# •1|1•1|1• CISCO.



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

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

Last Updated: February 27, 2017



# About Cisco Validated Designs

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit:

#### http://www.cisco.com/go/designzone

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

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

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

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

© 2017 Cisco Systems, Inc. All rights reserved.

# Table of Contents

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

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

Create WWNN Pools	
Create WWPN Pools	86
Create vHBA Templates for Fabric A and Fabric B	
Create the Storage Connection Policy Fabric-A	
Create the Storage Connection Policy Fabric-B	
Create a SAN Connectivity Policy	
Create Boot Policies	
Configure UCS LAN Connectivity	
Configure Uplink Port Channels to Cisco Nexus Switches	
Create MAC Address Pools	
Create VLANs	
Set Jumbo Frames in Cisco UCS Fabric	
Create Network Control Policy for Cisco Discovery Protocol	
Create vNIC Templates	
Create LAN Connectivity Policy	
Create Service Profile Template	
Create Service Profiles	
Storage LUN Mapping	
Adding Hosts and Mapping Volumes on the IBM Storwize V5000	
VMware vSphere Installation and Setup	
VersaStack VMware ESXi 6.0 Update 2 SAN Boot Installation	
Log in to Cisco UCS 6324 Fabric Interconnect	
VMware ESXi Installation	
Install ESXi on the Servers	
Set Up Management Networking for ESXi Hosts	
Log in to VMware ESXi Hosts Using VMware vSphere Client	
Install VMware Drivers for the Cisco Virtual Interface Card (VIC)	
Map Required VMFS Datastores	
Configure NTP on ESXi Hosts	
Move VM Swap File Location	
VersaStack VMware vCenter 6.0U2	
Install the Client Integration Plug-In	
Building the VMware vCenter Server Appliance	
Set Up vCenter Server	
Set Up vCenter Server with a Datacenter, Cluster, DRS and HA	

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



# **Executive Summary**

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

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

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

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

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

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

# VersaStack for Data Center Overview

# Introduction

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

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

# Audience

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

# Purpose of this document

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

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

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

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

# Solution Design and Architecture

# Architecture

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

http://www.cisco.com/en/US/products/ps10477/prod\_technical\_reference\_list.html

and IBM Interoperability Matrix:

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

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

### Physical Topology

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

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

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





The reference architecture covered in this document leverages the following:

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

This document guides you through the low-level steps for deploying the base architecture. These procedures cover everything from physical cabling to network, compute, and storage device configurations.

# Software Revisions

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

IBM:

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

Cisco:

http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html

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

#### Table 1 Software Revisions

# Configuration Guidelines

This document provides the details for configuring a fully redundant, highly available infrastructure. Therefore, reference is made to which component is being configured with each step, either 01 or 02 or A and B. For example, the Cisco UCS Fabric Interconnects are identified as FI-A or FI-B. This document is intended to enable you to fully configure the customer environment and during this process, various steps require you to insert customer-specific naming conventions, IP addresses, and VLAN schemes, as well as to record appropriate MAC addresses.

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

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

### Table 2 Necessary VLANs

### Table 3 Necessary VSANs

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

## Cisco UCS Central

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

#### Virtual Machines

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

#### Table 4 Machine List

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

# **Configuration Variables**

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

### Table 5 Customer Variables

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

Variable	Description	Customer Implementation Value
< <var_country_code>&gt;</var_country_code>	Two-letter country code	
< <var_state>&gt;</var_state>	State or province name	
< <var_city>&gt;</var_city>	City name	
< <var_org>&gt;</var_org>	Organization or company name	
< <var_unit>&gt;</var_unit>	Organizational unit name	
< <var_street_address>&gt;,</var_street_address>	Street address for support information	
< <var_contact_name>&gt;</var_contact_name>	Name of contact for support	
< <var_admin>&gt;</var_admin>	Secondary Admin account for storage login	
< <var_nexus_a_hostname>&gt;</var_nexus_a_hostname>	Cisco Nexus A host name	
< <var_nexus_a_mgmt0_ip>&gt;</var_nexus_a_mgmt0_ip>	Out-of-band Cisco Nexus A management IP address	
< <var_nexus_a_mgmt0_netmask>&gt;</var_nexus_a_mgmt0_netmask>	Out-of-band management net- work netmask	
< <var_nexus_a_mgmt0_gw>&gt;</var_nexus_a_mgmt0_gw>	Out-of-band management net- work default gateway	
< <var_nexus_b_hostname>&gt;</var_nexus_b_hostname>	Cisco Nexus B host name	
< <var_nexus_b_mgmt0_ip>&gt;</var_nexus_b_mgmt0_ip>	Out-of-band Cisco Nexus B management IP address	
< <var_nexus_b_mgmt0_netmask>&gt;</var_nexus_b_mgmt0_netmask>	Out-of-band management net- work netmask	
< <var_nexus_b_mgmt0_gw>&gt;</var_nexus_b_mgmt0_gw>	Out-of-band management net- work default gateway	
< <var_ib-mgmt_vlan_id>&gt;</var_ib-mgmt_vlan_id>	In-band management network VLAN ID	
< <var_native_vlan_id>&gt;</var_native_vlan_id>	Native VLAN ID	
< <var_vmotion_vlan_id>&gt;</var_vmotion_vlan_id>	VMware vMotion® VLAN ID	
< <var_vm-traffic_vlan_id>&gt;</var_vm-traffic_vlan_id>	VM traffic VLAN ID	
< <var_nexus_vpc_domain_id>&gt;</var_nexus_vpc_domain_id>	Unique Cisco Nexus switch VPC domain ID	
< <var_ucs_clustername>&gt;</var_ucs_clustername>	Cisco UCS Manager cluster host name	
< <var_ucsa_mgmt_ip>&gt;</var_ucsa_mgmt_ip>	Cisco UCS Fabric Intercon- nect (FI) A out-of-band management IP address	
< <var_ucs_mgmt_mask>&gt;</var_ucs_mgmt_mask>	Out-of-band management net- work netmask	
< <var_ucs_mgmt_gateway>&gt;</var_ucs_mgmt_gateway>	Out-of-band management net- work default gateway	

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

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

Source	Switch/ Port	Variable	WWPN
FC_NodeA-fabricA	Switch A FC3	< <var_wwpn_fc_nodea-fabrica>&gt;</var_wwpn_fc_nodea-fabrica>	
FC_NodeA-fabricB	Switch B FC3	< <var_wwpn_fc_nodea-fabricb>&gt;</var_wwpn_fc_nodea-fabricb>	

#### Table 6 WWPN Variables

Source	Switch/ Port	Variable	WWPN
FC_NodeB-fabricA	Switch A FC4	< <var_wwpn_fc_nodeb- fabricA&gt;&gt;</var_wwpn_fc_nodeb- 	
FC_NodeB-fabricB	Switch B FC4	< <var_wwpn_fc_nodeb- fabricB&gt;&gt;</var_wwpn_fc_nodeb- 	
VM-Host-infra-01-A	Switch A	< <var_wwpn_vm-host-infra-01- A&gt;&gt;</var_wwpn_vm-host-infra-01- 	
VM-Host-infra-01-B	Switch B	< <var_wwpn_vm-host-infra-01- B&gt;&gt;</var_wwpn_vm-host-infra-01- 	
VM-Host-infra-02-A	Switch A	< <var_wwpn_vm-host-infra-02- A&gt;&gt;</var_wwpn_vm-host-infra-02- 	
VM-Host-infra-02-B	Switch B	< <var_wwpn_vm-host-infra-02- B&gt;&gt;</var_wwpn_vm-host-infra-02- 	

# VersaStack Cabling

Figure 2 illustrates the VersaStack build process



# VersaStack Cabling

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

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

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

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

It is possible to order IBM Storwize V5030 systems in a different configuration from what is presented in the tables in this section. Before starting, be sure that the configuration matches the descriptions in the tables and diagrams in this section.

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

http://www.ibm.com/support/knowledgecenter/STHGUJ\_7.4.0/com.ibm.storwize.v5000.740.doc/v350 0\_qisascables\_b4jtyu.html?cp=STHGUJ&lang=en



### Figure 3 VersaStack Cabling Diagram

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

#### Table 7 Cisco Nexus 9000-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 9000-A	Eth1/3	10GbE	Cisco UCS fabric interconnect-A	Eth1/3

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

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

### Table 8 Cisco Nexus 9000-B Cabling Information

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

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

### Table 9 IBM Storwize V5030 Controller Node-A Cabling Information

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

Table 10 IBM Storwize V5030 Controller Node-B Cabling Information

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

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

# Table 11 Cisco UCS Fabric Interconnect A Cabling Information

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

### Table 12 Cisco UCS Fabric Interconnect B Cabling Information

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

# Network Configuration

### Cisco Nexus 9000 Initial Configuration Setup

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



#### Cisco Nexus A

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

On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning. Abort Auto Provisioning and continue with normal setup ?(yes/no)[n]: y ---- System Admin Account Setup ----Do you want to enforce secure password standard (yes/no) [y]: Enter the password for "admin": Confirm the password for "admin": ---- Basic System Configuration Dialog VDC: 1 ----This setup utility will quide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system. Please register Cisco Nexus9000 Family devices promptly with your supplier. Failure to register may affect response times for initial service calls. Nexus9000 devices must be registered to receive entitled support services. Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip the remaining dialogs. Would you like to enter the basic configuration dialog (yes/no): y Create another login account (yes/no) [n]: n Configure read-only SNMP community string (yes/no) [n]: Configure read-write SNMP community string (yes/no) [n]: Enter the switch name : <<var nexus A hostname>>

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Mgmt0 IPv4 address : <<var\_nexus\_A\_mgmt0\_ip>> Mgmt0 IPv4 netmask : <<var nexus A mgmt0 netmask>> Configure the default gateway? (yes/no) [y]: IPv4 address of the default gateway : <<var nexus A mgmt0 gw>> Configure advanced IP options? (yes/no) [n]: Enable the telnet service? (yes/no) [n]: Enable the ssh service? (yes/no) [y]: Type of ssh key you would like to generate (dsa/rsa) [rsa]: Number of rsa key bits <1024-2048> [1024]: 2048 Configure the ntp server? (yes/no) [n]: y NTP server IPv4 address : <<var global ntp server ip>> Configure default interface layer (L3/L2) [L2]: Configure default switchport interface state (shut/noshut) [noshut]: Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]: The following configuration will be applied: password strength-check switchname <<var nexus A hostname>> vrf context management ip route 0.0.0.0/0 <<var nexus A mgmt0 gw>> exit no feature telnet ssh key rsa 2048 force feature ssh ntp server <<var global ntp server ip>> system default switchport no system default switchport shutdown copp profile strict interface mgmt0 ip address <<var nexus A mgmt0 ip>><var nexus A mgmt0 netmask>> no shutdown Would you like to edit the configuration? (yes/no) [n]: Use this configuration and save it? (yes/no) [y]:

#### Cisco Nexus B

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

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

Abort Auto Provisioning and continue with normal setup ?(yes/no)[n]: y ---- System Admin Account Setup ----Do you want to enforce secure password standard (yes/no) [y]: Enter the password for "admin": Confirm the password for "admin": ---- Basic System Configuration Dialog VDC: 1 --- This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system. Please register Cisco Nexus9000 Family devices promptly with your supplier. Failure to register may affect response times for initial service calls. Nexus9000 devices must be registered to receive entitled support services. Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip the remaining dialogs. Would you like to enter the basic configuration dialog (yes/no): y Create another login account (yes/no) [n]: n Configure read-only SNMP community string (yes/no) [n]: Configure read-write SNMP community string (yes/no) [n]: Enter the switch name : <<var nexus B hostname>> Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Mgmt0 IPv4 address : <<var nexus B mgmt0 ip>> Mgmt0 IPv4 netmask : <<var nexus B mgmt0 netmask>> Configure the default gateway? (yes/no) [y]: IPv4 address of the default gateway : <<var nexus B mgmt0 gw>> Configure advanced IP options? (yes/no) [n]: Enable the telnet service? (yes/no) [n]: Enable the ssh service? (yes/no) [y]: Type of ssh key you would like to generate (dsa/rsa) [rsa]: Number of rsa key bits <1024-2048> [1024]: 2048

Configure the ntp server? (yes/no) [n]: y NTP server IPv4 address : <<var\_global\_ntp\_server\_ip>> Configure default interface layer (L3/L2) [L2]: Configure default switchport interface state (shut/noshut) [noshut]: Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]: The following configuration will be applied: password strength-check switchname <<var nexus B hostname>> vrf context management ip route 0.0.0.0/0 <<var nexus B mgmt0 gw>> exit no feature telnet ssh key rsa 2048 force feature ssh ntp server <<var global ntp server ip>> system default switchport no system default switchport shutdown copp profile strict interface mgmt0 ip address <<var nexus B mgmt0 ip>><<var nexus B mgmt0 netmask>> no shutdown Would you like to edit the configuration? (yes/no) [n]: Use this configuration and save it? (yes/no) [y]: 

# Enable Appropriate Cisco Nexus 9000 Features and Settings

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

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

- On each Nexus 9000, enter the configuration mode: config terminal
- 2. Use the following commands to enable the necessary features:

feature lacp

feature vpc feature interface-vlan

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

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

### Create VLANs for VersaStack IP Traffic

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

To create the necessary virtual local area networks (VLANs), complete the following step on both switches:

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

```
vlan <<var_ib-mgmt_vlan_id>>
name IB-MGMT-VLAN
vlan <<var_native_vlan_id>>
name Native-VLAN
vlan <<var_vmotion_vlan_id>>
name vMotion-VLAN
vlan <<var_vm_traffic_vlan_id>>
name VM-Traffic-VLAN
exit
copy run start
```

# Configure Virtual Port Channel Domain

#### Cisco Nexus 9000 A

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

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

vpc domain <<var nexus vpc domain id>>

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

role priority 10

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

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

4. Enable the following features for this vPC domain:

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

#### Cisco Nexus 9000 B

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

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

vpc domain <<var nexus vpc domain id>>

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

role priority 20

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

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

4. Enable the following features for this vPC domain:

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

### Configure Network Interfaces for the vPC Peer Links

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

#### Cisco Nexus 9000 A

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

```
interface Eth1/47
description VPC Peer <<var_nexus_B_hostname>>:1/47
interface Eth1/48
description VPC Peer <<var nexus B hostname>>:1/48
```

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

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

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

interface Pol0 description vPC peer-link

4. Make the port-channel a switchport, and configure a trunk to allow in-band management, VM traffic, vMotion and the native VLAN.

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>,
<<var_vmotion_vlan_id>>, <<var_vm_traffic_vlan_id>>,
```

5. Make this port-channel the VPC peer link and bring it up.

vpc peer-link
no shutdown
copy run start

#### Cisco Nexus 9000 B

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

```
interface Eth1/47
description VPC Peer <<var_nexus_A_hostname>>:1/47
interface Eth1/48
description VPC Peer <<var nexus A hostname>>:1/48
```

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

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

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

```
interface Pol0
description vPC peer-link
```

4. Make the port-channel a switchport, and configure a trunk to allow in-band management, VM traffic, vMotion and the native VLAN.

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>,
<<var_vmotion_vlan_id>>, <<var_vm_traffic_vlan_id>>,
```

5. Make this port-channel the VPC peer link and bring it up.

vpc peer-link
no shutdown
copy run start

# Configure Network Interfaces to Cisco UCS Fabric Interconnect

#### Cisco Nexus 9000 A

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

```
interface Pol3
```

```
description <<var ucs clustername>>-A
```

2. Make the port-channel a switchport, and configure a trunk to allow in-band management, VM traffic, vMotion and the native VLANs.

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>,
<<var_vmotion_vlan_id>>, <<var_vm_traffic_vlan_id>>,
```

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

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

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

mtu 9216

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

vpc 13

no shutdown

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

interface Eth1/3

```
description <<var ucs clustername>>-A:1/3
```

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

channel-group 13 force mode active no shutdown

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

interface Pol4

```
description <<var ucs clustername>>-B
```

 Make the port-channel a switchport, and configure a trunk to allow in-band management, VM traffic, vMotion and the native VLANs.

switchport
switchport mode trunk
switchport trunk native vlan <<var\_native\_vlan\_id>>
switchport trunk allowed vlan <<var\_ib-mgmt\_vlan\_id>>,
<<var vmotion vlan id>>, <<var vm traffic vlan id>>

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

spanning-tree port type edge trunk

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

mtu 9216

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

vpc 14

no shutdown

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

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

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

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

#### Cisco Nexus 9000 B

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

interface Pol4

description <<var ucs clustername>>-B

2. Make the port-channel a switchport, and configure a trunk to allow in-band management, VM traffic, vMotion and the native VLANs.

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>,
<<var_vmotion_vlan_id>>, <<var_vm_traffic_vlan_id>>
```

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

spanning-tree port type edge trunk

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

mtu 9216

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

vpc 14

no shutdown

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

interface Eth1/3

description <<var ucs clustername>>-B:1/3

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

channel-group 14 force mode active

no shutdown

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

interface Pol3

description <<var ucs clustername>>-A

9. Make the port-channel a switchport, and configure a trunk to allow in-band management, VM traffic, vMotion and the native VLANs.

```
switchport
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>,
<<var_vmotion_vlan_id>>, <<var_vm_traffic_vlan_id>>,
```

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

spanning-tree port type edge trunk

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

mtu 9216

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

vpc 13

no shutdown

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

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

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

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

# Management Plane Access for Servers and Virtual Machines

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

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

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

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

Cisco Nexus 9000 A int Eth1/36 description IB-management-access switchport mode access spanning-tree port type network switchport access vlan <<var ib-mgmt vlan id>> no shut feature interface-vlan int Vlan <<var ib-mgmt vlan id>> ip address <<var switch A inband mgmt ip address>>/<<var inband mgmt netmask>> no shut ip route 0.0.0.0/0 <<var inband mgmt gateway>> copy run start Cisco Nexus 9000 B int Eth1/36 description IB-management-access switchport mode access spanning-tree port type network switchport access vlan <<var ib-mgmt vlan id>> no shut feature interface-vlan int Vlan <<var ib-mgmt vlan id>> ip address <<var switch B inband mgmt ip address>>/<<var inband mgmt netmask>> no shut

ip route 0.0.0.0/0 <<var\_inband\_mgmt\_gateway>>
copy run start

Cisco Nexus 9000 A and B using Port Channel Example 2

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

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

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

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

```
switchport
switchport mode access
switchport access vlan <<var ib-mgmt vlan id>>
```

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

spanning-tree port type normal

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

```
vpc 9
```

no shutdown

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

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

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

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

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

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

# Storage Configuration

# IBM Storwize V5030

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

### Prerequisites

Begin this procedure only after the physical installation of the IBM Storwize V5000 has been completed. The computer used to initialize the IBM Storwize V5000 must have an Ethernet cable connecting the personal computer to the technician to the IBM Storwize V5000 as well as a supported browser installed. At the time of writing, the following browsers or later are supported with the management GUI; Firefox 32, Internet Explorer 10 and Google Chrome 37. Browser access to all system and service IPs is automatically configured to connect securely using HTTPS and SSL. Attempts to connect through HTTP will get redirected to HTTPS.

The system generates its own self-signed SSL certificate. On the first connection to the system, your browser may present a security exception because it does not trust the signer; you should allow the connection to proceed.

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

# IBM Storwize V5000 Initial Configuration

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

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

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

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



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



6. Connect an Ethernet cable between the port of the computer that is configured in step 3 and the technician port. After the connection is made, the system will automatically configure the IP and DNS settings for the personal computer if DHCP is available. If it is not available, the system will use the values you provided.
7. After the Ethernet port of the personal computer is connected, open a supported browser and browse to address http://install. (If you do not have DCHP, open a supported browser and go to the following static IP address 192.168.0.1). The browser is automatically directed to the initialization tool.

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



8. Click Next on the System Initialization welcome message.



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

IPv4	IPv6	
IP address:		
Subnet mask:		
Gateway:		

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



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

System Initialization	
Restarting Web Server	
*Rebooting:	9:49
■ Back Next ►	

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



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

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

## IBM Storwize V5000 GUI Setup

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

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

To setup IBM Storwize V5000, complete the following steps:

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



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

Story	wize <sup>®</sup> V5000
Storage N	Management (VersaStack)
User name:	superuser g
Password:	
	Log in 🕞
Licensed Material - Proper trademarks of the IBM Co	rty of IBM Corp. © IBM Corporation and other(s) 2016. IBM and Storwize are registered orporation in the United States, other countries, or both.

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

~	• @\/=	~~~		
Story	vize <sup>®</sup> V5	000		
Storage M	anagement (\	/ersaStack)		
New Password:				
Confirm				
Password:				
		Log in 🔁		
				2
Licensed Material - Property trademarks of the IBM Com	of IBM Corp. © IBM Corporation a	and other(s) 2016. IBM and Stor	wize are registered	IBM

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

System Setup		>
Welcome	Welcome	
System Name	Congratulations! You now have unmatched performance, availability, advanced functions and highly-scalable capacity right at your fingertips.	
Licensed Functions	→ Prerequisites	
Date and Time	Ensure that all hardware is cabled correctly and powered on     Obtain any optional licenses	
Encryption	Obtain email server IP address and port for call home	
Call Home		
Summary		
	Cancel	

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

System Setup	
⊘ Welcome	System Name
System Name	Enter a name for the system:
Licensed Functions	VersaStack-V5030
Date and Time	
Encryption	
Call Home	
Summary	
	Back Apply and Next      Cancel

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

System Setup		
System Setup  Welcome  System Name  Licensed Functions  Date and Time  Encryption  Call Home  Summany	Licensed Functions Additional licenses are required license agreement for proof of co FlashCopy: Remote Mirroring: Easy Tier: External Virtualization:	to use certain system functions. For auditing purposes, retain the ompliance. 1 Number of enclosures 0 Number of enclosures 1 Number of enclosures 0 Number of enclosures 0 Number of enclosures
Call Home Summary	External Virtualization:	0 Number of enclosures
Need Help	- Back	Apply and Next ►

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

System Setup		x
Welcome     System Name     Licensed Functions	Date and Time Select time and date settings. You can enter these settings manually Network Time Protocol (NTP) server to synchronize time on the syst	y or specify a tem.
<ul> <li>Date and Time</li> </ul>	Manually     Image: Server	
Encryption	IP address: (*	
Call Home	Time Zone: (GMT) Dublin, Edinburgh, London, Lisbon	*
Summary		
	Back Apply and Next ►	Cancel

8. Configure the date and time settings, inputting NTP server details <<var\_global\_ntp\_server\_ip>> if you have one. Click Apply and Next to proceed.

System Setup	x
⊘ Welcome	Encryption
System Name	Was the encryption feature purchased for this system?
⊘ Licensed Functions	No     Yos
⊘ Date and Time	0 103
<ul> <li>Encryption</li> </ul>	
Call Home	
Summary	
Need Help	■ Back Next ► Cancel

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

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

System Setup		2
<ul> <li>Welcome</li> <li>System Name</li> <li>Licensed Functions</li> <li>Date and Time</li> </ul>	System Location Service parts should be Company name:	BM UK
Encryption	System address:	Hursley Park
<ul> <li>Call Home</li> <li>System Location</li> </ul>	City:	Winchester
Contact Email Servers	State or province:	XX
Summary	Postal code:	SO21 2JN
	Country or region:	United Kingdom
	Comment:	Hursley Labs
		Back Next      Cancel

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

System Setup			×
<ul> <li>⊘ Welcome</li> <li>⊘ System Name</li> <li>⊘ Licensed Functions</li> </ul>	Contact The support center con	tacts this person to resolve issues on the syst	em.
⊘ Date and Time	Name:	(IBM	
S Encryption	Email:	ibm@ibm.com	
<ul> <li>Call Home</li> <li>System Location</li> <li>Contact Email Servers</li> <li>Summary</li> </ul>	Phone (primary): Phone (alternate):	0898 50 50 50	
	<b>■</b> B	ack Apply and Next ►	Cancel

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

System Setup			х
Welcome     System Name     Licensed Functions	Email Servers Call home and event notificatio	ns are routed through this email server. Port:	
Oate and Time	9.71.45.71	✓ 25 O	
Sencryption	Ping		
<ul> <li>Call Home</li> <li>System Location</li> <li>Contact</li> <li>Email Servers</li> </ul>			
Summary			
	Set up call home later		
Need Help	Back	Apply and Next ►	Cancel

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

system Setup				
Welcome	Summary			
System Name	System Information 2078-324:	781000T	✓ Online	
Licensed Functions	System name: Code level: NTP server:	VersaStack-V5 7.7.1.2 9.71.44.170	Date: Time: Time zone:	Dec 6, 2016 5:31:07 PM (GMT) Dublin, Edinburgh, London
Date and Time				(emi) sasing samasign sensen in
Encryption	Licensed Functions FlashCopy: Remote Mirroring:	100 enclo 100 enclo	sures sures	
Call Home	Easy Tier: External Virtualization: Compression:	100 enclo: 100 extern 100 enclo:	sures nal enclosures sures	
Summary	Call Home			
	System Location Company name: Street address: City: State or province: Postal code: Country or region: Comment:	IBM UK Hursley Park Winchester XX SO21 2JN United Kingdom Hursley Labs		
	Contact Contact name: Email address: Telephone (primary): Telephone (alternate):	IBM ibm@ibm.com 0898 50 50 50		
	Email Servers Server IP 9.71.45.71	Port 25		
	il			
		A Back	Finish	Cance

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

Setup Comple	ted	×
(j)	System setup is complete. You will be redirected to the management GUI.	
	Close	

14. Setup Complete. Click Close.



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



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



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

Network	Management IP Addresses
Management IP Addresses	The management IP address is assigned during the initialization of the system and represents a set of enclosures on the system that contains the management GUI and the command-line interface which manage the system. Click on a port to configure the system's management IP address. If you change management IP addresses, use the new IP address to log in to the management GUI again.
Service IPs	A system uses the same management IP addresses for all control enclosures.
Ethernet Ports	
Ethernet P	ort 1 (Primary)
IP Address 1	92.168.162.206
F Subnet Mask 2	55.255.252.0
Gateway 1	92.168.160.1
Show IPv6	OK

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

Network	Service IPs
Management IP Addresses	The service IP address provides access to the service interfaces on each individual node canister. Select the canister and click port 1 to configure a service IP address for the canister. The service IP address can be unconfigured by clearing the IPv4 or IPv6 fields or by setting the IPv4 address to 0.0.0 or the IPv6 address to 0::0.
Service IPs 1	Node Canister: left 2 ldentify
Ethernet Ports	
iSCSI Servi	ce IP (Port 1)
Fibi Cor IP Address	192.168.162.207
Fibi Subnet Mask Gateway	255.255.252.0
Show IPvô	OK Cancel

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



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



22. Select Create User.

	Name		
$\bigcirc$	admin		
- Authentic	ation Mode —		
O Local	Remot	e	
User Group	D		
Security	Admin	-	
— Local Cre	dentials		
Users must	have a passwoi	rd, an SSH public kev, or both.	
Password		Verify password	
		•••••	
Choose fi	c Key le No file cho	sen	
01100000 11		5011	

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

☆ VersaStack-V5030 > Access > Users		IBM Storwize V5000	superuser (Security Ad	ministrator)
User Groups All Users	Create User Gro	All Users	Log Out Modify Password Manage SSH Public Key	
SecurityAdmin	treate User ≣	Actions C Filter	Showing 1 user	Selecting 0 users
Administrator	Name	<ul> <li>User Group</li> </ul>	Password SSH Key	U.
	superuser	SecurityAdmin	Configured Yes	
CopyOperator				

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



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

Create Pool		
Ente	r a name:	
Bro	nze	

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

+ Create Poo	ol I≣ Actions					
Name		State	Capacity	RAID		1
÷	Bronze	No Storage			$\longrightarrow$	Add Storage

27. Select 'Add Storage'.

Assign Storage to Pool Bronze	х
Quick Advanced -	
Drive Assignment: Drives: Size: 558.41 GiB Enterprise 10K:	
Pool Bronze capacity: 3.24 TiB	
Assign Cancel	

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



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



30. Click Create Volumes.

Create Volumes X
Quick Volume Creation Advanced
Pool: Bronze   Quantity: Capacity:   Capacity savings: Name:   2 40   GIB Thin-provisioned   VM-Host-Infra-0 1 - 2   I/O group: Automatic Volume range: VM-Host-Infra-01-VM-Host-Infra-02 2 volumes Volume range: VM-Host-Infra-01-VM-Host-Infra-02 2 volumes in pool Bronze Caching I/O group: Automatic Caching I/O group: Automatic Total rand capacity: 1.60 GiB Total virtual capacity: 8.0.00 GiB
Create Create and Map to Host Cancel

31. Select a pre-set that you want for the ESXi boot volume. Select the storage pool you've just created, and select I/O group Automatic. Input quantity 2, capacity 40GB, desired capacity savings and name VM-Host-Infra-0. Additionally, change the starting ID to1. Click Create and then click Close.

Create Volumes	х
Quick Volume Creation Advance	n
Pool:       Bronze         Quantity:       Capacity:       Capacity savings:       Name:         1       500       GIB       Thin-provisioned       Infra_datastore_1         1       500       GIB       Thin-provisioned       Infra_datastore_1         1/0 group:       Automatic       Infra_datastore_1       Image:         1       volume name:       Infra_datastore_1       Image:       Image:         1       volume in pool Bronze       Caching I/O group:       Automatic         Caching I/O group:       Automatic       Image:       Image:         Total real capacity:       10.00 GIB       Image:       Image:	
Create and Map to Host Cancel	

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

Create Volumes		×
Basic	Quick Volume Creation Advanced	
Pool: Quantity: 1	Bronze   Total 3.24 TiB     Capacity:   Capacity savings:   Name:   100   GiB   Thin-provisioned   Infra_swap     Automatic   Summary 1 volume	
	Volume name: infra_swap 1 volume in pool Bronze Caching I/O group: Automatic Accessible I/O group: Automatic Total real capacity: 2.00 GIB Total virtual capacity: 100.00 GIB	
0	Create Create and Map to Host Cancel	

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

Name	State	Capacity	Pool	Host Mappings	UID
VM-Host-Infra-01	V Online	😨 40.00 GiB	mdiskgrp0	No	6005076300818A3F78000000000000000
VM-Host-Infra-02	V Online	() 40.00 GiB	mdiskgrp0	No	6005076300818A3F7800000000000001
infra_datastore_1	V Online	300.00 GiB	mdiekgrp0	No	6005076300818A3F780000000000002
infra_swap	V Online	100.00 GiB	mdiskgrp0	No	6005076300818A3F7800000000000003

34. Validate the volumes created.



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

Network	Fibre	Channe	el Ports			
Management IP Addresses	Each po commu	nt is confi nicate. Ea	gured identically across all no ch port is allowed to commun	des in the system. The c icate with hosts and stor	onnection determines with w age systems.	hich systems the port is allowed to
	i≣ Acti	ons 🔍	Filter		💡 You can change the	WWPN notation from the actions men
Service IPs	ID		System Connection	Owning Node	WWPN	Host IO Permitted
0	Θ	1	Any			
Ethernet Ports		1	Any	2(Right)	500507680D7458F1	No
		1	Any	2(Right)	500507680D0458F1	Yes
		1	Any	3(Left)	500507680D7458F0	No
I SCSI		1	Any	3(Left)	500507680D0458F0	Yes
	Θ	2	Any			
Fibre Channel		2	Any	2(Right)	500507680D0858F1	Yes
Connectivity	_	2	Any	2(Right)	500507680D7858F1	No
		2	Any	3(Left)	500507680D7858F0	No
Fibre Channel Ports		2	Any	3(Left)	500507680D0858F0	Yes
	•	3	Any			
	۲	4	Any			

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

#### Table 13 IBM V5030 - WWPN Information

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

# Cisco UCS Compute Configuration

## VersaStack Cisco UCS Initial Setup

This section provides detailed procedures for configuring the Cisco Unified Computing System (Cisco UCS) for use in a VersaStack environment. The steps are necessary to provision the Cisco UCS C-Series and B-Series servers and should be followed precisely to avoid improper configuration.

#### Cisco UCS Fabric Interconnect 6324 A

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

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

Enter the configuration method: console Enter the setup mode; setup newly or restore from backup. (setup/restore)? Setup You have chosen to setup a new fabric interconnect? Continue? (y/n): y Enforce strong passwords? (y/n) [y]: y Enter the password for "admin": <<var password>> Enter the same password for "admin": <<var password>> Is this fabric interconnect part of a cluster (select 'no' for standalone)? (yes/no) [n]: y Which switch fabric (A|B): A Enter the system name: <<var ucs clustername>> Physical switch Mgmt0 IPv4 address: <<var ucsa mgmt ip>> Physical switch Mgmt0 IPv4 netmask: <<var ucsa mgmt mask>> IPv4 address of the default gateway: <<var ucsa mgmt gateway>> Cluster IPv4 address: <<var\_ucs\_cluster\_ip>> Configure DNS Server IPv4 address? (yes/no) [no]: y DNS IPv4 address: <<var nameserver ip>> Configure the default domain name? y Default domain name: <<var dns domain name>> Join centralized management environment (UCS Central)? (yes/no) [n]: Enter

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

#### Cisco UCS Fabric Interconnect 6324 B

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

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

Enter the configuration method: console

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

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

Physical switch Mgmt0 IPv4 address: <<var ucsb mgmt ip>>

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

## VersaStack Cisco UCS Base Setup

#### Log in to Cisco UCS Manager

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

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

## Anonymous Reporting

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

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

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

Don't show this message again.

ОК	) (	Cancel	

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

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

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

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

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

- 1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
- 2. Select Pools > root > IP Pools > IP Pool ext-mgmt.
- 3. In the Actions pane, select Create Block of IPv4 Addresses.
- 4. Enter the starting IP address of the block and the number of IP addresses required, and the subnet and gateway information. <<var\_In-band\_mgmtblock\_net>>.
- 5. Click OK to create the IP block.
- 6. Click OK in the confirmation message.

	All	LAN / Pools / root / IP Pools / IP Pool ext-mgmt	
Equipment	<ul> <li>Network Control Policies</li> </ul>	General IP Addresses IP Blocks Faults	Events
	<ul> <li>QoS Policies</li> </ul>		
	<ul> <li>Threshold Policies</li> </ul>	Actions	Properties
Servers	VMQ Connection Policies		Name : ext-mgmt
品	usNIC Connection Policies	Create Block of IPv4 Addresses	Description :
	vNIC Templates	Create Block of IPv6 Addresses	GUID : 0000000-0000-0000-00000000000000
	Sub-Organizations	Create DNS Suffix	Size : 15 Assigned : 13
	▼ Pools	Create IPV4 WINS Server	Assignment Order :
SAN	* root	Show Pool Usage	
	▼ IP Pools		
VM	IP Pool ext-mgmt		

Synchronize Cisco UCS to NTP

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

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

	All	All / Time Zone Management / Timezone	
Equipment	LAN Cloud	General Events	
	<ul> <li>SAN Cloud</li> <li>root</li> </ul>	Actions	Properties
Servers	<ul> <li>Time Zone Management</li> </ul>	Add NTP Server	Time Zone : [za/New_York (Eastern Time) v]
古古 LAN	Timezone		v, Advanced Filter ↑ Export
	<ul> <li>Capability Catalog</li> <li>Adapters</li> </ul>		Name
SAN	Blade Servers		No data available
	CPUs		
VM	Crypto Cards		
	Fan Modules		
Storage	GPU Cards		🕀 Add 📄 Delete 🕕 Info
	IO Modules		
Chassis	Local Disks Memory Units		
20	PSUs		
Admin	Rack-Mount Servers		

## Configure UCS Servers

#### Edit Chassis Discovery Policy

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

- 1. In Cisco UCS Manager, click the Equipment tab in the navigation pane and select Equipment in the list on the left under the pulldown.
- 2. In the right pane, click the Policies tab.
- 3. Under Global Policies, set the Chassis/FEX Discovery Policy to match the number of uplink ports that are cabled between the Primary chassis to the Secondary Chassis.
- 4. Set the Rack Server Discovery Policy to Immediate.

quipment					
Main Topology View Fabric Interconnects	s Servers Thermal	Decommissioned	Firmware Management	Policies	Faults
Global Policies Autoconfig Policies	Server Inheritance Policies	Server Discovery Polic	es SEL Policy Po	ower Groups	
Chassis/FEX Discovery Policy					
Action : 2 Link	Ψ.				
Link Grouping Preference : ONONE	Port Channel				
Multicast Hardware Hash : Oisabled	CEnabled				
Rack Server Discovery Policy					
Action : Immediate User Ackno	owledged				
Scrub Policy : <pre> </pre> <pre> </pre>					
Rack Management Connection Policy					
Action : Auto Acknowledged User Ac	cknowledged				
Power Policy					
Redundancy : Non Redundant  N+1	Grid				
MAC Address Table Aging					
					Save Changes Reset Values

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

### Extending Cisco UCS Mini

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

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



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

#### Acknowledge Cisco UCS Chassis

To acknowledge all Cisco UCS chassis, complete the following steps:

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

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

	All	•	Equipme	nt / Chassis
Equipment	<ul> <li>Equipment</li> </ul>	1	< 1 5	Slots Instal
	<ul> <li>Chassis</li> </ul>		Filters	
U	Chassis 1	(oriman/)	_	
Servers	🔻 Chassis :	Remove Chassis		w All
品	► Fans	Decommission Chassis		Critical
LAN	IO Mod	Turn off Locator LED		Major
	► PSUs	Start Fault Suppression		Minor
	<ul> <li>Server</li> </ul>	Stop Fault Suppression		Warning
SAN	۶ ۲	Create Zoning Policy from In	iventory	Info
	▶ 5	Сору		Condition
	▶ 5	Copy XML		Cleared
		Delete		Soaking
				Suppressed
Storage	5			
	Rack-Mount	s		
Chassis	Servers			

### Enable Uplink Ports

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

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



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

#### Create UUID Suffix Pool

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

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

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

		Create UUID Suffix Pool	? ×
1	Define Name and Description	+ - 🏹 Advanced Filter 🔶 Export 🚔 Print	₽
2	Add UUID Blocks	Name From To	
		<b>[0000-0000000</b> 0000-00000000001 0000-00000	0000040
	Create a Blo	ck of UUID Suffixes ? ×	
	From : 0000-0000	00000001 Size : 64	
		OK Cancel	
		🕀 Add 🔟 Delete	
		< Prev Next > Finish Ca	incel

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

#### Create Server Pool

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

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

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

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

		Create S	erver	Poo	I												? >
1	Set Name and Description		s	ervers									Pool	ed Serve	ers		
	Add Convers						₽										¢
2	Add Servers	Chassis •	·			 					SI.	. R.	. U	. PID	A	S	C
		2	1			 					1 2			U	U	FL	28
		2	2			 		>>			1 1			U	U	FL	28
		2	3			 		<<									
		2	4			 											
		2	5			 											
		2	6			 											
		1	3			 	8										
		1	5			 											
		1	6			 											
		1	7			 											
		Model: Serial Number Vendor:	r:							Mod Seria Veno	el: al Nun dor:	ber:					
									< Pre	v				Finish		Can	cel

#### Create Host Firmware Package

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

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

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

Create Host Firmware Package	? ×
Name : VM-Host-Infra	
Description :	
How would you like to configure the Host Firmware Package?	
Simple	
Blade Package : 3.1(2c)B	
Rack Package : 3.1(2c)C v	
Excluded Components:	
Adapter Host NIC Option ROM CIMC Board Controller Fiex Flash Controller BIOS PSU SAS Expander Storage Controller Onboard Device Storage Device Bridge GPUs FC Adapters ✓ Local Disk	
	OK Cancel

#### Create Local Disk Configuration Policy (Optional)

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

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

To create a local disk configuration policy, complete the following steps:

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

- 2. Select Policies > root.
- 3. Right-click Local Disk Config Policies.
- 4. Select Create Local Disk Configuration Policy.
- 5. Enter SAN-Boot as the local disk configuration policy name.
- 6. Change the mode to No Local Storage.
- 7. Click OK to create the local disk configuration policy.
- 8. Click OK.

Create Local Dis		? ×			
Name	: SA	N-Boot			
Description	:				
Mode	: No	Local Storage	<b>T</b>		
FlexFlash					
FlexFlash State	: 💿	Disable 🔿 Enable			
If FlexFlash State is disabled Please ensure SD cards are n	, SD card	Is will become unave before disabling the	ailable immediately e FlexFlash State.	·-	
FlexFlash RAID Reporting St	ate : 💽	Disable O Enable			
					Canaal
				OK	Cancer

#### Create Power Control Policy

To create a power control policy for the Cisco UCS environment, complete the following steps:

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

- 5. Enter No-Power-Cap as the power control policy name.
- 6. Change the power capping setting to No Cap.
- 7. Click OK to create the power control policy.
- 8. Click OK.

## **Create Power Control Policy**

0	$\sim$
1	A

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.

04	Concol
UK	Cancel

#### Create Server Pool Qualification Policy (Optional)

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

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

- 1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
- 2. Select Policies > root.
- 3. Right-click Server Pool Policy Qualifications.
- 4. Select Create Server Pool Policy Qualification.
- 5. Enter UCSB-B200-M4 as the name for the policy.
- 6. Select Create Server PID Qualifications.
- 7. Enter UCSB-B200-M4 as the PID.
- 8. Click OK to create the server pool qualification policy.
- 9. Click OK, and then click OK again.

Create Server Pool Po	licy Qualification	? >
Naming		
Name : UCSB-B200-M4		
Description :		
This server pool policy qualification will	apply to new or re-discovered servers. Existing servers are not qualified until they are re-discovered	
Actions	Qualifications	
Create Adapter Qualifications	L T. Advanced Filter A Export Brint	\$
Create Chassis/Server Qualifications	Create Server PID Qualifications ? × Speed Stepping	Power Gro
Create Memory Qualifications		
Create CPU/Cores Qualifications		
Create Storage Qualifications		
Create Server PID Qualifications		
Create Power Group Qualifications		
Create Rack Qualifications		
	OK Cancel	
	ОК	Cancel

#### Create Server BIOS Policy

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

- 1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
- 2. Select Policies > root.
- 3. Right-click BIOS Policies.
- 4. Select Create BIOS Policy.
- 5. Enter VM-Host-Infra as the BIOS policy name.
- 6. Change the Quiet Boot setting to Disabled.
- 7. Click Next.

		Create BIOS Policy		? ×
0	Main	Name :	VM-Host-Infra	
2	Processor	Description : Reboot on BIOS Settings Change :	 O	
3	Intel Directed IO	Quiet Boot : Post Error Pause :	disabled	
0	RAS Memory	Resume Ac On Power Loss :	│ stay-off │ last-state │ reset ④ Platform Default	
5	Serial Port	Front Panel Lockout : Consistent Device Naming :	disabled       enabled       Platform Default         disabled       enabled       Platform Default	
6	USB			
0	PCI			
8	QPI			
9	LOM and PCIe Slots			
10	Trusted Platform			
1	Graphics Configuration			
12	Boot Options			
13	Server Management		< Prev Next > Finish Can	cel

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

		Create BIOS Policy		? ×
0	Main	Turbo Boost	: Odisabled OPlatform Default	
		Enhanced Intel Speedstep	: Odisabled OPlatform Default	
2	Processor	Hyper Threading	: Odisabled  enabled  Platform Default	
3	Intel Directed IO	Core Multi Processing	: all y	
		Execute Disabled Bit	: Odisabled O Platform Default	
4	RAS Memory	Virtualization Technology (VT)	: Odisabled • enabled OPlatform Default	
5	Serial Port	Hardware Pre-fetcher	: Odisabled Oenabled Platform Default	
		Adjacent Cache Line Pre-fetcher	: Odisabled O enabled O Platform Default	
6	USB	DCU Streamer Pre-fetch	: Odisabled Oenabled OPlatform Default	
7	PCI	DCU IP Pre-fetcher	: Odisabled Oenabled OPlatform Default	
		Direct Cache Access	: Odisabled O auto O Platform Default	-
8	QPI	Processor C State	: Odisabled Oenabled OPlatform Default	
	LOM and BCIe Slots	Processor C1E	: Odisabled O enabled O Platform Default	
	LOW and Pole Slots	Processor C3 Report	Platform Default	
10	Trusted Platform	Processor C6 Report	: Odisabled Oenabled OPlatform Default	
	Graphics Configuration	Processor C7 Report	Platform Default	
W	Graphics configuration	Processor CMCI	: O enabled O disabled O Platform Default	
12	Boot Options	CPU Performance	Platform Default	
		Max Variable MTRR Setting	: 🔿 auto-max 🔿 8 () Platform Default	
13	Server Management		< Prev Next > Finish Cano	el

- 16. Click next to go the Intel Directed IO Screen.
- 17. Change the VT for Direct IO to Enabled.

		Create BIOS Policy	? ×
1	Main	VT For Directed IO : Odisabled O enabled Platform Default	
	Draaaaa	Interrupt Remap : Odisabled Oenabled OPlatform Default	
2	Processor	Coherency Support : Odisabled enabled Platform Default	
3	Intel Directed IO	ATS Support : O disabled O enabled O Platform Default	
4	RAS Memory	Pass Through DMA Support : Odisabled Oenabled OPlatform Default	
5	Serial Port		
6	USB		
7	PCI		
8	QPI		
9	LOM and PCIe Slots		
10	Trusted Platform		
1	Graphics Configuration		
12	Boot Options		
13	Server Management	< Prev Next > Finish	Cancel

- 18. Click Next to go the RAS Memory screen.
- 19. Change the Memory RAS Config to maximum performance.
- 20. Change NUMA to Enabled.
- 21. Change LV DDR Mode to performance-mode.

		Create BIOS Policy	? ×
1	Main	Memory RAS Config : maximum-performance	
2	Processor	NUMA : disabled • enabled Platform Default	
		LV DDR Mode : Opwer-saving-mode operformance-mode auto Platform Default	
3	Intel Directed IO	DRAM Refresh Rate : Platform Default	
0	RAS Memory	DDR3 Voltage Selection : Oddr3-1500mv Oddr3-1350mv  Platform Default	
5	Serial Port		
6	USB		
7	PCI		
8	QPI		
9	LOM and PCIe Slots		
10	Trusted Platform		
1	Graphics Configuration		
12	Boot Options		
13	Server Management	< Prev Next > Finish	Cancel

- 22. Click Finish to create the BIOS policy.
- 23. Click OK.

### Create vNIC/vHBA Placement Policy for Virtual Machine Infrastructure Hosts

To create a vNIC/vHBA placement policy for the infrastructure hosts, complete the following steps:

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

Create Placement F	Policy	? ×
Name : Vi Virtual Slot Mapping Scheme :	M-Host-Infra	]
Ty Advanced Filter 🕴 Export	Print	\$
Virtual Slot	Selection Prefere	ence
1	Assigned Only	
2	All	
3	All	
4	All	
		OK Cancel

### Update Default Maintenance Policy

To update the default Maintenance Policy, complete the following steps:

- 1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
- 2. Select Policies > root.
- 3. Select Maintenance Policies > default
- 4. Change the Reboot Policy to User Ack.
- 5. Click Save Changes.
- 6. Click OK to accept the change.

	All	Servers / Policies / root / Mai	Intenance Policies / default
Equipment	<ul> <li>BIOS Policies</li> </ul>	General Events	
	<ul> <li>Boot Policies</li> </ul>	A still and	Descention
U	<ul> <li>Host Firmware Packages</li> </ul>	Actions	Properties
Servers	IPMI Access Profiles	Delete	Name : default
品	KVM Management Policies	Show Policy Usage	Description :
	Local Disk Config Policies	Use Global	Owner : Local
	<ul> <li>Maintenance Policies</li> </ul>		Soft Shutdown Timer : 150 Secs
	default		Reboot Policy : Immediate Ouser Ack Timer Automatic
SAN	Management Firmware Packages		On Next Boot (Apply pending changes at next reboot.)
	Memory Policy		
	Rower Control Policies		
VIVI	Device Control Policies		
	Power Sync Policies		
	<ul> <li>Scrub Policies</li> </ul>		

# Configure UCS SAN Connectivity

## Configure Unified Ports

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

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

•	All	Equipment / Fabric Interconnects / Fat	pric Interconnect A (subordinate)		
Equipment	▼ Equipment	General Physical Ports Physica	al Display FSM Faults Events Neighbors	Statistics	
Servers	<ul> <li>Chassis</li> <li>Rack-Mounts</li> <li>Servers</li> </ul>	Fault Summary	Physical Display		_
몲 LAN	Fabric Interconnects     Fabric Interconnect A (subordinate)	0 0 0 0			
SAN	<ul> <li>Fabric Interconnect B (primary)</li> </ul>	Status       Overall Status       Thermal       :        ↑ OK       Ethernet Mode       Ethernet Mode	💭 📕 Admin Down 📕 Fail 📕 Link Down		
		FC Mode : Switch	Properties		
		Oper Evac Mode : Off	Name : A Product Name : Cisco UCS 6324		
Storage		Actions	Vendor : Cisco Systems, Inc.	PID : UCS-FI-M-6324	
Chassis		Configure Evacuation Configure Unified Ports	Revision : 0 Available Memory : 4.894 (GB)	Serial : FCH19337NS1 Total Memory : 7.869 (GB)	
1		Internal Fabric Manager LAN Uplinks Manager	$\oplus$ Local Storage Information		
Admin		NAS Appliance Manager SAN Uplinks Manager	① Access		

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

**Configure Unified Ports** 

nstructions		—	
he position of the	slider determines the type of the p	ports.	
All the ports to the I	eft of the slider are Fibre Channel	ports (Purple), while the ports to the right are Etherne	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
ort 3	ether	Ethernet Uplink	
ort 4	ether	Ethernet Uplink	
		📕 Up 📕 Admin Down 📕 Fail 📕 Link Down	

? ×

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

#### Configure Fabric Interconnects in FC Switching Mode

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

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

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

	All	Equipment / Fabric Interconnects / Fabric Interconnect A (primary)		
Equipment	▼ Equipment	General Physical Ports Physical Dis	play FSM Faults Events Neighbors Statisti	cs
	Chassis	,	Product Name : Cisco UCS 6324	
U	<ul> <li>Rack-Mounts</li> </ul>	Actions	Vendor : Cisco Systems, Inc.	PID : UCS-FI-M-6324
Servers	Servers	Configure Evacuation	Revision : 0	Serial : FCH19337NS1
品	<ul> <li>Fabric Interconnects</li> </ul>	Configure Unified Ports	Available Memory : 4.824 (GB)	Total Memory: 7.869 (GB)
LAN	Fabric Interconnect A (primary)	Internal Fabric Manager	Local Storage Information	
	<ul> <li>Fabric Interconnect B (subordinate)</li> </ul>	LAN Uplinks Manager		
<b>=</b>		NAS Appliance Manager	+ Access	
SAN		SAN Uplinks Manager	() Lick Ausilability Dataila	
		SAN Storage Manager	+ High Availability Details	
VM		Disable Ports V	VLAN Port Count	
		Set Ethernet End-Host Mode		
Ð		Set Ethernet Switching Mode	+ FC Zone Count	
Storage		Set FC End-Host Mode		
		Set FC Switching Mode	Firmware	
Chassis		Activate Firmware	Boot-loader Version : v1.022.0	
		Management Interfaces	Kernel Version : 5.0(3)N2(3.12c)	
Admin			Package Version : 3.1(2c)A	
Aumin			Startup Kernel Version : 5.0(3)N2(3.12c)	

#### Create VSAN for the Fibre Channel Interfaces

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

- 1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
- 2. Expand the SAN > Storage Cloud tree.
- 3. Right-click VSANs.
- 4. Choose Create Storage VSAN.
- 5. Enter VSAN\_A as the name of the VSAN for fabric A.
- 6. Select the Enabled option for FC Zoning.
- 7. Click the Fabric A radio button.
- 8. Enter <<var\_vsan\_a\_id>> as the VSAN ID for fabric A.
- 9. Enter <<var\_fabric\_a\_fcoe\_vlan\_id>>as the FCoE VLAN ID for fabric A. and click OK, and click OK again.

Create Storage VSAN	? ×
Name : VSAN_A	
FC Zoning Settings	
FC Zoning : Disabled  Enabled	
Do <b>NOT</b> enable local zoning if fabric interconnect is connected	t to an upstream FC/FCoE switch.
○ Common/Global  ● Fabric A ○ Fabric B ○ Both Fabrics Co	onfigured 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 : 101	FCoE VLAN : 101
	OK Cancel

- 10. Right-click VSANs again and choose Create Storage VSAN.
- 11. Enter VSAN\_B as the name of the VSAN for fabric B.
- 12. Keep the Enabled option selected for FC Zoning.
- 13. Click the Fabric B radio button.
- 14. Enter <<var\_vsan\_b\_id>> as the VSAN ID for fabric B. Enter <<var\_fabric\_b\_fcoe\_vlan\_id>> as the FCoE VLAN ID for fabric B, click OK and then click OK again.

? ×
t to an upstream FC/FCoE switch.
onfigured Differently
A VLAN can be used to carry FCoE traffic and can be mapped to this VSAN.
Enter the VLAN ID that maps to this VSAN.
FCoE VLAN : 102
OK Cancel

## Configure the FC Ports as Storage Ports

To configure FC Storage Ports complete the following steps:

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



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

	All	Equipment / Fabric Interconne / Fabric Intercon	nnec / Fixed Module / FC Ports / FC Port 1
Fauioment	▼ Equipment	General Faults Events FSM Sta	tistics
	Chassis	Fach Company	Physical Disalas
U	<ul> <li>Rack-Mounts</li> </ul>	raut Summary	пузісаі Бізріаў
Servers	Servers	8 👽 🛆 🕚	
品	▼ Fabric Interconnects	0 0 0 0	
LAN	<ul> <li>Fabric Interconnect A (primary)</li> </ul>		
	<ul> <li>Fixed Module</li> </ul>	Status	
-	<ul> <li>Ethernet Ports</li> </ul>	Overall Status : 🛉 Up	Up 🖬 Admin Down 📕 Fail 🧧 Link Down
SAN	Port 3	Additional Info :	
	Port 4	Admin State : Enabled	
VM	Scalability Port 5	Actions	Properties
	* FC Ports		ID : 1 Slot ID : 1
$\mathbf{\Theta}$	FC Port 1	Disable Port	User Label :
Storage	FC Port 2	Configure as Uplink Port	WWPN : 20:01:8C:60:4F:A3:D4:80 Mode : F
	<ul> <li>Fabric Interconnect B (subordinate)</li> </ul>		Port Type : Physical Negotiated Speed : 8 Gbps
Chassis		Show Interface	VSAN : ic Dual/vsan default (1) *
			Transceiver Fabric A/vsan VSAN_A (101)
•			Type : S Fabric Dual/vsan default (1)
Admin			Model : FTLF8528P3BCV-CS
			Vander CISCO-FINISAD

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

- 11. Right-click and select configure as FC Storage Port.
- 12. Click Yes, then click OK.

	All	Equipment / Fabric Interconne / Fabric Interconne	ac / Fixed Module / FC Ports / FC Port 1 /
Equipment	▼ Equipment	General Faults Events FSM Statist	ics
	<ul> <li>Chassis</li> </ul>		
	▼ Rack-Mounts	Fault Summary	Physical Display
Servers	Servers	8 0 0	
品	<ul> <li>Fabric Interconnects</li> </ul>	0 0 0 0	
LAN	<ul> <li>Fabric Interconnect A (primary)</li> </ul>		
	<ul> <li>Fabric Interconnect B (subordinate)</li> </ul>	Status	
5	<ul> <li>Fixed Module</li> </ul>	Overall Status : 4 Admin Down	Up 📕 Admin Down 📕 Fail 📕 Link Down
SAN	Ethernet Ports	Additional Info : Administratively down	
	▼ FC Ports	Admin State : Disabled	Presenting
VM	FC Port 1	Actions	roperues
	Enable FC Por	Port	ID : 2 Slot ID : 1
	Disable	a Port	User Label :
Storage	Configure as Uplink P	Port ure as Unlink Port	WWPN : 20:02:8C:60:4F:BC:29:40 Mode : F
	Configure as FC Stor	age Port	Port Type : Physical Negotiated Speed : 8 Gbps
	Copy	nterface	VSAN : Fabric ( *
ChidSSIS			Transceiver
4	Delete		Type : Sfp

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

	All	Equipment / Fabric Interconne / Fabric Interconnec / Fixed Module / FC Ports / FC Port 1				
Equipment	▼ Equipment	General Faults Events FSM Statistics				
	<ul> <li>Chassis</li> <li>Rack-Mounts</li> </ul>	Fault Summary Physical Display				
Servers	Servers	8 0 0 0 0 00000000000000000000000000000				
品 LAN	<ul> <li>Fabric Interconnects</li> <li>Fabric Interconnect A (primary)</li> </ul>					
	<ul> <li>Fabric Interconnect B (subordinate)</li> <li>Fixed Module</li> </ul>	Status Overall Status :      Up Admin Down Fai Link Down				
	<ul> <li>Ethernet Ports</li> <li>FC Ports</li> </ul>	Additional Info : Admin State : Enabled				
VM	FC Port 1	Actions	-			
Storage	FC Port 2	Enable Port         ID         : 1         Slot ID         : 1           Disable Port         User Label :         User Label :         VWPN         : 20:01:80:60:4F:BC:29:40         Mode         : E				
		Configure as FC Storage Port Port Type : Physical Negotiated Speed : Indeterminate				
Chassis Admin		Snow metrace     vsavi     ic usarysan denaut (1) *       Transceiver Fabric Blycan VSAN_B (102)       Type     : s Fabric Dual/vsan default (1)       Model : FTLF8528P38CV-CS				

#### Create WWNN Pools

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

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

- 2. Choose Pools > root.
- 3. Right-click WWNN Pools.
- 4. Choose Create WWNN Pool.
- 5. Enter WWNN\_Pool as the name of the WWNN pool.
- 6. (Optional) Add a description for the WWNN pool.
- 7. Click Next.
- 8. Click Add to add a block of WWNNs.
- 9. Keep the default block of WWNNs, or specify a base WWNN.
- 10. Specify a size for the WWNN block that is sufficient to support the available blade or server resources.
- 11. Click OK.
- 12. Click Finish.
- 13. Click OK.

		All	SAN	SAN / Pools / root / WWNN Pools				
	Equipment	* SAN	0000	INN POOIS				
Ĩ		SAN Cloud				Create WWNN Pool	? × [	
	U	Storage Cloud					1	ned
	Servers	Policies		Define Nan	ne and Description	+ - Ty Advanced Filter 🛧 Export 🖶 Print	\$	
	品	* Pools	6	Add WWN	0	Name From To		
	LAN	🔻 root 🕚	U		Create WW	VN Block ? × po:25:E	35:00:00:3F	
	0	IQN Pools			From : 20:00:00:	25:85:00:00:00 Size : 64		
		WWNN Pools				se of WM/Ne in the SAN fabric, you are strongly encouraged to use		
		▶ WWPN Pools			the following WWN	prefix:		
		WWxN Pools			20:00:00:25:b5:xx:	xxxx		
	VM	Sub-Organizations						
	B					OK Cancel		
	A					Add Delete		
	Chassis					< Prev Finish	Cancel	

#### Create WWPN Pools

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

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

In this procedure, two WWPN pools are created: one for fabric A and one for fabric B.

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

	All	SAN	/ Pools / root / WWPN Pools			
	* SAN	ww	PN Pools			
Equipment	SAN Cloud			Create WWPN Pool	? ×	
	Storage Cloud					ned
Servers	Policies	U	Define Name and Description	Name : WWPN_Pool_A		
品	▼ Pools	2	Add WWN Blocks	Assignment Order:		
LAN	🔻 root 🕦			Assignment Order :		
A	IQN Pools					
SAN	WWNN Pools					
	WWPN Pools					
Y	WWxN Pools					
VM	Sub-Organizations					
Storage						
Chassis					01	
				Next > Finish	Cancel	
		_		🛨 Add 🔢 Delete 🕕 Info		

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

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

- 10. Specify a size for the WWPN block that is sufficient to support the available blade or server resources.
- 11. Click OK.

- 12. Click Finish to create the WWPN pool.
- 13. Click OK.

Crea	te WWN Block	? ×
From :	20:00:00:25:B5:01:0A:00	Size : 64 🌲
To ensui the follow	re uniqueness of WWNs in the S wing WWN prefix:	SAN fabric, you are strongly encouraged to use
20:00:00	):25:b5:xx:xx:xx	
		OK Cancel
14. F	Right-click WWPN Pools.	

- 15. Choose Create WWPN Pool.
- 16. Enter WWPN\_Pool\_B as the name for the WWPN pool for fabric B.
- 17. (Optional) Enter a description for this WWPN pool.
- 18. Click Next.
- 19. Click Add to add a block of WWPNs.
- 20. Enter the starting WWPN address in the block for fabric B.



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

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

#### Create vHBA Templates for Fabric A and Fabric B

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

- 1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
- 2. Choose Policies > root.
- 3. Right-click vHBA Templates.
- 4. Choose Create vHBA Template.
- 5. Enter vHBA\_Template\_A as the vHBA template name.
- 6. Click the radio button Fabric A.
- 7. In the Select VSAN list, Choose VSAN\_A.
- 8. In the WWPN Pool list, Choose WWPN\_Pool\_A.
- 9. Click OK to create the vHBA template.
- 10. Click OK.

	All	Create vHBA Template	? ×
Equipment	* SAN	Name : vHBA_Template_A	
A	SAN Cloud	Description :	
Servers	Storage Cloud     Policies	Fabric ID : • A B Redundancy	
몲	SAN Cloud	Redundancy Type : No Redundancy O Primary Template O Secondary Template	
LAN	* root 🕐 Default vHBA Behavior	Select VSAN : VSAN_A	
SAN	Fibre Channel Adapter Policies	Template Type :  initial Template Updating Template Max Data Field Size : 2048	
0	<ul> <li>SAN Connectivity Policies</li> </ul>	WWPN Pool : WWPN_Pool_A(60/64) V	
VM	Storage Connection Policies	QoS Policy : <pre><not set=""> ▼</not></pre>	
	Inreshold Policies     VHBA Templates	Pin Group : <pre> cnot set&gt; v</pre>	
Storage	<ul> <li>Sub-Organizations</li> </ul>	Stats Threshold Policy : default 🔻	
	▶ Pools		
Chaissis			
Admin			
		ОК Са	ncel

- 11. In the navigation pane, click the SAN tab.
- 12. Choose Policies > root.

- 13. Right-click vHBA Templates.
- 14. Choose Create vHBA Template.
- 15. Enter vHBA\_Template\_B as the vHBA template name.
- 16. Click the radio button Fabric B.
- 17. In the Select VSAN list, Choose VSAN\_B.
- 18. In the WWPN Pool, Choose WWPN\_Pool\_B.
- 19. Click OK to create the vHBA template.
- 20. Click OK.

#### Create vHBA Template

?	$\times$

Name	:	vHBA_Template_B
Description	:	
Fabric ID	:	
Redundancy		
Redundancy Type		:      No Redundancy      Primary Template      Secondary Template
Select VSAN	:	VSAN_B Create VSAN
Template Type	:	● Initial Template    Updating Template
Max Data Field Size	:	2048
WWPN Pool	;	WWPN_Pool_B(64/64) •
QoS Policy	:	<not set=""> ▼</not>
Pin Group	:	<not set=""></not>
Stats Threshold Policy :		default 🔻

#### Create the Storage Connection Policy Fabric-A

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

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

ОК

Cancel

	All	SAN / Policies / root / Storage Connection Policies
Equipment	* SAN	Storage Connection Policies
Equipment	SAN Cloud	+ - T <sub>ℓ</sub> Advanced Filter ↑ Export   Print
	Storage Cloud	Name Description WWPN
Servers	<ul> <li>Policies</li> </ul>	▶ Fabric-A
品	SAN Cloud	▶ Fabric-B
LAN	🔻 root 🕔	
	Default vHBA Behavior	
	Fibre Channel Adapter Policies	
SAN	LACP Policies	
	<ul> <li>SAN Connectivity Policies</li> </ul>	
VM	<ul> <li>Storage Con Create Storage Connect</li> </ul>	ation Policy
	Threshold Policies	
Storage	<ul> <li>vHBA Templates</li> </ul>	
Storage	Sub-Organizations	
	Pools	
Chassis		

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

Create Storage Name : Fabric-A Description : Zoning Type : None FC Target Endpoints	Single Initiator Single Target   Single Initiator	or Multiple Targets	? ×
Te Advanced Filter 🔶 Exp	port 🚔 Print		\$
WWPN	Path	VSAN	
	⊕ Add      □ Delet	e 🕚 Info	Cancel

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

- 10. Select VSAN VSAN\_A.
- 11. Click OK to create the FC Target Endpoint.

	All	Create Storage Connection Policy
Equipment	* SAN	Name : Fabric-A
	SAN Cloud	Description :
	Storage Cloud	Zoning Type : O None O Single Initiator Single Target  Single Initiator Multiple Targets
Servers	<ul> <li>Policies</li> </ul>	FC Target Endpoints
品	SAN Cloud	Create EC Target Endpoint
LAN	🔻 root 🚺	oreater o rarget Endpoint
0	Default vHBA Behavior	WWPN : 50:05:07:68:0D:04:58:F1
	Fibre Channel Adapter Policies	Description :
SAN	LACP Policies	Path : O A O B
	SAN Connectivity Policies	Select VSAN VSAN A (101) V Create VSAN Create Storage VSAN
VM	Storage Connection Policies	
<b>A</b>	Threshold Policies	
Storago	vHBA Templates	OK Cancel
Storage	Sub-Organizations	

- 12. Click the Add button to add the FC Target Endpoint.
- 13. Enter the WWPN for Node 2 Fabric A <<var\_wwpn\_Node2-switch-A>>.
- 14. Select Path A.
- 15. Select VSAN VSAN\_A.
- 16. Click OK to create the FC Target Endpoint.
- 17. Click OK to create the storage connection policy.

	All	Create Storage Connection Policy ?	X
Equipment	▼ SAN	Name : Fabric-A	
	SAN Cloud	Description :	
U	Storage Cloud	Zoning Type : O None O Single Initiator Single Target O Single Initiator Multiple Targets	
Servers	▼ Policies	FC Target Endpoints	
品	SAN Cloud	Create EC Target Endpoint	$\times$
LAN	▼ root 🕦		
	Default vHBA Behavior	WWPN : 50:05:07:68:0D:04:58:F0	
	Fibre Channel Adapter Policies	Description :	
SAN	LACP Policies	Path : OA OB	
	SAN Connectivity Policies	Select VSAN : VSAN VSAN_A (101)   Create VSAN Create Storage VSAN	
VM	Storage Connection Policies		
8	Threshold Policies		
Storago	vHBA Templates	ОК Сапсеі	)
Storage	Sub-Organizations		

### Create the Storage Connection Policy Fabric-B

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

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

16. Click OK to create the storage connection policy.

### Create a SAN Connectivity Policy

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

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

	All	SAN / Policies / root / SAN Connectivity Policies	
	▼ SAN	SAN Connectivity Policies	
Equipment	SAN Cloud	Te Advanced Filter 🔶 Export 📑 Print	
	Storage Cloud	Name	D
Servers	<ul> <li>Policies</li> </ul>	Dual-Fabric	
品	SAN Cloud	Test-FCOE	
LAN	🔻 root 🕚		
	Default vHBA Behavior		
	Fibre Channel Adapter Policies		
SAN	LACP Policies		
	SAN Connertitie Balisies     Create SAN Connectiv	vity Policy	
VM	Storage Connection Policies		
	Threshold Policies		
	vHBA Templates		
Storage	Sub-Organizations		
	▶ Pools		
Chassis			

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

	e					
WWNN Assignr	nent:	WWNN_Pool(64/64)		•		
Create WWNN P	ool					
The WWNN will b The available/tota	e assigned from I WWNNs are di	the selected pool. splayed after the pool nar	me.			
Jame			WWPN			_
		N	o data available			
			a 🕀 Add 🕚 Modif			
					OK Cancel	)
7. Enter Nar	me Fabric-	A.				
8. Click Use	e vHBA-ter	nplate.				
9. Select vH	IBA_Temp	late_A.				
10. Select Ad	dapter Poli	cy VMware.				
reate vHBA						?
ame :	Fabric-A					
se vHBA Template :						
edundancy Pair :			Peer Name :			
IBA Template : vH	BA_Template_A	~ -	Create VHBA Te	emplate		
Adapter Policy : <	not set> 🔻		Create Fibre Ch	nannel Adapter Polic	су	
	<not set=""></not>					
	Domain Policie:	5				
	Solaris					
	/MWare					
N N	Windows					
	WindowsBoot					
	Jerault					

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

Create SAN Connectiv	vity Policy	? ×
Name : Dual-Fabric Description : A server is identified on a SAN by its Wo associated with this profile. World Wide Node Name	rld Wide Node Name (WWNN). Specify how the system should assign a WWNN	to the server
WWNN Assignment: Create WWNN Pool The WWNN will be assigned from The available/total WWNNs are d	WWNN_Pool(64/64)         • the selected pool.         isplayed after the pool name.	
Name	WW/PN	
vHBA Fabric-B	Derived	
vHBA If default		
👻 vHBA Fabric-A	Derived	
vHBA If default		
		K Cancel

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

	All	SAN / Policies / root / SAN Connectivity Polic / Dual-Fabric
Equipment	* SAN	General VHBA Initiator Groups Events
	SAN Cloud     Storage Cloud	Ty Advanced Filter ↑ Export ⊕ Print 🗘
Servers	<ul> <li>Policies</li> </ul>	Name Storage Connection Policy Name
品	SAN Cloud	No data available
LAN	🔻 root 🕚	
A	Default vHBA Behavior	
	<ul> <li>Fibre Channel Adapter Policies</li> </ul>	
SAN	LACP Policies	
	<ul> <li>SAN Connectivity Policies</li> </ul>	(+) Add 🗊 Delete 🕕 Info
VM	Dual-Fabric	
	Storage Connection Policies	Details
	Threshold Policies	General Events
Storage	vHBA Templates	

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

Create vHBA Initiator Group		? ×
vHBA Initiator Group       Name     :       Fabric-A       Description :		-
Select VMBA Initiators	\$	-
Select	Name	
$\checkmark$	Fabric-A	
	Fabric-B	
Storage Connection Policy: Fabric-A  Create Storage Connection Policy		I
	ОК С	ancel

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

	All	SAN / Policies / root / SAN Connectivity Polic / Dual-	Fabric	
Equipment	▼ SAN	General vHBA Initiator Groups Events		
	SAN Cloud	T. Advanced Filter ▲ Export ♣ Print		ň
U	Storage Cloud	Second and a second second	Disease Describes Delles Marco	*
Servers	* Policies	Name	Storage Connection Policy Name	
县	SAN Cloud	Fabric-A	Fabric-A	
LAN	🔻 root 🔇	Fabric-B	Fabric-B	
	Default vHBA Behavior			
	Fibre Channel Adapter Policies			
SAN	LACP Policies			
	<ul> <li>SAN Connectivity Policies</li> </ul>		(+) Add i Delete (1) Info	
VM	Dual-Fabric			
	Storage Connection Policies	Details		

#### **Create Boot Policies**

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

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



#### Table 14 IBM V5030 - WWPN Information

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

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

You will use the WWPN variables that were logged in the storage section of the WWPN table.

- 1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
- 2. Choose Policies > root.
- 3. Right-click Boot Policies.
- 4. Choose Create Boot Policy.
- 5. Enter Boot-Fabric-A as the name of the boot policy.
- 6. (Optional) Enter a description for the boot policy.
- 7. Keep the Reboot on Boot Order Change check box unchecked.
- 8. Expand the Local Devices drop-down menu and Choose Add CD/DVD (you should see local and remote greyed out).

Create Boot Policy	/											?
Name	: Boot-Fab	ric-A										
Description	:											
Reboot on Boot Order Change	: 🗆											
Enforce vNIC/vHBA/iSCSI Name	et 🔽											
Boot Mode	: 💿 Legac	y 🔾 Uefi										
The type (primary/secondary) do the effective order of boot devic Enforce VNIC/VHBA/ISCSI Nar it is not selected, the vNICs/vH	es not indicat es within the ne is selected 3As are selec	e a boot on same devic d and the vi ted if they	der presence. e class (LAN/Storag NIC/vHBA/iSCSI doe exist, otherwise the	e/iSCSI) is s not exist, vNIC/vHBA	determine a config e with the k	d by PCle rror will b west PC	e bus scan o be reported. le bus scan	rder. order is use	ed.			
<ul> <li>Local Devices</li> </ul>		Boot Ord	er	♠ Export	🚔 Print							ö
Add Local Disk		T -	1. Playaneou rinor		while/	Tuno	1404/51		Slot N	Reat	Reat	Deseri
Add Local LUN		Name		0r	VINIC/	Type	VVVVIN	LUN N	SIDE IN	BOOL	BOOL	Desch.
Add Local JBOD		CD/D	VD	1								
Add SD Card												
Add Internal USB												
Add External USB												
Add Embedded Local LUN												
Add Embedded Local Disk												
					1 Move	Up 🦊	Move Down	🗓 Delete	9			
dd CD/DVD												
Add CD/DVD Add Local CD/DVD												
Add CD/DVD Add Local CD/DVD Add Remote CD/DVD												
Add CD/DVD Add Local CD/DVD Add Remote CD/DVD Add Floppy												
Add CD/DVD Add Local CD/DVD Add Remote CD/DVD Add Floppy Add Local Floppy												
Add CD/DVD Add Local CD/DVD Add Remote CD/DVD Add Floppy Add Local Floppy Add Remote Floppy												

- 9. Expand the vHBAs drop-down menu and Choose Add SAN Boot.
- 10. In the Add SAN Boot dialog box, enter Fabric-A in the vHBA field.
- 11. Make sure that the Primary radio button is selected as the SAN boot type.
- 12. Click OK to add the SAN boot initiator.

Add	SAN Boot	? ×
vHBA :	Fabric-A	
Type :	● Primary ◯ Secondary ◯ Any	
	ОК Са	ncel

- 13. From the vHBA drop-down menu, choose Add SAN Boot Target.
- 14. Keep 0 as the value for Boot Target LUN.
- 15. Enter the WWPN for Node 1 connected to UCS Fabric Interconnect A << var\_wwpn\_FC\_NodeA-fabricA >>
- 16. Keep the Primary radio button selected as the SAN boot target type.
- 17. Click OK to add the SAN boot target.

Add SAN Bo	ot Target	? ×
Boot Target LUN :	0	
Boot Target WWPN :	50:05:07:68:0D:04:58:F0	
Type :	Primary      Secondary	
	ОК	Cancel

- 18. From the vHBA drop-down menu, choose Add SAN Boot Target.
- 19. Keep 0 as the value for Boot Target LUN.
- 20. Enter the WWPN for Node 2 connected to UCS Fabric Interconnect A << var\_wwpn\_FC\_NodeB-fabricA >>
- 21. Click OK to add the SAN boot target.

Add SAN Bo	? ×	
Boot Target LUN :	0	
Boot Target WWPN :	50:05:07:68:0D:08:58:F0	
Type :	OPrimary  Secondary	
	ОК	Cancel

- 22. From the vHBA drop-down menu, choose Add SAN Boot.
- 23. In the Add SAN Boot dialog box, enter Fabric-B in the vHBA box.
- 24. The SAN boot type should automatically be set to Secondary.
- 25. Click OK to add the SAN boot initiator.
- 26. From the vHBA drop-down menu, choose Add SAN Boot Target.
- 27. Keep 0 as the value for Boot Target LUN.
- 28. Enter the WWPN for Node 2 connected to UCS Fabric Interconnect B << var\_wwpn\_FC\_NodeB-fabricB >>
- 29. Keep Primary as the SAN boot target type.
- 30. Click OK to add the SAN boot target.

Add SAN Boot T	arget ?×
Boot Target LUN : 0	
Boot Target WWPN : 50:0	5:07:68:0D:04:58:F1
Type : • Pr	imary O Secondary
	OK Cancel

- 31. From the vHBA drop-down menu, choose Add SAN Boot Target.
- 32. Keep 0 as the value for Boot Target LUN.
- 33. Enter the WWPN for Node 1 connected to UCS Fabric Interconnect B << var\_wwpn\_FC\_NodeAfabricB >>
- 34. Click OK to add the SAN boot target.

Add SAN Bo	? ×	
Boot Target LUN :	0	
Boot Target WWPN :	50:05:07:68:0D:08:58:F1	
Type :	OPrimary  Secondary	
	ОК	Cancel

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

Create Boot Policy									? ×
Name :	Boot-Fabr	c-A							
Description :									
Reboot on Boot Order Change :									
Enforce vNIC/vHBA/iSCSI Name :	<ul> <li>Image: A start of the start of</li></ul>								
Boot Mode :	Legacy	Uefi							
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 p ame device cla and the vNIC/v ed if they exist	oresence. Iss (LAN/Storage/iSi /HBA/iSCSI does no , otherwise the vNIC	CSI) is determine t exist, a config e /vHBA with the lo	d by P rror wi owest I	Cle bus scan o ill be reported. PCle bus scan	rder. order is used.		
Local Devices		Boot Order							
⊕ vNICs		+ - Tr	Advanced Filter 🔺	Export 🖶 Print	;/v	Туре	WWN		¢
⊖ vHBAs		👻 SAN F	Primary	Fabrio	:-A	Primary			
Add SAN Boot		SA	N Target Primary			Primary	50:05:07:68:0D:04:58:F0	0	
Add SAN Boot Target		SA	N Target Secondar	У		Secondary	50:05:07:68:0D:08:58:F0	0	- 1
		👻 SAN S	Secondary	Fabrio	:-В	Secondary			
+ iSCSI vNICs		SA	N Target Primary			Primary	50:05:07:68:0D:04:58:F1	0	
		C.A.	N Taraat Sacandar	1 Mov	e Up	Move Dow	50:05:07:69:00:09:59:51	0	
+ CIMC Mounted vMedia									
+ EFI Shell									



## Configure UCS LAN Connectivity

#### Configure Uplink Port Channels to Cisco Nexus Switches

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

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

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

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

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

		Create Port Channel	? ×
0	Set Port Channel Name	ID : 13	
2	Add Ports	Name : vPC-13-Nexus	
		< Prov Next > Finish C	ancel

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

1	Set Port Channel Name		Ports				Ports in the	port chan	inel
2	Add Ports	Slot ID	Aggr. Po Port	MAC		Slot ID	Aggr. Po	Port	MAC
			No data available			1	0	3	8C:60:4
					>>	1	0	4	8C:60:4
					<<				

- 12. In the navigation pane, under LAN > LAN Cloud, expand the fabric B tree.
- 13. Right-click Port Channels.
- 14. Select Create Port Channel.
- 15. Enter 14 as the unique ID of the port channel.
- 16. Enter vPC-14-Nexus as the name of the port channel.
- 17. Click Next.
- 18. Select the following ports to be added to the port channel:
  - Slot ID 1 and port 3
  - Slot ID 1 and port 4
- 19. Click >> to add the ports to the port channel.
- 20. Click Finish to create the port channel.
- 21. Click OK.

#### Create MAC Address Pools

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

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

2. Select Pools > root.

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

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

	All   LAN / Pools / root / MAC Pools								
Equipment	* LAN			Create MAC Pool	? ×				
	<ul> <li>LAN Cloud</li> <li>Appliances</li> </ul>	0	Define Name and Description	Name : MAC_Pool_A	As	ssigr			
Servers	Internal LAN     Policies	2	Add MAC Addresses	Description     :       Assignment Order :        • Default        · Sequential					
LAN	<ul><li>▼ Pools</li><li>▼ root <ul><li></li></ul></li></ul>				1				
SAN	IP Pools      MAC Pools								
	<ul> <li>Sub-Organizations</li> </ul>								
Storage	<ul> <li>Netflow Monitoring</li> <li>Flow Record Definitions</li> </ul>								
Chassis	Flow Exporters     Flow Monitors     Flow Monitor Sessions			< Prev Next > Finish Ca	Incel				

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

For the VersaStack solution, the recommendation is to place 0A in the next-to-last octet of the starting MAC address to identify all of the MAC addresses as fabric A addresses.

10. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources.
|   |  | Create MAC Pool  | ? × |
|---|--|--|-----|
| 1 | Define Name and Description                                  | + - Ty Advanced Filter 🛧 Export 🖶 Print                              | \$  |
| 2 | Add MAC Addresses  | Name From To   |     |
|   | Create a Block of N  | VAC Addresses ? ×  | F   |
|   | First MAC Address : 00:25:B5:                                | :07:0A:00 Size : 64  |     |
|   | To ensure uniqueness of MACs in prefix:<br>00:25:B5:xx:xx:xx | the LAN fabric, you are strongly encouraged to use the following MAC |     |
|   |  |  |     |
|   |  | OK Cancel  |     |
|   |  | 🕀 Add 🗎 Delete   |     |
|   |  | < Prev Next > Finish Cano  | el  |

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

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

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

		Create MAC Pool	? ×
1	Define Name and Description	+ - Ty Advanced Filter 🛧 Export 📑 Print	≎
2	Add MAC Addresses	Name From To	
	Create a Block of N	AC Addresses ? ×	F
	First MAC Address : 00:25:85:	07:0B:00 Size : 64	
	To ensure uniqueness of MACs in t prefix: 00:25:B5:xx:xx:xx	he LAN fabric, you are strongly encouraged to use the following MAC	
		🕀 Add 🛅 Delete	
		<b>&lt; Prev</b> Next > Finish Can	cel

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

### Create VLANs

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

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

In this procedure, five VLANs are created.

2. Select LAN > LAN Cloud.

- 3. Right-click VLANs.
- 4. Select Create VLANs
- 5. Enter IB-MGMT-VLAN as the name of the VLAN to be used for management traffic.
- 6. Keep the Common/Global option selected for the scope of the VLAN.
- 7. Enter <<var\_ib-mgmt\_vlan\_id>> as the ID of the management VLAN.
- 8. Keep the Sharing Type as None.
- 9. Click OK and then click OK again.

Create VLANs		? ×
VLAN Name/Prefix : IB-M0	GMT-VLAN	
Multicast Policy Name : <not< td=""><td>t set&gt;      Create Multicast Policy</td><td></td></not<>	t set>      Create Multicast Policy	
Common/Global	○ Fabric B ○ Both Fabrics Configured Differently	
You are creating global VLANs the term of the term of VLAN IDs.(e.g	hat map to the same VLAN IDs in all available fabrics. g. " 2009-2019" , " 29,35,40-45" , " 23" , " 23,34-45" )	
VLAN IDs : 11		
Sharing Type : None F	Primary Isolated Community	
	Check Overlap OK C	ancel

- 10. Right-click VLANs.
- 11. Select Create VLANs
- 12. Enter vMotion-VLAN as the name of the VLAN to be used for vMotion.
- 13. Keep the Common/Global option selected for the scope of the VLAN.
- 14. Enter the <<var\_vmotion\_vlan\_id>> as the ID of the vMotion VLAN.
- 15. Keep the Sharing Type as None.
- 16. Click OK, and then click OK again.

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

### Set Jumbo Frames in Cisco UCS Fabric

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

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

	All 👻	LAN / LAN C	loud / QoS Sys	stem Class							
Equipment	▼ LAN	General	Events FS	SM							
	<ul> <li>▼ LAN Cloud</li> <li>▶ Fabric A</li> </ul>	Priority	Enable	d CoS	Packet Drop	Weight		Weight (%)	мти		Multicast Optimized
Servers	Fabric B	Platinum		5		10	v	N/A	normal	Ŧ	
品	QoS System Class	Gold		4		0		N/A	normal	, 	
LAN	<ul> <li>LAN Pin Groups</li> </ul>			-	_	5	5		normai	,	
	Threshold Policies	Silver		2		8	Ψ.	N/A	normal	<b>T</b>	
SAN	<ul> <li>VLAN Groups</li> </ul>	Bronze		1		7		N/A	normal	<b>V</b>	
	▶ VLANs	Best	3	Anv		r		50	0010		
Y	<ul> <li>Appliances</li> </ul>	Effort		,		5	5		9210	<u>,</u>	
VM	Fabric A	Fibre Channel	V	3		5	<b>V</b>	50	fc		N/A
	Fabric B										
Storage	▶ VLANs										
	<ul> <li>Internal LAN</li> </ul>										
	Internal Fabric A										
Chassis	Internal Fabric B										
20	Threshold Policies										
Admin	<ul> <li>Policies</li> </ul>										
	▶ Pools										
	<ul> <li>Traffic Monitoring Sessions</li> </ul>										
	<ul> <li>Netflow Monitoring</li> </ul>										

## Create Network Control Policy for Cisco Discovery Protocol

To create a network control policy that enables Cisco Discovery Protocol (CDP) on virtual network ports, complete the following steps:

- 1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
- 2. Select Policies > root.
- 3. Right-click Network Control Policies.
- 4. Select Create Network Control Policy
- 5. Enter Enable\_CDP as the policy name.
- 6. For CDP, select the Enabled option.
- 7. Click OK to create the network control policy.

Create Netw	ork Control Policy	? ×
Name	: Enable_CDP	1
Description	:	
CDP	: Disabled • Enabled	
MAC Register Mode	: • Only Native Vlan 🔿 All Host Vlans	
Action on Uplink Fail	: O Link Down O Warning	
MAC Security		
Forge : O Allow	Deny	1
LLDP		
	ОК Са	ancel

8. Click OK.

### Create vNIC Templates

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

#### Create Management vNICs

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

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

reate vN	IC Temp	olate		?
lame	: vNIC	_Mgmt_A		
Description	:			
abric ID Redundancy	: •	Fabric A 🚫 Fabric B 📃 Enable Fa	ilover	
Redundancy Ty	/pe :	O No Redundancy  Primary Templ	ate 🔿 Secondary Template	
Peer Redundar	cy Template :	<not set=""> V</not>		
rget				
/ Adapter VM				
Warning				
f <b>VM</b> is selected f a port profile o	l, a port profile f the same nar	by the same name will be created. ne exists, and updating template is sele	cted, it will be overwritten	
emplate Type	: 🔾 In	itial Template <ul> <li>Updating Template</li> </ul>		
VLANs				
Te Advanced File	ter 🔺 Export	reint 👘 Print		¢
Select		Name	Native VLAN	
		default	0	
$\checkmark$		IB-MGMT-VLAN	0	
$\checkmark$		Native-VLAN	۲	

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

	default	0	
$\checkmark$	IB-MGMT-VLAN	0	
$\checkmark$	Native-VLAN	۲	
	VM-Traffic-VLAN	0	
	vMotion-VLAN	0	
CDN Source :	● vNIC Name ◯ User Defined		
MTU :	1500		
MAC Pool :	MAC_Pool_A(32/32) V		
QoS Policy :			
Network Control Policy			
Network Control Policy .	Enable_CDP V		
Pin Group :	<not set=""></not>		
Stats Threshold Policy :	default 🔻		
<b>Connection Policies</b>			
Dynamic vNIC Connect	ion Policy : <not set=""> V</not>		
			OK Cancel

18. Click OK to create the vNIC template.

19. Click OK.

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

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

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

Create vNIC	Template			? ×
Name Description Fabric ID	: vNIC_Mgmt_B : : Fabric A () Fab	ric B Fnable Failover		
Redundancy	. 0.100.001.00.00			
Redundancy Type Peer Redundancy Te	: No Redundance emplate : vNIC_Mgmt_A	ry ○ Primary Template ④ S	Secondary Template	
Target				
Adapter				
Warning				
If <b>VM</b> is selected, a p If a port profile of the	ort profile by the same name same name exists, and upda	will be created. ting template is selected, it w	vill be overwritten	
Template Type	: O Initial Template  U	pdating Template		
Ty Advanced Filter	🛧 Export 🛛 🖶 Print			¢
Select	Name		Native VLAN	
	defaul	t	0	
$\checkmark$	IB-MG	MT-VLAN	0	
$\checkmark$	Native	-VLAN	۲	
			ок	Cancel

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

#### VLANs ₽ Ty Advanced Filter Export 🖶 Print Select Name Native VLAN default $\checkmark$ **IB-MGMT-VLAN** ۲ $\checkmark$ Native-VLAN VM-Traffic-VLAN vMotion-VLAN vNIC Name User Defined CDN Source 2 MTU 1500 1 MAC Pool MAC\_Pool\_B(32/32) \* QoS Policy <not set> 🔻 Network Control Policy : Enable\_CDP 🔻 Pin Group Ŧ <not set> Stats Threshold Policy : default 🔻 **Connection Policies** Oynamic vNIC UsNIC VMQ Dynamic vNIC Connection Policy : <not set> 🔻

? ×

**OK** 

Cancel

118

- 18. Click OK to create the vNIC template.
- 19. Click OK.

### Create vMotion vNICs

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

reate vNIC	C Template		?
ame escription abric ID <b>Redundancy</b>		Failover	
Redundancy Type Peer Redundancy	e : No Redundancy  Primary Ter	nplate 🔿 Secondary Template	
rget '_ Adapter _ VM			
Warning <b>VM</b> is selected, a a port profile of t emplate Type	a port profile by the same name will be created. he same name exists, and updating template is s : O Initial Template () Updating Template	elected, it will be overwritten	
/LANs			
Advanced Filter	🛉 Export 🖷 Print		\$
Select	Name	Native VLAN	
	default	0	
	IB-MGMT-VLAN	0	
	Native-VLAN	0	
		ОК	Cancel

- 13. Set vMotion as the native VLAN.
- 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.

\_

Te Advanced Filter + Export	Print		\$
Select	Name	Native VLAN	
	default	0	
	IB-MGMT-VLAN	0	
	Native-VLAN	0	
	VM-Traffic-VLAN	0	
✓	vMotion-VLAN	۲	
QoS Policy : <a href="https://www.commons.com"></a>	cdd a		
Pin Group : <a>Anot set</a> Stats Threshold Policy : default	> Y		

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

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

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

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

Create vNIC Ten	nplate		?
Name : VN Description : Fabric ID : Redundancy Redundancy Type Peer Redundancy Template	IC_vMotion_B  Fabric A  Fabric B Enable Faile  No Redundancy Primary Template  Cont set>	ver	
rget Adapter VM Warning f VM is selected, a port profi f a port profile of the same of	<not set=""> Domain Policies vNIC_Mgmt_A vNIC_vMotion_A</not>	ed, it will be overwritten	
Template Type : O	Initial Template   Updating Template		
Ty Advanced Filter + Exp	ort 🖶 Print	No. 10 AN	\$
Select	Name		
	default	Õ	
	IB-MGMT-VLAN Native-VLAN	0	
		$\cap$	
		ОК	Cancel

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

**VLANs** 

Select	Name	Native VLAN	
	default	0	
	IB-MGMT-VLAN	0	
	Native-VLAN	0	
	VM-Traffic-VLAN	0	
✓	vMotion-VLAN	۲	
MAC Pool : MAC_P QoS Policy : <a href="https://www.controlPolicy">MAC_P</a> QoS Policy : <a href="https://www.controlPolicy">cont set</a> Vertificates Threshold Policy : <a href="https://www.controlPolicy">default</a> Connection Policies	ool_B(32/32) CDP		
Dynamic vNIC usNIC VN Dynamic vNIC Connection Policy	IQ : <not set=""> V</not>	ок	Cancel

? ×

17. Click OK to create the vNIC template.

18. Click OK.

### Create VM Traffic vNICs

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

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

Create	vNIC	Template
--------	------	----------

? ×

Name : vNIC_VM_A			
Description :			
Fabric ID :  Fabric / Redundancy	A 🔘 Fabric B 📃 Enable F	ailover	
Redundancy Type : No	Redundancy   Primary Temp	late 🔾 Secondary Template	
<pre>Peer Redundancy Template . <not pre="" s<=""></not></pre>	et> 🔻		
Target Adapter VM VM			
Warning If VM is selected, a port profile by the s If a port profile of the same name exists	ame name will be created. ; and updating template is sel	ected, it will be overwritten	
Template Type : Initial Tem	blate <ul> <li>Updating Template</li> </ul>		
🏹 Advanced Filter 🔺 Export 👘 Pri	nt		\$
Select	Name	Native VLAN	
	default	0	
	IB-MGMT-VLAN	0	
	Native-VLAN	0	
		ок	Cancel

- 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.

VLANs

Select	Name	Native VLAN	
	default	0	
	IB-MGMT-VLAN	0	
	Native-VLAN	0	
$\checkmark$	VM-Traffic-VLAN	0	
	vMotion-VLAN	0	
C Pool : M/ S Policy : <n twork Control Policy : En Group : <nc ats Threshold Policy : de connection Policies</nc </n 	AC_Pool_A(32/32)   ot set> able_CDP fault		
Dynamic vNIC () usNIC ()     vynamic vNIC Connection P	○ VMQ olicy : <a href="https://www.set&gt;">&gt;&gt;&gt;&gt;"&gt;&gt;&gt;&gt;"&gt;&gt;&gt;&gt;"&gt;&gt;&gt;&gt;"&gt;&gt;&gt;&gt;&gt;"&gt;&gt;&gt;&gt;&gt;"&gt;&gt;&gt;&gt;"&gt;&gt;&gt;&gt;</a>		

? ×

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

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

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

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

? ×

Name :	vNIC_VM_B		
Description :			
Fabric ID : Redundancy	○ Fabric A  ● Fabric B  En En	able Failover	
Redundancy Type	: ON Redundancy OPrimary	Template      Secondary Template	
Peer Redundancy Temp	late : <not set=""> V</not>		
Target	<not set=""></not>		
Adapter	Domain Policies		
VM	vNIC_Mgmt_A		
	vNIC_VM_A		
	vNIC_vMotion_A		
Warning			
If <b>VM</b> is selected, a port p If a port profile of the sam	rofile by the same name will be create the name exists, and updating template	ed. is selected, it will be overwritten	
Template Type :	<ul> <li>Initial Template          <ul> <li>Updating Temp</li> </ul> </li> </ul>	blate	
VLANs			
Ty Advanced Filter	Export 🖷 Print		¢
Select	Name	Native VLAN	
	default	0	
	IB-MGMT-VLAN	0	
	Native-VLAN	0	
		ок	Cancel

11. Select Updating Template as the template type.

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

VLANs

Select	Name	Native VLAN	
	default	0	
	IB-MGMT-VLAN	0	
	Native-VLAN	0	
$\checkmark$	VM-Traffic-VLAN	0	
	vMotion-VLAN	0	
AC Pool : oS Policy : etwork Control Policy : n Group : tats Threshold Policy : Connection Policies	MAC_Pool_B(32/32)   cnot set>  cnable_CDP  not set>  finable_		
Dynamic vNIC usNIC Dynamic vNIC Connection	○ VMQ Policy : <a href="https://www.enditeduction.org"></a>		

? ×

- 18. Click OK to create the vNIC template.
- 19. Click OK.

## Create LAN Connectivity Policy

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

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

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

• / `
1

OK Cancel

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

Create vNI	С		? ×
Name : 01-Mgmt	-В		
Use vNIC Template	e: 🗹		
Redundancy Pair :		Peer Name :	
vNIC Template :	<not set=""> 🔻</not>	Create vNIC Template	
Adaptor Dorfor	<not set=""></not>		1
Adapter Periori	Domain Policies		
Adapter Policy	vNIC_Mgmt_A	Create Ethernet Adapter Policy	
	vNIC_Mgmt_B		
	vNIC_VM_A		
	vNIC_VM_B		
	vNIC_vMotion_A		
	vNIC_vMotion_B		



- 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 vN	С	?	$\times$
Name : 02-vMot	ion-A		
Use vNIC Templat	te : 🔽		
Redundancy Pair	: 🗆	Peer Name :	
vNIC Template :	<not set=""> 🔻</not>	Create vNIC Template	
Adapter Perfor	<not set=""></not>		
Adapter Perform	Domain Policies		
Adapter Policy	vNIC_Mgmt_A	Create Ethernet Adapter Policy	
	vNIC_Mgmt_B		
	vNIC_VM_A		
	vNIC_VM_B		
	vNIC_vMotion_A		
	vNIC_vMotion_B		



- 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.





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

Create vN	IC		? ×
Name : 04-VM-	A		
Use vNIC Templa	te : 🗹		
Redundancy Pair	: 🗆	Peer Name :	
vNIC Template :	<not set=""> 🔻</not>	Create vNIC Template	
Adaptar Darfar	<not set=""></not>		
Adapter Perfori	Domain Policies	-	
Adapter Policy	vNIC_Mgmt_A	Create Ethernet Adapter Policy	
	vNIC_Mgmt_B		
	vNIC_VM_A		
	vNIC_VM_B		
	vNIC_vMotion_A		
	vNIC_vMotion_B		

ОК

Cancel

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

Create	vNIC	;			? ×
Name : 0	5-VM-B				
Use vNIC T	Femplate :				
Redundanc	cy Pair: [			Peer Name :	
vNIC Temp	olate : <	not set> 🔻		Create vNIC Template	
Adaptor D	Dorfor	<not set=""></not>			1
Adapter P	-erion -	Domain Policie	es		
Adapter F	Policy	vNIC_Mgmt_4	4	Create Ethernet Adapter Policy	
		vNIC_Mgmt_E	3		
		vNIC_VM_A			
		vNIC_VM_B			
		vNIC_vMotion	_A		
		vNIC_vMotion	_В		
	_				

OK Cancel

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

Create LAN Connectivi	ty Policy		? X
Name : Infra-LAN-Policy			
Description :			
Click Add to specify one or more vNICs the	hat the server should use to connect to th	e LAN.	
Name	MAC Address	Native VLAN	
vNIC 05-VM-B	Derived		1
vNIC 04-VM-A	Derived		
vNIC 03-vMotion-B	Derived		
vNIC 02-vMotion-A	Derived		
vNIC 01-Mgmt-B	Derived		
vNIC 00-Mamt-A	Derived	Modify	
⊕ Add iSCSI vNICs			

- 41. Click OK to create the LAN Connectivity Policy.
- 42. Click OK.

## Create Service Profile Template

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

OK

Cancel

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

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

5. Enter VM-Host-Infra-Fabric-A as the name of the service profile template. This service profile template is configured to boot from IBM Storwize V5030 Node 1 on fabric A.

### 6. Select the "Updating Template" option.

7. Under UUID, select UUID\_Pool as the UUID pool.

		Create Service Profile Template	? ×
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 the template and enter a description.	is
2	Storage Provisioning	Name : VM-Host-Infra-Frbric-A	
3	Networking	The template will be created in the following organization. Its name must be unique within this organization. Where : org-root	
•	SAN Connectivity	Type : Initial Template @ Updating Template	
5	Zoning	Specify how the UUID will be assigned to the server associated with the service generated by this template.	
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		
9	Maintenance Policy	Optionally enter a description for the profile. The description can contain information about when and where the service profile should be used.	
10	Server Assignment		
1	Operational Policies		
		Next> Hinish Canc	

8. Click Next.

Configure Storage Provisioning

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



2. Click Next.

### Configure Networking Options

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

		Create Service Profile Template					
0	Identify Service Profile Template	Optionally specify LAN configuration information.					
		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? ○ Simple ○ Expert ○ No vNICs ● Use Connectivity Policy					
5	Zoning	LAN Connectivity Policy : <a href="https://www.connectivityPolicy">create LAN Connectivity Policy</a>					
6	vNIC/vHBA Placement	Initiator Name Assignn					
7	vMedia Policy	Create IQN Suffix Pool					
8	Server Boot Order	<b>WARNING</b> : 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						
1	Operational Policies						
		< Prev Next > Finish	Cancel				

4. Click Next.

## Configure Storage Options

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

		Create Service Profile Template						
0	Identify Service Profile Template	Optionally specify disk policies and SAN configuration information.						
		How would you like to configure	SAN connectivity?					
2	Storage Provisioning	○ Simple ○ Expert ○ No vHBAs ④ Use Connectivity Policy						
3	Networking	SAN Connectivity Policy : Du	al-Fabric V	Create SAN Connectivity Policy				
0	SAN Connectivity	D	Domain Policies					
5	Zoning							
6	vNIC/vHBA Placement							
7	vMedia Policy							
8	Server Boot Order							
9	Maintenance Policy							
10	Server Assignment							
1	Operational Policies							
				< Prev	Next > Finish	Cancel		

- 3. Click Next.
- 4. Click Next on the Zoning Options page.

## Configure vNIC/HBA Placement

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

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

		Create Service Pro	ofile Templa	te			?	
1	Identify Service Profile	Specify how vNICs and vHBAs are placed on physical network adapters						
2	Template Storage Provisioning	vNIC/vHBA Placement specifies h in a server hardware configuration Select Placement: VM-Host	now vNICs and vHBAs n independent way. t-Infra	are placed on physical ne	etwork adapters (r ment Policy	nezzanine)		
3	Networking		Virtual Network Interfaces Policy (read only)					
4	SAN Connectivity	Name		Name	Order	Selection Preference Assigned Only		
5	Zoning	No data available	->> assign >>	vHBA Fabric-A	1			
6	vNIC/vHBA Placement		<< remove <<	vHBA Fabric-B vNIC 00-Mg	2 3			
7	vMedia Policy			vNIC 01-Mg	4			
8	Server Boot Order		I	white the system	▲ Move Up ↓	Move Down		
9	Maintenance Policy							
10	Server Assignment							
U	Operational Policies							
					< Prev	Next > Finish	Cancel	

### Configure vMedia Policy

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



3. Click Next.

## Configure Server Boot Order

1. Select Boot-Fabric-A for Boot Policy.
|                         |   | Create Service Profile Template  | ? ×           |
|-------------------------|---|--|---------------|
| 0                       | Identify Service Profile  | Optionally specify the boot policy for this service profile template.  |               |
|                         | Template  | Select a boot policy.  |               |
| 2                       | Storage Provisioning  | Boot Policy: Boot-fabric-A 🔻 Create Boot Policy  |               |
| 3                       | Networking  | Name     : Boot-fabric-A       Description     :   |               |
| •                       | SAN Connectivity  | Reboot on Boot Order Change : No<br>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/iSCSI) is determined by PCIe bus scan order.<br>If Enforce vNIC/vHBA/ISCSI Name is selected and the vNIC/vHBA/ISCSI does not exist, a config error will be reported.<br>If it is not selected the vNICe/vHBAs are selected if they evice, otherwise the vNIC/vHBA/ISCBI does not exist.  |               |
|                         |   | In this not selected, the whosp mans are selected in they exist, otherwise the whop man with the lowest hole bas scale order is used.  |               |
| 7                       | vMedia Policy   | Boot Order   |               |
| 7<br>8                  | vMedia Policy<br>Server Boot Order  | Boot Order         +       — Ty Advanced Filter <ul> <li>Print</li> </ul> Name       Order <li>VNIC/VHB</li> <li>Type</li> <li>WWN</li> <li>LUN Name</li> <li>Slot Numb</li> <li>Boot Path</li> <li>Desc</li>  | ¢             |
| 7<br>8<br>9             | vMedia Policy<br>Server Boot Order<br>Maintenance Policy  | Boot Order     +     -     Type     WWN     LUN Name     Slot Numb     Boot Name     Boot Path     Desc       CD/DVD     1   | ¢<br>cription |
| 7<br>8<br>9             | vMedia Policy Server Boot Order Maintenance Policy  | Boot Order<br>+ - Try Advanced Filter ↑ Export ♣ Print<br>Name Order ▲ vNIC/vHB Type WWN LUN Name Slot Numb Boot Name Boot Path Desc<br>CD/DVD 1<br>► San 2  | cription      |
| 7<br>8<br>9<br>10       | vMedia Policy Server Boot Order Maintenance Policy Server Assignment                                  | Boot Order<br>+ - TyAdvanced Filter ↑ Export ● Print<br>Name Order ▲ vNIC/vHB Type WWN LUN Name Slot Numb Boot Name Boot Path Desc<br>CD/DVD 1<br>▶ San 2  | ¢<br>cription |
| 7<br>8<br>9<br>10       | vMedia Policy<br>Server Boot Order<br>Maintenance Policy<br>Server Assignment<br>Operational Policies | Boot Order<br>+ - Try Advanced Filter ↑ Export ♣ Print<br>Name Order ▲ vNIC/vHB Type WWN LUN Name Slot Numb Boot Name Boot Path Desc<br>CD/DVD 1<br>> San 2  | Cription      |
| 7<br>8<br>9<br>10<br>11 | vMedia Policy<br>Server Boot Order<br>Maintenance Policy<br>Server Assignment<br>Operational Policies | Boot Order<br>+ - T Advanced Filter ↑ Export ♣ Print<br>Name Order • vNIC/VHB Type WWN LUN Name Slot Numb Boot Name Boot Path Desc<br>CD/DVD 1<br>► San 2  | Cription      |
| 7<br>9<br>10<br>11      | vMedia Policy Server Boot Order Maintenance Policy Server Assignment Operational Policies             | Boot Order          +       -       > Advanced Filter       • Export       • Print         Name       Order       •       vNIC/vHB       Type       WWN       LUN Name       Boot Name       Boot Path       Desc         CD/DVD       1       •       San       2       • | cription      |
| 7<br>8<br>9<br>10<br>11 | vMedia Policy<br>Server Boot Order<br>Maintenance Policy<br>Server Assignment<br>Operational Policies | Boot Order          +       -       > Advanced Filter <ul> <li>Export</li> <li>Print</li> <li>Name</li> <li>Order</li> <li>VNIC/VHB</li> <li>Type</li> <li>WWN</li> <li>LUN Name</li> <li>Slot Numb</li> <li>Boot Name</li> <li>Boot Path</li> <li>Desc</li> <li>CD/DVD</li> <li>San</li> <li>San</li> <li>Sat Uah</li> <li>Boot Parameters</li> <li>Sat Uah</li> <li>Boot Parameters</li> </ul>   | Cription      |

2. Click Next to continue to the next section.

# Configure Maintenance Policy

1. Change the Maintenance Policy to default.

		Create Service Profile Template	? ×
0	Identify Service Profile Template	Specify how disruptive changes such as reboots, network interruptions, and firmware upgrades should be applied to the server associated wit service profile.	th this
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: Select (no policy used by default)  Create Maintenance Policy	
0	SAN Connectivity	Select (no policy used by default) Domain Policies	
6	Zoning	default	
6	vNIC/vHBA Placement	No maintenance policy is selected by default. The service profile will immediately reboot when disruptive changes are applied.	
0	vMedia Policy		
8	Server Boot Order		
9	Maintenance Policy		
10	Server Assignment		
0	Operational Policies		
		< Prev Next > Finish Cance	8

2. Click Next.

### Configure Server Assignment

To configure server assignment, complete the following steps:

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

		Create Service Profile Template	? ×
0	Identify Service Profile	Optionally specify a server pool for this service profile template.	
	Template	You can select a server pool you want to associate with 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	Op Down	
5	Zoning	The service profile template will be associated with one of the servers in the selected pool.	from
6	vNIC/vHBA Placement	the list. Server Pool Qualification : <a href="https://www.server.edu/server.e&lt;/th&gt;&lt;th&gt;mon&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;7&lt;/th&gt;&lt;th&gt;vMedia Policy&lt;/th&gt;&lt;th&gt;Restrict Migration : &lt;a href=" https:="" www.example.com"="">com set&gt;</a>	
8	Server Boot Order	Firmware Managem     Domain Policies     UCSB-B200-M4     International Adapter)	
9	Maintenance Policy	all-chassis	
10	Server Assignment		
1	Operational Policies		
		< Prev Next > Finish Can	icel

6. Click Next.

### Configure Operational Policies

To configure the operational policies, complete the following steps:

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

		Create Service Profile Template	? ×
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-Infra 🔻	
•	SAN Connectivity	External IPMI 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 : default  Create Power Control Policy ont set>	
10	Server Assignment	Scrub Policy     Domain Policies	
1	Operational Policies	KVM Managem     default	
		< Prev Next >	Finish Cancel

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

### **Create Service Profiles**

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

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

Create Service Profiles F	rom Template 🛛 ? ×
Naming Prefix : VM-Host-Infra-0	
Name Suffix Starting Number : 1	
Number of Instances : 2	
	OK Cancel

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

### Backup the Cisco UCS Manager Configuration

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

http://www.cisco.com/c/en/us/td/docs/unified\_computing/ucs/ucs-manager/GUI-User-Guides/Admin-Management/3 1/b\_Cisco\_UCS\_Admin\_Mgmt\_Guide\_3\_1/b\_Cisco\_UCS\_Admin\_Mgmt\_Guide\_3\_1\_chapter\_01001.ht ml

### Adding Servers

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

### Gather Necessary WWPN Information

After the Cisco UCS service profiles have been created, each infrastructure blade in the environment will have a unique configuration. To proceed with the SAN-BOOT deployment, specific information must be gathered from each Cisco UCS blade and from the IBM controllers. Insert the required information in the table below.

1. To gather the vHBA WWPN information, launch the Cisco UCS Manager GUI. In the navigation pane, click the Servers tab. Expand Servers > Service Profiles > root. Click each service profile and click Storage and select vHBAs from the panel right side.

	Hermon	13031 VIVIOS	Boot Order	VIItual Ivid	runes roz	ones Policies	Server Details	CINC Sessions	FSIVI	VIE
torage Profiles	Local Disk Configurati	ion Policy	HBAs vi	IBA Initiator Gro	ups					
		Local Disk	Policy	: SAN-Boot						
		Local Disk	Policy Instand	e: org-root/loo	cal-disk-config-	SAN-Boot				
		SAN Conne	ectivity Policy	1						
		SAN Conn	ectivity Policy	: D	al-Fabric					
		0/11/00/11	socivity i olicy							
		SAN Conn	ectivity Policy	Instance : org-	root/san-conn-p	ool-Dual-Fabric				
		SAN Conn Create SAN	ectivity Policy Connectivity	Instance : org-	root/san-conn-p	ool-Dual-Fabric				
		SAN Conn Create SAN	ectivity Policy Connectivity	Instance : org- Policy	root/san-conn-p	ool-Dual-Fabric				
Configuration C	hange of vNICs/vHBAs/l	SAN Conn Create SAN SCSI vNICs is a	ectivity Policy Connectivity	Instance : org- Policy	root/san-conn-p policy.	ool-Dual-Fabric				
Configuration C	hange of vNICs/vHBAs/i	SAN Conn Create SAN SCSI vNICs is a	ectivity Policy Connectivity	Instance : org- Policy	root/san-conn-r	ool-Dual-Fabric				
Configuration C IBAs	hange of vNICs/vHBAs/i	SAN Conn Create SAN SCSI vNICs is a	ectivity Policy Connectivity	Instance : org- Policy	root/san-conn-p	ool-Dual-Fabric				4
Configuration C IBAs & Advanced Filter Name	n The Export Print	SAN Conn Create SAN SCSI vNICs is a Desir	ectivity Policy Connectivity Illowed due t	Instance : org- Policy o connectivity (	root/san-conn-policy.	Desired Place	Actual Placem	Admin Host Port	Actual Hos	st Poi
Configuration C IBAs Advanced Filter Name vHBA Fabri	hange of vNICs/vHBAs/line r	SAN Conn Create SAN SCSI vNICs is a Desir	ectivity Policy Connectivity Illowed due t	Actual Order	root/san-conn-p policy. Fabric ID A	Desired Place	Actual Placem	Admin Host Port ANY	Actual Hos	st Po
Configuration C IBAs Advanced Filter Name vHBA Fabri vHBA Fabri	Thange of vNICs/vHBAs/R           r         Export         Print           WWPN         20:00:00:25:85:01:0A:2         20:00:00:25:85:01:0B:2	SAN Conn Create SAN SCSI vNICs is a Desir 2F 1 2F 2	ectivity Policy Connectivity Illowed due t	Actual Order 4.	Fabric ID A B	Desired Place 1	Actual Placern 1	Admin Host Port ANY ANY	Actual Hos 1 2	st Por

2. Record the WWPN information that is displayed for both the Fabric A vHBA and the Fabric B vHBA for each service profile into the WWPN variable table provided.

#### Table 15 ESXi Hosts – WWPN Information

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

# Storage LUN Mapping

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

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

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

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

骨 VersaStack_V5030 > Monitoring > <b>System</b>	IBM Storwize V5000	superuser (Security Administra
Actions 🛛		
E		
Hosts		
Ports by Host		
Volumes by Host		
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	FIT IT IT AN	
7.24 TIB		18.12 TIB
Allocated	15.00 TIB	Volume Capacity 1.2 : 1 Over Brevisioned
	System	Over Friendeld
Allocated - 7 A TID / 1 C AN TID / 1 C AN TID / 1 C AN TID / 4 CAN		Health Status

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

🗥 Versa	aStack_V5030 > Hosts > <b>Hosts</b> IBM Storwize V5000	
	Add Host E Actions Filter	
	Add Host Type I do Porte	×
	Host connections: O Fibre Channel	
	Name:	
	Host port (WWPN): No candidate ports found	
	▶ Advanced	
21	Add Cancel	
3 0		

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

- 5. For Fibre Channel Ports open the drop-down menu and select or input the WWPN's for the Fabric-A path vHBA's, <<var\_wwpn\_VM-Host-infra-01-a>>, and click Add Port to List.
- 6. Click the drop-down menu again, and select or Input the **WWPN's for the Fabric**-B path, <<wwpn\_VM-Host-infra-01-b>>, and click add port to list.
- 7. Leave Advanced Settings as default (as below) and click Add Host, then click Close.

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

Н	ost connections: <a>isin bre Channel</a> <ul> <li>iSCSI</li> </ul>
Name:	VM-Host-Infra-01
Host port (WWPN):	2000025B5010A2F 🗨 🕀 🝚
	2000025B5010B2F C - 🕀 👄
Host type:	Generic
I/O groups:	All

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

12. Select the B port by selecting the var for the Fabric-B path, <<wwpn\_VM-Host-infra-02-b>>, and click Add Port To List. Leave the Advanced Settings as default and click Add Host, then click Close.

Add Host		Х
Но	st connections: <ul> <li>Fibre Channel</li> <li>iSCSI</li> </ul>	
Name:	VM-Host-Infra-02	
Host port (WWPN):	2000025B5010A3F	
	2000025B5010B3F C - 0	
Host type:	Generic	
I/O groups:	All	
	Add Cancel	

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



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

#### ☆ VersaStack\_V5030 > Volumes > Volumes

lame	State	Pool	UID	Host Mappings	Capacity
VM-Host-Infra-01			600507638081001EE800000000000002	No	📵 40.00 GiB
VM-Host-Infra-02	Rename		600507638081001EE80000000000003	No	40.00 GiB
infra_datastore_01	Map to Host		600507638081001EE80000000000004	No	📵 500.00 GiB
infra_datastore_02	Shrink		600507638081001EE800000000000005	No	📵 500.00 GiB
infra_swap	Expand		600507638081001EE80000000000000	No	📵 100.00 GiB
	Modify Capacity Savings				
	Modify Mirror Sync Rate				
	Cache Mode				
	Modify Open VMS UDID				
	Unmap All Hosts				
	View Mapped Hosts				
	Modify I/O Group				
	Space Savings	•			
	Migrate to Another Pool				
	Export to Image Mode				
	Duplicate				
	Add Volume Copy				
	Enable Access to Stale Copy	y			
	Delete				
	Properties				
	Volume Copy Properties				

IBM Storwize V5000

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

☆ Versa	iStack_V5030 > Volumes > <b>Volum</b>	es		IBM Storwize	V5000			
	+ Create Volumes 🗄 Actions	Q Filter						
	Name	State	Pool	UID	Host Mapping	js Capac	ity	
	VM-Host-Infra-01	✓ Online	Pool0	600507638081001EE80000000	000002	No (	40.00 GiB	
	VM-Host-Infra-02	✓ Online	Pool0	600507638081001EE80000000	000003	No (	40.00 GiB	
	infra_datastore_01	✓ Online	Pool0	600507638081001EE80000000	0000004	No 📵	500.00 GiB	
	infra_datastore_02	✓ Online	Pool0	600507638081001EE80000000	000005	No 📵	500.00 GiB	
	infra_swap	✓ Online	Pool0	600507638081001EE80000000	000006	No 🕞	100.00 GiB	
9 1 1 1 1				Map Volume VM-Host-Infra-01 to Ho Select the Host: Select VM-Host-Infra-01 VM-Host-Infra-02	ost Cancel	x		

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

- 17. Right-click the volume VM-Host-Infra-02 and click Map to host.
- 18. In the drop-down, select VM-Host-Infra-02.

Map Volume VM-Host-Infra-02 to Host	×
Select the Host:	
VM-Host-Infra-02	
Map Cancel	

- 19. Click Map and then click Close on the *Modify Mappings* dialogue box
- 20. Map the volumes Infra\_datastore\_1 and infra\_swap to the ESXi servers following the steps specified above.
- 21. Right-click while the volumes infra\_datastore\_1 and infra\_swap are selected.
- 22. In the drop-down, select VM-Host-Infra-01 and VM-Host-Infra-02.

Map 2 Volumes to Host	×
Select the Host:	
VM-Host-Infra-01,VM-Host-Infra-02	
Map Cancel	

# VMware vSphere Installation and Setup

# VersaStack VMware ESXi 6.0 Update 2 SAN Boot Installation

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

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

To download the Custom ESX ISO:

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

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

### Log in to Cisco UCS 6324 Fabric Interconnect

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

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

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

	All	•	Servers / Servi	ce Profiles	/ root / Sen	rice Profile VM-I	Host-Infra					
Equipment	<ul> <li>Servers</li> </ul>		General	Storage	Network	iSCSI vNICs	Boot Order	Virtual Machines	FC Zones	Policies	Server Details	CIMC S
	<ul> <li>Service Profiles</li> </ul>	3	Fault Summar	v			Properties					
U	🔻 root 🕚			,								
Servers	<ul> <li>VM-Host</li> </ul>	Infra-01			≙	$\odot$				WARN	IING	
品	iSCSI v	Shutdown Server		)	0	0		Thi	s service profile	e is not modif	iable because it is b	ound to
LAN	▼ vHBAs	Reset						To mo	the service dify this service	e profile templ e profile, plea	ate VM-Host-Infra se unbind it from th	e template
	► vHBA	KVM Console					Nome					
<b>E</b>	► vHBA	SSH to CIMC for SoL		юк			Name	: VM-H	ost-Infra-UI			
SAN	▶ vNICs	Rename Service Profile		ils			User Label	·				
	N/M_Host	Create a Clone					Description	:				
9	► VIVI-HOSI-						Owner	: Local				
VM	Sub-Orga	Disassociate Service Pro	ofile				Unique Identifier	: 36201	36a-e47e-11	e0-0000-000	00000000f	
A	<ul> <li>Service Profile</li> </ul>	Change Service Profile	Association	State			UUID Pool	: UUID	Pool			
	Policies	Accession with Server D					UUID Pool Instan	ce : org-ro	ot/uuid-pool-l	JUID_Pool		
Storage	Pools	Associate with Server P	001				Associated Serve	er : sys/ch	assis-1/blade-	-2		
	<ul> <li>Schedules</li> </ul>	HIDD TO 2 LOMPISTO	Reset				Service Profile To	emplate : VM-H	ost-Infra	1.7		

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

#### VMware ESXi Installation

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

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

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

• • •	Virtual Media - Map CD/DVD
Drive/Image File:	Custom-Cisco-6.0.2.1.iso  Browse
	✓ Read Only
	Map Device Cancel

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

### Install ESXi on the Servers

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

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

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

### Set Up Management Networking for ESXi Hosts

Adding a management network for each VMware host is necessary for managing the host. To add a management network for the VMware hosts, complete the following steps on each ESXi host in the following section.

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

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

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

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

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

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

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

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

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

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

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

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

#### Download VMware vSphere Client

To download the VMware vSphere Client and install Remote CLI, complete the following steps:

- 1. Open a web browser on the management workstation and navigate to the VM-Host-Infra-01 management IP address.
- 2. Download and install the vSphere Client for Windows.

### Download VMware vSphere CLI

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

1. Click the following link:

https://my.vmware.com/web/vmware/details?downloadGroup=VCLI60U2&productId=491

- 2. Select your OS and Click Download.
- 3. Save it to destination folder.
- 4. Run the VMware-vSphere-CLI-xxxx.exe.
- 5. Click Next.
- 6. Accept the terms for the license and click Next.
- 7. Click Next on the Destination Folder screen.
- 8. Click install and Finish.

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

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

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

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

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

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

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

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

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

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

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

fnic Driver version 1.6.0.28 enic Driver version 2.3.0.10

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

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

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

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

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

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

reboot

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

#### Map Required VMFS Datastores

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

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

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

Setting Started Summary Virtual Machines Resource Allocation Performance Configuration Users Events Permissions								
Hardware	View: Datastores Dev	ices						
Health Status	Datastores							Refresh
Processors	Identification	Device	Drive Type	Capacity	Free	Туре	Last Update	Hardware Ac
Memory	datastore1	IBM Fibre Channel	Non-SSD	2.50 GB	1.92 GB	VMF55	2/22/2016 3:21:54 PM	Supported
<ul> <li>Storage</li> </ul>	infra-datastore-1	IBM Fibre Channel	Non-SSD	499.75 GB	498.80 GB	VMFS5	2/22/2016 5:58:55 PM	Supported
Networking	infra-swap	IBM Fibre Channel	Non-SSD	99.75 GB	98.80 GB	VMFS5	2/22/2016 3:21:54 PM	Supported
Storage Adapters								
Network Adapters								

### Configure NTP on ESXi Hosts

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

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

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

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

### Move VM Swap File Location

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

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

🖁 Virtual Machine Swapfile Loca	ition			×
Swapfile Location C Store the swapfile in the same This is a recommended option.	directory as the	virtual machine.		
Store the swapfile in a swapfile <u>A</u> This option could degrade	e datastore select vMotion performa	ted below. ance for the affe	cted virtual m	achines.
Name	Capacity	Provisioned	Free	Туре
[infra_swap]	99.75 GB	41.30 GB	58.45 GB	VMFS

# VersaStack VMware vCenter 6.0U2

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

### Install the Client Integration Plug-In

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

- 1. Download the .iso installer for the version 6.0U2 vCenter Server Appliance and Client Integration Plug-in.
- 2. Mount the ISO image on the management station.
- 3. In the software installer directory, navigate to the vcsa directory and double-click VMware-ClientIntegrationPlugin-6.0.0.exe. The Client Integration Plug-in installation wizard appears.



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

# Building the VMware vCenter Server Appliance

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

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

2 Connect to target server       Index to a notioning netrice agreement of the end of the proceeding.         3 Set up virtual machine       VMWARE END USER LICENSE AGREEMENT         4 Select deployment type       PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR         5 Set up Single Sign-on       Site         5 Single Sign-on Site       INPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE         8 Select datastore       MPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUINARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUINARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUINARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUINARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUINARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUINARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUINARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUINARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUINARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUINARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUINARE TO THE VENDOR THE VENDO	End User License Agreement	End User License Agreement Please read the following license agreement before proceeding
Set up virtual machine       VMWARE END USER LICENSE AGREEMENT         Select deployment type       PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.         Select appliance size       Select datastore         Configure database       IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE: AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUIR AREFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.         1 Customer Experience       EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, Your use of the Software only permitted in a non-production environment and for the period limited by the License Key. Notwithstand any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.         1. DEFINITIONS.       1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly control by is under common control with or controls that narty and here "control" means an ownership. voting or any other section and there "control" means an ownership. voting or any other section and there "control" means an ownership. voting or any other section and there "control" means an ownereship. voting or any other section any oth	Connect to target server	
Select deployment type         Set up Single Sign-on         Single Sign-on Site         Select appliance size         Select datastore         Configure database         0 Network Settings         1 Customer Experience         nprovement Program         2 Ready to complete         L1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly control         1. DEFINITION S.	Set up virtual machine	VMWARE END USER LICENSE AGREEMENT
Set up Single Sign-on       USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.         Select appliance size       IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ('EULA'). IF YOU DO NOT AGREE TO THE TERMS OF THIS END USER LICENSE AGREEMENT ('EULA'). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUINT A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.         EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, Your use of the Software only permitted in a non-production environment and for the period limited by the License Key. Notwithstand any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.         1. DEFINITIONS.       1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly control by is under common control with, or controls that nativ, and here "control" means an ownership, voting or 4	Select deployment type	DI EASE NOTE THAT THE TERMS OF THIS END LISED LICENSE AGREEMENT SHALL GOVERN YOUR
ingle Sign-on Site       IN STALLATION OF THE SOFTWARE.         elect appliance size       IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE         elect datastore       AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT         onfigure database       SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUIND A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.         Customer Experience       EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, Your use of the Software only permitted in a non-production environment and for the period limited by the License Key. Notwithstand any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.         1. DEFINITIONS.       1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly control by is under common control with or controls that party and here "control" means an ownership, voting or indirectly controls.	et up Single Sign-on	USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE
elect appliance size       IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUINA REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.         Customer Experience       EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, Your use of the Software only permitted in a non-production environment and for the period limited by the License Key. Notwithstand any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.         1. DEFINITIONS.       1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly control by is under common control with or controls that narty and here "control" means an ownership, voting or software is provided "AS-IS".	ingle Sign-on Site	INSTALLATION OF THE SOFTWARE.
elect datastore       INDMIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE         onfigure database       AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT         DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED         SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUINA REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.         Customer Experience       EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, Your use of the Software only permitted in a non-production environment and for the period limited by the License Key. Notwithstand any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.         1. DEFINITIONS.       1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly control by is under common control with or controls that party and here "control" means an ownership wating or software is provided to means an ownership wating or software is party and here "control" means an ownership wating or software is party and here "control" means an ownership wating or software is party and here "control" means an ownership wating or software is party and here "control" means an ownership wating or software is party and here "control" means an ownership wating or software is party and here "control" means an ownership wating or software is party and here "control" means an ownership wating or software is party and here "control" means an ownership wating or software is party and here "control" means an ownership wating or software is party and here "control" means an ownership wating or s	elect appliance size	IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE
onfigure database       DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED         Network Settings       SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUING A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.         Evaluation Difference       Evaluation Difference         rovement Program       Ready to complete         Ready to complete       I. DEFINITIONS.         1. The filiate?       The spect to a party at a given time, an entity that then is directly or indirectly controls	elect datastore	AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO BE BOOND BY THE TERMS OF THIS END USER LICENSE
Vetwork Settings         Customer Experience         rovement Program         Ready to complete         EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, Your use of the Software only permitted in a non-production environment and for the period limited by the License Key. Notwithstand any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.         1. DEFINITION S.         1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly control by is under common control with or controls that party and here "control" means an ownership voting or detection.	onfigure database	DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST
<ul> <li>EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, Your use of the Software only permitted in a non-production environment and for the period limited by the License Key. Notwithstand any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.</li> <li>1. DEFINITION S.</li> <li>1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly control by is under common control with or controls that party and here "control" means an ownership voting or it.</li> </ul>	letwork Settings	A REFUND OF THE LICENSE FEE, IF ANY, THAT YOU PAID FOR THE SOFTWARE.
<ul> <li>only permitted in a non-production environment and for the period limited by the License Key. Notwithstand any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.</li> <li>1. DEFINITION S.</li> <li>1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly control with or controls that party and here "control" means an ownership voting or it.</li> </ul>	Customer Experience	EVALUATION LICENSE. If You are licensing the Software for evaluation purposes, Your use of the Software is
<ul> <li>1. DEFINITION S.</li> <li>1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly control by is under common control with or controls that party and here "control" means an ownership, voting or </li> </ul>	ovement Program	only permitted in a non-production environment and for the period limited by the License Key. Notwithstanding any other provision in this EULA, an Evaluation License of the Software is provided "AS-IS" without indemnification, support or warranty of any kind, expressed or implied.
<b>1.1 "Affiliate"</b> means, with respect to a party at a given time, an entity that then is directly or indirectly control by is under common control with or controls that party and here "control" means an ownership, voting or	Ready to complete	1. DEFINITION S.
		1.1 "Affiliate" means, with respect to a party at a given time, an entity that then is directly or indirectly controlled by is under common control with or controls that party and here "control" means an ownership voting or
✓ I accept the terms of the license agreement.		✓ I accept the terms of the license agreement.

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

VMware vCenter Server Applianc	e Deployment		
<ul> <li>1 End User License Agreement</li> <li>2 Connect to target server</li> </ul>	Connect to target server Specify the ESXi host or vCenter	Server on which to deploy the vCenter S	erver Appliance.
3 Set up virtual machine	FQDN or IP Address:	192.168.162.102	]
4 Select deployment type 5 Set up Single Sign-on	User name:	root	] 0
6 Single Sign-on Site 7 Select appliance size	Password:	I	]
<ul> <li>8 Select datastore</li> <li>9 Configure database</li> <li>10 Network Settings</li> <li>11 Customer Experience</li> <li>Improvement Program</li> <li>12 Ready to complete</li> </ul>	<ul> <li>Before proceeding, if the tar</li> <li>Make sure the ESXi host</li> <li>When deploying to a vSp portgroup. After deployment</li> </ul>	get is an ESXi host: is not in lock down mode or maintenance here Distributed Switch (VDS), the applia ent, it can be moved to a static or dynamic	mode. nce must be deployed to an ephemeral ; portgroup.
		Back	Next Finish Cancel

- 6. Click Yes to accept the certificate.
- 7. On the Set up virtual machine screen, enter the vCenter Server Appliance name, set the password for the root user, and click Next.

Mware vCenter Server Appliance Deployment					
<ul> <li>✓ 1 End User License Agreement</li> <li>✓ 2 Connect to target server</li> </ul>	Set up virtual machine Specify virtual machine settings	s for the vCenter Server Appliance to t	be deployed.		
3 Set up virtual machine 4 Select deployment type	Appliance name:	vCenter	0		
5 Set up Single Sign-on	OS user name:	root			
6 Single Sign-on Site 7 Select appliance size	OS password:		0		
8 Select datastore 9 Configure database	Confirm OS password:	•••••			
10 Network Settings 11 Customer Experience					
Improvement Program 12 Ready to complete					
		Back	Next Finish	Cancel	

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

<ul> <li>1 End User License Agreement</li> <li>2 Connect to target server</li> </ul>	Select deployment type Select the services to deploy onto this appliance.					
<ul> <li>3 Set up virtual machine</li> <li>4 Select deployment type</li> <li>5 Set up Single Sign-on</li> <li>6 Single Sign-on Site</li> <li>7 Select appliance size</li> <li>8 Select datastore</li> <li>9 Configure database</li> <li>10 Network Settings</li> <li>11 Ready to complete</li> </ul>	vCenter Server 6.0 requires a Platform Services Controller, which contains shared services such as Single Sign-On, Licensing, and Certificate Management. An embedded Platform Services Controller is deployed on the same Appliance VM as vCenter Server. An external Platform Services Controller is deployed in a separate Appliance VM. For smaller installations, consider vCenter Server with an embedded Platform Services Controller. For larger installations with multiple vCenter Servers, consider one or more external Platform Services Controllers. Refer to the vCenter Server documentation for more information. Note: Once you install vCenter Server, you can only change from an embedded to an external Platform Services Controller with a fresh install. <b>Embedded Platform Services Controller</b> Install vCenter Server with an Embedded Platform Services Controller					
	External Platform Services Controller O Install Platform Services Controller Install vCenter Server (Requires External Platform Services Controller) VM or Host VM or Host VCenter Server VM or Host VCenter Server					

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

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

S VMware vCenter Server Appliance Deployment					
<ul> <li>✓ 1 End User License Agreement</li> <li>✓ 2 Connect to target server</li> </ul>	Set up Single Sign-on (SSO) Create or join a SSO domain. An	ISSO configuration cannot be changed afte	er deployment.		
<ul> <li>3 Set up virtual machine</li> <li>4 Select deployment type</li> </ul>	<ul> <li>Create a new SSO domain</li> <li>Join an SSO domain in an ex</li> </ul>	isting vCenter 6.0 platform services control	ler		
5 Set up Single Sign-on 6 Select appliance size	vCenter SSO User name:	administrator			
7 Select datastore	vCenter SSO Password:		0		
8 Configure database 9 Network Settings	Confirm password:	••••••	]		
10 Customer Experience Improvement Program	SSO Domain name:	vsphere.local	0		
11 Ready to complete	SSO Site name:	VersaStack	0		
	▲ Before proceeding, make Active Directory domain name.	sure that the vCenter Single Sign-On doma	ain name used is different than your		
		Back	Next Finish Cancel		

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

End User License Agreement	Select appliance size Specify a deployment size	for the new appliance
<ul> <li>2 Connect to target server</li> <li>3 Set up virtual machine</li> <li>4 Select deployment type</li> <li>5 Set up Single Sign-on</li> <li>6 Select appliance size</li> <li>7 Select datastore</li> <li>8 Configure database</li> <li>9 Network Settings</li> <li>10 Customer Experience</li> <li>Improvement Program</li> <li>11 Ready to complete</li> </ul>	Appliance size: <b>Description:</b> This will deploy a Tiny V This option contains vCe	Tiny (up to 10 hosts, 100 VMs)         Tiny (up to 10 hosts, 1,000 VMs)         Small (up to 100 hosts, 1,000 VMs)         Medium (up to 400 hosts, 4,000 VMs)         Large (up to 1000 hosts, 10,000 VMs)         M configured with 2 vCPUs and 8 GB of memory and requires 120 GB of disk space.         Inter Server with an embedded Platform Services Controller.

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

Mware vCenter Server Appliance Deployment						
<ul> <li>1 End User License Agreement</li> <li>2 Connect to target server</li> <li>3 Set up virtual machine</li> <li>4 Select deployment type</li> </ul>	Select datastore Select the storage location for this deployment The following datastores are accessible. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.					
<ul> <li>✓ 5 Set up Single Sign-on</li> <li>✓ 6 Select appliance size</li> </ul>	Name	Туре	Capacity	Free	Provisioned	Thin Provisioning
7 Select datastore	infra_swap	VMFS	99.75 GB	57.29 GB	42.46 GB	true
8 Configure database	infra_datastor	VMFS	499.75 GB	266.08 GB	233.67 GB	true
9 Network Settings	datastore1	VMFS	32.5 GB	31.55 GB	0.95 GB	true
Improvement Program	infra_datastor	VMFS	499.75 GB	203.78 GB	295.97 GB	true
11 Ready to complete	Enable Thin Di	sk Mode 🚯				
				Back	Next Finish	Cancel

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

VMware vCenter Server Appliance Deployment			
<ul> <li>VMware vCenter Server Appliance</li> <li>1 End User License Agreement</li> <li>2 Connect to target server</li> <li>3 Set up virtual machine</li> <li>4 Select deployment type</li> <li>5 Set up Single Sign-on</li> <li>6 Select appliance size</li> <li>7 Select datastore</li> <li>8 Configure database</li> </ul>	e Deployment Configure database Configure the database for this deployment   Use an embedded database (PostgreSQL) Use Oracle database		
9 Network Settings 10 Customer Experience Improvement Program 11 Ready to complete			
	Back Next Finish Cancel		

### 14. In the "Network Settings" page, configure the below settings:

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

Mware vCenter Server Appliance Deployment			
1 End User License Agreement	Network Settings Configure network settings for this deployment.		
<ul> <li>✓ 3 Set up virtual machine</li> </ul>	Choose a network:	VM Network 🔻	0
4 Select deployment type			
✓ 5 Set up Single Sign-on	IP address family:	IPv4 v	
✓ 6 Select appliance size			
7 Select datastore	Network type:	static 🔹	
✓ 8 Configure database			
9 Network Settings	Network address:	192.168.162.100	
10 Customer Experience	System name (EODN or ID		
Improvement Program	address]:	vcenter.versastack.lab	0
11 Ready to complete	Subnet mask:	255.255.252.0	]
	Network gateway:	192.168.160.1	]
	Network DNS Servers (separated by commas)	192.168.162.50	]
	Configure time sync:	<ul> <li>Synchronize appliance time with ESXi</li> <li>Use NTP servers (Separated by comr</li> </ul>	host mas)
		Back	Next Finish Cancel

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

T VMware vCenter Server Appliance Deployment		
✓ 1 End User License Agreement	Ready to complete Please review your set	ings before starting the installation.
<ul> <li>2 Connect to target server</li> <li>3 Set up virtual machine</li> <li>4 Select deployment type</li> <li>5 Set up Single Sign-on</li> <li>6 Select appliance size</li> <li>7 Select datastore</li> <li>8 Configure database</li> <li>9 Network Settings</li> <li>10 Customer Experience</li> <li>Improvement Program</li> <li>11 Ready to complete</li> </ul>	Target server info: Name: Installation type: Deployment type: Deployment configuration: Datastore: Disk mode: Network mapping: IP allocation: Host Name Time synchronization: Database: Properties:	192.168.162.101 VersaStack-vCenter Install Embedded Platform Services Controller Tiny (up to 10 hosts, 100 VMs) infra_datastore_2 thin Network 1 to VM Network IPv4 , static 192.168.160.254 embedded SSH enabled = True Customer Experience Improvement Program = Disabled SSO User name = administrator SSO Domain name = vsphere.local SSO Site name = versastack Network 1 IP address = 192.168.162.100 Host Name = vcenter.versastack.lab Network 1 netmask = 255.255.252.0 Default gateway = 192.168.160.1 DNS = 192.168.162.50
		Back Next Finish Cancel

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

## Set Up vCenter Server

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

- 1. Using a web browser, navigate to <a href="https://<<var\_vcenter\_ip/FQDN>>">https://<<var\_vcenter\_ip/FQDN>>">https://<<var\_vcenter\_ip/FQDN>>">https://<<var\_vcenter\_ip/FQDN>>">https://<<var\_vcenter\_ip/FQDN>>">https://<<var\_vcenter\_ip/FQDN>>">https://<<var\_vcenter\_ip/FQDN>>">https://<<var\_vcenter\_ip/FQDN>>">https://<<var\_vcenter\_ip/FQDN>>">https://<<var\_vcenter\_ip/FQDN>>">https://<<var\_vcenter\_ip/FQDN>>">https://<<var\_vcenter\_ip/FQDN>>">https://<<var\_vcenter\_ip/FQDN>>">https://<<var\_vcenter\_ip/FQDN>">https://<<var\_vcenter\_ip/FQDN>">https://<</a>
- 2. Click the link labeled Log in to vSphere Web Client.



3. If prompted, run the VMWare Remote Console Plug-in.



4. Log in as root, with the root password entered above in the vCenter installation.

5. Click Login.

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

To setup the vCenter Server, complete the following steps:

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



4. Rename the datacenter and click OK.

1 New Datacenter	r (? ) >>
Datacenter name:	VersaStack_DC
Location:	vcenter.versastack.lab
	OK Cancel

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



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

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

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

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

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

1 Add Host		() »
1 Name and location	Enter the name or IP addres	ss of the host to add to vCenter Server.
2 Connection settings	Host name or IP address:	VM-Host-Infra-01.versastack.lab
3 Host summary	Location:	UrsaStack_MGMT
4 Resource pool	Туре:	ESXI -
5 Ready to complete		
		Back Next Finish Cancel

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

<b>•</b> :	Add Host		?)	•
~	<ol> <li>Name and location</li> <li>Connection settings</li> <li>Host summary</li> <li>Resource pool</li> <li>Ready to complete</li> </ol>	Enter the administrative account information for the host. The vSphere Web Client will use this information to connect to the host and establish a permanent account for its operations. User name: root Password: ******		
		Back Next Finish Car	ncel	

- 11. Repeat this procedure to add other Hosts to the cluster.
- 12. In vSphere in the left pane right-click the cluster VersaStack\_MGMT, and click Rescan Storage.

• • • VSphere Web Client ×							
$\leftarrow \rightarrow \mathbb{C}$ A https://192.168.162.100/vsphere-client/?csp#extensionId%3Dvsphere.core.hos $\Rightarrow$ $\square$ $\square$ $\blacksquare$							
Apps 📄 CEC Indexes	🚞 Common Tools  🗎 Imported From	m Safari 🚞 Internal Support 📄 News 📄 Popular	»				
vmware <sup>®</sup> vSphere	Actions - VersaStack_MGMT Add Host	C Administrator@VSPHERE.LOCAL - I Help	<b>~</b> 1				
Navigator	New Virtual Machine						
	New vApp New Resource Pool	Monitor Manage Related Objects	A				
	Restore Resource Pool Tree	Vhen you add a sources become					
	Storage	New Datastore					
	Host Profiles	Rescan Storage Vi					
	Edit Default VM Compatibility	Resource					
	🛃 Assign License	ual SAN (VSAN)					
	Settings	, in the second s					
	Move To		😤 N				
	Rename		<b>•</b>				
	lags	Data					
	Add Permission	vSenter Server					
	X Delete						
	All vRealize Orchestrator plugin Action	s >					

## Configure ESXi Networking

To configure the ESXi networking, complete the following steps:

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

vmware <sup>®</sup> vSphere Web Cli	ent <del>n</del> ≘		U   Administrator@VSPHERE.LOCAL	
VmWare' vSphere Web Cli Navigator Home Versastacklab Versastack_DC Versastack_DC Versastack_MGMT Versastack_MGMT Versastack_MGMT Versastack_MGMT Versastack-Vcenter Versastack-vCenter	ent fills wm-host-infra-01.versastack. Getting Started Summary Mo Settings Networking Storage Virtual switches VMkernel adapters Physical adapters TCP/IP configuration Advanced	ab Actions ▼ nitor Manage Related Objects Alarm Definitions Tags Permissions Virtual switches Switch Switch	Uiscovered Issues	•   Help •
₩ VSM_primary		Standard switch: vSwitch0 (Management Net X    X    X    X    X    X    X	twork)	<b>Č</b> 

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

vm-host-infra-01.versastack.lab - N	lanage Physical Network Adapters f	or vSwitch0 ?
Assigned adapters:	All Properties CDP LLDP	
+ 🗙 🔒 🐥	Adapter	Cisco Systems
Active adapters		Inc Cisco VIC Ethernet NIC
vmnic0	Name	vmnic1 ::
Standby adapters	Location	PCI 0000:07:00.0
🛒 vmnic1	Driver	enic
Unused adapters	Status	
	Status	Connected
	Configured speed, Duplex	10000 Mb, Full Duplex
	Actual speed, Duplex	10000 Mb, Full Duplex
	Networks	192.168.160.191- 192.168.160.191 ( VLAN11 )
	DirectPath I/O	
	Status	Supported
		•
		OK Cancel

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

vm-host-infra-01.versastack.la	b - Add Networking	?
1 Select connection type	Select connection type Select a connection type to create.	
<ol> <li>Select target device</li> <li>Connection settings</li> <li>Port properties</li> <li>IPv4 settings</li> <li>Ready to complete</li> </ol>	VMkernel Network Adapter     The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, ISCSI,     NFS, FCGE, Fault Tolerance, Virtual SAN and host management.     Physical Network Adapter     A physical network adapter handles the network traffic to other hosts on the network.     Virtual Machine Port Group for a Standard Switch     A port group handles the virtual machine traffic on standard switch.	
	Back Next Finish	Cancel

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

Ē	☐ vm-host-infra-01.versastack.lab - Add Networking				
~	1 Select connection type 2 Select target device	Select target device Select a target device for the new connection.			
	<ul> <li>3 Create a Standard Switch</li> <li>4 Connection settings</li> <li>4a Port properties</li> <li>4b IPv4 settings</li> <li>5 Ready to complete</li> </ul>	Select an existing standard switch         VSwitch0         Browse			
		Back Next Finish Cancel			

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



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

Add Physical Adapters to the Switch						
Failover order group: Network Adapters:	Active adapters        Active adapters     •       All     Properties     CDP     LLDP					
vmnic3 vmnic4 vmnic5	Adapter Name Location Driver <b>Status</b>	Cisco Systems Inc Cisco VIC Ethernet NIC vmnic2 PCI 0000:08:00.0 enic				
		OK Cancel				

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



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

vm-host-infra-01.versastack.lab -	Add Networking					?
✓ 1 Select connection type	Create a Standard Switch	h			_	
✓ 2 Select target device	Add Physical Adapters	s to the Switch		X	) 	
<ul> <li>3 Create a Standard Switch</li> <li>4 Connection settings</li> <li>4a Port properties</li> <li>4b IPv4 settings</li> <li>5 Ready to complete</li> </ul>	Failover order group: Network Adapters: vmnic3 vmnic4 vmnic5	Standby adapters <ul> <li>Active adapters</li> <li>Standby adapters</li> <li>Unused adapters</li> <li>Adapter</li> </ul> <li>Adapter</li> <li>Name         <ul> <li>Location</li> <li>Driver</li> <li>Status</li> <li>Status</li> </ul> </li>	• LLDP	Cisco Systems Inc Cisco VIC Ethernet NIC vmnic3 PCI 0000:0e:00.0 enic Connected	rms Inc Cisco VIC Ethernet NIC 3:00.0 Full Duplex Full Duplex s	
		Cisco Disco	very Protoco	DK Cancel	ed Next Finish Ca	ncel

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



#### 12. Click Next.

vm-host-infra-01.versastack.lab -	Add Networking	?
<ul> <li>1 Select connection type</li> <li>2 Select torget device</li> </ul>	Port properties Specify VMkernel port settings.	
<ul> <li>2 Solicit larger derive</li> <li>3 Create a Standard Switch</li> <li>4 Connection settings</li> <li>4a Port properties</li> <li>4b IPv4 settings</li> <li>5 Ready to complete</li> </ul>	VMkernel port settings Network label: VLAN ID: IP settings:	VMkernel vMotion B173 • IPv4 •
	TCP/IP stack:	Default 🔹 🚺
	Available services	
	Enable services:	<ul> <li>✓ vMotion traffic</li> <li>Provisioning traffic</li> <li>Fault Tolerance logging</li> <li>Management traffic</li> <li>vSphere Replication traffic</li> <li>vSphere Replication NFC traffic</li> <li>Virtual SAN traffic</li> </ul>
		Back Next Finish Cancel

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

vm-host-infra-01.versastack.lab -	Add Networking			?
<ul> <li>1 Select connection type</li> <li>2 Select target device</li> </ul>	IPv4 settings Specify VMkernel IPv4 settings.			
<ul> <li>2 Select target device</li> <li>3 Create a Standard Switch</li> <li>4 Connection settings</li> <li>4a Port properties</li> <li>4b IPv4 settings</li> <li>5 Ready to complete</li> </ul>	Specify VMkernel IPv4 settings. Obtain IPv4 settings automatically Use static IPv4 settings IPv4 address: Subnet mask: Default gateway for IPv4: DNS server addresses:	172.17.73.11         255.255.255.0]         192.168.160.1         192.168.162.50		
			Back Next	Finish Cancel

14. Enter <<var\_vm\_host\_infra\_vmotion\_01\_ip>> in the filed for IPv4 address, and <<var\_vmotion\_subnet\_mask>> for the Subnet mask. Click Next.

vm-host-infra-01.versastack.lab -	Add Networking		?
<ul> <li>1 Select connection type</li> <li>2 Select target device</li> </ul>	Ready to complete Review your settings selections before	e finishing the wizard.	
<ul> <li>2 Select target device</li> <li>3 Create a Standard Switch</li> <li>4 Connection settings</li> <li>4a Port properties</li> <li>4b IPv4 settings</li> <li>5 Ready to complete</li> </ul>	Review your settings selections before New standard switch: Assigned adapters: New port group: VLAN ID: TCP/IP stack: vMotion traffic: Provisioning traffic: Fault Tolerance logging: Management traffic: vSphere Replication traffic: vSphere Replication NFC traffic: Virtual SAN traffic: IPv4 settings IPv4 address: Subnet mask:	e finishing the wizard. vSwitch1 vmnic3, vmnic2 VMkernel vMotion 3173 Default Enabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled 172.17.73.11 (static) 255.255.255.0	
			Back Next Finish Cancel

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

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

Navigator   Image   Ima	vmware <sup>®</sup> vSphere Web Clie	ent <b>n</b> ≘		Ŭ │ Administrator@VSPHERE.LOCAL -	Help •
Getting Started Summary Monitor     Manage        Cetting Started Summary Monitor     Manage	Navigator I	wm-host-infra-01.versastack.la	ab Actions -		≡∗
	Navigator	vm-host-infra-01.versastack.li     Getting Started Summary Mo     Settings Networking Storage	ab       Actions *         nitor       Manage       Related Objects         Alarm Definitions       Tags       Permissions         Virtual switches       Image       Image         Image       Image       Image       Image         Switch       Image       Image       Image         Switch       Image       Image       Image       Image         Standard switch:       vSwitch1       Image       Image       Image         Standard switch:       vSwitch1       Image       Image       Image       Image         VLAN ID:       3173       VMkernel Ports (1)       Image       Image	Discovered Issues	Č

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

T vSwitch1 - Edit Settings			?
VSwitch1 - Edit Settings  Properties Security Traffic shaping Teaming and failover	Number of ports: MTU (Bytes):	Elastic 9000 T	3
		ОК	Cancel

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

vmware <sup>®</sup> vSphere Web Clie	ent nt≣				ا لک ا	ministrator@VSPHERE.LO	CAL 🗸 🕴 Help 🗸
VMWARe' vSphere Web Clic Navigator Home Venter.versastack.lab VersaStack_DC VersaStack_DC VersaStack_MGMT VersaStack_MGMT VersaStack_VC VersaStack_vCenter VersaStack-vCenter VersaStack-vCenter	Image: Started Summary Mo       Getting Started Summary Mo       Settings       Networking       Storage       Virtual switches       VMkernel adapters       TCP/IP configuration       Advanced	Actions nitor Manag Alarm Definitio VMkernel ac Se Se I Device I Device I D	e Related Objects ens Tags Permissions dapters	Switch	U   Add IP Address 192.168.162.101 172.17.73.11	ministrator@VSPHERE.LO	CAL - I Help -
		All Pro Port prop Network	perties IP Settings Polic erties ( label	cies VMkernel vMotion			* 

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

💌 vmk1 - Edit Settings		?
Port properties	MTU: 9000	
NIC settings		
IPv4 settings		
IPv6 settings		
Analyze impact		
	ОК	Cancel

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

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

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

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

vmware <sup>,</sup> vSphere Web Cl	ient nt≘	U   Administrator@VSPHERE.LOCAL -   Help
Navigator	VersaStack_DC Actions -	Ξ.
( Home ) 🔊	Getting Started Summary Monitor Manage Related Objects	
		⊗ _
✓ ② vcenter.versastack.lab	What is a Datacenter?	
Versa     Actions - VersaStack     New Cluster     New Folder     Distributed Switch     New Virtual Machin     New Virtual Machin     New Vapp from Lib     Opploy OVF Templ     Storage     Edit Default VM Cc     Migrate VM to Ano     Move To     Rename     Tans	pc       a primary container of such as hosts and vitual         Image: schedule	Virtual Machines Host atacenter
Add Permission	Explore Further	
Alarms	st Learn more about da	atacenters
🗙 Delete	luster Learn how to create	datacenters
All vRealize Orches	strator plugin Actions	

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

Level 2 Switch			(?) <b>}</b>
1 Name and location	Name:	DSwitch VersaStack	
2 Select version	Location:	VersaStack_DC	
3 Edit settings			
4 Ready to complete			
		Back Next Finish	Cancel

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

Sew Distributed Switch		(?) ₩
<ul> <li>1 Name and location</li> <li>2 Select version</li> </ul>	Select version Specify a distributed switch version.	
<ul><li>3 Edit settings</li><li>4 Ready to complete</li></ul>	<ul> <li>Distributed switch: 6.0.0 This version is compatible with VMware ESXi version 6.0 and later. The following new features are available: Network I/O Control version 3, and IGMP/MLD snooping.</li> </ul>	
	Distributed switch: 5.5.0 This version is compatible with VMware ESXi version 5.5 and later. The following new features are available: Traffic Filtering and Marking, and enhanced LACP support.	
	Distributed switch: 5.1.0 This version is compatible with VMware ESXi version 5.1 and later. The following new features are available: Management Network Rollback and Recovery, Health Check, Enhanced Port Mirroring, and LACP.	
	Distributed switch: 5.0.0 This version is compatible with VMware ESXi version 5.0 and later. The following new features are available: User-defined network resource pools in Network I/O Control, NetFlow, and Port Mirroring.	
	Back Next Finish	Cancel

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

Length Switch		(?) **
<ul> <li>1 Name and location</li> <li>2 Select version</li> <li>3 Edit settings</li> <li>4 Ready to complete</li> </ul>	Edit settings Specify number of uplink Number of uplinks: Network I/O Control: Default port group: Port group name:	ports, resource allocation and default port group.
		Back Next Finish Cancel

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



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



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

2 New Distributed Port Group		(?	) <b>}}</b>
1 Select name and location	Name:	VM Network	٦
2 Configure settings	Location:	BSwitch VersaStack	
3 Ready to complete			
		Back Next Finish Cance	

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

2 New Distributed Port Group					(? )»
<ul> <li>1 Select name and location</li> <li>2 Configure settings</li> </ul>	Configure settings Set general properties of the	new port group.			
3 Ready to complete	Port binding: Port allocation:	Static binding Elastic	<b>T</b>		
	Number of ports: Network resource pool:	Elastic port groups automatica     (default)	Illy increase or decrease the	In umber of ports as needed.	
	VLAN	νΥ	_		
	VLAN type: VLAN ID:	VLAN         •           3174         •			
	Advanced	ies configuration			
			Back	Next Finish Ca	ancel

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



#### Add the ESXi Hosts to the vDS

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

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

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

vmware vSphere Web Clie	ent <b>A</b> ≣		Ŭ   Administrator@VSPHERE.LOCAL -	Help
Navigator	Vcenter.versastack.lab Actions -			
Navigator	Getting Started       Summary       Monitor       Manage         What is vCenter Server?       vCenter Server allows you to manage multiple ESX/ESX! hosts and the virtual machines on them. Because these environments can grow very large, vCenter Server provides useful all machines into clusters all machines into clusters stems can be managed by creater so that their individual a presented and managed of glass".         Another Network       •       •         •       •       •         •       •       •         •       •       •         •       •       •         •       •       •         •       •       •         •       •       •         •       •       •         •       •       •         •       •       •         •       •       •         •       •       •         •       •       •         •       •       •         •       •       •         •       •       •         •       •       •         •       •       •         •       •       •         •       •       •         •       •	Related Objects         Image: Control of the state		8

2. Leave Add hosts selected and click Next.

Add and Manage Hosts		2
1 Select task	Select task Select a task to perform on this distributed switch.	
<ul> <li>2 Select hosts</li> <li>3 Select network adapter tasks</li> <li>4 Manage physical network adapters</li> <li>5 Manage VMkernel network adapters</li> <li>6 Analyze impact</li> <li>7 Ready to complete</li> </ul>	<ul> <li>Add hosts Add new hosts to this distributed switch. </li> <li>Manage host networking Manage networking of hosts attached to this distributed switch. </li> <li>Remove hosts Remove hosts from this distributed switch. </li> <li>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.</li></ul>	
	Back Next Einich Cancel	1
	Data mext Prinish Cancer	J.

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

	🕼 Add and Manage Hosts							?	
~	1	Select task Select hosts	Select hosts Select hosts to add to this distribut	ted switch.					
	3	Select network adapter tasks							
	4	Manage physical network adapters	Host		Host Status				
	5	Manage VMkernel network adapters		This list is	empty.				
	6	Analyze impact							
	7	Ready to complete							
			Configure identical network set	tings on multiple hosts (template	mode). 📵				
						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.

D	Add and Manage Hosts									
<ul> <li>1 Select task</li> <li>2 Select hosts</li> </ul>				Select hosts Select hosts to add to this distributed switch						
	3	Select network adap tasks	Select ne	w hosts			×			
	4	Manage physical ne adapters	Incom	npatible Hosts		Q Filter	•			
	_	Manage VMkernel n	🖌 Host		Host State	Cluster				
	Э	adapters	🗹 📋 vr	m-host-infra-01.versastack.l	Connected	VersaStack_MGMT				
	6	Analyze impact	Vr 📄 Vr	m-host-infra-02.versastack.l	Connected	VersaStack_MGMT				
	7	Ready to complete								
			MQ	Find •			2 items			
						ОК	Cancel			
			_							
				Configure identical netwo	rk settings on multiple hosts (template m	node). 🚯				
						Back	Next	Finish	Cancel	

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

6	Add and Manage Hosts		(?)
×.	1 Select task	Select hosts Select hosts to add to this distributed switch.	
	3 Select nots 3 Select network adapter tasks	+ New hosts X Remove	
	4 Manage physical network adapters	Host	Host Status
	5 Manage VMkernel network adapters	<ul> <li>(New) vm-host-infra-01.versastack.lab</li> <li>(New) vm-host-infra-02.versastack.lab</li> </ul>	Connected
	6 Analyze impact	-	
	7 Ready to complete		
		Configure identical network settings on multiple hosts (template m	node). 🛈
			Back Next Finish Cancel

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

D	Add and Manage Hosts (?)							
<b>~</b>	1 Select task 2 Select hosts	Select template host Select a template host to apply its network configuration on this switch to the other hosts.						
	3 Select template host							
	4 Select network adapter tasks Manage physical network	Host 1▲ ⊙ 1 vm-host-infra-01.versas	Physical Adapters - On This Switch / All 0 / 6	VMkernel Adapters - On This Switch / All 0 / 2				
	<ul> <li><sup>5</sup> adapters (template mode)</li> <li><sup>6</sup> Manage VMkernel network adapters (template mode)</li> <li>7 Analyze impact</li> <li>8 Ready to complete</li> </ul>	○ 1 vm-host-infra-02.versasta	0/6	0/2				
		Services (vm-host-infra-01.versa: Fault Tolerance logging: Management traffic: vSphere Replication traffic: vMotion traffic: Virtual SAN traffic:	stack.lab)  vmk0  vmk1 	Back Next	Finish Cancel			

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



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

Add and Manage Hosts					?					
<ul> <li>✓ 1 Select task</li> <li>✓ 2 Select hosts</li> </ul>	Manage physical network adapters (terr Add or remove physical network adapters	<b>uplate mode)</b> to this distributed switch.								
✓ 3 Select template host	Configure or review physical network	Configure or review physical network adapter assignments for the template host in this switch.								
<ul> <li>Select network adapter tasks</li> </ul>	🔚 Assign uplink 🖙 Reset changes 🚯 View settings									
5 Manage physical network	Host/Physical Network Adapters	1 A In Use by Switch	Uplink	Uplink Port Group						
adapters (template mode)	🗾 vmnic0	vSwitch0	-							
6 Analyze impact	🗾 vmnic1	vSwitch0	-							
7 Ready to complete	🗾 vmnic2	vSwitch1	-							
	🗾 vmnic3	vSwitch1	-							
	对 vmnic4		-							
	对 vmnic5				_					
	Apply the physical network adapter a Apply to all Reset all View set	ssignments on this switch for th	he template host to all hos	its.						
	Host/Physical Network Adapters	1 ▲ In Use by Switch	Uplink	Uplink Port Group						
	✓ 1 vm-host-infra-02.versastack.lab									
	On this switch									
	<ul> <li>On other switches/unclaimed</li> </ul>				::					
	🗾 vmnic0	vSwitch0								
	vmnic1	vSwitch0	-							
	vmnic2	vSwitch1	-							
	O				•					
l			Back	Next Finish	Cancel					

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

Add and Manage Hosts								
✓ 1 Select task Man Add	age physical network adapters (template	mode)	0					
✓ 2 Select hosts	Select an Oplink for Vinnic4		×					
✓ 3 Select template host	Uplink	Assigned Adapter		witch.				
✓ 4 Select network adapter tasks	Uplink 1	-						
5 Manage physical network	Uplink 2				Uplink Port Group			
6 Analyze impact	(Auto-assign)				-	<b>A</b>		
7 Deschute complete								
7 Ready to complete					-			
					-	-		
0				ll hosts.				
+								
Hos					Uplink Port Group			
		OK	Cancel			<b>^</b>		
			Carloci	J				
	<ul> <li>On other switches/unclaimed</li> </ul>					::		
	ymnic0	vSwitch0						
	wnnic1	vSwitch0						
	wnnic2	vSwitch1			-	-		
			Back	Next	Finish	Cancel		

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

Add and Manage Hosts				?		
<ul> <li>1 Select task</li> <li>2 Select hosts</li> </ul>	Manage physical network adapters (te Add or remove physical network adapter	emplate mode) rs to this distributed switch.				
✓ 3 Select template host	1 Configure or review physical netwo	rk adapter assignments for the te	emplate host in this switch	l.		
<ul> <li>Select network adapter tasks</li> </ul>	🔚 Assign uplink 😭 Reset changes 🌘	View settings				
5 Manage physical network	Host/Physical Network Adapters	1 A In Use by Switch	Uplink	Uplink Port Group		
adapters (template mode)	对 vmnic5 (Assigned)		Uplink 2	DSwitch VersaSta-DVU		
6 Analyze impact	<ul> <li>On other switches/unclaimed</li> </ul>					
7 Ready to complete	vmnic0	vSwitch0				
	vmnic1	vSwitch0	-			
	vmnic2	vSwitch1	-	"		
	vmnic3	vSwitch1	-			
				<b>v</b>		
	<ul> <li>Apply the physical network adapter assignments on this switch for the template host to all hosts.</li> <li>Apply to all Reset all  View settings</li> </ul>					
	Host/Physical Network Adapters	1 A In Use by Switch	Uplink	Uplink Port Group		
	• 1 vm-host-infra-02.versastack.lab			A		
	vmnic4 (Assigned)	-	Uplink 1	DSwitch VersaSta-DVU **		
	vmnic5 (Assigned)	-	Uplink 2	DSwitch VersaSta-DVU		
	- On other switches/unclaimed					
	vmnic0	vSwitch0	-			
	- maried			Ψ		
			Back	Next Finish Cancel		

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

🕼 Add and Manage Hosts								
<ul> <li>Analyze impact Review the impact this configuration change might have on some network dependent services.</li> </ul>								
✓ 3 Select template host Overall impact status: ⊘ No impact								
<ul> <li>Select network adapter tasks</li> </ul>	Host / Impact Analysis per Service 1 🖌 Status							
<ul> <li>Manage physical network</li> <li>adapters (template mode)</li> </ul>	vm-host-infra-01.versastack.lab							
6 Analyze impact	iSCSI 📀 No impact							
7 Ready to complete	iSCSI		No impact					
		No Home	a allo act and					
		NO REMS	selected					
			Back Next	Finish Cancel				

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



# Appendix

## Cisco Nexus 9000 Example Configurations

#### Cisco Nexus 9000 A

VersaStack\_V5030\_Mini-A# sh running-config

!Command: show running-config

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

version 7.0(3)I2(4) switchname VersaStack\_V5030\_Mini-A vdc VersaStack\_V5030\_Mini-A id 1 limit-resource vlan minimum 16 maximum 4094

limit-resource vrf minimum 2 maximum 4096

limit-resource port-channel minimum 0 maximum 511

limit-resource u4route-mem minimum 248 maximum 248

limit-resource u6route-mem minimum 96 maximum 96

limit-resource m4route-mem minimum 58 maximum 58

limit-resource m6route-mem minimum 8 maximum 8

feature telnet cfs eth distribute feature lacp feature vpc

username admin password 5 \$1\$xqcEGkDT\$/lpogNkFXi8RTWhgAuSnD1 role network-admin ssh key rsa 2048 ip domain-lookup copp profile strict

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

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

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

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

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

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

```
ntp server 192.168.160.254
```

vlan 1-2,11,3173-3174

vlan 2

name Native-VLAN

vlan 11

name IB-MGMT-VLAN

vlan 3173

name vMotion-VLAN

vlan 3174

name VM-Traffic-VLAN

spanning-tree port type edge bpduguard default

spanning-tree port type edge bpdufilter default

spanning-tree port type network default

vrf context management

ip route 0.0.0.0/0 192.168.160.1

vpc domain 10

peer-switch

role priority 10

peer-keepalive destination 192.168.162.202 source 192.168.162.201

Appendix

delay restore 150

peer-gateway

auto-recovery

ip arp synchronize

interface port-channel10 description vPC peer-link switchport mode trunk switchport trunk native vlan 2 switchport trunk allowed vlan 11,3173-3174 spanning-tree port type network vpc peer-link

interface port-channel13 description VersaStack\_UCS-Mini-A switchport mode trunk switchport trunk native vlan 2 switchport trunk allowed vlan 11,3173-3174 spanning-tree port type edge trunk mtu 9216 vpc 13

interface port-channel14 description VersaStack\_UCS-Mini-B switchport mode trunk switchport trunk native vlan 2 switchport trunk allowed vlan 11,3173-3174 spanning-tree port type edge trunk mtu 9216

vpc 14

interface port-channel15

description IB-MGMT

switchport mode trunk

switchport access vlan 11

switchport trunk allowed vlan 11

spanning-tree port type network

vpc 15

interface Ethernet1/1

interface Ethernet1/2

interface Ethernet1/3

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

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan 11,3173-3174

mtu 9216

channel-group 13 mode active

interface Ethernet1/4

description VersaStack\_UCS-Mini-B:1/4

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan 11,3173-3174

mtu 9216

channel-group 14 mode active

interface Ethernet1/5

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19 interface Ethernet1/20 interface Ethernet1/21 interface Ethernet1/22 interface Ethernet1/23 interface Ethernet1/24 interface Ethernet1/25 interface Ethernet1/26 interface Ethernet1/27 interface Ethernet1/28 interface Ethernet1/29 interface Ethernet1/30 interface Ethernet1/31 interface Ethernet1/32 interface Ethernet1/33
interface Ethernet1/35

interface Ethernet1/36

description IB-MGMT-SWITCH\_uplink

switchport mode trunk

switchport access vlan 11

switchport trunk allowed vlan 11

channel-group 15 mode active

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40

interface Ethernet1/41

interface Ethernet1/42

interface Ethernet1/43

interface Ethernet1/44

interface Ethernet1/47

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

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan 11,3173-3174

channel-group 10 mode active

interface Ethernet1/48

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

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan 11,3173-3174

channel-group 10 mode active

interface Ethernet1/49

interface Ethernet1/50

interface Ethernet1/51

interface Ethernet1/52

interface Ethernet1/53

interface mgmt0 vrf member management ip address 192.168.162.201/22 line console line vty session-limit 16 boot nxos bootflash:/nxos.7.0.3.I2.4.bin

VersaStack\_V5030\_Mini-A# exit

## Cisco Nexus 9000 B

VersaStack\_V5030\_Mini-B# sh running-config

!Command: show running-config

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

version 7.0(3)I2(4) switchname VersaStack\_V5030\_Mini-B vdc VersaStack\_V5030\_Mini-B id 1 limit-resource vlan minimum 16 maximum 4094 limit-resource vrf minimum 2 maximum 4096 limit-resource port-channel minimum 0 maximum 511 limit-resource u4route-mem minimum 248 maximum 248 limit-resource u6route-mem minimum 96 maximum 96 limit-resource m4route-mem minimum 58 maximum 58 limit-resource m6route-mem minimum 8 maximum 8 Appendix

feature telnet

cfs eth distribute

feature lacp

feature vpc

username admin password 5 \$1\$9MAImrSw\$7LR4R1BI06flWSbkgI6KM/ role network-admin ssh key rsa 2048 ip domain-lookup copp profile strict snmp-server user admin network-admin auth md5 0xca1d453021a34c63cd343709533f6187 priv 0xca1d453021a34c63cd343709533f6187 localizedkey rmon event 1 log trap public description FATAL(1) owner PMON@FATAL rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL rmon event 3 log trap public description ERROR(3) owner PMON@ERROR rmon event 4 log trap public description WARNING(4) owner PMON@WARNING rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO ntp server 192.168.160.254

vlan 1-2,11,3173-3174

vlan 2

name Native-VLAN

vlan 11

name IB-MGMT-VLAN

vlan 3173

name vMotion-VLAN

vlan 3174

name VM-Traffic-VLAN

spanning-tree port type edge bpduguard default spanning-tree port type edge bpdufilter default spanning-tree port type network default vrf context management ip route 0.0.0/0 192.168.160.1 vpc domain 10 peer-switch role priority 10 peer-keepalive destination 192.168.162.201 source 192.168.162.202 delay restore 150 peer-gateway auto-recovery ip arp synchronize

## interface port-channel10

description vPC peer-link switchport mode trunk switchport trunk native vlan 2 switchport trunk allowed vlan 11,3173-3174 spanning-tree port type network vpc peer-link

interface port-channel13 description VersaStack\_UCS-Mini-A switchport mode trunk switchport trunk native vlan 2 switchport trunk allowed vlan 11,3173-3174 spanning-tree port type edge trunk mtu 9216

vpc 13

interface port-channel14 description VersaStack\_UCS-Mini-B switchport mode trunk switchport trunk native vlan 2 switchport trunk allowed vlan 11,3173-3174 spanning-tree port type edge trunk mtu 9216 vpc 14

interface port-channel15

description IB-MGMT

switchport mode trunk

switchport access vlan 11

switchport trunk allowed vlan 11

spanning-tree port type network

vpc 15

interface Ethernet1/1

interface Ethernet1/2

interface Ethernet1/3

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

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan 11,3173-3174

mtu 9216

channel-group 14 mode active

interface Ethernet1/4

description VersaStack\_UCS-Mini-A:1/4

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan 11,3173-3174

mtu 9216

channel-group 13 mode active

interface Ethernet1/5

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Eth	nernet1/14	
interface Eth	nernet1/15	
interface Eth	nernet1/16	
interface Eth	nernet1/17	
interface Eth	nernet1/18	
interface Eth	nernet1/19	
interface Eth	nernet1/20	
interface Eth	nernet1/21	
interface Eth	nernet1/22	
interface Eth	nernet1/23	
interface Eth	nernet1/24	
interface Eth	nernet1/25	
interface Eth	nernet1/26	
interface Eth	nernet1/27	
interface Eth	nernet1/28	

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface Ethernet1/33

interface Ethernet1/34

interface Ethernet1/35

interface Ethernet1/36

description IB-MGMT-SWITCH\_uplink

switchport mode trunk

switchport access vlan 11

switchport trunk allowed vlan 11

channel-group 15 mode active

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/42

interface Ethernet1/43

interface Ethernet1/44

interface Ethernet1/45

interface Ethernet1/46

interface Ethernet1/47

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

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan 11,3173-3174

channel-group 10 mode active

interface Ethernet1/48

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

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan 11,3173-3174

channel-group 10 mode active

interface Ethernet1/51

interface Ethernet1/52

interface Ethernet1/53

interface Ethernet1/54

interface mgmt0

vrf member management

ip address 192.168.162.202/22

line console

line vty

session-limit 16

boot nxos bootflash:/nxos.7.0.3.l2.4.bin

VersaStack\_V5030\_Mini-B# exit

## About the Authors

Sreenivasa Edula, Technical Marketing Engineer, Cisco UCS Data Center Solutions Engineering, Cisco Systems, Inc.

Sreeni has over 17 years of experience in Information Systems with expertise across Cisco Data Center technology portfolio, including DC architecture design, virtualization, compute, network, storage and cloud computing.

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

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

## Acknowledgements

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

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