FlexPod Datacenter with Cisco UCS Mini and VMware vSphere 5.5

Deployment Guide for FlexPod Datacenter with Cisco UCS Mini and VMware vSphere 5.5 with Direct Attached SAN Storage

Last Updated: March 5, 2015

Cisco Validated Design

Building Architectures to Solve Business Problems

About the Author

Gangoor Sridhara, Systems Engineer, Cisco Systems, Inc.

Gangoor Sridhara is a Systems Engineer with Cisco UCS Solutions and Performance Group. Gangoor has experience in Cisco Unified Computing System, storage and server virtualization design. Gangoor has worked on Enterprise Storage solutions, server virtualization, performance and analysis, and has worked on database performance benchmark tests. Gangoor holds certification from VMware and NetApp. Gangoor has worked as a Technical Marketing Engineer at NetApp before joining Cisco.

John George, Reference Architect, Infrastructure and Cloud Engineering, NetApp

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

Acknowledgments

For their support and contribution to the design, validation, and creation of this Cisco Validated Design, we would like to acknowledge the significant contribution and expertise that resulted in developing this document:

- John Kennedy, Technical Marketing Engineer, Cisco Systems, Inc.
- Muhammad Ashfaq, Systems Engineer, Cisco Systems, Inc.
- Lindsey Street, Solutions Architect, Infrastructure and Cloud Engineering, NetApp

About Cisco Validated Design (CVD) Program

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

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

FlexPod Datacenter with Cisco UCS Mini and VMware vSphere 5.5

Overview

The current industry trend in data center design is towards shared infrastructures. By using virtualization with prevalidated 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, customers increase agility and reduce costs. Cisco® and NetApp® have partnered to deliver FlexPod, which uses best-in-class 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

This document describes the architecture and deployment procedures of an infrastructure composed of Cisco, NetApp, and VMware® virtualization that uses FC-based storage serving Fibre Channel protocol. The intended audience for this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineering, and customers who want to deploy the core FlexPod architecture with NetApp clustered Data ONTAP® on the Cisco UCS Mini platform. Readers of this document are expected to have experience installing and configuring the solution components used to deploy the FlexPod Datacenter solution.

Purpose of This Document

This FlexPod Datacenter solution combines Cisco UCS Mini and VMware vSphere® 5.5 update 1 with NetApp FAS255x series storage arrays to support Enterprises in Datacenter environments. This document describes how to deploy the solution and use Cisco UCS Central for centralized management of the data center.

FlexPod Datacenter with Cisco UCS Mini

The data center market segment is shifting toward heavily virtualized private, hybrid, and public cloud computing models running on industry-standard systems. These environments require uniform design points that can be repeated for ease of management and scalability.

These factors have led to the need for predesigned computing, networking, and storage building blocks optimized to lower the initial design cost, simplify management, and enable horizontal scalability and high levels of utilization.

Use cases include:

- Enterprise Datacenter (small failure domains)
- Service Provider Datacenter (small failure domains)

The FlexPod® Datacenter solution combines NetApp® storage systems, Cisco® Unified Computing System servers, and Cisco Nexus fabric into a single, flexible architecture. FlexPod Datacenter can scale up for greater performance and capacity or scale out for environments that need consistent, multiple deployments; FlexPod also has the flexibility to be sized and optimized to accommodate different use cases including app workloads such as MS SQL Server, Exchange 2010, MS SharePoint 2010, SAP, Red Hat, VDI (VMware View/Citrix XenDesktop), or Secure Multi-tenancy (SMT) environments. FlexPod Datacenter delivers:

- Faster Infrastructure, Workload and Application provisioning
- Improved IT Staff Productivity
- Reduced Downtime
- Reduce Cost of Datacenter Facilities, Power, and Cooling
- Improved Utilization of Compute Resources
- Improved Utilization of Storage Resources

The FlexPod Datacenter with Cisco UCS Mini allows IT departments to address Datacenter infrastructure challenges using a streamlined architecture following compute, network and storage best practices.

Note Please refer to the FlexPod with UCS Mini Design Guide at http://www.cisco.com/c/dam/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_ucsmini_design.pdf for more design and use case details.

Architecture

The FlexPod architecture is highly modular or "podlike." Although each customer's FlexPod unit varies in its exact configuration, after a FlexPod unit is built, it can easily be scaled as requirements and demands change. The unit can be scaled both up (adding resources to a FlexPod unit) and out (adding more FlexPod units).

Specifically, FlexPod is a defined set of hardware and software that serves as an integrated foundation for both virtualized and nonvirtualized solutions. VMware vSphere built on FlexPod includes NetApp storage, NetApp Data ONTAP, Cisco Nexus networking, the Cisco Unified Computing System™ (Cisco UCS Mini), and VMware vSphere software in a single package. The design is flexible enough that

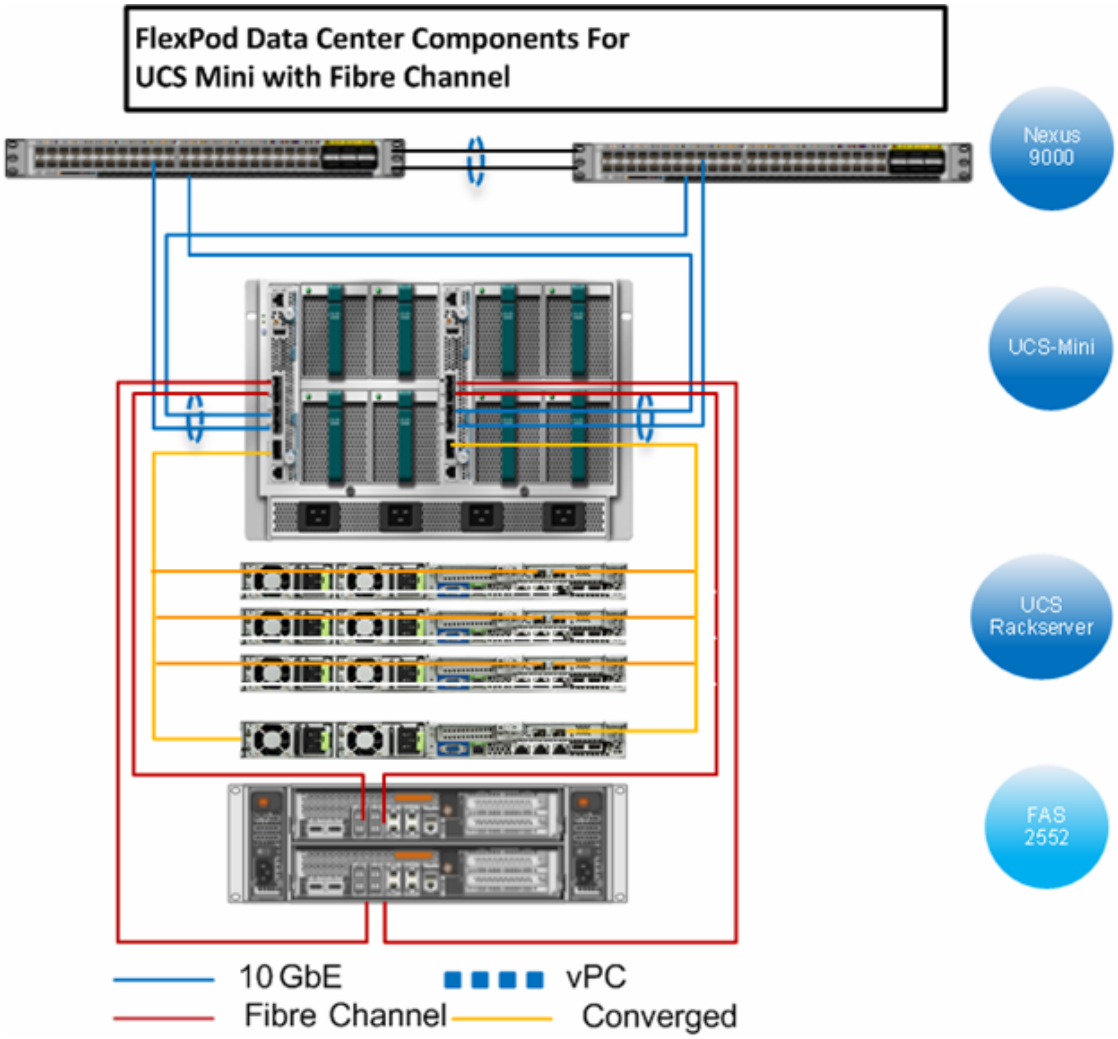
networking, computing, and storage can fit in one data center rack or be deployed according to a customer's data center design. Port density enables the networking components to accommodate multiple configurations of this kind.

One benefit of the FlexPod architecture is the ability to customize or "flex" the environment to suit a customer's requirements. This is why the reference architecture detailed in this document highlights the resiliency, cost benefit, and ease of deployment of an Fibre Channel (FC) based storage solution. A storage system capable of serving multiple protocols across a single interface allows for customer choice and investment protection because it is a wire-once architecture.

Figure 1 illustrates the VMware vSphere built on FlexPod components and the network connections for a configuration with FC-based storage. This design uses Cisco Nexus® 9372, Cisco UCS C-Series and B-Series with the Cisco UCS virtual interface card (VIC, and the NetApp FAS family of storage controllers connected in a highly available design by using Cisco Virtual PortChannels (vPCs). This infrastructure is deployed to provide FC booted hosts with block-level access to shared storage datastores.

This architecture provides FC connected storage only. Future architectures will provide FCoE and IP-based storage protocol connections to storage.

Figure 1 ***VMware vSphere Built on FlexPod Components***



The reference configuration includes:

- Two Cisco Nexus 9000 series switches
- Two Cisco UCS 6324UP Fabric Interconnects built in to Cisco UCS Mini chassis
- Support for up to 12 servers
- Support for eight Cisco UCS B-Series servers without any additional blade server chassis with Cisco virtual interface card (VIC)
- Support for Cisco UCS C-Series servers with Cisco UCS virtual interface card
- One NetApp FAS255X (HA pair) running clustered Data ONTAP

Figure 1 illustrates the VMware vSphere built on FlexPod components and network connections for a configuration with directly attached FC-based storage. These procedures cover everything from physical cabling to compute and storage configuration to configuring virtualization with VMware vSphere.

The Cisco UCS Mini supports directly attaching NetApp storage to the Cisco UCS 6324 Fabric Interconnect. This removes the requirement to have a dedicated FC switching environment as all SAN switching and zoning are performed by the Cisco UCS 6324 Fabric Interconnect and managed through the Cisco UCS Manager.

Cisco UCS Mini Overview

Cisco UCS Mini is designed for customers who need fewer servers but still want the robust management capabilities provided by Cisco UCS Manager. This solution delivers servers, storage, and 10 Gigabit networking in an easy-to-deploy, compact form factor.

Cisco UCS Mini consisits of the following components:

- Cisco UCS B200 M3 Blade Server—Delivering performance, versatility, and density without compromise, the Cisco UCS B200 M3 Blade Server addresses the broadest set of workloads.
- Cisco UCS 5108 Blade Server Chassis—A chassis can accommodate up to eight half-width Cisco UCS B200 M3 Blade Servers.
- Cisco UCS 6324 Fabric Interconnect—The Cisco UCS 6324 provides the same unified server and networking capabilities as the top-of-rack 6200 Series Fabric Interconnect embedded within the Cisco UCS 5108 Blade Server Chassis.
- Cisco UCS Manager—Cisco UCS Manager provides unified, embedded management of all software and hardware components in a Cisco UCS Mini solution.

Optional Solution Components

- Cisco UCS C220 M3 Rack-Mount Server—This one-rack-unit (1RU) server offers superior performance and density over a wide range of business workloads.
- Cisco UCS C240 M3 Rack-Mount Server—This 2RU server is designed for both performance and expandability over a wide range of storage-intensive infrastructure workloads.
- Cisco UCS Central—Cisco UCS Central manages multiple Cisco UCS Mini and Cisco UCS domains. (See the Appendix for implementation details.)

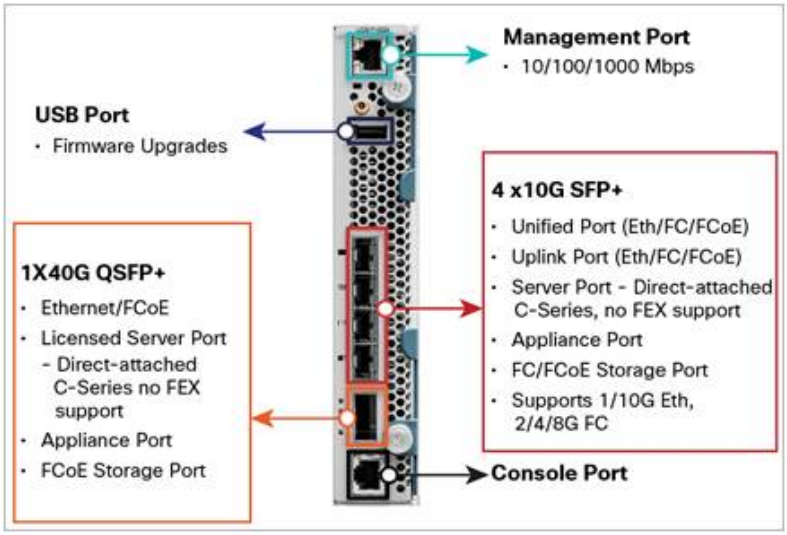
The key to delivering the power of Cisco Unified Computing System in a smaller form factor known as Cisco UCS Mini is the Cisco UCS 6324 Fabric Interconnect. The Cisco UCS 6324 Fabric Interconnect supports the integrated UCS Management software as well as, LAN and storage connectivity for the Cisco UCS 5108 Blade Server Chassis and direct-connect rack-mount servers.

From a networking perspective, the Cisco UCS 6324 Fabric Interconnect supporting deterministic, low-latency, line-rate 10 Gigabit Ethernet on all ports with switching capacity of up to 500Gbps, independent of packet size and enabled services. Sixteen 10Gbps links connect to the servers, providing a 20Gbps link from each Cisco UCS 6324 Fabric Interconnect to each server.

The fabric interconnect supports multiple traffic classes over a lossless Ethernet fabric from the blade through the fabric interconnect. Significant TCO savings come from Fibre Channel over Ethernet (FCoE)-optimized server design in which network interface cards (NICs), host bus adapters (HBAs), cables, and switches can be consolidated (Figure 3).

The Cisco UCS 6324 Fabric Interconnect Fabric Interconnect (Figure 2) is a 10 Gigabit Ethernet, FCoE, and Fibre Channel switch offering up to 500-Gbps throughput and up to four unified ports and one scalability port.

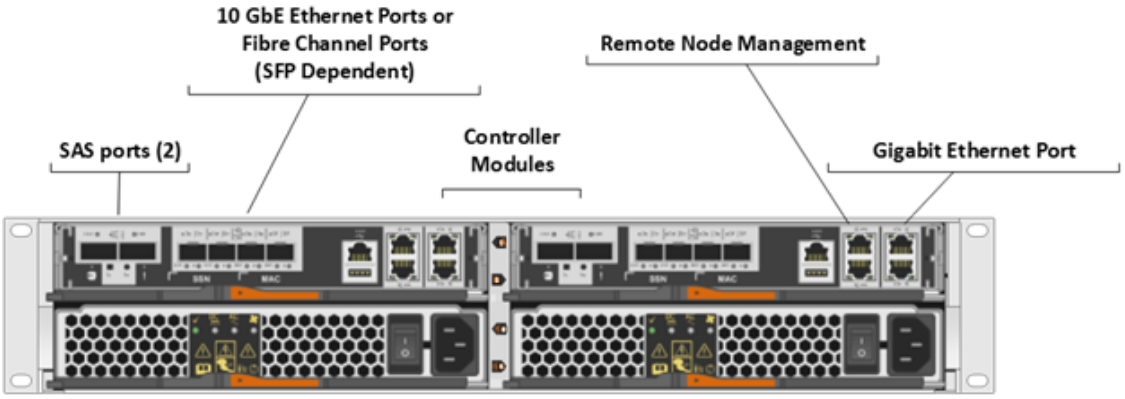
Figure 2 Cisco UCS FI-6324 Fabric Interconnect Details



FAS 2552

Storage is provided by a NetApp FAS2552 unified storage system running clustered Data ONTAP; the FAS2552 provides a highly available (HA) configuration in one chassis. The FAS controllers use a switchless cDOT deployment model through the use of 10 Gbe loopback cables. SAN A and B best practices are honored and ALUA enabled host based multi-pathing allows for redundant and optimal 8-Gbps Fibre Channel paths into the NetApp controllers. This model supports only Fibre Channel access to storage. Scalability is achieved by adding storage capacity (disk/shelves) to an existing HA pair.

Figure 3 FAS2552 System Details

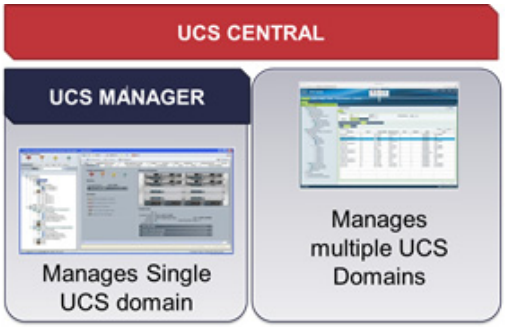


Management Tools to Facilitate Configuration and Operations

Cisco Datacenter solution component Cisco UCS Manager (UCSM) provides unified management that uses a policy-based model to improve agility and reduce risk. UCSM uses auto-discovery to detect inventory, manage, and provision system components as they are added or changed, UCSM offers a comprehensive open XML API to facilitate integration with third-party system management tools.

Cisco UCS Central Software extends the simplicity and agility of managing a single Cisco UCS domain across multiple Cisco UCS domains. Cisco UCS Central Software allows organizations to easily work on a global scale, putting computing capacity close to users while managing infrastructure with centrally defined policies. Cisco UCS Central supports a centralized policy model across multiple Cisco UCS domains in a given organization simplifying operations, visibility and control.

Figure 4 Cisco UCS Management Hierarchy



Note The implementation of Cisco UCS Central is addressed in the appendix of this document.

FlexPod with Cisco UCS Mini extends across both the FlexPod DataCenter and FlexPod Express solutions. This document covers the FlexPod DataCenter solution with FC storage and is intended to be installed in a DataCenter. The FlexPod Express solution with FC storage is covered in another document and is intended to be installed in a Remote Office or Branch Office. One method of deploying this solution is to deploy Cisco UCS Central and VMware vCenter at the DataCenter location and to remotely manage the FlexPod Express solutions at all the Remote or Branch offices from the Datacenter location.

Software Revisions

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

Table 1 Software Revisions

Layer	Compute	Version or Release	Details
Compute	Cisco UCS Fabric Interconnect FI-6324UP	3.0(1c)	Embedded management
	Cisco UCS C 220 M3	3.0(1c)	Software bundle release
	Cisco UCS B 200 M3	3.0(1c)	Software bundle release
	Cisco eNIC	2.1.2.50	Ethernet driver for Cisco VIC
	Cisco fNIC	1.6.0.10	FCoE driver for Cisco VIC
	Cisco VIC 1240	3.0(1c)	Cisco Virtual Interface card firmware
Network	Cisco Nexus switch Nexus 9372PX	6.1(2)I2(2a)	Operating system version
Storage	NetApp FAS2552-HA	Clustered Data ONTAP 8.2.2	Operating system version
Software	Cisco UCS hosts	VMware vSphere ESXi™ 5.5 U1	Operating system version
	Microsoft® .NET Framework	3.5.1	Feature enabled within Windows® operating system
	VMware vCenter™	5.5U1	VM (1 each): VMware vCenter
	NetApp OnCommand®	6.1	VM (1 each): OnCommand
	NetApp Virtual Storage Console (VSC)	5.0	VM (1 each): NetApp Virtual Storage Console—Plug-in within VMware vCenter
	Cisco Nexus 1000v	5.2(1)SV2	Virtual services blade (VSM)
	Cisco UCS Central	1.1(2a)	Manager of multiple UCS domains

Configuration Guidelines

This document provides 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. For example, node 01 and node 02 are used to identify the two NetApp storage controllers that are provisioned with this document and Cisco Nexus A and Cisco Nexus B identify 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 are identified sequentially: VM-Host-Infra-01, VM-Host-Infra-02,

and so on. 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 a0a-<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 2 describes the VLANs necessary for deployment as outlined in this guide. The VM-Mgmt VLAN is used for management interfaces of the VMware vSphere hosts. Table 3 lists the virtual storage area networks (VSANs) necessary for deployment as outlined in this guide.

Table 5 lists the configuration variables that are used throughout this document. This table can be completed based on the specific site variables and used in implementing the document configuration steps.

The Cluster management and Node management interfaces will be on the Out-of-band management VLAN. Confirm that there is a Layer 3 route between the Out-of band and In-band management VLANs.

Table 2 Necessary VLANs

VLAN Name	VLAN Purpose	ID Used in Validating This Document
Mgmt in band	VLAN for in-band management interfaces	128
Mgmt out of band	VLAN for out-of-band management interfaces	128
Native	VLAN to which untagged frames are assigned	2
vMotion	VLAN designated for the movement of VMs from one physical host to another	3173
VM Traffic	VLAN for VM application traffic	3174

Table 3 Necessary VSANss

VSAN Name	VSAN Purpose	ID Used in Validating This Document
VSAN A	VSAN for Fabric A traffic. ID matches FCoE-A VLAN	101
VSAN B	VSAN for Fabric B traffic. ID matches FCoE-B VLAN	102

Table 4 VMware Virtual Machines Created

Virtual Machine Description	Host Name
vCenter Server	
NetApp Virtual Storage Console (VSC)	
NetApp OnCommand® Unified Manager	
Cisco UCS Central	
Active Directory (if not present)	

Table 5 Configuration Variables

Variable	Description	Customer Implementation Value
<<var_node01_mgmt_ip>>	Out-of-band management IP for cluster node 01	
<<var_node01_mgmt_mask>>	Out-of-band management network netmask	
<<var_node01_mgmt_gateway>>	Out-of-band management network default gateway	
<<var_url_boot_software>>	Data ONTAP 8.2.2 URL; format: http://	
<<var_#_of_disks>>	Number of disks to assign to each storage controller	
<<var_node02_mgmt_ip>>	Out-of-band management IP for cluster node 02	
<<var_node02_mgmt_mask>>	Out-of-band management network netmask	
<<var_node02_mgmt_gateway>>	Out-of-band management network default gateway	
<<var_clustername>>	Storage cluster host name	
<<var_cluster_base_license_key>>	Cluster base license key	
<<var_fcp_license>>	License key for FCP	
<<var_password>>	Global default administrative password	
<<var_clustermgmt_ip>>	Out-of-band management IP for the storage cluster	
<<var_clustermgmt_mask>>	Out-of-band management network netmask	
<<var_clustermgmt_gateway>>	Out-of-band management network default gateway	
<<var_dns_domain_name>>	DNS domain name	
<<var_nameserver_ip>>	DNS server IP(s)	
<<var_node_location>>	Node location string for each node	
<<var_node01>>	Cluster node 01 host name	
<<var_node02>>	Cluster node 02 host name	
<<var_num_disks>>	Number of disks to assign to each storage data aggregate	
<<var_node01_sp_ip>>	Out-of-band cluster node 01 service processor management IP	
<<var_node01_sp_mask>>	Out-of-band management network netmask	
<<var_node01_sp_gateway>	Out-of-band management network default gateway	
<<var_node02_sp_ip>>	Out-of-band cluster node 02 device processor management IP	
<<var_node02_sp_mask>>	Out-of-band management network netmask	
<<var_node02_sp_gateway>	Out-of-band management network default gateway	
<<var_timezone>>	FlexPod time zone (for example, America/New_York)	
<<var_global_ntp_server_ip>>	NTP server IP address	

<<var_snmp_contact>>	Administrator e-mail address	
<<var_snmp_location>>	Cluster location string	
<<var_oncommand_server_fqdn>>	OnCommand virtual machine fully qualified domain name (FQDN)	
<<var_oncommand_server_ip>>	OnCommand virtual machine management IP Address	
<<var_oncommand_server_netmask>>	Out-of-band management network netmask	
<<var_oncommand_server_gateway>>	Out-of-band management network default gateway	
<<var_ucs_central_ip>>	UCS Central management IP	
<<var_ucs_central_netmask>>	Out-of-band management network netmask	
<<var_ucs_central_gateway>>	Out-of-band management network default gateway	
<<var_ucs_central_hostname>>	UCS Central fully qualified domain name (FQDN)	
<<var_snmp_community>>	Storage cluster SNMP v1/v2 community name	
<<var_mailhost>>	Mail server host name	
<<var_storage_admin_email>>	Administrator e-mail address	
<<var_security_cert_vserver_common_name>>	Infrastructure Vserver FQDN	
<<var_security_cert_vservser_authority>>	Infrastructure Vserver Security Certificate Authority	
<<var_security_cert_vserver_serial_no>>	Infrastructure Vserver security certificate serial number	
<<var_country_code>>	Two-letter country code	
<<var_state>>	State or province name	
<<var_city>>	City name	
<<var_org>>	Organization or company name	
<<var_unit>>	Organizational unit name	
<<var_security_cert_cluster_common_name>>	Storage cluster FQDN	
<<var_security_cert_cluster_authority>>	Storage cluster security certificate authority	
<<var_security_cert_cluster_serial_no>>	Storage cluster security certificate serial number	
<<var_security_cert_node01_common_name>>	Cluster node 01 FQDN	
<<var_security_cert_node01_authority>>	Cluster node 01 security certificate authority	
<<var_security_cert_node01_serial_no>>	Cluster node 01 security certificate serial number	
<<var_security_cert_node02_common_name>>	Cluster node 02 FQDN	
<<var_security_cert_node02_authority>>	Cluster node 02 security certificate authority	

<<var_security_cert_node02_serial_no>>	Cluster node 02 security certificate serial number	
<<var_nexus_A_hostname>>	Cisco Nexus A host name	
<<var_nexus_A_mgmt0_ip>>	Out-of-band Cisco Nexus A management IP address	
<<var_nexus_A_mgmt0_netmask>>	Out-of-band management network netmask	
<<var_nexus_A_mgmt0_gw>>	Out-of-band management network default gateway	
<<var_nexus_B_hostname>>	Cisco Nexus B host name	
<<var_nexus_B_mgmt0_ip>>	Out-of-band Cisco Nexus B management IP address	
<<var_nexus_B_mgmt0_netmask>>	Out-of-band management network netmask	
<<var_nexus_B_mgmt0_gw>>	Out-of-band management network default gateway	
<<var_ib-mgmt_vlan_id>>	In-band management network VLAN ID	
<<var_native_vlan_id>>	Native VLAN ID	
<<var_oob-mgmt_vlan_id>>	Out of band management network VLAN ID	
<<var_nfs_vlan_id>>	NFS VLAN ID	
<<var_pkt-ctrl_vlan_id>>	Cisco Nexus 1000v packet control VLAN ID	
<<var_vmotion_vlan_id>>	VMware vMotion® VLAN ID	
<<var_vm-traffic_vlan_id>>	VM traffic VLAN ID	
<<var_nexus_vpc_domain_id>>	Unique Cisco Nexus switch VPC domain ID	
<<var_vsan_a_id>>	Fabric A VSAN ID	
<<var_vsan_b_id>>	Fabric B VSAN ID	
<<var_ucs_clustername>>	Cisco UCS Manager cluster host name	
<<var_ucsa_mgmt_ip>>	Cisco UCS Fabric Interconnect (FI) A out-of-band management IP address	
<<var_ucsa_mgmt_mask>>	Out-of-band management network netmask	
<<var_ucsa_mgmt_gateway>>	Out-of-band management network default gateway	
<<var_ucs_cluster_ip>>	Cisco UCS Manager cluster IP address	
<<var_ucsb_mgmt_ip>>	Cisco UCS FI B out-of-band management IP address	
<<var_vsm_domain_id>>	Unique Cisco Nexus 1000v virtual supervisor module (VSM) domain ID	
<<var_vsm_mgmt_ip>>	Cisco Nexus 1000v VSM management IP address	
<<var_vsm_mgmt_mask>>	In-band management network netmask	
<<var_vsm_mgmt_gateway>>	In-band management network default gateway	
<<var_vsm_hostname>>	Cisco Nexus 1000v VSM host name	
<<var_vcenter_server_ip>>	vCenter Server IP	
<<var_nodename>>	Name of node	

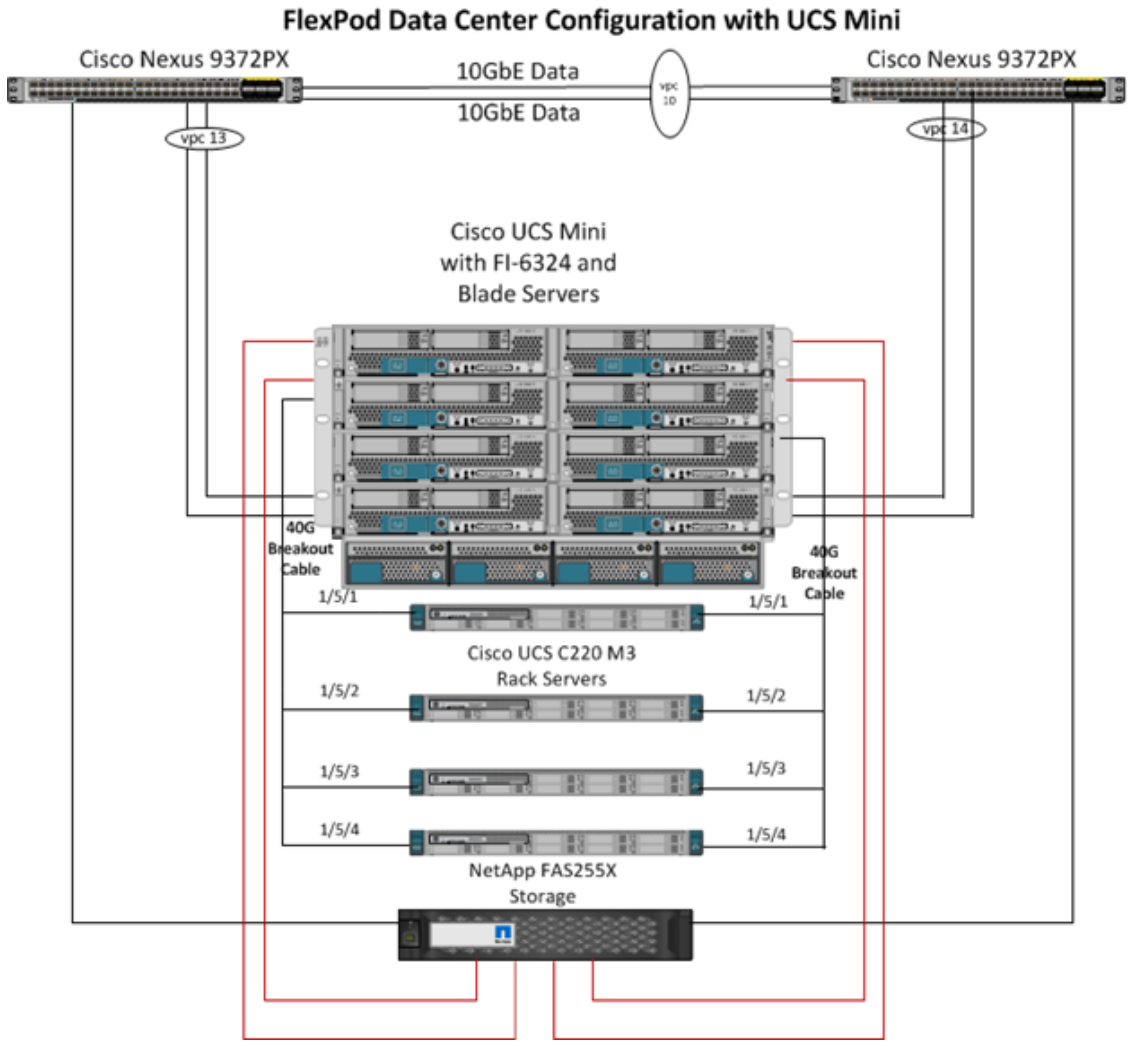
<<var_node01_rootaggrname>>	Root aggregate name of Node 01	
<<var_clustermgmt_port>>	Port for cluster management	
<<var_global_domain_name>>	Domain name	
<<var_dns_ip>>	IP address of the DNS server	
<<var_vsadmin_password>>	Password for VS admin account	
<<var_vserver_mgmt_ip>>	Management IP address for Vserver	
<<var_vserver_mgmt_mask>>	Subnet mask for Vserver	
<<var_rule_index>>	Rule index number	
<<var_ftp_server>>	IP address for FTP server	
<<var_vm_host_infra_01_A_wwpn>>	WWPN of VM-Host-Infra-01 vHBA-A	
<<var_vm_host_infra_02_A_wwpn>>	WWPN of VM-Host-Infra-02 vHBA-A	
<<var_fcp_lif01a_wwpn>>	WWPN of FCP_LIF01a	
<<var_fcp_lif02a_wwpn>>	WWPN of FCP_LIF02a	
<<var_vm_host_infra_01_B_wwpn>>	WWPN of VM-Host-Infra-01 vHBA-B	
<<var_vm_host_infra_02_B_wwpn>>	WWPN of VM-Host-Infra-02 vHBA-B	
<<var_fcp_lif01b_wwpn>>	WWPN of FCP_LIF01b	
<<var_fcp_lif02b_wwpn>>	WWPN of FCP_LIF02b	
<<var_vmhost_infra01_ip>>	VMware ESXi host 01 in-band management IP	
<<var_vmhost_infra02_ip>>	VMware ESXi host 02 in-band management IP	
<<var_vmotion_vlan_id_ip_host-01>>	vMotion VLAN IP address for ESXi host 01	
<<var_vmotion_vlan_id_mask_host-01>>	vMotion VLAN netmask for ESXi host 01	
<<var_vmotion_vlan_id_ip_host-02>>	vMotion VLAN IP address for ESXi host 02	
<<var_vmotion_vlan_id_mask_host-02>>	vMotion VLAN netmask for ESXi host 02	

Physical Infrastructure

FlexPod Cabling on Clustered Data ONTAP

Figure 5 illustrates the cabling diagram for a FlexPod configuration running clustered Data ONTAP.

Figure 5 FlexPod Cabling Diagram in Clustered Data ONTAP



The information provided in Table 6 through Table 13 corresponds to device connectivityin the architecture shown in Figure 5.

Table 6 Cisco Nexus 9372PX A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port	Cabling Code
Cisco Nexus 9372PX A	Eth1/3	10GbE	Cisco UCS Fabric Interconnect A	Eth1/3	
	Eth1/4	10GbE	Cisco UCS Fabric Interconnect B	Eth1/3	
	Eth1/13	10GbE	Cisco Nexus 9372PX B	Eth1/13	
	Eth1/14	10GbE	Cisco Nexus 9372PX B	Eth1/14	
	MGMT0	GbE	GbE management switch	Any	

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

Table 7 Cisco Nexus 9372PX B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port	Cabling Code
Cisco Nexus 9372PX B	Eth1/3	10GbE	Cisco UCS Fabric Interconnect A	Eth1/4	
	Eth1/4	10GbE	Cisco UCS Fabric Interconnect B	Eth1/4	
	Eth1/13	10GbE	Cisco Nexus 9372PX A	Eth1/13	
	Eth1/14	10GbE	Cisco Nexus 9372PX A	Eth1/14	
	MGMT0	GbE	GbE management switch	Any	

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

Table 8 NetApp controller A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port	Cabling Code
NetApp controller A	e0M	GbE	1000MbE management switch	Any	
	e0P	GbE	NetApp Controller B	e0P	
	e0a	GbE	gbE management switch	Any	
	0c	8Gb/s FC	Cisco Fabric Interconnect FI-6324 A	Eth1/1	
	0d	8Gb/s FC	Cisco Fabric Interconnect FI-6324 B	Eth1/1	
	e0e	10GbE	NetApp Controller B	e0e	
	e0f	10GbE	NetApp Controller B	e0f	

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

Table 9 NetApp controller B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port	Cabling Code
NetApp controller B	e0M	GbE	GbE management switch	Any	
	e0P	GbE	NetApp Controller B	e0P	
	e0a	GbE	gbE management switch	Any	
	0c	8Gb/s FC	Cisco Fabric Interconnect FI-6324 A	Eth1/2	
	0d	8Gb/s FC	Cisco Fabric Interconnect FI-6324 B	Eth1/2	
	e0e	10GbE	NetApp Controller A	e0e	
	e0f	10GbE	NetApp Controller A	e0f	

Note When the term `e0M` is used, the physical Ethernet port to which the Table 8 and Table 9 reference is the port indicated by a wrench icon on the rear of the chassis.

Table 10 Cisco UCS Fabric Interconnect A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port	Cabling Code
Cisco UCS Fabric Interconnect A	Eth1/1	8 Gb/s FC	NetApp Storage Node A	0c	
	Eth1/2	8 Gb/s FC	NetApp Storage Node B	0c	
	Eth1/3	10GbE	Cisco Nexus 9372PX A	Eth1/3	
	Eth1/4	10GbE	Cisco Nexus 9372PX B	Eth1/3	
	MGMT0	GbE	GbE Management Switch	Any	

Table 11 Cisco UCS Fabric Interconnect B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port	Cabling Code
Cisco UCS Fabric Interconnect B	Eth1/1	8 Gb/s FC	NetApp Storage Node A	0c	
	Eth1/2	8 GB/s FC	NetApp Storage Node B	0c	
	Eth1/3	10GbE	Cisco Nexus 9372PX A	Eth1/4	
	Eth1/4	10GbE	Cisco Nexus 9372PX B	Eth1/4	
	MGMT0	GbE	GbE Management Switch	Any	

Table 12 Cisco UCS C-Series 3 (C220 M3)

Local Device	Local Port	Connection	Remote Device	Remote Port	Cabling Code
Cisco UCS C-Series 3 UCS C220 M3	Port 1	10GbE	Fabric Interconnect A	Eth 1/5/1 (40Gb breakout cable)	
	Port 2	10GbE	Fabric Interconnect B	Eth 1/5/1 (40Gb breakout cable)	

Table 13 Cisco UCS C-Series 3 (C220 M3)

Local Device	Local Port	Connection	Remote Device	Remote Port	Cabling Code
Cisco UCS C-Series 3 UCS C220 M3	Port 1	10GbE	Fabric Interconnect A	Eth 1/5/2 (40Gb breakout cable)	
	Port 2	10GbE	Fabric Interconnect B	Eth 1/5/2 (40Gb breakout cable)	

Table 14 Cisco VIC Card Layout for Single-Wire Management

Slot	Part Number	Description
	Cisco UCS VIC1240	4-port 10 Gigabit Ethernet, Fibre Channel over Ethernet (FCoE)-capable modular LAN on motherboard (mLOM) designed exclusively for the M3 generation of Cisco UCS B-Series Blade Servers. When used in combination with an optional Port Expander, the Cisco UCS VIC 1240 capabilities can be expanded to eight ports of 10 Gigabit Ethernet.
	Cisco UCS VIC1225	A Cisco® innovation, the Cisco UCS Virtual Interface Card (VIC) 1225 is a dual-port Enhanced Small Form-Factor Pluggable (SFP+) 10 Gigabit Ethernet and Fibre Channel over Ethernet (FCoE)-capable PCI Express (PCIe) card designed exclusively for Cisco UCS C-Series

Storage Configuration

Controller FAS255X Series

Table 15 Controller FAS25XX Series Prerequisites

Controller FAS25XX Series Prerequisites
To plan the physical location of the storage systems, refer to the Site Requirements Guide and refer to the following sections: • Site Preparation • System Connectivity Requirements • Circuit Breaker, Power Outlet Balancing, System Cabinet Power Cord Plugs, and Console Pinout Requirements • FAS255X • Series Systems

NetApp Hardware Universe

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

To verify component compatibility, complete the following steps:

1. Confirm that the hardware and software components are supported with the version of Data ONTAP that you plan to install by checking the NetApp Hardware Universe at the NetApp Support site.
2. Access the Hardware Universe Application to view the System Configuration guides. Click the Controllers tab to view the compatibility between Data ONTAP software versions and NetApp storage appliances with the desired specifications.
3. Alternatively, to compare components by storage appliance, click Compare Storage Systems.

Controllers

Follow the physical installation procedures for the controllers in the FAS255x documentation located at the NetApp Support site.

Disk Shelves

NetApp storage systems support a wide variety of disk shelves and disk drives. The complete list of supported disk shelves is available at the NetApp Support site.

For SAS disk shelf and NetApp storage controller cabling guidelines, refer to the SAS Disk Shelves Universal SAS and ACP Cabling Guide.

Clustered Data ONTAP 8.2.2

Complete the Configuration Worksheet

Before running the setup script, complete the configuration worksheet from the product manual. The configuration worksheet is available in the Clustered Data ONTAP 8.2 Software Setup Guide at the NetApp Support site.

Note This system will be set up in a two-node switchless cluster configuration.

Table 16 Clustered Data ONTAP Software Installation Prerequisites

Cluster Detail	Cluster Detail Value
Cluster node 01 IP address	`<<var_node01_mgmt_ip>>`
Cluster node 01 netmask	`<<var_node01_mgmt_mask>>`
Cluster node 01 gateway	`<<var_node01_mgmt_gateway>>`
Cluster node 02 IP address	`<<var_node02_mgmt_ip>>`
Cluster node 02 netmask	`<<var_node02_mgmt_mask>>`
Cluster node 02 gateway	`<<var_node02_mgmt_gateway>>`
Data ONTAP 8.2.2 URL	`<<var_url_boot_software>>`

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. Enable autoboot.

   ```
   setenv AUTOBOOT true
   ```
3. Allow the system to boot up.

   ```
   autoboot
   ```
4. Press Ctrl-C when prompted.

Note If Data ONTAP 8.2.2 is not the version of software being booted, continue with the following steps to install new software. If Data ONTAP 8.2.2 is the version being booted, select option 8 and `yes` to reboot the node and go to step 14.

5. To install new software, first select option 7.

   ```
   7
   ```
6. Answer `yes` to perform an upgrade.

   ```
   y
   ```
7. Select e0M for the network port you want to use for the download.

   ```
   e0M
   ```
8. Select yes to reboot now.

   ```
   y
   ```

9. After reboot, enter the IP address, netmask, and default gateway for e0M in their respective places.

```
<<var_node01_mgmt_ip>> <<var_node01_mgmt_mask>> <<var_node01_mgmt_gateway>>
```

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

Note This web server must be pingable.

```
<<var_url_boot_software>>
```

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

```
Enter
```

12. Enter yes to set the newly installed software as the default to be used for subsequent reboots.

```
y
```

13. Enter yes to reboot the node.

```
y
```

Note 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.

14. Press Ctrl-C to exit autoboot when you see this message:

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

15. From the Loader-A prompt, enter:

```
printenv
```

Note If `bootarg.init.boot_clustered` `true` is not listed, the system is not set to boot in clustered Data ONTAP.

16. If the system is not set to boot in clustered Data ONTAP, at the Loader-A prompt, run the following command to make sure the system boots in clustered Data ONTAP:

```
setenv bootarg.init.boot_clustered true
setenv bootarg.bsdportname e0M
```

17. At the Loader-A prompt, enter:

```
autoboot
```

18. When you see `Press Ctrl-C for Boot Menu:`

```
Ctrl - C
```

19. Select option 4 for clean configuration and initialize all disks.

```
4
```

20. Answer yes to `Zero disks, reset config and install a new file system.`

```
y
```

21. Enter yes to erase all the data on the disks.

```
y
```

Note The initialization and creation of the root volume can take 90 minutes or more to complete, depending on the number of disks attached. After initialization is complete, the storage system reboots. You can continue to node 02 configuration while the disks for node 01 are zeroing.

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. Enable autoboot.

   ```
   setenv AUTOBOOT true
   ```
3. Allow the system to boot up.

   ```
   autoboot
   ```
4. Press Ctrl-C when prompted.

   ```
   Ctrl-C
   ```

Note If Data ONTAP 8.2.2 is not the version of software being booted, continue with the following steps to install new software. If Data ONTAP 8.2.2 is the version being booted, select option 8 and `yes` to reboot the node and go to step 14.

5. To install new software first, select option 7.

   ```
   7
   ```
6. Answer yes to perform a nondisruptive upgrade.

   ```
   y
   ```
7. Select e0M for the network port you want to use for the download.

   ```
   e0M
   ```
8. Select yes to reboot now.

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

   ```
   <<var_node02_mgmt_ip>> <<var_node02_mgmt_mask>> <<var_node02_mgmt_gateway>>
   ```
10. Enter the URL where the software can be found.

Note This web server must be pingable.

11. <<var_url_boot_software>>
12. Press Enter for the user name, indicating no user name.

    ```
    Enter
    ```
13. Select yes to set the newly installed software as the default to be used for subsequent reboots.

    ```
    y
    ```
14. Select yes to reboot the node.

    ```
    y
    ```

Note 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.

15. Press Ctrl-C to exit autoboot when you see this message:

    ```
    Starting AUTOBOOT press Ctrl-C to abort…
    ```
16. From the Loader-A prompt, enter:

```
printenv
```

Note If `bootarg.init.boot_clustered true` is not listed, the system is not set to boot in clustered Data ONTAP.

17. If the system is not set to boot in clustered Data ONTAP, at the Loader-A prompt, enter the following command to make sure the system boots in clustered Data ONTAP:

```
setenv bootarg.init.boot_clustered true
setenv bootarg.bsdportname e0M
```

18. At the Loader-A prompt, enter:

```
autoboot
```

19. When you see `Press Ctrl-C for Boot Menu`, enter:

```
Ctrl - C
```

20. Select option 4 for clean configuration and initialize all disks.

```
4
```

21. Answer yes to `Zero disks, reset config and install a new file system.`

```
y
```

22. Enter yes to erase all the data on the disks.

```
y
```

Note The initialization and creation of the root volume can take 90 minutes or more to complete, depending on the number of disks attached. When initialization is complete, the storage system reboots.

Cluster Create in Clustered Data ONTAP

Table 17 Cluster Create in Clustered Data ONTAP Prerequisites

Cluster Detail	Cluster Detail Value
Cluster name	`<<var_clustername>>`
Clustered Data ONTAP base license	`<<var_cluster_base_license_key>>`
Cluster management IP address	`<<var_clustermgmt_ip>>`
Cluster management netmask	`<<var_clustermgmt_mask>>`
Cluster management port	`<<var_clustermgmt_port>>`
Cluster management gateway	`<<var_clustermgmt_gateway>>`
Cluster node01 IP address	`<<var_node01_mgmt_ip>>`
Cluster node01 netmask	`<<var_node01_mgmt_mask>>`
Cluster node01 gateway	`<<var_node01_mgmt_gateway>>`

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.

The Cluster Setup wizard starts running on the console.

```
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}:
```

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

To create a new cluster, complete the following steps:

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

   ```
   create
   ```
2. Type `no` for single node cluster option

   ```
   Do you intend for this node to be used as a single node cluster? {yes, no}
   [no]: no
   ```
3. Type `no` for cluster network using network switches.

   ```
   Will the cluster network be configured to use network switches? [yes]:no
   ```
4. Activate HA and set storage failover.

   ```
   Non-HA mode, Reboot node to activate HADo you want to reboot now to set
   storage failover (SFO) to HA mode? {yes, no}[yes]: Enter
   ```
5. After the reboot, enter `admin` in the login prompt.

   ```
   admin
   ```
6. Enter `create` on the cluster setup wizard to create the cluster.

   ```
   create
   ```
7. Repeat steps 3 and 4, if the cluster setup wizard prompts again.
8. The system defaults are displayed. Enter `no` to use the system defaults. Use the following prompts to configure the cluster ports.

   ```
   Existing cluster interface configuration found:

   Port    MTU     IP              Netmask
   e0e     9000    169.254.166.221 255.255.0.0

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

   System Defaults:Private cluster network ports [e0e,e0f].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
   ```
9. The steps to create a cluster are displayed.

   ```
   Enter the cluster name: <<var_clustername>>
   Enter the cluster base license key: <<var_cluster_base_license_key>>
   Creating cluster <<var_clustername>>
   Enter an additional license key []:<<var_fcp_license>>
   ```

Note The cluster is created. This can take a minute or two.

Note For this validated architecture NetApp recommends installing license keys for NetApp SnapRestore®, NetApp FlexClone®, and NetApp SnapManager® Suite. Additionally, install all required storage protocol licenses. After you finish entering the license keys, press Enter.

```
Enter the cluster administrators (username "admin") password:
<<var_password>>
Retype the password: <<var_password>>
Enter the cluster management interface port [e0a]: e0a
Enter the cluster management interface IP address: <<var_clustermgmt_ip>>
Enter the cluster management interface netmask: <<var_clustermgmt_mask>>
Enter the cluster management interface default gateway:
<<var_clustermgmt_gateway>>
```

10. Enter the DNS domain name.

```
Enter the DNS domain names:<<var_dns_domain_name>>
Enter the name server IP addresses:<<var_nameserver_ip>>
```

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

11. Set up the node.

```
Where is the controller located []:<<var_node_location>>
Enter the node management interface port [e0M]: e0M
Enter the node management interface IP address: <<var_node01_mgmt_ip>>
Enter the node management interface netmask:<<var_node01_mgmt_mask>>
Enter the node management interface default
gateway:<<var_node01_mgmt_gateway>>
```

Note The node management interface can be on the same subnet as the cluster management interface, or it can be on a different subnet.

12. Enter no for IPV4 DHCP on the service processor.

```
Enable IPv4 DHCP on the service processor interface [yes]: no
```

13. Set up the service processor (SP).

```
Enter the service processor interface IP address: <<var_node01_sp_ip>>
Enter the service processor interface netmask: <<var_node01_sp_netmask>>
Enter the service processor interface default gateway:
<<var_node01_sp_gateway>>
```

14. Log in to the cluster interface with the admin user id and <<var_password>>.

Cluster Join-In Clustered Data ONTAP

Table 18 Cluster Join-In Clustered Data ONTAP Prerequisites

Cluster Detail	Cluster Detail Value
Cluster name	<<var_clustername>>
Cluster management IP address	<<var_clustermgmt_ip>>
Cluster node02 IP address	<<var_node02_mgmt_ip>>
Cluster node02 netmask	<<var_node02_mgmt_mask>>

Cluster node02 gateway	<<var_node02_mgmt_gateway>>

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.

To join the cluster, complete the following steps:

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

   ```
   admin
   ```

2. The Cluster Setup wizard starts running on the console.

   ```
   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}:
   ```

Note 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. To activate HA and set storage failover, complete the following steps.

   ```
   Non-HA mode, Reboot node to activate HADo you want to reboot now to set
   storage failover (SFO) to HA mode? {yes, no}[yes]: Enter
   ```

5. After the reboot, continue the Cluster Join process.

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

   ```
   Existing cluster interface configuration found:

   Port    MTU     IP              Netmask
   e0e     9000    169.254.935.144 255.255.0.0

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

   System Defaults:Private cluster network ports [e0e,e0f].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
   ```

Note The cluster creation process can take a minute or two.

7. The steps to join a cluster are displayed.

   ```
   Enter the name of the cluster you would like to join
   [<<var_clustername>>]:Enter
   ```

Note The node should find the cluster name.

8. Set up the node.

```
Enter the node management interface port [e0M]: e0M
Enter the node management interface IP address: <<var_node02_mgmt_ip>>
Enter the node management interface netmask: <<var_node02_netmask>>Enter
Enter the node management interface default gateway: <<var_node02_gw>>Enter
```

Note The node management interface can be on the same subnet as the cluster management interface, or it can be on a different subnet.

9. Type no for IPV4 DHCP on the service processor.

```
Enable IPv4 DHCP on the service processor interface [yes]: no
```

10. Set up the Service Processor (SP).

```
Enter the service processor interface IP address: <<var_node01_sp_ip>>
Enter the service processor interface netmask: <<var_node01_sp_netmask>>
Enter the service processor interface default gateway:
<<var_node01_sp_gateway>>
```

Log in to the Cluster

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

Zero All Spare Disks

To zero all spare disks in the cluster, complete the following step:

1. Run the following command:

```
disk zerospares
```

Note Disk autoassign should have assigned half of the connected disks to each node in the HA pair. If a different disk assignment is required, disk auto-assignment must be disabled on both nodes in the HA pair by running the `disk option modify` command. Spare disks can then be moved from one node to another by running the `disk removeowner` and `disk assign` commands.

Set Onboard UTA2 Ports Personality

To set onboard UTA2 port personalities, complete the following steps:

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

```
clus::> ucadmin show
                     Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------  -----------
clus-01       0c       fc       target     -        -          online
clus-01       0d       fc       target     -        -          online
```

```
clus-01       0e       cna      target     -        -          online
clus-01       0f       cna      target     -        -          online
clus-02       0c       fc      target     -        -         online
clus-02       0d       fc      target     -        -         online
clus-02       0e       cna      target     -        -          online
clus-02       0f       cna      target     -        -          online
8 entries were displayed.
```

2. Verify that the Current Mode of the fc ports (0c and 0d) that are in use is `fc` and the Current Type is set to `target`. If not, run the following command to change the port personality:

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

Note The ports must be offline to run the previous command. To take an adapter offline, run the `fcp adapter modify –node <home node of the port> -adapter <port name> -state down` command. Ports must be converted in pairs, for example, 0c and 0d. After which, 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:

1. Run the following command:

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

Failover Groups Management in Clustered Data ONTAP

To create a management port failover group, complete the following step:

1. Run the following commands:

```
network interface failover-groups create -failover-group fg-cluster-mgmt
-node <<var_node01>> -port e0a
network interface failover-groups create -failover-group fg-cluster-mgmt
-node <<var_node02>> -port e0a
```

Assign Management Failover Group to Cluster Management LIF

To assign the management port failover group to the cluster management LIF, complete the following step:

1. Run the following commands:

```
network interface modify –vserver <<var_clustername>> -lif cluster_mgmt
–failover-group fg-cluster-mgmt
```

Failover Groups Node Management in Clustered Data ONTAP

To create a management port failover group, complete the following step:

1. Run the following commands:

```
network interface failover-groups create -failover-group fg-node-mgmt01
-node <<var_node01>> -port e0a
network interface failover-groups create -failover-group fg-node-mgmt01
-node <<var_node01>> -port e0M
network interface failover-groups create -failover-group fg-node-mgmt02
-node <<var_node02>> -port e0a
network interface failover-groups create -failover-group fg-node-mgmt02
-node <<var_node02>> -port e0M
```

Assign Node Management Failover Groups to Node Management LIFs

To assign the management port failover group to the cluster management LIF, complete the following step:

1. Run the following commands:

```
network interface modify -vserver <<var_node01>> -lif mgmt1 -auto-revert
true -failover-group fg-node-mgmt01
network interface modify –vserver <<var_node02>> -lif mgmt1 –auto-revert
true –failover-group fg-node-mgmt02
```

Aggregates in Clustered Data ONTAP

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

To create new aggregates, complete the following steps:

1. Run the following commands:

```
aggr create -aggregate aggr1_node1 -nodes <<var_node01>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_node2 -nodes <<var_node02>> -diskcount
<<var_num_disks>>
```

Note Retain at least one disk (select the largest disk) in the configuration as a spare. A best practice is to have at least one spare for each disk type and size.

Note Start with five disks initially; you can add disks to an aggregate when additional storage is required.

Note 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. Disable NetApp Snapshot® copies for the two data aggregates recently created.

```
node run <<var_node01>> aggr options aggr1_node1 nosnap on
node run <<var_node02>> aggr options aggr1_node2 nosnap on
```

3. Delete any existing Snapshot copies for the two data aggregates.

```
node run <<var_node01>> snap delete -A -a -f aggr1_node1
node run <<var_node02>> snap delete -A -a -f aggr1_node2
```

4. 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 <<var_node01_rootaggrname>>
```

Resize Node Root Volumes

To resize the node root volumes to avoid the root aggregate full warning, complete the following step:

1. Resize the node root volumes.

```
volume size -vserver <<var_node01>> -volume vol0 -new-size 250GB
volume size -vserver <<var_node02>> -volume vol0 -new-size 250GB
```

Storage Failover in Clustered Data ONTAP

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

1. Verify the status of storage failover.

```
storage failover show
```

Note Both the nodes <<var_node01>> and <<var_node02>> must be capable of performing a takeover. Go to step 5, if the nodes are capable of performing a takeover.

2. Enable failover on one of the two nodes.

```
storage failover modify -node <<var_node01>> -enabled true
```

Note Enabling failover on one node enables it for both nodes.

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

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

```
cluster ha show
```

4. Go to step 6 if high availability is configured.
5. Enable HA mode only for the two-node cluster.

Note Do not run this command for clusters with more than two nodes because it will cause 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 <<var_node02_mgmt_ip>> -node
<<var_node01>>
storage failover modify –hwassist-partner-ip <<var_node01_mgmt_ip>> -node
<<var_node02>>
```

Disable Flow Control on 10GbE and 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 step:

1. Run the following commands:

```
net port modify -node <<var_node01>> -port e0e,e0f -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

net port modify -node <<var_node02>> -port e0e,e0f -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
net port show –fields flowcontrol-admin
```

Disable Unused FcoE Ports

Unused switchless cluster interconnect FCoE ports should be disabled. To disable these ports, complete the following steps:

1. Run the following commands:

```
fcp adapter modify -node <<var_node01>> -adapter 0c -state down
fcp adapter modify -node <<var_node01>> -adapter 0d -state down
fcp adapter modify -node <<var_node02>> -adapter 0c -state down
?
fcp adapter modify -node <<var_node02>> -adapter 0d -state down
fcp adapter show -fields state
```

NTP in Clustered Data ONTAP

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

1. To set the time zone for the cluster, run the following command:

   ```
   timezone <<var_timezone>>
   ```

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

2. To set the date for the cluster, run the following command:

   ```
   date <ccyymmddhhmm.ss>
   ```

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

3. Configure the Network Time Protocol (NTP) for each node in the cluster.

```
system services ntp server create -node <<var_node01>> -server
<<var_global_ntp_server_ip>> system services ntp server create -node
<<var_node02>> -server <<var_global_ntp_server_ip>>
```

SNMP in Clustered Data ONTAP

To configure SNMP, complete the following steps:

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

```
snmp contact <<var_snmp_contact>>
snmp location "<<var_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 <<var_oncommand_server_fqdn>>
```

SNMPv1 in Clustered Data ONTAP

To configure SNMPv1, complete the following step:

1. Set the shared secret plain-text password, which is called a community.

```
snmp community delete all
snmp community add ro <<var_snmp_community>>
Use the delete all command with caution. If community strings are used for
other monitoring products, the delete all command will remove them.
```

SNMPv3 in Clustered Data ONTAP

SNMPv3 requires that a user be defined and configured for authentication. To configure SNMPv3, complete the following step:

1. Create a user called snmpv3user.

```
security login create -username snmpv3user -authmethod usm -application snmp
```

2. Enter the authoritative entity's engine ID and select md5 as the authentication protocol.
3. Run the security snmpusers command to view the engine ID.
4. Enter an eight-character minimum-length password for the authentication protocol, when prompted.
5. Select des as the privacy protocol.
6. Enter an eight-character minimum-length password for the privacy protocol, when prompted.

AutoSupport HTTPS in Clustered Data ONTAP

AutoSupport sends support summary information to NetApp through HTTPS. To configure AutoSupport, complete the following step:

1. Run the following command:

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

Cisco Discovery Protocol in Clustered Data ONTAP

To enable CDP on the NetApp storage controllers, complete the following step:

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

1. Enable CDP on Data ONTAP.

```
node run -node <<var_node01>> options cdpd.enable on
node run -node <<var_node02>> options cdpd.enable on
```

Vserver (Storage Virtual Machine)

To create an infrastructure Vserver, complete the following steps:

1. Run the Vserver setup wizard.

```
vserver setup

Welcome to the Vserver Setup Wizard, which will lead you through
the steps to create a virtual storage server that serves data to clients.

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 your answers to previous questions, and
"exit" if you want to quit the Vserver Setup Wizard. Any changes
you made before typing "exit" will be applied.

You can restart the Vserver Setup Wizard by typing "vserver setup". To
accept a default
or omit a question, do not enter a value.

Vserver Setup wizard creates and configures only data Vservers.
If you want to create a Vserver with Infinite Volume use the vserver create
command.


Step 1. Create a Vserver.
You can type "back", "exit", or "help" at any question.
```

2. Enter the Vserver name.

```
Enter the Vserver name:Infra_Vserver
```

3. Select the Vserver data protocols to configure.

```
Choose the Vserver data protocols to be configured {nfs, cifs, fcp, iscsi,
ndmp}: fcp
```

4. Select the Vserver client services to configure.

```
Choose the Vserver client services to configure {ldap, nis, dns}:Enter
```

5. Enter the Vserver root volume aggregate:

```
Enter the Vserver's root volume aggregate {aggr1_node1, aggr1_node2}
[aggr1_node1]:aggr1_node1
```

6. Enter the Vserver language setting. English is the default

```
[C].
```

7. Enter the Vserver language setting, or enter `help` to see all languages

```
[C.UTF-8]:
```

8. Enter the Vserver security style:

```
Enter the Vserver root volume's security style {mixed, ntfs, unix} [unix]:
Enter
```

9. Answer no to `Do you want to create a data volume?`

```
Do you want to create a data volume?  {yes, no} [Yes]: no
```

10. Answer no to `Do you want to create a logical interface?`

```
Do you want to create a logical interface?  {yes, no} [Yes]: no
```

11. Answer no to `Do you want to Configure FCP? {yes, no} [yes]: no.`

```
Do you want to Configure FCP? {yes, no} [yes]: no
```

12. Add the two data aggregates to the `Infra_Vserver` aggregate list for NetApp Virtual Console.

```
vserver modify –vserver Infra_Vserver –aggr-list aggr1_node1, aggr1_node2
```

FCP Service in Clustered Data ONTAP

To create the FCP service, complete the following step:

1. Create the FCP service on each Vserver. This command also starts the FCP service and sets the FCP worldwide node name (WWNN) for the Vserver.

```
fcp create -vserver Infra_Vserver
fcp show
```

HTTPS Access in Clustered Data ONTAP

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 by running the following command:

```
security certificate show
```

3. For each Vserver shown, the certificate common name should match the DNS FQDN of the Vserver. The four default certificates should be deleted and replaced by either self-signed certificates or certificates from a Certificate Authority (CA) To delete the default certificates, run the following commands:

Note 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.

```
security certificate delete [TAB] …
Example: security certificate delete -vserver Infra_Vserver -common-name
3.cert.1414163766 -ca 3.cert.1414163766 -type server -serial 544A6D36
```

4. To generate and install self-signed certificates, run the following commands as one-time commands. Generate a server certificate for Infra_Vserver, the cluster Vserver, and each node Vserver. Again, use TAB completion to aid in completing these commands.

```
security certificate create [TAB] …
Example: security certificate create -common-name fvl2-infra.rtp.netapp.com
-type server -size 2048 -country US -state "North Carolina" -locality "RTP"
-organization "NetApp" -unit "ICE" -email-addr "abc@netapp.com" -expire-days
365 -hash-function SHA256 -vserver  Infra_Vserver
```

5. To obtain the values for the parameters that would be required in the following step, run the `security certificate show` command.

6. Enable each certificate that was just created using the –server-enabled true and –client-enabled false parameters. Again use TAB completion.

```
security ssl modify [TAB] …
Example: security ssl modify -vserver Infra_Vserver -server-enabled true
-client-enabled false -ca fvl2-infra.fvl.rtp.netapp.com -serial 544A71D7
-common-name fvl2-infra.fvl.rtp.netapp.com
```

7. Configure and enable SSL and HTTPS access and disable HTTP access.

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web service
requests to be
         interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http -action
allow
system services firewall policy create -policy mgmt -service http -action
deny -ip-list 0.0.0.0/0
```

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

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

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

FlexVol in Clustered Data ONTAP

To create a NetApp FlexVol® volume, complete the following step:

1. The following information is required to create a FlexVol volume: the volume's name, size, and the aggregate on which it will exist. Create two VMware datastore volumes, a server boot volume, and a volume to hold the OnCommand database LUN. Also, update the Vserver root volume load sharing mirrors to make the NFS mounts accessible.

```
volume create -vserver Infra_Vserver -volume infra_datastore_1 -aggregate
aggr1_node2 -size 1TB -state online -policy default -space-guarantee none
-percent-snapshot-space 0

volume create -vserver Infra_Vserver -volume infra_swap -aggregate
aggr1_node1 -size 200GB -state online -policy default -space-guarantee none
-percent-snapshot-space 0 -snapshot-policy none


volume create -vserver Infra_Vserver -volume esxi_boot -aggregate
aggr1_node1 -size 100GB -state online -policy default -space-guarantee none
-percent-snapshot-space 0
```

LUN in Clustered Data ONTAP

To create LUNs, complete the following step:

1. Create two boot LUNS and two FC datastore LUNs.

lun create -vserver Infra_Vserver -volume esxi_boot -lun VM-Host-Infra-01 -size 15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra_Vserver -volume esxi_boot -lun VM-Host-Infra-02 -size 15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra_Vserver -volume infra_datastore_1 -lun infra_datastore_1 -size 500GB -ostype vmware -space-reserve disabled
lun create -vserver Infra_Vserver -volume infra_swap -lun infra_swap -size 100GB -ostype vmware -space-reserve disabled

Deduplication in Clustered Data ONTAP

To enable deduplication on appropriate volumes, complete the following step:

1. Run the following commands:

```
volume efficiency on –vserver Infra_Vserver -volume infra_datastore_1
volume efficiency on –vserver Infra_Vserver -volume esxi_boot
```

FCP LIF in Clustered Data ONTAP

To create FC LIFs, complete the following step:

1. Create four FC LIFs, two on each node.

```
network interface create -vserver Infra_Vserver -lif fcp_lif01a -role data
-data-protocol fcp -home-node <<var_node01>> -home-port 0c –status-admin up
–failover-policy disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra_Vserver -lif fcp_lif01b -role data
-data-protocol fcp -home-node <<var_node01>> -home-port 0d –status-admin up
–failover-policy disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra_Vserver -lif fcp_lif02a -role data
-data-protocol fcp -home-node <<var_node02>> -home-port 0c –status-admin up
–failover-policy disabled –firewall-policy data –auto-revert false
```

```
network interface create -vserver Infra_Vserver -lif fcp_lif02b -role data
-data-protocol fcp -home-node <<var_node02>> -home-port 0d –status-admin up
–failover-policy disabled –firewall-policy data –auto-revert false
```

Add Infrastructure Vserver Administrator

To add the infrastructure Vserver administrator and Vserver administration logical interface in the out-of-band management network, complete the following step:

1. Run the following commands:

```
network interface create –vserver Infra_Vserver –lif vsmgmt –role data
–data-protocol none –home-node <<var_node02>> -home-port  e0a –address
<<var_vserver_mgmt_ip>> -netmask <<var_vserver_mgmt_mask>> -status-admin up
–failover-policy nextavail –firewall-policy mgmt –auto-revert true
–failover-group fg-cluster-mgmt

Note: the Vserver management IP here should be in the same subnet as the
storage cluster management IP.

Note: you will see that a routing group is created with the above command.
Use that routing group in the command below where you see
<<var_routing_group>>.

network routing-groups route create –vserver Infra_Vserver –routing-group
d<< var_routing_group >> -destination 0.0.0.0/0 –gateway
<<var_vserver_mgmt_gateway>>

security login password –username vsadmin –vserver Infra_Vserver
Enter a new password:  <<var_vsadmin_password>>
Enter it again:  <<var_vsadmin_password>>

security login unlock –username vsadmin –vserver Infra_Vserver
```

Server Configuration

FlexPod Cisco UCS Base

Perform Initial Setup of Cisco UCS 6324 Fabric Interconnect 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 C-Series and B-Series servers and should be followed precisely to avoid improper configuration.

Cisco UCS Fabric Interconnect 6324 A

Cisco Unified Computing System (Cisco UCS) uses access layer networking and servers. This high-performance, next-generation server system provides a data center with a high degree of workload agility and scalability.

Cisco UCS Manager 3.0 supports the 6324 Fabric Interconnect that integrates the FI into the UCS Chassis and provides an integrated solution for a smaller deployment environment. Cisco UCS Mini simplifies the system management and saves cost for the low scale deployments.

The hardware and software components support Cisco's unified fabric, which runs multiple types of data center traffic over a single converged network adapter.

Initial System Setup

The first time that you access a fabric interconnect in a Cisco UCS domain, a setup wizard prompts you for the following information required to configure the system:

- Installation method (GUI or CLI)
- Setup mode (restore from full system backup or initial setup)
- System configuration type (standalone or cluster configuration)
- System name
- Admin password
- Management port IPv4 address and subnet mask, or IPv6 address and prefix
- Default gateway IPv4 or IPv6 address
- DNS Server IPv4 or IPv6 address
- Default domain name

Table 19 Worksheet to Complete Cisco UCS Fabric Interconnect Setup

Field	Description
System Name	The name assigned to Cisco UCS domain. In a cluster configuration, the system adds –A to the fabric interconnect assigned to fabric A, and –B to the fabric interconnect assigned to fabric B
Admin Password	The password used for the Admin account on the fabric interconnect
Management IP Address	The Ipv4 or Ipv6 address for the management port on the fabric interconnect
Management Netmask	The IPv4 subnet mask or IPv6 prefix for the management port on the fabric interconnect.
Default Gateway	The IPv4 or IPv6 address for the default gateway assigned to the management port on the fabric interconnect.
DNS Server IP address	The Ipv4 or Ipv6 address for the DNS server assigned to the fabric interconnect
Domain Name	The name of the domain in which the fabric interconnect resides

Table 20 Cisco UCS Fabric B Management IP Address

Field	Description
Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv4 Address field.	Enter an IPv4 address for the Mgmt0 interface on the local fabric interconnect.

Peer FI is IPv6 Cluster Enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv6 Address field.	Enter an IPv6 address for the Mgmt0 interface on the local fabric interconnect.

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 6224 Fabric Interconnect.

```
Enter the configuration method. (console/gui) ? console

  Enter the setup mode; setup newly or restore from backup. (setup/restore)
? setup

  You have chosen to setup a new Fabric interconnect. Continue? (y/n): y

  Enforce strong password? (y/n) [y]:

  Enter the password for "admin":
  Confirm the password for "admin":<<var_password>>
  Enter the password for "admin":":<<var_password>>
  Confirm the password for "admin":

  Is this Fabric interconnect part of a cluster(select 'no' for standalone)?
(yes/no) [n]: yes

  Enter the switch fabric (A/B) []: A

  Enter the system name:  <<var_ucs_clustername>>

  Physical Switch Mgmt0 IP address : <<var_ucsa_mgmt_ip>>

  Physical Switch Mgmt0 IPv4 netmask : <<var_ucsa_mgmt_mask>>

  IPv4 address of the default gateway : <<var_ucsa_mgmt_gateway>>

  Cluster IPv4 address :

  Configure the DNS Server IP address? (yes/no) [n]: <<var_nameserver_ip>>

Configure the DNS Server IP address (yes/no) [n]: y
         DNS IPv4 address : <<var_nameserver_ip>>

  Configure the default domain name? (yes/no) [n]: y

  Join centralized management environment (UCS Central)? (yes/no) [n]: n


 NOTE: Cluster IP will be configured only after both Fabric Interconnects
are initialized.          UCSM will be functional only after peer FI is
configured in clustering mode.

  Apply and save the configuration (select 'no' if you want to re-enter)?
(yes/no): yes
  Applying configuration. Please wait.

  Configuration file - Ok
```

2. Review the settings displayed on the console. If they are correct, answer `yes` to apply and save the configuration.

3. Wait for the login prompt to verify that the configuration has been saved.

Cisco UCS Fabric Interconnect 6324 B

The first time that you access a fabric interconnect in a Cisco UCS domain, a setup wizard prompts you for the following information required to configure the system:

- Installation method (GUI or CLI)
- Setup mode (restore from full system backup or initial setup)
- System configuration type (standalone or cluster configuration)
- System name
- Admin password
- Management port IPv4 address and subnet mask, or IPv6 address and prefix
- Default gateway IPv4 or IPv6 address
- DNS Server IPv4 or IPv6 address
- Default domain name

Table 21 Worksheet to Complete Cisco UCS Fabric Interconnect Setup

Field	Description
System Name	The name assigned to Cisco UCS domain. In a cluster configuration, the system adds –A to the fabric interconnect assigned to fabric A, and –B to the fabric interconnect assigned to fabric B
Admin Password	The password used for the Admin account on the fabric interconnect
Management IP Address	The IPv4 or Ipv6 address for the management port on the fabric interconnect
Management Netmask	The IPv4 subnet mask or IPv6 prefix for the management port on the fabric interconnect.
Default Gateway	The IPv4 or IPv6 address for the default gateway assigned to the management port on the fabric interconnect.
DNS Server IP address	The Ipv4 or Ipv6 address for the DNS server assigned to the fabric interconnect
Domain Name	The name of the domain in which the fabric interconnect resides

Table 22 Cisco UCS Fabric B Management IP Address

Field	Description
Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv4 Address field.	Enter an IPv4 address for the Mgmt0 interface on the local fabric interconnect.
Peer FI is IPv6 Cluster Enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv6 Address field.	Enter an IPv6 address for the Mgmt0 interface on the local fabric interconnect.

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 6248 Fabric Interconnect.

```
Enter the configuration method. (console/gui) ? console

  Installer has detected the presence of a peer Fabric interconnect. This
Fabric interconnect will be added to the cluster. Continue (y/n) ? y

  Enter the admin password of the peer Fabric interconnect:
    Connecting to peer Fabric interconnect... done
    Retrieving config from peer Fabric interconnect... done
    Peer Fabric interconnect Mgmt0 IPv4 Address: <<var_ucsb_mgmt_ip>>
    Peer Fabric interconnect Mgmt0 IPv4 Netmask: <<var_ucsb_mgmt_mask>>
    Cluster IPv4 address          :

    Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric
Interconnect Mgmt0 IPv4 Address

  Physical Switch Mgmt0 IP address :


  Apply and save the configuration (select 'no' if you want to re-enter)?
(yes/no): yes
  Applying configuration. Please wait.

  Configuration file - Ok


Cisco UCS Mini 6300 Series Fabric Interconnect
ucs2-B login:
```

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

FlexPod Cisco UCS FC vSphere on Clustered Data ONTAP

Log into Cisco UCS Manager

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 6324 Fabric Interconnect cluster address.
2. Click the Launch UCS Manager link to download the Cisco UCS Manager software.
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.

Cisco UCS Manager Software to Version 3.0(1c)

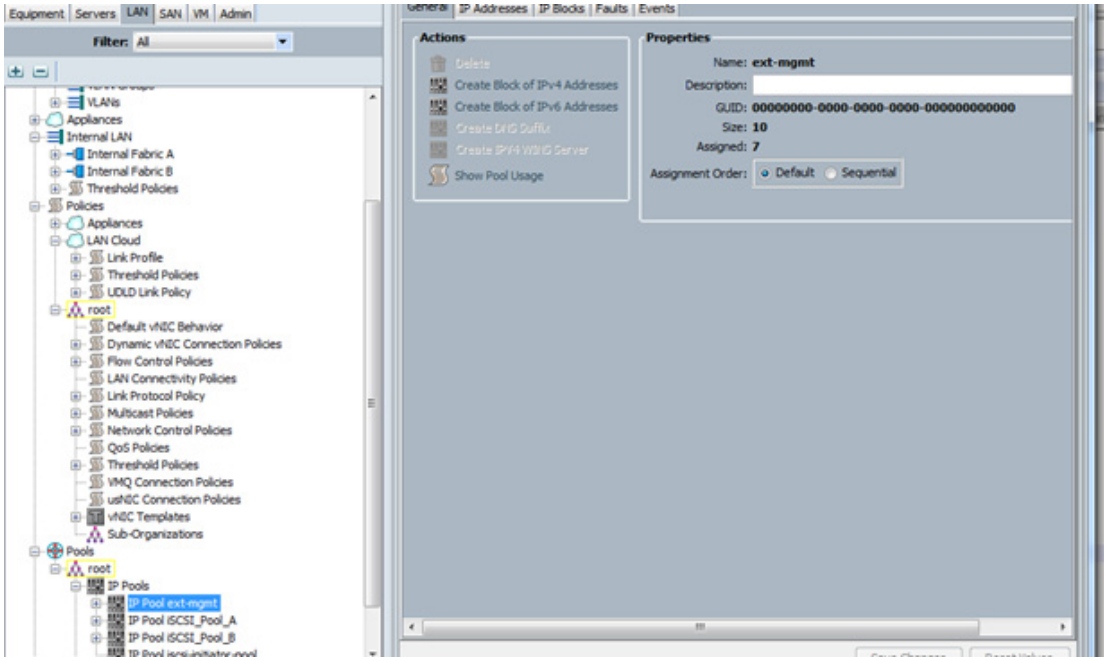
The Cisco UCS-mini chassis comes with UCSM 3.0(1c) release. This document assumes the use of Cisco UCS Manager Software version 3.0(1c). To upgrade the Cisco UCS Manager software and the UCS 6324 Fabric Interconnect software to a higher versionof the firmware,) refer to Cisco UCS Manager Install and Upgrade Guides.

Add a Block of IP Addresses for Out-of-band KVM Access

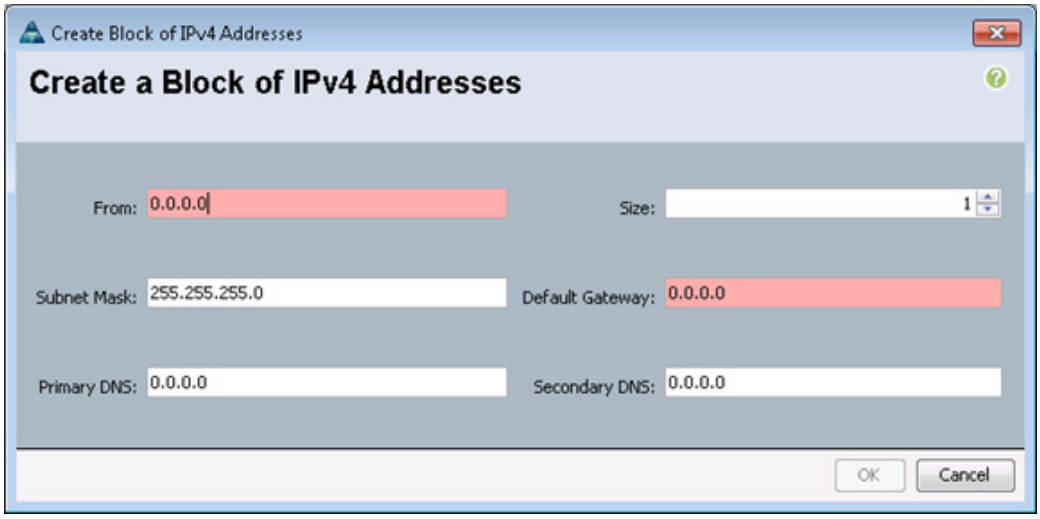
To create a block of IP addresses for server keyboard, video, mouse (KVM) access in the Cisco UCS environment, complete the following steps:

Note This block of IP addresses should be in the same subnet as the management IP addresses for the Cisco UCS Manager.

1. In Cisco UCS Manager, in the navigation pane, click the LAN tab.
2. Select Pools > root > IP Pools > IP Pool ext-mgmt.



3. In the Actions pane, select Create Block of IP Addresses.
4. Enter the starting IP address of the block and the number of IP addresses required, and the subnet and gateway information.



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

Synchronize Cisco UCS to NTP

To synchronize the Cisco UCS environment to the NTP server, complete the following steps:

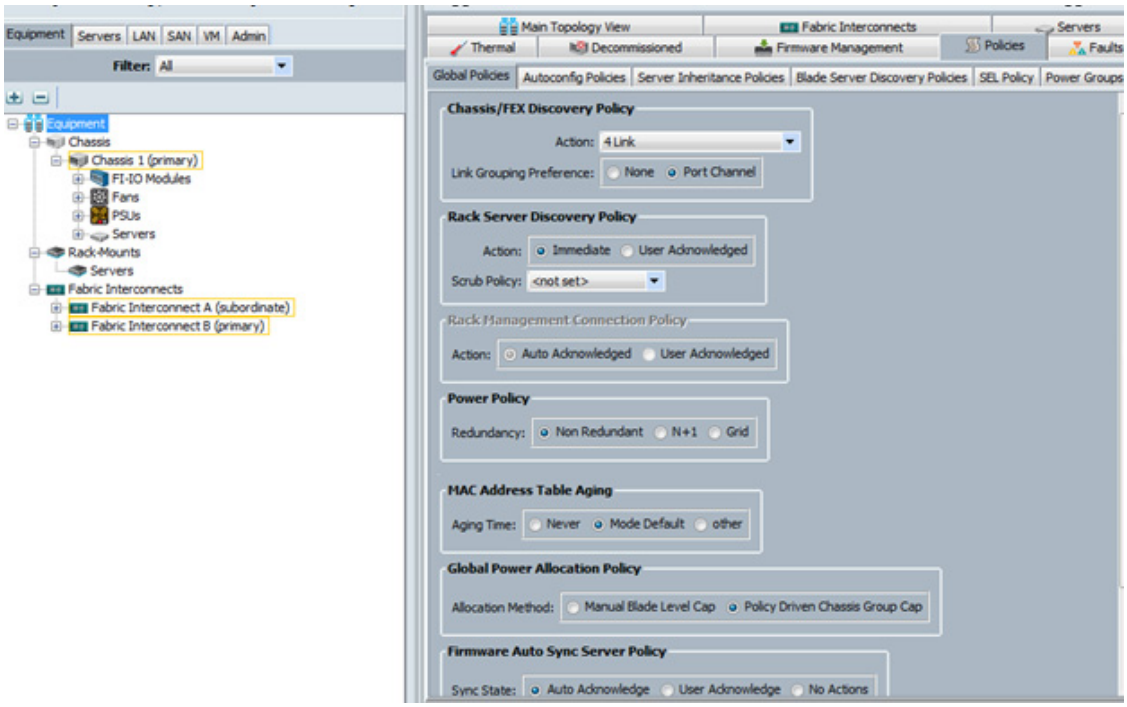
1. In Cisco UCS Manager, in the navigation pane, click the Admin tab .
2. Select All > Timezone Management.
3. In the Properties pane, select the appropriate time zone in the Timezone menu.
4. Click Save Changes, and then click OK.
5. Click Add NTP Server.
6. Enter `<<var_global_ntp_server_ip>>` and click OK.
7. Click OK.

Edit Chassis Discovery Policy

Setting the discovery policy simplifies the addition of B-Series Cisco UCS chassis and Cisco UCS C-Series servers.

To modify the chassis discovery policy, complete the following steps:

1. In Cisco UCS Manager, in the navigation pane, click the Equipment node and select Equipment in the list on the left.
2. In the right pane, click the Policies tab.
3. Under Global Policies, set the Chassis/FEX Discovery Policy to 4-link.
4. Set the Link Grouping Preference to Port Channel.

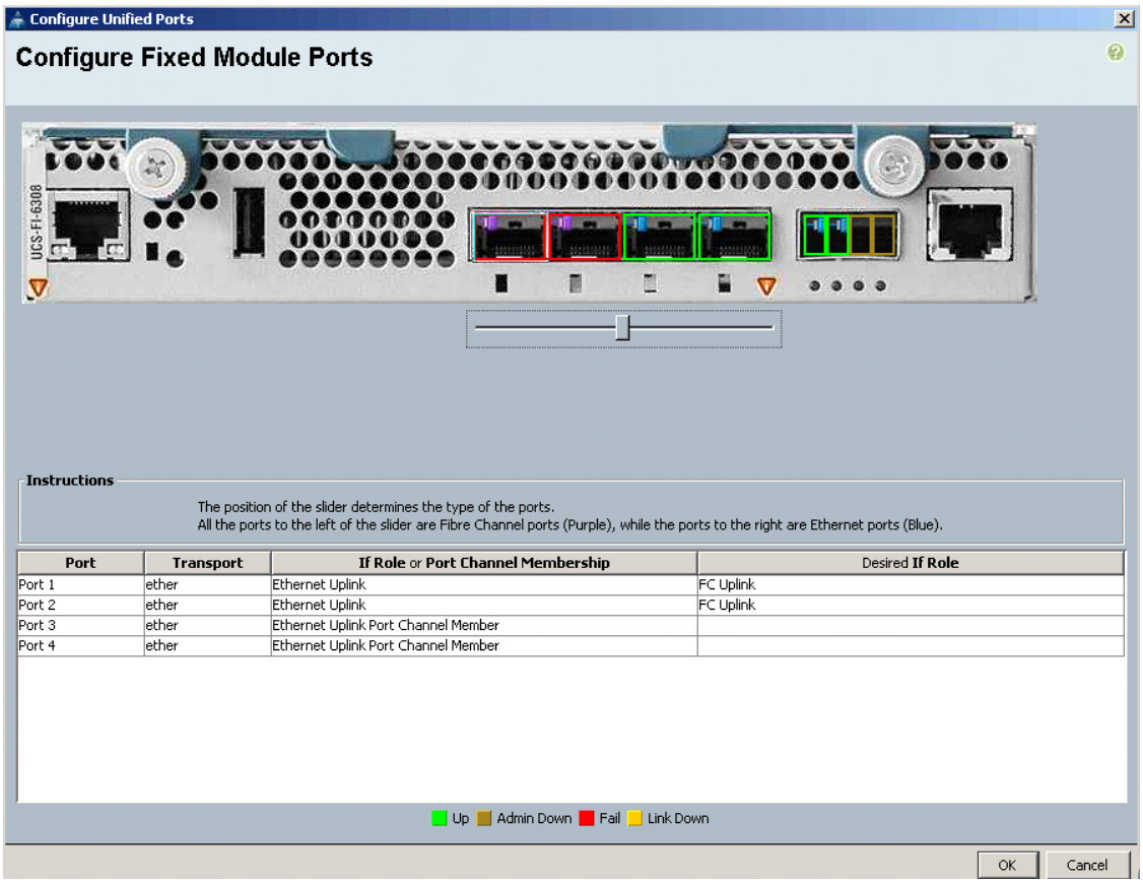


5. Click Save Changes.
6. Click OK.

Convert Unified Ports to FC

Ethernet ports 1/1 and 1/2 on each 6324 Fabric Interconnect need to be converted from Ethernet mode to Fiber Channel mode in order to connect to storage.

1. In Cisco UCS Manager, in the navigation pane, click the Equipment tab and select Fabric Interconnects > Fabric Interconnect A in the list on the left.
2. In the right pane, click Configure Unified Ports under Actions.
3. Click Yes on the warning that appears.
4. In the Configure Fixed Module Ports window, move the slider to the right to make ports 1 and 2 FC and leave ports 3 and 4 Ethernet as shown below.



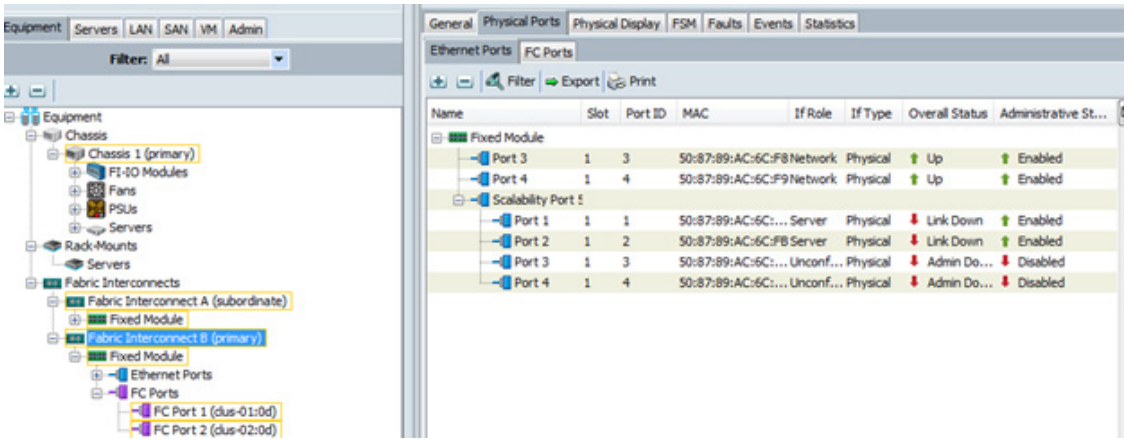
5. Click OK.
6. Click Yes and OK to apply the changes and reboot the Fabric Interconnect.
7. When the Fabric Interconnect has rebooted (this may require you to reconnect to Cisco UCS Manager), log back in and repeat this procedure for Fabric Interconnect B.

Enable Server Uplink and Storage Ports

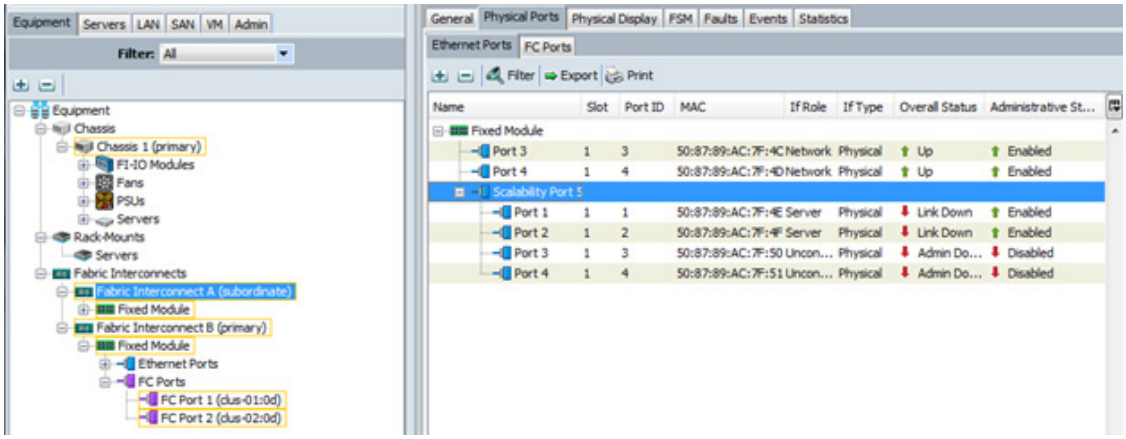
To enable server and uplink ports, complete the following steps:

1. In Cisco UCS Manager, in the navigation pane, click the Equipment tab.
2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module.
3. Expand Ethernet Ports.
4. Select the ports that are connected directly to C-Series rack servers, right-click them, and select Configure as Server Port.
5. Click Yes to confirm server ports and click OK.
6. Select ports 3 and 4 that are connected to the Cisco Nexus 9372 switches, right-click them, and select Configure as Uplink Port.
7. Click Yes to confirm uplink ports and click OK.
8. In the right pane, select the FC Ports tab and expand Fixed Module.
9. Select FC Port 1 and PC Port 2, right-click, and select Configure as FC Storage Port.

10. Click Yes to confirm and click OK
11. In the left pane, navigate to Fabric Interconnect B. In the right pane, navigate to the Physical Ports tab > Ethernet Ports tab. Confirm that ports have been configured correctly in the IfRole column.



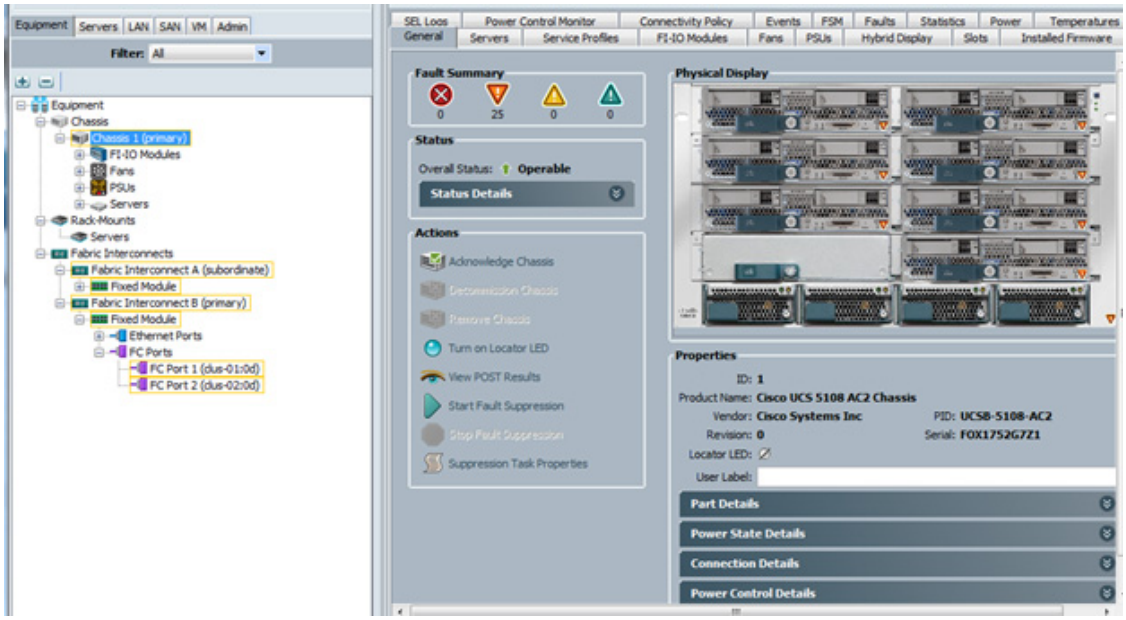
12. Select Equipment > Fabric Interconnects > Fabric Interconnect B > Fixed Module.
13. Expand Ethernet Ports.
14. Select the ports that are connected directly connected to C-Series rack servers, right-click them, and select Configure as Server Port.
15. Click Yes to confirm server ports and click OK.
16. Select ports 3 and 4 that are connected to the Cisco Nexus 9372 switches, right-click them, and select Configure as Uplink Port.
17. Click Yes to confirm the uplink ports and click OK.
18. In the right pane, select the FC Ports tab and expand Fixed Module.
19. Select FC Port 1 and PC Port 2, right-click, and select Configure as FC Storage Port.
20. Click Yes to confirm and click OK.
21. In the left pane, navigate to Fabric Interconnect A. In the right pane, navigate to the Physical Ports node > Ethernet Ports node. Confirm that ports have been configured correctly in the IfRole column. Repeat this steo for Fabric Interconnect B.



Acknowledge Cisco UCS Chassis

To acknowledge all Cisco UCS chassis, complete the following steps:

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

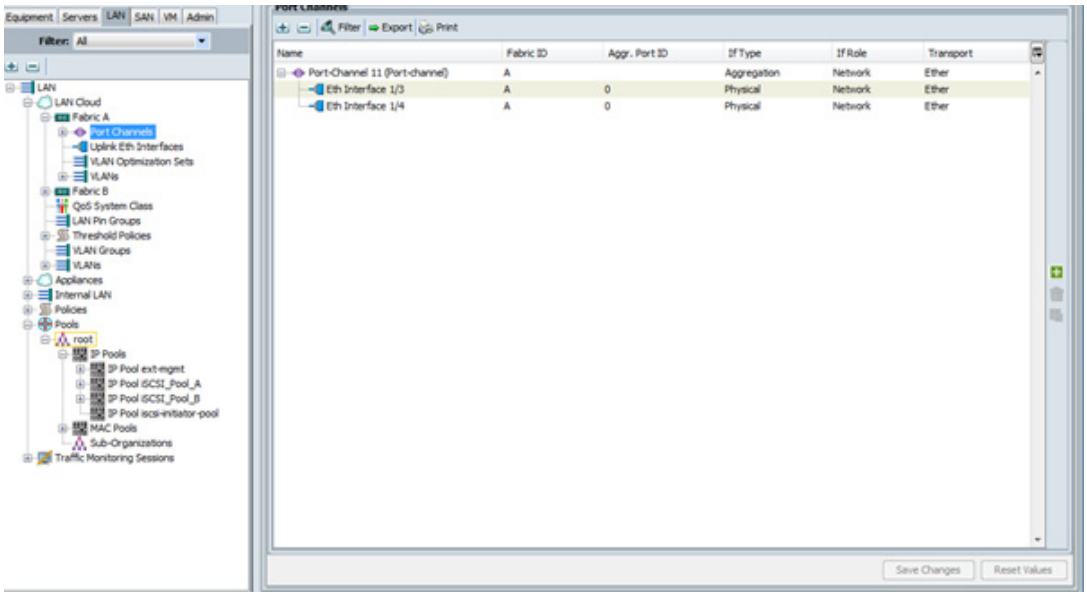


4. Click Yes and then click OK to complete acknowledging the chassis.

Create Uplink Port Channels to Cisco Nexus 9372PX Switches

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

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. In this procedure, two port channels are created: one from Fabric A to both Cisco Nexus 9372PX switches and one from Fabric B to both Cisco Nexus 9372PX switches.
3. Under LAN > LAN Cloud, expand node Fabric A tree.



4. Verify that two ports are configured as Ethernet network connectivity. If not, click the interface and and click 'Configure as Uplink Port'.
5. Configure second interface as uplink port.

Create an Organization

Organizations are used to organize resources and restrict access to various groups within the IT organization, thereby enabling multi-tenancy of the compute resources.

Note Although this document does not assume the use of organizations this procedure provides instructions for creating one.

To configure an organization in the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, from the New menu in the toolbar at the top of the window, select Create Organization.
2. Enter a name for the organization.
3. Optional: Enter a description for the organization.
4. Click OK.
5. Click OK in the confirmation message.

Create MAC Address Pools

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

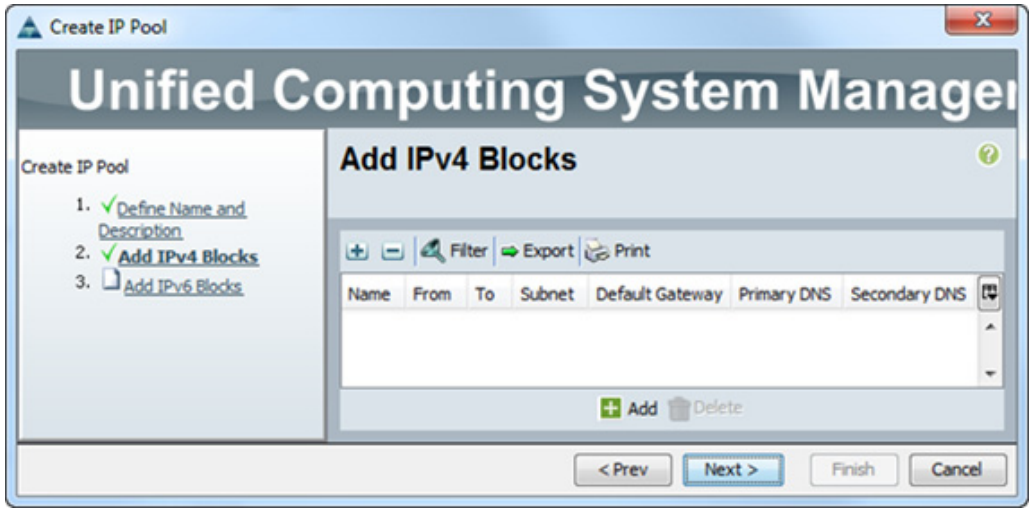
1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Pools > root.

Note 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 namefor MAC pool.
6. Optional: Enter a description for the MAC pool.

Note Keep the Assignment Order at Default.

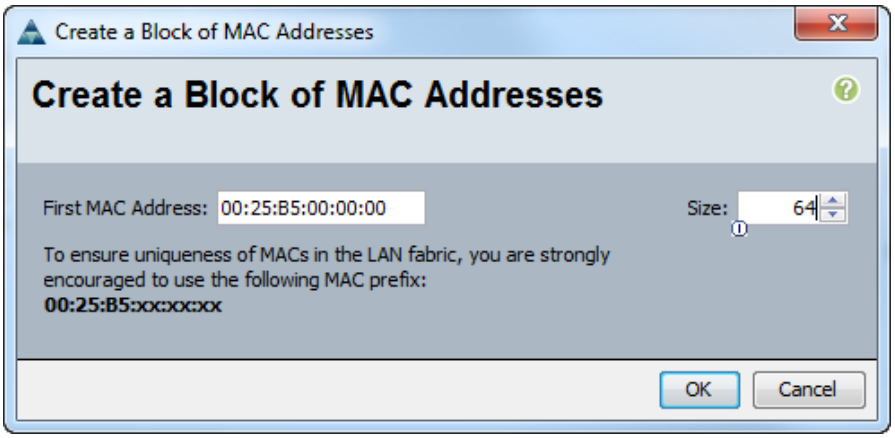
7. Click Next.



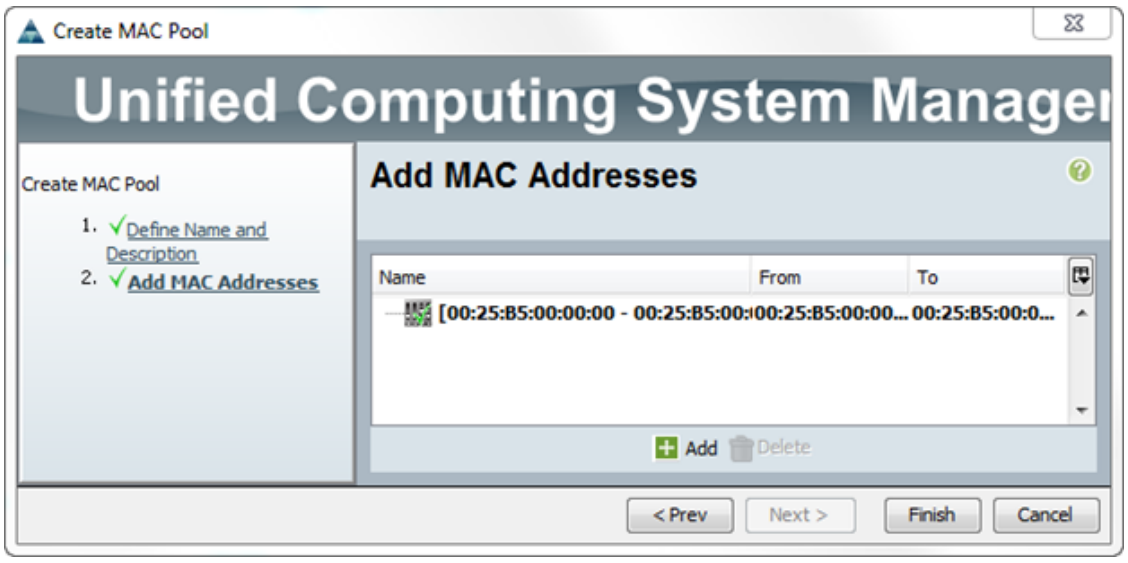
8. Click Add.
9. Specify a starting MAC address.

Note 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.

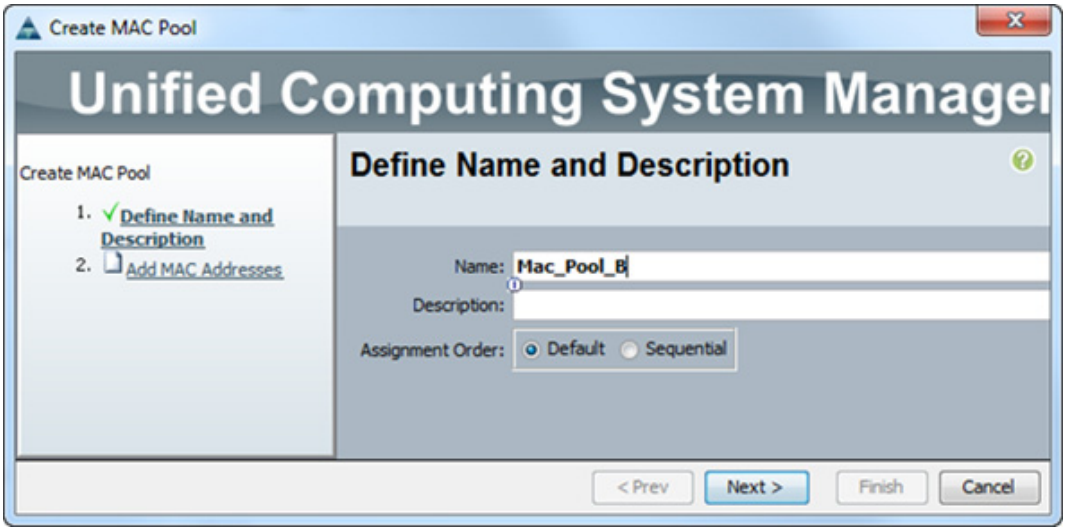
10. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources.



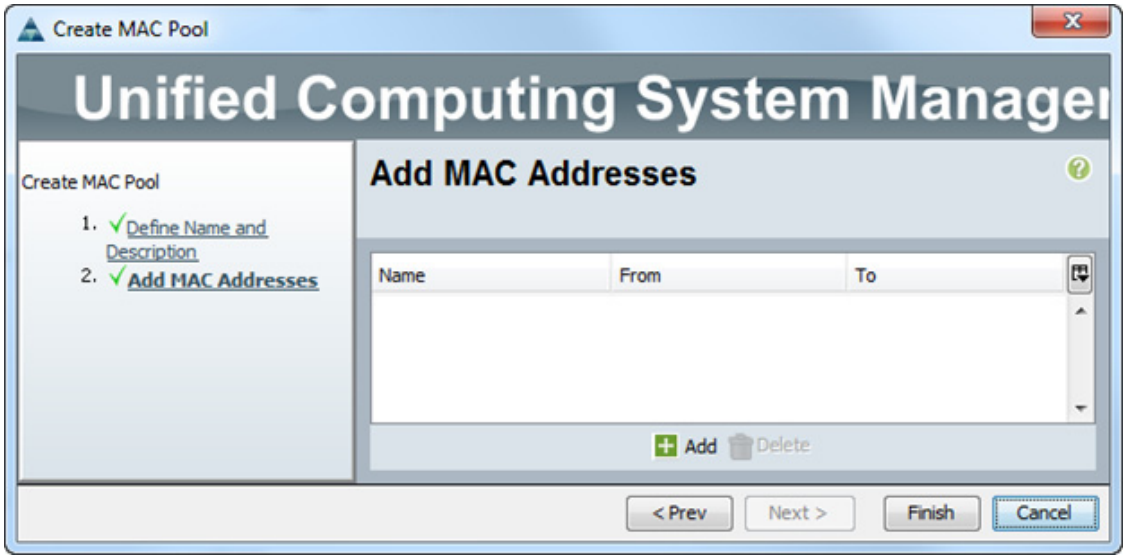
11. Click OK.



12. Click Finish.
13. In the confirmation message, click OK.
14. Right-click MAC Pools under the root organization.
15. Select Create MAC Pool to create the MAC address pool.
16. Enter `MAC_Pool_B` as the name for MAC pool.
17. Optional: Enter a description for the MAC pool.
18. Select Default for the Assignment Order.



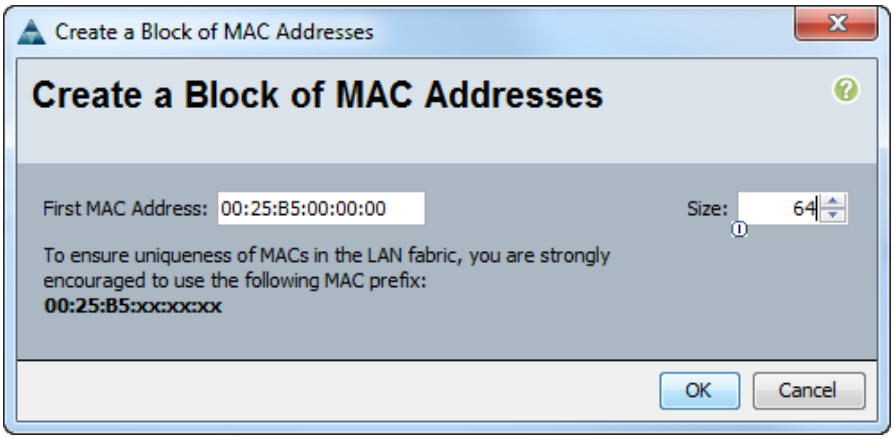
19. Click Next.



20. Click Add.
21. Specify a starting MAC address.

Note For the FlexPod solution, the recommendation is 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.

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



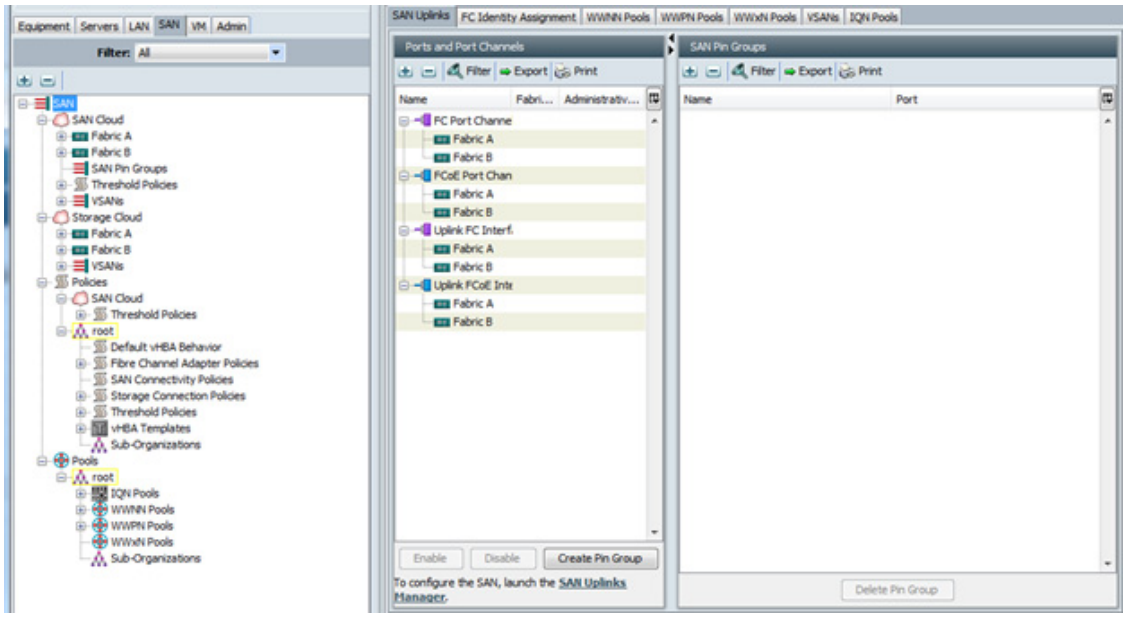
23. Click OK.

24. Click Finish.
25. In the confirmation message, click OK.

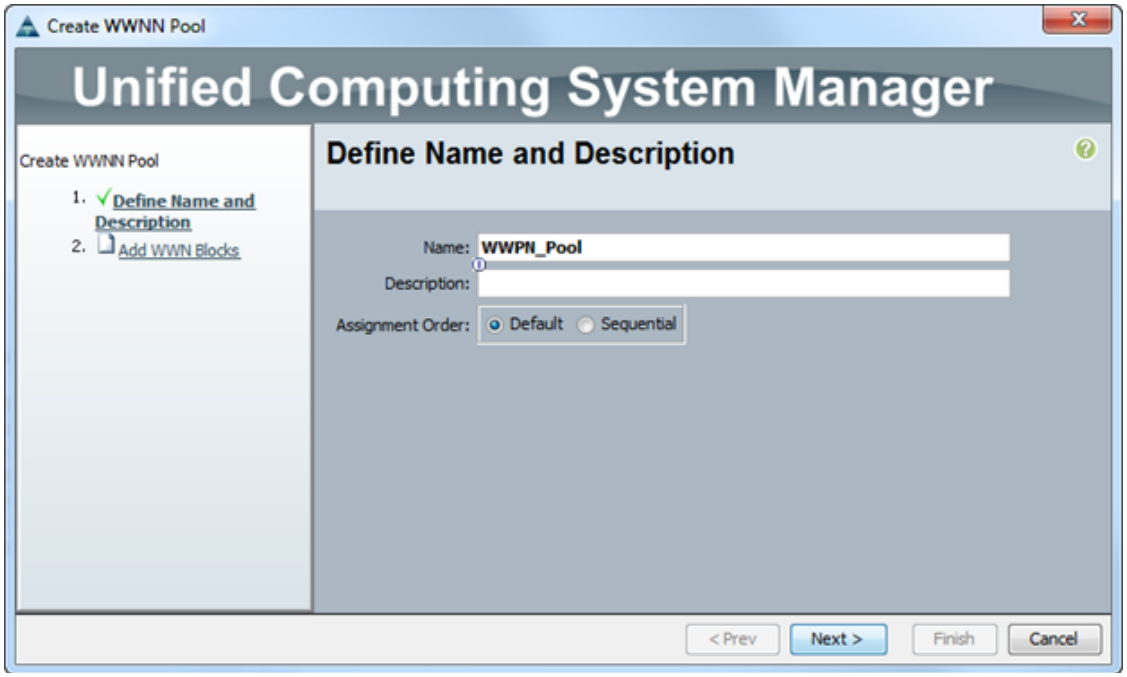
Create WWNN Pools

To configure the necessary World Wide Node Name (WWNN) pools for the Cisco UCS environment, complete the following steps:

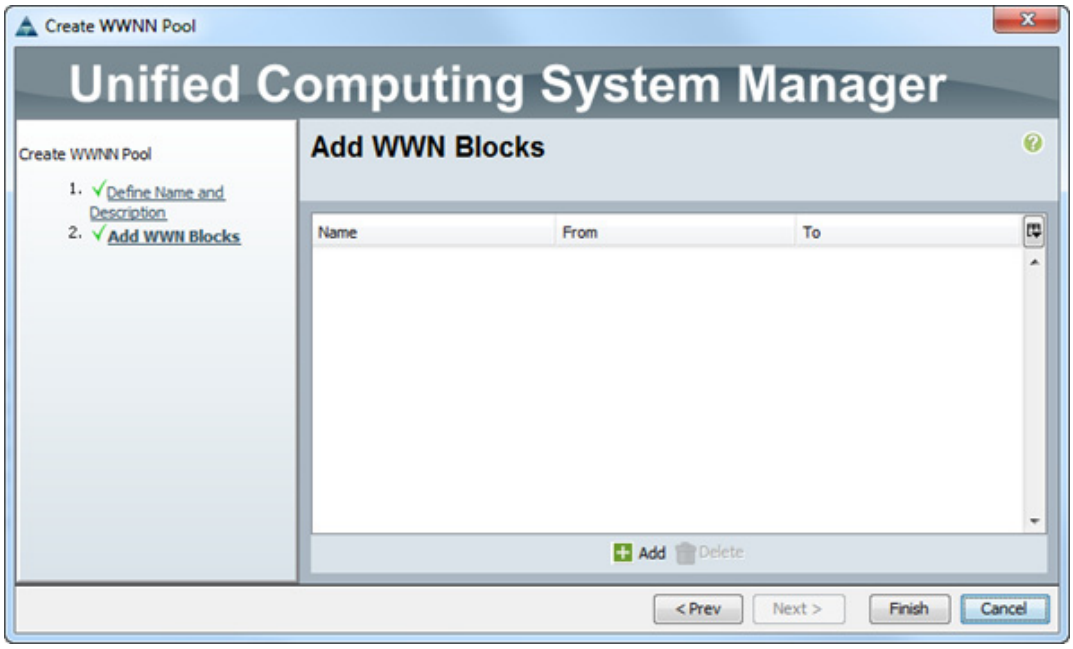
1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Select Pools > root.



3. Right-click WWNN Pools.
4. Select Create WWNN Pool.
5. Enter `WWNN_Pool` as the name for WWNN pool.
6. Optional: Add a description for the WWNN pool.
7. Select Default for the Assignment Order.

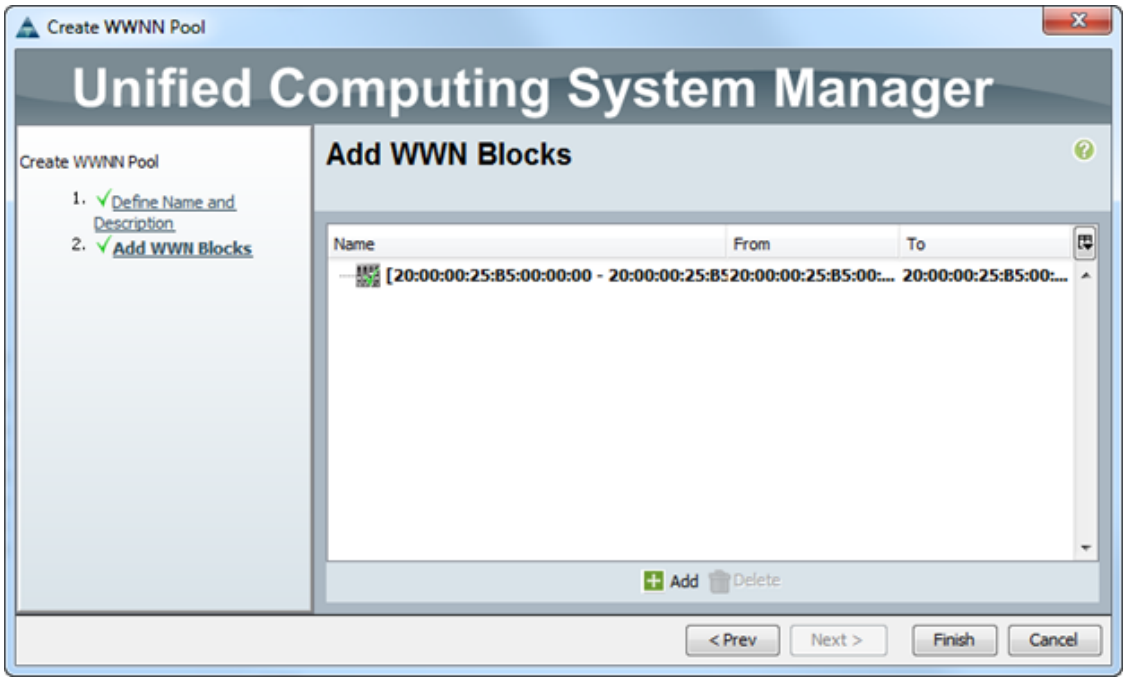


8. Click Next.



9. Click Add to add a block of WWNNs.
10. Either retain the default block of WWNNs, or specify a base WWNN.
11. Specify a size for the WWNN block that is sufficient to support the available blade or server resources.

12. Click OK.



13. Click Finish.
14. Click OK.

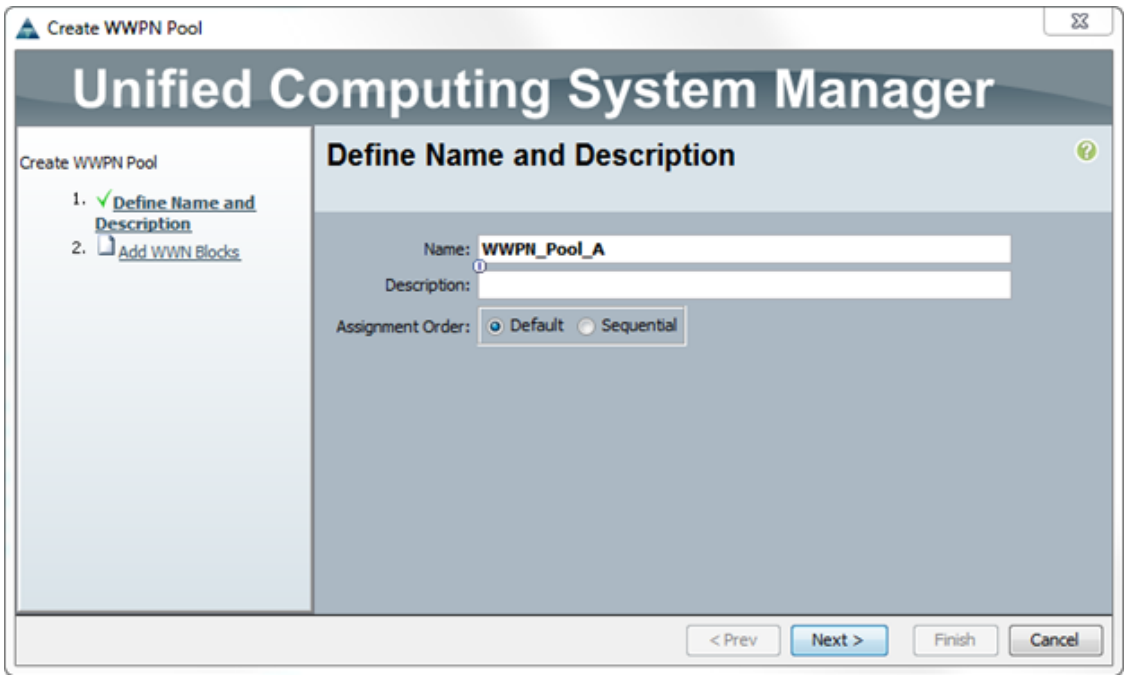
Create WWPN Pools

To configure the necessary World Wide Port Name (WWPN) pools for the Cisco UCS environment, complete the following steps:

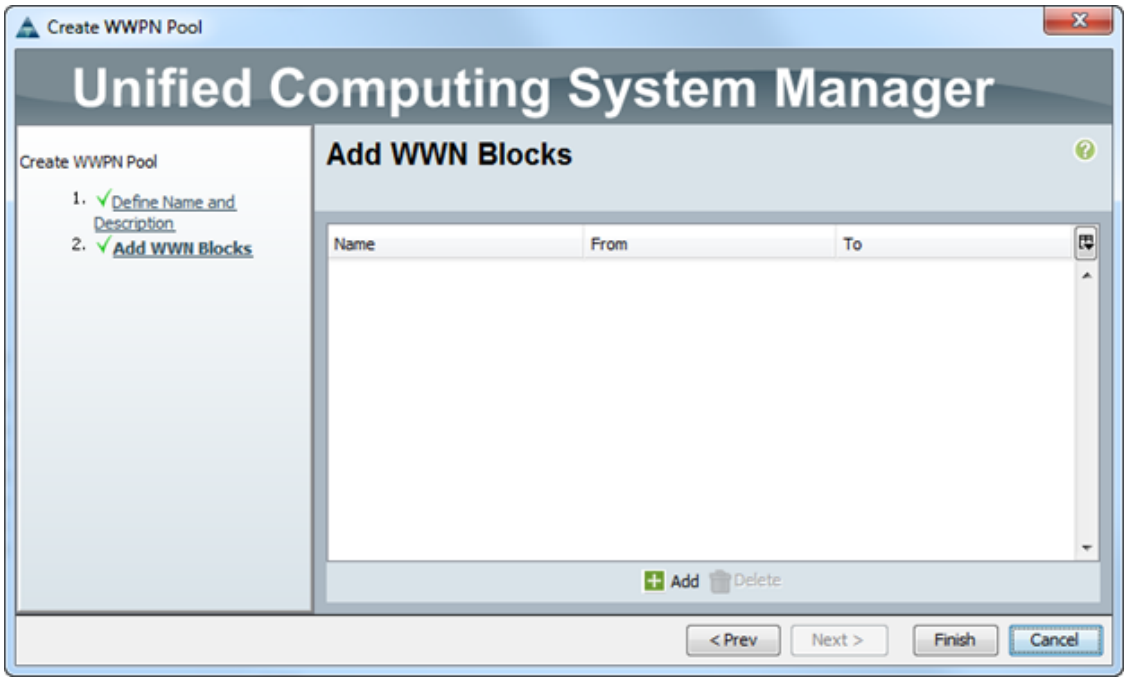
1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Select Pools > root.

Note In this procedure, two WWPN pools are created: one for Fabric A and one for Fabric B.

3. Right-click WWPN Pools.
4. Select Create WWPN Pool.
5. Enter `WWPN_Pool_A` as the name for WWPN pool for Fabric A.
6. Optional: Enter a description for this WWPN pool.
7. Select Default for Assignment Order.



8. Click Next.

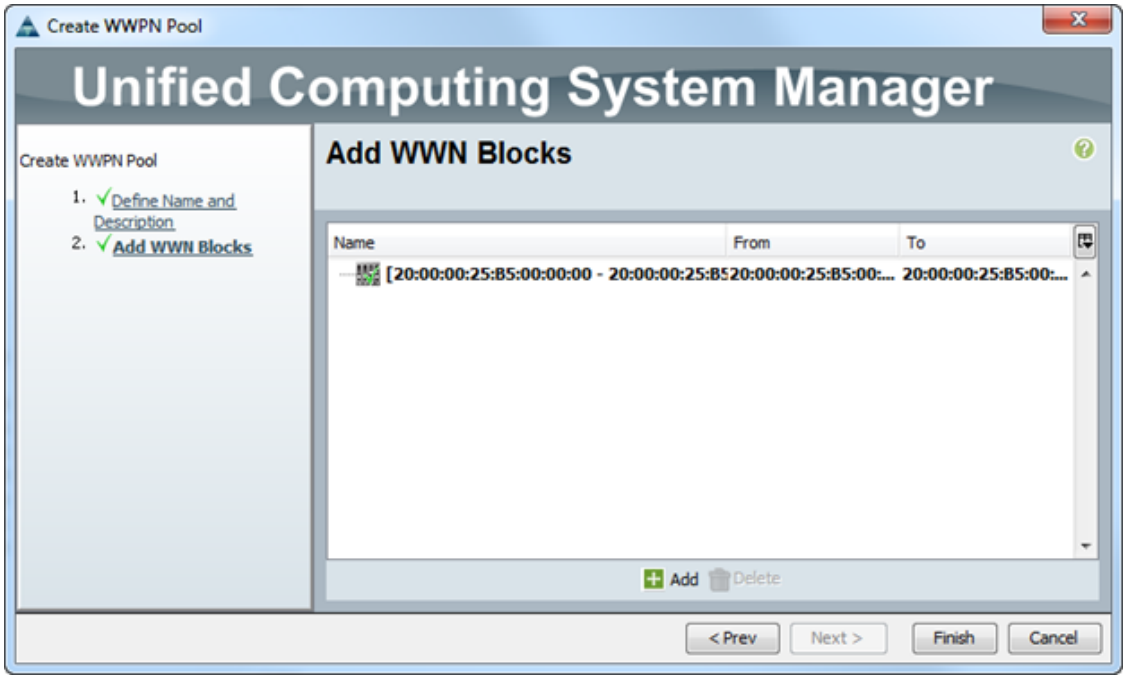


9. Click Add to add a block of WWPNs.
10. Specify the starting WWPN in the block for Fabric A.

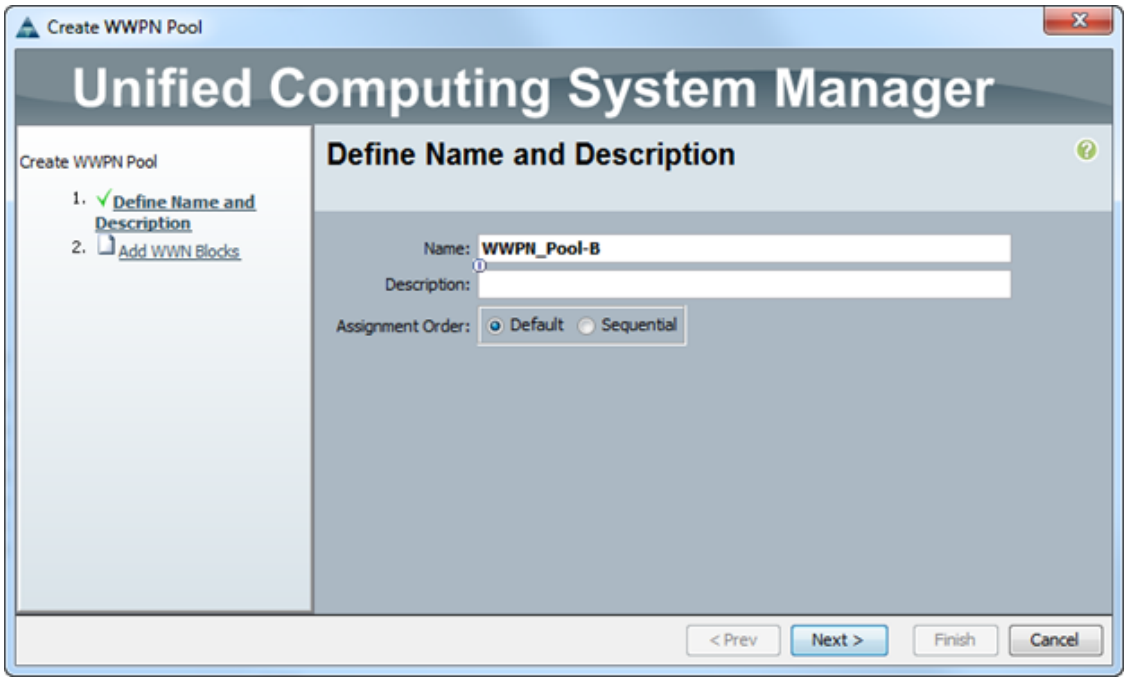
Note For the FlexPod solution, the recommendation is to place 0A in the next-to-last octet of the starting WWPN to identify all the WWPNs in this pool as Fabric A addresses.

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

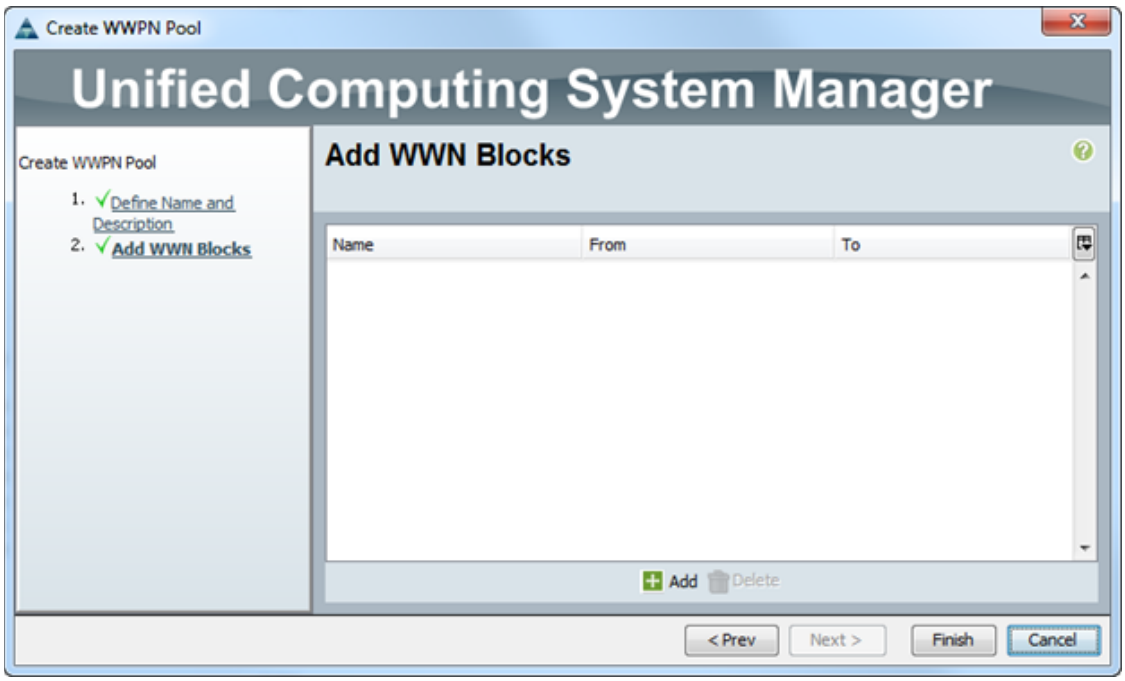
12. Click OK.



13. Click Finish to create the WWPN pool.
14. Click OK.
15. Right-click WWPN Pools.
16. Select Create WWPN Pool.
17. Enter `WWPN_Pool_B` as the name for the WWPN pool for Fabric B.
18. Optional: Enter a description for this WWPN pool.
19. Select Default for the Assignment Order.



20. Click Next.

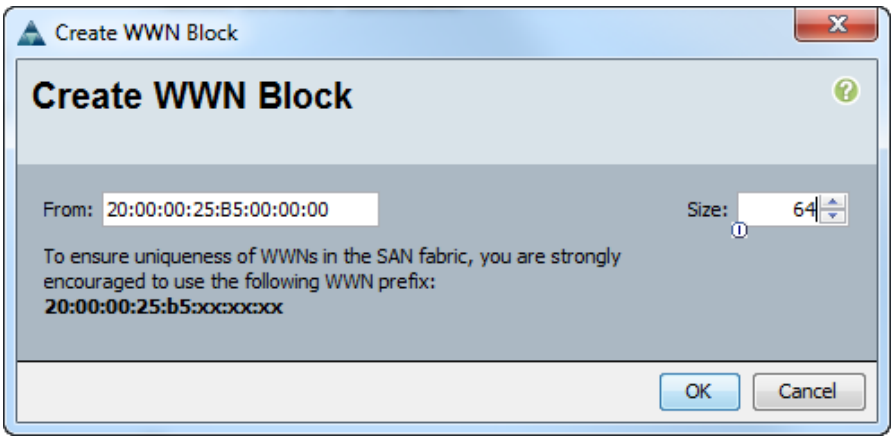


21. Click Add to add a block of WWPNs.

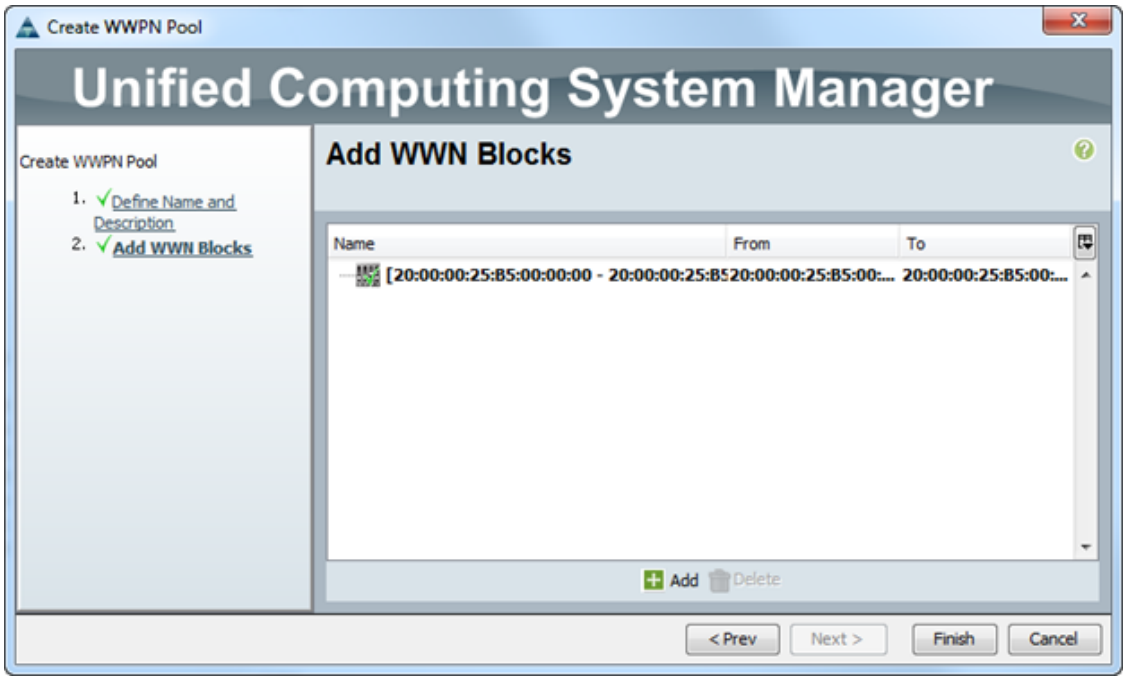
22. Enter the starting WWPN address in the block for Fabric B.

Note For the FlexPod solution, the recommendation is to place 0B in the next to last octet of the starting WWPN to identify all the WWPNs in this pool as Fabric B addresses.

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



24. ClickOK.



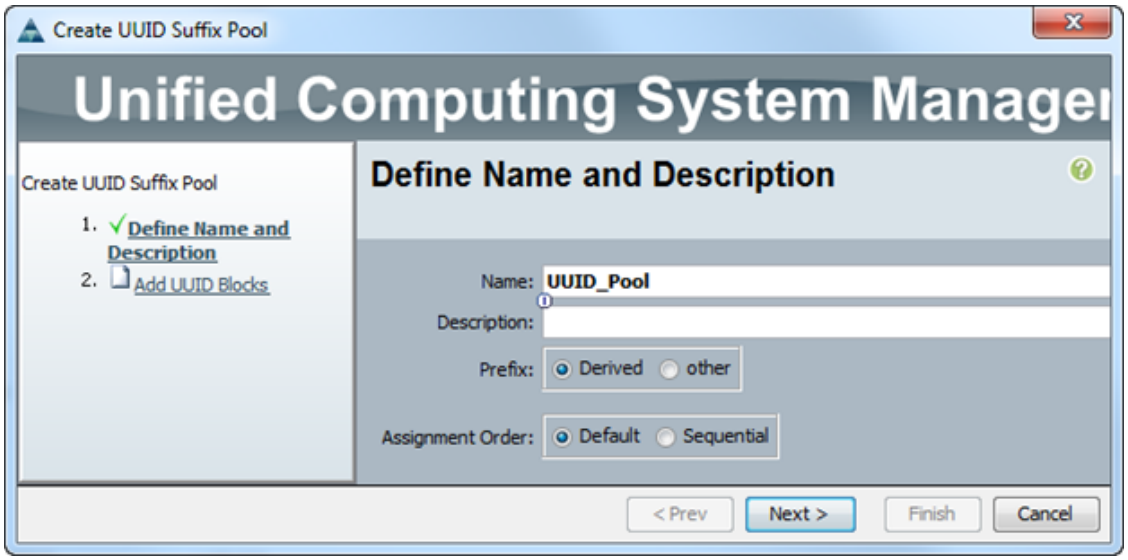
25. Click Finish.
26. Click OK.

Create UUID Suffix Pool

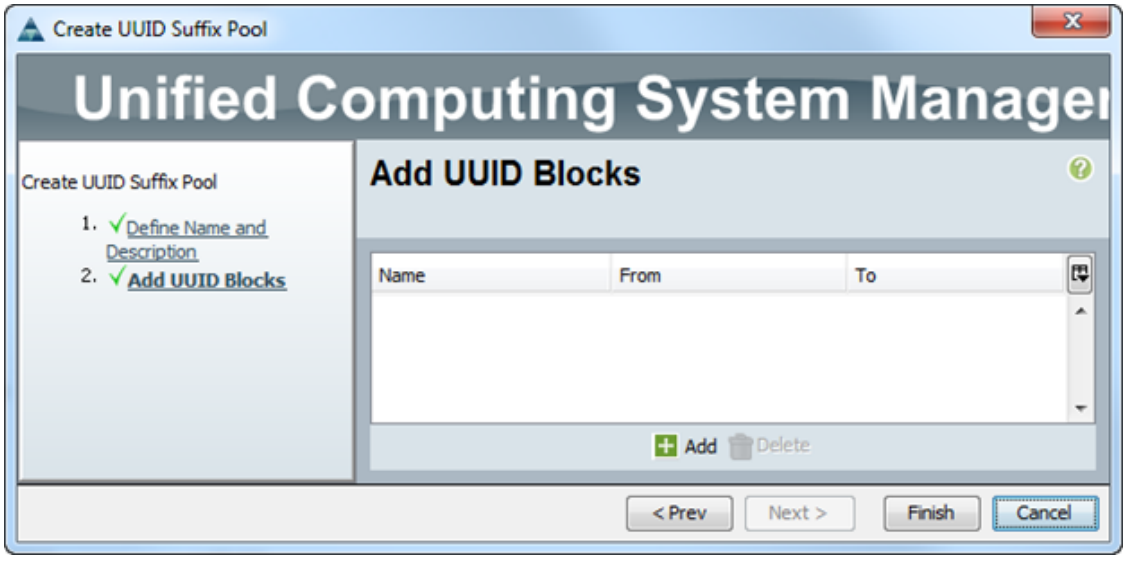
To configure the necessary universally unique identifier (UUID) suffix pool for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Pools > root.

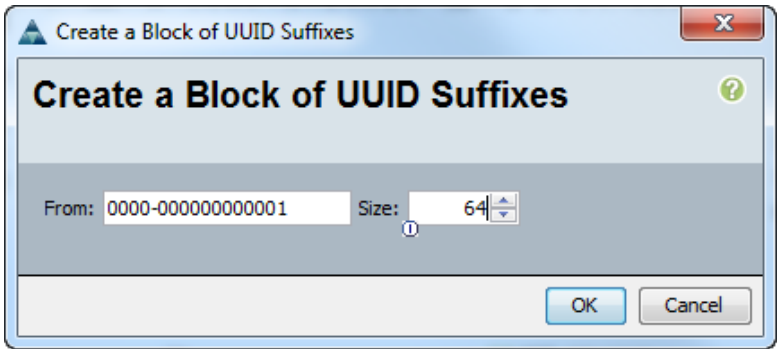
3. Right-click UUID Suffix Pools.
4. Select Create UUID Suffix Pool.
5. Enter `UUID_Pool` as the name for UUID suffix pool.
6. Optional: Enter a description for UUID suffix pool.
7. Select the Derived option for Prefix.
8. Select Default for the Assignment Order.



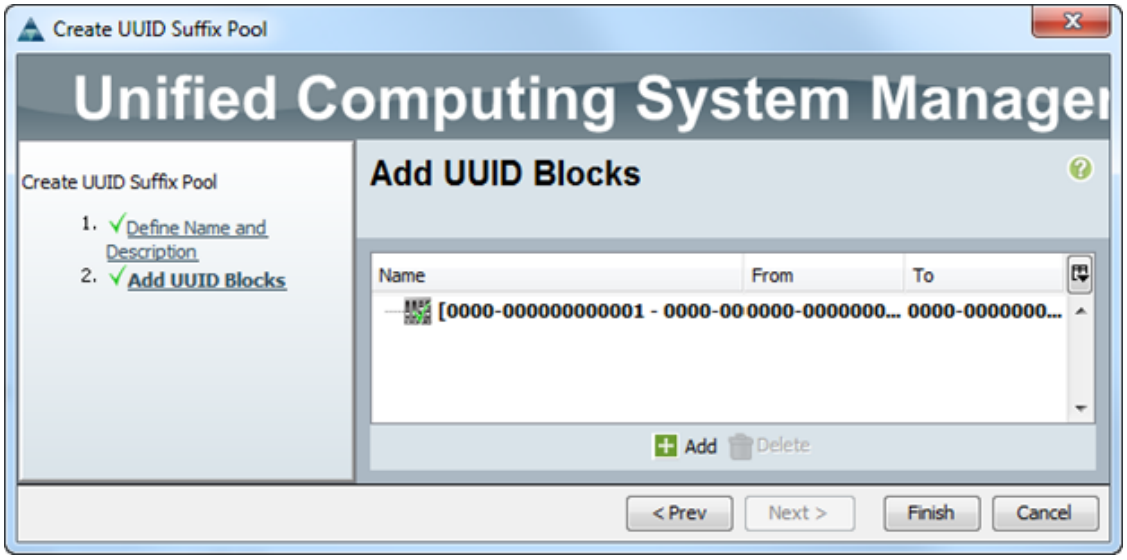
9. Click Next.



10. Click Add to add a block of UUIDs.
11. Select From option as 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.



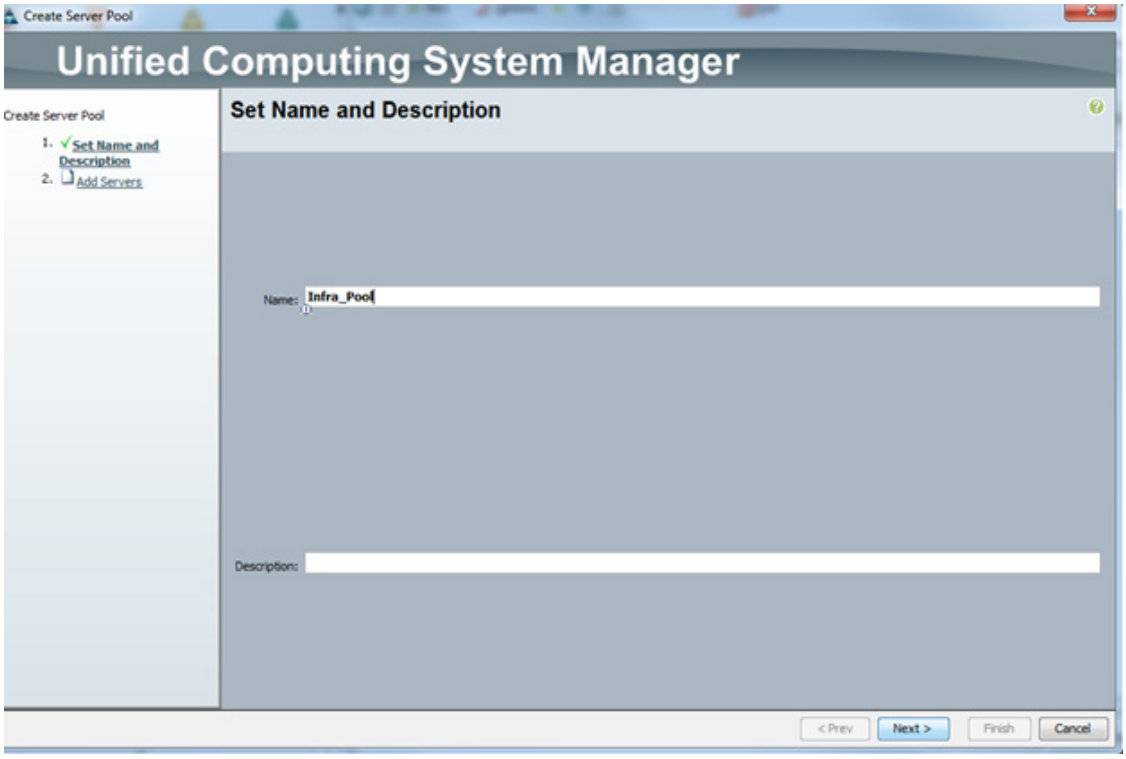
14. Click Finish.
15. Click OK.

Create Server Pool

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

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

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Pools > root.
3. Right-click Server Pools.
4. Select Create Server Pool.
5. Enter `Infra_Pool` as the name for server pool.
6. Optional: Enter a description for the server pool.



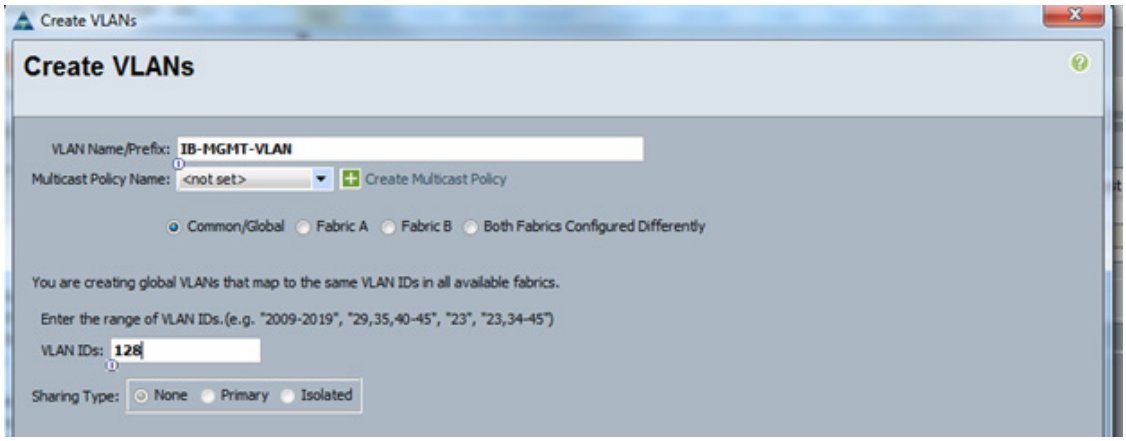
7. Click Next.
8. Select two servers to be used for the VMware management cluster and click >> to add them to the `Infra_Pool` server pool.

9. Click Finish.
10. Click OK.

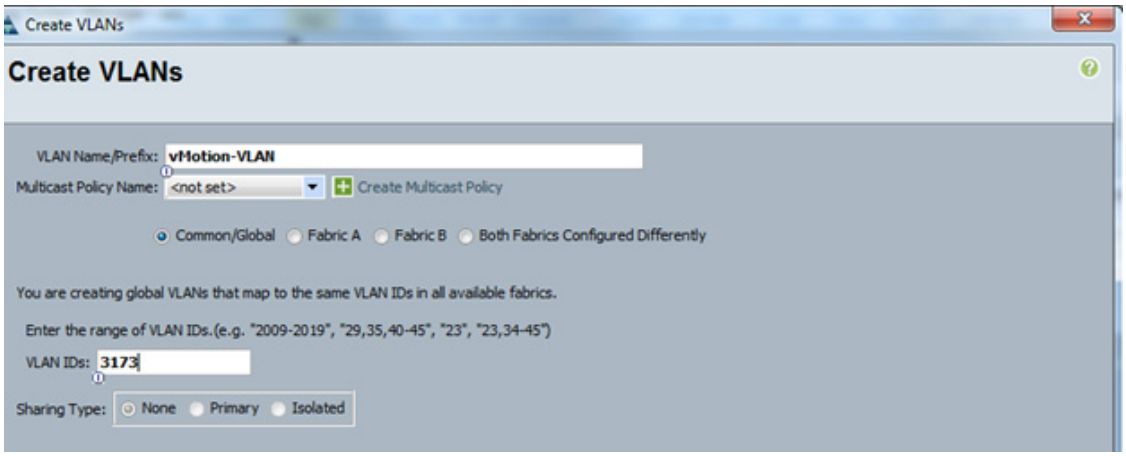
Create VLANs

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

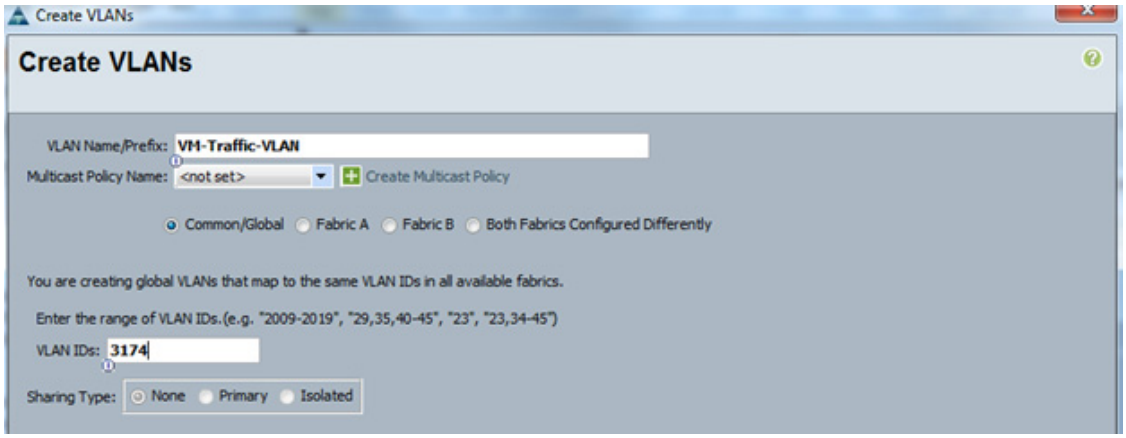
1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. In this procedure, five VLANs are created.
3. Select LAN > LAN Cloud.
4. Right-click VLANs.
5. Select Create VLANs.
6. Enter `IB-MGMT-VLAN` as the name for VLAN to be used for management traffic.
7. Retain the Common/Global option selected for the scope of the VLAN.
8. Enter `<<var_ib-mgmt_vlan_id>>` as the ID of the management VLAN.
9. Retain the Sharing Type as None.



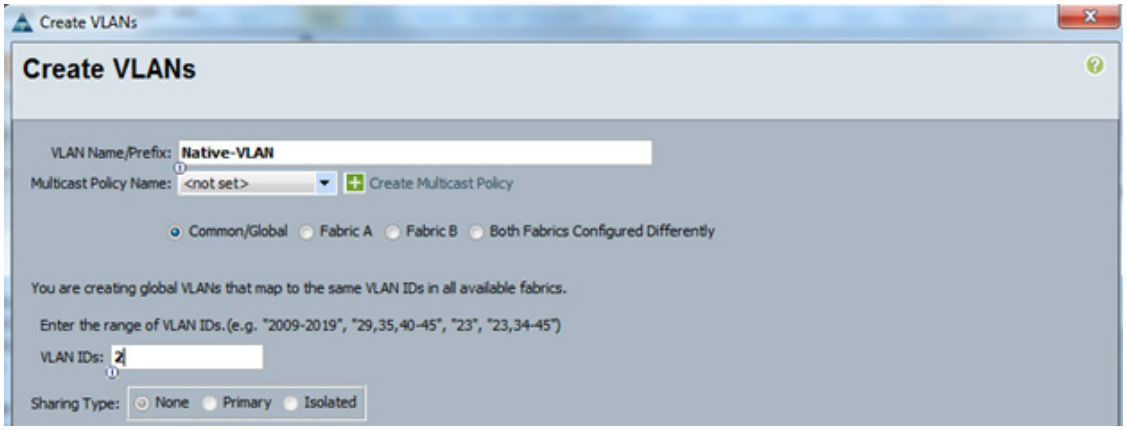
10. Click OK, and then click OK again.
11. Right-click VLANs.
12. Select Create VLANs.
13. Click OK, and then click OK again.
14. Right-click VLANs.
15. Select Create VLANs.
16. Enter `vMotion-VLAN` as the name for the VLAN to be used for vMotion.
17. Retain the Common/Global option selected for the scope of the VLAN.
18. Enter the `<<var_vmotion_vlan_id>>` as the ID of the vMotion VLAN.
19. Retain the Sharing Type as None.



20. Click OK, and then click OK again.
21. Right-click VLANs.
22. Select Create VLANs.
23. Enter `VM-Traffic-VLAN` as the name for the VLAN to be used for the VM traffic.
24. Retain the Common/Global option selected for the scope of the VLAN.
25. Enter the `<<var_vm-traffic_vlan_id>>` for the VMTraffic VLAN.
26. Retain the Sharing Type as None.



27. Click OK, and then click OK again.
28. Right-click VLANs.
29. Select Create VLANs.
30. Enter `Native-VLAN` as the name for the VLAN to be used as the native VLAN.
31. Keep the Common/Global option selected for the scope of the VLAN.
32. Enter the `<<var_native_vlan_id>>` as the ID for the native VLAN.
33. Keep the Sharing Type as None.



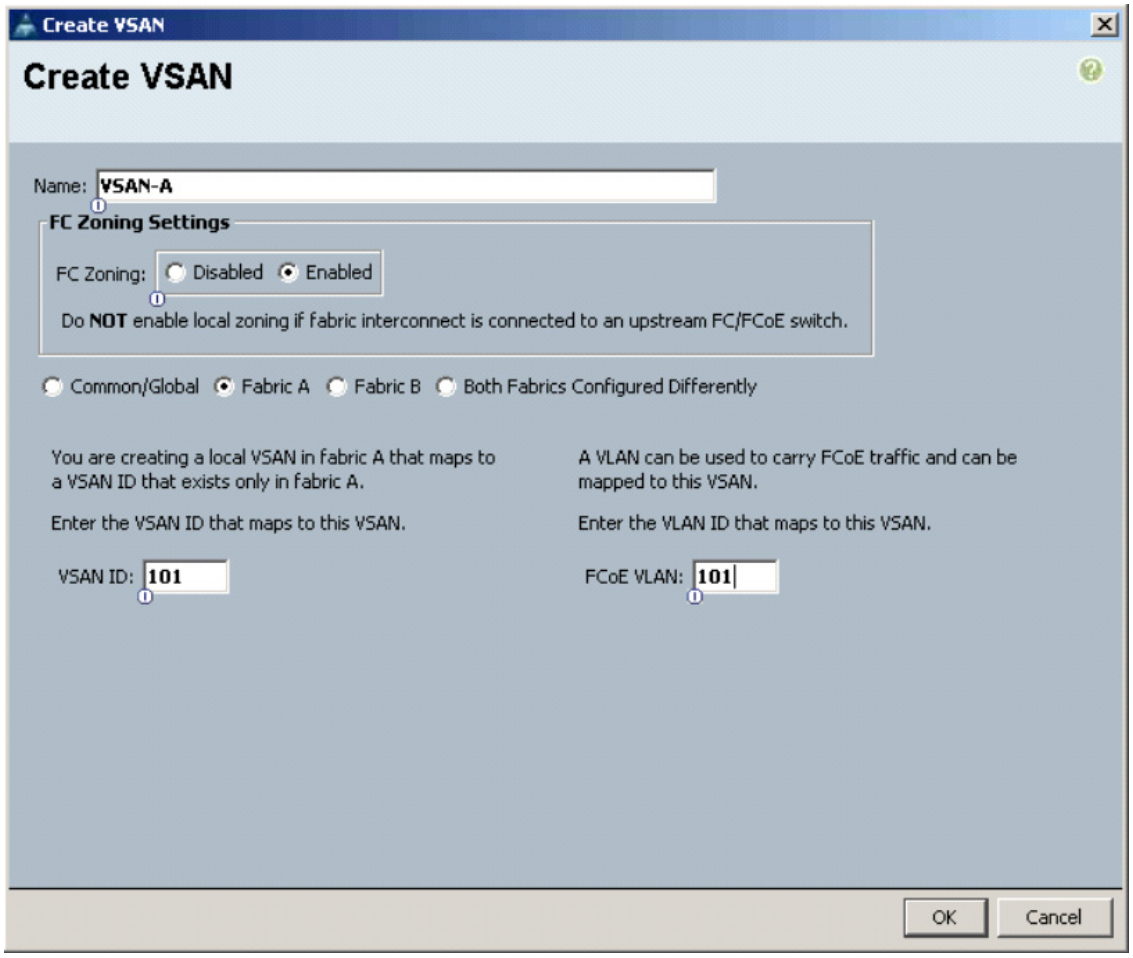
34. Click OK, and then click OK again.
35. Expand the list of VLANs in the navigation pane, right-click the newly created `Native-VLAN` and select Set as Native VLAN.
36. Click Yes and then click OK.

Create VSANs and Configure FS Storage Ports

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

1. In Cisco UCS Manager, click the SAN tab in the navigation pane.
2. Expand the SAN > SAN Cloud tree.
3. Right-click VSANs.
4. Select Create VSAN.
5. Enter `VSAN_A` as the name for the VSAN for Fabric A.
6. Select the Enabled option for FC Zoning.
7. Select Fabric A.
8. Enter `<<var_vsan_a_id>>` as the VSAN ID for Fabric A.
9. Enter `<<var_fabric_a_fcoe_vlan_id>>`as the FCoE VLAN ID for Fabric A.

Note For the FlexPod solution, it is recommended to use the same ID for the VSAN and the FC VLAN required for Fabric A.



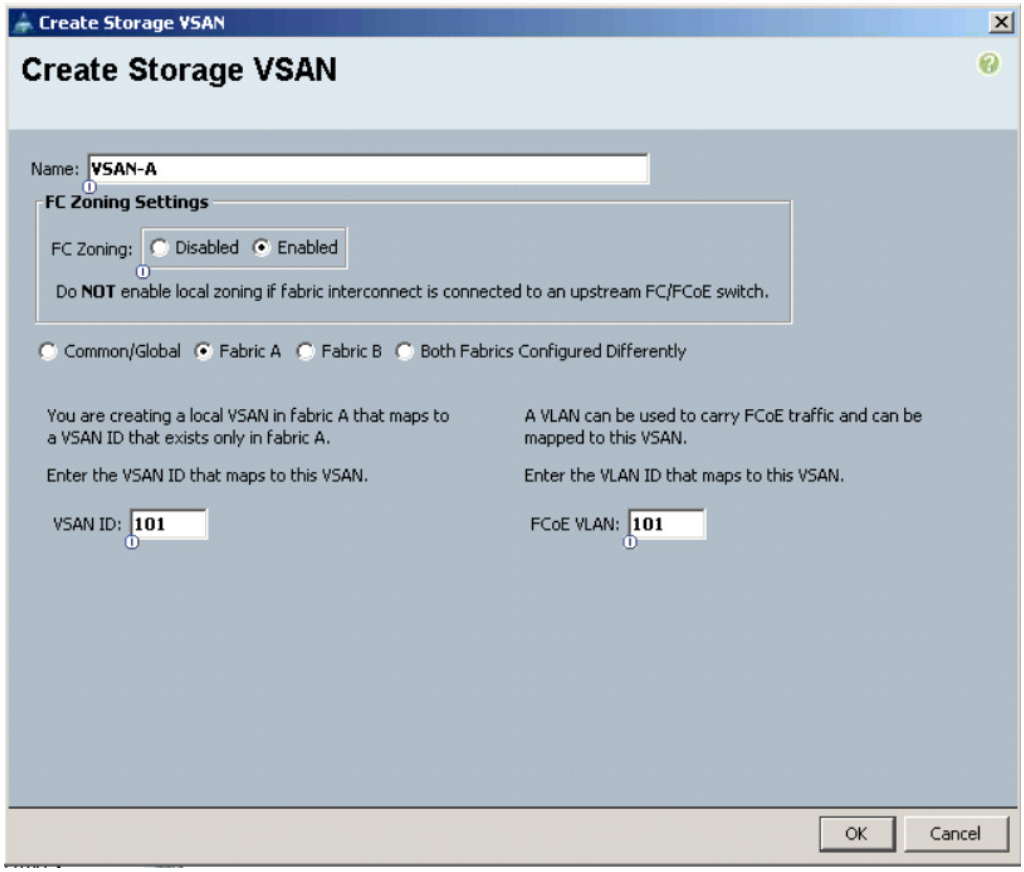
10. Click OK and click OK again to create the VSAN.
11. Right-click VSANs.
12. Select Create VSAN.
13. Enter `VSAN_B` as the name for the VSAN for Fabric B.
14. Select the Enabled option for FC Zoning.
15. Select Fabric B.
16. Enter `<<var_vsan_b_id>>` as the VSAN ID for Fabric B.
17. Enter `<<var_fabric_b_fcoe_vlan_id>>` as the FCoE VLAN ID for Fabric B.

Note NetApp recommends using the same ID for the VSAN and the FCoE VLAN required for Fabric B.

18. Click OK, and then click OK again to create the VSAN.
19. Expand the SAN > Storage Cloud tree.
20. Right-click VSANs.
21. Select Create Storage VSAN.
22. Enter `VSAN_A` as the name for the VSAN for Fabric A.

23. Select the Enabled option for FC Zoning.
24. Select Fabric A.
25. Enter `<<var_vsan_a_id>>` as the VSAN ID for Fabric A.
26. Enter `<<var_fabric_a_fcoe_vlan_id>>`as the FCoE VLAN ID for Fabric A.

Note For the FlexPod solution, it is recommended to use the same ID for the VSAN and the FC VLAN required for Fabric A.



27. Click OK and then click OK again to create the VSAN.
28. Right-click VSANs.
29. Select Create Storage VSAN.
30. Enter `VSAN_B` as the name for the VSAN for Fabric B.
31. Select the Enabled option for FC Zoning.
32. Select Fabric B.
33. Enter `<<var_vsan_b_id>>` as the VSAN ID for Fabric B.
34. Enter `<<var_fabric_b_fcoe_vlan_id>>` as the FCoE VLAN ID for Fabric B.

Note NetApp recommends using the same ID for the VSAN and the FCoE VLAN required for Fabric B.

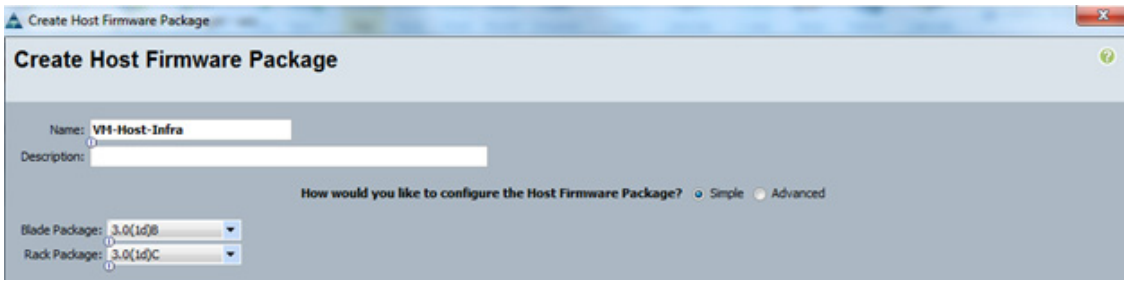
35. Click OK and then click OK again to create the VSAN.
36. In the navigation pane, under SAN > SStorage, expand the Fabric A tree.
37. Right-click FC Port Channels.
38. Expand Storage FC Interfaces
39. Select FC Interface 1/1.
40. In the User Label field, put in information indicating the storage controller port, such as <storage_controller_01_name>:0c. Click Save Changes and OK.
41. Select the Fabric A VSAN and select Save Changes and OK.
42. Select FC Interface 1/2.
43. In the User Label field, put in information indicating the storage controller port, such as <storage_controller_02_name>:0c. Click Save Changes and OK.
44. Select the Fabric A VSAN and select Save Changes and OK.

Create 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 the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Host Firmware Packages.
4. Select Create Host Firmware Package.
5. Enter `VM-Host-Infra` as the name for the host firmware package.
6. Leave Simple selected.
7. Select the version 3.0(1c) for both the Blade and Rack Packages.

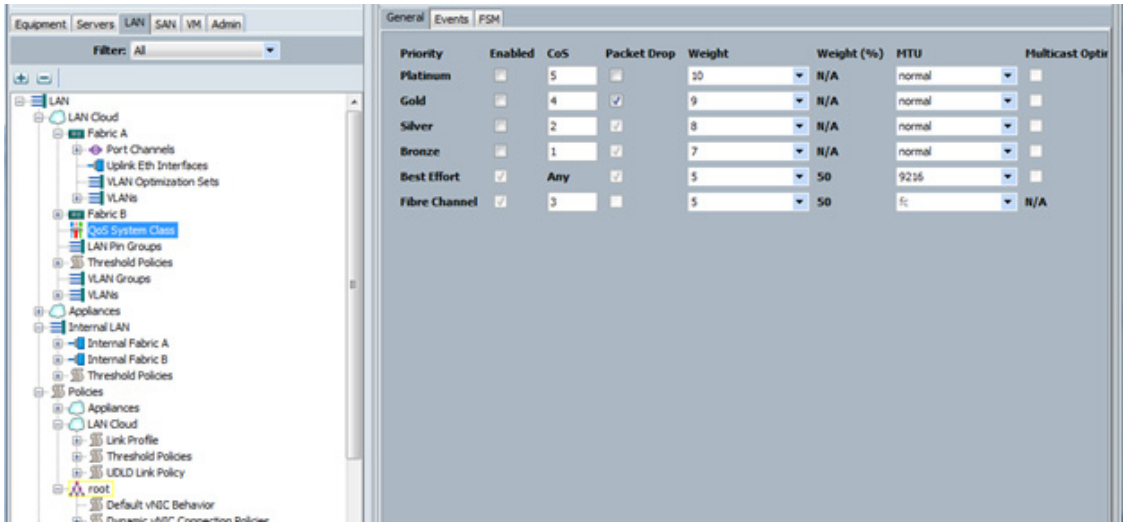


8. Click OK to create the host firmware package.
9. Click OK.

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, in the navigation pane, click the LAN tab.
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.
6. Click OK.

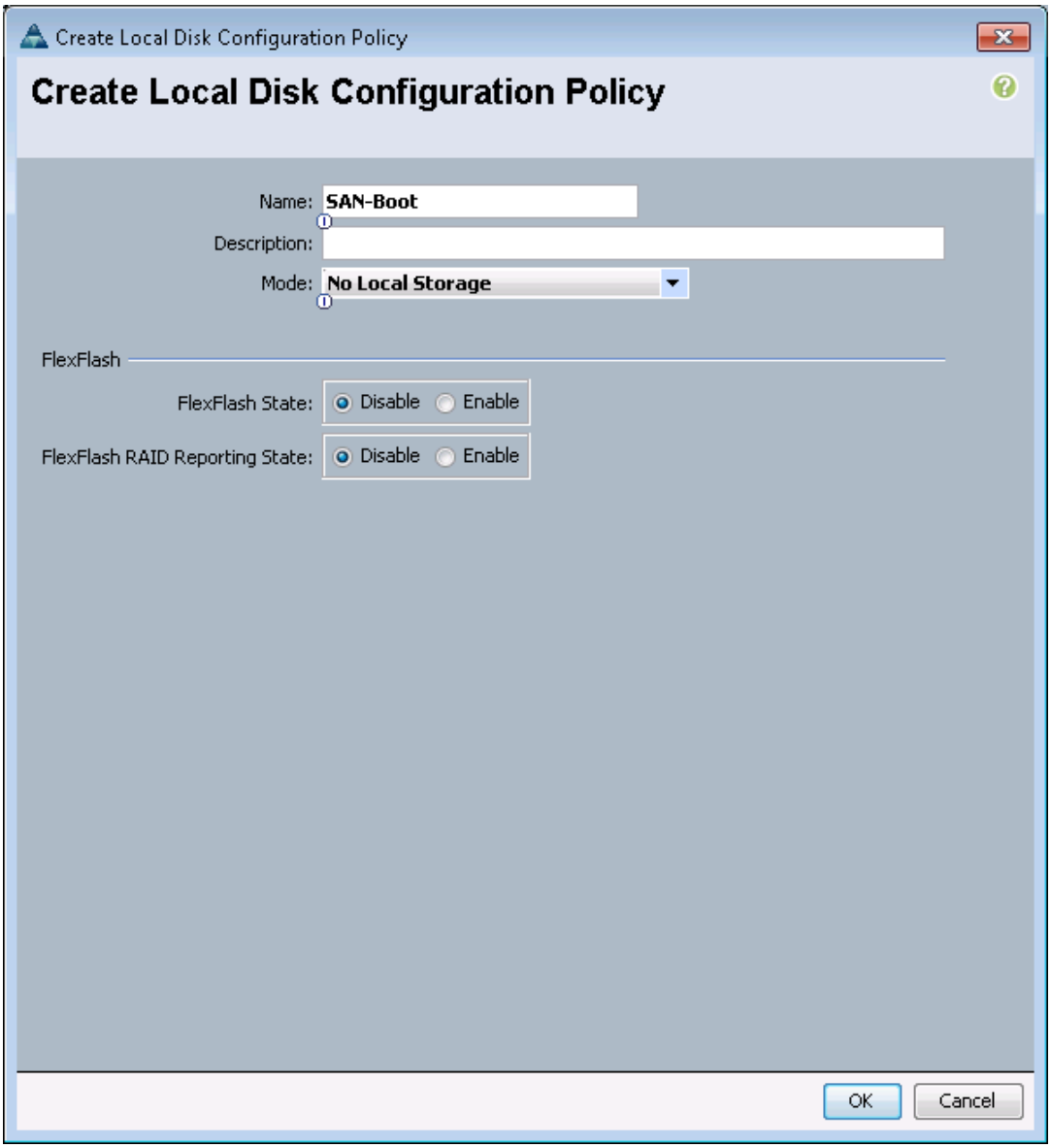
Create Local Disk Configuration Policy (Optional)

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

Note 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, in the navigation pane, click the Servers tab.
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. Retain the FlexFlash State and FlexFlash Raid Reporting State at Disable.



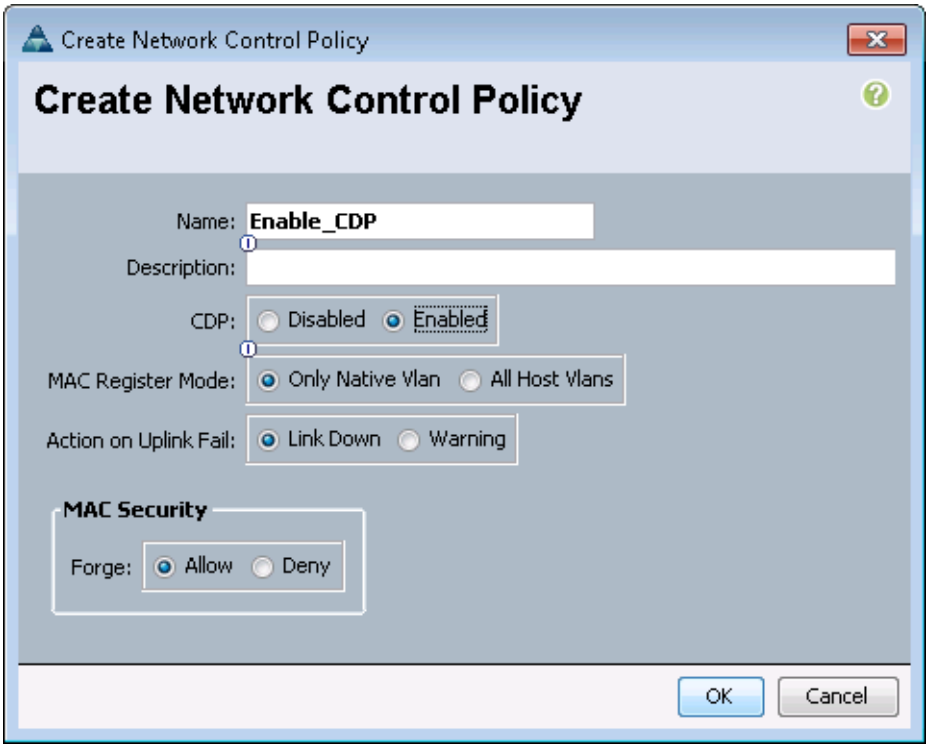
8. Click OK to create the local disk configuration policy.
9. Click OK.

Create Network Control Policy for Cisco Discovery Protocol

To create a network control policy that enables Cisco Discovery Protocol (CDP) on virtual network ports, complete the following steps:

1. In Cisco UCS Manager, in the navigation pane, click the LAN tab.
2. Select Policies > root.
3. Right-click Network Control Policies.
4. Select Create Network Control Policy.

5. Enter `Enable_CDP` as the policy name.
6. For CDP, select the Enabled option.

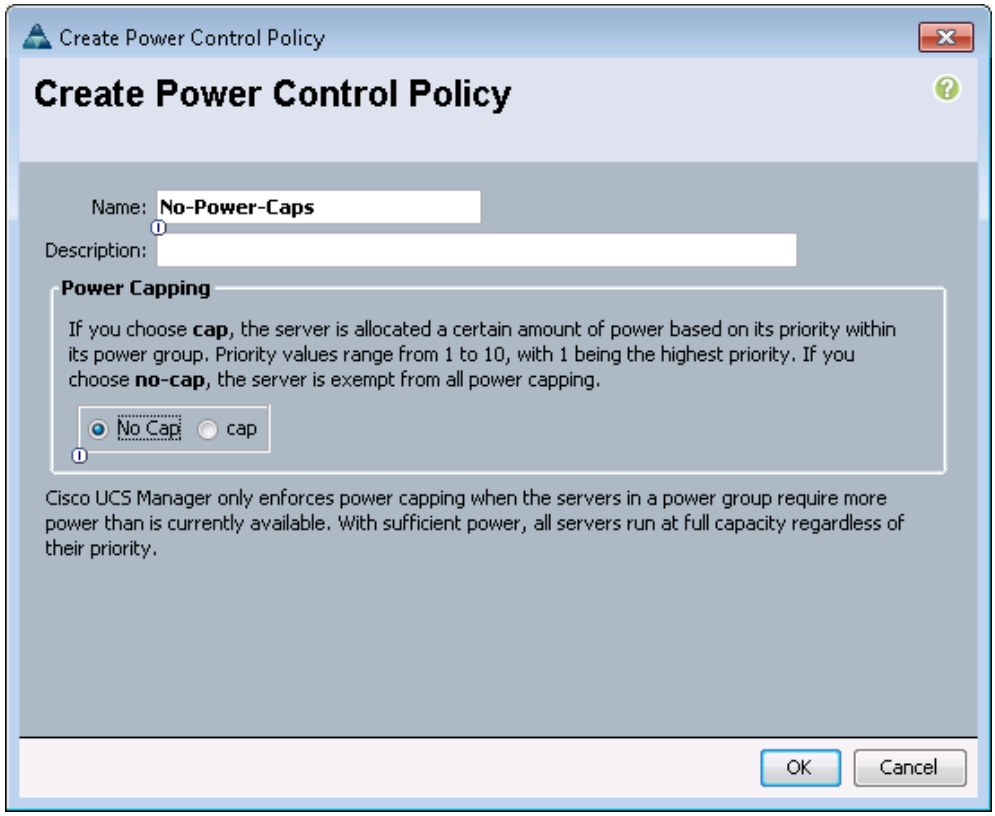


7. Click OK to create the network control policy.
8. Click OK.

Create Power Control Policy

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

1. In Cisco UCS Manager, in the navigation pane, click the Servers tab.
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.



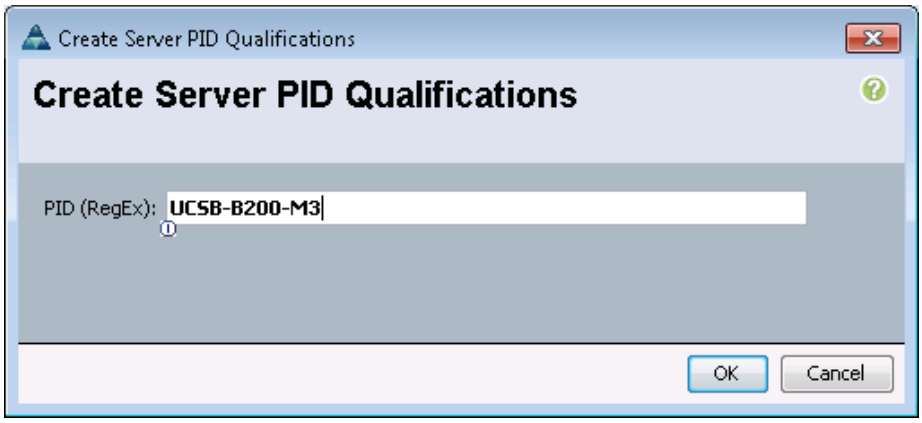
7. Click OK to create the power control policy.
8. Click OK.

Create Server Pool Qualification Policy (Optional)

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

Note This example creates a policy for a Cisco UCS B200-M3 server.

1. In Cisco UCS Manager, in the navigation pane, click the Servers tab.
2. Select Policies > root.
3. Right-click Server Pool Policy Qualifications.
4. Select Create Server Pool Policy Qualification.
5. Enter `UCSB-B200-M3` as the name for the policy.
6. In the left pane, under Actions Select Create Server PID Qualifications.
7. Enter `UCSB-B200-M3` as the PID.

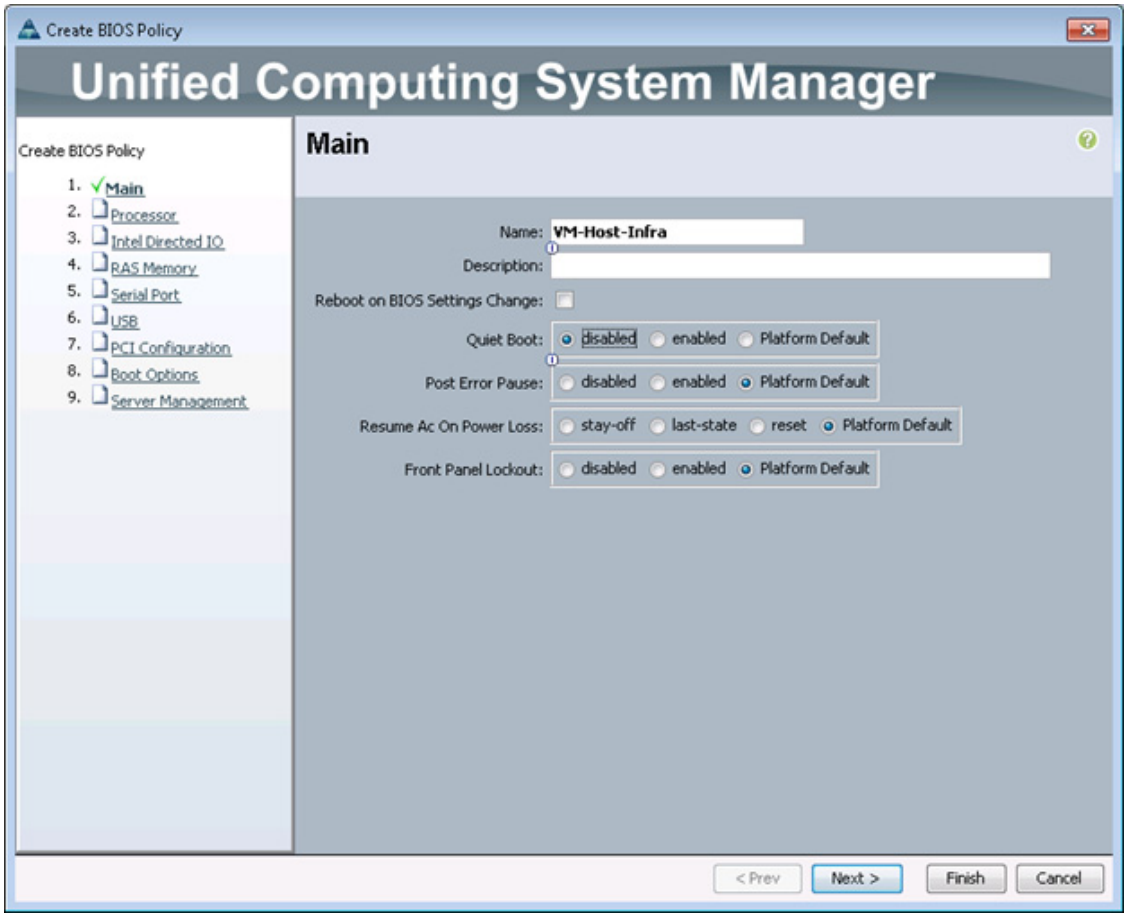


8. Click OK to create the server pool qualification policy.
9. Click OK and then click OK again.

Create Server BIOS Policy

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

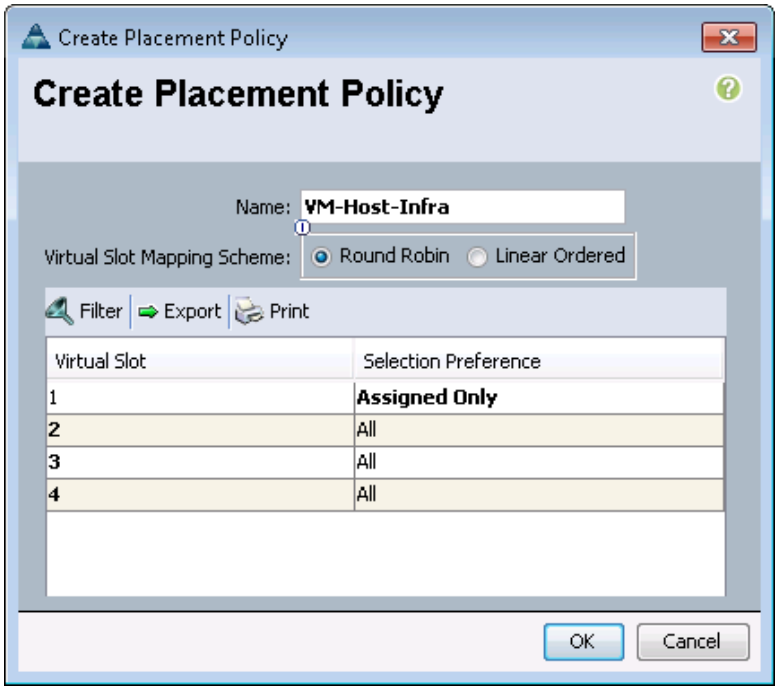
1. In Cisco UCS Manager, in the navigation pane, click the Servers tab.
2. Select Policies > root.
3. Right-click BIOS Policies.
4. Select Create BIOS Policy.
5. Enter `VM-Host-Infra` as the BIOS policy name.
6. Change the Quiet Boot setting to Disabled.



7. Click Finish to create the BIOS policy.
8. Click OK.

Create vNIC/vHBA Placement Policy for Virtual Machine Infrastructure Hosts

1. To create a vNIC/vHBA placement policy for the infrastructure hosts, complete the following steps:
2. In Cisco UCS Manager, in the navigation pane, click the Servers tab.
3. Select Policies > root.
4. Right-click vNIC/vHBA Placement Policies.
5. Select Create Placement Policy.
6. Enter `VM-Host-Infra` as the name for the placement policy.
7. Click 1 and under the Selection Preference select Assigned Only.

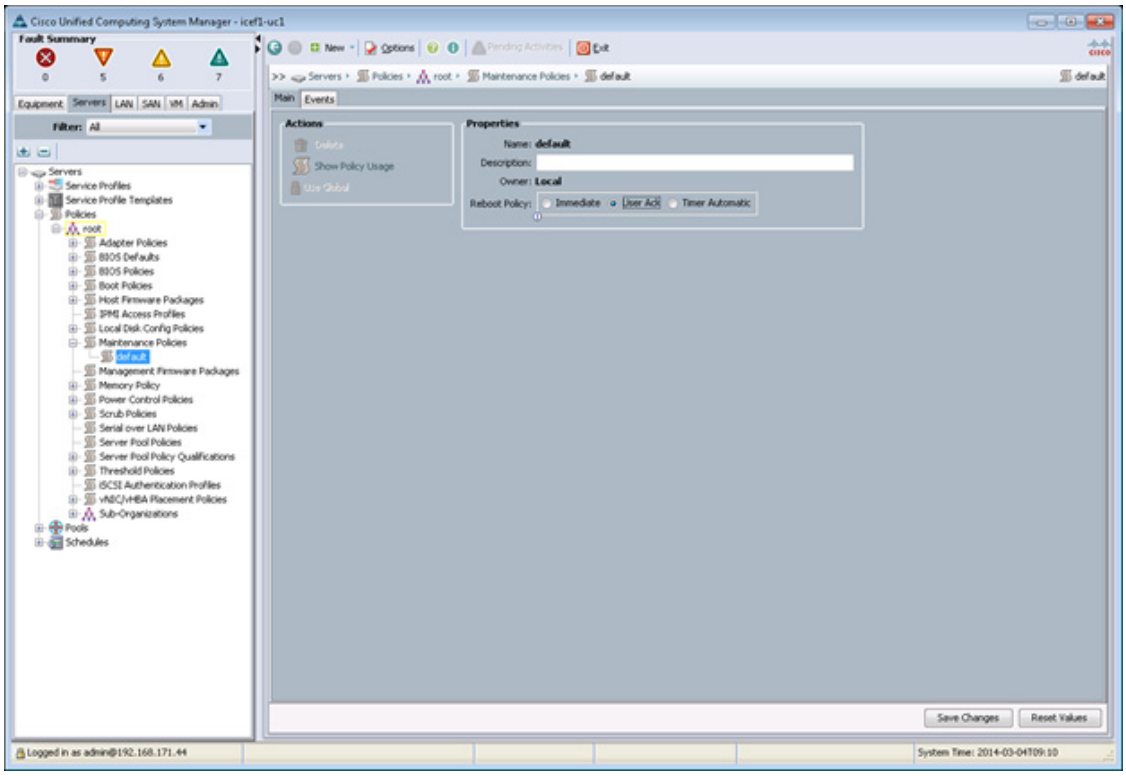


8. Click OK and then click OK again.

Update Default Maintenance Policy

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

1. In Cisco UCS Manager, in the navigation pane, click the Servers tab.
2. Choose Policies > root.
3. Choose Maintenance Policies > default.
4. Change the Reboot Policy to User Ack.



5. Click Save Changes.
6. Click OK to acknowledge the change.

Create vNIC Templates

To create multiple virtual network interface card (vNIC) templates for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, in the navigation pane, click the LAN tab.
2. Select Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter `vNIC_Template_A` as the vNIC template name.
6. For Fabric ID, select Fabric A.

Note Do not select the Enable Failover checkbox.

Note Under Target, do not select the VM checkbox.

7. Select Updating Template as the Template Type.
8. Under VLANs, select the checkboxes for `IB-MGMT-VLAN, Native-VLAN, VM-Traffic-VLAN`, and `vMotion-VLAN`.

9. Set `Native-VLAN` as the native VLAN.
10. For MTU, enter `9000`.
11. In the MAC Pool list, select `MAC_Pool_A`.
12. In the Network Control Policy list, select `Enable_CDP`.
13. Click OK to create the vNIC template.
14. Click OK.
15. In the navigation pane, select the LAN tab.
16. Select Policies > root.
17. Right-click vNIC Templates.
18. Select Create vNIC Template.
19. Enter `vNIC_Template_B` as the vNIC template name.
20. Select Fabric B.

Note Do not select the Enable Failover checkbox.

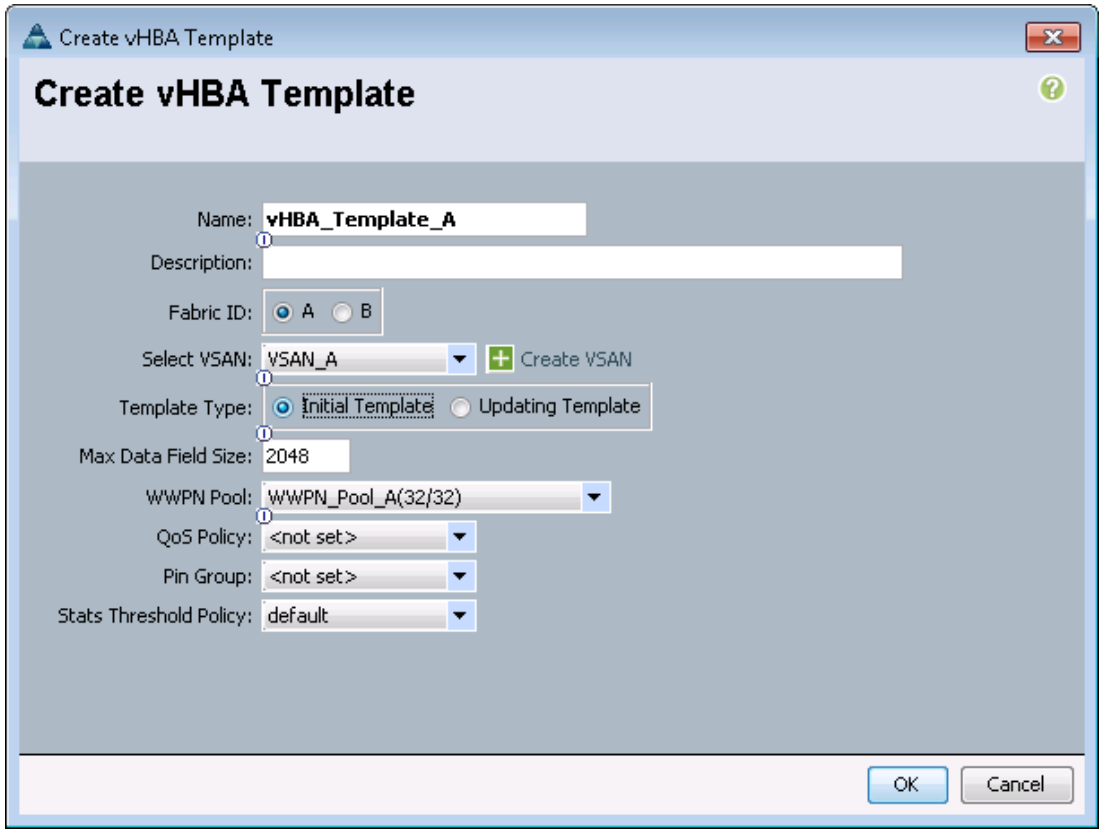
Note Under Target, do not select VM checkbox.

21. Select Updating Template as the template type.
22. Under VLANs, select the checkboxes for `IB-MGMT-VLAN, Native-VLAN, VM-Traffic-VLAN`, and `vMotion-VLAN`.
23. Set `Native-VLAN` as the native VLAN.
24. For MTU, enter `9000`.
25. In the MAC Pool list, select `MAC_Pool_B`.
26. In the Network Control Policy list, select `Enable_CDP`.
27. Click OK to create the vNIC template.
28. Click OK.

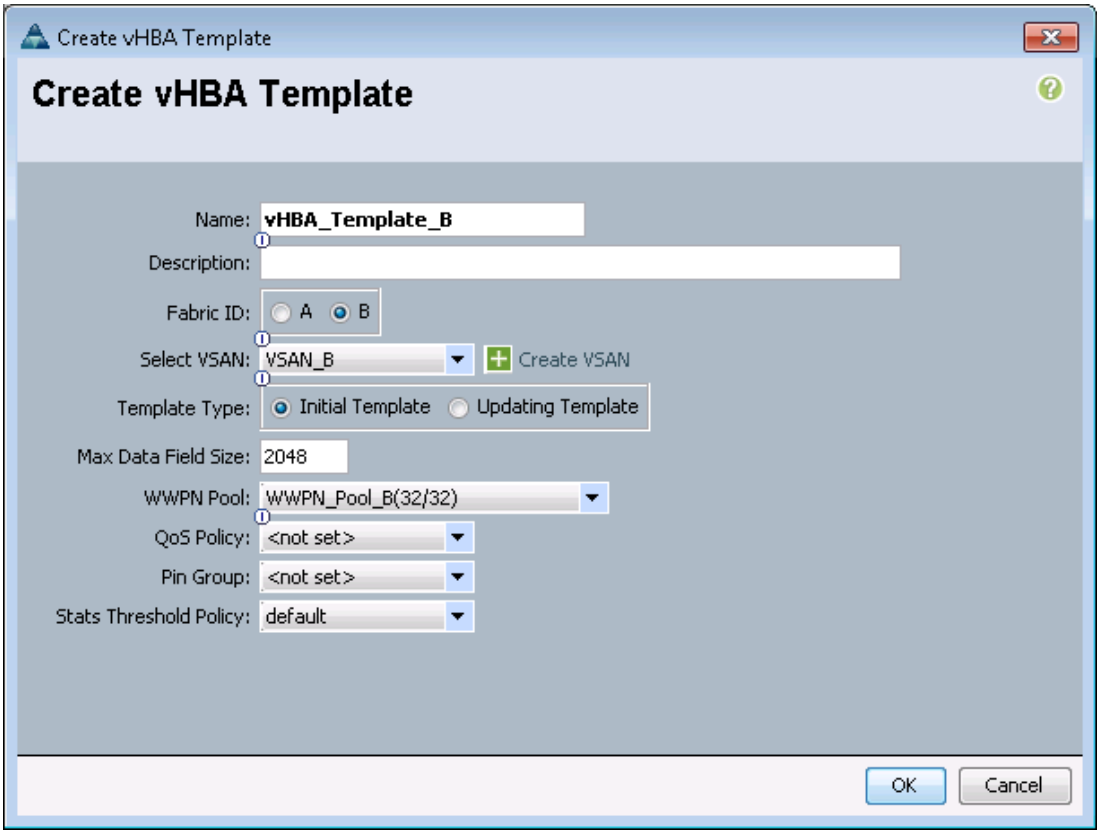
Create vHBA Templates for Fabric A and Fabric B

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

1. In Cisco UCS Manager, in the navigation pane, click the SAN tab.
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. Select A for Fabric ID.
7. In the Select VSAN list, select `VSAN_A`.
8. In the WWPN Pool list, select `WWPN_Pool_A`.



9. Click OK to create the vHBA template.
10. Click OK.
11. In the navigation pane, click the SAN tab.
12. Select Policies > root.
13. Right-click vHBA Templates.
14. Select Create vHBA Template.
15. Enter `vHBA_Template_B` as the vHBA template name.
16. Select B for Fabric ID.
17. In the Select VSAN list, select `VSAN_B`.
18. In the WWPN Pool, select `WWPN_Pool_B`.



19. Click OK to create the vHBA template.
20. Click OK.

Create Boot Policies

This procedure applies to a Cisco UCS environment in which two FCoE logical interfaces (LIFs) are on cluster node 1 (`fcp_lif01a` and `fcp_lif01b`) and two FCoE LIFs are on cluster node 2 (`fcp_lif02a` and `fcp_lif02b`). Also, it is assumed that the A LIFs are connected to Fabric A (Cisco UCS 6324 Fabric Interconnect A) and the B LIFs are connected to Fabric B (Cisco Fabric Interconnect B).

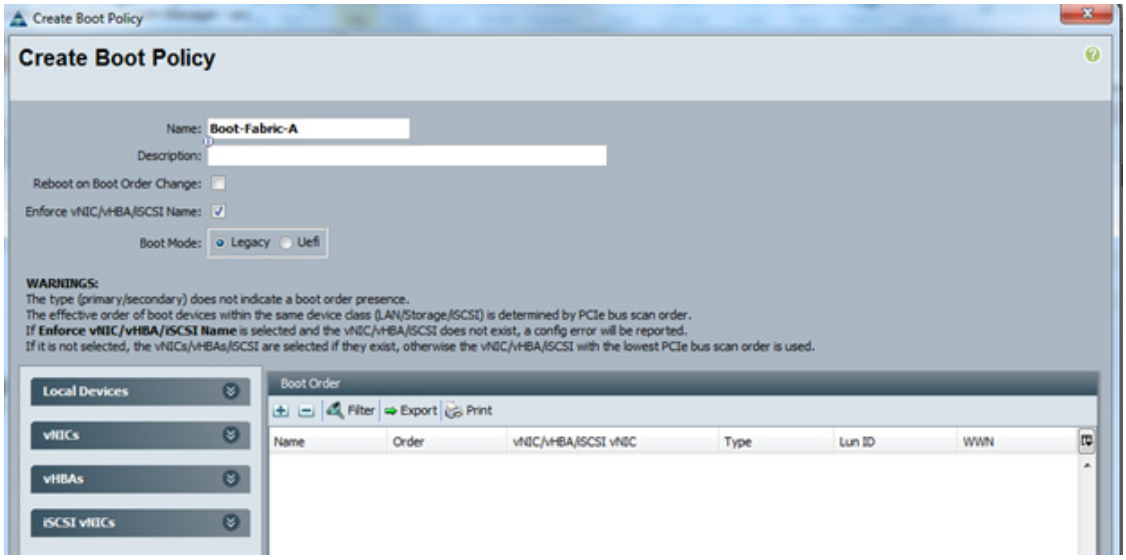
Two boot policies are configured in this procedure. The first policy configures the primary target to be `fcp_lif01a` and the second boot policy configures the primary target to be `fcp_lif01b`.

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

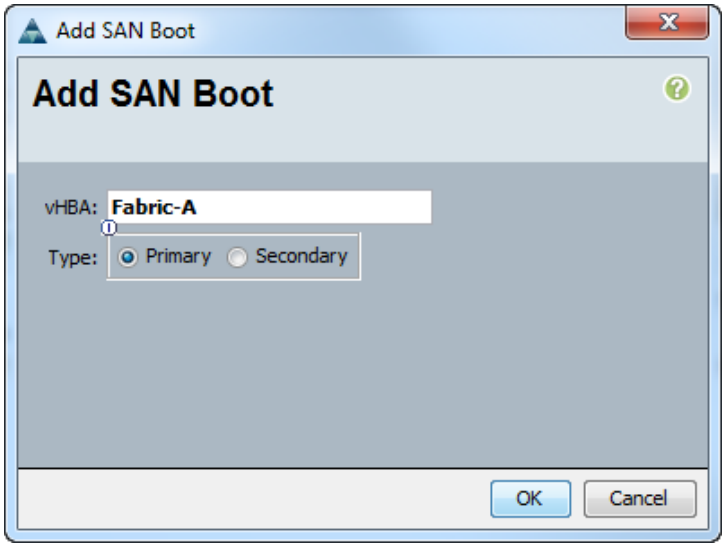
1. In Cisco UCS Manager, in the navigation pane, click the Servers tab.
2. Select Policies > root.
3. Right-click Boot Policies.
4. Select Create Boot Policy.
5. Enter `Boot-Fabric-A` as the name for the boot policy.
6. Optional: Enter a description for the boot policy.

Note Do not select the Reboot on Boot Order Change checkbox.

7. Expand the Local Devices drop-down menu, select Add Remote CD/DVD.



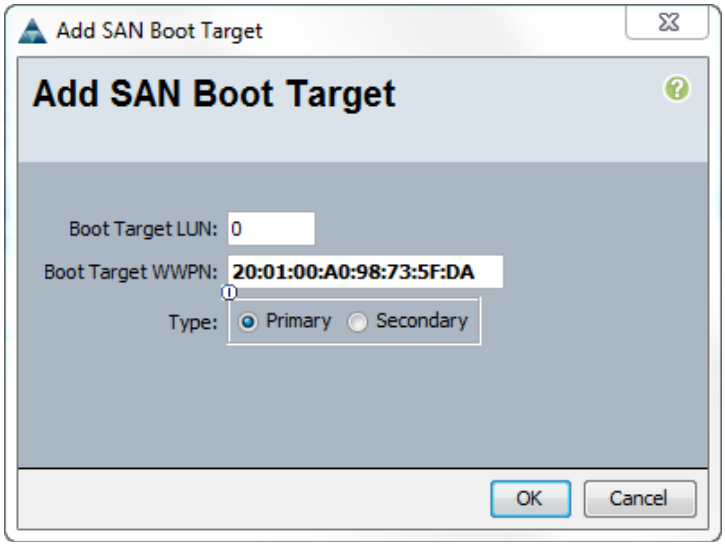
8. Expand the vHBAs drop-down menu and select Add SAN Boot.
9. In the Add SAN Boot dialog box, enter `Fabric-A` in the vHBA field.
10. Confirm that Primary is selected for the Type option.



11. Click OK to add the SAN boot initiator.
12. From the vHBA drop-down menu, select Add SAN Boot Target.
13. Keep `0` as the value for Boot Target LUN.
14. Enter the WWPN for `fcp_lif01a`.

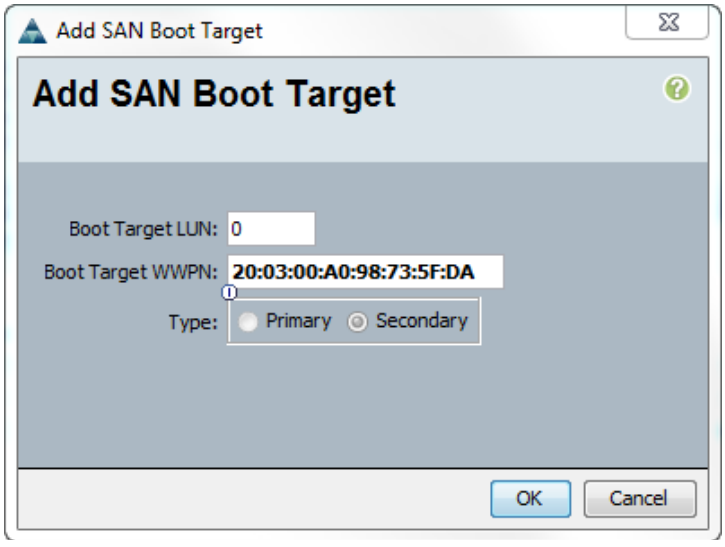
Note To obtain this information, log in to the storage cluster and run the `network interface show` command.

15. Select Primary for the SAN boot target type.

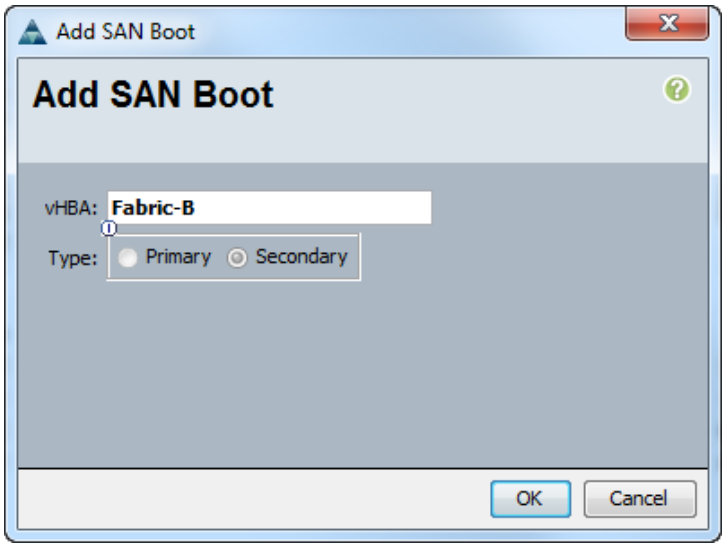


16. Click OK to add the SAN boot target.
17. From the vHBA drop-down menu, select Add SAN Boot Target.
18. Enter `0` as the value for Boot Target LUN.
19. Enter the WWPN for `fcp_lif02a`.

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



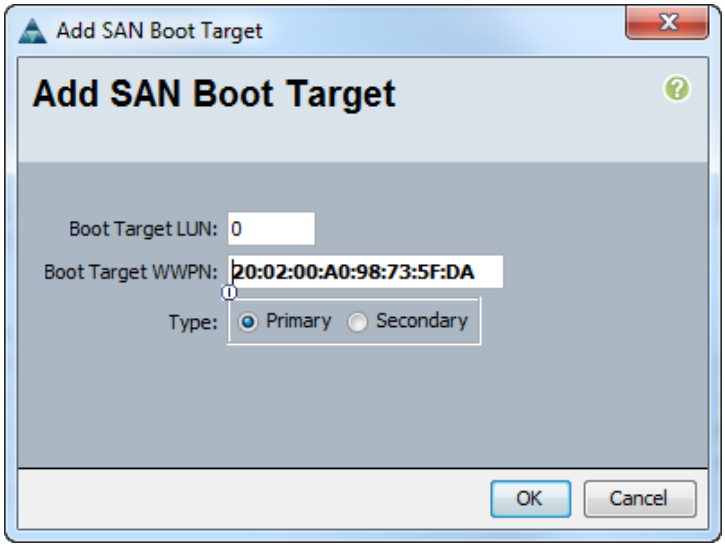
20. Click OK to add the SAN boot target.
21. From the vHBA drop-down menu, select Add SAN Boot.
22. In the Add SAN Boot dialog box, enter `Fabric-B` in the vHBA box.
23. The SAN boot type should automatically be set to Secondary, and the Type option should be unavailable.



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 `fcp_lif01b`.

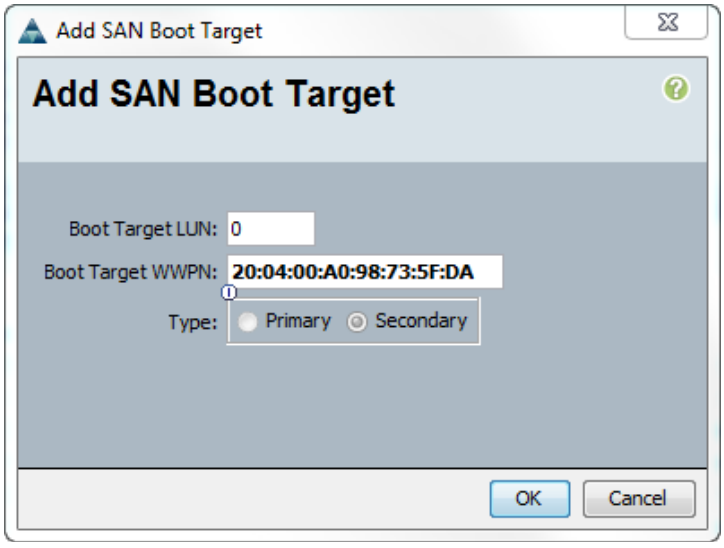
Note To obtain this information, log in to the storage cluster and run the `network interface show` command.

28. Select Primary for the SAN boot target type.

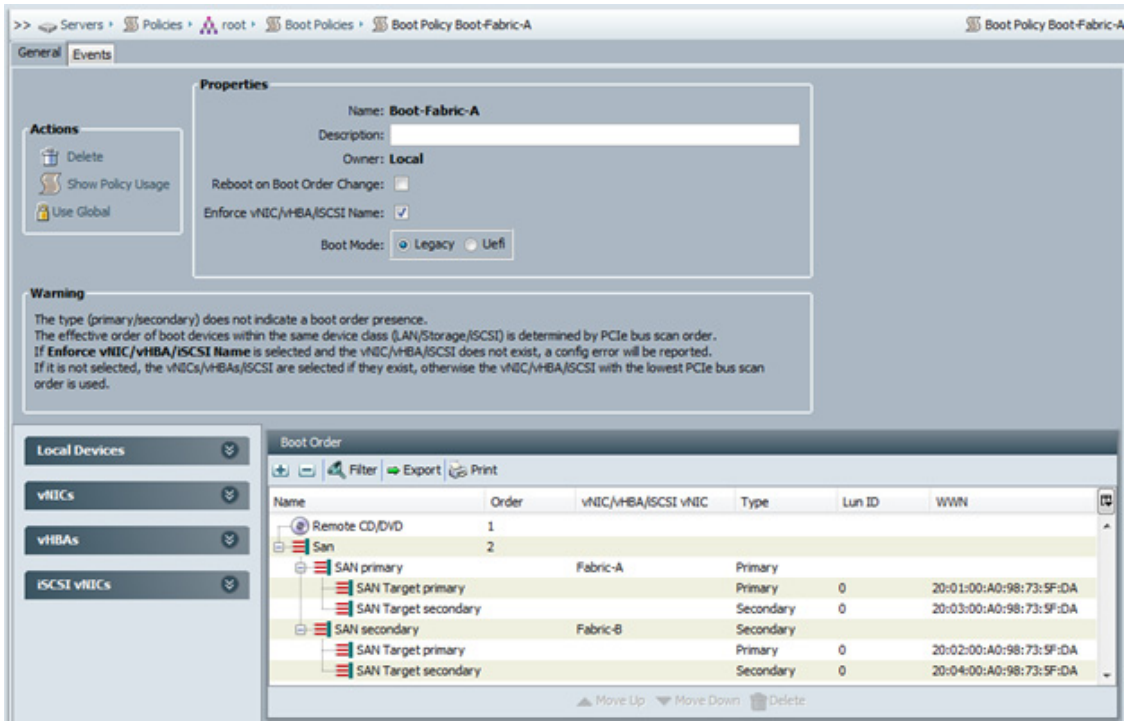


29. Click OK to add the SAN boot target.
30. From the vHBA drop-down menu, select Add SAN Boot Target.
31. Keep `0` as the value for Boot Target LUN.
32. Enter the WWPN for `fcp_lif02b`.

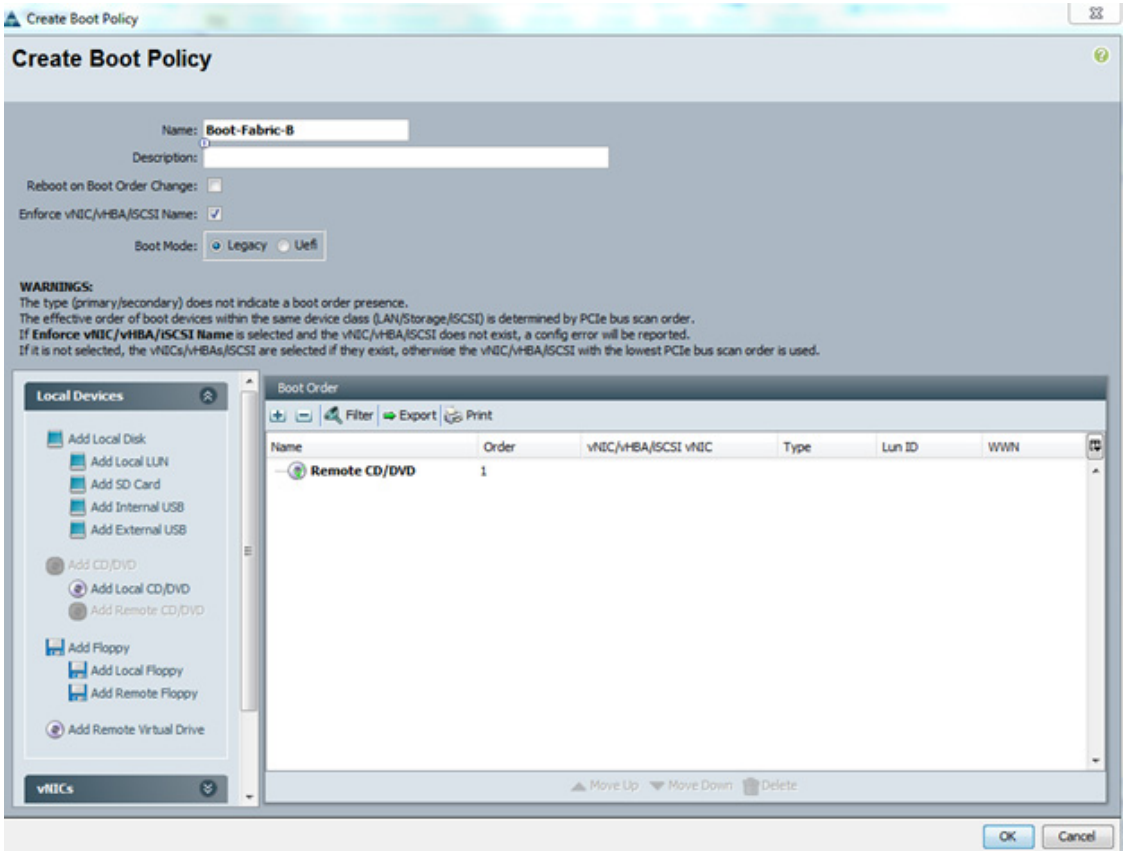
Note To obtain this information, log in to the storage cluster and run the `network interface show` command.



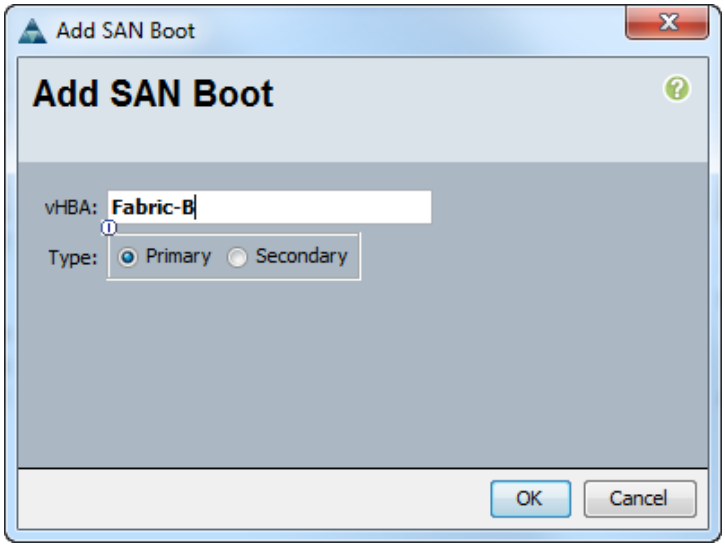
33. Click OK to add the SAN boot target.



34. Click OK then click OK again to create the boot policy.
35. Right-click Boot Policies again.
36. Select Create Boot Policy.
37. Enter `Boot-Fabric-B` as the name for the boot policy.
38. Optional: Enter a description of the boot policy.
39. Do not select the Reboot on Boot Order Change option.
40. From the Local Devices drop-down menu, select Add Remote CD/DVD.



41. From the vHBA drop-down menu, select Add SAN Boot.
42. In the Add SAN Boot dialog box, enter `Fabric-B` in the vHBA box.
43. Confirm that Primary option is selected for the SAN boot type.

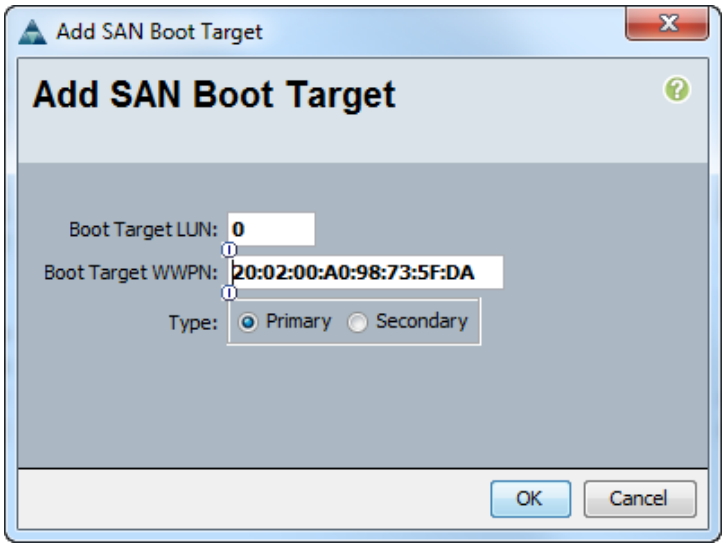


44. Click OK to add the SAN boot initiator.

45. From the vHBA drop-down menu, select Add SAN Boot Target.
46. Enter `0` as the value for Boot Target LUN.
47. Enter the WWPN for `fcp_lif01b`.

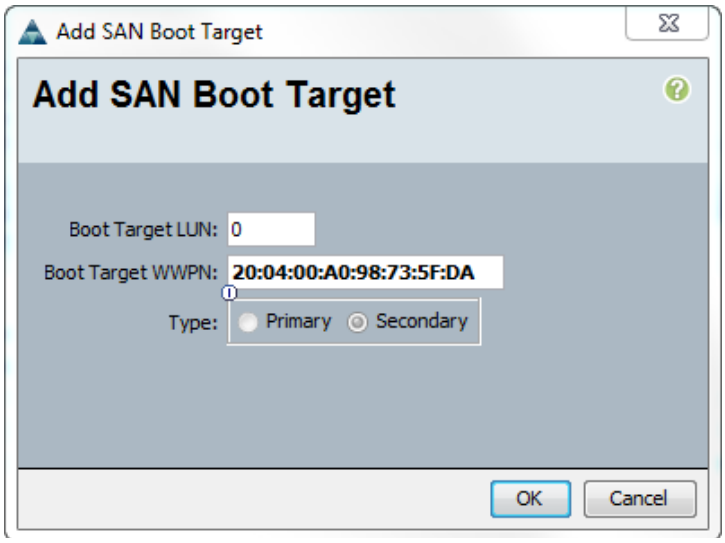
Note To obtain this information, log in to the storage cluster and run the `network interface show` command.

48. Select Primary option for the SAN boot target type.

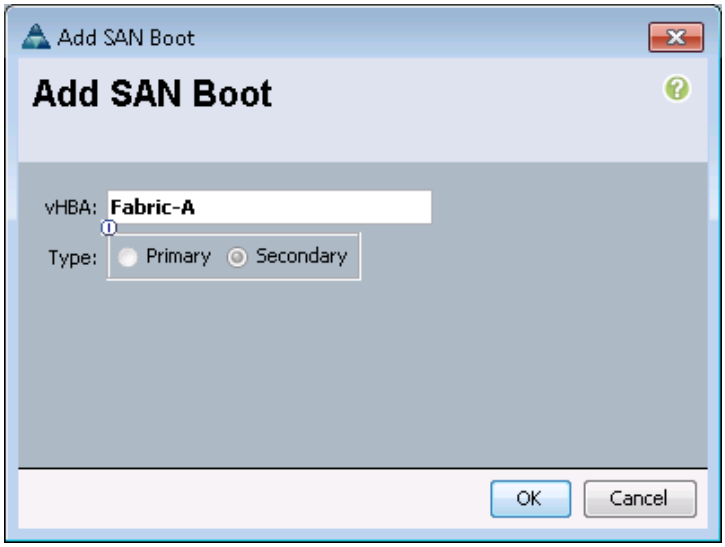


49. Click OK to add the SAN boot target.
50. From the `vHBA` drop-down menu, select Add SAN Boot Target.
51. Enter `0` as the value for Boot Target LUN.
52. Enter the WWPN for `fcp_lif02b`.

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



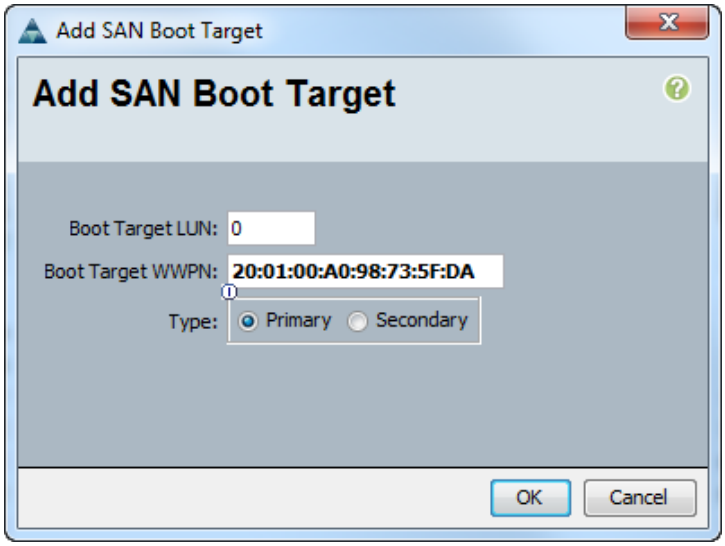
53. Click OK to add the SAN boot target.
54. From the vHBA menu, select Add SAN Boot.
55. In the Add SAN Boot dialog box, enter `Fabric-A` in the vHBA box.
56. The SAN boot type should automatically be set to Secondary, and the Type option should be unavailable.



57. Click OK to add the SAN boot initiator.
58. From the vHBA menu, select Add SAN Boot Target.
59. Enter `0` as the value for Boot Target LUN.
60. Enter the WWPN for `fcp_lif01a`.

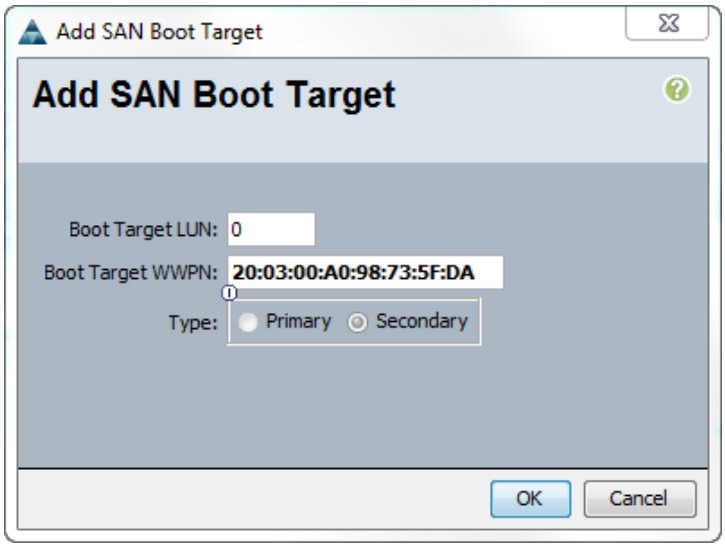
Note To obtain this information, log in to the storage cluster and run the `network interface show` command.

61. Select the Primary option for the SAN boot target type.

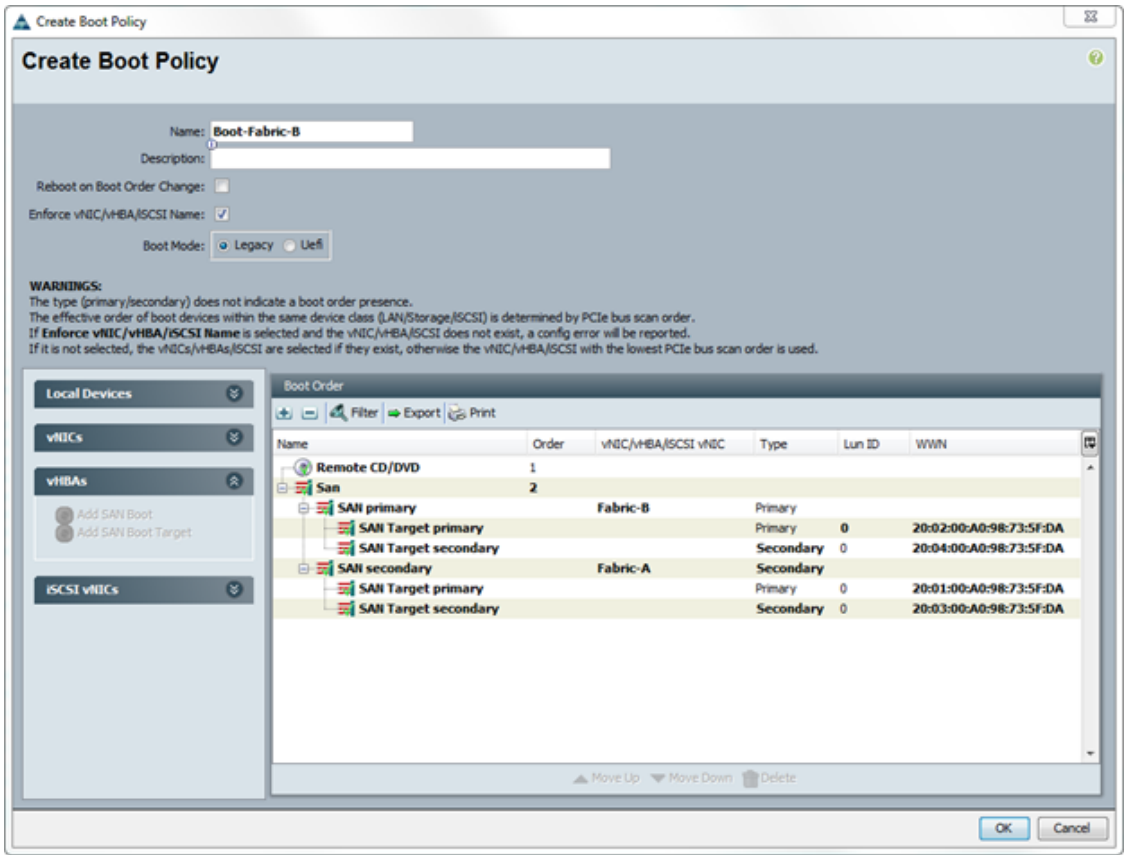


62. Click OK to add the SAN boot target.
63. From the vHBA drop-down menu, select Add SAN Boot Target.
64. Enter `0` as the value for Boot Target LUN.
65. Enter the WWPN for `fcp_lif02a`.

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



66. Click OK to add the SAN boot target.



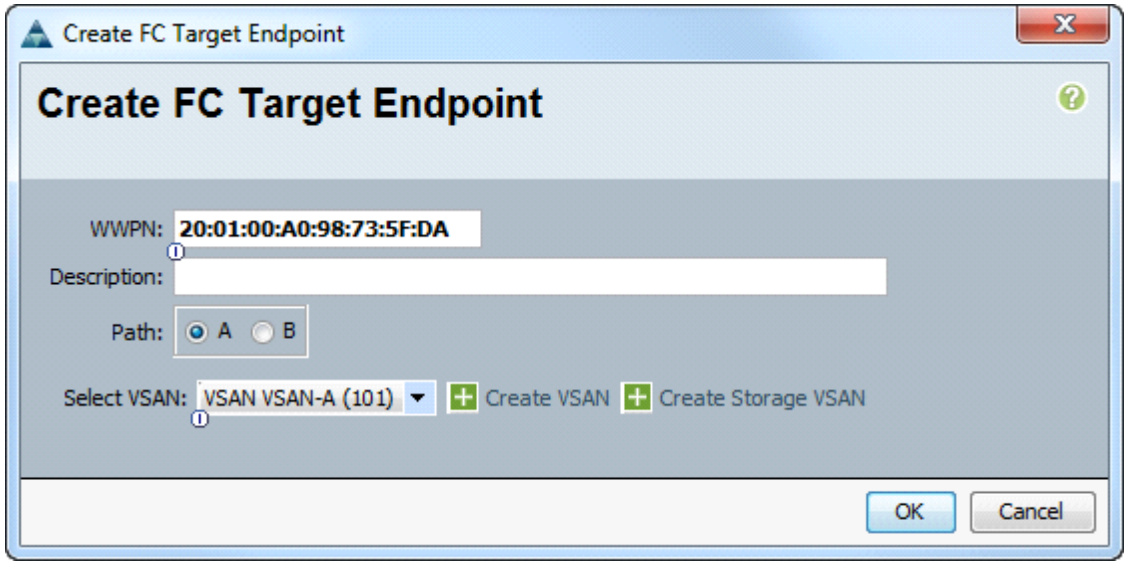
67. Click OK and then click OK again to create the boot policy.

Create Storage Connection Policies

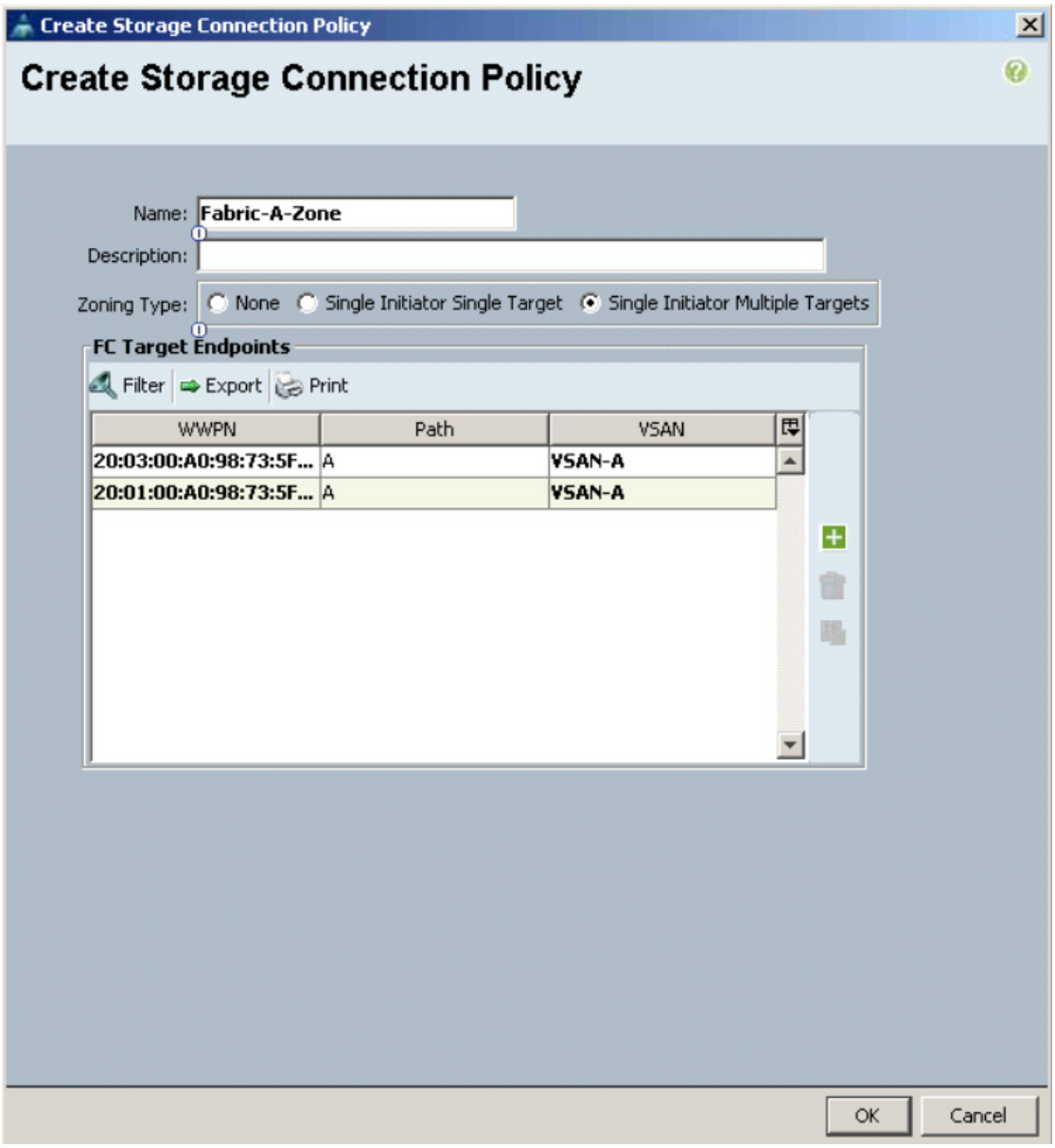
In this procedure, two storage connection policies are created for Fiber Channel zoning of server HBAs to storage: one for Fabric A and one for Fabric B.

To create the storage connection policies, complete the following steps:

1. In Cisco UCS Manager, in the navigation pane, click the SAN tab.
2. Select Policies > root > Storage Connection Policies.
3. Right-click Storage Connection Policies and select Create Storage Connection Policy.
4. Name the policy Fabric-A-Zone and select Single Initiator Multiple Targets.
5. Click the green Plus Sign on the lower right of the window to add a FC Target Endpoint.
6. Enter the WWPN of fcp_lif01a just as was done above on the Boot Policy and leave the Path A selected.
7. Select VSAN-A.

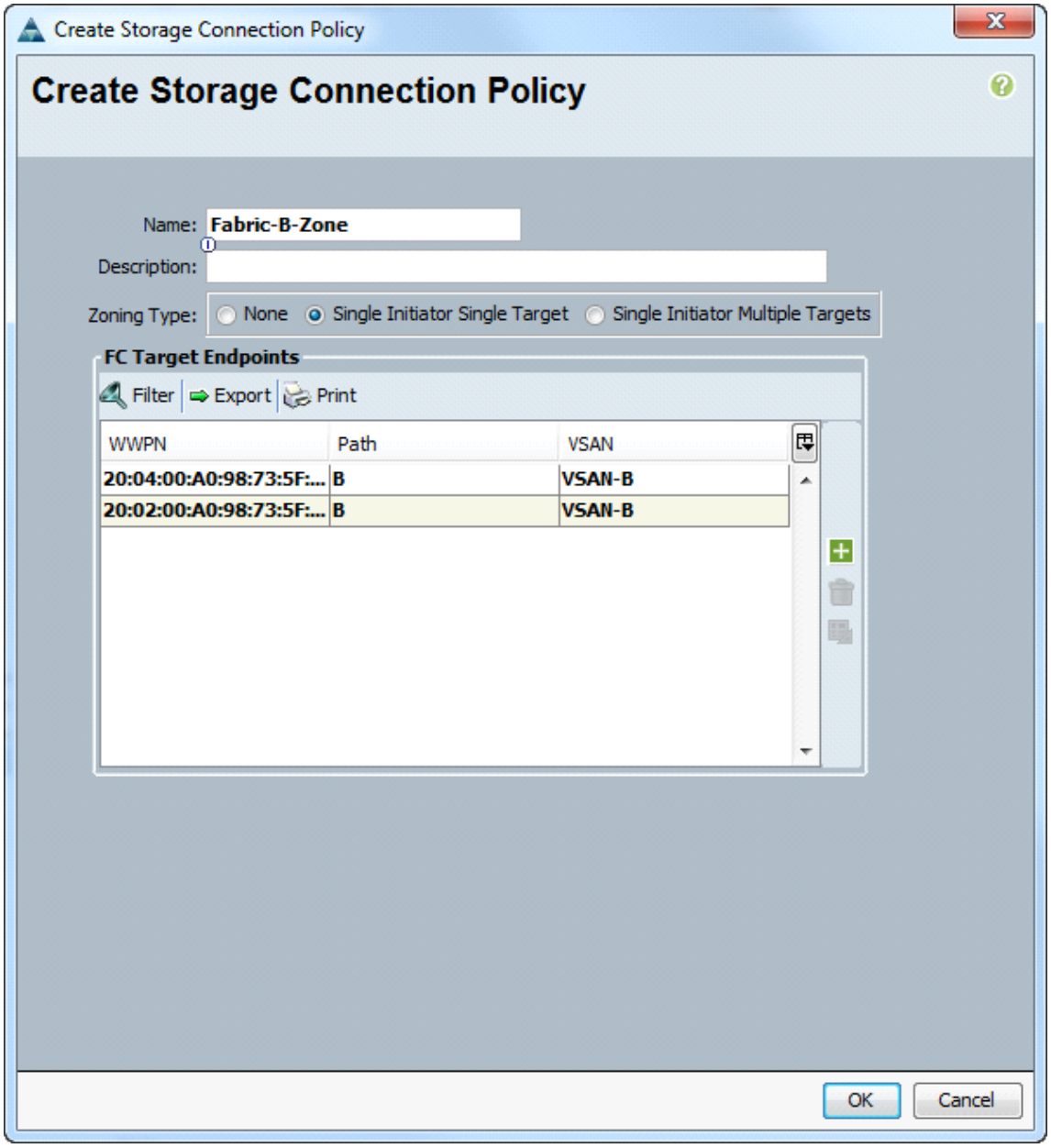


8. Select OK to add the endpoint.
9. Click the green Plus Sign on the lower right of the window to add a second FC Target Endpoint.
10. Enter the WWPN of fcp_lif02a and leave the Path A selected.
11. Select VSAN-A.
12. Click OK to add the endpoint.



13. Click OK and OK again to add the Storage Connection Policy.
14. Right-click Storage Connection Policies and select Create Storage Connection Policy.
15. Name the policy Fabric-B-Zone and select Single Initiator Multiple Targets.
16. Click the green Plus Sign on the lower right of the window to add a FC Target Endpoint.
17. Enter the WWPN of fcp_lif01b just as was done above on the Boot Policy and select the Path B.
18. Select VSAN-B.
19. Select OK to add the endpoint.
20. Click the green Plus Sign on the lower right of the window to add a second FC Target Endpoint.
21. Enter the WWPN of fcp_lif02b and select Path B.

22. Select VSAN-B.
23. Click OK to add the endpoint.



24. Click OK and OK again to add the Storage Connection Policy.

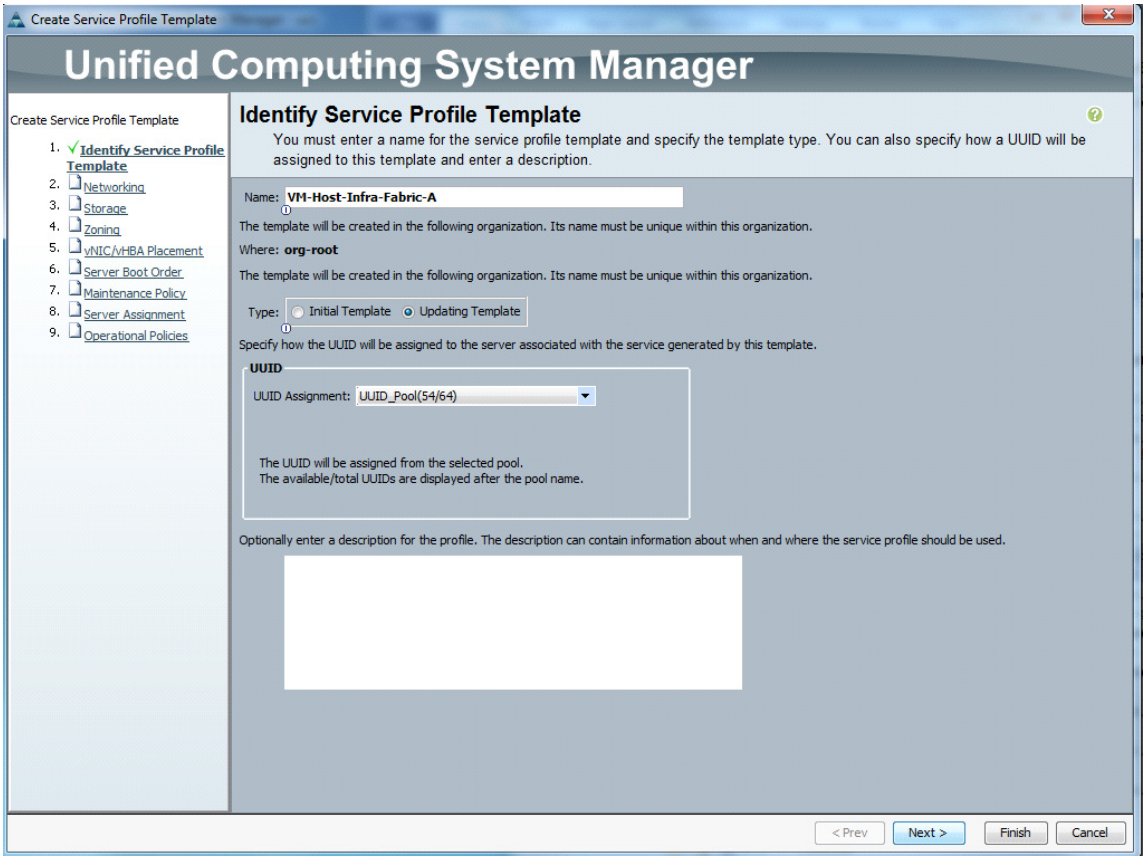
Create Service Profile Templates

In this procedure, two service profile templates are created: one for Fabric A boot and one for Fabric B boot. The first profile is created and then cloned and modified for the second host.

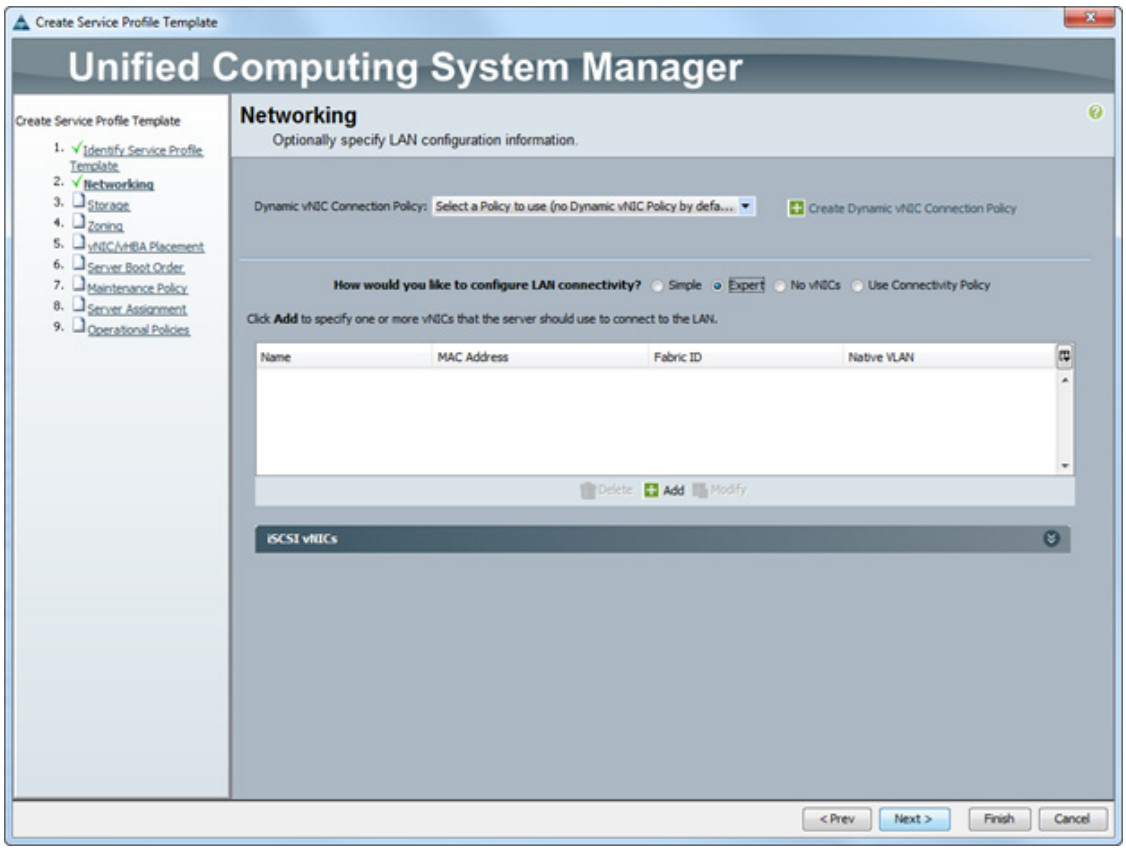
To create service profile templates, complete the following steps:

1. In Cisco UCS Manager, in the navigation pane, click the Servers tab.

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. Identify the Service Profile Template:
   a. Enter `VM-Host-Infra-Fabric-A` as the name for the service profile template. This service profile template is configured to boot from Node 1 on Fabric A.
   b. Select the Updating Template option.
   c. Under UUID, select `UUID_Pool` as the UUID pool.



   d. Click Next.
6. Configure the Networking options:
   a. Retain the default setting for Dynamic vNIC Connection Policy.
   b. Select the Expert option to configure the LAN connectivity.



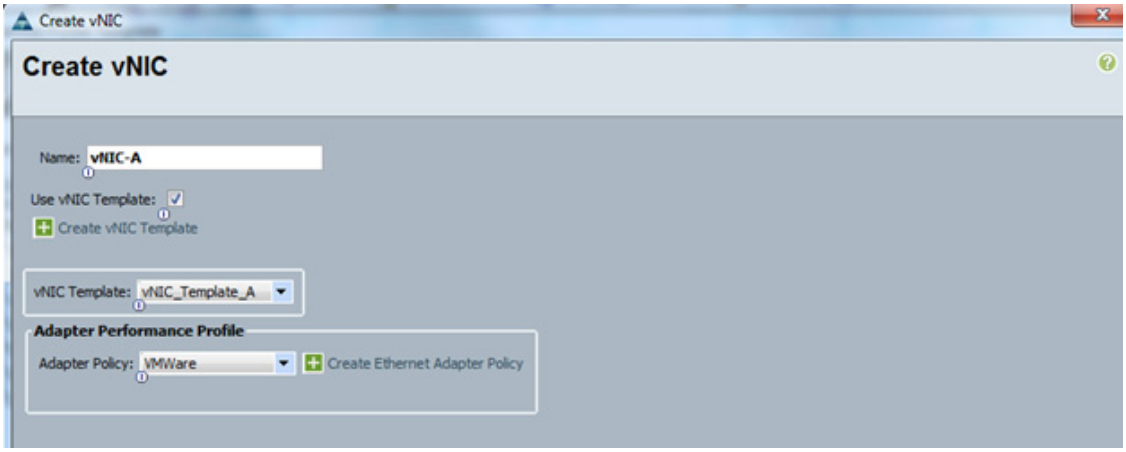
c. Click the upper Add button to add a vNIC to the template.

d. In the Create vNIC dialog box, enter `vNIC-A` as the name for vNIC.

e. Select the Use vNIC Template checkbox.

f. In the vNIC Template list, select `vNIC_Template_A`.

g. In the Adapter Policy list, select VMWare.



h. Click OK to add this vNIC to the template.

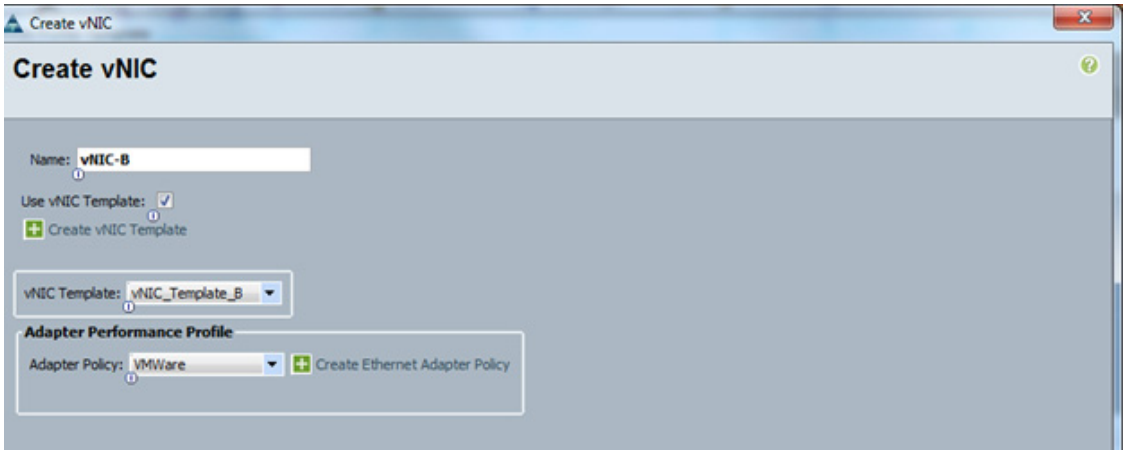
i. On the Networking page of the wizard, click the Add button to add another vNIC to the template.

j. In the Create vNIC box, enter `vNIC-B` as the name for vNIC.

k. Select the Use vNIC Template checkbox.

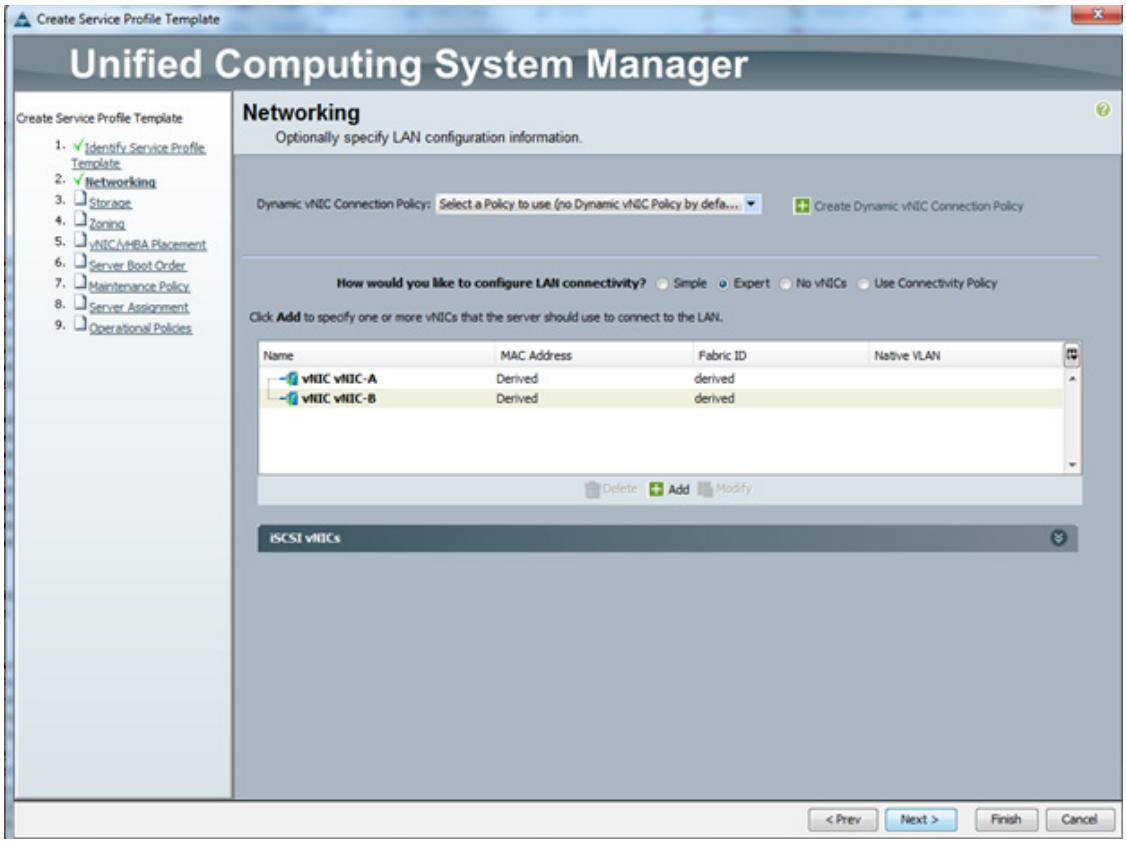
l. In the vNIC Template list, select `vNIC_Template_B`.

m. In the Adapter Policy list, select VMWare.



n. Click OK to add the vNIC to the template.

o. Review the table in the Networking page to confirm that both vNICs were created.



p. Click Next.

7. Configure the Storage options:

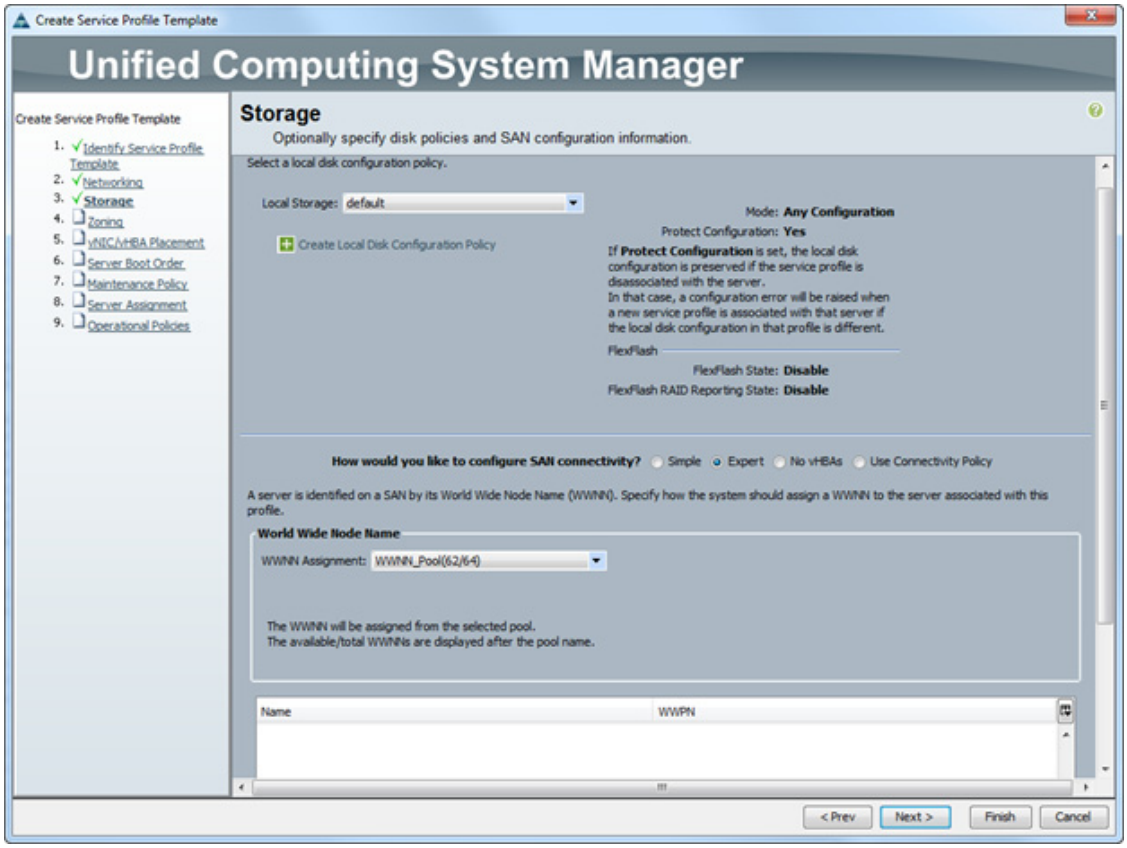
a. Select a local disk configuration policy:

– If the server in question has local disks, select default in the Local Storage list.

– If the server in question does not have local disks, select `SAN-Boot`.

b. Select the Expert option to configure the SAN connectivity.

c. In the WWNN Assignment list, select `WWNN_Pool`.



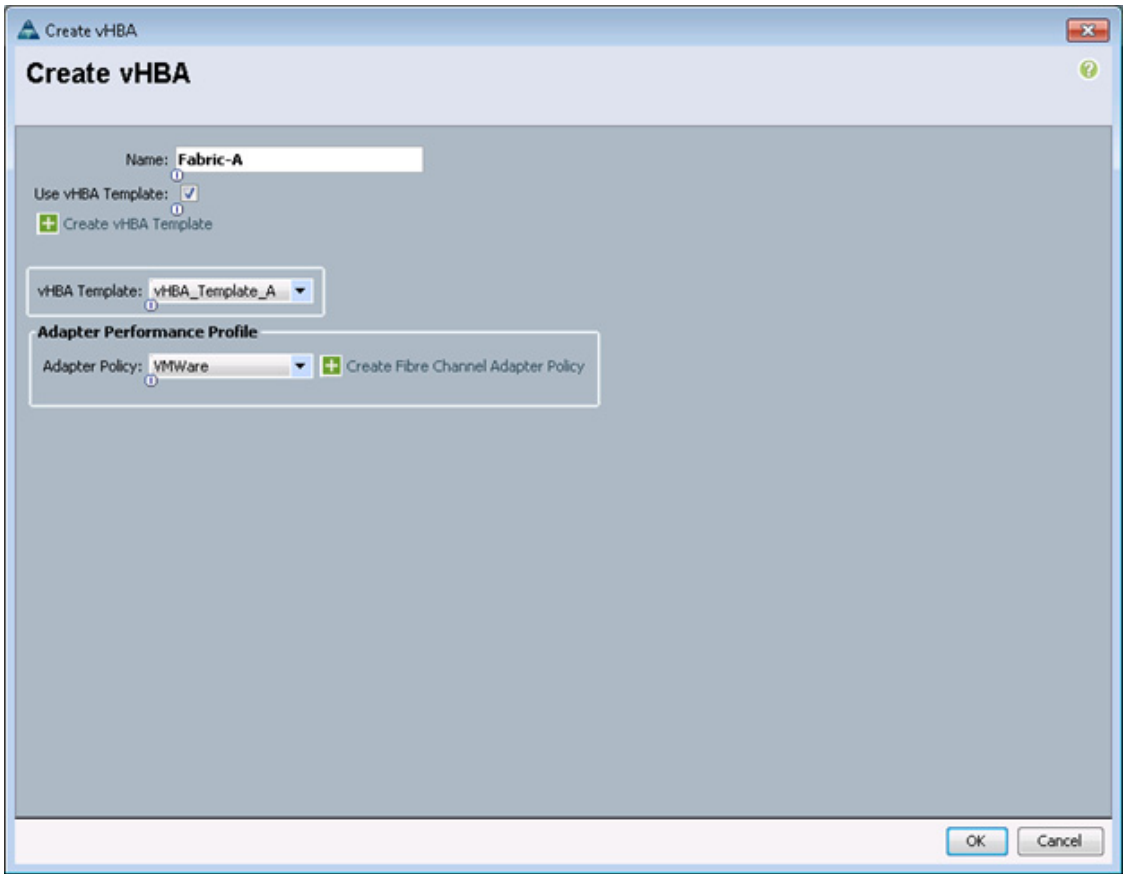
d. Click the Add button to add a vHBA to the template.

e. In the Create vHBA dialog box, enter `Fabric-A` as the name for vHBA.

f. Select the Use vHBA Template checkbox.

g. In the vHBA Template list, select `vHBA_Template_A`.

h. In the Adapter Policy list, select VMware.



i. Click OK to add this vHBA to the template.

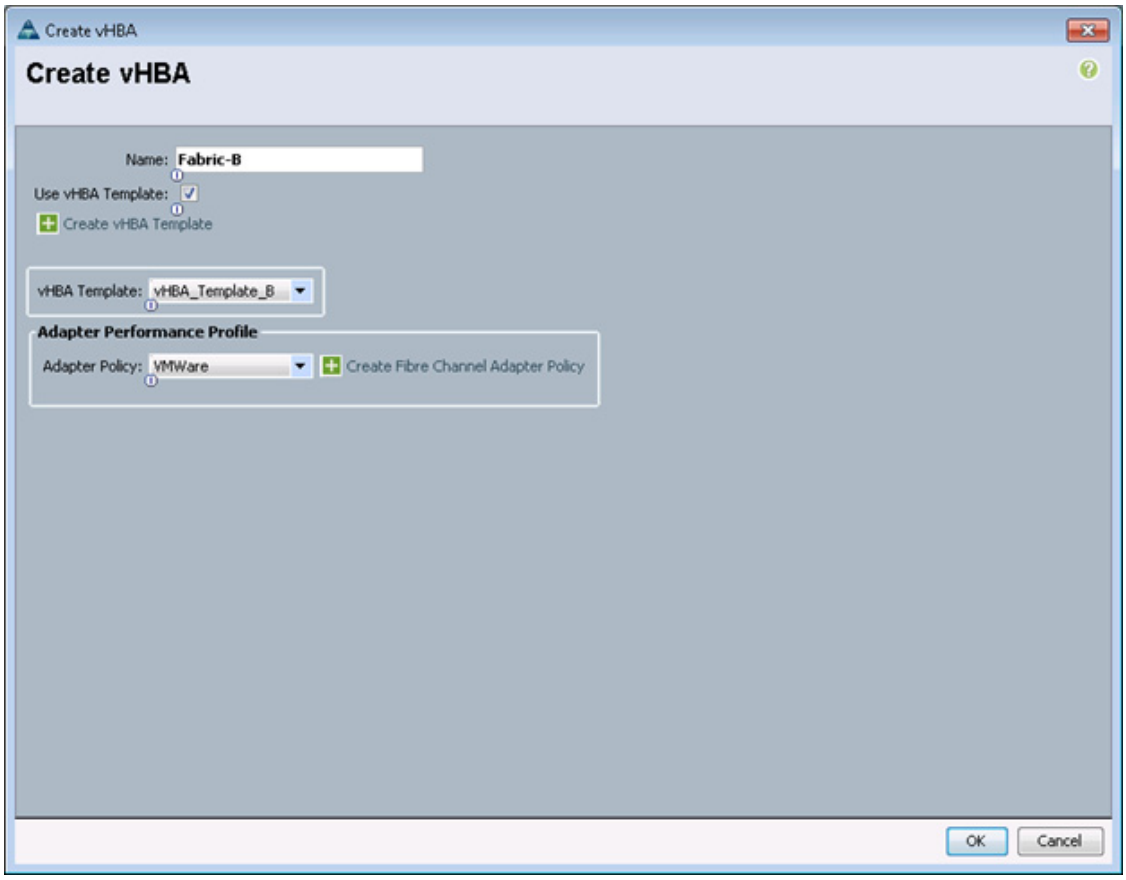
j. On the Storage page of the wizard, click Add to add another vHBA to the template.

k. In the Create vHBA dialog box, enter `Fabric-B` as the name for vHBA.

l. Select the checkbox for Use HBA Template.

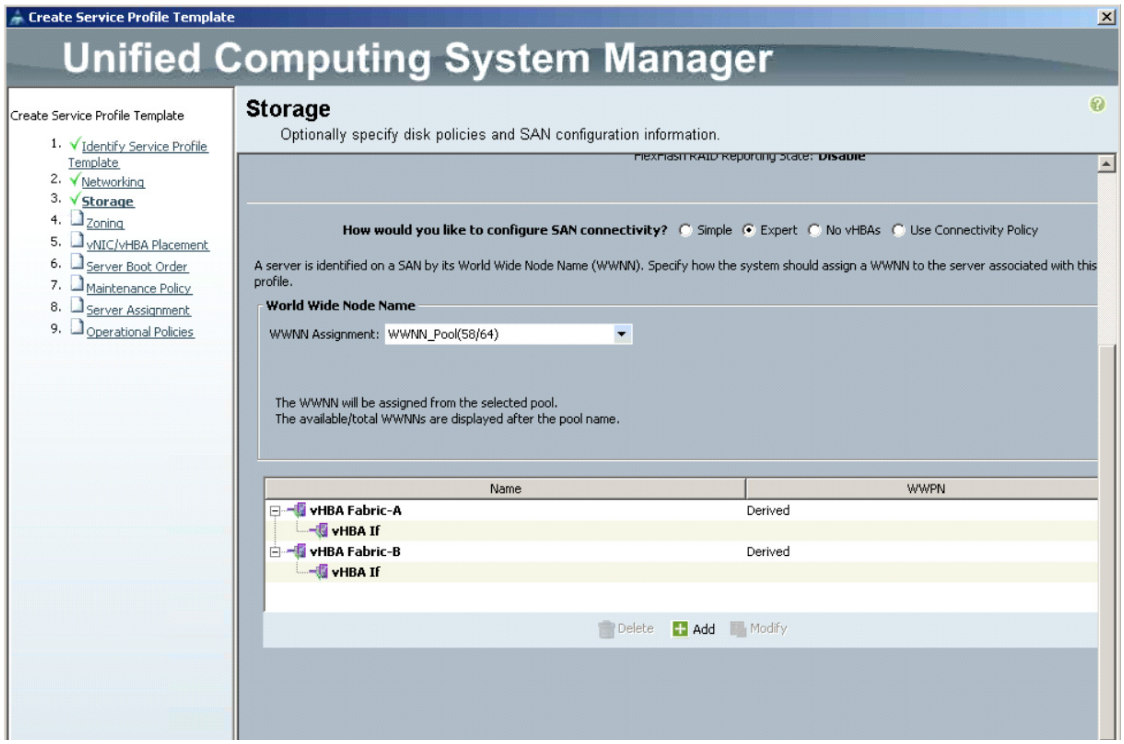
m. In the vHBA Template list, select `vHBA_Template_B`.

n. In the Adapter Policy list, select VMware.



o. Click OK to add the vHBA to the template.

p. Review the table on the Storage page to verify that both vHBAs were created.

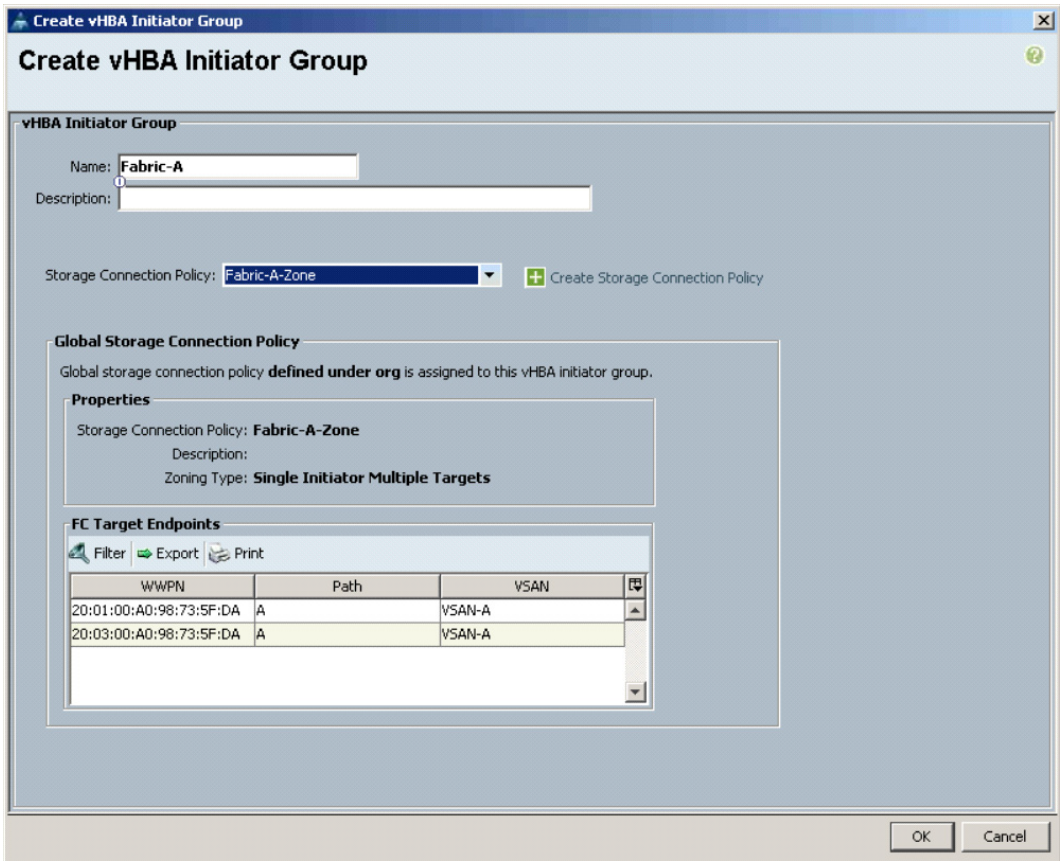


q. Click Next.

8. Set up Zoning.

a. On the Zoning selection, click the green plus sign to add a vHBA Initiator Group.

b. Name the vHBA Initiator Group Fabric-A and select the Fabric-A-Zone Storage Connection Policy.



c. Click OK to add the vHBA Initiator Group.

d. Select the Fabric-A vHBA Initiator and the Fabric-A vHBA Initiator Group and click Add To to add the initiator to the Initiator Group.

e. On the Zoning selection, click the green plus sign to add a vHBA Initiator Group.

f. Name the vHBA Initiator Group Fabric-B and select the Fabric-B-Zone Storage Connection Policy.

g. Click OK to add the vHBA Initiator Group.

h. Select the Fabric-B vHBA Initiator and the Fabric-B vHBA Initiator Group and click Add To to add the initiator to the Initiator Group.

i. Click Next to continue

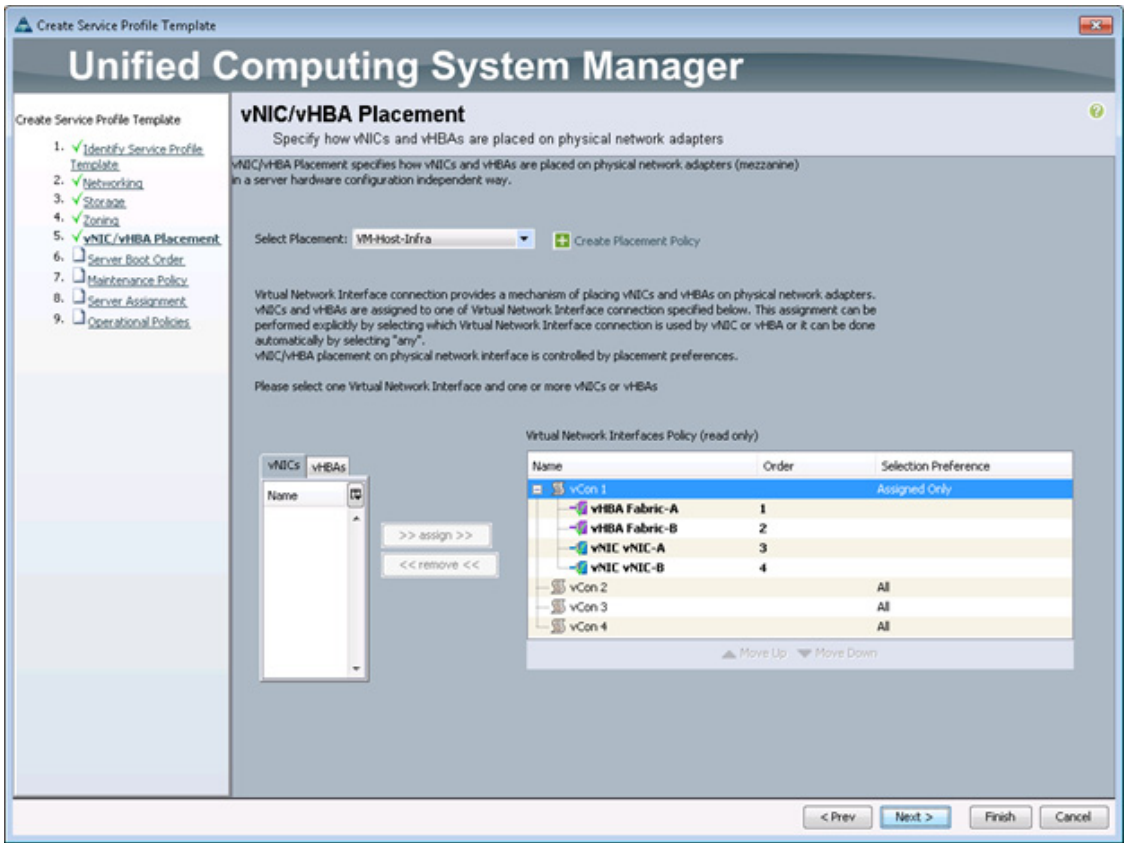
9. Set the vNIC/vHBA placement options.

a. In the Select Placement list, select the `VM-Host-Infra` placement policy.

b. Select `vCon1` and assign the vHBAs/vNICs to the virtual network interfaces policy in the following order:

- `vHBA Fabric-A`
- `vHBA Fabric-B`
- `vNIC-A`
- `vNIC-B`

c. Review the table to verify that all of the vNICs and vHBAs were assigned to the policy in the appropriate order.



d. Click Next.

10. Set the Server Boot Order:

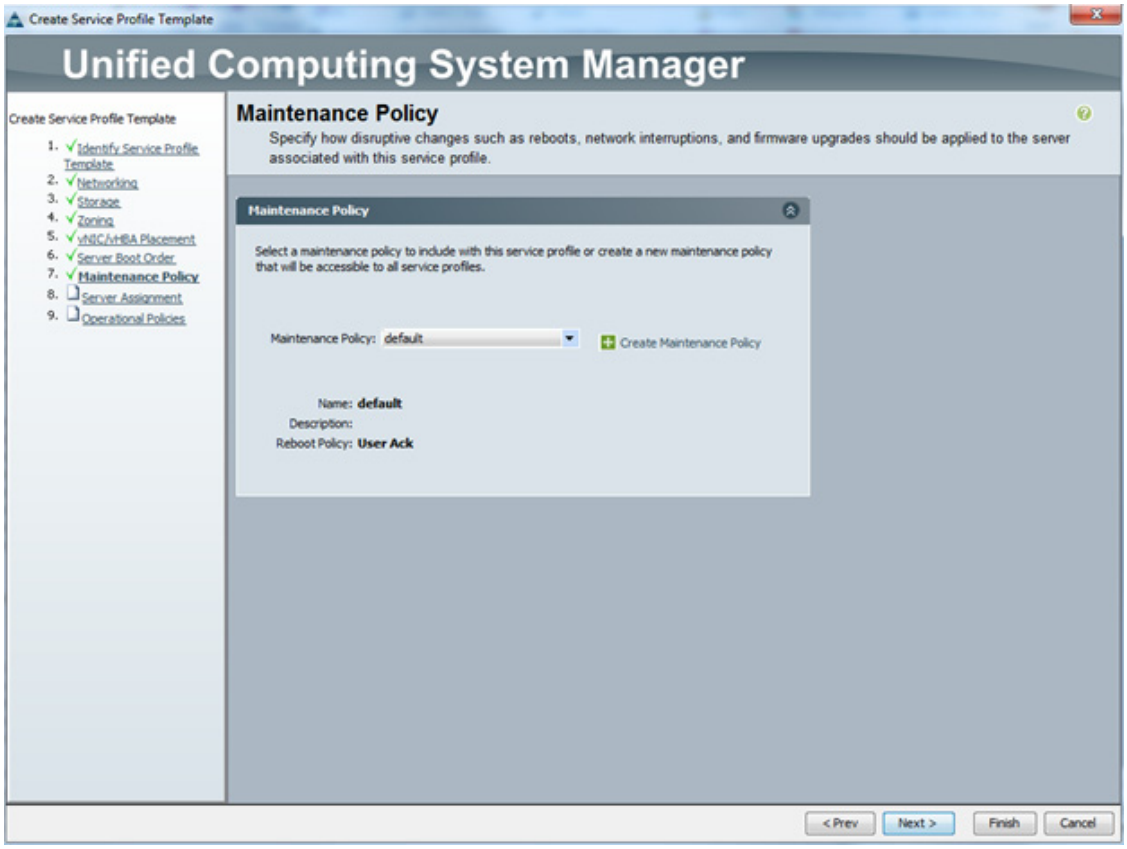
a. In the Boot Policy list, select `Boot-Fabric-A`.

b. Review the table to verify that all of the boot devices were created and identified. Verify that the boot devices are in the correct boot sequence.

c. Click Next.

11. Add a Maintenance Policy:

a. Confirm that maintenance policy is set to default.



b. Click Next.

12. Specify the Server Assignment:

a. In the Pool Assignment list, select `Infra_Pool`.

b. Optional: Select a Server Pool Qualification policy.

c. Select Down as the power state to be applied when the profile is associated with the server.

d. Expand Firmware Management and select `VM-Host-Infra` from the Host Firmware list.

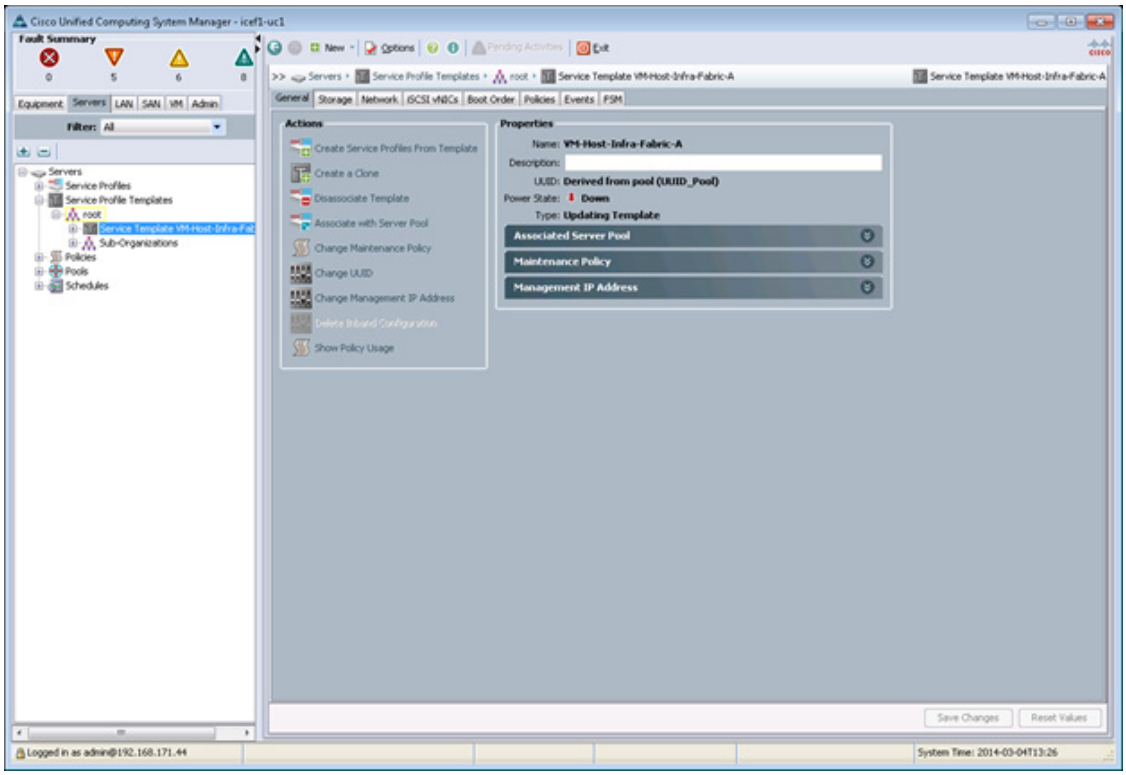
e. Click Next.

13. Add Operational Policies:

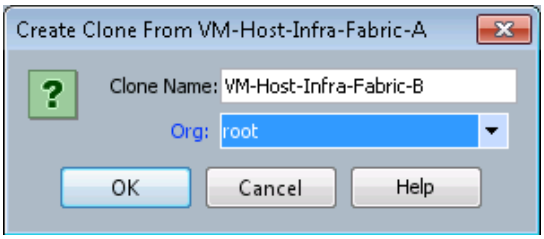
a. In the BIOS Policy list, select `VM-Host-Infra`.

b. Expand Power Control Policy Configuration and select `No-Power-Cap` in the Power Control Policy list.

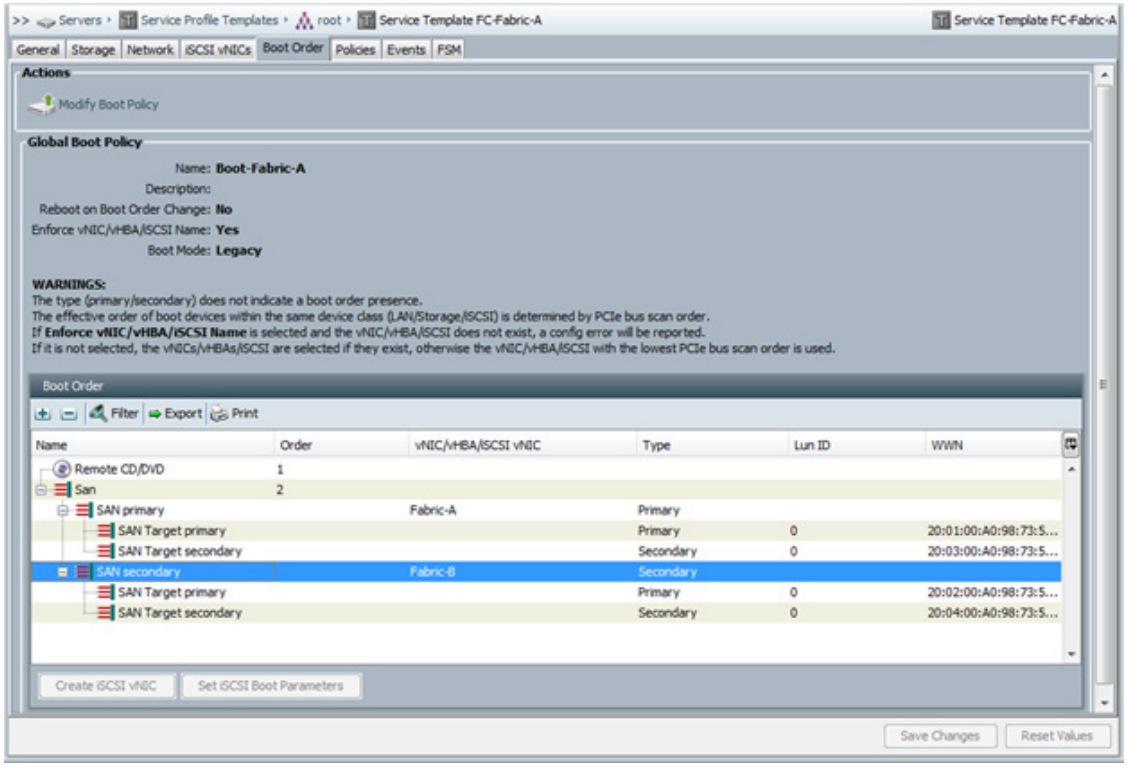
14. Click Finish to create the service profile template.
15. Click OK in the confirmation message.
16. Click the Servers tab in the navigation pane.
17. Select Service Profile Templates > root.



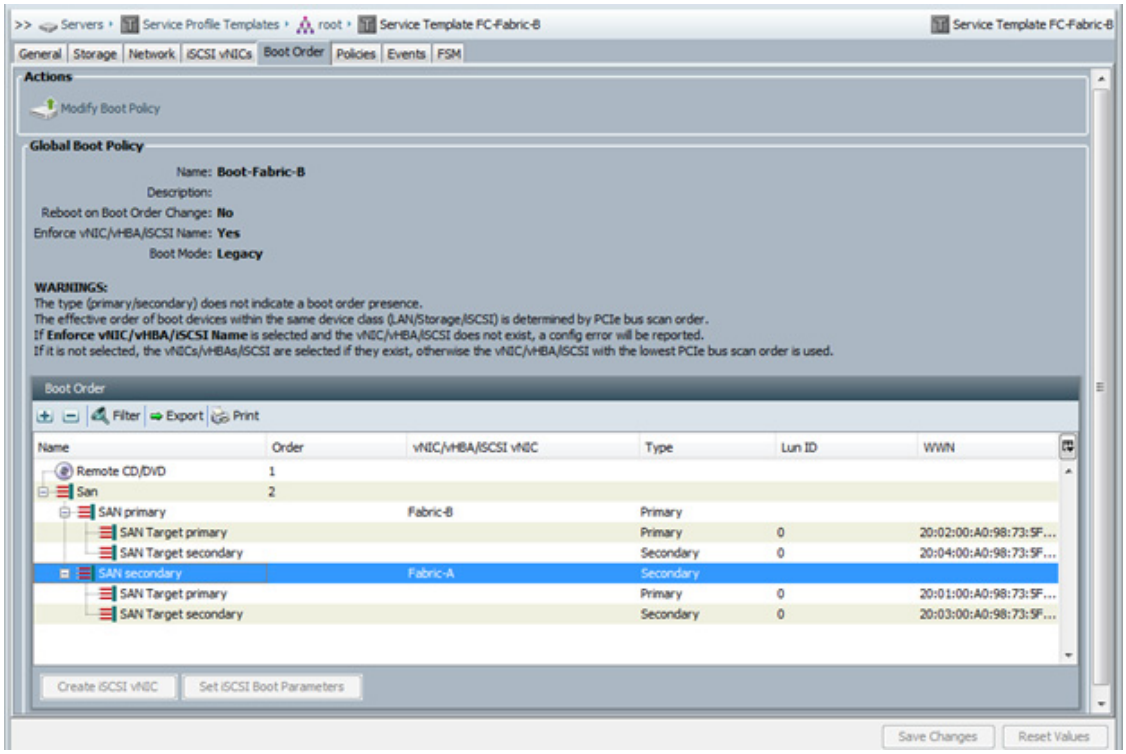
18. Right-click the previously created `VM-Host-Infra-Fabric-A` template.
19. Select Create a Clone.
20. In the dialog box, enter `VM-Host-Infra-Fabric-B` as the name for clone, select the root Org, and click OK.



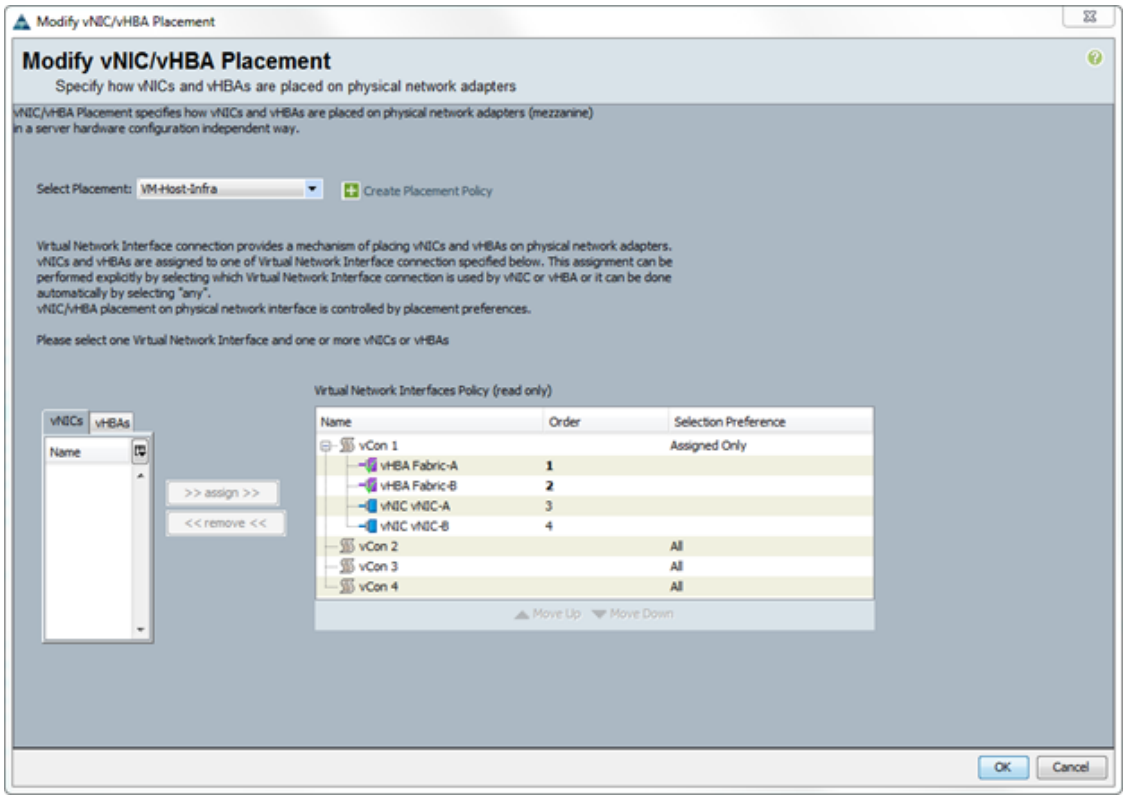
21. Click OK.
22. Select the newly cloned service profile template and click the Boot Order tab.



23. Click Modify Boot Policy.
24. In the Boot Policy list, select `Boot-Fabric-B`.



25. Click OK, and then click OK again to close the confirmation window.
26. In the right pane, click the Network tab, and then click Modify vNIC/HBA Placement.
27. Expand `vCon 1` and move `vHBA Fabric-B` ahead of `vHBA Fabric-A` in the placement order.

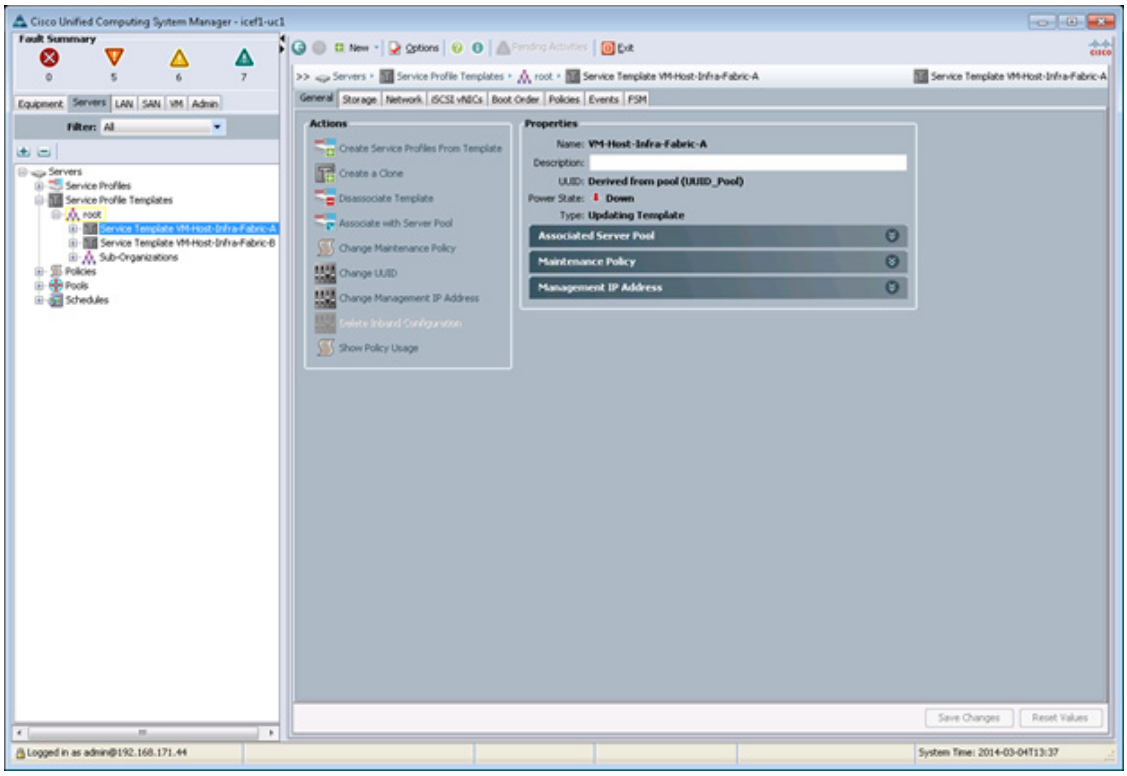


28. Click OK and then click OK again.

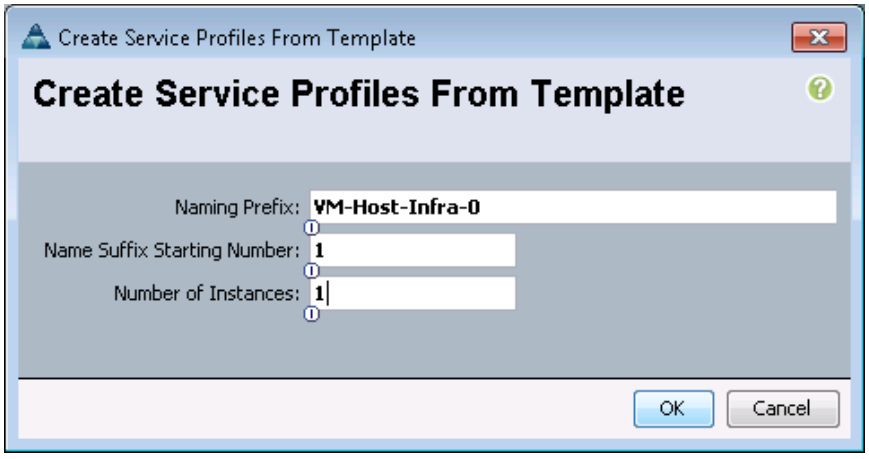
Create Service Profiles

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

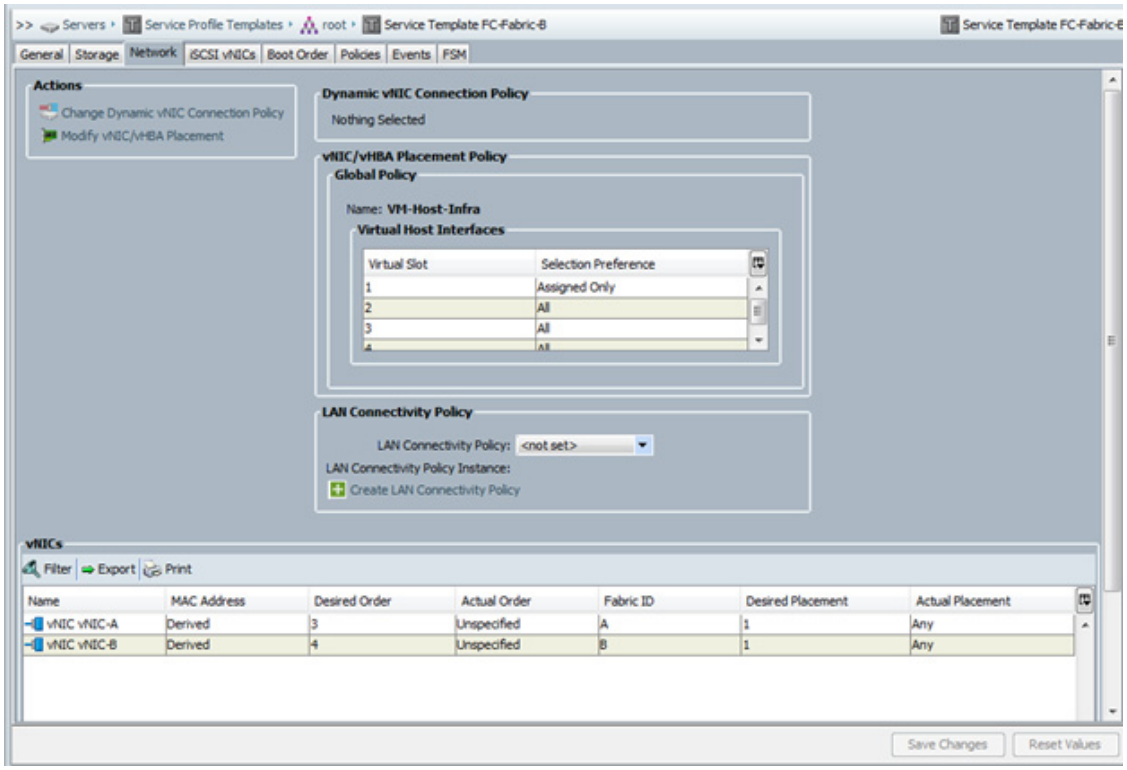
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select `Service Profile Templates > root > Service Template VM-Host-Infra-Fabric-A`.



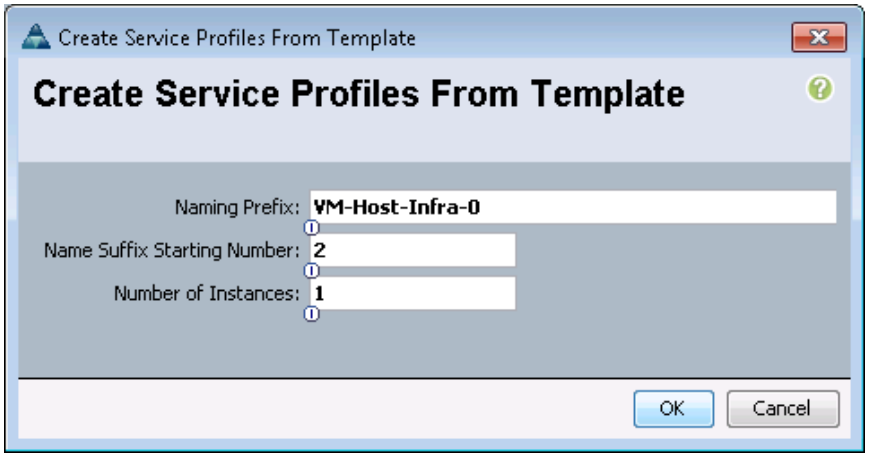
3. Right-click `VM-Host-Infra-Fabric-A` and select Create Service Profiles from Template.
4. Enter `VM-Host-Infra-0` as the Naming Prefix.
5. Enter 1 as the Suffix Starting Number.
6. Enter `1` as the Number of Instances to create.



7. Click OK to create the service profile.
8. Click OK in the confirmation message.
9. Select `Service Profile Templates > root > Service Template VM-Host-Infra-Fabric-B`.



10. Right-click `VM-Host-Infra-Fabric-B` and select Create Service Profiles from Template.
11. Enter `VM-Host-Infra-0` as the Naming Prefix.
12. Enter 2 as the Suffix Starting Number.
13. Enter `1` as the Number of Instances to create.



14. Click OK to create the service profile.
15. In the confirmation message, click OK.
16. Verify that the service profiles `VM-Host-Infra-01` and `VM-Host-Infra-02` have been created. The service profiles are automatically associated with the servers in their assigned server pools.

17. Optional: Select each newly created service profile and enter the server host name or the FQDN in the User Label field in the General tab. Click Save Changes to map the server host name to the service profile name.

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 blade in the environment will have a unique configuration. To proceed with the FlexPod deployment, specific information must be gathered from each Cisco UCS blade and from the NetApp controllers. Insert the required information into Table 23 and Table 24.

Table 23 FCP LIFs for FC WWPNs

FCP LIFs	FC WWPN
fcp_lif01a	
fcp_lif01b	
fcp_lif02a	
fcp_lif02b	

Note To gather the FC WWPN, log in to the storage cluster and run the `network interface show` command.

Table 24 vHBA WWPNs for Fabric A and Fabric B

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

Note To gather the vHBA WWPN information, launch the Cisco UCS Manager GUI. In the navigation pane, click the Servers tab. Expand Servers > Service Profiles > root. Click each service profile then click the Storage tab in the right pane and then click the vHBAs tab. In Table 24, record the WWPN information that is displayed in the right pane for both vHBA Fabric-A and vHBA Fabric-B for each service profile.

Storage Networking

FlexPod Cisco Nexus Base

The following procedures describe how to configure the Cisco Nexus switches for use in a base FlexPod environment.

Set Up Initial Configuration

Cisco Nexus 9372PX A

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

1. Configure the switch.

Note 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": <<var_password>>
Confirm the password for "admin": <<var_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: <<var_nexus_A_hostname>>
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:
Enter
Mgmt0 IPv4 address: <<var_nexus_A_mgmt0_ip>>
Mgmt0 IPv4 netmask: <<var_nexus_A_mgmt0_netmask>>
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway: <<var_nexus_A_mgmt0_gw>>
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
   Number of rsa key bits <1024-2048> : 1024
  Configure the ntp server? (yes/no) [n]: y
  NTP server IPv4 address: <<var_global_ntp_server_ip>>
  Enter basic FC configurations (yes/no) [n]: 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 <<var_nexus_B_hostname>>, complete the following steps:

1. Configure the switch.

Note 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": <<var_password>>
Confirm the password for "admin": <<var_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: <<var_nexus_B_hostname>>
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:
Enter
Mgmt0 IPv4 address: <<var_nexus_B_mgmt0_ip>>
Mgmt0 IPv4 netmask: <<var_nexus_B_mgmt0_netmask>>
Configure the default gateway? (yes/no) [y]: Enter
IPv4 address of the default gateway: <<var_nexus_B_mgmt0_gw>>
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
   Number of rsa key bits <1024-2048> : 1024
  Configure the ntp server? (yes/no) [n]: y
  NTP server IPv4 address: <<var_global_ntp_server_ip>>
  Enter basic FC configurations (yes/no) [n]: 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 FCoE Storage vSphere on Clustered Data ONTAP

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 lacp
feature vpc
feature interface-vlan
```

```
feature lldp
```

Set Global Configurations

Cisco Nexus 9372PX A and Cisco Nexus 9372PX B

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

1. Run the following commands to set global configurations and jumbo frames in QoS:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
port-channel load-balance ethernet source-dest-port
policy-map type network-qos jumbo
class type network-qos class-default
mtu 9216
exit
exit
system qos
service-policy type network-qos jumbo
exit
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 the switches:

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

```
vlan <<var_ib-mgmt_vlan_id>>
name IB-MGMT-VLAN
exit
vlan <<var_native_vlan_id>>
name Native-VLAN
exit
vlan <<var_vmotion_vlan_id>>
name vMotion-VLAN
exit
vlan <<var_vm-traffic_vlan_id>>
name VM-Traffic-VLAN
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:

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

```
interface Eth1/1
description <<var_node01>>:e0a
```

```
interface Eth1/3
description <<var_ucs_clustername>>-A:1/1
exit
interface Eth1/4
description <<var_ucs_clustername>>-B:1/1
exit
interface Eth1/13
description <<var_nexus_B_hostname>>:1/13
exit
interface Eth1/14
description <<var_nexus_B_hostname>>:1/14
exit
interface eth1/19
description <<Mgmt-Switch>>:1/24
exit
```

Cisco Nexus 9372PX B

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

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

```
interface Eth1/3
description <<var_ucs_clustername>>-A:1/2
exit
interface Eth1/4
description <<var_ucs_clustername>>-B:1/2
exit
interface Eth1/13
description <<var_nexus_A_hostname>>:1/13
exit
interface Eth1/14
description <<var_nexus_A_hostname>>:1/14
exit
interface eth1/19
description <<Mgmt-Switch>>:1/31
exit
```

Create Port Profiles

Cisco Nexus 9372PX A and Cisco Nexus 93972PX B

Port profiles are used to simplify ongoing network administration and configuration. Ports with similar configurations can be grouped within port profiles. Configuration changes can then be made to the port profile and will be applied to all port members of the port profile. FlexPod recommends port profiles for the following port types:

- FAS uplink ports
- Cisco UCS Ethernet ports
- Cisco Nexus VPC ports

To create the Ethernet traffic port profiles, complete the following step on both the switches:

1. From the Global configuration mode, run the following commands

```
port-profile type port-channel UCS-Ethernet
  switchport mode trunk
```

```
  switchport trunk native vlan 2
  switchport trunk allowed vlan <<var_vmotion_vlan_id>>,
<<var_vm-traffic_vlan_id>>, <<var_ib-mgmt_vlan_id>>
  spanning-tree port type edge trunk
  state enabled
port-profile type port-channel vPC-Peer-Link
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>,
<<var_pkt-ctrl_vlan_id>>, <<var_vmotion_vlan_id>>,
<<var_vm-traffic_vlan_id>>
  spanning-tree port type network
  state enabled
  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 the switches:

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

```
interface Po10
description vPC peer-link
exit
interface Eth1/13-14
channel-group 10 mode active
no shutdown
exit
interface Po13
description <<var_ucs_clustername>>-A
exit
interface Eth1/1
channel-group 13 mode active
no shutdown
exit
interface Po14
description <<ucs_cluternname>>-B
exit
interface Eth1/2
channel-group 14 mode active
no shutdown
exit
copy run start
```

Add Port Profiles to Port Channels

Port channels and their member ports inherit their configuration from the previously configured Port Profiles.

Cisco Nexus 9372PX A and Cisco Nexus 9372PX B

To assign Port Profiles to the appropriate port channels complete the following step on both the switches:

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

```
interface Po10
inherit port-profile vPC-Peer-Link
exit
interface Po13
inherit port-profile UCS-Ethernet
exit
interface Po14
inherit port-profile UCS-Ethernet
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:

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

```
vpc domain <<var_nexus_vpc_domain_id>>
role priority 10
peer-keepalive destination <<var_nexus_B_mgmt0_ip>> source
<<var_nexus_A_mgmt0_ip>>
auto-recovery
exit
interface Po10
vpc peer-link
exit
interface Po13
vpc 13
exit
interface Po14
vpc 14
exit
copy run start
```

Cisco Nexus 9372PX B

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

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

```
vpc domain <<var_nexus_vpc_domain_id>>
role priority 20
peer-keepalive destination <<var_nexus_A_mgmt0_ip>> source
<<var_nexus_B_mgmt0_ip>>
auto-recovery
exit
interface Po10
vpc peer-link
exit
interface Po11
vpc 11
exit
interface Po12
vpc 12
```

```
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 Networking

Clustered Data ONTAP SAN Boot Storage Setup

Create Igroups

To create igroups, complete the following step:

1. From the cluster management node SSH connection, run the following commands:

```
igroup create –vserver Infra_Vserver –igroup VM-Host-Infra-01 –protocol fcp
–ostype vmware –initiator <<var_vm_host_infra_01_A_wwpn>>,
<<var_vm_host_infra_01_B_wwpn>>
igroup create –vserver Infra_Vserver –igroup VM-Host-Infra-02 –protocol fcp
–ostype vmware –initiator <<var_vm_host_infra_02_A_wwpn>>,
<<var_vm_host_infra_02_B_wwpn>>
igroup create –vserver Infra_Vserver –igroup MGMT-Hosts –protocol fcp
–ostype vmware –initiator <<var_vm_host_infra_01_A_wwpn>>,
<<var_vm_host_infra_01_B_wwpn>>, <<var_vm_host_infra_02_A_wwpn>>,
<<var_vm_host_infra_02_B_wwpn>>
```

Note To view the three igroups created in this step, run the `igroup show` command.

Map Boot LUNs to Igroups

To map boot LUNs to igroups, complete the following step:

1. From the cluster management SSH connection, run the following commands:

```
lun map –vserver Infra_Vserver –volume esxi_boot –lun VM-Host-Infra-01
–igroup VM-Host-Infra-01 –lun-id 0
lun map –vserver Infra_Vserver –volume esxi_boot –lun VM-Host-Infra-02
–igroup VM-Host-Infra-02 –lun-id 0
lun map –vserver Infra_Vserver –volume infra_datastore_1 –lun
infra_datastore_1 –igroup MGMT-Hosts –lun-id 1
lun map –vserver Infra_Vserver –volume infra_swap –lun infra_swap –igroup
MGMT-Hosts –lun-id 2
```

VMware vSphere 5.5 Update 1 Setup

FlexPod VMware ESXi 5.5 Update 1 FC on Clustered Data ONTAP

This section provides detailed instructions for installing VMware ESXi 5.5 Update 1 in a FlexPod environment. After the procedures are completed, two FCP-booted ESXi hosts will be provisioned. These deployment procedures are customized to include the environment variables.

Note 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 Fibre Channel Protocol (FCP) boot logical unit numbers (LUNs).

Download Cisco Custom Image for ESXi 5.5.0 U1

1. Click the following link vmware login page.
2. Type your email or customer number and the password and then click Log in.
3. Click on the following link CiscoCustomImage5.5.0U1.
4. Click Download.
5. Save it to your destination folder.

Log in to Cisco UCS 6324 Fabric Interconnect

Cisco UCS Manager

The 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. To download the Cisco UCS Manager software, click the Launch UCS Manager link.
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 the Servers tab.
7. Select Servers > Service Profiles > root > `VM-Host-Infra-01`.
8. Right-click `VM-Host-Infra-01` and select KVM Console.
9. If prompted to accept an Unencrypted KVM session, accept as necessary.
10. Select Servers > Service Profiles > root > `VM-Host-Infra-02`.
11. Right-click `VM-Host-Infra-02` and select KVM Console.
12. If prompted to accept an Unencrypted KVM session, accept as necessary.

Set Up VMware ESXi Installation

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

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

1. In the KVM window, click the Virtual Media node.
2. If prompted to accept an Unencrypted KVM session, accept as necessary.
3. Click Add Image.
4. Browse to the ESXi installer ISO image file and click Open.
5. Select the Mapped checkbox to map the newly added image.
6. Click the KVM tab to monitor the server boot.
7. Boot the server by selecting Boot Server and clicking OK. Then click OK again.

Install ESXi

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

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

1. On reboot, the machine detects the presence of the ESXi installation media. Select the ESXi installer from the boot menu that is displayed.
2. After the installer is finished loading, press Enter to continue with the installation.
3. Read and accept the end-user license agreement (EULA). Press F11 to accept and continue.
4. Select the NetApp LUN that was previously set up as the installation disk for ESXi and press Enter to continue with the installation.
5. Select the appropriate keyboard layout and press Enter.
6. Enter and confirm the root password and press Enter.
7. The installer issues a warning that the selected disk will be repartitioned. Press F11 to continue with the installation.
8. After the installation is complete, click on the Virtual Media tab and clear the ✓ mark next to the ESXi installation media. Click Yes.

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

9. From the KVM tab, press Enter to reboot the server.

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 the Management Network option and press Enter.
4. Select the VLAN (Optional) option and press Enter.
5. Enter the `<<var_ib-mgmt_vlan_id>>` and press Enter.
6. From the Configure Management Network menu, select IP Configuration and press Enter.
7. Select the Set Static IP Address and Network Configuration option by using the space bar.
8. Enter the IP address for managing the first ESXi host: `<<var_vm_host_infra_01_ip>>`.
9. Enter the subnet mask for the first ESXi host.
10. Enter the default gateway for the first ESXi host.
11. Press Enter to accept the changes to the IP configuration.
12. Select the IPv6 Configuration option and press Enter.
13. Using the spacebar, unselect Enable IPv6 (restart required) and press Enter.
14. Select the DNS Configuration option and press Enter.

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

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

4. Select the VLAN (Optional) option and press Enter.
5. Enter the `<<var_ib-mgmt_vlan_id>>` and press Enter.
6. From the Configure Management Network menu, select IP Configuration and press Enter.
7. Select the Set Static IP Address and Network Configuration option by using the space bar.
8. Enter the IP address for managing the second ESXi host: `<<var_vm_host_infra_02_ip>>`.
9. Enter the subnet mask for the second ESXi host.
10. Enter the default gateway for the second ESXi host.
11. Press Enter to accept the changes to the IP configuration.
12. Select the IPv6 Configuration option and press Enter.
13. Using the spacebar, clear Enable IPv6 (restart required) and press Enter.
14. Select the DNS Configuration option and press Enter.

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

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

Download VMware vSphere Client and vSphere Remote CLI

To download the VMware vSphere Client and install Remote CLI, 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 .

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

3. Click the following link VMware vSphere CLI 5.5
4. Select your OS and Click Download.
5. Save it to destination folder.

6. Run the VMware-vSphere-CLI-5.5.0.exe.
7. Click Next.
8. Accept the terms for the license and click Next.
9. Click Next on the Destination Folder screen.
10. Click Install.
11. Click Finish.

Note Install VMware vSphere CLI 5.5 on the management workstation

Log in to VMware ESXi Hosts by Using VMware vSphere Client

ESXi Host VM-Host-Infra-01

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

1. Open the recently downloaded VMware vSphere Client and enter the IP address of `VM-Host-Infra-01` as the host you are trying to connect to: `<<var_vm_host_infra_01_ip>>`.
2. Enter `root` for the user name.
3. Enter the root password.
4. Click Login to connect.

ESXi Host VM-Host-Infra-02

To log in to the `VM-Host-Infra-02` ESXi host by using the VMware vSphere Client, complete the following steps:

1. Open the recently downloaded VMware vSphere Client and enter the IP address of `VM-Host-Infra-02` as the host you are trying to connect to: `<<var_vm_host_infra_02_ip>>`.
2. Enter `root` for the user name.
3. Enter the root password.
4. Click Login to connect.

Install VMware ESXi Patches

To install VMware ESXi patches on the ESXi host VM-Host-Infra-01 and VM-Host-Infra-02, complete the following steps:

1. Download the following VMware ESXi patches to the Management workstation:
   - EP 02 - Express Patch 02
   - EP 04 - Express Patch 04

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

1. From each vSphere Client, select the host in the inventory.

2. Click the Summary tab to view the environment summary.
3. From Resources > Storage, right-click `datastore1` and select Browse Datastore.
4. Click the fourth button and select Upload File.
5. Navigate to the saved location for the downloaded patches and select `ESXi550-201404001.zip`.
6. Click Open to upload the file to datastore1.
7. Click the fourth button and select Upload File.
8. Navigate to the saved location for the downloaded patches and select `ESXi550-201406001.zip`.
9. Click Open to upload the file to datastore1.
10. Right click on the ESXi host and select Enter Maintenance Mode, Click Yes.
11. From the management workstation, open the VMware vSphere Remote CLI that was previously installed.
12. At the command prompt, run the following commands to account for each host

```
esxcli –s <<var_vm_host_infra_01_ip>> -u root –p <<var_password>> software
vib update -d /vmfs/volumes/datastore1/ESXi550-201404001.zip
esxcli –s <<var_vm_host_infra_02_ip>> -u root –p <<var_password>> software
vib update -d /vmfs/volumes/datastore1/ESXi550-201404001.zip
esxcli –s <<var_vm_host_infra_01_ip>> -u root –p <<var_password>> software
vib update -d /vmfs/volumes/datastore1/ESXi550-201406001.zip
esxcli –s <<var_vm_host_infra_02_ip>> -u root –p <<var_password>> software
vib update -d /vmfs/volumes/datastore1/ESXi550-201406001.zip
```

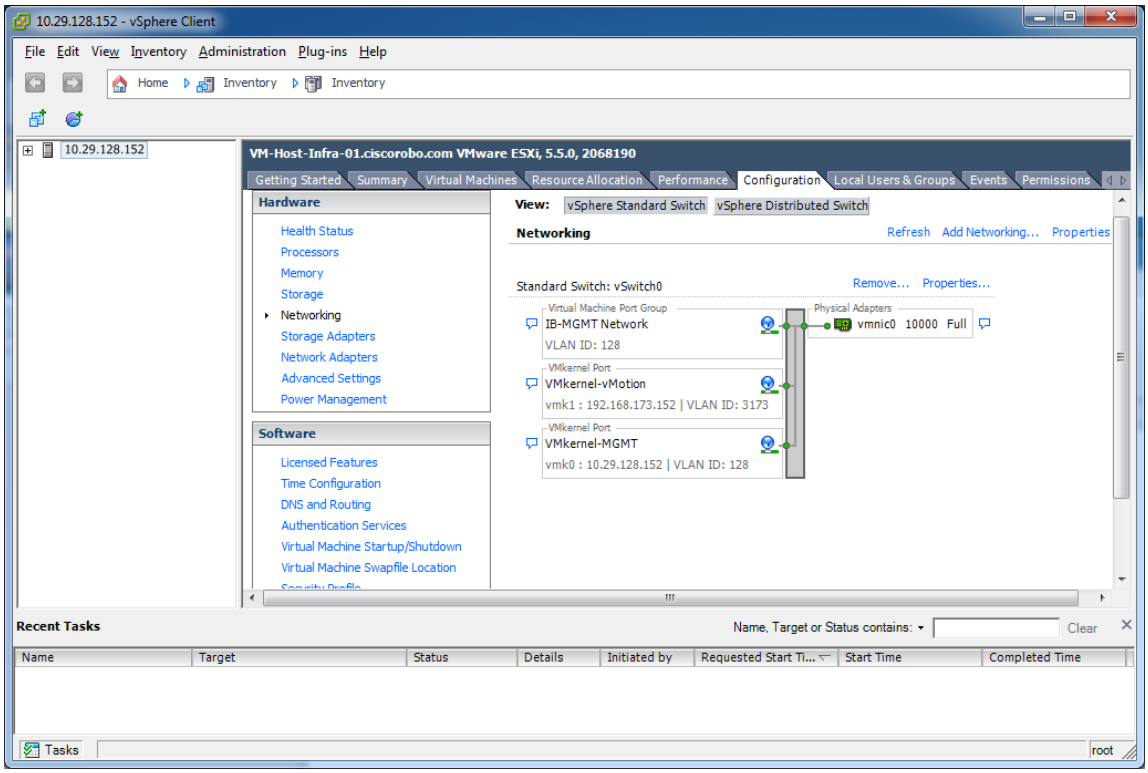
Set Up VMkernel Ports and Virtual Switch

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 vSphere Client, select the host in the inventory.
2. Click the Configuration tab.
3. In the Hardware pane, click Networking.
4. On the right side of `vSwitch0`, click Properties.
5. Select the vSwitch configuration and click Edit.
6. From the General tab, change the MTU to `9000`.
7. Click OK to close the properties for `vSwitch0`.
8. Select the Management Network configuration and click Edit.
9. Change the network label to `VMkernel-MGMT` and select the Management Traffic checkbox.
10. Click OK to finalize the edits for Management Network.
11. Select the VM Network configuration and click Edit.
12. Change the network label to `IB-MGMT Network` and enter `<<var_ib-mgmt_vlan_id>>` in the VLAN ID (Optional) field.
13. Click OK to finalize the edits for VM Network.

14. Click Add to add a network element.
15. Select VMkernel and click Next.
16. Change the network label to `VMkernel-vMotion` and enter `<<var_vmotion_vlan_id>>` in the VLAN ID (Optional) field.
17. Select the Use This Port Group for vMotion checkbox.
18. Click Next to continue with the vMotion VMkernel creation.
19. Enter the IP address `<<var_vmotion_vlan_id_ip_host-01>>` and the subnet mask `<<var_vmotion_vlan_id_mask_host-01>>` for the vMotion VLAN interface for `VM-Host-Infra-01`.
20. Click Next to continue with the vMotion VMkernel creation.
21. Click Finish to finalize the creation of the vMotion VMkernel interface.
22. Select the VMkernel-vMotion configuration and click Edit.
23. Change the MTU to `9000`.
24. To finalize the edits for the VMkernel-vMotion network, click OK.
25. To finalize the ESXi host networking setup, close the dialog box. The networking for the ESXi host should be similar to the following example:

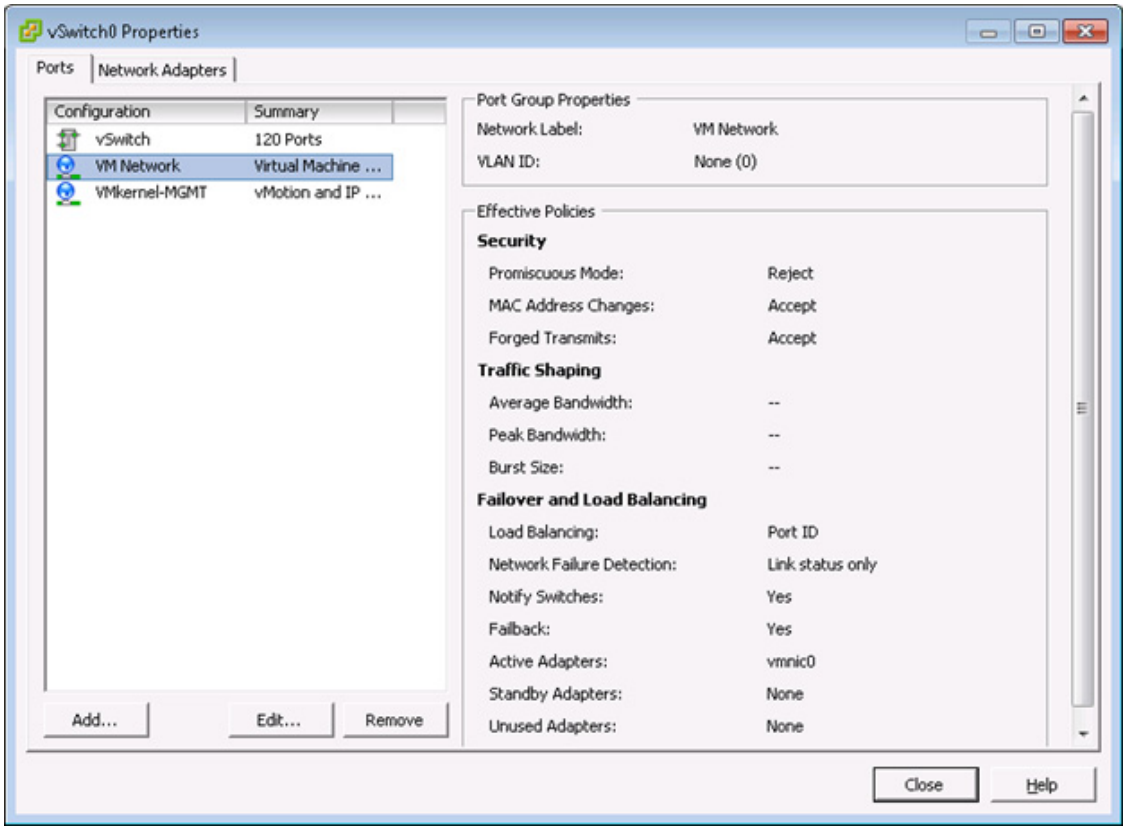


ESXi Host VM-Host-Infra-02

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

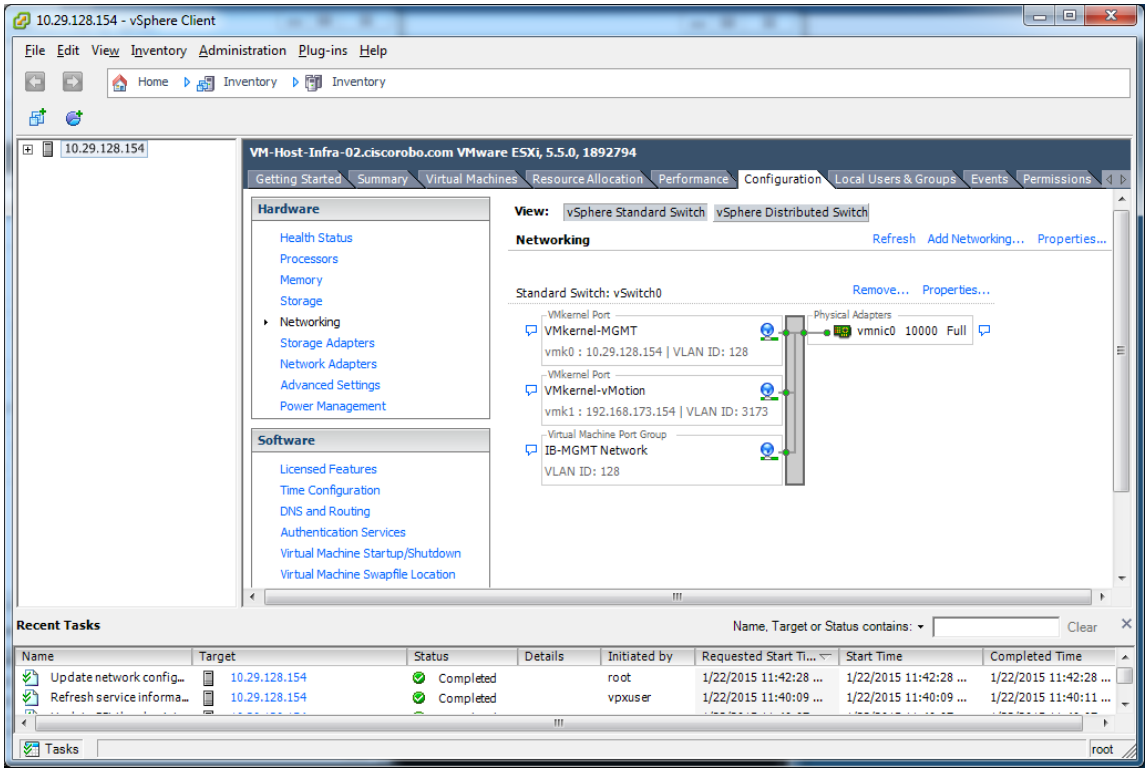
1. From the vSphere Client, select the host in the inventory.

2. Click the Configuration tab.
3. Click Networking in the Hardware pane.
4. Click Properties on the right side of `vSwitch0`.
5. Select the vSwitch configuration and click Edit.
6. From the General tab, change the MTU to `9000`.
7. To close the properties for `vSwitch0`, click OK.
8. Select the Management Network configuration and click Edit.
9. Change the network label to `VMkernel-MGMT` and select the Management Traffic checkbox.
10. To finalize the edits for the Management Network, click OK.



11. Select the VM Network configuration and click Edit.
12. Change the network label to `IB-MGMT Network` and enter `<<var_ib-mgmt_vlan_id>>` in the VLAN ID (Optional) field.
13. To finalize the edits for the VM Network, click OK.
14. To add a network element, click Add.
15. Select VMkernel and click Next.
16. To add a network element, click Add.
17. Select VMkernel and click Next.
18. Change the network label to `VMkernel-vMotion` and enter `<<var_vmotion_vlan_id>>` in the VLAN ID (Optional) field.

19. Select the Use This Port Group for vMotion checkbox.
20. To continue with the vMotion VMkernel creation, click Next.
21. Enter the IP address `<<var_vmotion_vlan_id_ip_host-02>>` and the subnet mask `<<var_vmotion_vlan_id_mask_host-02>>` for the vMotion VLAN interface for `VM-Host-Infra-02`.
22. To continue with the vMotion VMkernel creation, click Next.
23. To finalize the creation of the vMotion VMkernel interface, click Finish.
24. Select the VMkernel-vMotion configuration and click Edit.
25. Change the MTU to `9000`.
26. To finalize the edits for the VMkernel-vMotion network, click OK.
27. To finalize the ESXi host networking setup, close the dialog box. The networking for the ESXi host should be similar to the following example:

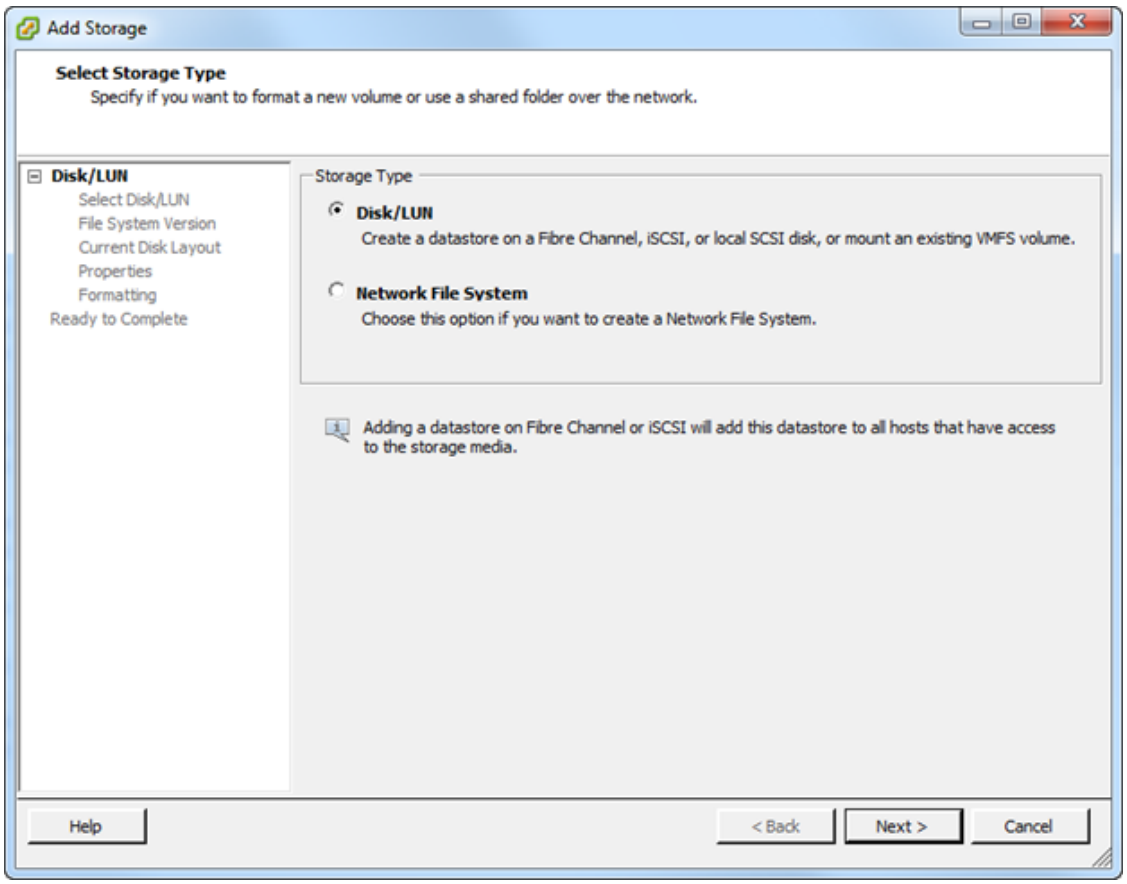


Mount Required Datastores

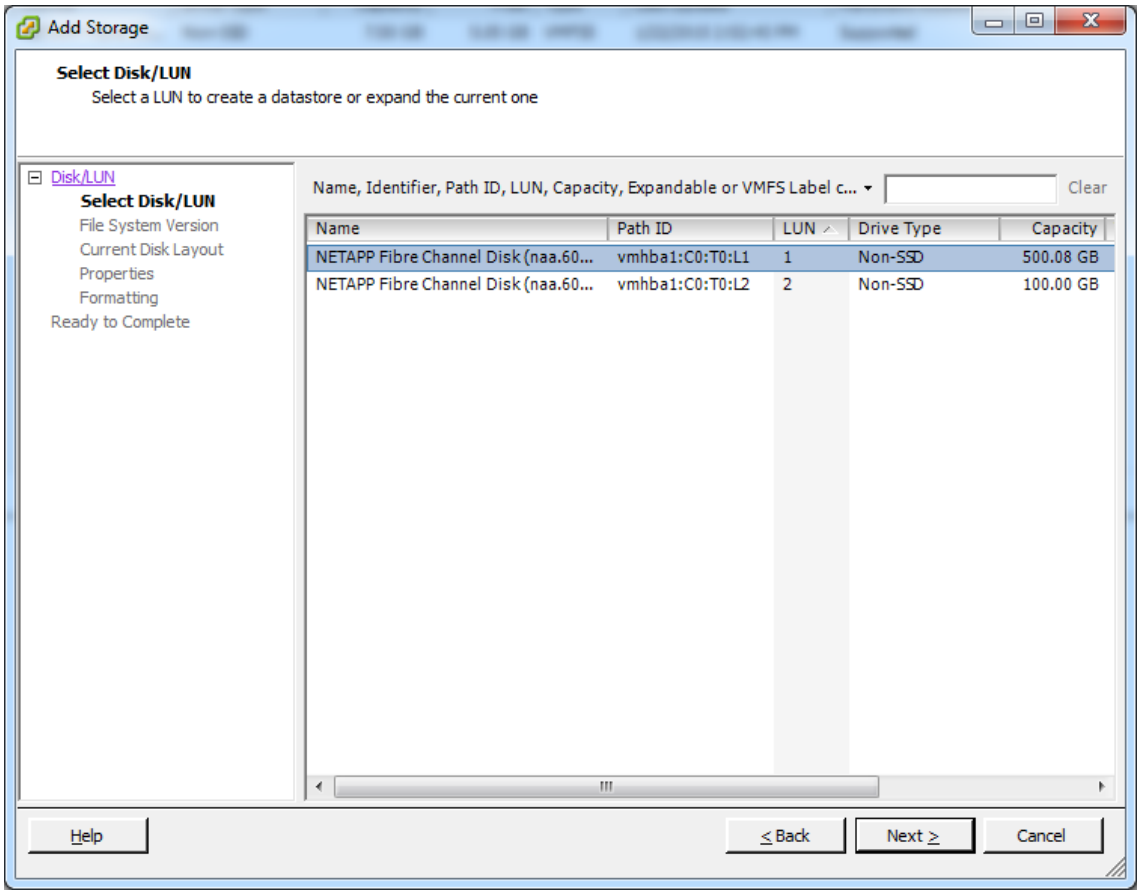
ESXi Hosts VM-Host-Infra-01 and VM-Host-Infra-02

To mount the required datastores, complete the following steps on each ESXi host:

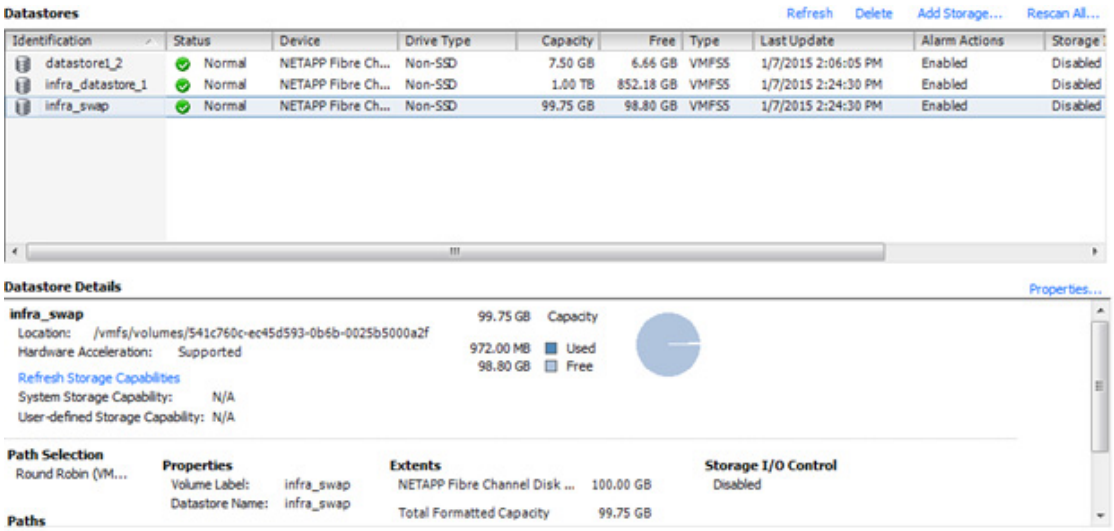
1. From the vSphere Client, select the host in the inventory.
2. To enable configurations, click the Configuration tab.
3. Click Storage in the Hardware pane.
4. From the Datastores area, click Add Storage to open the Add Storage wizard.



5. Select Disk/LUN and click Next.



6. Select LUN 1 (Capacity 500.08 GB) and click Next.
7. Select VMFS-5 and click Next.
8. Click Next.
9. Enter `infra_datastore_1` as the datastore name.Select Maximum available space and click Next.
10. To finalize the creation of the VMFS datastore, click Finish.
11. From the Datastores area, click Add Storage to open the Add Storage wizard.
12. Select Disk/LUN and click Next.
13. Select LUN 2 and click Next.
14. Select VMFS-5 and click Next.
15. Click Next.
16. Enter `infra_swap` as the datastore name.
17. Select Maximum available space and click Next.
18. To finalize the creation of the VMFS datastore, click Finish.



Note It is not necessary to add the two VMFS datastores on VM-Host-Infra-02. From the Datastores area, simply click Rescan All to add the datastores.

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:

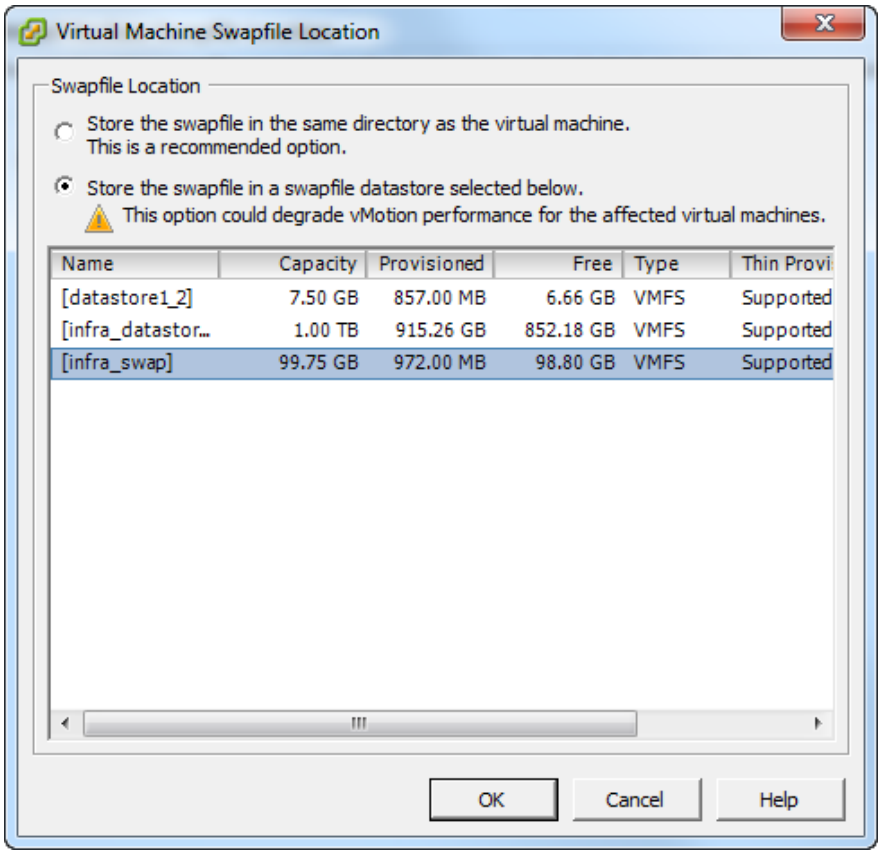
1. From the vSphere Client, select the host in the inventory.
2. To enable configurations, click the Configuration tab.
3. Click Time Configuration in the Software pane.
4. Click Properties at the upper-right side of the window.
5. At the bottom of the Time Configuration dialog box, click Options.
6. In the NTP Daemon (ntpd) Options dialog box, complete the following steps:
   a. Click General in the left pane and select Start and stop with host.
   b. Click NTP Settings in the left pane and click Add.
7. In the Add NTP Server dialog box, enter `<<var_global_ntp_server_ip>>` as the IP address of the NTP server and click OK.
8. In the NTP Daemon Options dialog box, select the Restart NTP service to apply changes checkbox and click OK.
9. In the Time Configuration dialog box, complete the following steps:
   a. Select the NTP Client Enabled checkbox and click OK.
   b. Verify that the clock is now set to approximately the correct time.
   c. The NTP server time may vary slightly from the host time.

Move VM Swap File Location

ESXi Hosts 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 vSphere Client, select the host in the inventory.
2. To enable configurations, click the Configuration tab.
3. Click Virtual Machine Swapfile Location in the Software pane.
4. Click Edit at the upper-right side of the window.
5. Select "Store the swapfile in a swapfile datastore selected below."
6. Select `[infra_swap]` as the datastore in which to house the swap files.



7. Click OK to finalize moving the swap file location.

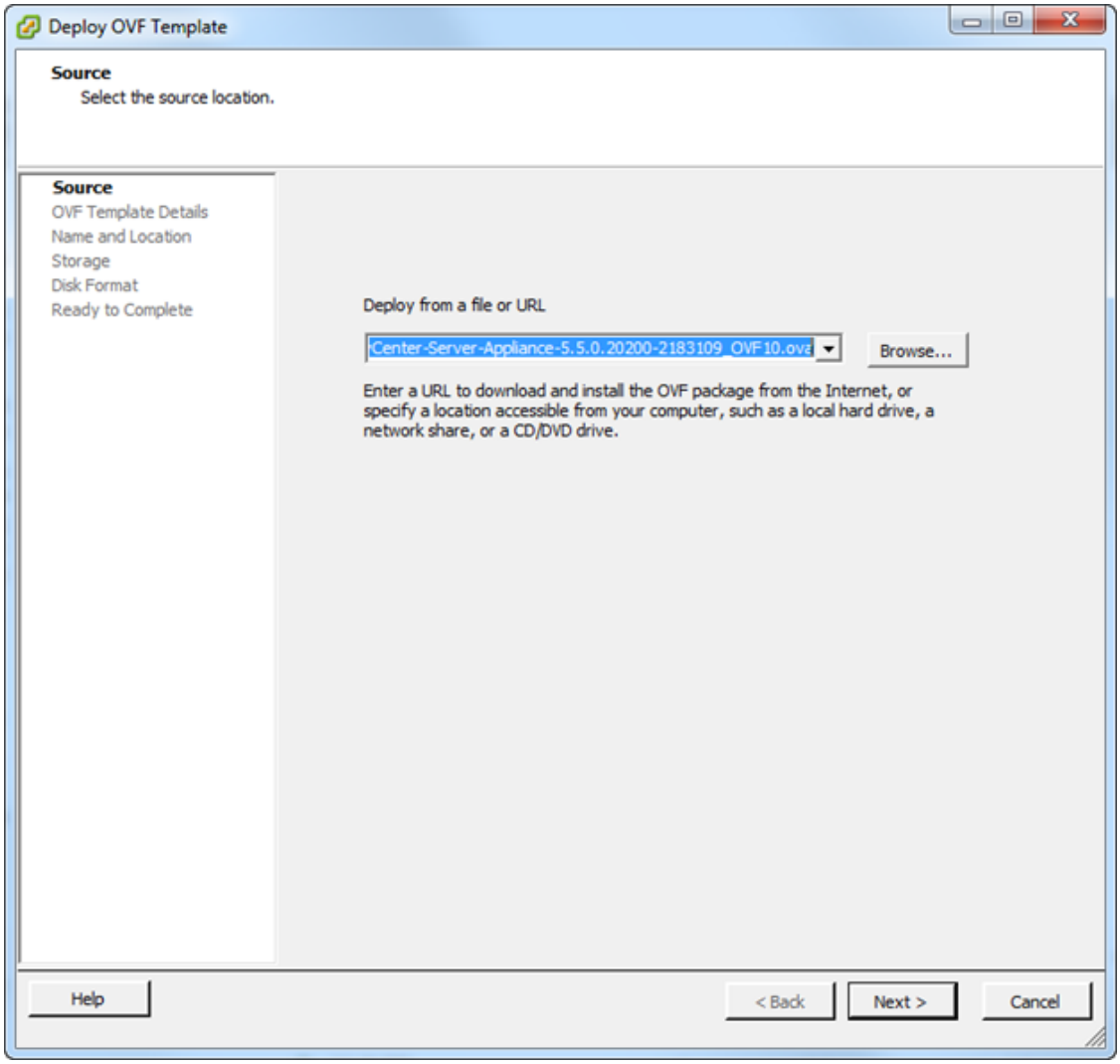
FlexPod VMware vCenter Appliance 5.5 Update 1

The procedures in the following subsections provide detailed instructions for installing VMware vCenter 5.5 Update 2 in a FlexPod environment. After the procedures are completed, a VMware vCenter Server will be configured.

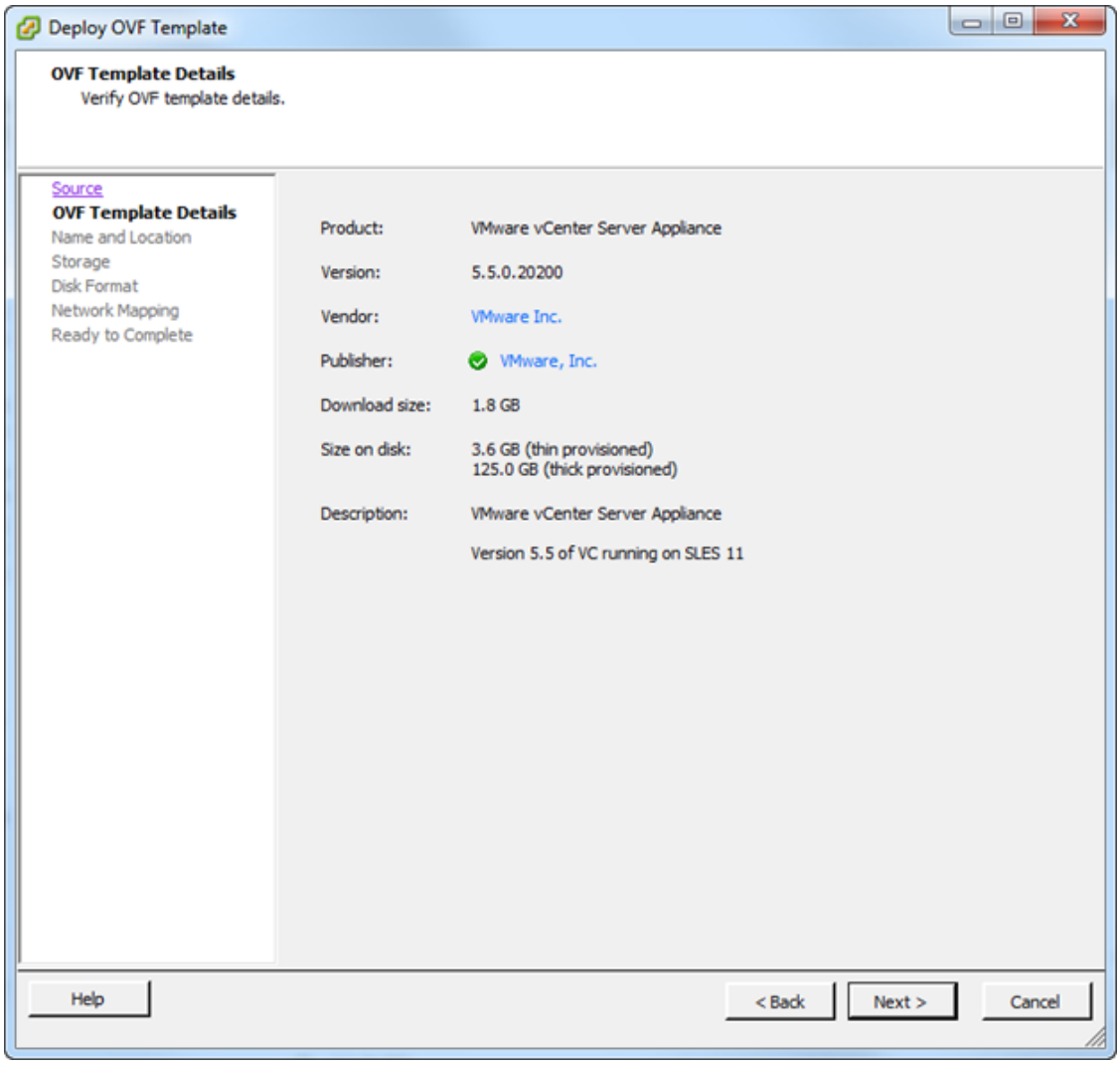
Build and Set up VMware vCenter VM

To build the VMWare vCenter VM, complete the following steps:

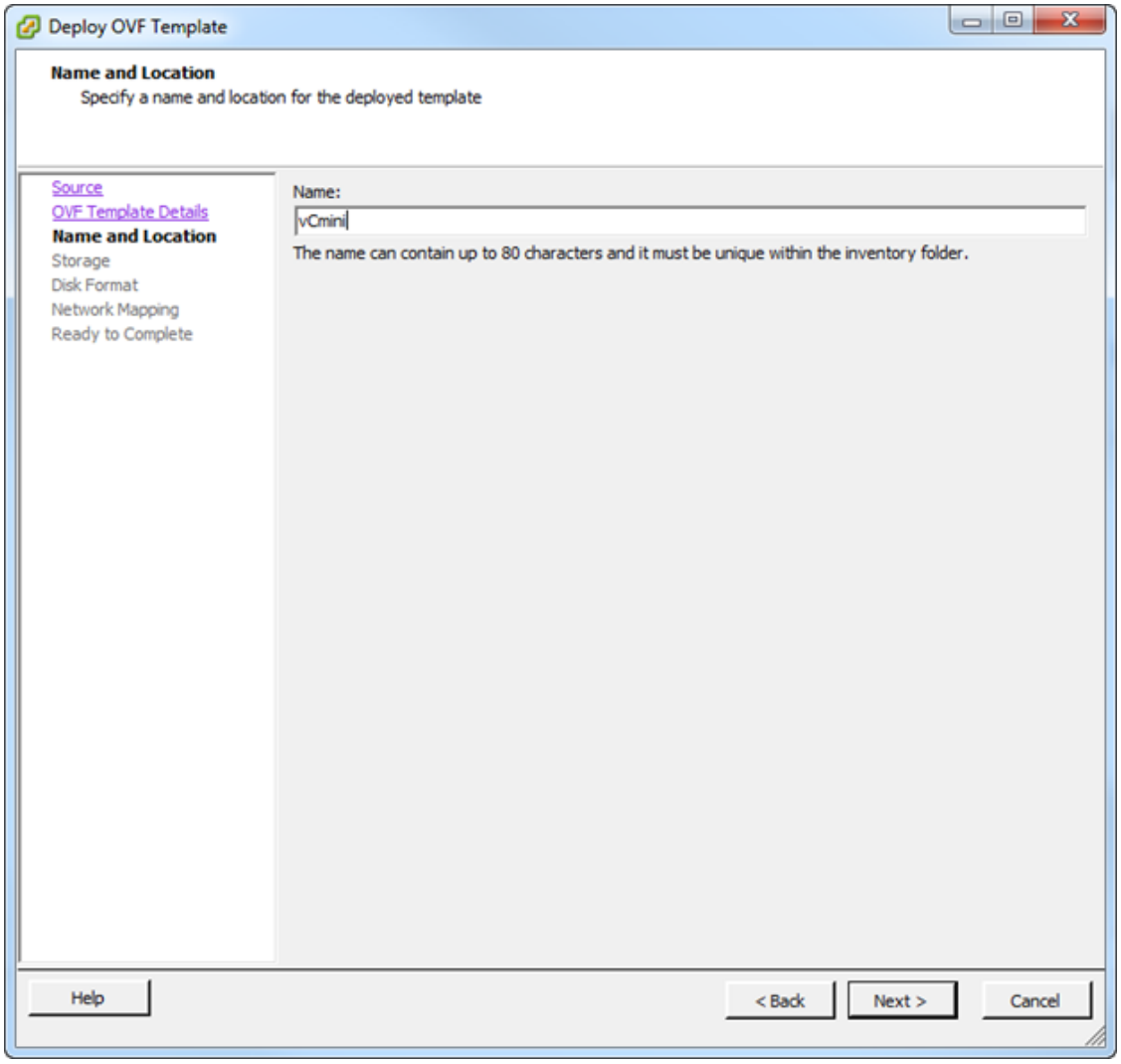
1. From the vSphere 5 download page on the VMware Web site, download the `.OVA` file for the vCenter Server appliance onto your system.
2. Open the vSphere Infrastructure client, and enter `<<var_vm_host_infra_01_ip>>` in the IP address/hostname field. Enter root as the user name and the root password in the password field.
3. Click Login.



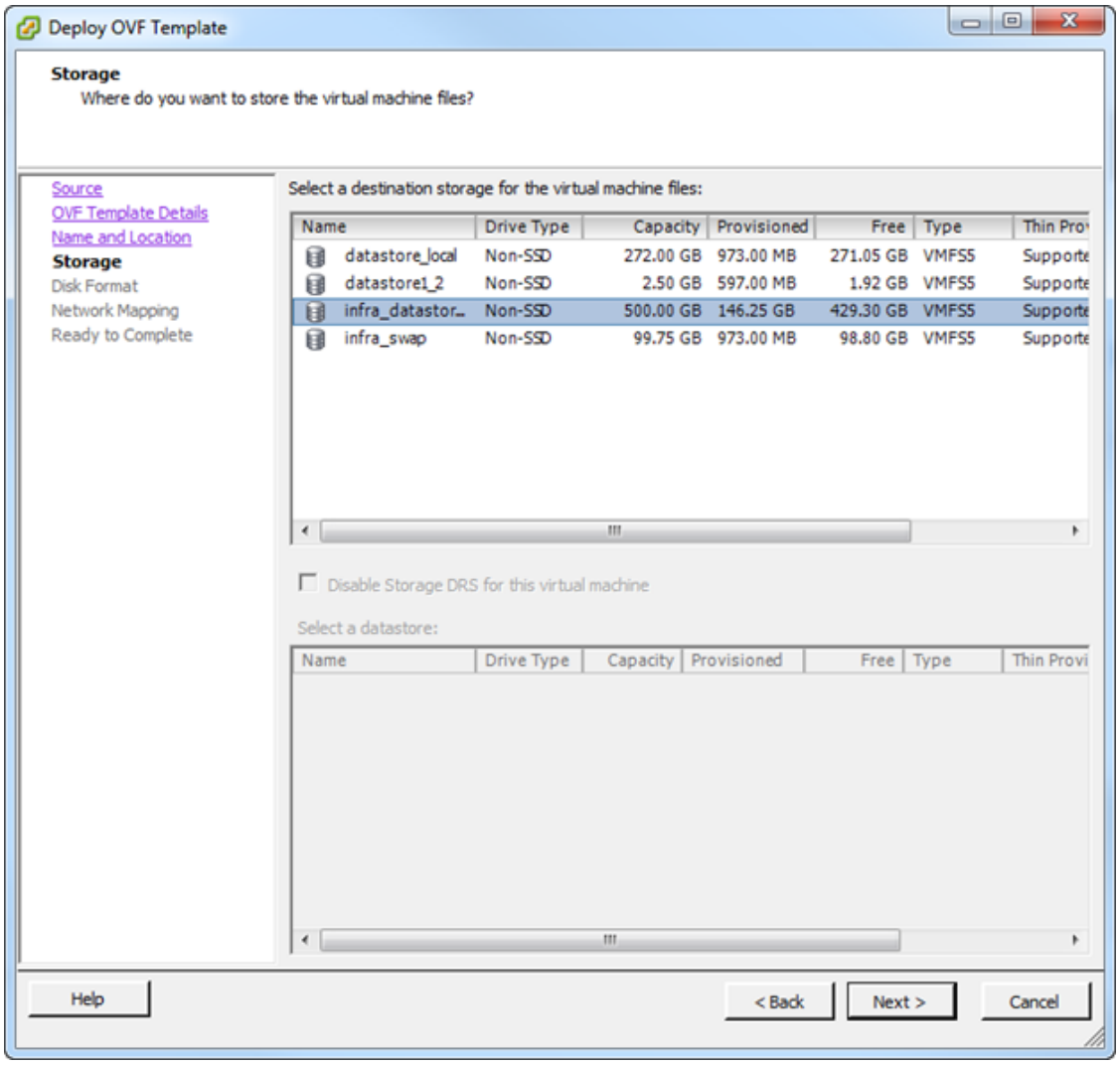
4. From the vSphere Client interface, click File > Deploy OVF Template.
5. Browse to the location where the OVF file was downloaded in step 1.
6. Click Next to continue installation.


Deploy OVF Template
OVF Template Details
Verify OVF template details.
Source
OVF Template Details
Name and Location
Storage
Disk Format
Network Mapping
Ready to Complete
Product:
VMware vCenter Server Appliance
Version:
5.5.0.20200
Vendor:
VMware Inc.
Publisher:
VMware, Inc.
Download size:
1.8 GB
Size on disk:
3.6 GB (thin provisioned)
125.0 GB (thick provisioned)
Description:
VMware vCenter Server Appliance
Version 5.5 of VC running on SLES 11
Help
< Back
Next >
Cancel

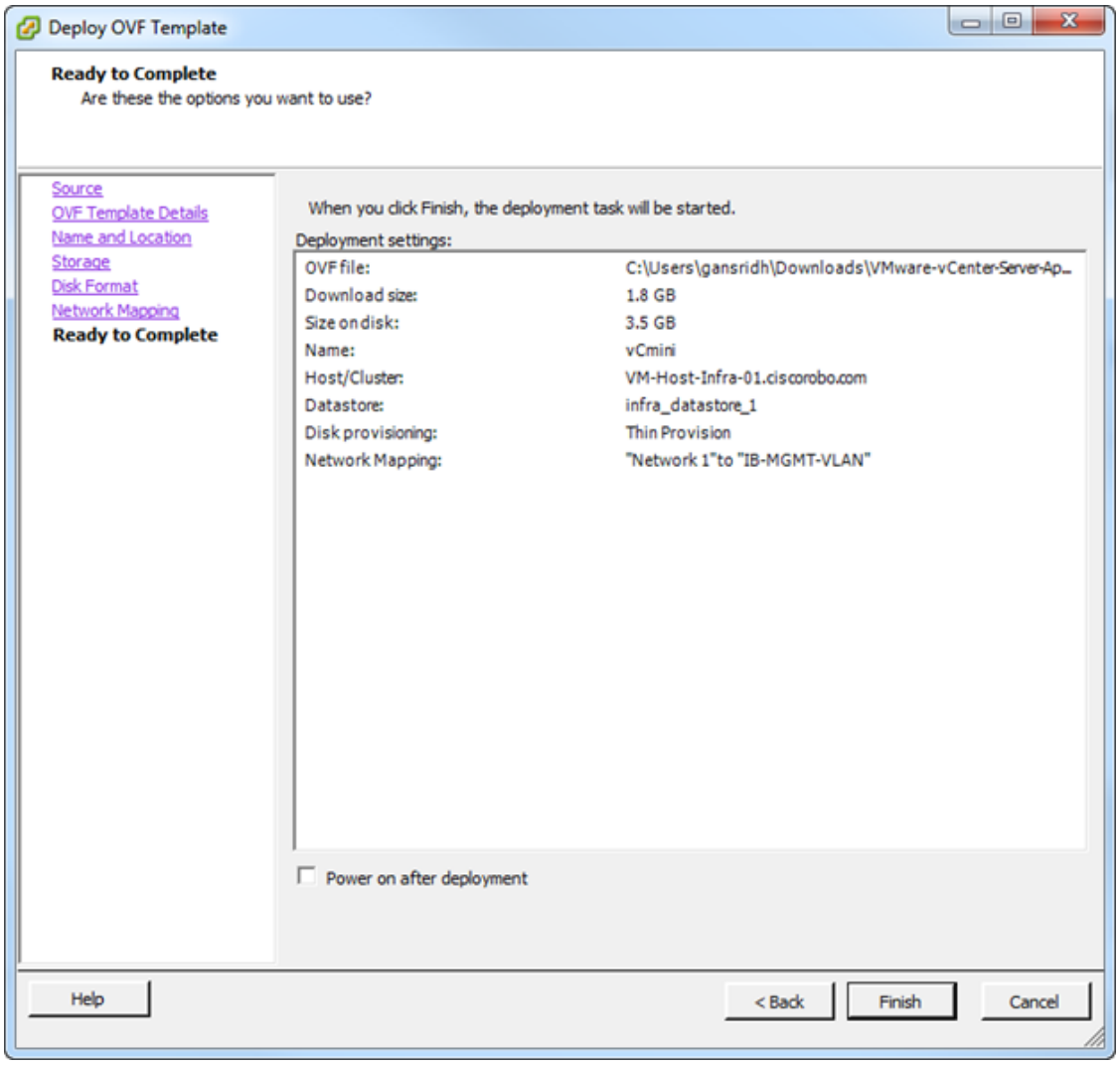
7. Click Next.



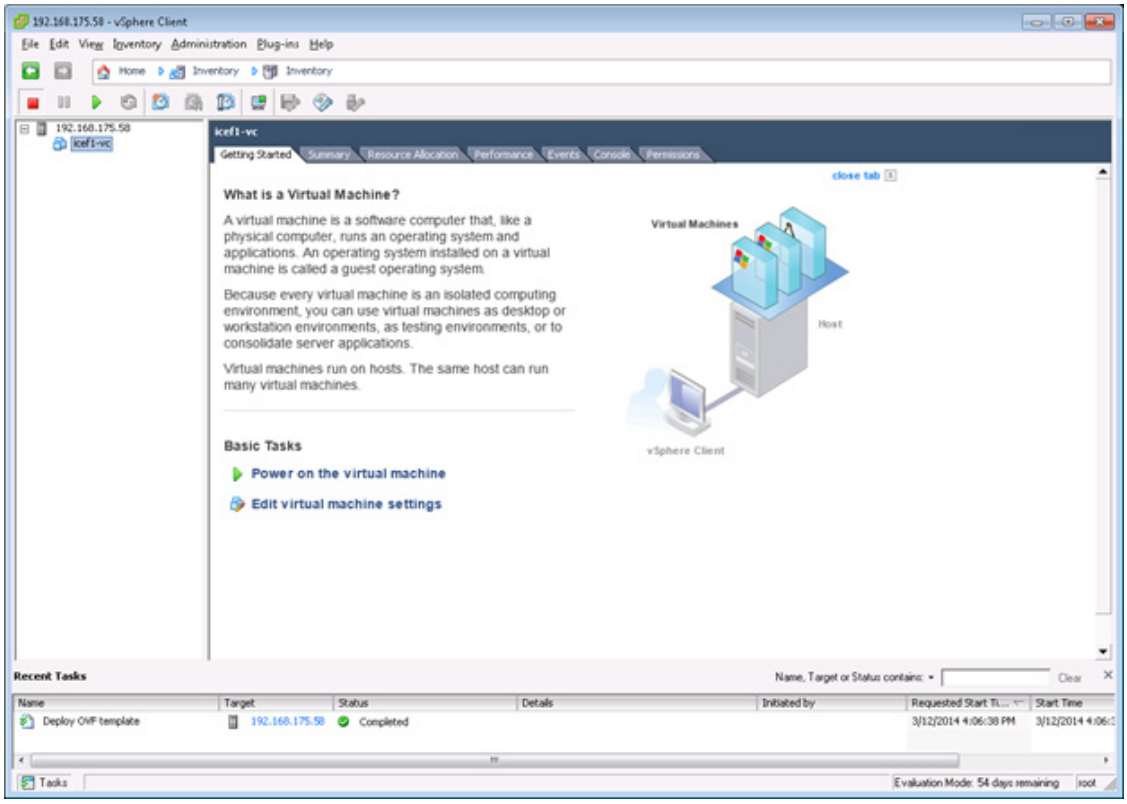
8. Provide a name for the vCenter VM, then click Next to continue.



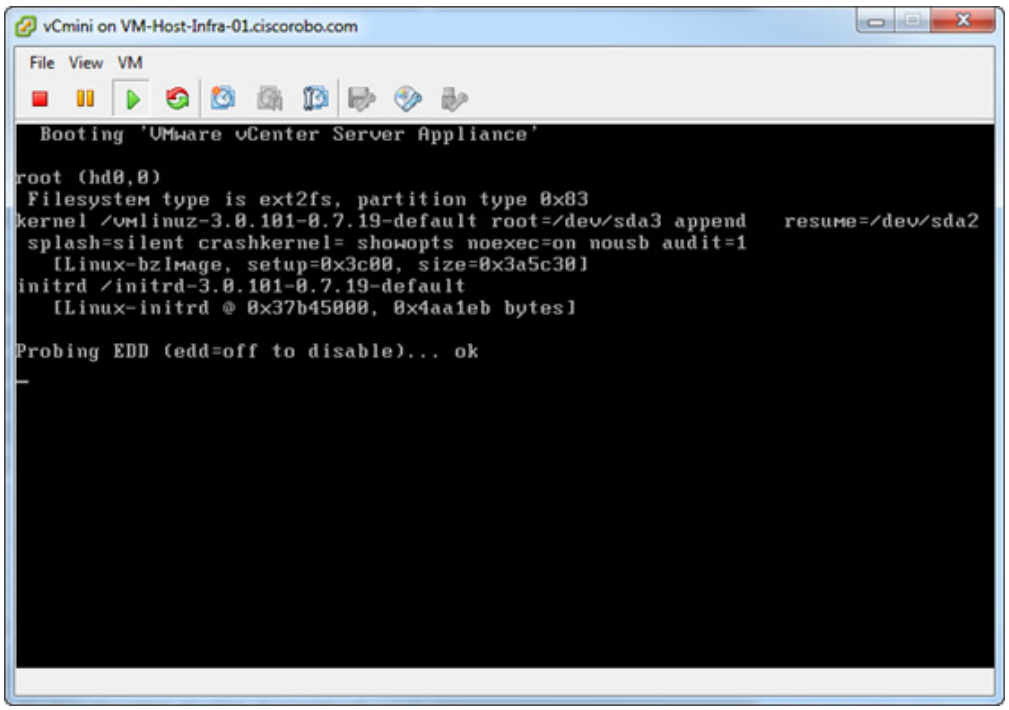
9. Select `infra_datastore_1` as the location for the vCenter VM virtual disks, then click Next to continue.
10. Review the disk format selection and click Next to continue.



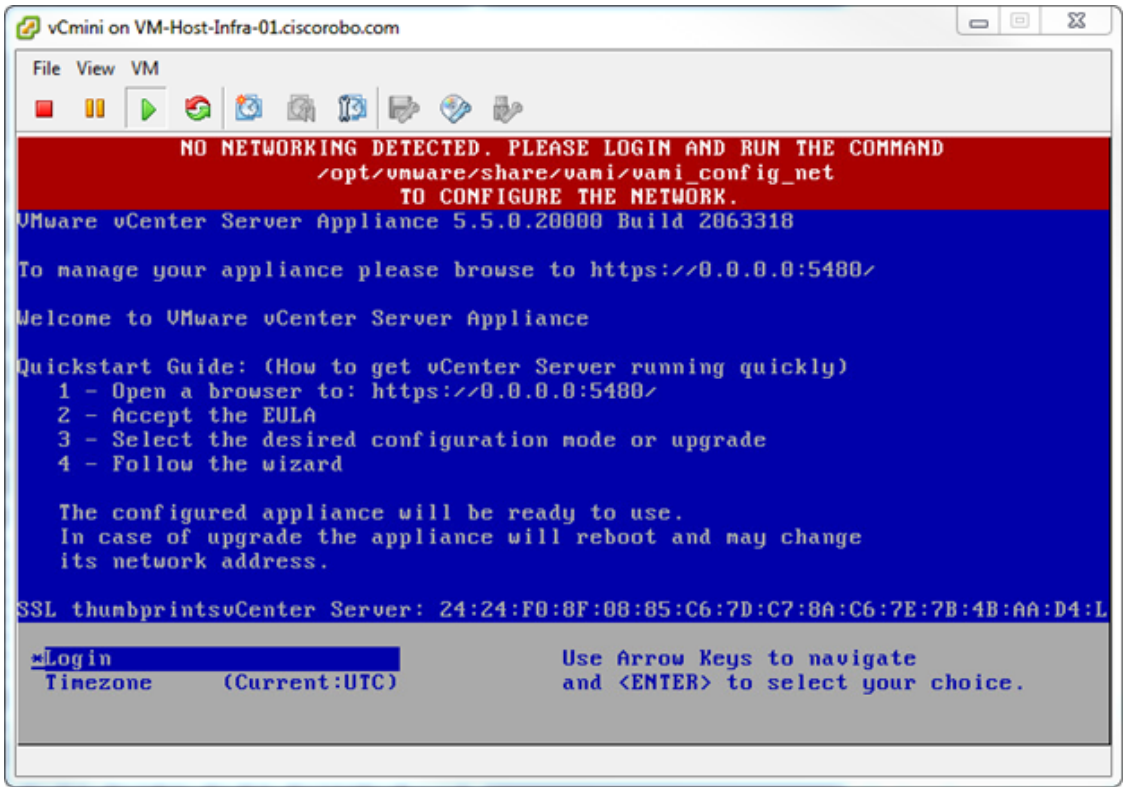
11. Review the installation details and click Finish to continue.
12. After the installation has been completed, click the plus symbol to the left of the host IP address in the left pane of the vSphere Client window.



13. Right-click the vCenter VM and click Power > Power On.
14. Right-click the vCenter VM and click Open Console to open a console view.



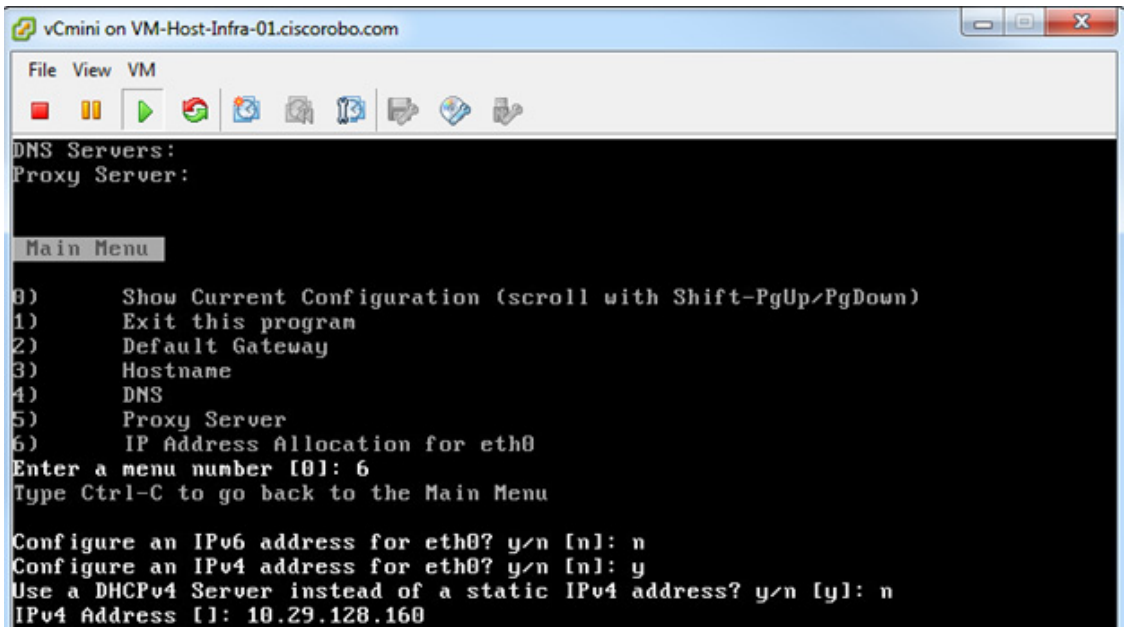
15. Wait for the Virtual Machine to boot.



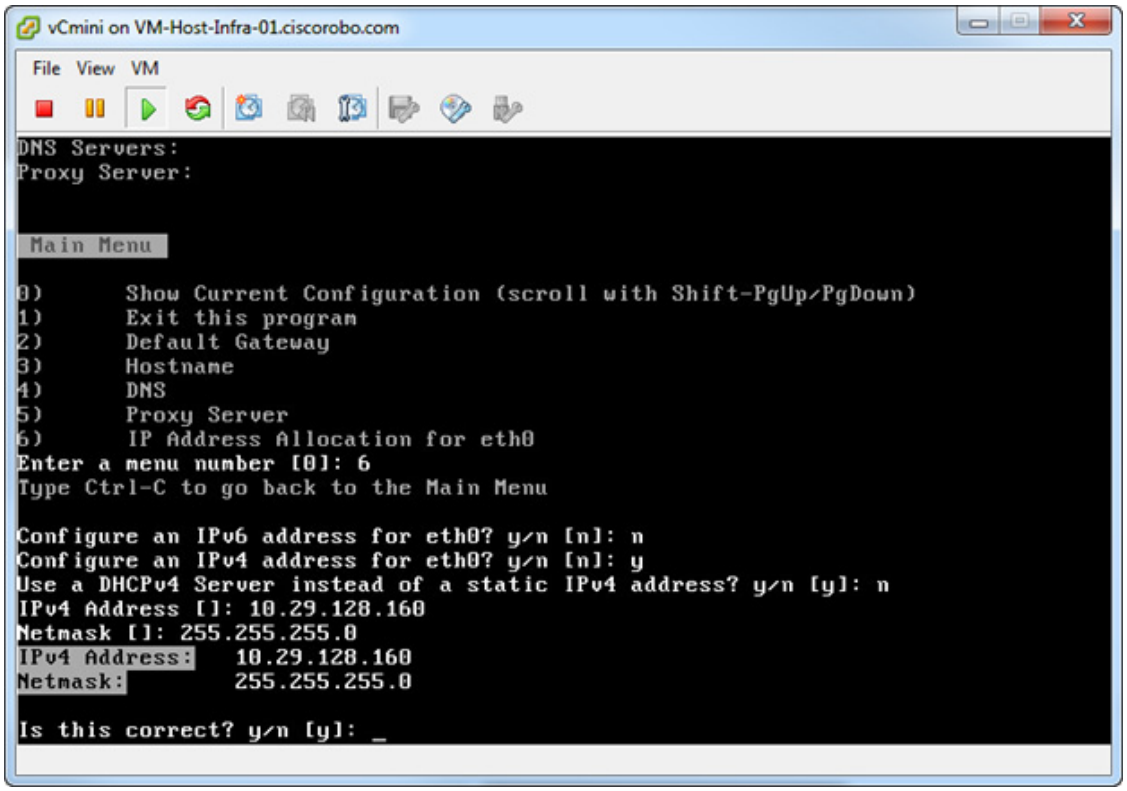
16. The preceding screen is displayed, if the vCenter appliance does not receive an IP address through DHCP. Press Enter to Login.

Note If the in-band management network provides a DHCP server and provided an IP address to the vCenter server, proceed to step 30.

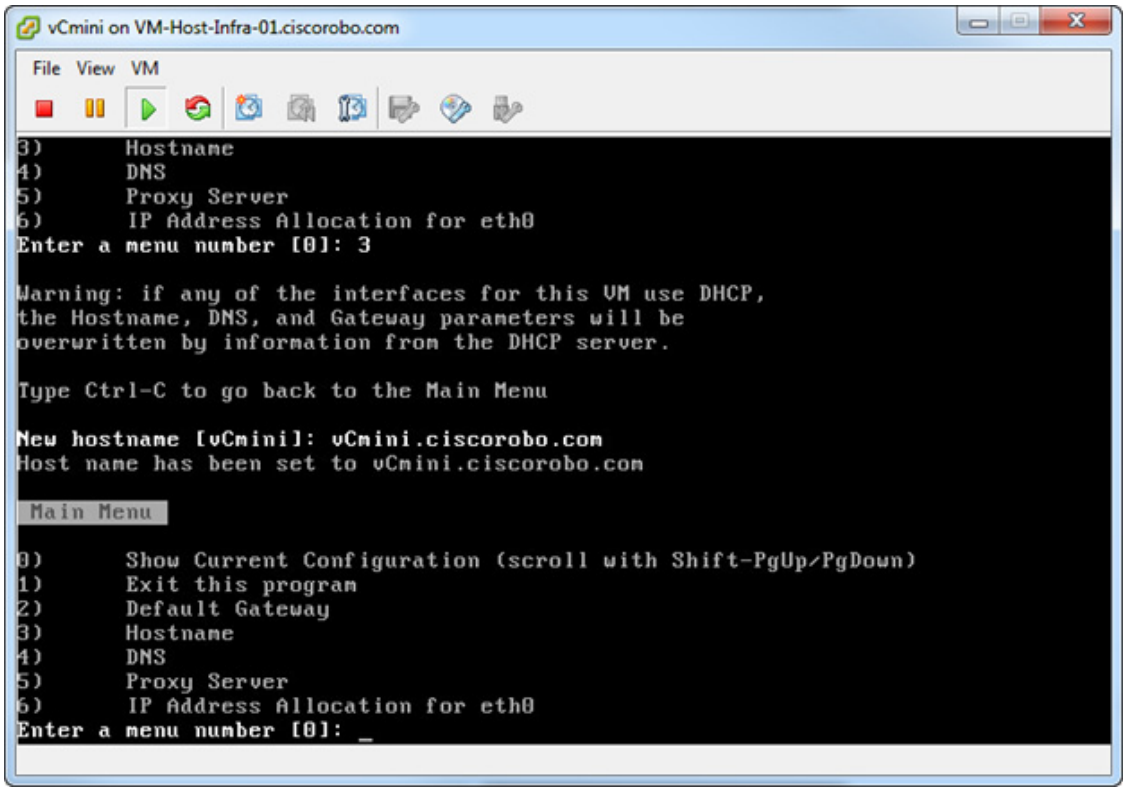
17. From the login screen type `root` as the login and press Enter
18. Type `vmware` as the password and press Enter.
19. From the prompt, type `/opt/vmware/share/vami/vami_config_net` and click Enter.



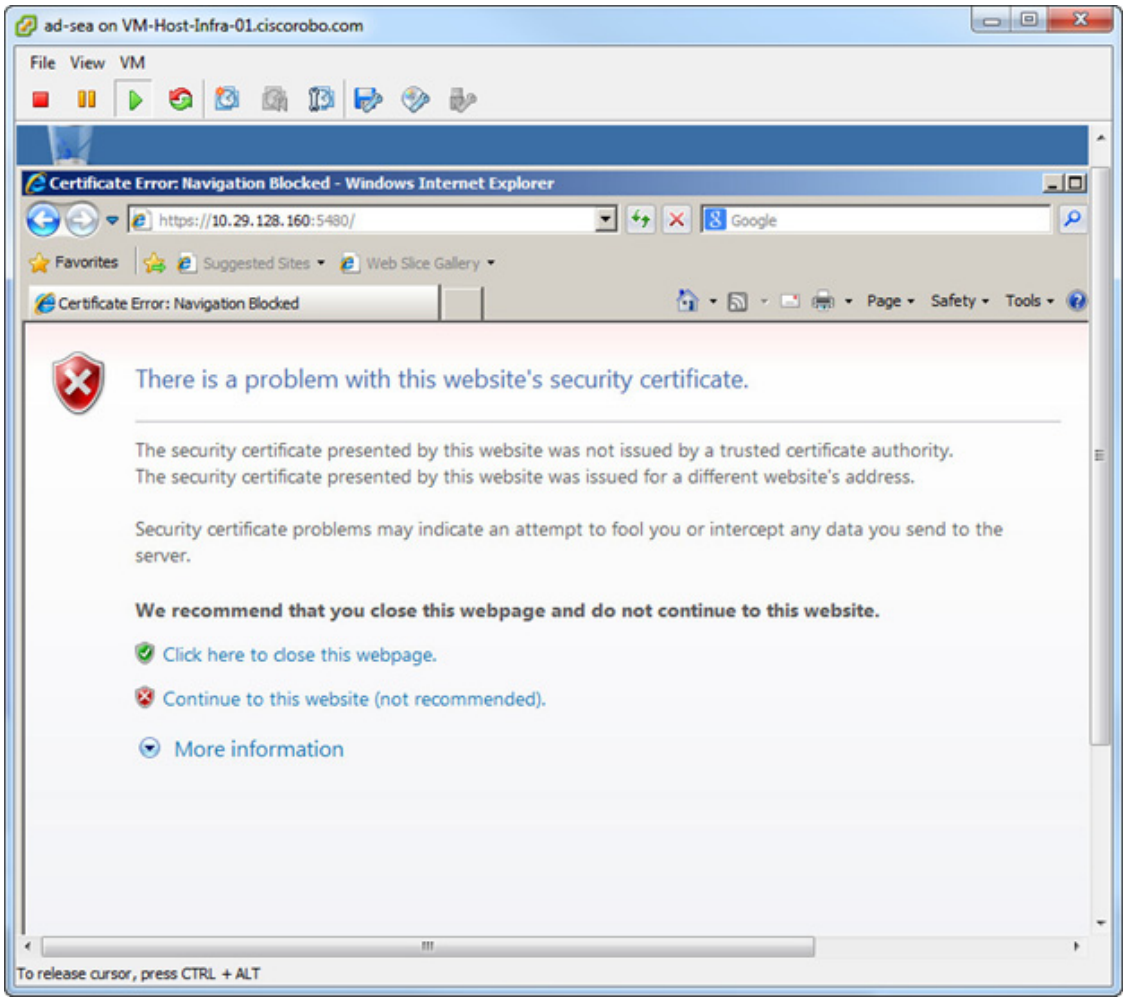
20. To configure the IP address for the vCenter server, type `6` and press Enter.
21. To disable IPv6, type `n` and press Enter.
22. To choose to configure an IPv4 address, type `y` and press Enter.
23. To use a static address instead of a DHCP address, type `n` and press Enter.
24. Type `<<var_vcenter_ip_address>>` and press Enter.
25. Type `<<var_vcenter_netmask>>` and press Enter.



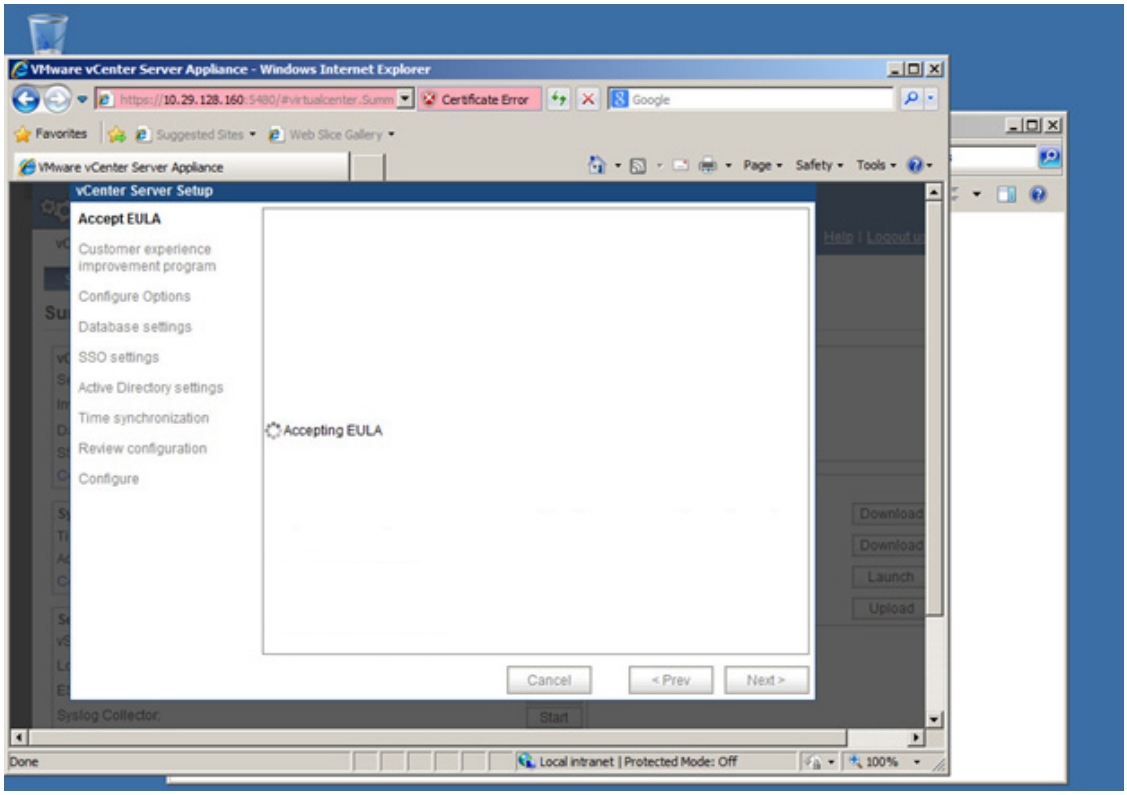
26. Review the IP address and subnet mask. Type y and press Enter to complete the configuration.
27. Type 3 and press Enter to enter the Hostname of the vCenter Server.



28. Type `2` and press Enter to configure the default gateway IP address.
29. Type `4` and press Enter to configure the DNS information for the vCenter server.
30. Type `<<var_DNS_1_IP>>` and press Enter.
31. Type `<<var_DNS_2_IP>>` and press Enter to accept the configuration changes.
32. Type `2` and press Enter to exit the configuration dialogue.
33. Type `exit` and press Enter to log out of the prompt.
34. Follow the instructions on the welcome screen to open a browser window to the URL shown.

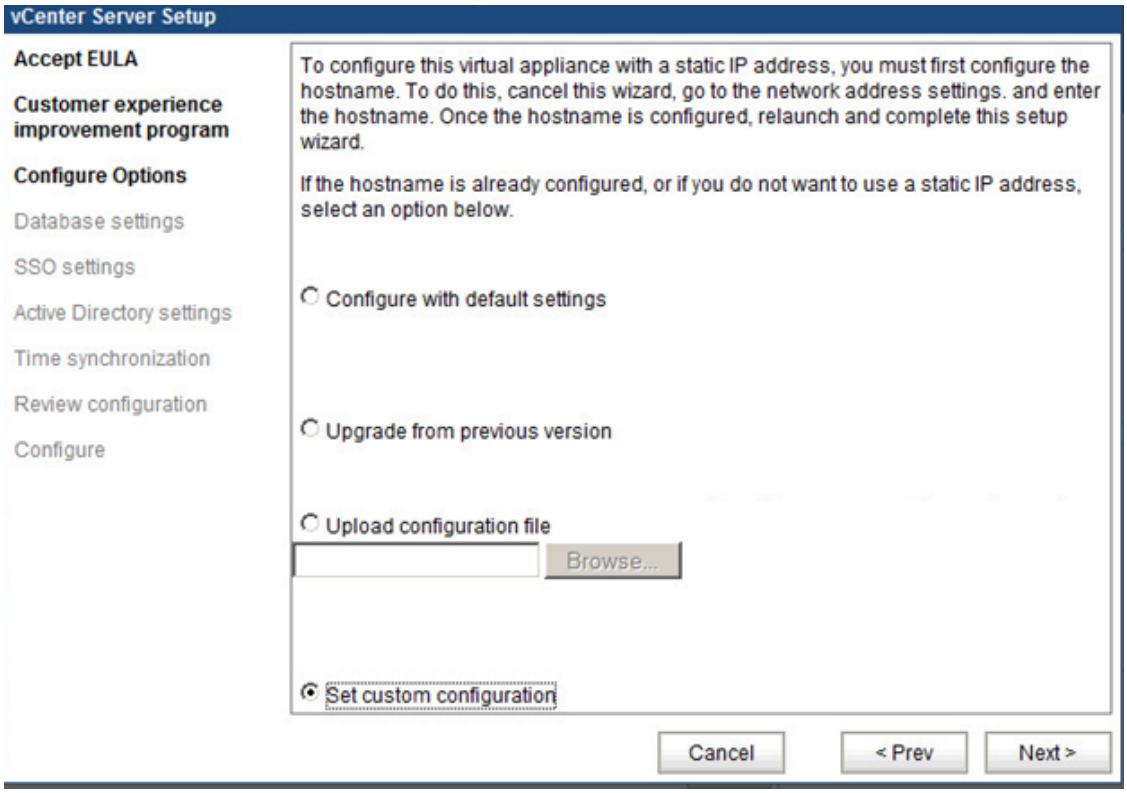


35. Click Continue to this website and enter the User name and `vmware` for the password. Click Login.

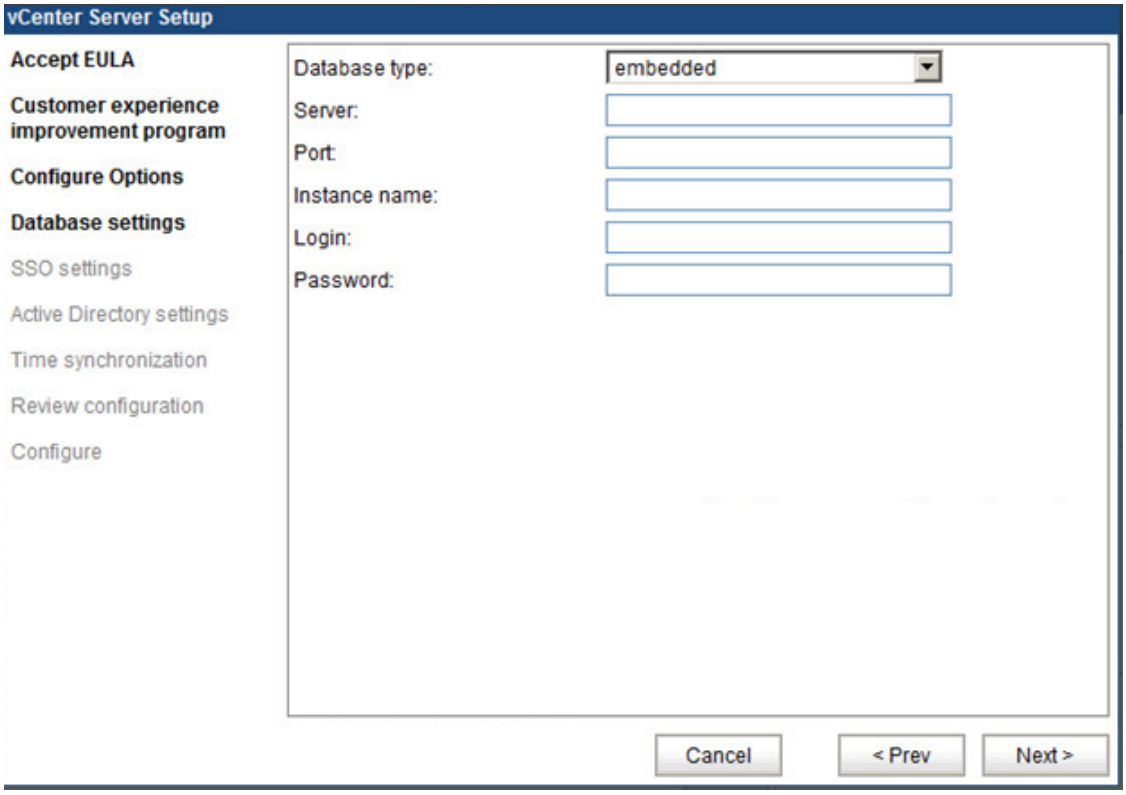


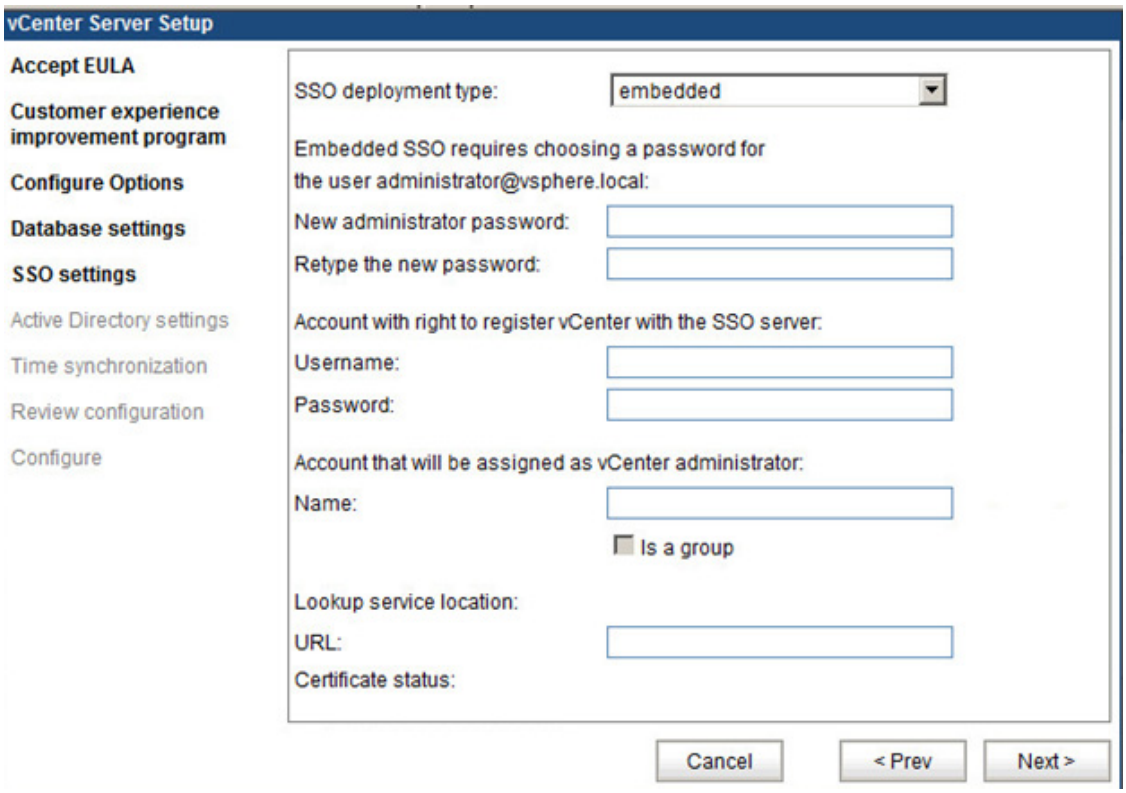
36. Select the Accept license agreement checkbox, click Next to continue.

37. Click Next.



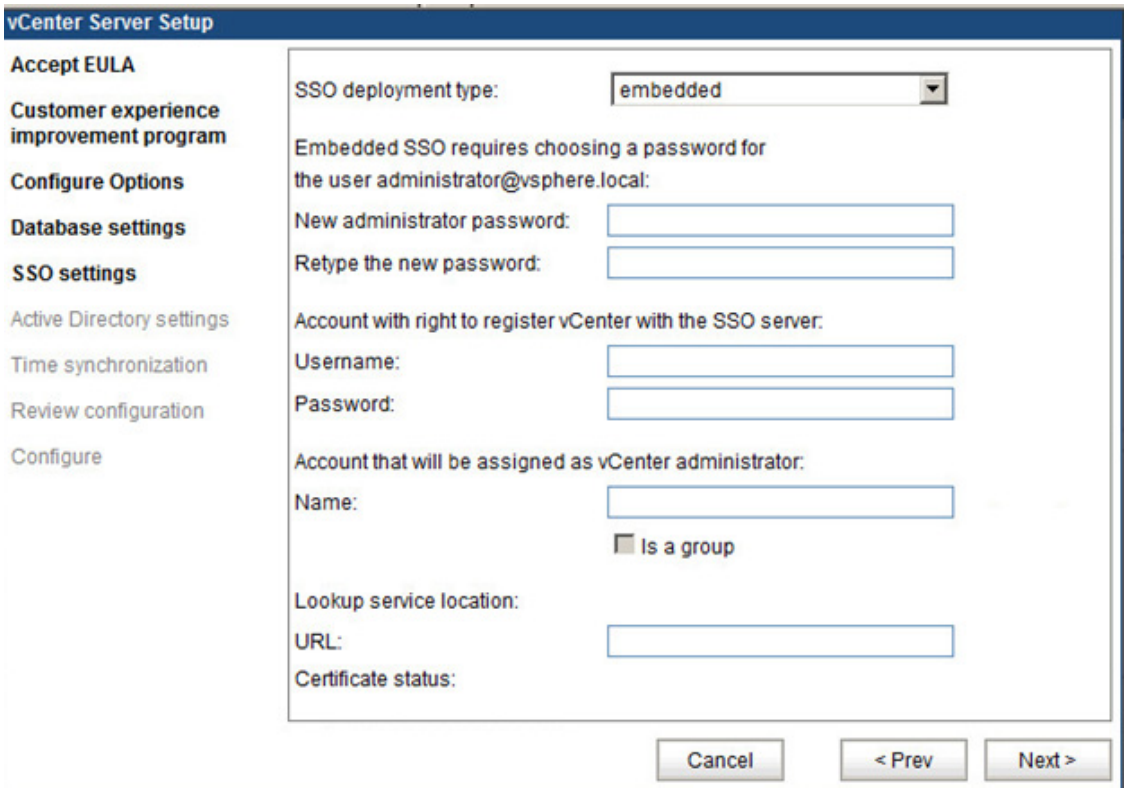
38. Select the Set custom configuration option then click Next to continue.


vCenter Server Setup
Accept EULA
Customer experience improvement program
Configure Options
Database settings
SSO settings
Active Directory settings
Time synchronization
Review configuration
Configure
Database type:
embedded
Server:
Port:
Instance name:
Login:
Password:
Cancel
< Prev
Next >

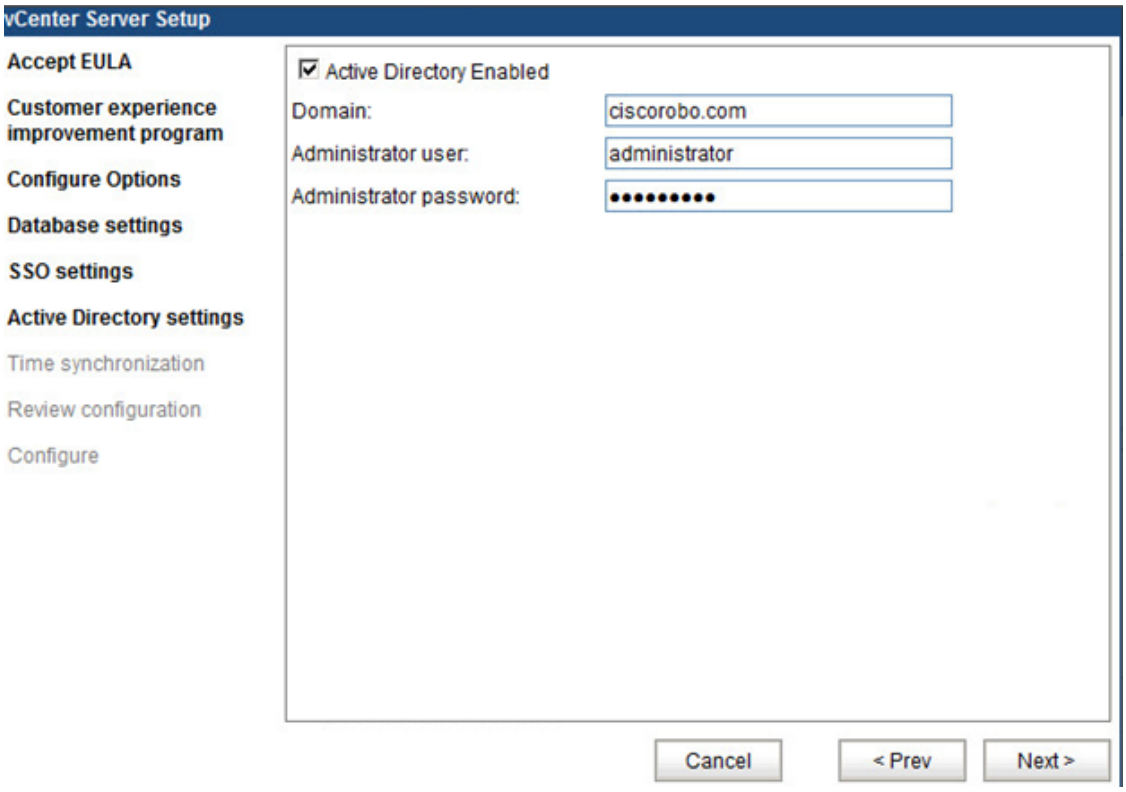

vCenter Server Setup
Accept EULA
Customer experience improvement program
Configure Options
Database settings
SSO settings
Active Directory settings
Time synchronization
Review configuration
Configure
SSO deployment type:
embedded
Embedded SSO requires choosing a password for the user administrator@vsphere.local:
New administrator password:
Retype the new password:
Account with right to register vCenter with the SSO server:
Username:
Password:
Account that will be assigned as vCenter administrator:
Name:
Is a group
Lookup service location:
URL:
Certificate status:
Cancel
< Prev
Next >

39. Click Next to accept an embedded database.

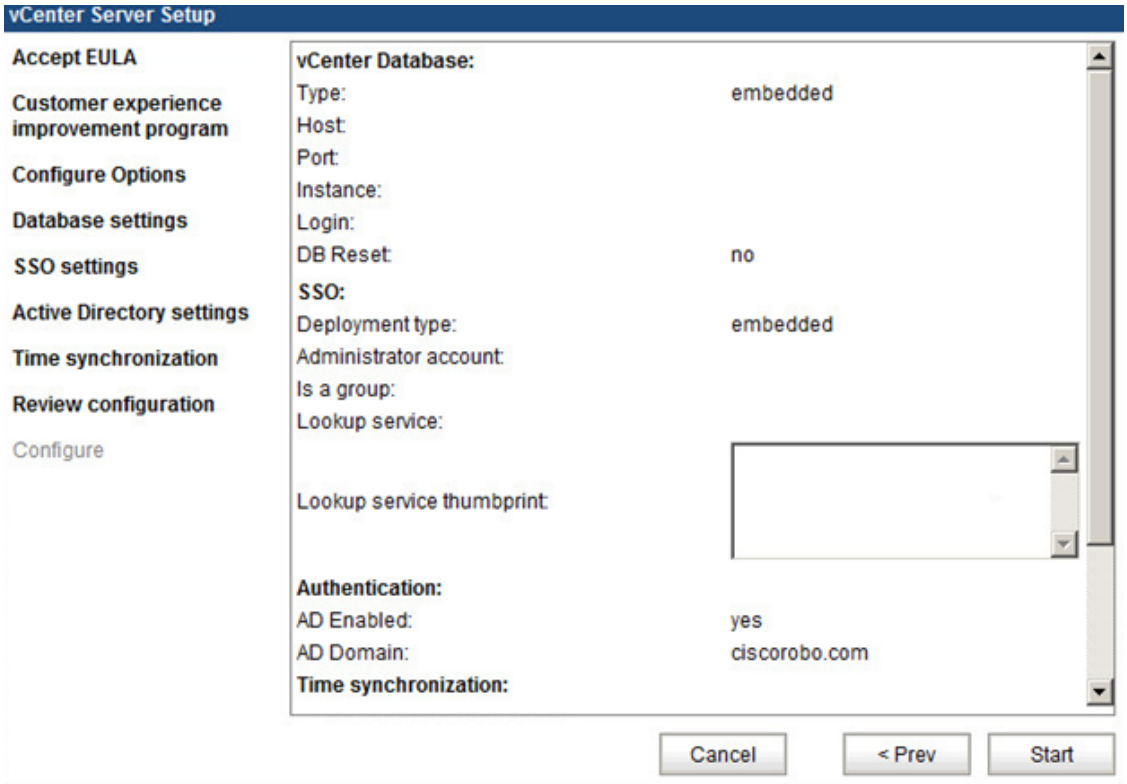
Note An Oracle database can alternatively be used and is recommended for vCenter installations supporting 1000 or more hosts.



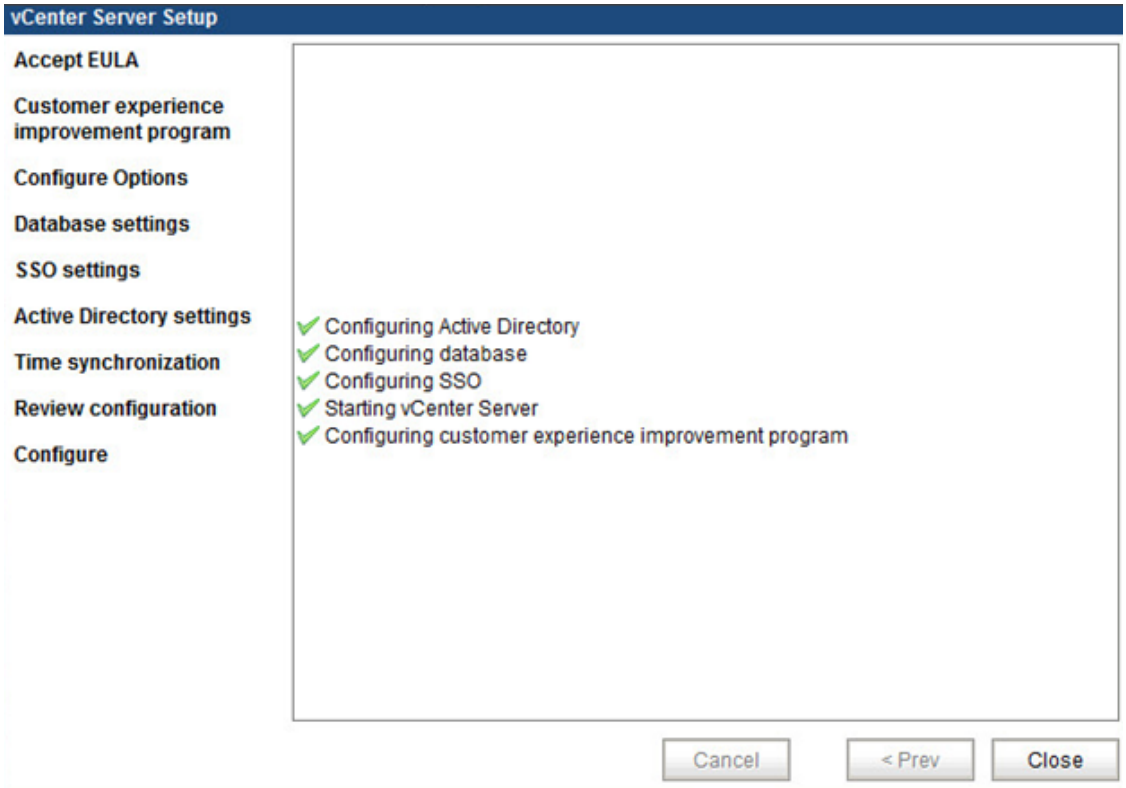
40. Enter the password in the password field, click Next to accept an embedded SSO deployment.



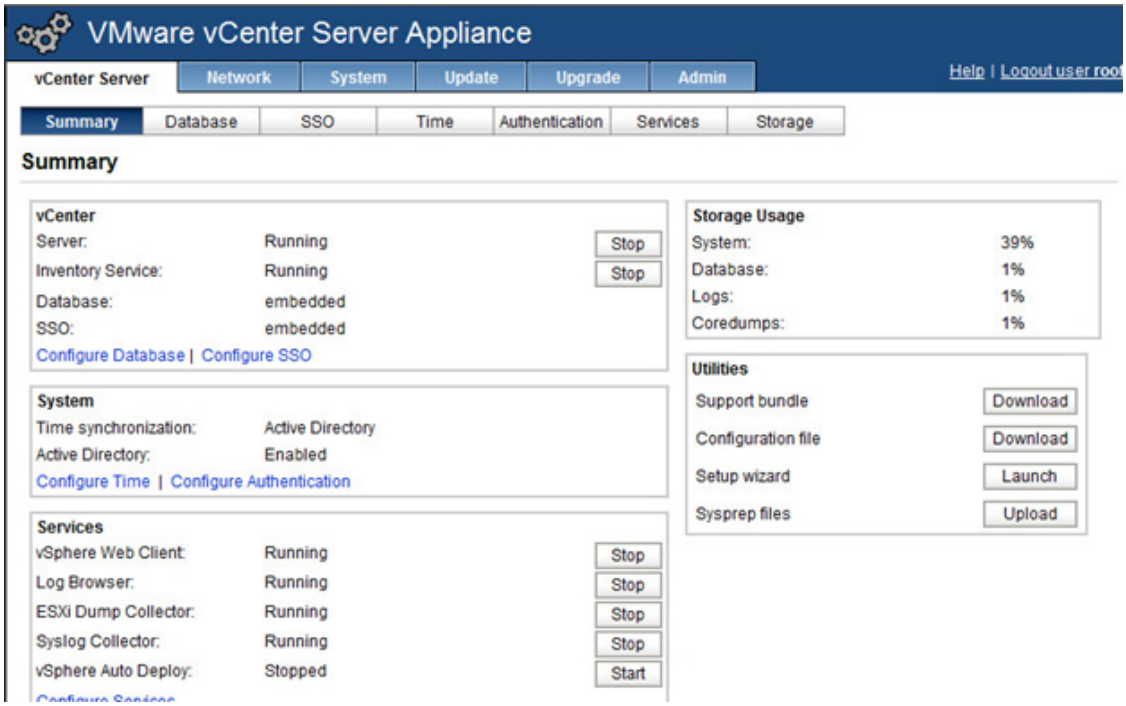
41. Select the Active Directory Enabled checkbox to configure Active Directory based user permissions.
42. Enter the domain, administrator user name, and administrator password in the fields then click Next to continue.



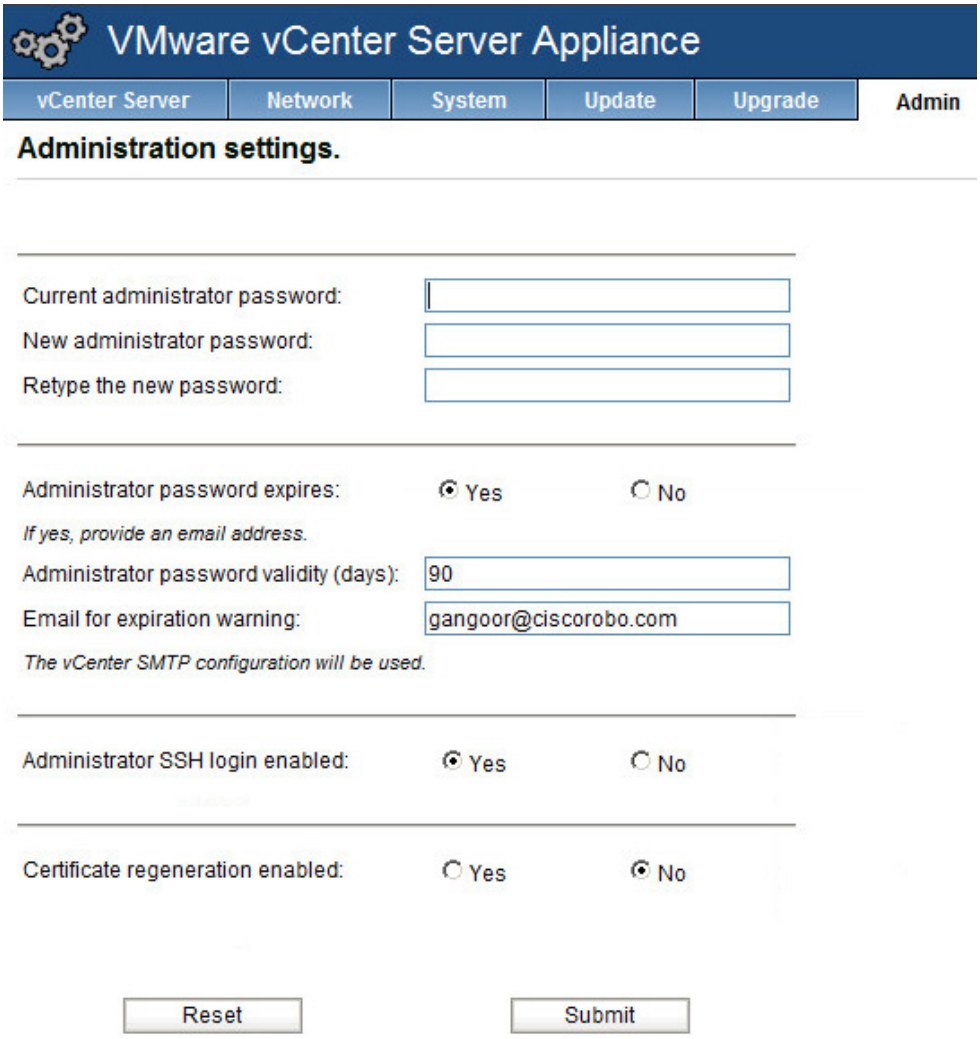
43. Wait for the configuration to complete.



44. Review the configuration settings and click Start to complete the configuration. The vCenter server will create all of the necessary configurations and database structures specified in the preceding section. This step may require several minutes. Click Close after the configuration has completed.



45. Change the root user password and enabling SSH login and the password expiry settings.

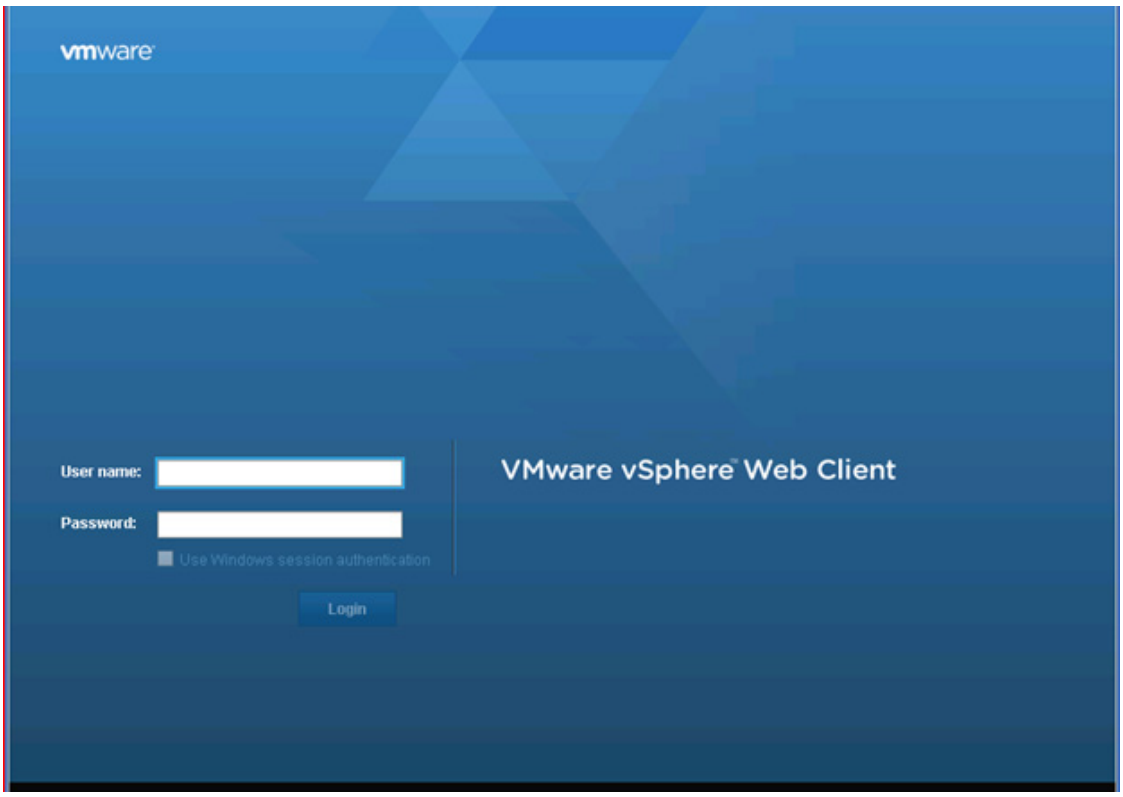


46. Click Close.

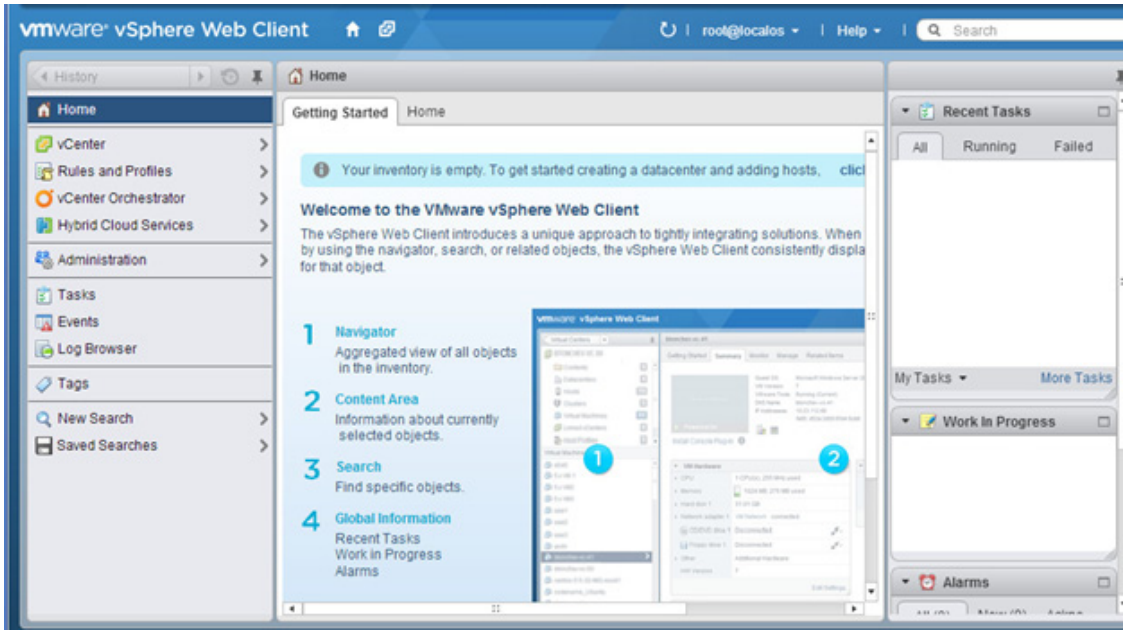
Log into the vSphere Web Client

1. Using a web browser, navigate to `https://<<var_vcenter_ip>>`.

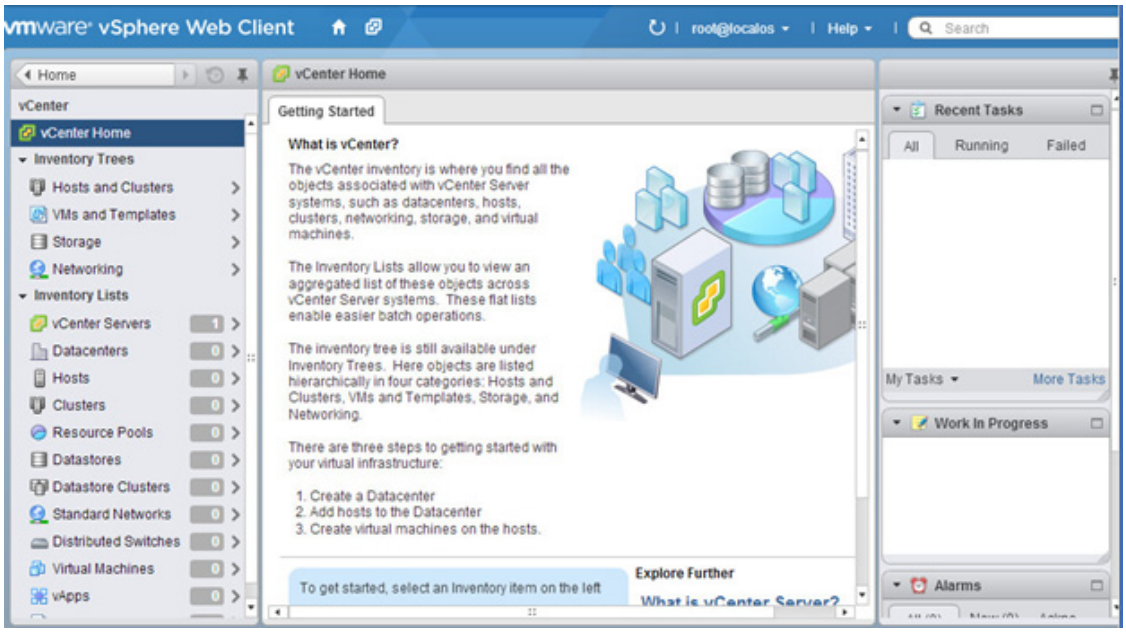
2. Click the link labeled Log in to vSphere Web Client.



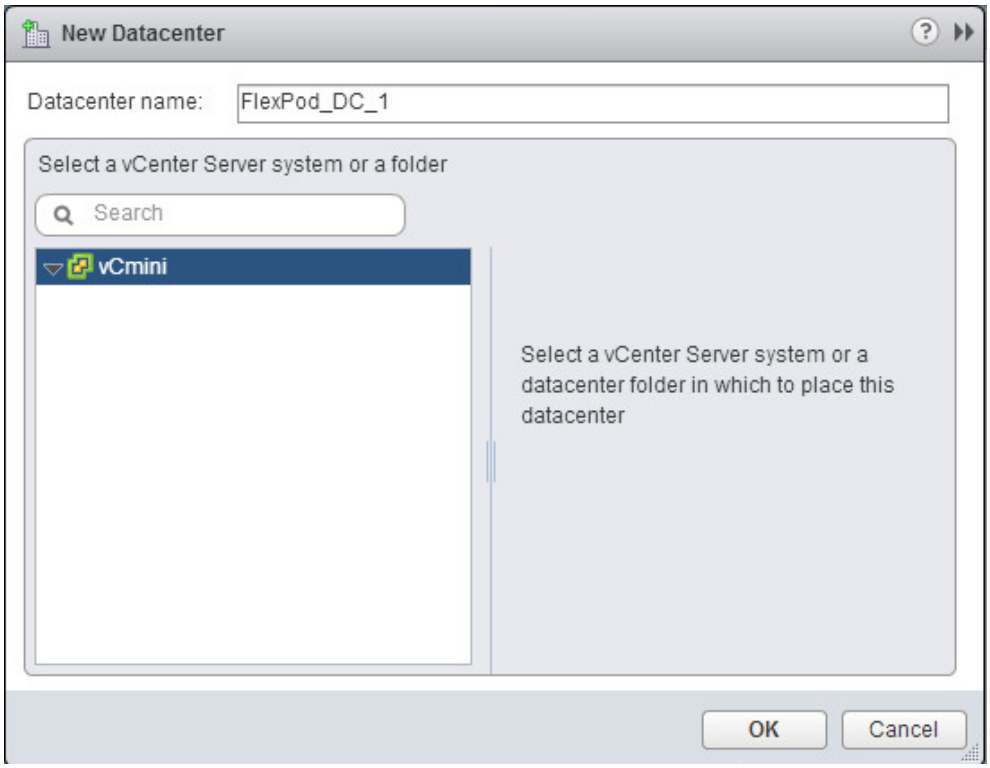
3. If prompted, run the VMWare Remote Console Plug-in.
4. Log in using the root user name and password.



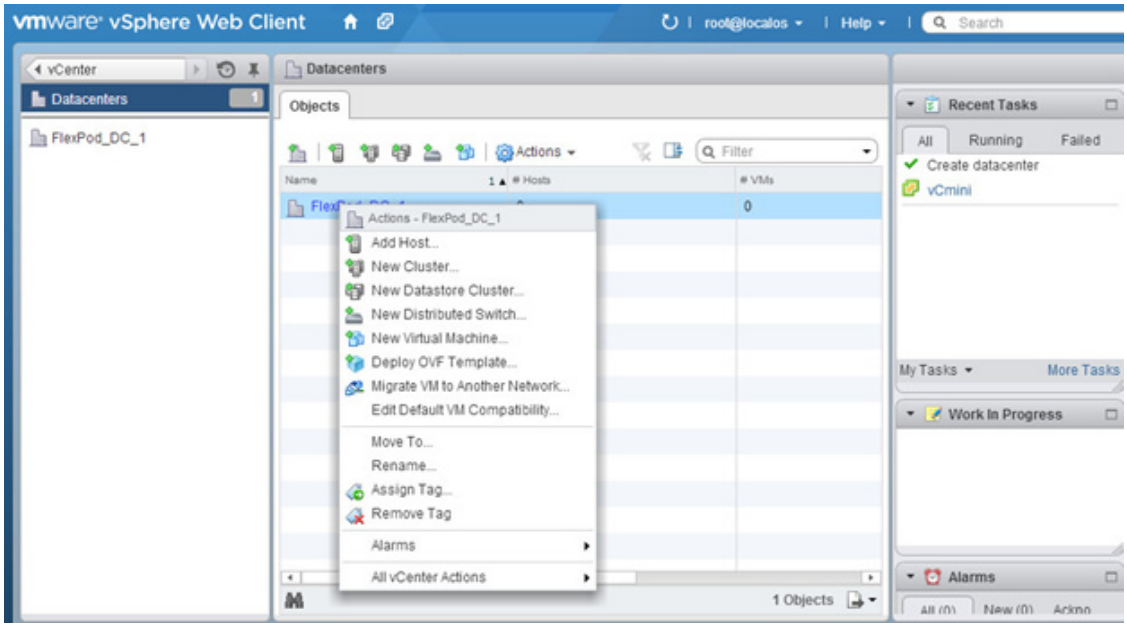
5. Click the vCenter link on the left panel.



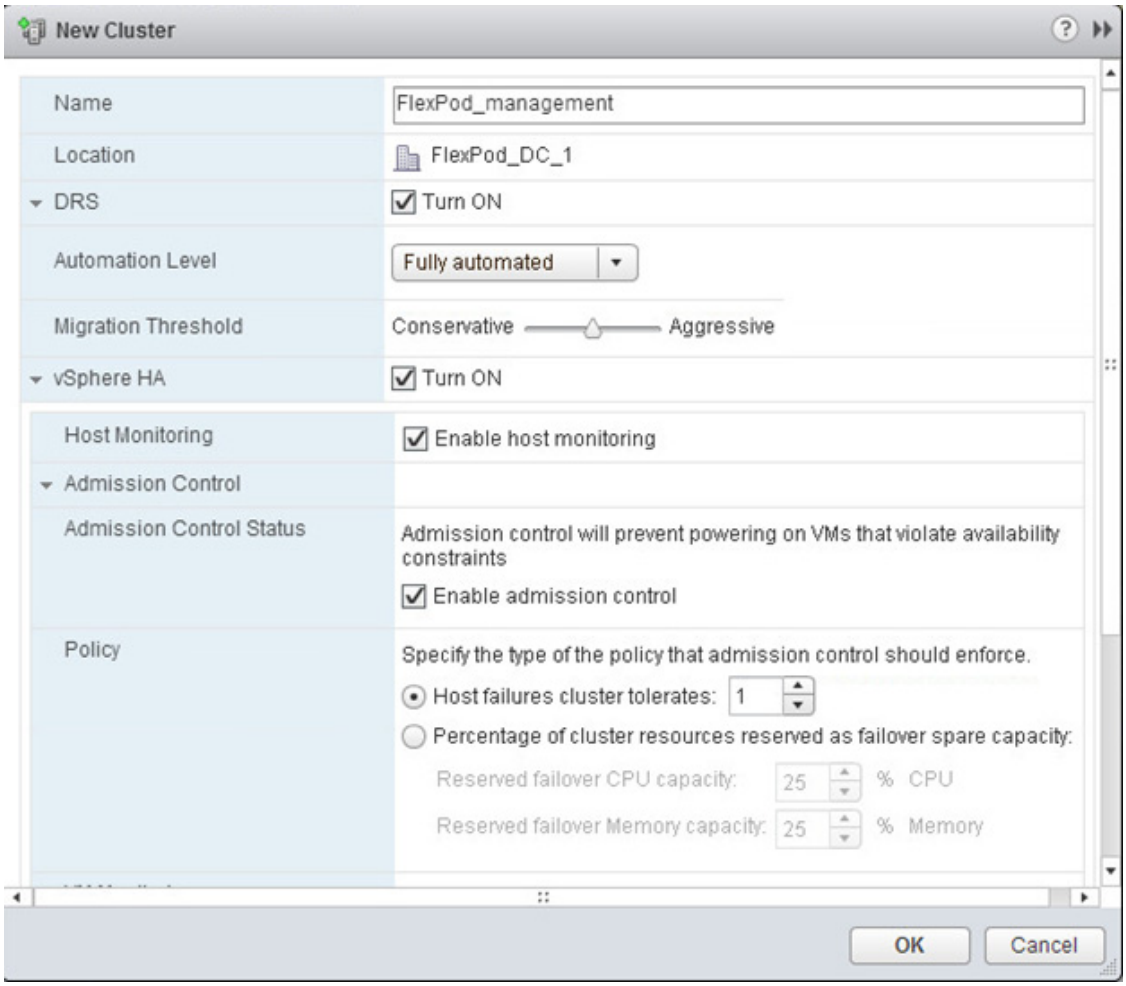
6. Click the Datacenters link on the left panel.
7. To create a Datacenter, click the icon in the center pane which has the green plus symbol above it.



8. Type `FlexPod_DC_1` as the Datacenter name.
9. Click the vCenter server available in the list. Click OK to continue.

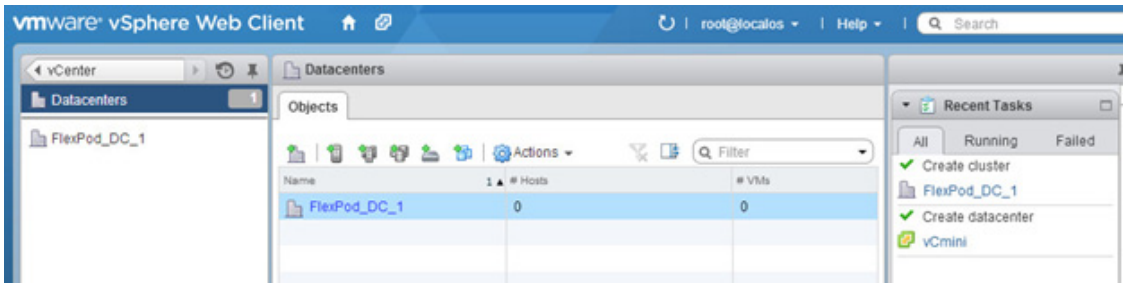


10. Right-click Datacenters > FlexPod_DC_1 in the list in the center pane, then click New Cluster.
11. Name the cluster FlexPod_Management.
12. Select DRS. Retain the default values.
13. Select vSphere HA. Retain the default values.



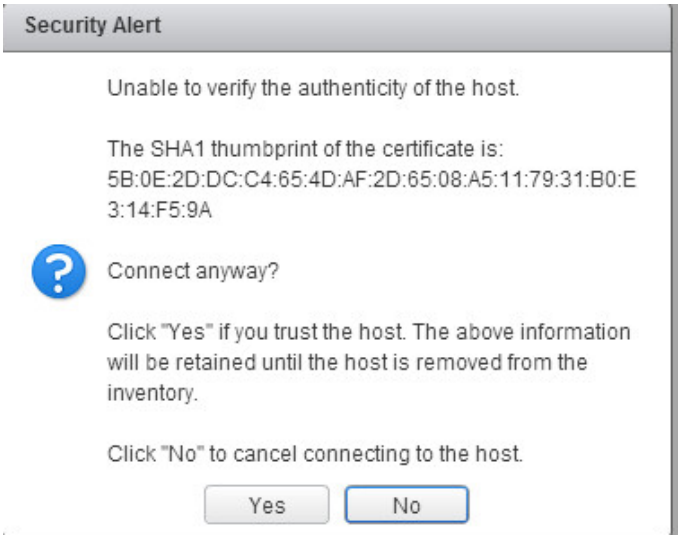
Note If mixing Cisco UCS B or C-Series M2 and M3 servers within a vCenter cluster, it is necessary to enable VMware Enhanced vMotion Compatibility (EVC) mode. For more information about setting up EVC mode, refer to Enhanced vMotion Compatibility (EVC) Processor Support.

14. Click OK to create the new cluster.
15. Click FlexPod_DC_1 in the left pane.

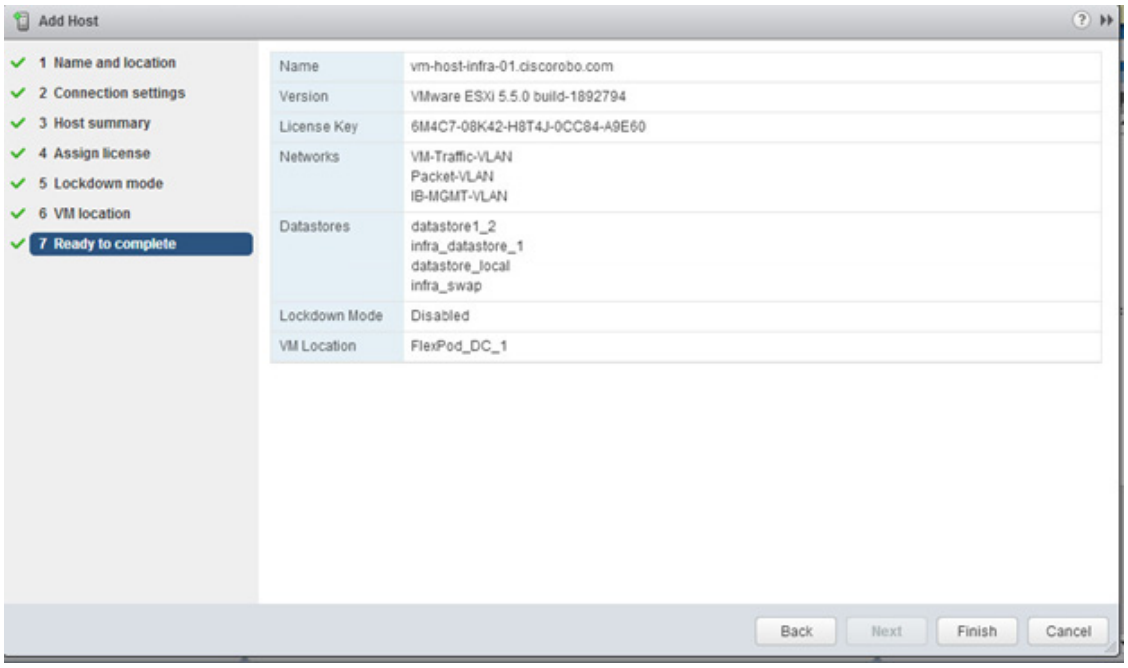


16. Right-click FlexPod_Management in the center pane and click Add Host.

17. Type `<<var_esx_host_1_ip>>` and click Next.
18. Type `root` as the user name and `<<var_esx_host_password>>` as the password. Click Next to Continue.



19. Click Yes to accept the certificate.
20. Review the host details, and click Next to continue.
21. Assign a license, and click Next to continue.
22. Click Next to continue.
23. Click Next to continue.



24. Review the configuration parameters then click Finish to add the host.

25. Repeat this for VM-Host-Infra-02.

vSphere Update Manager Installation and Configuration

Build and Set Up VMware vCenter Update Manager VM

Build Microsoft Windows 2008 R2 VM

Note Alternatively, a VM can be deployed from an existing template or follow these steps.

ESXi Host VM-Host-Infra-01

Note It is recommended to build Windows 2008 R2 virtual machine from an existing OVA file to save time. Once the VM is built from OVA file, complete the configuration settings. Deploying a VM from template is not given below. To deploy a VM from a template or OVA file, use the vSphere Client or the vCenter web client.

To build a SQL Server virtual machine (VM) for the `VM-Host-Infra-01` ESXi host, complete the following steps:

1. Log in to the host using the VMware vSphere Client.
2. In the vSphere Client, select the host in the inventory pane.
3. Right-click the host and select New Virtual Machine.
4. Select Custom and click Next.
5. Enter a name for the VM. Click Next.
6. Select `infra_datastore_1`. Click Next.
7. Select Virtual Machine Version: 10 and Click Next.
8. Verify that the Windows option and the Microsoft Windows Server 2008 R2 (64-bit) version are selected. Click Next.
9. Select two virtual sockets and one core per virtual socket. Click Next.
10. Select 4GB of memory. Click Next.
11. Select one network interface card (NIC).
12. For NIC 1, select the `IB-MGMT-VLAN Network` option and the `VMXNET 3` adapter. Click Next.
13. Retain the LSI Logic SAS option for the SCSI controller selection. Click Next.
14. Retain the Create a New Virtual Disk option selection. Click Next.
15. Make the disk size at least 60GB. Click Next.
16. Select the Disk Provisioning option and Click Next.
17. Click Next with the default setting for Virtual Device Node
18. Select the checkbox for Edit the Virtual Machine Settings Before Completion. Click Continue.
19. Click the Options tab.

20. Select Boot Options.
21. Select the Force BIOS Setup checkbox.
22. Click Finish.
23. From the left pane, expand the host field by clicking the plus sign (+).
24. Right-click the newly created SQL Server VM and click Open Console.
25. Click the third button (green right arrow) to power on the VM.
26. Click the ninth button (CD with a wrench) to map the Windows Server 2008 R2 SP1 ISO, and then select Connect to ISO Image on Local Disk.
27. Navigate to the Windows Server 2008 R2 SP1 ISO, select it, and click Open.
28. Click in the BIOS Setup Utility window and use the right arrow key to navigate to the Boot menu. Use the down arrow key to select CD-ROM Drive. Press the plus (+) key twice to move CD-ROM Drive to the top of the list. Press F10 and Enter to save the selection and exit the BIOS Setup Utility.
29. The Windows Installer boots. Select the appropriate language, time and currency format, and keyboard. Click Next.
30. Click Install Now.
31. Confirm that the Windows Server 2008 R2 Standard (Full Installation) option is selected. Click Next.
32. Read and accept the license terms and click Next.
33. Select Custom (advanced). Make sure that Disk 0 Unallocated Space is selected. Click Next to allow the Windows installation to complete.
34. After the Windows installation is complete and the VM has rebooted, click OK to set the Administrator password.
35. Enter and confirm the Administrator password and click the blue arrow to log in. Click OK to confirm the password change.
36. After logging in to the VM desktop, from the VM console window, select the VM menu. Under Guest, select Install/Upgrade VMware Tools. Click OK.
37. If prompted to eject the Windows installation media before running the setup for the VMware tools, click OK, then click OK.
38. In the dialog box, select Run `setup64.exe`.
39. In the VMware Tools installer window, click Next.
40. Confirm that Typical is selected and click Next.
41. Click Install.
42. If prompted to Trust Software from VMware, Inc, select the checkbox to always trust, and click Install.
43. Click Finish.
44. Click Yes to restart the VM.
45. After the reboot is complete, select the VM menu. Under Guest, select Send Ctrl+Alt+Del and then enter the password to log in to the VM.
46. Set the time zone for the VM, IP address, gateway, and host name. Add the VM to the Windows AD domain.

Note A reboot is required.

47. If necessary, activate Windows.
48. Log back in to the VM and download and install all required Windows updates.

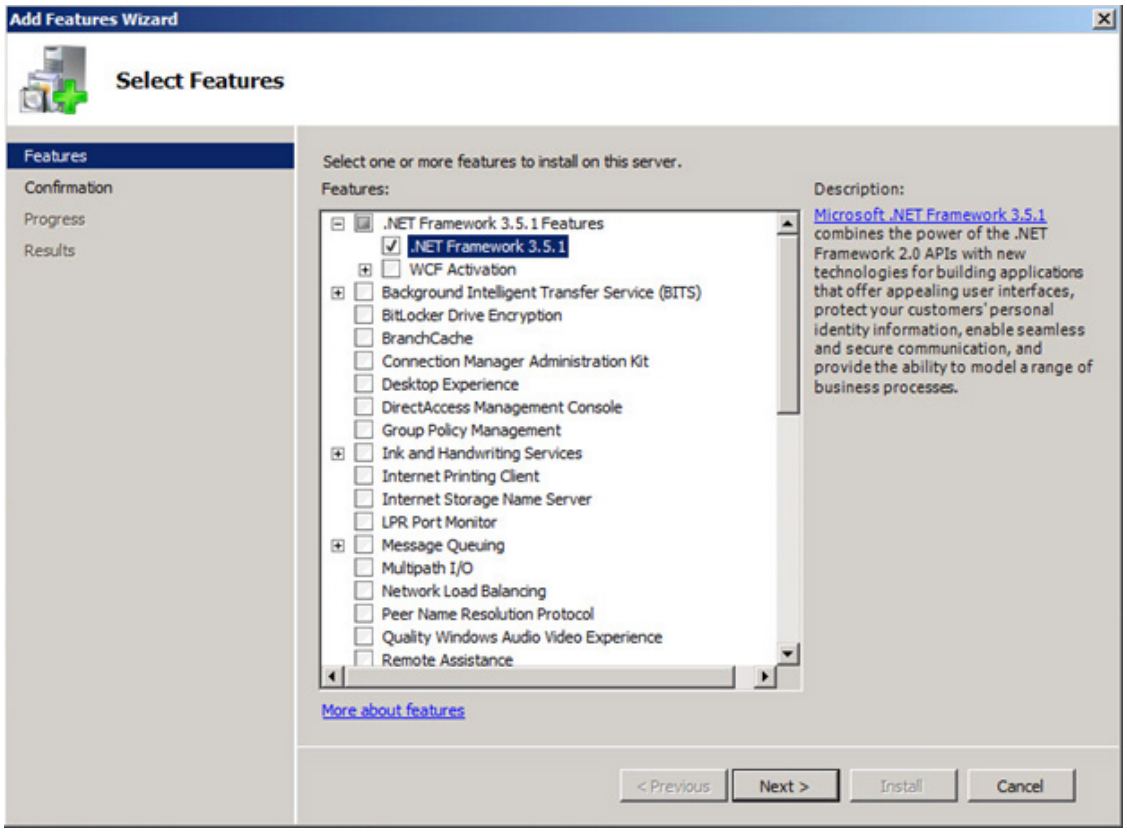
Note This process requires several reboots.

Install Microsoft SQL Server 2008 R2

vCenter SQL Server VM

To install SQL Server on the vCenter SQL Server VM, complete the following steps:

1. Connect to an AD domain controller in the FlexPod Windows domain and add an admin user for the FlexPod using the Active Directory Users and Computers tool. This user should be a member of the Domain Administrators security group.
2. Log in to the vCenter SQL Server VM as the FlexPod admin user and open Server Manager.
3. Expand Features and click Add Features.
4. Expand .NET Framework 3.5.1 Features and select only .NET Framework 3.5.1.

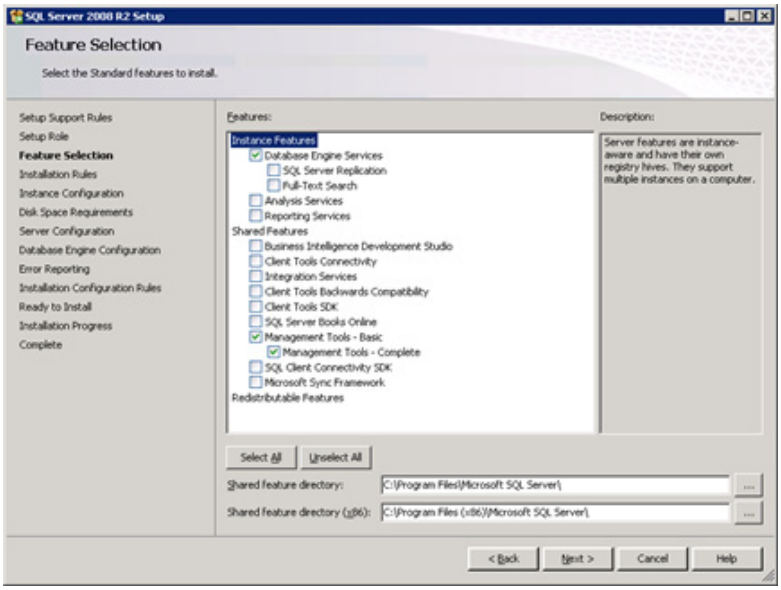


5. Click Next.

6. Click Install.
7. Click Close.
8. Open Windows Firewall with Advanced Security by navigating to Start > Administrative Tools > Windows Firewall with Advanced Security.
9. Select Inbound Rules and click New Rule.
10. Select Port and click Next.
11. Select TCP and enter the specific local port `1433`. Click Next.
12. Select Allow the Connection. Click Next, and then click Next again.
13. Name the rule `SQL Server` and click Finish.
14. Close Windows Firewall with Advanced Security.
15. In the vCenter SQL Server VMware console, click the ninth button (CD with a wrench) to map the Microsoft SQL Server 2008 R2 ISO. Select Connect to ISO Image on Local Disk.
16. Navigate to the SQL Server 2008 R2 ISO, select it, and click Open.
17. In the dialog box, click Run `SETUP.EXE`.
18. In the SQL Server Installation Center window, click Installation on the left.
19. Select New Installation or Add Features to an Existing Installation.
20. Click OK.
21. Select Enter the Product Key. Enter a product key and click Next.
22. Read and accept the license terms and choose whether to select the second checkbox. Click Next.
23. Click Install to install the setup support files.
24. Address any warnings except for the Windows firewall warning. Click Next.

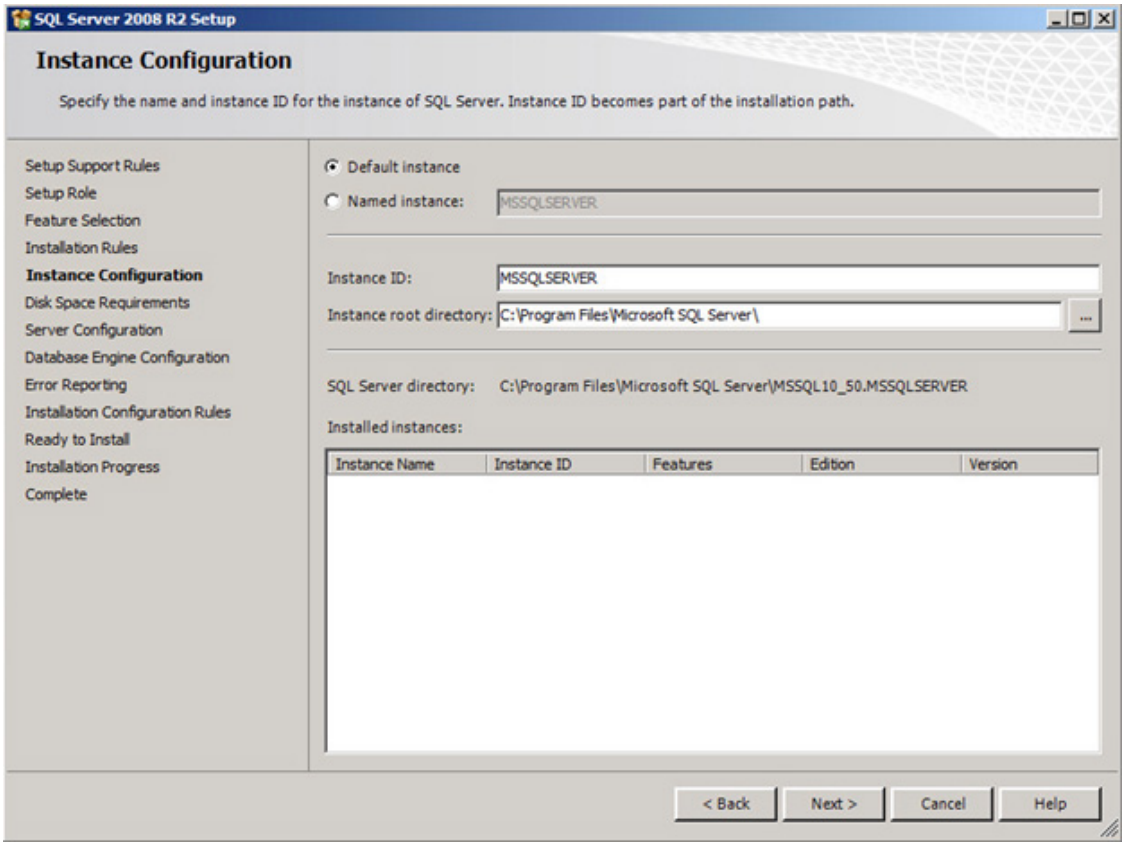
Note The Windows firewall issue was addressed in step 13.

25. Select SQL Server Feature Installation and click Next.
26. Under Instance Features, select only Database Engine Services.
27. Under Shared Features, select Management Tools - Basic and Management Tools - Complete. Click Next.



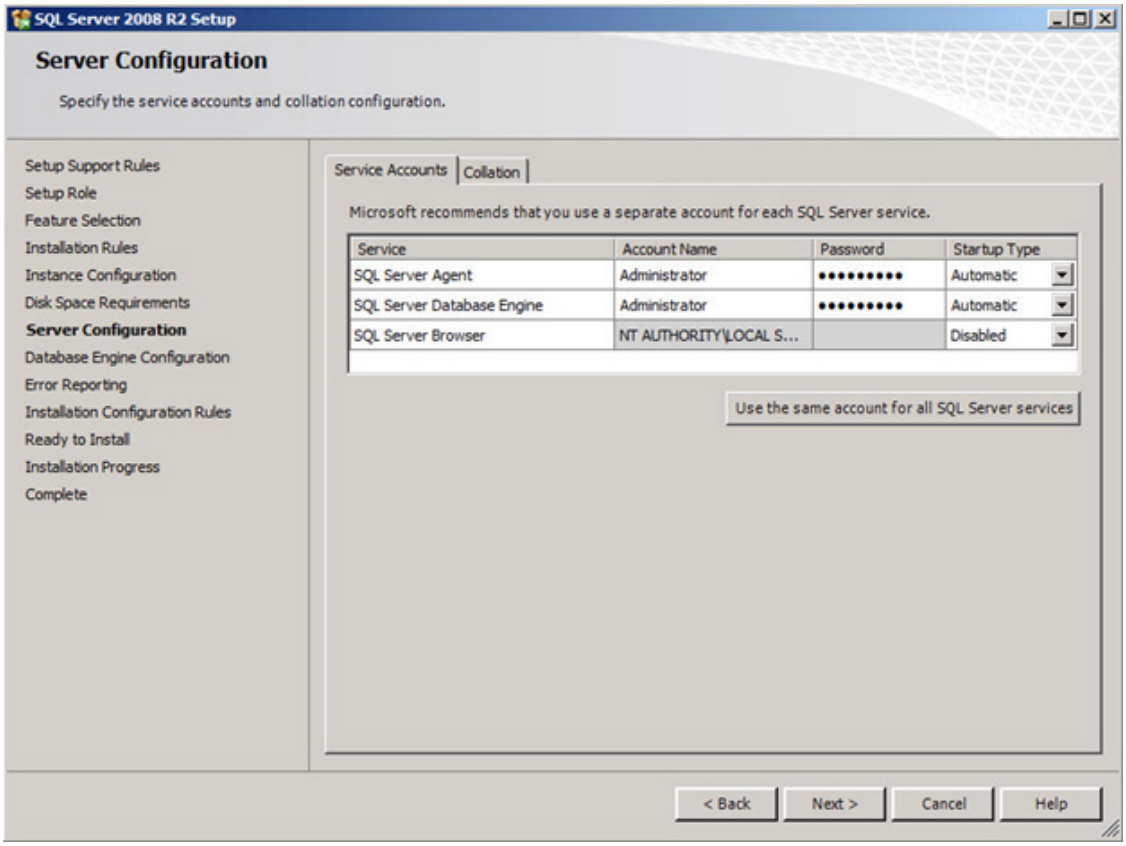
28. Click Next.

29. Keep Default Instance selected. Click Next.

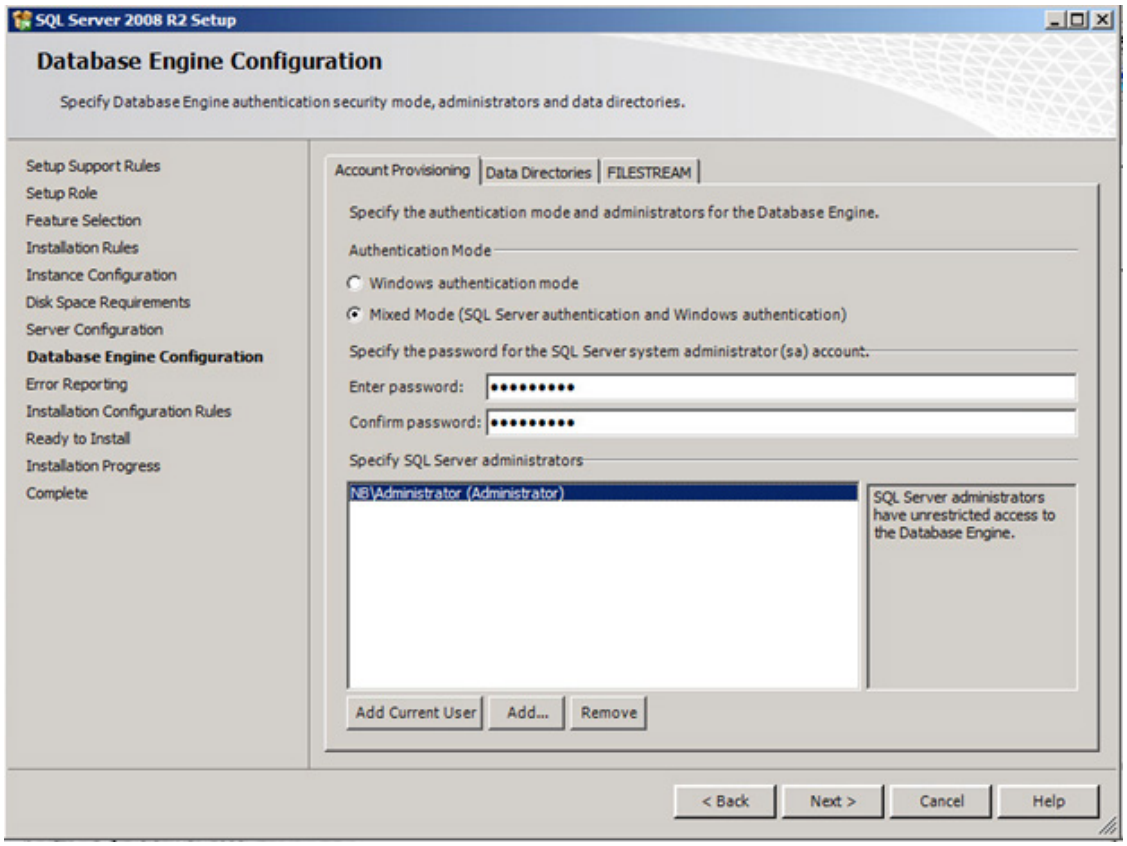


30. Click Next for Disk Space Requirements.

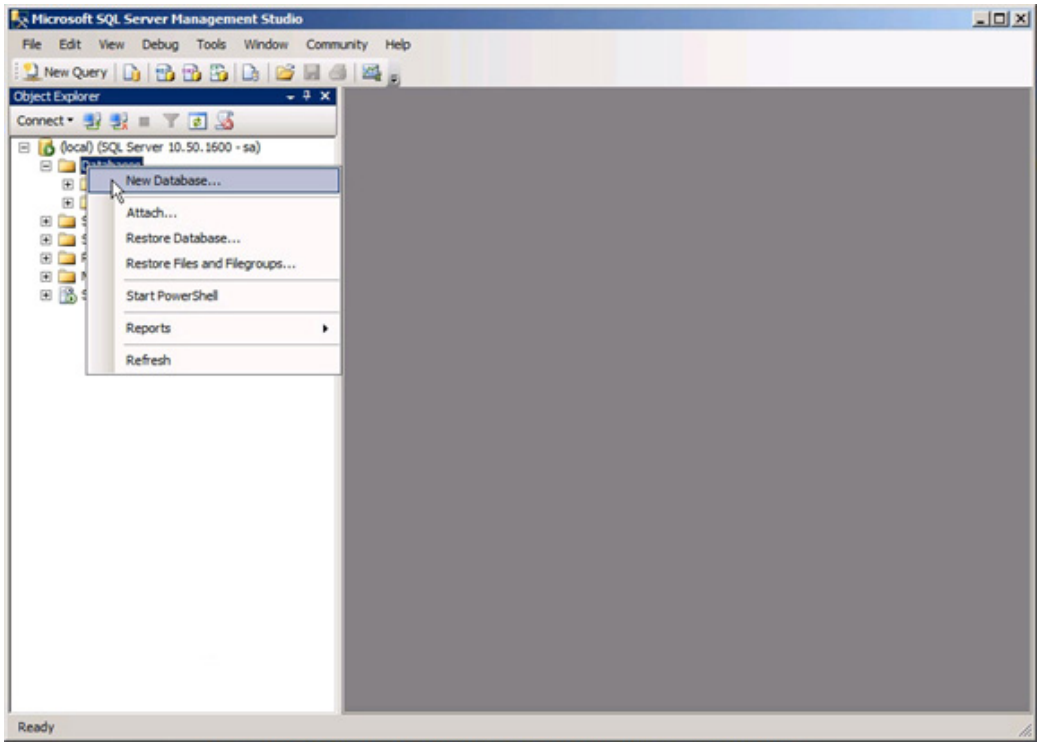
31. For the SQL Server Agent service, click in the first cell in the Account Name column and then click <<Browse…>>.
32. Enter the local machine administrator name (for example, `systemname\Administrator`), click Check Names, and click OK.
33. Enter the administrator password in the first cell under Password.
34. Change the startup type for SQL Server Agent to Automatic.
35. For the SQL Server Database Engine service, select Administrator in the Account Name column and enter the administrator password again. Click Next.



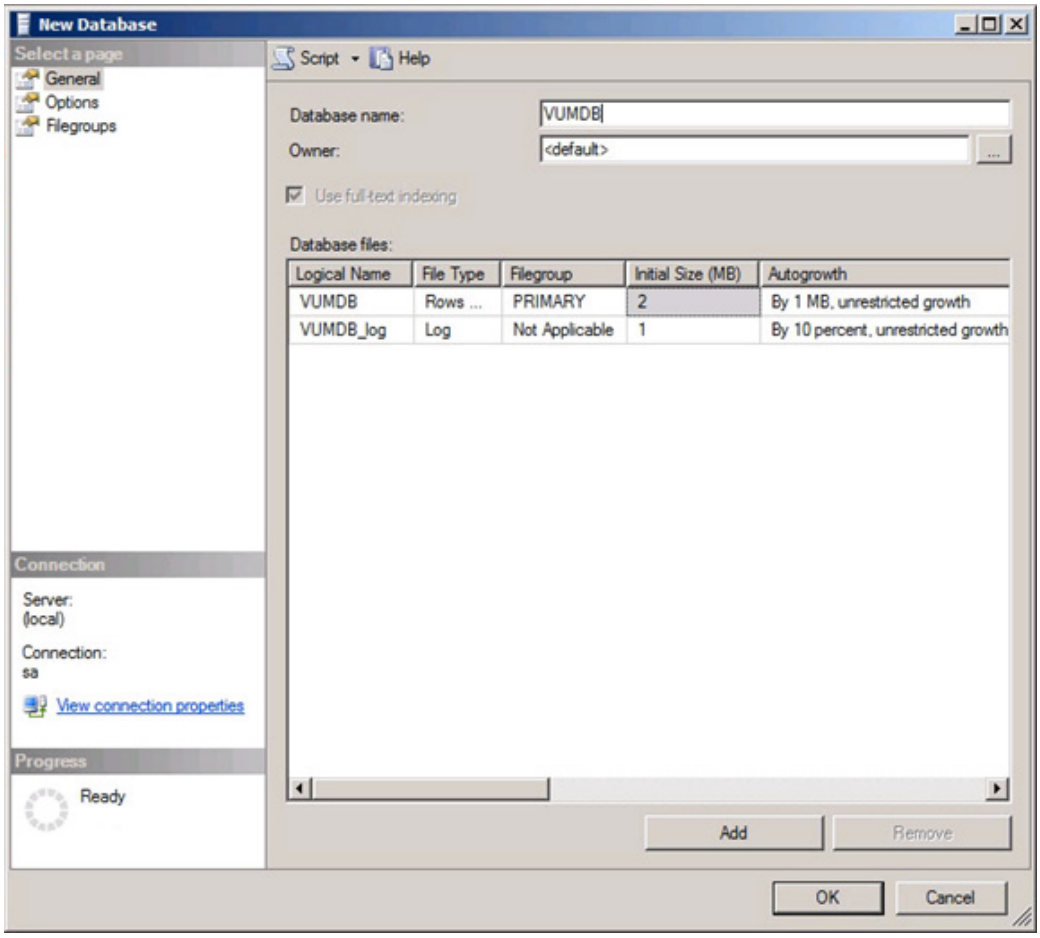
36. Select Mixed Mode (SQL Server Authentication and Windows Authentication). Enter and confirm the password for the SQL Server system administrator (sa) account, click Add Current User and click Next.



37. Choose whether to send error reports to Microsoft. Click Next.
38. Click Next.
39. Click Install.
40. After the installation is complete, click Close to close the SQL Server installer.
41. Close the SQL Server Installation Center.
42. Install all available Microsoft Windows updates by navigating to Start > All Programs > Windows Update.
43. Open the SQL Server Management Studio by selecting Start > All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio.
44. Under Server Name, select the local machine name. Under Authentication, select SQL Server Authentication. Enter `sa` in the Login field and enter the `sa` password. Click Connect.
45. In the left pane, right-click Databases.
46. Select New Database.



47. Under Database Name, enter VUMDB.



48. Click OK.
49. Close Microsoft SQL Server Management Studio.
50. Disconnect the Microsoft SQL Server 2008 R2 ISO from the SQL Server VM.

Build VMware vCenter Update Manager VM

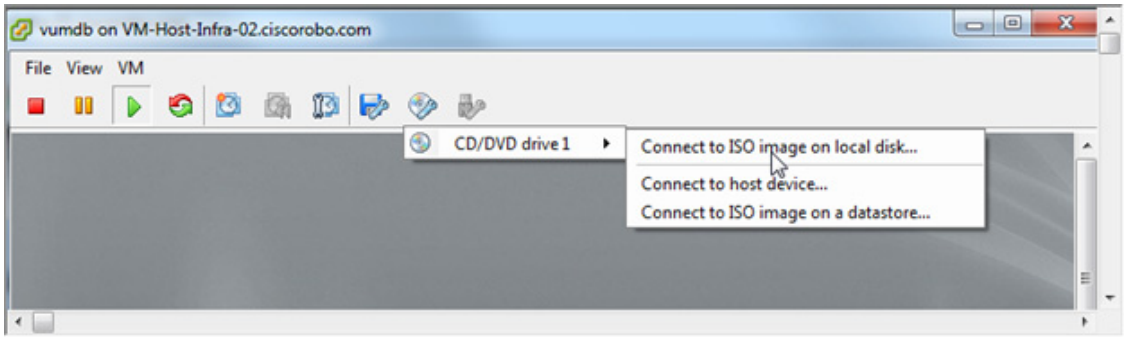
To build the VMware vCenter VUM, complete the following steps:

1. Using the instructions for building a SQL Server VM provided in the section Build Microsoft Windows 2008 R2 VM build a VMware vCenter VM with the following configuration in the `<<var_ib-mgmt_vlan_id>>` VLAN:
   - 4GB RAM
   - Two CPUs
   - One virtual network interface
   - 125GB hard disk
2. Start the VM, install VMware Tools, and assign an IP address and host name to it.

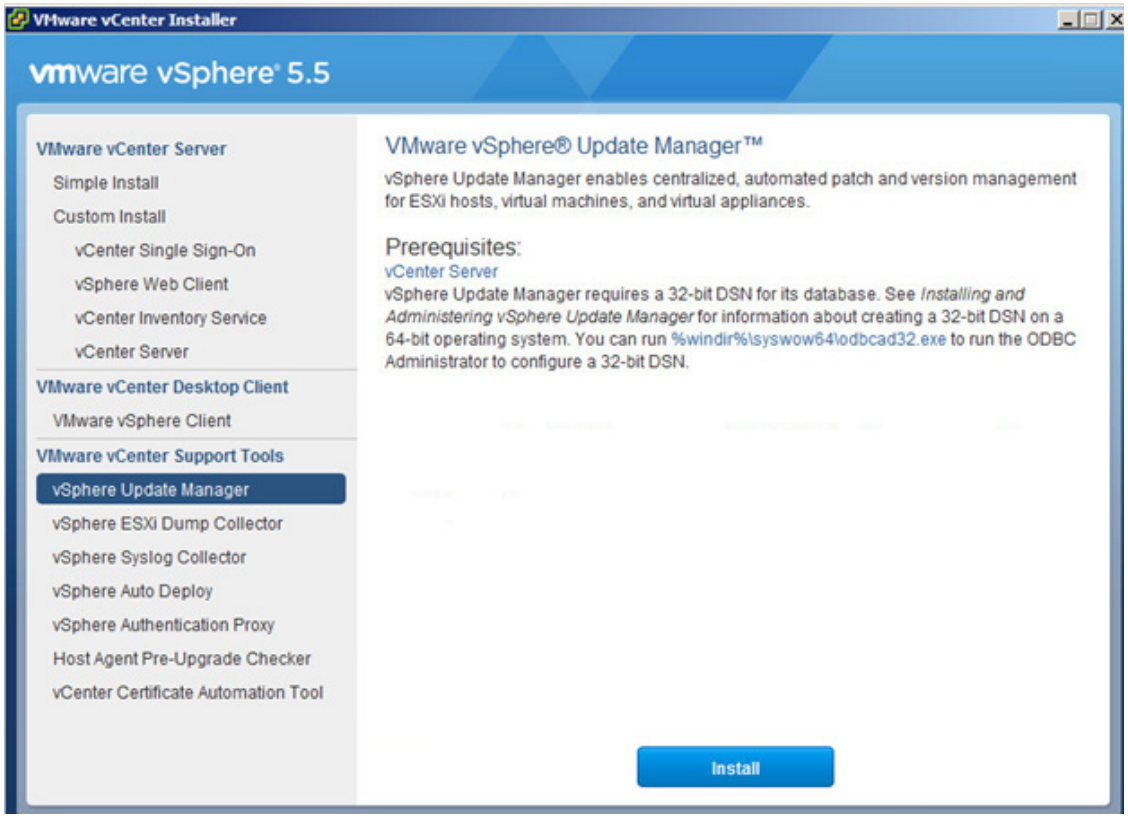
Set up VMware vCenter Update Manager VM

To set up the newly built VMware vCenter Update Manager VM, complete the following steps:

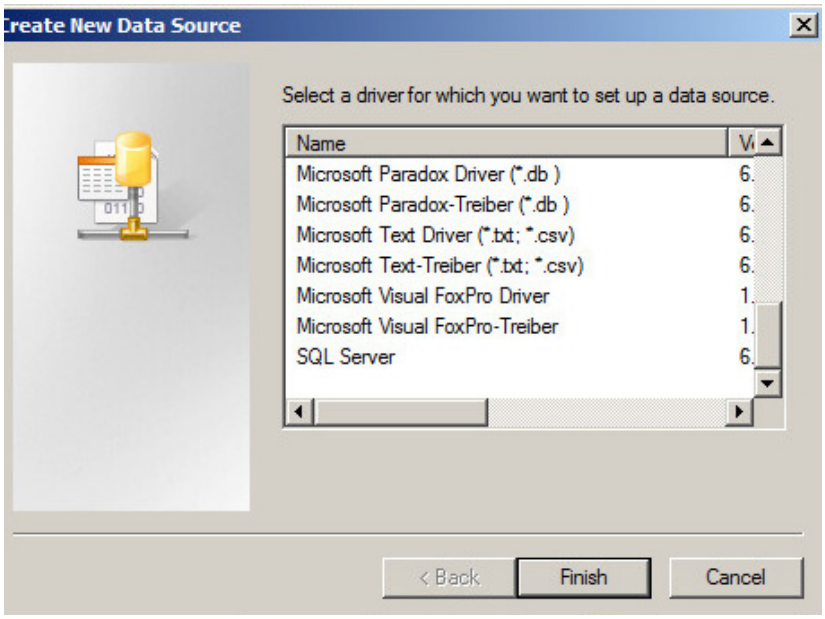
1. Connect the vSphere VIM Installation iso to the CDROM of the VUM VM.



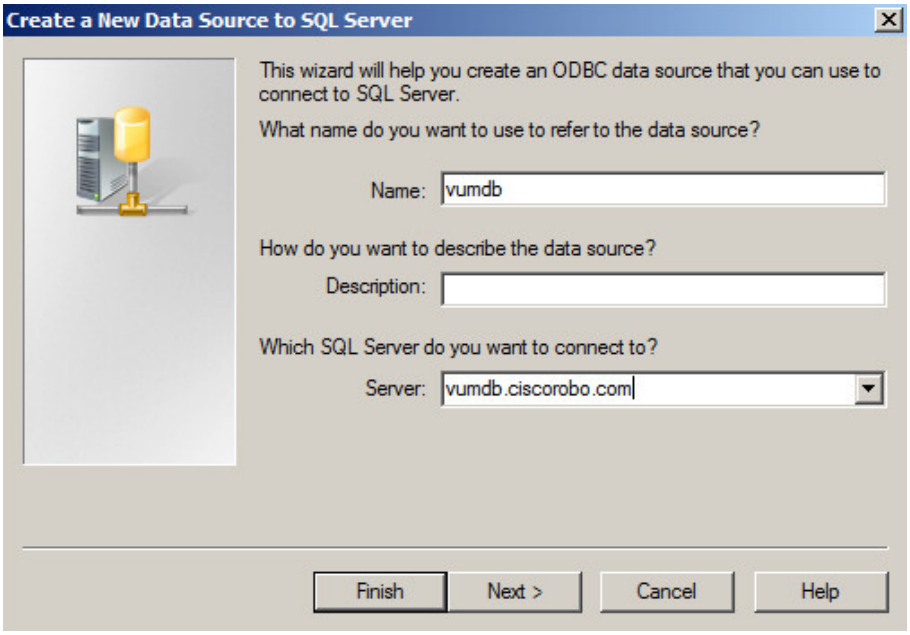
2. Run Setup.exe from the CDROM in the VUM VM. Select vSphere Update Manager.
3. Click the link for %windir%\syswow64\odbcad32.exe.



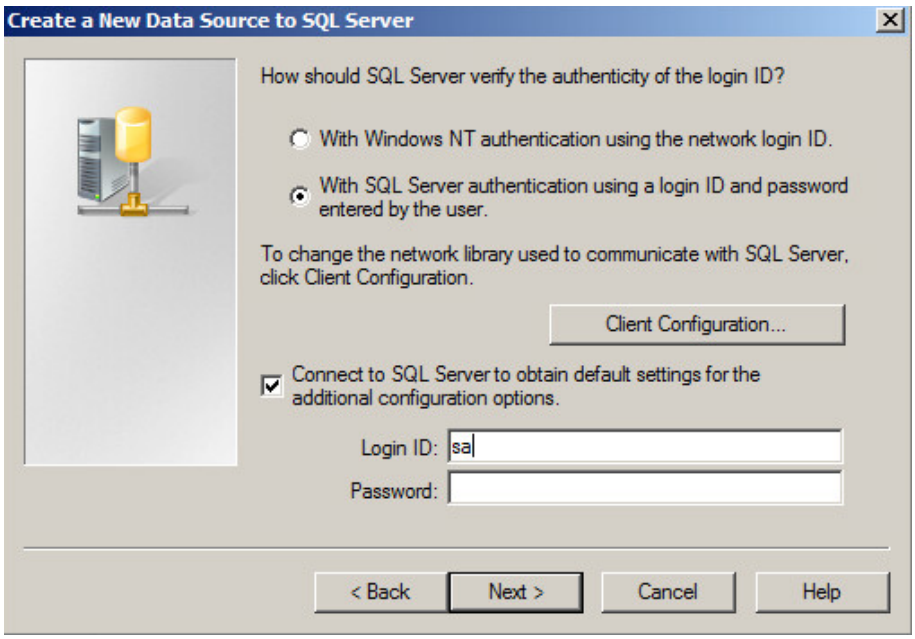
4. Select the System Tab. Click Add.
5. On the Create New Data Source dialog box, choose SQL Server and click Finish.



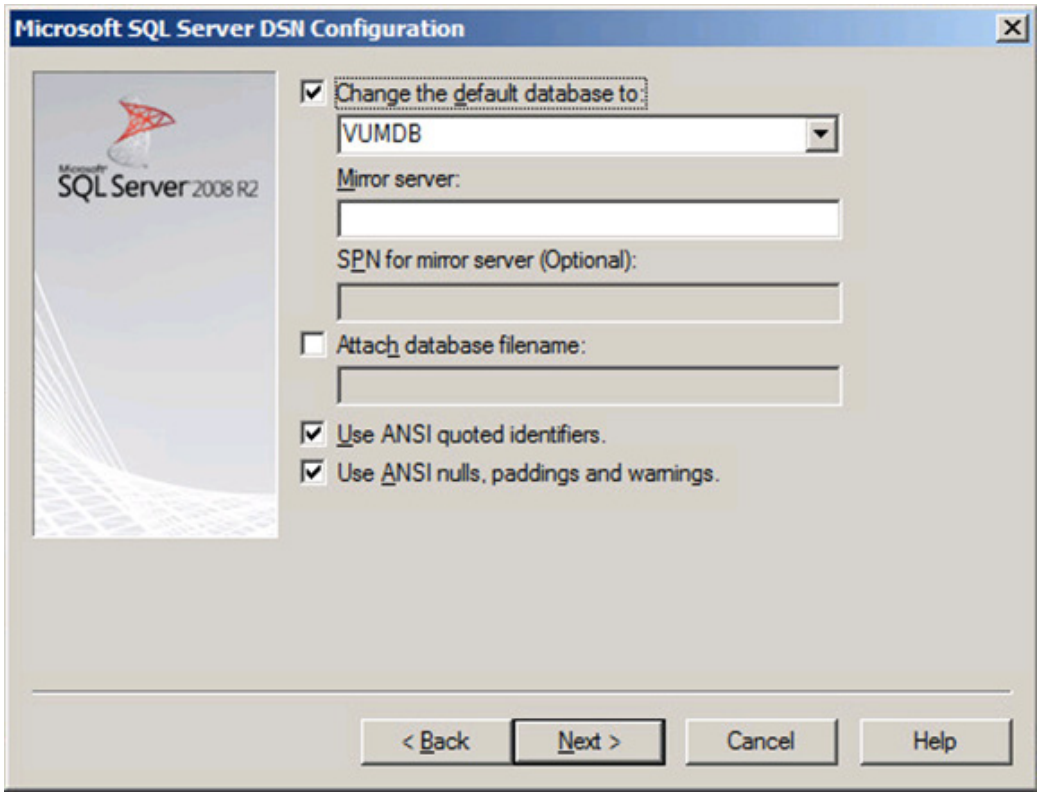
6. In the Create a New Data Source to SQL Server dialog box, enter the name ("vumdb") and Server FQDN and click Next.



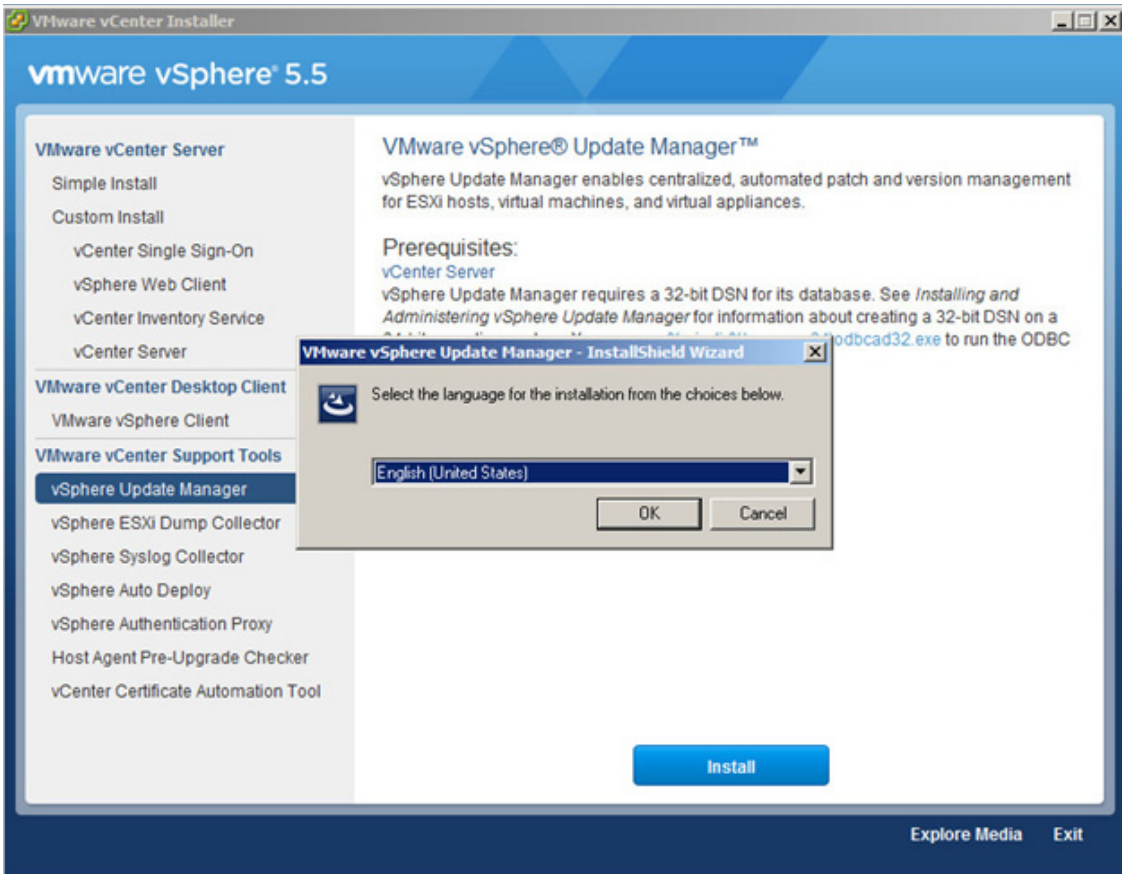
7. Click OK.
8. In the System Tab, select VUMDB and click Configure.
9. Click Next.
10. On the Microsoft SQL Server DSN Configuration dialog, select With SQL Server authentication. For Login ID: enter `sa`. For Password: enter the `sa` password. Click Next.



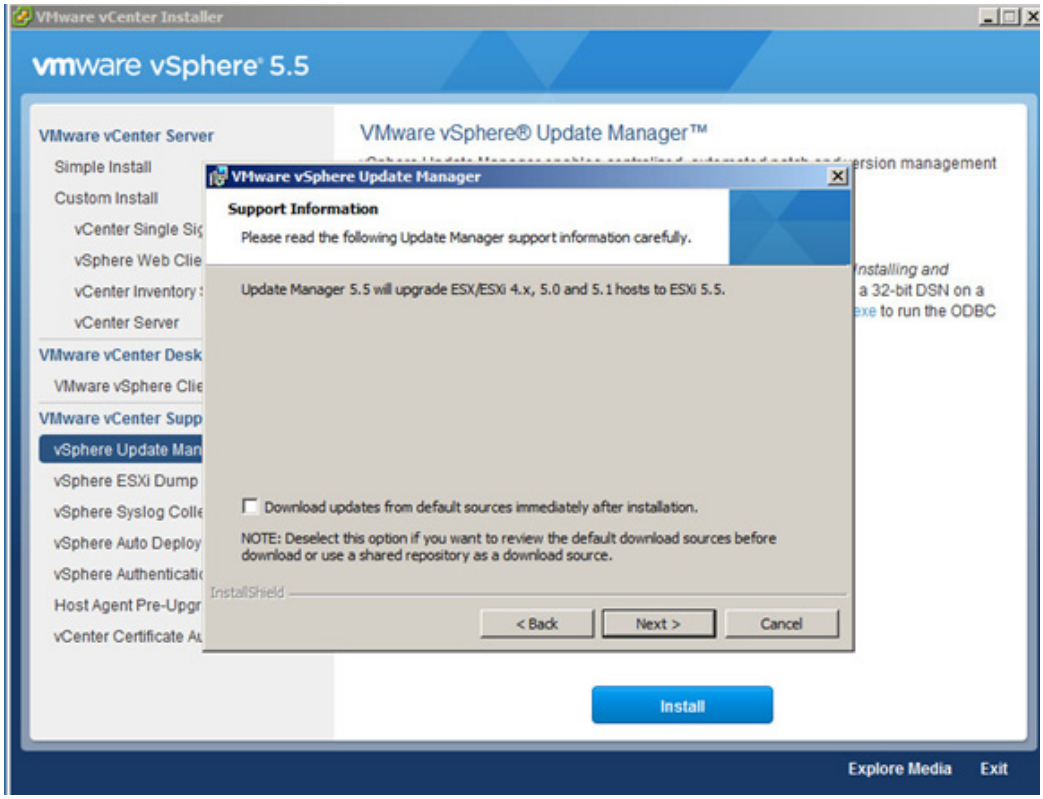
11. Select Change the default database to: and select VUMDB. Click Next.



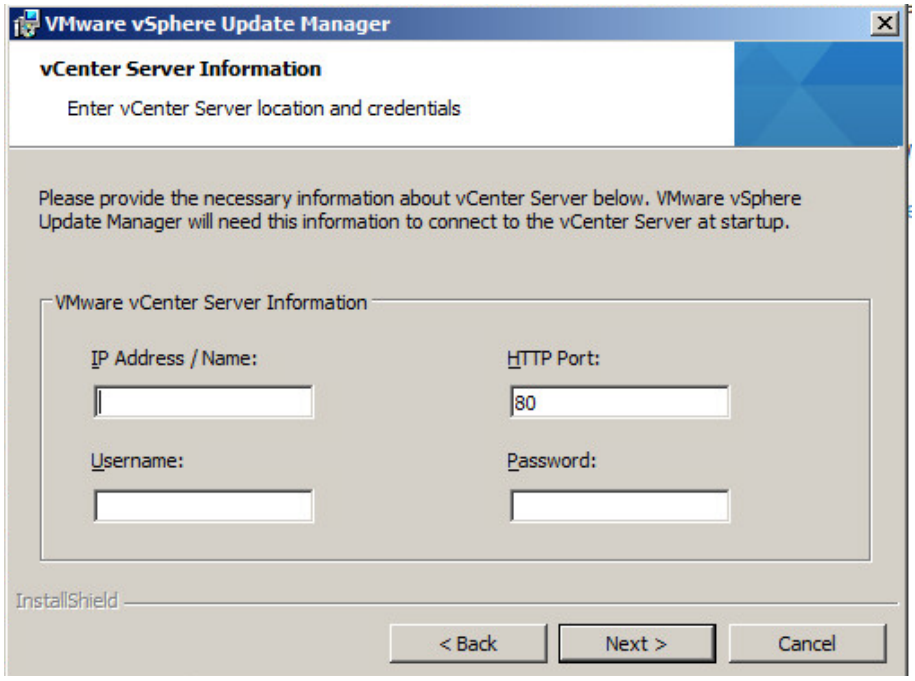
12. Click Finish.
13. On the VMware vCenter Installer dialog box, confirm that vSphere Update Manager is still selected and click Install. Then click OK.



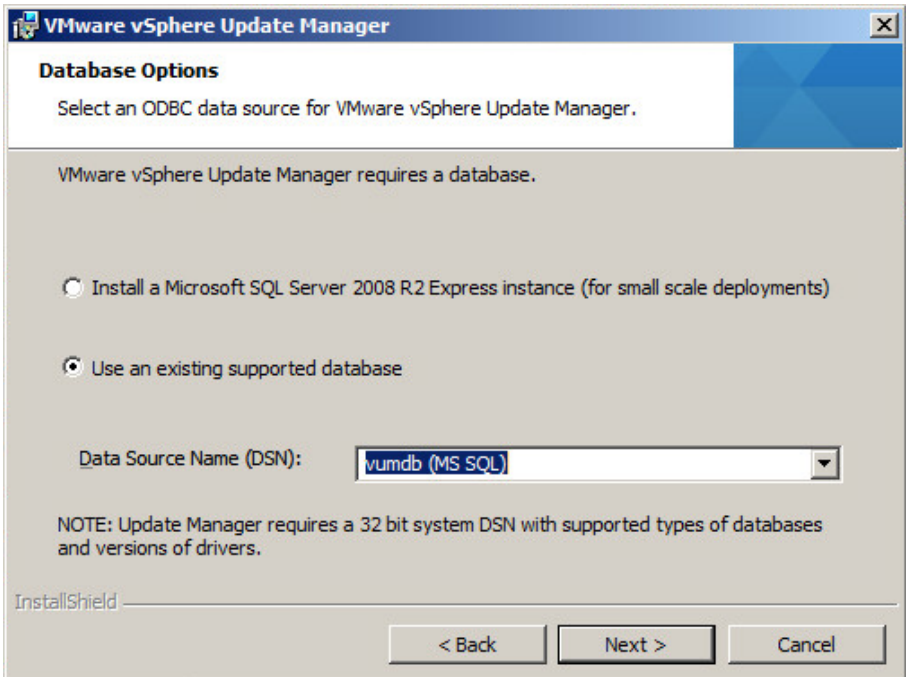
14. Select English and click OK.



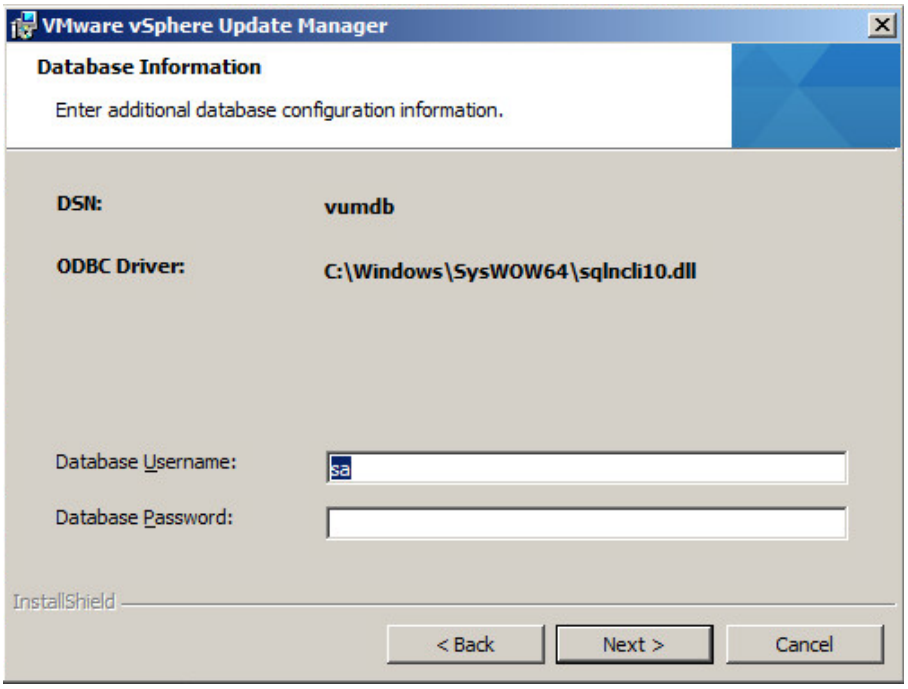
15. On the InstallShield wizard, click Next.
16. Select I accept the terms in the license agreement and click Next.
17. Clear the Download updates from default sources immediately after installation checkbox.
18. Click Next.
19. In the vCenter Server Information window, enter the FQDN of the vCenter server, the username root and the root password for the vCenter Server. Click Next.



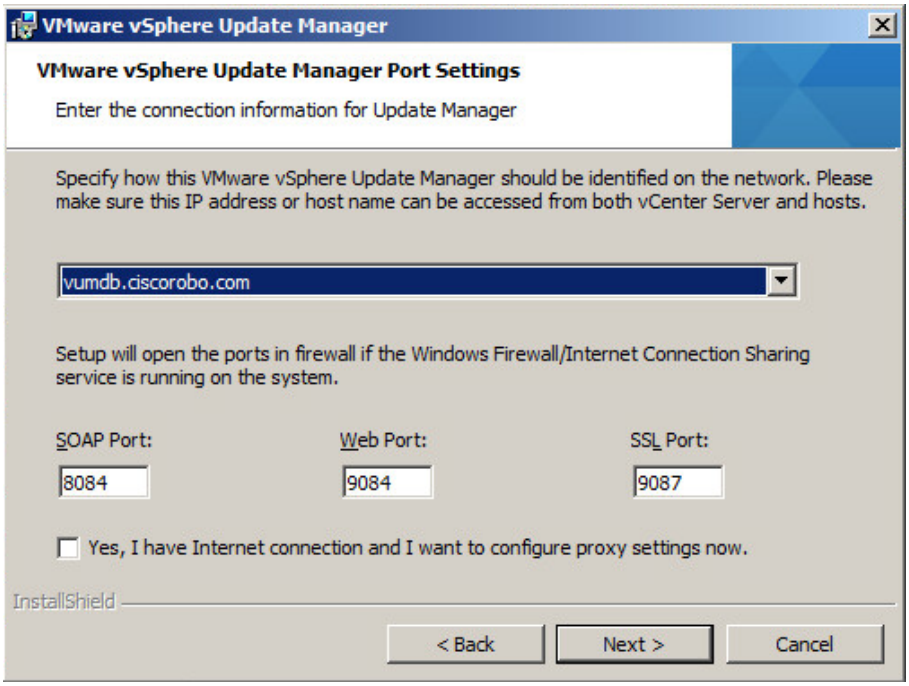
20. On the Database Options, select Use an existing supported database. For Data Source Name, choose vumdb (MS SQL). Click Next.



21. Confirm `sa` is entered for the Database Username. For the Database Password, enter the password for `sa`. Click Next.



22. Specify the Update Manager Port Settings as shown below and Click Next



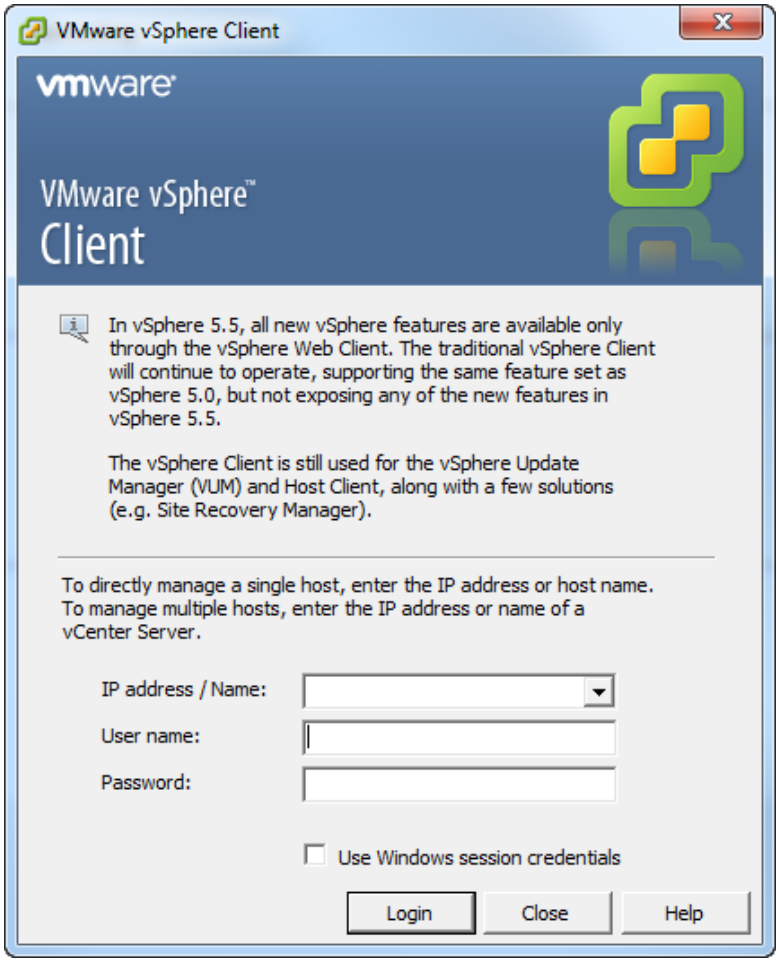
23. Click Next.
24. Click Next.
25. Click Install.
26. Click Finish.

Set Up VMware vCenter Client

VMware vCenter web client can be used to manage VMware Infrastructure. To directly manage a single ESXi server, VMware vSphere Client has to be installed. Following procedure explains the steps to login to a ESXi server using vSphere Client.

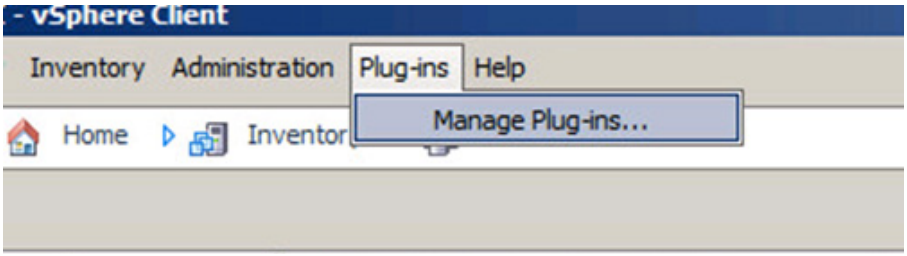
To set up the VMware vCenter client, complete the following steps:

27. Execute the vCenter Client and connect to the vCenter server by entering the IP address/ESXi hostname, user and password. Click Login.



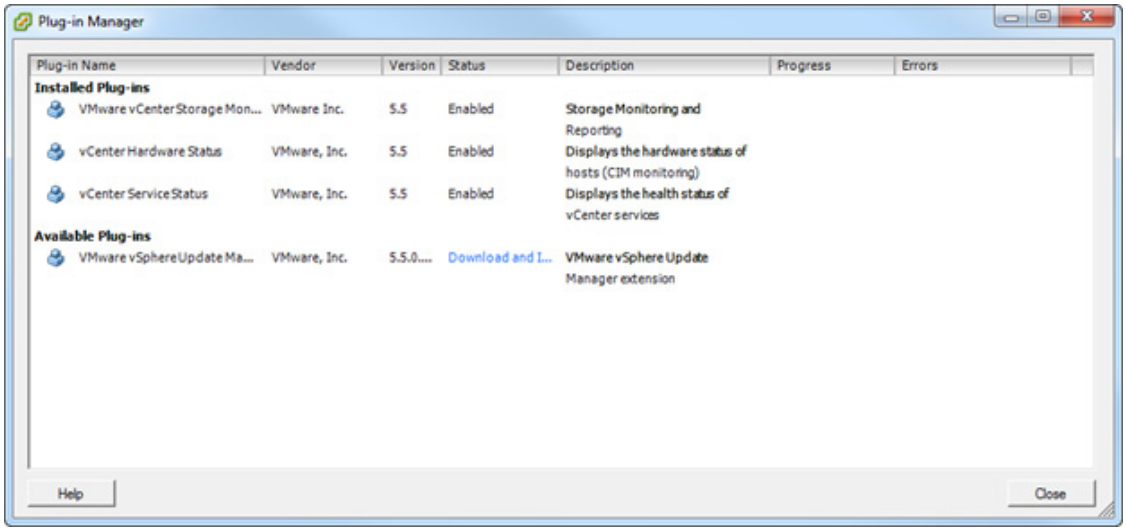
28. In the Security Warning dialog box, select the "Install this certificate…" option and click Ignore.

29. In the Plug-ins menu, click Manage Plug-ins.



30. In the Plug-in Manager dialog box, under Available Plug-ins, for the VMware vSphere Update Manager Extension, click the Download and Install link.

Note If it is already installed, it will show under Installed Plug-ins. If it is already installed, click Close. If the Update Manager Extension is shown under available Plug-ins, click Download and install link.



31. If a Security Warning dialog box occurs, select Run.
32. Click OK.
33. In the InstallShield wizard for VMware vSphere Update Manager, click Next.
34. Click Next.
35. Select the I accept the terms in the license agreement option and click Next.
36. Click Install.
37. Click Finish.

Download Updated Cisco VIC eNIC and fNIC Drivers

To download the Cisco virtual interface card (VIC) eNIC and fNIC drivers, complete the following steps:

Note The eNIC version used in this configuration is 2.1.2.50, and the fNIC version is 1.6.0.10.

1. Open a web browser on the management workstation and navigate to:
   - VMware ESXi 5.x Driver for Cisco enic
   - VMware ESXi 5.x Driver for Cisco fnic
2. Log in and download the eNIC and fNIC drivers.
3. Extract the offline zip bundle files from the downloaded zip files:

   Navigate to `enic-2.1.2.50_enic-2.1.2.50-1856276.zip> enic-2.1.2.50_esx55-offline_bundle-1906033.zipNavigate to fnic_driver_1.6.0.10_esx55-1897613.zip> fnic_driver_1.6.0.10_esx55-offline_bundle-1897613`
4. Document the saved location.

Load Updated Cisco VIC eNIC and fNIC Drivers

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

Note On enabling VMware Update Manager, all the latest available critical and optional patches will be installed onto the ESXi hosts. Verify that the patches that you are going to install on the ESXi hosts are supported as per NetApp Interoperability Matrix Tool.

Note Make sure VMs are not connected to any removable device

To load the updated versions of the eNIC and fNIC drivers for the Cisco VIC, complete the following steps for the hosts on each vSphere Client:

1. From the vSphere Client, Click Home, Update Manager.
2. Select the Patch Repository tab.
3. Click Import Patches.

4. Click Browse and navigate to the location of the enic offline bundle file.
5. Select the offline bundle file for the enic driver, click Open.
6. Click Next. Click Finish.
7. Repeat the steps 2-6 for importing fnic offline bundle.
8. Click Baselines and Groups tab. On the Baselines pane, click Create to create a new Base line.
9. Enter the name of the Patch and choose Host Extension for the Baseline Type. Click Next.
10. Choose the enic and fnic offline bundle and add it using the down arrow button. Click Next.
11. Click Finish.
12. Click Home, Hosts and Clusters button.
13. Right-click on the FlexPod_Management cluster and select Edit Settings.
14. Clear the Turn On vSphere HA checkbox.
15. Click Home > Hosts and Clusters. Select the first ESXi host.
16. Click the Update Manager tab.
17. Click Attach on the top right corner of the Update Manager pane.
18. Choose the Host Extension baseline which is created in the preceding step. Click Attach.
19. Click Remediate. Accept all the defaults. Click Finish.
20. Repeat the steps 15-19 to load the enic and fnic drivers for another ESXi host.
21. Click Home, Hosts, and Clusters button.
22. Right-click the FlexPod_Management cluster and select Edit Settings.
23. Select the Turn On vSphere HA checkbox.

Set Up the Cisco Nexus 1000V Switch using Cisco Switch Update Manager

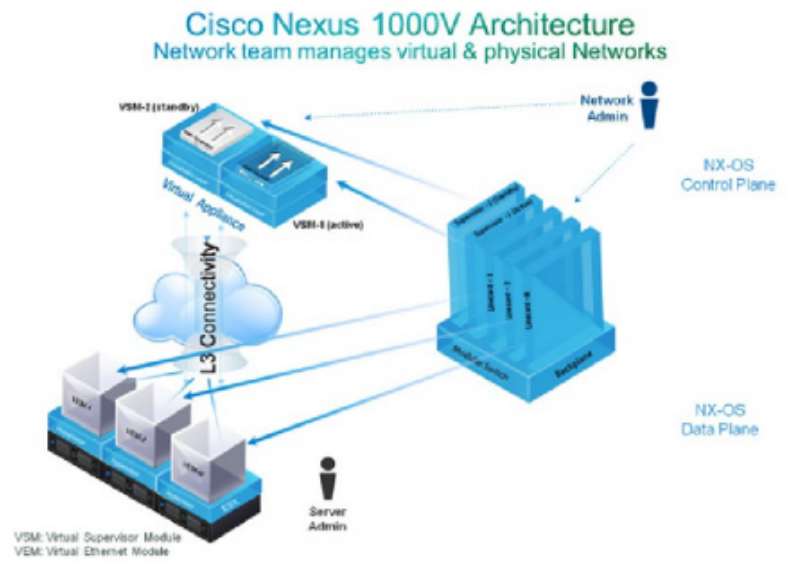
Cisco Nexus 1000V

The Cisco Nexus 1000V is a distributed virtual switch solution that is fully integrated within the VMware virtual infrastructure, including VMware vCenter, for the virtualization administrator. This solution offloads the configuration of the virtual switch and port groups to the network administrator to enforce a consistent data center network policy. The Cisco Nexus 1000V is compatible with any upstream physical access layer switch that is compliant with Ethernet standard, Cisco Nexus switches, and switches from other network vendors. The Cisco Nexus 1000V is compatible with any server hardware that islisted in the VMware Hardware Compatibility List (HCL).

The Cisco Nexus 1000Vhas the following components:

- Virtual Supervisor Module (VSM)-The control plane of the switch and a VM that runs Cisco NX-OS.
- Virtual Ethernet Module (VEM)-A virtual line card that is embedded in each VMware vSphere (ESXi) host. The VEM is partly inside the kernel of the hypervisor and partly in a user-world process, called the VEM Agent.

Figure 6 Cisco Nexus 1000V Architecture

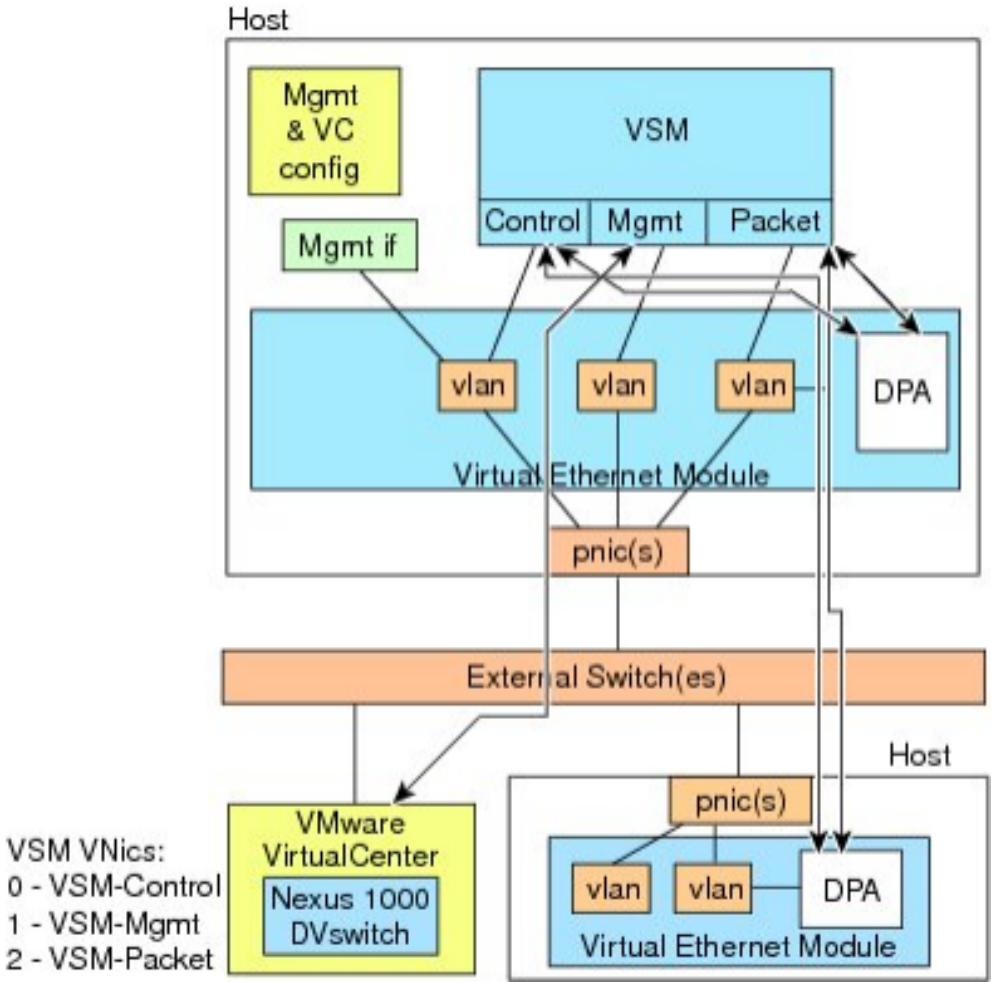


Layer 3 control mode is the preferred method of communication between the VSM and the VEMs. In Layer 3 control mode, the VEMs can be in a different subnet than the VSM and from each other. Active and standby VSM control ports should be Layer 2 adjacent. These ports are used to communicate the HA protocol between the active and standby VSMs. Each VEM needs a designated VMkernel NIC interface that is attached to the VEM that communicates with the VSM. This interface, which is called the Layer 3 Control vmknic, must have a system port profile applied to it (see System Port Profiles and System VLANs), so the VEM can enable it before contacting the VSM.

In Layer 2 control mode, the VSM and VEMs are in the same subnet. You can install the VSM and VEMs on different ESXi hosts or on the same ESXi host. This figure shows a VSM and VEM that are running on the same host in Layer 2 control mode.

Figure 7VSM and VEM on the same host in Layer 2 Control mode.

Figure 7 VSM and VEM in Layer 2 Control Mode



Cisco Nexus 1000V can be installed using Cisco Virtual Switch Update Manager.

This section describes the steps involved the installation of Cisco Nexus 1000V using Cisco Virtual Sw Cisco Virtual Switch Update Manager is the graphical user interface (GUI) that you use to install the VSMs in high availability (HA) or standalone mode and the VEMs on ESXi hosts. The Cisco Virtual Switch Update Manager graphical user interface (GUI) is an integral part of VMware vSphere Web Client and it can only be accessed by logging into VMware vSphere Web Clientitch Update Manager.

Layer 3 control mode is the preferred method of communication between the VSM and VEMs. This figure shows an example of a Layer 3 control mode topology where redundant VSM VMs are installed. The software for the primary VSM is installed on ESXi 1, and the software for the secondary VSM is installed on ESXi 2.

Summary Steps

Make sure that all of the Cisco Virtual Switch Update Manager requirements have been met before you install Cisco Virtual Switch Update Manager.

For details, refer to the Cisco Nexus 1000V documents.

1. Make sure that all of the VMware software requirements have been met.

Note Cisco Nexus 1000V Release 5.2(1)SV3(1.x) supports ESXi 5.5, ESXi 5.1 and ESXi 5.0 versions. It does not support earlier versions

The Cisco Nexus 1000V installation using Cisco VirtualSwitch Update Manager hasthe following prerequisites:

- You have installed Cisco Virtual Switch Update Manager.
- You have installed and prepared vCenter Server for host management using the instructions from VMware.
- You have installed VMware vSphere Web Client.
- You have installed the VMware Enterprise Plus license on the hosts.
- You are familiar with the Cisco Nexus 1000V topology diagram.
- You must create port groups for the Control and Management VLANs on the Cisco Nexus 1000V.
- You must have the Distributed Switch-Create, Extension-Register, Update privilege permissions enabled on the vCenter Server.

2. Gather the required information for the installation.

   Cisco Virtual Switch Update Manager requires information about your Cisco Nexus 1000V for VMwaredeployment. Cisco Virtual Switch Update Manager uses this information to configure the VSMs and VEMs during the installation and deployment

   The following information is required:

   – Name of the datacenter in which the switch will be installed
   – Switch deployment type (whether you are installing the switch as a high availability pair or a single
   – standalone switch)
   – Switch VSM version (the Cisco Nexus 1000V version to be installed)
   – VM port group for the switch's control traffic
   – VM port group for the switch's management traffic
   – Host IP address
   – SVS domain ID (a unique ID for the switch)
   – IP address, subnet mask, and gateway IP address for switch connectivity
   – IP address, subnet mask, and gateway IP address for management
   – Switch name and password

   Obtain the following about the switch:

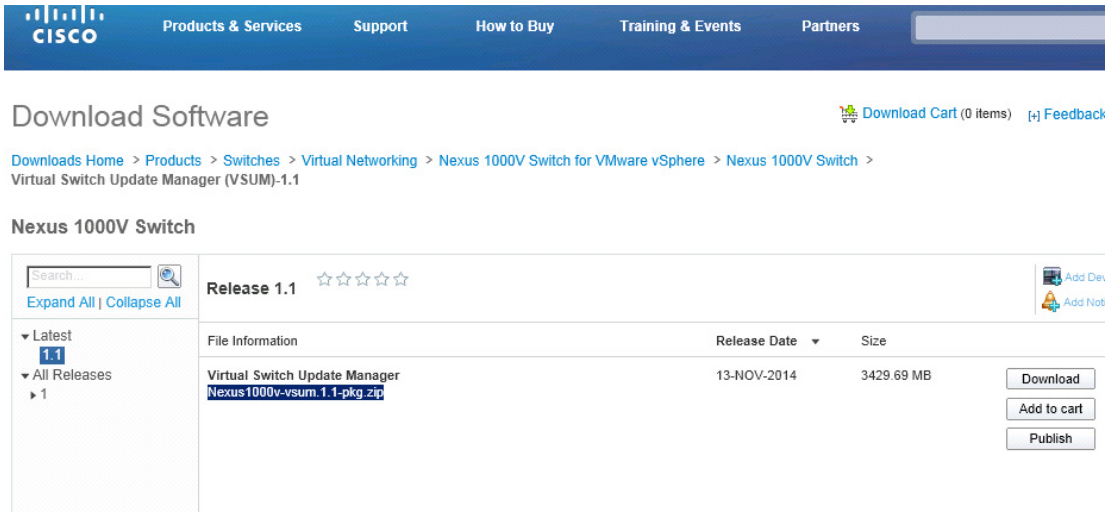
   – VM port group for the control traffic of the switch
   – VM port group for the management traffic of the switch
   – IP address for management
   – Subnet mask
   – Gateway IP address
   – Datacenter in which the switch will be installed
   – Domain ID (a unique ID for the switch)

– Password (the default username is admin)

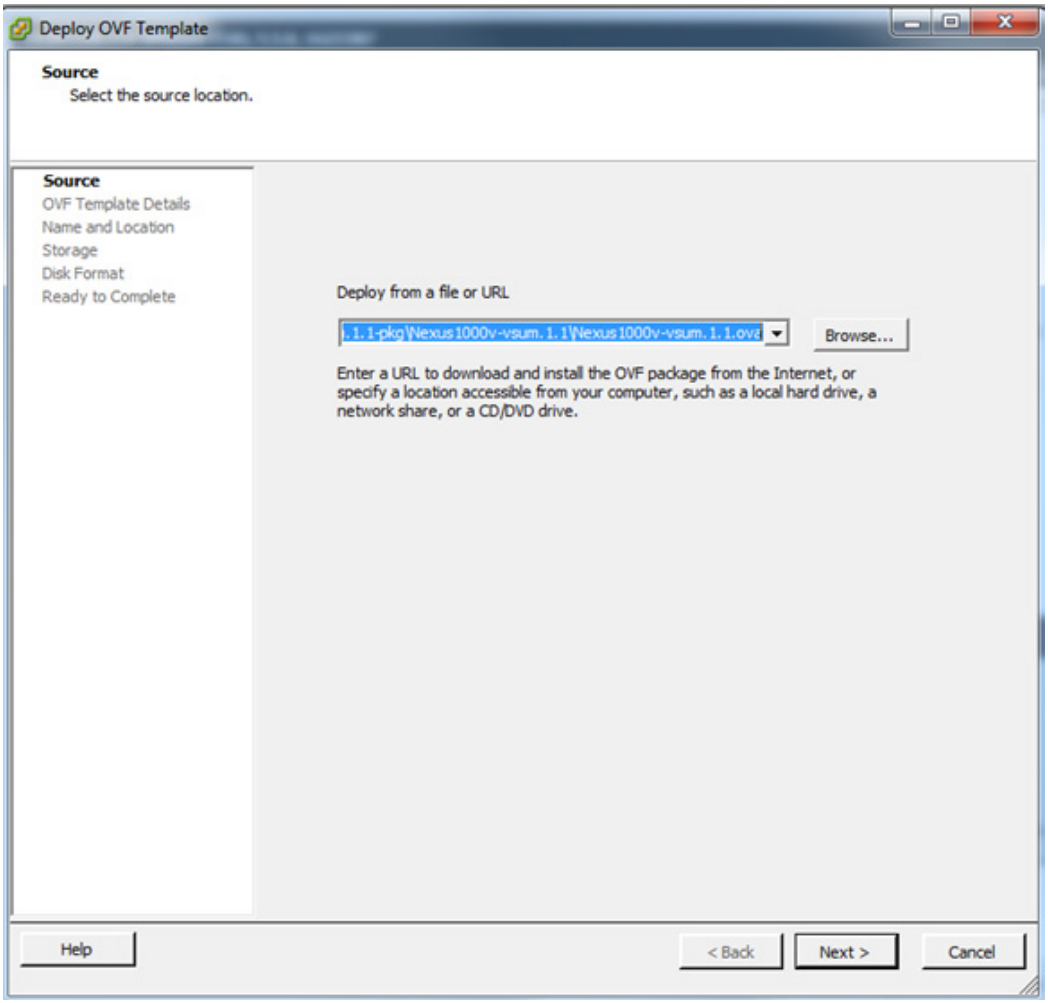
3. Deploy Cisco Virtual Switch Update Manager.
4. Add hosts to the Cisco Nexus 1000V distributed virtual switch (DVS), which installs the Virtual Ethernet Modules (VEMs) and migrates the hosts to the Cisco Nexus 1000V.

Note Prior to installing Cisco Nexus 1000V, Cisco Virtual Switch Update Manager has to be installed.

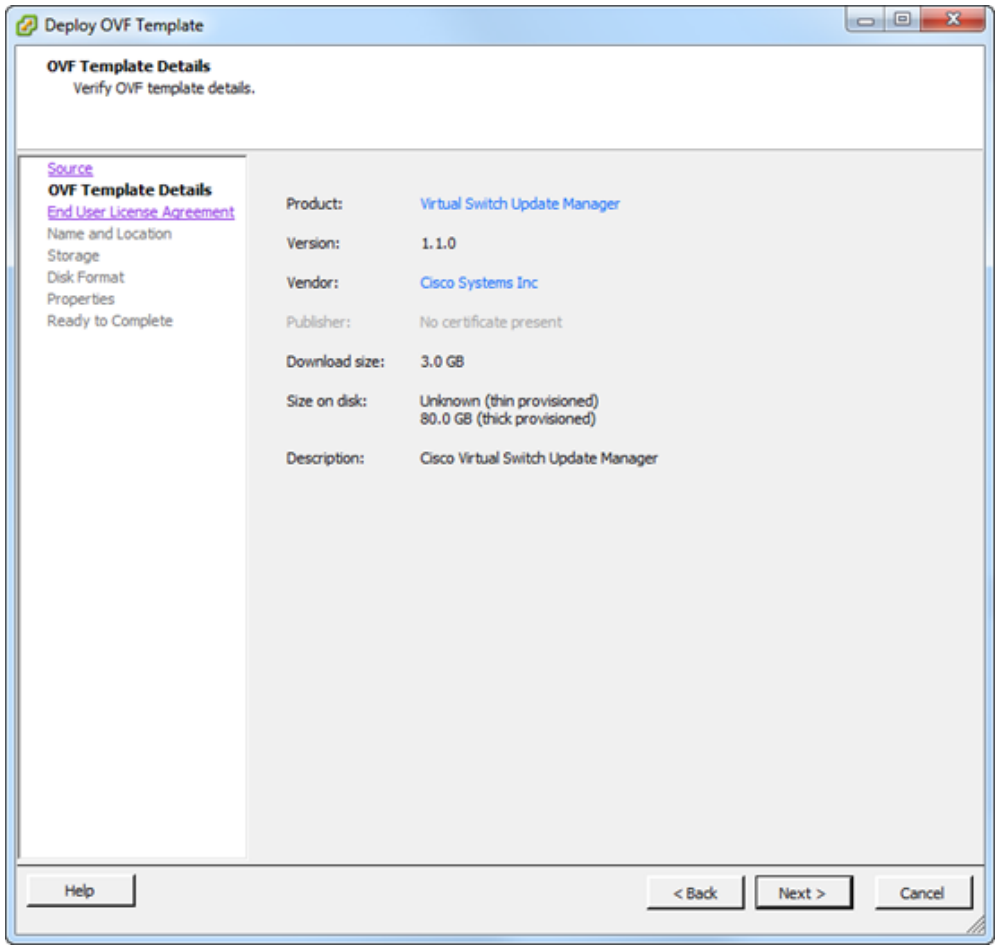
1. Log in and Download the N1kv installation software from www.cisco.com.



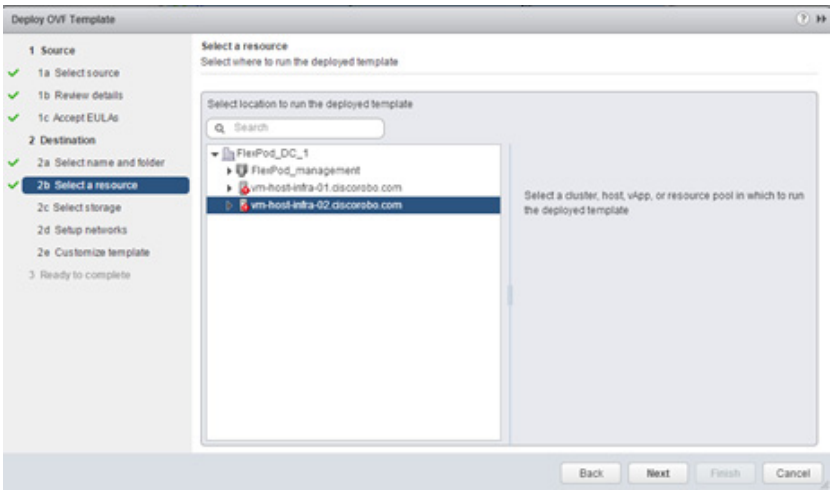
2. Unzip the Package.
3. From the vSphere Client, click File and select Deploy OVF Template. Browse to the unzipped OVA file.



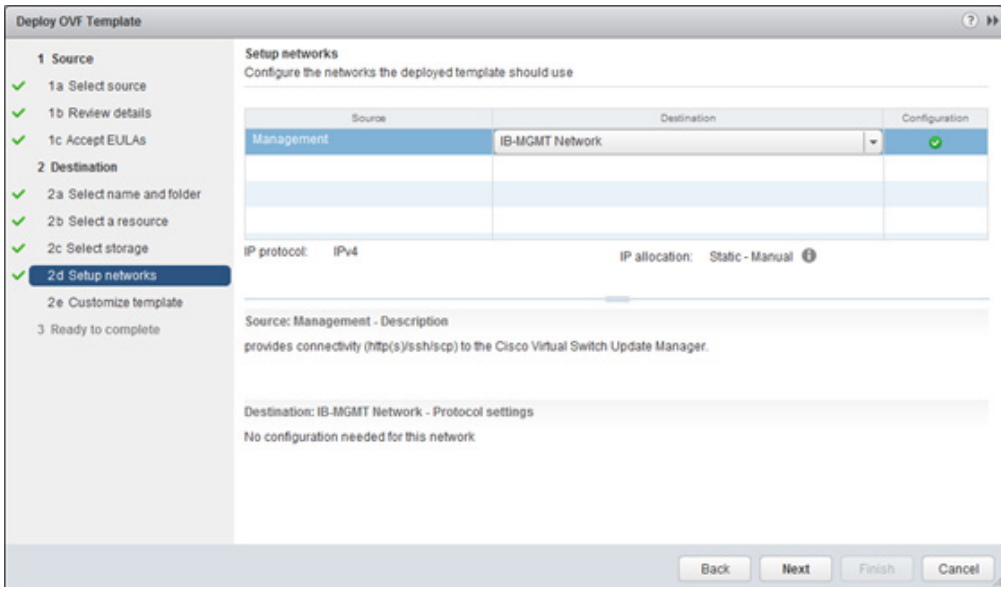
4. Click Next then click Next again.



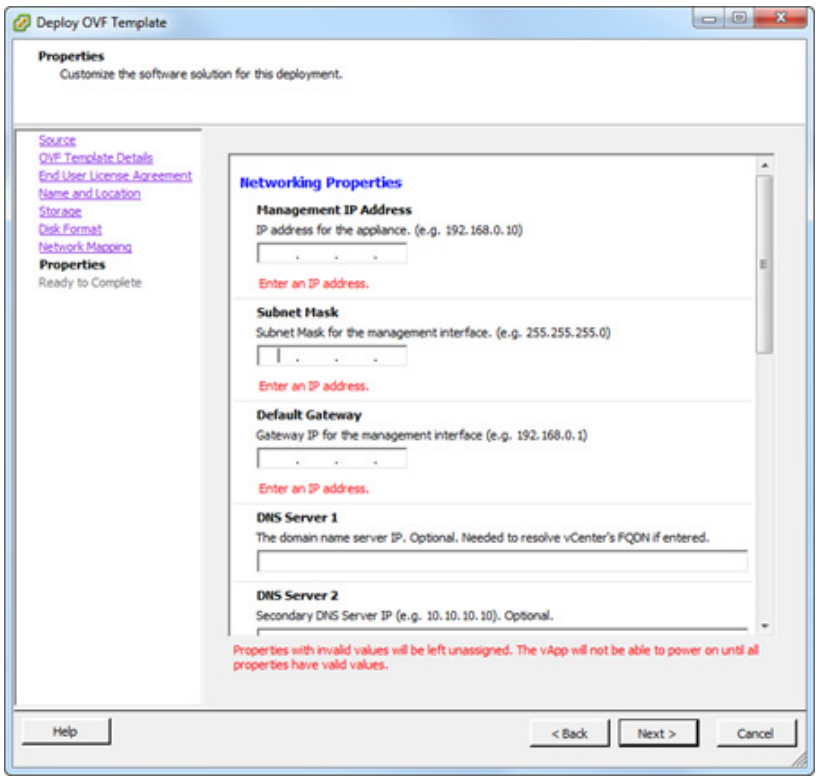
5. Click Next.
6. Review the license agreement, click Next after accepting the EULA.
7. Enter Virtual Machine name and click Next on the Name and Location screen.
8. Select FlexPod_DC-1 as the Host Cluster and click Next.



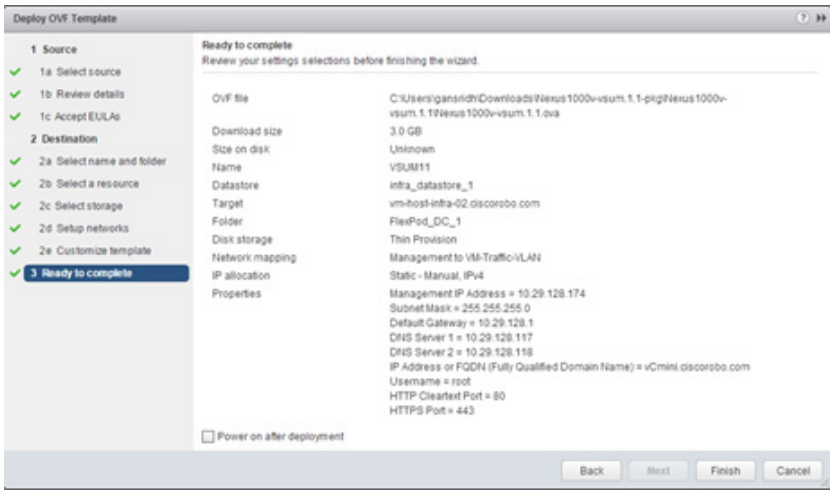
9. Select infra_datatore_1 as the Datastore and click Next.
10. Choose a disk format and click Nex.t
11. For Network Mapping, make sure that the Management mapped to IB-MGMT Network. Then click Next.



12. On the properties screen input `<<var_vsm_mgmt_ip>> <<var_vsm_mgmt_mask>> <<var_vsm_mgmt_gateway>> <<var_DNS>> <<var_Vcenter_ip>>` and login information for the VCenter For domain accounts do not use domainname\user account format . Accept default ports and click Next.
13. Select the virtual disk format and the datastore (infra_datastore_1) and click Next.
14. Select the network settings for VSUM management and click Next.
15. Enter the deployment properties information such as IP address. Expand the vCenter properties to enter the Make sure to scroll down and enter all the required data and then click Next.



16. Review the setting selections and click Finish to create Cisco VSUM server.



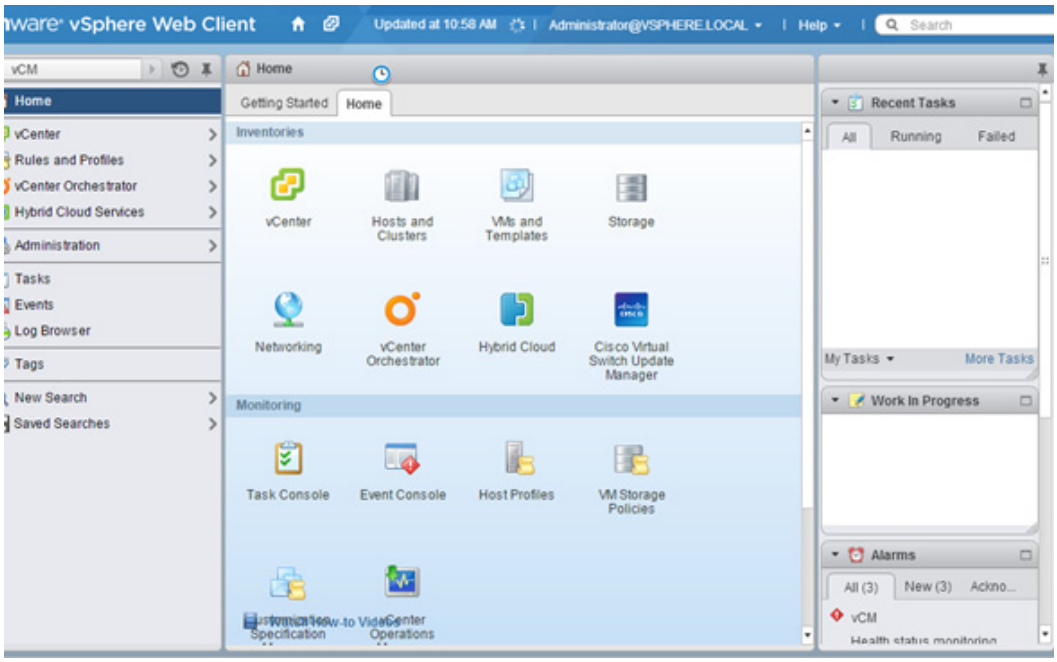
17. Wait for the deployment of VM to complete.

18. Power the Cisco VSUM Virtual Machine and wait until the VM is booted successfully. After the VM boots in a few minute the Plugin is registered. Validate the plugin in the vSphere client by clicking Plug-ins, manage plug-ins in the top menu bar and look under available plug-ins.

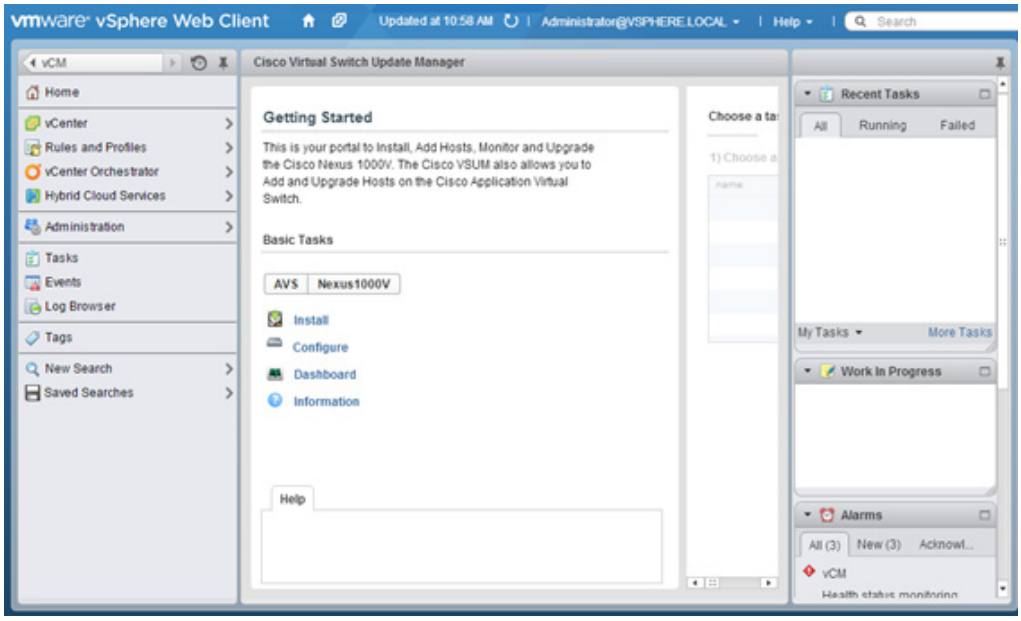
Install the VSM through the Cisco Virtual Switch update Manager

On the machine where you will run the browser for the VMware vSphere Web Client, you should have installed Adobe Flash as well the Client Integration plugin for the web client. The plug-in can be downloaded from the lower left corner of the web client login page. Log out of vCenter and continue with step 1.

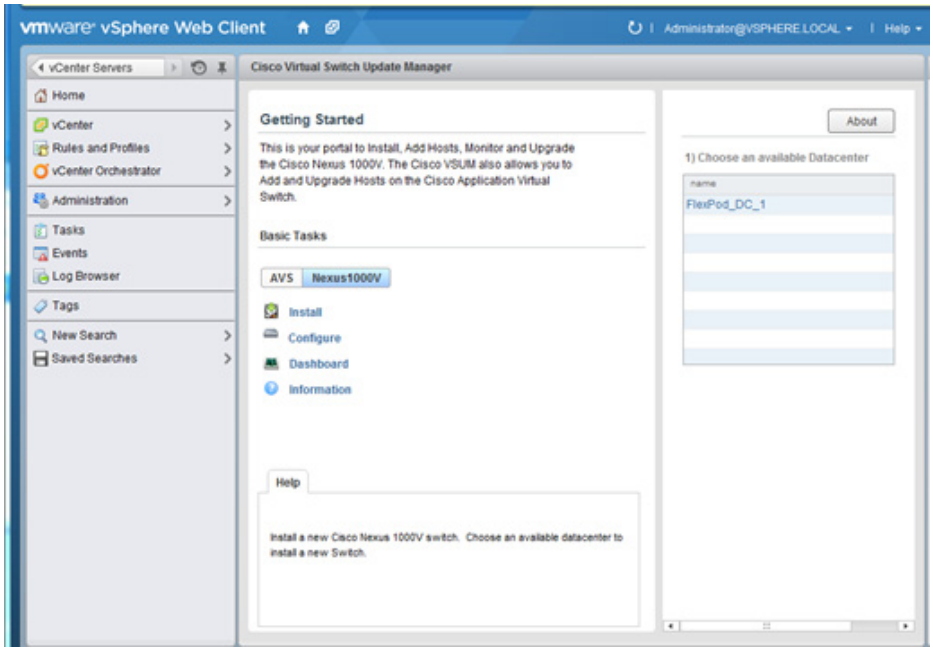
1. Launch the vSphere Web client interface `https://<<Vshpere_host_ip>>:9443/vsphere-client` and login. Login using Administrator@vsphere.local user credentials.
2. Select the home tab and click Cisco Virtual Switch Update Manager.



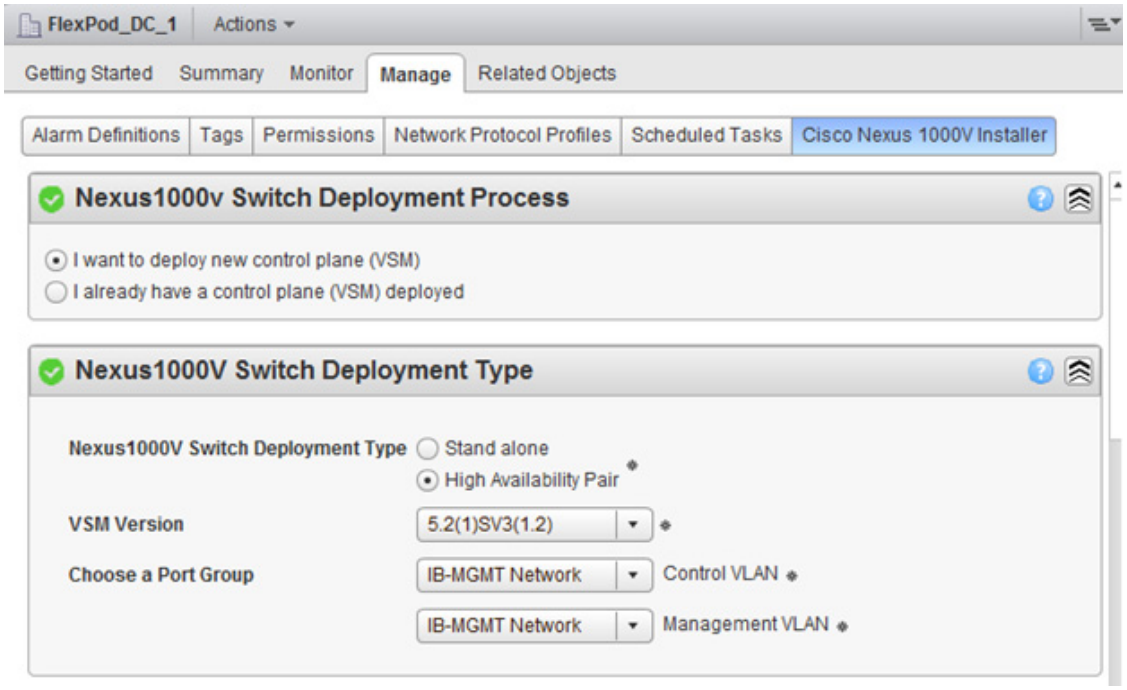
3. Click the Nexus1000V button, then click Install.



4. Click the FlexPod_DC_1 datacenter in the right screen.

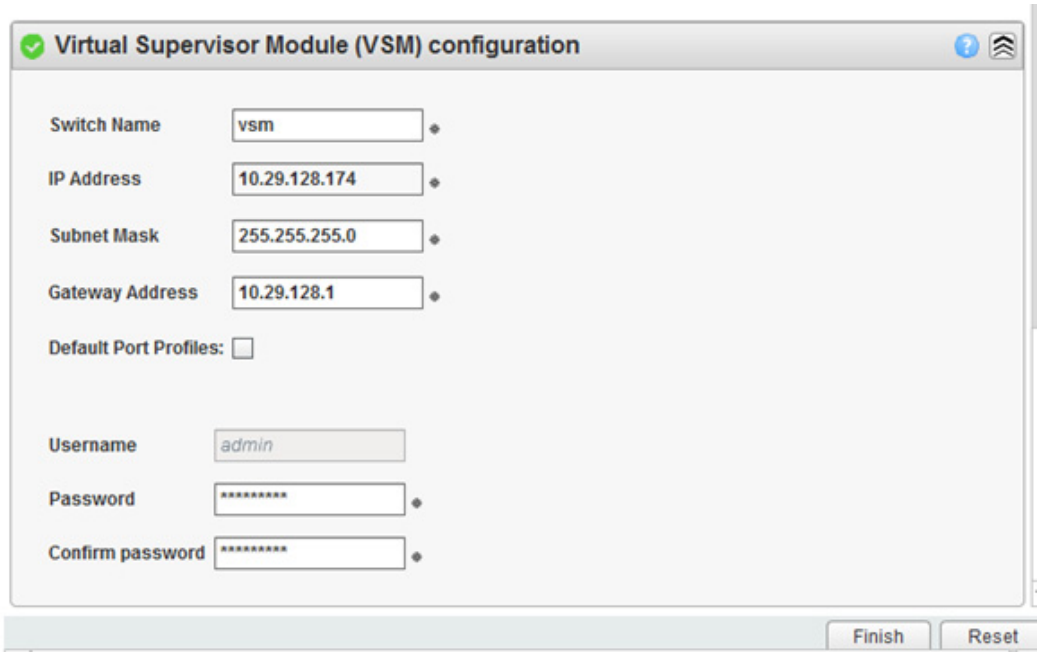


5. Select vsm on the right and click Manage.
6. Keep the default for deploy new VSM ,and High Availability Pair. Select IB-Mgmt for the control and Management VLAN.

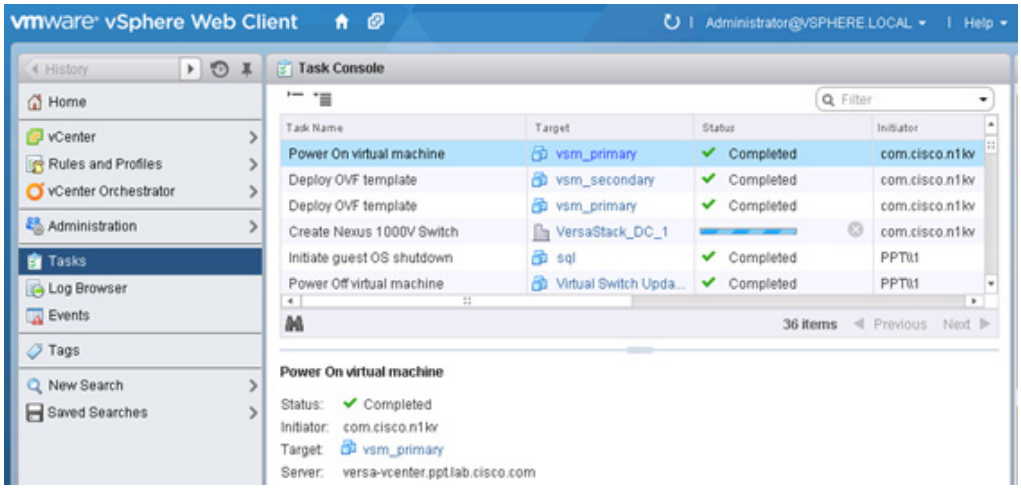


7. Enter a domain ID for the switch configuration section.

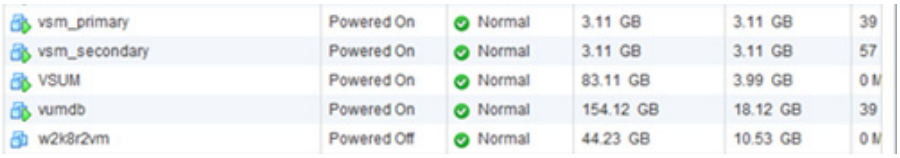
8. Enter the following information for the VSM configuration `<<var_vsm_switch_name>>`, `<<var_vsm_ip>>`, `<<var_vsm_netmask>>`, `<<var_vsm_gateway>>`, `<<var_password>>` then click Finish.



9. Launch a second VSphere Client to monitor the progress. Click Tasks in the left pane. It will take a few minutes to complete.



10. Verify that two VSM virtual machines are created.



Perform Base Configuration of the Primary VSM

To perform the base configuration of the primary VSM, complete the following steps:

1. Use an SSH client, log in to the primary Cisco Nexus 1000V VSM as admin.
2. Run the following configuration commands:

```
config t
ntp server <<var_global_ntp_server_ip>> use-vrf management

vlan <<var_ib-mgmt_vlan_id>>
name IB-MGMT-VLAN
vlan <<var_vmotion_vlan_id>>
name vMotion-VLAN
vlan <<var_vm-traffic_vlan_id>>
name VM-Traffic-VLAN
vlan <<var_native_vlan_id>>
name Native-VLAN
exit


port-profile type ethernet system-uplink
vmware port-group
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>,
<<var_vmotion_vlan_id>>, <<var_vm-traffic_vlan_id>>
channel-group auto mode on mac-pinning
no shutdown
system vlan <<var_ib-mgmt_vlan_id>>, >>, <<var_vmotion_vlan_id>>,
<<var_vm-traffic_vlan_id>>
system mtu 9000
state enabled
exit


port-profile type vethernet IB-MGMT-VLAN
vmware port-group
switchport mode access
switchport access vlan <<var_ib-mgmt_vlan_id>>
no shutdown
system vlan <<var_ib-mgmt_vlan_id>>
state enabled
exit

exit

port-profile type vethernet vMotion-VLAN
vmware port-group
switchport mode access
switchport access vlan <<var_vmotion_vlan_id>>
no shutdown
system vlan <<var_vmotion_vlan_id>>
state enabled
exit

port-profile type vethernet VM-Traffic-VLAN
```

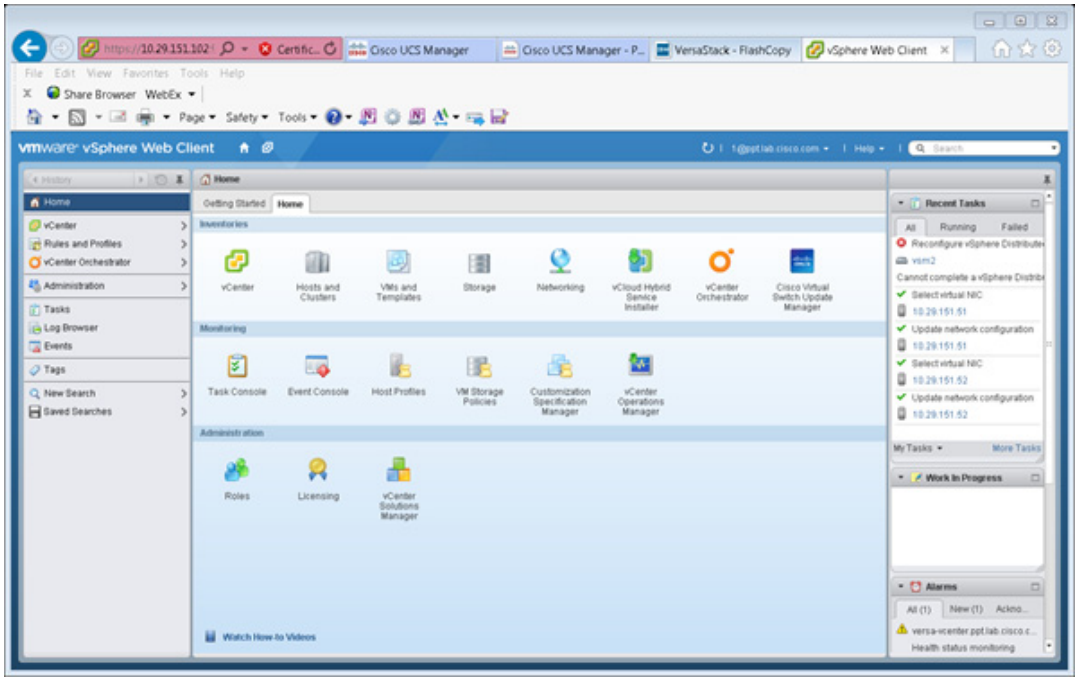
```
vmware port-group
switchport mode access
switchport access vlan <<var_vm-traffic_vlan_id>>
no shutdown
system vlan <<var_vm-traffic_vlan_id>>
state enabled
exit

port-profile type vethernet n1kv-L3
capability l3control
vmware port-group
switchport mode access
switchport access vlan <<var_ib-mgmt_vlan_id>>
no shutdown
system vlan <<var_ib-mgmt_vlan_id>>
state enabled
exit
copy run start
```

Migrate Networking Components for ESXi Hosts to Cisco Nexus 1000V

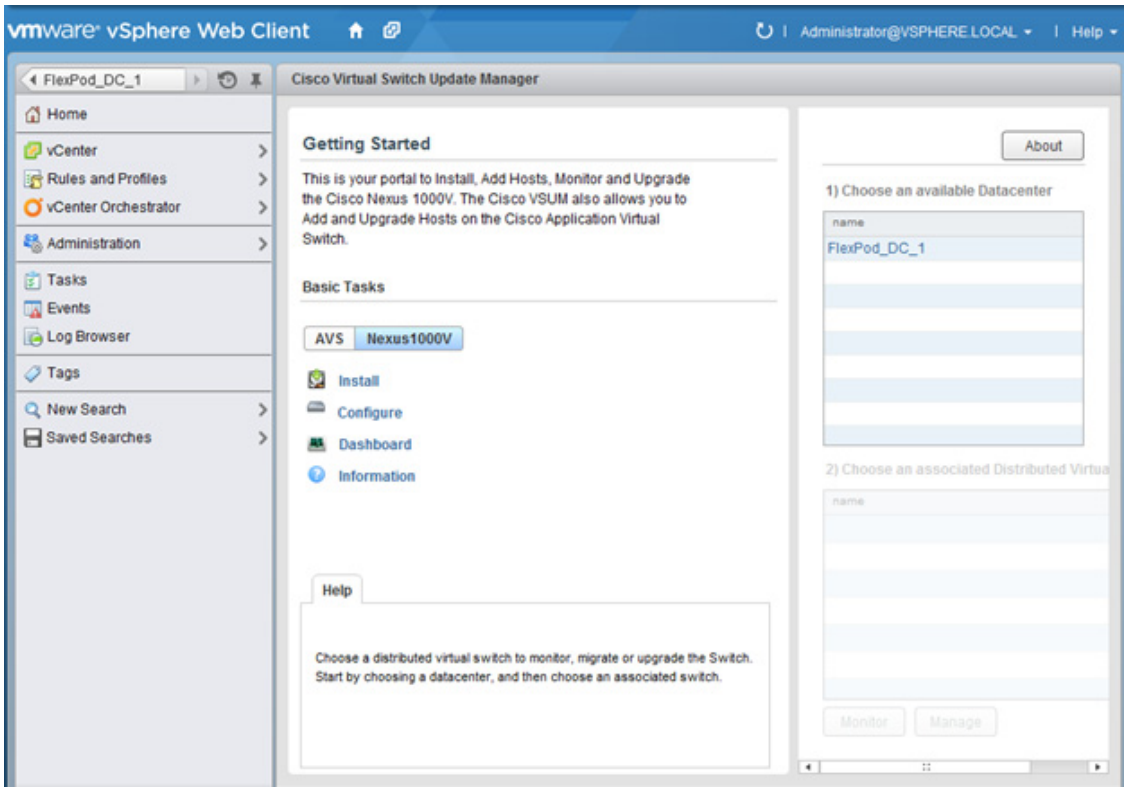
vSphere Client Connect to vCenter

To migrate the networking components for the ESXi hosts to the Cisco Nexus 1000V, complete the following steps:

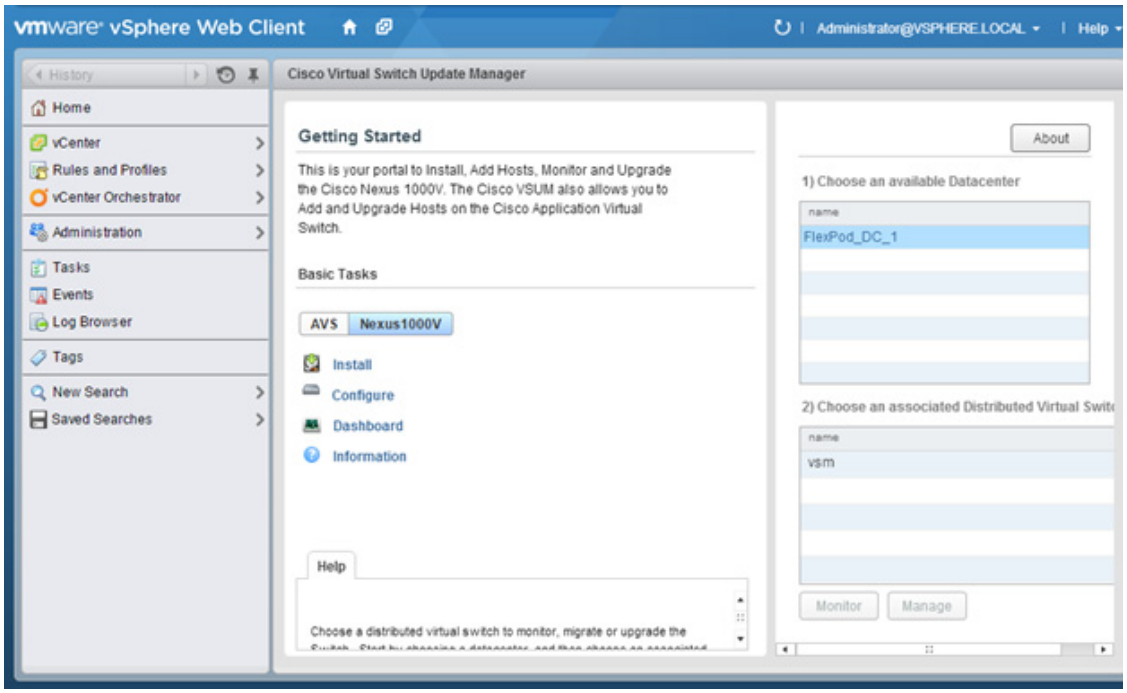
1. In the vSphere web client click the home tab and click the Cisco Virtual Switch Update Manager.



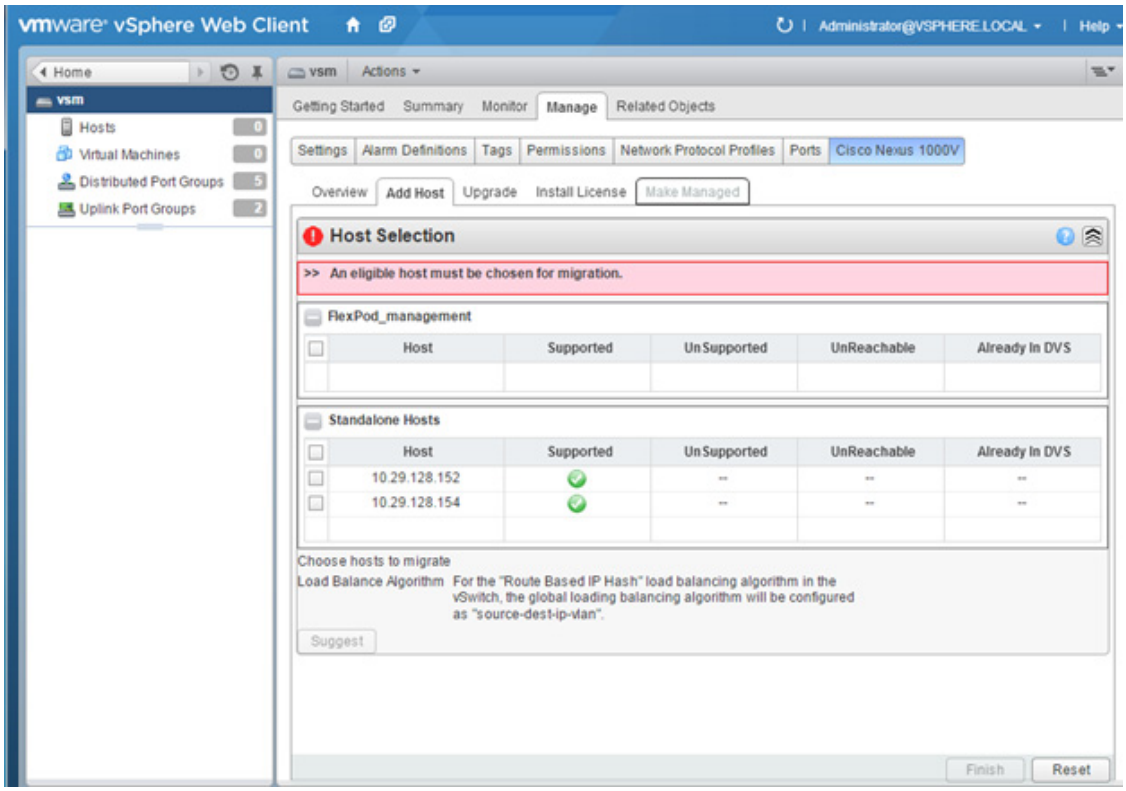
2. Click the Nexus 1000v and click Configure.



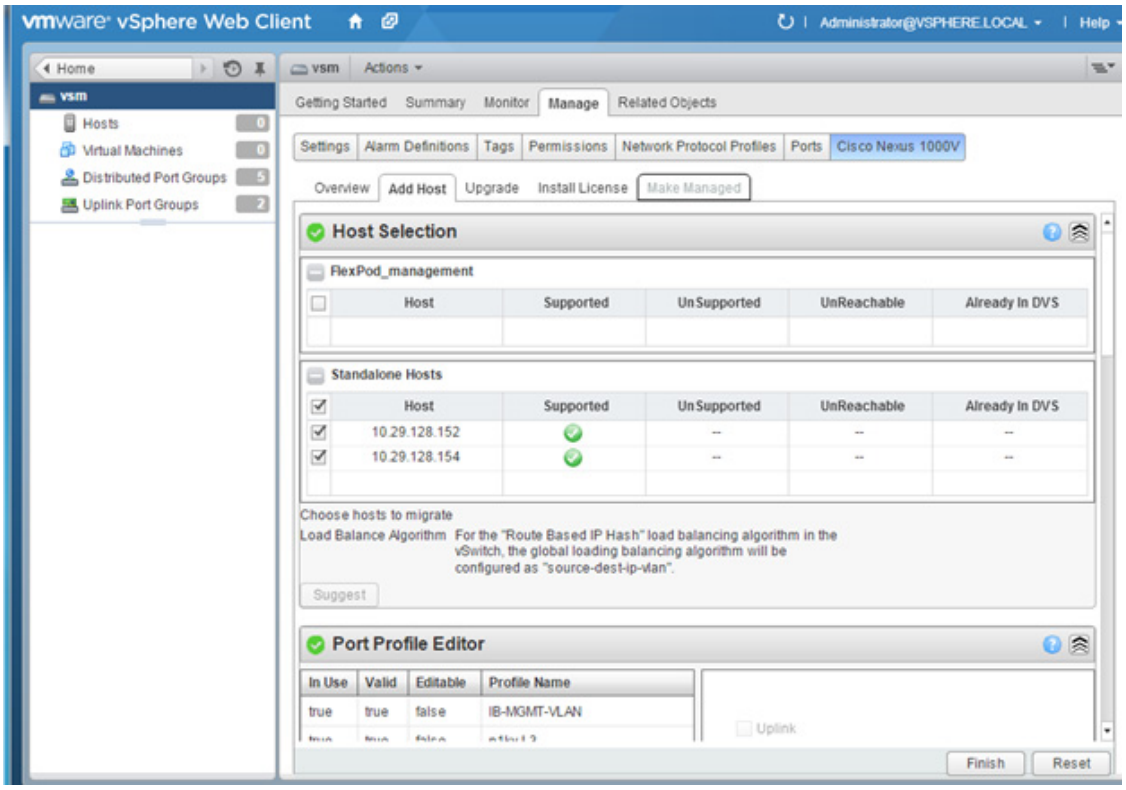
3. Click the Datcenter, then click the Distributed Virtual Switch and select manage.



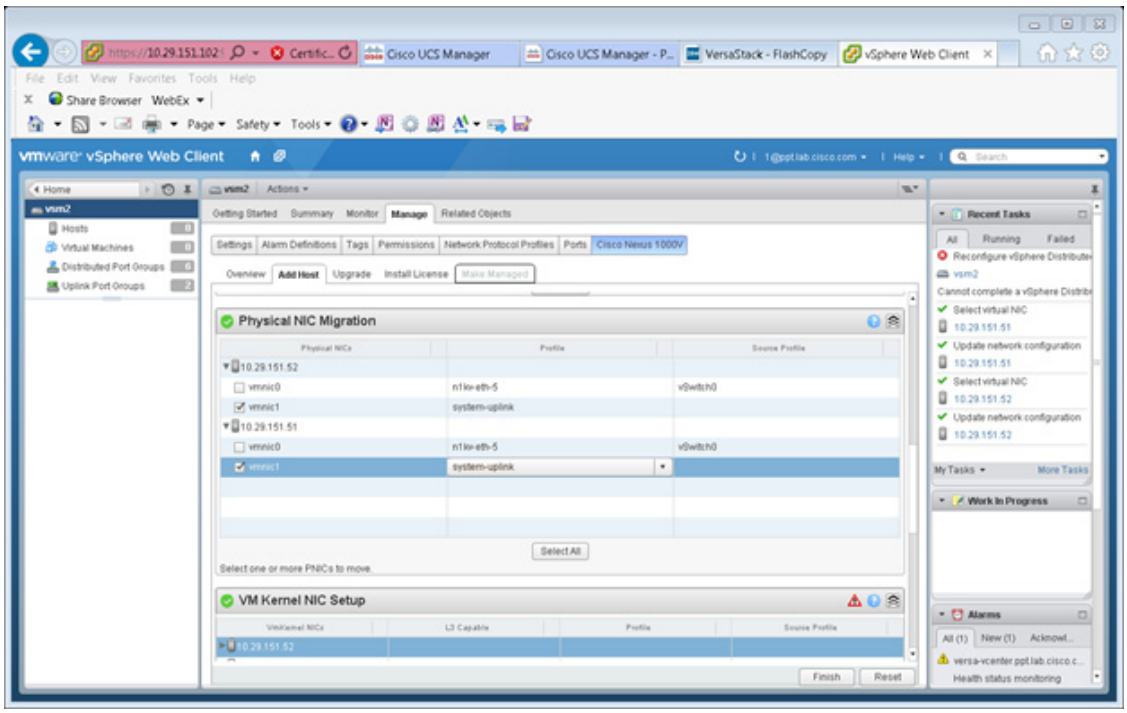
4. Click the add host tab then select the plus sign next to the FlexPod_managnement , then click the top check box to both Hosts.



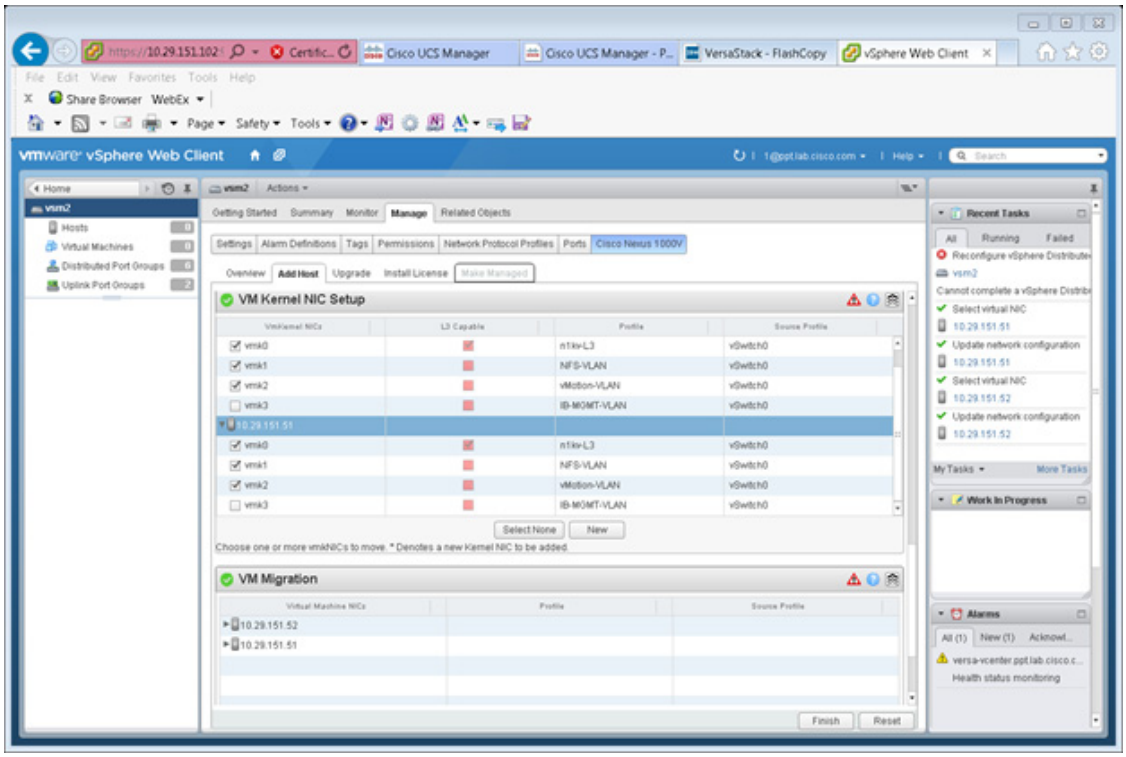
5. Click Suggest.



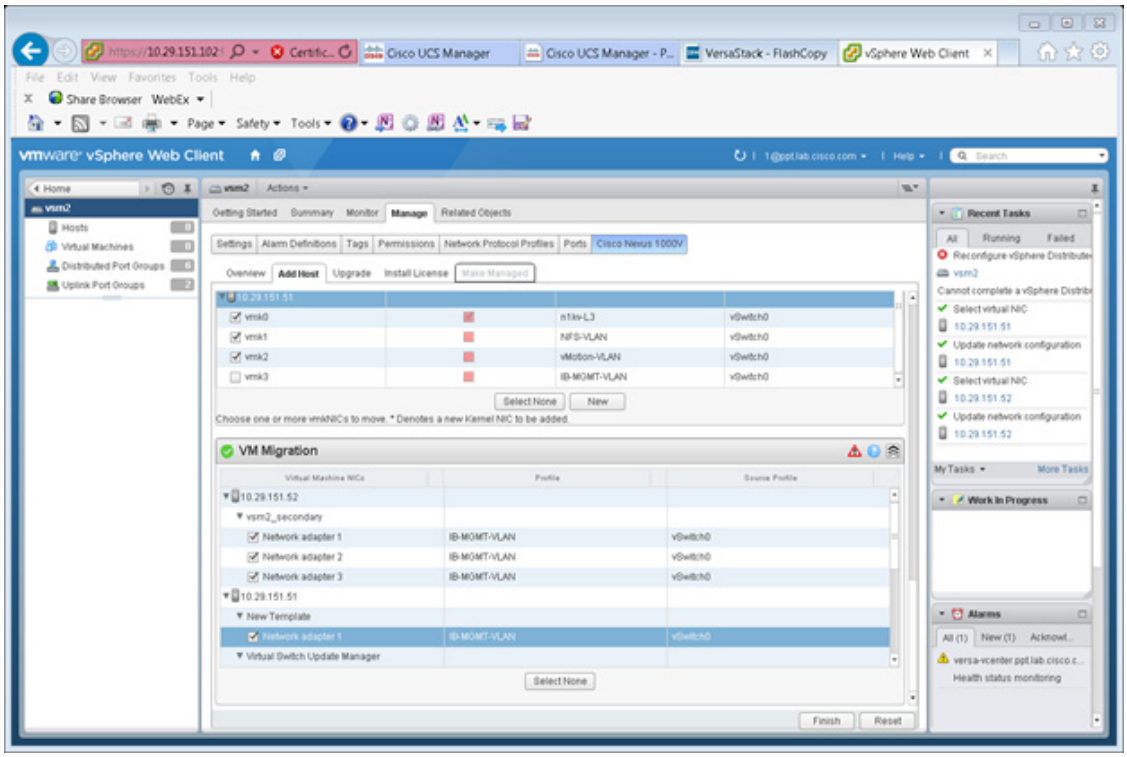
6. Select the Physical NIC Migration and select the Unused Nic vmnic1 for migration. and select System Uplink in the middle pane.



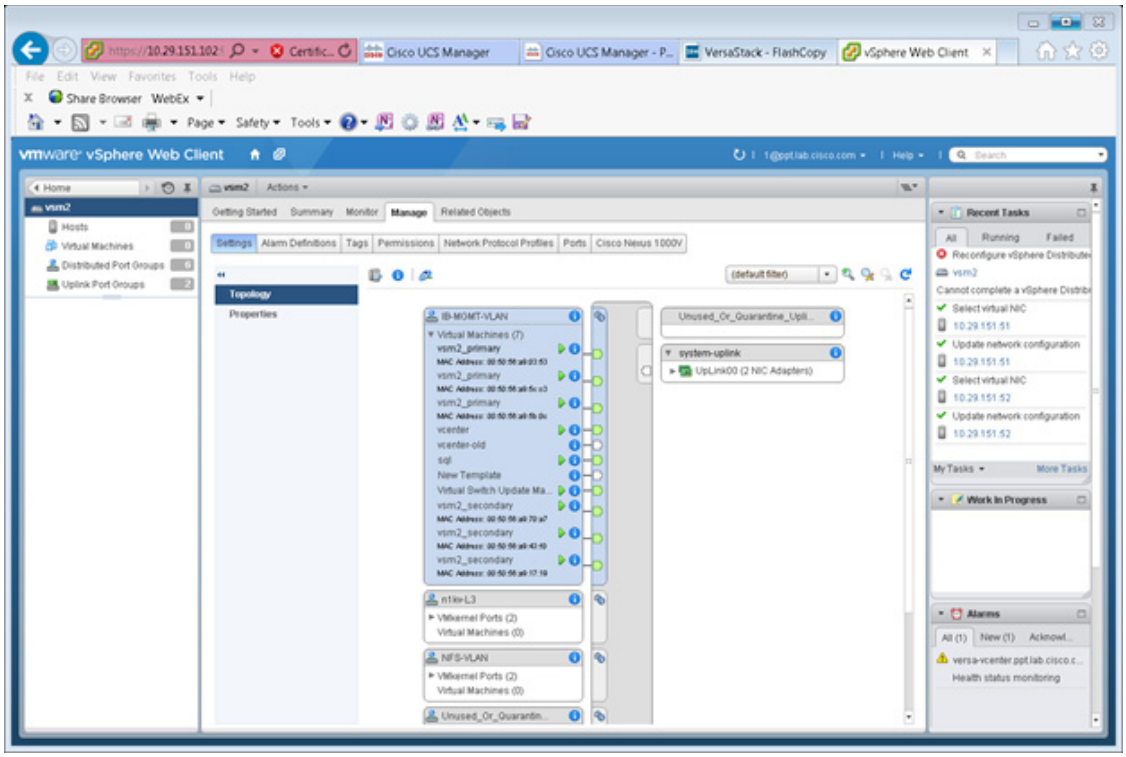
7. For the VM Kernel Nic Setup, deselect vmk3.



8. For VM migration click the button next to the virtual machine to expand the target profile. Repeat this for each Virtual Machine.



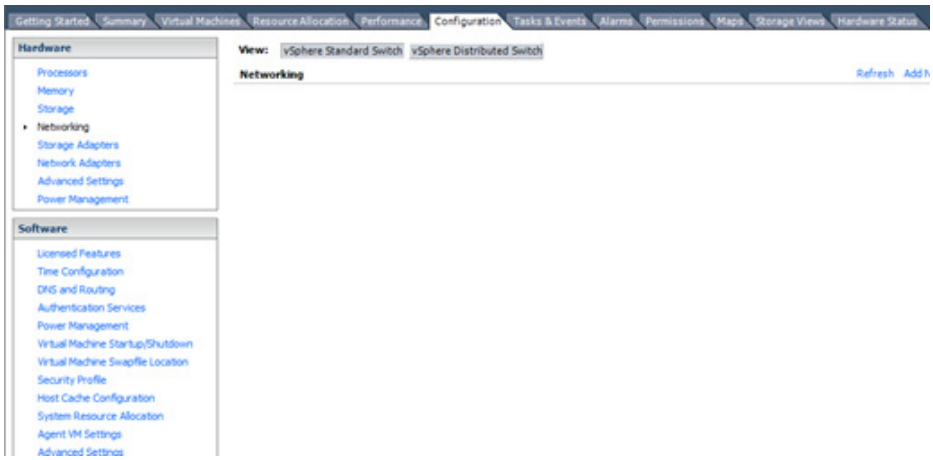
9. Click Finish.
10. When the migration completes, click Settings then Topology and expand the virtual machines to view the network connections.



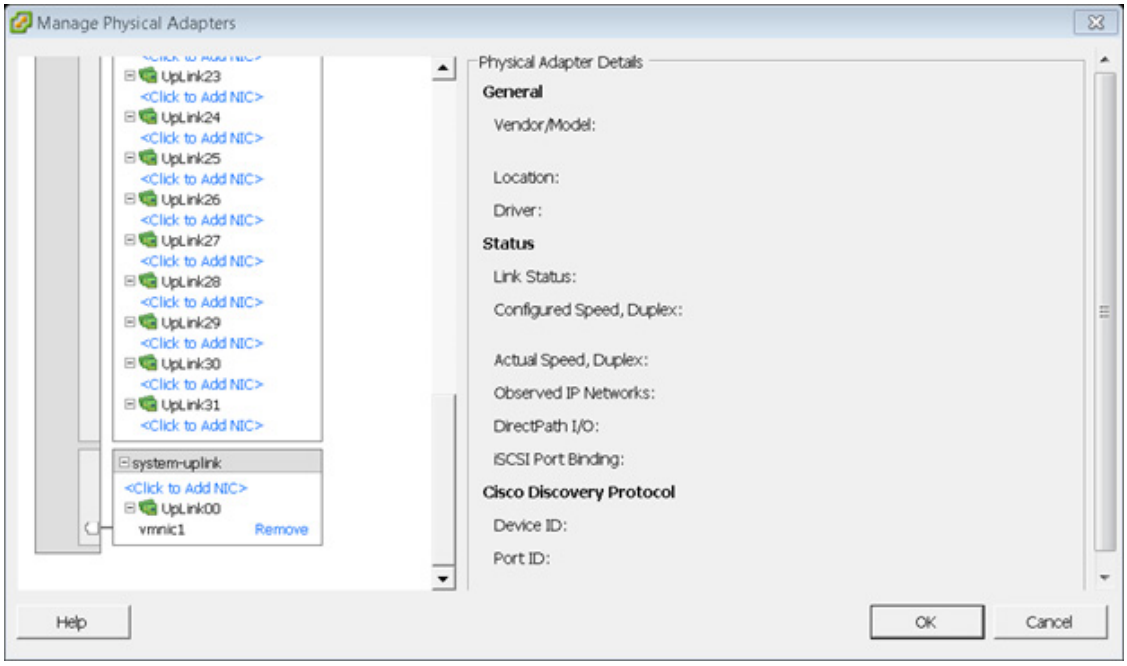
11. Remove networking standard switch Components for ESXi Hosts.
12. Remove the unused standard switch components and assign the second vnic on all ESXi servers.

ESXi Host VM-Host-Infra-01 (Repeat the steps in this section for all the ESXi Hosts)

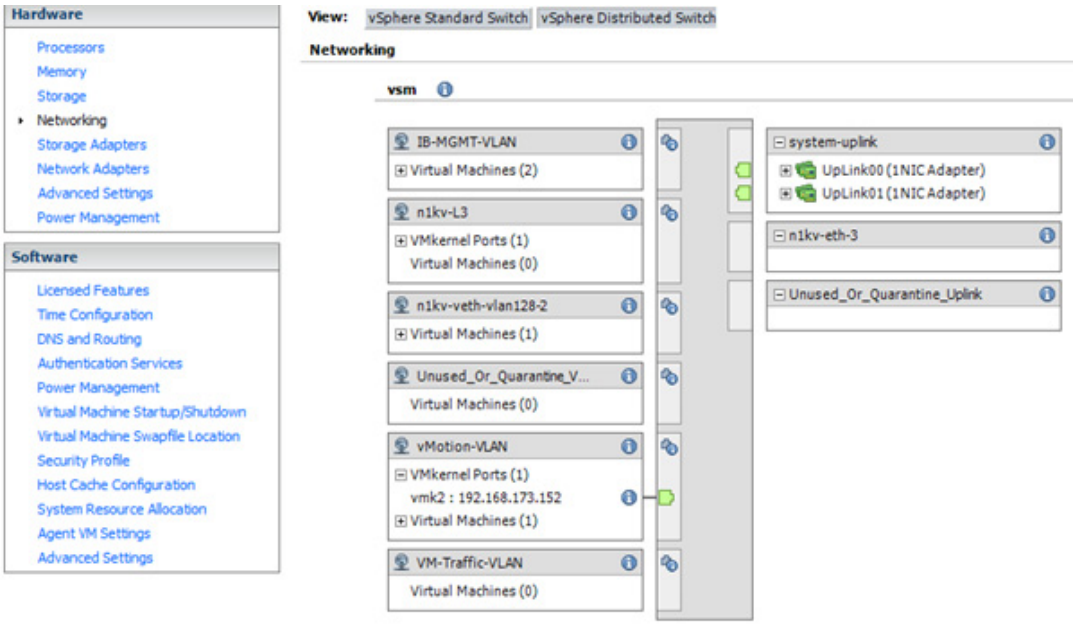
1. Open the From each vSphere Client, select the host in the inventory.
2. Click the Configuration tab.
3. Click Networking.
4. Select the VSphere Standard switch then Properties.
5. Remove the network adpaters on the vSwitch0 (Standard Switch).
6. Remove the vSwitch0.



7. After vSwitch0 has disappeared from the screen, click vSphere Distributed Switch at the top next to View.
8. Click Manage Physical Adapters.
9. Scroll down to the system-uplink box and click Add NIC.
10. Choose vmnic0 and click OK then OK again.



11. Verify that the NIC adapters are added correctly to the system-uplink.

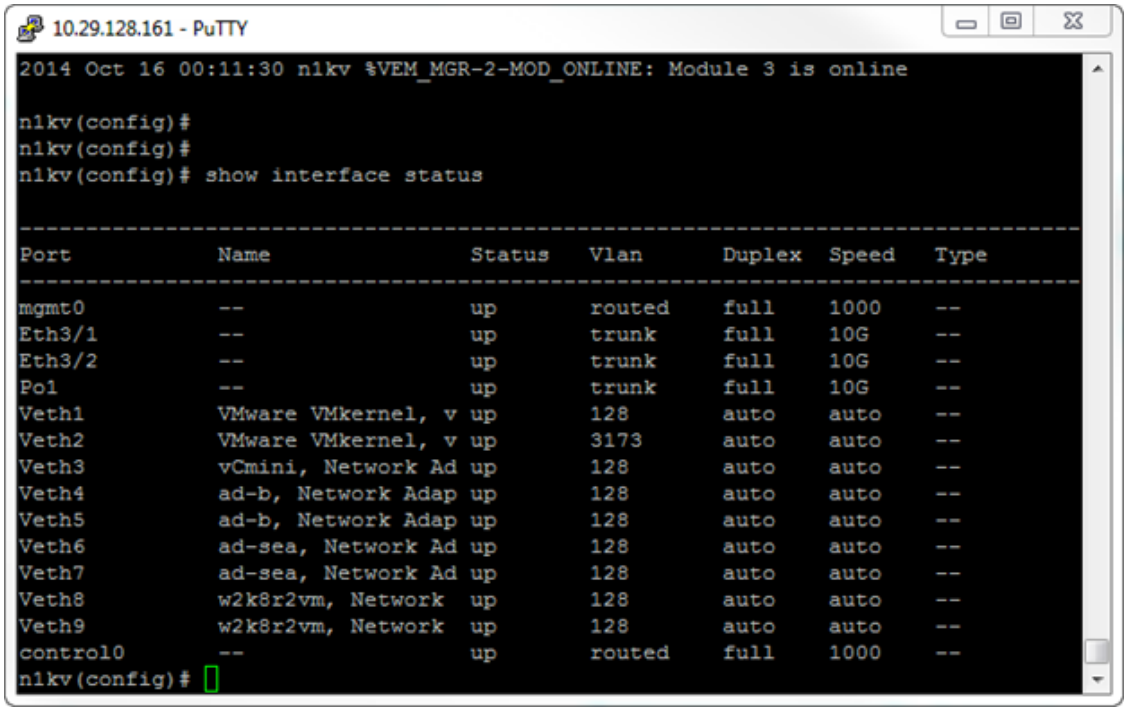


For more information about the 1000v switch, please visit the web site:

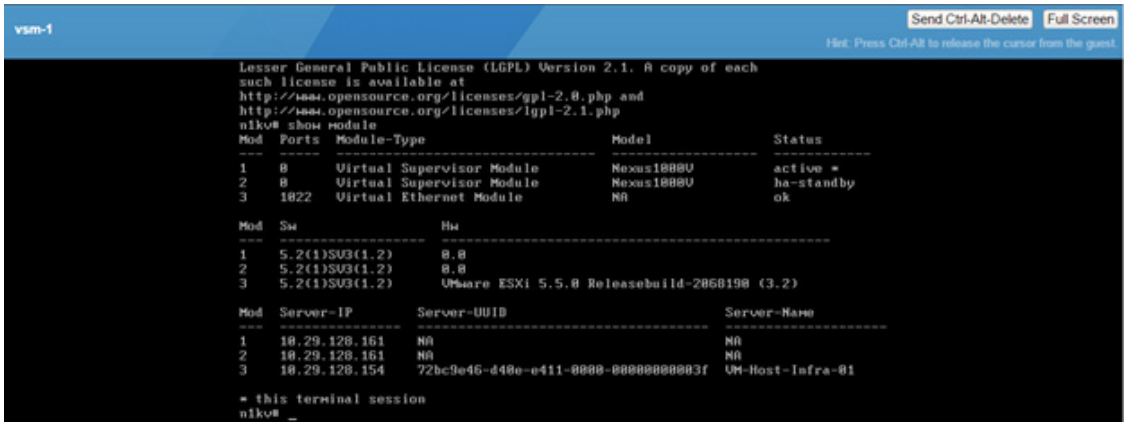
http://www.cisco.com/c/en/us/products/switches/nexus-1000v-switch-vmware-vsphere/index.html

Virtual Ethernet Module (VEM)

1. 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.



2. Run `show module` and verify that the two ESXi hosts are present as modules.



3. Run `copy run start`.
4. Type `exit` to log out of the Cisco Nexus 1000v.

FlexPod Management Tool Setup

NetApp Virtual Storage Console 5.0 Deployment Procedure

VSC 5.0 Preinstallation Considerations

The following licenses are required for Virtual Storage Console (VSC) on storage systems that run clustered Data ONTAP 8.2.2:

- FCP license
- FlexClone (for provisioning and cloning only)
- SnapRestore (for backup and recovery)
- SnapManager suite

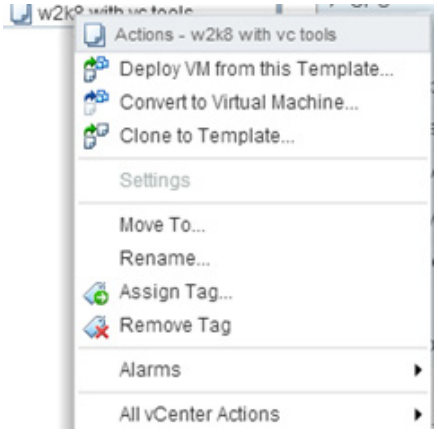
Install VSC 5.0

To install the VSC 5.0 software, complete the following steps:

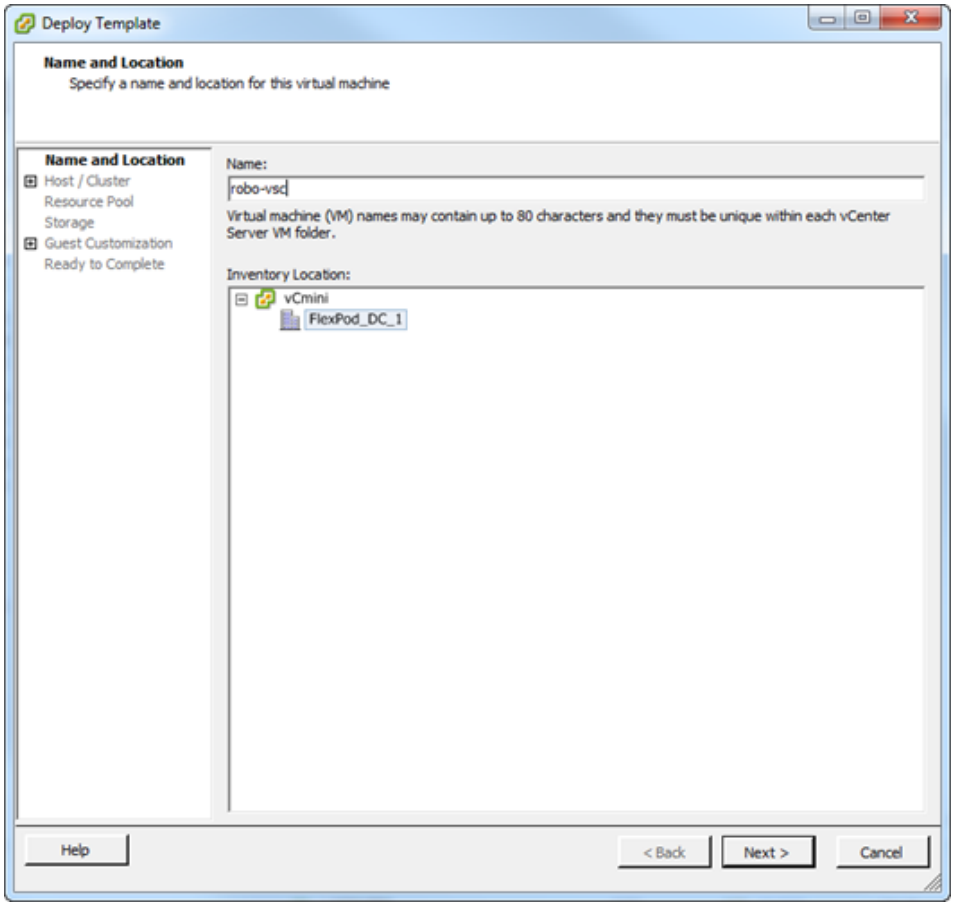
1. Build a VSC virtual machine with 4GB RAM, two CPUs, and one virtual network interface in the `<<var_ib-mgmt_vlan_id>>` VLAN. The virtual network interface should be a VMXNET 3 adapter.
2. Bring up the VM, install VMware Tools, assign IP addresses, and join the machine to the Active Directory domain.
3. Install the current version of Adobe Flash Player on the VM.
4. Install all Windows updates on the VM.

Note The following steps explain the procedure to install Windows 2008 R2 on a VM from an OVA file. VMs can also be deployed by using a Windows 2008 R2 ISO file.

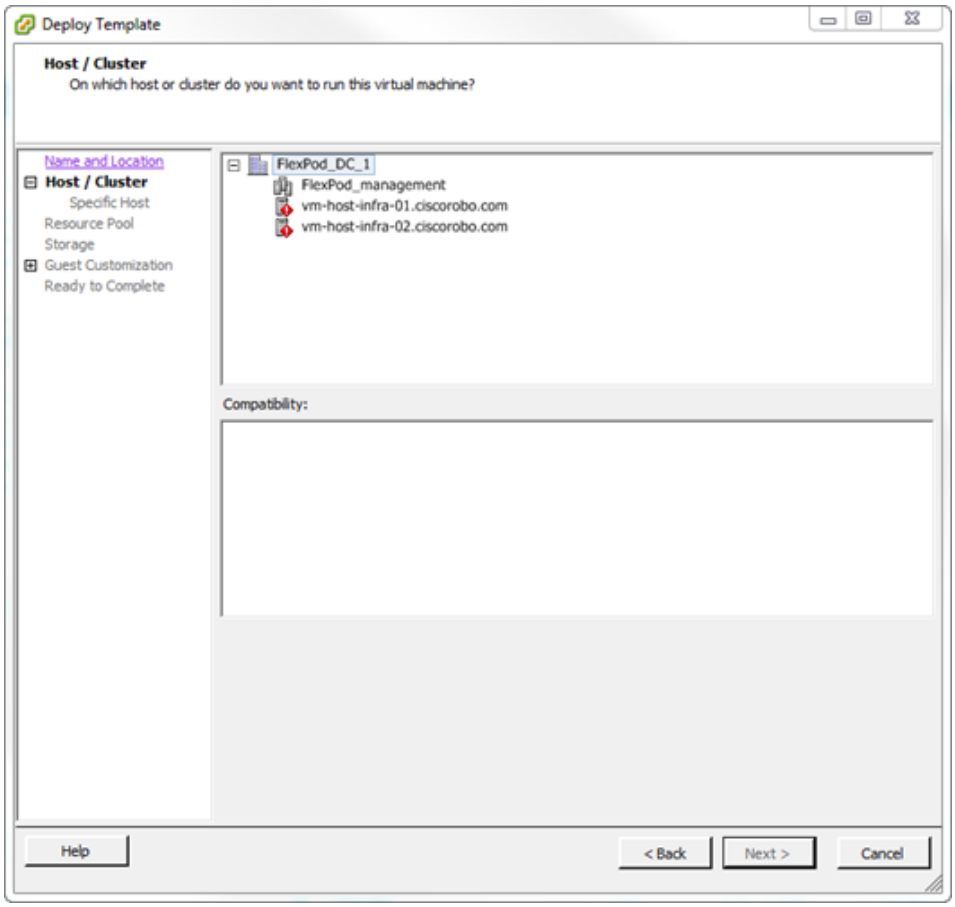
5. Deploy a Windows VM from an existing template. Select the template and click Deploy VM from this Template.



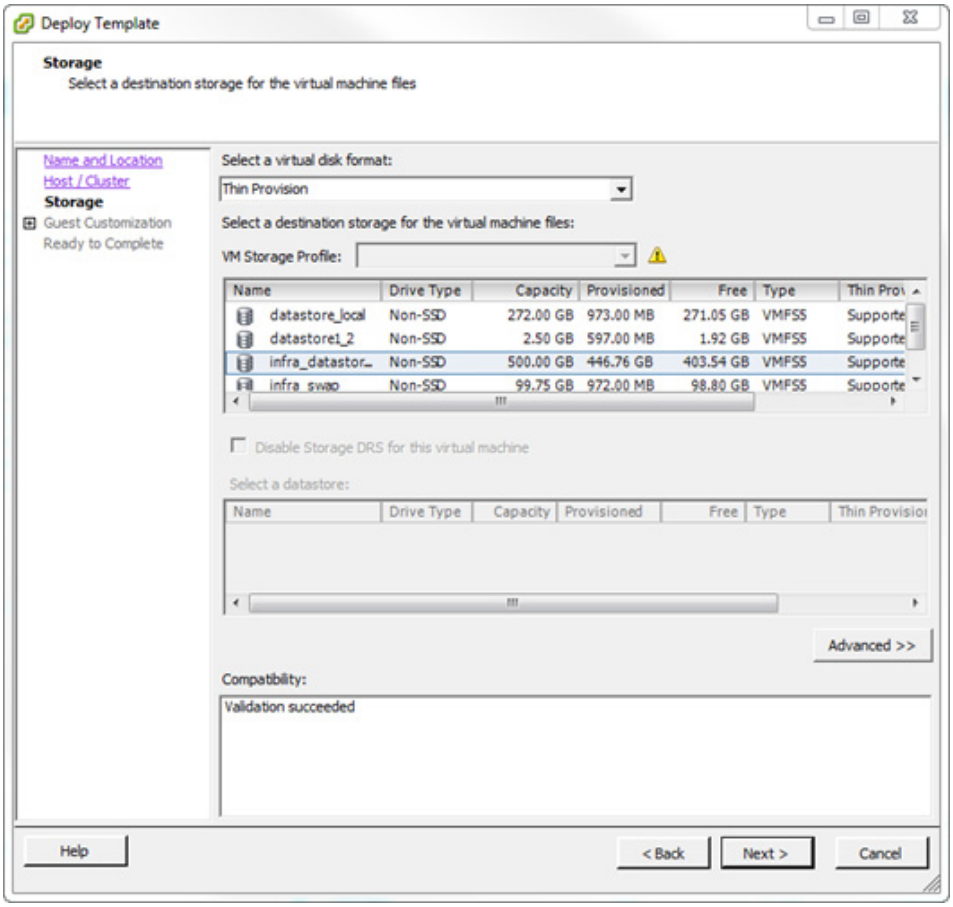
6. Enter the VM Name and select the inventory location.



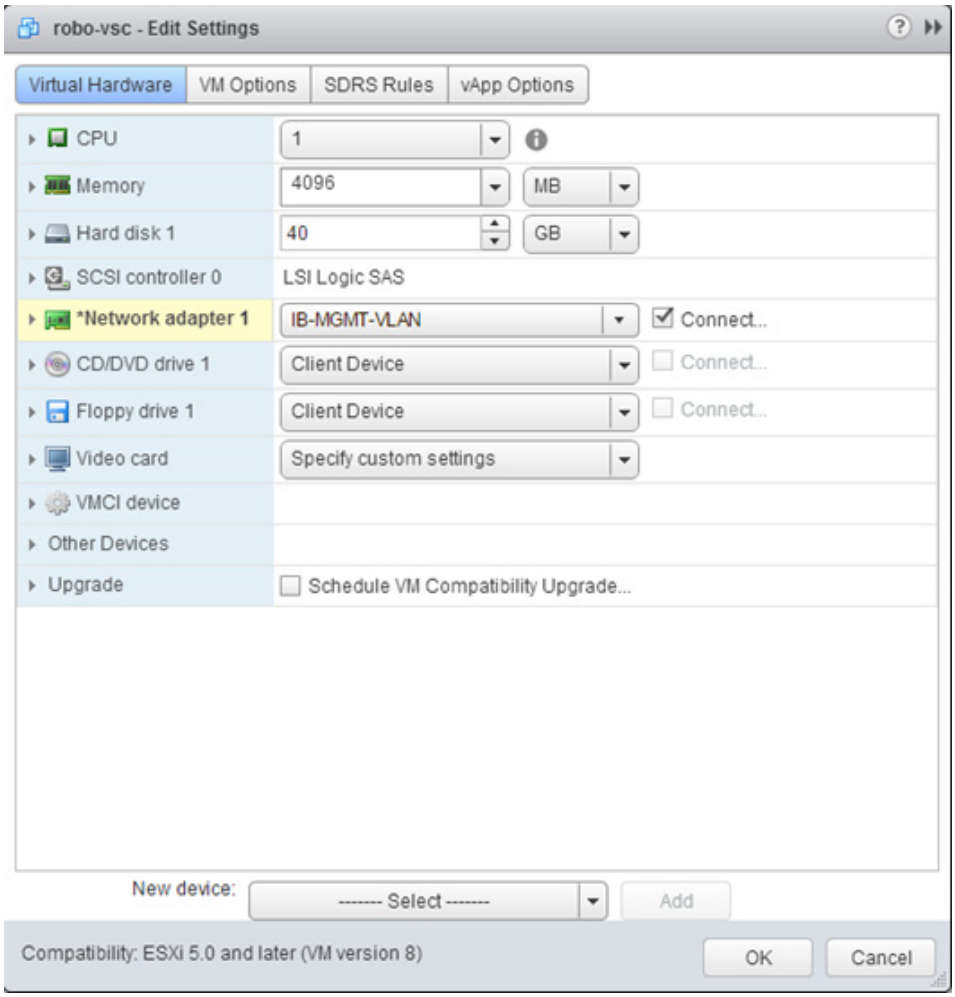
7. Select the host/cluster for the VM to run on.



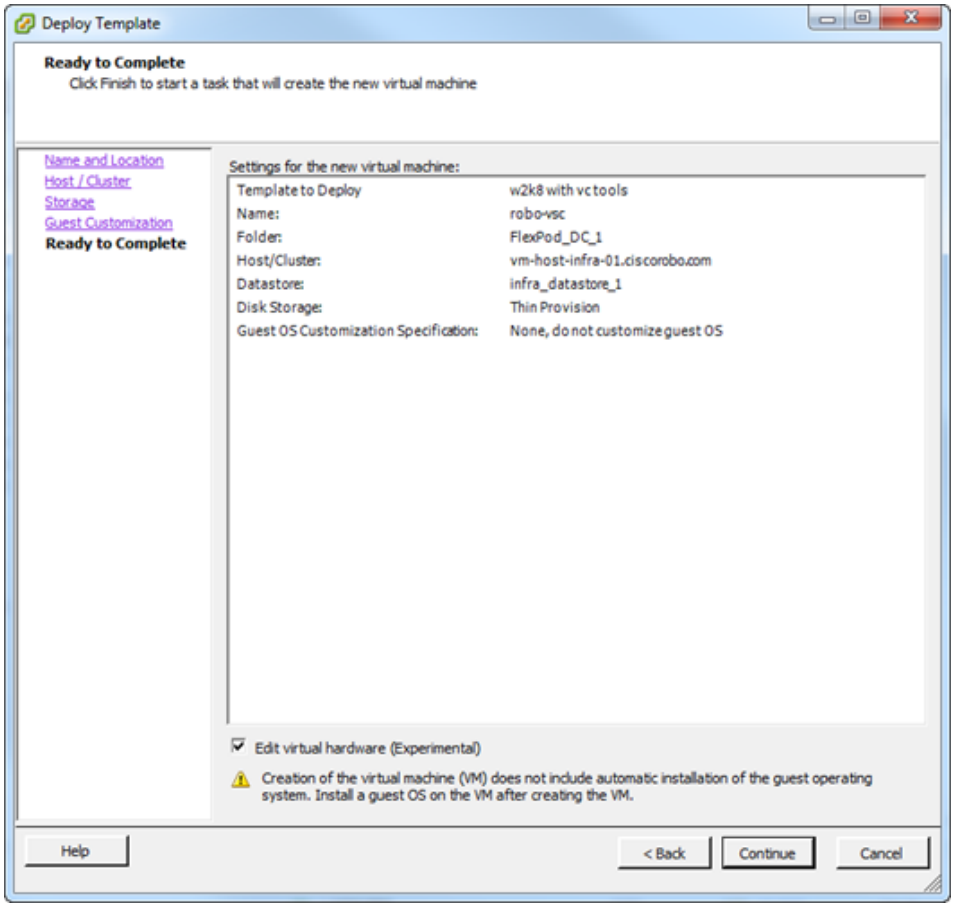
8. Select the destination storage for the VM files.



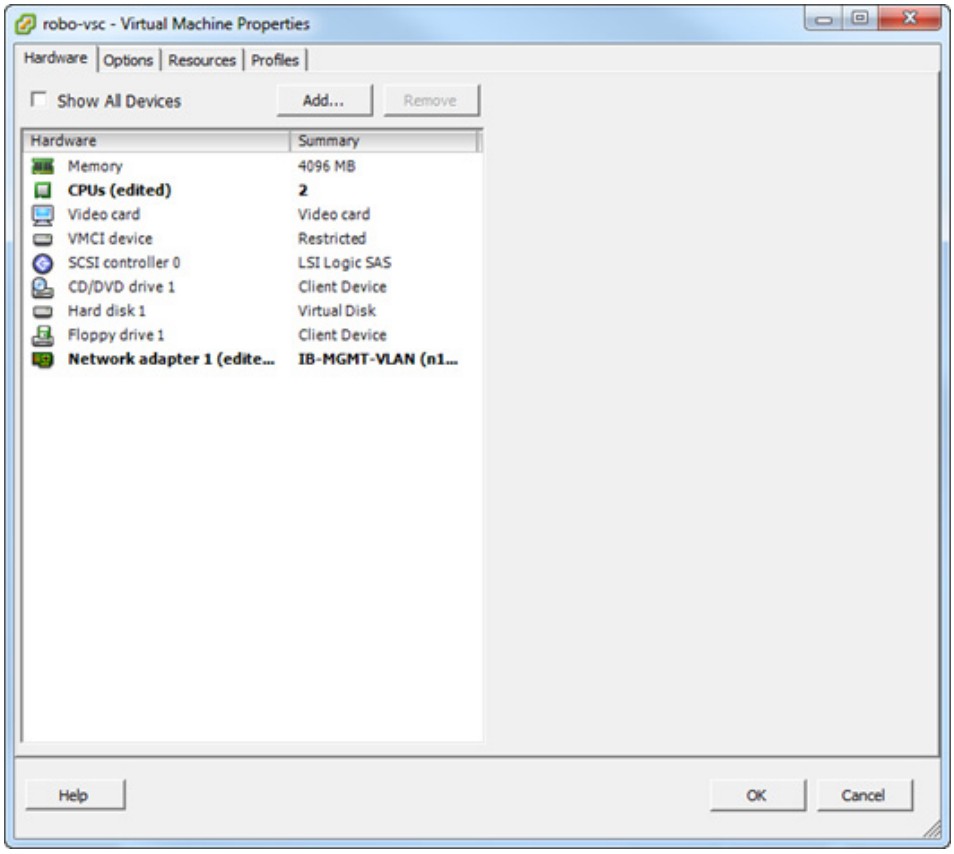
9. Select the resource requirements, such as the number of CPUs, memory and network adapter.



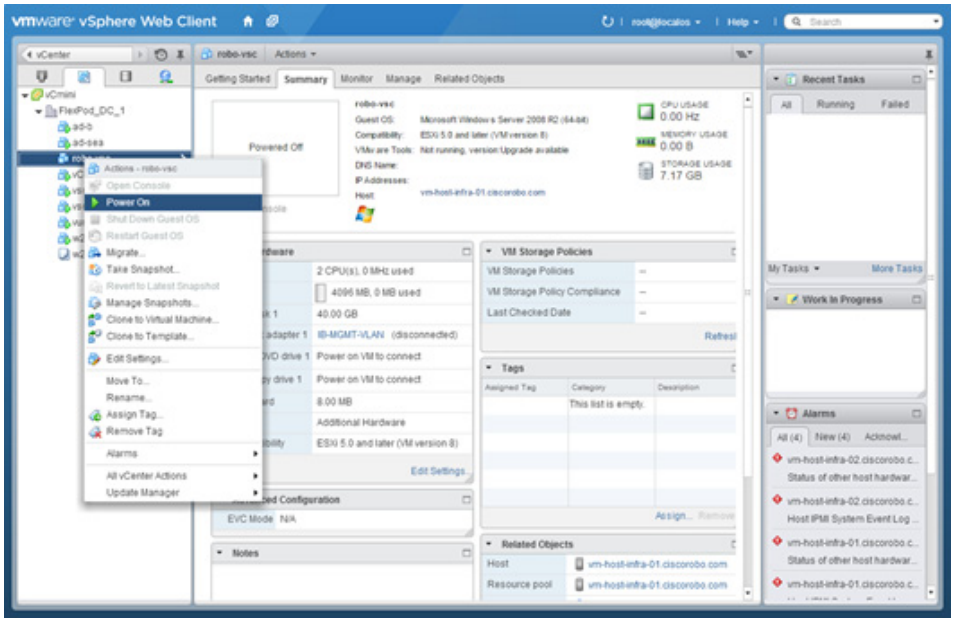
10. Verify the settings and click Continue.



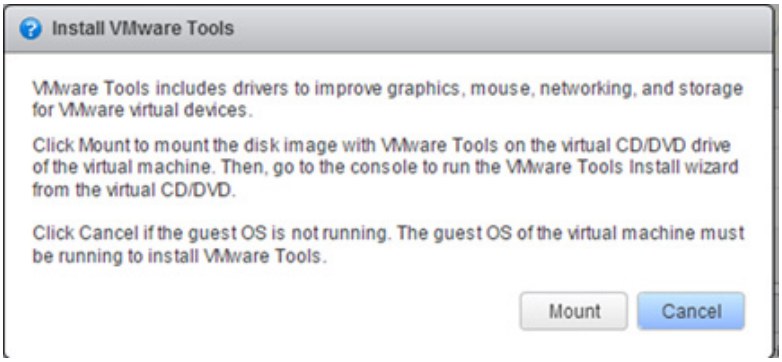
11. Complete the VM deployment by clicking Continue and click Edit Settings for the VM created. Verify that the VM has 2 CPUs, 4096MB of memory, and the appropriate network adapter. Click OK.



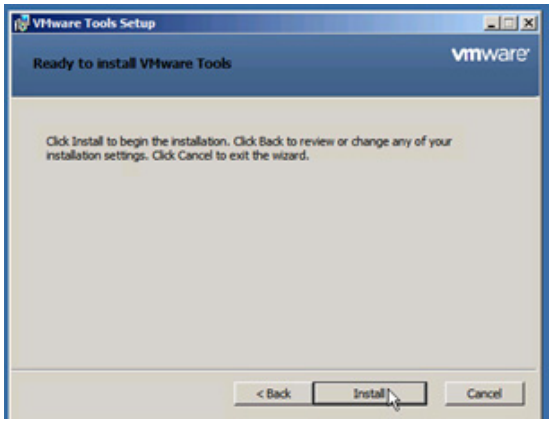
12. Power on the new VM to install and configure NetApp Virtual Storage Console.



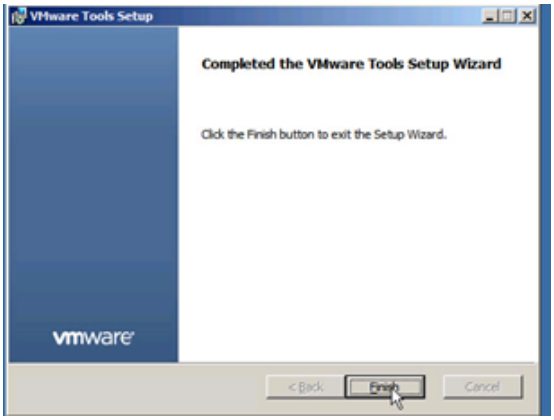
13. Click Install VMware Tools.
14. Click Mount to complete the VMware Tools installation.



15. Click Run setup64.exe.
16. Click Next to start the VMWare Tools Installation wizard.
17. Click Next to choose a typical installation.

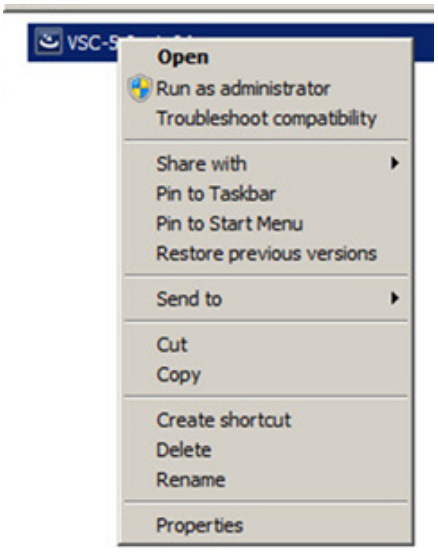


18. Click Install.

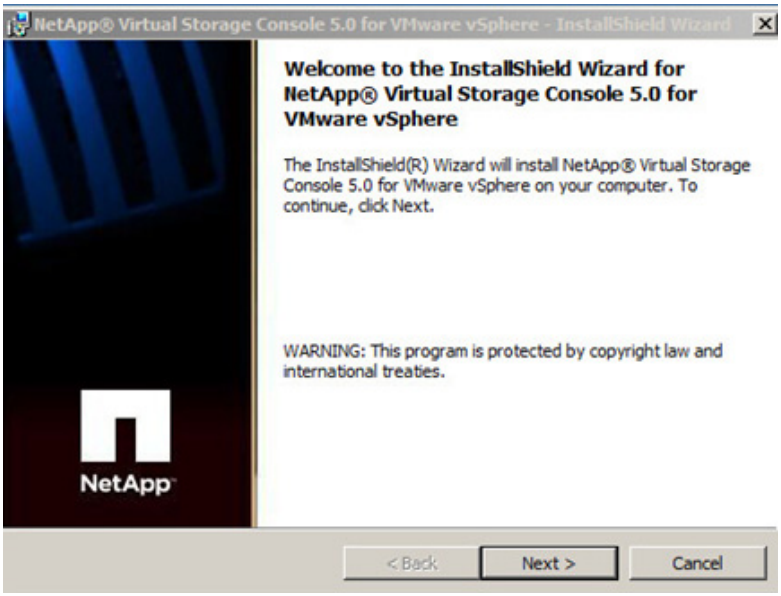


19. Click Finish to finish the installation.
20. Click Yes to restart the VM.
21. Log in to the VM.

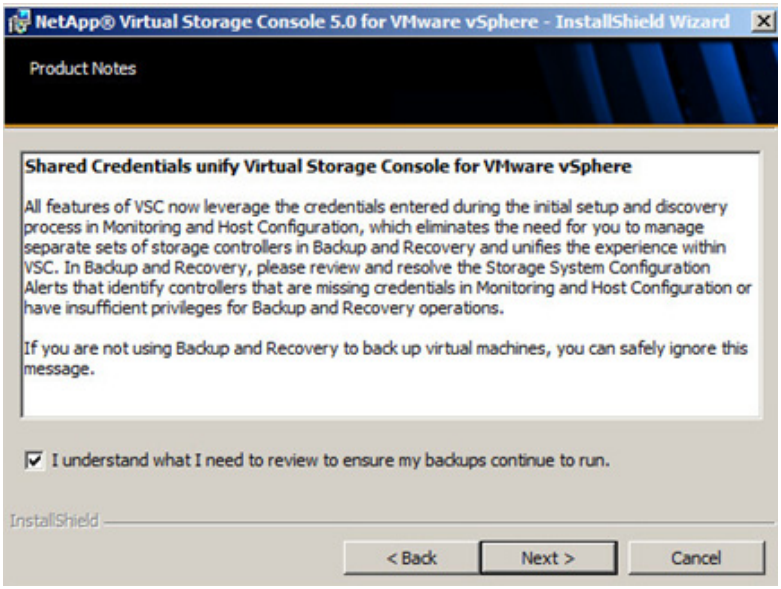
22. Download Virtual Storage Console 5.0 for VMWare from the NetApp Support site.
23. Download the x64 version of Virtual Storage Console 5.0 from the NetApp Support site.



24. Right-click the file downloaded in step 23 and select Run as Administrator.

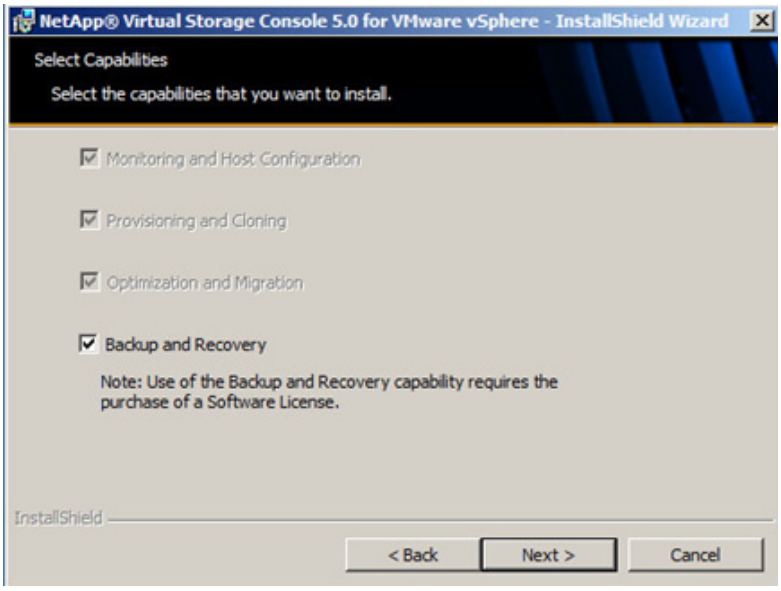


25. On the InstallShield Wizard welcome page, click Next.
26. Select the checkbox to accept the message and click Next.

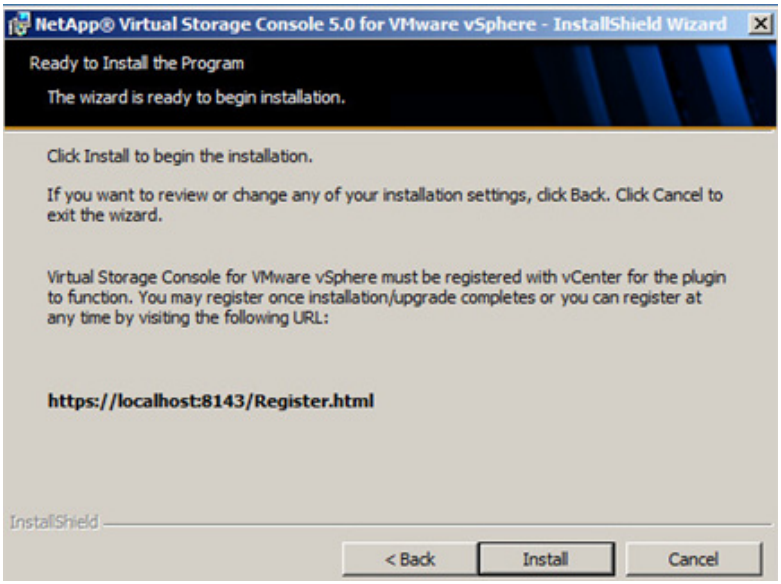


27. Select the checkbox on the Product Notes page and click Next.
28. Select the Backup and Recovery capability checkbox and click Next.

Note The backup and recovery capability requires an additional license.



29. Click Next to accept the default installation location.

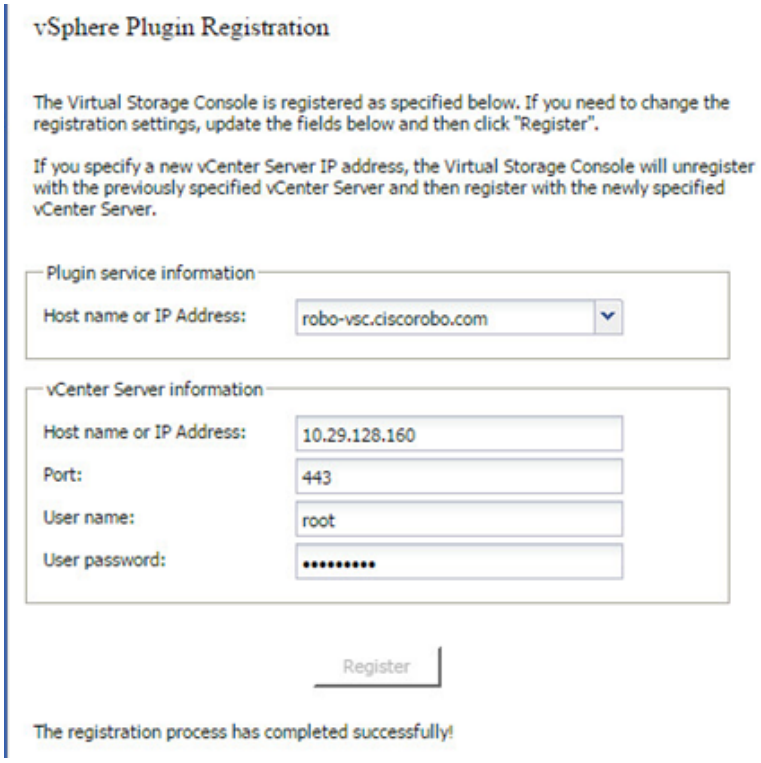


30. Click Install.
31. Click Finish.

Register VSC 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.
2. Click Continue to This Website (Not Recommended).
3. In the Plug-in Service Information section, select the local IP address from the drop-down list that the vCenter Server uses to access the VSC server.
4. In the vCenter Server Information section, enter the host name or IP address, user name (FlexPod admin user), and the user password for the vCenter Server. Click Register to complete the registration.



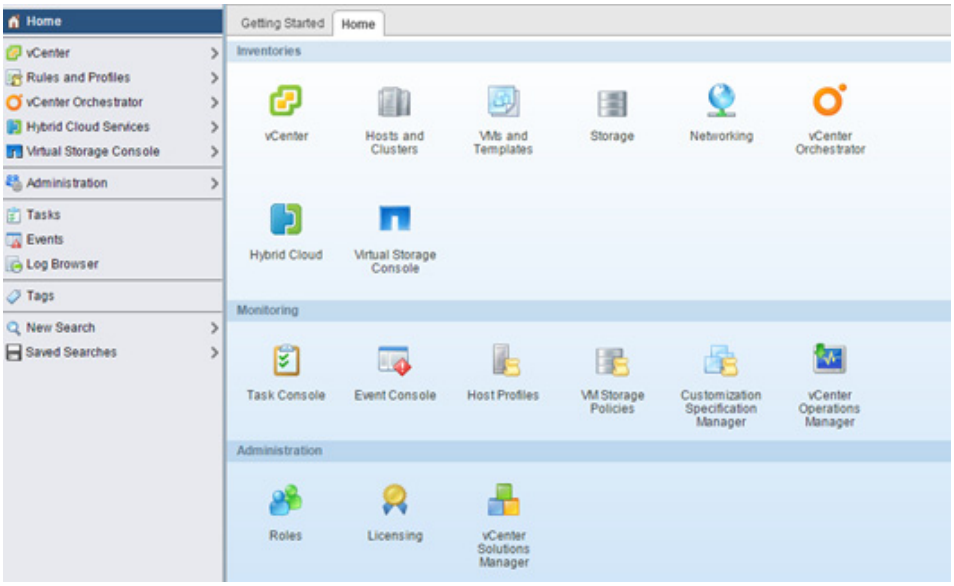
After registration is complete, the storage controllers are discovered automatically.

Note The storage discovery process will take some time.

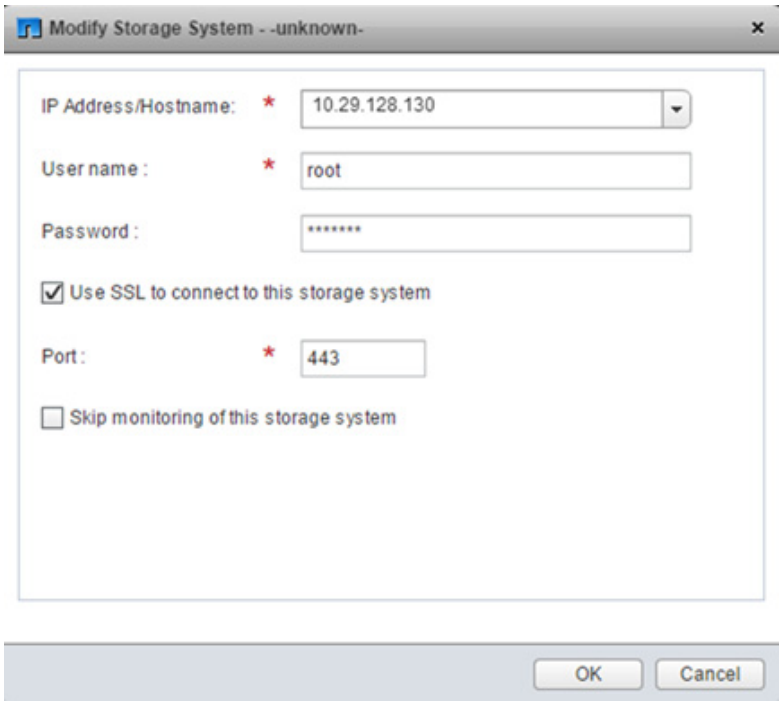
Discover and Add Storage Resources

To discover storage resources for the monitoring and host configuration and the provisioning and cloning capabilities, 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.

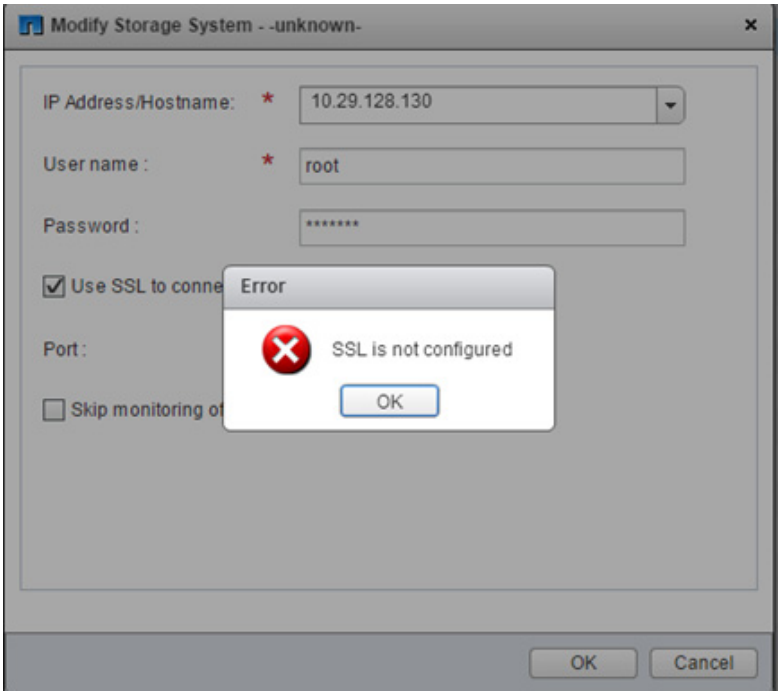


2. On the Home page, click the Home tab and click Virtual Storage Console.



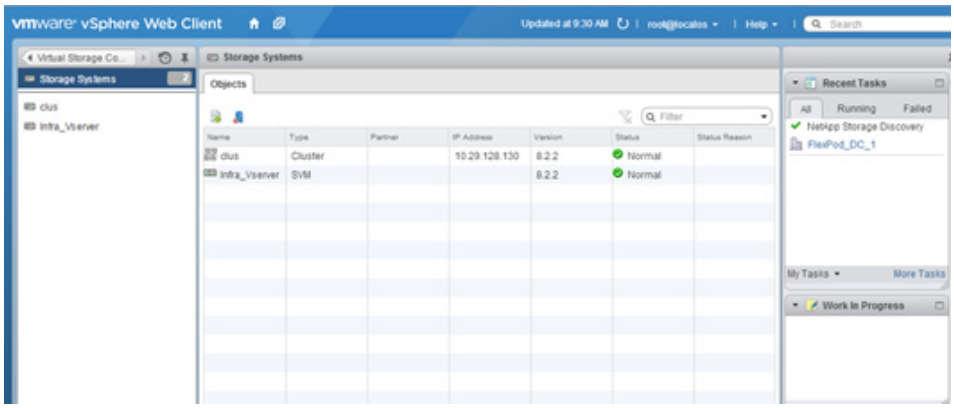
3. Modify the storage system by entering the IP address, user credentials, and the port number. Click OK.
4. If the SSL Is Not Configured error is displayed, click OK, log in to the VSC VM, and run the `ssl setup` command to configure SSL on the NetApp VSC virtual machine. This command must be run from an Administrator command prompt. Right-click the Command Prompt icon and select Run as Administrator. Otherwise, go to step 5.

Note Only run the `ssl setup` command if you see the SSL Is Not Configured error.




```
C:\>"Program Files\NetApp\Virtual Storage Console\bin\vsc.bat" ssl setup -genera
te-passwords
[ INFO] Generating private key password...
[ INFO] Generating keystore password...
[ INFO] Generating public/private key pair with RSA algorithm and keysize 2048..
.
[ INFO] Generating self-signed certificate for CN=robo-vsc.ciscorobo.com (SHA1Wi
thRSAEncryption) which is valid until Sun Oct 13 13:01:27 PDT 2024...
[ INFO] Generating keystore at C:\Program Files\NetApp\Virtual Storage Console\e
tc\nvpf.keystore...
[ INFO] Storing keystore properties in etc\keystore.properties. This file should
 be secured by an administrator. If the administrator moves this file, be sure t
o configure the correct path for http.ssl.keystore.properties in etc\nvpf.overri
de.

C:\>_
```

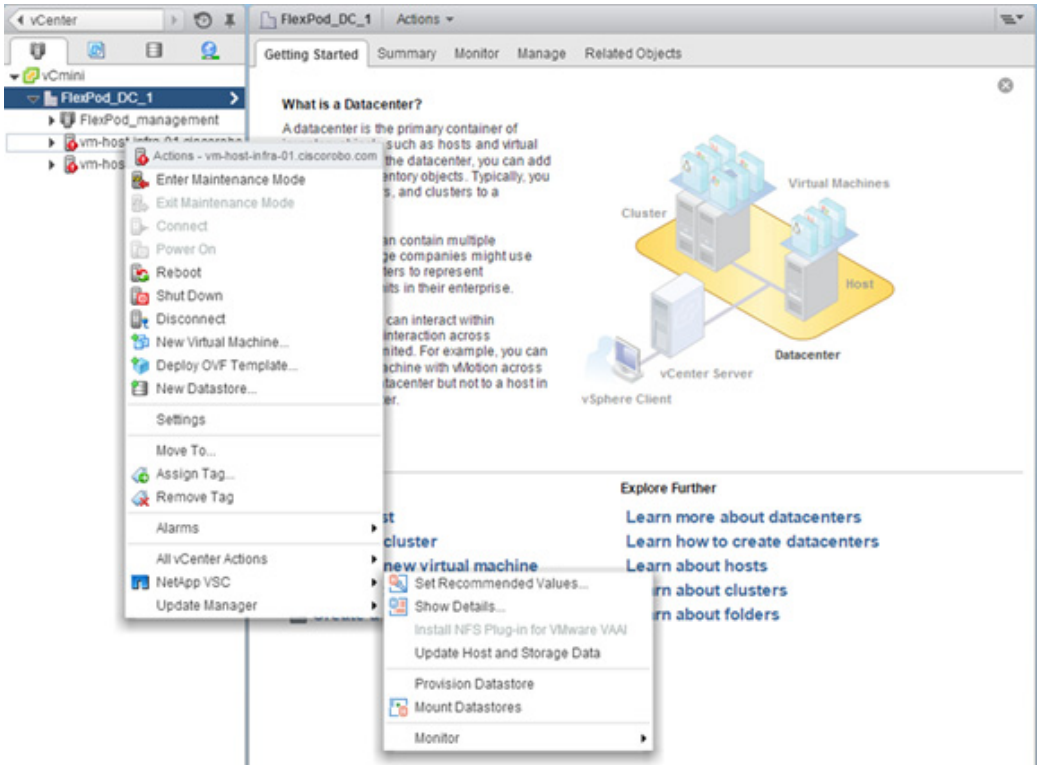
5. From VMware vSphere web client, verify that the storage systems are discovered.



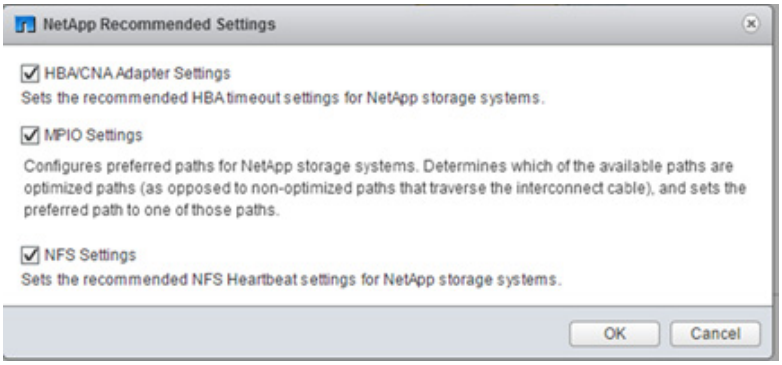
Optimal Storage Settings for ESXi Hosts

VSC allows storage-related settings to be automatically configured for all ESXi hosts connected to NetApp storage controllers. To use these settings, complete the following steps:

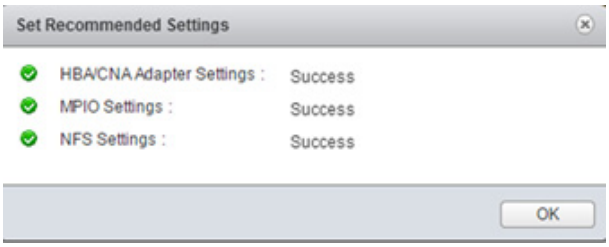
1. From the Home page, click vCenter > Hosts and Clusters.



2. Right-click each ESXi host and select NetApp VSC > Set Recommended Values.



3. Select the settings that you want to apply to the vSphere hosts and click OK to apply the settings.



4. Click OK.

VSC 5.0 Backup and Recovery

Prerequisites to use Backup and Recovery Capability

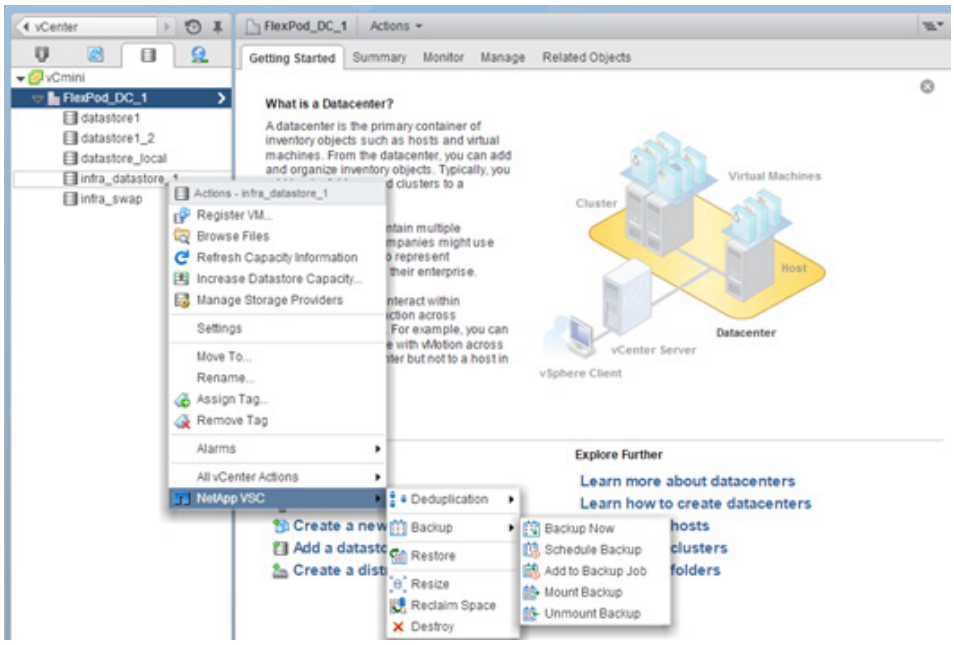
Before using the backup and recovery capability to schedule backups and restore datastores, virtual machines, or virtual disk files, make sure that the storage systems that contain the datastores and virtual machines for which you are creating backups have valid storage credentials.

If you plan to leverage the SnapMirror update option, add all of the destination storage systems with valid storage credentials.

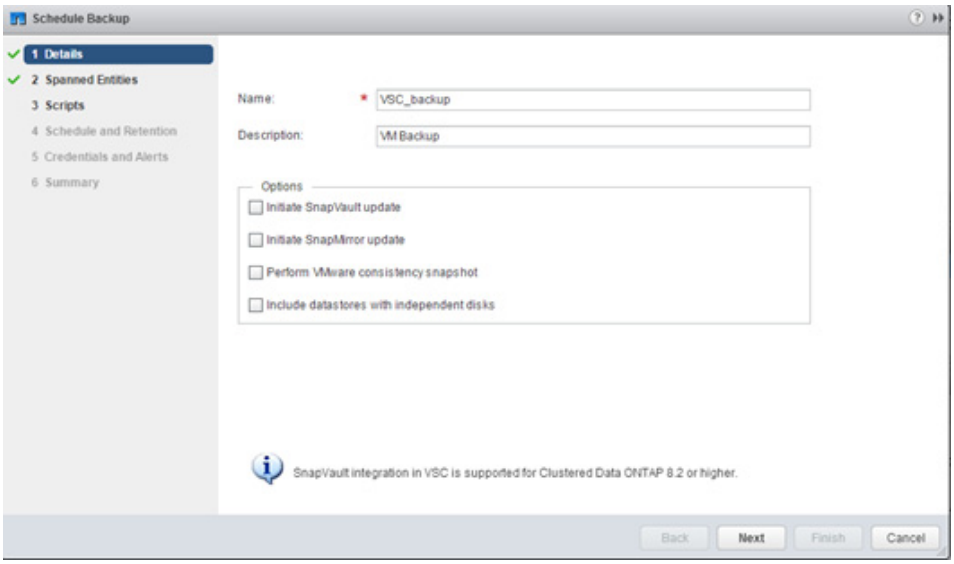
Backup and Recovery Configuration

To configure a backup job for a datastore, complete the following steps:

1. From the Home page, click the Home tab and click Storage.



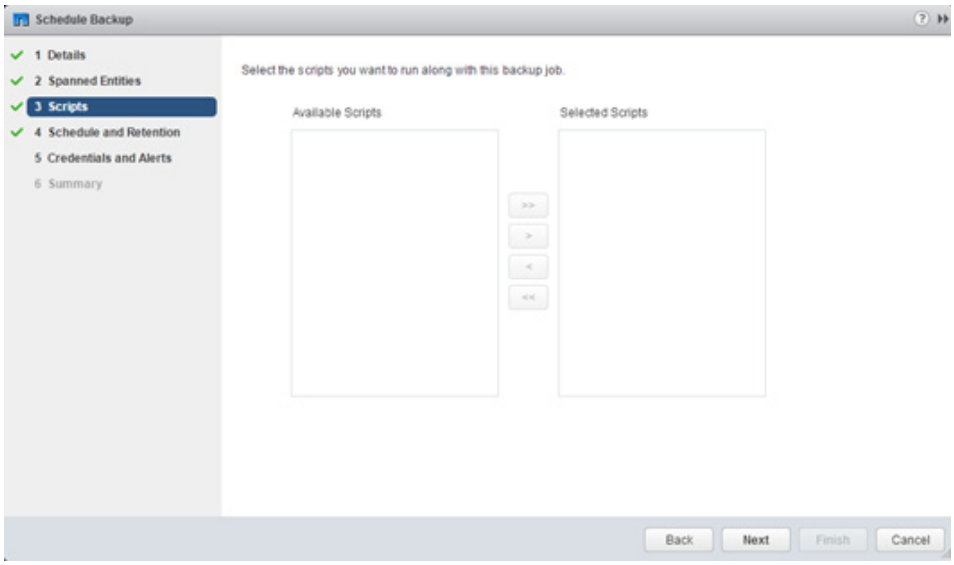
2. Right-click a datastore and select NetApp VSC > Backup > Schedule Backup.
3. To schedule a one-time backup, select Backup Now instead of Schedule Backup.



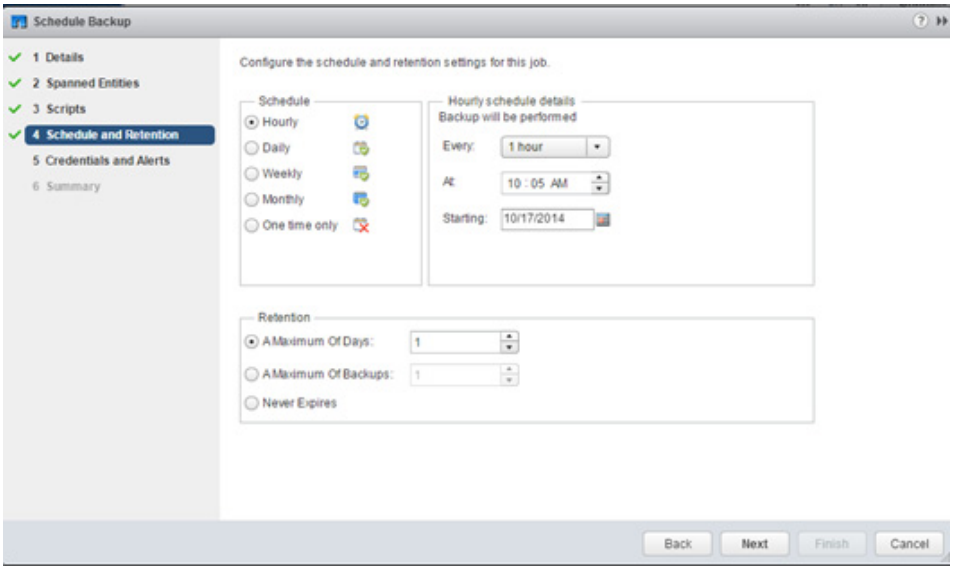
4. Enter a backup job name and description.

Note To create a VMware snapshot for each backup, select Perform VMware Consistency Snapshot in the Options pane.

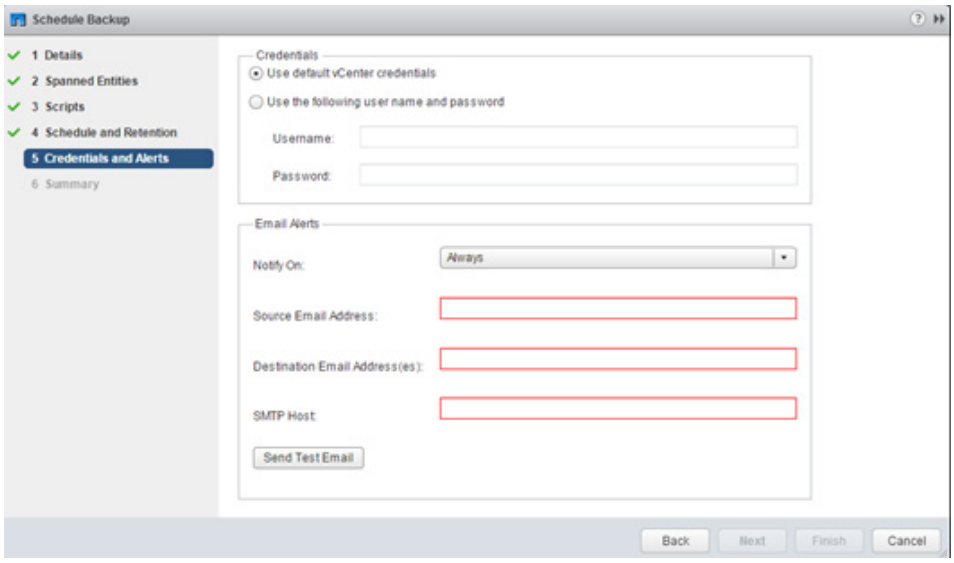
5. Click Next.
6. Click Next.



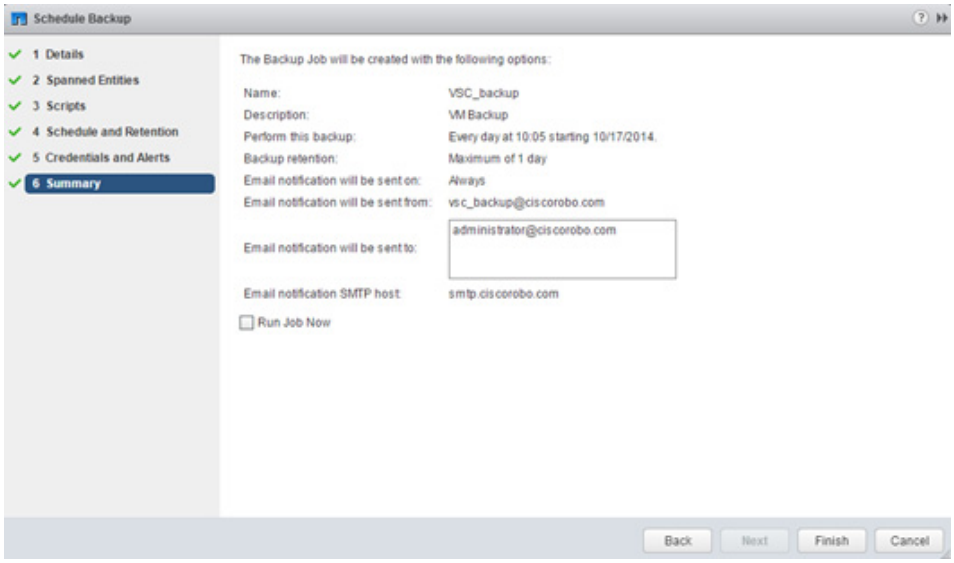
7. Select one or more backup scripts, if available, and click Next.



8. Select the hourly, daily, weekly, or monthly schedule for this backup job and click Next.
9. Use the default vCenter credentials or enter the user name and password for the vCenter Server and click Next.



10. Specify backup retention details as per requirements. Enter an e-mail address for receiving e-mail alerts. You can add multiple e-mail addresses by using semicolons to separate e-mail addresses. Click Next.



11. Review the summary page and click Finish. To run the job immediately, select the Run Job Now checkbox. Click Finish.

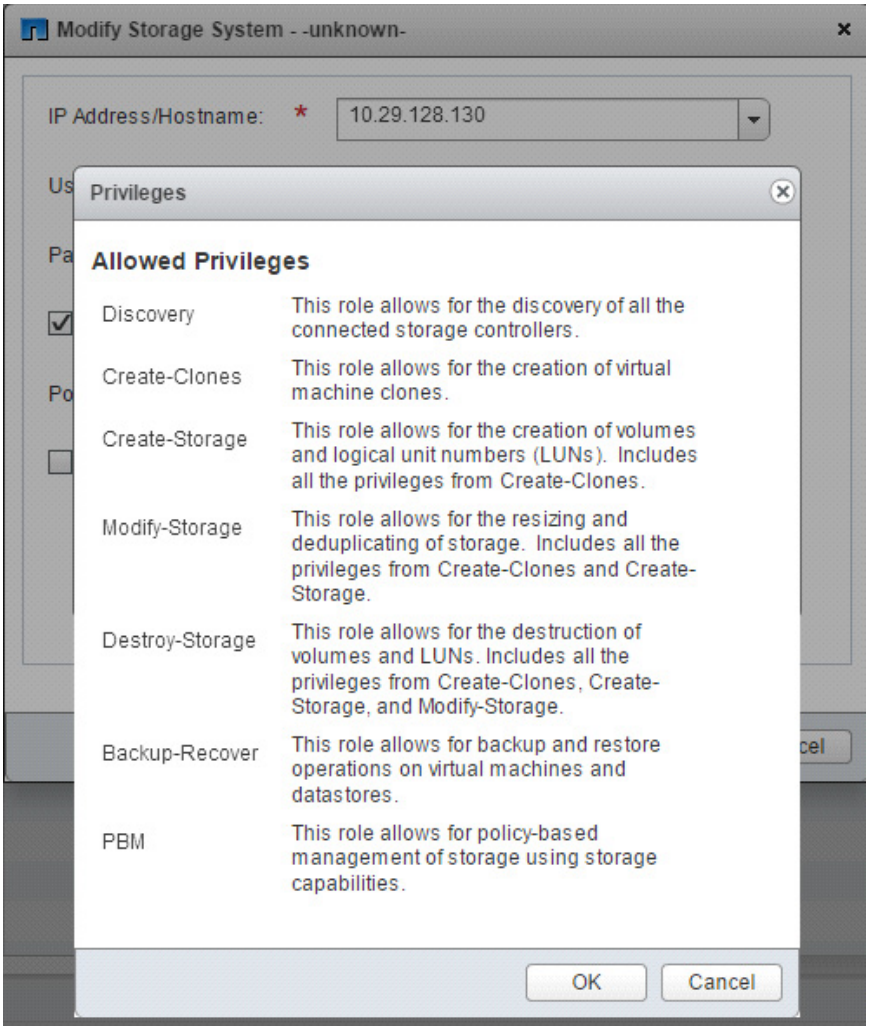
12. Click OK.

13. On the storage cluster interface, run the following command to disable automatic Snapshot copies of the volume:

```
volume modify -volume infra_datastore_1 -snapshot-policy none
```

14. Run the following command to delete any existing automatic Snapshot copies that have been created on the volume:

```
volume snapshot show -volume infra_datastore_1
volume snapshot delete -volume infra_datastore_1 <snapshot name>
```



15. Verify the allowed privileges on the storage system and click OK.

OnCommand Unified Manager 6.1

OnCommand Unified Manager OVF Deployment

To install the NetApp OnCommand® Unified Manager, complete the following steps:

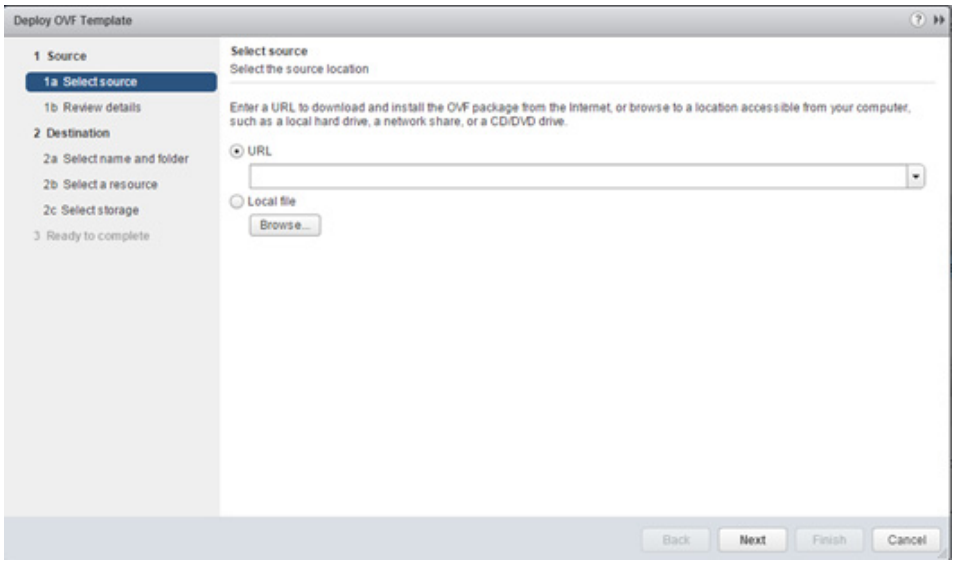
1. Download and review the OnCommand Unified Manager for Clustered Data ONTAP 6.1 Installation and Setup Guide.

Note VMware high availability for the Unified Manager virtual appliance is not supported. The virtual appliance can be deployed on a VMware server that is a member of a VMware high-availability environment, but using the VMware high-availability functionality is not supported.

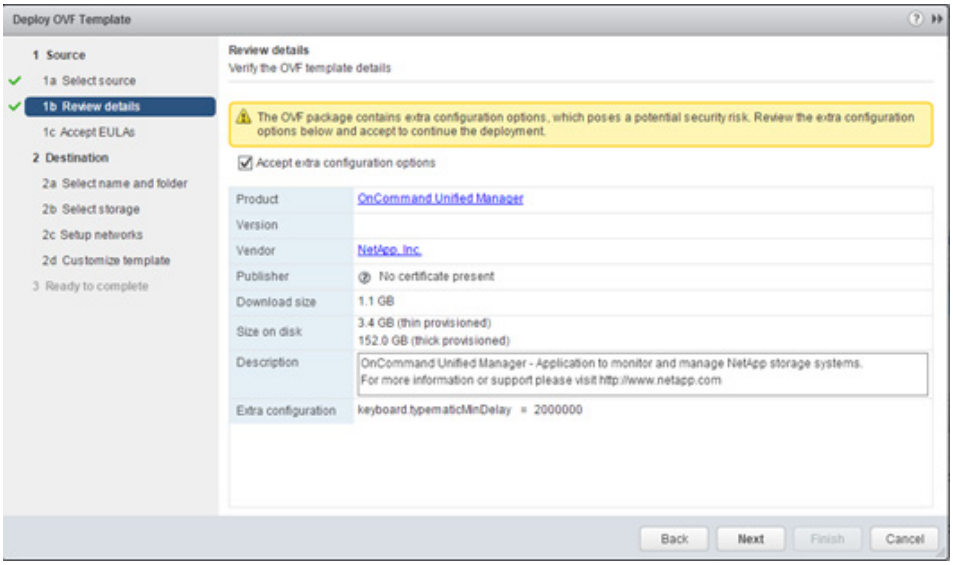
If deployment fails because of insufficient resources when using an HA-enabled environment, modify the following default VMware settings:

- Decrease the VM resources CPU and memory settings.
- Decrease the vSphere HA admission control policy to use less than the default percentage of CPU and memory.
- Modify the cluster features VM options by disabling the VM restart priority and leaving the host isolation response powered on.

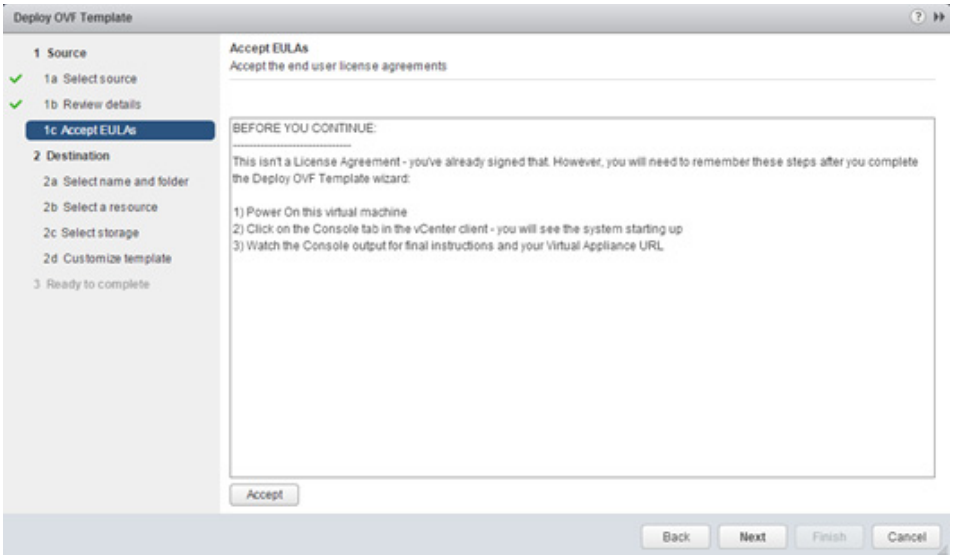
2. Download OnCommand Unified Manager (`OnCommandUnifiedManager-6.1.ova`) from the NetApp Support site.
3. Log in to the vSphere web client. Click vCenter > VMs and Templates.
4. At the top of the center pane, click Actions > Deploy OVF Template.



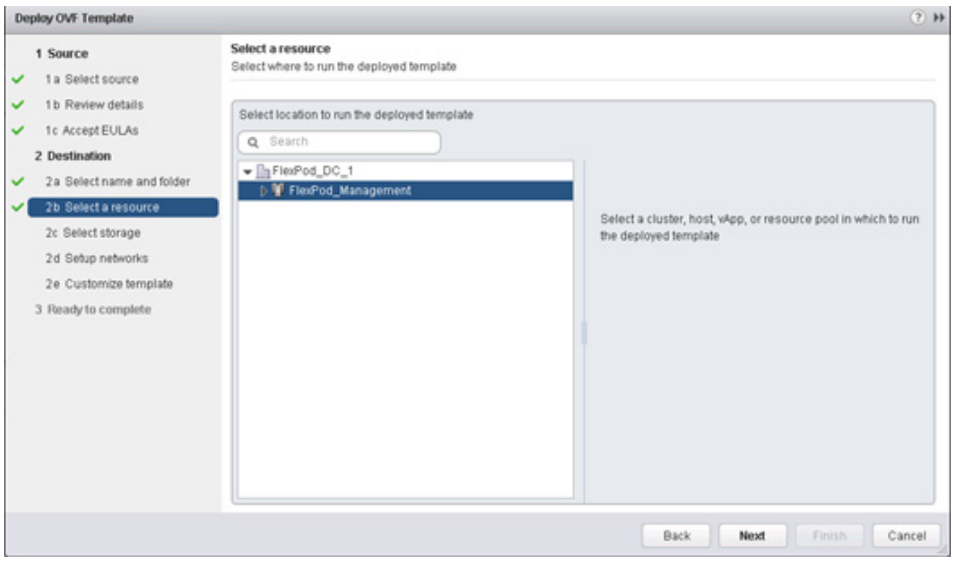
5. Click Browse to navigate to the .ova file that was downloaded locally. Click Open to select the file.



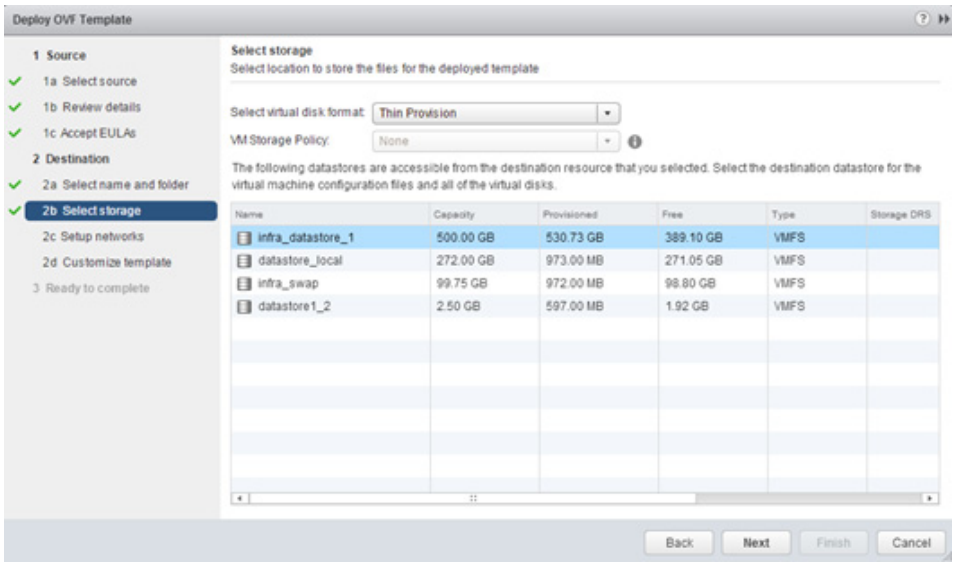
6. Select the Accept Extra Configuration Options checkbox and click Next.



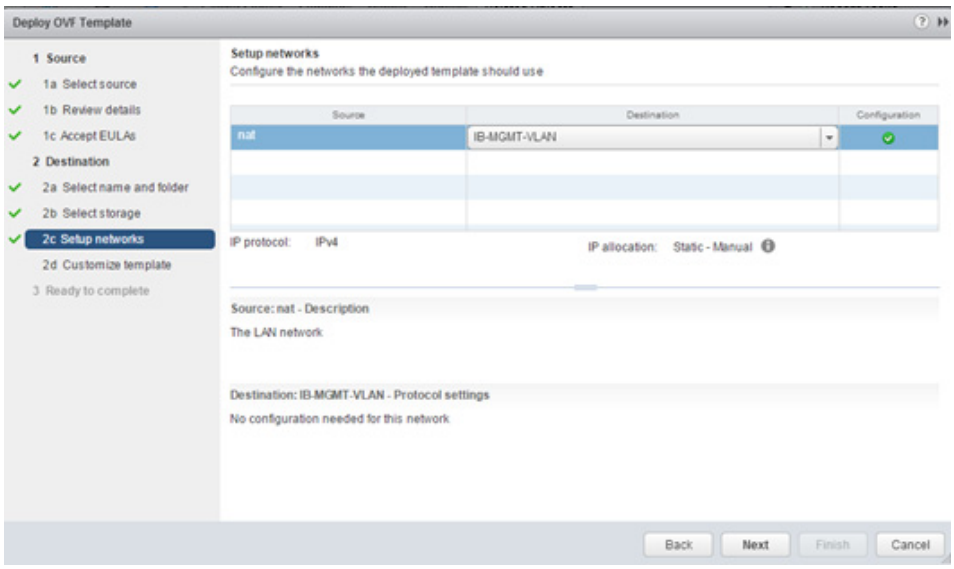
7. Select the checkbox to accept the extra configuration options and click Next.
8. Read the EULA and click Accept to accept the agreement. Click Next.
9. Enter the name of the VM and select the FlexPod_DC_1 folder to hold the VM. Click Next.



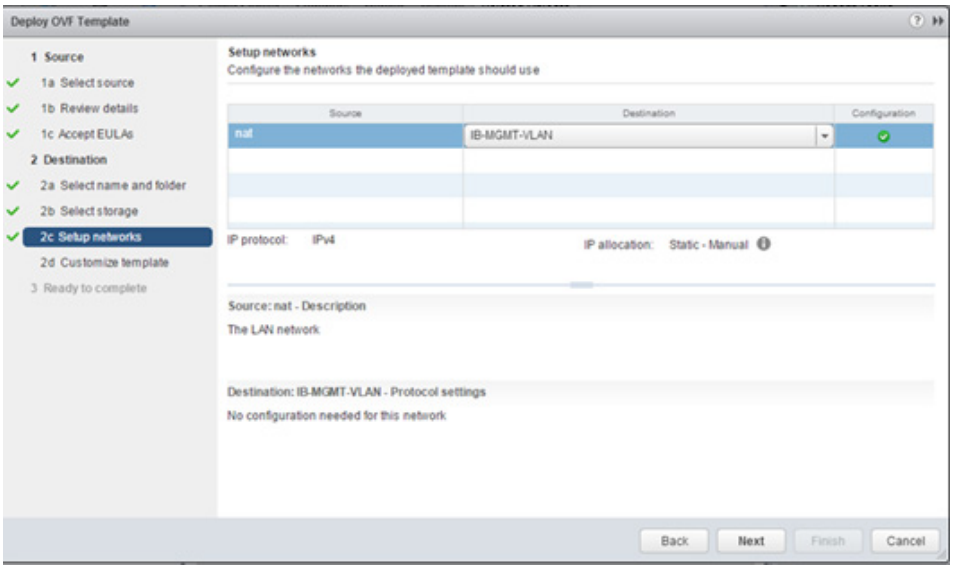
10. Select FlexPod_Management within the FlexPod_DC_1 datacenter as the destination compute resource pool to host the VM. Click Next.



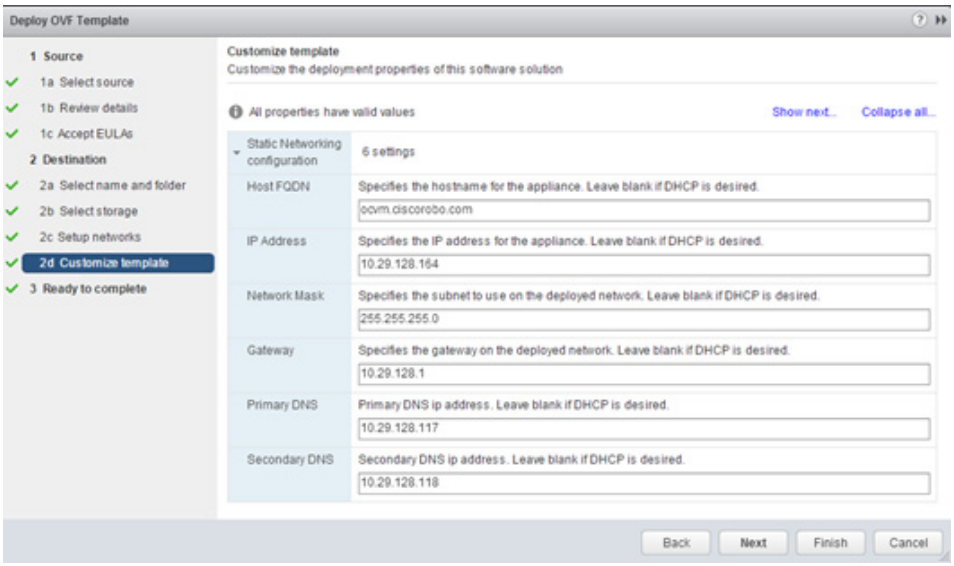
11. Select infra_datastore_1 as the storage target for the VM and select Thin Provision as the virtual disk format. Click Next.



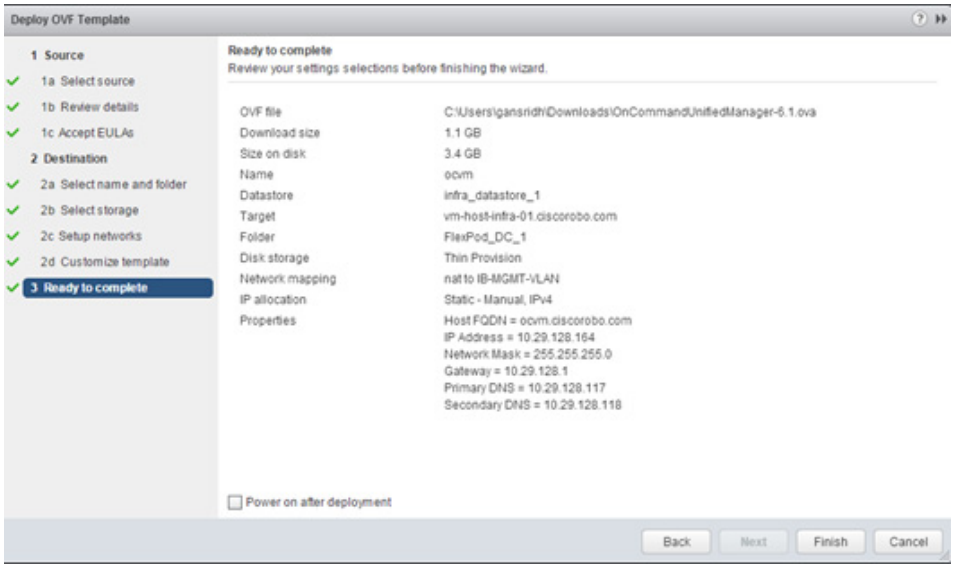
12. Select IB-MGMT Network as the destination network for the nat source network. Click Next.



13. Enter the hostname, IP address, network subnet mask, gateway, and DNS information.



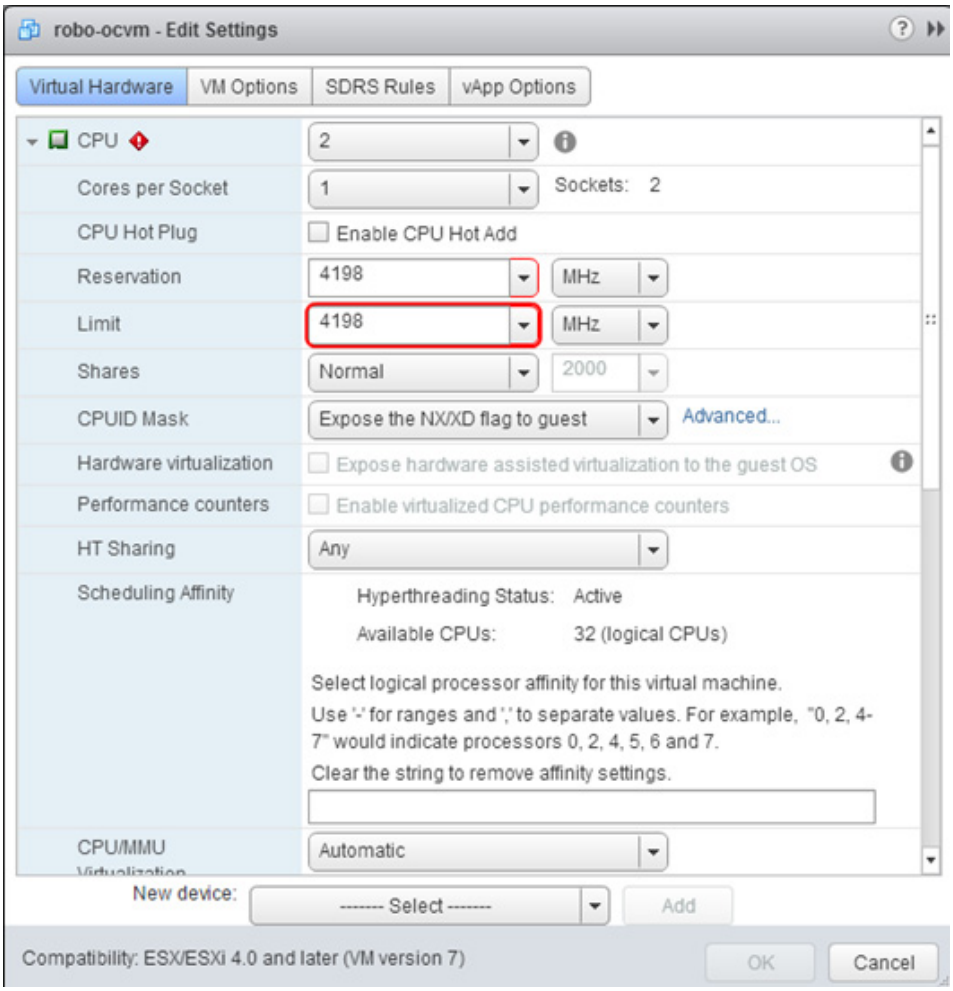
14. Verify the details for the host name, IP address, network mask, gateway, primary DNS, and secondary DNS. Click Finish.



15. Do not select the Power On After Deployment checkbox.
16. Review the configuration details. Click Finish.
17. In the left pane, click Virtual Machines. Right-click the newly created virtual machine, and select Edit Settings.
18. Click the CPU tab to expand the CPU options.
19. Set the number of CPUs to match the number of CPUs present in the host.
20. Set the reservation and limit (MHz values) by using the following calculation:

    (Number of CPUs) × (Processor speed of the CPUs in the host)

For example, if a host has two CPUs operating at a speed of 2099MHz, then the reservation and limit should be set to 4198.



Note To determine the proper resource size for your environment, refer to the OnCommand Unified Manager 6.1 Sizing Guide.

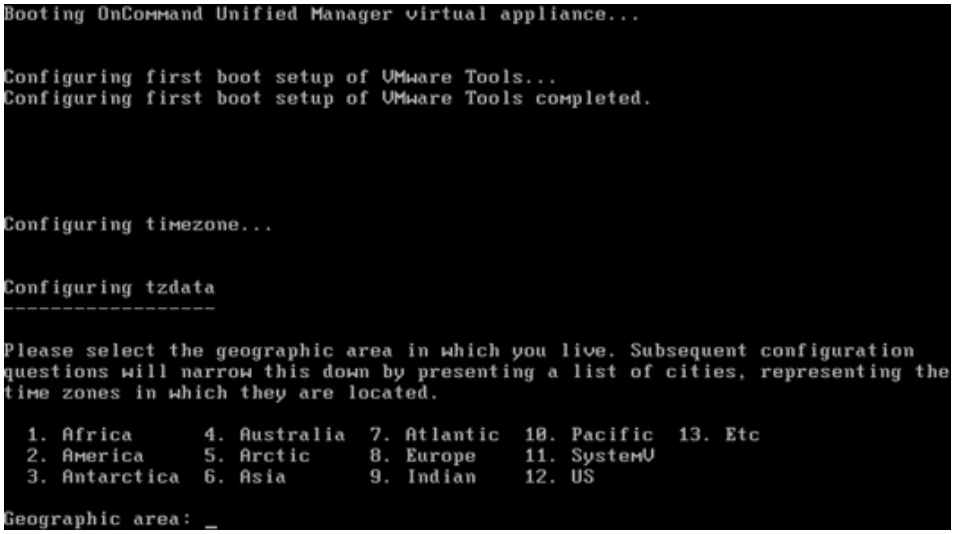
21. Click OK to accept the changes.
22. Right-click the VM in the left-hand pane and click Power On.

OnCommand Unified Manager Basic Setup

To perform the basic setup for OnCommand Unified Manager, complete the following steps:

1. Right-click the VM in the left-hand pane. Click Open Console.
2. Set up OnCommand Unified Manager by answering the following questions in the console window:

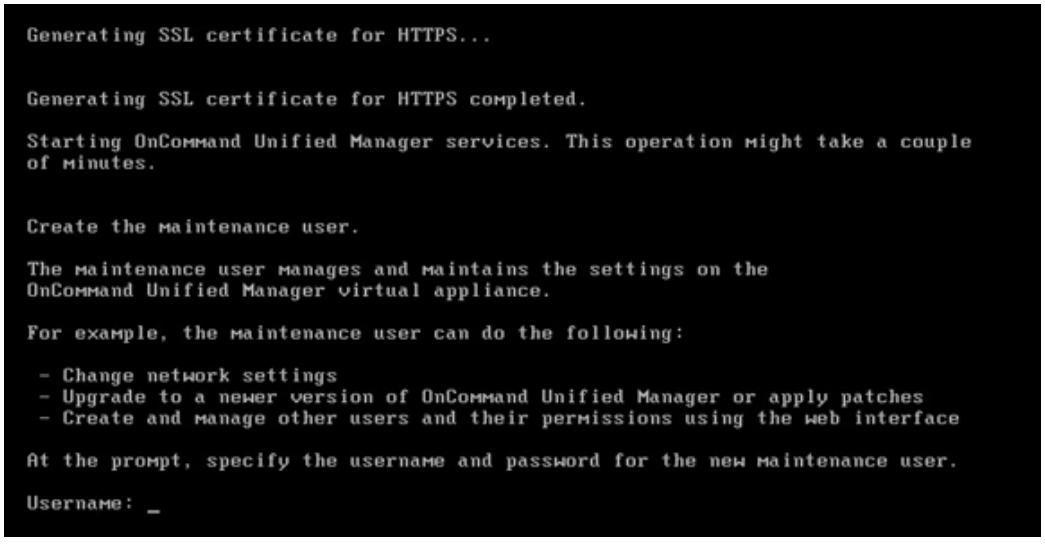
```
Georaphic area: <<Enter your geographic location>>
Time zone: <<Select the city or region corresponding to your time zone>>
```



3. Create a maintenance user account.

Note The maintenance user manages and maintains the settings on the OnCommand Unified Manager virtual appliance.

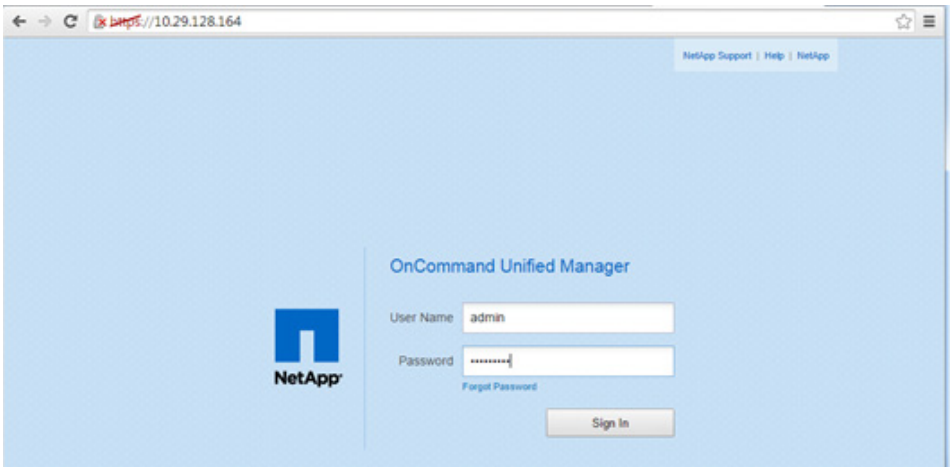
```
Username : admin
Enter new UNIX password: <<var_password>>
Retype new UNIX password: <<var_password>>
```



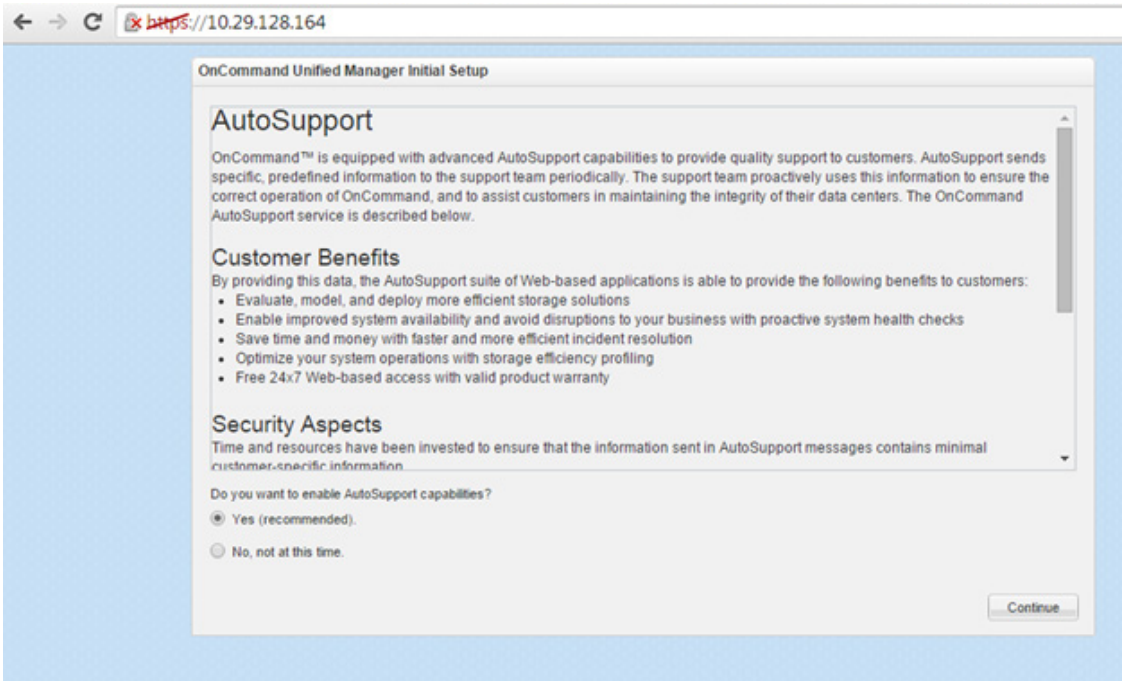
OnCommand Unified Manager Initial Setup

To perform the initial setup for OnCommand Unified Manager, complete the following steps:

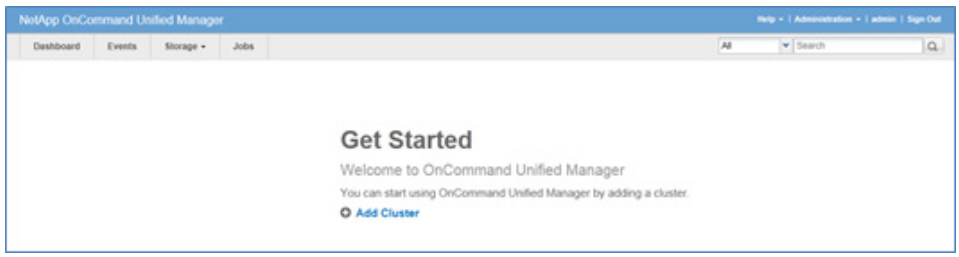
1. Using a web browser, navigate to the OnCommand Unified Manager using the URL: `https://<<var_oncommand_server_ip>>`.



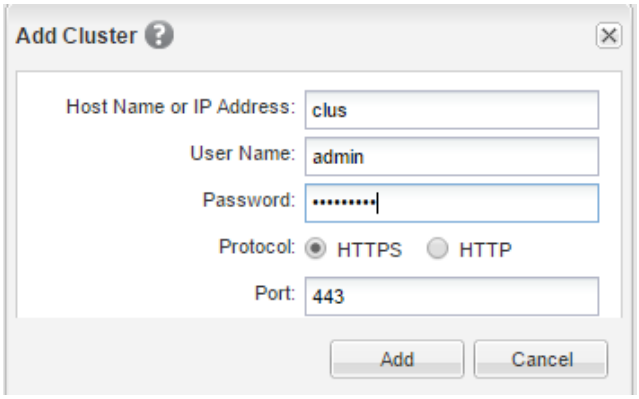
2. Log in by using the maintenance user account credentials.
3. Select Yes to enable AutoSupport capabilities.



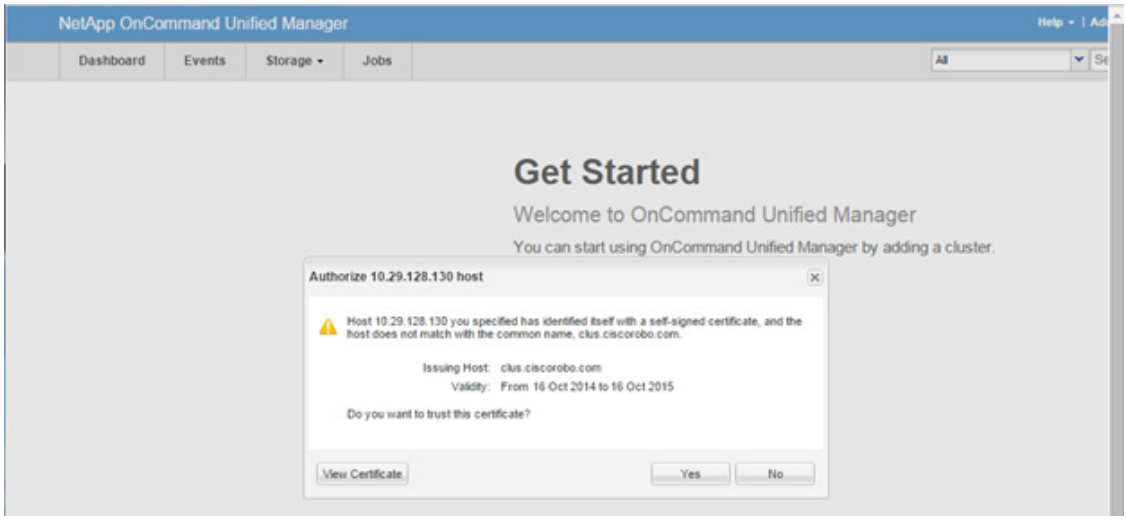
4. Click Continue.
5. Enter the NTP Server IP address `<<var_global_ntp_server_ip>>`.
6. Enter the Maintenance User Email `<<var_storage_admin_email>>`.
7. Enter the SMTP Server Hostname.
8. Click Save.
9. Click Add Cluster.



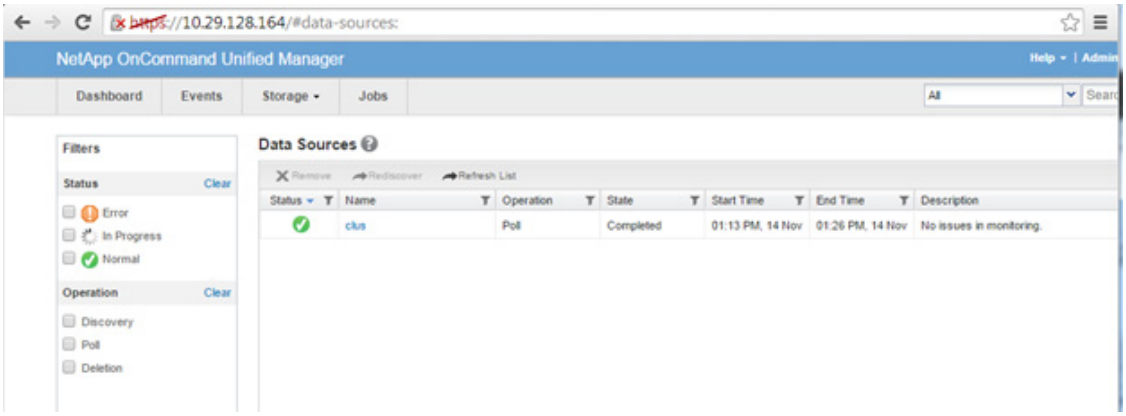
10. Enter the cluster management IP address, user name, password, protocol, and port.



11. ClickAdd.



12. Click Yes.
13. The cluster add operation might take a couple of minutes.
14. After the cluster is added, click the Storage tab and select Clusters to access the cluster.

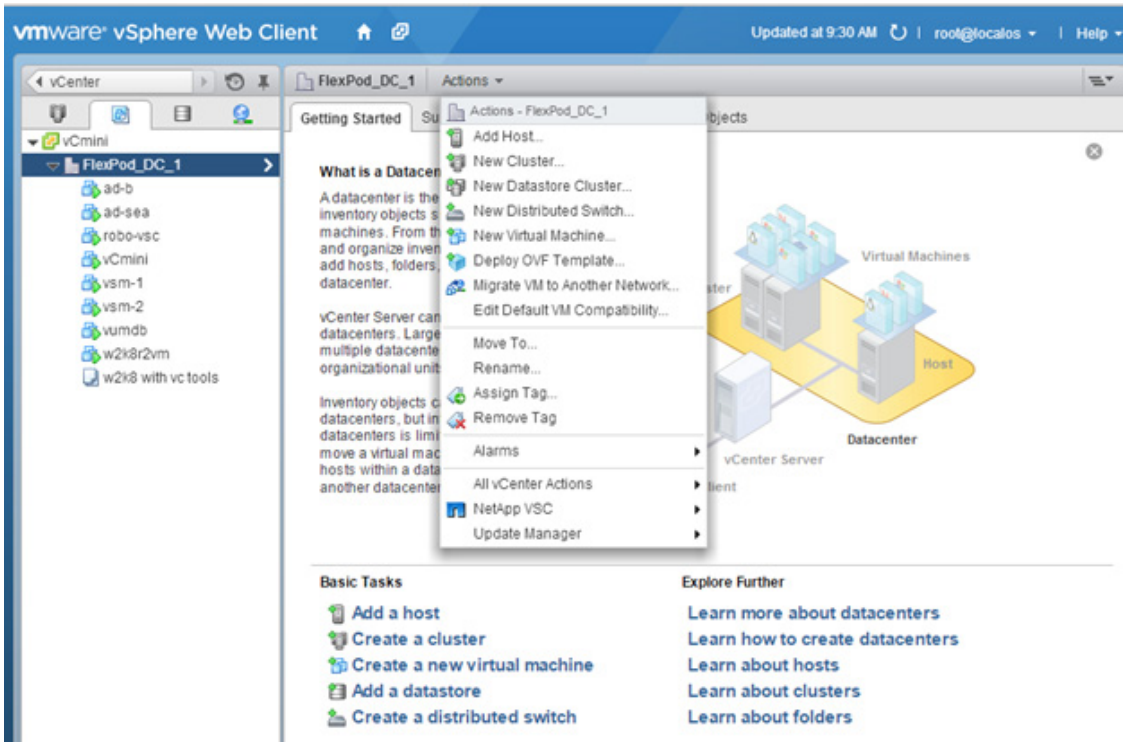


NetApp VASA Provider for Clustered Data ONTAP Deployment Procedure

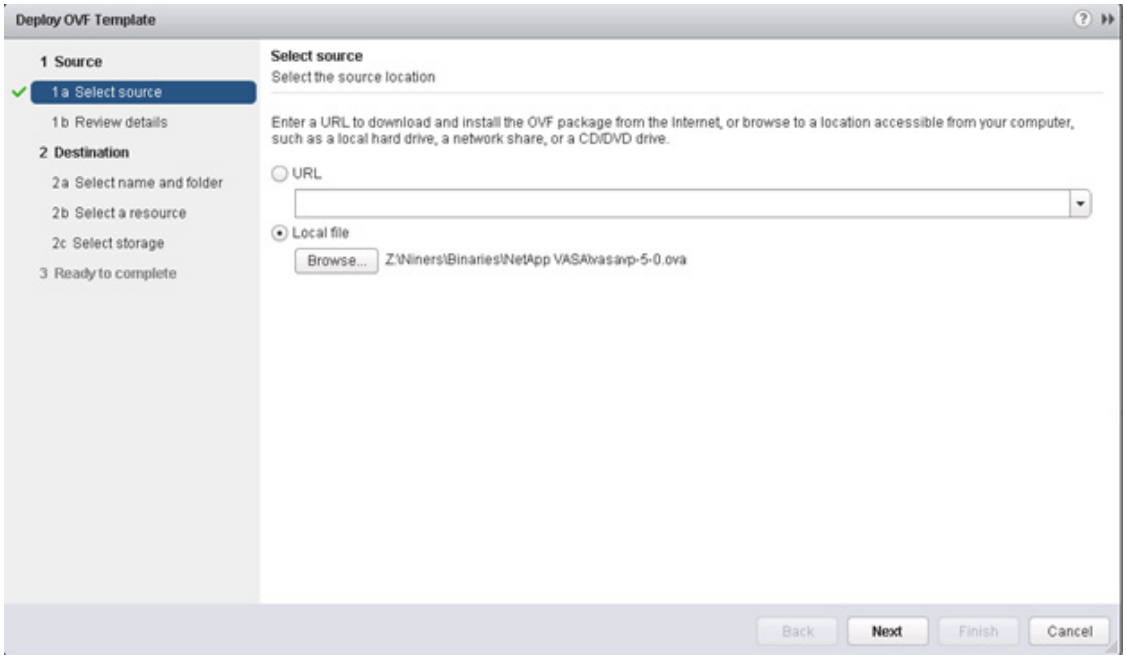
VASA Provider for clustered Data ONTAP uses VMware VASA (vSphere APIs for Storage Awarenessto provide better storage management. By providing information about storage used by Virtual Storage Console for VMware vSphere to the vCenter Server, VASA Provider enables you to make more intelligent virtual machine provisioning decisions and allows the vCenter Server to warn you when certain storage conditions may affect your VMware environment. Virtual Storage Console for VMware vSphere is the management console for VASA Provider.

To install the NetApp VASA provider, complete the following steps:

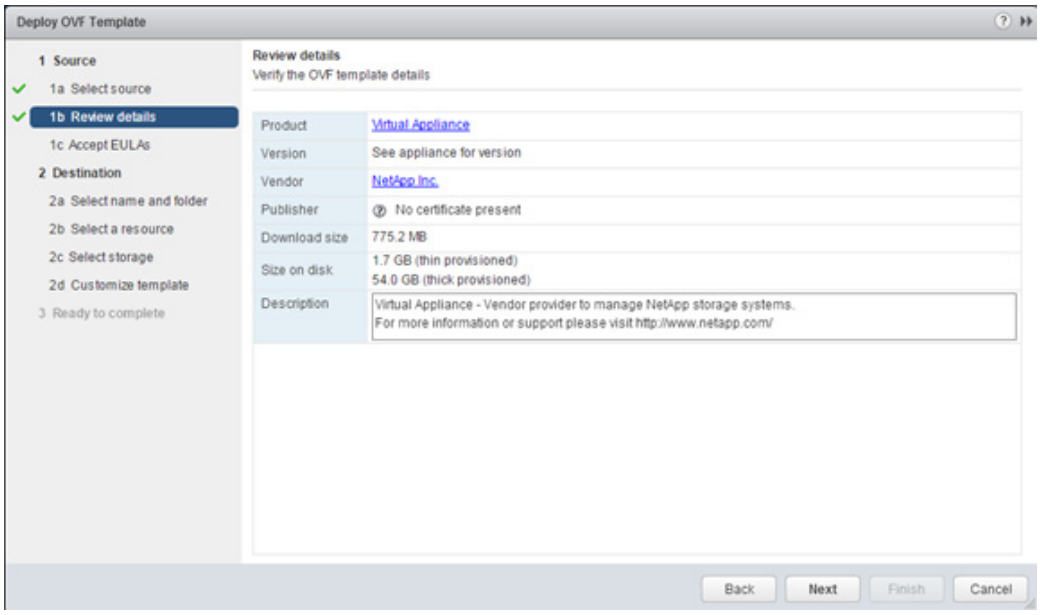
1. Download the VASA provider from NetApp support site.
2. Log into the vSphere Web Client. Go to vCenter > VMs and Templates
3. At the top of the center pane, click Actions > Deploy OVF Template.



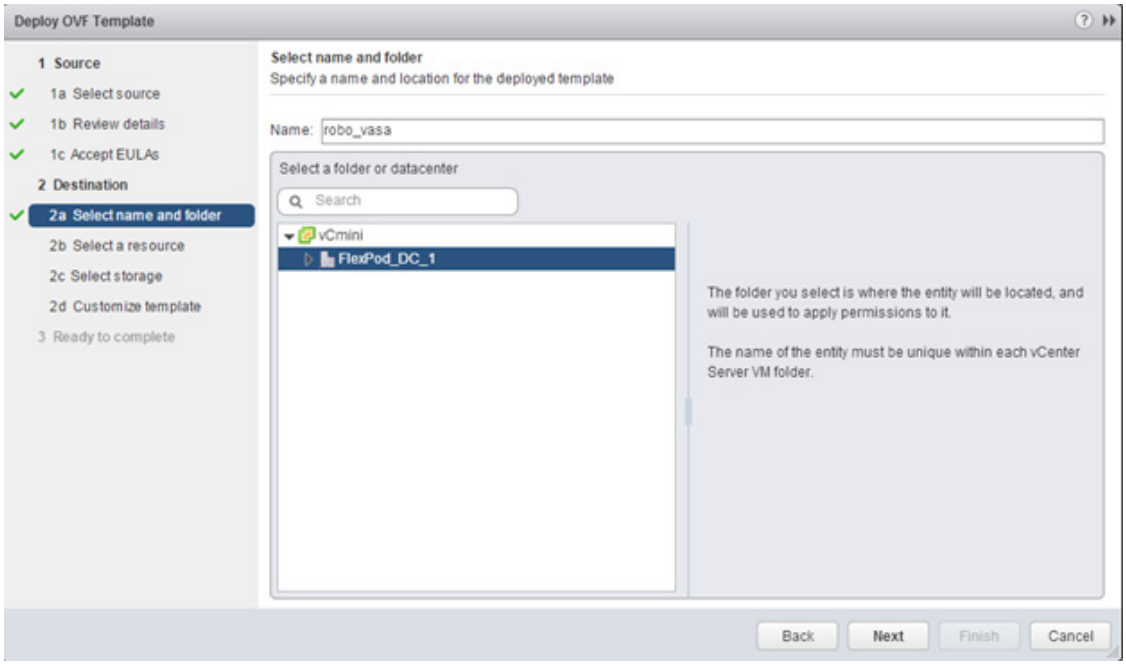
4. Browse the .ova file that was downloaded locally. Click Open to select the file.



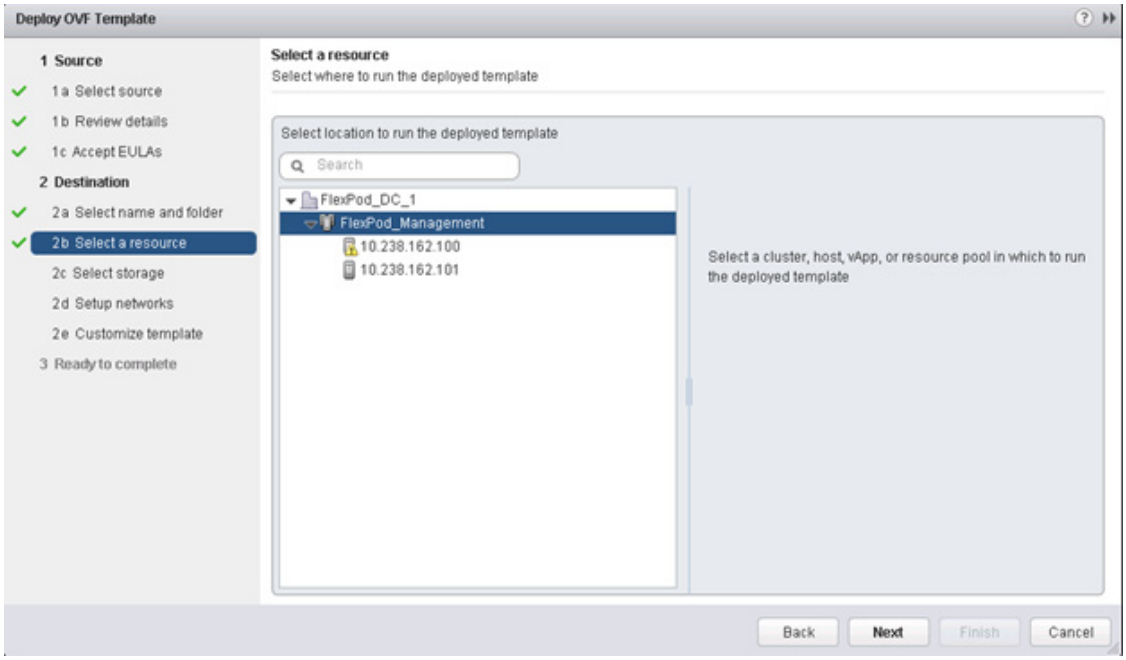
5. Click Next to proceed with the selected file.
6. Click Next.



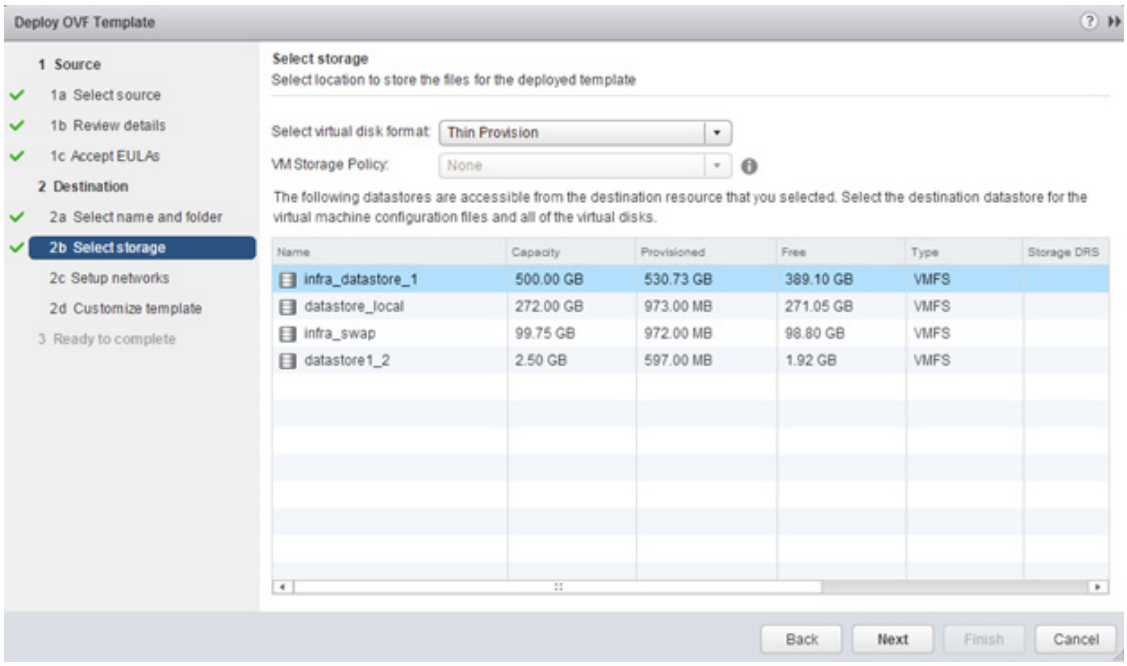
7. Read the EULA, then click the Accept button to accept the agreement. Click Next to continue.
8. Enter the name of the VM and select the `FlexPod_DC_1` folder to hold the VM. Click Next to continue.



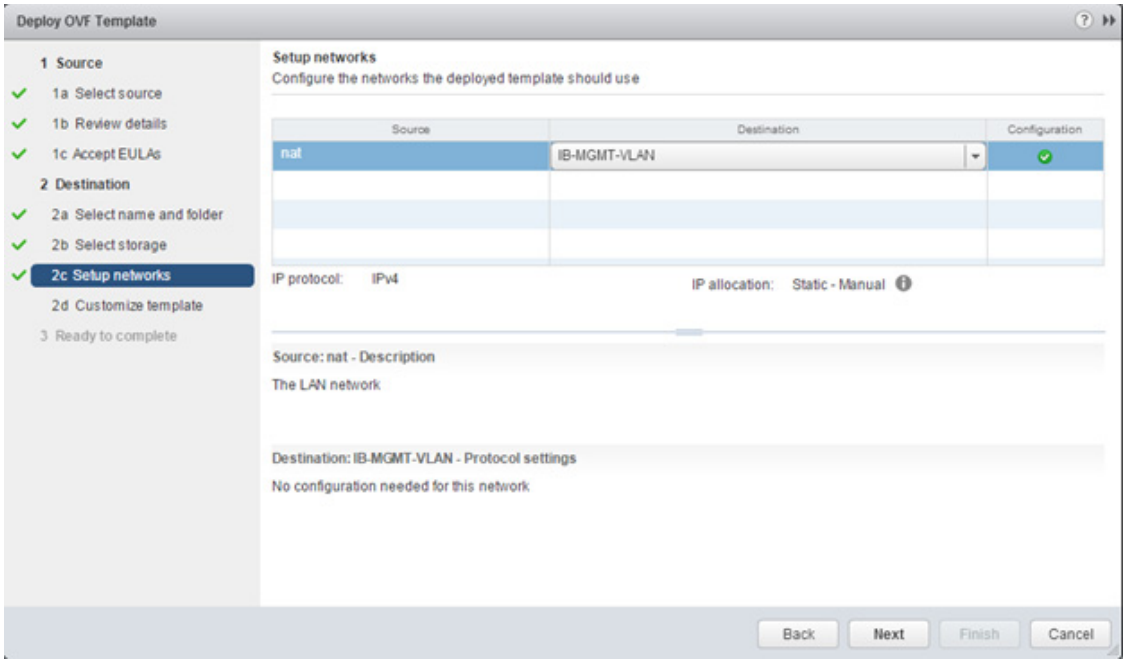
9. Select FlexPod_Management within the FlexPod_DC_1 Datacenter as the destination compute resource pool to host the VM. Click Next to continue.



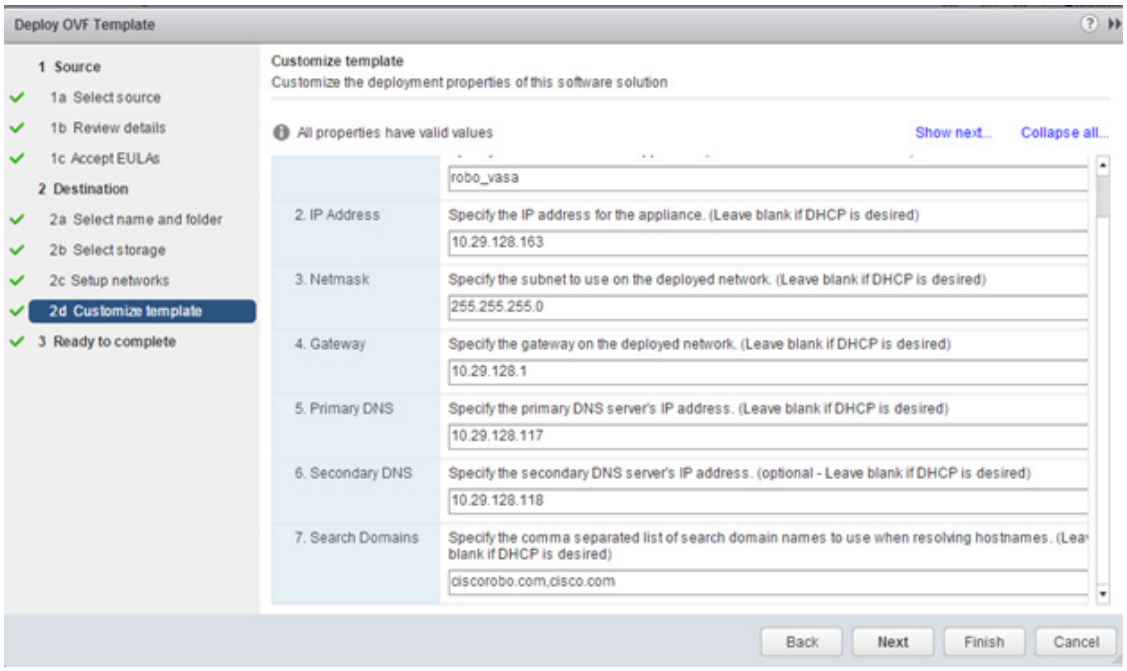
10. Select `infra_datastore_1` as the storage target for the VM and select Thin Provision as the Virtual disk format. Click Next to continue.



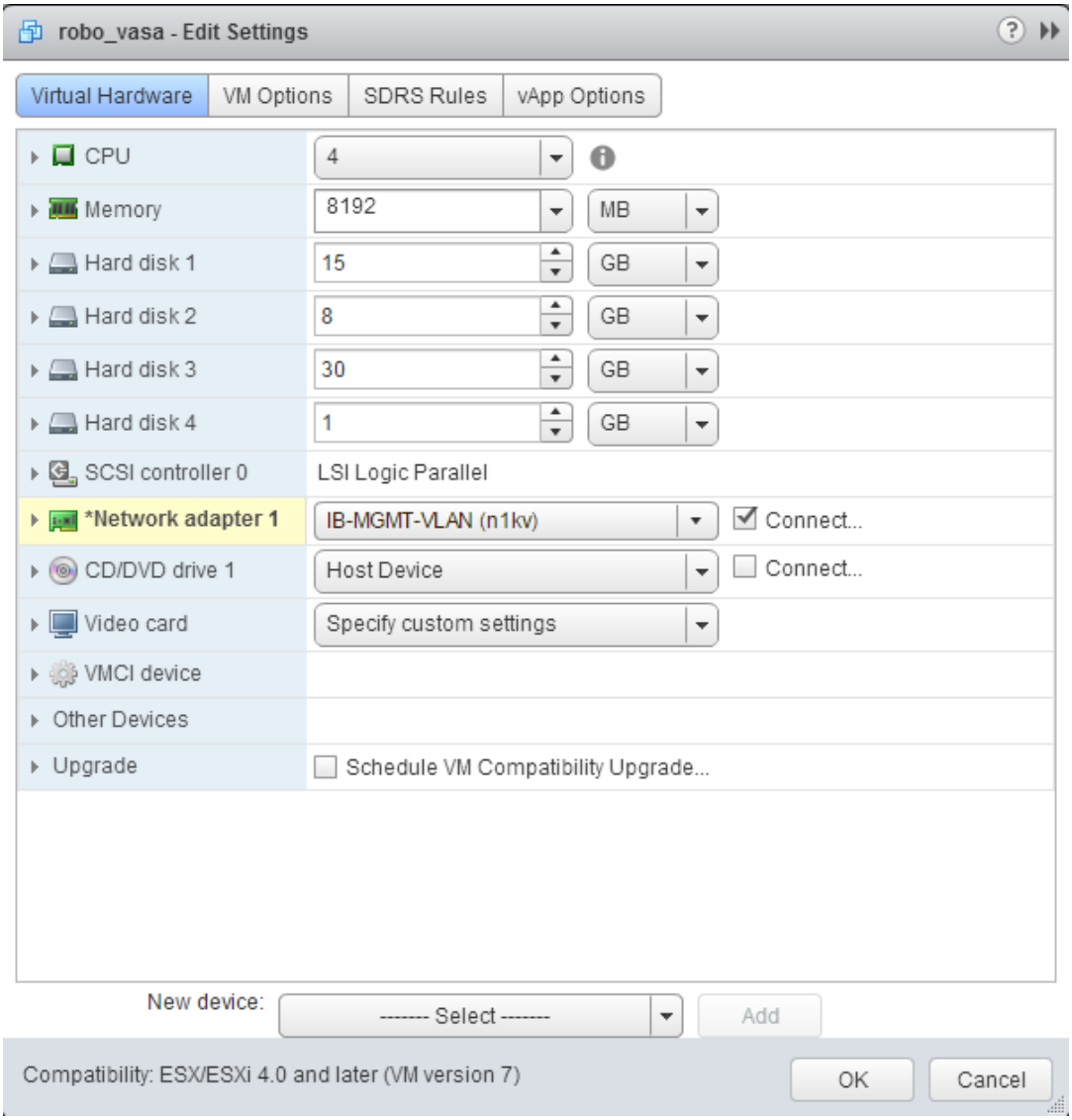
11. Select IB-MGMT Network as the destination network to the nat source network. Click Next.



12. Fill out the details for the host name, IP address, network mask, gateway, primary DNS, and secondary DNS. Click Next.



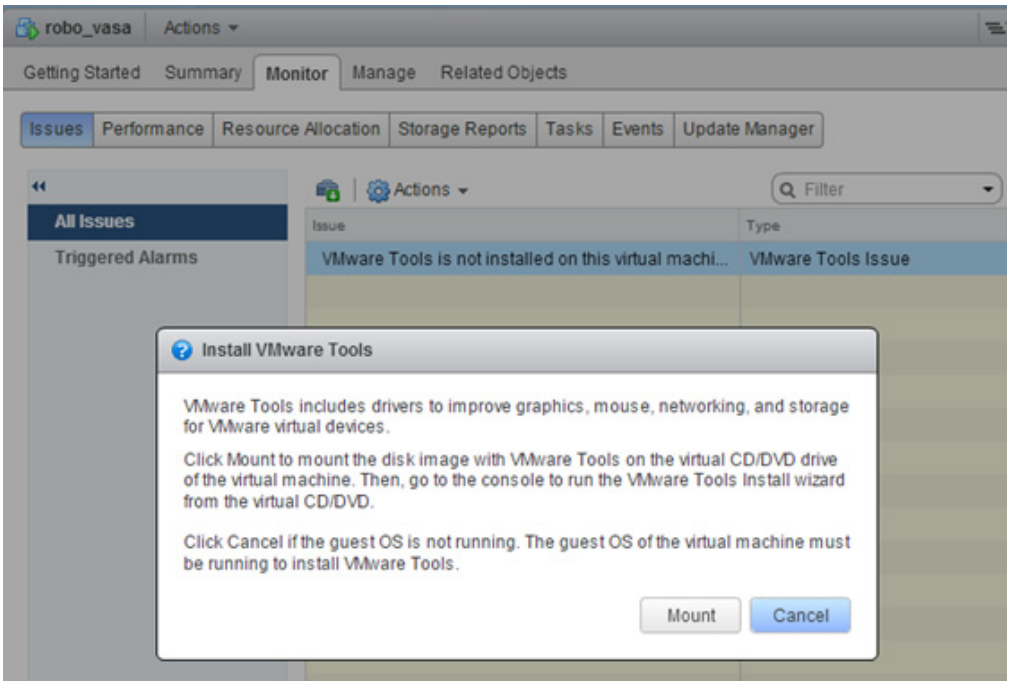
13. Leave Power on after deployment unchecked and click Finish.
14. After the Virtual Machine is created, make changes to the Network adapter, if required and Click OK.



15. Power on the Virtual Machine
16. Right-click the VASA VM and click Open Console. VASA Provider installation will prompt for installing the VMware tools.

```
VMware Tools installation


Before you can continue the VASA Provider installation, you must install
 the VMware Tools:

   1.  Select VM > Guest > Install/Upgrade VMware Tools.

   2.  Follow the prompts provided by the VMware Tools wizard.
       * If VMware Tools are currently installed, select the option
         "Interactive Tools Upgrade".
       * If this the first time you have deployed VMware Tools, click OK
         at the "Install VMware Tools" pop-up box.

Now press ENTER to continue the VASA Provider installation.


Searching for VMware Tools archive...
Unpacking VMware Tools archive...
Running VMware Tools install script..
_
```

17. In the web client, click on the VASA VM. Click Summary tab.
18. Click Install VMware Tools and switch back to VASA VM console window.

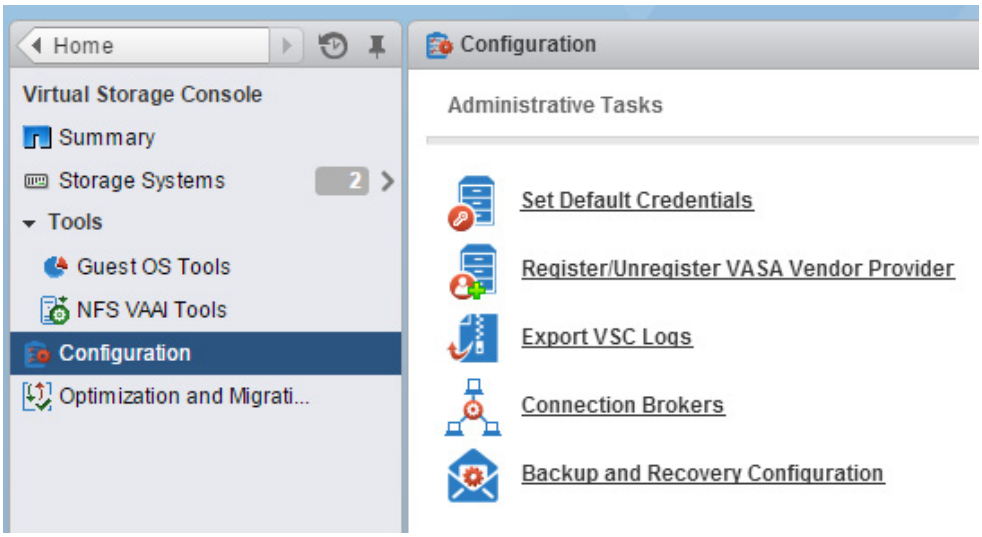


19. In the VASA VM console, press Enter to continue the VASA provider installation.
20. Switch back to web client. Right-click VASA VM and select Edit Settings. Set CD/DVD device type to Client Device.
21. Switch back to VASA VM console window and press Enter to reboot the VM.
22. Upon reboot, the VASA appliance will prompt for maint and vpserver passwords. Type the new passwords accordingly.

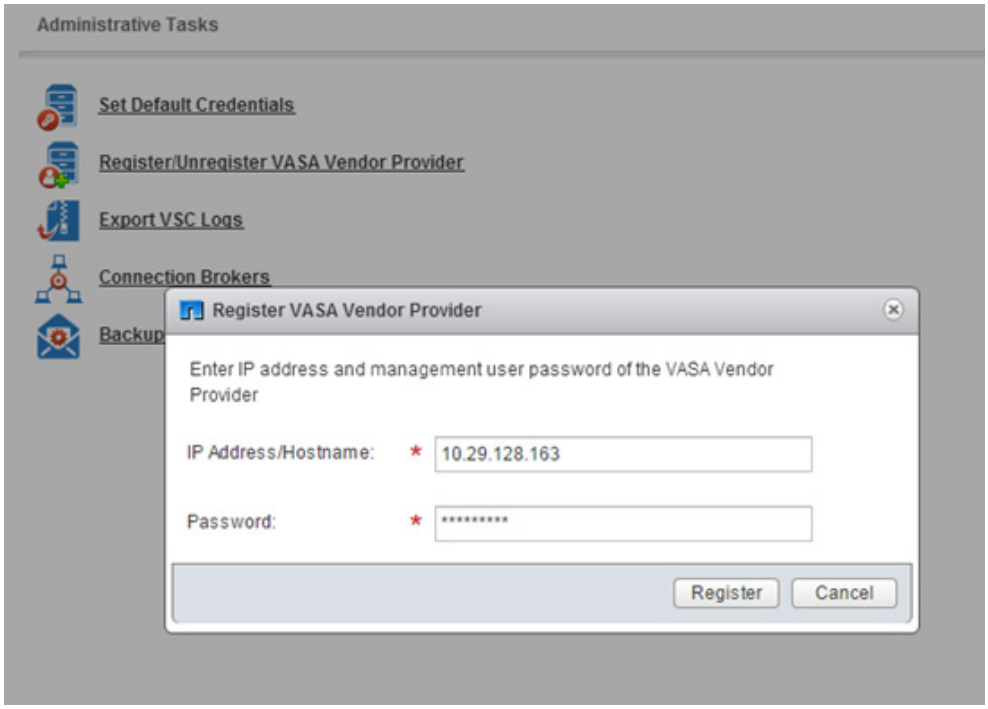
Registering VASA Provider for Clustered Data ONTAP with VSC

To register the VASA provider for clustered Data ONTAP, complete the following steps:

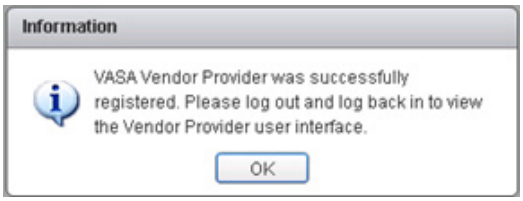
1. Log in to the web client and click Virtual Storage Console.
2. Click Configuration.
3. Click Register/Unregister VASA Vendor Provider.



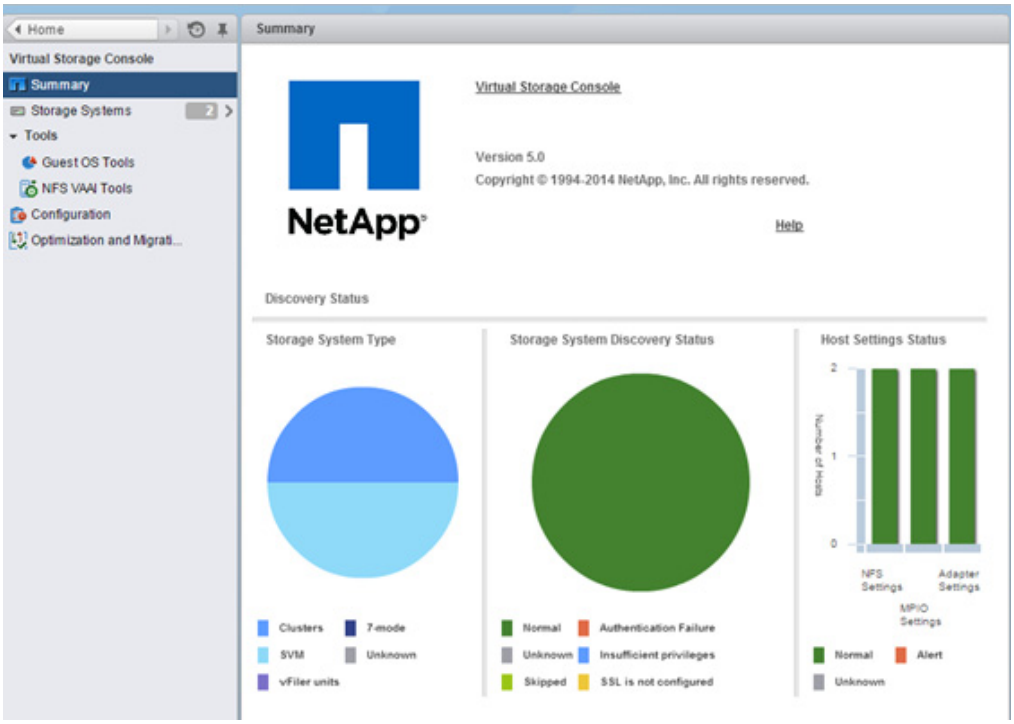
4. Enter the IP address and password for the VASA VM. Click Register.



5. Click OK in the message box, log out of the web client, and log back in to view the vendor provider user interface.



6. Review the Virtual Storage Console Summary page.



Appendix

Build Windows Active Directory Server VM(s)

For detailed guidance deploying a Windows Active Directory server, refer to one of the following documents:

- Windows 2012R2 http://technet.microsoft.com/en-us/library/jj574166.aspx
- Windows 2008R2 http://technet.microsoft.com/en-us/library/cc755059(v=ws.10).aspx

Network Connectivity at Branch

FlexPod infrastructure is deployed at the Data Center to manage multiple branches from a central location.

To address the network connectivity failure issue, it is recommended to have an additional Active Directory machine at each branch. This approach allows the local (Branch) administrators can continue to manage the local infrastructure needs in case of WAN link connectivity issue.

Cisco UCS Central - Multi Domain Management

Cisco UCS Central software manages multiple, globally distributed Cisco UCS domains with thousands of servers from a single pane. In a deployment with this solution at the DataCenter, Cisco UCS Central can be used to globally setup and manage the Cisco UCS Managers at multiple branch offices. The branch office setups of this solution will be detailed in the FlexPod Express with Cisco UCS Mini Deployment Guide.

This section provides a detailed overview of Cisco UCS Central setup in standalone mode.

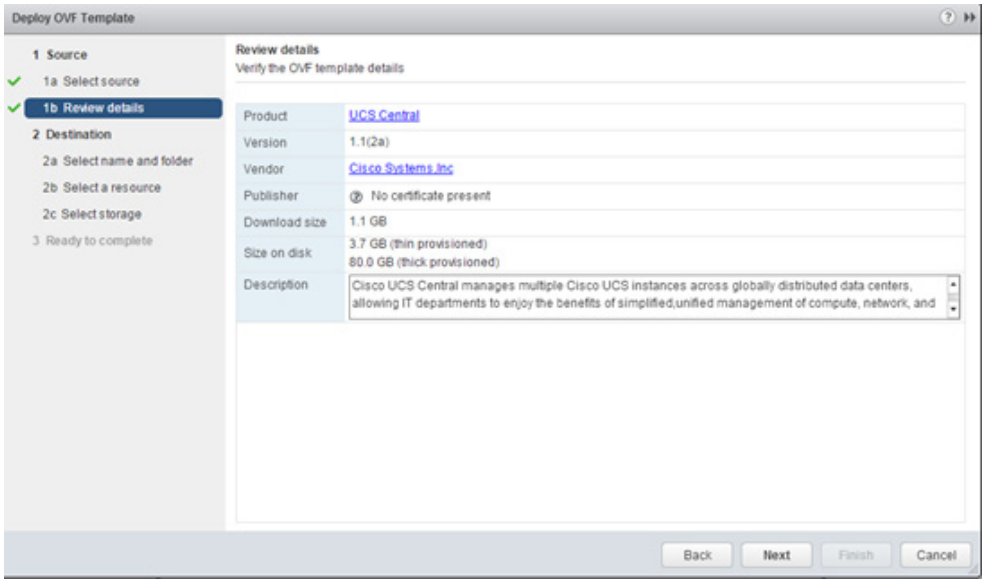
The installation and upgrade guide is available at: http://www.cisco.com/en/US/docs/unified_computing/ucs/ucs-central/install-upgrade/1.1/b_UCSC_Installation_and_Upgrade_Guide_11.html

Obtain the Cisco UCS Central Software

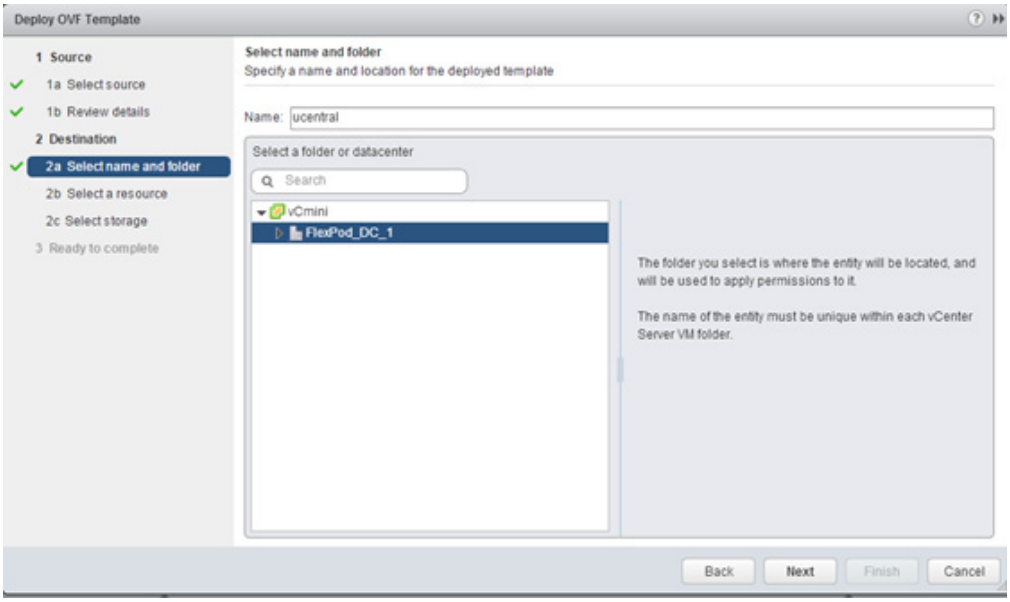
1. Navigate to the Cisco UCS Central Download page.
2. Download the OVA file ucs-central.1.1.2a.ova.

Install the Cisco UCS Central Software

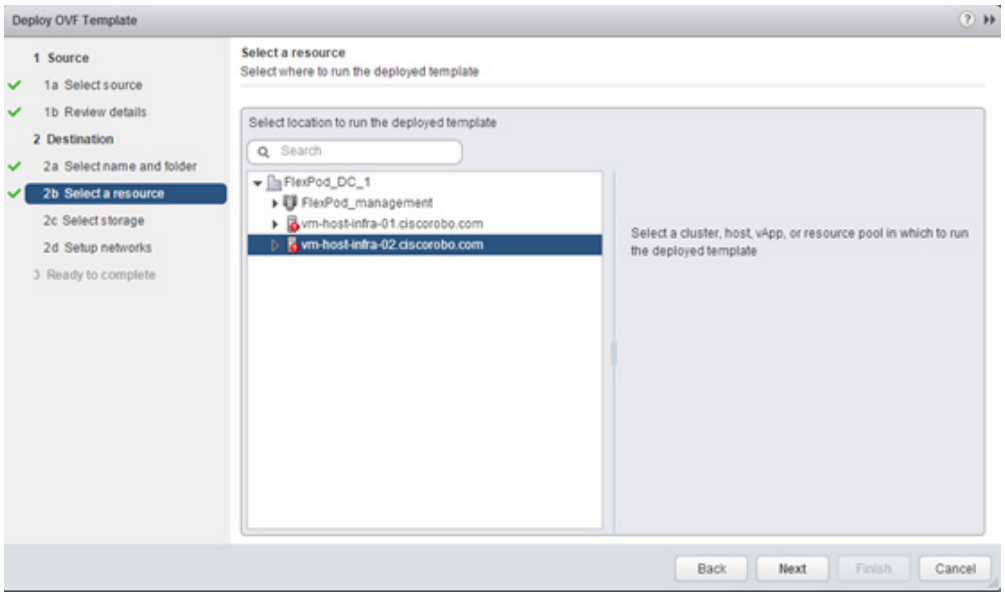
1. Using the vSphere web client, log in to the vCenter Server as FlexPod admin user.
2. Go to vCenter > VMs and Templates. At the top of the center pane, click Actions > Deploy OVF Template.
3. Browse to the OVA file that was downloaded. Click Next.
4. Click Next.
5. Modify the default name if desired and select the Inventory Location. Click Next.



6. Review the details to verify the OVF template details and click Next.



7. Select a cluster/server on which you want to host the UCS Central virtual machine. Click Next.



8. Select a host to run the deployed template
9. Select the datastore in which the virtual machine files will be stored. Click Next.
10. Click Next.
11. Select the checkbox to power on the VM after deployment.
12. Click Finish.

Note Do not proceed until the virtual machine has finished booting.

13. Open a console window to the UCS Central virtual machine.

```
Shutting down cmon:                                        [  OK  ]
Validating the installation medium's disk (/dev/mapper/VolGroup01-LogVol00) spee
d
Average disk read speed measured: 373
Disk speed validation - Succeeded
Setup new configuration or restore full-state configuration from backup[setup/re
store]  - setup

Enter the UCS Central VM eth0 IPv4 Address  : 10.29.128.165
Enter the UCS Central VM eth0 IPv4 Netmask  : 255.255.255.0
Enter the VM IPv4 Default Gateway  : 10.29.128.1


Is this VM part of a cluster(select 'no' for standalone) (yes/no)  ? no

Enter the UCS Central VM Hostname  : ucentral
Enter the DNS Server IPv4 Address  : 10.29.128.117
Enter the Default Domain Name  : ciscorobo.com

Use a Shared Storage Device for Database (yes/no)  ? no
Enforce Strong Password (yes/no)  ? yes
Enter the admin Password  :
Confirm admin Password :
Values do not match, please try again
Enter the admin Password  : _
```

14. Enter the IPv4 address, Network and gateway information in the console window

```
Setup new configuration or restore full-state configuration from
backup[setup/restore] - setup
Enter the UCS Central VM eth0 IPv4 Address : <<var_ucs_central_ip>>
Enter the UCS Central VM eth0 IPv4 Netmask : <<var_ucs_central_netmask>>
Enter the VM IPv4 Default Gateway : <<var_ucs_central_gateway>>
Is this VM part of a cluster (select 'no' for standalone) (yes/no)? no
Enter the UCS Central VM Hostname : <<var_ucs_central_hostname>>
Enter the DNS Server IPv4 Address : <<var_nameserver_ip>>
Enter the Default Domain Name : <<var_dns_domain_name>>
Use a Shared Storage Device for Database (yes/no)? no
Enforce Strong Password (yes/no)? yes
Enter the admin Password : <<var_password>>
Confirm admin Password : <<var_password>>
Enter the Shared Secret :  enter the shared secret (or password) that you
want
to use to register one or more Cisco UCS domains with Cisco UCS Central
Confirm Shared Secret : re-enter the Shared Secret
Do you want Statistics collection [yes / no]? yes
Enter the Statistics DB Type [D=Default (internal Pstgres db) / P=Postgres /
O=Oracle] : D
Proceed with this configuration? Please confirm [yes/no] - yes
```

Note If you wish to modify/answer the prompts again, enter no in the above prompt.

15. After confirming that you want to proceed with the configuration, the network interface reinitializes with your settings and Cisco UCS Central can be accessed using the IP address.

Access the Cisco UCS Central GUI

1. Using a web browser, navigate to the <<var_ucs_central_hostname>> using https://<<var_ucs_central_ip>>.
2. Log in with the user name as admin and the admin password.
3. Click the Operations Management tab, expand Domain Groups > Domain Group root.
4. Select Operational Policies.
5. Select Time Zone in the right pane, and select the desired time zone.
6. Click Add NTP Server.
7. Provide the NTP Server IP Address <<var_global_ntp_server_ip>> and click OK.
8. Click Save.

Add Cisco UCS Managers to Cisco UCS Central

Cisco UCS Managers are be added into the Cisco UCS Central by logging into the Cisco UCS Manager and registering the Cisco UCS Manager with Cisco UCS Central.

To add UCS Manager to UCS Central, complete the following steps:

1. Log in to the Cisco UCS Manager.
2. In the navigation pane, click the Adminnode.
3. In the Admin tab expand the All folder, select Communication Management > UCS Central.
4. In the UCS Central tab, in the Actions section, click Register with UCS Central.

5. Enter the host name or IP address of the UCS Central.
6. Enter the Shared Secret. Click OK.
7. Click Accept to terminate any open GUI sessions to the UCS Manager.
8. Select the checkbox to view the Navigator for the UCS Central. Click OK.
9. Verify the Registration Status.

Bill of Materials for Cisco UCS Used in This Validation

Table 25 and Table 26 provides the details of components used in the in the Data Center CVD. This section provides the bill of material (BoM) information about the Cisco hardware used in the FlexPod architecture. The hardware and software components required to deploy the FlexPod solution explained in this design guide.

Table 25 Cisco Component s Description - Bill of Materials

Description	Part Number
UCS Chassis 5108	UCS-5108-AC2
6324UP Fabric Interconencts	UCS-FI-M-6324
UCS B200 M3 Blades	UCSB-B200-M3
10 Gbps SFP+ multifiber mode	SFP-10G-SR
8 Gbps SFP+ fibre mode	DP-SFP-FC8G-SW
1000Base-T copper module	CIS-GLC-T-NP-OE
Cisco 40-Gigabit QSFP+ Transceiver Modules **(Breakout cable for scalability port to connect rack servers)**	QSFP-4SFP10G-CU5M

Table 26 Cisco UCS-Mini Components - Bill of Materials

Product Bundle	Sub Components	
UCS-MINI-Z001	UCS Unified Computing System	
UCSB-5108-AC2	UCSB-5108-PKG-HW	UCS 5108 Packing for chassis with half width blades
	N20-FW013	UCS Blade Server Chassis FW Package 3.0
	N01-UAC1	Single phase AC power module for UCS 5108
	N20-CAK	Accessory kit for UCS 5108 Blade Server Chassis
	UCSB-B200-M3	UCS B200 M3 Blade Server w/o CPU, memory, HDD, mLOM/mezz
	UCS-CPU-E52680B	2.80 GHz E5-2680 v2/115W 10C/25MB Cache/DDR3 1866MHz
	UCS-MR-1X162RZ-A	16GB DDR3-1866-MHz RDIMM/PC3-14900/dual rank/x4/1.5v

	A03-D600GA2	600GB 6Gb SAS 10K RPM SFF HDD/hot plug/drive sled mounted
	UCSB-MLOM-40G-01	Cisco UCS VIC 1240 modular LOM for blade servers
	UCSB-HS-01-EP	CPU Heat Sink for UCS B200 M3 and B420 M3
	UCSB-M3-V2-LBL	Cisco M3 – v2 CPU asset tab ID label
	UCSB-PSU-2500ACDV	2500W Platinum AC Hot Plug Power Supply- DV
	UCS-US515P-C19	NEMA 5-15 to IEC-C19 13ft US
	UCS-FI-M-6324	UCS 6324 In-Chassis FI with 4 UP, 1x40G Exp Port, 16 10Gb do
	N10-MGT013	UCS Manager 3.0 for 6324

Table 27 Cisco Nexus 9372—Bill of Material

Product Bundle	Sub Components	Description
N9K-C9372PX-B18Q		Nexus 9372PX bundle PID. 2 Nexus 9372PX Switches

Note This is a bill of materials information. Please work your trusted advisor for completeness of your order.

For more information about the part numbers and options available for customization, see Cisco UCS 6324 Fabric Interconnect datasheet at:

http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-6300-series-fabric-interconnects/datasheet-c78-732207.html

Cisco Nexus 9372 Example Configurations

Cisco Nexus 9372 A

```
!Command: show running-config
!Time: Thu Jan  8 19:05:25 2015

version 6.1(2)I2(2a)
hostname n9k-a
policy-map type network-qos jumbo
  class type network-qos class-default
    mtu 9216
vdc n9k-a id 1
  allocate interface Ethernet1/1-48
  allocate interface Ethernet2/1-12
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8
```

```
feature telnet
cfs eth distribute
feature interface-vlan
feature lacp
feature vpc
feature lldp

username admin password 5 $1$L.7M7uW.$1OEBj/djom6dbicBmDWaR.
role network-admin
no password strength-check
ip domain-lookup
system qos
  service-policy type network-qos jumbo
copp profile strict
snmp-server user admin network-admin auth md5 0x02b6373181dc6994a3a7808ad778bb7c
 priv 0x02b6373181dc6994a3a7808ad778bb7c localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO

vlan 1-2,128, 3173-3174
vlan 2
  name Native-VLAN
vlan 128
  name IB-MGMT-VLAN
vlan 3173
  name vMotion-VLAN
vlan 3174
  name VM-Traffic-VLAN

spanning-tree port type edge bpduguard default
spanning-tree port type network default
vrf context management
  ip route 0.0.0.0/0 10.29.128.1
port-channel load-balance src-dst l4port
vpc domain 45
  role priority 10
  peer-keepalive destination 10.29.128.201 source 10.29.128.200
  auto-recovery
port-profile type port-channel vPC-Peer-Link
  switchport
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128, 3173-3174
  spanning-tree port type network
  state enabled
port-profile type port-channel UCS-Ethernet
  switchport
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128, 3173-3174
  spanning-tree port type edge trunk
  state enabled
```

```
interface port-channel10
  inherit port-profile vPC-Peer-Link
  description vPC peer-link
  vpc peer-link

interface port-channel13
  inherit port-profile UCS-Ethernet
  description ucs-A
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128, 3173-3174
  vpc 13
  switchport

interface port-channel14
  inherit port-profile UCS-Ethernet
  description ucs-B
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128, 3173-3174
  vpc 14
  switchport

interface port-channel15
  description clus-01
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 901-902,3170
  spanning-tree port type edge trunk
  vpc 15

interface port-channel16
  description clus-02
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 901-902,3170
  spanning-tree port type edge trunk
  vpc 16

interface Ethernet1/1


interface Ethernet1/2

interface Ethernet1/3
  description clus-01:0c
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128, 3173-3174
  channel-group 13 mode active

interface Ethernet1/4
  description ucs-b:1/1
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128, 3173-3174
  channel-group 14 mode active
```

```
interface Ethernet1/5

interface Ethernet1/6


interface Ethernet1/7


interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13
  description n9k-a:1/13
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128, 3173-3174
  channel-group 10 mode active

interface Ethernet1/14
  description n9k-a:1/14
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128, 3173-3174
  channel-group 10 mode active

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19
  description mgmtuplink:0/23
  switchport access vlan 128
  speed 1000

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26
```

```
interface Ethernet1/27
interface Ethernet1/28
interface Ethernet1/29
interface Ethernet1/30
interface Ethernet1/31
interface Ethernet1/32
interface Ethernet1/33
interface Ethernet1/34
interface Ethernet1/35
interface Ethernet1/36
interface Ethernet1/37
interface Ethernet1/38
interface Ethernet1/39
interface Ethernet1/40
interface Ethernet1/41
interface Ethernet1/42
interface Ethernet1/43
interface Ethernet1/44
interface Ethernet1/45
interface Ethernet1/46
interface Ethernet1/47
interface Ethernet1/48
interface Ethernet2/1
interface Ethernet2/2
interface Ethernet2/3
interface Ethernet2/4
interface Ethernet2/5
interface Ethernet2/6
interface Ethernet2/7
```

```
interface Ethernet2/8

interface Ethernet2/9

interface Ethernet2/10

interface Ethernet2/11

interface Ethernet2/12

interface mgmt0
  vrf member management
  ip address 10.29.128.203/24
line console
line vty
boot nxos bootflash:/n9000-dk9.6.1.2.I2.2a.bin
```

Cisco Nexus 9372 B

```
!Command: show running-config
!Time: Thu Jan  8 19:07:37 2015

version 6.1(2)I2(2a)
hostname n9k-b
policy-map type network-qos jumbo
  class type network-qos class-default
    mtu 9216
vdc n9k-b id 1
  allocate interface Ethernet1/1-48
  allocate interface Ethernet2/1-12
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

feature telnet
cfs eth distribute
feature interface-vlan
feature lacp
feature vpc
feature lldp

username admin password 5 $1$vNh4Rwhk$ceMm/4KFH7VotGGnSxSqm1  role network-admin
no password strength-check
ip domain-lookup
system qos
  service-policy type network-qos jumbo
copp profile strict
snmp-server user admin network-admin auth md5 0xe1df2ff11f65fbac79908ff0fd61dae1
 priv 0xe1df2ff11f65fbac79908ff0fd61dae1 localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
```

```
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO

vlan 1-2,128,901-902, 3173-3174
vlan 2
  name Native-VLAN
vlan 128
  name IB-MGMT-VLAN
vlan 3173
  name vMotion-VLAN
vlan 3174
  name VM-Traffic-VLAN

spanning-tree port type edge bpduguard default
spanning-tree port type network default
vrf context management
  ip route 0.0.0.0/0 10.29.128.1
port-channel load-balance src-dst l4port
vpc domain 45
  role priority 20
  peer-keepalive destination 10.29.128.200 source 10.29.128.201
  auto-recovery
port-profile type port-channel vPC-Peer-Link
  switchport
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128, 3173-3174
  spanning-tree port type network
  state enabled

port-profile type port-channel UCS-Ethernet
  switchport
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128, 3173-3174
  spanning-tree port type edge trunk
  state enabled


interface Vlan1



interface port-channel10
  inherit port-profile vPC-Peer-Link
  description vPC peer-link
  vpc peer-link

interface port-channel13
  inherit port-profile UCS-Ethernet
  description ucs-A
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128, 3173-3174
  vpc 13

interface port-channel14
```

```
  inherit port-profile UCS-Ethernet
  description ucs-B
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128, 3173-3174
  vpc 14

interface Ethernet1/1


interface Ethernet1/2

interface Ethernet1/3
  description ucs-a:1/2
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128, 3173-3174
  channel-group 13 mode active

interface Ethernet1/4
  description ucs-b:1/2
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128, 3173-3174
  channel-group 14 mode active

interface Ethernet1/5


interface Ethernet1/6


interface Ethernet1/7
interface Ethernet1/8
interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13
  description n9k-b:1/13
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128, 3173-3174
  channel-group 10 mode active

interface Ethernet1/14
  description n9k-b:1/13
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128, 3173-3174
  channel-group 10 mode active

interface Ethernet1/15
```

```
interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19
  description mgmtuplink:0/23
  switchport access vlan 128
  speed 1000

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface Ethernet1/33

interface Ethernet1/34

interface Ethernet1/35

interface Ethernet1/36

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40

interface Ethernet1/41

interface Ethernet1/42

interface Ethernet1/43
```

```
interface Ethernet1/44

interface Ethernet1/45

interface Ethernet1/46

interface Ethernet1/47

interface Ethernet1/48

interface Ethernet2/1

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet2/5

interface Ethernet2/6

interface Ethernet2/7

interface Ethernet2/8

interface Ethernet2/9

interface Ethernet2/10
interface Ethernet2/11

interface Ethernet2/12
interface mgmt0
  vrf member managemet
  ip  address 10.29.128.204/24
  line console
line vty
boot nxos bootflash:/n9000-dk9.6.1.2.I2.2a.bin
```