VersaStack for Data Center with Direct Attached Storage

Deploying Cisco Unified Computing System and Cisco Nexus 9000 Series Switches, IBM Storwize V7000 Unified Storage and VMware vSphere 5.5 Update 2, using Fabric Interconnect Direct Attached Storage

Last Updated: July 28, 2015

Cisco Validated Design

Building Architectures to Solve Business Problems

About the Authors

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

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, Inc.

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

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

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

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

VersaStack for Data Center with Direct Attached Storage

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

This design leverages the flexibility of the Cisco Fabric Interconnect to operate in FC Switching Mode. This deployment model eliminates the need for a separate Fibre Channel Switch to help reduce deployment costs. UCS Manager San Connectivity Policies are used to help automate SAN zoning for the administrator.

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 System™ (Cisco UCS®), Cisco 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:

- Common Infrastructure services on redundant and self-contained hardware.

- 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 Fabric Interconnect direct attached design allows connection to the IBM Storwize V7000 storage controllers without the use of separate Fibre Channel Switch. VersaStack 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

- 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.

- Support for up to a total of 4 V7000 control enclosures, up to 80 V7000 expansion enclosures, and up to 1056 SFF or large form-factor (LFF) 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 Nexus 9000 based VersaStack architecture. Please check IBM and Cisco support Matrix links in the VersaStack Design Guide for latest supported versions. To validate your enic version run the "ethtool -i vmnic0" through the command line of the ESX host.

Table 1   *Software Revisions*

Layer	Device	Version or Release	Details
Compute	Cisco UCS fabric interconnect	2.2(3d)	Embedded management
	Cisco UCS C 220 M3/M4	2.2(3d)	Software bundle release
	Cisco UCS B 200 M3/ M4	2.2(3d)	Software bundle release
	Cisco enic	2.1.2.59	Ethernet driver for Cisco VIC
Network	Cisco Nexus 9396	6.1(2)I3(1)	Operating system version
Storage	IBM Storwize V7000	7.3.0.9	Software version
	IBM Storwize V7000 Unified	1.5.0.5-1	Software version
Software	Cisco UCS hosts	VMware vSphere ESXi™ 5.5u2	Operating system version
	Microsoft SQL Server®	Microsoft SQL Server 2008 R2 SP1	VM (1 each): SQL Server DB
	VMware vCenter™	5.5u2	VM (1 each): VMware vCenter
	Cisco Nexus 1000v	5.2(1)SV3(1.2)	Software version
	Virtual Switch Update Manager (VSUM)	1.1	Virtual Switch Deployment Software

IBM System Storage Interoperability Center:

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

Cisco UCS Interoperability Matrix:

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

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

Figure 2   Overview of VLAN Usage

Table 3   VMware Virtual Machine 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 4   Configuration Variables

Variable	Description	Customer Implementation Value
`<<var_node01_mgmt_ip>>`	Out-of-band management IP for cluster node 01	
`<<var_node01_mgmt_mask>>`	Out-of-band management network netmask	
`<<var_node01_mgmt_gateway>>`	Out-of-band management network default gateway	
`<<var_node02_mgmt_ip>>`	Out-of-band management IP for cluster node 02	
`<<var_node02_mgmt_mask>>`	Out-of-band management network netmask	
`<<var_node02_mgmt_gateway>>`	Out-of-band management network default gateway	
`<<var_cluster_mgmt_ip>>`	Out-of-band management IP for cluster	
`<<var_cluster_mgmt_mask>>`	Out-of-band management network netmask	
`<<var_cluster_mgmt_gateway>>`	Out-of-band management network default gateway	
`<<var_password>>`	Global default administrative password	
`<<var_dns_domain_name>>`	DNS domain name	
`<<var_nameserver_ip>>`	DNS server IP(s)	
`<<var_timezone>>`	VersaStack time zone (for example, America/New_York)	
`<<var_global_ntp_server_ip>>`	NTP server IP address	
`<<var_email_contact>>`	Administrator e-mail address	
`<<var_admin_phone>>`	Local contact number for support	
`<<var_mailhost_ip>>`	Mail server host IP	
`<<var_country_code>>`	Two-letter country code	
`<<var_state>>`	State or province name	
`<<var_city>>`	City name	
`<<var_org>>`	Organization or company name	
`<<var_unit>>`	Organizational unit name	

<<var_street_address>>,	Street address for support information	
<<var_contact_name>>	Name of contact for support	
<<var_admin>>	Secondary Admin account for storage login	
<<var_nexus_A_hostname>>	Cisco Nexus A host name	
<<var_nexus_A_mgmt0_ip>>	Out-of-band Cisco Nexus A management IP address	
<<var_nexus_A_mgmt0_netmask>>	Out-of-band management network netmask	
<<var_nexus_A_mgmt0_gw>>	Out-of-band management network default gateway	
<<var_nexus_B_hostname>>	Cisco Nexus B host name	
<<var_nexus_B_mgmt0_ip>>	Out-of-band Cisco Nexus B management IP address	
<<var_nexus_B_mgmt0_netmask>>	Out-of-band management network netmask	
<<var_nexus_B_mgmt0_gw>>	Out-of-band management network default gateway	
<<var_ib-mgmt_vlan_id>>	In-band management network VLAN ID	
<<var_native_vlan_id>>	Native VLAN ID	
<<var_nfs_vlan_id>>	NFS VLAN ID	
<<var_vmotion_vlan_id>>	VMware vMotion® VLAN ID	
<<var_vm-traffic_vlan_id>>	VM traffic VLAN ID	
<<var_nexus_vpc_domain_id>>	Unique Cisco Nexus switch VPC domain ID	
<<var_ucs_clustername>>	Cisco UCS Manager cluster host name	
<<var_ucsa_mgmt_ip>>	Cisco UCS fabric interconnect (FI) A out-of-band management IP address	
<<var_ucsa_mgmt_mask>>	Out-of-band management network netmask	
<<var_ucsa_mgmt_gateway>>	Out-of-band management network default gateway	
<<var_ucs_cluster_ip>>	Cisco UCS Manager cluster IP address	
<<var_ucsb_mgmt_ip>>	Cisco UCS FI B out-of-band management IP address	
<<var_cimc_mask>>	Out-of-band management network netmask	
<<var_cimc_gateway>>	Out-of-band management network default gateway	
<<var_vsm_domain_id>>	Unique Cisco Nexus 1000v virtual supervisor module (VSM) domain ID	
<<var_vsm_mgmt_ip>>	Cisco Nexus 1000v VSM management IP address	

`<<var_vsm_updatemgr_mgmt_ip>>`	Virtual Switch Update Manager IP address	
`<<var_vsm_mgmt_mask>>`	In-band management network netmask	
`<<var_vsm_mgmt_gateway>>`	In-band management network default gateway	
`<<var_vsm_hostname>>`	Cisco Nexus 1000v VSM host name	
`<<var_ftp_server>>`	IP address for FTP server	
`<<var_UTC_offset>>`	UTC time offset for your area	
`<<var_vsan_a_id>>`	Vsan id for Fabric A (101 is used)	
`<<var_vsan_B_id>>`	Vsan id for Fabric B (102 is used)	
`<<var_fabric_a_fcoe_vlan_id>>`	Fabric id for Fabric A (101 is used)	
`<<var_fabric_b_fcoe_vlan_id>>`	Fabric id for Fabric B (102 is used)	
`<<var_In-band_mgmtblock_net>>`	Block of IP addresses for KVM access for UCS	
`<<var_v7000_unified_management _IP>>,`	V7000 Unified MGMT IP	
`<<var_file_module_1_service ip>>`	V7000 Unified node console MGMT IP node 1	
`<<var_file_module_2_service ip>>`	V7000 Unified node console MGMT IP node 2	
`<<var_filemodule_name>>`	Netbios name for V7000 unified cluster	
`<<var_unified_bond_ip_network> >`	Network ip for the V7000 unified bond for NFS	
`<<var_unified_bond_ip_Netmask> >`	Network Mask for the V7000 unified bond for NFS	
`<<var_unified_bond_ip_gateway> >`	Gateway Mask for the V7000 unified bond for NFS	
`<<var_unified_bond_public_ip>>`	Network IP address that is mounted from NFS hosts for the V7000 unified bond	
`<<var_unified_datastore_name>>`	NFS Datastore for V7000 unified	
`<<var_vmhost_infra_01_ip>>`	VMware ESXi host 01 in-band Mgmt IP	
`<<var_vmhost_infra_01_2nd_ip>>`	VMware ESXi host 01 secondary in-band Mgmt IP	
`<<var_nfs_vlan_id_ip_host-01>>`	NFS VLAN IP address for ESXi host 01	
`<<var_nfs_vlan_id_mask_host-01 >>`	NFS VLAN netmask for ESXi host 01	
`<<var_vmotion_vlan_id_ip_host- 01>>`	vMotion VLAN IP address for ESXi host 01	
`<<var_vmotion_vlan_id_mask_hos t-01>>`	vMotion VLAN netmask for ESXi host 01	
The last 6 variables should be repeated for all ESXi hosts		

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 7.3.0.9, 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 5 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_qisascables_b4jtyu.html?cp=ST3FR7%2F1-3-0-1-3&lang=en

Figure 3 *VersaStack Block and File Cabling Diagram*

Figure 4 *VersaStack Block-Only Cabling Diagram*

Figure 5　　　*VersaStack Management Cabling*

Table 5 through Table 15 provide the details of all the connections in use.

Table 5   Cisco Nexus 9000-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 9000-A	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
	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

* 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=).

Table 6   Cisco Nexus 9000-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 9000-B	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
	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.

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

Table 7   *IBM Storwize V7000 File Module-A Cabling Information*

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

Table 8   *IBM Storwize V7000 File Module-B Cabling Information*

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

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	Cisco UCS fabric interconnect-A	fc1/31
	FC4	8gbps	Cisco UCS fabric interconnect-B	fc1/31

Table 10   IBM Storwize V7000 Controller Node-2 Cabling Information

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	Cisco UCS fabric interconnect-A	fc1/32
	FC4	8gbps	Cisco UCS fabric interconnect-B	fc1/32

Table 11   Cisco UCS Fabric Interconnect-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect-A	Mgmt0	GbE	GbE management switch	Any
	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	V7000 Controller, Node-1	fc1/3
	fc32	8gbps	V7000 Controller, Node-2	fc1/3
	L1	GbE	Cisco UCS fabric interconnect-B	L1
	L2	GbE	Cisco UCS fabric interconnect-B	L2

Table 12   Cisco UCS Fabric Interconnect-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect-B	Mgmt0	GbE	GbE management switch	Any
	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	V7000 Controller, Node-1	fc1/4
	fc32	8gbps	V7000 Controller, Node-2	fc1/4
	L1	GbE	Cisco UCS fabric interconnect-A	L1
	L2	GbE	Cisco UCS fabric interconnect-A	L2

Table 13   Cisco Rack-Mount Server Cabling Information

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

Table 14   Cisco Nexus Rack FEX A Cabling Information

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 15   Cisco Nexus Rack FEX B Cabling Information

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

Detailed information about supported hardware, device driver, firmware and software level information can be found at:

http://www-01.ibm.com/support/docview.wss?uid=ssg1S1004622

Complete the Configuration Worksheet

Before starting the setup, complete the Configuration worksheet from the IBM Storwize V7000 Knowledge Center (Table 16).

Table 16   Configuration Worksheets

	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.doc/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.unified.150.doc/ifs_completeconfdata.html?lang=en

VersaStack System Build Process

Figure 6 illustrates the VersaStack system build workflow.

Figure 6   VersaStack Installation Workflow

Cisco Nexus 9000 Network Initial Configuration Setup

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

Cisco Nexus A

1. To set up the initial configuration for the first 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_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]:
[########################################] 100%
Copy complete.
```

Cisco Nexus B

1. 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]:
Use this configuration and save it? (yes/no) [y]:
[#####################################] 100%
Copy complete.
```

Enable Appropriate Cisco Nexus 9000 Features and Settings

Cisco Nexus 9000 A and Cisco Nexus 9000 B

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

Note   On each Nexus 9000, enter configuration mode:

```
config terminal
```

2. 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:

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
```

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 Po10
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 Po10
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 UCS Fabric Interconnect

Cisco Nexus 9000 A

1. Define a description for the port-channel connecting to <<var_ucs_clustername>>-A.

```
interface Po13
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 mode active
no shutdown
```

8. Define a description for the port-channel connecting to <<var_ucs_clustername>>-B

```
interface Po14
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 mode active
no shutdown
copy run start
```

Configure Network Interfaces to UCS Fabric Interconnect

Cisco Nexus 9000 B

1. 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

```
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  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 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 through 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

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_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
```

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 through HTTP will get redirected to HTTPS.

The system generates its own self-signed SSL certificate. On 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 settings.

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.

   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.

![Note icon]

Note 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

3. Open a browser and go to address https://install which will direct you to the initialization wizard.

4. When asked how the node will be used, select "As the first node in a new system"

5. 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>>`.

6. 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.

7. 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.

8. Log in as superuser with password of passw0rd.

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

10. On the Welcome to system setup screen hit Next.

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

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

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

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

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

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

17. 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.

18. Insert Contact details **<<var_contact_name>> <<var_email_contact>> <<var_admin_phone>><<var_city>>** then click Apply and Next and click Close.

19. 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.

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

21. 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.

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

23. Review the Summary and click Finish. Review and close the tasks completed screen and click Close.

24. 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.

25. Click the Settings icon in the lower left screen, and select the Network tab.

26. 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 click Close.

27. 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 .

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

29. 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.

30. 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.

31. 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.

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

33. 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.

✎

Note 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.

34. 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.

35. Input quantity 1, capacity 500GB, and name infra_datastore_1. Click Create, then click Close.

36. 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.

37. 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.

38. Select Fiber Channel Ports in the lower left menu, then expand ports 3 and 4 to show the WWPNs.

Note 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.

39. 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 17   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 and make sure that the configuration process has completed before proceeding. It could take approximately 3-5 minutes.

Cisco UCS 6248 B

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

1. 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(3d)

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

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

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.

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.

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.

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.

Change FI to FC Switching Mode on FI-A and FI-B

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

1. Navigate to the Equipment tab in the left pane and expand the Fabric Interconnects object.

2. Select Fabric Interconnect A, in the left pane, General tab, and click Set FC Switch Mode in the left pane.

3. Click yes, then OK.

4. Wait for the Fabric Interconnects to reboot before proceeding. This should take approximately 5 minutes for the reboot of both nodes.

Enable Fibre Channel Ports

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

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 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.

3. Select the Fabric Interconnect A, (primary), then select Configure Unified Ports, and hit 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 Storage VSANs

These steps provide details for configuring the necessary VSANs and FC Port Channels for the Cisco UCS environment.

1. Select the SAN tab at the top left of the window.

2. Expand the Storage Cloud tree.

3. Right-click VSANs

4. Select Create Storage VSAN.

5. Enter VSAN_A as the VSAN name for fabric A.

6. Set the Enabled option for the FC Zoning Setting

7. Select Fabric A.

8. Enter the VSAN ID for fabric A. <<var_vsan_a_id>>

9. Enter the FCoE VLAN ID for fabric A. <<var_vsan_a_id>>

10. Click OK and then OK to create the VSAN.

11. Right-click VSANs.

12. Select Create Storage VSAN.

13. Enter VSAN_B as the VSAN name for fabric B.

14. Set the Enabled option for the FC Zoning Settings

15. Select Fabric B.

16. Enter the VSAN ID for fabric B. <<var_vsan_b_id>>

17. Enter the FCoE VLAN ID for fabric B. <<var_vsan_b_id>>

18. Click OK and then OK to create the VSAN.

Configure the FC Storage Ports

To configure FC Storage Ports complete the following steps:

1. Select the Equipment tab on the top left of the window.

2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module.

3. Expand the FC Ports object.

4. Select FC port 31 that is connected to the IBM storage array.

5. Select configure as FC storage port in the on the General tab.

6. Click Yes, then click OK

7. Select FC port 32 that is connected to the IBM storage array.

8. Select configure as FC storage port in the on the General tab.

9. Click Yes, then Click OK.

10. Select Equipment > Fabric Interconnects > Fabric Interconnect B

11. (primary) > Fixed Module.

12. Expand the FC Ports object.

13. Select FC port 31 that is connected to the IBM storage array.

14. Select configure as FC storage port in the on the General tab.

15. Click Yes, then click OK.

16. Select FC port 32 that is connected to the IBM storage array.

17. Select configure as FC storage port in the on the General tab.

18. Click Yes, then click OK.

Configure the VSAN for the FC Storage Ports

To configure VSAN-A and VSAN-B, complete the following steps:

1. Select the Equipment tab on the top left of the window.

2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module.

3. Expand the FC Ports object.

4. Select FC port 31 that is connected to the IBM storage array.

5. In the right pane, click the VSAN drop-down menu and select Fabric A / vsan VSAN_A (101).

6. Click the Save Changes button then click OK.

7. Select FC port 32 that is connected to the IBM storage array.

8. In the right pane, click the VSAN drop-down menu and select Fabric A / vsan VSAN_A (101).

9. Click the Save Changes button then click OK.

10. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.

11. Expand the FC Ports object.

12. Select FC port 31 that is connected to the storage array.

13. In the right pane, click the VSAN drop-down menu and select Fabric B / vsan VSAN_B (102).

14. Click the Save Changes button then click OK.

15. Select FC port 32 that is connected to the storage array.

16. In the right pane, click the VSAN drop-down menu and select Fabric B / vsan VSAN_B(102).

17. Click the Save Changes button then click OK.

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 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 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.

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

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

11. Click OK.

12. Click Finish to create the WWPN pool.

13. Click OK.

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.

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

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

22. Click OK.

23. Click Finish.

24. Click OK.

Create vHBA Templates for Fabric A and Fabric B

To create multiple virtual host bus adapter (vHBA) templates for the Cisco UCS environment, 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.

11. In the navigation pane, click the SAN tab.

12. Choose Policies > root.

13. Right-click vHBA Templates.

14. Choose Create vHBA Template.

15. Enter vHBA_Template_B as the vHBA template name.

16. Click the radio button Fabric B.

17. In the Select VSAN list, Choose VSAN_B.

18. In the WWPN Pool, Choose WWPN_Pool_B.

19. Click OK to create the vHBA template.

20. Click OK.

Create the Storage Connection Policy Fabric-A

To create a storage policy for Fabric-A that will help create the FC fabric zoning, follow these steps:

1. Select the SAN tab at the top left of the window.

2. Go to Policies > root.

3. Right-click Storage Connection Policies.

4. Select Create Storage Connection Policy.

5. Enter Storage Connection Policy name Fabric-A.

6. Select the Zoning Type Single Initiator Multiple Targets.

Create Storage Connection Policy

Name: Fab-A-Infra

Description:

Zoning Type: ◯ None ◯ Single Initiator Single Target ◉ Single Initiator Multiple Targets

FC Target Endpoints

Filter ⇒ Export 🖨 Print

WWPN	Path	VSAN

7. Click the plus icon to add the FC Target Endpoint.

8. Enter the WWPN for Node 1 Fabric A <<var_wwpn_Node1-switch-A>>.

9. Select Path A.

10. Select VSAN VSAN_A.

Create FC Target Endpoint

WWPN: 50:05:07:68:0B:23:20:FC

Description: node1-A

Path: ◉ A ◯ B

Select VSAN: VSAN VSAN-A (1... ▼ ➕ Create VSAN

                <not set>
                VSAN VSAN-A (101)
                VSAN default (1)

11. Click OK to create the FC Target Endpoint.

12. Click the plus icon to add the FC Target Endpoint.

13. Enter the WWPN for Node 2 FC path A <<var_wwpn_Node2-switch-A>>.

14. Select Path A.

15. Select VSAN VSAN_A.

16. Click OK to create the FC Target Endpoint.

17. Click OK to create the storage connection policy.

Create the Storage Connection Policy Fabric-B

To create the storage connection policy for Fabric-B, complete the following steps:

1. Select the SAN tab at the top left of the window.

2. Go to Policies > root .

3. Right-click Storage Connection Policies.

4. Select Create Storage Connection Policy.

5. Enter Storage Connection Policy name. Fabric-B.

6. Select the Zoning Type Single Initiator Multiple Targets.

7. Click the plus icon to add the FC Target Endpoint.

8. Enter the WWPN for Node 1 Fabric B <<var_wwpn_Node1-Switch-B>>.

9. Select Path B.

10. Select VSAN VSAN_B.

11. Click OK to create the FC Target Endpoint.

12. Click the plus icon to add the FC Target Endpoint.

13. Enter the WWPN for <<var_wwpn_Node2-switch-B>>.

14. Select Path B.

15. Select VSAN VSAN_B.

16. Click OK to create the FC Target Endpoint.

17. Click OK to create the storage connection policy.

Create a SAN Connectivity Policy

To create a San Connectivity Policy that will be leveraged for automated Fibre Channel zone creation on the Fabric interconnect, follow these steps:

1. Select the SAN tab at the top left of the window.

2. Go to Policies > root.

3. Right click the SAN Connectivity Policies, and Click create New San Connectivity policy.

4. Input name Dual-Fabric.

5. Select WWNN_Pool for WWNN Assignment .

Create SAN Connectivity Policy

Name: Dual-Fabric
Description:

A server is identified on a SAN by its World Wide Node Name (WWNN). Specify how the system should assign a WWNN to the server associated with this profile.

World Wide Node Name

WWNN Assignment: WWNN_Pool(30/32)

➕ Create WWNN Pool

The WWNN will be assigned from the selected pool.
The available/total WWNNs are displayed after the pool name.

Name	WWPN

🗑 Delete ➕ Add 📝 Modify

OK   Cancel

6. Click the Add button on the bottom.

7. Enter Name Fabric-A.

8. Click Use vHBA-template.

9. Select vHBA_Template_A.

10. Select Adapter Policy VMware.

11. Click OK.

12. Click Add.

13. Enter Name Fabric-B.

14. Select Use vHBA Template.

15. Select vHBA-Template-B.

16. Select Adapter Policy VMware.

17. Click OK to complete the policy creation.

18. Click OK.

19. Expand the San Connectivity Policies and click the Dual-Fabric policy.

20. In the right screen, click the HBA initiator groups tab.

21. Click the green add button on the right side.

22. Enter Fabric-A for the Name.

23. Click the Fabric-A select box.

24. For Storage Connection Policy, Select Fabric-A.

25. Click OK, then click OK again.

26. Click the Add button.

27. For the Name input Fabric-B.

28. Select the checkbox Fabric-B.

29. For Storage Connection Policy, Select Fabric-B.

30. Click OK, then Click OK again.

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.

6. Click Yes, then click OK.

Create Uplink Port Channels to Cisco Nexus Switches

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

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

✎

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.

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.

✎

Note 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.

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.

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.

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:

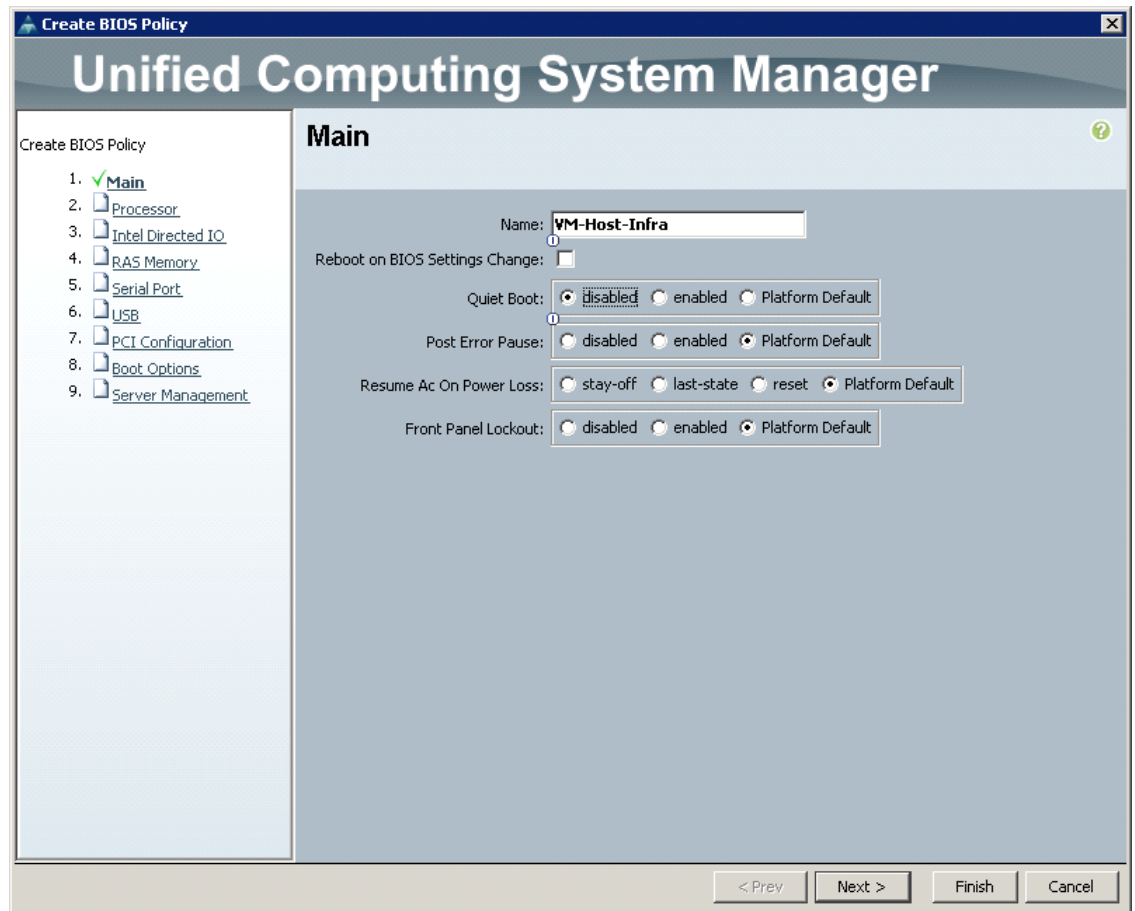Note   Consider creating unique server pools to achieve the granularity that is required in your environment.

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.

Note   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.

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.

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(3d) for Blade Servers. Also Select the 2.2(3d) for the Rack Package if using rack servers.

8. Click OK to create the host firmware package.

9. Click OK.

Set Jumbo Frames in Cisco UCS Fabric

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

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

2. Select LAN > LAN Cloud > QoS System Class.

3. In the right pane, click the General tab.

4. On the Best Effort row, enter 9216 in the box under the MTU column.

5. Click Save Changes in the bottom of the window.

6. Click OK.

Create Local Disk Configuration Policy

This will create a SAN boot disk policy. 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 for San-Boot, complete the following steps:

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

2. Select Policies > root.

3. Right-click Local Disk Config Policies.

4. Select Create Local Disk Configuration Policy.

5. Enter SAN-Boot as the local disk configuration policy name.

6. Change the mode to No Local Storage.

7. Click OK, to create the local disk configuration policy.

8. Click OK.

Create Network Control Policy for Cisco Discovery Protocol

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

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

2. Select Policies > root.

3. Right-click Network Control Policies.

4. Select Create Network Control Policy

5. Enter Enable_CDP as the policy name.

6. For CDP, select the Enabled option.

7. Click OK to create the network control policy.

8. Click OK.

Create Power Control Policy

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

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

2. Select Policies > root.

3. Right-click Power Control Policies.

4. Select Create Power Control Policy

5. Enter No-Power-Cap as the power control policy name.

6. Change the power capping setting to No Cap.

7. Click OK to create the power control policy.

8. Click OK.

Create Server Pool Qualification Policy (Optional)

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

Note This example creates a policy for a B200-M3 server. If you have purchased B200-M4 servers, please change the values of M3 to M4.

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 BIOS Policy

These polices below are for optimal performance for VMware. Depending on your requirements, you can change the settings appropriately. Please consult Cisco UCS documentation. To create a server BIOS policy for the Cisco UCS environment, complete the following steps:

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

2. Select Policies > root.

3. Right-click BIOS Policies.

4. Select Create BIOS Policy

5. Enter VM-Host-Infra as the BIOS policy name.

6. Change the Quiet Boot setting to Disabled.

7. Click Next.

8. Change Turbo Boost to enabled.

9. Change Enhanced Intel Speedstep to enabled.

10. Change Hyper Threading to enabled.

11. Change Core Multi Processing to all.

12. Change Execution Disabled Bit to enabled.

13. Change Virtualization Technology (VT) to enabled.

14. Change Direct Cache Access to enabled.

15. Change CPU Performance to Enterprise.

16. Click next to go the Intel Directed IO Screen.

17. Change the VT for Direct IO to enabled.

✎

Note   With the Cisco VM-FEX technology, virtual machines can now directly write to the virtual network interface cards (NICs) when the directed I/O option is enabled at the BIOS level.

18. Click next to go the RaS Memory screen.

19. Change the Memory RAS Config to maximum performance,

20. Change NUMA to enabled.

21. Change LV DDR Mode to performance-mode.

22. Click Finish to create the BIOS policy.

23. Click OK.

Create vNIC/vHBA Placement Policy for Virtual Machine Infrastructure Hosts

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

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

2. Select Policies > root.

3. Right-click vNIC/vHBA Placement Policies.

4. Select Create Placement Policy.

5. Enter VM-Host-Infra as the name of the placement policy.

6. Click 1 and select Assigned Only.

7. Click OK, and then click OK again.

Update the 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:

Note 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

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.

Create Boot Policies

This procedure applies to a Cisco UCS environment in which two FC interfaces are on cluster node 1 and two FC interfaces are on cluster node 2.

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

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

> **Note** You will be using the WWPN variables that were logged in the storage section 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).

9. Scroll down on the left side and 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.

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.

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.

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

23. In the Add SAN Boot dialog box, enter Fabric-B in the vHBA box.

24. The SAN boot type should automatically be set to Secondary

25. Click OK to add the SAN boot initiator.

26. From the vHBA drop-down menu, choose Add SAN Boot Target.

27. Keep 0 as the value for Boot Target LUN.

28. Enter the WWPN for node 2 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.

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.

35. Click OK, and then 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 <<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.

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.

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.

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

Name: vNIC-A

Use vNIC Template: ☑

➕ Create vNIC Template

vNIC Template: vNIC_Template_A ▼

Adapter Performance Profile

Adapter Policy: VMWare ▼ ➕ Create Ethernet Adapter Policy

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.

    l. 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.

7. Configure the Storage options:

    a. Choose a local disk configuration policy:

      – If the server in question has local disks, choose default in the Local Storage list.

      – If the server in question does not have local disks, choose SAN-Boot.

    b. Click the Use Connectivity Policy radio button to configure the SAN connectivity.

    c. For the SAN connectivity Policy select Dual-Fabric.

    d. Click Next.

8. Accept the 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.

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.

12. Add a Maintenance Policy:

    a. Choose the Default Maintenance Policy.

    b. Click Next.

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.

14. Add Operational Policies:

    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.

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.

22. Click OK.

23. Choose the newly cloned service profile template and click the Boot Order tab.

24. Click Modify Boot Policy.

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

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.

29. Click OK, and then click OK again.

Create Service Profiles

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.

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.

15. Click OK in the confirmation message.

16. 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.

17. (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 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

Add More Servers

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

Gather the Necessary WWPN Information

After the Cisco UCS service profiles have been created, each infrastructure blade in the environment will have a unique configuration. To proceed with the SAN-BOOT deployment, specific information must be gathered from each Cisco UCS blade and from the IBM controllers. Insert the required information into Table 18.

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 hit copy.

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

Table 18   WWPN's for Cisco VM-Hosts

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	

SAN Boot

This section details hw to add the host mappings for the host profiles created through Cisco 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 login with your superuser or admin account.

2. In the left pane click Host icon, which is the 5th icon down and click the Hosts menu item.

3. Click Create Host in the upper left menu to bring up the Create Host wizard.

4. Select the Fiber Channel Host option.

5. For Host Name input VM-Host-Infra-01.

6. For Fibre Channel Ports open the drop-down menu and select or input the WWPN's for the A path vHBA's, <<var_wwpn_VM-Host-infra-01-a>>, and click Add Port to List.

7. 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.

8. Leave Advanced Settings as default and click Create Host,

9. Click Close.

✎

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

10. Click Create Host to create the 2nd host.

11. Select the Fiber Channel Host option.

12. For Host Name input VM-Host-Infra-02.

13. 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.

14. Then select the B port by selecting the var for the B path, <<wwpn_VM-Host-infra-02-b>>, and click add port to list.

15. Leave Advanced Settings as default and click Create Host.

16. Click Close.

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

18. Right-click the volume VM-Host-Infra-01 and select Map to Host.
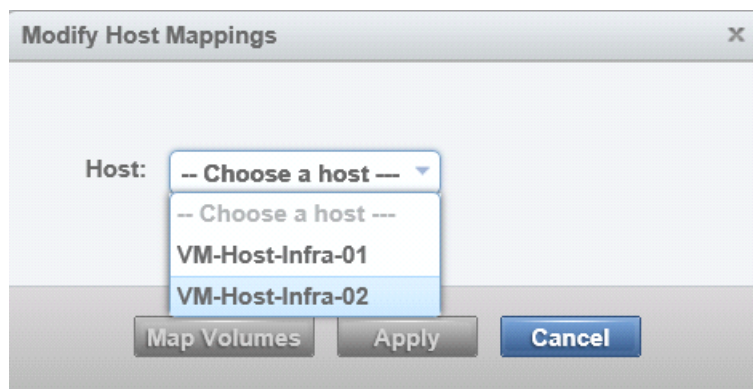
19. In the drop-down, select VM-Host-Infra-01.
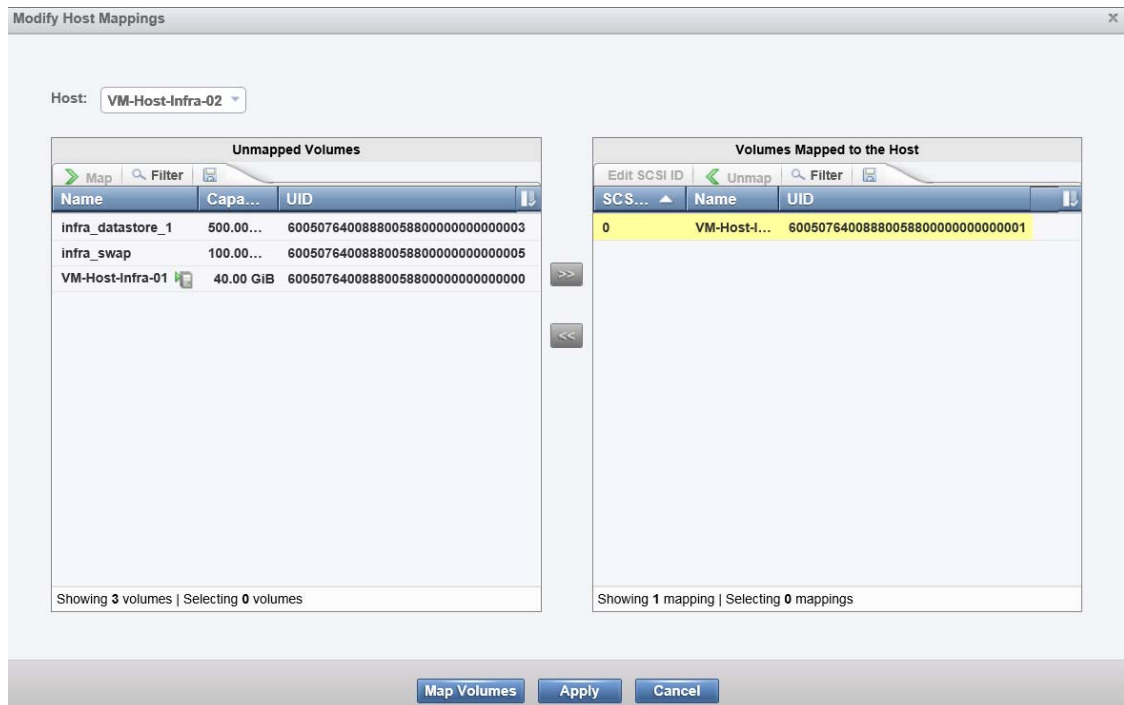

20. Select Map Volumes, then click Close.

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

22. Select Map Volumes, then click Close.

VersaStack VMware ESXi 5.5 Update 2 SAN Boot Install

This section provides detailed instructions for installing VMware ESXi 5.5 Update 2 in a VersaStack environment. After the procedures are completed, two San-booted ESXi hosts will be provisioned. These deployment procedures are customized to include the environment variables.

Note 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 U2 GA ISO file which is downloaded from the below URL. 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-ESXI55U2-CISCO&productId=353

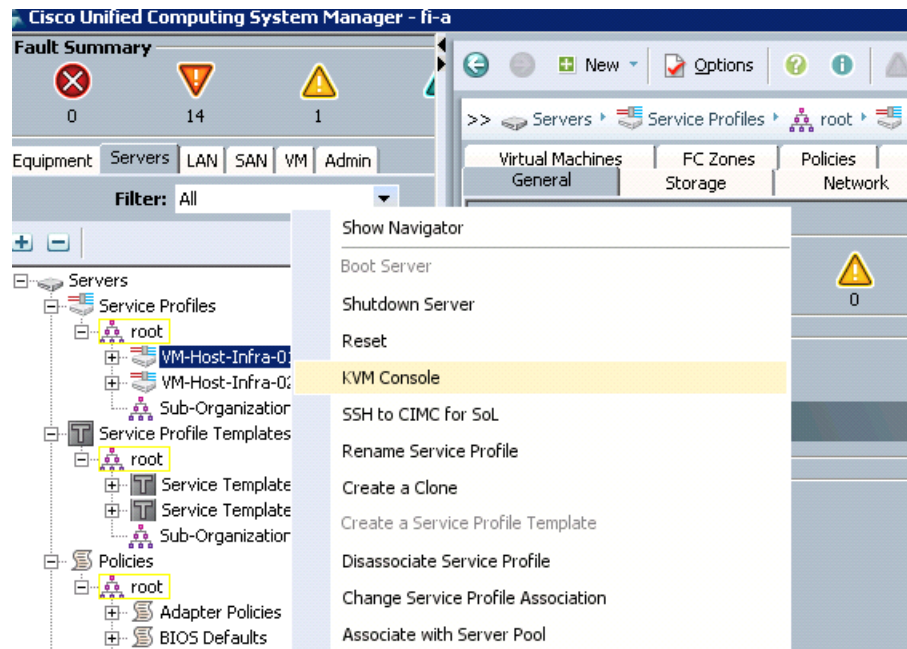## Log in to Cisco UCS 6200 Fabric Interconnect

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.

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.

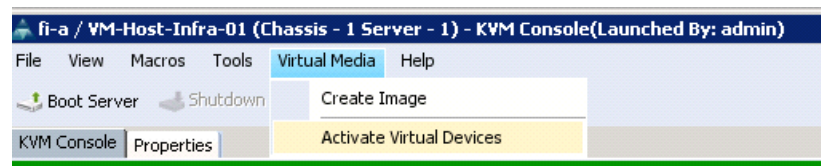8. Right-click VM-Host-Infra-02 and select KVM Console Actions > KVM Console.

Set Up VMware ESXi Installation

ESXi Hosts VM-Host-Infra-01 and VM-Host-Infra-02
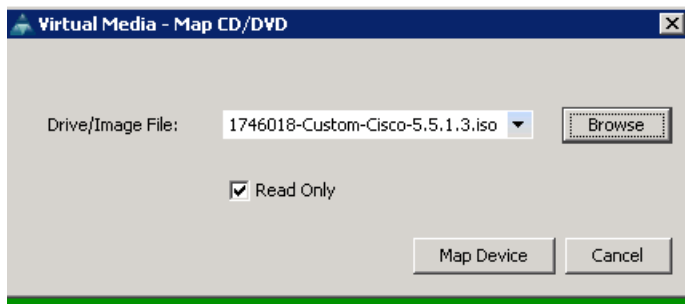
To prepare the server for the OS installation, complete the following steps on each ESXi host:

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.

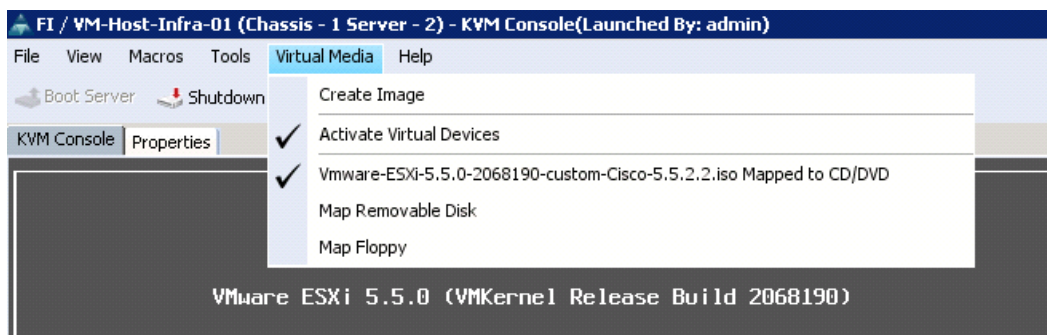4. Select the Map Device to map the newly added image.

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 window, press Enter to reboot the server.

Set Up Management Networking for ESXi Hosts

Adding a management network for each VMware host is necessary for managing the host. To add a management network for the VMware hosts, 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.

> **Note** 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.

Note   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.

> **Note** These applications are downloaded from the VMware website and Internet access is required on the management workstation.

Log in to VMware ESXi Hosts Using VMware vSphere Client

ESXi Host VM-Host-Infra-01

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

1. Open the recently downloaded VMware vSphere Client and enter the IP address of VM-Host-Infra-01 as the host you are trying to connect to: <<var_vm_host_infra_01_ip>>.

2. Enter root for the user name.

3. Enter the root password.

4. Click Login to connect.

5. ESXi Host VM-Host-Infra-02

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

7. 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>>.

8. Enter root for the user name.

9. Enter the root password.

10. Click Login to connect.

Set Up VMkernel Ports and Virtual Switch

ESXi Host VM-Host-Infra-01

Note 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.

Note 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, and then click Close.

Map Required VMFS Datastores

✎

Note   This section uses the VMFS datastores. If adding the IBM File Module, you can later migrate data to NFS datastores.

Map the VMFS datastores to the first host.

✎

Note   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 Datastores area, click rescan all, then click ok
5. From the Datastores area, click Add Storage to open the Add Storage wizard.
6. Select Disk/Lun and click Next.
7. Select the 500GB Datastore lun and click Next
8. Accept default VMFS setting and click Next
9. Click Next for the disk layout
10. Enter infra_datastore_1 as the datastore name.
11. Click Next to retain maximum available space
12. Click Finish.
13. Click Add Storage to open the Add Storage wizard.
14. Select Disk/Lun and click Next.
15. Select the 100GB swap lun and click Next.
16. Accept the default VMFS setting and click Next.
17. Click Next for the disk layout.
18. Enter infra_swap as the datastore name.
19. Click Next to retain maximum available space.
20. 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.

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

VersaStack VMware vCenter 5.5 Update 2

The procedures in the following subsections provide detailed instructions for installing VMware vCenter 5.5 Update 2 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 2, 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 section "Build Windows Active Directory Server VM(s)" in 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.

Note   This process requires several reboots.

46. Add the VM to the Windows AD domain.

Note   A reboot is required.

47. If necessary, activate Windows.

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

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.

5. Click Next.

6. Click Install.

7. Click Close.

8. 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.

15. 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.

✎

Note   The Windows firewall issue was addressed in the prior 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.

29. Keep Default Instance selected. Click Next.

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.

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]
go
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
go
use VCDB
go
sp_addlogin @loginame=[vpxuser], @passwd=N'<Password>', @defdb='VCDB',
@deflanguage='us_english'
go
ALTER LOGIN [vpxuser] WITH CHECK_POLICY = OFF
go
CREATE USER [vpxuser] for LOGIN [vpxuser]
go
use MSDB
go
CREATE USER [vpxuser] for LOGIN [vpxuser]
go
use VCDB
go
sp_addrolemember @rolename = 'db_owner', @membername = 'vpxuser'
go
use MSDB
go
sp_addrolemember @rolename = 'db_owner', @membername = 'vpxuser'
go
```

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:

1. Using the instructions for building a SQL Server VM provided in the section "Build Microsoft SQL Server VM," 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.

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.

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.

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

16. Click Finish.

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

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.

Note   A restart might be required.

Install VMware vCenter Server

vCenter Server VM

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 2 (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.

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

10. Click Next on the Site screen.

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.

14. Enter yes for the SSL popup is displayed.

VMware vSphere Web Client

15:74:39:D8:54:B4:D0:3F:71:21:61:FE:44:ED:1F:62:84:7F:4F:A2

This is the SSL SHA1 fingerprint of the SSO Lookup Service leaf certificate.
To accept and continue, click Yes. Otherwise, click No.

Yes   No

15. Enter the license Key.

VMware vCenter Simple Install

License Key

Enter the license key.

License key:

If you do not enter a license key, vCenter Server will be installed in evaluation mode.

InstallShield

< Back   Next >   Cancel

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

17. Select VCDB and click Next.

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

19. Click Next. Read the warning message and then click OK (you will need to take separate action backup the SQL database).

20. Click Next to use the SYSTEM Account.

21. Click Next to accept the default ports.

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 click OK

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. Select the appropriate language and click OK.

4. In the vSphere ESXi Dump Collector Installation Wizard, click Next.

5. Click Next.

6. Accept the terms in the License Agreement and click Next.

7. Click Next to accept the default Destination Folders.

8. Click Next to accept a Standalone installation.

9. Click Next to accept the default ESXi Dump Collector Server Port (6500).

10. Select the VMware vCenter Server IP address from the drop-down menu. Click Next.

11. Click Install to complete the installation.

12. Click Finish.

13. Click Exit in the VMware vCenter Installer window.

14. Disconnect the VMware vCenter ISO from the vCenter VM.

15. Install all available Microsoft Windows updates by navigating to Start > All Programs > Windows Updates.

16. A restart might be required.

17. Back on the Management Workstation, open the VMware vSphere CLI command prompt.

18. Set each ESXi Host to coredump to the ESXi Dump Collector by running the following commands:

Note Make sure to type these commands to be sure the hyphens are translated correctly (You can also do a find and replace with the hyphens in your text editor such as notepad).

```
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 check
esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>>
```

Set Up vCenter Server

vCenter Server VM

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

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.

6. Click Next.

7. Accept the defaults for vSphere DRS. Click Next.

8. Accept the defaults for Power Management. Click Next.

9. Accept the defaults for vSphere HA. Click Next.

10. Accept the defaults for Virtual Machine Options. Click Next.

11. Accept the defaults for VM Monitoring. Click Next.

12. Accept the defaults for VMware EVC. Click Next.

IMPORTANT: If mixing UCS B or C-Series 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.

13. Select "Store the swapfile in the datastore specified by the host". Click Next.

14. Click Finish.

15. Right-click the newly created VersaStack_Management cluster and select Add Host.

16. 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.

17. Click Yes.

18. Click Next.

19. Select Assign a New License Key to the Host. Click Enter Key and enter a vSphere license key. Click OK, and then click Next.

20. Click Next.

21. Click Next.

22. Click Finish. VM-Host-Infra-01 is added to the cluster.

23. 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.

10. Click OK.

Note   A warning displays stating that there is no network management redundancy if there is only one physical adapter assigned to vSwitch0. The optional Cisco 1000v virtual switch shown later is this document will resolve 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. Click the configuration tab and in the hardware pane, click Networking then click properties of vSwitch0. In the Network adapters tab, click Add and select the unclaimed adapter vmnic1, then click Next, then click Next again, and then clickFinish.

Move VM Swap File Location

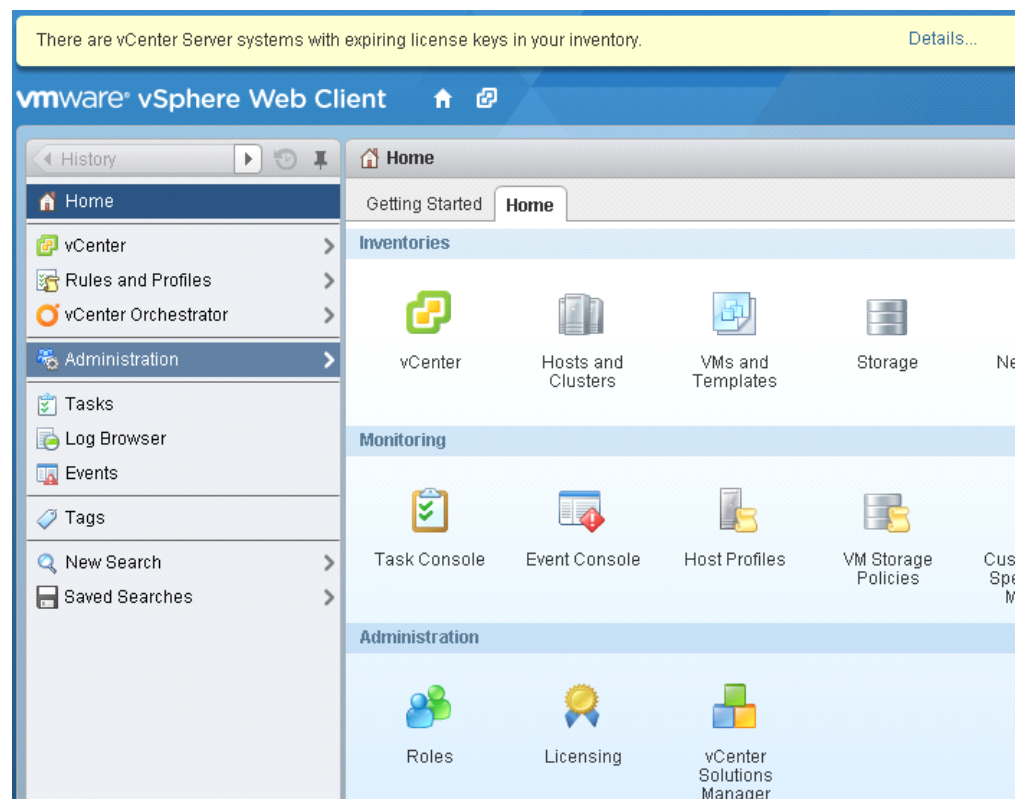### ESXi Hosts VM-Host-Infra-01 and VM-Host-Infra-02

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

This section details how to add a user to provide admin and login permissions in the vSphere Web client and also using VSphere client

1. Open a browser to the vSphere web client https://<<vSphere_ip>>:9443/vsphere-client/

2. Log in as administrator@vsphere.local with the admin password.
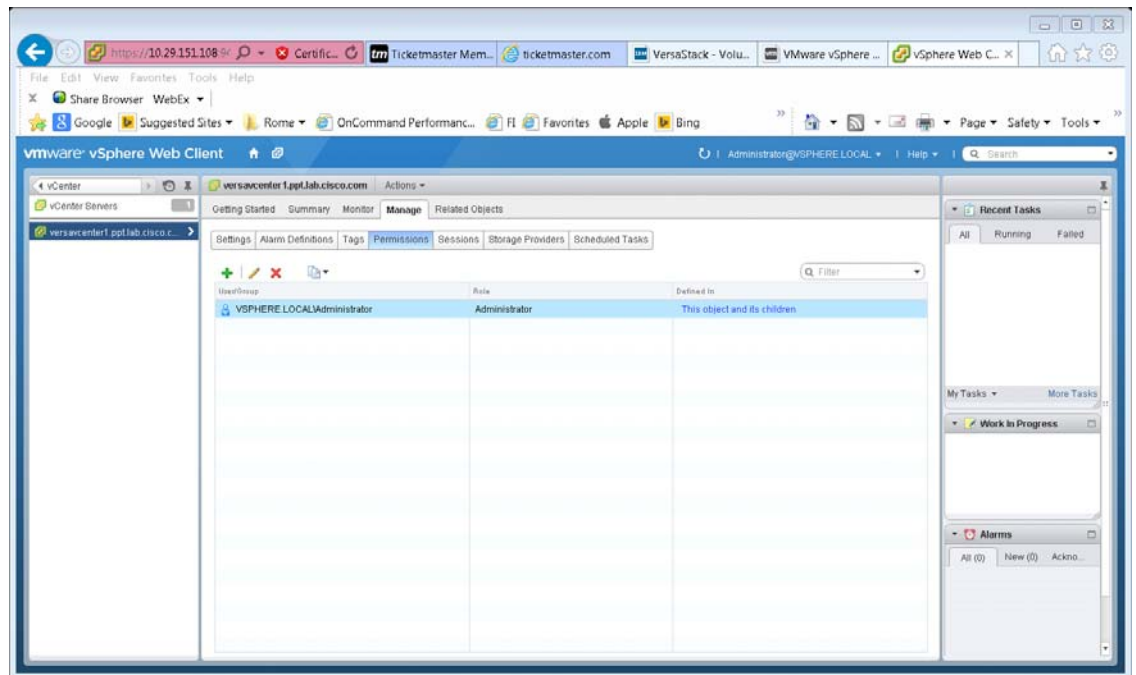
3. Click the Administration item in the left pane

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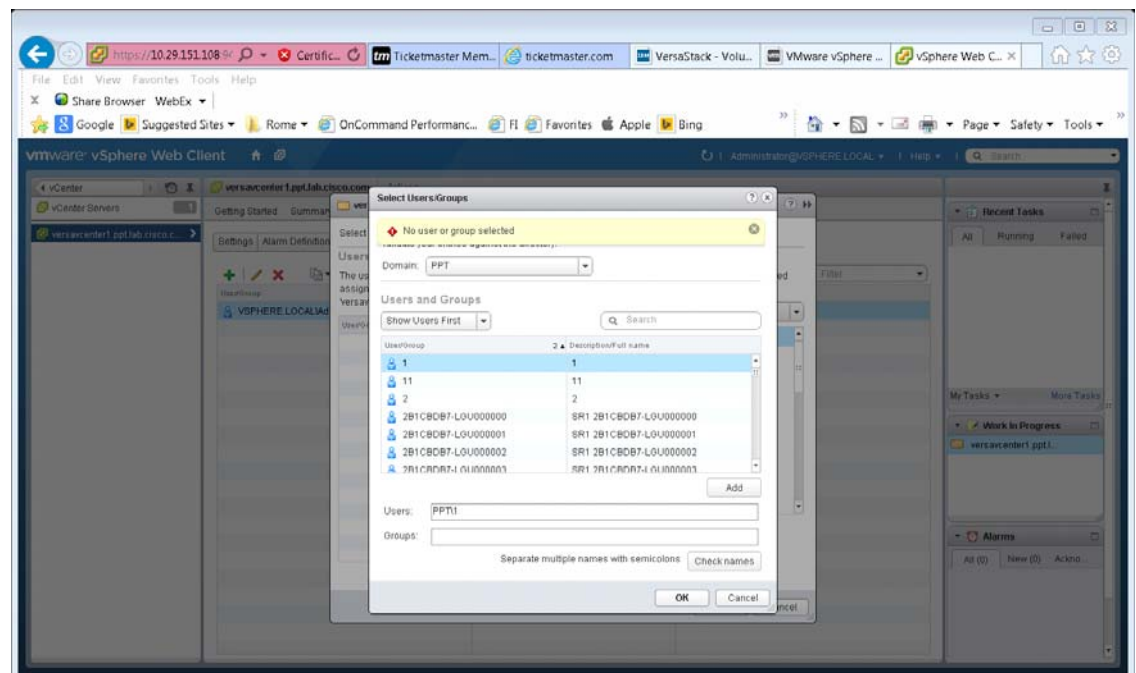

5. Select the home button in the top left.

6. Click vCenter to show the vCenter screen.

7. Click vCenter Servers under Inventory list.

8. Click the vCenter server name in the left pane, and click the Manage Tab in the right pane.
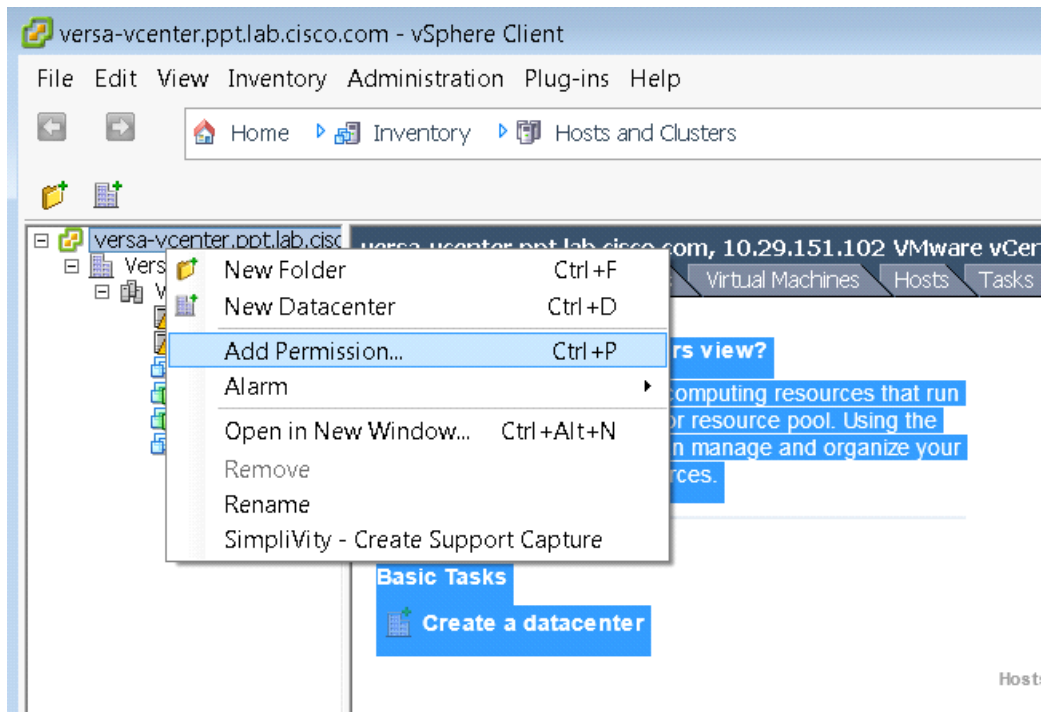
9. Click Permissions.

10. Click the green + sign to add a user. Select Add in the Add Permission Window. Choose the domain, and highlight the user.
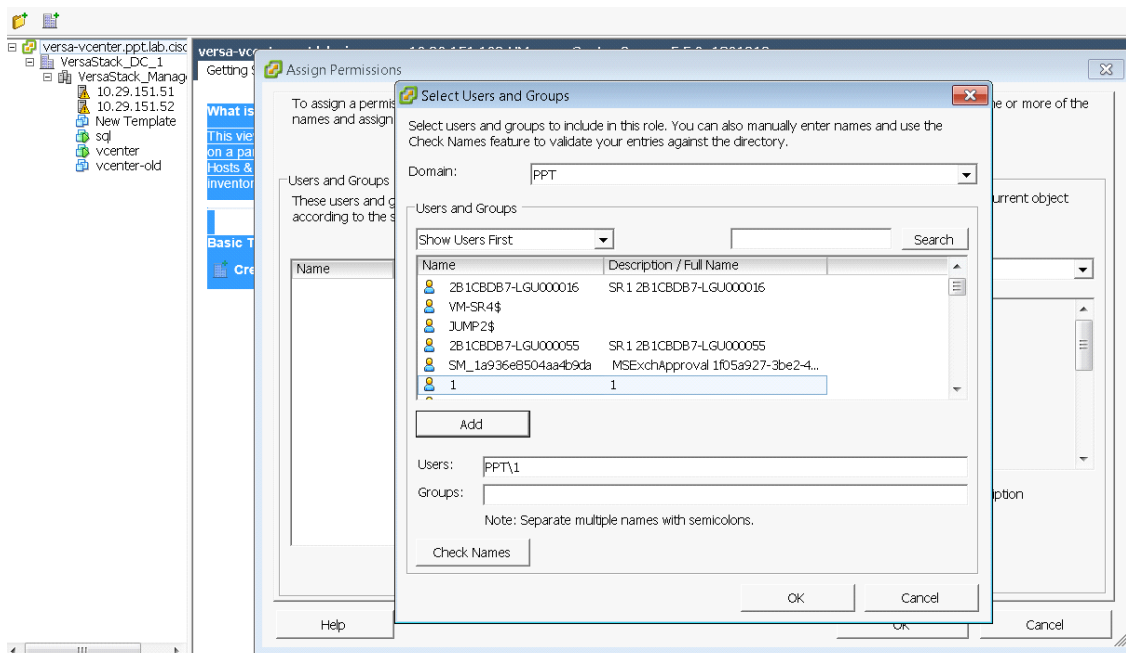
11. Click Add then click OK.

12. For assigned roll, choose administrator then click OK. You may now login as that user in your vSphere web client.
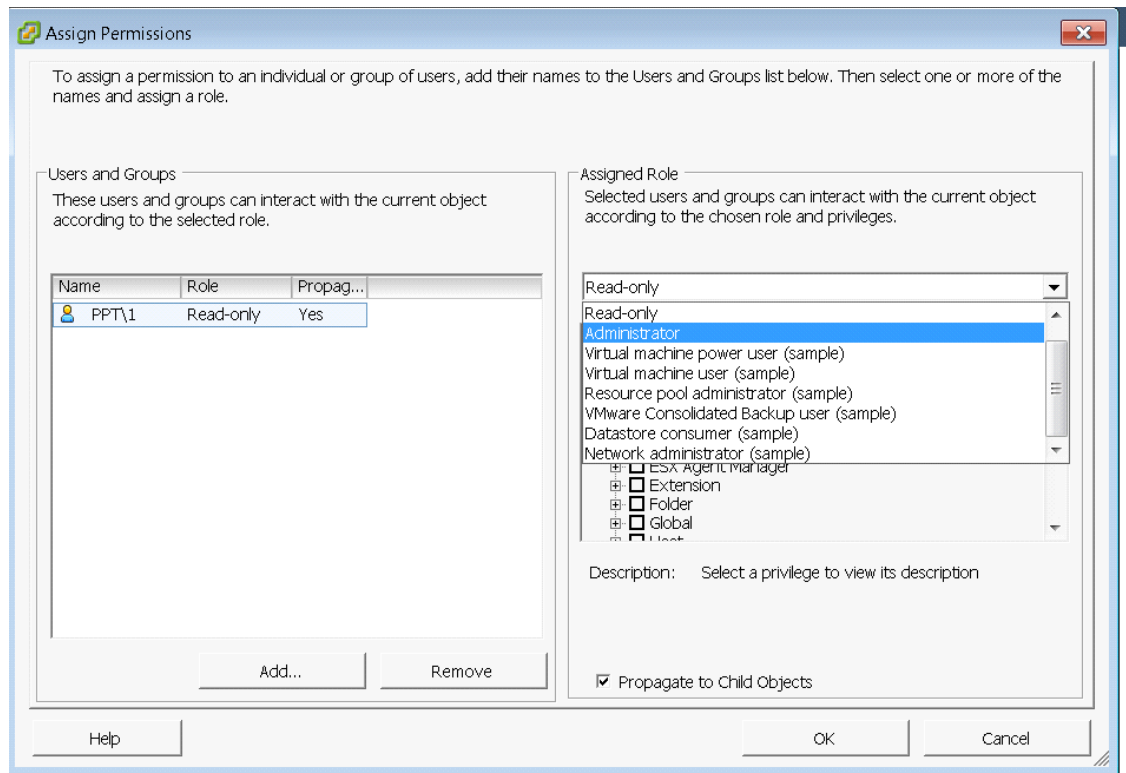
13. Open the vSphere Client application, log in as the administrator account and right click the vCenter name in the top left and Click Add Permissions.

14. Select Add.

15. Select the proper domain in the drop-down.

16. Highlight a user and click Add, then click OK.

17. Change the Assigned Role to Administrator in the drop-down, and Click Ok. You may now log off as administrator and back in as that domain user in the vSphere Client.

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 NFS Datastores. This section is not used unless you purchased the optional IBM Storwize V7000 file modules. The File Modules should be powered on before proceeding.

Initialization of the IBM Storwize V7000 file modules

Note   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

Fix Central provides fixes and updates for your system's software, hardware, and operating system. Not looking for fixes or updates? Please visit Passport Advantage to download most purchased software products, or My Entitled Systems Support to download system software.

For additional information, click on the following link.
➥ Getting started with Fix Central

| Find product | Select product |

Type the product name to access a list of product choices.

When using the keyboard to navigate the page, use the **Tab** or **down arrow** keys to navigate the results list.

Product selector*

| IBM Storwize V7000 Unified | ❯

Release*

| All ▾ |

Platform*

| All ▾ |

[Continue]

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

    d. Enter your system details and follow instructions to download the utility.

Note The required system information can be obtained by login in the IBM web client, and from the monitoring icon in the left pane, click system details menu item, expanding your VersaStack components tree, and click the cluster enclosure.

    2. 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
```

    3. 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.
```

    4. Run stopemail

```
stopemail
```

    5. Use the CLI to run the up2nas utility, which will check that the V7000 control enclosure is connected to the file modules through direct fibrechannel 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=7.3.0.9
    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)
```
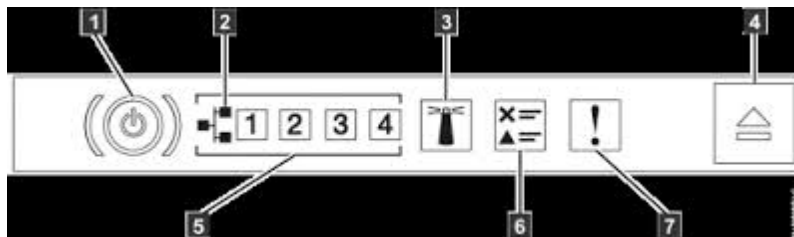
6. For the "Do you have the IP addresses", type y. The address for the V7000 cluster should be shown.

```
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 ?
```

7. 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)
```

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

9. Type y and press Enter.

10. Locate the USB flash drive that came packaged with the file modules, then type y and hit enter.

✎

Note   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
```
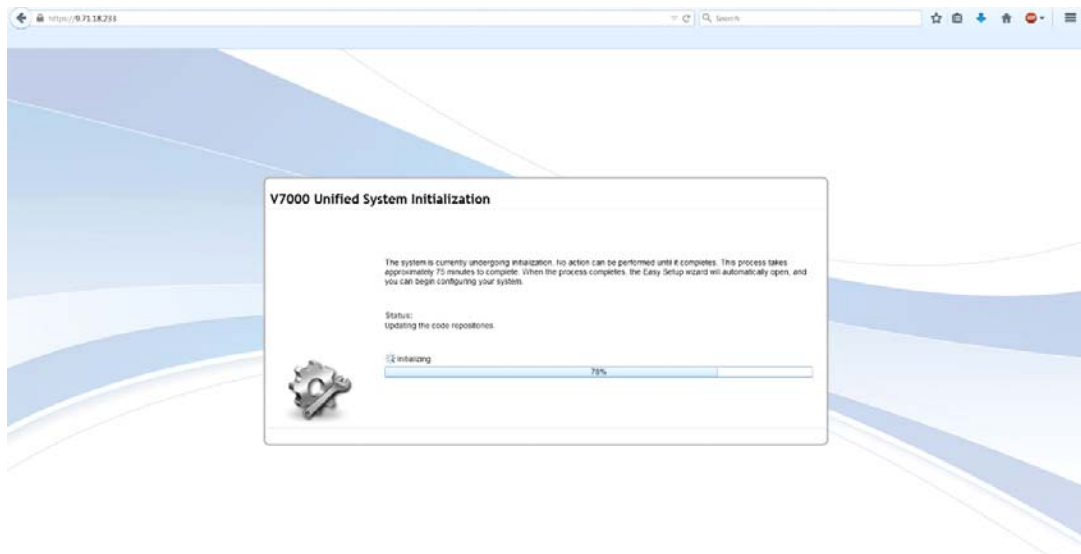
11. Check the rear of the V7000 control enclosure, and you should see the amber fault LED blinking on the left-hand canister.

12. Follow the instruction to insert the USB flash drive into a USB port on the canister with the blinking amber LED,

13. Wait for the amber LED to stop blinking and go out. This will take up to 60 seconds, or approximately 40 blinks. When the amber LED stops blinking, type y and hit 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
```

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

15. Follow the instruction to insert the USB flash drive into a USB port in the upper file module.

16. Wait for the blue identify LED on the upper file module to stop blinking, and go out. This can take up to 3 minutes. The blue identify LED on the lower file module should continue to blink a further 3 or 4 times, then go out.

```
#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.
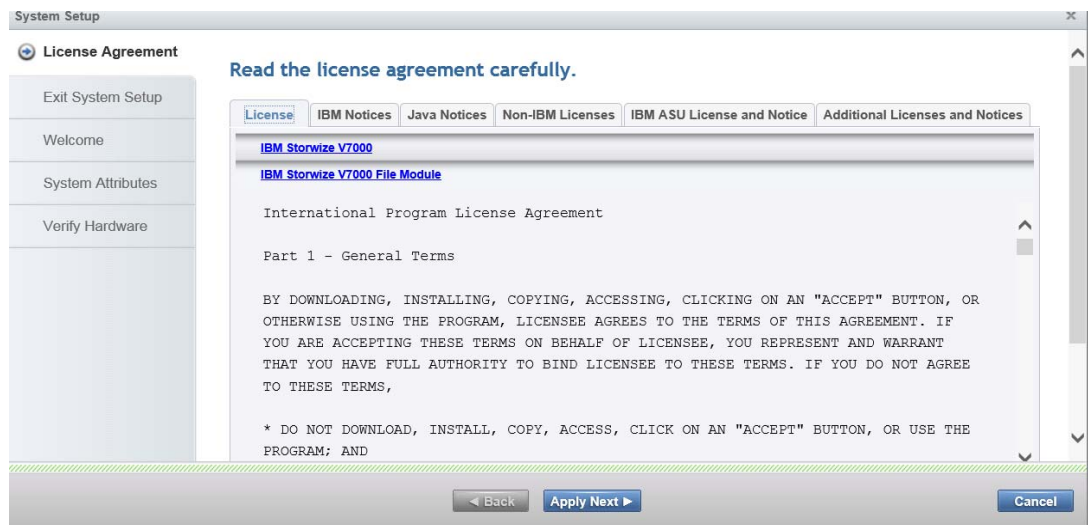```

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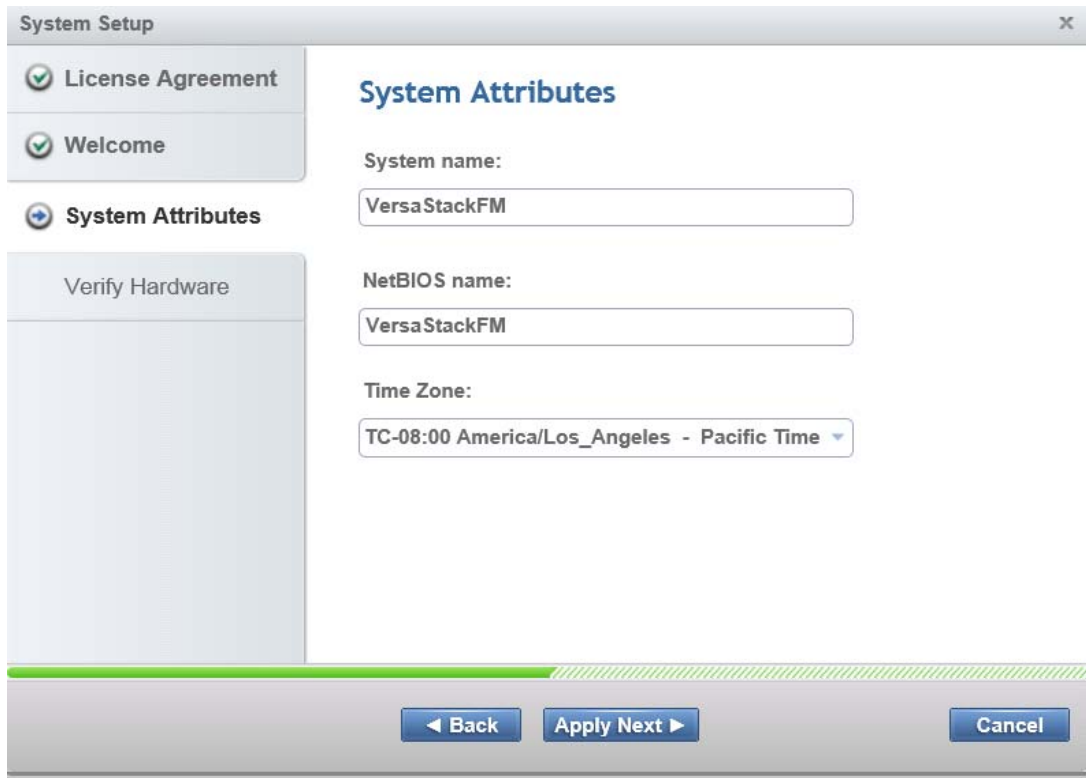
**18.** When initialization is complete, the management GUI login page will load. Login using the admin account with password admin0001.
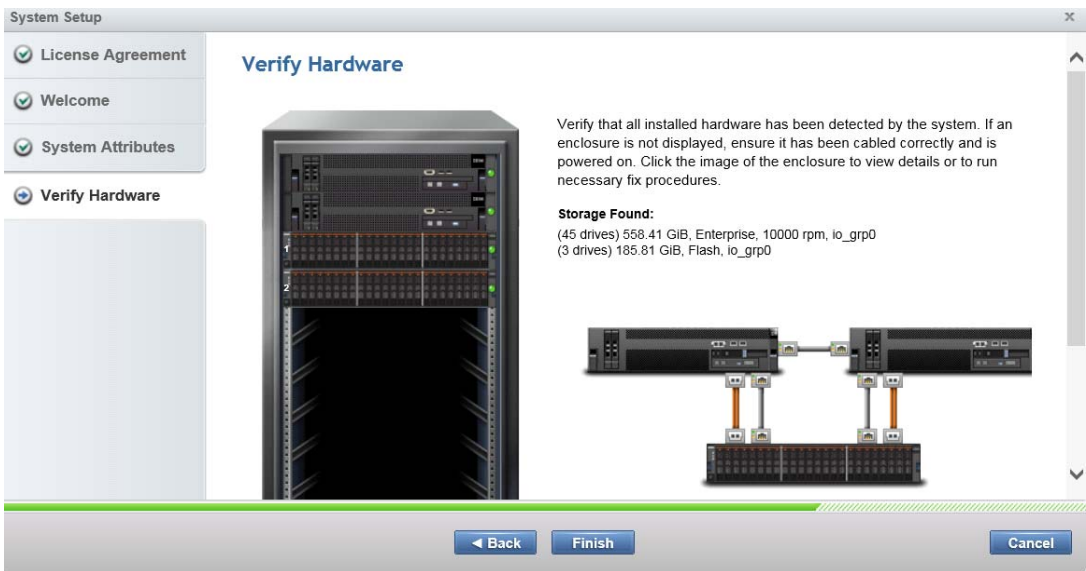


**19.** Review the license agreement, scroll to the bottom and click I agree and click Apply Next, then click Close.



**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.
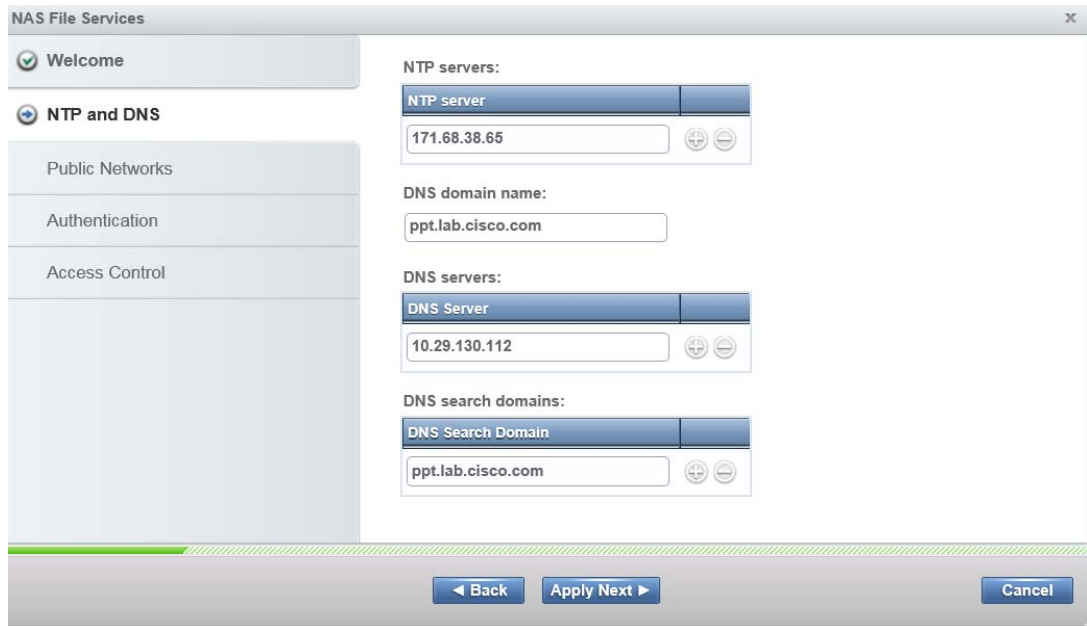


23. Click Close.

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



25. Click Next on the Welcome screen .

26. On the NTP and DNS  screen enter the <<var_global_ntp_server_ip>> <<var_dns_domain_name>> <<var_nameserver_ip>>,  add any search domains and click Apply Next, then click Close.

27. Click create Network to bring up the Network Screen.

28. On the Network screen, input values for your NFS network. <<var_unified_bond_ip_network>> <<var_unified _bond_ip_Netmask>> <<var_nfs_vlan_id>> <<var_unified_bond_ip_gateway>> <<var_unified_bond_public_ip>> . The IP address field is the address of the subnet, example 172.17.72.0 and the Public Network IP is the actual network IP you will mount from vSphere, example 172.17.72.41.

29. Select the 10gig card for the interface (ethX1).

30. Click OK, then click Close, then click Next.

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

**31.** Select the authentication method of Active Directory then click Next.



**32.** Input the Domain Controller IP, Domain Admin username and login. Do not include the domain name when specifying the User ID. Click Next.
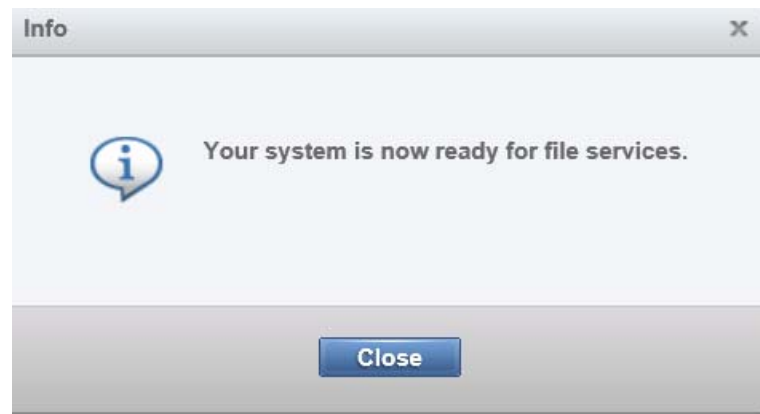
33. For the Kerberos screen accept the default and Click Next.

34. For ID Mapping Method accept the default of Master and click Next.

35. For the ID Mapping Role screen accept the default and click Next.

36. For the Automatic ID Mapping screen accept the default and click Next.

37. For the Netgroups for NFS screen accept the default and click Apply Next , then click Close.



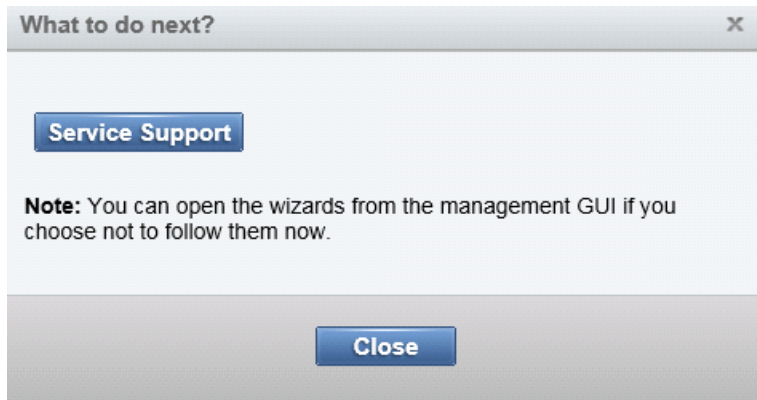38. Select the primary Sharing Method as NFS and click Next.

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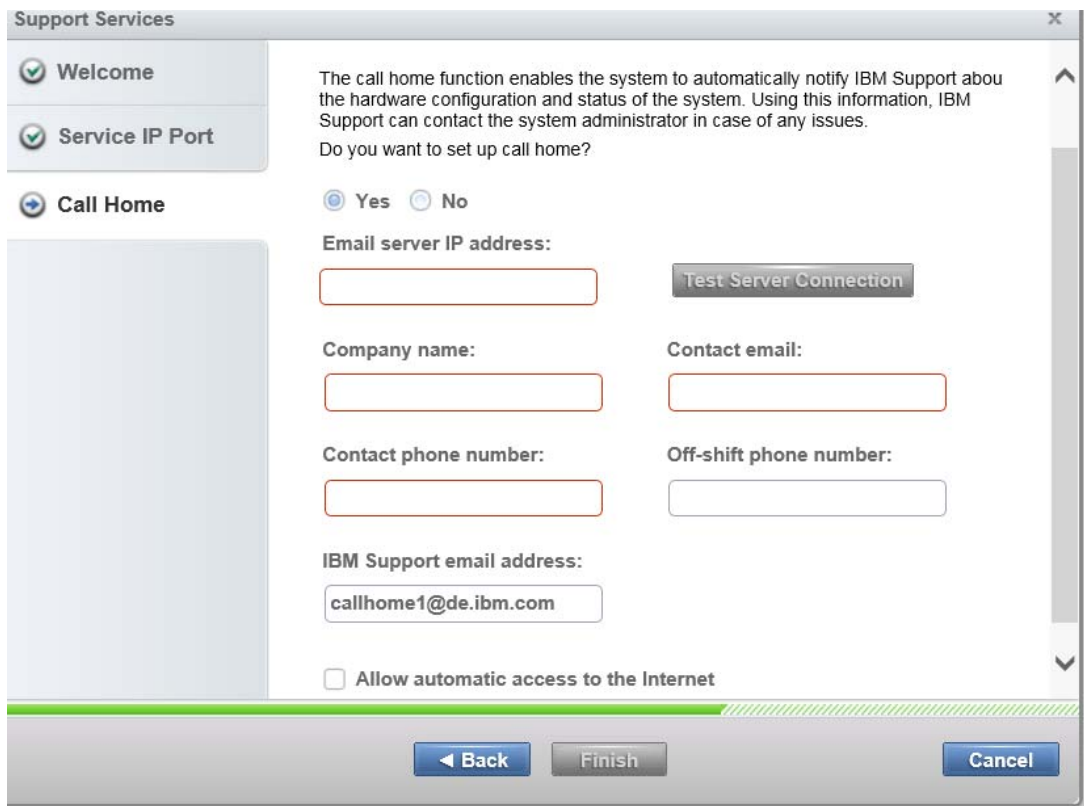


**40.** On the "What to do Next?" screen, click Service Support.

**41.** Click Next on the Welcome Screen.

42. For the Service IP Port screen click Nex.t

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



44. Click Finish then click Close.

45. Click Close again to complete a wizard. This will initialize a reboot.

# 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 the bottom left icon for settings, Network in the menu, then click NAS Public Networks.

**2.** Right-click the interface and click delete, then Yes, then clcik Close.



**3.** Open a putty session and login to the IP address of the file module as admin with password of admin0001.

**4.** Run "lsnwinterface -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 (1)
UP      1000             1500
```

```
mgmt001st001 ethXsl0_0 e4:1f:13:d6:0d:88 SUBORDINATE
UP      1000            1500
mgmt001st001 ethXsl0_1 e4:1f:13:d6:0d:88 SUBORDINATE
UP      1000            1500
mgmt001st001 ethX1   00:00:c9:bb:af:06 MASTER      active-backup (1)
UP      10000           1500
mgmt001st001 ethXsl1_0 00:00:c9:bb:af:06 SUBORDINATE
UP      10000           1500
mgmt001st001 ethXsl1_1 00:00:c9:bb:af:06 SUBORDINATE
UP      10000           1500
mgmt002st001 ethX0   e4:1f:13:d5:f3:e0 MASTER      active-backup (1)
UP      1000            1500
mgmt002st001 ethXsl0_0 e4:1f:13:d5:f3:e0 SUBORDINATE
UP      1000            1500
mgmt002st001 ethXsl0_1 e4:1f:13:d5:f3:e0 SUBORDINATE
UP      1000            1500
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
UP      10000           1500
mgmt002st001 ethXsl1_1 00:00:c9:bb:ae:ce SUBORDINATE
UP      10000           1500
EFSSG1000I The command completed successfully.
```

5. Remove the 10 gig bond. In this example, 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 "lsnwinterface -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
UP      10000           1500
mgmt001st001 eth1     00:00:c9:bb:af:08
UP      10000           1500
mgmt001st001 ethX0   e4:1f:13:d6:0d:88 MASTER      active-backup (1)
UP      1000            1500
mgmt001st001 ethXsl0_0 e4:1f:13:d6:0d:88 SUBORDINATE
UP      1000            1500
mgmt001st001 ethXsl0_1 e4:1f:13:d6:0d:88 SUBORDINATE
UP      1000            1500
mgmt002st001 ethX0   e4:1f:13:d5:f3:e0 MASTER      active-backup (1)
UP      1000            1500
mgmt002st001 ethXsl0_0 e4:1f:13:d5:f3:e0 SUBORDINATE
UP      1000            1500
mgmt002st001 ethXsl0_1 e4:1f:13:d5:f3:e0 SUBORDINATE
UP      1000            1500
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
UP      10000           1500
mgmt002st001 ethXsl1_1 00:00:c9:bb:ae:ce SUBORDINATE
UP      10000           1500
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 "lsnwinterface -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 (1)
UP       1000            1500
mgmt001st001 ethXsl0_0 e4:1f:13:d6:0d:88 SUBORDINATE
UP       1000            1500
mgmt001st001 ethXsl0_1 e4:1f:13:d6:0d:88 SUBORDINATE
UP       1000            1500
mgmt001st001 ethX1     00:00:c9:bb:af:06 MASTER               802.3ad (4)
layer3+4            UP      20000             9000
mgmt001st001 ethXsl1_0 00:00:c9:bb:af:06 SUBORDINATE
UP       10000           9000
mgmt001st001 ethXsl1_1 00:00:c9:bb:af:06 SUBORDINATE
UP       10000           9000
mgmt002st001 ethX0    e4:1f:13:d5:f3:e0 MASTER       active-backup (1)
UP       1000            1500
mgmt002st001 ethXsl0_0 e4:1f:13:d5:f3:e0 SUBORDINATE
UP       1000            1500
mgmt002st001 ethXsl0_1 e4:1f:13:d5:f3:e0 SUBORDINATE
UP       1000            1500
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
UP       10000           1500
mgmt002st001 ethXsl1_1 00:00:c9:bb:ae:ce SUBORDINATE
UP       10000           1500
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.
```

10. 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 (1)
UP       1000            1500
mgmt001st001 ethXsl0_0 e4:1f:13:d6:0d:88 SUBORDINATE
UP       1000            1500
```

```
mgmt001st001 ethXsl0_1 e4:1f:13:d6:0d:88 SUBORDINATE
UP      1000            1500
mgmt001st001 ethX1     00:00:c9:bb:af:06 MASTER           802.3ad (4)
layer3+4              UP     20000          9000
mgmt001st001 ethXsl1_0 00:00:c9:bb:af:06 SUBORDINATE
UP      10000           9000
mgmt001st001 ethXsl1_1 00:00:c9:bb:af:06 SUBORDINATE
UP      10000           9000
mgmt002st001 eth0     00:00:c9:bb:ae:ce
UP      10000           1500
mgmt002st001 eth1     00:00:c9:bb:ae:d0
UP      10000           1500
mgmt002st001 ethX0    e4:1f:13:d5:f3:e0 MASTER        active-backup (1)
UP      1000            1500
mgmt002st001 ethXsl0_0 e4:1f:13:d5:f3:e0 SUBORDINATE
UP      1000            1500
mgmt002st001 ethXsl0_1 e4:1f:13:d5:f3:e0 SUBORDINATE
UP      1000            1500
EFSSG1000I The command completed successfully.
```

11. 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 clicking opening the file module management console by clicking the Settings in the left tab, click Network in the menu, and clicking NAS Public Networks.

13. Click Create Network.

14. 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 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. Click OK.

15. Click Close.

16. Repeat this process to create any additional required networks.

Configuring the Cisco Nexus Switch Networking

In this section we will be creating 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 Po11
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>>,
```

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 9216
```

6. 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 Po11
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
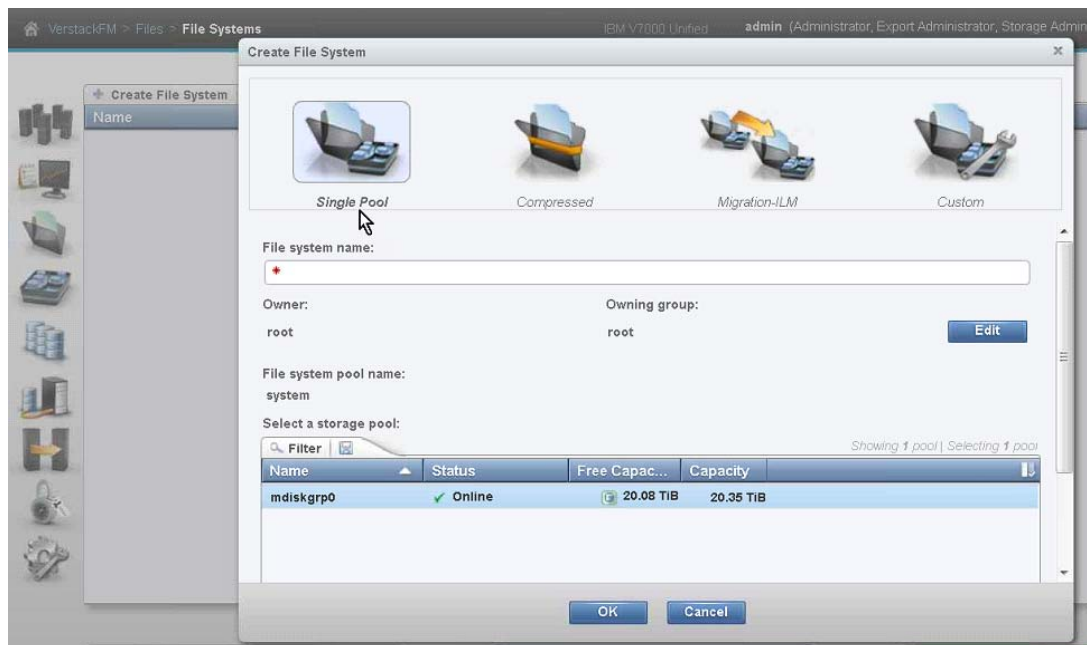
   ```
   interface Eth1/2
   description <<var_filemodule_name>>-A
   ```
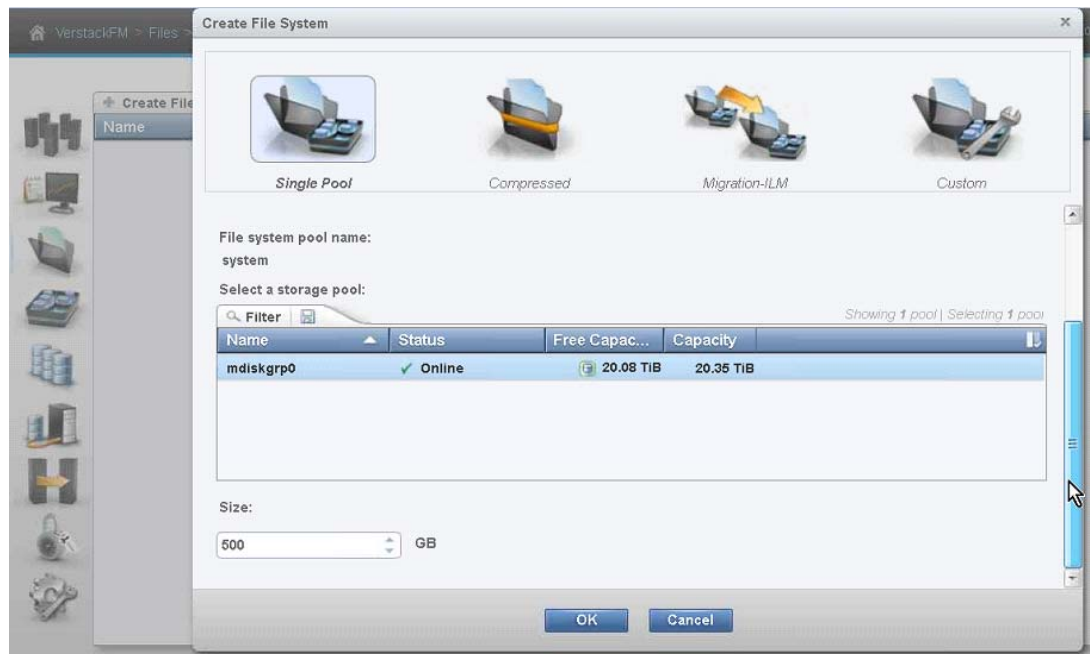
15. Apply it to a port channel and bring up the interface.

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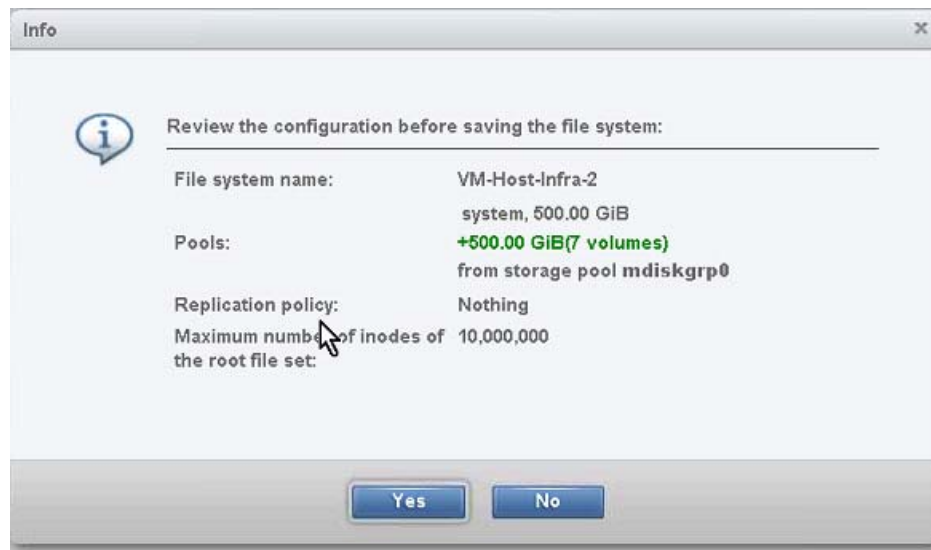   ```

# Creating a NAS Datastore and Export

1. Open the Storwize File Module management console and select Files in the left Menu, then File Systems.
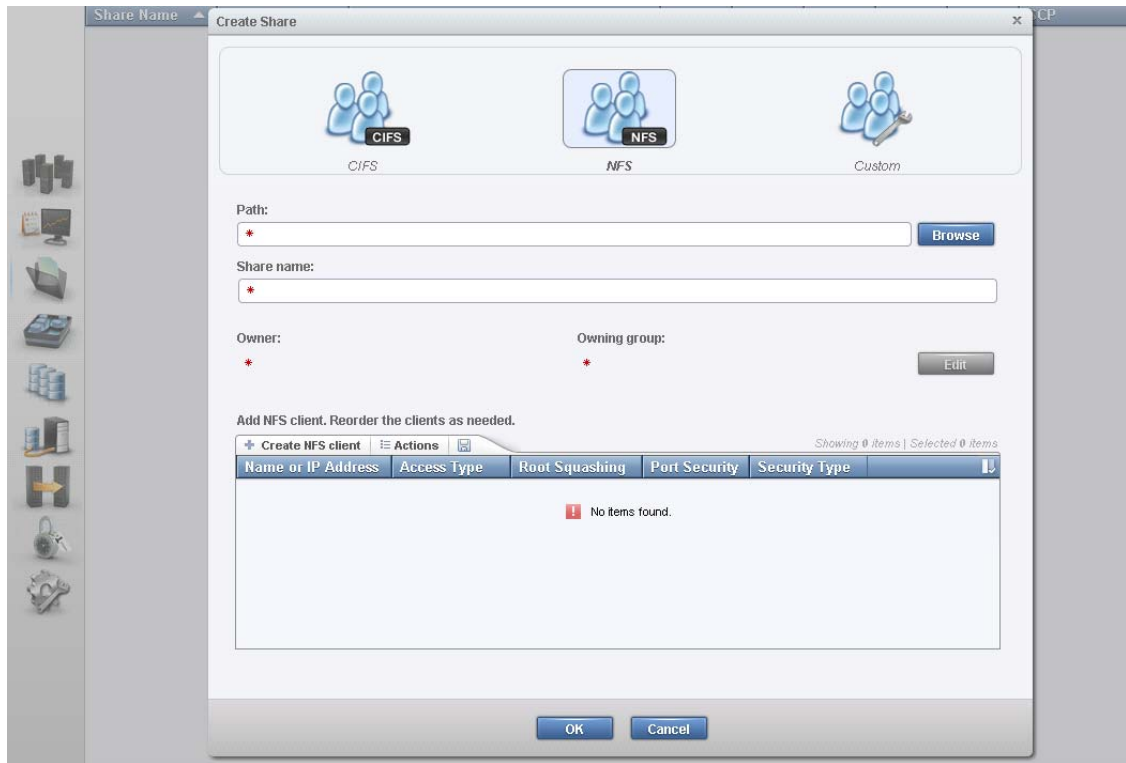


2. Click Create File Systems.

3. 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.
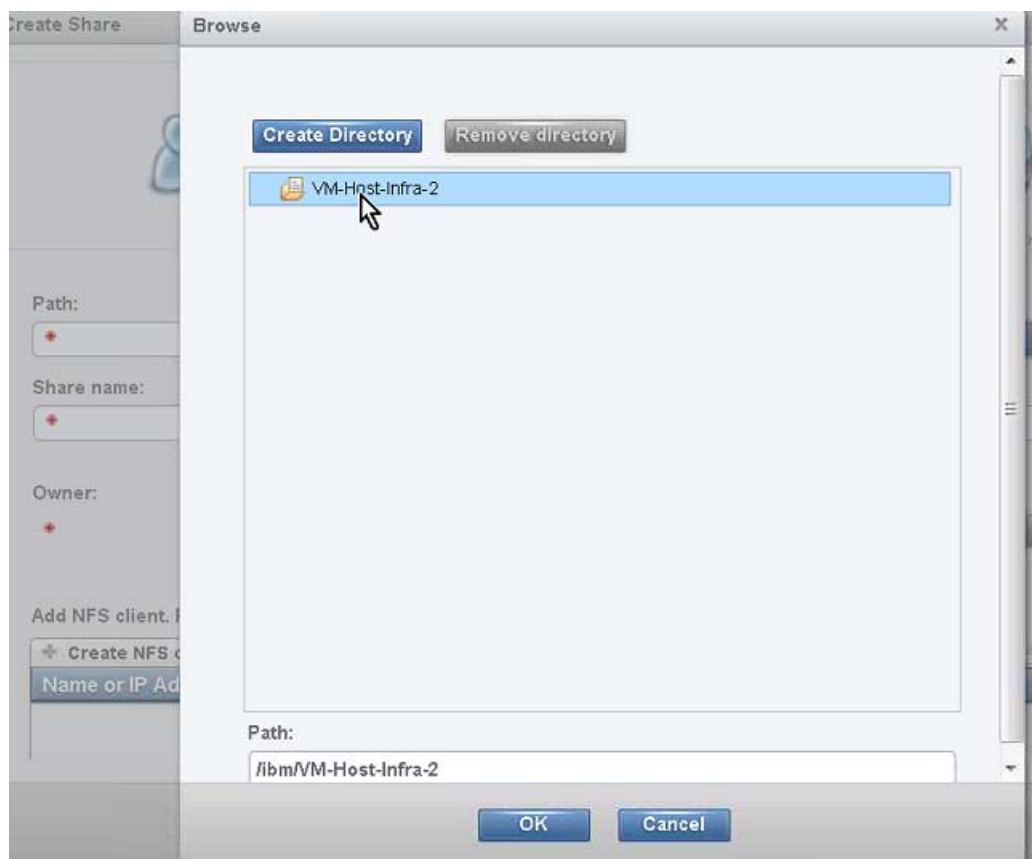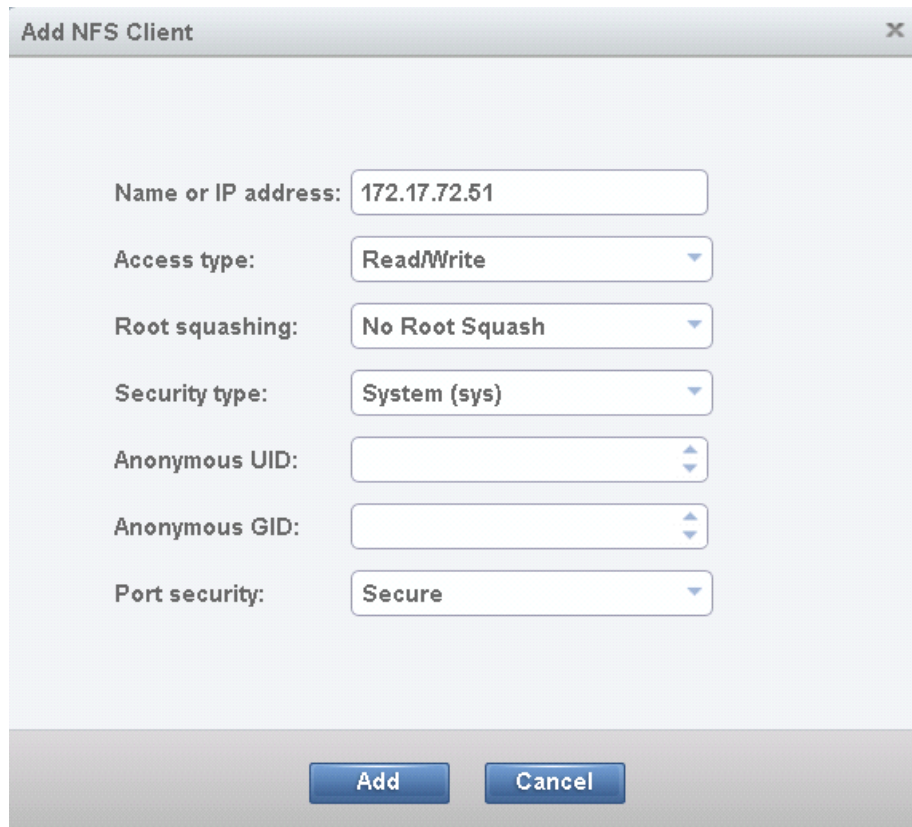
4. Click OK, then click Yes.



5. Click Close when the operation completes.

6. Click the Files icon in the left menu bar and then click Shares.

7. Click Create Share.

8. Click NFS for Share type in the center of the screen then click browse to select the directory, then click OK.

9. Enter the share name, and if required edit the owner and owning group.

10. Click Create NFS clien.t

11. Input the NFS-Vlan VMkernel IP for Host ESX host 1 , <<var_nfs_vlan_id_ip_host-01>> for the Name or IP address.

12. Change the Access Type to Read/Write.

13. Change the Root squashing to No Root Squash.

14. Click Add.

15. Click Create NFS client.

16. Input the NFS-Vlan VMkernel IP for Host ESX host 2 <<var_nfs_vlan_id_ip_host-02>>for the IP address.

17. Change the Access Type to Read/Write.

18. Change the Root squashing to No Root Squash.

19. Click Add.

20. Repeat  Create NFS client for any additional ESX hosts.

21. Click OK to create the share. Click Close.

# Mounting the NAS Datastore on ESX

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 Storage from the Hardware menu

3. Click Add Storage.

**4.** Select Network File System and click Next.



**5.** Input  <<var_unified _bond_public_ip>>for the server name, the share path for the folder, and <<var_unified_datastore_name>> for Datastore Name.

**6.** Click Next, then click Finish.

✏️

**Note**  You can list NFS share paths by opening a putty session to the file module management IP and typing in the command. "lsexport".



7.  Select ESX Node 2, VM-Host-infra-2, click the Configuration tab, and then click Storage in the Hardware menu.

8.  Click Add Storage.

9.  Select Network File System and click Next.

Add Storage

Locate Network File System
Which shared folder will be used as a vSphere datastore?
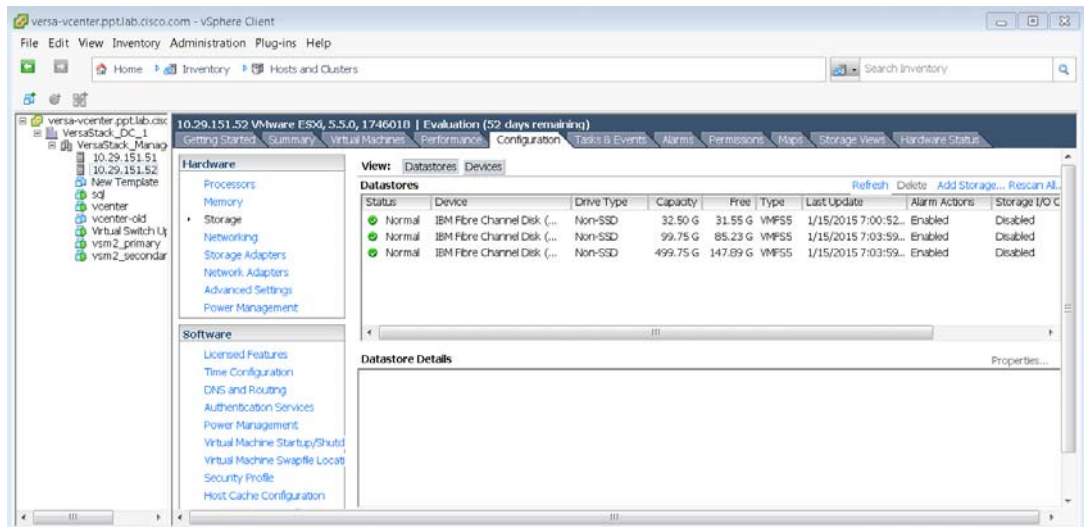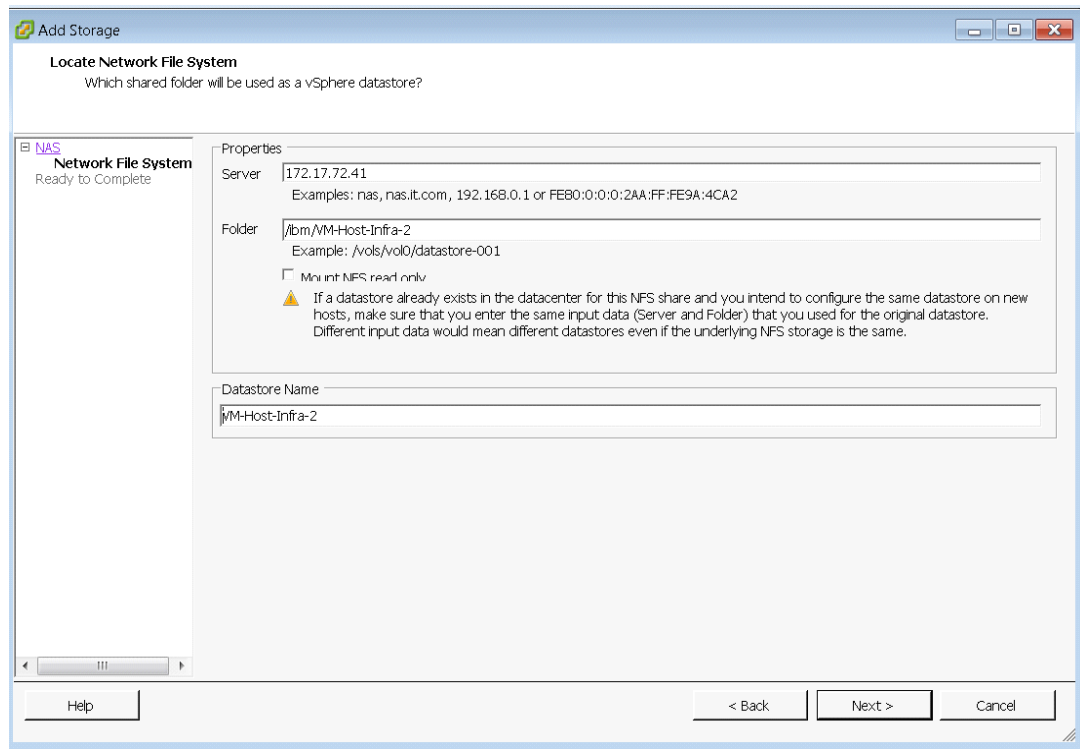
NAS
Network File System
Ready to Complete

Properties

Server  172.17.72.41
Examples: nas, nas.it.com, 192.168.0.1 or FE80:0:0:0:2AA:FF:FE9A:4CA2

Folder  /ibm/VM-Host-Infra-2
Example: /vols/vol0/datastore-001

☐ Mount NFS read only

⚠ 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
VM-Host-Infra-2

Help                                           < Back    Next >    Cancel

✎

**Note**    It is recommended that you also create and map a separate Swap file Datastore for VM's.

✎

**Note**    Optionally, you can use vMotion to migrate servers from you VMFS datastores to your 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).
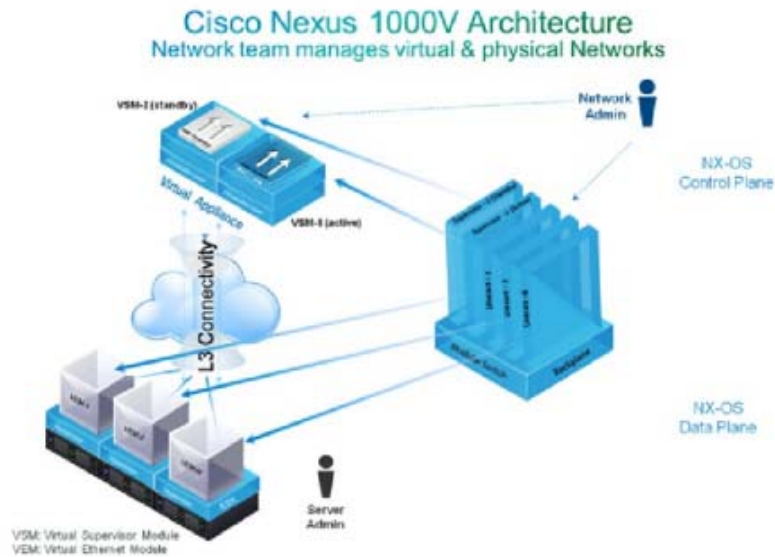
The Cisco Nexus 1000V has the following components:

- 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.

*Figure 7    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.

# Installation Steps

To create management network redundancy prior to the migration, we will create a temporary VMkernel for each ESX host.

## ESXi Host VM-Host-Infra-01 (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 for vSwitch0.
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 N1kv Virtual Switch Update Manager

1. Log in and Download the N1kv installation software from www.cisco.com.



2. Unzip the package.

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

4.  Click next, then click Next.

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 the IB-Mgmt Network and click Next.

11. On the properties Screen for Network properties  input <<var_vsm_updatemgr_mgmt_ip>> <<var_vsm_mgmt_mask>> <<var_vsm_mgmt_gateway>> <<var_nameserver_ip>> .

12. For the vCenter properties portion, enter the vCenter IP address and login information. For Username accounts, use the Admistrator@vSphere.local login format and do not use domainname\user account format.

13. Accept default ports and click Next

**14.** Review the summary screen.

**15.** Click Finish.

**16.** After the VM is created. Power on the virtual machine.

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

## Install the VSM Through the Cisco Virtual Switch Update Manager

✎

**Note** 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 vSphere web client. The plug-in can be downloaded from the lower left corner of the web client login page.

1. Launch the vSphere Web client interface https://<<Vshpere_host_ip>>:9443/vsphere-client and log in.

2. Select the home tab and click Cisco Virtual Switch Update Manager.



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

**4.** Click the VersaStack datacenter in the right screen.

**5.** Keep the default for deploy new VSM  and High Availability Pair.

**6.** Select IB-Mgmt for the Control and Management VLAN.

**7.** For the Host Selection, click the Suggest button and choose the Datastores.



**8.** Enter a domain ID for the Switch Configuration section.

9.  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>>.

10. Click Finish.

**Note**  You can launch a second VSphere Client to help monitor the progress by clicking tasks in the left pane on the home screen. The process will take a few minutes to complete.

## 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 l3control
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
```

Migrate Networking Components for ESXi Hosts to Cisco Nexus 1000V

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.

3. Click the Datcenter, then click the Distributed Virtual Switch and select Manage.

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

5. Click the suggest button.

6. Scroll down and select the Physical NIC Migration.

7. Expand each host and select the unused Nic vmnic1 for migration.

8. Deselect the vmnic0 for each host.

9. Select system uplink in the middle pane for the vmnic1 for each host.

10. Scroll down and for the VM Kernel Nic Setup, expand each host, and deselect vmk3 which is the temporary management kernel we created for this migration.

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

12. Click Finish.

13. When the migration completes, click the settings then topology and expand the virtual machines to view the network connections.

Remove Networking Standard Switch Components for ESXi Hosts

In this section we will remove the temporary management networks we created for the migration. We will remove the unused standard switch components, and also assign the second physical nic to the vSphere Distributed Switch.

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 Properties.

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

6. Click Close.

7. Validate you still are focused on the VSphere Standard Switch and click Remove to remove VSwitch0.

8. Click Yes to the warning popup.

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

10. Click Manage Physical Adapters.

11. Scroll down to the system-uplink box and click Add NIC.

12. Choose vmnic0 and click OK, then click OK again.

13. 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.

14. If there are warnings, right-click each node, and click Reconfigure for vSphere HA.

Remove the Redundancy for the NIC in Cisco UCS Manager

While creating the ESXi vNIC template settings, the default was to enable failover on the vNic. Once you have deployed the N1kV that setting is no longer needed and should be disabled. If you did not enable failover in Cisco UCS Manager, you can skip these steps.

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 click Yes, then click OK.

5. Repeat these steps for vNic_Template_B

Note   A reboot of the ESXi hosts is required for this change.

For more information about the 1000v switch, including how to update the software after installation, please visit this 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 of IBM backup and disaster recovery solutions, go to:
http://www-03.ibm.com/systems/storage/solutions/backup-and-disaster-recovery/

Bill of Materials

Table 19   Bill of Materials for IBM Storwize V7000

Part Number	Product Description	Quantity Required
IBM Storwize V7000 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 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 20   Bill of Material for Cisco Nexus 9300 Series Switch

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

Table 21   Bill of Materials for Cisco UCS Blade Servers and Chassis

Part Number	Product Description	Quantity Required
Cisco UCS Unified Compute 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-VIC-M83-8P	Cisco UCS VIC 1380 mezzanine adapter for blade servers	4

UCSB-MLOM-40G-03	Cisco UCS VIC 1340 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 22   Bill of Materials for Cisco Fabric Interconnect

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 23   Bill 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

Table 24   *Bill of Materials for Cisco Rack-Mount 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   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.

Note A reboot is required.

45. If necessary, activate Windows.

46. Download and install all required Windows updates.

Note 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.

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.

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

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

60. Select the appropriate forest functional level and click Next.

61. Keep DNS server selected and click Next.

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 9396A
vdc 9396A 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$3EBiF6qi$5rsOBsKixsV1msqzXg11E.  role network-admin
no password strength-check
ssh key rsa 2048
ip domain-lookup
copp profile strict
snmp-server user admin network-admin auth md5 0x20244f474f767e6333c873e98d13609f
 priv 0x20244f474f767e6333c873e98d13609f 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

spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
spanning-tree port type network default
vrf context management
  ip route 0.0.0.0/0 10.29.151.1
```

```
vpc domain 10
  peer-switch
  role priority 10
  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 3171-3175
  spanning-tree port type network
  vpc peer-link

interface port-channel11
  description filemodule-A
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3171-3175
  spanning-tree port type edge trunk
  mtu 9216
  vpc 11

interface port-channel12
  description filemodule-B
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3171-3175
  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 FI-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 filemodule-A
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3171-3175
  mtu 9216
  channel-group 11 mode active

interface Ethernet1/2
  description filemodule-B
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3171-3175
  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
  description FI-A:1/25
  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
  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 b:1/47
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3171-3175
  channel-group 10 mode active

interface Ethernet1/48
  description VPC Peer b:1/48
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3171-3175
  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 9396B
```

```
vdc 9396B 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 $1$lFTCi98T$wua3eFR8FVuFibbVMjuGI0  role network-admin
no password strength-check
ssh key rsa 2048
ip domain-lookup
copp profile strict
snmp-server user admin network-admin auth md5 0x351fcf3cdf5b6e138a61a8a442ffafc6
 priv 0x351fcf3cdf5b6e138a61a8a442ffafc6 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

spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
spanning-tree port type network default
vrf context management
  ip route 0.0.0.0/0 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
  ip arp synchronize
```

```
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 filemodule-a
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3171-3175
  spanning-tree port type edge trunk
  mtu 9216
  vpc 11

interface port-channel12
  description filemodules-b
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3171-3175
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12

interface port-channel13
  description FI-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 FI-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 filemodule-b
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3171-3175
```

```
    mtu 9216
    channel-group 12 mode active

interface Ethernet1/2
  description filemodule-a
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 3171-3175
  mtu 9216
  channel-group 11 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
  description FI-B:1/25
  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 partner: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 partner: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 10.29.151.15/24
line console
line vty
boot nxos bootflash:/n9000-dk9.6.1.2.I3.1.bin
```
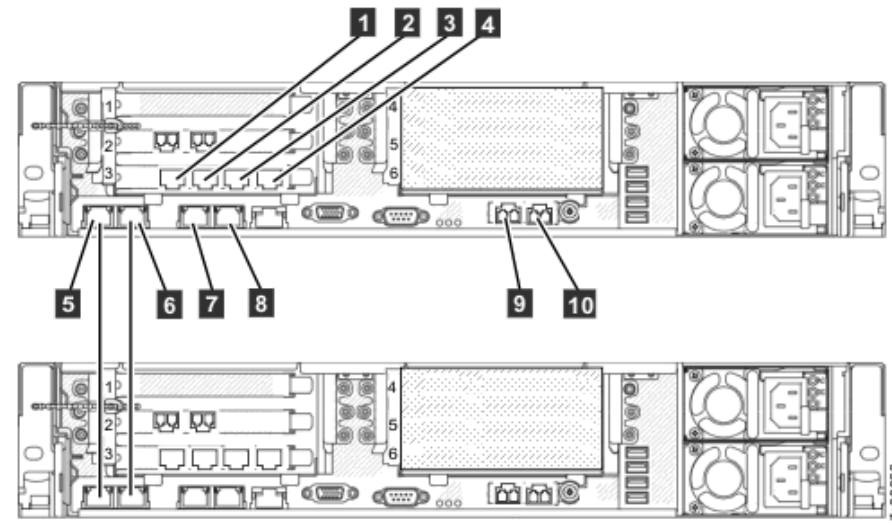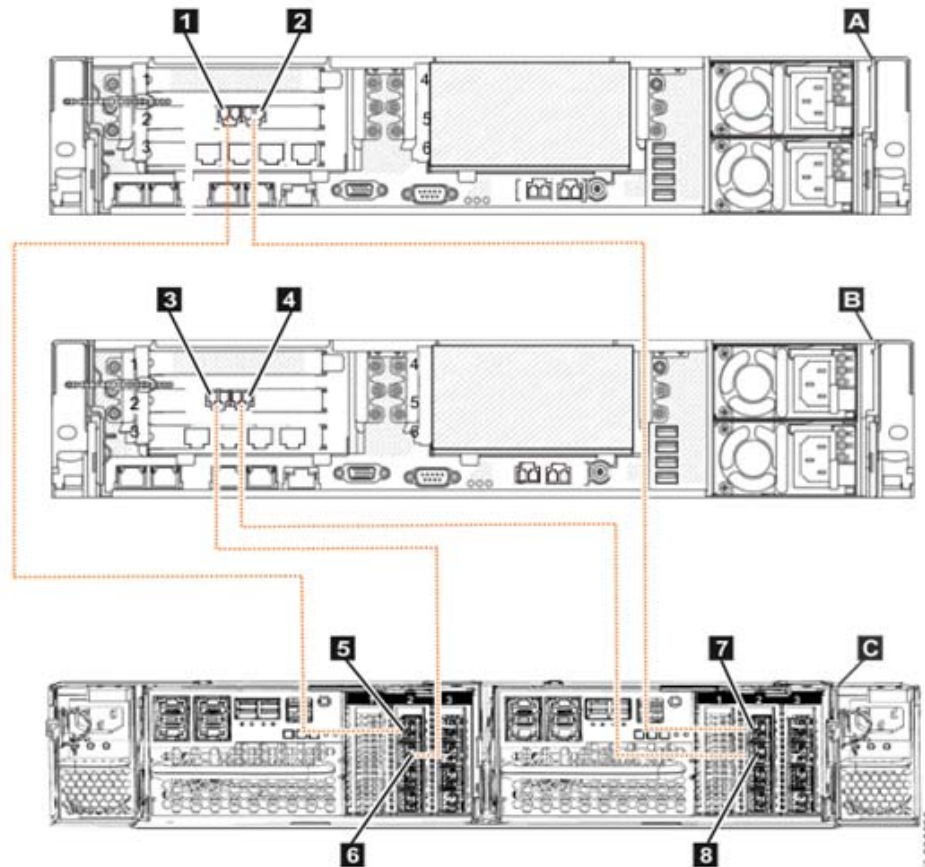
Additional IBM Storwize V7000 Control Enclosure and V7000 File Module Port information

Figure 8   *Ethernet port use on File Modules*

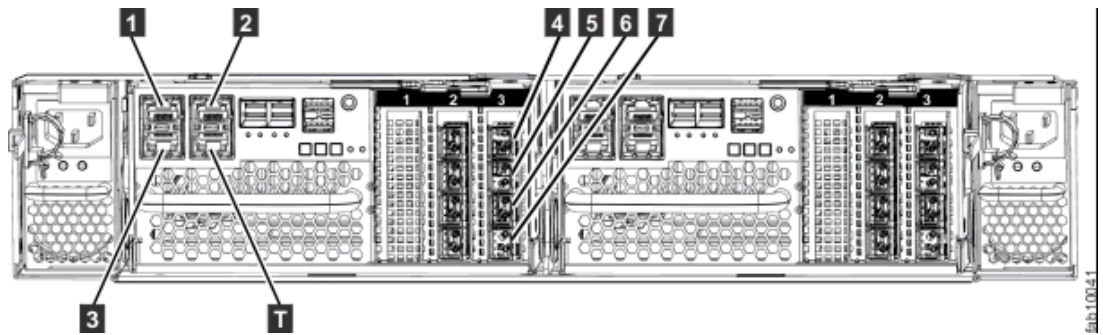| ID	Port	IP address is assigned by InitTool	Use
1	Ethernet port 7		Connect to a switch for public file access
2	Ethernet port 8		Connect to a switch for public file access
3	Ethernet port 9		Connect to a switch for public file access
4	Ethernet port 10		Connect to a switch for public file access
5	Ethernet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

Figure 9   *IBM Storwize V7000 File Module Ports*

Key

- A A - File module 1

- B B - File module 2

- C C - Storwize V7000 Gen2 control enclosure (2076-524)

- 1 1 - File module 1 - Fibre Channel port 1

- 2 2 - File module 1 - Fibre Channel port 2

- 3 3 - File module 2 - Fibre Channel port 1

- 4 4 - File module 2 - Fibre Channel port 2

- 5 5 - Node canister 1 (left) - Fibre Channel port 1

- 6 6 - Node canister 1 (left) - Fibre Channel port 2

- 7 7 - Node canister 2 (right) - Fibre Channel port 1

- 8 8 - Node canister 2 (right) - Fibre Channel port 2

Figure 10   *IBM Storwize V7000 Control Enclosure Ports*

Key

- 1, 2: 1GbE management, iSCSI and IP replication ports

- 3: 1GbE iSCSI and IP replication port

- 4-7: 8GbE fibrechannel ports