

FlexPod Datacenter with VMware vSphere 6.0 and Fibre Channel

Deployment Guide for FlexPod Datacenter with Fibre Channel SAN and VMware vSphere 6.0 and ONTAP 9

Last Updated: November 11, 2016



About Cisco Validated Designs

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit

<http://www.cisco.com/go/designzone>.

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

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

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

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

© 2016 Cisco Systems, Inc. All rights reserved.

Table of Contents

| | |
|---|----|
| About Cisco Validated Designs | 2 |
| Executive Summary | 10 |
| Solution Overview..... | 11 |
| Introduction | 11 |
| Audience | 11 |
| Purpose of this Document..... | 11 |
| What's New? | 11 |
| Solution Design..... | 12 |
| Architecture..... | 12 |
| Physical Topology..... | 13 |
| Deployment Hardware and Software | 17 |
| Software Revisions | 17 |
| Configuration Guidelines..... | 17 |
| Physical Infrastructure..... | 19 |
| FlexPod Cabling | 19 |
| Network Switch Configuration..... | 26 |
| Physical Connectivity | 26 |
| FlexPod Cisco Nexus Base | 26 |
| Set Up Initial Configuration | 26 |
| FlexPod Cisco Nexus Switch Configuration..... | 28 |
| Enable Licenses..... | 28 |
| Set Global Configurations | 29 |
| Create VLANs..... | 29 |
| Add NTP Distribution Interface..... | 30 |
| Add Individual Port Descriptions for Troubleshooting..... | 30 |
| Create Port Channels..... | 32 |
| Configure Port Channel Parameters..... | 34 |
| Configure Virtual Port Channels | 35 |
| Uplink into Existing Network Infrastructure | 37 |
| Storage Configuration | 38 |
| AFF80XX Series Controllers..... | 38 |
| NetApp Hardware Universe | 38 |
| Controllers..... | 38 |

| | |
|--|----|
| Disk Shelves | 38 |
| Clustered Data ONTAP 9.0 | 38 |
| Complete Configuration Worksheet | 38 |
| Configure ONTAP Nodes | 39 |
| Log In to the Cluster | 48 |
| Zero All Spare Disks | 48 |
| Set Onboard Unified Target Adapter 2 Port Personality | 49 |
| Set Auto-Revert on Cluster Management | 49 |
| Set Up Management Broadcast Domain | 49 |
| Set Up Service Processor Network Interface | 50 |
| Create Aggregates | 50 |
| Verify Storage Failover..... | 51 |
| Disable Flow Control on UTA2 Ports | 51 |
| Disable Unused FCoE Capability on CNA Ports | 52 |
| Configure Network Time Protocol | 52 |
| Configure Simple Network Management Protocol..... | 52 |
| Configure AutoSupport | 53 |
| Enable Cisco Discovery Protocol | 53 |
| Create Jumbo Frame MTU Broadcast Domains in Clustered Data ONTAP | 53 |
| Create Interface Groups | 53 |
| Create VLANs..... | 54 |
| Create Storage Virtual Machine | 54 |
| Create Load-Sharing Mirrors of SVM Root Volume | 54 |
| Create Block Protocol (FC) Service..... | 55 |
| Configure HTTPS Access | 55 |
| Configure NFSv3 | 56 |
| Create FlexVol Volumes..... | 56 |
| Create Boot LUNs..... | 56 |
| Schedule Deduplication | 57 |
| Create FCP LIFs..... | 57 |
| Create NFS LIF | 57 |
| Add Infrastructure SVM Administrator..... | 57 |
| Server Configuration | 59 |
| Cisco UCS Base Configuration..... | 59 |
| Perform Initial Setup of Cisco UCS 6332-16UP and 6248UP Fabric Interconnects for FlexPod Environments..... | 59 |

| | |
|---|-----|
| Cisco UCS Setup | 61 |
| Log in to Cisco UCS Manager | 61 |
| Upgrade Cisco UCS Manager Software to Version 3.1(2b) | 61 |
| Anonymous Reporting | 61 |
| Configure Cisco UCS Call Home | 62 |
| Configure Unified Ports | 62 |
| Add Block of IP Addresses for KVM Access | 65 |
| Synchronize Cisco UCS to NTP | 66 |
| Edit Chassis Discovery Policy | 67 |
| Enable Server and Uplink Ports | 68 |
| Acknowledge Cisco UCS Chassis and FEX | 69 |
| Create Uplink Port Channels to Cisco Nexus Switches | 70 |
| Create a WWNN Pool for FC Boot | 71 |
| Create WWPN Pools | 72 |
| Create VSANs | 75 |
| Create FC Uplink Port Channels | 77 |
| Create vHBA Templates | 80 |
| Create SAN Connectivity Policy | 82 |
| Create MAC Address Pools | 84 |
| Create UUID Suffix Pool | 87 |
| Create Server Pool | 88 |
| Create VLANs | 88 |
| Modify Default Host Firmware Package | 91 |
| Set Jumbo Frames in Cisco UCS Fabric | 92 |
| Create Local Disk Configuration Policy (Optional) | 93 |
| Create Network Control Policy for Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) | 94 |
| Create Power Control Policy | 95 |
| Create Server Pool Qualification Policy (Optional) | 96 |
| Create Server BIOS Policy | 98 |
| Update the Default Maintenance Policy | 99 |
| Create vNIC Templates | 99 |
| Create LAN Connectivity Policy | 106 |
| Create vMedia Policy for VMware ESXi 6.0 U2 Install Boot | 109 |
| Create Boot Policy (FC Boot) | 111 |
| Create Service Profile Template (FC Boot) | 115 |

| | |
|---|-----|
| Create vMedia Service Profile Template | 122 |
| Create Service Profiles | 123 |
| Add More Servers to FlexPod Unit | 123 |
| Gather Necessary Information | 124 |
| SAN Switch Configuration | 125 |
| Physical Connectivity | 125 |
| FlexPod Cisco MDS Base | 125 |
| Set Up Initial Configuration | 125 |
| FlexPod Cisco MDS Switch Configuration | 127 |
| Enable Licenses | 127 |
| Configure Individual Ports | 128 |
| Create Port Descriptions - Fabric B | 129 |
| Create VSANs | 130 |
| Create Device Aliases | 130 |
| Create Zones | 131 |
| Storage Configuration - Boot LUNs and Igroups | 132 |
| Clustered Data ONTAP Boot Storage Setup | 132 |
| Create Igroups | 132 |
| Map Boot LUNs to igroups | 132 |
| VMware vSphere 6.0 U2 Setup | 133 |
| VMware ESXi 6.0 U2 | 133 |
| Download Cisco Custom Image for ESXi 6.0 U2 | 133 |
| Log in to Cisco UCS 6300/6200 Fabric Interconnect | 133 |
| Set Up VMware ESXi Installation | 134 |
| Install ESXi | 134 |
| Set Up Management Networking for ESXi Hosts | 135 |
| Download VMware vSphere Client (Optional) | 138 |
| Log in to VMware ESXi Hosts by Using VMware Host Client | 138 |
| Set Up VMkernel Ports and Virtual Switch | 138 |
| Install VMware Drivers for the Cisco Virtual Interface Card (VIC) | 143 |
| Mount Required Datastores | 144 |
| Configure NTP on ESXi Hosts | 147 |
| Move VM Swap File Location | 148 |
| VMware vCenter 6.0 U2 | 148 |
| Install the Client Integration Plug-in | 148 |

| | |
|--|-----|
| Building the VMware vCenter Server Appliance | 149 |
| Setting Up VMware vCenter Server | 157 |
| Add AD User Authentication to vCenter (Optional) | 162 |
| FlexPod VMware vSphere Distributed Switch (vDS) | 164 |
| Configure the VMware vDS in vCenter | 164 |
| FlexPod Management Tools Setup..... | 167 |
| Cisco UCS Performance Manager..... | 167 |
| Cisco UCS Performance Manager OVA Deployment | 167 |
| Cisco UCS Performance Manager Initial Configuration..... | 170 |
| Cisco UCS Performance Manager Deployment | 177 |
| Cisco UCS Performance Manager Configuration of FlexPod Infrastructure..... | 182 |
| NetApp Virtual Storage Console 6.2P2 Deployment Procedure..... | 187 |
| Virtual Storage Console 6.2 Pre-installation Considerations | 187 |
| Install Virtual Storage Console 6.2P2 | 187 |
| Register Virtual Storage Console with vCenter Server..... | 189 |
| Install NetApp NFS VAAI Plug-in..... | 190 |
| Discover and Add Storage Resources | 191 |
| Optimal Storage Settings for ESXi Hosts..... | 191 |
| Virtual Storage Console 6.2P2 Backup and Recovery | 193 |
| OnCommand Performance Manager 7.0 | 197 |
| OnCommand Performance Manager Open Virtualization Format (OVF) Deployment | 197 |
| OnCommand Performance Manager Basic Setup | 201 |
| OnCommand Unified Manager 7.0..... | 204 |
| OnCommand Unified Manager OVF Deployment..... | 204 |
| OnCommand Unified Manager Basic Setup | 210 |
| Link OnCommand Performance Manager and OnCommand Unified Manager..... | 213 |
| Sample Tenant Provisioning..... | 217 |
| Provisioning a Sample Application Tenant | 217 |
| Appendix | 220 |
| Cisco UCS Direct Storage Connect Base Configuration | 220 |
| Perform Initial Setup of Cisco UCS 6332-16UP and 6248UP Fabric Interconnects for FlexPod Environments..... | 220 |
| Cisco UCS Direct Storage Connect Setup | 222 |
| Log in to Cisco UCS Manager..... | 222 |
| Upgrade Cisco UCS Manager Software to Version 3.1(2b) | 222 |
| Anonymous Reporting | 222 |

| | |
|---|-----|
| Configure Cisco UCS Call Home..... | 223 |
| Place UCS Fabric Interconnects in Fiber Channel Switching Mode | 223 |
| Configure Unified Ports..... | 224 |
| Add Block of IP Addresses for KVM Access | 227 |
| Synchronize Cisco UCS to NTP..... | 228 |
| Edit Chassis Discovery Policy | 229 |
| Enable Server and Uplink Ports..... | 230 |
| Acknowledge Cisco UCS Chassis and FEX | 231 |
| Create Uplink Port Channels to Cisco Nexus Switches | 231 |
| Create a WWNN Pool for FC Boot..... | 232 |
| Create WWPN Pools..... | 234 |
| Create Storage VSANs | 237 |
| Assign VSANs to FC Storage Ports..... | 239 |
| Create vHBA Templates | 240 |
| Create SAN Connectivity Policy..... | 243 |
| Create MAC Address Pools | 245 |
| Create UUID Suffix Pool..... | 248 |
| Create Server Pool | 249 |
| Create VLANs..... | 249 |
| Modify Default Host Firmware Package | 252 |
| Set Jumbo Frames in Cisco UCS Fabric..... | 253 |
| Create Local Disk Configuration Policy (Optional) | 254 |
| Create Network Control Policy for Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) | 255 |
| Create Power Control Policy..... | 256 |
| Create Server Pool Qualification Policy (Optional)..... | 257 |
| Create Server BIOS Policy | 259 |
| Update the Default Maintenance Policy..... | 260 |
| Create vNIC Templates..... | 260 |
| Create LAN Connectivity Policy | 267 |
| Create vMedia Policy for VMware ESXi 6.0 U2 Install Boot | 270 |
| Create Boot Policy (FC Boot) | 272 |
| Create Service Profile Templates (FC Boot)..... | 276 |
| Create vMedia Service Profile Template | 283 |
| Create Service Profiles | 284 |
| Add More Servers to FlexPod Unit | 284 |

| | |
|--|-----|
| Gather Necessary Information..... | 285 |
| Adding Direct Connected Tenant FC Storage..... | 285 |
| Create Storage Connection Policies | 285 |
| Map Storage Connection Policies vHBA Initiator Groups in SAN Connectivity Policy | 286 |
| FlexPod Cisco Nexus 1000V vSphere..... | 287 |
| Install Cisco Virtual Switch Update Manager | 287 |
| Install the Cisco Nexus 1000V in VMware using VSUM | 291 |
| Perform Base Configuration of the Primary VSM | 295 |
| Add VMware ESXi Hosts to Cisco Nexus 1000V | 297 |
| Migrate ESXi Host Redundant Network Ports to Cisco Nexus 1000V | 299 |
| Cisco Nexus 1000V vTracker | 300 |
| About the Authors..... | 302 |
| Acknowledgements | 302 |



Executive Summary

Cisco Validated Designs include systems and solutions that are designed, tested, and documented to facilitate and improve customer deployments. These designs incorporate a wide range of technologies and products into a portfolio of solutions that have been developed to address the business needs of customers. Cisco and NetApp have partnered to deliver FlexPod, which serves as the foundation for a variety of workloads and enables efficient architectural designs that are based on customer requirements. A FlexPod solution is a validated approach for deploying Cisco and NetApp technologies as a shared cloud infrastructure.

This document describes the Cisco and NetApp® FlexPod Datacenter with Cisco UCS Manager unified software release 3.1(2b) and VMware vSphere 6.0 U2. Cisco UCS Manager (UCSM) 3.1 provides consolidated support of all current Cisco UCS Fabric Interconnect models (6200, 6300, 6324 (Cisco UCS Mini)), 2200/2300 series IOM, Cisco UCS B-Series, and Cisco UCS C-Series. FlexPod Datacenter with Cisco UCS unified software release 3.1(2b), Fiber Channel SAN, and VMware vSphere 6.0 U2 is a predesigned, best-practice data center architecture built on the Cisco Unified Computing System (UCS), the Cisco Nexus® 9000 family of switches, the Cisco MDS family of switches, and NetApp AFF.

Solution Overview

Introduction

The current industry trend in data center design is towards shared infrastructures. By using virtualization along with pre-validated IT platforms, enterprise customers have embarked on the journey to the cloud by moving away from application silos and toward shared infrastructure that can be quickly deployed, thereby increasing agility and reducing costs. Cisco and NetApp have partnered to deliver FlexPod, which uses best of breed storage, server and network components to serve as the foundation for a variety of workloads, enabling efficient architectural designs that can be quickly and confidently deployed.

Audience

The audience for this document includes, but is not limited to; sales engineers, field consultants, professional services, IT managers, partner engineers, and customers who want to take advantage of an infrastructure built to deliver IT efficiency and enable IT innovation.

Purpose of this Document

This document provides a step by step configuration and implementation guide for the FlexPod Datacenter with Cisco UCS Fabric Interconnects, NetApp AFF, Cisco MDS, and Cisco Nexus 9000 solution. For the design decisions and technology discussion of the solution, please refer to FlexPod Datacenter with VMware 6.0 and Fiber Channel Design Guide:

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi60u2_fc_design.html

What's New?

The following design elements distinguish this version of FlexPod from previous FlexPod models:

- Addition of Cisco MDS Multilayer Fabric Switches to FlexPod
- Support for the Cisco UCS 3.1(2b) unified software release, Cisco UCS B200-M4 servers, and Cisco UCS C220-M4 servers
- Support for the latest release of NetApp Data ONTAP® 9.0
- Fiber channel and NFS storage design
- Validation of VMware vSphere 6.0 U2

Solution Design

Architecture

FlexPod is a defined set of hardware and software that serves as an integrated foundation for both virtualized and non-virtualized solutions. VMware vSphere® built on FlexPod includes NetApp All Flash FAS storage, Cisco Nexus® networking, the Cisco Unified Computing System (Cisco UCS®), and VMware vSphere software in a single package. The design is flexible enough that the networking, computing, and storage can fit in one data center rack or be deployed according to a customer's data center design. Port density enables the networking components to accommodate multiple configurations of this kind.

One benefit of the FlexPod architecture is the ability to customize or "flex" the environment to suit a customer's requirements. A FlexPod can easily be scaled as requirements and demand change. The unit can be scaled both up (adding resources to a FlexPod unit) and out (adding more FlexPod units). The reference architecture detailed in this document highlights the resiliency, cost benefit, and ease of deployment of a fibre channel IP-based storage solution. A storage system capable of serving multiple protocols across a single interface allows for customer choice and investment protection because it truly is a wire-once architecture.

Figure 1 shows the VMware vSphere built on FlexPod components and the network connections for a configuration with the Cisco UCS 6332-16UP Fabric Interconnects and Cisco MDS-based fiber channel (FC) storage. This design has 40 Gb Ethernet connections between the UCS 5108 Blade Chassis and C-Series rackmounts and the Cisco UCS Fabric Interconnect, and between the UCS Fabric Interconnect and Cisco Nexus 9000. This design also has 16 Gb FC connections between the UCS Fabric Interconnect and Cisco MDS, and also between the Cisco MDS and the NetApp AFF family of storage controllers. This infrastructure is deployed to provide FC-booted hosts with file-level and block-level access to shared storage. The reference architecture reinforces the "wire-once" strategy, because as additional storage is added to the architecture, no re-cabling is required from the hosts to the Cisco UCS fabric interconnect.

Physical Topology

Figure 1 FlexPod with Cisco UCS 6332-16UP Fabric Interconnects and Cisco MDS SAN

Unified Computing System
 UCS 6332-16UP Fabric Interconnects & UCS B and C Series Servers

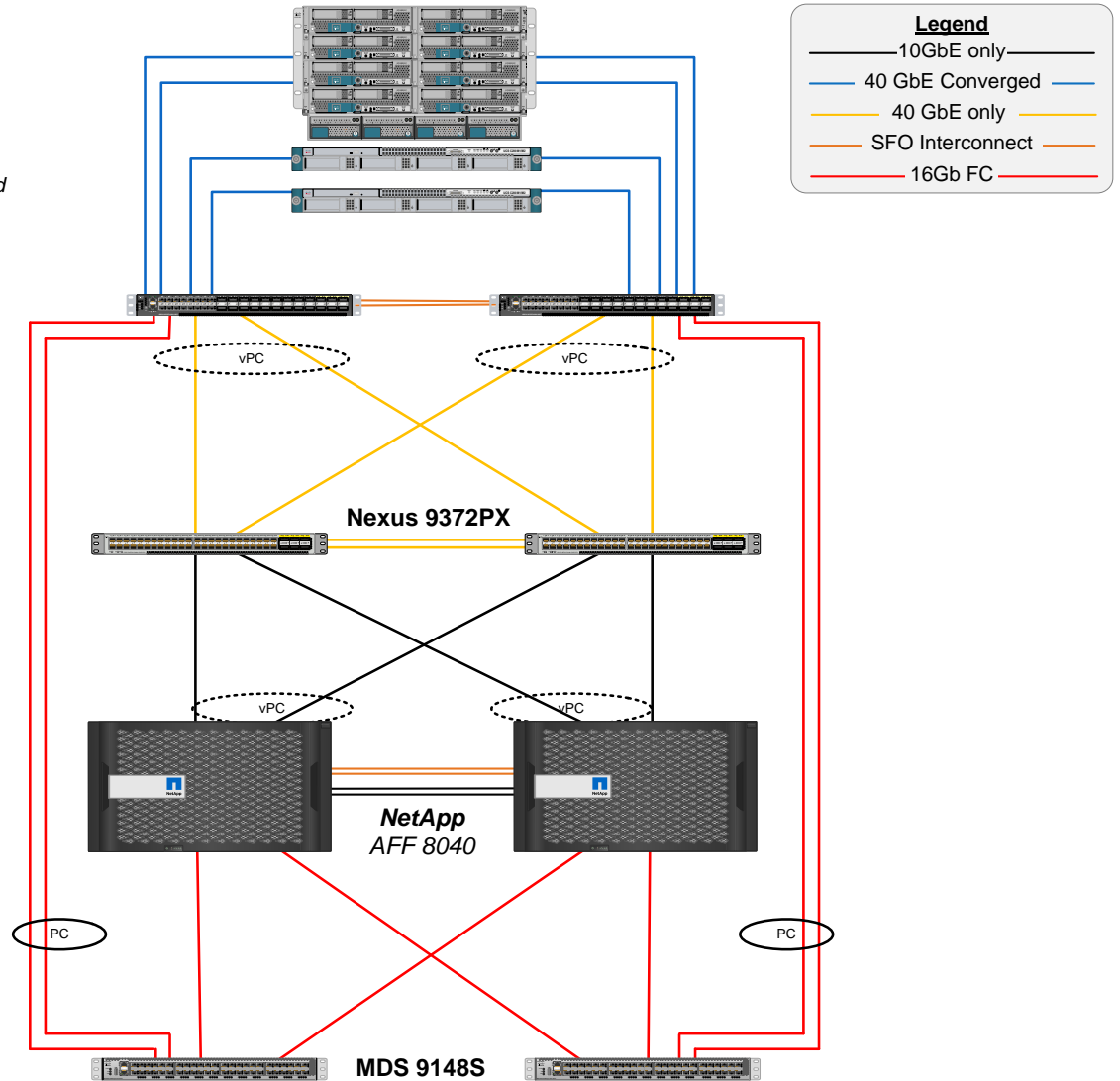


Figure 2 shows the VMware vSphere built on FlexPod components and the network connections for a configuration with the Cisco UCS 6248 Fabric Interconnects and Cisco MDS-based fiber channel (FC) storage. This design has 10 Gb Ethernet connections throughout the architecture. This design also has 8 Gb FC connections between the Cisco UCS Fabric Interconnect and Cisco MDS, and 16 Gb FC connections between the Cisco MDS and the NetApp AFF family of storage controllers. This infrastructure is also deployed to provide FC-booted hosts with file-level and block-level access to shared storage.

Figure 2 FlexPod with Cisco UCS 6248 Fabric Interconnects and Cisco MDS SAN

Unified Computing System
 UCS 6248 Fabric Interconnects,
 Nexus 2232 Fabric Extender
 & UCS C and B Series Servers

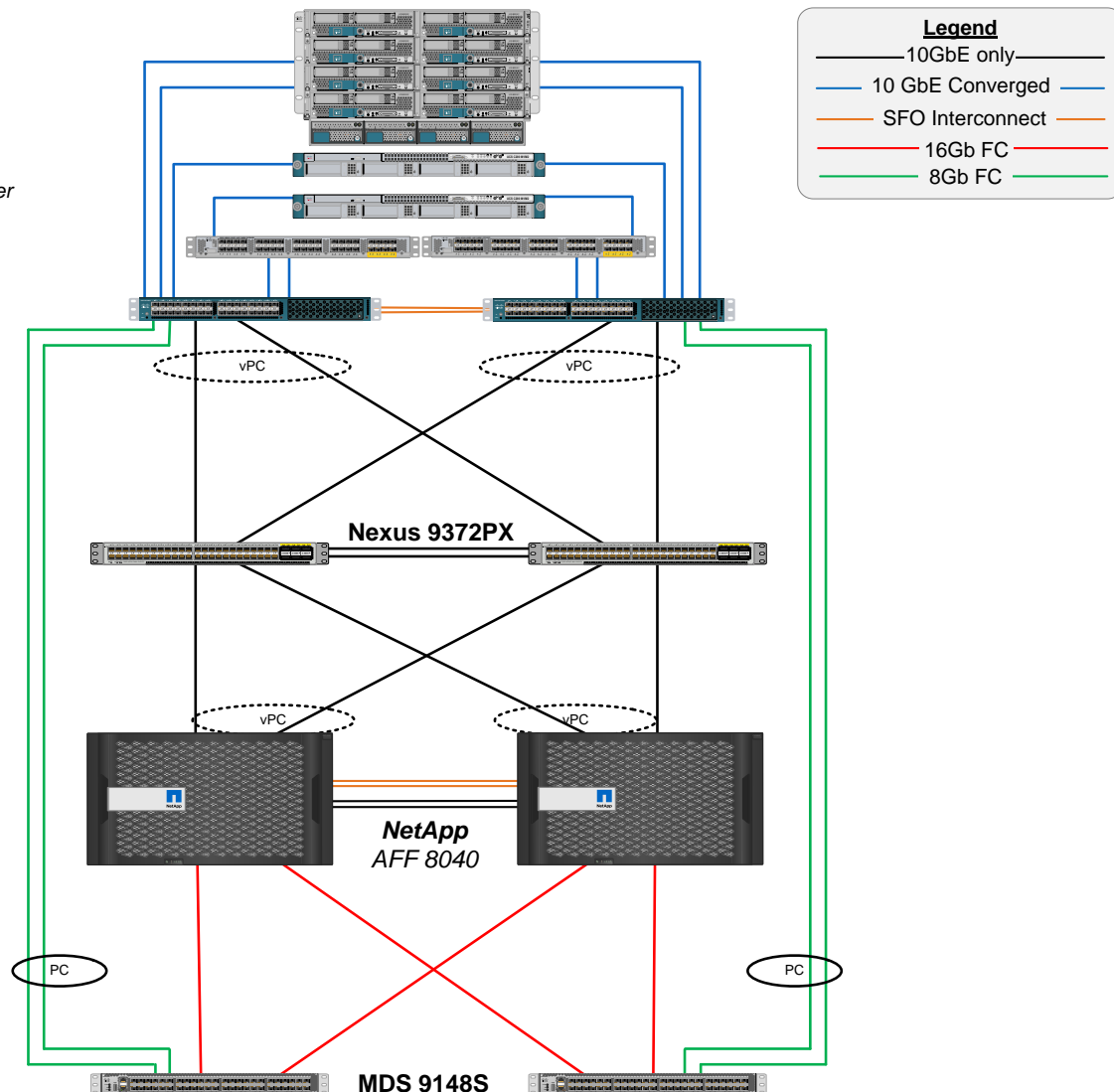


Figure 3 shows the VMware vSphere built on FlexPod components and the network connections for a configuration with the Cisco UCS 6332-16UP Fabric Interconnects with storage FC connections directly connected to the fabric interconnect. This design has 40 Gb Ethernet connections between the Cisco UCS 5108 Blade Chassis and C-Series rackmounts and the Cisco UCS Fabric Interconnect, and between the Cisco UCS Fabric Interconnect and Cisco Nexus 9000. This design also has 16 Gb FC connections between the Cisco UCS Fabric Interconnect and the NetApp AFF family of storage controllers. FC Zoning is done in the Cisco UCS Fabric Interconnect. This infrastructure is deployed to provide FC-booted hosts with file-level and block-level access to shared storage with use cases that do not require the Cisco MDS SAN connectivity or scale.

Figure 3 FlexPod with Cisco UCS 6332-16UP Fabric Interconnects and Cisco UCS Direct Connect SAN

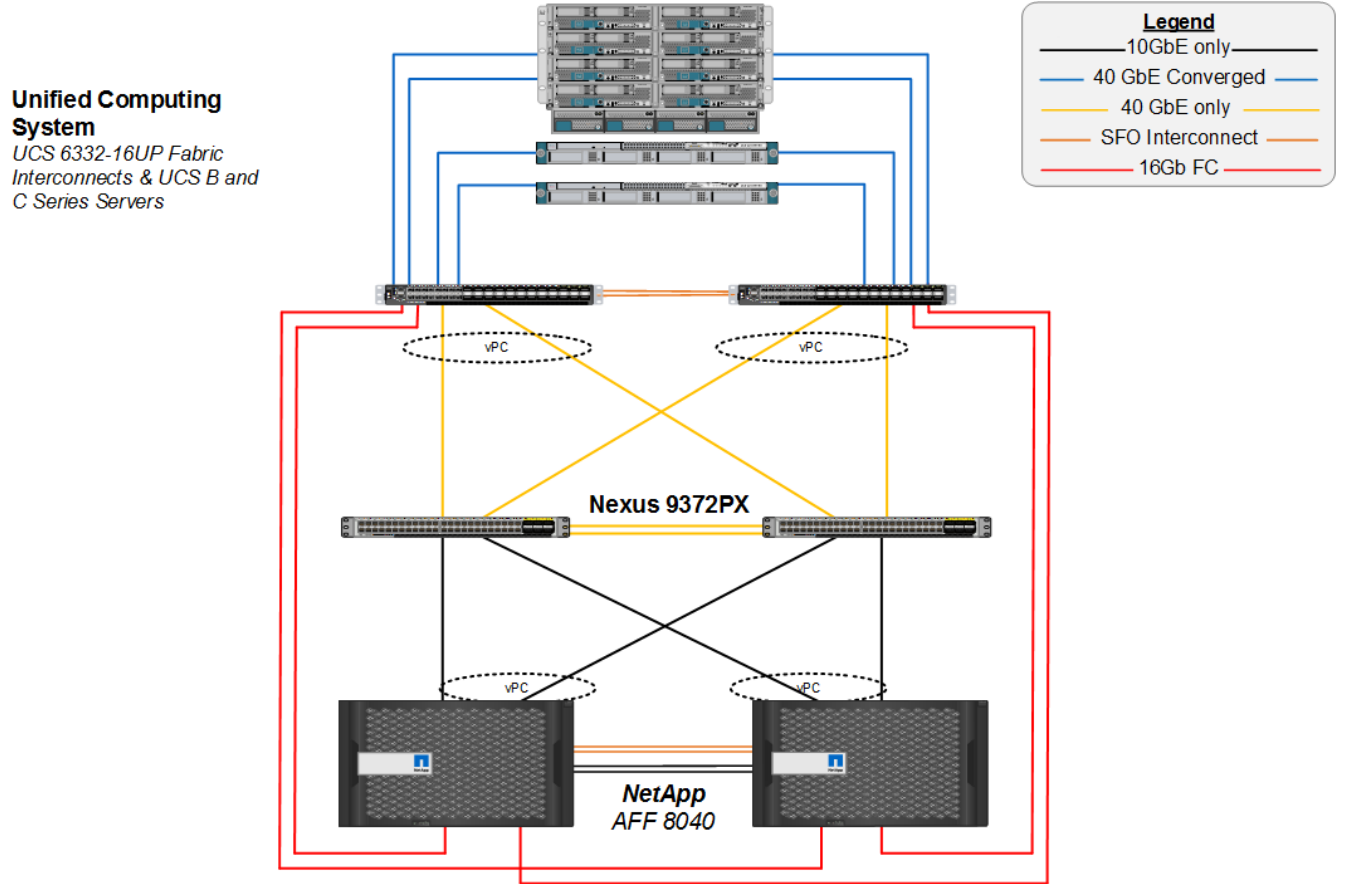
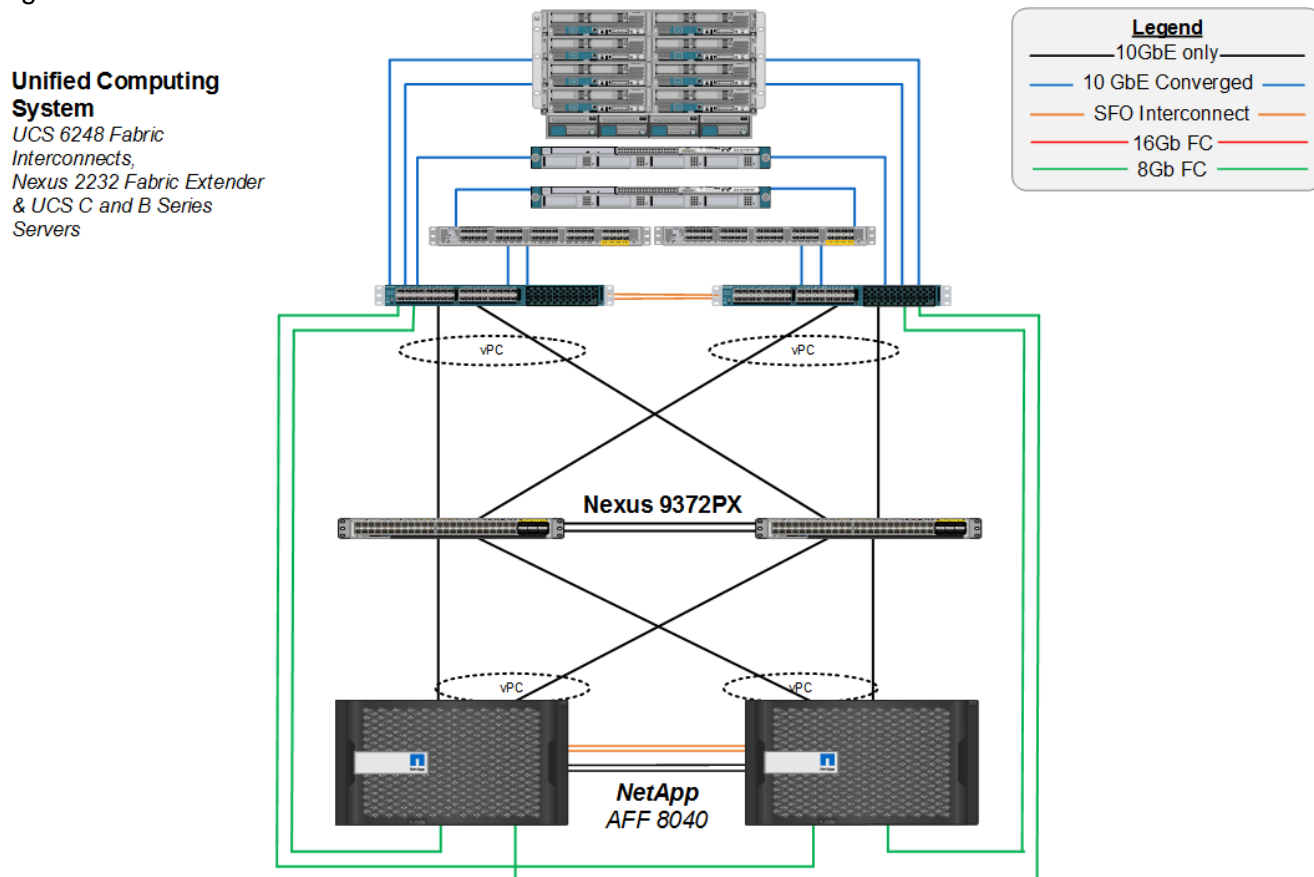


Figure 4 shows the VMware vSphere built on FlexPod components and the network connections for a configuration with the Cisco UCS 6248 Fabric Interconnects with storage FC connections directly connected to the fabric interconnect. This design has 10 Gb Ethernet connections throughout the architecture. This design also has 8 Gb FC connections between the Cisco UCS Fabric Interconnect and the NetApp AFF family of storage controllers. This infrastructure is also deployed to provide FC-booted hosts with file-level and block-level access to shared storage with use cases that do not require the Cisco MDS SAN connectivity or scale.

Figure 4 FlexPod with Cisco UCS 6248 Fabric Interconnects and Cisco UCS Direct Connect SAN



The reference hardware configuration includes:

- Two Cisco Nexus 9372PX switches
- Two Cisco UCS 6332-16UP or Two Cisco UCS 6248UP fabric interconnects
- Two Cisco MDS 9148S Fiber Channel switches
- One NetApp AFF8040 (HA pair) running clustered Data ONTAP with Disk shelves and Solid State Drives (SSD)

For server virtualization, the deployment includes VMware vSphere 6.0 U2. Although this is the base design, each of the components can be scaled easily to support specific business requirements. For example, more (or different) servers or even blade chassis can be deployed to increase compute capacity, additional disk shelves can be deployed to improve I/O capability and throughput, and special hardware or software features can be added to introduce new features. This document guides you through the low-level steps for deploying the base architecture, as shown in Figure 1 through Figure 4. These procedures cover everything from physical cabling to network, compute and storage device configurations.

Deployment Hardware and Software

Software Revisions

Table 1 lists the software revisions for this solution.

Table 1 Software Revisions

| Layer | Device | Image | Comments |
|----------|---|----------------------|--|
| Compute | Cisco UCS Fabric Interconnects 6200 and 6300 Series, Cisco UCS B-200 M4, Cisco UCS C-220 M4 | 3.1(2b) | Includes the Cisco UCS-IOM 2304, 2208XP, and 2204XP Cisco UCS Manager, Cisco UCS VIC 1340 and Cisco UCS VIC 1385 |
| | Cisco eNIC | 2.3.0.10 | |
| | Cisco fNIC | 1.6.0.28 | |
| Network | Cisco Nexus 9000 NX-OS | 7.0(3)I1(3) | |
| | Cisco Nexus 1000V | 5.2(1)SV3(2.1) | |
| Storage | NetApp AFF 8040 | Data ONTAP 9.0 | |
| Software | Cisco UCS Manager | 3.1(2b) | |
| | Cisco UCS Performance Manager | 2.0.2 | |
| | VMware vSphere ESXi | 6.0 U2 Build 4192238 | |
| | VMware vCenter | 6.0 U2 | |
| | NetApp Virtual Storage Console (VSC) | 6.2P2 | |
| | NetApp OnCommand Performance Manager | 7.0 | |
| | NetApp OnCommand Unified Manager | 7.0 | |

Configuration Guidelines

This document provides the details for configuring a fully redundant, highly available configuration for a FlexPod unit with clustered Data ONTAP storage. Therefore, reference is made to which component is being configured with each step, either 01 or 02 or A and B. For example, node01 and node02 are used to identify the two NetApp storage controllers that are provisioned with this document, and Cisco Nexus A or Cisco Nexus B identifies the pair of Cisco Nexus switches that are configured. The Cisco UCS fabric interconnects are similarly configured. Additionally, this document details the steps for provisioning multiple Cisco UCS

hosts, and these examples are identified as: VM-Host-Infra-01, VM-Host-Infra-02 to represent infrastructure and production hosts deployed to each of the fabric interconnects in this document. Finally, to indicate that you should include information pertinent to your environment in a given step, <text> appears as part of the command structure. See the following example for the network port vlan create command:

Usage:

```
network port vlan create ?

[-node] <nodename>                Node

{ [-vlan-name] {<netport>|<ifgrp>} VLAN Name

| -port {<netport>|<ifgrp>}        Associated Network Port

[-vlan-id] <integer> }            Network Switch VLAN Identifier
```

Example:

```
network port vlan -node <node01> -vlan-name i0a-<vlan id>
```

This document is intended to enable you to fully configure the customer environment. In this process, various steps require you to insert customer-specific naming conventions, IP addresses, and VLAN schemes, as well as to record appropriate MAC addresses. Table 3 lists the virtual machines (VMs) necessary for deployment as outlined in this guide. Table 2 describes the VLANs necessary for deployment as outlined in this guide.

Table 2 Necessary VLANs

| VLAN Name | VLAN Purpose | ID Used in Validating This Document |
|------------------|--|-------------------------------------|
| Out of Band Mgmt | VLAN for out-of-band management interfaces | 13 |
| In-Band Mgmt | VLAN for in-band management interfaces | 113 |
| Native | VLAN to which untagged frames are assigned | 2 |
| NFS | VLAN for Infrastructure NFS traffic | 3050 |
| vMotion | VLAN for VMware vMotion | 3000 |
| VM-Traffic | VLAN for Production VM Interfaces | 900 |

Table 3 lists the VMs necessary for deployment as outlined in this document.

Table 3 Virtual Machines

| Virtual Machine Description | Host Name |
|-------------------------------|-----------|
| Active Directory (AD) | |
| vCenter Server | |
| NetApp VSC | |
| OnCommand Unified Manager | |
| OnCommand Performance Manager | |

| Virtual Machine Description | Host Name |
|-------------------------------|-----------|
| Cisco UCS Performance Manager | |

Physical Infrastructure

FlexPod Cabling

The information in this section is provided as a reference for cabling the physical equipment in a FlexPod environment. To simplify cabling requirements, the tables include both local and remote device and port locations.

The tables in this section contain the details for the prescribed and supported configuration of the NetApp AFF8040 running clustered Data ONTAP 9.0



For any modifications of this prescribed architecture, consult the [NetApp Interoperability Matrix Tool](#) (IMT).

This document assumes that out-of-band management ports are plugged into an existing management infrastructure at the deployment site. These interfaces will be used in various configuration steps

Be sure to use the cabling directions in this section as a guide.

The NetApp storage controller and disk shelves should be connected according to best practices for the specific storage controller and disk shelves. For disk shelf cabling, refer to the Universal SAS and ACP Cabling Guide: https://library.netapp.com/ecm/ecm_get_file/ECMM1280392.

Table 4 through Table 13 Table 13 provide the details of all the connections in use in the validation lab. Please use these tables as a reference.



In the lab used for this validation, both Cisco UCS 6248UP and Cisco UCS 6332-16UP Fabric Interconnects were used as noted in these tables.

Table 4 Cisco Nexus 9372-A Cabling Information

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|--------------------|------------|------------|--------------------------|-------------|
| Cisco Nexus 9372 A | Eth1/1 | 10GbE | NetApp Controller 1 | e0b |
| | Eth1/2 | 10GbE | NetApp Controller 2 | e0b |
| | Eth1/9 | 10GbE | Cisco UCS 6248UP FI A | Eth1/27 |
| | Eth1/10 | 10GbE | Cisco UCS 6248UP FI B | Eth1/27 |
| | Eth1/49 | 40GbE | Cisco Nexus 9372 B | Eth1/49 |
| | Eth1/50 | 40GbE | Cisco Nexus 9372 B | Eth1/50 |
| | Eth1/51 | 40GbE | Cisco UCS 6332-16UP FI A | Eth1/39 |

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|--------------|------------|------------|--------------------------|-------------|
| | Eth1/52 | 40GbE | Cisco UCS 6332-16UP FI B | Eth1/39 |
| | MGMT0 | GbE | GbE management switch | Any |



The vPC peer link shown here on 40 GbE ports 1/49 and 1/50 could also be placed on 10 GbE ports. It is recommended to make the total bandwidth of the vPC peer link at least 40 Gb/s if using 40 GbE ports in this architecture.

Table 5 Cisco Nexus 9372-B Cabling Information

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|--------------------|------------|------------|--------------------------|-------------|
| Cisco Nexus 9372 B | Eth1/1 | 10GbE | NetApp Controller 1 | e0d |
| | Eth1/2 | 10GbE | NetApp Controller 2 | e0d |
| | Eth1/9 | 10GbE | Cisco UCS 6248UP FI A | Eth1/28 |
| | Eth1/10 | 10GbE | Cisco UCS 6248UP FI B | Eth1/28 |
| | Eth1/49 | 40GbE | Cisco Nexus 9372 A | Eth1/49 |
| | Eth1/50 | 40GbE | Cisco Nexus 9372 A | Eth1/50 |
| | Eth1/51 | 40GbE | Cisco UCS 6332-16UP FI A | Eth1/40 |
| | Eth1/52 | 40GbE | Cisco UCS 6332-16UP FI B | Eth1/40 |
| | MGMT0 | GbE | GbE management switch | Any |

Table 6 NetApp Controller-1 Cabling Information

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---------------------|------------|------------|-----------------------|-------------|
| NetApp controller 1 | e0M | GbE | GbE management switch | Any |
| | e0i | GbE | GbE management switch | Any |
| | e0P | GbE | SAS shelves | ACP port |
| | e0a | 10GbE | NetApp Controller 2 | e0a |
| | e0b | 10GbE | Cisco Nexus 9372 A | Eth1/1 |
| | e0c | 10GbE | NetApp Controller 2 | e0c |
| | e0d | 10GbE | Cisco Nexus 9372 B | Eth1/1 |

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|--------------|------------|------------|------------------------------|-------------|
| | 0e | 16Gb FC | Cisco MDS 9148S A | FC 1/1 |
| | 0f | 16Gb FC | Cisco MDS 9148S B | FC 1/1 |
| | 0g | 8/16Gb FC | For Direct Connect to UCS FI | |
| | 0h | 8/16Gb FC | For Direct Connect to UCS FI | |



When the term e0M is used, the physical Ethernet port to which the table is referring is the port indicated by a wrench icon on the rear of the chassis.

Table 7 NetApp Controller 2 Cabling Information

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---------------------|------------|------------|------------------------------|-------------|
| NetApp controller 2 | e0M | GbE | GbE management switch | Any |
| | e0i | GbE | GbE management switch | Any |
| | e0P | GbE | SAS shelves | ACP port |
| | e0a | 10GbE | NetApp Controller 1 | e0a |
| | e0b | 10GbE | Cisco Nexus 9372 A | Eth1/2 |
| | e0c | 10GbE | NetApp Controller 1 | e0c |
| | e0d | 10GbE | Cisco Nexus 9372 B | Eth1/2 |
| | 0e | 16Gb FC | Cisco MDS 9148S A | FC 1/2 |
| | 0f | 16Gb FC | Cisco MDS 9148S B | FC 1/2 |
| | 0g | 8/16Gb FC | For Direct Connect to UCS FI | |
| | 0h | 8/16Gb FC | For Direct Connect to UCS FI | |

Table 8 Cisco UCS 6332-16UP Fabric Interconnect A Cabling Information

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---------------------------------|------------|------------|--------------------------------|-------------|
| Cisco UCS fabric interconnect A | FC 1/1 | 16Gb FC | Cisco MDS 9148S A | FC 1/11 |
| | FC 1/2 | 16Gb FC | Cisco MDS 9148S A | FC 1/12 |
| | Eth1/17 | 40GbE | Cisco UCS Chassis 1 2304 FEX A | IOM 1/1 |

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|--------------|------------|------------|--------------------------------|-----------------|
| | Eth1/18 | 40GbE | Cisco UCS Chassis 1 2304 FEX A | IOM 1/2 |
| | Eth1/19 | 40GbE | Cisco UCS C-Series 1 | VIC 1385 Port 0 |
| | Eth1/39 | 40GbE | Cisco Nexus 9372 A | Eth1/51 |
| | Eth1/40 | 40GbE | Cisco Nexus 9372 B | Eth1/51 |
| | MGMT0 | GbE | GbE management switch | Any |
| | L1 | GbE | Cisco UCS 6332-16UP FI B | L1 |
| | L2 | GbE | Cisco UCS 6332-16UP FI B | L2 |

Table 9 Cisco UCS 6332-16UP Fabric Interconnect B Cabling Information

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---------------------------------|------------|------------|--------------------------------|-----------------|
| Cisco UCS fabric interconnect B | FC 1/1 | 16Gb FC | Cisco MDS 9148S B | FC 1/11 |
| | FC 1/2 | 16Gb FC | Cisco MDS 9148S B | FC 1/12 |
| | Eth1/17 | 40GbE | Cisco UCS Chassis 1 2304 FEX B | IOM 1/1 |
| | Eth1/18 | 40GbE | Cisco UCS Chassis 1 2304 FEX B | IOM 1/2 |
| | Eth1/19 | 40GbE | Cisco UCS C-Series 1 | VIC 1385 Port 1 |
| | Eth1/39 | 40GbE | Cisco Nexus 9372 A | Eth1/52 |
| | Eth1/40 | 40GbE | Cisco Nexus 9372 B | Eth1/52 |
| | MGMT0 | GbE | GbE management switch | Any |
| | L1 | GbE | Cisco UCS 6332-16UP FI B | L1 |
| | L2 | GbE | Cisco UCS 6332-16UP FI B | L2 |

Table 10 Cisco UCS 6248UP Fabric Interconnect A Cabling Information

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---------------------------------|------------|------------|-------------------|-------------|
| Cisco UCS fabric interconnect A | FC 1/31 | 8Gb FC | Cisco MDS 9148S A | FC 1/9 |

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|--------------|------------|------------|--------------------------------|-----------------|
| | FC 1/32 | 8Gb FC | Cisco MDS 9148S A | FC 1/10 |
| | Eth1/1 | 10GbE | Cisco UCS Chassis 2 2204 FEX A | IOM 1/1 |
| | Eth1/2 | 10GbE | Cisco UCS Chassis 2 2204 FEX A | IOM 1/2 |
| | Eth1/7 | 10GbE | Cisco UCS C-Series 2 | VIC 1227 Port 0 |
| | Eth1/27 | 10GbE | Cisco Nexus 9372 A | Eth1/9 |
| | Eth1/28 | 10GbE | Cisco Nexus 9372 B | Eth1/9 |
| | MGMT0 | GbE | GbE management switch | Any |
| | L1 | GbE | Cisco UCS 6248UP FI B | L1 |
| | L2 | GbE | Cisco UCS 6248UP FI B | L2 |

Table 11 Cisco UCS 6248UP Fabric Interconnect B Cabling Information

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|---------------------------------|------------|------------|------------------------------|-----------------|
| Cisco UCS fabric interconnect B | FC 1/31 | 8Gb FC | Cisco MDS 9148S B | FC 1/9 |
| | FC 1/32 | 8Gb FC | Cisco MDS 9148S B | FC 1/10 |
| | Eth1/1 | 10GbE | Cisco UCS Chassis 2204 FEX B | IOM 1/1 |
| | Eth1/2 | 10GbE | Cisco UCS Chassis 2204 FEX B | IOM 1/2 |
| | Eth1/7 | 10GbE | Cisco UCS C-Series 2 | VIC 1227 Port 1 |
| | Eth1/27 | 10GbE | Cisco Nexus 9372 A | Eth1/10 |
| | Eth1/28 | 10GbE | Cisco Nexus 9372 B | Eth1/10 |
| | MGMT0 | GbE | GbE management switch | Any |
| | L1 | GbE | Cisco UCS 6248UP FI B | L1 |
| | L2 | GbE | Cisco UCS 6248UP FI B | L2 |

Table 12 Cisco UCS C-Series 1

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|----------------------|------------|------------|--------------------------|-------------|
| Cisco UCS C-Series 1 | Port 0 | 40GbE | Cisco UCS 6332-16UP FI A | Eth1/19 |
| | Port 1 | 40GbE | Cisco UCS 6332-16UP FI B | Eth1/19 |

Table 13 Cisco UCS C-Series 2

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|----------------------|------------|------------|-----------------------|-------------|
| Cisco UCS C-Series 2 | Port 0 | 10GbE | Cisco UCS 6248UP FI A | Eth1/7 |
| | Port 1 | 10GbE | Cisco UCS 6248UP FI B | Eth1/7 |

Table 14 Cisco MDS 9148S-A Cabling Information

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|-------------------|------------|------------|--------------------------|-------------|
| Cisco MDS 9148S-A | FC1/1 | 16Gb FC | NetApp Controller 1 | 0e |
| | FC1/2 | 16Gb FC | NetApp Controller 2 | 0e |
| | FC1/9 | 8Gb FC | Cisco UCS 6248UP FI A | FC1/31 |
| | FC1/10 | 8Gb FC | Cisco UCS 6248UP FI A | FC1/32 |
| | FC1/11 | 16Gb FC | Cisco UCS 6332-16UP FI A | FC1/1 |
| | FC1/12 | 16Gb FC | Cisco UCS 6332-16UP FI A | FC1/2 |
| | MGMT0 | GbE | GbE management switch | Any |



Two additional links can be connected from the Cisco UCS 6248UP fabric interconnects to provide the full storage FC bandwidth to the fabric interconnect.

Table 15 Cisco MDS 9148S-B Cabling Information

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|-------------------|------------|------------|--------------------------|-------------|
| Cisco MDS 9148S-B | FC1/1 | 16Gb FC | NetApp Controller 1 | 0f |
| | FC1/2 | 16Gb FC | NetApp Controller 2 | 0f |
| | FC1/9 | 8Gb FC | Cisco UCS 6248UP FI B | FC1/31 |
| | FC1/10 | 8Gb FC | Cisco UCS 6248UP FI B | FC1/32 |
| | FC1/11 | 16Gb FC | Cisco UCS 6332-16UP FI B | FC1/1 |

| Local Device | Local Port | Connection | Remote Device | Remote Port |
|--------------|------------|------------|--------------------------|-------------|
| | FC1/12 | 16Gb FC | Cisco UCS 6332-16UP FI B | FC1/2 |
| | MGMT0 | GbE | GbE management switch | Any |

Network Switch Configuration

This section provides a detailed procedure for configuring the Cisco Nexus 9000s to use in a FlexPod environment. Follow these steps precisely, failure to do so could result in an improper configuration.

Physical Connectivity

Follow the physical connectivity guidelines for FlexPod as covered in the section "FlexPod Cabling."

FlexPod Cisco Nexus Base

The following procedures describe how to configure the Cisco Nexus switches for use in a base FlexPod environment. This procedure assumes the use of Nexus 9000 7.0(3)I1(3).



The following procedure includes setup of NTP distribution on the In-Band Management VLAN. The interface-vlan feature and ntp commands are used to set this up. This procedure also assumes the default VRF will be used to route the In-Band Management VLAN.

Set Up Initial Configuration

Cisco Nexus 9372PX A

To set up the initial configuration for the Cisco Nexus A switch on <nexus-A-hostname>, complete the following steps:

1. Configure the switch.



On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning.

```

Abort Power on Auto Provisioning and continue with normal setup? (yes/no) [n]: yes

Do you want to enforce secure password standard (yes/no): yes

Enter the password for "admin": <password>

Confirm the password for "admin": <password>

Would you like to enter the basic configuration dialog (yes/no): yes

Create another login account (yes/no) [n]: Enter

Configure read-only SNMP community string (yes/no) [n]: Enter

Configure read-write SNMP community string (yes/no) [n]: Enter

Enter the switch name: <nexus-A-hostname>

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter

Mgmt0 IPv4 address: <nexus-A-mgmt0-ip>

```

```

Mgmt0 IPv4 netmask: <nexus-A-mgmt0-netmask>

Configure the default gateway? (yes/no) [y]: Enter

IPv4 address of the default gateway: <nexus-A-mgmt0-gw>

Configure advanced IP options? (yes/no) [n]: Enter

Enable the telnet service? (yes/no) [n]: Enter

Enable the ssh service? (yes/no) [y]: Enter

Type of ssh key you would like to generate (dsa/rsa) [rsa]: Enter

Number of rsa key bits <1024-2048> [1024]: Enter

Configure the ntp server? (yes/no) [n]: y

NTP server IPv4 address: <global-ntp-server-ip>

Configure default interface layer (L3/L2) [L2]: Enter

Configure default switchport interface state (shut/noshut) [noshut]: shut

Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]: Enter

Would you like to edit the configuration? (yes/no) [n]: Enter

2. Review the configuration summary before enabling the configuration.

Use this configuration and save it? (yes/no) [y]: Enter

```

Cisco Nexus 9372PX B

To set up the initial configuration for the Cisco Nexus B switch on <nexus-B-hostname>, complete the following steps:

1. Configure the switch.



On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning.

```

Abort Power on Auto Provisioning and continue with normal setup? (yes/no) [n]: yes

Do you want to enforce secure password standard (yes/no): yes

Enter the password for "admin": <password>

Confirm the password for "admin": <password>

Would you like to enter the basic configuration dialog (yes/no): yes

Create another login account (yes/no) [n]: Enter

Configure read-only SNMP community string (yes/no) [n]: Enter

Configure read-write SNMP community string (yes/no) [n]: Enter

Enter the switch name: <nexus-B-hostname>

```

```
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
Mgmt0 IPv4 address: <nexus-B-mgmt0-ip>
Mgmt0 IPv4 netmask: <nexus-B-mgmt0-netmask>
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway: <nexus-B-mgmt0-gw>
Configure advanced IP options? (yes/no) [n]: Enter
Enable the telnet service? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter

Type of ssh key you would like to generate (dsa/rsa) [rsa]: Enter
Number of rsa key bits <1024-2048> [1024]: Enter
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address: <global-ntp-server-ip>
Configure default interface layer (L3/L2) [L2]: Enter
Configure default switchport interface state (shut/noshut) [noshut]: shut
Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]: Enter
Would you like to edit the configuration? (yes/no) [n]: Enter

2. Review the configuration summary before enabling the configuration.

Use this configuration and save it? (yes/no) [y]: Enter
```

FlexPod Cisco Nexus Switch Configuration

Enable Licenses

Cisco Nexus 9372PX A and Cisco Nexus 9372PX B

To license the Cisco Nexus switches, complete the following steps:

1. Log in as admin.
2. Run the following commands:

```
config t
feature interface-vlan
feature lACP
feature vpc
feature lldp
```


Set Global Configurations

Cisco Nexus 9372PX A and Cisco Nexus 9372PX B

To set global configurations, complete the following step on both switches:

1. Run the following commands to set global configurations:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
port-channel load-balance src-dst l4port
ntp server <global-ntp-server-ip> use-vrf management
ntp master 3
ip route 0.0.0.0/0 <ib-mgmt-vlan-gateway>
copy run start
```

Create VLANs

Cisco Nexus 9372PX A and Cisco Nexus 9372PX B

To create the necessary virtual local area networks (VLANs), complete the following step on both switches:

1. From the global configuration mode, run the following commands:

```
vlan <ib-mgmt-vlan-id>
name IB-MGMT-VLAN
exit
vlan <native-vlan-id>
name Native-VLAN
exit
vlan <vmotion-vlan-id>
name vMotion-VLAN
exit
vlan <vm-traffic-vlan-id>
name VM-Traffic-VLAN
exit
vlan <infra-nfs-vlan-id>
name Infra-NFS-VLAN
exit
```

Add NTP Distribution Interface

Cisco Nexus 9372PX A

From the global configuration mode, run the following commands:

```
ntp source <switch-a-ntp-ip>
interface Vlan<ib-mgmt-vlan-id>
ip address <switch-a-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exit
```

Cisco Nexus 9372PX B

From the global configuration mode, run the following commands:

```
ntp source <switch-b-ntp-ip>
interface Vlan<ib-mgmt-vlan-id>
ip address <switch-b-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exit
```

Add Individual Port Descriptions for Troubleshooting

Cisco Nexus 9372PX A

To add individual port descriptions for troubleshooting activity and verification for switch A, complete the following step:



In this step and in further sections, configure the <ucs-6248-clustername> and <ucs-6332-clustername> interfaces as appropriate to your deployment.

From the global configuration mode, run the following commands:

```
interface Eth1/1
description <st-node01>:e0b
exit
interface Eth1/2
description <st-node02>:e0b
exit
interface Eth1/9
description <ucs-6248-clustername>-a:1/27
exit
```

```
interface Eth1/10
description <ucs-6248-clustername>-b:1/27
exit

interface Eth1/49
description <nexus-B-hostname>:1/49
exit

interface Eth1/50
description <nexus-B-hostname>>:1/50
exit

interface Eth1/51
description <ucs-6332-clustername>-a:1/39
exit

interface Eth1/52
description <ucs-6332-clustername>-b:1/39
exit
```

Cisco Nexus 9372PX B

To add individual port descriptions for troubleshooting activity and verification for switch B, complete the following step:

From the global configuration mode, run the following commands:

```
interface Eth1/1
description <st-node01>:e0d
exit

interface Eth1/2
description <st-node02>:e0d
exit

interface Eth1/9
description <ucs-6248-clustername>-a:1/28
exit

interface Eth1/10
description <ucs-6248-clustername>-b:1/28
exit

interface Eth1/49
```

```
description <nexus-A-hostname>:1/49
exit
interface Eth1/50
description <nexus-A-hostname>:1/50
exit
interface Eth1/51
description <ucs-6332-clustername>-a:1/40
exit
interface Eth1/52
description <ucs-6332-clustername>-b:1/40
exit
```

Create Port Channels

Cisco Nexus 9372PX A and Cisco Nexus 9372PX B

To create the necessary port channels between devices, complete the following step on both switches:

From the global configuration mode, run the following commands:

```
interface Po10
description vPC peer-link
exit
interface Eth1/49-50
channel-group 10 mode active
no shutdown
exit
interface Po11
description <st-node01>
exit
interface Eth1/1
channel-group 11 mode active
no shutdown
exit
interface Po12
description <st-node02>
exit
```

```
interface Eth1/2
channel-group 12 mode active
no shutdown
exit
interface Po19
description <ucs-6248-clustername>-a
exit
interface Eth1/9
channel-group 19 mode active
no shutdown
exit
interface Po110
description <ucs-6248-clustername>-b
exit
interface Eth1/10
channel-group 110 mode active
no shutdown
exit
interface Po151
description <ucs-6332-clustername>-a
exit
interface Eth1/51
channel-group 151 mode active
no shutdown
exit
interface Po152
description <ucs-6332-clustername>-b
exit
interface Eth1/52
channel-group 152 mode active
no shutdown
exit
```

```
copy run start
```

Configure Port Channel Parameters

Cisco Nexus 9372PX A and Cisco Nexus 9372PX B

To configure port channel parameters, complete the following step on both switches:

From the global configuration mode, run the following commands:

```
interface Po10

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan <ib-mgmt-vlan-id>, <infra-nfs-vlan-id>, <vmotion-vlan-id>, <vm-traffic-
vlan-id>

spanning-tree port type network

exit

interface Po11

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan <infra-nfs-vlan-id>

spanning-tree port type edge trunk

mtu 9216

exit

interface Po12

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan <infra-nfs-vlan-id>

spanning-tree port type edge trunk

mtu 9216

exit

interface Po19

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan <ib-mgmt-vlan-id>, <infra-nfs-vlan-id>, <vmotion-vlan-id>, <vm-traffic-
vlan-id>

spanning-tree port type edge trunk

mtu 9216
```

```

exit

interface Po110

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan <ib-mgmt-vlan-id>, <infra-nfs-vlan-id>, <vmotion-vlan-id>, <vm-traffic-
vlan-id>

spanning-tree port type edge trunk

mtu 9216

exit

interface Po151

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan <ib-mgmt-vlan-id>, <infra-nfs-vlan-id>, <vmotion-vlan-id>, <vm-traffic-
vlan-id>

spanning-tree port type edge trunk

mtu 9216

exit

interface Po152

switchport mode trunk

switchport trunk native vlan 2

switchport trunk allowed vlan <ib-mgmt-vlan-id>, <infra-nfs-vlan-id>, <vmotion-vlan-id>, <vm-traffic-
vlan-id>

spanning-tree port type edge trunk

mtu 9216

exit

copy run start

```

Configure Virtual Port Channels

Cisco Nexus 9372PX A

To configure virtual port channels (vPCs) for switch A, complete the following step:

From the global configuration mode, run the following commands:

```

vpc domain <nexus-vpc-domain-id>

role priority 10

peer-keepalive destination <nexus-B-mgmt0-ip> source <nexus-A-mgmt0-ip>

```

```
peer-switch
peer-gateway
auto-recovery
delay restore 150
exit
interface Po10
vpc peer-link
exit
interface Po11
vpc 11
exit
interface Po12
vpc 12
exit
interface Po19
vpc 19
exit
interface Po110
vpc 110
exit
interface Po151
vpc 151
exit
interface Po152
vpc 152
exit
copy run start
```

Cisco Nexus 9372PX B

To configure vPCs for switch B, complete the following step:

From the global configuration mode, run the following commands:

```
vpc domain <nexus-vpc-domain-id>
role priority 20
peer-keepalive destination <nexus-A-mgmt0-ip> source <nexus-B-mgmt0-ip>
```



```
peer-switch
peer-gateway
auto-recovery
delay restore 150
exit
interface Po10
vpc peer-link
exit
interface Po11
vpc 11
exit
interface Po12
vpc 12
exit
interface Po19
vpc 19
exit
interface Po110
vpc 110
exit
interface Po151
vpc 151
exit
interface Po152
vpc 152
exit
copy run start
```

Uplink into Existing Network Infrastructure

Depending on the available network infrastructure, several methods and features can be used to uplink the FlexPod environment. If an existing Cisco Nexus environment is present, NetApp recommends using vPCs to uplink the Cisco Nexus 9372PX switches included in the FlexPod environment into the infrastructure. The previously described procedures can be used to create an uplink vPC to the existing environment. Make sure to run `copy run start` to save the configuration on each switch after the configuration is completed.

Storage Configuration

AFF80XX Series Controllers

See the following sections in the Site Requirements Guide to plan the physical location of the storage systems:

- Site Preparation
- System Connectivity Requirements
- Circuit Breaker, Power Outlet Balancing, System Cabinet Power Cord Plugs, and Console Pinout Requirements
- 80xx Series Systems

NetApp Hardware Universe

The NetApp Hardware Universe (HWU) application provides supported hardware and software components for any specific ONTAP version. It provides configuration information for all the NetApp storage appliances currently supported by ONTAP software. It also provides a table of component compatibilities.

Confirm that the hardware and software components that you would like to use are supported with the version of ONTAP that you plan to install by using the [HWU application](#) at the [NetApp Support](#) site. Access the [HWU](#) application to view the system configuration guides. Click the Controllers tab to view the compatibility between different version of ONTAP software and the NetApp storage appliances with your desired specifications. Alternatively, to compare components by storage appliance, click Compare Storage Systems.

Controllers

Follow the physical installation procedures for the controllers found in the [AFF8000 Series product documentation](#) on the [NetApp Support](#) site.

Disk Shelves

NetApp storage systems support a wide variety of disk shelves and disk drives. The complete list of [disk shelves](#) that are supported by the AFF 80xx is available on the [NetApp Support](#) site.

When using SAS disk shelves with NetApp storage controllers, refer to the [SAS Disk Shelves Universal SAS and ACP Cabling Guide](#) for proper cabling guidelines.

Clustered Data ONTAP 9.0

Complete Configuration Worksheet

Before running the setup script, complete the cluster setup worksheet from the [ONTAP 9 Software Setup Guide](#). You must have access to the [NetApp Support](#) site to open the cluster setup worksheet.

Configure ONTAP Nodes

Before running the setup script, review the configuration worksheets in the [ONTAP 9 Software Setup Guide](#) to learn about configuring ONTAP. Table 16 lists the information needed to configure two ONTAP nodes. Customize the cluster detail values with the information applicable to your deployment.

Table 16 ONTAP software installation prerequisites

| Cluster Detail | Cluster Detail Value |
|---------------------------|-----------------------|
| Cluster Node01 IP address | <node01-mgmt-ip> |
| Cluster Node01 netmask | <node01-mgmt-mask> |
| Cluster Node01 gateway | <node01-mgmt-gateway> |
| Cluster Node02 IP address | <node02-mgmt-ip> |
| Cluster Node02 netmask | <node02-mgmt-mask> |
| Cluster Node02 gateway | <node02-mgmt-gateway> |
| Data ONTAP 9.0 URL | <url-boot-software> |

Configure Node 01

To configure node 01, complete the following steps:

1. Connect to the storage system console port. You should see a Loader-A prompt. However, if the storage system is in a reboot loop, press Ctrl-C to exit the autoboot loop when you see this message:

```
Starting AUTOBOOT press Ctrl-C to abort...
```

2. Allow the system to boot up.

```
autoboot
```

3. Press Ctrl-C when prompted.



If ONTAP 9 is not the version of software being booted, continue with the following steps to install new software. If ONTAP 9 is the version being booted, select option 8 and *y* to reboot the node. Then continue with step 14.

4. To install new software, select option 7.

```
7
```

5. Enter *y* to perform an upgrade.

```
y
```

6. Select e0M for the network port you want to use for the download.

```
e0M
```

7. Enter `y` to reboot now.

```
y
```

8. Enter the IP address, netmask, and default gateway for `e0M` in their respective places.

```
<node01-mgmt-ip> <node01-mgmt-mask> <node01-mgmt-gateway>
```

9. Enter the URL where the software can be found.



This web server must be pingable.

```
<url-boot-software>
```

10. Press Enter for the user name, indicating no user name.

11. Enter `y` to set the newly installed software as the default to be used for subsequent reboots.

```
y
```

12. Enter `y` to reboot the node.

```
y
```



When installing new software, the system might perform firmware upgrades to the BIOS and adapter cards, causing reboots and possible stops at the Loader-A prompt. If these actions occur, the system might deviate from this procedure.

13. Press **Ctrl-C** when you see this message:

```
Press Ctrl-C for Boot Menu
```

14. Select option 4 for **Clean Configuration and Initialize All Disks**.

```
4
```

15. Enter `y` to **zero disks, reset config, and install a new file system**.

```
y
```

16. Enter `y` to erase all the data on the disks.

```
y
```



The initialization and creation of the root aggregate can take 90 minutes or more to complete, depending on the number and type of disks attached. When initialization is complete, the storage system reboots. Note that SSDs take considerably less time to initialize. You can continue with the node 02 configuration while the disks for node 01 are zeroing.

Configure Node 02

To configure node 02, complete the following steps:

1. Connect to the storage system console port. You should see a Loader-A prompt. However, if the storage system is in a reboot loop, press Ctrl-C to exit the autoboot loop when you see this message:

```
Starting AUTOBOOT press Ctrl-C to abort...
```

2. Allow the system to boot up.

```
autoboot
```

3. Press Ctrl-C when prompted.



If ONTAP 9 is not the version of software being booted, continue with the following steps to install new software. If ONTAP 9 is the version being booted, select option 8 and *y* to reboot the node. Then continue with step 14.

4. To install new software, select option 7.

```
7
```

5. Enter *y* to perform an upgrade.

```
y
```

6. Select e0M for the network port you want to use for the download.

```
e0M
```

7. Enter *y* to reboot now.

```
y
```

8. Enter the IP address, netmask, and default gateway for e0M in their respective places.

```
<node02-mgmt-ip> <node02-mgmt-mask> <node02-mgmt-gateway>
```

9. Enter the URL where the software can be found.



This web server must be pingable.

```
<url-boot-software>
```

10. Press Enter for the user name, indicating no user name.

11. Enter *y* to set the newly installed software as the default to be used for subsequent reboots.

```
y
```

12. Enter y to reboot the node.

```
y
```



When installing new software, the system might perform firmware upgrades to the BIOS and adapter cards, causing reboots and possible stops at the Loader-A prompt. If these actions occur, the system might deviate from this procedure.

13. Press Ctrl-C when you see this message:

```
Press Ctrl-C for Boot Menu
```

14. Select option 4 for Clean Configuration and Initialize All Disks.

```
4
```

15. Enter y to zero disks, reset config, and install a new file system.

```
y
```

16. Enter y to erase all the data on the disks.

```
y
```



The initialization and creation of the root aggregate can take 90 minutes or more to complete, depending on the number and type of disks attached. When initialization is complete, the storage system reboots. Note that SSDs take considerably less time to initialize.

Set Up Node

From a console port program attached to the storage controller A (node 01) console port, run the node setup script. This script appears when ONTAP 9 boots on the node for the first time.

1. Follow the prompts to set up node 01:

```
Welcome to node setup.

You can enter the following commands at any time:
"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
"exit" or "quit" - if you want to quit the setup wizard.
Any changes you made before quitting will be saved.

To accept a default or omit a question, do not enter a value.

This system will send event messages and weekly reports to NetApp Technical Support.
To disable this feature, enter "autosupport modify -support disable" within 24 hours.
Enabling AutoSupport can significantly speed problem determination and resolution should a problem occur on
your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/

Type yes to confirm and continue {yes}: yes

Enter the node management interface port [e0M]: Enter
Enter the node management interface IP address: <node01-mgmt-ip>
Enter the node management interface netmask: <node01-mgmt-mask>
Enter the node management interface default gateway: <node01-mgmt-gateway>
```

```
A node management interface on port e0M with IP address <node01-mgmt-ip> has been created

This node has its management address assigned and is ready for cluster setup.

To complete cluster setup after all nodes are ready, download and run the System Setup utility from the
NetApp Support Site and use it to discover the configured nodes.

For System Setup, this node's management address is: <node01-mgmt-ip>.

Alternatively, you can use the "cluster setup" command to configure the cluster.
```

2. Press Enter and log in to the node with the admin user ID and no password.
3. At the node command prompt, enter the following commands to set HA mode for storage failover.



If the node responds that the HA mode was already set, then proceed with step 4.

```
::> storage failover modify -mode ha
Mode set to HA. Reboot node to activate HA.

::> system node reboot

Warning: Are you sure you want to reboot node "localhost"? {y|n}: y
```

4. After reboot, set up the node with the preassigned values.

```
Welcome to node setup.

You can enter the following commands at any time:
"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
"exit" or "quit" - if you want to quit the setup wizard.
Any changes you made before quitting will be saved.

To accept a default or omit a question, do not enter a value.

Enter the node management interface port [e0M]: Enter
Enter the node management interface IP address [<node01-mgmt-ip>]: Enter
Enter the node management interface netmask [<node01-mgmt-mask>]: Enter
Enter the node management interface default gateway [<node01-mgmt-gateway>]: Enter

This node has its management address assigned and is ready for cluster setup.

To complete cluster setup after all nodes are ready, download and run the System Setup utility from the
NetApp Support Site and use it to discover the configured nodes.

For System Setup, this node's management address is: <node01-mgmt-ip>.

Alternatively, you can use the "cluster setup" command to configure the cluster.
```

5. Log in to the node as the admin user with no password.
6. Repeat this procedure for storage cluster node 02.

Create Cluster on Node 01

In ONTAP, the first node in the cluster performs the cluster create operation. All other nodes perform a cluster join operation. The first node in the cluster is considered node 01.

Table 17 Cluster create in ONTAP prerequisites

| Cluster Detail | Cluster Detail Value |
|----------------|----------------------|
|----------------|----------------------|

| Cluster Detail | Cluster Detail Value |
|-------------------------------|----------------------------|
| Cluster name | <clustername> |
| ONTAP base license | <cluster-base-license-key> |
| Cluster management IP address | <clustermgmt-ip> |
| Cluster management netmask | <clustermgmt-mask> |
| Cluster management gateway | <clustermgmt-gateway> |
| Cluster node01 IP address | <node01-mgmt-ip> |
| Cluster node01 netmask | <node01-mgmt-mask> |
| Cluster node01 gateway | <node01-mgmt-gateway> |

1. Run the cluster setup command to start the Cluster Setup wizard.

```
cluster setup
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
"exit" or "quit" - if you want to quit the cluster setup wizard.
Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
Do you want to create a new cluster or join an existing cluster? {create, join}:
```



If a login prompt appears instead of the Cluster Setup wizard, start the wizard by logging in with the factory default settings and then enter the `cluster setup` command.

2. Run the following command to create a new cluster:

```
create
```

3. Enter no for the single-node cluster option.

```
Do you intend for this node to be used as a single node cluster? {yes, no} [no]: no
```

4. Enter no for a cluster network using network switches.

```
Will the cluster network be configured to use network switches? [yes]:no
```

5. The system defaults are displayed. Enter yes to use the system defaults. Use the following prompts to configure the cluster ports.

```
Existing cluster interface configuration found:
```

```
Port    MTU    IP            Netmask
e0a     9000   169.254.118.102 255.255.0.0
e0c     9000   169.254.191.92  255.255.0.0
```



```
Do you want to use this configuration? {yes, no} [yes]: no
```

```
System Defaults:
Private cluster network ports [e0a,e0c].
Cluster port MTU values will be set to 9000.
Cluster interface IP addresses will be automatically generated.
```

```
Do you want to use these defaults? {yes, no} [yes]: yes
```



If four ports are being used for the switchless cluster interconnect, enter e0a, e0b, e0c, and e0d for the private cluster network ports above.

6. The steps to create a cluster are displayed.

```
Enter the cluster administrators (username "admin") password: <password>
Retype the password: <password>
```

```
It can take several minutes to create cluster interfaces...
```

```
Step 1 of 5: Create a Cluster
You can type "back", "exit", or "help" at any question.
```

```
Enter the cluster name: <clustername>
Enter the cluster base license key: <cluster-base-license-key>
Creating cluster <clustername>
Enter an additional license key []:<var-fcp-license>
```



The cluster is created. This can take a few minutes.



For this validated architecture, NetApp recommends installing license keys for NetApp SnapRestore® data recovery software, NetApp FlexClone® data replication technology, and the NetApp SnapManager® suite. In addition, install all required storage protocol licenses and all licenses that came with the AFF bundle. After you finish entering the license keys, press Enter.

```
Enter the cluster management interface port [e0e]: e0i
Enter the cluster management interface IP address: <clustermgmt-ip>
Enter the cluster management interface netmask: <clustermgmt-mask>
Enter the cluster management interface default gateway: <clustermgmt-gateway>
```

7. Enter the DNS domain name.

```
Enter the DNS domain names:<dns-domain-name>
Enter the name server IP addresses:<nameserver-ip>
```



If you have more than one name server IP address, separate the IP addresses with a comma.

8. Set up the node.

```
Where is the controller located []:<node-location>
Enter the node management interface port [e0M]: e0M
Enter the node management interface IP address [<node01-mgmt-ip>]: Enter
Enter the node management interface netmask [<node01-mgmt-mask>]: Enter
Enter the node management interface default gateway [<node01-mgmt-gateway>]: Enter
```

```

The node management interface has been modified to use port e0M with IP address <node01-mgmt-ip>.
This system will send event messages and weekly reports to NetApp Technical Support.
To disable this feature, enter "autosupport modify -support disable" within 24 hours.
Enabling AutoSupport can significantly speed problem determination and resolution should a problem occur on
your system.
For further information on AutoSupport, please see: http://support.netapp.com/autosupport/
Press enter to continue: Enter
Cluster "<<var_clustername>>" has been created.
To complete cluster setup, you must join each additional node to the cluster by running "cluster setup" on
each node.

Once all nodes have been joined to the cluster, see the Clustered Data ONTAP Software Setup Guide for
information about additional system configuration tasks. You can find the Software Setup Guide on the NetApp
Support Site.

To complete system configuration, you can use either OnCommand System Manager or the Data ONTAP command-line
interface.

To access OnCommand System Manager, point your web browser to the cluster management IP address
(<clustermgmt-ip>).
To access the command-line interface, connect to the cluster management IP address (for example, ssh
admin@<clustermgmt-ip>).

<clustername>::>

```



The node management interface can be on the same subnet as the cluster management interface, or it can be on a different subnet. In this document, we assume that it is on the same subnet.

Join Node 02 to Cluster

The first node in the cluster performs the `cluster create` operation. All other nodes perform a `cluster join` operation. The first node in the cluster is considered node 01, and the node joining the cluster in this example is node 02.

Table 18 Cluster `join` in ONTAP prerequisites

| Cluster Detail | Cluster Detail Value |
|-------------------------------|-----------------------|
| Cluster name | <clustername> |
| Cluster management IP address | <clustermgmt-ip> |
| Cluster node02 IP address | <node02-mgmt-ip> |
| Cluster node02 netmask | <node02-mgmt-mask> |
| Cluster node02 gateway | <node02-mgmt-gateway> |

To join node 02 to the existing cluster, complete the following steps:

1. If prompted, enter `admin` in the login prompt.

```
admin
```

2. Run the `cluster setup` command to start the Cluster Setup wizard.

```
cluster setup
```

```
This node's storage failover partner is already a member of a cluster.
```

Storage failover partners must be members of the same cluster.
The cluster setup wizard will default to the cluster join dialog.

Welcome to the cluster setup wizard.
You can enter the following commands at any time:
"help" or "?" - if you want to have a question clarified,
"back" - if you want to change previously answered questions, and
"exit" or "quit" - if you want to quit the cluster setup wizard.
Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
Do you want to create a new cluster or join an existing cluster?
{join}:



If a login prompt is displayed instead of the Cluster Setup wizard, start the wizard by logging in using the factory default settings, and then enter the cluster setup command.

3. Run the following command to join a cluster:

```
join
```

4. Data ONTAP detects the existing cluster and agrees to join the same cluster. Follow the prompts to join the cluster.

Existing cluster interface configuration found:

| Port | MTU | IP | Netmask |
|------|------|-----------------|-------------|
| e0a | 9000 | 169.254.1.79 | 255.255.0.0 |
| e0c | 9000 | 169.254.100.157 | 255.255.0.0 |

Do you want to use this configuration? {yes, no} [yes]: no

System Defaults:
Private cluster network ports [e0a,e0c].
Cluster port MTU values will be set to 9000.
Cluster interface IP addresses will be automatically generated.



If four ports are being used for the switchless cluster interconnect, enter e0a, e0b, e0c, and e0d for the private cluster network ports above.

```
Do you want to use these defaults? {yes, no} [yes]:Enter
It can take several minutes to create cluster interfaces...
```

5. The steps to join a cluster are displayed.

```
Step 1 of 3: Join an Existing Cluster
You can type "back", "exit", or "help" at any question.

Enter the name of the cluster you would like to join [<clustername>]:Enter
Joining cluster <clustername>
Starting cluster support services ..

This node has joined the cluster <<var_clustername>>.

Step 2 of 3: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.

SFO is enabled.

Step 3 of 3: Set Up the Node
```

You can type "back", "exit", or "help" at any question.

Notice: HA is configured in management.



The node should find the cluster name. Cluster joining can take a few minutes.

6. Set up the node.

```

Enter the node management interface port [e0M]: e0M
Enter the node management interface IP address [<node02-mgmt-ip>]: Enter
Enter the node management interface netmask [<node02-netmask>]: Enter
Enter the node management interface default gateway [<node02-gw>]: Enter
The node management interface has been modified to use port e0M with IP address <node02-mgmt-ip>.
This system will send event messages and weekly reports to NetApp Technical Support.
To disable this feature, enter "autosupport modify -support disable" within 24 hours.
Enabling AutoSupport can significantly speed problem determination and resolution should a problem occur on
your system.
For further information on AutoSupport, please see: http://support.netapp.com/autosupport/
Press enter to continue: Enter

This node has been joined to cluster "<clustname>".
To complete cluster setup, you must join each additional node to the cluster by running "cluster setup" on
each node.

Once all nodes have been joined to the cluster, see the Clustered Data ONTAP Software Setup Guide for
information about additional system configuration tasks. You can find the Software Setup Guide on the NetApp
Support Site.

To complete system configuration, you can use either OnCommand System Manager or the Data ONTAP command-line
interface.

To access OnCommand System Manager, point your web browser to the cluster management IP address
(<clustermgmt-ip>).
To access the command-line interface, connect to the cluster management IP address (for example, ssh
admin@<clustermgmt-ip>).

```



The node management interface can be on the same subnet as the cluster management interface, or it can be on a different subnet. In this document, we assume that it is on the same subnet.

Log In to the Cluster

To log in to the cluster, complete the following steps:

1. Open an SSH connection to either the cluster IP or host name.
2. Log in to the admin user with the password you provided earlier.

Zero All Spare Disks

To zero all spare disks in the cluster, run the following command:

```
disk zerospares
```



Advanced Data Partitioning should have created a root partition and two data partitions on each SSD drive in an All Flash FAS configuration. Disk autoassign should have assigned one data partition to each node in an HA Pair. If a different disk assignment is required, disk autoassignment must be disabled on both nodes in the HA pair by running the `disk option modify` command. Spare partitions can then be moved from one node to another by running the `disk removeowner` and `disk assign` commands.

Set Onboard Unified Target Adapter 2 Port Personality

To set the personality of the onboard unified target adapter 2 (UTA2), complete the following steps:

1. Verify the Current Mode and Current Type properties of the ports by running the `ucadmin show` command.

```
ucadmin show
```

| Node | Adapter | Current Mode | Current Type | Pending Mode | Pending Type | Admin Status |
|-------------|---------|--------------|--------------|--------------|--------------|--------------|
| <st-node01> | 0e | fc | target | - | - | online |
| <st-node01> | 0f | fc | target | - | - | online |
| <st-node01> | 0g | cna | target | - | - | online |
| <st-node01> | 0h | cna | target | - | - | online |
| <st-node02> | 0e | fc | target | - | - | online |
| <st-node02> | 0f | fc | target | - | - | online |
| <st-node02> | 0g | cna | target | - | - | online |
| <st-node02> | 0h | cna | target | - | - | online |

8 entries were displayed.

2. Verify that the Current Mode and Current Type properties for all ports are set properly. Set ports used for Fibre Channel (FC) connectivity to mode `fc`; otherwise, set them to the mode `cna`. That includes FCoE ports, which should be set to the mode `cna`. The port type for all protocols should be set to `target`. Change the port personality with the following command:

```
ucadmin modify -node <home-node-of-the-port> -adapter <port-name> -mode {fc|cna} -type target
```



The ports must be offline to run this command. To take an adapter offline, run the `fc adapter modify -node <home-node-of-the-port> -adapter <port-name> -state down` command. Ports must be converted in pairs (for example, 0e and 0f). After conversion, a reboot is required, and the ports must be brought back to the up state.

Set Auto-Revert on Cluster Management

To set the `auto-revert` parameter on the cluster management interface, complete the following step:



A storage virtual machine (SVM) is referred to as a `Vserver` (or `vserver`) in the GUI and CLI.

Run the following command:

```
network interface modify -vserver <clustername> -lif cluster_mgmt -auto-revert true
```

Set Up Management Broadcast Domain

By default, all network ports are included in the default broadcast domain. Network ports used for data services (for example, e0b, e0d, e0g, e0h, e0j, e0k, and e0l) should be removed from the default

broadcast domain, leaving just the management network ports (e0i and e0M). To perform this task, run the following commands:

```
broadcast-domain remove-ports -broadcast-domain Default -ports <st-node01>:e0b,<st-node01>:e0d, <st-
node01>:e0g,<st-node01>:e0h,<st-node01>:e0j,<st-node01>:e0k,<st-node01>:e0l,<st-node02>:e0b,<st-
node02>:e0d,<st-node02>:e0g,<st-node02>:e0h,<st-node02>:e0j,<st-node02>:e0k,<st-node02>:e0l
broadcast-domain show
```

Set Up Service Processor Network Interface

To assign a static IPv4 address to the service processor on each node, run the following commands:

```
system service-processor network modify -node <st-node01> -address-family IPv4 -enable true -dhcp none -ip-
address <node01-sp-ip> -netmask <node01-sp-mask> -gateway <node01-sp-gateway>

system service-processor network modify -node <st-node02> -address-family IPv4 -enable true -dhcp none -ip-
address <node02-sp-ip> -netmask <node02-sp-mask> -gateway <node02-sp-gateway>
```



The service processor IP addresses should be in the same subnet as the node management IP addresses.

Create Aggregates

An aggregate containing the root volume is created during the ONTAP setup process. To create additional aggregates, determine the aggregate name, the node on which to create it, and the number of disks it contains.

To create new aggregates, complete the following steps:

1. Run the following commands:

```
aggr create -aggregate aggr1_node01 -node <st-node01> -diskcount <num-disks>
aggr create -aggregate aggr1_node02 -node <st-node02> -diskcount <num-disks>
```



You should have the minimum number of hot spare disks for hot spare disk partitions recommended for your aggregate.



For all flash aggregates, you should have a minimum of one hot spare disk or disk partition. For non-flash homogenous aggregates, you should have a minimum of two hot spare disks or disk partitions. For Flash Pool aggregates, you should have a minimum of two hot spare disks or disk partitions for each disk type.



Start with five disks initially; you can add disks to an aggregate when additional storage is required. In an AFF configuration with a small number of SSDs, you might want to create an aggregate with all but one remaining disk (spare) assigned to the controller.



The aggregate cannot be created until disk zeroing completes. Run the `aggr show` command to display aggregate creation status. Do not proceed until both `aggr1_node1` and `aggr1_node2` are online.

2. Rename the root aggregate on node 01 to match the naming convention for this aggregate on node 02.

```
aggr show
aggr rename -aggregate aggr0 -newname <node01-rootaggrname>
```

Verify Storage Failover

To confirm that storage failover is enabled, run the following commands for a failover pair:

1. Verify the status of storage failover.

```
storage failover show
```



Both <st-node01> and <st-node02> must be capable of performing a takeover. Continue with step 3 if the nodes are capable of performing a takeover.

2. Enable failover on one of the two nodes.

```
storage failover modify -node <st-node01> -enabled true
```



Enabling failover on one node enables it for both nodes.

3. Verify the HA status for a two-node cluster.



This step is not applicable for clusters with more than two nodes.

```
cluster ha show
```

4. Continue with step 6 if high availability is configured.
5. Only enable HA mode for two-node clusters. Do not run this command for clusters with more than two nodes because it causes problems with failover.

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. Verify that hardware assist is correctly configured and, if needed, modify the partner IP address.

```
storage failover hwassist show
storage failover modify -hwassist-partner-ip <node02-mgmt-ip> -node <st-node01>
storage failover modify -hwassist-partner-ip <node01-mgmt-ip> -node <st-node02>
```

Disable Flow Control on UTA2 Ports

NetApp recommends disabling flow control on all of the 10GbE and UTA2 ports that are connected to external devices. To disable flow control, complete the following steps:

1. Run the following commands to configure node 01:

```
network port modify -node <st-node01> -port e0b,e0d,e0e,e0f,e0g,e0h -flowcontrol-admin none
```

```
Warning: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y
```

2. Run the following commands to configure node 02:

```
network port modify -node <st-node02> -port e0b,e0d,e0e,e0f,e0g,e0h -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y
network port show -fields flowcontrol-admin
```

Disable Unused FCoE Capability on CNA Ports

If a UTA2 port is set to CNA mode and is only expected to handle Ethernet data traffic (for example NFS), then the unused FCoE capability of the port should be disabled by setting the corresponding FCP adapter to state down with the `fc adapter modify` command. Here are some examples:

```
fc adapter modify -node <st-node01> -adapter 0g -state down
fc adapter modify -node <st-node01> -adapter 0h -state down
fc adapter modify -node <st-node02> -adapter 0g -state down
fc adapter modify -node <st-node02> -adapter 0h -state down
fc adapter show -fields state
```

Configure Network Time Protocol

To configure time synchronization on the cluster, complete the following steps:

1. Set the time zone for the cluster.

```
timezone <timezone>
```



For example, in the eastern United States, the time zone is `America/New_York`.

2. Set the date for the cluster.

```
date <ccyyymmddhhmm.ss>
```



The format for the date is `<[Century] [Year] [Month] [Day] [Hour] [Minute] . [Second]>` (for example, `201309081735.17`).

3. Configure the Network Time Protocol (NTP) servers for the cluster.

```
cluster time-service ntp server create -server <switch-a-ntp-ip>
cluster time-service ntp server create -server <switch-b-ntp-ip>
```

Configure Simple Network Management Protocol

To configure the Simple Network Management Protocol (SNMP), complete the following steps:

1. Configure basic SNMP information, such as the location and contact. When polled, this information is visible as the `sysLocation` and `sysContact` variables in SNMP.

```
snmp contact <snmp-contact>
snmp location "<snmp-location>"
snmp init 1
```



```
options snmp.enable on
```

2. Configure SNMP traps to send to remote hosts, such as a DFM server or another fault management system.

```
snmp traphost add <oncommand-um-server-fqdn>
```

Configure SNMPv1 Access

To configure SNMPv1 access, set the shared, secret plain-text password (called a community):

```
snmp community add ro <snmp-community>
```

Configure AutoSupport

NetApp AutoSupport® sends support summary information to NetApp through HTTPS. To configure AutoSupport, run the following command:

```
system node autosupport modify -node * -state enable -mail-hosts <mailhost> -transport https -support enable -noteto <storage-admin-email>
```

Enable Cisco Discovery Protocol

To enable the Cisco Discovery Protocol (CDP) on the NetApp storage controllers, run the following command to enable CDP on ONTAP:

```
node run -node * options cdpd.enable on
```



To be effective, CDP must also be enabled on directly connected networking equipment such as switches and routers.

Create Jumbo Frame MTU Broadcast Domains in Clustered Data ONTAP

To create a data broadcast domain with an MTU of 9000, run the following commands to create a broadcast domain for NFS on ONTAP:

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
```

Create Interface Groups

To create the LACP interface groups for the 10GbE data interfaces, run the following commands:

```
ifgrp create -node <st-node01> -ifgrp a0a -distr-func port -mode multimode_lacp
ifgrp add-port -node <st-node01> -ifgrp a0a -port e0b
ifgrp add-port -node <st-node01> -ifgrp a0a -port e0d

ifgrp create -node <st-node02> -ifgrp a0a -distr-func port -mode multimode_lacp
ifgrp add-port -node <st-node02> -ifgrp a0a -port e0b
ifgrp add-port -node <st-node02> -ifgrp a0a -port e0d

ifgrp show
```

Create VLANs

To create VLANs, create NFS VLAN ports and add them to the NFS broadcast domain:

```
network port modify -node <st-node01> -port a0a -mtu 9000
network port modify -node <st-node02> -port a0a -mtu 9000
network port vlan create -node <st-node01> -vlan-name a0a-<infra-nfs-vlan-id>
network port vlan create -node <st-node02> -vlan-name a0a-<infra-nfs-vlan-id>

broadcast-domain add-ports -broadcast-domain Infra_NFS -ports <st-node01>:a0a-<infra-nfs-vlan-id>, <st-
node02>:a0a-<infra-nfs-vlan-id>
```

Create Storage Virtual Machine

To create an infrastructure SVM, complete the following steps:

1. Run the vserver create command.

```
vserver create -vserver Infra-SVM -rootvolume rootvol -aggregate aggr1_node01 -rootvolume-security-style unix
```

2. Select the SVM data protocols to configure, keeping fcp and nfs.

```
vserver remove-protocols -vserver Infra-SVM -protocols iscsi,cifs,ndmp
```

3. Add the two data aggregates to the Infra-SVM aggregate list for the NetApp VSC.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_node01,aggr1_node02
```

4. Enable and run the NFS protocol in the Infra-SVM.

```
nfs create -vserver Infra-SVM -udp disabled
```

5. Turn on the SVM vstorage parameter for the NetApp NFS VAAI plugin.

```
vserver nfs modify -vserver Infra-SVM -vstorage enabled
vserver nfs show
```

Create Load-Sharing Mirrors of SVM Root Volume

To create a load-sharing mirror of an SVM root volume, complete the following steps:

1. Create a volume to be the load-sharing mirror of the infrastructure SVM root volume on each node.

```
volume create -vserver Infra-SVM -volume rootvol_m01 -aggregate aggr1_node01 -size 1GB -type DP
volume create -vserver Infra-SVM -volume rootvol_m02 -aggregate aggr1_node02 -size 1GB -type DP
```

2. Create a job schedule to update the root volume mirror relationships every 15 minutes.

```
job schedule interval create -name 15min -minutes 15
```

3. Create the mirroring relationships.

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path Infra-SVM:rootvol_m01 -type LS -schedule
15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path Infra-SVM:rootvol_m02 -type LS -schedule
15min
```

4. Initialize the mirroring relationship.

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol
snapmirror show
```

Create Block Protocol (FC) Service

Run the following command to create the FCP service on each SVM. This command also starts the FCP service and sets the WWN for the SVM.

```
fcv create -vserver Infra-SVM
fcv show
```

Configure HTTPS Access

To configure secure access to the storage controller, complete the following steps:

1. Increase the privilege level to access the certificate commands.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. Generally, a self-signed certificate is already in place. Verify the certificate, and obtain parameters (for example, <serial-number>) by running the following command:

```
security certificate show
```

3. For each SVM shown, the certificate common name should match the DNS FQDN of the SVM. Delete the two default certificates and replace them with either self-signed certificates or certificates from a certificate authority (CA). To delete the default certificates, run the following commands:

```
security certificate delete -vserver Infra-SVM -common-name Infra-SVM -ca Infra-SVM -type server -serial <serial-number>
```



Deleting expired certificates before creating new certificates is a best practice. Run the `security certificate delete` command to delete expired certificates. In the following command, use TAB completion to select and delete each default certificate.

4. To generate and install self-signed certificates, run the following commands as one-time commands. Generate a server certificate for the Infra-SVM and the cluster SVM. Use TAB completion to aid in the completion of these commands.

```
security certificate create -common-name <cert-common-name> -type server -size 2048 -country <cert-country> -state <cert-state> -locality <cert-locality> -organization <cert-org> -unit <cert-unit> -email-addr <cert-email> -expire-days <cert-days> -protocol SSL -hash-function SHA256 -vserver Infra-SVM
```

5. To obtain the values for the parameters required in step 6 (<cert-ca> and <cert-serial>), run the `security certificate show` command.
6. Enable each certificate that was just created by using the `-server-enabled true` and `-client-enabled false` parameters. Use TAB completion to aid in the completion of these commands.

```
security ssl modify -vserver <clustername> -server-enabled true -client-enabled false -ca <cert-ca> -serial <cert-serial> -common-name <cert-common-name>
```

7. Disable HTTP cluster management access.

```
system services firewall policy delete -policy mgmt -service http -vserver <clustername>
```



It is normal for some of these commands to return an error message stating that the entry does not exist.

8. Change back to the normal admin privilege level and set up the system to allow SVM logs to be available by web.

```
set -privilege admin
vserver services web modify -name spi|ontapi|compat -vserver * -enabled true
```

Configure NFSv3

To configure NFSv3 on the SVM, complete the following steps:

1. Create a new rule for the infrastructure NFS subnet in the default export policy.

```
vserver export-policy rule create -vserver Infra-SVM -policyname default -ruleindex 1 -protocol nfs -clientmatch <infra-nfs-subnet-cidr> -rorule sys -rwrule sys -superuser sys -allow-suid false
```

2. Assign the FlexPod export policy to the infrastructure SVM root volume.

```
volume modify -vserver Infra-SVM -volume rootvol -policy default
```

Create FlexVol Volumes

The following information is required to create a NetApp FlexVol® volume:

- The volume name
- The volume size
- The aggregate on which the volume exists

To create a FlexVol volume, run the following commands:

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate aggr1_node02 -size 500GB -state online -policy default -junction-path /infra_datastore_1 -space-guarantee none -percent-snapshot-space 0

volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_node01 -size 100GB -state online -policy default -junction-path /infra_swap -space-guarantee none -percent-snapshot-space 0 -snapshot-policy none

volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_node01 -size 100GB -state online -policy default -space-guarantee none -percent-snapshot-space 0

snapmirror update-ls-set -source-path Infra-SVM:rootvol
```

Create Boot LUNs

To create two boot LUNs, run the following commands:

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-01 -size 15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-02 -size 15GB -ostype vmware -space-reserve disabled
```

Schedule Deduplication

On NetApp All Flash FAS systems, deduplication is enabled by default. To schedule deduplication, complete the following step:

After the volumes are created, assign a once-a-day deduplication schedule to `esxi_boot` and `infra_datastore_1`:

```
efficiency modify -vserver Infra-SVM -volume esxi_boot -schedule sun-sat@0
efficiency modify -vserver Infra-SVM -volume infra_datastore_1 -schedule sun-sat@0
```

Create FCP LIFs

Run the following commands to create four FCP LIFs (two on each node) per attached fabric interconnect:

```
network interface create -vserver Infra-SVM -lif fcp_lif01a -role data -data-protocol fcp -home-node <st-node01> -home-port 0e -status-admin up

network interface create -vserver Infra-SVM -lif fcp_lif01b -role data -data-protocol fcp -home-node <st-node01> -home-port 0f -status-admin up

network interface create -vserver Infra-SVM -lif fcp_lif02a -role data -data-protocol fcp -home-node <st-node02> -home-port 0e -status-admin up

network interface create -vserver Infra-SVM -lif fcp_lif02b -role data -data-protocol fcp -home-node <st-node02> -home-port 0f -status-admin up

network interface show
```

Create NFS LIF

To create an NFS LIF, run the following commands:

```
network interface create -vserver Infra-SVM -lif nfs_infra_swap -role data -data-protocol nfs -home-node <st-node01> -home-port a0a-<infra-nfs-vlan-id> -address <node01-nfs_infra_swap-ip> -netmask <node01-nfs_infra_swap-mask> -status-admin up -failover-policy broadcast-domain-wide -firewall-policy data -auto-revert true

network interface create -vserver Infra-SVM -lif nfs_infra_datastore_1 -role data -data-protocol nfs -home-node <st-node02> -home-port a0a-<infra-nfs-vlan-id> -address <node02-nfs_infra_datastore_1-ip> -netmask <node02-nfs_infra_datastore_1-mask> -status-admin up -failover-policy broadcast-domain-wide -firewall-policy data -auto-revert true

network interface show
```



NetApp recommends creating a new LIF for each datastore.

Add Infrastructure SVM Administrator

To add the infrastructure SVM administrator and SVM administration LIF in the out-of-band management network, complete the following steps:

1. Run the following commands:

```
network interface create -vserver Infra-SVM -lif svm-mgmt -role data -data-protocol none -home-node <st-  
node02> -home-port e0i -address <svm-mgmt-ip> -netmask <svm-mgmt-mask> -status-admin up -failover-policy  
broadcast-domain-wide -firewall-policy mgmt -auto-revert true
```



The SVM management IP in this step should be in the same subnet as the storage cluster management IP.

2. Create a default route to allow the SVM management interface to reach the outside world.

```
network route create -vserver Infra-SVM -destination 0.0.0.0/0 -gateway <svm-mgmt-gateway>  
  
network route show
```

3. Set a password for the SVM vsadmin user and unlock the user.

```
security login password -username vsadmin -vserver Infra-SVM  
Enter a new password: <password>  
Enter it again: <password>  
  
security login unlock -username vsadmin -vserver Infra-SVM
```



A cluster serves data through at least one and possibly multiple SVMs. We have just gone through creating a single SVM. If you would like to configure your environment with multiple SVMs, this is a good time to create additional SVMs.

Server Configuration

Cisco UCS Base Configuration

This FlexPod deployment will show configuration steps for both the Cisco UCS 6332-16UP and Cisco UCS 6248UP Fabric Interconnects (FI) in a design that will support Fibre Channel connectivity to the NetApp AFF through the Cisco MDS.

Configuration steps will be referenced for both fabric interconnects and will be called out by the specific model where steps have differed.

This section contains the Cisco UCS deployment for when the Cisco MDS is used as the fiber channel SAN switches. For the alternate Cisco UCS deployment with storage FC ports directly connected to the Cisco UCS fabric interconnects, please see the Appendix.

Perform Initial Setup of Cisco UCS 6332-16UP and 6248UP Fabric Interconnects for FlexPod Environments

This section provides detailed procedures for configuring the Cisco Unified Computing System (Cisco UCS) for use in a FlexPod environment. The steps are necessary to provision the Cisco UCS B-Series and C-Series servers and should be followed precisely to avoid improper configuration.

Cisco UCS Fabric Interconnect A

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

1. Connect to the console port on the first Cisco UCS fabric interconnect.

```
Enter the configuration method: gui
```

```
Physical switch Mgmt0 IP address: <ucsa-mgmt-ip>
```

```
Physical switch Mgmt0 IPv4 netmask: <ucsa-mgmt-mask>
```

```
IPv4 address of the default gateway: <ucsa-mgmt-gateway>
```

4. Using a supported web browser, connect to <https://<ucsa-mgmt-ip>>, accept the security prompts, and click the **'Express Setup'** link under HTML.
5. Select Initial Setup and click Submit.
6. Select Enable clustering, Fabric A, and IPv4.
7. Fill in the Virtual IP Address with the UCS cluster IP.
8. Completely fill in the System setup section. For system name, use the overall UCS system name. For the Mgmt IP Address, use <ucsa-mgmt-ip>.

Enable clustering
 Standalone mode
 Synchronize

Fabric Setup: Fabric A Fabric B

IPv4
 IPv6

Virtual IP Address: . . .

System setup

Enforce strong password?: Yes No

System name:

Admin Password: **Confirm Admin password:**

Mgmt IP Address: . . . **Mgmt IP Netmask:** . . .

Default Gateway: . . .

DNS Server IP: . . . **Domain Name :**

UCS Central managed environment

UCS Central IP: . . . **Shared Secret:**

9. Click Submit.

Cisco UCS Fabric Interconnect B

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

1. Connect to the console port on the second Cisco UCS fabric interconnect.

Enter the configuration method: `gui`

Physical switch Mgmt0 IP address: `<ucsb-mgmt-ip>`

Physical switch Mgmt0 IPv4 netmask: `<ucsb-mgmt-mask>`

IPv4 address of the default gateway: `<ucsb-mgmt-gateway>`

2. Using a supported web browser, connect to <https://<ucsb-mgmt-ip>>, accept the security prompts, and click the **'Express Setup'** link under HTML.
3. Under System setup, enter the Admin Password entered above and click Submit.
4. Enter <ucsb-mgmt-ip> for the Mgmt IP Address and click Submit.

Cisco UCS Setup

Log in to Cisco UCS Manager



The steps are the same between the UCS 6332-16UP and the UCS 6248UP Fabric Interconnects unless otherwise noted

To log in to the Cisco Unified Computing System (UCS) environment, complete the following steps:

1. Open a web browser and navigate to the Cisco UCS fabric interconnect cluster address.



You may need to wait at least 5 minutes after configuring the second fabric interconnect for UCS Manager to come up.

2. Click the Launch UCS Manager link under HTML to launch Cisco UCS Manager.
3. If prompted to accept security certificates, accept as necessary.
4. When prompted, enter admin as the user name and enter the administrative password.
5. Click Login to log in to Cisco UCS Manager.

Upgrade Cisco UCS Manager Software to Version 3.1(2b)

This document assumes the use of Cisco UCS 3.1(2b). To upgrade the Cisco UCS Manager software and the Cisco UCS Fabric Interconnect software to version 3.1(2b), refer to [Cisco UCS Manager Install and Upgrade Guides](#).

Anonymous Reporting

To create anonymous reporting, complete the following step:

1. In the Anonymous Reporting window, select whether to send anonymous data to Cisco for improving future products. If you select Yes, enter the IP address of your SMTP Server. Click OK.



Anonymous reporting can also be configured later by selecting Admin > Communication Management > Call Home and selecting the Anonymous Reporting tab.

Anonymous Reporting

Cisco Systems, Inc. will be collecting feature configuration and usage statistics which will be sent to Cisco Smart Call Home server anonymously. This data helps us prioritize the features and improvements that will most benefit our customers.

If you decide to enable this feature in future, you can do so from the "Anonymous Reporting" in the Call Home settings under the Admin tab.

[View Sample Data](#)

Do you authorize the disclosure of this information to Cisco Smart CallHome?

Yes No

Don't show this message again.

OK

Cancel

Configure Cisco UCS Call Home

It is highly recommended by Cisco to configure Call Home in UCSM. Configuring Call Home will accelerate resolution of support cases. To configure Call Home, complete the following steps:

1. In Cisco UCS Manager, click Admin on the left.
2. Select All > Communication Management > Call Home.
3. Change the State to On.
4. Fill in all the fields according to your Management preferences and click Save Changes and OK to complete configuring Call Home.

Configure Unified Ports


Fiber Channel port configurations differ slightly between the 6332-16UP and the 6248UP Fabric Interconnects. Both Fabric Interconnects have a slider mechanism within the UCSM GUI interface, but the fiber channel port selection options for the 6332-16UP are from the first 16 ports starting from the first port on the left, and configured in increments of the first 6, 12, or all 16 of the unified ports. With the 6248UP, the port selection options will start from the right of the 32 fixed ports, or the right of the 16 ports of the expansion module, going down in contiguous increments of 2.

To enable the fiber channel ports, complete the following steps for the 6332-16UP:

1. In Cisco UCS Manager, click Equipment on the left.
2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary).

3. Select Configure Unified Ports.
4. Click Yes on the pop-up window warning that changes to the fixed module will require a reboot of the fabric interconnect and changes to the expansion module will require a reboot of that module.
5. Within the Configured Fixed Ports pop-up window move the gray slider bar from the left to the right to select either 6, 12, or 16 ports to be set as FC Uplinks.

Configure Unified Ports ? X



Instructions

The position of the slider determines the type of the ports.
All the ports to the left of the slider are Fibre Channel ports (Purple), while the ports to the right are Ethernet ports (Blue).

| Port | Transport | If Role or Port Channel Membership | Desired If Role |
|---------|-----------|------------------------------------|-----------------|
| Port 1 | ether | Unconfigured | FC Uplink |
| Port 2 | ether | Unconfigured | FC Uplink |
| Port 3 | ether | Unconfigured | FC Uplink |
| Port 4 | ether | Unconfigured | FC Uplink |
| Port 5 | ether | Unconfigured | FC Uplink |
| Port 6 | ether | Unconfigured | FC Uplink |
| Port 7 | ether | Unconfigured | |
| Port 8 | ether | Unconfigured | |
| Port 9 | ether | Unconfigured | |
| Port 10 | ether | Unconfigured | |
| Port 11 | ether | Unconfigured | |
| Port 12 | ether | Unconfigured | |
| Port 13 | ether | Unconfigured | |
| Port 14 | ether | Unconfigured | |
| Port 15 | ether | Unconfigured | |
| Port 16 | ether | Unconfigured | |

OK
Cancel


6. Click OK, then Yes, then OK to continue
7. Select Equipment > Fabric Interconnects > Fabric Interconnect B (primary)
8. Select Configure Unified Ports.
9. Click Yes on the pop-up window warning that changes to the fixed module will require a reboot of the fabric interconnect and changes to the expansion module will require a reboot of that module.
10. Within the Configured Fixed Ports pop-up window move the gray slider bar from the left to the right to select either 6, 12, or 16 ports to be set as FC Uplinks.
11. Click OK, then Yes, then OK to continue.
12. Wait for both Fabric Interconnects to reboot.


13. Log back into UCS Manager.

To enable the fiber channel ports, complete the following steps for the 6248UP:

1. In Cisco UCS Manager, click Equipment on the left.
2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary)
3. Select Configure Unified Ports.
4. Click Yes on the pop-up window warning that changes to the fixed module will require a reboot of the fabric interconnect and changes to the expansion module will require a reboot of that module.
5. Configure the Fixed Module Ports from the subsequent Configure Fixed Module Ports pop-up window, or click on the Configure Expansion Module Ports button to select from expansion module ports.
6. Within either option, move the gray slider bar from the right to the left selecting ports in increments of two to set as FC Uplinks.

Configure Unified Ports ? X





Instructions

The position of the slider determines the type of the ports.
 All the ports to the left of the slider are Ethernet ports (Blue), while the ports to the right are Fibre Channel ports (Purple).

| Port | Transport | If Role or Port Channel Membership | Desired If Role |
|---------|-----------|------------------------------------|-----------------|
| Port 1 | ether | Unconfigured | |
| Port 2 | ether | Unconfigured | |
| Port 3 | ether | Unconfigured | |
| Port 4 | ether | Unconfigured | |
| Port 5 | ether | Unconfigured | |
| Port 6 | ether | Unconfigured | |
| Port 7 | ether | Unconfigured | |
| Port 8 | ether | Unconfigured | |
| Port 9 | ether | Unconfigured | |
| Port 10 | ether | Unconfigured | |
| Port 11 | ether | Unconfigured | |
| Port 12 | ether | Unconfigured | |
| Port 13 | ether | Unconfigured | |
| Port 14 | ether | Unconfigured | |
| Port 15 | ether | Unconfigured | |

Configure Fixed Module Ports
Configure Expansion Module Ports
Finish
Cancel

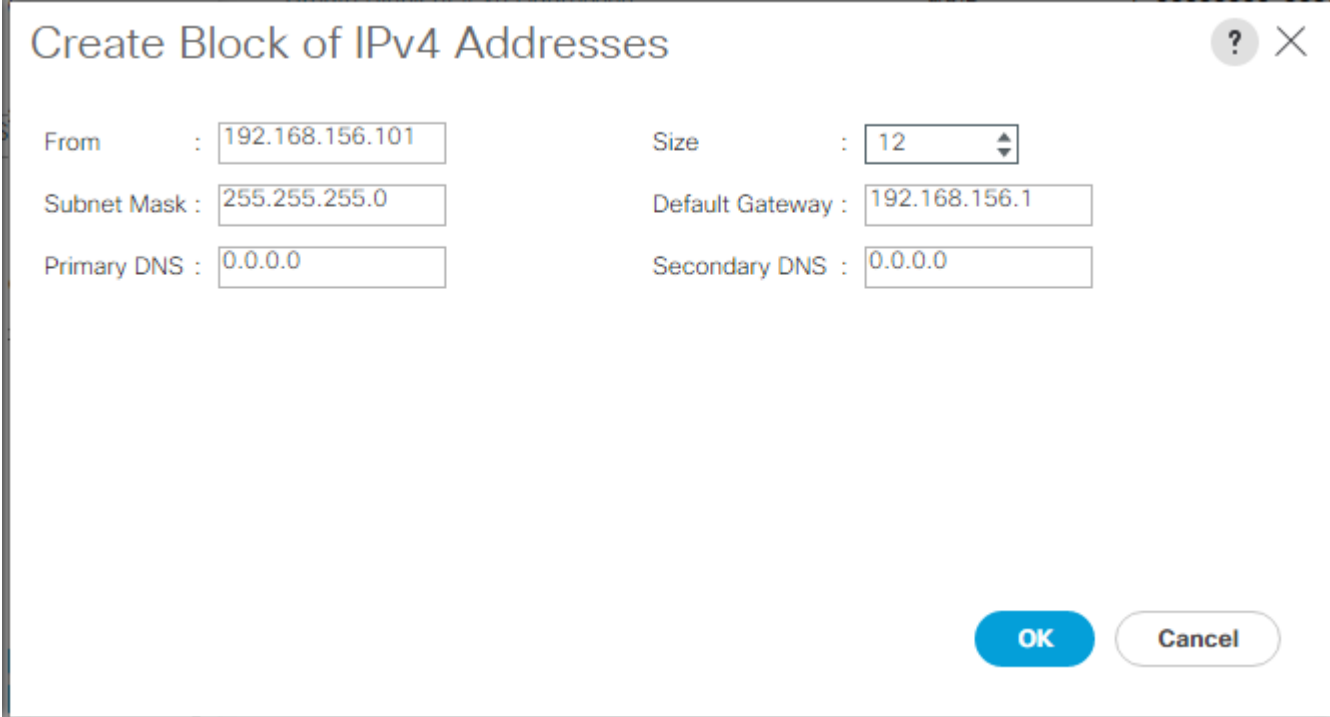
7. Click Finish. Click Yes on the confirmation. Click OK.

8. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate)
9. Select Configure Unified Ports.
10. Click Yes on the pop-up window warning that changes to the fixed module will require a reboot of the fabric interconnect and changes to the expansion module will require a reboot of that module.
11. Configure the Fixed Module Ports from the subsequent Configure Fixed Module Ports pop-up window, or click on the Configure Expansion Module Ports button to select from expansion module ports.
12. Within either option move the gray slider bar from the right to the left selecting ports in increments of two to set as FC Uplinks.
13. Click Finish. Click Yes on the confirmation. Click OK.
14. Wait for both Fabric Interconnects to reboot.
15. Log back into Cisco UCS Manager.

Add Block of IP Addresses for KVM Access

To create a block of IP addresses for in band server Keyboard, Video, Mouse (KVM) access in the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click LAN on the left.
2. Expand Pools > root > IP Pools.
3. Right-click IP Pool ext-mgmt and select Create Block of IPv4 Addresses.
4. Enter the starting IP address of the block, number of IP addresses required, and the subnet mask and gateway information.



Create Block of IPv4 Addresses ? X

From : 192.168.156.101 Size : 12

Subnet Mask : 255.255.255.0 Default Gateway : 192.168.156.1

Primary DNS : 0.0.0.0 Secondary DNS : 0.0.0.0

OK Cancel

5. Click OK to create the block.
6. Click OK in the confirmation message.

Synchronize Cisco UCS to NTP

To synchronize the Cisco UCS environment to the NTP servers in the Nexus 9372 switches, complete the following steps:

1. In Cisco UCS Manager, click Admin on the left.
2. Expand All > Time Zone Management.
3. Select Timezone.
4. In the Properties pane, select the appropriate time zone in the Timezone menu.
5. Click Save Changes, and then click OK.
6. Click Add NTP Server.
7. Enter <switch-a-ntp-ip> and click OK. Click OK on the confirmation.

Add NTP Server ? X

NTP Server :

OK Cancel

8. Click Add NTP Server.

9. Enter <switch-b-ntp-ip> and click OK. Click OK on the confirmation.

All / Time Zone Management / Timezone

General Events

Actions

Add NTP Server

Properties

Time Zone :

NTP Servers

Advanced Filter Export Print

| Name |
|-----------------------|
| NTP Server 10.1.156.4 |
| NTP Server 10.1.156.5 |

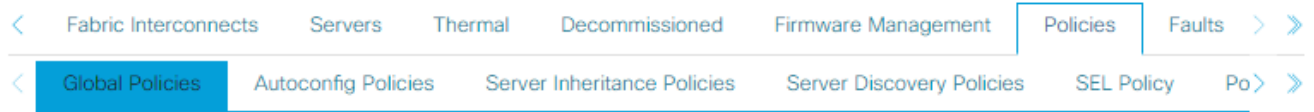
Edit Chassis Discovery Policy

Setting the discovery policy simplifies the addition of B-Series Cisco UCS chassis and of additional fabric extenders for further C-Series connectivity. To modify the chassis discovery policy, complete the following steps:

1. In Cisco UCS Manager, click Equipment on the left and select Equipment in the second list.
2. In the right pane, click the Policies tab.
3. Under Global Policies, set the Chassis/FEX Discovery Policy to match the minimum number of uplink ports that are cabled between the chassis or fabric extenders (FEXes) and the fabric interconnects.

- Set the Link Grouping Preference to Port Channel. If Backplane Speed Preference appears, leave it set at 40G. If the environment being setup contains a large amount of multicast traffic, set the Multicast Hardware Hash setting to Enabled.

Equipment



Chassis/FEX Discovery Policy

| | | |
|--------------------------|---|--|
| Action | : | 2 Link |
| Link Grouping Preference | : | <input type="radio"/> None <input checked="" type="radio"/> Port Channel |
| Multicast Hardware Hash | : | <input checked="" type="radio"/> Disabled <input type="radio"/> Enabled |

- Click Save Changes.
- Click OK.

Enable Server and Uplink Ports

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

- In Cisco UCS Manager, click Equipment on the left.
- Expand Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module.
- Expand Ethernet Ports.
- Select the ports that are connected to the chassis, Cisco FEX, and direct connect UCS C-Series servers, right-click them, and select “Configure as Server Port.”
- Click Yes to confirm server ports and click OK.
- Verify that the ports connected to the chassis, C-series servers and Cisco FEX are now configured as server ports.
- Select the ports that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.



The last 6 ports of the UCS 6332 and UCS 6332-16UP FIs will only work with optical based QSFP transceivers and AOC cables, so they can be better utilized as uplinks to upstream resources that might be optical only.

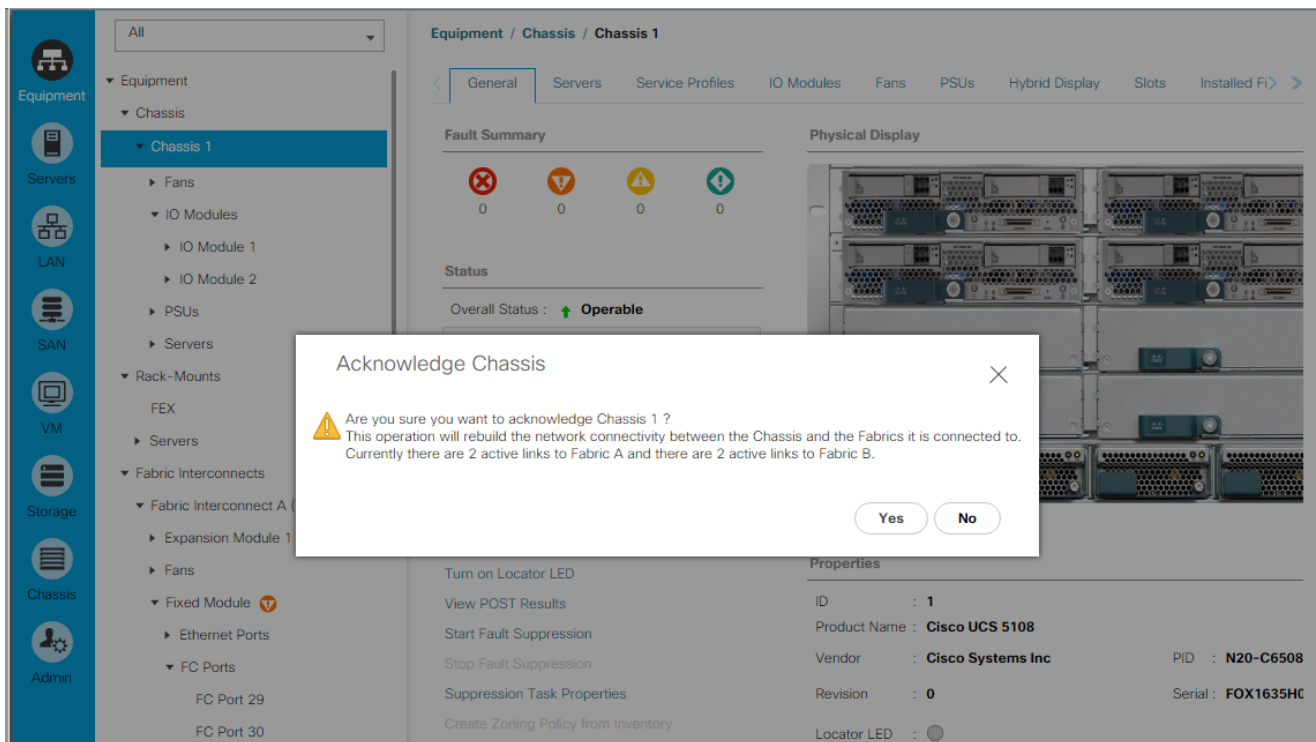
- Click Yes to confirm uplink ports and click OK.
- Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.

10. Expand Ethernet Ports.
11. Select the ports that are connected to the chassis, C-series servers or to the Cisco 2232 FEX (two per FEX), right-click them, and select Configure as Server Port.
12. Click Yes to confirm server ports and click OK.
13. Select the ports that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.
14. Click Yes to confirm the uplink ports and click OK.

Acknowledge Cisco UCS Chassis and FEX

To acknowledge all Cisco UCS chassis and any external 2232 FEX modules, complete the following steps:

1. In Cisco UCS Manager, click Equipment on the left.
2. Expand Chassis and select each chassis that is listed.
3. Right-click each chassis and select Acknowledge Chassis.



4. Click Yes and then click OK to complete acknowledging the chassis.
5. If Nexus 2232 FEX are part of the configuration, expand Rack Mounts and FEX.
6. Right-click each FEX that is listed and select Acknowledge FEX.
7. Click Yes and then click OK to complete acknowledging the FEX.

Create Uplink Port Channels to Cisco Nexus Switches

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

1. In Cisco UCS Manager, click LAN on the left.



In this procedure, two port channels are created: one from fabric A to both Cisco Nexus switches and one from fabric B to both Cisco Nexus switches.

2. Under LAN > LAN Cloud, expand the Fabric A tree.
3. Right-click Port Channels.
4. Select Create Port Channel.
5. Enter 13 as the unique ID of the port channel.
6. Enter vPC-13-Nexus as the name of the port channel.
7. Click Next.
8. Select the ports connected to the Nexus switches to be added to the port channel:
9. Click >> to add the ports to the port channel.
10. Click Finish to create the port channel.
11. Click OK.
12. In the navigation pane, under LAN > LAN Cloud, expand the fabric B tree.
13. Right-click Port Channels.
14. Select Create Port Channel.
15. Enter 14 as the unique ID of the port channel.
16. Enter vPC-14-Nexus as the name of the port channel.
17. Click Next.
18. Select the ports connected to the Nexus switches to be added to the port channel:
19. Click >> to add the ports to the port channel.
20. Click Finish to create the port channel.
21. Click OK.

Create a WWNN Pool for FC Boot

To configure the necessary WWNN pool for the Cisco UCS environment, complete the following steps on Cisco UCS Manager.


1. Select SAN on the left.
2. Select Pools > root.
3. Right-click WWNN Pools under the root organization.
4. Select Create WWNN Pool to create the WWNN pool.
5. Enter WWNN-Pool for the name of the WWNN pool.
6. Optional: Enter a description for the WWNN pool.
7. Select Sequential for Assignment Order.


The screenshot shows the 'Create WWNN Pool' wizard interface. The left sidebar has a blue vertical bar with two steps: '1 Define Name and Description' (highlighted) and '2 Add WWN Blocks'. The main content area is titled 'Create WWNN Pool' and contains the following fields and options:

- Name**: WWNN-Pool
- Description**: (empty field)
- Assignment Order**: Default Sequential

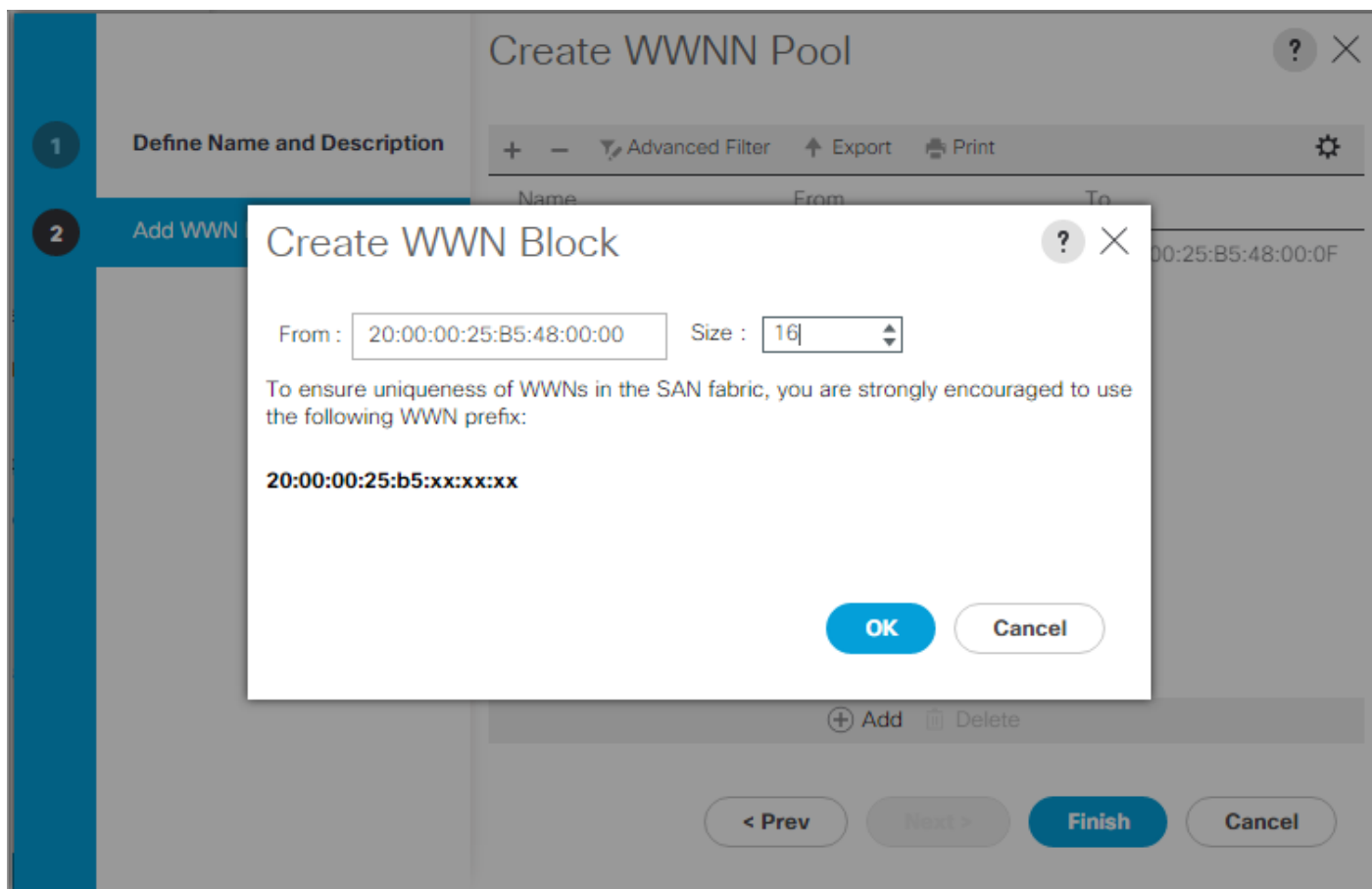
At the bottom of the wizard, there are four buttons: '< Prev' (disabled), 'Next >' (active), 'Finish' (disabled), and 'Cancel'.

8. Click Next.
9. Click Add.
10. Modify the From field as necessary for the UCS Environment.

 Modifications of the WWNN block, as well as the WWPN and MAC Addresses, can convey identifying information for the UCS domain. Within the From field in our example, the 6th octet was changed from 00 to 48 to represent as identifying information for this being in the UCS 6248 in the 4th cabinet.

 Also, when having multiple UCS domains sitting in adjacency, it is important that these blocks, the WWNN, WWPN, and MAC hold differing values between each set.

11. Specify a size of the WWNN block sufficient to support the available server resources.



12. Click OK.

13. Click Finish and OK to complete creating the WWNN pool.

Create WWPN Pools

To configure the necessary WWPN pools for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click SAN on the left.
2. Select Pools > root.

3. In this procedure, two WWPN pools are created, one for each switching fabric.
4. Right-click WWPN Pools under the root organization.
5. Select Create WWPN Pool to create the WWPN pool.
6. Enter WWPN-Pool-A as the name of the WWPN pool.
7. Optional: Enter a description for the WWPN pool.
8. Select Sequential for Assignment Order.

Create WWPN Pool

1 Define Name and Description

2 Add WWN Blocks

Name : WWPP-Pool-A

Description :

Assignment Order : Default Sequential

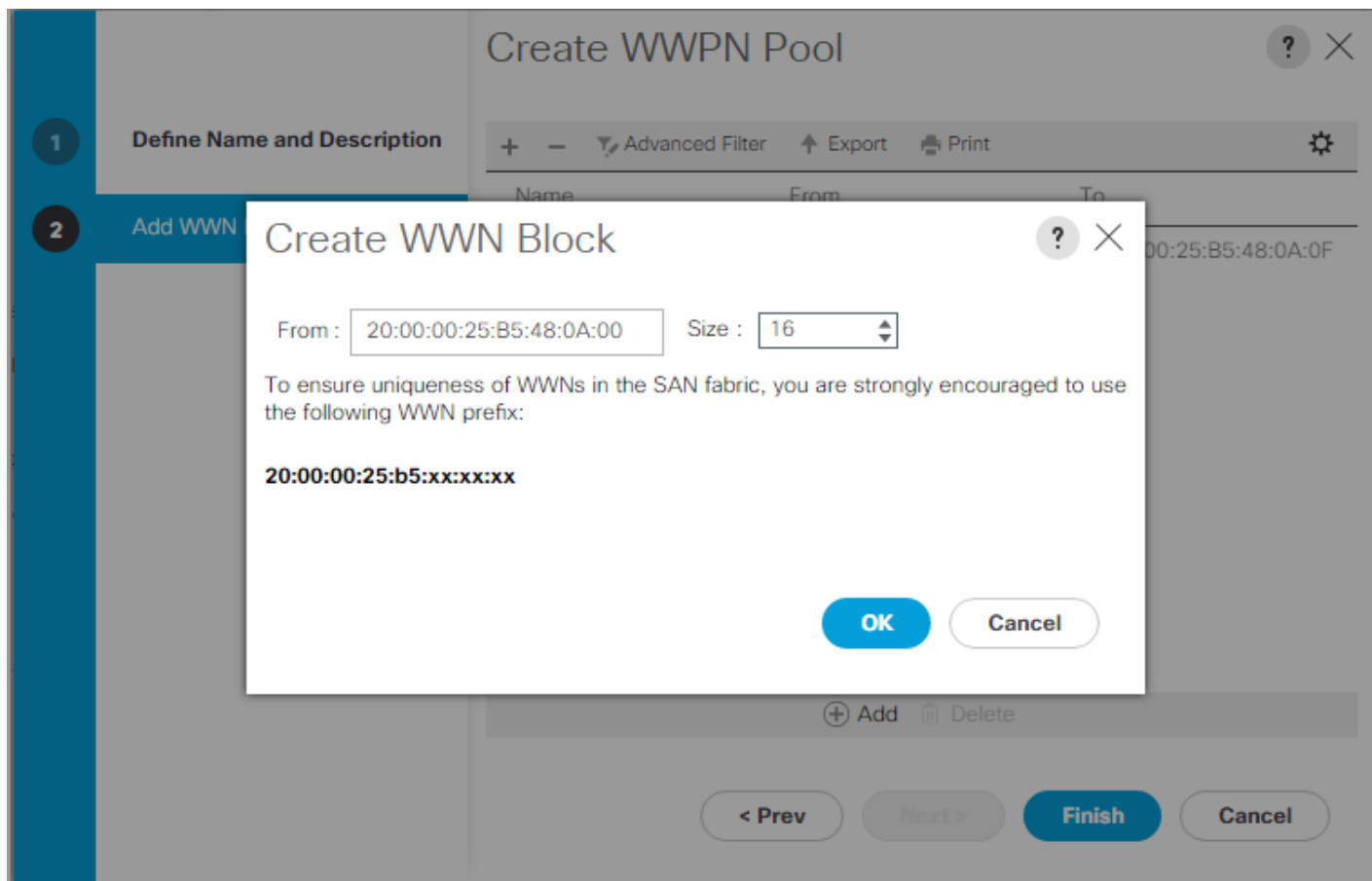
< Prev Next > Finish Cancel

9. Click Next.
10. Click Add.
11. Specify a starting WWPN.



For the FlexPod solution, the recommendation is to place 0A in the next-to-last octet of the starting WWPN to identify all of the WWPNs as fabric A addresses. Merging this with the pattern we used for the WWNN we see a WWPN block starting with 20:00:00:25:B5:48:0A:00.

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



13. Click OK.
14. Click Finish.
15. In the confirmation message, click OK.
16. Right-click WWPN Pools under the root organization.
17. Select Create WWPN Pool to create the WWPN pool.
18. Enter `WWPN-Pool-B` as the name of the WWPN pool.
19. Optional: Enter a description for the WWPN pool.
20. Select Sequential for Assignment Order.
21. Click Next.
22. Click Add.
23. Specify a starting WWPN.



For the FlexPod solution, the recommendation is to place 0B in the next-to-last octet of the starting WWPN to identify all of the WWPNs as fabric A addresses. Merging this with the pattern we used for the WWNN we see a WWPN block starting with `20:00:00:25:B5:48:0B:00`.

24. Specify a size for the WWPN address pool that is sufficient to support the available blade or server resources.
25. Click OK.
26. Click Finish.
27. In the confirmation message, click OK.

Create VSANs

To configure the necessary virtual storage area networks (VSANs) for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the SAN on the left.



In this procedure, two VSANs are created.

2. Select SAN > SAN Cloud.
3. Right-click VSANs.
4. Select Create VSAN.
5. Enter `VSAN-A` as the name of the VSAN to be used for Fabric A
6. Leave FC Zoning set at Disabled.
7. Select Fabric A.
8. Enter a unique VSAN ID and a corresponding FCoE VLAN ID that matches the configuration in the MDS switch for Fabric A. It is recommended to use the same ID for both parameters and to use something other than 1.

Create VSAN ? X

Name :

FC Zoning Settings

FC Zoning : Disabled Enabled

Do **NOT** enable local zoning if fabric interconnect is connected to an upstream FC/FCoE switch.

Common/Global Fabric A Fabric B Both Fabrics Configured Differently

You are creating a local VSAN in fabric A that maps to a VSAN ID that exists only in fabric A.

Enter the VSAN ID that maps to this VSAN.

VSAN ID :

A VLAN can be used to carry FCoE traffic and can be mapped to this VSAN.

Enter the VLAN ID that maps to this VSAN.

FCoE VLAN :

9. Click OK and then click OK again.

10. Under SAN Cloud, right-click VSANs.

11. Select Create VSAN.

12. Enter VSAN-B as the name of the VSAN to be used for Fabric B.

13. Leave FC Zoning set at Disabled.

14. Select Fabric B.

15. Enter a unique VSAN ID and a corresponding FCoE VLAN ID that matches the configuration in the MDS switch for Fabric B. It is recommended use the same ID for both parameters and to use something other than 1.

Create VSAN ? X

Name :

FC Zoning Settings

FC Zoning : Disabled Enabled

Do **NOT** enable local zoning if fabric interconnect is connected to an upstream FC/FCoE switch.

Common/Global Fabric A Fabric B Both Fabrics Configured Differently

You are creating a local VSAN in fabric B that maps to a VSAN ID that exists only in fabric B.

Enter the VSAN ID that maps to this VSAN.

VSAN ID :

A VLAN can be used to carry FCoE traffic and can be mapped to this VSAN.

Enter the VLAN ID that maps to this VSAN.

FCoE VLAN :

16. Click OK, and then click OK again.

Create FC Uplink Port Channels

To create the FC Uplink Port Channels and assign the appropriate VSANs to them for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click SAN on the left.
2. Select SAN > SAN Cloud.
3. Expand Fabric A and select FC Port Channels.
4. Right-click FC Port Channels and select Create FC Port Channel.
5. Set a unique ID for the port channel and provide a unique name for the port channel.
6. Click Next.
7. Select the ports connected to Cisco MDS A and use >> to add them to the port channel.

Create FC Port Channel

Port Channel Admin Speed :

| Ports | | |
|-------|---------|----------------|
| Port | Slot ID | WWPN |
| 29 | 1 | 20:1D:54:7F... |
| 30 | 1 | 20:1E:54:7F... |

>>
<<

| Ports in the port channel | | |
|---------------------------|---------|----------------|
| Port | Slot ID | WWPN |
| 31 | 1 | 20:1F:54:7F... |
| 32 | 1 | 20:20:54:7F... |

Slot ID:
WWPN:

8. Click Finish to complete creating the port channel.
9. Click OK the confirmation.
10. Under FC Port-Channels, select the newly created port channel.
11. In the right pane, use the pulldown to select VSAN-A.

SAN / SAN Cloud / Fabric A / FC Port Channels / FC Port-Chann...

| General | Ports | Faults | Events | Statistics |
|--|-------|---|--------|------------|
| Status Overall Status : ▼ Failed Additional Info : No operational members | | Properties ID : 101 Fabric ID : A Port Type : Aggregation Transport Type : Fc | | |
| Actions Enable Port Channel Disable Port Channel Add Ports | | Name : <input type="text" value="SPO-101"/> Description : <input type="text"/> VSAN : <input type="text" value="Fabric A/vsan VSAN-A"/> ▼ Port Channel Admin Speed : <input type="text" value="Auto"/> ▼ Operational Speed(Gbps) : 0 | | |

12. Click Save Changes to assign the VSAN.
13. Click OK.
14. Expand Fabric B and select FC Port Channels.
15. Right-click FC Port Channels and select Create FC Port Channel.
16. Set a unique ID for the port channel and provide a unique name for the port channel.
17. Click Next.
18. Select the ports connected to Cisco MDS B and use >> to add them to the port channel.
19. Click Finish to complete creating the port channel.
20. Click OK on the confirmation.
21. Under FC Port-Channels, select the newly created port channel.
22. In the right pane, use the pulldown to select VSAN-B.
23. Click Save Changes to assign the VSAN.
24. Click OK.

Create vHBA Templates

To create the necessary virtual host bus adapter (vHBA) templates for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click SAN on the left.
2. Select Policies > root.
3. Right-click vHBA Templates.
4. Select Create vHBA Template.
5. Enter `vHBA-Template-A` as the vHBA template name.
6. Keep Fabric A selected.
7. Leave Redundancy Type set to No Redundancy.
8. Select VSAN-A.
9. Leave Initial Template as the Template Type.
10. Select `WWPN-Pool-A` as the WWPN Pool.
11. Click OK to create the vHBA template.
12. Click OK.

Create vHBA Template ? X

Name : vHBA-Template-A

Description :

Fabric ID : A B

Redundancy

Redundancy Type : No Redundancy Primary Template Secondary Template

Select VSAN : VSAN-A Create VSAN

Template Type : Initial Template Updating Template

Max Data Field Size : 2048

WWPN Pool : WWPN-Pool-A(16/16) ▼

QoS Policy : <not set> ▼

Pin Group : <not set> ▼

Stats Threshold Policy : default ▼

13. Right-click vHBA Templates.
14. Select Create vHBA Template.
15. Enter vHBA-Template-B as the vHBA template name.
16. Leave Redundancy Type set to No Redundancy.
17. Select Fabric B as the Fabric ID.
18. Select VSAN-B.
19. Leave Initial Template as the Template Type.
20. Select WWPN-Pool-B as the WWPN Pool.

21. Click OK to create the vHBA template.
22. Click OK.

Create SAN Connectivity Policy

To configure the necessary Infrastructure SAN Connectivity Policy, complete the following steps:

1. In Cisco UCS Manager, click SAN on the left.
2. Select SAN > Policies > root.
3. Right-click SAN Connectivity Policies.
4. Select Create SAN Connectivity Policy.
5. Enter FC-Boot as the name of the policy.
6. Select the previously created WWNN-Pool for the WWNN Assignment.
7. Click the Add button at the bottom to add a vHBA.
8. In the Create vHBA dialog box, enter Fabric-A as the name of the vHBA.
9. Select the Use vHBA Template checkbox.
10. In the vHBA Template list, select vHBA-Template-A.
11. In the Adapter Policy list, select VMWare.

Create vHBA ? X

Name :

Use vHBA Template :

Redundancy Pair : Peer Name :

vHBA Template : Create vHBA Template

Adapter Performance Profile

Adapter Policy : Create Fibre Channel Adapter Policy

12. Click OK.

13. Click the Add button at the bottom to add a second vHBA.

14. In the Create vHBA dialog box, enter Fabric-B as the name of the vHBA.

15. Select the Use vHBA Template checkbox.

16. In the vHBA Template list, select vHBA-Template-B.

17. In the Adapter Policy list, select VMWare.

18. Click OK.

Create SAN Connectivity Policy ? X

Name :

Description :

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

World Wide Node Name

WWNN Assignment:

[Create WWNN Pool](#)

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

| Name | WWPN |
|-----------------|---------|
| ▶ vHBA Fabric-B | Derived |
| ▶ vHBA Fabric-A | Derived |

🗑 Delete ➕ Add ⓘ Modify

19. Click OK to create the SAN Connectivity Policy.

20. Click OK to confirm creation.

Create MAC Address Pools

To configure the necessary MAC address pools for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click LAN on the left.
2. Select Pools > root.



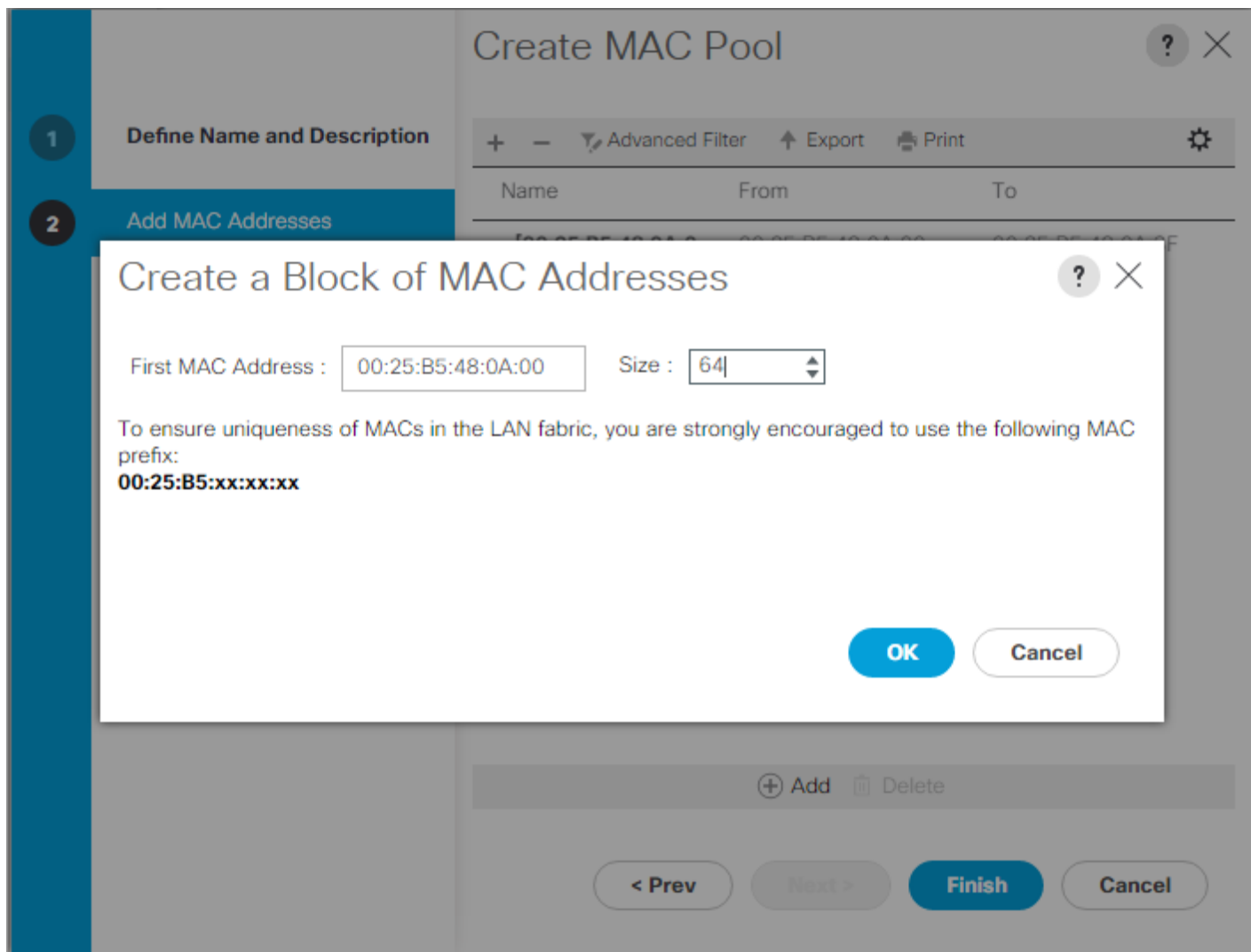
In this procedure, two MAC address pools are created, one for each switching fabric.

3. Right-click MAC Pools under the root organization.
4. Select Create MAC Pool to create the MAC address pool.
5. Enter `MAC-Pool1-A` as the name of the MAC pool.
6. Optional: Enter a description for the MAC pool.
7. Select Sequential as the option for Assignment Order.
8. Click Next.
9. Click Add.
10. Specify a starting MAC address.



For the FlexPod solution, the recommendation is to place `0A` in the next-to-last octet of the starting MAC address to identify all of the MAC addresses as fabric A addresses. In our example, we have carried forward the of also embedding the UCS domain number information giving us `00:25:B5:48:0A:00` as our first MAC address.

11. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources.



12. Click OK.
13. Click Finish.
14. In the confirmation message, click OK.
15. Right-click MAC Pools under the root organization.
16. Select Create MAC Pool to create the MAC address pool.
17. Enter MAC-Pool1-B as the name of the MAC pool.
18. Optional: Enter a description for the MAC pool.
19. Select Sequential as the option for Assignment Order.
20. Click Next.
21. Click Add.

22. Specify a starting MAC address.



For the FlexPod solution, it is recommended to place 0B in the next to last octet of the starting MAC address to identify all the MAC addresses in this pool as fabric B addresses. Once again, we have carried forward in our example of also embedding the UCS domain number information giving us 00:25:B5:48:0B:00 as our first MAC address.

23. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources.

24. Click OK.

25. Click Finish.

26. In the confirmation message, click OK.

Create UUID Suffix Pool

To configure the necessary universally unique identifier (UUID) suffix pool for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click Servers on the left.
2. Select Pools > root.
3. Right-click UUID Suffix Pools.
4. Select Create UUID Suffix Pool.
5. Enter `UUID-Pool` as the name of the UUID suffix pool.
6. Optional: Enter a description for the UUID suffix pool.
7. Keep the prefix at the derived option.
8. Select Sequential for the Assignment Order.
9. Click Next.
10. Click Add to add a block of UUIDs.
11. Keep the From field at the default setting.
12. Specify a size for the UUID block that is sufficient to support the available blade or server resources.
13. Click OK.
14. Click Finish.
15. Click OK.

Create Server Pool

To configure the necessary server pool for the Cisco UCS environment, complete the following steps:



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

1. In Cisco UCS Manager, click Servers on the left.
2. Select Pools > root.
3. Right-click Server Pools.
4. Select Create Server Pool.
5. Enter `Infra-Pool1` as the name of the server pool.
6. Optional: Enter a description for the server pool.
7. Click Next.
8. Select two (or more) servers to be used for the VMware management cluster and click >> to add them to the `Infra-Pool1` server pool.
9. Click Finish.
10. Click OK.

Create VLANs

To configure the necessary virtual local area networks (VLANs) for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click LAN on the left.



In this procedure, five unique VLANs are created. See Table 2

2. Select LAN > LAN Cloud.
3. Right-click VLANs.
4. Select Create VLANs.
5. Enter `Native-VLAN` as the name of the VLAN to be used as the native VLAN.
6. Keep the Common/Global option selected for the scope of the VLAN.
7. Enter the native VLAN ID.
8. Keep the Sharing Type as None.

- Click OK, and then click OK again.

Create VLANs ? X

VLAN Name/Prefix :

Multicast Policy Name : [Create Multicast Policy](#)

Common/Global
 Fabric A
 Fabric B
 Both Fabrics Configured Differently

You are creating global VLANs that map to the same VLAN IDs in all available fabrics.
Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")

VLAN IDs :

Sharing Type : None Primary Isolated Community

- Expand the list of VLANs in the navigation pane, right-click the newly created `Native-VLAN` and select Set as Native VLAN.
- Click Yes, and then click OK.
- Right-click VLANs.
- Select Create VLANs
- Enter `IB-MGMT` as the name of the VLAN to be used for management traffic.
- Keep the Common/Global option selected for the scope of the VLAN.
- Enter the In-Band management VLAN ID.
- Keep the Sharing Type as None.
- Click OK, and then click OK again.
- Right-click VLANs.

20. Select Create VLANs.
21. Enter `Infra-NFS` as the name of the VLAN to be used for NFS.
22. Keep the Common/Global option selected for the scope of the VLAN.
23. Enter the Infrastructure NFS VLAN ID.
24. Keep the Sharing Type as None.
25. Click OK, and then click OK again.
26. Right-click VLANs.
27. Select Create VLANs.
28. Enter `vMotion` as the name of the VLAN to be used for vMotion.
29. Keep the Common/Global option selected for the scope of the VLAN.
30. Enter the vMotion VLAN ID.
31. Keep the Sharing Type as None.
32. Click OK, and then click OK again.
33. Right-click VLANs.
34. Select Create VLANs.
35. Enter `VM-Traffic` as the name of the VLAN to be used for VM Traffic.
36. Keep the Common/Global option selected for the scope of the VLAN.
37. Enter the VM-Traffic VLAN ID.
38. Keep the Sharing Type as None.
39. Click OK, and then click OK again.

VLANs

Advanced Filter Export Print

| Name | ID | Type | Transport | Native | VLAN Shar... |
|-----------------------|------|------|-----------|--------|--------------|
| VLAN default (1) | 1 | Lan | Ether | No | None |
| VLAN Native-VLAN (2) | 2 | Lan | Ether | Yes | None |
| VLAN IB-MGMT (113) | 113 | Lan | Ether | No | None |
| VLAN VM-Traffic (900) | 900 | Lan | Ether | No | None |
| VLAN vMotion (3000) | 3000 | Lan | Ether | No | None |
| VLAN Infra-NFS (3050) | 3050 | Lan | Ether | No | None |

+ Add Delete Info

Details

General Org Permissions VLAN Group Membership Faults Events

Fault Summary **Properties**

Modify Default Host Firmware Package

Firmware management policies allow the administrator to select the corresponding packages for a given server configuration. These policies often include packages for adapter, BIOS, board controller, FC adapters, host bus adapter (HBA) option ROM, and storage controller properties.

To create a firmware management policy for a given server configuration in the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click Servers on the left.
2. Select Policies > root.
3. Expand Host Firmware Packages.
4. Select default.
5. In the Actions pane, select Modify Package Versions.
6. Select the version 3.1(2b) for both the Blade and Rack Packages.

Modify Package Versions ✕

Blade Package :

Rack Package :

Excluded Components:

Adapter
 Host NIC Option ROM
 CIMC
 Board Controller
 Flex Flash Controller
 BIOS
 PSU
 SAS Expander
 Storage Controller Onboard Device
 Storage Device Bridge
 GPUs
 FC Adapters
 Local Disk
 HBA Option ROM

7. Click OK then OK again to modify the host firmware package.

Set Jumbo Frames in Cisco UCS Fabric

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

1. In Cisco UCS Manager, click LAN on the left.
2. Select LAN > LAN Cloud > QoS System Class.
3. In the right pane, click the General tab.

4. On the Best Effort row, enter 9216 in the box under the MTU column.
5. Click Save Changes in the bottom of the window.
6. Click OK

LAN / LAN Cloud / QoS System Class

| Priority | Enabled | CoS | Packet Drop | Weight | Weight (%) | MTU | Multicast Optimized |
|---------------|-------------------------------------|-----|-------------------------------------|--------|------------|--------|--------------------------|
| Platinum | <input type="checkbox"/> | 5 | <input type="checkbox"/> | 10 | N/A | normal | <input type="checkbox"/> |
| Gold | <input type="checkbox"/> | 4 | <input checked="" type="checkbox"/> | 9 | N/A | normal | <input type="checkbox"/> |
| Silver | <input type="checkbox"/> | 2 | <input checked="" type="checkbox"/> | 8 | N/A | normal | <input type="checkbox"/> |
| Bronze | <input type="checkbox"/> | 1 | <input checked="" type="checkbox"/> | 7 | N/A | normal | <input type="checkbox"/> |
| Best Effort | <input checked="" type="checkbox"/> | Any | <input checked="" type="checkbox"/> | 5 | 50 | 9216 | <input type="checkbox"/> |
| Fibre Channel | <input checked="" type="checkbox"/> | 3 | <input type="checkbox"/> | 5 | 50 | fc | N/A |

Create Local Disk Configuration Policy (Optional)

A local disk configuration for the Cisco UCS environment is necessary if the servers in the environment do not have a local disk.



This policy should not be used on servers that contain local disks.

To create a local disk configuration policy, complete the following steps:

1. In Cisco UCS Manager, click Servers on the left.
2. Select Policies > root.
3. Right-click Local Disk Config Policies.
4. Select Create Local Disk Configuration Policy.
5. Enter SAN-Boot as the local disk configuration policy name.
6. Change the mode to No Local Storage.
7. Click OK to create the local disk configuration policy.

Create Local Disk Configuration Policy ? X

Name : SAN-Boot

Description :

Mode : No Local Storage ▼

FlexFlash

FlexFlash State : Disable Enable

If **FlexFlash State** is disabled, SD cards will become unavailable immediately.
Please ensure SD cards are not in use before disabling the FlexFlash State.

FlexFlash RAID Reporting State : Disable Enable

8. Click OK.

Create Network Control Policy for Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP)

To create a network control policy that enables CDP and LLDP on virtual network ports, complete the following steps:

1. In Cisco UCS Manager, click LAN on the left.
2. Select Policies > root.
3. Right-click Network Control Policies.
4. Select Create Network Control Policy.
5. Enter `Enable-CDP-LLDP` as the policy name.
6. For CDP, select the Enabled option.
7. For LLDP, scroll down and select Enabled for both Transmit and Receive.
8. Click OK to create the network control policy.

Create Network Control Policy ? ×

CDP : Disabled Enabled

MAC Register Mode : Only Native Vlan All Host Vlans

Action on Uplink Fail : Link Down Warning

MAC Security

Forge : Allow Deny

LLDP

Transmit : Disabled Enabled

Receive : Disabled Enabled

OK **Cancel**

9. Click OK.

Create Power Control Policy

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

1. In Cisco UCS Manager, click Servers tab on the left.
2. Select Policies > root.

3. Right-click Power Control Policies.
4. Select Create Power Control Policy.
5. Enter `No-Power-Cap` as the power control policy name.
6. Change the power capping setting to No Cap.
7. Click OK to create the power control policy.
8. Click OK.

Create Power Control Policy ? ×

Name :

Description :

Fan Speed Policy :

Power Capping

If you choose **cap**, the server is allocated a certain amount of power based on its priority within its power group. Priority values range from 1 to 10, with 1 being the highest priority. If you choose **no-cap**, the server is exempt from all power capping.

No Cap cap

Cisco UCS Manager only enforces power capping when the servers in a power group require more power than is currently available. With sufficient power, all servers run at full capacity regardless of their priority.

Create Server Pool Qualification Policy (Optional)

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



This example creates a policy for Cisco UCS B-Series and Cisco UCS C-Series servers with the Intel E2660 v4 Xeon Broadwell processors.

1. In Cisco UCS Manager, click Servers on the left.
2. Select Policies > root.
3. Right-click Server Pool Policy Qualifications.
4. Select Create Server Pool Policy Qualification.
5. Name the policy UCS-Broadwell.
6. Select Create CPU/Cores Qualifications.
7. Select Xeon for the Processor/Architecture.
8. Select UCS-CPU-E52660E as the PID.
9. Click OK to create the CPU/Core qualification.
10. Click OK to create the policy then OK for the confirmation.

Create CPU/Cores Qualifications ? ×

| | | | |
|--------------------------|---|-------------------------|---|
| Processor Architecture : | <input type="text" value="Xeon"/> | PID (RegEx) : | <input type="text" value="UCS-CPU-E52660E"/> |
| Min Number of Cores : | <input checked="" type="radio"/> Unspecified <input type="radio"/> select | Max Number of Cores : | <input checked="" type="radio"/> Unspecified <input type="radio"/> select |
| Min Number of Threads : | <input checked="" type="radio"/> Unspecified <input type="radio"/> select | Max Number of Threads : | <input checked="" type="radio"/> Unspecified <input type="radio"/> select |
| CPU Speed (MHz) : | <input checked="" type="radio"/> Unspecified <input type="radio"/> select | CPU Stepping : | <input checked="" type="radio"/> Unspecified <input type="radio"/> select |

Create Server BIOS Policy

To create a server BIOS policy for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click Servers on the left.
2. Select Policies > root.
3. Right-click BIOS Policies.
4. Select Create BIOS Policy.
5. Enter VM-Host as the BIOS policy name.
6. Change the Quiet Boot setting to disabled.
7. Change Consistent Device Naming to enabled.
8. Click Finish to create the BIOS policy.

Create BIOS Policy ? ×

1 Main

2 Processor

3 Intel Directed IO

4 RAS Memory

5 Serial Port

6 USB

7 PCI

8 QPI

9 LOM and PCIe Slots

10 Trusted Platform

11 Graphics Configuration

12 Boot Options

13 Server Management

Name : VM-Host

Description :

Reboot on BIOS Settings Change :

Quiet Boot : disabled enabled Platform Default

Post Error Pause : disabled enabled Platform Default

Resume Ac On Power Loss : stay-off last-state reset Platform Default

Front Panel Lockout : disabled enabled Platform Default

Consistent Device Naming : disabled enabled Platform Default

< Prev Next > Finish Cancel

9. Click OK.

Update the Default Maintenance Policy

To update the default Maintenance Policy, complete the following steps:

1. In Cisco UCS Manager, click Servers on the left.
2. Select Policies > root.
3. Select Maintenance Policies > default.
4. Change the Reboot Policy to User Ack.
5. Click **“On Next Boot”** to delegate maintenance windows to server administrators.

Servers / Policies / root / Maintenance Poli... / default

| General | Events |
|--|---|
| <p>Actions</p> <p>Delete</p> <p>Show Policy Usage</p> <p>Use Global</p> | <p>Properties</p> <p>Name : default</p> <p>Description : <input type="text"/></p> <p>Owner : Local</p> <p>Soft Shutdown Timer : <input type="text" value="150 Secs"/></p> <p>Reboot Policy : <input type="radio"/> Immediate <input checked="" type="radio"/> User Ack <input type="radio"/> Timer Automatic</p> <p><input checked="" type="checkbox"/> On Next Boot (Apply pending changes at next reboot.)</p> |

6. Click Save Changes.
7. Click OK to accept the change.

Create vNIC Templates

To create multiple virtual network interface card (vNIC) templates for the Cisco UCS environment, complete the following steps. A total of 6 vNIC Templates will be created.

Create Infrastructure vNICs

1. In Cisco UCS Manager, click LAN on the left.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter Infra-A as the vNIC template name.

6. Keep Fabric A selected.
7. Do not select the Enable Failover checkbox.
8. Set Redundancy Type set at to Primary Template. Leave Peer Redundancy Template set to <not set>.
9. Under Target, make sure that only the Adapter checkbox is selected.
10. Select Updating Template as the Template Type.
11. Under VLANs, select the checkboxes for IB-MGMT, Infra-NFS, and Native-VLAN VLANs.
12. Set Native-VLAN as the native VLAN.
13. Select vNIC Name for the CDN Source.
14. For MTU, enter 9000.
15. In the MAC Pool list, select MAC-Pool-A.
16. In the Network Control Policy list, select Enable-CDP-LLDP.

Create vNIC Template ? X

Template Type : Initial Template Updating Template

VLANs

Advanced Filter Export Print ⚙️

| Select | Name | Native VLAN |
|-------------------------------------|-------------|----------------------------------|
| <input type="checkbox"/> | default | <input type="radio"/> |
| <input checked="" type="checkbox"/> | IB-MGMT | <input type="radio"/> |
| <input checked="" type="checkbox"/> | Infra-NFS | <input type="radio"/> |
| <input checked="" type="checkbox"/> | Native-VLAN | <input checked="" type="radio"/> |
| <input type="checkbox"/> | VM-Traffic | <input type="radio"/> |
| <input type="checkbox"/> | vMotion | <input type="radio"/> |

CDN Source : vNIC Name User Defined

MTU :

MAC Pool :

QoS Policy :

Network Control Policy :

Pin Group :

Stats Threshold Policy :

Connection Policies

Dynamic vNIC usNIC VMQ

Dynamic vNIC Connection Policy :

17. Click OK to create the vNIC template.

18. Click OK.

Repeat these equivalent steps for template Infra-B:

1. Select LAN on the left.
2. Select Policies > root.
3. Right-click vNIC Templates.

4. Select Create vNIC Template
5. Enter Infra-B as the vNIC template name.
6. Select Fabric B.
7. Do not select the Enable Failover checkbox.
8. Set Redundancy Type Secondary Template. Select Infra-A as the Peer Redundancy Template.
9. Under Target, make sure that only the Adapter checkbox is selected.
10. Since Peer Redundancy Templates are being used, it is not necessary to select the template type.
11. It is not necessary to select VLANs.
12. Select vNIC Name for the CDN Source.
13. It is not necessary to set the MTU.
14. In the MAC Pool list, select MAC-Pool-B.
15. It is not necessary to select the Network Control Policy.
16. Click OK to create the vNIC template.
17. Click OK.

Create vMotion vNICs

1. In Cisco UCS Manager, click LAN on the left.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter vMotion-A as the vNIC template name.
6. Keep Fabric A selected.
7. Do not select the Enable Failover checkbox.
8. Set Redundancy Type to Primary Template. Leave Peer Redundancy Template set to <not set>.
9. Under Target, make sure that only the Adapter checkbox is selected.
10. Select Updating Template as the Template Type.
11. Under VLANs, select the checkbox for the vMotion VLAN.

12. Select vNIC Name for the CDN Source.
13. For MTU, enter 9000.
14. In the MAC Pool list, select MAC-Pool-A.
15. In the Network Control Policy list, select Enable-CDP-LLDP.

Create vNIC Template ? X

If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type : Initial Template Updating Template

VLANs

Advanced Filter Export Print ⚙️

| Select | Name | Native VLAN |
|-------------------------------------|-------------|-------------|
| <input type="checkbox"/> | default | ○ |
| <input type="checkbox"/> | IB-MGMT | ○ |
| <input type="checkbox"/> | Infra-NFS | ○ |
| <input type="checkbox"/> | Native-VLAN | ○ |
| <input type="checkbox"/> | VM-Traffic | ○ |
| <input checked="" type="checkbox"/> | vMotion | ○ |

CDN Source : vNIC Name User Defined

MTU :

MAC Pool :

QoS Policy :

Network Control Policy :

Pin Group :

Stats Threshold Policy :

Connection Policies

Dynamic vNIC usNIC VMQ

16. Click OK to create the vNIC template.
17. Click OK.

Repeat the following equivalent steps for template vMotion-B:

1. Select LAN on the left.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template
5. Enter vMotion-B as the vNIC template name.
6. Select Fabric B.
7. Do not select the Enable Failover checkbox.
8. Set Redundancy Type to Secondary Template. Select vMotion-A for Peer Redundancy Template.
9. Under Target, make sure that only the Adapter checkbox is selected.
10. Select vNIC Name for the CDN Source.
11. In the MAC Pool list, select MAC-Pool-B.
12. Click OK to create the vNIC template.
13. Click OK.

Create Distributed Virtual Switch (DVS) vNICs

1. Select LAN on the left.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter DVS-Template-A as the vNIC template name.
6. Leave Fabric A selected. Do not select the Enable Failover checkbox.
7. Set Redundancy Type to Primary Template. Leave Peer Redundancy Template set to <not set>.
8. Under Target, make sure that only the Adapter checkbox is selected.
9. Select Updating Template for Template Type.
10. Under VLANs, select only VM-Traffic.
11. Do not set a native VLAN.

12. Select vNIC Name for the CDN Source.
13. Under MTU, enter 9000.
14. From the MAC Pool list, select MAC-Pool-A.
15. From the Network Control Policy list, select Enable-CDP-LLDP.

Create vNIC Template ? X

If **VM** is selected, a port profile by the same name will be created.
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type : Initial Template Updating Template

VLANs

Advanced Filter Export Print ⚙️

| Select | Name | Native VLAN |
|-------------------------------------|-------------|-----------------------|
| <input type="checkbox"/> | default | <input type="radio"/> |
| <input type="checkbox"/> | IB-MGMT | <input type="radio"/> |
| <input type="checkbox"/> | Infra-NFS | <input type="radio"/> |
| <input type="checkbox"/> | Native-VLAN | <input type="radio"/> |
| <input checked="" type="checkbox"/> | VM-Traffic | <input type="radio"/> |
| <input type="checkbox"/> | vMotion | <input type="radio"/> |

CDN Source : vNIC Name User Defined

MTU :

MAC Pool : ▼

QoS Policy : ▼

Network Control Policy : ▼

Pin Group : ▼

Stats Threshold Policy : ▼

Connection Policies

16. Click OK to complete creating the vNIC template.
17. Click OK.

Repeat the following equivalent steps for DVS-Template-B:

1. Select LAN on the left.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter DVS-Template-B as the vNIC template name.
6. Select Fabric B. Do not select the Enable Failover checkbox.
7. Set Redundancy Type to Secondary Template. Select DVS-Template-A for Peer Redundancy Template.
8. Under Target, make sure that only the Adapter checkbox is selected.
9. Select vNIC Name for the CDN Source.
10. From the MAC Pool list, select MAC-Pool-B.
11. From the Network Control Policy list, select Enable-CDP-LLDP.
12. Click OK to complete creating the vNIC template.
13. Click OK.

Create LAN Connectivity Policy

To configure the necessary Infrastructure LAN Connectivity Policy, complete the following steps:

1. In Cisco UCS Manager, click LAN on the left.
2. Select LAN > Policies > root.
3. Right-click LAN Connectivity Policies.
4. Select Create LAN Connectivity Policy.
5. Enter FC-Boot as the name of the policy.
6. Click the upper Add button to add a vNIC.
7. In the Create vNIC dialog box, enter 00-Infra-A as the name of the vNIC.
8. Select the Use vNIC Template checkbox.
9. In the vNIC Template list, select Infra-A.
10. In the Adapter Policy list, select VMWare.

11. Click OK to add this vNIC to the policy.

Create vNIC ? ×

Name :

Use vNIC Template :

Redundancy Pair :

Peer Name :

vNIC Template :

Create vNIC Template

Adapter Performance Profile

Adapter Policy :

Create Ethernet Adapter Policy

12. Click the upper Add button to add another vNIC to the policy.

13. In the Create vNIC box, enter 01-Infra-B as the name of the vNIC.

14. Select the Use vNIC Template checkbox.

15. In the vNIC Template list, select Infra-B.

16. In the Adapter Policy list, select VMWare.

17. Click OK to add the vNIC to the policy.

18. Click the upper Add button to add a vNIC.

19. In the Create vNIC dialog box, enter 02-vMotion-A as the name of the vNIC.
20. Select the Use vNIC Template checkbox.
21. In the vNIC Template list, select vMotion-A.
22. In the Adapter Policy list, select VMWare.
23. Click OK to add this vNIC to the policy.
24. Click the upper Add button to add a vNIC to the policy.
25. In the Create vNIC dialog box, enter 03-vMotion-B as the name of the vNIC.
26. Select the Use vNIC Template checkbox.
27. In the vNIC Template list, select vMotion-B.
28. In the Adapter Policy list, select VMWare.
29. Click OK to add this vNIC to the policy.
30. Click the upper Add button to add a vNIC.
31. In the Create vNIC dialog box, enter 04-DVS-A as the name of the vNIC.
32. Select the Use vNIC Template checkbox.
33. In the vNIC Template list, select DVS-Template-A.
34. In the Adapter Policy list, select VMWare.
35. Click OK to add this vNIC to the policy.
36. Click the upper Add button to add a vNIC to the policy.
37. In the Create vNIC dialog box, enter 05-DVS-B as the name of the vNIC.
38. Select the Use vNIC Template checkbox.
39. In the vNIC Template list, select DVS-Template-B.
40. In the Adapter Policy list, select VMWare.
41. Click OK to add this vNIC to the policy.

Create LAN Connectivity Policy ? X

Name :

Description :

Click **Add** to specify one or more vNICs that the server should use to connect to the LAN.

| Name | MAC Address | Native VLAN |
|-------------------|-------------|-------------|
| vNIC 05-DVS-B | Derived | |
| vNIC 04-DVS-A | Derived | |
| vNIC 03-vMotion-B | Derived | |
| vNIC 02-vMotion-A | Derived | |
| vNIC 01-Infra-B | Derived | |
| vNIC 00-Infra-A | Derived | |

🗑 Delete ➕ Add ⓘ Modify

➕ Add iSCSI vNICs

OK
Cancel

42. Click OK, then OK again to create the LAN Connectivity Policy.

Create vMedia Policy for VMware ESXi 6.0 U2 Install Boot

In the NetApp Data ONTAP setup steps an HTTP web server is required, which will be used for hosting NetApp Data ONTAP as well as VMware software. The vMedia Policy created here will map the VMware ESXi 6.0U2 ISO to the Cisco UCS server in order to boot the ESXi installation. To create this policy, complete the following steps:

1. In Cisco UCS Manager, select Servers on the left.
2. Select Policies > root.
3. Right-click vMedia Policies.

4. Select Create vMedia Policy.
5. Name the policy ESXi-6.0U2-HTTP.
6. Enter **“Mounts Cisco Custom ISO for ESXi 6.0U2”** in the Description field.
7. Click Add.
8. Name the mount ESXi-6.0U2-HTTP.
9. Select the CDD Device Type.
10. Select the HTTP Protocol.
11. Enter the IP Address of the web server.



Since DNS server IPs were not entered into the KVM IP earlier, it is necessary to enter the IP of the web server instead of the hostname.

12. Enter Vmware-ESXi-60U2-4192238-Cisco-Custom-6.0.2.3.iso as the Remote File name.



This VMware ESXi Cisco Custom ISO can be downloaded from [CiscoCustomImage6.0U2Patch3](#).

13. Enter the web server path to the ISO file in the Remote Path field.

Create vMedia Mount ? X

Name :

Description :

Device Type : CDD HDD

Protocol : NFS CIFS HTTP HTTPS

Hostname/IP Address :

Image Name Variable : None Service Profile Name

Remote File :

Remote Path :

Username :

Password :

14. Click OK to create the vMedia Mount.

15. Click OK then OK again to complete creating the vMedia Policy.



For any new servers added to the Cisco UCS environment the vMedia service profile template can be used to install the ESXi host. On first boot the host will boot into the ESXi installer since the SAN mounted disk is empty. After ESXi is installed, the vMedia will not be referenced as long as the boot disk is accessible.

Create Boot Policy (FC Boot)

This procedure applies to a Cisco UCS environment in which two FC logical interfaces (LIFs) are on cluster node 1 and two FC LIFs are on cluster node 2 for each Cisco UCS Fabric Interconnect:

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

1. In Cisco UCS Manager, click Servers on the left.
2. Select Policies > root.
3. Right-click Boot Policies.
4. Select Create Boot Policy.
5. Enter `Boot-FC-Fabric-A` as the name of the boot policy.
6. Optional: Enter a description for the boot policy.



Do not select the Reboot on Boot Order Change checkbox.

7. Keep the Reboot on Boot Order Change option cleared.
8. Expand the Local Devices drop-down menu and select `Add Remote CD/DVD`.
9. Expand the vHBAs drop-down menu and select `Add SAN Boot`.
10. Select the Primary Type.
11. Enter `Fabric-A` in the vHBA field.
12. Confirm that Primary is selected for the Type option.

Add SAN Boot ? X

vHBA :

Type : Primary Secondary Any

OK **Cancel**

13. Click OK to add the SAN boot initiator.

14. From the vHBA drop-down menu, select Add SAN Boot Target.
15. Keep 0 as the value for Boot Target LUN.
16. Enter the WWPN for `fc0_01a`.



To obtain this information, log in to the storage cluster and run the `network interface show` command.

17. Select Primary for the SAN boot target type.

Add SAN Boot Target ? X

Boot Target LUN : 0

Boot Target WWPN : 20:01:00:a0:98:5b:4a:86

Type : Primary Secondary

OK Cancel

16. Click OK to add the SAN boot target.
17. From the vHBA drop-down menu, select Add SAN Boot Target.
18. Enter 0 as the value for Boot Target LUN.
19. Enter the WWPN for `fc0_02a`.
20. Click OK to add the SAN boot target.
21. From the vHBA drop-down menu, select Add SAN Boot.
22. In the Add SAN Boot dialog box, enter `Fabric-B` in the vHBA box.

23. The SAN boot type should automatically be set to Secondary.
24. Click OK to add the SAN boot initiator.
25. From the vHBA drop-down menu, select Add SAN Boot Target.
26. Keep 0 as the value for Boot Target LUN.
27. Enter the WWPN for `fc01b`.
28. Select Primary for the SAN boot target type.
29. Click OK to add the SAN boot target.
30. From the vHBA drop-down menu, select Add SAN Boot Target.
31. Keep 0 as the value for Boot Target LUN.
32. Enter the WWPN for `fc02b`.
33. Click OK to add the SAN boot target.
34. Expand CIMC Mounted Media and select Add CIMC Mounted CD/DVD.

Create Boot Policy ? ✕

Name :

Description :

Reboot on Boot Order Change :

Enforce vNIC/vHBA/iSCSI Name :

Boot Mode : Legacy Uefi

WARNINGS:
 The type (primary/secondary) does not indicate a boot order presence.
 The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.
 If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.
 If it is not selected, the vNICs/vHBAs are selected if they exist, otherwise the vNIC/vHBA with the lowest PCIe bus scan order is used.

Local Devices

Add Local Disk

- Add Local LUN
- Add Local JBOD
- Add SD Card
- Add Internal USB
- Add External USB
- Add Embedded Local LUN
- Add Embedded Local Disk

Add CD/DVD

- Add Local CD/DVD
- Add Remote CD/DVD

Add Floppy

- Add Local Floppy

Boot Order

| Name | vNIC/vHBA/iSCSI vNIC | WWN |
|---------------------|----------------------|-----|
| Remote CD/DVD | 1 | |
| San | 2 | |
| SAN Primary | Fabric-A | ... |
| SAN Secondary | Fabric-B | ... |
| CIMC Mounted CD/DVD | 3 | |

35. Click OK, then click OK again to create the boot policy.

Create Service Profile Template (FC Boot)

In this procedure, one service profile template for Infrastructure ESXi hosts is created for Fabric A boot.

To create the service profile template, complete the following steps:

1. In Cisco UCS Manager, click Servers on the left.
2. Select Service Profile Templates > root.
3. Right-click root.
4. Select Create Service Profile Template to open the Create Service Profile Template wizard.
5. Enter VM-Host-Infra-FC-A as the name of the service profile template. This service profile template is configured to boot from storage node 1 on fabric A.
6. Select the "Updating Template" option.

- Under UUID, select UUID_Pool as the UUID pool.

Create Service Profile Template ? X

You must enter a name for the service profile template and specify the template type. You can also specify how a UUID will be assigned to this template and enter a description.

Name :

The template will be created in the following organization. Its name must be unique within this organization.
Where : **org-root**

The template will be created in the following organization. Its name must be unique within this organization.
Type : Initial Template Updating Template

Specify how the UUID will be assigned to the server associated with the service generated by this template.
UUID

UUID Assignment:

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

Optionally enter a description for the profile. The description can contain information about when and where the service profile should be used.

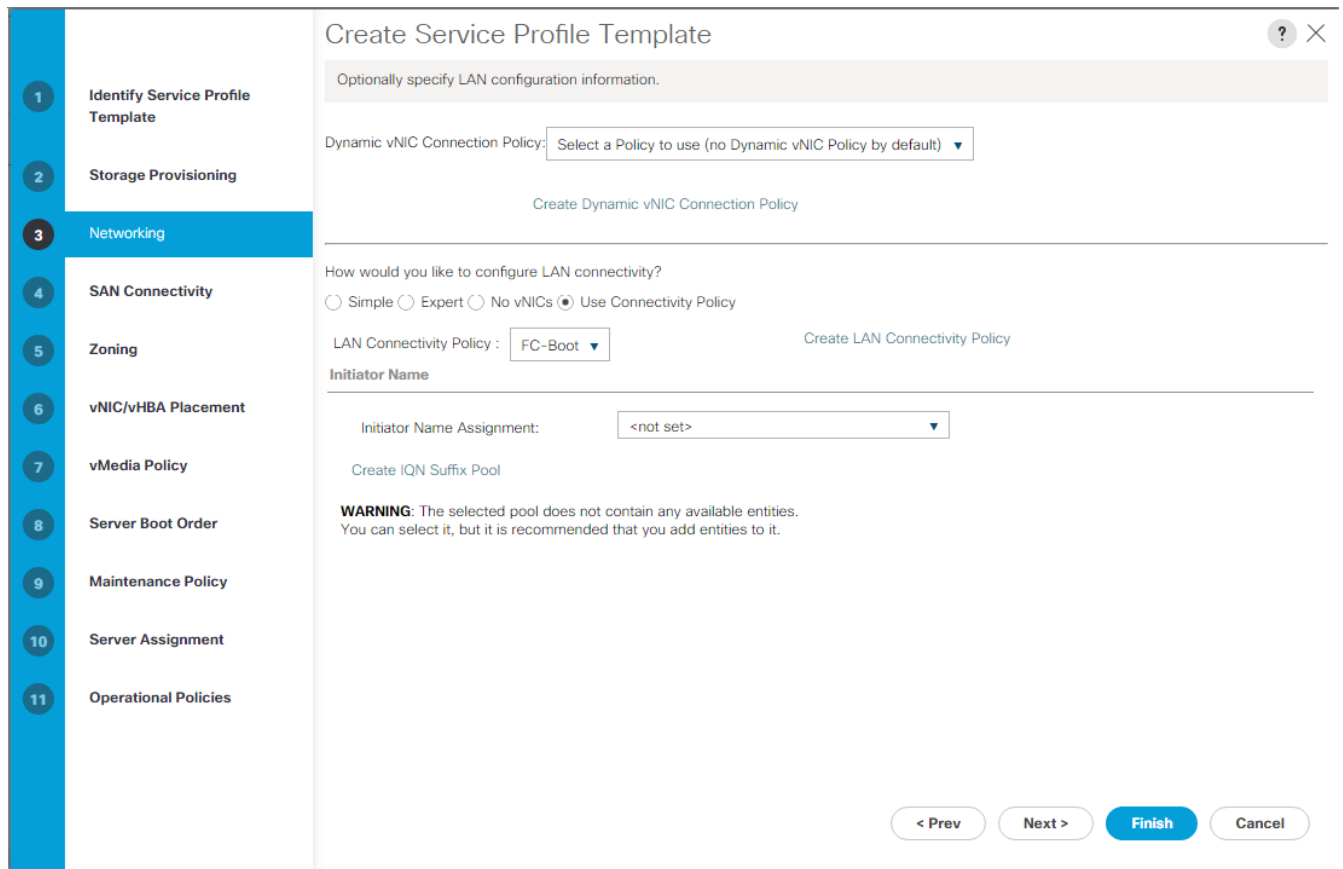
- Click Next.

Configure Storage Provisioning

- If you have servers with no physical disks, click on the Local Disk Configuration Policy tab and select the SAN-Boot Local Storage Policy. Otherwise, select the default Local Storage Policy.
- Click Next.

Configure Networking Options

- Keep the default setting for Dynamic vNIC Connection Policy.
- Select the **“Use Connectivity Policy”** option to configure the LAN connectivity.
- Select FC-Boot from the LAN Connectivity Policy pull-down.
- Leave Initiator Name Assignment at <not set>.



6. Click Next.

Configure Storage Options

1. Select the Use Connectivity Policy option for the “How would you like to configure SAN connectivity?” field.
2. Select the FC-Boot option from the SAN Connectivity Policy pull-down.

Create Service Profile Template ? X

Optionally specify disk policies and SAN configuration information.

How would you like to configure SAN connectivity?

Simple
 Expert
 No vHBAs
 Use Connectivity Policy

SAN Connectivity Policy : FC-Boot ▼ Create SAN Connectivity Policy

< Prev
Next >
Finish
Cancel

3. Click Next.

Configure Zoning Options

1. Set no Zoning options and click Next.

Configure vNIC/HBA Placement

1. In the “Select Placement” list, leave the placement policy as “Let System Perform Placement”.
2. Click Next.

Configure vMedia Policy

1. Do not select a vMedia Policy.
2. Click Next.

Configure Server Boot Order

1. Select Boot-FC-Fabric-A for Boot Policy.

Create Service Profile Template

Optionally specify the boot policy for this service profile template.

Select a boot policy.

Boot Policy: **Boot-FC-Fabric-A** Create Boot Policy

Name : **Boot-FC-Fabric-A**
 Description :
 Reboot on Boot Order Change : **No**
 Enforce vNIC/vHBA/iSCSI Name : **Yes**
 Boot Mode : **Legacy**

WARNINGS:
 The type (primary/secondary) does not indicate a boot order presence.
 The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.
 If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.
 If it is not selected, the vNICs/vHBAs are selected if they exist, otherwise the vNIC/vHBA with the lowest PCIe bus scan order is used.

Boot Order

| Name | Order | vNIC/vHB... | Type | WWN | LUN Name | Slot Num... | Boot Name | Boot Path | Description |
|-------|-------|-------------|-----------|--------------|----------|-------------|-----------|-----------|-------------|
| SA... | | Fabric-A | Primary | | | | | | |
| ... | | | Primary | 20:01:00:... | 0 | | | | |
| ... | | | Secondary | 20:04:00:... | 0 | | | | |
| SA... | | Fabric-B | Secondary | | | | | | |
| ... | | | Primary | 20:02:00:... | 0 | | | | |
| ... | | | Secondary | 20:03:00:... | 0 | | | | |

Create iSCSI vNIC Set iSCSI Boot Parameters Set UEFI Boot Parameters

< Prev Next > Finish Cancel

2. Click Next to continue to the next section.

Configure Maintenance Policy

1. Change the Maintenance Policy to default.

Create Service Profile Template ? X

Specify how disruptive changes such as reboots, network interruptions, and firmware upgrades should be applied to the server associated with this service profile.

⊖ Maintenance Policy

Select a maintenance policy to include with this service profile or create a new maintenance policy that will be accessible to all service profiles.

Maintenance Policy: [Create Maintenance Policy](#)

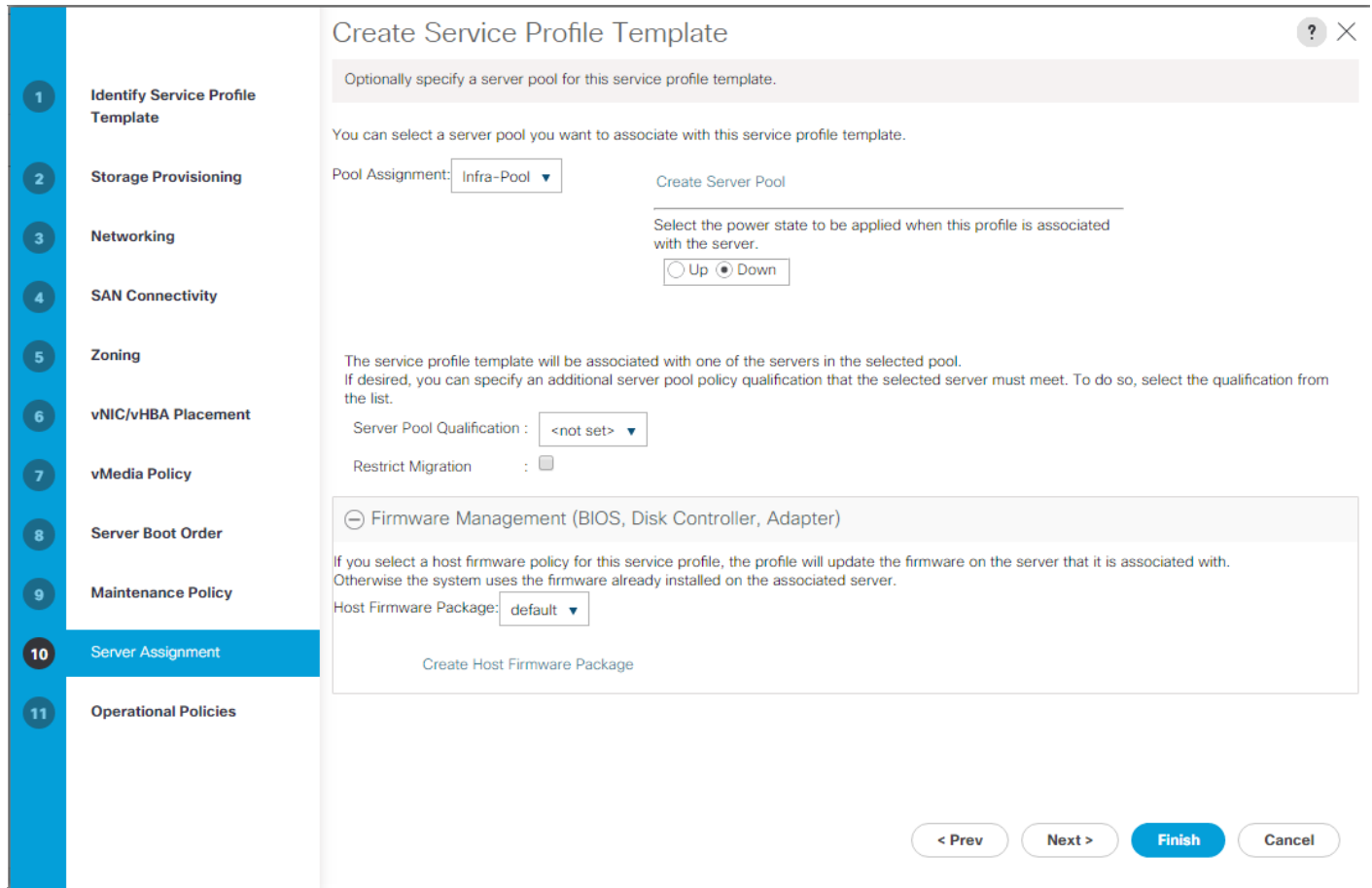
Name : **default**
 Description :
 Soft Shutdown Timer : **150 Secs**
 Reboot Policy : **User Ack**

2. Click Next.

Configure Server Assignment

To configure server assignment, complete the following steps:

1. In the Pool Assignment list, select Infra-Pool.
2. Select Down as the power state to be applied when the profile is associated with the server.
3. Optional: select **“UCS-Broadwell”** for the **Server Pool Qualification**.
4. Expand **Firmware Management** at the bottom of the page and select the default policy



5. Click Next.

Configure Operational Policies

To configure the operational policies, complete the following steps:

1. In the BIOS Policy list, select VM-Host.
2. Expand Power Control Policy Configuration and select No-Power-Cap in the Power Control Policy list.

Create Service Profile Template ? X

Optionally specify information that affects how the system operates.

⊖ BIOS Configuration

If you want to override the default BIOS settings, select a BIOS policy that will be associated with this service profile

BIOS Policy : VM-Host ▼

+ External IPMI Management Configuration

+ Management IP Address

+ Monitoring Configuration (Thresholds)

⊖ Power Control Policy Configuration

Power control policy determines power allocation for a server in a given power group.

Power Control Policy : No-Power-Cap ▼ [Create Power Control Policy](#)

+ Scrub Policy

+ KVM Management Policy

< Prev Next > **Finish** Cancel

3. Click Finish to create the service profile template.
4. Click OK in the confirmation message.

Create vMedia Service Profile Template

To create service profiles from the service profile template, complete the following steps:

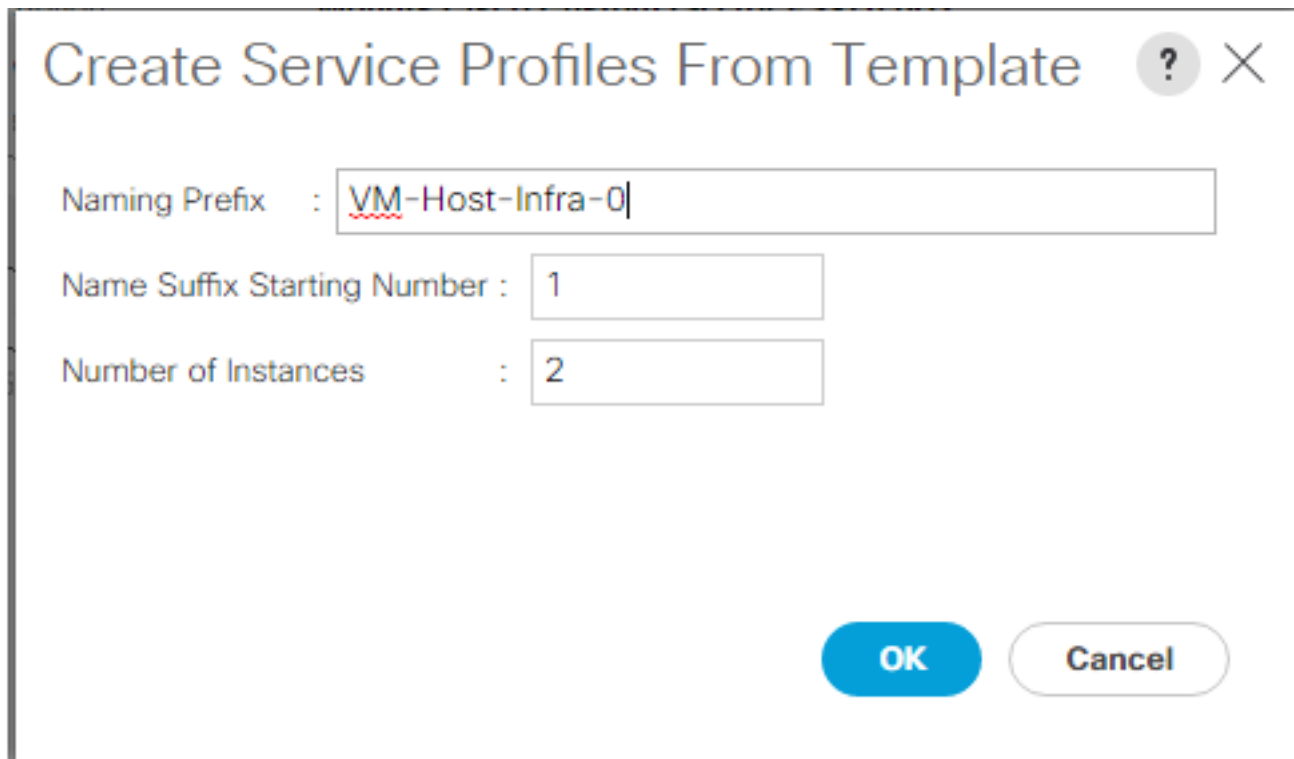
1. Connect to UCS Manager and click Servers on the left.
2. Select Service Profile Templates > root > Service Template VM-Host-Infra-FC-A.
3. Right-click Service Template VM-Host-Infra-FC-A and select Create a Clone.
4. Name the clone VM-Host-Infra-FC-A-vM and click OK.
5. Select Service Template VM-Host-Infra-FC-A-vM.
6. In the right pane, select the vMedia Policy tab.
7. Under Actions, select Modify vMedia Policy.
8. Using the pulldown, select the ESXi-6.0U2-HTTP vMedia Policy.

9. Click OK then OK again to complete modifying the Service Profile Template.

Create Service Profiles

To create service profiles from the service profile template, complete the following steps:

1. Connect to UCS Manager and click Servers on the left.
2. Select Service Profile Templates > root > Service Template VM-Host-Infra-FC-A-vM.
3. Right-click VM-Host-Infra-FC-A-vM and select Create Service Profiles from Template.
4. Enter VM-Host-Infra-0 as the service profile prefix.
5. Enter 1 as “Name Suffix Starting Number.”
6. Enter 2 as the “Number of Instances.”
7. Click OK to create the service profiles.



Create Service Profiles From Template ? X

Naming Prefix :

Name Suffix Starting Number :

Number of Instances :

OK **Cancel**

8. Click OK in the confirmation message.

Add More Servers to FlexPod Unit

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

Gather Necessary Information

After the Cisco UCS service profiles have been created, each infrastructure server in the environment will have a unique configuration. To proceed with the FlexPod deployment, specific information must be gathered from each Cisco UCS server and from the NetApp controllers. Insert the required information into Table 19 and Table 20.

Table 19 WWPNs from NetApp Storage

| SVM | Target LIF WWPN (FC) |
|-----------|----------------------|
| Infra-SVM | fcp_lif01a |
| | fcp_lif01b |
| | fcp_lif02a |
| | fcp_lif02b |



To obtain the FC WWPNs, run the `network interface show` command on the storage cluster management interface.

Table 20 FC WWPNs for fabric A and fabric B

| Cisco UCS Service Profile Name | Initiator: WWPNs (FC) | Variables |
|--------------------------------|-----------------------|--|
| VM-Host-Infra-01 | | <vm-host-infra-01-wwpna> <vm-host-infra-01-wwpnb> |
| VM-Host-Infra-02 | | <vm-host-infra-02-wwpna> <vm-host-infra-02-wwpnb> |



To obtain the FC vHBA WWPN information in Cisco UCS Manager GUI, go to Servers > Service Profiles > root. Click each service profile and then click the “Storage” tab, then “vHBAs” tab on the right. The WWPNs are displayed in the table at the bottom of the page.

SAN Switch Configuration

This section provides a detailed procedure for configuring the Cisco MDS 9000s for use in a FlexPod environment. Follow these steps precisely because failure to do so could result in an improper configuration.

If directly connecting storage to the UCS fabric interconnects, skip this section.

Physical Connectivity

Follow the physical connectivity guidelines for FlexPod as covered in the section “FlexPod Cabling.”

FlexPod Cisco MDS Base

The following procedures describe how to configure the Cisco Nexus switches for use in a base FlexPod environment. This procedure assumes the use of the Cisco MDS 9148s with NX-OS

Set Up Initial Configuration

Cisco MDS 9148S A

To set up the initial configuration for the Cisco MDS A switch, <mds-A-hostname>, complete the following steps:



On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning

1. Configure the switch using the command line.

```
Do you want to enforce secure password standard (yes/no) [y]: Enter
Enter the password for "admin": <password>
Confirm the password for "admin": <password>
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]: Enter
Configure read-only SNMP community string (yes/no) [n]: Enter
Configure read-write SNMP community string (yes/no) [n]: Enter
Enter the switch name : <mds-A-hostname> Enter
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
Mgmt0 IPv4 address : <mds-A-mgmt0-ip> Enter
Mgmt0 IPv4 netmask : <mds-A-mgmt0-netmask> Enter
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway : <mds-A-mgmt0-gw> Enter
Configure advanced IP options? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter
```

```

Type of ssh key you would like to generate (dsa/rsa) [rsa]: Enter
Number of rsa key bits <1024-2048> [1024]: Enter
Enable the telnet service? (yes/no) [n]: Enter
Configure congestion/no_credit drop for fc interfaces? (yes/no) [y]: Enter
Enter the type of drop to configure congestion/no_credit drop? (con/no) [c]: Enter
Enter milliseconds in multiples of 10 for congestion-drop for port mode F
in range (<100-500>/default), where default is 500. [d]: Enter
Enable the http-server? (yes/no) [y]: Enter
Configure timezone? (yes/no) [n]: Enter
Configure summertime? (yes/no) [n]: Enter
Configure the ntp server? (yes/no) [n]: yes
NTP server IPv4 address : <switch-a-ntp-ip>
Configure default switchport interface state (shut/noshut) [shut]: Enter
Configure default switchport trunk mode (on/off/auto) [on]: Enter
Configure default switchport port mode F (yes/no) [n]: yes
Configure default zone policy (permit/deny) [deny]: Enter
Enable full zoneset distribution? (yes/no) [n]: yes
Configure default zone mode (basic/enhanced) [basic]: Enter

```

2. Review the configuration.

```

Would you like to edit the configuration? (yes/no) [n]: Enter
Use this configuration and save it? (yes/no) [y]: Enter

```

Cisco MDS 9148S B

To set up the initial configuration for the Cisco MDS B switch, <mds-B-hostname>, complete the following steps:



On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning

1. Configure the switch using the command line.

```

Do you want to enforce secure password standard (yes/no) [y]: Enter
Enter the password for "admin": <password>
Confirm the password for "admin": <password>
Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]: Enter
Configure read-only SNMP community string (yes/no) [n]: Enter
Configure read-write SNMP community string (yes/no) [n]: Enter

```

```

Enter the switch name : <mds-B-hostname> Enter
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
Mgmt0 IPv4 address : <mds-B-mgmt0-ip> Enter
Mgmt0 IPv4 netmask : <mds-B-mgmt0-netmask> Enter
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway : <mds-B-mgmt0-gw> Enter
Configure advanced IP options? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter
Type of ssh key you would like to generate (dsa/rsa) [rsa]: Enter
Number of rsa key bits <1024-2048> [1024]: Enter
Enable the telnet service? (yes/no) [n]: Enter
Configure congestion/no_credit drop for fc interfaces? (yes/no) [y]: Enter
Enter the type of drop to configure congestion/no_credit drop? (con/no) [c]: Enter
Enter milliseconds in multiples of 10 for congestion-drop for port mode F
in range (<100-500>/default), where default is 500. [d]: Enter
Enable the http-server? (yes/no) [y]: Enter
Configure timezone? (yes/no) [n]: Enter
Configure summertime? (yes/no) [n]: Enter
Configure the ntp server? (yes/no) [n]: yes
NTP server IPv4 address : <<var_global_ntp_server_ip>>
Configure default switchport interface state (shut/noshut) [shut]: Enter
Configure default switchport trunk mode (on/off/auto) [on]: Enter
Configure default switchport port mode F (yes/no) [n]: yes
Configure default zone policy (permit/deny) [deny]: Enter
Enable full zoneset distribution? (yes/no) [n]: yes
Configure default zone mode (basic/enhanced) [basic]: Enter

```

2. Review the configuration.

```

Would you like to edit the configuration? (yes/no) [n]: Enter
Use this configuration and save it? (yes/no) [y]: Enter

```

FlexPod Cisco MDS Switch Configuration

Enable Licenses

Cisco MDS 9148S A and Cisco MDS 9148S B

To enable the correct features on the Cisco MDS switches, complete the following steps:

1. Log in as admin
2. Run the following commands:

```
configure terminal
feature npiv
feature fport-channel-trunk
```

Configure Individual Ports

Cisco MDS 9148S A

To configure individual ports and port-channels for switch A, complete the following step:



In this step and in further sections, configure the <ucs-6248-clustername> and <ucs-6332-clustername> interfaces as appropriate to your deployment.

From the global configuration mode, run the following commands:

```
interface fc1/1
switchport description <st-node01>:0e
switchport trunk mode off
port-license acquire
no shut

interface fc1/2
switchport description <st-node02>:0e
switchport trunk mode off
port-license acquire
no shutdown
exit

interface fc1/9
switchport description <ucs-6248-clustername>-a:1/31
port-license acquire
channel-group 110
no shutdown
exit

interface fc1/10
switchport description <ucs-6248-clustername>-b:1/31
port-license acquire
channel-group 110
no shutdown
exit

interface fc1/11
switchport description <ucs-6332-clustername>-a:1/1
port-license acquire
channel-group 112
no shutdown
exit

interface fc1/12
switchport description <ucs-6332-clustername>-b:1/1
port-license acquire
channel-group 112
no shutdown
exit

interface port-channel110
channel mode active
switchport mode F
switchport trunk allowed vsan 101
switchport description <ucs-6248-clustername>
```

```

switchport rate-mode dedicated

interface port-channel112
channel mode active
switchport mode F
switchport trunk allowed vsan 101
switchport description <ucs-6332-clustername>
switchport rate-mode dedicated

```

Create Port Descriptions - Fabric B

To configure individual ports and port-channels for switch B, complete the following step:

From the global configuration mode, run the following commands:

```

interface fc1/1
switchport description <st-node01>:0f
switchport trunk mode off
port-license acquire
no shut

interface fc1/2
switchport description <st-node02>:0f
switchport trunk mode off
port-license acquire
no shutdown
exit

interface fc1/9
switchport description <ucs-6248-clustername>-a:1/32
port-license acquire
channel-group 111
no shutdown
exit

interface fc1/10
switchport description <ucs-6248-clustername>-a:1/32
port-license acquire
channel-group 111
no shutdown
exit

interface fc1/11
switchport description <ucs-6332-clustername>-a:1/2
port-license acquire
channel-group 113
no shutdown
exit

interface fc1/12
switchport description <ucs-6332-clustername>-a:1/2
port-license acquire
channel-group 113
no shutdown
exit

interface port-channel111
channel mode active
switchport mode F
switchport trunk allowed vsan 102
switchport description <ucs-6248-clustername>
switchport rate-mode dedicated

interface port-channel113
channel mode active
switchport mode F
switchport trunk allowed vsan 102
switchport description <ucs-6332-clustername>
switchport rate-mode dedicated

```

Create VSANs

Cisco MDS 9148S A

To create the necessary VSANs for fabric A and add ports to them, complete the following step:

From the global configuration mode, run the following commands:

```
vsan database
vsan 101
vsan 101 name Fabric-A
exit
vsan database
vsan 101 interface fc1/1
vsan 101 interface fc1/2
vsan 101 interface port-channel110
vsan 101 interface port-channel112
```

Cisco MDS 9148S B

To create the necessary VSANs for fabric A and add ports to them, complete the following step:

From the global configuration mode, run the following commands:

```
vsan database
vsan 102
vsan 102 name Fabric-B
exit
vsan database
vsan 102 interface fc1/1
vsan 102 interface fc1/2
vsan 102 interface port-channel111
vsan 102 interface port-channel113
```

Create Device Aliases

Cisco MDS 9148S A

To create device aliases for Fabric A that will be used to create zones, complete the following step:

From the global configuration mode, run the following commands:

```
configure terminal
device-alias database
device-alias name fcp_lif01a pwnn <fcp_lif01a-wwpn>
device-alias name fcp_lif02a pwnn <fcp_lif02a-wwpn>
device-alias name VM-Host-Infra-01-A pwnn <vm-host-infra-01-wwpna>
device-alias name VM-Host-Infra-02-A pwnn <vm-host-infra-02-wwpna>
device-alias commit
```

Cisco MDS 9148S B

To create device aliases for Fabric B that will be used to create zones, complete the following step:

From the global configuration mode, run the following commands:

```
configure terminal
device-alias database
device-alias name fcp_lif01b pwnn <fcp_lif01b-wwpn>
device-alias name fcp_lif02b pwnn <fcp_lif02b-wwpn>
device-alias name VM-Host-Infra-01-B pwnn <vm-host-infra-01-wwpnb>
device-alias name VM-Host-Infra-02-B pwnn <vm-host-infra-02-wwpnb>
```

```
device-alias commit
```

Create Zones

Cisco MDS 9148S A

To create the required zones on Fabric A, run the following commands:

```
configure terminal
zone name VM-Host-Infra-01-A vsan 101
member device-alias VM-Host-Infra-01-A
member device-alias fcp_lif01a
member device-alias fcp_lif02a
exit
zone name VM-Host-Infra-02-A vsan 101
member device-alias VM-Host-Infra-02-A
member device-alias fcp_lif01a
member device-alias fcp_lif02a
exit
zoneset name Fabric-A vsan 101
member VM-Host-Infra-01-A
member VM-Host-Infra-02-A
exit
zoneset activate name Fabric-A vsan 101
exit
show zoneset active vsan 101
```

Cisco MDS 9148S B

To create the required zones on Fabric B, run the following commands:

```
configure terminal
zone name VM-Host-Infra-01-B vsan 102
member device-alias VM-Host-Infra-01-B
member device-alias fcp_lif01b
member device-alias fcp_lif02b
exit
zone name VM-Host-Infra-02-B vsan 102
member device-alias VM-Host-Infra-02-B
member device-alias fcp_lif01b
member device-alias fcp_lif02b
exit
zoneset name Fabric-B vsan 102
member VM-Host-Infra-01-B
member VM-Host-Infra-02-B
exit
zoneset activate name Fabric-B vsan 102
exit
show zoneset active vsan 102
```

Storage Configuration – Boot LUNs and Igroups

Clustered Data ONTAP Boot Storage Setup

Create Igroups

Create igroups by entering the following commands from the cluster management node SSH connection:

```
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-01 -protocol fcp -ostype vmware -initiator <vm-host-
infra-01-wwpna>, <vm-host-infra-01-wwpnb>
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-02 -protocol fcp -ostype vmware -initiator <vm-host-
infra-02-wwpna>, <vm-host-infra-02-wwpnb>
igroup create -vserver Infra-SVM -igroup MGMT-Hosts -protocol fcp -ostype vmware -initiator <vm-host-infra-
01-wwpna>, <vm-host-infra-01-wwpnb>, <vm-host-infra-02-wwpna>, <vm-host-infra-02-wwpnb>
```



Use the values listed in **Error! Reference source not found.** and **Error! Reference source not found.** for the WWPN information.

To view the three igroups you just created, type `igroup show`.

Map Boot LUNs to igroups

From the storage cluster management SSH connection, enter the following commands:

```
lun map -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-01 -igroup VM-Host-Infra-01 -lun-id 0
lun map -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-02 -igroup VM-Host-Infra-02 -lun-id 0
```


VMware vSphere 6.0 U2 Setup

VMware ESXi 6.0 U2

This section provides detailed instructions for installing VMware ESXi 6.0 in an environment. After the procedures are completed, two booted ESXi hosts will be provisioned.

Several methods exist for installing ESXi in a VMware environment. These procedures focus on how to use the built-in keyboard, video, mouse (KVM) console and virtual media features in Cisco UCS Manager to map remote installation media to individual servers and connect to their boot logical unit numbers (LUNs).

Download Cisco Custom Image for ESXi 6.0 U2

If the VMware ESXi custom image has not been downloaded, complete the following steps to complete the download.

1. Click the following link: [CiscoCustomImage6.0U2Patch3](#).
2. You will need a user id and password on www.cisco.com to download this software.
3. Download the .iso file.



This ESXi 6.0 U2 Patch 3 Cisco custom image includes updates for the fnic and eNIC drivers. The versions that are part of this image are: eNIC: 2.3.0.7; fNIC: 1.6.0.25. These drivers need to be upgraded.

Log in to Cisco UCS 6300/6200 Fabric Interconnect

Cisco UCS Manager

The Cisco UCS IP KVM enables the administrator to begin the installation of the operating system (OS) through remote media. It is necessary to log in to the UCS environment to run the IP KVM.

To log in to the Cisco UCS environment, complete the following steps:

1. Open a web browser and enter the IP address for the Cisco UCS cluster address. This step launches the Cisco UCS Manager application.
2. Click the Launch UCS Manager link under HTML to launch the HTML 5 UCS Manager GUI.
3. If prompted to accept security certificates, accept as necessary.
4. When prompted, enter admin as the user name and enter the administrative password.
5. To log in to Cisco UCS Manager, click Login.
6. From the main menu, click Servers on the left.
7. Select Servers > Service Profiles > root > VM-Host-Infra-01.

8. Right-click VM-Host-Infra-01 and select KVM Console.
9. Follow the prompts to launch the Java-based KVM console.
10. Select Servers > Service Profiles > root > VM-Host-Infra-02.
11. Right-click VM-Host-Infra-02. and select KVM Console.
12. Follow the prompts to launch the Java-based KVM console.

Set Up VMware ESXi Installation

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



Skip this section if you are using vMedia policies. The ISO file will already be connected to KVM.

To prepare the server for the OS installation, complete the following steps on each ESXi host:

1. In the KVM window, click Virtual Media.
2. Click Activate Virtual Devices.
3. If prompted to accept an Unencrypted KVM session, accept as necessary.
4. Click Virtual Media and select Map CD/DVD.
5. Browse to the ESXi installer ISO image file and click Open.
6. Click Map Device.
7. Click the KVM tab to monitor the server boot.

Install ESXi

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

To install VMware ESXi to the FC-bootable LUN of the hosts, complete the following steps on each host:

1. Boot the server by selecting Boot Server and click OK, then click OK again.
2. On reboot, the machine detects the presence of the ESXi installation media. Select the ESXi installer from the boot menu that is displayed.
3. After the installer is finished loading, press Enter to continue with the installation.
4. Read and accept the end-user license agreement (EULA). Press F11 to accept and continue.
5. Select the LUN that was previously set up as the installation disk for ESXi and press Enter to continue with the installation.
6. Select the appropriate keyboard layout and press Enter.

7. Enter and confirm the root password and press Enter.
8. The installer issues a warning that the selected disk will be repartitioned. Press F11 to continue with the installation.
9. After the installation is complete, click on the Virtual Media tab and clear the ✓ mark next to the ESXi installation media. Click Yes.



The ESXi installation image must be unmapped to make sure that the server reboots into ESXi and not into the installer.

10. After the installation is complete, press Enter to reboot the server.
11. In Cisco UCS Manager, bind the current service profile to the non-vMedia service profile template to prevent mounting the ESXi installation iso over HTTP.

Set Up Management Networking for ESXi Hosts

Adding a management network for each VMware host is necessary for managing the host. To add a management network for the VMware hosts, complete the following steps on each ESXi host:

ESXi Host VM-Host-Infra-01

To configure the `vm-host-infra-01` ESXi host with access to the management network, complete the following steps:

1. After the server has finished rebooting, press F2 to customize the system.
2. Log in as root, enter the corresponding password, and press Enter to log in.
3. Select the Configure Management Network option and press Enter.
4. Select Network Adapters and press Enter.
5. Verify that the numbers in the Hardware Label field match the numbers in the Device Name field.
6. Using the space bar, select `vmnic1` to add to the management vSwitch. Press Enter.
7. Select the VLAN (Optional) option and press Enter.
8. Enter the `<ib-mgmt-vlan-id>` and press Enter.
9. Select IPv4 Configuration and press Enter.
10. Select the Set static IPv4 address and network configuration option by using the space bar.
11. Enter the IP address for managing the first ESXi host: `<vm-host-infra-01-ip>`.
12. Enter the subnet mask for the first ESXi host.
13. Enter the default gateway for the first ESXi host.

14. Press Enter to accept the changes to the IP configuration.
15. Select the IPv6 Configuration option and press Enter.
16. Using the spacebar, select `Disable IPv6 (restart required)` and press Enter.
17. Select the DNS Configuration option and press Enter.



Since the IP address is assigned manually, the DNS information must also be entered manually.

18. Enter the IP address of the primary DNS server.
19. Optional: Enter the IP address of the secondary DNS server.
20. Enter the fully qualified domain name (FQDN) for the first ESXi host.
21. Press Enter to accept the changes to the DNS configuration.
22. Press Esc to exit the Configure Management Network submenu.
23. Press Y to confirm the changes and return to the main menu.
24. The ESXi host reboots. After reboot, press F2 and log back in as root.
25. Select Test Management Network to verify that the management network is set up correctly and press Enter.
26. Press Enter to run the test.
27. Press Enter to exit the window.
28. Select Troubleshooting Options and press Enter.
29. Select Enable SSH and press Enter.
30. Press Esc to return to the main menu.
31. Press Esc to log out of the VMware console.

ESXi Host VM-Host-Infra-02

To configure the `vm-Host-Infra-02` ESXi host with access to the management network, complete the following steps:

1. After the server has finished rebooting, press F2 to customize the system.
2. Log in as root and enter the corresponding password.
3. Select the Configure Management Network option and press Enter.
4. Select Network Adapters and press Enter.

5. Verify that the numbers in the Hardware Label field match the numbers in the Device Name field.
6. Using the space bar, select vmnic1 to add to the management vSwitch. Press Enter.
7. Select the VLAN (Optional) option and press Enter.
8. Enter the <ib-mgmt-vlan-id> and press Enter.
9. Select IPv4 Configuration and press Enter.
10. Select the Set static IPv4 address and network configuration option by using the space bar.
11. Enter the IP address for managing the second ESXi host: <vm-host-infra-02-ip>.
12. Enter the subnet mask for the second ESXi host.
13. Enter the default gateway for the second ESXi host.
14. Press Enter to accept the changes to the IP configuration.
15. Select the IPv6 Configuration option and press Enter.
16. Using the spacebar, select Disable IPv6 (restart required) and press Enter.
17. Select the DNS Configuration option and press Enter.



Because the IP address is assigned manually, the DNS information must also be entered manually.

18. Enter the IP address of the primary DNS server.
19. Optional: Enter the IP address of the secondary DNS server.
20. Enter the FQDN for the second ESXi host.
21. Press Enter to accept the changes to the DNS configuration.
22. Press Esc to exit the Configure Management Network submenu.
23. Press Y to confirm the changes and return to the main menu.
24. The ESXi host reboots. After reboot, press F2 and log back in as root.
25. Select Test Management Network to verify that the management network is set up correctly and press Enter.
26. Press Enter to run the test.
27. Press Enter to exit the window.
28. Select Troubleshooting Options and press Enter.

29. Select Enable SSH and press Enter.
30. Press Esc to return to the main menu.
31. Press Esc to log out of the VMware console.

Download VMware vSphere Client (Optional)

To download the VMware vSphere Client, complete the following steps:

1. Open a web browser on the management workstation and navigate to the VM-Host-Infra-01 management IP address.
2. Download and install the vSphere Client for Windows.



This application is downloaded from the VMware website and Internet access is required on the management workstation.

Log in to VMware ESXi Hosts by Using VMware Host Client

ESXi Host VM-Host-Infra-01

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

1. Open a web browser on the management workstation and navigate to the VM-Host-Infra-01 management IP address.
2. Click Open the VMware Host Client.
3. Enter root for the user name.
4. Enter the root password.
5. Click Login to connect.
6. Repeat this process to log into VM-Host-Infra-02 in a separate browser tab or window.

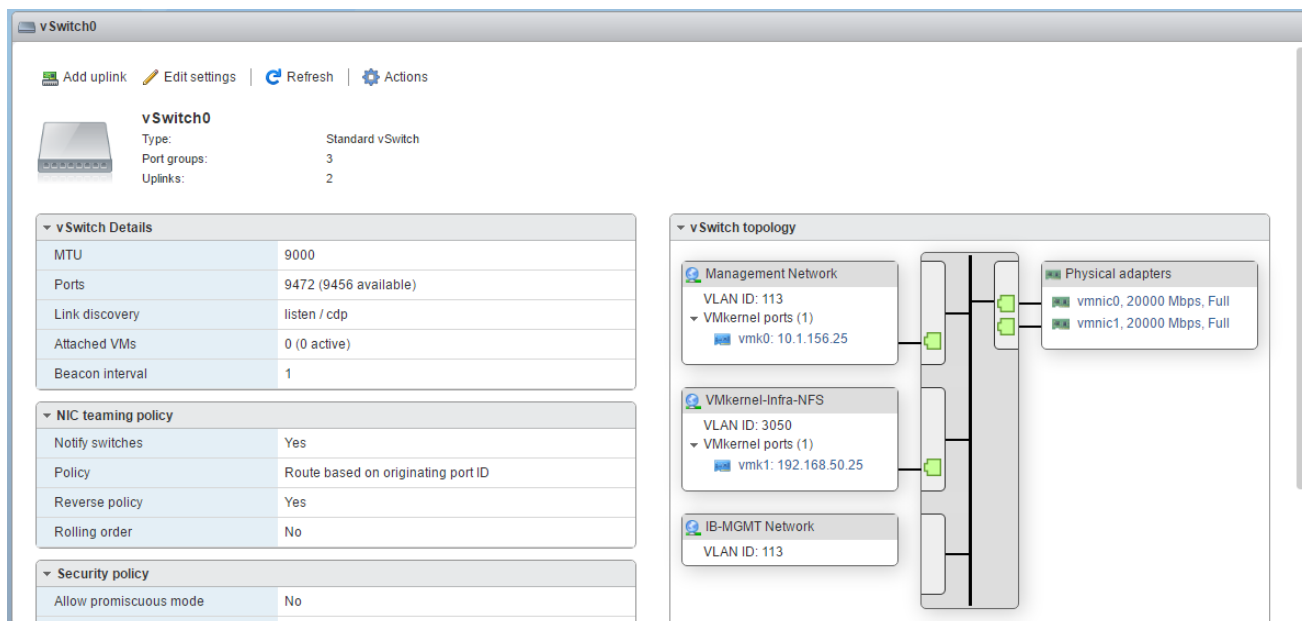
Set Up VMkernel Ports and Virtual Switch

ESXi Host VM-Host-Infra-01

To set up the VMkernel ports and the virtual switches on the `VM-Host-Infra-01` ESXi host, complete the following steps:

1. From the Host Client, select Networking on the left.
2. In the center pane, select the Virtual switches tab.
3. Select vSwitch0.

4. Select Edit settings.
5. Change the MTU to 9000.
6. Expand NIC teaming.
7. To the right of Failover order, select vmnic1.
8. Click Mark active. Verify the Status for vmnic1 changes to Active.
9. Click Save.
10. On the left, select Networking, then select the Port groups tab.
11. In the center pane, right-click VM Network and select Remove.
12. Click Remove to complete removing the port group.
13. In the center pane, select Add port group.
14. Name the port group IB-MGMT Network and enter <ib-mgmt-vlan-id> in the VLAN ID field.
15. Click Add to finalize the edits for the IB-MGMT Network.
16. At the top, select the VMkernel NICs tab.
17. Click Add VMkernel NIC.
18. For New port group, enter VMkernel-Infra-NFS
19. Enter <nfs-vlan-id> for the VLAN ID
20. Change the MTU to 9000.
21. Select Static IPv4 settings and expand IPv4 settings.
22. Enter the ESXi host NFS IP address and netmask.
23. Do not select any of the Services.
24. Click Create.
25. Select vSwitch0. The properties for vSwitch0 VMkernel NICs should be similar to the following example:



26. On the left, select Networking, then select the Virtual switches tab.
27. In the center pane, select Add standard virtual switch.
28. Name the vSwitch vMotion-vSwitch.
29. Change the MTU to 9000 and make sure vmnic2 is selected for Uplink 1.
30. Select Add uplink.
31. Make sure vmnic3 is selected for Uplink 2.
32. Click Add to add the vSwitch.
33. In the center pane, select the newly added vMotion-vSwitch. Click Edit settings.
34. Expand NIC teaming and select vmnic2. Click Mark standby to pin vMotion to UCS fabric B.
35. Click Save.
36. On the left, select Networking and then select the VMkernel NICs tab in the center pane.
37. Click Add VMkernel NIC.
38. For New port group, enter VMkernel-vMotion.
39. Select the vMotion-vSwitch Virtual switch.
40. Enter <vmotion-vlan-id> for the VLAN ID
41. Change the MTU to 9000.

42. Select Static IPv4 settings and expand IPv4 settings.
43. Enter the ESXi host vMotion IP address and netmask.
44. Select the vMotion stack TCP/IP stack.
45. Click Create.

The screenshot shows the ESXi Networking console for host esxi-01.vikings.cisco.com. The 'VMkernel NICs' tab is selected, displaying a table of three VMkernel NICs: vmk0, vmk1, and vmk2. Each row shows the NIC name, its associated port group, the TCP/IP stack, the services it provides, and its IPv4 and IPv6 addresses.

| Name | Portgroup | TCP/IP stack | Services | IPv4 address | IPv6 addresses |
|------|--------------------|----------------------|------------|----------------|----------------|
| vmk0 | Management Network | Default TCP/IP stack | Management | 10.1.156.25 | None |
| vmk1 | VMkernel-Infra-NFS | Default TCP/IP stack | | 192.168.50.25 | None |
| vmk2 | VMkernel-vMotion | vMotion stack | vMotion | 192.168.100.25 | None |

ESXi Host VM-Host-Infra-02

To set up the VMkernel ports and the virtual switches on the VM-Host-Infra-02 ESXi host, complete the following steps:

1. From the Host Client, select Networking on the left.
2. In the center pane, select the Virtual switches tab.
3. Select vSwitch0.
4. Select Edit settings.
5. Change the MTU to 9000.
6. Expand NIC teaming.
7. To the right of Failover order, select vmnic1.
8. Click Mark active. Verify the Status for vmnic1 changes to Active.
9. Click Save.
10. On the left, select Networking, then select the Port groups tab.
11. In the center pane, right-click VM Network and select Remove.
12. Click Remove to complete removing the port group.
13. In the center pane, select Add port group.
14. Name the port group IB-MGMT Network and enter <ib-mgmt-vlan-id> in the VLAN ID field.
15. Click Add to finalize the edits for the IB-MGMT Network.

16. At the top, select the VMkernel NICs tab.
17. Click Add VMkernel NIC.
18. For New port group, enter VMkernel-Infra-NFS
19. Enter <nfs-vlan-id> for the VLAN ID
20. Change the MTU to 9000.
21. Select Static IPv4 settings and expand IPv4 settings.
22. Enter the ESXi host NFS IP address and netmask.
23. Do not select any of the Services.
24. Click Create.
25. Select vSwitch0. The properties for vSwitch0 VMkernel NICs should be similar to the following example:

The screenshot displays the configuration for vSwitch0. The top section shows the vSwitch name and type (Standard vSwitch) with 3 port groups and 2 uplinks. Below this are three expandable sections: vSwitch Details, NIC teaming policy, and Security policy. The vSwitch topology diagram on the right shows the vSwitch connected to three networks: Management Network (VLAN 113) with VMkernel port vmk0 (10.1.156.26), VMkernel-Infra-NFS (VLAN 3050) with VMkernel port vmk1 (192.168.50.26), and IB-MGMT Network (VLAN 113). Physical adapters vmnic0 and vmnic1 are also shown connected to the vSwitch.

| vSwitch Details | |
|-----------------|-----------------------|
| MTU | 9000 |
| Ports | 9472 (9456 available) |
| Link discovery | listen / cdp |
| Attached VMs | 0 (0 active) |
| Beacon interval | 1 |

| NIC teaming policy | |
|--------------------|------------------------------------|
| Notify switches | Yes |
| Policy | Route based on originating port ID |
| Reverse policy | Yes |
| Rolling order | No |

| Security policy | |
|------------------------|----|
| Allow promiscuous mode | No |

26. On the left, select Networking, then select the Virtual switches tab.
27. In the center pane, select Add standard virtual switch.
28. Name the vSwitch vMotion-vSwitch.
29. Change the MTU to 9000 and make sure vmnic2 is selected for Uplink 1.
30. Select Add uplink.

31. Make sure vmnic3 is selected for Uplink 2.
32. Click Add to add the vSwitch.
33. In the center pane, select the newly added vMotion-vSwitch. Click Edit settings.
34. Expand NIC teaming and select vmnic2. Click Mark standby to pin vMotion to UCS fabric B.
35. Click Save.
36. On the left, select Networking and then select the VMkernel NICs tab in the center pane.
37. Click Add VMkernel NIC.
38. For New port group, enter VMkernel-vMotion.
39. Select the vMotion-vSwitch Virtual switch.
40. Enter <vmotion-vlan-id> for the VLAN ID
41. Change the MTU to 9000.
42. Select Static IPv4 settings and expand IPv4 settings.
43. Enter the ESXi host vMotion IP address and netmask.
44. Select the vMotion stack TCP/IP stack.
45. Click Create.

The screenshot shows the VMware vSphere Networking console for host esxi-02.vikings.cisco.com. The 'VMkernel NICs' tab is selected, displaying a table of three VMkernel NICs: vmk1, vmk0, and vmk2. Each row shows the NIC name, its associated port group, the selected TCP/IP stack, and the assigned IPv4 and IPv6 addresses.

| Name | Portgroup | TCP/IP stack | Services | IPv4 address | IPv6 addresses |
|------|--------------------|----------------------|------------|----------------|----------------|
| vmk1 | VMkernel-Infra-NFS | Default TCP/IP stack | | 192.168.50.26 | None |
| vmk0 | Management Network | Default TCP/IP stack | Management | 10.1.156.26 | None |
| vmk2 | VMkernel-vMotion | vMotion stack | vMotion | 192.168.100.26 | None |

Install VMware Drivers for the Cisco Virtual Interface Card (VIC)

Download and unzip the following VMware VIC Drivers to the Management workstation:

[fnic Driver version 1.6.0.28](#)

[enic Driver version 2.3.0.10](#)

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

To install VMware VIC Drivers on the ESXi host VM-Host-Infra-01 and VM-Host-Infra-02, complete the following steps:

1. From each Host Client, select Storage on the left.
2. Right-click datastore1 and select Browse.
3. In the Datastore browser, click Upload.
4. Navigate to the saved location for the downloaded VIC drivers and select `fnic_driver_1.6.0.28-offline_bundle-4179603.zip`.
5. Click Open to upload the file to datastore1.
6. Click Upload again.
7. Navigate to the saved location for the downloaded VIC drivers and select `ESXi6.0-enic-2.3.0.10-offline_bundle-4303638.zip`.
8. Click Open to upload the file to datastore1.
9. Make sure the files have been uploaded to both ESXi hosts.
10. Connect to each ESXi host through ssh from a shell connection or putty terminal.
11. Login as root with the root password.
12. Run the following commands on each host:

```
esxcli software vib update -d /vmfs/volumes/datastore1/fnic_driver_1.6.0.28-offline_bundle-4179603.zip  
esxcli software vib update -d /vmfs/volumes/datastore1/ESXi6.0-enic-2.3.0.10-offline_bundle-4303638.zip
```

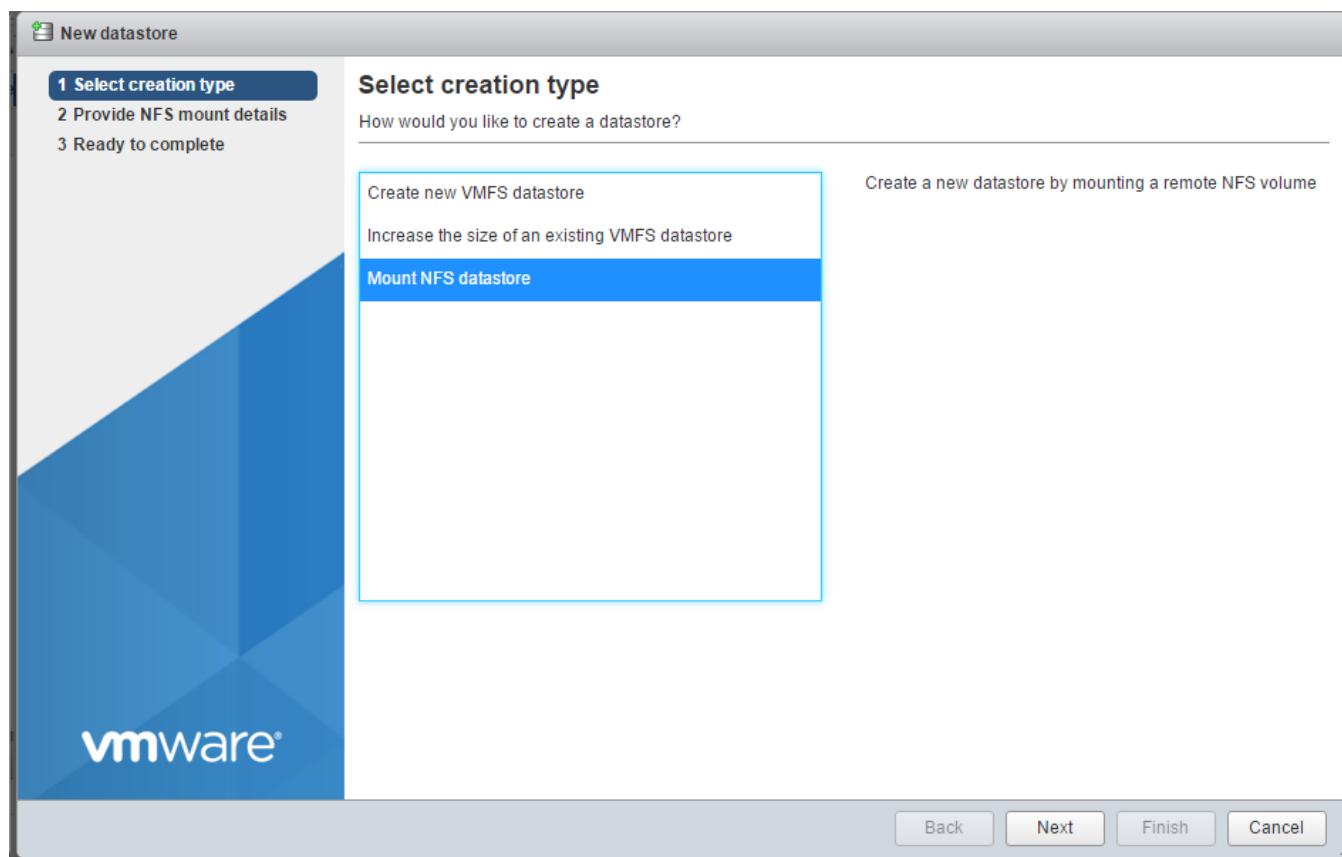
13. Reboot each host by typing `reboot` from the SSL interface after both commands have been run.
14. Log into the Host Client on each host once reboot is complete.

Mount Required Datastores

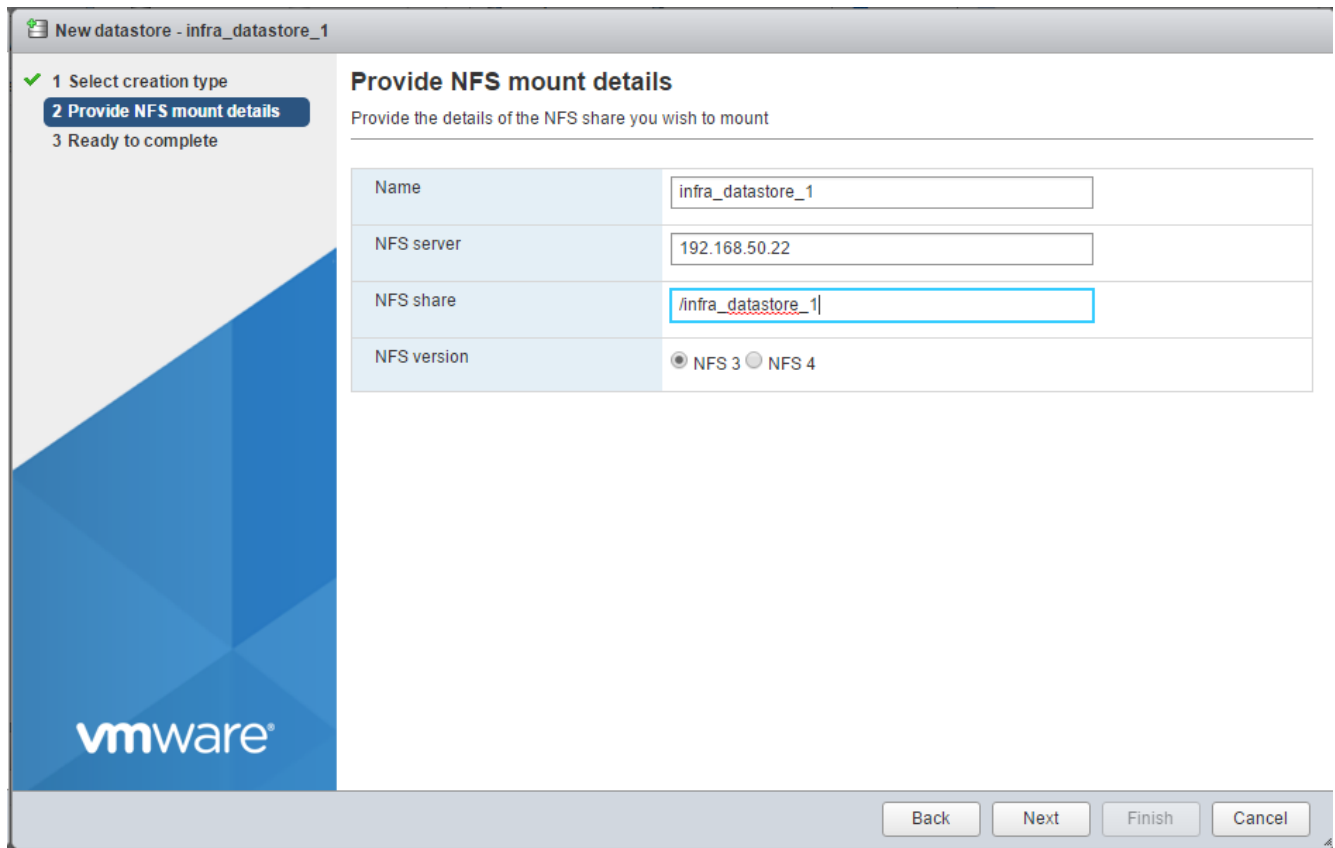
ESXi Hosts VM-Host-Infra-01 and VM-Host-Infra-02

To mount the required datastores, complete the following steps on each ESXi host:

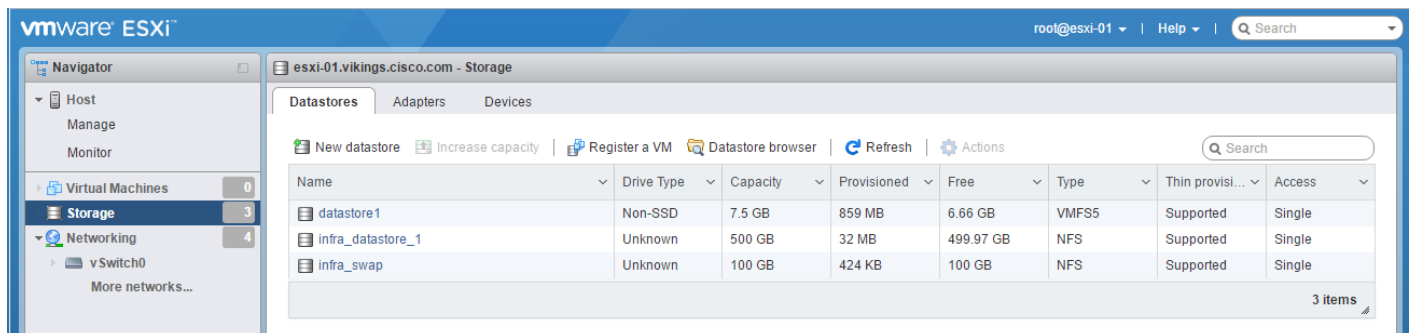
1. From the Host Client, select Storage on the left.
2. In the center pane, select New Datastore to add a new datastore.
3. In the New datastore popup, select Mount NFS datastore and click Next.



4. Input `infra_datastore_1` for the datastore name. Input the IP address for the `nfs_infra_datastore_1` LIF for the NFS server. Input `/infra_datastore_1` for the NFS share. Leave the NFS version set at NFS 3. Click Next.



5. Click Finish. The datastore should now appear in the datastore list.
6. In the center pane, select New Datastore to add a new datastore.
7. In the New datastore popup, select Mount NFS datastore and click Next.
8. Input infra_swap for the datastore name. Input the IP address for the nfs_swap LIF for the NFS server. Input /infra_swap for the NFS share. Leave the NFS version set at NFS 3. Click Next.
9. Click Finish. The datastore should now appear in the datastore list.



10. Mount both datastores on both ESXi hosts.

Configure NTP on ESXi Hosts

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

To configure Network Time Protocol (NTP) on the ESXi hosts, complete the following steps on each host:

1. From the Host Client, select Manage on the left.
2. In the center pane, select the Time & date tab.
3. Click Edit settings.
4. Make sure Use Network Time Protocol (enable NTP client) is selected.
5. Use the pulldown to select Start and stop with host.
6. Enter the two Nexus 9372 switch NTP addresses in the NTP servers box separated by a comma.

Edit time configuration

Specify how the date and time of this host should be set.

Manually configure the date and time on this host

10/13/2016 4:09 PM

Use Network Time Protocol (enable NTP client)

NTP service startup policy: Start and stop with host

NTP servers: 10.1.156.4,10.1.156.5

Separate servers with commas, e.g. 10.31.21.2, fe00::2800

Save Cancel

7. Click Save to save the configuration changes.
8. Select Actions > NTP service > Start.
9. Verify that NTP service is now running and the clock is now set to approximately the correct time.



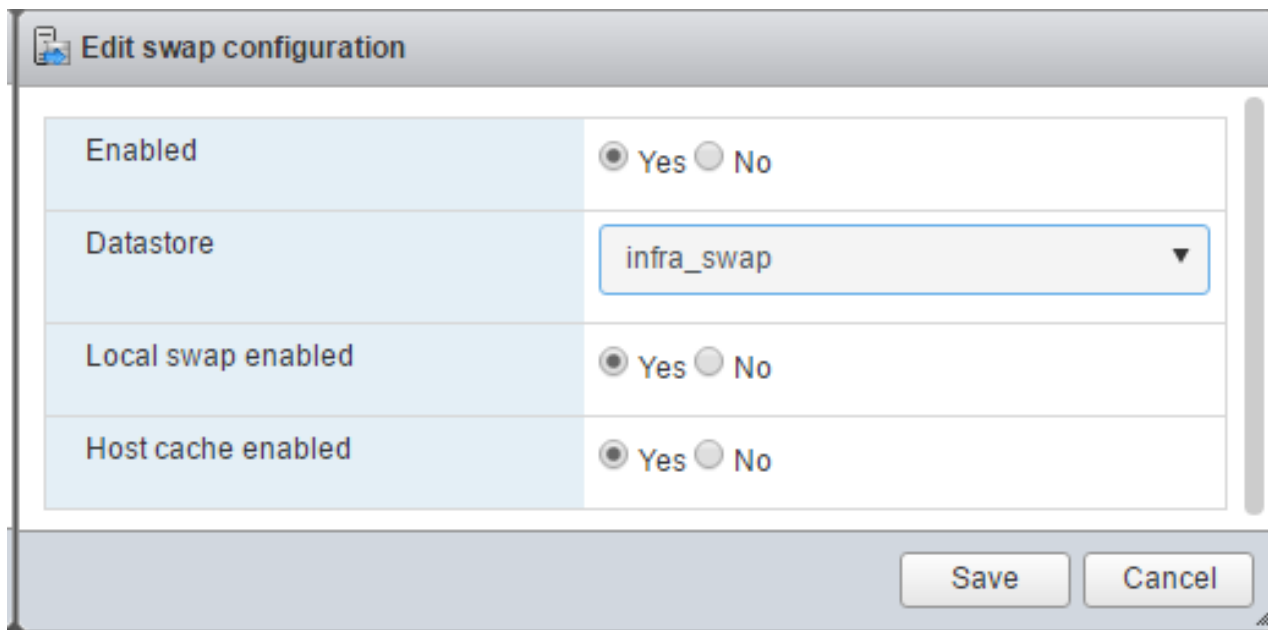
The NTP server time may vary slightly from the host time.

Move VM Swap File Location

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

To move the VM swap file location, complete the following steps on each ESXi host:

1. From the Host Client, select Manage on the left.
2. In the center pane, select the Swap tab.
3. Select Edit settings.
4. Use the Datastore pulldown to select infra_swap.



5. Click Save to save the configuration.

VMware vCenter 6.0 U2

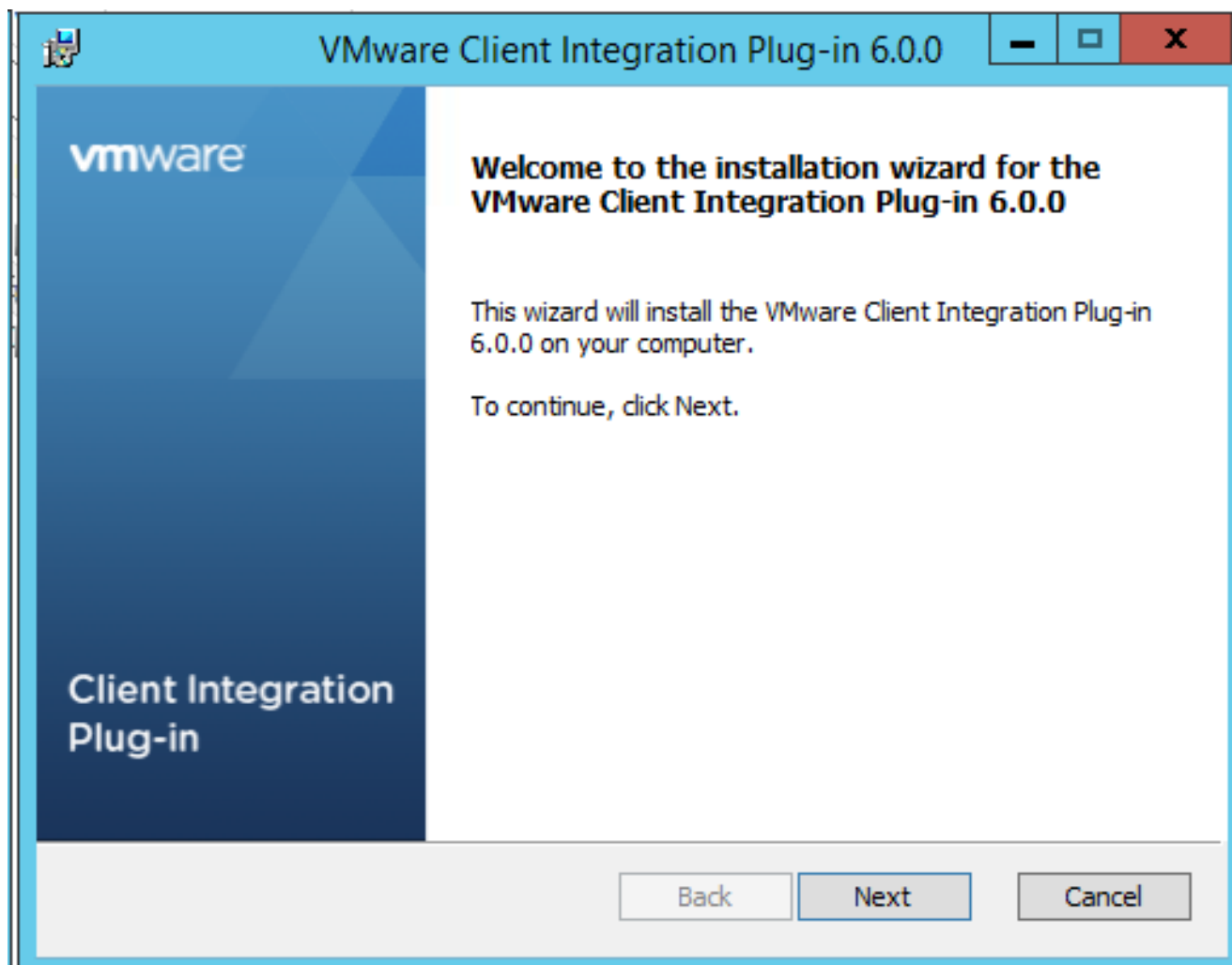
The procedures in the following subsections provide detailed instructions for installing the VMware vCenter 6.0 U2 Server Appliance in an environment. After the procedures are completed, a VMware vCenter Server will be configured.

Install the Client Integration Plug-in

To install the client integration plug-in, complete the following steps:

1. Locate and copy the VMware-VCSA-all-6.0.0-3634788.iso file to the desktop of the management workstation. This iso is for the VMware vSphere 6.0U2 vCenter Server Appliance.
2. Using ISO mounting software, mount the ISO image as a disk on the management workstation. (For example, with the Mount command in Windows Server 2012).

3. In the mounted disk directory, navigate to the vcsa directory and double-click VMware-ClientIntegrationPlugin-6.0.0.exe. The Client Integration Plug-in installation wizard appears.



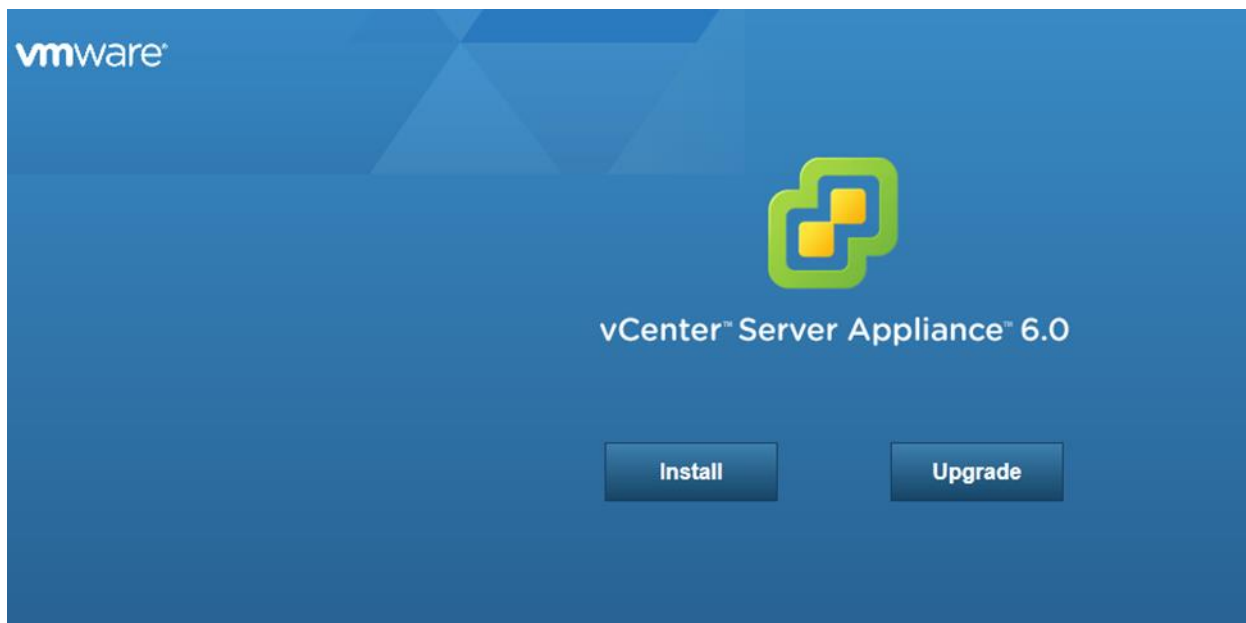
4. On the Welcome page, click Next.
5. Read and accept the terms in the End-User License Agreement and click Next.
6. Click Next.
7. Click Install.
8. Click Finish.

Building the VMware vCenter Server Appliance

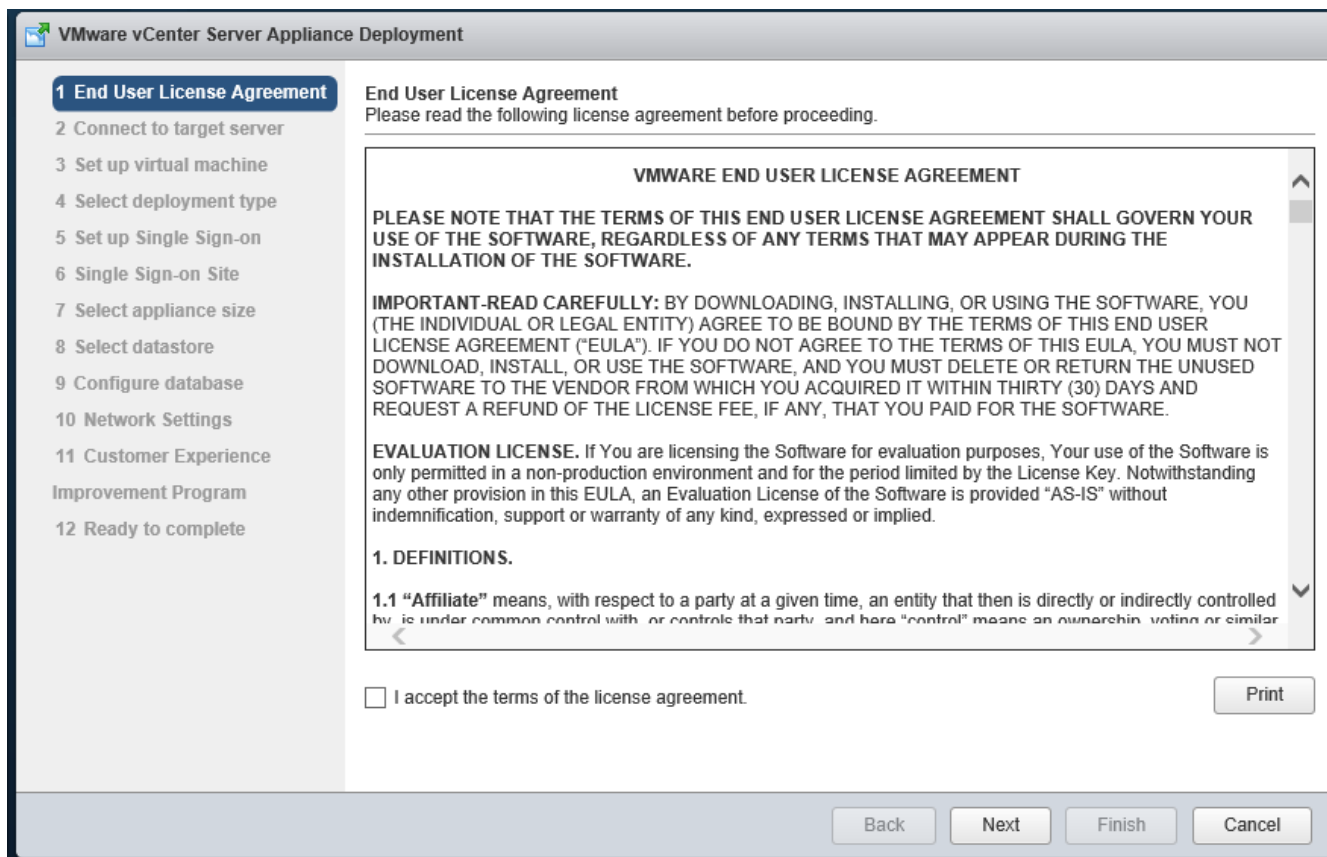
To build the VMware vCenter virtual machine, complete the following steps:

1. In the mounted disk main directory, double-click vcsa-setup.html.
2. Allow the plug-in to run in the browser when prompted.

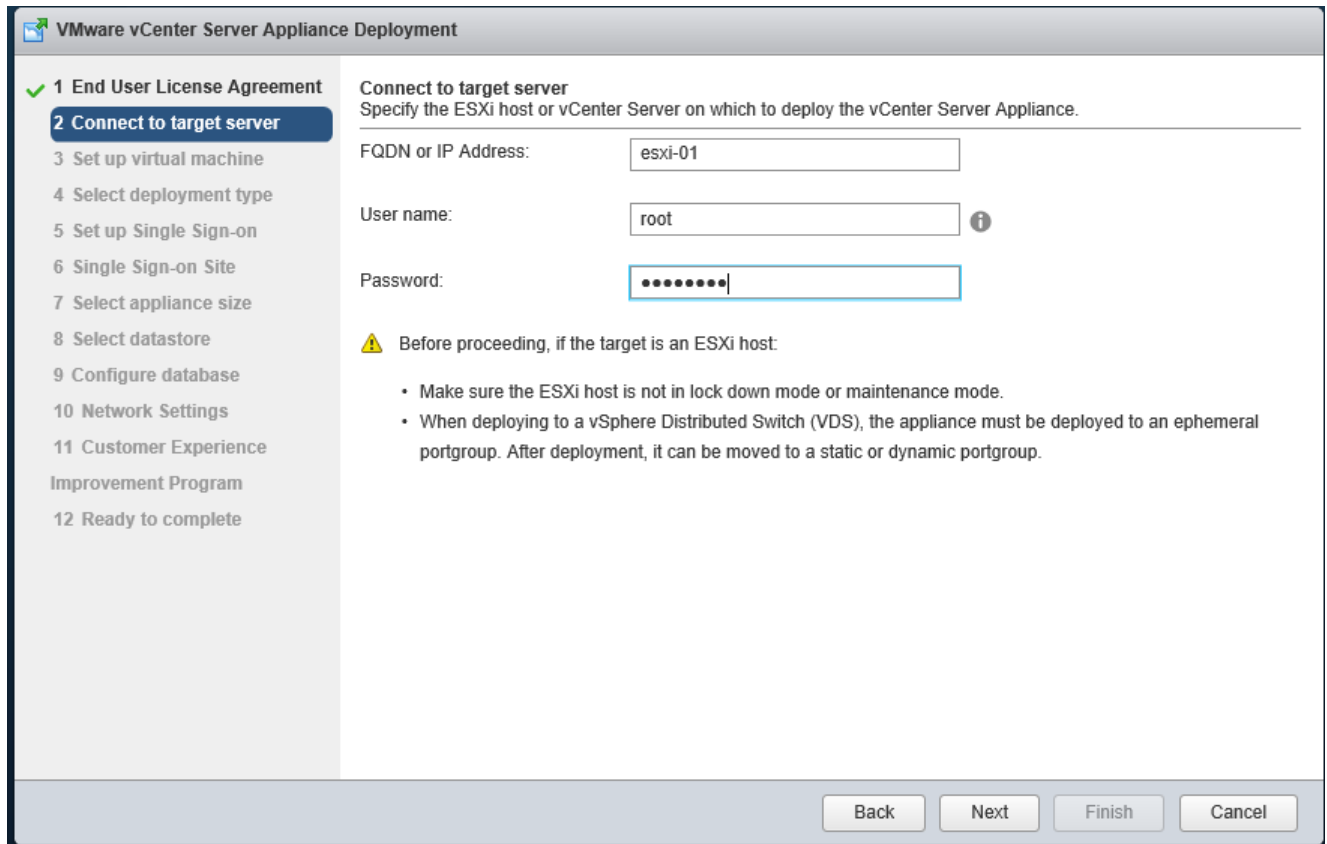
3. On the Home page, click Install to start the vCenter Server Appliance deployment wizard.



4. Read and accept the license agreement, and click Next.



5. In the “Connect to target server” page, enter the ESXi host name or IP address, User name and Password.



6. Click Yes to accept the certificate.
7. Enter the Appliance name and password details in the “Set up virtual machine” page.

The screenshot shows the VMware vCenter Server Appliance Deployment wizard. The title bar reads "VMware vCenter Server Appliance Deployment". On the left, a progress list shows steps 1 through 12. Steps 1 and 2 are completed with green checkmarks. Step 3, "Set up virtual machine", is the current step and is highlighted in blue. Steps 4 through 12 are listed below it. The main area is titled "Set up virtual machine" with the subtitle "Specify virtual machine settings for the vCenter Server Appliance to be deployed." Below this, there are four input fields: "Appliance name:" with the value "vc", "OS user name:" with the value "root", "OS password:" with a masked password of seven dots, and "Confirm OS password:" with a masked password of seven dots. Information icons (i) are present next to the appliance name and OS password fields. At the bottom right, there are four buttons: "Back", "Next", "Finish", and "Cancel".

VMware vCenter Server Appliance Deployment

✓ 1 End User License Agreement
✓ 2 Connect to target server
3 Set up virtual machine
4 Select deployment type
5 Set up Single Sign-on
6 Single Sign-on Site
7 Select appliance size
8 Select datastore
9 Configure database
10 Network Settings
11 Customer Experience Improvement Program
12 Ready to complete

Set up virtual machine
Specify virtual machine settings for the vCenter Server Appliance to be deployed.

Appliance name: ⓘ

OS user name:

OS password: ⓘ

Confirm OS password:

Back Next Finish Cancel

8. In the “Select deployment type” page, choose “Install vCenter Server with an embedded Platform Services Controller.”

VMware vCenter Server Appliance Deployment

- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- 4 Select deployment type**
- 5 Set up Single Sign-on
- 6 Single Sign-on Site
- 7 Select appliance size
- 8 Select datastore
- 9 Configure database
- 10 Network Settings
- 11 Customer Experience Improvement Program
- 12 Ready to complete

Select deployment type
Select the services to deploy onto this appliance.

vCenter Server 6.0 requires a Platform Services Controller, which contains shared services such as Single Sign-On, Licensing, and Certificate Management. An embedded Platform Services Controller is deployed on the same Appliance VM as vCenter Server. An external Platform Services Controller is deployed in a separate Appliance VM. For smaller installations, consider vCenter Server with an embedded Platform Services Controller. For larger installations with multiple vCenter Servers, consider one or more external Platform Services Controllers. Refer to the vCenter Server documentation for more information.

Note: Once you install vCenter Server, you can only change from an embedded to an external Platform Services Controller with a fresh install.

Embedded Platform Services Controller

Install vCenter Server with an Embedded Platform Services Controller

External Platform Services Controller

Install Platform Services Controller

Install vCenter Server (Requires External Platform Services Controller)

Back Next Finish Cancel

9. Click Next.

10. In the “Set up Single Sign-On” page, select “Create a new SSO domain.”

11. Enter the SSO password, Domain name and Site name.

VMware vCenter Server Appliance Deployment

- ✓ 1 End User License Agreement
- ✓ 2 Connect to target server
- ✓ 3 Set up virtual machine
- ✓ 4 Select deployment type
- 5 Set up Single Sign-on**
- 6 Select appliance size
- 7 Select datastore
- 8 Configure database
- 9 Network Settings
- 10 Customer Experience Improvement Program
- 11 Ready to complete

Set up Single Sign-on (SSO)
Create or join a SSO domain. An SSO configuration cannot be changed after deployment.

Create a new SSO domain
 Join an SSO domain in an existing vCenter 6.0 platform services controller

vCenter SSO User name: administrator

vCenter SSO Password: ⓘ

Confirm password:

SSO Domain name: ⓘ

SSO Site name: ⓘ

⚠ Before proceeding, make sure that the vCenter Single Sign-On domain name used is different than your Active Directory domain name.

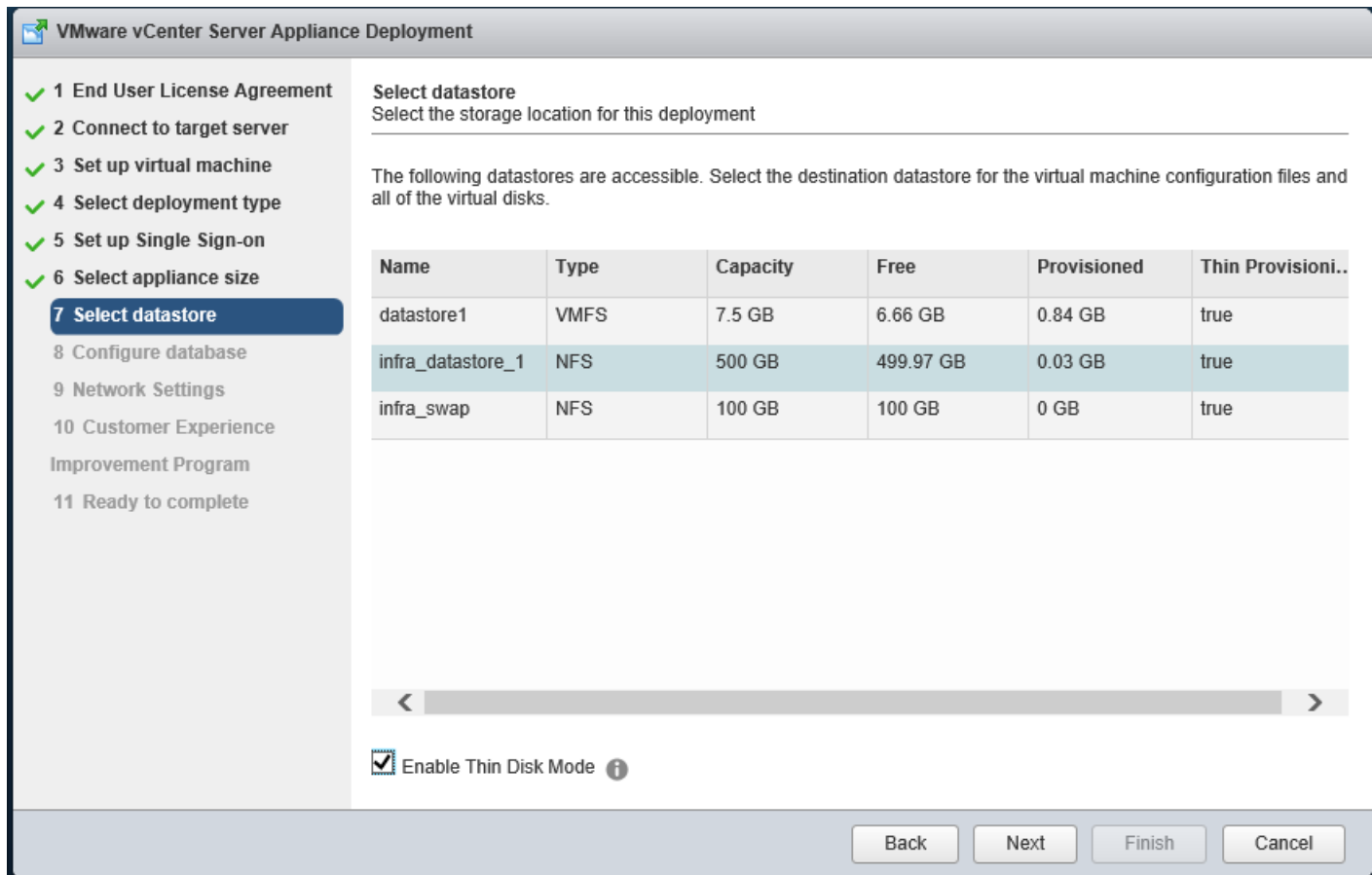
Back Next Finish Cancel

12. Click Next.

13. Select the appliance size. For example, “Tiny (up to 10 hosts, 100 VMs).”

14. Click Next.

15. In the “Select datastore” page, choose `infra_datastore_1`. Also, select Enable Thin Disk Mode.



16. Click Next.

17. Select embedded database in the “Configure database” page. Click Next.

18. In the “Network Settings” page, configure the below settings:

- a. Choose a Network: IB-MGMT Network
- b. IP address family: IPV4
- c. Network type: static
- d. Network address: <vcenter-ip>
- e. System name: <vcenter-fqdn>
- f. Subnet mask: <vcenter-subnet-mask>
- g. Network gateway: <vcenter-gateway>
- h. Network DNS Servers: <dns-server>
- i. Configure time sync: Use NTP servers – fill in NTP servers
- j. (Optional). Enable SSH

The screenshot shows the 'VMware vCenter Server Appliance Deployment' wizard. The left sidebar contains a list of steps: 1 End User License Agreement, 2 Connect to target server, 3 Set up virtual machine, 4 Select deployment type, 5 Set up Single Sign-on, 6 Select appliance size, 7 Select datastore, 8 Configure database, 9 Network Settings (highlighted), 10 Customer Experience Improvement Program, and 11 Ready to complete. The main area displays network configuration fields: IP address family (IPv4), Network type (static), Network address (10.1.156.100), System name [FQDN or IP address] (vc.vikings.cisco.com), Subnet mask (255.255.255.0), Network gateway (10.1.156.1), Network DNS Servers (separated by commas) (10.1.156.9), and Configure time sync (Use NTP servers (Separated by commas) selected, with 10.1.156.4,10.1.156.5 entered). An 'Enable ssh' checkbox is checked. At the bottom are 'Back', 'Next', 'Finish', and 'Cancel' buttons.

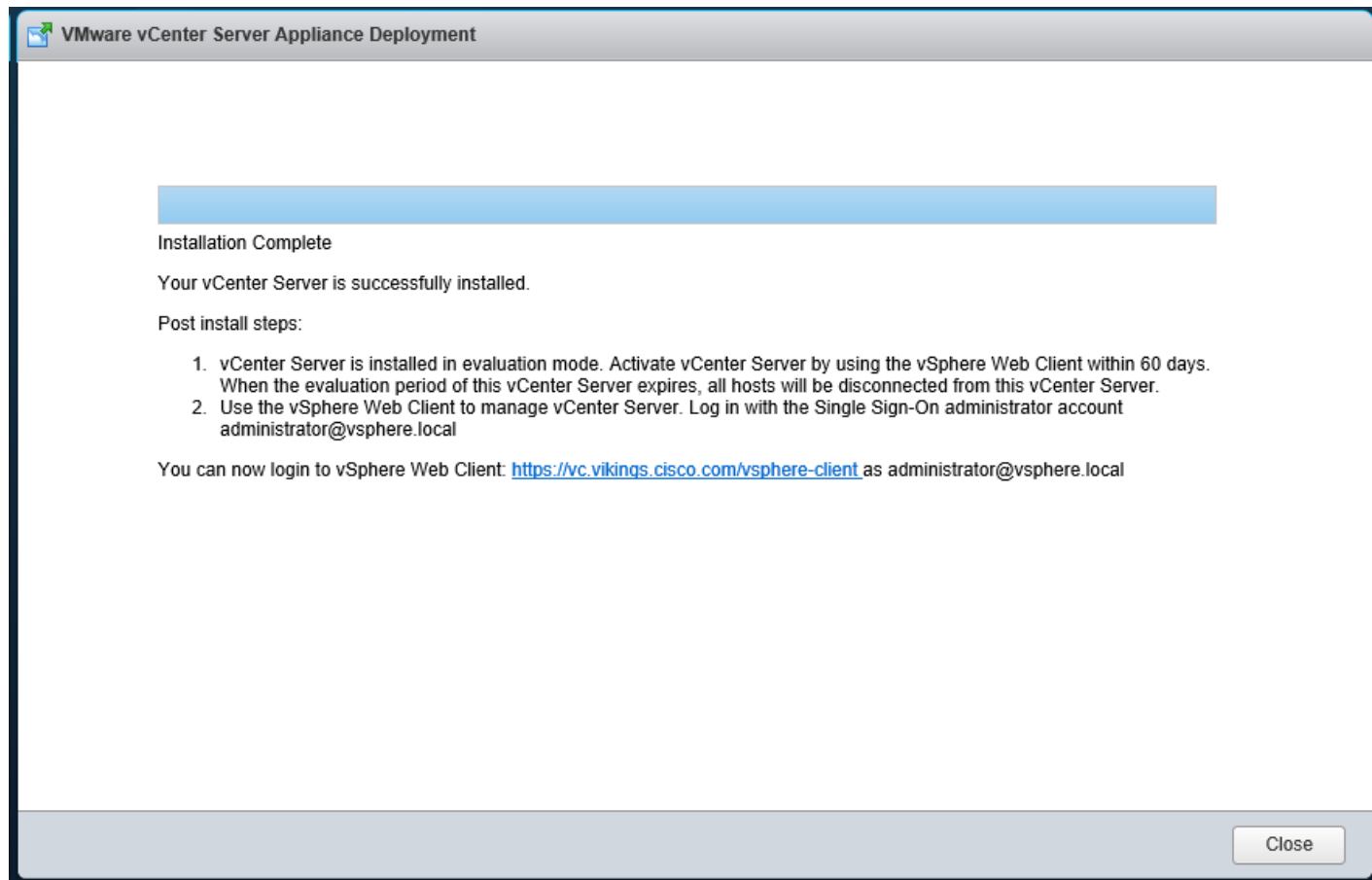
| | |
|--|--|
| IP address family: | IPv4 |
| Network type: | static |
| Network address: | 10.1.156.100 |
| System name [FQDN or IP address]: | vc.vikings.cisco.com |
| Subnet mask: | 255.255.255.0 |
| Network gateway: | 10.1.156.1 |
| Network DNS Servers (separated by commas) | 10.1.156.9 |
| Configure time sync: | <input type="radio"/> Synchronize appliance time with ESXi host <input checked="" type="radio"/> Use NTP servers (Separated by commas) 10.1.156.4,10.1.156.5 |
| <input checked="" type="checkbox"/> Enable ssh | |

19. Click Next.

20. Indicate whether to join the VMware Customer Experience Improvement Program and click Next.

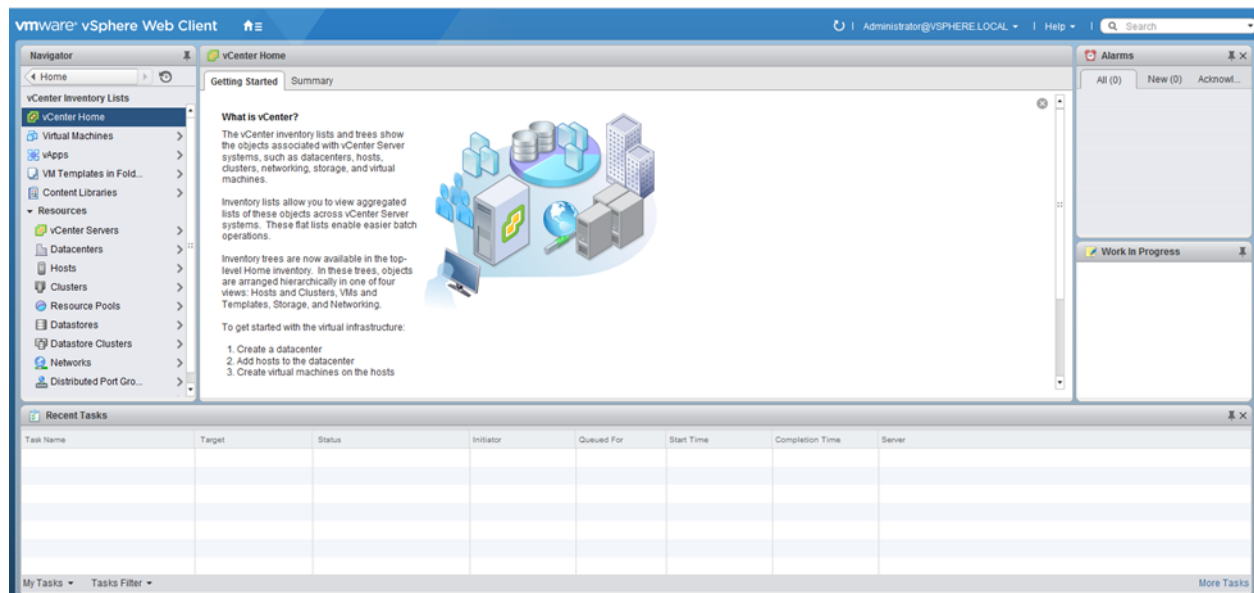
21. Review all values and click Finish to complete the installation.

22. The vCenter appliance installation will take a few minutes to complete.

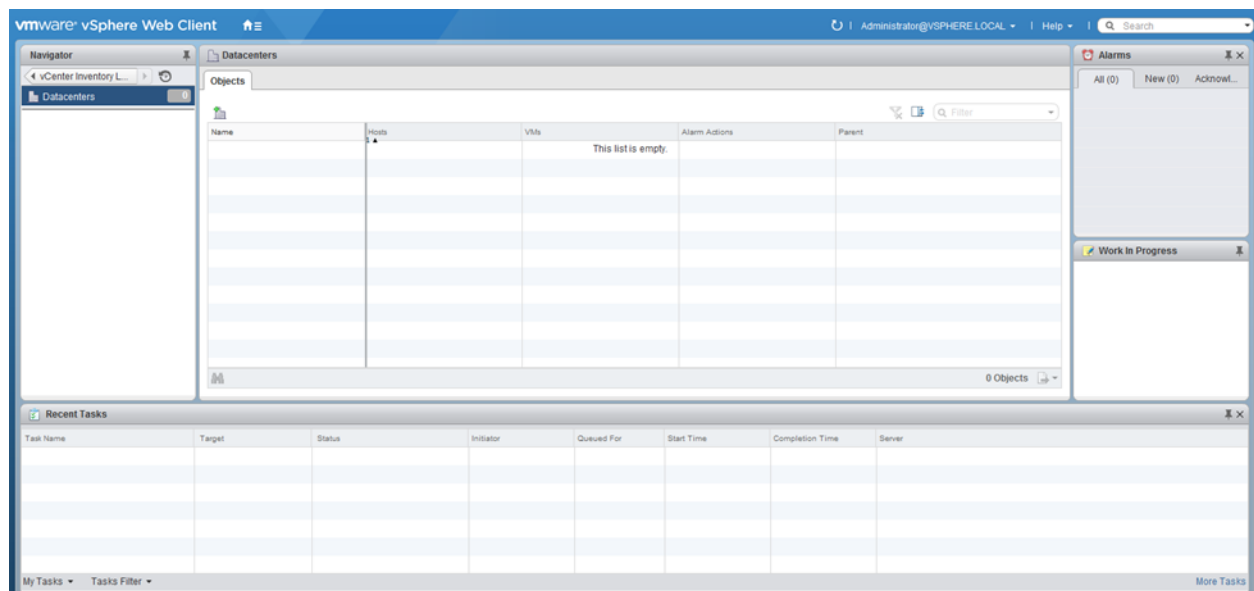


Setting Up VMware vCenter Server

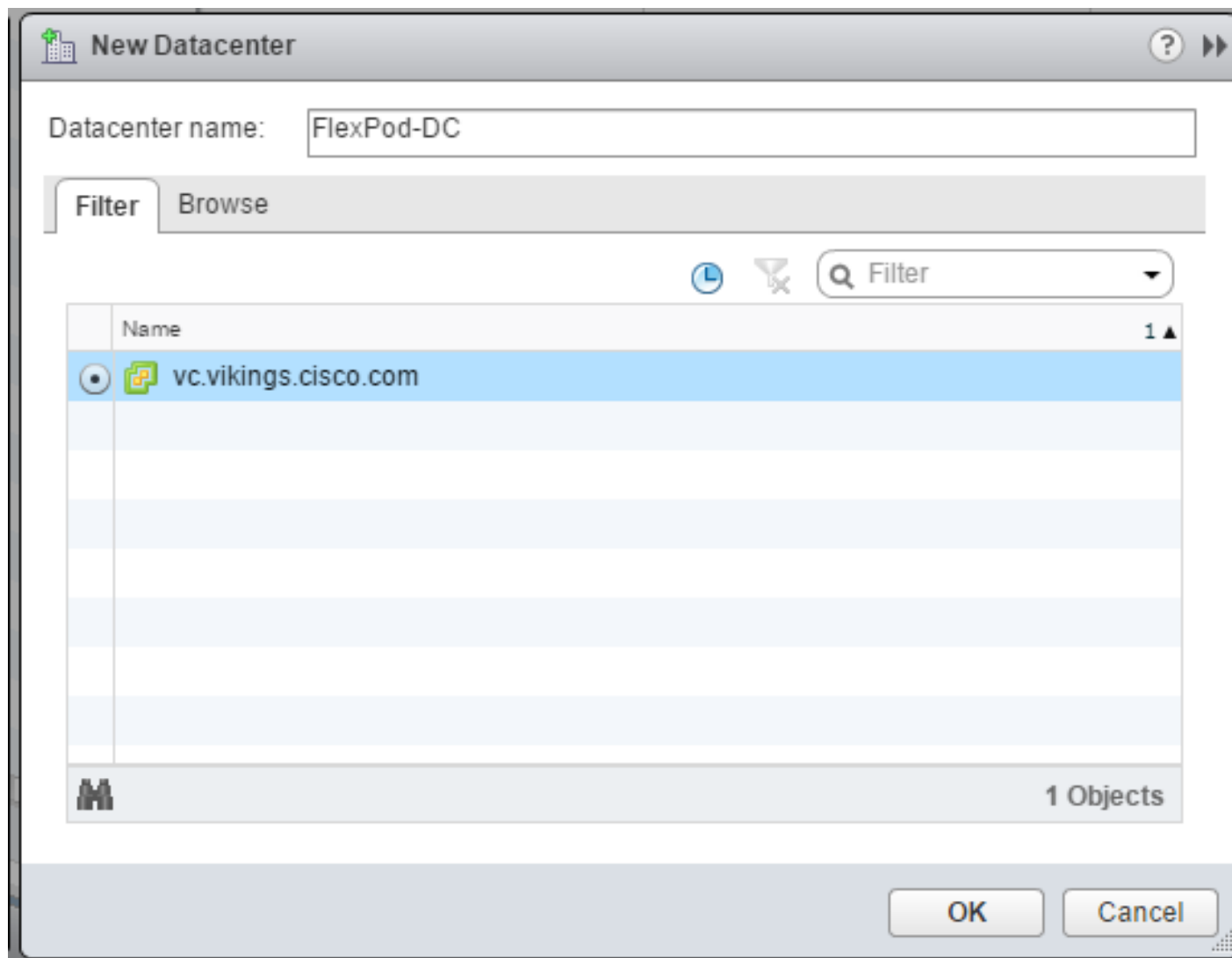
1. Using a web browser, navigate to <https://<vcenter-ip>>.
2. Click Log in to vSphere Web Client.
3. Log in using the Single Sign-On username and password created during the vCenter installation.
4. Navigate to vCenter Inventory Lists in the left pane.



5. Under Resources, click Datacenters in the left plane.



6. To create a Datacenter, click the leftmost icon in the center pane that has a green plus symbol above it.
7. Type "FlexPod-DC" in the Datacenter name field.
8. Select the vCenter Name/IP option.
9. Click OK.



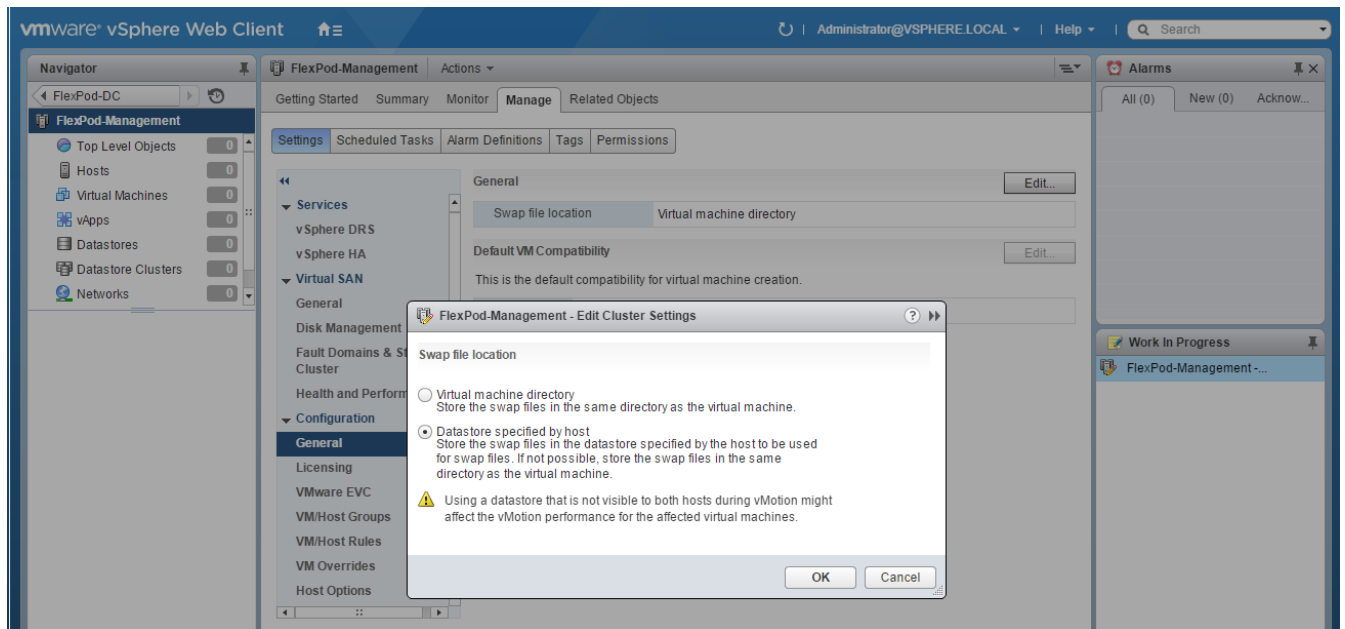
10. Right-click the data center FlexPod-DC in the list in the center pane. Click New Cluster.
11. Name the cluster FlexPod-FIManagement.
12. Check the box to turn on DRS. Leave the default values.
13. Check the box to turn on vSphere HA. Leave the default values.

| | |
|--------------------------|--|
| Name | FlexPod-Management |
| Location | FlexPod-DC |
| DRS | <input checked="" type="checkbox"/> Turn ON |
| Automation Level | Fully automated |
| Migration Threshold | Conservative ——— Aggressive |
| vSphere HA | <input checked="" type="checkbox"/> Turn ON |
| Host Monitoring | <input checked="" type="checkbox"/> Enable host monitoring |
| Admission Control | |
| Admission Control Status | Admission control will prevent powering on VMs that violate availability constraints <input checked="" type="checkbox"/> Enable admission control |
| Policy | Specify the type of the policy that admission control should enforce. <input checked="" type="radio"/> Host failures cluster tolerates: 1 <input type="radio"/> Percentage of cluster resources reserved as failover spare capacity: Reserved failover CPU capacity: 25 % CPU Reserved failover Memory capacity: 25 % Memory |
| VM Monitoring | |
| VM Monitoring Status | Disabled Overrides for individual VMs can be set from the VM Overrides page from Manage Settings area. |
| Monitoring Sensitivity | Low ——— High |
| EVC | Disable |
| Virtual SAN | <input type="checkbox"/> Turn ON |

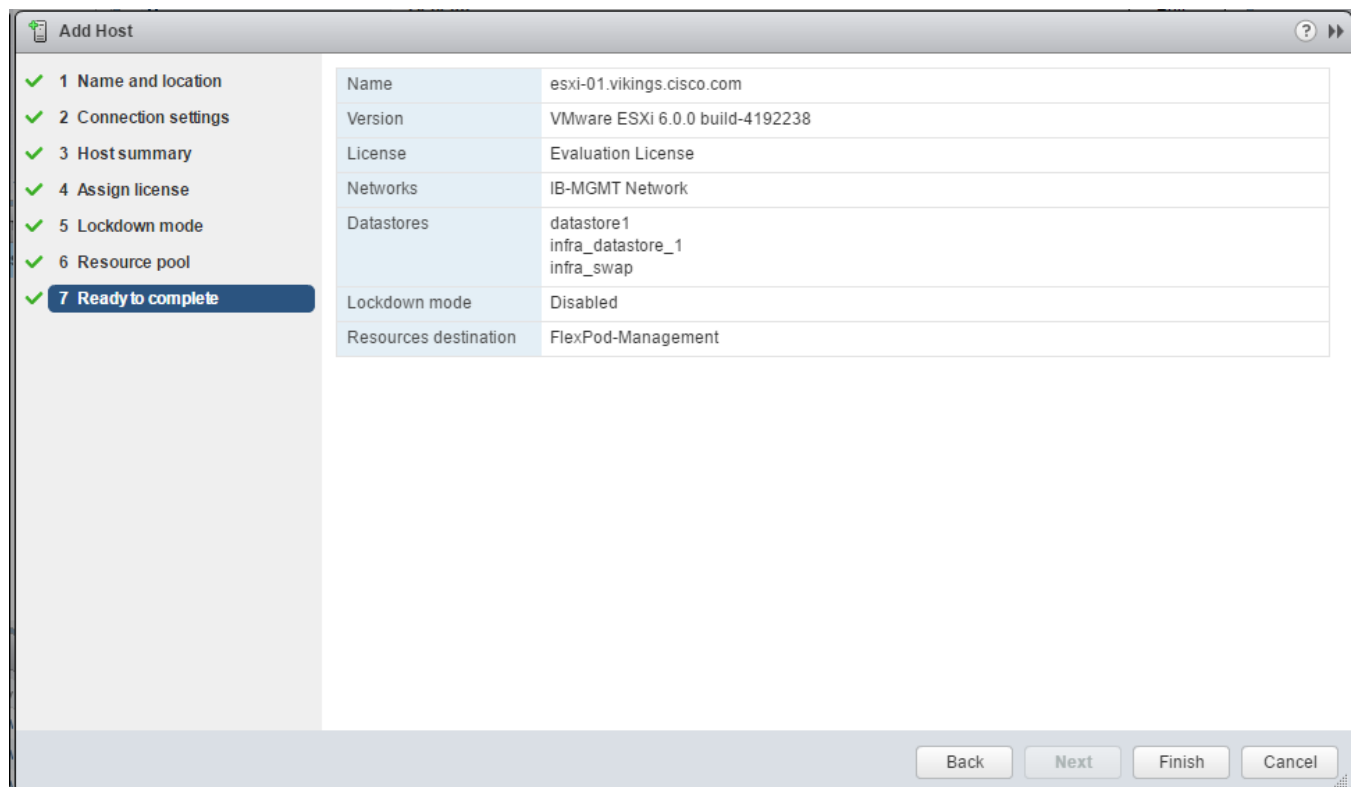
OK Cancel

14. Click OK to create the new cluster.
15. On the left pane, double click the “FlexPod-DC”.
16. Click Clusters.

17. Under the Clusters pane, right click FlexPod-Management and select Settings.
18. Select Configuration > General in the list on the left and select Edit to the right of General.
19. Select Datastore specified by host and click OK.



20. On the left, right-click FlexPod-Management and click Add Host.
21. In the Host field, enter either the IP address or the FQDN name of one of the VMware ESXi hosts. Click Next.
22. Type root as the user name and the root password. Click Next to continue.
23. Click Yes to accept the certificate.
24. Review the host details and click Next to continue.
25. Assign a license or leave in evaluation mode and click Next to continue.
26. Click Next to continue.
27. Click Next to continue.
28. Review the configuration parameters, then click Finish to add the host.



29. Repeat the steps 21 to 29 to add the remaining VMware ESXi hosts to the cluster.



Two VMware ESXi hosts will be added to the cluster.

Add AD User Authentication to vCenter (Optional)

If an AD Infrastructure is set up in this FlexPod environment, you can setup in AD and authenticate from vCenter.

1. In the AD Infrastructure, using the Active Directory Users and Computers tool, setup a Domain Administrator user with a user name such as flexadmin (FlexPod Admin).
2. Connect to <https://<vcenter-ip>>, and select Log in to vSphere Web Client.
3. Log in as Administrator@vsphere.local (or the SSO user set up in vCenter installation) with the corresponding password.
4. In the center pane, select System Configuration under Administration.
5. On the left, select Nodes and under Nodes select the vCenter.
6. In the center pane, select the manage tab, and within the Settings select Active Directory and click Join.
7. Fill in the AD domain name, the Administrator user, and the domain Administrator password. Click OK.

8. On the left, right-click the vCenter and select Reboot.
9. Input a reboot reason and click OK. The reboot will take approximately 10 minutes for full vCenter initialization.
10. Log back into the vCenter Web Client.
11. In the center pane, select System Configuration under Administration.
12. On the left, select Nodes and under Nodes select the vCenter.
13. In the center pane under the Manage tab, select Active Directory. Make sure your Active Directory Domain is listed.
14. Navigate back to the vCenter Home.
15. In the center pane under Administration, select Roles.
16. On the left under Single Sign-On, select Configuration.
17. In the center pane, select the Identity Sources tab.
18. Click the green + sign to add an Identity Source.
19. Select the Active Directory (Integrated Windows Authentication) Identity source type.
20. Your AD domain name should be filled in. Leave Use machine account selected and click OK.
21. Your AD domain should now appear in the Identity Sources list.
22. On the left, under Single Sign-On, select Users and Groups.
23. In the center pane, select your AD domain for the Domain.
24. Make sure the FlexPod Admin user setup in step 1 appears in the list.
25. On the left under Administration, select Global Permissions.
26. Select the Manage tab, and click the green + sign to add a User or Group.
27. In the Global Permission Root - Add Permission window, click Add.
28. In the Select Users/Groups window, select your AD Domain.
29. Under Users and Groups, select either the FlexPod Admin user or the Domain Admins group.



The FlexPod Admin user was created in the Domain Admins group. The selection here depends on whether the FlexPod Admin user will be the only user used in this FlexPod or you would like to add other users later. By selecting the Domain Admins group, any user placed in that group in the AD domain will be able to login to vCenter as an Administrator.

30. Click Add, then click Check names to verify correctness of the names. Click OK to acknowledge the correctness of the names.
31. Click OK to add the selected User or Group.
32. Verify the added User or Group is listed under Users and Groups and the Administrator role is assigned.
33. Click OK.
34. Log out and log back into the vCenter Web Client as the FlexPod Admin user. You will need to add the domain name to the user, for example, flexadmin@domain.

FlexPod VMware vSphere Distributed Switch (vDS)

This section provides detailed procedures for installing the VMware vDS on the FlexPod ESXi Management Hosts. An alternate procedure for installing the Cisco Nexus 1000V instead of the VMware vDS is covered in the Appendix.

In the Cisco UCS setup section of this document three sets of vNICs (Infra-A and B, vMotion-A and B, and DVS-A and B) were setup. The vmnic ports associated with the DVS-A and B vNICs will be migrated to VMware vDS in this procedure. The critical infrastructure VLAN interfaces will stay on vSwitch0 and vMotion will stay on the vMotion-vSwitch. The tenant or application interfaces (currently only the VM-Traffic VLAN interface) will be placed on the vDS.

A VM-Traffic VLAN port group will be added to the vDS. Any additional VLAN-based port groups added to the vDS would need to have the corresponding VLANs added to the Cisco UCS LAN cloud, to the Cisco UCS DVS-A and B vNIC templates, and to the Nexus 9K switches and Cisco UCS vPC and peer-link interfaces on the switches.

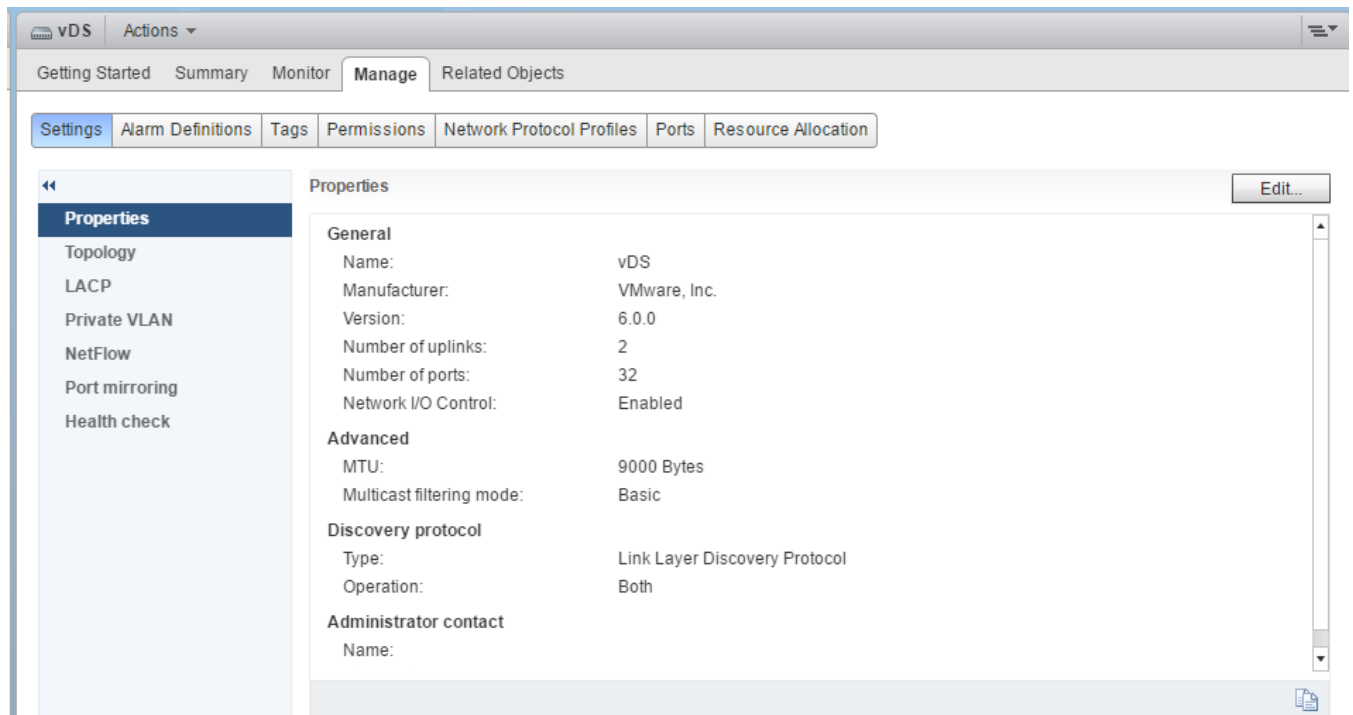
Configure the VMware vDS in vCenter

VMware vSphere Web Client

To configure the vDS, complete the following steps:

1. After logging into the VMware vSphere Web Client, select Networking under the Home tab.
2. Right the FlexPod-DC datacenter and select Distributed Switch > New Distributed Switch.
3. Give the Distributed Switch a descriptive name and click Next.
4. Make sure Distributed switch: 6.0.0 is selected and click Next.
5. Change the Number of uplinks to 2 and enter VM-Traffic Network for the Port group name. Click Next.
6. Review the information and click Finish to complete creating the vDS.
7. On the left, expand the FlexPod-DC datacenter and the newly created vDS. Select the newly created vDS.

8. Select the VM-Traffic Network port group. In the center pane, select the Manage tab, then the Settings tab. The Edit button can be used to change the number of ports in the port group to a number larger than the default of 8. All of the other properties of the port group can also be changed under Edit.
9. Select the vDS on the left. Click Edit on the right.
10. On the left in the Edit Settings window, select Advanced.
11. Change the MTU to 9000. The Discovery Protocol can optionally be changed to Link Layer Discovery Protocol and the Operation to Both. Click OK.

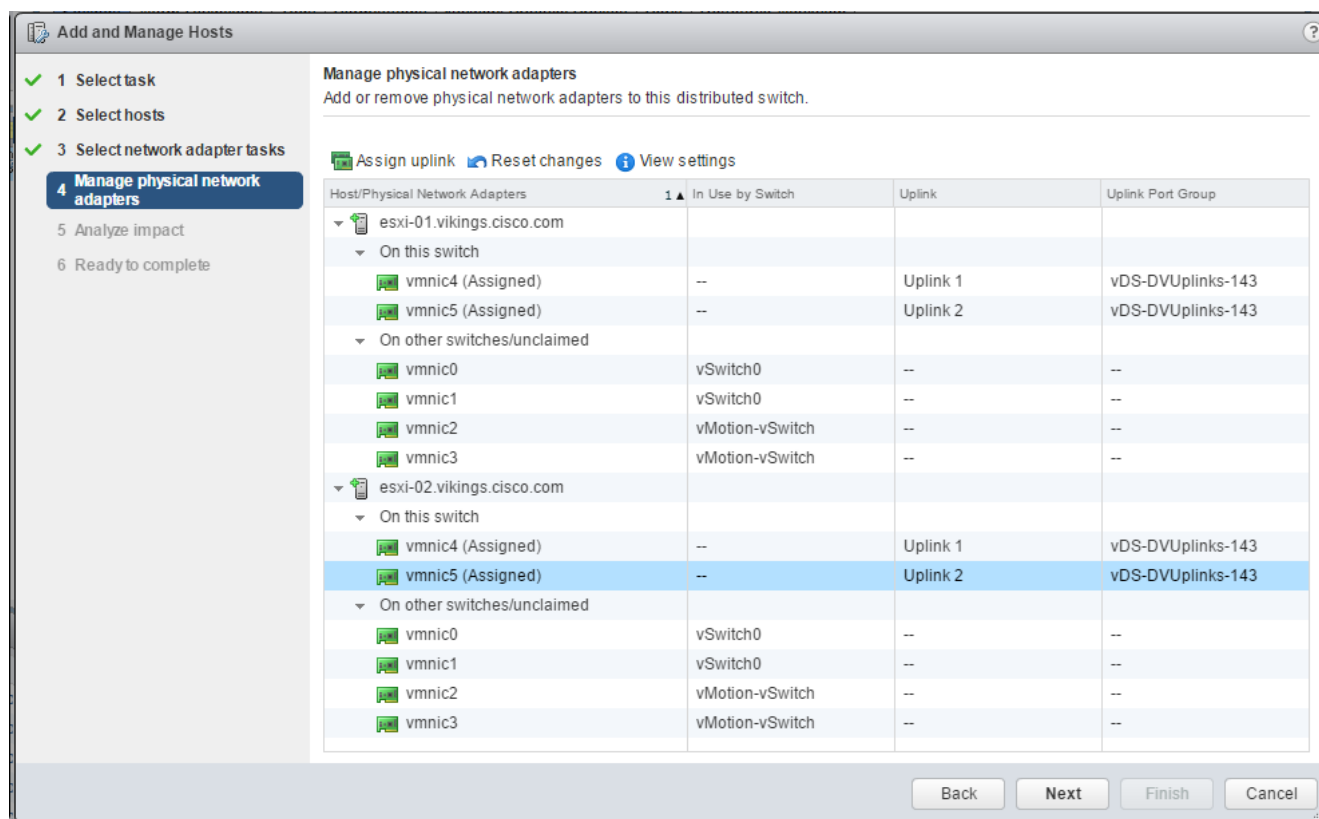


12. On the left, right-click the vDS and select Add and Manage Hosts.
13. Make sure Add hosts is selected and click Next.
14. Click the green + sign to add hosts. Select the two FlexPod Management hosts and click OK. Click Next.
15. Make sure just Manage physical adapters is selected and click Next.



In this case, we are not migrating any VMkernel adapters to the vDS.

16. Select vmnic4 on the first host and click Assign uplink. Select Uplink 1 and click OK. Repeat this process to assign vmnic4 and vmnic5 from both hosts to the vDS.



17. Click Next.

18. Click Next.

19. Click Finish to complete adding the two ESXi hosts to the vDS.

FlexPod Management Tools Setup

Cisco UCS Performance Manager

This section describes the deployment and initial configuration of Cisco UCS Performance Manager within a FlexPod.



For full requirements and installation options, download and review the [Cisco UCS Performance Manager Installation Guide, Release 2.0.2](#).

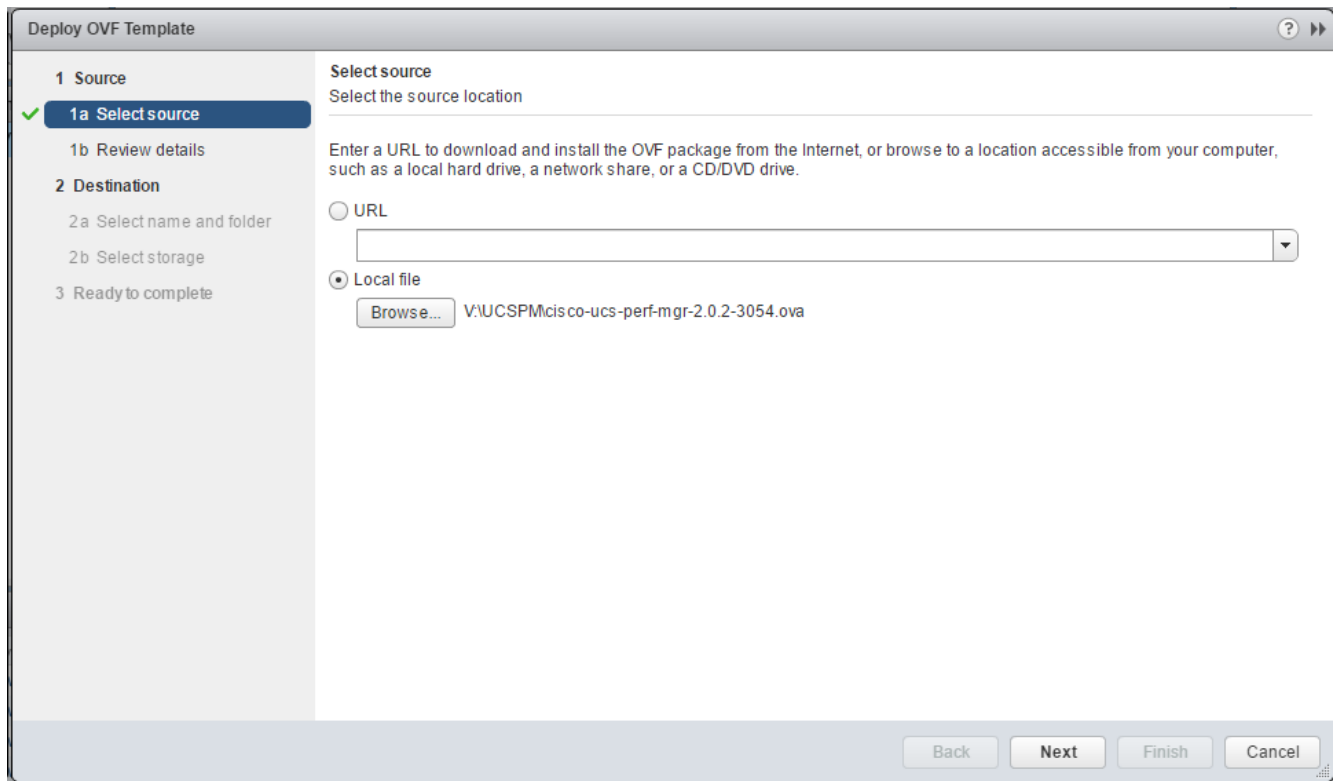
Cisco UCS Performance Manager OVA Deployment

1. Download the Cisco UCS Performance Manager 2.0.2 OVA file from the [Cisco UCS Performance Manager Download Site](#) to your workstation.
2. Use the VMware vSphere Web Client to log in to vCenter as the FlexPod Administrator user and then select Hosts and Clusters from the Home view.

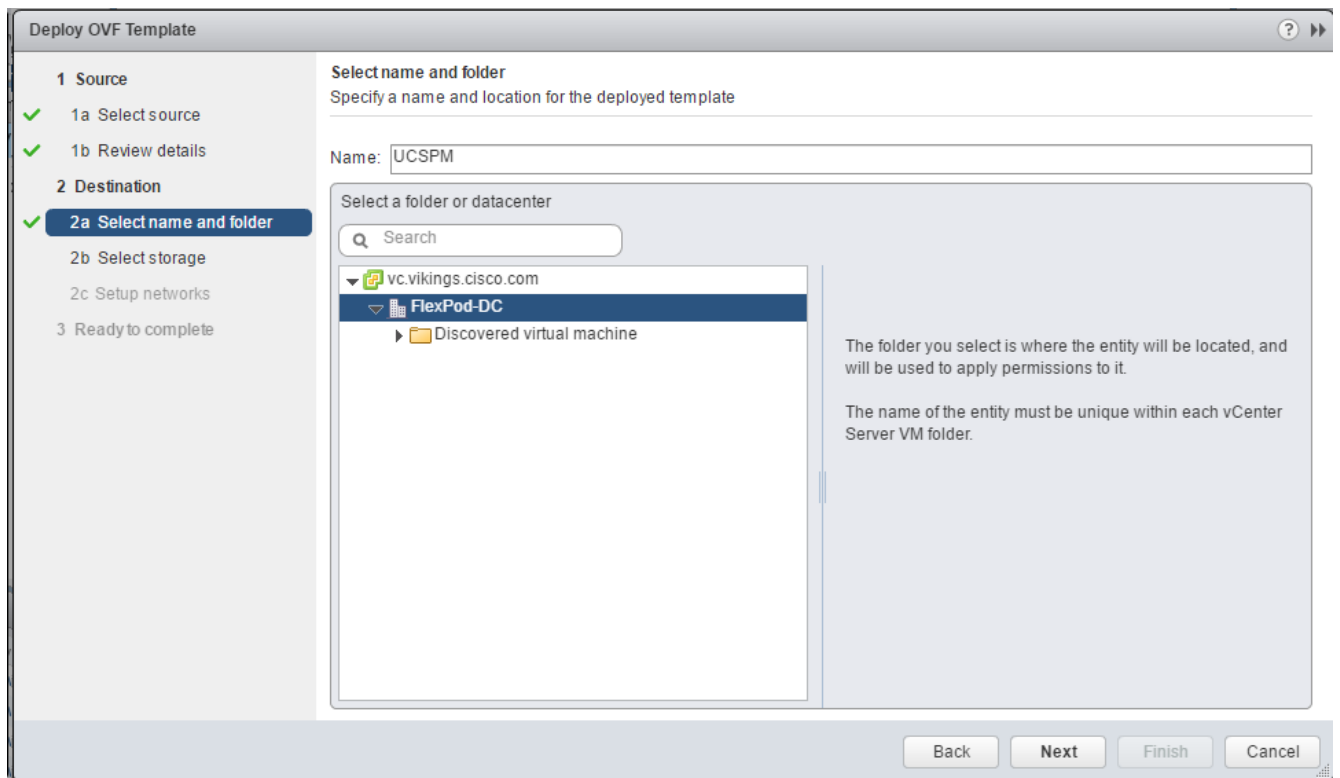


The standard vSphere Client can be used for installation, but instructions will vary slightly.

3. Right-click the FlexPod-Management Cluster to deploy to, and select Deploy OVF Template from the pulldown options.
4. In the Select source panel, specify the path of the Cisco UCS Performance Manager package as a Local file and browse to find its location, and then click Next.



5. Click Next to continue past the Review details pane.
6. In the Select name and folder pane, name the virtual machine, pick the FlexPod-DC data center to deploy to and alternately a folder within that datacenter.



7. Click Next.
8. Specify infra_datastore_1 and the Thin Provision virtual disk format.

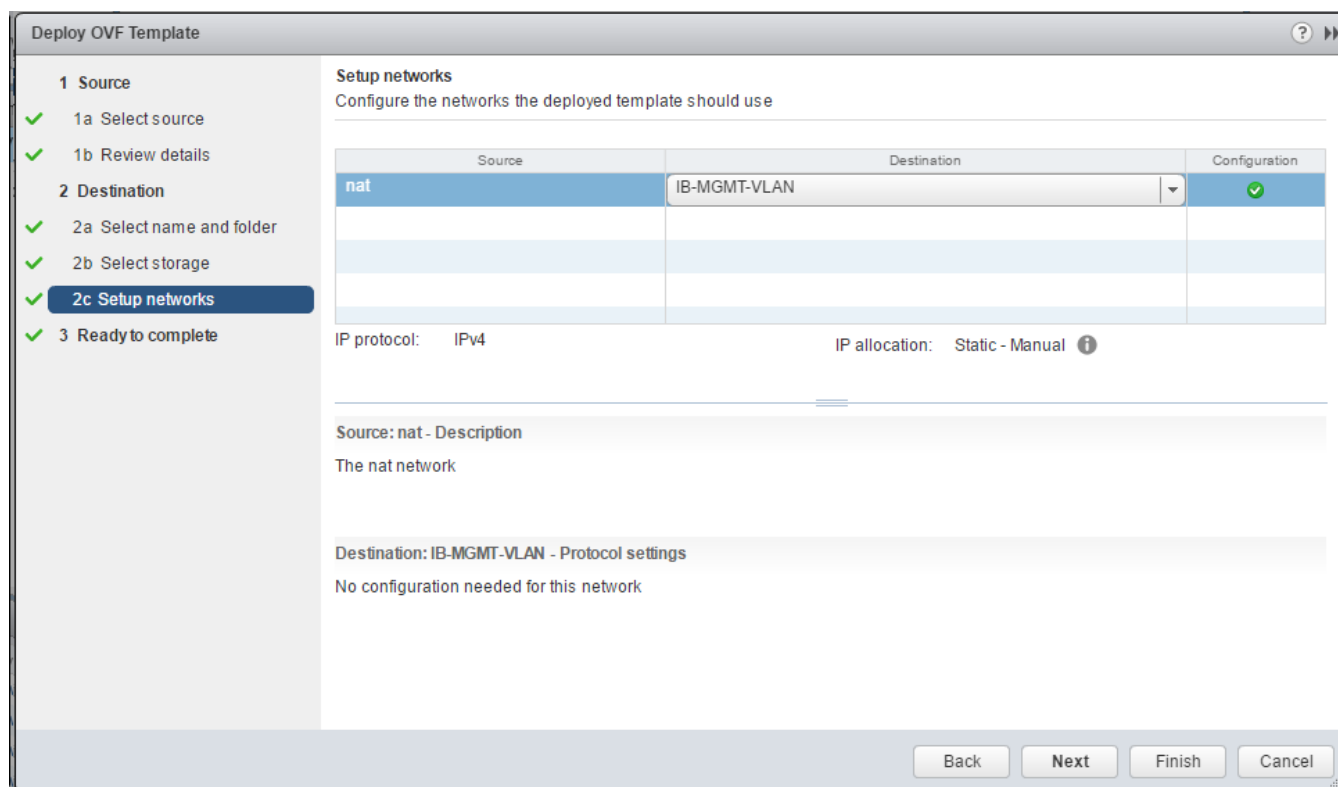
The screenshot shows the 'Deploy OVF Template' wizard. The left sidebar indicates the current step is '2b Select storage'. The main area is titled 'Select storage' and contains the following elements:

- Section: **Select storage**
Select location to store the files for the deployed template
- Field: Select virtual disk format: **Thin Provision** (dropdown menu)
- Field: VM Storage Policy: **Datastore Default** (dropdown menu)
- Text: The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.
- Table of available datastores:

| Name | Capacity | Provisioned | Free | Type | Storage DRS |
|-------------------|-----------|-------------|-----------|--------|-------------|
| infra_datastore_1 | 500.00 GB | 268.97 GB | 415.32 GB | NFS v3 | |
| infra_swap | 100.00 GB | 10.95 MB | 99.99 GB | NFS v3 | |
| datastore1 | 7.50 GB | 860.00 MB | 6.66 GB | VMFS | |
| datastore1 (1) | 7.50 GB | 860.00 MB | 6.66 GB | VMFS | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

At the bottom of the wizard, there are four buttons: **Back**, **Next**, **Finish**, and **Cancel**.

9. Click Next.
10. Specify the IB-MGMT-VLAN port group within the Setup Networks pane.



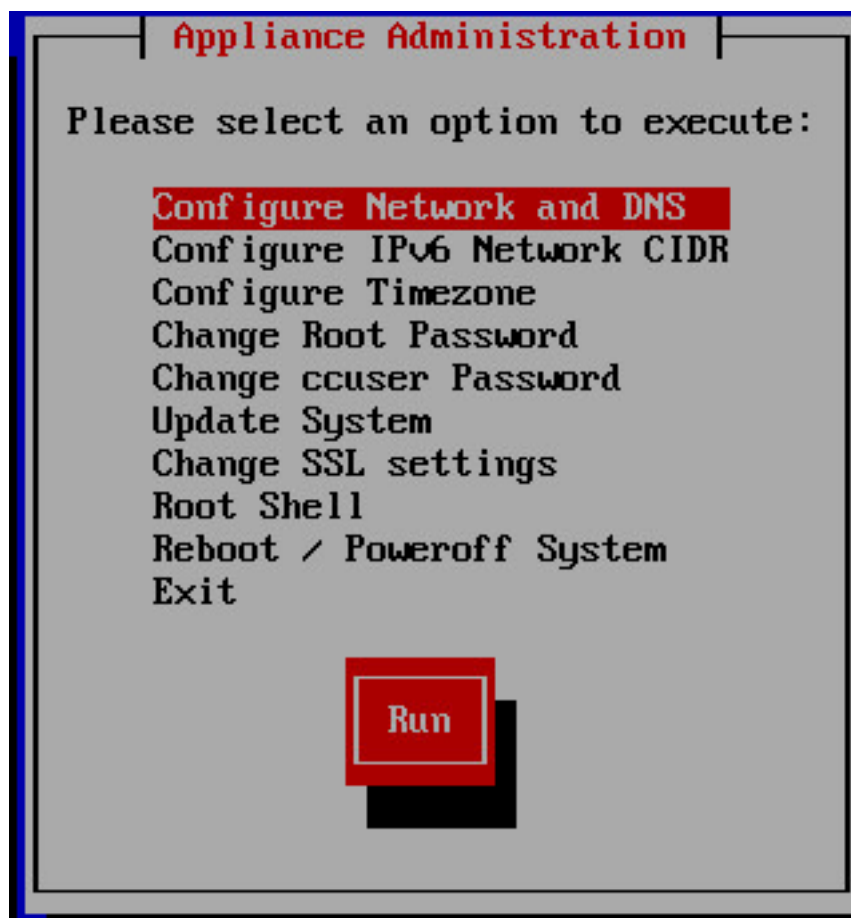
11. Click Next.
12. Review the options in the Ready to complete pane, and make sure that “Power on after deployment” is not selected.
13. Click Finish to deploy the appliance from the Deploy OVF Template wizard.
14. When the appliance has finished deploying, select the VM from within the Hosts and Clusters section of the vSphere Web Client and under the Summary tab select Launch Remote Console.
15. Click the green arrow icon to power on the VM.

Cisco UCS Performance Manager Initial Configuration

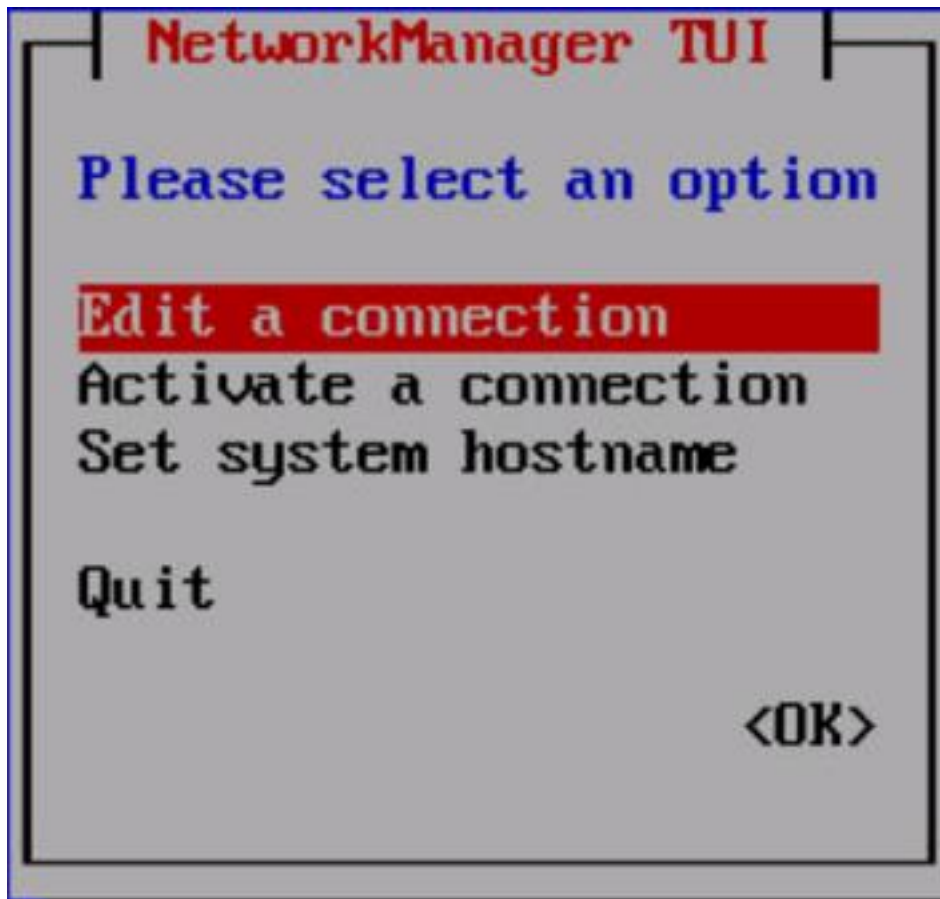
1. Open up the Console of the newly provisioned UCS Performance Manager VM from the vSphere web client.
2. From the UCS Performance Manager VM Remote Console, login to the root account with the password “ucspm”
3. Set a new root password and a password for the account “ccuser” when prompted.
4. Within the following screen, leave Master selected to configure the appliance as the Control Center master host.



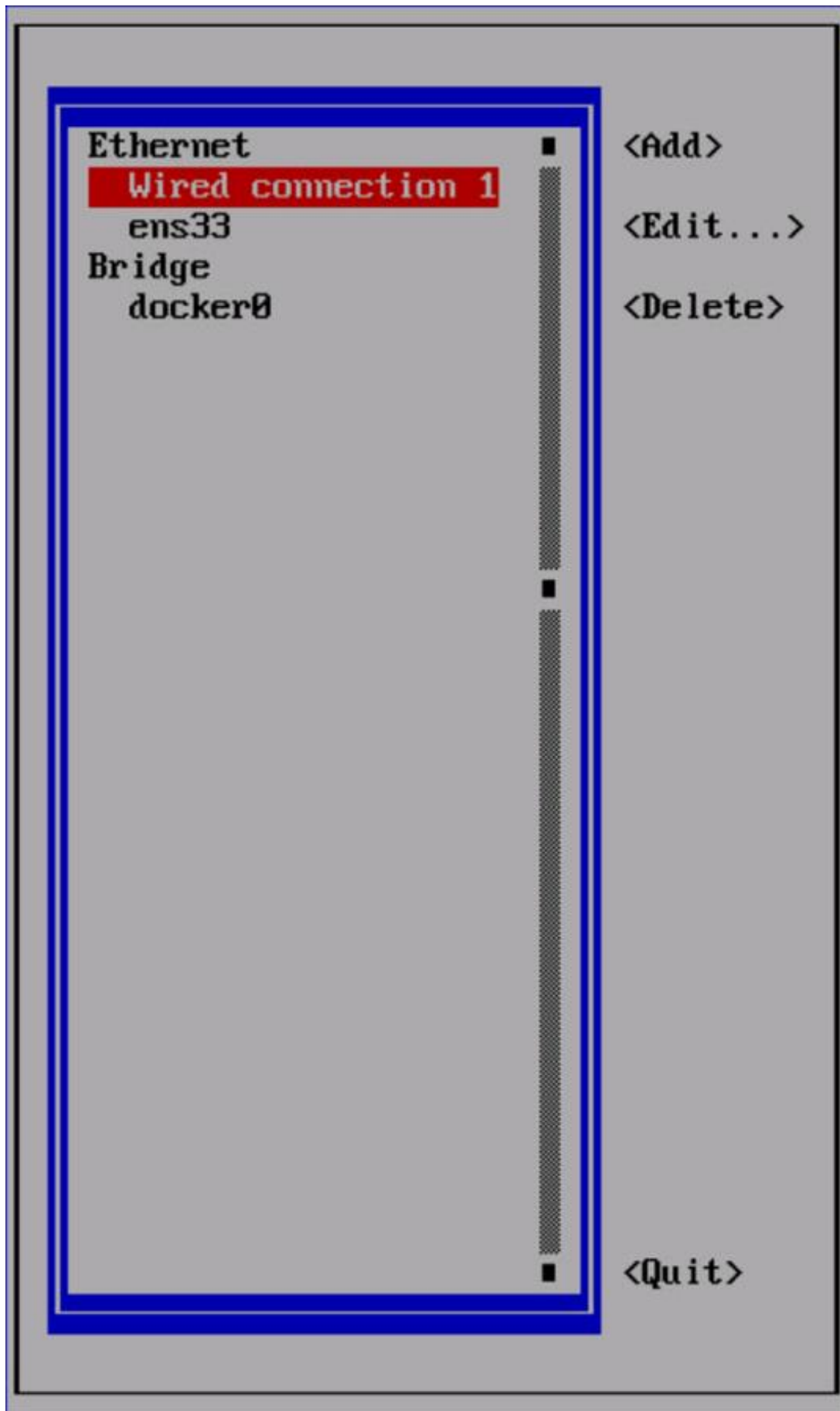
5. Press Enter to initiate a reboot and log back in with the root account after the appliance is back up.
6. Press Return from the Appliance Administration screen with Configure Network and DNS selected.



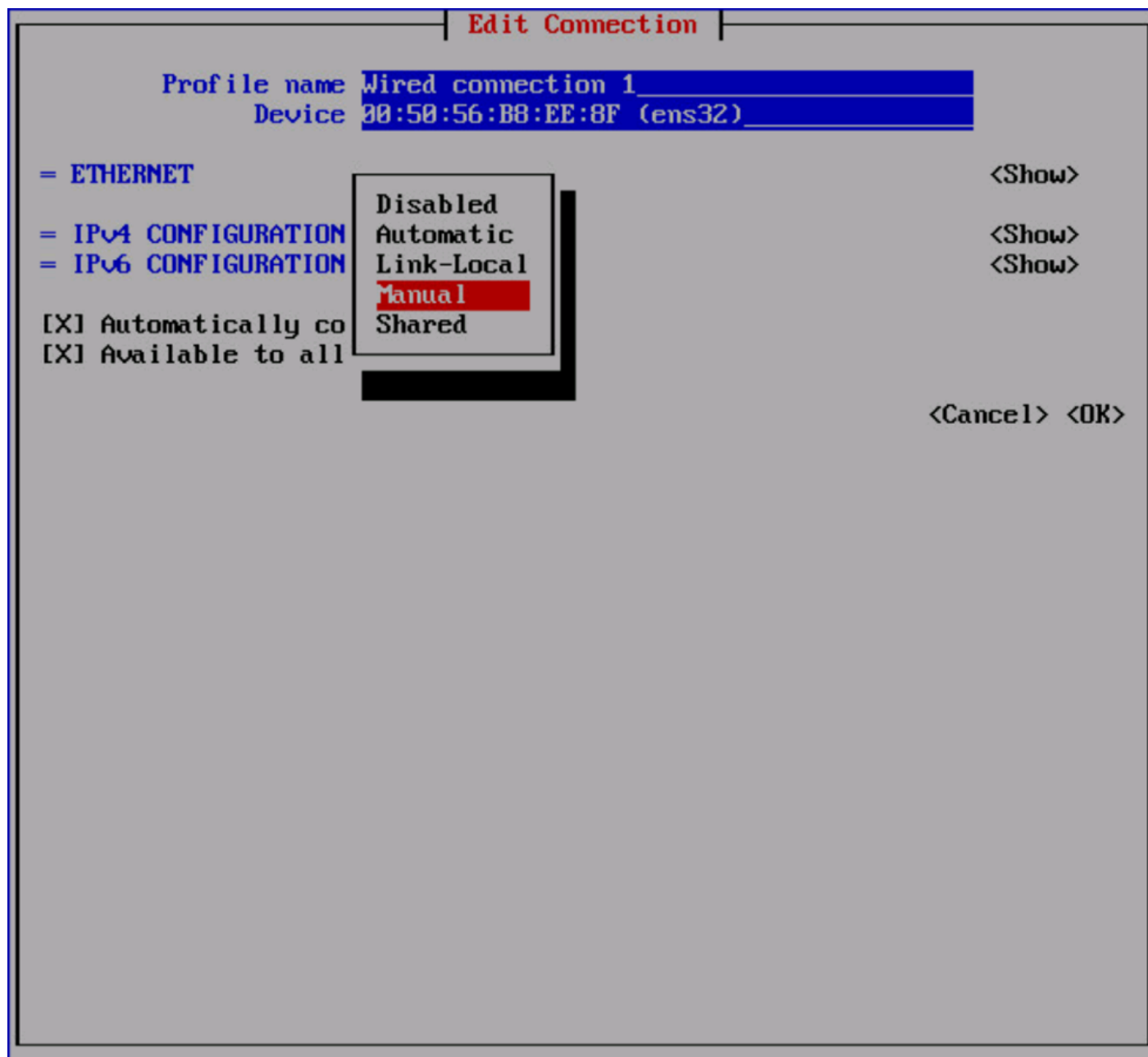
7. Leave Edit a connection selected with the NetworkManager TUI screen and press Enter.



8. Select Wired connection 1, and press return to edit.



9. Arrow down to the IPV4 CONFIGURATION option and hit enter to change the option from Automatic to Manual.



10. Right arrow over to <Show> next to the IPV4 CONFIGURATION and press return to bring up the options.

Edit Connection

Profile name **Wired connection 1**

Device **00:50:56:B8:EE:8F (ens32)**

= ETHERNET <Show>

■ IPv4 CONFIGURATION **<Manual>** <Hide>

Addresses **10.1.156.18/24** <Remove>
<Add...>

Gateway **10.1.156.1**

DNS servers **192.168.156.9** <Remove>
<Add...>

Search domains **vikings.cisco.com** <Remove>
<Add...>

Routing (No custom routes) <Edit...>

Never use this network for default route

Require IPv4 addressing for this connection

= IPv6 CONFIGURATION **<Ignore>** <Show>

Automatically connect

Available to all users

<Cancel> <OK>

11. Add the assigned IP address/netmask, Gateway, DNS server(s), and any Search Domains.

12. Optionally change the IPV6 CONFIGURATION option from Automatic to Ignore.

13. Arrow down until <OK> is highlighted and press Return.

14. Hit the right arrow within the interface selection menu you are returned to, arrow further down until <Quit> is selected and hit return. Press Return for the confirmation message.

15. Hit return to once again select Configure Network and DNS and press Return.

16. Arrow down until Set system hostname is selected and press Return.

17. Enter cc-master for the Hostname and press Return.
18. Arrow down until Configure Timezone is highlighted and press Return. Press Return for the confirmation message.
19. Use the arrow key to highlight the appropriate timezone, use the tab key to highlight Select, and press Return.
20. Arrow down to have Reboot / Poweroff System highlighted and press Return to initiate a reboot.
21. Make sure Reboot is highlighted and use the tab key to highlight OK. Press Return to reboot the virtual machine. Press Return for the confirmation message.

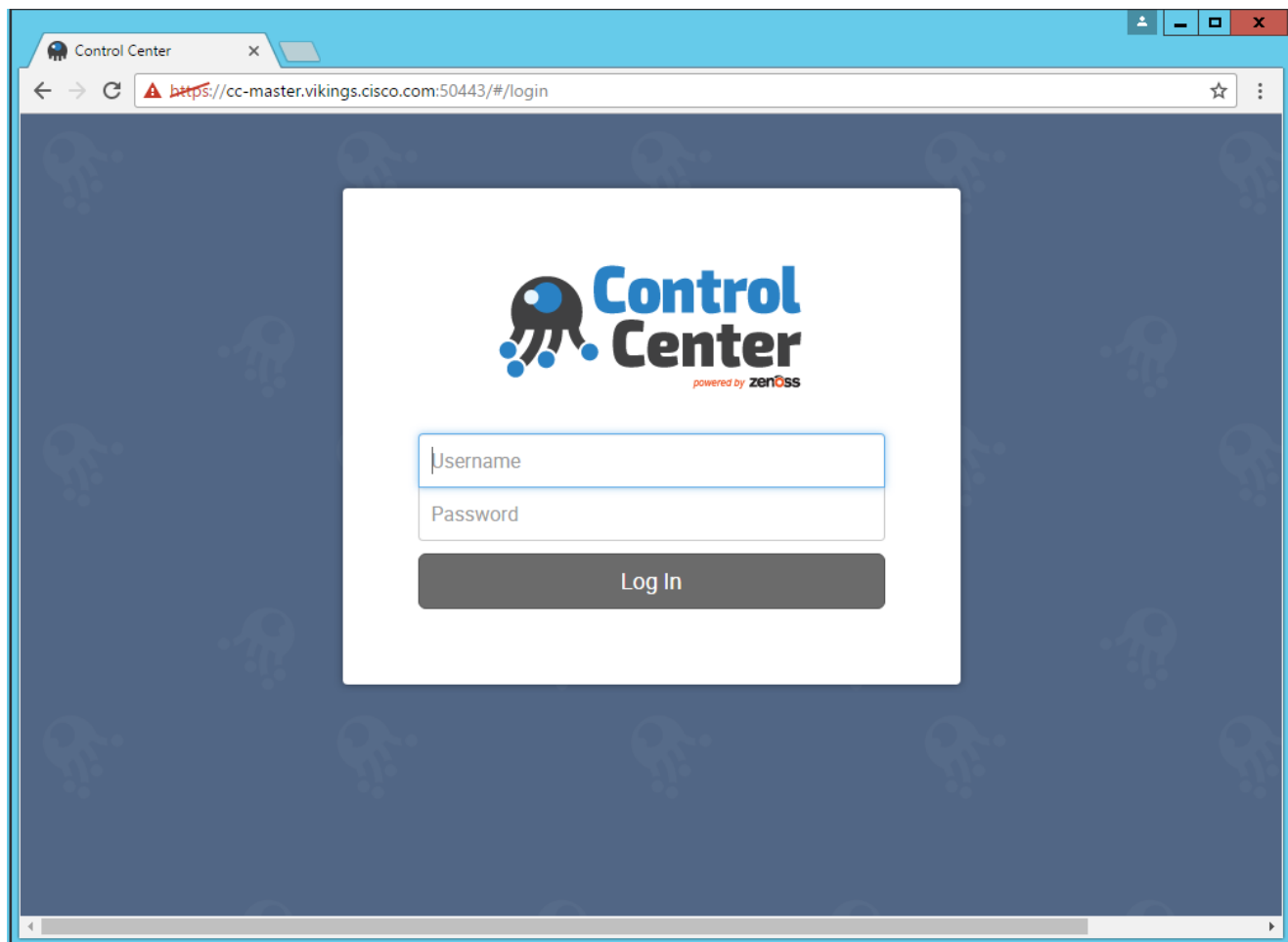
Cisco UCS Performance Manager Deployment

The base IP or hostname of the UCS Performance Manager master host will allow a connection the Control Center that the UCS Performance Manager virtual host is provisioned from.

In our example, *ControlCenter* was registered in our DNS as cc-master.vikings.cisco.com, and was accessible as <http://cc-master.vikings.cisco.com/> or through the IP assigned to it. The UCS Performance Manager needs to resolve in DNS as a CNAME alias or local /etc/hosts entry from the browsing system as ucspm.*ControlCenter* which was “ucspm.cc-master.vikings.cisco.com” in our example.

To deploy the Cisco UCS Performance Manager, complete the following steps:

1. Login to the Control Center page with the ccuser account, confirm any Security Exceptions identified when connecting.



2. The initial login will bring up a Deployment Wizard to provision the UCS Performance Manager virtual host. If this does not come up, it can be initiated by selecting the +Application button in the mid to upper right of the screen.
3. Enter the Host and port values (ucspm.cc-master.vikings.cisco.com on port 4979 in our example), select default for the Resource Pool ID, and leave the RAM Limit blank.

Deployment Wizard

Step 1
Add Host

Step 2
Select Applications

Step 3
Select Resource Pool

Step 4
Deploy Applications

Add Host

Host:

Port:

Resource Pool ID:

RAM Limit:

4. Click Next.
5. Select ucspm (v2.0.2) as the application to install.
6. Click Next.
7. Select default as the resource pool.

The screenshot shows the 'Deployment Wizard' interface. On the left, a vertical sidebar contains four steps: Step 1 (Add Host), Step 2 (Select Applications), Step 3 (Select Resource Pool), and Step 4 (Deploy Applications). Step 3 is currently selected and highlighted in blue. The main area of the wizard displays the text 'Select the resource pool to install to:' above a table. The table has four columns: 'Resource Pool', 'Description', 'Memory', and 'CPU Cores'. A single row is visible with the values 'default', 'Default Pool', '0.00 GB', and '0'. At the bottom right of the wizard, there are two buttons: 'Back' and 'Next'.

| Resource Pool | Description | Memory | CPU Cores |
|---------------|--------------|---------|-----------|
| default | Default Pool | 0.00 GB | 0 |

8. Click Next.
9. Click Next to accept the default Resource Pool.
10. Specify a Deployment ID name to provision the application.

11. Click Deploy to provision.

12. In the Actions column of the Applications table, click the Start option of the ucspm (v2.0.2) row.

| Application | Description | Status | Deployment ID | Resource Pool | Public Endpoints | Actions |
|-------------------|-------------------------------|---------|---------------|---------------|--|-------------------|
| Internal Services | Internal Services | Running | Internal | N/A | N/A | N/A |
| ucspm (v2.0.2) | Cisco UCS Performance Manager | Stopped | FlexPod | default | https://ucspm.cc-master.vikings.cisco.com:50443 https://cc-master.vikings.cisco.com | Start Stop Delete |

13. A Start Service dialog window will pop-up.

14. Select Start Service and 47 Children.

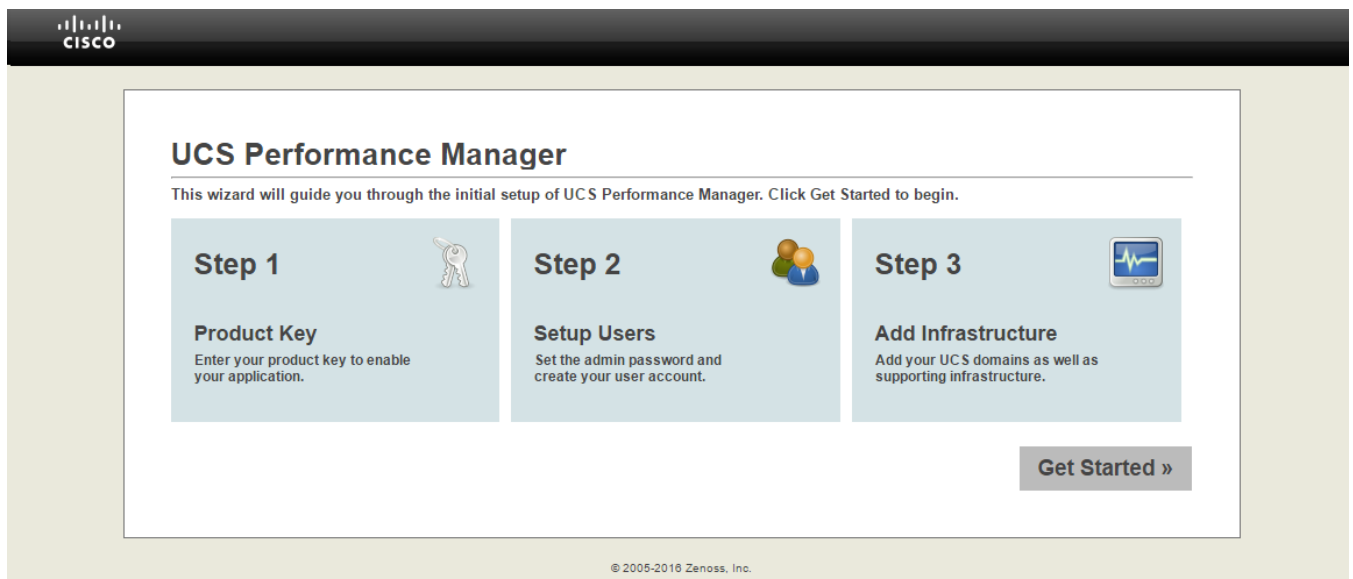
15. In the Application column of the Applications table, click ucspm in the ucspm row.

16. Wait until the ucspm (v2.0.2) application shows a blue checkmark icon under Status. Typically, services take 4-5 minutes to start. When no application shows a red exclamation point icon, Cisco UCS Performance Manager is running.

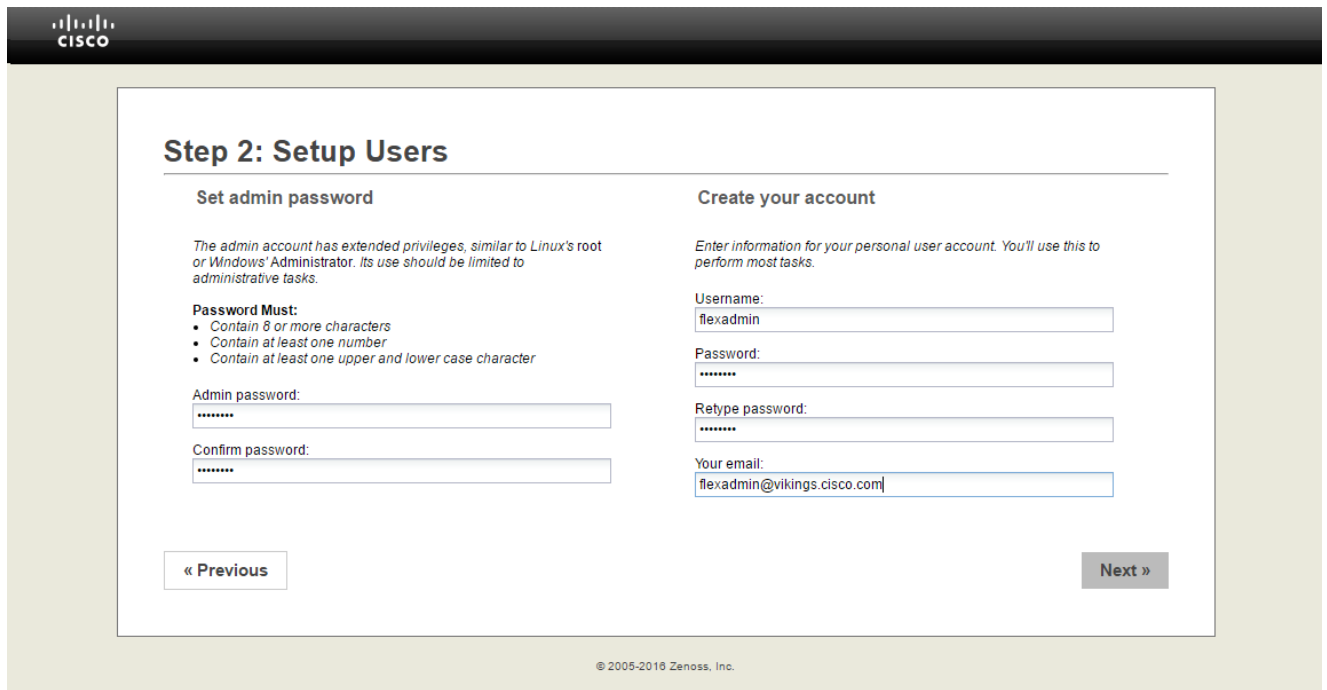
Cisco UCS Performance Manager Configuration of FlexPod Infrastructure

To configure the FlexPod infrastructure using the Cisco UCS Performance Manager, complete the following steps:

1. Using another web browser session, connect to the Cisco UCS Performance Manager virtual host using the DNS CNAME or local entry configured within the host the browser is running from (<https://ucspm.cc-master.vikings.cisco.com/>).
2. Scroll down to the bottom of the licensing screen that first appears, select the “Click this box to verify you agree to the License.” in the bottom left, and click Accept License in the bottom right of the page.



3. Click the “Get Started” option in the initial screen.
4. Click Add License File in the following screen if you are adding one, or click Next in the Licensing screen, if you are going to run with the 30 day trial.
5. Specify an admin password and create a local account on the following screen.

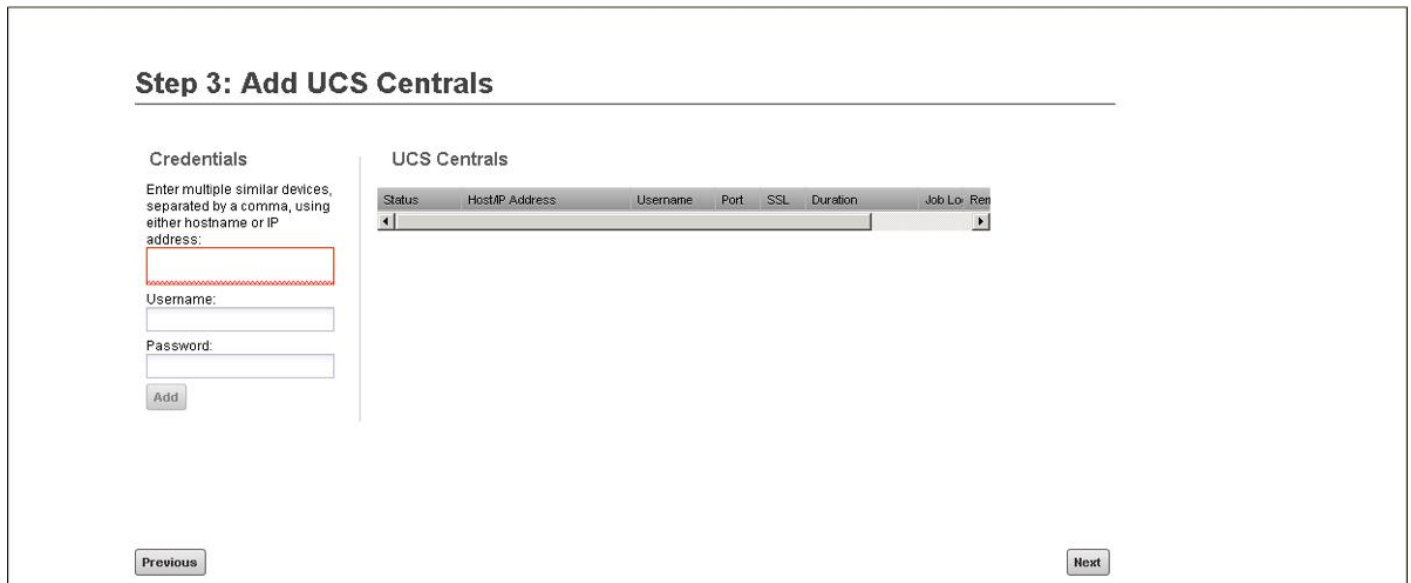


6. Click Next.



Administrator and admin accounts were used as the access accounts in this section. In a production environment it may be more appropriate to use dedicated read only accounts.

7. Add a UCS Central IP, administrative account, and password if you have one independently deployed in your environment (UCS Central is not covered in this document.)



8. Click Next.

9. Add in the UCS Fabric Interconnect(s) virtual IPs for UCS Domains to be monitored in your environment.

Step 4: Add UCS Domains

Credentials

Enter multiple similar devices, separated by a comma, using either hostname or IP address:

d04-6248.vikings.cisco.com,d04-6332.vikings.cisco.com

Username:
admin

Password:

Add

« Previous

Next »

Domains

| Status | Host/IP Address | Username | Port | SSL | Duration |
|---------|-----------------------------|----------|------|------|----------|
| Success | d04-6248.vikings.cisco.c... | admin | 443 | true | 18 seco |
| Success | d04-6332.vikings.cisco.c... | admin | 443 | true | 24 seco |

© 2005-2016 Zenoss, Inc.

10. Click Add, wait for all domains to show a Status of Success, then click Next.
11. Select Network from the Category column to add in the Nexus Switches to be monitored.
12. If the Cisco Nexus 1000V is used, select Cisco Nexus 1000V (SNMP + Netconf). Enter the Cisco Nexus 1000V hostname or IP address, the appropriate SNMP read-only community string, and the admin user id and password. Click Add.



An SNMP read-only community, for example flexpod, can be added to the Nexus 1000V by entering the following command from config terminal: `snmp-server community flexpod ro`. Remember to save the configuration.

13. Select Cisco Nexus 9000 and enter the IPs or hostnames and credentials for access.



The command “feature nxapi” must be entered into each Nexus 9K switch in order for UCSPM to connect to it.

14. Click Add.
15. Select Cisco MDS 9000 (SNMP). Enter the Cisco MDS 9148s hostnames or IP addresses and the appropriate SNMP read-only community string. Click Add.



An SNMP read-only community, for example flexpod, can be added to the MDS 9148s by entering the following command from config terminal: `snmp-server community flexpod ro`. Remember to save the configuration.

Step 5: Add Infrastructure

| Category | Type | Connection Information |
|---|---|--|
| <input checked="" type="radio"/> Network <input type="radio"/> Storage <input type="radio"/> Server <input type="radio"/> Hypervisor <input type="radio"/> Control Center | Cisco b500 (SNMP) Cisco Nexus 5000 (SNMP + Netconf) Cisco Nexus 7000 (SNMP + Netconf) Cisco Nexus 1000V (SNMP + Netconf) Cisco Nexus 3000 (SNMP + Netconf) Cisco Nexus 9000 (NX-API + Netconf) Cisco VSS (SNMP) Cisco MDS 9000 (SNMP) | Enter multiple similar devices, separated by a comma, using either hostname or IP Address: <input type="text" value="d04-9148s-a.vikings.cisco.com,d04-9148s-b.vikings.cisco.com"/> SNMP Community String: <input type="text" value="flexpod"/> <input type="button" value="Add"/> |

Devices

| Status | Host | Credentials | Type | Duration | Job Log | Remove | Retry |
|---------|---|---------------------|----------------------|------------|----------------------------------|--------|-------|
| Success | vsm.vikings.cisco.com | flexpod_admin.fl... | Cisco Nexus 1000... | 25 seconds | 73d63b51-3c6f... | | |
| Success | n9k-a.vikings.cisco.com | admin | Cisco Nexus 9000 ... | 29 seconds | 6bdc9bad-e754... | | |
| Success | n9k-b.vikings.cisco.com | admin | Cisco Nexus 9000 ... | 25 seconds | aa0f6b46-7ee7... | | |
| Success | d04-9148s-a.vikings.cisco.com | flexpod.flexpod | Cisco MDS 9000 (S... | 26 seconds | 06d22bde-3ef4... | | |
| Success | d04-9148s-b.vikings.cisco.com | flexpod.flexpod | Cisco MDS 9000 (S... | 24 seconds | 5fb26e0a-3900... | | |

« Previous

Next »

16. Click Storage from the Category column to add in the NetApp AFF.
17. Select NetApp C-Mode Filer (ZAPI) and enter the IP and credentials for access.
18. Click the “Use SSL?” checkmark box.
19. Click Add.
20. Click Hypervisor from the Category column to add in the vCenter Server.
21. Select vSphere EndPoint (SOAP) and enter a Device Name, the IP or hostname and credentials for access to vCenter.
22. Click the “Use SSL?” checkmark box.

Step 5: Add Infrastructure

Category

- Network
- Storage
- Server
- Hypervisor
- Control Center

Type

- vSphere EndPoint (SOAP)
- Microsoft Hyper-V (WinRM)

Connection Information

Hostname / IP Address:
vc.vikings.cisco.com

Username:
flexadmin@vikings.cisco.com

Password:

Use SSL?:

Devices

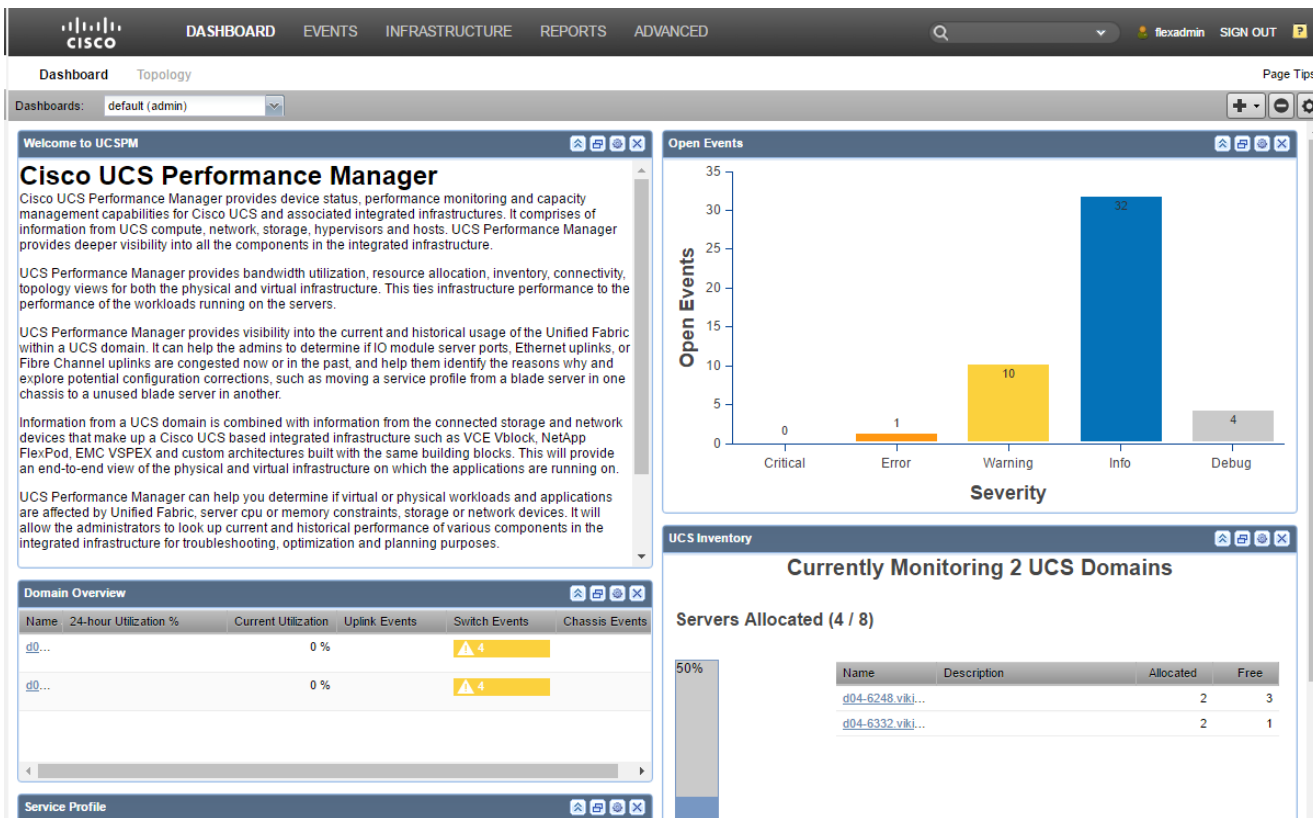
| Status | Host | Credentials | Type | Duration | Job Log | Remove | Retry |
|---------|-------------------------------|--------------------|------------------------|------------|-------------------|--------|-------|
| Success | n9k-a.vikings.cisco.com | admin | Cisco Nexus 9000 ... | 29 seconds | 0b0c90a0-8754... | | |
| Success | n9k-b.vikings.cisco.com | admin | Cisco Nexus 9000 ... | 25 seconds | aa0f6b46-7ee7... | | |
| Success | d04-9148s-a.vikings.cisco.com | flexpod.flexpod | Cisco MDS 9000 (S... | 26 seconds | 06d22bde-3ef4... | | |
| Success | d04-9148s-b.vikings.cisco.com | flexpod.flexpod | Cisco MDS 9000 (S... | 24 seconds | 5fb26e0a-3900... | | |
| Success | vikings.vikings.cisco.com | admin.true | NetApp C-Mode Fil... | 21 seconds | bb7960e8-1aa9... | | |
| Success | vc.vikings.cisco.com | vc.vikings.cisc... | vSphere EndPoint (...) | 59 seconds | 7e5e3f97-f191-... | | |

23. Click Next.

24. Fill in the SMTP information for your email server. If you do not have an SMTP server, skip this step.

25. Click Finish.

The initial configuration of UCS Performance Manger to access the FlexPod environment is now complete.



Reference the [Cisco UCS Performance Manager Administration Guide, Release 2.0.2](#) for further use and configuration of Cisco UCS Performance Manager.

NetApp Virtual Storage Console 6.2P2 Deployment Procedure

This section describes the deployment procedures for the NetApp VSC.

Virtual Storage Console 6.2 Pre-installation Considerations

The following licenses are required for VSC on storage systems that run clustered Data ONTAP 8.3.2:

- Protocol licenses (NFS, iSCSI, and FCP)
- FlexClone (for provisioning and cloning only)
- SnapRestore (for backup and recovery)
- The SnapManager Suite

Install Virtual Storage Console 6.2P2

To install the VSC 6.2P2 software, complete the following steps:

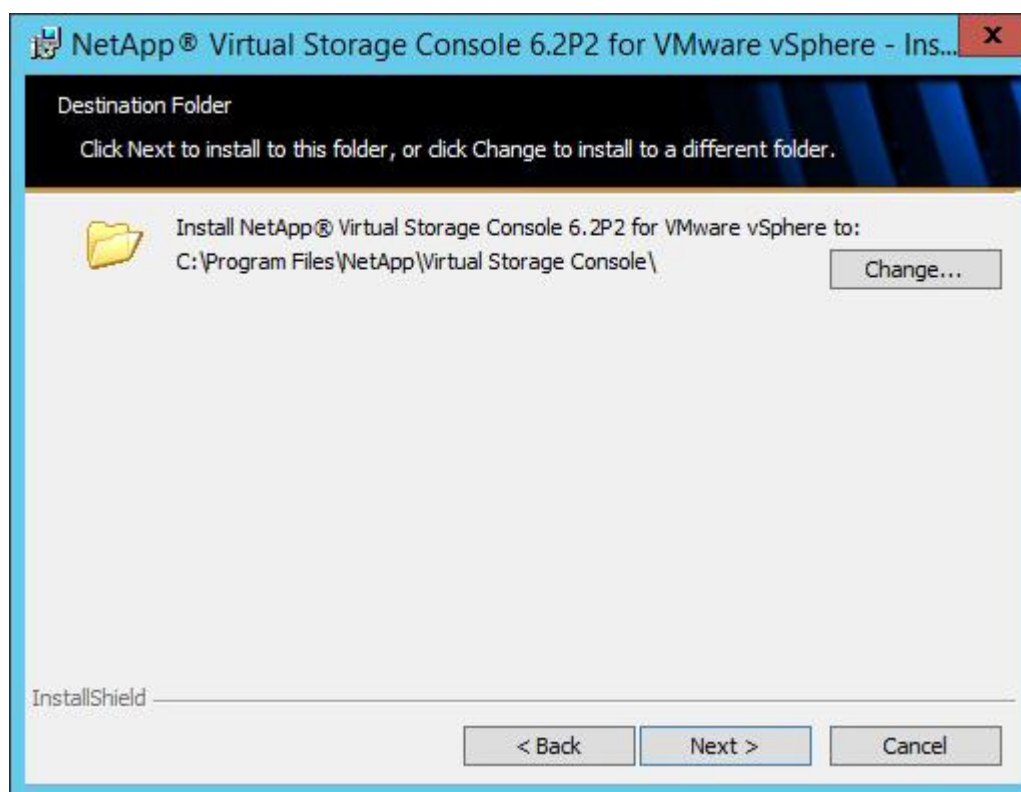
1. Build a VSC VM with Windows Server 2012 R2, 4GB of RAM, two CPUs, and one virtual network interface in the IB-MGMT Network port group. The virtual network interface should be a VMXNET 3 adapter.

2. Bring up the VM, install VMware Tools, assign the IP address and gateway in the IB-MGMT subnet, and join the machine to the Active Directory domain.
3. Activate Adobe Flash Player in Windows Server 2012 R2 by installing Desktop Experience under the User Interfaces and Infrastructure Feature on the VM.
4. Install all Windows updates on the VM.
5. Log in to the VSC VM as the FlexPod Admin user using the VMware console.
6. From the VMware console on the VSC VM, download the x64 version of [Virtual Storage Console 6.2P2](#) from the [NetApp Support](#) site.
7. Right-click the VSC-6.2P2-win64.exe file downloaded in step 5 and select Run as Administrator.
8. Select the appropriate language and click OK.
9. On the Installation wizard Welcome page, click Next.
10. Select the checkbox to accept the message and click Next.



The Backup and Recovery capability requires an additional license.

11. Click Next to accept the default installation location.



12. Click Install.



13. Click Finish.

Register Virtual Storage Console with vCenter Server

To register the VSC with the vCenter Server, complete the following steps:

1. A browser window with the registration URL opens automatically when the installation phase is complete. If the URL does not open automatically, open <https://localhost:8143/Register.html> in Internet Explorer.
2. Click Continue to This Website (Not Recommended).
3. In the Plug-in Service Information section, select the local IP address of the VSC VM.
4. In the vCenter Server Information section, enter the host name or IP address, the user name (FlexPod admin user or root), and the user password for the vCenter Server. Click Register to complete the registration.

vSphere Plugin Registration

The Virtual Storage Console is registered as specified below. If you need to change the registration settings, update the fields below and then click "Register".

If you specify a new vCenter Server IP address, the Virtual Storage Console will unregister with the previously specified vCenter Server and then register with the newly specified vCenter Server.

| | |
|----------------------------|--|
| Plugin service information | |
| Host name or IP Address: | <input type="text" value="vsc.vikings.cisco.com"/> ▼ |
| vCenter Server information | |
| Host name or IP Address: | <input type="text" value="vc.vikings.cisco.com"/> ✕ |
| Port: | <input type="text" value="443"/> |
| User name: | <input type="text" value="administrator@vsphere.local"/> |
| User password: | <input type="password" value="••••••••"/> |

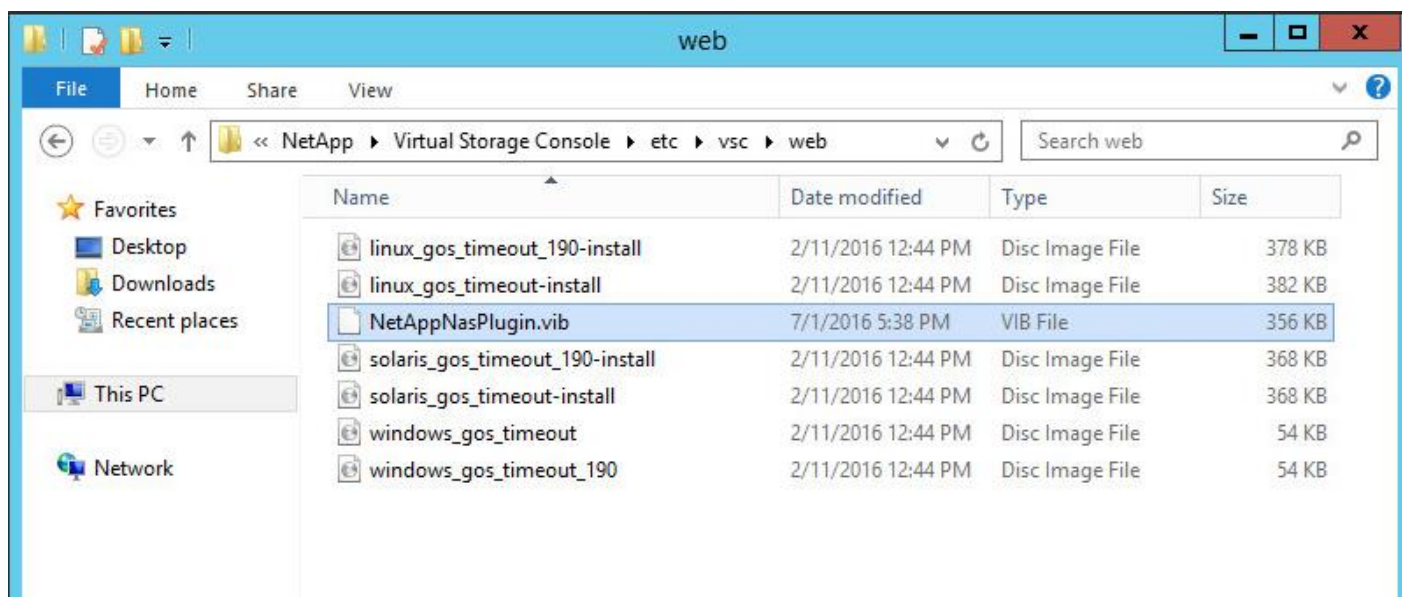
Register

5. Upon successful registration, storage controller discovery begins automatically.

Install NetApp NFS VAAI Plug-in

To install the NetApp NFS VAAI Plug-in, complete the following steps:

1. Onto the VSC VM, download the NetApp NFS Plug-in 1.1.0 for VMware .vib file from the [NFS Plugin Download](#).
2. Rename the downloaded file NetAppNasPlugin.vib.
3. Move the file to the "C:\Program Files\NetApp\Virtual Storage Console\etc\vsc\web" folder.



Discover and Add Storage Resources

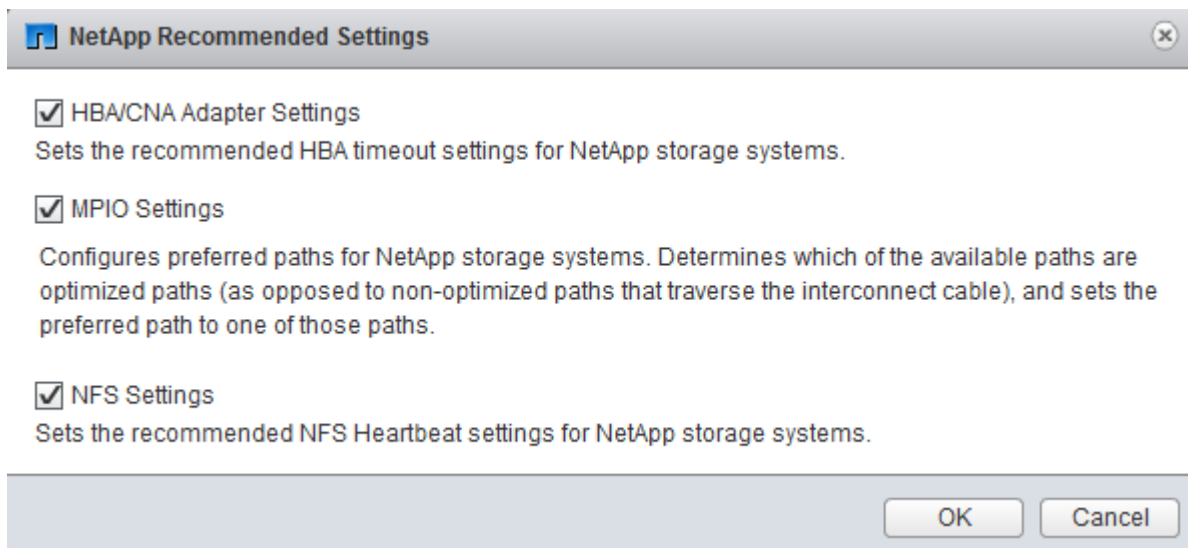
To discover storage resources for the Monitoring and Host Configuration capability and the Provisioning and Cloning capability, complete the following steps:

1. Using the vSphere web client, log in to the vCenter Server as the FlexPod admin user. If the vSphere web client was previously opened, close it and then reopen it.
2. In the Home screen, click the Home tab and click Virtual Storage Console.
3. Select Storage Systems. Under the Objects tab, click Actions > Modify.
4. In the IP Address/Hostname field, enter the storage cluster management IP. Enter admin for the user name and the admin password for password. Confirm Use TLS to Connect to This Storage System is selected. Click OK.
5. Click OK to accept the controller privileges.
6. Wait for the Storage Systems to update. You may need to click Refresh to complete this update.

Optimal Storage Settings for ESXi Hosts

VSC allows for the automated configuration of storage-related settings for all ESXi hosts that are connected to NetApp storage controllers. To use these settings, complete the following steps:

1. From the Home screen, click vCenter > Hosts and Clusters. For each ESXi host, right-click and select NetApp VSC > Set Recommended Values for these hosts.

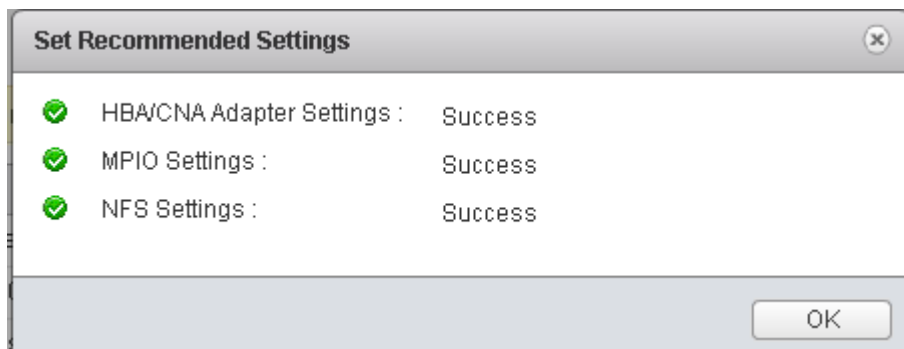


2. Check the settings that are to be applied to the selected vSphere hosts. Click OK to apply the settings.



This functionality sets values for HBAs and converged network adapters (CNAs), sets appropriate paths and path-selection plug-ins, and verifies appropriate settings for software-based I/O (NFS and iSCSI).

3. Click OK.



4. From the Home screen in the vSphere Web Client, select Virtual Storage Console.
5. On the left under Virtual Storage Console, select NFS VAAI Tools.
6. Make sure that NFS Plug-in for VMware VAAI Version 1.1.0-0 is shown.
7. Click Install on Host.
8. Select both ESXi hosts and click Install.
9. For each host for which settings were adjusted in the previous step, place the host in maintenance mode, reboot the host, and exit maintenance mode.

Virtual Storage Console 6.2P2 Backup and Recovery

Prerequisites for Use of Backup and Recovery Capability

Before you begin using the Backup and Recovery capability to schedule backups and restores of your datastores, VMs, or virtual disk files, you must confirm that the storage systems that contain the datastores and VMs for which you are creating backups have valid storage credentials.

If you plan to leverage the SnapMirror update option, add all of the destination storage systems with valid storage credentials.

Backup and Recovery Configuration

To configure a backup job for a datastore, complete the following steps

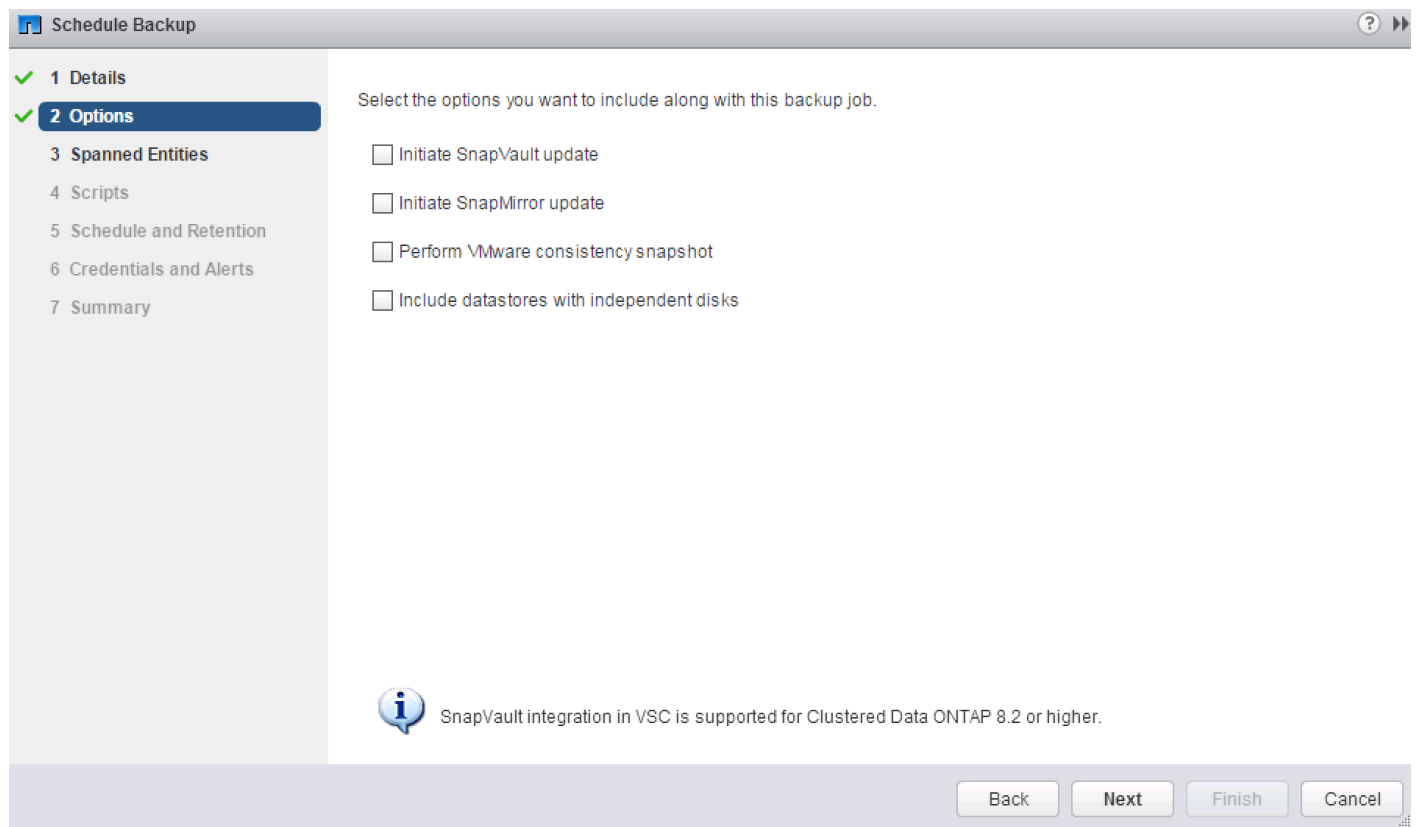
1. From the Home screen of the vSphere Web Client, select the Home tab and click Storage.
2. On the left, expand the datacenter.
3. Right-click the datastore that you need to backup. Select NetApp VSC > Schedule Backup.



If you prefer a one-time backup, choose Backup Now instead of Schedule Backup.

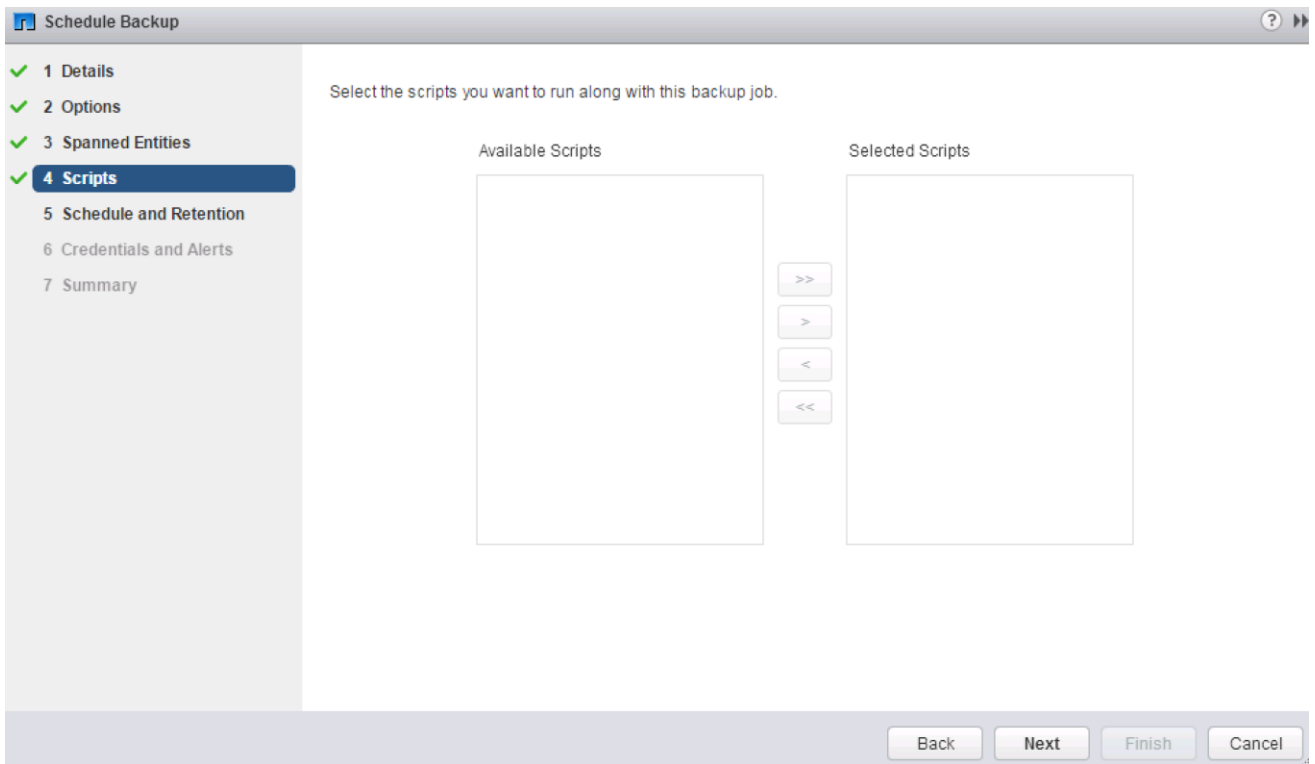
4. Type a backup job name and description. Click Next.

5. Select the options necessary for the backup.

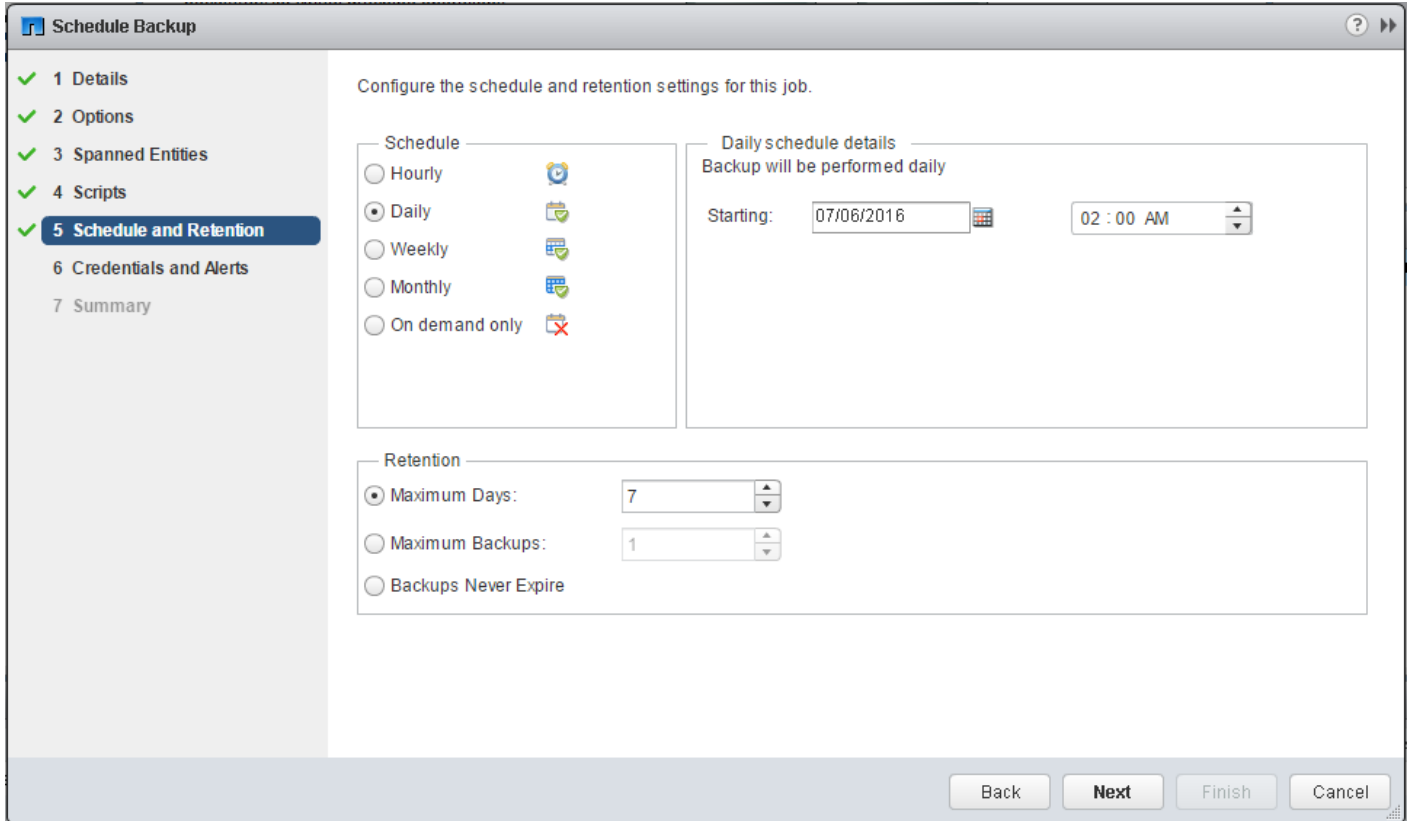


For consistent VM snapshots, select Perform VMware Consistency Snapshot to make a VMware snapshot of each VM just before the NetApp Snapshot copy is made. The VMware snapshot is then deleted after the NetApp Snapshot copy is made.

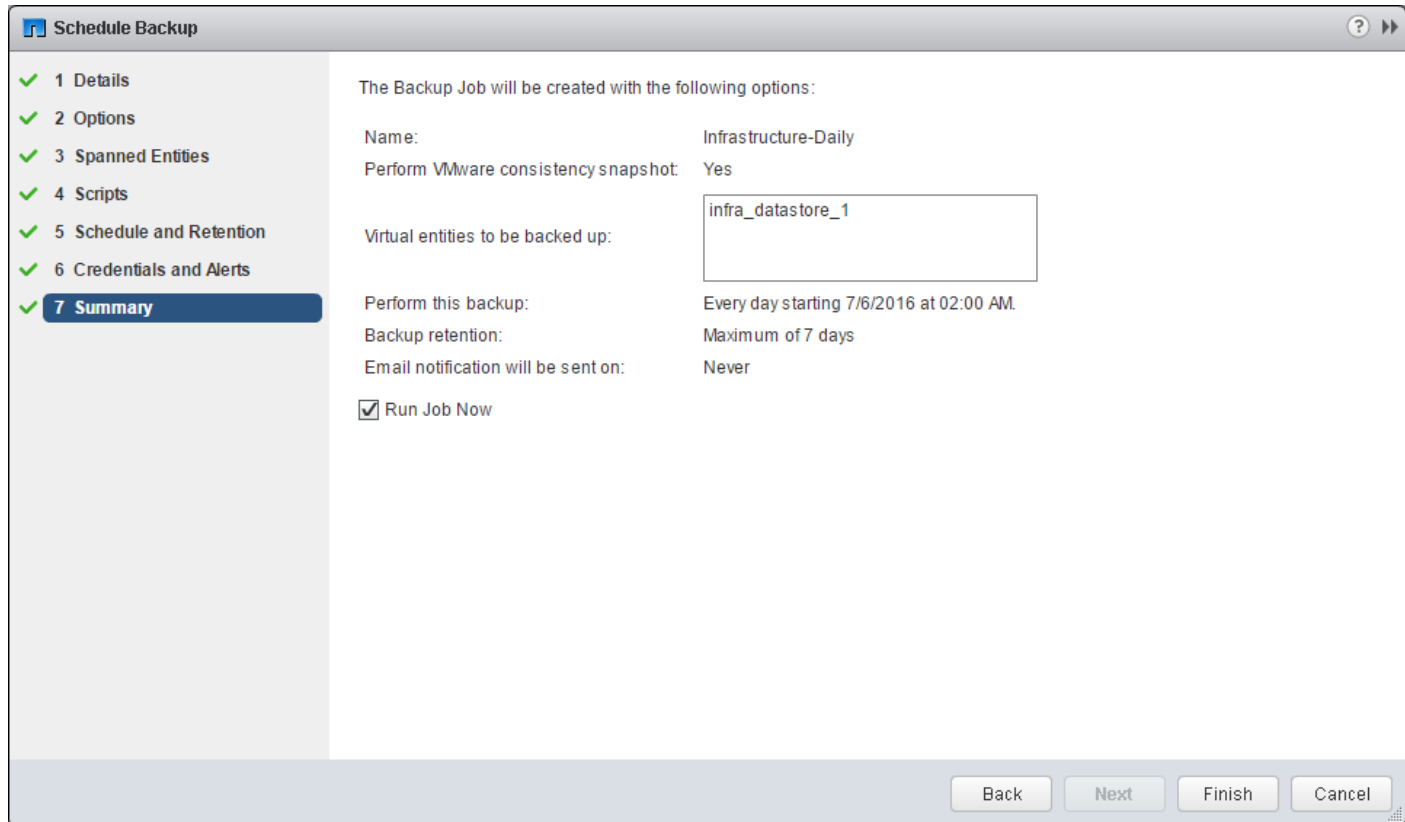
6. Click Next in the Options screen.
7. Click Next in the Spanned Entities screen.
8. Select one or more backup scripts if available, and click Next in the Scripts screen.



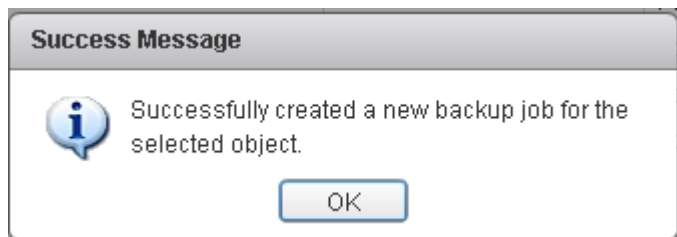
- 9. Select the hourly, daily, weekly, or monthly schedule and retention policy that you want for this back-up job. Click Next.



10. Use the default vCenter credentials or enter the user name and password for the vCenter server. Click Next.
11. Specify any needed backup notification details. Enter an e-mail address and mail server address for receiving e-mail alerts. You can add multiple e-mail addresses by using semicolons to separate them. Click Next.



12. Review the summary page and click Finish. If you want to run the job immediately, select the Run Job Now option and then click Finish.
13. Click OK.



14. You can also create other backup jobs with overlapping schedules. For example, you can create weekly or monthly backups that overlay daily backups.
15. On the storage cluster interface, automatic Snapshot copies of the volume can now be disabled because NetApp VSC is now handling scheduled backups. To do so, enter the following command:


```
volume modify -vserver Infra-SVM -volume infra_datastore_1 -snapshot-policy none
```

16. Also, to delete any existing automatic Snapshot copies that have been created on the volume, enter the following command:

```
volume snapshot show -vserver Infra-SVM -volume infra_datastore_1
volume snapshot delete -vserver Infra-SVM -volume infra_datastore_1 -snapshot <snapshot-name>
```



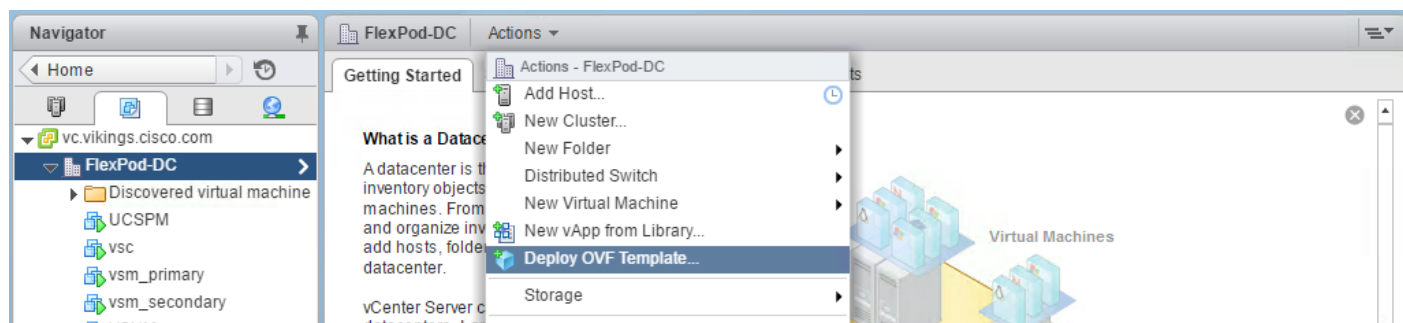
The wildcard character * can be used in Snapshot names in the previous command.

OnCommand Performance Manager 7.0

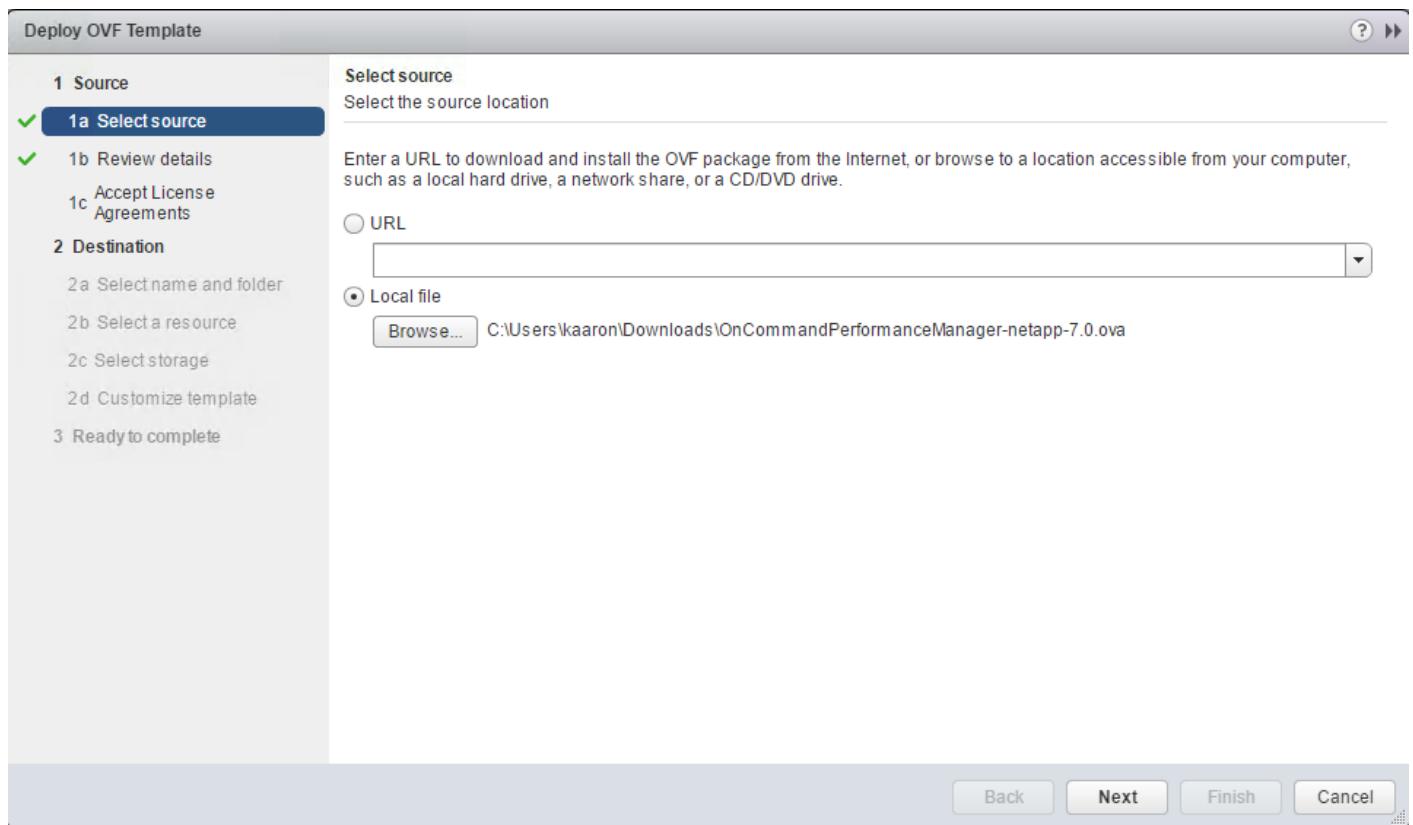
OnCommand Performance Manager Open Virtualization Format (OVF) Deployment

To install the OnCommand Performance Manager, complete the following steps:

1. Download and review the [OnCommand Performance Manager 7.0 Installation and Administration Guide for VMware Virtual Appliances](#).
2. Download OnCommand Performance Manager version 2.1 ([OnCommandPerformanceManager-netapp-7.0.ova](#)). Click Continue at the bottom of the page and follow the prompts to complete the installation.
3. Log in to the vSphere Web Client. Select Home > VMs and Templates.
4. At the top of the center pane, select Actions > Deploy OVF Template.

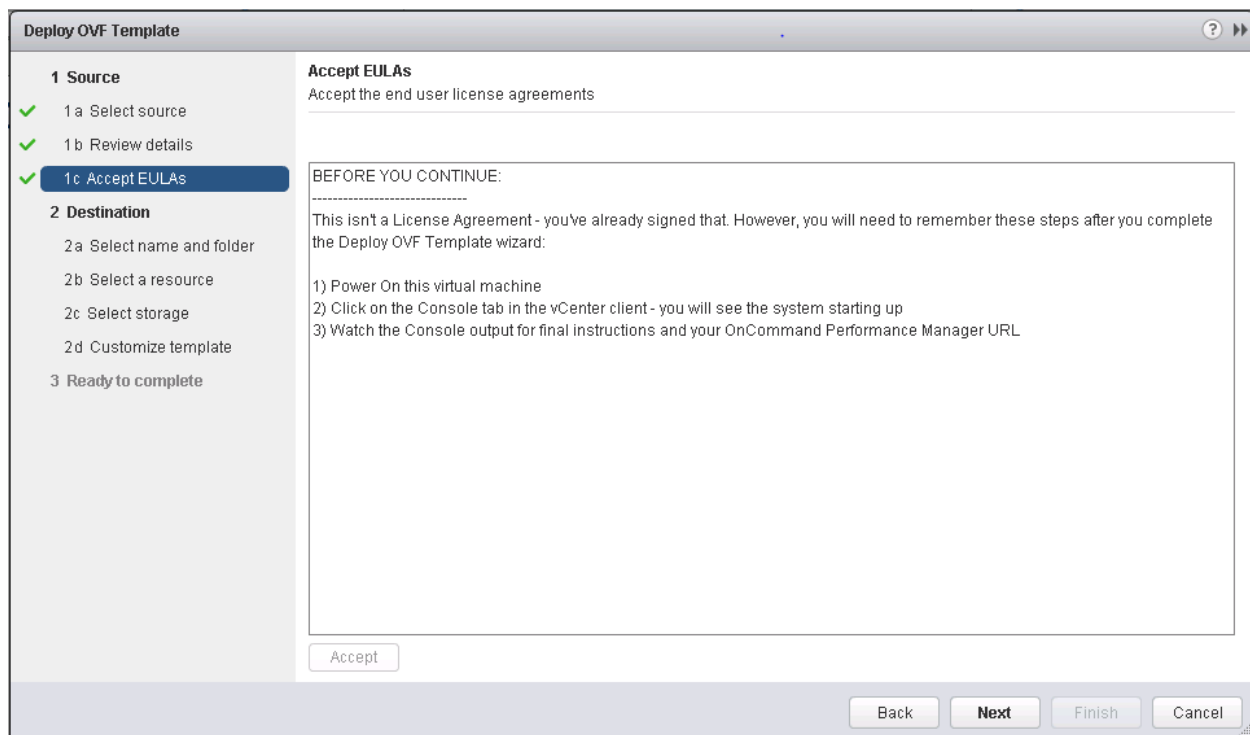


5. Browse to the OnCommandPerformanceManager-netapp-7.0.ova file that was downloaded locally. Click Open to select the file. Click Next to proceed with the selected file.

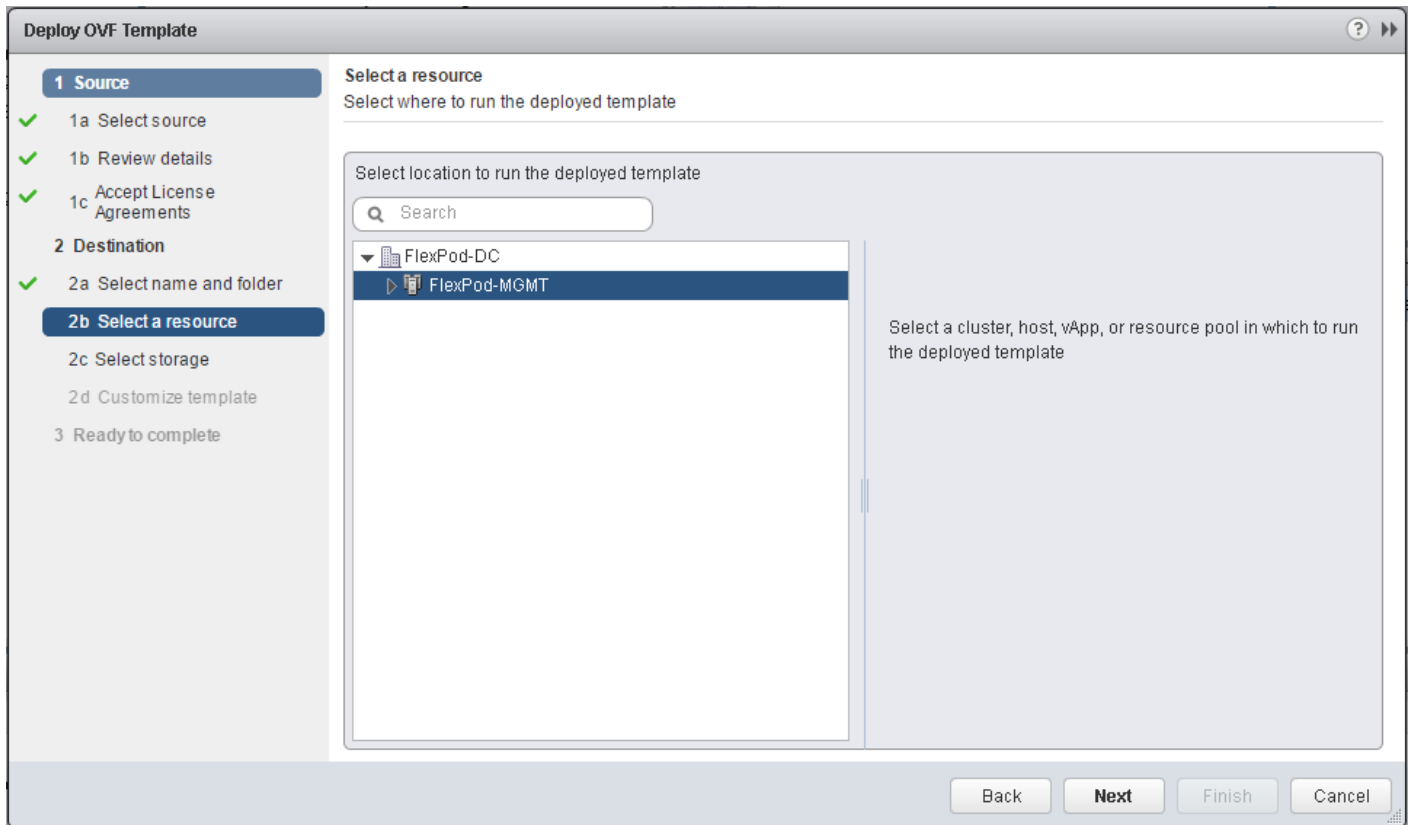


6. Review the details and click Next.

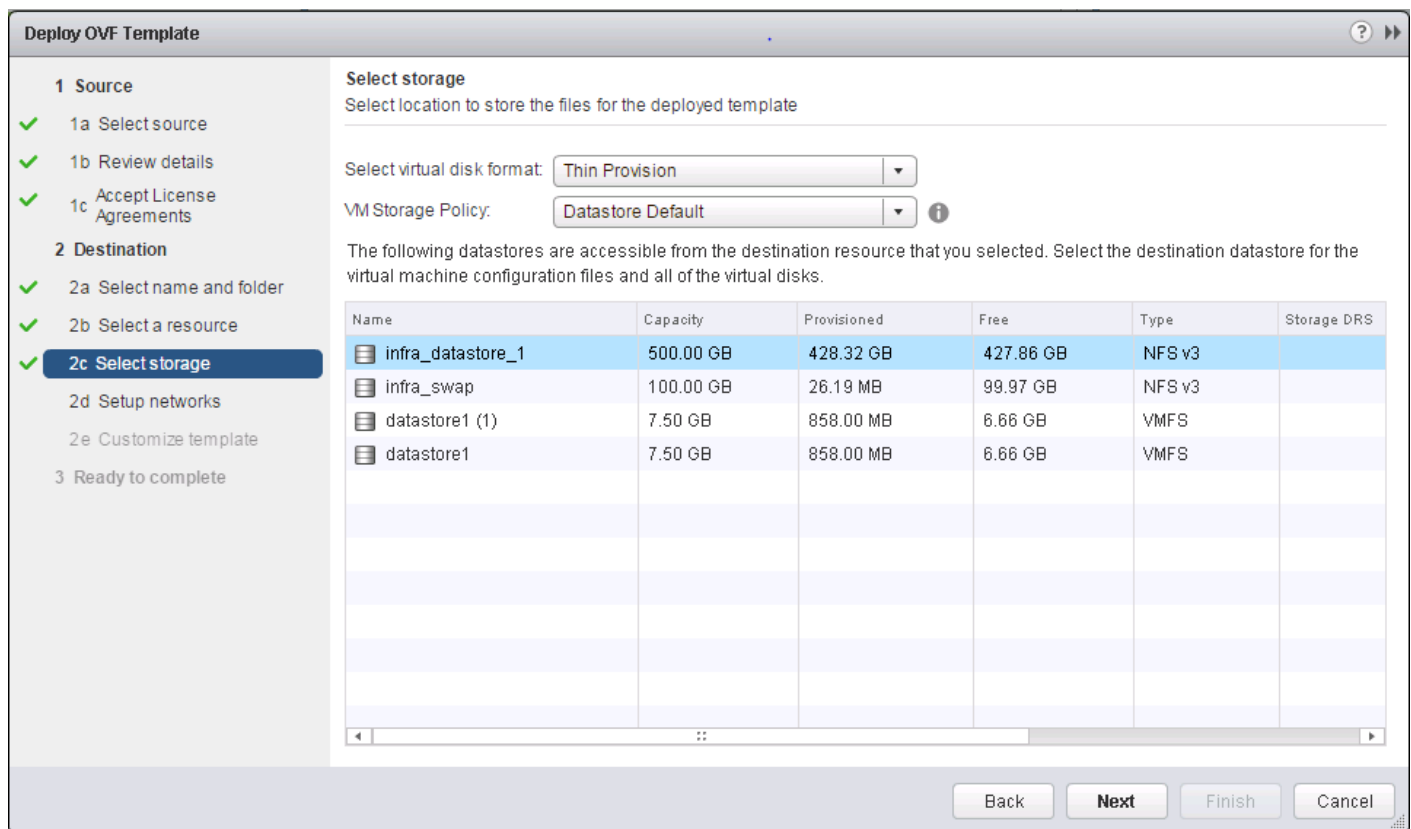
7. Click Accept to accept the agreement. Click Next.



8. Enter the name of the VM and select the FlexPod-DC folder to hold the VM. Click Next.
9. Select FlexPod-MGMT within the FlexPod-DC datacenter as the destination compute resource pool to host the VM. Click Next to continue.



10. Select infra_datastore_1 as the storage target for the VM and select Thin Provision as the virtual disk format. Click Next.



11. Select IB-MGMT Network as the destination network to the nat source network. It is not necessary for this VM to be in the core-services network. Click Next.
12. Do not enable DHCP. Fill out the details for the host name, IP address, network mask, gateway, primary DNS, and secondary DNS. Click Next to continue.
13. Deselect Power On After Deployment.
14. Review the configuration details. Click Finish to begin deploying the VM with the provided configuration details.
15. In the left pane, select Home > Hosts and Clusters. Expand the FlexPod-Management cluster and select the newly created OnCommand Performance Manager VM. After OVF deployment is complete, right-click the newly created VM and select Edit Settings.
16. Expand the CPU options, and complete the following steps:
 - a. The minimum required CPU reservation is 9572MHz. Determine the CPU frequency of the host server.
 - b. Set the number of CPUs to the number of CPUs required ($9572 / \text{the CPU Frequency of the host}$ rounded up to the next even number).
 - c. Set the number of cores per socket where the sockets number on the right matches the number of CPU sockets in the host. For example, if a host has two CPUs operating at a

speed of 1999MHz, then the VM needs six virtual CPUs ($9572 / 1999 = 4.79$: rounded to 6 virtual CPUs). If the host has two physical CPU sockets, then allocate three cores per socket.

See the [OnCommand Performance Manager 7.0 Installation and Administration Guide for VMware Virtual Appliances](#) for guidance on these settings.



17. Click OK to accept the changes.

18. Right-click the VM in the left-hand pane. Click Power On.

OnCommand Performance Manager Basic Setup

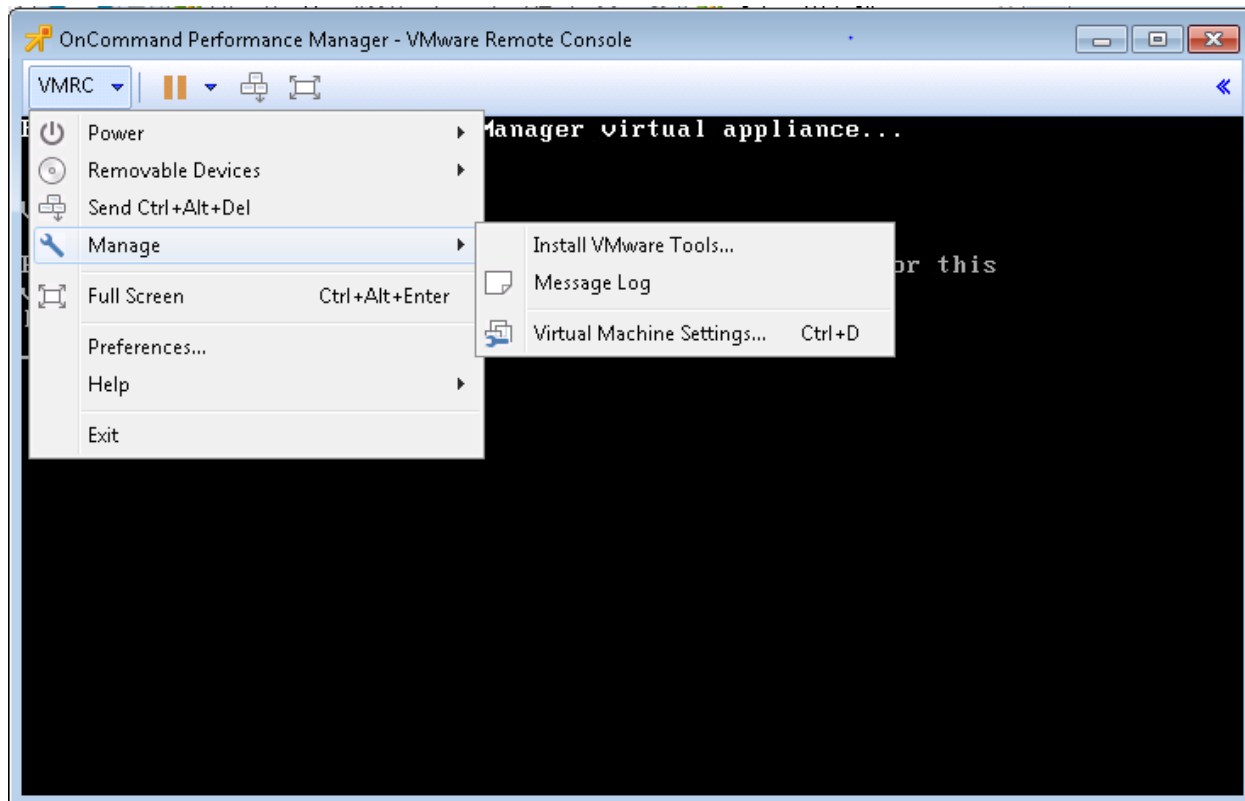
To setup the OnCommand Performance Manager, complete the following steps:

1. Select the VM in the left-hand pane. In the center pane, select Launch Remote Console.



It might be necessary to download and install the remote console at this point.

2. After VMware Tools Installation comes up in the VMware Remote Console window, select VMRC > Manage > Install VMware Tools. VMware Tools installs in the VM.



3. Set up OnCommand Performance Manager by answering the following questions in the console window:

```
Geographic area: <<Enter your geographic location>>
Time zone: <<Select the city or region corresponding to your time zone>>
```

These commands complete the network configuration checks, generate SSL certificates, and start the OnCommand Performance Manager services.

To Create a Maintenance User account, follow these prompts:



The maintenance user manages and maintains the settings on the OnCommand Performance Manager virtual appliance.

```
Username : admin
Enter new UNIX password: <password>
Retype new UNIX password: <password>
```

4. With a web browser, navigate to the OnCommand Performance Manager using the URL `https:// <on-command-pm-ip>`.

5. Log in using the maintenance user account (admin) credentials.
6. Enter a maintenance user e-mail address, SMTP mail server information, and the NTP server IP address. Click Save.
7. Select Yes to enable AutoSupport capabilities. Click Save.
8. Click Save to not change the admin password.
9. Enter the storage cluster host name or IP address, the storage cluster admin user name, and the storage cluster admin password. Click Add Cluster, and click Save to complete setup. It may take up to 15 minutes for the cluster to be visible in OnCommand Performance Manager.

The screenshot shows the OnCommand Performance Manager interface. At the top, there is a navigation bar with 'PERFORMANCE' selected and tabs for Dashboard, Events, Storage, Configuration, and Administration. Below the navigation bar, there is a search bar and a 'Type: All' dropdown. The main content area displays 'All Clusters in Your Environment' with a 'Refresh' button. A specific cluster 'a01-aff8040' is highlighted, showing a 'View Cluster Details' button. Below this, there are five performance metrics cards: Latency (SVMs, Volumes, LUNs), IOPS (Nodes, SVMs), MBps (Nodes, SVMs), Disk Utilization (Aggregates), and Node Utilization (Nodes). Each card contains green checkmarks indicating good performance.

10. After the cluster is added it can be accessed by selecting Administration > Manage Data Sources.

The screenshot shows the 'Manage Data Sources' page in the OnCommand Performance Manager. The left sidebar has 'Management' selected, with sub-items 'Users' and 'Data Sources'. Below that is a 'Setup' section with items like Authentication, AutoSupport, Email, HTTPS Certificate, Network, and NTP Server. The main content area has 'Manage Data Sources' with '+ Add', 'Edit', and 'Remove' buttons. A table lists the data sources:

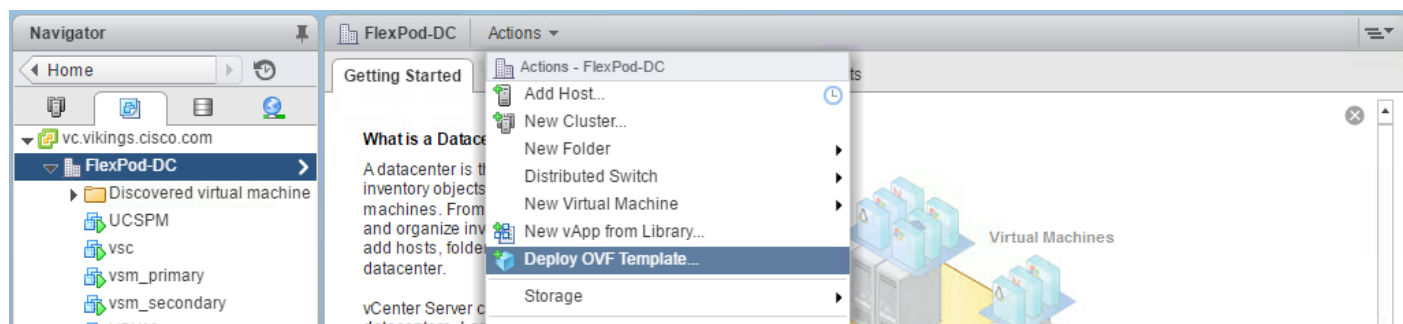
| <input type="checkbox"/> | Name | Host Name or IP Ad | Protocol | Port | User Name | Status | Status Message |
|--------------------------|-------------|--------------------|----------|------|-----------|--------|----------------|
| <input type="checkbox"/> | a01-aff8040 | 192.168.1.20 | HTTPS | 443 | admin | Normal | |

OnCommand Unified Manager 7.0

OnCommand Unified Manager OVF Deployment

To install the OnCommand Unified Manager, complete the following steps:

1. Download and review the [OnCommand Unified Manager 7.0 Installation and Setup Guide](#).
2. Download OnCommand Unified Manager version 7.0 (OnCommandUnifiedManager-7.0.ova), from http://mysupport.netapp.com/NOW/download/software/oncommand_cdot/7.0/. Click Continue at the bottom of the page and follow the prompts to download the .ova file.
3. Log in to the vSphere web client as the FlexPod admin user. From the Home screen, select VMs and Templates.
4. At the top of the center pane, click Actions > Deploy OVF Template.



5. Browse to the .ova file that was downloaded locally. Click Open to select the file. Click Next to proceed with the selected file.

Deploy OVF Template

1 Source

- ✓ **1a Select source**
- ✓ 1b Review details
- 1c Accept License Agreements

2 Destination

- 2a Select name and folder
- 2b Select storage
- 2c Setup networks
- 2d Customize template

3 Ready to complete

Select source
Select the source location

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

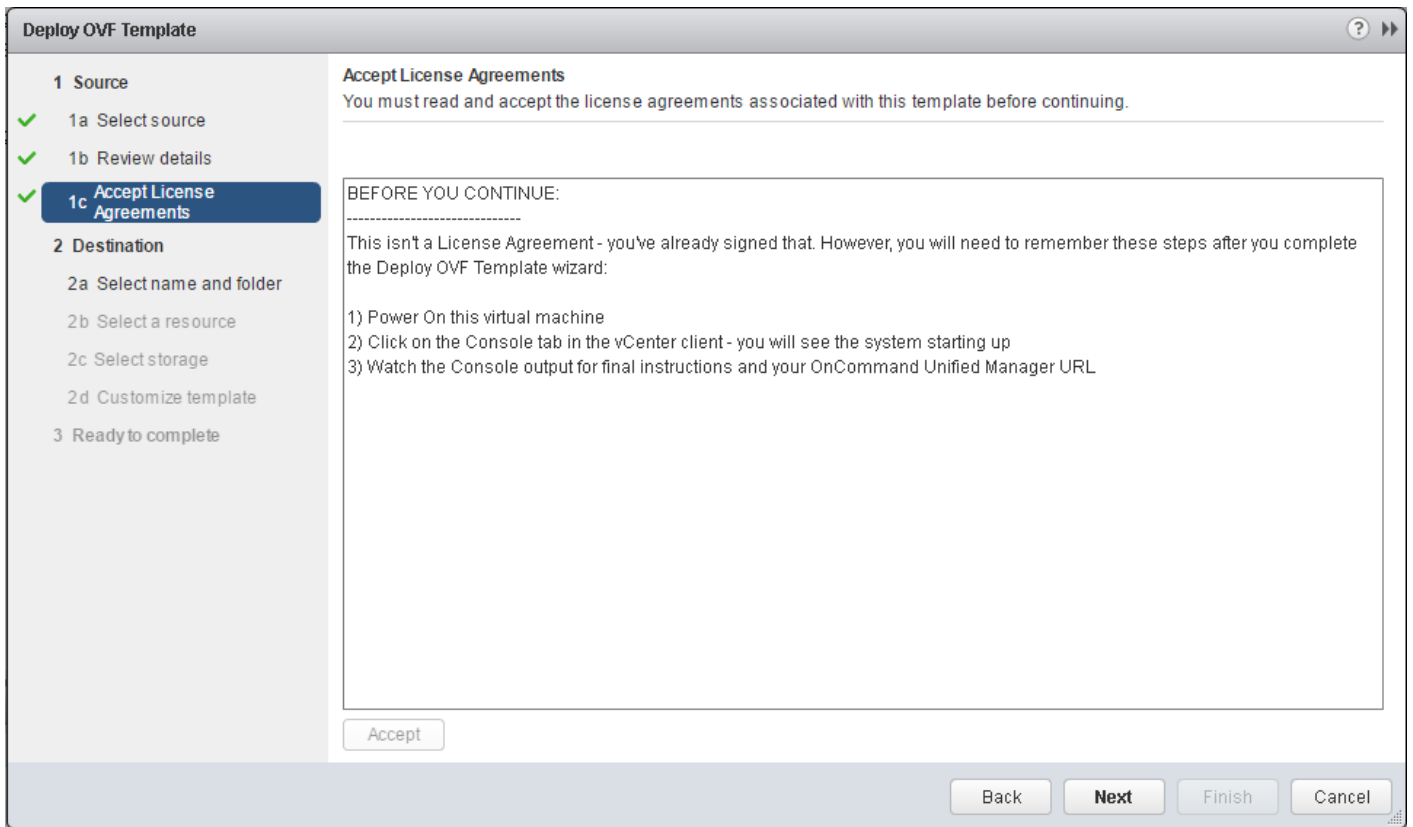
URL

Local file

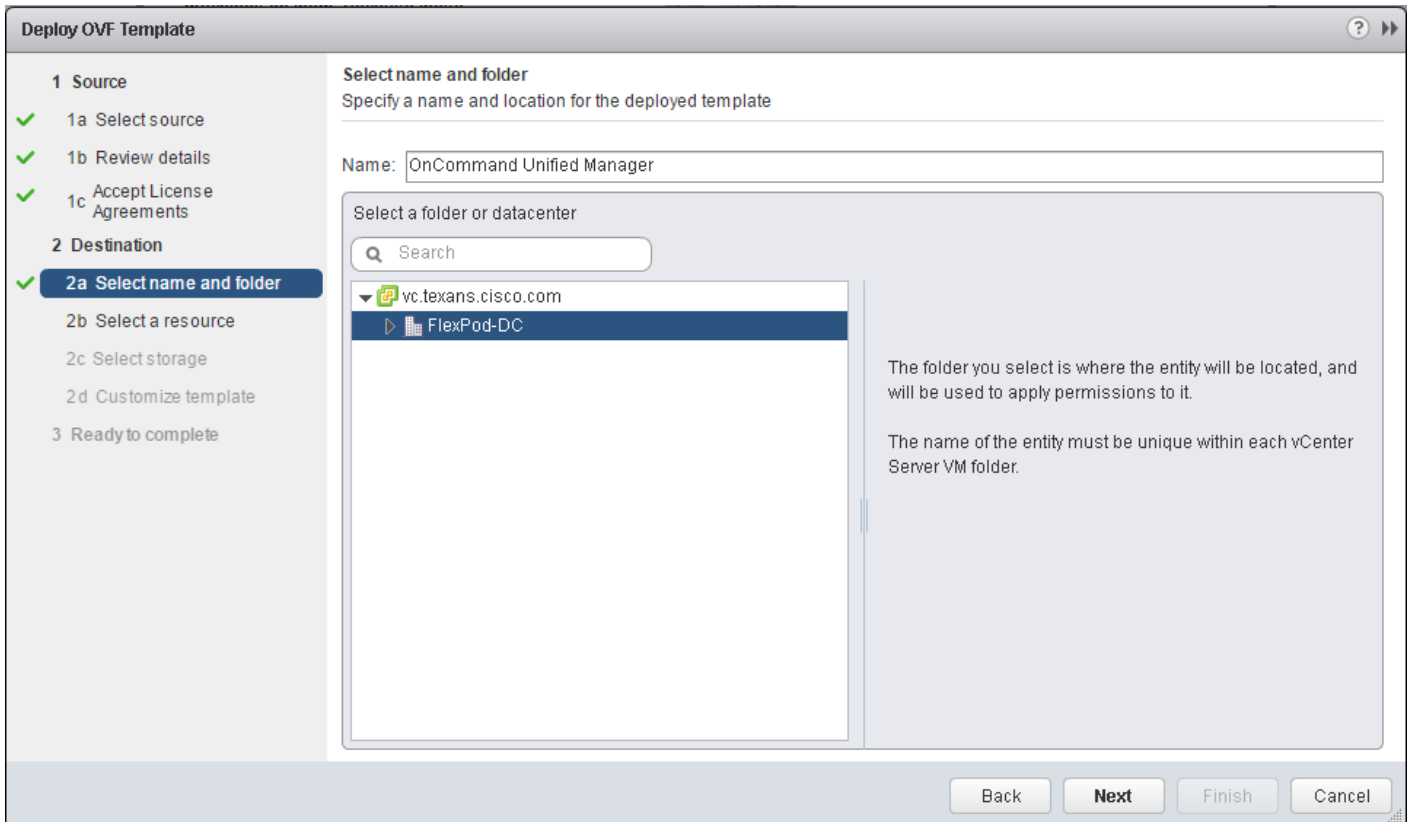
C:\Users\kaaron\Downloads\OnCommandUnifiedManager-7.0.ova

6. Click Next.

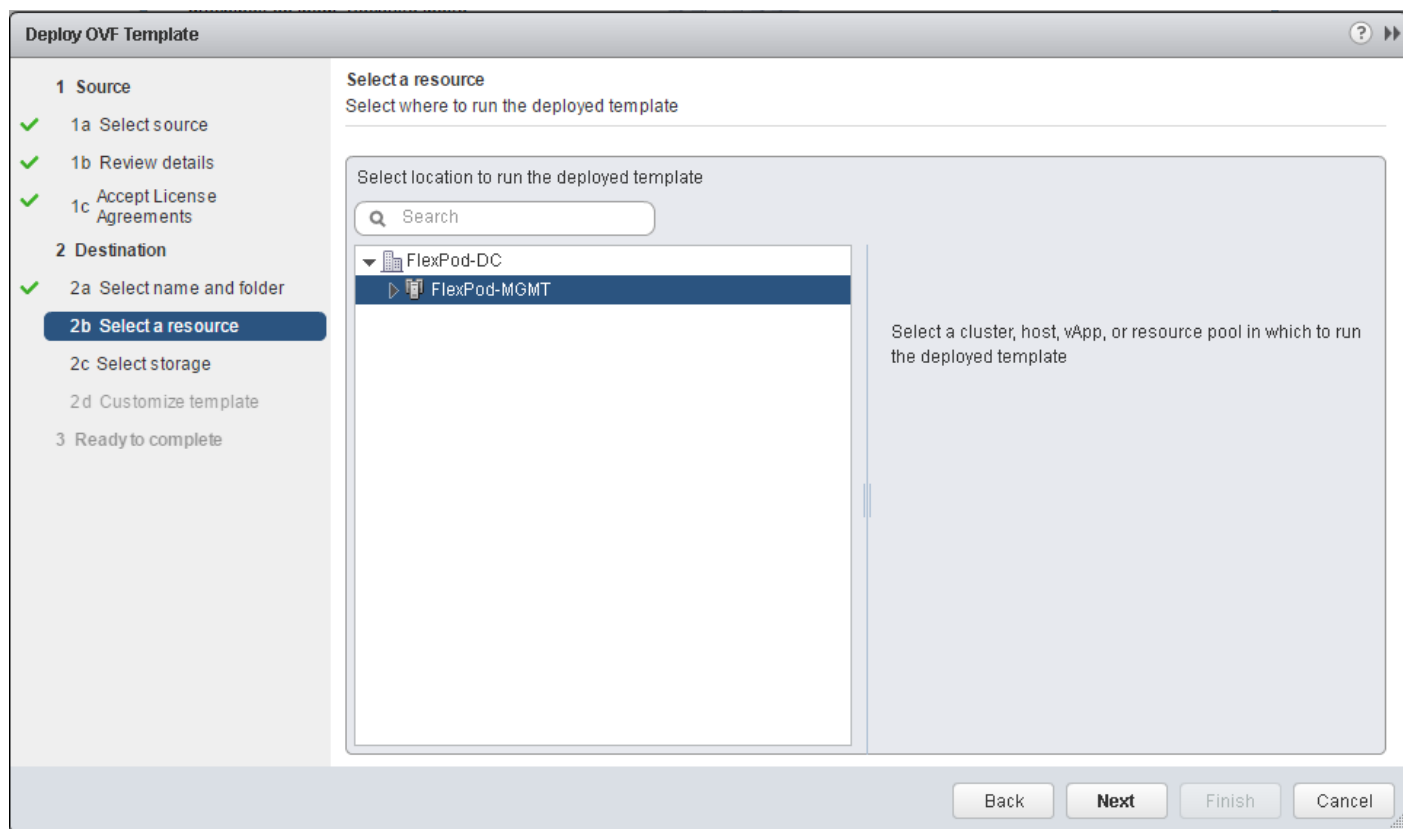
7. Click Accept to accept the agreement and click Next.



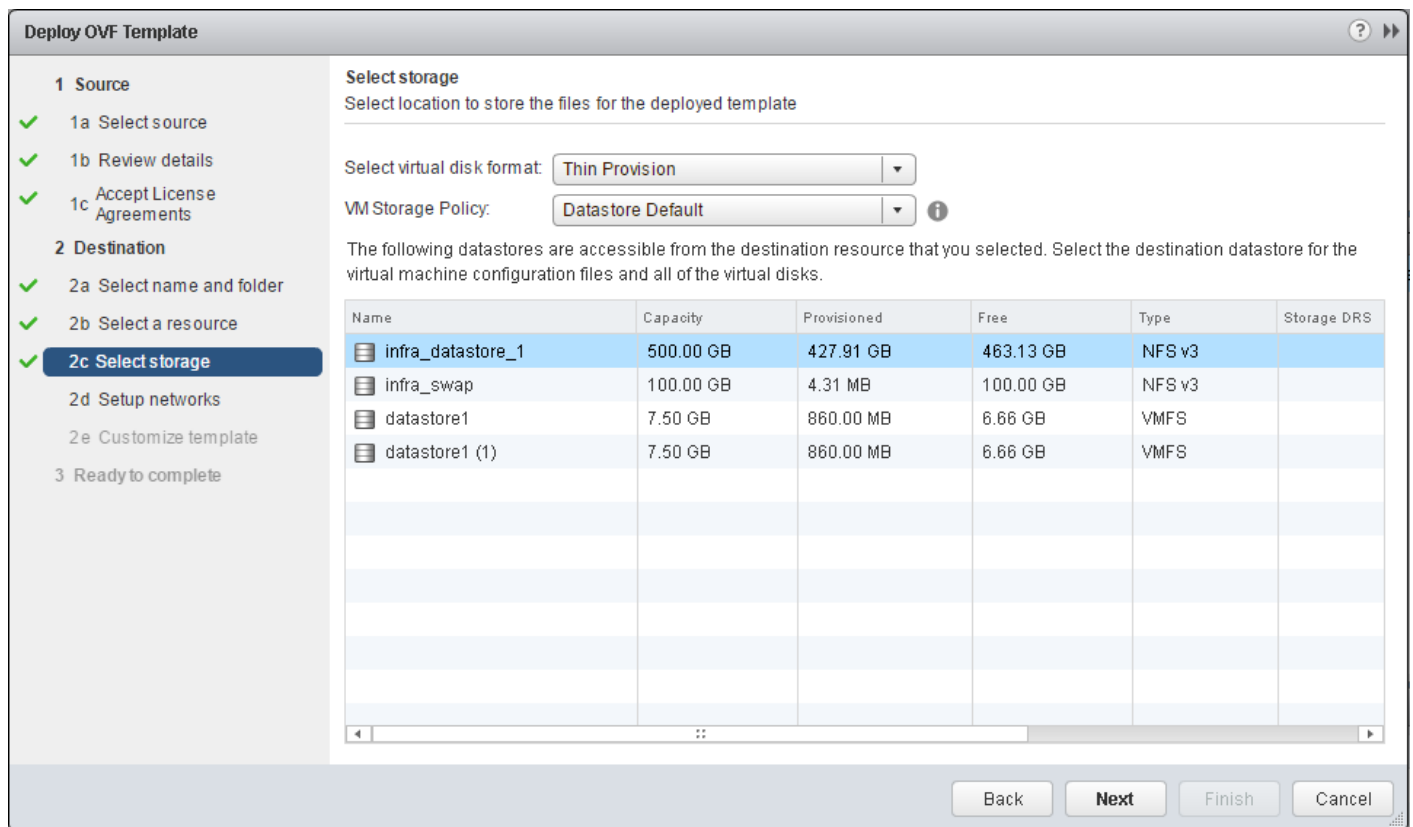
8. Enter the name of the VM and select the FlexPod-DC folder to hold the VM. Click Next.



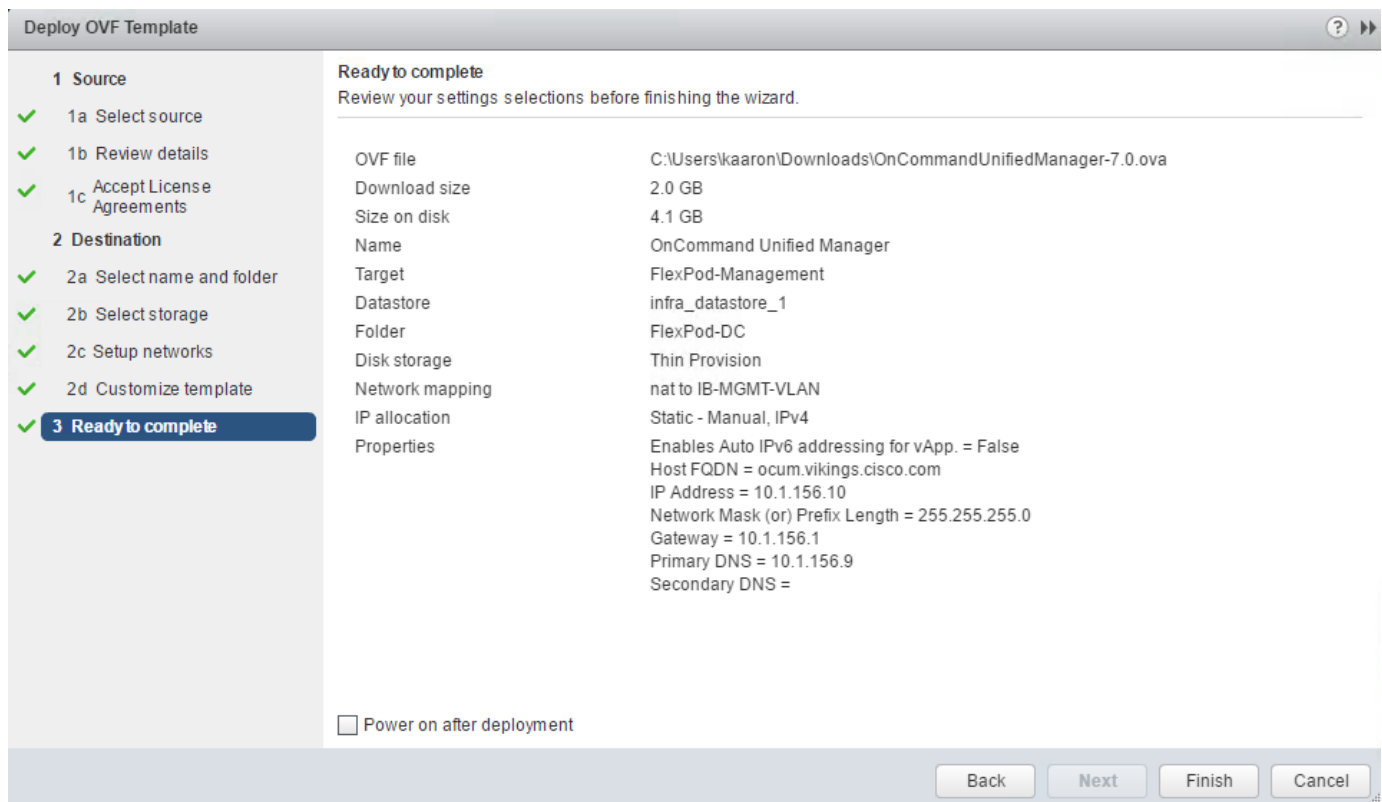
9. Select FlexPod-MGMT within the FlexPod-DC datacenter as the destination compute resource pool to host the VM. Click Next.



10. Select infra_datastore_1 as the storage target for the VM and select Thin Provision as the virtual disk format. Click Next.



11. Select IB-MGMT Network as the destination network to the nat source network. It is not necessary for this VM to be in the core-services network. Click Next.
12. Fill out the details for the host FQDN, IP address, network mask, gateway, primary DNS, and secondary DNS. Click Next to continue.
13. Make sure Power On After Deployment is cleared.
14. Review the configuration details. Click Finish to begin deploying the VM with the provided configuration details.

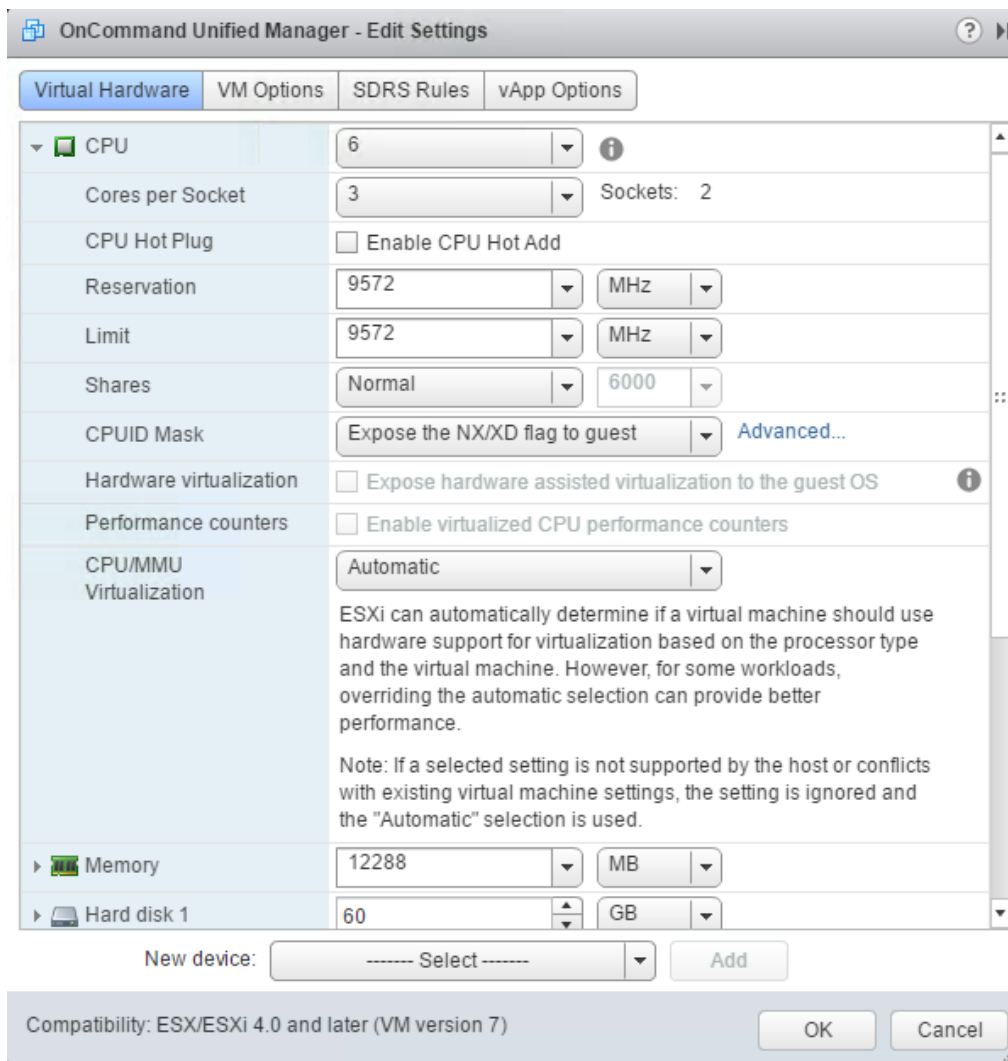


15. In the left pane, select vCenter -> Virtual Machines. After OVF deployment is complete, right-click the newly created VM and select Edit Settings.

16. Expand the CPU options, and complete the following steps:

- a. The recommended CPU Reservation is 9572MHz. Determine the CPU frequency of the host server.
- b. Set the number of CPUs to the number of CPUs required (9572 / the CPU frequency of the host rounded up to the next even number).
- c. Set the number of cores per socket where the sockets number on the right matches the number of CPU sockets in the host. For example, if a host has two CPUs operating at a speed of 1999MHz, then the VM needs six virtual CPUs (9572 / 1999 = 4.79: rounded to 6 virtual CPUs). If the host has two physical CPU sockets, then allocate three cores per socket.

Use the [OnCommand Unified Manager 7.0 Installation and Setup Guide](#) for guidance on these settings.



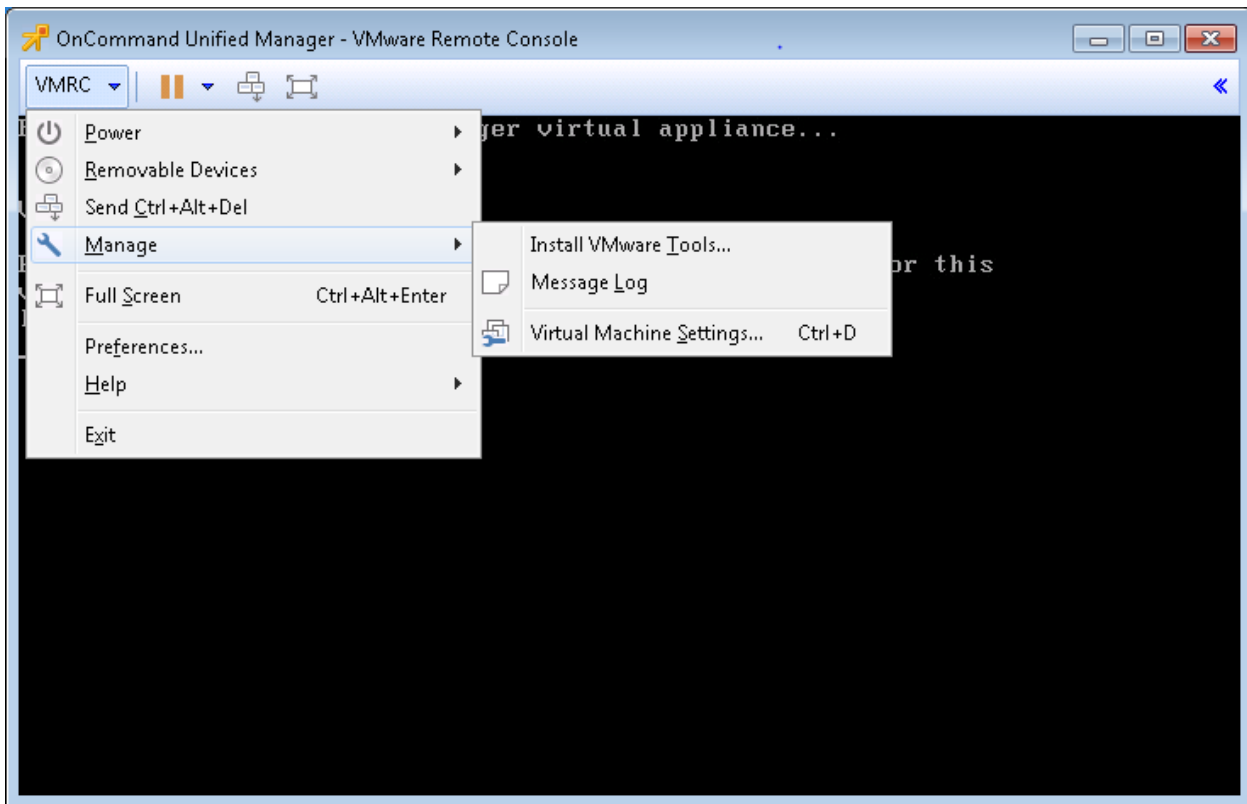
17. Click OK to accept the changes.

18. Right-click the VM in the left-hand pane. Click Power On.

OnCommand Unified Manager Basic Setup

To setup the OnCommand Unified Manager, complete the following steps:

1. Select the VM in the left-hand pane. In the center pane, select Open with Remote Console.
2. In the VMware Remote Console (VMRC) window, select Manage > Install VMware Tools. VMware Tools installs in the VM.




3. Set up OnCommand Unified Manager by answering the following questions in the console window:

```
Geographic area: <<Enter your geographic location>>
Time zone: <<Select the city or region corresponding to your time zone>>
```

These commands complete the network configuration, generate SSL certificates for HTTPS, and start the OnCommand Unified Manager services.

4. To create a maintenance user account, run the following commands:

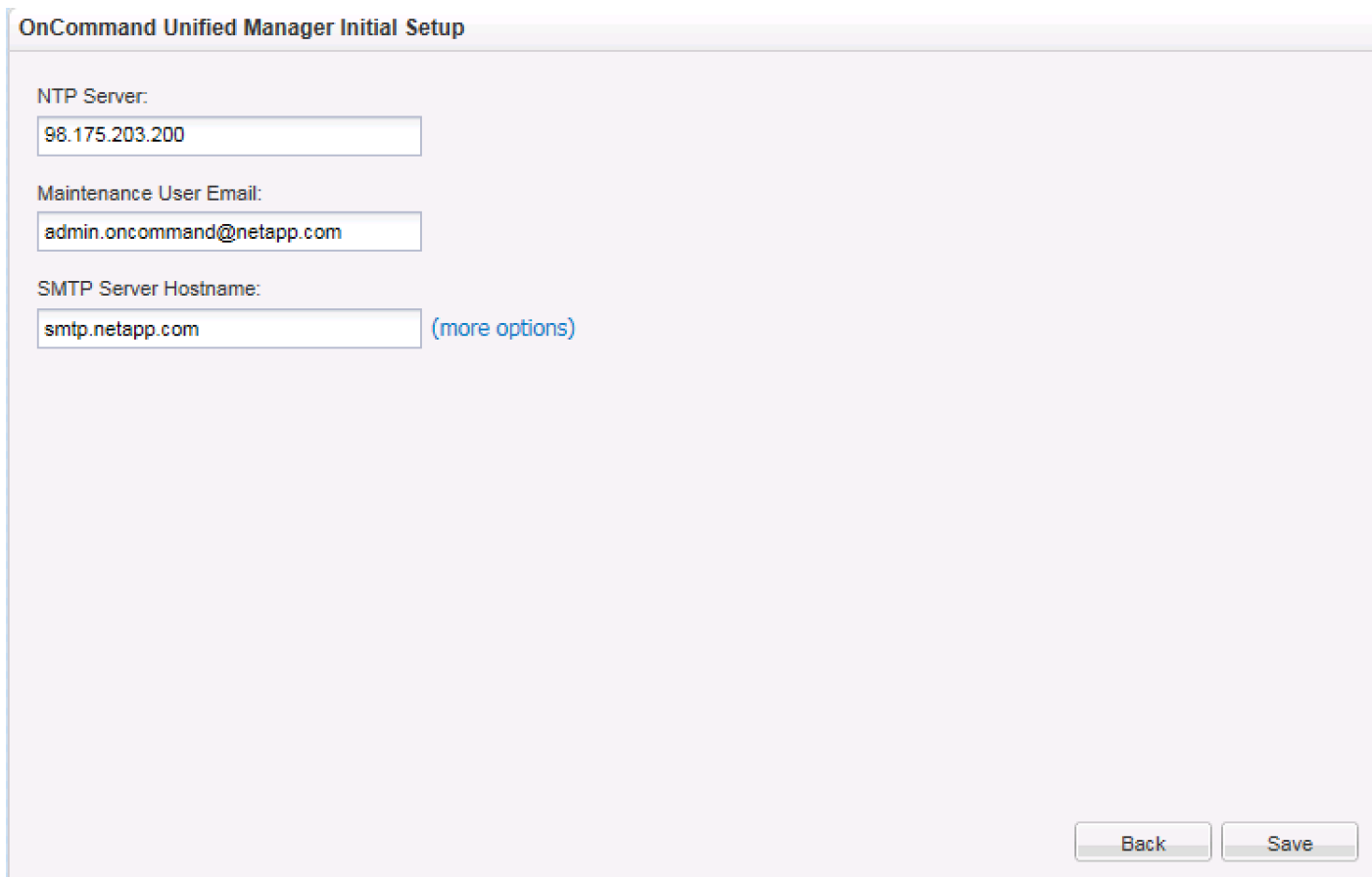
 The maintenance user manages and maintains the settings on the OnCommand Unified Manager virtual appliance.

```
Username : admin
Enter new UNIX password: <password>
Retype new UNIX password: <password>
```

5. With a web browser, navigate to the OnCommand Unified Manager using the URL https:// <oncommand-server-ip>.
6. Log in using the Maintenance User account credentials.
7. Select Yes to enable AutoSupport capabilities.
8. Click Continue.
9. Provide the NTP Server IP address <ntp-server-ip>.

10. Provide the maintenance user e-mail <storage-admin-email>.

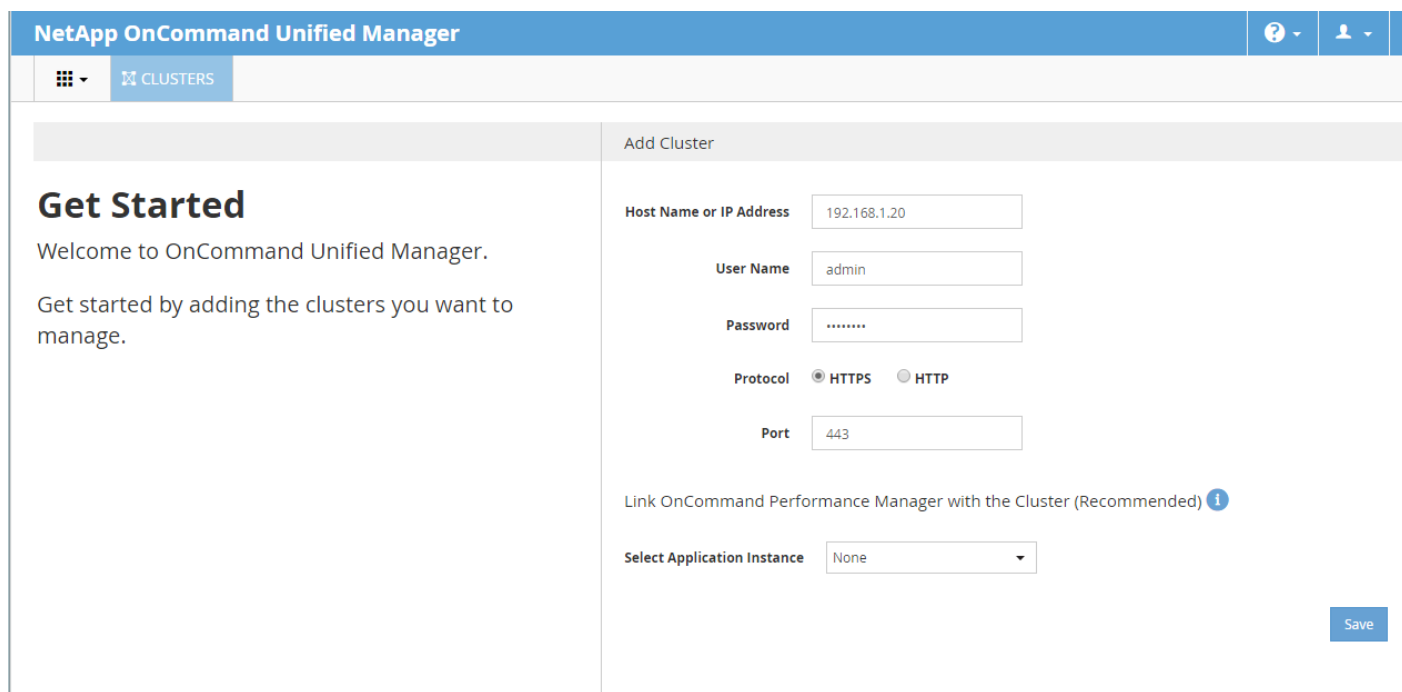
11. Provide the SMTP server hostname.



The screenshot shows a web-based configuration form titled "OnCommand Unified Manager Initial Setup". It contains three input fields: "NTP Server" with the value "98.175.203.200", "Maintenance User Email" with the value "admin.oncommand@netapp.com", and "SMTP Server Hostname" with the value "smtp.netapp.com". A blue link "(more options)" is located to the right of the SMTP field. At the bottom right of the form are two buttons: "Back" and "Save".

12. Click Save.

13. Provide the cluster management IP address, user name, password, protocol, and port. Leave Application Instance for OnCommand Performance Manager set to None.

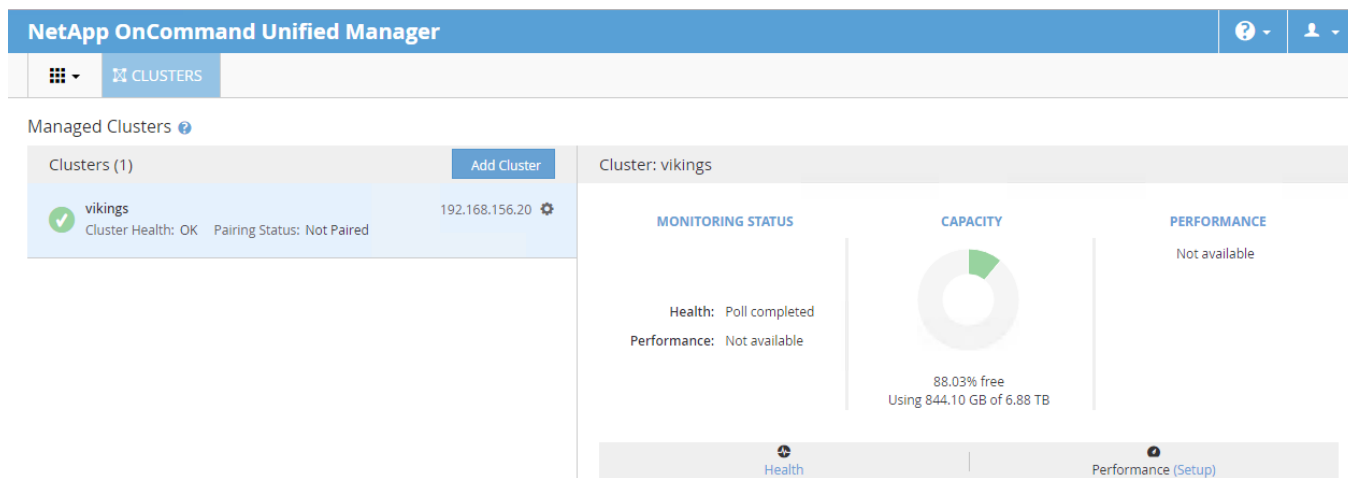


14. Click Save. If asked to trust the certificate for the storage cluster, click Yes.



The Cluster Add operation might take a couple of minutes.

15. On the left, select the storage cluster that was just added. Verify that the cluster has been added to OnCommand Unified Manager.

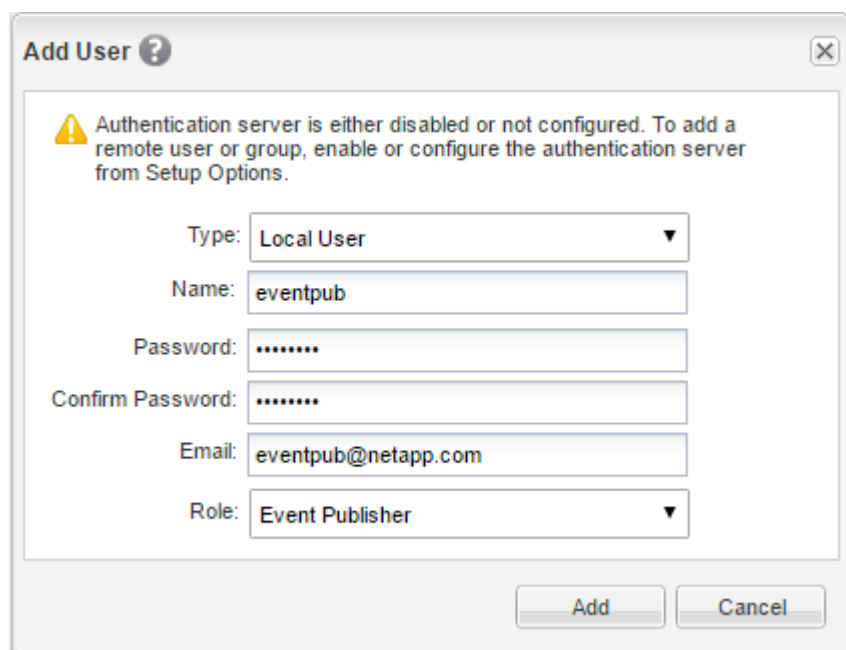


Link OnCommand Performance Manager and OnCommand Unified Manager

To link OnCommand Performance Manager and OnCommand Unified Manager, complete the following steps:

1. Select the icon in the upper left-hand corner of the OnCommand Unified Manager web interface and select Health.

2. In the upper right, use the Administration drop-down to select Manage Users.
3. In the upper left, click Add to add a user.
4. Name the user eventpub and enter and confirm a password. Enter an e-mail address for this user that is different than the admin e-mail entered earlier for OnCommand Unified Manager. Select the Event Publisher Role.



Add User ? [X]

⚠ Authentication server is either disabled or not configured. To add a remote user or group, enable or configure the authentication server from Setup Options.

Type: Local User ▼

Name: eventpub

Password:

Confirm Password:

Email: eventpub@netapp.com

Role: Event Publisher ▼

Add Cancel

5. Click Add to add the user.
6. Back in the vSphere web client, select the OnCommand Performance Manager VM. In the center pane, select Open with Remote Console.
7. Log in to the OnCommand Performance Manager console with the admin user and password.

```

OnCommand Performance Manager - VMware Remote Console
VMRC | || |
ocpm login: admin
Password:
Linux OnCommand 3.2.0-4-amd64 #1 SMP Debian 3.2.81-1 x86_64

OnCommand Performance Manager Maintenance Console

Version      : 7.0
System ID    : 6ff76dd1-8946-439d-a7c3-ee8950083423
Status       : Running

Main Menu
-----
1 ) Upgrade
2 ) Network Configuration
3 ) System Configuration
4 ) Support/Diagnostics
5 ) Reset Server Certificate
6 ) Unified Manager Integration
7 ) External Data Provider
8 ) Backup/Restore
9 ) Polling Interval Configuration

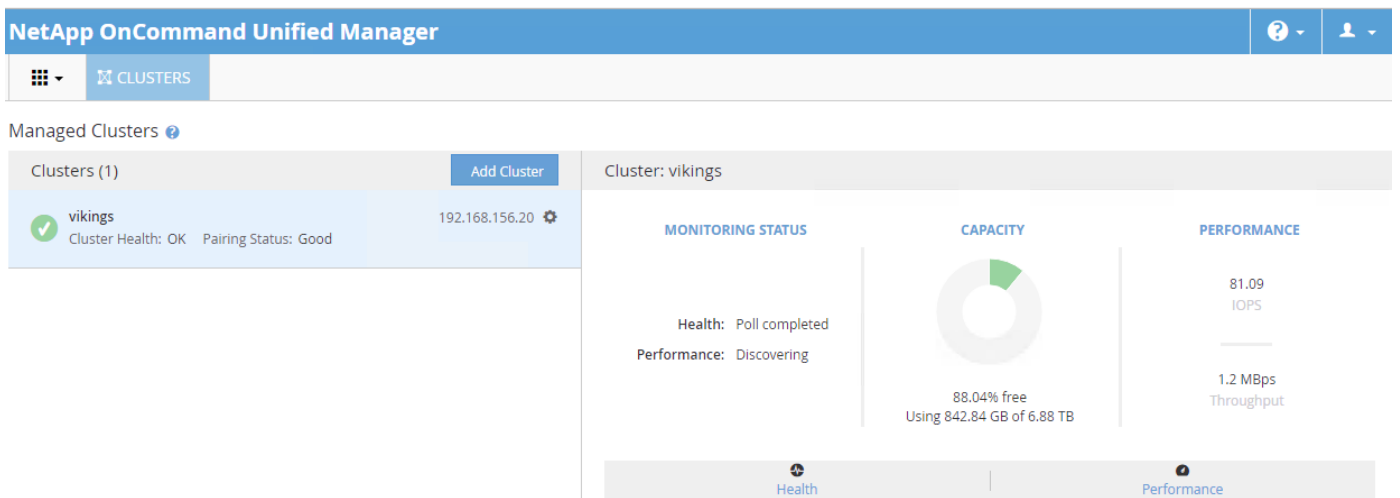
x ) Exit

Enter your choice: _

```

8. Select option 6 for Unified Manager Integration.
9. Select option 1 for full integration.
10. Select option 2 to enable full integration.
11. Enter y to continue.
12. Enter the OnCommand Unified Manager IP address.
13. Enter y to accept the security certificate.
14. Enter admin for the administrator username.
15. Enter the admin password.
16. Enter the event publisher username (eventpub) entered above.
17. Enter the eventpub password.
18. Enter a unique name for the Performance Manager (for example, ocpm-1).
19. Review the settings and enter y if they are correct.

- 20. Press any key to restart the OnCommand Performance Manager service.
- 21. Press any key to continue.
- 22. Enter option 1 to display the full integration settings.
- 23. Press any key to continue.
- 24. Log out of the OnCommand Performance Manager console and return to the OnCommand Unified Manager web interface.
- 25. Using the icon in the upper left-hand corner, bring up the OnCommand Unified Manager dashboard.
- 26. Select the storage cluster on the left. Verify that the pairing status is now Good and that performance numbers show up on the right under Performance.



Sample Tenant Provisioning

Provisioning a Sample Application Tenant

This section provides a sample procedure for provisioning an application tenant. The procedure refers to previous sections of this document and can be used as a guide and modified as needed when provisioning an application tenant.

1. Plan your application tenant and determine what storage protocols will be provided in the tenant. In the architecture covered in this document, fiber channel, NFS, iSCSI, and CIFS/SMB can be provided to the tenant. Also, plan what network VLANs the tenant will use. It is recommended to have a VLAN for virtual machine management traffic. One or two VLANs (iSCSI needs two if VMware RDM LUNs or iSCSI datastores will be provisioned) are also needed for each storage protocol used except fiber channel. Fiber channel will have new storage LIFs defined with the same VSANs configured for the FlexPod Infrastructure.
2. In the Nexus 9372s, declare all added VLANs and configure the VM VLAN as an allowed VLAN on the UCS port channels and the vPC peer link. Also, Layer 3 with HSRP or VRRP can be configured in the Nexus 9372 switches to provide this VLAN access to the outside. Layer 3 setup is not covered in this document, but is covered in the Nexus 9000 documentation. Configure the storage VLANs on the UCS and storage port channels, and on the vPC peer link. The VM VLAN can also be added to the storage port channels in order to configure the tenant SVM management interface on this VLAN.
3. In the storage cluster:
 - a. Create a broadcast domain with MTU 1500 for the tenant SVM management interface. Create a broadcast domain with MTU 9000 for each tenant storage protocol except fiber channel.
 - b. Create VLAN interface ports on the node interface group on each node for tenant SVM management (VM VLAN) and for the VLAN for each storage protocol except fiber channel. Add these VLAN ports to the appropriate broadcast domains.
 - c. Create the tenant SVM and follow all procedures in that section.
 - d. Create Load-Sharing Mirrors for the tenant SVM.
 - e. Create the FC service for the tenant SVM if fiber channel is being deployed in this tenant.
 - f. Optionally, create a self-signed security certificate for the tenant SVM.
 - g. Configure NFSv3 for the tenant SVM.
 - h. Create a VM datastore volume in the tenant SVM.
 - i. Create a once-a-day deduplication schedule on the VM datastore volume.
 - j. If fiber channel is being deployed in this tenant, configure four FCP LIFs in the tenant SVM on the same fiber channel ports as in the Infrastructure SVM.
 - k. Create an NFS LIF in the tenant SVM on the same node as the VM datastore volume.
 - l. Create a boot LUN in the esxi_boot volume in the Infra-SVM for each tenant VMware ESXi host.

- m. Add the tenant SVM Administrator, SVM management LIF on the SVM management VLAN port, and default route for the SVM.
4. In the UCS one method of tenant setup is to dedicate a VMware ESXi cluster and set of UCS servers to each tenant. Service profiles will be generated for at least two tenant ESXi hosts. These hosts can boot from LUNs from the esxi_boot volume in the Infra-SVM, but will also have access to FC storage in the tenant SVM.
 - a. Create a Server Pool for the tenant ESXi host servers.
 - b. Create all tenant VLANs in the LAN Cloud.
 - c. Add the tenant VLANs to the DVS vNIC templates.



If setting up iSCSI VLANs, you are not using the Nexus 1000V, and you will have iSCSI datastores or iSCSI RDM mapped LUNs, add the iSCSI VLANs to the Infra vNIC templates so that the VMkernel ports can be placed on vSwitch0. Testing has shown that unless these VMkernel ports are placed on a vSwitch or a Nexus 1000V with System VLANs, on host reboot iSCSI storage mapped on VMkernel ports will not be mapped until a manual rescan of the Software iSCSI Initiator is completed.

- d. Generate service profiles from the service profile template with the vMedia policy for the tenant ESXi hosts. Remember to bind these service profiles to the service profile template without the vMedia policy after VMware ESXi installation.
5. In the Cisco MDS 9148S switches:
 - a. Create device aliases for the tenant ESXi host vHBAs and the FC LIFs in the tenant storage SVM.
 - b. Create zones for the tenant ESXi hosts with fiber channel targets from both the storage Infra-SVM and the tenant SVM.
 - c. Add these zones to the Fabric zoneset and activate the zoneset.
 6. In the storage cluster:
 - a. Create igroups for the tenant ESXi hosts in both the Infra-SVM and tenant SVM. Also, create an igroup in the tenant SVM that includes the WWPNs for all tenant ESXi hosts to support shared storage from the tenant SVM.
 - b. In Infra-SVM, map the boot LUNs created earlier to the tenant ESXi hosts. Tenant FC storage can be created later using either NetApp VSC or NetApp SnapDrive.
 7. Install and configure VMware ESXi on all tenant host servers. Map the infra_swap datastore and set it to the swap datastore on each host. It is not necessary to map infra_datastore_1.
 8. In VMware vCenter, create a cluster for the tenant ESXi hosts, remembering to set the cluster to use the swap datastore specified by the host. Add the hosts to the cluster.
 9. Using the vCenter Web Client, add the tenant hosts to the VMware vDS. In the VMware vDS, add port-profiles for the tenant VLANs.

10. Back in vCenter, add in any necessary VMkernel ports for storage interfaces remembering to set the MTU correctly on these interfaces. Mount the tenant NFS datastore on the tenant cluster if one was created.
11. Using the NetApp VSC plugin to the vCenter Web Client, set recommended values for all tenant ESXi hosts. Install the NetApp NFS Plug-in for VMware VAAI for all tenant hosts and reboot each host. Optionally, create a VSC backup job for the tenant NFS datastore.
12. You can now begin provisioning virtual machines on the tenant cluster. The NetApp VSC plugin can be used to provision both fiber channel and NFS datastores.

Appendix

Cisco UCS Direct Storage Connect Base Configuration

This FlexPod deployment will show configuration steps for both the Cisco UCS 6332-16UP and Cisco UCS 6248UP Fabric Interconnects (FI) in a design that will support Fibre Channel connectivity to the NetApp AFF through the Cisco MDS.

Configuration steps will be referenced for both fabric interconnects and will be called out by the specific model where steps have differed.

This section contains the Cisco UCS deployment for when the Cisco MDS is used as the fiber channel SAN switches.

Perform Initial Setup of Cisco UCS 6332-16UP and 6248UP Fabric Interconnects for FlexPod Environments

This section provides detailed procedures for configuring the Cisco Unified Computing System (Cisco UCS) for use in a FlexPod environment. The steps are necessary to provision the Cisco UCS B-Series and C-Series servers and should be followed precisely to avoid improper configuration.

Cisco UCS Fabric Interconnect A

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

1. Connect to the console port on the first Cisco UCS fabric interconnect.

```
Enter the configuration method: gui
```

```
Physical switch Mgmt0 IP address: <ucsa-mgmt-ip>
```

```
Physical switch Mgmt0 IPv4 netmask: <ucsa-mgmt-mask>
```

```
IPv4 address of the default gateway: <ucsa-mgmt-gateway>
```

2. Using a supported web browser, connect to <https://<ucsa-mgmt-ip>>, accept the security prompts, and click the 'Express Setup' link under HTML.
3. Select Initial Setup and click Submit.
4. Select Enable clustering, Fabric A, and IPv4.
5. Fill in the Virtual IP Address with the UCS cluster IP.
6. Completely fill in the System setup section. For system name, use the overall UCS system name. For the Mgmt IP Address, use <ucsa-mgmt-ip>.

| | |
|--|--|
| <input checked="" type="radio"/> Enable clustering <input type="radio"/> Standalone mode <input type="radio"/> Synchronize | |
| Fabric Setup: <input checked="" type="radio"/> Fabric A <input type="radio"/> Fabric B | |
| <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 | |
| Virtual IP Address: <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="156"/> . <input type="text" value="50"/> | |
| System setup | |
| Enforce strong password?: <input checked="" type="radio"/> Yes <input type="radio"/> No | |
| System name: <input type="text" value="d04-6248"/> | |
| Admin Password: <input type="password" value="*****"/> | Confirm Admin password: <input type="password" value="*****"/> |
| Mgmt IP Address: <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="156"/> . <input type="text" value="51"/> | Mgmt IP Netmask: <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/> |
| Default Gateway: <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="156"/> . <input type="text" value="1"/> | |
| DNS Server IP: <input type="text" value="10"/> . <input type="text" value="1"/> . <input type="text" value="156"/> . <input type="text" value="9"/> | Domain Name : <input type="text" value="vikings.cisco.com"/> |
| UCS Central managed environment | |
| UCS Central IP: <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> | Shared Secret: <input type="text"/> |

7. Click Submit.

Cisco UCS Fabric Interconnect B

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

1. Connect to the console port on the second Cisco UCS fabric interconnect.

Enter the configuration method: `gui`

Physical switch Mgmt0 IP address: `<ucsb-mgmt-ip>`

Physical switch Mgmt0 IPv4 netmask: `<ucsb-mgmt-mask>`

IPv4 address of the default gateway: `<ucsb-mgmt-gateway>`

2. Using a supported web browser, connect to <https://<ucsb-mgmt-ip>>, accept the security prompts, and click the 'Express Setup' link under HTML.
3. Under System setup, enter the Admin Password entered above and click Submit.
4. Enter <ucsb-mgmt-ip> for the Mgmt IP Address and click Submit.

Cisco UCS Direct Storage Connect Setup

Log in to Cisco UCS Manager



The following steps are the same between the UCS 6332-16UP and the UCS 6248UP Fabric Interconnects unless otherwise noted.

To log in to the Cisco Unified Computing System (UCS) environment, complete the following steps:

1. Open a web browser and navigate to the Cisco UCS fabric interconnect cluster address.



You may need to wait at least 5 minutes after configuring the second fabric interconnect for UCS Manager to come up.

2. Click the Launch UCS Manager link under HTML to launch Cisco UCS Manager.
3. If prompted to accept security certificates, accept as necessary.
4. When prompted, enter admin as the user name and enter the administrative password.
5. Click Login to log in to Cisco UCS Manager.

Upgrade Cisco UCS Manager Software to Version 3.1(2b)

This document assumes the use of Cisco UCS 3.1(2b). To upgrade the Cisco UCS Manager software and the Cisco UCS Fabric Interconnect software to version 3.1(2b), refer to [Cisco UCS Manager Install and Upgrade Guides](#).

Anonymous Reporting

To create anonymous reporting, complete the following step:

1. In the Anonymous Reporting window, select whether to send anonymous data to Cisco for improving future products. If you select Yes, enter the IP address of your SMTP Server. Click OK.

Anonymous Reporting

Cisco Systems, Inc. will be collecting feature configuration and usage statistics which will be sent to Cisco Smart Call Home server anonymously. This data helps us prioritize the features and improvements that will most benefit our customers.

If you decide to enable this feature in future, you can do so from the "Anonymous Reporting" in the Call Home settings under the Admin tab.

[View Sample Data](#)

Do you authorize the disclosure of this information to Cisco Smart CallHome?

Yes No

Don't show this message again.

OK Cancel

Configure Cisco UCS Call Home

Cisco highly recommends configuring Call Home in Cisco UCS Manager. Configuring Call Home will accelerate resolution of support cases. To configure Call Home, complete the following steps:

1. In Cisco UCS Manager, click Admin on the left.
2. Select All > Communication Management > Call Home.
3. Change the State to On.
4. Fill in all the fields according to your Management preferences and click Save Changes and click OK to complete configuring Call Home.

Place UCS Fabric Interconnects in Fiber Channel Switching Mode

In order to use Fiber Channel Storage Ports for storage directly connected to the Cisco UCS fabric interconnects, the fabric interconnects must be changed from fiber channel end host mode to fiber channel switching mode.

To place the fabric interconnects in fiber channel switching mode, complete the following steps:

1. In Cisco UCS Manager, click Equipment on the left.
2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary).
3. In the center pane, select set FC Switching Mode. Click Yes and OK for the confirmation message.

4. Wait for both Fabric Interconnects to reboot by monitoring the console ports and log back into Cisco UCS Manager.


Configure Unified Ports

Fiber Channel port configurations differ slightly between the 6332-16UP and the 6248UP Fabric Interconnects. Both Fabric Interconnects have a slider mechanism within the Cisco UCS Manager GUI interface, but the fiber channel port selection options for the 6332-16UP are from the first 16 ports starting from the first port on the left, and configured in increments of the first 6, 12, or all 16 of the unified ports. With the 6248UP, the port selection options will start from the right of the 32 fixed ports, or the right of the 16 ports of the expansion module, going down in contiguous increments of 2.

To enable the fiber channel ports, complete the following steps for the 6332-16UP:

1. In Cisco UCS Manager, click Equipment on the left.
2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary).
3. Select Configure Unified Ports.
4. Click Yes on the pop-up window warning that changes to the fixed module will require a reboot of the fabric interconnect and changes to the expansion module will require a reboot of that module.
5. Within the Configured Fixed Ports pop-up window move the gray slider bar from the left to the right to select either 6, 12, or 16 ports to be set as FC Uplinks.

Configure Unified Ports ? X



Instructions

The position of the slider determines the type of the ports.
All the ports to the left of the slider are Fibre Channel ports (Purple), while the ports to the right are Ethernet ports (Blue).

| Port | Transport | If Role or Port Channel Membership | Desired If Role |
|---------|-----------|------------------------------------|-----------------|
| Port 1 | ether | Unconfigured | FC Uplink |
| Port 2 | ether | Unconfigured | FC Uplink |
| Port 3 | ether | Unconfigured | FC Uplink |
| Port 4 | ether | Unconfigured | FC Uplink |
| Port 5 | ether | Unconfigured | FC Uplink |
| Port 6 | ether | Unconfigured | FC Uplink |
| Port 7 | ether | Unconfigured | |
| Port 8 | ether | Unconfigured | |
| Port 9 | ether | Unconfigured | |
| Port 10 | ether | Unconfigured | |
| Port 11 | ether | Unconfigured | |
| Port 12 | ether | Unconfigured | |
| Port 13 | ether | Unconfigured | |
| Port 14 | ether | Unconfigured | |
| Port 15 | ether | Unconfigured | |
| Port 16 | ether | Unconfigured | |

6. Click OK, then Yes, then OK to continue
7. Select Equipment > Fabric Interconnects > Fabric Interconnect B (primary)
8. Select Configure Unified Ports.
9. Click Yes on the pop-up window warning that changes to the fixed module will require a reboot of the fabric interconnect and changes to the expansion module will require a reboot of that module.
10. Within the Configured Fixed Ports pop-up window move the gray slider bar from the left to the right to select either 6, 12, or 16 ports to be set as FC Uplinks.
11. Click OK, then Yes, then OK to continue.
12. Wait for both Fabric Interconnects to reboot.
13. Log back into UCS Manager.

To enable the fiber channel ports, complete the following steps for the 6248UP:

1. In Cisco UCS Manager, click Equipment on the left.

2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary)
3. Select Configure Unified Ports.
4. Click Yes in the pop-up window warning that changes to the fixed module will require a reboot of the fabric interconnect and changes to the expansion module will require a reboot of that module.
5. Configure the Fixed Module Ports from the subsequent Configure Fixed Module Ports pop-up window, or click on the Configure Expansion Module Ports button to select from expansion module ports.
6. Within either option, move the gray slider bar from the right to the left selecting ports in increments of two to set as FC Uplinks.

Configure Unified Ports ? X

Instructions

The position of the slider determines the type of the ports.
 All the ports to the left of the slider are Ethernet ports (Blue), while the ports to the right are Fibre Channel ports (Purple).

| Port | Transport | If Role or Port Channel Membership | Desired If Role |
|---------|-----------|------------------------------------|-----------------|
| Port 1 | ether | Unconfigured | |
| Port 2 | ether | Unconfigured | |
| Port 3 | ether | Unconfigured | |
| Port 4 | ether | Unconfigured | |
| Port 5 | ether | Unconfigured | |
| Port 6 | ether | Unconfigured | |
| Port 7 | ether | Unconfigured | |
| Port 8 | ether | Unconfigured | |
| Port 9 | ether | Unconfigured | |
| Port 10 | ether | Unconfigured | |
| Port 11 | ether | Unconfigured | |
| Port 12 | ether | Unconfigured | |
| Port 13 | ether | Unconfigured | |
| Port 14 | ether | Unconfigured | |
| Port 15 | ether | Unconfigured | |

7. Click Finish. Click Yes to confirm. Click OK.
8. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate)
9. Select Configure Unified Ports.

10. Click Yes in the pop-up window warning that changes to the fixed module will require a reboot of the fabric interconnect and changes to the expansion module will require a reboot of that module.
11. Configure the Fixed Module Ports from the subsequent Configure Fixed Module Ports pop-up window, or click on the Configure Expansion Module Ports button to select from expansion module ports.
12. Within either option move the gray slider bar from the right to the left selecting ports in increments of two to set as FC Uplinks.
13. Click Finish. Click Yes on the confirmation. Click OK.
14. Wait for both Fabric Interconnects to reboot by monitoring the console ports.
15. Log back into Cisco UCS Manager.

Add Block of IP Addresses for KVM Access

To create a block of IP addresses for in band server Keyboard, Video, Mouse (KVM) access in the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click LAN on the left.
2. Expand Pools > root > IP Pools.
3. Right-click IP Pool ext-mgmt and select Create Block of IPv4 Addresses.
4. Enter the starting IP address of the block, number of IP addresses required, and the subnet mask and gateway information.

Create Block of IPv4 Addresses ? X

| | | | |
|---------------|--|-------------------|--|
| From : | <input type="text" value="192.168.156.101"/> | Size : | <input type="text" value="12"/> |
| Subnet Mask : | <input type="text" value="255.255.255.0"/> | Default Gateway : | <input type="text" value="192.168.156.1"/> |
| Primary DNS : | <input type="text" value="0.0.0.0"/> | Secondary DNS : | <input type="text" value="0.0.0.0"/> |


OK Cancel

5. Click OK to create the block.
6. Click OK in the confirmation message.

Synchronize Cisco UCS to NTP

To synchronize the Cisco UCS environment to the NTP servers in the Nexus 9372 switches, complete the following steps:

1. In Cisco UCS Manager, click Admin on the left.
2. Expand All > Time Zone Management.
3. Select Timezone.
4. In the Properties pane, select the appropriate time zone in the Time Zone pulldown.
5. Click Save Changes and then click OK.
6. Click Add NTP Server.
7. Enter <switch-a-ntp-ip> and click OK. Click OK to confirm.



The screenshot shows a dialog box titled "Add NTP Server". The dialog has a title bar with a question mark icon and a close button (X). The main content area contains the text "NTP Server :" followed by a text input field containing the IP address "10.1.156.4". At the bottom right of the dialog, there are two buttons: "OK" (blue) and "Cancel" (white with a grey border).

8. Click Add NTP Server.
9. Enter <switch-b-ntp-ip> and click OK. Click OK to confirm.

All / Time Zone Management / Timezone

General

Events

Actions

Add NTP Server

Properties

Time Zone : America/New_York (Eastern) ▼

NTP Servers

▼ Advanced Filter ↑ Export 🖨 Print

| Name |
|-----------------------|
| NTP Server 10.1.156.4 |
| NTP Server 10.1.156.5 |

Edit Chassis Discovery Policy

Setting the discovery policy simplifies the addition of B-Series Cisco UCS chassis and of additional fabric extenders for further C-Series connectivity. To modify the chassis discovery policy, complete the following steps:

1. In Cisco UCS Manager, click Equipment on the left and select Equipment in the second list.
2. In the right pane, click the Policies tab.
3. Under Global Policies, set the Chassis/FEX Discovery Policy to match the minimum number of uplink ports that are cabled between the chassis or fabric extenders (FEXes) and the fabric interconnects.
4. Set the Link Grouping Preference to Port Channel. If Backplane Speed Preference appears, leave it set at 40G. If the environment being setup contains a large amount of multicast traffic, set the Multicast Hardware Hash setting to Enabled.

Equipment

<
Fabric Interconnects
Servers
Thermal
Decommissioned
Firmware Management
Policies
Faults
>
>>

<
Global Policies
Autoconfig Policies
Server Inheritance Policies
Server Discovery Policies
SEL Policy
Po>
>>

Chassis/FEX Discovery Policy

Action : 2 Link ▼

Link Grouping Preference :
 None Port Channel

Multicast Hardware Hash :
 Disabled Enabled

5. Click Save Changes.

6. Click OK.

Enable Server and Uplink Ports

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

1. In Cisco UCS Manager, click Equipment on the left.
2. Expand Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module.
3. Expand Ethernet Ports.
4. Select the ports that are connected to the chassis, Cisco FEX, and direct connect UCS C-Series servers, right-click them, and select **“Configure as Server Port.”**
5. Click Yes to confirm server ports and click OK.
6. Verify that the ports connected to the chassis, C-series servers and Cisco FEX are now configured as server ports.
7. Select the ports that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.



The last 6 ports of the Cisco UCS 6332 and Cisco UCS 6332-16UP FIs will only work with optical based QSFP transceivers and AOC cables, so they can be better utilized as uplinks to upstream resources that might be optical only.

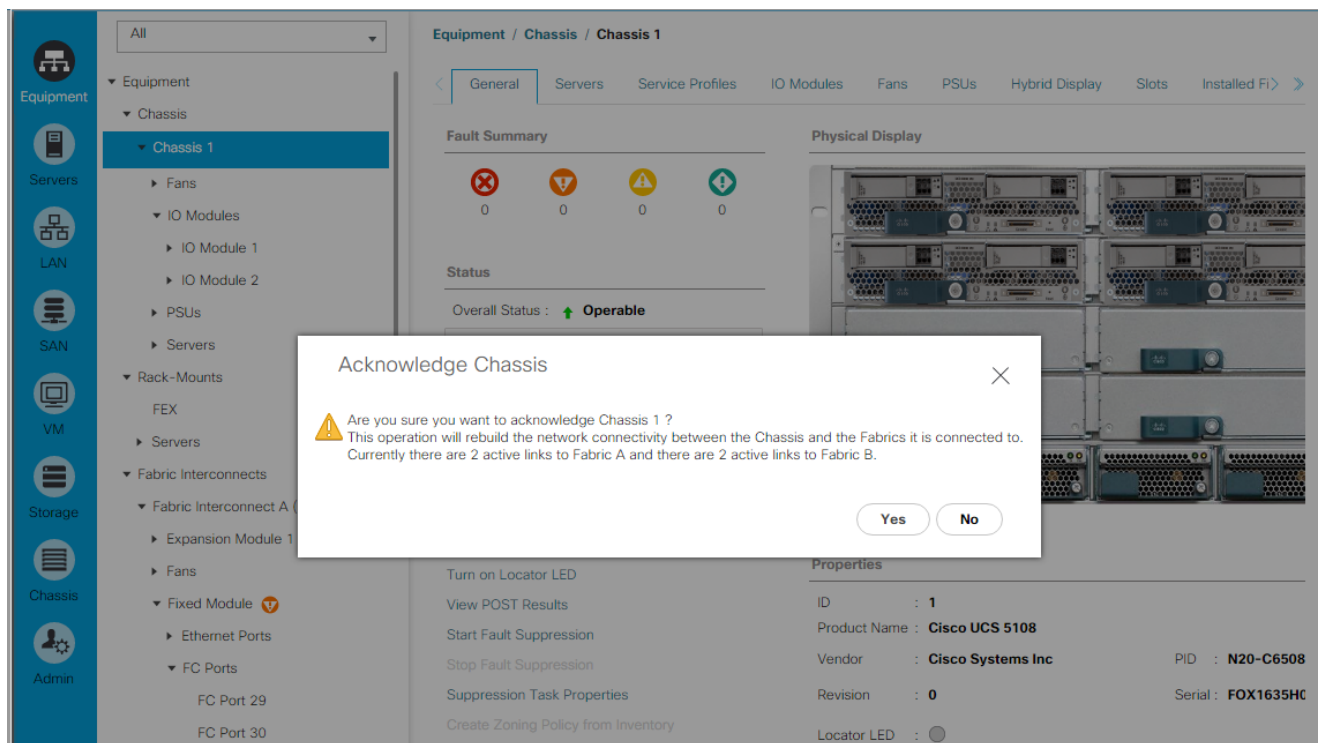
8. Click Yes to confirm uplink ports and click OK.
9. Expand FC Ports under Fabric Interconnect A.
10. Select the ports that are connected to the NetApp storage controllers, right-click them, and select Configure as FC Storage Port.
11. Click Yes to confirm FC Storage ports and click OK.
12. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.
13. Expand Ethernet Ports.
14. Select the ports that are connected to the chassis, C-series servers or to the Cisco 2232 FEX (two per FEX), right-click them, and select Configure as Server Port.
15. Click Yes to confirm server ports and click OK.
16. Select the ports that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.
17. Click Yes to confirm the uplink ports and click OK.

18. Expand FC Ports under Fabric Interconnect A.
19. Select the ports that are connected to the NetApp storage controllers, right-click them, and select Configure as FC Storage Port.
20. Click Yes to confirm FC Storage ports and click OK.

Acknowledge Cisco UCS Chassis and FEX

To acknowledge all Cisco UCS chassis and any external 2232 FEX modules, complete the following steps:

1. In Cisco UCS Manager, click Equipment on the left.
2. Expand Chassis and select each chassis that is listed.
3. Right-click each chassis and select Acknowledge Chassis.



4. Click Yes and then click OK to complete acknowledging the chassis.
5. If Nexus 2232 FEX are part of the configuration, expand Rack Mounts and FEX.
6. Right-click each FEX that is listed and select Acknowledge FEX.
7. Click Yes and then click OK to complete acknowledging the FEX.

Create Uplink Port Channels to Cisco Nexus Switches

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

1. In Cisco UCS Manager, click LAN on the left.



In this procedure, two port channels are created: one from fabric A to both Cisco Nexus switches and one from fabric B to both Cisco Nexus switches.

2. Under LAN > LAN Cloud, expand the Fabric A tree.
3. Right-click Port Channels.
4. Select Create Port Channel.
5. Enter 13 as the unique ID of the port channel.
6. Enter vPC-13-Nexus as the name of the port channel.
7. Click Next.
8. Select the ports connected to the Nexus switches to be added to the port channel:
9. Click >> to add the ports to the port channel.
10. Click Finish to create the port channel.
11. Click OK.
12. In the navigation pane, under LAN > LAN Cloud, expand the fabric B tree.
13. Right-click Port Channels.
14. Select Create Port Channel.
15. Enter 14 as the unique ID of the port channel.
16. Enter vPC-14-Nexus as the name of the port channel.
17. Click Next.
18. Select the ports connected to the Nexus switches to be added to the port channel:
19. Click >> to add the ports to the port channel.
20. Click Finish to create the port channel.
21. Click OK.

Create a WWNN Pool for FC Boot

To configure the necessary WWNN pool for the Cisco UCS environment, complete the following steps on Cisco UCS Manager.

1. Select SAN on the left.
2. Select Pools > root.
3. Right-click WWNN Pools under the root organization.
4. Select Create WWNN Pool to create the WWNN pool.
5. Enter WWNN-Pool for the name of the WWNN pool.
6. Optional: Enter a description for the WWNN pool.
7. Select Sequential for Assignment Order.

The screenshot shows the 'Create WWNN Pool' configuration window. The left sidebar has two steps: '1 Define Name and Description' (highlighted) and '2 Add WWN Blocks'. The main area contains three fields: 'Name' with the value 'WWNN-Pool', 'Description' (empty), and 'Assignment Order' with radio buttons for 'Default' and 'Sequential' (selected). At the bottom are buttons for '< Prev', 'Next >', 'Finish', and 'Cancel'.

8. Click Next.
9. Click Add.
10. Modify the From field as necessary for the UCS Environment.

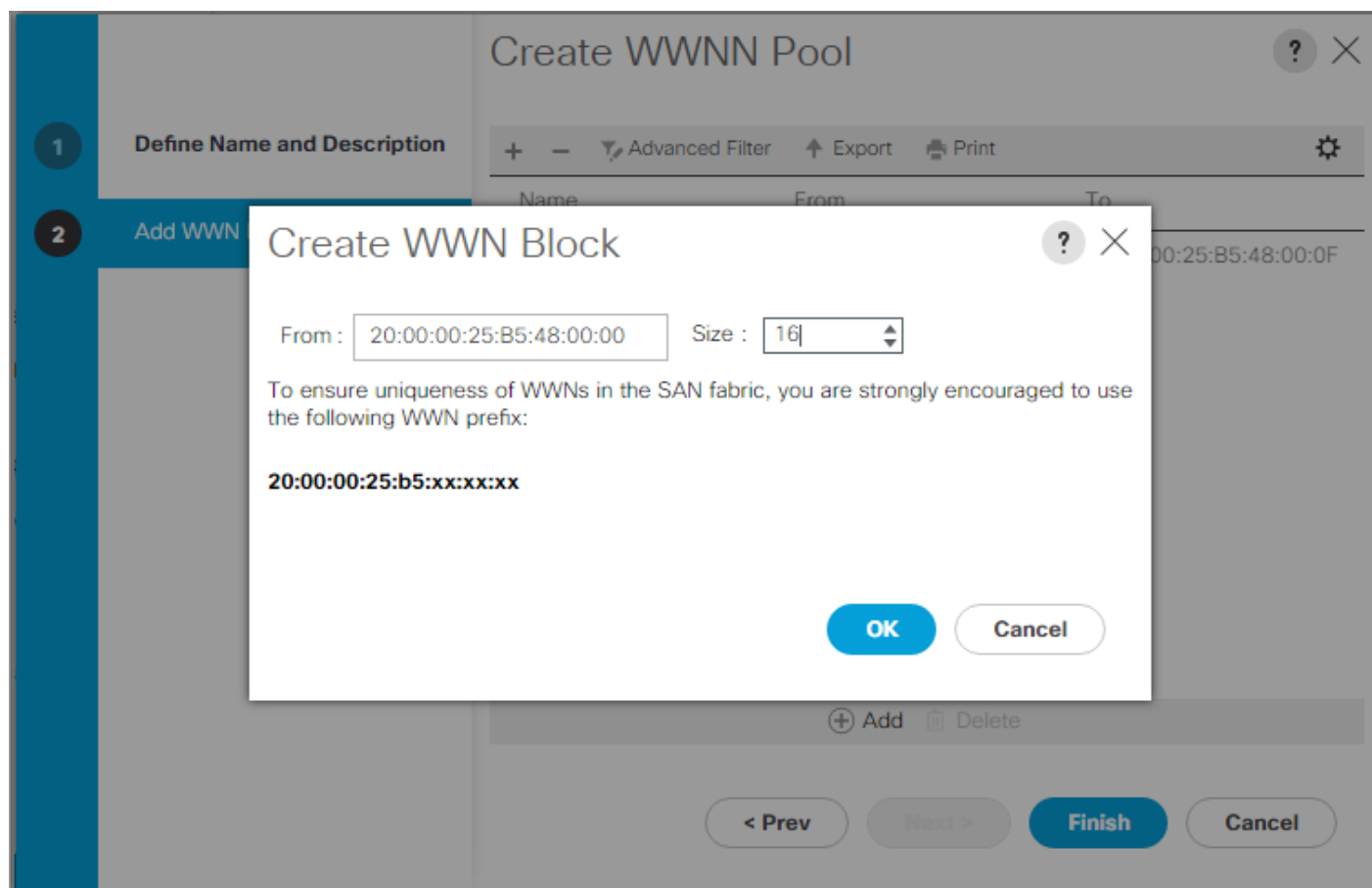


Modifications of the WWNN block, as well as the WWPN and MAC Addresses, can convey identifying information for the Cisco UCS domain. Within the From field in our example, the 6th octet was changed from 00 to 48 to represent as identifying information for this being in the Cisco UCS 6248 in the 4th cabinet.



Also, when having multiple Cisco UCS domains sitting in adjacency, it is important that these blocks, the WWNN, WWPN, and MAC hold differing values between each set.

- Specify a size of the WWNN block sufficient to support the available server resources.



- Click OK.

- Click Finish and OK to complete creating the WWNN pool.

Create WWPN Pools

To configure the necessary WWPN pools for the Cisco UCS environment, complete the following steps:

- In Cisco UCS Manager, click SAN on the left.
- Select Pools > root.
- In this procedure, two WWPN pools are created, one for each switching fabric.
- Right-click WWPN Pools under the root organization.
- Select Create WWPN Pool to create the WWPN pool.

6. Enter WWPN-Pool-A as the name of the WWPN pool.
7. Optional: Enter a description for the WWPN pool.
8. Select Sequential for Assignment Order.

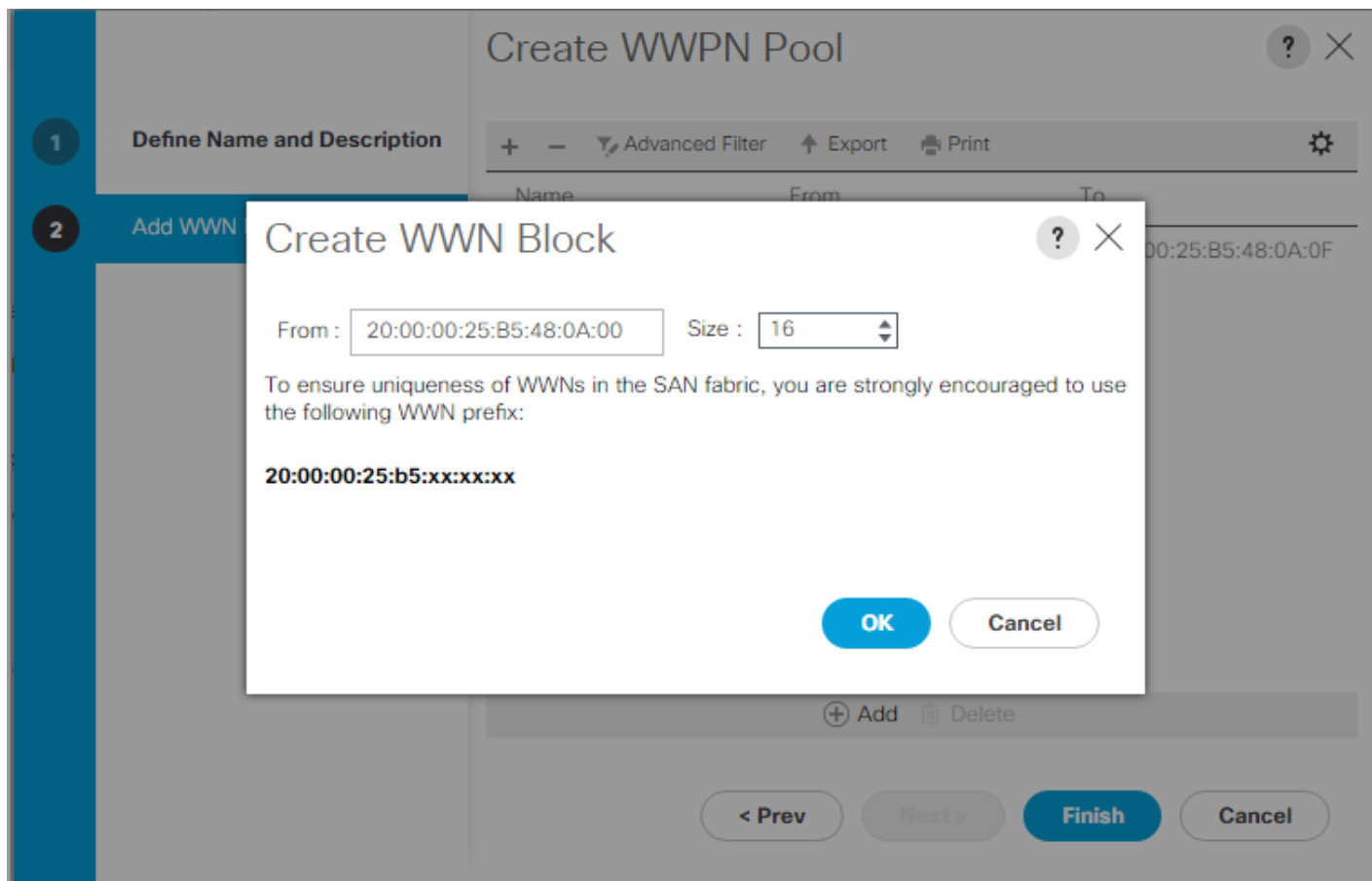
The screenshot shows a configuration window titled "Create WWPN Pool". On the left, a blue sidebar contains two steps: "1 Define Name and Description" (which is currently active) and "2 Add WWN Blocks". The main content area has three input fields: "Name" with the value "WWPP-Pool-A", "Description" (empty), and "Assignment Order" with radio buttons for "Default" and "Sequential" (the latter is selected). At the bottom of the window are four buttons: "< Prev", "Next >", "Finish", and "Cancel".

9. Click Next.
10. Click Add.
11. Specify a starting WWPN.



For the FlexPod solution, the recommendation is to place 0A in the next-to-last octet of the starting WWPN to identify all of the WWPNs as fabric A addresses. Merging this with the pattern we used for the WWNN we see a WWPN block starting with 20:00:00:25:B5:48:0A:00.

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



13. Click OK.
14. Click Finish.
15. In the confirmation message, click OK.
16. Right-click WWPN Pools under the root organization.
17. Select Create WWPN Pool to create the WWPN pool.
18. Enter WWPN-Pool-B as the name of the WWPN pool.
19. Optional: Enter a description for the WWPN pool.
20. Select Sequential for Assignment Order.
21. Click Next.
22. Click Add.
23. Specify a starting WWPN.



For the FlexPod solution, the recommendation is to place 0B in the next-to-last octet of the starting WWPN to identify all of the WWPNs as fabric A addresses. Merging this with the pattern we used for the WWNN we see a WWPN block starting with 20:00:00:25:B5:48:0B:00.

24. Specify a size for the WWPN address pool that is sufficient to support the available blade or server resources.
25. Click OK.
26. Click Finish.
27. In the confirmation message, click OK.

Create Storage VSANs

To configure the necessary virtual storage area networks (VSANs) for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the SAN on the left.



In this procedure, two VSANs are created.

2. Select SAN > Storage Cloud.
3. Right-click VSANs.
4. Select Create Storage VSAN.
5. Enter VSAN-A as the name of the VSAN to be used for Fabric A
6. Set FC Zoning to Enabled.
7. Select Fabric A.
8. Enter a unique VSAN ID and a corresponding FCoE VLAN ID for Fabric A. It is recommended to use the same ID for both parameters and to use something other than 1.

Create Storage VSAN ? X

Name :

FC Zoning Settings

FC Zoning : Disabled Enabled

Do **NOT** enable local zoning if fabric interconnect is connected to an upstream FC/FCoE switch.

Common/Global Fabric A Fabric B Both Fabrics Configured Differently

You are creating a local VSAN in fabric A that maps to a VSAN ID that exists only in fabric A.

Enter the VSAN ID that maps to this VSAN.

VSAN ID :

A VLAN can be used to carry FCoE traffic and can be mapped to this VSAN.

Enter the VLAN ID that maps to this VSAN.

FCoE VLAN :

9. Click OK, and then click OK again.
10. Under Storage Cloud, right-click VSANs.
11. Select Create Storage VSAN.
12. Enter VSAN-B as the name of the VSAN to be used for Fabric B.
13. Set FC Zoning to Enabled.
14. Select Fabric B.
15. Enter a unique VSAN ID and a corresponding FCoE VLAN ID for Fabric B. It is recommended use the same ID for both parameters and to use something other than 1.

Create Storage VSAN ? X

Name :

FC Zoning Settings

FC Zoning : Disabled Enabled

Do **NOT** enable local zoning if fabric interconnect is connected to an upstream FC/FCoE switch.

Common/Global Fabric A Fabric B Both Fabrics Configured Differently

You are creating a local VSAN in fabric B that maps to a VSAN ID that exists only in fabric B.

Enter the VSAN ID that maps to this VSAN.

VSAN ID :

A VLAN can be used to carry FCoE traffic and can be mapped to this VSAN.

Enter the VLAN ID that maps to this VSAN.

FCoE VLAN :

16. Click OK, and then click OK again.

Assign VSANs to FC Storage Ports

To assign storage VSANs to FC Storage Ports, complete the following steps:

1. In Cisco UCS Manager, click SAN on the left.
2. Select SAN > Storage Cloud.
3. Expand Fabric A and Storage FC Interfaces.
4. Select the first FC Interface.
5. For User Label, enter the storage controller name and port. Click Save Changes and OK.
6. Use the pulldown to select VSAN VSAN-A. Click Save Changes and OK.

SAN / Storage Cloud / Fabric A / Storage FC... / FC Interfac...

General Faults Events

| Actions | Properties |
|-------------------|--|
| Enable Interface | ID : 29 Slot ID |
| Disable Interface | Fabric ID : A |
| | User Label : vikings-01:0g |
| | Port Type : Physical Network Type |
| | Transport Type : Fc Role |
| | Locale : External Port |
| | VSAN : Fabric A/vsan VSAN-A Fill Pattern |

7. Select the second FC Interface.
8. For User Label, enter the storage controller name and port. Click Save Changes and OK.
9. Use the pulldown to select VSAN VSAN-A. Click Save Changes and OK.
10. Expand Fabric B and Storage FC Interfaces.
11. Select the first FC Interface.
12. For User Label, enter the storage controller name and port. Click Save Changes and OK.
13. Use the pulldown to select VSAN VSAN-B. Click Save Changes and OK.
14. Select the second FC Interface.
15. For User Label, enter the storage controller name and port. Click Save Changes and OK.
16. Use the pulldown to select VSAN VSAN-B. Click Save Changes and OK.

Create vHBA Templates

To create the necessary virtual host bus adapter (vHBA) templates for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click SAN on the left.
2. Select Policies > root.

3. Right-click vHBA Templates.
4. Select Create vHBA Template.
5. Enter vHBA-Template-A as the vHBA template name.
6. Keep Fabric A selected.
7. Leave Redundancy Type set to No Redundancy.
8. Select VSAN-A.
9. Leave Initial Template as the Template Type.
10. Select WWPN-Pool-A as the WWPN Pool.
11. Click OK to create the vHBA template.
12. Click OK.

Create vHBA Template ? X

Name : vHBA-Template-A

Description :

Fabric ID : A B

Redundancy

Redundancy Type : No Redundancy Primary Template Secondary Template

Select VSAN : VSAN-A

Template Type : Initial Template Updating Template

Max Data Field Size : 2048

WWPN Pool : WWPN-Pool-A(16/16) ▼

QoS Policy : <not set> ▼

Pin Group : <not set> ▼

Stats Threshold Policy : default ▼

13. Right-click vHBA Templates.
14. Select Create vHBA Template.
15. Enter vHBA-Template-B as the vHBA template name.
16. Leave Redundancy Type set to No Redundancy.
17. Select Fabric B as the Fabric ID.
18. Select VSAN-B.
19. Leave Initial Template as the Template Type.
20. Select WWPN-Pool-B as the WWPN Pool.

21. Click OK to create the vHBA template.
22. Click OK.

Create SAN Connectivity Policy

To configure the necessary Infrastructure SAN Connectivity Policy, complete the following steps:

1. In Cisco UCS Manager, click SAN on the left.
2. Select SAN > Policies > root.
3. Right-click SAN Connectivity Policies.
4. Select Create SAN Connectivity Policy.
5. Enter FC-Boot as the name of the policy.
6. Select the previously created WWNN-Pool for the WWNN Assignment.
7. Click the Add button at the bottom to add a vHBA.
8. In the Create vHBA dialog box, enter Fabric-A as the name of the vHBA.
9. Select the Use vHBA Template checkbox.
10. In the vHBA Template list, select vHBA-Template-A.
11. In the Adapter Policy list, select VMWare.

Create vHBA ? X

Name :

Use vHBA Template :

Redundancy Pair : Peer Name :

vHBA Template : Create vHBA Template

Adapter Performance Profile

Adapter Policy : Create Fibre Channel Adapter Policy

12. Click OK.

13. Click the Add button at the bottom to add a second vHBA.

14. In the Create vHBA dialog box, enter Fabric-B as the name of the vHBA.

15. Select the Use vHBA Template checkbox.

16. In the vHBA Template list, select vHBA-Template-B.

17. In the Adapter Policy list, select VMWare.

18. Click OK.

Create SAN Connectivity Policy ? X

Name :

Description :

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

World Wide Node Name

WWNN Assignment:

[Create WWNN Pool](#)

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

| Name | WWPN |
|-----------------|---------|
| ▶ vHBA Fabric-B | Derived |
| ▶ vHBA Fabric-A | Derived |

🗑 Delete ➕ Add ⓘ Modify

19. Click OK to create the SAN Connectivity Policy.

20. Click OK to confirm creation.

Create MAC Address Pools

To configure the necessary MAC address pools for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click LAN on the left.
2. Select Pools > root.



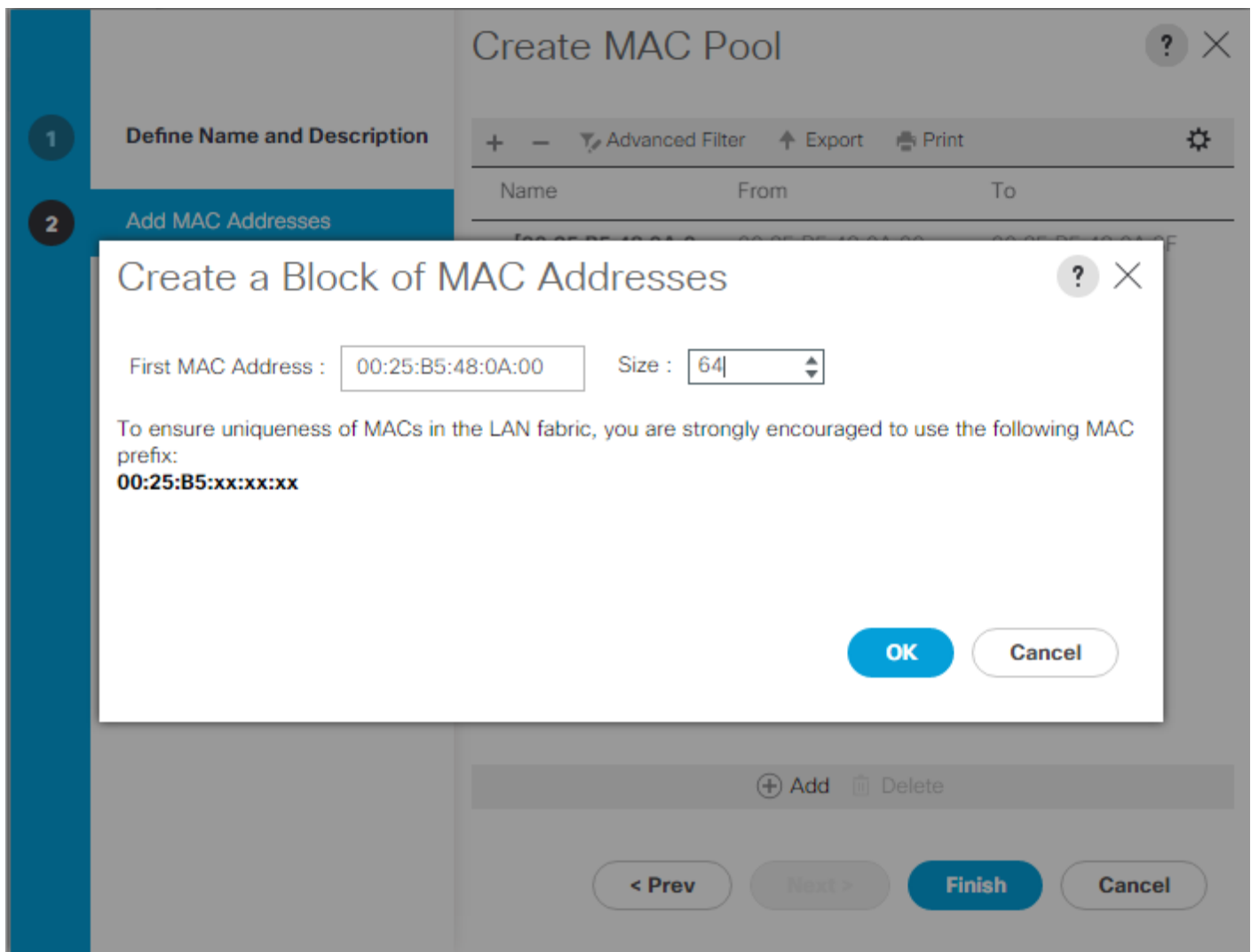
In this procedure, two MAC address pools are created, one for each switching fabric.

3. Right-click MAC Pools under the root organization.
4. Select Create MAC Pool to create the MAC address pool.
5. Enter MAC-Pool-A as the name of the MAC pool.
6. Optional: Enter a description for the MAC pool.
7. Select Sequential as the option for Assignment Order.
8. Click Next.
9. Click Add.
10. Specify a starting MAC address.



For the FlexPod solution, the recommendation is to place 0A in the next-to-last octet of the starting MAC address to identify all of the MAC addresses as fabric A addresses. In our example, we have carried forward the of also embedding the UCS domain number information giving us 00:25:B5:48:0A:00 as our first MAC address.

11. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources, noting that 6 virtual network interfaces (vNICs) will be created on each server.



12. Click OK.
13. Click Finish.
14. In the confirmation message, click OK.
15. Right-click MAC Pools under the root organization.
16. Select Create MAC Pool to create the MAC address pool.
17. Enter MAC-Pool-B as the name of the MAC pool.
18. Optional: Enter a description for the MAC pool.
19. Select Sequential as the option for Assignment Order.
20. Click Next.
21. Click Add.

22. Specify a starting MAC address.



For the FlexPod solution, it is recommended to place 0B in the next to last octet of the starting MAC address to identify all the MAC addresses in this pool as fabric B addresses. Once again, we have carried forward in our example of also embedding the UCS domain number information giving us 00:25:B5:48:0B:00 as our first MAC address.

23. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources.

24. Click OK.

25. Click Finish.

26. In the confirmation message, click OK.

Create UUID Suffix Pool

To configure the necessary universally unique identifier (UUID) suffix pool for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click Servers on the left.
2. Select Pools > root.
3. Right-click UUID Suffix Pools.
4. Select Create UUID Suffix Pool.
5. Enter UUID-Pool as the name of the UUID suffix pool.
6. Optional: Enter a description for the UUID suffix pool.
7. Keep the prefix at the derived option.
8. Select Sequential for the Assignment Order.
9. Click Next.
10. Click Add to add a block of UUIDs.
11. Keep the From field at the default setting.
12. Specify a size for the UUID block that is sufficient to support the available blade or server resources.
13. Click OK.
14. Click Finish.
15. Click OK.

Create Server Pool

To configure the necessary server pool for the Cisco UCS environment, complete the following steps:



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

1. In Cisco UCS Manager, click Servers on the left.
2. Select Pools > root.
3. Right-click Server Pools.
4. Select Create Server Pool.
5. Enter Infra-Pool as the name of the server pool.
6. Optional: Enter a description for the server pool.
7. Click Next.
8. Select two (or more) servers to be used for the VMware management cluster and click >> to add them to the Infra-Pool server pool.
9. Click Finish.
10. Click OK.

Create VLANs

To configure the necessary virtual local area networks (VLANs) for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click LAN on the left.



In this procedure, five unique VLANs are created. See Table 2

2. Select LAN > LAN Cloud.
3. Right-click VLANs.
4. Select Create VLANs.
5. Enter Native-VLAN as the name of the VLAN to be used as the native VLAN.
6. Keep the Common/Global option selected for the scope of the VLAN.
7. Enter the native VLAN ID.
8. Keep the Sharing Type as None.

- Click OK, and then click OK again.

Create VLANs ? X

VLAN Name/Prefix :

Multicast Policy Name : [Create Multicast Policy](#)

Common/Global
 Fabric A
 Fabric B
 Both Fabrics Configured Differently

You are creating global VLANs that map to the same VLAN IDs in all available fabrics.
Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")

VLAN IDs :

Sharing Type : None Primary Isolated Community

- Expand the list of VLANs in the navigation pane, right-click the newly created Native-VLAN and select Set as Native VLAN.
- Click Yes, and then click OK.
- Right-click VLANs.
- Select Create VLANs
- Enter IB-MGMT as the name of the VLAN to be used for management traffic.
- Keep the Common/Global option selected for the scope of the VLAN.
- Enter the In-Band management VLAN ID.
- Keep the Sharing Type as None.
- Click OK, and then click OK again.
- Right-click VLANs.

20. Select Create VLANs.
21. Enter Infra-NFS as the name of the VLAN to be used for NFS.
22. Keep the Common/Global option selected for the scope of the VLAN.
23. Enter the Infrastructure NFS VLAN ID.
24. Keep the Sharing Type as None.
25. Click OK, and then click OK again.
26. Right-click VLANs.
27. Select Create VLANs.
28. Enter vMotion as the name of the VLAN to be used for vMotion.
29. Keep the Common/Global option selected for the scope of the VLAN.
30. Enter the vMotion VLAN ID.
31. Keep the Sharing Type as None.
32. Click OK, and then click OK again.
33. Right-click VLANs.
34. Select Create VLANs.
35. Enter VM-Traffic as the name of the VLAN to be used for VM Traffic.
36. Keep the Common/Global option selected for the scope of the VLAN.
37. Enter the VM-Traffic VLAN ID.
38. Keep the Sharing Type as None.
39. Click OK, and then click OK again.

VLANs

Advanced Filter Export Print

| Name | ID | Type | Transport | Native | VLAN Shar... |
|-----------------------|------|------|-----------|--------|--------------|
| VLAN default (1) | 1 | Lan | Ether | No | None |
| VLAN Native-VLAN (2) | 2 | Lan | Ether | Yes | None |
| VLAN IB-MGMT (113) | 113 | Lan | Ether | No | None |
| VLAN VM-Traffic (900) | 900 | Lan | Ether | No | None |
| VLAN vMotion (3000) | 3000 | Lan | Ether | No | None |
| VLAN Infra-NFS (3050) | 3050 | Lan | Ether | No | None |

+ Add Delete Info

Details

General Org Permissions VLAN Group Membership Faults Events

Fault Summary **Properties**

Modify Default Host Firmware Package

Firmware management policies allow the administrator to select the corresponding packages for a given server configuration. These policies often include packages for adapter, BIOS, board controller, FC adapters, host bus adapter (HBA) option ROM, and storage controller properties.

To create a firmware management policy for a given server configuration in the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click Servers on the left.
2. Select Policies > root.
3. Expand Host Firmware Packages.
4. Select default.
5. In the Actions pane, select Modify Package Versions.
6. Select the version 3.1(2b) for both the Blade and Rack Packages.

Modify Package Versions [X]

Blade Package : 3.1(2b)B ▼

Rack Package : 3.1(2b)C ▼

Excluded Components:

- Adapter
- Host NIC Option ROM
- CIMC
- Board Controller
- Flex Flash Controller
- BIOS
- PSU
- SAS Expander
- Storage Controller Onboard Device
- Storage Device Bridge
- GPUs
- FC Adapters
- Local Disk
- HBA Option ROM

OK Apply Cancel Help

7. Click OK then OK again to modify the host firmware package.

Set Jumbo Frames in Cisco UCS Fabric

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

1. In Cisco UCS Manager, click LAN on the left.
2. Select LAN > LAN Cloud > QoS System Class.
3. In the right pane, click the General tab.

4. On the Best Effort row, enter 9216 in the box under the MTU column.
5. Click Save Changes in the bottom of the window.
6. Click OK.

LAN / LAN Cloud / QoS System Class

| Priority | Enabled | CoS | Packet Drop | Weight | Weight (%) | MTU | Multicast Optimized |
|---------------|-------------------------------------|-----|-------------------------------------|--------|------------|--------|--------------------------|
| Platinum | <input type="checkbox"/> | 5 | <input type="checkbox"/> | 10 | N/A | normal | <input type="checkbox"/> |
| Gold | <input type="checkbox"/> | 4 | <input checked="" type="checkbox"/> | 9 | N/A | normal | <input type="checkbox"/> |
| Silver | <input type="checkbox"/> | 2 | <input checked="" type="checkbox"/> | 8 | N/A | normal | <input type="checkbox"/> |
| Bronze | <input type="checkbox"/> | 1 | <input checked="" type="checkbox"/> | 7 | N/A | normal | <input type="checkbox"/> |
| Best Effort | <input checked="" type="checkbox"/> | Any | <input checked="" type="checkbox"/> | 5 | 50 | 9216 | <input type="checkbox"/> |
| Fibre Channel | <input checked="" type="checkbox"/> | 3 | <input type="checkbox"/> | 5 | 50 | fc | N/A |

Create Local Disk Configuration Policy (Optional)

A local disk configuration for the Cisco UCS environment is necessary if the servers in the environment do not have a local disk.



This policy should not be used on servers that contain local disks.

To create a local disk configuration policy, complete the following steps:

1. In Cisco UCS Manager, click Servers on the left.
2. Select Policies > root.
3. Right-click Local Disk Config Policies.
4. Select Create Local Disk Configuration Policy.
5. Enter SAN-Boot as the local disk configuration policy name.
6. Change the mode to No Local Storage.
7. Click OK to create the local disk configuration policy.

Create Local Disk Configuration Policy ? ×

Name : SAN-Boot

Description :

Mode : No Local Storage ▼

FlexFlash

FlexFlash State : Disable Enable

If **FlexFlash State** is disabled, SD cards will become unavailable immediately.
Please ensure SD cards are not in use before disabling the FlexFlash State.

FlexFlash RAID Reporting State : Disable Enable

8. Click OK.

Create Network Control Policy for Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP)

To create a network control policy that enables CDP and LLDP on virtual network ports, complete the following steps:

1. In Cisco UCS Manager, click LAN on the left.
2. Select Policies > root.
3. Right-click Network Control Policies.
4. Select Create Network Control Policy.
5. Enter Enable-CDP-LLDP as the policy name.
6. For CDP, select the Enabled option.
7. For LLDP, scroll down and select Enabled for both Transmit and Receive.
8. Click OK to create the network control policy.

Create Network Control Policy

CDP : Disabled Enabled

MAC Register Mode : Only Native Vlan All Host Vlans

Action on Uplink Fail : Link Down Warning

MAC Security

Forge : Allow Deny

LLDP

Transmit : Disabled Enabled

Receive : Disabled Enabled

OK **Cancel**

9. Click OK.

Create Power Control Policy

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

1. In Cisco UCS Manager, click Servers tab on the left.
2. Select Policies > root.

3. Right-click Power Control Policies.
4. Select Create Power Control Policy.
5. Enter No-Power-Cap as the power control policy name.
6. Change the power capping setting to No Cap.
7. Click OK to create the power control policy.
8. Click OK.

Create Power Control Policy ? ×

Name :

Description :

Fan Speed Policy :

Power Capping

If you choose **cap**, the server is allocated a certain amount of power based on its priority within its power group. Priority values range from 1 to 10, with 1 being the highest priority. If you choose **no-cap**, the server is exempt from all power capping.

No Cap cap

Cisco UCS Manager only enforces power capping when the servers in a power group require more power than is currently available. With sufficient power, all servers run at full capacity regardless of their priority.

Create Server Pool Qualification Policy (Optional)

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



This example creates a policy for Cisco UCS B-Series and Cisco UCS C-Series servers with the Intel E2660 v4 Xeon Broadwell processors.

1. In Cisco UCS Manager, click Servers on the left.
2. Select Policies > root.
3. Right-click Server Pool Policy Qualifications.
4. Select Create Server Pool Policy Qualification.
5. Name the policy UCS-Broadwell.
6. Select Create CPU/Cores Qualifications.
7. Select Xeon for the Processor/Architecture.
8. Select UCS-CPU-E52660E as the PID.
9. Click OK to create the CPU/Core qualification.
10. Click OK to create the policy then OK for the confirmation.

Create CPU/Cores Qualifications ? ×

| | | | |
|--------------------------|---|-------------------------|---|
| Processor Architecture : | <input type="text" value="Xeon"/> | PID (RegEx) : | <input type="text" value="UCS-CPU-E52660E"/> |
| Min Number of Cores : | <input checked="" type="radio"/> Unspecified <input type="radio"/> select | Max Number of Cores : | <input checked="" type="radio"/> Unspecified <input type="radio"/> select |
| Min Number of Threads : | <input checked="" type="radio"/> Unspecified <input type="radio"/> select | Max Number of Threads : | <input checked="" type="radio"/> Unspecified <input type="radio"/> select |
| CPU Speed (MHz) : | <input checked="" type="radio"/> Unspecified <input type="radio"/> select | CPU Stepping : | <input checked="" type="radio"/> Unspecified <input type="radio"/> select |

Create Server BIOS Policy

To create a server BIOS policy for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click Servers on the left.
2. Select Policies > root.
3. Right-click BIOS Policies.
4. Select Create BIOS Policy.
5. Enter VM-Host as the BIOS policy name.
6. Change the Quiet Boot setting to disabled.
7. Change Consistent Device Naming to enabled.
8. Click Finish to create the BIOS policy.

Create BIOS Policy

Name : VM-Host

Description :

Reboot on BIOS Settings Change :

Quiet Boot : disabled enabled Platform Default

Post Error Pause : disabled enabled Platform Default

Resume Ac On Power Loss : stay-off last-state reset Platform Default

Front Panel Lockout : disabled enabled Platform Default

Consistent Device Naming : disabled enabled Platform Default

< Prev Next > Finish Cancel

9. Click OK.

Update the Default Maintenance Policy

To update the default Maintenance Policy, complete the following steps:

1. In Cisco UCS Manager, click Servers on the left.
2. Select Policies > root.
3. Select Maintenance Policies > default.
4. Change the Reboot Policy to User Ack.
5. Click **“On Next Boot”** to delegate maintenance windows to server administrators.

Servers / Policies / root / Maintenance Poli... / default

| General | Events |
|--|---|
| <p>Actions</p> <p>Delete</p> <p>Show Policy Usage</p> <p>Use Global</p> | <p>Properties</p> <p>Name : default</p> <p>Description : <input type="text"/></p> <p>Owner : Local</p> <p>Soft Shutdown Timer : <input type="text" value="150 Secs"/></p> <p>Reboot Policy : <input type="radio"/> Immediate <input checked="" type="radio"/> User Ack <input type="radio"/> Timer Automatic</p> <p><input checked="" type="checkbox"/> On Next Boot (Apply pending changes at next reboot.)</p> |

6. Click Save Changes.
7. Click OK to accept the change.

Create vNIC Templates

To create multiple virtual network interface card (vNIC) templates for the Cisco UCS environment, complete the following steps. A total of 6 vNIC Templates will be created.

Create Infrastructure vNICs

1. In Cisco UCS Manager, click LAN on the left.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter Infra-A as the vNIC template name.

6. Keep Fabric A selected.
7. Do not select the Enable Failover checkbox.
8. Set Redundancy Type to Primary Template. Leave Peer Redundancy Template set to <not set>.
9. Under Target, make sure that only the Adapter checkbox is selected.
10. Select Updating Template as the Template Type.
11. Under VLANs, select the checkboxes for IB-MGMT, Infra-NFS, and Native-VLAN VLANs.
12. Set Native-VLAN as the native VLAN.
13. Select vNIC Name for the CDN Source.
14. For MTU, enter 9000.
15. In the MAC Pool list, select MAC-Pool-A.
16. In the Network Control Policy list, select Enable-CDP-LLDP.

Create vNIC Template ? X

Template Type : Initial Template Updating Template

VLANs

Advanced Filter Export Print ⚙

| Select | Name | Native VLAN |
|-------------------------------------|-------------|----------------------------------|
| <input type="checkbox"/> | default | <input type="radio"/> |
| <input checked="" type="checkbox"/> | IB-MGMT | <input type="radio"/> |
| <input checked="" type="checkbox"/> | Infra-NFS | <input type="radio"/> |
| <input checked="" type="checkbox"/> | Native-VLAN | <input checked="" type="radio"/> |
| <input type="checkbox"/> | VM-Traffic | <input type="radio"/> |
| <input type="checkbox"/> | vMotion | <input type="radio"/> |

CDN Source : vNIC Name User Defined

MTU :

MAC Pool :

QoS Policy :

Network Control Policy :

Pin Group :

Stats Threshold Policy :

Connection Policies

Dynamic vNIC usNIC VMQ

Dynamic vNIC Connection Policy :

17. Click OK to create the vNIC template.

18. Click OK.

Repeat the following steps for template Infra-B:

1. Select LAN on the left.
2. Select Policies > root.
3. Right-click vNIC Templates.

4. Select Create vNIC Template
5. Enter Infra-B as the vNIC template name.
6. Select Fabric B.
7. Do not select the Enable Failover checkbox.
8. Set Redundancy Type to Secondary Template. Select Infra-A for Peer Redundancy Template.
9. Under Target, make sure that only the Adapter checkbox is selected.
10. Since Peer Redundancy Templates are being used, it is not necessary to select the Template Type.
11. It is not necessary to select VLANs.
12. Select vNIC Name for the CDN Source.
13. It is not necessary to set the MTU.
14. In the MAC Pool list, select MAC-Pool-B.
15. It is not necessary to select the Network Control Policy.
16. Click OK to create the vNIC template.
17. Click OK.

Create vMotion vNICs

1. In Cisco UCS Manager, click LAN on the left.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter vMotion-A as the vNIC template name.
6. Keep Fabric A selected.
7. Do not select the Enable Failover checkbox.
8. Set Redundancy Type to Primary Template. Leave Peer Redundancy Template set to <not set>.
9. Under Target, make sure that only the Adapter checkbox is selected.
10. Select Updating Template as the Template Type.
11. Under VLANs, select the checkbox for the vMotion VLAN.

12. Select vNIC Name for the CDN Source.
13. For MTU, enter 9000.
14. In the MAC Pool list, select MAC-Pool-A.
15. In the Network Control Policy list, select Enable-CDP-LLDP.

Create vNIC Template ? X

If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type : Initial Template Updating Template

VLANs

Advanced Filter Export Print ⚙

| Select | Name | Native VLAN |
|-------------------------------------|-------------|-------------|
| <input type="checkbox"/> | default | ○ |
| <input type="checkbox"/> | IB-MGMT | ○ |
| <input type="checkbox"/> | Infra-NFS | ○ |
| <input type="checkbox"/> | Native-VLAN | ○ |
| <input type="checkbox"/> | VM-Traffic | ○ |
| <input checked="" type="checkbox"/> | vMotion | ○ |

CDN Source : vNIC Name User Defined

MTU :

MAC Pool :

QoS Policy :

Network Control Policy :

Pin Group :

Stats Threshold Policy :

Connection Policies

Dynamic vNIC usNIC VMQ

16. Click OK to create the vNIC template.
17. Click OK.

Repeat these equivalent steps for template vMotion-B:

1. Select LAN on the left.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template
5. Enter vMotion-B as the vNIC template name.
6. Select Fabric B.
7. Do not select the Enable Failover checkbox.
8. Set Redundancy Type to Secondary Template. Select vMotion-A for Peer Redundancy Template.
9. Under Target, make sure that only the Adapter checkbox is selected.
10. Select vNIC Name for the CDN Source.
11. In the MAC Pool list, select MAC-Pool-B.
12. Click OK to create the vNIC template.
13. Click OK.

Create Distributed Virtual Switch (DVS) vNICs

1. Select LAN on the left.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter DVS-Template-A as the vNIC template name.
6. Leave Fabric A selected. Do not select the Enable Failover checkbox.
7. Set Redundancy Type to Primary Template. Leave Peer Redundancy Template set to <not set>.
8. Under Target, make sure that only the Adapter checkbox is selected.
9. Select Updating Template for Template Type.
10. Under VLANs, select only VM-Traffic.
11. Do not set a native VLAN.

12. Select vNIC Name for the CDN Source.
13. Under MTU, enter 9000.
14. From the MAC Pool list, select MAC-Pool-A.
15. From the Network Control Policy list, select Enable-CDP-LLDP.

Create vNIC Template ? X

If **VM** is selected, a port profile by the same name will be created.
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type : Initial Template Updating Template

VLANs

Advanced Filter Export Print ⚙

| Select | Name | Native VLAN |
|-------------------------------------|-------------|-----------------------|
| <input type="checkbox"/> | default | <input type="radio"/> |
| <input type="checkbox"/> | IB-MGMT | <input type="radio"/> |
| <input type="checkbox"/> | Infra-NFS | <input type="radio"/> |
| <input type="checkbox"/> | Native-VLAN | <input type="radio"/> |
| <input checked="" type="checkbox"/> | VM-Traffic | <input type="radio"/> |
| <input type="checkbox"/> | vMotion | <input type="radio"/> |

CDN Source : vNIC Name User Defined

MTU :

MAC Pool : ▼

QoS Policy : ▼

Network Control Policy : ▼

Pin Group : ▼

Stats Threshold Policy : ▼

Connection Policies

16. Click OK to complete creating the vNIC template.
17. Click OK.

Repeat these equivalent steps for DVS-Template-B:

1. Select LAN on the left.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter DVS-Template-B as the vNIC template name.
6. Select Fabric B. Do not select the Enable Failover checkbox.
7. Set Redundancy Type to Secondary Template. Select DVS-Template-A for the Peer Redundancy Template.
8. Under Target, make sure that only the Adapter checkbox is selected.
9. Select vNIC Name for the CDN Source
10. From the MAC Pool list, select MAC-Pool-B.
11. Click OK to complete creating the vNIC template.
12. Click OK.

Create LAN Connectivity Policy

To configure the necessary Infrastructure LAN Connectivity Policy, complete the following steps:

1. In Cisco UCS Manager, click LAN on the left.
2. Select LAN > Policies > root.
3. Right-click LAN Connectivity Policies.
4. Select Create LAN Connectivity Policy.
5. Enter FC-Boot as the name of the policy.
6. Click the upper Add button to add a vNIC.
7. In the Create vNIC dialog box, enter 00-Infra-A as the name of the vNIC.
8. Select the Use vNIC Template checkbox.
9. In the vNIC Template list, select Infra-A.
10. In the Adapter Policy list, select VMWare.
11. Click OK to add this vNIC to the policy.

Create vNIC ? ×

Name :

Use vNIC Template :

Redundancy Pair :

Peer Name :

vNIC Template :

Create vNIC Template

Adapter Performance Profile

Adapter Policy :

Create Ethernet Adapter Policy

12. Click the upper Add button to add another vNIC to the policy.
13. In the Create vNIC box, enter 01-Infra-B as the name of the vNIC.
14. Select the Use vNIC Template checkbox.
15. In the vNIC Template list, select Infra-B.
16. In the Adapter Policy list, select VMWare.
17. Click OK to add the vNIC to the policy.
18. Click the upper Add button to add a vNIC.
19. In the Create vNIC dialog box, enter 02-vMotion-A as the name of the vNIC.

20. Select the Use vNIC Template checkbox.
21. In the vNIC Template list, select vMotion-A.
22. In the Adapter Policy list, select VMWare.
23. Click OK to add this vNIC to the policy.
24. Click the upper Add button to add a vNIC to the policy.
25. In the Create vNIC dialog box, enter 03-vMotion-B as the name of the vNIC.
26. Select the Use vNIC Template checkbox.
27. In the vNIC Template list, select vMotion-B.
28. In the Adapter Policy list, select VMWare.
29. Click OK to add this vNIC to the policy.
30. Click the upper Add button to add a vNIC.
31. In the Create vNIC dialog box, enter 04-DVS-A as the name of the vNIC.
32. Select the Use vNIC Template checkbox.
33. In the vNIC Template list, select DVS-Template-A.
34. In the Adapter Policy list, select VMWare.
35. Click OK to add this vNIC to the policy.
36. Click the upper Add button to add a vNIC to the policy.
37. In the Create vNIC dialog box, enter 05-DVS-B as the name of the vNIC.
38. Select the Use vNIC Template checkbox.
39. In the vNIC Template list, select DVS-Template-B.
40. In the Adapter Policy list, select VMWare.
41. Click OK to add this vNIC to the policy.

Create LAN Connectivity Policy ? X

Name :

Description :

Click **Add** to specify one or more vNICs that the server should use to connect to the LAN.

| Name | MAC Address | Native VLAN |
|-------------------|-------------|-------------|
| vNIC 05-DVS-B | Derived | |
| vNIC 04-DVS-A | Derived | |
| vNIC 03-vMotion-B | Derived | |
| vNIC 02-vMotion-A | Derived | |
| vNIC 01-Infra-B | Derived | |
| vNIC 00-Infra-A | Derived | |

🗑 Delete ➕ Add ⓘ Modify

➕ Add iSCSI vNICs

OK
Cancel

42. Click OK, then OK again to create the LAN Connectivity Policy.

Create vMedia Policy for VMware ESXi 6.0 U2 Install Boot

In the NetApp Data ONTAP setup steps an HTTP web server is required, which will be used for hosting NetApp Data ONTAP as well as VMware software. The vMedia Policy created here maps the VMware ESXi 6.0U2 ISO to the Cisco UCS server in order to boot the ESXi installation. To create this policy, complete the following steps:

1. In Cisco UCS Manager, select Servers on the left.
2. Select Policies > root.
3. Right-click vMedia Policies.

4. Select Create vMedia Policy.
5. Name the policy ESXi-6.0U2-HTTP.
6. Enter “Mounts Cisco Custom ISO for ESXi 6.0U2” in the Description field.
7. Click Add.
8. Name the mount ESXi-6.0U2-HTTP.
9. Select the CDD Device Type.
10. Select the HTTP Protocol.
11. Enter the IP Address of the web server.



Since DNS server IPs were not entered into the KVM IP earlier, it is necessary to enter the IP of the web server instead of the hostname.

12. Enter Vmware-ESXi-60U2-4192238-Cisco-Custom-6.0.2.3.iso as the Remote File name.



This VMware ESXi Cisco Custom ISO can be downloaded from [CiscoCustomImage6.0U2Patch3](#).

13. Enter the web server path to the ISO file in the Remote Path field.

Create vMedia Mount ? X

Name :

Description :

Device Type : CDD HDD

Protocol : NFS CIFS HTTP HTTPS

Hostname/IP Address :

Image Name Variable : None Service Profile Name

Remote File :

Remote Path :

Username :

Password :

14. Click OK to create the vMedia Mount.

15. Click OK then OK again to complete creating the vMedia Policy.



For any new servers added to the Cisco UCS environment the vMedia service profile template can be used to install the ESXi host. On first boot the host will boot into the ESXi installer since the SAN mounted disk is empty. After ESXi is installed, the vMedia will not be referenced as long as the boot disk is accessible.

Create Boot Policy (FC Boot)

This procedure applies to a Cisco UCS environment in which two FC logical interfaces (LIFs) are on cluster node 1 and two FC LIFs are on cluster node 2 for each Cisco UCS Fabric Interconnect:

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

1. In Cisco UCS Manager, click Servers on the left.
2. Select Policies > root.
3. Right-click Boot Policies.
4. Select Create Boot Policy.
5. Enter `Boot-FC-Fabric-A` as the name of the boot policy.
6. Optional: Enter a description for the boot policy.



Do not select the Reboot on Boot Order Change checkbox.

7. Keep the Reboot on Boot Order Change option cleared.
8. Expand the Local Devices drop-down menu and select `Add Remote CD/DVD`.
9. Expand the vHBAs drop-down menu and select `Add SAN Boot`.
10. Select the Primary Type.
11. Enter `Fabric-A` in the vHBA field.
12. Confirm that Primary is selected for the Type option.

Add SAN Boot ? X

vHBA :

Type : Primary Secondary Any

OK Cancel

13. Click OK to add the SAN boot initiator.

14. From the vHBA drop-down menu, select Add SAN Boot Target.
15. Keep 0 as the value for Boot Target LUN.
16. Enter the WWPN for `fc_p_lif01a`.



To obtain this information, log in to the storage cluster and run the `network interface show` command.

17. Select Primary for the SAN boot target type.

Add SAN Boot Target ? X

Boot Target LUN : 0

Boot Target WWPN : 20:01:00:a0:98:5b:4a:86

Type : Primary Secondary

OK Cancel

16. Click OK to add the SAN boot target.
17. From the vHBA drop-down menu, select Add SAN Boot Target.
18. Enter 0 as the value for Boot Target LUN.
19. Enter the WWPN for `fc_p_lif02a`.
20. Click OK to add the SAN boot target.
21. From the vHBA drop-down menu, select Add SAN Boot.
22. In the Add SAN Boot dialog box, enter `Fabric-B` in the vHBA box.

23. The SAN boot type should automatically be set to Secondary.
24. Click OK to add the SAN boot initiator.
25. From the vHBA drop-down menu, select Add SAN Boot Target.
26. Keep 0 as the value for Boot Target LUN.
27. Enter the WWPN for `fc01_lif01b`.
28. Select Primary for the SAN boot target type.
29. Click OK to add the SAN boot target.
30. From the vHBA drop-down menu, select Add SAN Boot Target.
31. Keep 0 as the value for Boot Target LUN.
32. Enter the WWPN for `fc02_lif02b`.
33. Click OK to add the SAN boot target.
34. Expand CIMC Mounted Media and select Add CIMC Mounted CD/DVD.

Create Boot Policy ? ✕

Name :

Description :

Reboot on Boot Order Change :

Enforce vNIC/vHBA/iSCSI Name :

Boot Mode : Legacy Uefi

WARNINGS:
 The type (primary/secondary) does not indicate a boot order presence.
 The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.
 If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.
 If it is not selected, the vNICs/vHBAs are selected if they exist, otherwise the vNIC/vHBA with the lowest PCIe bus scan order is used.

Local Devices

Add Local Disk

- Add Local LUN
- Add Local JBOD
- Add SD Card
- Add Internal USB
- Add External USB
- Add Embedded Local LUN
- Add Embedded Local Disk

Add CD/DVD

- Add Local CD/DVD
- Add Remote CD/DVD

Add Floppy

- Add Local Floppy

Boot Order

| Name | vNIC/vHBA/iSCSI vNIC | WWN | ... | ... | ... | ... | ... |
|---------------------|----------------------|-----|-----|-----|-----|-----|-----|
| Remote CD/DVD | | 1 | | | | | |
| San | | 2 | | | | | |
| ▶ SAN Primary | Fabric-A | | | | | | |
| ▶ SAN Secondary | Fabric-B | | | | | | |
| CIMC Mounted CD/DVD | | 3 | | | | | |

35. Click OK, then click OK again to create the boot policy.

Create Service Profile Templates (FC Boot)

In this procedure, one service profile template for Infrastructure ESXi hosts is created for Fabric A boot.

To create the service profile template, complete the following steps:

1. In Cisco UCS Manager, click Servers on the left.
2. Select Service Profile Templates > root.
3. Right-click root.
4. Select Create Service Profile Template to open the Create Service Profile Template wizard.
5. Enter VM-Host-Infra-FC-A as the name of the service profile template. This service profile template is configured to boot from storage node 1 on fabric A.
6. Select the "Updating Template" option.

- Under UUID, select UUID_Pool as the UUID pool.

- Click Next.

Configure Storage Provisioning

- If you have servers with no physical disks, click on the Local Disk Configuration Policy and select the SAN-Boot Local Storage Policy. Otherwise, select the default Local Storage Policy.
- Click Next.

Configure Networking Options

- Keep the default setting for Dynamic vNIC Connection Policy.
- Select the “Use Connectivity Policy” option to configure the LAN connectivity.
- Select FC-Boot from the LAN Connectivity Policy pull-down.
- Leave Initiator Name Assignment at <not set>.

Create Service Profile Template ? X

Optionally specify LAN configuration information.

Dynamic vNIC Connection Policy: ▼

[Create Dynamic vNIC Connection Policy](#)

How would you like to configure LAN connectivity?

Simple Expert No vNICs Use Connectivity Policy

LAN Connectivity Policy : ▼ [Create LAN Connectivity Policy](#)

Initiator Name

Initiator Name Assignment: ▼

[Create IQN Suffix Pool](#)

WARNING: The selected pool does not contain any available entities.
You can select it, but it is recommended that you add entities to it.

< Prev Next > **Finish** Cancel

5. Click Next.

Configure Storage Options

1. Select the **Use Connectivity Policy** option for the “How would you like to configure SAN connectivity?” field.
2. Pick the **FC-Boot** option from the SAN Connectivity Policy pull-down.

Create Service Profile Template ? X

Optionally specify disk policies and SAN configuration information.

How would you like to configure SAN connectivity?

Simple
 Expert
 No vHBAs
 Use Connectivity Policy

SAN Connectivity Policy : FC-Boot ▼ Create SAN Connectivity Policy

< Prev
Next >
Finish
Cancel

3. Click Next.

Configure Zoning Options

1. Set no Zoning options and click Next.

Configure vNIC/HBA Placement

1. In the “Select Placement” list, leave the placement policy as “Let System Perform Placement”.
2. Click Next.

Configure vMedia Policy

1. Do not select a vMedia Policy.
2. Click Next.

Configure Server Boot Order

1. Select Boot-FC-Fabric-A for Boot Policy.

Create Service Profile Template

Optionally specify the boot policy for this service profile template.

Select a boot policy.

Boot Policy: [Create Boot Policy](#)

Name : **Boot-FC-Fabric-A**
 Description :
 Reboot on Boot Order Change : **No**
 Enforce vNIC/vHBA/iSCSI Name : **Yes**
 Boot Mode : **Legacy**

WARNINGS:
 The type (primary/secondary) does not indicate a boot order presence.
 The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.
 If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.
 If it is not selected, the vNICs/vHBAs are selected if they exist, otherwise the vNIC/vHBA with the lowest PCIe bus scan order is used.

Boot Order

+ - Advanced Filter Export Print

| Name | Order | vNIC/vHB... | Type | WWN | LUN Name | Slot Num... | Boot Name | Boot Path | Description |
|-------|-------|-------------|-----------|--------------|----------|-------------|-----------|-----------|-------------|
| SA... | | Fabric-A | Primary | | | | | | |
| ... | | | Primary | 20:01:00:... | 0 | | | | |
| ... | | | Secondary | 20:04:00:... | 0 | | | | |
| SA... | | Fabric-B | Secondary | | | | | | |
| ... | | | Primary | 20:02:00:... | 0 | | | | |
| ... | | | Secondary | 20:03:00:... | 0 | | | | |

[Create iSCSI vNIC](#) [Set iSCSI Boot Parameters](#) [Set UEFI Boot Parameters](#)

< Prev Next > **Finish** Cancel

- Click Next to continue to the next section.

Configure Maintenance Policy

- Change the Maintenance Policy to default.

Create Service Profile Template ? X

Specify how disruptive changes such as reboots, network interruptions, and firmware upgrades should be applied to the server associated with this service profile.

⊖ Maintenance Policy

Select a maintenance policy to include with this service profile or create a new maintenance policy that will be accessible to all service profiles.

Maintenance Policy: [Create Maintenance Policy](#)

Name : **default**
 Description :
 Soft Shutdown Timer : **150 Secs**
 Reboot Policy : **User Ack**

2. Click Next.

Configure Server Assignment

To configure server assignment, complete the following steps:

1. In the Pool Assignment list, select Infra-Pool.
2. Select Down as the power state to be applied when the profile is associated with the server.
3. **Optional:** select “UCS-Broadwell” for the Server Pool Qualification.
4. Expand Firmware Management at the bottom of the page and select the default policy

Create Service Profile Template

Optionally specify a server pool for this service profile template.

You can select a server pool you want to associate with this service profile template.

Pool Assignment: [Create Server Pool](#)

Select the power state to be applied when this profile is associated with the server.

Up Down

The service profile template will be associated with one of the servers in the selected pool. If desired, you can specify an additional server pool policy qualification that the selected server must meet. To do so, select the qualification from the list.

Server Pool Qualification :

Restrict Migration :

Firmware Management (BIOS, Disk Controller, Adapter)

If you select a host firmware policy for this service profile, the profile will update the firmware on the server that it is associated with. Otherwise the system uses the firmware already installed on the associated server.

Host Firmware Package:

[Create Host Firmware Package](#)

[< Prev](#) [Next >](#) [Finish](#) [Cancel](#)

5. Click Next.

Configure Operational Policies

To configure the operational policies, complete the following steps:

1. In the BIOS Policy list, select VM-Host.
2. Expand Power Control Policy Configuration and select No-Power-Cap in the Power Control Policy list.

Create Service Profile Template ? X

Optionally specify information that affects how the system operates.

⊖ BIOS Configuration

If you want to override the default BIOS settings, select a BIOS policy that will be associated with this service profile

BIOS Policy : VM-Host ▼

⊕ External IPMI Management Configuration

⊕ Management IP Address

⊕ Monitoring Configuration (Thresholds)

⊖ Power Control Policy Configuration

Power control policy determines power allocation for a server in a given power group.

Power Control Policy : No-Power-Cap ▼ [Create Power Control Policy](#)

⊕ Scrub Policy

⊕ KVM Management Policy

< Prev Next > **Finish** Cancel

3. Click Finish to create the service profile template.
4. Click OK in the confirmation message.

Create vMedia Service Profile Template

To create service profiles from the service profile template, complete the following steps:

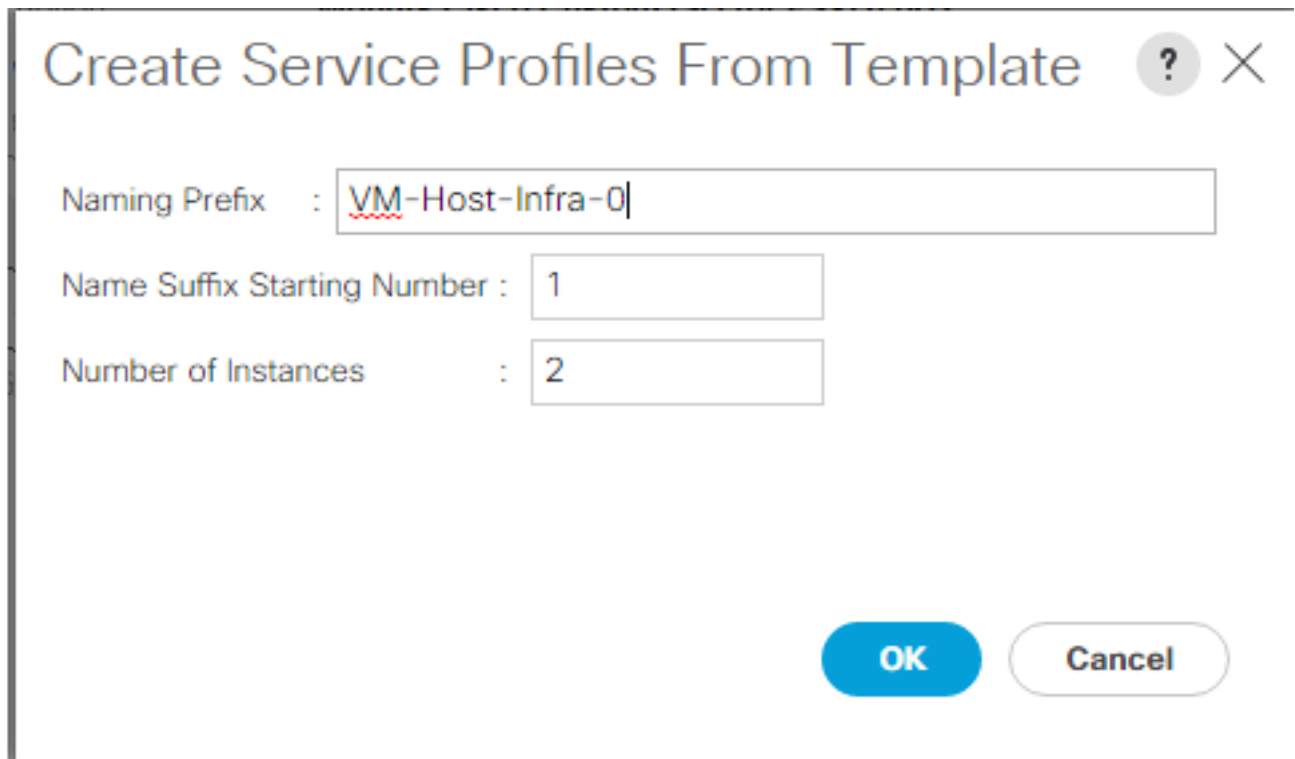
1. Connect to UCS Manager, click Servers on the left.
2. Select Service Profile Templates > root > Service Template VM-Host-Infra-FC-A.
3. Right-click Service Template VM-Host-Infra-FC-A and select Create a Clone.
4. Name the clone VM-Host-Infra-FC-A-vM and click OK.
5. Select Service Template VM-Host-Infra-FC-A-vM.
6. In the right pane, select the vMedia Policy tab.
7. Under Actions, select Modify vMedia Policy.
8. Using the pulldown, select the ESXi-6.0U2-HTTP vMedia Policy.

9. Click OK then OK again to complete modifying the Service Profile Template.

Create Service Profiles

To create service profiles from the service profile template, complete the following steps:

1. Connect to UCS Manager, click Servers on the left.
2. Select Service Profile Templates > root > Service Template VM-Host-Infra-FC-A-vM.
3. Right-click VM-Host-Infra-FC-A-vM and select Create Service Profiles from Template.
4. Enter VM-Host-Infra-0 as the service profile prefix.
5. Enter 1 as “Name Suffix Starting Number.”
6. Enter 2 as the “Number of Instances.”
7. Click OK to create the service profiles.



Create Service Profiles From Template ? X

Naming Prefix :

Name Suffix Starting Number :

Number of Instances :

OK Cancel

8. Click OK in the confirmation message.

Add More Servers to FlexPod Unit

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

Gather Necessary Information

After the Cisco UCS service profiles have been created, each infrastructure server in the environment will have a unique configuration. To proceed with the FlexPod deployment, specific information must be gathered from each Cisco UCS server and from the NetApp controllers. Insert the required information into Error! Reference source not found.and Table 22 .

Table 21 WWPNS from NetApp Storage

| SVM | Target LIF WWPN (FC) |
|-----------|----------------------|
| Infra-SVM | fcp_lif01a |
| | fcp_lif01b |
| | fcp_lif02a |
| | fcp_lif02b |



To obtain the FC WWPNS, run the `network interface show` command on the storage cluster management interface.

Table 22 FC WWPNS for Fabric A and Fabric B

| Cisco UCS Service Profile Name | Initiator: WWPNS (FC) | Variables |
|--------------------------------|-----------------------|--|
| VM-Host-Infra-01 | | <vm-host-infra-01-wwpna> <vm-host-infra-01-wwpnb> |
| VM-Host-Infra-02 | | <vm-host-infra-02-wwpna> <vm-host-infra-02-wwpnb> |



To obtain the FC vHBA WWPN information in Cisco UCS Manager GUI, go to Servers > Service Profiles > root. Click each service profile and then click the “Storage” tab, then “vHBAs” tab on the right. The WWPNS are displayed in the table at the bottom of the page.

Adding Direct Connected Tenant FC Storage

To add FC storage from an additional storage SVM, two storage connection policies, one for each fabric must be added in UCS Manager and attached to vHBA Initiator Groups in the SAN Connectivity Policy. These steps were not shown in the initial deployment above because it is not necessary to zone boot targets. Boot targets are automatically zoned in the fabric interconnect when zoning is enabled on the fabric VSAN. To add direct connected tenant FC storage from a tenant SVM, complete the following steps:

Create Storage Connection Policies

In this procedure, one storage connection policy is created for each fabric.

To create the storage connection policies, complete the following steps:

1. In Cisco UCS Manager, click SAN on the left.
2. Right-click SAN > Policies > root > Storage Connection Policies and select Create Storage Connection Policy.
3. Name the policy to indicate a tenant on Fabric A.
4. Select the Single Initiator Multiple Targets Zoning Type.
5. Click Add to add a target.
6. Enter the WWPN of the first fabric A FC LIF in the tenant SVM connected to fabric interconnect A. Select Path A and VSAN VSAN-A. Click OK.
7. Click Add to add a target.
8. Enter the WWPN of the second fabric A FC LIF in the tenant SVM connected to fabric interconnect A. Select Path A and VSAN VSAN-A. Click OK.
9. Click OK then OK again to complete adding the Storage Connection Policy.
10. Right-click SAN > Policies > root > Storage Connection Policies and select Create Storage Connection Policy.
11. Name the policy to indicate a tenant on Fabric B.
12. Select the Single Initiator Multiple Targets Zoning Type.
13. Click Add to add a target.
14. Enter the WWPN of the first fabric B FC LIF in the tenant SVM connected to fabric interconnect B. Select Path B and VSAN VSAN-B. Click OK.
15. Click Add to add a target.
16. Enter the WWPN of the second fabric B FC LIF in the tenant SVM connected to fabric interconnect B. Select Path B and VSAN VSAN-B. Click OK.
17. Click OK then OK again to complete adding the Storage Connection Policy.

Map Storage Connection Policies vHBA Initiator Groups in SAN Connectivity Policy

In this procedure, storage connection policies are mapped to vHBA initiator groups for each fabric.

To create the storage connection policy mappings, complete the following steps:

1. In Cisco UCS Manager, click SAN on the left.
2. Select SAN > Policies > root > SAN Connectivity Policies > FC-Boot.
3. In the center pane, select the vHBA Initiator Groups tab.

4. Click Add to add a vHBA Initiator Group.
5. Name the group Fabric A and select the Fabric A Initiator.
6. Use the pulldown to select the Fabric A Storage Connection Policy.
7. Click OK and OK to complete adding the Initiator Group.
8. Click Add to add a vHBA Initiator Group.
9. Name the group Fabric B and select the Fabric B Initiator.
10. Use the pulldown to select the Fabric B Storage Connection Policy.
11. Click OK and OK to complete adding the Initiator Group.

FlexPod Cisco Nexus 1000V vSphere

This section provides an alternate set of procedures for installing a pair of high-availability (HA) Cisco Nexus 1000V Virtual Supervisor Modules (VSMs) into the VMware vSphere environment as part of the Cisco Nexus 1000V distributed virtual switch (DVS), instead of the VMware vDS. This procedure assumes that the Cisco Nexus 1000V software version 5.2(1)SV3(2.1) has been downloaded from [Cisco Nexus 1000V Download Link](#) and not expanded (just download the pkg.zip file). Additionally, this procedure assumes that Cisco Virtual Switch Update Manager (VSUM) version 2.0 has been downloaded from [Cisco VSUM Download Link](#) and expanded. This procedure also assumes that VMware vSphere 6.0 Enterprise Plus licensing is installed.

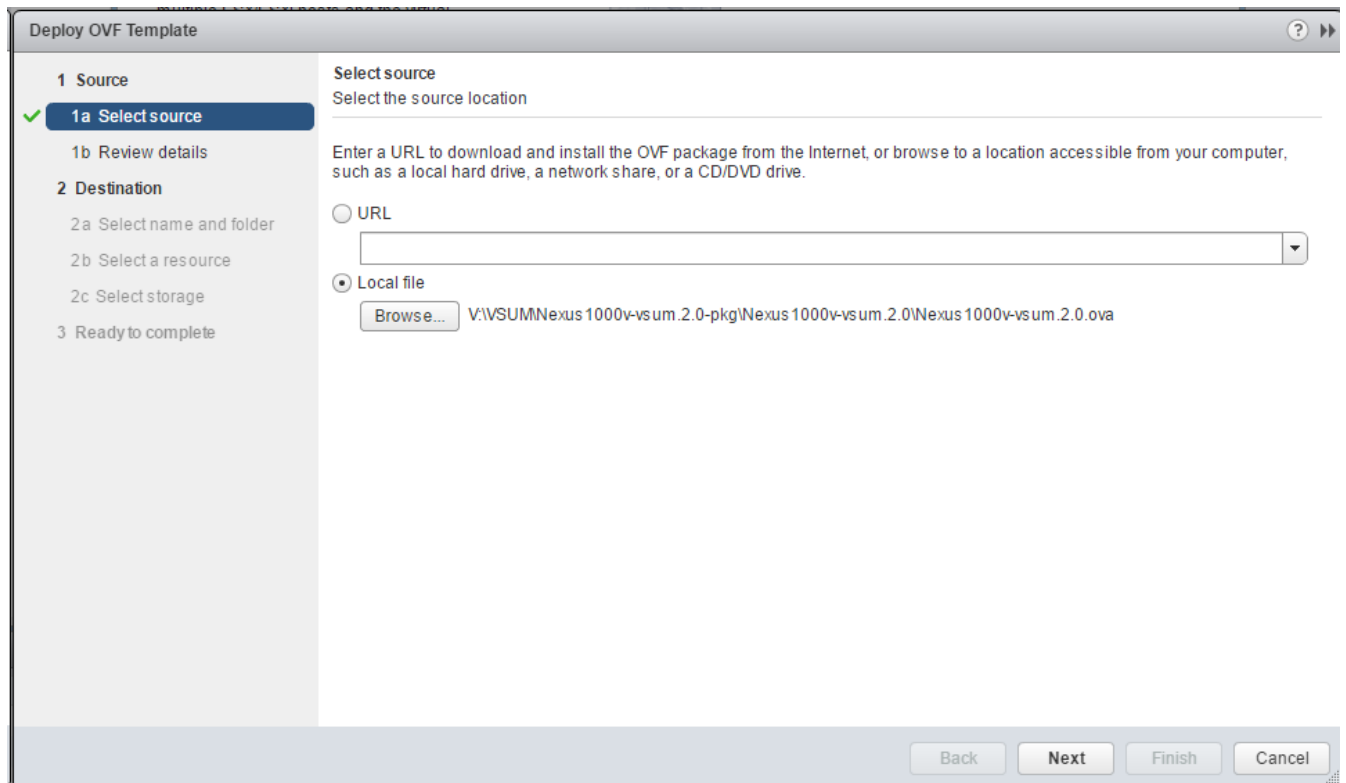
In the Cisco UCS setup section of this document, three sets of vNICs (Infra-A and B, vMotion-A and B, and DVS-A and B) were setup. The vmnic ports associated with the Infrastructure and DVS vNICs will be migrated to the Nexus 1000V with two different uplink profiles. The critical infrastructure VLAN interfaces will stay on the Infra-A and Infra-B uplinks and the tenant or application interfaces (currently only the VM-Traffic VLAN interface) will be placed on the DVS-A and DVS-B uplinks. The vMotion vSwitch will not be migrated to the Nexus 1000V.

Install Cisco Virtual Switch Update Manager

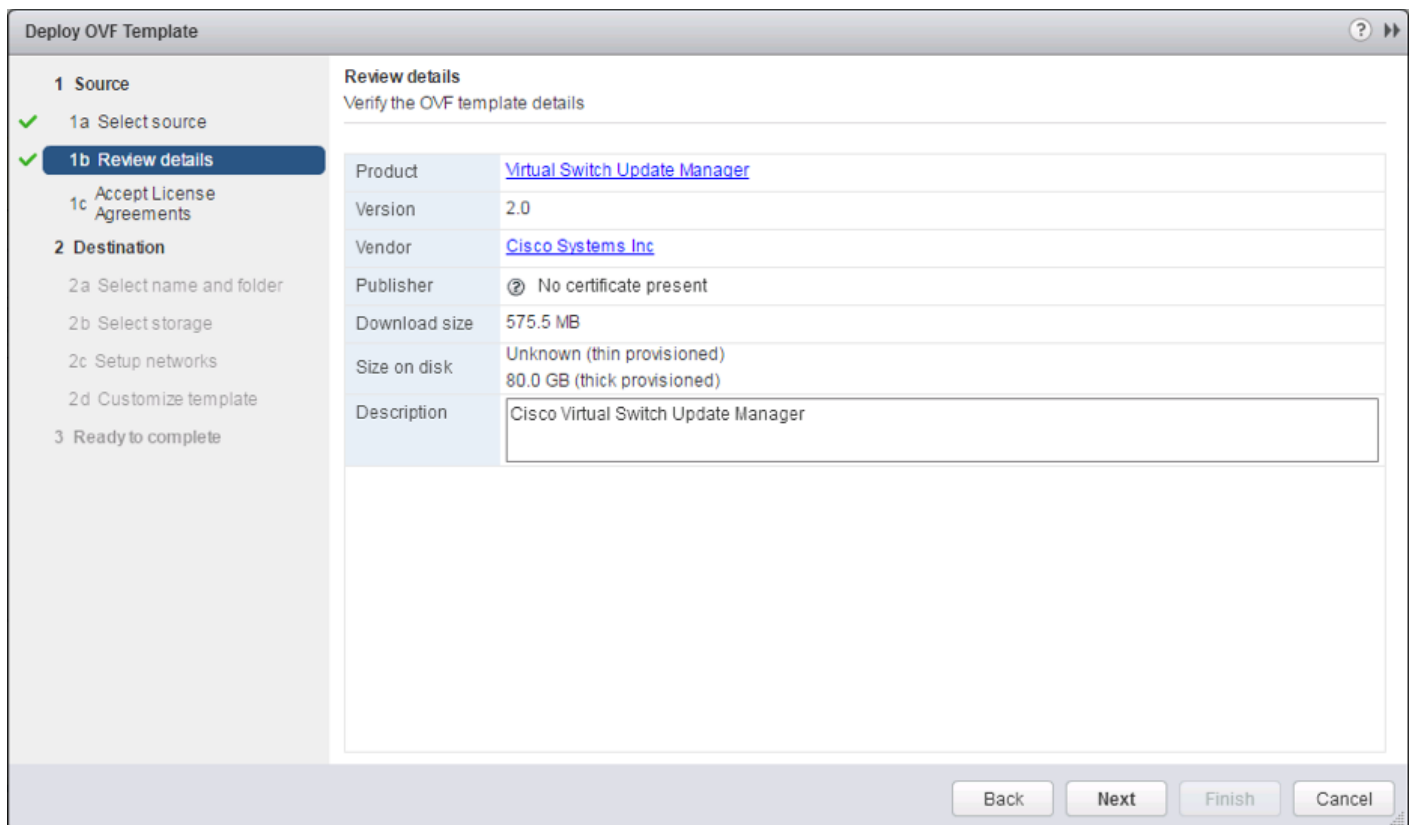
VMware vSphere Web Client

To install the Cisco Virtual Switch Upgrade Manager from OVA in the VMware virtual environment, complete the following steps:

1. Log into the VMware vSphere Web Client.
2. In the pane on the right, click VMs and Templates.
3. In the center pane, select Actions > Deploy OVF Template.
4. Select Browse and browse to and select the Nexus1000v-vsum.2.0.ova file.
5. Click Open.
6. Click Next.



7. Review the details and click Next.



8. Click Accept to accept the License Agreement and click Next.

9. Name the Virtual Machine, select the FlexPod-DC datacenter and click Next.

10. Select the FlexPod-Management cluster and click Next.

11. Select infra_datastore_1 and the Thin Provision virtual disk format and click Next.

Deploy OVF Template

1 Source

- ✓ 1 a Select source
- ✓ 1 b Review details
- ✓ 1 c Accept License Agreements

2 Destination

- ✓ 2 a Select name and folder
- ✓ 2 b Select a resource
- ✓ **2 c Select storage**
- 2 d Setup networks
- 2 e Customize template

3 Ready to complete

Select storage
Select location to store the files for the deployed template

Select virtual disk format:

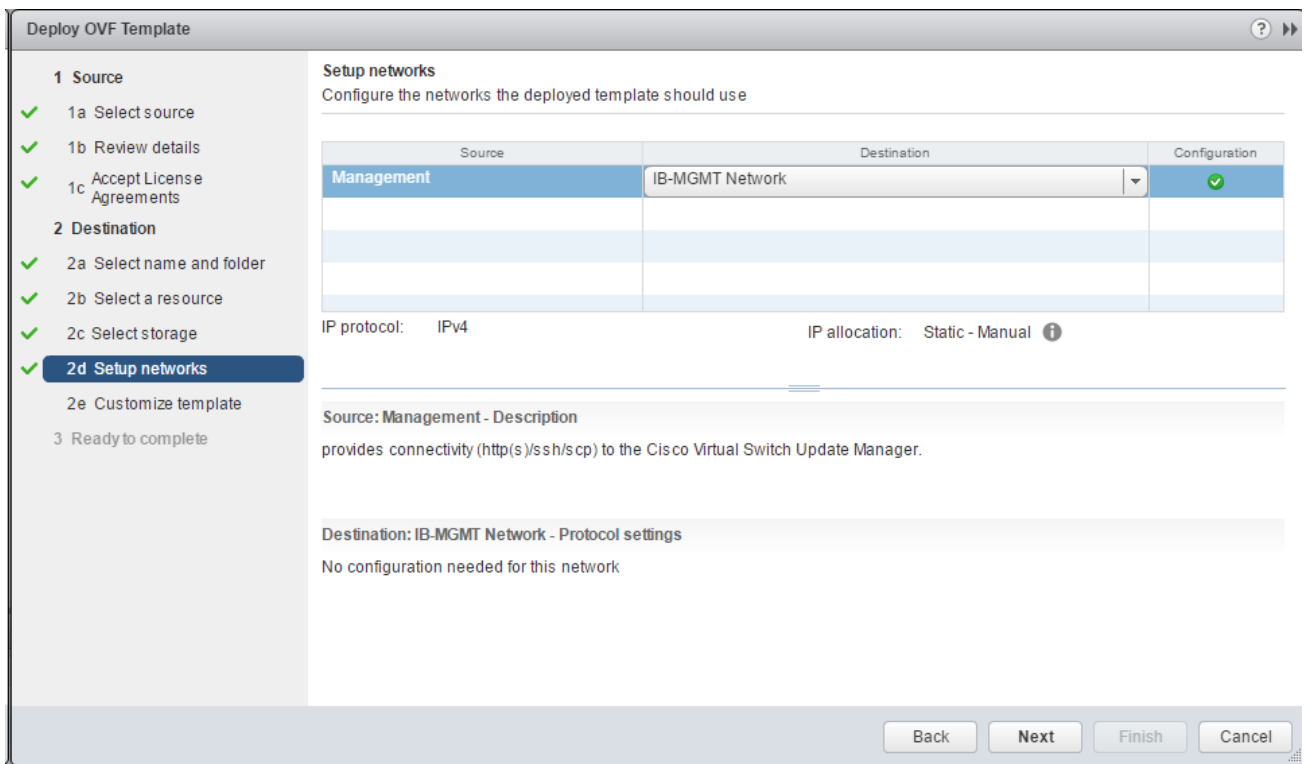
VM Storage Policy: ⓘ

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

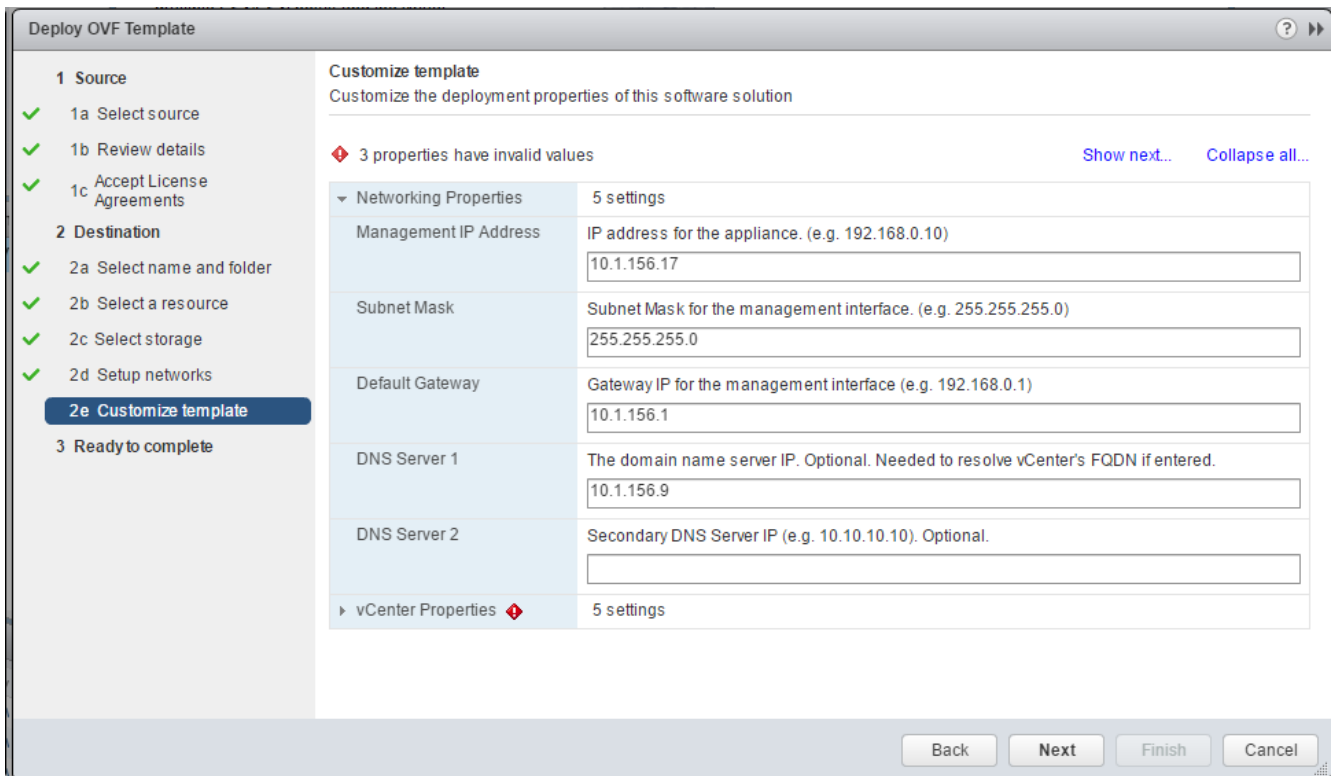
| Name | Capacity | Provisioned | Free | Type | Storage DRS |
|-------------------|-----------|-------------|-----------|--------|-------------|
| infra_datastore_1 | 500.00 GB | 182.44 GB | 420.06 GB | NFS v3 | |
| infra_swap | 100.00 GB | 26.06 MB | 99.97 GB | NFS v3 | |
| datastore1 (1) | 7.50 GB | 858.00 MB | 6.66 GB | VMFS | |
| datastore1 | 7.50 GB | 858.00 MB | 6.66 GB | VMFS | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Back Next Finish Cancel

12. Select IB-MGMT Network and click Next.



13. Fill in the Networking Properties within the Customize template dialog.



14. Expand the vCenter Properties and fill in vCenter address, Username, and Password fields.

Deploy OVF Template

1 Source

- ✓ 1a Select source
- ✓ 1b Review details
- ✓ 1c Accept License Agreements

2 Destination

- ✓ 2a Select name and folder
- ✓ 2b Select a resource
- ✓ 2c Select storage
- ✓ 2d Setup networks
- 2e Customize template**
- ✓ 3 Ready to complete

Customize template
Customize the deployment properties of this software solution

All properties have valid values [Show next...](#) [Collapse all...](#)

| | |
|--|--|
| DNS Server 2 | Secondary DNS Server IP (e.g. 10.10.10.10). Optional. |
| vCenter Properties 5 settings | |
| IP Address or FQDN (Fully Qualified Domain Name) | The IP address or FQDN (e.g. foo.example.com) of the vCenter to register with. |
| Username | vCenter username. User must be able to manage extensions. |
| Password | Password for the above username. |
| HTTP Cleartext Port | Needed for tunneled secure communication. |
| HTTPS Port | |

Back Next Finish Cancel

15. Click Next.

16. Review all settings and click Finish.

17. Wait for the Deploy OVF template task to complete.

18. Select the Home button in VMware vSphere Web Client and select Hosts and Clusters.

19. Expand the FlexPod-Management cluster and select the Virtual Switch Update Manager VM from the Summary tab.

20. Click Launch Remote Console at the left of the Summary tab. If a security warning pops up, click Allow. If you do not have the Remote Console installed, use the Download Remote Console link to download and install the Remote Console.

21. If a security certificate warning pops up, click Connect Anyway.

22. Power on the Virtual Switch Update Manager VM.

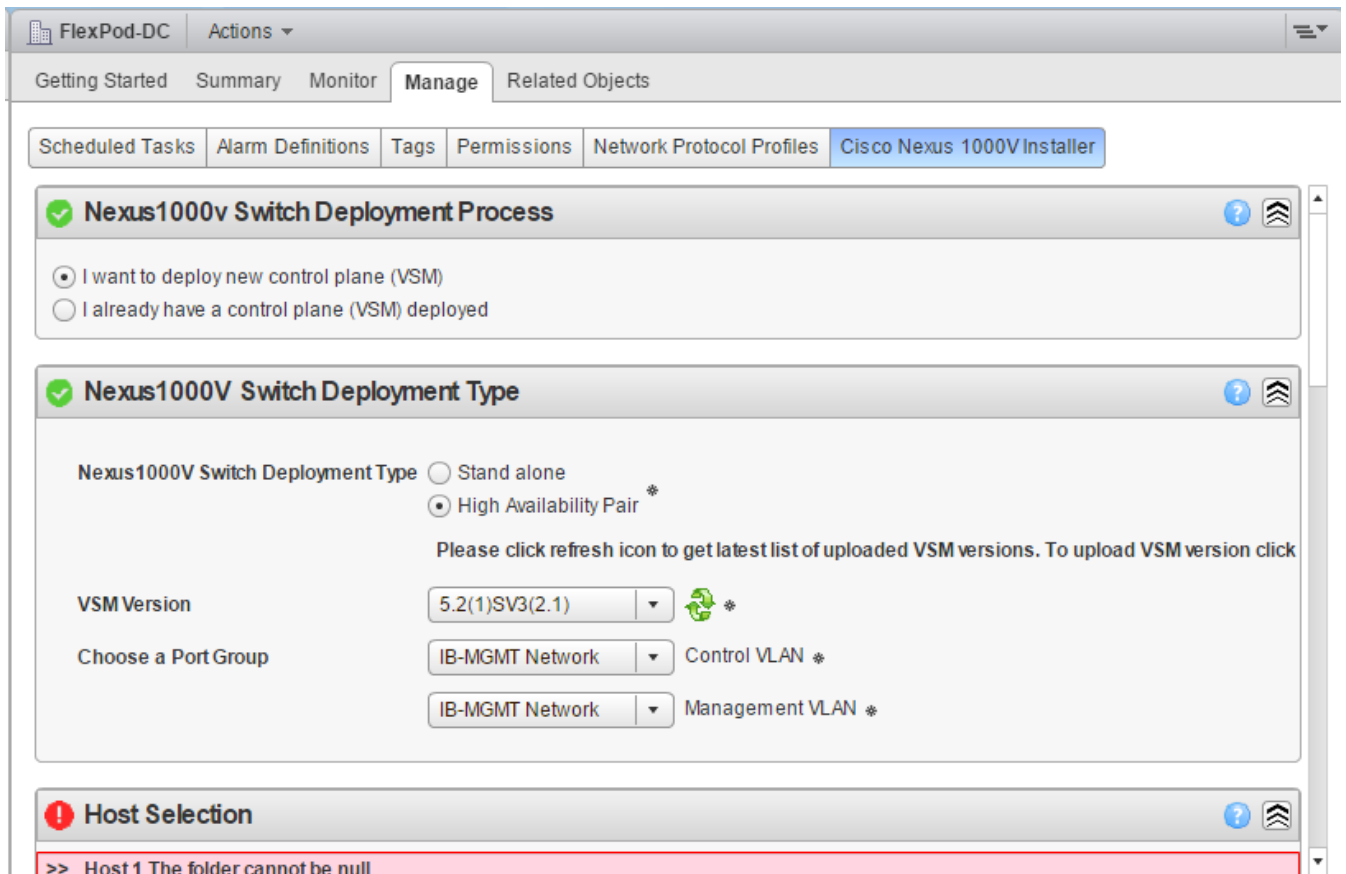
23. Once the VM has completely booted up, close the Remote Console, log out, and log back into the VMware vSphere Web Client.

Install the Cisco Nexus 1000V in VMware using VSUM

VMware vSphere Web Client

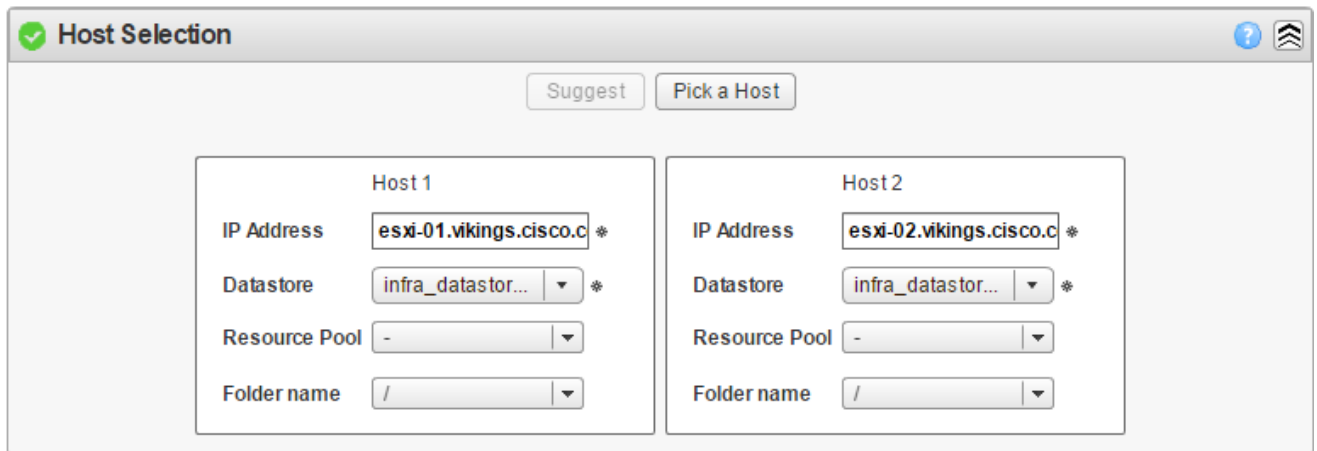
To install the Cisco Nexus 1000V, complete the following steps:

1. After logging back into the VMware vSphere Web Client, Cisco Virtual Switch Update Manager should now appear under the Home tab. Select Cisco Virtual Switch Update Manager.
2. Under Image Tasks, select Upload. VSUM should currently show no Nexus 1000V software images.
3. On the right, under Upload switch image, click Upload.
4. In the Virtual Switch Update Manager tab, click Choose File
5. Browse to the Nexus1000v.5.2.1.SV3.2.1-pkg.zip file downloaded earlier, select it, and click Open.
6. Click Upload. Wait for the file to be uploaded and installed.
7. Click OK. Close the Virtual Switch Update Manager tab and return to the vSphere Web Client.
8. On the right, click Refresh and verify that the Nexus 1000V software image is now uploaded.
9. Under Basic Tasks, select Nexus 1000V.
10. Click Install.
11. In the pane on the right, select FlexPod-DC.
12. Under Nexus1000v Switch Deployment Process, select I want to deploy new control plane (VSM).
13. Under Nexus 1000V Switch Deployment Type, make sure High Availability Pair is selected and select IB-MGMT Network for both the Control VLAN and Management VLAN.



14. Scroll down under Host Selection and click Suggest.

15. Under the two FlexPod-Management hosts, select infra_datastore_1 for the Datastore.



16. Scroll down under Switch Configuration and enter a unique VSM Domain ID and make sure the Management IP Address Deployment Type is selected.

Switch Configuration

Domain ID: *

Deployment Type: Management IP Address
 Control IP Address

17. Scroll down under Virtual Supervisor Module (VSM) configuration and fill in the requested information.

Virtual Supervisor Module (VSM) configuration

Switch Name *

IP Address *

Subnet Mask *

Gateway Address *

Default Port Profiles:

Username

Password *

Confirm password *

18. Click Finish. The primary and secondary VSMS will be deployed, powered on, and the DVS will be registered in vCenter.
19. Click the Home button.
20. Select Cisco Virtual Switch Update manager.
21. Under Basic tasks, select Nexus 1000v.
22. Click Configure.
23. In the pane on the right, select FlexPod-DC.
24. The Nexus 1000v Switch should now appear under the Choose an associated Distributed Virtual Switch section.

Perform Base Configuration of the Primary VSM

SSH Connection to Primary VSM

To perform the base configuration of the primary VSM, complete the following steps:

Using an SSH client, log in to the primary Cisco Nexus 1000V VSM as admin.

1. Run the following configuration commands.

```
config t
ntp server <switch-a-ntp-ip> use-vrf management
ntp server <switch-b-ntp-ip> use-vrf management
vlan <ib-mgmt-vlan-id>
name IB-MGMT-VLAN
vlan <infra-nfs-vlan-id>
name Infra-NFS-VLAN
vlan <vm-traffic-vlan-id>
name VM-Traffic-VLAN
vlan <native-vlan-id>
name Native-VLAN
exit
port-profile type ethernet infra-uplink
vmware port-group
switchport mode trunk
switchport trunk native vlan <native-vlan-id>
switchport trunk allowed vlan <ib-mgmt-vlan-id>, <infra-nfs-vlan-id>
channel-group auto mode on mac-pinning
no shutdown
system vlan <ib-mgmt-vlan-id>, <infra-nfs-vlan-id>
system mtu 9000
state enabled

port-profile type ethernet tenant-uplink
vmware port-group
switchport mode trunk
switchport trunk allowed vlan <vm-traffic-vlan-id>
```

```
channel-group auto mode on mac-pinning
no shutdown
system mtu 9000
state enabled
```

```
port-profile type vethernet IB-MGMT-VLAN
vmware port-group
switchport mode access
switchport access vlan <<ib-mgmt-vlan-id>
no shutdown
system vlan <ib-mgmt-vlan-id>
state enabled
```

```
port-profile type vethernet Infra-NFS-VLAN
vmware port-group
switchport mode access
switchport access vlan <infra-nfs-vlan-id>
no shutdown
system vlan <infra-nfs-vlan-id>
state enabled
```

```
port-profile type vethernet VM-Traffic-VLAN
vmware port-group
switchport mode access
switchport access vlan <<vm-traffic-vlan-id>
no shutdown
state enabled
```

```
port-profile type vethernet nlkv-L3
capability l3control
vmware port-group
switchport mode access
switchport access vlan <ib-mgmt-vlan-id>
```

```
no shutdown

system vlan <ib-mgmt-vlan-id>

state enabled

exit

copy run start
```

Add VMware ESXi Hosts to Cisco Nexus 1000V

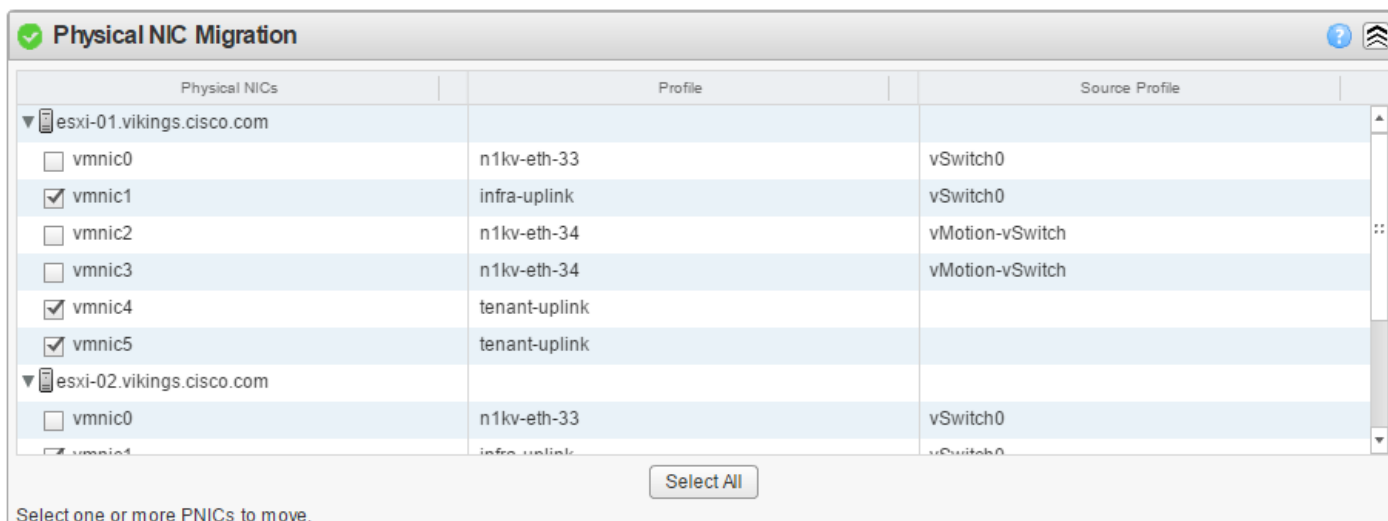
VMware vSphere Web Client

To and VMware ESXi hosts, complete the following steps:



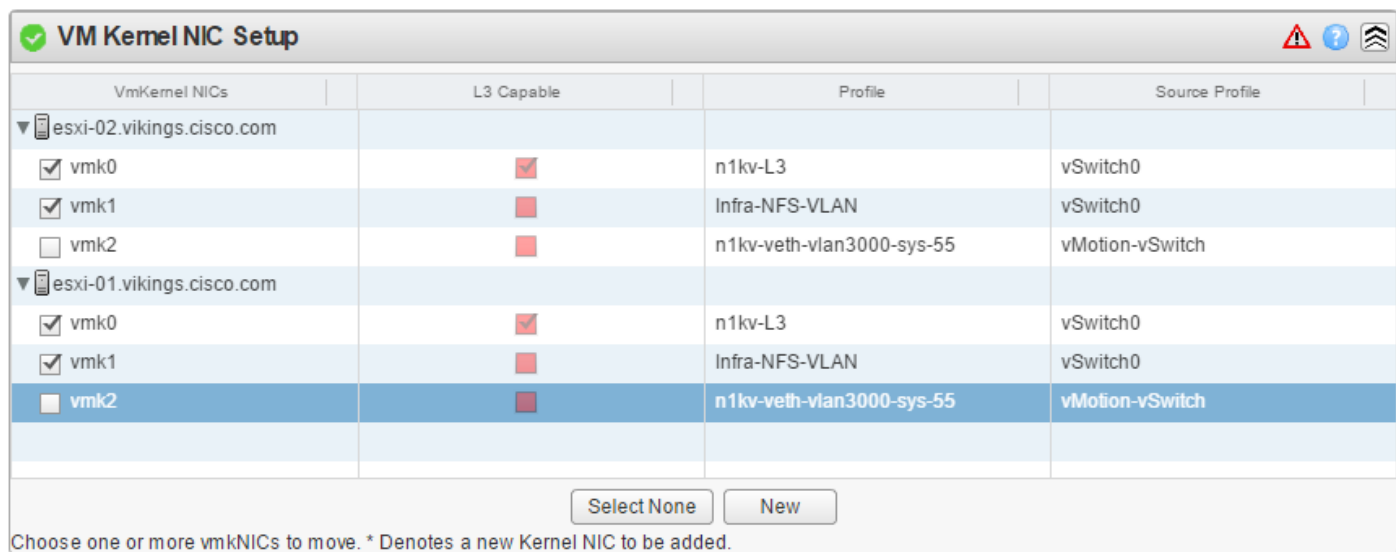
The vMotion-vSwitch will not be migrated to the Nexus 1000V.

1. Back in the VMware vSphere Web Client, from the Home tab, select Cisco Virtual Switch Update Manager.
2. Under Basic Tasks, select Nexus 1000V.
3. Select Configure.
4. Select the FlexPod-DC datacenter on the right.
5. Select the VSM on the lower right.
6. Click Manage.
7. In the center pane, select the Add Host tab.
8. Expand the FlexPod-Management ESXi Cluster and select both FlexPod Management Hosts.
9. Click Suggest.
10. Scroll down to Physical NIC Migration and expand each ESXi host.
11. On both hosts, unselect vmnic0, vmnic2, and vmnic3 and select vmnic1, vmnic4, and vmnic5. For vmnic1, select the infra-uplink Profile. For vmnic4 and vmnic5, select the tenant-uplink Profile.



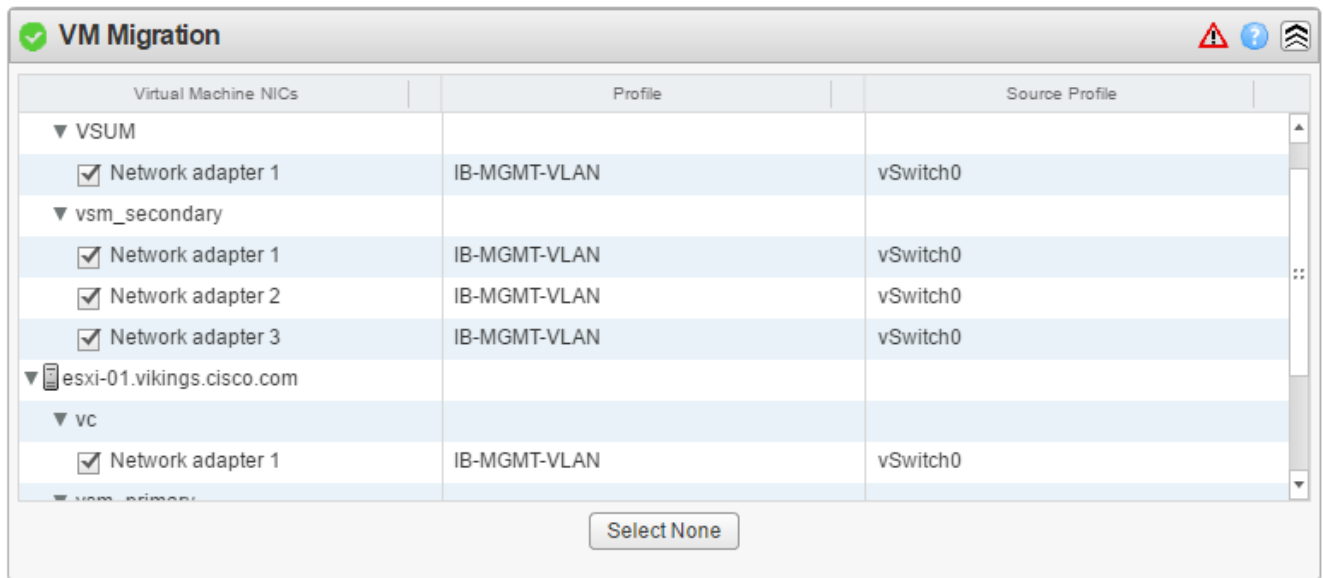
12. Scroll down to VM Kernel NIC Setup and expand both ESXi hosts.

13. Select the appropriate profiles for each vmk port, making sure to select n1kv-L3 for vmk0. Unselect vmk2, it will not be migrated away from the vMotion-vSwitch. The Profile fields should already be correctly selected.



14. Scroll down to VM Migration and expand both ESXi hosts.

15. Select the IB-MGMT-VLAN profile for all Virtual Machine interfaces.



16. Click Finish.

The progress of the virtual switch installation can be monitored from the VMware vSphere Client interface.

Migrate ESXi Host Redundant Network Ports to Cisco Nexus 1000V

To migrate the ESXi host redundant network ports, complete the following steps:

1. In the VMware vSphere Web Client window, select Home > Hosts and Clusters.
2. On the left expand the Datacenter and cluster, and select the first VMware ESXi host.
3. In the center pane, select the Manage tab, then select Networking.
4. Select Virtual switches, then vSwitch0. All of the port groups on vSwitch0 should be empty. Click the red X under Virtual switches to delete vSwitch0.
5. Click Yes to remove vSwitch0. It may be necessary to refresh the Web Client to see the deletion.
6. The Nexus 1000V VSM should now be the only virtual switch. Select it and select the third icon above it under Virtual switches (Manage the physical network adapters connected to the selected switch).
7. Click the green plus sign to add an adapter.
8. For UpLink03, select the infra-uplink port group and make sure vmnic0 is the Network adapter. Click OK.
9. Click OK to complete adding the Uplink. It may be necessary to refresh the Web Client to see the addition.
10. Repeat this procedure for the second ESXi host.

11. From the SSH client that is connected to the Cisco Nexus 1000V, run show interface status to verify that all interfaces and port channels have been correctly configured.

12. Run show module and verify that the two ESXi hosts are present as modules.

```
vsm.vikings.cisco.com - PuTTY
Mod  Ports  Module-Type          Model              Status
-----
1    0      Virtual Supervisor   Nexus1000V        active *
2    0      Virtual Supervisor   Nexus1000V        ha-standby
3    1022   Virtual Ethernet    NA                 ok
4    1022   Virtual Ethernet    NA                 ok

Mod  Sw              Hw
-----
1    5.2(1)SV3(2.1)  0.0
2    5.2(1)SV3(2.1)  0.0
3    5.2(1)SV3(2.1)  VMware ESXi 6.0.0 Releasebuild-4192238 (6.0)
4    5.2(1)SV3(2.1)  VMware ESXi 6.0.0 Releasebuild-4192238 (6.0)

Mod  Server-IP      Server-UUID          Server-Name
-----
1    10.1.156.16    NA                   NA
2    10.1.156.16    NA                   NA
3    10.1.156.26    7ea8fc3d-638a-e611-0000-000000480002  esxi-02.vikings.cisco.com
4    10.1.156.25    7ea8fc3d-638a-e611-0000-000000480001  esxi-01.vikings.cisco.com

--More--
```

13. Run copy run start.

Cisco Nexus 1000V vTracker

SSH Connection to Primary VSM

The vTracker feature on the Cisco Nexus 1000V switch provides information about the virtual network environment. To connect SSH to the primary VSM, complete the following steps:

1. From an ssh interface connected to the Cisco Nexus 1000V VSM, enter the following:

```
config t
feature vtracker
copy run start
show vtracker upstream-view
show vtracker vm-view vnic
show vtracker vm-view info
```



```
show vtracker module-view pnic
```

```
show vtracker vlan-view
```

About the Authors

John George, Technical Marketing Engineer, Cisco UCS Data Center Solutions Engineering, Cisco Systems, Inc.

John George recently moved to Cisco from Netapp and has been focused on designing, developing, validating, and supporting the FlexPod Converged Infrastructure since its inception. Before his roles with FlexPod, he supported and administered a large worldwide training network and VPN infrastructure. John holds a Master's degree in Computer Engineering from Clemson University.

Aaron Kirk, Technical Marketing Engineer, Infrastructure and Cloud Engineering, NetApp

Aaron Kirk is a Technical Marketing Engineer in the NetApp Infrastructure and Cloud Engineering team. He focuses on producing validated reference architectures that promote the benefits of end-to-end datacenter solutions and cloud environments. Aaron has been at NetApp since 2010, previously working as an engineer on the MetroCluster product in the Data Protection Group. Aaron holds a Bachelor of Science in Computer Science and a Masters of Business Administration from North Carolina State University.

Acknowledgements

For their support and contribution to the design, validation, and creation of this Cisco Validated Design, the authors would like to thank:

- Dave Klem, NetApp