FlexPod Deployment Guide

Last Updated: February 23, 2012
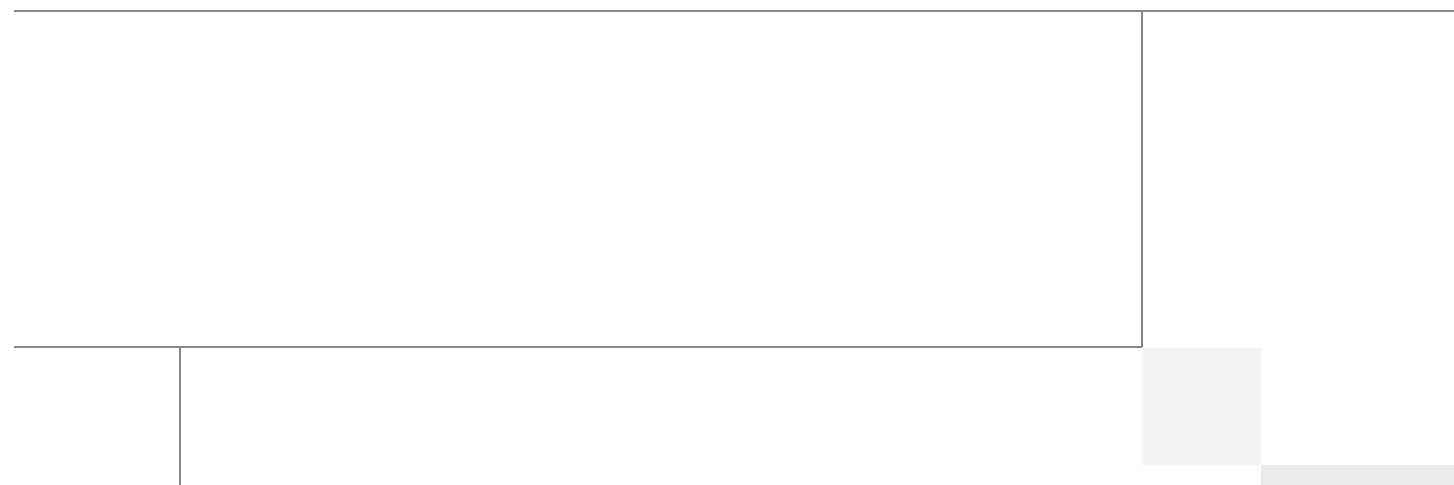
About the Authors

David Antkowiak, Solutions Architect, Systems Development Unit, Cisco Systems

David Antkowiak is a Solutions Architect with the Systems Development Unit (SDU). With over 10 years of experience in various private and government organizations, his areas of focus have included virtual desktop infrastructure, server virtualization, cloud migration, and storage design. Prior to joining Cisco, David was Solutions Architect at JetBlue. David holds a masters degree from Florida State University and two VMware certifications.

David Antkowiak

Ramesh Isaac, Technical Marketing Engineer, Systems Development Unit, Cisco

Ramesh Isaac has worked in data center and mixed-use lab settings since 1995. He started in information technology supporting UNIX environments and focused on designing and implementing multi-tenant virtualization solutions in Cisco labs over the last couple of years. Ramesh holds certifications from Cisco, VMware, and Red Hat.

Ramesh Isaac

Jon Benedict, Reference Architect, Infrastructure and Cloud Engineering, NetApp

Jon Benedict is a reference architect in the Infrastructure & Cloud Engineering team at NetApp. Jon is largely focused on designing, building, and evangelizing cloud and shared storage solutions based around NetApp for enterprise customers. Prior to NetApp, he spent many years as a consultant, integrator, and engineer with expertise in Unix and Linux. Jon holds many industry certifications including several from Red Hat.

Jon Benedict

Chris Reno, Reference Architect, Infrastructure and Cloud Engineering, NetApp

Chris Reno is a reference architect in the NetApp Infrastructure and Cloud Enablement group and is focused on creating, validating, supporting, and evangelizing solutions based on NetApp products. Before being employed in his current role, he worked with NetApp product engineers designing and developing innovative ways to perform Q&A for NetApp products, including enablement of a large grid infrastructure using physical and virtualized compute resources. In these roles, Chris gained expertise in stateless computing, netboot architectures, and virtualization.

Chris Reno

About Cisco Validated Design (CVD) Program

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit http://www.cisco.com/go/designzone.

FlexPod Deployment Guide

FlexPod Overview

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

FlexPod™ is a predesigned, base configuration that is built on the Cisco® Unified Computing System™ (UCS™), Cisco Nexus® data center switches, and NetApp® FAS storage components and includes a range of software partners. FlexPod can scale up for greater performance and capacity or it can scale out for environments that need consistent, multiple deployments. FlexPod is a baseline configuration, but also has the flexibility to be sized and optimized to accommodate many different use cases.

Cisco and NetApp have developed FlexPod as a platform that can address current virtualization needs and simplify data center evolution to ITaaS infrastructure.

FlexPod serves as a base infrastructure layer for a variety of IT solutions. A number of solutions have been built on the FlexPod architecture, including Microsoft® SharePoint®, VMware View™, VMware vSphere™, and Secure Multi-tenancy, among others. These FlexPod solutions can be found at:

- http://www.netapp.com/us/technology/flexpod/
- http://www.cisco.com/en/US/netsol/ns964/index.html

NetApp partners may access additional information at: https://fieldportal.netapp.com/.

Audience

This document describes the basic architecture of FlexPod as well as the general procedures for deploying the base FlexPod system. The intended audience for this document includes, but is not limited to, sales engineers, field consultants, professional services personnel, IT managers, partner engineering personnel, and customers who want to deploy the base FlexPod architecture.

Note For more detailed deployment information, Cisco and NetApp partners should contact their local account teams or visit http://www.netapp.com/us/technology/flexpod/.

FlexPod Architecture

Cisco and NetApp have provided documentation around best practices for building the FlexPod shared infrastructure stack. As part of the FlexPod offering, Cisco and NetApp designed a reference architecture with a technical specifications sheet and bill of materials that is highly modular or "pod-like". Although each customer's FlexPod system may 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 a foundation for data center deployments. FlexPod includes NetApp storage, Cisco networking, and the Cisco Unified Computing System in a single package in which the computing and storage fit in one data center rack and the networking resides in a separate rack. Due to port density the networking components can accommodate multiple instances of FlexPod systems. Figure 1 shows the FlexPod components.

The solution can be scaled while still maintaining its integrity, either by adding more FlexPod units or by adding to the solution components. A number of solutions can be built on top of one or more FlexPod units, providing enterprise flexibility, supportability, and manageability.

Figure 1 and Figure 2 outline the possible NetApp Filer interconnect choices. The first topology in Figure 1 is an FCoE-only implementation, while the second in Figure 2 adds the option of native FC connectivity. These interconnects are not interdependent and may be deployed together or separately to meet customer hypervisor or application support requirements. Both deployments are fully supported.

Figure 1   *FlexPod FCoE and 10 GbE Based Architecture*

Access

Qty 2: Cisco Nexus 5548

vPC   vPC

Unified Computing System

Qty 2: Cisco UCS 6120
Fabric Interconnect

2 10 GbE with
FCoE per
Fabric Extender

Qty 6: Cisco UCS B200 M2

Qty 9: Cisco UCS B250 M2

Qty 6: Cisco UCS 2140
Fabric Extender

Qty 3: Cisco UCS 5108
Chassis

Storage

FCoE
+2 x 10 GbE

FCoE
2 x 13 GbE

NetApp
FAS3210 HA Pair w/Qty. 4
DS2246 Disk Shelves
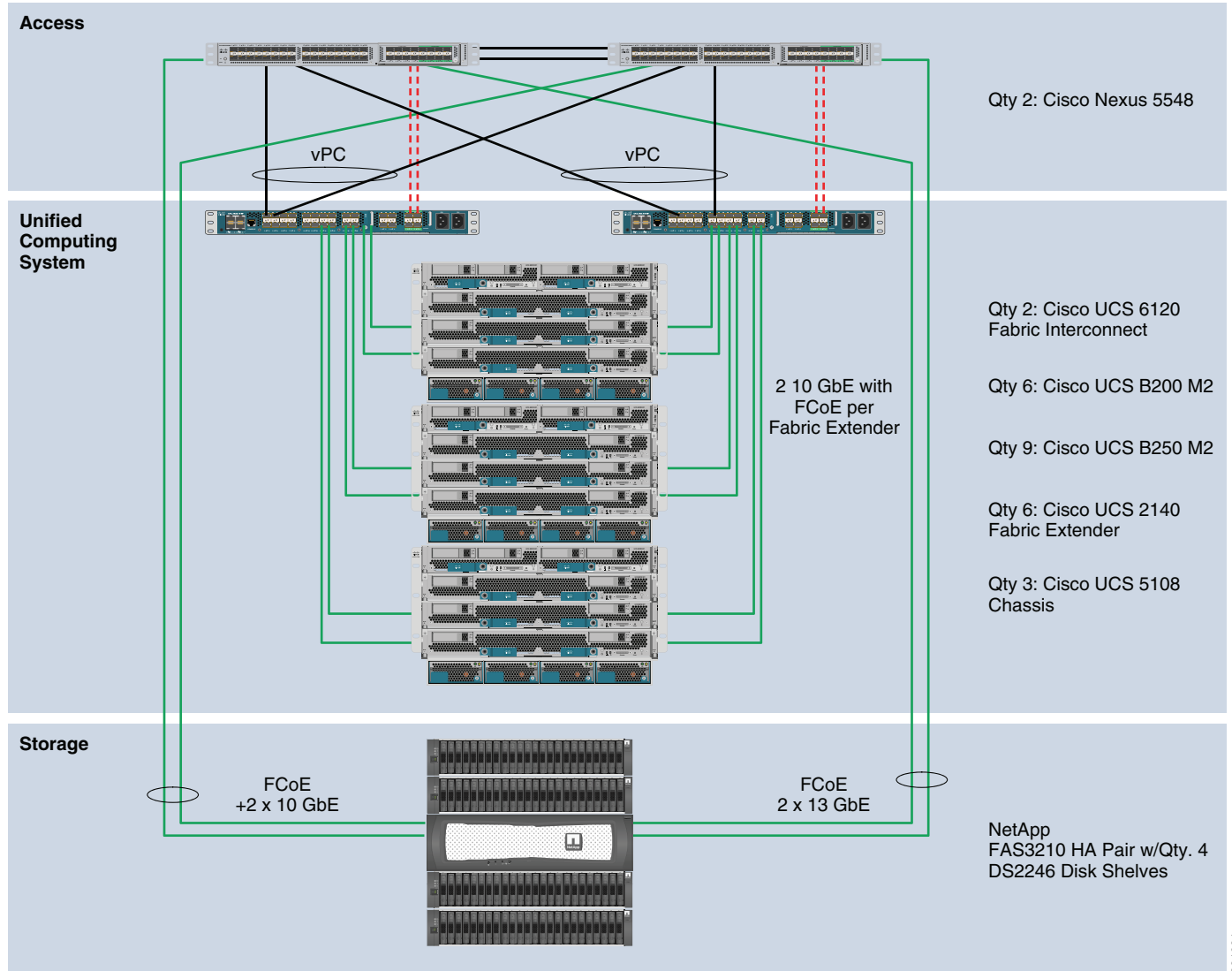
291691

Figure 2   *FlexPod FC and 10 GbE Based Architecture*
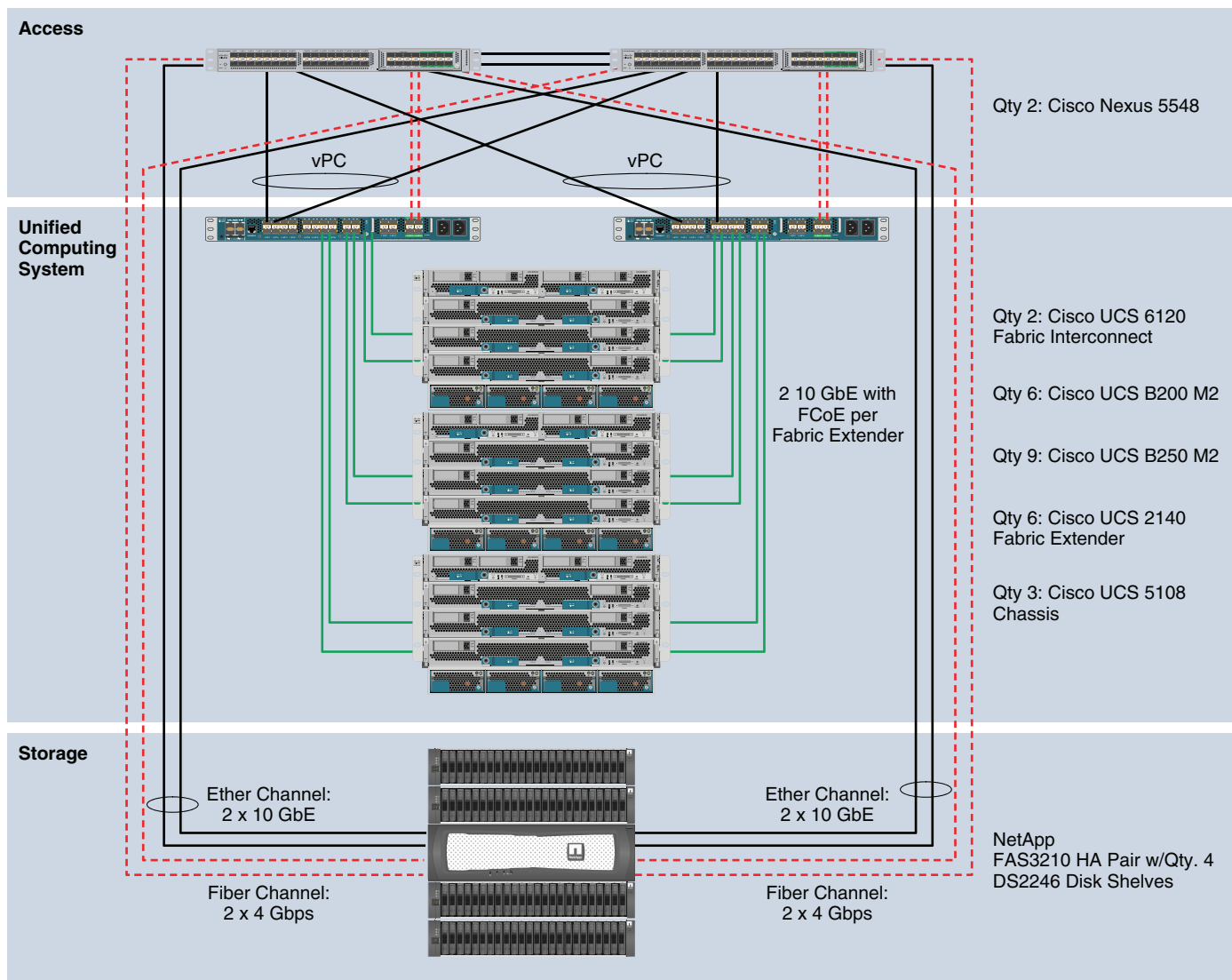
The default hardware is detailed in the FlexPod technical specifications and includes two Cisco Nexus 5548 switches, two Cisco UCS 6120 fabric interconnects, and three chassis of Cisco UCS blades with two fabric extenders per chassis. Storage is provided by a NetApp FAS3210CC (HA configuration within a single chassis) with accompanying disk shelves. All systems and fabric links feature redundancy, providing end-to-end high availability. This is the default base design, but each of the components can be scaled flexibly to support a specific customer's business requirements. For example, more (or different) blades and chassis could be deployed to increase compute capacity, additional disk shelves could be deployed to improve IO capacity and throughput, or special hardware or special hardware or software features may be added to introduce new features (such as NetApp FlashCache for dedupe-aware caching).

The remainder of this document guides the reader through the steps necessary to deploy the base architecture as shown above. This includes everything from physical cabling to compute and storage configuration.

FlexPod Configuration Deployment

The following section provides detailed information on configuring all aspects of a base FlexPod unit. Because the FlexPod architecture is flexible, the exact configuration detailed below may vary from customer implementations depending on specific requirements. Although customer implementations may deviate from the information that follows, the practices, features, and configurations below should still be used as a reference for building a customized FlexPod deployment.

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 to simplify cabling requirements.

Note The following tables are for the prescribed and supported configuration of the FAS3210 running Data ONTAP® 8.0.1. This configuration leverages a dual-port 10GbE add-on adapter and the on-board SAS ports for disk shelf connectivity. Onboard FC storage target ports are still supported for legacy implementations. For any modifications of this prescribed architecture, consult the currently available Interoperability Matrix Tool (IMT): http://now.netapp.com/matrix.

Note See the Site Requirements guide when deploying a storage system to ensure power and cooling requirements are met:
http://now.netapp.com/NOW/public/knowledge/docs/hardware/NetApp/site/pdf/site.pdf.

Note The FlexPod deployment guide assumes that out-of-band management ports are plugged into existing management infrastructure at the deployment site.

Note Be sure to cable as detailed below, because failure to do so will necessitate changes to the following deployment procedures as specific port locations are mentioned.

Note It is possible to order a FAS3210A system in a different configuration than the one prescribed below. Ensure that your configuration matches the one described in the tables and diagrams below before starting.

Note The tables below indicate recommended cabling for both FC- and FCoE-based architectures.

Note For FCoE-based architectures, the Fibre Channel protocol is addressed with the FCoE storage target adapters as indicated in Table 1.

> **Note** For FC-based architectures, the Fibre Channel protocol is addressed with native FC storage target ports as indicated in Table 2.

Table 1   FlexPod Ethernet Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 5548 A	Eth1/1	10GbE or FCoE	NetApp Controller A	e2a
	Eth1/2	10GbE or FCoE	NetApp Controller B	e2a
	Eth1/5	10GbE	Cisco Nexus 5548 B	Eth1/5
	Eth1/6	10GbE	Cisco Nexus 5548 B	Eth1/6
	Eth1/7	10GbE	Cisco UCS Fabric Interconnect A	Eth1/7
	Eth1/8	10GbE	Cisco UCS Fabric Interconnect B	Eth1/7
	MGMT0	100MbE	100MbE Management Switch	Any
Cisco Nexus 5548 B	Eth1/1	10GbE or FCoE	NetApp Controller A	e2b
	Eth1/2	10GbE or FCoE	NetApp Controller B	e2b
	Eth1/5	10GbE	Cisco Nexus 5548 A	Eth1/5
	Eth1/6	10GbE	Cisco Nexus 5548 A	Eth1/6
	Eth1/7	10GbE	Cisco UCS Fabric Interconnect A	Eth1/8
	Eth1/8	10GbE	Cisco UCS Fabric Interconnect B	Eth1/8
	MGMT0	100MbE	100MbE Management Switch	Any
	e0M	100MbE	100MbE Management Switch	Any
	e0P	1GbE	SAS shelves	ACP port
NetApp Controller A	e2a	10GbE or FCoE	Nexus 5548 A	Eth1/1
	e2b	10GbE or FCoE	Nexus 5548 B	Eth1/1
	e0M	100MbE	100MbE Management Switch	Any
	e0P	1GbE	SAS shelves	ACP port
NetApp Controller B	e2a	10GbE or FCoE	Nexus 5548 A	Eth1/2
	e2b	10GbE or FCoE	Nexus 5548 B	Eth1/2
	Eth1/7	10GbE	Nexus 5548 A	Eth1/9
	Eth1/7	10GbE	Nexus 5548 B	Eth1/9
	Eth1/7	10GbE	Nexus 5548 A	Eth1/9
	Eth1/8	10GbE	Nexus 5548 B	Eth1/9

Table 1   *FlexPod Ethernet Cabling Information*

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect	Eth1/1	10GbE/FCoE	Chassis 1 FEX A	port 1
	Eth1/2	10GbE/FCoE	Chassis 1 FEX A	port 2
	Eth1/3	10GbE/FCoE	Chassis 2 FEX A	port 1
	Eth1/4	10GbE/FCoE	Chassis 2 FEX A	port 2
	Eth1/5	10GbE/FCoE	Chassis 3 FEX A	port 1
	Eth1/6	10GbE/FCoE	Chassis 3 FEX A	port 2
	MGMT0	100MbE	100MbE Management Switch	Any
	L1	1GbE	UCS Fabric Interconnect B	L1
	L2	1GbE	UCS Fabric Interconnect B	L2
Cisco UCS Fabric Interconnect	Eth1/1	10GbE/FCoE	Chassis 1 FEX B	port 1
	Eth1/2	10GbE/FCoE	Chassis 1 FEX B	port 2
	Eth1/3	10GbE/FCoE	Chassis 2 FEX B	port 1
	Eth1/4	10GbE/FCoE	Chassis 2 FEX B	port 2
	Eth1/5	10GbE/FCoE	Chassis 3 FEX B	port 1
	Eth1/6	10GbE/FCoE	Chassis 3 FEX B	port 2
	MGMT0	100MbE	100MbE Management Switch	Any
	L1	1GbE	UCS Fabric Interconnect A	L1
	L2	1GbE	UCS Fabric Interconnect A	L2
	Eth1	1GbE	Nexus 5548 A (only used with vSphere)	Eth1/7
	Eth2	1GbE	Nexus 5548 B (only used with vSphere)	Eth1/7
	Eth1	1GbE	Nexus 5548 A (only used with vSphere)	Eth1/8
	Eth2	1GbE	Nexus 5548 B (only used with vSphere)	Eth1/8

Table 2   *FlexPod Fibre Channel Cabling Information*

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco Nexus 5548 A	FC2/1	FC	NetApp Controller A	0c
	FC2/2	FC	NetApp Controller B	0c
	FC2/3	FC	Cisco UCS Fabric Interconnect A	FC2/1
	FC2/4	FC	UCS Fabric Interconnect A	FC2/2
Cisco Nexus 5548 B	FC2/1	FC	NetApp Controller A	0d
	FC2/2	FC	NetApp Controller B	0d
	FC2/3	FC	Cisco UCS Fabric Interconnect B	FC2/1
	FC2/4	FC	UCS Fabric Interconnect B	FC2/2
NetApp Controller A	0c	FC	Cisco Nexus 5548 A	FC2/1
	0d	FC	Cisco Nexus 5548 B	FC2/1

Table 2   ***FlexPod Fibre Channel Cabling Information***

Local Device	Local Port	Connection	Remote Device	Remote Port
NetApp Controller B	0c	FC	Cisco Nexus 5548 A	FC2/2
	0d	FC	Cisco Nexus 5548 B	FC2/2
Cisco UCS Fabric Interconnect	FC2/1	FC	Cisco Nexus 5548 A	FC2/3
	FC2/2	FC	Cisco Nexus 5548 A	FC2/4
Cisco UCS Fabric Interconnect	FC2/1	FC	Cisco Nexus 5548 B	FC2/3
	FC2/2	FC	Cisco Nexus 5548 B	FC2/4

Figure 3   *FlexPod Cabling*

Qty 2: Cisco Nexus 5548

Qty 2: Cisco UCS 6120

Qty 3: Cisco UCS 5108

Qty 1: NetApp 3210A

■ = Used FCoE Port   ■ = Used 10 GbE Port

■ = Used 1 GbE Port   ■ = Used FC Port

■ = Used SAS Port
(Disk Shelf Connectivity)
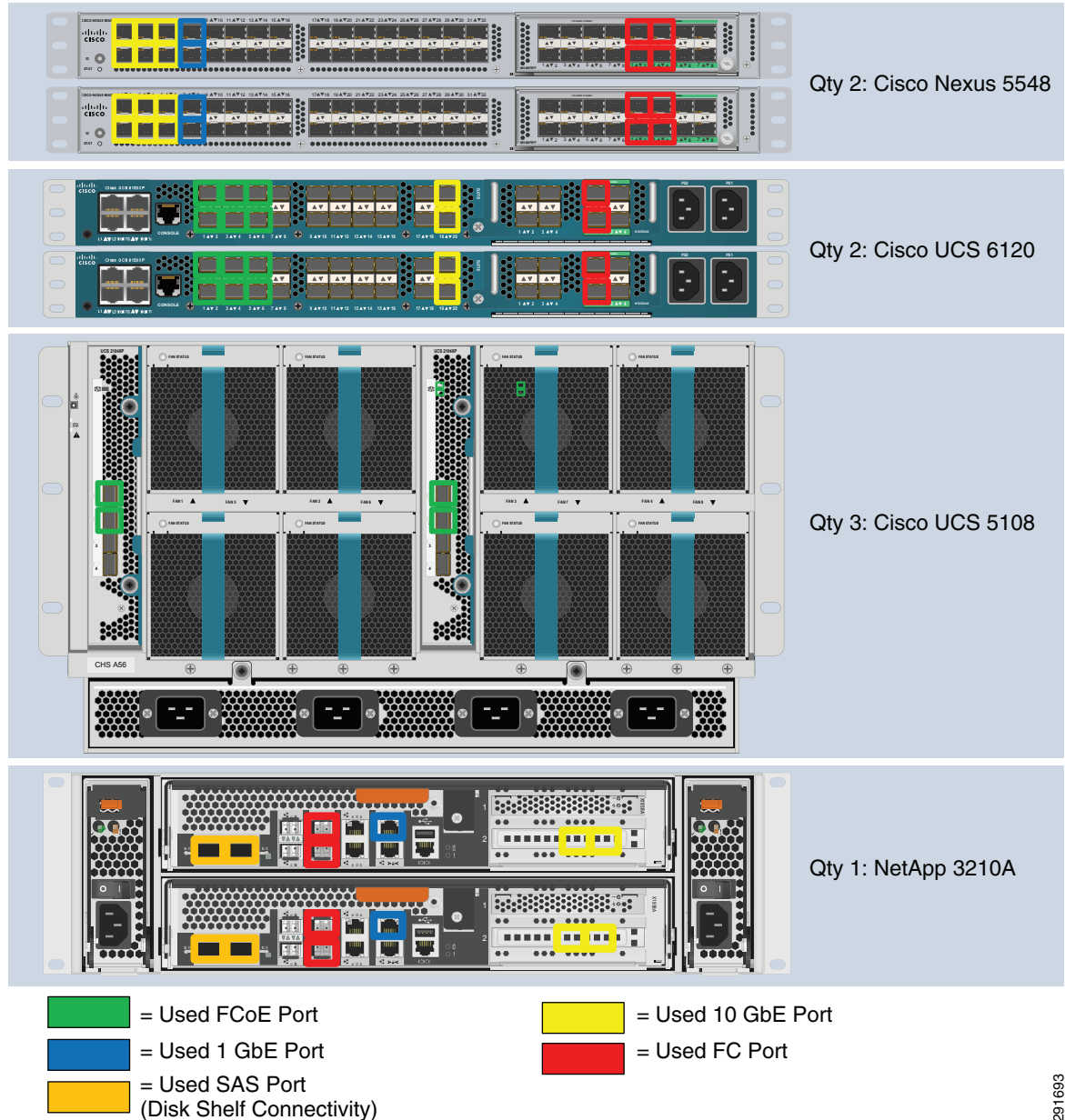
291693

NetApp FAS3210A Deployment Procedure—Part I

This section describes the procedures for configuring the NetApp FAS3210A for use in a FlexPod environment. This section has the following objectives:

- Establishment of a functional Data ONTAP 8.0.1 failover cluster with proper licensing

- Creation of data aggregates

- Creation of flexible volumes

- Configuration of NFS exports if using NFS for infrastructure volumes

- Creation of infrastructure vFiler® unit

The following measures should be taken to meet these objectives:

- Assign the storage controller disk wwnership.
- Ensure Data ONTAP 8.0.1 is installed.

✎

Note Upgrade or downgrade to Data ONTAP 8.0.1 if necessary.

- Set up Data ONTAP8.0.1.
- Install Data ONTAP to the on-board flash storage.
- Install required licenses.
- Start FCP service and enable proper FC port configuration.
- Enable active-active configuration between the two storage systems.
- Create the data aggregate "aggr1".
- Enable 802.1q VLAN trunking and add the NFS VLAN.
- Harden storage system logins and security.
- Create SNMP requests role and assign SNMP login privileges.
- Create SNMP management group and assign SNMP request role to it.
- Create SNMP user and assign to SNMP management group.
- Enable SNMP on the storage controllers.
- Delete SNMP v1 communities from storage controllers.
- Set SNMP contact information for each of the storage controllers.
- Set SNMP location information for each of the storage controllers.
- Establish SNMP trap destinations.
- Re-Initialize SNMP on the storage controllers.
- Enable FlashCache.
- Create the necessary infrastructure volumes (flexible volumes) for infrastructure services.
- Create the infrastructure IP space.
- Create the infrastructure vFiler units.
- Map the necessary infrastructure volumes to the infrastructure vFiler units.
- Set the priority levels for the volumes.

Cisco Nexus 5548 Deployment Procedure—Part I

This section describes the procedures for deploying the Cisco Nexus 5548 platforms for use in a FlexPod system and achieves the following objectives:

- Establish a functional pair of Cisco Nexus 5548 switches with proper licensing and features enabled.
- Establish connectivity between FlexPod elements including the use of traditional and virtual port channels.
- Establish connectivity to existing data center infrastructure.

The following actions are necessary to configure the Cisco Nexus 5548 switches for use in a FlexPod environment.

- Execute the Cisco Nexus 5548 setup script.
- Enable the appropriate Cisco Nexus features and licensing.
- Set global configurations.
- Create necessary VLANs including NFS and management.
- Add individual port descriptions for troubleshooting.
- Create necessary port channels including the vPC peer-link.
- Add Port Channel configurations.
- Configure virtual Port Channels (vPCs) to UCS fabric interconnects and NetApp controllers.
- Configure uplinks into existing network infrastructure, preferably by using vPC.
- Save the configuration.

Cisco Unified Computing System Deployment Procedure

This section provides the procedure for configuring the Cisco Unified Computing System for use in a FlexPod environment. This workflow should achieve the following goals:

- Creates a functional Cisco UCS fabric cluster
- Creates the logical building blocks for UCS management model including MAC, WWNN, WWPN, UUID and server pools, vNIC and vHBA templates, and VLANs and VSANs via UCSM
- Defines policies enforcing inventory discovery, network control, and server boot rules via UCSM
- Creates Service Profile templates
- Instantiates Service Profiles by association templates to physical blades

The following process should be followed for proper configuration.

- Execute the initial setup of the Cisco UCS 6100 Fabric Interconnects.
- Log into the Cisco UCS Manager via Web browser.
- Edit the Chassis Discovery Policy to reflect the number of links from the chassis to the fabric interconnects.
- Enable Fibre Channel Server and Uplink Ports.
- Create an Organization that manages the FlexPod infrastructure and owns the logical building blocks.
- Create MAC Address Pools under infrastructure organization.
- Create global VLANs, including NFS and OS data VLANs.
- Create a Network Control Policy under infrastructure Organization.
- Set Jumbo Frames in UCS Fabric.
- Create global VSANs.
- Create WWNN Pool under infrastructure Organization.
- Create WWPN Pools under infrastructure Organization.
- Create vNIC Template under infrastructure Organization using previously defined pools.

- Create vHBA Templates for Fabric A and B under infrastructure Organization.

- Create necessary Ethernet and SAN uplink Port-Channels to the Cisco Nexus 5548 Switches.

- Create WWNN Pool under infrastructure Organization.

- Create WWPN Pools under infrastructure Organization.

- Create global VSANs.

- Create vHBA Templates for Fabric A and B under infrastructure Organization.

- Create Boot Policies under infrastructure Organization.

- Create Server Pools under infrastructure Organization.

- Create UUID Suffix Pools under infrastructure Organization.

- Create Service Profile Templates under infrastructure Organization.

- Create Service Profiles under infrastructure Organization.

- Add a block of IP Addresses for KVM access.

- Backup the configuration of the running system, taking into consideration the backup location, the types of backup operations, the methods of backing up the configuration, and the need for scheduled backups.

Gather Necessary Information

Once the Cisco UCS Service Profiles have been created above, 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 as well as from the Netapp controllers. Table 3 and Table 4 detail the information that is needed for later use.

Table 3   *NetApp FAS3210A FC Portname Information*

NetApp FAS3210 A	0c or 2a	
	0d or 2b	
NetApp FAS3210 B	0c or 2a	
	0d or 2b	

Note   On each NetApp controller use the "show fcp adapters" command to gather the above information.

Table 4   *Cisco UCS Blade WWPN Information*

Cisco UCS Service Profile Name	vHBA_A WWPN	vHBA_B WWPN

Cisco Nexus 5548 Deployment Procedure—Part II

This section describes the procedures for additional Fibre Channel functionality on the Cisco Nexus 5548 platforms within the FlexPod environment and achieves the following objectives:

- Creates VSANs and VFCs, assigns FC ports to SAN Port Channels and appropriate VSANs, and turns on FC ports
- Defines Fibre Channel aliases for Service Profiles and NetApp controller target ports
- Establishes Fibre Channel Zoning and working sets

The following measures should be taken on each Nexus platform:

- Create VSANs for fabric "A" or "B" on respective Nexus platform.
- Create necessary SAN port channels to be connected to UCS Fabric Interconnect.
- Assign to VSAN appropriate FC interfaces or, alternatively for FCoE use, create vFC ports and map to the defined VSANs.
- Create device aliases on each Cisco Nexus 5548 for each service profile using corresponding fabric PWWN.
- Create device aliases on each Cisco Nexus 5548 for each service NetApp controller using corresponding fabric PWWN.
- Create zones for each service profile and assign devices as members by using Fibre Channel aliases.
- Activate the zoneset.
- Save the configuration.
- Backup the configuration of the running system, taking into consideration the backup location, the types of backup operations, the methods of backing up the configuration, and the need for scheduled backups

NetApp FAS3210A Deployment Procedure—Part II

This section describes additional procedures necessary on the NetApp controllers to provide UCS stateless boot functionality. At the end of this workflow the following objectives should be met:

- Fibre Channel target ports defined
- Fibre Channel interface groups (iGroups) defined for each service profile
- Boot LUNs allocated for each Cisco UCS service profile
- Boot LUN mapped to associated Cisco UCS service profile

The following process outlines the steps necessary:

- Create the necessary volume for boot of the UCS hosts.
- Create LUNs for booting of the UCS hosts and house them within the newly created volume.
- Create any necessary iGroups. For those OSes that support ALUA, NetApp recommends enabling ALUA on the iGroups for the host.
- Map the newly created iGroups to their respective LUNs in a 1:1 fashion.
- Following the necessary zoning, LUN creation, and mapping, you can boot the UCS host.

- Backup the configuration of the running system, taking into consideration the backup location, the types of backup operations, the methods of backing up the configuration, and the need for scheduled backups.

NetApp Operations Manager Deployment Procedure

There are a variety of choices available to manage the storage in a FlexPod environment, including NetApp FilerView, NetApp Virtual Storage Console (VSC), NetApp Operations Manager, and Microsoft Windows System Manager. The following section provides the general procedures for configuring NetApp Operations Manager, which is part of the DataFabric® Manager (DFM) 4.0 suite for use in a FlexPod environment. After completing this section the following should be available:

- A Microsoft Windows 2008 virtual machine (VM or bare metal) running NetApp DataFabric Manager Suite including:
    - Operations Manager
    - Provisioning Manager
    - Protection Manager
- NetApp Operations Manager monitoring both FlexPod storage controllers

The following section provides the procedures for configuring NetApp Operations Manager for use in a FlexPod environment.

- Install DFM on the same Windows virtual machine hosting the virtual storage controller through a Web browser (Windows).

✎

Note DFM is available at: http://now.netapp.com/NOW/download/software/dfm_win/Windows/.

- Generate a secure SSL key for the DFM HTTPs server.
- Enable HTTPs.
- Add a license in DFM server.
- Enable SNMP v3 configuration.
- Configure AutoSupport™ information.
- Run diagnostics to verify DFM communication with FlexPod controllers.
- Configure an SNMP trap host.
- Configure Operations Manager to generate e-mails for every Critical or higher event and send e-mails

Appendix—FlexPod Configuration Information

The following tables outline the information tht must be available to complete the setup and deployment of a FlexPod system.

Global Configuration Information

This information is used throughout the deployment across multiple layers in the environment.

Table 5   *FlexPod Global Configuration Information*

Name	Customized Value	Description
VLAN ID for NFS traffic		Provide the appropriate VLAN ID used for NFS traffic throughout the FlexPod environment
Network address for NFS traffic		Provide the network address for NFS VLAN traffic in CIDR notation (that is, 192.168.30.0/24)
VLAN ID for Management traffic		Provide the appropriate VLAN ID used for Management traffic throughout the FlexPod environment
VLAN ID for native VLAN		Provide the appropriate VLAN ID that will be used for the native VLAN ID throughout the FlexPod environment.
Default password		Provide the default password that will be used in initial configuration of the environment. NOTE: It is recommended to change this password as needed on each device once the initial configuration is complete.
DNS/Nameserver name		Provide the IP address of the appropriate nameserver for the environment.
Domain name suffix		Provide the appropriate domain name suffix for the environment.
VSAN ID for Fabric A		The VSAN ID that will be associated with Fabric A. This will be associated with both FC and FCoE traffic for Fabric A.
VSAN ID for Fabric B		The VSAN ID that will be associated with Fabric B. This will be associated with both FC and FCoE traffic for Fabric B.
FCoE VLAN ID for Fabric A		Provide the VLAN ID of the VLAN that will be mapped to the FCoE traffic on fabric A.
FCoE VLAN ID for Fabric B		Provide the VLAN ID of the VLAN that will be mapped to the FCoE traffic on fabric B.
SSL country name code		Provide the appropriate SSL country name code.
SSL state or province name		Provide the appropriate SSL state or province name.
SSL locality name		Provide the appropriate SSL locality name (city, town, etc.).
SSL organization name		Provide the appropriate SSL organization name (company name).
SSL organizational unit		Provide the appropriate SSL organizational unit (division).

NetApp Configuration Information

The information in Table 6 through Table 9 is specific to the NetApp portion of the deployment only.

Table 6   ***NetApp FAS3210A Configuration Information***

Name	Customized Value	Description
FAS3210 A hostname		Provide the hostname for NetApp FAS3210 A.
FAS3210 B hostname		Provide the hostname for NetApp FAS3210 B.
Netboot interface name		Designate the appropriate interface to use for initial netboot of each controller. Interface e0M is the recommended interface.
NetApp Data ONTAP 8.0.1 Netboot kernel location		Provide the full TFTP path to the 8.0.1 Data ONTAP boot image.
NetApp FAS3210 A management interface IP address		Provide the IP Address for the management interface on NetApp FAS3210 A
NetApp FAS3210 B management interface IP address		Provide the IP Address for the management interface on NetApp FAS3210 B
NetApp FAS3210 A management interface subnet mask		Provide the subnet mask for the management interface on NetApp FAS3210 A
NetApp FAS3210 B management interface subnet mask		Provide the subnet mask for the management interface on NetApp FAS3210 B.
NetApp FAS3210 A management interface gateway IP address		Provide the gateway IP address for the management interface on NetApp FAS3210 A.
NetApp FAS3210 B management interface gateway IP address		Provide the gateway IP address for the service processor interface on NetApp FAS3210 B.
NetApp FAS3210A administration host IP address		Provide the IP address of the host that will be used for administering the NetApp FAS3210A.
NetApp FAS3210A location		Provide a description of the physical location where the NetApp chassis resides.
NetApp FAS3210 A service processor interface IP address		Provide the IP address for the service processor interface on NetApp FAS3210 A.
NetApp FAS3210 B service processor interface IP address		Provide the IP address for the service processor interface on NetApp FAS3210 B.
NetApp FAS3210 A service processor interface subnet mask		Provide the subnet mask for the service processor interface on NetApp FAS3210 A.
NetApp FAS3210 B service processor interface subnet mask		Provide the subnet mask for the service processor interface on NetApp FAS3210 B.
NetApp FAS3210 A service processor interface gateway IP address		Provide the gateway IP address for the service processor interface on NetApp FAS3210 A.

Table 6 **NetApp FAS3210A Configuration Information**

Name	Customized Value	Description
NetApp FAS3210 B service processor interface gateway IP address		Provide the gateway IP address for the service processor interface on NetApp FAS3210 B.
NetApp FAS3210A Mailhost name		Provide the appropriate Mailhost name.
NetApp FAS3210A Mailhost IP address		Provide the appropriate Mailhost IP address.
NetApp DataONTAP 8.0.1 flash image location		Provide the "http" or "https" Web address of the NetApp Data ONTAP 8.0.1 flash image to install the image to the on-board flash storage.
NetApp FAS3210A administrator's e-mail address		Provide the e-mail address for the NetApp administrator to receive important alerts/messages via e-mail.
NetApp FAS3210A infrastructure vFiler IP address		Provide the IP address for the infrastructure vFiler™ unit on FAS3210A. Note: This interface will be used for the export of NFS datastores and possibly iSCSI LUNs to the necessary ESXi hosts.
NetApp FAS3210A infrastructure vFiler administration host IP		Provide the IP address of the host that will be used to administer the infrastructure vFiler unit on FAS3210A. This variable might have the same IP address as the administration host IP address for the physical controllers as well.
NetApp FAS3210B infrastructure vFiler IP address		Provide the IP address for the infrastructure vFiler unit on FAS3210B. Keep in mind that this interface will be used for the export of NFS datastores and possibly iSCSI LUNs to the necessary ESXi hosts.
NetApp FAS3210B infrastructure vFiler administration host IP address		Provide the IP address of the host that will be used to administer the infrastructure vFiler unit on FAS3210B. This variable might possibly have the same IP address as the administration host IP address for the physical controllers as well.

Table 7 **NetApp Licensing Configuration Information**

Name	Customized Value	Description
NetApp Cluster license code		Provide the license code to enable cluster mode within the FAS3210 A configuration.
NetApp Fibre Channel license code		Provide the license code to enable the Fibre Channel protocol.
NetApp Flash Cache license code		Provide the license code to enable the installed Flash Cache adapter.

Table 7　　　　**NetApp Licensing Configuration Information**

Name	Customized Value	Description
NetApp NearStore license code		Provide the license code to enable the NearStore® capability which is required to enable deduplication.
NetApp Deduplication license code		Provide the license code to enable deduplication.
NetApp NFS license code		Provide the license code to enable the NFS protocol.
NetApp MultiStore® license code		Provide the license code to enable MultiStore.
NetApp FlexClone® license code		Provide the license code to enable FlexClone.

Table 8　　　　**NetApp Disk and Volume Configuration Information**

Name	Customized Value	Description
NetApp FAS3210 A total disks attached		Number of disks assigned to controller A using software ownership. NOTE: Do not include the three disks used for the root volume in this number.
NetApp FAS3210 B total disks attached		Number of disks assigned to controller B using software ownership. NOTE: Do not include the three disks used for the root volume in this number.
NetApp FAS3210 A total disks in Aggregate 1		Number of disks to be assigned to aggr1 on controller A.
NetApp FAS3210 B total disks in Aggregate 1		Number of disks to be assigned to aggr1 on controller B.
NetApp FAS3210 A ESXi boot volume size		Each UCS server will boot using the FC protocol. Each FC LUN will be stored in a volume on either controller A or controller B. Choose the appropriate volume size depending on the environment.
NetApp FAS3210 B ESXi boot volume size		Each UCS server will boot using the FC protocol. Each FC LUN will be stored in a volume on either controller A or controller B. Choose the appropriate volume size depending on the environment.

Table 9　　　　**NetApp Data Fabric Manager Configuration Information**

Name	Customized Value	Description
NetApp DFM server hostname		Provide the hostname for the NetApp DFM server instance.
NetApp DFM server IP address		Provide the IP address to be assigned to the NetApp DFM server.

Table 9   NetApp Data Fabric Manager Configuration Information

Name	Customized Value	Description
NetApp DFM server license key		Provide the license key for the NetApp DFM server.
Mailhost IP address or hostname		Provide address of the mailhost that will be used to relay AutoSupport™ e-mails.
SNMP community string		Provide the appropriate SNMP community string.
SNMP username		Provide the appropriate SNMP username.
SNMP password		Provide the appropriate SNMP password.
SNMP Traphost		Provide the IP address or hostname for the SNMP traphost.
SNMP request role		Provides the request role for SNMP.
SNMP managers		Users who have the ability to manage SNMP.
SNMP site name		Provides the site name as required by SNMP.
Enterprise SNMP trap destination		Provides the appropriate enterprise SNMP trap destination.

Cisco Configuration Information

The information in Table 10 and Table 11 is specific to the Cisco portion of the deployment only.

Table 10   Cisco Nexus 5548 Configuration Information

Name	Customized Value	Description
Cisco Nexus 5548 A hostname		Provide the hostname for the Cisco Nexus 5548 A.
Cisco Nexus 5548 B hostname		Provide the hostname for the Cisco Nexus 5548 B.
Cisco Nexus 5548 A Management Interface IP Address		Provide the IP address for the mgmt0 interface on the Cisco Nexus 5548 A.
Cisco Nexus 5548 B Management Interface IP Address		Provide the IP address for the mgmt0 interface on the Cisco Nexus 5548 B.
Cisco Nexus 5548 A Management Interface Subnet Mask		Provide the subnet mask for the mgmt0 interface on the Cisco Nexus 5548 A.
Cisco Nexus 5548 B Management Interface Subnet Mask		Provide the subnet mask for the mgmt0 interface on the Cisco Nexus 5548 B.
Cisco Nexus 5548 A Management Interface Gateway IP Address		Provide the gateway IP address for the mgmt0 interface on the Cisco Nexus 5548 A.
Cisco Nexus 5548 B Management Interface Gateway IP Address		Provide the gateway IP address for the mgmt0 interface on the Cisco Nexus 5548 B.
Cisco Nexus 5548 Virtual Port Channel (vPC) Domain ID		Provide a unique vpc domain id for the environment.

Table 11   ***Cisco Unified Computing System Configuration Information***

Name	Customized Value	Description
Cisco UCS Fabric Interconnect A hostname		Provide the hostname for Fabric Interconnect A.
Cisco UCS Fabric Interconnect B hostname		Provide the hostname for Fabric Interconnect B.
Cisco UCS Name		Both Cisco UCS Fabric Interconnects will be clustered together as a single Cisco UCS. Provide the hostname for the clustered system.
Cisco UCS IP		Both Cisco UCS Fabric Interconnects will be clustered together as a single Cisco UCS. Provide the IP address for the clustered system.
Cisco UCS Fabric Interconnect A Management Interface IP Address		Provide the IP address for Fabric Interconnect A's Management Interface.
Cisco UCS Fabric Interconnect B Management Interface IP Address		Provide the IP address for Fabric Interconnect B's Management Interface.
Cisco UCS Fabric Interconnect A Management Netmask		Provide the subnet mask for Fabric Interconnect A's Management Interface.
Cisco UCS Fabric Interconnect B Management Interface Netmask		Provide the subnet mask for Fabric Interconnect B's Management Interface.
Cisco UCS Fabric Interconnect A Management Interface Gateway		Provide the gateway IP address for Fabric Interconnect A's Management Interface.
Cisco UCS Fabric Interconnect B Management Interface Gateway		Provide the gateway IP address for Fabric Interconnect B's Management Interface.
Cisco UCS Infrastructure Organization		A Cisco UCS organization will be created for the necessary "Infrastructure" resources. Provide a descriptive name for this organization.
Starting MAC Address for Fabric A		A pool of MAC addresses will be created for each fabric. Depending on the environment, certain MAC addresses may already be allocated. Identify a unique MAC address as the starting address in the MAC pool for Fabric A. It is recommended, if possible, to use either "0A" or "0B" as the second to last octet in order to distinguish from MACs on fabric A or fabric B.
Starting MAC Address for Fabric B		A pool of MAC addresses will be created for each fabric. Depending on the environment, certain MAC addresses may already be allocated. Identify a unique MAC address as the starting address in the MAC pool for Fabric B. It is recommended, if possible, to use either "0A" or "0B" as the second to last octet in order to more easily distinguish from MACs on fabric A or fabric B.

Table 11   *Cisco Unified Computing System Configuration Information*

Name	Customized Value	Description
Starting WWPN for Fabric A		A pool of wwpns will be created for each fabric. Depending on the environment, certain wwpns may already be allocated. Identify a unique wwpn as the starting point in the wwpn pool for Fabric A. It is recommended, if possible, to use either "0A" or "0B" as the second to last octet in order to more easily distinguish from wwpns on fabric A or fabric B.
Starting WWPN for Fabric B		A pool of wwpns will be created for each fabric. Depending on the environment, certain wwpns may already be allocated. Identify a unique wwpn as the starting point in the wwpn pool for Fabric B. It is recommended, if possible, to use either "0A" or "0B" as the second to last octet in order to more easily distinguish from wwpns on fabric A or fabric B.

NetApp FAS3200 Sample Configuration

Appliance Sample Interface Configuration

```
ntap3200-1a> ifconfig -a
c0a: flags=0x354a867<UP,BROADCAST,RUNNING,MULTICAST,TCPCKSUM> mtu 9000 PRIVATE
inet 192.168.1.85 netmask-or-prefix 0xffffff00 broadcast 192.168.1.255
ether 00:a0:98:13:d2:d0 (auto-unknown-enabling) flowcontrol full
c0b: flags=0x3d4a867<UP,BROADCAST,RUNNING,MULTICAST,TCPCKSUM> mtu 9000 PRIVATE
inet 192.168.2.135 netmask-or-prefix 0xffffff00 broadcast 192.168.2.255
ether 00:a0:98:13:d2:d1 (auto-10g_kr-fd-up) flowcontrol full
e0M: flags=0x694c867<UP,BROADCAST,RUNNING,MULTICAST,TCPCKSUM,NOWINS> mtu 1500
inet 10.61.185.144 netmask-or-prefix 0xffffff00 broadcast 10.61.185.255
partner e0M (not in use)
ether 00:a0:98:13:d2:d2 (auto-100tx-fd-up) flowcontrol full
e0P: flags=0x2d4c867<UP,BROADCAST,RUNNING,MULTICAST,TCPCKSUM> mtu 1500
inet 192.168.2.48 netmask-or-prefix 0xfffffc00 broadcast 192.168.3.255 noddns
ether 00:a0:98:13:d2:d3 (auto-100tx-fd-up) flowcontrol full
e0a: flags=0x250c866<BROADCAST,RUNNING,MULTICAST,TCPCKSUM> mtu 1500
ether 00:a0:98:13:d2:ce (auto-unknown-cfg_down) flowcontrol full
e0b: flags=0x250c866<BROADCAST,RUNNING,MULTICAST,TCPCKSUM> mtu 1500
ether 00:a0:98:13:d2:cf (auto-unknown-cfg_down) flowcontrol full
e2a: flags=0x8bd0a867<BROADCAST,RUNNING,MULTICAST,TCPCKSUM,VLAN> mtu 9000
ether 02:a0:98:13:d2:d0 (auto-10g_sr-fd-up) flowcontrol full
trunked vif0
e2b: flags=0x8bd0a867<BROADCAST,RUNNING,MULTICAST,TCPCKSUM,VLAN> mtu 9000
ether 02:a0:98:13:d2:d0 (auto-10g_sr-fd-up) flowcontrol full
trunked vif0
lo: flags=0x1948049<UP,LOOPBACK,RUNNING,MULTICAST,TCPCKSUM> mtu 8160
inet 127.0.0.1 netmask-or-prefix 0xff000000 broadcast 127.0.0.1
ether 00:00:00:00:00:00 (RNIC Provider)
vif0: flags=0xa3d0a863<BROADCAST,RUNNING,MULTICAST,TCPCKSUM,VLAN> mtu 9000
ether 02:a0:98:13:d2:d0 (Enabled virtual interface)
vif0-900: flags=0x394a863<UP,BROADCAST,RUNNING,MULTICAST,TCPCKSUM> mtu 9000
inet 192.168.90.144 netmask-or-prefix 0xffffff00 broadcast 192.168.90.255
partner vif0-900 (not in use)
```

```
ether 02:a0:98:13:d2:d0 (Enabled virtual interface)
```

Sample Startup Information Configuration

```
ntap3200-1a> rdfile /etc/rc
hostname ntap3200-1a
vif create lacp vif0 -b ip e1a e1b
vlan create vif0 3150 900
ifconfig e0M `hostname`-e0M netmask 255.255.255.0 mtusize 1500 -wins flowcontrol full
partner e0M
route add default 10.61.185.1 1
routed on
options dns.domainname rtp.netapp.com
options dns.enable on
options nis.enable off
savecore
vlan create vif0 900
ifconfig vif0-900 mtusize 9000
ifconfig vif0-900 partner vif0-900
ifconfig vif0-900 192.168.90.144 netmask 255.255.255.0
vlan add vif0 3150
ifconfig vif0-3150 `hostname`-vif0-3150 netmask 255.255.255.0 mtusize 1500 -wins partner
vif0-3150
ifconfig vif0-3150 192.168.150.1 netmask 255.255.255.0
```

Sample Volume Information

```
ntap3200-1a> vol status
         Volume State           Status           Options
infrastructure_root online         raid_dp, flex     guarantee=none,
                                                      fractional_reserve=0
           vol0 online           raid_dp, flex     root
infrastructure_datastore_1 online         raid_dp, flex     guarantee=none,
                                 sis                 fractional_reserve=0
esxi_boot_A online           raid_dp, flex     guarantee=none,
                                 sis                 fractional_reserve=0
```

Sample LUN Information

```
ntap3200-1a> lun show -m
LUN path                              Mapped to         LUN ID  Protocol
-----------------------------------------------------------------------
/vol/esxi_boot_A/ucs2b-1-sc    ucs2b-1-sc_A         0        FCP
                                    ucs2b-1-sc_B         0       FCP
```

Sample Initiator Group (iGroup) Information

```
ntap3200-1a> igroup show
    ucs2b-1-sc_A (FCP) (ostype: "Hypervisor or Bare Metal":
        20:00:00:25:b5:00:0a:9f (logged in on: 0c)
    ucs2b-1-sc_B (FCP) (ostype: "Hypervisor or Bare Metal"):
        20:00:00:25:b5:00:0b:df (logged in on: 0d)
```

Sample vFiler Unit Structure

```
ntap3200-1a> vfiler status
vfiler0                          running
```

```
infrastructure_1_vfiler          running
```

Sample List of Defined ipspaces and Interface Assignment

```
ntap3200-1a> ipspace list
Number of ipspaces configured: 3
default-ipspace              (e0M e0P e0a e0b )
infrastructure               (vif0-900 )
```

Sample vFiler Unit Context Route Configuration

```
infrastructure_1_vfiler@ntap3200-1a> route -s
Routing tables

Internet:
Destination      Gateway        Flags     Refs     Use  Interface
192.168.90       link#12        UC          0        0  vif0-900
192.168.90.109   0:50:56:70:f8:9a  UHL       2      409  vif0-900
192.168.90.110   0:50:56:77:8a:ac  UHL       2     5181  vif0-900
192.168.90.111   0:50:56:70:c0:80  UHL       2        9  vif0-900
192.168.90.112   0:50:56:7b:df:f9  UHL       2        9  vif0-900
192.168.90.117   0:50:56:a0:0:0    UHL       0       18  vif0-900
```

Sample vFiler Unit Context Exported Directories and Files

```
infrastructure_1_vfiler@ntap3200-1a> exportfs
/vol/infrastructure_datastore_1-sec=sys,rw=192.168.90.109:192.168.90.110:192.168.90.111:19
2.168.90.112:192.168.95.10,root=192.168.90.109:192.168.90.110:192.168.90.111:192.168.90.11
2:192.168.95.10
/vol/infrastructure_root-sec=sys,rw,anon=0
```

Cisco Nexus 5548 Sample Running Configuration

```
!Command: show running-config
!Time: Wed Aug 10 11:35:26 2011

version 5.0(3)N1(1c)
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 $1$JpsspOIX$jk0ujNUh8cxcm2b7lOEaG0  role network-admin
ip domain-lookup
switchname ice5548-1
system jumbomtu 9000
logging event link-status default
ip access-list classify_COS_4
  10 permit ip 192.168.102.0/24 any
  20 permit ip any 192.168.102.0/24
ip access-list classify_COS_5
  10 permit ip 192.168.101.0/24 any
  20 permit ip any 192.168.101.0/24
class-map type qos class-fcoe
```

```
class-map type qos match-all Silver_Traffic
  match access-group name classify_COS_4
class-map type qos match-all Platinum_Traffic
  match access-group name classify_COS_5
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
policy-map type qos Global_Classify
  class Platinum_Traffic
    set qos-group 2
  class Silver_Traffic
    set qos-group 4
  class class-fcoe
    set qos-group 1
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 Silver_Traffic_NQ
  match qos-group 4
class-map type network-qos class-ip-multicast
  match qos-group 2
class-map type network-qos Platinum_Traffic_NQ
  match qos-group 2
policy-map type network-qos Setup_QOS
  class type network-qos Platinum_Traffic_NQ
    set cos 5
    mtu 9000
  class type network-qos Silver_Traffic_NQ
    set cos 4
    mtu 9000
  class type network-qos class-fcoe
    pause no-drop
    mtu 2158
  class type network-qos class-default
    multicast-optimize
system qos
  service-policy type qos input Global_Classify
  service-policy type queuing input fcoe-default-in-policy
  service-policy type queuing output fcoe-default-out-policy
  service-policy type network-qos Setup_QOS
snmp-server user admin network-admin auth md5 0x91d2518e00e2d50e9e5d213bee818692 priv
0x91d2518e00e2d50e9e5d213bee818692 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 101
  fcoe vsan 101
  name FCoE_Fabric_A
vlan 186
  name MGMT-VLAN
vlan 3101
  name NFS-VLAN
vlan 3102
  name vMotion-VLAN
vlan 3103
  name Packet-Control-VLAN
vlan 3104
  name VM-Traffic-VLAN
```

```
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
spanning-tree port type network default
vpc domain 23
  role priority 10
  peer-keepalive destination 10.61.185.70 source 10.61.185.69
vsan database
  vsan 101 name "Fabric_A"
device-alias database
  device-alias name ice3270-1a_2a pwwn 50:0a:09:81:8d:dd:92:bc
  device-alias name ice3270-1b_2a pwwn 50:0a:09:81:9d:dd:92:bc
  device-alias name esxi41_host_ice3270-1a_2a1_A pwwn 20:00:00:25:b5:00:0a:0f
  device-alias name esxi41_host_ice3270-1b_2b1_A pwwn 20:00:00:25:b5:00:0a:1f

device-alias commit

fcdomain fcid database
  vsan 1 wwn 20:42:00:05:9b:79:7a:80 fcid 0x800000 dynamic
  vsan 1 wwn 20:41:00:05:9b:79:7a:80 fcid 0x800001 dynamic
  vsan 101 wwn 50:0a:09:81:8d:dd:92:bc fcid 0x4e0000 dynamic
!              [ice3270-1a_2a]
  vsan 101 wwn 50:0a:09:81:9d:dd:92:bc fcid 0x4e0001 dynamic
!              [ice3270-1b_2a]
  vsan 101 wwn 20:42:00:05:9b:79:7a:80 fcid 0x4e0002 dynamic
  vsan 101 wwn 20:41:00:05:9b:79:7a:80 fcid 0x4e0003 dynamic
  vsan 101 wwn 20:00:00:25:b5:00:0a:0f fcid 0x4e0004 dynamic
!              [esxi41_host_ice3270-1a_2a1_A]
  vsan 101 wwn 20:00:00:25:b5:00:0a:1f fcid 0x4e0005 dynamic
!              [esxi41_host_ice3270-1b_2b1_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 186,3101-3104
  spanning-tree port type network

interface port-channel11
  description ice3270-1a
  switchport mode trunk
  vpc 11
  switchport trunk native vlan 2
  switchport trunk allowed vlan 101-102,186,3101
  spanning-tree port type edge trunk

interface port-channel12
  description ice3270-1b
  switchport mode trunk
  vpc 12
  switchport trunk native vlan 2
  switchport trunk allowed vlan 101-102,186,3101
  spanning-tree port type edge trunk

interface port-channel13
  description iceucsm-2a-m
  switchport mode trunk
  vpc 13
  switchport trunk native vlan 2
  switchport trunk allowed vlan 186,3101-3104
```

```
        spanning-tree port type edge trunk

interface port-channel14
  description iceucsm-2b-m
  switchport mode trunk
  vpc 14
  switchport trunk native vlan 2
  switchport trunk allowed vlan 186,3101-3104
  spanning-tree port type edge trunk

interface port-channel20
  description Po20:iceds-1:Po12
  switchport mode trunk
  vpc 20
  switchport trunk native vlan 2
  switchport trunk allowed vlan 186
  spanning-tree port type

!Command: show running-config
!Time: Wed Aug 10 11:36:57 2011

version 5.0(3)N1(1c)
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 $1$PBq/n2.b$g8jK3jqj8MelNDQKGRBD50  role network-admin
ip domain-lookup
switchname ice5548-2
system jumbomtu 9000
logging event link-status default
ip access-list classify_COS_4
  10 permit ip 192.168.102.0/24 any
  20 permit ip any 192.168.102.0/24
ip access-list classify_COS_5
  10 permit ip 192.168.101.0/24 any
  20 permit ip any 192.168.101.0/24
class-map type qos class-fcoe
class-map type qos match-all Silver_Traffic
  match access-group name classify_COS_4
class-map type qos match-all Platinum_Traffic
  match access-group name classify_COS_5
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
policy-map type qos Global_Classify
  class Platinum_Traffic
    set qos-group 2
  class Silver_Traffic
    set qos-group 4
  class class-fcoe
    set qos-group 1
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 Silver_Traffic_NQ
  match qos-group 4
class-map type network-qos class-ip-multicast
  match qos-group 2
class-map type network-qos Platinum_Traffic_NQ
  match qos-group 2
policy-map type network-qos Setup_QOS
  class type network-qos Platinum_Traffic_NQ
    set cos 5
    mtu 9000
  class type network-qos Silver_Traffic_NQ
    set cos 4
    mtu 9000
  class type network-qos class-fcoe
    pause no-drop
    mtu 2158
  class type network-qos class-default
    multicast-optimize
system qos
  service-policy type qos input Global_Classify
  service-policy type queuing input fcoe-default-in-policy
  service-policy type queuing output fcoe-default-out-policy
  service-policy type network-qos Setup_QOS
snmp-server user admin network-admin auth md5 0x7021e5331f25b481ed3ad26b96ccd729 priv
0x7021e5331f25b481ed3ad26b96ccd729 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 102
  fcoe vsan 102
  name FCoE_Fabric_B
vlan 186
  name MGMT-VLAN
vlan 3101
  name NFS-VLAN
vlan 3102
  name vMotion-VLAN
vlan 3103
  name Packet-Control-VLAN
vlan 3104
  name VM-Traffic-VLAN
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_2b pwwn 50:0a:09:82:8d:dd:92:bc
  device-alias name ice3270-1b_2b pwwn 50:0a:09:82:9d:dd:92:bc
  device-alias name esxi41_host_ice3270-1a_2a1_B pwwn 20:00:00:25:b5:00:0b:0f
  device-alias name esxi41_host_ice3270-1b_2b1_B pwwn 20:00:00:25:b5:00:0b:1f

device-alias commit

fcdomain fcid database
  vsan 1 wwn 20:42:00:05:9b:6f:7a:40 fcid 0x590000 dynamic
  vsan 1 wwn 20:41:00:05:9b:6f:7a:40 fcid 0x590001 dynamic
  vsan 102 wwn 50:0a:09:82:9d:dd:92:bc fcid 0xae0000 dynamic
!               [ice3270-1b_2b]
```

```
  vsan 102 wwn 50:0a:09:82:8d:dd:92:bc fcid 0xae0001 dynamic
!             [ice3270-1a_2b]
  vsan 102 wwn 20:42:00:05:9b:6f:7a:40 fcid 0xae0002 dynamic
  vsan 102 wwn 20:41:00:05:9b:6f:7a:40 fcid 0xae0003 dynamic
  vsan 102 wwn 20:00:00:25:b5:00:0b:0f fcid 0xae0004 dynamic
!             [esxi41_host_ice3270-1a_2a1_A]
  vsan 102 wwn 20:00:00:25:b5:00:0b:1f fcid 0xae0005 dynamic
!             [esxi41_host_ice3270-1b_2b1_A]


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 186,3101-3104
  spanning-tree port type network

interface port-channel11
  description ice3270-1a
  switchport mode trunk
  vpc 11
  switchport trunk native vlan 2
  switchport trunk allowed vlan 101-102,186,3101
  spanning-tree port type edge trunk

interface port-channel12
  description ice3270-1b
  switchport mode trunk
  vpc 12
  switchport trunk native vlan 2
  switchport trunk allowed vlan 101-102,186,3101
  spanning-tree port type edge trunk

interface port-channel13
  description iceucsm-2a-m
  switchport mode trunk
  vpc 13
  switchport trunk native vlan 2
  switchport trunk allowed vlan 186,3101-3104
  spanning-tree port type edge trunk

interface port-channel14
  description iceucsm-2b-m
  switchport mode trunk
  vpc 14
  switchport trunk native vlan 2
  switchport trunk allowed vlan 186,3101-3104
  spanning-tree port type edge trunk

interface port-channel20
  description Po20:iceds-1:Po12
  switchport mode trunk
  vpc 20
  switchport trunk native vlan 2
  switchport trunk allowed vlan 186
  spanning-tree port type net
```

Cisco Unified Computing System Configuration Extracts

All configurations in this section occur after the initial UCS cluster setup scripts have completed and the UCS Manager is accessible to the administrator. Use the configuration information described above to execute the setup script and complete the deployment required in your environment.

For more information on the initial setup of Cisco UCS Manager, go to: http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html and select the appropriate release of the "System Configuration" documentation.

Cisco Unified Computing System Configuration Examples and TechNotes

The latest Cisco UCS configuration examples and TechNotes may be found at: http://www.cisco.com/en/US/products/ps10281/prod_configuration_examples_list.html.

Sample Cisco Unified Computing System Initial CLI 1.4

The following video provides an example of the initial configuration of UCS from the command line interface: http://www.youtube.com/watch?v=86H_4lOeXfA&feature=related

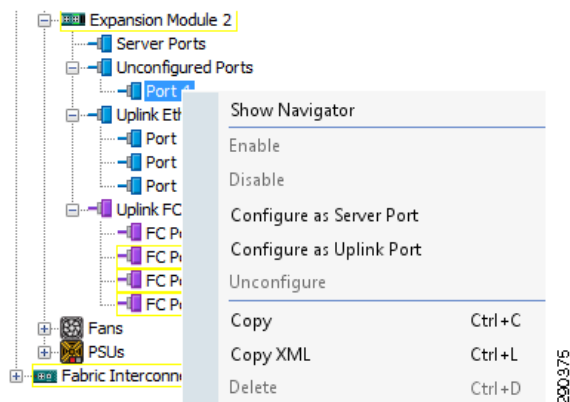## Sample Chassis Discovery Policy Configuration

Define the Chassis Discovery Policy to reflect the number of links from the chassis to the fabric interconnects. At a minimum FlexPod requires two links.

Figure 4   *Chassis Discovery Policy Screen*
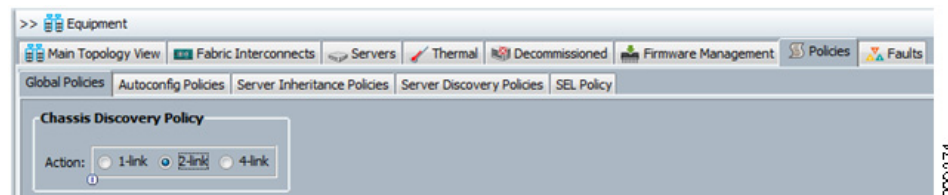
Define and enable Fibre Channel, Server, and Uplink Ports.

Figure 5   *Fibre Channel Server and Uplink Ports Screen*

The physical display after completing this procedure is shown in Figure 6.

Figure 6   *Physical Display after Procedure Completion*

Create an Organization

The use of organizations allows the physical UCS resources to be logically divided. Each organization can have its own policies, pools, and quality of service definitions. Organizations are hierarchical in nature, allowing sub-organizations to inherit characteristics from higher organizations or establish their policies, pools, and service definitions.

To create an Organization, go to the Main panel **New** menu drop-down list and select **Create Organization** to create an organization which manages the FlexPod infrastructure and owns the logical building blocks.

Figure 7 *Create Organization Screen*

Cisco Unified Computing System—Working with Pools, Policies, and Templates

The following video provides examples and instructions for working with pools, policies, and templates for the Cisco Unified Computing System:
http://www.youtube.com/watch?v=obmenIF4ggU&feature=related.

This UCS video covers the following topics.

Pools

Create MAC Address

Create vNIC

Create VLANs

Create VSANs

Create WWPNs

Servers

WWNN

UUID

Templates

vNIC

vHBA

Service Profile

Polices

QoS

Network Control

Pin Group

Boot

Power Control

Firmware

BIOS

Adapter

FC Port Channel and Trunking

The following video provides instructions and examples for setting up Fiber Channel port channel and trunking: http://www.youtube.com/watch?v=PpzKPguRTXc&feature=related.

Cisco Unified Computing System Block of IP Addresses for KVM Access

The following video provides instructions and examples for setting up the KVM address pool: http://www.youtube.com/watch?v=d0KTYItdU6g&NR=1.

References

- Cisco Nexus 5548 Switch: http://www.cisco.com/en/US/products/ps11215/index.html
- Cisco Unified Computing System: http://www.cisco.com/en/US/netsol/ns944/index.html
- NetApp FAS3210 Storage Controller: http://now.netapp.com/NOW/knowledge/docs/hardware/hardware_index.shtml#Storage%20appliances%20and%20V-series%20systems/gFilers
- NetApp Support (formerly NetApp on the Web (NOW®) site: http://.now.netapp.com