSwitch-DVUplink
	vmnic5 (Assigned)		Uplink 2	App-DSwitch-DVUplink
	 On other switches/unclaimed 			
	Vmnic0	Infra-DSwitch		
	pm vmnic1	Infra-DSwitch		
	Minic2	Infra-DSwitch		- ::
	Vmnic3	Infra-DSwitch		
	- 10.2.164.71			
	 On this switch 			
	vmnic4 (Assigned)	-	Uplink 1	App-DSwitch-DVUplink
	vmnic5 (Assigned)	-	Uplink 2	App-DSwitch-DVUplink
	 On other switches/unclaimed 			
	vmnic0	Infra-DSwitch		-
	vmnic1	Infra-DSwitch		-
		tata BALINA		÷
			Back	Next Finish Cancel

28. Click Next.

29. Click Next past Analyze impact.

Add and Manage Hosts		?
 1 Select task 2 Select hosts 3 Select network adapter tasks 4 Manage physical network adapters 5 Analyze impact 6 Ready to complete 	Ready to complete Review your settings selections before finishing the wizard. Number of managed hosts Hosts to add: 2 Number of network adapters for update Physical network adapters: 4	
	Back Next Finish Can	icel

30. Review the settings and click Finish to apply.

Create vMotion VMkernel adapters

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

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

Navigator	10.2.164.71 🛃 🛃 🕞 🛅	🛐 🚳 Actio	ons 👻		<u>I</u> I
	Summary Monitor Configure P	ermissions V	Ms Datastores Network	ks Update Manager	
Image: Image of the second	++ > Storage	VMkernel ad	apters ≧ ▼	Q Filter	•
✓ IProduction	✓ Networking	Device	Network Label	Switch	IP Address
■ 10.2.164.68	Virtual switches	💌 vmk1	🧕 iScsiBootPG	1 iScsiBootvSwitch	192.168.101.3
10.2.104.09 10.2.164.70	VMkernel adapters	👥 vmk2	VMKernel-iSCSI-B	1 vSwitch1	192.168.102.22
10.2.164.71	Physical adapters	👥 vmk0	🚨 IB-Mgmt	Infra-DSwitch	10.2.164.71
10.2.164.72	TCP/IP configuration				

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

Select Network			×
Show all columns			
G		Q Filter	•
Name	Distributed Switch		
2 App-1301	App-DSwitch		
App-1302	App-DSwitch		
2 App-1303	App-DSwitch		
🚨 IB-Mgmt	Infra-DSwitch		
2 vMotion	Infra-DSwitch		
A Find	•	5 items	Copy 🗸
		ОК	Cancel

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

10.2.164.71 - Add Networking		(?) ▶
 1 Select connection type 2 Select target device 3 Connection settings 3a Port properties 3b IPv4 settings 4 Ready to complete 	Select target device Select a target device for the new connection. • Select an existing network VMotion Browse	
	O New standard switch	
	Back Next Finish C	ancel

7. Click Next.

10.2.164.71 - Add Networking		(?	*
 1 Select connection type 2 Select target device 	Port properties Specify VMkernel port settings.		
 2 Select arger device 3 Connection settings 3a Port properties 3b IPv4 settings 4 Ready to complete 	VMIkemel port settings Network label: IP settings: TCP/IP stack: Available services Enabled services:	VMotion(Infra-DSwitch)	
		 Provisioning Fault Tolerance logging Management vSphere Replication vSphere Replication NFC vSAN 	
		Back Next Finish Cance	<u>ال</u>

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

10.2.164.71 - Add Networking		(?) **
 1 Select connection type 2 Select tarriet device 	IPv4 settings Specify VMkernel IPv4 settings.	
3 Connection settings 3 a Port properties	 Obtain IPv4 settings automatically Use static IPv4 settings 	
4 Ready to complete	IPv4 address: Subnet mask:	192.168.130.72 255.255.255.0
	Default gateway: DNS server addresses:	Override default gateway for this adapter
		Back Next Finish Cancel

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

10.2.164.71 - Add Networking						(€
 1 Select connection type 2 Select target device 	Ready to complete Review your settings selections before finishing the wizard.					
3 Connection settings	Distributed port group:	vMotion				
 3a Port properties 	Distributed switch:	Infra-DSwitch				
✓ 3b IPv4 settings	TCP/IP stack:	Default				
A Readute complete	vMotion:	Enabled				
4 Ready to complete	Provisioning:	Disabled				
	Fault Tolerance logging:	Disabled				
	Management:	Disabled				
	vSphere Replication:	Disabled				
	vSphere Replication NFC:	Disabled				
	vSAN:	Disabled				
	IPv4 settings					
	IPv4 address:	192.168.130.72 (static)				
	Subnet mask:	255.255.255.0				
			Back	Next	Finish	Cancel

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

11. Select the newly created vMotion VMkernel adapter.

Navigator I	🔒 10.2.164.71 🛛 🛃 🕞	6	🔥 🚳 Actio	ons 👻		≡*.
	Summary Monitor Configure	Per	missions V	Ms Datastores Networ	ks Update Manager	
Image: Constraint of the second s	++ > Storage		VMkemel adapters			
✓ III Production II.2.164.68	Virtual switches		Device	Network Label	Switch	IP Address 192.168.101.3
₩ 10.2.164.69 ₩ 10.2.164.70	VMkernel adapters Physical adapters		vmk2	VMKernel-iSCSI-B IB-Mgmt	vSwitch1	192.168.102.22 10.2.164.71
10.2.104.71	TCP/IP configuration Advanced	::	💓 vmk3	A vMotion	infra-DSwitch	192.168.130.72

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

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

🐖 vmk3 - Edit Settings		?
Port properties NIC settings IPv4 settings IPv6 settings Analyze impact	MTU: 9000	
		OK Cancel

14. Click OK to save the changes.

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

Appendix

Sample Switch Configuration

switchname AA12-9336C-A
vdc AA12-9336C-A id 1
limit-resource vlan minimum 16 maximum 4094
limit-resource vrf minimum 2 maximum 4096
limit-resource port-channel minimum 0 maximum 511
limit-resource u4route-mem minimum 248 maximum 248
limit-resource u6route-mem minimum 96 maximum 96
limit-resource m4route-mem minimum 58 maximum 58
limit-resource m6route-mem minimum 8 maximum 8

cfs eth distribute

feature interface-vlan
feature lacp
feature vpc
feature lldp

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

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

197

```
vlan 15
  name pure-oob
vlan 215
  name Management
vlan 1130
  name vMotion
vlan 1301
  name VM-Apps-1
vlan 1302
  name VM-Apps-2
vlan 1303
  name VM-Apps-3
vrf context management
  ip route 0.0.0/0 10.2.164.254
vpc domain 10
  peer-keepalive destination 10.2.164.91
```

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

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

interface port-channel129

```
Appendix
```

switchport mode trunk switchport trunk allowed vlan 215, 1130,1301-1303 spanning-tree port type edge trunk mtu 9216 vpc 129 interface port-channel130 switchport mode trunk switchport trunk allowed vlan 215,1130,1301-1303 spanning-tree port type edge trunk mtu 9216 vpc 130 interface Ethernet1/1 interface Ethernet1/2 interface Ethernet1/3 interface Ethernet1/4 interface Ethernet1/5 interface Ethernet1/6 interface Ethernet1/7 interface Ethernet1/8 interface Ethernet1/9 interface Ethernet1/10

interface Ethernet1/11 interface Ethernet1/12 interface Ethernet1/13 interface Ethernet1/14 interface Ethernet1/15 interface Ethernet1/16 interface Ethernet1/17 interface Ethernet1/18 interface Ethernet1/19 interface Ethernet1/20 interface Ethernet1/21 interface Ethernet1/22 interface Ethernet1/23 interface Ethernet1/24 interface Ethernet1/25

interface Ethernet1/26

```
interface Ethernet1/27
interface Ethernet1/28
interface Ethernet1/29
 description FSV-UCS-FI-A
  switchport mode trunk
  switchport trunk allowed vlan 215,1130,1301-1303
 spanning-tree port type edge trunk
 mtu 9216
 channel-group 129 mode active
interface Ethernet1/30
 description FSV-UCS-FI-B
 switchport mode trunk
 switchport trunk allowed vlan 215,1130,1301-1303
 mtu 9216
 channel-group 130 mode active
interface Ethernet1/31
interface Ethernet1/32
interface Ethernet1/33
  switchport mode trunk
 channel-group 133 mode active
interface Ethernet1/34
 switchport mode trunk
  channel-group 133 mode active
```

interface Ethernet1/35 interface Ethernet1/36 switchport mode trunk switchport trunk allowed vlan 15,115,215,1130,1301-1303 mtu 9216 channel-group 136 mode active interface mgmt0 vrf member management ip address 10.2.164.90/24 line console line vty no system default switchport shutdown

About the Authors

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

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

Acknowledgements

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

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