# FlexPod for VMware Deployment Model

Last Updated: February 24, 2011

Cisco Validated Design

Building Architectures to Solve Business Problems

# About the Authors

Chris O'Brien

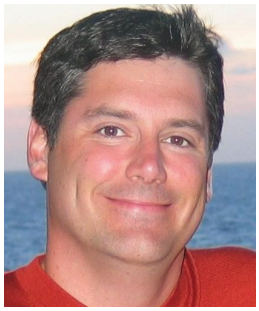
## Chris O'Brien, Solutions Architect, Systems Architecture and Strategy, Cisco Systems

Chris O'Brien is a Solutions Architect for data center technologies in Cisco's Systems Architecture and Strategy group. He is currently focused on data center design validation and application optimization. Previously, O'Brien was an application developer and has been working in the IT industry for more than 15 years.

John George

## John George, Reference Architect, Infrastructure and Cloud Enablement, NetApp

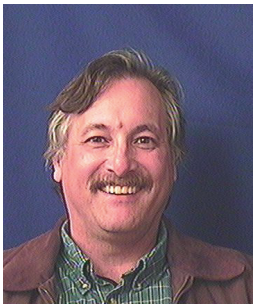
John George is a Reference Architect in NetApp's Infrastructure and Cloud Engineering group and is focused on developing, validating, and supporting cloud infrastructure solutions that include NetApp products. Before his current role, he supported and administrated Nortel's worldwide training network and VPN infrastructure. John holds a Master's Degree in Computer Engineering from Clemson University.



Mike Flannery

## Mike Flannery, Manager, High Velocity Technical Sales, NetApp

Mike Flannery leads the High Velocity Technical Sales group. Mike and his team focus on architecting, sizing, and validating NetApp storage configurations for customers in the Midsized Enterprise space. Mike has been with NetApp for 6 years and prior to NetApp Mike worked at Informix Software and IBM where he focused on Database and Data Management solutions.



Mark Hayakawa

## Mark Hayakawa, Technical Sales Architect, High Velocity Sales, NetApp

Mark Hayakawa is a Technical Sales Architect in the High Velocity Sales group. His primary duty is the creation, validation, and documentation of storage system configurations for the Mid Size Enterprise. Mark has been with NetApp for 10 years and in prior roles, he was a Technical Marketing Engineer supporting DB2, SAS, Lotus, SnapLock, and Storage Efficiency as well as a Field Technical Lead supporting archive and compliance.

Dustin Schoenbrun

## Dustin Schoenbrun, Systems Architect, Infrastructure and Cloud Enablement, NetApp

Dustin Schoenbrun is a Systems Architect in NetApp's Infrastructure and Cloud Engineering team who tests, validates, and documents solutions based on NetApp and other various vendor technologies. Before working for NetApp, he worked for the University of New Hampshire InterOperability Laboratory (UNH-IOL) where he tested next generation storage devices and developed test tools for FCoE devices.

Mike Zimmerman

## Mike Zimmerman, Reference Architect, Infrastructure and Cloud Enablement, NetApp

Mike Zimmerman is a Reference Architect in NetApp's Infrastructure and Cloud Engineering team. He focuses on the implementation, compatibility, and testing of various vendor technologies to develop innovative end-to-end cloud solutions for customers. Zimmerman started his career at NetApp as an architect and administrator of Kilo Client, NetApp's internal cloud infrastructure, where he gained extensive knowledge and experience building end-to-end shared architectures based upon server, network, and storage virtualization.

Wen Yu

## Wen Yu, Senior Infrastructure Technologist, VMware

Wen Yu is a Sr. Infrastructure Technologist at VMware, with a focus on partner enablement and evangelism of virtualization solutions. Wen has been with VMware for six years during which time four years have been spent providing engineering level escalation support for customers. Wen specializes in virtualization products for continuous availability, backup recovery, disaster recovery, desktop, and vCloud. Wen Yu is VMware, Red Hat, and ITIL certified.

Alan Crouch

## Alan Crouch, Technical Architect, Enterprise Infrastructure Management Solutions, NetApp

Alan Crouch is a Technical Architect in the Enterprise Infrastructure Management Solutions team, based out of NetApp's Sunnyvale Corporate Headquarters. He is focused on developing integrated storage management and automated provisioning solutions utilizing NetApp and partner technologies.

Alan is a seasoned IT professional with a career that spans nineteen years, in which time he has developed systems for a wide variety of businesses. As an experienced systems engineer, Alan has designed, built, documented, and managed application delivery solutions for companies in several industries including healthcare, ecommerce, network infrastructure, marketing, and high technology.

Ganesh Kamath

## Ganesh Kamath, Technical Architect, Enterprise Infrastructure Management Solutions, NetApp

Ganesh Kamath is a Technical Architect in NetApp's Enterprise Infrastructure Management Solutions team and is based in NetApp Bangalore. His focus is on storage infrastructure management solutions that include NetApp software as well as partner orchestration solutions. Ganesh's diverse experiences at NetApp include working as a Technical Marketing Engineer as well as a member of NetApp's Rapid Response Engineering team qualifying specialized solutions for our most demanding customers.

# 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 for VMware Deployment Model

# FlexPod for VMware Deployment Model

## FlexPod for VMware 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, NetApp® FAS storage components, and 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, NetApp, and VMware® have developed FlexPod for VMware as a platform that can address current virtualization needs and simplify their evolution to ITaaS infrastructure. FlexPod for VMware is built on the FlexPod infrastructure stack with added VMware components including VMware vSphere™, vCenter™ for virtualized application workloads.

FlexPod for VMware serves as a base infrastructure layer for a variety of IT solutions. A detailed study of six practical solutions deployed on FlexPod for VMware, including VDI with VMware View™ and Enhanced Secure Multi-tenancy, can be found in *FlexPod for VMware Solutions Guide* at: http://media.netapp.com/documents/tr-3884.pdf.

NetApp partners can access the *FlexPod Implementation Guide* at: https://fieldportal.netapp.com/viewcontent.asp?qv=1&docid=30428.

## Audience

This document describes the basic architecture of FlexPod for VMware as well as the general procedures for deploying a base FlexPod for VMware configuration. 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 for VMware architecture.

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

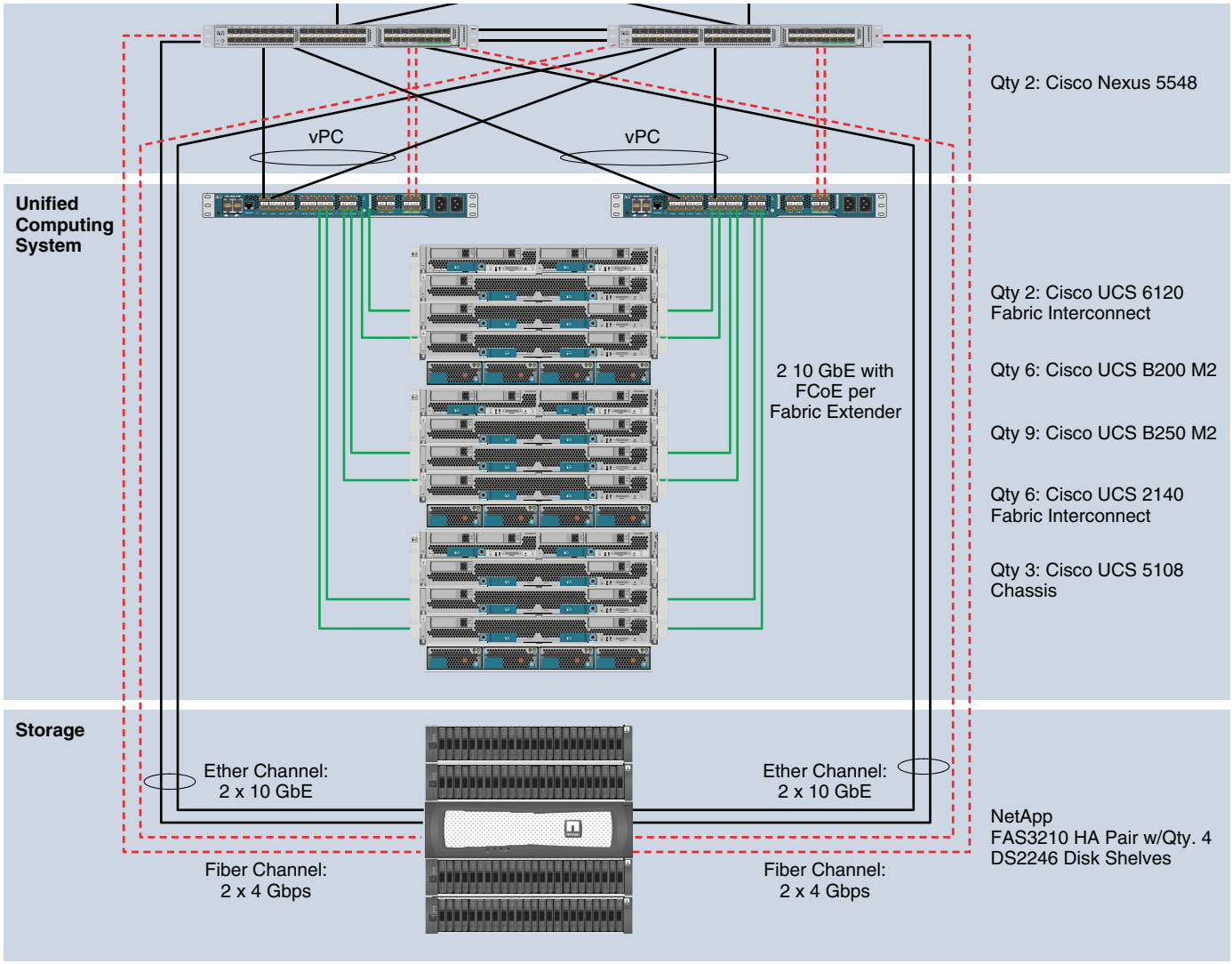
**Corporate Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# FlexPod for VMware Architecture

As the name details, the FlexPod architecture is highly modular or "pod" like. While each customer's FlexPod 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 an integrated building block for all virtualization solutions. FlexPod for VMware includes NetApp storage, Cisco networking, the Cisco Unified Computing System (Cisco UCS), and VMware virtualization software in a single package in which the computing and storage fit in one data center rack with the networking residing in a separate rack. Due to port density the networking components can accommodate multiple FlexPod for VMware configurations. Figure 1 shows the FlexPod for VMware components.

***Figure 1 FlexPod for VMware Components***




The default hardware involved 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 for end-to-end high availability. For server virtualization, the deployment includes VMware vSphere Enterprise Plus with vCenter Standard. 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 IO capacity and throughput, or special hardware or software features could be added to introduce new features (such as NetApp FlashCache for dedupe-aware caching or VMware View for VDI deployments).

The remainder of this document will guide 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 to configuring virtualization with VMware vSphere.

# FlexPod for VMware Configuration Deployment

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

## Cabling Information

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

**Note** The following tables are for the prescribed and supported configuration of the FAS3210 running Data ONTAP 7.3.5. This configuration leverages the onboard FC storage target ports, a dual-port 10GbE add-on adapter, and the onboard SAS ports for disk shelf connectivity. For any modifications of this prescribed architecture, consult the currently available Interoperability Matrix Tool (IMT): http://now.netapp.com/matrix.

**Note** The FlexPod for VMware 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 result in necessary changes to the deployment procedures that follow as specific port locations are mentioned.

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

*Table 1 FlexPod for VMware Ethernet Cabling Information*

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| Cisco Nexus[1] 5548 A | Eth1/1 | 10GbE | NetApp Controller A | e2a |
| | Eth1/2 | 10GbE | NetApp Controller B | e2a |
| | Eth1/5 | 10GbE | Cisco Nexus 5548 B | Eth1/5 |
| | Eth1/6 | 10GbE | Cisco Nexus 5548 B | Eth1/6 |
| | Eth1/7 | 1GbE | Cisco Nexus 1010 A | Eth1 |
| | Eth1/8 | 1GbE | Cisco Nexus 1010 B | Eth1 |
| | Eth1/9 | 10GbE | Cisco UCS Fabric Interconnect A | Eth1/7 |
| | Eth1/10 | 10GbE | Cisco UCS Fabric Interconnect B | Eth1/7 |
| | MGMT0 | 100MbE | 100MbE Management Switch | Any |
| Cisco Nexus[1] 5548 B | Eth1/1 | 10GbE | NetApp Controller A | e2b |
| | Eth1/2 | 10GbE | NetApp Controller B | e2b |
| | Eth1/5 | 10GbE | Cisco Nexus 5548 A | Eth1/5 |
| | Eth1/6 | 10GbE | Cisco Nexus 5548 A | Eth1/6 |
| | Eth1/7 | 1GbE | Cisco Nexus 1010 A | Eth2 |
| | Eth1/8 | 1GbE | Cisco Nexus 1010 B | Eth2 |
| | Eth1/9 | 10GbE | Cisco UCS Fabric Interconnect A | Eth1/8 |
| | Eth1/10 | 10GbE | Cisco UCS Fabric Interconnect B | Eth1/8 |
| | MGMT0 | 100MbE | 100MbE Management Switch | Any |
| NetApp Controller A | e0M | 100MbE | 100MbE Management Switch | Any |
| | e0P | 1GbE | SAS shelves | ACP port |
| | e2a | 10GbE | Nexus 5548 A | Eth1/1 |
| | e2b | 10GbE | Nexus 5548 B | Eth1/1 |
| NetApp Controller B | e0M | 100MbE | 100MbE management switch | any |
| | e0P | 1GbE | SAS shelves | ACP port |
| | e2a | 10GbE | Nexus 5548 A | Eth1/2 |
| | e2b | 10GbE | Nexus 5548 B | Eth1/2 |

*Table 1 FlexPod for VMware Ethernet Cabling Information*

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| Cisco UCS Fabric Interconnect | Eth1/7 | 10GbE | Nexus 5548 A | Eth1/9 |
| | Eth1/8 | 10GbE | Nexus 5548 B | Eth1/9 |
| | 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 | Eth1/7 | 10GbE | Nexus 5548 A | Eth1/10 |
| | Eth1/8 | 10GbE | Nexus 5548 B | Eth1/10 |
| | 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 |
| Nexus 1010 A | Eth1 | 1GbE | Nexus 5548 A | Eth1/7 |
| | Eth2 | 1GbE | Nexus 5548 B | Eth1/7 |
| Nexus 1010 B | Eth1 | 1GbE | Nexus 5548 A | Eth1/8 |
| | Eth2 | 1GbE | Nexus 5548 B | Eth1/8 |

1. The Cisco Nexus 1010 virtual appliances require the use of two 1GbE Copper SFP+'s (GLC-T=).

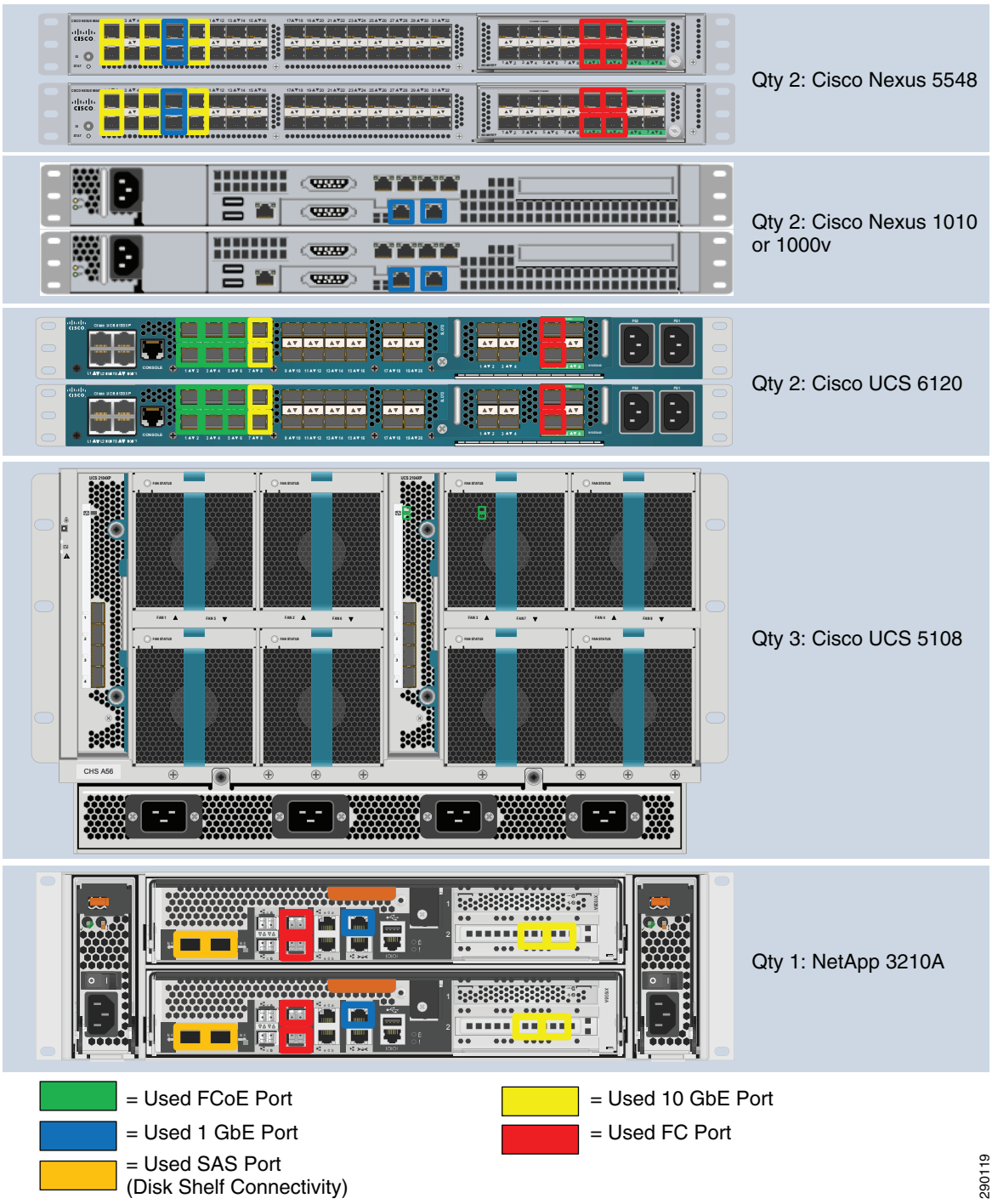
*Table 2 FlexPod for VMware Fibre Channel Cabling Information*

| 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 |

*Table 2 FlexPod for VMware Fibre Channel Cabling Information*

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---|---|---|---|---|
| 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 |
| 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 2 FlexPod Cabling*




# NetApp FAS3210A Deployment Procedure—Part I

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

- Establishment of a functional Data ONTAP 7.3.5 failover cluster with proper licensing
- Creation of data aggregates
- Creation of Flex volumes
- Configure NFS exports
- Creation of infrastructure vFiler

The following measures should be taken to meet these objectives:

- Assign the Controller Disk Ownership.
- Downgrade from Data ONTAP 8.0.1 to 7.3.5.

**Note** This step is not necessary if Data ONTAP 7.3.5 is already installed on your storage controllers.

- Set up Data ONTAP 7.3.5.
- Install Data ONTAP to the Onboard Flash Storage.
- Install Required Licenses.
- Start FCP service and ensure 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).
- Create the Infrastructure IP Space.
- Create the Infrastructure vFiler units.
- Map the necessary infrastructure volumes to the infrastructure vFiler.
- Export the infrastructure volumes to the ESXi servers over NFS.
- 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 for VMware and achieves the following objectives:

- Establish a functional pair of Cisco Nexus 5548 switches with proper licensing and feature enabled.
- Establish connectivity between FlexPod elements including via 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 for VMware environment.

- Execute the Cisco Nexus 5548 setup script.
- Enable the appropriate Cisco Nexus features and licensing.
- Set Global Configurations.
- Create Necessary VLANs including NFS, management, vMotion, Nexus 1000v control and packet, as well as VM data VLANs.
- 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 via vPC.
- Configure trunk ports for the Cisco Nexus 1010 virtual appliances.
- 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 for VMware 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, 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 which manages the FlexPod infrastructure and owns the logical building blocks.

- Create MAC Address Pools under infrastructure organization.
- Create global VLANs, including NFS, vMotion, Nexus 1000v control and packet, as well as VM data VLANs.
- Create a Network Control Policy under infrastructure Organization.
- Create vNIC Template under infrastructure Organization using previously defined pools.
- Create 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.

# Gather Necessary Information

Once the Cisco UCS Service Profiles have been created above, the infrastructure blades in the environment each have a unique configuration. In order to proceed with the FlexPod for VMware deployment, specific information must be gathered from each Cisco UCS blade as well as 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 | |
| | 0d | |
| NetApp FAS3210 B | 0c | |
| | 0d | |

**Note** On each NetApp controller use the “show fcp adapters” 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 for VMware environment and achieves the following objectives:

- Dedicated VSANs for each Fibre Channel fabric
- Allocates ports as Fibre Channel resources
- Defines Fibre Channel aliases for Service Profiles and NetApp controller 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.
- Assign to VSAN appropriate FC interfaces.
- 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 via Fibre Channel aliases.
- Activate the zoneset.
- Save the configuration.

# 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 igroups.
- Create LUNs for the Service Profiles.
- Map LUNs to igroups.

# VMware ESXi Deployment Procedure

This section describes the installation of ESXi on the Cisco UCS and should result in the following:

- A functional ESXi host
- NFS and vMotion network connectivity
- Availability of NFS datastores to the ESXi host

The following outlines the process for installing VMware ESXi within a FlexPod for VMware environment.

- VMware ESXi Deployment via UCSM KVM Console.

  There are multiple methods for installing ESXi within such an environment. In this case, an ISO image is mounted to via the KVM console to make ESXi accessible to the blade.
- Set up the ESXi Host's Administration Password.
- Set up the ESXi Host's Management Networking.
- Set up the management VLAN.
- Set up DNS.
- Set up the NFS and VMotion VMkernel ports with Jumbo Frames MTU.
- Access the ESXi host via Web browser and download VMware vSphere Client.
- Log into VMware ESXi Host using VMware vSphere Client.
- Set up the vMotion VMkernel Port on the Virtual Switch for individual hosts.
- Change VLAN ID for default VM-Traffic Port-group called "VM-Network".
- Mount the Required datastores for individual hosts.
- Set NTP time configuration for individual hosts.
- Move the swapfile from local to NFS export location.

# VMware vCenter Server Deployment Procedure

The following section describes the installation of VMware vCenter within a FlexPod for VMware environment and results in the following:

- A running VMware vCenter virtual machine
- A running SQL virtual machine acting as the vCenter database server
- A vCenter DataCenter with associated ESXi hosts
- VMware DRS and HA functionality enabled

The deployment procedures necessary to achieve these objectives include:

- Log into VMware ESXi Host using VMware vSphere Client.
- Build a SQL Server VM using Windows Server 2008 R2 x64 image.
- Create the required databases and database users. Use the script provided in the vCenter installation directory.

**Note** VMware vCenter can use one of a number of vendor Databases. This deployment guide assumes Microsoft SQL Server 2008. If a database server already exists and it is compatible with vCenter you can create the required database instance for vCenter and skip this step.

- Build a vCenter virtual machine on another Windows Server 2008 R2 virtual machine instance.
- Install SQL Server 2008 R2 Native Client on the vCenter virtual machine.
- Create Data Source Name referencing the SQL instance on the vCenter machine.
- Install VMware vCenter Server referencing the SQL server data source previously established.
- Create a vCenter Datacenter.
- Create a new management cluster with DRS and HA enabled.

- Add Hosts to the management cluster.

# Cisco Nexus 1010 and 1000V Deployment Procedure

The following section outlines the procedures to deploy the Cisco Nexus 1010 and 1000v platforms within a FlexPod for VMware environment. At the completion of this section the following should be in place:

- A clustered pair of Cisco Nexus 1010s
- An active/standby pair of Nexus 1000v virtual supervisor modules (VSM)
- The Nexus 1000v acting as the virtual distributed switching platform for vSphere supporting VM, NFS and vMotion traffic types

The following procedures are required to meet these objective.

- Log into Cisco Nexus 1010 virtual appliance console.
- Configure the CIMC or “out-of-band” management interface.
- Execute the Cisco Nexus 1010 Virtual Appliances setup.
- Create and install the Cisco Nexus 1000V VSM on a Nexus 1010 virtual service blade.
- Register the Cisco Nexus 1000V as a vCenter Plug-in.
- Configure Networking on the Cisco Nexus 1000V, including:
  - Management, NFS, vMotion and virtual machine data traffic VLANs
  - vCenter connectivity
  - Port profiles
- Install the Nexus 1000V VEMs on each ESXi host.
- Replace the default virtual switch with the Cisco Nexus 1000V and add uplink ports to Cisco Nexus 1000V.
- Enable Jumbo Frames in the Nexus 1000V.

# NetApp Virtual Storage Console Deployment Procedure

The following presents the general procedures for installing the NetApp Virtual Storage Console for use in a FlexPod for VMware environment.

- Install the NetApp Virtual Storage Console on a dedicated virtual machine running Microsoft Windows Server 2008 R2 x64 with 4 GB of RAM, 30 GB of storage, and two network interfaces for management and NFS traffic.

**Note** The VSC download is available at: http://.now.netapp.com.

**Note** This machine may also host the NetApp Data Fabric Manager.

- Configure the VSC plug-in to register with vCenter.
- Configure the VSC via vCenter NetApp tab to work with the FlexPod vFilers.

- Set the recommended values for ESXi hosts via NetApp best practices for HBA/CNA, MPIO, and NFS.

## NetApp Operations Manager Deployment Procedure

The following section provides the general procedures for configuring the NetApp Operations Manager which is part of the DataFabric Manager (DFM) 4.0 suite for use in a FlexPod for VMware environment. After completing this section the following should be available:

- A Microsoft Windows 2008 virtual machine running NetApp DataFabric Manager Suite including:
  - Operations Manager
  - Provisioning Manager
  - Protection Manger
- NetApp Operations Manager monitoring both FlexPod for VMware storage controllers

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

- Install DFM on the same Windows virtual machine hosting the virtual storage controller via 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 for VMware Configuration Information

The following tables outline the information which needs to be available to complete the setup and deployment of FlexPod for VMware.

## Global Configuration Information

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

*Table 5 FlexPod for VMware 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 | | 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 VMotion traffic | | Provide the appropriate VLAN ID used for vMotion traffic throughout the FlexPod environment. |
| Network address for VMotion traffic | | Network address for VMotion VLAN traffic in CIDR notation (that is, 192.168.30.0/24) |
| VLAN id for the Cisco Nexus 1000v Packet and Control traffic | | Provide the appropriate VLAN ID used for the Cisco Nexus 1000v packet and control traffic. |
| VLAN id for Native VLAN | | Provide the appropriate VLAN ID that will be used for the native VLAN id throughout the FlexPod environment. |
| VLAN id for VM Traffic | | Provide the appropriate VLAN ID that will be used for VM traffic by default. |
| 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. |

*Table 5 FlexPod for VMware Global Configuration Information*

| Name | Customized Value | Description |
|---|---|---|
| SSL Locality Name | | Provide the appropriate SSL Locality Name (City, Town, etc.). |
| SSL Organization Name | | Provide the appropriate SSL Organization Name (Company Name). |
| SSL Organization Unit | | Provide the appropriate SSL Organization 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 recommend interface. |
| NetApp FAS3210 A Netboot Interface IP Address | | Provide the IP Address for the netboot interface on NetApp FAS3210 B. |
| NetApp FAS3210 B Netboot Interface IP Address | | Provide the IP Address for the netboot interface on NetApp FAS3210 B. |
| NetApp FAS3210 A Netboot Interface Subnet Mask | | Provide the Subnet Mask for the netboot interface on NetApp FAS3210 A. |
| NetApp FAS3210 B Netboot Interface Subnet Mask | | Provide the Subnet Mask for the netboot interface on NetApp FAS3210 B. |
| NetApp FAS3210 A Netboot Interface Gateway IP Address | | Provide the Gateway IP Address for the netboot interface on NetApp FAS3210 A. |
| NetApp FAS3210 B Netboot Interface Gateway IP Address | | Provide the Gateway IP Address for the netboot interface on NetApp FAS3210 B. |
| NetApp DataONTAP 7.3.5 Netboot Kernel Location | | Provide the full tftp path to the 7.3.5 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. |

*Table 6 NetApp FAS3210A Configuration Information*

| Name | Customized Value | Description |
|---|---|---|
| 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. |
| 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 7.3.5 Flash Image Location | | Provide the “http” or “https” Web address of the NetApp DataONTAP 7.3.5 flash image to install the image to the onboard 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.<br>Note: This interface will be used for the export of NFS datastores and possibly iSCSI LUNs to the necessary ESXi hosts. |

*Table 6 NetApp FAS3210A Configuration Information*

| Name | Customized Value | Description |
|---|---|---|
| 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 | | 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. |
| 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 3 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 no include the 3 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 via 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 how many ESXi hosts will be in the environment. |
| NetApp FAS3210 B ESXi Boot Volume Size | | VMware allows the option to store VM swap files in a different location other than the default location within the specific VM directory itself. Choose the appropriate size for the common VM swap datastore volume. |

*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. |
| 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. |

*Table 9 NetApp Data Fabric Manager Configuration Information*

| Name | Customized Value | Description |
|---|---|---|
| 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 through Table 12 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 Nexus 1010 and 1000V Configuration Information*

| Name | Customized Value | Description |
|---|---|---|
| Cisco Nexus 1010 A Hostname | | Provide a hostname for the Cisco Nexus 1010 A virtual appliance. |
| Cisco Nexus 1010 B Hostname | | Provide a hostname for the Cisco Nexus 1010 B virtual appliance. |
| Cisco Nexus 1010 A CIMC IP Address | | Provide the IP address for the out-of-band management interface or CIMC on the Cisco Nexus 1010 A appliance. |

*Table 11 Cisco Nexus 1010 and 1000V Configuration Information*

| Name | Customized Value | Description |
|---|---|---|
| Cisco Nexus 1010 A CIMC netmask | | Provide the netmask for the out-of-band management interface or CIMC on the Cisco Nexus 1010 A appliance |
| Cisco Nexus 1010 A CIMC gateway | | Provide the gateway for the out-of-band management interface or CIMC on the Cisco Nexus 1010 A appliance. |
| Cisco Nexus 1010 A Hostname | | Provide the hostname for the Cisco Nexus 1010 A virtual appliance. |
| Cisco Nexus 1010 A Management Interface IP | | Provide the IP address for the management interface on the Cisco Nexus 1010 A appliance. |
| Cisco Nexus 1010 A Management Interface Netmask | | Provide the netmask for the management interface on the Cisco Nexus 1010 A appliance. |
| Cisco Nexus 1010 A Management Interface Gateway | | Provide the gateway for the management interface on the Cisco Nexus 1010 A appliance. |
| Cisco Nexus 1010 B CIMC IP Address | | Provide the IP address for the out-of-band management interface or CIMC on the Cisco Nexus 1010 B appliance. |
| Cisco Nexus 1010 B CIMC netmask | | Provide the netmask for the out-of-band management interface or CIMC on the Cisco Nexus 1010 B appliance |
| Cisco Nexus 1010 B CIMC gateway | | Provide the gateway for the out-of-band management interface or CIMC on the Cisco Nexus 1010 B appliance. |
| Cisco Nexus 1010 Domain ID | | Provide a unique domain id for the Cisco Nexus 1010 virtual appliances in the environment. |
| Primary Cisco Nexus 1000v Virtual Supervisor Module Hostname | | Provide the hostname for the primary VSM. |
| Primary Cisco Nexus 1000v Virtual Supervisor Module Management Interface IP Address | | Provide the IP Address for the management interface for the primary Cisco Nexus 1000v Virtual Supervisor Module. |
| Primary Cisco Nexus 1000v Virtual Supervisor Module Management Interface Netmask | | Provide the netmask for the management interface for the primary Cisco Nexus 1000v Virtual Supervisor Module. |
| Primary Cisco Nexus 1000v Virtual Supervisor Module Management Interface Gateway | | Provide the gateway for the management interface for the primary Cisco Nexus 1000v Virtual Supervisor Module. |
| Cisco Nexus 1000v Virtual Supervisor Module Domain ID | | Provide a unique domain id for the Cisco Nexus 1000v VSMs. This domain id should be different than the domain id used for the Cisco Nexus 1010 virtual appliance domain id. |

*Table 12 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 12 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. |

# VMware Configuration Information

The information in Table 13 is specific to the VMware portion of the deployment only.

*Table 13 VMware Configuration Information*

| Name | Customized Value | Description |
|---|---|---|
| ESXi Server 1 Hostname | | The hostname for the first esxi host in the infrastructure cluster. |
| ESXi Server 1 Management Interface IP Address | | The IP address for the management vmkernel port on the first host in the infrastructure cluster. |
| ESXi Server 1 Management Interface Netmask | | The netmask for the management vmkernel port on the first host in the infrastructure cluster. |
| ESXi Server 1 Management Interface Gateway | | The gateway for the management vmkernel port on the first host in the infrastructure cluster. |
| ESXi Server 1 NFS VMkernel Interface IP Address | | The IP Address for the nfs vmkernel port on the first host in the cluster. |
| ESXi Server 1 NFS VMkernel Interface Netmask | | The netmask for the nfs vmkernel port on the first host in the infrastructure cluster. |
| ESXi Server 1 VMotion VMkernel Interface IP Address | | The IP Address for the vmotion vmkernel port on the first host in the cluster. |
| ESXi Server 1 VMotion VMkernel Interface Netmask | | The netmask for the vmotion vmkernel port on the first host in the infrastructure cluster. |

*Table 13 VMware Configuration Information*

| Name | Customized Value | Description |
|---|---|---|
| ESXi Server 2 Hostname | | The hostname for the second esxi host in the infrastructure cluster. |
| ESXi Server 2 Management Interface IP Address | | The IP address for the management vmkernel port on the second host in the infrastructure cluster. |
| ESXi Server 2 Management Interface Netmask | | The netmask for the management vmkernel port on the second host in the infrastructure cluster. |
| ESXi Server 2 Management Interface Gateway | | The gateway for the management vmkernel port on the second host in the infrastructure cluster. |
| ESXi Server 2 NFS VMkernel Interface IP Address | | The IP Address for the nfs vmkernel port on the second host in the cluster. |
| ESXi Server 2 NFS VMkernel Interface Netmask | | The netmask for the nfs vmkernel port on the second host in the infrastructure cluster. |
| ESXi Server 2 VMotion VMkernel Interface IP Address | | The IP Address for the vmotion vmkernel port on the second host in the cluster. |
| ESXi Server 2 VMotion VMkernel Interface Netmask | | The netmask for the vmotion vmkernel port on the second host in the infrastructure cluster. |
| SQL Server VM Hostname | | The hostname of the SQL server virtual machine that will run the vCenter Server database. |
| SQL Server VM IP Address | | The IP address of the SQL server virtual machine that will run the vCenter Server database. |
| vCenter Server VM Hostname | | The hostname of the vCenter Server virtual machine. |
| vCenter Server VM IP Address | | The IP address of the vCenter Server virtual machine. |
| vCenter Server License Key | | The vCenter license key. |

# NetApp FAS3200 Sample Configuration

## Filer 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: vmware):
        20:00:00:25:b5:00:0a:9f (logged in on: 0c)
    ucs2b-1-sc_B (FCP) (ostype: vmware):
        20:00:00:25:b5:00:0b:df (logged in on: 0d)
```

## Sample vFiler 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 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 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

```
version 5.0(2)N2(1)
feature fcoe
```

```
feature npiv
feature telnet
cfs ipv4 distribute
cfs eth distribute
feature lacp
feature vpc
feature lldp
username admin password 5 $1$L3ZfgcnE$jVX7X6bkIQiIr32esCZ2O.  role network-admin
ip domain-lookup
ip domain-lookup
switchname n5k-2
system jumbomtu 9000
logging event link-status default
ip access-list classify_COS_4
  10 permit ip 192.168.91.0/24 any
  20 permit ip any 192.168.91.0/24
ip access-list classify_COS_5
  10 permit ip 192.168.90.0/24 any
  20 permit ip any 192.168.90.0/24
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-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-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
system qos
  service-policy type network-qos Setup_QOS
  service-policy type qos input Global_Classify
snmp-server user admin network-admin auth md5 0xbc83a1f2e2679352248d184bc5580243 priv
0xbc83a1f2e2679352248d184bc5580243 localizedkey
snmp-server enable traps entity fru
vrf context management
  ip route 0.0.0.0/0 10.61.185.1
vlan 1
vlan 185
  name MGMT_VLAN
vlan 900
```

```
  name NFS_VLAN
vlan 901
  name vMotion_VLAN
vlan 950
  name Packet_Control_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 ucs2b-1_B pwwn 20:00:00:25:b5:00:0b:df
  device-alias name ucs2b-2_B pwwn 20:00:00:25:b5:00:0b:ff
  device-alias name ntap3200-1a_0d pwwn 50:0a:09:82:8d:dd:93:e8
  device-alias name ntap3200-1b_0d pwwn 50:0a:09:82:9d:dd:93:e8

device-alias commit

fcdomain fcid database
  vsan 102 wwn 20:41:00:05:9b:79:07:80 fcid 0x9e0000 dynamic
  vsan 102 wwn 50:0a:09:82:00:05:5c:71 fcid 0x9e0001 dynamic
  vsan 102 wwn 50:0a:09:82:00:05:5c:b1 fcid 0x9e0002 dynamic
  vsan 102 wwn 20:00:00:25:b5:00:0b:df fcid 0x9e0003 dynamic
!              [ucs2b-1_B]
  vsan 102 wwn 20:00:00:25:b5:00:0b:ff fcid 0x9e0004 dynamic
!              [ucs2b-2_B]
  vsan 102 wwn 50:0a:09:82:9d:dd:93:e8 fcid 0x9e0005 dynamic
!              [ntap3200-1b_0d]
  vsan 102 wwn 50:0a:09:82:8d:dd:93:e8 fcid 0x9e0006 dynamic
!              [ntap3200-1a_0d]

interface port-channel10
  description vPC Peer-Link
  switchport mode trunk
  vpc peer-link
  switchport trunk native vlan 2
  spanning-tree port type network

interface port-channel11
  description ntap3200-1a
  switchport mode trunk
  vpc 11
  switchport trunk native vlan 2
  switchport trunk allowed vlan 900
  spanning-tree port type edge trunk

interface port-channel12
  description ntap3200-1b
  switchport mode trunk
  vpc 12
  switchport trunk native vlan 2
  switchport trunk allowed vlan 900
  spanning-tree port type edge trunk

interface port-channel13
  description ucsm-2-A
  switchport mode trunk
  vpc 13
  switchport trunk allowed vlan 185,900-901,950
  spanning-tree port type edge trunk
```

```
interface port-channel14
  description ucsm-2-B
  switchport mode trunk
  vpc 14
  switchport trunk allowed vlan 185,900-901,950
  spanning-tree port type edge trunk

interface port-channel20
  description mgmt-1 uplink
  switchport mode trunk
  vpc 20
  switchport trunk native vlan 2
  switchport trunk allowed vlan 185
  spanning-tree port type network

vsan database
  vsan 102 interface fc2/1
  vsan 102 interface fc2/2
  vsan 102 interface fc2/3

interface fc2/1
  no shutdown

interface fc2/2
  no shutdown

interface fc2/3
  no shutdown

interface fc2/4

interface Ethernet1/1
  description ntap3200-1a:e1b
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 900
  channel-group 11 mode active

interface Ethernet1/2
  description ntap3200-1b:e1b
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 900
  channel-group 12 mode active

interface Ethernet1/3

interface Ethernet1/4

interface Ethernet1/5
  description n5k-1:Eth1/5
  switchport mode trunk
  switchport trunk native vlan 2
  channel-group 10 mode active

interface Ethernet1/6
  description n5k-1:Eth1/6
  switchport mode trunk
  switchport trunk native vlan 2
  channel-group 10 mode active

interface Ethernet1/7
  description n1010-1:Eth2
  switchport mode trunk
```

```
  switchport trunk allowed vlan 185,950
  spanning-tree port type edge trunk
  speed 1000

interface Ethernet1/8
  description n1010-2:Eth2
  switchport mode trunk
  switchport trunk allowed vlan 185,950
  spanning-tree port type edge trunk
  speed 1000

interface Ethernet1/9
  description ucsm-2-A:Eth1/8
  switchport mode trunk
  switchport trunk allowed vlan 185,900-901,950
  channel-group 13 mode active

interface Ethernet1/10
  description ucsm-2-B:Eth1/8
  switchport mode trunk
  switchport trunk allowed vlan 185,900-901,950
  channel-group 14 mode active

interface Ethernet1/20
  description mgmt-1:Eth1/13
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 185
  channel-group 20 mode active

interface Ethernet2/1

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface mgmt0
  ip address 10.61.185.70/24
line console
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.5.0.2.N2.1.bin
boot system bootflash:/n5000-uk9.5.0.2.N2.1.bin
interface fc2/1
interface fc2/2
interface fc2/3
interface fc2/4
!Full Zone Database Section for vsan 102
zone name ucs2b-1_B vsan 102
    member pwwn 20:00:00:25:b5:00:0b:df
!               [ucs2b-1_B]
    member pwwn 50:0a:09:82:8d:dd:93:e8
!               [ntap3200-1a_0d]

zone name ucs2b-2_B vsan 102
    member pwwn 20:00:00:25:b5:00:0b:ff
!               [ucs2b-2_B]
    member pwwn 50:0a:09:82:9d:dd:93:e8
!               [ntap3200-1b_0d]

zoneset name flexpod vsan 102
    member ucs2b-1_B
    member ucs2b-2_B
```

```
zoneset activate name flexpod vsan 102
```

# Cisco Nexus 1010 Sample Running Configuration

```
version 4.0(4)SP1(1)
username admin password 5 $1$EVg2LPBC$EX8pjL9GBayKAaUmwjLjD.  role network-admin
ntp server 10.61.185.9
ip domain-lookup
ip host n1010-1 10.61.185.165
kernel core target 0.0.0.0
kernel core limit 1
system default switchport
snmp-server user admin network-admin auth md5 0x7ccf323f71b74c6cf1cba6d255e9ded9 priv
0x7ccf323f71b74c6cf1cba6d255e9ded9 localizedkey
snmp-server enable traps license
vrf context management
  ip route 0.0.0.0/0 10.61.185.1
switchname n1010-1
vlan 1,162,950
vlan 902
  name data
vdc n1010-1 id 1
  limit-resource vlan minimum 16 maximum 513
  limit-resource monitor-session minimum 0 maximum 64
  limit-resource vrf minimum 16 maximum 8192
  limit-resource port-channel minimum 0 maximum 256
  limit-resource u4route-mem minimum 32 maximum 80
  limit-resource u6route-mem minimum 16 maximum 48
network-uplink type 3
virtual-service-blade drs1-vsm1
  virtual-service-blade-type name VSM-1.0
  interface control vlan 950
  interface packet vlan 950
  ramsize 2048
  disksize 3
  no shutdown
virtual-service-blade drs2-vsm1
  virtual-service-blade-type name VSM-1.0
  interface control vlan 950
  interface packet vlan 950
  ramsize 2048
  disksize 3
  no shutdown
virtual-service-blade drs3-vsm1
  virtual-service-blade-type name VSM-1.0
  interface control vlan 950
  interface packet vlan 950
  ramsize 2048
  disksize 3
  no shutdown
virtual-service-blade NAM
  virtual-service-blade-type name NAM-1.0
  interface data vlan 902
  ramsize 2048
  disksize 53
  no shutdown primary

interface mgmt0
  ip address 10.61.185.165/16

interface control0
```

```
logging logfile messages 6
boot kickstart bootflash:/nexus-1010-kickstart-mz.4.0.4.SP1.1.bin
boot system bootflash:/nexus-1010-mz.4.0.4.SP1.1.bin
boot kickstart bootflash:/nexus-1010-kickstart-mz.4.0.4.SP1.1.bin
boot system bootflash:/nexus-1010-mz.4.0.4.SP1.1.bin
svs-domain
  domain id 51
  control vlan 950
  management vlan 162
```

# Cisco Nexus 1000v Sample Running Configuration

```
version 4.0(4)SV1(3b)
username admin password 5 $1$hgzMSZ3F$NCCbwTw4Z8QU5yjIo7Me11  role network-admin
ssh key rsa 2048
ntp server 10.61.185.3
ip domain-lookup
ip host n1010-1-vsm 10.61.185.137
kernel core target 0.0.0.0
kernel core limit 1
system default switchport
vem 3
  host vmware id 737ff954-0de3-11e0-0000-000000000001
vem 4
  host vmware id 737ff954-0de3-11e0-0000-000000000002
snmp-server user admin network-admin auth md5 0xfe02f063cf936282f39c604c06e628df priv
0xfe02f063cf936282f39c604c06e628df localizedkey
snmp-server enable traps license
vrf context management
  ip route 0.0.0.0/0 10.61.185.1
hostname n1010-1-vsm
vlan 1
vlan 185
  name MGMT-VLAN
vlan 900
  name NFS-VLAN
vlan 901
  name vMotion-VLAN
vlan 950
  name VM-Traffic-VLAN
vdc n1010-1-vsm id 1
  limit-resource vlan minimum 16 maximum 513
  limit-resource monitor-session minimum 0 maximum 64
  limit-resource vrf minimum 16 maximum 8192
  limit-resource port-channel minimum 0 maximum 256
  limit-resource u4route-mem minimum 32 maximum 80
  limit-resource u6route-mem minimum 16 maximum 48
port-profile type vethernet MGMT-VLAN
  vmware port-group
  switchport mode access
  switchport access vlan 185
  no shutdown
  system vlan 185
  state enabled
port-profile type vethernet NFS-VLAN
  vmware port-group
  switchport mode access
  switchport access vlan 900
  no shutdown
  system vlan 900
  state enabled
port-profile type ethernet Unused_Or_Quarantine_Uplink
```

```
  description Port-group created for Nexus1000V internal usage. Do not use.
  vmware port-group
  shutdown
  state enabled
port-profile type vethernet Unused_Or_Quarantine_Veth
  description Port-group created for Nexus1000V internal usage. Do not use.
  vmware port-group
  shutdown
  state enabled
port-profile type vethernet VM-Traffic-VLAN
  vmware port-group
  switchport mode access
  switchport access vlan 950
  no shutdown
  system vlan 950
  state enabled
port-profile type ethernet system-uplink
  description system profile for blade uplink ports
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 185,900-901,950
  system mtu 9000
  channel-group auto mode on mac-pinning
  no shutdown
  system vlan 185,900-901,950
  state enabled
port-profile type vethernet vMotion-VLAN
  vmware port-group
  switchport mode access
  switchport access vlan 901
  no shutdown
  system vlan 901
  state enabled

interface port-channel1
  inherit port-profile system-uplink
  mtu 9000

interface port-channel2
  inherit port-profile system-uplink
  mtu 9000

interface Ethernet3/1
  inherit port-profile system-uplink
  mtu 9000

interface Ethernet3/2
  inherit port-profile system-uplink
  mtu 9000

interface Ethernet4/1
  inherit port-profile system-uplink
  mtu 9000

interface Ethernet4/2
  inherit port-profile system-uplink
  mtu 9000

interface mgmt0
  ip address 10.61.185.137/24

interface Vethernet1
  inherit port-profile MGMT-VLAN
  description VMware VMkernel, vmk0
```

```
  vmware dvport 35

interface Vethernet2
  inherit port-profile NFS-VLAN
  description VMware VMkernel, vmk1
  vmware dvport 67

interface Vethernet3
  inherit port-profile vMotion-VLAN
  description VMware VMkernel, vmk2
  vmware dvport 130

interface control0
boot kickstart bootflash:/nexus-1000v-kickstart-mz.4.0.4.SV1.3b.bin sup-1
boot system bootflash:/nexus-1000v-mz.4.0.4.SV1.3b.bin sup-1
boot kickstart bootflash:/nexus-1000v-kickstart-mz.4.0.4.SV1.3b.bin sup-2
boot system bootflash:/nexus-1000v-mz.4.0.4.SV1.3b.bin sup-2
svs-domain
  domain id 10
  control vlan 950
  packet vlan 950
  svs mode L2
svs connection vCenter
  protocol vmware-vim
  remote ip address 10.61.185.114 port 80
  vmware dvs uuid "2d 5b 20 50 21 69 05 64-2c 68 d0 b3 63 bf b2 9f" datacenter-name
FlexPod_DC_1
  connect
```

# Cisco Unified Computing System Configuration Extracts

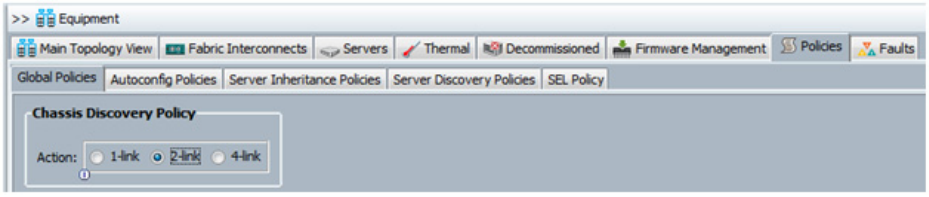
All configurations in this section occur after the initial UCS cluster setup scripts have completed and the UCS Manager is accessible to the administrator. Use the configuration information described above to execute the setup script and complete the deployment required in your environment.

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.

## Sample Chassis Discovery Policy Configuration

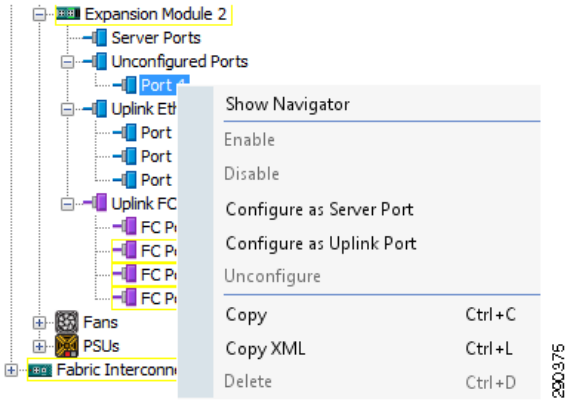
Define the Chassis Discovery Policy to reflect the number of links from the chassis to the fabric interconnects. FlexPod requires at a minimum two links.

***Figure 3 Chassis Discovery Policy Screen***




Define and enable Fibre Channel, Server, and Uplink Ports.

*Figure 4 Fibre Channel Server and Uplink Ports Screen*




The physical display after completing this procedure is shown in Figure 5.

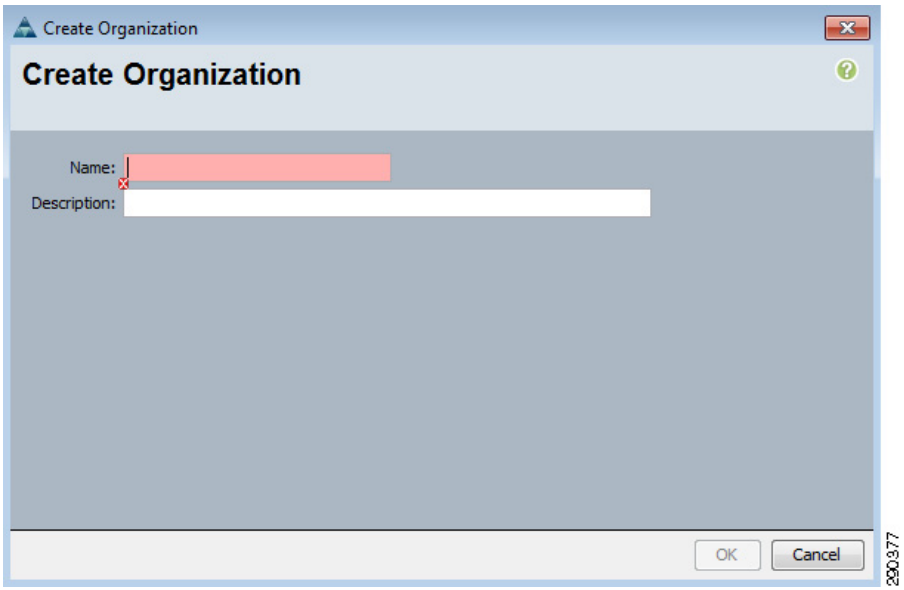
*Figure 5 Physical Display after Procedure Completion*


## 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.

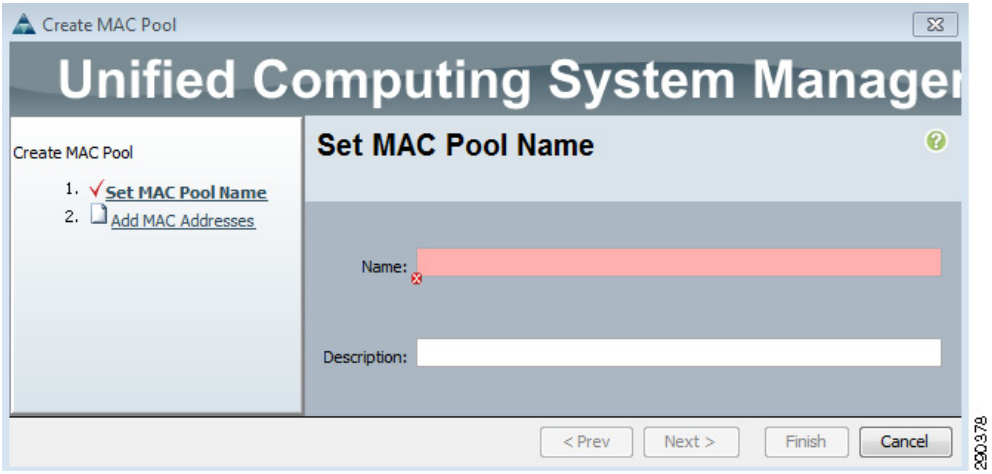
*Figure 6 Create Organization Screen*




## Create MAC Address Pools

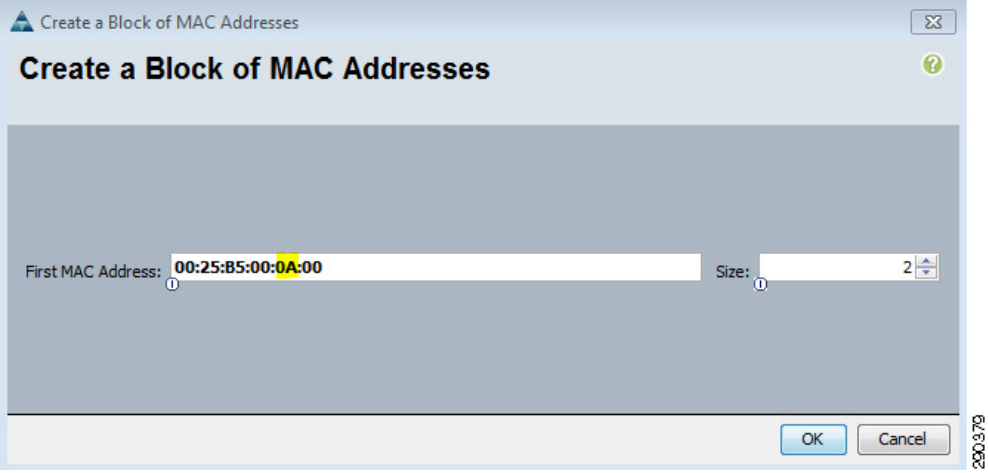
In the Navigation pane, select the **LAN** tab, click **Pools**, and select the proper sub-organization. On the Main panel, select **Create MAC Pool** and compete the form.

*Figure 7 Create MAC Pool Screen*



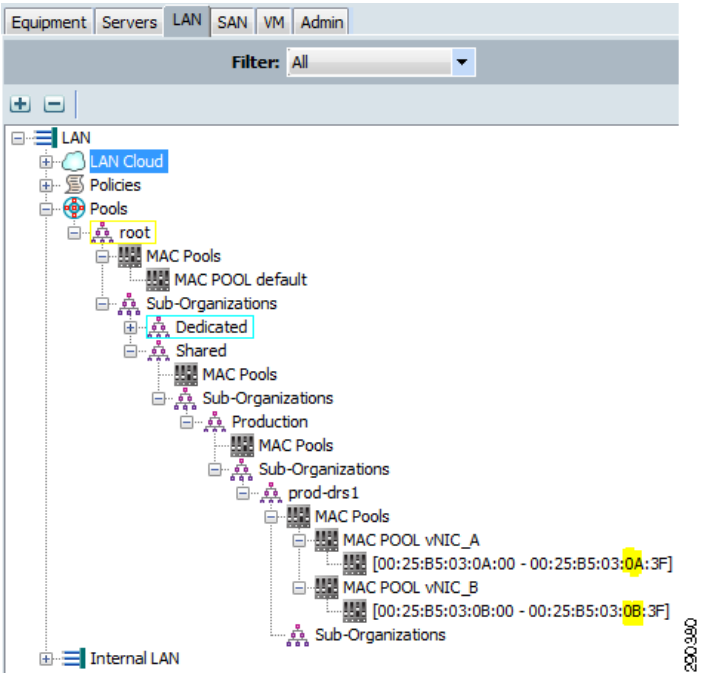

Click **Next** and complete the form. Notice that the MAC address field should indicate if the MAC Pool will be used in fabric a or fabric b in the second octet position; the size should be set to **2**.

*Figure 8 Create Block of MAC Addresses Screen*




In the example below, the "prod-drs1" organization defines two MAC pools. Each MAC pool uses a unique hex value to indicate the unique MAC address aligning with fabric A or fabric B. The alignment of organizations and resources is a fundamental feature of the Cisco UCS.

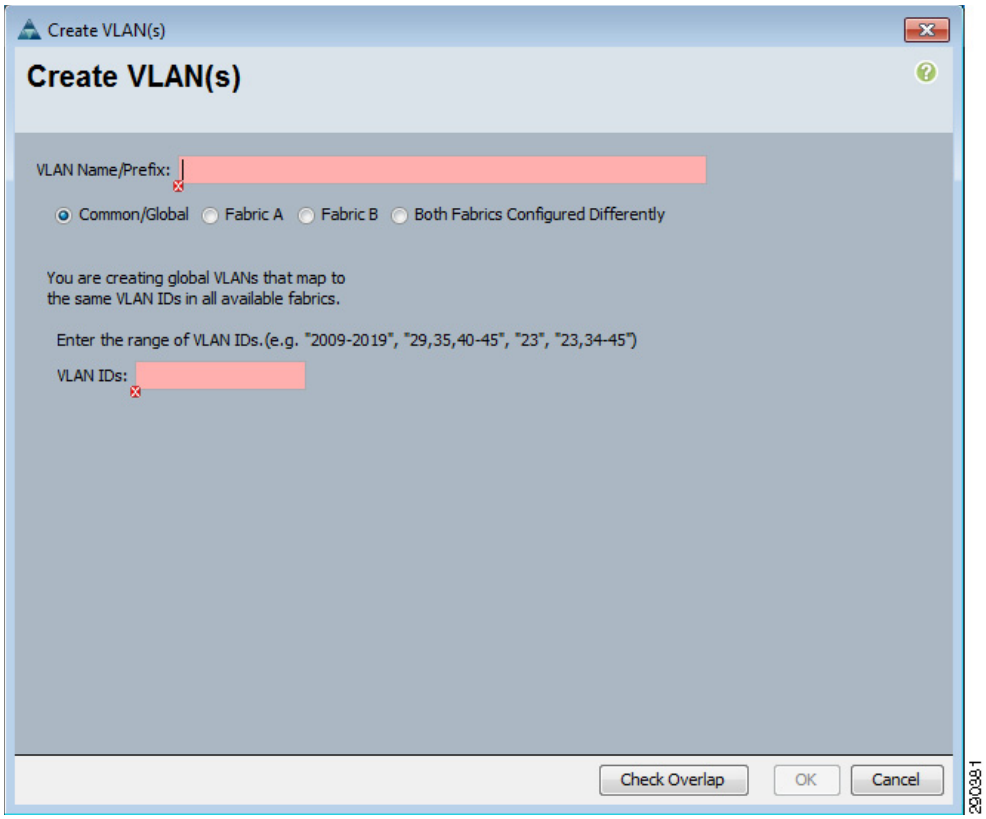
*Figure 9 MAC Pool Examples*




## Create Global VLAN Pools

In the Navigation pane, select the **LAN** tab, select **LAN Cloud**, and then select **VLANs**. On the main panel, click **New** and select **Create VLAN(s)**.

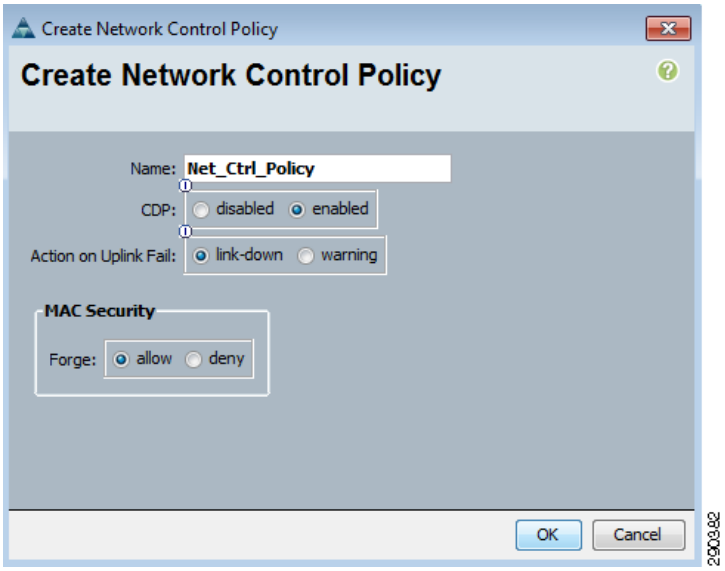
*Figure 10 Create LANs Screen*




## Create a Network Control Policy

In the Navigation pane select the **LAN** tab, select **LAN Cloud**, and then select **Policies**. Select the appropriate organization for the new network control policy. In the work pane, click the **General** tab and select **Create Network Control Policy**. Provide a name for the policy and select the enabled CDP radio button.

*Figure 11 Create Network Control Policy Screen*

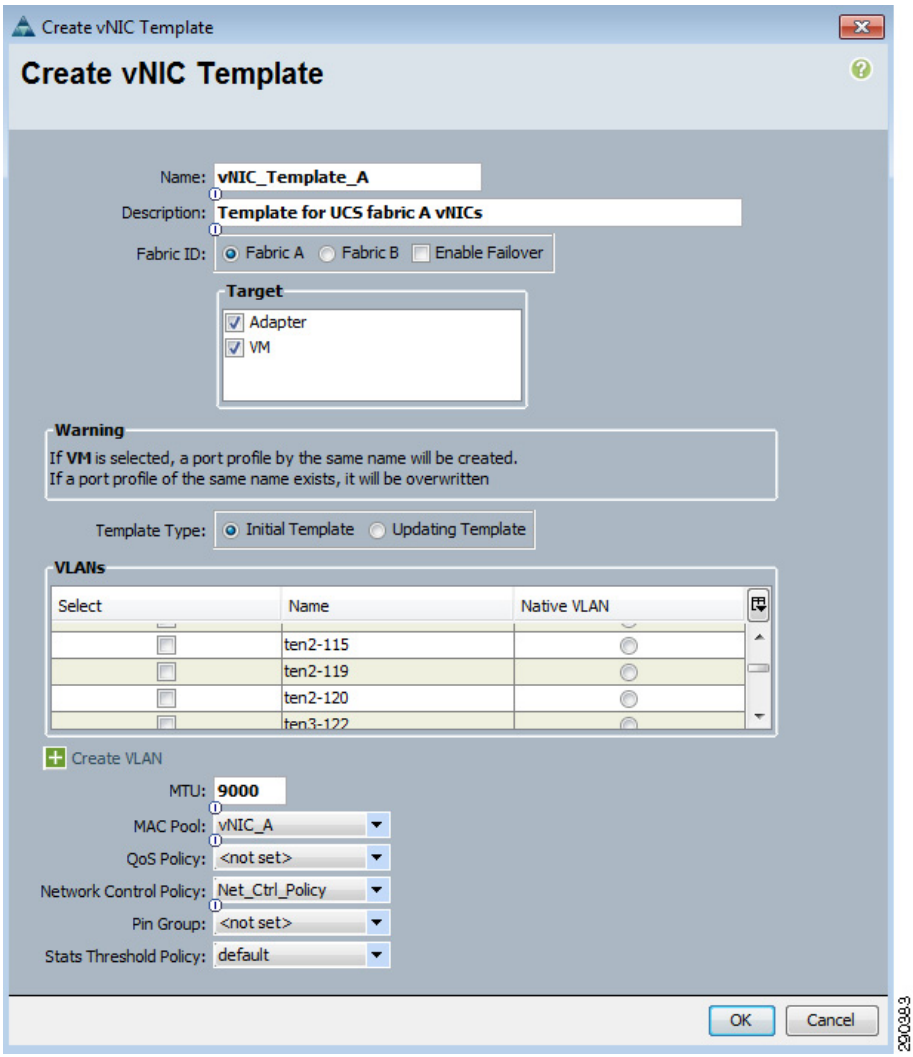



## Create vNIC Template

In the Navigation pane, select the **LAN** tab, select **LAN Cloud**, and then select **Policies**. Select the organization requiring a new vNIC Template. In the work pane, click the **General** tab and select **Create vNIC Template**. Complete the form and be sure to employ the previously-defined global VLANs, MAC pools, and Network Control Policy. The MTU should be set to 9000.

Create two vNIC templates, one for use in fabric a and one for use in fabric b. The only differences are the name, description, and MAC pool referenced.

*Figure 12 Create vNIC Template Screen*




## Define QoS Policies and Jumbo Frames

In the Navigation pane, select the **LAN** tab, select **LAN Cloud**, and then select **QoS System Class**. Set the Best Effort QoS system class to **9000** MTU.

## Create Uplink Port-Channels to the Cisco Nexus 5548 Switches

In the Navigation pane, select **LAN** tab, select **LAN Cloud**, and then select **Fabric A**. Right-click on the **Port Channels** item and select **Create Port Channel**. Complete the form and click **Next**. Select uplink ports Ethernet slot 2 ports 1 and 2 and click **OK**.

*Figure 13 Create Port Channel Screen*

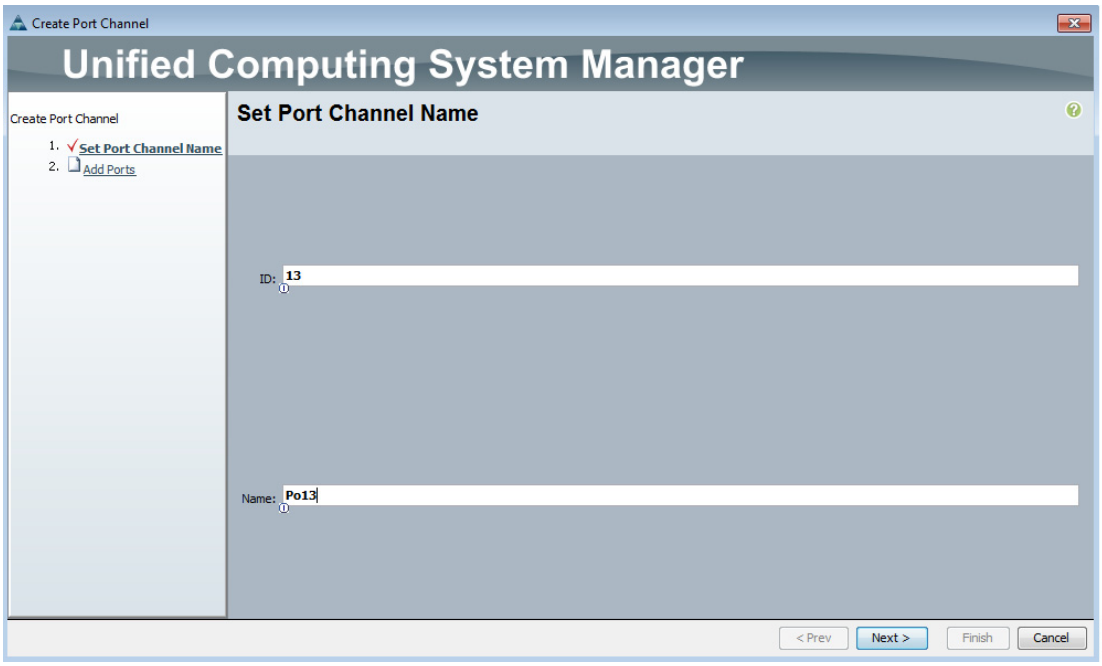
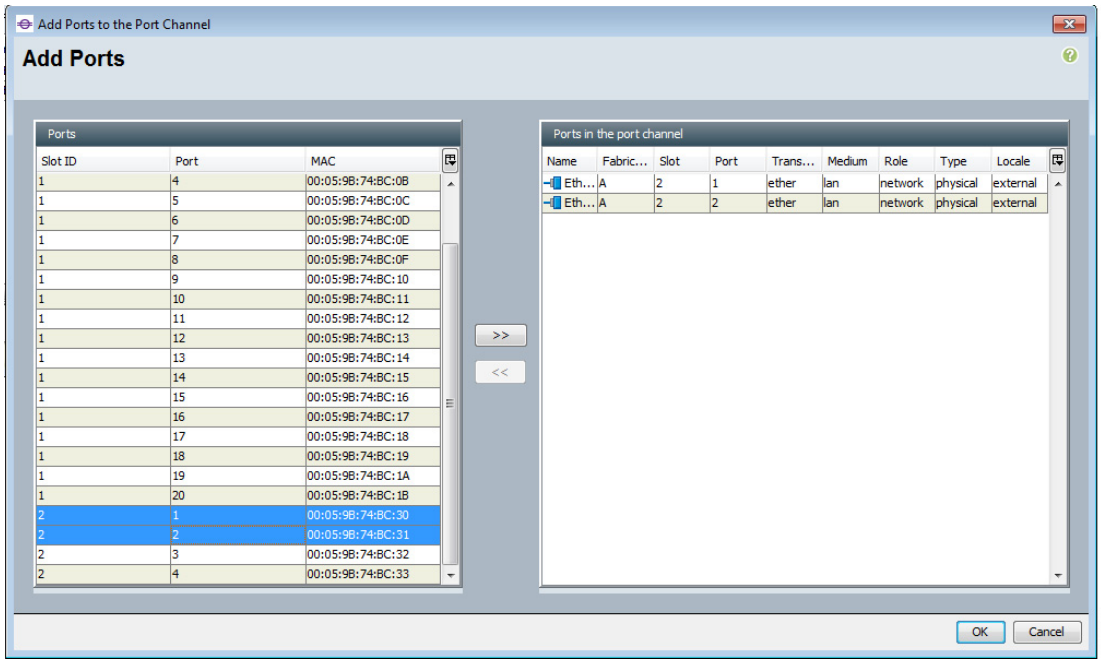


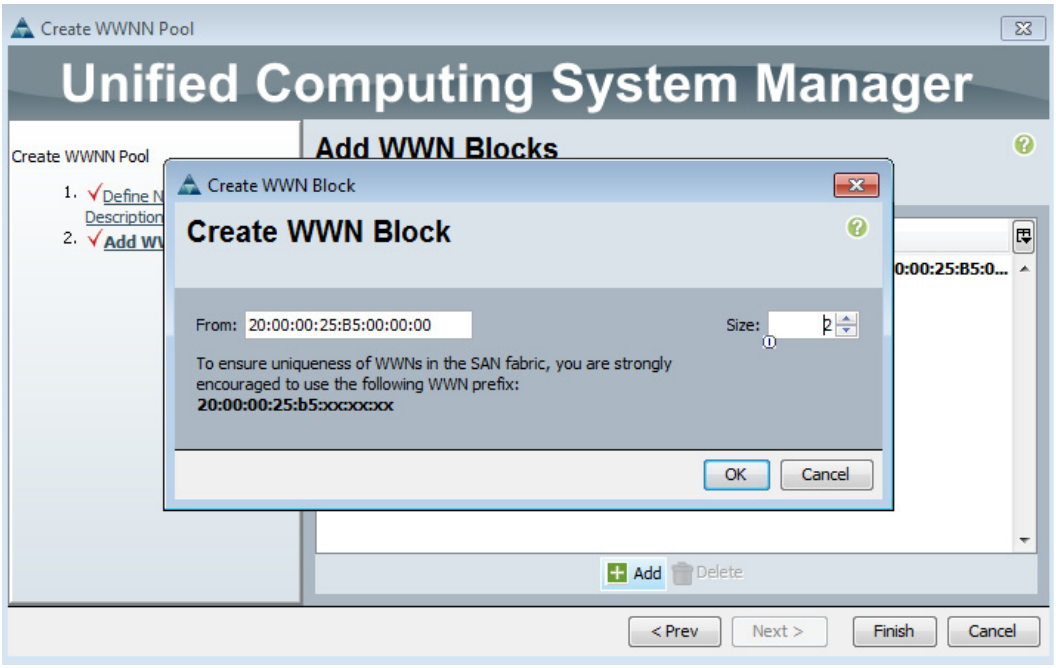

*Figure 14 Add Ports Screen*



## Create WWNN Pool

In the Navigation pane, select the **SAN** tab, select **Pools**, and select the appropriate sub-organization. Right-click on the **WWNN Pools** of that sub-organization and select the **Create WWNN Pool** item. A wizard will launch to create a WWNN Pool. Complete the first form using **WWNN_Pool** as the name. Click **Next** and then **Add** a WWN Block with a size of **2**. Click **OK**, then click **Finish**.

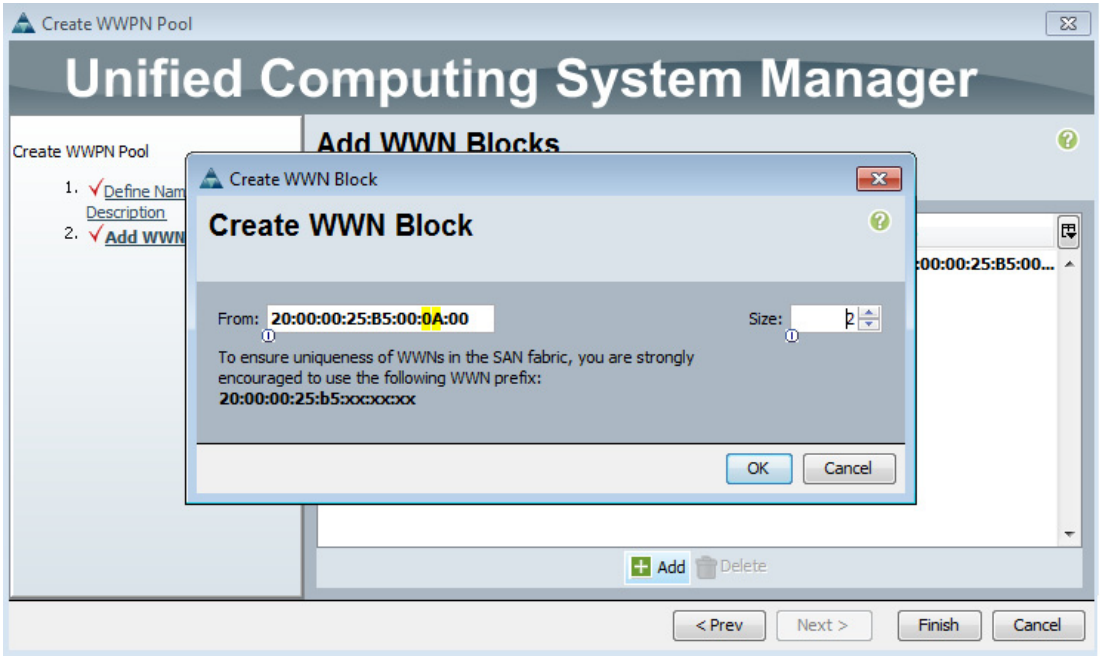
***Figure 15 Create WWNN Pool Screen***




## Create WWPN Pools

In the Navigation pane, select the **SAN** tab, select **Pools**, and select the appropriate sub-organization. Right-click on the **WWPN Pools** of that sub-organization and select the **Create WWPN Pool** item. A wizard will launch to create a WWPN Pool. Complete the first form using **WWNN_Pool_A** as the name. Click **Next** and then **Add** a WWN Block with a size of **2** and a block indicating the fabric assignment in the second octet. Click **OK**, then click **Finish**. Repeat this process to create another WWPN pool named **WWNN_Pool_B**.

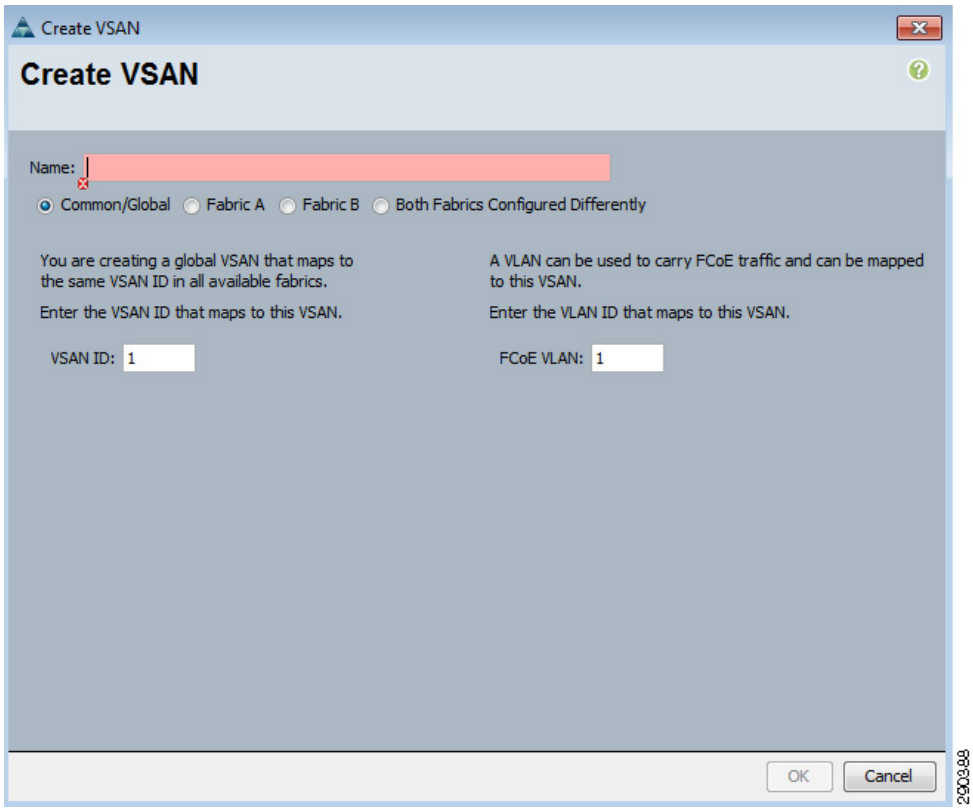
*Figure 16 Create WWPN Pool Screen*




## Create Global VSANs

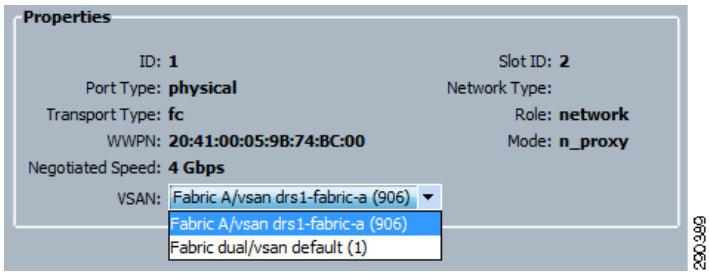
In the Navigation pane, select the **SAN** tab, select **SAN Cloud**, and then select **VSANs**. On the main panel, click **New**, then select **Create VSAN**. Create two VSANs, one for fabric a and one for fabric b.

*Figure 17 Create VSAN Screen*




The VSANs must then be associated to the appropriate fibre channel uplink ports. To associate the VSANs to the UCS fibre channel uplinks, select the **Equipment** tab in the Navigation pane. Select **Fabric Interconnect A** and **Expansion Module 2**. Select **Uplink FC Ports**, select F**C Port 1** uplink, and assign the previously created fabric a VSAN to the port by selecting it from the VSAN drop-down list on the work panel. Repeat this process for FC Port 2 on Fabric Interconnect A and for Fabric Interconnect B FC ports 1 and 2.

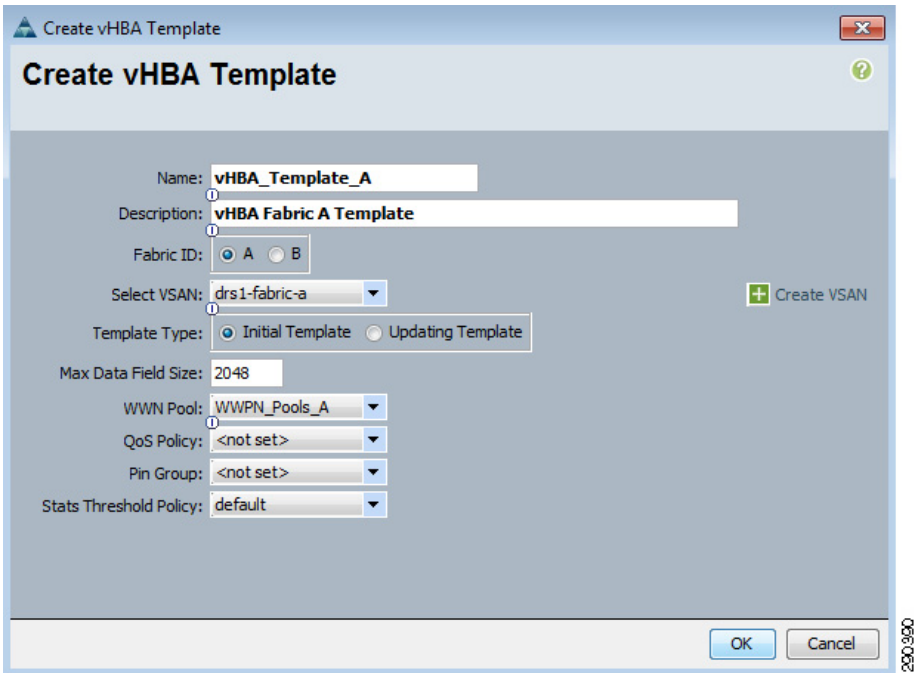
*Figure 18 VSAN Properties Screen*




## Create vHBA Templates

In the **SAN** tab on the Navigation pane, select **Policies** and the appropriate sub-organization. In the work panel, select **Create vHBA Template**; a wizard will launch. Name the template **vHBA_Template_A**, select the fabric a VSAN, and set the WWN Pool to the WWPN pool previously defined for fabric a. Repeat this process for Fabric B using similar naming standard and the appropriate selections.

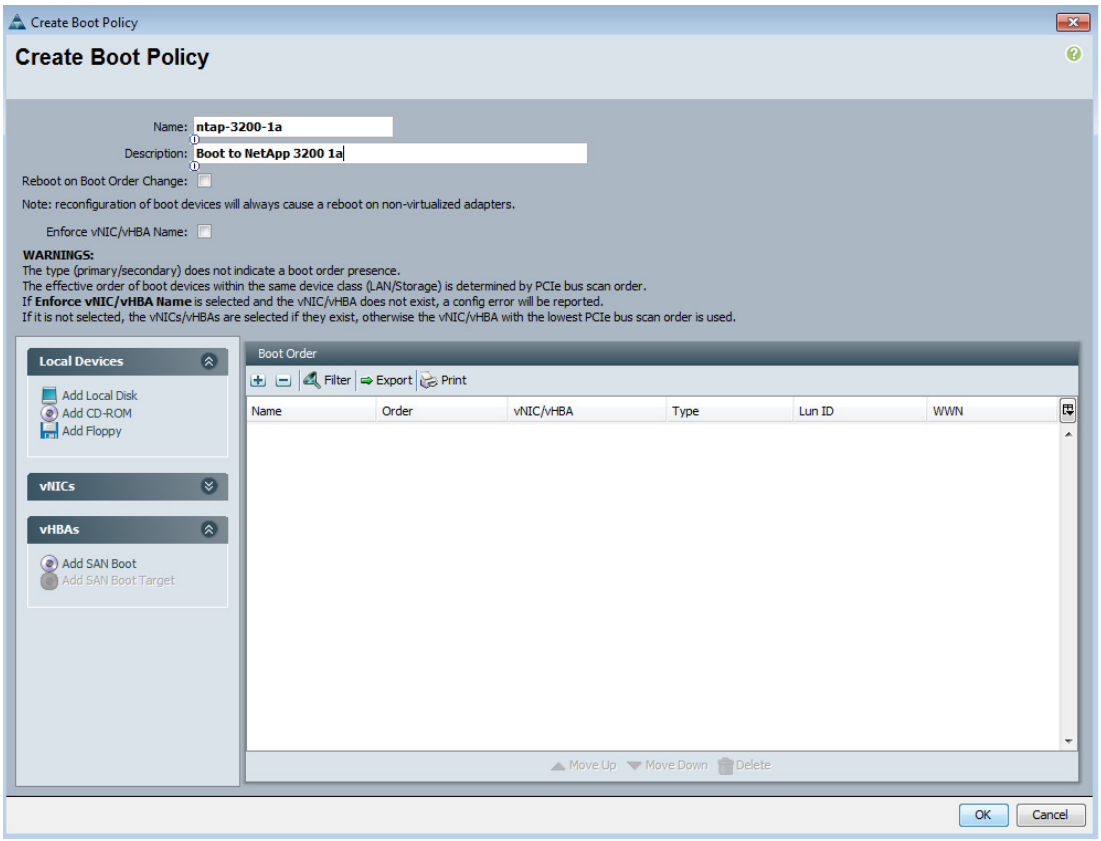
*Figure 19 Create vHBA Template Screen*




## Create Boot Policies

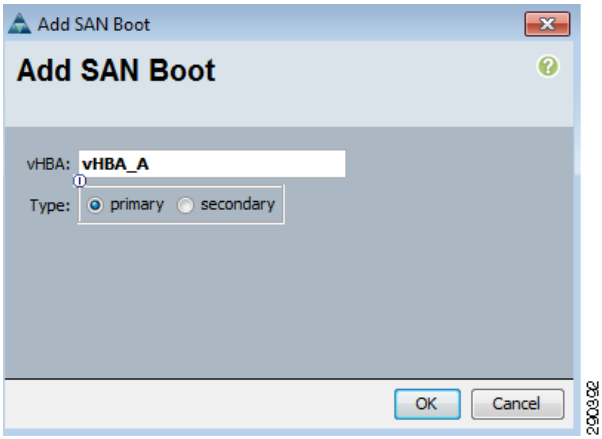
Navigate to the **Servers** tab in the Navigation pane and select **Policies** and the appropriate sub-organization. Select **Create Boot Policy** in the work pane. A wizard window will launch. Name the boot policy after the NetApp controller it will target and provide an optional description of the policy. Leave **Reboot on Boot Order Change** and **Enforce vNIC/vHBA Name** unchecked. Select **Add CD-ROM** under the **Local Devices** menu.

*Figure 20 Create Boot Policy Screen*



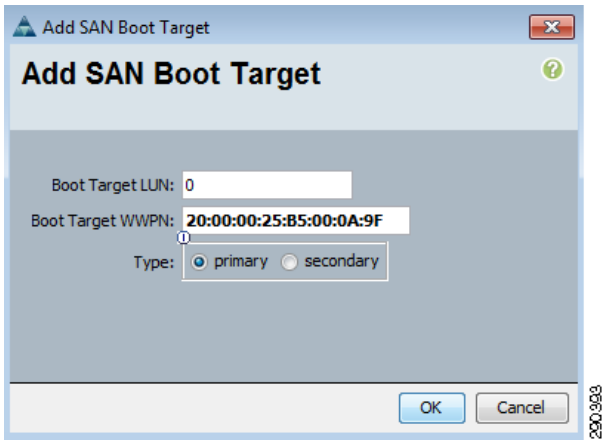

Select **Add SAN Boot** under the **vHBAs** menu.

*Figure 21 Add SAN Boot Screen*




Select **Add SAN Boot Target** under the **vHBAs** menu.

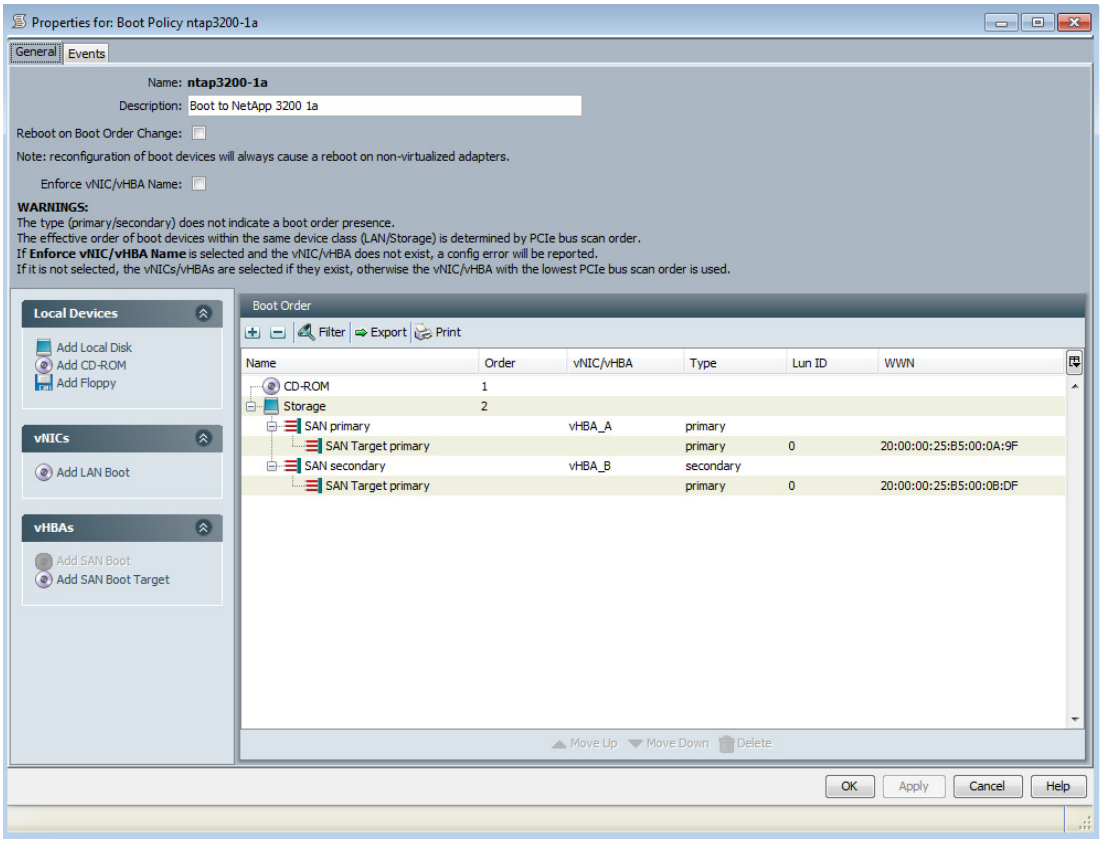
*Figure 22 Add SAN Boot Target Screen*




Note that the Boot Target WWPN matches the NetApp filer defined earlier.

Figure 23 is a complete view of Create Boot Policy workspace. Repeat this process for the secondary filer using similar naming conventions.

*Figure 23 Properties for Boot Policy Screen*



## Create Server Pools

Navigate to the **Servers** tab in the Navigation pane and select **Pools** and the appropriate sub-organization. In the work pane, select **Create Server Pool** to launch the Server Pool wizard application. Complete the forms and migrate the appropriate physical server blade resources into the pool. Click **Finish**.

***Figure 24 Create Server Pool Screen***

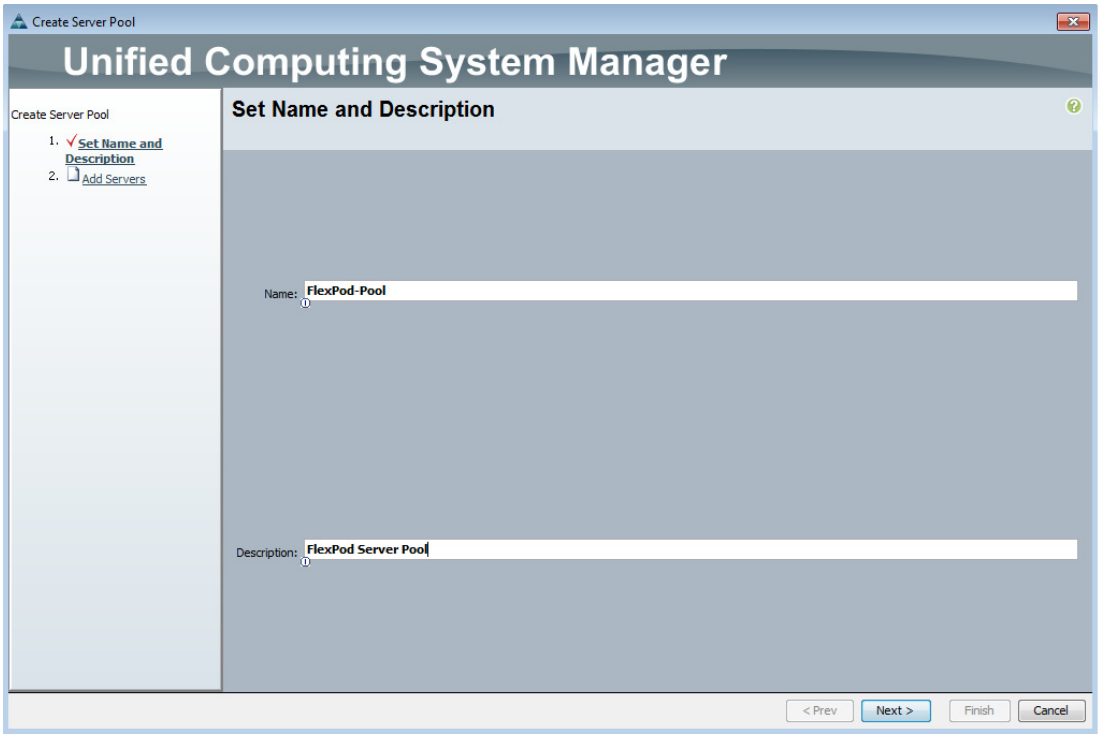
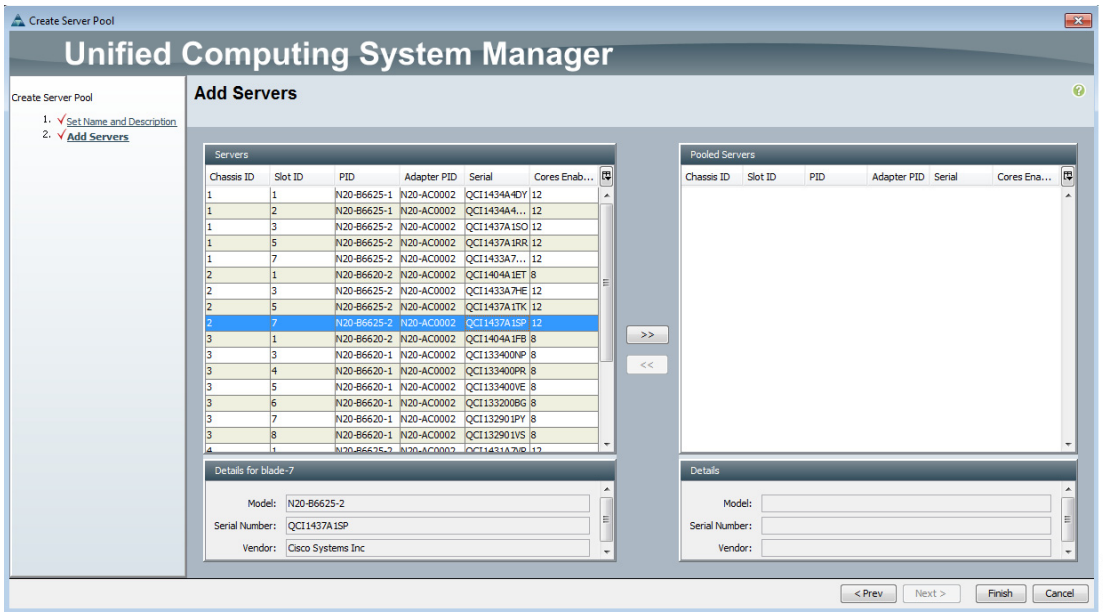


*Figure 25 Create Server Pool—Add Servers Screen*




## Create UUID Suffix Pools

Navigate to the **Servers** tab in the Navigation pane and select **Pools** and the appropriate sub-organization. In the work pane, select **Create UUID Suffix Pool** to launch the associated wizard application. Complete the associated forms and click **Finish**.

*Figure 26 Create UUID Suffix Pool Screen 1*

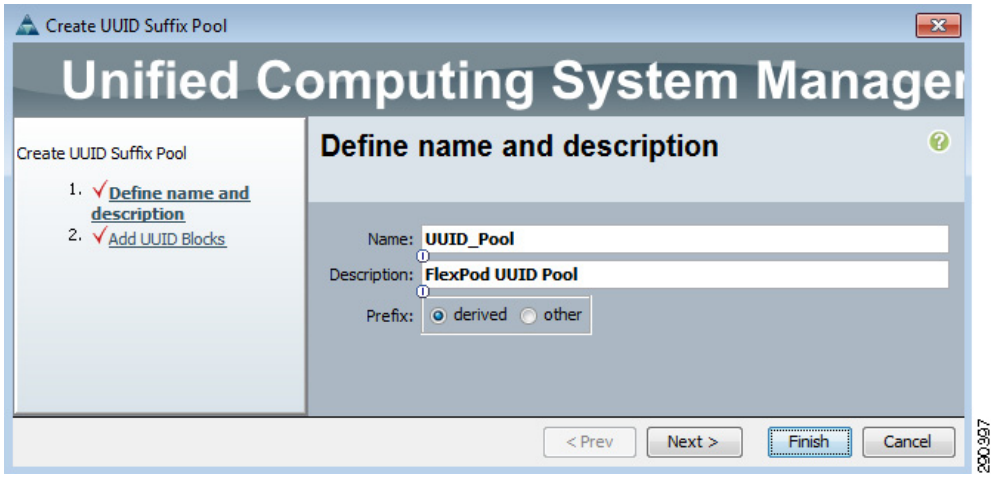
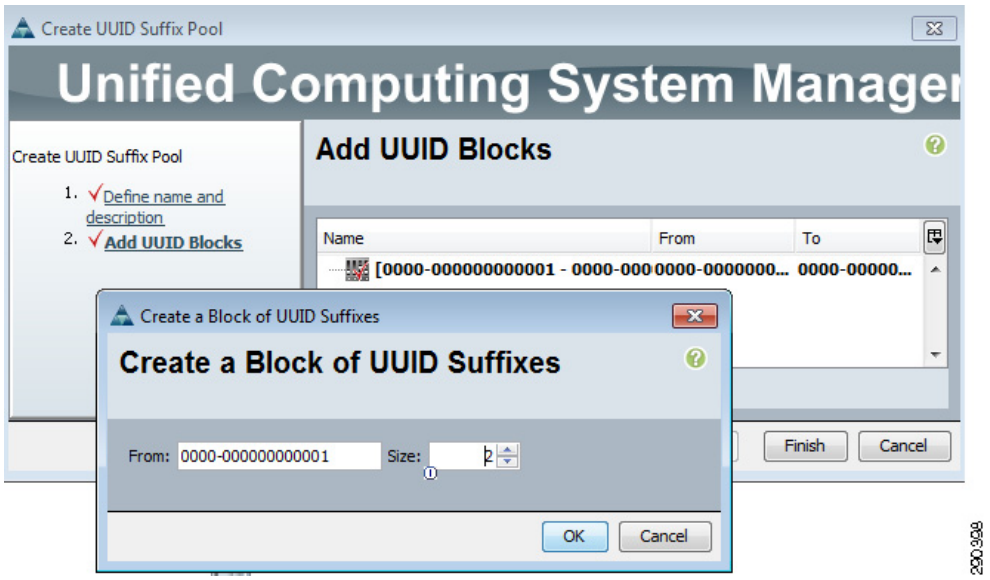


*Figure 27 Create UUID Suffix Pool Screen 2*

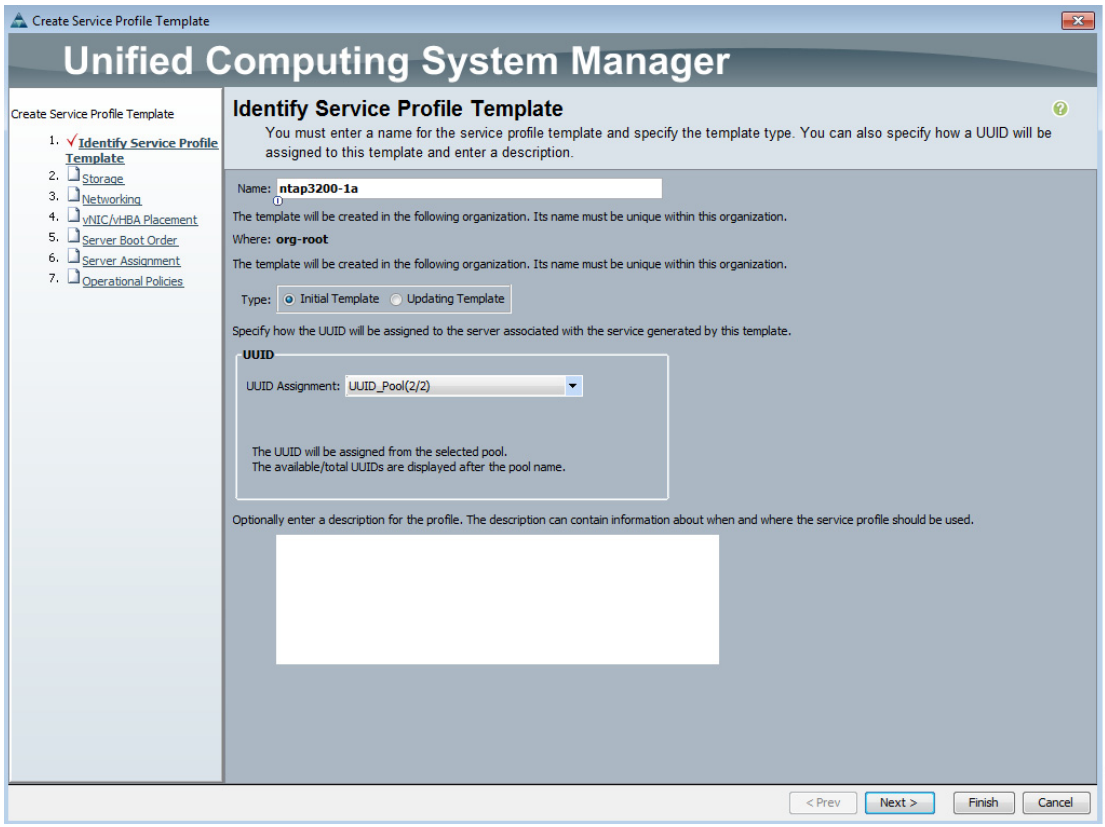



## Create Service Profile Templates

In the Navigation pane, select the **Servers** tab and select the **Service Profile Templates** and the appropriate sub-organization under this item. In the work pane, select **Create Service Profile Template**; the Create Service Profile Template wizard is launched.

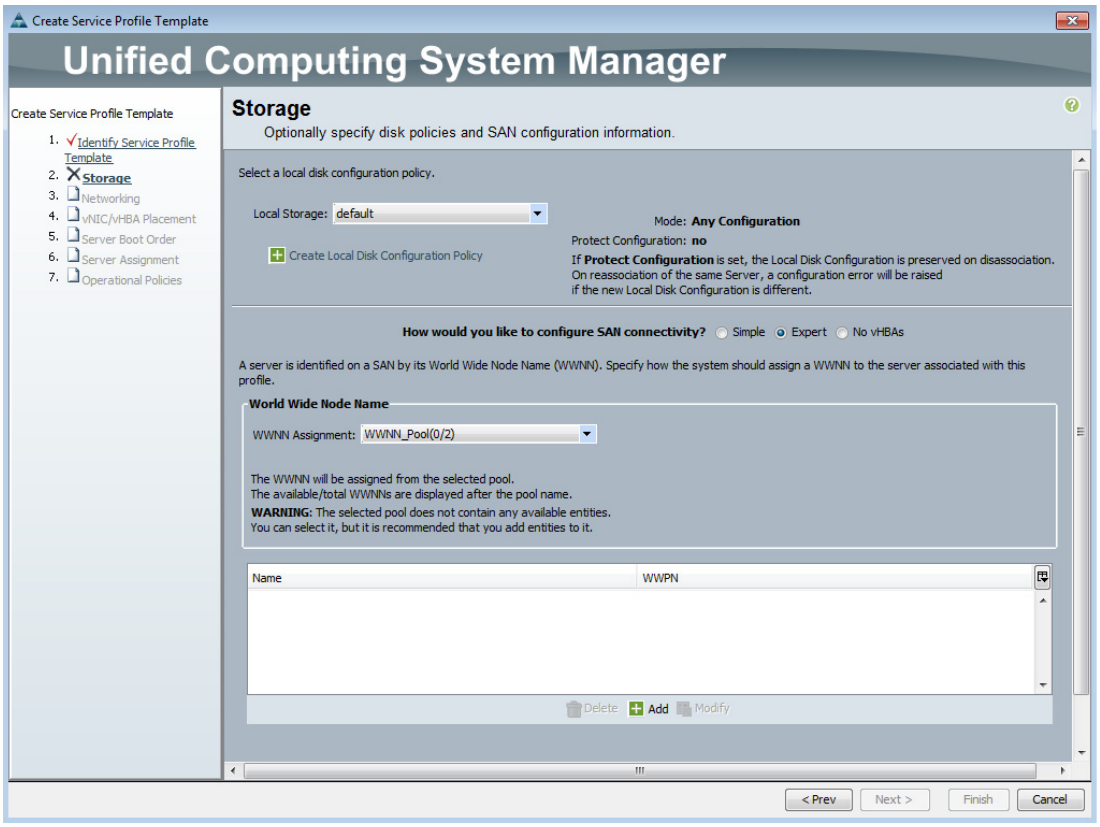
Provide a name for the service profile template; the name should reflect the NetApp controller used to boot service profiles based on this template. Select the UUID Suffix Pool previously defined. Click **Next**.

*Figure 28 Create Service Profile Template—Identify Service Profile Template Screen*



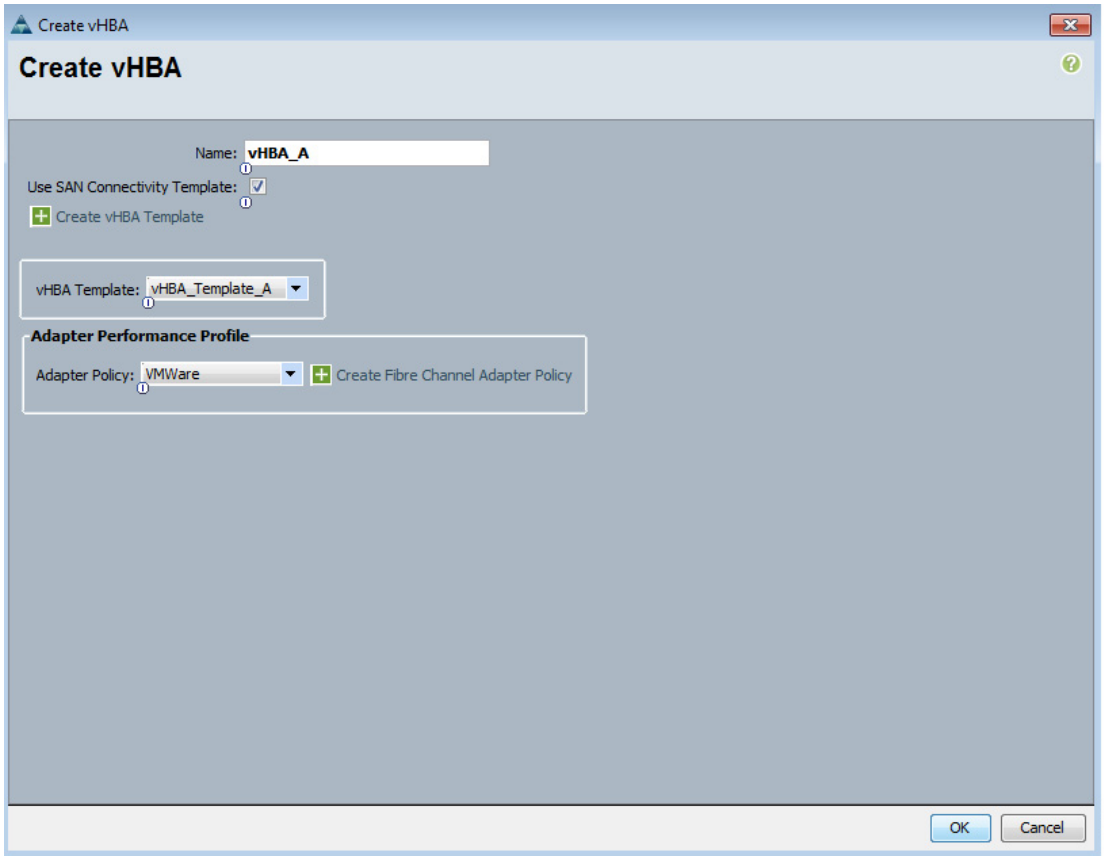

In the work pane, select **default** for Local Storage, select **Expert** SAN configuration mode, and select the WWNN Pool previously defined. Click **Add**.

*Figure 29 Create Service Profile Template—Storage Screen 1*



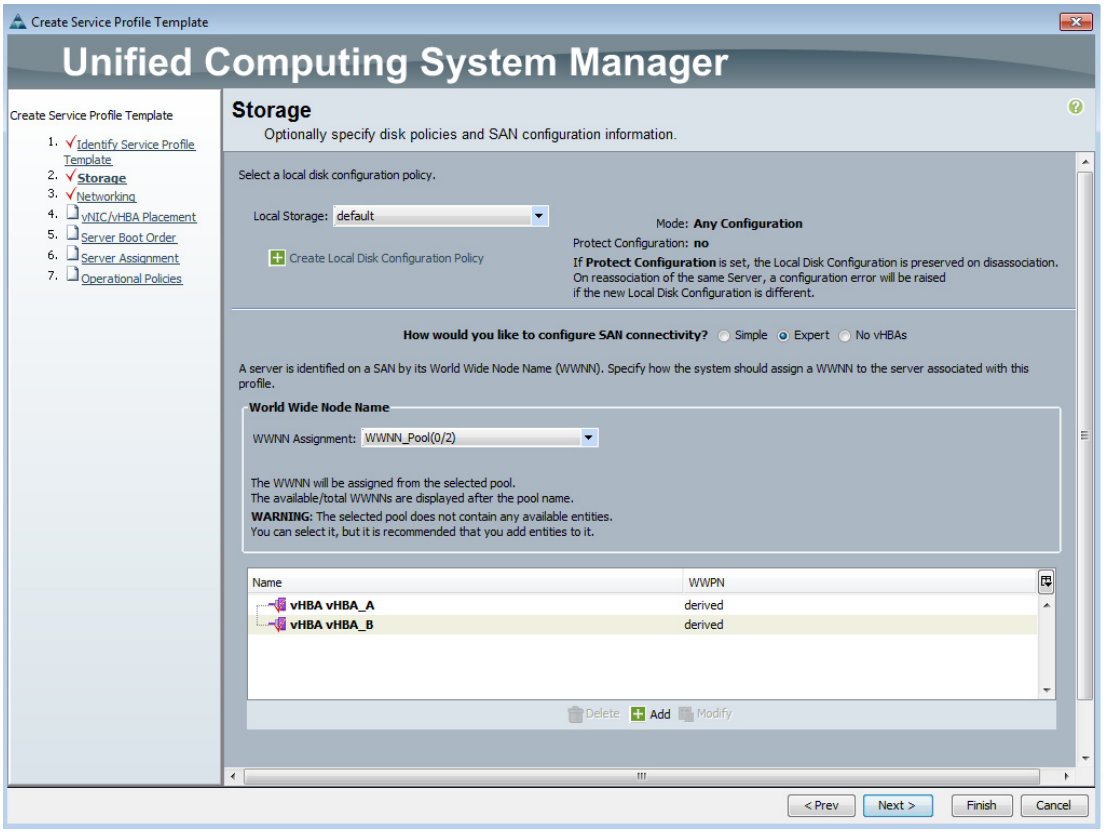

Type a name for the vHBA; it is considered best practice to include the fabric the vHBA is using. Select **Use SAN Connectivity Template** and then select the vHBA Template previously defined that is associated with the fabric. The Adapter Policy should be set to **VMWare**.

*Figure 30 Create vHBA Screen*



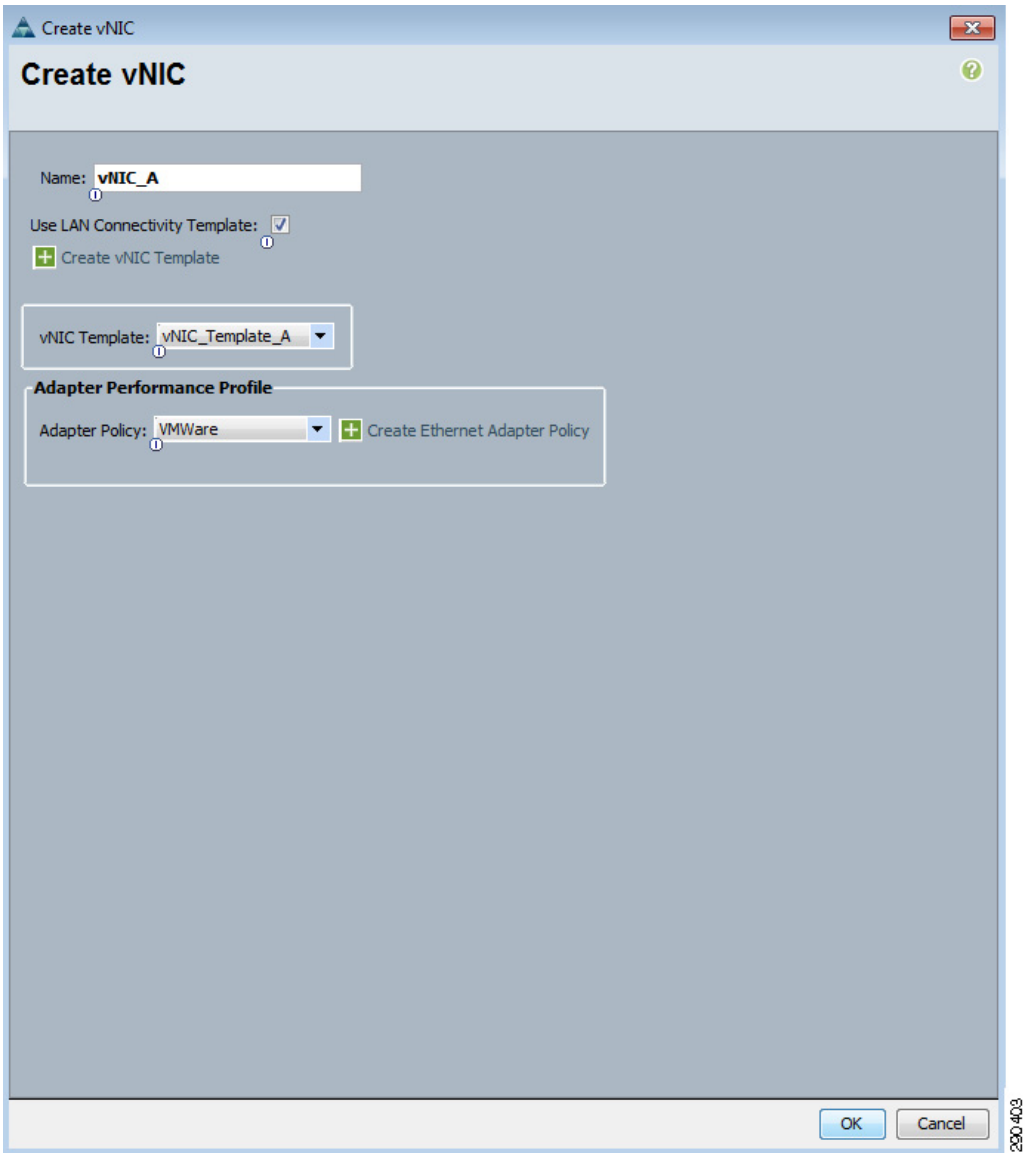

Repeat the previous step using similar naming standards, but referencing fabric b vHBA Template. Click **Next** after returning to the Create Service Profile Template Storage panel.

*Figure 31 Create Service Profile Template—Storage Screen 2*



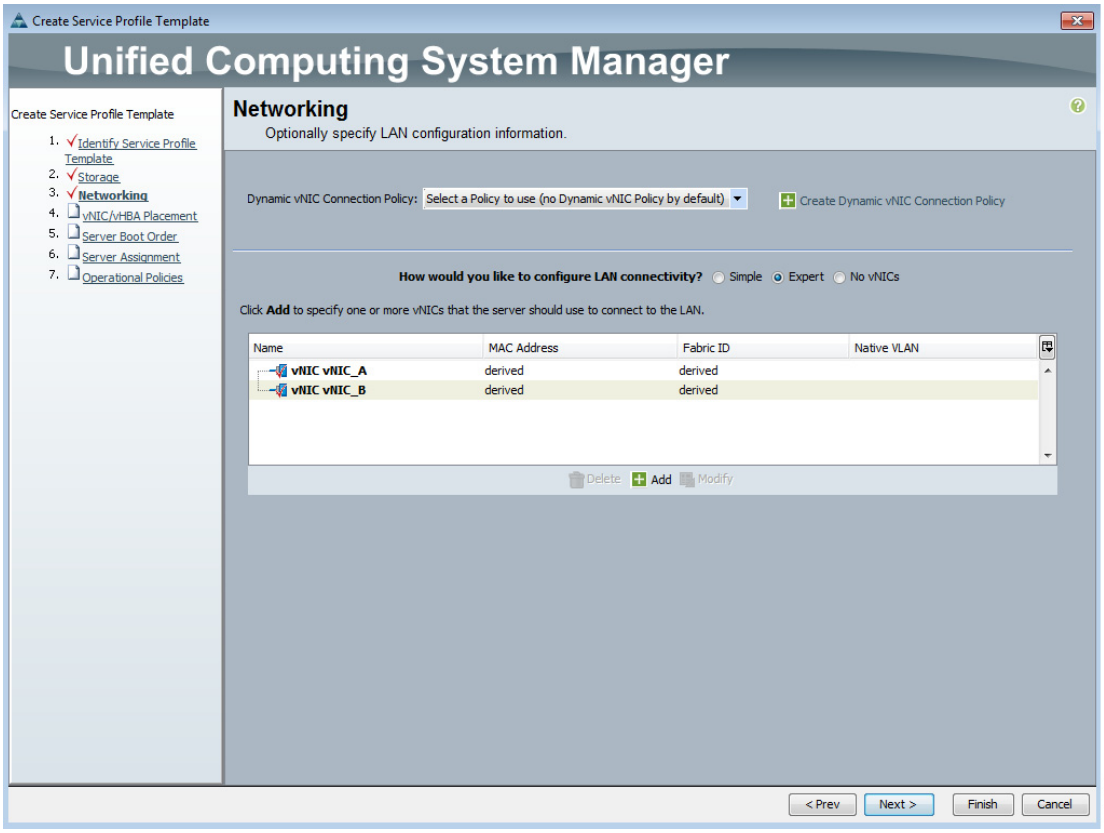

Type a name for the vNIC and select **Use LAN Connectivity Template**. Select the vNIC Template associated with fabric A that was previously created and select the **VMWare** adapter policy. Click **Next** to complete this phase. Repeat this process for the vNIC instantiation on fabric b.

*Figure 32 Create vNIC Screen*



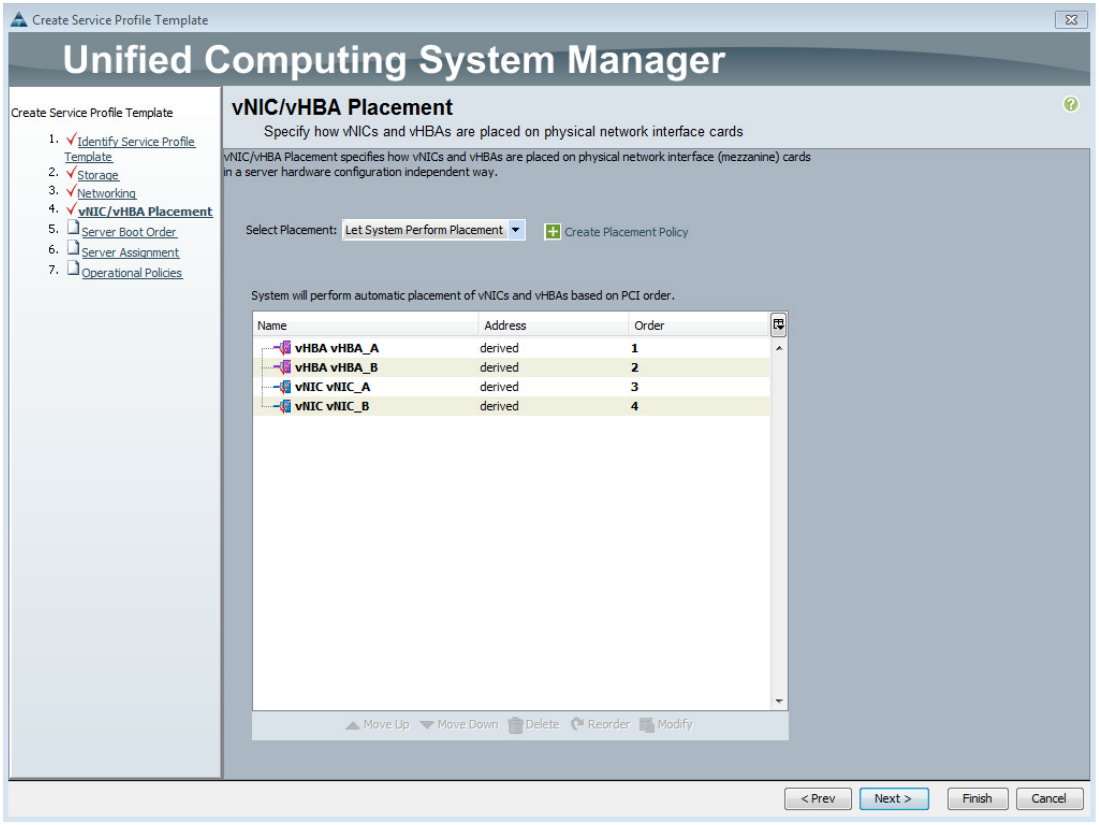

Click **Next** after successfully completing the Network phase of the Service Profile Template creation process.

*Figure 33 Create Service Profile Template—Networking Screen*



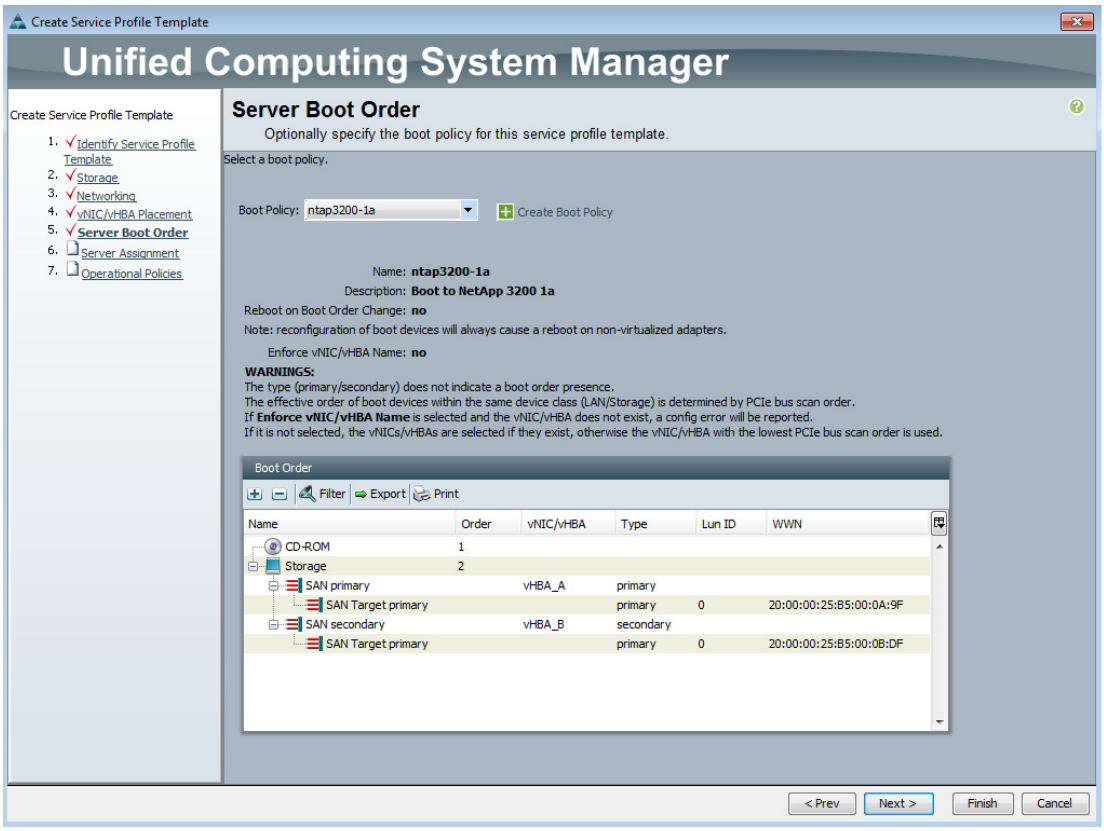

Click **Next** to accept the default placement by the system.

*Figure 34 Create Service Profile Template—vNIC/vHBA Placement Screen*



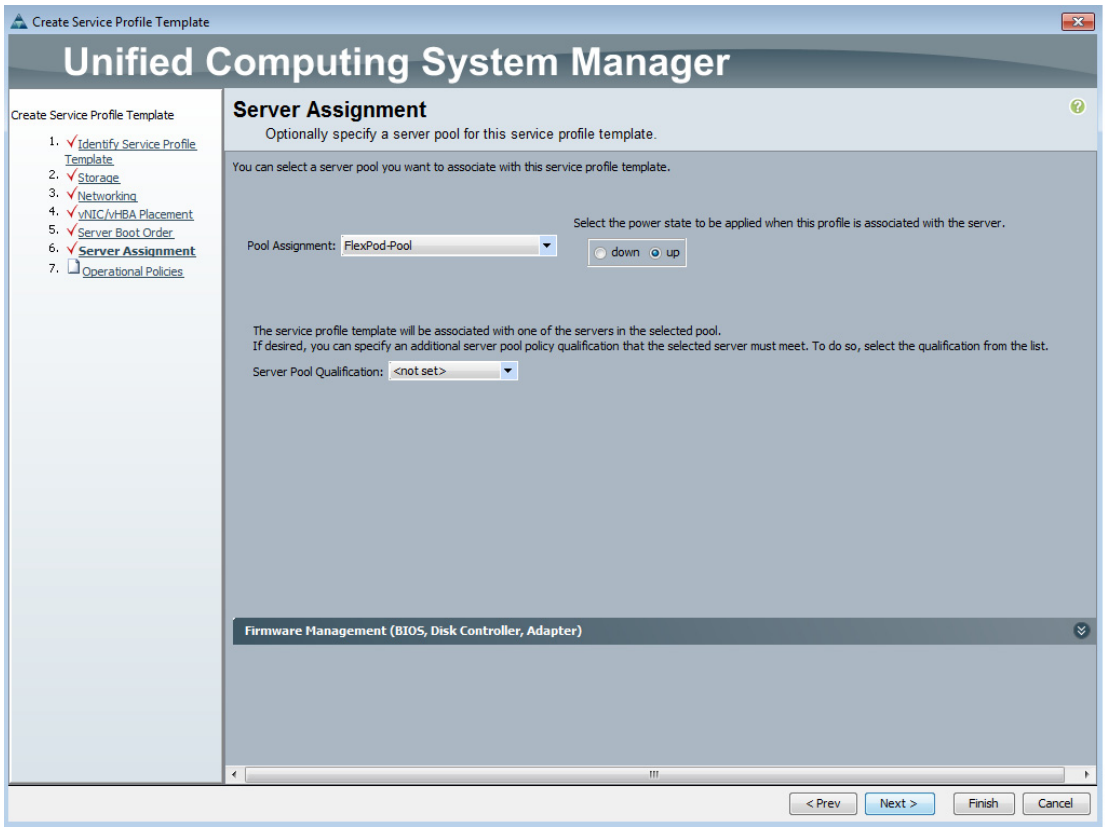

Select the boot policy defined previously for the filer support fabric a. Verify the order, adapters, and targets. Click **Next**.

*Figure 35 Create Service Profile Template—Server Boot Order Screen*




Select the previously-defined server pool associated with this sub-organization. Do not set **Server Pool Qualifications**. Click **Next**.

*Figure 36 Service Profile Template—Server Assignment Screen*



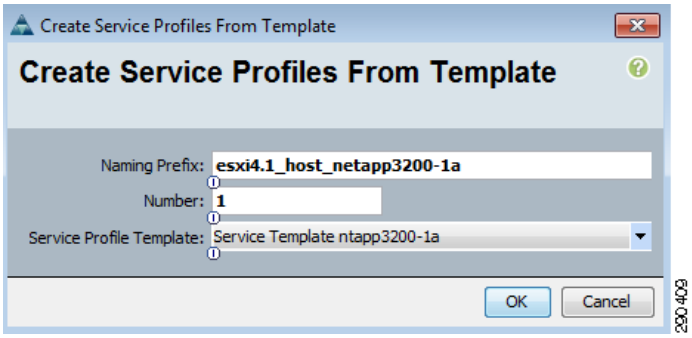

Keep the default operational policies and click **Finish**.

*Figure 37 Service Profile Template—Operational Policies Screen*


## Create Service Profile

In the Navigation pane, select the **Servers** tab and the appropriate sub-organization. In the work pane, select **Create Service Profiles From Template**. The Create Service Profile Template wizard will launch. Name the service profile to reflect the operating system, instance, and storage target. Set the **Number** to **1** and leverage the service profile template previously configured.

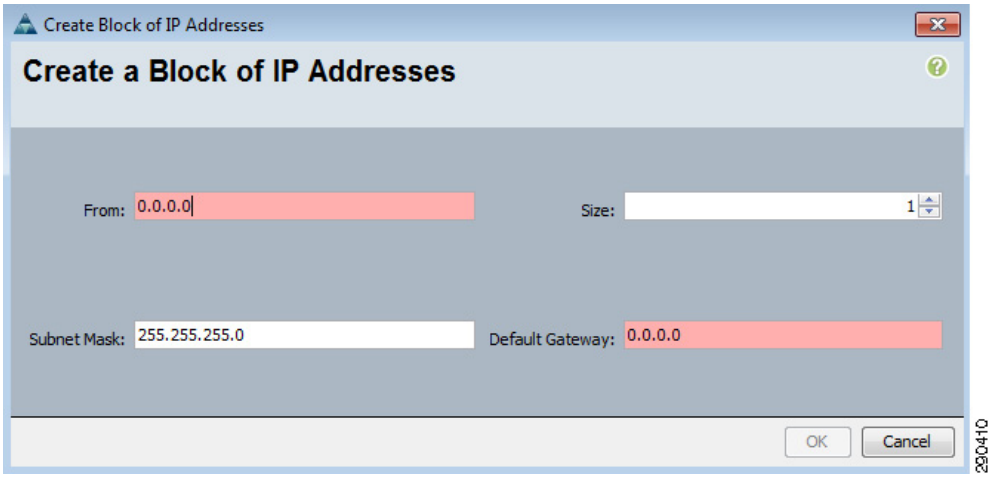
*Figure 38 Create Service Profiles From Template Screen*



## Add a Block of IP Addresses for KVM Access

In the Navigation pane, select **Communication Management** and then **Management IP Pool** to create a pool of KVM IP addresses. In the work pane, click **Create Block of IP Addresses** to launch a form-based wizard. Complete the form using the values related to your environment.

***Figure 39 Create a Block of IP Addresses Screen***




# References

- Cisco Nexus 1010 Virtual Services Appliance: http://www.cisco.com/en/US/products/ps10785/index.html
- Cisco Nexus 5548 Switch: http://www.cisco.com/en/US/products/ps11215/index.html
- Cisco Unified Computing System (UCS): 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 On The Web (NOW) Site: http://.now.netapp.com
- VMware vSphere: http://www.vmware.com/products/vsphere/