FlexPod Validated with Microsoft Private Cloud

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 ....................................................................................................................... 14

Cabling Information ......................................................................................................... 15

NetApp FAS3240A Deployment Procedure: Part 1 .......................................................... 20
  Assign Controller Disk Ownership ........................................................................... 20
  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 agr1 .................................................................................... 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 ......................................................... 27
  Enable Flash Cache ................................................................................................... 27
  Add VLAN Interfaces ................................................................................................. 27
  Add Infrastructure Volumes ....................................................................................... 29

Cisco Nexus 5548 Deployment Procedure: Part 1 .......................................................... 29
  Set up Initial Cisco Nexus 5548 Switch ................................................................ 29
  Enable Appropriate Cisco Nexus Features ............................................................. 31
  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
Link into Existing Network Infrastructure
Save the Configuration

Cisco Unified Computing System Deployment Procedure
Perform Initial Setup of the Cisco UCS 6248 Fabric Interconnects
Log into Cisco UCS Manager
Add a Block of IP Addresses for KVM Access
Synchronize Cisco UCS to NTP
Configure Unified Ports
Edit the Chassis Discovery Policy
Enable Server and Uplink Ports
Acknowledge the Cisco UCS Chassis
Create Uplink PortChannels to the Cisco Nexus 5548 Switches
Create an Organization
Create a MAC Address Pool
Create WWNN Pools
Create WWPN Pools
Create UUID Suffix Pools
Create Server Pools
Create VLANs
Create VSANs and SAN PortChannels
Create a FC Adapter Policy for NetApp Storage Arrays
Create a Firmware Management Package
Set Jumbo Frames and Enable Quality of Service in Cisco UCS Fabric
Create a Power Control Policy
Create a Local Disk Configuration Policy
Create a Server Pool Qualification Policy
Create a Server BIOS Policy

Create vNIC/HBA Placement Policy for Virtual Machine Infrastructure Hosts
Create a vNIC Template
Create VHBA Templates for Fabric A and B
Create Boot Policies
Creating Boot Policy for Fabric -B
Create Service Profile Templates
Create Service Profiles
Add a Block of IP Addresses for KVM Access
Synchronize Cisco UCS to NTP
Add More Server Blades to the FlexPod Unit

Gather Necessary Information
Cisco Nexus 5548 Deployment Procedure: Part 2
Create VSANs, Assign FC Ports, Turn on FC Ports
Create Device Aliases and Create Zones
NetApp FAS3240A Deployment Procedure: Part 2
Create iGroups
Create LUNs
Map LUNs to iGroup ................................................................. 136
Prepare the Host for Windows Server 2008 R2 SP1 Installation......................................................... 137
Install Windows Server 2008 R2 ........................................................................................................... 137
Configure MPIO ................................................................................................................................. 142
Install Microsoft Hotfixes ................................................................................................................... 142
Create Zones for Redundant Paths ...................................................................................................... 143
Verify MultiPath I/O Connections (Both Hyper-V Hosts) ................................................................. 144
Clone the Windows Server 2008 R2 SP1 Installation ........................................................................ 144
Configure Network Interfaces, Rename Servers, and Install Microsoft Windows Updates on Both Hyper-V Hosts ......................................................................................................................... 145
Install the Failover Cluster Feature .................................................................................................. 153
Install NetApp MultiPath IO Tools on Both Hyper-V Hosts ............................................................. 153
Verify MultiPath I/O Connections (Both Hyper-V Hosts) .................................................................. 153
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) .................................................. 159
Create Domain Controller Virtual Machine ....................................................................................... 162
Install Windows in a Domain Controller Virtual Machine ............................................................... 169
Install Active Directory Services ....................................................................................................... 171
  Join Virtual Machine Host VM-Host-Infra-01 to a Windows Domain ........................................... 173
  Join Virtual Machine Host VM-Host-Infra-02 to a Windows Domain ........................................... 174
Set Firewall Exceptions (Both Hyper-V Hosts) .................................................................................. 174
Configure Infrastructure Server Cluster ............................................................................................... 174
  Configure Cluster Network For CSV Network Traffic .................................................................. 181
Create Virtual Machines and Resource for Deploying Infrastructure Roles ..................................... 183
Create VHD for Infrastructure Roles .................................................................................................. 183
Create Infrastructure Virtual Machines ............................................................................................... 187
  Domain Controller Virtual Machine (optional) .............................................................................. 187
Modify the Virtual Machine Settings ................................................................................................. 192
  Configure Virtual Processor Count .................................................................................................. 194
  Configure Virtual LAN Identification .............................................................................................. 195
  Add iSCSI Fabric A Interface .......................................................................................................... 196
  Add iSCSI Fabric B Interface .......................................................................................................... 197
  Create Clustered Application or Service ......................................................................................... 206
  Configure Live Migration Network for the Virtual Machines ......................................................... 210
Optional Optimization for CSV and Live Migration Networks .......................................................... 212
  Disable NetBios over TCP/IP for the CSV Network ....................................................................... 212
Installing Highly Available Microsoft System Center Components .................................................. 213
Installing Clustered Microsoft SQL Server 2008 .............................................................................. 213
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 ......................................................................... 220
  Step 2: Adding Node 2 to SQL Server ............................................................................ 223
  Step 3: Verify Cluster Operation ..................................................................................... 224
  Step 4: Add SQL Server Instance .................................................................................... 224
  Step 5: Add Node 1 to SQL Server Cluster .................................................................... 226
  Step 6: Configure Remote Access .................................................................................... 226
  Step 7: Verify Cluster Operation ..................................................................................... 227
System Center Operations Manager Installation ................................................................. 227
  Installing System Center Operations Manager 2007 R2 .................................................. 227
    Step 1: Active Directory Preparation ............................................................................ 227
    Step 2: Deploy Operations Manager Database ........................................................... 228
    Step 3: Install Windows Server 2008 R2 SP1 Enterprise in the SCOM Virtual Machine ..... 229
    Step 4: Install Prerequisite Software ........................................................................... 229
    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 ............................................................... 233
    Step 8: Install Operation Manager Reporting ................................................................ 234
Configure Operations Manager ............................................................................................. 235
Install System Center Virtual Machine Manager ................................................................. 236
  Step 1: Active Directory Preparation ............................................................................ 236
  Step 2: Install Windows Server 2008 R2 SP1 Enterprise in the SCVMM Virtual Machines 237
  Step 3: Install Prerequisite Software ............................................................................ 237
Enable Jumbo Frames for iSCSI NICs in SCVMM Virtual Machine ...................................... 239
  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) .................. 245
  Step 10: SCOM Administrative Console ....................................................................... 250
Configure SCVMM SCOM Integration .................................................................................. 250
Install OnCommand Plug in 3.0 for Microsoft SCOM ............................................................ 251
Install Cisco UCS MP for Microsoft SCOM .......................................................................... 256
  Assigning an IP Address to the Management Port .......................................................... 260
  Creating an Account for Administrators ........................................................................ 261
  Adding an Account to a Profile ....................................................................................... 261
  Adjusting the Discovery Interval ..................................................................................... 262
Opalis Integration Server ....................................................................................................... 263
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™ is a predesigned configuration that is built on the Cisco® Unified Computing System® (Cisco UCS™), 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-a-service (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™ is the first converged data center platform that combines industry-standard, 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 1U 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 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-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](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.
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>
<thead>
<tr>
<th>Table 1 Software Revisions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Layer</strong></td>
</tr>
<tr>
<td>Compute</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Network</td>
</tr>
<tr>
<td>Storage</td>
</tr>
<tr>
<td>Software</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### 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 -g <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.

### Table 2 Necessary VLANs

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>VLAN Purpose</th>
<th>ID Used in this Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM-Mgmt</td>
<td>VLAN for management interfaces</td>
<td>805</td>
</tr>
<tr>
<td>Native</td>
<td>VLAN to which untagged frames are assigned</td>
<td>2</td>
</tr>
<tr>
<td>CSV</td>
<td>VLAN for cluster shared volume</td>
<td>801</td>
</tr>
<tr>
<td>iSCSI-A</td>
<td>VLAN for iSCSI traffic for fabric A</td>
<td>802</td>
</tr>
<tr>
<td>iSCSI-B</td>
<td>VLAN for iSCSI traffic for fabric B</td>
<td>807</td>
</tr>
<tr>
<td>Live Migration</td>
<td>VLAN designated for the movement of VM's from one physical host to another</td>
<td>803</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------------------------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>App Cluster</td>
<td>VLAN for cluster connectivity</td>
<td>806</td>
</tr>
<tr>
<td>Data</td>
<td>VLAN for application data</td>
<td>804</td>
</tr>
</tbody>
</table>

**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

- Cisco Nexus 5548 A
- Cisco Nexus 5548 B
- Cisco UCS Fabric Interconnect A
- Cisco UCS Fabric Interconnect B
- NetApp Controller A, FAS 3240
- NetApp Controller B, FAS 3240
- UCS 5108 Chassis 1

- **Green** = Used FCoE Port
- **Yellow** = Used 10 GbE Port
- **Blue** = Used 1 GbE Port
- **Red** = Used FC Port
- **Purple** = Used SAS Port (Disk Shelf Connectivity)
Table 3 Cisco Nexus 5548 A Ethernet Cabling Information

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

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

Table 4 Cisco Nexus 5548 B Ethernet Cabling Information

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

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

Table 5 NetApp controller A Ethernet Cabling Information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp controller A</td>
<td>e0M</td>
<td>100MbE</td>
<td>100MbE management switch</td>
<td>Any</td>
</tr>
<tr>
<td></td>
<td>e0P</td>
<td>GbE</td>
<td>SAS shelves</td>
<td>ACP port</td>
</tr>
<tr>
<td></td>
<td>e2a</td>
<td>10GbE</td>
<td>Cisco Nexus 5548 A</td>
<td>Eth1/1</td>
</tr>
<tr>
<td>Local Device</td>
<td>Local Port</td>
<td>Connection</td>
<td>Remote Device</td>
<td>Remote Port</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------</td>
<td>------------</td>
<td>--------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>e2b</td>
<td>10GbE</td>
<td>Cisco Nexus 5548 B</td>
<td>Eth1/1</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp controller B</td>
<td>e0M</td>
<td>100MbE</td>
<td>100MbE management switch</td>
<td>Any</td>
</tr>
<tr>
<td></td>
<td>e0P</td>
<td>GbE</td>
<td>SAS shelves</td>
<td>ACP port</td>
</tr>
<tr>
<td></td>
<td>e2a</td>
<td>10GbE</td>
<td>Cisco Nexus 5548 A</td>
<td>Eth1/2</td>
</tr>
<tr>
<td></td>
<td>e2b</td>
<td>10GbE</td>
<td>Cisco Nexus 5548 B</td>
<td>Eth1/2</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS fabric interconnect A</td>
<td>Eth1/19</td>
<td>10GbE</td>
<td>Cisco Nexus 5548 A</td>
<td>Eth1/3</td>
</tr>
<tr>
<td></td>
<td>Eth1/20</td>
<td>10GbE</td>
<td>Cisco Nexus 5548 B</td>
<td>Eth1/3</td>
</tr>
<tr>
<td></td>
<td>Eth1/1</td>
<td>FCoE/10GbE</td>
<td>Chassis 1 FEX A (if required)</td>
<td>Port 1</td>
</tr>
<tr>
<td></td>
<td>Eth1/2</td>
<td>FCoE/10GbE</td>
<td>Chassis 1 FEX A (if required)</td>
<td>Port 2</td>
</tr>
<tr>
<td></td>
<td>Eth1/3</td>
<td>FCoE/10GbE</td>
<td>Chassis 2 FEX A (if required)</td>
<td>Port 1</td>
</tr>
<tr>
<td></td>
<td>Eth1/4</td>
<td>FCoE/10GbE</td>
<td>Chassis 2 FEX A (if required)</td>
<td>Port 2</td>
</tr>
<tr>
<td></td>
<td>Eth1/5</td>
<td>FCoE/10GbE</td>
<td>Chassis 3 FEX A (if required)</td>
<td>Port 1</td>
</tr>
<tr>
<td></td>
<td>Eth1/6</td>
<td>FCoE/10GbE</td>
<td>Chassis 3 FEX A (if required)</td>
<td>Port 2</td>
</tr>
<tr>
<td></td>
<td>MGMT0</td>
<td>100MbE</td>
<td>100MbE management switch</td>
<td>Any</td>
</tr>
<tr>
<td></td>
<td>L1</td>
<td>GbE</td>
<td>Cisco UCS fabric interconnect B</td>
<td>L1</td>
</tr>
<tr>
<td></td>
<td>L2</td>
<td>GbE</td>
<td>Cisco UCS fabric interconnect B</td>
<td>L2</td>
</tr>
</tbody>
</table>
Table 8 Cisco UCS fabric interconnect B Ethernet cabling information

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

Table 9 Cisco Nexus 5548 A Fibre Channel cabling information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Nexus 5548 A</td>
<td>FC1/29</td>
<td>FC</td>
<td>Controller_A</td>
<td>0c</td>
</tr>
<tr>
<td></td>
<td>FC1/30</td>
<td>FC</td>
<td>Controller_B</td>
<td>0c</td>
</tr>
<tr>
<td></td>
<td>FC1/31</td>
<td>FC</td>
<td>Cisco UCS fabric interconnect A</td>
<td>Port 31</td>
</tr>
<tr>
<td></td>
<td>FC1/32</td>
<td>FC</td>
<td>Cisco UCS fabric interconnect A</td>
<td>Port 32</td>
</tr>
</tbody>
</table>

Table 10 Cisco Nexus 5548 B Fibre Channel cabling information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Nexus 5548 B</td>
<td>FC1/29</td>
<td>FC</td>
<td>Controller_A</td>
<td>0d</td>
</tr>
<tr>
<td></td>
<td>FC1/30</td>
<td>FC</td>
<td>Controller_B</td>
<td>0d</td>
</tr>
<tr>
<td></td>
<td>FC1/31</td>
<td>FC</td>
<td>Cisco UCS fabric interconnect A</td>
<td>Port 31</td>
</tr>
<tr>
<td></td>
<td>FC1/32</td>
<td>FC</td>
<td>Cisco UCS fabric interconnect A</td>
<td>Port 32</td>
</tr>
</tbody>
</table>
Table 11 Cisco UCS fabric interconnect A Fibre Channel cabling information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS fabric interconnect A</td>
<td>Port 31</td>
<td>FC</td>
<td>Cisco Nexus 5548 A</td>
<td>FC1/31</td>
</tr>
<tr>
<td></td>
<td>Port 32</td>
<td>FC</td>
<td>Cisco Nexus 5548 A</td>
<td>FC1/32</td>
</tr>
</tbody>
</table>

Table 12 Cisco UCS Fabric Interconnect B Fibre Channel cabling information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS fabric interconnect B</td>
<td>Port 31</td>
<td>FC</td>
<td>Cisco Nexus 5548 B</td>
<td>FC1/31</td>
</tr>
<tr>
<td></td>
<td>Port 32</td>
<td>FC</td>
<td>Cisco Nexus 5548 B</td>
<td>FC1/32</td>
</tr>
</tbody>
</table>

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 1 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 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™ 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 1 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 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™ 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 provides 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>`.
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 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>`.
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 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 qos.
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-qos system_nq_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.
2. 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`.
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`.
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`.
12. Type `exit`.
13. Type `interface Eth1/3`.
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 Po10.
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 Po11.
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 Po14.
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 Po10.
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 Po11.
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 Po14.
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 Po10.
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 Po11.
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, 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 Po10`.
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, 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 Po11`.
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 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.

**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.
3. Type peer-keepalive destination <Nexus B mgmt0 IP> source <Nexus A mgmt0 IP>.
4. Type exit.
5. Type interface Po10.
6. Type vpc peer-link.
7. Type exit.
8. Type interface Po11.
9. Type vpc 11.
10. Type exit.
11. Type interface Po12.
12. Type vpc 12.
13. Type exit.
15. Type vpc 13.
16. Type exit.
17. Type interface Po14.
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.
3. Type peer-keepalive destination <Nexus A mgmt0 IP> source <Nexus B mgmt0 IP>.
4. Type exit.
5. Type interface Po10.
6. Type vpc peer-link.
7. Type exit.
8. Type interface Po11.
9. Type vpc 11.
10. Type exit.
11. Type interface Po12.
12. Type vpc 12.
13. Type exit
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.
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.
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.

**Cisco UCS Manager**
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.

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.

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


9. Expand the Unconfigured Ethernet Ports section.

10. 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.

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.

**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.

**Cisco UCS Manager**

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**.
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 OK to enable.
15. Wait until the overall status of the Port Channel is up.
16. Click **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.
3. Right-click MAC Pools under the root organization.
4. Select Create MAC Pool to create the MAC address pool.
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.
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.

Cisco UCS Manager
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.

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.

Cisco UCS Manager
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 `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.
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.

Cisco UCS Manager
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. Click 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.
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.
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.
20. Right-click 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.
26. Right-click **VLANs**.
27. Select **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**.
38. Right-click 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.
50. In the list of VLANs in the left pane, right-click the newly created Native-VLAN and select **Set as Native VLAN**.

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.

**Cisco UCS Manager**

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 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.
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 a Firmware Management Package
These steps provide details for a firmware management policy for the Cisco UCS environment.
Cisco UCS Manager

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.
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.

Cisco UCS Manager

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**.
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.
7. Select the LAN tab on the left of the window.
8. Go to LAN > Policies > Root >


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.
15. Select Create QoS Policy.
16. Enter 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.
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 a Power Control Policy
These steps provide details for creating a Power Control Policy for the Cisco UCS environment.

Cisco UCS Manager
1. Select the Servers tab at the top left of the window.
2. Go to Policies > root.
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.
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.

**Cisco UCS Manager**

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**.
Create a Server Pool Qualification Policy
These steps provide details for creating a server pool qualification policy for the Cisco UCS environment.

Cisco UCS Manager
1. Select the Servers tab on the left of the window.
2. Go to Policies > root.
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.
Cisco UCS Manager

1. Select the Servers tab on the left of the window.
2. Go to Policies > root.
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.
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 a vNIC Template
These steps provide details for creating multiple vNIC templates for the Cisco UCS environment.

Cisco UCS Manager
1. Select the LAN tab on the left of the window.
2. Go to Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter CSV as the vNIC template name.
7. Click OK to complete creating the vNIC template.
8. Click OK.
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.
15. Click OK to complete creating the vNIC template.
16. Click OK.
17. Select the **LAN** tab on the left of the window.

18. Go to **Policies > root**.
19. **Right-click** vNIC Templates.
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.**
25. Select the **LAN** tab on the left of the window.
26. Go to Policies > root.
27. Right-click vNIC Templates.
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 OK.
33. Select the **LAN** tab on the left of the window.
34. Go to **Policies > root**.
35. Right-click **vNIC Templates**.
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.
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.
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 iSCSI-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 OK.
Create vHBA Templates for Fabric A and B
These steps provide details for creating multiple vHBA templates for the Cisco UCS environment.
Cisco UCS Manager

1. Select the VSAN tab on the left of the window.
2. Go to Policies > root.
3. Right-click vHBA Templates.
4. Select Create vNIC Template.
5. Enter VHBA-Template-A as the vHBA template name.
7. Click OK to complete creating the vHBA template.
8. Click OK.
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.
15. Click **OK** to complete creating the vHBA template.
16. Click **OK**.
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.

Cisco UCS Manager

1. Select the Servers tab at the top left of the window.
2. Go to Policies > root.
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.
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 0c 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.

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.

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.

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 OK to add the SAN boot target.

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 0d 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.
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 OK to add the SAN boot target.

```
Add SAN Boot

vHBA: Fabric-B
Type: Primary Secondary
```

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 0d 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.
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 0d 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.

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 OK to add the SAN boot target.
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 0c of controller A. To obtain this information, log in to controller A and run the `fcp show adapters` 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.

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 0c 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](image)

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 0c.
   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.

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 Create vHBA window displays. Name the vHBA Fabric-A.
h. Check the box for Use SAN Connectivity Template.
i. Select Fabric-A in the vHBA Template field.
k. Click OK to add the vHBA to the template.

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

![Create vHBA](image)

13. Verify – Review the table to make sure that both of the vHBAs were created.
14. Click Next to continue to the next section.

15. Networking Section
   a. Leave the Dynamic vNIC Connection Policy field at the default.
   b. Select Expert for the How would you like to configure LAN connectivity? option.
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.
i. Click Add to add a vNIC to the template.

j. The Create vNIC window displays. Name the vNIC LiveMigration.

k. Check the Use LAN Connectivity Template checkbox.

l. Select LiveMigration for the vNIC Template field.

m. Select Windows in the Adapter Policy field.

n. Click OK to add the vNIC to the template.
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.
u. Click 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 Create vNIC window displays. Name the vNIC VM-Data.

c. Check the Use LAN Connectivity Template checkbox.

dd. Select VM-Data for the vNIC Template field.

ee. Select Windows in the Adapter Policy field.

ff. Click OK to add the vNIC to the template.
gg. Click 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.

ll. Click OK to add the vNIC to the template.
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 **OK** to add the vNIC to the template.
22. Verify: Review the table to make sure that all of the vNICs were created.
23. Click **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.**
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
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.
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** **Next** to continue to the next section.
31. Maintenance Policy Section
   a. Keep the default of no policy used by default.
   b. Click Next to continue to the next section.

32. Server Assignment Section
   a. Select Default in the Pool Assignment 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.
33. Operational Policies Section
   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.
34. Select the Servers tab at the top left of the window.
35. Go to Service Profile Templates > root.
36. Select the previously created VM-Host-Infra-Fabric-A template
37. Click Create a 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.
41. Select Boot-Fabric-B Boot Policy and click OK.
42. Select the **Network** tab and click **Modify vNIC/HBA Placement Policy**.
43. Move vHBA Fabric-B ahead of vHBA Fabric-A in the placement order and click OK.
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.

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.
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.

**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.

<table>
<thead>
<tr>
<th>NetApp Controller</th>
<th>FC Port</th>
<th>FC Portname</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller A</td>
<td>0c</td>
<td></td>
</tr>
<tr>
<td>Controller B</td>
<td>0c</td>
<td>0d</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Cisco UCS Service Profile Name</th>
<th>Fabric-A WWPN</th>
<th>Fabric-B WWPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM-Host-Infra-01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VM-Host-Infra-02</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.
**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 fcl/29-32`.
7. Type `vsan <VSAN A ID> interface san-port-channel 1`.
8. Type `exit`.
9. Type `interface fcl/31-32`.
10. Type `channel-group 1 force`.
11. Type `no shutdown`.
12. Type `exit`.
14. Type `no shutdown`.
15. Type `exit`.
16. Type `show int san-port-channel 1` to confirm connectivity.
17. Type `interface fcl/29`.
18. Type `switchport description <Controller A:0c>`.
19. Type `exit`.
20. Type `interface fcl/30`.
21. Type `switchport description <Controller B:0c>`.
22. Type `exit`.
23. Type `interface fcl/31`.
25. Type `exit`.
26. Type `interface fcl/32`.
27. Type `switchport description <UCSM A:fcl/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.
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:0d>.
19. Type exit.
20. Type interface fc1/30.
21. Type switchport description <Controller B:0d>.
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_0c pwwn <Controller A 0c WWPN>.
5. Type device-alias name controller_B_0c pwwn <Controller B 0c 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_0c1_A.
   c. Type member device-alias controller_A_0c.
   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_0c1_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_0d pwwn <Controller A 0d 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_0d.
   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.

```bash
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:

```bash
igroup create -f -t hyper_v VM-Host-Infra-02<Fabric-A WWPN> <Fabric-B WWPN>.

igroup set VM-Host-Infra-02 alua 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:

```bash
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:

```bash
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 [www.cisco.com](http://www.cisco.com) 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.
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 Manager**
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.
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.
11. The Cisco VIC FCoE StorePort Drive will be selected. Click Next to load the driver.

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.

![Windows Installer DVD Remap](image)

17. Click **Next** to continue with installation. Do a standard installation of Windows Server 2008 R2 SP1 DataCenter Edition.
Note: Detailed steps for the installation of Windows Server 2008 R2 SP1 DataCenter Edition are not provided. Please reference Microsoft documentation 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.


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 right-clicking 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 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)
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,
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_0c`.
      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_0c`.
      6. Type `member device-alias controller_A_0c`.
      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_0d`.
   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_0d`.
   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 Manager 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

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-v-template /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-v-template <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.
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.
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.

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

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.
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.
3. 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.

<table>
<thead>
<tr>
<th>Virtual Network Name</th>
<th>Connection Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM-Data</td>
<td>External</td>
<td>Cisco VIC Interface</td>
</tr>
<tr>
<td>App-Cluster-Comm</td>
<td>External</td>
<td>Cisco VIC Interface #8</td>
</tr>
<tr>
<td>iSCSI-Fabric-A</td>
<td>External</td>
<td>Cisco VIC Interface #3</td>
</tr>
<tr>
<td>iSCSI-Fabric-B</td>
<td>External</td>
<td>Cisco VIC Interface #2</td>
</tr>
</tbody>
</table>

**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
- New virtual network
- VM-Data - Virtual Network
- Cisco VIC Ethernet Interface

Global Network Settings
- MAC Address Range
  00-15:5D-85:57-00 to 00-15:5D-8...

Virtual Network Properties
- Name: VM-Data - Virtual Network
- 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 the network adapter
- Internal only
- Private virtual machine network

Enable virtual LAN identification for management operating system
- VLAN 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.

More about managing virtual networks

OK Cancel Apply
App-Cluster-Comm

Virtual Network Manager

Virtual Networks
- New virtual network
- VM-Data - Virtual Network
- Cisco VIC Ethernet Interface
- App-Cluster-Comm
- Cisco VIC Ethernet Interface #8

Global Network Settings
- MAC Address Range: 00-15-3D-85-57-00 to 00-15-3D-8...

New Virtual Network
- Name: App-Cluster-Comm
- Notes:

Connection type
- What do you want to connect this network to?
  - External:
    - Cisco VIC Ethernet Interface #8
  - Allow management operating system to share this network adapter
  - Internal only
  - Private virtual machine network

Enable virtual LAN identification for management operating system

VLAN 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.
  - VLAN ID: 2

More about managing virtual networks

OK  Cancel  Apply
iSCSI-Fabric-A
Domain Controller Virtual Machine (optional)
Most environments will already have an active directory infrastructure and will not require additional domain controllers to 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.
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>
<thead>
<tr>
<th>VM Host</th>
<th>VM Name</th>
<th>Name</th>
<th>Location</th>
<th>Size</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infra-VM-Host-01</td>
<td>Infra-DC-01</td>
<td>Infra-DC-01.vhd</td>
<td>C:\ClusterStorage\CSV-01</td>
<td>60 GB</td>
<td>Fixed</td>
</tr>
<tr>
<td>Infra-VM-Host-02</td>
<td>Infra-DC-02</td>
<td>Infra-DC-02.vhd</td>
<td>C:\ClusterStorage\CSV-02</td>
<td>60 GB</td>
<td>Fixed</td>
</tr>
</tbody>
</table>

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.
Create Domain Controller Virtual Machine

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

Table 14 Virtual Machine Domains

<table>
<thead>
<tr>
<th>VM Host</th>
<th>VM Name</th>
<th>Hard Disk</th>
<th>Network</th>
<th>Memory</th>
<th>VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infra-VM-Host-01</td>
<td>Infra-DC-01</td>
<td>C:\ClusterStorage\CSV-01\Infra-DC-01.vhd</td>
<td>VM-Data Virtual Network</td>
<td>8 GB</td>
<td>804</td>
</tr>
<tr>
<td>Infra-VM-Host-02</td>
<td>Infra-DC-02</td>
<td>C:\ClusterStorage\CSV-02\Infra-DC-02.vhd</td>
<td>VM-Data Virtual Network</td>
<td>8 GB</td>
<td>804</td>
</tr>
</tbody>
</table>

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.
Assign Memory

Specify the amount of memory to allocate to the 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.

Memory: 8192 MB

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.

More about determining the memory to assign to a virtual machine.
Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual network, or it can remain disconnected.

Connection: VM-Data - Virtual Network

More about configuring network adapters
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.

- **Create a virtual hard disk**
  - Name: Infra-DC-01.vhd
  - Location: C:\VHD\Infra-DC-01\Infra-DC-01\Infra-DC-01.vhd
  - Size: 127 GB (Maximum: 2040 GB)

- **Use an existing virtual hard disk**
  - Location: C:\VHD\Infra-DC-01\Infra-DC-01-boot.vhd

- **Attach a virtual hard disk later**
Completing the New Virtual Machine Wizard

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.
Enable virtual LAN identification

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

VLAN ID

00:00:00:00:00:00

To remove the network adapter from this virtual machine, click 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.
Install Windows in a Domain Controller Virtual Machine
Installing Windows...

That's all the information we need right now. Your computer will restart several times during installation.

- Copying Windows files
- Expanding Windows files (90%)
- Installing Features
- Installing updates
- Completing installation
Install Active Directory Services

Add Roles Wizard

Select Server Roles

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
- [X] Active Directory Domain Services
- [ ] Active Directory Federation Services
- [ ] Active Directory Lightweight Directory Services
- [ ] Active Directory Rights Management Services
- [ ] Application Server
- [ ] DHCP Server
- [ ] DNS Server
- [ ] Fax Server
- [ ] File Services
- [ ] Hyper-V
- [ ] Network Policy and Access Services
- [ ] Print and Document Services
- [ ] Remote Desktop Services
- [ ] Web Server (IIS)
- [ ] Windows Deployment Services
- [ ] Windows Server Update Services

Description:

Active Directory Domain Services (AD 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 login process.

More about server roles

< Previous  Next >  Install  Cancel
Run **dcpromo** to configure the Domain Controllers.
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.
Note: Reboot

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

Set Firewall Exceptions (Both Hyper-V Hosts)

Add SnapDrive
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.

k. Select Yes to run all validation tests, and click Next, then Next again.

l. 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.
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 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.

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.

![Image of Failover Cluster Manager]

**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`.

   ```powershell
   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

<table>
<thead>
<tr>
<th>VM Host</th>
<th>VM Name</th>
<th>Name</th>
<th>Location</th>
<th>Size</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infra-VM-Host-01</td>
<td>Infra-SQL-01</td>
<td>Infra-SQL-01.vhd</td>
<td>C:\VHD\Infra-SQL-01</td>
<td>60 GB</td>
<td>Fixed</td>
</tr>
<tr>
<td>Infra-VM-Host-02</td>
<td>Infra-SQL-02</td>
<td>Infra-SQL-02.vhd</td>
<td>C:\VHD\Infra-SQL-01</td>
<td>60 GB</td>
<td>Fixed</td>
</tr>
<tr>
<td>Infra-VM-Host-01</td>
<td>Infra-SCOM-01</td>
<td>Infra-SCVMM-01.vhd</td>
<td>C:\ClusterStorage\CSV-01</td>
<td>60 GB</td>
<td>Fixed</td>
</tr>
<tr>
<td>Infra-VM-Host-02</td>
<td>Infra-SCVMM-01</td>
<td>Infra-SCVMM-01.vhd</td>
<td>C:\ClusterStorage\CSV-02</td>
<td>60 GB</td>
<td>Fixed</td>
</tr>
<tr>
<td>Infra-VM-Host-01</td>
<td>Infra-Opalis-01</td>
<td>Infra-Opalis-01.vhd</td>
<td>C:\ClusterStorage\CSV-01</td>
<td>60 GB</td>
<td>Fixed</td>
</tr>
</tbody>
</table>

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 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.
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.

Description:

Type: fixed size
Name: Infra-SQL-01.vhd
Location: C:\VHD\Infra-SQL-01
Size: 60 GB

To create the virtual hard disk and close this wizard, click Finish.
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.

Description:

- **Type:** Fixed size
- **Name:** Infra-SCVMM-01.vhd
- **Location:** C:\ClusterStorage\CSV-02
- **Size:** 60 GB

To create the virtual hard disk and close this wizard, click Finish.
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:

Description:

- **Type:** Fixed size
- **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.
Create Infrastructure Virtual Machines

Domain Controller Virtual Machine (optional)

Most environments will already have an active directory infrastructure and will not require additional domain controllers to 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.

Table 16 Infrastructure Virtual Machines

<table>
<thead>
<tr>
<th>VM Host</th>
<th>VM Name</th>
<th>Hard Disk</th>
<th>Network</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infra-VM-Host-01</td>
<td>Infra-SQL-01</td>
<td>C:\VHD\Infra-SQL-01\Infra-SQL-01.vhd</td>
<td>VM-Data – Virtual Network</td>
<td>8 GB</td>
</tr>
<tr>
<td>Infra-VM-Host-02</td>
<td>Infra-SQL-02</td>
<td>C:\VHD\Infra-SQL-02\Infra-SQL-02.vhd</td>
<td>VM-Data – Virtual Network</td>
<td>8 GB</td>
</tr>
</tbody>
</table>
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.
Completing the New Virtual Machine Wizard

You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

Description:

Name: Infra-SCOM-01
Memory: 8192 MB
Network: VM-Data - Virtual Network
Hard Disk: C:\ClusterStorage\CSV-02\Infra-SCOM-01.vhd

To create the virtual machine and close the wizard, click Finish.
Completing the New Virtual Machine Wizard

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:\HDD\infra-SQL-01\infra-SQL-01.vhd

To create the virtual machine and close the wizard, click Finish.
Completing the New Virtual Machine Wizard

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:\HDD\infra-SQL-01\infra-SQL-01.vhd

To create the virtual machine and close the wizard, click Finish.
Modify the Virtual Machine Settings

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

Table 17 Virtual Machine Settings

<table>
<thead>
<tr>
<th>VM Name</th>
<th>Logical Processors</th>
<th>Network</th>
<th>VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infra-SQL-01</td>
<td>4</td>
<td>VM-Data</td>
<td>804</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iSCSI Fabric-A</td>
<td>802</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iSCSI Fabric-B</td>
<td>802</td>
</tr>
<tr>
<td></td>
<td></td>
<td>App-Cluster-Comm</td>
<td>806</td>
</tr>
<tr>
<td>Infra-SQL-02</td>
<td>4</td>
<td>VM-Data</td>
<td>804</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iSCSI Fabric-A</td>
<td>802</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iSCSI Fabric-B</td>
<td>802</td>
</tr>
<tr>
<td></td>
<td></td>
<td>App-Cluster-Comm</td>
<td>806</td>
</tr>
<tr>
<td>Infra-SCOM-01</td>
<td>2</td>
<td>VM-Data</td>
<td>804</td>
</tr>
<tr>
<td>Infra-SCVMM-01</td>
<td>2</td>
<td>VM-Data</td>
<td>804</td>
</tr>
<tr>
<td>Infra-Opalis-01</td>
<td>2</td>
<td>VM-Data</td>
<td>804</td>
</tr>
</tbody>
</table>
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

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.

Number of logical processors:

Resource control:
- You can use resource controls to balance resources among virtual machines.
- Virtual machine reserve (percentage):
- Percent of total system resources:
- Virtual machine limit (percentage):
- Percent of total system resources:
- Relative weight:

Processor compatibility:
- 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 guest operating systems. Select the scenarios you want to enable:
  - Migrate to a physical computer with a different processor version
  - Run an older operating system, such as Windows NT
Configure Virtual LAN Identification

Network Adapter
Specify the configuration of the network adapter or remove the network adapter.
Network: VM-Data - Virtual Network

MAC Address
- Dynamic
- Static
- Enable spoofing of MAC addresses

Enable virtual LAN identification
The VLAN identifier specifies the virtual LAN that the virtual machine will use for all network communications through this network adapter.

VLAN ID
804

To remove the network adapter from this virtual machine, click 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.
Add iSCSI Fabric A Interface

Network Adapter
Specify the configuration of the network adapter or remove the network adapter.

Network:
- iSCSI-Fabric-A

MAC Address
- Dynamic
- Static
- Enable spoofing of MAC addresses

Enable virtual LAN identification
- VLAN ID
  - The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.
  - 802

To remove the network adapter from this virtual machine, click 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.
Add iSCSI Fabric B Interface

Specify the configuration of the network adapter or remove the network adapter.

Networks:
- SCSI-Fabric-B

Enable virtual LAN identification
- VLAN ID: 602

To remove the network adapter from this virtual machine, click Remove.
Specify the configuration of the network adapter or remove the network adapter.

**Network:**

- App-Cluster-Comm

**MAC Address**
- Dynamic
- Static

Enable spoofing of MAC addresses

**Enable virtual LAN identification**

**VLAN ID**

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

- 806

To remove the network adapter from this virtual machine, click 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.
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:\Windows\Infra-SQL-02\infra-SQL-02.vhd

To create the virtual machine and close the wizard, click Finish.
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.

Number of logical processors: 4
The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

804
Specify the configuration of the network adapter or remove the network adapter.

Network:
- iSCSI-Fabric-A

MAC Address
- Dynamic
- Static

Enable spoofing of MAC addresses

Enable virtual LAN identification
- VLAN ID: 802

To remove the network adapter from this virtual machine, click 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.
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:

**Description:**
- **Type:** fixed size
- **Name:** Infra-Opsis-01.vhd
- **Location:** C:\ClusterStorage\CSV-01
- **Size:** 60 GB

To create the virtual hard disk and close this wizard, click 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 was successfully configured for the service or application.

<table>
<thead>
<tr>
<th>Name</th>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infra-SCOM-01</td>
<td>✔</td>
<td>Success</td>
</tr>
<tr>
<td>Infra-SCCMM-01</td>
<td>✔</td>
<td>Success</td>
</tr>
</tbody>
</table>

To view the report created by the wizard, click View Report.
To close this wizard, click Finish.
High availability was successfully configured for the service or application.

Virtual Machine

<table>
<thead>
<tr>
<th>Name</th>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infra-SQL-01</td>
<td>✔️</td>
<td>Success</td>
</tr>
</tbody>
</table>

To view the report created by the wizard, click View Report. To close this wizard, click Finish.

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.
Infra-Opalis-01

Summary of Infra-Opalis-01

Status: Online
Auto Start: Yes
Alerts: None
Preferred Owners: None
Current Owner: VMHost infra-01

Virtual Machine

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect...</td>
<td></td>
</tr>
<tr>
<td>Start</td>
<td></td>
</tr>
<tr>
<td>Turn off...</td>
<td></td>
</tr>
<tr>
<td>Shut down...</td>
<td></td>
</tr>
<tr>
<td>Save</td>
<td></td>
</tr>
<tr>
<td>Settings...</td>
<td></td>
</tr>
<tr>
<td>Show the critical events for this resource</td>
<td></td>
</tr>
<tr>
<td>Show Dependency Report</td>
<td></td>
</tr>
<tr>
<td>More Actions...</td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td></td>
</tr>
<tr>
<td>Properties</td>
<td></td>
</tr>
<tr>
<td>Help</td>
<td></td>
</tr>
</tbody>
</table>

Cluster Shared Volumes

<table>
<thead>
<tr>
<th>Name</th>
<th>Current Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSV-01</td>
<td>VMHost infra-01</td>
</tr>
</tbody>
</table>
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.
4. Click the Advanced button.
5. Select the option Disable NetBios over TCP/IP and click OK.
Installing Highly Available Microsoft System Center Components

Installing Clustered Microsoft SQL Server 2008

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

Table 18 SQL Server data locations

<table>
<thead>
<tr>
<th>LUN</th>
<th>Purpose</th>
<th>Scope</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>LUN 1, iSCSI</td>
<td>SQL Server databases</td>
<td>Per instance</td>
<td>Varies</td>
</tr>
<tr>
<td>LUN 2, iSCSI</td>
<td>SQL Server logging</td>
<td>Per instance</td>
<td>Varies</td>
</tr>
<tr>
<td>LUN 3, iSCSI</td>
<td>SQL Server cluster quorum</td>
<td>Per cluster</td>
<td>1GB</td>
</tr>
<tr>
<td>LUN 4, iSCSI</td>
<td>SQL Server DTC</td>
<td>Per cluster</td>
<td>1GB</td>
</tr>
</tbody>
</table>

When the infrastructure has been completely deployed, deploy the following databases and instances.
Table 19 Databases

<table>
<thead>
<tr>
<th>DB Client</th>
<th>Instance Name</th>
<th>DB name</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMM SSP</td>
<td>&lt;Instance 1&gt;</td>
<td>&lt;SCVMMSSP&gt;</td>
<td>Win Auth</td>
</tr>
<tr>
<td>Ops Mgr</td>
<td>&lt;Instance 1&gt;</td>
<td>&lt;Ops Mgr_DB&gt;</td>
<td>Win Auth</td>
</tr>
<tr>
<td>Ops Mgr</td>
<td>&lt;Instance 2&gt;</td>
<td>&lt;Ops Mgr_DW_DB&gt;</td>
<td>Win Auth</td>
</tr>
<tr>
<td>VMM</td>
<td>&lt;Instance 1&gt;</td>
<td>&lt;VMM_DB&gt;</td>
<td>Win Auth</td>
</tr>
<tr>
<td>Opalis</td>
<td>&lt;Instance 2&gt;</td>
<td>&lt;Opalis_DB&gt;</td>
<td>Win Auth</td>
</tr>
</tbody>
</table>

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.

3. 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 SP1 Enterprise 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 Start > Administrative Tools > iSCSI initiator. Click Yes to start the Microsoft iSCSI service.

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](attachment:image)

**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.

User Name:

netapp\SnapDrive

Password:

********

Port ID: 443

[< Back  Next >  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**


**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 TCP and enter the Specific local port** 445. Click **Next.**
4. **Select Allow the connection** and click **Next then 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](image)

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.
   c. Repeat steps i-v for iSCSI network B.
   d. 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.
   l. 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.
   o. 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.

l. 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.
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.
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_lpin64\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.
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.
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. Click 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.

26. In the Data Directories tab:
   b. Change the User database log directory to the <Log LUN Drive Letter> and click Next.
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_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.

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 **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. 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 OK.
12. Click Next.

b. Data directories:
   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 Next and then click Close.

**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.
2. 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 used 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.
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.
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.
3. 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 http://go.microsoft.com/fwlink/?LinkID=89064&clcid=0x409 and then restart.

Step 6: Install SQL Server Reporting Services

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.
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.

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.


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

1. 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.

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**.
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.
2. 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.
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 into 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.
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 Internet Information Services 7 Management Pack for Operations Manager 2007
      - SQL Server Monitoring Management Pack
   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.
3. 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 SP1 Enterprise 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

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.
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.
13. Enter your Product key, and 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.
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.
6.

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 > Next > Install > Finish.

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 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.
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™ 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.
12. Enter `A` to always run NetApp Cmdlets.
13. Run `Add-OCStorageSystem` for each Controller.

**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**

<table>
<thead>
<tr>
<th>Account Name</th>
<th>Requested during</th>
<th>Used for</th>
<th>Prerequisites</th>
<th>High Security</th>
</tr>
</thead>
</table>
| Service Account    | VMMSSP server component setup | 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:  
   - Communicating with the VMM server and performing tasks that require interacting with the VMM server.  
   - Communicating with the VMMSSP database. | 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 | VMMSSP Web site component setup | Running 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

<table>
<thead>
<tr>
<th>Connection Type</th>
<th>Protocol</th>
<th>Default Port</th>
<th>Where to Change the Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMMSSP Web site to/from VMMSSP server</td>
<td>WCF</td>
<td>8000</td>
<td>During self-service portal setup. After setup, in the &lt;services&gt; section of the Microsoft.DITSC.ProvisioningService.exe.config file. For more information, see “Tuning the Self-Service Portal with Global Parameters” in the Virtual Machine Manager Self-Service Portal 2.0: Datacenter Administration Guide.</td>
</tr>
<tr>
<td>Client to/from VMMSSP Web site</td>
<td>HTTP/HTTPS</td>
<td>Without SSL: 80 With SSL: 443</td>
<td>During self-service portal setup. After setup, in the Site Bindings 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.</td>
</tr>
<tr>
<td>VMMSSP Web site to/from VMMSSP database</td>
<td>Tabular Data Stream (TDS)</td>
<td>1433</td>
<td>During self-service portal setup.</td>
</tr>
<tr>
<td>VMMSSP server to/from VMMSSP database</td>
<td>TDS</td>
<td>1433</td>
<td>During self-service portal setup.</td>
</tr>
<tr>
<td>VMMSSP Web site to/from virtual machine hosts</td>
<td>Remote Desktop Protocol (RDP)</td>
<td>2179</td>
<td>This port cannot be changed.</td>
</tr>
</tbody>
</table>

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 Active Directory 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 0 Active Directory Preparation.

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 Fundamental Windows Communication Foundation Concepts 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 0 Active Directory Preparation.

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 Understanding Sites, Applications and Virtual Directories on IIS 7.

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.

l. 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. Click Save and Close.

9. To delete a virtual machine action, navigate to DeleteVM > Edit.

10. Paste the ONTapDeleteVM.txt content into the Script section of the edit window.

11. Paste the ONTapDeleteVMLocked.txt content into the LockedScript section.

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. Click Save and Close.
14. Navigate to Infrastructure > ServiceRole > Edit.
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
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 Plugin 3.0 for Microsoft (x64) - InstallShield Wizard](image)

   6. Click Install then Click Finish.

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.

![Override Properties dialog box]

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.
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 Setup Wizard]

   The installer will guide you through the steps required to install CISCO UCS Management Pack on your computer.

   **WARNING:** This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

2. Enter a server name in the Server Name field. Click Next.
3. Select the Enable Virtualization checkbox if you want to support the discovery and monitoring of hypervisors and virtual machines. Click Next.
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.


4. Enter a path to folder where the management pack is installed in the Folder field.
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.
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 drop-down 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.
9. Select the IntervalSeconds checkbox.
10. Change the value in the Override Value column to another value, and click OK.
11. Click OK again.

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.

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.
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.
18. Repeat this process for any additional license files.

**Installing Opalis 6.3 Patch**

1. 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.

2. 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 po11.**
6. **Type switchport trunk allowed vlan add <Fabric A FCoE VLAN ID>**.
7. **Type exit.**
8. **Type interface vfc11.**
9. **Type bind interface po11.**
10. **Type no shutdown.**
11. **Type exit.**
12. **Type interface po12.**
13. **Type switchport trunk allowed vlan add <Fabric A 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 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 &lt;Fabric B FCoE VLAN ID&gt;.
2. Type name FCoE_Fabric_B.
3. Type fcoe vsan &lt;VSAN B ID&gt;.
4. Type exit.
5. Type interface po11.
6. Type switchport trunk allowed vlan add &lt;Fabric B FCoE VLAN ID&gt;.
7. Type exit.
8. Type interface vfc11.
9. Type bind interface po11.
10. Type no shutdown.
11. Type exit.
12. Type interface po12.
13. Type switchport trunk allowed vlan add &lt;Fabric B FCoE VLAN ID&gt;.
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 &lt;VSAN B ID&gt; name Fabric_B.
24. Type vsan &lt;VSAN B ID&gt; interface fc1/31-32.
25. Type vsan &lt;VSAN B ID&gt; interface san-port-channel 2.
26. Type vsan &lt;VSAN A ID&gt; interface vfc11.
27. Type vsan &lt;VSAN A ID&gt; 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 &lt;UCSM B:fc1/31&gt;.
36. Type exit.
37. Type interface fc1/32.
38. Type switchport description <UCSM B:fcl/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 pwn <Fabric-A WWPN>.
3. Type device-alias name VM-Host-Infra-02_A pwn <Fabric-A WWPN>.
4. Type device-alias name controller_A_2a pwn <Controller A 2a WWPN>.
5. Type device-alias name controller_B_2a pwn <Controller B 2a WWPN>.
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 pwn <Fabric-B WWPN>.
3. Type device-alias name VM-Host-Infra-02_B pwn <Fabric-B WWPN>.
4. Type device-alias name controller_A_2b pwn <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`.

9. Type `exit`.

10. After all of the zones for the Cisco UCS service profiles have been created, create a zoneset to organize and manage them.

11. 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`.

12. Activate the zoneset.
   a. Type `zoneset activate name flexpod vsan <Fabric B VSAN ID>`.
   b. Type `exit`.

13. Type `copy run start`.


**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>`.  

© 2012 Cisco. All rights reserved. This document is Cisco Public Information.
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)**

```bash
ice5548-1# show run
!Command: show running-config
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 qos-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-qos class-all-flood
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
policy-map type network-qos jumbo
class type network-qos class-fcoe
  pause no-drop
  mtu 2158
class type network-qos class-default
  mtu 9000
  multicast-optimize
system qos
  service-policy type network-qos 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 bpdu-guard default
spanning-tree port type edge bpdu-filter 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_0c 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
  ![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]
  vsan 101 wwn 20:00:00:25:b5:00:0a:1f fcid 0x550004 dynamic
  ![ice3270-1b_0d1_A]

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

© 2012 Cisco. All rights reserved. This document is Cisco Public Information.
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]
  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$uemTjt9Bz9c2SSA1DPOX 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 qos-group 1
class-map type queuing class-all-flood
  match qos-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-qos class-all-flood
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
policy-map type network-qos jumbo
class type network-qos class-fcoe
  pause no-drop
  mtu 2158
  class type network-qos class-default
  mtu 9000
  multicast-optimize
system qos
  service-policy type network-qos jumbo
slot 1
  port 29-32 type fc
snmp-server user admin network-admin auth md5 0xe481d1d2fee4aa498237df1852270e8 priv 0xe481d1d2fee4aa498237df1852270e8 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]
  vsan 102 wwn 20:00:00:25:b5:00:0b:0f fcid 0x3f0003 dynamic
  [ice3270-1a_0c1_B]
  vsan 102 wwn 20:00:00:25:b5:00:0b:1f fcid 0x3f0004 dynamic
  [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]
    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
    [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, Linkssys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networks, 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.