

VersaStack for Data Center

Deployment of Cisco Unified Computing System and Cisco Nexus 9000 Series Switches, IBM Storwize V7000 Unified Storage and VMware vSphere 5.5 Update 1 Last Updated: July 1, 2015



Building Architectures to Solve Business Problems

cisco.





About the Authors

Jeff Fultz, Technical Marketing Engineer, Server Access Virtualization Business Unit, Cisco Systems

Jeff has over 20 years of experience in Information Systems and Application Development focusing on data center management, backup, and virtualization optimization related technologies. As a member of multiple engineering solution teams, Jeff has deployed, designed and tested a wide variety of enterprise solutions encompassing Cisco, VMware, HyperV, SQL, and Microsoft Exchange to name a few. Jeff is a Microsoft Certified System Engineer with multiple patents filed in the datacenter solutions space.

Shivakumar Shastri, Technical Marketing Engineer, Server Access Virtualization Business Unit, Cisco Systems

Shiva has over 18 years of experience in various aspects of IT Infrastructure Engineering. Recent areas of focus include cloud automation, hyper-convergence, security and systems engineering of integrated stacks.

Sally Neate, Test Architect, Systems and Technology Group, IBM

Sally Neate has over 10 years of engineering experience in IBM's Systems and Technology group, and has been involved in the development of the Storwize product range from its inception. As system test lead for the Storwize and SAN Volume Controller 7.2 and 7.3 releases, Sally has designed and tested systems to meet the demands of a wide range of mid-range and enterprise environments.

About Cisco Validated Design (CVD) Program

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 (COLLEC-TIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUP-PLIERS 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)

© 2015 Cisco Systems, Inc. All rights reserved

cisco.



VersaStack for Data Center

Overview

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 siloed architectures. Cisco and IBM have partnered to deliver VersaStack, which uses best of breed storage, server and network components to serve as the foundation for a variety of workloads, enabling efficient architectural designs that can be deployed quickly and with confidence.

Audience

This document describes the architecture and deployment procedures of an infrastructure composed of Cisco®, IBM ®, and VMware® virtualization that uses IBM Storwize V7000 Unified storage serving both file and block protocols. The intended audience for this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineering, and customers who want to deploy the core VersaStack architecture with IBM Storwize V7000.

Architecture

The VersaStack architecture is highly modular or "Pod"-like. There is sufficient architectural flexibility and design options to scale as required with investment protection. The platform can be scaled up (adding resources to existing VersaStack units) and/or out (adding more VersaStack units).

Specifically, VersaStack is a defined set of hardware and software that serves as an integrated foundation for both virtualized and non-virtualized solutions. VMware vSphere® built on VersaStack includes IBM Storwize V7000, Cisco networking, the Cisco Unified Computing SystemTM (Cisco UCS®), Cisco MDS fiber-channel switches and VMware vSphere software in a single package. The design is flexible enough

that the networking, computing, and storage can fit in one data center rack or be deployed according to a customer's data center design. Port density enables the networking components to accommodate multiple configurations.

One benefit of the VersaStack architecture is the ability to meet any customer's capacity or performance needs in a cost effective manner. A storage system capable of serving multiple protocols across a single interface allows for customer choice and investment protection because it is a wire-once architecture.

This architecture references relevant criteria pertaining to resiliency, cost benefit, and ease of deployment of all components including IBM Storwize V7000 storage.

The architecture for this solution shown below uses two sets of hardware resources:

- 1. Common Infrastructure services on redundant and self-contained hardware.
- 2. VersaStack Pod

The common infrastructure services include Active Directory, DNS, DHCP, vCenter, Nexus 1000v virtual supervisor module (VSM) and any other shared service. These components are considered core infrastructure as they provide necessary data-center wide services where the VersaStack Pod resides. Since these services are integral to the deployment and operation of the platform, there is a need to adhere to best-practices in their design and implementation. This includes such features as high-availability, appropriate RAID setup and performance and scalability considerations given such services may need to be extended to multiple Pods. At a customer's site, depending on whether this is a new data center, there may not be a need to build this infrastructure piece.

Figure 1 illustrates the VMware vSphere built on VersaStack components and the network connections for a configuration with IBM Storwize V7000 Storage. This design uses the Cisco Nexus® 9396, and Cisco UCS B-Series with the Cisco UCS virtual interface card (VIC) and the IBM Storwize V7000 storage controllers connected in a highly available design using Cisco Virtual Port Channels (vPCs). This infrastructure is deployed to provide FC-booted hosts with file and block-level access to shared storage datastores.

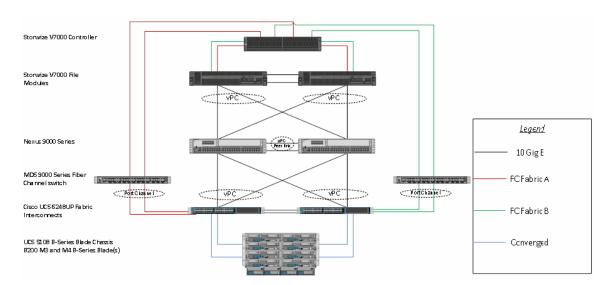


Figure 1 VersaStack

The reference hardware configuration includes:

- Two Cisco Nexus 9396 or 9372 switches
- Two Cisco UCS 6248UP Fabric Interconnects

- Two Cisco MDS 9148S Fibre-Channel switches
- · Support for 32 Cisco UCS C-Series servers without any additional networking components
- · Support for 8 Cisco UCS B-Series servers without any additional blade server chassis
- Support for 160 Cisco UCS C-Series and B-Series servers by way of additional fabric extenders and blade server chassis
- One IBM Storwize V7000 Unified system, comprising a V7000 control enclosure, V7000 expansion enclosure, and V7000 file modules. Support for up to 504 small form-factor (SFF) disks of any capacity.

For server virtualization, the deployment includes VMware vSphere. Although this is the base design, each of the components can be scaled easily to support specific business requirements. For example, more (or different) servers or even blade chassis can be deployed to increase compute capacity, additional disk shelves can be deployed to improve I/O capability and throughput, and special hardware or software features can be added to introduce new features.

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.

For Information regarding the design of VersaStack, please reference the Design guide at http://www.cisco.com/c/dam/en/us/td/docs/unified_computing/ucs/UCS_CVDs/Versastack_design.pdf

Important: This document implements the optional V7000 File Modules in the installation to add NAS support to our Block setup. There are notes in the appropriate sections to guide you if you are installing a Block only setup.

Software Revisions

 Table 1 details the software revisions used for validating various components of the Cisco Nexus 9000

 based VersaStack architecture.

Layer	Device	Version or Release	Details
Compute	Cisco UCS fabric interconnect	2.2(3b)	Embedded management
	Cisco UCS C 220 M3/M4	2.2(3b)	Software bundle release
	Cisco UCS B 200 M3/ M4	2.2(3b)	Software bundle release
	Cisco enic	2.1.2.42	Ethernet driver for Cisco VIC
Network	Cisco Nexus 9396	6.1(2) 3(1)	Operating system version
	Cisco MDS 9148S	6.2(9)	FC switch firmware version
Storage	IBM Storwize V7000	7.3.0.8	Software version
-	IBM Storwize V7000 Unified	1.5.0.5-1	Software version
Software	Cisco UCS hosts	VMware vSphere	Operating system version
		ESXi [™] 5.5u1	
	Microsoft SQL Server [®]	Microsoft SQL Server	VM (1 each): SQL Server DB
		2008 R2 SP1	
	VMware vCenter [™]	5.5u1	VM (1 each): VMware vCenter
	Cisco Nexus 1000v	5.2(1)SV3(1.2)	Software version
	Virtual Switch Update Manager	1.1	Virtual Switch Deployment
	(VSUM)		Software

Table 1Software Revisions

Configuration Guidelines

This document provides details on configuring a fully redundant, highly available VersaStack unit with IBM Storwize V7000 storage. Therefore, reference is made at each step to the component being configured as either 01 or 02. For example, node01 and node02 are used to identify the two IBM storage controllers that are provisioned with this document, and Cisco Nexus A and Cisco Nexus B identify the pair of Cisco Nexus switches that are configured. The Cisco UCS fabric Interconnects are similarly configured. Additionally, this document details the steps for provisioning multiple Cisco UCS hosts, and these are identified sequentially: VM-Host-Infra-01, VM-Host-Infra-02, and so on. Finally, to indicate that you should include information pertinent to your environment in a given step, <text> appears as part of the command structure. See the following example for the network port vlan create command:

Usage:

```
network port vlan create ?
   [-node] <nodename> Node
   { [-vlan-name] {<netport>|<ifgrp>} VLAN Name
   | -port {<netport>|<ifgrp>} Associated Network Port
   [-vlan-id] <integer> } Network Switch VLAN Identifier
Example:
```

network port vlan -node <node01> -vlan-name i0a-<vlan id>

This document is intended to enable you to fully configure the VersaStack Pod in the environment. Various steps require you to insert customer-specific naming conventions, IP addresses, and VLAN schemes, as well as to record appropriate MAC addresses.

Table 2 describes the VLANs necessary for deployment as outlined in this guide. Table 3 lists the virtual machines (VMs) necessary for deployment as outlined in this guide.

Table 2	Necessary	VLANs
---------	-----------	-------

VLAN Name	VLAN Name VLAN Purpose	
		This Document
Native	VLAN to which untagged frames are assigned	2
Mgmt out of band	VLAN for out-of-band management interfaces	3171
NFS	VLAN for NFS traffic	3172
vMotion	VLAN designated for the movement of VMs from one	3173
	physical host to another	
VM Traffic	VLAN for VM application traffic	3174
Mgmt in band	VLAN for in-band management interfaces	3175

I

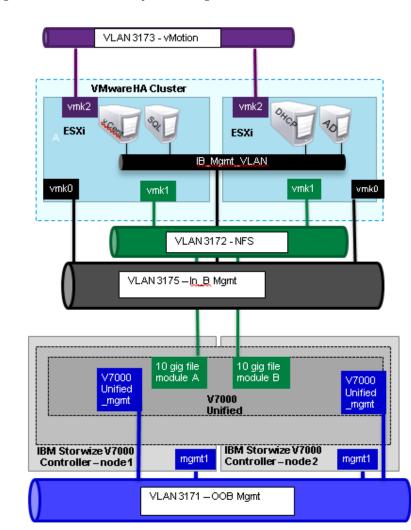


Figure 2 Overview of VLAN Usage

Table 3VMware Virtual Machines Created

Virtual Machine Description	Host Name	
Active Directory		
vCenter Server		
SLQ Server		
DHCP Server		

Table 4 lists the configuration variables that are used throughout this document. This table can be completed based on the specific site variables and used in implementing the document configuration steps.

Table 4Configuration Variables

ſ

Variable	Description	Customer Implementation Value
< <var_node01_mgmt_ip>></var_node01_mgmt_ip>	Out-of-band management IP for cluster node 01	

< <var_node01_mgmt_mask>></var_node01_mgmt_mask>	Out-of-band management network
<var gateway="" mgmt="" node01="">></var>	netmask Out-of-band management network
<var_node01_mgmc_gateway>></var_node01_mgmc_gateway>	default gateway
<var_node02_mgmt_ip>></var_node02_mgmt_ip>	Out-of-band management IP for
	cluster node 02
< <var_node02_mgmt_mask>></var_node02_mgmt_mask>	Out-of-band management network
	netmask
< <var gateway="" mgmt="" node02="">></var>	Out-of-band management network
	default gateway
< <var_cluster_mgmt_ip>></var_cluster_mgmt_ip>	Out-of-band management IP for
	cluster
< <var_cluster_mgmt_mask>></var_cluster_mgmt_mask>	Out-of-band management network
	netmask
< <var_cluster_mgmt_gateway>></var_cluster_mgmt_gateway>	Out-of-band management network
	default gateway
< <var_password>></var_password>	Global default administrative
	password
< <var_dns_domain_name>></var_dns_domain_name>	DNS domain name
< <var_nameserver_ip>></var_nameserver_ip>	DNS server IP(s)
< <var_timezone>></var_timezone>	VersaStack time zone (for
	example, America/New_York)
< <var_global_ntp_server_ip>></var_global_ntp_server_ip>	NTP server IP address
< <var_email_contact>></var_email_contact>	Administrator e-mail address
< <var_admin_phone>></var_admin_phone>	Local contact number for
	support
< <var_mailhost_ip>></var_mailhost_ip>	Mail server host IP
< <var_country_code>></var_country_code>	Two-letter country code
< <var_state>></var_state>	State or province name
< <var_city>></var_city>	City name
< <var_org>></var_org>	Organization or company name
< <var_unit>></var_unit>	Organizational unit name
< <var_street_address>>,</var_street_address>	Streed address for support
	information
< <var_contact_name>></var_contact_name>	Name of contact for support
< <var_admin>></var_admin>	Secondary Admin account for
	storage login
< <var_nexus_a_hostname>></var_nexus_a_hostname>	Cisco Nexus A host name
< <var_nexus_a_mgmt0_ip>></var_nexus_a_mgmt0_ip>	Out-of-band Cisco Nexus A
	management IP address
< <var_nexus_a_mgmt0_netmask></var_nexus_a_mgmt0_netmask>	Out-of-band management network netmask
<pre>> <<var a="" gw="" mgmt0="" nexus="">></var></pre>	Out-of-band management network
	default gateway
< <var_nexus_b_hostname>></var_nexus_b_hostname>	Cisco Nexus B host name
< <var_nexus_b_mgmt0_ip>></var_nexus_b_mgmt0_ip>	Out-of-band Cisco Nexus B
	management IP address

< <var b="" mgmt0="" netmask="" nexus=""></var>	Out-of-band management network	
>	netmask	
< <var_nexus_b_mgmt0_gw>></var_nexus_b_mgmt0_gw>	Out-of-band management network	
	default gateway	
< <var_ib-mgmt_vlan_id>></var_ib-mgmt_vlan_id>	In-band management network VLAN	
	ID	
< <var_native_vlan_id>></var_native_vlan_id>	Native VLAN ID	
< <var_nfs_vlan_id>></var_nfs_vlan_id>	NFS VLAN ID	
< <var_vmotion_vlan_id>></var_vmotion_vlan_id>	VMware vMotion [®] VLAN ID	
< <var_vm-traffic_vlan_id>></var_vm-traffic_vlan_id>	VM traffic VLAN ID	
< <var_nexus_vpc_domain_id>></var_nexus_vpc_domain_id>	Unique Cisco Nexus switch VPC	
	domain ID	
< <var_ucs_clustername>></var_ucs_clustername>	Cisco UCS Manager cluster host	
	name	
< <var_ucsa_mgmt_ip>></var_ucsa_mgmt_ip>	Cisco UCS fabric interconnect	
	(FI) A out-of-band management	
	IP address	
< <var_ucsa_mgmt_mask>></var_ucsa_mgmt_mask>	Out-of-band management network	
	netmask	
< <var_ucsa_mgmt_gateway>></var_ucsa_mgmt_gateway>	Out-of-band management network	
	default gateway	
< <var_ucs_cluster_ip>></var_ucs_cluster_ip>	Cisco UCS Manager cluster IP	
	address	
< <var_ucsb_mgmt_ip>></var_ucsb_mgmt_ip>	Cisco UCS FI B out-of-band	
	management IP address	
< <var_cimc_mask>></var_cimc_mask>	Out-of-band management network	
	netmask	
< <var_cimc_gateway>></var_cimc_gateway>	Out-of-band management network	
	default gateway	
< <var_vsm_domain_id>></var_vsm_domain_id>	Unique Cisco Nexus 1000v	
	virtual supervisor module (VSM)	
	domain ID	
< <var_vsm_mgmt_ip>></var_vsm_mgmt_ip>	Cisco Nexus 1000v VSM	
	management IP address	
< <var_vsm_updatemgr_mgmt_ip></var_vsm_updatemgr_mgmt_ip>		
>	IP address	
< <var_vsm_mgmt_mask>></var_vsm_mgmt_mask>	In-band management network	
A THOR WORM MORT COLOURS	netmask In-band management network	
< <var_vsm_mgmt_gateway>></var_vsm_mgmt_gateway>	0	
<var hostname="" vsm="">></var>	default gateway Cisco Nexus 1000v VSM host name	
< <var_ftp_server>></var_ftp_server>	IP address for FTP server	
<var_mds_a_hostname>></var_mds_a_hostname>	Name for the FC MDS Switch	
< <var_mds_a_mgmt0_ip>></var_mds_a_mgmt0_ip>	MDS switch Out-of-band Cisco	
CAUSE MDS & momt 0 potmosiles	Nexus B management IP address MDS switch Out-of-band Cisco	
< <var_mds_a_mgmt0_netmask>></var_mds_a_mgmt0_netmask>		
<var a="" gw="" mds="" mgmt0="">></var>	Nexus B management IP netmask MDS switch Out-of-band Cisco	
A		
	Nexus B management IP gateway	

I

Γ

< <var_mds_b_hostname>></var_mds_b_hostname>	Name for the FC MDS Switch
< <var_mds_b_mgmt0_ip>></var_mds_b_mgmt0_ip>	MDS switch Out-of-band Cisco
<var_mds_b_mgmt0_netmask>></var_mds_b_mgmt0_netmask>	Nexus B management IP address MDS switch Out-of-band Cisco
< <vai_mbs_b_mgmc0_necmask>></vai_mbs_b_mgmc0_necmask>	
<var_mds_b_mgmt0_gw>></var_mds_b_mgmt0_gw>	Nexus B management IP netmask MDS switch Out-of-band Cisco
	Nexus B management IP gateway
< <var offset="" utc="">></var>	UTC time offset for your area
	_
< <var_vsan_a_id>></var_vsan_a_id>	Vsan id for MDS switch A (101
	is used)
< <var_vsan_b_id>></var_vsan_b_id>	Vsan id for MDS switch B (102
	is used)
< <var_fabric_a_fcoe_vlan_id></var_fabric_a_fcoe_vlan_id>	Fabric id for MDS switch A (
>	101 is used)
< <var_fabric_b_fcoe_vlan_id></var_fabric_b_fcoe_vlan_id>	Fabric id for MDS switch B (
>	102 is used)
< <var_in-band_mgmtblock_net></var_in-band_mgmtblock_net>	Block of IP addresses for KVM
>	access for UCS
< <var_v7000_unified_manageme< td=""><td>V7000 Unified MGMT IP</td></var_v7000_unified_manageme<>	V7000 Unified MGMT IP
<pre>nt_IP>>, <<var_file_module_1_service< pre=""></var_file_module_1_service<></pre>	V7000 Unified node console MGMT
<pre>ip>> <<var_file_module_2_service< pre=""></var_file_module_2_service<></pre>	IP node 1 V7000 Unified node console MGMT
	IP node 2
<pre>ip>> <<var_filemodule_name>></var_filemodule_name></pre>	Netbios name for V7000 unified
	cluster
< <var bond="" ip="" networ<="" td="" unified=""><td>Network for the V7000 unified</td></var>	Network for the V7000 unified
k>>	bond for NFS
<-var unified bond ip Netmas	Network Mask for the V7000
k>>	unified bond for NFS
< <var bond="" gatewa<="" ip="" td="" unified=""><td>Gateway Mask for the V7000</td></var>	Gateway Mask for the V7000
y>>	unified bond for NFS
< <var_unified_bond_public_ip< td=""><td>Network IP address that is</td></var_unified_bond_public_ip<>	Network IP address that is
>>	mounted from NFS hosts for the
	V7000 unified bond
< <var_unified_datastore_name< td=""><td>NFS Datastore for V7000 unified</td></var_unified_datastore_name<>	NFS Datastore for V7000 unified
>>	
< <var_vmhost_infra_01_ip>></var_vmhost_infra_01_ip>	VMware ESXi host 01 in-band
	Mgmt IP
< <var_vmhost_infra_01_2nd_ip< td=""><td>VMware ESXi host 01 secondary</td></var_vmhost_infra_01_2nd_ip<>	VMware ESXi host 01 secondary
>>	in-band Mgmt IP
< <var_nfs_vlan_id_ip_host-01< td=""><td>NFS VLAN IP address for ESXi</td></var_nfs_vlan_id_ip_host-01<>	NFS VLAN IP address for ESXi
>>	host 01
<var_nfs_vlan_id_mask_host-< td=""><td>NFS VLAN netmask for ESXi host</td></var_nfs_vlan_id_mask_host-<>	NFS VLAN netmask for ESXi host
01>> < <var hos<="" id="" ip="" td="" vlan="" vmotion=""><td>01 vMotion VLAN IP address for</td></var>	01 vMotion VLAN IP address for
t-01>> < <var h<="" id="" mask="" td="" vlan="" vmotion=""><td>ESXi host 01 vMotion VLAN netmask for ESXi</td></var>	ESXi host 01 vMotion VLAN netmask for ESXi
ost-01>>	host 01
The last 6 variables should	
be repeated for all ESXi	
hosts	
110565	

Physical Infrastructure

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 V7000 running 7.3.0.8, and file modules running 1.5.0-1.

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

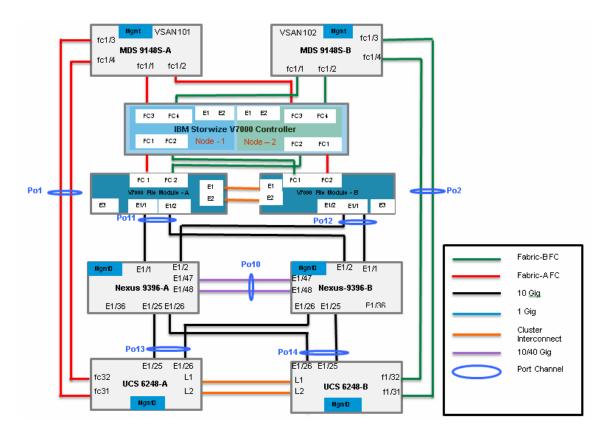
Be sure to follow the cabling directions in this section. Failure to do so will result in changes to the deployment procedures that follow because specific port locations are mentioned.

It is possible to order IBM Storwize V7000 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 through Figure 6 show cabling diagrams for a VersaStack configurations using the Cisco Nexus 9000 and IBM Storwize V7000 with and without the V7000 File Modules. For SAS cabling information, the V7000 control enclosure and expansion enclosure should be connected according to the cabling guide at the following URL:

http://www-

01.ibm.com/support/knowledgecenter/ST3FR7_7.3.0/com.ibm.storwize.v7000.730.doc/v3500_qisasca bles_b4jtyu.html?cp=ST3FR7%2F1-3-0-1-3&lang=en



1

Figure 3 VersaStack Block and File Cabling Diagram

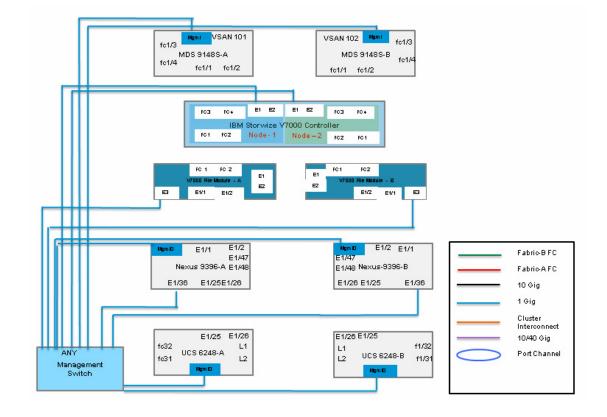
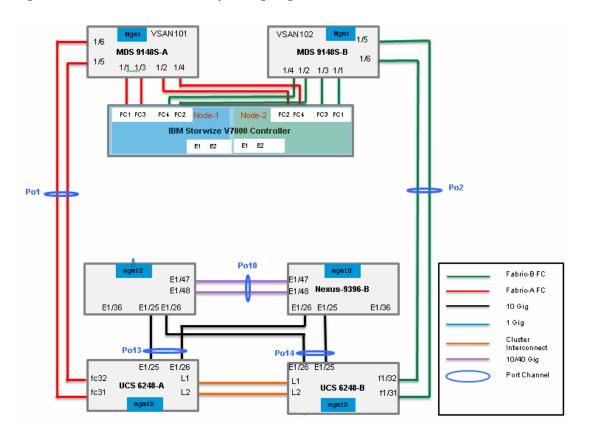


Figure 4 VersaStack Block and File Management Cabling Diagram

Γ



I

1

Figure 5 VersaStack Block Only Cabling Diagram

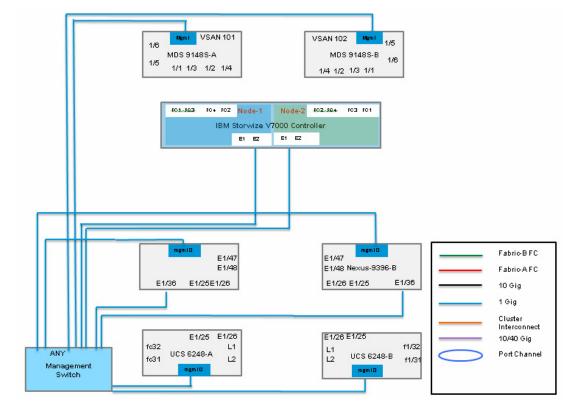


Figure 6 VersaStack Block Only Management Cabling Diagram

Table 5 through Table 17 provides the details of all the connections in use.

Γ

Local Device	Local Port	Connection	Remote Device	Remote Port
	Eth1/1	10GbE	IBM Storwize V7000 File Module-A	E1/1
	Eth1/2	10GbE	IBM Storwize V7000 File Module-B	E1/2
	Eth1/25	10GbE	Cisco UCS fabric interconnect-A	Eth1/25
Cisco Nexus 9000-A	Eth1/26	10GbE	Cisco UCS fabric interconnect-B	Eth1/26
	Eth1/47*	10GbE	Cisco Nexus 9000-B	Eth1/47
	Eth1/48*	10GbE	Cisco Nexus 9000-B	Eth1/48
	Eth1/36	GbE	GbE management switch	Any

1

 Table 5
 Cisco Nexus 9000 A Cabling Information

* The ports can be replaced with E2/11 and E2/12 for 40G connectivity

Note

For devices requiring GbE connectivity, use the GbE Copper SFP+s (GLC-T=).

Table 6Cisco Nexus 9000-B Cabling In	Information
--------------------------------------	-------------

Local Device	Local Port	Connection	Remote Device	Remote Port
	Eth1/1	10GbE	IBM Storwize V7000 File Module-B	E1/1
	Eth1/2	10GbE	IBM Storwize V7000 File Module-A	E1/2
	Eth1/25	10GbE	Cisco UCS fabric interconnect-B	Eth1/25
Cisco Nexus 9000-B	Eth1/26	10GbE	Cisco UCS fabric interconnect-A	Eth1/26
	Eth1/47*	10GbE	Cisco Nexus 9000-A	Eth1/47
	Eth1/48*	10GbE	Cisco Nexus 9000-A	Eth1/48
	Eth1/36	GbE	GbE management switch	Any

* The ports can be replaced with E2/11 and E2/12 for 40G connectivity.



For devices requiring GbE connectivity, use the GbE Copper SFP+s (GLC-T=).

Local Device	Local Port	Connection	Remote Device	Remote Port
	E3	GbE	GbE management switch	Any
	E1/1	10GbE	Cisco Nexus 9000-A	E1/1
	E1/2	10GbE	Cisco Nexus 9000-B	E1/2
IBM Storwize V7000 File Module-A	E1	1GbE	File Module-B	E1
Module-A	E2	1GbE	File Module-B	E2
	FC1	8gbps	V7000 Controller, Node-1	FC1
	FC2	8gbps	V7000 Controller, Node-2	FC2

 Table 7
 IBM Storwize V7000 File Module-A Cabling Information

 Table 8
 IBM Storwize V7000 File Module-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
	E3	GbE	GbE management switch	Any
	E1/1	10GbE	Cisco Nexus 9000-B	E1/1
	E1/2	10GbE	Cisco Nexus 9000-A	E1/2
IBM Storwize V7000 File Module-B	E1	1GbE	File Module-A	E1
NOQUIE-D	E2	1GbE	File Module-A	E2
	FC1	8gbps	V7000 Controller, Node-1	FC2
	FC2	8gbps	V7000 Controller, Node-2	FC1

 Table 9
 IBM Storwize V7000 Controller, Node-1 Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
IBM Storwize V7000 Controller, Node-1	E1/E2	GbE	GbE management switch	Any
	FC1	8gbps	V7000 File Module-A	FC1
	FC2	8gbps	V7000 File Module-B	FC1
	FC3	8gbps	MDS 9148S-A	fc1/1
	FC4	8gbps	MDS 9148S-B	fc1/1

Γ

Local Device	Local Port	Connection	Remote Device	Remote Port
IBM Storwize V7000 Controller, Node-2	E1/E2	GbE	GbE management switch	Any
	FC1	8gbps	V7000 File Module-B	FC2
	FC2	8gbps	V7000 File Module-A	FC2
	FC3	8gbps	MDS 9148S-A	fc1/2
	FC4	8gbps	MDS 9148S-B	fc1/2

Local Device	Local Port	Connection	Remote Device	Remote Port
	Mgmt0	GbE	GbE management switch	Any
	fc1/1	8gbps	IBM controller, Node-1	FC3
Cisco MDS 9148S-A	fc1/2	8gbps	IBM controller, Node-2	FC3
	fc1/3	8gbps	UCS Fabric Interconnect 6248-A	fc31
	fc1/4	8gbps	UCS Fabric Interconnect 6248-A	fc32

1

 Table 11
 Cisco Nexus MDS 9148S-A Cabling Information

Table 12 Cisco Nexus MDS 9148S-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
	Mgmt0	GbE	GbE management switch	Any
	fc1/1	8gbps	IBM controller, Node-1	FC4
Cisco MDS 9148S-B	fc1/2	8gbps	IBM controller, Node-2	FC4
	fc1/3	8gbps	UCS Fabric Interconnect 6248-B	fc31
	fc1/4	8gbps	UCS Fabric Interconnect 6248-B	fc32

Table 13 Cisco UCS Fabric Interconnect A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric	Mgmt0	GbE	GbE management switch	Any
interconnect-A	Eth1/25	10GbE	Cisco Nexus 9000-A	Eth 1/25
	Eth1/26	10GbE	Cisco Nexus 9000-B	Eth 1/26
	Eth1/1	10GbE	Cisco UCS Chassis FEX-A	IOM 1/1
	Eth1/2	10GbE	Cisco UCS Chassis FEX-A	IOM 1/2
	fc31	8gbps	Cisco MDS 9148S-A	fc1/3
	fc32	8gbps	Cisco MDS 9148S-A	fc1/4
	L1	GbE	Cisco UCS fabric interconnect-B	L1
	L2	GbE	Cisco UCS fabric interconnect-B	L2

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric	Mgmt0	GbE	GbE management switch	Any
interconnect-B	Eth1/25	10GbE	Cisco Nexus 9000-B	Eth 1/25
	Eth1/26	10GbE	Cisco Nexus 9000-A	Eth 1/26
	Eth1/1	10GbE	Cisco UCS Chassis FEX-B	IOM 1/1
	Eth1/2	10GbE	Cisco UCS Chassis FEX-B	IOM 1/2
	fc31	8gbps	Cisco MDS 9148S-B	fc1/3
	fc32	8gbps	Cisco MDS 9148S-B	fc1/4
	L1	GbE	Cisco UCS fabric interconnect-A	L1
	L2	GbE	Cisco UCS fabric interconnect-A	L2

Table 14 Cisco UCS Fabric Interconnect B Cabling Information

Table 15 Cisco UCS C-Series with Cisco Nexus 2232PP FEX

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS C-Series	Port 0	10GbE	Cisco Nexus 2232PP FEX A	Port 1
Server 1 with Cisco VIC	Port 1	10GbE	Cisco Nexus 2232PP FEX B	Port 1

Table 16Cisco Nexus Rack Fex A

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 2232PP FEX A	Fabric Port 1/1	10GbE	Cisco UCS fabric interconnect A	Port 3
	Fabric Port 1/2	10GbE	Cisco UCS fabric interconnect A	Port 4

Table 17Cisco Nexus Rack Fex B

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 2232PP FEX B	Fabric Port 1/1	10GbE	Cisco UCS fabric interconnect B	Port 3
	Fabric Port 1/2	10GbE	Cisco UCS fabric interconnect B	Port 4

Storage Compatibility and Interoperability

The IBM System Storage Interoperation Center (SSIC) provides information on supported external hardware and software for the specific IBM Storwize V7000 version.

Make sure that the hardware and software components are supported with the version of IBM Storwize V7000 that you plan to install by checking the SSIC. Click IBM System Storage Midrange Disk, then Storwize V7000 or Storwize V7000 Unified Host Attachment or Storage Controller Attachment.

• Software and hardware limitations for the specific IBM Storwize V7000 version can be found at:

http://www-01.ibm.com/support/docview.wss?uid=ssg1S1004628

• Further supported hardware, device driver, firmware and software level information can be found at: http://www-01.ibm.com/support/docview.wss?uid=ssg1S1004622

1

Complete the Configuration Worksheet

۵, Note

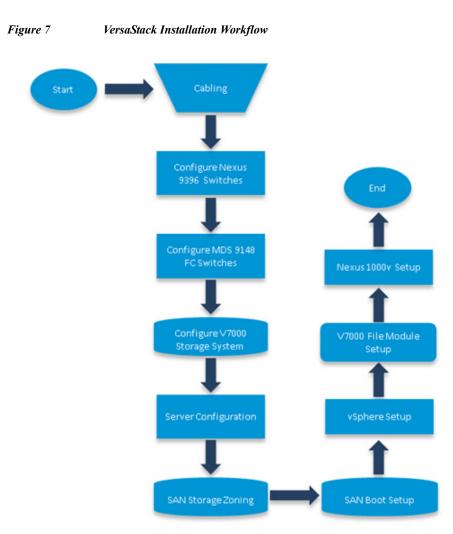
Before starting the setup, complete the Configuration worksheet from the IBM Storwize V7000 Knowledge Center.

	How to Access the Configuration Worksheet
Storwize V7000 Configuration Worksheet	http://www-01.ibm.com/support/knowledgecenter/ST3FR7_7.3.0/com.ibm.storwize.v7000.730.d oc/tbrd_completeconfdata.html?cp=ST3FR7%2F1-2-0-0-4
Storwize V7000 Unified Configuration Worksheet	http://www-01.ibm.com/support/knowledgecenter/ST5Q4U_1.5.0/com.ibm.storwize.v7000.unifie d.150.doc/ifs_completeconfdata.html?lang=en

Table 19

IBM Storwize V7000 Software Installation Prerequisites

Cluster Detail	Cluster Detail Value
Cluster Node01 IP address	< <var_node01_mgmt_ip>></var_node01_mgmt_ip>
Cluster Node01 netmask	< <var_node01_mgmt_mask>></var_node01_mgmt_mask>
Cluster Node01 gateway	< <var_node01_mgmt_gateway>></var_node01_mgmt_gateway>
Cluster Node02 IP address	< <var_node02_mgmt_ip>></var_node02_mgmt_ip>
Cluster Node02 netmask	< <var_node02_mgmt_mask>></var_node02_mgmt_mask>
Cluster Node02 gateway	< <var_node02_mgmt_gateway>></var_node02_mgmt_gateway>
Cluster IP address	< <var_cluster_mgmt_ip>></var_cluster_mgmt_ip>
Cluster netmask	< <var_cluster_mgmt_mask>></var_cluster_mgmt_mask>
Cluster gateway	< <var_cluster_mgmt_gateway>></var_cluster_mgmt_gateway>



VersaStack System Build Process

Cisco Nexus 9000 Network Initial Configuration Setup

These steps provide details for the initial Cisco Nexus 9000 Switch setup.

Cisco Nexus A

I

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



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

```
Abort Auto Provisioning and continue with normal setup ?(yes/no)[n]: y
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:
```

```
Enter the password for "admin":
  Confirm the password for "admin":
         ---- Basic System Configuration Dialog VDC: 1 ----
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
Please register Cisco Nexus9000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus9000 devices must be registered to receive
entitled support services.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
  Create another login account (yes/no) [n]: n
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : <<var nexus A hostname>>
  Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:
    Mgmt0 IPv4 address : <<var nexus A mgmt0 ip>>
    Mgmt0 IPv4 netmask : <<var nexus A mgmt0 netmask>>
  Configure the default gateway? (yes/no) [y]:
    IPv4 address of the default gateway : <<var nexus A mgmt0 gw>>
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]:
    Type of ssh key you would like to generate (dsa/rsa) [rsa]:
    Number of rsa key bits <1024-2048> [1024]: 2048
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var global ntp server ip>>
  Configure default interface layer (L3/L2) [L2]:
  Configure default switchport interface state (shut/noshut) [noshut]:
  Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]:
The following configuration will be applied:
 password strength-check
 switchname <<var_nexus_A_hostname>>
vrf context management
ip route 0.0.0.0/0 <<var nexus A mgmt0 gw>>
exit
no feature telnet
 ssh key rsa 2048 force
 feature ssh
 ntp server <<var global ntp server ip>>
 system default switchport
 no system default switchport shutdown
  copp profile strict
interface mgmt0
ip address <<var nexus A mgmt0 ip>> <<var nexus A mgmt0 netmask>>
no shutdown
Would you like to edit the configuration? (yes/no) [n]:
Use this configuration and save it? (yes/no) [y]:
Copy complete.
```

Cisco Nexus B

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

Note

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]:
```

Enable Appropriate Cisco Nexus 9000 Features and Settings

Cisco Nexus 9000 A and Cisco Nexus 9000 B

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

1. On each Nexus 9000, enter configuration mode:

```
config terminal2. Use the following commands to enable the necessary features:
```

```
feature udld
feature lacp
feature vpc
```

3. Configure 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 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:

I

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_nfs_vlan_id>>
name NFS-VLAN
vlan <<var_vmotion_vlan_id>>
name vMotion-VLAN
vlan <<var_vm_traffic_vlan_id>>
name VM-Traffic_VLAN
```

Configure Virtual Port Channel Domain

Cisco Nexus 9000 A

To configure virtual port channels (vPCs) 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 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 following features for this vPC domain:

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

Cisco Nexus 9000 B

To configure vPCs 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 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 following features for this vPC domain:

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

Configure Network Interfaces for the VPC Peer Links

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
```

VersaStack for Data Center

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, NFS, VM traffic, 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_nfs_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
```

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, NFS, VM traffic, 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_nfs_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

Configure Network Interfaces to Cisco UCS Fabric Interconnect

Cisco Nexus 9000 A

 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, NFS, VM traffic, 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_nfs_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 Eth1/25
description <<var_ucs_clustername>>-A:1/25
```

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
```

9. Make the port-channel a switchport, and configure a trunk to allow InBand management, NFS, and VM traffic VLANs 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_nfs_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 Eth1/26
description <<var ucs clustername>>-B:1/26
```

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

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

Configure Network Interfaces to UCS Fabric Interconnect

Cisco Nexus 9000 B

Define a description for the port-channel connecting to <<var_ucs_clustername>>-B
interface Po14

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

2. Make the port-channel a switchport, and configure a trunk to allow in-band management, NFS, VM traffic, 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_nfs_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 14 no shutdown

6. Define a port description for the interface connecting to <<var_ucs_clustername>>-B

I

interface Eth1/25

description <<var ucs clustername>>-B:1/25

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

9. Make the port-channel a switchport, and configure a trunk to allow InBand management, NFS, and VM traffic VLANs 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_nfs_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 Eth1/26
description <<var_ucs_clustername>>-A:1/26
```

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 VMs (optional)

There are multiple ways to configure the switch to uplink to your separate management switch. An example provided in this section where the management switch is top of rack and the Nexus 9000 series is connected to it via port 36. On each Nexus 9000 series switch, you configure an IP address on the interface VLAN and set up a default gateway. This will enable the Nexus switch to route traffic to the top of rack switch.

Cisco Nexus 9000 A

1. In configuration mode (config t), type the following commands:

```
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

In configuration mode (config t), type the following commands:

```
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 MDS 9148S Initial Configuration Setup

These steps provide details for the initial Cisco MDS Fibre Channel Switch setup.

Cisco MDS A

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

1. On initial boot and connection to the serial or console port of the switch, the MDS 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 ----
This setup utility will guide you through the basic configuration of
```

```
the system. Setup configures only enough connectivity for management
of the system.
Please register Cisco MDS 9000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. MDS devices must be registered to receive entitled
support services.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
  Create another login account (yes/no) [n]:
 Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
 Enter the switch name : <<var MDS A hostname>>
 Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:
   Mgmt0 IPv4 address : <<var_MDS_A_mgmt0_ip>>
   Mgmt0 IPv4 netmask : <<var_MDS_A_mgmt0_netmask>>
  Configure the default gateway? (yes/no) [y]:
    IPv4 address of the default gateway : <<var MDS_A_mgmt0_gw>>
  Configure advanced IP options? (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
 Enable the telnet service? (yes/no) [n]:
  Configure congestion/no_credit drop for fc interfaces? (yes/no)
                                                                       [y]:
 Enter the type of drop to configure congestion/no_credit drop? (con/no)
[c]:
   Enter milliseconds in multiples of 10 for congestion-drop for port mode
F
    in range (<100-500>/default), where default is 500.
                                                         [d]:
    Congestion-drop for port mode E must be greater than or equal to
    Congestion-drop for port mode F. Hence, Congestion drop for port
   mode E will be set as default.
 Enable the http-server? (yes/no) [y]:
 Configure clock? (yes/no) [n]:
 Configure timezone? (yes/no) [n]: y
Enter timezone config [PST/MST/CST/EST] : <<var_timezone>>
Enter Hrs offset from UTC [-23:+23] : <<var_UTC_offset>>
Enter Minutes offset from UTC [0-59] :
Configure summertime? (yes/no) [n]:
  Configure the ntp server? (yes/no) [n]: y
   NTP server IPv4 address : <<var global ntp server ip>>
  Configure default switchport interface state (shut/noshut) [shut]:
  Configure default switchport trunk mode (on/off/auto) [on]:
 Configure default switchport port mode F (yes/no) [n]:
  Configure default zone policy (permit/deny) [deny]:
 Enable full zoneset distribution? (yes/no) [n]:
  Configure default zone mode (basic/enhanced) [basic]:
The following configuration will be applied:
 password strength-check
  switchname mds-b
  interface mgmt0
```

```
ip address <<var MDS A mgmt0 ip>> <<var MDS A mgmt0 netmask>>
   no shutdown
 ip default-gateway <<var_MDS_A_mgmt0_gw>>
 ssh key rsa 2048 force
 feature ssh
 no feature telnet
 system timeout congestion-drop default mode F
 system timeout congestion-drop default mode E
 feature http-server
 clock timezone PST 0 0
 ntp server <<var global ntp server ip>>
 system default switchport shutdown
 system default switchport trunk mode on
 no system default zone default-zone permit
 no system default zone distribute full
 no system default zone mode enhanced
Would you like to edit the configuration? (yes/no) [n]:
Use this configuration and save it? (yes/no) [y]:
Copy complete.
```

Cisco MDS B

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

1. On initial boot and connection to the serial or console port of the switch, the MDS 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 ----
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
Please register Cisco MDS 9000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. MDS devices must be registered to receive entitled
support services.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
 Create another login account (yes/no) [n]:
 Configure read-only SNMP community string (yes/no) [n]:
 Configure read-write SNMP community string (yes/no) [n]:
 Enter the switch name : <<var_MDS_B_hostname>>
```

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

```
Mgmt0 IPv4 address : <<var MDS B mgmt0 ip>>
   Mgmt0 IPv4 netmask : <<var MDS B mgmt0 netmask>>
  Configure the default gateway? (yes/no) [y]:
    IPv4 address of the default gateway : <<var MDS B mgmt0 gw>>
  Configure advanced IP options? (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
 Enable the telnet service? (yes/no) [n]:
 Configure congestion/no credit drop for fc interfaces? (yes/no)
                                                                       [v]:
 Enter the type of drop to configure congestion/no_credit drop? (con/no)
[c]:
   Enter milliseconds in multiples of 10 for congestion-drop for port mode
F
    in range (<100-500>/default), where default is 500.
                                                         [d]:
   Congestion-drop for port mode E must be greater than or equal to
    Congestion-drop for port mode F. Hence, Congestion drop for port
   mode E will be set as default.
 Enable the http-server? (yes/no) [y]:
 Configure clock? (yes/no) [n]:
 Configure timezone? (yes/no) [n]: y
Enter timezone config [PST/MST/CST/EST] : <<var timezone>>
Enter Hrs offset from UTC [-23:+23] : <<var UTC offset>>
Enter Minutes offset from UTC [0-59] :
 Configure summertime? (yes/no) [n]:
  Configure the ntp server? (yes/no) [n]: y
   NTP server IPv4 address : <<var_global_ntp_server_ip>>
 Configure default switchport interface state (shut/noshut) [shut]:
 Configure default switchport trunk mode (on/off/auto) [on]:
  Configure default switchport port mode F (yes/no) [n]:
 Configure default zone policy (permit/deny) [deny]:
 Enable full zoneset distribution? (yes/no) [n]:
  Configure default zone mode (basic/enhanced) [basic]:
The following configuration will be applied:
 password strength-check
  switchname mds-b
 interface mgmt0
    ip address <<var MDS B mgmt0 ip>> <<var MDS B mgmt0 netmask>>
   no shutdown
 ip default-gateway <<var MDS B mgmt0 gw>>
 ssh key rsa 2048 force
  feature ssh
 no feature telnet
 system timeout congestion-drop default mode F
  system timeout congestion-drop default mode E
  feature http-server
 clock timezone PST 0 0
 ntp server <<var_global_ntp_server_ip>>
 system default switchport shutdown
 system default switchport trunk mode on
 no system default zone default-zone permit
 no system default zone distribute full
 no system default zone mode enhanced
Would you like to edit the configuration? (yes/no) [n]:
Use this configuration and save it? (yes/no) [y]:
```

Enable Appropriate Cisco MDS Features and Settings

Cisco MDS A and B

1. The following commands enable feature on both switches:

config

feature npiv feature fport-channel-trunk

Enable VSANs and Create Port channel

Cisco MDS A

- 1. Create Port Channel that will be uplinked to the fabric interconnect interface port-channel 1.
- 2. Create a VSAN and assign interfaces to it. Ports assigned to the port channel will also be in this Vsan. Configure the ports up.

```
vsan database
vsan <<var_vsan_a_id>>
vsan <<var_vsan_a_id>> interface fc1/1-2
vsan <<var_vsan_a_id>> interface po1
interface fc1/1-2
no shut
```

3. Activate the port channel.

۵, Note

The port channel ports will not be connected until the Fabric Interconnect is configured.

```
interface port-channel 1
channel mode active
switchport rate-mode dedicated
4. Assign interfaces to the port channel and save the config.
interface fc1/3-4
port-license acquire
channel-group 1 force
no shutdown
exit
copy run start
```

```
Note
```

You can run a "show int br" to validate the interfaces 1-4 are in the proper VSAN.

Cisco MDS B

- 1. Create Port Channel that will be uplinked to the fabric interconnect interface port-channel 2
- 2. Create a VSAN and assign interfaces. Ports assigned to the port channel will also be in this

```
vsan.
vsan database
vsan <<var_vsan_b_id>>
vsan <<var_vsan_b_id>> interface fc1/1-2
vsan <<var_vsan_b_id>> interface po2
interface fc1/1-2
no shut
```

3. Activate the port channel

Note

The port channel ports will not be connected until the Fabric Interconnect is configured.

```
interface port-channel 2
channel mode active
switchport rate-mode dedicated
```

4. Assign interfaces to the port channel and save the config.

```
interface fc1/3-4
  port-license acquire
  channel-group 2 force
  no shutdown
exit
copy run start
```

```
<u>Note</u>
```

You can run a "show int br" to validate the interfaces 1-4 are in the proper VSAN.

Storage Configuration

Secure Web Access to the IBM Storwize V7000 Service and Management GUI

Browser access to all system and service IPs is automatically configured to connect securely using HTTPS and SSL. Attempts to connect via HTTP will get redirected to HTTPS.

The system generates its own self-signed SSL certificate. Upon 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.

IBM Storwize V7000 Initial Configuration Setup

- 1. Configure an Ethernet port of a PC/laptop to allow DHCP to configure its IP address and DNS set.
- 2. Connect an Ethernet cable from the PC/laptop Ethernet port to the Ethernet port labelled "T" on the rear of either node canister in the V7000 control enclosure.



3. A few moments after the connection is made, the node will use DHCP to configure the IP address and DNS settings of the laptop/PC.



This will likely disconnect you from any other network connections you have on the laptop/PC. If you don't have DHCP on your PC/laptop, you can manually configure it with the following network settings: IPv4 address 192.168.0.2, mask to 255.255.255.0, gateway to 192.168.0.1, and DNS to 192.168.0.1

- 4. Open a browser and go to address https://install which will direct you to the initialization wizard.
- 5. When asked how the node will be used, select "As the first node in a new system."

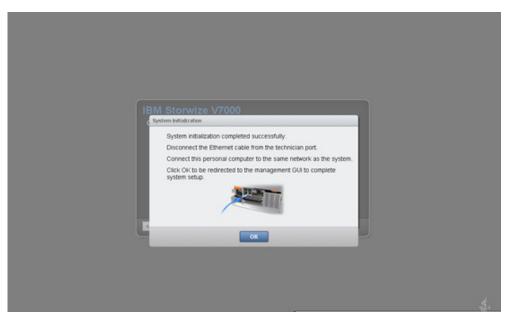
IBM Storwize V7000			
Welcome			
This wizard creates a new system or provides instructions on how to expand an existing system.			
system?			
	-		
Next >			
	This witzerd creates a new system or provides instructions on how to expand an existing system. Are you configuring the first control enclosure in a new system? • Yes • No	Welcome This wizard creates a new system or provides instructions on how to expand an existing system. Are you configuring the first control enclosure in a new system? • Yes	Welcome This wizard creates a new system or provides instructions on how to expand an existing system. Are you configuring the first control enclosure in a new system? • Yes

6. Follow the instructions that are presented by the initialization tool to configure the system with a management IP address <<var_cluster_mgmt_ip>>,<<var_cluster_mgmt_mask>> and <<var_cluster _mgmt_gateway>>.

I

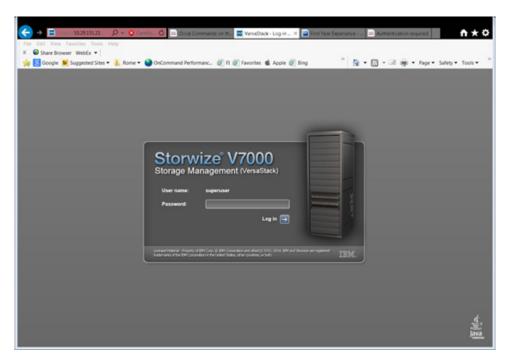
Forder * Con-	J* Phase: Dall	DLS-SVT	ds-stl-d.,	dallas-sxt2	Croups an	STG UK US	B multipath	DLS-SVT	A Raising A.S	ds-sx1-cl_	TMS/Dalla_	System	L ×	+	• 100	0	x
🔄 🔒 https://install/ie	evice/								C Q, Searc	h			☆ 0	4	† (9-	=
					System Initializa	ation			×								
					Create a	New System											
					@ Pvi	-											
					IP address												
					Subnet mask												
					Gateway.												
						4 840		Cano									
									_								

7. After you complete the initialization process, disconnect the cable as directed, between the PC/laptop and the technician port, and re-connect to your network with your previous settings.



- 8. Click OK to redirect your browser to the management GUI, at the IP address you configured. Note: you may have to wait up to 5 minutes for the management GUI to start up and become accessible.
- 9. Login as superuser with password of passw0rd.

I

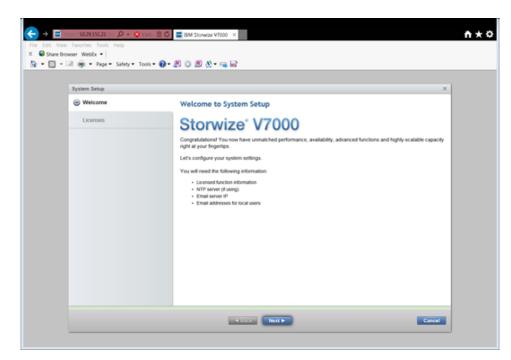


1

10. Change the password for superuser, then click Log In.

← → Ξ ===== 1028 151.21 == , 0 + ○ Caretor. C Ξ Versiónack + Log in ×	n+≎
File Edit View Favorites Tools Help X 🖨 Share Brosser WebEx •	
🚡 + 🖸 - 🗃 👼 - Page - Salety - Tools - 🕢 - 週 〇 遊 丛 - 瑞 🚔	_
Champing 1/7000	
Storwize V7000 Storage Management (VersaStack)	
New Passend	
Confirm Password	
Leg In 🗃	
The default preserved must be changed now.	
Lower Hamil Provide of PPLOGE DPLC Constant and Advect 2005, 2014. DPL of Known are regarded International the DPLC Constant on the Laked Data, they control, or both	
	<u></u>
	Java

11. On the welcome to system setup screen click Next.



Γ

12. Read and check agree to the license agreement, then click Next to proceed.

Welcome	License Addendum Java Notices Non-IBM Licenses Additional Licenses and Notices
o Helcomo	International Program License Agreement
 Licenses System License 	Part 1 - General Terms
Licensed Functions	BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN "ACCEPT" BUTTON, OR OTHERWISE USING THE PROGRAM, LICENSEE AGREES TO THE TERMS OF THIS AGREEMENT. IF YOU
System Name	ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU REPRESENT AND WARRANT THAT YOU HA' FULL AUTHORITY TO BIND LICENSEE TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS
Date and Time	* DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN "ACCEPT" BUTTON, OR USE THE PROGRAM; AND
Detected Enclosures	* PROMPTLY RETURN THE UNUSED MEDIA, DOCUMENTATION, AND PROOF OF ENTITLEMENT TO THE FROM WHOM IT WAS OBTAINED FOR A REFUND OF THE AMOUNT PAID. IF THE PROGRAM WAS
Email Event Notifications	DOWNLOADED, DESTROY ALL COPIES OF THE PROGRAM.
Configure Storage	 Definitions "Authorized Use" - the specified level at which Licensee is authorized to execute (
Summary	· (
	I agree with the terms in the license agreement.
	I do not agree with the terms in the license agreement.
	Back Nett Cancel

13. Enter the number for the licensed functions, then click Apply and Next. When the task completed window pops up and completes, click Close

		Licensed Licensed Functions Usersed System License - Licensed Functions Additional licenses are required to use certain system functions. On Storwice V7000 Gen2 systems, enclosure licenses are also required for the Eary Terr and Flash/Copy functions. These hos functions are based on the hord system and do not require and do not require and do not require and the provide system. For auditing purposes, estain the license agreement for proof of compliance. Date and Time Edental Vitualization: 7 Number of external encourses Remote Copy: 7 Number of external encourses Remote Copy: Bread Event Notifications Restime Compresson Number of enclosures	Licenses > System License > System License Addional licenses are required to use certain system functions. On Stowice V7000 Gen2 systems, enclosure licenses are ando required for the Lisary Ter and PlashCepy functions. These two functions are based on the hore system and do not require any additional required for on fis parent logistics. These two functions are based on the hore system my additional required for the case are made on the system. For auditing purposes, tetan the license agreement for proof of compliance. Date and Timo Extense Copy ? Number of extense Detected Enclosures Remote Copy ? Number of extense Email Event Notifications Readime Compression: ? Number of enclosures Configure Storage ?? Number of enclosures ?	Licenses Additional licenses are required to use certain system functions. On Stowice V7000 Gen2 systems, enclosure licenses are able required for the Easy Ter and PlashCopy functions. These two functions are based on the hord system and do not require any additional requires for use certain system functions. These two functions are based on the hord system any additional requires for the Easy Ter and PlashCopy functions. These two functions are based on the hord system any additional requires any additinted additional requires any additional requires any addi	Licenses - System License System License Licensed Functions Additional licenses are required to use certain system functions. On Stowice V7000 Gen2 systems, enclosure licenses are also required for the Easy Ter and FlashCopy functions. These two functions are based on the honor system and do not require any additional input on this panel to operate on the system. For auditing purposes, retain the license agreement for proof of compliance. Date and Timo
System License Additional licenses are required to use certain system functions. On Storwise V7000 Gen2 systems, enclosure licenses are also required for the Easy Ter and Fash/Copy functions. These two functions based on the horor system and do not require and additional system functions. These two functions based on the horor system and do not require and additional system functions. These two functions based on the horor system and do not require and additional system functions. These two functions based on the horor system and do not require and additional system. These two functions based on the horor system may be additional system functions. These two functions based on the horor system and do not require and the functions of extense agreement for proof of compliance. Date and Time Date and Time Date and Event Notifications Bending Copy: Thumber of extenses	System License Additional licenses are required to use certain system functions. On Stavuise VTGID Gen2 systems, Licensed Functions Licensed Functions exclusions functions are ablance required for the target frame of Earling functions. These two bunctions are based on the honor system and do not require any additional input on this panel to operate on the system. For auditing purposes, retain the license agreement for proof of compliance. Internet External Virtualization: 7 Internet for compliance External Virtualization: 7 Internet for compliance Bendle Copy: 7 Number of external enclosures Bead-time Compression 1	System License Additional licenses are required to use certain system functions. On Storeite VDDD Gen2 systems, elicensed Panctions solutions licenses are and provided to the required for the carry first and failed by first and	System Lienne Additional liennes are regimed to use certain system functions. On Storwise VTOD Gend systems, enclosure liennes are also regimed to use certain system functions. The store burnishon are based on the hours system and do not regime any additional input on this panel to genate on the system. System Name Date and Time Detected Enclosures Email Event Notifications Configure Storage Reader Copy Reader Copy Number of enclosures Reader Copy Number of enclosures	System Lisense Additional licenses are regulared to use certain system functions. On Stavuler Virtico Bach systems, enclosure iterates are also required to the system rear of Earliery functions. These the burnchos are based on the honor system and do not require any additional input on this panel to operate on the system. For auditing purposes, retain the license agreement for proof of compliance. Defected Enclosures Email Event Notifications Email Event Notifications Read-time Compression: 7 Number of enclosures Read-time Compression: 7 Number of enclosures	System License Licensed Functions Licensed Functions Licensed Functions Substruct VTOD GenC systems, enclosure Elements are also required to use certain system functions. On Storwise VTOD GenC systems, enclosure Elements are also required to use certain system functions. These the burchiso are based on the hours system and do not require any additional input on this panel to operate on the system. For additing purposes, retain the license agreement for proof of compliance. Defected Enclosures Email Event Notifications Configure Storage Readime Compression. T Number of enclosures
System Name For auditing purposes, retain the license agreement for proof of compliance. Date and Time External Visualization: 7 Number of external enclosures Remote Copy: 7 Small Event Notifications Remote Copy: 7	storm Name For auditing purposes, setain the license agreement for proof of compliance. External Virtualization: T Number of external enclosures Remote Copy: T Number of enclosures Rest/me Corpression	System Name For auditing purposes, setain the locense agreement for proof of compliance. Date and Time External Vhailization: 7 Detected Enclosures Remote Copy: 7 Email Event Notifications Read-time Compresson For enclosures	System Name For auditing purposes, retain the license agreement for proof of compliance. Date and Time Edemal Vehalization: 7 Detected Enclosures Remote Copy: 7 Email Event Notifications Readime Compressor: 7 Configure Storage Readime Compressor: 7	System Name For auditing purposes, retain the license agreement for proof of compliance. Date and Time External Vihalization. 7 Detected Enclosures Email Event Notifications 7 Email Event Notifications Real-time Congressor. 7 Number of enclosures Real-time Congressor. 7	System Name For auditing purposes, retain the license agreement for proof of compliance. Date and Time Edemal Whatsation: 7 Detected Enclosures Remote Copy: 7 Email Event Nutifications Readime Compressor: 7 Configure Storage Readime Compressor: 7
Defected Enclosures External Virtualization: 7 Number of external enclosures External Virtualization: 7 Number of enclosures External External Processing External Pro	Extense Visualization: 7 Number of extense exclusives Include Enclosures Remote Copy: 7 Number of enclosures all Event Notifications Residene Congression 9 number of enclosures	Detected Enclosures Email Event Notifications Email Event Notifications Email Event Notifications Resisting Corpresson Email Event Notifications Ema	Enternal Vinalization: 7 Number of external enclosures Defected Enclosures Remote Copy: 7 Number of enclosures Email Event Notifications Resideme Conpression: 7 Number of enclosures Configure Storage Resideme Conpression: 7 Number of enclosures	Defected Enclosures Exercise Vihialization: 7 Number of external enclosures Email Event Notifications Remote Copy: 7 Number of enclosures Configure Storage Real-time Compression: 7 Number of enclosures	Enternal Vinalization: 7 Number of external enclosures Defected Enclosures Remote Copy: 7 Number of enclosures Email Event Notifications Resideme Conpression: 7 Number of enclosures Configure Storage Resideme Conpression: 7 Number of enclosures
Y Number of extension Remote Copy: Number of exclosures Remote Copy: Number of exclosures	teched Enclosures Remote Copy: 7 Number of extensises Remote Copy: 7 Number of extensises Remote Copy: 7 Number of exclosures Read-time Congression	T Number of external enclosures Renote Copy T Number of enclosures Renote Copy T Number of enclosures Read-time Compression Read-time Compression	Detected Enclosures 7 Number of exclosures Email Event Notifications Remote Copy 7 Number of enclosures Configure Storage Real-time Compresson: 7 Number of enclosures	Defected Enclosures 7 Number of external enclosures Email Event Notifications Remote Copy: 7 Number of enclosures Configure Storage Real-time Compresson: 7 Number of enclosures	Detected Enclosures 7 Number of exclosures Email Event Notifications Remote Copy 7 Number of enclosures Configure Storage Real-time Compresson: 7 Number of enclosures
The Second Secon	al Event Notifications 7 Number of enclosures	Email Event Notifications T Number of enclosures Real-line Congression	Email Event Notifications 7 Number of enclosures Configure Storage 7 Number of enclosures	Email Event Notifications T Number of enclosures Configure Storage Real-time Compression T Number of enclosures	Email Event Notifications 7 Number of enclosures Configure Storage 7 Number of enclosures
Real-time Concession:	nfigure Storage 7 Number of enclosures	Configure Storage Realtime Compression 7 Number of enclosures	Configure Storage 7 Number of enclosures	Configure Storage 7 Number of enclosures	Configure Storage 7 Number of enclosures
2 Tonfigure Storage 7 Number of enclosures			Summary	Summary	Summary
Summary	mmary	Summary	outrine y		
Configure Storage 7 Number of enclosures	mmary	Summary	our many		

1

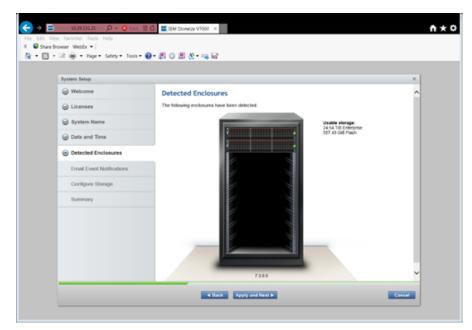
14. Change the system name if required then click Apply and Next.

System Setup	X
@ Welcome	System Name
⊘ Licenses	Enter a name for the system:
System Name	verapstack ×
Date and Time	
Detected Enclosures	
Email Event Notifications	
Configure Storage	
Summary	D2
Millin	
	Back Apply and Next Cancel

15. Click the NTP server button and enter the NTP server address. Click Apply and Next then view and close the tasks completed window.

System Setup			1
@ Welcome	Date and Time		
Ucenses System Name	Select time and date settings. Yo Time Protocol (NTP) server to sy	w can enter these settings manually or specify a Network nchronize time on the system.	
Oate and Time	 Manually 	NTP Server	
Detected Enclosures	1P address:	171.68.38.65	
Email Event Notifications	*Time Zone:	(OMT-8:00) US Pacific Time -	
Configure Storage			
Summary			

16. Validate the enclosures you have connected are properly detected. If there are any discrepancies please revisit the cabling section of this document. Click Apply and Next. View and close the tasks completed window.



17. Click Yes to input the email information for event notification.

Γ

System Setup		×
@ Welcome		
⊘ Licenses	Email Event Notifications	
System Name	Email alerts can be sent to the support center, your staff, or both. Call home automatically notifies the support center when events occur on your system and sends inventory	
-	reports. Support personnel can contact you to resolve these problems.	
Oate and Time	Do you want to set up email notifications, which includes call home?	
Obtected Enclosures	Yes No	
Email Event Notifications		
System Location		
Contact Details Email Servers		
Call Home		
Email Notifications		
Configure Storage		
Summary	0	

1

18. Fill out system location and contact details <<var_org>> <<var_street_address>>, <<var_city>> <<var_state>> <<var_zip>> <<var_country_code>>, then click Apply and Next. View and close the tasks completed screen.

System Setup		
@ Welcome		
C Licenses	System Location	
-	Enter the company name and address	to ship parts.
System Name	"Company name:	Cisco
 Date and Time 	"Street address:	275 East Java dr
Detected Enclosures		519 East Java or
Email Event Notifications	"City:	San Jose
 System Location Contact Details 	"State or province:	CA
Email Servers Call Home	"Postal code:	
Email Notifications	Postal Code:	99134
Configure Storage	"Country or region:	US -
Summary		

19. Insert Contact details. <<var_contact_name>> <<var_email_contact>> <<var_admin_phone>><<var_city>> Then Click Apply and Next and click close.

ø

System Setup		×
 Welcome Licenses System Name 	Contact Details Enter the name and contact information for the person in your organization that the support center can contact to help resolve problems on the system.	ď
O Date and Time	*Contact name:	
Detected Enclosures	*Email address:	
 Email Event Notifications System Location Contact Details Email Servers Call Home Email Notifications 	*Telephone (primary): Telephone (alternate): *Machine location:	
Configure Storage		
Summary		
	Back Apply and Next	Cancel

20. Input the email server IP address <<var_mailhost_ip>> and change the port if necessary, then click Apply and Next. View and close the task completed window. Click Apply and Next.

System Setup			×
@ Welcome	Email Servers		
G Licenses	Specify the IP address of at least one	email server that your company uses.	
System Name	IP Address	Server Port	
Obte and Time	173.36.13.143	25 00	
Detected Enclosures			
Email Event Notifications System Location Contact Details Email Servers Call Home Email Notifications			
Configure Storage			
Summary			

21. On the Call Home validation window, Click Apply and Next, then click Close.

Γ

System Setup			×
⊘ Welcome	Call Hor	ne	
G Licenses	Email notific	ation for the support center is automatically configured.	
⊘ System Name	Email: Type:	callhome1@de.ibm.com Errors Inventory	
Date and Time		inveniory	
O Detected Enclosures			
 Email Event Notifications System Location Contact Details Email Servers Call Home Email Notifications 			
Configure Storage			
Summary		8	
		Back Apply and Next ►	Cancel

1

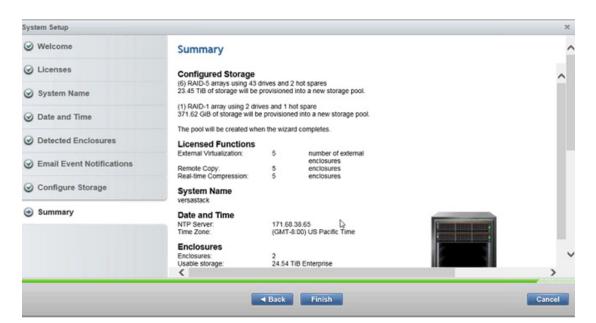
22. Enter the email addresses for all administrators that should be notified when issues occur as well and any other parties that need info or inventory <<var_email_contact>>. Click Apply and Next, then review and close the tasks completed screen.

the second s							
System Setup							×
@ Licenses	Email Notification	s					
-	Enter any local users to rece	eive notifica	tions when	events	OCCUP.		
 System Name 	Email Address my.email@mail.com	Enor	Warning ©	info	Inventory	00	
Ø Date and Time	corp_inventory@mail.com		õ	8		00	
Oetected Enclosures	(æ	8	00	
Email Event Notifications System Location Contact Details Email Servers Call Nome Email Notifications							
Configure Storage							
Summary							

23. Click Yes on the automatically configure internal storage now button, then Next.

System Setup			x
 Welcome Licenses System Name Date and Time Detected Enclosures 	Configure Storage Would you like to automatic	ally configure internal storage now?	^
Email Event Notifications Configure Storage Summary			
		Back Next ►	Cancel

24. Review the summary and click Finish. Review and close the tasks completed screen and click Close



25. Click Cancel to the Create Hosts popup, as these will be created after the Cisco Fabric Interconnects are configured. Optionally you can the view an introductory tour of the management gui using the link.

ſ

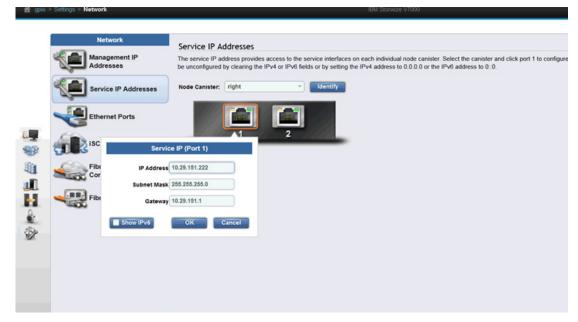
→ ■ 10.2033121 Ø × 10 Control File Edit View Flooriths Tools Help × ● Share Booser Weble × 1 Tools Tools № Page × Safety × Tools × <	 ☑ VensSlack-System × ☑ ④ ◎ Ø 处 • □ □ 	n ★⊅
VersaStack > Monitoring > System	IBM Storwize V7000	superuser (Security Administrator) 💠 🕥
	Task α After you have set up your system, configure settings for each host that is connected to some other than the system. Create Hosts	X
	Cancel	
Allocated, 8 bytes / 20, 30 (20, (2%)	3) Q Renting Tacks (/)	Rodh Stan

1

26. Click the settings icon in the lower left screen, and select the Network tab.

H	iscsi	
Ser and a series of the series	Fibre Channel Settings Event Notifications	
S.	Directory Services	Ś
	Support General	

27. Click the Service IP Addresses menu item on the left, and click the port 1 picture to enter the node management port IP address, Netmask and Gateway <<var_node01_mgmt_ip>> <<var_node01_mgmt_mask>> <<var_node01_mgmt_gateway>> then Click OK then Close.



28. Click the "Node Canister: " drop down menu item and change the selection to "left", and click the port 1 picture to enter the node management port IP address, Netmask and Gateway <<var_node02_mgmt_ip>> <<var_node02_mgmt_mask>> <<var_node02_mgmt_gateway>>. Click OK, then Close .

會 gpio > Settings > Network	IBM Storwize V7000
Addresses Addresses Service IP Addresses Ethernet Ports Isc	56.255.26.0

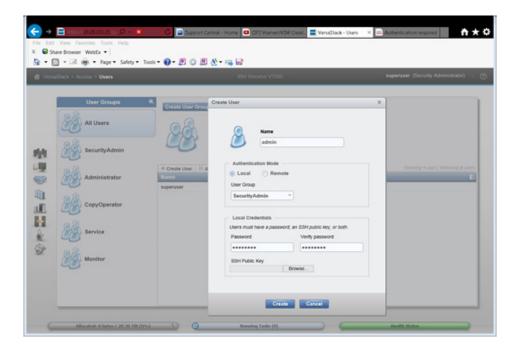
29. In the left menu, hover over each of the icons to become familiar with the GUI options.

I

Suggeste	d Tasks
	Pools Volumes by Pool Internal Storage External Storage
	MDisks by Pools System Migration
1	
	Overview
S.	Watch e-Learning: Overview

1

30. Create a separate administrator user, click the lock icon in the left pane, to open the Users pane. Click Create User, input user name <<var_admin>> and input a password <<var_password>>. Click Create, then Close.



- **31.** Log off by selecting the superuser account in the upper right pane, and clicking Log Out. Log back in using the admin account that was created.
- **32.** Click the 4th icon from the top in the left pane to access the Volumes pane. Click Create Volume in the top left to bring up the Create Volume wizard.

Create Values - Volume Create Values	Create Volume					×	outering 8 ve
Naroe				1			
	Generic	Thin-Provision	Minor	Thin Mirror	Compressed		
	When the first pre-existing install	compressed volume is cr ations, planning is required	eated, the performanc d to implement Real-tin	e of existing volumes r re Compression.	night be affected. In		
	Select a Pool						
	Name	A Status	Tree Core	Showing 1 c Capacity	poor Selecting @ poors		
	mdiskgrp0	V Online	and the second se	25 THE 20.25 THE			

33. Select Thin-Provision in the Select a Preset section. Select the mdiskgroup0 in the Select a Pool section.

+create Volumes - Volumes	ute Volume	IBM Storware V7000		admin. (Security Admensionator)
¥ Jano	Select a Preset	Free Capac Ca	Arror Compressor Arror Compressor Deserger (Joint Strategy of Joint Deserger (Joint Strategy of Joint Deserger (Joint Strategy of Joint Deserger (Joint Strategy of Joint Strategy of Joint Deserger (Joint Strategy of J	

ſ

34. To create SAN boot volumes for ESX, in the Volume Details section input: quantity 2, capacity 40GB, name VM-Host-Infra-0, and change the starting numbers 1. Click Create then click Close.

aStack > Volumes > Volumes	IEM Storwore V7000 admin (Security Administrato
Create Volume III Actio Name	Create Volume X ung divisions (Selecting div
	Select a Preset
	Genere Tain-Providen Minor Tain Minor Compressed
	Select a Pool
	Primary Poot indisage()
	Volume Details
	Quantity 2 Capacity 40 Gill * Name VM-Host-Infra-0 1 - 2
	Summary: 2 this-provisioned volumes, 80.00 Gi8 total virtual capacity, 1.60 Gi8 total real capacity, 20.35 T/8 thee in pool



If you plan to add the V7000 file modules and use NFS Datastores for your VM's, you can later delete the volumes created in the next steps after you migrate the VM's.

1

- **35.** To create a VMFS Datastore for Virtual Machines, click Create Volume, select Thin-Provision or another preset you desire, and select mdiskgroup0 for the pool.
- 36. Input quantity 1, capacity 500GB, and name infra_datastore_1. Click Create, then click Close.

VersaStack > Volumes > Volumes	IOM Storware V7000	admin (Security Administrator) (
Create Volume Marie Vid-Host-Intra-0 Vid-Host-Intra-0	Select a Preset Select a Preset Genero Tein-Prevision Afror Tein Mirror Compressed Select a Pool Primary Pool: Reading Details Quantity Capacity 600 Select a Pool Select a Pool Primary Pool: Capacity 600 Gasetty Select a Pool Capacity 600 Gasetty Select a Pool Capacity 600 Gasetty Capacity 600 Gasetty Select a Pool Capacity 600 Gasetty Capacity 600 Gasetty Capacity 600 Gasetty Select a Pool Gasetty Capacity 600 Gasetty Select a Pool Gasetty Capacity 600 Gasetty Capacity 600 Gasetty Capacity 600 Gasetty Gasetty Cap	

37. To create a swap file VMFS volume, click Create Volume, select Thin-Provision, input mdiskgrp0, quantity 1, capacity 100GB, and name infra_swap. Click Create, then click Close.

naŝ	Rock > Volumes > Volumes	10M Skorware V7000 admin (Secu	nty Administrator)
-	Craste Volume III Acto Nation Imita_datastore_1 VM-Host-Inftra-02 VM-Host-Inftra-02		
		Generic Thin-Provision Mirror Thin Mirror Compressed Select a Pool Primary Poot mdskupp0 CCC	
		Volume Details Quantity 1 2 Capacity 100 GB * Name Infina_sweity Sign Sign	

- **38.** Collect the information for the for the Fiber Channel WWPN's that will be used later for SAN boot by selecting hovering of the cog icon in the left pane to bring up the Settings menu, then click Network.
- 39. Select Fiber Channel Ports in the lower left menu, then expand ports 3 and 4 to show the WWPNs.



ſ

If you are deploying a block only system using all 4 fiber channel ports, also collect the information for port 1 and 2 and they will also be zoned to the FC switch.

	iscsi
Salar Salar	Fibre Chappel Settings Event Notifications
	Directory Services Network
	General

Net	work	Fibre	Channe	el Port	5			
Manag Addre	gement IP sses				tically across all nodes in the s is allowed to communicate with		ection determines with which systems the po ge systems.	rt is allowe
Saraja	e IP Addresses		ons Q	Filter				
	e il Auditesses	ID			System Connection	Node	WWPN	
5.001		۲	1		Any			
Ether	net Ports	۲	2		Any			
			э		Any			
600 ·····				э	Any	1(Left)	500507680B2320FC	
ISCSI				э	Any	2(Right)	500507680B2320FD	
			4		Any			
Fibre	Channel			4	Any	1(Left)	500507680B2420FC	
Conne								

40. Fill in the WWPN numbers in the chart below as they will be required later when configuring FC zones. The data for the Hosts will be collected later in this document. For example, ID 3 on node 1 in the above picture corresponds to FC_Node1-3 in the spreadsheet.

Table 20	WWPN's for IBM Storwize	V7000
----------	-------------------------	-------

Source	Switch Target	Variable	WWPN
FC_Node1-1			
FC_Node1-2			
FC_Node1-3	Switch A FC1	var_wwpn_Node1-switch-A	
FC_Node1-4	Switch B FC1	var_wwpn_Node1-Switch-B	
FC_Node2-1			
FC_Node2-2			
FC_Node2-3	Switch A FC2	var_wwpn_Node2-switch-A	
FC_Node2-4	Switch B FC2	var_wwpn_Node2-switch-B	
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	

Server Configuration

VersaStack Cisco UCS Base

Perform Initial Setup of Cisco UCS 6248 Fabric Interconnect for VersaStack Environments

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 6248 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 6248 fabric interconnect.

```
Enter the configuration method: console
Enter the setup mode; setup newly or restore from backup.(setup/restore)? Setup
You have choosen to setup a 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.

Cisco UCS 6248 B

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

4. Power on the 2nd module and connect to the console port on the second Cisco UCS 6248 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
```

Cisco UCS for IBM Storwize V7000

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 6248 fabric interconnect cluster address.
- 2. Click the Launch UCS Manager link to download the Cisco UCS Manager software.
- 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.

Upgrade Cisco UCS Manager Software to Version 2.2(3B)

This document assumes the use of Cisco UCS Manager Software version 2.2(3B). To upgrade the Cisco UCS Manager software and the UCS 6248 Fabric Interconnect software to version 2.2(3B), refer to Cisco UCS Manager Install and Upgrade Guides.

Add Block of IP Addresses for 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:

Note

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

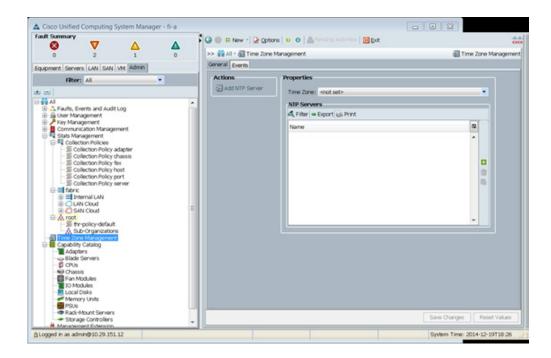
- 1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
- 2. Select Pools > root > IP Pools > IP Pool ext-mgmt.
- 3. In the Actions pane, select Create Block of IP Addresses.
- 4. Enter the starting IP address of the block and the number of IP addresses required, and the subnet and gateway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

Fault Summary	> ≡ LAN + ⊕ Pools + ▲ root + Ⅲ IF	
Equipment Servers LAN SAN VM Admin	General IP Addresses IP Blocks Fault	
Filter: Al Image: Construction of the second sec	Actions Create Block of IPv4 Addresses Create Block of IPv6 Addresses Create IPv6 Vi8/S Sonv Show Pool Usage	Properties Name: ext-mgnt Description: Gttb: exococool-ecce-ecce-eccece State: 0 Assignment Order: O Default Sequential
		Save Changes Reset Values
å Logged in as admin@10.29.151.12		System Time: 2014-12-19T18:

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.



Edit Chassis Discovery Policy

I

Setting the discovery policy simplifies the addition of B-Series Cisco UCS chassis and of additional fabric extenders for further C-Series connectivity.

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.
- 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 chassis or fabric extenders (FEXes) and the fabric interconnects.
- 4. Set the Link Grouping Preference to Port Channel.
- 5. Click Save Changes.
- 6. Click OK.

0 2 0 2 <th>ult Summary</th> <th>V</th> <th>Δ.</th> <th>4</th> <th></th> <th>Qptions 😜 📵 🛕 Pending</th> <th>ACTIVITIES 🛛 📴 Exit</th> <th></th> <th>:</th>	ult Summary	V	Δ.	4		Qptions 😜 📵 🛕 Pending	ACTIVITIES 🛛 📴 Exit		:
Imperient Servers LAN SAN VM Admin Ifter: All Imperiant NB Decommissioned Firmware Management Structures Imperiant Imperiant Imperiant Imperiant Structures Statuses Imperiant Imperiant Imperiant Imperiant Statuses Statuses <t< th=""><th>0</th><th>2</th><th>1</th><th>0</th><th>>> 🙀 Equipment</th><th></th><th></th><th></th><th>Equipme</th></t<>	0	2	1	0	>> 🙀 Equipment				Equipme
Filter: All Closes Closes Closes Closes Closes Server Discovery Polices Blade Server Discovery Polices Selver Discovery Polices Chassis/FEX Discovery Policy Actor: Allink Link Link Link Link Link Link Reck Server Discovery Policy Actor: Closes Server Discovery Policy Actor: Closes Closes Reck Server Discovery Policy Actor: Closes Reck Management Connection Policy Reck Management Connection Policy Actor: Closes Reck Management Connection Policy Actor: Closes	upment Server	LAN SAN	VM Admin						
Consistence Consisten									
Save Changes Reset Values	Rack-Mou	5			Link Grouping Pri Rack Server Di Acton: Scrub Policy: Rack Managem Acton: Auto Power Policy Redundancy: MAC Address T Aging Time: Global Power A Allocation Metho	Actor: 4 Link efference: None Port Chi scovery Policy Immediate User Admowled ot set> Pert Connection Policy Admowledged User Admowledged Nen Redundant N+1 able Aging Never Mode Default oth location Policy d: Manual Blade Level Cap	tgad viedgad ad • Policy Driven Chassis Group Cap	Save Changes	Reset Values

1

Enable Server and 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 the ports that are connected to the chassis and / or to the Cisco 2232 FEX (two per FEX), right-click them, and select Configure as Server Port.

ault Summary	A A	G 🔘 🛙 Ne	w • 🖵 Qptions 😜	0	nding Activities 🛛 📴 Exit	*
v v	1 0	>> iii Equip	ment • 🚥 Fabric Interc	connects ·	E Fabric Interconnect A (primary) • E Fixed Module • - Eth	ernet Ports + -
quipment Servers LAN	SAN VM Admin	General Fa	ults Events FSM Sta	tistics		
filter: A		Fault Su	mmary		Physical Display	
		8	V 🛆		and the second	
Equipment		0	0 0	0	STREET	
- Chassis		Status			📕 Up 🧱 Admin Down 📕 Fail 🔜 Link Down	
- FEX		Overall !	Status: 4 Admin Dow	m	Properties	
Servers	cts		al Info: Administratively	y down	ID: 1 Slot ID: 1	
Fabric Interco Fixed Mod	nnect A (primary)	Admin	State: Disabled		User Label:	
E - Etherne		Actions			MAC: 00:2A/6A/CD/F0/EB	
Por	LAN Uplinks Manager		Pert		Mode: Access Port Type: Physical Role: Unconfigured	
Por	ti manala interior		e Port			
Por Por			fare		Transceiver	
- Por	tt Dirable		la.m		Type: HEBGB CUSH Model: 1-2853783-2	
Por Por	Configure as Server P	ort	Interface		Vendor: CISCO-TYCO	
Por Por		ort			Serial: TED101701RC	
Por	t : Configure as FCoE Up	link Port				
Por Por	t Conligure as PCOE Sit					
- Por	Configure as Applian	ce Port				
Por Por	enreeningare					
Port Port						
Por	Lincontinues SColl Sta					
Por Por	t.					
- Por	Linconfigure hoth					
Pon	ti	Ctrl+C			Save Charges	Bonet Values

- 5. Click Yes to confirm server ports and click OK.
- 6. Verify that the ports connected to the chassis and / or to the Cisco 2232 FEX are now configured as server ports.

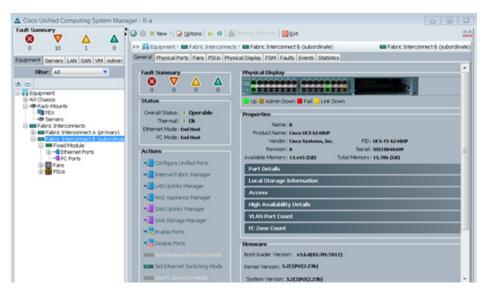
mary A	G 🔘 🛙 No	w - 📿 Options	● ● ▲Pending /	ctivites 🔯	Exit			
6 1 1	>> 👬 Equip	ment • 🖿 Fabric	Interconnects + 🚥 Fab	oric Interconne	ect A (primary) +	Fixed Module Et	hernet Ports EFeed	Mo
	Ethernet P	orts						-
Servers LAN SAN VM Admin	d Fibr +1	boort dis Print of	Role: + Mall Mun	configured 🔽	Network Serv	er 🖌 ECoE Uniek 🖌	Unified Uplink 🔽 Appliance	-
Filter: Al 💌				-				
	Skit	Port ID	MAC	If Role	If Type	Overall Status	Administrative State	
	1	1	00:2A:6A:CD:F		Physical	t Up	t Enabled	
- Center Ports - Cen	1	2	00:2A:6A:CD:F	. Server	Physical	t Up	I Enabled	
Port 2								
Port 3								
Port 4								
Port 5								
- Port 6								
Port 7								
Port 8								
Port 9								
Port 10								
Port 11								
Port 12								
Port 12 Port 13								
Port 12 Port 13 Port 14								
Port 12 Port 13 Port 14 Port 15								
Port 12 Port 13 Port 13 Port 15 Port 15 Port 16								
Port 12 Port 13 Port 14 Port 15 Port 16 Port 16								
- Port 12 - Port 13 - Port 14 - Port 15 - Port 15 - Port 16 - Port 18								
- Port 12 - Port 13 - Port 14 - Port 15 - Port 15 - Port 15 - Port 16 - Port 19 - Port 19								
 Port 12 Port 13 Port 14 Port 15 Port 16 Port 17 Port 18 								
Port 12 Port 13 Port 14 Port 14 Port 15 Port 15 Port 17 Port 17 Port 18 Port 19 Port 20								
Port 12 Port 13 Port 14 Port 14 Port 15 Port 16 Port 16 Port 17 Port 18 Port 19 Port 20 Port 21								
Port 12 Port 13 Port 13 Port 14 Port 15 Port 15 Port 16 Port 17 Port 19 Port 19 Port 20 Port 22 Port 23								
Port 12 Port 14 Port 14 Port 15 Port 15 Port 16 Port 19 Port 19 Port 20 Port 20 Port 21 Port 22 Port 23 Port 24								
#123 #113 #114 #115 #115 #116 #117 #118 #119 #120 #122 #122 #122 #122 #122 #125								
Port 12 Port 13 Port 14 Port 15 Port 15 Port 15 Port 19 Port 19 Port 20 Port 22 Port 22 Port 22 Port 23 Port 24 Port 25 Port 25								
Port 12 Port 13 Port 14 Port 15 Port 15 Port 16 Port 17 Port 10 Port 20 Port 20 Port 22 Port 22 Port 22 Port 24 Port 24 Port 24 Port 25 Port 26 Port 26 Por								
Port 12 Port 13 Port 14 Port 15 Port 15 Port 15 Port 16 Port 10 Port 10 Port 20 Port 22 Port 22 Port 23 Port 25 Port 25 Port 25 Port 27								
Port 12 Port 13 Port 14 Port 15 Port 15 Port 16 Port 19 Port 20 Port 22 Port 22 Port 22								
rt 12 rt 13 rt 14 rt 14 rt 15 rt 16 rt 16 rt 16 rt 17 rt 18 rt 19 rt 20 rt 21 rt 22 rt 23 rt 24 rt 24 rt 25 rt 25 rt 25 rt 27 rt 25 rt 27 rt 29 rt 29								
12 13 14 15 16 17 18 19 10 10 12 12 14 15 16 17 18 19 10 10 10 10 10 10 10 14 15 16 17 19 19 14 15 16 17 10 14 15 16 16 17 10 16 17 10 16 17 10 16 17 10 16 17 10 16 17 10 16 17 10 16 17 10 16 17 10 16 17 10 10 10 10 10 10 10 10 10 10 10 10 10								
12 13 14 14 15 15 16 17 19 20 22 23 23 24 25 24 25 26 27 28							ve Charges] [Reset Va	

- 7. Select ports 25 and 26 that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.
- 8. Click Yes to confirm uplink ports and click OK.
- 9. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.
- 10. Expand Ethernet Ports.
- 11. Select the ports that are connected to the chassis or to the Cisco 2232 FEX (two per FEX), right-click them, and select Configure as Server Port.
- 12. Click Yes to confirm server ports and click OK.
- 13. Select ports 25 and 26 that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.
- 14. Click Yes to confirm the uplink ports and click OK.

Enable Fibre Channel Ports

To enable server and FC uplink 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 B which should be the subordinate FI, and select Configure Unified Ports, Click Yes.



2. Slide the lever to change the port 31-32 to change the ports to Fiber Channel. Click Finish then Yes to the reboot message. Click OK.

1

configu	re Fixed Mo	dule Ports		
-dealer and			· · · · · · · · · · · · · · · · · · ·	
cite				
		anten an berten berten berten ber		
		0		
Instructio	ns			
	The position of the	a slider determines the type of the ports.		
			a marke to the sight and Fiber Channel much (Durch)	
			e ports to the right are Fibre Channel ports (Purple).	
Doet	All the ports to the	e left of the slider are Ethernet ports (Blue), while th		
	All the ports to the Transport	e left of the slider are Ethernet ports (Blue), while the If Role or Port Channel Membership	e ports to the right are Fibre Channel ports (Purple). Desired If Role	
Port 18	All the ports to the Transport jether	e left of the slider are Ethernet ports (Blue), while th If Role or Port Channel Membership Unconfigured		-
Port 18 Port 19	All the ports to the Transport ether ether	e left of the slider are Ethernet ports (Blue), while th If Role or Port Channel Membership Unconfigured Unconfigured		ŀ
Port 18 Port 19 Port 20	All the ports to the Transport ether ether ether	e left of the slider are Ethernet ports (Blue), while th If Role or Port Channel Membership Unconfigured Unconfigured Unconfigured		ľ
Port 18 Port 19 Port 20 Port 21	All the ports to the Transport ether ether ether ether	a left of the slider are Ethernet ports (Blue), while th If Role or Port Channel Membership Unconfigured Unconfigured Unconfigured		ľ
Port 18 Port 19 Port 20 Port 21 Port 22	All the ports to the Transport other other other other other	e left of the slider are Ethernet ports (Blue), while th If Role or Port Channel Membership Unconfigured Unconfigured Unconfigured Unconfigured		ľ
Port 18 Port 19 Port 20 Port 21 Port 22 Port 23 Port 23	All the ports to the transport efter efter efter efter efter efter efter	a left of the slider are Ethernet ports (Bkae), while th If Role or Port Channel Membership Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured		ľ
Port 18 Port 19 Port 20 Port 21 Port 22 Port 23 Port 24	All the ports to the other ether ether ether ether ether ether ether ether	a left of the slider are Ethernet ports (Blue), while th If Role or Port Channel Membership Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured		
Port 18 Port 19 Port 20 Port 21 Port 22 Port 23 Port 24 Port 25	All the ports to the Transport ether ether ether ether ether ether ether ether ether ether ether ether	e left of the slider are Ethernet ports (Blue), while th If Role or Port Channel Membership Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Ethernet Uplink		
Port 18 Port 19 Port 20 Port 21 Port 22 Port 23 Port 24 Port 25 Port 26	All the ports to the Transport lether lethe	a left of the slider are Ethernet ports (Bkae), while th If Role or Port Channel Membership Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Ethernet Uplink Ethernet Uplink		
Port 18 Port 19 Port 20 Port 21 Port 22 Port 23 Port 23 Port 24 Port 25 Port 25 Port 26 Port 27	All the ports to the Transport other other other other other other other other other other other other	a left of the silder are Ethernet ports (Blue), while th If Role or Port Channel Membership Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Ethernet Uplink Ethernet Uplink		
Port 18 Port 19 Port 20 Port 21 Port 22 Port 23 Port 23 Port 24 Port 25 Port 25 Port 26 Port 27 Port 28	All the ports to the Transport other ether ether ether ether ether ether ether ether ether ether ether ether	a left of the slider are Ethernet ports (Bkae), while th If Role or Port Channel Membership Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Ethernet Uplink Ethernet Uplink Unconfigured Unconfigured		
Port 18 Port 19 Port 20 Port 21 Port 22 Port 23 Port 24 Port 25 Port 25 Port 25 Port 26 Port 27 Port 28 Port 29	All the ports to the Transport other othe	a left of the slider are Ethernet ports (Blue), while th If Role or Port Channel Membership Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Ethernet Uplink Ethernet Uplink Unconfigured Unconfigured Unconfigured Unconfigured		
Port 18 Port 19 Port 20 Port 21 Port 22 Port 23 Port 23 Port 24 Port 25 Port 26 Port 26 Port 27 Port 28 Port 29 Port 30	All the ports to the Transport other othe	left of the slider are Ethernet ports (Blue), while th If Role or Port Channel Membership Unconfigured Unconfigured	Desired If Role	
Port 18 Port 19 Port 20 Port 21 Port 22 Port 23 Port 24 Port 25 Port 25 Port 25 Port 25 Port 27 Port 28 Port 29	All the ports to the Transport other othe	a left of the slider are Ethernet ports (Blue), while th If Role or Port Channel Membership Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Unconfigured Ethernet Uplink Ethernet Uplink Unconfigured Unconfigured Unconfigured Unconfigured		

- 3. When the subordinate has completed reboot, select the Fabric Interconnect A, (primary), then select Configure Unified Ports, and click Yes.
- 4. Slide the Bar to the left to select ports 31-32 for FC (purple), click finish, and say Yes to the reboot message. You will need to re-login to the client after the reboot of the FI completes

Create VSAN for the Fibre Channel Interfaces

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

- 1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
- 2. Expand the SAN > SAN Cloud tree. Then fabric A
- 3. Right-click VSANs.
- 4. Choose Create VSAN.
- 5. Enter VSAN_A as the name of the VSAN for fabric A.
- 6. Keep the Disabled option selected 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 OK again.

Create VSAN	0
Name: VSAN_A FC Zoning Settings FC Zoning: Olisabled Enabled	
Do NOT enable local zoning if fabric interconnect is Ocommon/Global	
You are creating a global VSAN that maps to the same VSAN ID in all available fabrics.	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. On the SAN tab, expand SAN, SAN Cloud, Fabric-B and Right-click VSANs.
- 11. Right-click Vsans and choose Create VSAN.
- 12. Enter VSAN_B as the name of the VSAN for fabric B.
- 13. Keep the Disabled option selected for FC Zoning.
- 14. Click the Fabric B radio button.

ſ

15. 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, then click OK and OK.

1

▲ Create VSAN		83
Create VSAN		0
		_
Name: VSAN_B		
FC Zoning Settings		
FC Zoning: O Disabled C Enabled		
Do NOT enable local zoning if fabric interconnect	t is connected to an upstream FC/FCoE switch.	
Common/Global	Both Fabrics Configured Differently	
You are creating a global VSAN that maps to the same VSAN ID in all available fabrics.	A VLAN can be used to carry FCoE traffic and be mapped to this VSAN.	l can
Enter the VSAN ID that maps to this VSAN.	Enter the VLAN ID that maps to this VSAN.	
VSAN ID: 102	FCoE VLAN: 102	
0	0	
	ОКСа	incel

Create Port Channels for the Fibre Channel Interfaces

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

Fabric-A

- 1. In the navigation pane, under SAN > SAN Cloud, expand the Fabric A tree.
- 2. Right-click FC Port Channels
- 3. Choose Create Port Channel.
- 4. Enter 1 for the port channel ID and Po1 for the port channel name.
- 5. Click Next then choose ports 31 and 32 and click >> to add the ports to the port channel. Click Finish.

sate Port Channel	Add Port	ts							
1. √ <u>SetPortChannel</u> <u>Name</u> 2. √ <u>Add Ports</u>	Port Channel	Port Channel Admin Speed: Auto							
	Ports		_			Ports in the	port channel	_	i.
	Port	Skot ID	WWPN			Port	Slot ID	WWPN	5
	F			*		31 32	1	20:1F:00:24:6A 20:20:00:24:6A	
	Silot ID:					Details Slot ID:			

6. Check the check box for Show Navigator for FC Port-Channel 1 (Fabric A).

Create	Port Channel
i	Successfully created FC Port-Channel 1 (Fabric A).
	ОК

7. Under the Vsan drop-down, select vsan 101.

tatus Overall Status: 💙 Failed Idditional Info: No operational members	Properties ID: 1 Fabric ID: A	
Ctions End-to Port Channel Cosable Port Channel	Port Type: Aggregation Transport Type: Fc Name: ool Description: VSAN: Fabric A/rsan 101 (101) Port Channel Admin Speed: Auto Operational Speed:(Zpp): 0	

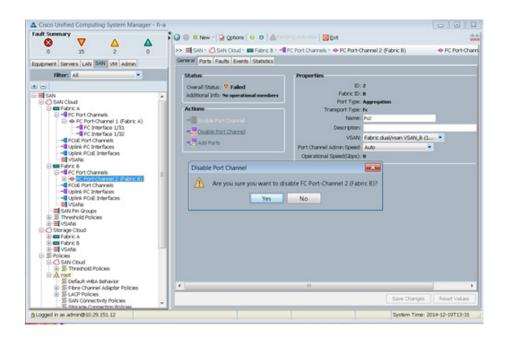
- 8. Click Apply, and then click OK.
- 9. Click OK to close the navigator.

Fabric-B

Γ

1. Click the SAN tab. In the navigation pane, under SAN > SAN Cloud, expand the Fabric B tree.

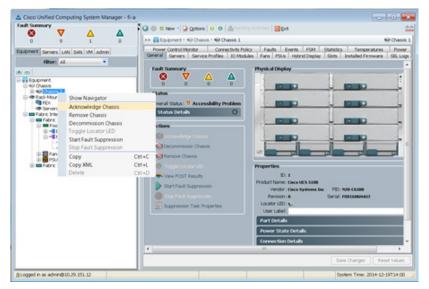
- 2. Right-click FC Port Channels
- 3. Choose Create Port Channel.
- 4. Enter 2 for the port channel ID and Po2 for the port channel name.
- 5. Click Next.
- 6. Choose ports 31 and 32 and click >> to add the ports to the port channel.
- 7. Click Finish.
- 8. Check the check box for Show Navigator for FC Port-Channel 2 (Fabric b).
- 9. Under the Vsan drop-down, select VSAN 102, click Apply, click OK.
- **10.** To initialize a quick sync of the connections to the MDS switch, right click the port channel created, and select disable port channel, then re-enable the port channel. Repeat this step for the port channel created for Fabric-A.



Acknowledge Cisco UCS Chassis and FEX

To acknowledge all Cisco UCS chassis and external 2232 FEX modules, 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 each chassis and select Acknowledge Chassis, click Yes, then click OK.



- 4. If C-Series servers are part of the configuration, expand Rack Mounts and FEX.
- 5. Right-click each FEX that is listed and select Acknowledge FEX.

Cisco Unified Computing System Manager	kef1-uc1		
Pitter: Al ▼ Colponet 0 0 Solution 0 0 States 0 0 Overal Status 0 0 States 0 0			
	>> 👬 Equipment + 🐲 Radi-Hounts + 🐚 PEX + 🐚 PEX 2	1	REX 2
pupment Servers LAW SAN VM Admin	General Fabric Ports Bacigiane Ports Fans 30 Modules	PSUs Connectivity Policy Faults Events PSM Statistics	
		cal Display	
Easpment	0 0 0 0		
Rechildren R	Coverd Status: Coverd Status Status Details Note: N/A Volkage: N/A Thermal: N/A Actions Status Price Status Price N/A Thermal: N/A Coverd Status N/A Coverd N/A Coverd N/A	ID: 2 ct Name: Caco Nesus 2232TP Vinder: Osco Systems PEI: N2K-C2 Revision: 0 Serial Number (SN): SSI152 ator UED: •	0 0
		Save Changes	Reset Values
Logged in as admin@192.168.175.44		System Time: 200	2-07-26710-50

Create Uplink Port Channels to Cisco Nexus Switches

ſ

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.

Note

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		×
Unified C	omputing System Manager	
Create Port Channel	Set Port Channel Name	0
1. VSet Port Channel Name		
2. Add Ports		
	ID: 13	
	0	
	Name: VPC-13-Nexus	-
	0	
	< Prev Next > Finish Can	cel

- 8. Select the following ports to be added to the port channel:
- Slot ID 1 and port 25
- Slot ID 1 and port 26
- 9. Click >> to add the ports to the port channel.
- 10. Click Finish to create the port channel.
- 11. Click OK.
- 12. In the navigation pane, under LAN > LAN Cloud, expand the fabric B tree.

- 13. Right-click Port Channels.
- 14. Select Create Port Channel.
- 15. Enter 14 as the unique ID of the port channel.
- 16. Enter vPC-14-NEXUS as the name of the port channel.
- 17. Click Next.
- 18. Select the following ports to be added to the port channel:

- Slot ID 1 and port 25
- Slot ID 1 and port 26
- **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

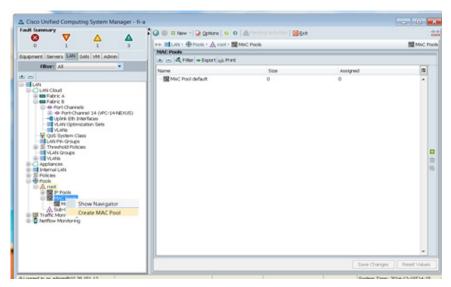
To configure the necessary MAC address pools for the Cisco UCS environment, complete the following steps:

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

Note

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



I

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 a Block of MAC Addresses	×
Create a Block of MAC Addresses	0
First MAC Address: 00:25:85:07:0A:00 To ensure uniqueness of MACs in the LAN fabric, you are strongly encouraged to use the following MAC prefix: 00:25:85:xx:xx:xx	Size: 32 🚍
	OK Cancel

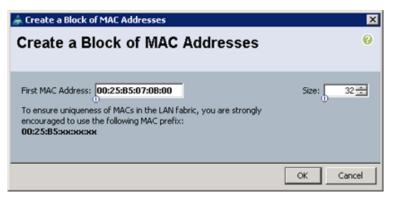
- 11. Click OK.
- 12. Click Finish.
- 13. In the confirmation message, click OK.
- 14. Right-click MAC Pools under the root organization.
- 15. Select Create MAC Pool to create the MAC address pool.
- **16.** Enter MAC_Pool_B as the name of the MAC pool.
- 17. Optional: Enter a description for the MAC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

Note

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.

I



- 22. Click OK.
- 23. Click Finish.

24. In the confirmation message, click OK.

Create UUID Suffix Pool

To configure the necessary universally unique identifier (UUID) suffix pool for the Cisco UCS environment, 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 a Block of UUID Suffixes	×
Create a Block of UUID Suffixes	0
From: 0000-00000000001 Size: 32	
- -	
	. 1
OK Can	cel

- 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 management cluster and click >> to add them to the Infra_Pool server pool.
- 9. Click Finish.
- 10. 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.

reate VLANs			
VLAN Name/Prefix: IB-MGMT-VLAN			
ulticast Policy Name: <not set=""> T 🔛 Create Multicast Policy</not>			
Common/Global C Fabric A C Fabric B C Both Fabrics Configured Differently			
ou are creating global VLANs that map to the same VLAN IDs in all available fabrics.			
Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")			
VLAN IDs: 3175			
haring Type: 💽 None 🔿 Primary 🔿 Isolated			
	Check Overlap	OK G	

10. Right-click VLANs.

- **11.** Select Create VLANs
- 12. Enter NFS-VLAN as the name of the VLAN to be used for NFS.
- 13. Keep the Common/Global option selected for the scope of the VLAN.
- 14. Enter the <<var_nfs_vlan_id>> for the NFS VLAN.
- 15. Keep the Sharing Type as None.
- 16. Click OK, and then click OK again.
- 17. Right-click VLANs.

I

- **18.** Select Create VLANs
- 19. Enter vMotion-VLAN as the name of the VLAN to be used for vMotion.
- 20. Keep the Common/Global option selected for the scope of the VLAN.
- 21. Enter the <<var_vmotion_vlan_id>> as the ID of the vMotion 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 VM-Traffic-VLAN as the name of the VLAN to be used for the VM traffic.
- 27. Keep the Common/Global option selected for the scope of the VLAN.
- **28.** Enter the <<var_vm-traffic_vlan_id>> for the VM Traffic VLAN.
- **29.** Keep the Sharing Type as None.
- 30. Click OK, and then click OK again.
- 31. Right-click VLANs.
- 32. Select Create VLANs
- 33. Enter Native-VLAN as the name of the VLAN to be used as the native VLAN.
- 34. Keep the Common/Global option selected for the scope of the VLAN.
- **35.** Enter the <<var_native_vlan_id>> as the ID of the native VLAN.
- **36.** Keep the Sharing Type as None.
- 37. Click OK and then click OK again.
- **38.** Expand the list of VLANs in the navigation pane, right-click the newly created Native-VLAN and select Set as Native VLAN.
- 39. Click Yes, and then click OK.

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 2.2(3b) for both the Blade and Rack Packages.
- 8. Click OK to create the host firmware package.
- 9. Click OK.

Create Host Firmware Pa	ackage	83
reate Host Firmwa	are Package	6
Name: VM-Host-Infra		
Description:		
	How would you like to configure the Host Firmware Package? Simple Advanced 	
Blade Package: 2.2(3b)B	<u> </u>	
Rack Package: <not set=""></not>	•	
		CK Cancel

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 OK.

ſ

ult Summary		🔾 🔘 🗖 New -	Optio		0 APending		et .			-+
🛛 🗸 🖉 🖉	8									
0 2 1 3		>> = LAN • ()		1. H Ø	75 System Class				_	QOS System Clas
upment Servers LAN SAN VM Admin		General Events	FSM							
Filter: All		Priority	Enabled	Co5	Packet Drop	Weight	Weight (%)	MTU		Multicast Optimize
e		Platinum		5		10	 N/A 	normal	۲	
I LAN	-	Gold		4	V	9	 N/A 	normal	*	
CAN Cloud Could Coul		Silver		2	V	8	• N/A	normal	•	
Fabric B GoS System Class		Bronze		1	V	7	• N/A	normal		
LAN Pin Groups		Best Effort		Any		5	• 50	9216	•	
VLAN Groups		Fibre Channel		3		5	* 50	fc		N/A
Binternal Fabric B Binternal Fabric B Bintershold Policies Policies Policie Cud Difference D										

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.

Note

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.

A Create Local Disk Configuration Policy	×
Create Local Disk Configuration Policy	0
	_
Name: SAN-Boot	
Description:	
Mode: No Local Storage	
FlexFlash	
FlexFlash State: O Disable C Enable	
If FlexFlash State is disabled, SD cards will become unavailable immediately. Please ensure SD cards are not in use before disabling the FlexFlash State.	
FlexFlash RAID Reporting State: O Disable C Enable	
OK	Cancel

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.

ſ

- 3. Right-click Network Control Policies.
- 4. Select Create Network Control Policy
- 5. Enter Enable_CDP as the policy name.
- 6. For CDP, select the Enabled option.
- 7. Click OK to create the network control policy.

🌲 Create Network C	ontrol Policy	×
Create Netw	ork Control Policy	0
Name:	Enable_CDP	
CDP:	C Disabled C Enabled	
MAC Register Mode:	Only Native Vlan C All Host Vlans	
Action on Uplink Fail:	Link Down C Warning	
MAC Security		
Forge: Allow	C Deny	
		OK Cancel

8. Click OK.

Create Power Control Policy

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

1

- 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	×
Create Power Control Policy	0
-	
Name: No-Power-Cap	
Description:	
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 Capi C cap	
Cisco UCS Manager only enforces power capping when the servers in a power group require more power	r
than is currently available. With sufficient power, all servers run at full capacity regardless of their priority.	
OK Canc	el

Create Server Pool Qualification Policy (Optional)

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



ſ

This example creates a policy for a B200-M3 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-M3 as the name for the policy.
- 6. Select Create Server PID Qualifications.
- 7. Enter UCSB-B200-M3 as the PID.
- 8. Click OK to create the server pool qualification policy.
- 9. Click OK, and then click OK again.

Create Server Pool Policy Qualification		×
Create Server Pool Polic	y Qualification	0
Naming Name: UCS-B200-M3 Description: This server pool policy qualification will apply	o new or re-discovered servers. Existing servers are not qualified until they are re-discovered	
Actions	Qualifications	
Create Adapter Qualifications Create Chassis/Server Qualifications Create Memory Qualifications Create CPU/Cores Qualifications Create Storage Qualifications Create Server PID Qualifications Create Power Group Qualifications Create Rack Qualifications	Create Server PID Qualifications Create Server PID Qualifications Create Server PID Qualifications Output Output	
	PID (RegEx): UCS-8200-M3	8
	ОК Са	ncel

1

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 Finish to create the BIOS policy.
- 8. Click OK.

Create BIOS Policy	Main	
Venin Venin	Name: VM-Host-Infra Reboot on BIOS Settings Change: Quiet Boot: disabled enabled Platform Default Post Error Pause: disabled enabled Platform Default Resume Ac On Power Loss: stay-off last-state reset Platform Default Front Panel Lockout: disabled enabled Platform Default	

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.

Γ

- 3. Right-click vNIC/vHBA Placement Policies.
- 4. Select Create Placement Policy.
- 5. Enter VM-Host-Infra as the name of the placement policy.
- 6. Click 1 and select Assigned Only.
- 7. Click OK and then click OK again.

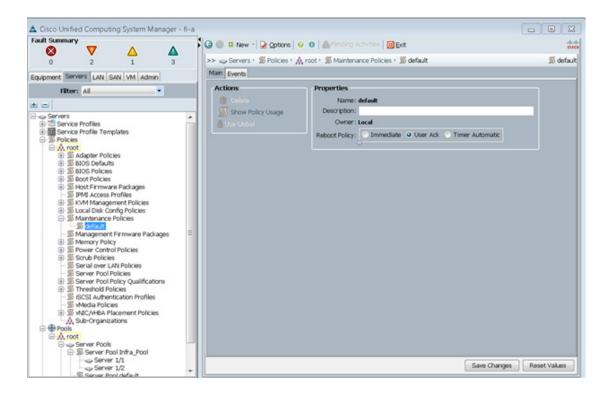
Create Placement Policy	X				
Create Placement Policy					
Name: VM-I	lost-Infra				
Virtual Slot Mapping Scheme:	ound Robin 🔘 Linear Ordered				
🕰 Filter 🖨 Export 😸 Print					
Virtual Slot	Selection Preference				
1	Assigned Only				
2	All				
3	All				
4	All				
	OK Cancel				

1

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.



Create vNIC Templates

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

۵, Note

I

The "Enable Failover" option is used for the vNICs in these steps as default, however, if deploying the optional N1kV virtual switch, the "Enable Failover" options for the vNICs should remain unchecked. "

- 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_Template_A as the vNIC template name.
- 6. Keep Fabric A selected.
- 7. Select the Enable Failover checkbox.
- 8. Under Target, make sure that the VM checkbox is not selected.
- 9. Select Updating Template as the Template Type.
- 10. Under VLANs, select the checkboxes for IB-MGMT-VLAN, NFS-VLAN, Native-VLAN, VM-Traffic-VLAN, and vMotion-VLAN.
- 11. Set Native-VLAN as the native VLAN.
- **12.** For MTU, enter 9000.

- **13.** In the MAC Pool list, select MAC_Pool_A.
- 14. In the Network Control Policy list, select Enable_CDP.
- **15.** Click OK to create the vNIC template.
- 16. Click OK.

Marca	WIC Toppolate A				
	vNIC_Template_A				
Description			_		
Fabric ID:	Fabric A C Fabric B	Enable Failover			
	0 Target				
	Adapter				
	MV III				
Warning	1 01 1 H				
	rt profile by the same name		18		
a port profile of the	same name exists, and upd	ating template is selected,	, it will be	overwritten	
	O tablel Tamalata O th	dation Townlate			
Template Type:	Initial Template 🔍 Up	dating remplate			
LANs	U				
Filter 👄 Export 😪	Print				
	Manua	Nation 18, 481	m		
Select	Name	Native VLAN	C\$		
v	IB-MGMT-VLAN		-		
v	NFS-VLAN		- 11		
V	Native-VLAN		=		
V	VM-Traffic-VLAN				
	vMotion-VLAN			J	
v					
Create VLAN	9000				
Create VLAN MTU:	0				
Create VLAN MTU: MAC Pool:	0 MAC_Pool_A(32/ •				
Create VLAN MTU: MAC Pool:	0				
Create VLAN MTU: MAC Pool: QoS Policy:	MAC_Pool_A(32/				
Create VLAN MTU: MAC Pool: QoS Policy: twork Control Policy:	MAC_Pool_A(32/				
Create VLAN MTU: MAC Pool: QoS Policy: twork Control Policy: Pin Group:	MAC_Pool_A(32/ MAC_Pool_A(32/ MAC_Pool_A(32/				
Create VLAN MTU: QoS Policy: twork Control Policy: Pin Group: ats Threshold Policy:	MAC_Pool_A(32/ MAC_Pool_A(32/ MAC_Pool_A(32/				
Create VLAN MTU: QoS Policy: twork Control Policy: Pin Group: ats Threshold Policy:	MAC_Pool_A(32/ MAC_Pool_A(32/ MAC_Pool_A(32/				
Create VLAN MTU: MAC Pool: QoS Policy: twork Control Policy: Pin Group:	MAC_Pool_A(32/ MAC_Pool_A(32/ Anot set> Anot set> default				

1

- 17. In the navigation pane, select the LAN tab.
- **18.** Select Policies > root.
- 19. Right-click vNIC Templates.
- **20.** Select Create vNIC Template
- **21.** Enter vNIC_Template_B as the vNIC template name.

- 22. Select Fabric B.
- 23. Select the Enable Failover checkbox.
- 24. Select Updating Template as the template type.
- 25. Under VLANs, select the checkboxes for IB-MGMT-VLAN, NFS-VLAN, Native-VLAN, VM-Traffic-VLAN, and vMotion-VLAN.
- 26. Set Native-VLAN as the native VLAN.
- **27.** For MTU, enter 9000.
- 28. In the MAC Pool list, select MAC_Pool_B.
- 29. In the Network Control Policy list, select Enable_CDP.
- **30.** Click OK to create the vNIC template.
- 31. Click OK.

I

Create vNIC Tem	plate			
reate vNIC T	emplate			
Name	e: vNIC_Template_B	-		
Description	0 1:			
		Contractor Continuer		
Fabric II): Fabric A Sebric B	Enable Fallover		
	Target			
	Adapter			
	_ ∨M			
Warning				
	port profile by the same name	will be created		
	e same name exists, and upd		t it will be	werwritten
a por c prome or ca	e same name exists, and upu	ading template is selected	, it will be	Ver Writter
Template Type	e: 🔘 Initial Template 🧕 Up	dating Template		
	0	in the second		
/LANs				
🔍 Filter 👄 Export 🕯	🗟 Print			
- mor - copore le				
	Name	Native VLAN	E.	
	Name default	Native VLAN		
		Native VLAN	E\$	
Select	default	Native VLAN		
Select	default IB-MGMT-VLAN		-	
Select	default IB-MGMT-VLAN NFS-VLAN		-	
Select	default IB-MGMT-VLAN NFS-VLAN Native-VLAN			
Select	default IB-MGMT-VLAN NFS-VLAN Native-VLAN VM-Traffic-VLAN			
Select	default IB-MGMT-VLAN NFS-VLAN VM-Traffic-VLAN VM-Traffic-VLAN			
Select	default IB-MGMT-VLAN NFS-VLAN VM-Traffic-VLAN VM-Traffic-VLAN I: 9000 I: MAC_Pool_B(32/ •			
Select	default IB-MGMT-VLAN NFS-VLAN Native-VLAN VM-Traffic-VLAN VM-Traffic-VLAN I: 000 I: MAC_Pool_B(32/ • y: <not set=""></not>			
Select	default IB-MGMT-VLAN NFS-VLAN VM-Traffic-VLAN			
Select	default IB-MGMT-VLAN NFS-VLAN VM-Traffic-VLAN			
Select	default IB-MGMT-VLAN NFS-VLAN Native-VLAN VM-Traffic-VLAN VM-Traffic-VLAN I: MAC_Pool_B(32/ • (<not set=""> • (<not set)="" •<br="">(<not set=""> • (<not set)="" •<br="">(<not< td=""><td></td><td></td><th></th></not<></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not>			
Select	default IB-MGMT-VLAN NFS-VLAN Native-VLAN VM-Traffic-VLAN VM-Traffic-VLAN I: MAC_Pool_B(32/ • y: <not set=""> y: <not set=""> y: <not set=""> y: default •</not></not></not>			
Select	default IB-MGMT-VLAN NFS-VLAN Native-VLAN VM-Traffic-VLAN VM-Traffic-VLAN I: MAC_Pool_B(32/ • : <not set=""> • : <not se<="" set="" td=""><td></td><td></td><th></th></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not>			
Select	default IB-MGMT-VLAN NFS-VLAN Native-VLAN VM-Traffic-VLAN VM-Traffic-VLAN I: MAC_Pool_B(32/ • y: <not set=""> • y: <not set=""> • y: <not set=""> • y: default •</not></not></not>			

1

Create WWNN Pools

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

- 1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
- **2.** Choose Pools > root.
- 3. Right-click WWNN Pools.
- 4. Choose Create WWNN Pool.
- 5. Enter WWNN_Pool as the name of the WWNN pool.

- 6. (Optional) Add a description for the WWNN pool.
- 7. Click Next.
- 8. Click Add to add a block of WWNNs.
- 9. Keep the default block of WWNNs, or specify a base WWNN.
- **10.** Specify a size for the WWNN block that is sufficient to support the available blade or server resources.
- 11. Click OK.
- 12. Click Finish.
- 13. Click OK.

🔺 Create WWNN Pool				×
Unified C	omputing	System Ma	nager	
Create WWNN Pool 1. √ <u>Define Name and</u>	Add WWN Block	(S		0
Description 2. √Add WWN Blocks	Name	From	То	1
	一飜 [20:00:00:25:B5:	00:00:00 - 20:00:20:00:00:25:	85 20:00:00:25:85	*
		🗄 Add 👕 Delete		
		< Prev Next >	Finish Cano	el

Create WWPN Pools

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

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

Note

I

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.
- 7. Click Next.

- 8. Click Add to add a block of WWPNs.
- 9. Specify the starting WWPN in the block for fabric A.
- **10.** Specify a size for the WWPN block that is sufficient to support the available blade or server resources.
- 11. Click OK.
- 12. Click Finish to create the WWPN pool.
- 13. Click OK.

🖨 Create WWN Block		×
Create WWN Block		0
From: 20:00:00:25:B5:01:0A:00 To ensure uniqueness of WWNs in the SAN fabric, you are strongly encouraged to use the following WWN prefix: 20:00:00:25:b5:xx:xx:xx	Size:	32÷
	ОК	Cancel

- 14. Right-click WWPN Pools.
- 15. Choose Create WWPN Pool.
- 16. Enter WWPN_Pool_B as the name for the WWPN pool for fabric B.
- 17. (Optional) Enter a description for this WWPN pool.
- 18. Click Next.
- 19. Click Add to add a block of WWPNs.
- 20. Enter the starting WWPN address in the block for fabric B.
- **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, follow these 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.

🛕 Create vHBA Templ	ate	×
Create vHBA Te	emplate	0
Name:	vHBA_Template_A	
Description:		
Fabric ID:	• A • B	
Select VSAN:	VSAN_A	
Template Type:	Initial Template Updating Template	
Max Data Field Size:	2048	
WWPN Pool:	WWPN_Pool_A(32/32)	
QoS Policy:	<not set=""></not>	
Pin Group:	<not set=""></not>	
Stats Threshold Policy:	default 🔹	
		OK Cancel

- 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.

ſ

🛕 Create vHBA Templ	ate	×
Create vHBA Te	mplate	0
Name:	vHBA_Template_B	
Description:		_
Fabric ID:	○ A ● B	
Select VSAN:	VSAN_B	
Template Type:	 Initial Template Oupdating Template 	
Max Data Field Size:	2048	
WWPN Pool:	WWPN_Pool_B(32/32)	
QoS Policy:	<not set=""></not>	
Pin Group:	<not set=""></not>	
Stats Threshold Policy:	default 🗧	
		OK Cancel

Create Boot Policies

This procedure applies to a Cisco UCS environment in which two FC interfaces are used on the IBM V7000 Storwize cluster node 1 and two FC interfaces are used on cluster node 2. Also, it is assumed that the A interfaces are connected to fabric A and the B interfaces are connected to fabric B.

Two boot policies are configured in this procedure. The first policy configures the primary target to be fcp_lif01a and the second boot policy configures the primary target to be fcp_lif01b.

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

Note

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).

reate Boot Policy							
Name: I	Boot-Fabric-A						
Description:							
Reboot on Boot Order Change:							
force vNIC/VHBA/ISCSI Name:	v						
Boot Mode:	Legacy Uefi						
/ARNINGS: he type (primary/secondary) doe	s not indicate a boot ord	er presence					
he effective order of boot device	s within the same device	class (LAN/Stora	ge/ISCSI) is determined by PCIe				
Enforce vNIC/vHBA/iSCSI Na	me is selected and the v	NIC/MBA/ISCSI	does not exist, a config error will	be reported.			
it is not selected, the vNBCs/VHB	As//SCSI are selected if t	ney exist, otherw	ISE THE WALC/WHEAVISCEL WITH THE	iowest ricie bu	s scarrorder is di	,eu.	
	As//SCSI are selected if t	ney exist, otherw	ISE THE WILL/WHEA/ISCSI WITH THE	lowest r cie bu	s actin or dan is d.	ieu.	
				bwest r cie bu			
Local Devices	Boot Order			Type	Lun ID	www	
Local Devices 🔹	Boot Order	• Export 🗟 Print	1		_	_	
Local Devices	Boot Order Boot Order d. Filter = Name -@ CD/DVD	• Export 🕝 Print Order	1		_	_	
Local Devices 🔹	Boot Order	• Export 🕝 Print Order	1		_	_	
Local Devices	Boot Order Boot Order d. Filter = Name -@ CD/DVD	• Export 🕝 Print Order	1		_	_	
Local Devices	Boot Order Boot Order d. Filter = Name -@ CD/DVD	• Export 🕝 Print Order	1		_	_	
Local Devices	Boot Order Boot Order d. Filter = Name -@ CD/DVD	• Export 🕝 Print Order	1		_	_	
Local Devices	Boot Order Boot Order d. Filter = Name -@ CD/DVD	• Export 🕝 Print Order	1		_	_	
Local Devices	Boot Order Boot Order d. Filter = Name -@ CD/DVD	• Export 🕝 Print Order	1		_	_	
Local Devices	Boot Order Boot Order d. Filter = Name -@ CD/DVD	• Export 🕝 Print Order	1		_	_	
Local Devices	Boot Order Boot Order d. Filter = Name -@ CD/DVD	• Export 🕝 Print Order	1		_	_	
Local Devices	Boot Order Boot Order d. Filter = Name -@ CD/DVD	• Export 🕝 Print Order	1	Туре	_	_	

- 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.

Γ

🚖 Add 9	5AN Boot	×
Add	SAN Boot	0
(Fabric-A	
Type:	Primary C Secondary	
		OK Cancel

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 going to switch A << var_wwpn_Node1-switch-A>>
- 16. Keep the Primary radio button selected as the SAN boot target type.
- 17. Click OK to add the SAN boot target.

📥 Add SAN Boot Target	×
Add SAN Boot Target	0
Boot Target LUN: 0 Boot Target WWPN: 1:05: 07:68:08:23:20:FE Type: O Primary O Secondary	
OK	Cancel

- 18. From the vHBA drop-down menu, choose Add SAN Boot Target.
- **19.** Keep 0 as the value for Boot Target LUN.
- 20. Enter the WWPN for node 2 going to switch A << var_wwpn_Node2-switch-A>>
- 21. Click OK to add the SAN boot target.

📥 Add SAN Boot Target	×
Add SAN Boot Target	0
Boot Target LUN: 0	
Boot Target WWPN: 1:05:07:68:0B;24:20:FD	
Type: Primary @ Secondary	
	OK Cancel

- 22. From the vHBA drop-down menu, choose Add SAN Boot.
- 23. In the Add SAN Boot dialog box, enter Fabric-B in the vHBA box.

- 24. The SAN boot type should automatically be set to Secondary
- 25. Click OK to add the SAN boot initiator.

🚔 Add SAN Boot	×
Add SAN Boot	0
MRA: Eshvic-R	
VHBA: Fabric-B Type: O Primary O Secondary	
Type: 🔍 Primary 💽 Secondary	
	OK Cancel
	Cancer

- 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 switch B <<var_wwpn_Node2-switch-B>>
- **29.** Keep Primary as the SAN boot target type.
- **30.** Click OK to add the SAN boot target.

📥 Add SAN Boot Target	×
Add SAN Boot Target	0
Deat Terret U.M.	
Boot Target LUN: 0	
Boot Target WWPN: 1:05:07:68:0B:23:20:FD	
Type: O Primary 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 switch B <<var_wwpn_Node1-Switch-B>>
- **34.** Click OK to add the SAN boot target.

I

Add SAN Boot Target	×
Add SAN Boot Target	0
Boot Target LUN: 0	
Boot Target WWPN: 1:05:07:68:0B:24:20:FC	
Type: OPrimary OSecondary	
	OK Cancel

- 35. Click OK, and then click OK again to create the boot policy.
- 36. Right-click Boot Policies again.
- 37. Choose Create Boot Policy.
- 38. Enter Boot-Fabric-B as the name of the boot policy.
- **39.** (Optional) Enter a description of the boot policy.
- 40. Keep the Reboot on Boot Order Change check box unchecked.
- 41. From the Local Devices drop-down menu choose Add CD/DVD.
- 42. From the vHBA drop-down menu choose Add SAN Boot.
- 43. In the Add SAN Boot dialog box, enter Fabric-B in the vHBA box.
- 44. Make sure that the Primary radio button is selected as the SAN boot type.
- 45. Click OK to add the SAN boot initiator.
- 46. From the vHBA drop-down menu, choose Add SAN Boot Target.
- 47. Keep 0 as the value for Boot Target LUN.
- **48.** Enter the WWPN for var_wwpn_Node1-Switch-B.
- **49.** Keep Primary as the SAN boot target type.
- 50. Click OK to add the SAN boot target.
- 51. From the vHBA drop-down menu, choose Add SAN Boot Target.
- **52.** Keep 0 as the value for Boot Target LUN.
- 53. Enter the WWPN for var_wwpn_Node2-switch-B.
- 54. Click OK to add the SAN boot target.
- 55. From the vHBA menu, choose Add SAN Boot.
- 56. In the Add SAN Boot dialog box, enter Fabric-A in the vHBA box.
- **57.** The SAN boot type should automatically be set to Secondary, and the Type option should be unavailable.

I

- 58. Click OK to add the SAN boot initiator.
- 59. From the vHBA menu, choose Add SAN Boot Target.
- 60. Keep 0 as the value for Boot Target LUN.

- 61. Enter the WWPN for var_wwpn_Node2-switch-A.
- 62. Keep Primary as the SAN boot target type.
- 63. Click OK to add the SAN boot target.
- 64. From the vHBA drop-down menu, choose Add SAN Boot Target.
- **65.** Keep 0 as the value for Boot Target LUN.
- 66. Enter the WWPN for var_wwpn_Node1-switch-A.
- 67. Click OK to add the SAN boot target.
- 68. Click OK and then click OK again to create the boot policy.

							1
eate Boot Policy							
Name: Br	oot-Fabric-D						
Description:							
eboot on Boot Order Change:	1						
orce vNIC/HBA//SCSI Name:	2						
Boot Mode:	Legacy Ouefi						
RNINGS:							
	not indicate a boot order presence.						
	within the same device class (LAN/Storage/6						
	me is selected and the vNIC/VHBA//SCSI does						
is not selected, the vNICs/VHBAs	s/ISCSI are selected if they exist, otherwise t	the vNIC/VHB/	VISCSI with the lowest PCIe	bus scan order i	s used.		
Add Remote CD/DVD							
	Boot Order				_		
Add Floppy	± = 4 Filter ⇒ Export (\$ Print	_			_		1
	🛓 🖃 🔩 Filter 👄 Export 🔅 Print	Order	-	Terr	1.00 10		
Add Floppy	te te la Filter ⇒ Export i Print Name	Order	WIC/HBA/ISCSI WIC	Туре	Lun ID	www	
Add Floppy Add Local Floppy Add Remote Floppy		1	WIC/HBA/ISCSI WIC	Туре	Lun ID	WWN	
Add Floppy	b ⊂ 4 Filter → Export i Print Name © CO/DVD ⊐ San				Lun ID	www	
Add Floppy Add Local Floppy Add Remote Floppy		1	WIC/HBA/ISCSI WIC	Primary			
Add Floppy Add Local Floppy Add Remote Floppy Add Remote Virtual Drive		1		Primary Primary	0	50:05:07:68:08:23:20:FD	
Add Floppy Add Local Floppy Add Remote Floppy		1	Fabric-B	Primary Primary Secondary			
Add Floppy Add Local Floppy Add Remote Floppy Add Remote Virtual Drive MC Mounted vMedia	b = 《 Filter → Export i Frint Name	1		Primary Primary Secondary Secondary	0	50:05:07:68:08:23:20:FD 50:05:07:68:08:24:20:FC	
Add Floppy Add Local Floppy Add Remote Floppy Add Remote Virtual Drive		1	Fabric-B	Primary Primary Secondary Secondary Primary	0 0	50:05:07:68:08:23:20:FD 50:05:07:68:08:24:20:FC 50:05:07:68:08:23:20:FC	
Add Floppy Add Local Floppy Add Remote Floppy Add Remote Virtual Drive CINC Mounted vMedia Atts	b = 《 Filter → Export i Frint Name	1	Fabric-B	Primary Primary Secondary Secondary Primary	0	50:05:07:68:08:23:20:FD 50:05:07:68:08:24:20:FC	
Add Floppy Add Local Floppy Add Remote Floppy Add Remote Virtual Drive MC Mounted vMedia		1	Fabric-B	Primary Primary Secondary Secondary Primary	0 0	50:05:07:68:08:23:20:FD 50:05:07:68:08:24:20:FC 50:05:07:68:08:23:20:FC	
Add Floppy Add Local Floppy Add Remote Floppy Add Remote Virtual Drive Add Remote Virtual Drive CINC Mounted vMedia Attos		1	Fabric-B	Primary Primary Secondary Secondary Primary	0 0	50:05:07:68:08:23:20:FD 50:05:07:68:08:24:20:FC 50:05:07:68:08:23:20:FC	
Add Floppy Add Local Floppy Add Remote Floppy Add Remote Virtual Drive ChilC Mounted Virtual Crive AIDs		1	Fabric-B	Primary Primary Secondary Secondary Primary	0 0	50:05:07:68:08:23:20:FD 50:05:07:68:08:24:20:FC 50:05:07:68:08:23:20:FC	
Add Floppy Add Local Floppy Add Remote Floppy Add Remote Virtual Drive Add Remote Virtual Drive CINC Mounted vMedia Attos		1	Fabric-B	Primary Primary Secondary Secondary Primary	0 0	50:05:07:68:08:23:20:FD 50:05:07:68:08:24:20:FC 50:05:07:68:08:23:20:FC	
Add Floppy Add Local Floppy Add Remote Floppy Add Remote Virtual Drive ChilC Mounted Virtual Crive AIDs		1	Fabric-B	Primary Primary Secondary Secondary Primary	0 0	50:05:07:68:08:23:20:FD 50:05:07:68:08:24:20:FC 50:05:07:68:08:23:20:FC	
Add Floppy Add Local Floppy Add Remote Floppy Add Remote Virtual Drive CIMC Mounted VMedia Adds a Add Savi Boot		1	Fabric-B	Primary Primary Secondary Primary Secondary	0 0	50:05:07:68:08:23:20:FD 50:05:07:68:08:24:20:FC 50:05:07:68:08:23:20:FC	
Add Floppy Add Local Floppy Add Remote Floppy Add Remote Virtual Drive CIMC Mounted vMedia Add Saw Boot Add Add Add Add Add Add Add Add Add Ad		1	Fabric-B Fabric-A	Primary Primary Secondary Primary Secondary	0 0	50:05:07:68:08:23:20:FD 50:05:07:68:08:24:20:FC 50:05:07:68:08:23:20:FC	

Create Service Profile Templates

In this procedure, two service profile templates are created: one for fabric A boot and one for fabric B boot. The first profile is created and then cloned and modified for the second host.

To create service profile templates, follow these steps:

- 1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
- 2. Choose Service Profile Templates > root.
- 3. Right-click root.
- 4. Choose Create Service Profile Template to open the Create Service Profile Template wizard.
- 5. Identify the Service Profile Template:
 - **a.** Enter VM-Host-Infra-Fabric-A as the name of the service profile template. This service profile template is configured to boot from node 1 on fabric A.

- b. Click the Updating Template radio button.
- c. Under UUID, choose UUID_Pool as the UUID pool.
- d. Click Next.

Unified C	Computing System Manager
Unified C Create Service Profile Template 1. Videntify Service 2. Ustworking 3. Storage 4. Joning 5. ViNC/HEA Placement 6. Mantenance Policy 9. Server Assignment 10. Operational Policies	Computing System Manager 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 UUD will be assigned to this template and enter a description. Name: VM-text-Infra-fabric-A The template will be created in the following organization. Its name must be unique within this organization. Where: erg-root The template will be created in the following organization. Its name must be unique within this organization. Type: Initial Template UDD dating Template Specify how the UUD will be assigned to the server associated with the service generated by this template. UUD UDD Assignment: UUD_Pool(33/33) The UUD will be assigned from the selected pool. The available/total UUDs are displayed after the pool name. Cotonally enter a description for the profile. The description can contain information about when and where the service profile should be used.
	< Prev Next > Finish Cancel

- 6. Configure the Networking options:
 - a. Keep the default setting for Dynamic vNIC Connection Policy.
 - b. Click the Expert radio button to configure the LAN connectivity.
 - c. Click Add to add a vNIC to the template.
 - d. In the Create vNIC dialog box, enter vNIC-A as the name of the vNIC.

- e. Check the Use vNIC Template check box.
- f. In the vNIC Template list, choose vNIC_Template_A.
- g. In the Adapter Policy list, choose VMWare.
- h. Click OK to add this vNIC to the template.

Create vNIC	0
Name: whit-A	
Name: wiic-A	
Use vNIC Template: V Create vNIC Template	
Create mild rempiate	
vNIC Template: vNIC_Template_A	
Adapter Performance Profile	
Adapter Policy: MWare Create Ethernet Adapter Policy	
Ŭ.	
	OK Cancel

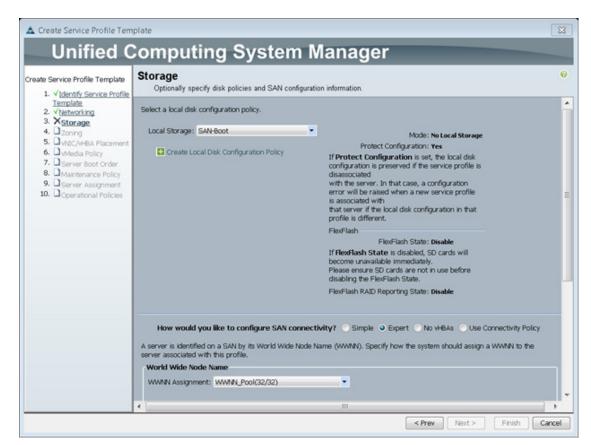
- i. On the Networking page of the wizard, click Add to add another vNIC to the template.
- j. In the Create vNIC box, enter vNIC-B as the name of the vNIC.
- **k.** Check the Use vNIC Template check box.
- I. In the vNIC Template list, choose vNIC_Template_B.
- m. In the Adapter Policy list, choose VMWare.
- **n.** Click OK to add the vNIC to the template.
- o. Review the table in the Networking page to make sure that both vNICs were created.
- p. Click Next.

I

Unified (Computing S	System Ma	nager		-		
Create Service Profile Template 1. √Identify Service Profile	Networking Optionally specify LAN cor	nfiguration information.			(
Template 2. √Networking 3. □Storage 4. □Zoning 5. □ <u>VNIC/WBA Placement</u>	Dynamic WillC Connection Policy: Select a Policy to use (no Dynamic WillC Policy by defa						
6. U <u>vMedia Policy</u> 7. U <u>Server Boot Order</u> 8. U <u>Maintenance Policy</u> 9. U <u>Server Assignment</u>		ike to configure LAN connect ore vNICs that the server should		rt 🔿 No vNICs 🔿 Use Conn	ectivity Policy		
10. Operational Policies	Name	MAC Address	Fabric ID	Native VLAN	a l		
	-S VNIC VNIC-A	Derived Derived	derived derived		^		
		1 Delete	Add Modify		÷		
	ISCS1 vNICs				8		

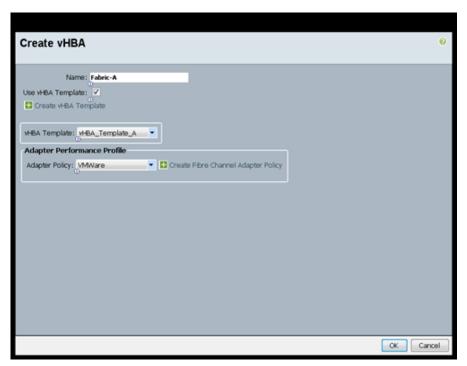
1

- 7. Configure the Storage options:
 - **a.** Choose a local disk configuration policy:
 - **b.** If the server in question has local disks, choose default in the Local Storage list.
 - c. If the server in question does not have local disks, choose SAN-Boot.
 - d. Click the Expert radio button to configure the SAN connectivity.
 - e. In the WWNN Assignment list, choose WWNN_Pool.



- f. Click Add at the bottom of the page to add a vHBA to the template.
- g. In the Create vHBA dialog box, enter Fabric-A as the name of the vHBA.
- h. Check the Use vHBA Template check box.
- i. In the vHBA Template list, choose vHBA_Template_A.
- j. In the Adapter Policy list, choose VMware.
- k. Click OK to add this vHBA to the template.

ſ



- **I.** On the Storage page of the wizard, click Add at the bottom of the page to add another vHBA to the template.
- m. In the Create vHBA dialog box, enter Fabric-B as the name of the vHBA.
- n. Check the check box for Use HBA Template.
- o. In the vHBA Template list, choose vHBA_Template_B.
- p. In the Adapter Policy list, choose VMware.
- q. Click OK to add the vHBA to the template.
- r. Review the table in the Storage page to verify that both A and B vHBAs were created.

I

s. Click Next.

reate Service Profile Template	Storage Optionally specify disk policies and SAN c	onformation information		0
√Identify Service Profile Template 2 √Networking 3. √Storage 4. √Zoning 5. □ <u>vNeCM-BA Placement 6. □ vMedia Policy 7. □ Server Root Order 8. □ <u>Maintenance Policy 9</u>. □ Server Assignment </u>	How would you like to configure SAN	FlexFlash RAID Reporting State: Disable connectivity? Simple Expert No vHBAs Use Connectivity Poli de Node Name (WWNN). Specify how the system should assign a WWNN to the		^
10. Operational Policies	WWMN Assignment: WWMN_Pool(32/32) The WWNN will be assigned from the select	•		
	The available/total WWWWs are displayed af			
	The available/total WWIWs are displayed af	ter the pool name.		
	The available/total WWNWs are displayed af	ter the pool name.	8	
	Name	ter the pool name. WWPN Derived	8	
	The available/total WWNWs are displayed af	ter the pool name.	•	
	The available/total WWNNs are displayed af Name State of the state of	ter the pool name. WWPN Derived		
	The available/total WWNNs are displayed af Name State of the state of	ter the pool name. WWPN Derived	•	

- 8. Set no Zoning options and click Next.
- 9. 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-A
 - vNIC-B
 - **c.** Review the table to verify that all vNICs and vHBAs were assigned to the policy in the appropriate order.
 - d. Click Next.

ſ

Create Service Profile Template		Placement	ed on physical network adapters			0
	n a server hardwa Select Placeme Virtual Network network adapt WICs and VHB/ assignment car performed expl it can be done automatically b	re configuration independent: VM+Host-Infra Interface connection provi- rs. is are assigned to one of V- be	VHBAs are placed on physical net it way. Create Placemen des a mechanism of placing vNICs rtual Network Interface connection ual Network Interface connection	nt Policy and vHBAs on pl n specified below	nysical . This	
		ement on physical network	interface is controlled by placeme and one or more vNICs or vHBAs			
	Please select o	ement on physical network ne Vintual Network Interfact	and one or more vNICs or vHBAs Virtual Network Interfaces Polk	; ;y (read only)		
	Please select of	ement on physical network	and one or more vNICs or vHBAs Virtual Network Interfaces Polic Name		Selection Preference	
	Please select of vNICs vHBAI Name	ement on physical network ne Vintual Network Interfact	and one or more vNICs or vHBAs Virtual Network Interfaces Polk	; ;y (read only)	Selection Preference Assigned Only All All	•

- 10. Click next to bypass the vMedia policy screen
- 11. Set the Server Boot Order:
 - a. In the Boot Policy list, choose Boot-Fabric-A.
 - **b.** Review the table to verify that all boot devices were created and identified. Verify that the boot devices are in the correct boot sequence.
 - c. Click Next.

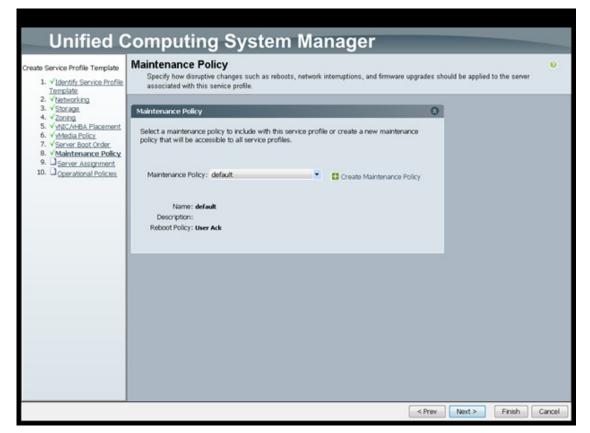
	Computing Sys	stem	manayer					
Create Service Profile Template	Server Boot Order							0
1. √Identify Service Profile	Optionally specify the boot policy f	or this servic	e profile template.					
Template	Select a boot policy.							
 ✓Networking. 								
 ✓<u>Storage</u> 	Boot Policy: Boot-Fabric-A							
4. √Zoning	BOOT POILCY: BOOT-FADINC-A	• 🖬 🖉	Create Boot Policy					
 ✓<u>vNIC/vHBA Placement</u> ✓<u>vMedia Policy</u> 								
7. √Server Boot Order	Name: Boot	Fabric A						
8. Maintenance Policy	Description:	Tabric-A						
9. Server Assignment	Reboot on Boot Order Change: No							
10. Operational Policies	Enforce vNIC/VHBA/ISCSI Name: Yes							
	Boot Mode: Lega							
	Boot Mode: Lega	сy						
	WARNINGS:							
	The type (primary/secondary) does no							
	The type (primary/secondary) does no The effective order of boot devices w/	thin the same	e device class (LAN/Storage/					
	The type (primary/secondary) does no The effective order of boot devices wi If Enforce vNIC/vHBA/iSCSI Name	thin the same is selected a	e device class (LAN/Storage/ nd the vNIC/VHBA/ISCSI doe	s not exist, a cor	nfig error will	be reported.	an order is	111
	The type (primary/secondary) does no The effective order of boot devices w/	thin the same is selected a	e device class (LAN/Storage/ nd the vNIC/VHBA/ISCSI doe	s not exist, a cor	nfig error will	be reported.	an order is	Ш
	The type (primary/secondary) does no The effective order of boot devices wi If Enforce vNIC/vHBA/iSCSI Name	thin the same is selected a	e device class (LAN/Storage/ nd the vNIC/VHBA/ISCSI doe	s not exist, a cor	nfig error will	be reported.	an order is	
	The type (primary/secondary) does no The effective order of boot devices wi If Enforce vNIC/vHBA/ISCSI Name If it is not selected, the vNICs/VHBA/K	thin the same is selected a	e device class (LAN/Storage/ nd the vNIC/VHBA/ISCSI doe	s not exist, a cor	nfig error will	be reported.	an order is	
	The type (primary/secondary) does no The effective order of boot devices wi If Enforce vNIC/vHBA/ISCSI Name If it is not selected, the vNICs/vHBA/8 Boot Order	thin the same is selected a	e device class (LAN/Storage/ nd the vNIC/VHBA/ISCSI doe	s not exist, a cor	nfig error will	be reported.	an order is	11
	The type (primary/secondary) does no The effective order of boot devices will If Enforce wNIC/wHBA/SECSI Name If it is not selected, the vNICs/vHBA/S Boot Order (b) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c	thin the same is selected a SCSI are sele	e device class (LAN/Storage/ nd the vNBC/HBA//SCSI doe icted if they exist, otherwise	s not exist, a cor the vNIC/vHBA/t	nfig error will SCSI with the	l be reported. a lowest PCIe bus sci	an order is	
	The type (primary/secondary) does no The effective order of boot devices will if Enforce will(vHBA/SESI Name If it is not selected, the vHICs/HBAs/8 Boot Order (a) (a) (A) Fifter = Export (a) Print Name (a) (c)(DVD) (c) (c)(DVD) (c) (c)(DVD)	thin the same is selected a SCSI are sele	e device class (LAN/Storage/ nd the vNBC/HBA//SCSI doe icted if they exist, otherwise	s not exist, a cor the vNIC/vHBA/t	nfig error will SCSI with the	l be reported. a lowest PCIe bus sci	an order is	11
	The type (primary/secondary) does no The effective order of boot devices will If Enforce wNIC/vHBA/SECSI Name If it is not selected, the vNICs/vHBAs/S Boot Order (b) □ (d) Filter → Export (c) Print Name (c) CD/DVD (c) San (c) = San (c) San primary	thin the same is selected a SCSI are sele Order 1	e device class (LAN/Storage/ nd the vNBC/HBA//SCSI doe icted if they exist, otherwise	s not exist, a cor the vNIC/vHBA/t	nfig error will SCSI with the	l be reported. a lowest PCIe bus sci	an order is	11
	The type (primary/secondary) does no The effective order of boot devices will if Enforce willC/vHBA/KBCSI Name If it is not selected, the vNICs/VHBAS/K Boot Order Color Boot Order Color San San San primary San Jarget primary	thin the same is selected a SCSI are sele Order 1	e device class (LAN/Storage) nd the vNIC/HBA/SCSI doe cted if they exist, otherwise wNIC/HBA/SCSI wIIC	s not exist, a cor the vNIC/VHBA/I Type Primary Primary	ofig error will SCSI with the Lun ID	l be reported. e lowest PCIe bus sci www. 50:05:07:68:08:2	23:20:FC	11
	The type (primary/secondary) does no The effective order of boot devices will if Enforce will(\rightarrow KI/CSU Name If it is not selected, the vNICs/MBAs/8 Boot Order Boot Order Boot Order Boot Order CO(DVD) San San SAN primary SAN Target secondary	thin the same is selected a SCSI are sele Order 1	e device class (LAN/Storage) nd the vNIC/HBA/ISCSI doe ccted if they exist, otherwise wNIC/HBA/ISCSI wIIC Fabric-A	s not exist, a cor the vNIC/VHBA/r Type Primary Primary Secondary	nfig error will SCSI with the	l be reported. e lowest PCIe bus sci	23:20:FC	
	The type (primary/secondary) does no The effective order of boot devices will if Enforce will(\rflowHBAS/KPCSI Name If it is not selected, the vNICs/M-BAS/K Boot Order Boot Order Boot Order CD/DVD San San San San primary SAN Target primary SAN Target secondary SAN Secondary	thin the same is selected a SCSI are sele Order 1	e device class (LAN/Storage) nd the vNIC/HBA/SCSI doe cted if they exist, otherwise wNIC/HBA/SCSI wIIC	s not exist, a cor the vNIC/VHBA/I Type Primary Primary Secondary Secondary	onfig error will SCSI with the Lun ID	l be reported. l lowest PCIe bus sci www 50:05:07:68:08:2 50:05:07:68:08:2	23:20:FC 24:20:FD	I
	The type (primary/secondary) does no The effective order of boot devices will if Enforce willC/vHBAS/K Boot Order Content Co	thin the same is selected a SCSI are sele Order 1	e device class (LAN/Storage) nd the vNIC/HBA/ISCSI doe ccted if they exist, otherwise wNIC/HBA/ISCSI wIIC Fabric-A	s not exist, a cor the vMIC/VHBA/t Type Primary Primary Secondary Primary	o Uun ID 0	l be reported. e lowest PCIe bus sci www 50:05:07:68:08:2 50:05:07:68:08:2 50:05:07:68:08:2	23:20:FC 24:20:FD 23:20:FD	
	The type (primary/secondary) does no The effective order of boot devices will if Enforce will(\rflowHBAS/KPCSI Name If it is not selected, the vNICs/M-BAS/K Boot Order Boot Order Boot Order CD/DVD San San San San primary SAN Target primary SAN Target secondary SAN Secondary	thin the same is selected a SCSI are sele Order 1	e device class (LAN/Storage) nd the vNIC/HBA/ISCSI doe ccted if they exist, otherwise wNIC/HBA/ISCSI wIIC Fabric-A	s not exist, a cor the vNIC/VHBA/I Type Primary Primary Secondary Secondary	onfig error will SCSI with the Lun ID	l be reported. l lowest PCIe bus sci www 50:05:07:68:08:2 50:05:07:68:08:2	23:20:FC 24:20:FD 23:20:FD	
	The type (primary/secondary) does no The effective order of boot devices will if Enforce willC/vHBAS/K Boot Order Content Co	thin the same is selected a SCSI are sele Order 1	e device class (LAN/Storage) nd the vNIC/HBA/ISCSI doe ccted if they exist, otherwise wNIC/HBA/ISCSI wIIC Fabric-A	s not exist, a cor the vMIC/VHBA/t Type Primary Primary Secondary Primary	o Uun ID 0	l be reported. e lowest PCIe bus sci www 50:05:07:68:08:2 50:05:07:68:08:2 50:05:07:68:08:2	23:20:FC 24:20:FD 23:20:FD	

12. Add a Maintenance Policy:

- a. Choose the Default Maintenance Policy.
- b. Click Next.

I

Γ



- 13. Specify the Server Assignment:
 - a. In the Pool Assignment list, choose Infra_Pool.
 - b. (Optional) Choose a Server Pool Qualification policy.
 - c. Choose Down as the power state to be applied when the profile is associated with the server.
 - **d.** Expand Firmware Management at the bottom of the page and choose VM-Host-Infra from the Host Firmware list.
 - e. Click Next.

Create Service Profile Template 1. √Identify Service Profile	Server Assignment Optionally specify a server pool for this service pro	file template.	0
1 • Jenning John Add Proving 2 • √Networking 3 • Storage 4 • √Zoning 5 • √MSCAHBA Placement 6 • √MAcda Policy 7 • ✓Server BootOrder 8 • √Mantenance Policy 9 • <u>Server Assignment</u> 10. □ _{Operational Policies}	You can select a server pool you want to associate with Pool Assignment: Infra_Pool • The service profile template will be associated with If desired, you can specify an additional server pool meet. To do so, select the qualification from the list. Server Pool Qualification: UCS8-8200-M3 • Restrict Migration:	Create Server Pool Select the power state to be applied when this profile is associated with the server. Up Down Down Down Down Down Down Down Down	
	Firmware Management (BIOS, Disk Controller, A If you select a host firmware policy for this service po- server that it is associated with. Otherwise the system uses the firmware already inst Host Firmware: <u>MM-Host-Infra</u>	rofile, the profile will update the firmware on the	2

14. Add Operational Policies:

I

Γ

- a. In the BIOS Policy list, choose VM-Host-Infra.
- **b.** Expand Power Control Policy Configuration and choose No-Power-Cap in the Power Control Policy list.

Unified C	Computing System Manager			1
Create Service Profile Template 1. √ <u>Identify Service Profile</u>	Operational Policies Optionally specify information that affects how the system operates.			0
<u>Template</u> 2. √ <u>Natworking</u> 3. √ <u>Storage</u> 4. √ <u>Zoning</u> 5. √ <u>vMC/MBA Placement</u> 6. √ <u>vMedia Policy</u> 7. √ <u>Server Boot Order</u>	BLOS Configuration If you want to override the default BLOS settings, select a BLOS policy that will be associated with this service profile BLOS Policy: OMHOST-Infra C Create BLOS Policy	0		
 ✓<u>Maintenance Policy</u> ✓<u>Server Assignment</u> 	External IPMI Management Configuration	Θ		
10. √ <u>Operational Policies</u>	Management IP Address	Θ		
	Monitoring Configuration (Thresholds)	Θ		
	Power Control Policy Configuration	0		
	Power control policy determines power allocation for a server in a given power group. Power Control Policy: No-Power-Cap			
	Scrub Policy	Θ		
	KVM Management Policy	Θ		
	< Prev No	ot >	Finish	Cancel

- 15. Click Finish to create the service profile template.
- 16. Click OK in the confirmation message.
- 17. Click the Servers tab in the navigation pane.
- **18.** Choose Service Profile Templates > root.
- 19. Right-click the previously created VM-Host-Infra-Fabric-A template.
- 20. Choose Create a Clone.
- **21.** In the dialog box, enter VM-Host-Infra-Fabric-B as the name of the clone, choose the root Org, and click OK.

? Clone Na	me: VM-Host-Infra	-Fabric-B
•	rg: root	•
ОК	Cancel	Help

- 22. Click OK.
- 23. Choose the newly cloned service profile template and click the Boot Order tab.

ault Summary	loo an IDamila	01.0	and the second second			
8 V 🛆 🔺	🚱 🌑 🖽 New - 😡 Options 🕴	0 Meeting	conces @ Eat			
0 2 1 3	>> 🥪 Servers * 🛅 Service Profi	le Templates 🕴 🙏 r	root + 🔝 Service Template V	M-Host-Infra-Fa	bric-B	Service Template VM+
subment Servers LAN SAN VM Admin	General Storage Network ISCS	SI vNICs vMedia Po	olicy Boot Order Policies E	vents FSM		
	Actions					
Filter: All	Modify Boot Policy					
-	COMPLEXATION 1					
Servers	Global Boot Policy					
Service Profiles	Name	: Boot-Fabric-A				
A root	Description	1				
Service Profile Templates	Reboot on Boot Order Change					
. A root	Enforce vNIC/VHBA//SCSI Name					
Service Template VM-Host-Infra-Fabric-	A Deat Made					
Service Template VMHost-Infra-Fabric+	3	. cegacy				
	WARNINGS:					
III - U VNICs	The type (primary/secondary) of					
	The effective order of boot devi					
- ∬ Sub-Organizations ∋ ∭ Policies	If Enforce vNIC/vHBA/iSCSI	Name is selected a	ind the vNIC/VHBA/ISCSI doe	s not exist, a cor	nfig error will	I be reported.
		Name is selected a	ind the vNIC/VHBA/ISCSI doe	s not exist, a cor	nfig error will	I be reported.
Sub-Organizations Sub-Organiza	If Enforce vNIC/vHBA/iSCSI	Name is selected a	ind the vNIC/VHBA/ISCSI doe	s not exist, a cor	nfig error will	I be reported.
	If Enforce vAIC/vHBA/ISCSI If it is not selected, the vMCs/v Boot Order	Name is selected a HBAs//SCSI are sele	ind the vNIC/VHBA/ISCSI doe	s not exist, a cor	nfig error will	I be reported.
	If Enforce vNIC/vHBA/iSCSI If it is not selected, the vNICs/v	Name is selected a HBAs//SCSI are sele	ind the vNIC/VHBA/ISCSI doe	s not exist, a cor	nfig error will	I be reported.
	If Enforce vAIC/vHBA/ISCSI If it is not selected, the vMCs/v Boot Order	Name is selected a HBAs//SCSI are sele	ind the vNIC/VHBA/ISCSI doe	s not exist, a cor	nfig error will	I be reported.
	If Enforce vNIC/vHBA/ISCSI If it is not selected, the vNICs/v Boot Order	Name is selected a HBAs//SCSI are sele Print	nd the VNIC/HBA/ISCSI doe coad if they exist, otherwise	s not exist, a cor the vf&C/vHBA/t	nfig errior will SCSI with the	l be reported. e lowest PCIe bus scan on
	If Enforce VNIC/VHEA/ISCSI If it is not selected, the VAICs/V Doot Order (d) (a) (d), Filter + Export de Name	Name is selected a HBAs/ISCSI are sele Print Order	nd the VNIC/HBA/ISCSI doe coad if they exist, otherwise	s not exist, a cor the vf&C/vHBA/t	nfig errior will SCSI with the	l be reported. e lowest PCIe bus scan on
	If Enforce v4E/v4BA/EDSE If it is not selected, the v4Cs/v Boot Onder d_ □ d_ Fitter = Export de Name □ @ CD/CVD	Name is selected a HBAS/ISCSI are sele Print Order 1	nd the VNIC/HBA/ISCSI doe coad if they exist, otherwise	s not exist, a cor the vf&C/vHBA/t	nfig errior will SCSI with the	l be reported. e lowest PCIe bus scan on
A sub-Organizations Selected Se	If Enforce v4IC/v4BA/BC/SDSI If it is not selected, the v4ICs/v Boot Order 	Name is selected a HBAs/ISCSI are selected Print Order 1 2	nd the VAC/HBA/ISOSI doe Includ if they exist, otherwise WBC/HBA/ISOSI VAC	s not exist, a cor the vH8C/VHBA/V Type	nfig errior will SCSI with the	I be reported. e lowest PCIe bus scan on
	If Enforce vAIC/vHBA/EDGS If it is not selected, the vAICs/v Boot Order 	Name is selected a HBAs/ISCSI are selected Print Order 1 2 RY	nd the VAC/HBA/ISOSI doe Includ if they exist, otherwise WBC/HBA/ISOSI VAC	s not exist, a cor the vH2C/VHBA/I Type Primary	nfig error wil SCSI with the	I be reported. e lowest PCIe bus scan on WWN 50:05:07:68:08:23:20
Sub-Organizations Solo-Organizations Solo-Organizations Solo-Solo-Solo-Solo-Solo-Solo-Solo-S	If Enforce vHE/vHBA/EDSE If it is not selected, the vHCA/M Boot Order	Name is selected a HBAS/GCSI are sele Print Order 1 2 ry dary	nd the VAC/HBA/ISOSI doe Includ if they exist, otherwise WBC/HBA/ISOSI VAC	s not exist, a cor the vHBC/VHBA/I Type Primary Primary	nfig error will SCSI with the Lun ID	I be reported. e lowest PCIe bus scan on WWN 50:05:07:68:08:23:20
A sub-Organizations Section Policies Section	If Enforce v4IC/v4BA/EDGSI If it is not selected, the v4ICs/v Boot Order	Name is selected a HBAs//SCSI are selected a	nd the VMC/AHBA/ISOSI doe sched if they exist, otherwise W&C/AHBA/ISOSI VMC Fabric-A	s not exist, a cor the vNBC/V+BA/i Type Primary Primary Secondary	nfig error will SCSI with the Lun ID	I be reported. e lowest PCIe bus scan on www. 50:05:07:68:08:23:20 50:05:07:68:08:24:20
A Sub-Organizations Sub-Organizations Solutions Solutions Solution Solu	If Enforce vHE/vHBA/EDSE If it is not selected, the vHCA/M Boot Order	Name is selected a HBAs//SCSI are selected a	nd the VMC/AHBA/ISOSI doe sched if they exist, otherwise W&C/AHBA/ISOSI VMC Fabric-A	s not exist, a cos the vhBC/vHBA/t Type Primary Primary Secondary Secondary	nfig error will SCSI with the Lun ID	I be reported. e lowest PCIe bus scan on www. 50:05:07:68:08:23:20 50:05:07:68:08:24:20
A Sub-Organizations Sub-Organizations Sub-Organizations Sub-Organizations Sub-Organizations Sub-Organization	If Enforce v4IC/v4BA/EDGSI If it is not selected, the v4ICs/v Boot Order	Name is selected a HBAs//SCSI are selected a	nd the VMC/AHBA/ISOSI doe sched if they exist, otherwise W&C/AHBA/ISOSI VMC Fabric-A	s not exist, a cos the vMC/vHBA/i Type Primary Primary Secondary Primary	nfig error will SCSI with the Lun ID 0 0	I be reported. e lowest PCIe bus scan on WWW 50:05:07:66:08:23:20 50:05:07:66:08:23:20 50:05:07:66:08:23:20
A Sub-Organizations Sub-Organizations Solutions Solutions Solution Solu	If Enforce v4IC/v4BA/EDGSI If it is not selected, the v4ICs/v Boot Order	Name is selected a HBAs//SCSI are selected a	nd the VMC/AHBA/ISOSI doe sched if they exist, otherwise W&C/AHBA/ISOSI VMC Fabric-A	s not exist, a cos the vMC/vHBA/i Type Primary Primary Secondary Primary	nfig error will SCSI with the Lun ID 0 0	I be reported. e lowest PCIe bus scan on WWW 50:05:07:66:08:23:20 50:05:07:66:08:23:20 50:05:07:66:08:23:20
Sub-Organizations Sub-Organizations Sub-Organizations Sub-Organizations Sub-Organizations Sub-Organization	If Enforce v4EC/v4BA/EDGSL If it is not selected, the v4CGA/ Boot Order	Name is selected a HBAs//SCSI are selected a	nd the VMC/AHBA/ISOSI doe acted if they exist, otherwise VMBC/AHBA/ISOSI VMBC Fabric-A Fabric-B	s not exist, a cos the vMC/vHBA/i Type Primary Primary Secondary Primary	nfig error will SCSI with the Lun ID 0 0	I be reported. e lowest PCIe bus scan on WWW 50:05:07:66:08:23:20 50:05:07:66:08:23:20 50:05:07:66:08:23:20
A Sub-Organizations Sub-Organizations Sub-Organizations Sub-Organizations Sub-Organizations Sub-Organizations Sub-Organization	If Enforce v4IC/v4BA/EDGSI If it is not selected, the v4ICs/v Boot Order	Name is selected a HBAs//SCSI are selected a	nd the VMC/AHBA/ISOSI doe sched if they exist, otherwise W&C/AHBA/ISOSI VMC Fabric-A	s not exist, a cos the vMC/vHBA/i Type Primary Primary Secondary Primary	nfig error will SCSI with the Lun ID 0 0	l be reported. e lowest PCIe bus scan orc www. 50:05:07:68:08:22:20 50:05:07:68:08:24:20 50:05:07:68:08:22:20

24. Click Modify Boot Policy.

I

Γ

25. In the Boot Policy list, choose Boot-Fabric-B.

odify Boot Policy							G
oot Policy: Boot-Fabric-B	💌 🚺 Crea	te Boot Policy					
Name: Boo	t-Fabric-B						
Description:							
Reboot on Boot Order Change: No							
Enforce vNIC/vHBA/ISCSI Name: Yes							
Boot Mode: Leg	асу						
WARNINGS: The type (primary/secondary) does i	oot indicate a l	haat ordar processo					
			coch is datawa	inad by PCTa	hus econ order		
The effective order of hoot devices y	vithin the same	e device class (LAN/Storage/					
The effective order of boot devices v f Enforce vNIC/vHBA/iSCSI Nam							
	e is selected a	ind the vNIC/VHBA/ISCSI does	s not exist, a cor	nfig error will	I be reported.	used.	
f Enforce vNIC/vHBA/ISCSI Nam f it is not selected, the vNICs/vHBAs	e is selected a	ind the vNIC/VHBA/ISCSI does	s not exist, a cor	nfig error will	I be reported.	used.	
f Enforce vNIC/vHBA/iSCSI Nam	e is selected a	ind the vNIC/VHBA/ISCSI does	s not exist, a cor	nfig error will	I be reported.	used.	
f Enforce vNIC/vHBA/ISCSI Nam f it is not selected, the vNICs/vHBAs	e is selected a /ISCSI are sele	ind the vNIC/VHBA/ISCSI does	s not exist, a cor	nfig error will	I be reported.	used.	
f Enforce vNIC/vHBA/ISCSI Nam f it is not selected, the vNICs/vHBAs Boot Order	e is selected a /ISCSI are sele	ind the vNIC/VHBA/ISCSI does	s not exist, a cor	nfig error will	I be reported.	used.	
f Enforce vNIC/vHBA/ISCSI Nam f it is not selected, the vNICs/vHBAs, Boot Order	e is selected a /ISCSI are sele t	nd the vNIC/VHBA/ISCSI doe acted if they exist, otherwise	s not exist, a cor the vNIC/vHBA/r	nfig error wil SCSI with th	l be reported. e lowest PCIe bus scan order is		
f Enforce vNIC/vHBA/ISCSI Nam f it is not selected, the vNICs/vHBAs, Boot Order du □ dL Filter ⇒ Export cs Print Name □ @ CD/DVD	e is selected a /ISCSI are sele t Order	nd the vNIC/VHBA/ISCSI doe acted if they exist, otherwise	s not exist, a cor the vNIC/vHBA/r	nfig error wil SCSI with th	l be reported. e lowest PCIe bus scan order is		
f Enforce vNIC/vHBA/ISCSI Nam f it is not selected, the vNICs/vHBAs Boot Order	e is selected a /ISCSI are sele t Order 1	nd the vNIC/VHBA/ISCSI doe acted if they exist, otherwise	s not exist, a cor the vNIC/VHBA/k Type	nfig error wil SCSI with th	l be reported. e lowest PCIe bus scan order is		
f Enforce vNIC/vHBA/ISCSI Nam f it is not selected, the vNICs/vHBAs, Boot Order	e is selected a /ISCSI are sele t Order 1	ind the WIC/WBA/ISCSI doe acted if they exist, otherwise WIC/WBA/ISCSI WIC	s not exist, a cor the vNIC/vHBA/r	nfig error wil SCSI with th	l be reported. e lowest PCIe bus scan order is		
f Enforce vNIC/vHBA/ISCSI Nam f it is not selected, the vNICs/vHBAs, Boot Order	e is selected a /ISCSI are sele t Order 1	ind the WIC/WBA/ISCSI doe acted if they exist, otherwise WIC/WBA/ISCSI WIC	s not exist, a cor the vNIC/VHBA/k Type Primary Primary	nfig error will SCSI with th	l be reported. e lowest PCIe bus scan order is WWN		
f Enforce vNIC/vHBA/ISCSI Nam f it is not selected, the vNICs/vHBAs, Boot Order	e is selected a /ISCSI are sele t Order 1	ind the WIC/WBA/ISCSI doe acted if they exist, otherwise WIC/WBA/ISCSI WIC	s not exist, a cor the vNIC/VHBA/I Type Primary	fig error will SCSI with th	I be reported. e lowest PCIe bus scan order is WWN 50:05:07:68:08:23:20:FD		
f Enforce vNIC/vHBA/ISCSI Nam f it is not selected, the vNICs/vHBA; Root Order	e is selected a /ISCSI are sele t Order 1	Ind the VAIC/VHBA/ISCSI does acted if they exist, otherwise VAIC/VHBA/ISCSI VAIC Fabric-B	s not exist, a cor the vNIC/VHBA/t Type Primary Primary Secondary	fig error will SCSI with th	I be reported. e lowest PCIe bus scan order is WWN 50:05:07:68:08:23:20:FD		
f Enforce vNIC/vHBA/ISCSI Nam f it is not selected, the vNICs/vHBA; Boot Order	e is selected a /ISCSI are sele t Order 1	Ind the VAIC/VHBA/ISCSI does acted if they exist, otherwise VAIC/VHBA/ISCSI VAIC Fabric-B	s not exist, a cor the vNIC/HBA/t Type Primary Primary Secondary Secondary	unfig error will SCSI with the Lun ID	I be reported. e lowest PCIe bus scan order is WWN 50:05:07:68:08:23:20:FD 50:05:07:68:08:24:20:FC		
f Enforce vNIC/vHBA/ISCSI Nam f it is not selected, the vNICs/vHBAs Boot Order	e is selected a /ISCSI are sele t Order 1	Ind the VAIC/VHBA/ISCSI does acted if they exist, otherwise VAIC/VHBA/ISCSI VAIC Fabric-B	s not exist, a cor the vNIC/VHBA/t Type Primary Primary Secondary Primary	fig error will SCSI with th Lun ID 0	I be reported. e lowest PCIe bus scan order is WWN 50:05:07:68:08:23:20:FD 50:05:07:68:08:23:20:FC 50:05:07:68:08:23:20:FC		
f Enforce vNIC/vHBA/ISCSI Nam f it is not selected, the vNICs/vHBAs Boot Order	e is selected a /ISCSI are sele t Order 1	Ind the VAIC/VHBA/ISCSI does acted if they exist, otherwise VAIC/VHBA/ISCSI VAIC Fabric-B	s not exist, a cor the vNIC/VHBA/t Type Primary Primary Secondary Primary	fig error will SCSI with th Lun ID 0	I be reported. e lowest PCIe bus scan order is WWN 50:05:07:68:08:23:20:FD 50:05:07:68:08:23:20:FC 50:05:07:68:08:23:20:FC		
f Enforce vNIC/vHBA/ISCSI Nam f it is not selected, the vNICs/vHBA; Boot Order	e is selected a /ISCSI are sele t Order 1 2	nd the VNIC/VHBA/ISCSI doe acted if they exist, otherwise VNIC/VHBA/ISCSI VNIC Fabric-B Fabric-A	s not exist, a cor the vNIC/VHBA/t Type Primary Primary Secondary Primary	unifig error will SCSI with the Lun ID	I be reported. e lowest PCIe bus scan order is WWN 50:05:07:68:08:23:20:FD 50:05:07:68:08:23:20:FC 50:05:07:68:08:23:20:FC		
f Enforce vNIC/vHBA/ISCSI Nam f it is not selected, the vNICs/vHBAs Boot Order	e is selected a /ISCSI are sele t Order 1	nd the VNIC/VHBA/ISCSI doe acted if they exist, otherwise VNIC/VHBA/ISCSI VNIC Fabric-B Fabric-A	s not exist, a cor the vNIC/VHBA/t Type Primary Primary Secondary Primary	unifig error will SCSI with the Lun ID	I be reported. e lowest PCIe bus scan order is WWN 50:05:07:68:08:23:20:FD 50:05:07:68:08:23:20:FC 50:05:07:68:08:23:20:FC		
f Enforce vNIC/vHBA/ISCSI Nam f it is not selected, the vNICs/vHBA; Boot Order	e is selected a /ISCSI are sele t Order 1 2	nd the VNIC/VHBA/ISCSI doe acted if they exist, otherwise VNIC/VHBA/ISCSI VNIC Fabric-B Fabric-A	s not exist, a cor the vNIC/VHBA/t Type Primary Primary Secondary Primary	unifig error will SCSI with the Lun ID	I be reported. e lowest PCIe bus scan order is WWN 50:05:07:68:08:23:20:FD 50:05:07:68:08:23:20:FC 50:05:07:68:08:23:20:FC		

I

- 26. Click OK and then click OK again.
- 27. In the right pane, click the Network tab and then click Modify vNIC/HBA Placement.
- **28.** Select VM-Host-Infra and Expand vCon 1 and move vHBA Fabric-B ahead of vHBA Fabric-A in the placement order.
 - a. Click OK and then click OK again.

	acement s	pecifies how vNICs and	I vHBAs are placed on physical n	etwork adapters	(mezzanine)	
erver ha	ardware o	onfiguration independer	nt way.			
elect Pla	cement:	VM-Host-Infra	 Create Placem 	ant Policy		
irtual Ne	stwork Inte	Inface connection provid	des a mechanism of placing vNIC	s and vHBAs on p	physical	
etwork a	idapters.		rtual Network Interface connecti			
ssignmer	nt can be					
		by selecting which Virt	tual Network Interface connection	n is used by vNIC	or vHBA or	
termine have a						
can be o utomatic		lecting "any".				
utomatic	ally by sei		interface is controlled by placem	ient preferences.		
utomatic NIC/VHBA	ally by sei A placeme	nt on physical network	interface is controlled by placem and one or more vNICs or vHB/			
utomatic NIC/VHBA	ally by sei A placeme	nt on physical network				
utomatic NIC/VHBA	ally by sei A placeme	nt on physical network		As		
utomatic NIC/VHBA	ally by sel A placeme lect one V	nt on physical network	e and one or more vNICs or vHB/	As	Selection Preference	
utomatic NIC/VHBA lease sel	ally by sel A placeme lect one V	nt on physical network	e and one or more vNICs or vHB/ Virtual Network Interfaces Po Name S VCon 1	As licy (read only)		
vNICs	A placeme lect one V	nt on physical network Intual Network Interface	e and one or more vNICs or vHBA Virtual Network Interfaces Po Name S vCon 1	as licy (read only) Order 1	Selection Preference	
vNICs	A placeme lect one V v+BAs	nt on physical network	e and one or more vNICs or vHBA Virtual Network Interfaces Po Name S vCon 1 S vCon 1	licy (read only) Order 1 2	Selection Preference	
vNICs	A placeme lect one V v+BAs	nt on physical network Intual Network Interface	e and one or more vNICs or vHBA Virtual Network Interfaces Po Name Stron 1 	licy (read only) Order 1 2 3	Selection Preference	
vNICs	A placeme lect one V v+BAs	nt on physical network intual Network Interface	e and one or more vNICs or vHBA Virtual Network Interfaces Po Name Strange vCon 1 VHBA Fabric-B VHBA Fabric-A VHBC vNIC-A	licy (read only) Order 1 2	Selection Preference Assigned Only	
vNICs	A placeme lect one V v+BAs	nt on physical network intual Network Interface	e and one or more vNICs or vHBA Virtual Network Interfaces Po Name S VCon 1 VHBA Fabric-B VHBA Fabric-A VHBC VNIC-A VNIC vNIC-B VCon 2	licy (read only) Order 1 2 3	Selection Preference	
vNICs	A placeme lect one V v+BAs	nt on physical network intual Network Interface	e and one or more vNICs or vHBA Virtual Network Interfaces Po Name Strange vCon 1 VHBA Fabric-B VHBA Fabric-A VHBC vNIC-A	licy (read only) Order 1 2 3	Selection Preference Assigned Only All	

Create Service Profiles

ſ

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

- 1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
- 2. Choose Service Profile Templates > root > Service Template VM-Host-Infra-Fabric-A.
- 3. Right-click VM-Host-Infra-Fabric-A and choose Create Service Profiles from Template.
- 4. Enter VM-Host-Infra-0 as the service profile prefix.
- 5. Enter 1 as the Name Suffix Staring Number.
- 6. Enter 1 as the Number of Instances
- 7. Click OK to create the service profile.

Create Service Profiles From Ten	nplate 🥹
Naming Prefix: VM-Host-Infra-0 Name Suffix Starting Number: 1 Number of Instances: 1	
	OK Cancel

- 8. Click OK in the confirmation message.
- 9. Choose Service Profile Templates > root > Service Template VM-Host-Infra-Fabric-B.
- 10. Right-click VM-Host-Infra-Fabric-B and choose Create Service Profiles from Template.
- 11. Enter VM-Host-Infra-0 as the service profile prefix.
- 12. Enter 2 as the Name Suffix Staring Number.
- 13. Enter 1 as the Number of Instances
- 14. Click OK to create the service profile.

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

15. Click OK in the confirmation message.

Verify that the service profiles VM-Host-Infra-01 and VM-Host-Infra-02 have been created. The service profiles are automatically associated with the servers in their assigned server pools.

16. (Optional) Choose each newly created service profile and enter the server host name or the FQDN in the User Label field in the General tab. Click Save Changes to map the server host name to the service profile name.

Backup the Cisco UCS Manager Configuration

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

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/gui/config/guide/2-2/b_UCSM_GUI_Configuration_Guide_2_2/b_UCSM_GUI_Configuration_Guide_2_2 chapter_0101010.html

Adding Servers

ſ

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

Gather Necessary 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 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 then expand the to see vHBAs, then click vHBA Fabric-A, in the general tab right click the WWPN and click Copy.



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

Source	Switch Target	Variable	WWPN
FC_Node1-1			
FC_Node1-2			
FC_Node1-3	Switch A FC1	var_wwpn_Node1-switch-A	
FC_Node1-4	Switch B FC1	var_wwpn_Node1-Switch-B	
FC_Node2-1			
FC_Node2-2			
FC_Node2-3	Switch A FC2	var_wwpn_Node2-switch-A	
FC_Node2-4	Switch B FC2	var_wwpn_Node2-switch-B	
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	

Table 21	WWPN's	for the	VM-Hosts
----------	--------	---------	----------

Cisco MDS 9148S SAN Zoning

These steps will configure zoning for the WWPN's from the server and the StorwizeV7000. We will be using the WWPN information collected in the previous steps for both the storage setup, and for server profile creation. There are 3 zones created, 2 for servers and 1 zone for cluster communication. If adding more Storwize V7000 control nodes, you will add the WWPN's to the cluster communication zone used below named V7000-cluster-comm.

```
Note
```

In this section we will be creating the zones for the configuration of a system that is using the V7000 FC ports 1 and 2 for a connection to the File Modules so they are not used in the MDS zoning. If you are using a block only setup, you would add the other WWPN's for all the interfaced connected to the MDS to the zones per the cabling instructions. Please use the following table for reference.

Cisco MDS - A Switch

1. Log in to the MDS switch and complete the following steps to create the WWPN aliases:

```
config
Enter configuration commands, one per line. End with CNTL/Z.
device-alias database
device-alias name VersaStack-Node1-A pwwn var_wwpn_Node1-switch-A
device-alias name VersaStack-Node2-A pwwn var_wwpn_Node2-switch-A
device-alias name VM-Host-Infra-01-A pwwn var_wwpn_VM-Host-Infra-01-A
device-alias name VM-Host-Infra-02-A pwwn var_wwpn_VM-Host-Infra-02-A
device-alias commit
```

2. Create the zones and add device-alias members for the 2 blade servers and 1 zone for V7000 cluster communications.

```
zone name VM-Host-Infra-01-A vsan 101
member device-alias VM-Host-Infra-01-A
member device-alias VersaStack-Node1-A
member device-alias VersaStack-Node2-A
exit
zone name VM-Host-Infra-02-A vsan 101
member device-alias VM-Host-Infra-02-A
member device-alias VersaStack-Node1-A
member device-alias VersaStack-Node2-A
exit
zone name V7000-cluster-comm-A vsan 101
member device-alias VersaStack-Node1-A
member device-alias VersaStack-Node1-A
member device-alias VersaStack-Node2-A
exit
```

3. Create a zoneset and add the 3 zones.

```
zoneset name VersaStack-A vsan 101
member VM-Host-Infra-01-A
member VM-Host-Infra-02-A
member V7000-cluster-comm-A
exit
```

4. Activate the zoneset.

zoneset activate name VersaStack-A vsan 101

```
<u>Note</u>
```

Validate all the HBA's are logged into the MDS switch. The V7000 and the Cisco servers should be powered on. To start the Cisco server's from Cisco UCS Manager, select the server tab, then click Server-Service-Profiles-root, and right-click VM-Host-Infra-01 then select boot server .

5. Validate the all powered on systems HBA's are logged into the switch.

```
sh zoneset active
zoneset name VersaStack-A vsan 101
    zone name VM-Host-Infra-01-A vsan 101
    * fcid 0x580201 [pwwn 20:00:025:b5:00:0a:0f] [VM-Host-Infra-01-A]
    * fcid 0x580100 [pwwn 50:05:07:68:0b:23:20:fc] [VersaStack-Node1-A]
    * fcid 0x580000 [pwwn 50:05:07:68:0b:24:20:fd] [VersaStack-Node2-A]
    zone name VM-Host-Infra-02-A vsan 101
    * fcid 0x580202 [pwwn 20:00:00:25:b5:00:0a:1f] [VM-Host-Infra-02-A]
    * fcid 0x580100 [pwwn 50:05:07:68:0b:23:20:fc] [VersaStack-Node1-A]
    * fcid 0x580000 [pwwn 50:05:07:68:0b:24:20:fd] [VersaStack-Node1-A]
    * fcid 0x580100 [pwwn 50:05:07:68:0b:24:20:fd] [VersaStack-Node2-A]
    zone name V7000-cluster-comm-A vsan 101
    * fcid 0x580100 [pwwn 50:05:07:68:0b:23:20:fc] [VersaStack-Node1-A]
    * fcid 0x580100 [pwwn 50:05:07:68:0b:23:20:fc] [VersaStack-Node1-A]
    * fcid 0x580100 [pwwn 50:05:07:68:0b:23:20:fc] [VersaStack-Node1-A]
    * fcid 0x580100 [pwwn 50:05:07:68:0b:23:20:fc] [VersaStack-Node1-A]
```

6. Save the configuration.

```
copy run start
```

Cisco MDS - B Switch

1. Log in to the MDS switch and complete the following steps to create the WWPN aliases:

```
config
Enter configuration commands, one per line. End with CNTL/Z.
device-alias database
device-alias name VersaStack-Node1-B pwwn var_wwpn_Node1-Switch-B
device-alias name VersaStack-Node2-B pwwn var_wwpn_Node2-switch-B
device-alias name VM-Host-Infra-01-B pwwn var_wwpn_VM-Host-Infra-01-B
device-alias name VM-Host-Infra-02-B pwwn var_wwpn_VM-Host-Infra-02-B
device-alias commit
```

2. Create the zones and add device-alias members for the 2 blade servers and 1 zone for V7000 cluster communications.

```
zone name VM-Host-Infra-01-B vsan 102
member device-alias VM-Host-Infra-01-B
member device-alias VersaStack-Node1-B
member device-alias VersaStack-Node2-B
exit
zone name VM-Host-Infra-02-B vsan 102
```

```
member device-alias VM-Host-Infra-02-B
member device-alias VersaStack-Node1-B
member device-alias VersaStack-Node2-B
exit
zone name V7000-cluster-comm-B vsan 102
member device-alias VersaStack-Node1-B
member device-alias VersaStack-Node2-B
exit
```

3. Create a zoneset and add the 3 zones.

```
zoneset name VersaStack-B vsan 102
member VM-Host-Infra-01-B
member VM-Host-Infra-02-B
member V7000-cluster-comm-B
```

4. Activate the zoneset.

zoneset activate name VersaStack-B vsan 102

```
<u>Note</u>
```

Validate all the HBA's are logged into the MDS switch. The V7000 and the Cisco servers should be powered on. To start the Cisco server's from UCSM, select the server tab, then click Server-Service-Profiles-root, and right click VM-Host-Infra-01 then select boot server.

5. Validate the all powered on systems HBA's are logged into the switch.

```
sh zoneset active
zoneset name VersaStack-B vsan 102
zone name VM-Host-Infra-01-B vsan 102
* fcid 0xae0201 [pwwn 20:00:00:25:b5:00:0b:0f] [VM-Host-Infra-01-B]
* fcid 0xae0100 [pwwn 50:05:07:68:0b:24:20:fc] [VersaStack-Node1-B]
* fcid 0xae0000 [pwwn 50:05:07:68:0b:23:20:fd] [VersaStack-Node2-B]
zone name VM-Host-Infra-02-B vsan 102
* fcid 0xae0202 [pwwn 20:00:00:25:b5:00:0b:1f] [VM-Host-Infra-02-B]
* fcid 0xae0100 [pwwn 50:05:07:68:0b:24:20:fc] [VersaStack-Node1-B]
* fcid 0xae0000 [pwwn 50:05:07:68:0b:23:20:fd] [VersaStack-Node2-B]
zone name V7000-cluster-comm-B vsan 102
* fcid 0xae0100 [pwwn 50:05:07:68:0b:24:20:fc] [VersaStack-Node1-B]
```

6. Save the configuration.

copy run start

SAN Boot

In this section we will be adding the host mappings for the host profiles created via UCS Manager to the V7000 storage, connecting to the boot LUNs, and doing the initial ESXi install. The WWPN's for the hosts will be required to complete this section.

Adding Hosts and Mapping the Boot Volumes on the IBM Storwize V7000

1. Open the Storwize V7000 management GUI by navigating to <<var_cluster_mgmt_ip>>and log in with your superuser or admin account. In the left pane click Host icon, which is the 5th icon down and click the Hosts menu item. Click Create Host in the upper left menu to bring up the Create Host wizard.

쉼 Versa	Stack > Hosts > Hosts	IBM Storwize V7000	superuser (Security Administrator)
	Create Host Actions Pilter Name Status Host	Type # of Ports Host Mappings	Showing Ø hosts Selecting Ø hosts
-	Create Host	No items found.	×
11 12	- Choose the Host T	hype	
	Fibre C	Channel Host ISC SI Host	-
(A)		Create Host Cancel	
¢	Allocated: 16.00 GB / 20.30 TB (0%)	Ronning Tasks (0)	Health Status

2. Select the Fiber Channel Host option. For Host Name input VM-Host-Infra-01. For Fibre Channel Ports open the drop-down menu and select or input the WWPN's for the A path vHBA's, vm-WM-Host-infra-01-a>>, and click Add Port to List. Click the drop-down menu again, and select or Input the host B port, <<wwpn_VM-Host-infra-01-b>>, and click add port to list. Leave Advanced Settings as default and click Create Host, then click Close.



I

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

Create Host	×
Host Name (optional): VM-Host-Infra-01 Fibre Channel Ports ? Add Port to List Rescan	
Port Definitions X ✓ 20000025B5000A0F X ✓ 20000025B5000B0F X	
Advanced Settings I/O Group Host Type	
✓ io_grp0	
✓ io_grp1	
✓ io_grp2	
✓ io_grp3	
Advanced Create Host Cancel	

1

3. Click Create Host to create the 2nd host. Select the Fiber Channel Host option. For Host Name input VM-Host-Infra-02. For Fibre Channel Ports open the drop-down menu and select the WWPN's for the A path vHBA's, <<var_wwpn_VM-Host-infra-02-a>>, and click Add Port to List. Select the B port by selecting the var for the B path, <<wwpn_VM-Host-infra-02-b>>, and click Add Port To List. Leave the Advanced Settings as default and click Create Host, then click Close.

Hos	st Name (optional): VM-Host-Infra-02
Fibre Channel Ports	Add Port to List Rescan
Port Definitions	
✓ 20000025B5000A1F	- ×
✓ 20000025B5000B1F	- ×
Advanced Settings	
/O Group	Host Type
✓ io_grp0	Generic (default)
✓ io_grp1	O HP/UX
✓ io_grp2	OpenVMS
✓ io_grp3	O TPGS

Γ

4. Click the Volumes icon in the left pane, then click the volumes menu item to display the created volumes.

4	Create Volume	s Q Filter				Showing 4 volumes Selecting 1 volume	: (50
N	ame	State	Capacity	Storage Pool	Host Mappings	UID	
	infra_datastore_1	🖌 Online	🧿 500.00 GiB	mdiskgrp0	No	60050764008880058800000000000000	
	infra_swap	🖌 Online	100.00 GiB	mdiskgrp0	No	60050764008880058800000000000005	
	VM-Host-Infra-01	🖌 Online	40.00 GiB	mdiskgrp0	No	60050764008880058800000000000000	
-	VM-Host-Infra-02	🖌 Online	40.00 GiB	mdiskgrp0	No	600507640088800588000000000000001	
5	Volumes	/olumes					

1

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

	+ Create Volume	Actions	Filter		
	Name		State	Capaci	ty
	infra_datastore	_1	 Online 		500.0
	infra_swap		 Online 		100.0
	VM-Host-Infra-	14	< A-!!	1	40.0
	VM-Host-Infra	Create Volu	me	2	40.0
and the second		Map to Host	:		
5		Unmap All H	losts		
P .		View Mappe	d Hosts		
		Duplicate V	olume		
		Move to An	other I/O Group		
1		Rename			
		Shrink			
-		Expand			
ž.		Migrate to A	nother Pool		
2		Export to In	age Mode		
		Delete			
		Volume Cop	y Actions	•	
		Properties			

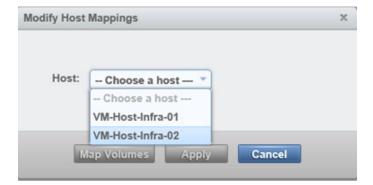
6. In the drop-down, select VM-Host-Infra-01.

Host:	Choose a host 💌	
	Choose a host	
	VM-Host-Infra-01	
	VM-Host-Infra-02	
IN	lap Volumes Apply Canc	el

7. Select Map Volumes then click Close.

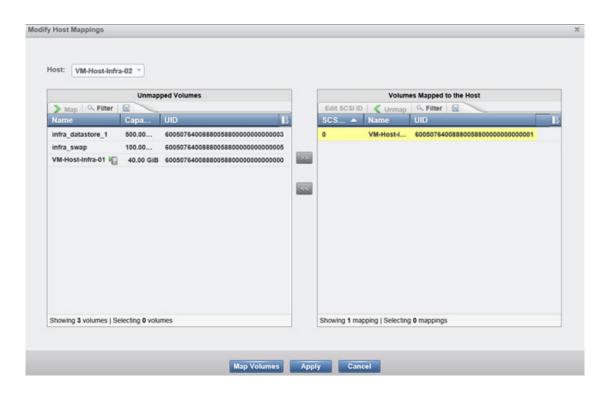
		ped Volumes			Volum	es Mapped to the Host	
> Map Q Filte			_	and the second se	Includes Propagation State	Q Filter	_
Name	Capa	UID	L.	SCS 🔺	Name	UID	
infra_datastore_1	500.00	60050764008880058800000000000	003	0	VM-Host-I	600507640088800588000000000000000	
infra_swap	100.00	60050764008880058800000000000					
VM-Host-Infra-02	40.00 GIB	60050764008880058800000000000	001				
			<<				
			_				

8. Right-click the volume VM-Host-Infra-02 and click Map to host and from the drop-down, choose host VM-Host-Infra-02.



Γ

9. Select Map Volumes, then click close.



VersaStack VMware ESXi 5.5 Update 1 SAN Boot Installation

This section provides detailed instructions for installing VMware ESXi 5.5 Update 1 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, we are using the **Cisco Custom ESXi 5.1.0 U1 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.

https://my.vmware.com/web/vmware/details?downloadGroup=OEM-ESXI55U1-CISCO&productId=3 53

Log in to Cisco UCS 6200 Fabric Interconnect

Cisco UCS Manager

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 UCS environment to run the IP KVM.

I

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

- 1. Download the Cisco Custom ISO for ESXi from the VMware website.
- 2. Open a web browser and enter the IP address for the Cisco UCS cluster address. This step launches the Cisco UCS Manager application.
- 3. Log in to Cisco UCS Manager by using the admin user name and password.
- 4. From the main menu, click the Servers tab.
- 5. Select Servers > Service Profiles > root > VM-Host-Infra-01.
- 6. Right-click VM-Host-Infra-01 and select KVM Console.
- 7. Select Servers > Service Profiles > root > VM-Host-Infra-02.
- 8. Right-click VM-Host-Infra-02 and select KVM Console Actions > KVM Console.

Fault Summary	🔨 📄 💷 New - 🕞 Options	00
0 14	1 >> 🥪 Servers ' 🥮 Service Profile	s 👌 🙏 root 🦂 S
Equipment Servers LAN SAN W		
Filter: All	General Storage	Network
* =	Show Navigator	
	Boot Server	
Servers Service Profiles	Shutdown Server	-
E 0, root	Reset	
🗊 💝 VM-Host-Infra-0		
WM-Host-Infra-0;	KVM Console	-
Sub-Organization	SSH to CIMC for SoL	
 Service Profile Templates , noot 	Rename Service Profile	
Service Template	Create a Clone	
Service Template	Create a Service Profile Template	
E- S Policies	Disassociate Service Profile	
⊟ root	Change Service Profile Association	
BIOS Defaults	Associate with Server Pool	

Set Up 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 the Virtual Media tab.



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



- 5. Click the KVM tab to monitor the server boot.
- 6. If the server is power on, first shutdown the server, then boot the server by selecting Boot Server and clicking OK, then click OK again.

Install ESXi

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 complete, click the check icon to clear the Mapped ISO (located in the Virtual Media tab of the KVM console) to unmap the ESXi installation image.



- **9.** The Virtual Media window might issue a warning stating that it is preferable to eject the media from the guest. Because the media cannot be ejected and it is read-only, simply click Yes to unmap the image.
- 10. From the KVM tab, press Enter to reboot the server.

Set Up Management Networking for ESXi Hosts

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

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 return to the main menu.
- 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 return to the main menu.
- 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.

vSphere Setup

In this section we will be setting up the VSphere environment using Windows 2008 and SQL server. The Virtual machines used in this procedure will be installed on a local Datastore one VersaStack for any Greenfield deployments, however these could be install on a different ESX clustered system or physical hardware if desired. This procedure will use the volumes previously created for VMFS Datastores.

Download VMware vSphere Client and vSphere Remote CLI

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 both the vSphere Client and the Windows version of vSphere Remote Command Line.



These applications are downloaded from the VMware website and Internet.

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:

- 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:

- 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.

Set Up VMkernel Ports and Virtual Switch

ESXi Host VM-Host-Infra-01 (Repeat the steps in this section for all the ESXi Hosts)

To set up the VMkernel ports and the virtual switches on the VM-Host-Infra-01 ESXi host, complete the following steps:

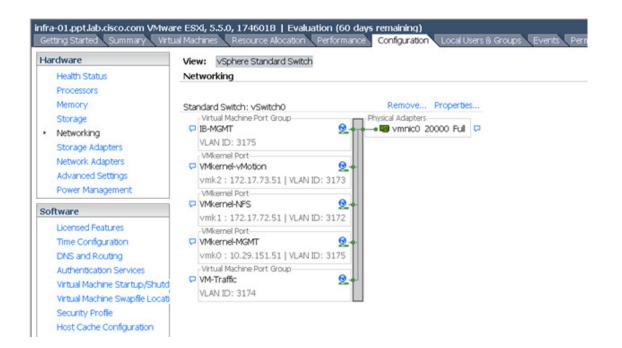
- 1. From each vSphere Client, select the host in the inventory.
- 2. Click the Configuration tab.
- 3. Click Networking in the Hardware pane.
- 4. Click Properties on the right side of vSwitch0.

- 5. Select the vSwitch configuration and click Edit.
- 6. From the General tab, change the MTU to 9000.
- 7. Click OK to close the properties for vSwitch0.
- 8. Select the Management Network configuration and click Edit.
- 9. Change the network label to VMkernel-MGMT and select the Management Traffic checkbox.
- 10. Click OK to finalize the edits for Management Network.
- 11. Select the VM Network configuration and click Edit.
- 12. Change the network label to IB-MGMT Network and enter <<var_ib-mgmt_vlan_id>> in the VLAN ID (Optional) field.
- 13. Click OK to finalize the edits for VM Network.
- 14. Click Add to add a network element.
- 15. Select VMkernel and click Next.
- 16. Change the network label to VMkernel-NFS and enter <<var_nfs_vlan_id>> in the VLAN ID (Optional) field.
- 17. Click Next to continue with the NFS VMkernel creation.
- 18. Enter the IP address <<var_nfs_vlan_id_ip_host-01>> and the subnet mask <<var_nfs_vlan_id_mask_host01>> for the NFS VLAN interface for VM-Host-Infra-01.
- 19. Click Next to continue with the NFS VMkernel creation.
- 20. Click Finish to finalize the creation of the NFS VMkernel interface.
- 21. Select the VMkernel-NFS configuration and click Edit.
- 22. Change the MTU to 9000.
- 23. Click OK to finalize the edits for the VMkernel-NFS network.
- 24. Click Add to add a network element.
- 25. Select VMkernel and click Next.
- 26. Change the network label to VMkernel-vMotion and enter <<var_vmotion_vlan_id>> in the VLAN ID (Optional) field.
- 27. Select the Use This Port Group for vMotion checkbox.
- 28. Click Next to continue with the vMotion VMkernel creation.
- 29. Enter the IP address <<var_vmotion_vlan_id_ip_host-01>> and the subnet mask <<var_vmotion_vlan_id_mask_host-01>> for the vMotion VLAN interface for VM-Host-Infra-01.
- 30. Click Next to continue with the vMotion VMkernel creation.
- 31. Click Finish to finalize the creation of the vMotion VMkernel interface.
- 32. Select the VMkernel-vMotion configuration and click Edit.
- **33.** Change the MTU to 9000.
- 34. Click OK to finalize the edits for the VMkernel-vMotion network.
- 35. Click add and select Virtual Machine Network, then click Next.
- **36.** Change the network label to VM-Traffic and enter <<var_vmtraffic_vlan_id>> in the VLAN ID (Optional) field

- 37. Click next, click finish to complete the creation of the VM-traffic network.
- 38. Close the dialog box to finalize the ESXi host networking setup.



This procedure uses 1 physical adapter (vmnic0) assigned to the vSphere Standard Switch (vSwitch0). If you plan to implement the 1000V Distributed Switch later in this document, this is sufficient. If your environment will be using the vSphere Standard Switch, you must assign another physical adapter to the switch. Click the properties of Vswitch0 on the configuration networking tab, click the Network Adapters tab, Click Add, select vmnic1, click Next, click Next, click Finish, click Close.



Map Required VMFS Datastores

Note

We are using the VMFS datastores in this section. If adding the IBM File Module, you can later migrate data to NFS datastores.

Map the VMFS Datastores to the First Host



The second Host will be mapped once the cluster is created.

- 1. Log in to the IBM Storwize V7000 management GUI.
- 2. Select the volumes icon on the left side screen and click the Volumes menu item.
- 3. Right-click the infra_datastore_1 volume and click map to host
- 4. Choose host VM-Host-Infra-1, then click map volumes, then close
- 5. Right-click the infra_swap volume and click map to host

6. Choose host VM-Host-Infra-1, then click map volumes, then close

ESXi Hosts VM-Host-Infra-01

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

- 1. From the vSphere Client, select the host VM-Host-Infra-01 in the inventory.
- 2. Click the Configuration tab to enable configurations.
- 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. Select the 500GB Datastore lun 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 Disk/Lun and click Next.
- 14. Select the 100GB swap lun and click Next.
- 15. Accept default VMFS setting and click Next.
- 16. Click next for the disk layout.
- 17. Enter infra swap as the datastore name.
- **18.** Click Next to retain maximum available space.
- 19. Click Finish.

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 to enable configurations.
- 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 Options.
- 6. In the NTP Daemon Options dialog box, complete the following steps:
 - a. Click General in the left pane and select Start and stop with host.
 - b. Click NTP Settings in the left pane and click Add.
- 7. In the Add NTP Server dialog box, enter <<var_global_ntp_server_ip>> as the IP address of the NTP server and click OK.
- 8. In the NTP Daemon Options dialog box, select the Restart NTP Service to Apply Changes checkbox and click OK.

- 9. In the Time Configuration dialog box, complete the following steps:
 - a. Select the NTP Client Enabled checkbox and click OK.
 - **b.** Verify that the clock is now set to approximately the correct time.

<u>Note</u>

The NTP server time may vary slightly from the host time.

VersaStack VMware vCenter 5.5 Update 1

The procedures in the following subsections provide detailed instructions for installing VMware vCenter 5.5 Update 1 in a VersaStack environment. After the procedures are completed, a VMware vCenter Server will be configured along with a Microsoft SQL Server database to provide database support to vCenter. These deployment procedures are customized to include the environment variables.

This procedure focuses on the installation and configuration of an external Microsoft SQL Server 2008 R2 database, but other types of external databases are also supported by vCenter. To use an alternative database, refer to the VMware vSphere 5.5 documentation.

To install VMware vCenter 5.5 Update 1, an accessible Windows Active Directory[®] (AD) Domain is necessary. If an existing AD Domain is not available, an AD virtual machine, or AD pair, can be set up in this VersaStack environment. Refer to the Appendix.

Build Microsoft SQL Server VM

ESXi Host VM-Host-Infra-01

To build a SQL Server virtual machine (VM) for the VM-Host-Infra-01 ESXi host, complete the following steps:

- 1. Log in to the host by using the VMware vSphere Client.
- 2. In the vSphere Client, select the host in the inventory pane.
- 3. Right-click the host and select New Virtual Machine.
- 4. Select Custom and click Next.
- 5. Enter a name for the VM. Click Next.
- 6. Select infra_datastore_1. Click Next.
- 7. Select Virtual Machine Version: 8. Click Next.
- 8. Verify that the Windows option and the Microsoft Windows Server[®] 2008 R2 (64-bit) version are selected. Click Next.
- 9. Select two virtual sockets and one core per virtual socket. Click Next.
- 10. Select 4GB of memory. Click Next.
- 11. Select one network interface card (NIC).
- 12. For NIC 1, select the IB-MGMT Network option and the VMXNET 3 adapter. Click Next.
- 13. Keep the LSI Logic SAS option for the SCSI controller selected. Click Next.
- 14. Keep the Create a New Virtual Disk option selected. Click Next.
- 15. Make the disk size at least 60GB. Click Next.

- 16. Click Next.
- 17. Select the checkbox for Edit the Virtual Machine Settings Before Completion. Click Continue.
- **18.** Click the Options tab.
- **19.** Select Boot Options.
- **20.** Select the Force BIOS Setup checkbox.
- 21. Click Finish.
- 22. From the left pane, expand the host field by clicking the plus sign (+).
- 23. Right-click the newly created SQL Server VM and click Open Console.
- 24. Click the third button (green right arrow) to power on the VM.
- 25. Click the ninth button (CD with a wrench) to map the Windows Server 2008 R2 SP1 ISO, and then select Connect to ISO Image on Local Disk.
- 26. Navigate to the Windows Server 2008 R2 SP1 ISO, select it, and click Open.
- 27. Click in the BIOS Setup Utility window and use the right arrow key to navigate to the Boot menu. Use the down arrow key to select CD-ROM Drive. Press the plus (+) key twice to move CD-ROM Drive to the top of the list. Press F10 and Enter to save the selection and exit the BIOS Setup Utility.
- **28.** The Windows Installer boots. Select the appropriate language, time and currency format, and keyboard. Click Next.
- 29. Click Install Now.
- **30.** Make sure that the Windows Server 2008 R2 Standard (Full Installation) option is selected. Click Next.
- **31.** Read and accept the license terms and click Next.
- **32.** Select Custom (Advanced). Make sure that Disk 0 Unallocated Space is selected. Click Next to allow the Windows installation to complete.
- **33.** After the Windows installation is complete and the VM has rebooted, click OK to set the Administrator password.
- **34.** Enter and confirm the Administrator password and click the blue arrow to log in. Click OK to confirm the password change.
- **35.** After logging in to the VM desktop, from the VM console window, select the VM menu. Under Guest, select Install/Upgrade VMware Tools. Click OK.
- **36.** If prompted to eject the Windows installation media before running the setup for the VMware tools, click OK, then click OK.
- **37.** In the dialog box, select Run setup64.exe.
- 38. In the VMware Tools installer window, click Next.
- 39. Make sure that Typical is selected and click Next.
- 40. Click Install.
- 41. Click Finish.
- **42.** Click Yes to restart the VM.
- **43.** After the reboot is complete, select the VM menu. Under Guest, select Send Ctrl+Alt+Del and then enter the password to log in to the VM.
- 44. Set the time zone for the VM, IP address, gateway, and host name.
- 45. Log back in to the VM and download and install all required Windows updates.

This process requires several	reboots.
46. Add the VM to the Wind	ows AD domain.

48. Log back in to the VM and download and install any additional required Windows updates.

Install Microsoft SQL Server 2008 R2

vCenter SQL Server VM

I

To install SQL Server on the vCenter SQL Server VM, complete the following steps:

- 1. Connect to an AD Domain Controller in the VersaStack Windows Domain and add an admin user for the VersaStack using the Active Directory Users and Computers tool. This user should be a member of the Domain Administrators security group.
- 2. Log in to the vCenter SQL Server VM as the VersaStack admin user and open Server Manager.
- 3. Expand Features and click Add Features.
- 4. Expand .NET Framework 3.5.1 Features and select only .NET Framework 3.5.1.

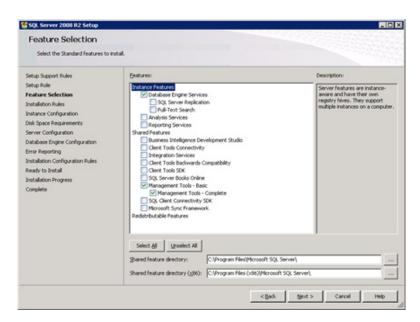
Add Features Wizard	×
Select Features	
Progress Results	Select one or more features to install on this server. Exture: NET Framework 3.5.1 Peatures Net for any peature transfer Service (BITS) BatLocker Drive Encryption BranchCache Connection Management Console Group Policy Management Group Policy Management DetectAccess Management Console Group Policy Management DetectAccess Management Console DetectAccess Management Console DetectAccess Management Order Printing Clent Drivement Storage Name Server DR Port Montor Multipath I/O Quality Windows Audo Wideo Experience Remote Assistance Totame Resolution Protocol Quality Windows Audo Wideo Experience Remote Assistance Totame Resolution Protocol Quality Windows Audo Wideo Experience Remote Assistance Totame Resolution Protocool Quality Windows Audo Wideo Experience Remote Assistance Totame Resolution Protocool Quality Windows Audo Wideo Experience Remote Assistance Totame Resolution Protocool Quality Windows Audo Wideo Experience Remote Assistance Totame Resolution Protocool Quality Windows Audo Wideo Experience Totame Resolution Protocool Totame Resoluti
	< Previous Next > [ristal] Cancel

- 5. Click Next.
- 6. Click Install.
- 7. Click Close.
- Open Windows Firewall with Advanced Security by navigating to Start > Administrative Tools > Windows Firewall with Advanced Security.
- 9. Select Inbound Rules and click New Rule.
- 10. Select Port and click Next.
- 11. Select TCP and enter the specific local port 1433. Click Next.
- 12. Select Allow the Connection. Click Next, and then click Next again.
- 13. Name the rule SQL Server and click Finish.
- 14. Close Windows Firewall with Advanced Security.
- In the vCenter SQL Server VMware console, click the ninth button (CD with a wrench) to map the Microsoft SQL Server 2008 R2 ISO. Select Connect to ISO Image on Local Disk.
- 16. Navigate to the SQL Server 2008 R2 ISO, select it, and click Open.
- 17. In the dialog box, click Run setup.exe.
- 18. In the SQL Server Installation Center window, click Installation on the left.
- 19. Select New Installation or Add Features to an Existing Installation.
- 20. Click OK.
- 21. Select Enter the Product Key. Enter a product key and click Next.
- 22. Read and accept the license terms and choose whether to select the second checkbox. Click Next.
- 23. Click Install to install the setup support files.
- 24. Address any warnings except for the Windows firewall warning. Click Next.



The Windows firewall issue was addressed in the previous steps.

- 25. Select SQL Server Feature Installation and click Next.
- 26. Under Instance Features, select only Database Engine Services.
- 27. Under Shared Features, select Management Tools Basic and Management Tools Complete. Click Next.



28. Click Next.

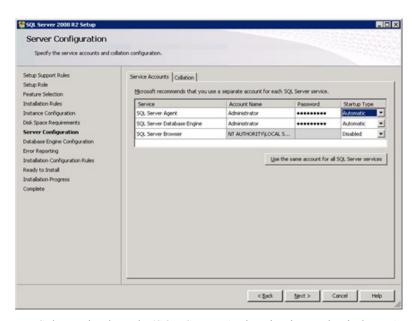
I

29. Keep the Default Instance selected. Click Next.

letup Support Rules	@ Default instance				
Setup Role Feature Selection	← Ngned instance:	MSSQLSERVER			
nstallation Rules Instance Configuration	Instance (D:	MSSQLSERVER			
Xisk Space Requirements ierver Configuration	Instance goot directory:	C:\Program Files	Microsoft SQL Server(2	
Natabase Engine Configuration Inter Reporting Installation Configuration Rules Leady to Install	SQL Server directory: Instaljed instances:	C:(Program Files)	Microsoft SQL Server(MSSQL10_50.MSSQL38	RVER
nstallation Progress Complete	Instance Name	Instance ID	Features	Editon	Version

- 30. Click Next for Disk Space Requirements.
- **31.** For the SQL Server Agent service, click in the first cell in the Account Name column and then click <<Browse...>>.
- **32.** Enter the local machine administrator name (for example, systemname\Administrator), click Check Names, and click OK.
- 33. Enter the administrator password in the first cell under Password.
- 34. Change the startup type for SQL Server Agent to Automatic.

35. For the SQL Server Database Engine service, select Administrator in the Account Name column and enter the administrator password again. Click Next.



36. Select Mixed Mode (SQL Server Authentication and Windows Authentication). Enter and confirm the password for the SQL Server system administrator (sa) account, click Add Current User and click Next.

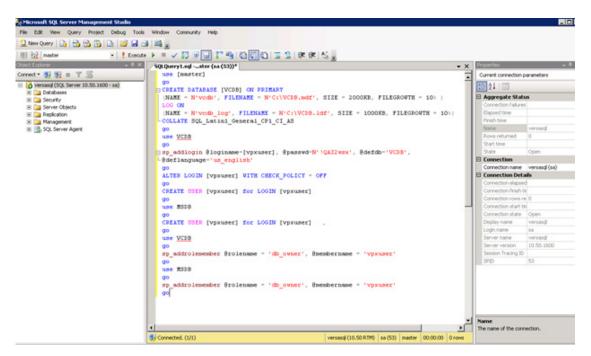
SQL Server 2008 R2 Setup Database Engine Config	guration
Specify Database Engine authentic	ation security mode, administrators and data directories.
Setup Support Rules Setup Role Feature Selection Installation Rules Instance Configuration Disk Space Requirements Server Configuration Database Engine Configuration Error Reporting Installation Configuration Rules Ready to Install Installation Progress Complete	Account Provisioning Data Directories FILESTREAM Specify the authentication mode and administrators for the Database Engine. Authentication Mode Windows authentication mode Windows authentication mode Mixed Mode (SQL Server authentication and Windows authentication) Specify the password for the SQL Server system administrator (sa) account. Enter password: Confirm password: Specify SQL Server administrators ICEVcef1-admin (cef1 admin) SQL Server administrators the Database Engine. Add Current User

- 37. Choose whether to send error reports to Microsoft. Click Next.
- 38. Click Next.
- **39.** Click Install.
- 40. After the installation is complete, click Close to close the SQL Server installer.
- 41. Close the SQL Server Installation Center.
- **42.** Install all available Microsoft Windows updates by navigating to Start > All Programs > Windows Update.
- **43.** Open the SQL Server Management Studio by selecting Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio.
- 44. Under Server Name, enter the local machine name. Under Authentication, select SQL Server Authentication. Enter sa in the Login field and enter the sa password. Click Connect.
- 45. Click New Query.
- 46. Run the following script, substituting the vpxuser password for <Password>:

```
use [master]
qo
CREATE DATABASE [VCDB] ON PRIMARY
(NAME = N'vcdb', FILENAME = N'C:\VCDB.mdf', SIZE = 2000KB, FILEGROWTH = 10% )
LOG ON
(NAME = N'vcdb log', FILENAME = N'C:\VCDB.ldf', SIZE = 1000KB, FILEGROWTH = 10%)
COLLATE SQL_Latin1_General_CP1_CI_AS
qo
use VCDB
qo
sp_addlogin @loginame=[vpxuser], @passwd=N'<Password>', @defdb='VCDB',
@deflanguage='us english'
qo
ALTER LOGIN [vpxuser] WITH CHECK_POLICY = OFF
go
CREATE USER [vpxuser] for LOGIN [vpxuser]
qo
use MSDB
qo
CREATE USER [vpxuser] for LOGIN [vpxuser]
go
use VCDB
qo
sp addrolemember @rolename = 'db owner', @membername = 'vpxuser'
qo
use MSDB
go
sp_addrolemember @rolename = 'db_owner', @membername = 'vpxuser'
qo
```

```
Note
```

This example illustrates the script.



- 47. Click Execute and verify that the query executes successfully.
- 48. Close Microsoft SQL Server Management Studio.
- 49. Disconnect the Microsoft SQL Server 2008 R2 ISO from the SQL Server VM.

Build and Set Up VMware vCenter VM

Build VMware vCenter VM

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

- Build a VMware vCenter VM with the following configuration in the <<var_ib-mgmt_vlan_id>> VLAN:
 - 4GB RAM
 - Two CPUs
 - One virtual network interface
- 2. Start the VM, install VMware Tools, and assign an IP address and host name to it in the Active Directory domain.

I

Set Up VMware vCenter VM

To set up the newly built VMware vCenter VM, complete the following steps:

- 1. Log in to the vCenter VM as the VersaStack admin user and open Server Manager.
- 2. Expand Features and click Add Features.
- 3. Expand .NET Framework 3.5.1 Features and select only .NET Framework 3.5.1.
- 4. Click Next.
- 5. Click Install.

- 6. Click Close to close the Add Features wizard.
- 7. Close Server Manager.
- 8. Download and install the client components of the Microsoft SQL Server 2008 R2 Native Client from the Microsoft Download Center.
- 9. Create the vCenter database data source name (DSN). Open Data Sources (ODBC) by selecting Start > Administrative Tools > Data Sources (ODBC).
- 10. Click the System DSN tab.
- 11. Click Add.
- 12. Select SQL Server Native Client 10.0 and click Finish.
- **13.** Name the data source VCDB. In the Server field, enter the IP address of the vCenter SQL server. Click Next.

Create a New Data Sour	rce to SQL Server
SQL Server 2008 R2	This wizard will help you create an ODBC data source that you can use to connect to SQL Server. What name do you want to use to refer to the data source? Name: VCDB How do you want to describe the data source? Description: Which SQL Server do you want to connect to? Server: 192.168.175.214
	Finish Next > Cancel Help

14. Select With SQL Server authentication using a login ID and password entered by the user. Enter vpxuser as the login ID and the vpxuser password. Click Next.

Ser.	How should SQL Server verify the authenticity of the login ID?
SQL Server 2008 R2	<u>With Integrated Windows authentication.</u> SEN (Optional):
	With SQL Server authentication using a login ID and password entered by the user.
	Login ID: vpxuser Password:
	Connect to SQL Server to obtain default settings for the additional configuration options.

15. Select Change the Default Database To and select VCDB from the list. Click Next.

1

6	Change the default database to:	
	VCDB	
SQL Server 2008 R2	Mirror server:	
	S <u>P</u> N for mirror server (Optional):	
	Attach database filename:	
	Use ANSI quoted identifiers.	
	Use ANSI nulls, paddings and warnings.	

- 16. Click Finish.
- 17. Click Test Data Source. Verify that the test completes successfully.

SQL Server ODBC Data Source Test	×
Test Results	
Microsoft SQL Server Native Client Version 10.50.1600	<u>^</u>
Running connectivity tests	
Attempting connection Connection established Verifying option settings Disconnecting from server	
TESTS COMPLETED SUCCESSFULLY!	
	<u> </u>
[OK]	

- 18. Click OK and then click OK again.
- 19. Click OK to close the ODBC Data Source Administrator window.
- **20.** Install all available Microsoft Windows updates by navigating to Start > All Programs > Windows Update.



A restart might be required.

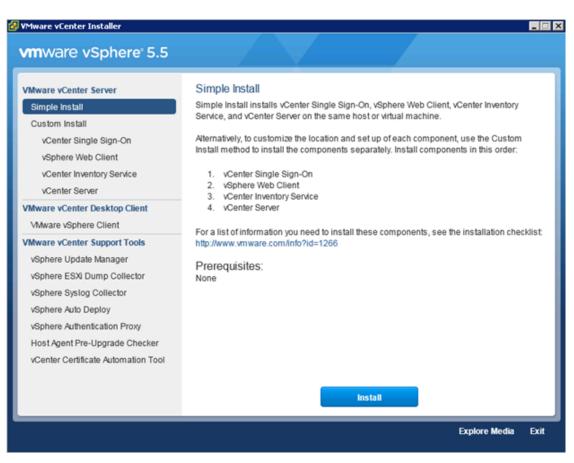
Install VMware vCenter Server

vCenter Server VM

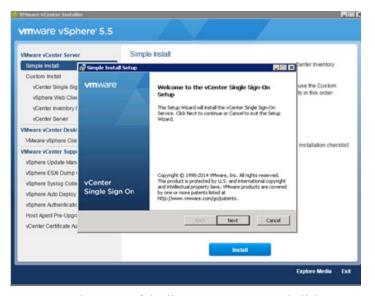
ſ

To install vCenter Server on the vCenter Server VM, complete the following steps:

- 1. In the vCenter Server VMware console, click the ninth button (CD with a wrench) to map the VMware vCenter ISO and select Connect to ISO Image on Local Disk.
- 2. Navigate to the VMware vCenter 5.5 Update 1 (VIMSetup) ISO, select it, and click Open.
- 3. In the dialog box, click Run autorun.exe.
- 4. In the VMware vCenter Installer window, make sure that VMware vCenter Simple Install is selected and click Install.



- 5. Click Yes if there is a User Account Control warning.
- 6. Click Next to install vCenter Single Sign On.



- 7. Accept the terms of the license agreement and click Next.
- 8. Click Next on Perquisites screen.

👘 Simple Install	×
Simple Insta	I Prerequisites Check
Host n	ame is VERSA-VCENTER
FQDN	is versa-vcenter.ppt.lab.cisco.com
IP Add	ress is 10.29.151.102
🗸 Machin	e is joined to ppt.lab.cisco.com
💙 DNS re	solution is successful
🔽 Ad	d ppt.lab.cisco.com as a native Active Directory identity source.
	Back Next Cancel

9. Enter and confirm <<var_password>> for administrator. Click Next.

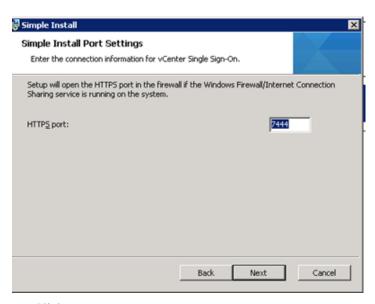
😽 Simple Install		×
	n-On Information r administrator account in default domain	
Domain Name:	vsphere.local	
User name:	Administrator	
Password:	•••••	
<u>C</u> onfirm Password:	••••••	
	Back Next	Cancel

10. Click Next on Site screen.

I

Γ

11. Accept Default HTTPS port and click Next.



- 12. Click Next
- **13.** Review the screen and click Install. This process will take approximately 20 minutes during which time multiple windows will launch.

l锷 Simple Install	×
Simple Install Information Review install options	
You have selected: New install Configured as first server in domain Domain name is vsphere.local HTTPS port is 7444 Site name is Default-First-Site Lookup service will be installed and configured new	
Back Install	Cancel

14. Enter yes for the SSL popup is displayed.



15. Enter the license Key.

cense Key			
Enter the license key.			
License key:			
1			
If you do not enter a licer	nse key, vCenter Serve	er will be installed	in evaluation
If you do not enter a licer mode.	nse key, v Center Serve	er will be installed	in evaluation
	nse key, vCenter Serve	er will be installed	in evaluation
	nse key, vCenter Serva	er will be installed	in evaluation
	nse key, vCenter Serve	er will be installed	in evaluation
	nse key, vCenter Serva	er will be installed	in evaluation

16. Change the radio button selection to use and existing instance.

17. Select VCDB and click Next.

Γ

🐯 YMware vCenter Simple Install	×
Database Options Select an ODBC data source for vCenter Server.	
vCenter Server requires a database.	
 Install a Microsoft SQL Server 2008 Express instance This option only suports deployments with up to 5 hosts or 50 virtual 	al machines
Use an existing supported database	
Data Source Name (DSN): VCDB (MS SQL)	×
InstallShield Sack Next :	> Cancel

18. Enter the password <<var_password>> for vpxuser

🙀 VMware vCenter Simple I	Install	×
Database Options		
Enter database server cred	lentials.	
DSN:	VCDB	
ODBC Driver:	SQL Server Native Client 10.0	
Database user name:	vpxuser	_
Database password:		
InstaliShield		
	< Back Next >	Cancel

19. Click Next and read and OK the warning message (you will need to take separate action for backup of the SQL database).

1

👸 VMware	vCenter Simple Install	×
Databas	2 Options	
Enter da	tabase server credentials.	
DSN:	VCDB	
ODBC I	VMware vCenter Server	×
	Your SQL Server database is currently set to the Full reco model. Without regular transaction log backups, they will eventually consume all available disk space. See this KB ar more information: http://kb.vmware.com/kb/1001046.	· ·
Databa		
Databa		ОК
InstaliShield	< Back Next >	Cancel

20. Click Next to use the SYSTEM Account.

VMware vCenter Simple Ins	itall
vCenter Server Service	
Enter the vCenter Server serv	ice account information.
	r service runs in the Windows Local System account. To run another administrative user service account, deselect the ount credentials.
Vise Windows Local System	Account
Account name:	
Account password:	
	versa-vcenter.ppt.lab.cisco.com
Eully Qualified Domain Name:	Preisa-reencer.ppc.iab.cisco.com
	enter Server installer grants the "Log on as a service" right
SECURITY ADVISORY: The vC	,

21. Click Next to accept the default ports.

r Installer				
禮VMware vCenter Simple Install				
Configure Ports				
Enter the connection information for vCenter Server.				
vCenter Server HITP port:	80			
vCenter Server HTTPS port:	443			
Heartbeat port (UDP):	902			
Web Services HTTP port:	8080			
Web Services HTTPS port:	8443			
Web Services Change Service Notification port:	60099			
vCenter Server LDAP port:	389			
vCenter Server SSL pgrt:	636			
Increase the number of available ephemeral ports				
This option prevents the pool of available ephemeral ports Server powers on more than 2000 virtual machines simulta				
InstallShield				
< Back	Next > Cancel			

- 22. Select the appropriate inventory size. Click Next.
- 23. Click Install. A new installer window will start and complete in approximately 10 minutes.
- 24. Click Finish, then OK

Γ

ESXi Dump Collector Setup

- 1. In the VMware vCenter Installer window, under vCenter Support Tools, select VMware VSphere ESXi Dump Collector.
- 2. On the right, click Install.
- 3. Click Yes.
- 4. Select the appropriate language and click OK.
- 5. In the vSphere ESXi Dump Collector Installation Wizard, click Next.
- 6. Click Next.
- 7. Accept the terms in the License Agreement and click Next.
- 8. Click Next to accept the default Destination Folders.
- 9. Click Next to accept a Standalone installation.
- 10. Click Next to accept the default ESXi Dump Collector Server Port (6500).
- 11. Select the VMware vCenter Server IP address from the drop-down menu. Click Next.
- 12. Click Install to complete the installation.
- 13. Click Finish.
- 14. Click Exit in the VMware vCenter Installer window.
- 15. Disconnect the VMware vCenter ISO from the vCenter VM.
- Install all available Microsoft Windows updates by navigating to Start > All Programs > Windows Updates.
- 17. A restart might be required.
- 18. Back on the Management Workstation, open the VMware vSphere CLI command prompt.
- 19. Set each ESXi Host to core dump to the ESXi Dump Collector by running the following commands:

Note Make sure to type these commands since sometimes the hyphens do not cut and paste correctly (or you can do a find and paste with the hyphens).

```
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> system
coredump network set --interface-name vmk0 --server-ipv4
<<var_vcenter_server_ip> --server-port 6500
esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>> system
coredump network set --interface-name vmk0 --server-ipv4
<<var_vcenter_server_ip> --server-port 6500
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> system
coredump network set --enable true
esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>> system
coredump network set --enable true
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> system
coredump network set --enable true
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> system
coredump network check
esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>> system
coredump network check
esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>> system
```

an Administrator: C:\Windows\system32\cmd.exe	_ 🗆 🗙
	_
C:\Program Files\VMware\VMware vSphere CLI\bin>esxcli -s 172.26.163.51 -u p H1ghV0lt system coredump network setinterface-name vmk0server-ipv4 6.163.50server-port 6500	
C:\Program Files\UMware\UMware uSphere CLI\bin>esxcli -s 172.26.163.52 -u p H1ghUOlt system coredump network setinterface-name vmk0server-ipv4 6.163.50server-port 6500	
C:\Program Files\UMware\UMware vSphere CLI\bin> C:\Program Files\UMware\UMware vSphere CLI\bin> C:\Program Files\UMware\UMware vSphere CLI\bin> C:\Program Files\UMware\UMware vSphere CLI\bin>esxcli -s 172.26.163.51 -u p HighUØlt system coredump network setenable true	root -
C:\Program Files\UMware\UMware vSphere CLI\bin>esxcli -s 172.26.163.52 -u p H1ghVOlt system coredump network setenable true	root -
C:\Program Files\UMware\UMware vSphere CLI\bin> C:\Program Files\UMware\UMware vSphere CLI\bin>esxcli -s 172.26.163.51 -u p H1ghV0lt system coredump network check Verified the configured netdump server is running	root -
C:\Program Files\VHware\VHware vSphere CLI\bin>esxcli -s 172.26.163.52 -u p H1ghV0lt system coredump network check Verified the configured netdump server is running	root -
C:\Program Files\UMware\UMware vSphere CLI\bin>_	
	-

Set Up vCenter Server

vCenter Server VM

I

To set up vCenter Server on the vCenter Server VM, complete the following steps:

- 1. Using the vSphere Client, log in to the newly created vCenter Server as the VersaStack admin user or administrator@vsphere.local and password.
- 2. Click File, New, Datacenter to Create a data center.
- 3. Right click to rename the datacenter Enter VersaStack_DC_1 as the data center name.
- 4. Right-click the newly created VersaStack_DC_1 data center and select New Cluster.
- 5. Name the cluster VersaStack_Management and select the checkboxes for Turn On vSphere HA and Turn on vSphere DRS. Click Next.

Cluster Features What features do you want to	enable for this cluster?
Cluster Features /sphere DRS Power Management /sphere HA Virtual Machine Options VM Monitoring /Mware EVC Mi Swapfle Location Ready to Complete	Name VersaStack_Management Cluster Features Select the features you would like to use with this cluster. Image: Turn On vSphere HA vSphere HA detects failures and provides rapid recovery for the virtual machines running within a cluster. Core downtime when heartbeats cannot be detected. vSphere HA must be turned on to use Fault Tolerance. Image: Turn On vSphere DRS vSphere DRS enables vCenter Server to manage hosts as an aggregate pool of resources. Cluster resources ca machines. vSphere DRS also enables vCenter Server to manage the assignment of virtual machines to hosts automatically running virtual machines to balance load and enforce resource allocation policies. vSphere DRS and VMware EVC should be enabled in the cluster in order to permit placing and migrating VMs with the cluster in order to permit placing and migrating VMs with the cluster in order to permit placing and migrating VMs with the cluster in order to permit placing and migrating VMs with the cluster in order to permit placing and migrating VMs with the cluster in order to permit placing and migrating VMs with the cluster in order to permit placing and migrating VMs with the cluster in order to permit placing and migrating VMs with the cluster in order to permit placing and migrating VMs with the cluster in order to permit placing and migrating VMs with the cluster in order to permit placing and migrating VMs with the cluster in order to permit placing and migrating VMs with the cluster in order to permit placing and migrating VMs with the cluster in order to permit placing and migrating VMs with the cluster in order to permit placing and migrating VMs with the cluster in order

- 6. Accept the defaults for vSphere DRS. Click Next.
- 7. Accept the defaults for Power Management. Click Next.
- 8. Accept the defaults for vSphere HA. Click Next.
- 9. Accept the defaults for Virtual Machine Options. Click Next.
- 10. Accept the defaults for VM Monitoring. Click Next.
- 11. Accept the defaults for VMware EVC. Click Next.

Important. If mixing Cisco UCS B or C-Series M2 M3 and 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.

- 12. Select "Store the swapfile in the datastore specified by the host". Click Next.
- 13. Click Finish.
- 14. Right-click the newly created VersaStack Management cluster and select Add Host.
- **15.** In the Host field, enter either the IP address or the host name of the VM-Host-Infra_01 host. Enter root as the user name and the root password for this host. Click Next.
- 16. Click Yes.
- 17. Click Next.
- **18.** Select Assign a New License Key to the Host. Click Enter Key and enter a vSphere license key. Click OK, and then click Next.

I

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

- 21. Click Finish. VM-Host-Infra-01 is added to the cluster.
- 22. Repeat this procedure to add VM-Host-Infra-02 to the cluster.

Map the Datastores on the IBM Storwize V7000 Second Host After Enabling the Cluster

- 1. Open the web client to the Storwize V7000.
- 2. Click the volumes button in the left pane and select volume to open the volumes screen.
- 3. Right-click the volume infra_datastore_1 and select map to host.
- 4. Choose host VM-Host-Infra-02 and select Map Volumes.
- 5. Click Map All volumes on the warning popup click close.
- 6. Right-click the volume infra_swap and select map to host.
- 7. Choose host VM-Host-Infra-02 and select Map Volumes.
- 8. Click Map All volumes on the warning popup click close.
- 9. In vSphere in the left pane right click the cluster VersaStack_Management, and click rescan for datastores.

Note

At this point of the install, there is a warning for no network management redundancy. The optional Cisco 1000v virtual switch shown later is this document will remedy that issue. If you are not installing 1000v, you should add the second Cisco network adapter to the VMware standard switch to each ESX hosts by clicking on the configuration tab, and in the hardware pane, click Networking, click the properties of vSwitch0. From the Network adapters tab, click Add and select the unclaimed adapter vmnic1, and click Next, then click Next again and then click Finish.

Move VM Swap File Location

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

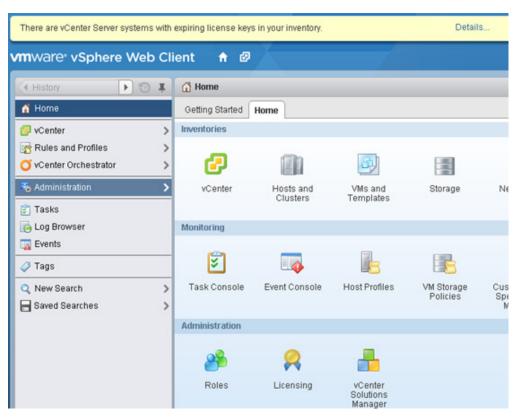
To move the VM swap file location, complete the following steps on each ESXi host:

- 1. From each vSphere Client, select the host in the inventory.
- 2. Click the Configuration tab to enable configurations.
- 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 infra swap as the datastore in which to house the swap files.
- 7. Click OK to finalize moving the swap file location.

Optional: Add Domain Account Permissions

In this section we will add a user to provide admin and login permissions in the Vshpere Web client and the VSphere client

- 1. Open a browser to the VSphere web client https://<<vSphere_ip>>:9443/vsphere-client/.
- 2. Log in as administrator@vshpere.local with the admin password.
- 3. Click the Administration item in the left pane.



4. Select configuration and identity sources tab and validate the domains you require are listed, or add and other domain with the green + .

mware [,] vSphere Web	Client 🕈 Ø			U I Administrator	@VSPHERELOCAL + I H
• Home > O	I SSO Configuration for	versa-vcenter.ppt.lab.cisco	o.com		
Administration	Policies Identity Source	ces Certificates			
 Access Control Roles 	+ / × @ @	Actions +			Q. Filter
	Name	Server URL	Туре	Domain	Aliat
 Single Sign-On 	-			vsphere.local	-
Users and Groups	-	-	Local OS	VERSA-VCENTER (default)	-
Configuration	ppt.lab.cisco.com	-	Active Directory (Integrated	ppt.lab.cisco.com	PPT
 Licensing 					
Licenses					
Reports					
 Solutions 					
Client Plug-Ins					
vCenter Server Extensions					

5. Select users and groups in the left pane and click Administrators.

Home E	I 🕹 vCenter Users and Groups		
Administration	Users Application Users Groups		
Access Control	🔶 📝 🗙 🖓 Actions 🗸		Q. Filter
Roles	Group Name	Domain	Depoiption
 Single Sign-On 	Users	vsphere.local	
Users and Oroups	SolutionUsers	vsphere.local	Well-known solution users' group, which contains
Configuration	DCAdmins	vsphere.local	
Licensing	VCOAdministrators	vsphere.local	VMware vCenter Orchestrator Administrators
Licenses	EdemailDPUsers	vsphere.local	Well-known external IDP users' group, which regis
Reports	Administrators	vsphere.local	
Solutions			
Client Plug-Ins			
vCenter Server Extensions			
	46		6 items

6. In the lower pane click the + to add group members.

I

Γ

Home > 🗇 🖡	S vCenter Users and Groups					
dministration	Users Application Users Groups					
Access Control	🔶 🖌 🗶 🖓 Actions -			Q Filter		
Roles Single Sign-On	Group Name	Domain		Description		
	Users	vsphere.local				
Users and Groups	SolutionUsers	vsphere.local		Well-known solution users' group, which co		
Configuration	DCAdmins	vsphere.local				
Licensing	VCOAdministrators	vsphere.local		VMware vCenter Orchestrator Administrator		
Licenses	EdemalDPUsers	vsphere.local		Well-known external IDP users' group, which		
Reports	Administrators	vsphere.local				
Solutions						
Client Plug-Ins						
vCenter Server Extensions						
	A6 6 item					
	Group Members					
	12			Q. Filter		
	Used Add member	Description/Full name	Domain	Member Type		
	Adr	Administrator vsphere.local	vsphere.local	User		

7. In the Add Principals dialog, select the proper domain, highlight a user, and click Add, then OK. You can now log in to the web client as that user.

udd Principals		(?
validate your entries against the directo	s in the Users text box. Click Check names ry.	to
Domain: ppt.lab.cisco.com		
Users and Groups		
Show Users First	Q Search	
Used/Group	2 A Description/Full name	
å 1	1	*
🔒 2	2	
281CBDB7-LGU000000	SR1 2B1CBDB7-LGU000000	
281CBDB7-LGU000001	SR1 2B1CBDB7-LGU000001	
281CBDB7-LGU000002	SR1 2B1CBDB7-LGU000002	
2B1CBDB7-LGU000003	SR1 2B1CBDB7-LGU000003	
281CBDB7-LGU000004	SR1 2B1CBDB7-LGU000004	٣
		Add
Users: ppt.lab.cisco.com\1		
Groups:		
Separate m	nultiple names with semicolons Check	names
	ОК	Cancel

8. In the vSphere client, log in as the administrator account and right-click the appropriate level for permissions and click Add Permissions.

I

File Edit View	opt.lab.cisco.com - vSphere Client Inventory Administration Plug-ins Help Home & 🛃 Inventory 🕨 🗊 Hosts and Clusters
	eritopt.leb.cisc uarea ucenter pat lab cisco com, 10.29.151.102 VMware vCer New Folder Ctrl + F Virtual Machines Hosts Tasks New Datacenter Ctrl + D Virtual Machines Hosts Tasks
	Add Permission Ctrl+P rs view? Alarm omputing resources that run
8	Open in New Window Ctrl+Alt+N Remove Rename
	SimpliVity - Create Support Capture Basic Tasks Create a datacenter Host

- 9. Select Add.
- **10.** Highlight a user and click Add, then click OK.

10.29.151.51 10.29.151.52	To assign a permit	🖉 Select Users and Groups 📃 🗾	e or more of the
New Template Sql This ver on a par	names and assign	Select users and groups to include in this role. You can also manually enter names and use the Check Names feature to validate your entries against the directory.	
vcenter-old Hosts & mventor	-Users and Groups	Domain: ppT 💌	
	These users and g according to the s	Users and Groups	urrent object
Basic T		Show Users First Search	
Cre	Name	Name Description / Full Name	2
		2 291C8D87-LGU000016 SR 1 291C8D87-LGU000016	
		3.MP2\$	
		281C8D87-LGU000055 SR1281C8D87-LGU000055	1
		SM_1a936e8504aa4b9da MSExchApproval 1f05a927-3be2-4	4
		8 1 1 *	
		Add	
		Users: ppt\1	
		Groups:	ption
		Note: Separate multiple names with semicolons.	
		Check Names	
		Check Names	
		OK Canoel	

I

Γ

11. Change the assigned role to the correct group, and click OK. Log off as administrator and back in as that domain user.

Fo assign a pe names and as		lividual or gro	up of users, add their r	ames to the Users and Groups list below. Then select one or	more of the
	ips nd groups can int he selected role.	eract with the	current object	Assigned Role Selected users and groups can interact with the curre according to the chosen role and privileges.	nt object
Name	Role	Propag		Read-only	
PPT\1	Read-only	Yes		Read-only Administrator Virbual machine power user (sample) Virbual machine user (sample) Resource pool administrator (sample) VMware Consolidated Backup user (sample) Datastore consumer (sample) Network administrator (sample) Image: Section administrator (sample) Imad	r n
	Ad	d	Remove	Propagate to Child Objects	

IBM Storwize V7000 File Module Configuration

The file modules are installed to leverage file level protocol in your VersaStack such as NFS and CIFS. In this section we will be creating and mapping NFS Datastores.



This section is not applicable unless you purchased the optional IBM Storwize V7000 file modules.

Initialization of the IBM Storwize V7000 file modules



You will need your IBM login account to download software.

- 1. Download the up2nas utility from IBM Fix Central.
 - a. Go to http://www-933.ibm.com/support/fixcentral/.
 - **b.** In product selector, enter "IBM Storwize V7000 Unified," select All releases and All platforms. Click Continue.

Fix Central

system. Not look	es fixes and updates for your system's software, hardware, and operating ing for fixes or updates? Please visit <u>Passport Advantage</u> to download most re products, or <u>My Entitled Systems Support</u> to download system software.
For additional info	rmation, click on the following link. I with Fix Central
Find product	Select product
Type the product	name to access a list of product choices.
When using the k the results list.	reyboard to navigate the page, use the Tab or down arrow keys to navigate
Product selector	*
IBM Storwize V70	00 Unified
Release*	
All	•
Platform [*] All •	
Continue	

2. Scroll down and in the "Product Tools" section, click StorageDisk-2073-ConversionUtility.

- **3.** Enter your system details and follow instructions to download the utility. This required system information can be obtained by login in the IBM web client, and from the monitoring icon in the left pane, click the system details menu item, expanding your VersaStack components tree, and click the cluster enclosure.
- 4. Use scp to copy the utility from a server to /upgrade of the V7000 control enclosure, using the management IP address:

scp IBM2076_INSTALL_up2nas_1.5.1.2 superuser@10.29.151.21:/upgrade/ superuser@10.29.151.21's password: IBM2076_INSTALL_up2nas_1.5.1.2 100% 12KB 12.3KB/s 00:00

5. SSH to the V7000 control enclosure using the management IP address, then use the CLI to install the utility:

```
applysoftware - file IBM2076_INSTALL_up2nas_1.5.1.2
CMMVC6227I The package installed successfully.
```

6. Run stopemail.

stopemail

7. Use the CLI to run the up2nas utility, which will check that the V7000 control enclosure is connected to the file modules through the direct fibre channel connection:

```
up2nas
#UP2NAS001I This is Version 1.5.1.2 of the upgrade to NAS checker utility
for adding IBM 2073 file modules to an existing IBM Storwize V7000 system
    has_nas_key=no
    code_level=7.3.0.8
    email_state=stopped
#UP2NAS003I The V7000 can see the file modules from the fibre channel ports
    lssoftwareupgradestatus=inactive.
    OK
#UP2NAS004I The V7000 is ready for the file modules to be added. #UP2NAS001A
Do you have the IP addresses that will be used for file module management ?
    (y/n)
```

8. For the do you have the IP addresses, type y.

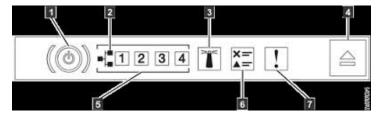
```
OK
V7000_SYSTEM_IP = 10.29.151.21
SUBNET_MASK = 255.255.255.0
GATEWAY_IP = 10.29.151.1
#UP2NAS002A What is the management IP address for the V7000 Unified system ?
```

9. Enter the <<var_v7000_unified_management_IP>>, <<var_file_module_1_service ip>> and <<var_file_module_2_service ip>> and wait for the tool to check the addresses are available.

```
#UP2NAS002A What is the management IP address for the V7000 Unified system ?
10.29.151.31
MANAGEMENT_IP = 10.29.151.31 subnet OK
#UP2NAS003A What is the service IP address for file module 1 ?
```

```
10.29.151.32
FILE_MODULE_1_IP = 10.29.151.31 subnet OK
#UP2NAS004A What is the service IP address for file module 2 ?
10.29.151.33
FILE_MODULE_2_IP = 10.29.151.33 subnet OK
#UP2NAS007I Please wait while the network is checked to make sure that these
new IP addresses are not already being used.
MANAGEMENT_IP=10.29.151.31 did not respond to ping
FILE_MODULE_1_IP=10.29.151.32 did not respond to ping
FILE_MODULE_2_IP=10.29.151.33 did not respond to ping
MANAGEMENT_IP = 10.29.151.31 OK
#UP2NAS009A Is the blue Identify LED blinking on each of the file modules ?
(y/n)
```

10. Confirm the blue identify LED is blinking on both file modules - #3 on the picture below:



- 11. Type y and press Enter.
- 12. Locate the USB flash drive that came packaged with the file modules, then type y and press Enter.



If you do not have the USB that came with the system, please use a blank writable USB.

```
#UP2NAS006A Do you have the USB flash drive that came with the file modules
? (y/n)
Y
OK
enclosure=1
canister=1
```

- **13.** Check the rear of the V7000 control enclosure and you should see the amber fault LED blinking on the left-hand canister.
- 14. Follow the instruction to insert the USB flash drive into a USB port on the canister with the blinking amber LED and wait for the amber LED to quit blinking and stop. This will take up to 60 seconds, or approximately 40 blinks. When the amber LED stops blinking, type y and press Enter.

```
#UP2NAS009I Put the USB flash drive into the control enclosure node canister
with the amber Fault LED blinking..
#UP2NAS007A The amber Fault LED should stop blinking about 14 blinks after
it is inserted
#UP2NAS007A But DO NOT remove the USB flash drive yet.
#UP2NAS007A Has the amber fault LED stopped blinking ? (y/n)
Y
OK
```

15. Remove the USB flash drive from the V7000 control enclosure

16. Follow the instruction to insert the USB flash drive into a USB port in the upper file module. Wait for the blue identify LED on the upper file module to quit blinking and stop. This can take up to 3 minutes. The blue identify LED on the lower file module should continue to blink another 3 or 4 times then stop.

#UP2NAS010I (1) Put the USB flash drive into the upper file module. #UP2NAS010I (2) Wait for the blue Identify LED on each of the file modules go out or start blinking again.

17. With a few minutes after inserting the USB flash drive, you will be able to open a browser and navigate to the file module management GUI using <<var_v7000_unified_management_IP>>,and monitor the initialization progress. The process could take over 30 minutes.

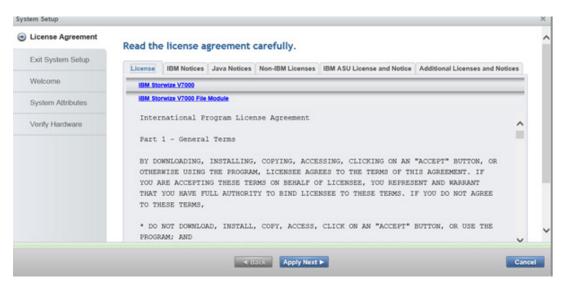
	v C Q Search	
 7000 Unified System Initialization		
 7000 onmed system initialization		-
The system is currently undergoing initialization. No action can be p	performed until & completes. This process takes	
approximately 75 minutes to complete, tohen the process complete you can begin configuring your system.	is. The Easy Setup woard will automatically open, and	
Status: Updating the code repositories.		
(2 interiorg		
See las		
SOR		

18. When initialization is complete, the management GUI login page will load. Log in using the admin account with password admin0001.

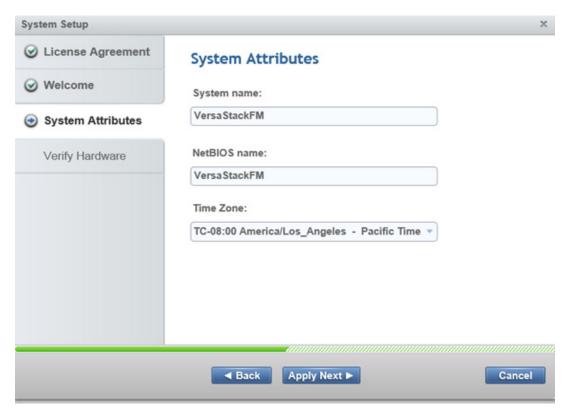
ſ



19. Review the license agreement, scroll to the bottom and click I agree and click Apply Next, then click Close.



- 20. Click Next on the Welcome screen.
- 21. Enter the <<var_filemodule_name>> for the system and re-enter, <<var_filemodule_name>> for the NetBIOS name and click the drop-down to select a timezone, click Apply Next. Wait a few minutes for the tasks to complete, then click Close.



22. On the Verify Hardware screen, review the drive counts and click Finish.



23. Click Close.

ſ



24. In the What to do next? window, click NAS File Services.

What to do next?	×
NAS File Services	
Service Support	
Note: You can open the wizards from the management GUI if you choose not to follow them now.	
Close	

- 25. Click Next.

NAS File Services		×
@ Welcome	NTP servers:	
NTP and DNS	NTP server	
-	171.68.38.65	
Public Networks	DNS domain name:	
Authentication	ppt.lab.cisco.com	
Access Control	DNS servers:	
	DNS Server	
	10.29.130.112	
	DNS search domains:	
	DNS Search Domain	
	ppt.lab.cisco.com	
		Cancel

- 27. Click Create Network to bring up the Network Screen.
- 28. On the Network screen, input <<var_unified_bond_ip_network>> <<var_unified _bond_ip_Netmask>> <<var_nfs_vlan_id>> <<var_unified_bond_ip_gateway>> <<var_unified_bond_public_ip>> Select the 10gig card for the interface (ethX1). The IP address field is the address of the subnet, example 172.17.72.0 and the Public Network is the actual network IP you will mount from vSphere, example 172.17.72.41. Click OK, then click Close, then click Next.

Note

I

Do not create any additional Networks at this point as we will delete this network and recreate it after setup to enable LACP support.

create Network		×
IP Address:	Network Mask:	
172.17.72.0	255.255.255.0	
VLAN ID:		
3172 🗘		
Default gateway:		
172.17.72.1		
Public network IP pool:		
IP Addresses		
172.17.72.41	00	
Additional gateways:		
Subnet	IP Addresses	
ſ		v
interface:		
ethX1 (10GbE) 💌		

29. Select the authentication method of Active Directory then click Next.

NAS File Services		×
Welcome	Authentication Method	
NTP and DNS	Select the user authentication method:	
Public Networks	Active Directory LDAP	
Authentication Active Directory Kerberos	 Samba primary domain controller (PDC) NIS (NFS clients only) 	
ID Mapping	Local Authentication	
Netgroups for NFS		
Access Control		
	Back Next	Cancel

I

1

30. Input the Domain Controller IP, Domain Admin username and login. Do not include the domain when specifying the User ID. Click Next.

NAS File Services			х
	Active Directory		
O NTP and DNS	Server:		
Public Networks	10.29.130.112		
Authorities	User ID:	Password:	
 Authentication Active Directory Kerberos 	1	•	
ID Mapping	Use preferred domain control	lers	
Netgroups for NFS	Domain controller		00
Access Control			
	Back Next)		Cancel

- **31.** For the Kerberos screen accept the default and click Next.
- 32. For ID Mapping Method accept the default of Master and click Next.
- 33. For the ID Mapping Role screen accept the default and click Next.
- 34. For the Automatic ID Mapping screen accept the default and click Next.
- 35. For the Netgroups for NFS screen accept the default and click Apply Next, then click Close.

NAS File Services			1
⊘ Welcome	Netgroups for NF	5	
✓ NTP and DNS	Use NIS server to sea	rch for netgroup for NFS clients	
Public Networks	NIS domain:		
Authentication			
ID Mapping	Server map:		
C ID mapping	NIS Server	NIS Domain	
Netgroups for NFS			
Access Control			
		a 1111	
	Back Ap	ply Next ►	Cancel

36. Select the primary Sharing Method as NFS and click Next.

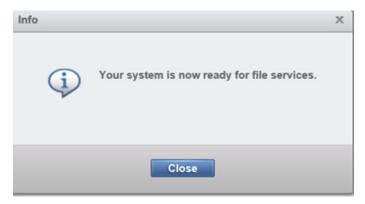
ſ



37. Accept the default permissions as these can be changed later and click Finish. Click Close.

NAS File Services					;
⊘ Welcome	Owner:		Owning group:	Owning group:	
ONTP and DNS	root		root	root	
Public Networks	Access Control				111 11
0.000	Туре	Name	Access	Read	Write
 Authentication 	Special Owner		Allow	~	~
•	Special Group		Allow	~	~
 Access Control Ownership and ACL 					
	Edit			_	>
	a Ba	ick Finish			Cancel

38. On the Info screen, click Close.



a. For What to do Next? Click Service Support. Click Next on the Welcome Screen.

What to do next?	×
Service Support	
Note: You can open the wizards from the management GUI if you choose not to follow them now.	
Close	

39. For the Service IP Port, accept the settings and click Next.

I

40. On the Call home screen enter the <<var_mailhost_ip>>,<<var_org>>, <<var_email_contact>> <<var_admin_phone>>.

Support Services		×
✓ Welcome	The call home function enables the system to automatically notify IBM Support abou the hardware configuration and status of the system. Using this information, IBM	^
Service IP Port	Support can contact the system administrator in case of any issues. Do you want to set up call home?	4
Call Home	Yes No No	
	Email server IP address:	
	Test Server Connection	
	Company name: Contact email:	
	Contact phone number: Off-shift phone number:	
	IBM Support email address:	
	callhome1@de.ibm.com	
	Allow automatic access to the Internet	~
	Back Finish Cancel	el

1

41. Click Finish then click Close, click Close again to complete a wizard. This will initialize a reboot.

🔆 EFSSG0010I An operating system reboot was initiated by admin.		50%
View more details		
EFSSG0292W The node mgmt002st001 was not restarted yet. Check later to see whether the action was successfully finished or not.	2:31	
The task is 50% complete.	2:31	PM
Running command:	2:31	PM
<pre>initnodenode mgmt001st001rebootcluster 18151646033387816619</pre>	2:31	PM
EFSSG1009W Rebooting the node might break the quorum configuration or cause loss of access	2:31	PM
EFSSG0010I An operating system reboot was initiated by admin.	2:31	PM 🗸



Deleting and Re-creating Network Bonds that are LACP Compliant and MTU of 9000

In this section we will be deleting the default network bond created during the wizard and recreating it as LACP compliant with the proper MTU size.

1. After the reboot login to the file module web console and click on the bottom left icon for settings, network in the menu, then click NAS Public Networks.

Network	Networks for I	NAS Clients		
NAS Public Networks	Configure the public r services to external of	network which external clients can us clients.	e to reach the system. This includes	all networks used to provide NAS
NAS Public Network	+ Create Network	E Actions Q. Filter	-	Showing 1 Item Selected 1
Interfaces	Subnet 🔺	Gateways	IP Addresses	
	172.17.72.01/24	0.0.0.0/0:172.17.72.1	172.17.72.41	
Service IP Addresses	18			
ISCSI				
- Incar				
Fibre Channel				
Connectivity				
IP Report				
Ethernet Ports for Block				
Storage				
	*	11		
	A CONTRACTOR OF A CONTRACTOR OFTA CONTRACTOR O			

2. Right-click the interface and click Delete, then click Yes, then click Close.

ſ

Network	Networks fo	or NAS Clients		
NAS Public Networks	Configure the pub services to extern	blic network which external clients can hal clients.	use to reach the system. This include	s all networks used to provide NAS
NAS Public Network	a second s	rk 🗉 Actions 🔍 Filter 📓		Showing 1 dem Selected 1 d
Interfaces	Subnet 172.17.72.31/94	 Gateways 00000172,17,72,1 	IP Addresses 172,17,72,41	
Service IP Addresses		Edit		
ISCSI				
Fibre Channel Connectivity				
IP Report				
Ethernet Ports for Block Storage				
	0.000			

I

- **3.** Open a Putty session and login to the IP address of the file module as admin with password of admin0001.
- 4. Run "Isnwinterface -x" to see the interfaces. Take note of the 10 gig bond interface.

```
[kd52x9w.ibm] $ lsnwinterface -x
Node
             Interface MAC
                                         Master/Subordinate Bonding mode
Transmit hash policy Up/Down Speed IP-Addresses MTU
mgmt001st001 ethX0
                        e4:1f:13:d6:0d:88 MASTER
                                                              active-backup
                                  1000
                                                      1500
(1)
                          UP
mgmt001st001 ethXs10_0 e4:1f:13:d6:0d:88 SUBORDINATE
UΡ
        1000
                            1500
mgmt001st001 ethXs10_1 e4:1f:13:d6:0d:88 SUBORDINATE
UΡ
        1000
                            1500
mgmt001st001 ethX1
                        00:00:c9:bb:af:06 MASTER
                                                              active-backup
                                                      1500
(1)
                          UP
                                  10000
mgmt001st001 ethXsl1_0 00:00:c9:bb:af:06 SUBORDINATE
UΡ
        10000
                            1500
mgmt001st001 ethXsl1_1 00:00:c9:bb:af:06 SUBORDINATE
        10000
UΡ
                            1500
mgmt002st001 ethX0
                        e4:1f:13:d5:f3:e0 MASTER
                                                              active-backup
                                                      1500
(1)
                                  1000
                          UP
mgmt002st001 ethXs10_0 e4:1f:13:d5:f3:e0 SUBORDINATE
UΡ
        1000
                            1500
mgmt002st001 ethXsl0_1 e4:1f:13:d5:f3:e0 SUBORDINATE
        1000
UΡ
                            1500
mgmt002st001 ethX1
                        00:00:c9:bb:ae:ce MASTER
                                                              active-backup
                                  10000
                                                      1500
(1)
                          UP
mgmt002st001 ethXsl1_0 00:00:c9:bb:ae:ce SUBORDINATE
UΡ
        10000
                            1500
mgmt002st001 ethXsl1_1 00:00:c9:bb:ae:ce SUBORDINATE
        10000
UΡ
                            1500
EFSSG1000I The command completed successfully.
```

5. Run "rmnwbond mgmt001st001 ethX1" to remove the network bond on file module 1.

```
[kd52x9w.ibm]$ rmnwbond mgmt001st001 ethX1
EFSSG1000I The command completed successfully.
```

6. Run "Isnwinterface -x " to view the interfaces and note on file module node 1, which interfaces are 10gig. (in this example eth0 and eth1 are 10 gig).

```
[kd52x9w.ibm] $ lsnwinterface -x
Node
             Interface MAC
                                          Master/Subordinate Bonding mode
Transmit hash policy Up/Down Speed IP-Addresses MTU
mgmt001st001 eth0
                     00:00:c9:bb:af:06
        10000
                            1500
TTP
                      00:00:c9:bb:af:08
mgmt001st001 eth1
UΡ
        10000
                            1500
mgmt001st001 ethX0
                        e4:1f:13:d6:0d:88 MASTER
                                                               active-backup
(1)
                          IIP
                                   1000
                                                       1500
mgmt001st001 ethXs10_0 e4:1f:13:d6:0d:88 SUBORDINATE
UP
        1000
                            1500
mgmt001st001 ethXs10_1 e4:1f:13:d6:0d:88 SUBORDINATE
UP
        1000
                            1500
mgmt002st001 ethX0
                        e4:1f:13:d5:f3:e0 MASTER
                                                               active-backup
(1)
                          IIP
                                   1000
                                                       1500
mgmt002st001 ethXs10_0 e4:1f:13:d5:f3:e0 SUBORDINATE
        1000
                            1500
TTP
mgmt002st001 ethXs10 1 e4:1f:13:d5:f3:e0 SUBORDINATE
        1000
                            1500
UP
                        00:00:c9:bb:ae:ce MASTER
mgmt002st001 ethX1
                                                               active-backup
(1)
                          IIP
                                   10000
                                                       1500
mgmt002st001 ethXsl1_0 00:00:c9:bb:ae:ce SUBORDINATE
UΡ
        10000
                            1500
mgmt002st001 ethXsl1 1 00:00:c9:bb:ae:ce SUBORDINATE
        10000
                             1500
UP
EFSSG1000I The command completed successfully.
```

7. Run the **mknwbond** command with the correct parameters to make a new bond with the 2 x 10 gig interfaces on file module node 1. The -mode 4 switch will enable LACP on the bond to allow the virtual port channels on the Cisco switch.

"mknwbond mgmt001st001 eth0, eth1 --mode 4 --mtu 9000"

[kd52x9w.ibm]\$ mknwbond mgmt001st001 eth0,eth1 --mode 4 --mtu 9000 EFSSG0577W Warning: creating a bond with mode 802.3ad (4) might require additional switch configuration work to access the network. EFSSG0089I Network bond ethX1 successfully created. EFSSG1000I The command completed successfully.

8. Run "Isnwinterface -x " to view the new bond. Note that it is 20 gig and 802.3ad.

```
[kd52x9w.ibm] $ lsnwinterface -x
Node
             Interface MAC
                                         Master/Subordinate Bonding mode
Transmit hash policy Up/Down Speed IP-Addresses MTU
mgmt001st001 ethX0
                        e4:1f:13:d6:0d:88 MASTER
                                                               active-backup
                                  1000
                                                      1500
(1)
                          UP
mgmt001st001 ethXs10 0 e4:1f:13:d6:0d:88 SUBORDINATE
UP
        1000
                            1500
mgmt001st001 ethXs10 1 e4:1f:13:d6:0d:88 SUBORDINATE
UΡ
        1000
                            1500
```

```
mgmt001st001 ethX1
                       00:00:c9:bb:af:06 MASTER
                                                              802.3ad (4)
                     UΡ
                              20000
layer3+4
                                                  9000
mgmt001st001 ethXsl1_0 00:00:c9:bb:af:06 SUBORDINATE
        10000
UΡ
                            9000
mgmt001st001 ethXsl1 1 00:00:c9:bb:af:06 SUBORDINATE
        10000
                            9000
UΡ
mgmt002st001 ethX0
                        e4:1f:13:d5:f3:e0 MASTER
                                                              active-backup
(1)
                          UP
                                  1000
                                                      1500
mgmt002st001 ethXs10_0 e4:1f:13:d5:f3:e0 SUBORDINATE
UP
        1000
                            1500
mgmt002st001 ethXs10_1 e4:1f:13:d5:f3:e0 SUBORDINATE
        1000
                            1500
UΡ
mgmt002st001 ethX1
                        00:00:c9:bb:ae:ce MASTER
                                                               active-backup
(1)
                          UP
                                  10000
                                                      1500
mgmt002st001 ethXsl1_0 00:00:c9:bb:ae:ce SUBORDINATE
        10000
UP
                            1500
mgmt002st001 ethXsl1 1 00:00:c9:bb:ae:ce SUBORDINATE
        10000
                            1500
UP
EFSSG1000I The command completed successfully.
```

9. Remove the bond from file module 2 "rmnwbond mgmt002st001 ethX1."

[kd52x9w.ibm]\$ rmnwbond mgmt002st001 ethX1 EFSSG1000I The command completed successfully.

 Run the "lsnwinterface -x" command and take note of the available 10gig interfaces for file module 2.

```
[kd52x9w.ibm] $ lsnwinterface -x
Node
             Interface MAC
                                         Master/Subordinate Bonding mode
Transmit hash policy Up/Down Speed IP-Addresses MTU
mgmt001st001 ethX0
                       e4:1f:13:d6:0d:88 MASTER
                                                              active-backup
                         UΡ
                                  1000
                                                      1500
(1)
mgmt001st001 ethXs10 0 e4:1f:13:d6:0d:88 SUBORDINATE
UΡ
        1000
                            1500
mgmt001st001 ethXs10_1 e4:1f:13:d6:0d:88 SUBORDINATE
UΡ
        1000
                            1500
mgmt001st001 ethX1
                       00:00:c9:bb:af:06 MASTER
                                                             802.3ad (4)
                     UΡ
                              20000
                                                  9000
layer3+4
mgmt001st001 ethXsl1_0 00:00:c9:bb:af:06 SUBORDINATE
ΠP
        10000
                            9000
mgmt001st001 ethXsl1_1 00:00:c9:bb:af:06 SUBORDINATE
UΡ
        10000
                            9000
mgmt002st001 eth0
                     00:00:c9:bb:ae:ce
        10000
                            1500
UΡ
mgmt002st001 eth1
                     00:00:c9:bb:ae:d0
ΠP
        10000
                            1500
mgmt002st001 ethX0
                       e4:1f:13:d5:f3:e0 MASTER
                                                              active-backup
                                                      1500
(1)
                          UP
                                  1000
mgmt002st001 ethXs10_0 e4:1f:13:d5:f3:e0 SUBORDINATE
UΡ
        1000
                            1500
mgmt002st001 ethXs10_1 e4:1f:13:d5:f3:e0 SUBORDINATE
UΡ
        1000
                            1500
EFSSG1000I The command completed successfully.
```

 Create a bond on file module node 2 with the available interfaces. "mknwbond mgmt002st001 eth0,eth1 --mode 4 --mtu 9000."

[kd52x9w.ibm]\$ mknwbond mgmt002st001 eth0,eth1 --mode 4 --mtu 9000 EFSSG0577W Warning: creating a bond with mode 802.3ad (4) might require additional switch configuration work to access the network. EFSSG0089I Network bond ethX1 successfully created.

12. Re-create the NAS Public Network by opening the File Module Management Console, open the Settings in the left tab, click Network and then click NAS Public Networks.



<<var_unified_bond_ip_gateway>> <<var_unified_bond_public_ip>>. Select the 20 gig network for the interface. The IP address field is the address of the subnet, example 172.17.72.0 and the Public Network are the actual network IPs you will mount from vSphere, example 172.17.72.41. Repeat to create any additional networks required at this point. Click OK, then click Close, and then click Next.

Create Network					×
IP Address:	Network	Mask:			
172.17.72.0	255.255.	255.0			
VLAN ID:					
3172					
Default gateway:					
172.17.72.1					
Public network IP pool:		Additional gateways:			
IP Addresses		Subnet	IP Addresses		
172.17.72.41				Θ	
Interface:					
Not attached 💌					
Not attached					
ethX0 (1GbE)		ок	Cancel		
ethX1 (20GbE)			Ganger		

Configuring the Cisco Nexus Switch Networking

In this section, you will create and configuring the Port Channels on the switch for the File modules. Port Channels will be created. Port Channel 11 will be for the V7000 File Module A and Port Channel 12 will be used for the File Module B.

Cisco Nexus 9000 A

- 1. Open a Putty session to the Cisco Nexus 9000 Switch A.
- 2. Define a description for the port-channel connecting to <<var_filemodule_name>>-A.

```
config -t
interface Poll
description <<var filemodule name>>-A
```

3. Make the port-channel a switchport, and configure a trunk to allow in-band management, NFS, VM, 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_nfs_vlan_id>>,
< <var_vmotion_vlan_id>>, <<var_vm_traffic_vlan_id>>,
```

I

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

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

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

mtu 9216

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

vpc 11 no shutdown

7. Define a port description for the interface <<var filemodule name>> -A.

```
interface Eth1/1
description <<var_filemodule_name>>-A
8. Apply it to a port channel and bring up the interface.
```

```
channel-group 11 force mode active no shutdown
```

9. Define a description for the port-channel connecting to <<var_filemodule_name>>-B.

```
interface Po12
description <<var_filemodule_name>>-B
```

10. Make the port channel a switchport and configure a trunk to allow InBand management, NFS, VM and also 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_nfs_vlan_id>>,
<<var_vmotion_vlan_id>>, <<var_vm_traffic_vlan_id>>,
```

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

spanning-tree port type edge trunk

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

mtu 9216

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

vpc 12 no shutdown

14. Define a port description for the interface <<var_filemodule_name>>-B.

```
interface Eth1/2
description <<var_filemodule_name>>-B
```

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

```
channel-group 12 force mode active
no shutdown
copy run start
```

Cisco Nexus 9000 B

- 1. Open a Putty session to the Cisco Nexus 9000 Switch B.
- 2. Define a description for the port-channel connecting to <<var_filemodule_name>>-B.

```
config -t
interface Po12
description <<var filemodule name>>-B
```

3. Make the port-channel a switchport and configure a trunk to allow in-band management, NFS, VM, 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_nfs_vlan_id>>,
< <var_vmotion_vlan_id>>, <<var_vm_traffic_vlan_id>>,
```

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

spanning-tree port type edge trunk

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

mtu 92166. Make this a VPC port-channel and bring it up.

vpc 12 no shutdown

7. Define a port description for the interface <<var filemodule name>>-B.

```
interface Eth1/1
description <<var filemodule name>>-B
```

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

```
channel-group 12 force mode active no shutdown
```

9. Define a description for the port-channel connecting to <<var filemodule name>>-A.

```
interface Poll
description <<var_filemodule_name>>-A
```

10. Make the port-channel a switchport and configure a trunk to allow InBand management, NFS, VM and also 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_nfs_vlan_id>>,
<<var_vmotion_vlan_id>>, <<var_vm_traffic_vlan_id>>,
```

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

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

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

mtu 9216

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

vpc 11 no shutdown

14. Define a port description for the interface <<var_filemodule_name>>-A.

```
interface Eth1/2
description <<var filemodule_name>>-A
```

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

```
channel-group 11 force mode active
no shutdown
copy run start
```

Create a NAS Datastore and Export

To create a NASA datastore, complete the following steps:

1. Open the management console and select files, then file systems, then click Create File Systems.

A VerstackFM > Files > File Syste	ms	6	M V7000 Unded admin (Admin	istrator, Export Administrator, Storage Admir
Create File System Name	Create File System	1	×.	×
	Single Pool	Compressed	Migration-ILM	Custom
	Owner: root File system pool name: system		Jwning group: oot	Edit
			Capac Capacity 20.08 TIB 20.35 TIB	Showing 1 pool Selecting 1 pool
· · · · · · · · · · · · · · · · · · ·		0	Cancel	

Leave Single Pool selected input the values for your datastore name
 <<var_unified_datastore_name>>, then scroll down to the bottom to input the size of
 your NFS datastore.

😭 VerstackFM > Files >	Create File System					×
Create File	Single Pool		Compressed	Migration-ILM	Custorn	
	File system pool name: system Select a storage pool:				Showing 1 pool Selecting 1 poor	
B	Name A	Status	Free Capac		В	
	Size:	≎ GB				
			ОК	Cancel		

1

3. Click OK and then click Yes.

V	File system name:	VM-Host-Infra-2	
		system, 500.00 GiB	
	Pools:	+500.00 GiB(7 volumes) from storage pool mdiskgrp0	
	Replication policy:	Nothing	
	Maximum numb of inodes of the root file set:	10,000,000	

4. Click the Files icon in the left menu bar and then click Shares, then click Create Share.

Share Name 🔺	Create Share			× CP
	CIFS		23	
194	CIFS	NES	Custom	_
	Path:		Browse	
A	Share name:			
<u> </u>	•			
4	Owner:	Owning group:		
	•	•	Edut	
-01	Add NFS client. Reorder the clients as r	weeded.		
	+ Create NFS client E Actions		Showing Ø Rems Selected Ø Ren	
H	Name or IP Address Access Typ		Security Type	2
A.		No items found.		
and the second s				
SP .				
		OK Cancel		

5. Click NFS for Share type in the center of the screen then click Browse to select the directory. Click OK.

reate Share	Browse	×	l
8	Create Directory Create Directory WM-Host-Infra-2		the second
Path:			
Share name:		=	
Owner:			
Add NFS client. I			
Name or IP Ad			l
	Path: //ibm/VM-Host-Infra-2		1
	OK Cancel		l

Γ

- 6. Enter the share name and if required edit the owner and owning group.
- 7. Click Create NFS client and input the NFS-Vlan VMkernel IP for Host esx host 1, <<var_nfs_vlan_id_ip_host-01>> for the IP address for the NFS vlan.
- 8. Change the Access Type to Read/Write and change the Root squashing to to No Root Squash. Click Add, then repeat these steps for ESX server 2 NFS VMkernel IP using the <<var_nfs_vlan_id_ip_host-02>> for the IP address.

Add NFS Client		x
Name or IP address:	172.17.72.51]
Access type:	Read/Write	•
Root squashing:	No Root Squash	•
Security type:	System (sys)	•
Anonymous UID:		
Anonymous GID:		
Port security:	Secure	•
	Add Cancel	

- 9. Click Ok to create the share.
- 10. Click Close.

Mount the NAS Datastore on ESX

To mount the NAS datastoreon ESX, complete the following steps:

- 1. Open the vSphere Client and select inventory, hosts and clusters and select host 1, VM-Host-infra-1.
- 2. Click the Configuration tab, then click Storage from the menu and then click Add Storage.

File Edit View Inventory /	Administration Plug-ins Help								
🖬 🖬 🛕 Home 🕨 👌	Inventory 🔸 🗊 Hosts and Cluste	rs					Search 1	inventory	
6 er 38									
Versa-vcenter.ppt.lab.csc Marao MersaStack_DC_1 Marao	10.29.151.51 VMware ESXi, 5.5. Getting Started Summary Virt.	0, 1746018 I al Machines F			ts Alarma	Permissions Mac	Storage Vews	Hardware Status	
10.29.151.51	Hardware	View: Data	stores Devices						
New Template	Processors	Datastores					Refresh D	elete Add Stor	19
sql vcenter	Memory	Status	Device	Drive Type	Capacity	Free Type	Last Update	Alarm Actions	
voenter-old Virtual Switch Ut	 Storage 	 Normal 	IBM Fibre Channel Disk. (Non-SSD	32.50 G	31.55 G VMPS5	1/15/20156:55:30.		
vsm2_primary	Networking	 Normal Normal 	IEM Fibre Channel Disk. (IEM Fibre Channel Disk. (Non-SSD Non-SSD	99.75 G	85.23 G VMFS5 147.89 G VMFS5	1/15/20156:55:30. 1/15/20156:55:30.		
🍅 vsm2_secondar	Storage Adapters Network Adapters Advanced Settings Power Management								
	Software	•			11				
	Licensed Features	Datastore D	etails						1
	Time Configuration DNS and Routing Authenbiation Services Power Management Virtual Machine Startup/Shutd Virtual Machine Startup/Shutd Virtual Machine Startup/Shutd Security Profile Host Cache Configuration								

3. Select Network File System and click Next.

Add Storage	
Select Storage Type Specify if you want to for	mat a new volume or use a shared folder over the network.
NAS Network: File System Ready to Complete	Storage Type C Disk/LUN Create a datastore on a Fibre Channel, ISCSI, or local SCSI disk, or mount an existing VMPS volume. Network File System Choose this option if you want to create a Network File System.
нер	< Back. Next > Cancel

4. In the <<var_unified _bond_public_ip>>for the server name, the share path for the folder, and <<var_unified_datastore_name>> for Datastore Name, then click Next, Then Finish

Note

Γ

To view the list NFS share paths by opening a Putty session to the file module management IP and typing in the command "lsexport"

Locate Network File Sys Which shared folder	stem will be used as a vSphere datastore?
AS Network File System eady to Complete	Properties Server 172.17.72.41 Examples: nas, nas.it.com, 192.168.0.1 or FEB0:0:0:0:2AA:FF:FE9A:4CA2 Folder //bm//MH-tost-infra-2 Example: /vols/vol0/datastore=001 Moi int MFS road only If a datastore already exists in the datacenter for this MFS share and you intend to configure the same datastore on new hosts, make sure that you enter the same input data (Server and Folder) that you used for the original datastore. Different input data would mean different datastore seven if the underlying NFS storage is the same.
	Datastore Name WH-Host-Infra-2
Help	< Back Next > Cancel

1

5. Select ESX Node 2, VM-Host-infra-2, and click Add Storage, then click Network file system and click Next.

	Administration Plug-ins Help		
🖬 👲 Home 🏄	Inventory 🕨 😗 Hosts and Cluster	15	Search Inventory
er set			
Untra-venter ppt lab.opt I venta-venter ppt lab.opt III vensitad, Dc_1 III (B) vensitad, Maray III (D2 151.51) III (D2 151.52) Children Kenglen III (TOD HIDTED VIHING EASING SED	Distance Designation Size Designation Tasks 8 Events Alamit. Permission Vew: Datatores Designation Tasks 8 Events Alamit. Permission Status Device Drive Type Capacity Free Image: Normal EMR/bre Channel Disk (Non-SSD 32:50 G 31:55 G Image: Normal EMR/bre Channel Disk (Non-SSD 99:75 G 85:23 G Image: Normal EMR/bre Channel Disk (Non-SSD 499:75 G 147:29 G	Reflech Deiste Add Storage Rescan Al Type Last Update Aarm Actions Storage Lo- WPS5 1/15/2015 7:00:52. Enabled Deabled WPS5 1/15/2015 7:01:59. makeled Deabled
	Software	x	,
	Licensed Features Time Configuration DNS and Routing Authenbration Services Power Management Virsul Machine Saruppfle Locat Security Frolle Host Cardin Configuration	Datastore Details	Properties

6. In the <<var_unified_bond_public_ip>> for the server name, NFS share path for the folder and <<var_unified_datastore_name>> for the Datastore Name, then click Next, then click Finish.

Locate Network File Sy: Which shared folder	stem wil be used as a vSphere datastore?
Network File System Ready to Complete	Properties Server [172.17.72.41] Examples: nas, nas.it.com, 192.168.0.1 or FEB0:0:0:0:2AA:FF:FE9A:4CA2 Folder [/bm//M-Host-infra-2] Example: /vols/vols/datastore-001 If a datastore already exists in the datacenter for this NFS share and you intend to configure the same datastore on new hosts, make sure that you enter the same input data (Server and Folder) that you used for the original datastore. Different input data would mean different datastores even if the underlying NFS storage is the same. Datastore Name [/M-Host-Infra-2]
e >	< Back Next > Cancel

- 7. It is recommended to also create and map a separate Swap file Datastore for VM's.
- 8. Optionally, use vMotion to migrate servers from the VMFS datastores to the NAS datastores.

Set Up the Optional Cisco Nexus 1000V Switch Using Cisco Switch Update Manager

Cisco Nexus 1000V

The Cisco Nexus 1000V is a distributed virtual switch solution that is fully integrated within the VMware virtual infrastructure, including VMware vCenter, for the virtualization administrator. This solution offloads the configuration of the virtual switch and port groups to the network administrator to enforce a consistent data center network policy. The Cisco Nexus 1000V is compatible with any upstream physical access layer switch that is compliant with Ethernet standard, Cisco Nexus switches, and switches from other network vendors. The Cisco Nexus 1000V is compatible with any server hardware that is listed in the VMware Hardware Compatibility List (HCL).

The Cisco Nexus 1000V has the following components:

- Virtual Supervisor Module (VSM)—The control plane of the switch and a VM that runs Cisco NX-OS.
- Virtual Ethernet Module (VEM)—A virtual line card that is embedded in each VMware vSphere (ESXi)host. The VEM is partly inside the kernel of the hypervisor and partly in a user-world process, called the VEM Agent.

Cisco Nexus 1000V Architecture

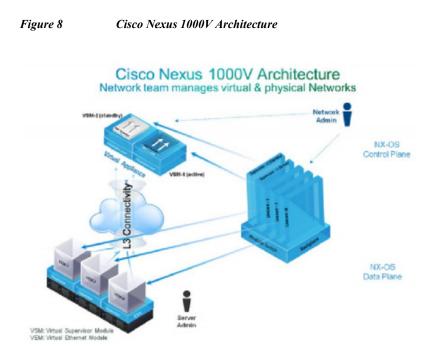


Figure 8illustrates the Cisco Nexus 1000V architecture.

Layer 3 control mode is the preferred method of communication between the VSM and the VEMs. In Layer 3 control mode, the VEMs can be in a different subnet than the VSM and from each other. Active and standby VSM control ports should be Layer 2 adjacent. These ports are used to communicate the HA protocol between the active and standby VSMs. Each VEM needs a designated VMkernel NIC interface that is attached to the VEM that communicates with the VSM. This interface, which is called the Layer 3 Control vmknic, must have a system port profile applied to it (see System Port Profiles and System VLANs), so the VEM can enable it before contacting the VSM.

1

Installation Process

To create network redundancy for the migration, create a temporary VMkernel.

ESXi Host VM-Host-Infra-01

Note

Repeat the steps in this section for all the ESXi Hosts.

- 1. From each vSphere Client, select the host in the inventory.
- 2. Click the Configuration tab.
- 3. Click Networking in the Hardware then properties
- 4. Click Add
- 5. Select VMkernel and click Next.

- 6. Change the network label to VMkernel-MGMT-2 and enter <<var_ib-mgmt_vlan_id>> in the VLAN ID (Optional) field.
- 7. Select Use this port for management traffic
- 8. Click Next to continue with the VMkernel creation.
- 9. Enter the IP address <<var_vmhost_infra_01_2nd_ip>> and the subnet mask for the VLAN interface for VM-Host-Infra-01.
- 10. Click Next to continue with the VMkernel creation.
- 11. Click Finish to finalize the creation of the new VMkernel interface.

Deploy the OVF Template for the Cisco Nexus 1000 Virtual Switch Update Manager

1. Log in and Download the Cisco Nexus 1000V installation software from www.cisco.com.

cisco	Products & Services	Support	How to Buy	Training & Events	Partne	ers 📃		
Download S	Software				I	A Download Ca	art (0 items)	(+) Feedbac
Downloads Home > Pr Virtual Switch Update		ual Networking > I	Nexus 1000V Switch fo	r VMware vSphere > Nex	us 1000V Swit	ch >		
Nexus 1000V Sw	itch							
								1
Expand All Collapse	Release 1.1	វជជជជ						Add De
Expand All Collapse	Release 1.1			Relea	se Date 👻	Size		
Expand All Collapse Latest All Releases	File Information Virtual Switch Upd	ate Manager			se Date 👻	Size 3429.69 MB		
Expand All Collapse	File Information	ate Manager					_	Add No

2. Unzip the package.

I

3. From the vSphere client, click File, Deploy OVF Template and browse to the unzipped ova file.

Deploy OVF Template		_ 🗆 ×
Source Select the source location.		
Source OVF Template Details Name and Location Storage Disk Format Ready to Complete	Deploy from a file or URL ?:\cisco_1000v/Nexus1000v-vsum.1.1\Nexus1000v-vsum.1.	
Help	<back next=""></back>	Cancel

1

- 4. Click Next, then click Next again.
- 5. Review the license agreement. Click Next.
- 6. Click Next on the Name and Location screen.
- 7. Select VersaStack_Management as the Host Cluster and click Next.
- 8. Select VM-Host-Infra-1 as the Datastore and click Next.
- 9. Choose a disk format and Click Next.
- 10. For Network Mapping make sure you have Management Mapped to IB-Mgmt and click Next.

Deploy O¥F Template			_
etwork Mapping	dealers discussion and		
What networks should the	deployed template use?		
Source			
OVF Template Details	Map the networks used in this OVF	template to networks in your inventory	
Ind User License Agreement			
Name and Location	Source Networks	Destination Networks	
lost / Cluster	Management	IB-MGMT	
<u>Storage</u> Disk Format			
Network Mapping			
roperties			
Ready to Complete			
	1		
	Description:		
	provides connectivity (http(s)/ssh	y/scp) to the Cisco Virtual Switch Update Manager.	
	,		
Help		< Back Next >	Cance
		COOK NOXC >	Conte

11. On the properties Screen input <<var_vsm_updatemgr_mgmt_ip>> <<var_vsm_mgmt_mask>> <<var_vsm_mgmt_gateway>> <<var_nameserver_ip>>. Enter the vCenter IP and login information. For domain accounts, use the Admistrator@Vshpere.local login format and do not use domainname\user account format. Accept default ports, and click Next.

I

Deploy OVF Template		_ 🗆 🗙
Properties Customize the software so	lution for this deployment.	
Source OVF Template Details End User License Agreement Name and Location Host / Cluster Storage Disk Format Network Mapping Properties Ready to Complete	Dres Server 2 Secondary DNS Server IP (e.g. 10.10.10.10). Optional.	
Help	< Back Next >	Cancel

1

12. Review the summary screen, click Power on after deployment and click Finish.

Source OVF Template Details	When you click Finish, the dep	loyment task will be started.
End User License Agreement	Deployment settings:	
Name and Location	OVF file:	Z:\cisco_1000v\Nexus1000v-vsum.1.1\new\Nexus1000v
Host / Cluster	Download size:	3.0 GB
Storage Disk Format	Size on disk:	80.0 GB
Network Mapping	Name:	Virtual Switch Update Manager
Properties	Folder:	VersaStack_DC_1
Ready to Complete	Host/Cluster:	VersaStack_Management
	Datastore:	VM-Host-Infra-1
	Disk provisioning:	Thick Provision Lazy Zeroed
	Network Mapping:	"Management" to "IB-MGMT"
	IP Allocation:	Fixed, IPv4
	Property:	IpV4Address = 10.29.151.30
	Property:	IpV4Netmask = 255.255.255.0
	Property:	IpV4Gateway = 10.29.151.1
	Property:	DnsServer1 = 10.29.130.112
	Property:	DnsServer2 =
	Property:	VcenterIPV4Address = 10.29.151.102
	Property:	VcenterUsername = administrator@vsphere.local
	Property:	VcenterHttpPort = 80
	Property:	VcenterHttpsPort = 443
	1	

13. After the VM boots in a few minute the Plugin is registered. Validate the plugin in the vSphere client by clicking Plug-ins, then Manage plug-ins in the top menu bar and look under Available Plug-ins.

	Avai	able Plug-ins				monitoring)
l		Cisco Nexus 1000V Ma	Cisco Syste	1.1	No clent side	Cisco Nexus 1000V Management System
l						
l						
	-	Help				

Γ

Install the VSM Through the Cisco Virtual Switch update Manager



On the machine where you will run the browser for the VMware vSphere Web Client, you should have installed Adobe Flash as well the Client Integration plugin for the web client. The plug-in can be downloaded from the lower left corner of the web client login page.

1

- 1. Launch the vSphere Web client interface https://<<Vshpere_host_ip>>:9443/vsphere-client and login.
- 2. Select the home tab and click Cisco Virtual Switch Update Manager.

📢 History 💽 🗧	. ₹	🚮 Home					
👔 Home		Getting Started	Home				🝷 🗊 Recent Task
 Ø vCenter ₩ Rules and Profiles ₩ Center On bookerster 	>		a	(C)		-	All Running
VCenter Orchestrator Administration	>	vCenter	Hosts and Clusters	VMs and Templates	Storage		
😨 Tasks 🔁 Log Browser 🙀 Events		Q	\$]	0	adjuster Crist D		
Tags Q New Search	>	Networking	vCloud Hybrid Service Installer	vCenter Orchestrator	Cisco Virtual Switch Update Manager	Cisco Virtual Switch	Update Manager
Raved Searches	>	Monitoring					🔹 📝 Work in Prog
		送 Task Console	Event Console	Host Profiles	VM Storage Policies		
			to Vieterations				Alarms All (1) New (1 All (2) Newsa-wcenter.pp

3. Click the Nexus 1000V button then click install.

A History) I	Cisco Virtual Switch Update Manager	
 Home ✓ Center Rules and Profiles ✓ vCenter Orchestrator 	>	Getting Started This is your portal to Install, Add Hosts, Monitor and Upgrade the Cisco Nexus 1000V. The Cisco VSUM also allows you to	About 1) Choose an available Datacente
Administration Tasks Log Browser	>	Add and Upgrade Hosts on the Cisco Application Virtual Switch. Basic Tasks	name VersaStack_DC_1
Events Tags New Search Saved Searches	>	AVS Nexus1000V Install Configure Dashboard Information	
		Help Install a new Cisco Nexus 1000V switch. Choose an available datacenter to install a new Switch.	•

- 4. Click the VersaStack datacenter in the right screen.
- 5. Keep the default for deploy new VSM and High Availability Pair. Select IB-Mgmt for the control and Management VLAN.

etting Started Summary Monitor Ma	nage Related Objects			
larm Definitions Tags Permissions N	letwork Protocol Profiles	Scheduled Tasks	Cisco Nexus 1000V Installer	
📀 Nexus1000v Switch Deployi	ment Process		0	8
● I want to deploy new control plane (VSM) □ I already have a control plane (VSM) de	Sec. 1997			
Nexus1000V Switch Deploy	ment Type		Q	*
Nexus1000V Switch Deploy Nexus1000V Switch Deployment Type		•	0	(i)
	 Stand alone 	•	Ø	()
Nexus1000V Switch Deployment Type	 Stand alone High Availability Pair 			(()

6. For the Host Selection, click the suggest button and choose the Datastores.

Γ

Host Selection	on								0 ≶
			Sug	gest	Pick a Host				
	н	lost 1				Host 2			
IP Addre	ess [1	10.29.151.51		•	IP Address	10.29.151.52		•	
Datasto	re [VM-Host-Infra-1	•	٠	Datastore	VM-Host-Infra-1	•	•	
Resourc	e Pool		-		Resource Pool)	
Folder n	ame	1	-		Folder name	1			

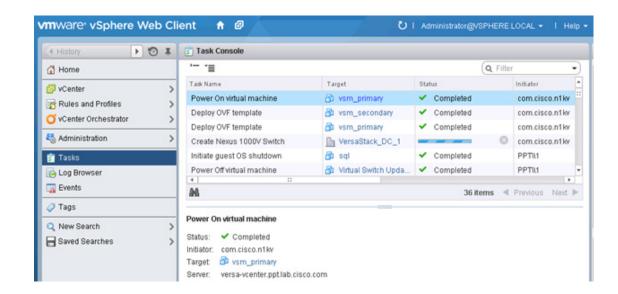
1

7. Enter a domain ID for the switch configuration section.

Switch Co	nfiguration	0 🙈
Domain ID:	21 *	
Deployment Ty	pe: 💿 Management IP Address	
	Control IP Address	

8. Enter the following information for the VSM configuration <<var_vsm_hostname>> <<var_vsm_mgmt_ip>>, <<var_vsm_mgmt_mask>> <<var_vsm_mgmt_gateway>> <<var_password>>, then click Finish. You can launch a second VSphere Client to monitor the progress. Click Tasks in the left pane. It will take a few minutes to complete.

rintaal oupers	visor Module (VS	SM) configuration	0 🗟
Switch Name	vsm	•	
P Address	10.29.131.40	•	
Subnet Mask	255.255.255.0	*	
Gateway Address	10.29.131.1	•	
Default Port Profile	s:		
Username	admin		
Username Password	admin	•	



Perform Base Configuration of the Primary VSM

To perform the base configuration of the primary VSM, complete the following steps:

- 1. Use an SSH client, log in to the primary Cisco Nexus 1000V VSM as admin.
- 2. Run the following configuration commands.

```
config t
ntp server <<var_global_ntp_server_ip>> use-vrf management
vlan <<var ib-mgmt vlan id>>
name IB-MGMT-VLAN
vlan <<var nfs vlan id>>
name NFS-VLAN
vlan <<var_vmotion_vlan_id>>
name vMotion-VLAN
vlan <<var vm-traffic vlan id>>
name VM-Traffic-VLAN
vlan <<var native vlan id>>
name Native-VLAN
exit
port-profile type ethernet system-uplink
vmware port-group
switchport mode trunk
switchport trunk native vlan <<var native vlan id>>
switchport trunk allowed vlan <<var ib-mgmt vlan id>>, <<var nfs vlan id>>,
<<var vmotion vlan id>>, <<var vm-traffic vlan id>>
channel-group auto mode on mac-pinning
no shutdown
system vlan <<var ib-mgmt vlan id>>, <<var nfs vlan id>>,
<<var vmotion vlan id>>, <<var vm-traffic vlan id>>
system mtu 9000
state enabled
exit
```

```
port-profile type vethernet IB-MGMT-VLAN
vmware port-group
switchport mode access
switchport access vlan <<var_ib-mgmt_vlan_id>>
no shutdown
system vlan <<var_ib-mgmt_vlan_id>>
state enabled
exit
port-profile type vethernet NFS-VLAN
vmware port-group
switchport mode access
switchport access vlan <<var_nfs_vlan_id>>
no shutdown
system vlan <<var_nfs_vlan_id>>
state enabled
exit
port-profile type vethernet vMotion-VLAN
vmware port-group
switchport mode access
switchport access vlan <<var_vmotion_vlan_id>>
no shutdown
system vlan <<var_vmotion_vlan_id>>
state enabled
exit
port-profile type vethernet VM-Traffic-VLAN
vmware port-group
switchport mode access
switchport access vlan <<var_vm-traffic_vlan_id>>
no shutdown
system vlan <<var_vm-traffic_vlan_id>>
state enabled
exit
port-profile type vethernet n1kv-L3
capability 13control
vmware port-group
switchport mode access
switchport access vlan <<var ib-mgmt vlan id>>
no shutdown
system vlan <<var_ib-mgmt_vlan_id>>
state enabled
exit
copy run start
```

I

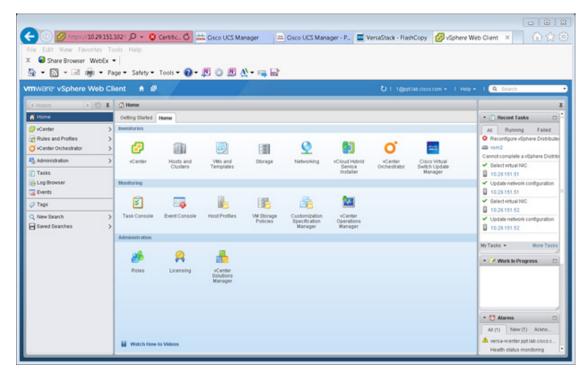
Migrate Networking Components for ESXi Hosts to Cisco Nexus 1000V

vSphere Client Connect to vCenter

I

To migrate the networking components for the ESXi hosts to the Cisco Nexus 1000V, complete the following steps:

1. In the vSphere web client, click the Home tab and click the Cisco Virtual Switch Update Manager.



2. Click the Nexus 1000v and click Configure.

Home Home Ketter Kette	Cisco Virtual Switch Update Manager			
vCenter >				
	Getting Started This is your portal to Install, Add Hosts, Monitor and Upgrade	Choose a task to begin	About	Pecent Tasks At Running Failed Reconfigure vSphere Distribut
VCenter Orchestrator >	the Cisco Nexus 1000V. The Cisco VSUM also allows you to Add and Upgrade Hosts on the Cisco Application Virtual Switch.			Cannot complete a vSphere Dist
Tasks Log Browser Events	Besic Tasks AVS Nexus1000V			Update network configuration
Tags New Search	Configure			Select virtual NBC 10.29.151.52 Update network configuration
Saved Searches >	Dashboard Information			0 10.29.151.52
				My Tasks • More Tas
	Rep			• • Alarms

1

3. Click Datacenter, then click Distributed Virtual Switch and select manage.

VCenter Orchestrator > The Cisco Nexus			Pecent Tasks All Running Failed
vCenter v	to Install, Add Hosts, Monitor and Upgrade	The Street of Street St	
Add and Upgrade		 Choose an available Datacenter 	Reconfigure vSphere Distribut
Marca and Anna and An	Hosts on the Cisco Application Vitual	name VerseStack_DO_1	Cannot complete a vSphere Distri Select virtual NIC
Tasks Basic Tasks Log Browser Events AVS Nexons	0007	-	Update network configuration 50.29.151.51
7 Tags 🔯 Install			Select virtual NIC 10.29.151.52
Saved Searches > 💻 Dashboard	Configure Configure DushDeard DushDeard DushDeard		Update network configuration
Information		2) Choose an associated Distributed Virtual Switch	My Tasks + More Task
		name wsm2	• 📝 Work In Progress
Heb			
	ed whus switch to monitor, nigrate or upgrade the Switch, a datacenter, and then choose an associated switch.		• 🖸 Alarms

4. Click the Add Host tab then select the plus sign next to Versastack_Management, then click the top check box to both Hosts.

re [,] vSphere Web Client	10			0.1	@setlabicisco.com + 1 Help +	I Q Search
10 I	2 Actions +				<i>H</i> *	
N2 Oetting	Started Summary Monitor Manage	Related Objects				Tecent Tasks
	gs Alam Defnitions Tags Permission	ns Network Protoco	Profiles Ports Cisco Nexus 1	0007		All Running Failed Reconfigure vSphere District
Distributed Port Groups Cve	niew Add Host Upgrade Install Lic	ense Make Manag	ped .			 ven2
Iplink Port Groups	Host Selection				0 🕅	Cannot complete a vSphere Dis
line in the second s					U A	Select virtual NIC
	FersaStack_Management					 Update network configuration
3	Host 10.29.151.52	Supported	UnSupported	UnReachable	Already In DVS	0 10.29.151.51
3	10.29.151.51	ő				Select virtual NIC 0 10.29.151.52
		0.000				 ✓ Update network configurate
0.5	itandalone Hosts					10.29.151.52
Choos	se hosts to migrade					
Load	Balance Algorithm For the "Route Based II global loading balancin	P Hash" load balanci ng algorithm will be c	ing algorithm in the vGw8ch, the onfigured as "source-dest-ip-vlan	e		My Tasks • More Ta
Sug	pest					* 📝 Work in Progress
						- C Alarms

5. Click Suggest.

Γ

Edit View Favorites T			Cisco UCS Manager	- Caco oca nanage	Tersesation	c - FlashCopy 🕜 vSphere W	Web Client × 🕜 ☆
Share Browser WebEx							
		ety - Tools -	0 - 🗷 O 🗷 🖄 - 🛶				
			• • • • • • • •				
Ware [,] vSphere Web C	lient f	0			01	1@pptlab.cisco.com + 1 Help	I Q. Search
Home > 🔿 🕱	⊡ vim2	Actions *					
vim2	Outling St	tarted Summary	Monitor Manage Related Object	N			• T Recent Tasks
Hosts	Courses	Later But Bar	Trace Browledge 100 and Brow				Al Running Failed
Virtual Machines	54mings	Aram Definitions	Tags Permissions Network Proto	corpronies Ports Cisco Neiu	5 1000V		O Reconfigure vSphere Distribu
Distributed Port Groups Distributed Port Groups Distributed Port Groups	Ovenie	rw Add Host U	ograde Install License Make Man	aged			a vsm2
	C Ho	st Selection				0 🕅	Cannot complete a vSphere Distr Select virtual NIC
						• • •	0 10.29.151.51
		saStack_Managem					✓ Update network configuration
	2	Host 10.29.151.53	Supported	UnSupported	UnReachable	Already in DVS	0 10.29.151.51
	8	10.29.151.51	ő	2			Select virtual NIC
	-						Update network configuration
	0.94	ndalone Hosts					10.29.151.52
	A COLORED	hosts to migrate					
	Load Bai	lance Algorithm For	the "Route Based IP Hash" load balar bal loading balancing algorithm will be	noing algorithm in the vOwtich, the	100 m		MyTasks • More Tas
	Suppe						* 📝 Work in Progress 🔅
	O Po	ort Profile Edito	r			08	
	In Use	Valid Editable	Profile Name				
	516	true false	IB-MOMT-VLAN	C) Uplink			
	tue	true faise	n1keL3	Trunk			- 🖸 Alarms
	500	true false	NES-VLAN	C L3 capable			All (1) New (1) Acknowl
	faise	true faise	system-uplink	O ISCSI MUS		1.0	1.4410

6. Select the Physical NIC Migration, and select the Unused Nic vmnic1 for migration. Select system uplink in the middle pane.

	ー age ー Safety ー Tools ー 🔞 ー 🍂 🐇	. # M D			
ware: vSphere Web Cl		2 22 <u>2</u> - 46 88	U I igsplabeises	om = Help =	I Q. Search
Home 🕨 🔊 🕱	ca vsm2 Actions +			W.*.	
Viun2 Alests	Oetting Started Summary Monitor Man	age Related Objects			* 👔 Recent Tasks
Vitual Machines	Overview Add Host Upgrade Instal	ILicense Make Managed			Reconfigure vSphere Distrib vsm2 Cannot complete a vSphere Dist
	O Physical NIC Migration			08	 Select virtual NIC 10.29.151.51
	Physical NCs # 10.29 151.52	Profile	Dourie Profile		Update network configuratio 10.29.151.51
	vmnic0	ntix-eth-5	vSwitch0		✓ Select virtual NIC
	Vermiet	system-uplink			0 10.29.151.52
	* 10.29.151.51				 Update network configuratio 10.29.151.52
	vmnic0	n1ke-eth-5	v9wtcn0	181	U 10.29.151.52
	🖬 verse 1	system-uplink	•		My Tasks + More Ta
					* 📝 Work In Progress
		Select All			
	Select one or more PNICs to move.				

1

7. For the VM Kernel NIC Setup, deselect vmk3, which is the temporary management kernel we created for this migration.

Share Browser WebEx							
• 🔊 • 🖃 👼 • Pi Ware: vSphere Web Cl	age • Safety • Tools • 🕢 • 🎘 lient n 🥔	0 10 12 • 🖘 1	d'	U I 1@eptiab.cisco.com + I Help +	I Q. Search		
Home > 🖸 I	a vin2 Actions -				1		
vim2	Oetting Started Summary Monitor	aname Related Objects			Recent Tasks		
Hosts					Al Running Failed		
Vidual Machines	Settings Alarm Definitions Tags Perm	issions Network Protocol	Profiles Ports Claco Nexus 1000V		Reconfigure vSphere Distribut		
Lostributed Port Groups	Oveniew Add Host Upgrade Inst	all License Make Manapi	a l		a vsm2		
Uplink Port Groups	VM Kernel NIC Setup	1		A O R ·	Cannot complete a vSphere Dist		
					Select virtual NIC		
	Veikemet NiCs	L3 Capable	Potla	Source Profile	0.29.151.51		
	Ø vmk0		n1k+L3	v0w8ch0 *	 Update network configuration 10.29.151.51 		
	Ø vmk1		NFS-VLAN vMoton-VLAN	v0wtch0 v0wtch0	Select virtual NIC		
	Ø vmk2	_	ID-MONT-VLAN	vgwech0	10.29.151.52		
	vmk3	-	IB-MORT-ADAM	Nowochu	✓ Update network configuration		
	R vmk0		nfiel3	vSwitch0	0 10.29.151.52		
	R vmkt		NES-VLAN	vSwitch0			
	R vmk2		Wollon-VLAN	vSw8ch0	MyTasks - More Task		
	U vmk0		IB-MONT-VLAN	v9wtch0	* 💉 Work in Progress 🔅		
	Choose one or more white? I to move #1						
		Choose one or more wildHCs to move. * Denotes a new Kernel NIC to be added.					
	VM Migration			۵ 😣 🛦			
	Virtual Machine NICs		Profile	Source Profile	• 🔁 Alarms		
	■10.29.151.52						
	■ 10.29.151.51				All (1) New (1) Acknowl		
					versa-vcenter.ppt.lab.cisco.c.		

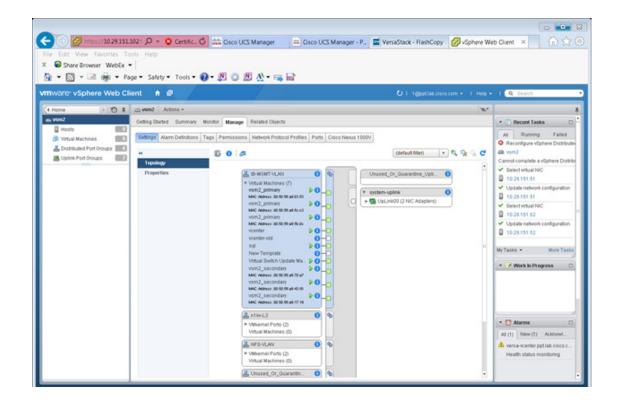
8. For VM migration click the button next to the virtual machine to expand the target profile and chose the correct profile which should be IB-MGMT-VLAN. Repeat this for each Virtual Machine.

Edit View Favorites T Share Browser WebEx								
	age = Safety = Tools = 🔞 = 👧 🌾							
		2 201 <u>22</u> - 1 46 18	•					
/are [,] vSphere Web C	lient 🕈 🖉			U 1 (geptiab.cis	co.com = 1 Help •	 I Q Search 		
ome 🕨 🕤 🕱	ca vsm2 Actions +				·			
um2	Getting Started Summary Monitor Man	age Related Objects				T Recent Tasks		
Hosts						Al Running Falled		
Vitual Machines		Settings Alarm Definitions Tags Permissions Network Protocol Profiles Ports Cisco Nesus 1000V						
Distributed Port Groups	Overnew Add Host Upgrade Install	Reconfigure vSphere Distribut wsm2						
Uplink Port Oroups	10 29 151 51	-			12	Cannot complete a vSphere Di		
	🖉 vmk0		n1ke-L3	v@wttch0		Select virtual NIC		
	🗹 vrskt		NFS-VLAN	v9w8ch0		Update network configuration		
	✓ vmk2		vMotion-VLAN	v9w8ch0		0 10.29.151.51		
	🗌 vmk3		IB-MOMT-VLAN	v9w8ch0	-	✓ Select virtual NIC		
		0 10.29.151.52						
	Choose one or more wrikNICs to move. * Der	 Update network configuration 						
	🔊 VM Migration					0.29.151.52		
	O VM Migration				▲ ♥ ⊗	MyTasks - More To		
	Vidual Mashine NICe		Polis	Source Profile		my rapids * more ra		
	¥ 10.29.151.52				-	* 📝 Work in Progress		
	▼ vsm2_secondary							
	Metwork adapter 1	IB-MOMT-VLAN		vSwitch0				
	Network adapter 2	IB-MOMT-VLAN		vSwitch0				
	Vetwork adapter 3	IB-MOMT-VLAN		VBwitch0				
	* Millio 29.151.51					* 🔁 Alarms		
	 Network adapter 1 	ID-MONT-VLAN		volvesho	_			
	Virtual Switch Update Manager	ID BORN HOW				All (1) New (1) Acknowl.		
	- The second second					versa-vcenter ppt lab cisco. Health status monitoring		
			Select None			Prevaien stadus monitoring		

9. Click Finish.

ſ

10. When the migration completes, click Settings then click Topology and expand the virtual machines to view the network connections.



Remove the Networking Standard Switch Components for ESXi Hosts

In this section, the unused standard switch components will be removed and the second VIC will be assigned.

1

ESXi Host VM-Host-Infra-01

Note

Repeat the steps in this section for all the ESXi Hosts.

- 1. From each vSphere Client, select the host in the inventory.
- 2. Click the Configuration tab.
- 3. Click Networking.
- 4. Select the VSphere Standard switch, then click Properties.

A					
versa-vcenter.ppt1ab.cisco.com - vSp					
File Edit View Inventory Administr					
🖬 🖬 🛕 Home 🕻 🚮 Invento	ry 🕨 🗊 Hosts and Ousters			Search Inventory	Q
et et 182					
B 🖉 versa-voenter.ppt.lab.cisco.com					
B WesaStack_DC_1 II gb VesaStack_Management	Getting Started Summary Viti	.0, 1746018 Evaluation (58 days remaining ual Machines Performance Configuration T		Maps Storage Vews Hardware Stat	
10.29.151.51	Hardware	Verw: VSphere Standard Switch VSphere D	stributed Switch		*
New Tempkate	Processors	Networking		Refeat Add Netw	orking Properties
sol sol	Memory				12
vcenter-cid	Storage	Standard Switch: vSwitch0	Remove Properties		âl
Wrtual Switch Update Mark vsm2_primary		Virtual Machine Port Group	Physical Adapters		
vsm2_secondary	Storage Adapters Network Adapters	VMkemel-vMotion 2+	Vinneo 20000 Par C		
	Advanced Settings	Virtual Machine Port Group			
	Power Management	VMkernelNPS			
		VLAN ID: 3172			
	Software	Virtual Machine Port Group VMkernel-MGMT 9			
	Licensed Features	VLANID: 3175			
	Time Configuration	-Virtual Machine Port Group			
	DNS and Routing	🕫 VM-Traffic 🔍 🔍 +			
	Authentication Services Power Management	MLAN ID: 3174			
	Vitual Machine Startup/Shutd	VMiemel Port VMiemel-MGMT-2			
	Virtual Machine Swapfle Locati	vmk3 : 10.29.151.151 VLANID: 3175			
	Security Profile	Virtual Machine Port Group			
	Host Cache Configuration	D IB-MGMT 2-			
	System Resource Allocation	8 2 virtual machine(s) VLAN ID: 3175 voenter			
e	Ament MA Cattorne	vouea at			
Recent Tasks				Name, Target or Status contains: •	Clear
Name Targ	et Status		Details	- Initiated by Re	
	10.29.151.51 Ø Com	pieted			V2015 4:35:49PM
	10.29.151.51 © Com				/2015-4:35:51PM

- 5. Click the temporary network VMkernel-MGMT-2 created for the migration and click Remove.
- 6. Click Yes, then clickYes again.

Ports Network Adapters	Summary	Port Properties	
Switch VMkernel-VMotion VMkernel-VMotion VMkernel-MFS VMkernel-MSMT VMkernel-MSMT-2 VMkernel-MSMT-2 B-MSMT	120 Ports Virtual Mach Virtual Mach Virtual Mach Virtual Mach Virtual Mach	Network Label: VMkernel-MGMT-2 VLN ID: 3175 VMotion: Disabled Fault Tolerance Disabled Logging: Disabled ISCSI Port Binding: Disabled NAC Settings Mic Settings MAC Address: 00:50:56:56:76:b5 MTU: 1500	
		IP Settings IP Address: 10.29.151.151 Subnet Mask: 255.255.255.0 View Routing Table	1
		Effective Polcies Security Promiscuous Mode: Reject MAC Address Changes: Accept Forged Transmits: Accept Traffic Shaping	
		Average Bandwidth: Peak Bandwidth: Burst Size: Faikover and Load	
Add	Edit Remove	Balancing Load Education: Dest ID	-

7. Click Close.

Γ

- 8. Validate you still are focused on the VSphere standard switch and click Remove to remove this switch.
- 9. Click Yes to the warning popup.

Versa-vcenter.ppt.lab.cisco.com	- Sohara Giant				• 8
File Edit View Inventory Adm					C 63
🖬 🖬 💁 Home 🕨 🛃 Im	ventory > (5) Hosts and C			search Inventory	٩
6 er 36 versa-venter ppLab.csco.com 8 juversatsak, DC, 1 10.29,151.52 10.29,351.52 0 New Template 9 software	1029(13)132 4500	are ESS, 55.0, 1746018 Evaluation (SB days re- annum) antual Nature: Antonnacio Configura View: VSphere Standard Switch VSp Networking	on Tasks & Events Alarms Per	mussoni, Mapil (Storage View), Hardware Statue Refeath Add Networking Prog	per 201
di vomte-old di Vitual Switch Update di vom 2_primary di vom 2_precondary	Man Storage Networking Storage Adapter Network Adapter Advanced Settin Power Managem	s C Wikemel-Woton 2 + +	Remove Properbes scal Adapters wmnco 20000 Pull		
	Boftware Licensed Feature Time Configure Authentication S Power Managem Withui Machine S Security Profile Host Cache Con	on VILAN ID: 3175 VILAN ID: 3175 VILAN ID: 3174 VILAN ID: 3174 MILAN ID: 3174 MILAN ID: 3174 MILAN ID: 3175 VILAN ID: 3175			
	System Resource				
•	+ (<		12		
Recent Tasks	200300			Name. Terget or Status contains: •	Clear
Remove virtual NC Remove port group Lipdate network configuration Remove virtual switch	Target 10.29.151.51 10.29.151.51 10.29.151.51 10.29.151.51 10.29.151.51 10.29.151.51	Status Completed Completed Completed Completed Completed	Details	 Initiated by Requested Start T PPTN1 19/20154-88-00 PPTN1 19/20154-88-00 PPTN1 19/20154-81-00 PPTN1 19/20154-51-00 PPTN1 19/20154-51-00 	5PM 6PM 4PM 4PM
Update network configuration Remove virtual NIC	10.29.15151	Completed Completed		PPT\1 1/9/2015.4:52:25 PPT\1 1/9/2015.4:55:16	

 After vSwitch0 has disappeared from the screen, click vSphere Distributed Switch at the top next to View.

1

- 11. Click Manage Physical Adapters.
- 12. Scroll down to the system-uplink box and click Add NIC.
- 13. Choose vmnic0 and click OK, then click OK again.

Manage Physical Adapters		23
Image Projects Image	 Physical Adapter Details General Vendor/Model: Location: Driver: Status Link Status: Configured Speed, Duplex: Actual Speed, Duplex: Actual Speed, Duplex: Observed IP Networks: DirectPath I/O: ISCSI Port Binding: Cisco Discovery Protocol Device ID: Port ID: 	
Help	O	Cancel

- 14. Validate there are no warnings for the ESX nodes. From each vSphere Client, select the Hosts and Clusters in the inventory section, click the Summary tab.
- 15. If there are warnings, right-click each node and click Reconfigure for vSphere HA.

File Edit View Inve	ntor	y Administration Plug-ins	Help		
🖸 🔯 🙆 Hom	ie I	🕽 Inventory 🕨 🗊 Hosts a	and Clusters		
ප් සේ සි					
versavcenter.ppt.l Eleventer.ppt.l Eleventer.ppt.l	_1 Mani 1.51	agement Getting	Started Sun		0, 1746018 E Jal Machines Pe
10.29.15 Sol Venter	6	New Virtual Machine New Resource Pool New vApp	Ctrl+N Ctrl+O Ctrl+A		 Distributed vsm
🍅 vsm_prin 👼 vsm_sec	vsm_sec	Disconnect Enter Maintenance Mode			92 II € VI
		Rescan for Datastores Add Permission Alarm	Ctrl+P	-	Srin ∎vr Vi
		Host Profile	•	·	S⊉ n
	10 10 10	Shut Down Enter Standby Mode Reboot Power On		bes Lip/Shutd vfile Locab	
Recent Tasks		Report Summary Report Performance			
Name Reconfigure vSphere		Open in New Window C Remove	tri+Alt+N	Status Com	nlatad
 Neconigure vapriere 		Reconfigure for vSphere HA	ł		precedu

Remove the Redundancy for the NIC in Cisco UCS Manager

While creating the ESXi vNIC template settings, the default was to enable hardware failover on the vNIC. When you have deployed the N1kV, that setting is no longer required and should be disabled.

- 1. Launch UCS Manager and click the Lan tab.
- 2. Click Policies, root, vNic templates.
- 3. Click vNic_Template_A, and on the General Tab uncheck enable failover.
- 4. Click Save Changes, then Yes, then ok.
- 5. Repeat action for vNic_Template_B.



ſ

Reboot the ESXi hosts to implement the change.

It Summary	s 😥 🚯 📥 Pending Activities 🔯 Exit
a a a a a a a a a a a a a a a a a a a	
U 2 1 3	🕅 vháC Templates + 📷 vháC Template vháC_Template_A 👘 vháC Template vháC_Template_
ipment Servers LAN SAN VM Admin General VLANs Faults Ev	ents
Filter: All	Properties
Modify VLANs	Name: vMIC_Template_A
LAN II Delete	Description:
CLAN Cloud Show Policy Usage	Owner: Local
Fabric B	Fabric ID: Fabric A Fabric B Fabric B Fable Failover
QoS System Class	Target
-== LAN Pin Groups 	√ Adapter
VLAN Groups	T VM
THE VLANS	
Appliances	
Internal LAN Enternal Fabric A	Template Type: Initial Template Updating Template
🕀 – 🖪 Internal Fabric B	MTU: 9000
Threshold Policies	
S Policies Appliances	Policies
B O LAN Chud	MAC Pool: MAC_Pool_A(30/ *
⊖ A root	QoS Policy: <not set=""></not>
- Default vNIC Behavior - Dynamic vNIC Connection Policies	Network Control Policy: Enable_CDP
The second secon	Pin Group: <not set=""></not>
1 ILAOP Policies	Stats Threshold Policy: default
- S LAN Connectivity Policies	Connection Policies
S Link Protocol Policy Multicast Policies	
Solution Policies	Dynamic vN8C UsN8C VMQ
- S QoS Policies	Dynamic vNIC Connection Policy: <not set=""></not>
Si Threshold Policies Si VMO Connection Policies	
- III usNIC Connection Policies	
C Templates	
MIC Template MIC_Template_A MIC Template MIC_Template_B	

For more information about the 1000v switch, including how to update the software after installation, please visit the web site:

http://www.cisco.com/c/en/us/products/switches/nexus-1000v-switch-vmware-vsphere/index.html

Backup Management and other Software

IBM Solutions

IBM is well known for management software. Added value to this solution can be obtained by installing IBM's Storage Management Console for VMware vCenter. Please visit the IBM website to obtain the latest version at http://www.ibm.com/us/en/.

For details about IBM backup and disaster recovery solutions, please refer to: http://www-03.ibm.com/systems/storage/solutions/backup-and-disaster-recovery/

Bill of Materials

Γ

Part Number	Product Description	Quantity Required
IBM Storwize V7000 C	Components	
2076-524	IBM Storwize V7000 SFF Control	1
5305	5m Fiber Cable (LC)	8
9730	Power Cord - PDU connection	1
AG00	Shipping and Handling NC	1
AHB1	8Gb FC Adapter Pair	1
AHC1	Compression Accelerator	1
AHCB	Cache Upgrade	1
AHH1	200GB 2.5 Inch Flash Drive	3
AHF1	600GB 10K 2.5 Inch HDD	21
5639-CB7	IBM Storwize Family Software V7000 Controller V7.3	1
UBJSC1	Base Software Controller Per Storage Device with 1 Year SW Maint	1
UBJWC1	Full Feature Controller Per Storage Device with 1 Year SW Maint	1
2076-24F	IBM Storwize V7000 SFF Expansion	1
9730	Power Cord - PDU connection	1
ACUA	0.6m 12Gb SAS Cable(mSAS HD)	2
AGBK	Shipping and Handling 24F	1
AHF1	600GB 10K 2.5 Inch HDD	24
5639-XB7	IBM Storwize Family Software V7000 Expansion	1
UBPNC1	Base Software Expansion Per Storage Device with 1 Year SW Maint	1
UBPTC1	Full Feature Expansion Per Storage Device with 1 Year SW Maint	1
Optional IBM Storwize	e V7000 File Module Components	
2073-720	IBM Storwize V7000 Unified	2
1176	Unified shipment of 2073 and 2076	2
5305	5 m Fiber Optic Cable LC-LC	4
5709	Ethernet Cable - 9ft-Green-CAT 5E	2
9730	Power Cord - PDU connection	2
AGB7	Shipping and Handling 720	2
5639-VF1	IBM Storwize V7000 File Module Software V1.5	2
3450	ESD	2
5809	Storwize V7000 Unified Pubs	2
5819	Storwize V7000 Unified DVD	2
U9ZRC1	Per Storage Device w/1Yr SW Maint	2

Table 22Bill of Materials for IBM Storwize V7000

Part Number	Product Description	Quantity Required	
Cisco Nexus 9300 Switching Components			
N9K-C9372PX	Nexus 9300 with 48p 10G SFP+ and 6p 40G QSFP+	2	
N3K-C3064-ACC-KIT	Nexus 9300 Accessory Kit	2	
NXA-FAN-30CFM-F	Nexus 2K/3K/9K Single Fan, port side exhaust airflow	8	
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	4	
N9K-PAC-650W-B	Nexus 9300 650W AC PS, Port-side Exhaust	4	
N9KDK9-612I3.1	Nexus 9500 or 9300 Base NX-OS Software Rel 6.1(2)I3(1)	2	

1

Table 23 Bill of Materials for Nexus 9300 Series S	Switch
--	--------

Table 24Bill of Materials Cisco MDS

Part Number	Product Description	Quantity Required
Cisco MDS FC Switch		
DS-C9148S-12PK9	MDS 9148S 16G FC switch, w/ 12 active ports	2
DS-9148S-KIT-CSCO	MDS 9148S Accessory Kit for Cisco	2
M91S5K9-6.2.9	MDS 9100 Supervisor/Fabric-5, NX-OS Software Release 6.2.9	2
DS-SFP-FC8G-SW	8 Gbps Fibre Channel SW SFP+, LC	24
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	4

Table 25Bill of Materials for Cisco UCS Blade Servers and Chassis

Part Number	Product Description	Quantity Required
Cisco UCS Unified Computing System		
UCSB-5108-AC2	UCS 5108 Blade Server AC2 Chassis, 0 PSU/8 fans/0 FEX	1
UCS-IOM-2208XP	UCS 2208XP I/O Module (8 External, 32 Internal 10Gb Ports)	2
UCSB-5108-PKG-HW	UCS 5108 Packaging for chassis with half width blades.	1
N20-CBLKP	Power supply unit blanking panel for UCS 5108	1
N01-UAC1	Single phase AC power module for UCS 5108	1
N20-FAN5	Fan module for UCS 5108	8
N20-FW012	UCS Blade Server Chassis FW Package 2.2	1
N20-CBLKB1	Blade slot blanking panel for UCS 5108/single slot	4

N20-CAK	Accessory kit for UCS 5108 Blade Server Chassis	1
UCSB-B200-M4	UCS B200 M4 w/o CPU, mem, drive bays, HDD, mezz	4
UCS-CPU-E52650D	2.30 GHz E5-2650 v3/105W 10C/25MB Cache/DDR4 2133MHz	8
UCS-MR-1X162RU-A	16GB DDR4-2133-MHz RDIMM/PC4-17000/dual rank/x4/1.2v	32
UCSB-MLOM-PT-01	Cisco UCS Port Expander Card (mezz) for VIC	4
UCSB-MLOM-40G-01	Cisco UCS VIC 1240 modular LOM for blade servers	4
UCSB-HS-EP-M4-F	CPU Heat Sink for UCS B200 M4 Socket 1 (Front)	4
UCSB-HS-EP-M4-R	CPU Heat Sink for UCS B200 M4 Socket 2 (Rear)	4
UCSB-LSTOR-BK	FlexStorage blanking panels w/o controller, w/o drive bays	8
UCSB-PSU-2500ACDV	2500W Platinum AC Hot Plug Power Supply - DV	4
CAB-C19-CBN	Cabinet Jumper Power Cord, 0 VAC 16A, C20-C19 Connectors	4

Table 26Bill of Materials for Cisco Fabric Interconnect

I

Γ

Part Number	Product Description	Quantity Required
Cisco UCS UCS-FI-6248UP Fabric Interconnect		
UCS-FI-6248UP	UCS 6248UP 1RU Fabric Int/No PSU/32 UP/ 12p LIC	2
UCS-ACC-6248UP	UCS 6248UP Chassis Accessory Kit	2
UCS-PSU-6248UP-AC	UCS 6248UP Power Supply/100-240VAC	4
N10-MGT012	UCS Manager v2.2	2
UCS-BLKE-6200	UCS 6200 Series Expansion Module Blank	2
UCS-FAN-6248UP	UCS 6248UP Fan Module	4
UCS-FI-DL2	UCS 6248 Layer 2 Daughter Card	2
CAB-9K12A-NA	Power Cord, 1VAC 13A NEMA 5-15 Plug, North America	4

Table 27Bill of Materials for Cisco Rack FEX

Part Number Product Description		Quantity Required	
Cisco FEX			
N2K-C2232PF	Nexus 2232PP with 16 FET, choice of airflow/power	2	
NXA-AIRFLOW-SLV	Nexus Airflow Extension Sleeve	2	
N2K-F10G-F10G	N2K Uplink option FET-10G to FET-10G	2	
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	4	

FET-10G	10G Line Extender for FEX	32
N2232PP-FA-BUN	Standard airflow pack: N2K-C2232PP-10GE, 2AC PS, 1Fan	1

I

1

Table 28	Bill of Materials	for Cisco	Rack Servers
----------	-------------------	-----------	---------------------

Part Number	Product Description	Quantity Required	
Cisco UCS Rack Servers			
UCSC-C220-M4S	UCS C220 M4 SFF w/o CPU, mem, HD, PCIe, PSU, rail kit	2	
UCS-CPU-E52640D	2.60 GHz E5-2640 v3/90W 8C/20MB Cache/DDR4 1866MHz	4	
UCS-MR-1X162RU-A	16GB DDR4-2133-MHz RDIMM/PC4-17000/dual rank/x4/1.2v	16	
UCSC-PCIE-CSC-02	Cisco VIC 1225 Dual Port 10Gb SFP+ CNA	2	
UCSC-CMAF-M4	Reversible CMA for C220 M4 friction & ball bearing rail kits	2	
UCSC-RAILF-M4	Friction Rail Kit for C220 M4 rack servers	2	
UCS-SD-32G-S	32GB SD Card for UCS servers	4	
UCSC-PSU1-770W	770W AC Hot-Plug Power Supply for 1U C-Series Rack Server	4	
CAB-9K12A-NA	Power Cord, 125VAC 13A NEMA 5-15 Plug, North America	4	
N20-BBLKD	UCS 2.5 inch HDD blanking panel	16	
UCSC-HS-C220M4	Heat sink for UCS C220 M4 rack servers	4	
UCSC-MLOM-BLK	MLOM Blanking Panel	2	

Note This Bill of Materials is using the Cisco 1200 series VIC. At the time of this publication the Cisco 1300 VIC series are undergoing qualification testing by IBM. When validated, you can substitute the newer VIC. Please consult with the IBM and Cisco compatibility guides for the latest hardware supported.

Appendix

Build Windows Active Directory Server VM(s)

ESXi Host VM-Host-Infra-01

To build an Active Directory Server virtual machine (VM) for the VM-Host-Infra-01 ESXi host, complete the following steps:

- 1. Log in to the host by using the VMware vSphere Client.
- 2. In the vSphere Client, select the host in the inventory pane.
- 3. Right-click the host and select New Virtual Machine.
- 4. Select Custom and click Next.
- 5. Enter a name for the VM. Click Next.
- 6. Select infra_datastore_1. Click Next.
- 7. Select Virtual Machine Version: 10. Click Next.
- 8. Verify that the Windows option and the Microsoft Windows Server 2008 R2 (64-bit) version are selected. Click Next.
- 9. Select two virtual sockets and one core per virtual socket. Click Next.
- 10. Select 4GB of memory. Click Next.
- 11. Select one network interface card (NIC).
- 12. For NIC 1, select the IB-MGMT Network option and the VMXNET 3 adapter. Click Next.
- 13. Keep the LSI Logic SAS option for the SCSI controller selected. Click Next.
- 14. Keep the Create a New Virtual Disk option selected. Click Next.
- 15. Make the disk size at least 60GB. Click Next.
- 16. Click Next.
- 17. Select the checkbox for Edit the Virtual Machine Settings Before Completion. Click Continue.
- 18. Click the Options tab.
- 19. Select Boot Options.
- 20. Select the Force BIOS Setup checkbox.
- 21. Click Finish.
- 22. From the left pane, expand the host field by clicking the plus sign (+).
- 23. Right-click the newly created AD Server VM and click Open Console.
- 24. Click the third button (green right arrow) to power on the VM.
- **25.** Click the ninth button (CD with a wrench) to map the Windows Server 2008 R2 SP1 ISO, and then select Connect to ISO Image on Local Disk.
- 26. Navigate to the Windows Server 2008 R2 SP1 ISO, select it, and click Open.
- 27. Click in the BIOS Setup Utility window and use the right arrow key to navigate to the Boot menu. Use the down arrow key to select CD-ROM Drive. Press the plus (+) key twice to move CD-ROM Drive to the top of the list. Press F10 and Enter to save the selection and exit the BIOS Setup Utility.

- **28.** The Windows Installer boots. Select the appropriate language, time and currency format, and keyboard. Click Next.
- **29.** Click Install now.
- **30.** Make sure that the Windows Server 2008 R2 Standard (Full Installation) option is selected. Click Next.
- 31. Read and accept the license terms and click Next.
- **32.** Select Custom (Advanced). Make sure that Disk 0 Unallocated Space is selected. Click Next to allow the Windows installation to complete.
- **33.** After the Windows installation is complete and the VM has rebooted, click OK to set the Administrator password.
- **34.** Enter and confirm the Administrator password and click the blue arrow to log in. Click OK to confirm the password change.
- **35.** After logging in to the VM desktop, from the VM console window, select the VM menu. Under Guest, select Install/Upgrade VMware Tools. Click OK.
- **36.** If prompted to eject the Windows installation media before running the setup for the VMware tools, click OK, then click OK.
- **37.** In the dialog box, select Run setup64.exe.
- 38. In the VMware Tools installer window, click Next.
- **39.** Make sure that Typical is selected and click Next.
- 40. Click Install.
- 41. Click Finish.
- 42. Click Yes to restart the VM.
- **43.** After the reboot is complete, select the VM menu. Under Guest, select Send Ctrl+Alt+Del. Then enter the password to log in to the VM.
- 44. Set the time zone for the VM, IP address, gateway, and host name.



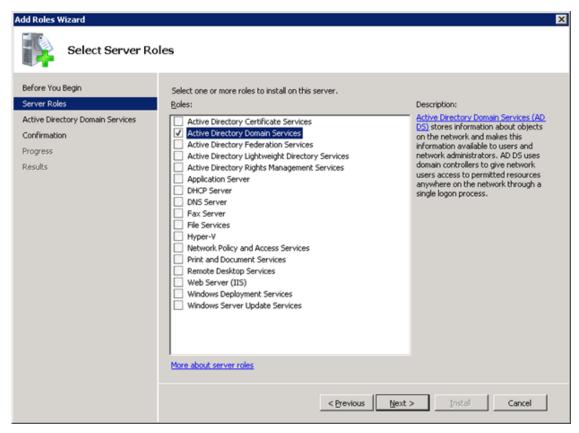
A reboot is required.

- 45. If necessary, activate Windows.
- **46.** Download and install all required Windows updates.



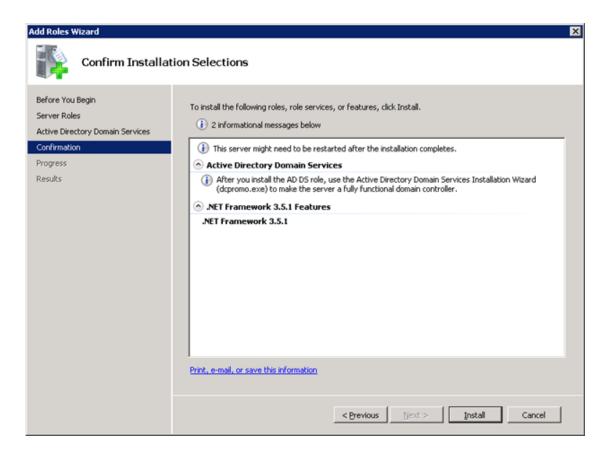
This process requires several reboots.

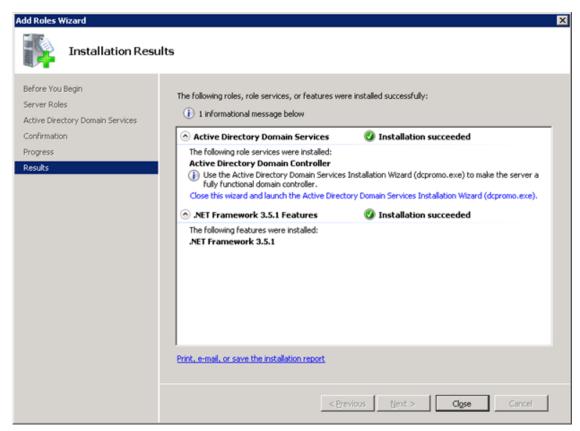
- 47. Open Server Manager.
- **48.** On the left, click Roles, the select Add Roles on the right.
- 49. Click Next.
- 50. In the list, select the checkbox next to Active Directory Domain Services.
- 51. In the popup, click Add Required Features to add .NET Framework 3.5.1.



- 52. Click Next.
- 53. Click Next.
- 54. Click Install.

ſ





- **55.** In the middle of the window, click Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe).
- 56. In the Active Directory Domain Services Installation Wizard, click Next.
- 57. Click Next.

I

58. Select "Create a new domain in a new forest" and click Next.

	ployment Configuration eate a domain controller for		or a new forest.	
C Existing	forest			
CA	ld a domain controller to an	existing domain		
	eate a new domain in an ex is server will become the fir		the new domain.	
Create	a new gomain in a new fore	at		
More abou	possible deployment confic	<u>urations</u>		
		< Back	Next >	Cancel

59. Type the FQDN of the Windows domain for this VersaStack and click Next.

the forest.	orest root domain. Its name is also the name of	-
Type the fully qualified domain name	e (FQDN) of the new forest root domain.	
EQDN of the forest root domain:		_
Example: corp.contoso.com		

- 60. Select the appropriate forest functional level and click Next.
- 61. Keep DNS server selected and click Next.

ditional Domain Controller Options		
Select additional options for this domain controller.		
DNS server		
🔽 Global catalog		
<u>Read-only domain controller (RODC)</u>		
Additional information:		
The first domain controller in a forest must be a glo cannot be an RODC.	-	_
	-	_
cannot be an RODC. We recommend that you install the DNS Server se	-	_
cannot be an RODC. We recommend that you install the DNS Server se controller.	-	_
cannot be an RODC. We recommend that you install the DNS Server se controller.	-	_
cannot be an RODC. We recommend that you install the DNS Server se controller.	-	_

- 62. If one or more DNS servers exist that this domain can resolve from, select Yes to create a DNS delegation. If this AD server is being created on an isolated network, select No, to not create a DNS delegation. The remaining steps in this procedure assume a DNS delegation is not created. Click Next.
- 63. Click Next to accept the default locations for database and log files.
- 64. Enter and confirm <<var_password>> for the Directory Services Restore Mode Administrator Password. Click Next.
- 65. Review the Summary information and click Next. Active Directory Domain Services will install.
- 66. Click Finish.
- 67. Click Restart Now to restart the AD Server.
- 68. After the machine has rebooted, log in as the domain Administrator.
- 69. Open the DNS Manager by clicking Start > Administrative Tools > DNS.
- 70. Optional: Add Reverse Lookup Zones for your IP address ranges.
- 71. Expand the Server and Forward Lookup Zones. Select the zone for the domain. Right-click and select New Host (A or AAAA). Populate the DNS Server with Host Records for all components in the VersaStack.
- 72. Optional: Build a second AD server VM. Add this server to the newly created Windows Domain and activate Windows. Install Active Directory Domain Services on this machine. Launch dcpromo.exe at the end of this installation. Choose to add a domain controller to a domain in an existing forest. Add this domain controller to the domain created earlier. Complete the installation of this second domain controller. After vCenter Server is installed, affinity rules can be created to keep the two AD servers running on different hosts.

Cisco Nexus 9000 Example Configurations

Cisco Nexus 9000 A

```
version 6.1(2)I3(1)
switchname nexus-a
vdc nexus-a id 1
  allocate interface Ethernet1/1-48
  allocate interface Ethernet2/1-12
 limit-resource vlan minimum 16 maximum 4094
 limit-resource vrf minimum 2 maximum 4096
 limit-resource port-channel minimum 0 maximum 512
 limit-resource u4route-mem minimum 248 maximum 248
 limit-resource u6route-mem minimum 96 maximum 96
 limit-resource m4route-mem minimum 58 maximum 58
 limit-resource m6route-mem minimum 8 maximum 8
cfs eth distribute
feature udld
feature interface-vlan
feature lacp
feature vpc
username admin password 5 $1$KZWYvfcW$.0SpzBMZIWDgxPaOvD1.w/ role
network-admin
ssh key rsa 2048
ip domain-lookup
copp profile strict
snmp-server user admin network-admin auth md5
0xab33b1fdbd4cbb3b0833d0a10044ec4d priv 0xab33b1fdbd4cbb3b0833d0a
10044ec4d 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 171.68.38.65
ip route 0.0.0.0/0 10.29.151.1
vlan 1-2,3172-3175
vlan 2
 name Native-VLAN
vlan 3172
 name NFS-VLAN
vlan 3173
 name vMotion-VLAN
vlan 3174
 name VM-Traffic-VLAN
vlan 3175
 name IB-MGMT-VLAN
vrf context management
 ip route 0.0.0.0/0 10.29.151.1
vpc domain 10
 peer-switch
 role priority 10
```

Appendix

```
peer-keepalive destination 10.29.151.15 source 10.29.151.14
 delay restore 150
 peer-gateway
 auto-recovery
 ip arp synchronize
interface Vlan1
interface Vlan3175
 no shutdown
 no ip redirects
 ip address 10.29.151.253/24
 no ipv6 redirects
interface port-channel10
  description vPC peer-link
  switchport mode trunk
 switchport trunk native vlan 2
  switchport trunk allowed vlan 3172-3175
  spanning-tree port type network
 vpc peer-link
interface port-channel11
  description file module nodeA
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3172-3174
  spanning-tree port type edge trunk
 mtu 9216
 vpc 11
interface port-channel12
  description file module nodeB
 switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3172-3175
  spanning-tree port type edge trunk
 mtu 9216
 vpc 12
interface port-channel13
  description ucs-A
  switchport mode trunk
 switchport trunk native vlan 2
  switchport trunk allowed vlan 3172-3175
 spanning-tree port type edge trunk
 mtu 9216
 vpc 13
interface port-channel14
 description ucs-b
  switchport mode trunk
 switchport trunk native vlan 2
  switchport trunk allowed vlan 3172-3175
 spanning-tree port type edge trunk
 mtu 9216
 vpc 14
```

```
interface Ethernet1/1
 description file module nodeA
 switchport mode trunk
 switchport trunk native vlan 2
 switchport trunk allowed vlan 3172-3174
 mtu 9216
 channel-group 11 mode active
interface Ethernet1/2
 description file module nodeB
 switchport mode trunk
 switchport trunk native vlan 2
 switchport trunk allowed vlan 3172-3175
 mtu 9216
 channel-group 12 mode active
interface Ethernet1/3
interface Ethernet1/4
interface Ethernet1/5
interface Ethernet1/6
interface Ethernet1/7
interface Ethernet1/8
interface Ethernet1/9
interface Ethernet1/10
interface Ethernet1/11
interface Ethernet1/12
interface Ethernet1/13
interface Ethernet1/14
interface Ethernet1/15
interface Ethernet1/16
interface Ethernet1/17
interface Ethernet1/18
interface Ethernet1/19
interface Ethernet1/20
interface Ethernet1/21
interface Ethernet1/22
interface Ethernet1/23
```

```
interface Ethernet1/24
interface Ethernet1/25
 switchport mode trunk
 switchport trunk native vlan 2
 switchport trunk allowed vlan 3172-3175
 mtu 9216
 channel-group 13 mode active
interface Ethernet1/26
 switchport mode trunk
  switchport trunk native vlan 2
 switchport trunk allowed vlan 3172-3175
 mtu 9216
 channel-group 14 mode active
interface Ethernet1/27
interface Ethernet1/28
interface Ethernet1/29
interface Ethernet1/30
interface Ethernet1/31
interface Ethernet1/32
interface Ethernet1/33
interface Ethernet1/34
interface Ethernet1/35
interface Ethernet1/36
  switchport access vlan 3175
  spanning-tree port type network
interface Ethernet1/37
interface Ethernet1/38
interface Ethernet1/39
interface Ethernet1/40
interface Ethernet1/41
interface Ethernet1/42
interface Ethernet1/43
interface Ethernet1/44
interface Ethernet1/45
interface Ethernet1/46
```

```
interface Ethernet1/47
  description VPC Peer Nexus-b:1/47
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3172-3175
  channel-group 10 mode active
interface Ethernet1/48
  description VPC Peer Nexus-b:1/48
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3172-3175
  channel-group 10 mode active
interface Ethernet2/1
interface Ethernet2/2
interface Ethernet2/3
interface Ethernet2/4
interface Ethernet2/5
interface Ethernet2/6
interface Ethernet2/7
interface Ethernet2/8
interface Ethernet2/9
interface Ethernet2/10
interface Ethernet2/11
interface Ethernet2/12
interface mgmt0
 vrf member management
  ip address 10.29.151.14/24
line console
line vty
boot nxos bootflash:/n9000-dk9.6.1.2.I3.1.bin
```

Cisco Nexus 9000 B

```
version 6.1(2)I3(1)
switchname nexus-B
vdc nexus-B id 1
  allocate interface Ethernet1/1-48
  allocate interface Ethernet2/1-12
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 512
  limit-resource u4route-mem minimum 248 maximum 248
```

```
limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
 limit-resource m6route-mem minimum 8 maximum 8
cfs eth distribute
feature udld
feature interface-vlan
feature lacp
feature vpc
username admin password 5 $1$XJ1VGLo9$uc07fUb3s2P3JJeeFCxAh0 role
network-admin
ssh key rsa 2048
ip domain-lookup
copp profile strict
snmp-server user admin network-admin auth md5
0x58c14ea179ccb2d533144bb710d6a20b priv 0x58c14ea179ccb2d533144bb
710d6a20b 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 171.68.38.65
ip route 0.0.0.0/0 10.29.151.1
vlan 1-2,3172-3175
vlan 2
 name Native-VLAN
vlan 3172
 name NFS-VLAN
vlan 3173
 name vMotion-VLAN
vlan 3174
 name VM-Traffic-VLAN
vlan 3175
 name IB-MGMT-VLAN
vrf context management
  ip route 0.0.0.0/0 10.29.151.1
vpc domain 10
 peer-switch
 role priority 20
 peer-keepalive destination 10.29.151.14 source 10.29.151.15
 delay restore 150
 peer-gateway
 auto-recovery
interface Vlan1
interface Vlan3175
 no shutdown
 no ip redirects
  ip address 10.29.151.254/24
 no ipv6 redirects
interface port-channel10
  description vPC peer-link
```

```
switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3172-3175
  spanning-tree port type network
 vpc peer-link
interface port-channel11
 description file module node A
 switchport mode trunk
 switchport trunk native vlan 2
 switchport trunk allowed vlan 3172-3174
  spanning-tree port type edge trunk
 mtu 9216
 vpc 11
interface port-channel12
 description file module nodeB
 switchport mode trunk
 switchport trunk native vlan 2
 switchport trunk allowed vlan 3172-3175
 spanning-tree port type edge trunk
 mtu 9216
 vpc 12
interface port-channel13
 description ucs-a
 switchport mode trunk
 switchport trunk native vlan 2
 switchport trunk allowed vlan 3172-3175
 spanning-tree port type edge trunk
 mtu 9216
 vpc 13
interface port-channel14
 description ucs-b
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3172-3175
 spanning-tree port type edge trunk
 mtu 9216
 vpc 14
interface Ethernet1/1
 description file module nodeB
 switchport mode trunk
 switchport trunk native vlan 2
 switchport trunk allowed vlan 3172-3175
 mtu 9216
  channel-group 12 mode active
interface Ethernet1/2
 description file node A
 switchport mode trunk
 switchport trunk native vlan 2
 switchport trunk allowed vlan 3172-3174
 mtu 9216
 channel-group 11 mode active
```

1

- interface Ethernet1/3
- interface Ethernet1/4
- interface Ethernet1/5
- interface Ethernet1/6
- interface Ethernet1/7
- interface Ethernet1/8
- interface Ethernet1/9
- interface Ethernet1/10
- interface Ethernet1/11
- interface Ethernet1/12
- interface Ethernet1/13
- interface Ethernet1/14
- interface Ethernet1/15
- interface Ethernet1/16
- interface Ethernet1/17
- interface Ethernet1/18
- interface Ethernet1/19
- interface Ethernet1/20
- interface Ethernet1/21
- interface Ethernet1/22
- interface Ethernet1/23
- interface Ethernet1/24
- interface Ethernet1/25
 switchport mode trunk
 switchport trunk native vlan 2
 switchport trunk allowed vlan 3172-3175
 mtu 9216
 channel-group 14 mode active
- interface Ethernet1/26
 switchport mode trunk
 switchport trunk native vlan 2
 switchport trunk allowed vlan 3172-3175
 mtu 9216
 channel-group 13 mode active

interface Ethernet1/27 interface Ethernet1/28 interface Ethernet1/29 interface Ethernet1/30 interface Ethernet1/31 interface Ethernet1/32 interface Ethernet1/33 interface Ethernet1/34 interface Ethernet1/35 interface Ethernet1/36 description ib-management-access switchport access vlan 3175 spanning-tree port type network interface Ethernet1/37 interface Ethernet1/38 interface Ethernet1/39 interface Ethernet1/40 interface Ethernet1/41 interface Ethernet1/42 interface Ethernet1/43 interface Ethernet1/44 interface Ethernet1/45 interface Ethernet1/46 interface Ethernet1/47 description VPC Peer Nexus-A:1/47 switchport mode trunk switchport trunk native vlan 2 switchport trunk allowed vlan 3172-3175 channel-group 10 mode active interface Ethernet1/48 description VPC Peer Nexus-A:1/48 switchport mode trunk switchport trunk native vlan 2 switchport trunk allowed vlan 3172-3175 channel-group 10 mode active

interface Ethernet2/1

I

interface Ethernet2/2 interface Ethernet2/3 interface Ethernet2/4 interface Ethernet2/5 interface Ethernet2/6 interface Ethernet2/7 interface Ethernet2/8 interface Ethernet2/9 interface Ethernet2/10 interface Ethernet2/11 interface Ethernet2/12 interface mgmt0 vrf member management ip address 10.29.151.15/24 line console line vty boot nxos bootflash:/n9000-dk9.6.1.2.I3.1.bin

Cisco MDS Example Configurations

MDS 9148S A

```
version 6.2(9)
power redundancy-mode redundant
feature npiv
feature fport-channel-trunk
role name default-role
  description This is a system defined role and applies to all users.
  rule 5 permit show feature environment
 rule 4 permit show feature hardware
  rule 3 permit show feature module
  rule 2 permit show feature snmp
  rule 1 permit show feature system
username admin password 5 $1$brR83.dk$/z40z1QEcPNZxHeYZWHVg1 role network-admin
ssh key rsa 2048
ip domain-lookup
ip host mds-a 10.29.151.18
aaa group server radius radius
snmp-server user admin network-admin auth md5 0x8fea5f7f943f41f0d6bc6da5601fa40f
priv 0x8fea5f7f943f41f0d6bc6da
5601fa40f 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 171.68.38.65
vsan database
  vsan 101
device-alias database
  device-alias name VM-Host-Infra-01-A pwwn 20:00:00:25:b5:00:0a:0f
  device-alias name VM-Host-Infra-02-A pwwn 20:00:00:25:b5:00:0a:1f
  device-alias name VersaStack-Nodel-A pwwn 50:05:07:68:0b:23:20:fc
  device-alias name VersaStack-Node2-A pwwn 50:05:07:68:0b:24:20:fd
device-alias commit
fcdomain fcid database
 vsan 1 wwn 20:20:00:2a:6a:cd:fd:00 fcid 0x6f0000 dynamic
 vsan 1 wwn 20:1f:00:2a:6a:cd:fd:00 fcid 0x6f0100 dynamic
 vsan 1 wwn 50:05:07:68:0b:23:20:fc fcid 0x6f0200 dynamic
             [VersaStack-Node1-A]
  vsan 1 wwn 50:05:07:68:0b:22:20:fd fcid 0x6f0300 dynamic
  vsan 1 wwn 50:05:07:68:0b:24:20:fd fcid 0x6f0400 dynamic
.
             [VersaStack-Node2-A]
  vsan 1 wwn 50:05:07:68:0b:21:20:fc fcid 0x6f0500 dynamic
  vsan 101 wwn 50:05:07:68:0b:24:20:fd fcid 0x580000 dynamic
1
               [VersaStack-Node2-A]
 vsan 101 wwn 50:05:07:68:0b:23:20:fc fcid 0x580100 dynamic
               [VersaStack-Node1-A]
1
 vsan 101 wwn 24:01:00:2a:6a:cd:fd:00 fcid 0x580200 dynamic
 vsan 101 wwn 20:00:00:25:b5:00:0a:0f fcid 0x580201 dynamic
1
               [VM-Host-Infra-01-A]
  vsan 101 wwn 20:00:00:25:b5:00:0a:1f fcid 0x580202 dynamic
1
               [VM-Host-Infra-02-A]
interface port-channel1
  channel mode active
  switchport rate-mode dedicated
vsan database
  vsan 101 interface port-channel1
 vsan 101 interface fc1/1
  vsan 101 interface fc1/2
clock timezone PST -8 0
switchname mds-a
line console
line vty
boot kickstart bootflash:/m9100-s5ek9-kickstart-mz.6.2.9.bin
boot system bootflash:/m9100-s5ek9-mz.6.2.9.bin
interface fc1/3
interface fc1/4
interface fc1/1
interface fc1/2
interface fc1/5
interface fc1/6
interface fc1/7
interface fc1/8
interface fc1/9
interface fc1/10
```

interface fc1/11 interface fc1/12 interface fc1/13 interface fc1/14 interface fc1/15 interface fc1/16 interface fc1/17 interface fc1/18 interface fc1/19 interface fc1/20 interface fc1/21 interface fc1/22 interface fc1/23 interface fc1/24 interface fc1/25 interface fc1/26 interface fc1/27 interface fc1/28 interface fc1/29 interface fc1/30 interface fc1/31 interface fc1/32 interface fc1/33 interface fc1/34 interface fc1/35 interface fc1/36 interface fc1/37 interface fc1/38 interface fc1/39 interface fc1/40 interface fc1/41 interface fc1/42 interface fc1/43 interface fc1/44 interface fc1/45 interface fc1/46 interface fc1/47 interface fc1/48 interface fc1/3 interface fc1/4 !Active Zone Database Section for vsan 101 zone name VM-Host-Infra-01-A vsan 101 member pwwn 20:00:00:25:b5:00:0a:0f l [VM-Host-Infra-01-A] member pwwn 50:05:07:68:0b:23:20:fc 1 [VersaStack-Node1-A] member pwwn 50:05:07:68:0b:24:20:fd [VersaStack-Node2-A] ï zone name VM-Host-Infra-02-A vsan 101 member pwwn 20:00:00:25:b5:00:0a:1f [VM-Host-Infra-02-A] 1 member pwwn 50:05:07:68:0b:23:20:fc l [VersaStack-Node1-A] member pwwn 50:05:07:68:0b:24:20:fd 1 [VersaStack-Node2-A] zone name V7000-cluster-comm-A vsan 101

```
member pwwn 50:05:07:68:0b:23:20:fc
l
                [VersaStack-Node1-A]
    member pwwn 50:05:07:68:0b:24:20:fd
                [VersaStack-Node2-A]
1
zoneset name VersaStack-A vsan 101
    member VM-Host-Infra-01-A
    member VM-Host-Infra-02-A
    member V7000-cluster-comm-A
zoneset activate name VersaStack-A vsan 101
do clear zone database vsan 101
!Full Zone Database Section for vsan 101
zone name VM-Host-Infra-01-A vsan 101
    member pwwn 20:00:00:25:b5:00:0a:0f
1
                [VM-Host-Infra-01-A]
    member pwwn 50:05:07:68:0b:23:20:fc
!
                [VersaStack-Node1-A]
    member pwwn 50:05:07:68:0b:24:20:fd
l
                [VersaStack-Node2-A]
zone name VM-Host-Infra-02-A vsan 101
    member pwwn 20:00:00:25:b5:00:0a:1f
!
                [VM-Host-Infra-02-A]
   member pwwn 50:05:07:68:0b:23:20:fc
l
                [VersaStack-Node1-A]
    member pwwn 50:05:07:68:0b:24:20:fd
1
                [VersaStack-Node2-A]
zone name V7000-cluster-comm-A vsan 101
    member pwwn 50:05:07:68:0b:23:20:fc
1
                [VersaStack-Node1-A]
    member pwwn 50:05:07:68:0b:24:20:fd
                [VersaStack-Node2-A]
1
zoneset name VersaStack-A vsan 101
    member VM-Host-Infra-01-A
    member VM-Host-Infra-02-A
    member V7000-cluster-comm-A
interface fc1/1
  port-license acquire
  no shutdown
interface fc1/2
  port-license acquire
  no shutdown
interface fc1/3
  port-license acquire
  channel-group 1 force
  no shutdown
interface fc1/4
  port-license acquire
  channel-group 1 force
  no shutdown
```

```
interface fc1/5
 port-license acquire
interface fc1/6
 port-license acquire
interface fc1/7
 port-license acquire
interface fc1/8
 port-license acquire
interface fc1/9
 port-license acquire
interface fc1/10
 port-license acquire
interface fc1/11
 port-license acquire
interface fc1/12
 port-license acquire
interface fc1/13
interface fc1/14
interface fc1/15
interface fc1/16
interface fc1/17
interface fc1/18
interface fc1/19
interface fc1/20
interface fc1/21
interface fc1/22
interface fc1/23
interface fc1/24
interface fc1/25
interface fc1/26
interface fc1/27
interface fc1/28
interface fc1/29
```

interface fc1/30

interface fc1/31

interface fc1/32

interface fc1/33

interface fc1/34

interface fc1/35

interface fc1/36

interface fc1/37

interface fc1/38

interface fc1/39

interface fc1/40

interface fc1/41

interface fc1/42

interface fc1/43

interface fc1/44

interface fc1/45

interface fc1/46

interface fc1/47

interface fc1/48

interface mgmt0
 ip address 10.29.151.18 255.255.255.0
 ip default-gateway 10.29.151.1

MDS 9148S B

```
version 6.2(9)
power redundancy-mode redundant
feature npiv
feature fport-channel-trunk
role name default-role
  description This is a system defined role and applies to all users.
  rule 5 permit show feature environment
  rule 4 permit show feature hardware
  rule 3 permit show feature module
  rule 2 permit show feature snmp
  rule 1 permit show feature system
username admin password 5 $1$iZDk0a3X$Wk0RSkgxjjuqk.Q82e.Rs1 role network-admin
```

```
ssh key rsa 2048
ip domain-lookup
ip host mds-b 10.29.151.19
aaa group server radius radius
snmp-server user admin network-admin auth md5 0xec1798634e2e7aea40c9d4500f80e937
priv 0xec1798634e2e7aea40c9d45
00f80e937 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 171.68.38.65
vsan database
  vsan 102
device-alias database
  device-alias name VM-Host-Infra-01-B pwwn 20:00:00:25:b5:00:0b:0f
  device-alias name VM-Host-Infra-02-B pwwn 20:00:00:25:b5:00:0b:1f
  device-alias name VersaStack-Node1-B pwwn 50:05:07:68:0b:24:20:fc
  device-alias name VersaStack-Node2-B pwwn 50:05:07:68:0b:23:20:fd
device-alias commit
fcdomain fcid database
  vsan 1 wwn 20:20:00:2a:6a:cd:ff:80 fcid 0xbb0000 dynamic
  vsan 1 wwn 20:1f:00:2a:6a:cd:ff:80 fcid 0xbb0100 dynamic
  vsan 1 wwn 50:05:07:68:0b:22:20:fc fcid 0xbb0200 dynamic
 vsan 1 wwn 50:05:07:68:0b:24:20:fc fcid 0xbb0300 dynamic
н
             [VersaStack-Node1-B]
  vsan 1 wwn 50:05:07:68:0b:23:20:fd fcid 0xbb0400 dynamic
             [VersaStack-Node2-B]
1
  vsan 1 wwn 50:05:07:68:0b:21:20:fd fcid 0xbb0500 dynamic
  vsan 102 wwn 50:05:07:68:0b:23:20:fd fcid 0xae0000 dynamic
Т
               [VersaStack-Node2-B]
  vsan 102 wwn 50:05:07:68:0b:24:20:fc fcid 0xae0100 dynamic
               [VersaStack-Node1-B]
  vsan 102 wwn 24:02:00:2a:6a:cd:ff:80 fcid 0xae0200 dynamic
  vsan 102 wwn 20:00:00:25:b5:00:0b:0f fcid 0xae0201 dynamic
               [VM-Host-Infra-01-B]
н
 vsan 1 wwn 24:02:00:2a:6a:cd:ff:80 fcid 0xbb0600 dynamic
  vsan 102 wwn 20:00:00:25:b5:00:0b:1f fcid 0xae0202 dynamic
               [VM-Host-Infra-02-B]
1
interface port-channel2
  channel mode active
  switchport rate-mode dedicated
vsan database
  vsan 102 interface port-channel2
 vsan 102 interface fc1/1
  vsan 102 interface fc1/2
clock timezone pst -8 0
switchname mds-b
line console
line vty
boot kickstart bootflash:/m9100-s5ek9-kickstart-mz.6.2.9.bin
boot system bootflash:/m9100-s5ek9-mz.6.2.9.bin
interface fc1/3
```

```
interface fc1/4
interface fc1/1
interface fc1/2
interface fc1/5
interface fc1/6
interface fc1/7
interface fc1/8
interface fc1/9
interface fc1/10
interface fc1/11
interface fc1/12
interface fc1/13
interface fc1/14
interface fc1/15
interface fc1/16
interface fc1/17
interface fc1/18
interface fc1/19
interface fc1/20
interface fc1/21
interface fc1/22
interface fc1/23
interface fc1/24
interface fc1/25
interface fc1/26
interface fc1/27
interface fc1/28
interface fc1/29
interface fc1/30
interface fc1/31
interface fc1/32
interface fc1/33
interface fc1/34
interface fc1/35
interface fc1/36
interface fc1/37
interface fc1/38
interface fc1/39
interface fc1/40
interface fc1/41
interface fc1/42
interface fc1/43
interface fc1/44
interface fc1/45
interface fc1/46
interface fc1/47
interface fc1/48
interface fc1/3
interface fc1/4
!Active Zone Database Section for vsan 102
zone name VM-Host-Infra-01-B vsan 102
   member pwwn 20:00:00:25:b5:00:0b:0f
!
                [VM-Host-Infra-01-B]
    member pwwn 50:05:07:68:0b:24:20:fc
!
                [VersaStack-Node1-B]
    member pwwn 50:05:07:68:0b:23:20:fd
1
                [VersaStack-Node2-B]
```

I

```
zone name VM-Host-Infra-02-B vsan 102
    member pwwn 20:00:00:25:b5:00:0b:1f
                [VM-Host-Infra-02-B]
1
   member pwwn 50:05:07:68:0b:24:20:fc
                [VersaStack-Node1-B]
1
    member pwwn 50:05:07:68:0b:23:20:fd
                [VersaStack-Node2-B]
!
zone name V7000-cluster-comm-B vsan 102
    member pwwn 50:05:07:68:0b:24:20:fc
I.
                [VersaStack-Node1-B]
    member pwwn 50:05:07:68:0b:23:20:fd
!
                [VersaStack-Node2-B]
zoneset name VersaStack-B vsan 102
    member VM-Host-Infra-01-B
    member VM-Host-Infra-02-B
    member V7000-cluster-comm-B
zoneset activate name VersaStack-B vsan 102
do clear zone database vsan 102
!Full Zone Database Section for vsan 102
zone name VM-Host-Infra-01-B vsan 102
    member pwwn 20:00:00:25:b5:00:0b:0f
                [VM-Host-Infra-01-B]
!
    member pwwn 50:05:07:68:0b:24:20:fc
1
                [VersaStack-Node1-B]
    member pwwn 50:05:07:68:0b:23:20:fd
1
                [VersaStack-Node2-B]
zone name VM-Host-Infra-02-B vsan 102
    member pwwn 20:00:00:25:b5:00:0b:1f
                [VM-Host-Infra-02-B]
1
    member pwwn 50:05:07:68:0b:24:20:fc
1
                [VersaStack-Node1-B]
    member pwwn 50:05:07:68:0b:23:20:fd
                [VersaStack-Node2-B]
!
zone name V7000-cluster-comm-B vsan 102
    member pwwn 50:05:07:68:0b:24:20:fc
I.
                [VersaStack-Node1-B]
    member pwwn 50:05:07:68:0b:23:20:fd
!
                [VersaStack-Node2-B]
zoneset name VersaStack-B vsan 102
    member VM-Host-Infra-01-B
    member VM-Host-Infra-02-B
    member V7000-cluster-comm-B
interface fc1/1
  port-license acquire
  no shutdown
interface fc1/2
  port-license acquire
  no shutdown
```

interface fc1/3 port-license acquire channel-group 2 force no shutdown interface fc1/4 port-license acquire channel-group 2 force no shutdown interface fc1/5 port-license acquire interface fc1/6 port-license acquire interface fc1/7 port-license acquire interface fc1/8 port-license acquire interface fc1/9 port-license acquire interface fc1/10 port-license acquire interface fc1/11 port-license acquire interface fc1/12 port-license acquire interface fc1/13 interface fc1/14 interface fc1/15 interface fc1/16 interface fc1/17 interface fc1/18 interface fc1/19 interface fc1/20 interface fc1/21 interface fc1/22 interface fc1/23 interface fc1/24

VersaStack for Data Center

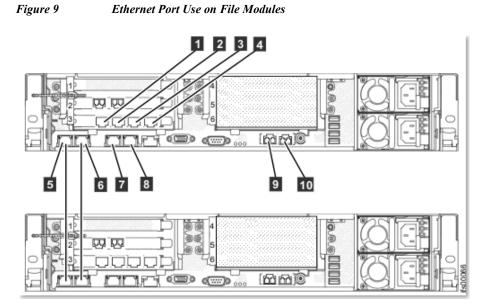
- interface fc1/25
- interface fc1/26
- interface fc1/27
- interface fc1/28
- interface fc1/29
- interface fc1/30
- interface fc1/31
- interface fc1/32
- interface fc1/33
- interface fc1/34
- interface fc1/35
- interface fc1/36
- interface fc1/37
- interface fc1/38
- interface fc1/39
- interface fc1/40
- interface fc1/41
- interface fc1/42
- interface fc1/43
- interface fc1/44
- interface fc1/45
- interface fc1/46
- interface fc1/47
- interface fc1/48

I

interface mgmt0
 ip address 10.29.151.19 255.255.255.0
ip default-gateway 10.29.151.1

Additional IBM Storwize V7000 Control Enclosure and V7000 File Module Port Information

1



ID	Port	IP address is	Use
		assigned by	
		InitTool	
1	Ethernet port 7		Connect to a switch for public
			file access
2	Ethernet port 8		Connect to a switch for public
			file access
3	Ethernet port 9		Connect to a switch for public
			file access
4	Ethernet port 10		Connect to a switch for public
			file access
5	Ethernet port 1	From the internal IP	Connect to the other file
		address range	module
6	Ethernet port 2	From the internal IP	Connect to the other file
		address range	module
7	Ethernet port 3	File module service	Connect to a switch for public
		and system	file access and system
		management IP	management
		address	
8	Ethernet port 4		Connect to a switch for public
			file access
9	Ethernet port 5		Connect to a switch for public
	(10 Gbps optical)		file access and optional
			system management
10	Ethernet port 6		Connect to a switch for public
	(10 Gbps optical)		file access

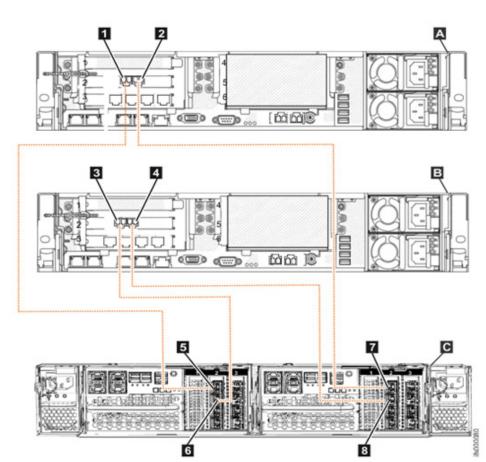
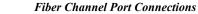


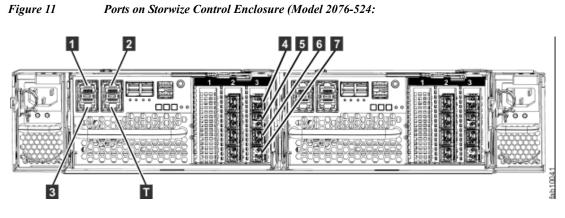
Figure 10 Fib



Key

Γ

- A File module 1
- B File module 2
- C Storwize V7000 Gen2 control enclosure (2076-524)
- 1 File module 1 Fibre Channel port 1
- 2 File module 1 Fibre Channel port 2
- 3 File module 2 Fibre Channel port 1
- 4 File module 2 Fibre Channel port 2
- 5 Node canister 1 (left) Fibre Channel port 1
- 6 Node canister 1 (left) Fibre Channel port 2
- 7 Node canister 2 (right) Fibre Channel port 1
- 8 Node canister 2 (right) Fibre Channel port 2



1

Key

- 1, 2: 1GbE management, iSCSI and IP replication ports
- 3: 1GbE iSCSI and IP replication port
- 4-7: 8GbE fibrechannel ports