

# FlexPod Validated with Microsoft Private Cloud

### Reference Architecture and Deployment Guide for Microsoft Windows Server 2008 R2 and Microsoft System Center 2007

February 2012







### **Table of Contents**

FlexPod Validated with Microsoft Private Cloud	1
Overview	7
Benefits of Cisco Unified Computing System	7
Benefits of Cisco Nexus 5548UP	8
Benefits of NetApp FAS Family of Storage Controllers	8
Benefits of Microsoft Private Cloud Solution	9
Audience	10
Architecture	10
Software Revisions	12
Configuration Guidelines	13
Deployment	11
Cabling Information	14
NetApp FAS3240A Deployment Procedure: Part 1	20
Assign Controller Disk Ownership	
Set up Data ONTAP 8.0.2	21
Install Data ONTAP to Onboard Flash Storage	24
Harden Storage System Logins and Security	24
Install Required Licenses	24
Configure Native FC ports as FC Targets adapters	25
Enable Active-Active Controller Configuration Between Two Storage Systems	25
Start FCP	25
Start iSCSI	25
Set up Storage System NTP Time Synchronization and CDP enablement	25
Create Data Aggregate aggr1	26
Create SNMP Requests Role and Assign SNMP Login Privileges	26
Create SNMP Management Group and Assign SNMP Request Role	26
Create SNMP User and Assign to SNMP Management Group	26
Set up SNMP v1 Communities on Storage Controllers	27
Set up SNMP Contact Information for each Storage Controller	27
Set SNMP Location Information for Each Storage Controller	27
Reinitialize SNMP on Storage Controllers	21
Add VLAN Interfaces	21
Add Infrastructure Volumes	20
Cisco Nexus 5548 Deployment Procedure: Part 1	29
Set up Initial Cisco Nexus 5548 Switch	29
Enable Appropriate Cisco Nexus Features	
Set Global Configurations	31
Configure FC Ports	33
Create Necessary VLANs	34
Add Individual Port Descriptions for Troubleshooting	35
Create Necessary PortChannels	36
Add PortChannel Configurations	38



Configure Virtual PortChannels	40
Link into Existing Network Infrastructure	41
Save the Configuration	41
Cisco Unified Computing System Deployment Procedure	
Perform Initial Setup of the Cisco UCS 6248 Fabric Interconnects	42
Log into Cisco UCS Manager	43
Add a Block of IP Addresses for KVM Access	43
Synchronize Cisco UCS to NTP	43
Configure Unified Ports	43
Edit the Chassis Discovery Policy	44
Enable Server and Uplink Ports	44
Acknowledge the Cisco UCS Chassis	46
Create Uplink PortChannels to the Cisco Nexus 5548 Switches	
Create an Organization	52
Create a MAC Address Pool	52
Create WWNN Pools	54
Create WWPN Pools	55
Create UUID Suffix Pools	57
Create Server Pools	59
Create VLANs	59
Create VSANs and SAN PortChannels	64
Create a FC Adapter Policy for NetApp Storage Arrays	66
Create a Firmware Management Package	67
Create Firmware Package Policy	69
Set Jumbo Frames and Enable Quality of Service in Cisco UCS Fabric	72
Create a Power Control Policy	75
Create a Local Disk Configuration Policy	77
Create a Server Pool Qualification Policy	79
Create a Server BIOS Policy	80
Create vNIC/HBA Placement Policy for Virtual Machine Infrastructure Hosts	82
Create a vNIC Template	83
Create vHBA Templates for Fabric A and B	96
Create Boot Policies	99
Creating Boot Policy for Fabric -B	104
Create Service Profile Templates	108
Create Service Profiles	130
Add a Block of IP Addresses for KVM Access	131
Synchronize Cisco UCS to NTP	131
Add More Server Blades to the FlexPod Unit	132
Gather Necessary Information	132
Cisco Nexus 5548 Deployment Procedure: Part 2	132
Create VSANs, Assign FC Ports, Turn on FC Ports	132
Create Device Aliases and Create Zones	134
NetApp FAS3240A Deployment Procedure: Part 2	136
Create iGroups	136
Create LUNs	136



Map LUNs to iGroup	
Prepare the Host for Windows Server 2008 R2 SP1 Installation	
Install Windows Server 2008 R2	
Configure MPIO	142
Install Microsoft Hotfixes	142
Create Zones for Redundant Paths	
Verify MultiPath I/O Connections (Both Hyper-V Hosts)	
Clone the Windows Server 2008 R2 SP1 Installation	
Configure Network Interfaces, Rename Servers, and Install Microsoft Windows U	pdates on Both
Hyper-V Hosts	
Install the Failover Cluster Feature	
Install NetApp MultiPath IO Tools on Both Hyper-V Hosts	
Verify MultiPath I/O Connections (Both Hyper-V Hosts)	
Verify MultiPath I/O Connections	153
Creating Microsoft Hyper-V Virtual Network Switches	154
VM-Date Hyper-V Network Switch	155
App-Cluster-Comm	156
iSCSI-Fabric-A	157
iSCSI-Fabric-B	158
Domain Controller Virtual Machine (optional)	158
Create VHD for Domain Controller Virtual Machine (Optional)	
Create Domain Controller Virtual Machine	
Install Windows in a Domain Controller Virtual Machine	
Install Active Directory Services	
Join Virtual Machine Host VM-Host-Infra-01 to a Windows Domain	
Join Virtual Machine Host VM-Host-Infra-02 to a Windows Domain	
Set Firewall Exceptions (Both Hyper-V Hosts)	
Configure Infrastructure Server Cluster	
Configure Cluster Network For CSV Network Traffic	
Create Virtual Machines and Resource for Denloving Infrastructure Roles	183
Create VHD for Infrastructure Roles	183
Create Infrastructure Virtual Machines	187
Domain Controller Virtual Machine (ontional)	187
Modify the Virtual Machine Settings	
Configure Virtual Processor Count	194
Configure Virtual LAN Identification	
Add iSCSI Fabric A Interface	
Add iSCSI Fabric B Interface	
Create Clustered Application or Service	
Configure Live Migration Network for the Virtual Machines	
Optional Optimization for CSV and Live Migration Networks	
Disable NetBios over TCP/IP for the CSV Network	212
Installing Highly Available Microsoft System Center Components	
Installing Clustered Microsoft SQL Server 2008	
Active Directory Preparation	214



Configure Windows Failover Cluster for the SQL Server	214
Set Firewall Exceptions	216
Enable Jumbo Frames for iSCSI NICs in SQL Cluster Virtual Machines	216
Configure SQL Server Cluster	217
Install SQL Server 2008 Cluster	220
Step 1: Installing SQL Server on Node 1	
Step 2: Adding Node 2 to SQL Server	
Step 3: Verify Cluster Operation	
Step 4: Add SQL Server Instance	
Step 5: Add Node 1 to SQL Server Cluster	
Step 6: Configure Remote Access	
Step 7: Verify Cluster Operation	227
System Center Operations Manager Installation	227
Installing System Center Operations Manager 2007 R2	
Step 1: Active Directory Preparation	
Step 2: Deploy Operations Manager Database	
Step 3: Install Windows Server 2008 R2 SP1 Enterprise in the SCOM Virtual Machine	
Step 4: Install Prerequisite Software	
Step 6: Install SQL Server Reporting Services	230
Step 5: Install Operations Manager	231
Step 6: Configure Web Console Security	232
Step 7: Provision Data Warehouse Database	
Step 8: Install Operation Manager Reporting	234
Configure Operations Manager	
Install System Center Virtual Machine Manager	
Step 1: Active Directory Preparation	
Step 2: Install Windows Server 2008 R2 SP1Enterprise in the SCVMM Virtual Machines	237
Step 3: Install Prerequisite Software	237
Enable Jumbo Frames for iSCSI NICs in SCVMM Virtual Machine	
NetApp SnapDrive 6.4	240
Step 4: Provision Storage	241
Step 5: Install System Center Virtual Machine Manager	242
Step 6: Install System Center Virtual Machine Manager Administrator Console	243
Step 7: Configure SCVMM	244
Step 8: Install the OnCommand Plugin 3.0 Rapid Provisioning cmdlets	244
Step 9: Installing the Virtual Machine Manager Self-Service Portal (Optional)	
Step 10: SCOM Administrative Console	
Configure SCVMM SCOM Integration	
Install OnCommand Plugin 3.0 for Microsoft SCOM	
Install Cisco UCS MP for Microsoft SCOM	
Assigning an IP Address to the Management Port	
Creating an Account for Administrators	
Adding an Account to a Profile	
Adjusting the Discovery Interval	
Opalis Integration Server	



Installing Opalis 6.2.2 SP1	
Installing Opalis 6.3 Patch	
Appendix	
Alternate Cisco Nexus 5548 Deployment Procedure: Part 2 for FCoE	
Create VSANs, Assign FC Ports, Turn on FC Ports	
Create Device Aliases and Create Zones	
Alternate Create Zones for Redundant Paths for FCoE	
Cisco Nexus Configurations	271
Nexus A (sample running config)	271
Nexus B (sample running config)	278
References	
Authors	
About Cisco Validated Design (CVD) Program	



### **Overview**

Industry trends indicate a vast data center transformation toward shared infrastructures. Enterprise customers are moving away from silos of information and toward shared infrastructures, to virtualized environments, and eventually to the cloud to increase agility and reduce costs.

FlexPod<sup>™</sup> is a predesigned configuration that is built on the Cisco® Unified Computing System® (Cisco UCS<sup>™</sup>), Cisco Nexus® data center switches, NetApp® FAS storage components, and Microsoft Windows Server and System Center software. FlexPod is a base configuration, but can scale up for greater performance and capacity, or it can scale out for environments that need consistent, multiple deployments. It has the flexibility to be sized and optimized to accommodate many different use cases.

Flexpod is a platform that can address current virtualization needs and simplify the evolution to IT-as-aservice (ITaaS) infrastructure. FlexPod for Microsoft Private Cloud can help improve agility and responsiveness, reduce TCO, and increase business alignment and focus.

This document focuses on deploying an infrastructure capable of supporting Windows Server, Microsoft Hyper-V and Microsoft System Center as the foundation for private cloud infrastructure. For a detailed study of several practical solutions deployed on FlexPod, refer to NetApp Technical Report 3884, FlexPod Solutions Guide.

### Benefits of Cisco Unified Computing System

Cisco Unified Computing System<sup>™</sup> is the first converged data center platform that combines industrystandard, x86-architecture servers with networking and storage access into a single converged system. The system is entirely programmable using unified, model-based management to simplify and speed deployment of enterprise-class applications and services running in bare-metal, virtualized, and cloud computing environments.

The system's x86-architecture rack-mount and blade servers are powered by Intel® Xeon® processors. These industry-standard servers deliver world-record performance to power mission-critical workloads. Cisco servers, combined with a simplified, converged architecture, drive better IT productivity and superior price/performance for lower total cost of ownership (TCO). Building on Cisco's strength in enterprise networking, Cisco Unified Computing System is integrated with a standards-based, high-bandwidth, low-latency, virtualization-aware unified fabric . The system is wired once to support the desired bandwidth and carries all Internet protocol, storage, inter-process communication, and virtual machine traffic with security isolation, visibility, and control equivalent to physical networks. The system meets the bandwidth demands of today's multicore processors, eliminates costly redundancy, and increases workload agility, reliability, and performance.

Cisco Unified Computing System is designed from the ground up to be programmable and self integrating. A server's entire hardware stack, ranging from server firmware and settings to network profiles, is configured through model-based management. With Cisco virtual interface cards, even the number and type of I/O interfaces is programmed dynamically, making every server ready to power any workload at any time. With model-based management, administrators manipulate a model of a desired system configuration, associate a model's service profile with hardware resources, and the system configures itself to match the model. This automation speeds provisioning and workload migration with accurate and rapid scalability. The result is increased IT staff productivity, improved compliance, and reduced risk of failures due to inconsistent configurations.

Cisco Fabric Extender technology reduces the number of system components to purchase, configure, manage, and maintain by condensing three network layers into one. It eliminates both blade server and hypervisor-based switches by connecting fabric interconnect ports directly to individual blade servers and virtual machines. Virtual networks are now managed exactly as physical networks are, but with massive scalability. This represents a radical simplification over traditional systems, reducing capital and operating costs while increasing business agility, simplifying and speeding deployment, and improving performance.





Cisco Unified Computing System helps organizations go beyond efficiency: it helps them become more effective through technologies that breed simplicity rather than complexity. The result is flexible, agile, high-performance, self-integrating information technology, reduced staff costs with increased uptime through automation, and more rapid return on investment.

### **Benefits of Cisco Nexus 5548UP**

The Cisco Nexus 5548UP Switch delivers innovative architectural flexibility, infrastructure simplicity, and business agility, with support for networking standards. For traditional, virtualized, unified, and high-performance computing (HPC) environments, it offers a long list of IT and business advantages, including:

- Architectural Flexibility
- Unified ports that support traditional Ethernet, Fibre Channel (FC), and Fibre Channel over Ethernet (FCoE)
- Synchronizes system clocks with accuracy of less than one microsecond, based on IEEE 1588
- Offers converged Fabric extensibility, based on emerging standard IEEE 802.1BR, with Fabric Extender (FEX) Technology portfolio, including:
- Cisco Nexus 2000 FEX
- Adapter FEX
- VM-FEX

Infrastructure Simplicity

- Common high-density, high-performance, data-center-class, fixed-form-factor platform
- Consolidates LAN and storage
- Supports any transport over an Ethernet-based fabric, including Layer 2 and Layer 3 traffic
- Supports storage traffic, including iSCSI, NAS, FC, RoE, and IBoE
- Reduces management points with FEX Technology

**Business Agility** 

- Meets diverse data center deployments on one platform
- Provides rapid migration and transition for traditional and evolving technologies
- Offers performance and scalability to meet growing business needs

Specifications at-a Glance

- A 1 -rack-unit, 1/10 Gigabit Ethernet switch
- 32 fixed Unified Ports on base chassis and one expansion slot totaling 48 ports
- The slot can support any of the three modules: Unified Ports, 1/2/4/8 native Fibre Channel, and Ethernet or FCoE
- Throughput of up to 960 Gbps

### **Benefits of NetApp FAS Family of Storage Controllers**

The NetApp Unified Storage Architecture provides customers with an agile and scalable storage platform. All NetApp storage systems use the Data ONTAP® operating system to provide SAN (FCoE, FC, iSCSI), NAS (CIFS, NFS), and primary and secondary storage within a single unified platform so that all virtual desktop data components can be hosted on the same storage array. A single process for activities such as installation, provisioning, mirroring, backup, and upgrading is used throughout the entire product line from the entry level to enterprise-class controllers. Having a single set of software and processes brings





great simplicity to even the most complex enterprise data management challenges. Unifying storage and data management software and processes reduces the complexity of data ownership, enables companies to adapt to their changing business needs without interruption, and results in a reduction in total cost of ownership.

In a shared infrastructure, the availability and performance of the storage infrastructure are critical because storage outages or performance issues can affect thousands of users. The storage architecture must provide a high level of availability and performance. For detailed documentation surrounding best practices, NetApp and its technology partners have developed a variety of best practice documents.

Recommended support documents:

- NetApp storage systems: <u>www.netapp.com/us/products/storage-systems/</u>
- NetApp TR-3437: Storage Best Practices and Resiliency Guide
- NetApp TR-3450: Active-Active Controller Overview and Best Practices Guidelines
- NetApp TR-3749: NetApp and VMware vSphere Storage Best Practices
- NetApp TR-3705: NetApp and VMware View Solution Guide
- NetApp TR-3824: MS Exchange 2010 Best Practices Guide
- NetApp TR-3633: Oracle 11g Best Practices Guide

### **Benefits of Microsoft Private Cloud Solution**

Microsoft private cloud solutions, built on Microsoft Windows Server and System Center, dramatically change the way that enterprise customers produce and consume IT services by creating a layer of abstraction over pooled IT resources.

Hyper-V is Microsoft's hypervisor which provides a scalable, reliable, and highly available platform with unlimited virtualization rights included in the Windows Server Datacenter Edition. Features in Windows Server increase availability and performance, improves management, and simplifies methods for deployment including live migration.

When combined with System Center, customers benefit from enterprise class virtualization, end-to-end service management and deep insight to keep applications up and running more reliably.

Microsoft private cloud solutions enable application-level management and monitoring providing deep applications insights with the ability to automatically orchestrate resources enable you to deliver applications as services, rapidly resolve problems, increase application uptime and meet desired SLAs. In addition, it supports Microsoft and non-Microsoft hypervisors, operating systems, and support for open source tools allowing you to leverage your existing infrastructure investments and skills.

Microsoft Private Cloud solutions offer the best economics by integrating a highly available and easy to manage multi-server platform with breakthrough efficiency and ubiquitous automation. It also provides Dynamic, multi-tenant virtualization, storage and networking infrastructure providing maximum flexibility for delivering and connecting to cloud services.

Go to http://microsoft.com/privatecloud to learn more about Microsoft offerings..



### **Audience**

This document describes the architecture and deployment procedures of an infrastructure comprised of Cisco, NetApp and Microsoft virtualization. The intended audience of this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineering, and customers who want to deploy the core FlexPod architecture.

### Architecture

The FlexPod architecture is highly modular or "pod" like. While each customer's FlexPod unit might vary in its exact configuration, once a FlexPod unit is built, it can easily be scaled as requirements and demand change. This includes scaling both up (adding additional resources within a FlexPod unit) and out (adding additional FlexPod units).

Specifically, FlexPod is a defined set of hardware and software that serves as an integrated foundation for all virtualization solutions. Microsoft Private Cloud Solution validated with FlexPod includes NetApp storage, Cisco networking, the Cisco Unified Computing System, and Microsoft virtualization software in a single package in which the computing and storage can fit in one data center rack with the networking residing in a separate rack or deployed according to a customer's datacenter design. Due to port density, the networking components can accommodate multiple such configurations.

This document details the deployment of MS Hyper-V on top of a FlexPod infrastructure. As such, this document focuses on infrastructure deployment as well as OS provisioning and best practices. Figure 1 shows the Hyper-V built on FlexPod components and the network connections for a configuration with FC and Ethernet based storage. One benefit of a FlexPod architecture is the ability to customize or "flex" the environment to suit a customers' requirements. For this reason, an alternate FCoE-based storage configuration is included in the Appendix.





#### Figure 1 FlexPod for Microsoft Private Cloud components



The reference configuration includes:

- Two Cisco Nexus 5548 switches
- Two Cisco UCS 6248 fabric interconnects
- One chassis of Cisco UCS blades with two fabric extenders per chassis
- FAS3240A (HA Pair)

Storage is provided by a NetApp FAS3240A (HA configuration within a single chassis) with accompanying disk shelves. All systems and fabric links feature redundancy, providing for end-to-end high availability (HA). For server virtualization, the deployment includes MS Hyper-V. While this is the default base design, each of the components can be scaled flexibly to support the specific business requirements in question. For example, more (or different) blades and chassis could be deployed to increase compute capacity, additional disk shelves could be deployed to improve I/O capacity and throughput, or special hardware or software features could be added to introduce new features.

The remainder of this document guides you through the low-level steps of deploying the base architecture, as shown in



Figure 1. This includes everything from physical cabling, to compute and storage configuration, to configuring virtualization with MS Hyper-V.

### **Software Revisions**

It is important to note the software versions used in this document. Table 1 details the software revisions used throughout this document.

#### Table 1 Software Revisions

Layer	Compute	Version or Release	Details
Compute	Cisco UCS Fabric Interconnect	2.0(1t)	Embedded management
	CISCO OC3 B-200-IVI2	2.0(11)	
Network	Nexus Fabric Switch	5.0(3)N2(2a)	Operating system version
Storage	NetApp FAS3240 HA	ONTAP 8.0.2	Operating system version
Software	Cisco UCS Hosts	Microsoft Windows Server 2008 R2 SP1 Data Center Edition + MS Hyper-V Role	Operating system version
	.NET Framework	3.5.1	Feature enabled within Windows operating system
	Microsoft Hotfixes	KB2517329 KB2552040 KB2494016 KB2520235 KB2531907 KB2522766 KB2528357	Miscellaneous Microsoft Hotfixes required
	NetApp SnapDrive for Windows	6.4 64-bit	NetApp integration within Windows operating system
	Data ONTAP DSM	3.5	Windows MPIO software
	MS SQL Server	Windows 2008 SP2	VM (2): SQL Server DB
	Systems Center Operation Manager	2007 R2	VM (1):
	Systems Center Virtual Machine Manager	2008 R2 SP1	VM (1):
	Systems Center Opalis	6.3	VM (1):
	OnCommand Plug-In	3.0	NetApp Integration within Systems Center





Layer	Compute	Version or Release	Details
	Cisco UCS Management Pack R2	2.1.0	Cisco Integration within System Center Operations Manager
	Cisco UCS Power Tools	0.9.3.1	Cisco UCS Power Shell Management Cmdlets

### **Configuration Guidelines**

This document provides details for configuring a fully redundant, highly-available configuration. As such, references are made as to which component is being configured with each step whether that be A or B. For example, Controller A and Controller B, are used to identify the two NetApp storage controllers that are provisioned with this document while Nexus A and Nexus B identify the pair of Cisco Nexus switches that are configured. The Cisco UCS fabric interconnects are configured likewise. Additionally, this document details steps for provisioning multiple UCS hosts and these are identified sequentially, VM-Host-Infra-01 and VM-Host-Infra-02, and so on. Finally, when indicating that the reader should include information pertinent to their environment in a given step, this is indicated with the inclusion of <italicized text> as part of the command structure. See the example below for the vlan create command:

controller A> vlan create

```
Usage:
```

```
vlan create [-g {on|off}] <ifname> <vlanid list>
            vlan add <ifname> <vlanid list>
            vlan delete -q <ifname> [<vlanid list>]
            vlan modify -g {on|off} <ifname>
            vlan stat <ifname> [<vlanid list>]
Example:
controller A> vlan create vif0 <management VLAN ID>
```

This document is intended to allow the reader to fully configure the customer environment. In order to do so, there are various steps which will require you to insert your own naming conventions, IP address and VLAN schemes as well as record appropriate WWPN, WWNN, or MAC addresses. Table 2 details the list of VLANs necessary for deployment as outlined in this guide. Note that in this document that the VM-Data VLAN is used for virtual machine management interfaces. The VM-Mgmt VLAN is used for management interfaces of the Hyper-V hosts. A Layer-3 route must exist between the VM-Mgmt and VM-Data VLANS.

VLAN Name	VLAN Purpose	ID Used in this Document
VM-Mgmt	VLAN for management interfaces	805
Native	VLAN to which untagged frames are assigned	2
CSV	VLAN for cluster shared volume	801
iSCSI-A	VLAN for iSCSI traffic for fabric A	802
iSCSI-B	VLAN for iSCSI traffic for fabric B	807

#### **Table 2 Necessary VLANs**



Live Migration	VLAN designated for the movement of VM's from one physical host to another	803
App Cluster	VLAN for cluster connectivity	806
Data	VLAN for application data	804

### Deployment

This document details the necessary steps to deploy base infrastructure components as well as provisioning MS Hyper-V as the foundation for virtualized workloads. At the end of these deployment steps, you will be prepared to provision your applications on top of a MS Hyper-V virtualized infrastructure. The outlined procedure includes:

- Initial NetApp Controller configuration
- Initial Cisco UCS configuration
- Initial Cisco Nexus configuration
- Creation of necessary VLANs and VSANs for management, basic functionality, and specific to the MS virtualized infrastructure
- Creation of necessary vPCs to provide HA among devices
- Creation of necessary service profile pools: WWPN, world-wide node name (WWNN), MAC, server, and so forth
- Creation of necessary service profile policies: adapter, boot, and so forth
- Creation of two service profile templates from the created pools and policies: one each for fabric A and B
- Provisioning of two servers from the created service profiles in preparation for OS installation
- Initial configuration of the infrastructure components residing on the NetApp Controller
- Deployment of MS Hyper-V
- Deployment of MS System Center
- Deployment of the NetApp Plug-ins





The Microsoft Private Cloud Solution validated with FlexPod architecture is flexible; therefore, the exact configuration detailed in this section might vary for customer implementations depending on specific requirements. Although customer implementations might deviate from the information that follows, the best practices, features, and configurations listed in this section should still be used as a reference for building a customized MS Hyper-V built on FlexPod architecture.

### **Cabling Information**

The following information is provided as a reference for cabling the physical equipment in a FlexPod environment. The tables include both local and remote device and port locations in order to simplify cabling requirements.

The tables in this section contain details for the prescribed and supported configuration of the FAS3240 running Data ONTAP 8.0.2. This configuration leverages a dual-port 10GbE adapter as well as the native FC target ports and the onboard SAS ports for disk shelf connectivity. For any modifications of this prescribed architecture, consult the currently available NetApp Interoperability Matrix Tool (IMT).

This document assumes that out-of-band management ports are plugged into an existing management infrastructure at the deployment site.

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

It is possible to order a FAS3240A system in a different configuration from what is prescribed in the tables in this section. Before starting, be sure the configuration matches what is described in the tables and diagrams in this section

Figure 2 shows a FlexPod cabling diagram. The labels indicate connections to end points rather than port numbers on the physical device. For example, connection 1 is an FCoE target port connected from NetApp controller A to Nexus 5548 A. SAS connections 23, 24, 25, and 26 as well as ACP connections 27 and 28 should be connected to the NetApp storage controller and disk shelves according to best practices for the specific storage controller and disk shelf quantity.





#### Figure 2 FlexPod Cabling Diagram







#### Table 3 Cisco Nexus 5548 A Ethernet Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 5548 A	Eth1/1	10GbE	NetApp controller A	e2a
	Eth1/2	10GbE	NetApp controller B	e2a
	Eth1/5	10GbE	Cisco Nexus 5548 B	Eth1/5
	Eth1/6	10GbE	Cisco Nexus 5548 B	Eth1/6
	Eth1/3	10GbE	Cisco UCS fabric interconnect A	Eth1/19
	Eth1/4	10GbE	Cisco UCS fabric interconnect B	Eth1/19
	MGMT0	100MbE	100MbE management switch	Any

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

#### Table 4 Cisco Nexus 5548 B Ethernet Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 5548 B	Eth1/1	10GbE	NetApp controller A	e2b
	Eth1/2	10GbE	NetApp controller B	e2b
	Eth1/5	10GbE	Cisco Nexus 5548 A	Eth1/5
	Eth1/6	10GbE	Cisco Nexus 5548 A	Eth1/6
	Eth1/3	10GbE	Cisco UCS fabric interconnect A	Eth1/20
	Eth1/4	10GbE	Cisco UCS fabric interconnect B	Eth1/20
	MGMT0	100MbE	100MbE management switch	Any

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

#### Table 5 NetApp controller A Ethernet Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
NetApp controller A	e0M	100MbE	100MbE management switch	Any
	e0P	GbE	SAS shelves	ACP port
	e2a	10GbE	Cisco Nexus 5548 A	Eth1/1





Local Device	Local Port	Connection	Remote Device	Remote Port
	e2b	10GbE	Cisco Nexus 5548 B	Eth1/1

#### Table 6 NetApp controller B Ethernet cabling information

Local Device	Local Port	Connection	Remote Device	Remote Port
NetApp controller B	e0M	100MbE	100MbE management switch	Any
	e0P	GbE	SAS shelves	ACP port
	e2a	10GbE	Cisco Nexus 5548 A	Eth1/2
	e2b	10GbE	Cisco Nexus 5548 B	Eth1/2

#### Table 7 Cisco UCS fabric interconnect A Ethernet cabling information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect	Eth1/19	10GbE	Cisco Nexus 5548 A	Eth1/3
A	Eth1/20	10GbE	Cisco Nexus 5548 B	Eth1/3
	Eth1/1	FCoE/10GbE	Chassis 1 FEX A	Port 1
	Eth1/2	FCoE/10GbE	Chassis 1 FEX A	Port 2
	Eth1/3	FCoE/10GbE	Chassis 2 FEX A (if required)	Port 1
	Eth1/4	FCoE/10GbE	Chassis 2 FEX A (if required)	Port 2
	Eth1/5	FCoE/10GbE	Chassis 3 FEX A (if required)	Port 1
	Eth1/6	FCoE/10GbE	Chassis 3 FEX A (if required)	Port 2
	MGMT0	100MbE	100MbE management switch	Any
	L1	GbE	Cisco UCS fabric interconnect B	L1
	L2	GbE	Cisco UCS fabric interconnect B	L2





#### Table 8 Cisco UCS fabric interconnect B Ethernet cabling information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect	Eth1/19	10GbE	Cisco Nexus 5548 A	Eth1/4
В	Eth1/20	10GbE	Cisco Nexus 5548 B	Eth1/4
	Eth1/1	10GbE/FCoE	Chassis 1 FEX B	Port 1
	Eth1/2	10GbE/FCoE	Chassis 1 FEX B	Port 2
	Eth1/3	10GbE/FCoE	Chassis 2 FEX B (if required)	Port 1
	Eth1/4	10GbE/FCoE	Chassis 2 FEX B (if required)	Port 2
	Eth1/5	10GbE/FCoE	Chassis 3 FEX B (if required)	Port 1
	Eth1/6	10GbE/FCoE	Chassis 3 FEX B (if required)	Port 2
	MGMT0	100MbE	100 MbE management switch	Any
	L1	GbE	Cisco UCS fabric interconnect A	L1
	L2	GbE	Cisco UCS fabric interconnect A	L2

#### Table 9 Cisco Nexus 5548 A Fibre Channel cabling information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 5548 A	FC1/29	FC	Controller_A	0c
	FC1/30	FC	Controller_B	0c
	FC1/31	FC	Cisco UCS fabric interconnect A	Port 31
	FC1/32	FC	Cisco UCS fabric interconnect A	Port 32

#### Table 10 Cisco Nexus 5548 B Fibre Channel cabling information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 5548 B	FC1/29	FC	Controller_A	0d
	FC1/30	FC	Controller_B	0d
	FC1/31	FC	Cisco UCS fabric interconnect A	Port 31
	FC1/32	FC	Cisco UCS fabric interconnect A	Port 32





#### Table 11 Cisco UCS fabric interconnect A Fibre Channel cabling information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect A	Port 31	FC	Cisco Nexus 5548 A	FC1/31
	Port 32	FC	Cisco Nexus 5548 A	FC1/32

#### Table 12 Cisco UCS Fabric Interconnect B Fibre Channel cabling information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS fabric interconnect B	Port 31	FC	Cisco Nexus 5548 B	FC1/31
	Port 32	FC	Cisco Nexus 5548 B	FC1/32

### NetApp FAS3240A Deployment Procedure: Part 1

The following section provides a detailed procedure for configuring the NetApp FAS3240 A for use in a MS-HyperV built on FlexPod environment. These steps should be followed precisely. Failure to do so could result in an improper configuration.

**Note:** The configuration steps detailed in this section provides guidance for configuring the FAS3240A running ONTAP 8.0.2.

#### Assign Controller Disk Ownership

These steps provide details for assigning disk ownership and disk initialization and verification.

#### Controller A

- 1. During controller boot, when prompted for Boot Menu, press CTRL-C.
- 2. At the menu prompt, select option 5 for Maintenance mode boot.
- 3. Type Yes if prompted with Continue to boot?
- 4. Type disk show. No disks should be assigned to the controller.
- 5. Reference the Local System ID: value for the following disk assignment.
- **Note:** Half the total number of disks in the environment are assigned to this controller and half to the other controller. Divide the number of disks in half and use the result in the following command for the <# of disks>.
- 6. Type disk assign -n <#>.
- 7. Type halt to reboot the controller.
- 8. If the controller stops at a LOADER-A> prompt, type autoboot to start Data ONTAP.
- 9. During controller boot, when prompted, press CTRL-C.
- 10. At the menu prompt, select option 4 for Clean configuration and initialize all disks.
- 11. The installer asks if you want to zero the disks and install a new file system. Answer y.
- 12. A warning displays that this will erase all of the data on the disks. Answer y that you are sure this is what you want to do.



**Note:** The initialization and creation of the root volume can take 75 minutes or more to complete, depending on the number of disks attached. Once initialization is complete, the storage system reboots.

#### **Controller B**

- 1. During controller boot, when prompted to Press CTRL-C for special boot menu, press CTRL-C.
- 2. At the menu prompt, select option 5 for Maintenance mode boot.
- 3. Type Yes if prompted with Continue to boot?
- 4. Type disk show. No disks should be assigned to the controller.
- 5. Reference the Local System ID: value for the following disk assignment.
- **Note:** The initialization and creation of the root volume can take 75 minutes or more to complete, depending on the number of disks attached. Once initialization is complete, the storage system reboots.
- 6. Type disk assign -n <#>.
- 7. Type halt to reboot the controller.
- 8. If the controller stops at a LOADER-B> prompt, type autoboot to start Data ONTAP.
- 9. During controller boot, when prompted to Press CTRL-C for Boot Menu, press CTRL-C.
- 10. At the menu prompt, select option 4 for Clean configuration and initialize all disks.
- 11. The installer asks if you want to zero the disks and install a new file system. Answer y.
- 12. A warning displays that this will erase all of the data on the disks. Answer y that you are sure this is what you want to do.
- **Note:** The initialization and creation of the root volume can take 75 minutes or more to complete, depending on the number of disks attached. Once initialization is complete, the storage system reboots.

#### Set up Data ONTAP 8.0.2

These steps provide details for setting up Data ONTAP 8.0.2.

#### **Controller A**

- 1. After the disk initialization and the creation of the root volume, Data ONTAP setup begins.
- 2. Enter the hostname of the storage system.
- 3. Answer y for setting up interface groups.
- 4. Enter 1 for the number of interface groups to configure.
- 5. Name the interface vif0.
- 6. Enter 1 to specify the interface as LACP.
- 7. Enter I to specify IP load balancing
- 8. Enter 2 for the number of links for vif0.
- 9. Enter e2a for the name of the first link.
- 10. Enter e2b for the name of the second link.
- 11. Enter the controller in-band management address when prompted for an IP address for vif0.
- 12. Enter the netmask for the controller in-band management address.
- 13. Enter y for interface group vif0 taking over a partner interface.



- 14. Enter vif0 for the name of the interface to be taken over.
- 15. Press Enter to accept the blank IP address for e0a.
- 16. Enter n for interface e0a taking over a partner interface.
- 17. Press Enter to accept the blank IP address for e0b.
- 18. Enter n for interface e0b taking over a partner interface.
- 19. Enter the IP address of the out-of-band management interface, e0M.
- 20. Enter the subnet mask for  ${\tt eOM}.$
- 21. Enter y for interface e0M taking over a partner IP address during failover.
- 22. Enter  ${\tt e0M}$  for the name of the interface to be taken over.
- 23. Press Enter to accept the default flow control of full.
- 24. Answer n to continuing setup through the Web interface.
- 25. Enter the IP address for the default gateway for the storage system.
- 26. Enter the IP address for the administration host.
- 27. Enter the local timezone (for example, PST, MST, CST, or EST).
- 28. Enter the location for the storage system.
- 29. Answer y to enable DNS resolution.
- 30. Enter the DNS domain name.
- 31. Enter the IP address for the first nameserver.
- 32. Answer n to finish entering DNS servers, or answer y to add up to two more DNS servers.
- 33. Answer n for running the NIS client.
- 34. Press Enter to acknowledge the AutoSupport<sup>™</sup> message.
- 35. Answer y to configuring the SP LAN interface.
- 36. Answer n to setting up DHCP on the SP LAN interface.
- 37. Enter the IP address for the SP LAN interface.
- 38. Enter the subnet mask for the SP LAN interface.
- 39. Enter the IP address for the default gateway for the SP LAN interface.
- 40. Enter the fully qualified domain name for the mail host to receive SP messages and AutoSupport.
- 41. Enter the IP address for the mail host to receive SP messages and AutoSupport.
- 42. Enter the new administrative (root) password.
- 43. Enter the new administrative (root) password again to confirm.
- 44. After these steps are completed, the controller should display a password prompt. Enter the administrative password to login as root.

#### Controller B

- 1. After the disk initialization and the creation of the root volume, Data ONTAP setup begins.
- 2. Enter the hostname of the storage system.
- 3. Answer y for setting up interface groups.
- 4. Enter 1 for the number of interface groups to configure.
- 5. Name the interface vif0.



- 6. Enter 1 to specify the interface as LACP.
- 7. Enter I to specify IP load balancing
- 8. Enter 2 for the number of links for vif0.
- 9. Enter e2a for the name of the first link.
- 10. Enter e2b for the name of the second link.
- 11. Enter the controller in-band management address when prompted for an IP address for vif0.
- 12. Enter the netmask for the controller in-band management address.
- 13. Enter y for interface group vif0 taking over a partner interface.
- 14. Enter vif0 for the name of the interface to be taken over.
- 15. Press Enter to accept the blank IP address for e0a.
- 16. Enter n for interface e0a taking over a partner interface.
- 17. Press Enter to accept the blank IP address for e0b.
- 18. Enter n for interface e0b taking over a partner interface.
- 19. Enter the IP address of the out-of-band management interface, e0M.
- 20. Enter the subnet mask for e0M.
- 21. Enter y for interface e0M taking over a partner IP address during failover.
- 22. Enter  ${\tt e0M}$  for the name of the interface to be taken over.
- 23. Press Enter to accept the default flow control of full.
- 24. Answer n to continuing setup through the Web interface.
- 25. Enter the IP address for the default gateway for the storage system.
- 26. Enter the IP address for the administration host.
- 27. Enter the local timezone (for example, PST, MST, CST, or EST).
- 28. Enter the location for the storage system.
- 29. Answer y to enable DNS resolution.
- 30. Enter the DNS domain name.
- 31. Enter the IP address for the first nameserver.
- 32. Answer n to finish entering DNS servers, or answer y to add up to two more DNS servers.
- 33. Answer n for running the NIS client.
- 34. Press Enter to acknowledge the AutoSupport<sup>™</sup> message.
- 35. Answer y to configuring the SP LAN interface.
- 36. Answer n to setting up DHCP on the SP LAN interface.
- 37. Enter the IP address for the SP LAN interface.
- 38. Enter the subnet mask for the SP LAN interface.
- 39. Enter the IP address for the default gateway for the SP LAN interface.
- 40. Enter the fully qualified domain name for the mail host to receive SP messages and AutoSupport.
- 41. Enter the IP address for the mail host to receive SP messages and AutoSupport.
- 42. Enter the new administrative (root) password.
- 43. Enter the new administrative (root) password again to confirm.



44. After these steps are completed, the controller should display a password prompt. Enter the administrative password to login as root.

#### Install Data ONTAP to Onboard Flash Storage

These steps provide details for installing Data ONTAP to the onboard flash storage.

#### For Controller A and Controller B

- 1. Install the Data ONTAP image to the onboard flash device by using the software install and indicate the http or https Web address of the NetApp Data ONTAP 8.0.2 flash image.
- 2. After this is complete, type download and press Enter to download the software to the flash device.

#### Harden Storage System Logins and Security

These steps provide details for hardening the storage system logins and security.

#### For Controller A and Controller B

- 1. Type secureadmin disable ssh.
- 2. Type secureadmin setup -f ssh to enable ssh on the storage controller.
- 3. If prompted, type yes to rerun ssh setup.
- 4. Accept the default values for ssh1.x protocol.
- 5. Enter 1024 for ssh2 protocol.
- 6. Enter yes if the information specified is correct and to create the ssh keys.
- 7. Type options telnet.enable off to disable telnet on the storage controller.
- 8. Type secureadmin setup ssl to enable ssl on the storage controller.
- 9. If prompted, type yes to rerun ssl setup.
- 10. Enter the country name code, state or province name; locality name; organization name, and organization unit name.
- 11. Enter the fully qualified domain name of the storage system.
- 12. Enter the administrator's e-mail address.
- 13. Accept the default for days until the certificate expires.
- 14. Enter 1024 for the ssl key length.
- 15. Enter options httpd.admin.enable off to disable http access to the storage system.
- 16. Enter options httpd.admin.ssl.enable on to enable secure access to FilerView.

#### **Install Required Licenses**

These steps provide details for licensing relevant storage licenses for feature enablement, which are used in this reference architecture.

Note: Recommended licenses include:

- near\_store: To enable the nearstore personality on a controller
- a\_sis: To enable advanced single instance storage availability
- cluster (cf): To configure storage controllers into an HA pair
- CIFS: To enable the CIFS protocol
- FCP: To enable the FCP protocol
- iSCSI: To enable the iSCSI protocol



- flash\_cache: To enable usage of the Flash Cache module
- flex\_clone: To enable the provisioning of NetApp Flex Clones

Note: If deduplication is required, license near-store prior to licensing a\_sis.

#### For Controller A and Controller B

- 1. Type license add < necessary licenses> to add licenses to the storage system.
- 2. Type license to double-check the installed licenses.
- 3. Type reboot to reboot the storage controller.

#### **Configure Native FC ports as FC Targets adapters**

These steps provide details for configuring the native FC ports as target ports.

#### For Controller A and Controller B

1. Type fcadmin config.

This allows the administrator to confirm the state of the native fc ports. If the ports are configured as initiators as opposed to targets proceed to step 2. For the following changes to take effect, a reboot must occur.

- 2. Type fc admin config -t target 0c.
- 3. Type fc admin config -t target 0d.
- 4. Type reboot to reboot the storage controller.

#### Enable Active-Active Controller Configuration Between Two Storage Systems

This step provides details for enabling active-active controller configuration between the two storage systems.

#### Controller A only

1. After both controllers have rebooted, type cf enable and press Enter to enable active-active controller configuration.

#### **Start FCP**

This step provides details for enabling the fibre channel protocol.

#### For Controller A and Controller B

1. Type fcp start.

#### Start iSCSI

This step provides details for enabling the iSCSI protocol.

#### For Controller A and Controller B

1. Type iscsi start.

#### Set up Storage System NTP Time Synchronization and CDP enablement

These steps provide details for setting up storage system NTP time synchronization and enablement of Cisco Discovery Protocol (CDP).

#### For Controller A and Controller B



- 1. Type date CCyymmddhhmm where CCyy is the four-digit year, mm is the two-digit month, dd is the two-digit day of the month, hh is the two-digit hour, and the second mm is the two-digit minute to set the storage system time to the actual time.
- 2. Type options timed.proto ntp to synchronize with an NTP server.
- 3. Type options timed.servers <NTP server IP> to add the NTP server to the storage system list.
- 4. Type options timed.enable on to enable NTP synchronization on the storage system.
- 5. Type options cdpd.enable on.

#### Create Data Aggregate aggr1

These steps provide details for creating the data aggregate aggr1. In most cases, this command finishes quickly, but depending on the state of each disk, it might be necessary to zero some or all of the disks in order to add them to the aggregate. This might take up to 60 minutes to complete.

#### **Controller A**

1. Type aggr create aggr1 -B 64 <# of disks for aggr1> to create aggr1 on the storage controller.

#### **Controller B**

1. Type aggr create aggr1 -B 64 <# of disks for aggr1>to create aggr1 on the storage controller.

#### Create SNMP Requests Role and Assign SNMP Login Privileges

These steps provide details for creating SNMP requests role and assign SNMP login privileges.

#### For Controller A and Controller B

1. Run the following command: useradmin role add <*Controller SNMP request role>* -a login-snmp.

#### **Create SNMP Management Group and Assign SNMP Request Role**

This step provides details for creating SNMP management group and assigning a SNMP request role to it.

#### For Controller A and Controller B

1. Run the following command: useradmin group add <Controller SNMP managers> -r <Controller SNMP request role>.

#### Create SNMP User and Assign to SNMP Management Group

This step provides details for creating SNMP user and assigning it to an SNMP management group.



#### For Controller A and Controller B

1. Run the following command: useradmin user add <Controller SNMP users> -g <Controller SNMP managers>.

After the user is created, the system prompts for a password. Enter the SNMP password when prompted.

#### Set up SNMP v1 Communities on Storage Controllers

These steps provide details for setting up SNMP v1 communities on the storage controllers so that OnCommand System Manager can be used.

#### For Controller A and Controller B

- 1. Run the following command: snmp community delete all.
- 2. Run the following command: snmp community add ro <Controller SNMP community>.

#### Set up SNMP Contact Information for each Storage Controller

This step provide details for setting SNMP contact information for each of the storage controllers.

#### For Controller A and Controller B

1. Run the following command: snmp contact <Controller admin email address>.

#### Set SNMP Location Information for Each Storage Controller

This step provides details for setting SNMP location information for each of the storage controllers. For Controller A and Controller B

1. Run the following command: snmp location <Controller SNMP site name>.

#### **Reinitialize SNMP on Storage Controllers**

This step provides details for reinitializing SNMP on the storage controllers.

#### For Controller A and Controller B

1. Run the following command: snmp init 1.

#### **Enable Flash Cache**

This step provides details for enabling the NetApp Flash Cache module, if installed. **For Controller A and Controller B** 

1. Enter the following command to enable Flash Cache on each controller: options flexscale.enable on.

#### Add VLAN Interfaces

These steps provide details for adding VLAN interfaces on the storage controllers.

#### **Controller A**

- 1. Run the following command: VLAN add vif0-<iSCSI A VLAN ID>.
- 2. Run the following command: wrfile -a /etc/rc vlan add vif0-<iSCSI A VLAN ID>.



- 3. Run the following command: ifconfig vif0-<iSCSI A VLAN ID> mtusize 1500 partner vif0-<iSCSI A VLAN ID>.
- 4. Run the following command: wrfile -a /etc/rc ifconfig vif0-<iSCSI A VLAN ID> mtusize 1500 partner vif0-<iSCSI A VLAN ID>.
- 5. Run the following command: ifconfig vif0-<iSCSI A VLAN ID> <Controller A iSCSI A VLAN IP> netmask <iSCSI A VLAN netmask>.
- 6. Run the following command: wrfile -a ifconfig vif0-<iSCSI VLAN ID> <Controller A iSCSI A VLAN IP> netmask <iSCSI A VLAN netmask>.
- 7. Run the following command: VLAN add vif0-<isCSI B VLAN ID>.
- 8. Run the following command: wrfile -a /etc/rc vlan add vif0-<iSCSI B VLAN ID>.
- Run the following command: ifconfig vif0-<iSCSI B VLAN ID> mtusize 1500 partner vif0-<iSCSI B VLAN ID>.
- 10. Run the following command: wrfile -a /etc/rc ifconfig vif0-<iSCSI B VLAN ID> mtusize 1500 partner vif0-<iSCSI B VLAN ID>.
- 11. Run the following command: ifconfig vif0-<iSCSI B VLAN ID> <Controller A iSCSI B VLAN IP> netmask <iSCSI B VLAN netmask>.
- 12. Run the following command: wrfile -a ifconfig vif0-<iSCSI VLAN ID> <Controller A iSCSI B VLAN IP> netmask <iSCSI B VLAN netmask>.

#### 13.

#### **Controller B**

- 1. Run the following command: VLAN add vif0-<isCSI A VLAN ID>.
- 2. Run the following command: wrfile -a /etc/rc vlan add vif0-<iSCSI A VLAN ID>.
- Run the following command: ifconfig vif0-<iSCSI A VLAN ID> mtusize 1500 partner vif0-<iSCSI A VLAN ID>.
- 4. Run the following command: wrfile -a /etc/rc ifconfig vif0-<iSCSI A VLAN ID> mtusize 1500 partner vif0-<iSCSI A VLAN ID>.
- 5. Run the following command: ifconfig vif0-<iSCSI A VLAN ID> <Controller B iSCSI A VLAN IP> netmask <iSCSI A VLAN netmask>.
- 6. Run the following command: wrfile -a ifconfig vif0-<iSCSI VLAN ID> <Controller B iSCSI A VLAN IP> netmask <iSCSI A VLAN netmask>.
- 7. Run the following command: VLAN add vif0-<isCSI B VLAN ID>.
- 8. Run the following command: wrfile -a /etc/rc vlan add vif0-<iSCSI B VLAN ID>.
- 9. Run the following command: ifconfig vif0-<iSCSI B VLAN ID> mtusize 1500 partner vif0-<iSCSI B VLAN ID>.
- 10. Run the following command: wrfile -a /etc/rc ifconfig vif0-<iSCSI B VLAN ID> mtusize 1500 partner vif0-<iSCSI B VLAN ID>.
- 11. Run the following command: ifconfig vif0-<iSCSI B VLAN ID> <Controller B iSCSI B VLAN IP> netmask <iSCSI B VLAN netmask>.
- 12. Run the following command: wrfile -a ifconfig vif0-<iSCSI VLAN ID> <Controller B iSCSI B VLAN IP> netmask <iSCSI B VLAN netmask>.



#### Add Infrastructure Volumes

These steps provide details for adding volumes on the storage controller for SAN boot of the Cisco UCS hosts as well as virtual machine provisioning.

**Note:** As this configuration calls for an active / active use of the storage controllers, volumes are created on both controllers and the load is distributed.

#### **Controller A**

- 1. Run the following command: vol create CSV A -s none aggr1 500g.
- 2. Run the following command: sis on /vol/CSV A.
- 3. Run the following command: vol create win boot A -s none aggr1 1t.
- 4. Run the following command: sis on /vol/win\_boot\_A.
- 5. Run the following command: vol create Infra iSCSI A -s none aggr1 1500g.
- 6. Run the following command: sis on /vol/Infra iSCSI A.

#### Controller B

- 1. Run the following command: vol create CSV B -s none aggr1 500g.
- 2. Run the following command: sis on /vol/CSV\_B.
- 3. Run the following command: vol create win boot B -s none aggr1 1t.
- 4. Run the following command: sis on /vol/win\_boot\_B.
- 5. Run the following command: vol create Infra iSCSI B -s none aggr1 1500g.
- 6. Run the following command: sis on /vol/Infra\_iSCSI\_B.

#### **Cisco Nexus 5548 Deployment Procedure: Part 1**

The following section provides a detailed procedure for configuring the Cisco Nexus 5548 switches for use in a FlexPod environment. Follow these steps precisely because failure to do so could result in an improper configuration.

**Note:** The configuration steps detailed in this section provides guidance for configuring the Nexus 5548 UP running release 5.0(3)N2(2a).

This configuration also leverages the native VLAN on the trunk ports to discard untagged packets, by setting the native VLAN on the PortChannel, but not including this VLAN in the allowed VLANs on the PortChannel.

#### Set up Initial Cisco Nexus 5548 Switch

These steps provide details for the initial Cisco Nexus 5548 Switch setup.

#### Cisco Nexus 5548 A

On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start.

- 1. Enter yes to enforce secure password standards.
- 2. Enter the password for the admin user.
- 3. Enter the password a second time to commit the password.
- 4. Enter yes to enter the basic configuration dialog.
- 5. Create another login account (yes/no) [n]: Enter.



- 6. Configure read-only SNMP community string (yes/no) [n]: Enter.
- 7. Configure read-write SNMP community string (yes/no) [n]: Enter.
- 8. Enter the switch name: <Nexus A Switch name> Enter.
- 9. Continue with out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter.
- 10. Mgmt0 IPv4 address: <Nexus A mgmt0 IP> Enter.
- 11. Mgmt0 IPv4 netmask: <Nexus A mgmt0 netmask> Enter.
- 12. Configure the default gateway? (yes/no) [y]: Enter.
- 13. IPv4 address of the default gateway: <Nexus A mgmt0 gateway> Enter.
- 14. Enable the telnet service? (yes/no) [n]: Enter.
- 15. Enable the ssh service? (yes/no) [y]: Enter.
- 16. Type of ssh key you would like to generate (dsa/rsa):rsa.
- 17. Number of key bits <768–2048> :1024 Enter.
- 18. Configure the ntp server? (yes/no) [y]: Enter.
- 19. NTP server IPv4 address: <NTP Server IP> Enter.
- 20. Enter basic FC configurations (yes/no) [n]: Enter.
- 21. Would you like to edit the configuration? (yes/no) [n]: Enter.
- 22. Be sure to review the configuration summary before enabling it.
- 23. Use this configuration and save it? (yes/no) [y]: Enter.
- 24. Configuration may be continued from the console or by using SSH. To use SSH, connect to the mgmt0 address of Nexus A.
- 25. Log in as user admin with the password previously entered.

#### Cisco Nexus 5548 B

On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start.

- 1. Enter yes to enforce secure password standards.
- 2. Enter the password for the admin user.
- 3. Enter the password a second time to commit the password.
- 4. Enter yes to enter the basic configuration dialog.
- 5. Create another login account (yes/no) [n]: Enter.
- 6. Configure read-only SNMP community string (yes/no) [n]: Enter.
- 7. Configure read-write SNMP community string (yes/no) [n]: Enter.
- 8. Enter the switch name: <Nexus B Switch name> Enter.
- 9. Continue with out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter.
- 10. Mgmt0 IPv4 address: <Nexus B mgmt0 IP> Enter.
- 11. Mgmt0 IPv4 netmask: <Nexus B mgmt0 netmask> Enter.
- 12. Configure the default gateway? (yes/no) [y]: Enter.
- 13. IPv4 address of the default gateway: <Nexus B mgmt0 gateway> Enter.



- 14. Enable the telnet service? (yes/no) [n]: Enter.
- 15. Enable the ssh service? (yes/no) [y]: Enter.
- 16. Type of ssh key you would like to generate (dsa/rsa):rsa.
- 17. Number of key bits <768–2048> :1024 Enter.
- 18. Configure the ntp server? (yes/no) [y]: Enter.
- 19. NTP server IPv4 address: <NTP Server IP> Enter.
- 20. Enter basic FC configurations (yes/no) [n]: Enter.
- 21. Would you like to edit the configuration? (yes/no) [n]: Enter.
- 22. Be sure to review the configuration summary before enabling it.
- 23. Use this configuration and save it? (yes/no) [y]: Enter.
- 24. Configuration may be continued from the console or by using SSH. To use SSH, connect to the mgmt0 address of Nexus A.
- 25. Log in as user admin with the password previously entered.

#### **Enable Appropriate Cisco Nexus Features**

These steps provide details for enabling the appropriate Cisco Nexus features.

#### For Nexus A and Nexus B

- 1. Type config t to enter the global configuration mode.
- 2. Type feature lacp.
- 3. Type feature fcoe.
- 4. Type feature npiv.
- 5. Type feature vpc.
- 6. Type feature fport-channel-trunk.

#### **Set Global Configurations**

These steps provide details for setting global configurations.

#### For Nexus A and Nexus B

- 1. From the global configuration mode, type spanning-tree port type network default to make sure that, by default, the ports are considered as network ports in regards to spanning-tree.
- 2. Type spanning-tree port type edge bpduguard default to enable bpduguard on all edge ports by default.
- 3. Type spanning-tree port type edge bpdufilter default to enable bpdufilter on all edge ports by default.
- 4. Type ip access-list classify\_Silver.
- 5. Type 10 permit ip <iSCSI-A net address> any .where the variable is the network address of the iSCSI-A VLAN in CIDR notation (i.e. 192.168.102.0/24).
- 6. Type 20 permit ip any <iSCSI-A net address>.
- 7. Type 30 permit ip <iSCSI-B net address> any.
- 8. Type 40 permit ip any <iSCSI-B net address>.
- 9. Type exit.



10. Type class-map type qos match-all class-gold. 11. Type match cos 4. 12. Type exit. 13. Type class-map type qos match-all class-silver. 14. Type match cos 2. 15. Type match access-group name classify Silver. 16. Type exit. 17. Type class-map type queuing class-gold. 18. Type match qos-group 3. 19. Type exit. 20. Type class-map type queuing class-silver. 21. Type match qos-group 4. 22. Type exit. 23. Type policy-map type qos system\_qos\_policy. 24. Type class class-gold. 25. Type set qos-group 3. 26. Type class class-silver. 27. Type set qos-group 4. 28. Type class class-fcoe. 29. Type set qos-group 1. 30. Type exit. 31. Type exit. 32. Type policy-map type queuing system q in policy. 33. Type class Type queuing class-fcoe. 34. Type bandwidth percent 20. 35. Type class type queuing class-gold. 36. Type bandwidth percent 33. 37. Type class type queuing class-silver. 38. Type bandwidth percent 29. 39. Type class type queuing class-default. 40. Type bandwidth percent 18. 41. Type exit. 42. Type exit. 43. Type policy-map type queuing system q out policy. 44. Type class type queuing class-fcoe. 45. Type bandwidth percent 20. 46. Type class type queuing class-gold.



47. Type bandwidth percent 33. 48. Type class type queuing class-silver. 49. Type bandwidth percent 29. 50. Type class type queuing class-default. 51. Type bandwidth percent 18. 52. Type exit. 53. Type exit. 54. Type class-map type network-qos class-gold. 55. Type match qos-group 3. 56. Type exit. 57. Type class-map type network-qos class-silver. 58. Type match qos-group 4. 59. Type exit. 60. Type policy-map type network-qos system nq policy. 61. Type class type network-qos class-gold. 62. Type set cos 4. 63. Type mtu 9000. 64. Type class type network-qos class-fcoe. 65. Type pause no-drop. 66. Type mtu 2158. 67. Type class type network-qos class-silver. 68. Type set cos 2. 69. Type mtu 9000. 70. Type class type network-qos class-default. 71. Type mtu 9000. 72. Type exit. 73. Type system gos. 74. Type service-policy type qos input system qos policy. 75. Type service-policy type queuing input system q in policy. 76. Type service-policy type queuing output system q out policy. 77. Type service-policy type network-gos system ng policy. 78. Type exit. 79. Type copy run start.

#### **Configure FC Ports**

These steps provide details for configuring the necessary FC ports on the Nexus devices. **Nexus A and Nexus B** 

1. Type slot 1.



- Type port 29-32 type fc.
   Note: If you are using FCoE between the Nexus 5548 and storage, change this to: Type port 31-32 type fc.
- 3. Type copy run start.
- 4. Type reload.

The Nexus switch will reboot. This will take several minutes.

#### **Create Necessary VLANs**

These steps provide details for creating the necessary VLANs.

#### Nexus A and Nexus B

Following switch reload, Log in as user admin with the password previously entered.

- 1. Type config-t.
- 2. Type vlan <VM-MGMT VLAN ID>.
- 3. Type name VM-MGMT-VLAN.
- 4. Type exit.
- 5. Type vlan <Default VLAN ID>.
- 6. Type name Native-VLAN.
- 7. Type exit.
- 8. Type vlan <CSV VLAN ID>.
- 9. Type name CSV-VLAN.
- 10. Type exit.
- 11. Type vlan <iSCSI A VLAN ID>.
- 12. Type name iSCSI-A-VLAN.
- 13. Type exit.
- 14. Type vlan <iSCSI B VLAN ID>.
- 15. Type name iSCSI-B-VLAN.
- 16. Type exit.
- 17. Type vlan <Live Migration VLAN ID>.
- 18. Type name Live-Migration-VLAN.
- 19. Type exit.
- 20. Type vlan <App-Cluster VLAN ID>.
- 21. Type name App-Cluster-Comm-VLAN.
- 22. Type exit.
- 23. Type vlan <VM Data VLAN ID>.
- 24. Type name VM-Data-VLAN.
- 25. Type exit.

# cisco



#### Add Individual Port Descriptions for Troubleshooting

These steps provide details for adding individual port descriptions for troubleshooting activity and verification.

#### Cisco Nexus 5548 A

- 1. From the global configuration mode, type interface Eth1/1.
- 2. Type description <Controller A:e2a>.
- 3. Type exit.
- 4. Type interface Eth1/2.
- 5. Type description <Controller B:e2a>.
- 6. Type exit.
- 7. Type interface Eth1/5.
- 8. Type description <Nexus B:Eth1/5>.
- 9. Type exit.
- 10. Type interface Eth1/6.
- 11. Type description <Nexus B:Eth1/6>.
- 12. Type exit.
- 13. Type interface Eth1/3.
- 14. Type description <UCSM A:Eth1/19>.
- 15. Type exit.
- 16. Type interface Eth1/4.
- 17. Type description <UCSM B:Eth1/19>.
- 18. Type exit.

#### Cisco Nexus 5548 B

- 1. From the global configuration mode, type interface Eth1/1.
- 2. Type description <Controller A:e2b>.
- 3. Type exit.
- 4. Type interface Eth1/2.
- 5. Type description <Controller B:e2b>.
- 6. Type exit.
- 7. Type interface Eth1/5.
- 8. Type description <Nexus A:Eth1/5>.
- 9. Type exit.
- 10. Type interface Eth1/6.
- 11. Type description <Nexus A:Eth1/6>.
- 12. Type exit.
- 13. Type interface Eth1/3.
- 14. Type description <UCSM A:Eth1/20>.



- 15. Type exit.
- 16. Type interface Eth1/4.
- 17. Type description <UCSM B:Eth1/20>.
- 18. Type exit.

#### **Create Necessary PortChannels**

These steps provide details for creating the necessary PortChannels between devices. **Cisco Nexus 5548 A** 

- 1. From the global configuration mode, type interface Pol0.
- 2. Type description vPC peer-link.
- 3. Type exit.
- 4. Type interface Eth1/5-6.
- 5. Type channel-group 10 mode active.
- 6. Type no shutdown.
- 7. Type exit.
- 8. Type interface Poll.
- 9. Type description <Controller A>.
- 10. Type exit.
- 11. Type interface Eth1/1.
- 12. Type channel-group 11 mode active.
- 13. Type no shutdown.
- 14. Type exit.
- 15. Type interface Po12.
- 16. Type description <Controller B>.
- 17. Type exit.
- 18. Type interface Eth1/2.
- 19. Type channel-group 12 mode active.
- 20. Type no shutdown.
- 21. Type exit.
- 22. Type interface Po13.
- 23. Type description <UCSM A>.
- 24. Type exit.
- 25. Type interface Eth1/3.
- 26. Type channel-group 13 mode active.
- 27. Type no shutdown.
- 28. Type exit.
- **29. Type** interface Pol4.
- **30.** Type description *<UCSM B>*.


- 31. Type exit.
- 32. Type interface Eth1/4.
- 33. Type channel-group 14 mode active.
- 34. Type no shutdown.
- 35. Type exit.
- 36. Type copy run start.

#### Cisco Nexus 5548 B

- 1. From the global configuration mode, type interface Pol0.
- 2. Type description vPC peer-link.
- 3. Type exit.
- 4. Type interface Eth1/5-6.
- 5. Type channel-group 10 mode active.
- 6. Type no shutdown.
- 7. Type exit.
- 8. Type interface Poll.
- 9. Type description <Controller A>.
- 10. Type exit.
- 11. Type interface Eth1/1.
- 12. Type channel-group 11 mode active.
- 13. Type no shutdown.
- 14. Type exit.
- **15.** Type interface Pol2.
- 16. Type description <Controller B>.
- 17. Type exit.
- 18. Type interface Eth1/2.
- 19. Type channel-group 12 mode active.
- 20. Type no shutdown.
- 21. Type exit.
- 22. Type interface Po13.
- 23. Type description <UCSM A>.
- 24. Type exit.
- 25. Type interface Eth1/3.
- 26. Type channel-group 13 mode active.
- 27. Type no shutdown.
- 28. Type exit.



- **29. Type** interface Pol4.
- **30.** Type description *<UCSM B>*.
- 31. Type exit.
- 32. Type interface Eth1/4.
- 33. Type channel-group 14 mode active.
- 34. Type no shutdown.
- 35. Type exit.
- **36.** Type copy run start.

#### Add PortChannel Configurations

These steps provide details for adding PortChannel configurations. **Cisco Nexus 5548 A** 

- 1. From the global configuration mode, type interface Pol0.
- 2. Type switchport mode trunk.
- 3. Type switchport trunk native vlan <Native VLAN ID>.
- 4. Type switchport trunk allowed vlan <MGMT VLAN ID, CSV VLAN ID, iSCSI A VLAN ID, iSCSI B VLAN ID, Live Migration VLAN ID, VM Cluster Comm VLAN ID, VM Data VLAN ID>.
- 5. Type spanning-tree port type network.
- 6. Type no shutdown.
- 7. Type exit.
- 8. Type interface Poll.
- 9. Type switchport mode trunk.
- 10. Type switchport trunk native vlan <MGMT VLAN ID>.
- 11. Type switchport trunk allowed vlan <MGMT VLAN ID, iSCSI A VLAN ID, iSCSI B VLAN ID>.
- 12. Type spanning-tree port type edge trunk.
- 13. Type no shut.
- 14. Type exit.
- 15. Type interface Po12.
- 16. Type switchport mode trunk.
- 17. Type switchport trunk native vlan <MGMT VLAN ID>.
- 18. Type switchport trunk allowed vlan <MGMT VLAN ID, iSCSI A, iSCSI B VLAN ID >.
- 19. Type spanning-tree port type edge trunk.
- 20. Type no shut.
- 21. Type exit.
- 22. Type interface Po13.
- 23. Type switchport mode trunk.



- 24. Type switchport trunk native vlan <Native VLAN ID>.
- 25. Type switchport trunk allowed vlan <MGMT VLAN ID, CSV VLAN ID, iSCSI A VLAN ID, iSCSI B VLAN ID, Live Migration VLAN ID, VM Cluster Comm VLAN ID, VM Data VLAN ID>.
- 26. Type spanning-tree port type edge trunk.
- 27. Type no shut.
- 28. Type exit.
- 29. Type interface Po14.
- 30. Type switchport mode trunk.
- 31. Type switchport trunk native vlan <Native VLAN ID>.
- 32. Type switchport trunk allowed vlan <<MGMT VLAN ID, CSV VLAN ID, iSCSI A VLAN ID, iSCSI B VLAN ID, Live Migration VLAN ID, VM Cluster Comm VLAN ID, VM Data VLAN ID>.
- 33. Type spanning-tree port type edge trunk.
- 34. Type no shut.
- 35. Type exit.
- 36. Type copy run start.

#### Cisco Nexus 5548 B

- 1. From the global configuration mode, type interface Pol0.
- 2. Type switchport mode trunk.
- 3. Type switchport trunk native vlan <Native VLAN ID>.
- 4. Type switchport trunk allowed vlan <MGMT VLAN ID, CSV VLAN ID, iSCSI A, iSCSI B VLAN ID, VLAN ID, Live Migration VLAN ID, VM Cluster Comm VLAN ID, VM Data VLAN ID>.
- 5. Type spanning-tree port type network.
- 6. Type no shutdown.
- 7. Type exit.
- 8. Type interface Poll.
- 9. Type switchport mode trunk.
- 10. Type switchport trunk native vlan <MGMT VLAN ID>.
- 11. Type switchport trunk allowed vlan <<MGMT VLAN ID, iSCSI A VLAN ID, iSCSI B VLAN ID>.
- 12. Type spanning-tree port type edge trunk.
- 13. Type no shut.
- 14. Type exit.
- 15. Type interface Po12.
- 16. Type switchport mode trunk.
- 17. Type switchport trunk native vlan <MGMT VLAN ID>.
- 18. Type switchport trunk allowed vlan < iSCSI A VLAN ID>.



- 19. Type spanning-tree port type edge trunk.
- 20. Type no shut.
- 21. Type exit.
- 22. Type interface Po13.
- 23. Type switchport mode trunk.
- 24. Type switchport trunk native vlan <Native VLAN ID>.
- 25. Type switchport trunk allowed vlan <MGMT VLAN ID, CSV VLAN ID, iSCSI A VLAN ID, iSCSI B VLAN ID, Live Migration VLAN ID, VM Cluster Comm VLAN ID, VM Data VLAN ID>.
- 26. Type spanning-tree port type edge trunk.
- 27. Type no shut.
- 28. Type exit.
- 29. Type interface Pol4.
- 30. Type switchport mode trunk.
- 31. Type switchport trunk native vlan <Native VLAN ID>.
- 32. Type switchport trunk allowed vlan <<MGMT VLAN ID, CSV VLAN ID, iSCSI A VLAN ID, iSCSI B VLAN ID, Live Migration VLAN ID, VM Cluster Comm VLAN ID, VM Data VLAN ID>.
- 33. Type spanning-tree port type edge trunk.
- 34. Type no shut.
- 35. Type exit.
- **36.** Type copy run start.

#### **Configure Virtual PortChannels**

These steps provide details for configuring virtual PortChannels (vPCs).

#### Cisco Nexus 5548 A

- 1. From the global configuration mode, type vpc domain <Nexus vPC domain ID>.
- 2. Type role priority 10.
- Type peer-keepalive destination <Nexus B mgmt0 IP> source <Nexus A mgmt0 IP>.
- 4. Type exit.
- 5. Type interface Pol0.
- 6. Type vpc peer-link.
- 7. Type exit.
- 8. Type interface Poll.
- 9. Type vpc 11.
- 10. Type exit.
- 11. Type interface Po12.
- 12. Type vpc 12.



- 13. Type exit.
- 14. Type interface Po13.
- **15. Type** vpc 13.
- 16. Type exit.
- 17. Type interface Pol4.
- **18. Type** vpc 14.
- 19. Type exit.
- 20. Type copy run start.

#### Cisco Nexus 5548 B

- 1. From the global configuration mode, type vpc domain <Nexus vPC domain ID>.
- 2. Type role priority 20.
- Type peer-keepalive destination <Nexus A mgmt0 IP> source <Nexus B mgmt0 IP>.
- 4. Type exit.
- 5. Type interface Pol0.
- 6. Type vpc peer-link.
- 7. Type exit.
- 8. Type interface Poll.
- 9. Type vpc 11.
- 10. Type exit.
- 11. Type interface Po12.
- **12. Type** vpc 12.
- 13. Type exit
- 14. Type interface Po13.
- 15. Type vpc 13.
- 16. Type exit.
- 17. Type interface Po14.
- 18. Type vpc 14.
- 19. Type exit.
- 20. Type copy run start

#### Link into Existing Network Infrastructure

Depending on the available network infrastructure, several methods and features can be used to uplink the FlexPod environment. If an existing Cisco Nexus environment is present, NetApp recommends using vPCs to uplink the Cisco Nexus 5548 switches included in the FlexPod environment into the infrastructure. The previously described procedures can be used to create an uplink vPC to the existing environment.

#### Save the Configuration

Nexus A and Nexus B





Type copy run start.

### **Cisco Unified Computing System Deployment Procedure**

The following section provides a detailed procedure for configuring the Cisco Unified Computing System for use in a FlexPod environment. These steps should be followed precisely because a failure to do so could result in an improper configuration.

#### Perform Initial Setup of the Cisco UCS 6248 Fabric Interconnects

These steps provide details for initial setup of the Cisco UCS 6248 fabric Interconnects

#### Cisco UCS 6248 A

- 1. Connect to the console port on the first Cisco UCS 6248 fabric interconnect.
- 2. At the prompt to enter the configuration method, enter console to continue.
- 3. If asked to either do a new setup or restore from backup, enter setup to continue.
- 4. Enter y to continue to set up a new fabric interconnect.
- 5. Enter y to enforce strong passwords.
- 6. Enter the password for the admin user.
- 7. Enter the same password again to confirm the password for the admin user.
- 8. When asked if this fabric interconnect is part of a cluster, answer y to continue.
- 9. Enter A for the switch fabric.
- 10. Enter the cluster name for the system name.
- 11. Enter the Mgmt0 IPv4 address.
- 12. Enter the Mgmt0 IPv4 netmask.
- 13. Enter the IPv4 address of the default gateway.
- 14. Enter the cluster IPv4 address.
- 15. To configure DNS, answer y.
- 16. Enter the DNS IPv4 address.
- 17. Answer y to set up the default domain name.
- 18. Enter the default domain name.
- 19. Review the settings that were printed to the console, and if they are correct, answer yes to save the configuration.
- 20. Wait for the login prompt to make sure the configuration has been saved.

#### Cisco UCS 6248 B

- 1. Connect to the console port on the second Cisco UCS 6248 fabric interconnect.
- 2. When prompted to enter the configuration method, enter console to continue.
- 3. The installer detects the presence of the partner fabric interconnect and adds this fabric interconnect to the cluster. Enter y to continue the installation.
- 4. Enter the admin password for the first fabric interconnect.
- 5. Enter the Mgmt0 IPv4 address.
- 6. Answer yes to save the configuration.



7. Wait for the login prompt to confirm that the configuration has been saved.

#### Log into Cisco UCS Manager

These steps provide details for logging into the Cisco UCS environment.

- 1. Open a Web browser and navigate to the Cisco UCS 6248 fabric interconnect cluster address.
- 2. Select the Launch link to download the Cisco UCS Manager software.
- 3. If prompted to accept security certificates, accept as necessary.
- 4. When prompted, enter admin for the username and enter the administrative password and click Login to log in to the Cisco UCS Manager software.

#### Add a Block of IP Addresses for KVM Access

These steps provide details for creating a block of KVM ip addresses for server access in the Cisco UCS environment.

#### **Cisco UCS Manager**

- 1. Select the Admin tab at the top of the left window.
- 2. Select All > Communication Management.
- 3. Right-click Management IP Pool.
- 4. Select Create Block of IP Addresses.
- 5. Enter the starting IP address of the block and number of IPs needed as well as the subnet and gateway information.
- 6. Click OK to create the IP block.
- 7. Click OK in the message box.

#### Synchronize Cisco UCS to NTP

These steps provide details for synchronizing the Cisco UCS environment to the NTP server.

#### **Cisco UCS Manager**

- 1. Select the Admin tab at the top of the left window.
- 2. Select All > Timezone Management.
- 3. Right-click Timezone Management.
- 4. In the right pane, select the appropriate timezone in the Timezone drop-down menu.
- 5. Click Save Changes and then OK.
- 6. Click Add NTP Server.
- 7. Input the NTP server IP and click OK.

#### **Configure Unified Ports**

These steps provide details for modifying an unconfigured Ethernet port into a FC uplink port ports in the Cisco UCS environment.

**Note:** Modification of the unified ports leads to a reboot of the fabric interconnect in question. This reboot can take up to 10 minutes.



- 1. Navigate to the Equipment tab in the left pane.
- 2. Select Fabric Interconnect A.
- 3. In the right pane, click the General tab.
- 4. Select Configure Unified Ports.
- 5. Select Yes to launch the wizard.
- 6. Use the slider tool and move one position to the left to configure the last two ports (31 and 32) as FC uplink ports.
- 7. Ports 31 and 32 now have the "B" indicator indicating their reconfiguration as FC uplink ports.
- 8. Click Finish.
- 9. Click OK.
- 10. The Cisco UCSM GUI will close as the primary fabric interconnect reboots.
- 11. Upon successful reboot, open a Web browser and navigate to the Cisco UCS 6248 fabric interconnect cluster address.
- 12. When prompted, enter admin for the username and enter the administrative password and click Login to log in to the Cisco UCS Manager software.
- 13. Navigate to the Equipment tab in the left pane.
- 14. Select Fabric Interconnect B.
- 15. In the right pane, click the General tab.
- 16. Select Configure Unified Ports.
- 17. Select Yes to launch the wizard.
- 18. Use the slider tool and move one position to the left to configure the last two ports (31 and 32) as FC uplink ports.
- 19. Ports 31 and 32 now have the "B" indicator indicating their reconfiguration as FC uplink ports.
- 20. Click Finish.
- 21. Click OK.

#### **Edit the Chassis Discovery Policy**

These steps provide details for modifying the chassis discovery policy as the base architecture includes two uplinks from each fabric extender installed in the Cisco UCS chassis.

### Cisco UCS Manager

- 1. Navigate to the Equipment tab in the left pane.
- 2. In the right pane, click the Policies tab.
- 3. Under Global Policies, change the Chassis Discovery Policy to 2-link.
- 4. Click Save Changes in the bottom right corner.

#### **Enable Server and Uplink Ports**

These steps provide details for enabling Fibre Channel, server and uplinks ports.

#### **Cisco UCS Manager**

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 Unconfigured Ethernet Ports section.
- 4. Select the number of ports that are connected to the Cisco UCS chassis (2 per chassis), right-click them, and select Configure as Server Port.

8 8 1 >>1	🖥 Equipment 🔹 💼 Fabric I	Interconnects + 💷 P	abric Interc	vinect A (p	anany) + 🗰 Pice	d Nodule + -@ Unconfigur	ed Ethernet Ports	-C Uno
nt Servers LAN SAN VM Admin	configured Ethernet Port	8						-
Filter Al	ster = Export 25 Print							
50	Port ID	MAC	If Rg	ie .	If Type	Overal Status	Administrative State	
Louis Contraction of the second secon	1	\$4000000	Detel Unor	rhpured.	100ypesi	Autori Down	4 Deabed	1
e) Chasse •		\$477-02-00	debil Unco	fored		<ul> <li>Acmin Down</li> </ul>	Ended	
Rack-Hounts		5407F10E11C1	SHIGA UNION	figured	Physical	AdminiDown	8 Deabled	
- Ray FEX	-	provide the	der genegen and	foreil	(Truesday)	Admini Down	E Durbeit	
Servers 1	Enably			figured	Physical	V Stp Not Present	4 Disabled	
Fabric Diterconnects	Ditable			foured	Physical	V Sto Not Present	4 Disabled	
Fabric Interconnect A (primary)	Configure as G	tver Port		foured	Physical	V Sto Not Present	4 Disabled	
and Protocold	eveningurt at on	INTERNE STR		found	Physical	Sfp Not Present	4 Deabled	
Applance Form	Configure as th	plank Port		faced	Physical	V Sto Not Present	Disabled	-
Monitoron Effernet Parts	Configure at FC	oE Storage Port		fored	Physical	V Sto Not Present	A Disabled	
- Monitoring FC Ports	Continue at An	oliance Port		fored	Physical	Sto Not Present	4 Disabled	-
-d Server Parts				fored	Physical	V Sta Not Present	& Doubled	
-Storage FC Ports				forced	Divisional	T Statiot Present	A Dunbled	-
<ul> <li>B Anconfigurent Coherrent Partiel</li> </ul>	Copy		Ctrl+C	fored	Divisional	City Not Dessard	1 Deabled	
-Q Uplink Ethernet Ports	Conv XMI		Cutal	fored	Diversion	Clin Not Drasant	1 Deabled	- 12
- Uplink PC Ports	- copy rome		COL.	for and	Property.	Chattat Barrant	<ul> <li>Dealers</li> </ul>	- 15
III Fan Module 1	Defete		Ctrl+D	ngurea	Prysca	V stp not Present	Lisabled	-
E Fan Nodule 2	17	24 7 111 10.1	SUME /S LUNCO	inguned	pulace.	V SID NUL IMESERIE	<ul> <li>Disabled</li> </ul>	-
1 2 P2.4	18	0407418851361	INE 79 UNCO	inguned	РТурса	V stp Not Present	• Lisaored	_
Patric Diterconnect 8 (subordinate)	19	54:7P #E:1C1	194:74 Unco	nfigured	Physical	V Stp Net Present	Deabled	_
tanlinere flerte	20	54.7P#E11C:	04:75 Unco	nfigured	Physical	V Stp Not Present	Disabled	2
ECall Stocade Ports	21	54:7P1EE11C1	:04:7C Unca	figured	Physical	V Stp Not Present	Disabled	
Monitoring Ethernet Ports	22	54(7P)(EE)(1C)	:04:70 Unca	nfigured	Physical	V Sfp Not Present	Disabled	
Monitoring PC Ports	23	54:7P (8E) 1C:	:04:7E Unco	nfigured	Physical	Stp Not Present	Disabled	
-d Server Ports	24	54.开册:10:	04.不 Unco	ofigured	Physical	V Stp Not Present	Disabled	
- Storage FC Ports 1	25	54(不)担()()	04:80 Unce	nfgureit	Physical	Stp Not Present	4 Disabled	
🗟 Choonfigured Ethernet Ports 1	- 26	547F18:3C	04:81 Unco	nfigured	Physical	V Stp Not Present	Disabled	
- Uplink Ethernet Porta 1	27	547F3E:101	:04:82 Unco	figured	Physical	V Stp Not Present	Disabled	
- Uplink PC Ports 1	28	S4:7FIEE:1C:	04.83 Unco	figured	Physical	Sfp Not Present	Disabled	
Fan Module 1	29	54:7P-IEE:3C	04:84 Unco	figured	Physical	Sto Not Present	4 Disabled	-
E B Fan Nod, At 2		0.0			Contraction of the	110-01-0110-0110-01	and the second second	

5. A prompt displays asking if this is what you want to do. Click Yes, then OK to continue.



Fault S	ummary		0.	1 New - 9 Q	ptions 0 0	Arester	Activities 0	Dit				-j. d. case
0			>> <b>11</b> E	alphent + 💷 P	abric Interconnect	i na fabr	ic Interconnect /	A (primary) + 🛲 P	ixed Module 🕴 📲 Ser	ver Ports	-C Server I	Ports
Equipment	NT Servers LAN SAN VM	Admin	A Fiter	a Deport 100 P	rint.							
	Filter: Al		Set	Port ID	MAC	1f Role	IfType	Overall Status	Administrative State	License State	License Grace Pe	
+ =			1	1	54:7F:EE:1	Server	Physical	t Up	t Enabled	License Ok	0 *	
(2.4	U Chassis	24	1	2	\$4:7F:EE:1	Server	Physical	1 10	# Enabled	License Ok	0	
10 <b>4</b>	Rack-Mounts		1	3	54:7F:EE:1	Server	Physical	1 40	1 Enabled	License Ok	0	
1	FEX		1	4	\$4:7F:EE:1	Server	Physical	1 Up	1 Enabled	License Ok	0	
	Appkance Ports     Appkance Ports     Appkance Ports     Monitoring PDP     Monitoring PDP     Appkance Ports     Appkance     A	toris minit Ports forts torts Ports E subordinate) torts torts torts torts themet Ports Ports Statemet Ports Ports								Save Quar	per Reset Values	
¥.	11	124	1							1.055740.5077	ese film sources	į

- 6. Select ports 19 and 20 that are connected to the Cisco Nexus 5548 switches, right-click them, and select Configure as Uplink Port.
- 7. A prompt displays asking if this is what you want to do. Click Yes, then OK to continue.
- 8. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.
- 9. Expand the Unconfigured Ethernet Ports section.
- 10. Select ports the number of ports that are connected to the Cisco UCS chassis (2 per chassis), rightclick them, and select Configure as Server Port.
- 11. A prompt displays asking if this is what you want to do. Click Yes, then OK to continue.
- 12. Select ports 19 and 20 that are connected to the Cisco Nexus 5548 switches, right-click them, and select Configure as Uplink Port.
- 13. A prompt displays asking if this is what you want to do. Click Yes, then OK to continue.

#### Acknowledge the Cisco UCS Chassis

The connected chassis needs to be acknowledged before it can be managed by Cisco UCS Manager.

- 1. Select Chassis 1 in the left pane.
- 2. Click Acknowledge Chassis.





Cisco UCS Manager acknowledges the chassis and the blades servers in it.





#### Create Uplink PortChannels to the Cisco Nexus 5548 Switches

These steps provide details for configuring the necessary PortChannels out of the Cisco UCS environment.

- 1. Select the LAN tab on the left of the window.
- **Note:** Two PortChannels are created, one from fabric A to both Cisco Nexus 5548 switches and one from fabric B to both Cisco Nexus 5548 switches.
- 2. Under 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 PortChannel.
- 6. Enter vPC-13-N5548 as the name of the PortChannel.
- 7. Click Next.



Create Port Channel	
Unified C	Computing System Manager
Create Port Channel 1. √ Set Port Channel Name 2. ⊔ Add Ports	Set Port Channel Name
	ID= 13
	Name: vPC-13-85548
	<pre>     Read     Princh     Cancel </pre>

- 8. Select the port with slot ID: 1 and port: 19 and also the port with slot ID: 1 and port 20 to be added to the PortChannel.
- 9. Click >> to add the ports to the PortChannel.
- 10. Click Finish to create the PortChannel.
- 11. Select the check box for Show navigator for Port-Channel 13 (Fabric A)
- 12. Click OK to continue.
- 13. Under Actions, select Enable Port Channel.
- 14. In the pop-up box, click Yes, then  ${\tt OK}$  to enable.





- 15. Wait until the overall status of the Port Channel is up.
- 16. Click  $\ensuremath{\mathsf{OK}}$  to close the Navigator.





- 17. Under LAN Cloud, expand the Fabric B tree.
- 18. Right-click Port Channels.
- 19. Select Create Port Channel.
- 20. Enter 14 as the unique ID of the PortChannel.
- 21. Enter vPC-14-N5548 as the name of the PortChannel.
- 22. Click Next.
- 23. Select the port with slot ID: 1 and port: 19 and also the port with slot ID: 1 and port 20 to be added to the PortChannel.
- 24. Click >> to add the ports to the PortChannel.
- 25. Click Finish to create the PortChannel.
- 26. Select Check box for Show navigator for Port-Channel 14 (Fabric B).
- 27. Click OK to continue.
- 28. Under Actions, select Enable Port Channel.
- 29. In the pop-up box, click Yes, then OK to enable.
- 30. Wait until the overall status of the Port Channel is up
- 31. Click OK to close the Navigator.



#### **Create an Organization**

These steps provide details for configuring an organization in the Cisco UCS environment. Organizations are used as a means to organize and restrict access to various groups within the IT organization, thereby enabling multi-tenancy of the compute resources. This document does not assume the use of Organizations, however the necessary steps are included below.

#### Cisco UCS Manager

- 1. From the New... menu at the top of the window, select Create Organization.
- 2. Enter a name for the organization.
- 3. Enter a description for the organization (optional).
- 4. Click OK.
- 5. In the message box that displays, click OK.

#### **Create a MAC Address Pool**

These steps provide details for configuring the necessary MAC address pool for the Cisco UCS environment.

#### **Cisco UCS Manager**

- 1. Select the LAN tab on the left of the window.
- 2. Select Pools > root.

Note: One MAC address pool is created.

- 3. Right-click MAC Pools under the root organization .
- 4. Select Create MAC Pool to create the MAC address pool.



Fault Summary	Q D D New - Q Options Q 0	A Pending Relation       Ext	-0-0
🔕 🔻 🛆 🔬	a Hun Bran Ann Ma		III use seen data in
0 0 5 2	second and the second s	ec vois - M Mec Polic detaut	IN POAL POOL DETAUL
Equipment Servers UNI SAN VM Admin	General MAC Addresses   MACs   Paults   I	Exents	
Filter: Al 👻	Actions	Properties	
+ -	1 Delete	Nane: default	
VLANS *	Create a Block of MAC Addresses	Description:	
🗊 🚥 Fabric B	Show Pool Libage	Szmi 0	
Port Channels     Port Channel 14 (Fabric R)		August. C	
VLANS			
LAN Pin Groups			
III - 10 Threshold Policies			
H Applances			
🕀 📑 Internal LAN			
S Threshold Policies			
Section			
E-CLAN Cloud			
E Threshold Policies			
Connection Policies			
E Row Control Policies			
Second Seco			
E Threshold Policies			
vfilC Templates			
B A root			
D Pool (scsi-initiator-pool)			
MAC FOOL default			
A Sub-Organizators			Save Changes Reset Volues
m the mane musicing sessors			

- 5. Enter MAC\_Pool for the name of the MAC pool.
- 6. (Optional) Enter a description of the MAC pool.
- 7. Click Next.
- 8. Click Add.
- 9. Specify a starting MAC address.
- 10. Specify a size of the MAC address pool sufficient to support the available blade resources.

Create a Block of MAC Addresses		Q
First MAC Address: 00:25:B5:E1:26:B0 To ensure uniqueness of MACs in the LAN fabric, you are strongly encouraged to use the following MAC prefix: 00:25:B5:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Size:	100 🜩
	ОК	Cancel



- 11. Click OK.
- 12. Click Finish.
- 13. In the message box that displays, click OK.

#### **Create WWNN Pools**

These steps provide details for configuring the necessary WWNN pools for the Cisco UCS environment.

- 1. Select the SAN tab at the top left of the window.
- 2. Select Pools > root.
- 3. Right-click WWNN Pools
- 4. Select Create WWNN Pool.

Fault Summary	🕒 🍈 🖪 New - 🕞 Options	0 0 Aferding Accession 0 Ext	-di-di-
	>> = SAN + @ Pools + A roo	at + 🛞 WWMH Fools + 🛞 WWMH Pool node-default	🛞 WWWN Pool node-default
Equipment Servers LAN SAN VM Admin	General WWW Initiator Blocks 3	vitiators Faults Events	
Filter:     Al       SAN     SAN Ooud       SAN     Pabric A       Pabric A     Pabric B       SAN Drud     Pabric A       Pabric B     SAN Provention       SAN Drud     Pabric B       SAN Drud     Pabric B       SAN Drud     Pabric B       SAN Drud     Pabric B       SAN Druge Cloud     Pabric B       San Cloud     Pabric B       San Cloud     San Cloud       San Pabric B     San Cloud       San Second     San Cloud       San Cloud     San Cloud </th <th>Actions Delete Coate WWFi Black Coate WWFi Black Coate WWFi Black Coate WWFi Black Coate WWFi Black</th> <th>Properties Name: node-default Purpose: Node Www Assignment Desopton: Size: 0 Assgred: 0</th> <th></th>	Actions Delete Coate WWFi Black Coate WWFi Black Coate WWFi Black Coate WWFi Black Coate WWFi Black	Properties Name: node-default Purpose: Node Www Assignment Desopton: Size: 0 Assgred: 0	
			Save Chariges Reset Values

- 5. Enter WWNN Pool as the name of the WWNN pool.
- 6. (Optional) Add a description for the WWNN pool.
- 7. Click Next to continue.
- 8. Click Add to add a block of WWNN's.
- 9. The default is fine, modify if necessary.
- 10. Specify a size of the WWNN block sufficient to support the available blade resources.





- 11. Click OK to proceed.
- 12. Click Finish to proceed.
- 13. Click OK to finish.

#### **Create WWPN Pools**

These steps provide details for configuring the necessary WWPN pools for the Cisco UCS environment.

- 1. Select the SAN tab at the top left of the window.
- 2. Select Pools > root.
- 3. Two WWPN pools are created, one for fabric A and one for fabric B.
- 4. Right-click WWPN Pools
- 5. Select Create WWPN Pool.





- 6. Enter  ${\tt WWPN\_Pool\_A}$  as the name for the WWPN pool for fabric A.
- 7. (Optional). Give the WWPN pool a description.
- 8. Click Next.
- 9. Click Add to add a block of WWPNs.
- 10. Enter the starting WWPN in the block for fabric A.
- 11. Specify a size of the WWPN block sufficient to support the available blade resources.

Sreate WWWN BIOCK		(
From: 20:00:00:25:B5:D8:08:FF To ensure uniqueness of WWNs in the SAN fabric, you are strongly encouraged to use the following WWN prefix: 20:00:00:25:b5:xx:xx:xx	Size:	100 🜩



- 12. Click OK.
- 13. Click Finish to create the WWPN pool.
- 14. Click OK.
- 15. Right-click WWPN Pools
- 16. Select Create WWPN Pool.
- 17. Enter WWPN Pool B as the name for the WWPN pool for fabric B.
- 18. (Optional) Give the WWPN pool a description.
- 19. Click Next.
- 20. Click Add to add a block of WWPNs.
- 21. Enter the starting WWPN in the block for fabric B.
- 22. Specify a size of the WWPN block sufficient to support the available blade resources.
- 23. Click OK.
- 24. Click Finish.
- 25. Click OK to finish.

#### **Create UUID Suffix Pools**

These steps provide details for configuring the necessary UUID suffix pools for the Cisco UCS environment.

- 1. Select the Servers tab on the top left of the window.
- 2. Select Pools > root.
- 3. Right-click UUID Suffix Pools
- 4. Select Create UUID Suffix Pool.





- 5. Name the UUID suffix pool UUID\_Pool.
- 6. (Optional) Give the UUID suffix pool a description.
- 7. Leave the prefix at the derived option.
- $8. \quad Click \; {\tt Next} \; to \; continue.$
- 9. Click Add to add a block of UUID's
- 10. The From field is fine at the default setting.
- 11. Specify a size of the UUID block sufficient to support the available blade resources.

Crea	ate a E	llock	ofU	UID	Suffi	(es	0
From:	96E7-DD7 D	FE3F5FCD	<b>)7</b> S	iize:	100 💠		
						ОК	Cancel

12. Click OK.





13. Click Finish to proceed.

14. Click OK to finish.

#### **Create Server Pools**

These steps provide details for configuring the necessary UUID suffix pools for the Cisco UCS environment.

#### **Cisco UCS Manager**

- 1. Select the Servers tab at the top left of the window.
- 2. Select Pools > root.
- 3. Right-click Server Pools.
- 4. Select Create Server Pool.
- 5. Name the server pool Infra\_Pool.
- 6. (Optional) Give the server pool a description.
- 7. Click Next to continue to add servers.
- 8. Select two B200 servers to be added to the Infra\_Pool server pool. Click >> to add them to the pool.
- 9. Click Finish.

10. Select OK to finish.

#### Create VLANs

These steps provide details for configuring the necessary VLANs for the Cisco UCS environment.

#### **Cisco UCS Manager**

1. Select the LAN tab on the left of the window.

Note: Eight VLANs are created.

- 1. Select LAN Cloud.
- 2. Right-click VLANs.
- 3. Select Create VLANs.
- 4. Enter MGMT-VLAN as the name of the VLAN to be used for management traffic.
- 5. Keep the Common/Global option selected for the scope of the VLAN.
- 6. Enter the VLAN ID for the management VLAN. Keep the sharing type as none.
- 7. Click OK.



Create VLANs	×
Create VLANs	0
VLAN Name/Prefix: VM-Mgmt-VLAN   Common/Global Control Fabric A Control Both Fabrics Configured Differently	
You are creating global VLANs that map to the same VLAN IDs in all available fabrics. Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45") VLAN IDs: 805	
Sharing Type:  None Primary Isolated	
Check Overlap	OK Cancel

8. Right-click VLANs.

- 9. Select Create VLANs.
- 10. Enter CSV-VLAN as the name of the VLAN to be used for the CSV VLAN.
- 11. Keep the Common/Global option selected for the scope of the VLAN.
- 12. Enter the VLAN ID for the CSV VLAN.
- 13. Click OK.
- 14. Right-click VLANs.
- 15. Select Create VLANs.
- 16. Enter iSCSI-VLAN-A as the name of the VLAN to be used for the first iSCSI VLAN.
- 17. Keep the Common/Global option selected for the scope of the VLAN.
- 18. Enter the VLAN ID for the first iSCSI VLAN .
- 19. Click OK.





🚔 Create ¥LANs	×
Create VLANs	0
VLAN Name/Prefix: SCSI-Fabric-A Common/Global C Fabric A Fabric B Both Fabrics You are creating global VLANs that map to the same VLAN IDs in all available fabrics. Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45") VLAN IDs: 802 Sharing Type: None Primary Isolated	Configured Differently
	Check Overlap OK Cancel

20. Right-click  ${\tt VLANs}$  .

- 21. Select Create VLANs.
- 22. Enter iSCSI-VLAN-B as the name of the VLAN to be used for the second iSCSI VLAN.

23. Keep the Common/Global option selected for the scope of the VLAN.

24. Enter the VLAN ID for the second iSCSI VLAN.

25. Click OK.



🗼 Create VLANs	×
Create VLANs	0
VLAN Name/Prefix: iSCSI-Fabric-B	
Common/Global C Fabric A C Fabric B C Both Fabrics Configured Differently	
You are creating global VLANs that map to the same VLAN IDs in all available fabrics.	
Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")	
VLAN IDs: 807	
Sharing Type:  O None O Primary O Isolated	
Check Overlap OK Can	cel

- 26. Right-click VLANs.
- $27. \ Select \ \mbox{Create VLANs.}$
- 28. Enter Live Migration-VLAN as the name of the VLAN to be used for the live migration VLAN.
- 29. Keep the Common/Global option selected for the scope of the VLAN.
- 30. Enter the VLAN ID for the live migration VLAN.
- 31. Click OK, then OK.
- 32. Right-click VLANs.
- 33. Select Create VLANs.
- 34. Enter App-Cluster-Comm-VLAN as the name of the VLAN to be used for the VM CLuster VLAN.
- 35. Keep the Common/Global option selected for the scope of the VLAN.
- 36. Enter the VLAN ID for the VM Cluster VLAN.
- 37. Click OK.



🚔 Create VLANs	×
Create VLANs	0
VLAN Name/Prefix: App-Cluster-Comm Common/Global C Fabric A C Fabric B Both Fabrics Configured Differently Vou are creating global VLANs that map to the same VLAN IDs in all available fabrics. Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45") VLAN IDs: 806 Sharing Type: None Primary Isolated	
Check Overlap OK Ca	ancel

- 38. Right-click  ${\tt VLANs}$  .
- **39. Select** Create VLANs.
- 40. Enter VM-Data-VLAN as the name of the VLAN to be used for the VM data VLAN.
- 41. Keep the Common/Global option selected for the scope of the VLAN.
- 42. Enter the VLAN ID for the VM data VLAN.
- 43. Click OK.
- 44. Right-click VLANs.
- 45. Select Create VLANs.
- 46. Enter Native-VLAN as the name of the VLAN to be used for the Native VLAN.
- 47. Keep the Common/Global option selected for the scope of the VLAN.
- 48. Enter the VLAN ID for the Native VLAN.
- 49. Click OK.



🗼 Create VLANs	X
Create VLANs	0
VLAN Name/Prefix: Native Common/Global Pabric A Pabric B Both Fabrics Configured Differ You are creating global VLANs that map to the same VLAN IDs in all available fabrics. Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45") VLAN IDs: 2 Sharing Type: None Primary Isolated	ently
Check Overla	p OK Cancel

50. In the list of VLANs in the left pane, right-click the newly created Native-VLAN and select <code>Set as Native VLAN</code>.

51. Click Yes and OK.

#### **Create VSANs and SAN PortChannels**

These steps provide details for configuring the necessary VSANs and SAN PortChannels for the Cisco UCS environment. By default, VSAN 1 is used created and can be used. Alternate VSANs can be created as necessary.

- 1. Select the SAN tab at the top left of the window.
- 2. Expand the SAN Cloud tree.
- 3. Right-click VSANs.
- 4. Select Create VSAN.
- 5. Enter VSAN A as the VSAN name for fabric A.
- 6. Keep the Disabled option selected for the Default Zoning
- 7. Select Fabric A.



- 8. Enter the VSAN ID for fabric A.
- 9. Enter the FCoE VLAN ID for fabric A.
- 10. Click OK and then OK to create the VSAN.
- 11. Right-click VSANs.
- 12. Select Create VSAN.
- 13. Enter  $\ensuremath{\texttt{VSAN}\_B}$  as the VSAN name for fabric B.
- 14. Keep the Disabled option selected for the Default Zoning
- 15. Select Fabric B.
- 16. Enter the VSAN ID for fabric B.
- 17. Enter the FCoE VLAN ID for fabric B.
- 18. Click OK and then OK to create the VSAN.
- 19. Under SAN Cloud, expand the Fabric A tree.
- 20. Right-click FC Port Channels
- 21. Select Create Port Channel.
- 22. Click Yes and then enter 1 for the PortChannel ID and SPo1 for the PortChannel name.
- 23. Click Next.
- 24. Select ports 31 and 32 and click >> to add the ports to the PortChannel.
- 25. Click Finish.
- 26. Select the Check box for Show navigator for FC Port-Channel 1 (Fabric A)
- 27. Click OK to complete creating the PortChannel.
- 28. In the VSAN pull-down under Properties select the vsan VSAN A for fabric A.
- 29. Click Apply, then click OK.
- 30. Under Actions, click Enable Port Channel.
- 31. Click Yes and then OK to enable the Port Channel. This action also enables the two FC ports in the PortChannel.
- 32. Click OK to Close the Navigator.
- 33. Under SAN Cloud, expand the Fabric B tree.
- 34. Right-click FC Port Channels
- 35. Select Create Port Channel.
- 36. Click Yes, and then enter 2 for the PortChannel ID and SPo2 for the PortChannel name.
- 37. Click Next.
- 38. Select ports 31 and 32 and click >> to add the ports to the PortChannel.
- 39. Click Finish.
- 40. Select Check box for Show navigator for FC Port-Channel 1 (Fabric B)
- 41. Click OK to complete creating the PortChannel.
- 42. In the VSAN pull-down under Properties select VSAN\_B for fabric B.
- 43. Click Apply, then click OK.
- 44. Under Actions, click Enable Port Channel.



- 45. Click Yes, then OK to enable the PortChannel. This action also enables the two FC ports in the PortChannel.
- 46. Click OK to Close the Navigator.

#### Create a FC Adapter Policy for NetApp Storage Arrays

These steps provide details for a FC adapter policy for NetApp storage arrays..

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



- 4. Use Windows-NetApp as the name of the Fibre Channel Adapter Policy.
- 5. The default values are appropriate for most configurable items. Expand the Options dropdown. and set the Link Down Timeout (MS) option to 5000.
- 6. Click OK to complete creating the FC adapter policy
- 7. Click OK.





🌲 Create Fibre Channel Adaj	oter Policy			×
Create Fibre Cha	nnel Adapter P	olicy		0
		-		
Name:   Windows-Net/	Арр			
				_
Resources			8	
Options			8	
FCP Error Recovery:	Disabled C Enabled			
Flogi Retries:	8	[0-infinite]		
Flogi Timeout (ms):	4000	[1000-255000]		
Plogi Retries:	8	[0-255]		
Plogi Timeout (ms):	20000	[1000-255000]		
Port Down Timeout (ms):	30000	[0-240000]		
Port Down IO Retry:	30	[0-255]		
Link Down Timeout (ms):	5000	[0-240000]		
IO Throttle Count:	16	[1-1024]		
Max LUNs Per Target:	256	[1-1024]		
Interrupt Mode:	• Msi X C Msi C Intx			
			OK Can	el I

### Create a Firmware Management Package

These steps provide details for a firmware management policy for n the Cisco UCS environment.



- 1. Select the Servers tab at the top left of the window.
- 2. Select Policies > root.
- 3. Right Click Management Firmware Packages
- 4. Select create Management Firmware Package.
- 5. Enter VM-Host-Infra as the management firmware package name.
- 6. Select the appropriate packages and versions of the Server Management Firmware For servers that you have.
- 7. Click OK to complete creating the management firmware package.
- 8. Click OK.

Fault Summary	G 🕕 🛛 Her	v 🔹 😡 Qotions (	O Alminghi	Exit			-10- Em
	>> _ Jervers	Poldes • 🙏	noot • 🖾 Management	Firmware Packages		/ Management /	firmware Package
	Hanagemen	t Firmware Packag					
Equipment Servers LAN SAN VM Admin	Here day	ther - Export 123	Prant				
Filter: Al		and the second second	and a second			in the second	1
er es l	Thane	( ype	Vendor	Photos	Preserva	version	100
FC Adapter Policy Windows     FC Adapter Policy Windows NetApp     FC Adapter Policy default     FD Defaul							<b>日</b> 供 使
··· ∭ Sub-Organizations ⊕ ⊕ Pools	-					( personal processing of	(*)
(ii) (iii) Schedules						Save Changes	Reset Volumes



Marrier VPL-Hos	t-Infra					
0	C MARK	1				
schpbori:						
Mer = Export (5	8 Print					
ect	Vendor	Model	P90	Presence	Version	-
111	Cisco Systems Inc	Osco UCS 8230 M2	8230-8A5E-M2	N/A	<not set=""></not>	1.
10	Osco Systems Inc	Osco UCS 8440 MZ	8440-8ASE-M2	N/A	<not set=""></not>	1
13	Cisco Systems Inc	Osco UCS 8200 M1	N20-86620-1	N/A	<not set=""></not>	1
	Cisco Systems Inc.	Osco UCS 8250 M1	N20-06620-2	NIA	<not set=""></not>	1
3	Cisco Systems Inc	Cisco UCS 8200 M2	N20-86625-1	N/A	2.0(1s)	1
P	Osco Systems Inc	Osco UCS 8250 M2	N20-86625-2	N/A	<not set=""></not>	1
1	Cisco Systems Inc	Osco-UCS 8230 M1	N20-86730-1	N/A	<not set=""></not>	1
	Cisco Systems Inc	Cisco UCS 8440 M1	N20-86740-2	N/A	<not set=""></not>	1
1	Osco Systems Inc	Osco UCS C200 M1	R200-1120402	FUA	<not set=""></not>	1
6	Oaco Systems Inc	Clace UCS C209 M2	R200-1120402W	34/A	quot set>	1
	Osco Systems Inc.	Osco UCS C210 M1	R210-2121605	N/A	<not set=""></not>	1
1	Cisco Systems Inc	Osco UCS C210 MZ	R210-2121605W	NIA	<rul><li>anot set&gt;</li></rul>	1
100	Osco Systems Inc.	Cinco UCS C250 M1	R250-2480805	NIA	<notset></notset>	1
100	Cisco Systems Inc	Osco UCS C250 M2	R250-2480805W	NIA	<not set=""></not>	 1
	Land Systems Jrk	CHEO OLA CASO PA	F-237-6406038	700	Contracts	

#### **Create Firmware Package Policy**

These steps provide details for creating a firmware management policy for a given server configuration in the Cisco UCS environment. Firmware management policies allow the administrator to select the corresponding packages for a given server configuration. These often include adapter, BIOS, board controller, FC adapters, HBA option ROM, and storage controller properties.

- 1. Select the Servers tab at the top left of the window.
- 2. Select Policies > root.
- 3. Right Click Host Firmware Packages.
- 4. Select Create Host Firmware Package.
- 5. Enter the name of the host firmware package for the corresponding server configuration.
- 6. Navigate the tabs of the Create Host Firmware Package Navigator and select the appropriate packages and versions for the server configuration.
- 7. Click OK to complete creating the host firmware package.
- 8. Click OK.



Fault Summary	Q @ D New - Q Opt	ons   0 0   @red	did Activities 🛛 🔘	Exit			
S V 🛆	>> wije Servers + 🛞 Policier	• A root • S Host F	rmware Packages			1 Host Firm	nware Packages
	Host Firmware Packages						1
Equipment Servers LAN SAN VM Admin	庄 📇 🛋 Filter 🖨 Expo	rt 🚓 Print					
Filter: Al	Name	Type	Vendor	Model	Presence	Version	R.
Adapter Policy Univare     FC Adapter Policy Univers	Cisco Systems, in	c N20-866255erver 8 c N20-866255erver 8	, Cisco Systems, I.,	N20-66625-1	Present	55500.2.0.1d.0.09302.	
C Adapter Policy Vertault     C Adapter Policy Vertault     C SCSI Adapter Policy Vertault     S SCSI Adapter Policy Vertault     S StOS Policies     Default     S Dot Policy Adapter Policy Vertault     S Stor Policy Vertault     S Default     S Default     S Default     S Default     S Default     S Stor Policy Vertault     S Store Policy Vertau							(1) (1)
Management Firmware Packages     Management Firmware Packages     South Policies     Send over LAN Policies						Seve Changes	• eset Values



Faelt Summary	G D B	New - Contro		A Pariate Activities	() Evit				. dis
8 V A	>>Set	vers • 🐒 Policies	A root -	5 Host Firmware Packag	es + 🚿 VM-Host-In	fra		∭ WM	ene Host-brifte
Equipment Servers LAN CAN MA Admin	General	lventa							
	Actions	e	Propertie						
Filter: Al		and a second		and the state of the last					
de ci		CHIR.	-	e. www.mosc-initra					
	100 A	how Policy Usage		an prospective rest					
H Adapter Policies	Adapter	8105 Board Contr	oller FC Adap	HEA Option ROM	Storage Controller				
Eth Adapter Policy Linux	d, Filter	e Export ice Print							
- 1 Eth Adapter Policy VMWarePassThrv	Select	Vende	x.	Model	P2D	Presence	Version		-
SEth Adapter Policy Windows		Cisco :	Systems Inc.	Cisco UCS MS (R-8	N20-A80002	N/A	<not set=""></not>		
Eth Adapter Policy default		Cisco 5	systems Inc	CISCO UCS M81KR	N20-AC0002	Present	2.0(is)		
E FC Adapter Policy UNUM		Ceco	lystems Inc	Osco UC5 M73/R-E	N20-AE0002	N/A	<not.set></not.set>	13	
- I FC Adapter Policy Windows		Cisco 1	systems Inc	Osco UCS M72KR-E	N20-AE0102	74/A	<not set=""></not>		
- 5 PC Adapter Policy Windows-NetApp		Cisco	systems Inc	Cisco UCS N6 \$4R-1	N20-AI0102	N/A	knot set>		
- SFC Adapter Policy default		Cisco :	lystems Inc	Cisco UCS M71KR-Q	N20-AQ0002	N/A	<not set=""></not>		
5CSI Adapter Policy default		Cisco 1	Systems Inc	Cisco UCS M72KR-Q	N20-AQ0102	N/A	<not set=""></not>		
16-30 BIOS Defaults		Broade	om Corp.	Broadcom 10GbE Ad	N20X-ABPCI01	NJA	<not set=""></not>		
E 10 BIOS Pokces		Osco :	ystema Inc	Osco UCS P81E	N2XX-ACPCI01	N/A	<not set=""></not>		
T un anar taka		Emulei	Corp.	Emulex OCe10102+F	NZXX-AEPC201	N/A	<not set=""></not>		1 1 1 1
In- St Boot Policies		Intel C	orp.	Intel 10GbE Adapter	N2XX-AIPCI01	N/A	<not set=""></not>		10
Boot Policy default		Qlogic	Corp.	QLogic QLE8152	N2XX-AQPCI01	N/A	<riot set=""></riot>		
Boot Parky sag     Boot Parky sag     Boot Parky sag     Boot Parky subtry     Boot Parks     Boot Park     Default     D	_		_			ľ	Save Olavura	Repri	T



Fault Summary	3 10 11 New - 2 Opt	ors 0 0 Afenang Albenan	0 Exit			
	>> an Servers + S Polce	s + 🗛 root + 🌋 Host Firmware Packag	es + 🕮 VM-Host-Infr	a l	- 	M Host-Infra
	General Events					
Equipment Servers LAN SAN VM Admin	A. 4100	N BOULERS				
filter: Al	ACOURS	Propercies				
± =	Delette	Name: VM-Host-Infra				
A root A Sub-Organizations	Show Policy Usage	Description: Infrastructure Host				
Adapter Policies	Adapter BIOS Board Con	troller FC Adapters HBA Option ROM	Storage Controller			
Eth Adapter Policy Linux	A Piter - Export (S Pro	t.				
1 Eth Adapter Policy VMWarePassThrv	Select Ven	Sor Model	P2D	Presence	Version	-
SE Eth Adapter Policy Windows	E Coc	Systems, Inc. Cisco UCS 8230 M2	8230-8A5E-M2	N/A	<not set=""></not>	
- Si Eth Adapter Policy default	Cisco	Systems, Inc. Cisco UCS 8440 M2	8440-845E-M2	N/A	<riot set=""></riot>	-
FC Adapter Policy Unux     FC Adapter Policy UMWare     FC Adapter Policy Windows	E Cecz	Systems, Inc. Osco UCS 8200 M1	N20-86620-1	N/A	<rot set=""></rot>	
	Intel	Corp. Osco UCS 8200 M1	N20-86620-1	N/A	<not set=""></not>	•
- 5 PC Adapter Policy Windows-NetApp	Cscc	Systems, Inc. Cisco UCS 8250 M1	N20-86620-2	N/A	<not set=""></not>	•
- 10 PC Adapter Policy default	Intel	Corp. Cisco UCS 8250 M1	N20-86625-2	N/A	<rue set=""></rue>	•
- SCSI Adapter Policy default	V Cisc	o Systems, Inc. Cisco UCS 8200 H2	N20-86625-1	N/A	55500.2.0.1d.0	-
(8-30 BIOS Defaults	Cece	Systems, Inc. Cisco UCS 8250 M2	N20-86625-2	NIA	<not set=""></not>	•
E 10 BIOS Policies	E Osc	Systems, Inc. Osco UCS 8230 M1	N20-86730-1	PA/A	<not set=""></not>	-
- Xis Default	Cisco	Systems, Inc. Osco UCS 8440 M1	N20-86740-2	N/A	<not set=""></not>	•
ID: 40 Root Printers	Cocc	Systems, Inc. Cisco UCS C200 M1	R200-1120402	N/A	knot seto-	•
Boot Policy default	Cisco	Systems, Inc. Cisco UCS C200 M2	R200-1120402W	N/A	<riot set=""></riot>	•
Boot Policy dag	Cata	Systems, Inc. Osco UCS C210 M1	R210-2121605	N/A	<not set=""></not>	
- 1 Boot Policy utility	Caca	Systems, Inc. Osco UCS C210 M2	R210-2121605W	N/A	<not set=""></not>	•
Host Firmware Packages	E Cso	Systems, Inc. Cisco UCS C250 M1	R250-2480805	N/A	<not set=""></not>	•
- Default	Cec	Systems, Inc. Cisco UCS C250 M2	R250-2480805W	NA	<not set=""></not>	•
Bill Access Infiles     Bill Access Infiles     Bill Access Infiles     Bill Local Disk Config Polices     Bill Management Pirmare Packages     Bill Power Control Polices     Bill Scrub Polices	-			ſ	Save Changes Res	- et Values

#### Set Jumbo Frames and Enable Quality of Service in Cisco UCS Fabric

These steps provide details for setting Jumbo frames and enabling the quality of server in the Cisco UCS Fabric.

#### **Cisco UCS Manager**

- 1. Select the LAN tab at the top left of the window.
- 2. Go to LAN Cloud > QoS System Class.
- 3. In the right pane, click the General tab
- 4. On the Gold and Silver Priority, and Best Efforts row, type 9000 in the MTU boxes.
- 5. Click Save Changes in the bottom right corner.

#### 6. Click OK to continue.

Equipment Servers LAN SAN VM Admin	acment Servers LAN SAN VM Advin General Events FSM									
Filter: Al	Priority	Inabled	Co5	Packet Drop	Weight		Weight (%)	мти		Multicast Optimized
a -	Platinum	F	3	E.	10		N/A	normal		
	Gold	N.	4	N.	9		33	9000		
EF CLAN Cloud	Silver	R	2	R I	8		29	9000		
🗁 🚥 Pabric D	Bronze		1	V	2		N/A	normal		
Ort Channels	Best Effort	P	Any	E	5		18	9000		
VLANs OoS Switzen Class	Fibre Channe		3	Г	5	٠	20	fc.	٠	N/A

7. Select the LAN tab on the left of the window.




Servers     Exaument     Servers     Se	S Policies
0 0 4 Eautoment   Servers [LAN]   SAN   MA   Admin   filter: Al Name	
Esument Servers [LAN] SAN (M) Admin Filter: Al Admin Servers [LAN] SAN (M) Admin Admin Admin Servers [LAN] Servers [LAN] SAN (M) Admin Ad	
filter: Al Nane	
Nane Nane	
	10
AN	

8. Go to LAN > Policies > Root >

- 9. Right-click QoS Policies.
- 10. Select Create QoS Policy.
- 11. Enter LiveMigration as the QoS Policy name.
- 12. Change the Priority to Gold. Leave Burst (Bytes) set to 10240. Leave Rate (Kbps) set to line-rate. Leave Host Control set to None.
- 13. Click OK in the bottom right corner.



Create QoS Policy	X
Create QoS Policy	0
Name: LiveMigration	
Priority: Gold Burst(Bytes): 10240	
Rate(Kbps): line-rate Host Control:   None  Full	
	OK Cancel

- 14. Right-click QoS Policies.
- 15. Select Create QoS Policy.
- 16. Enter  $\ensuremath{\texttt{CSV}}$  as the QoS Policy name.
- 17. Change the Priority to Gold. Leave Burst (Bytes) set to 10240. Leave Rate (Kbps) set to line-rate. Leave Host Control set to None.
- 18. Click OK in the bottom right corner.

🗼 Create QoS Policy	×
Create QoS Policy	0
Name: CSV Egress Priority: Cold Burst(Bytes): 10240 Rate(Kbps): line-rate Host Control: None Full	
	OK Cancel

19. Right-click QoS Policies.





- 20. Select Create QoS Policy.
- 21. Enter iSCSI as the QoS Policy name.
- 22. Change the Priority to Silver. Leave Burst (Bytes) set to 10240. Leave Rate (Kbps) set to line-rate. Leave Host Control set to None.
- 23. Click OK in the bottom right corner.

🗼 Create QoS Policy	×
Create QoS Policy	Ø
Name: iSCSI	
Priority: Silver Burst(Bytes): 10240	
Rate(Kbps): line-rate Host Control:  None C Full	
[	OK Cancel

### **Create a Power Control Policy**

These steps provide details for creating a Power Control Policy for the Cisco UCS environment.

- 1. Select the Servers tab at the top left of the window.
- 2. Go to Policies > root.
- 3. Right-click Power Controller Policies.
- 4. Select Create Power Control Policy.
- 5. Enter No-Power-Cap as the power control policy name.
- 6. Change the Power Capping to No Cap.
- 7. Click OK to complete creating the host firmware package.
- 8. Click OK.



Fault Summary	🔾 🔘 🖬 New - ⊋ Options 🕡 🛈	Printing Activities   O Dat	-0-0
	>> - Servers + S Polices + A root +	S Power Control Policies	S Power Control Policies
	Power Control Policies Events	- Torreson and the second s	
Equipment, servers LAN, SAN, Will Admin	🕁 👝 🛋 Filter 🛥 Export 🚓 Print		
Fitteri Al	Name	Power Priority	in.
dbi       Image: Control of Control o	- E orfault	5	Start Careto
4 III +	II		and on the II and the



Create Po	wer Control Pol	icy				×
Create	Power C	ontrol Po	licy			0
Name:	No-Power-Ca	0				
If you cho its power not	opping tose cap, the se group. Priority v o-cap, the serve	rver is allocated a alues range from 1 r is exempt from a	certain amount o to 10, with 1 be Ill power capping.	f power based on it: ing the highest prior	s priority w ity. If you	vithin
O Cisco UCS M power than i their priority	Capi 🕜 cap anager only enfo is currently availa	rces power cappin ble. With sufficien	g when the serve t power, all serve	ers in a power group ers run at full capaci	o require m ty regardle	ore ess of
				[	ок	Cancel

## **Create a Local Disk Configuration Policy**

These steps provide details for creating a local disk configuration for the Cisco UCS environment, which is necessary if the servers in question do not have a local disk.

**Note:** This policy should not be used on blades that contain local disks.

- 1. Select the Servers tab on the left of the window.
- 2. Go to 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. Uncheck the Protect Configuration box.
- 7. Click OK to complete creating the host firmware package.
- 8. Click OK.



Fault Summary	😡 🌚 🖽 New - 😡 Qotions 😜 🛛 🛕 Tranko Katrina	Exit	-di-di-
8 V A	Secure 1 Secure 1 A mot 1 Stand Det Carlo Pale	101	S Local Disk Config Policies
0 0	Local Disk Config Policies		20 King over Guild Lange
Equipment Servers LAN SAN VM Admin	🚓 👝 🛋 Filter 🛥 Export 🚓 Print		
Filter: Al	Name	Made	10
del mail       A root         A sub-Organizations       Sub-Organizations         Sub-Organization       Sub-Organizations         Sub-Organizations       Sub-Organizations         Sub-Organization       Sub-Organizations         Sub-Organizations       Sub-Organizations         Sub-Organizations       Sub-Organizations         Sub-Organizations       Sub-Organizations         Sub-Organizations       Sub-Organizations         Sub-Organizations       Sub-Organizations         Sub-Organizations       Sub-Organizations	S Local Disk Configuration Policy default	Any Configuration	
4	10	1	save charges 11 repet values



Create Local Disk Configuration Policy	X
Create Local Disk Configuration Policy	0
Name:       SAN-Boot         Description:          Mode:       No Local Storage         Protect Configuration is set, the Local Disk Configuration is preserved on disassociation.         On reassociation of the same Server, a configuration error will be raised         if the new Local Disk Configuration is different.	Cancel
	Cancer

## **Create a Server Pool Qualification Policy**

These steps provide details for creating a server pool qualification policy for the Cisco UCS environment.

- 1. Select the Servers tab on the left of the window.
- 2. Go to Policies > root.
- 3. Right-click Server Pool Qualification Policies.



- 4. Select Create Server Pool Policy Qualification.
- 5. Select Server Model Qualifications.
- 6. Enter B200 M2 as the Model(RegEx).
- 7. Click OK to complete creating the host firmware package.
- 8. Click OK.



### **Create a Server BIOS Policy**

These steps provide details for creating a server BIOS policy for the Cisco UCS environment.



- 1. Select the Servers tab on the left of the window.
- $2. \quad Go \ to \ {\tt Policies} \ > \ {\tt root}.$
- 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 property to Disabled.
- 7. Click Finish to complete creating the BIOS policy.
- 8. Click OK.

Fault Summary	G @ B New - Cobors 0 0 Alexandra Control 0 Exit	-0de-
	>> aug Servers 1 III Polices 1 A root 1 III BLOS Polices	E BLOS Policies
	6005 Polices Puerts	
Equipment, Servers LAN SAN VM Admin	the indication of the Prot	
Filter: Al 🗸		m
e a	B- A root	
A root:     A cost:     A cost:     Adopter Policy Univer     Second Secon		Tarie Changes Reset Values
S) VAEC/VHBA Placement Policies		Save Charges   Reset Values





eate BIOS Policy	Main	
<ol> <li>Processor</li> <li>Intel Directed IO</li> <li>RAS Memory</li> <li>Serial Port</li> <li>USB</li> <li>PCI Configuration</li> <li>Boot Options</li> <li>Server Management</li> </ol>	Name: VM-Host-Infra Reboot on BIOS Settings Change: Quiet Boot: Quiet Boot: Outer Dost Error Pause: Stay-off I last-state • reset • Platform Default Resume Ac On Power Loss: Stay-off I last-state • reset • Platform Default Front Panel Lockout: ACPI 10 Support disabled • enabled • Platform Default ACPI 10 Support Stay-off • last-state • reset • Platform Default Control Panel Lockout: Control	

## **Create vNIC/HBA Placement Policy for Virtual Machine Infrastructure Hosts**

- 1. Right-click vNIC/HBA Placement policy and select create.
- 2. Enter the name VM-Host-Infra.
- 3. Click 1 and select Assign Only.
- 4. Click OK.



📥 Create Place	ement Policy				×
Create P	Placement Po	olicy			0
Name: VM-Ho	ost-Infra	_			
Virtual Slot 1 2 3 4	Selection Preference All All Assigned Only Exclude Dynamic Exclude Unassigned				
				ОК	Cancel

### **Create a vNIC Template**

These steps provide details for creating multiple vNIC templates for the Cisco UCS environment.

- 1. Select the LAN tab on the left of the window.
- 2. Go to Policies > root.
- 3. Right-click vNIC Templates.



Fault Summary	Q 0 0 New - Q Qo	tons   😧 🛛   🛕 (=======   🔟 t	vit.	-0 610
	>> = LAN + SPolder	A root + I vill vill Templates		VNIC Templates
Constant and and and	villC Templates			
Equipment   Servers LAM   SAN   VM   Admin	1 - A File	art 🚓 Print		
Filter: Al	Name	VLAN	Native VLAN	R
18 C				
LAN Cloud CLAN Cloud CLAN Cloud Classics C		Add 🏾		
III IIII Irathc Monitoring Sessions			178222	Names   Restart tid or
e			parte o	andra II neser sance

- 4. Select Create vNIC Template.
- 5. Enter CSV as the vNIC template name.
- 6. Leave Fabric A checked. Check the Enable Failover box. Under target, unselect the VM box. Select Updating Template as the Template Type. Under VLANs, select CSV VLAN and set as Native VLAN. Under MTU, enter 9000. Under MAC Pool:, select default. Under QOS Policy: select CSV.
- 7. Click OK to complete creating the vNIC template.
- 8. Click OK.

# ...... CISCO



х

## 📥 Create vNIC Template

Create vNIC Te	emplate		0
Name: C Description:	S Fabric A C Eabric B 🔽 Epable E	ailover	
- Warning	Target ✓ Adapter ✓ VM		
If <b>VM</b> is selected, a port p If a port profile of the sar Template Type:	profile by the same name will be creat ne name exists, and updating templat Initial Template C Updating Temp	ed. e is selected, it will be overwrit plate	ten
Select	Name	Native VLAN	<b>₽</b>
	default	0	
	App-Cluster-Comm	0	
	CSV-VLAN	•	
	LiveMigration-VLAN	0	<b></b>
Create VLAN	000		
Warning Make sure that the MTU h corresponding to the Egre	as the same value in the <u>QoS System</u> iss priority of the selected QoS Policy.	<u>Class</u>	
MAC Pool: de	fault 💌		
QoS Policy: C	5V 🔽		
Network Control Policy:	not set> 🔻		
Pin Group: <	not set> 🔻		
Stats Threshold Policy: de	fault		
			OK Cancel

9. Select the LAN tab on the left of the window.

10. Go to Policies > root.

11. Right-click vNIC Templates.



- 12. Select Create vNIC Template.
- 13. Enter LiveMigration as the vNIC template name.
- 14. Check Fabric B. Check the Enable Failover box. Under target, unselect the VM box. Select Updating Template as the Template Type. Under VLANs, select Live-Migration-VLAN and set as Native VLAN. Under MTU, enter 9000. Under MAC Pool:, select Default. Under QoS Policy, select Live-Migration.
- 15. Click OK to complete creating the vNIC template.
- 16. Click  $\ensuremath{\mathsf{OK}}$  .



				and the second se	
reate vNIC	Templa	te			
Name:	LiveMigrat	ion			
Description:	UR				
Fabric ID:	C Fabric A	Fabric B      Enat	ole Failover		
i statestica (	D				
		4			
	VM				
	L				
Warning					
If VM is selected, a po If a port profile of the	rt profile by th same name ex	ne same name will be o dists, and updating tem	reated. Inlate is selected, it will be ove	rwritten	
in a port prome of the	same name er		place is selected, it will be ove	, mitteri	
Template Type:	<ul> <li>Initial Te</li> </ul>	mplate 🜔 Updating T	emplate		
VLANs					
Select	Na	me	Native VLAN	R.	
	def	ault	0		
	(2)	/-VLAN	0	E	
	(3)			TOTOTOTOTOTOTOTOTOTOTO (	
	Live	Migration-VLAN	٢		
	Live	Migration-VLAN Data-VLAN	<u> </u>	-	
Create VLAN	Live	Migration-VLAN Data-VLAN		•	
Create VLAN	9000	Migration-VLAN Data-VLAN			
Create VLAN MTU:	9000	Migration-VLAN Data-VLAN			
Create VLAN MTU: Warning Make sure that the MTU	9000 D U has the sam	Migration-VLAN Data-VLAN e value in the <u>QoS Sys</u>	e Class		
Create VLAN MTU: Warning Make sure that the MTI corresponding to the E	9000 D U has the sam	Migration-VLAN Data-VLAN the value in the <u>QoS Sys</u> of the selected QoS Po	e Class		
Create VLAN MTU: Warning Make sure that the MTI corresponding to the E MAC Pool:	9000 D U has the sam gress priority default	Migration-VLAN Data-VLAN e value in the <u>QoS Sys</u> of the selected QoS Po	etem Class		
Create VLAN MTU: Warning Make sure that the MTU corresponding to the E MAC Pool: OoS Policy:	9000 D U has the sam gress priority default D LiveMigration	Migration-VLAN Data-VLAN e value in the <u>QoS Sys</u> of the selected QoS Po	item Class		
Create VLAN Create VLAN MTU: Warning Make sure that the MTI corresponding to the E MAC Pool: QoS Policy: Network Control Policy:	9000 D U has the sam gress priority default D LiveMigratior (ont set>	Migration-VLAN Data-VLAN e value in the <u>QoS Sys</u> of the selected QoS Po	e Class stem Class		
Create VLAN  TU:  Warning  Make sure that the MTU corresponding to the E  MAC Pool: QoS Policy:  Network Control Policy: Pin Group:	9000 D D U has the sam gress priority default D LiveMigratior C (not set>	Migration-VLAN Data-VLAN e value in the <u>QoS Sys</u> of the selected QoS Pro	e Class olicy.		
Create VLAN TU: Warning Make sure that the MTI corresponding to the E MAC Pool: QoS Policy: Vetwork Control Policy: Pin Group: Stats Threshold Policy:	9000 D U has the sam gress priority default LiveMigration <not set=""> <not set=""> default</not></not>	Migration-VLAN Data-VLAN e value in the <u>QoS Sys</u> of the selected QoS Po	e tem Class blicy.		
Create VLAN	9000 D D U has the sam gress priority default D LiveMigratior C <not set=""> <not set=""> default</not></not>	Migration-VLAN Data-VLAN e value in the <u>QoS Sys</u> of the selected QoS Pro	etem Class Slicy.		

17. Select the  ${\tt LAN}$  tab on the left of the window.

18. Go to Policies > root.





- 19. Right-click <code>vNIC Templates</code>.
- 20. Select Create vNIC Template.
- 21. Enter VM-MGMT as the vNIC template name.
- 22. Check Fabric A. Check the Enable Failover box. Under target, unselect the VM box. Select Updating Template as the Template Type. Under VLANs, select MGMT-VLAN. Set as Native VLAN. Under MAC Pool:, select MAC Pool.
- 23. Click OK to complete creating the vNIC template.
- 24. Click OK.



📥 Create vNIC Template				×
Create vNIC Temp	late			Ø
Name: VM-Mgr	mt			
Description:				
Fabric ID: 💽 Fabr	ic A 🔿 Fabric B 🔽 Enab	le Failover		
Target	:			
🔽 Ada	pter			
I VM				
Warning				
If <b>VM</b> is selected, a port profile t	by the same name will be cr	eated.		
If a port profile of the same nam	e exists, and updating tem	plate is selected, it will be overwrit	ten	
Template Type: 💿 Initia	al Template 🔘 Updating Te	emplate		
VLANs				
Select	Name	Native VLAN	E.	
	VM-Data-VLAN	0		
	VM-Mgmt-VLAN	O		
	iSCSI-Fabric-A	0		
	iSCSI-Fabric-B	0	<u> </u>	
+ Create VLAN				
MTU: 1500	]			
MAC Pool: default	-			
QoS Policy: <pre></pre>	> 🔻			
Network Control Policy: <not set<="" td=""><td>&gt; 🔻</td><td></td><td></td><td></td></not>	> 🔻			
Pin Group: <not set<="" td=""><td>&gt; 🔻</td><td></td><td></td><td></td></not>	> 🔻			
Stats Threshold Policy: default	-			
			ОК	Cancel

25. Select the LAN tab on the left of the window.

- **26.** Go to Policies > root.
- 27. Right-click <code>vNIC Templates</code>.
- 28. Select Create vNIC Template.



- **29.** Enter App-Cluster-Comm as the vNIC template name.
- 30. Check Fabric B. Check the Enable Failover box. Under target, unselect the VM box. Select Updating Template as the Template Type. Under VLANs, select App-Cluster-Comm. Do not set a Native VLAN. Under MTU, enter 1500. Under MAC Pool, select default.
- 31. Click OK to complete creating the vNIC template.
- 32. Click  $\ensuremath{\mathsf{OK}}$  .



📥 Create vNIC Templa	te					×
Create vNIC	Templ	ate				0
Name:	App-Clust	ter-Comm				
Description:						
Fabric ID:	🔿 Fabric	A 💿 Fabric I	B 🔽 Enable Fai	lover		
(	i) - Target -			]		
	Adapt	er		-		
	🗖 VM					
Warping						
If VM is selected, a no	rt profile by	the same nar	ne will he creater	4.		
If a port profile of the	same name	exists, and up	dating template	is selected, it will be overwr	ritten	
	Contractor 1	remelate C	_ J_L' T			
Iemplate Type:	D Tuiciai I	i emplace		<u>ace</u>		
VLANs				1		
Select		N	ame	Native VLAN	<b></b>	
	a 0	erault 	2000	0	<b>^</b>	
		SV-VLAN		0		
	Li	iveMigration-V	'LAN	0	<b>_</b>	
	1			· -		
Create VLAN	4500					
MIU:	1500					
MAC Pool:	default D	•				
QoS Policy:	<not set=""></not>	•				
Network Control Policy:	<not set=""></not>	•				
Pin Group:	<not set=""></not>	-				
Stats Threshold Policy:	default	-				
					Or	Cancel
						Cancer

33. Select the LAN tab on the left of the window.

- 34. Go to Policies > root.
- 35. Right-click <code>vNIC Templates</code>.
- 36. Select Create vNIC Template.
- 37. Enter VM-Data as the vNIC template name.



- 38. Check Fabric A. Check the Enable Failover box. Under target, unselect the VM box. Select Updating Template as the Template Type. Under VLANs, select VM. Do not set a Native VLAN. Under MAC Pool, select Default.
- 39. Click OK to complete creating the vNIC template.
- 40. Click OK.

Create vNIC	Temp	late			6
Name:	VM-Data D	a			
Description:			10	_	
Fabric ID;	• Fabri	c A 💿 Fabric B 🔽 Enal	ble Failover		
	D Target				
	🗸 Adap	oter			
	VM				
Warning	· · · · ·				
terma a selected a se	rt profile b	v the same name will be c	reated.		
IT VPLIS SElected, a DO					
If a port profile of the	same name	e exists, and updating ten	nplate is selected, it will be over	rwritten	
If a port profile of the	same name	e exists, and updating ten	nplate is selected, it will be over	rwritten	
If a port profile of the s	same name	e exists, and updating ten	nplate is selected, it will be over Template	rwritten	
If opert profile of the s Template Type:	same name O Initial D	e exists, and updating ten	nplate is selected, it will be over Template	rwritten	
If verifies selected, a po If a port profile of the s Template Type: VLANs Select	same name O Initial D	e exists, and updating ten	nplate is selected, it will be over Template Native VLAN	rwritten	
Template Type: VLANs	same name	e exists, and updating ten I Template	nplate is selected, it will be over	rwritten	
Template Type:	same name	e exists, and updating ten I Template  Updating Name default CSV-VLAN	Native VLAN	rwritten	
Template Type: VLANs Select	Same name	e exists, and updating ten I Template O Updating <sup>1</sup> Name default CSV-VLAN LiveMigration-VLAN VM-Data-VLAN	Native VLAN	rwritten	
If verifies selected, a point of the selected of the select selec	same name	e exists, and updating ten I Template Name default CSV-VLAN LiveMigration-VLAN VM-Data-VLAN	Native VLAN	rwritten	
If verifies selected, a po If a port profile of the s Template Type: VLANS Select Select Create VLAN	same name	e exists, and updating ten I Template  Updating Name default CSV-VLAN LiveMigration-VLAN VM-Data-VLAN	Native VLAN	rwritten	
If verifies selected, a po If a port profile of the s Template Type: VLANS Select Create VLAN MTU:	Same name	e exists, and updating ten I Template  Dpdating  Name default CSV-VLAN LiveMigration-VLAN VM-Data-VLAN	nplate is selected, it will be over	rwritten	
If verifies selected, a po If a port profile of the s Template Type: VLANS Select Create VLAN MTU: MAC Pool:	1500	e exists, and updating ten I Template Name default CSV-VLAN LiveMigration-VLAN VM-Data-VLAN	Native VLAN	rwritten	
Template Type: Template Type: VLANS Select Create VLAN MTU: QoS Policy:	1500 default cont set:	e exists, and updating ten ITemplate O Updating Name default CSV-VLAN LiveMigration-VLAN VM-Data-VLAN	nplate is selected, it will be over	rwritten	
If verifies selected, a po If a port profile of the s Template Type: VLANS Select Create VLAN MTU: MAC Pool: QoS Policy: Network Control Policy:	1500 default () <not set:<="" td=""><td>e exists, and updating ten I Template  Updating Name default CSV-VLAN LiveMigration-VLAN VM-Data-VLAN</td><td>Native VLAN</td><td>rwritten</td><td></td></not>	e exists, and updating ten I Template  Updating Name default CSV-VLAN LiveMigration-VLAN VM-Data-VLAN	Native VLAN	rwritten	
If verifies selected, a po If a port profile of the s Template Type: VLANS Select Create VLAN MTU: MAC Pool: QoS Policy: Network Control Policy: Pin Group:	1500 default conot set: <not set:<="" td=""><td>e exists, and updating ten I Template  Updating Name default CSV-VLAN LiveMigration-VLAN VM-Data-VLAN</td><td>nplate is selected, it will be over</td><td>rwritten</td><td></td></not>	e exists, and updating ten I Template  Updating Name default CSV-VLAN LiveMigration-VLAN VM-Data-VLAN	nplate is selected, it will be over	rwritten	
If verifies selected, a po If a port profile of the s Template Type: VLANS Select Create VLAN MTU: MAC Pool: QoS Policy: Network Control Policy: Pin Group: Stats Threshold Policy:	1500 default onot set: <not set:<br="">default</not>	e exists, and updating ten I Template  Updating Name default CSV-VLAN LiveMigration-VLAN VM-Data-VLAN	nplate is selected, it will be over	rwritten	



- 41. Select the LAN tab on the left of the window.
- 42. Go to Policies > root.
- 43. Right-click vNIC Templates.
- 44. Select Create vNIC Template.
- 45. Enter iSCSI-A as the vNIC template name.
- 46. Check Fabric A. Uncheck the Enable Failover box. Under target, unselect the VM box. Select Updating Template as the Template Type. Under VLANS, select iSCSI-VLAN-A. Do not set a Native VLAN. Under MTU, enter 9000. Under MAC Pool, select MAC\_Pool. Under QoS Policy, select iSCSI.
- 47. Click OK to complete creating the vNIC template.
- 48. Click OK.



🚔 Create vNIC Template				×
Create vNIC Temp	late			0
Name: iSCSI-Fa	abric-A			
Description:			1	
e Li zo la celu	a Al Constant Di Castella Cata			
	ICA O Fabrico   Chable Fallo	Jver		
Target				
Ada	pter			
Warning				
If <b>VM</b> is selected, a port profile t	by the same name will be created.	selected it will be overwritten		
In a port prome or the same ham	e exists, and apadeing template is			
Template Type: 💿 Initia	l Template 🔘 Updating Templat	e		
VLANs				
Select	Name	Native VLAN	<b>₽</b>	
	PXE-Boot	0		
	VM-Data-VLAN	0		
	VM-Mgmt-VLAN	<u> </u>		
	ISCSI-VLAN	0	<b>_</b>	
🛨 Create VLAN				
MTU: 9000				
Warning				
Make sure that the MTU has the	same value in the <u>QoS System Cl</u> . rity of the selected QoS Policy	ass		
corresponding to the Egress pho	ncy of the selected QOS Policy.			
MAC Pool: default	-			
QoS Policy: iSCSI	•			
Network Control Policy: <not set<="" td=""><td>&gt; •</td><td></td><td></td><td></td></not>	> •			
Pin Group: <not set<="" td=""><td>&gt; •</td><td></td><td></td><td></td></not>	> •			
Stats Threshold Policy: default	▼			
			OK	Cancel

49. Select the LAN tab on the left of the window.

- 50. Go to Policies > root.
- 51. Right-click vNIC Templates.



- 52. Select Create vNIC Template.
- **53.** Enter **i**SCSI-B as the vNIC template name.
- 54. Check Fabric B. Uncheck the Enable Failover box. Under target, unselect the VM box. Select Updating Template as the Template Type. Under VLANS, select iSCSI-VLAN-B. Do not set a Native VLAN. Under MTU, enter 9000. Under MAC Pool, select MAC\_Pool. Under QoS Policy, select iSCSI.
- 55. Click OK to complete creating the vNIC template.
- 56. Click  $\ensuremath{\mathsf{OK}}$  .



reate vNIC	Templat	e		
		20		
Name:	iSCSI-Fabric	c-B		
Description:	1			
Fabric ID:	C Fabric A		ailover	
	Target			
	Adapter		_	
	VM			
	1			
Warning				
If VM is selected, a po	rt profile by th	e same name will be creat	ed.	
If a port profile of the	same name exi	ists, and updating templat	e is selected, it will be overwrit	ten
Template Type:	Initial Ten	nplate C Updating Tem	blate	
VLANS		2011		
Select		Name	Native VLAN	<b></b>
	PXE	-Boot	0	<u> </u>
	VM-	Data-VLAN	C	
	VM-I	Mgmt-VLAN	0	
	VM-I ISCS	Mgmt-Vlan 5I-Vlan	<u> </u>	<b>•</b>
Create VLAN	VM-I iSCS	Mgmt-VLAN 51-VLAN	C	<b>•</b>
Create VLAN	VM- 15C5	Mgmt-VLAN 51-VLAN	C	
Create VLAN MTU:	VM-1 iSCS 9000	Mgmt-VLAN 5I-VLAN	C	
Create VLAN Warning Make sure that the MT	9000	Mgmt-VLAN 3I-VLAN	Class	
Create VLAN MTU: Warning Make sure that the MT corresponding to the E	9000 U has the same gress priority of	Mgmt-VLAN 5I-VLAN e value in the <u>QoS System</u> of the selected QoS Policy	<u>Class</u>	
Create VLAN MTU: Warning Make sure that the MT corresponding to the E	9000 D U has the same gress priority o	Mgmt-VLAN 5I-VLAN e value in the <u>QoS System</u> of the selected QoS Policy	Class	
Create VLAN MTU: Warning Make sure that the MT corresponding to the E MAC Pool:	9000 D U has the same gress priority o default	Mgmt-VLAN 5I-VLAN e value in the <u>QoS System</u> of the selected QoS Policy	<u>Class</u>	
Create VLAN TU: Warning Make sure that the MT corresponding to the E MAC Pool: QoS Policy:	9000 U has the same gress priority of default ISCSI	Mgmt-VLAN 5I-VLAN e value in the <u>QoS System</u> of the selected QoS Policy	(Closs	
Create VLAN MTU: Warning Make sure that the MT corresponding to the E MAC Pool: QoS Policy: letwork Control Policy:	U has the same gress priority of default ISCSI (not set>	Mgmt-VLAN 5I-VLAN e value in the <u>QoS System</u> of the selected QoS Policy	(Class	
Create VLAN MTU: Warning Make sure that the MT corresponding to the E MAC Pool: QoS Policy: letwork Control Policy: Pin Group:	VM- iSCS U has the same gress priority of default iSCSI (not set> <not set=""></not>	Mgmt-VLAN 5I-VLAN e value in the <u>QoS System</u> of the selected QoS Policy	(Class	
Create VLAN MTU: Warning Make sure that the MT corresponding to the E MAC Pool: QoS Policy: Jetwork Control Policy: Pin Group: Stats Threshold Policy:	VM- iSCS 0 U has the same gress priority of default 0 SCSI 0 <not set=""> <not set=""> default</not></not>	Mgmt-VLAN 5I-VLAN e value in the <u>QoS System</u> of the selected QoS Policy • • • •		

## Create vHBA Templates for Fabric A and B

These steps provide details for creating multiple vHBA templates for the Cisco UCS environment.



- 1. Select the VSAN tab on the left of the window.
- 2. Go to Policies > root.
- 3. Right-click vHBA Templates.

Fault Summary	😧 🌑 💀 New + 😥 Options 😥 O 🔺 Antonio Activities 🔟 Exit	dud- tuteo
	>> = SAN + SProices + A root + B vrBA Templates	*+EA Templates
Equipment Servers LAN SAN VM Admin	vittA Templates	
niter: Al	In C. wooder (gerein)	
	Nane :	
FC Adapter Polcy Windows NetApp     FC Adapter Polcy Windows NetApp     FC Adapter Polcy default     Foreshold Polces     Foreshold Polces     Foreshold Polce     Foreshold Polce     Foreshold Polce     Foreshold Polce     Foreshold Polce     Foreshold Polce     FC Adapter Polce     FC Adapter Polce     FC Adapter Polce     FT - 20     FC Adapter Polce     FT     FC Adapter Polce     FC Adapter Polce		Save Changes Reset Values

- 4. Select Create vNIC Template.
- 5. Enter VHBA-Template-A as the vHBA template name.
- 6. Select Fabric A. Under Select VSAN, select VSAN\_A. Under WWN Pool, select WWPN\_Pool.
- 7. Click OK to complete creating the vHBA template.
- 8. Click OK.



Create vHBA Template	Create vHBA Templat	e		×
Name: Fabric-A   Description:   Fabric ID:   A   B   Select VSAN:   default   Template Type:   Initial Template   Updating Template   Max Data Field Size:   2048   WWN Pool:   default   QoS Policy:   Anot set>   Pin Group:   Anot set>   Stats Threshold Policy:   default	Create vHBA	Template		0
Description: Fabric ID: A B Select VSAN: default Create VSAN Template Type: Initial Template Oupdating Template Max Data Field Size: 2048 WWN Pool: default QoS Policy: <not set=""> Pin Group: <not set=""> Stats Threshold Policy: default &lt;</not></not>	Name:	Fabric-A		
Fabric ID: A B   Select VSAN: default Create VSAN   Template Type: Initial Template Updating Template   Max Data Field Size: 2048   WWN Pool: default   QoS Policy: <not set="">   Pin Group: <not set="">   Stats Threshold Policy: default</not></not>	Description:			
Select VSAN: default   Template Type: Initial Template   Max Data Field Size: 2048   WWN Pool: default   QoS Policy: <not set="">   Pin Group: <not set="">   Stats Threshold Policy: default</not></not>	Fabric ID:	• A • B		
Template Type: Initial Template O Updating Template Max Data Field Size: 2048 WWN Pool: default QoS Policy: <not set=""> Pin Group: <not set=""> Stats Threshold Policy: default</not></not>	Select VSAN:	default	•	Create VSAM
Max Data Field Size: 2048 WWN Pool: default QoS Policy: <not set=""> Pin Group: <not set=""> Stats Threshold Policy: default</not></not>	Template Type:	<ul> <li>Initial Template</li> </ul>	Updating Template	
WWN Pool: default  QoS Policy: <not set=""> Pin Group: <not set=""> Stats Threshold Policy: default</not></not>	( Max Data Field Size:	D 2048		
QoS Policy: <a href="https://www.sets-andlesender-communication-communicatio-commu communicatio-communicatio-communicatio-communicatio-communi</td> <td>WWN Pool:</td> <td>default</td> <td></td> <td></td>	WWN Pool:	default		
Pin Group: <pre><not set=""> </not></pre>	QoS Policy:	<not set=""></not>	•	
Stats Threshold Policy: default	Pin Group:	<not set=""></not>		
	Stats Threshold Policy:	default	•	
				OK Cancel

- 9. Select the VSAN tab on the left of the window.
- 10. Go to Policies > root.
- 11. Right-click vHBA Templates.
- 12. Select Create vHBA Template.
- **13.** Enter VHBA-Template-B as the vHBA template name.
- 14. Select Fabric B. Under Select VSAN, select VSAN\_B. Under WWN Pool, select WWPN\_Pool.
- 15. Click OK to complete creating the vHBA template.
- 16. Click OK.



🛕 Create vHBA Templat	e		X
Create vHBA	Template		0
Name:	Fabric-B		
Description:	-		
Fabric ID:	O A @ B		
Select VSAN:	D default	•	Create VSAN
Template Type:	🕐 Initial Templati	e 🧿 Updating Template	
Max Data Field Size:	2048		
WWN Pool:	default		
QoS Policy:	<not set=""></not>		
Pin Group:	<not set=""></not>		
Stats Threshold Policy:	default		
			OK Cancel

### **Create Boot Policies**

These steps provide details for creating boot policies for the Cisco UCS environment. These directions apply to an environment in which each storage controller 0c port is connected to fabric A and each storage controller 0d port is connected to fabric B. In these steps, 2 boot policies will be configured. The first policy will configure the primary target to be controller A port 0c and the second boot policy primary target will be controller B port 0d.

**Note:** If you are using FCoE between the Nexus 5548 and the NetApp Storage systems to substitute port 2a for port 0c and port 2b for port 0d in this procedure

- 1. Select the Servers tab at the top left of the window.
- 2. Go to Policies > root.
- 3. Right-click Boot Policies.





- 4. Select Create Boot Policy.
- 5. Name the boot policy Boot-Fabric-A.
- 6. (Optional) Give the boot policy a description.
- 7. Leave Reboot on Boot Order Change and Enforce vNIC/vHBA Name unchecked.
- 8. Expand the Local Devices drop-down menu and select Add CD-ROM.
- 9. Expand the vHBAs drop-down menu and select Add SAN Boot.
- 10. Enter Fabric-A in the vHBA field in the Add SAN Boot window that displays.
- 11. Make sure that Primary is selected as the type.
- 12. Click OK to add the SAN boot initiator.



🚔 Add SAN Boot	×
Add SAN Boot	0
vHBA: Fabric-A Type: • Primary • Secondary	
	OK Cancel

- 13. Under the vHBA drop-down menu, select Add SAN Boot Target. Keep the value for Boot Target LUN as 0.
- 14. Enter the WWPN for the primary FC adapter interface Oc of controller A. To obtain this information, log in to controller A and run the fcp show adapters command.
- 15. Be sure to use the FC portname for 0c and not the FC node name.
- 16. Keep the type as Primary.
- 17. Click OK to add the SAN boot target.

🛕 Add SAN Boot Ta	rget	×
Add SAN B	oot Target	0
Boot Target LUN:	0	
Boot Target WWPN:	50:0A:09:82:8D:73:42:07	
()pc)		
		OK Cancel

- 18. Under the vHBA drop-down menu, select Add SAN Boot Target. Keep the value for Boot Target LUN as 0.
- 19. Enter the WWPN for the primary FC adapter interface 0c of controller B. To obtain this information, log in to the controller B and run the fcp show adapters command.



20. Be sure to use the FC portname for port 0c and not the FC node name.

21. Click OK to add the SAN boot target.

Add SAN BOULT	pot Target	6
	or ranger	
Boot Target LUN:	0	
Boot Target WWPN:	50:0A:09:82:9D:73:42:07	
Type:	O Primary 💿 Secondary	
		OK Cancel

- 22. Select Add SAN Boot under the vHBA drop-down menu.
- 23. Enter Fabric-B in the vHBA field in the Add SAN Boot window that displays.
- 24. The type should automatically be set to Secondary and it should be grayed out. This is fine.
- 25. Click OK to add the SAN boot target.

🚔 Add SAN Boot	×
Add SAN Boot	0
vHBA: Fabric-B	
Type: Primary 💿 becondary	
	OK Cancel

- 26. Select Add SAN Boot Target under the vHBA drop-down menu.
- 27. The Add SAN Boot Target window displays. Keep the value for Boot Target LUN as 0.
- 28. Enter the WWPN for the primary FC adapter interface 0d of the controller B. To obtain this information, log in to controller B and run the fcp show adapters command.





- 29. Be sure to use the FC portname for port 0d and not the FC node name.
- 30. Keep the type as Primary.
- 31. Click  $\ensuremath{\mbox{\tiny OK}}$  to add the SAN boot target.

🛕 Add SAN Boot Tai	rget	×
Add SAN Bo	oot Target	0
Boot Target LUN: Boot Target WWPN: Type:	0 50:0A:09:81:9D:73:42:07 Primary Secondary	
		OK Cancel

- **32. Under the vHBA drop-down menu, select** Add SAN Boot Target. Keep the value for Boot Target LUN as 0.
- 33. Enter the WWPN for the primary FC adapter interface Od of controller A. To obtain this information, log in to controller A and run the fcp show adapters command.
- 34. Be sure to use the FC portname for port 0d and not the FC node name.
- 35. Click OK to add the SAN boot target.

🛕 Add SAN Boot Target		
Add SAN Bo	oot Target	0
Boot Target LUN: Boot Target WWPN:	0 50:0A:09:81:9D:73:42:07	
Туре:	Primary Secondary	
		OK Cancel





### **Creating Boot Policy for Fabric -B**

- 1. Right-click Boot Policies again.
- 2. Select Create Boot Policy.
- 3. Name the boot policy Boot-Fabric-B.
- 4. (Optional) Give the boot policy a description.
- 5. Leave Reboot on Boot Order Change and Enforce vNIC/vHBA Name unchecked.
- 6. Expand the Local Devices drop-down menu and select Add CD-ROM.
- 7. Click the vHBA drop-down menu and select Add SAN Boot.
- 8. Enter Fabric-B in the vHBA field in the Add SAN Boot window that displays.
- 9. Make sure that Primary is selected as the type.
- 10. Click  $\ensuremath{\mbox{\tiny OK}}$  to add the SAN boot target.

🌲 Add SAN Boot	×
Add SAN Boot	0
VHBA: Fabric-B	
Type: 💽 Primary 🔿 Secondary	
	OK Cancel

- 11. Under the vHBA drop-down menu, select Add SAN Boot Target. Keep the value for Boot Target LUN as 0.
- 12. Enter the WWPN for the primary FC adapter interface Od of controller B. To obtain this information, log in to controller B and run the fcp show adapters command.
- 13. Be sure to use the FC portname for port 0d and not the FC node name.
- 14. Keep the type as Primary.
- 15. Click OK to add the SAN boot target.



🗼 Add SAN Boot Target	×
Add SAN Boot Target	0
Deat Tarach U.M. O	
Boot Target LUN: U	_
Boot Target WWPN: 50:0A:09:81:9D:73:42:07	
Type: 💿 Primary 🔿 Secondary	
	OK Cancel

- 16. Under the vHBA drop-down menu, select Add SAN Boot Target. Keep the value for Boot Target LUN as 0.
- 17. Enter the WWPN for the primary FC adapter interface Od of controller A. To obtain this information, log in to controller A and run the fcp show adapters command.
- 18. Be sure to use the FC portname for port 0d and not the FC node name.
- 19. Click OK to add the SAN boot target.

🚔 Add SAN Boot Target	×
Add SAN Boot Target	0
Boot Target LUN: 0 Boot Target WWPN: 50:0A:09:81:8D:73:42:07 Type: Primary © Secondary	
[	OK Cancel

- 20. Select Add SAN Boot under the vHBA drop-down menu.
- 21. Enter Fabric-A in the vHBA field in the Add SAN Boot window that displays.
- 22. The type should automatically be set to Secondary and it should be grayed out. This is fine.
- 23. Click  $\ensuremath{\mbox{\scriptsize OK}}$  to add the SAN boot target.



🚔 Add SAN Boot	×
Add SAN Boot	0
OHRA) Eshvic-A	
Type: 🖸 Primary 💿 Secondary	
	OK Cancel

- 24. Select Add SAN Boot Target under the vHBA drop-down menu.
- 25. The Add SAN Boot Target window displays. Keep the value for Boot Target LUN as 0.
- 26. Enter the WWPN for the primary FC adapter interface <code>0c</code> of controller A. To obtain this information, log in to controller A and run the <code>fcp show adapters</code> command.
- 27. Be sure to use the FC portname for port 0c and not the FC node name.
- 28. Keep the type as Primary.
- 29. Click OK to add the SAN boot target.

🚔 Add SAN Boot Target	×
Add SAN Boot Target	0
Boot Target LUN: 0 Boot Target WWPN: 50:0A:09:82:9D:73:42:07 Type: • Primary • Secondary	
OK	Cancel

**30. Under the vHBA drop-down menu, select** Add SAN Boot Target. Keep the value for Boot Target LUN as 0.



- 31. Enter the WWPN for the primary FC adapter interface Oc of controller B. To obtain this information, log in to controller B and run the fcp show adapters command.
- 32. Be sure to use the FC portname for port 0c and not the FC node name.
- 33. Click OK to add the SAN boot target.

🌲 Add SAN Boot Target	×
Add SAN Boot Target	0
Ū	
Boot Target LUN: 0	
Boot Target WWPN: 50:0A:09:82:8D:73:42:07	-
Type: 🖸 Primary 🖸 Secondary	
	OK Cancel

34. Click OK to create the boot policy in the Create Boot Policy pop-up window.



## **Create Service Profile Templates**

This section details the creation of two service profile templates: one for fabric A and one for fabric B.

### **Cisco UCS Manager**

- 1. Select the Servers tab at the top left of the window.
- 2. Go to Service Profile Templates > root.
- 3. Right-click root.
- 4. Select Create Service Profile Template.
- 5. The Create Service Profile Template window displays.
  - a. These steps detail configuration info for the Identify the Service Profile Template Section.
  - b. Name the service profile template VM-Host-Infra-Fabric-A. This service profile template is configured to boot from controller A port Oc.
  - c. Select Updating Template.
  - d. In the UUID section, select UUID Pool as the UUID pool.
  - e. Click Next to continue to the next section.

Create Service Profile Template 18 Unified Computing System Manager Identify Service Profile Template 10 Create Service Profile Template You must enter a name for the service profile template and specify the template type. You can also specify how a UUID will be 1. Videntify Service Profile assigned to this template and enter a description Template 2. Storage Name: VH-Host-Infra-Fabric-A 3. Diversional 4. D WITCAHBA Placement The template will be created in the following organization. Its name must be unique within this organization 6. Gerver Boot Order Where: org-root 6. Hantenance Pokcy The template will be created in the following organization. Its name must be unique within this organization. 7. Server Assument 8. Deperational Policies Type: Initial Template . Updating Template Specify how the UUID will be assigned to the server associated with the service generated by this template. UUID UKIID Assignment: default(100/100) . The UUID will be assigned from the selected pool. The available/total UUIDs are displayed after the pool name. Optionally enter a description for the profile. The description can contain information about when and where the service profile should be used. <Prev Next> Finish Cancel

6. Storage section




- a. Select Default for the Local Storage field.
- b. Select the appropriate local storage policy if the server in question does not have local disk.
- c. Select SAN-Boot for the local disk configuration policy.
- d. Select the Expert option for the How would you like to configure SAN connectivity field.
- e. In the WWNN Assignment field, select WWNN\_Pool.
- f. Click the Add button at the bottom of the window to add vHBAs to the template.
- g. The  $\mbox{Create vHBA}$  window displays. Name the vHBA  $\mbox{Fabric-A}.$
- h. Check the box for Use SAN Connectivity Template.
- i. Select Fabric-A in the vHBA Template field.
- j. Select Windows-NetApp in the Adapter Policy field.
- k. Click OK to add the vHBA to the template.

Create vHBA	
Create vHBA	0
Name: Fabric-A Use SAN Connectivity Template:	
vHBA Template: Fabric-A	
Adapter Performance Profile Adapter Policy: Windows-NetApp  Create Fibre Channel Adapter Policy	
	OK Cancel

- 7. Click the Add button at the bottom of the window to add vHBAs to the template.
- 8. The  $\mbox{Create vHBA}$  window displays. Name the vHBA  $\mbox{Fabric-B}.$
- 9. Check the box for Use SAN Connectivity Template.
- 10. Select Fabric-B in the vHBA Template field.





- 11. Select Windows-NetApp in the Adapter Policy field.
- 12. Click  $\ensuremath{\mbox{OK}}$  to add the vHBA to the template.

Create vHBA	<b>X</b>
Create vHBA	0
Name: Fabric-B	
Use SAN Connectivity Template:	
vHBA Template: Fabric-B	
Adapter Performance Profile Adapter Policy: Windows-NetApp Create Fibre Channel Adapter Policy	
	OK Cancel

13. Verify – Review the table to make sure that both of the vHBAs were created.



eate Service Profile Template 1. √ <u>Identify Service Profile</u>	Storage Optionally specify disk policies and SAN confi	guration information.	
Temolate 2. V Storses 3. Distional 4. Unit Cheffield Placement 5. Server Boot Order 6. Distort Boot Order 7. Diserver Assornment 8. Diserver Assornment 8. Diserver Assornment	Select a local disk configuration policy. Local Storage: SAN-Boot .	Node: No Local Storage Protect Configuration: ee If Protect Configuration is set, the Local Disk Configuration is press On reasosciation of the same Server, a configuration error will be rate of the new Local Disk Configuration is different. Infigure SAR connectivity? Simple: e: Expert No vHSAs (WWNW). Spectry how the system should assign a WWNW to the server as	erved on disassociation, d
	The WWWW will be assigned from the selected pool. The evaluable/total WWWW are displayed after the pool	nane.	
	The WWWW will be assigned from the selected pool. The available/total WWWWs are displayed after the pool	ume. WWFN	( <b>a</b> )
	The WWWW will be assigned from the selected pool. The available/total WWWW are displayed after the pool Name 	ww.FN Derived Derived	

14. Click  ${\tt Next}$  to continue to the next section.

#### 15. Networking Section

- a. Leave the Dynamic vNIC Connection Policy field at the default.



Create Service Profile Template	91.14	A DESC N R. O.	(Case		
Unified (	Comput	ing System	Manager		
Create Service Profile Template 1.  4 Identify Service Profile Template 2.  4 Storage 3.  4 Retworking 4.  9 utiC/wHtA Placement 5.  9 Server Bost Order,	Networking Optionally spe	city LAN configuration information			0
	Dynamic vNBC Corne	stem Paksy: Select a Poksy to use (no D	ynamic vNIC Policy by default) 🔹	Create Dynamic vHIE Connection Policy	
6. Di <u>Maintenance Policy</u> 7. Di <u>Server Assonment</u> 8. Di <u>Operational Policies</u>	Cick. Add to specify o	How would you like to config te or more vNBCs that the server should	pure LAN connectivity? Simple	· Eggett No vHICs	
	Name	MAC Address	Fabric ID	Native VLAN	4
					*
			Add Minory		
	ISCSI VIRICE				8
	× .		.17		- •
				< Prev Next > Finah	Caricel

- c. Click Add to add a vNIC to the template.
- d. The Create vNIC window displays. Name the vNIC CSV.
- e. Check the Use LAN Connectivity Template checkbox.
- f. Select CSV for the vNIC Template field.
- g. Select Windows in the Adapter Policy field.
- h. Click OK to add the vNIC to the template.



Create vNIC	×
Create vNIC	0
Name: CSV	
Use LAN Connectivity Template:	
vNIC Template: CSV	
Adapter Policy: Windows	
	OK Cancel

- i. Click Add to add a vNIC to the template.
- j. The <code>Create vNIC</code> window <code>displays</code>. Name the <code>vNIC</code> <code>LiveMigration</code>.
- k. Check the Use LAN Connectivity Template checkbox.
- I. Select LiveMigration for the vNIC Template field.
- m. Select Windows in the Adapter Policy field.
- n. Click  $\ensuremath{\mbox{OK}}$  to add the vNIC to the template.



A Create vNIC	x
Create vNIC	0
Name: LiveMigration	
Create vNIC Template	
VNIC Template: LiveMigration	
Adapter Policy: Windows	
OK Can	cel

- o. Click Add to add a vNIC to the template.
- p. The Create vNIC window displays. Name the vNIC VM-MGMT.
- q. Check the Use LAN Connectivity Template checkbox.
- r. Select VM-MGMT for the vNIC Template field.
- s. Select Windows in the Adapter Policy field.
- t. Click OK to add the vNIC to the template.



A Create vNIC	×
Create vNIC	0
Name: VM-Mgmt Use LAN Connectivity Template:  Use LAN Connectivity Template:  Connectivity Template:	
	Cancel

- u. Click  ${\tt Add}$  to add a vNIC to the template.
- v. The Create vNIC window displays. Name the vNIC AppApp-Cluster-Comm.
- w. Check the Use LAN Connectivity Template checkbox.
- x. Select AppApp-Cluster-Comm for the vNIC Template field.
- y. Select Windows in the Adapter Policy field.
- z. Click OK to add the vNIC to the template.
- aa. Click Add to add a vNIC to the template.
- bb. The  $\mbox{Create vNIC}$  window displays. Name the vNIC VM-Data.
- cc. Check the Use LAN Connectivity Template checkbox.
- dd. Select <code>VM-Data</code> for the <code>vNIC</code> Template field.
- ee. Select Windows in the Adapter Policy field.
- ff. Click  $\ensuremath{\mathsf{OK}}$  to add the vNIC to the template.



A Create vNIC	
Create vNIC	0
Name: VM-Data	
Create vNIC Template	
Adapter Performance Profile	
OK (	Cancel

- gg. Click  ${\tt Add}$  to add a vNIC to the template.
- hh. The Create vNIC window displays. Name the vNIC iSCSI-Fabric-A.
- ii. Check the Use LAN Connectivity Template checkbox.
- jj. Select iSCSI-Fabric-A for the vNIC Template field.
- kk. Select Windows in the Adapter Policy field.
- II. Click OK to add the vNIC to the template.



Create vNIC	<b>X</b>
Create vNIC	0
Name: iSCSI-Fabric-A	
Use LAN Connectivity Template:	
vNIC Template: ISCSI-Fabric-A	
Adapter Performance Profile Adapter Policy: Windows Create Ethernet Adapter Policy	
	OK Cancel

- 16. Click Add to add a vNIC to the template.
- 17. The Create vNIC window displays. Name the vNIC iSCSI-Fabric-B.
- 18. Check the Use LAN Connectivity Template checkbox.
- **19.** Select iSCSI-Fabric-B for the vNIC Template field.
- 20. Select Windows in the Adapter Policy field.
- 21. Click  $\ensuremath{\mbox{oK}}$  to add the vNIC to the template.



A Create vNIC	<b>X</b>
Create vNIC	0
Name: iSCSI-Fabric-B	
Use LAN Connectivity Template:	
Create vNIC Template	
vNIC Template: ISCSI-Fabric-B	
Adapter Performance Profile	
Adapter Policy: Windows	
	K Cancel

22. Verify: Review the table to make sure that all of the vNICs were created.



eate Service Profile Template  1.  / Identify Service Profile Template  2.  / Envoide  3.  / Retworking  4.  UnitC/rettA Placement  5.  Server Boot Order	Optionally specify LAN configur	ation information		
	Dynamic VNIC Connection Palicy: Select a Policy to use (no Dynamic VNIC Policy by default) • Conste Dynamic VNIC Connection Policy			
U <u>Mantenance Policy</u> Diserver, Assament U <u>Operational Policies</u>	How would Click Add to specify one or more vhill's the	I you like to configure LAN can at the server should use to connect	nectivity? Simple o	Expert No vfillCa
	Name	MAC Address	Fabric ID	Native VLAN
		Derived	derived	
	-fg vNIC VM-Data	Derived	derived	
	-g vNIC CSV	Derived	derived	
	- 🕼 vRIC LiveHigration	Derived	derived	
	- VNIC ISCSI-Fabric-A	Derived	derived	
		Server 1	Add III Hoolv	
	ISCSE VILLOS			

- 23. Click  ${\tt Next}$  to continue to the next section.
- 24. vNIC/vHBA Placement Section
- 25. Select the VM-Host-Infra Placement Policy in the Select Placement field.





Specify how vN	<b>Placement</b> ICs and vHBAs are place	ed on physical network adapters			
Virtual Network Interf vNICs and vHBAs are performed explicitly bi automatically by selec vNIC/vHBA placement Please select one Virtu	cifies how vNICs and vHBAs iguration independent way. I-Host-Infra ace connection provides a m assigned to one of Virtual Net y selecting which Virtual Netw ting "any". t on physical network interface ual Network Interface and on	are placed on physical network adapter  Create Placement Policy  Create Placement Policy  Create Placement Policy  chanism of placing vNICs and vHBAs or  stwork Interface connection specified by vN  ce is controlled by placement preference  a or more vNICs or vHBAs	s (mezzanine) n physical network adapters elow. This assignment can b IC or vHBA or it can be don as.	i, e 3	
		IS OF THOSE WALLS OF WIDAS			
		Virtual Network Interfaces Policy (rea	d only)		-
VNICs VHBAs		Virtual Network Interfaces Policy (rea	d only)	Selection Preference	Ī
VNICs VHBAs		Virtual Network Interfaces Policy (real Name	d only) Order	Selection Preference Assigned Only	
VNICs VHBAS		Virtual Network Interfaces Policy (rear Name S vCon 1 VCon 2	d only) Order	Selection Preference Assigned Only All	
VNICs VHBAS	>> assign >>	Virtual Network Interfaces Policy (rear Name S vCon 1 VCon 2 VCon 3	d only) Order	Selection Preference Assigned Only All All	
VNICs VHBAS Name II iSCSI-Fabri A iSCSI-Fabri VM-Mgmt	>> assign >>	Virtual Network Interfaces Policy (real Name S vCon 1 S vCon 2 VCon 3 VCon 4	d only) Order	Selection Preference Assigned Only All All All	
VNICs VHBAs Name C iSCSI-Fabri iSCSI-Fabri VM-Mgmt CSV	>> assign >> << remove <<	Virtual Network Interfaces Policy (real Name S vCon 1 VCon 2 VCon 3 VCon 4	d only) Order	Selection Preference Assigned Only All All All	
VNICs VHBAs Name I iSCSI-Fabri iSCSI-Fabri VM-Mgmt CSV LiveMigrati	>> assign >> << remove <<	Virtual Network Interfaces Policy (rea Name S vCon 1 VCon 2 VCon 3 VCon 4	d only) Order	Selection Preference Assigned Only All All All	
VNICs VHBAs Name I iSCSI-Fabri iSCSI-Fabri VM-Mgmt CSV LiveMigrati App-Cluste	>> assign >> << remove <<	Virtual Network Interfaces Policy (real Name S vCon 1 S vCon 2 S vCon 3 S vCon 4	d only) Order	Selection Preference Assigned Only All All All	
VNICs VHBAs Name iSCSI-Fabri iSCSI-Fabri VM-Mgmt CSV LiveMigrati App-Cluste VM-Data	>> assign >> << remove <<	Virtual Network Interfaces Policy (real Name Virtual Network Interfaces Policy (real Name VCon 1 VCon 2 VCon 2 VCon 3 VCon 4	d only)	Selection Preference Assigned Only All All All	
VNICs VHBAs Name iSCSI-Fabri iSCSI-Fabri VM-Mgmt CSV LiveMigrati App-Cluste VM-Data	>> assign >> << remove <<	Virtual Network Interfaces Policy (real Name Virtual Network Interfaces Policy (real Name VCon 1 VCon 2 VCon 3 VCon 4	d only) Order Move Up Move Dov	Selection Preference Assigned Only All All All	

- 26. Select vCon1 assign the vNICs in the following order:
  - a. VM-Data
  - b. App-Cluster-Comm
  - c. LiveMigration
  - d. CSV
  - e. VM-Mgmt
  - f. iSCSI-Fabric-A
  - g. iSCSI-Fabric-B



THO TIDAT	lacement				
Specify how vNI	ICs and vHBAs are place	ed on physical network adapters			
JIC/vHBA Placement spe a server hardware confi	cifies how vNICs and vHBAs a guration independent way.	are placed on physical network adapters (mezzan	nine)		
Select Placement: VM	-Host-Infra	<ul> <li>Create Placement Policy</li> </ul>			
Virtual Network Inter- vNICs and vHBAs are performed explicitly by automatically by selec vNIC/vHBA placement	ace connection provides a me assigned to one of Virtual Net y selecting which Virtual Netwi ting "any". on physical network interface	chanism of placing vNICs and vHBAs on physical twork Interface connection specified below. This iork Interface connection is used by vNIC or vHB, e is controlled by placement preferences.	network adapters. assignment can be A or it can be done		
Fiedse select one virti	Jai Network Interface and one	e or more vNICs or vHBAs Virtual Network Interfaces Policy (read only)			
	Jai Network Interface and one	e or more vNICs or vHBAs Virtual Network Interfaces Policy (read only) Name	Order	Selection Preference	
VNICs VHBAs	al Network Interface and one	e or more vNICs or vHBAs Virtual Network Interfaces Policy (read only) Name	Order	Selection Preference Assigned Only	
VNICs VHBAs	al Network Interface and one	e or more vNICs or vHBAs Virtual Network Interfaces Policy (read only) Name - S vCon 1 - VNIC VM-Data	Order	Selection Preference Assigned Only	
VNICs VHBAs	al Network Interface and one	e or more vNICs or vHBAs Virtual Network Interfaces Policy (read only) Name Virtual Network Interfaces Policy (read only) Name Vame Von 1 VIIC VM-Data	Order 1 2	Selection Preference Assigned Only	<b>•</b>
VNICs VHBAS	al Network Interface and one	e or more vNICs or vHBAs Virtual Network Interfaces Policy (read only) Name Virtual Network Interfaces Policy (read only) Name Volume Vo	Order 1 2 3	Selection Preference Assigned Only	<b>•</b>
VNICs VHBAS	al Network Interface and one	e or more vNICs or vHBAs Virtual Network Interfaces Policy (read only) Name Virtual Network Interfaces Policy (read only) Name Voice 1 Voice	Order 1 2 3 4	Selection Preference Assigned Only	
VNICs VHBAS	>> assign >>         < <remove <<="" td=""></remove>	e or more vNICs or vHBAs Virtual Network Interfaces Policy (read only) Name Virtual Network Interfaces Policy (read only) Name Volume VOID 1 VOID 1 VO	Order 1 2 3 4 5	Selection Preference Assigned Only	
VNICs VHBAs	>> assign >>         < <remove <<="" td=""></remove>	e or more vNICs or vHBAs Virtual Network Interfaces Policy (read only) Name Vame Von 1 VIIC VM-Data VIIC App-Cluster-Comm VIIC LiveMigration VIIC CSV VIIC CSV VIIC SSI-Fabric-A	Order 1 2 3 4 5 6	Selection Preference Assigned Only	
VNICs VHBAs	al Network Interface and one	e or more vNICs or vHBAs Virtual Network Interfaces Policy (read only) Name Vame Vocn 1 VIIC VM-Data VIIC App-Cluster-Comm VIIC LiveMigration VIIC CSV VIIC CSV VIIC SCSI-Fabric-A VIIC iSCSI-Fabric-B	Corder 1 2 3 4 5 6 7	Selection Preference Assigned Only	
VNICs VHBAS	al Network Interface and one	e or more vNICs or vHBAs Virtual Network Interfaces Policy (read only) Name Virtual Network Interfaces Policy (read only) Name VIIC VM-Data VIIC App-Cluster-Comm VIIC App-Cluster-Comm VIIC LiveMigration VIIC CSV VIIC CSV VIIC ISCSI-Fabric-A VIIC ISCSI-Fabric-B Move L	Order 1 2 3 4 5 6 7 Jp Wove Down	Selection Preference Assigned Only	

27. Click the vHBA tab and add the vHBAs in the following order:

- a. Fabric-A
- b. Fabric-B
- 28. Verify: Review the table to make sure that all of the vHBAs and vNICs were created. The order of the vNICs and vHBAs is not important.



Specify how vNICs and vHBAs are plac	ed on physical network adapters			
NIC/vHBA Placement specifies how vNICs and vHBAs a server hardware configuration independent way.	are placed on physical network adapters (mezz	anine)		
Select Placement: VM-Host-Infra	Create Placement Policy			
VIICs and vHBAs are assigned to one of Virtual Ne performed explicitly by selecting which Virtual Ne automatically by selecting "any". vNIC/vHBA placement on physical network interfa- Please select one Virtual Network Interface and or	ection in the place of the second where and where on physic etwork Interface connection is used by vNIC or vh ice is controlled by placement preferences. ne or more vNICs or vHBAs	IBA or it can be done		
	Virtual Network Interfaces Policy (read only)			
VNICE VHBAS	Virtual Network Interfaces Policy (read only)	Order	Selection Preference	
VNICs VHBAS	Virtual Network Interfaces Policy (read only)	Order	Selection Preference	
VNICs VHBAS	Virtual Network Interfaces Policy (read only) Name Virtual VIIC LiveMigration VIIC CSV	Order 3 4	Selection Preference	<u> </u>
VNICs VHBAS	Virtual Network Interfaces Policy (read only) Name VIIC LiveMigration VIIC CSV VIIC VM-Mgmt	Order 3 4 5	Selection Preference	<u> </u>
VNICs VHBAS	Virtual Network Interfaces Policy (read only) Name VIC LiveMigration VIC CSV VIC CSV VIC VM-Mgmt VIC iSCSI-Fabric-A	Order 3 4 5 6	Selection Preference	
VNICs VHBAs Name C >> assign >> << remove <<	Virtual Network Interfaces Policy (read only) Name VIC LiveMigration VIC CSV VIC CSV VIC VM-Mgmt VIC iSCSI-Fabric-A VIC iSCSI-Fabric-B	Order 3 4 5 6 7	Selection Preference	
VNICs VHBAs	Virtual Network Interfaces Policy (read only) Name VIIC LiveMigration VIIC CSV VIIC CSV VIIC VM-Mgmt VIIC iSCSI-Fabric-A VIIC iSCSI-Fabric-B VIIC iSCSI-Fabric-B VIIA Fabric-A	Order 3 4 5 6 7 8	Selection Preference	
VNICs VHBAS	Virtual Network Interfaces Policy (read only) Name VIIC LiveMigration VIIC CSV VIIC CSV VIIC VM-Mgmt VIIC iSCSI-Fabric-A VIIC iSCSI-Fabric-B VIBA Fabric-A VIBA Fabric-A VIBA Fabric-B	Order 3 4 5 6 7 8 9	Selection Preference	
VNICs VHBAS Name C >> assign >> << remove <<	Virtual Network Interfaces Policy (read only) Name Name VIIC LiveMigration VIIC CSV VIIC CSV VIIC VM-Mgmt VIIC iSCSI-Fabric-A VIIC iSCSI-Fabric-B VIIC iSCSI-Fabric-B VIIBA Fabric-A VIIBA Fabric-B VIIC iSC I	Order 3 4 5 6 7 8 9	Selection Preference	
VNICs VHBAs Name C >> assign >> << remove <<	Virtual Network Interfaces Policy (read only) Name Name VIII LiveMigration VIII CSV VIII CSV VIII SCSI-Fabric-A VIII SCSI-Fabric-B VIII SCSI-Fabric-B VIII AFabric-B VIIIA Fabric-B VIII AFabric-B	Order 3 4 5 6 7 8 9 9	Selection Preference	

- 29. Click Next to continue to the next section.
- 30. Server Boot Order Section
  - a. Select Boot Fabric-A in the Boot Policy field.
  - b. Verify: Review the table to make sure that all of the boot devices were created and identified. Verify that the boot devices are in the correct boot sequence.
  - c. Click  ${\tt Next}$  to continue to the next section.



Create Service Profile Template  1. √ Identify Service Profile Template  2. √ Storace  3. √ bitescriand  4. √ vtfCAHBA Placement  5. √ Server Boot Order  6. □ Maintenance Policy  7. □ Server Assument  8. □ <u>Deerational Policies</u>	Server Boot Order						
	Select a boot policy. Boot Policy: Boot Fabric-A Name: Boot-Fabric-A Description: Reboot on Boot Order Orange: no Enforce VAICUAREA/ISCS2 Name: no WARDINGS: The type (privary/secondary) does not indicate a boot order presence.						
	The type (primary/secondary) does not The effective order of boot devices with	indicate a bo	ot order presence. device class (LAN/Storage/ISC	SI) is determine	d by PCIe by	a scan order.	
	The type (primary/secondary) does no The effective order of boot devices with If Enforce VIIIC/VHIBA/SCST Name If it is not selected, the vHICa/VHIBA/S Boot Once	indicate a bo in the same is selected a ICSL are selec	iot order presence. device class (LAN/Storage/ISC nd the vMIC/HBA/SCSI does Cled if they exist, otherwise th	SI) is determine not exist, a co re vNIC/vHSA/c	d by PCIe by rfig error will SCSI with the	n scan order . he reported. lowest PCJe bus scan order is	used.
	The type (primary/secondary) does no The effective order of boot devices with UF inforce VMEC/VHBA/SCST Name If it is not selected, the VHICs/VHBA/C Noct Order (c) (c) (d) Filter (c) Export (c) Pri	indicate a bo fin the same is selected a ICSL are selec nt	ot order presence. device class (LAN/Storage/SC device class (LAN/Storage/SC ded if the vitil/HSA/SCEI does ded if they exist, otherwise th	SI) is determine not exist, a co re MUC/HBA/C	d by PCIe by fig error will SCSI with the	n scan order . he reported. Invest PCIe bus scan order is	used.
	The type (primary/secondary) does not The effective order of boot devices with UF Enforce VMEC/VHBA/SCST Name If it is not selected, the VHICs/vHBA/C Soct Order If it is not selected, the VHICs/vHBA/C Not Order Name	indicate a bo fain the same is selected a iCSL are selec nt Order	ot order presence. device class (LAN/Storage/SC device class (LAN/Storage/SC ded if the vite/LANSASCSI does ded if they exist, otherwise the viteC/vHBA/SCSI viteC	SI) is determine not exist, a cor re vNUC/vHSA/t Type	d by PCIe by rig error will SCSI with the Lun ID	n scan order. he reported. Invest PCIe bus scan order is WWN	used.
	The type (primary/secondary) does not The effective order of boot devices with UF Enforce VMEC/VHBA/SCST Ranne UF it is not selected, the VHICs/vHBA/SC Boot Ordes (c) ImJ (c) Filer (c) Export (c) Pro- Name (c) CD ROM	indicate a bo ten the same is sciencted a iCSI are soler nt Order 1	ot order presence. device class (J.M.;Storage/SC device class (J.M.;Storage/SC ded if the vite/IHEA/ISCSI does ded if they exist, otherwise the viteC/IHEA/ISCSI viteC	SI) is determine not exist, a cor ne vNUC/vHSA/K Type	ed by PCIe by rfig error will SCSE with the Lun ID	n scan order . he reported. Invest PCIe bus scan order is WWN	used.
	The type (primary/secondary) does not The effective order of boot devices with If Enforce VIIIC/VIIIRA/SCST Ranne If it is not selected, the VIIICa/VIE/As/C Boot Order (*) (*) (*) (*) (*) (*) (*) (*) (*) (*)	indicate a bo ten the same is sciencted a iCSI are soler int Order 1 2	ot order presence. device class (J.Mr/Storage//SC device class (J.Mr/Storage//SC ded if the vite//HBA/SCSI does vMiC/vHBA/SCSI vMiC	SI) is determine not exist, a cor e vNIC/vHSA/t Type	id by PCIe by dig error will SCSI with the Lun ID	n scan order . be reported. Inwest PCIe bus scan order o WWM	used.
	The type (primary/secondary) does not The effective order of boot devices with If <b>Endocev WEIC/WEIR/SCST Rame</b> If it is not selected, the vMICa/vHB/a/C <b>Boot Cost</b> (a) (c) (A) (C) (c) (c) (c) (c) (c) Name (c) (c) (c) (c) (c) (c) (c) (c) (c) Name (c) (c) (c) (c) (c) (c) (c) (c) (c) (c)	indicate a bo im the same is selected a iCSI are selec nt Order 1 2	ot order presence. device class (J.Mr/Storage/St ded if the vHC/HEA/SCSI doc clad if they exist, otherwise the vHIC/vHBA/SCSI vHIC P/XE-Boot	SII) is determine not exist, a co he MUC/MHSAM Type Primary	id by PCIe by fig error will SCSI with the Lun ID	n soan order : be reported. Inwest PCIe bus soan order is WWN	used.
	The type (primary/secondary) does not The effective order of boot devices with Uf fullowice WILControl Articles and If it is not selected, the vPIControl Articles (d) Control (Control Control Articles) Name (CO ROM CO ROM	indicate a bo in the same is selected a iCSE are selected int Order 1 2 3	ot order presence. device class (LAN/Storage/BC device class (LAN/Storage/BC ded if the vital/HBA/SCSI does ded if they exist, otherwise if vitaC/vHBA/SCSI vHC P/E-Boot	SII) is determine not exist, a co re vNIC/VHSAX Type Primary	d by PCIe by fig error wit SCSI with the Lun ID	n scan order : he reportad. Invest PCIe bus scan order is WWN	used.
	The type (primary/secondary) does not The effective order of boot devices with UF inforce VIEC/VHEA/KET Name. If it is not selected, the VHICa/HEA/KET Boot Order (a) (a) (A) Filter (a) Export (a) Fil Name (a) (b) (C) ROM (b) (c) (c) (c) (c) (c) (c) Name (c) (c) (c) (c) (c) (c) (c) (c) (c) (c) Name (c) (c) (c) (c) (c) (c) (c) (c) (c) (c)	indicate a bo in the same is selected a cCSI are selected int Corder 1 2 3	ot order presenze. device class (LAN/Storage/ISC device class (LAN/Storage/ISC ded if the vite/viteSA/SCSI does ded if they exist, otherwise th viteC/vHBA/ISCSI viteC PXE-Boot PCE-Bonc-A	SII) is determine not exist, a cov e vNUC/vHSA/6 Type Primary Primary	d by PCIe by fig error will SCSI with the Lun ID	n scan order . he reported. Invest PC3e bus scan order is	used.
	The type (primary/secondary) does not The effective order of boot devices with If inforce VIIIC/VHBA/ICST Name If it is not selected, the VHICA/HBA/IC Nort Ordes If it is not selected, the VHICA/HBA/IC Norte If it is not selected, the VHICA/HBA/IC If it is	indicate a bo in the same is selected a scale of the scale of the scale of the same of the Corder 1 2 3	ot order presence. device class (J.M.;Storage/ISC device class (J.M.;Storage/ISC ded if the vite//viteSA/SCSI closes ded if they exist, otherwise the vMIC/viteBA/ISCSI vMIC PVE-Boot PC-Fabric-A	SII) is determine not exist, a cor- re vNUC/vHSA/6 Type Primary Primary Primary	d by PCIe by rfg error with SCSI with the Lun ID	e scan order : he reported. Invest PCIe bus scan order is WWN WWN	used.
	The type (primary/secondary) does not The effective order of boot devices with If Enforce VIEC/VHEA/SCST Rame If it is not selected, the VHICa/HEA/C Boot Ordes CD ROM CD ROM LAW PXE-Boot LAW PXE-Boot SAW Primary SAW Primary SAW Primary SAW Primary	indicate a bo in the same is selected a select ISSUME select Int Order 1 2 3	ot order presence. device class (J.Mr,Storrage/JSC device class (J.Mr,Storrage/JSC ded if the vite/InHEA/ISCSI closes ded if they exist, otherwise b vMBC/rHBA/ISCSI vMBC PXE-Boot PC-Fabric-A	SII) is determine not exist, a cor- re vNUC/vHSA/0 Type Primary Primary Primary Secondary	nd by PCIe by rfig error will ICSI with the Lun ID 0	e scan order : he reported. Invest PCIe bus scan order is WWN 90:04:09:82:8D:73:42:07 50:04:09:82:9D:73:42:07	used.
	The type (primary/secondary) does not The effective order of boot devices with If following with the secondary) Boot Ordes	Indicate a bo Im the same is selected a select ICSL are select I Corder 1 2 3	ot or der presenze device class (LAN/Storage/BC ded de vitil/HBA/SCSI does ded if they exist, otherwise if w/BC/vHBA/SCSI vHIC P/XE-Boot PC-Fabric-A PC-Fabric-B	SII) is determine not exist, a covie whttp://wttba/d Type Primary Primary Primary Secondary Secondary	nd by PCIe by rfig error will ISSI with the Lun ID 0 0	s scan order : be reported. Invest PCJe bus scan order s WWN 50:04:09:82:80:73:42:07 50:04:09:82:90:73:42:07	used.
	The type (primary/secondary) does not The effective order of boot devices with Uf fuldrock VIUE(UVHBA/KCST Name If it is not selected, the VIUCa/HBA/K Stat Order Stat Order D CD ROM CD ROM LAN PXE-Boot LAN PXE-Boot Starage Sta	indicate a bo in the same is secreted as is secreted as icSI are select int Order 1 2 3	ot order presence. device class (LAN/Storage/BC device class (LAN/Storage/BC ded # the vitil/viteSA/SCSI does ded # they exist, otherwise # vitilC/vitBA/SCSI vitilC PXE-Boot PC-Fabric-B PC-Fabric-B	SII) is determine not exist, a covie with C/AHBA/8 Type Primary Primary Primary Secondary Primary Secondary Primary	d by PCIe by hig error will CCSI with the Lun ID 0 0	s scan order : be reported. Invest PCIe bus scan order s WWN 90:04:09:82:80:73:42:07 50:04:09:82:90:73:42:07 50:04:09:81:90:73:42:07	used.

#### 31. Maintenance Policy Section

- a. Keep the default of no policy used by default.
- b. Click  ${\tt Next}$  to continue to the next section.
- 32. Server Assignment Section
  - a. Select Default in the Pool Assignment field.
  - b. Select VM-Host-Infra for the Server Pool Qualification field.
  - c. Select Up for the power state.
  - d. Select VM-Host-Infra in the Host Firmware field.
  - e. Select VM-Host-Infra in the Management Firmware field.
  - f. Click Next to continue to the next section.



e Service Profile Template 1.	Optionally specify a server pool for this service profile template.	
	You can select a server pool you want to associate with this service profile template.         Pool Assignment:       Image: Control Server Pool         Select the power state to be applied when this profile is associated with the server.         Image: Up image: Control Server Pool         The service profile template will be associated with one of the servers in the selected pool.         If desired, you can specify an additional server pool policy qualification that the selected server must meet. To do so, select the qualification from the lat.         Server Pool Qualification:         Image: Restrict Migrature:	
	Firmware Management (BIOS, Disk Controller, Adapter) If you select a host or management firmware pokry for this service profile template, the profile will update the firmware on the server that is is associated otherwise the system uses the firmware already installed on the associated server. Host firmware: VMHist 20/ra  Create Host firmware Package	C with.

#### 33. Operational Policies Section

- a. Select VM-Hot-Infra in the BIOS Policy field.
- b. Expand Power Control Policy Configuration.
- c. Select No-Power-Cap in the Power Control Policy field.
- d. Click Finish to create the Service Profile template.
- e. Click OK in the pop-up window to proceed.



2. Viscose 3. Viscose	0
Server Source Folds     If you want to override the default 800S settings, select     Veneroprice Folds     Source Asservant     Veneroprice Folds     Conste Block Policy	a BICIS policy that will be associated with this service profile Policy
8. Operational Policies. External IPPU Management Configuration	0
Hanagement IP Address	0
Honitoring Configuration (Thresholds)	0
Power Control Policy Configuration	0
Scrub Policy	0
Sorub Policy: default 🔹 💌 Create Sorub	Palicy

34. Select the Servers tab at the top left of the window.

35. Go to Service Profile Templates > root.

36. Select the previously created <code>VM-Host-Infra-Fabric-A</code> template

 $\mathbf{37.}\ \mathbf{Click}\ \mathtt{Create}\ \mathtt{a}\ \mathtt{Clone.}$ 





38. Enter VM-Host-Infra-Fabric-B in the Clone Name field and click OK.



- 39. Select the newly created service profile template and select the Boot Order tab.
- 40. Click Modify Boot Policy.



	G C New - Q Options () O	Armen	Carles Bat				
	>> 🚙 Servers I 🔝 Service Profile Terret	lates • A inst	· III Service Templete VM-Hor	d-Infra-Palaric-8		Service Template VM-Host-Infr	e-Pebric-
An and the second is and even in a located	General Storage Network SCSI vNICe	Boot Citaler p	okces Events PSH				
Entribusing residence ( 2001 ( 2004 ) 104 ( Adult)	Actions						
Filter Al	1 March - South Mary						
a a							
Service Profiles  Service Profiles  Service Profile  Service Profile  Service Profile  Service Template  Service Template  Service Template VM Host-Infto-Fabric-A  Service Template VM Host-Infto-Fabri	Name: Boot- Description: Reboot on Boot Order Change: no trifform: VHC/AMACEN Name: no WARKINGS The tope (privary/accordery) does not to The afflictive order of floot devices with 19 for force vHC/VHTRA/SCS1 Name: 19 ft is not selected, the VHCC/VHTRA/SC DOCTOR The tope Afflictive according to the second second the tope Afflictive according to the second second the tope Afflictive Afflictive Afflictive Afflictive the tope Afflictive Afflictive Afflictive Afflictive the tope Afflictive Afflictive Afflictive Afflictive the tope Afflictive Afflictive Afflictive Afflictive Afflictive	rabric A ndicate a boot o in the same days is selected and th 35 are selected	rder presence. an class (JAV/Clinenage/BCSS) in a e VECV/HEA/SCS3 does not ee if they want, othermise the VEC	Interneted by PCI det, a config error cyntRA/BCSI with	e bua acart orde will be reported the lowest PCJ	e. 6 e haa acars order in used.	
间 题 BOOS Policies	an en leg ran , a span (ge nin					75037	-
III Boot Policies	Name	Order	WIC/HEA/SCSI WIC	туре	Lun ID	WWN	
E B Host Pirmulare Packages	CD-ROM	1					
20 Dret Access mones	IG-ELAN	2					- 1
The second prove to be a second to b	LAN FIE Book		PXE-Boot	Prinary			- 11
III. I Mantenarus Policies	Christeller	3					- 1
III Mantanance Polices     III Management Firmware Packages	The set of						
Mantananus Polcas     Management Primare Packages     Software Control Polcases	E E SAN primary		PC-Pabric-A	Primary			
Mantananus Policies     Manageneni Firmware Packages     Si Manageneni Firmware Packages     Si Soruh Policies     Soruh Policies	SAN primary		PC-Pabric-A	Primary Primary	û	50/04/09(82)8D(73:42:07	
III - III Mantanarus Policies     Management Permisere Packages     Privagement Permisere Packages     Policies     Scrub Policies     Scrub Policies     Scrub Policies	SAN primary		PC-Palmo-A	Primary Primary Secondary	0 0	50:04:09(82)80(73:42:07 50:04:09(82)90(73:42:07	
III - III Maintanarus Policies     III - III Managenent Firmware Packages     III - III Power Control Policies     III - III Policies     Social Policies     Social Policies     Social Policies	B ■ 344 primary     SAN Target primary     SAN Target primary     SAN Target secondary     SAN secondary		PC-Palmo A	Primary Primary Secondary Secondary	0 0	50:04:09(82)80(73:42)07 50:04:09(82)50(73:42)07	1
Mantanance Police:     Manageneri Pormere Packages     Manageneri Pormere Packages     Scrub Polices     Scrub Polices     Servir Polices     Servir Polices     Server Poli Polices     Server Pol Police	SAN Target primary		PC-Palmo A PC-Palmo 8	Primary Primary Secondary Secondary Primary	0 0 0	50:04:09(82)80(73:42:07 50:04:09(82)50(73)42:07 50:04:09(82)50(73)42:07	
Mantanarus Policie:     Mantanarus Policie:     Mantagenent Primue Packages     Struk Policie:     Servis Policie:     Servis Policie:     Servis Policie:     Servis Policie:     Servis Policie:     Threshold Policie:     Servis Policie:     Threshold Policie:	SAN Target primary SAN Target primary SAN Target primary SAN Target primary SAN Target secondary		PC-Patric-8	Primary Primary Secondary Secondary Primary Secondary	0 0 0	50:04:09(82)80(73:42:07 50:04:09(82)50(73:42:07 50:04:09(81:90:73:42:07 50:04:09(81:90(73:42:07	

41. Select Boot-Fabric-B Boot Policy and click OK.



And Policy: Boot-Fabric-B Boot Policy: Boot-Fabric-B Boot Policy: Boot-Fabric-A Boot-Fabric-A default Active of diag nforce vNL utility VARNING he type (primary/seconda he effective order of boo f Enforce vNIC/vHBA/i fit is not selected, the vN Boot Order	FY) does not indicate a b devices within the same SCSI Name is selected a (Cs/VHBAs/ISCSI are sele port Print Order 1 2 3	eate Boot Policy oot order presence, : device class (LAN/Storage/ISC and the vNIC/vHBA/ISCSI does :cted if they exist, otherwise th vNIC/vHBA/ISCSI vNIC	CSI) is determine : not exist, a con he vNIC/vHBA/IS Type Primary	d by PCIe bu fig error will SCSI with the Lun ID	ıs scan order. be reported. lowest PCIe bus scan order is u WWN	used.
he type (primary/seconda he effective order of boo f Enforce vNIC/vHBA/if fit is not selected, the vN Boot Order	ry) does not indicate a b devices within the same SCSI Name is selected a lCs/vHBAs/ISCSI are sele port  Print Order 1 2 3	oot order presence. e device class (LAN/Storage/ISC and the vNIC/vHBA/ISCSI does ected if they exist, otherwise th vNIC/vHBA/ISCSI vNIC PXE-Boot	CSI) is determine s not exist, a con the vNIC/vHBA/is Type Primary	d by PCIe bu fig error will SCSI with the Lun ID	us scan order. be reported. lowest PCIe bus scan order is u WWN	used.
Aame CD-ROM CD-ROM LAN LAN Storage SAN primary SAN Targe SAN Targe SAN Targe	1 2 3	PXE-Boot	Primary	LUNID	WWWIN	<b>.</b>
CD+CUM LAN LAN PXE-Boot LAN Storage SAN primary SAN Targe SAN Targe SAN	2	PXE-Boot	Primary			
LAN PXE-Boot	3	PXE-Boot	Primary			
AN PXE-boot	3	PXE-BOOT	Primary			and the second se
SAN primary	3					
SAN Targe		CC Esbrie B	Drimary			
SAN Targe	neimanu		Primary	0	50-0A-00-81-9D-73-47-07	
SAN secondary	secondary		Secondary	0	50-04-09-81-8D:73-42-07	
		FC-Eabric-A	Secondary	, in the second se	50101105101105175112107	
SAN Targe	rorimary	i ci ubici	Primary	0	50:04:09:82:8D:73:42:07	
SAN Targe	secondary		Secondary	0	50:04:09:82:9D:73:42:07	-
Create ISCSI vNIC	Set iSCSI Boot Param	ieters				

42. Select the <code>Network</code> tab and <code>click</code> <code>Modify</code> <code>vNIC/HBA</code> <code>Placement</code> <code>Policy</code>.



<u>.</u>	Actions Change Dampier, and Correction Par	Dynamic V Nothing Se	NC Connection Po lected	akcy .				
a-01 -a-02 -d1 -d12 diore	- Andry All John Receiver	vRIE/vHBA Global Pr Roser 1 Veter	Placement Policy No Host-Indea di Host Listerfaces	r.				
late WHHest-Infra-Fabric A ICs App-Cluster-Comm (CS) LiveMignation		- 20	What Skt	Ansighed Onli Als Als Als Als	dan Freference r	*		
VM-Ceta etwork VM-Ceta-VCAV VM-Mgnit advork VM-Mgnit-VCAN	VNICe							
WHCKSta etwork WHCKSE-KAW WHMpot etwork WHMpot-VLAN (SCSI-Fabric A SCSI-Fabric A	white the mini dig frame a bapart (g) front Name	Mai' Others	Descerif Order	L Schull Partie	L Reburth	Description	Actual Discovery	Name of AN
WHCHAID etwork WHCHCE-VLAN WHHgait etwork WHHgait-VLAN (ICSI-Febre-A CSI-Febre-A CSI-Febre-A	whice a. c. d, rite = toport op hvet Nerve 	MAC Address	Destruct Order	Actual Order	Pebric ID	Descent Placement	Actual Placement	Nativa VLAN
WHORNE etwark WHORSE-KAW WHHgait etwark WHHgait-VLAN (CCSLPatent-A CCSLPatent-A CSSLPatent-A STAN WHERE WHAT Patent A	VHEA	MAC Address Derived	Descried Order	Rotual Order Unspecified	Palane ID A B	Destroit Placement	Actual Flacorverst Acty	Netres VLAN
WHORE etwals WHORE-KAW WHAget WHAget WHAget VLAN (CSI-Fabre A CSI-Fabre A CSI-Fabre A CSI-Fabre A CSI-Fabre A CSI-Fabre A	VINCe	MAC Address Derived	Descrief Order	Sidual Order Unspecified	Palane ID A B	Destroi Placement	Actual Flacement	Native VLAN
WHOODE Bevork WHOODE-KAN WHAIpot anvois WHAIpot-VIAN GCSI-Patric A GCSI-Patric A GCSI-Patric A GCSI-Patric A GCSI-Patric A GCSI-Patric A GCSI-Patric A	VMICe 	MAC Address Derived Derived	Desired Order L	Actual Order Unspecified	Palene ID A B D A	Destract Placement	Actual Placement Any Any	C C
WHOOSE Heven WHOSE-HAN WHApat Anvart WHApat HAN GCSI-Halas A GCSI-Halas A GCSI-Halas A GCSI-Halas A GCSI-Halas A Hores	VNICe 	MAC Address Derived Derived	Desired Order	Rotual Order Unspecified Unspecified	Palane ID A B B A B A	Desired Placevers	Actual Placement Any Any Any	Native VLAN C
INFORME Revense INFORMATIONI INFORMATIONI INFO	WHICH	MAC Address Derived Derived Derived	Destruct Order L 2	Actual Order Unspecified Unspecified Unspecified	Pakes ID AB DA DA	Destroi Maircont 1 1	Actual Theorem A	Native HLAN C C
WEOKIS Weikget Weikget Weikget Weikget Weiker GCS-Falme-A MCS-Ealer-A MCS-EALER-A MCS-EALE	VHICH 	MAC Address Derived Derived Derived Derived	Destruct Order 1 2 3	Adual Orde Unspected Unspected Unspected	Palme ID AB DA DA AB	Destroit Placement	Actual Flacement Any Any Any Any	Native VLAN C C (F
WEONE Bework WEAppl WEAppl WEAppl WEAPPL WEAPPL WEA	VNICA 	MAC Address Derived Derived Derived Derived	Deered Order t 2 3	Actual Order Unspectfiel Unspectfiel Unspectfiel Unspectfiel	Palme ID AB BA BA AB	Denred Placement 1 1 1	Actual Fisconert Any Any Any Any Any	Native VLAN C G G
INF Code Revolus (MP Code - V.CAV) VM - Major Amore VM - Major - V.CAV VM - States - A VM - Code - Code - Code VM - Code - Code - Code VM - Code - Code More - Code - Code - Code More - Code - Code - Code - Code - Code More - Code - Code - Code - Code - Code More - Code - Code - Code - Code - Code More - Code - Code - Code - Code - Code More - Code - Code - Code - Code - Code More - Code - Code - Code - Code - Code More - Code - Code - Code - Code - Code More - Code - Code - Code - Code - Code More - Code - Code - Code - Code - Code More - Code - Code - Code - Code - Code - Code More - Code - Code - Code - Code - Code - Code More - Code - Code - Code - Code - Code - Code More - Code - Code - Code - Code - Code - Code More - Code - Code - Code - Code - Code - Code More - Code - Code - Code - Code - Code - Code More - Code - Code - Code - Code - Code - Code - Code More - Code - Cod	VINC:	MAC Address Derived Derived Derived	Desmed Order L 2 3 4 5	Actual Order Unspectived Unspectived Unspectived Unspectived	Pakes ID AB DA DA AB AB	Destroit Placement 1 1 1	Actual Tisconvert Any Any Any Any Any Any	Network MAN C C F
WEOKID WHORE SEARCH WHORE WHORE A WORK WHORE A WORK WHORE A WITH A SEARCH WITH A SEARCH W	VHICH	MAC Address Derived Derived Derived Derived	Desired Order 1 3 4 5	Adual Onler Uniperfied Uniperfied Uniperfied Uniperfied Uniperfied	Palment) AB DA DA AB AB	Desired Flateneers	Actual Placement Any Any Any Any Any Any	Native VLAN C G G G
Information of the second seco	VHICE  VHICE	MAC Address Derived Derived Derived Derived	Desred Order L 2 3 4 5	Adual Order Unipedied Unipedied Unipedied Unipedied	Paine ID AB DA DA AB AB	Denred Placement	Actual Flacourert Arry Arry Arry Arry Arry Arry Arry	Natives VLAN C C G G G
onto WHY Cost - KAN Mynk An Anno A An Anno A Anno A An Anno A Anno A Anno A An Anno A Anno Anno	VHICH	MAC Address Derived Derived Derived Derived	Desmed Order 1 2 3 4 5 6	Actual Order Uniper/Ned Uniper/Ned Uniper/Ned Uniper/Ned Uniper/Ned Uniper/Ned	Pakric ID AB DA DA AB AB AB	Desired Placement	Actual Placement Arry Arry Arry Arry Arry Arry Arry	Name HAN C G G G
Moots work WHOse-YCAH HHAput Nook WHAput-NCAH SCI-Patro A York Anton Anna Anna Moots Anna Anna Anna Patro Anna Anna Anna Patro Anna Anna Patro Anna Anna Anna Anna Anna Anna Anna Anna	VHICH	MAC Address Derived Derived Derived Derived Derived	Descred Order 1 2 3 4 5 6	Actual Order Unspeched Unspeched Unspeched Unspeched Unspeched Unspeched	Pakes ID AE DA BA AB AB AB	Coursed Placement	Actual Placement Arry Arry Arry Arry Arry Arry Arry Arr	Native VLAN C C G G G G

43. Move vHBA Fabric-B ahead of vHBA Fabric-A in the placement order and click OK.

er nærdivære conniguration inde	dCs and vHBAs are placed ependent way.	on physical network adapters (a	nezzarine)				
t Placement: VM-Host-Infra	. 0	Greate Placement Policy					
a Network Interface connects s and vHBAs are assigned to	on provides a mechanism o one of Virtual Network Inte	I placing vNBCs and vHBAs on pl efface connection specified below	hysical netwo w. This assign	inh adapters. Iment can be			
med explicitly by selecting w	Noh Virtual Network Interf	ace connection is used by vNIC of	or viela or it	can be done			
natically by selecting "any". (vHBA placement on physical	network interface is contro	ded by placement preferences.					
and the second second		and the second se					
e select one Virtual Network I	interface and one or more	VNICs or VHBAs					
	00001000	MODEL 101 1014	411				
	Virtual N	stwork Interfaces Policy (read or	nhy)				
ICs VHEAS		Name		Order	Selection Preference		
Name 📿		- VNIC VM-Mgnt	5			1	
-		VNIC ISCSI-Pabric-A	6				
22.84	10722:	VNDC ISCSI-Fabric-B	7			1.1	
Course of the second	1100 02	VHBA Fabric 8	8				
	1012 101	NE VIBA PADIC-A	1.85			_	
		v.on z				- 1	
		vicen d				-	
		PLAN 1		-		20	
			Strength, 1	Theve Down (			
-							
<u>.</u>							



#### **Create Service Profiles**

These steps provide details for creating a service profile from a template.

#### **Cisco UCS Manager**

- 1. Select the Servers tab at the top left of the window.
- 2. Select Service Profile Templates VM-Host-Infra-Fabric-A
- 3. Right-click and select Create Service Profile From Template.
- 4. Enter VM-Host-Infra-0 for the service profile prefix.
- 5. Enter 1 for the number of service profiles to create.
- 6. Click OK to create the service profile.

Create Service Profiles From Template	×
Create Service Profiles From Template	0
Naming Prefix: VM-Host-Infra-0 Number: 1	
ОК	ancel

- 7. Click OK in the message box.
- 8. Select Service Profile Templates VM-Host-Infra-Fabric-B
- 9. Right-click and select Create Service Profile From Template.
- **10.** Enter VM-Host-Infra-0 for the service profile prefix.
- 11. Enter 1 for the number of service profiles to create.
- 12. Click OK to create the service profile.

Create Service Profiles From Template	×
Create Service Profiles From Template	0
Naming Prefix: VM-Host-Infra-0 T Number: 1 T	
ОК	Cancel



- 13. Click OK in the message box.
- 14. Verify that Service Profiles VM-Host-Infra-01 and VM-Host-Infra-02 are created. The service profiles will automatically be associated with the servers in their assigned server pools.

Image: Source in Source i	Fault Summary	😡 🕕 🖬 New - 😥 Options 👘 🕕 🧥	mana karana 🔯 ba	
Example       Sector		>> _ teves - Steves infes - A root	Service Profile WHeat Info-02	Service Profile VM Heat Infra-1
A Sub-Departmentors	Experient Seneral Law SAN an Adam Teller: Al - Teller: A	Serent Denne (Network SCCI vicio Serent Park Samanery 2 2 2 2 5 2 5 2 5 2 5 2 5 2 5 2	Criter (Versal Hadrons   Polonis   Serve Details   PIPA' VEP Polonis   Fuelds   Dennis Properties Pending Activities Pending Dampitons: Pending Dampitons: Pendin	

#### Add a Block of IP Addresses for KVM Access

These steps provide details for creating a block of KVM ip addresses for server access in the Cisco UCS environment.

#### **Cisco UCS Manager**

- 1. Select the Admin tab at the top of the left window.
- 2. Select All > Communication Management.
- 3. Right-click Management IP Pool.
- 4. Select Create Block of IP Addresses.
- 5. Enter the starting IP address of the block and number of IPs needed as well as the subnet and gateway information.
- 6. Click OK to create the IP block.
- 7. Click OK in the message box.

#### Synchronize Cisco UCS to NTP

These steps provide details for synchronizing the Cisco UCS environment to the NTP server.

#### **Cisco UCS Manager**

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



- 2. Select All > Timezone Management.
- 3. Right-click Timezone Management.
- 4. In the right pane, select the appropriate timezone in the Timezone drop-down menu.
- 5. Click Save Changes and then OK.
- 6. Click Add NTP Server.
- 7. Input the NTP server IP and click OK.

#### Add More Server Blades to the FlexPod Unit

Add server pools, service profile templates, and service profiles 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 Necessary Information**

After the Cisco UCS service profiles have been created (in the previous steps), the infrastructure blades in the environment each have a unique configuration. To proceed with the FlexPod deployment, specific information must be gathered from each Cisco UCS blade and from the NetApp controllers. Insert the required information in the tables below.

NetApp Controller	FC Port	FC Portname
Controllor A	0c	
Controller A	0d	
Controllor P	0c	
Controller B	Od	

### Note: On each NetApp controller use show fcp adapters to gather the information above. If using FCoE between storage and the Cisco Nexus 5548s, substitute 2a for 0c and 2b for 0d.

Cisco UCS Service Profile Name	Fabric-A WWPN	Fabric-B WWPN
VM-Host-Infra-01		
VM-Host-Infra-02		

**Note:** To gather the information in the table above, launch the Cisco UCS Manager GUI, and in the left pane select the Servers tab. From there, expand Servers > Service Profiles > root > . Click each service profile and then click the Storage tab on the right. While doing so, record the WWPN information in the right display window for both vHBA\_A and vHBA\_B for each service profile in the table above.

### Cisco Nexus 5548 Deployment Procedure: Part 2

These steps provide details for completing the configuration of the Nexus infrastructure for the FlexPod environment.

#### Create VSANs, Assign FC Ports, Turn on FC Ports

These steps provide details for configuring VSANs, assigning FC ports and enabling FC ports.

# cisco



**Note:** This procedure sets up Fibre Channel connections between the Nexus 5548s and the NetApp Storage Systems. If you want to use FCoE connections between the Nexus 5548s and the NetApp Storage Systems using the NetApp Unified Target Adapter (UTA). Use the Alternate Cisco Nexus 5548 Deployment Procedure: Part 2 in the Appendix.

#### Cisco Nexus 5548 A

- 1. From the global configuration mode, type interface san-port-channel 1.
- 2. Type channel mode active.
- 3. Type exit.
- 4. Type vsan database.
- 5. Type vsan <VSAN A ID> name Fabric\_A.
- 6. Type vsan <VSAN A ID> interface fc1/29-32.
- 7. Type vsan <VSAN A ID> interface san-port-channel 1.
- 8. Type exit.
- 9. Type interface fc1/31-32.
- 10. Type channel-group 1 force.
- 11. Type no shutdown.
- 12. Type exit.
- 13. Type interface fc1/29-30.
- 14. Type no shutdown.
- 15. Type exit.
- 16. Type show int san-port-channel 1 to confirm connectivity.
- 17. Type interface fc1/29.
- 18. Type switchport description <Controller A:Oc>.
- 19. Type exit.
- 20. Type interface fc1/30.
- 21. Type switchport description <Controller B:Oc>.
- 22. Type exit.
- 23. Type interface fc1/31.
- 24. Type switchport description <UCSM A:fc1/31>.
- 25. Type exit.
- 26. Type interface fc1/32.
- 27. Type switchport description <UCSM A:fc1/32>.
- 28. Type exit.

#### Cisco Nexus 5548 B

- 1. From the global configuration mode, type interface san-port-channel 2.
- 2. Type channel mode active.
- 3. Type exit.



- 4. Type vsan database.
- 5. Type vsan <VSAN B ID> name Fabric\_B.
- 6. Type vsan <VSAN B ID> interface fc1/29-32.
- 7. Type vsan <VSAN B ID> interface san-port-channel 2.
- 8. Type exit.
- 9. Type interface fc1/31-32.
- 10. Type channel-group 2 force.
- 11. Type no shutdown.
- 12. Type exit.
- 13. Type interface fc1/29-30.
- 14. Type no shutdown.
- 15. Type exit.
- 16. Type show int san-port-channel 2 to confirm connectivity.
- 17. Type interface fc1/29.
- 18. Type switchport description <Controller A:Od>.
- 19. Type exit.
- 20. Type interface fc1/30.
- 21. Type switchport description <Controller B:Od>.
- 22. Type exit.
- 23. Type interface fc1/31.
- 24. Type switchport description <UCSM B:fc1/31>.
- 25. Type exit.
- 26. Type interface fc1/32.
- 27. Type switchport description <UCSM B:fc1/32>.
- 28. Type exit.

#### **Create Device Aliases and Create Zones**

These steps provide details for configuring device aliases and zones for the primary boot path. Instructions are given for all target ports, however, the redundant path is enabled following operating system installation..

#### Cisco Nexus 5548 A

- 1. From the global configuration mode, type device-alias database.
- 2. Type device-alias name VM-Host-Infra-01 A pwwn <Fabric-A WWPN>.
- 3. Type device-alias name VM-Host-Infra-02 A pwwn <Fabric-A WWPN>.
- 4. Type device-alias name controller A Oc pwwn <Controller A Oc WWPN>.
- 5. Type device-alias name controller\_B\_Oc pwwn <Controller B Oc WWPN>. Get this information from the table in section Gather Necessary Information.
- 6. After all of the necessary device-alias are created, type exit.



- 7. Type device-alias commit.
- 8. Create the zone for each service profile.
  - a. Type zone name VMVM-Host-Infra-01 A vsan <Fabric A VSAN ID>.
  - b. Type member device-alias ucs controller A Oc1 A.
  - c. Type member device-alias controller A Oc.
  - d. Type exit.
- 9. After the zone for the primary path of the first Cisco UCS service profiles has been created, create a zoneset to organize and manage them.
- 10. Create the zoneset and add the necessary members.
  - a. Type zoneset name flexpod vsan <Fabric A VSAN ID>.
  - b. Type member ucs controller A Oc1 A.
  - c. Type exit.
- 11. Activate the zoneset.
  - a. Type zoneset activate name flexpod vsan < Fabric A VSAN ID>.
  - b. Type exit.
- 12. Type copy run start.

#### Cisco Nexus 5548 B

- 1. From the global configuration mode, type device-alias database.
- 2. Type device-alias name VMVM-Host-Infra-01 B pwwn <Fabric-B WWPN>.
- 3. Type device-alias name ucs controller B 0d1 B pwwn <Fabric-B WWPN>.
- 4. Type device-alias name controller A Od pwwn <Controller A Od WWPN>.
- 5. Type device-alias name controller\_B\_0d pwwn <Controller B 0d WWPN>. Get this information from the tables in the section Gather Necessary Information.
- 6. After all of the necessary device-alias are created, type exit.
- 7. Type device-alias commit.
- 8. Create the zones for each service profile.
  - a. Type zone name VM-Host-Infra-02 B vsan <Fabric B VSAN ID>.
  - b. Type member device-alias ucs controller B 0d1 B.
  - c. Type member device-alias controller B Od.
  - d. Type exit.
- 9. After all of the zones for the Cisco UCS service profiles have been created, create a zoneset to organize and manage them.
- 10. Create the zoneset and add the necessary members.
  - a. Type zoneset name flexpod vsan <Fabric B VSAN ID>.
  - b. Type member VM-Host-Infra-02\_B.
  - c. Type exit.
- 11. Activate the zoneset.
  - a. Type zoneset activate name flexpod vsan <Fabric A VSAN ID>.





#### b. Type exit.

12. Type copy run start.

### NetApp FAS3240A Deployment Procedure: Part 2

The following sections provide detailed procedures for configuring the interface groups (or igroups), creating LUNs for the service profiles on the storage controllers, and mapping those LUNs to the igroups to be accessible to the service profiles.

#### **Create iGroups**

These steps provide details for configuring the necessary iGroups on the storage controller which enable the mapping of a given host the its storage resources.

#### Controller A

These steps provide details for assigning igroup configuration for each vHBA.

```
igroup create -f -t hyper_v VMVM-Host-Infra-01 <Fabric-A WWPN> <Fabric-B
WWPN>.
```

igroup set VMVM-Host-Infra-01 alua yes.

#### **Controller B**

For the first service profile to boot off of controller B do the following to create igroups for each vHBA:

igroup create -f -t hyper v VM-Host-Infra-02<Fabric-A WWPN> <Fabric-B WWPN>.

igroup setVM-Host-Infra-02alua yes.

#### **Create LUNs**

These steps provide details for configuring the necessary LUNs on the storage controller for deployment of the SAN booted Windows 2008 R2 SP1 operating system. This LUN, when prepared, will be used as the base for cloning multiple installations.

#### **Controller A**

For the first service profile to boot off of controller A do the following to create the LUN for the OS installation:

lun create -s 250g -t hyper v -o noreserve /vol/win boot A/ hyper-v-host

#### Map LUNs to iGroup

These steps provide details for mapping the necessary LUN on the storage controller to the created iGroups.

#### **Controller A**

For the first service profile to boot off of controller A map the LUN for the OS installation:

lun map /vol/win boot A/hyper-v-host VM-Host-Infra-01 0.





### Prepare the Host for Windows Server 2008 R2 SP1 Installation

These steps provide the details necessary to prepare the host for the installation of Windows Server 2008 R2.

**Note:** In order for the Windows Installer to recognize the Fiber Channel SAN boot disk for each server, the Cisco UCS fnic driver must be loaded into the windows installer during installation. Please download the latest Unified Computing System (UCS) Drivers from <u>www.cisco.com</u> under Cisco UCS B-Series Blade Server Software and place the iso on the same machine with the Windows Server 2008 R2 SP1 DVD iso.

### **Cisco UCS Manager**

- 1. In the KVM window, select the Virtual Media tab.
- 2. Click the Add Image... button in the window that displays.
- 3. Browse to the Windows Server 2008 R2 SP1iso image file.
- 4. Click Open to add the image to the list of virtual media.
- 5. Click the checkbox for Mapped next to the entry corresponding to the image you just added.
- 6. In the KVM window, select the KVM tab to monitor during boot..
- 7. In the KVM window, select the Boot Server button in the upper left corner.
- 8. Click OK.
- 9. Click OK.

### Install Windows Server 2008 R2

These steps provide the details necessary for the installation of Windows Server 2008 R2.

#### **Cisco UCS Manger**

- 1. In the KVM window, select the Boot Server button in the upper left corner.
- 2. Click OK.
- 3. Click OK.
- 4. Reboot the blade using the Boot Server button at the top of the KVM window.

Note: It does not matter whether you use a soft or hard reboot, because the blades do not have an OS.

- 5. On reboot, the machine detects the presence of the Windows Server 2008 R2 SP1install media.
- 6. Select Next from the Install Windows window that displays and proceed to install Windows Server 2008 R2 SP1DataCenter Edition Full Installation.

**Note:** During installation the Cisco VIC FCoE Storport Miniport driver will need to be loaded.

7. When the screen displays to select the installation disk, select Load Driver.



G A Install Windows					
Where do you want	to install Window	s?			
Name		Total Size	Free Space Type		
Sefresh       Drive options (advanced)         Image: Load Driver       Image: Load Driver         Image: No drives were found. Click Load Driver to provide a mass storage driver for installation.					
			<b>₽</b>	Next	

- 8. In order to load the appropriate driver, unmap the Windows Installer DVD in the Virtual Media tab.
- 9. Browse to and map the Cisco Drivers iso downloaded earlier.
- 10. Browse to the \Windows\Storage\Cisco\M81KR\W2K8R2\x64 folder on the mounted iso.

Load Driver				
To install the device driver meeded to access your hard drive, insert the installation media containing the driver files, and then click OK.				
Note: The installation media can be a floppy disk, CD, DVD, or USB flash drive.				
<u>B</u> rowse OK Cancel				





Browse for Folder				
Browse to the driver(s), and then dick OK				
<ul> <li>Computer</li> <li>Floppy Disk Drive (A:)</li> <li>Removable Disk (C:)</li> <li>CD Drive (D:) CD_ROM</li> <li>Boot (X:)</li> </ul>				
OK Cancel				

11. The Cisco VIC FCoE StorePort Drive will be selected. Click Next to load the driver.

0	Notall Windows	×
	Select the driver to be installed.	
	Cisco VIC FCoE Storport Miniport (D:\fnicwl64.inf)	
	Lide driver that are not compatible with bardware on this computer	
	The drivers that are not compatible with hardware on this computer.	
	Browse Rescan	lext

- 12. Switch to the Virtual Media tab.
- 13. Uncheck the check box for the currently mapped ISO image for Mapped next to the entry corresponding to the image you just added.





- 14. Remap the Windows Installer DVD by checking the Mapped box next to the ISO image.
- 15. Switch back to the KVM tab.
- 16. The boot LUN will now be visible as a selectable storage device for the Windows installation. Click the Refresh button to allow the installer to recognize the Windows Installer DVD.

<u> </u>	🍹 Instal	l Windows			×
	Where	e do you want to install Window	s?		
		Name	Total Size	Free Space Type	
		Disk 1 Unallocated Space	60.0 GB	60.0 GB	
		_			
ા	Mathematical System         Drive options (advanced)			iced)	
	🕑 <u>L</u> oad	d Driver			
<b>A</b>	<u>W</u> indow	rs cannot be installed to this disk. (Show o	details)		
					Next

17. Click Next to continue with installation. Do a standard installation of Windows Server 2008 R2 SP1DataCenter Edition.



Name		Total Size	Free Space	Type
Disk 1 Unal	llocated Space	60.0 GB	60.0 GB	.,,
€ <u>↑ R</u> efresh			Drive option	s ( <u>a</u> dvanced)

- **Note:** Detailed steps for the installation of Windows Server 2008 R2 SP1DataCenter Edition are not provided. Please reference Microsoft documentation in for this information.
- 18. Following completion of the installation of Windows 2008 R2, which may require several server reboots, log into the server with an administrative account.
- 19. In the KVM window, select the Virtual Media tab.
- 20. Click the Add Image... button in the window that displays.
- 21. Browse to the Cisco Drivers iso image file.
- 22. Click Open to add the image to the list of virtual media.
- 23. Click the checkbox for Mapped next to the entry corresponding to the image you just added.
- 24. Within the KVM console of the host, browse to Device Manager. This can be accomplished by rightclicking My Computer and selecting Properties and selecting Device Manager.
- 25. Select the first Ethernet Controller in the Other Devices category.
- 26. Right-click and select Update Driver Software.
- 27. Click Browse my computer for driver software and browse to the \Windows\Network\Cisco\M81KR\W2K8R2\x64 folder on the virtual CD drive.

 $28. \ Click \ {\tt Next} \ .$ 

- **29.** Click Close to complete the driver installation.
- **30.** At the top of the Device Manager window, click Action > Scan for Hardware Changes button to install the Cisco driver to the remaining Ethernet interfaces.
- 31. Click the x at the top right corner to close the Device Manager window.





**Note**: At this point, if you have a DHCP server installed on your Management Network, the Management Network Interface should come up with an IP address. If you do not have DHCP, use the later procedure "Configure Network Interfaces and Rename Server" to determine which Network Interface is on the Management VLAN and configure it with a static IP with connection to the outside world.

- 32. Right-click My Computer and select Manage.
- 33. The Server Manager window displays.
- 34. Right-click Features.
- 35. Install the following features:
  - .NET Framework 3.5.1 Features. (WCF Activation is not required)
  - Multipath I/O
- 36. Return to Server Manager and right-click Roles.
- 37. Select Add Role.
- 38. Select the Hyper-V role and click Next to complete the installation wizard.
- 39. Chose the option not to reboot the server. The server will be rebooted after the next step.

### **Configure MPIO**

- 1. Click Start, select Administrative Tools, and click MPIO
- 2. Click the Add button and enter NETAPP LUN. (There are two spaces between NETAPP and LUN)

Add MPIO Support	X
Enter the Vendor and Product Ids (a: 16 characters) of the devices you wa	s a string of 8 characters followed by ant to add MPIO support for.
Device Hardware ID:	
NETAPP LUN	
R	OK Cancel

- 3. A reboot is required. Click OK to reboot the server.
- 4. After the server reboots, login again with administrator rights and open the MPIO configuration utility again.
- 5. Verify the NETAPP LUN entry is in the list.
- 6. Open the Device Manger by clicking Start > Run, and typing devmgmt.msc.
- 7. Expand the Disk Drives node and verify that you entered the NETAPP LUN Multi-Path Disk Device. Additional SAN paths for redundancy.

### **Install Microsoft Hotfixes**

Install the following Windows HotFixes:

• KB2517329,



- KB2552040,
- KB2522766
- KB2528357.

This will require multiple reboots.

### **Create Zones for Redundant Paths**

These steps provide details for configuring zones for the redundant boot path for each service profile.

**Note:** If FCoE is being used between the Nexus 5548s and Storage, use the Alternate Create Zones for Redundant Paths section in the Appendix.

#### Cisco Nexus 5548 A

- 1. From the global configuration mode, create the zones for the redundant path for each service profile.
  - a. Type zone name VM-Host-Infra-01\_A vsan <Fabric A VSAN ID>.
    - 1. Type member device-alias controller\_B\_Oc.
    - 2. Type exit.
    - 3. Type zone name VM-Host-Infra02\_A vsan <Fabric A VSAN ID>.
    - 4. Type member device-alias VM-Host-Infra02\_A.
    - 5. Type member device-alias controller\_B\_Oc.
    - 6. Type member device-alias controller\_A\_Oc.
    - 7. Type exit.
- 2. Modify the zoneset and add the necessary members.
  - a. Type zoneset name flexpod vsan <Fabric A VSAN ID>.
    - 8. Type member VM-Host-Infra-02.
    - 9. Type exit.
- 3. Activate the zoneset.
  - a. Type zoneset activate name flexpod vsan <Fabric A VSAN ID>.
    - 10. Type exit.
    - 11. Type copy run start.

#### Cisco Nexus 5548 B

- 1. From the global configuration mode, create the zones for the redundant path for each service profile.
  - a. Type zone name VM-Host-Infra-01 B vsan <Fabric B VSAN ID>.
  - b. Type member device-alias alias VM-Host-Infra-01\_B.
  - c. Type member device-alias controller A Od.
  - d. Type member device-alias controller\_B\_0d.
  - e. Type exit.
  - f. Type zone name VM-Host-Infra-02\_B vsan <Fabric B VSAN ID>.
  - g. Type member device-alias controller A Od.
  - h. Type exit.
- 2. Modify the zoneset and add the necessary members.



- a. Type zoneset name flexpod vsan <Fabric B VSAN ID>.
- b. Type member VM-Host-Infra-01\_B.
- c. Type exit.
- 3. Activate the zoneset.
  - a. Type zoneset activate name flexpod vsan <Fabric B VSAN ID>.
  - b. Type exit.
- 4. Type copy run start.

### Verify MultiPath I/O Connections (Both Hyper-V Hosts)

#### **Both Cisco UCS Hosts**

- 1. Open the Device Manger by clicking Start > Run, and typing devmgmt.msc.
- 2. Expand the Disk Drives node and verify that you entered the NETAPP LUN Multi-Path Disk Device. Additional SAN paths for redundancy.

### **Clone the Windows Server 2008 R2 SP1 Installation**

During these steps, you will be guided through the creation of a golden Windows image which once created is used for rapid cloning of the Windows 2008 R2 SP1 installation. At this point, the boot LUN for the first server can be cloned and prepared using Microsoft Sysprep to be used for host VM-Host-Infra-02 and future Servers.

Cloning is a NetApp feature that enables the rapid provisioning of resources while requiring very little storage at the time of creation. If this process is used, it is important to have only one fabric path enabled, through zoning, for the given server. Following server provisioning, multipath I/O and the NetApp DSM is installed.

If an alternative method for installing Windows is being used, such as Windows Deployment Services, then cloning the boot LUN is not necessary.

#### **Cisco UCS Manager**

- 1. Within the KVM console of the host, confirm that all Windows updates have been installed. Windows Update will display a status of Windows is up to date.
- 2. Select Start > Logoff > Shut down to power down the host.

#### **NetApp Controller A**

- 1. Clone the first boot LUN, by typing clone start /vol/win\_boot\_A/hyper-v-host /vol/win boot A/hyper-v-template. Wait for the clone operation to complete.
- 2. Unmap the first boot LUN by typing lun unmap /vol/win\_boot\_A/hyper-v-host VM-Host-Infra-01.
- 3. Map the cloned LUN by typing lun map /vol/win\_boot\_A/hyper-v-template VM-Host-Infra-01 0

#### **Cisco UCS Manager**

- 1. Within the KVM console of the host, boot the server and log in with an administrator account.
- 2. Click Restart Later if prompted to restart the server.




3. Launch C:\Windows\system32\sysprep\sysprep.exe. Select the Generalize button and the Shutdown option. The server should prep then shutdown.

#### **NetApp Controller A**

- 1. Clone the Hyper-V Golden Template LUN by typing clone start /vol/win\_boot\_A/hyper-vtemplate /vol/win boot A/ VM-Host-Infra-01. Wait for the clone operation to complete.
- 2. Unmap the Hyper-V Golden Template LUN by typing lun unmap /vol/win\_boot\_A/hyper-v-template VM-Host-Infra-01.
- 3. Map the cloned LUN by typing lun map /vol/win\_boot\_A/ VM-Host-Infra-01 VM-Host-Infra-01 0.
- 4. Make sure that ndmpd is enabled on both NetApp controllers by typing ndmpd on on both controllers.
- 5. Copy the Hyper-V Golden Template LUN from NetApp Controller A to NetApp Controller B by typing ndmpcopy -da <ControllerB username>:<password> /vol/win\_boot\_A/hyper-vtemplate <ControllerB IP>:/vol/win\_boot\_B/. You now have a copy of the golden Hyper-V LUN on each storage controller, and a LUN of the host image that can be updated and Sysprepped in the future on Controller A.

#### **NetApp Controller B**

- 1. Online the just-copied LUN by typing lun online /vol/win boot B/hyper-v-template.
- 2. Clone the Hyper-V Golden Template LUN, by typing clone start /vol/win\_boot\_B/hyper-v-template /vol/win\_boot\_B/VM-Host-Infra-02. Wait for the clone operation to complete.
- 3. Map the cloned LUN by typing lun map /vol/win\_boot\_B/ VM-Host-Infra-02 VM-Host-Infra-02 0.

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

- 1. Using the UCS KVM Console, boot up both hosts.
- 2. Complete Windows Setup.

# Configure Network Interfaces, Rename Servers, and Install Microsoft Windows Updates on Both Hyper-V Hosts

These steps provide details for naming the Windows network interfaces according to the VLANs in which they reside for VM-Host-Infra-01. This is achieved by matching the MAC addresses assigned in the service profile with the network interfaces presented in the operating system. Also, during this section, the server is renamed as well as Windows Updates performed. Repeat these steps for the second Hyper-V host.

#### **Cisco UCS Manager**

- 1. In the KVM window, select the Properties tab.
- 2. Select the Network tab. The corresponding vNICs are displayed along with their MAC addresses.



	Help								
Startforver Shutdow	m Server 🙁 Reset								
M Console Properties									
General Scrace Network	SCSI vNICa Boot Order	Vetual Ma	chines   Policies   Serve	r Details   Faults   Events					
	÷	Salar march	and the second						_
Actions		Dynamic	vMIC Connection Pol	licy					
		Nothing	Selected						
most australia		William Ale							
		WNIE/VHI	<b>BA Placement Policy</b>						
		Nothing:	Selected						
		Nothing :	Selected						
white		Nothing :	Selected						
vNICs.		Nothing :	Selected						
vNEs ¶rike → Espot @Pir	¢	Nothing :	Selected			1			
vhites d, Filter - Export - Go Pir Name:	n MAC Address	Nothing 1	Selected Desired Order	Actual Order	Pabric 10	Desired Placement		Actual Placement	12
vNICs	<ul> <li>MAC Address 00:25:85:E1:26:ED</li> </ul>	Nothing 1	Selected Desired Order	Actual Order	Pabric ID B A	Desired Placement	1	Actual Placement	17
VNICA II, Piller  = Export (25 Pir None VIGC Apo-Cluster-Comm II VIGC CSV	MAC Address 00:25:65:E1:25:ED 00:25:65:E1:27:0F	Nothing 1	Selected Desired Order	Actual Order 7	Pabric 10 B A A B	Desired Placement Any Any	1	Actual Placement	17
vNECs d Title → Doort (@ Prin Name: Title App-Ouster-Comm - WID Care - WID Care - WID Care	r MAC Address 00:25:85:E1:25:ED 00:25:85:E1:25:0F 00:25:85:E1:25:EF	Nothing 1	Selected Desired Order	Actual Order 7 3	Pabric ID B A A B B A	Desired Placement Any Any Any	1	Actual Placement	17 
vhtEx I, Riter i - Diport i up Prin Name: Pi vHD: App-Cluster-Comm - vHD: Com - vHD: Chrefig alon - vHD: WHOata	<pre># MAC Address 00:25:85:E1:26:ED 00:25:85:E1:27:0F 00:25:85:E1:26:CF 00:25:85:E1:26:CF</pre>	Nothing 1	Selected Desired Order	Actual Order 7 9 2	Patric 10 B A A B B A A B	Desired Hacement Any Any Any Any	1	Actual Placement	1
VNIC: C Piler = Export (S Pile Name: VIDC App-Ouster-Comm - WIDC CSV - WIDC LiveNignation - WIDC LiveNignation - WIDC VM-Oata - WIDC WM-Oata	F TMAC Address T0125:85:E1:26:ED T0125:85:E1:26:EF T0125:85:E1:26:EF T0125:85:E1:26:EF	Nothing 1	Selected Desired Order	Actual Order 7 3 4 2 1	Palanc 30 8 A A B 8 A A B A B A B	Desired Placement Any Any Any Any Any Any		Actual Placement	
VNICA II, Piller de Doont (20 Pir Name VIGC Ap-Cluster-Comm VIGC LiveNigration VIGC VN-Alla VIGC VN-Allare VIGC VN-Allare VIGC SS-Fabric A	<ul> <li>MAC Address</li> <li>00:25:65:E1:26:ED</li> <li>00:25:65:E1:27:0F</li> <li>00:25:65:E1:26:CF</li> <li>00:25:65:E1:26:CF</li> <li>00:25:65:E1:26:CF</li> <li>00:25:65:E1:26:CF</li> </ul>	Nothing 1	Selected Desired Order	Actual Order 7 3 4 2 1 5	Pabric ID II A A B B A A B A B A B A B A	Desired Placement Any Any Any Any Any Any Any		Actual Placement	11 A

- 3. Within the KVM console of the host, browse to the Network Connections window, This can be accomplished by selecting Start and right-clicking Network. Then in the Network and Sharing Center that displays, select Change Adapter Settings.
- 4. Right-click the first network adapter.
- 5. Select Status.







6. In the Status window that appears, select the Details button.



🖣 Local Area Connect	tion 3 Statu	IS	×
General	43		
'			
Connection			,
IPv4 Connectivity:		No netwo	ork access
IPv6 Connectivity:		No netwo	ork access
Media State:			Enabled
Duration:			01:24:30
Speed:			10.0 Gbps
Details			
Activity			
	Sent —	<b>!</b>	Received
Packets:	1,161	T.	0
Properties	🕑 Disable	Diagnose	
			<u>C</u> lose

7. In the Network Connection Details window, note the Physical Address, which is the MAC address for the vNIC.



**Note:** Cross-reference this address with the MAC addresses for the provisioned vNICs as detailed in step 2 of this section.

Ne	etwork Connection Detai	ils X
	Network Connection Details:	
	Property	Value
	Connection-specific DN	
	Description	Cisco VIC Ethernet Interface #8
	Physical Address	00-25-R5-E1-26-ED
	DHCP Enabled	Yes
	Autoconfiguration IPv4	169.254.132.111
	IPv4 Subnet Mask	255.255.0.0
	IPv4 Default Gateway	
	IPv4 DNS Server	
	IPv4 WINS Server	v
	NetBIOS over Topip En	
	IPv6 Default Gateway	1690::00941008:1090:846F%46
	IPv6 DNS Servers	fec0:0:0.ffff::1%1
		fec0:0:0:ffff::2%1
		fec0:0:0.ffff::3%1
	<u> </u>	
		Qlose

8. Click Close.

9. In the Network Connection window, right-click the interface whose MAC address was just determined.

10. Select Rename.





11. Name the interface the same as the corresponding vNIC within the service profile provisioned within Cisco UCS Manager.







- 12. Repeat this process for all network interfaces.
- 13. Following renaming of all the network interfaces, configure the binding order.
- 14. In the Network Connection window, press the ALT key and hold for a few seconds until the Menu Bar displays.
- 15. Click Advanced > Advanced Settings...
- 16. Under the Connections section of the Advanced Settings window, use the arrows to modify the binding order. The recommended binding order is:
  - a. VM-Data
  - b. App-Cluster-Comm
  - c. Live Migration
  - d. CSV
  - e. VM-Mgmt
  - f. iSCSI Fabric-A





g. iSCSI-Fabric-B

Advanced Settings	X
Adapters and Bindings Provider Order	
Connections are listed in the order in which they are accessed network services.	by
Connections:	
→ VM-Data → App-Cluster-Comm → LiveMigration → CSV	• t •
Bindings for iSCS-Fabric-B:	
□ ➡ File and Printer Sharing for Microsoft Networks □ ➡ Internet Protocol Version 6 (TCP/IPv6)	t
Internet Protocol Version 4 (TCP/IPv4)     Image: A constant of the second	\$
Internet Protocol Version 6 (TCP/IPv6)     internet Protocol Version 4 (TCP/IPv4)	
ОК	Cancel

- 17. Click OK to set the binding order.
- 18. In the Network Connection window, right-click individual interfaces (excluding VM-Data and App-Comm-Cluster) and select Properties to navigate to the interface properties, enabling IP address assignment.
- 19. Assign IP addresses to all interfaces except the VM-Data and App-Comm-Cluster interfaces.
- 20. Click the x at the top right corner to close the Network Connections window.
- 21. Within the KVM console of the host, browse to the System window. This can be accomplished by right-clicking My Computer and selecting Properties.
- 22. In the System window that displays, select Change Settings.
- 23. In the System Properties window that displays, select Change.
- 24. Assign the Server Hostname and Workgroup.
- 25. Click OK.
- 26. A restart is required. Click OK.
- 27. Following reboot, log-in to the server with an administrator account.
- 28. Within the KVM console of the host, browse to the System window. This can be accomplished by right-clicking My Computer and selecting Properties.
- 29. Install all Windows Updates on the server by selecting the Windows Update link in the lower left-hand corner.



### Install the Failover Cluster Feature

#### Cisco UCS Hosts VM-Host-Infra-01 and HostVM-Host-Infra-02

- 1. In Server Manager, right-click Features and select Add Features.
- 2. Check Failover Cluster and click Next.
- 3. Click Install.

### Install NetApp MultiPath IO Tools on Both Hyper-V Hosts

#### Cisco UCS Hosts VM-Host-Infra-01 and HostVM-Host-Infra-02

- 1. Using the UCS KVM Console,download NetApp SnapDrive for Windows version 6.4 64-bit from the NetApp on the Web (NOW) website.
- 2. Install Microsoft Hotfixes KB2494016, KB2520235, and KB2531907.
- Using the SnapDrive version 6.4 Installation and Administration Guide as a reference, install SnapDrive for Windows version 6.4. Note that the SnapDrive6.4 Installer program should be run as Administrator. Also, note during installation that https credentials need to be entered for Storage Systems and do not use Protection Manager Integration.
- 4. Download the Data ONTAP DSM 3.5 for Windows MPIO software under MultiPath I/O for Windows on the NOW website.
- 5. Using the Data ONTAP DSM 3.5 for Windows MPIO Installation and Administration Guide as a reference, install Data ONTAP DSM 3.5 for Windows MPIO. Choose Yes to install the Hyper-V Guest Utilities. At the end of the DSM Installation, click Yes to Reboot Now.

### Verify MultiPath I/O Connections (Both Hyper-V Hosts)

#### **Both Cisco UCS Hosts**

- 1. Using the UCS KVM Console, boot and log into the server.
- 2. In Windows Server Manager, under Storage, navigate to Data ONTAP® DSM Manager, Virtual Disks, Disk 1, and verify four available paths to the disk.

### Verify MultiPath I/O Connections

#### Cisco UCS Hosts VM-Host-Infra-01 and VM-Host-Infra-02

- 1. Using the Cisco UCS KVM Console, boot and log into the server. Note that a reboot will be required for the multipath software drivers to install.
- 2. In Windows Server Manager, under Storage, navigate to Data ONTAP® DSM Manager, Virtual Disks, Disk 1, and verify four available paths to the disk.





### **Creating Microsoft Hyper-V Virtual Network Switches**

Create the following Virtual Network Switches on both infrastructure hosts.

Virtual Network Name	Connection Type	Interface
VM-Data	External	Cisco VIC Interface
App-Cluster-Comm	External	Cisco VIC Interface #8
iSCSI-Fabric-A	External	Cisco VIC Interface #3
iSCSI-Fabric-B	External	Cisco VIC Interface #2

Note: Interface numbers may vary.

- 1. Open Hyper-V Manager.
- 2. Select the Hyper-V server and click Virtual Network Manager in the action pane on the right.
- 3. Select External and click Add.
- 4. Provide a name that matches the network name used in the Network Interface Configuration section.
- 5. Select External connection type and the matching interface for each network adapter.
- 6. Click Apply.
- 7. Click New Virtual Network.
- 8. Select External.
- 9. Click Add.
- 10. Repeat steps 4 through 9 for all Virtual Machine Networks.





\_ 🗆 🗙

#### **VM-Date Hyper-V Network Switch**

### 🖉 🖗 Virtual Network Manager

Virtual Networks	📩 Virtual Network Properties
New virtual network	Newsy VM Data - Virtual Natwork
Lisco VIC Ethernet Interface	
Global Network Settings	Microsoft Virtual Switch
Cisco VIC Ethernet Interface  Cisco VIC Ethernet Interface  MAC Address Range 00-15-5D-85-57-00 to 00-15-5D-8	Microsoft Virtual Switch         Notes:         Connection type         What do you want to connect this network to?         External:         Cisco VIC Ethernet Interface         Allow management operating system to share this network adapter         Internal only         Private virtual machine network         Kan ID         The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.         2
	Remove
	More about managing virtual networks
	<u>Q</u> K <u>C</u> ancel <u>Apply</u>





# App-Cluster-Comm

Virtual Network Manager	
* Virtual Networks	New Virtual Network
New virtual network	
VM-Data - Virtual Network	Name: App-Cluster-Comm
App-Cluster-Comm	A
Cisco VIC Ethernet Interface #8	No <u>t</u> es:
Global Network Settings	
00-15-5D-85-57-00 to 00-15-5D-8	Connection type
	Cisco VIC Ethernet Interface #8
	Allow management operating system to share this network adapter
	O Internal only
	Private virtual machine network
	Enable virtual LAN identification for management operating system
	system will use for all network communications through this network adapter. This
	setting does not affect virtual machine networking.
	2
	<u></u> emove
	More about managing virtual networks
	OK Cancel Apply





#### **iSCSI-Fabric-A**







#### iSCSI-Fabric-B



### **Domain Controller Virtual Machine (optional)**

Most environments will already have and active directory infrastructure and will not require additional domain controllers do be deployed for the Hyper-V FlexPod. The optional domain controllers can be omitted from the configuration in this case or used as a resource domain. The domain controller virtual machines will not be clustered because redundancy is provided by deploying multiple domain controllers running in virtual machines on different servers. Since these virtual machines reside on Hyper-V hosts that run Windows Failover cluster, but are not clustered themselves, Hyper-V Manager should be used to manage them instead of Virtual Machine Manager.



**Note:** The domain controller network interfaces must be accessible by the all virtual machines and the virtual machines hosts. For the configuration presented in this document, the IP subnet on VLAN VM-Mgmt must have a layer 3 route to the IP subnet on VLAN VM-Data.

#### **Create VHD for Domain Controller Virtual Machine (Optional)**

Create the following VHD storage resources that will be used by the virtual machines running system center roles:

#### Table 13 VHD Storage Resources

VM Host	VM Name	Name	Location	Size	Туре
Infra-VM-	Infra-DC-01	Infra-DC-01.vhd	C:\ClusterStorage\CSV-01	60 GB	Fixed
Host-01					
Infra-VM-	Infra-DC-02	Infra-DC-02.vhd	C:\ClusterStorage\CSV-02	60 GB	Fixed
Host-02					

- 1. Open the Hyper-V Manager and select the Hyper-V server in the left pane.
- 2. Click New in the right action pane and select Hard Disk.

늘 New Virtual Hard Disk Wiz	zard X
Choose Disk	Туре
Before You Begin Choose Disk Type Specify Name and Location Configure Disk Summary	What type of virtual hard disk do you want to create?                 Figed size                  This type of disk provides better performance and is recommended for servers running applications with high levels of disk activity. The .vhd file is created using the size of the fixed virtual hard disk. It does not change when data is added or deleted.                 Oppnanically expanding             This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The .vhd file is small when the disk is created and grows as data is written to it.                 Opfferencing             This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to the data or operating system without affecting the parent disk, so that you can revert the changes easily.                 More about virtual hard disks                 Qrevious             Next >             Einish             Cancel
	< <u>Previous</u> <u>Next</u> > <u>Finish</u> Cancel



늘 New Virtual Hard Disk Wiz	ard	×
Specify Name	e and Location	
Before You Begin	Specify the name and location of the virtual hard disk file.	
Choose Disk Type	Name: Infra-DC-01-boot.vhd	
Specify Name and Location Configure Disk	Location: C:\VHD\Infra-DC-01\ Browse	
Summary		
	< Previous Next > Finish Cancel	



늘 New Virtual Hard Disk Wiz	zard			×
Configure Di	isk			
Before You Begin Choose Disk Type Specify Name and Location Configure Disk Summary	You can create a blank virtual hard Create a new blank virtual hard Size: 60 GB (Maximum: 3 Copy the contents of the specific Physical Hard Disk \\. PHYSICALDRIVE0 \\. PHYSICALDRIVE1 \\. PHYSICALDRIVE2 \\. PHYSICALDRIVE3 \\. PHYSICALDRIVE4	I disk or copy the contents of an e I disk 2040 GB) fied physical disk: Size 130 GB 120 GB 500 GB 500 GB not set	existing physical dis	k.
	₿	< Previous Next >	Finish	Cancel



늘 New Virtual Hard Disk Wiz	ard
Completing t	the New Virtual Hard Disk Wizard
Before You Begin Choose Disk Type Specify Name and Location Configure Disk Summary	You have successfully completed the New Virtual Hard Disk Wizard. You are about to create the following virtual hard disk. Description: Type: fixed size Name: Infra-DC-01-boot.vhd Location: C:\VHD\Infra-DC-01 Size: 60 GB
	To create the virtual hard disk and close this wizard, click Finish.

### **Create Domain Controller Virtual Machine**

Create the following virtual machines that will be used by the domain controller roles.

Table	14	Virtual	Machine	Domains
Tuble		V II LUUI	macrimic	Domanis

VM Host	VM Name	Hard Disk	Network	Memory	VLAN ID
Infra-VM- Host-01	Infra-DC-01	C:\ClusterStorage\CSV- 01\Infra-DC-01.vhd	VM-Data – Virtual Network	8 GB	804
Infra-VM-	Infra-DC-02	C:\ClusterStorage\CSV-	VM-Data – Virtual	8 GB	804
Host-02		02\Infra-DC-02.vhd	Network		

- 1. Open Hyper-V Manager and select the Hyper-V server in the left pane.
- 2. Click New in the right action pane and select Virtual Machine.
- 3. Provide the name. Check the box for storing the virtual machine in a different location and provide the path. Click Next.
- 4. Enter the memory size and click Next.
- 5. Select the Network connection VM-Data-Virtual Network. Click Next.
- 6. Select the option to use an existing virtual hard disk and specify the path to the VHD created in the previous section. Click Next.





- 7. Select the option to install the operating system later and click Finish.
- 8. Repeat steps 1 through 7 for each virtual machine.

ኪ New Virtual Machine Wiza	nd X
Specify Nam	e and Location
Before You Begin Specify Name and Location Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	Choose a name and location for this virtual machine.         The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.         Name:       Infra-DC-01         You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.         ✓       Store the virtual machine in a different location         Location:       C:\VHD\Infra-DC-01\         Prowse       If you plan to take snapshots of this virtual machine, select a location that has enough free space. Snapshots include virtual machine data and may require a large amount of space.
	< Previous Next > Einish Cancel



ኪ New Virtual Machine Wiza	rd 🔀
Assign Memo	ory
Before You Begin Specify Name and Location Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	<ul> <li>Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 8 MB through 65536 MB. To improve performance, specify more than the minimum amount recommended for the operating system.</li> <li>Memory: 8192 MB</li> <li>When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.</li> <li>More about determining the memory to assign to a virtual machine</li> </ul>
	< Previous Next > Finish Cancel



🏚 New Virtual Machine Wiza	rd 🔀
Configure Ne	etworking
Before You Begin Specify Name and Location Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual network, or it can remain disconnected.   Cgnnection:   VM-Data - Virtual Network   More about configuring network adapters
	< Previous Next > Finish Cancel



ኪ New Virtual Machine Wiza	rd	X
Connect Virt	ual Hard Disk	
Before You Begin Specify Name and Location Assign Memory	A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.	
Configure Networking Connect Virtual Hard Disk Summary	Name:         Infra-DC-01.vhd           Location:         C:\VHD\Infra-DC-01\Infra-DC-01\           Size:         127         GB (Maximum: 2040 GB)	
	Use an existing virtual hard disk      Location: C:\VHD\Infra-DC-01\Infra-DC-01-boot.vhd Browse	
	C Attach a virtual hard disk later	
	< Previous Next > Finish Cancel	



🏚 New Virtual Machine Wiza	ard
Completing	the New Virtual Machine Wizard
Before You Begin Specify Name and Location Assign Memory Configure Networking Connect Virtual Hard Disk Summary	You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine. Description: Name: Infra-DC-01 Memory: 8192 MB Network: VM-Data - Virtual Network Hard Disk: C:\VHD\Infra-DC-01\Infra-DC-01-boot.vhd
	To create the virtual machine and close the wizard, click Finish.
	< <u>Previous</u> <u>Next</u> > <u>Finish</u> Cancel









### Install Windows in a Domain Controller Virtual Machine

Where do you want to install Win	dows?		
Name	Total Size	Free Space Type	
Disk 0 Unallocated Space	60.0 GB	60.0 GB	
Image: Refresh           Image: Load Driver		Drive options ( <u>a</u> dvanced)	
		Next	
		<u>N</u> ext	









### **Install Active Directory Services**

Add Roles Wizard		×
Select Server Ro	les	
Before You Begin Server Roles Active Directory Domain Services Confirmation Progress Results	Select one or more roles to install on this server.         Roles:         Active Directory Certificate Services         Active Directory Pederation Services         Active Directory Federation Services         Active Directory Rights Management Services         Active Directory Rights Management Services         Active Directory Rights Management Services         Application Server         DHCP Server         DNS Server         Fax Server         File Services         Print and Document Services         Remote Desktop Services         Windows Deployment Services         Windows Server Update Services         Windows Server roles	<ul> <li>Description:</li> <li>Active Directory Domain Services (AD)</li> <li>DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.</li> </ul>



## Add Roles Wizard Installation Progress Before You Begin The following roles, role services, or features are being installed: Server Roles Active Directory Domain Services Active Directory Domain Services .NET Framework 3.5.1 Features Confirmation Progress Results Installing... < Previous Next > Install Cancel $\searrow$

Run dcpromo to configure the Domain Controllers.

🖅 Run	×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	dcpromo
	This task will be created with administrative privileges.
	OK Cancel <u>B</u> rowse





Complete the domain controller installation and repeat the process on VM-Host-Infra-02 to install the redundant domain controller.

#### Join Virtual Machine Host VM-Host-Infra-01 to a Windows Domain

**Note:** The domain name service for each virtual machine host must be configured to use the domain name server that is running on a different physical server for the purpose of high availability.

Computer Name/Domain Changes	×
You can change the name and the membersh computer. Changes might affect access to net <u>More information</u>	ip of this work resources.
Computer name:	
VMHost-Infra-01	
Full computer name: VMHost-Infra-01	More
Member of	
O Workgroup:	
WORKGROUP	
ОК	Cancel





#### Note: Reboot

Join Virtual Machine Host VM-Host-Infra-02 to a Windows Domain

Computer Name/Domain Changes	×
You can change the name and the membership of this computer. Changes might affect access to network resources. <u>More information</u>	
Computer name:	
VMHost-Infra-02	
Full computer name: VMHost-Infra-02	
More	
Member of	1
Domain:	
flexpod.test	
C Workgroup:	
WORKGROUP	
OK Cancel	

Note: Reboot is required.

#### Set Firewall Exceptions (Both Hyper-V Hosts)

Open Windows Firewall with Advanced Security, by clicking Start > Administrative Tools > Windows Firewall with Advanced Security.

#### Add SnapDrive

- 1. Highlight Inbound Rules and click New Rule.
- 2. Select Program and click Next.
- 3. Enter the program path for the SnapDrive Service for example, %ProgramFiles%\NetApp\SnapDrive\SWSvc.exe.
- 4. Click Next, then select the "Allow the Connection" options and click Next, then Next again.
- 5. Enter the rule Name <SnapDrive> and Description, and click Finish.

#### **Configure Infrastructure Server Cluster**

- 1. Log in to VM-Host-Infra-01 using a domain administrative account with local privileges.
- 2. Open Server Manager and browse to Features > Failover Cluster Manager.
- 3. Validate cluster feasibility:
  - a. Select Validate a Configuration, then click Next.
  - b. Add both nodes one at a time into the Enter server name text field, and click Next.



- c. Select Run only tests I select and click Next.
- d. Scroll down to the storage section and clear all the storage related checkboxes.
- **Note:** These will run after you attach storage.
  - e. Click Next > Next.
  - f. Review the report and resolve any issues found by the validation wizard before continuing.
  - g. Click Finish.



- 4. Create majority node cluster:
  - h. In the Failover Cluster Manager, select Create a Cluster.
  - i. In the Welcome screen, click Next.





×

j. Add both nodes one at a time into the Enter server name text field, and click Next.

Select Servers				
Before You Begin Select Servers Access Point for Administering the Cluster Confirmation Creating New Cluster Summary	Add the names of all the s Enter server name: Selected servers:	servers that you want to have in the cluster. You must add at le whost-infra-01 flexpod.test whost-infra-02 flexpod.test	ast one server. Browse Add Remove	
		< Previous Next >	Cancel	

- k. Select Yes to run all validation tests, and click Next, then Next again.
- I. Select Run all test and click Next, then Next again.
- m. Click Finish. At this time you may safely ignore any warnings or errors related to clustered disks.





#### n. Enter the Cluster Name, Cluster IP, and click Next.

🚏 Create Cluster Wizard 🔀 🔀 💌					
Access P	pint for Administering t	he Cluster			
Before You Begin Select Servers Access Point for Administering the Cluster Confirmation	Type the name you want to use Cluster Name: Infra-Cl One or more IPv4 addresses cou sure the network is selected, and	when administering the cluster. lus-01 uld not be configured automatically. For e d then type an address.	ach network to be used, make		
Creating New Cluster Summary	Networks	Address ).0/24 10.10.0.4	1		
	More about the administrative.	Access Point for a cluster < Previous	Next > Cancel		





o. Review the configuration, click Next, then click Finish.

📲 Create Cluster Wi	zard		×
Summary	,		
Before You Begin Select Servers Access Point for	You have succe	essfully completed the Create Cluster Wizard.	
Administering the Cluster		Create Cluster	<b>_</b>
Confirmation			
Creating New Cluster	Cluster:	Infra-Clus-01	
Summary	Node:	vmhost-infra-01.flexpod.test	
	Node:	vmhost-infra-02.flexpod.test	
	IP Address:	Node and Disk Majority ( Cluster Disk 3 ) 10.10.0.41	•
	To view the report created by the wizard, click View Report. To close this wizard, click Finish.		View Report
		ß	
			Finish

- 5. Provision cluster storage:
  - a. Create a Quorum Disk:
    - i. Log in to the cluster host server and open SnapDrive.
    - ii. Select Disks and click Create Disk.
    - iii. In the Welcome screen, click Next.
    - iv. Enter the IP/FQDN for the Controller A and click Add.
    - v. When enumeration has completed, select the target volume where you intend to add the LUN.
    - vi. Add a LUN Name, LUN Description and click Next.
  - vii. Select Shared (Microsoft Cluster Services only) and click Next.
  - viii. Verify both nodes are shown for your cluster and click Next.
  - ix. Select Assign a Drive Letter and pick a drive letter.
  - x. Set the LUN Size to the size designated earlier, click Next, then Next again.
  - xi. Highlight each node in the Cluster and select All Fiber Channel Initiators to map the new LUN.
  - xii. Click Next, then Select Automatic and click Next.
  - xiii. Make sure that Select a cluster group by this node is selected.
  - xiv. Select the Cluster Group name Available Storage, click Next, then click Finish.





- xv. Repeat for CSV-01, and CSV-02 LUNs. Do not assign a Drive Letter or Volume Mount Point to these LUNs, and also place these LUNs in Available Storage.
- 6. Change cluster quorum settings:
  - a. From the node that currently owns the cluster open Failover Cluster Manager.
  - b. Right-click the virtual cluster name for the cluster you built earlier, and select More Actions > Configure Cluster Quorum Settings. Open the Configure Cluster Quorum Wizard.
  - c. In the Before You Begin screen, click  ${\tt Next.}$
  - d. Select Node and Disk Majority and click Next.
  - e. Select the Quorum disk with the mapped drive letter and click Next.
  - f. Review the confirmation for accuracy and click Next, then click Finish.
- 7. Enable Cluster Shared Volumes:
  - a. From the node that currently owns the cluster open Failover Cluster Manager.
  - b. In the Configure Section, select Enable Cluster Shared Volumes.



- c. Check I have read the above notice and click OK.
- d. Right-click Cluster Shared Volumes and select Add Storage.
- e. Select the volume corresponding to CSV-01 and click OK. You can look in SnapDrive to determine which volume is CSV-01.
- f. Right-click Cluster Shared Volumes and select Add Storage.





- g. Select the remaining volume corresponding to CSV-02 and click OK.
- h. Select Cluster Shared Volumes on the left.
- i. Right-click the CSV-01 volume in the center pane and select Properties. Rename the resource CSV-01.
- j. Repeat the resource rename for CSV-02.

Cluster Shared Volumes	Recent Cluster Events: 🔺 Error: 5, Warning: 2				
Summary of Cluster Shared Volumes					
<b>Storage:</b> 2 Total Disks - 2 online	Total Capacity: Total: 1,000.07 GB Free Space: 999.86 GB Percent Free: 100%				
Disk	Status	Current Owner			
🗆 🚍 CSV-01	Online	VMHost-Infra-01			
C:\ClusterStorage\Volume1	File System: NTFS	500 GB (100.0% free )			
🖃 🚍 CSV-02	🕥 Online	VMHost-Infra-02			
C:\ClusterStorage\Volume2	File System: NTFS	500.07 GB (100.0% free )			
	ß				

- 8. Rename Cluster Volume Mappings:
  - a. On Host 1, open Windows Explorer and browse to C:\ClusterStorage.
  - b. Right-click Volume1 and rename it CSV-01.
  - c. Right-click Volume2 and rename it CSV-02.
- 9. Validate cluster (from the node that currently owns the cluster):




- a. Open Failover Cluster Manager and right-click the virtual cluster name for the cluster you built earlier, and select Validate This Cluster.
- b. Click Next, then Select Run All Tests and click Next.
- c. Review the report and resolve any issues found by the validation wizard before continuing.
- d. Click Finish.
- 10. Rename Cluster Networks:
  - a. From the Failover cluster Manager, Under Networks, select Cluster Network 1.
  - b. Expand the Network Connections.
  - c. Right-click the Cluster Network 1.
  - d. Select Rename.
  - e. Rename the Network to the adapter name.
  - f. Repeat these steps for the remaining cluster networks. Rename each one to the adapter name for that Cluster Network.

Failover Cluster Manager	Services and applications Recent Cluster Events: None in the		Recent Cluster Events: None in the last 24 hours
Inita-Clus-01.ttexpod.test      Services and applications			
<ul> <li>Services and applications</li> <li>Infra-SCOM-01</li> <li>Infra-SCVMM-01</li> <li>Infra-Opalis-01</li> <li>WMHost-Infra-01</li> <li>WMHost-Infra-02</li> <li>Cluster Shared Volumes</li> <li>Storage</li> <li>Networks</li> <li>WM-Data</li> <li>Live Migration</li> <li>CSV</li> <li>WM-Mgmt</li> <li>Cluster Events</li> </ul>	Name Infra-SCOM-01 Infra-SCVMM-01 Infra-Opalis-01	Status  Colline  Coll	Ty     Current Owner     Auto       Virt     VMHost-Infra-02     Yes       Virt     VMHost-Infra-02     Yes       Virt     VMHost-Infra-01     Yes

#### Configure Cluster Network For CSV Network Traffic

- 1. Open a PowerShell command window.
- 2. Enter the PowerShell command Import-Module failoverclusters.
- 3. Enter the PowerShell command get-clusternetworkinterface | fl network, name. PS C:\Users\administrator.FLEXPOD> Import-Module failoverclusters

```
PS C:\Users\administrator.FLEXPOD> Get-ClusterNetworkInterface | fl
network, name
Network : Cluster Network 1
Name : VMHost-Infra-01 - VM-Date-Software Switch
```

```
Network : Cluster Network 1
Name : VMHost-Infra-02 - VM-Data Software
Network : Cluster Network 2
```



```
Name : VMHost-Infra-01 - LiveMigration
Network : Cluster Network 2
Name : VMHost-Infra-02 - LiveMigration
Network : Cluster Network 3
Name : VMHost-Infra-01 - CSV
Network : Cluster Network 3
Name : VMHost-Infra-02 - CSV
Network : Cluster Network 4
Name : VMHost-Infra-01 - VM-Mgmt
Network : Cluster Network 4
Name : VMHost-Infra-02 - VM-Mgmt
```

4. Enter the PowerShell command get-clusternetwork | fl name, metric.

```
PS C:\Users\administrator.FLEXPOD> Get-ClusterNetwork | fl name,
metric
```

```
Name : Cluster Network 1
Metric : 10100
Name : Cluster Network 2
Metric : 1100
Name : Cluster Network 3
Metric : 1200
Name : Cluster Network 4
Metric : 10000
```

5. Change the CSV network metric by entering the PowerShell command (get-clusternetwork "Cluster Network 3").Metric=900

PS C:\Users\administrator.FLEXPOD> ( Get-ClusterNetwork "Cluster Network 3").Metric = 900

6. Enter the PowerShell command get-clusternetwork | fl name, metric.

PS C:\Users\administrator.FLEXPOD> Get-ClusterNetwork | fl name, metric

Name : Cluster Network 1 Metric : 10100 Name : Cluster Network 2 Metric : 1100





```
Name : Cluster Network 3
Metric : 900
Name : Cluster Network 4
Metric : 10000
```

## **Create Virtual Machines and Resource for Deploying Infrastructure Roles**

### **Create VHD for Infrastructure Roles**

Create the following VHD storage resources that will be used by the virtual machines running system center roles:

#### Table 15 VHD Storage Resources

VM Host	VM Name	Name	Location	Size	Туре
Infra-VM-	Infra-SQL-01	Infra-SQL-01.vhd	C:\VHD\Infra-SQL-01	60 GB	Fixed
Host-01					
Infra-VM-	Infra-SQL-02	Infra-SQL-02.vhd	C:\VHD\Infra-SQL-01	60 GB	Fixed
Host-02					
Infra-VM-	Infra-SCOM-01	Infra-SCVMM-01.vhd	C:\ClusterStorage\CSV-01	60 GB	Fixed
Host-01					
Infra-VM-	Infra-SCVMM-01	Infra-SCVMM-01.vhd	C:\ClusterStorage\CSV-02	60 GB	Fixed
Host-02					
Infra-VM-	Infra-Opalis-01	Infra-Oplis-01.vhd	C:\ClusterStorage\CSV-01	60 GB	Fixed
Host-01					

1. Open the Hyper-V Manager and select the Hyper-V server in the left pane.

- 2. Click New and select Hard Disk.
- 3. Choose the Fixed size disk type and click Next.
- 4. Provide the VHD name and location, and click I Next.
- 5. Select Create a new blank virtual hard disk and provide the disk size. Click Next.
- 6. Click Finish.
- 7. Repeat steps 1 through 6 for each VHD.



X

#### hew Virtual Hard Disk Wizard





## 늘 New Virtual Hard Disk Wizard x Completing the New Virtual Hard Disk Wizard You have successfully completed the New Virtual Hard Disk Wizard. You are about to create the following virtual hard disk. Before You Begin Choose Disk Type Description: Specify Name and Location Type: fixed size Configure Disk Name: Infra-SCVMM-01.vhd Summary Location: C:\ClusterStorage\CSV-02 Size: 60 GB To create the virtual hard disk and close this wizard, click Finish. < Previous <u>Finish</u> Cancel



### x 늘 New Virtual Hard Disk Wizard Completing the New Virtual Hard Disk Wizard You have successfully completed the New Virtual Hard Disk Wizard. You are about to create the following virtual hard disk. Before You Begin Choose Disk Type Description: Specify Name and Location Type: fixed size Configure Disk Name: Infra-SCOM-01.vhd Summary Location: C:\ClusterStorage\CSV-02 Size: 60 GB To create the virtual hard disk and close this wizard, click Finish. < Previous <u>N</u>ext > Einish Cancel





hew Virtual Hard Disk Wiz	ard X
Completing t	the New Virtual Hard Disk Wizard
Before You Begin Choose Disk Type Specify Name and Location	You have successfully completed the New Virtual Hard Disk Wizard. You are about to create the following virtual hard disk. Description: Type: fixed size
Configure Disk Summary	Name: Infra-SCOM-01.vhd Location: C:\ClusterStorage\CSV-02 Size: 60 GB
	To create the virtual hard disk and close this wizard, click Finish.          < Previous

## **Create Infrastructure Virtual Machines**

### **Domain Controller Virtual Machine (optional)**

Most environments will already have and active directory infrastructure and will not require additional domain controllers do be deployed for the Hyper-V FlexPod. The optional domain controllers can be omitted from the configuration in this case or used as a resource domain. The domain controller virtual machines will not be clustered because redundancy is provided by deploying multiple domain controllers running in virtual machines on different servers. Since these virtual machines reside on Hyper-V hosts that run Windows Failover cluster, but are not clustered themselves, Hyper-V Manager should be used to manage them instead of Virtual Machine Manager.

Create the following virtual machines that will be used by the virtual machines running system center roles.

VM Host	VM Name	Hard Disk	Network	Memory
Infra-VM-	Infra-SQL-01	C:\VHD\Infra-SQL-	VM-Data – Virtual Network	8 GB
Host-01		01Infra-SQL-01.vhd		
Infra-VM-	Infra-SQL-02	C:\VHD\Infra-SQL-	VM-Data – Virtual Network	8 GB
Host-02		01\Infra-SQL-02.vhd		

#### Table 16 Infrastructure Virtual Machines





X

Infra-VM- Host-01	Infra-SCOM-01	C:\ClusterStorage\CSV- 01\Infra-SCVMM- 01.vhd	VM-Data – Virtual Network	8 GB
Infra-VM- Host-02	Infra-SCVMM-01	C:\ClusterStorage\CSV- 02\Infra-SCVMM- 01.vhd	VM-Data – Virtual Network	8 GB
Infra-VM- Host-01	Infra-Opalis-01	C:\ClusterStorage\CSV- 01\Infra-Oplis-01.vhd	VM-Data – Virtual Network	8 GB

- 1. Open the Hyper-V Manager and select the Hyper-V server in the left pane.
- 2. Click New in the right action pane and select Virtual Machine.
- 3. Provide the name. Check the box for storing the virtual machine in a different location and provide the path. Click Next.
- 4. Enter the memory size and Click Next.
- 5. Select the Network connection VM-Data-Virtual Network. Click Next.
- 6. Select the option to use an existing virtual hard disk and specify the path to the VHD created in the previous section. Click Next.
- 7. Select the option to install the operating system later and click Finish.
- 8. Repeat steps 1 through 7 for each virtual machine.

#### 捷 New Virtual Machine Wizard

Completing	the New Virtual Machine Wizard
Before You Begin Specify Name and Location Assign Memory	You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine. Description:
Configure Networking Connect Virtual Hard Disk Summary	Memory: 8192 MB Network: VM-Data - Virtual Network Hard Disk: C:\ClusterStorage\CSV-02\Infra-SCVMM-01.vhd
	To create the virtual machine and dose the wizard, dick Finish. $$\begin{aligned} \hline \begin{aligned} \hline$
	< Previous Next > Finish Cancel



### × ኪ New Virtual Machine Wizard **Completing the New Virtual Machine Wizard** Before You Begin You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine. Specify Name and Location Description: Assign Memory Name: Infra-SCOM-01 Configure Networking Memory: 8192 MB Connect Virtual Hard Disk Network: VM-Data - Virtual Network Summary Hard Disk: C:\ClusterStorage\CSV-02\Infra-SCOM-01.vhd To create the virtual machine and close the wizard, click Finish. $\mathbb{R}$ Next > < Previous Finish Cancel



🎦 New Virtual Machine Wiza	rd	[
Completing	the New Virtual Machine Wizard	
Before You Begin Specify Name and Location Assign Memory Configure Networking Connect Virtual Hard Disk Summary	You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine. Description: Name: Infra-SQL-01 Memory: 8192 MB Network: VM-Data - Virtual Network Hard Disk: C:\VHD\Infra-SQL-01\Infra-SQL-01.vhd	
	To create the virtual machine and close the wizard, click Finish.	
	< Previous Next > Finish Cancel	



🎦 New Virtual Machine Wiza	ırd
Completing	the New Virtual Machine Wizard
Before You Begin Specify Name and Location Assign Memory Configure Networking Connect Virtual Hard Disk Summary	You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine. Description: Name: Infra-SQL-01 Memory: 8192 MB Network: VM-Data - Virtual Network Hard Disk: C:\VHD\Infra-SQL-01\Infra-SQL-01.vhd
	To create the virtual machine and close the wizard, click Finish.
	< Previous Next > Finish Cancel



🄁 New Virtual Machine Wiza	rd	<u>&lt;</u>
Completing t	the New Virtual Machine Wizard	
Before You Begin Specify Name and Location Assign Memory Configure Networking Connect Virtual Hard Disk Summary	You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine. Description: Name: Infra-SQL-02 Memory: 8192 MB Network: VM-Data - Virtual Network Hard Disk: C: \VHD\Infra-SQL-02\Infra-SQL-02.vhd	
	To create the virtual machine and close the wizard, click Finish.	
	<pre></pre>	

## **Modify the Virtual Machine Settings**

Update the logical processor setting and virtual network adapters with the following information.

### **Table 17 Virtual Machine Settings**

VM Name	Logical Processors	Network	VLAN ID
		VM-Data	804
Infra SOL 01	1	iSCSI Fabric-A	802
	4	iSCSI Fabric-B	802
		App-Cluster-Comm	806
	4	VM-Data	804
Infra SOL 02		iSCSI Fabric-A	802
IIIIIa-SQL-02		iSCSI Fabric-B	802
		App-Cluster-Comm	806
Infra-SCOM-01	2	VM-Data	804
	2	VM-Data	804
Infra-SCVMM-01		iSCSI Fabric-A	802
		iSCSI Fabric-B	802
Infra-Opalis-01	2	VM-Data	804



Update the virtual machine setting using the following procedure.

- 1. Using the Hyper-V Manager select the virtual machine in the center pane.
- 2. Click Settings in the lower right pane.
- 3. Click Processor in the left Hardware pane.
- 4. Configure the correct number of logical processors using the drop down box and the information in the table above.
- 5. Select the VM-Data network adapter in the right pane.
- 6. Check the box that enables virtual LAN identification.
- 7. Enter the VLAN ID in the text box from the table above.
- 8. Click Apply.
- 9. Select Add Hardware in the right pane to add additional network adapters.
- 10. Select Network Adapter and click the Add button.
- 11. Select the appropriate network in the Network dropdown box.
- 12. Check the box that enables virtual LAN identification.
- 13. Enter the VLAN ID in the text box from the table above.

14. Click Apply.

- 15. Repeat steps 9 through 14 to add additional network adapters.
- 16. Click OK to close the settings window.
- 17. Repeat steps 1 through 16 for all virtual machines.





### **Configure Virtual Processor Count**







## **Configure Virtual LAN Identification**

Settings for Infra-SQL-01	
Infra-SQL-01	
<ul> <li>Hardware</li> <li>Add Hardware</li> <li>BIOS Boot from CD</li> <li>Memory 8192 MB</li> <li>Processor 4 Virtual processors</li> <li>IDE Controller 0</li> <li>Hard Drive</li> </ul>	Image: Provide the set work adapter         Specify the configuration of the network adapter or remove the network adapter.         Network:         VM-Data - Virtual Network         Image: MAC Address         Image: Open constraints
INTRA-SQL-01.VNd IDE Controller 1  DVD Drive None SSCSI Controller  Network Adapter VM-Data - Virtual Network COM 1 None COM 2	<ul> <li>Enable spoofing of MAC addresses</li> <li>✓ Enable virtual LAN identification</li> <li>VLAN ID</li> <li>The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.</li> <li>804</li> </ul>
<ul> <li>None</li> <li>Diskette Drive None</li> <li>Management</li> <li>Name Infra-SQL-01</li> <li>Integration Services All services offered</li> <li>Snapshot File Location C:\ClusterStorage\CSV-01\Infra-S</li> <li>Automatic Start Action</li> <li>Destart if proving up up upping</li> </ul>	To remove the network adapter from this virtual machine, dick Remove. <u>Remove</u> Image: the second
Restart if previously running Automatic Stop Action Save	QK <u>C</u> ancel <u>Apply</u>





### Add iSCSI Fabric A Interface

Infra-SQL-01       Image: Control of the network adapter or remove the network adapter.         Memory       BiDS         BiDS Boot from CD       Image: Control of the network adapter or remove the network adapter.         Memory       BiDS Control of the network adapter or remove the network adapter.         Image: Discourse of the network adapter or remove the network adapter.       Image: Control of the network adapter or remove the network adapter.         Image: Control of the network adapter of the network adapter.       Image: Control of the network adapter or remove the network adapter.         Image: Control of the network adapter of the network adapter.       Image: Control of the network adapter or remove the network adapter.         Image: Control of the network adapter of the network adapter or remove the network adapter or remove the network adapter.       Image: Control of the network adapter or remove the network adapter.         Image: Control of the network adapter instead of this network adapter or when integration services are not installed in the guest operating system.       Image: Control of the network adapter install of the network adapter or when integration services are not installed in the guest operating system.         Image: Start Action Restart if previously running       Image: Cont of the network adapter install of the network adapter installed in the guest operating system.         Image: Start Action Restart if previously running       Image: Cont of the network adapter installed in the guest operating system.	Settings for Infra-SQL-01	
A Hardware         Add Hardware         BIOS         Boot from CD         Memory         Bits         Bits         Processor         4 Virtual processors         Bits         IDE Controller 0         Hard Drive         Infra-SQL-01.vhd         Bits         SCSI Controller         Wetwork Adapter         VM-Data - Virtual Network         None         COM 1         None         COM 2         None         COM 2         None         Diskette Drive         None         Diskette Drive         None         Diskette Drive         None         Station of the guest operating system or when integration services are not installed in the guest operating system.         Infra-SQL-01         Matematic Start Action         CK       Cancel         Automatic Start Action         Restart if previously running </th <th>Infra-SQL-01</th> <th>▲ ▶ Q.</th>	Infra-SQL-01	▲ ▶ Q.
Add Hardware BIOS Boot from CD Boot from CD Memory BI92 MB Processor 4 Virtual processors Uirtual processors Uirtual processors Uirtual processors Uirtual processors Uirtual processors Uirtual Address Uirtu	* Hardware	🔋 Network Adapter
BIOS         Boot from CD         Boot from CD         Memory         B122.MB         Processor         4 Virtual processors         IDE Controller 0         Infra-SQL-01.vhd         DVD Drive         None         SCSI Controller         None         SCSI Controller         None         COM 1         None         COM 2         None         COM 2         None         COM 2         None         ScSI-Fabric-A         COM 1         None         Soldette Drive         None         Secsion freed	Might Add Hardware	
Boot mon CD Wetwork: SISE Fabric-A SISE Controller 0 Hard Drive Infra-SQL-01.vhd DVD Drive None SISE Controller DVD Drive None SISE Controller Metwork Adapter VH-Data - Virtual Network None SISE Controller Metwork Adapter SISE - Fabric-A COM 1 None A Hanagement None A Hanagement Max Addresse Metwork adapter instead of this network adapter to perform a network based installation of the guest operating system. Metwork adapter to perform a network based installation of the guest operating system. Metwork adapter to perform a network based installation of the guest operating system. Metwork adapter to perform a network based installation of the guest operating system. Metwork adapter to perform a network based installation of the guest operating system. Metwork adapter to perform a network based installation of the guest operating system. Metwork adapter to perform a network based installation of the guest operating system. Metwork adapter to perform a None A Hanagement Metwork Start Action Restart if previously running	EIOS	Specify the configuration of the network adapter of remove the network adapter.
Memory         BY Memory         Processor         4 Virtual processors         B DE Controller 0         Hard Drive         Infra-SQL-01.vhd         D DD Drive         None         SSSI Controller         None         SSSI Controller         None         SSSI Controller         None         COM 1         None         COM 1         None         COM 1         None         COM 2         None         Thra-SQL-01         Diskette Drive         None         Thra-SQL-01         Static Adapter         Static Static Controller         Name         Thra-SQL-01         Thra-SQL-01         Static Static Static Controller         Name         Thra-SQL-01         Static Controller         Name         Thra-SQL-01         Static Controller         Name         Thra-SQL-01         Name         Thra-SQL-01         Name         Thra-SQL-01         Na	Boot from CD	Network:
Processor       4 Virtual processors         ■ IDE Controller 0       ● Dynamic         ● Hard Drive       Infra-SQL-01.vhd         ■ IDE Controller 1       ● DVD Drive         None       ● Enable spoofing of MAC addresses         ▼ None       ● Enable virtual LAN identification         VLAN Identifier specifies the virtual LAN that this virtual machine will use for all network Adapter         SCSI-Fabric-A         ● Diskette Drive None         ● Automatic Start Action Restrices All services offered         ● Sinaphot File Location C:\Cluster-Storage\CSV-01[Infr         ● Automatic Start Action Restart if previously running         ● Automatic Start Action         ● Cotter Disketter Drive None	8192 MB	ISCSI-Fabric-A
4 Virtual processors         IDE Controller 0         Hard Drive         Infra-SQL-01.vhd         VLAN ID         None         SCSI Controller         VLAN ID         None         COM 1         None         Diskette Drive         None         COM 1         None         Diskette Drive         None         Infra-SQL-01         Infra-SQL-01         Infra-SQL-01         Infra-SQL-01         Infra-SQL-01         Infra-SQL-01         Intervices offered         Sapaphot File Location         C:/ClusterStorage/CSV-01[Infr         Automatic Start Action         Restart if previously running         OK       Cancel       Apply	Processor	MAC Address
<ul> <li>IDE Controller 0</li> <li>Hard Drive Infra-SQL-01.vhd</li> <li>IDE Controller 1</li> <li>DVD Drive None</li> <li>SCSI Controller</li> <li>Hetwork Adapter VH-Data - Virtual Network</li> <li>Network Adapter ISCSI-Fabric-A</li> <li>COM 1 None</li> <li>Diskette Drive None</li> <li>Management</li> <li>Integration Services Al services offered Sapshot File Location C:{Uster Storage}(SSV-01{Infr})</li> <li>Automatic Start Action Restart if previously running</li> <li>OK Cancel Apply</li> </ul>	4 Virtual processors	C Dynamic
<ul> <li>Hard Drive Infra-SQL-01.vhd</li> <li>DVD Drive None</li> <li>SCSI Controller</li> <li>Intervork Adapter iSCSI-Fabric-A</li> <li>None</li> <li>CCM 1 None</li> <li>Diskette Drive None</li> <li>Diskette Drive None</li> <li>State Drive None</li> <li>Diskette Drive None</li> <li>State Drive None</li> <li>Integration Services Al services offered</li> <li>Snapshot File Location C:\ClusterStorage\CSV-01\unfr Automatic Start Action Restart if previously running</li> <li>Mane Management</li> <li>Name Marking CSV-01\unfr None</li> <li>Mane Management</li> <li>Name Marking Start Action Restart if previously running</li> <li>Management</li> <li></li></ul>	🖃 🔝 IDE Controller 0	O Static
<ul> <li>DE Controller 1</li> <li>DVD Drive None</li> <li>SCSI Controller</li> <li>Network Adapter VM-Data - Virtual Network</li> <li>Network Adapter iSCSI-Fabric-A</li> <li>COM 1 None</li> <li>COM 1 None</li> <li>COM 2 None</li> <li>Diskette Drive None</li> <li>Diskette Drive None</li> <li>Mangement</li> <li>Infa-SQL-01</li> <li>Integration Services Al services offered</li> <li>Snapshot File Location C: (ClusterStorage\CSV-01\Infr Automatic Start Action Restart if previously running</li> <li>M</li> <li>Cancel</li> <li>Apply</li> </ul>	Hard Drive Infra-SQL-01.vhd	
PVD Drive None SCSI Controller Wetwork Adapter Whota-ta-Virtual Network Network Adapter SCSI-Fabric-A COM 1 None COM 2 None COM 2 None Diskette Drive None Management Infra-SQL-01 Integration Services Al services offered Snapshot File Location C: (ClusterStorage (CSV-01)Infr Mutomatic Start Action Restart if previously running OK Cancel Apply	IDE Controller 1	
None   SCSI Controller   Network Adapter   VH-Data - Virtual Network   Network Adapter   VH-Data - Virtual Network   Network Adapter   SCSI-Fabric-A   COM 1   None   COM 2   None   Diskette Drive   None   Amagement   Infra-SQL-01   Integration Services   All services offered   Snapshot File Location   C: ClusterStorage/CSV-01Unfr   Automatic Start Action   Restart if previously running     OK   Cance	DVD Drive	Enable spoofing of MAC addresses
<ul> <li>SCSI Controller</li> <li>Network Adapter VM-Data - Virtual Network</li> <li>Network Adapter VSCSI-Fabric-A</li> <li>COM 1 None</li> <li>COM 2 None</li> <li>Diskette Drive None</li> <li>Management</li> <li>Infra-SQL-01</li> <li>Integration Services All services offered</li> <li>Snapshot File Location C: (-ClusterStorage\CSV-01\infr Automatic Start Action Restart if previously running</li> <li>Management</li> <li>OK</li> <li>Cancel</li> <li>Apply</li> </ul>	None	
Image: Network Adapter VH-Data - Virtual Network         Image: Network Adapter isCSI-Fabric-A         Image: SCSI-Fabric-A         Image: COM 1         None         Image: COM 2         Name         Image: Comparison Services         All services offered         Image: Commont         Image:	SCSI Controller	Enable virtual LAN identification
WH-Data - Virtual Network         Network Adapter         iSCSI-Fabric-A         COM 1         None         COM 2         None         Diskette Drive         None         K Management         Image: Integration Services         All services offered         Snapshot File Location         C:(JusterStorage\CSV-01\Infr         Automatic Start Action         Restart if previously running             OK       Cancel       Apply	Network Adapter	VLAN ID
<ul> <li>Retwork Adapter</li> <li>Interview Communications and ogn and network adapter.</li> <li>Interview Communications and ogn and network adapter from this virtual machine, click Remove.</li> <li>Interview Communications and ogn and network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.</li> <li>Integration Services         <ul> <li>Automatic Start Action</li></ul></li></ul>	VM-Data - Virtual Network	The VLAN identifier specifies the virtual LAN that this virtual machine will use for all
B02         Image: COM 1         None         COM 2         None         Diskette Drive         None         Image: Com 2         Name         Infra-SQL-01         Image: Com 2         Image: Com 2         Name         Infra-SQL-01         Image: Com 2	iSCST-Fabric-A	
None   Image: COM 2   None   Image: Diskette Drive   None   Image: None   <	COM 1	802
<ul> <li>COM 2 None</li> <li>Diskette Drive None</li> <li>Management</li> <li>Name Infra-SQL-01</li> <li>Integration Services All services offered</li> <li>Snapshot File Location C: \ClusterStorage \CSV-01\Infr</li> <li>Automatic Start Action Restart if previously running</li> </ul>	None	To some up the network adaptes from this with all marking, click Demous
None       Remove         Diskette Drive       None         None       Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.         Image: Integration Services       All services offered         Snapshot File Location       C:\ClusterStorage\CSV-01\Infr         Automatic Start Action       The reviously running         Restart if previously running       OK	T COM 2	To remove the network adapter from this virtual machine, click Remove.
<ul> <li>Diskette Drive None</li> <li>Management</li> <li>Name Infra-SQL-01</li> <li>Integration Services All services offered</li> <li>Snapshot File Location C:\ClusterStorage\CSV-01\Infr</li> <li>Automatic Start Action Restart if previously running</li> </ul>	None	Remove
None <ul> <li>Management</li> <li>Infra-SQL-01</li> <li>Integration Services</li> <li>All services offered</li> <li>Snapshot File Location</li> <li>C:\ClusterStorage\CSV-01\Infr</li> <li>Automatic Start Action</li> <li>Restart if previously running</li> </ul> <li>OK</li> <li>Cancel</li> <li>Apply</li>	Diskette Drive	Use a legacy network adapter instead of this network adapter to perform a
Imagement       Services are not installed in the guest operating system.         Imagement       Infra-SQL-01         Imagement       Infra-SQL-01         Imagement       Infra-SQL-01         Imagement       Imagement         Imagement       I	None	network-based installation of the guest operating system or when integration
Integration Services         All services offered         Sapshot File Location         C:\ClusterStorage\CSV-01\Infr         Automatic Start Action         Restart if previously running         OK       Cancel	× Management	services are not installed in the guest operating system.
Integration Services         All services offered         Sapshot File Location         C:\ClusterStorage\CSV-01\Infr         Automatic Start Action         Restart if previously running         OK       Cancel	Infra-SOL-01	
All services offered Snapshot File Location C:\ClusterStorage\CSV-01\Infr Automatic Start Action Restart if previously running	Integration Services	
Snapshot File Location         C:\ClusterStorage\CSV-01\Infr         Automatic Start Action         Restart if previously running         OK       Cancel	All services offered	
Automatic Start Action         Restart if previously running         OK       Cancel	Snapshot File Location C:\ClusterStorage\CSV-01\Infr	
Restart if previously running       OK     Cancel     Apply	Automatic Start Action	
OK Cancel Apply	Restart if previously running	
		OK Cancel Apply





### Add iSCSI Fabric B Interface

5	ettings for Infra-SQL-01		
In	fra-SQL-01	•	
*	Hardware	•	Network Adapter
	BIOS Boot from CD		Specify the configuration of the network adapter or remove the network adapter. Network:
	Memory 8192 MB		iSCSI-Fabric-B
	Processor     4 Virtual processors		MAC Address     Dynamic
=	IDE Controller 0		O <u>S</u> tatic
	Hard Drive Infra-SQL-01.vhd		
	IDE Controller 1		Enable spoofing of MAC addresses
	None SCSI Controller		Enable virtual LAN identification
	Network Adapter VM-Data - Virtual Network		VLAN ID The VLAN identifier specifies the virtual LAN that this virtual machine will use for all
	Network Adapter iSCSI-Fabric-A		network communications through the network adapter.
	Network Adapter iSCSI-Fabric-B		
	COM 1 None		Remove
	COM 2		Use a legacy network adapter instead of this network adapter to perform a
	Diskette Drive		network-based installation of the guest operating system or when integration services are not installed in the guest operating system.
\$	Management		
	Name		
	Integration Services		
	Snapshot File Location C:\ClusterStorage\CSV-01\Infr	<b>•</b>	
	-		
			<u>O</u> K <u>C</u> ancel <u>A</u> pply









捷 New Virtual Machine Wiza	rd	×			
Completing t	the New Virtual Machine Wizard				
Before You Begin Specify Name and Location Assign Memory	You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine. Description:				
Configure Networking Connect Virtual Hard Disk Summary	Name: Infra-SQL-02 Memory: 8192 MB Network: VM-Data - Virtual Network Hard Disk: C:\VHD\Infra-SQL-02\Infra-SQL-02.vhd				
	, To create the virtual machine and close the wizard, click Finish.				
	<previous next=""> Finish Cancel</previous>				



nfra-SQL-02	▲ ▶ Q.
t Hardware	Processor
Md Hardware BIOS Boot from CD	You can modify the number of virtual processors based on the number of processors on the physical machine. You can also modify other resource control settings.
Memory 8192 MB	Number of logical processors: 4
Processor     4 Virtual processors	More about virtual processors  Resource control
DE Controller 0	You can use resource controls to balance resources among virtual machines.
Hard Drive Infra-SOL-02.vhd	Virtual machine reserve (percentage):
IDE Controller 1	Percent of total system resources: 0
None	Virtual machine limit (percentage): 100
SCSI Controller	Percent of total system resources: 16
VM-Data - Virtual Network	Relative weight: 100
None	More about resource control
None	Processor compatibility
Diskette Drive	You can limit the processor features that a virtual machine can use. This improves the virtual machine's compatibility with different processor versions and older quest
Management	operating systems. Select the scenarios you want to enable:
I Name Infra-SQL-02	Migrate to a physical computer with a different processor version
Integration Services	Run an older operating system, such as Windows NT
Snapshot File Location C: \ClusterStorage \CSV-02\Infra-S	
Automatic Start Action Restart if previously running	
Automatic Stop Action Save	



infra-SQL-02	▲ ▶   Q.
<ul> <li>Hardware</li> <li>Add Hardware</li> <li>BIOS Boot from CD</li> <li>Memory 8192 MB</li> <li>Processor 4 Virtual processors</li> <li>IDE Controller 0</li> <li>Hard Drive Infra-SQL-02.vhd</li> </ul>	Network Adapter Specify the configuration of the network adapter or remove the network adapter. Network: VM-Data - Virtual Network MAC Address © Dynamic © Static 00 - 00 - 00 - 00 - 00
<ul> <li>IDE Controller 1</li> <li>DVD Drive None</li> <li>SCSI Controller</li> <li>Network Adapter VM-Data - Virtual Network</li> <li>COM 1 None</li> <li>COM 2 None</li> <li>Diskette Drive Diskette Drive</li> </ul>	<ul> <li>Enable spoofing of MAC addresses</li> <li>Enable virtual LAN identification</li> <li>VLAN ID</li> <li>The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.</li> <li>804</li> <li>To remove the network adapter from this virtual machine, dick Remove.</li> </ul>
<ul> <li>Management         <ul> <li>Name                 Infra-SQL-02</li> <li>Integration Services                 All services offered</li> <li>Snapshot File Location                 C:\ClusterStorage\CSV-02\Infra-S</li> <li>Automatic Start Action                 Restart if previously running</li> <li>Automatic Stop Action                 Save</li> </ul> </li> </ul>	Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.



nfra-SQL-02	
<ul> <li>Hardware</li> <li>Add Hardware</li> <li>BIOS Boot from CD</li> <li>Memory 8192 MB</li> </ul>	Network Adapter     Specify the configuration of the network adapter or remove the network adapter.     Network:     ISCSI-Fabric-A     MAC Address
4 Virtual processor IDE Controller 0 Hard Drive Infra-SQL-02.vhd	Dynamic     Static
<ul> <li>IDE Controller 1</li> <li>DVD Drive None</li> <li>SCSI Controller</li> <li>Network Adapter VM-Data - Virtual Network</li> <li>Network Adapter iSCSI-Fabric-A</li> <li>COM 1 None</li> </ul>	<ul> <li>Enable spoofing of MAC addresses</li> <li>Enable virtual LAN identification</li> <li>VLAN ID</li> <li>The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.</li> <li>802</li> </ul>
COM 2 None Diskette Drive None Management Management Name Infra-SQL-02 Integration Services All services offered Spanshot File Location	To remove the network adapter from this virtual machine, dick Remove.
C:\ClusterStorage\CSV-02\Infr Automatic Start Action Restart if previously running	



nfra-SQL-02	
<ul> <li>Hardware</li> <li>Add Hardware</li> <li>BIOS Boot from CD</li> <li>Memory 8192 MB</li> <li>Processor 4 Virtual processors</li> <li>IDE Controller 0</li> <li>Hard Drive Infra-SQL-02.vhd</li> <li>IDE Controller 1</li> <li>DVD Drive None</li> <li>SCSI Controller</li> <li>Network Adapter iSCSI-Fabric-A</li> <li>Network Adapter iSCSI-Fabric-B</li> </ul>	Network Adapter Specify the configuration of the network adapter or remove the network adapter. Network: ISCSI-Fabric-B MAC Adoress O Dynamic Static I
COM 1 None COM 2 None Diskette Drive None Management Name Infra-SQL-02 Integration Services All services offered Snapshot File Location C:\ClusterStorage\CSV-02\Infr	Remove  Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.



infra-SQL-02	•	▲ ▶ Q.
A Hardware		🔋 Network Adapter
┪ Add Hardware		
Nos BIOS		Specify the configuration of the network adapter or remove the network adapter.
Boot from CD		Network:
Memory		App-Cluster-Comm
8192 MB		MAC Address
Processor		Dynamic
4 Virtual processors		
i i i De Controller 0		○ Static
Infra-SOL-02 vbd		
		Enable spoofing of MAC addresses
None		
SCSI Controller		Enable virtual LAN identification
VM-Data - Virtual Network		The VLAN identifier specifies the virtual LAN that this virtual machine will use for all
Network Adapter		network communications through this network adapter.
iSCSI-Fabric-A		806
Network Adapter		
iSCSI-Fabric-B		To remove the network adapter from this virtual machine, click Remove
📮 Network Adapter		
App-Cluster-Comm	- 11	Remove
🐺 COM 1		I Lies a legacy network adapter instead of this network adapter to perform a
None		network-based installation of the guest operating system or when integration
COM 2		services are not installed in the guest operating system.
None		
None		
Management		
	-	
Infra-SOL-02		
Integration Services		
All services offered	<b>T</b>	
—	-	



늘 New Virtual Hard Disk Wiz	ard
Completing t	the New Virtual Hard Disk Wizard
Before You Begin Choose Disk Type Specify Name and Location Configure Disk Summary	You have successfully completed the New Virtual Hard Disk Wizard. You are about to create the following virtual hard disk. Description:           Type:         fixed size           Name:         Infra-Opalis-01.vhd           Location:         C:\clusterStorage\CSV-01           Size:         60 GB
	To create the virtual hard disk and dose this wizard, dick Finish.





### **Create Clustered Application or Service**

- 1. Navigate to Failover Cluster Manager and select the cluster name in the left pane.
- 2. Click Configure a Service or Application in the right pane.
- 3. Scroll down to select Virtual Machine and click Next.
- 4. Select the Virtual Machines to cluster and click Next.
- Infra-SCOM-01
- Infra-SCVMM-01
- Infra-OPALIS-01



**Note:** Do not select the SQL Server or Domain Controller virtual machines. These virtual machines are not clustered.

🤯 High Availability W	/izard	×
Select Se	ervice or Application	
Before You Begin Select Service or Application Select Virtual Machine Configure High Availability Summary	Select the service or application that you want to configure for high availability:         Generic Application         Generic Script         Generic Service         Internet Storage Name Service (ISNS) Server         Message Queuing         Other Server         Print Server         Virtual Machine         Virtual Machine         Virtual Machine         More about services and applications you can configure for high availability	
	< <u>P</u> revious <u>N</u> ext > Cancel	]



🧑 High Availability W	izard		×
to Summary			
Before You Begin Select Service or Application	High availability was successfully configu	ared for the service or application.	
Select Virtual Machine			
Confirmation	Name	Result	Description
Configure High Availability	Infra-SCOM-01		Success
Summary	Infra-SCVMM-01		Success
			<b>•</b>
	To view the report created by the wizard, click Vie To close this wizard, click Finish.	ew Report.	View Report
			<u> </u>



🧑 High Availability W	fizard		×
Summary			
Before You Begin	High availability was successfully configured for the s	service or application.	
Select Service or Application			
Select Virtual Machine	Vintual Mashing		<b></b>
Confirmation	Virtual Machine		
Configure High Availability	Name	Result	Description
Summary	Infra-SQL-01		Success
			<b>•</b>
	To view the report created by the wizard, click View Report. To close this wizard, click Finish.		View Report
		Ŀ}	
			Finish





### **Configure Live Migration Network for the Virtual Machines**

- 1. Navigate to any clustered virtual machine under Services and applications object in the left pane.
- 2. Right-click on the virtual machine in the center pane and select Properties.
- 3. Clear the checkbox for all networks except the Live Migration network.
- 4. Click OK to accept the settings.



Hailover Cluster Manager □ 申 Infra-Clus-01.flexpod.test	Infra-Opalis-01			
Services and applications     Infra-Opalis-01     Infra-SCOM-01     Infra-SCVMM-01	Summary of	Infra-Opalis-01		
🕂 🖼 Nodes	Status: Online		Auto Start: Yes	
Cluster Shared Volumes	Alerts: <none></none>			
Ӓ Storage	Preferred Owners: <n< th=""><th>one&gt;</th><th></th><th></th></n<>	one>		
Retworks     Guster Events	Current Owner: VMHo	st-Infra-02		
	Name		Status	
	Virtual Machine			
	🛨 🎽 Virtual Machine I	Connect		
		Start		
	Cluster Shared Volum	Turn off		
	Name	Shut down		Current Owner
		Save		VMHost-Infra-02
		Settings		
		Show the critical events for this	s resource	
		Show Dependency Report		
		More Actions	•	
		Delete		
		Properties		
		Help		
	1			





Virtual Machine Infra-SCO	M-01 Properti	es		×
General	Dependencie	es	Policies	ļ
Advanced Policies	Settings	Network f	or live migration	
Select one or more network Use the buttons to list them preferred at the bottom.	s for this virtual r in order from mo	nachine to use st preferred at	for live migratic the top to least	n.
Name			Up Down	
VM-Mgmt				-
	ОК	Cancel	Apply	

## **Optional Optimization for CSV and Live Migration Networks**

### Disable NetBios over TCP/IP for the CSV Network

- 1. Open Network Connections.
- 2. Right-click on the CSV Network adapter and select Properties.
- 3. Select Internet Protocol Version 4 (TCP/IP) and click Properties.
- 4. Click the Advanced button.
- 5. Select the option Disable NetBios over TCP/IP and click OK.





Internet Protocol Version 4 (TCP/IPv4) Properties	Advanced TCP/IP Settings
General	IP Settings DNS WINS
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.	WINS addresses, in order of use:
O Obtain an IP address automatically	
• Use the following IP address:	Add Edit Remove
IP address: 10 . 10 . 1 . 31	TELMUOSTE laskas is sanklad, it sankas to all some stiges for which
Subnet mask: 255 . 255 . 255 . 0	TCP/IP is enabled.
Default gateway:	Enable LMHOSTS lookup     Import LMHOSTS
C O <u>b</u> tain DN5 server address automatically	NetBIOS setting
☐ Use the following DNS server addresses:	Use NetBIOS setting from the DHCP server. If static IP address
Preferred DNS server:	is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.
Alternate DNS server:	Enable NetBIOS over TCP/IP     Disable NetBIOS over TCP/IP
Vaļidate settings upon exit	
OK Cancel	OK Cancel

## Installing Highly Available Microsoft System Center Components

## Installing Clustered Microsoft SQL Server 2008

The main management component is a clustered Microsoft SQL Server<sup>®</sup> with two dedicated SQL Server instances. Each instance will require the following iSCSI LUNs listed in Table 1.

LUN	Purpose	Scope	Size
LUN 1, iSCSI	SQL Server databases	Per instance	Varies
LUN 2, iSCSI	SQL Server logging	Per instance	Varies
LUN 3, iSCSI	SQL Server cluster quorum	Per cluster	1GB
LUN 4, iSCSI	SQL Server DTC	Per cluster	1GB

#### Table 18 SQL Server data locations

When the infrastructure has been completely deployed, deploy the following databases and instances.





#### Table 19 Databases

DB Client	Instance Name	DB name	Authentication
VMM SSP	<instance 1=""></instance>	<scvmmssp></scvmmssp>	Win Auth
Ops Mgr	<instance 1=""></instance>	<ops mgr_db=""></ops>	Win Auth
Ops Mgr	<instance 2=""></instance>	<ops mgr_dw_db=""></ops>	Win Auth
VMM	<instance 1=""></instance>	<vmm_db></vmm_db>	Win Auth
Opalis	<instance 2=""></instance>	<opalis_db< td=""><td>Win Auth</td></opalis_db<>	Win Auth

This section provides step-by-step instructions for installing Server 2008.

For detailed installation help, reference the Setup Help file included with the SQL Server download or product DVD.

### **Active Directory Preparation**

1. Create three domain user accounts to perform the following actions.

Note: These accounts require no special delegation:

- SQL Server Agent (ex. SQLAgent)
- SQL Server DB Engine (for example, SQLDatabase)
- Snap Drive User (for example, SnapDrive)
- 2. Global Security group for the System Center SQL Server Administrators.
- Add the <SQL Server Agent> and <SQL Server DB Engine> to the < System Center SQL Server Administrators > group.

### **Configure Windows Failover Cluster for the SQL Server**

- 1. Install Windows Server 2008 R2 SP1Enterprise in the SQL server virtual machines.
- 2. Update Windows Server with the latest available updates.
- 3. Install antivirus software and configure according to the guidelines provided in Knowledge Base article ID 961804 on the Microsoft Support Web site.
- 4. Log in and add the <SnapDrive> account and the <System Center SQL Server Administrators> group to the local administrator group.
- 5. Log in using the account from <SnapDrive>.
- 6. Enable the ISCSI Initiator by clicking <code>Start > Administrative Tools > iSCSI initiator. Click Yes to start the Microsoft iSCSI service.</code>
- 7. Click Ok to close the iSCSI Initiator Properties Panel.
- 8. Install all the prerequisites software from the sections below.

### Windows Features

- 1. Open Server Manager and select Features.
- 2. Click the Add Features link launching the Add Features wizard.
- 3. Expand .NET Framework 3.5.1 Features.



- 4. Select the .NET Framework 3.5.1 Feature.
- 5. Select the Failover Clustering feature.
- 6. Select the Multipath I/O feature.
- 7. Click Next > Install.

#### NetApp SnapDrive 6.4

- 1. Download NetApp SnapDrive 6.4.
- 2. Install Microsoft Hotfixes KB2494016-x64, KB2520235-x64, and KB2531907-x64.
- 3. Launch the SnapDrive Installer, click Next, and Accept the EULA and click Next.
- 4. Select the Storage based Licensing method and click Next.
- 5. Enter your User Name, and Organization information, and click Next.
- 6. Enter the Account information for the <SnapDrive > account created earlier.
- 7. Click Next.
- 8. Click Next and then select the Enable Transport Protocol Settings Option.
- 9. Select HTTPS.
- 10. Enter the user name and password for the Storage System administrative account.
- 11. Click Next > Next > Next > Install > Finish.

🚏 SnapDrive® - Installation Wizard	×
Transport Protocol Default Setting Specify Default Transport Setting for Storage System(s)	
✓ Enable Transport Protocol Settings	
© RPC © HTTP © HTTPS Specify the user name and password for the HTTP/HTTPS Protocol selection	on.
User Name: netapp\SnapDrive Password: •••••••	
Port ID: 443 InstallShield <back next=""></back>	Cancel

### NetApp DSM MPIO 3.5

- 1. Download NetApp DSM MPIO 3.5 package from the NOW.netapp.com Site.
- 2. Install Microsoft Hotfixes KB2522766-x64 and KB2528357-v2-x64. A restart is required after each Hotfix.



- 3. Launch the DSM MPIO Installer.
- 4. Click Next then click OK to acknowledge the EULA requirement.
- 5. Accept the EULA and click Next.
- 6. Enter the DSM License Key and click Next.
- 7. Leave the system account selected and click Next.
- 8. Click Next, then Next again then Install and when complete Restart the system.

### **Set Firewall Exceptions**

 Open Windows Firewall with Advanced Security by clicking Start > Administrative Tools > Windows Firewall with Advanced Security.

#### SnapDrive

- 1. Highlight Inbound Rules and click New Rule.
- 2. Select Program and click Next.
- 3. Enter the program path for the SnapDrive Service for example, %ProgramFiles%\NetApp\SnapDrive\SWSvc.exe.
- 4. Click Next, then select Allow the Connection and click Next, then Next again.
- 5. Enter the rule Name <SnapDrive> and Description, and click Finish.

#### SQL Server

- 1. Click New Rule.
- 2. Select Port and click Next.
- 3. Select TCP and enter the Specific local port 1433. Click Next.
- 4. Select Allow the connection and click Next then Next again.
- 5. Give a rule Name <SQL Server> and Description, and click Finish.
- 6. Repeat for the Data warehouse SQL Server instance using a port of your specification (e.g, 1444).

#### **SQL Server Discovery**

- 1. Click New Rule.
- 2. Select Port and click Next.
- 3. Select  ${\tt TCP}$  and enter the Specific local port 445. Click  ${\tt Next}.$
- 4. Select Allow the connection and click Next, then click Next again.
- 5. Give a rule Name <SQL Server Discovery> and Description, and click Finish.

### **Enable Jumbo Frames for iSCSI NICs in SQL Cluster Virtual Machines**

- 1. Open Network Connections.
- 2. Right-click on the iSCSI-Fabric-A Network adapter and click Properties, and then click the Configure button.
- 3. Select Advanced tab.


- Note: Select Jumbo Packet in the Property list box and set the value to 9014 Bytes. The 9014 Byte value in this dialog box is the correct Hyper-V synthetic adapter setting for UCS, Nexus and FAS array MTU setting of 9000 Bytes.
- 4. Repeat steps 2 through 4 for the second iSCSI Adapter and the App-Cluster Adapter.

Microsoft Virtual Machine Bus Network Adapter #3 Properties	×
General Advanced Driver Details	
General       Advanced       Driver       Details         The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.         Property:       IPv4 Checksum Offload         Unubo Packet       Unubo Packet         Large Send Offload Version 2 (IPv4)       9014 Bytes         Network Address       TCP Checksum Offload (IPv4)         TCP Checksum Offload (IPv4)       UDP Checksum Offload (IPv6)         UDP Checksum Offload (IPv6)       UDP Checksum Offload (IPv6)	
OK Cano	cel

## **Configure SQL Server Cluster**

- 1. Log in to node 1 using a domain administrative account with local privileges.
- 2. Open Server Manager and browse to Features > Failover Cluster Manager.
- 3. Validate cluster feasibility:
  - a. Select Validate a Configuration, then click Next.
  - b. Add both nodes one at a time into the Enter Name text field, and click Next.
  - c. Select Run only tests I select and click Next.
  - d. Scroll down to the storage section and clear all the storage related checkboxes.
- **Note:** These will run after you attach your iSCSI storage.
  - e. Click Next > Next.
  - f. Review the report and resolve any issues found by the validation wizard before continuing.
  - g. Click Finish.
- 4. Create a majority node cluster:



- a. In the Failover Cluster Manager, select Create a Cluster.
- b. In the Welcome screen, click Next.
- c. Add both nodes one at a time into the Enter Name text field, and click Next.
- d. Select Yes to run all validation tests, and click Next, then Next again.
- e. Select Run all test and click Next, then Next again.
- f. Click Finish. At this time you may safely ignore any warnings or errors related to clustered disks.
- g. Enter the Cluster Name, Cluster IP, and click Next.
- h. Review the configuration, and click Next, then click Finish.
- 5. Provision cluster storage:
  - a. Log in to node 1 using a domain administrative account with local privileges.
  - b. Establish iSCSI Connections. Log in to the cluster host server and open SnapDrive. Browse to iSCSI Management within SnapDrive. Click Establish iSCSI Session.
    - i. Enter the IP or name of the vFiler0 instance NetApp controller. Click Next.
    - ii. Select the source and destination IP addresses associated with iSCSI network A.
    - iii. If CHAP authentication is required configure it at this time, then click Next.
    - iv. Review for accuracy and click Finish.
    - v. Repeat steps i-v for iSCSI network B.
  - c. Repeat for NetApp Controller B.
- 6. Create quorum:
  - a. Log in to the cluster host server and open SnapDrive.
  - b. Select Disks and click Create Disk.
  - c. In the Welcome screen, click Next.
  - d. Enter the IP/FQDN for the Storage Controller and click Add.
  - e. When enumeration has completed, select the target volume where you intend to add the LUN.
  - f. Add a LUN Name, LUN Description and click Next.
  - g. Select Shared (Microsoft Cluster Services only) and click Next.
  - h. Verify both nodes are shown for your cluster and click Next.
  - i. Select Assign a Drive Letter and pick a drive letter.
  - j. Set the LUN Size to the size designated earlier, click Next then Next again.
  - k. Highlight each node in the Cluster and select the iSCSI initiators to map the new LUN.
  - I. Click Next, then Select Automatic and click Next.
  - m. Make sure that Select a cluster group by this node is selected.
  - n. Select the Cluster Group name, and click Next and then click Finish.
  - Repeat for SQL and Data Warehouse Server Data and SQL and Data Warehouse Server Log LUNs.
- 7. Create data LUNs (DTC):
  - a. Log in to the cluster host server and open SnapDrive.
  - b. Select Disks and click Create Disk.



- c. In the Welcome screen, click Next.
- d. Enter the IP/FQDN for the Storage Controller and click Add.
- e. When the enumeration has completed, select the target volume where you intend to add the LUN.
- f. Add a LUN Name and LUN Description. Click Next.
- g. Select Shared (Microsoft Cluster Services only) and click Next.
- h. Verify both nodes are shown for your cluster and click Next.
- i. Select Assign a Drive Letter and pick a drive letter.
- j. Set the LUN Size to the size designated earlier, click Next, then Next again.
- k. Highlight each node in the Cluster, and select the *iSCSI* initiators to map the new LUN.
- I. Click Next then select Automatic and click Next.
- m. Make sure that Select a cluster group by this node is selected.
- n. Select the Available Storage group name. Click Next then click Finish.
- o. Repeat these steps for all remaining LUNs.
- 8. Change cluster quorum settings:
  - a. From the node that currently owns the cluster open Failover Cluster Manager.
  - b. Right-click the virtual cluster name for the cluster you built earlier, and select More Actions > Configure Cluster Quorum Settings.
  - c. In the Before You Begin screen, click Next..
  - d. Select Node and Disk Majority and click Next.
  - e. Select the Quorum disk and click Next.
  - f. Review the confirmation for accuracy and click Next then click Finish.
- 9. Validate cluster (from the node that currently owns the cluster):
  - a. Open Failover Cluster Manager and right-click the virtual cluster name for the cluster you built earlier, and select Validate This Cluster.
  - b. Click Next, then Select "Run All Tests" and click Next.
  - c. Review the report and resolve any issues found by the validation wizard before continuing.
  - d. Click Finish.
- 10. Create MSTC resource:
  - a. From the Node that currently owns the cluster open Failover Cluster Manager.
  - b. Open the virtual cluster name for the cluster you created earlier, and select Services and applications.
  - c. From the actions pane, select Configure a Service or Application, then click Next.
  - d. Select Distributed Transaction Coordinator (DTC) and click Next.
  - e. Confirm the Name of the new resource, enter a IP Address and click Next.
  - f. Select the DTC Drive provisioned earlier and click Next.
  - g. Verify the configuration and click Next to create resource, and click Finish.
  - h. Rename the cluster networks according to purpose. For example, VM-Data, iSCSI-A.
  - i. Right-click on the two iSCSI networks and select Properties.





- j. Select the radio button to Do not allow cluster network communication on this network.
- k. Click OK.

## Install SQL Server 2008 Cluster

### Step 1: Installing SQL Server on Node 1

- 1. Log in to Node 1 using a domain administrative account with local privileges.
- 2. Download SQL Server 2008 Service Pack 1.
- 3. Extract the Service Pack on to the SQL Server Drive by running the following command: SQLServer2008R2SP1-KB252858-x64-ENU.exe /x:C:\SP1
- 4. Install the SQL Server Setup support Files by running the following command: C:\SP1\1033\_enu\_lp\x64\setup\sqlsupport\_msi\sqlsupport.msirsfx.msi
- 5. Click Next, accept the License Agreement, then click Next.
- 6. Enter the Name and Company information and click Next, click Install, then click Finish.
- 7. From a command prompt launch the setup.exe from the SQL Server 2008 DVD by running the following command:

<DVD Drive Letter>:\Setup.exe /PCUSource=C:\SP1

- 8. Acknowledge any compatibility warnings. Click Installation.
- 9. Select Installation, New SQL Server failover cluster installation.
- 10. Acknowledge any compatibility warnings. Click OK.
- 11. Resolve any failed prerequisite checks and click OK.
- 12. Click Install to install setup support files.
- 13. Resolve any support rule errors and click Next.
- 14. Enter your Product key and click Next.
- 15. Accept the Microsoft Software License Terms. Click Next.
- 16. Feature selection:
  - a. Under Instance features, select the following:
    - 1. Instance Features
    - 2. Database Engine Services
    - 3. Shared Features
    - 4. Management Tools Basic
  - b. Change the Shared feature directory and the shared feature directory (x86) to point to the HD designated for SQL Server.
  - c. Click Next.



Feature Selection Select the Standard features to i clustered.	nstall. For clustered installations, only Database Engine Services and Analysis Se	rvices can be
ietup Support Rules	Features:	Description:
roduct Key icense Terms ieature Selection nstance Configuration Disk Space Requirements Cluster Resource Group Cluster Network Configuration Cluster Network Configuration Cluster Security Policy ierver Configuration Database Engine Configuration Cror and Usage Reporting Cluster Installation Rules Ready to Install nstallation Progress Complete	Instance Features	Server features are instance- aware and have their own registry hives. They support multiple instances on a computer.
	Select All         Unselect All           Shared feature directory:         D:\Program Files\Microsoft SQL Server\           Shared feature directory (x86);         D\Program Files (x86)\Microsoft SQL Server\	rver)

- 17. Enter the SQL Server Network Name.
- 18. Select Default instance. Change the Instance root directory to point to the SQL Server HD. Click Next.
- 19. In the Disk Space Requirements page, click Next.
- 20. Select the SQL Server (MSSQLSERVER) cluster resource. Click Next.
- 21. Select the shared disks for the Database and Logs and click Next.
- 22. Specify SQL Server Instance network settings and click Next.
- 23. Select Use service SIDs and click Next.
- 24. Service accounts:
  - a. Enter the <SQL Server Agent> account information into the SQL Server Agent.
  - b. Enter the <SQL Server DB Engine> account to the SQL Server Database Engine.
  - $c. \quad Click \; {\tt Next}.$
- 25. Database engine configuration:
  - a. In the Account Provisioning window:
    - 5. Select Windows authentication mode.
    - 6. Under Specify System Center SQL Server Administrators, click Add.





7. In the resulting popup enter the <System Center SQL Server Administrators Group> created earlier. Click OK.

Database Engine Config	juration
Specify Database Engine authentica	ition security mode, administrators and data directories.
Setup Support Rules Product Key License Terms Feature Selection Instance Configuration Disk Space Requirements Cluster Resource Group Cluster Disk Selection Cluster Network Configuration Cluster Network Configuration Cluster Security Policy Server Configuration Database Engine Configuration Error and Usage Reporting Cluster Installation Rules Ready to Install Installation Progress Complete	Account Provisioning       Data Directories       FILESTREAM         Specify the authentication mode and administrators for the Database Engine.         Authentication Mode       •         • Windows authentication mode       •         • Windows authentication mode       •         • Mixed Mode (SQL Server authentication and Windows authentication)       •         Built-in SQL Server system administrator account       •         Enter password:       •         Confirm password:       •         Specify SQL Server administrators       •         SEA-TM\System Center SQL Server Administrators (System Center SQL Server Administrators have unrestricted access to the Database Engine.         Add Current User       Add

26. In the Data Directories tab:

- a. Change the Data root Directory to the <Database LUN Drive Letter>.
- b. Change the User database log directory to the <Log LUN Drive Letter> and click Next.



Finstall a SQL Server Failover Cluste Database Engine Config	uration		
Specify Database Engine authentica	tion security mode, administrators ar	nd data directories.	
Setup Support Rules Product Key License Terms Feature Selection Instance Configuration Disk Space Requirements Cluster Resource Group Cluster Disk Selection Cluster Network Configuration Cluster Security Policy Server Configuration <b>Database Engine Configuration</b> Error and Usage Reporting Cluster Installation Rules Ready to Install Installation Progress Complete	Account Provisioning Data Dir Data root directory: System database directory: User database log directory: Temp DB directory: Temp DB log directory: Backup directory:	ectories FILESTREAM	
		< Back Next > Cancel	Help

- 27. Choose whether or not to send error reports to Microsoft and click Next.
- 28. Resolve any Cluster Installation Rules and click Next, then click Install.
- 29. Review the installation report. Click Next, then click Close.

### Step 2: Adding Node 2 to SQL Server

- 1. Download SQLServer2008 Service Pack 1.
- 2. Extract the Service Pack onto the SQL Server Drive by running the following command: SQLServer2008R2SP1-KB2528583-x64-ENU.exe /x:C:\SP1
- 3. Install the SQL Server Setup support Files by running the following command: C:\SP1\1033\_enu\_lp\x64\setup\sqlsupport\_msi\sqlsupport.msi
- 4. Click Next, Accept the License Agreement, and then click Next.
- 5. Enter the Name and Company information.
- 6. Click Next, click Install, then click Finish.
- 7. From a command prompt launch the setup.exe from the SQL Server 2008 DVD by running the following command:

<DVD Drive Letter>:\Setup.exe /PCUSource=C:\SP1



- 8. Acknowledge any compatibility warnings and click Run Program.
- 9. Select Installation, Add node to a SQL Server failover cluster.
- 10. Acknowledge any compatibility warnings. Click Run Program.
- 11. Resolve any failed prerequisite checks and click OK.
- 12. Click Install to install setup support files.
- 13. Resolve any Support Rule errors and click Next.
- 14. Enter your Product key and click Next.
- 15. Accept the Microsoft Software License Terms. Click Next.
- 16. Select SQL Server instance name MSSQLSERVER. Click Next.
- 17. Enter the Passwords for all service accounts, and click Next.
- 18. Choose whether or not to send error reports to Microsoft. Click Next.
- 19. Resolve any Cluster Installation Rules and click Next, and then click Install.
- 20. Review the Add Node Progress. Click Next and then click Close.

### **Step 3: Verify Cluster Operation**

- 1. Open the Failover Cluster Manager.
- 2. Expand Services and applications and select SQL Server (MSSQLSERVER).
- 3. Select Move this service or application to..., then click Move to node <Node 2>.
- 4. At the confirmation prompt click Move SQL Server (MSSQLSERVER to <Node 2>.
- 5. Repeat for the DTC cluster resource.
- 6. Failback all resources to node 1.

### Step 4: Add SQL Server Instance

- 1. Log in to node 2 using a domain administrative account with local privileges.
- 2. From a command prompt launch the setup.exe from the SQL Server 2008 DVD by running the following command:

<DVD Drive Letter>:\Setup.exe /PCUSource=<C:\SP1

- 3. Acknowledge any compatibility warnings. Click Run Program.
- 4. Select Installation, Add Node to a SQL Server Failover cluster.
- 5. Acknowledge any compatibility warnings. Click OK.
- 6. Resolve any failed prerequisite checks.
- 7. Click Install to install setup support files.
- 8. Resolve any Support Rule errors and click Next.
- 9. Enter your Product key and click Next.
- 10. Accept the Microsoft Software License Terms, Click Next.
- 11. Under Instance features, select the following and click Next. Database Engine Services
- 12. Instance configuration:
  - a. Enter the SQL Server Network Name.





### b. Select Named Instance and enter an instance name.

### 🍀 Install a SQL Server Failover Cluster

Setup Support Rules     Specify a failover clip       Product Key     failover clip       License Terms     SQL Server       Feature Selection     Instance Configuration       Disk Space Requirements     © Named       Cluster Resource Group     Instance I       Cluster Network Configuration     Instance I       Cluster Security Policy     Instance I       Server Configuration     SQL Server       Database Engine Configuration     SQL Server	network name for uster on the netwo er Network Name: t instance d instance: ID:	scsquor	5QL Server failover 02 02	r cluster. This will b	e the name used to	o identify your
Cluster Installation Rules Detected :	root directory: er directory: SQL Server instan:	D:\Progr	02 ram Files\Microsoft ram Files\Microsoft atures on this comp	SQL Server\  SQL Server\MSSQL suter:	.10.5C5QL002	
Ready to Install Installation Progress Complete MSSQLSE	e Cluster Networ Name ERVER SCSQL0	k 01	Features SQLEngine,SQ	Edition Standard	Version 10.1.2531.0	Instance ID MSSQL10.MSSQL

- 13. In the Disk Space Requirements page, click Next.
- 14. Select the SQL Server (<Data Warehouse Instance name>) cluster resource and click Next.
- 15. Select the shared disks for the Database and Logs, and click  ${\tt Next.}$
- 16. Specify SQL Server Instance network settings and click Next.
- 17. Select Use service SIDs and click Next.
- 18. Service accounts:
  - a. Enter the <SQL Server Agent> password information into the SQL Server Agent.
  - b. Enter the <SQL Server DB Engine> password to the SQL Server Database Engine.
  - c. Click Next.
- 19. Database Engine Configuration:
  - a. Account provisioning:
    - $8. \hspace{0.1in} \texttt{Select Windows authentication mode.}$
    - 9. Under Specify System Center SQL Server Administrators click Add.
    - 10. In the resulting popup enter the <System Center SQL Server Administrators Group> created earlier.



- 11. Click  $\ensuremath{\mathsf{OK}}$  .
- 12. Click Next.
- b. Data directories:
  - 1. Change the Data root Directory to the <Database LUN Drive Letter>.
  - 2. Change the User database log directory to the <Log LUN Drive Letter>.
  - 3. Click Next.
- 20. Choose whether or not to send error reports to Microsoft and click Next.
- 21. Resolve any Cluster Installation Rules and click Next, then click Install.
- 22. Review the installation report and click Next, then click Close.

### Step 5: Add Node 1 to SQL Server Cluster

1. From a command prompt Launch the Setup.exe from the SQL Server 2008 DVD by running the following command:

<DVD Drive Letter>:\Setup.exe /PCUSource=C:\SP1

- 2. Acknowledge any compatibility warnings. Click Run Program.
- 3. Select Installation, Add node to a SQL Server failover cluster.
- 4. Acknowledge any compatibility warnings, click Run Program.
- 5. Resolve any failed prerequisite checks, and click OK.
- 6. Click Install to install setup support files.
- 7. Resolve any Support Rule errors and click Next.
- 8. Enter your Product key, and click Next.
- 9. Accept the Microsoft Software License Terms, click Next.
- 10. Select SQL Server instance name <Data Warehouse Instance name>. Click Next.
- 11. Enter the passwords for all service accounts. Click Next.
- 12. Choose whether or not to send error reports to Microsoft. Click Next.
- 13. Resolve any Cluster Installation Rules. Click Next and then click Install.
- 14. Review the Add Node Progress and click  ${\tt Next}$  and then click <code>Close</code>.

### **Step 6: Configure Remote Access**

- 1. Log in to the Data Warehouse SQL Server instance.
- 2. Open SQL Server Configuration Manager by clicking Start > All Programs > Microsoft SQL Server 2008 > Configuration Tools > SQL Server Configuration Manager.
- 3. Expand SQL Server Network Configuration, and select Protocols for <Data Warehouse Instance name>.
- 4. Right-click TCP/IP and select Properties.
- 5. Click the IP Address tab.
- 6. Scroll down and for every interface you want to enable SQL Server communications, change enabled to True and enter the port added to the firewall earlier (for example, 1444).
- 7. Click Apply.





### **Step 7: Verify Cluster Operation**

- 1. Open Failover Cluster Manager.
- Expand Services and applications and select SQL Server (<Data Warehouse Instance name>).
- 3. Select Move this service or application to ..., Click Move to node <Node 1>.
- 4. At the confirmation prompt click Move SQL Server (<Data Warehouse Instance name>to <Node 1>.
- 5. Repeat for the DTC cluster resource.
- 6. Failback all resources to Node 1.

## **System Center Operations Manager Installation**

For detailed installation help, refer to the Setup Help file included with the SCOM download or product DVD.

**Important**: Before installing SCOM components, see the System Requirements section to make sure you have all prerequisite software and hardware installed.

## Installing System Center Operations Manager 2007 R2

#### **Step 1: Active Directory Preparation**

- 1. Create five domain user accounts to perform the following actions. With the exception of the SDK and Action account, no special delegation is required. The Action account needs to have local administrator permissions on any Windows system you intend to manage, as this is the account use to install the Operations Manager Agent. The SDK account needs to be able to modify its own SPN.
  - a. Management Server Action (for example, OpsMgrAction)
  - b. SDK and Configuration Service (for example, OpsMgrSDK)
  - c. Data Reader (for example, OpsMgrReader)
  - d. Data Warehouse Write Action (for example, OpsMgrWrite)
  - e. Operations Manager Administrator (for example, OpsMgrAdmin)
- 2. Create a Global Security group for the Operations Manager Administrators.
- 3. Add the <Operations Manager administrator> and < SDK and Configuration Service > accounts to the <Operations Manager Administrative> group.
- 4. Add the <Operations Manager administrator> account to the <SQL Server Administrators> group.
- 5. With a Domain Administrators account open ADSIEdit:
  - a. Find the SDK domain user account, right-click and select Properties.
  - b. Select the Security tab, click Advanced.
  - c. Click Add. Type SELF in the object box and click OK.
  - d. Select the Properties tab.
  - e. Change the Apply to: This object only.
  - f. Scroll down and select the Allow checkbox for Read servicePrincipalName and Write servicePrincipalName.



📜 Permission Entry for OpsMgrSDK			×
Object Properties			
			1
Name: SELF		Change	I
Apply to: This object only		<b>•</b>	
Permissions:	Allow	Deny	
Read seeAlso			
Write seeAlso			
Read serialNumber			L
Write serialNumber			L
Read serverReferenceBL			
Write serverReferenceBL			
Read servicePrincipalName	$\checkmark$		
Write servicePrincipalName	$\checkmark$		
Read showInAddressBook			
Write showInAddressBook			
Read showInAdvancedViewOnly			L
Apply these permissions to chiests and	lov.		L
containers within this container only	/or		L
Managing permissions			
	ОК	Cancel	

g. Click OK > OK > OK, and close ADSIEdit.

### Step 2: Deploy Operations Manager Database

- 1. Log in to SQL Server instance, through a domain account that is a member of the <SQL Server Administrators> group.
- 2. Launch SetupOM.exe from SCOM DVD.
- 3. Select Check Prerequisites: Select Operational Database, and click Check.
- 4. Resolve any issues and click Close.
- 5. Select Install Operations Manager 2007 R2 and in the Welcome screen click Next.
- 6. Accept license agreement and click Next.
- 7. Enter User Name, Organization and click Next.
- 8. Select only the database component and click Next.





🙀 System Center Operations Manager 2007 R2 Setup	×
Custom Setup Select the components that you want to install.	NUT N
Click an icon in the list below to change how that component will be installed. Component description This component installs Microsoft Operations Manager database. This component requires 4972KB on your hard drive.	
Location: D:\Program Files\System Center Operations Manager 2007\ Browse	
Help Disk Usage < Back Next > Cancel	]

- 9. Enter the Management Group name.
- 10. Under Operations Manager Administrators, click Browse. Enter the <Operations Manager Administrative group>.
- 11. Click Next , then click Next.
- 12. Verify that the Data File and Log File locations are going to the correct LUNS and click Next.
- 13. Select whether or not to send error reporting to Microsoft. Click Next.
- 14. Click Install.
- 15. Click Finish.

#### Step 3: Install Windows Server 2008 R2 SP1 Enterprise in the SCOM Virtual Machine

- 1. Update Windows Server with the latest available updates and any prescribed Anti-Virus software.
- 2. Log in and add the <Operations Manager Administrative group> and <SDK and Configuration Service> account to the local administrators group.
- 3. Log in with the <Operations Manager Administrator> account to install the prerequisite software.

### Step 4: Install Prerequisite Software

#### Windows Features

- 1. Open Server Manager and select Features, then Add Features, this launches the Wizard.
- 2. Expand .NET Framework 3.5.1 Features and select the .NET Framework 3.5.1 sub-feature.
- Scroll down to SNMP Services and select the SNMP Service, then click Next >Install > Close.



### **IIS Server Role**

- 1. Open Server manager and select Roles, then click Add Roles, this launches the Wizard.
- 2. Select Web Server (IIS), click Next, and make sure the following Role Services are selected.
- IIS Web Server
- Common HTTP
  - Static Content
  - Default Document
  - Directory Browsing
  - HTTP Errors
- Application Development
  - ASP .NET
  - .Net Extensibility
  - ISAPI Extensions
  - ISAPI Filters
- Health and Diagnostics
  - HTTP Logging
  - Request Monitor
- Security
  - Windows Authentication
  - Request Filtering
- Performance
  - Static Content Compression
- Management Tools
  - IIS Management Console
  - IIS 6 Management Compatibility
    - IIS 6 Metabase Compatibility
    - IIS 6 WMI Compatibility
- 3. Click Next.
- 4. Click Install.
- 5. Click Close.

### Install ASP.NET Ajax Extensions 1.0

Download and Install the ASP.NET Ajax Extensions from <u>http://go.microsoft.com/fwlink/?LinkID=89064&clcid=0x409</u> and then restart.

### Step 6: Install SQL Server Reporting Services

- 1. Download SQLServer2008 Service Pack 1.
- 2. Extract the Service Pack onto the SCOM Server Drive by running the following command: SQLServer2008SP1-KB968369-x64-ENU.exe /x:C:\SP1
- 3. Install the SQL Server Setup support Files by running the following command:





C:\SP1\x64\setup\1033\sqlsupport.msi

- h. Click Next, Accept the license agreement and click Next.
- a. Enter the Name, and Company information. Click Next then click Install.
- 4. From a command prompt launch the Setup.exe from the SQL Server 2008 DVD by running the following command:

<DVD Drive Letter>:\Setup.exe /PCUSource=<SCOM Drive Letter>:\SP1

- 5. Acknowledge any compatibility warnings. Click Run Program.
- 6. Select Installation, New SQL Server stand-alone installation.
- 7. Acknowledge any compatibility warnings. Click Run Program.
- 8. Resolve any failed prerequisite checks and click OK.
- 9. Click Install to install setup support files.
- 10. Resolve any Support Rule errors and click Next.
- 11. Enter your Product key, and click Next, then Accept the Software License Terms. Click Next.
- 12. Under Instance features Select the following:
  - a. Reporting Services
- 13. Change the Shared feature directory and Shared feature directory (x86) to the <SCOM drive letter>.
- 14. Change the Instance root directory to the <SCOM drive letter> and click Next then Next again.
- 15. Select NT AUTHORITY\NETWORK SERVICE for the reporting service account name and click Next.
- 16. Click Next.
- 17. Choose whether or not to send error reports, and usage data to Microsoft, and click Next.
- 18. Fix any Installation Rule errors, and click Next, then Next again, then Install.
- 19. Review the installation report and click Close.

### **Step 5: Install Operations Manager**

- 1. Launch SetupOM.exe from the Operations Manager DVD.
- 2. Click Check Prerequisites.
- 3. From the Prerequisite Viewer, select Server, Console, PowerShell, Web Console, and Reporting, Click Check.
- 4. Resolve any issues found before continuing, and click Close.
- 5. Click Install Operations Manager 2007 R2.
- 6. Click Next on the welcome screen.
- 7. Accept the EULA and click Next.
- 8. Enter your Username, and Organization information. Click Next.
- 9. In the Custom Setup screen:
  - a. Select the Management Server, User Interfaces, Command Shell, and Web Console.
  - b. Change the installation path for each component by highlighting them one at a time, and clicking Browse. Change the path to the <SCOM Drive Letter>.





c. Click Next.

🙀 System Center Operations Manager 2007 R	2 Setup 🗙
<b>Custom Setup</b> Select the components that you want to install.	A H
Click an icon in the list below to change how that con	nponent will be installed. Component description This component installs Microsoft Operations Manager Management Server. This component requires 319MB on your hard drive.
Location: D:\Program Files\System Center Operations Manage	r 2007\Br <u>o</u> wse
Help Disk Usage < B	ack <u>N</u> ext > Cancel

- 10. Enter the FQDN for the virtual SQL Server Instance created earlier. Click Next.
- 11. Enter the account information for the <Management Server Action> account. Click Next.
- 12. Enter the account information for the <SDK and Configuration Service> account. Click Next.
- 13. Select Use Windows Authentication and click Next.
- 14. Choose whether or not to participate in the customer experience improvement program, and click Next.
- 15. Clear the Start Console checkbox and click Finish.
- 16. Encryption key backup:
  - a. Click Next then select Backup the Encryption key and click Next.
  - b. Enter a UNC path not on the operations manager server and click Next.
  - c. Enter a password to secure the encryption key and click Next, then click Finish.

### Step 6: Configure Web Console Security

- Open IIS Manager by selecting Start > Administrative Tools > Internet Information Services (IIS) Manager.
- 2. Click the root of the IIS management server (servername <domain>\user).
- 3. In the center pane, scroll down and open Server Certificates.
- 4. In the actions pane click Create Self-Signed Certificate. Enter a name for the new certificate, click OK.
- 5. Expand Server, expand Sites, and select Operations Manager 2007 Web Console.



- 6. In the actions pane click Bindings and do as follows:
  - d. Click Add.
  - e. Change the type to https, and select the new certificate.
  - f. Click OK and then click Close.

### Step 7: Provision Data Warehouse Database

- 1. Log in to data warehouse SQL Server instance, using a domain account that is a member of the <SQL Server Administrators> group.
- 2. Launch SetupOM.exe from SCOM DVD.
- 3. Select Check Prerequisites:
  - a. Select Data Warehouse and click Check.
  - b. Resolve any issues found and click Close.
- 4. Select Install Operations Manager 2007 R2 Reporting.
- 5. In the Welcome screen, click Next.
- 6. Accept license agreement and click Next.
- 7. Enter User Name, Organization and click Next.
- 8. In the Custom Setup screen:
  - a. Select only the Data Warehouse component.
  - b. Change the installation path to point to the SQL Server VHD, and click Next.

🙀 Operations Manager 2007 R2 Reporting 9	Setup 🗙			
Custom Setup				
Select the components that you want to install.				
Click an icon in the list below to change how that (	component will be installed.			
Data Warehouse Reporting Server	Component description This component installs Microsoft Operations Manager Data Warehouse. This component requires 1373KB on your hard drive.			
Location:       D:\Program Files\System Center Operations Manager 2007\       Help     Disk Usage       < Back				

- 9. Select the SQL Server Data Warehouse Instance and click Next.
- 10. Verify that the Data File and Log File locations are going to the correct LUNS and click Next.



- 11. Click Install.
- 12. Click Finish.

### **Step 8: Install Operation Manager Reporting**

- 1. Log in to Operations Manager Server.
- Launch the SQL Server Reporting Services by clicking Start > All Programs > Microsoft SQL Server 2008 > Configuration Tools > Reporting Services Configuration Manager.
- 3. Click Connect.
- 4. Verify that the Report Service Status is Started.
- 5. Select Web Service URL from the left pane.
- 6. Click Apply to create the Web instance.
- 7. Select Database from the left pane.
- 8. Click Change Database.
- 9. Select Create a new report server database and click Next.
- 10. Enter the FQDN for the SQL Database Failover Cluster.
- 11. Click Next.
- 12. Accept all defaults and click Next.
- 13. Leave the credentials set to Service Credentials and click Next.
- 14. Click Next to provision the database.
- 15. Click Finish.
- 16. Select Report Manager URL from the left pane.
- 17. Click Apply to create the virtual directory.
- 18. Select E-mail Settings from the left pane.
- 19. Enter the Sender Address and SMTP server and click Apply.
- 20. Click Exit to close the Report Server Configuration server.
- 21. Launch SetupOM.exe from SCOM DVD.
- 22. Select Install Operations Manager 2007 R2 Reporting.
- 23. In the Welcome screen, click Next.
- 24. Accept license agreement and click Next.
- 25. Enter User Name, Organization and click Next.
- 26. Select Reporting Server and click Next.
- 27. Enter the FQDN for the SCOM Server and click Next.
- 28. In the Data Warehouse screen, enter:
  - a. Enter the Name and Instance of the Data Warehouse SQL Server instance.
  - b. Enter the SQL Server Port that was configured for remote access.
  - c. Click Next.





🙀 Operations Manager 2007 R2 Rep	oorting Setup
Connect to the Operations Manag	er Data Warehouse
Specify the name of the SQL Server of warehouse.	database instance that hosts the Operations Manager data
SQL Server database instance (SQL Server\SQL Instance)	scsql002.sea-tm.netapp.com\scsql002
<u>S</u> QL database name	OperationsManagerDW
SQL Server <u>P</u> ort	1444
	< <u>Back N</u> ext > Cancel

- 29. Select the Reporting server and click Next.
- **30. Enter the account information for the** <Data Warehouse Write Action> account, and click Next.
- 31. Enter the account information for the <Data Reader> account and click Next.
- 32. Choose whether or not to send operational data reports to Microsoft and click Next.
- 33. Click Install.
- 34. Click Finish.

## **Configure Operations Manager**

- 1. Log in to Operations Manager Server.
- 2. Open the Operations Manager Console, by clicking Start > All Programs > System Center Operations Manager 2007 R2 > Operations Console.
- 3. Add devices to manage:
  - a. From the top center pane click Required: Configure computers and devices to manage.
  - b. Select Windows Computers and click Next.
  - c. Select Advanced discovery and click Next.
  - d. Select Browse for or type computer names and click Browse.
  - e. Enter all management and Hyper-V hosts and click Next.
  - f. Select Use selected Management Server Action Account, click Discover.



- g. Select all devices to monitor, click Next, and then click Finish.
- 4. Enable Agent proxy for cluster hosts.
  - a. From the Operations Manager Console select Administration.
  - b. In the right pane expand Device management and select Agent Managed.
  - c. Select the first cluster host. Right-click, and select Properties.
  - d. Click the Security tab.
  - e. Check Allow this agent to act as a proxy and discover managed object on other computers.
  - f. Click OK.
  - g. Repeat for each cluster host in your environment.
- 5. Add Management Packs:
  - a. Download and install the following Management Packs from Microsoft. Note the installers only extract the management packs into the correct folders, accept all defaults.
    - Windows Server Operating System Management Pack for Operations Manager 2007
    - <u>Windows Server Internet Information Services 7 Management Pack for Operations Manager</u>
       <u>2007</u>
    - <u>Windows Server Failover Clustering Management Pack for Operations Manager 2007</u>
    - <u>Windows Server Hyper-V Management Pack for Operations Manager 2007</u>
    - <u>SQL Server Monitoring Management Pack</u>
  - b. From the Operations Manager Console, select Administration.
  - c. In the top left under Actions: click Import management packs.
  - d. Click Add > Add from disk...
  - e. Browse to %ProgramFiles(x86)%\System Center Management Packs.
  - f. In the following order expand each folder for all the management packs just added, when expanded Select all the .MP files and click Open.
    - 1. Windows Server Base OS System Center Operations Manager 2007 MP
    - 2. Internet Information Services MP
    - 3. Windows Cluster Operations Manager 2007 MP
    - 4. Windows Server Hyper-V Operations Manager 2007 MP
    - 5. SQLServerMP
  - g. When all the MP has been added to the wizard, click Install.
  - h. Click Yes.
  - i. When all MP have finished importing click Close.

## Install System Center Virtual Machine Manager

### **Step 1: Active Directory Preparation**

- 1. Create two domain user accounts to perform the following actions. These account require no special delegation.
  - SCVMM Database (for example, SCVMMDatabase)
  - SCVMM Service (for example, SCVMMService)



- 2. Create a Global Security group for the SCVMM Server Administrators.
- Add the <SCVMM Service> and < Management Server Action > accounts to the <SCVMM Server Administrators> group.
- 4. Add the <SCVMM Service> to the <Operations Manager Administrators> group.
- 5. Add the <SCVMM Database> to the <SQL Server Administrators> group.

### Step 2: Install Windows Server 2008 R2 SP1Enterprise in the SCVMM Virtual Machines

- 1. Update Windows Server with the latest updates.
- 2. Install antivirus software.
- 3. Log in and add the <SCVMM Server Administrators> group, <SnapDrive>, and <SCVMM Service > accounts to the local administrators group.
- 4. Log in using an account with both domain and local administrative privileges.

### Step 3: Install Prerequisite Software

### Windows Features

- 1. Open Server Manager and select Features.
- 2. Click the Add Features link launching the Add Features wizard.
- 3. Expand .NET Framework 3.5.1 Features.
- 4. Select the .NET Framework 3.5.1 Feature.
- 5. Select the Multipath I/O feature.
- 6. Click Next > Install > Close.

### Add Web Server Role

- 1. Open Server Manager and select Roles.
- 2. Click Add Role.
- 3. Select Web Server (IIS) and click Next.
- 4. In the introduction to IIS page, click Next.
- 5. Select the following role service:
- IIS Web Server
- Common HTTP
  - Static Content
  - Default Document
  - Directory Browsing
  - HTTP Errors
- Application Development
  - ASP .NET
  - .Net Extensibility
  - ISAPI Extensions
  - ISAPI Filters
- Health and Diagnostics
  - HTTP Logging



- Request Monitor
- Security
  - Request Filtering
- Performance
  - Static Content
- Management Tools
  - IIS Management Console
  - IIS 6 Management Compatibility
    - IIS 6 Metabase Compatibility
    - IIS 6 WMI Compatibility
- 6. Click Next > Install > Close.

### Install SQL Management Tools - Basic

- 1. Download SQLServer2008 Service Pack 1.
- 2. Extract the Service Pack onto the SCVMM Server Drive by running the following command: SQLServer2008SP1-KB968369-x64-ENU.exe /x:<SCVMM Drive Letter>:\SP1
- 3. Install the SQL Server Setup support Files by running the following command: <SCVMM Drive Letter>:\SP1\x64\setup\1033\sqlsupport.msi
- 4. Click Next. Accept the license agreement and click Next.
- 5. Enter the Name, and Company information, click Next, and then click Install.
- 6. From a command prompt launch the Setup.exe from the SQL Server 2008 DVD by running the following cmd.

<DVD Drive Letter>:\Setup.exe /PCUSource=<SCVMM Drive Letter>:\SP1

- 7. Acknowledge any compatibility warnings and click Run Program.
- 8. Select Installation, New SQL Server stand-alone installation.
- 9. Acknowledge any compatibility warnings and click Run Program.
- 10. Resolve any failed prerequisite checks and click OK.
- 11. Click Install to install setup support files.
- 12. Resolve any Support Rule errors. Click Next.
- 13. Enter your Product key, and click  ${\tt Next}.$
- 14. Accept the Microsoft Software License Terms. Click Next.
- 15. In the Feature Selection screen:
  - a. Under Instance features select the following:
    - 1. Shared Features
    - 2. Management Tools –Basic
  - b. Change the Shared feature directory and the Shared feature directory (x86) to the <SCVMM drive letter> and click Next.





Feature Selection Select the Standard features to clustered.	nstall. For clustered installations, only Database Engine Services and Analysis	Services can be
etup Support Rules	Features:	Description:
Product Key License Terms F <b>eature Selection</b> Disk Space Requirements Error and Usage Reporting Installation Rules Ready to Install Installation Progress Complete	Instance Features Database Engine Services SQL Server Replication Full-Text Search Analysis Services Reporting Services Shared Features Business Intelligence Development Studio Client Tools Connectivity Integration Services Client Tools Backwards Compatibility Client Tools SDK SQL Server Books Online Management Tools - Basic Management Tools - Complete SQL Client Connectivity SDK Microsoft Sync Framework Redistributable Features	Server features are instance- aware and have their own registry hives. They support multiple instances on a computer
	Select All     Unselect All       Shared feature directory:     D:\Program Files\Microsoft SQL Server	ər\
	Shared feature directory (x86): D:\Program Files (x86)\Microsoft SQL	. Server\

- 16. Choose whether or not to send error reports and usage data to Microsoft, and click Next.
- 17. Fix any Installation Rule errors. Click Next, click Install, then click Next.
- 18. Review the installation report and click Close.

#### Enable iSCSI

- 1. Enable the ISCSI Initiator by clicking Start > Administrative Tools > iSCSI initiator. Click Yes to start the Microsoft iSCSI service.
- 2. Click OK to close the iSCSI Initiator Properties Panel.

## **Enable Jumbo Frames for iSCSI NICs in SCVMM Virtual Machine**

- 1. Open Network Connections.
- 2. Right-click on the iSCSI-Fabric-A Network adapter and click Properties, then click the Configure button.
- 3. Select Advanced tab.
- 4. Select Jumbo Packet in the property list box and set the value to 9014 Bytes.
- **Note:** The 9014 Byte value in this dialog box is the correct Hyper-V synthetic adapter setting for UCS, Nexus and FAS array MTU setting of 9000 Bytes.
- 5. Repeat steps 2 through 4 for the second iSCSI Adapter..





b.	
Microsoft Virtual Machine Bus Netrork Adapter #3 Propertie	es X
General Advanced Driver Details	
The following properties are available for this network adapter. Click the property you want to change on the left, and then select its valu on the right. Property: IPv4 Checksum Offload Jumbo Packet Large Send Offload Version 2 (IPv4) Large Send Offload Version 2 (IPv6) Network Address TCP Checksum Offload (IPv4) TCP Checksum Offload (IPv6) UDP Checksum Offload (IPv6) UDP Checksum Offload (IPv6)	
ОК	Cancel

### NetApp SnapDrive 6.4

- 1. Download NetApp SnapDrive 6.4.
- 2. Launch the SnapDrive Installer, click Next and Accept the EULA and click Next.
- 3. Select the Storage based Licensing method and click Next.
- 4. Enter your User Name, and Organization information, and click Next.
- 5. Enter the Account information for the <SnapDrive > account created earlier.
- 6. Click Next.
- 7. Click Next and then select the Enable Transport Protocol Settings Option Select HTTPS.

.

8. Enter the UserName and Password for Storage Systems root user



9.	Click Next > Next > Install > Finish.					
	🙀 SnapDrive® - Installation Wizard					
	Transport Protocol Default Setting	(				
	Specify Default Transport Setting for Storage System(s)					
	Enable Transport Protocol Settings					
	C RPC	]				
	C HTTP					
	HTTPS					

netapp\SnapDrive		
<u>P</u> assword:		
•••••		
Port ID: 443		

### NetApp DSM MPIO 3.5

- 1. Download NetApp DSM MPIO 3.5 package from the NOW.netapp.com Site.
- 2. Install Microsoft Hotfixes KB2522766-x64 and KB2528357-v2-x64. A restart is required after each Hotfix.
- 3. Launch the DSM MPIO Installer.
- 4. Click Next then click OK to acknowledge the ALUA requirement.
- 5. Accept the EULA and click Next.
- 6. Enter the DSM License Key and click Next.
- 7. Leave the system account selected and click Next.
- 8. Click Next, then Next again then Install and once complete restart the system.

### Step 4: Provision Storage

- 1. Log in to the SCVMM server using a domain administrative account with local privileges.
- 2. Establish iSCSI Connections.
  - a. Open SnapDrive.
  - b. Browse to iSCSI Management within SnapDrive.
  - c. Click Establish iSCSI Session.
    - 1. Enter the IP/name of the NetApp controller. Click Next.
    - 2. Select the source and destination IP addresses associated with iSCSI network A.
    - 3. If CHAP authentication is required configure at this time.



- 4. Click Next. Review for accuracy and then click Finish.
- 5. Repeat for iSCSI network B.
- 3. Create VM library drive:
  - a. Open SnapDrive and selects Disks and click Create Disk.
  - b. In the Welcome screen, click Next.
  - c. Enter the IP/FQDN for the vFiler0 Controller, and click Add.
  - d. When the enumeration has completed, select the target volume where you intend to add the LUN.
  - e. Add a LUN Name, LUN Description, and click  ${\tt Next.}$
  - f. Select Dedicated. Click Next.
  - g. Select Assign a Drive Letter, and pick a drive letter.
  - h. Set the LUN Size, for example 500g, and click Next.
  - i. Select the iSCSI initiators to map the new LUN to, and click Next.
  - j. Select Automatic and click Next and then click Finish.

### Step 5: Install System Center Virtual Machine Manager

- 1. From the product DVD or network share, double-click setup.exe.
- 2. In the Setup menu, click VMM Server.
- 3. In the License Terms page, click I accept the terms of this agreement. Click Next.
- 4. In the Customer Experience Improvement Page (CEIP) page, click Yes to participate or No to opt out of the CEIP. Click Next.
- 5. In the Product Registration page, enter your name and the name of your company. Click Next.
- 6. In the Prerequisites Check page, review any alerts or warnings about inadequate hardware or uninstalled software prerequisites. You can continue if you receive warnings, but alerts must be resolved before you can proceed with the installation. Click Next.
- 7. In the Installation Settings page, select the appropriate path for your System Center SCVMM2008 program files location. These should be placed on the SCVMM VHD provisioned earlier.
- 8. In the SQL Server Settings page:
  - a. Select Use a supported version of SQL Server.
  - b. Enter the FQDN of the virtual SQL Server Cluster.
  - c. Select Use the following credentials.
  - d. Enter the <SCVMM Database> account and password.
  - e. Select the default MSSQLSERVER instance.
  - f. Select Create a new database and click Next.



🖏 SQL Serve	r Settings		0		
License Terms Microsoft Update Customer Experience Improvement Program Product Registration Prerequisites Check	Do you want to use an existing instance of SQL Server or install Microsoft SQL Server 2005 Express Edition SP3?  C Instal SQL Server 2005 Express Edition SP3 Database location C: VProgram Files/Microsoft System Center Virtual Machine Manager 2008 R2/DB Browse C: Use a supported version of SQL Server				
Installation Location SQL Server Settings Library Share Settings Installation Settings	Server name	scsq01 sea-im netapo com			
	User name and domain:	nhials sea-tm\SCVMMDatabase Format: Domain\Username			
Summary of Settings	Password:				
Installation	Select or enter a SQL instance:	MSSQLSERVER			
	Select or enter a database:	VituaManagerDB			
		✓ Create a new database			
		Previous Next Cano	el		

- 9. In the Library Share Settings page, click Change to change the share location. Select the LUN provisioned earlier, click Make New Folder, rename the new folder to Virtual machine Manager Library Files. Select the Virtual machine Manager Library Files Folder. Click OK.
- 10. Click Next.

During installation, the Setup Wizard creates a folder named VHDs and two virtual hard disks of different sizes (16GB and 60GB) that you can use to create a new virtual machine or use as additional disk drives.

11. In the Port Assignments page, assign the ports you want to use for communications and file transfers between SCVMM components. If Windows Firewall is turned on the wizard will attempt to add firewall exceptions for each port.

**Important :** You can change the default port settings to avoid conflicts with other applications in your environment. However, the port settings that you assign for the SCVMM server must identically match the port settings you assign when installing associated SCVMM components.

- 12. Under VMM Service Account, select Other account. Enter the <SCVMM Service> account information. Click Next, and then click Install.
- 13. In the Installation page, after setup is complete, click the link in the Status window to check for the latest SCVMM updates.

#### Step 6: Install System Center Virtual Machine Manager Administrator Console

- 1. From the product DVD or network share, double-click setup.exe.
- 2. In the Setup menu, click VMM Administrator Console.
- 3. In the License Terms page click I accept the terms of this agreement. Click Next.
- 4. In the Customer Experience Improvement Page (CEIP) page, click Next.



- 5. In the Prerequisites Check page, review any alerts or warnings about inadequate hardware or uninstalled software prerequisites. You can continue if you receive warnings, but alerts must be resolved before you can proceed with the installation. Click Next.
- 6. In the Installation Settings page, select the appropriate path for your System Center SCVMM2008 program files location. These should be placed on the SCVMM VHD provisioned earlier.
- 7. In the Configuration Settings page, do one of the following:
  - a. Click Next to use the default port (8100) for the SCVMM Administrator Console to communicate with the SCVMM server.
  - b. Assign a different port that you want to use for the SCVMM Administrator Console to communicate with the SCVMM server, and then click Next.

**Important:** The port settings that you assign for the SCVMM Administrator Console must identically match the port settings that you assigned in the SCVMM server.

- 8. Click Install.
- 9. In the Installation page, after setup is complete, check for the latest VMM updates, and open VMM Administrator Console. Click Close.

The Connect to Server dialog box opens the first time you open the console.

- 10. In the Connect to Server dialog box.
- 11. Click Connect to connect to the local SCVMM server (localhost) using the default port (8100).
- 12. In the Server name box, type the name of the computer where the SCVMM server is installed, followed by a colon and the port that you want to use to connect the SCVMM Administrator Console to the SCVMM server, and then click Connect.

### Step 7: Configure SCVMM

- 1. From the Virtual Machine Manager (VMM) console, select All Hosts. From the Actions pane select Add host.
- 2. Select Windows Server-based host on an Active Directory domain, and enter credentials for a domain account that has permissions to both search AD, and to install the agent on the Hyper-V hosts.
- 3. Click Search and do the following:
  - a. Select the Hyper-V checkbox, and click Search.
  - b. Select every Hyper-V host you want to add to SCVMM, and click Add, then Yes, then Yes, then OK.
- 4. Click Next, Next, then Next again.
- 5. Click Add Hosts.

### Step 8: Install the OnCommand Plugin 3.0 Rapid Provisioning cmdlets

- 1. Download OnCommand Plugin 3.0 from the NOW<sup>™</sup> site. Although the cmdlets are a separate product from OnCommand Plugin, they share a common installer.
- 2. Launch the OnCommand Plugin executable file.
- 3. In the Welcome screen click Next.
- 4. Accept the EULA, and click Next.
- 5. Enter User Name and Organization. Click Next.
- 6. Change the installation path to point to the SCVVM VHD (for example, D:\Program Files\NetApp\OnCommand\MS\_Plugin\) Click Next.



- 7. Select only the Cmdlets feature and click Next >Install > Finish.
- 8. Enter the credentials for the SCVMM Service account and click Next.
- 9. Open the Rapid Provisioning PowerShell prompt by launching the OnCommand® Cmdlets link on the desktop.
- 10. Type Set-ExecutionPolicy -ExecutionPolicy AllSigned. Type Y to confirm.
- 11. Close and reopen OnCommand® Cmdlets.
- 12. Enter A to always run NetApp Cmdlets.
- 13. Run Add-OCStorageSystem for each Controller.
- 14. Test by running Get-OCStorage.

### Step 9: Installing the Virtual Machine Manager Self-Service Portal (Optional)

The Self-Service Portal Setup wizard installs all three of the self-service portal components.

### Table 20 Service accounts requested during self-service portal setup

Account Name	Requested during	Used for	Prerequisites	High Security
Service Account	VMMSSP server component setup	<ul> <li>Running the Windows Service implementation of the VMMSSP server component, the Virtual Machine Manager Self-Service Portal 2.0 service, and underlying services and processes. The server component also uses this account for external communication, such as:</li> <li>Communicating with the VMM server and performing tasks that require interacting with the VMM server.</li> <li>Communicating with the VMMSSP database.</li> </ul>	Make sure this is an Active Directory domain account. Before you install the VMMSSP server component, make sure this account has administrative permissions on the VMM Administrator Console. You must also make sure that this account is granted Local Administrator permissions on the computer where you plan to install the server component.	Use a low- privilege domain account
Application Pool Identity	pplication oolVMMSSP Web site component setupRunning the application pool used for the VMMSSP Web site component. The VMMSSP Web site component also uses this account for external communication, such as:•Communicating with the VMMSSP server and database components.•Running tasks that require interacting with the other self- service portal components.		This account can be a domain account.	Use a low- privilege domain account.





#### Table 21 Ports and protocols for the self-service portal

Connection Type	Protocol	Default Port	Where to Change the Setting
VMMSSP Web site to/from VMMSSP server	WCF	8000	During self-service portal setup. After setup, in the <b><services></services></b> section of the Microsoft.DITSC.ProvisioningService.exe.config file. For more information, see "Tuning the Self-Service Portal with Global Parameters" in the <i>Virtual Machine Manager</i> <i>Self-Service Portal 2.0: Datacenter Administration Guide</i> .
Client to/from VMMSSP Web site	HTTP/HTTPS	Without SSL: 80 With SSL: 443	During self-service portal setup. After setup, in the <b>Site Bindings</b> dialog box for the VMMSSP Web site in IIS. For information about configuring SSL for the portal, see the "Post Installation: Hardening the Self-Service Portal Website" section in this guide.
VMMSSP Web site to/from VMMSSP database	Tabular Data Stream (TDS)	1433	During self-service portal setup.
VMMSSP server to/from VMMSSP database	TDS	1433	During self-service portal setup.
VMMSSP Web site to/from virtual machine hosts	Remote Desktop Protocol (RDP)	2179	This port cannot be changed.

### **Preparation Checklist**

Before you install the self-service portal, be sure that you have prepared the following:

- A service account and an application pool identity for the self-service portal, as defined in Table 20.
   Important: You must create the service account and application pool identity before you run the Self-Service Portal Setup wizard. The wizard does not create new accounts.
- If appropriate, a SQL Server maintenance account as described in the section <u>Active Directory</u> Preparation.
- If appropriate, firewall port exceptions for the ports listed in Table 21.

**Important:** You must have administrator permissions on the computers on which you intend to install the self-service portal components. You also must be a member of the local Administrators group on the computer running SQL Server.

### To Install the VMMSSP Server Component and Database Component

- **Note:** This procedure assumes that you have a separate database server available, running SQL Server 2008 Enterprise Edition or Standard Edition.
- 1. Download the SetupVMMSSP.exe file and place it in the computer on which you want to install the VMMSSP server component.



- 2. To begin the installation process, on the computer on which you are installing the server component, right-click SetupVMMSSP.exe, and click Run as administrator.
- 3. In the Welcome page, click Install.
- 4. Review and accept the license agreement and click Next.
- 5. Click VMMSSP server component and click Next.
- 6. In the Check Prerequisites for the Server Component page, wait for the wizard to complete the prerequisite checks, and then review the results. If any of the prerequisites are missing, follow the instructions provided. When all of the prerequisites are met, click Next.
- 7. Accept or change the file location and then click Next.
- 8. Configure the VMMSSP database:
  - a. In Database server, type the name of the database server that will host the new VMMSSP database (or that hosts an existing database).
  - b. Click Get Instances to get the SQL Server instances available in the database server. In SQL Server instance, select the SQL Server instance that manages the new (or existing) database.
  - c. In Port, type the port number that the SQL Server instance uses for incoming and outgoing communication. The default port is 1433.
  - d. Under Credentials, click the type of authentication that the database will use for incoming connections (Windows authentication or SQL Server authentication).
  - e. If you clicked SQL Server authentication, type the user name and password of a SQL Server account to use to access the database.
  - f. If you want the self-service portal to create a new database (for example, if you are running the Setup wizard for the first time), click Create a new database.

**Important:** If you are installing the self-service portal for the first time you must select the option to create a new database.

Note: The self-service portal database name is DITSC, and cannot be changed.

g. If you want the self-service portal to use an existing database, click Use an existing database. The DITSC database is selected, and cannot be changed.

**Important:** If you are upgrading from the release candidate version of the self-service portal, make sure you have followed the procedure in "Upgrading from the Release Candidate Version of the Self-Service Portal" before continuing.

- h. When you finish configuring the self-service portal database, click Next.
- 9. Type the user name, password, and domain of the service account for the VMMSSP server component. Click Test account to make sure that this account functions. When finished, click Next.
- **Note:** For more information about considerations and requirements for the service account, see section <u>0 Active Directory Preparation</u>.
- 10. Enter the settings to configure the server component. These settings include the port numbers of the WCF endpoint for the TCP protocol. When finished, click Next.



- **Note:** The VMMSSP server component uses the TCP endpoint port to listen for client requests. The WCF service uses the HTTP endpoint port for publishing the self-service portal service metadata. The metadata will be available using HTTP protocol with a GET request. For more information about WCF endpoints, see the <u>Fundamental Windows Communication Foundation Concepts</u> topic in the MSDN Library.
- 11. In the Datacenter administrators box, type the names of the accounts that you want to be able to administer the self-service portal. In the self-service portal, these users will be members of the DCIT Admin user role and have full administrative permissions.
- **Note:** For more information about the DCIT Admin user role, see the section <u>0 Active Directory</u> <u>Preparation</u>.
- 12. In the Installation Summary page, review the settings that you selected, and then click Install. When the installation finishes, click Close.

### To Install the VMMSSP Web Site Component

**Important:** This procedure assumes that you have already installed the VMMSSP server component, and that you have placed the downloaded SetupVMMSSP.exe file on all computers on which you plan to install the VMMSSP Web site component.

- 1. To begin the installation process, on the computer on which you are installing the VMMSSP Web site component, right-click SetupVMMSSP.exe and then click Run as administrator.
- 2. On the Welcome page, click Install.
- 3. Review and accept the license agreement and then click Next.
- 4. Click VMMSSP Web site component and then click Next.
- 5. In the Check Prerequisites for the VMMSSP Website Component page, wait for the wizard to complete the prerequisite checks, and then review the results. If any of the prerequisites are missing, follow the instructions provided. When all of the prerequisites are met, click Next.
- 6. Accept or change the file location and then click Next.
- 7. You can use this setting to install the component on a computer other than the one running the Setup wizard.
- 8. Use the following steps to configure the IIS Web site for the self-service portal. For information about the IIS Web site properties required to configure the portal, see <u>Understanding Sites</u>, <u>Applications</u> and <u>Virtual Directories on IIS 7</u>.
- **Note:** For information about the application pool identity required to configure the VMMSSP Web site component, see the "Service Accounts" section earlier in this document.
  - a. In IIS Website name, type the name that IIS will use for the self-service portal. The default name is VMMSSP.
  - b. In Port number, type the port number that IIS will use for the self-service portal. The default port is 80.
  - c. In Application pool name, type a name for the application pool that the Setup wizard will create for the VMMSSP Web site. The default name is VMMSSPAppPool.
  - d. Type the domain, user name, and password of the account that you have configured for the application pool to use. For information about the application pool identity for the self-service portal, see the "Service Accounts" section earlier in this document.
  - e. When you finish configuring the IIS properties for the self-service portal, click Next.
- 9. Use the following steps to configure the VMMSSP database.



- f. In Database server, type the name of the database server that hosts the database that you configured for the VMMSSP server component.
- g. To see a list of the SQL Server instances associated with the specified database server, click Get Instances. In SQL Server instance, select the SQL Server instance that manages the new (or existing) VMMSSP database.
- h. In Port, type the port number that the SQL Server instance uses for incoming and outgoing communication. The default port is 1433.
- i. Under Credentials, click the type of authentication that the database uses for incoming connections (Windows authentication or SQL Server authentication).
- j. If you clicked SQL Server authentication, type the user name and password of a SQL Server account to use to access the database. Make sure that this account information matches the information you configured when you installed the VMMSSP server component.
- k. Click Use an existing database. The self-service portal automatically locates the existing DITSC database.
- I. When you finish configuring the database, click Next.
- 10. Enter the settings to configure how the VMMSSP Web site communicates with the VMMSSP server component. These settings include the host name of the WCF server (the name of the computer running the VMMSSP server component) and the TCP endpoint port number to communicate with the server component. When finished, click Next.
- 11. On the Installation Summary page, review the settings that you selected, and then click Install. When the installation finishes, click Close.

#### **To Enable SSP Rapid Provisioning**

- 1. In the Self-Service Portal, navigate to Self Service Portal Settings > Customize Virtual Machine Actions > MasterActionXML.
- 2. Select CopyActionXML.
- 3. Type the name for the new action script.

For example, enter ONTapRapidProvisioning.

- 4. To create a virtual machine action, navigate to CreateVM > Edit.
- 5. Paste the ONTapCreateVM.txt content into the Script section of the edit window.
- 6. Paste the ONTapCreateVMLocked.txt content into the LockedScript section.
- 7. Set the options for the create action script.
  - a. For the Successful Return Code, enter 0.
  - b. Select the Timeout box and enter 9999.
  - c. Clear the Continue on Error box.
- 8. 8. Click Save and Close.
- 9. 9. To delete a virtual machine action, navigate to DeleteVM > Edit.
- 10. 10. Paste the ONTapDeleteVM.txt content into the Script section of the edit window.
- 11. 11. Paste the ONTapDeleteVMLocked.txt content into the LockedScript section.
- 12. 12. Set the options for the delete action script.
  - a. For the Successful Return Code, enter 0.
  - b. Select the Timeout box and enter 9999.
  - c. Clear the Continue on Error box.



- 13. 13. Click Save and Close.
- 14. 14. Navigate to Infrastructure > ServiceRole > Edit.
- 15. 15. From the Action XML drop-down list, select ONTapRapidProvisioning.
- **Note:** This step makes sure that the use of the script during the CreateVM or DeleteVM action. This script name must match the name you used to create the script.

#### Step 10: SCOM Administrative Console

- 1. From the SCOM DVD or network share double-click SetupOM.exe.
- 2. Select Install Operation Manager 2007 R2.
- 3. In the Welcome screen, click Next.
- 4. In the License Terms page, click I accept the terms of this agreement and click Next.
- 5. In the Product Registration page, enter your name and the name of your company. Click Next.
- 6. In the feature selection page, select only the User Interface, and Command Shell. Change the installation to target the SCVMM VHD, and click Next.
- 7. In the Customer Experience Improvement Page (CEIP) page, click Yes to participate or No to opt out of the CEIP, and click Next.
- 8. Click Install.
- 9. Uncheck Start the Console.
- 10. Click Finish.

## **Configure SCVMM SCOM Integration**

- 1. Log in to the SCOM server with a domain account that is both a SCVMM and SCOM Administrator.
- 2. From the product DVD or network share, double-click setup.exe.
- 3. In the Setup menu, click Configure Operations Manager.
- 4. In the License Terms page click I accept the terms of this agreement and click Next.
- 5. In the Microsoft Update page select either Use Microsoft Update or I don't want to use Microsoft Update. Click Next.
- 6. In the Customer Experience Improvement Page (CEIP) page, and click Next.
- 7. In the Prerequisites Check page, review any alerts or warnings about inadequate hardware or uninstalled software prerequisites. You can continue if you receive warnings, but alerts must be resolved before you can proceed with the installation. Click Next.
- 8. In the Installation Settings page, select the appropriate path for your System Center SCVMM2008 program files location. These should be placed on the SCOM VHD provisioned earlier. (ex. D:\Program Files\Microsoft System Center Virtual Machine Manager 2008 R2).
- 9. In the Port Assignment page, enter the FQDN for the SCVMM server and the port specified during SCVMM installation.
- 10. Click Install.
- 11. In the Installation page, after setup is complete, click the link in the Status window to check for the latest SCVMM updates.

The Connect to Server dialog box opens the first time you open the console.



12. In the Server name box, enter the name of the computer where the SCVMM server is installed, followed by a colon and the port that you want to use to connect the SCVMM Administrator Console to the SCVMM server and click Connect.

**Important:** The port settings that you assign for the SCVMM Administrator Console must identically match the port settings that you assigned in the SCVMM server.

- 13. Click Install.
- 14. In the Installation page, after setup is complete, select the start console checkbox and click close.
- 15. The Connect to Server dialog box opens, enter the FQDN to the SCVMM server, and click connect.
- 16. Enable PRO Scripts:
  - d. From within the VMM console click the PowerShell icon, launching a PowerShell console.
  - e. At the prompt, type A to select [A]lways to always trust remote signed scripts from this snap-in. If you do not see a prompt, the policy already allows PRO to run scripts.
- 17. Enable PRO Tips:
  - a. From the Administration pane, select General.
  - b. Right-click Pro Settings and select Modify.
  - c. Click Enable PTO Tips.
  - d. Click OK.
- 18. Configure System Center integration.
  - e. From within the VMM console, click Administration and then System Center.
  - f. Right-click Operations Manager Reporting URL, and select Modify.
  - g. Enter http://<SCOM Server>/ ReportServer and click OK.
  - h. Right-click Operations Manager Server and select Modify.
  - i. Enter the FQDN of the Operations Manager Server and click OK.
- 19. Close the VMM console.

## Install OnCommand Plugin 3.0 for Microsoft SCOM

- 1. In the SCOM Server, log in to Operations Manager using a domain account with permissions.
- 2. Download OnCommand Plugin 3.0 for Microsoft (x64) from the NOW site.
- 3. Launch the installer:
  - a. In the welcome screen, click Next.
  - b. Accept the EULA and click Next.
  - c. Enter a User Name, and Organization information, and click Next.
  - d. Click Next.
  - e. Select the following features under Products and click Next:
  - 1. SCOM Management Packs
    - a. Storage Monitoring with Reporting
    - b. Hyper-V Storage Monitoring with Reporting
    - c. MetroCluster™ Monitoring and Management (optional)
  - 2. Documentation



🛃 OnCommand Plug	in 3.0 for Micros	oft (x64) - Instal	Shield Wizard	X		
Feature Selection						
Select the features y	ou want to install.			NetApp		
Click on an icon in the li		Help				
	OnCommand Plug-i SCOM Management Storage Mor Repo V Repo V Repo V Repo V Repo V Repo V Repo	Feature Description The Data ONTAP MetroCluster management pack monitors configuration and availability of MetroCluster pairs. This MP helps optimize MetroCluster he This feature requires 1029KB on your hard drive. It has 1 of 1 subfeatures selected. The subfeatures require 25KB on your hard drive.				
Install to: C:\Program Files\NetApp\OnCommand\MS_Plugin\ 						
InstallShield						
	Disk <u>S</u> pace	< <u>B</u> ack	<u>N</u> ext >	Cancel		
OnCommand Plug-	in 3.0 for Microso	oft (x64) - Install	Shield Wizard	X		
Feature Selection Select the features y	ou want to install.			NetApp		
Click on an icon in the li	st below to select or	r deselect a feature		Help		
Hyper-V Storage Monitorin Reporting WetroCluster Monitoring ar MetroCluster Monit			Feature Descrip Collects Hyper-V ONTAP storage the Hyper-V hos	tion / VM and Data information from it.		
* X •	uires 0KB on					
Install to:				Chance		
The Later Later				Lnange		
InstallShield		[				
	Disk Space	< Back	Next >	Cancel		

- 4. Enter the credentials for the OpsMgr Administrator and click Next.
- 5. Click Install, then Finish.


- 6. Deploy the OnCommand Plugin 3.0 Agent.
  - a. Log in to each Hyper-V host and run the OnCommand Plugin installer.
  - b. From the welcome screen click Next.
  - c. Accept the EULA and click Next.
  - d. Click Next.
  - e. Select only the OnCommand Discovery Agent and Click Next.

🙀 OnCommand Plug-in 3.0 for Microsoft (x64) - Install	Shield Wizard	×
Feature Selection Select the features you want to install.		NetApp
Click on an icon in the list below to select or deselect a feature.		Help
NetApp OnCommand Plug-in 3.0 for Microsof   Image: SCOM Management Packs   Image: SCOM Management Pa	Feature Descript Collects Hyper-V ONTAP storage i the Hyper-V host This feature requ your hard drive.	ion VM and Data nformation from t. uires 95KB on
C:\Program Files\WetApp\OnCommand\MS_Plugin\		<u>C</u> hange
InstallShield Disk Space < Back	<u>N</u> ext >	Cancel

- 6. Click Install then Click Finish.
- 7. Repeat for each Hyper-V host.
- 7. Configure SNMP:
  - a. Open Server Manager. Select Configuration and select Services.
  - b. Scroll down to SNMP Service, right-click and select Properties.
  - c. Click the Security tab.
  - d. Under Accepted community names, click Add.
  - e. Under Community rights select READ ONLY, and enter a Community Name. This community name should be the SNMP v1 ro community name on the two storage controllers.
  - f. Under Accept SNMP packets from these hosts click Add.
  - g. Enter the hostname or IP Address for the NetApp controller.
  - h. Repeat for each controller in your environment, and then click OK.
- 8. Enable Data ONTAP discovery:
  - a. From the Operations Manager Console, click Authoring > Management Packs Objects > Rules.
  - b. In the top look for box enter Data ONTAP, and click Find Now.





- c. Scroll down to Type: Management Server.
- d. Right-click Data ONTAP: Discovery Rule and click Overrides > Override the Rule > For all objects of class: Management Server.
- e. Select the OverRide checkbox for the row where Parameter Name is Enabled.
- f. Change the Override Value selection to True, and then click OK.

verrid	e Propertie	25						>
Rule na Catego Overrid	ame: ny: es target:	Data ON Discover Class: Ma	TAP: Discovery Rule y anagement Server				Show Bule Proper	ties
Uverno	e-controlled	Parameters:	Paramatar Tuna	DefaultValue	Queride Value		Change Status	
*		Enabled	Boolean	False	True	False	[Added]	
	Г	Interval Seconds	Integer	86400	86400	86400	[No change]	
	Г	Sync Time	String	21:00	21:00	21:00	[No change]	
		TimeoutSeconds	Integer	3600	3600	3600	[No change]	
Details:								
Enabl The n Mana effecti	led ew custom o gement Pack ive value for	verride will be created i <. Click apply to view th this parameter.	n the 'Default ie new	cription			1	Edit
Mana	gement pa	ick						
Select	destination r	nanagement pack:						
Defau	ult Managem	ent Pack					<ul> <li>New.</li> </ul>	
н	lelp					ок 🛛 А	pply Can	icel
3						12		1

- g. Go to Type: Data ONTAP Virtualization: Management Server
- h. Right-click Data ONTAP PRO: Discovery Rule, and click Overrides > Override the Rule > For all objects of class: Data ONTAP Virtualization: Management Server.
- i. Select the Override checkbox for the row where Parameter Name is Enabled.
- j. Change the Override Value selection to True, and then click OK.



Rule na	ime:	Data ON	AP PRO: Discovery	Rule				
Ivenid	es target:	Class: Ga	tewau					
)venid	e-controlled	parameters:					Show Rule Propertie	S
	Override	Parameter Name	Parameter Type	Default Value	Override Value	Effective Value	Change Status	
		Arguments	String	\$MPEIement	\$MPElement\$	\$MPElement\$	[No change]	Т
•	2	Enabled	Boolean	False	True 💌	False	[Added]	T
		Interval Seconds	Integer	14400	14400	14400	[No change]	Т
		Sync Time	String	2.30	2:30	2:30	[No change]	Τ
		Timeout Seconds	Integer	900	900	900	[No change]	T
etails:	ed		Des	cription				đi
The n Mana effect	ew custom o gement Pack ve value for	verride will be created in "Click apply to view th this parameter.	n the 'Default e new	cription.				
	gement pa	ck						
Mana								
<b>1ana</b> Select	destination n	nanagement pack:						
<b>1ana</b> Select Defat	destination n It Manageme	nanagement pack: ent Pack					New	

- k. (Optional) If MetroCluster is a part of your installation, you can enable the Data ONTAP MetroCluster: Discovery Rule.
- 9. Discover NetApp controllers:
  - I. From the Operations Manager Console, select administration.
  - a. From the left pane click Discovery Wizard.
  - b. Select Network Device and click Next.
  - c. Enter an IP Range, and the community string entered on the storage systems and click Discover.
  - d. Select the checkboxes next to the IP addresses of the two storage controllers and click Next.
  - e. Click Finish.
- 10. Add NetApp controllers:
  - a. From the Operations Manager Console select Monitoring.
  - b. Expand Monitoring and select Discovered Inventory.
  - c. From the Action pane, select Change Target Type. (If there is no action pane, select View > Actions, or press Ctrl+T.)
  - d. In the resulting popup select Management Server and click OK.
  - e. From the Actions pane under Health Service Tasks, Select Data ONTAP: Run discovery task.
  - f. After the task is finished, click close.
- 11. Add controller credentials:
  - a. From the Operations Manager Console select Monitoring.
  - b. Expand Monitoring, and select Discovered Inventory.
  - c. From the Actions pane under Health Service Tasks, Select Data ONTAP: Manage Controller Credentials.





d. Enter the login credentials for each controller. Note that it may be necessary to use the Data ONTAP: Add Controller Task to add the controllers before putting in credentials.

### Install Cisco UCS MP for Microsoft SCOM

In the Operation Manager KMS Server, log in to Operations Manager using a domain account with permissions.

To install the management pack, follow these steps:

1. Start Cisco.UCS.MP.Install.msi and click Next.

CISCO UCS Management Pack			_ 🗆 ×
Welcome to the CISCO Setup Wizard	UCS Man	agement Pa	
The installer will guide you through the st your computer.	eps required to i	nstall CISCO UCS M	anagement Pack on
WARNING: This computer program is pro Unauthorized duplication or distribution o or criminal penalties, and will be prosecul	otected by copy if this program, o ted to the maxim	right law and internal r any portion of it, ma um extent possible u	tional treaties. ay result in severe civil nder the law.

2. Enter a server name in the Server Name field. Click Next.





🖁 CISCO UCS Management Pack			
Connection to Microso Manager 2007 R2	oft System C	enter Operatio	
Microsoft System Center Operations I	Manager 2007 R2 wł	nere the Management Pa	ck will be
-			
Server name:			
VM11.VMM-LAB.LOCAL			27
	Cancel	K Back	<u>N</u> ext>
	-	-1. (*	

3. Select the Enable Virtualization checkbox if you want to support the discovery and monitoring of hypervisors and virtual machines. Click Next.



🕞 CISCO UCS Management Pack	
Virtualization	
Select this option if you want CISCO UCS Management Port to hypervisors and virtual machines. System Center Virtual Mach (version 2.0.3451.0) is required. Enable Virtualization	o support discovery and monitoring of ine Manager 2008 Management Pack
Cancel	<back next=""></back>

Enabling virtualization support requires that System Center Virtual Machine Manager (SCVMM) 2008 (version 2.0.3451.0) be installed, prior to the installation of the Cisco UCS Manager Management Pack. Prior to installation, the management packs specific to SCVMM 2008 must be installed in the Operations Manager console. Consult the SCVMM and SCOM R2 documentation for any installation details.

System Center Virtual Machine Manager 2008 Management Pack version 2.0.3451.0 is required for SCOM 2007 R2.

4. Enter a path to folder where the management pack is installed in the Folder field.





CISCO UCS Management Pack	
Select Installation Folder	
The installer will install CISCO UCS Management Pack to the following	folder.
To install in this folder, click "Next". To install to a different folder, enter	it below or click "Browse".
Folder:	
C:\Program Files\CISCO\CISCO UCS Management Pack\	Browse
	Disk Cost
C:\Program Files\CISCO\CISCO UCS Management Pack\	Browse Disk Cost o uses this computer:
<ul> <li><u>E</u>veryone</li> <li>Just me</li> </ul>	

5. Select the Everyone or Just Me radio button to install the management pack for yourself or for anyone else who uses it and click Next.





🕞 CISCO UCS Management Pack	
Confirm Installation	
The installer is ready to install CISCO UCS Management Pack on your computer. Click "Next" to start the installation.	
Cancel < Back	Next>

- 6. Click Next to confirm the installation and then click Close.
- 7. Perform the following steps if during the installation an error occurred and you were asked to import an appropriate management pack independently:
  - a. Click Go on the top tool bar in System Center Operations Manager and then click Administration on the drop-down menu.
  - b. Right-click the Management Packs node, and then select Import Management Packs on the dropdown menu.
  - c. The Import Management Packs wizard appears.
  - d. Click Add, and then select Add from Disk.
  - e. Click No in Online Catalog Connection.
  - f. Navigate to the folder selected during installation process in the Select Management Packs to Import dialog box.
  - g. Click Open, and then click Install.
  - h. Click Close when the management pack is imported.

#### Assigning an IP Address to the Management Port

To assign an IP address to the management port, follow these steps:

- 1. Click Go on the top tool bar in the SCOM and then select Authoring from the drop-down menu.
- 2. Expand the Management Pack Templates node.
- 3. Select Cisco UCS Management Port and then click the Add Monitoring Wizard tab under the top tool bar.



- a. The Add Monitoring Wizard appears and Cisco UCS Management Port is selected in the Select the Monitoring Type area.
- 4. Use the wizard to add a management port IP address and port number:
  - a. Click Next.
  - b. Enter an IP address and port number in the URL field and click Next.
  - c. Enter a name in the Name field.
  - d. When you enter a name, it appears in the Create Destination Management Pack field. Alternatively, you can select the Use Existing Management Pack or Create New checkbox to create a management pack or browse for a preexisting management pack.
  - e. (Optional) Enter a description in the Description field and click Next.
  - f. (Optional) Select the Virtualization checkbox, if you want to monitor any virtual machines. Click Next.
  - g. Use the Summary page to make sure that you have the proper configuration. Click Create.

An IP address is now assigned to the management port.

#### **Creating an Account for Administrators**

- 1. To create an account for administrators, follow these steps:
- 2. Click Go on the top tool bar in the SCOM, and then select Administration from the drop-down menu.
- 3. Right-click Accounts, and then select Create Run as Accounts from the drop-down menu.

The Create Run as Accounts wizard appears.

- **Note:** By using the Run as Accounts option, you create an account for an administrator to log in to the Cisco UCS system from SCOM to retrieve required information. The administrator account details must be available in the Cisco UCS system to authenticate the user.
- 4. Use the wizard to create an account:
  - a. Read the introduction, and then click Next.
  - b. Select Simple Authentication from the Run as Account Type drop-down list.
  - c. Enter a display name in the Display Name field.
  - d. (Optional) Enter a description in the Description field, and then click Next.
  - e. Enter a user name in the User Name field.
  - f. Enter a password in the Password field, and then reenter the same password in the Confirm Password field.
  - g. Select the Less Secure radio button and click Create.

An account for the administrator is now created.

#### Adding an Account to a Profile

To add an account to a profile, follow these steps:

- 1. Click Go on the top tool bar in the SCOM and then select Administration from the drop-down menu.
- 2. Click Profiles.
- 3. Right-click the appropriate account and then select Properties from the drop-down menu. The Run as Profile wizard appears.
- 4. Use the wizard to create an account:
  - a. Click Run as Accounts.



- b. Click the Add icon.
- c. Select an account from the Run as Account drop-down list.
- d. Click either the All Targeted Objects or the A Selected Class radio button, and then click OK.

The account is now added to the profile.

#### Adjusting the Discovery Interval

To adjust the discovery interval, follow these steps:

- 1. Click Go on the top tool bar in the SCOM, and then select Authoring from the drop-down menu.
- 2. Click the Objects Discoveries node, and then click Scope.
- 3. Click Clear All, and then select the View all Targets radio button.
- 4. Enter Chassis in the Look For field.
- 5. Select the Chassis checkbox and click OK.
- **Note:** The Management Pack column value has to match the name entered while processing the management pack template.
- 6. Double-click the Chassis Discovery row.



- 7. Click the Overrides tab and click Override.
- 8. Select For all Objects of Class: Management Port from the drop-down menu.



thorng	Object Discovering				Action
2 Adhoring	Panagement part abouts an	this supplify Gauss		Grange Stope	· · · · · · · · · · · · · · · · · · ·
Hanapowet Path Teraheter	- Land for-	- Drafflew George			1 de Pagerie
CIE DI DI DI SI SWARD	See	Tage	Playage and Fast	Tubble to be all	The 14 2000
Prismus Monitority: 109 And	- Incontrol In Children	A Decemp Properties		6	The Orientes +
- 1 Unit-Aliman Log/Ter	A Creation Decision	I wanted the set of th	(Translet)	110	X Dates
Called Areas Services		a) anonexercanae) condrama ( performan	Annual and A	1	Destartor
ally Whichon Spirited	2	write as and to note the decreas contraction in	to can overable the conteputies by		Strebate Santar Canadam
10 Debibuted applications					Harago (Hib
The Management Face Objects		Should like terring it with the same b. A with the Service	and the Town have		Soleni Carter Operation Menager Ciribre
attributes		instante Diserte des discourses for all inflations instantes			
Coard Discovered					1
Re-Converties		E-en.			1
2 Rocks Good Tracting	177	and the second s			1
Taske	0	weather over an access presented set of this discussory then	up route.		1
All views	0	innerie: Charge Needfald and e fors ME in ME in all	Palme measures		1
					1
	4		Contract of Contra		1
		APPROPRIATE AND DESCRIPTION OF			1
		and a second sec	Million and Million Commission		1
	17	In the same a particular statement of the same			1
	- 44	servers. From Pol. Manual Pol. documents the documentary	MM (		1
	1.000	The community			100 C
tentiong Wourd -	-				
Serie	Statistics and the other				
	Shareh Dec				1
the second se					
Automa	Hasaperert P				
	18 Tape		which is a second second	11	
Papernel	insetty		II. Epid	الر الم	
A dela del del la Ciner	Created 1000	Contra preserver			
Contraction of the second	Scape collegisters, reliabilitad	Non, and then address			
Contraction of the local division of the loc	the Paper Onester	*			

- 9. Select the IntervalSeconds checkbox.
- 10. Change the value in the Override Value column to another value, and click OK.
- 11. Click OK again.

ri|iii|ii cisco

The discovery interval is now adjusted.

**Note:** You must perform these steps for all classes of objects, such as Management Port, Chassis, Server, Organization, and Associated Service Profile. To change the intervals for Rules and Monitors perform the steps, but start from the node Rules or Monitors.

### **Opalis Integration Server**

This section provides a step-by-step guide for installing Opalis Integration Server. Opalis is an optional component that provides runbook automation. NetApp integration is provided via OnCommand plug-in for Microsoft environments. Note that these instructions assume a new installation of Opalis Integration Server 6.3. Since Opalis 6.3 is a patch on top of 6.2.2, the instructions below will walk through installing 6.2.2 and will apply the 6.3 patch on top of the base 6.2.2 install. See Opalis documentation for other install scenarios.

### Installing Opalis 6.2.2 SP1

Before you begin create a service account for Opalis. It is recommended that this be a dedicated domain account with a nonexpiring password. Add this account to the local administrators group before installing Opalis. Also, this account will need access to the SQL Server created in the SQL Server section so you will need to add this account to the SQL Server security group ("Operations Manager SQL Server Admins") created in that section.

1. Run opalis\_full.exe or other source media to begin installation process.





- 2. Agree to license terms and provide an extract location.
- 3. Before installing the 6.3 patch, you must install Opalis 6.2.2. Open the Opalis 6.2.2.zip folder and within that folder, open the Opalis Integration Server 6.22\_6.2.2.5229.zip folder.

Edit View Favorites ]	ools	Help							0
Back 🔹 🕥 🔹 🛷 🔎 Sear	ch 🌾	Folders							
	II~1.№	45B\LOCALS~1\Temp\Ten	nporary Directory	1 for Opalis 6	.2.2.zip\C	palis Integ	gration :	Server 6.22_6.2.2.5229.zip	>
	- 10	Name *	Туре	Packed	Has	Size	R	Date	a
Folder Tasks	*	3rdparty	File Folder	0 KB		0 KB	0%	11/26/2009 12:45 PM	
		Client	File Folder	0 KB		0 KB	0%	11/26/2009 12:45 PM	
Extract all files		Documentation	File Folder	0 KB		0 KB	0%	11/26/2009 12:45 PM	
		ManagementServer	File Folder	0 KB		0 KB	0%	11/26/2009 12:45 PM	
out pl	~	OperatorConsole	File Folder	0 KB		0 KB	0%	11/26/2009 12:45 PM	
Uther Places	^	Reports	File Folder	0 KB		0 KB	0%	11/26/2009 12:46 PM	
Temporary Directory 1 for		C Support	File Folder	0 KB		0 KB	0%	11/26/2009 12:46 PM	
Opalis 6.2.2.zip		Autorun.ico	Icon	1 KB	No	8 KB	94%	9/24/2009 12:29 PM	
My Documents		Autorun.inf	Setup Inform	1 KB	No	1 KB	5%	1/22/2008 11:53 AM	
My Network Places		Setup.exe	Application	170 KB	No	400 KB	58%	11/11/2009 12:13 PM	

- 4. Extract this zip file to a local directory.
- 5. Right-click Install Opalis Integration Server and then click Run as administrator.
- 6. Select Install Opalis Integration Server, click "Step 1. Install Management Server."
- 7. Click Next on the first screen. Accept the license and click Next.
- 8. Enter user information and click Next. Accept the default installation folder and click Next.
- 9. Enter the service account. As noted previously, it is recommended that this be a domain account with a non-expiring password.

🙀 Opalis Integrati	on Server v6.2.2 - Manag	gement Service Set	up	
Logon Informatio	n			1. 🔶
The following log Management Ser	on information is used by the vice.	Opalis Integration Serve	er C	palis
Specify a user Service. Use names must b	account to be used by the 0 the Browse button to choose a in the format of DOMAIN\U	palis Integration Server users from your networl serName.	Manager « For don	nent nains, user
User Name:	mydomain\OpalisServiceA	eet		Browse
Password:	*****			
Wise Installation Wiza	d®			
		< <u>B</u> ack <u>N</u>	ext >	Cancel

- 10. Click Next to begin the installation.
- 11. Click Finish when the installation is complete.
- 12. Click Step 2: Configure the Database.
- 13. Accept the default database type, SQL Server. Click Next.
- 14. Enter the database details created in the SQL Server installation section of this document. Click Next.
- 15. Select Create New Database and accept the default database name. Click Finish.
- 16. Run Step 3: Import a license and click Import.
- 17. Open your .lic file for the Opalis base pack (5-OISBP\_25.lic) and enter your license key.





Import Licen	se 🗙
<u>K</u> ey:	{B3DBAA89-0715-48E8-95AA-6DAF0C689944}
License file:	\Opalis License\Licenses\Licenses\5-OISBP_25.lic
	OK Cancel

18. Repeat this process for any additional license files.

### Installing Opalis 6.3 Patch

- Open the Management Server installation folder. By default, this is located in System Drive: Program Files\Opalis Software\Opalis Integration Server\Management Service. Browse to the Components\Objects folder.
- Copy the OpalisIntegrationServer\_FoundationObjects.msi file provided in the Opalis 6.3 zip file to the System Drive:\Program Files (x86)\Opalis Software\Opalis Integration Server\Management Service\Components\Objects directory. Replace the existing file.
- 3. Run the OpalisIntegrationServer\_ManagementService\_630\_PATCH.msp installer. Do not change any of the default values.
- 4. Deploy your Opalis Clients via the deployment manager.
- 5. After you deploy the clients from the Deployment Manager, copy the OpalisIntegrationServer\_Client\_630\_PATCH.msp file included in the 6.3 release to each client.
- 6. Run the OpalisIntegrationServer\_Client\_630\_PATCH.msp installer. Do not change any of the default values.



### Appendix

### Alternate Cisco Nexus 5548 Deployment Procedure: Part 2 for FCoE

These steps provide details for completing the configuration of the Nexus infrastructure for the FlexPod environment.

#### Figure 3 Nexus Infrastructure for the FlexPod Environment



#### Create VSANs, Assign FC Ports, Turn on FC Ports

These steps provide details for configuring VSANs, assigning FC ports and enabling FC ports.

**Note:** This procedure sets up FCoE connections between the Nexus 5548s and the NetApp Storage Systems. If you want to use FCoE connections between the Nexus 5548s and the NetApp Storage Systems using the NetApp Unified Target Adapter (UTA). Use the Alternate Cisco Nexus 5548 Deployment Procedure: Part 2 in the Appendix.

#### Cisco Nexus 5548 A

- 1. From the global configuration mode, type vlan <Fabric A FCOE VLAN ID>.
- 2. Type name FCoE\_Fabric\_A.
- 3. Type fcoe vsan <VSAN A ID>.



- 4. Type exit.
- 5. Type interface poll.
- 6. Type switchport trunk allowed vlan add <Fabric A FCoE VLAN ID>.
- 7. Type exit.
- 8. Type interface vfc11.
- 9. Type bind interface poll.
- 10. Type no shutdown.
- 11. Type exit.
- 12. Type interface pol2.
- 13. Type switchport trunk allowed vlan add <Fabric A FCoE VLAN ID>.
- 14. Type exit.
- 15. Type interface vfc12.
- 16. Type bind interface pol2.
- 17. Type no shutdown.
- 18. Type exit.
- 19. Type interface san-port-channel 1.
- 20. Type channel mode active.
- 21. Type exit.
- 22. Type channel mode active.
- 23. Type vsan database.
- 24. Type vsan <VSAN A ID> name Fabric\_A.
- 25. Type vsan <VSAN A ID> interface fc1/31-32.
- 26. Type vsan <VSAN A ID> interface san-port-channel 1.
- 27. Type vsan <VSAN A ID> interface vfc11.
- 28. Type vsan <VSAN A ID> interface vfc12.
- 29. Type exit.
- **30**. Type interface fc1/31-32.
- **31.** Type channel-group 1 force.
- 32. Type no shutdown.
- 33. Type exit.
- 34. Type show int san-port-channel 1 to confirm connectivity.
- **35.** Type interface fc1/31.
- 36. Type switchport description <UCSM A:fc1/31>.
- 37. Type exit.
- **38.** Type interface fc1/32.
- **39. Type** switchport description <UCSM A:fc1/32>.
- 40. Type exit.



#### Cisco Nexus 5548 B

1. From the global configuration mode, type vlan <Fabric B FCoE VLAN ID>. 2. Type name FCoE Fabric B. 3. Type fcoe vsan <VSAN B ID>. 4. Type exit. 5. Type interface poll. 6. Type switchport trunk allowed vlan add <Fabric B FCoE VLAN ID>. 7. Type exit. 8. Type interface vfc11. 9. Type bind interface poll. 10. Type no shutdown. 11. Type exit. 12. Type interface po12. 13. Type switchport trunk allowed vlan add <Fabric B FCoE VLAN ID>. 14. Type exit. 15. Type interface vfc12. 16. Type bind interface po12. 17. Type no shutdown. 18. Type exit. 19. Type interface san-port-channel 2. 20. Type channel mode active. 21. Type exit. 22. Type vsan database. 23. Type vsan <VSAN B ID> name Fabric B. 24. Type vsan <VSAN B ID> interface fc1/31-32. 25. Type vsan <VSAN B ID> interface san-port-channel 2. 26. Type vsan <VSAN A ID> interface vfc11. 27. Type vsan <VSAN A ID> interface vfc12. 28. Type exit. 29. Type interface fc1/31-32. **30.** Type channel-group 2 force. 31. Type no shutdown. 32. Type exit. 33. Type show int san-port-channel 2 to confirm connectivity 34. Type interface fc1/31. 35. Type switchport description <UCSM B:fc1/31>. 36. Type exit.

# cisco



- **37.** Type interface fc1/32.
- **38**. **Type** switchport description <UCSM B:fc1/32>.
- 39. Type exit.

#### **Create Device Aliases and Create Zones**

These steps provide details for configuring device aliases and zones for the primary boot path. Instructions are given for all target ports, however, the redundant path is enabled following operating system installation..

#### Cisco Nexus 5548 A

- 1. From the global configuration mode, type device-alias database.
- 2. Type device-alias name VM-Host-Infra-01\_A pwwn <Fabric-A WWPN>.
- 3. Type device-alias name VM-Host-Infra-02 A pwwn <Fabric-A WWPN>.
- 4. Type device-alias name controller A 2a pwwn <Controller A 2a WWPN>.
- 5. Type device-alias name controller B 2a pwwn <Controller B 2a WWPN>.

Get this information from the table in section Gather Necessary Information.

- 6. After all of the necessary device-alias are created, type exit.
- 7. Type device-alias commit.
- 8. Create the zone for each service profile.
  - a. Type zone name VM-Host-Infra-01 A vsan <Fabric A VSAN ID>.
  - b. Type member device-alias VM-Host-Infra-01 A.
  - c. Type member device-alias controller\_A\_2a.
  - d. Type exit.
- 9. After the zone for the primary path of the first Cisco UCS service profiles has been created, create a zoneset to organize and manage them.

#### 10. Create the zoneset and add the necessary members.

- a. Type zoneset name flexpod vsan <Fabric A VSAN ID>.
- b. Type member VM-Host-Infra-01 A.
- c. Type exit.

11. Activate the zoneset.

- a. Type zoneset activate name flexpod vsan < Fabric A VSAN ID>.
- b. Type exit.
- 12. Type copy run start.

#### Cisco Nexus 5548 B

- 1. From the global configuration mode, type device-alias database.
- 2. Type device-alias name VM-Host-Infra-01\_B pwwn <Fabric-B WWPN>.
- 3. Type device-alias name VM-Host-Infra-02 B pwwn <Fabric-B WWPN>.
- 4. Type device-alias name controller A\_2b pwwn <Controller A 0d WWPN>.



5. Type device-alias name controller\_B\_2b pwwn <Controller B 0d WWPN>. Get this information from the tables in the section Gather Necessary Information.

- 6. After all of the necessary device-alias are created, type exit.
- 7. Type device-alias commit.
- 8. Create the zones for each service profile.
  - a. Type zone name VM-Host-Infra-02 B vsan <Fabric B VSAN ID>.
  - b. Type member device-alias VM-Host-Infra-02 B.
  - c. Type member device-alias controller\_B\_0d.
- 6. Type exit.
- 9. After all of the zones for the Cisco UCS service profiles have been created, create a zoneset to organize and manage them.
- 10. Create the zoneset and add the necessary members.
  - a. Type zoneset name flexpod vsan <Fabric B VSAN ID>.
  - b. Type member VM-Host-Infra-02 B.
  - c. Type exit.
- 11. Activate the zoneset.
  - a. Type zoneset activate name flexpod vsan <Fabric B VSAN ID>.
  - b. Type exit.
  - 20. Type copy run start.
- 12. Return to the section NetApp FAS3240A Deployment Procedure: Part 2.

### Alternate Create Zones for Redundant Paths for FCoE

These steps provide details for configuring zones for the secondary boot path for each service profile.

#### Cisco Nexus 5548 A

- 1. From the global configuration mode, create the zones for the redundant path for each service profile.
  - a. Type zone name VM-Host-Infra-01 A vsan <Fabric A VSAN ID>.
    - 1. Type member device-alias controller B 2a.
    - 2. Type exit.
    - 3. Type zone name VM-Host-Infra-02\_A vsan <Fabric A VSAN ID>.
    - 4. Type member device-alias VM-Host-Infra-02\_A.
    - 5. Type member device-alias controller\_B\_2a.
    - 6. Type member device-alias controller\_A\_2a.
    - 7. Type exit.
- 2. Modify the zoneset and add the necessary members.
  - a. Type zoneset name flexpod vsan <Fabric A VSAN ID>.
- 3. Type member VM-Host-Infra-02.
- 4. Type exit.
- 5. Activate the zoneset.
  - a. Type zoneset activate name flexpod vsan <Fabric A VSAN ID>.



- 6. Type exit.
- 7. Type copy run start.

#### Cisco Nexus 5548 B

- 1. From the global configuration mode, create the zones for the redundant path for each service profile.
  - a. Type zone name VM-Host-Infra-01\_B vsan <Fabric B VSAN ID>.
  - b. Type member device-alias VM-Host-Infra-01\_B.
  - c. Type member device-alias controller\_A\_2b.
  - d. Type member device-alias controller\_B\_2b.
  - e. Type exit.
  - f. Type zone name VM-Host-Infra-02 B vsan <Fabric B VSAN ID>.
  - g. Type member device-alias controller\_A\_2b.
  - h. Type exit.
- 2. Modify the zoneset and add the necessary members.
  - a. Type zoneset name flexpod vsan <Fabric B VSAN ID>.
  - b. Type member VM-Host-Infra-01 B.
  - c. Type exit.
- 3. Activate the zoneset.
  - a. Type zoneset activate name flexpod vsan <Fabric B VSAN ID>.
  - b. Type exit.
- 4. Type copy run start.

Note: Return to Clone the Windows Server 2008 R2 SP1 Installation section.

### **Cisco Nexus Configurations**

#### Nexus A (sample running config)

ice5548-1# show run !Command: show running-config !Time: Thu Jan 26 22:39:15 2012 version 5.0(3)N2(2a) feature fcoe feature npiv feature fport-channel-trunk no feature telnet no telnet server enable cfs eth distribute feature lacp feature vpc feature lldp username admin password 5 \$1\$vhyEnoq8\$fEeCFXDyQDTPDBltqDhU0. role network-admin ip domain-lookup hostname ice5548-1 system jumbomtu 9000 logging event link-status default



class-map type qos class-fcoe class-map type queuing class-fcoe match qos-group 1 class-map type queuing class-all-flood match gos-group 2 class-map type queuing class-ip-multicast match gos-group 2 class-map type network-gos class-fcoe match qos-group 1 class-map type network-gos class-all-flood match qos-group 2 class-map type network-gos class-ip-multicast match qos-group 2 policy-map type network-gos jumbo class type network-gos class-fcoe pause no-drop mtu 2158 class type network-qos class-default mtu 9000 multicast-optimize system gos service-policy type network-gos jumbo slot 1 port 29-32 type fc snmp-server user admin network-admin auth md5 0x2e8af112d36e9af1466f4e4db0ce36a3 priv 0x2e8af112d36e9af1466f4e4db0ce36a3 localizedkey snmp-server enable traps entity fru ntp server 10.61.185.11 use-vrf management vrf context management ip route 0.0.0.0/0 10.61.185.1 vlan 1 vlan 2 name Native-VLAN vlan 186 name MGMT-VLAN vlan 3101 name CSV-VLAN vlan 3102 name iSCSI-VLAN-A vlan 3103 name Live-Migration-VLAN vlan 3104 name App-Cluster-Comm-VLAN vlan 3105 name VM-Data-VLAN vlan 3106 name iSCSI-VLAN-B spanning-tree port type edge bpduguard default spanning-tree port type edge bpdufilter default spanning-tree port type network default vpc domain 23 role priority 10 peer-keepalive destination 10.61.185.70 source 10.61.185.69



vsan database vsan 101 name "Fabric\_A" device-alias database device-alias name ice3270-1a\_0c pwwn 50:0a:09:83:8d:7d:92:bc device-alias name ice3270-1b Oc pwwn 50:0a:09:83:9d:7d:92:bc device-alias name ice3270-1a 0c1 A pwwn 20:00:00:25:b5:00:0a:0f device-alias name ice3270-1b\_0d1\_A pwwn 20:00:00:25:b5:00:0a:1f device-alias commit fcdomain fcid database vsan 101 wwn 24:01:54:7f:ee:23:52:40 fcid 0x550000 dynamic vsan 101 wwn 50:0a:09:83:8d:7d:92:bc fcid 0x550001 dynamic Į. [ice3270-1a\_0c] vsan 101 wwn 50:0a:09:83:9d:7d:92:bc fcid 0x550002 dynamic ! [ice3270-1b\_0c] vsan 101 wwn 20:00:00:25:b5:00:0a:0f fcid 0x550003 dynamic [ice3270-1a 0c1 A] 1 vsan 101 wwn 20:00:00:25:b5:00:0a:1f fcid 0x550004 dynamic [ice3270-1b 0d1 A] 1 interface san-port-channel 1 channel mode active interface port-channel10 description vPC peer-link switchport mode trunk vpc peer-link switchport trunk native vlan 2 switchport trunk allowed vlan 186,3101-3106 spanning-tree port type network interface port-channel11 description ice3270-1a switchport mode trunk vpc 11 switchport trunk native vlan 186 switchport trunk allowed vlan 186,3101-3102,3106 spanning-tree port type edge trunk interface port-channel12 description ice3270-1b switchport mode trunk vpc 12 switchport trunk native vlan 186 switchport trunk allowed vlan 186,3101-3102,3106 spanning-tree port type edge trunk interface port-channel13 description iceucsm-2a switchport mode trunk vpc 13 switchport trunk native vlan 2 switchport trunk allowed vlan 186,3101-3106 spanning-tree port type edge trunk



interface port-channel14 description iceucsm-2b switchport mode trunk vpc 14 switchport trunk native vlan 2 switchport trunk allowed vlan 186,3101-3106 spanning-tree port type edge trunk

interface port-channel20 description icecore switchport mode trunk vpc 20 switchport trunk native vlan 2 switchport trunk allowed vlan 186 spanning-tree port type network vsan database vsan 101 interface san-port-channel 1 vsan 101 interface fc1/29 vsan 101 interface fc1/30

interface fc1/29 no shutdown

interface fc1/30 no shutdown

interface fc1/31 channel-group 1 force no shutdown

interface fc1/32 channel-group 1 force no shutdown

interface Ethernet1/1 description ice3270-1a:e2a switchport mode trunk switchport trunk native vlan 186 switchport trunk allowed vlan 186,3101-3102,3106 channel-group 11 mode active

interface Ethernet1/2 description ice3270-1b:e2a switchport mode trunk switchport trunk native vlan 186 switchport trunk allowed vlan 186,3101-3102,3106 channel-group 12 mode active

interface Ethernet1/3 description iceucsm-2a:Eth1/19 switchport mode trunk switchport trunk native vlan 2



switchport trunk allowed vlan 186,3101-3106 channel-group 13 mode active

interface Ethernet1/4 description iceucsm-2b:Eth1/19 switchport mode trunk switchport trunk native vlan 2 switchport trunk allowed vlan 186,3101-3106 channel-group 14 mode active

interface Ethernet1/5 description ice5548-2:Eth1/5 switchport mode trunk switchport trunk native vlan 2 switchport trunk allowed vlan 186,3101-3106 channel-group 10 mode active

interface Ethernet1/6 description ice5548-2:Eth1/6 switchport mode trunk switchport trunk native vlan 2 switchport trunk allowed vlan 186,3101-3106 channel-group 10 mode active

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 description icecore:Eth1/21 switchport mode trunk



switchport trunk native vlan 2 switchport trunk allowed vlan 186 channel-group 20 mode active

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28

interface mgmt0 ip address 10.61.185.69/24 line console line vty boot kickstart bootflash:/n5000-uk9-kickstart.5.0.3.N2.2a.bin boot system bootflash:/n5000-uk9.5.0.3.N2.2a.bin interface fc1/31 interface fc1/32 interface fc1/29 interface fc1/30 interface fc1/31 interface fc1/32 **!Full Zone Database Section for vsan 101** zone name ice3270-1a\_0c1\_A vsan 101 member pwwn 20:00:00:25:b5:00:0a:0f [ice3270-1a\_0c1\_A] 1 member pwwn 50:0a:09:83:8d:7d:92:bc ! [ice3270-1a\_0c] member pwwn 50:0a:09:83:9d:7d:92:bc ! [ice3270-1b\_0c] zone name ice3270-1b\_0d1\_A vsan 101 member pwwn 20:00:00:25:b5:00:0a:1f ! [ice3270-1b\_0d1\_A] member pwwn 50:0a:09:83:8d:7d:92:bc [ice3270-1a\_0c] ! member pwwn 50:0a:09:83:9d:7d:92:bc

[ice3270-1b\_0c]

zoneset name flexpod vsan 101 member ice3270-1a\_0c1\_A member ice3270-1b\_0d1\_A





zoneset activate name flexpod vsan 101



#### Nexus B (sample running config)

ice5548-2# show run

!Command: show running-config !Time: Thu Jan 26 22:43:40 2012

version 5.0(3)N2(2a) feature fcoe feature npiv feature fport-channel-trunk no feature telnet no telnet server enable cfs eth distribute feature lacp feature vpc feature lldp username admin password 5 \$1\$QwOvH6l4\$uemTijt9Bz9c2SSA1DPOX. role network-admin ip domain-lookup hostname ice5548-2 system jumbomtu 9000 logging event link-status default class-map type qos class-fcoe class-map type queuing class-fcoe match gos-group 1 class-map type queuing class-all-flood match gos-group 2 class-map type queuing class-ip-multicast match qos-group 2 class-map type network-qos class-fcoe match qos-group 1 class-map type network-gos class-all-flood match gos-group 2 class-map type network-gos class-ip-multicast match qos-group 2 policy-map type network-gos jumbo class type network-gos class-fcoe pause no-drop mtu 2158 class type network-qos class-default mtu 9000 multicast-optimize system gos service-policy type network-qos jumbo slot 1 port 29-32 type fc snmp-server user admin network-admin auth md5 0xe481d1d2fee4aaa498237df1852270e8 priv 0xe481d1d2fee4aaa498237df1852270e8 localizedkey snmp-server enable traps entity fru ntp server 10.61.185.11 use-vrf management vrf context management ip route 0.0.0.0/0 10.61.185.1 vlan 1 vlan 2



name Native-VLAN vlan 186 name MGMT-VLAN vlan 3101 name CSV-VLAN vlan 3102 name iSCSI-VLAN-A vlan 3103 name Live-Migration-VLAN vlan 3104 name App-Cluster-Comm-VLAN vlan 3105 name VM-Data-VLAN vlan 3106 name iSCSI-VLAN-B spanning-tree port type edge bpduguard default spanning-tree port type edge bpdufilter default spanning-tree port type network default vpc domain 23 role priority 20 peer-keepalive destination 10.61.185.69 source 10.61.185.70 vsan database vsan 102 name "Fabric\_B" device-alias database device-alias name ice3270-1a\_0d pwwn 50:0a:09:84:8d:7d:92:bc device-alias name ice3270-1b\_0d pwwn 50:0a:09:84:9d:7d:92:bc device-alias name ice3270-1a 0c1 B pwwn 20:00:00:25:b5:00:0b:0f device-alias name ice3270-1b 0d1 B pwwn 20:00:00:25:b5:00:0b:1f device-alias commit fcdomain fcid database vsan 102 wwn 24:02:54:7f:ee:23:8b:00 fcid 0x3f0000 dynamic vsan 102 wwn 50:0a:09:84:9d:7d:92:bc fcid 0x3f0001 dynamic ! [ice3270-1b\_0d] vsan 102 wwn 50:0a:09:84:8d:7d:92:bc fcid 0x3f0002 dynamic [ice3270-1a 0d] 1 vsan 102 wwn 20:00:00:25:b5:00:0b:0f fcid 0x3f0003 dynamic 1 [ice3270-1a 0c1 B] vsan 102 wwn 20:00:00:25:b5:00:0b:1f fcid 0x3f0004 dynamic 1 [ice3270-1b\_0d1\_B] interface san-port-channel 2 channel mode active interface port-channel10 description vPC peer-link switchport mode trunk vpc peer-link switchport trunk native vlan 2 switchport trunk allowed vlan 186,3101-3106

```
spanning-tree port type network
```



interface port-channel11 description ice3270-1a switchport mode trunk vpc 11 switchport trunk native vlan 186 switchport trunk allowed vlan 186,3101-3102,3106 spanning-tree port type edge trunk

interface port-channel12 description ice3270-1b switchport mode trunk vpc 12 switchport trunk native vlan 186 switchport trunk allowed vlan 186,3101-3102,3106 spanning-tree port type edge trunk

interface port-channel13 description iceucsm-2a switchport mode trunk vpc 13 switchport trunk native vlan 2 switchport trunk allowed vlan 186,3101-3106 spanning-tree port type edge trunk

interface port-channel14 description iceucsm-2b switchport mode trunk vpc 14 switchport trunk native vlan 2 switchport trunk allowed vlan 186,3101-3106 spanning-tree port type edge trunk

interface port-channel20 description icecore switchport mode trunk vpc 20 switchport trunk native vlan 2 switchport trunk allowed vlan 186 spanning-tree port type network vsan database vsan 102 interface san-port-channel 2 vsan 102 interface fc1/29 vsan 102 interface fc1/30

interface fc1/29 no shutdown

interface fc1/30 no shutdown

interface fc1/31 channel-group 2 force



#### no shutdown

interface fc1/32 channel-group 2 force no shutdown

interface Ethernet1/1 description ice3270-1a:e2b switchport mode trunk switchport trunk native vlan 186 switchport trunk allowed vlan 186,3101-3102,3106 channel-group 11 mode active

interface Ethernet1/2 description ice3270-1b:e2b switchport mode trunk switchport trunk native vlan 186 switchport trunk allowed vlan 186,3101-3102,3106 channel-group 12 mode active

interface Ethernet1/3 description iceucsm-2a:Eth1/20 switchport mode trunk switchport trunk native vlan 2 switchport trunk allowed vlan 186,3101-3106 channel-group 13 mode active

interface Ethernet1/4 description iceucsm-2b:Eth1/20 switchport mode trunk switchport trunk native vlan 2 switchport trunk allowed vlan 186,3101-3106 channel-group 14 mode active

interface Ethernet1/5 description ice5548-1:Eth1/5 switchport mode trunk switchport trunk native vlan 2 switchport trunk allowed vlan 186,3101-3106 channel-group 10 mode active

interface Ethernet1/6 description ice5548-1:Eth1/6 switchport mode trunk switchport trunk native vlan 2 switchport trunk allowed vlan 186,3101-3106 channel-group 10 mode active

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 description icecore:Eth1/22 switchport mode trunk switchport trunk native vlan 2 switchport trunk allowed vlan 186 channel-group 20 mode active
- interface Ethernet1/21
- interface Ethernet1/22
- interface Ethernet1/23
- interface Ethernet1/24
- interface Ethernet1/25
- interface Ethernet1/26
- interface Ethernet1/27
- interface Ethernet1/28
- interface mgmt0 ip address 10.61.185.70/24 line console line vty boot kickstart bootflash:/n5000-uk9-kickstart.5.0.3.N2.2a.bin boot system bootflash:/n5000-uk9.5.0.3.N2.2a.bin interface fc1/31 interface fc1/32 interface fc1/29



interface fc1/30 interface fc1/31 interface fc1/32 !Full Zone Database Section for vsan 102 zone name ice3270-1a 0c1 B vsan 102 member pwwn 20:00:00:25:b5:00:0b:0f ! [ice3270-1a\_0c1\_B] member pwwn 50:0a:09:84:8d:7d:92:bc [ice3270-1a\_0d] 1 member pwwn 50:0a:09:84:9d:7d:92:bc ! [ice3270-1b\_0d] zone name ice3270-1b\_0d1\_B vsan 102 member pwwn 20:00:00:25:b5:00:0b:1f ! [ice3270-1b\_0d1\_B] member pwwn 50:0a:09:84:8d:7d:92:bc ! [ice3270-1a\_0d] member pwwn 50:0a:09:84:9d:7d:92:bc 1 [ice3270-1b\_0d]

zoneset name flexpod vsan 102 member ice3270-1a\_0c1\_B member ice3270-1b\_0d1\_B



### References

### Authors

John George, Reference Architect, Infrastructure and Cloud Engineering, NetApp

John George is a Reference Architect in the NetApp Infrastructure and Cloud Engineering team and is focused on developing, validating, and supporting cloud infrastructure solutions that include NetApp products. Before his current role, he supported and administered Nortel's worldwide training network and VPN infrastructure. John holds a Master's degree in computer engineering from Clemson University.

Mike Mankovsky, Technical Marketing Engineer, Cisco

Mike Mankovsky is a Unified Computing System architect focusing on Microsoft solutions with extensive experience in Hyper-V, storage systems, and Microsoft Exchange Server. He has expert product knowledge in Microsoft Windows storage technologies and data protection technologies.

Chris Reno, Reference Architect, Infrastructure and Cloud Engineering, NetApp

Chris Reno is a Reference Architect in the NetApp Infrastructure and Cloud Enablement team and is focused on creating, validating, supporting, and evangelizing solutions based on NetApp products. Chris has his Bachelors of Science degree in International Business and Finance and his Bachelors of Arts degree in Spanish from the University of North Carolina – Wilmington while also holding numerous industry certifications.

Lindsey Street, Systems Architect, Infrastructure and Cloud Engineering, NetApp

Lindsey Street is a systems architect in the NetApp Infrastructure and Cloud Engineering team. She focuses on the architecture, implementation, compatibility, and security of innovative vendor technologies to develop competitive and high-performance end-to-end cloud solutions for customers. Lindsey started her career in 2006 at Nortel as an interoperability test engineer, testing customer equipment interoperability for certification. Lindsey has her Bachelors of Science degree in Computer Networking and her Master's of Science in Information Security from East Carolina University.





### 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 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)

© 2012 Cisco Systems, Inc. All rights reserved.



# CISCO.

Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA <u>www.cisco.com</u> Tel: 408 526-4000

800 553-NETS (6387) Fax: 408 527-0883

© 2012 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. (0805R)

C07-614444-01