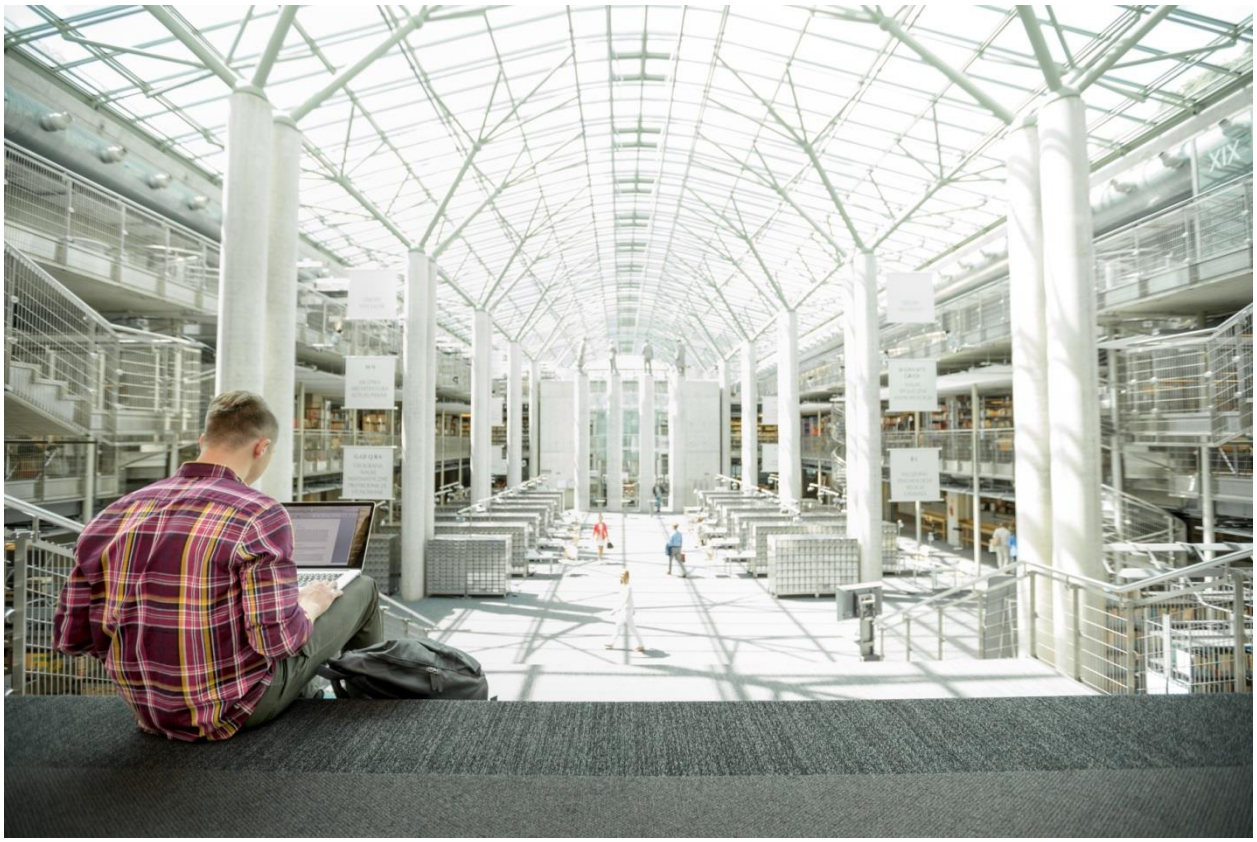


FlexPod Express with Cisco UCS Mini and VMware vSphere 5.5 with IP-Based Storage

Deployment Guide for FlexPod Express with Cisco UCS-Mini and VMware vSphere 5.5 Update 2 with IP-Based Storage

Last Updated: August 28, 2015

About Cisco Validated Designs

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

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

Table of Contents

Executive Summary

The FlexPod Express with Cisco UCS Mini is a pre-validated and modular architecture built with proven best of-breed technologies. Because FlexPod solutions are rigorously tested, the solution drastically reduces server virtualization planning and configuration overhead while contributing to IT transformation through faster deployments, greater choice of components and flexibility at reduced risk.

This Cisco Validated Design (CVD) leverages the FlexPod Express Infrastructure with VMware vSphere. This solution uses Cisco components such as the Cisco UCS Mini compute chassis, Cisco Nexus 3000 series networking, Cisco UCS Central (Optional) and the NetApp FAS2552 storage system. The platform has sufficient scalability in compute and storage areas, if necessary. This Cisco Validated Design document defines the architectural design and deployment procedure of the previously defined FlexPod Express Infrastructure with VMware ESXi with a focus on features and options that underscore functionality, scalability and standardized management as well as simplicity, efficiency, and flexibility.

Solution Overview

The current industry trend in infrastructure design is towards shared infrastructures. By using virtualization with pre-validated IT platforms, 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 Express, 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 use IP-based storage. 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 Express 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 Express solution.

Purpose of This Document

This FlexPod Express solution combines Cisco UCS Mini, Cisco Nexus 3000 series networking and VMware vSphere® 5.5 update 2 with NetApp FAS255x series storage arrays to support Enterprises in Data Center environments. This document describes how to deploy the solution and use Cisco UCS Central for centralized management of the infrastructure.

Solution Summary

The infrastructure 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 and vertical scalability and high levels of utilization.

Use cases include:

- Remote Office/ Branch Office
- Small Medium Business

The FlexPod® Express solution combines NetApp® storage systems, Cisco® Unified Computing System servers, and Cisco Nexus fabric into a single, flexible architecture. FlexPod Express 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, MS Exchange, MS SharePoint, SAP, Red Hat or VDI (VMware View/Citrix XenDesktop).

FlexPod Express delivers:

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

The FlexPod Express with Cisco UCS Mini allows IT departments to address 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

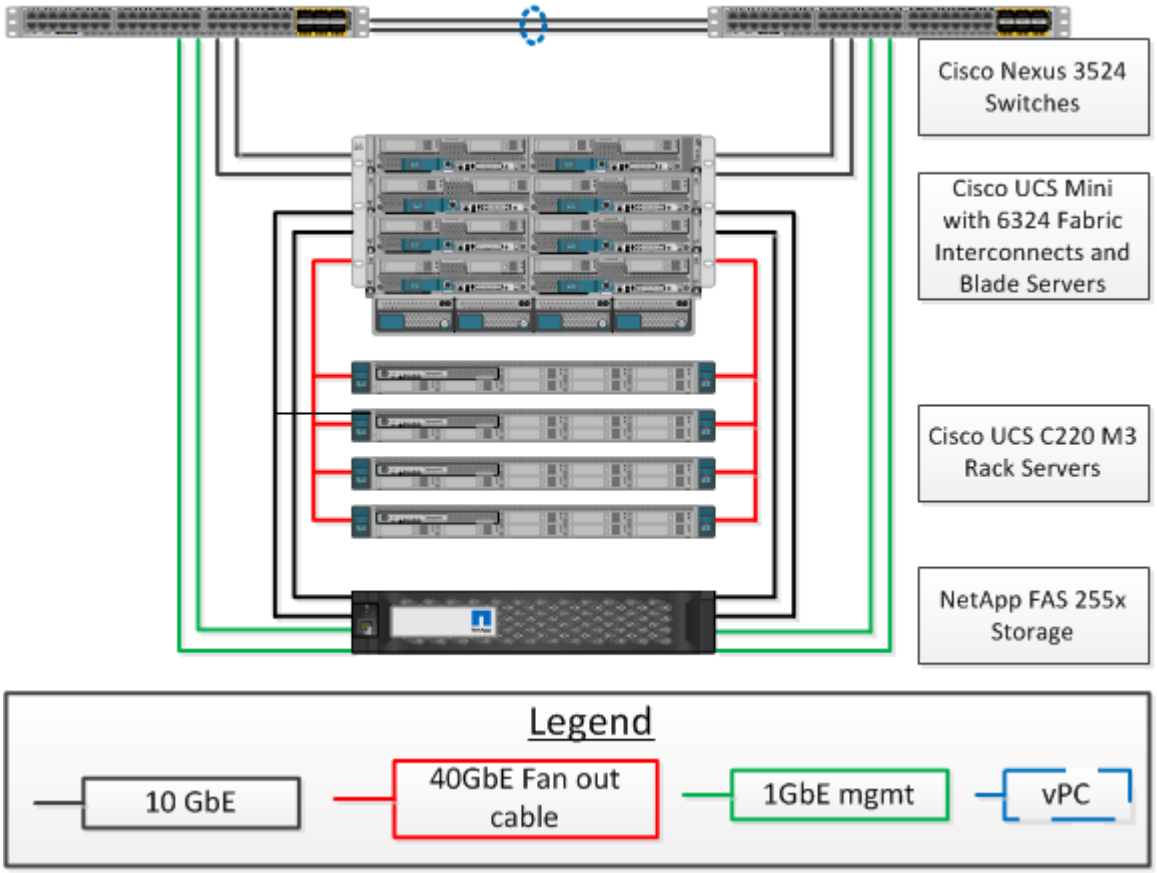
The FlexPod architecture is highly modular or “podlike.” Although each customer’s FlexPod unit varies in its exact configuration, after a FlexPod unit is built, it can easily be scaled as requirements and demands change. The unit can be scaled both up (adding resources to a FlexPod unit) and out (adding 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 infrastructure 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 Ethernet based storage solution.

Figure 1 illustrates the VMware vSphere built on FlexPod components and the network connections for a configuration with IP-based storage. This design uses Cisco Nexus® 3524, 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 iSCSI-booted hosts with block-level and file-level access to shared storage datastores.

Figure 1 VMware vSphere Built on FlexPod Express Components



The reference configuration includes:

- Two Cisco Nexus 3000 series switches – Note that standard Ethernet switches can be used in this solution as long as they provide VLAN-level paths between the two Cisco UCS Fabric Interconnects.
- Two Cisco UCS 6324UP Fabric Interconnects built in to the 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 Express components and network connections for a configuration with directly attached IP-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.

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 consists of the following components.

- **Cisco UCS B200 M4 Blade Server** – Delivering performance, versatility, and density without compromise, the Cisco UCS B200 M4 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 M4 Blade Servers.
- **Cisco UCS 6324 Fabric Interconnect** – The 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** – 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 Server** – This one-rack-unit (1RU) server offers superior performance and density over a wide range of business workloads.
- **Cisco UCS C240 M3 Rack 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 UCS domains. (see appendix section for implementation details)

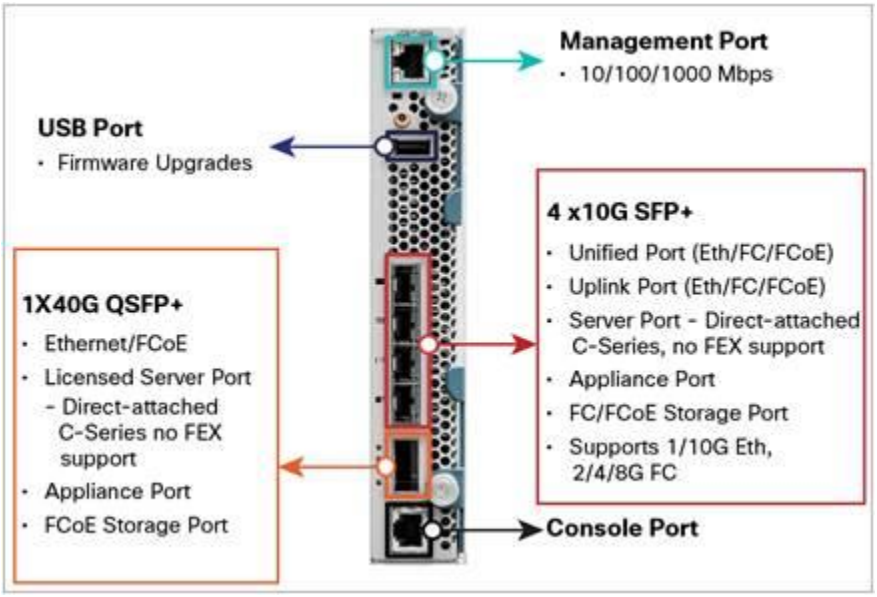
The key to delivering the power of Cisco Unified Computing System in a smaller form factor known as Cisco UCS Mini is the Cisco UCS 6324 Fabric Interconnect. The Cisco UCS 6324 Fabric Interconnect supports the integrated Cisco UCS Management software as well as, LAN and storage connectivity for the Cisco 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 an optimized server design in which network interface cards (NICs), host bus adapters (HBAs), cables, and switches can be consolidated.

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

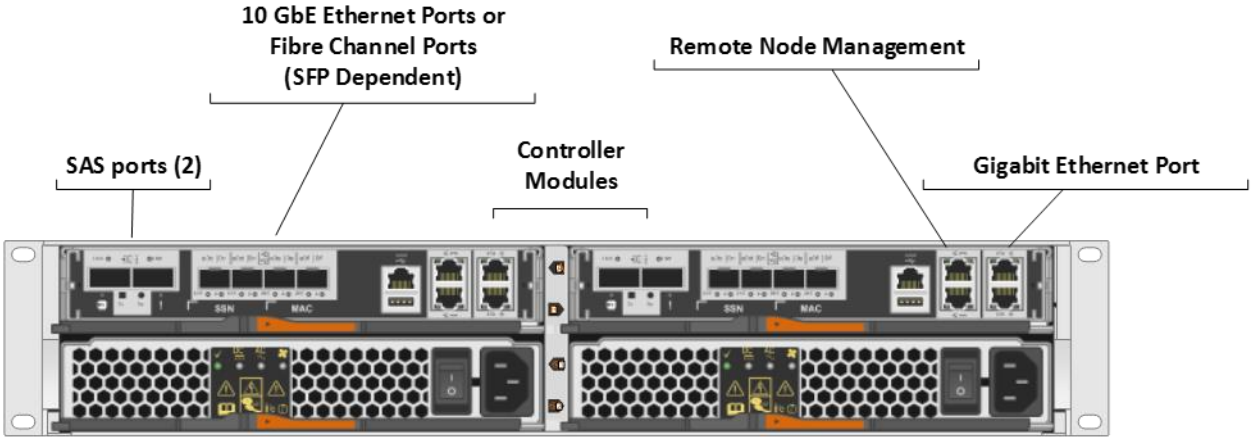
Figure 2 Cisco UCS FI-6324 Fabric Interconnect Details



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 using 10 GbE loopback cables. SAN A and SAN B best practices are honored and ALUA-enabled host-based multi-pathing allows for redundant and optimal 10-Gbps paths into the NetApp controllers. This model in this configuration supports iSCSI, NFS and CIFS access to storage. Scalability is achieved by adding storage capacity (disk/shelves) to an existing HA pair.

Figure 3 FAS2552 System Details

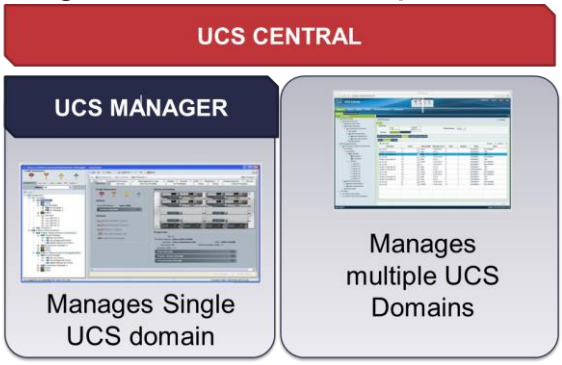


Management Tools to Facilitate Configuration and Operations

Cisco Data Center 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 work easily 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 Express solution with IP-base storage and is intended to be installed in a Remote Office or Branch Office. The FlexPod Data Center solution with IP-base storage is covered in another document and is intended to be installed in a DataCenter. 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(2c)	Embedded management
	Cisco UCS C 220 M4	3.0(2c)	Software bundle release
	Cisco UCS B 200 M4	3.0(2c)	Software bundle release
	Cisco eNIC	2.1.2.69	Ethernet driver for Cisco VIC
	Cisco fNIC	1.6.0.16	FCoE driver for Cisco VIC
	Cisco VIC 1240	4.0(3a)	Cisco Virtual Interface card firmware
	Cisco VIC 1340	4.0(3a)	Cisco Virtual Interface card firmware
	Cisco VIC 1225	4.0(3a)	Cisco Virtual Interface card firmware
Network	Cisco Nexus switch Nexus 3524	6.0(2)A6(2)	Operating system version
Storage	NetApp FAS2552-HA	Clustered Data ONTAP 8.3	Operating system version
Software	Cisco UCS hosts	VMware vSphere ESXi™ 5.5 U2	Operating system version
	VMware vCenter™	5.5U2	VM (1 each): VMware vCenter from OVA
	NetApp OnCommand Unified Manager®	6.2	VM (1 each): OnCommand from OVA
	NetApp Virtual Storage Console (VSC)	6.0	VM (1 each): Microsoft Windows Server NetApp Virtual Storage Console—Plug-in within VMware vCenter
	NetApp vStorage APIs for Storage Awareness (VASA) Provider	6.0	VM (1 each):VASA Provider from OVA
	NetApp NFS Plugin for VMware vStorage APIs for Array Integration (VAAI)	1.0.21	VMware VIB installed on each ESXi host and stored on VSC server
	Cisco Nexus 1000v	5.2(1)SV3(1.3)	VM (2) Virtual Supervisor Modules (VSMs) from OVA
	Cisco UCS Central	1.3(1a)	Manager of multiple UCS domains

Configuration Guidelines

This document provides details for configuring a fully redundant, highly available FlexPod Express configuration with NetApp 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 identifies the pair of Cisco Nexus switches that are configured. The Cisco UCS Fabric Interconnects are similarly configured. Additionally, this document details the steps for provisioning multiple Cisco UCS hosts, and these 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 4 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.

Note: 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
NFS	VLAN for NFS	3170
iSCSI-A	VLAN for iSCSI-A	3171
iSCSI-B	VLAN for iSCSI-B	3172
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 VMware Virtual Machines (VMs) 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 4 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_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	

Variable	Description	Customer Implementation Value
<<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_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	

Variable	Description	Customer Implementation Value
<<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	

Variable	Description	Customer Implementation Value
<<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_svm_mgmt_ip>>	Management IP address for SVM	
<<var_svm_mgmt_mask>>	Subnet mask for SVM	
<<var_rule_index>>	Rule index number	
<<var_ftp_server>>	IP address for FTP server	
<<var_node01_iscsi_lif01a_ip>>	IP of node 01 iSCSI LIF 01a	
<<var_node01_iscsi_lif01a_mask>>	Subnet Mask of node 01 iSCSI LIF 01a	
<<var_node01_iscsi_lif01b_ip>>	IP of node 01 iSCSI LIF 01b	
<<var_node01_iscsi_lif01b_mask>>	Subnet Mask of node 01 iSCSI LIF 01b	
<<var_node02_iscsi_lif01a_ip>>	IP of node 02 iSCSI LIF 01a	
<<var_node02_iscsi_lif01a_mask>>	Subnet Mask of node 02 iSCSI LIF 01a	
<<var_node02_iscsi_lif01b_ip>>	IP of node 02 iSCSI LIF 01b	
<<var_node02_iscsi_lif01b_mask>>	Subnet Mask of node 02 iSCSI LIF 01b	
<<var_vmhost_infra01_ip>>	VMware ESXi host 01 in-band management IP	

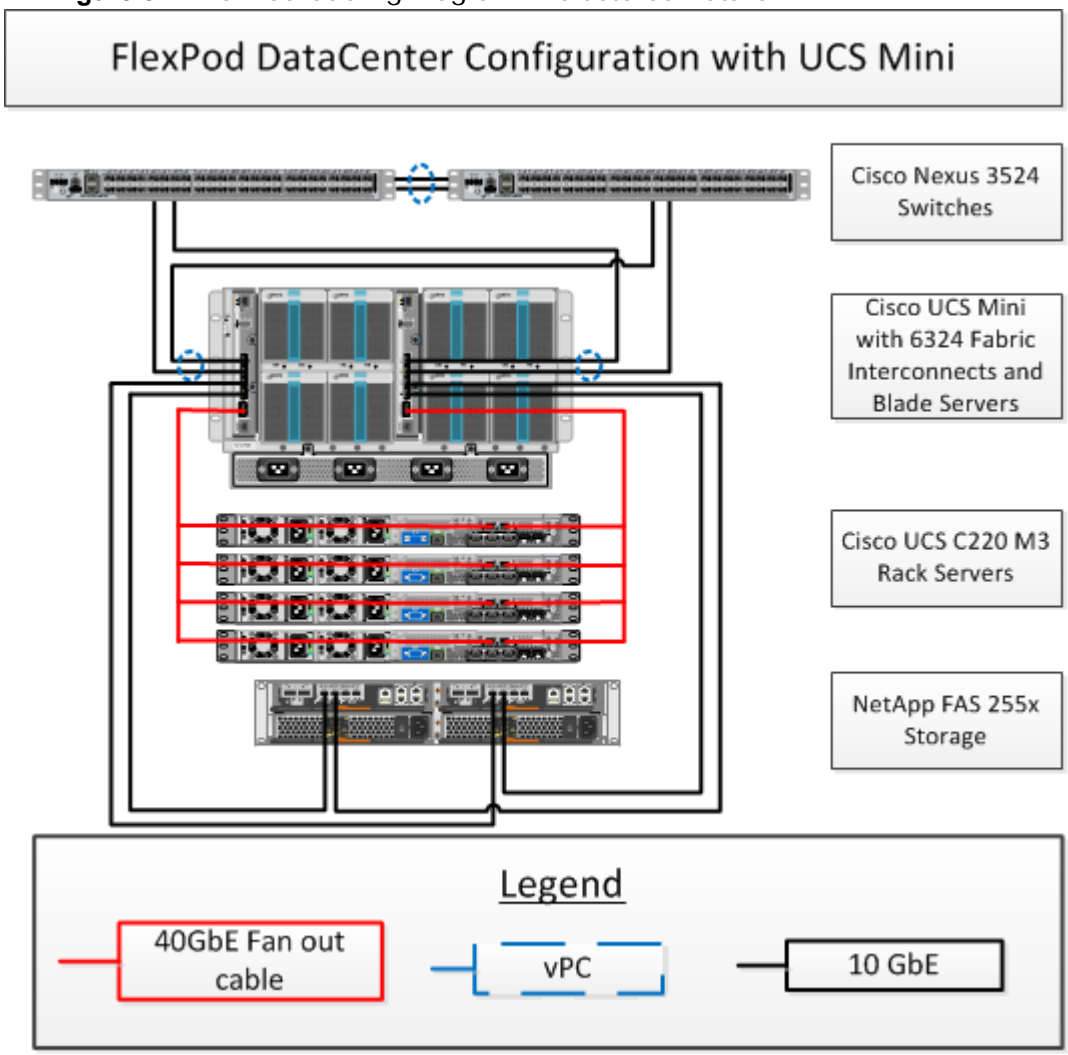
Variable	Description	Customer Implementation Value
<<var_vmhost_infra02_ip>>	VMware ESXi host 02 in-band management IP	
<<var_vmotion_vlan_id_ip_host-01>>	vMotion VLAN IP address for ESXi host 01	
<<var_vmotion_vlan_id_mask_host-01>>	vMotion VLAN netmask for ESXi host 01	
<<var_vmotion_vlan_id_ip_host-02>>	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 5 through Table 14 corresponds to device connectivity in the architecture shown in Figure 5.

Table 5 Cisco Nexus 3524 A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
	Eth1/1	GbE	NetApp Storage Node A	e0M
	Eth1/2	GbE	NetApp Storage Node B	e0a
	Eth1/3	10GbE	Cisco UCS Fabric Interconnect A	Eth1/3

Local Device	Local Port	Connection	Remote Device	Remote Port
	Eth1/4	10GbE	Cisco UCS Fabric Interconnect B	Eth1/3
	Eth1/13	10GbE	Cisco Nexus 3524 B	Eth1/13
	Eth1/14	10GbE	Cisco Nexus 3524 B	Eth1/14
	Eth1/21	GbE	Cisco UCS Fabric Interconnect A	mgmt0
	mgmt0	GbE	Cisco Nexus 3524 B	mgmt0

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

Table 6 Cisco Nexus 3524 B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
	Eth1/1	GbE	NetApp Storage Node B	e0M
	Eth1/2	GbE	NetApp Storage Node A	e0a
	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 3524 A	Eth1/13
	Eth1/14	10GbE	Cisco Nexus 3524 A	Eth1/14
	Eth1/21	GbE	Cisco UCS Fabric Interconnect B	mgmt0
	mgmt0	GbE	Cisco Nexus 3524 A	mgmt0

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

Table 7 NetApp Controller A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
NetApp controller A	e0M	GbE	Cisco Nexus 3524 A	Eth1/1
	e0P	GbE	NetApp Controller B	e0P
	e0a	GbE	Cisco Nexus 3524 B	Eth1/2
	e0c	10GbE	Cisco UCS Fabric Interconnect A	Eth1/1
	e0d	10GbE	Cisco UCS Fabric Interconnect 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 referring is the port indicated by a wrench icon on the rear of the chassis.

Table 8 NetApp Controller B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
NetApp controller B	e0M	GbE	Cisco Nexus 3524 B	Eth1/1
	e0P	GbE	NetApp Controller A	e0P
	e0a	GbE	Cisco Nexus 3524 B	Eth1/2
	e0c	10GbE	Cisco UCS Fabric Interconnect A	Eth1/2
	e0d	10GbE	Cisco UCS Fabric Interconnect 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 referring is the port indicated by a wrench icon on the rear of the chassis.

Table 9 Cisco UCS Fabric Interconnect A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect A	Eth1/1	10GbE	NetApp Controller A	e0c
	Eth1/2	10GbE	NetApp Controller B	e0c
	Eth1/3	10GbE	Cisco Nexus 3524 A	Eth1/3
	Eth1/4	10GbE	Cisco Nexus 3524 B	Eth1/3
	mgmt0	GbE	Cisco Nexus 3524 A	Eth1/21

Table 10 Cisco UCS Fabric Interconnect B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect B	Eth1/1	10GbE	NetApp Controller A	e0d
	Eth1/2	10GbE	NetApp Controller B	e0d
	Eth1/3	10GbE	Cisco Nexus 3524 A	Eth1/4
	Eth1/4	10GbE	Cisco Nexus 3524 B	Eth1/4
	MGMT0	GbE	Cisco Nexus 3524 B	Eth1/21

Table 11 Cisco UCS C-Series 3 (C220 M3)

Local Device	Local Port	Connection	Remote Device	Remote Port	Cabling Code
Cisco UCS C-Series 1 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 12 Cisco UCS C-Series 3 (C220 M3)

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

Table 14 Cisco UCS C-Series 3 (C220 M3)

Local Device	Local Port	Connection	Remote Device	Remote Port	Cabling Code
Cisco UCS C-Series 4 UCS C220 M3	Port 1	10GbE	Fabric Interconnect A	Eth 1/5/4 (40Gb breakout cable)	
	Port 2	10GbE	Fabric Interconnect B	Eth 1/5/4 (40Gb breakout cable)	

Networking Switch Configuration

FlexPod Cisco Nexus Base

The following section details the Cisco Nexus 3524 switch configuration for use in a FlexPod Express environment. Note that a pair of standard Ethernet switches can be used here. It is desired both from a functionality and support perspective that Cisco Nexus switches be used.

Set Up Initial Configuration

The initial boot and connection to the console port of the switch, the Cisco NX-OS setup automatically starts. This initial configuration addresses basic settings, such as the switch name, the mgmt0 interface configuration, and Secure Shell (SSH) setup, and defines the control-plane policing policy.

The first major decision involves the configuration of the management network for the switches. For FlexPod Express, there are different options for configuring the mgmt0 interfaces. The first involves configuring and cabling the mgmt0 interfaces into an existing out-of-band network. In this instance, when a management network already exists, all you need are valid IP addresses and the netmask configuration for this network and a connection from the mgmt0 interfaces to this network.

The other option, for installations without a dedicated management network, involves cabling the mgmt0 interfaces of each Cisco Nexus 3524 switch together in a back-to-back configuration. Any valid IP address and netmask can be configured on each mgmt0 interface as long as they are in the same network. Because they are configured back to back with no switch or other device in between, no default gateway configuration is needed, and they should be able to communicate with each other. This link cannot be used for external management access such as SSH access, but it will be used for the virtual PortChannel (vPC) peer keepalive traffic. To enable SSH management access to the switch, you need to configure the in-band interface VLAN IP address on an SVI, as discussed later in this document. This document assumes this option is being used.

Cisco Nexus 3524 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]: n
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]: Enter
Configure default interface layer (L3/L2) [L2]: Enter
Configure default switchport interface state (shut/noshut) [noshut]: shut
Configure CoPP System Policy Profile ( default / l2 / l3) [default]: Enter
Would you like to edit the configuration? (yes/no) [n]: Enter
```

Note: If back-to-back mgmt0 vPC keepalive is being used, use a private IP address for <<var_nexus_A_mgmt0_ip>> and do not specify a gateway.

2. Review the configuration summary before enabling the configuration.

```
Use this configuration and save it? (yes/no) [y]: Enter
Would you like to save the running-config to startup-config? (yes/no) [n]: y
```

Cisco Nexus 3524 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]: n
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]: Enter
Configure default interface layer (L3/L2) [L2]: Enter
Configure default switchport interface state (shut/noshut) [noshut]: shut
Configure CoPP System Policy Profile ( default / l2 / l3) [default]: Enter
Would you like to edit the configuration? (yes/no) [n]: Enter
```

2. If back-to-back mgmt0 vPC keepalive is being used, use a private IP address for <<var_nexus_B_mgmt0_ip>> in the same subnet as <<var_nexus_A_mgmt0_ip>> and do not specify a gateway.

3. Review the configuration summary before enabling the configuration.

```
Use this configuration and save it? (yes/no) [y]: Enter
Would you like to save the running-config to startup-config? (yes/no) [n]: y
```

Enable Licenses

Cisco Nexus 3524 A and Cisco Nexus 3524 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 3524 A and Cisco Nexus 3524 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:

```
ntp server <<var_global_ntp_server_ip>> use-vrf default
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 3524 A and Cisco Nexus 3524 B

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

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

```
vlan <<var_ib-mgmt_vlan_id>>
name IB-MGMT-VLAN
exit
vlan <<var_oob-mgmt_vlan_id>>
name OOB-MGMT-VLAN
exit
vlan <<var_native_vlan_id>>
name Native-VLAN
exit
vlan <<var_nfs_vlan_id>>
name NFS-VLAN
exit
vlan <<var_vmotion_vlan_id>>
name vMotion-VLAN
exit
```

```
vlan <<var_vm-traffic_vlan_id>>
name VM-Traffic-VLAN
exit
vlan <<var_iscsi_a_vlan_id>>
name iSCSI-A-VLAN
exit
vlan <<var_iscsi_b_vlan_id>>
name iSCSI-B-VLAN
exit
```

Add Individual Port Descriptions for Troubleshooting

Cisco Nexus 3524 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>>:e0M
exit
interface Eth1/2
description <<var_node02>>:e0a
exit
interface Eth1/3
description <<var_ucs_clustername>>-A:1/3
exit
interface Eth1/4
description <<var_ucs_clustername>>-B:1/3
exit
interface Eth1/21
description <<var_ucs_clustername>>-A:mgmt0
exit
interface Eth1/13
description <<var_nexus_B_hostname>>:1/13
exit
interface Eth1/14
description <<var_nexus_B_hostname>>:1/14
exit
```

Cisco Nexus 3524 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 Eth1/1
description <<var_node02>>:e0M
exit
interface Eth1/2
description <<var_node01>>:e0a
exit
interface Eth1/3
description <<var_ucs_clustername>>-A:1/4
exit
interface Eth1/4
description <<var_ucs_clustername>>-B:1/4
exit
interface Eth1/21
description <<var_ucs_clustername>>-B:mgmt0
exit
interface Eth1/13
description <<var_nexus_A_hostname>>:1/13
exit
interface Eth1/14
```

```
description <<var_nexus_A_hostname>>:1/14
exit
```

Configure Device Management Ports

Cisco Nexus 3524 A

To configure device management ports on switch A, complete the following steps:

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

```
interface Eth1/1
speed 1000
switchport access vlan <<var_oob-mgmt_vlan_id>>
spanning-tree port type edge
no shutdown
exit
interface Eth1/2
speed 1000
switchport access vlan <<var_oob-mgmt_vlan_id>>
spanning-tree port type edge
no shutdown
exit
interface Eth1/21
speed 1000
switchport access vlan <<var_oob-mgmt_vlan_id>>
spanning-tree port type edge
no shutdown
exit
copy run start
```

Cisco Nexus 3524 B

To configure device management ports on switch B, complete the following steps:

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

```
interface Eth1/1
speed 1000
switchport access vlan <<var_oob-mgmt_vlan_id>>
spanning-tree port type edge
vpc orphan-port suspend
no shutdown
exit
interface Eth1/2
speed 1000
switchport access vlan <<var_oob-mgmt_vlan_id>>
spanning-tree port type edge
vpc orphan-port suspend
no shutdown
exit
interface Eth1/21
speed 1000
switchport access vlan <<var_oob-mgmt_vlan_id>>
spanning-tree port type edge
vpc orphan-port suspend
no shutdown
exit
copy run start
```

Create Port Channels

Cisco Nexus 3524 A and Cisco Nexus 3524 B

To create the necessary port channels between devices, complete the following step on both 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 Eth1/3
channel-group 13 mode active
no shutdown
exit
interface Po14
description <<var_ucs_clustername>>-B
exit
interface Eth1/4
channel-group 14 mode active
no shutdown
exit
copy run start
```

Configure Port Channels

Cisco Nexus 3524 A and Cisco Nexus 3524 B

To configure the appropriate port channels complete the following steps on both switches:

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

```
interface Po10
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_oob-mgmt_vlan_id>>, <<var_nfs_vlan_id>>,
<<var_vmotion_vlan_id>>, <<var_vm-traffic_vlan_id>>, <<var_iscsi_a_vlan_id>>, <<var_iscsi_b_vlan_id>>
spanning-tree port type network
exit
interface Po13
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_nfs_vlan_id>>, <<var_vmotion_vlan_id>>,
<<var_vm-traffic_vlan_id>>, <<var_iscsi_a_vlan_id>>, <<var_iscsi_b_vlan_id>>
spanning-tree port type edge trunk
exit
interface Po14
switchport mode trunk
switchport trunk native vlan 2
switchport trunk allowed vlan <<var_ib-mgmt_vlan_id>>, <<var_nfs_vlan_id>>, <<var_vmotion_vlan_id>>,
<<var_vm-traffic_vlan_id>>, <<var_iscsi_a_vlan_id>>, <<var_iscsi_b_vlan_id>>
spanning-tree port type edge trunk
exit
copy run start
```

Configure Virtual Port Channels

Cisco Nexus 3524 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>>
peer-switch
role priority 10
peer-keepalive destination <<var_nexus_B_mgmt0_ip>> source <<var_nexus_A_mgmt0_ip>>
peer-gateway
auto-recovery
exit
interface Po10
vpc peer-link
exit
interface Po13
vpc 13
exit
interface Po14
vpc 14
exit
copy run start
```

Cisco Nexus 3524 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>>
peer-switch
role priority 20
peer-keepalive destination <<var_nexus_A_mgmt0_ip>> source <<var_nexus_B_mgmt0_ip>>
peer-gateway
auto-recovery
exit
interface Po10
vpc peer-link
exit
interface Po13
vpc 13
exit
interface Po14
vpc 14
exit
copy run start
```

Performing In-Band Management SVI Configuration

In-band management using SSH in the FlexPod Express environment is handled by an SVI. To configure the in-band management on each switch, you must configure an IP address on the interface VLAN and set up a default gateway. Note that this setup can be in either the in-band or out-of-band management VLAN.

1. From configuration mode (`config t`), type the following commands to configure the Layer 3 SVI for management purposes.

Switches A and B

```
int Vlan<<ib_mgmt_vlan_id>>
ip address <<inband_mgmt_ip_address>>/<<inband_mgmt_netmask>>
no shutdown
exit

ip route 0.0.0.0/0 <<inband_mgmt_gateway>>

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 3524 switches included in the FlexPod environment into the infrastructure. Make sure to uplink both the in-band and out-of-band management VLANs to ensure access to the Cisco UCS Fabric Interconnects and to storage. The previously described procedures can be used to create an uplink vPC to the existing environment. Make sure to run `copy run start` to save the configuration on each switch after the configuration is completed.

Storage Configuration

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 NetApp Hardware Universe. In the NetApp Hardware Universe, refer to the following sections: • Electrical Requirements • Supported Power Cords • Onboard Ports and Cables Refer to the site requirements guide replacement tutorial for finding NetApp FAS platform information using the NetApp Hardware Universe.

NetApp Hardware Universe

The NetApp Hardware Universe lists the supported hardware and software components for a 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. Log in to the Hardware Universe application to view the new NetApp system configuration solution.
3. After you log in to Hardware Universe, click the Controllers tab to view the compatibility between Data ONTAP software versions and NetApp storage appliances with the desired specifications. Alternatively, to compare components by storage appliance, click Compare Storage Systems.

Controllers

Follow the physical installation procedures for the controllers in the FAS255x documentation 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.

Configure Clustered Data ONTAP 8.3

Configure Clustered Data ONTAP Nodes

Before running the setup script, review the configuration worksheets in the Clustered Data ONTAP 8.2 Software Setup Guide to learn about the information required to configure clustered Data ONTAP. Table 16 lists the information that you will need to configure two clustered Data ONTAP nodes. You should customize the cluster detail values with the information that is applicable to your deployment.

Note: Before running the setup script, complete the configuration worksheet from the Clustered Data ONTAP Software Setup Guide on the NetApp Support site. This system is configured 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 8.3 URL	<<var_url_boot_software>>

Configure Node 01

To configure node 01, complete the following steps:

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

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

2. Set boot monitor defaults.

```
set-defaults
```

3. Allow the system to boot up.

```
autoboot
```

4. Press Ctrl-C when prompted.

Note: If Data ONTAP 8.3 is not the version of software being booted, continue with the following steps to install new software. If Data ONTAP 8.3 is the version being booted, select option 8 and `yes` to reboot the node. Then continue with step 14.

5. To install new software, select option 7.

```
7
```

6. Answer yes to perform a disruptive 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.

```
Press Ctrl-C when you see this message:Press Ctrl-C for Boot Menu.
```

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

```
4
```

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

```
y
```

16. 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 re-boots. You can continue with the node 02 configuration while the disks for node 01 are zeroing.

Configure Node 02

To configure node 02, complete the following steps:

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

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

2. Set boot monitor defaults.

```
set-defaults
```

3. Allow the system to boot up.

```
autoboot
```

4. Press Ctrl-C when prompted.

```
Ctrl-C
```

Note: If Data ONTAP 8.3 is not the version of software being booted, continue with the following steps to install new software. If Data ONTAP 8.3 is the version being booted, select option 8 and `yes` to reboot the node. Then continue with step 14.

5. To install new software, select option 7.

```
7
```

6. Answer yes to perform a disruptive 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.

```
<<var_url_boot_software>>
```

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

```
Enter
```

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

```
y
```

13. 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.

14. Press `Ctrl-C` when you see this message:

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

15. Select option 4 for `Clean Configuration and Initialize All Disks`.

```
4
```

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

```
y
```

17. 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.

Set Up Node

From a console port program attached to the storage controller A (node 01) console port, run the node setup script. This script appears when Data ONTAP 8.3 boots on the node for the first time.

1. Follow the prompts to set up node 01.

```
Welcome to node setup.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the setup wizard.
```

```
     Any changes you made before quitting will be saved.

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



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

Type yes to confirm and continue {yes}: yes

Enter the node management interface port [e0M]: Enter
Enter the node management interface IP address: <<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>>
A node management interface on port e0M with IP address <<var_node01_mgmt_ip>> has been created.


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

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

For System Setup, this node's management address is: <<var_node01_mgmt_ip>>.

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

2. Press Return and log in to the node with the admin user id and no password.

3. At the node command prompt, enter `yes` to reboot the node.

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

::> system node reboot

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

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

```
Welcome to node setup.

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

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



Enter the node management interface port [e0M]: Enter
Enter the node management interface IP address [<<var_node01_mgmt_ip>>]: Enter
Enter the node management interface netmask [<<var_node01_mgmt_mask>>]: Enter
Enter the node management interface default gateway [<<var_node01_mgmt_gateway>>]: Enter


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

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

For System Setup, this node's management address is: <<var_node01_mgmt_ip>>.
```

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

5. Log in to the node with the admin user and no password.

6. Repeat this procedure for storage cluster node 02.

Create Cluster on Node 01

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

Table 17 Cluster Create in 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>>

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

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

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. Enter `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. Enter `no` for cluster network using network switches.

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

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

```
Existing cluster interface configuration found:

Port    MTU     IP              Netmask
e0e     9000    169.254.70.234  255.255.0.0
e0f     9000    169.254.210.105 255.255.0.0

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

5. The steps to create a cluster are displayed.

```
Enter the cluster administrators (username "admin") password: <<var_password>>
Retype the password: <<var_password>>
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_iscsi_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. In addition, install all required storage protocol licenses (iSCSI and NFS). After you finish entering the license keys, press Enter.

```
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>>
```

6. 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.

7. Set up the node.

```
Where is the controller located []:<<var_node_location>>
Enter the node management interface port [e0M]: Enter
Enter the node management interface IP address [<<var_node01_mgmt_ip>>]: Enter
Enter the node management interface netmask [<<var_node01_mgmt_mask>>]: Enter
Enter the node management interface default gateway [<<var_node01_mgmt_gateway>>]: 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. In this document, it is assumed to be on the same subnet.

Join Node 02 to Cluster

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

Table 18 Cluster Join in 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>>`

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

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

```
admin
```

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

```
cluster setup

This node's storage failover partner is already a member of a cluster.
Storage failover partners must be members of the same cluster.
The cluster setup wizard will default to the cluster join dialog.



Welcome to the cluster setup wizard.

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

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.


Do you want to create a new cluster or join an existing cluster? {join}:
```

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

```
Existing cluster interface configuration found:

Port    MTU     IP              Netmask
e0e     9000    169.254.134.133 255.255.0.0
e0f     9000    169.254.11.51   255.255.0.0

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

5. 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. The cluster joining can take a few minutes.

6. Set up the node.

```
Enter the node management interface port [e0M]: Enter
Enter the node management interface IP address [<<var_node02_mgmt_ip>>]: Enter
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. In this document, it is assumed to be the same subnet.

Log In to Cluster

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

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

Zero All Spare Disks

To zero all spare disks in the cluster, 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 autoassignment 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 the personality of the onboard Unified Target Adapter 2 (UTA2), 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      cna      target     -        -          online
clus-01       0d      cna      target     -        -          online
clus-01       0e      cna      target     -        -          online
clus-01       0f      cna      target     -        -          online
clus-02       0c      cna      target     -        -          online
clus-02       0d      cna      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 all the ports in use is `cna` and the Current Type is set to `target`. If not, change the port personality by running the following command:

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

Note: The ports must be offline to run this 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:

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

1. Run the following command:

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

Set Up Management Broadcast Domain

To set up the Default broadcast domain for management network interfaces, complete the following step:

1. Run the following commands:

```
broadcast-domain remove-ports –broadcast-domain Default –ports <<var_node01>>:e0b, <<var_node02>>:e0b
```

Set Auto revert on Node Management LIFs

To set up the node management interfaces to automatically revert to their home ports, complete the following steps:

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

1. Run the following commands:

```
network interface modify -vserver <<var_clustername>> -lif <<var_node01>>_mgmt1 -auto-revert true
```

```
network interface modify -vserver <<var_clustername>> -lif <<var_node02>>_mgmt1 -auto-revert true
```

Set Up Service Processor Network Interface

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

1. Run the following commands:

```
system service-processor network modify -node <<var_node01>> -address-family IPv4 -enable true -dhcp none -
ip-address <<var_node01_sp_ip>> -netmask <<var_node01_sp_mask>> -gateway <<var_node01_sp_gateway>>

system service-processor network modify -node <<var_node02>> -address-family IPv4 -enable true -dhcp none -
ip-address <<var_node02_sp_ip>> -netmask <<var_node02_sp_mask>> -gateway <<var_node02_sp_gateway>>
```

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

Create Aggregates

An aggregate containing the root volume is created during the 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_node01 -nodes <<var_node01>> -diskcount <<var_num_disks>>
aggr create -aggregate aggr1_node02 -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. In this configuration with a FAS2552 or FAS2554, it may be desirable to create an aggregate with all but one remaining disk (spare) assigned to the controller.

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_node01 nosnap on
node run <<var_node02>> aggr options aggr1_node02 nosnap on
```

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

```
node run <<var_node01>> snap delete -A -a -f aggr1_node01
node run <<var_node02>> snap delete -A -a -f aggr1_node02
```

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>>
```

Verify Storage Failover

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

1. Verify the status of storage failover.

```
storage failover show
```

Note: Both the nodes <<var_node01>> and <<var_node02>> must be capable of performing a takeover. Continue with step 3, if the nodes are capable of performing a takeover.

2. Enable failover on one of the two nodes.

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

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

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

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

```
cluster ha show
```

4. Continue with step 6 if high availability is configured.

5. 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 UTA2 Ports

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

1. Run the following commands to configure node 01:

```
network port modify -node <<var_node01>> -port e0c,e0d,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
```

2. Run the following commands to configure node 02:

```
network port modify -node <<var_node02>> -port e0c,e0d,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
network port show -fields flowcontrol-admin
```

Disable Unused FcoE Ports

Unused switchless cluster interconnects and data FCoE ports should be disabled. To disable these ports, complete the following step:

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_node01>> -adapter 0e -state down
fcp adapter modify -node <<var_node01>> -adapter 0f -state down
fcp adapter modify -node <<var_node02>> -adapter 0c -state down
fcp adapter modify -node <<var_node02>> -adapter 0d -state down
fcp adapter modify -node <<var_node02>> -adapter 0e -state down
fcp adapter modify -node <<var_node02>> -adapter 0f -state down
fcp adapter show -fields state
```

Configure NTP

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) servers for the cluster.

```
cluster time-service ntp server create -server <<var_global_ntp_server_ip>>
```

Configure SNMP

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>>
```

Configure SNMPv1 Access

To configure SNMPv1 access, complete the following step:

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

```
snmp community add ro <<var_snmp_community>>
```

Note: Use the `delete all` command with caution. If community strings are used for other monitoring products, the `delete all` command will remove them.

Configure AutoSupport

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>>
```

Enable Cisco Discovery Protocol

To enable Cisco Discovery Protocol (CDP) on the NetApp storage controllers, complete the following step:

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

1. Run the following command to enable CDP on Data ONTAP:

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

Create Jumbo Frame MTU Broadcast Domains in Clustered Data ONTAP

To create a data broadcast domain with an MTU of 9000, complete the following step:

1. Run the following commands to create a broadcast domain on Data ONTAP:

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

Remove 10GbE Data Ports from Default Broadcast Domain

To remove the 10GbE data ports from the default broadcast domain, complete the following step:

1. Run the following command to remove the 10GbE ports from the default broadcast domain:

```
broadcast-domain remove-ports -broadcast-domain Default -ports <<var_node01>>:e0c,
<<var_node01>>:e0d,<<var_node02>>:e0c,<<var_node02>>:e0d
```

Create VLAN Interfaces

To create VLAN interfaces, complete the following steps:

1. Create NFS VLAN ports and add them to the data broadcast domain.

```
network port vlan create –node <<var_node01>> -vlan-name e0c-<<var_nfs_vlan_id>>
network port vlan create –node <<var_node01>> -vlan-name e0d-<<var_nfs_vlan_id>>
network port vlan create –node <<var_node02>> -vlan-name e0c-<<var_nfs_vlan_id>>
network port vlan create –node <<var_node02>> -vlan-name e0d-<<var_nfs_vlan_id>>

network port modify –node <<var_node01>> -port e0c –mtu 9000
network port modify –node <<var_node01>> -port e0d –mtu 9000
network port modify –node <<var_node02>> -port e0c –mtu 9000
network port modify –node <<var_node02>> -port e0d –mtu 9000

broadcast-domain add-ports -broadcast-domain Infra_NFS -ports <<var_node01>>:e0c-<<var_nfs_vlan_id>>,
<<var_node01>>:e0d-<<var_nfs_vlan_id>>, <<var_node02>>:e0c-<<var_nfs_vlan_id>>, <<var_node02>>:e0d-
<<var_nfs_vlan_id>>
```

2. Create iSCSI VLAN ports and add them to the data broadcast domain.

```
network port vlan create –node <<var_node01>> -vlan-name e0c-<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_node01>> -vlan-name e0d-<<var_iscsi_vlan_B_id>>
network port vlan create –node <<var_node02>> -vlan-name e0c-<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_node02>> -vlan-name e0d-<<var_iscsi_vlan_B_id>>

broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports <<var_node01>>:e0c-
<<var_iscsi_vlan_A_id>>,<<var_node02>>:e0c-<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports <<var_node01>>:e0d-
<<var_iscsi_vlan_B_id>>,<<var_node02>>:e0d-<<var_iscsi_vlan_B_id>>
```

Create Storage Virtual Machine

To create an infrastructure storage virtual machine (SVM, formerly known as Vserver), complete the following steps:

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

1. Run the `vserver create` command.

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

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

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

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

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

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

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

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

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

Create Load-Sharing Mirror of SVM Root Volume

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

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

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

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

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

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

3. Create the mirroring relationships.

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

4. Initialize the mirroring relationship.

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

Create iSCSI Service

To create the iSCSI service, complete the following step:

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

1. Create the iSCSI service on each SVM. This command also starts the iSCSI service and sets the iSCSI IQN for the SVM.

```
iscsi create -vserver Infra-SVM
iscsi show
```

Configure HTTPS Access

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

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

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 SVM shown, the certificate common name should match the DNS FQDN of the SVM. The two 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-SVM -common-name Infra-SVM -ca Infra-SVM -type server -
serial 552429A6
```

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

```
security certificate create [TAB] …
Example: security certificate create -common-name infra-svm.ciscorobo.com -type  server -size 2048 -country
US -state "California" -locality "San Jose" -organization "Cisco" -unit "UCS" -email-addr "abc@cisco.com" -
expire-days 365 -protocol SSL -hash-function SHA256 -vserver Infra-SVM
```

5. To obtain the values for the parameters that would be required in step 6, run the `security certificate show` command.

6. Enable each certificate that was just created by using the `-server-enabled true` and `-client-enabled false` parameters. Use TAB completion to aid in the completion of these commands.

```
security ssl modify [TAB] …
Example: security ssl modify -vserver clus -server-enabled true -client-enabled false -ca clus.ciscorobo.com
-serial 55243646 -common-name clus.ciscorobo.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 -vserver <<var_clustername>>
```

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

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

Configure NFSv3

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

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

1. Create a new rule for each ESXi host in the default export policy. Assign a rule for each ESXi host created so that each host has its own rule index. For example, the first ESXi host has rule index 1, the second ESXi host has rule index 2, and so on.

```
vserver export-policy rule create -vserver Infra-SVM -policyname default -ruleindex 1 -protocol nfs -
clientmatch <<var_esxi_host1_nfs_ip>> -rorule sys -rwrule sys -superuser sys -allow-suid false
vserver export-policy rule create -vserver Infra-SVM -policyname default -ruleindex 2 -protocol nfs -
clientmatch <<var_esxi_host2_nfs_ip>> -rorule sys -rwrule sys -superuser sys -allow-suid false
vserver export-policy rule show
```

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

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

Create FlexVol Volume

The following information is required to create a FlexVol volume:

- Volume name
- Volume size
- Aggregate on which the volume exists

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

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

1. Run the following commands:

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

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

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

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

Create Boot LUNs

To create two boot LUNs, complete the following step:

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

1. Run the following commands:

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

Enable Deduplication

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

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

1. Run the following commands:

```
volume efficiency on -vserver Infra-SVM -volume infra_datastore_1
volume efficiency on -vserver Infra-SVM -volume esxi_boot
```

Create iSCSI LIFs

To create four iSCSI LIFs (two on each node), complete the following step:

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

1. Run the following commands:

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data -data-protocol iscsi -home-node
<<var_node01>> -home-port e0c-<<var_iscsi_vlan_A_id>> -address <<var_node01_iscsi_lif01a_ip>> -netmask
<<var_node01_iscsi_lif01a_mask>> -status-admin up -failover-policy disabled -firewall-policy data -auto-
revert false

network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data -data-protocol iscsi -home-node
<<var_node01>> -home-port e0d-<<var_iscsi_vlan_B_id>> -address <<var_node01_iscsi_lif01b_ip>> -netmask
<<var_node01_iscsi_lif01b_mask>> -status-admin up -failover-policy disabled -firewall-policy data -auto-
revert false

network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data -data-protocol iscsi -home-node
<<var_node02>> -home-port e0c-<<var_iscsi_vlan_A_id>> -address <<var_node02_iscsi_lif01a_ip>> -netmask
<<var_node02_iscsi_lif01a_mask>> -status-admin up -failover-policy disabled -firewall-policy data -auto-
revert false

network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data -data-protocol iscsi -home-node
<<var_node02>> -home-port e0d-<<var_iscsi_vlan_B_id>> -address <<var_node02_iscsi_lif01b_ip>> -netmask
<<var_node02_iscsi_lif01b_mask>> -status-admin up -failover-policy disabled -firewall-policy data -auto-
revert false

network interface show
```

Create NFS LIF

To create an NFS LIF, complete the following step:

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

1. Run the following commands:

```
network interface create -vserver Infra-SVM -lif nfs_infra_swap -role data -data-protocol nfs -home-node
<<var_node01>> -home-port e0d-<<var_nfs_vlan_id>> -address <<var_node01_nfs_lif_infra_swap_ip>> -netmask
<<var_node01_nfs_lif_infra_swap_mask>> -status-admin up -failover-policy broadcast-domain-wide -firewall-
policy data -auto-revert true

network interface create -vserver Infra-SVM -lif nfs_infra_datastore_1 -role data -data-protocol nfs -home-
node <<var_node02>> -home-port e0d-<<var_nfs_vlan_id>> -address <<var_node02_nfs_lif_infra_datastore_1_ip>> -
netmask <<var_node02_nfs_lif_infra_datastore_1_mask>> -status-admin up -failover-policy broadcast-domain-wide
-firewall-policy data -auto-revert true

network interface show
```

Note: NetApp recommends creating a new LIF for each datastore. Note that both NFS lifs created here are placed on VLAN interface ports connected to the Fabric B Cisco UCS Fabric Interconnect. Corresponding NFS VMware VMkernel ports will also be pinned to Fabric B in the Cisco Nexus 1000V.

Add Infrastructure SVM Administrator

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

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

1. Run the following commands:

```
network interface create -vserver Infra-SVM -lif vsmgmt -role data -data-protocol none -home-node
<<var_node02>> -home-port  e0a -address <<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> -status-admin up -
failover-policy broadcast-domain-wide -firewall-policy mgmt -auto-revert true
```

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

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

```
network route create -vserver Infra-SVM -destination 0.0.0.0/0 -gateway <<var_svm_mgmt_gateway>>

network route show
```

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

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

security login unlock -username vsadmin -vserver Infra-SVM
```

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 remote office/branch office environment using UCS Central from a central location. The steps are necessary to provision the Cisco UCS C-Series and B-Series servers and should be followed precisely to avoid improper configuration.

Note: This document contains steps to set up a centralized Cisco UCS Central implementation and assumes that Cisco UCS Central has already been installed. The appendix of this document contains a procedure for installing Cisco UCS Central at a central location. The FlexPod DataCenter version of this document can be downloaded here. This version contains a section on deploying the FlexPod Cisco UCS (without Cisco UCS Central) if you are deploying a standalone Cisco UCS system. The Cisco UCS Central Best Practices Guide is available here: https://communities.cisco.com/docs/DOC-35264.

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 UCS Fabric A 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 6248 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

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

  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 : <<var_ucs_cluster_ip>>

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

       DNS IP address : <<var_nameserver_ip>>

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

  Join centralized management environment (UCS Central)? (yes/no) [n]: yes
        UCS central IPv4 address: <<var_UCS_central_ip>>
        Enter the shared secret to join <<var_UCS_central_ip>>: <<var_UCS_central_secret>>


 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 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:<<var_password>>
    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: <<var_ucs_cluster_address>>

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

  Physical Switch Mgmt0 IP address : <<var_ucsb_mgmt_ip>>


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

  Configuration file - Ok
```

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

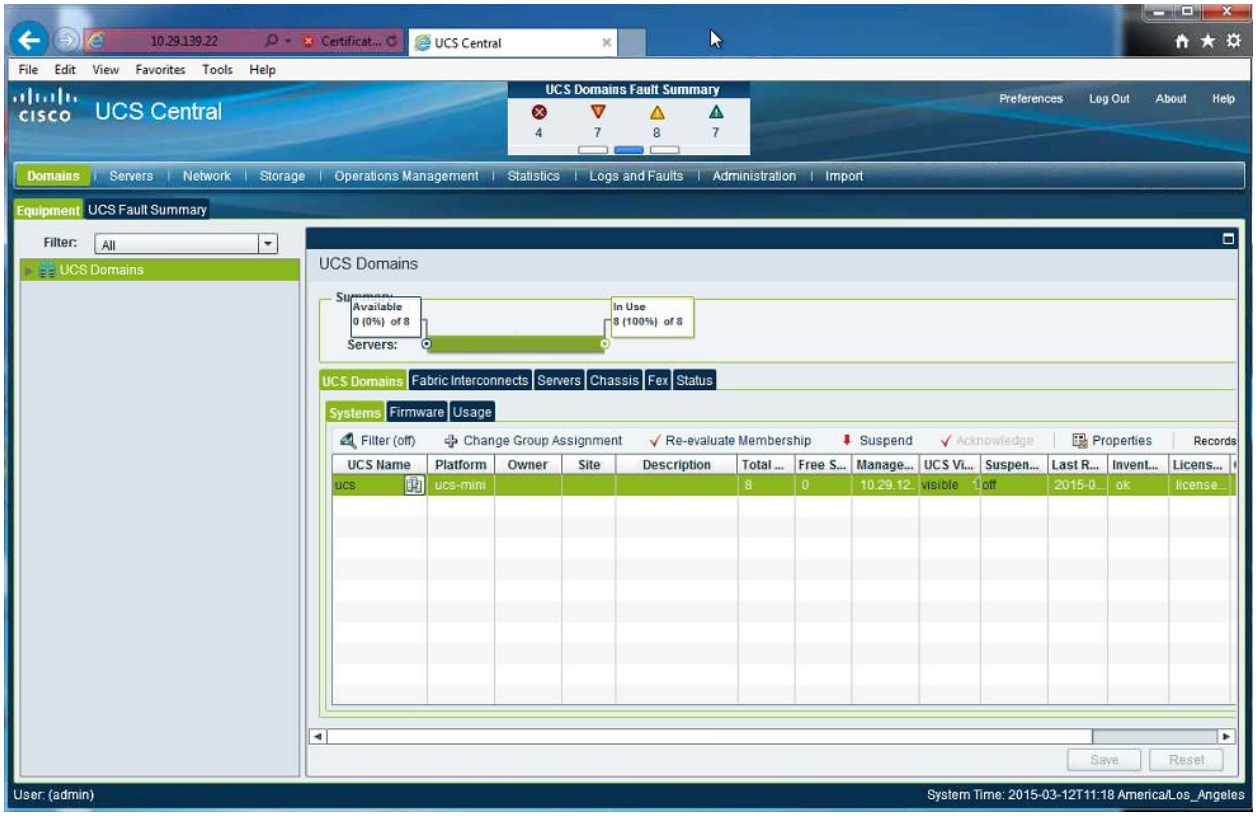
FlexPod Cisco UCS vSphere on Clustered Data ONTAP

Log in to Cisco UCS Central

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

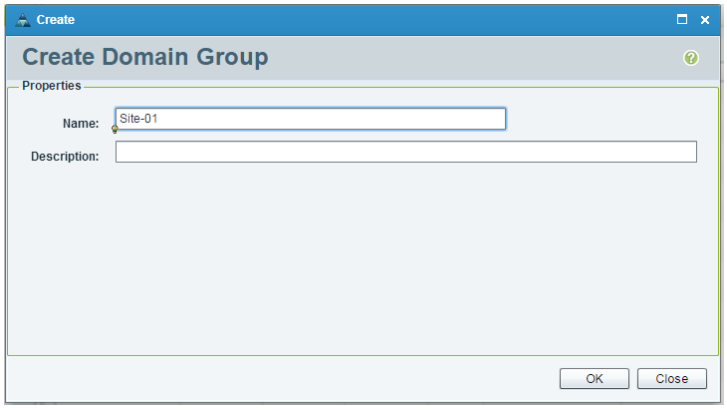
1. Open a web browser and navigate to the Cisco UCS Central address

2. When prompted, enter `admin` as the user name and enter the administrative password.
3. To log in to Cisco UCS Central, click Login.



Add Cisco UCS Domain to Cisco UCS Domain Group

1. To add your newly created UCS Domain to a domain group, complete the following steps.
2. Select the Domains tab.
3. Expand UCS Domains > Domain Groups in the left pane.
4. Right-click Domain Group root in the left pane and select Create Domain Group.
5. Name the Domain Group “Site-XX” and click OK.

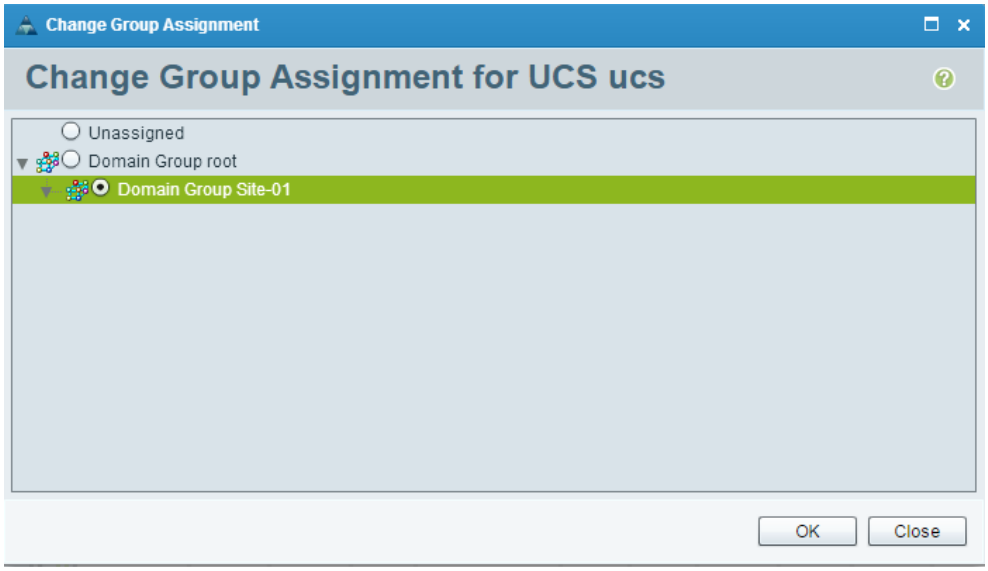


6. In the left pane, select UCS Domains. The newly created UCS Domain should appear in the list in the right pane.

Note: It may take a few minutes for the newly created UCS Domain to appear under `Ungrouped Domains`

7. Right-click the newly created UCS Domain and select Change Group Assignment

8. Expand Domain Group root and select the Domain Group Site-XX radio button.



9. Click OK. Click Yes to confirm the warning.

Cisco UCS Manager Software Version 3.0(2c)

This document assumes the use of Cisco UCS Manager Software version 3.0(2c). To upgrade the Cisco UCS Manager software and the UCS 6324 Fabric Interconnect software refer to Cisco UCS Manager Install and Upgrade Guides.

1. In UCS Central, Click the Domains tab. Select UCS Domains in the left pane and the Firmware tab in the right pane.

2. In the list, if version 3.0(2c) is not installed, follow the Install and Upgrade guide link above to install the infrastructure software bundle on Cisco UCS Manager. Make sure that the 3.0(2c) software packages for B and C-Series servers are NOT installed on the Cisco UCS Fabric Interconnects.

Note: It may take a few minutes before the FW Version appears for the new UCS domain.

Open Cisco UCS Manager from Cisco UCS Central

To access Cisco UCS Manager from Cisco UCS Central

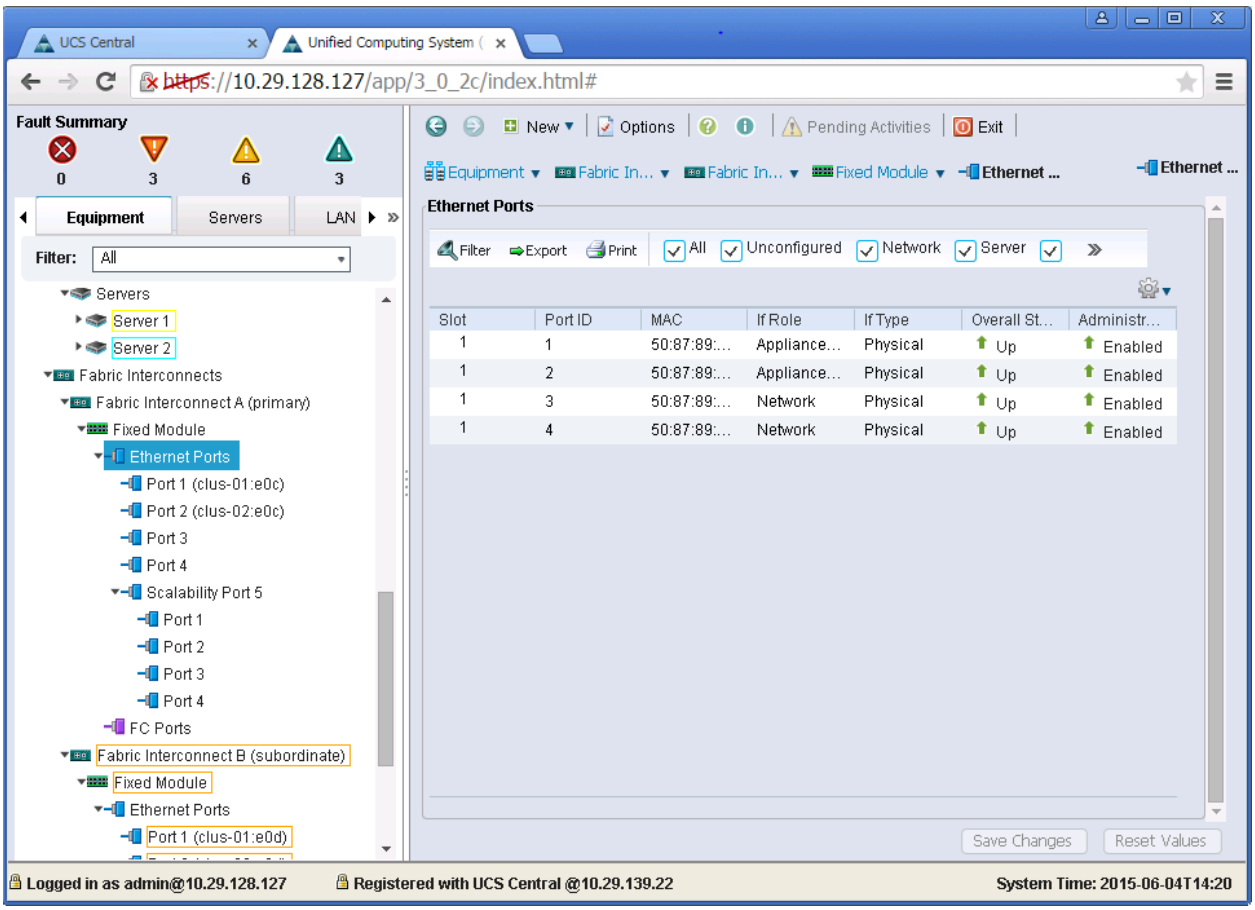
1. Click the Domains Tab. Select UCS Domains in the left pane.

2. In the list in the right pane, click the button to the right of the UCS domain name.
3. Click Accept to accept the security certificate.
4. Navigate the security prompts to get to the UCS Manager web page.
5. Click Launch UCS Manager in the HTML box.
6. Enter `admin` as the user id and <<var_password>> as the password.
7. Respond to the Anonymous Reporting dialog and click OK.

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. Expand Equipment > Fabric Interconnects > Fabric Interconnect A > Fixed Module.
3. Expand Ethernet Ports.
4. One at a time, 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 1 and 2 that are connected to the NetApp Storage Controllers, right-click them, and select Configure as Appliance Port.
7. Click Yes to confirm appliance ports.
8. On the Configure as Appliance Port window, click OK.
9. Click OK to confirm.
10. Select ports 3 and 4 that are connected to the Cisco Nexus 3524 switches, right-click them, and select Configure as Uplink Port.
11. Click Yes to confirm uplink ports and click OK.
12. In the left pane, select Fixed Module under Fabric Interconnect A.
13. Under the Ethernet Ports tab, confirm that ports have been configured correctly in the IfRole column. If any port C-Series servers were configured on the Scalability port, click on it to verify port connectivity there.



14. Expand Equipment > Fabric Interconnects > Fabric Interconnect B > Fixed Module.

15. Expand Ethernet Ports.

16. One at a time, select the ports that are connected directly to C-Series rack servers, right-click them, and select Configure as Server Port.

17. Click Yes to confirm server ports and click OK.

18. Select ports 1 and 2 that are connected to the NetApp Storage Controllers, right-click them, and select Configure as Appliance Port.

19. Click Yes to confirm appliance ports.

20. On the Configure as Appliance Port window, click OK.

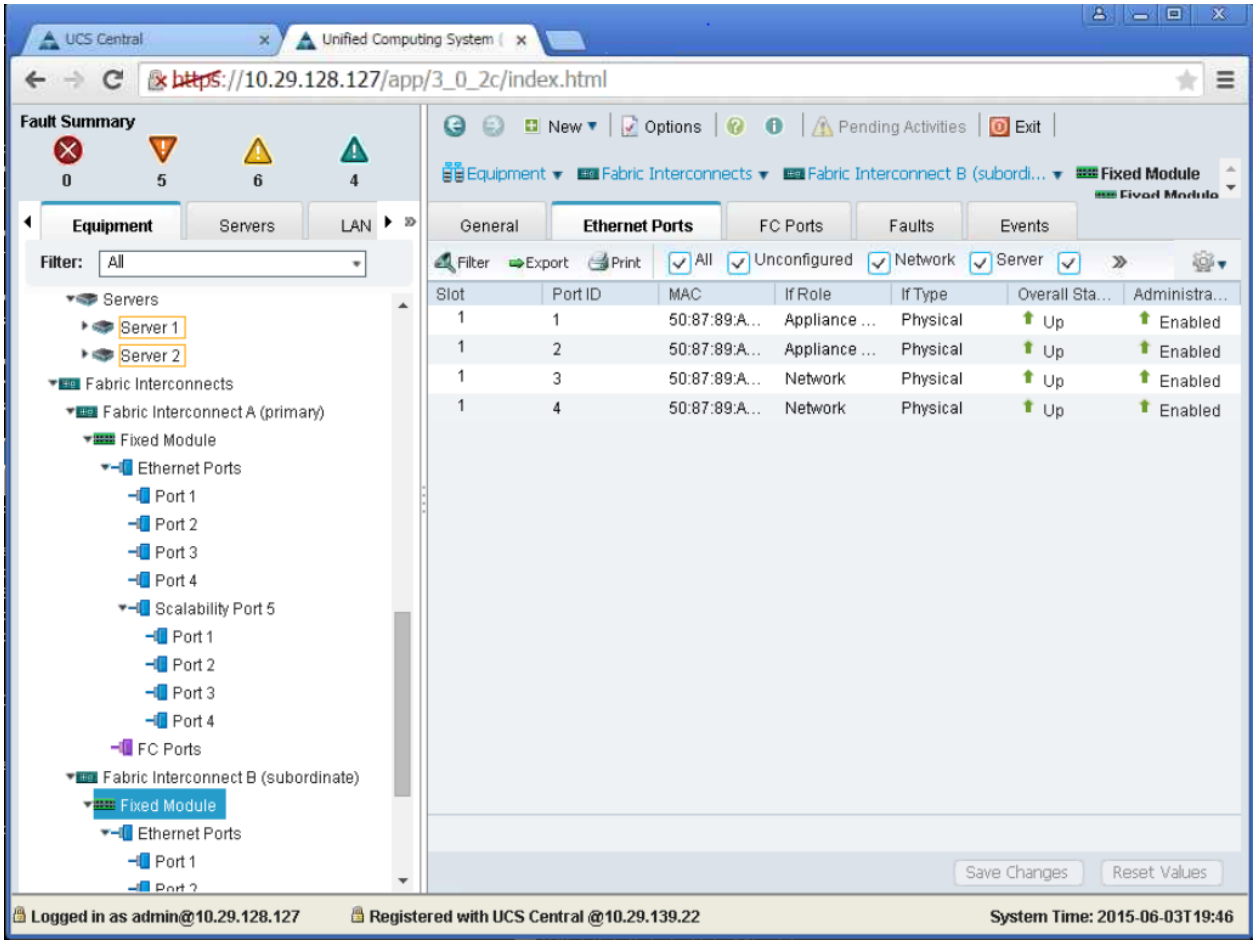
21. Click OK to confirm.

22. Select Ethernet ports 3 and 4 that are connected to the Cisco Nexus 3524 switches, right-click them, and select Configure as Uplink Port.

23. Click Yes to confirm the uplink ports and click OK.

24. In the left pane, select Fixed Module under Fabric Interconnect B.

25. Under the Ethernet Ports tab, confirm that ports have been configured correctly in the IfRole column. If any port C-Series servers were configured on the Scalability port, click it to verify port connectivity there.



Create Uplink Port Channels to Cisco Nexus 3524 Switches

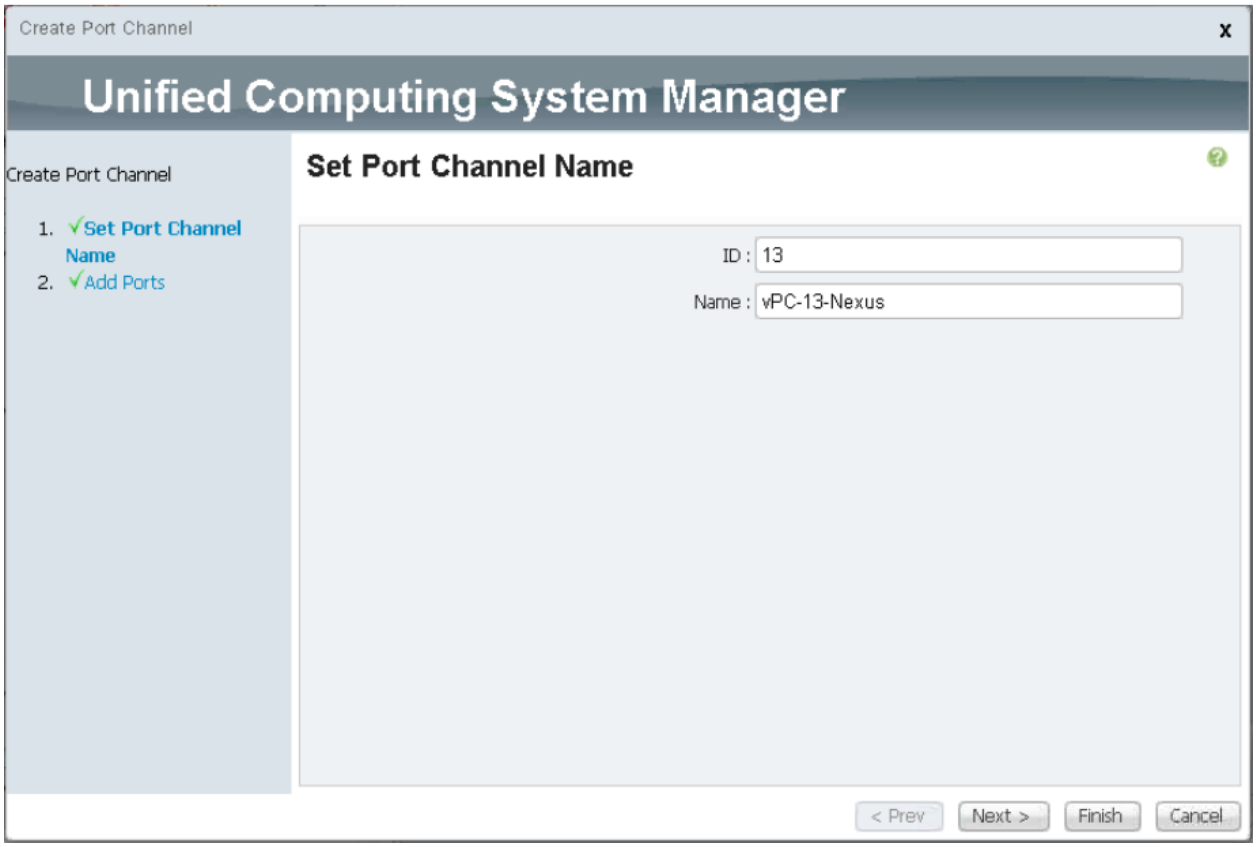
To configure the necessary port channels in the Cisco UCS environment, complete the following steps:

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

Note: In this procedure, two port channels are created: one from Fabric A to both Cisco Nexus 3524 switches and one from Fabric B to both Cisco Nexus 3524 switches. If using standard switches, modify this procedure accordingly. If using 1 GE switches and GLC-T SFPs on the Fabric Interconnects, the interface speeds of Ethernet ports 1/3 and 1/4 in the Fabric Interconnects will be need to be set to 1 Gb/s.

2. Under LAN > LAN Cloud, expand the Fabric A tree.
3. Right-click Port Channels.
4. Select Create Port Channel.
5. Enter `13` as the unique ID of the port channel.

6. Enter `vPC-13-Nexus` as the name of the port channel.
7. Click Next.



8. Select the following ports to be added to the port channel:
   - Slot ID 1 and port 3
   - Slot ID 1 and port 4
9. Click >> to add the ports to the port channel.
10. Click Finish to create the port channel.
11. Click OK.
12. Under Port Channels, select the newly created port-channel.
13. The port-channel should have an Overall Status of Up.
14. In the navigation pane, under LAN > LAN Cloud, expand the Fabric B tree.
15. Right-click Port Channels.
16. Select Create Port Channel.

17. Enter `14` as the unique ID of the port channel.
18. Enter `vPC-14-Nexus` as the name of the port channel.
19. Click Next.
20. Select the following ports to be added to the port channel:
    - Slot ID 1 and port 3
    - Slot ID 1 and port 4
21. Click >> to add the ports to the port channel.
22. Click Finish to create the port channel.
23. Click OK.
24. Under Port Channels, select the newly created port-channel.
25. The port-channel should have an Overall Status of Up.

Create an Organization (Optional)

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:

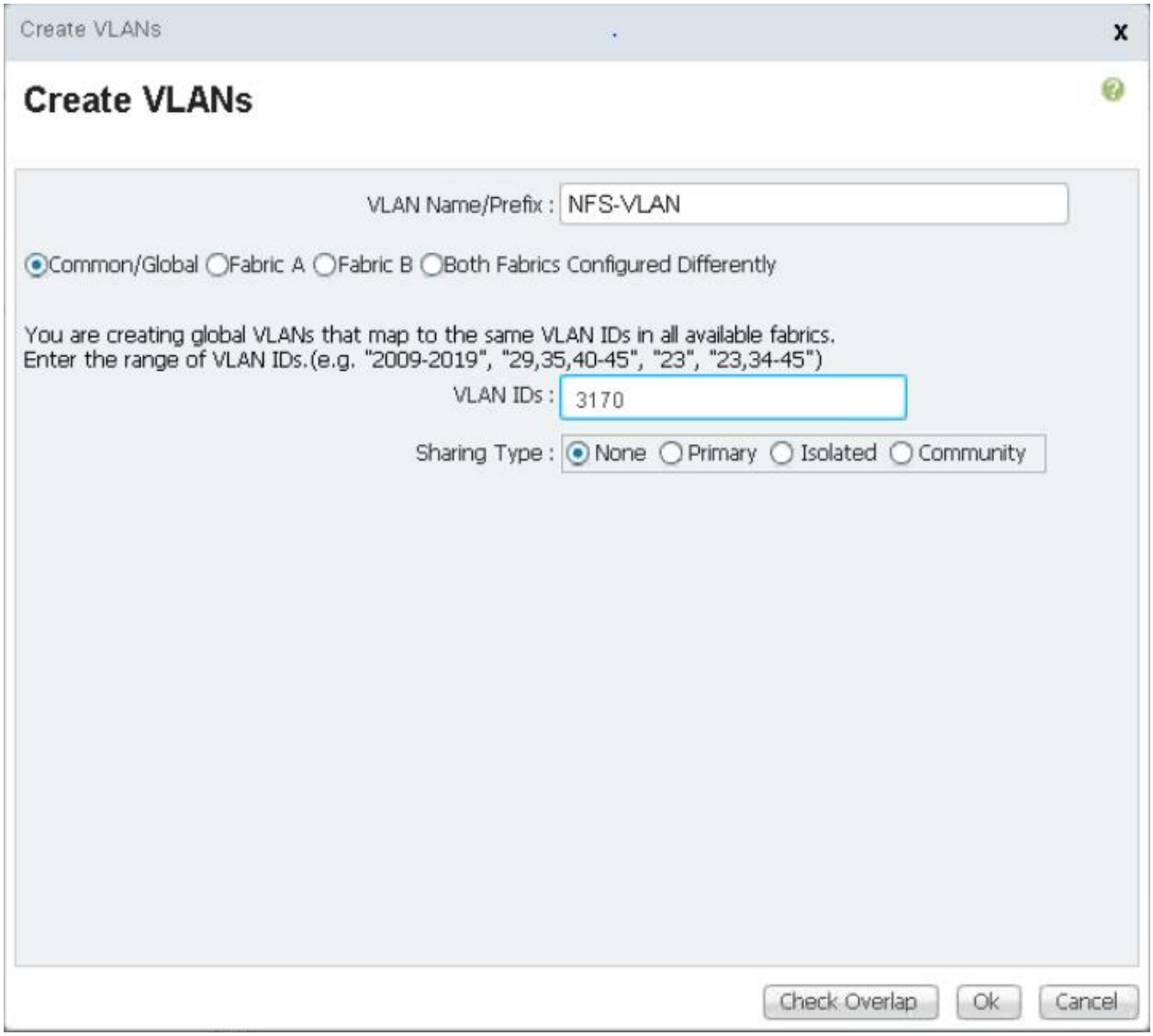
1. In Cisco UCS Manager, from the New menu in the toolbar at the top of the window, select Create Organization.
2. Enter a name for the organization.
3. Optional: Enter a description for the organization.
4. Click OK.
5. Click OK in the confirmation message.

Configure Storage Appliance Ports and Storage VLANs

Follow the steps below to configure the storage appliance ports and storage VLANs.

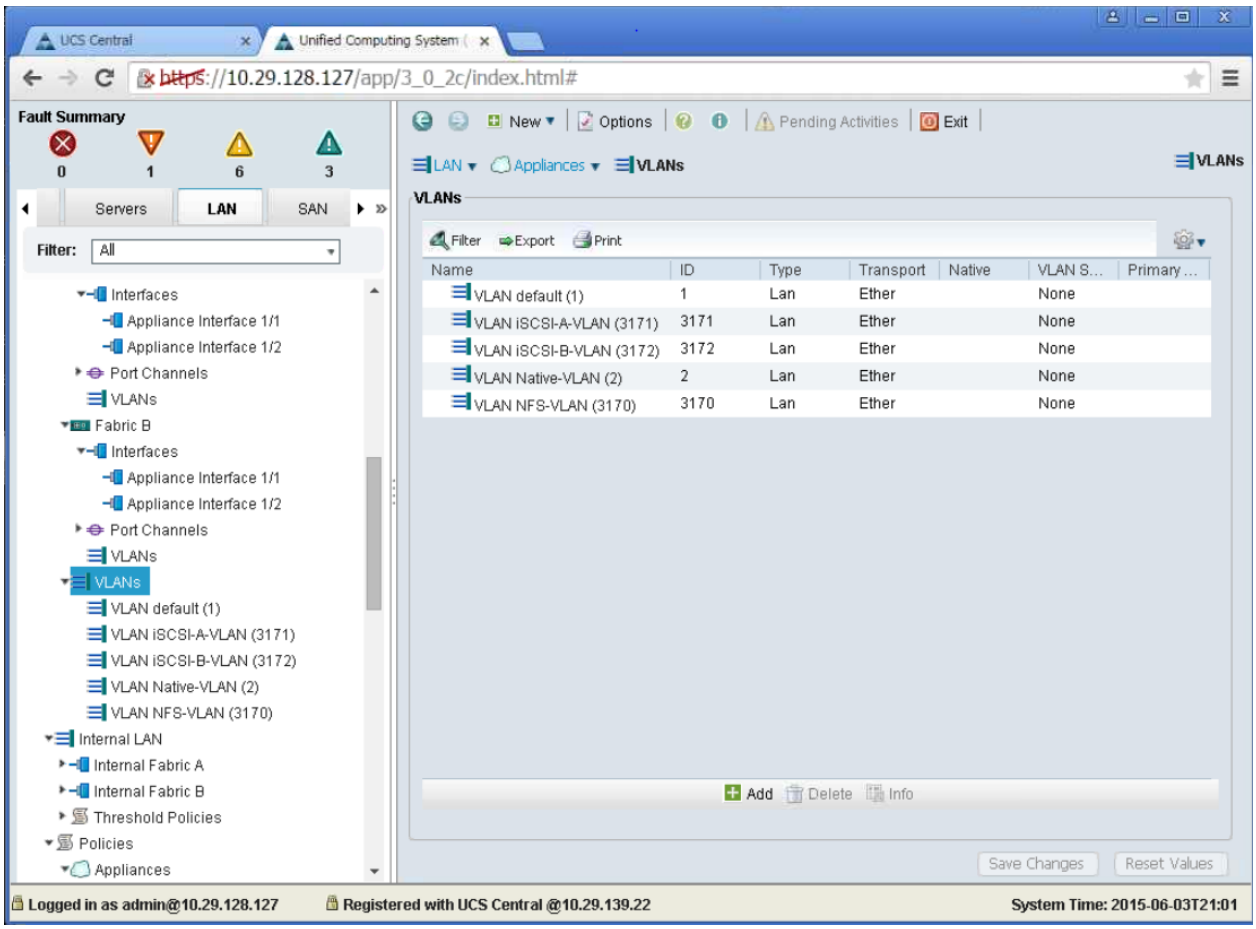
1. In the Cisco UCS Manager, select the LAN tab.
2. Expand the Appliances cloud.
3. Right-click VLANs under Appliances Cloud.

4. Select Create VLANs.
5. Enter `NFS-VLAN` as the name for the Infrastructure NFS VLAN.
6. Leave Common/Global selected.
7. Enter <<var_nfs_vlan_id>> for the VLAN ID.
8. Leave Sharing Type set to None.



9. Click OK, and then click OK again to create the VLAN.
10. Right-click VLANs under Appliances Cloud.
11. Select Create VLANs.
12. Enter `iSCSI-A-VLAN` as the name for the Infrastructure iSCSI Fabric A VLAN.

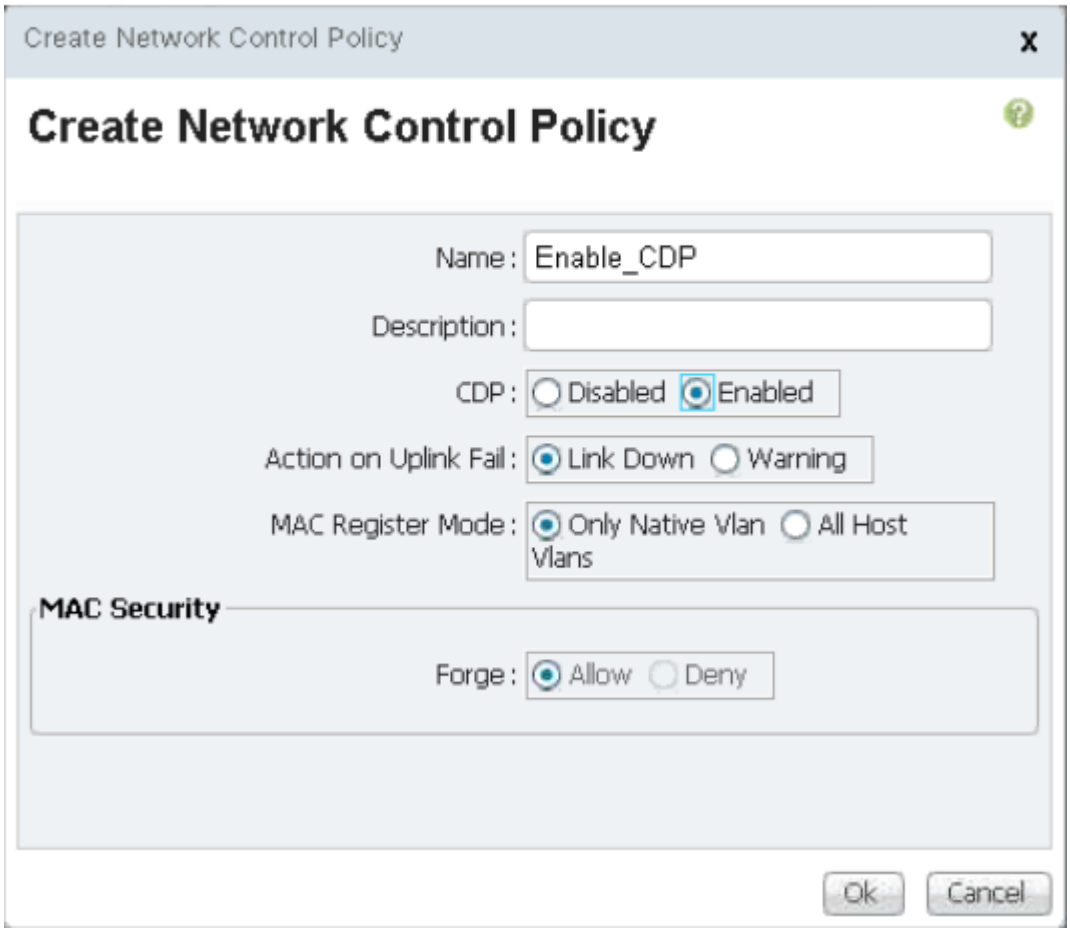
13. Leave Common/Global selected.
14. Enter <<var_iscsi-a_vlan_id>> for the VLAN ID.
15. Click OK, and then click OK again to create the VLAN.
16. Right-click VLANs under Appliances Cloud.
17. Select Create VLANs.
18. Enter `iSCSI-B-VLAN` as the name for the Infrastructure iSCSI Fabric B VLAN.
19. Leave Common/Global selected.
20. Enter <<var_iscsi-b_vlan_id>> for the VLAN ID.
21. Click OK, and then click OK again to create the VLAN.
22. Right-click VLANs under Appliances Cloud.
23. Select Create VLANs.
24. Enter `Native-VLAN` as the name for the Native VLAN.
25. Leave Common/Global selected.
26. Enter <<var_native_vlan_id>> for the VLAN ID.
27. Click OK, and then click OK again to create the VLAN.



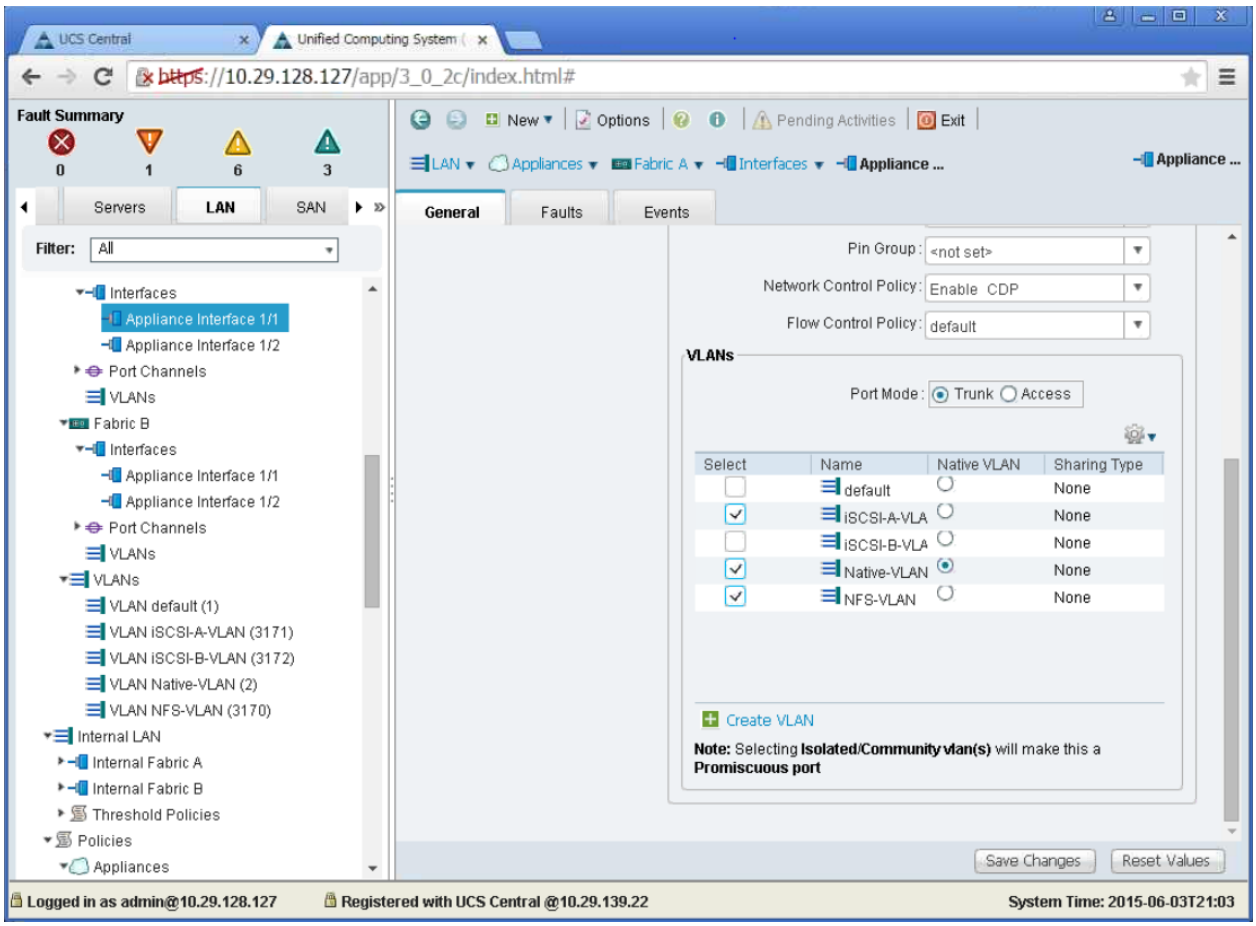
28. In the navigation pane, under LAN > Policies, expand Appliances and right-click Network Control Policies.

29. Select Create Network Control Policy.

30. Name the policy Enable_CDP and select Enabled next to CDP.



31. Click OK and then click OK again to create the policy.
32. In the navigation pane, under LAN > Appliances Cloud, expand the Fabric A tree.
33. Expand Interfaces.
34. Select Appliance Interface 1/1.
35. In the User Label field, put in information indicating the storage controller port, such as <storage_controller_01_name>:e0c. Click Save Changes and OK.
36. Select the Enable_CDP Network Control Policy and select Save Changes and OK.
37. Under VLANs, select the iSCSI-A-VLAN, NFS VLAN, and Native VLAN. Set the Native-VLAN as the Native VLAN. Unselect the default VLAN.



38. Click Save Changes and OK.

39. Select Appliance Interface 1/2 under Fabric A.

40. In the User Label field, put in information indicating the storage controller port, such as <storage_controller_02_name>:e0c. Click Save Changes and OK.

41. Select the Enable_CDP Network Control Policy and select Save Changes and OK.

42. Under VLANs, select the iSCSI-A-VLAN, NFS VLAN, and Native VLAN. Set the Native-VLAN as the Native VLAN. Unselect the default VLAN.

43. Click Save Changes and OK.

44. In the navigation pane, under LAN > Appliances Cloud, expand the Fabric B tree.

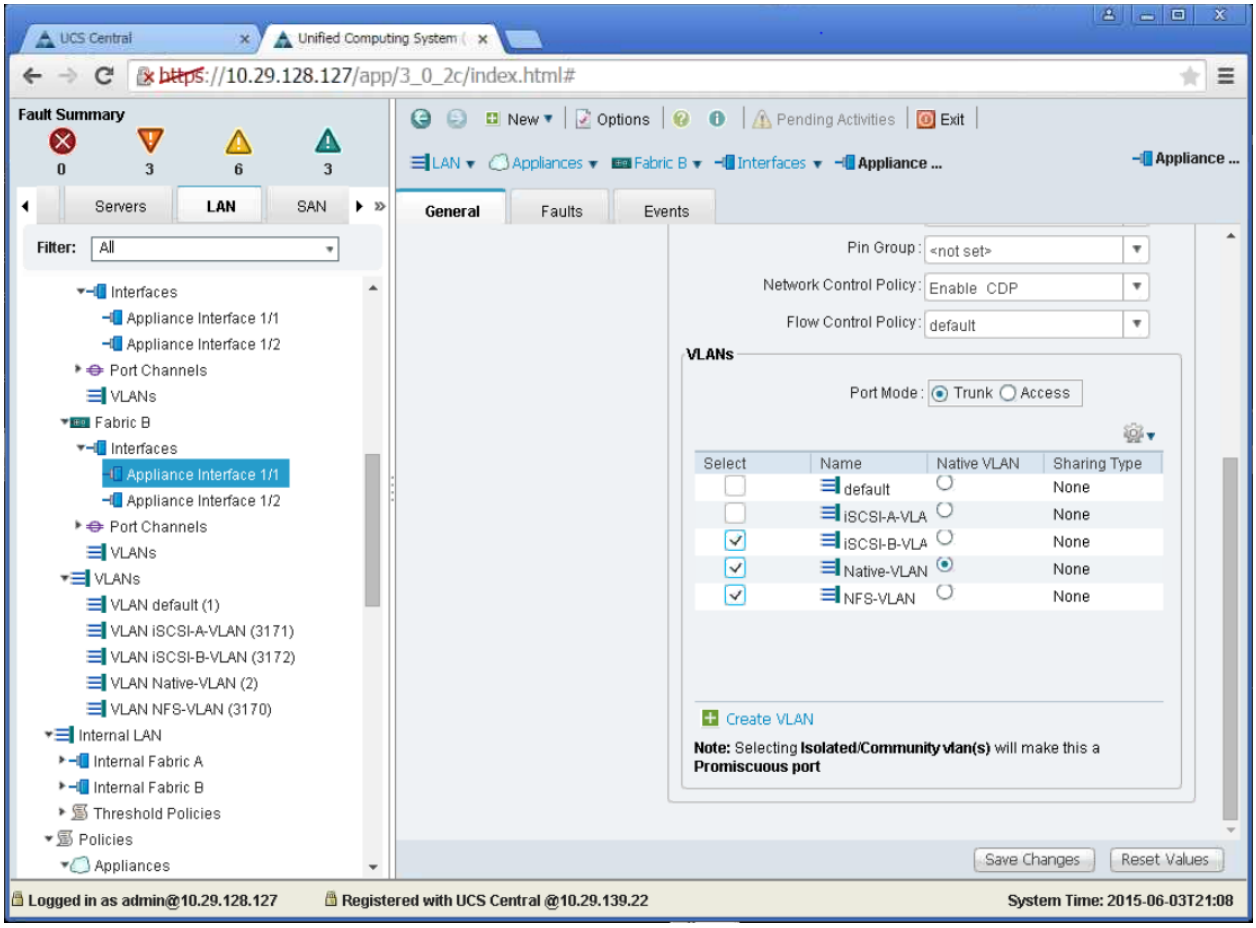
45. Expand Interfaces.

46. Select Appliance Interface 1/1.

47. In the User Label field, put in information indicating the storage controller port, such as <storage_controller_01_name>:e0d. Click Save Changes and OK.

48. Select the Enable_CDP Network Control Policy and select Save Changes and OK.

49. Under VLANs, select the iSCSI-B-VLAN, NFS VLAN, and Native VLAN. Set the Native-VLAN as the Native VLAN. Unselect the default VLAN.



50. Click Save Changes and OK.

51. Select Appliance Interface 1/2 under Fabric B.

52. In the User Label field, put in information indicating the storage controller port, such as <storage_controller_02_name>:e0d. Click Save Changes and OK.

53. Select the Enable_CDP Network Control Policy and select Save Changes and OK.

54. Under VLANs, select the iSCSI-B-VLAN, NFS VLAN, and Native VLAN. Set the Native-VLAN as the Native VLAN. Unselect the default VLAN.

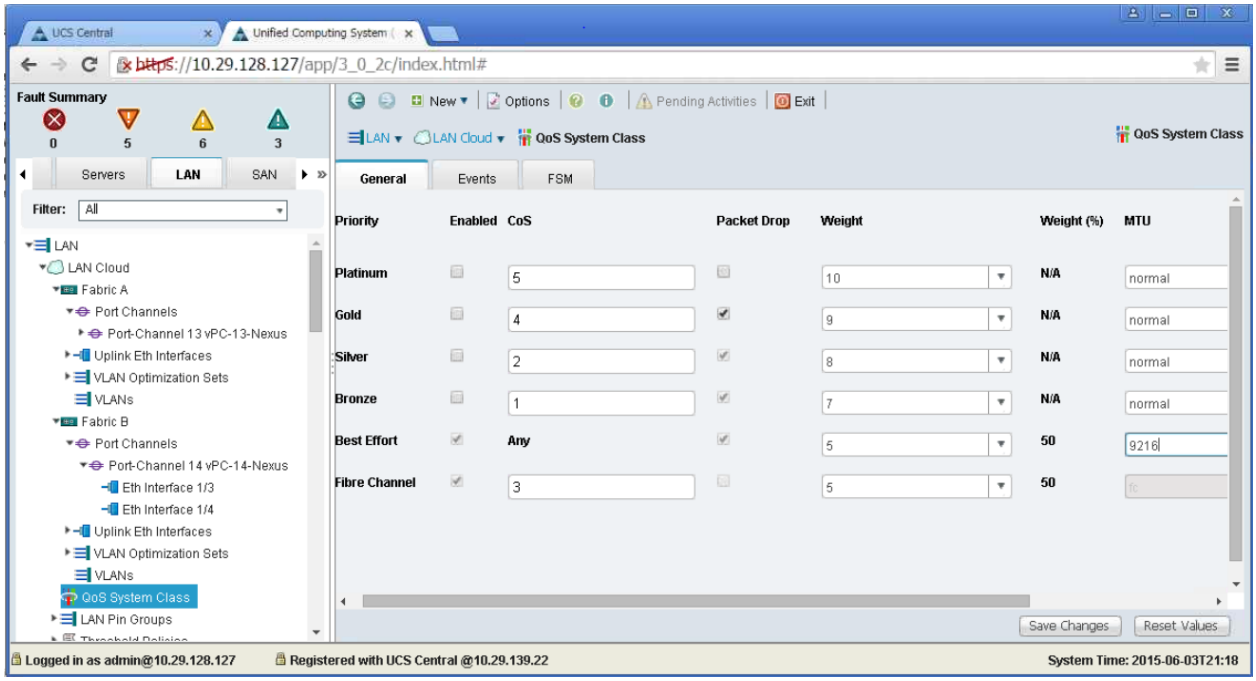
55. Click Save Changes and OK.

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.

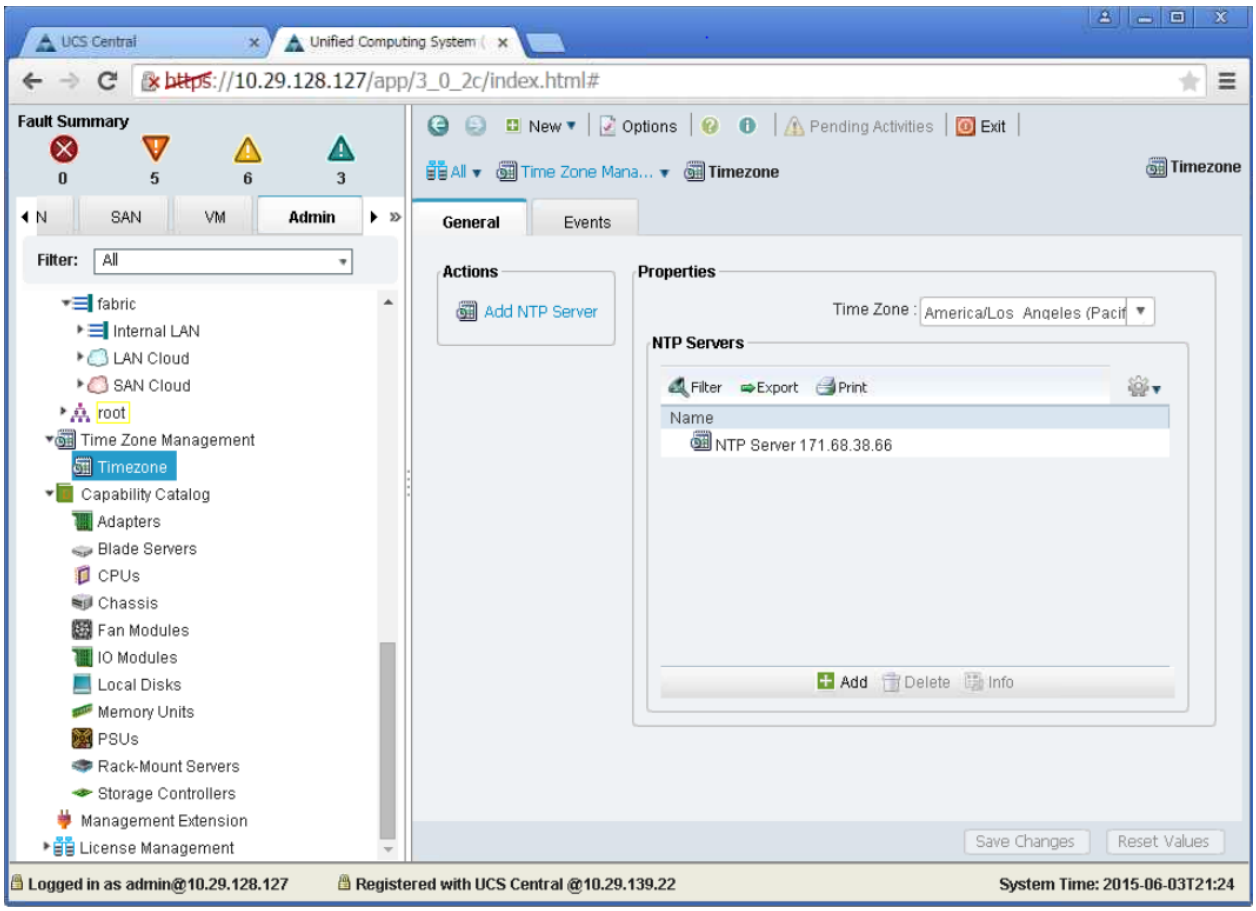


5. Click Save Changes.
6. Click OK.

Synchronize Cisco UCS to NTP

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

1. In Cisco UCS Manager, select the Admin tab. In the left pane, expand All and select Time Zone Management > Timezone.
2. Select the appropriate Time Zone and click Save Changes.
3. Click OK.
4. Select Add NTP server
5. Enter `<<var_global_ntp_server_ip>>` and click OK.
6. Click OK at the confirmation dialogue.

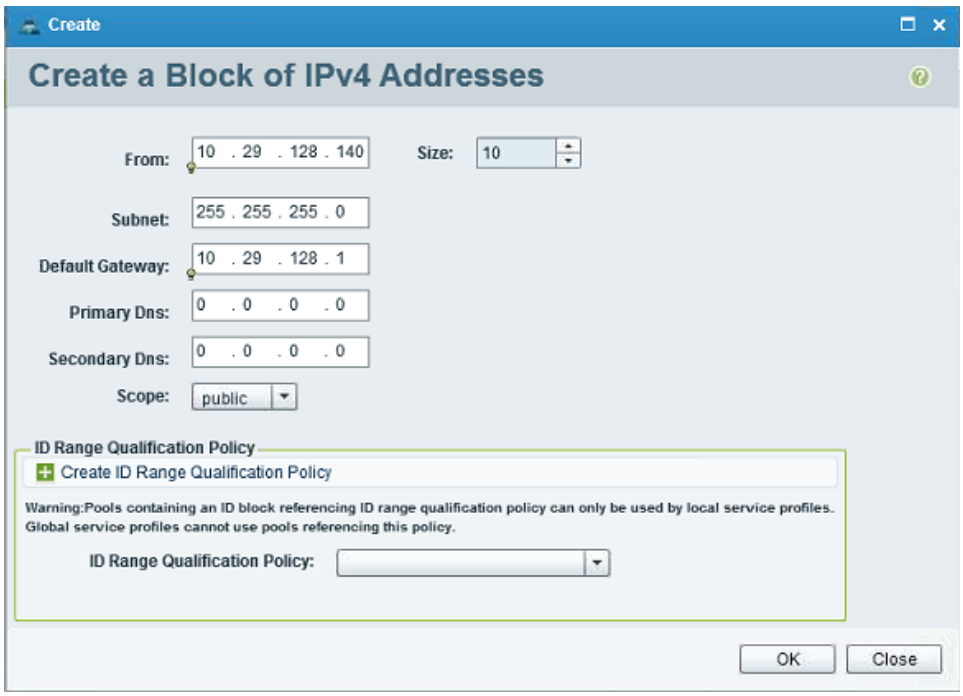


Add Block of IP Addresses for Out-of-Band KVM Access

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 Central, click the Network tab
2. Expand Network > Pools > root > IP Pools.
3. Right-click IP Pools and select Create IP Pool.
4. Name the pool Site-XX-ext-mgmt and select the IP Blocks tab.
5. Select Create a Block of IPv4 Addresses
6. Fill in the From, Size, Subnet, and Default Gateway fields.



7. Click OK.
8. Click OK to create the IP Pool.

Acknowledge Cisco UCS Chassis

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

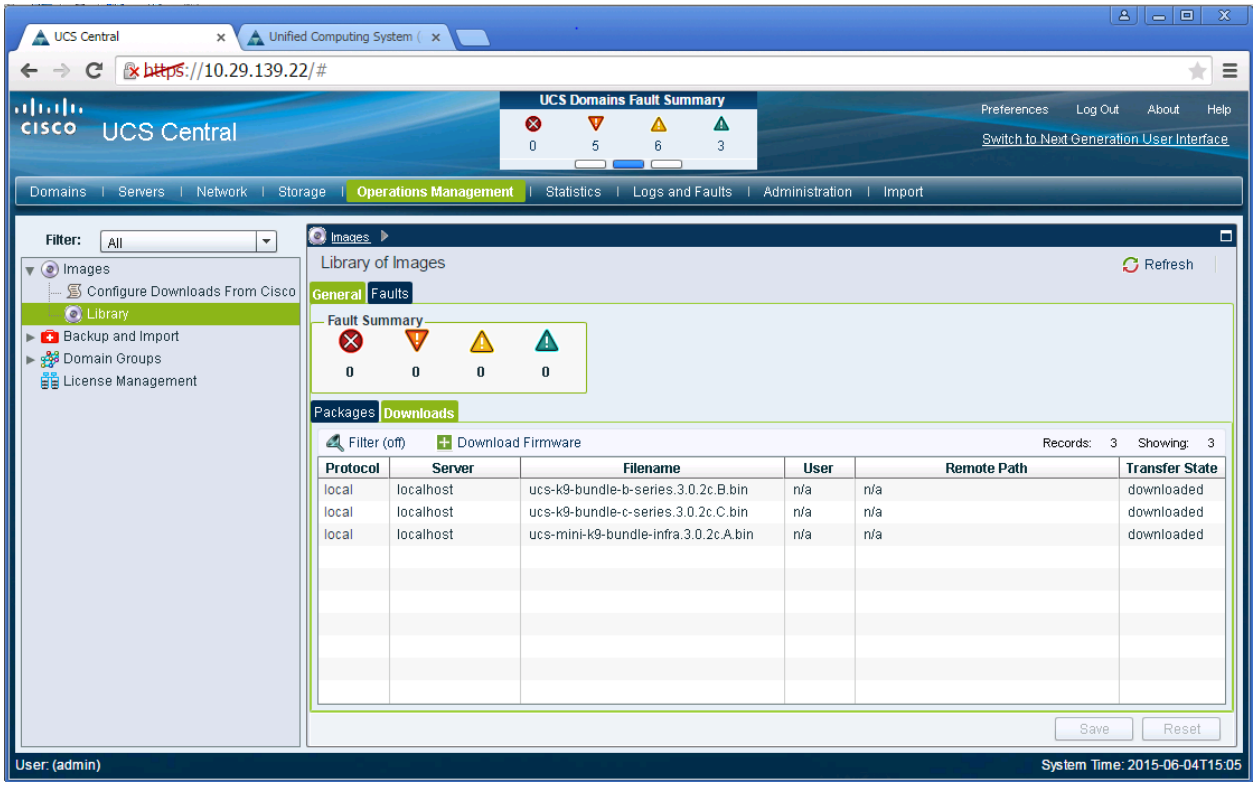
1. In Cisco UCS Central, click the Domains tab, then the Equipment tab on the left.
2. Expand UCS Domains> Domain Groups> Domain Group root> Domain Group Site-XX >UCS Domain>Chassis
3. Right-click the Chassis 1 and select Properties.
4. In the Properties window, select Acknowledge Chassis.
5. Click OK and then click OK to complete acknowledging the chassis.
6. Click Close to close the Properties window.

Load Cisco UCS Version 3.0(2c) Firmware Images into Cisco UCS Central

To load the UCS version 3.0(2c) firmware images into UCS Central, complete the following steps:

1. Download from www.cisco.com the UCS version 3.0(2c) Infrastructure, B-Series, and C-Series bundles to a folder on the management workstation.
2. In Cisco UCS Central, click the Operations Management tab.
3. In the left pane, expand Images and select Library.

4. In the center pane, select the Downloads tab.
5. Click Download Firmware.
6. In the Download Firmware window, select Local File System.
7. Select Download into Image library.
8. Click Choose File and browse to and select the B-Series bundle for version 3.0(2c).
9. Click Open.
10. Click Submit.
11. Click OK.
12. Click Download Firmware.
13. In the Download Firmware window, select Local File System.
14. Select Download into Image library.
15. Click Choose File and browse to and select the C-Series bundle for version 3.0(2c).
16. Click Open.
17. Click Submit.
18. Click OK.
19. Click Download Firmware.
20. In the Download Firmware window, select Local File System.
21. Select Download into Image library.
22. Click Choose File and browse to and select the infra bundle for version 3.0(2c).
23. Click Open.
24. Click Submit.
25. Click OK.
26. All three bundles should now be loaded into UCS Central.

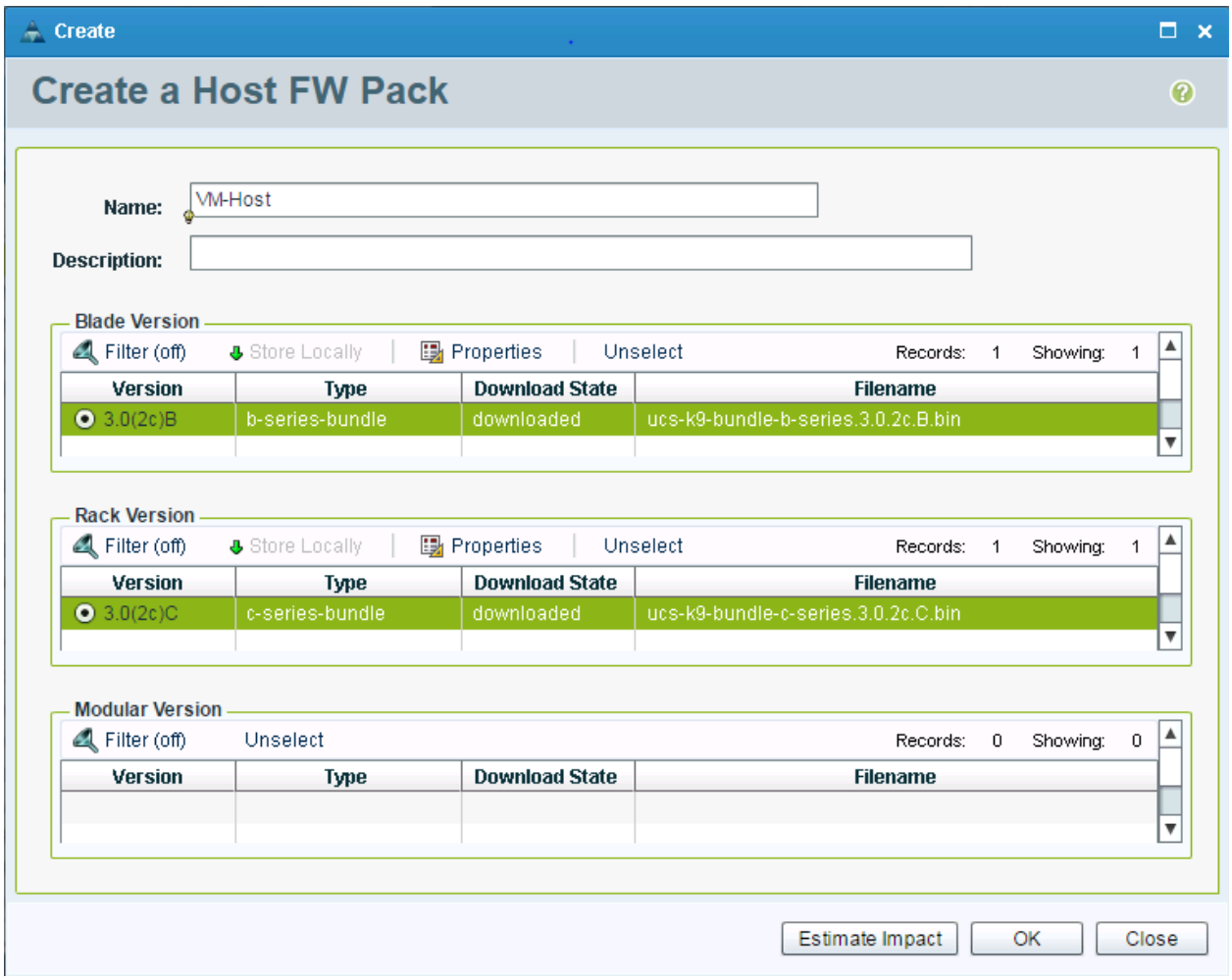


Create Host Firmware Package

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 Central, click the Servers tab.
2. In the left pane, expand Servers> Policies > root.
3. Right-click Host Firmware Packages.
4. Select Create a Host FW Pack.
5. Enter `VM-Host` as the name for the host firmware package.
6. Select the version 3.0(2c) for the blade version and rack version packages.



7. Click OK to create the host firmware package.

Create MAC Address Pools

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

Note: In this procedure, two large MAC Pools are created to cover all sites managed by UCS Central. Note that site-based MAC Pools can also be created.

1. In Cisco UCS Central, click the Network tab.
2. Expand Pools >root > MAC Pools.

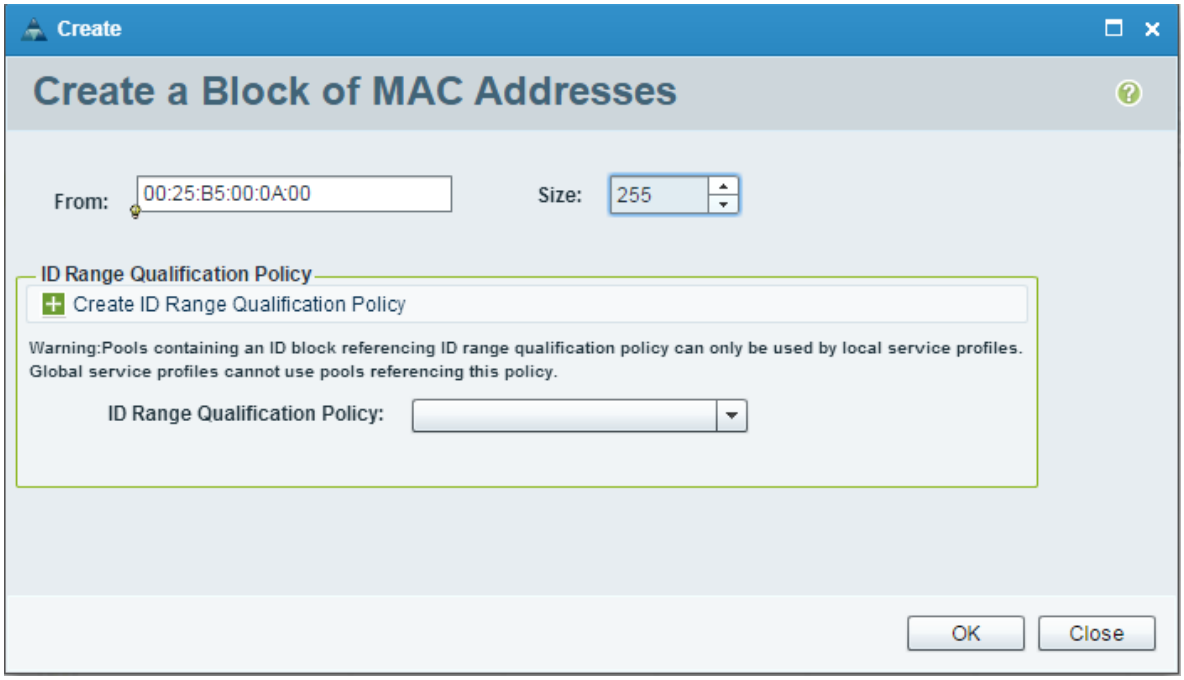
Note: In this procedure, two MAC address pools are created, one for each switching fabric.

3. Right-click MAC Pools and select create MAC pool
4. Enter `MAC_Pool_A` as the name for the MAC pool.

5. Optional: Enter a description for the MAC pool.
6. Click the MAC Blocks tab, then click Create a block of MAC Addresses.
7. 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.

8. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources at all sites managed by UCS Central.



9. Click OK
10. In the create window, click OK.
11. Right-click MAC Pools and select create MAC pool
12. Enter `MAC_Pool_B` as the name for the MAC pool.
13. Optional: Enter a description for the MAC pool.
14. Click the MAC Blocks Tab, then click Create a block of MAC Addresses.
15. Specify a starting MAC address.

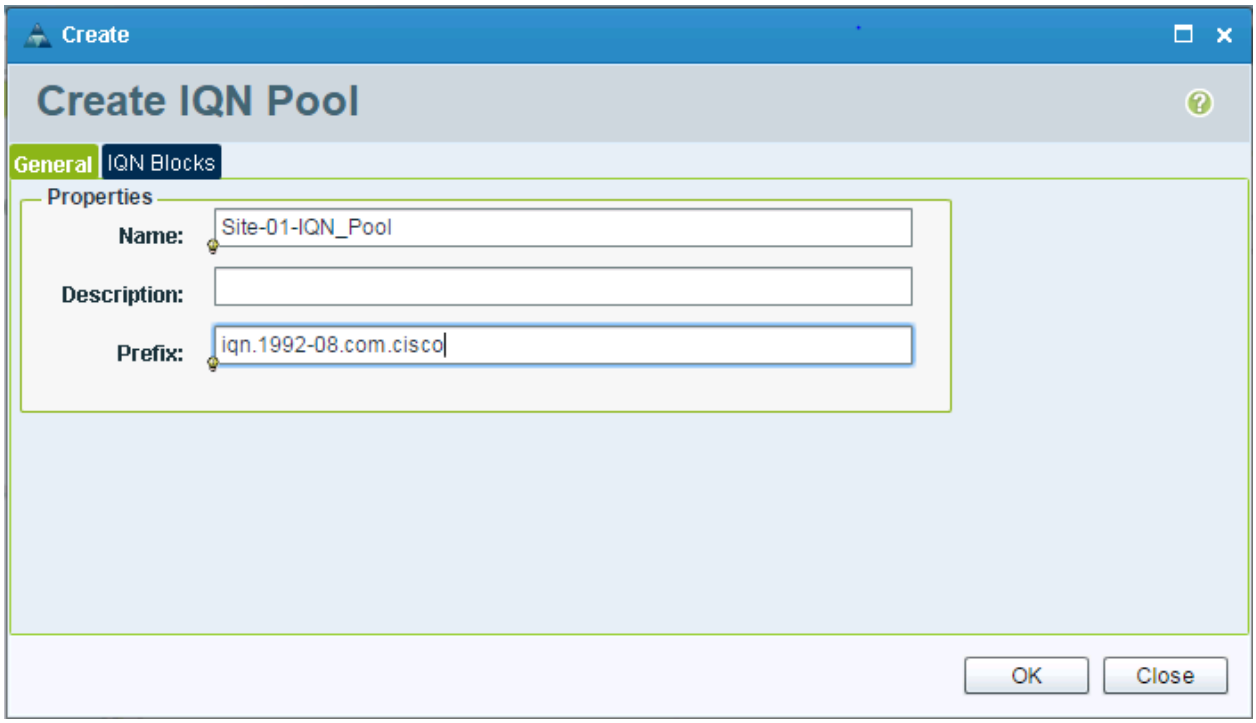
Note: For the FlexPod solution, the recommendation is to place `0B` in the next to last octet of the starting MAC address to identify all the MAC addresses in this pool as Fabric B addresses.

16. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources at all sites managed by UCS Central.
17. Click OK.
18. Click OK
19. In the create window, click OK.

Create iSCSI IQN Pool

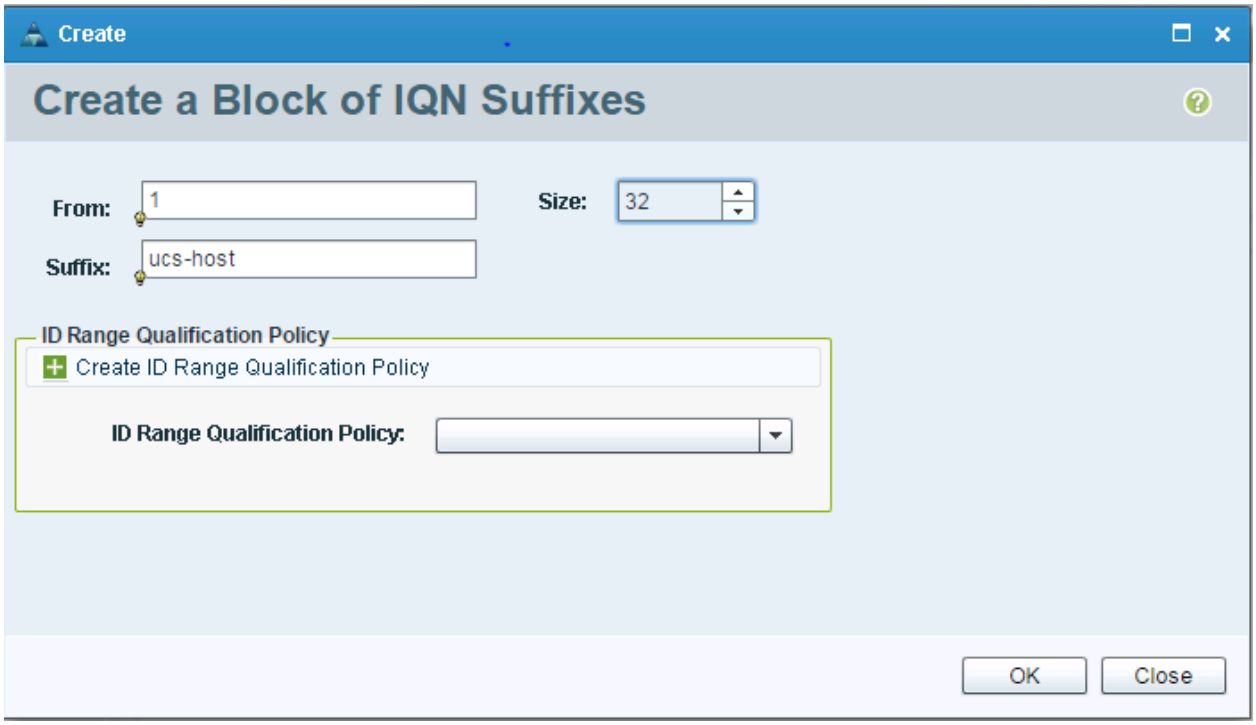
To configure the necessary IQN pool for the local site Cisco UCS environment, complete the following steps:

1. In Cisco UCS Central, click the Storage tab.
2. Expand Storage > Pools > root.
3. Right-click IQN Pools.
4. Select Create IQN Pool.
5. Enter `Site-XX-IQN_Pool` as the name for IQN pool.
6. Optional: Add a description for the IQN pool.
7. Enter iqn.1992-08.com.cisco as the Prefix.



8. Select the IQN Blocks tab.
9. Click Create a Block of IQN Suffixes.

10. Enter 1 for From.
11. Enter ucs-host for the Suffix.
12. Enter a size appropriate to your environment.



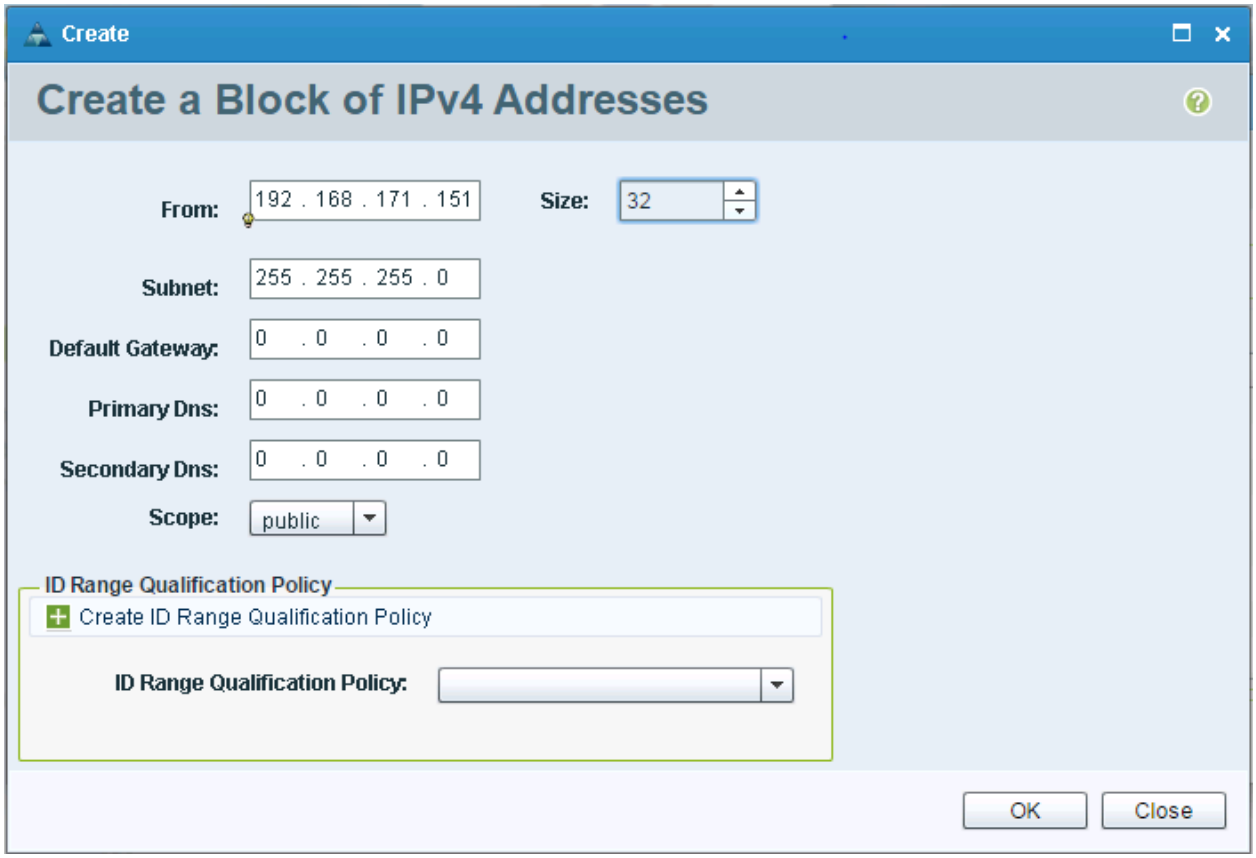
13. Click OK.
14. Click OK to complete creating the IQN pool.

Create iSCSI Initiator IP Address Pools

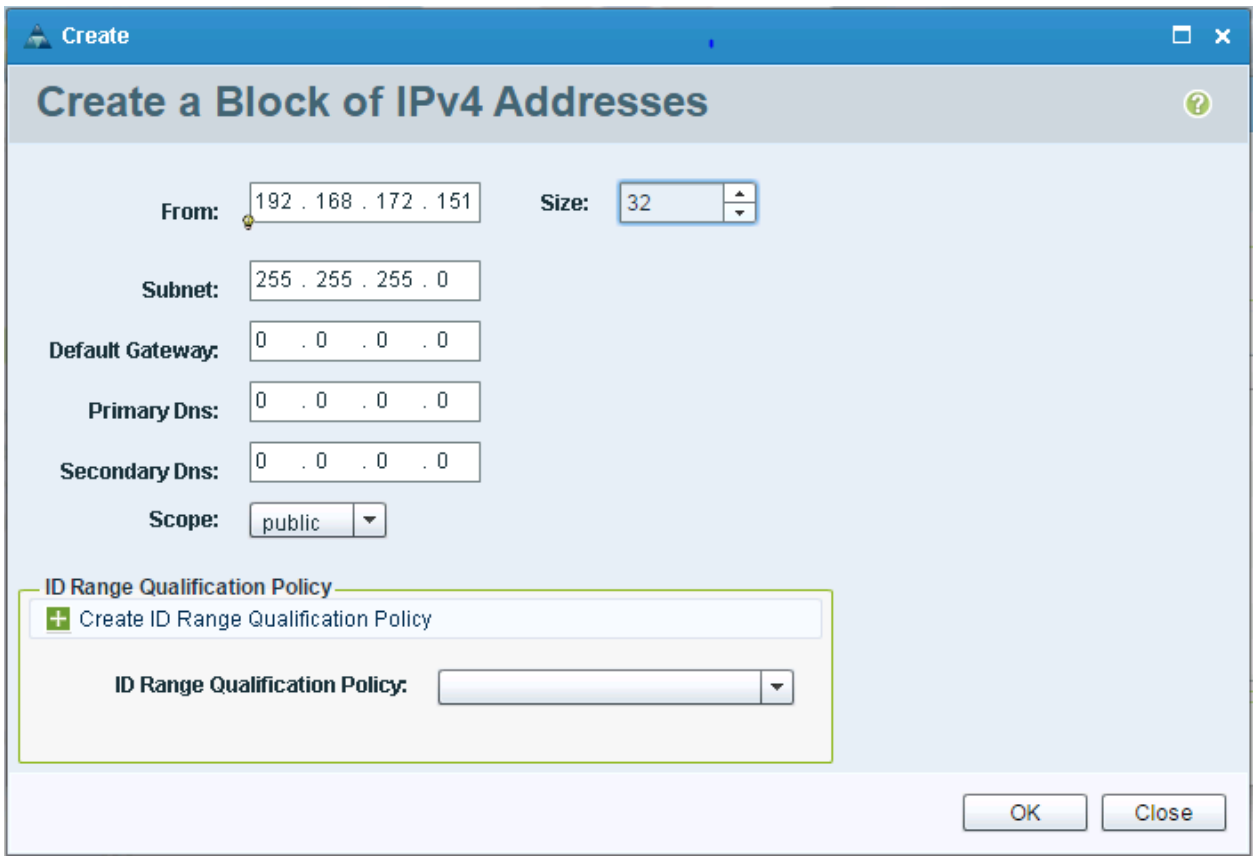
To configure the necessary IQN pools for the local site Cisco UCS environment, complete the following steps:

1. In Cisco UCS Central, click the Network tab.
2. Expand Network > Pools > root.
3. Right-click IP Pools.
4. Select Create IP Pool.
5. Enter `Site-XX-iSCSI_Initiator_A` as the name for the IP pool.
6. Optional: Add a description for the IP pool.
7. Select the IP Blocks tab.
8. Click Create a Block of IPv4 Addresses.

9. Enter a starting IP address in the subnet from the site iSCSI A VLAN
10. Enter a size appropriate to your environment
11. Enter the appropriate subnet mask



12. Click OK.
13. In the Create window, click OK to complete creating the IP pool.
14. Right-click IP Pools.
15. Select Create IP Pool.
16. Enter `Site-XX-iSCSI_Initiator_B` as the name for IP pool.
17. Select the IP Blocks tab.
18. Click Create a Block of IPv4 Addresses.
19. Enter a starting IP address in the subnet from the iSCSI B VLAN
20. Enter a size appropriate to your environment
21. Enter the appropriate subnet mask



22. Click OK.

23. In the Create window, click OK to complete creating the IP pool.

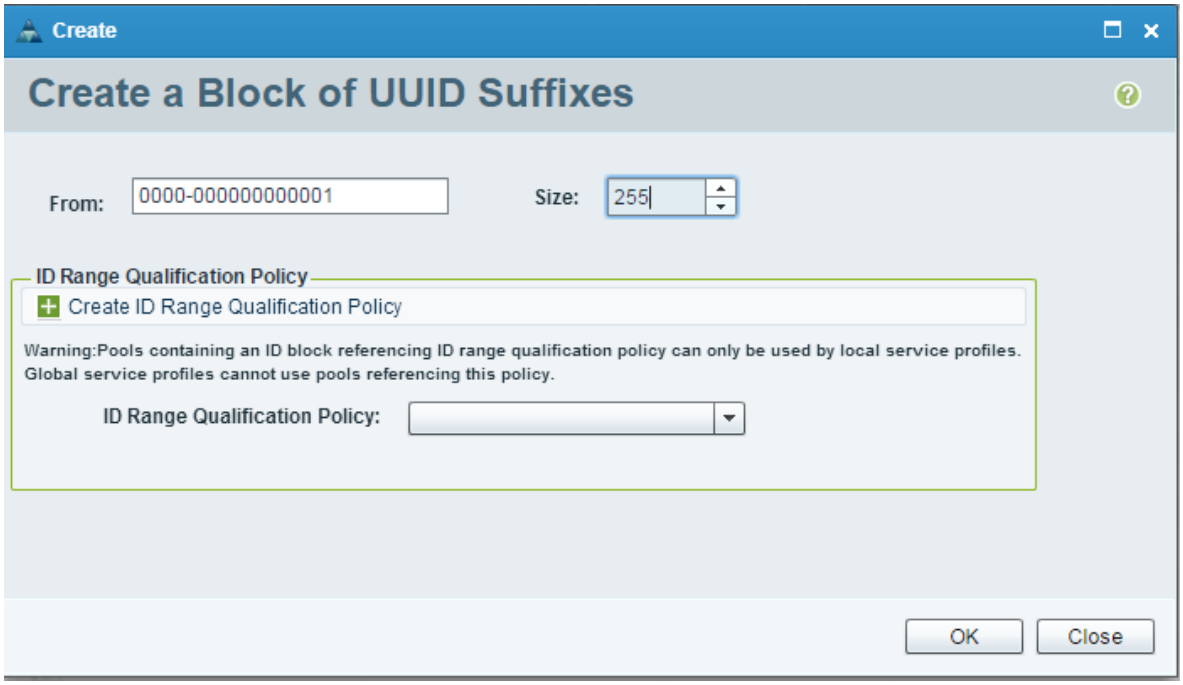
Create UUID Suffix Pool

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

> Note: In this procedure, one large UUID Pool is created to cover all sites managed by UCS Central. Note that site-based UUID Pools can also be created.

1. In Cisco UCS Central, click the Servers tab.
2. Expand Servers > 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 the UUID Blocks tab.
9. Click Create a Block of UUID Suffixes
10. Leave the default setting in the From field.
11. Specify a size for the UUID block that is sufficient to support the available blade or server resources at all sites managed by UCS Central.



12. Click OK.
13. Click OK.

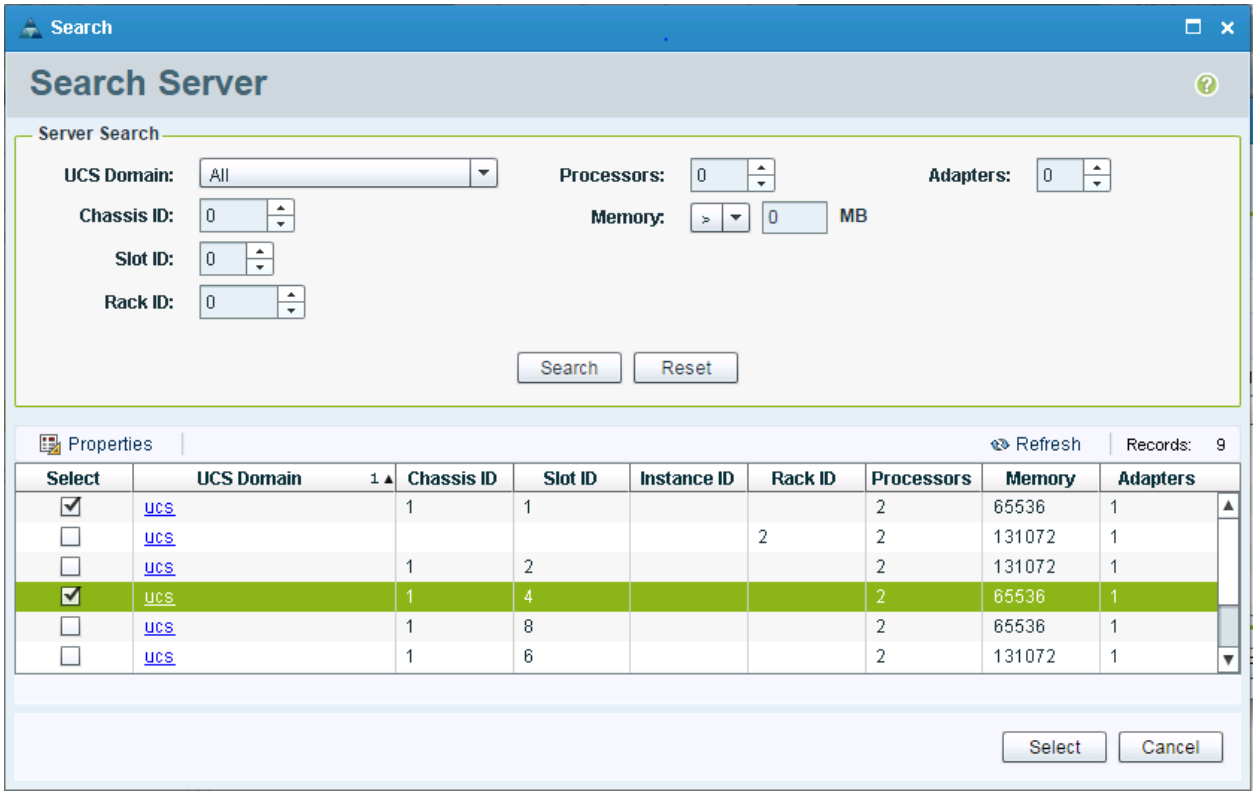
Create Server Pool

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 Central, click the Servers tab.
2. Expand Servers < Pools< root.
3. Right-click Server Pools.
4. Select Create Server Pool.
5. Enter `Site-XX-Infra-Pool` as the name for the server pool.

6. Optional: Enter a description for the server pool.
7. Click Next.
8. Select Search Server < Search
9. Select two servers from the appropriate UCS Domain to be used for the infrastructure servers at the remote site.



10. Click Select.
11. Click Finish.

Create VLANs

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

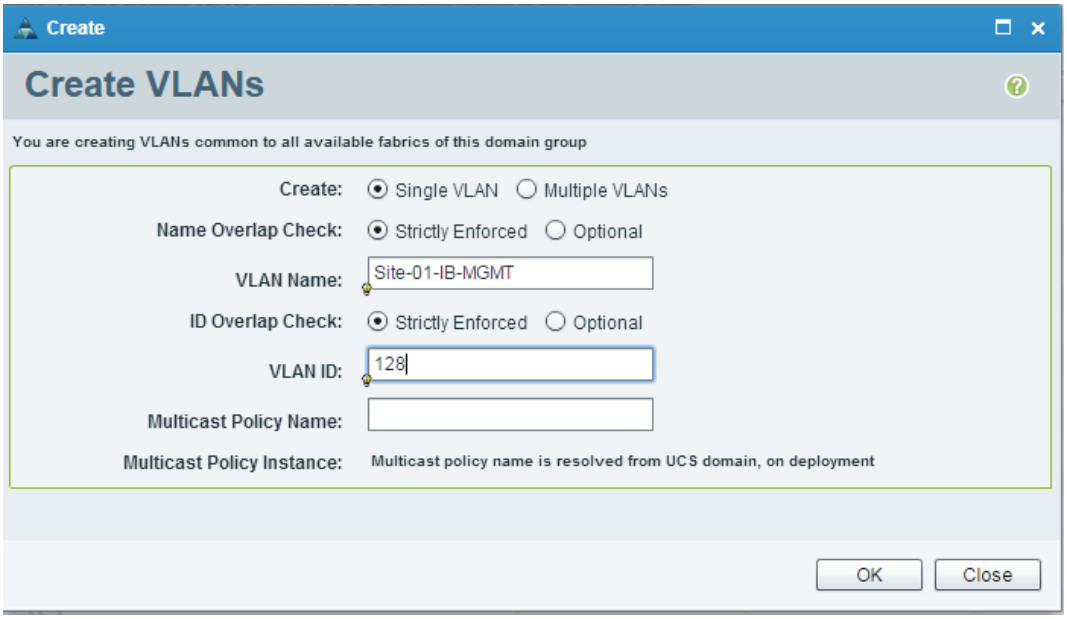
Note: In this procedure, a unique set of VLANs is created at each remote site. To create VLANs that appear in all sites, place them in Domain Group root.

1. In Cisco UCS Central, click the Network tab.
2. In the left pane, expand Network > Domain Groups> Domain Group root > Domain Group Site-XX > LAN.
3. Select LAN Cloud under Domain Group Site-XX.

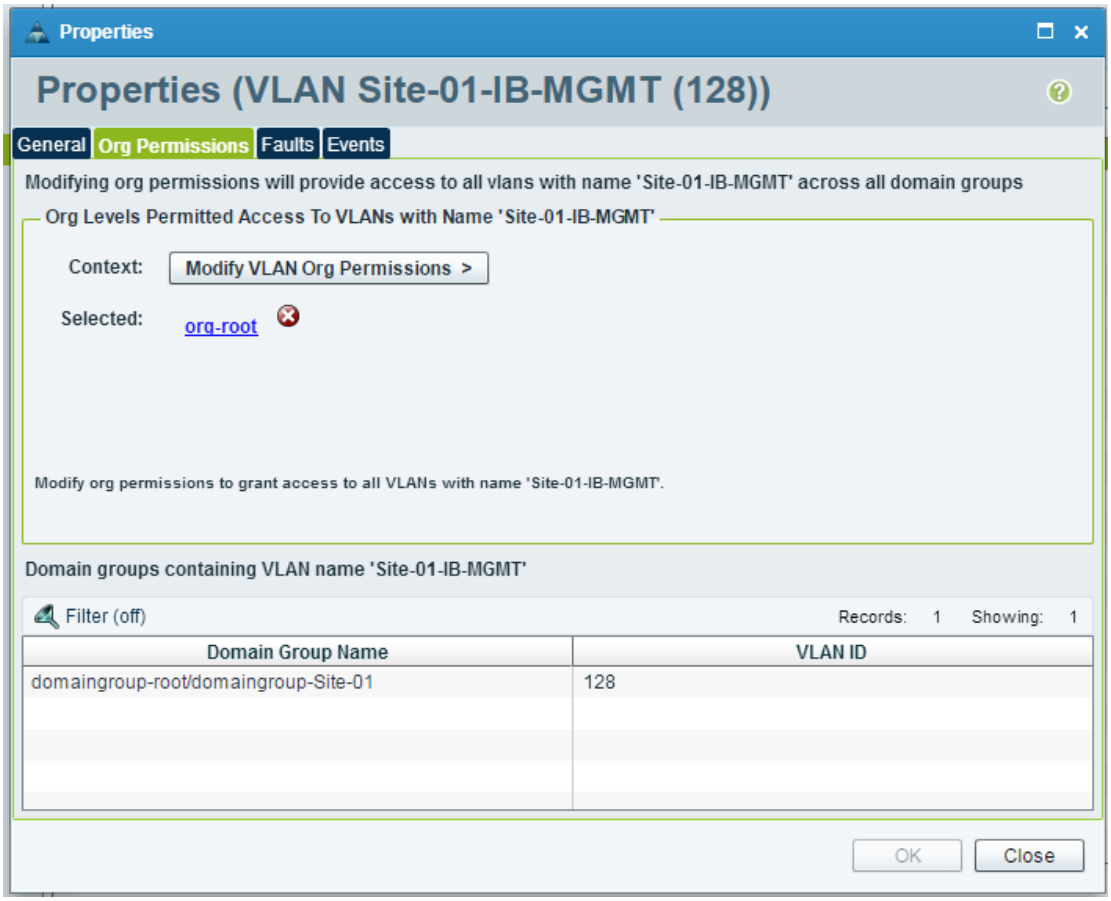
4. In the right pane, click Create VLANs.

Note: In this procedure, seven VLANs are created.

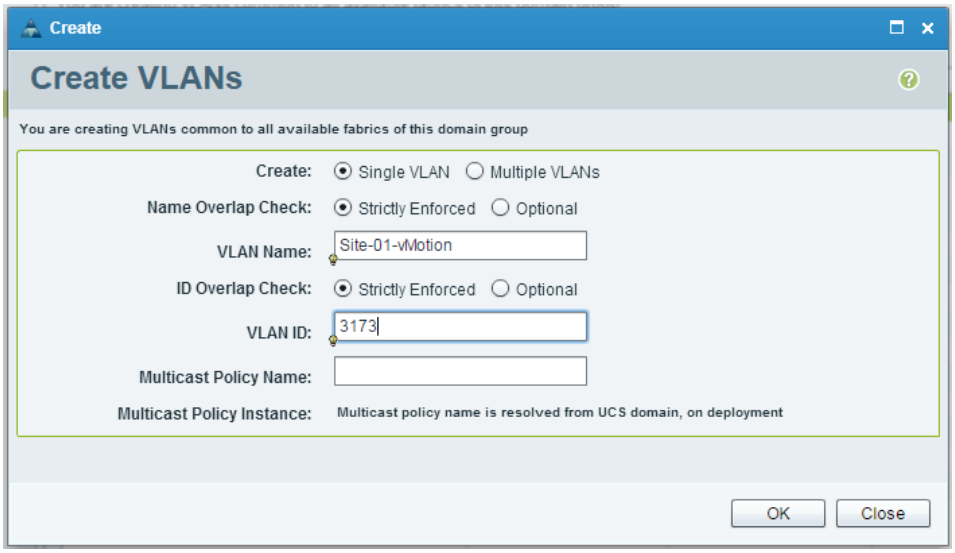
5. Select Single VLAN in the create option.
6. Select Strictly Enforced in the Name Overlap check.
7. Enter `Site-XX-IB-MGMT` as the name for VLAN to be used for management traffic.
8. Select Strictly enforced as the ID Overlap check
9. Enter `<<var_ib-mgmt_vlan_id>>` as the ID of the management VLAN.



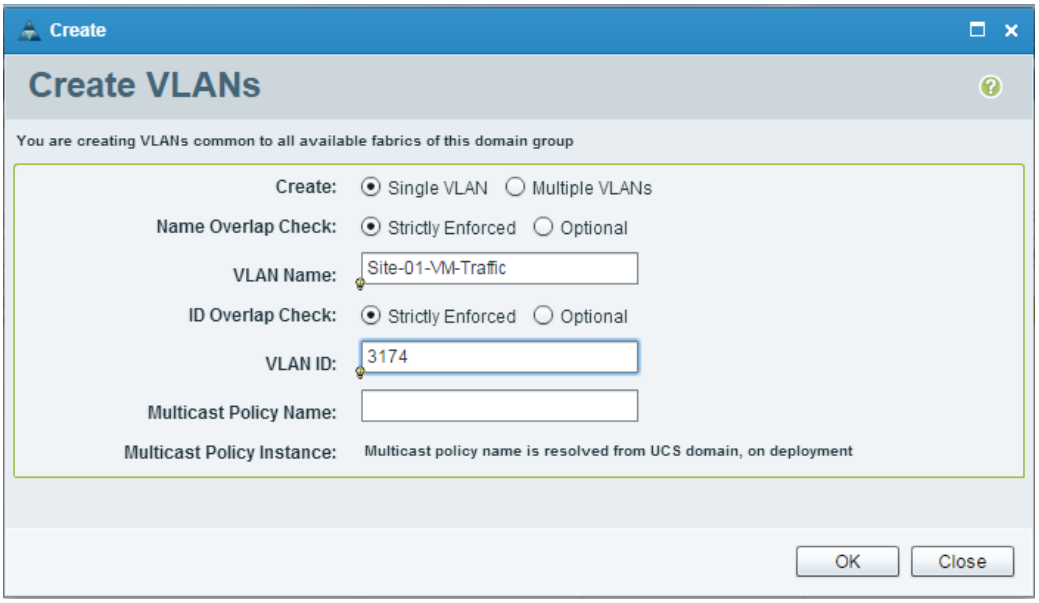
10. Click OK.
11. In the right pane, select the Site-XX-IB-MGMT VLAN just created, and click Properties.
12. Click the Org Permissions tab and select the Modify VLAN Org Permissions button.
13. Select the checkbox for the root organization.
14. Select the Modify VLAN Org Permissions button again.
15. Click OK.



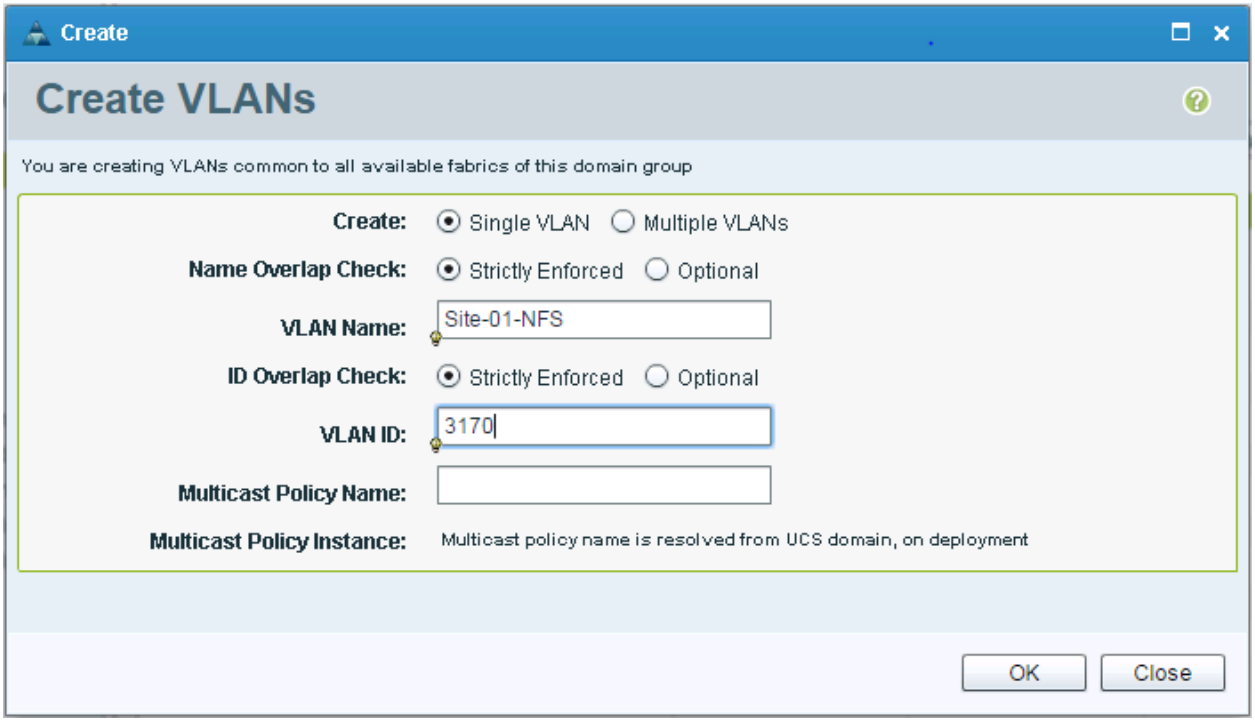
16. In the right pane, click Create VLANs.
17. Select Single VLAN in the create option.
18. Select Strictly Enforced in the Name Overlap check.
19. Enter `Site-XX-vMotion` as the name for the VLAN to be used for vMotion.
20. Select Strictly enforced as the ID Overlap check
21. Enter the `<<var_vmotion_vlan_id>>` as the ID of the vMotion VLAN.



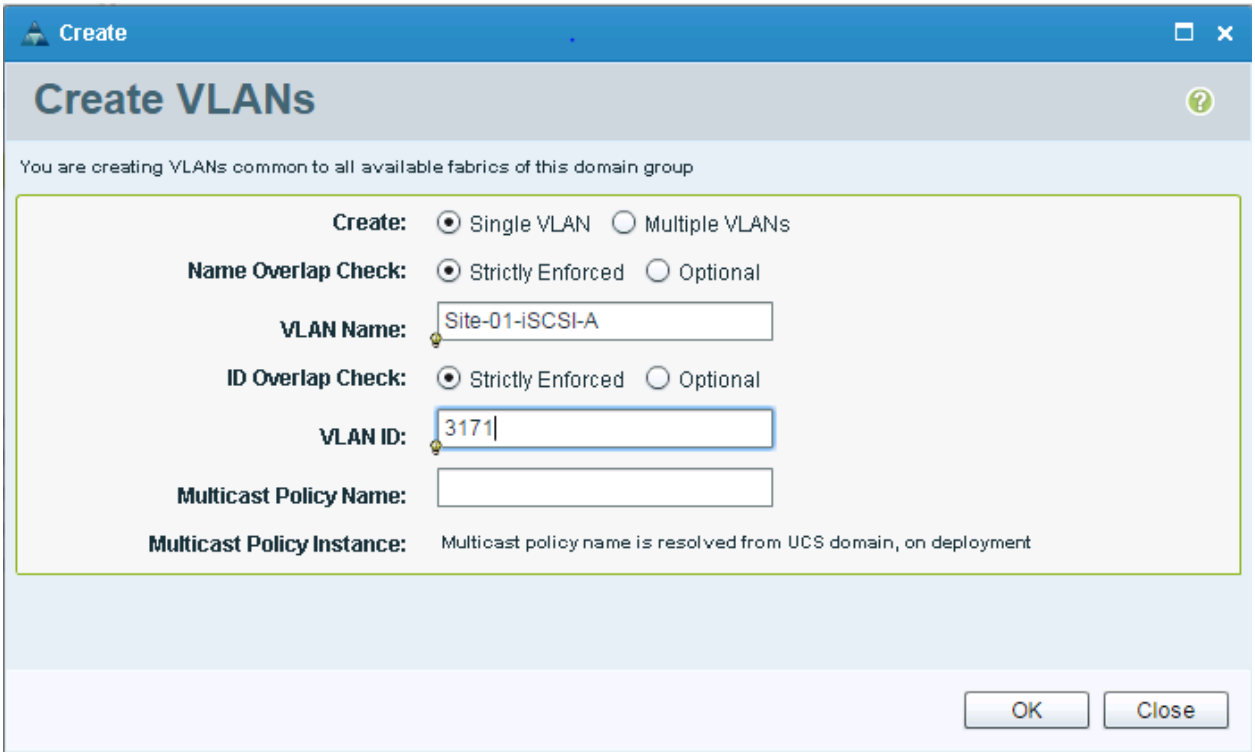
22. Click OK,
23. In the right pane, select the Site-XX-vMotion VLAN just created, and click Properties.
24. Click the Org Permissions tab and select the Modify VLAN Org Permissions button.
25. Select the checkbox for the root organization.
26. Select the Modify VLAN Org Permissions button again.
27. Click OK.
28. In the right pane, click Create VLANs
29. Select Single VLAN in the create option
30. Select Strictly Enforced in the Name Overlap check
31. Enter `Site-XX-VM-Traffic` as the name for the VLAN to be used for the VM traffic.
32. Select Strictly enforced as the ID Overlap check
33. Enter the `<<var_vm-traffic_vlan_id>>` for the VM Traffic VLAN.



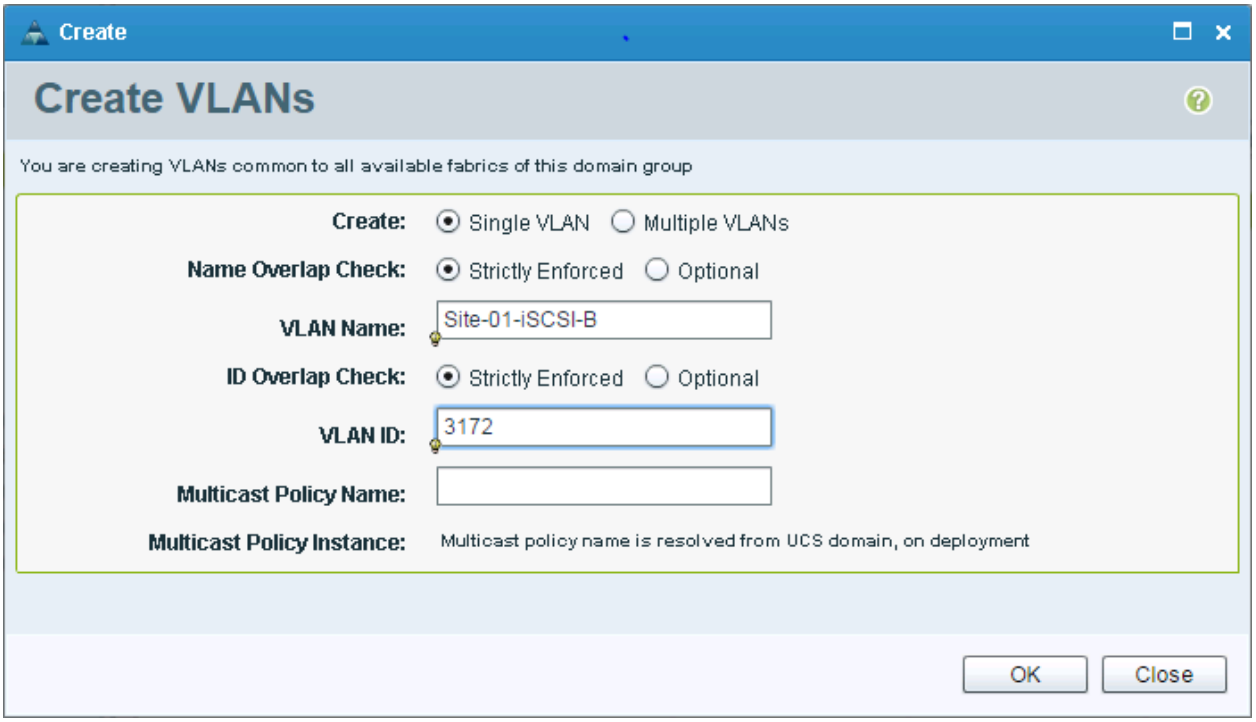
34. Click OK
35. In the right pane, select the Site-XX-VM-Traffic VLAN just created, and click Properties.
36. Click the Org Permissions tab and select the Modify VLAN Org Permissions button.
37. Select the checkbox for the root organization.
38. Select the Modify VLAN Org Permissions button again.
39. Click OK.
40. In the right pane, click Create VLANs.
41. Select Single VLAN in the create option.
42. Select Strictly Enforced in the Name Overlap check.
43. Enter `Site-XX-NFS` as the name for VLAN to be used for management traffic.
44. Select Strictly enforced as the ID Overlap check
45. Enter `<<var_nfs_vlan_id>>` as the ID of the NFS VLAN.



46. Click OK.
47. In the right pane, select the Site-XX-NFS VLAN just created, and click Properties.
48. Click the Org Permissions tab and select the Modify VLAN Org Permissions button.
49. Select the checkbox for the root organization.
50. Select the Modify VLAN Org Permissions button again.
51. Click OK.
52. In the right pane, click Create VLANs.
53. Select Single VLAN in the create option.
54. Select Strictly Enforced in the Name Overlap check.
55. Enter `Site-XX-iSCSI-A` as the name for the VLAN to be used for iSCSI for Fabric A.
56. Select Strictly enforced as the ID Overlap check
57. Enter the `<<var_iscsi-a_vlan_id>>` as the ID of the iSCSI-A VLAN.



58. Click OK,
59. In the right pane, select the Site-XX-iSCSI-A VLAN just created, and click Properties.
60. Click the Org Permissions tab and select the Modify VLAN Org Permissions button.
61. Select the checkbox for the root organization.
62. Select the Modify VLAN Org Permissions button again.
63. Click OK.
64. In the right pane, click Create VLANs
65. Select Single VLAN in the create option
66. Select Strictly Enforced in the Name Overlap check
67. Enter `Site-XX-iSCSI-B` as the name for the VLAN to be used for iSCSI for Fabric B.
68. Select Strictly enforced as the ID Overlap check
69. Enter the `<<var_iscsi-b_vlan_id>>` for the iSCSI-B VLAN.



70. Click OK

71. In the right pane, select the Site-XX-iSCSI-B VLAN just created, and click Properties.

72. Click the Org Permissions tab and select the Modify VLAN Org Permissions button.

73. Select the checkbox for the root organization.

74. Select the Modify VLAN Org Permissions button again.

75. Click OK.

76. In the right pane, click Create VLANs

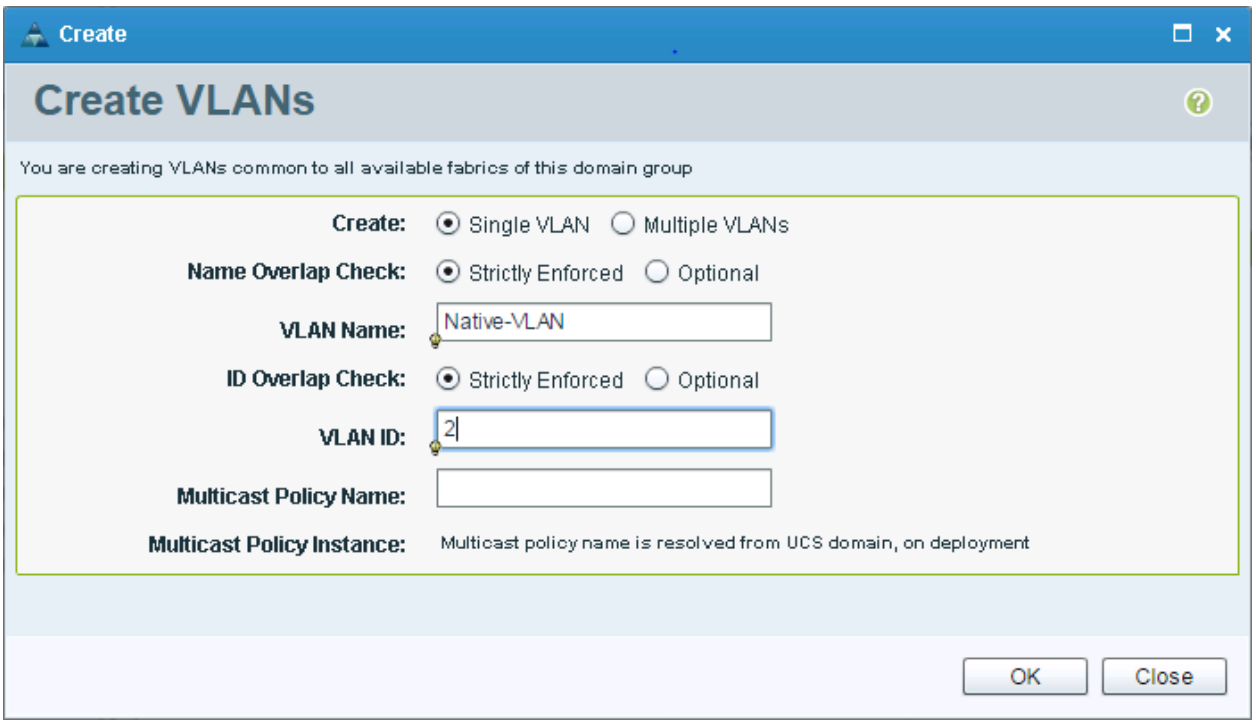
77. Select Single VLAN in the create option

78. Select Strictly Enforced in the Name Overlap check

79. Enter `Native-VLAN` as the name for the VLAN to be used as the native VLAN.

80. Select Strictly enforced as the ID Overlap check

81. Enter the `<<var_native_vlan_id>>` as the ID for the native VLAN.



82. Click OK

83. In the right pane, select the Native-VLAN just created, and click Properties.

84. Click the Org Permissions tab and select the Modify VLAN Org Permissions button.

85. Select the checkbox for the root organization.

86. Select the Modify VLAN Org Permissions button again.

87. Click OK.

Create Local Disk Configuration Policy (Optional)

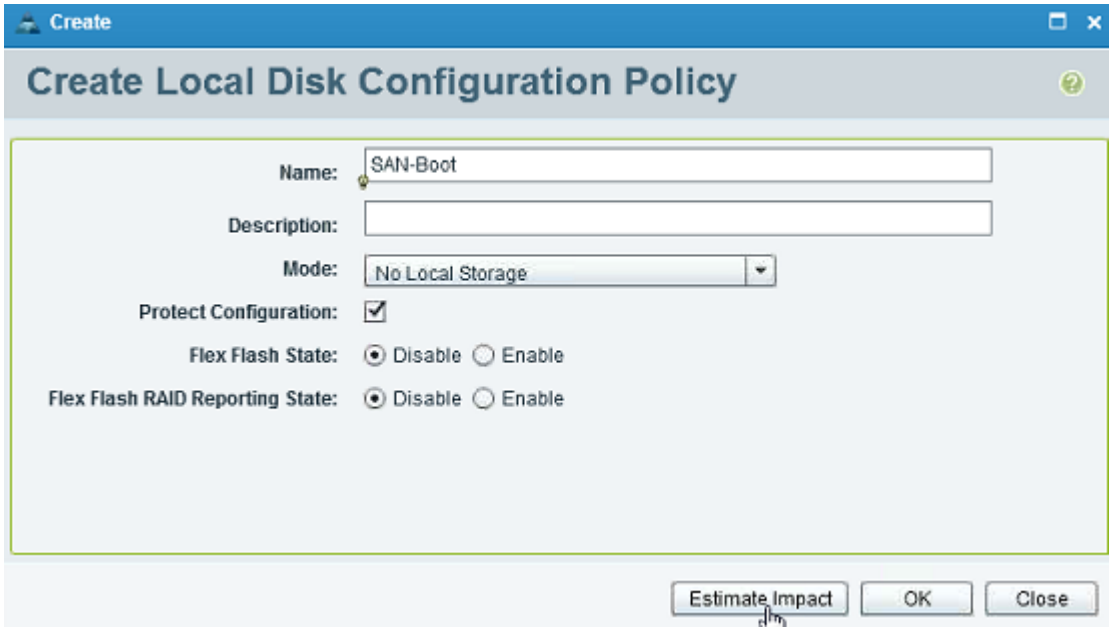
A local disk configuration for the Cisco UCS environment is necessary if the servers in the environment do not have a local disk.

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 Central, click the Servers tab.
2. Expand Servers > 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.

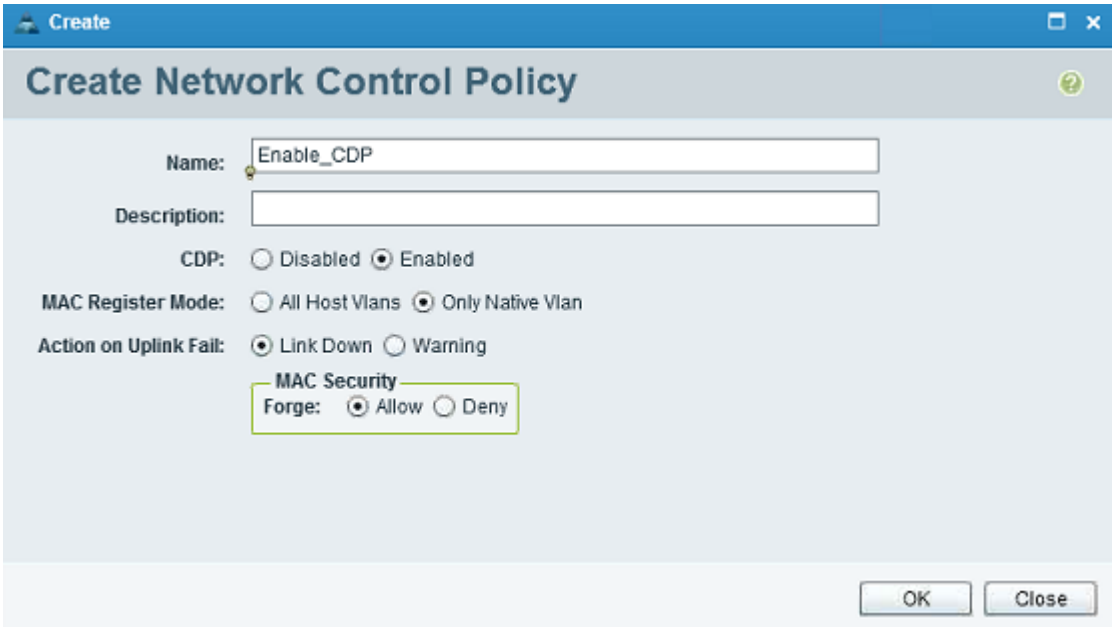


8. Click OK to create the Local Disk Configuration Policy.

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 Central, click the Network tab.
2. Expand Network > 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.

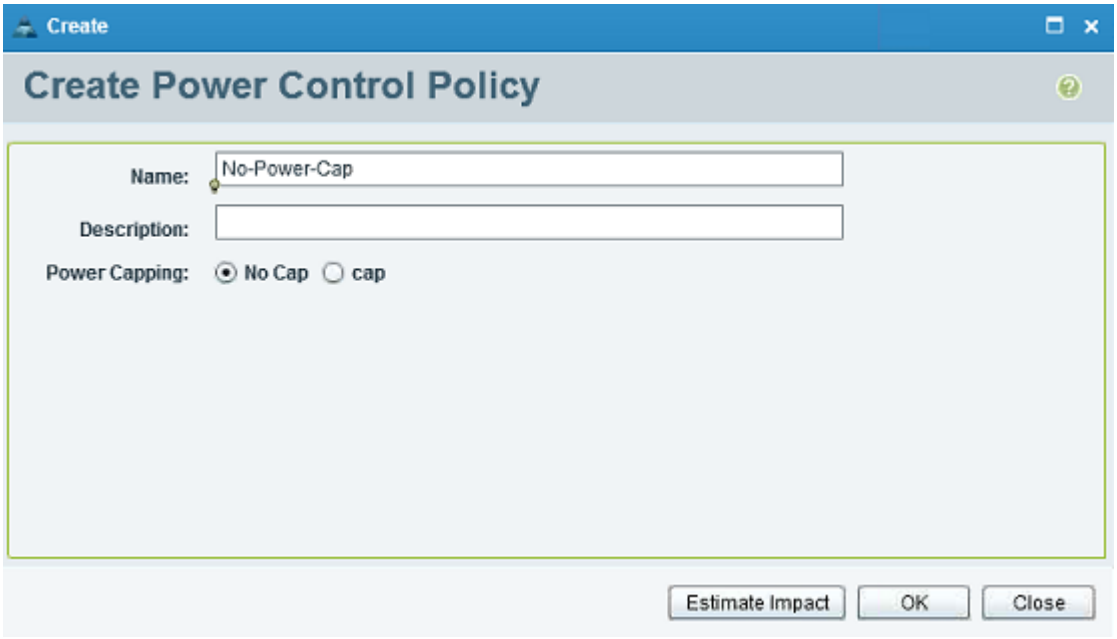


7. Click OK to create the network control policy.

Create Power Control Policy

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

1. In Cisco UCS Central, click the Servers tab.
2. Expand Servers > 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.



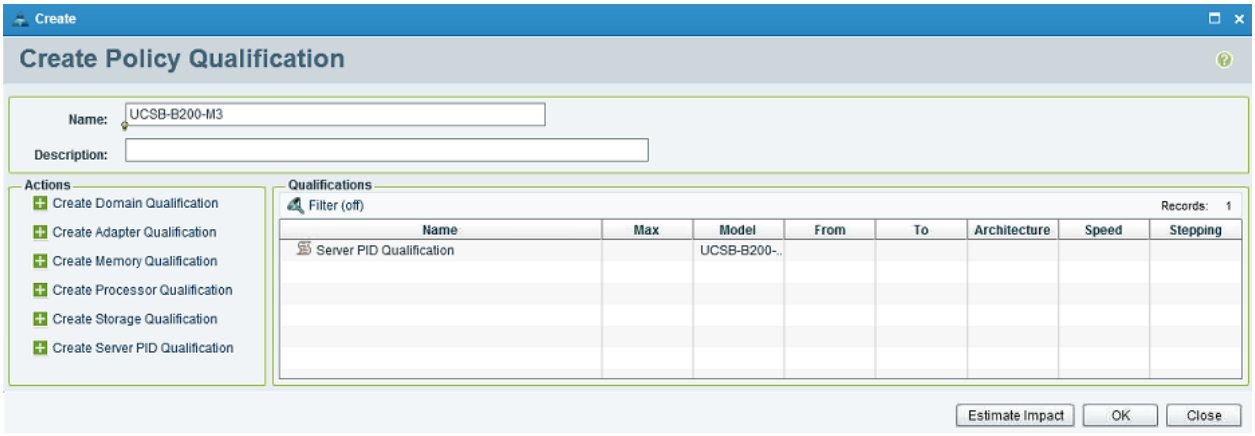
7. Click OK to create the power control policy.

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 B200-M4 server.

1. In Cisco UCS Central, click the Servers tab.
2. Expand Servers > Policies > root.
3. Right-click Server Pool Policy Qualifications.
4. Select Create Policy Qualification.
5. Enter `UCSB-B200-M4` as the name for the policy.
6. In the left pane, under Actions Select Create Server PID Qualification.
7. Enter `UCSB-B200-M4` as the PID.
8. Click OK to create the Server PID Qualification.

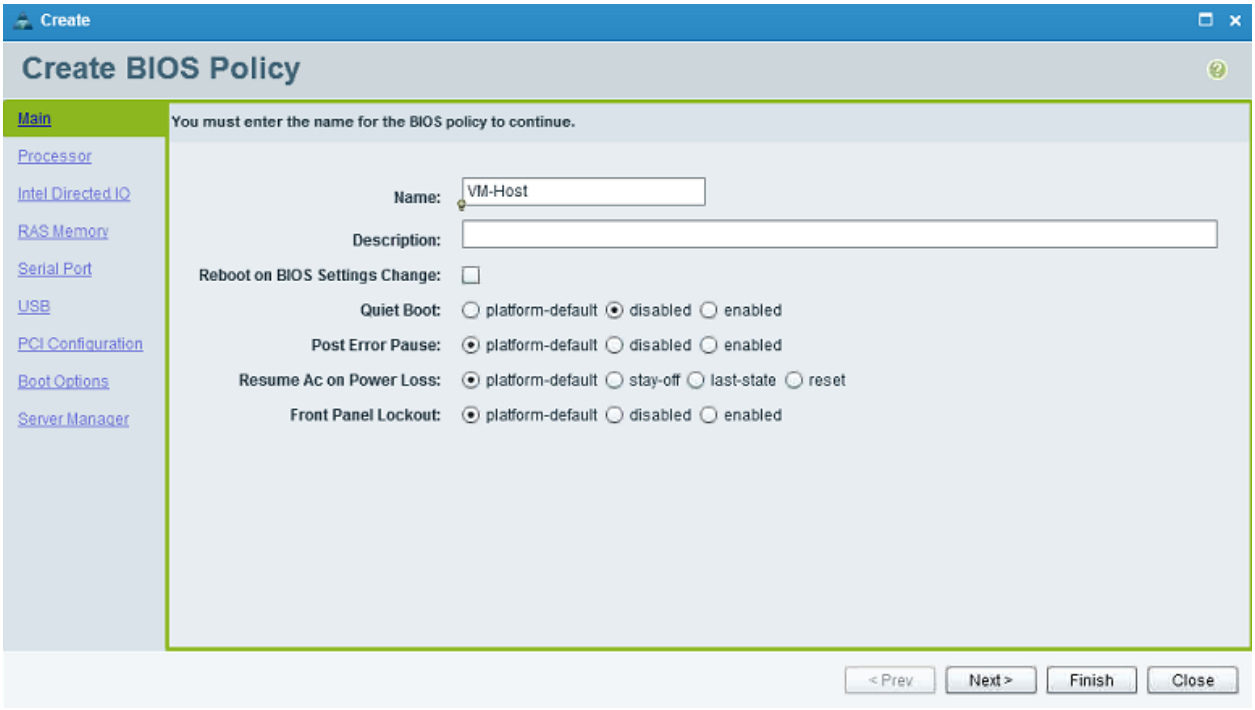


9. Click OK to create the policy.

Create Server BIOS Policy

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

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

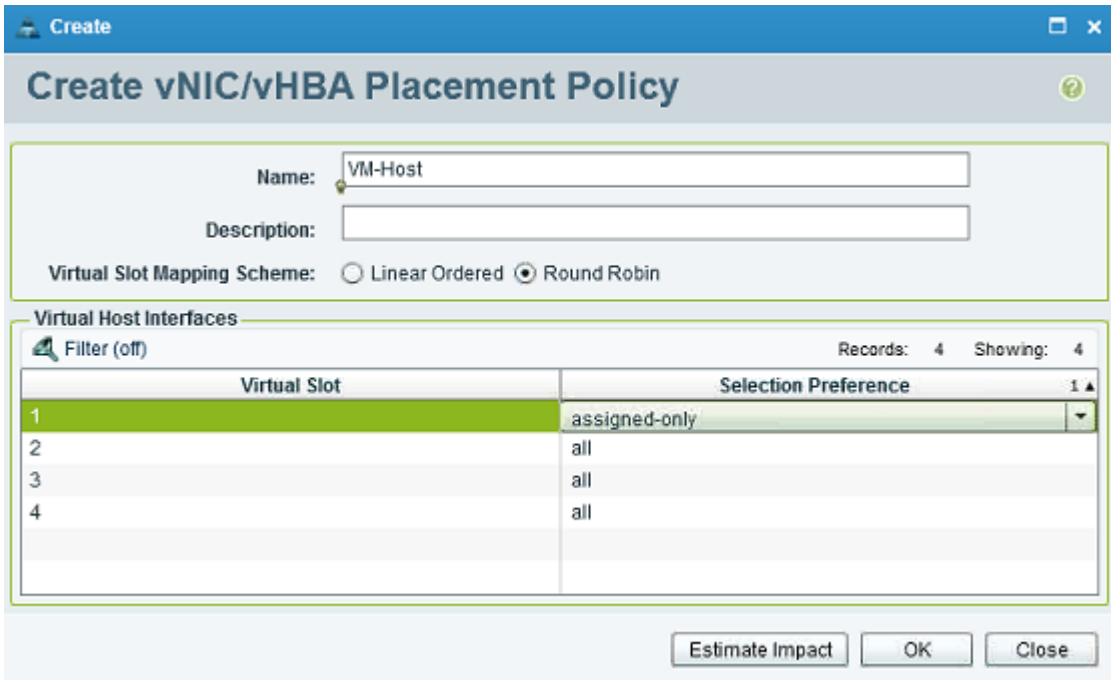


7. Click Finish to create the BIOS policy.

Create vNIC/vHBA Placement Policy for Virtual Machine Hosts

To create a vNIC/vHBA placement policy for the VM hosts, complete the following steps:

1. In Cisco UCS Central, click the Servers tab.
2. Expand Servers > Policies > root.
3. Right-click vNIC/vHBA Placement Policies.
4. Select Create vNIC/vHBA Placement Policy.
5. Enter `VM-Host` as the name for the placement policy.
6. Click Virtual Slot 1 and under the Selection Preference select assigned-only.



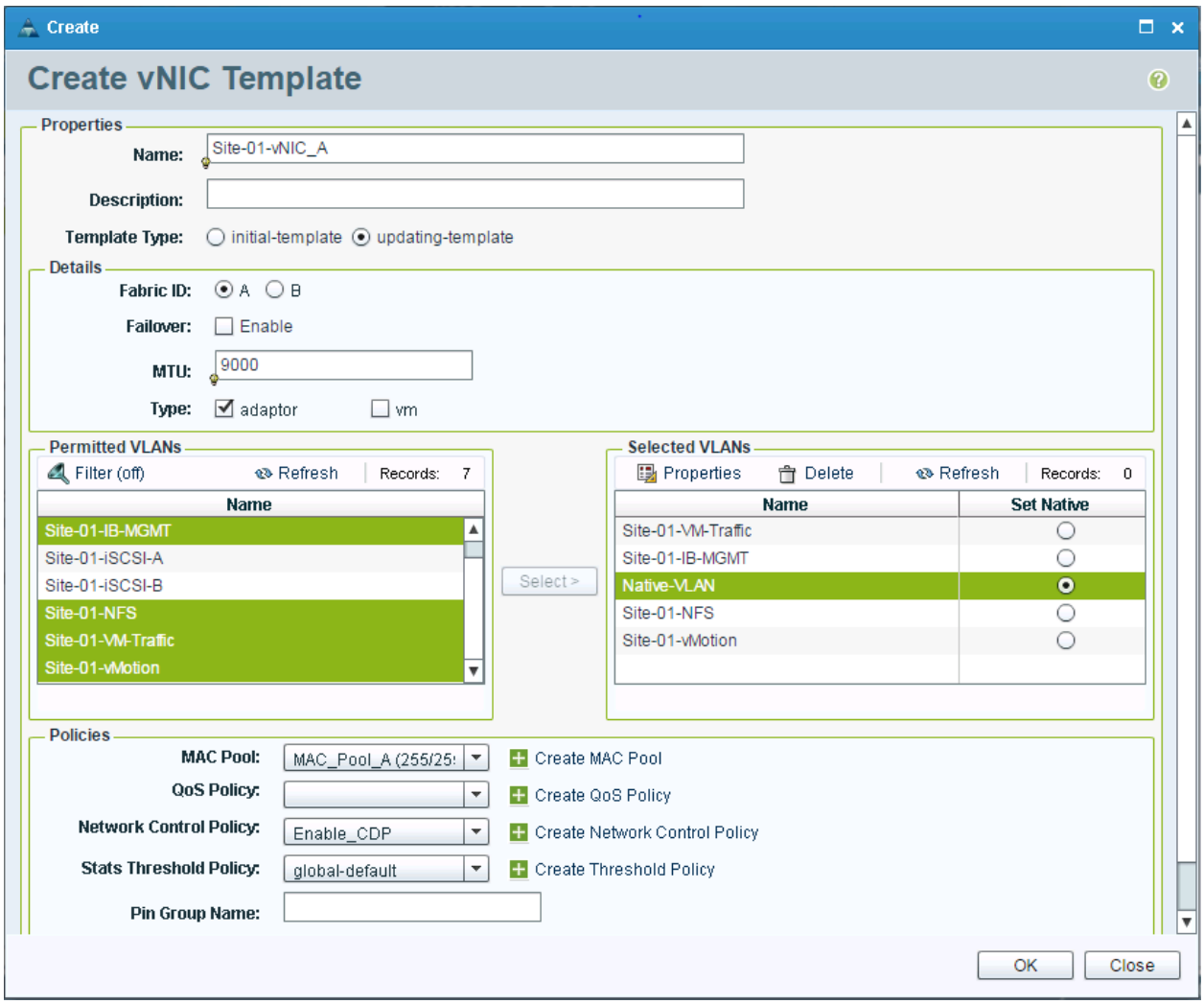
7. Click OK.

Create vNIC Templates

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

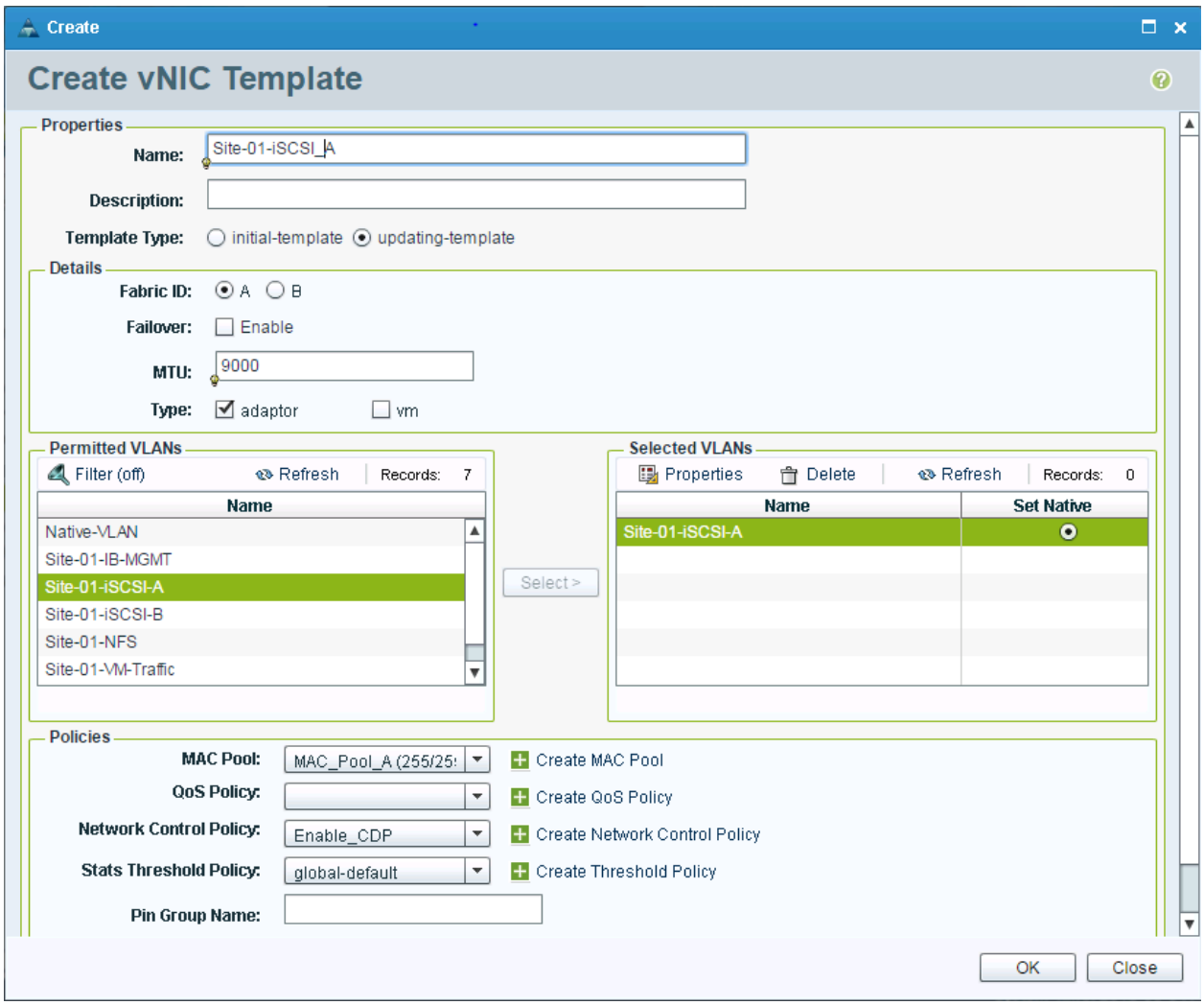
1. In Cisco UCS Central, click the Network tab.
2. Expand Network > Policies > root.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.

5. Enter `Site-XX-vNIC_A` as the vNIC template name.
6. Select updating-template as the Template Type.
7. For Fabric ID, select Fabric A.
8. Do not select the Enable Failover checkbox.
9. For MTU, enter `9000`.
10. Under Type, ensure adaptor is selected.
11. Under Permitted VLANs, select `Native-VLAN`, `Site-XX-IB-MGMT`, `Site-XX-NFS`, `Site-XX-VM-Traffic`, and `Site-XX-vMotion`. Use the Ctrl key to make this multiple selection.
12. Click Select. These VLANs should now appear under Selected VLANs.
13. Set `Native-VLAN` as the native VLAN.
14. In the MAC Pool list, select `MAC_Pool_A`.
15. In the Network Control Policy list, select `Enable_CDP`.



16. Click OK to create the vNIC template.
17. Back in UCS Central, right-click vNIC Templates.
18. Select Create vNIC Template.
19. Enter `Site-XX-vNIC_B` as the vNIC template name.
20. Select updating-template as the Template Type.
21. For Fabric ID, select Fabric B.
22. Do not select the Enable Failover checkbox.
23. For MTU, enter `9000`.
24. Under Type, ensure adaptor is selected.
25. Under Permitted VLANs, select `Native-VLAN`, `Site-XX-IB-MGMT`, `Site-XX-NFS`, `Site-XX-VM-Traffic`, and `Site-XX-vMotion`. Use the Ctrl key to make this multiple selection.

26. Click Select. These VLANs should now appear under Selected VLANs.
27. Set `Native-VLAN` as the native VLAN.
28. In the MAC Pool list, select `MAC_Pool_B`
29. In the Network Control Policy list, select `Enable_CDP`.
30. Click OK.
31. Right-click vNIC Templates.
32. Select Create vNIC Template.
33. Enter `Site-XX-iSCSI_A` as the vNIC template name.
34. Select updating-template as the Template Type.
35. For Fabric ID, select Fabric A.
36. Do not select the Enable Failover checkbox.
37. For MTU, enter `9000`.
38. Under Type, ensure adaptor is selected.
39. Under Permitted VLANs, select `Site-XX-iSCSI-A`.
40. Click Select. This VLAN should now appear under Selected VLANs.
41. Set `Site-XX-iSCSI-A` as the native VLAN.
42. In the MAC Pool list, select `MAC_Pool_A`.
43. In the Network Control Policy list, select `Enable_CDP`.



44. Click OK to create the vNIC template.

45. Back in UCS Central, right-click vNIC Templates.

46. Select Create vNIC Template.

47. Enter `Site-XX-iSCSI_B` as the vNIC template name.

48. Select updating-template as the Template Type.

49. For Fabric ID, select Fabric B.

50. Do not select the Enable Failover checkbox.

51. For MTU, enter `9000`.

52. Under Type, ensure adaptor is selected.

53. Under Permitted VLANs, select `Site-XX-iSCSI-B`.

54. Click Select. These VLANs should now appear under Selected VLANs.

55. Set `Site-XX-iSCSI-B` as the native VLAN.

56. In the MAC Pool list, select `MAC_Pool_B`

57. In the Network Control Policy list, select `Enable_CDP`.

58. Click OK.

Create Boot Policy

This procedure applies to a Cisco UCS environment in which two iSCSI logical interfaces (LIFs) are on cluster node 1 (`iscsi_lif01a` and `iscsi_lif01b`) and two iSCSI LIFs are on cluster node 2 (`iscsi_lif02a` and `iscsi_lif02b`). Also, it is assumed that the A LIFs are connected to Fabric A (Cisco UCS 6324 A) and the B LIFs are connected to Fabric B (Cisco UCS 6324 B).

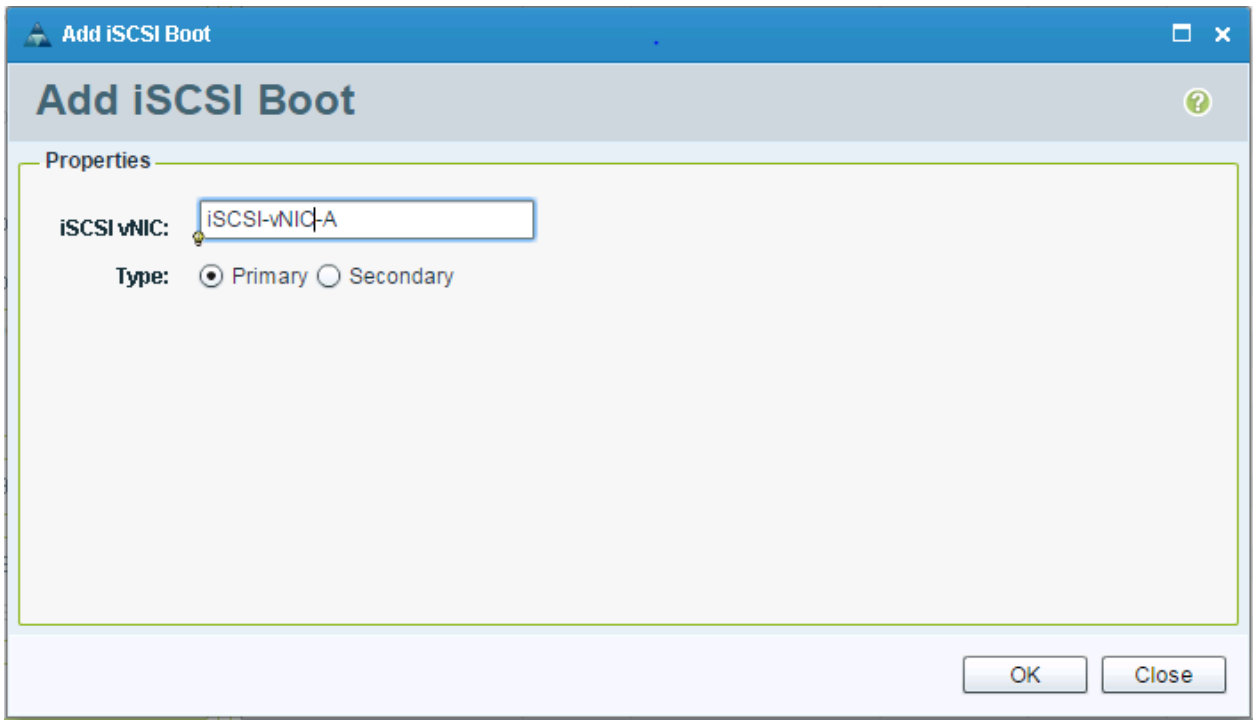
One boot policy is configured in this procedure.

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

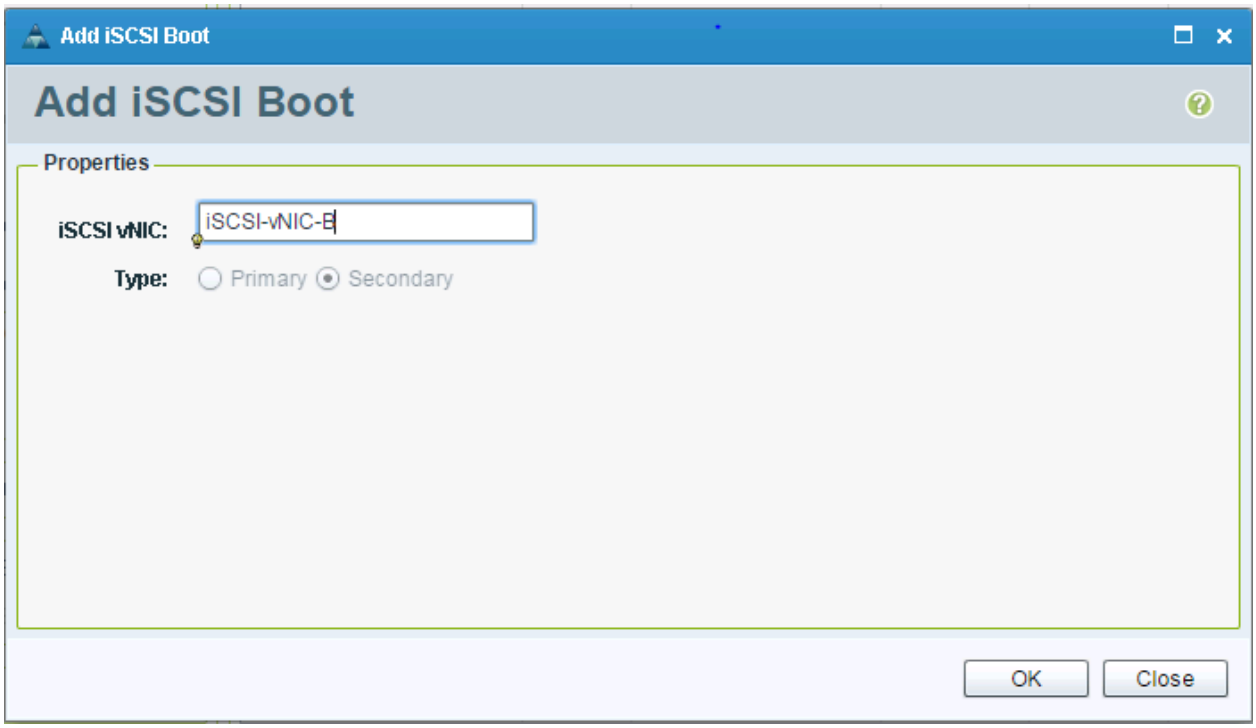
1. In Cisco UCS Central, click the Servers tab.
2. Expand Servers > Policies > root.
3. Right-click Boot Policies.
4. Select Create Boot Policy.
5. Enter `Site-XX-Fabric-A` as the name for the boot policy.
6. Optional: Enter a description for the boot policy.

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

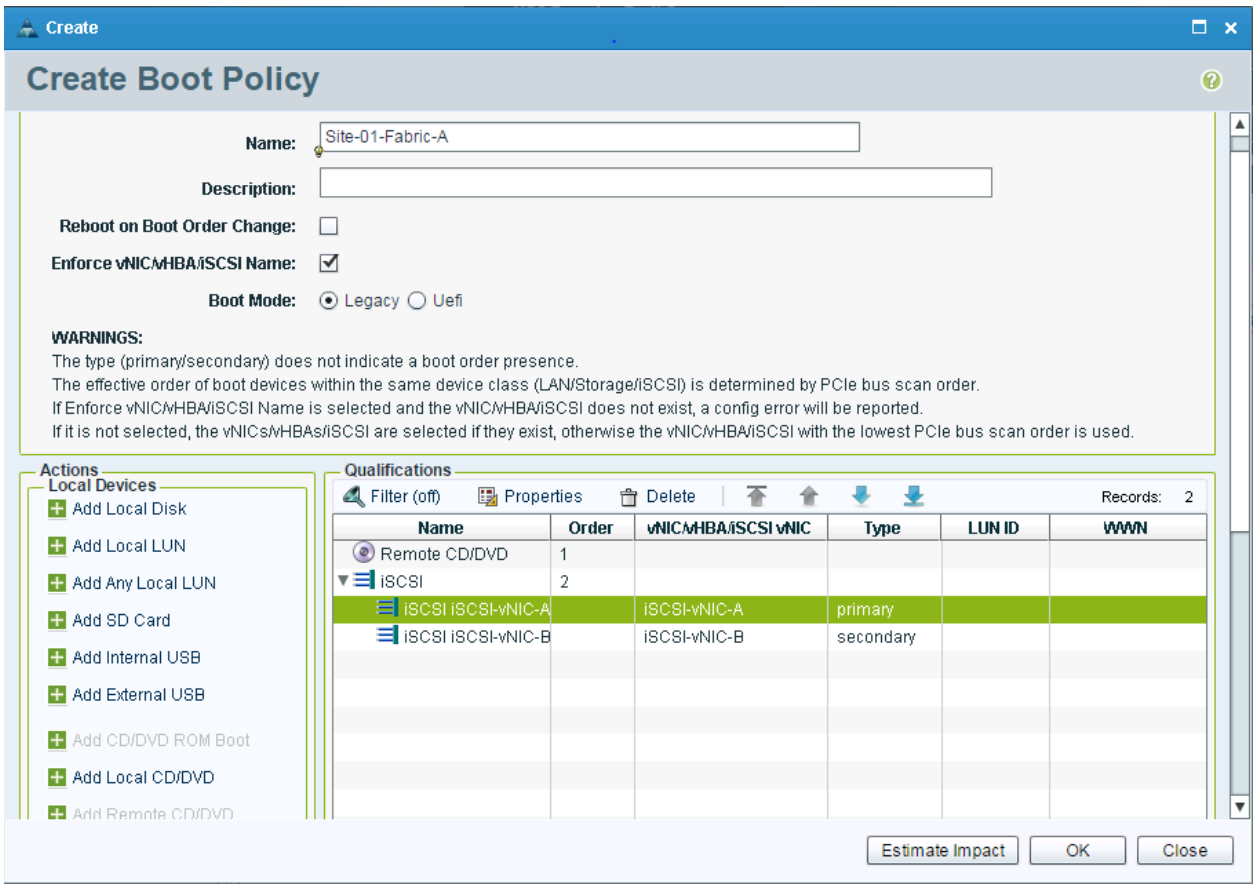
7. Leave the Boot Mode set to Legacy.
8. Select Add Remote CD/DVD.
9. Under iSCSI vNICs, select Add iSCSI Boot.
10. In the Add iSCSI Boot dialog box, enter `iSCSI-vNIC-A` in the iSCSI vNIC field.
11. Click OK.



12. Click OK to add the iSCSI boot initiator.
13. On the left, select Add iSCSI Boot.
14. In the Add SAN Boot dialog box, enter `iSCSI-vNIC-B` in the iSCSI vNIC box.



15. Click OK to add the iSCSI boot initiator.



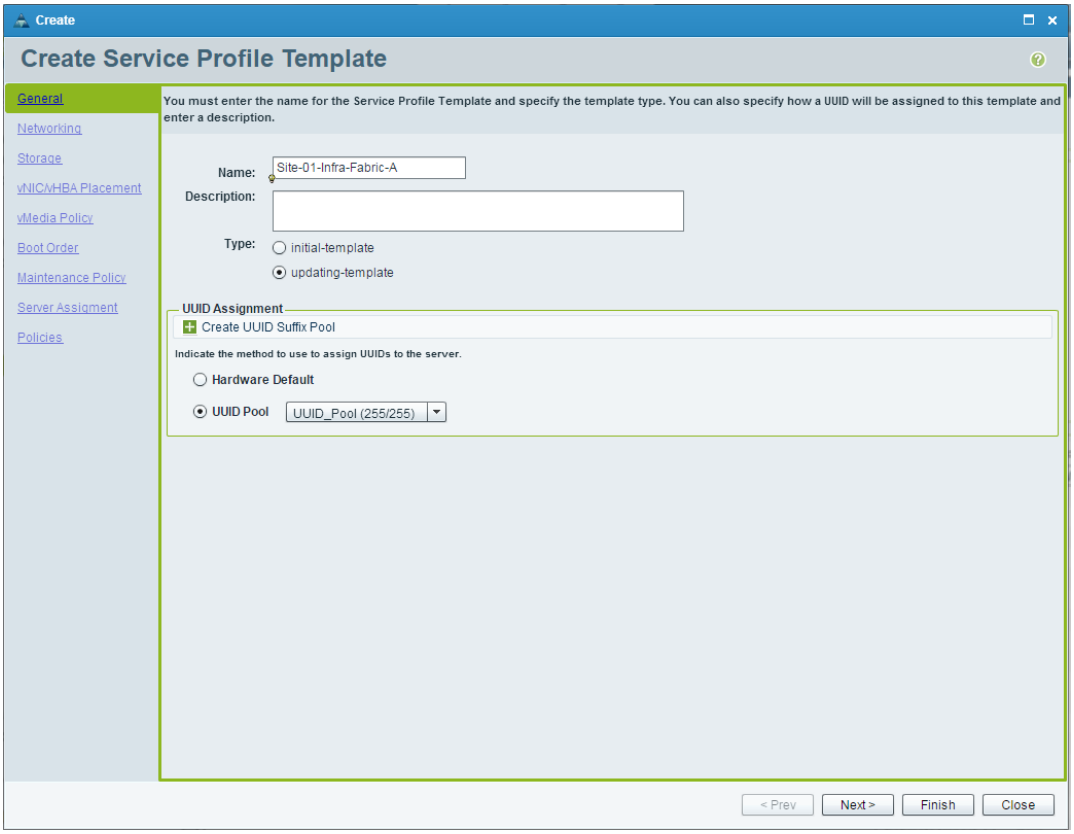
16. Click OK to create the boot policy.

Create Service Profile Template

In this procedure, a service profile template is created for the remote site.

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

1. In Cisco UCS Central, click the Servers tab.
2. Expand Servers > Global Service Profile Templates.
3. Right-click root.
4. Select Create Service Profile Template to open the Create Service Profile Template wizard.
5. Under General:
   a. Enter `Site-XX-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 mode Configuration Type to configure the LAN connectivity.

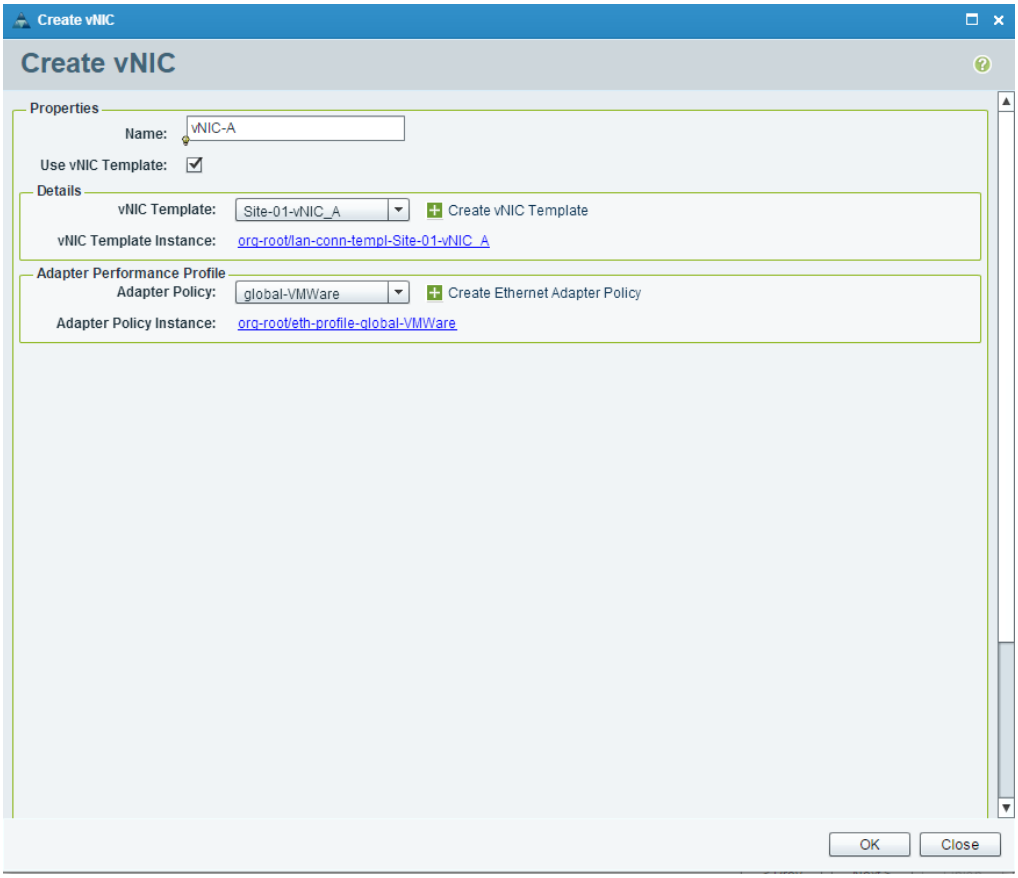
c. Click Create vNIC to add a vNIC to the template.

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 `Site-XX-vNIC_A`.

g. In the Adapter Policy list, select global-VMWare.



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

i. On the Networking page of the wizard, click Create vNIC again.

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 `Site-XX-vNIC_B`.

m. In the Adapter Policy list, select global-VMWare.

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

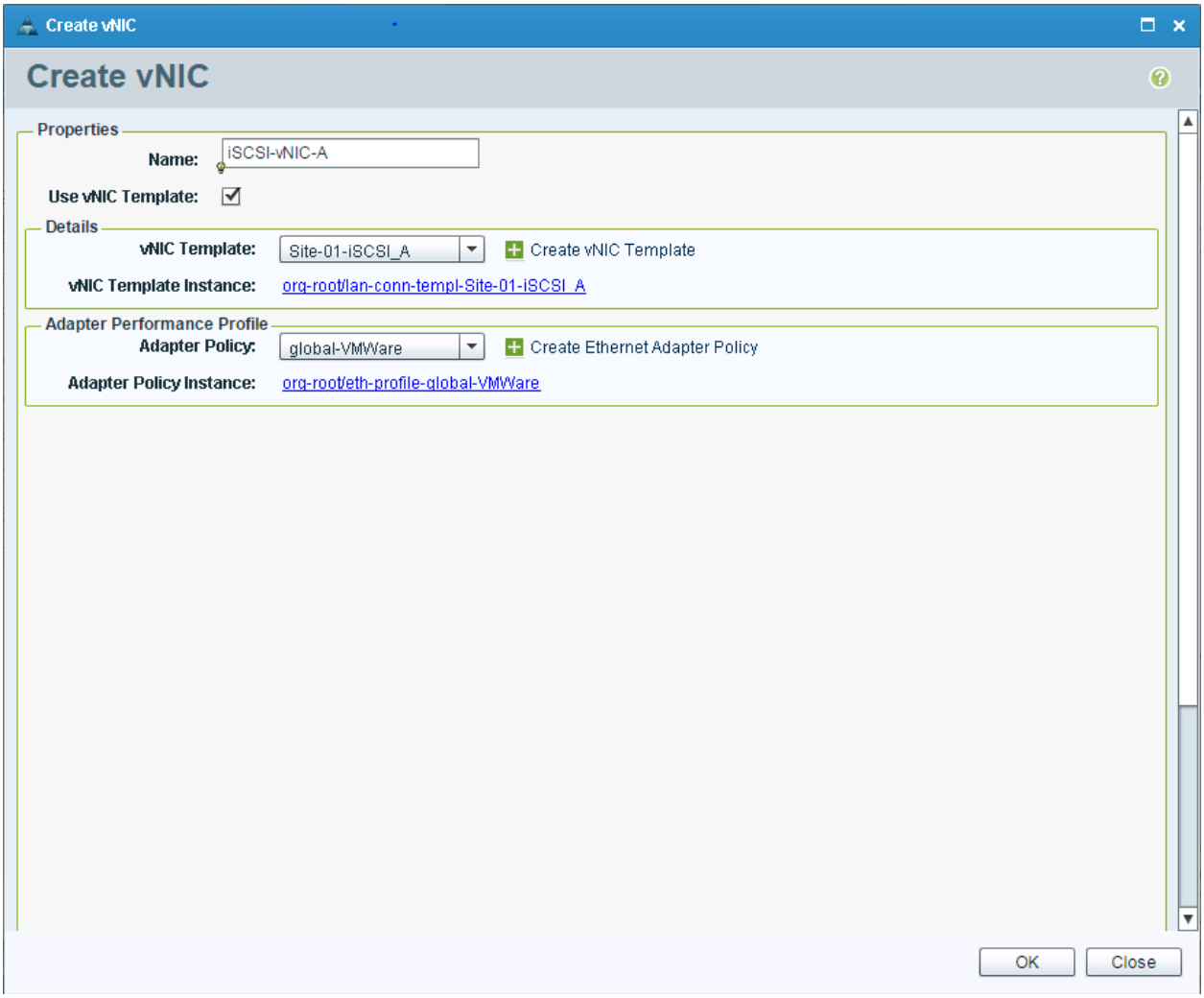
o. Click Create vNIC to add a vNIC to the template.

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

q. Select the Use vNIC Template checkbox.

r. In the vNIC Template list, select `Site-XX-iSCSI_A`.

s. In the Adapter Policy list, select global-VMWare.



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

u. On the Networking page of the wizard, click Create vNIC again.

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

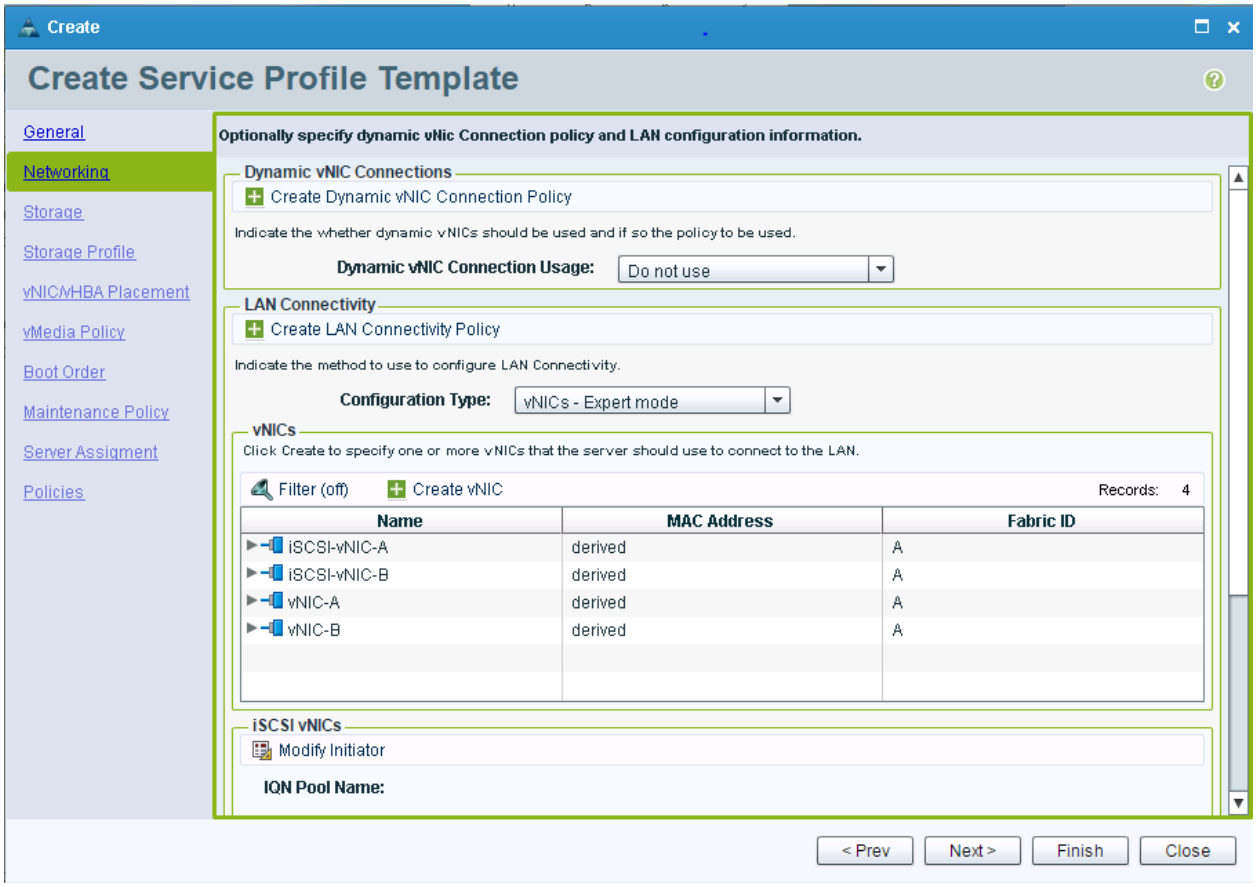
w. Select the Use vNIC Template checkbox.

x. In the vNIC Template list, select `Site-XX-iSCSI_B`.

y. In the Adapter Policy list, select global-VMWare.

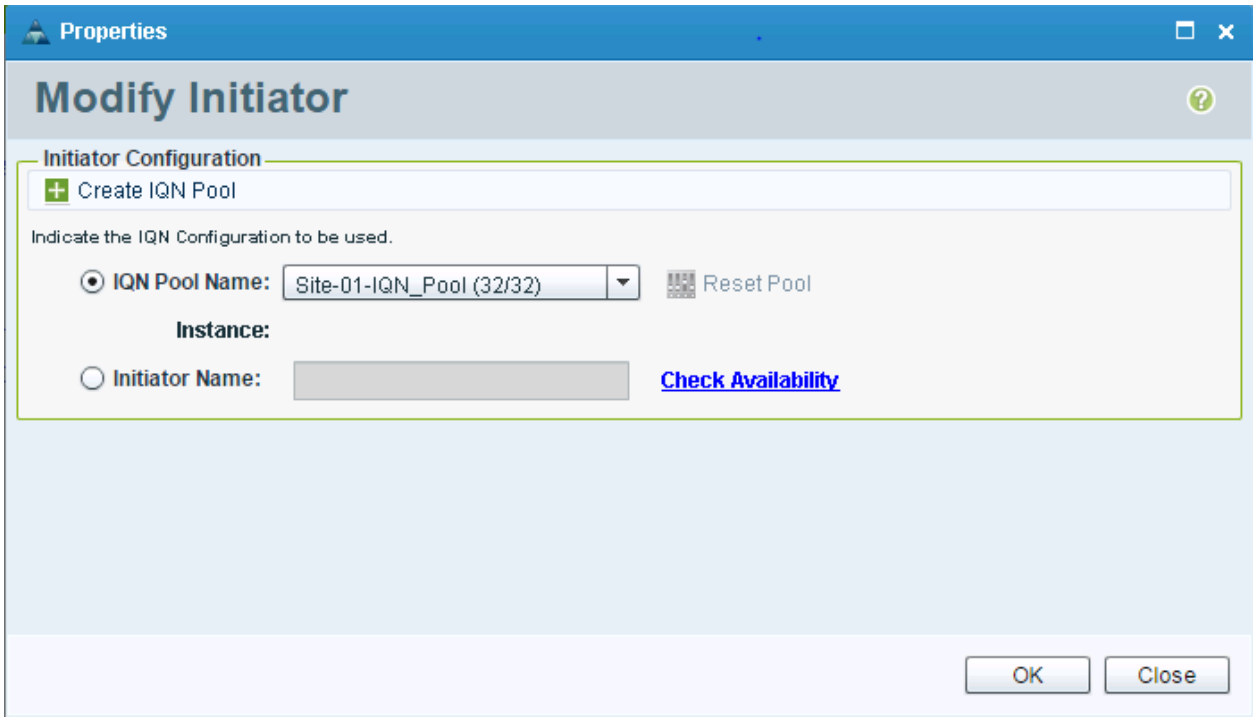
z. Click OK to add the vNIC to the template.

aa. Review the table in the Networking page to confirm that all four vNICs were created.



bb. Select Modify Initiator.

cc. In the Properties window, select IQN Pool Name and select the Site-XX-IQN_Pool.



dd. Click OK.

ee. Click Next.

7. Configure the Storage options:

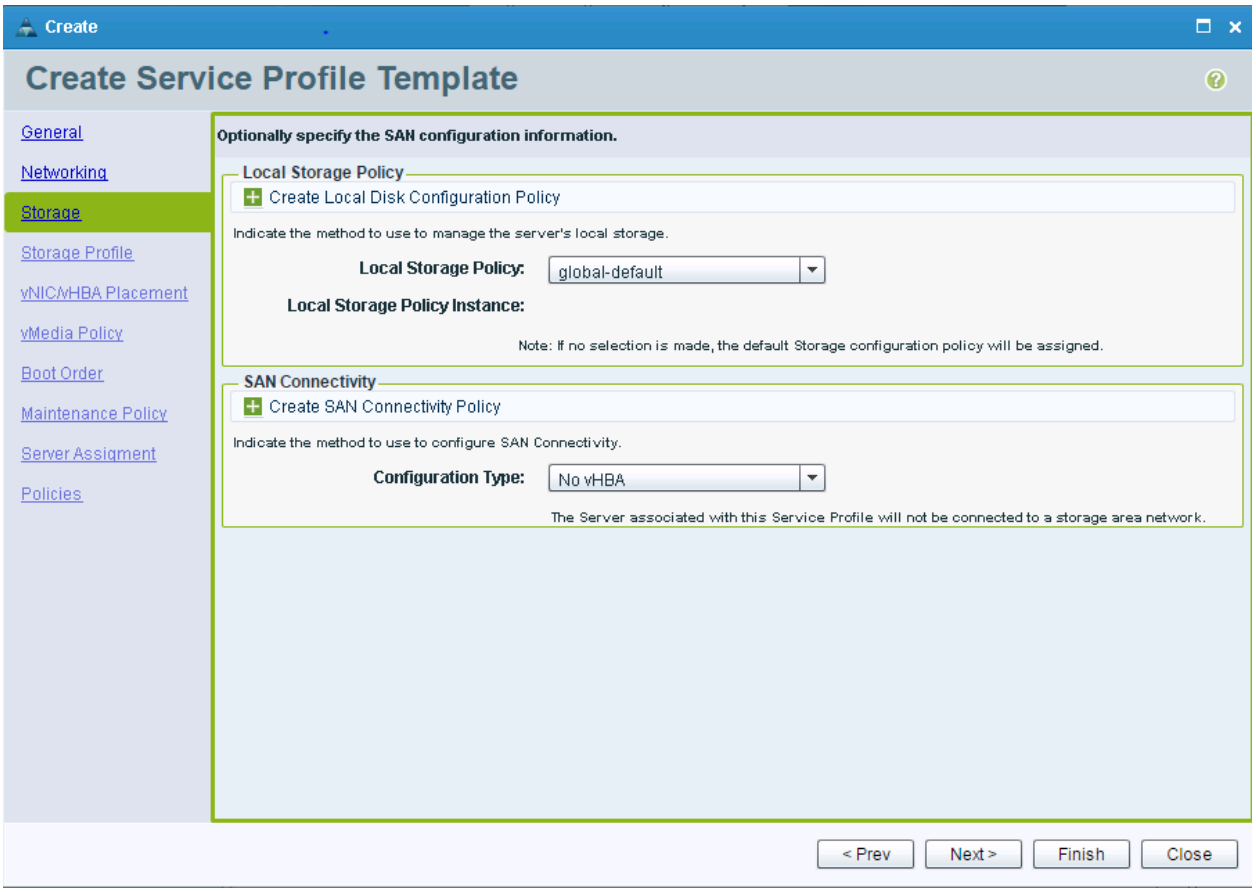
   a. Select a local disk configuration policy:

      i. If the server in question has local disks, select global-default in the Local Storage list.

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

   b. Select the No vHBA to configure the SAN connectivity.

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



   d. Click Next.

8. For the Storage Profile Section, just click Next.

9. For the vNIC/vHBA Placement Section:

   a. Select Placement Policy for the assignment Method

   b. Select VM-Host for the Placement Policy

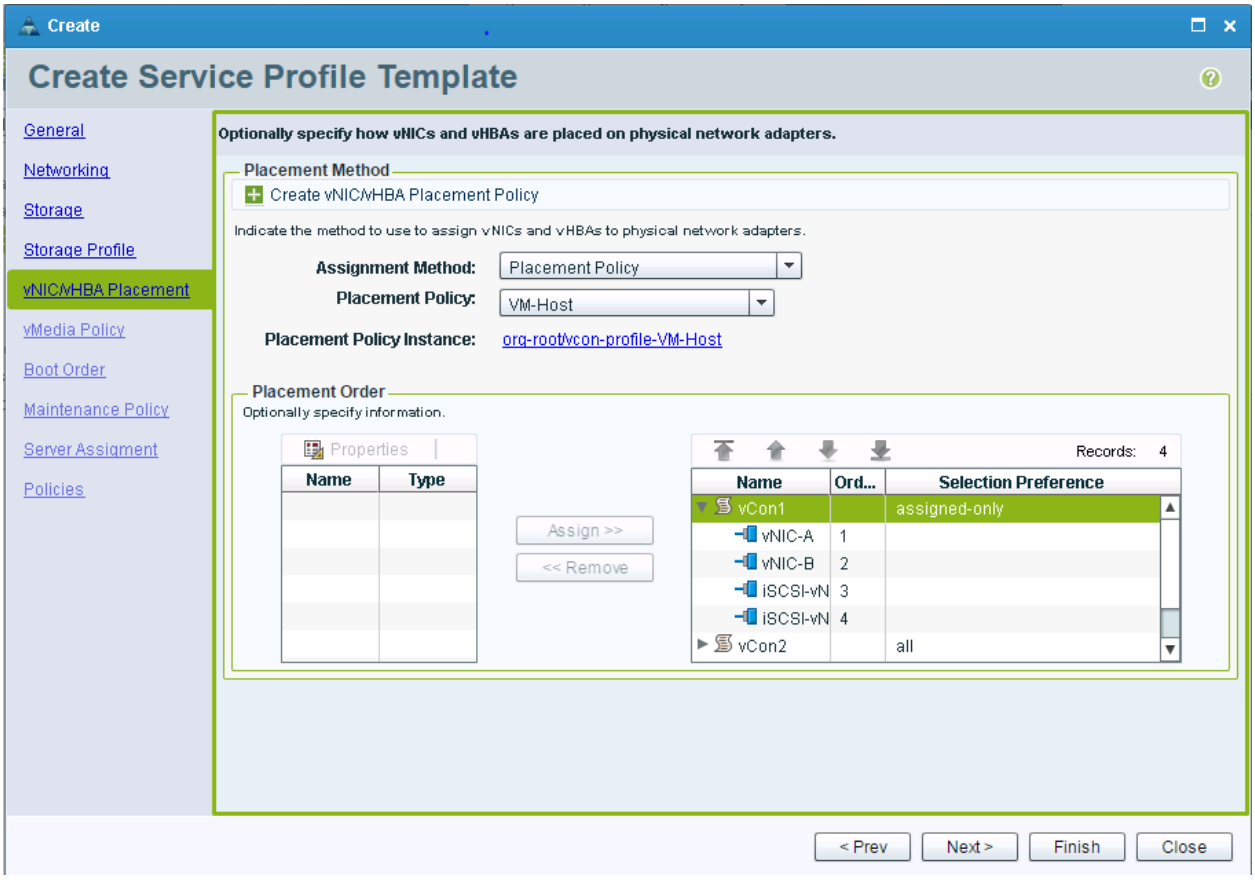
   c. Select assigned-only and vCon1, then assign the following adapters to vCon1:

      i. vNIC-A

ii. vNIC-B

iii. iSCSI-vNIC-A

iv. iSCSI-vNIC-B



d. Click Next.

10. For the vMedia Policy, just click Next.

11. Set the Boot Order:

    a. Select Boot Policy for the Configuration Type.

    b. Select Site-XX-Fabric-A as the Boot Policy.

12. Add a Maintenance Policy:

    a. Confirm that the Maintenance Policy is set to global-default.

    b. Click Next.

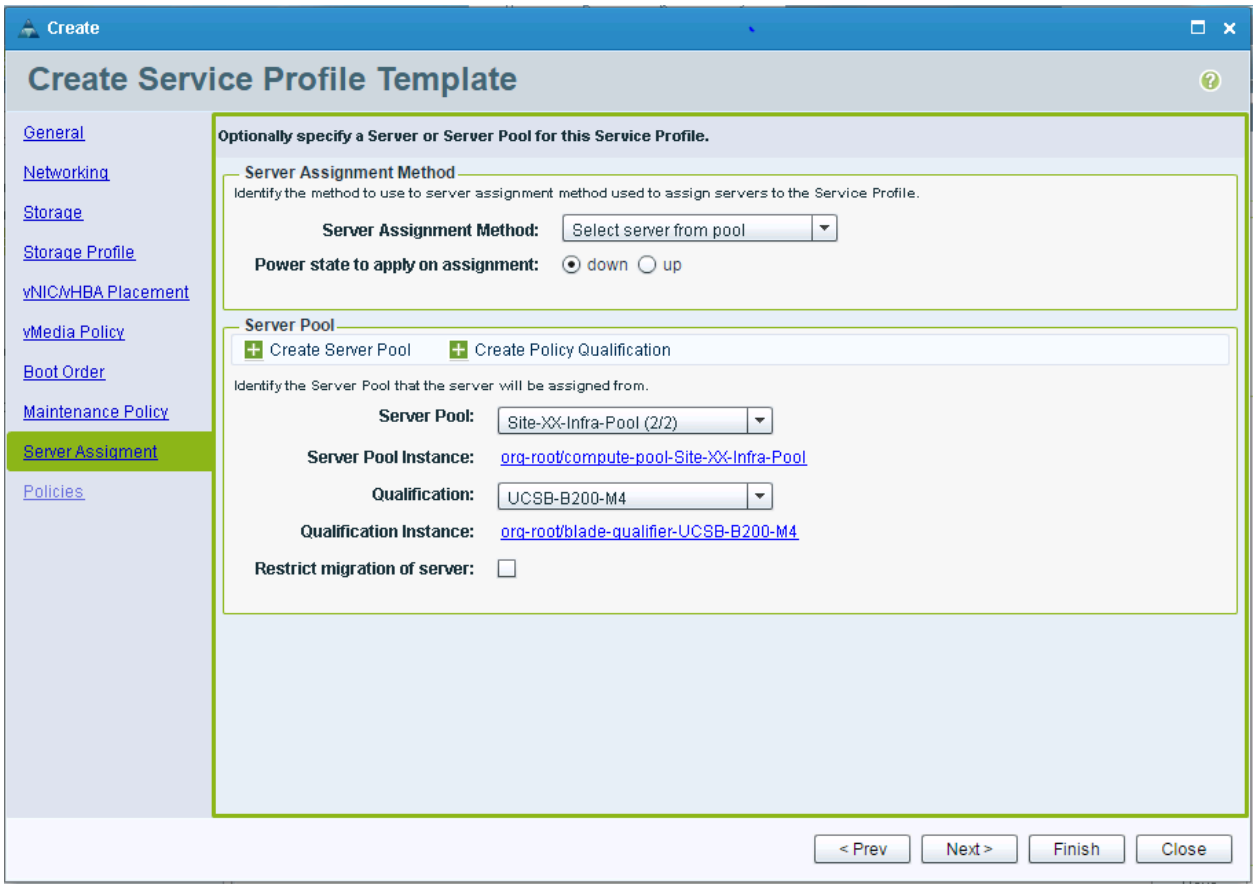
13. Specify the Server Assignment:

    a. Select Server from pool for the Server Assignment Method.

    b. Select down for the Power State to apply on assignment.

    c. Select Site-XX-Infra-Pool as the Server Pool.

d. Optional: Select a Server Pool Qualification policy.



e. Click Next.

14. Add Policies:

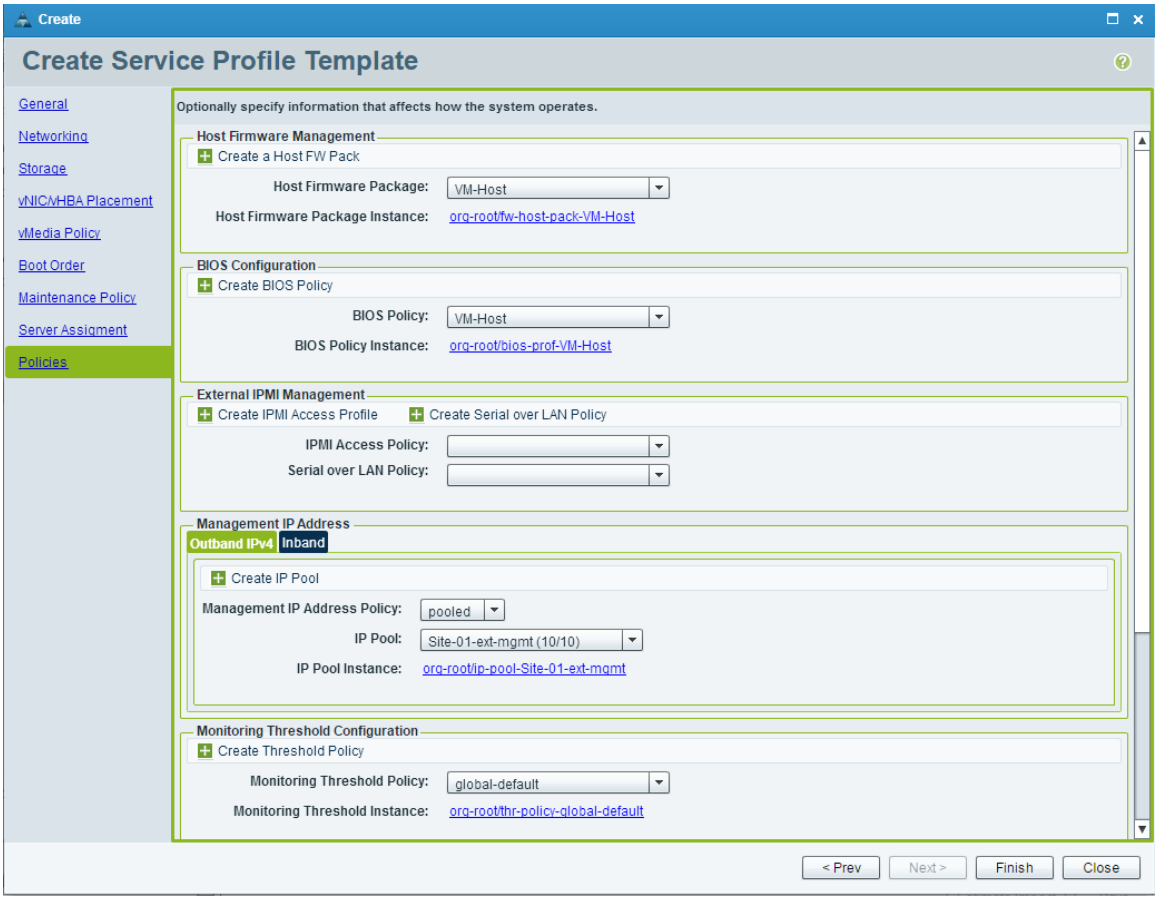
a. Select VM-Host as the Host Firmware Package

b. Select VM-Host and the BIOS Policy

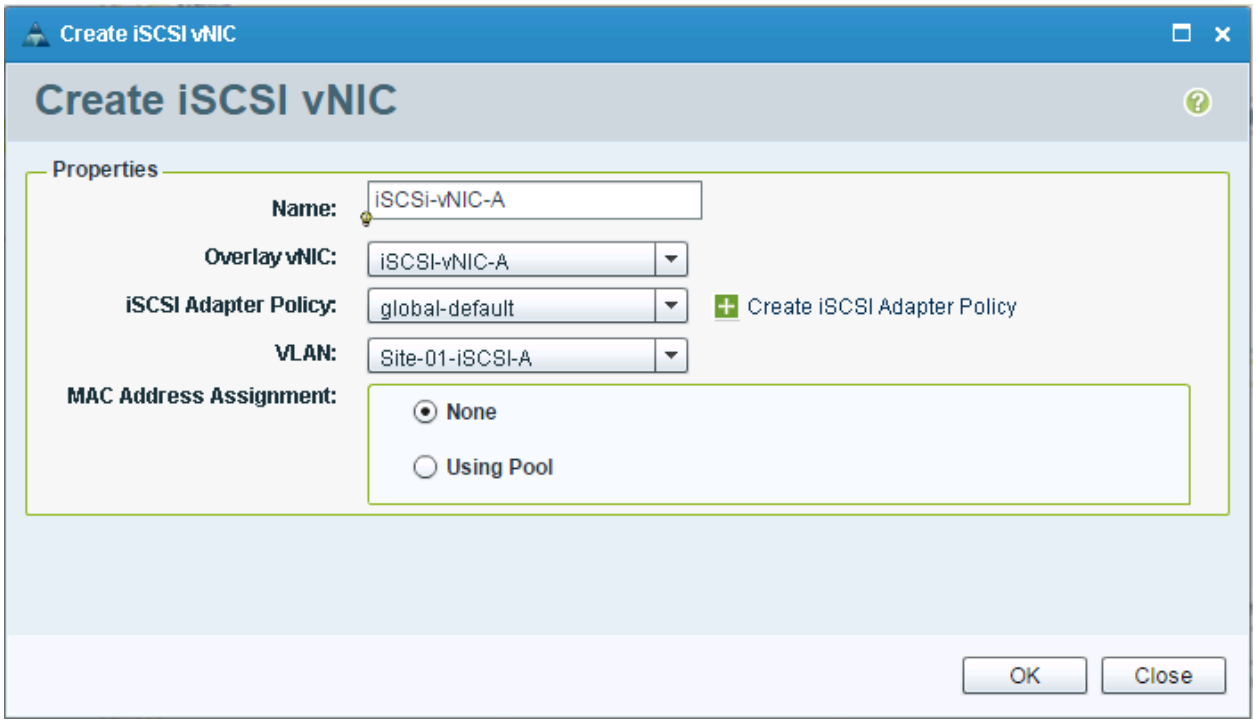
c. Select pooled for Management IP address Policy

d. Select Site-XX-ext-mgmt as the IP Pool

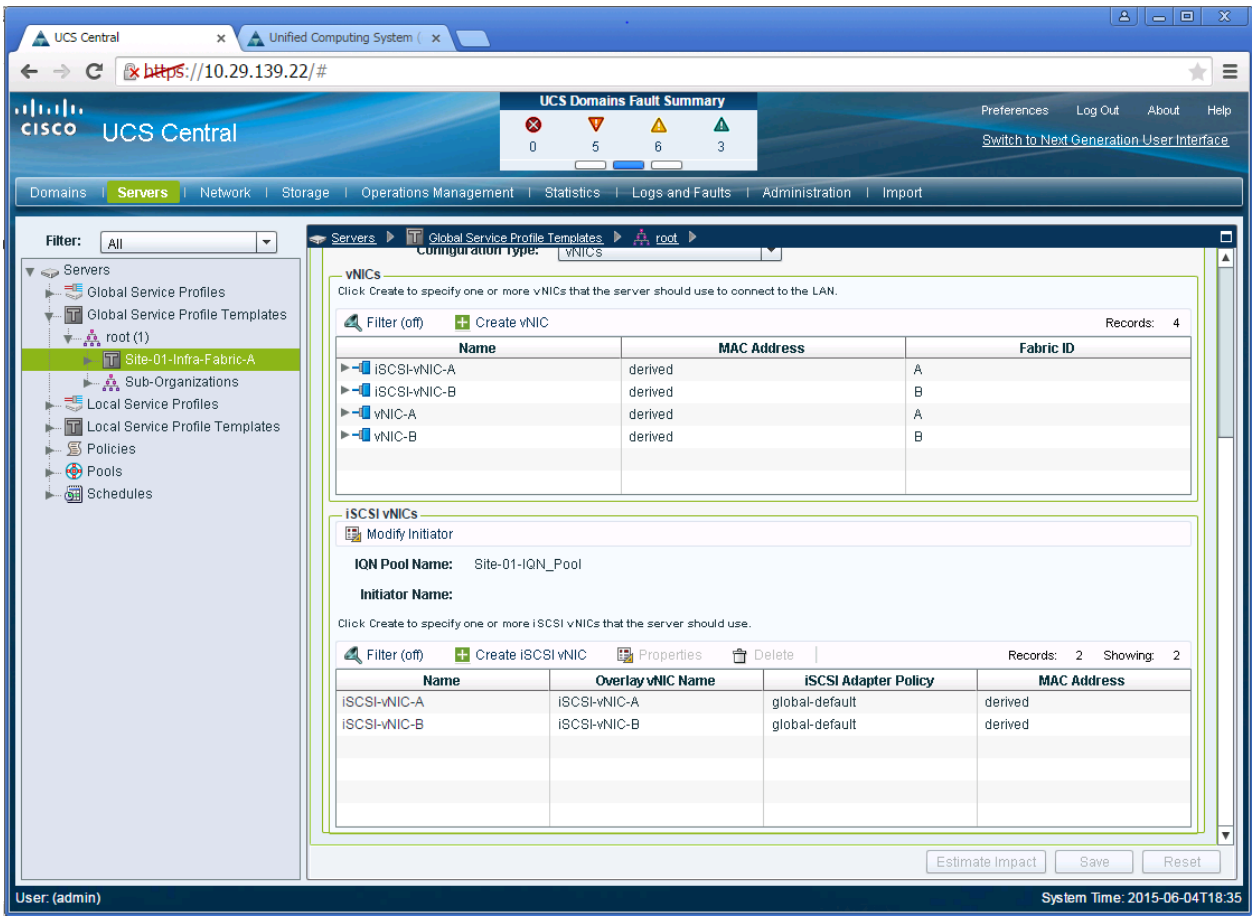
e. Select No-Power-Cap as the Power Control Policy



15. Click Finish to create the service profile template.
16. In the list on the left, select the newly create `Site-XX-Infra-Fabric-A` Global Service Profile Template.
17. Select the Network tab in the center pane.
18. Scroll down and select Create iSCSI vNIC.
19. In the Create iSCSI vNIC window, set the name to `iSCSI-vNIC-A`.
20. Set the Overlay vNIC to iSCSI-vNIC-A.
21. Set the VLAN to Site-XX-iSCSI-A.



22. Click OK.
23. Click Save.
24. Select Create iSCSI vNIC.
25. In the Create iSCSI vNIC window, set the name to `iSCSI-vNIC-B`.
26. Set the Overlay vNIC to iSCSI-vNIC-B.
27. Set the VLAN to Site-XX-iSCSI-B.
28. Click OK.
29. Click Save.



30. In the center pane, select the Boot Order tab.

31. Under Boot Order, expand iSCSI and select iSCSI-vNIC-A.

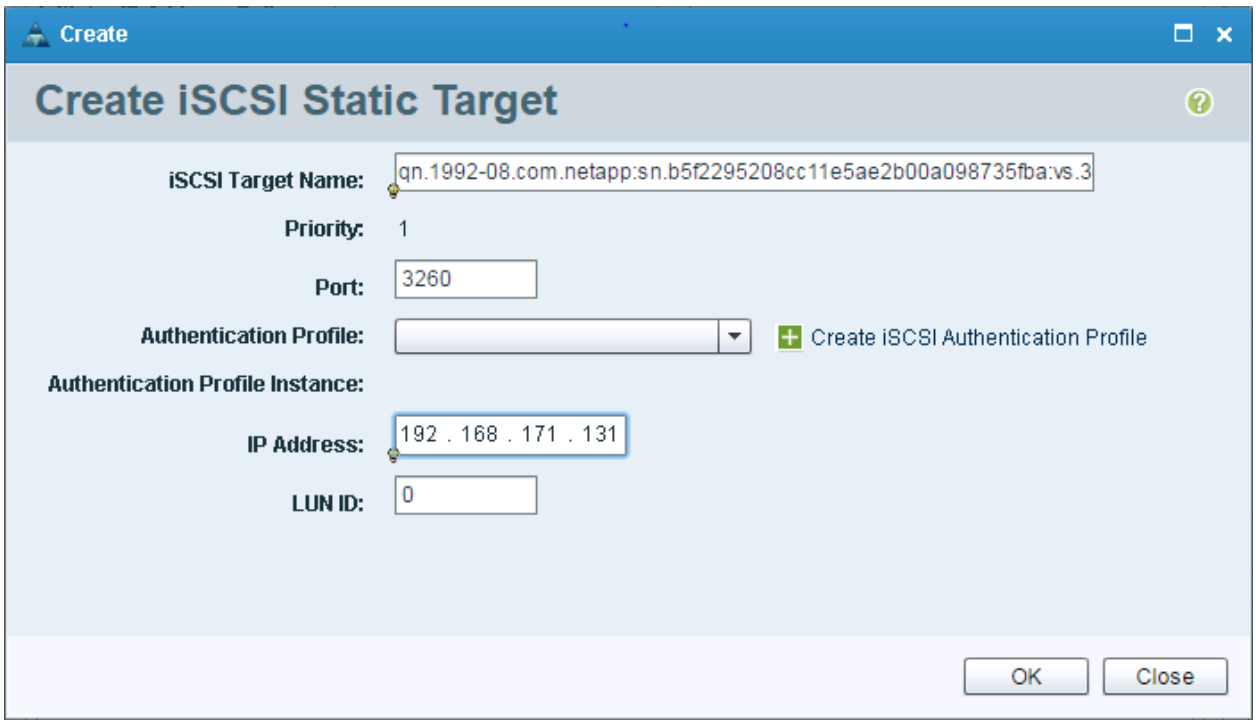
32. Select Set iSCSI Boot Parameters.

33. Set the Initiator IP Address Policy to IP Pools and select the Site-XX-iSCSI_Initiator_A IP Pool.

34. Scroll down and select Create iSCSI Static Target.

35. To get the iSCSI Target Name, log into the Storage Cluster and type `iscsi show`. The iscsi target name for the Infra-SVM will be shown.

36. To get the IP address, on the Storage Cluster interface type `network interface show`. Get the IP address of `iscsi_lif01a`.



37. Click OK to create the iSCSI static target.

38. Select Create iSCSI Static Target.

39. To get the iSCSI Target Name, log into the Storage Cluster and type `iscsi show`. The iscsi target name for the Infra-SVM will be shown.

40. To get the IP address, on the Storage Cluster interface type `network interface show`. Get the IP address of `iscsi_lif02a`.

41. Click OK to complete setting the Fabric A iSCSI Boot Parameters.

42. Select iSCSI-vNIC-B.

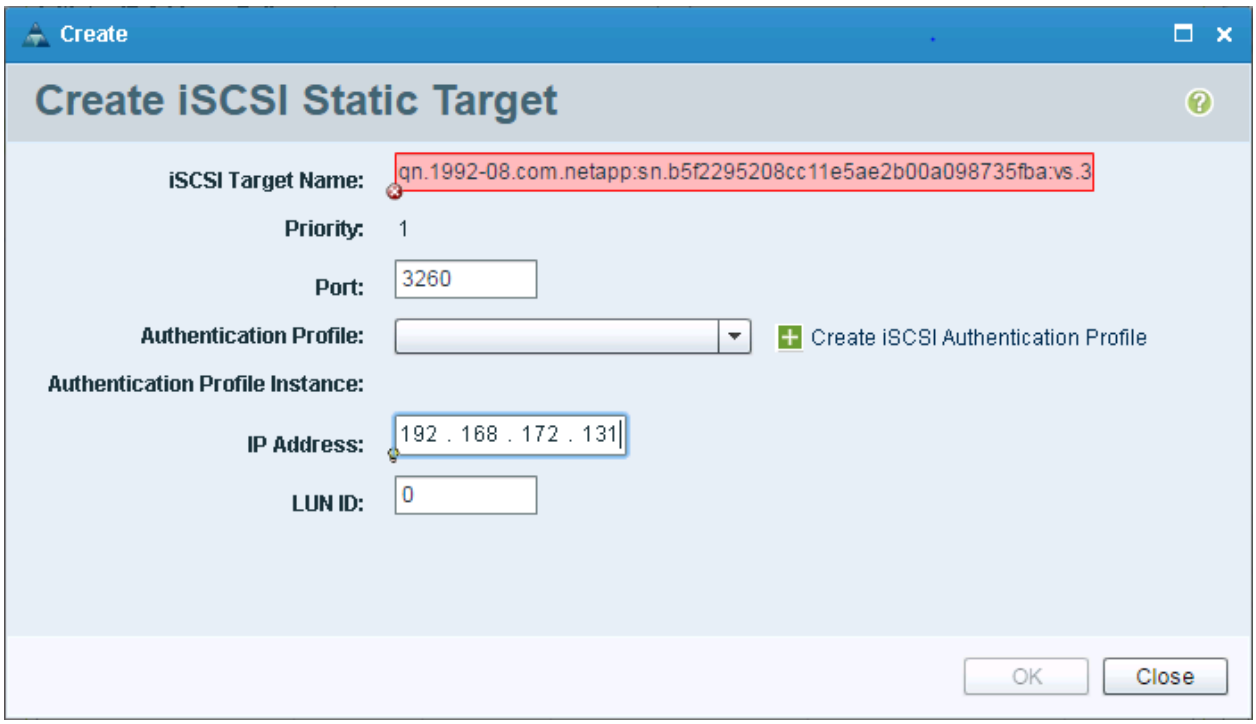
43. Select Set iSCSI Boot Parameters.

44. Set the Initiator IP Address Policy to IP Pools and select the Site-XX-iSCSI_Initiator_B IP Pool.

45. Scroll down and select Create iSCSI Static Target.

46. To get the iSCSI Target Name, log into the Storage Cluster and type `iscsi show`. The iscsi target name for the Infra-SVM will be shown.

47. To get the IP address, on the Storage Cluster interface type `network interface show`. Get the IP address of `iscsi_lif01b`.



48. Click OK to create the iSCSI static target.

49. Select Create iSCSI Static Target.

50. To get the iSCSI Target Name, log into the Storage Cluster and type `iscsi show`. The iscsi target name for the Infra-SVM will be shown.

51. To get the IP address, on the Storage Cluster interface type `network interface show`. Get the IP address of `iscsi_lif02b`.

52. Click OK to complete setting the Fabric B iSCSI Boot Parameters.

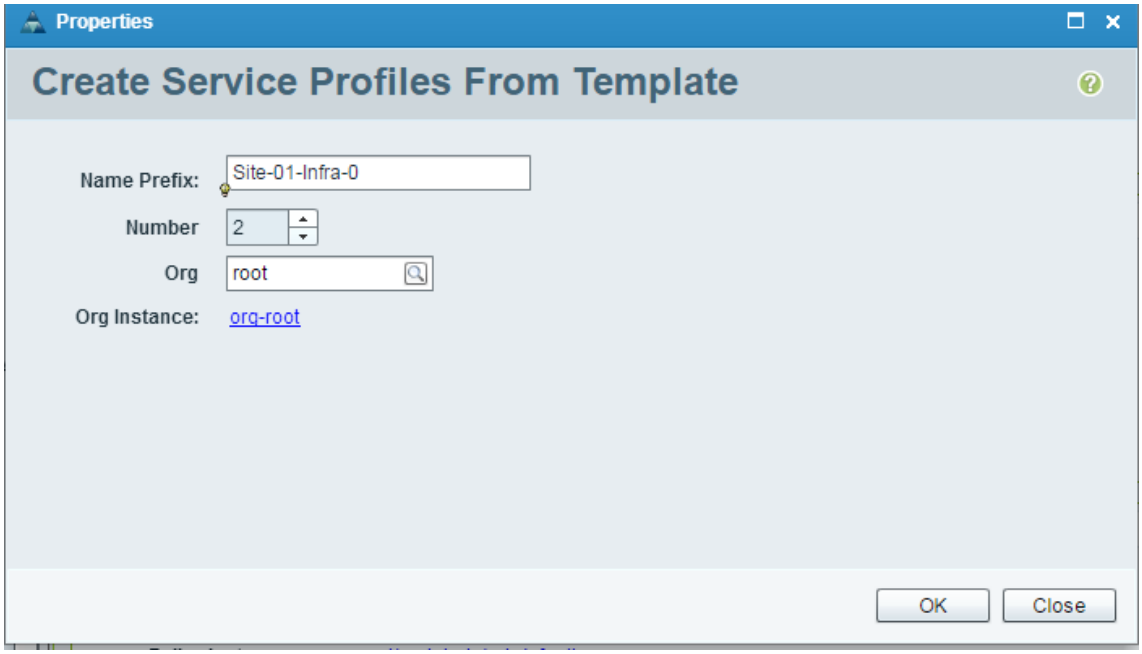
53. Click Save.

Create Service Profiles

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

1. In Cisco UCS Central, click the Servers tab.
2. Expand Servers > Global Service Profile Templates > root.
3. Right click Site-XX-Infra-Fabric-A.
4. Select Create Service Profiles From Template
5. Enter `Site-XX-Infra-0` as the Naming Prefix.
6. Enter `2` as the Number of Instances to create.

7. Select root as the Org



8. Click OK to create the service profiles.

9. Click OK in the confirmation message.

10. Verify that the service profiles `Site-01-Infra-01` and `Site-01-Infra-02` have been created. The service profiles are automatically associated with the servers in their assigned server pools.

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 22.

Table 22 iSCSI IQNs and IPs for Each ESXi Host

Cisco UCS Service Profile Name	iSCSI IQN	iSCSI-vNIC-A IP	iSCSI-vNIC-B IP
VM-Host-Infra-01			
VM-Host-Infra-02			

Note: To gather the iSCSI IQN information, launch the local Cisco UCS Manager. Click the Servers tab. Expand Servers > Service Profiles > root. Click each service profile then click the iSCSI vNICs

tab in the right pane. The iSCSI Initiator Name is the host's iSCSI IQN. To get the iSCSI vNIC IP addresses, click the Boot Order tab. Expand iSCSI in the list below and select an iSCSI vNIC. At the bottom of the page, select Set iSCSI Boot Parameters. The IP address is shown in this window.

Storage Configuration Part 2

Clustered Data ONTAP SAN Boot Storage Setup

Create iSCSI Igroups

To create igroups, complete the following step:

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

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

```
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-01 –protocol iscsi –ostype vmware –initiator
<<var_vm_host_infra_01_IQN>>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-02 –protocol iscsi –ostype vmware –initiator
<<var_vm_host_infra_02_IQN>>
igroup create –vserver Infra-SVM –igroup MGMT-Hosts –protocol iscsi –ostype vmware –initiator
<<var_vm_host_infra_01_IQN>>, <<var_vm_host_infra_02_IQN>>
igroup show
```

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:

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

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

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

VMware vSphere 5.5 Update 2 Setup

FlexPod VMware ESXi 5.5 Update 2 on Clustered Data ONTAP

This section provides detailed instructions for installing VMware ESXi 5.5 Update 2 in a FlexPod environment. After the procedures are completed, two iSCSI-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 iSCSI boot.

Download Cisco Custom Image for ESXi 5.5.0 U2

1. Click on 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 CiscoCustomImage5.5.0U2
4. Click Download
5. Save it to your destination folder.

Log in to Cisco UCS 6324 Fabric Interconnect

Cisco UCS Central

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 Central KVM page to run the IP KVM.

To log in to the Cisco UCS Central KVM page, complete the following steps:

1. Open a web browser and enter the IP address for Cisco UCS Central using https://.
2. When prompted, enter `admin` as the user name and enter the administrative password.
3. Click Launch KVM.
4. At the top of the window, select the root organization and click Search.
5. Right-click the Site-XX-Infra-01 Service Profile and select KVM Console.
6. Click OK and follow the steps to launch the Java .jnlp file. Respond to all prompts.
7. Open a KVM window for the Site-XX-Infra-02 Service Profile.

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 menu.
2. If prompted to accept an Unencrypted KVM session, accept as necessary.
3. Click Activate Virtual Devices
4. Click the virtual media menu again and select map CD/DVD
5. Click browse and browse to the ESXi installer ISO image file and click Open.
6. Click Map device
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. 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. Once the test is complete, 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. Once the test is complete, 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 application is downloaded from the VMware website and Internet access is required on the management workstation.

3. Click on the following link VMware vSphere CLI 5.5 Update 2.
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 Update 2 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:

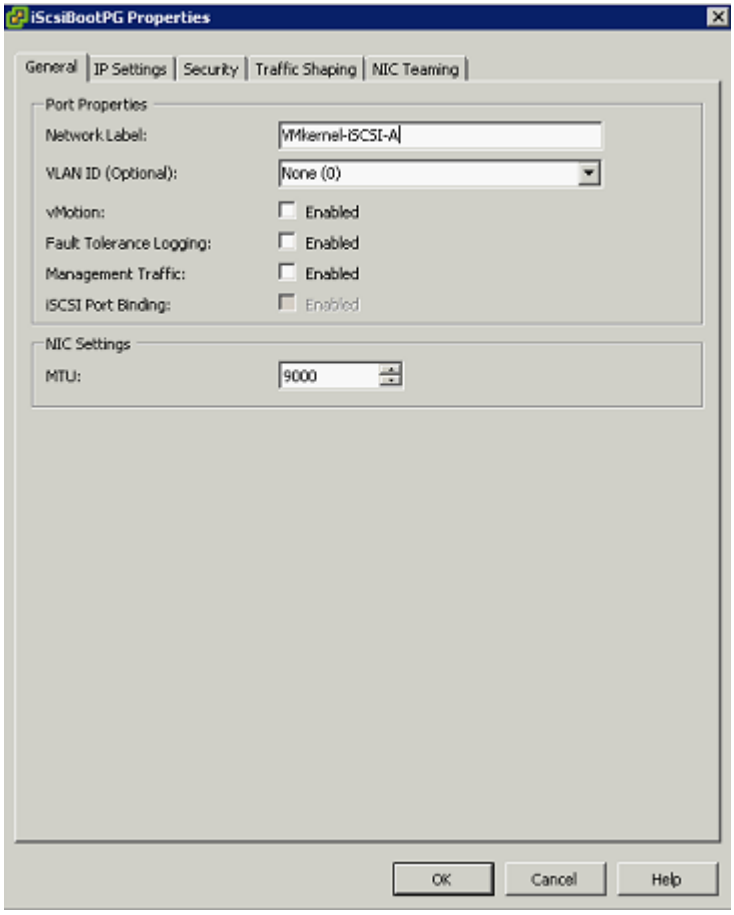
1. Open the recently downloaded VMware vSphere Client and enter the IP address of `VM-Host-Infra-02` as the host you are trying to connect to: `<<var_vm_host_infra_02_ip>>`.
2. Enter `root` for the user name.
3. Enter the root password.
4. Click Login to connect.

Setup iSCSI Networking for iSCSI Booted Servers

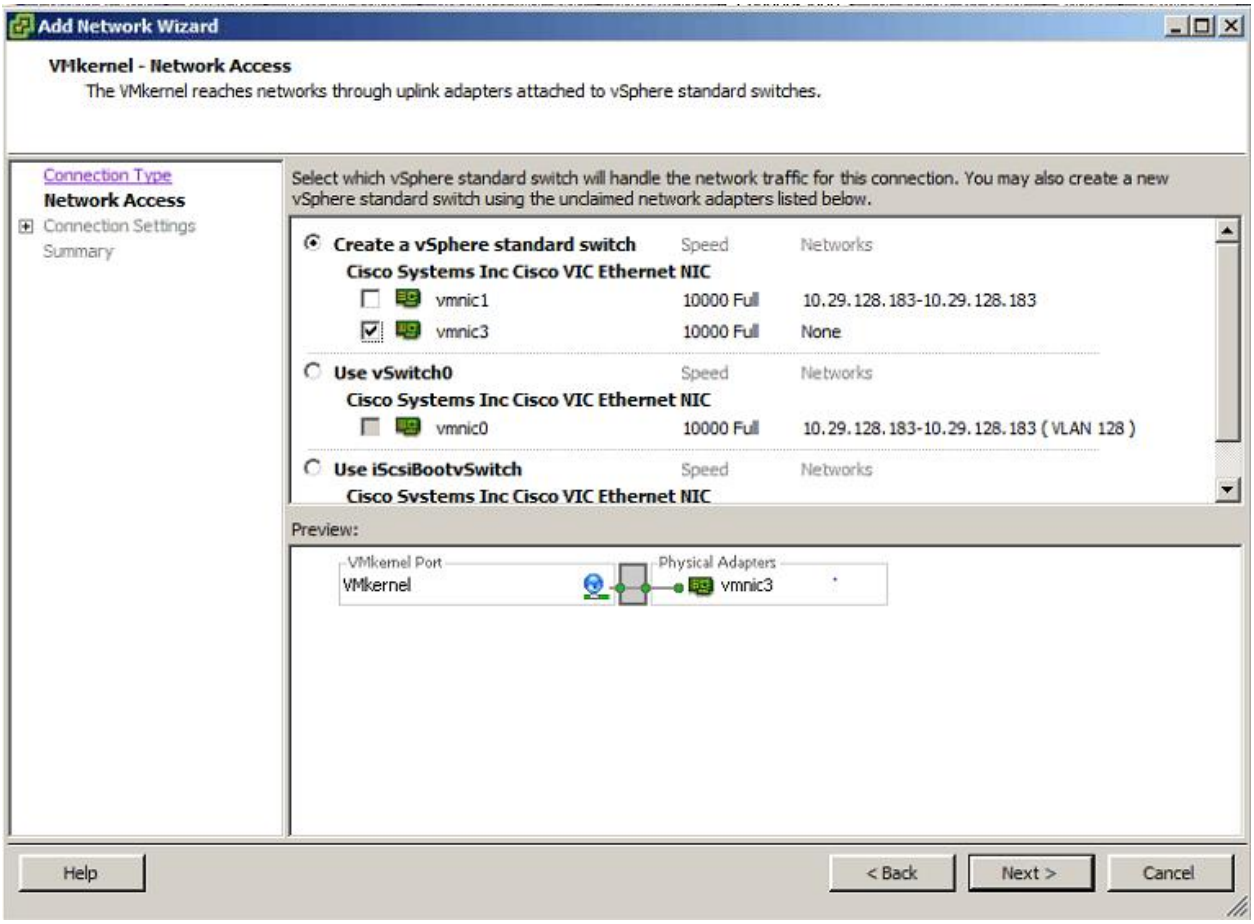
ESXi Hosts VM-Host-Infra-01 and VM-Host-Infra-02

To set up iSCSI Networking for both ESXi hosts, complete the following steps:

1. Launch the VMware vSphere client
2. Connect to the host with the `root` user id and password
3. In the vSphere client in the right pane, select the configuration tab
4. In the Hardware pane select Networking
5. To the right of the iScsiBootvSwitch, select Properties
6. Select the vSwitch configuration and click Edit
7. Change the MTU to 9000 and click OK
8. Select the iScsBootPG configuration and click Edit
9. Change the Network label to VMKernel-iSCSI-A
10. Change the MTU to 9000
11. Do not set a VLAN.

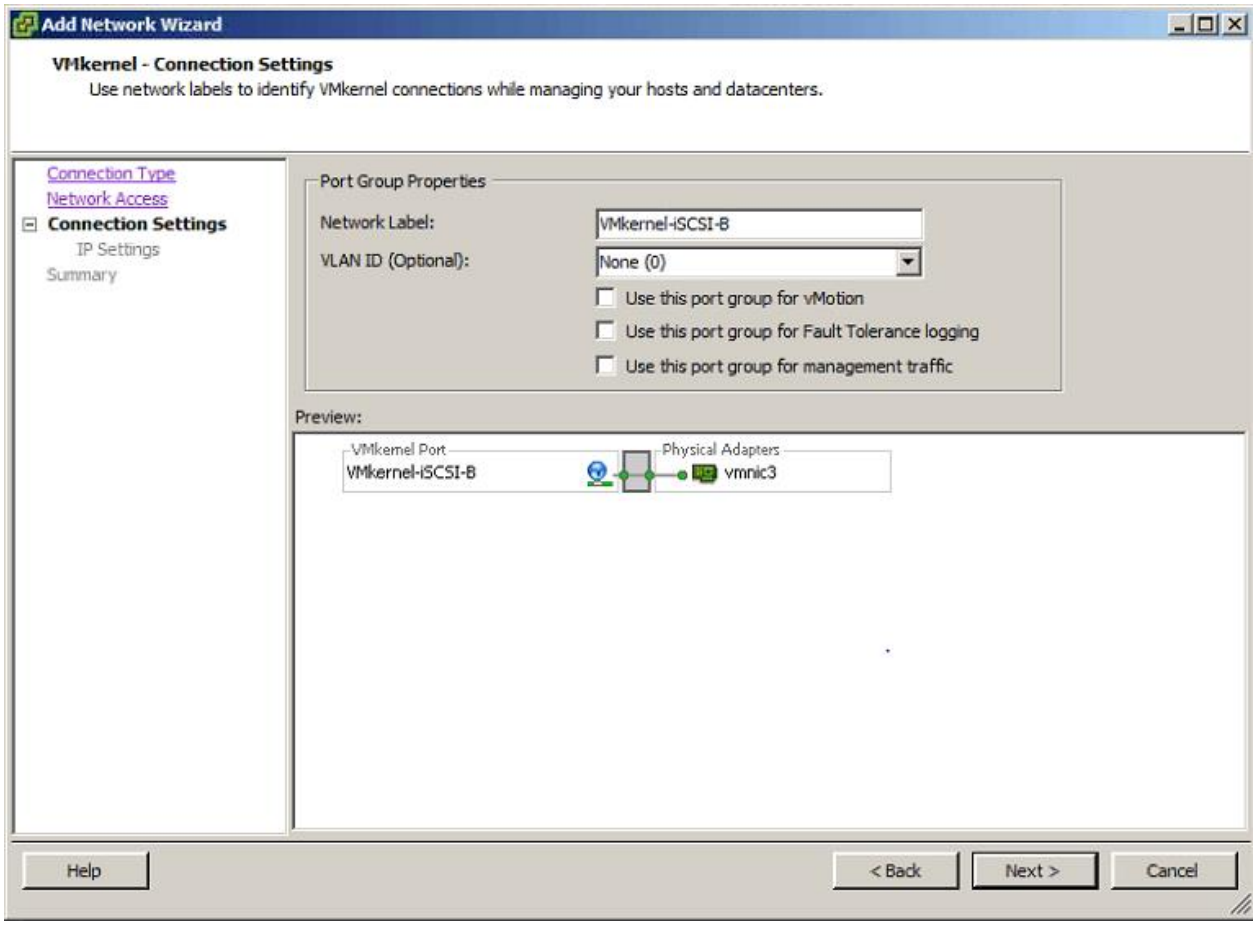


12. Click OK.
13. Click Close to close the iScsiBootvSwitch Properties window.
14. On the right, select Add Networking.
15. Select the VMkernel Connection Type and click Next.
16. Remove the selection from vmnic1 and select vmnic3.



17. Click Next.

18. Set the Network Label to VMkernel-iSCSI-B. Leave the VLAN ID set to None.

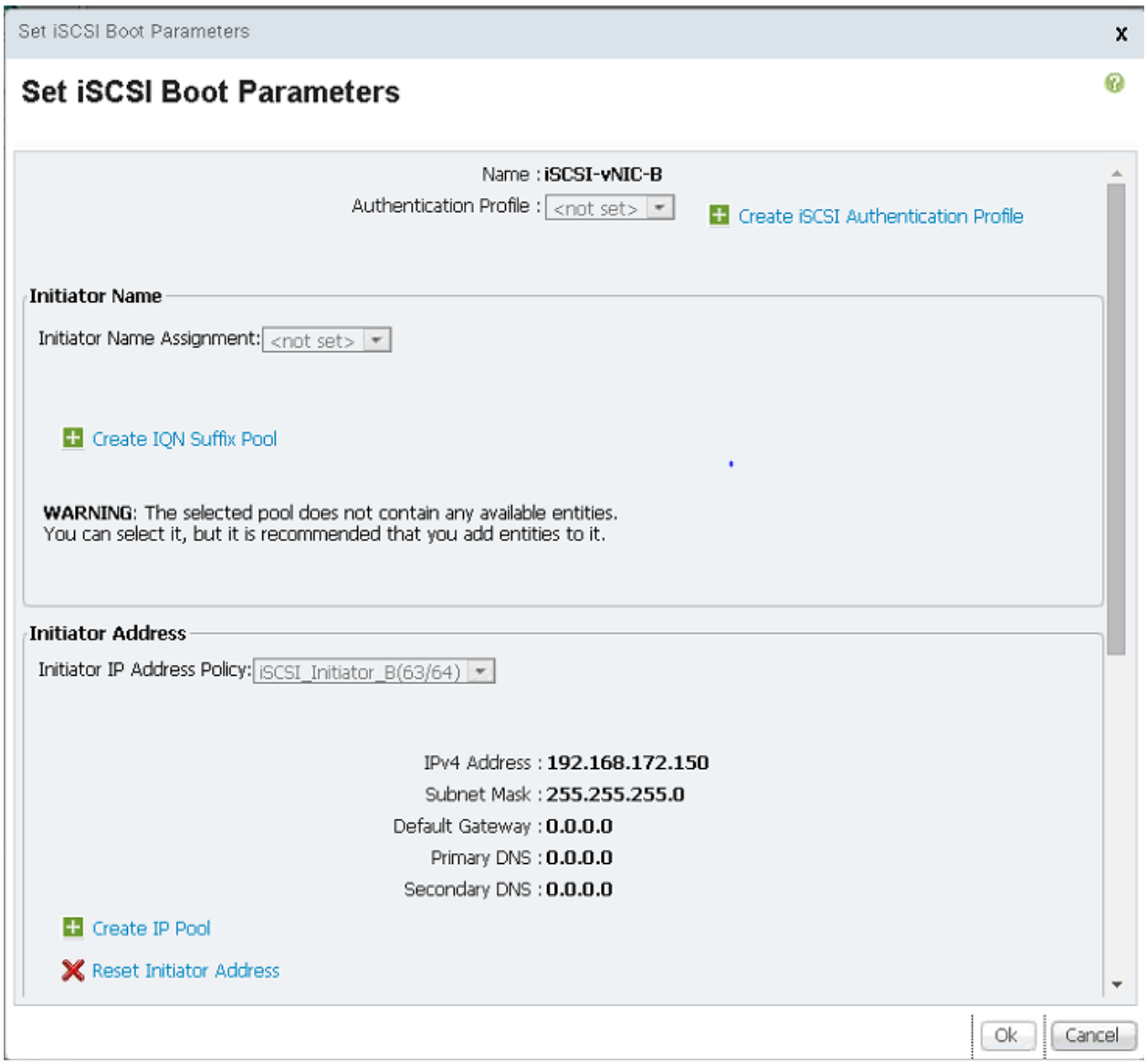


19. Click Next.

20. Retrieve the VMkernel IP address from Cisco UCS Manager.

21. In UCS Manager, select the Server's Service Profile and under the Boot Order tab expand iSCSI.

22. Select iSCSI-vNIC-B and click Set iSCSI Boot Parameters. The initiator IP Address will display.



23. In the vSphere client, enter the IP Address and net mask you just retrieved from Cisco UCS Manager.
24. Click Next and Finish to create the vSwitch and VMkernel port.
25. Select Properties to the right of vSwitch1.
26. In the vSwitch1 Properties window, select the vSwitch configuration and click Edit.
27. Change the MTU to 9000 and click OK.
28. Select the VMkernel-iSCSI-B configuration and click Edit.
29. Change the MTU to 9000 and click OK.
30. Click Close to close the vSwitch1 Properties window.
31. Click Storage Adapters in the Hardware pane.

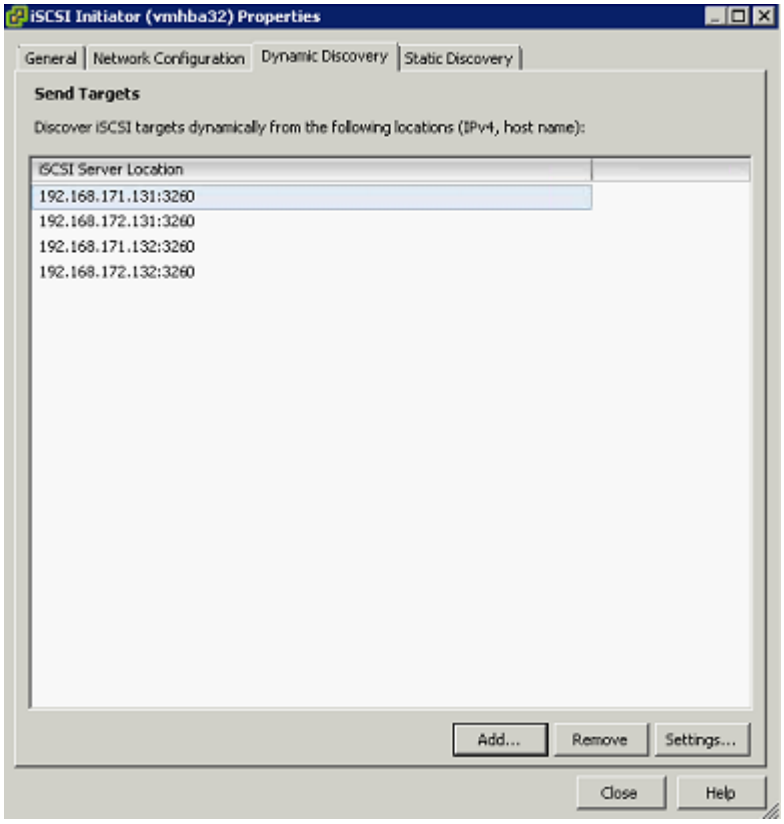
32. Select the iSCSI Software Adapter and click Properties.

33. Select the Dynamic Discovery tab and click Add.

34. Enter the IP address of `iscsi_lif01a`.

35. Click OK.

36. Repeat putting in the IP addresses of `iscsi_lif01b`, `iscsi_lif02a` and `iscsi_lif02b`.



37. Click Close and then click Yes to rescan the host bus adapter.

You should now see 4 connected paths in the Details pane.

Install VMware Drivers for the Cisco Virtual Interface Card (VIC)

Follow the below steps to install VMware VIC Drivers on the ESXi host VM-Host-Infra-01 and VM-Host-Infra-02

1. Download and extract the following VMware VIC Drivers to the Management workstation -

   - fnic Driver version 1.6.0.16
   - enic Driver version 2.2.2.69

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 VIC drivers and select `fnic_driver_1.6.0.16-offline_bundle-2574267.zip`.
6. Click Open and Yes to upload the file to datastore1.
7. Click the fourth button and select Upload File.
8. Navigate to the saved location for the downloaded VIC drivers and select `enic-2.1.2.69-offline_bundle-2581703.zip`.
9. Click Open and Yes to upload the file to datastore1.
10. Make sure the files have been uploaded to both ESXi hosts.
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/fnic_driver_1.6.0.16-offline_bundle-2574267.zip
esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>> software vib update -d
/vmfs/volumes/datastore1/ fnic_driver_1.6.0.16-offline_bundle-2574267.zip
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> software vib update -d
/vmfs/volumes/datastore1/enic-2.1.2.69-offline_bundle-2581703.zip
esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>> software vib update -d
/vmfs/volumes/datastore1/ enic-2.1.2.69-offline_bundle-2581703.zip
```

13. Back in the vSphere Client for each host, right click the host and select Reboot.
14. Click Yes and OK to reboot the host.
15. Log back into each host with vSphere Client.

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 VMkernel-MGMT.
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 IB-MGMT 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. Click Add to add a network element.
26. Select VMkernel and click Next.
27. Change the network label to `VMkernel-NFS` and enter `<<var_nfs_vlan_id>>` in the VLAN ID (Optional) field.
28. Click Next to continue with the NFS VMkernel creation.

29. Enter the IP address `<<var_nfs_vlan_id_ip_host-01>>` and the subnet mask `<<var_nfs_vlan_id_mask_host-01>>` for the NFS VLAN interface for `VM-Host-Infra-01`.

30. Click Next to continue with the NFS VMkernel creation.

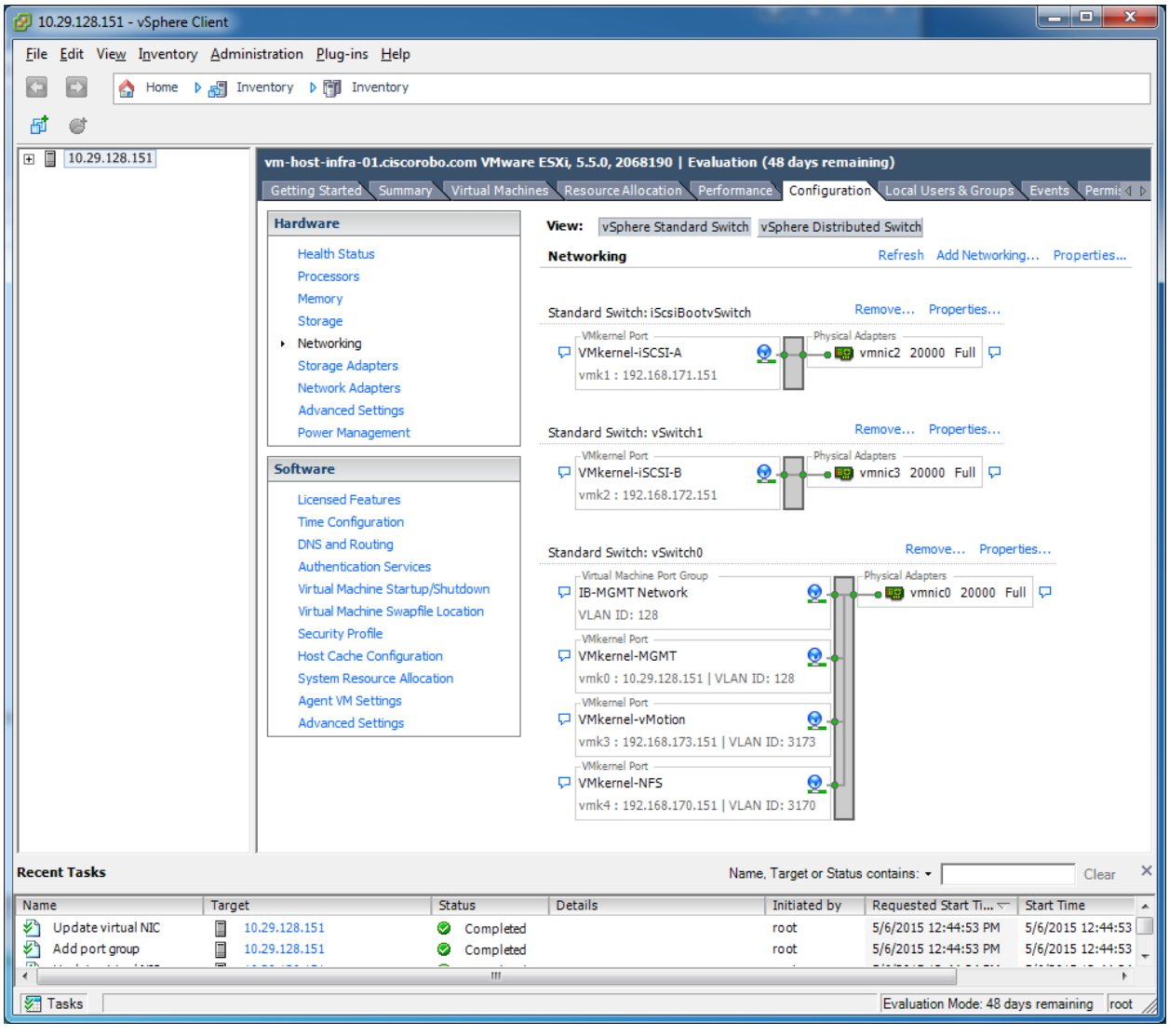
31. Click Finish to finalize the creation of the NFS VMkernel interface.

32. Select the VMkernel-NFS configuration and click Edit.

33. Change the MTU to `9000`.

34. To finalize the edits for the VMkernel-NFS network, click OK.

35. To finalize the ESXi host networking setup, close the dialog box. The networking for the ESXi host should be similar to the following example:

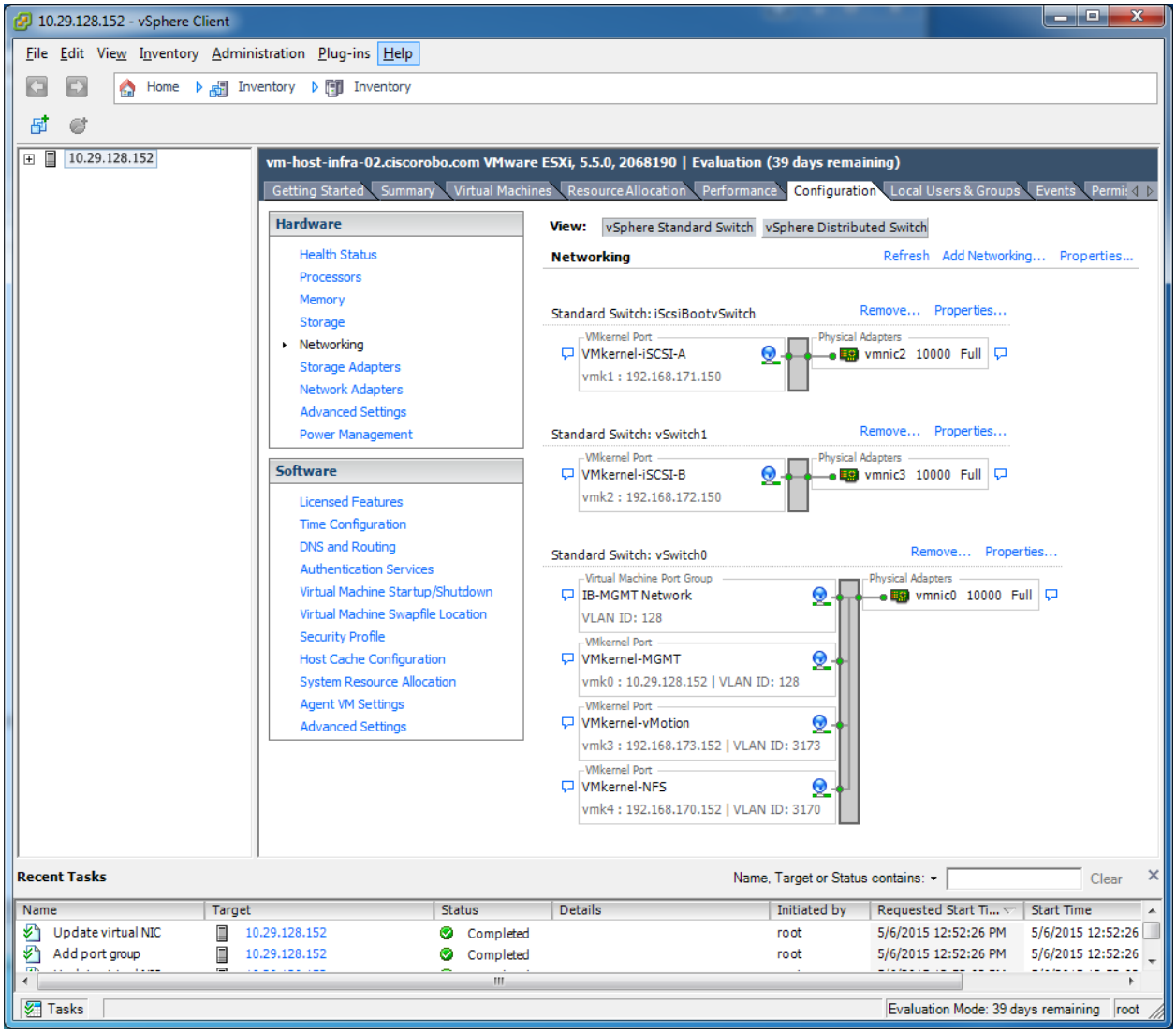


ESXi Host VM-Host-Infra-02

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 VMkernel-MGMT, 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 IB-MGMT 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 add a network element, click Add.
28. Select VMkernel and click Next.
29. Change the network label to `VMkernel-NFS` and enter `<<var_nfs_vlan_id>>` in the VLAN ID (Optional) field.
30. To continue with the NFS VMkernel creation, click Next.
31. Enter the IP address `<<var_nfs_vlan_id_ip_host-02>>` and the subnet mask `<<var_nfs_vlan_id_mask_host-02>>` for the NFS VLAN interface for `VM-Host-Infra-02`.
32. To continue with the NFS VMkernel creation, click Next.
33. To finalize the creation of the NFS VMkernel interface, click Finish.
34. Select the VMkernel-NFS configuration and click Edit.
35. Change the MTU to `9000`.
36. To finalize the edits for the VMkernel-NFS network, click OK.
37. To finalize the ESXi host networking setup, close the dialog box. The networking for the ESXi host should be similar to the following example:

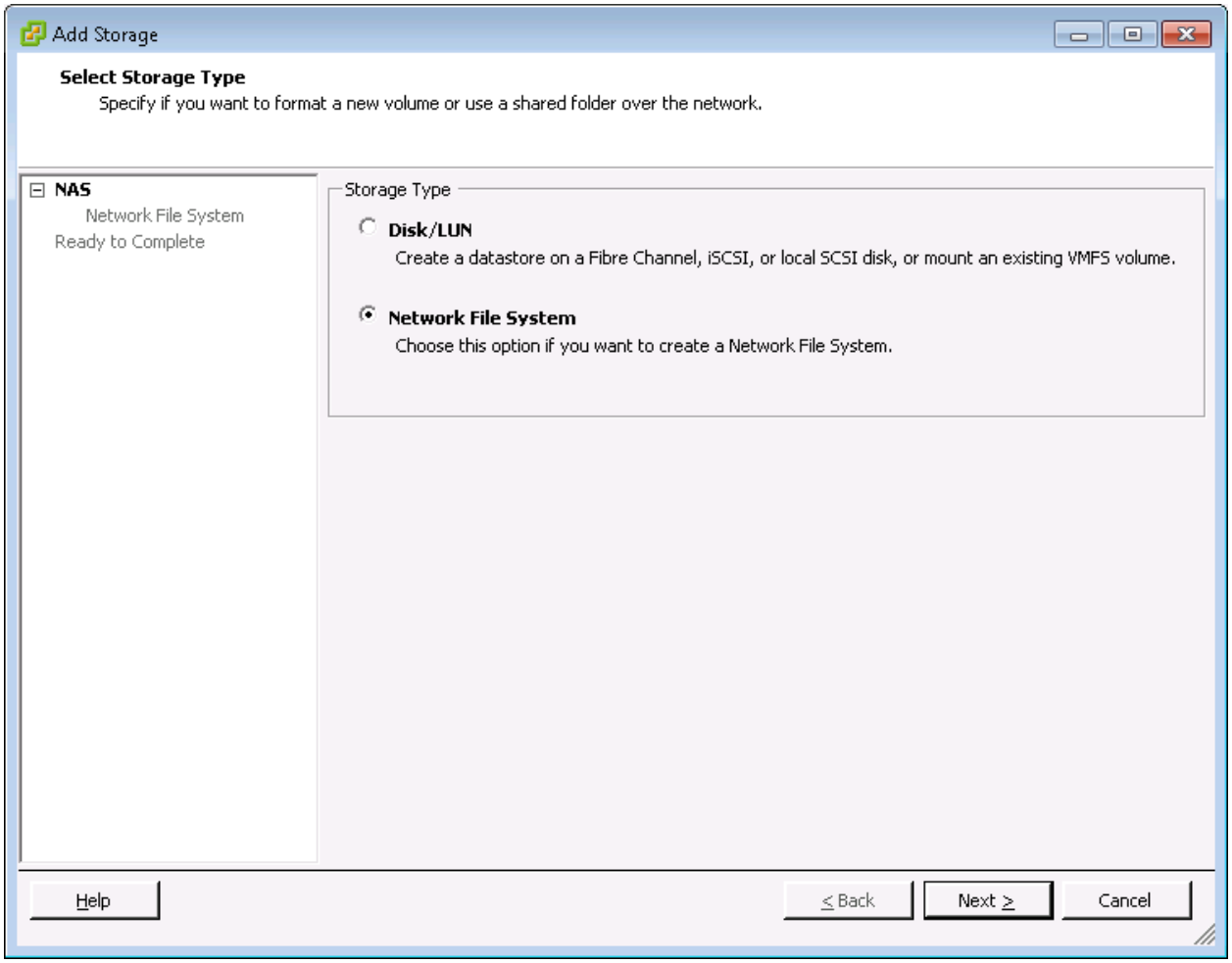


Mount Required Datastores

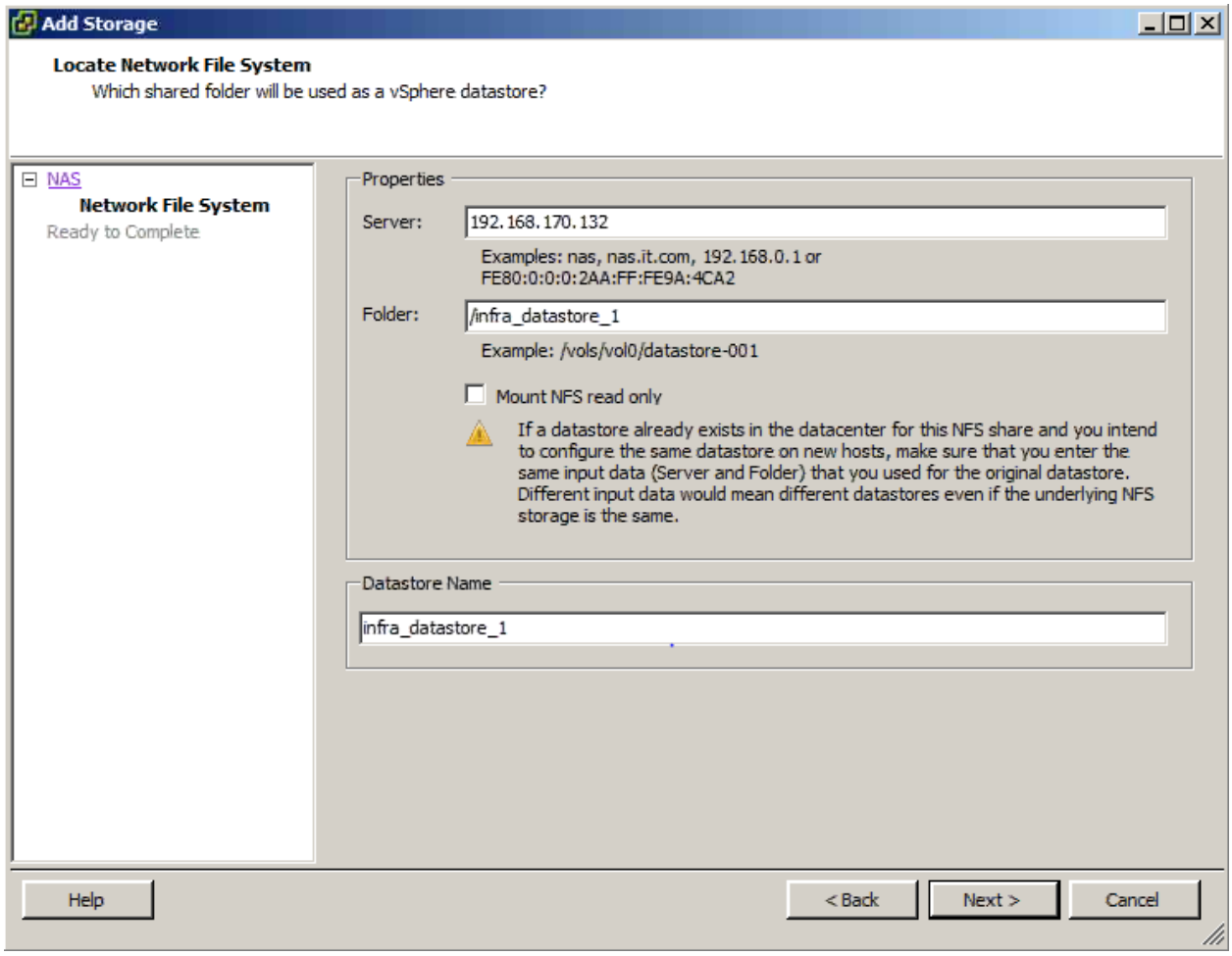
ESXi Hosts VM-Host-Infra-01 and VM-Host-Infra-02

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. 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 Network File System and click Next.



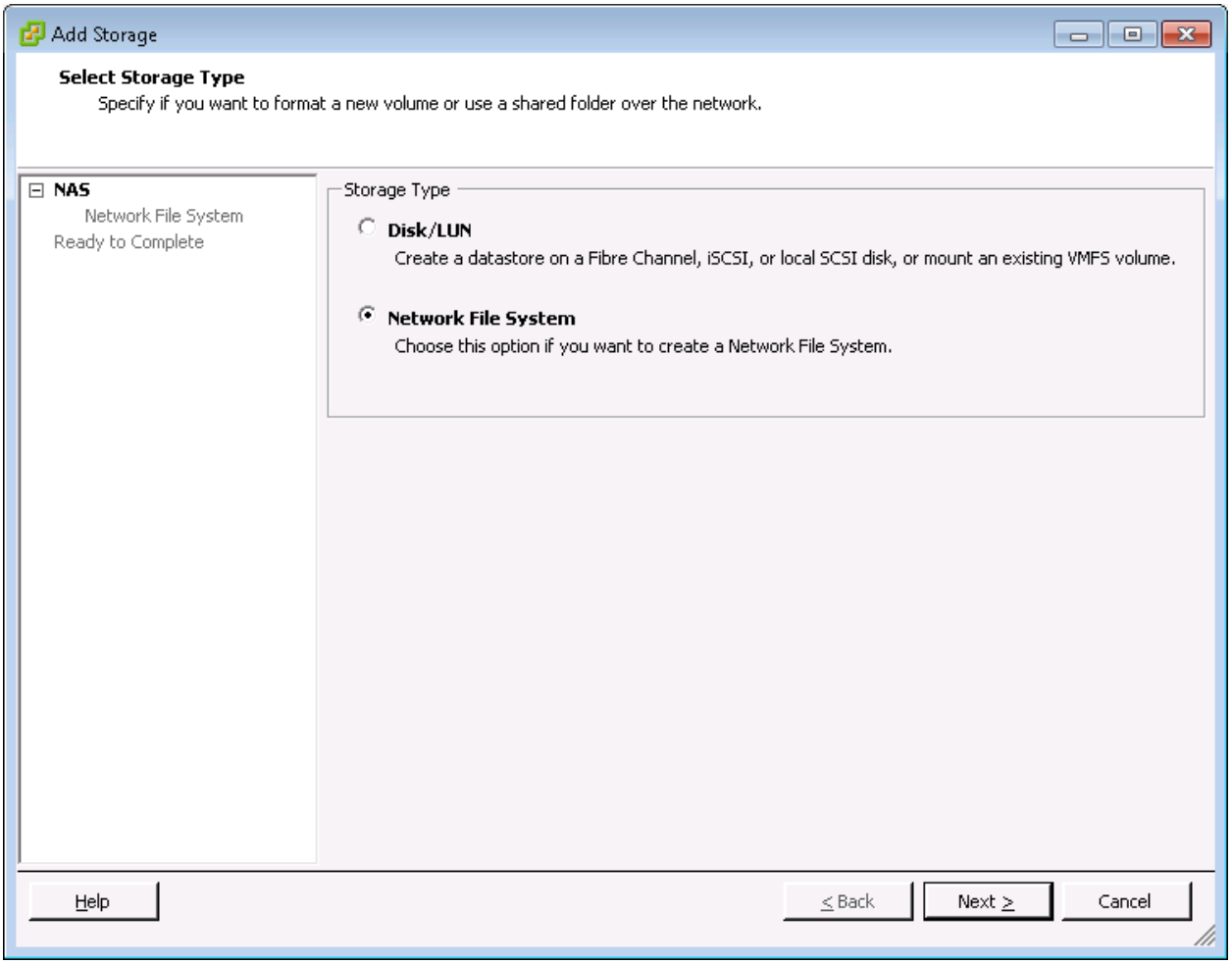
6. The wizard prompts for the location of the NFS export. Enter `<<var_node02_nfs_infra_datastore_1_ip>>` as the IP address for LIF `nfs_infra_datastore_1`.
7. Enter `/infra_datastore_1` as the path for the NFS export.
8. Confirm that the Mount NFS read only checkbox is not selected.
9. Enter `infra_datastore_1` as the datastore name.



10. To continue with the NFS datastore creation, click Next.

11. To finalize the creation of the NFS datastore, click Finish.

12. From the Datastores area, click Add Storage to open the Add Storage wizard.



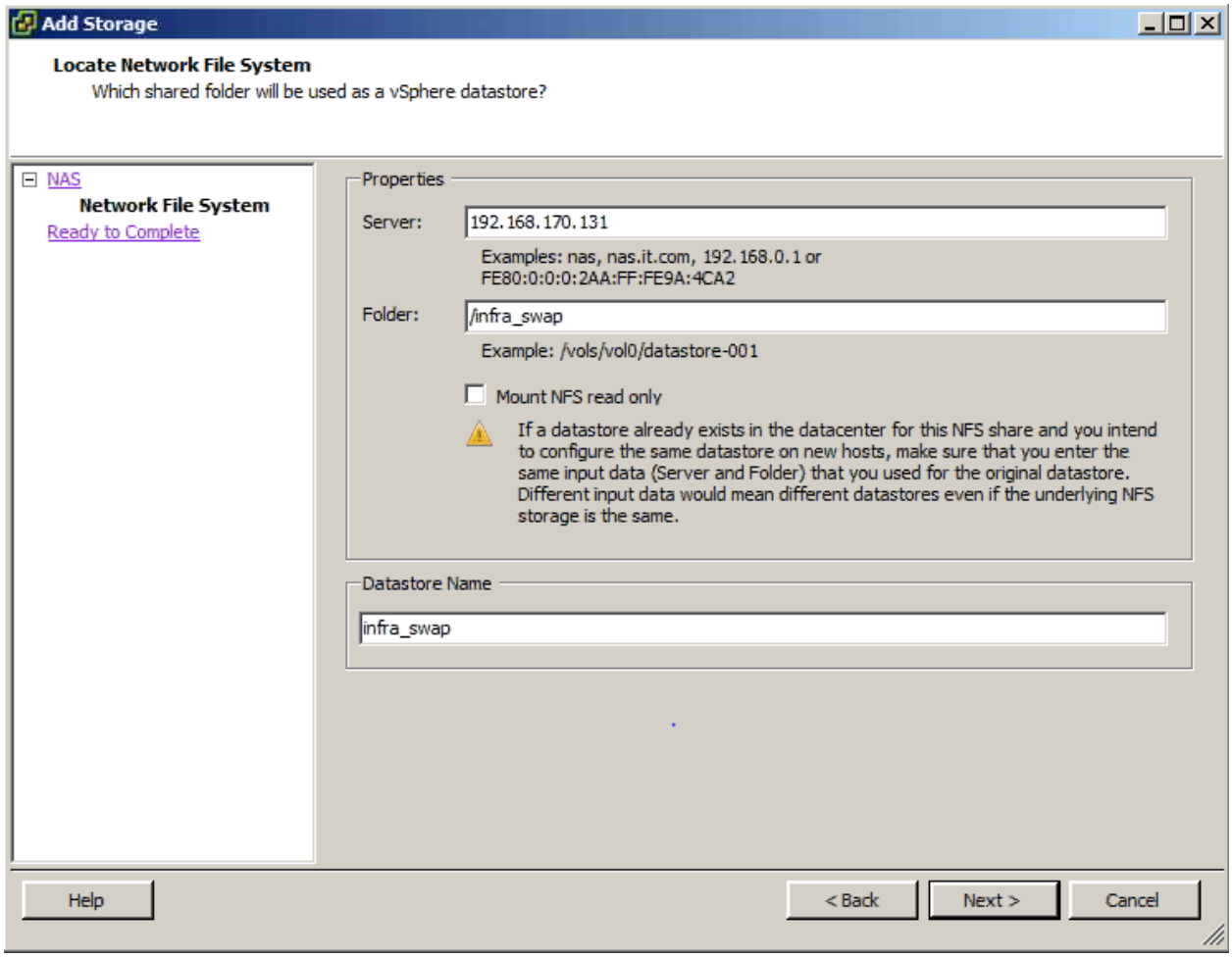
13. Select Network File System and click Next.

14. The wizard prompts for the location of the NFS export. Enter `<<var_node01_nfs_infra_swap_ip>>` as the IP address for LIF `nfs_infra_swap`.

15. Enter `/infra_swap` as the path for the NFS export.

16. Confirm that the Mount NFS read only checkbox is not selected.

17. Enter `infra_swap` as the datastore name.



18. To continue with the NFS datastore creation, click Next.

19. To finalize the creation of the NFS datastore, click Finish.

Configure NTP on ESXi Hosts

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

1. To configure Network Time Protocol (NTP) on the ESXi hosts, complete the following steps on each host:

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

3. Click the Configuration tab.

4. Click Time Configuration in the Software pane.

5. Click Properties at the upper-right side of the window.

6. At the bottom of the Time Configuration dialog box, click Options.

7. In the NTP Daemon (ntpd) Options dialog box, complete the following steps:

   a. Click General in the left pane, select Start, and stop with host.

b. Click NTP Settings in the left pane and click Add.

8. In the Add NTP Server dialog box, enter `<<var_global_ntp_server_ip>>` as the IP address of the NTP server and click OK.

9. In the NTP Daemon Options dialog box, select the Restart NTP service to apply changes checkbox and click OK.

10. 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.

Note: 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.

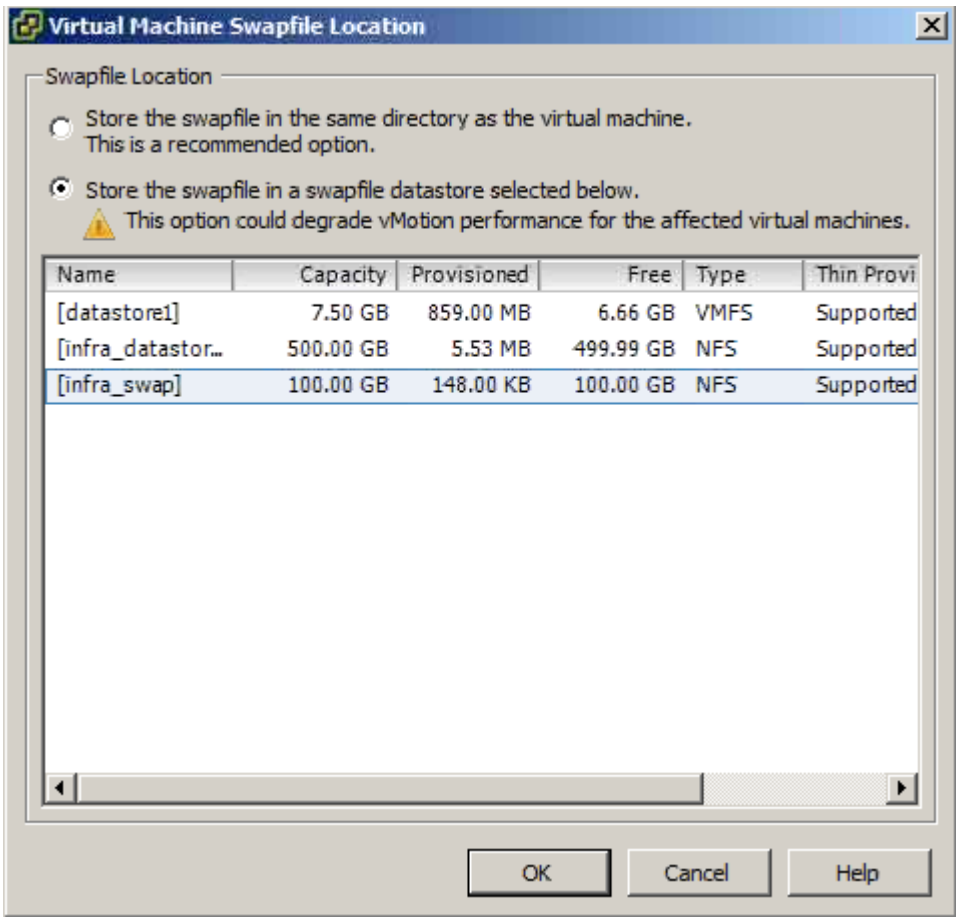
2. Click the Configuration tab.

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 2

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.

Note: If a centralized vCenter is being used in this deployment, it is not necessary to install the vCenter Appliance. If a centralized vCenter is being used, continue in this procedure below at the point where an ESXi host cluster is being added to the vCenter. A suggested name for this cluster is Site-XX. Note that if a central Cisco Nexus 1000V is also being used in this deployment, the cluster that is being created should be in the same VMware Datacenter as the Nexus 1000V.

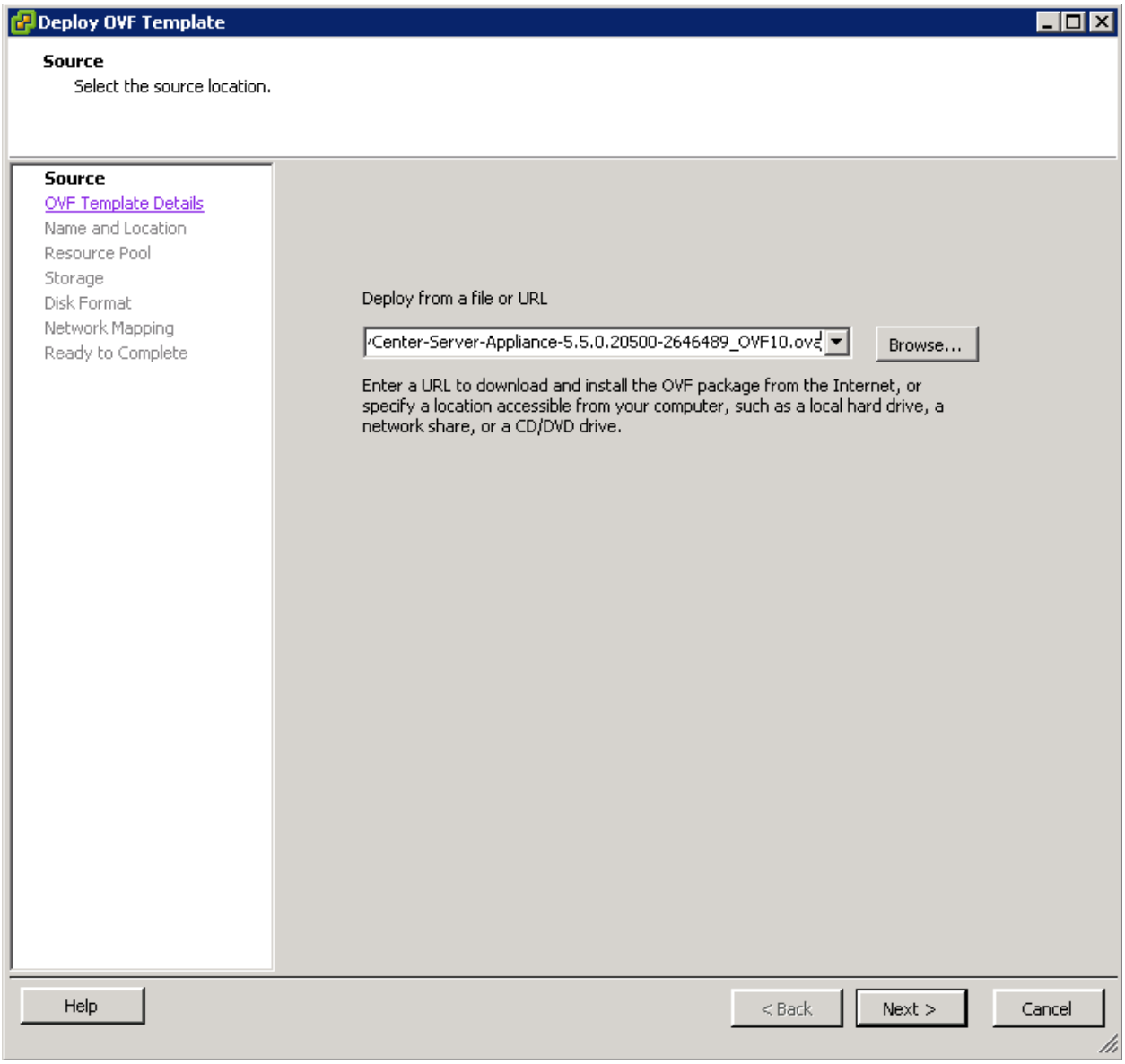
Build and Set up VMware vCenter VM

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

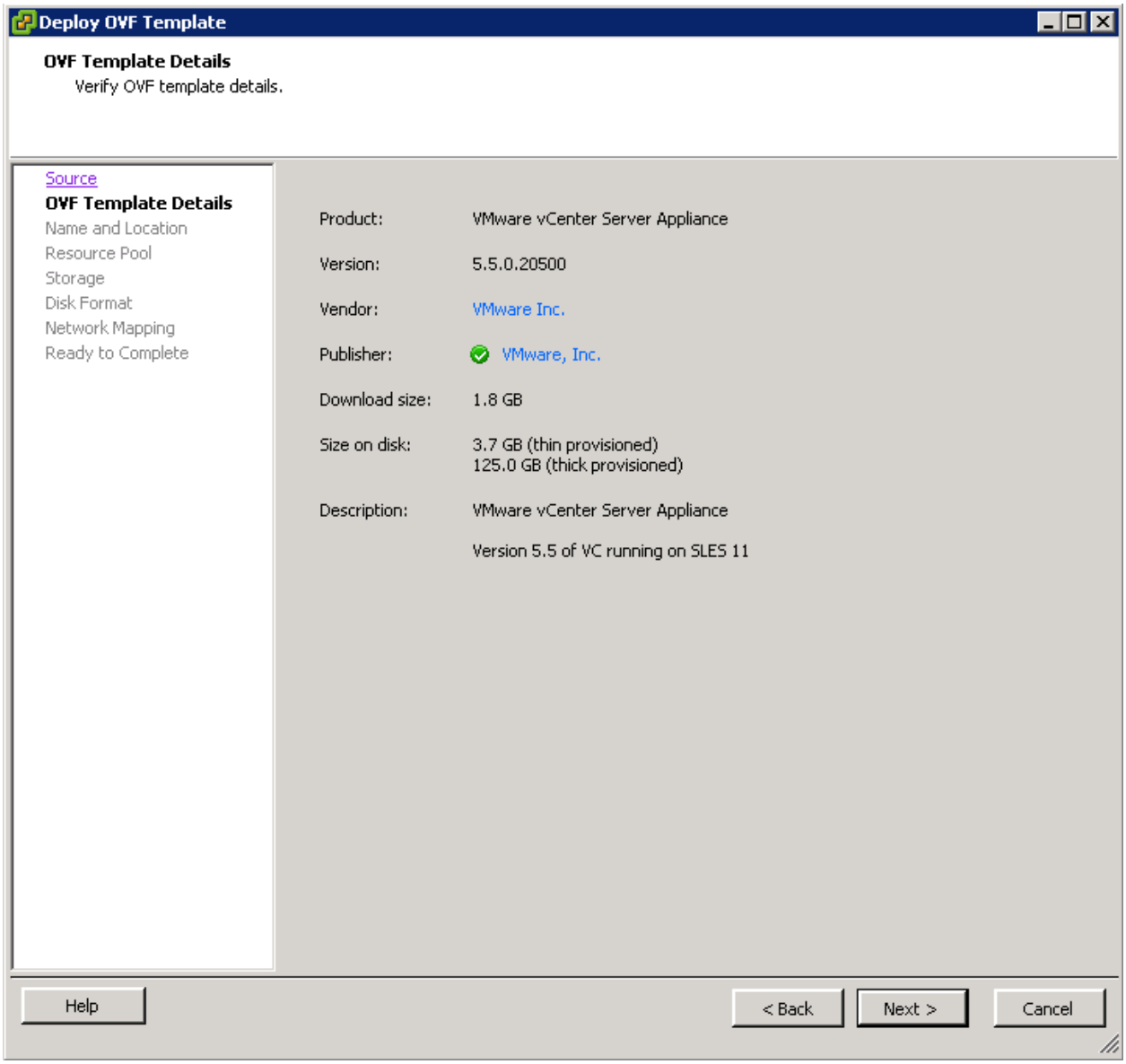
1. From the vSphere 5 download page on the VMware Web site, download the `.OVA` file for the vCenter Server appliance version 5.5 update 2 onto your system.

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.

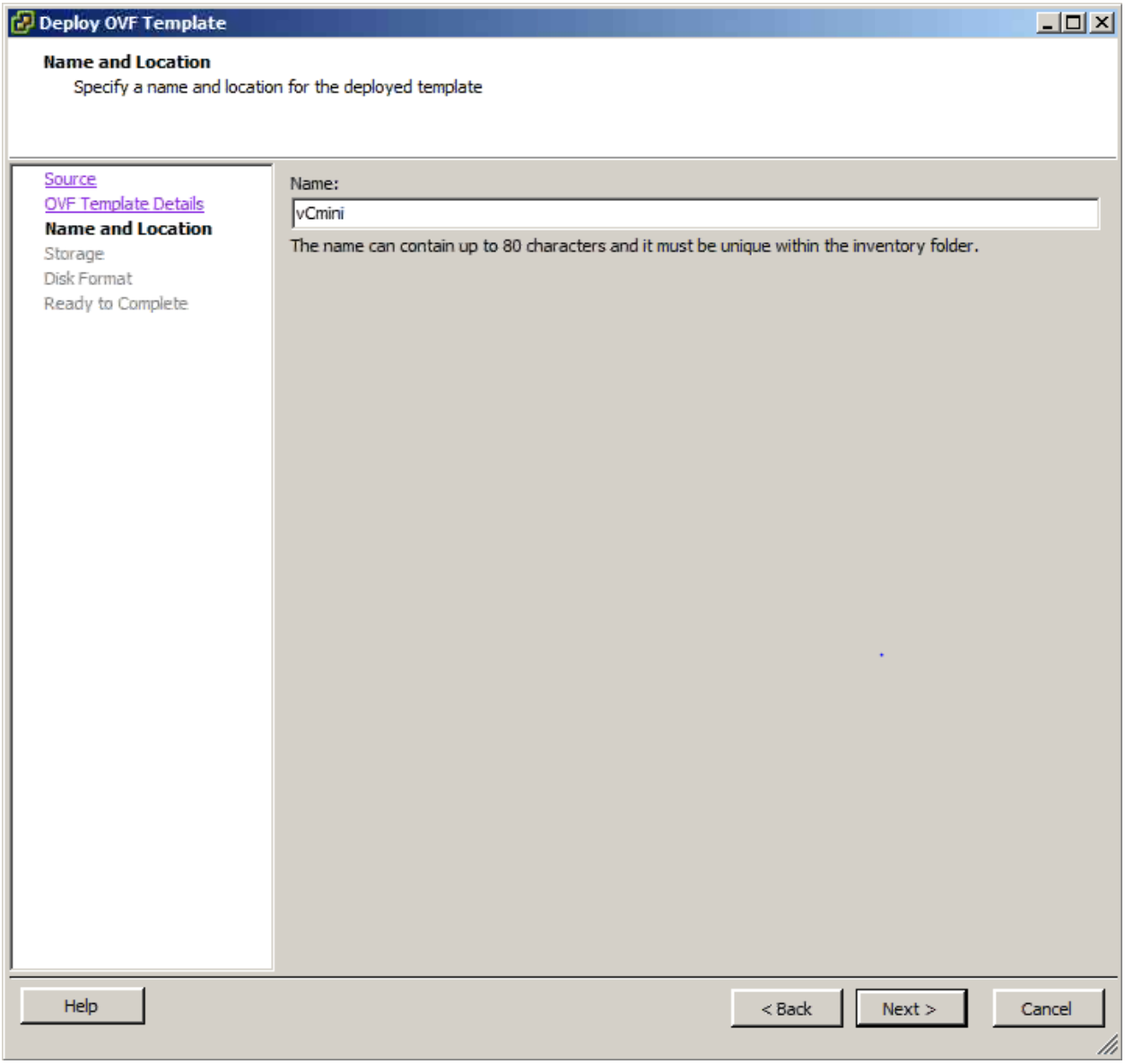


6. Click Next to continue installation.

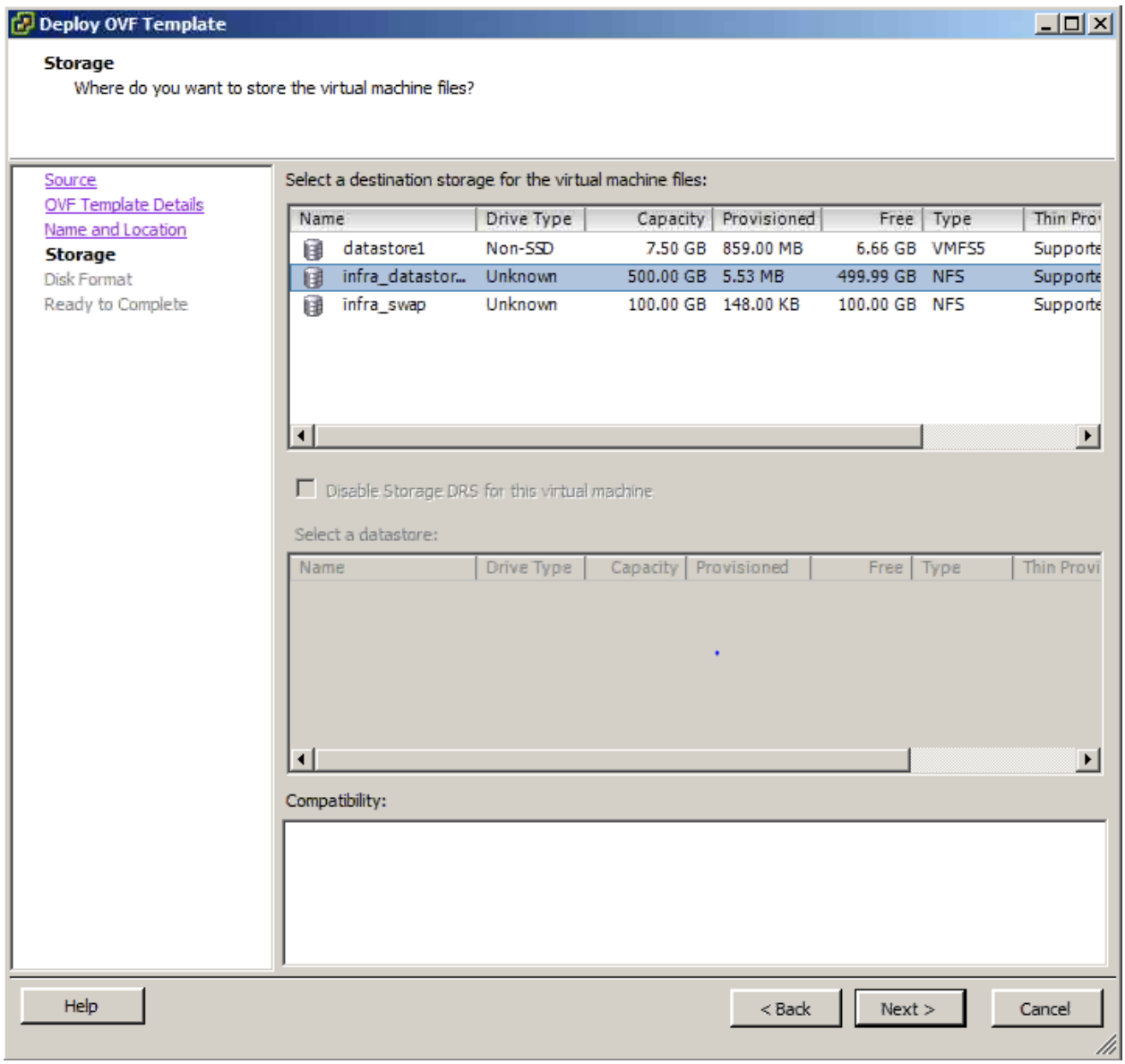


7. Click Next after reviewing the OVF Template Details window.

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

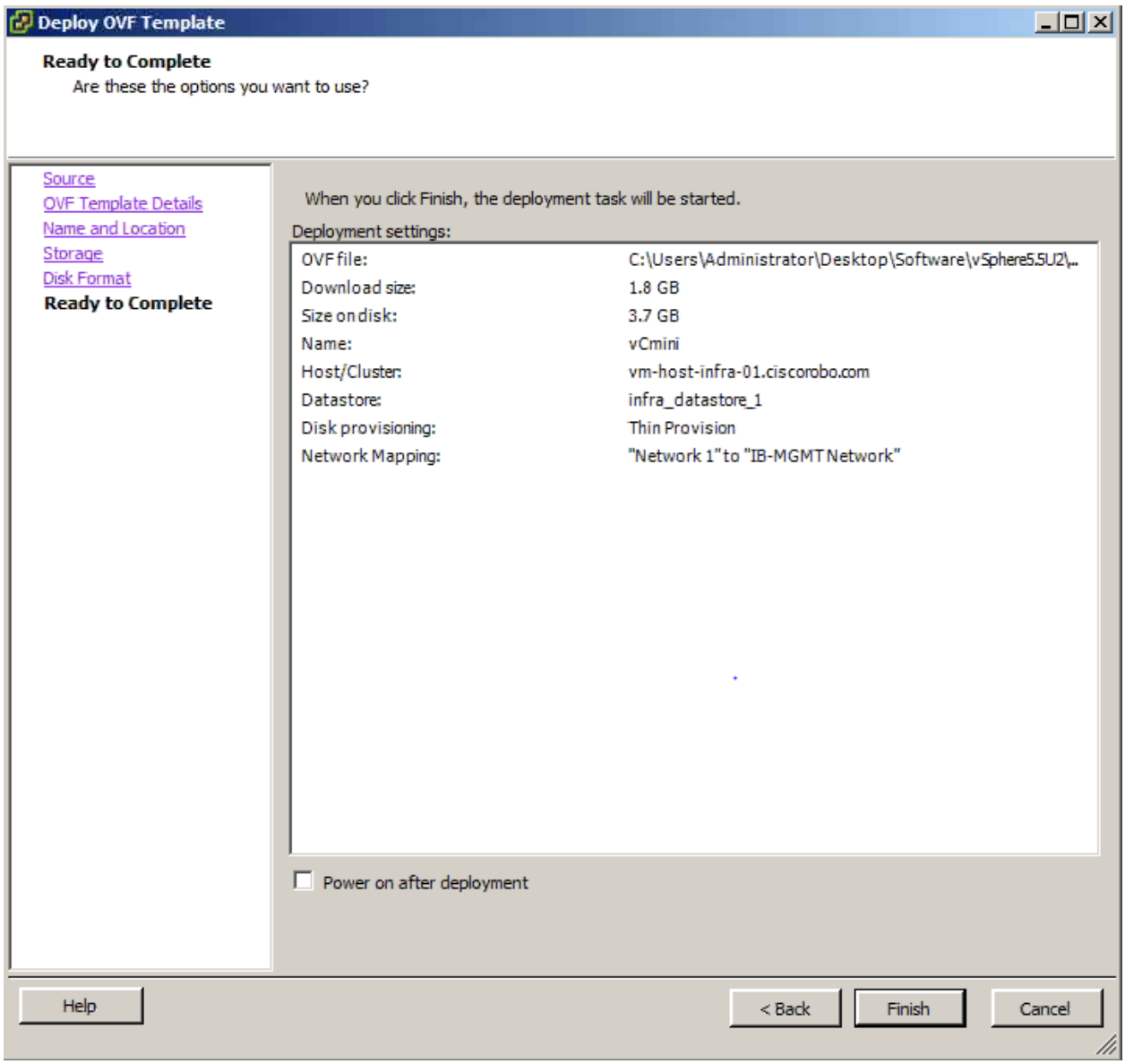


9. Select `infra_datastore_1` as the location for the vCenter VM virtual disks, then click Next to continue.



10. Review the disk format selection, and click Next to continue.

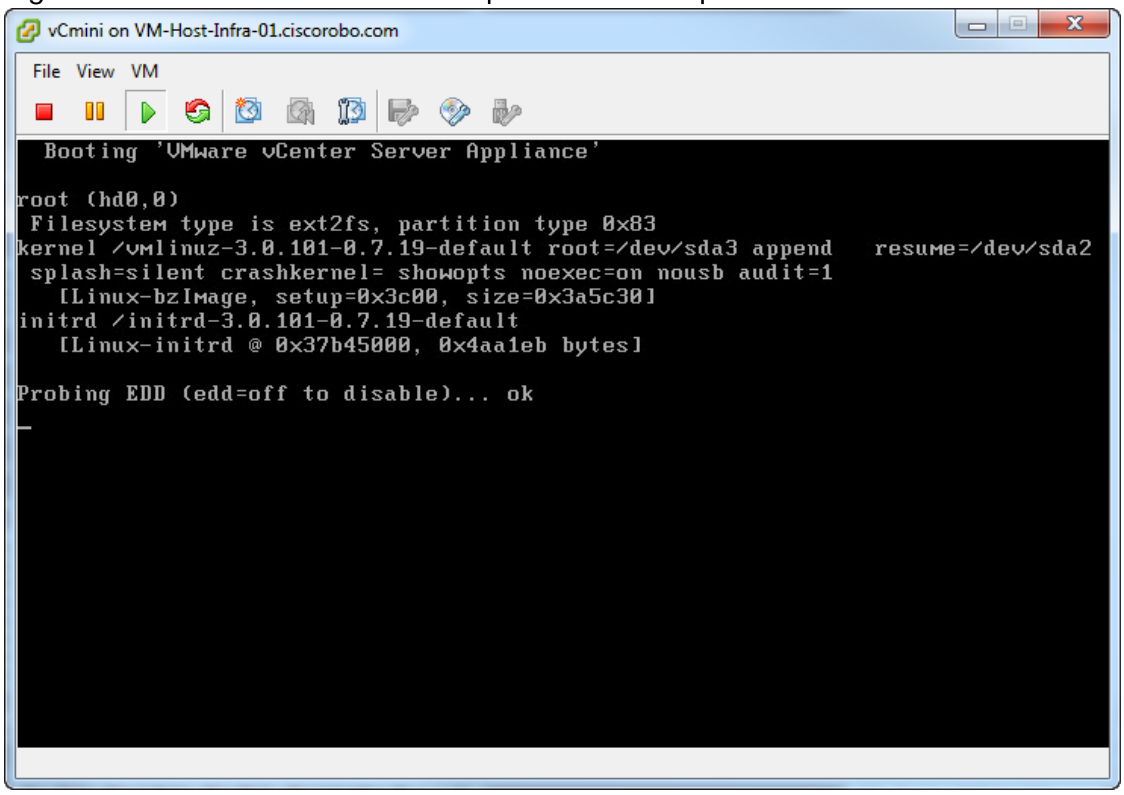
11. Review the installation details, and click Finish to continue.



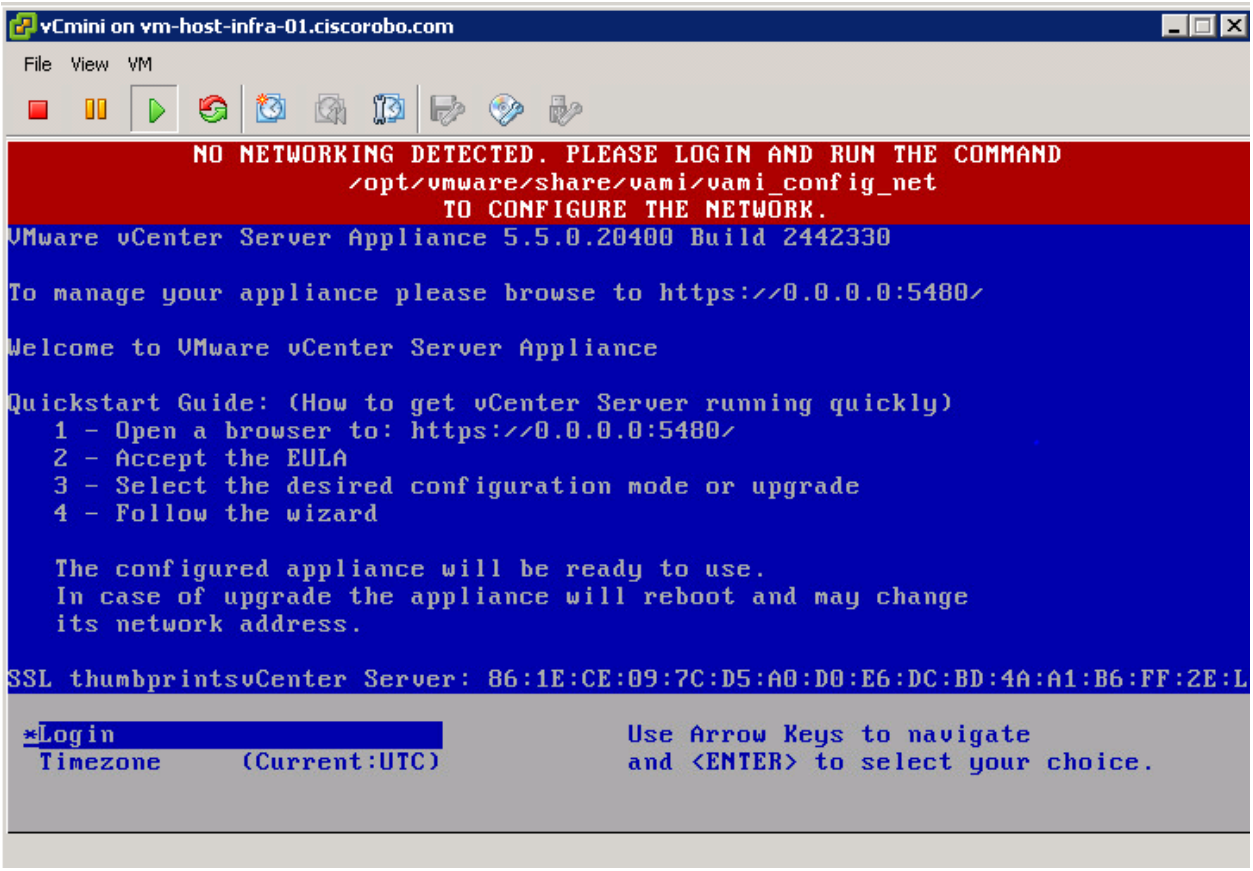
12. After the installation has been completed, click the plus symbol to the left of the host in the left pane of the vSphere Client window.

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 window.



15. Wait for the Virtual Machine to boot.



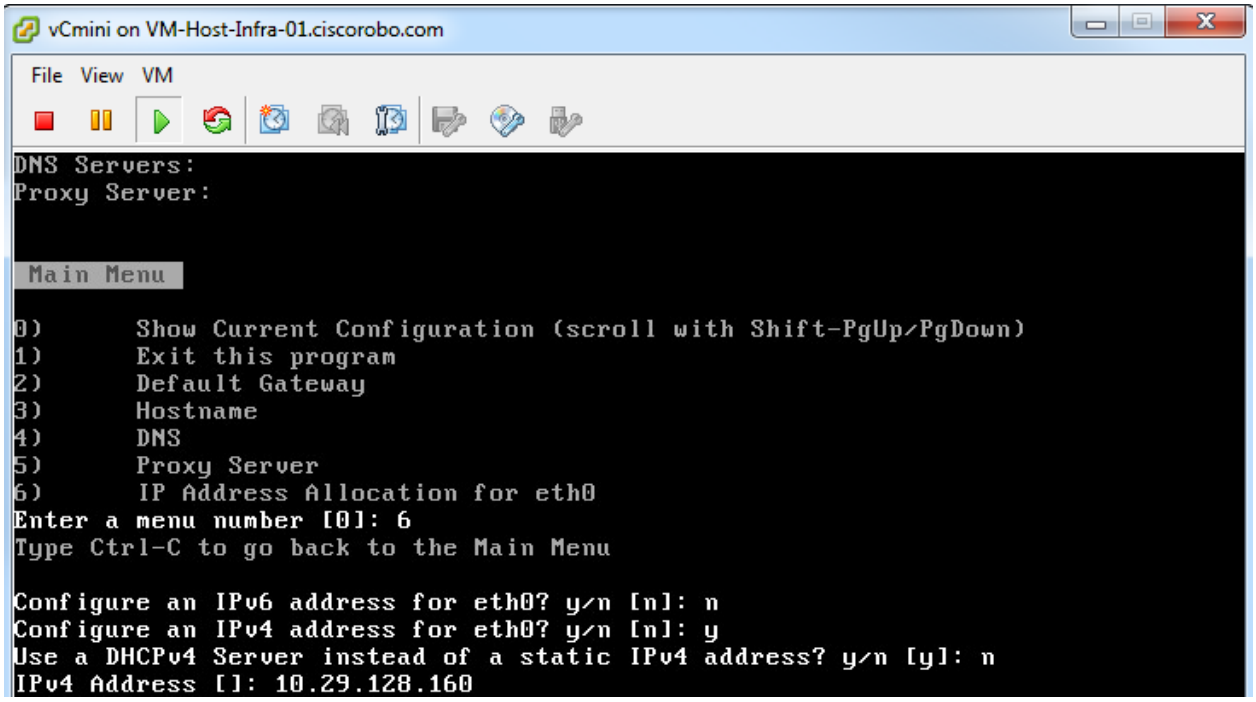
16. The preceding screen is displayed, if the vCenter appliance does not receive an IP address through DHCP. Press Enter to Login.

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 press Enter.



20. To configure the IP address for the vCenter server, type `6` and press Enter.

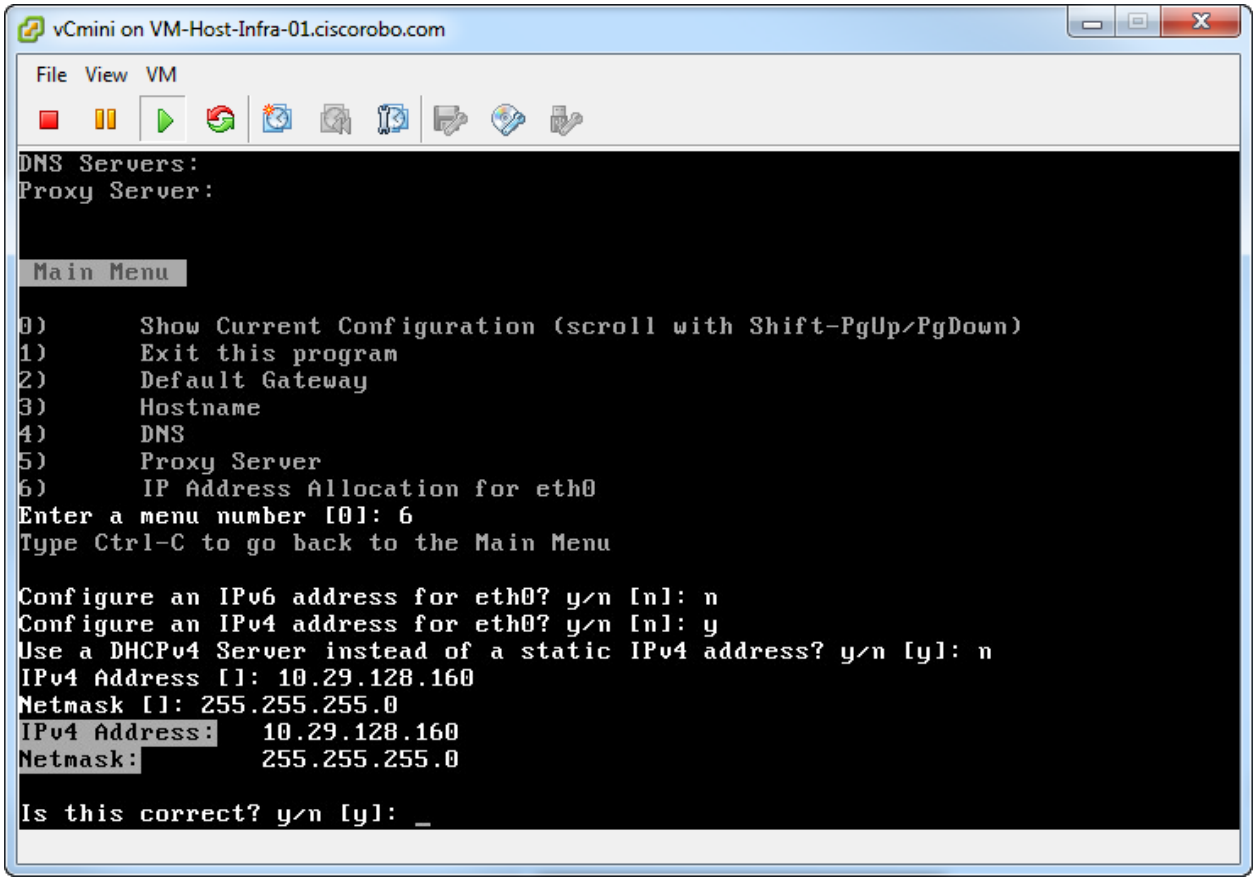
21. To disable IPv6, type `n` and press Enter.

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.

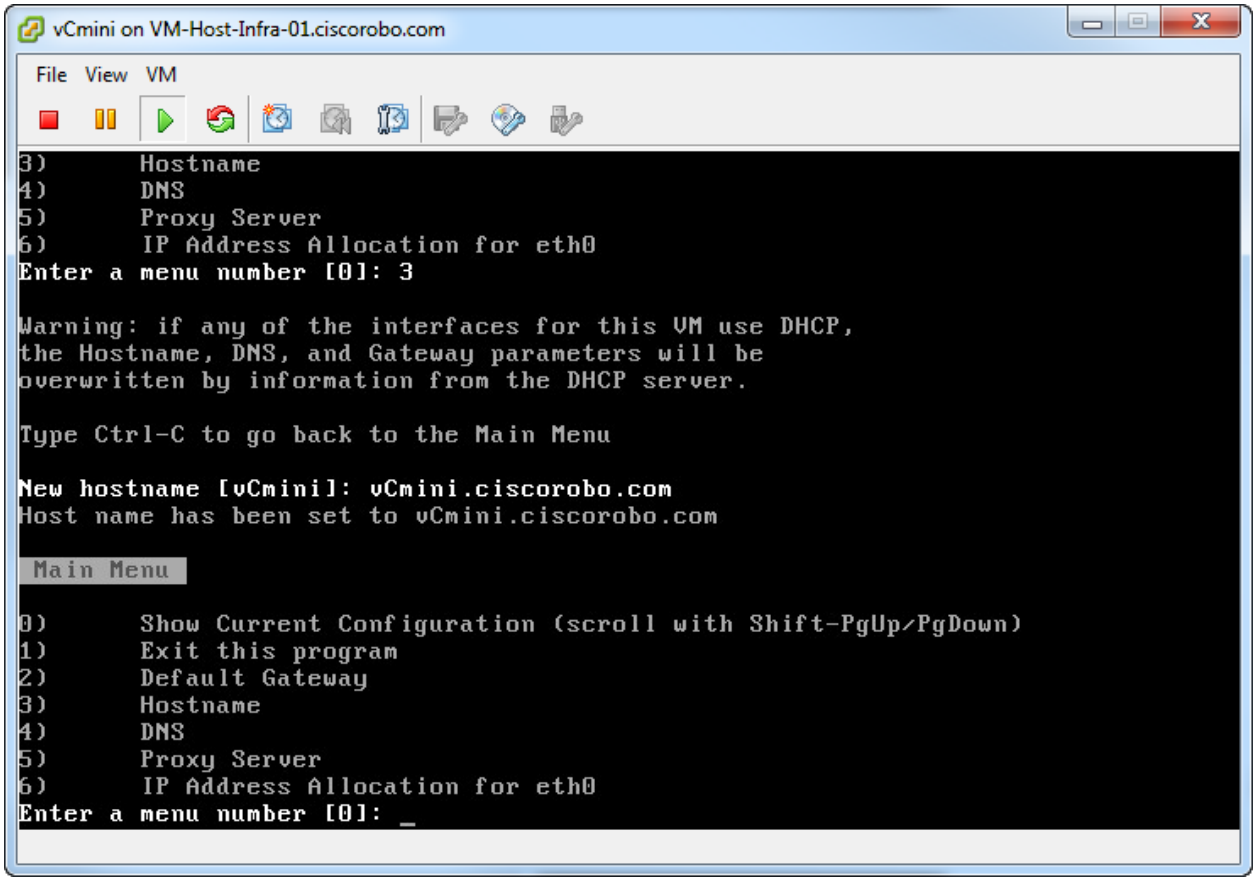
25. Type `<<var_vcenter_netmask>>` and press Enter.



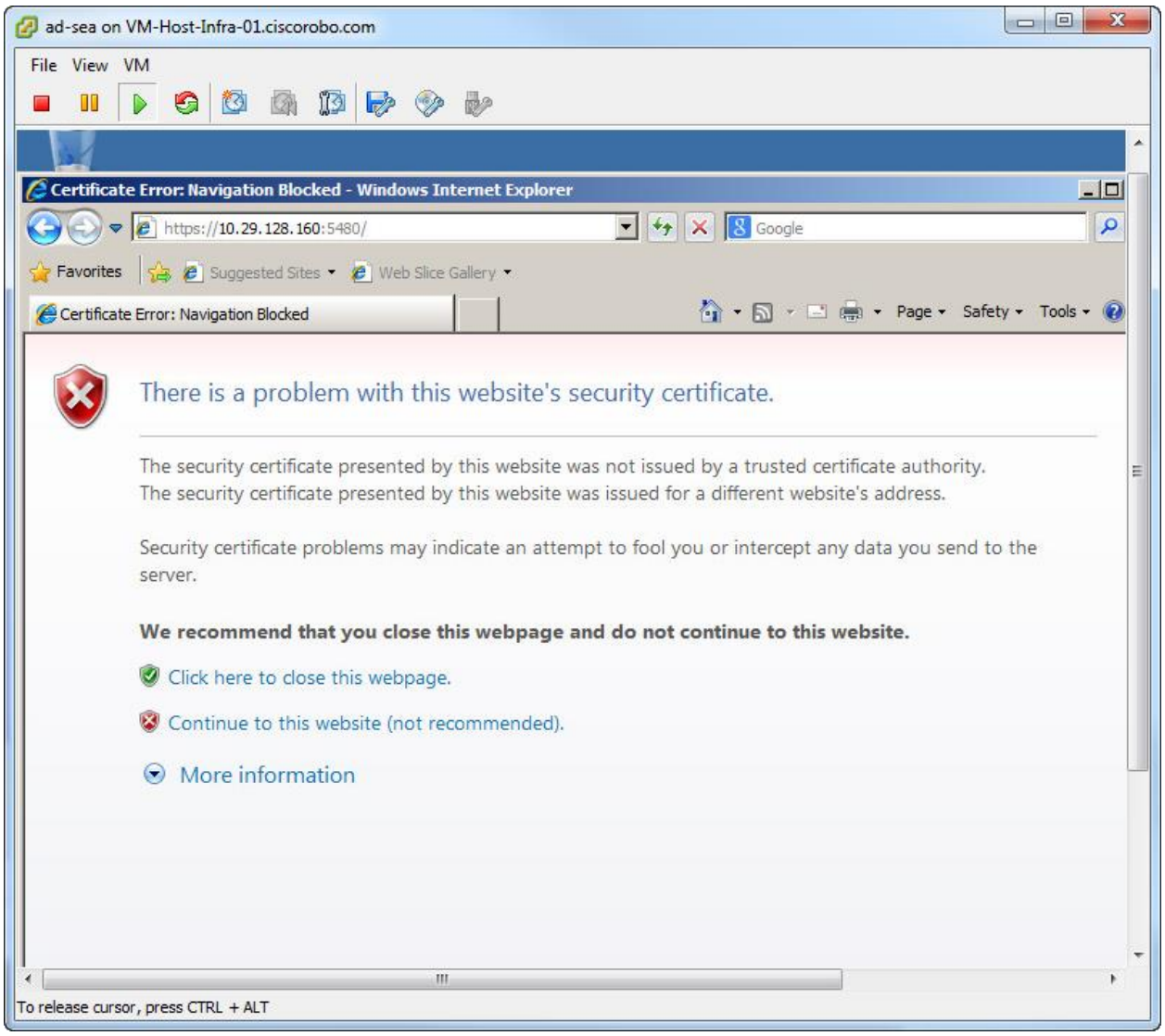
26. Review the IP address and subnet mask. Type `y` and press Enter to complete the configuration.

27. Type 3 and press Enter to enter the Hostname of the vCenter Server.

28. Enter the Hostname and press Enter.

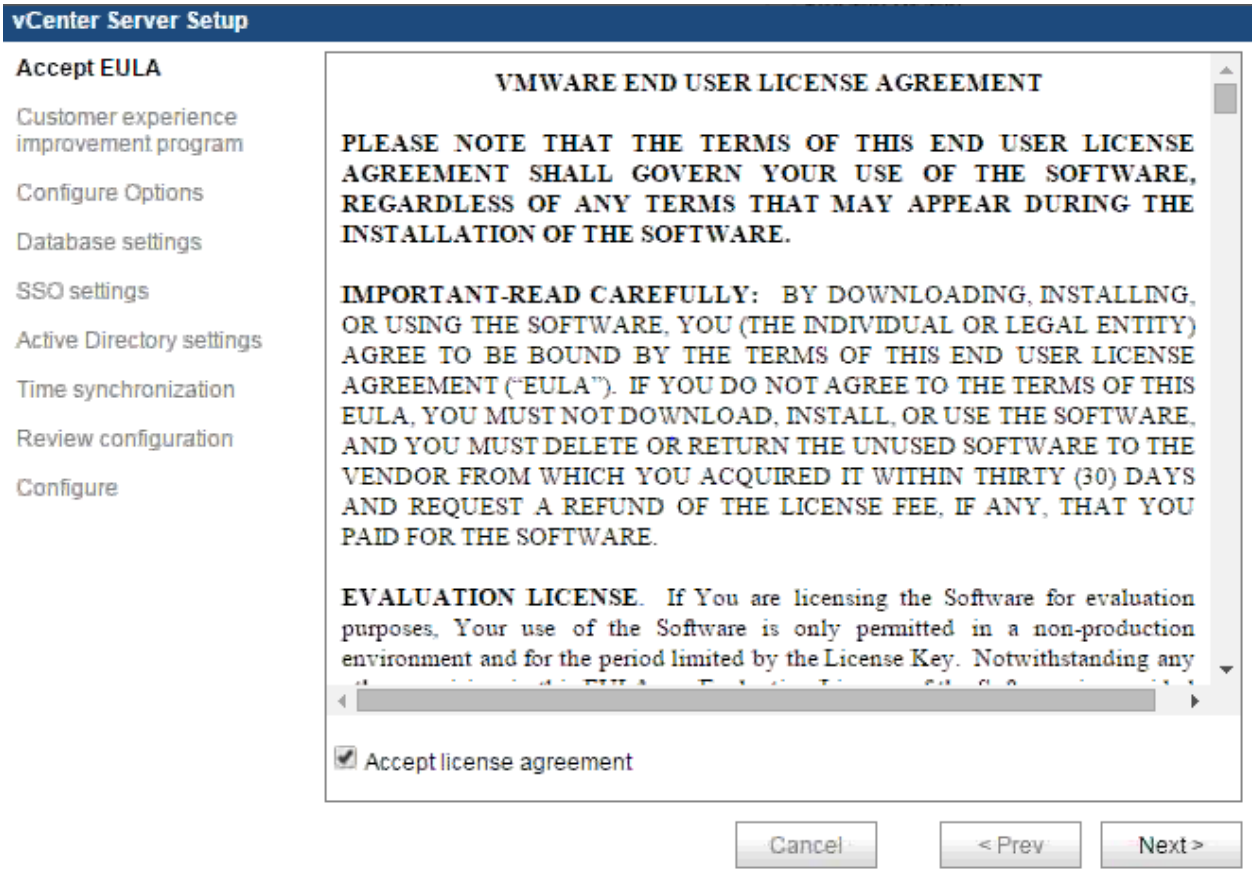


29. Type `2` and press Enter to configure the default gateway IP address.
30. Type `0` and press Enter to associate the default gateway with interface eth0.
31. Enter the default gateway address and press Enter. Just press Enter for the IPv6 Default Gateway.
32. Type `4` and press Enter to configure the DNS information for the vCenter server.
33. Type `<<var_DNS_1_IP>>` and press Enter.
34. Type `<<var_DNS_2_IP>>` and press Enter to accept the configuration changes.
35. Type `0` and review the configuration.
36. Type `1` and press Enter to exit the configuration dialogue.
37. Type `exit` and press Enter to log out.
38. Follow the instructions on the welcome screen to open a browser window to the URL shown.



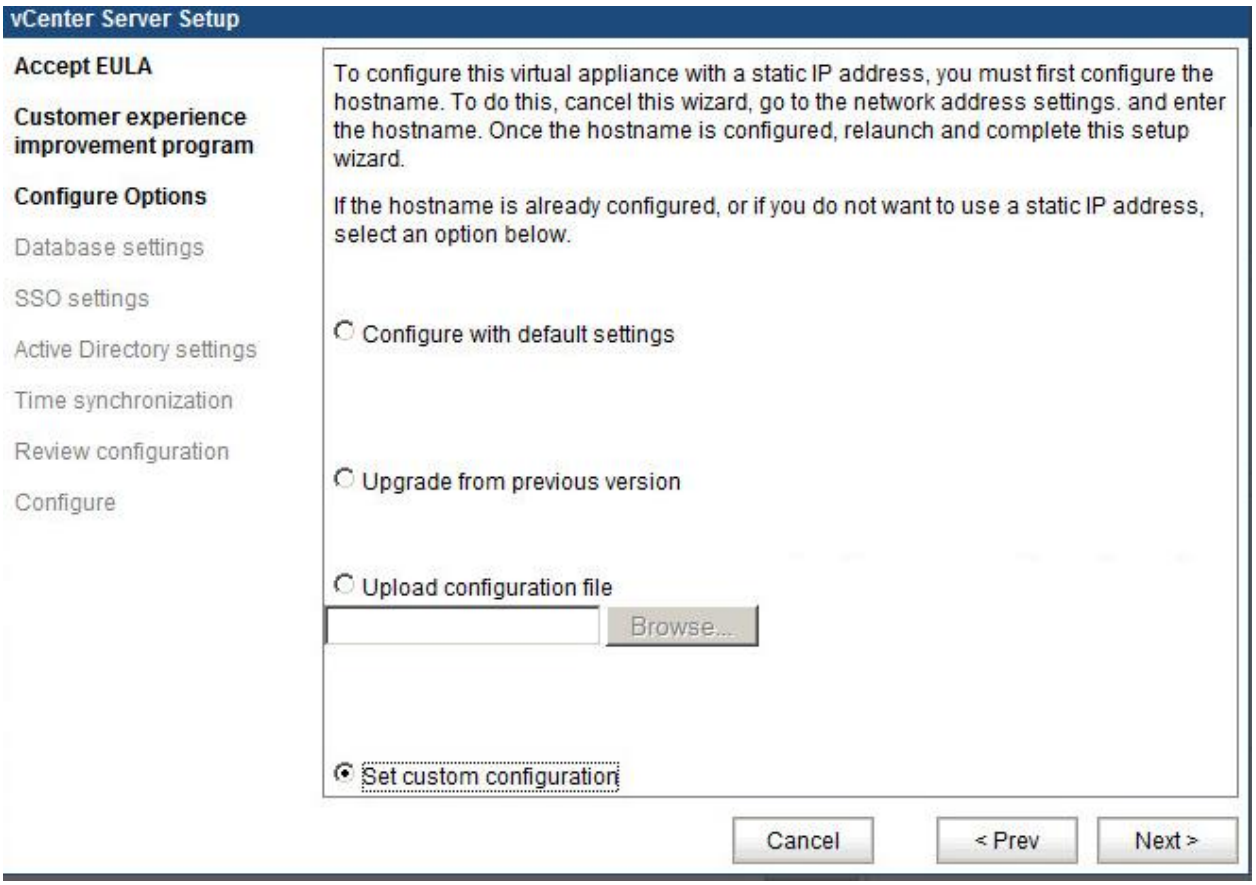
39. Click Continue to this website and enter `root` for the User name and `vmware` for the password. Click Login.

40. Use the checkbox to accept the license agreement and click Next.



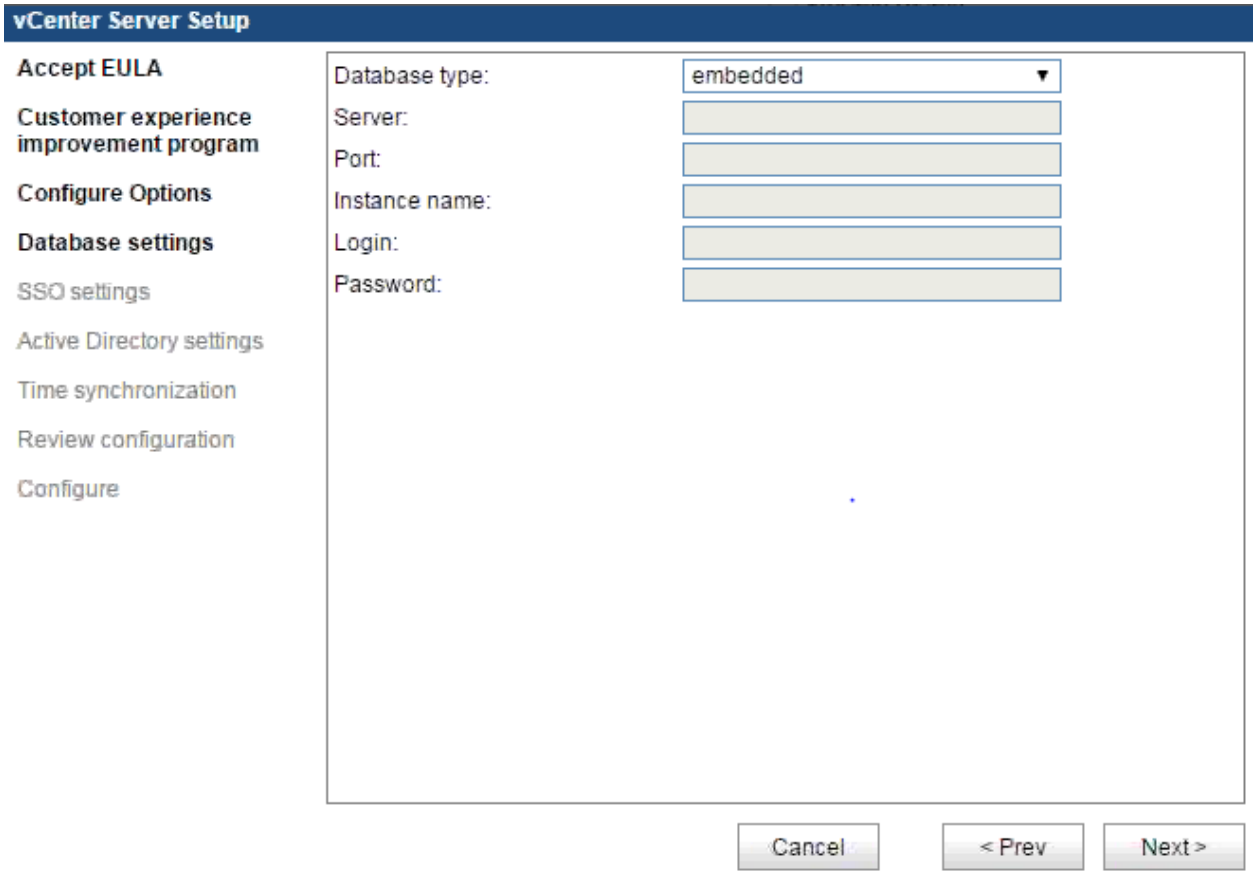
41. Decide whether to enable data collection and click Next.

42. Select Set custom configuration and click Next.

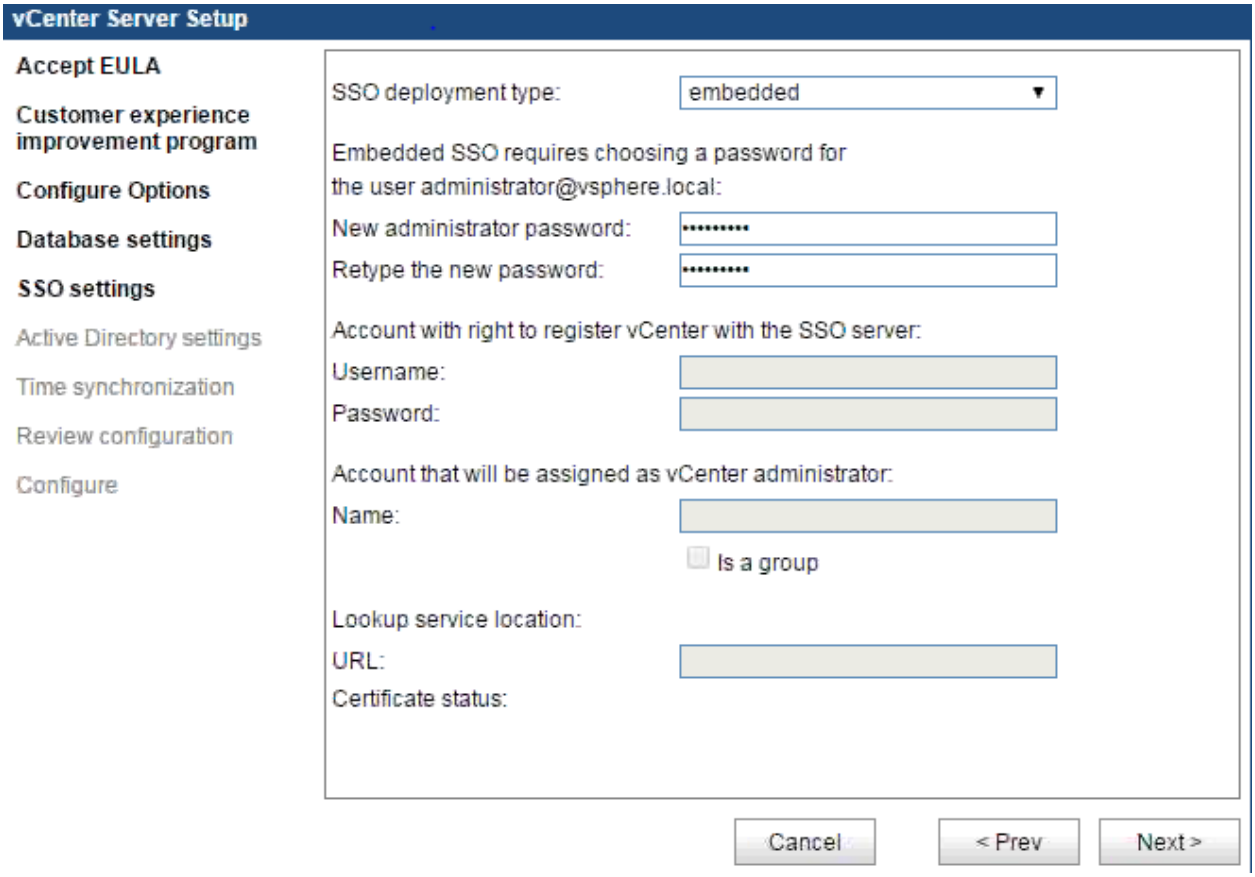


43. Click Next to accept an embedded database.

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

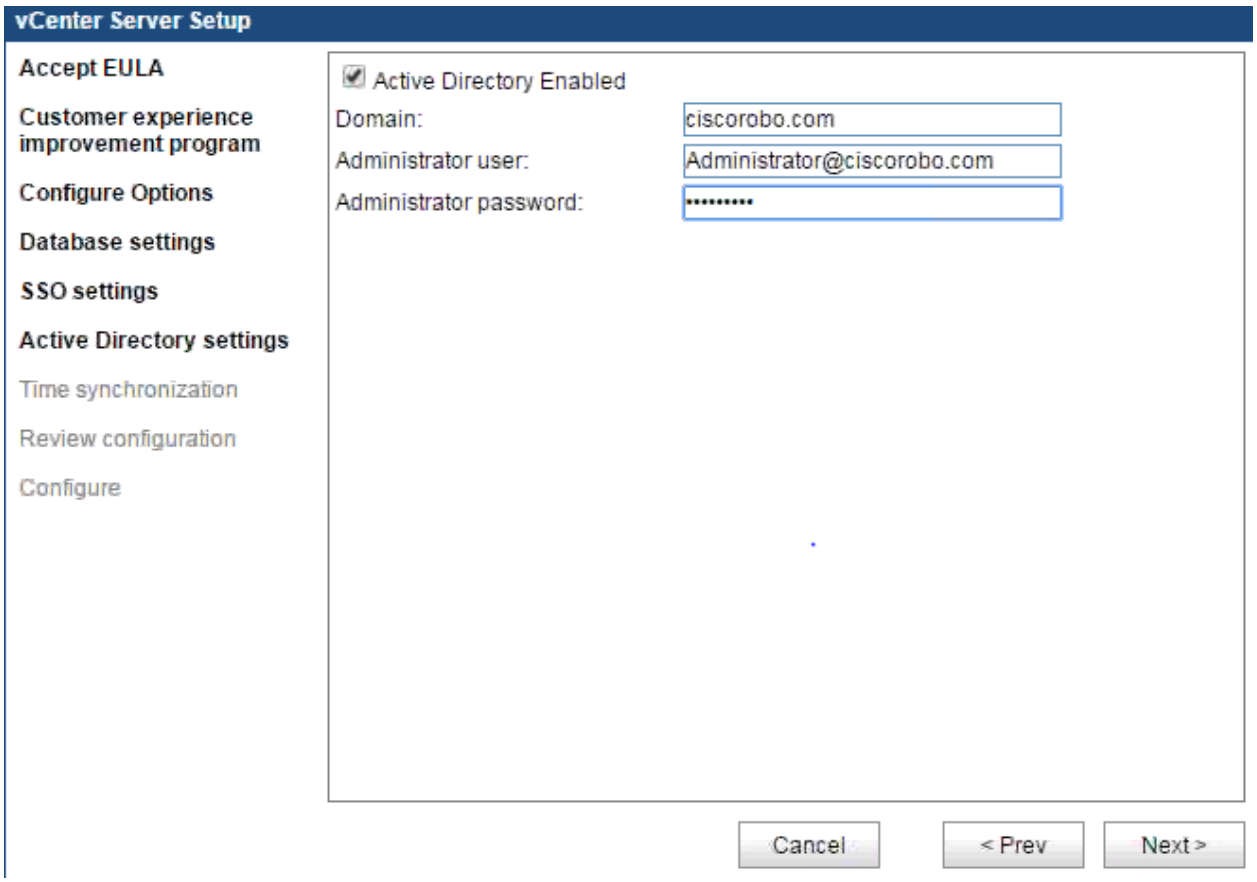


44. Enter and retype the password for the administrator@vsphere.local user in the password field, click Next to accept an embedded SSO deployment.

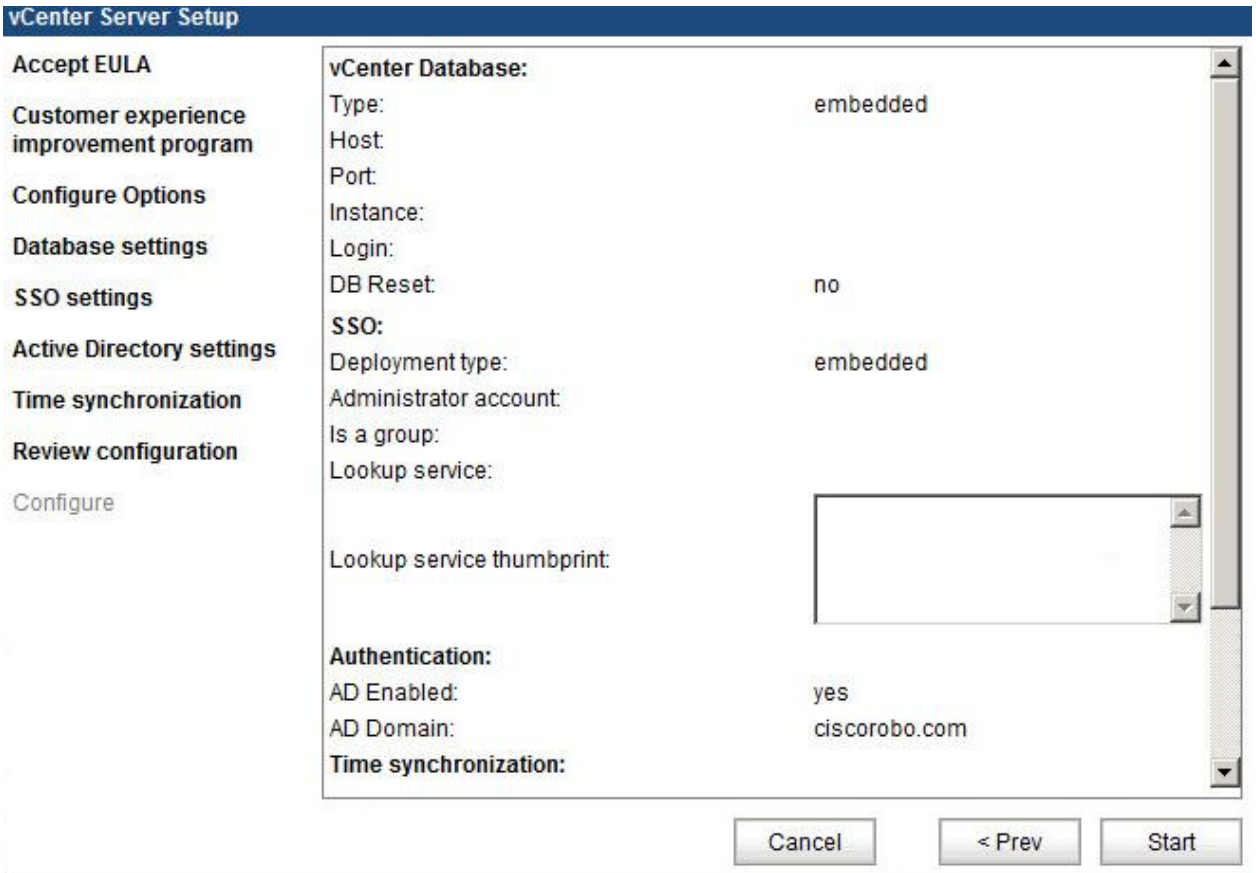


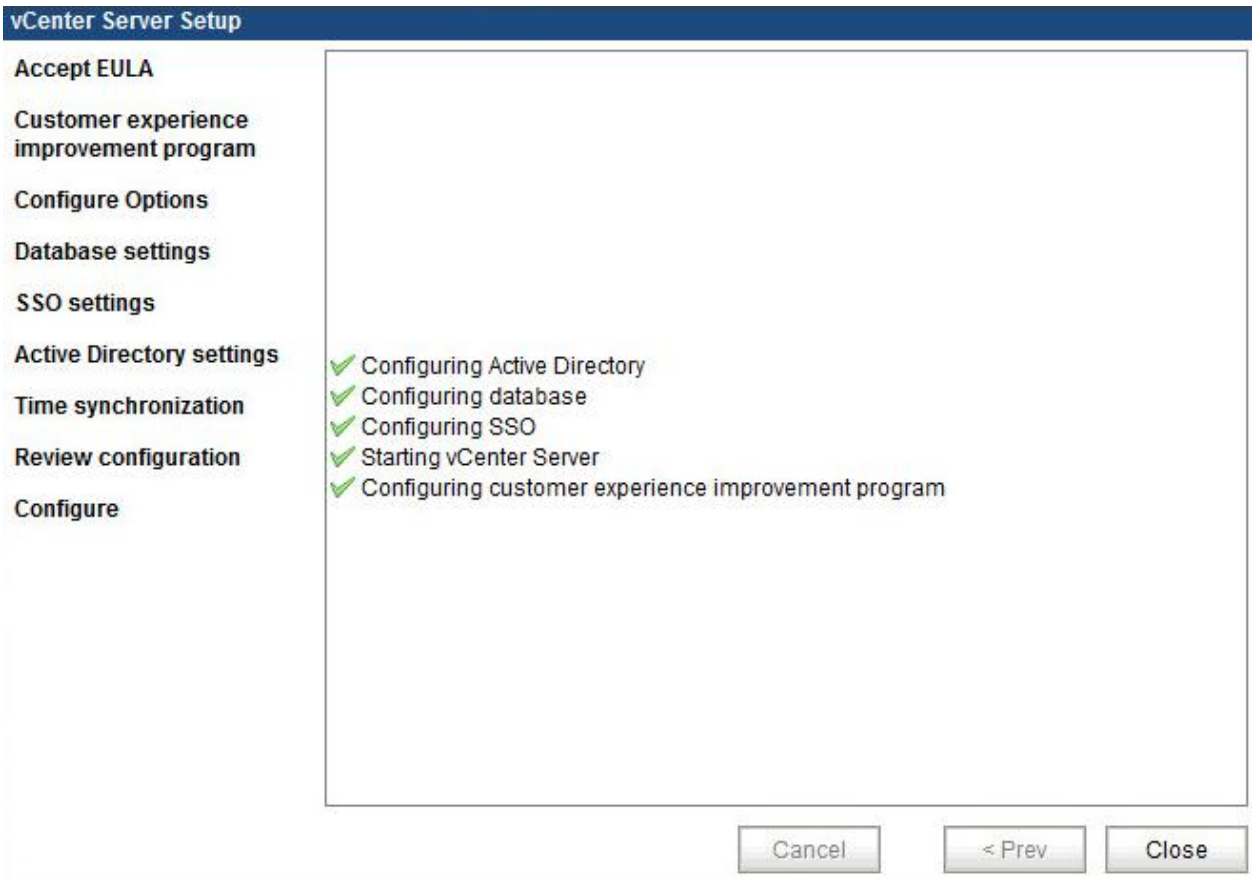
45. Select the Active Directory Enabled checkbox to configure Active Directory based user permissions.

46. Enter the domain, administrator user name, and administrator password in the fields then click Next to continue.

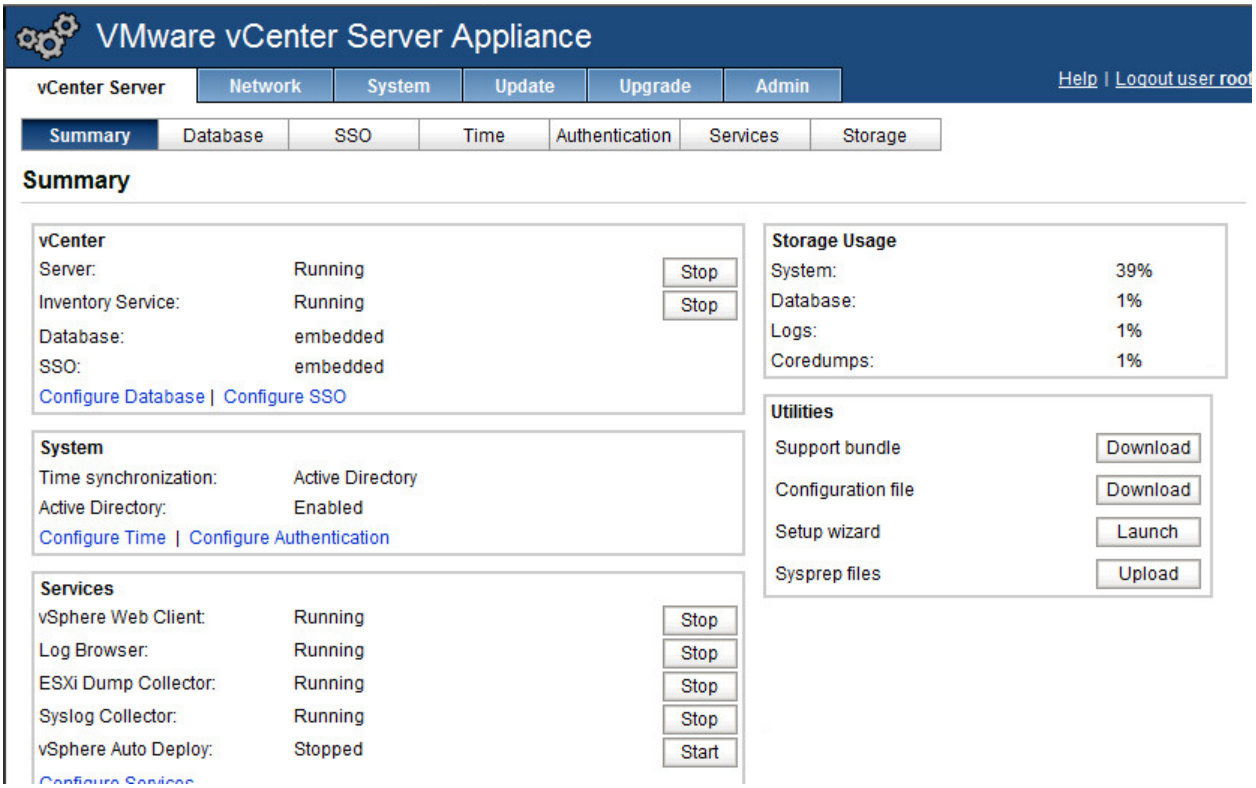


47. Review the configuration settings and click Start to complete the configuration. The vCenter server will create all of the necessary configurations and database structures specified in the preceding section. This step may require several minutes. Click Close after the configuration has completed.

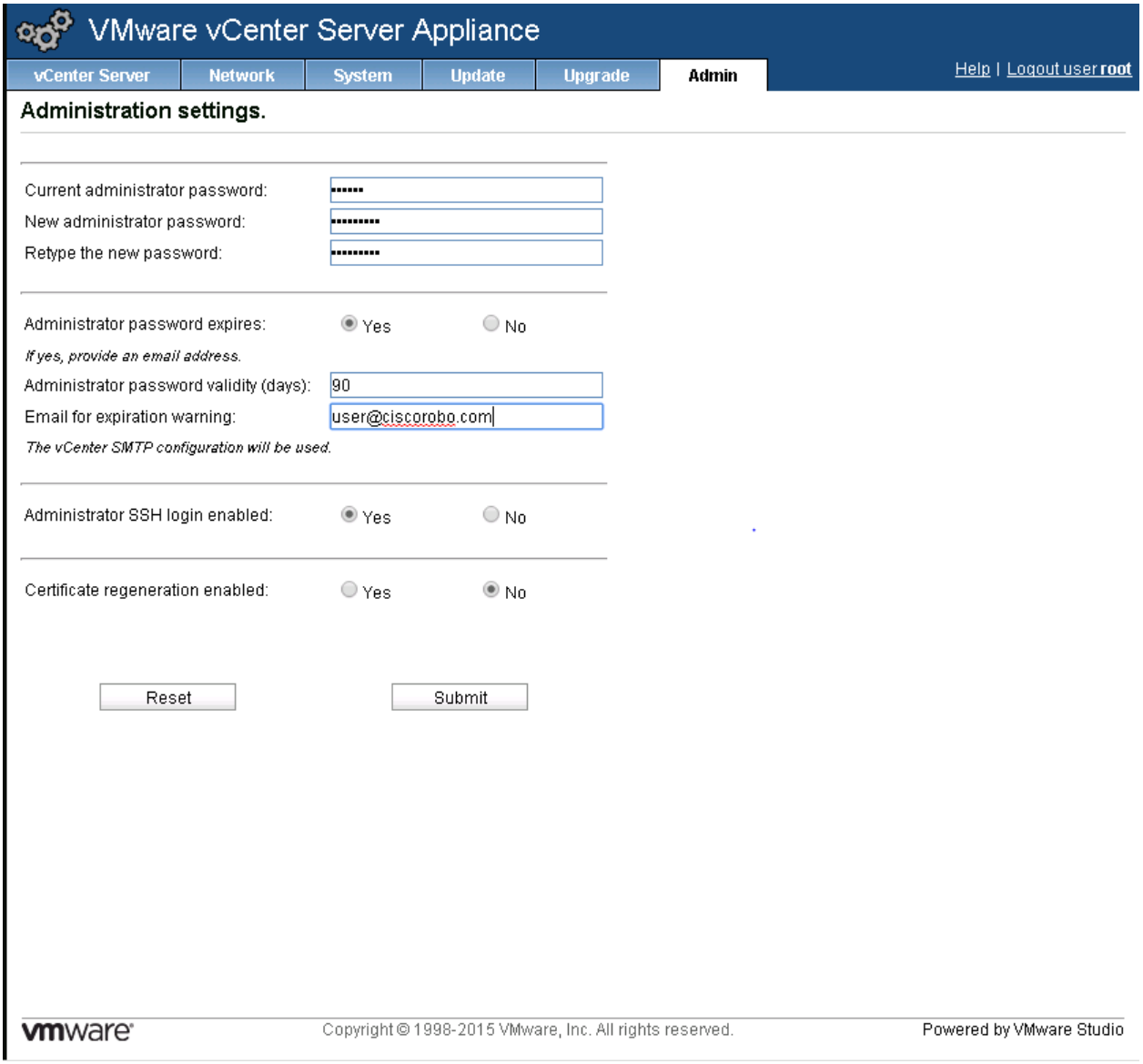

vCenter Server Setup
Accept EULA
Customer experience improvement program
Configure Options
Database settings
SSO settings
Active Directory settings
Time synchronization
Review configuration
Configure
vCenter Database:
Type: embedded
Host:
Port:
Instance:
Login:
DB Reset: no
SSO:
Deployment type: embedded
Administrator account:
Is a group:
Lookup service:
Lookup service thumbprint:
Authentication:
AD Enabled: yes
AD Domain: ciscorobo.com
Time synchronization:
Cancel
< Prev
Start


vCenter Server Setup
Accept EULA
Customer experience improvement program
Configure Options
Database settings
SSO settings
Active Directory settings
Time synchronization
Review configuration
Configure
Configuring Active Directory
Configuring database
Configuring SSO
Starting vCenter Server
Configuring customer experience improvement program
Cancel
< Prev
Close

48. The VMware vCenter Server Appliance Summary screen will appear. Verify that vCenter Server is running.



49. Click the Admin tab. Change the root user (administrator) password and enable SSH login and the password expiry settings. Click Submit.

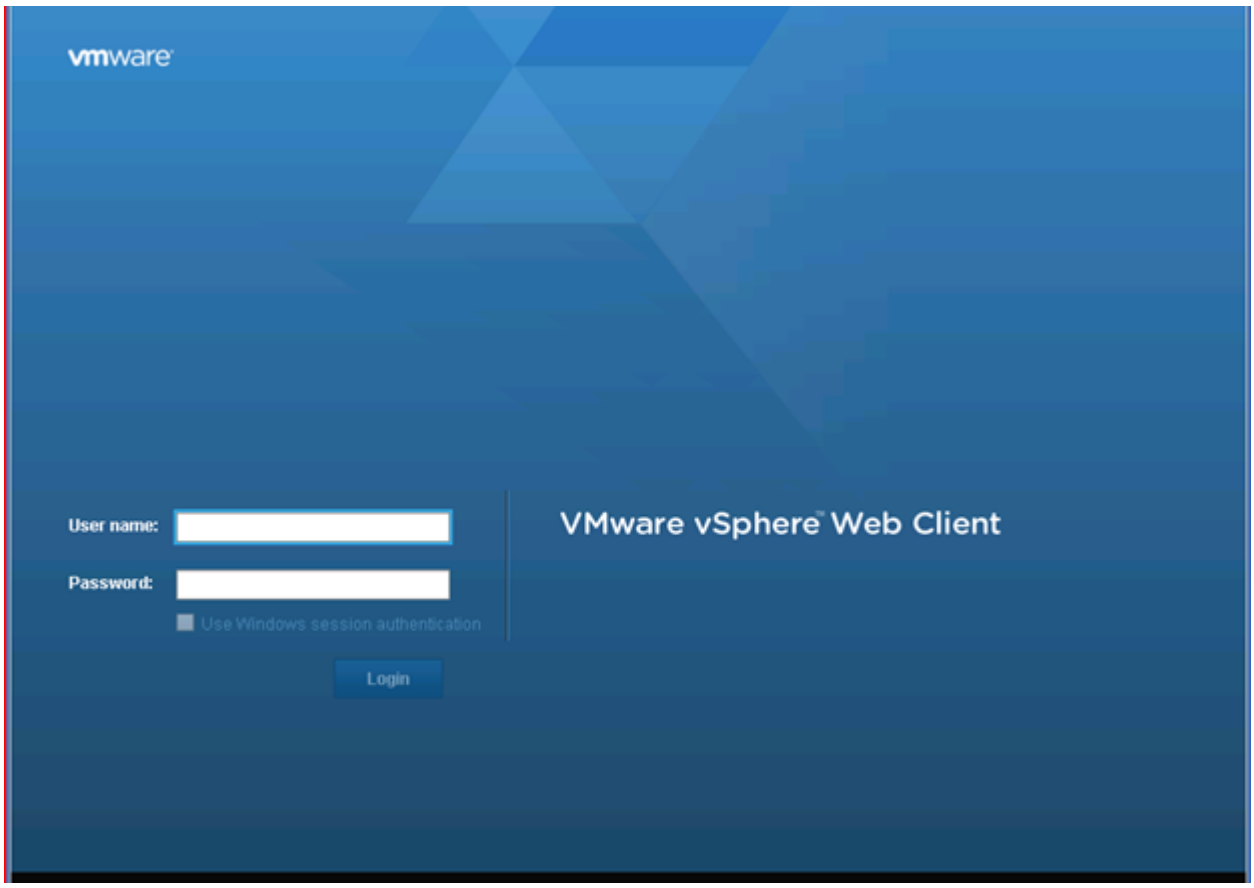


50. Log out of the VMware vCenter Server Appliance interface.

Log in to the vSphere Web Client

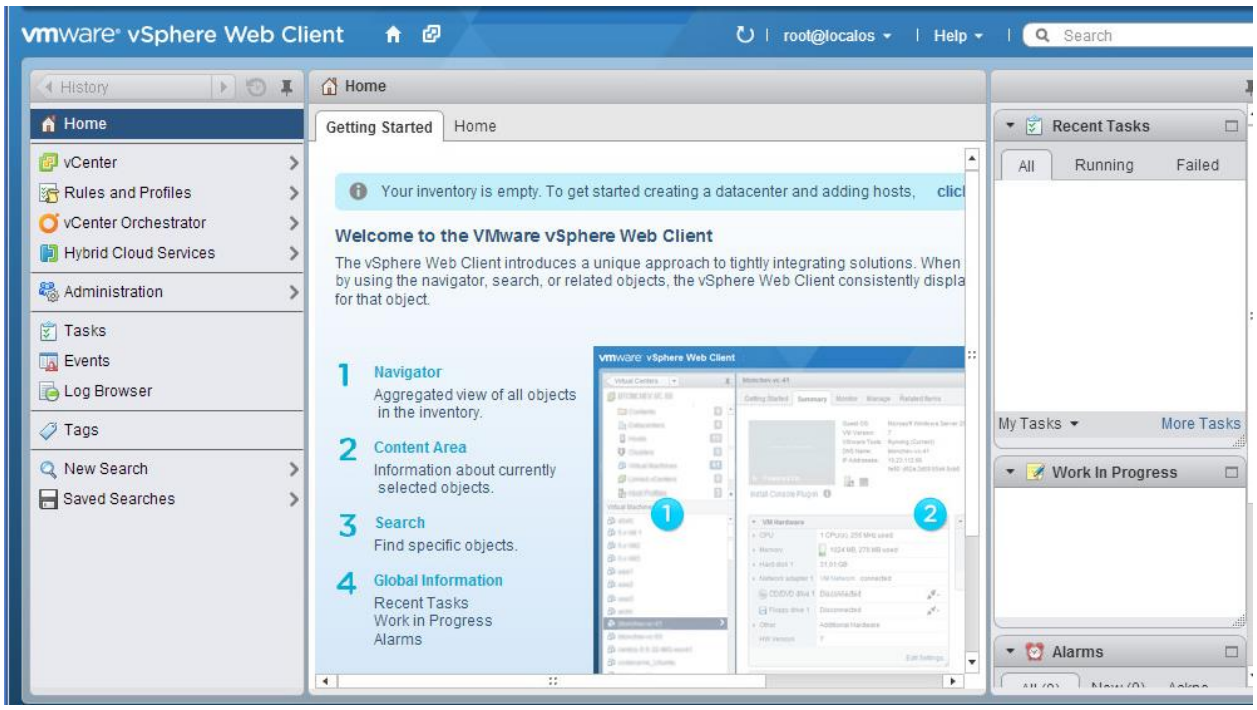
1. Using a web browser, navigate to `https://<<var_vcenter_ip>>`.

2. Click Log in to vSphere Web Client.

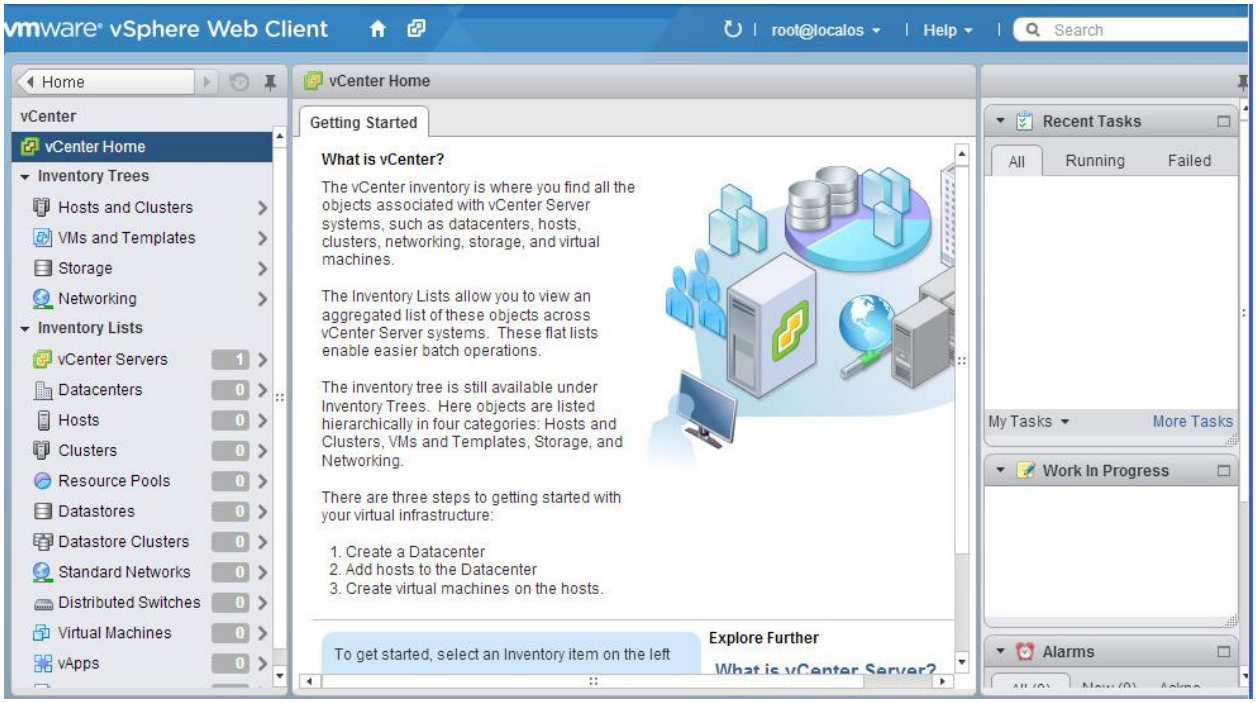


3. If prompted, download and run the VMWare Remote Console Plug-in. Reconnect to the VMware vSphere Web Client login page.

4. Log in using the root user name and password.

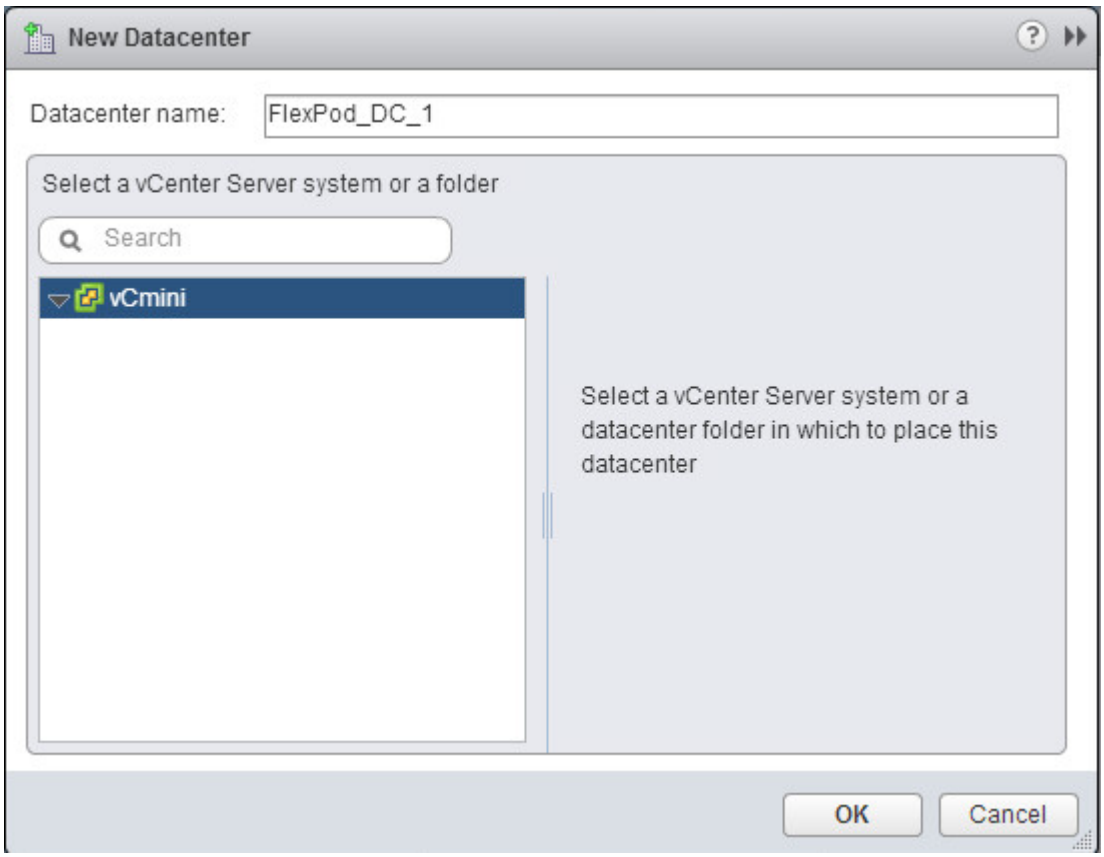


5. Click the vCenter link on the left panel.



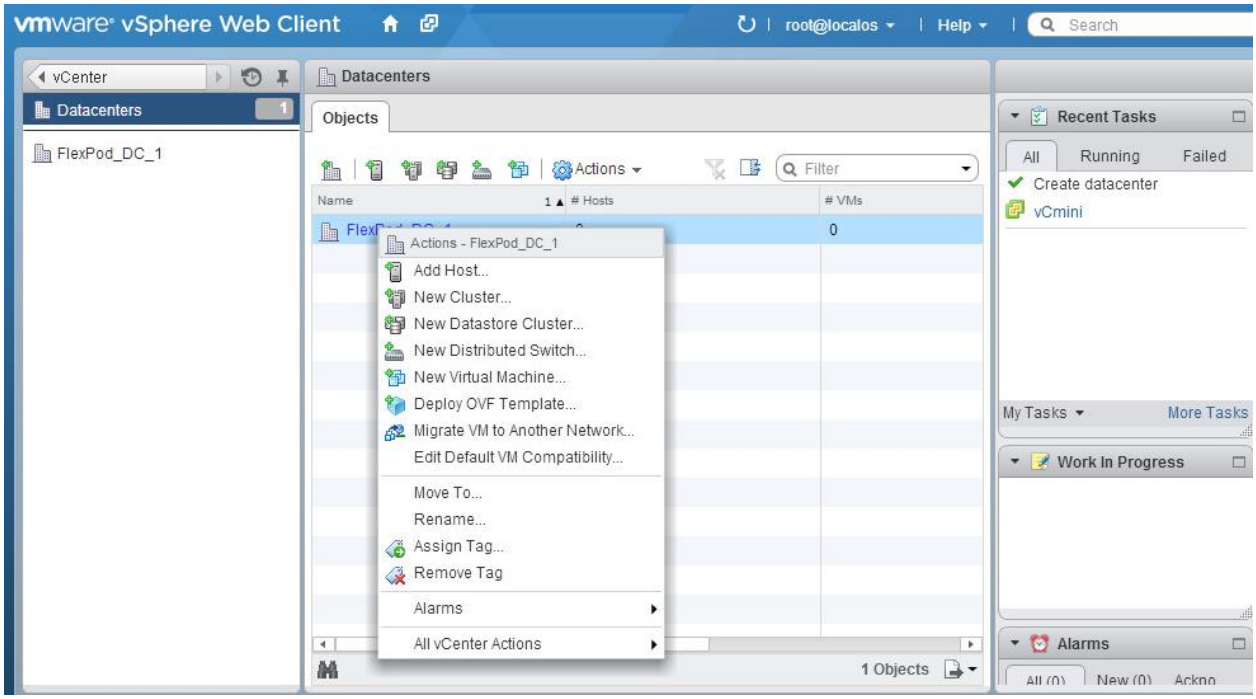
6. Click the Datacenter link on the left panel.

7. To create a Datacenter, click the icon in the center pane that 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.

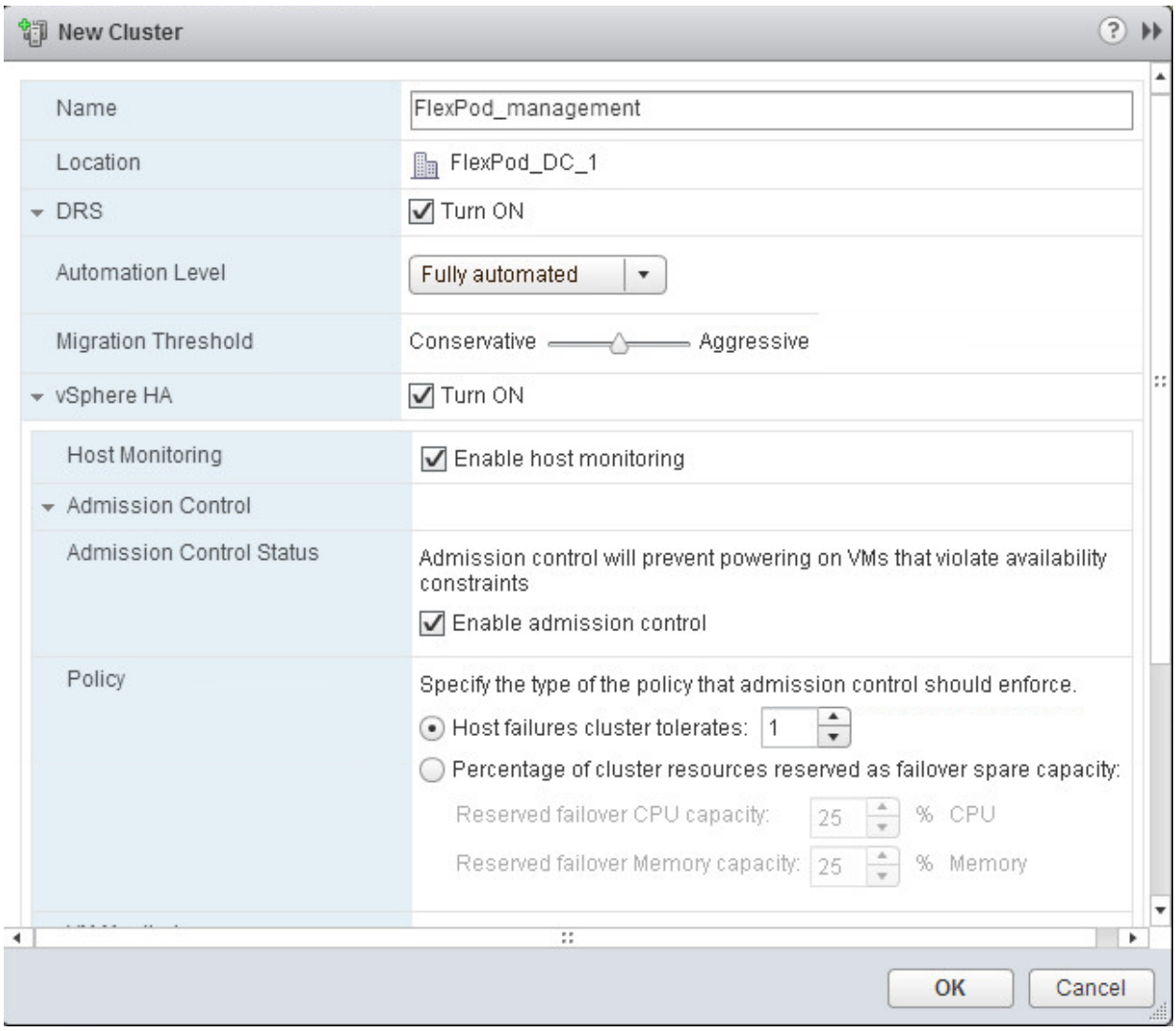


10. Right-click Datacenters > FlexPod_DC_1 in the list in the center pane, then click New Cluster.

11. Name the cluster FlexPod_Management. Name the cluster Site-XX if using a centralized vCenter.

12. Select the checkbox to turn on DRS. Retain the default values.

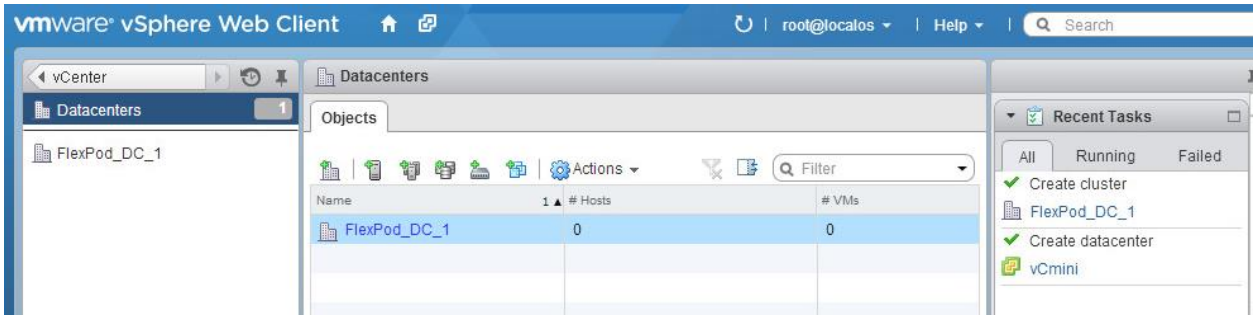
13. Select the checkbox to turn on vSphere HA. Retain the default values.



Note: If mixing Cisco UCS B or C-Series M3 and M4 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.

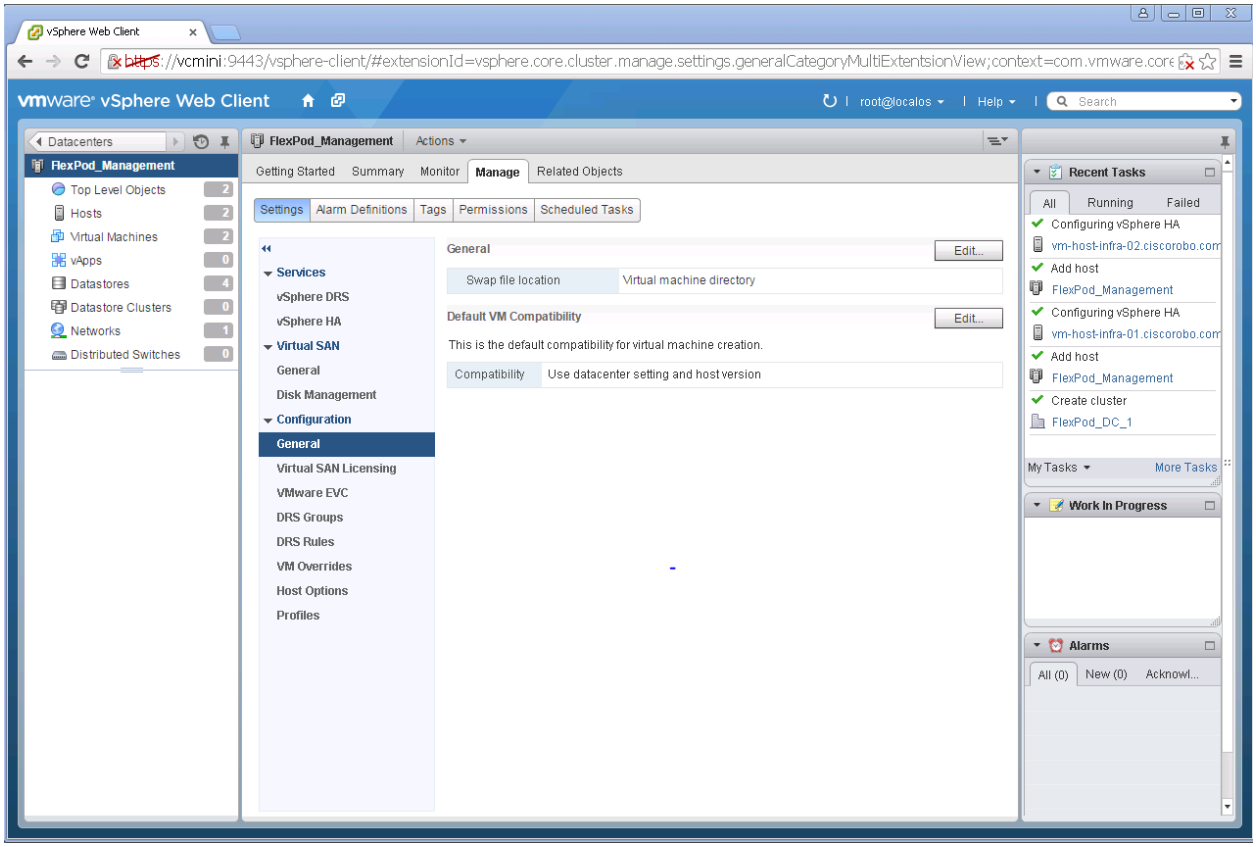


16. Click the Related Objects tab.

17. Click the Clusters tab.

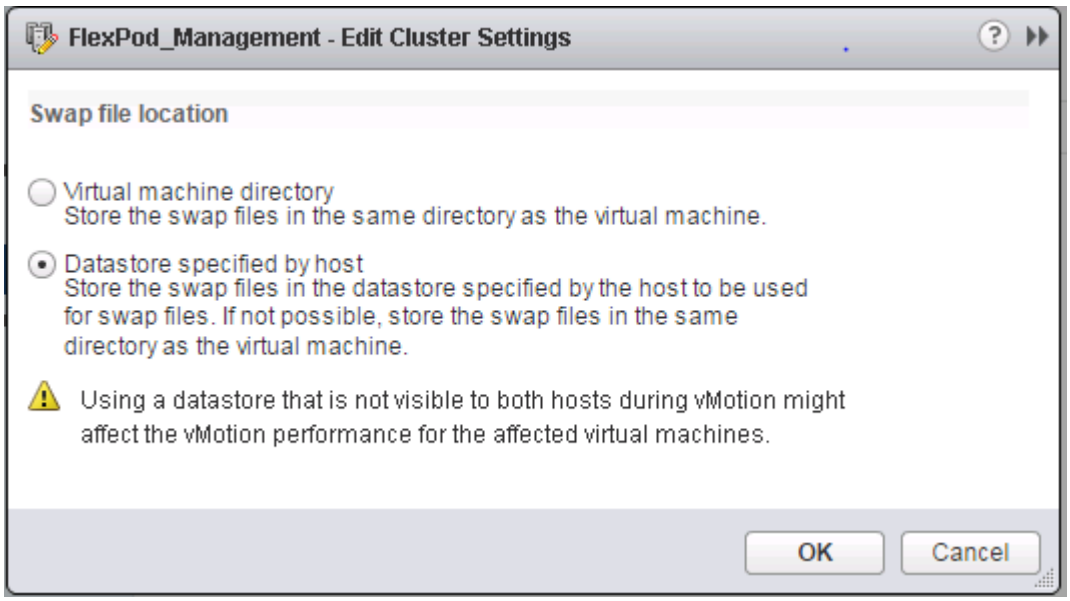
18. Click the FlexPod_Management (or Site-XX) cluster in the center pane.

19. Right-click the FlexPod_Management (or Site-XX) cluster in the left pane and select Settings.

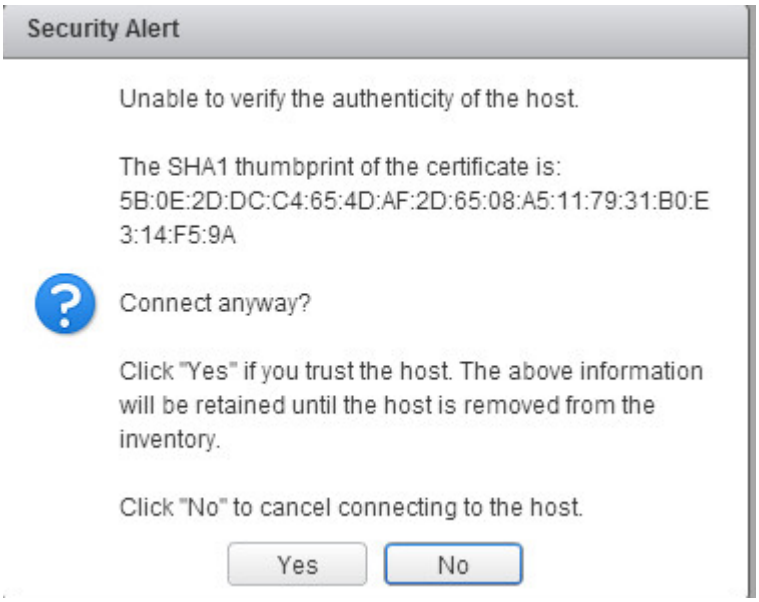


20. In the center pane click General under Configuration then click the Edit button on the right to change the Swap file location.

21. Select Datastore specified by host and click OK.



22. Right-click FlexPod_Management (or Site-XX) in the left pane, and click Add Host.
23. Type `<<var_esx_host_1_ip>>` or the ESXi Host 1 hostname and click Next.
24. Type `root` as the user name and `<<var_esx_host_password>>` as the password. Click Next to Continue

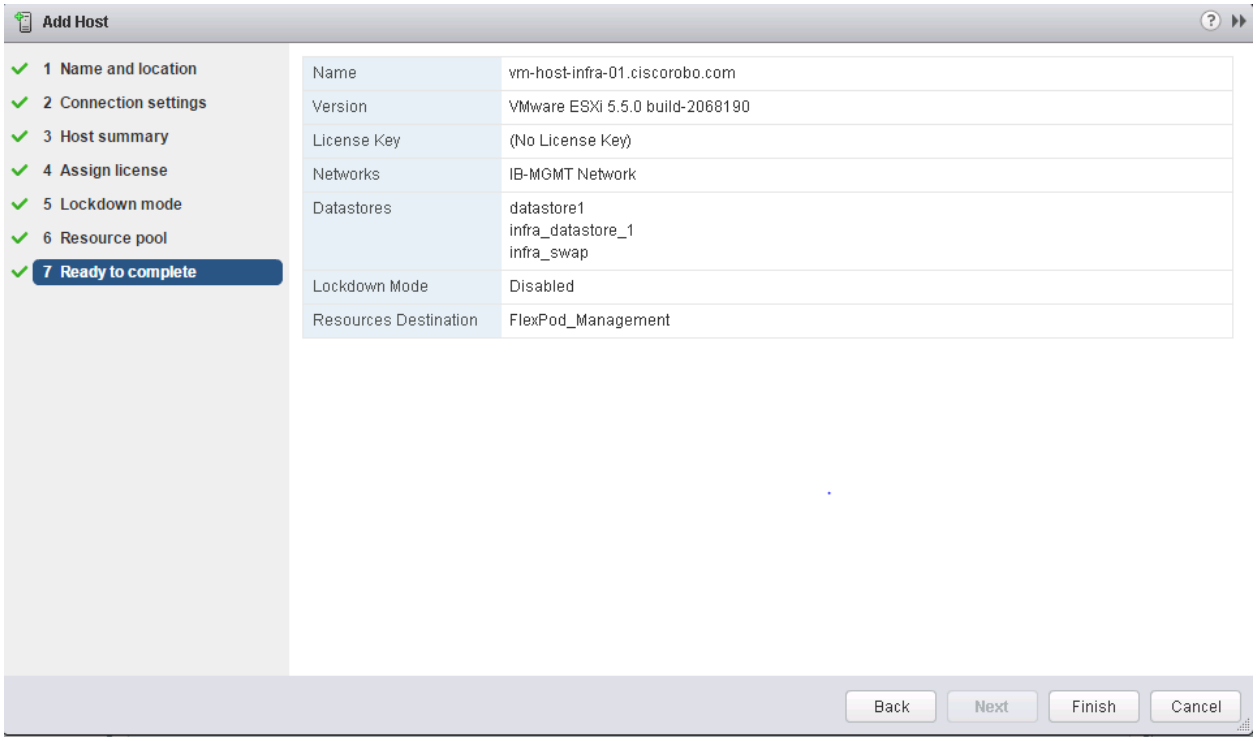


25. Click Yes to accept the certificate.
26. Review the host details and click Next to continue.
27. Assign a license and click Next to continue.

28. Click Next to continue.

29. Click Next to continue.

30. Review the configuration parameters, and then click Finish to add the host.



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

ESXi Dump Collector Setup for iSCSI-Booted Hosts

ESXi hosts booted with iSCSI using the VMware iSCSI software initiator need to be configured to do core dumps to the ESXi Dump Collector that is part of vCenter. The Dump Collector is enabled by default on the vCenter Appliance.

1. On the Management Workstation, open the VMware vSphere CLI command prompt.

2. Set each iSCSI-booted ESXi Host to coredump to the ESXi Dump Collector by running the following commands:

```
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> system coredump network set --interface-
name vmk0 --server-ipv4 <<var_vcenter_server_ip> --server-port 6500
esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>> system coredump network set --interface-
name vmk0 --server-ipv4 <<var_vcenter_server_ip> --server-port 6500
```

```
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> system coredump network set --enable true
esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>> system coredump network set --enable true
```

```
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> system coredump network check
esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>> system coredump network check
```

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

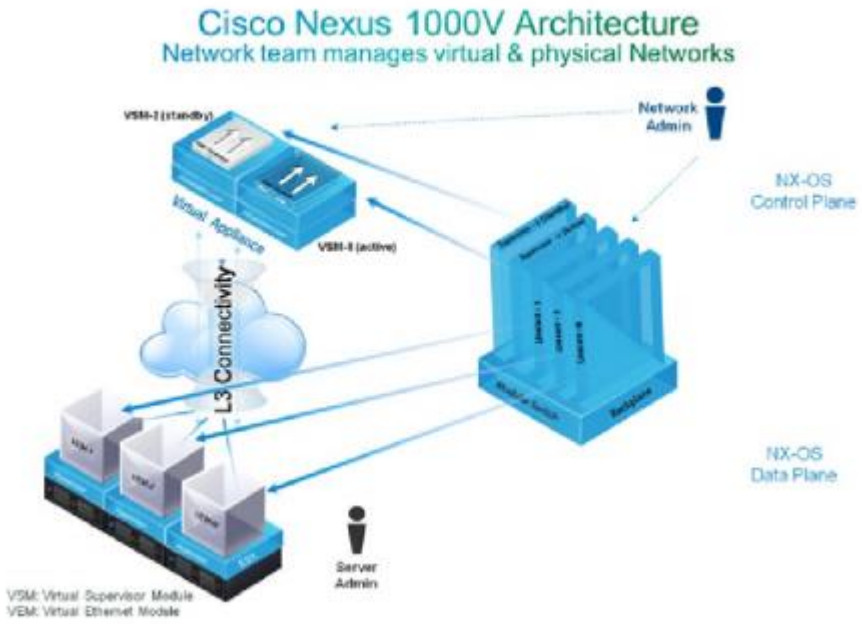
Cisco Nexus 1000V

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 is listed in the VMware Hardware Compatibility List (HCL).

The Cisco Nexus 1000V has the following components:

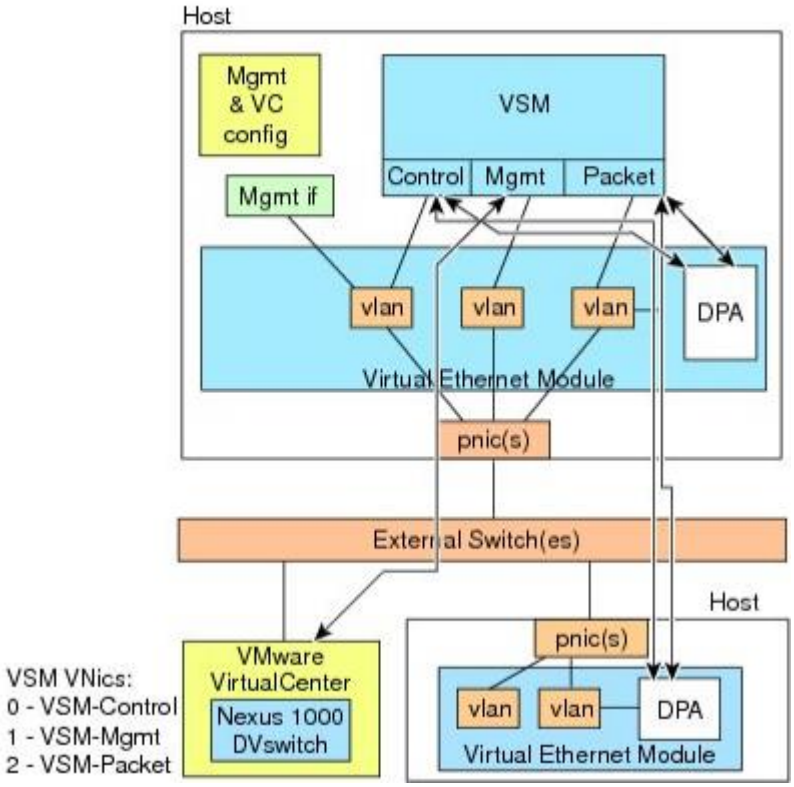
- Virtual Supervisor Module (VSM)—The control plane of the switch and a VM that runs Cisco NX-OS.
- Virtual Ethernet Module (VEM)—A virtual line card that is embedded in each VMware vSphere (ESXi) host. The VEM is partly inside the kernel of the hypervisor and partly in a user-world process, called the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



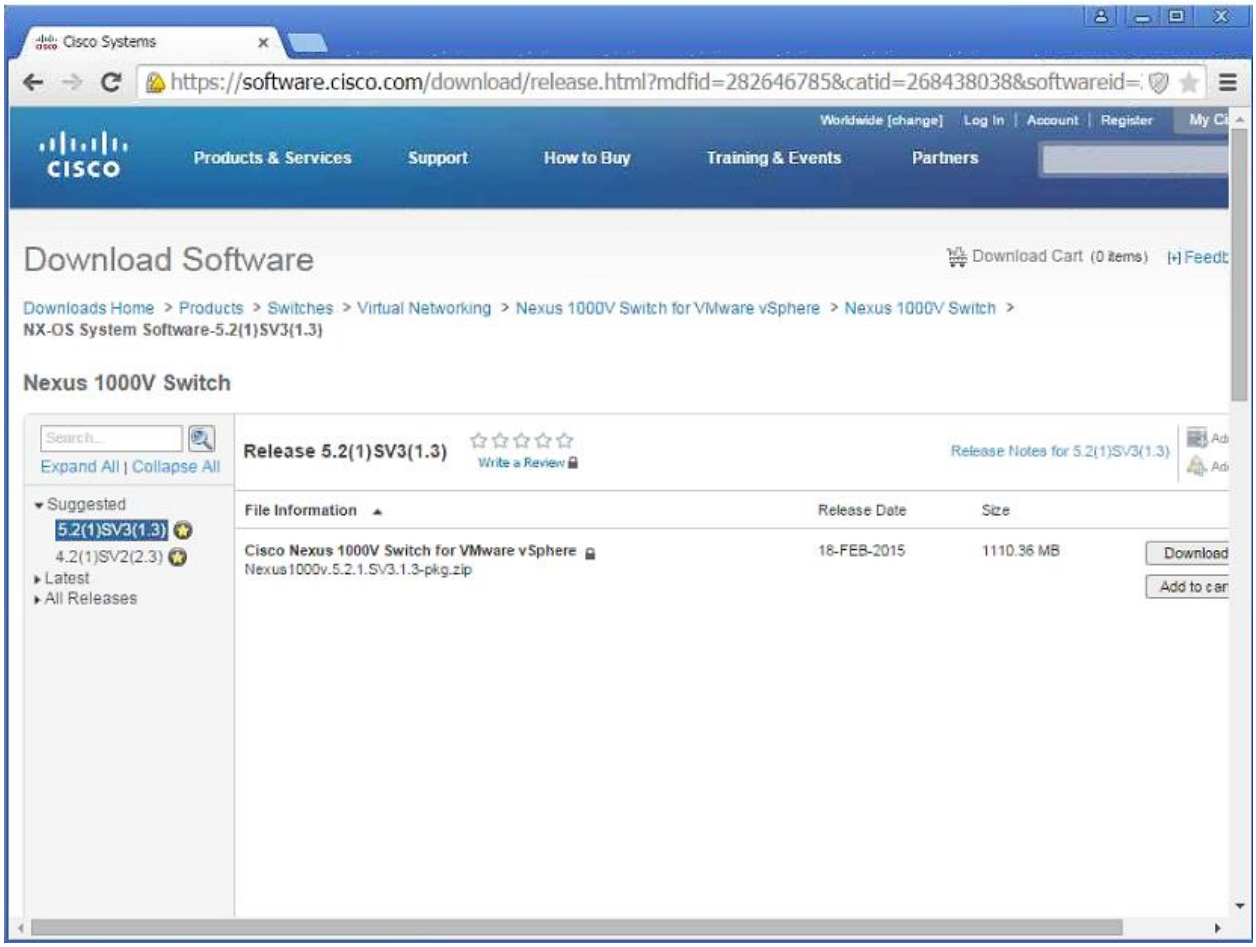
This section describes the steps involved in the installation of Cisco Nexus 1000V.

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.

Note: If a centralized Nexus 1000V VSM pair is being used, it is not necessary to install the Nexus 1000V VSM. Continue this procedure at the heading Install Virtual Ethernet Module (VEM) on each VMware ESXi Host below. Note that is important that the Nexus 1000V VSM is connected to the same VMware vCenter Datacenter that the ESXi hosts are in.

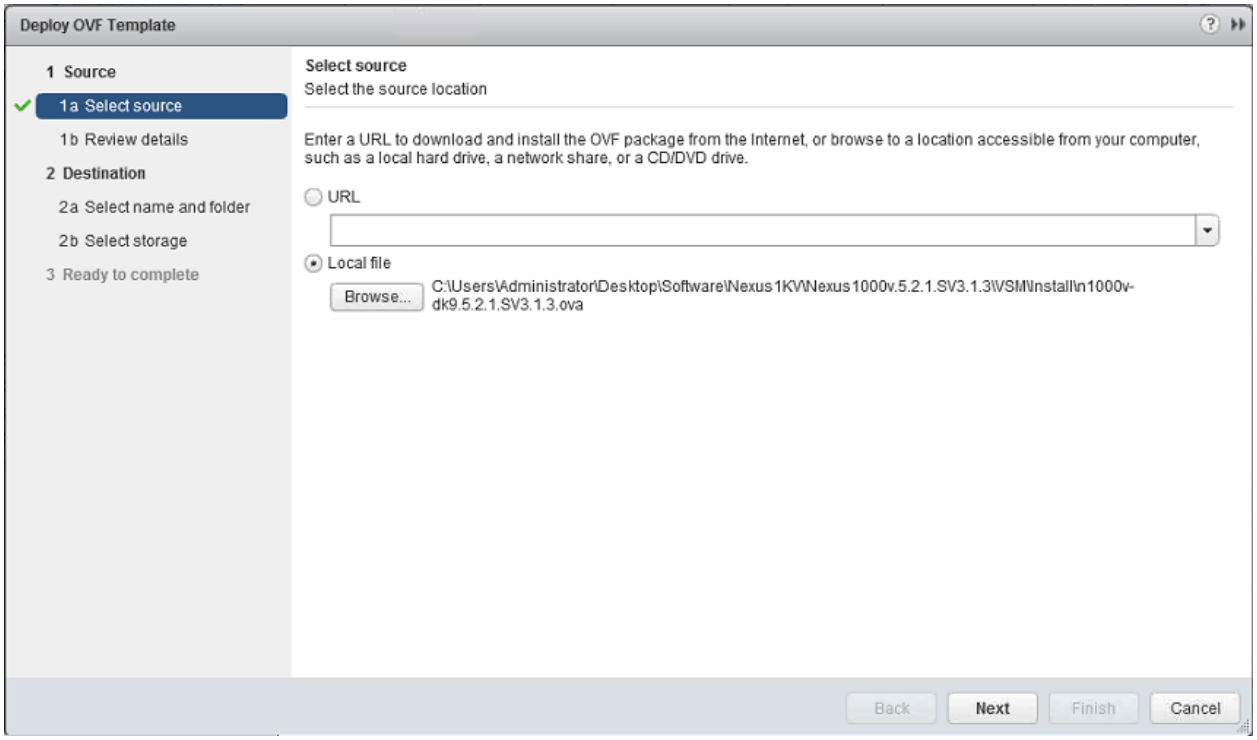
To install the Cisco Nexus 1000V, complete the following steps

1. Login and download the Cisco Nexus 1000V version 5.2(1)SV3(1.3) installation software from www.cisco.com

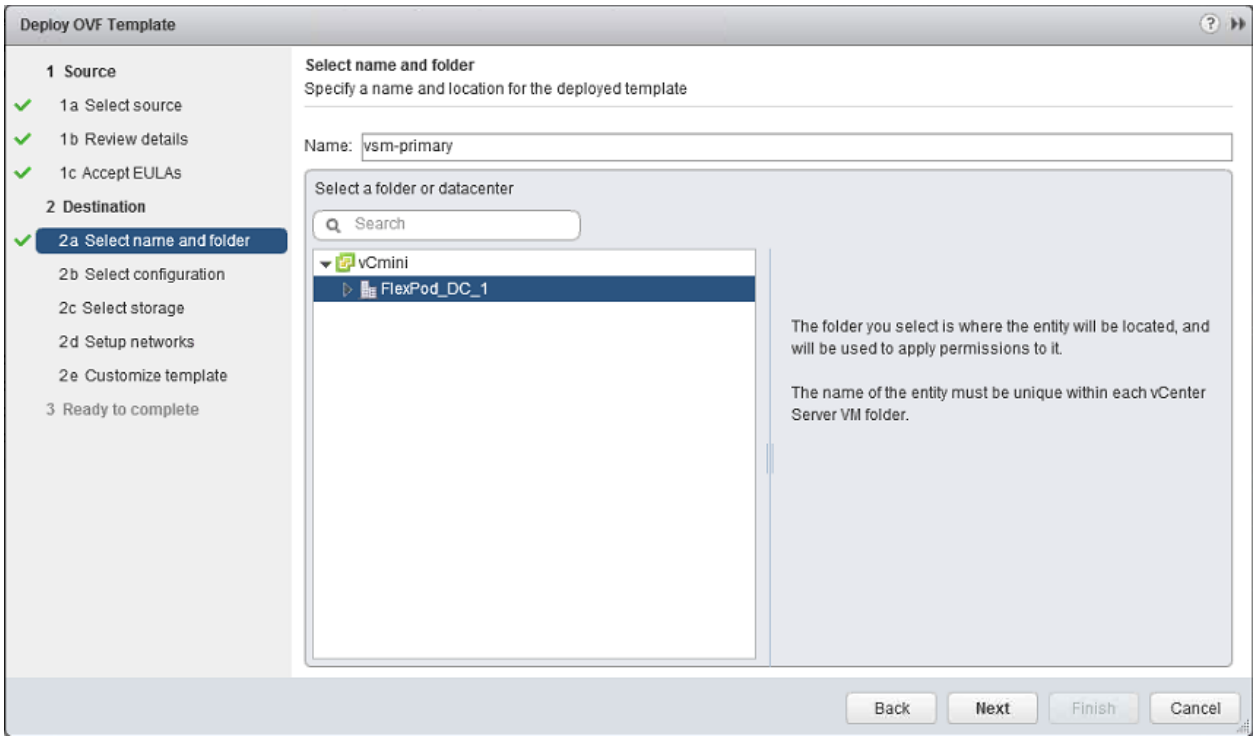


2. Unzip the package, and then unzip the Nexus1000v.5.2.1.Sv3.1.3.zip package to get the Nexus 1000v VSM OVA.

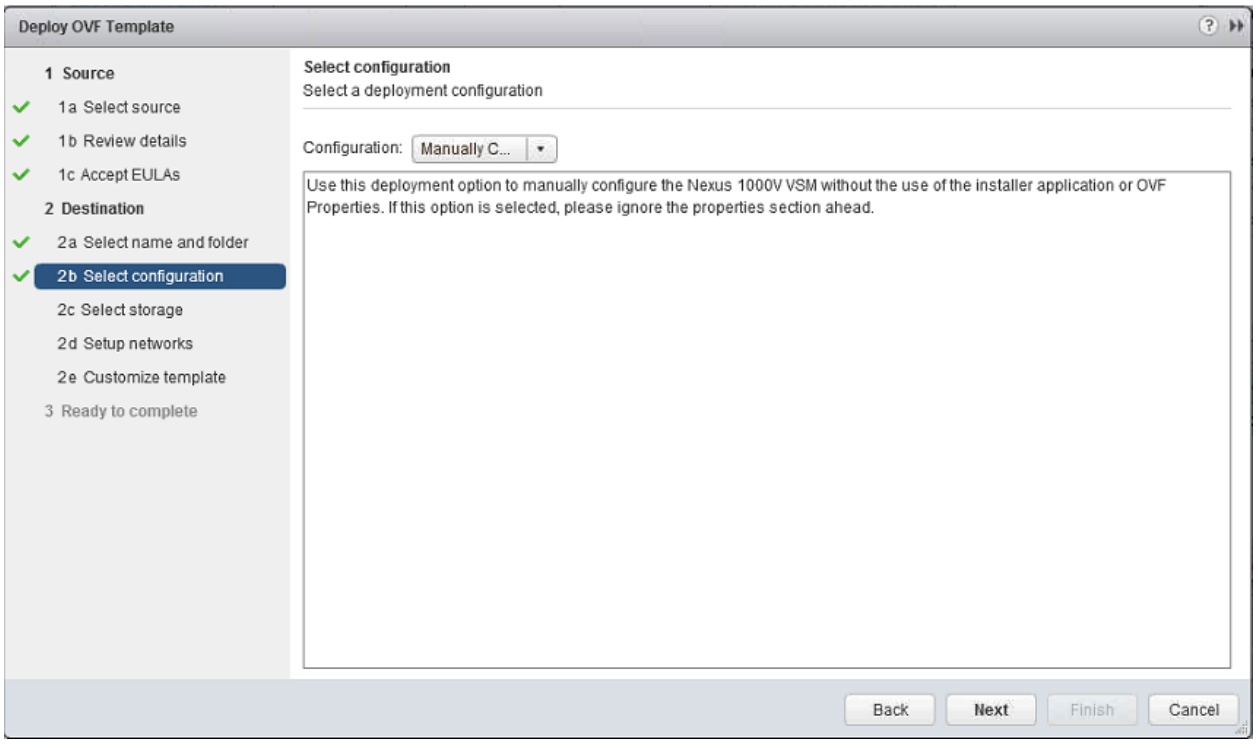
3. From the vSphere Web Client, under Hosts and Clusters, right-click the FlexPod_Management cluster and select Deploy OVF Template. Browse to the unzipped VSM/Install/n1000v-dk9.5.2.1.SV3.1.3.ova file and click Open. Click Next.



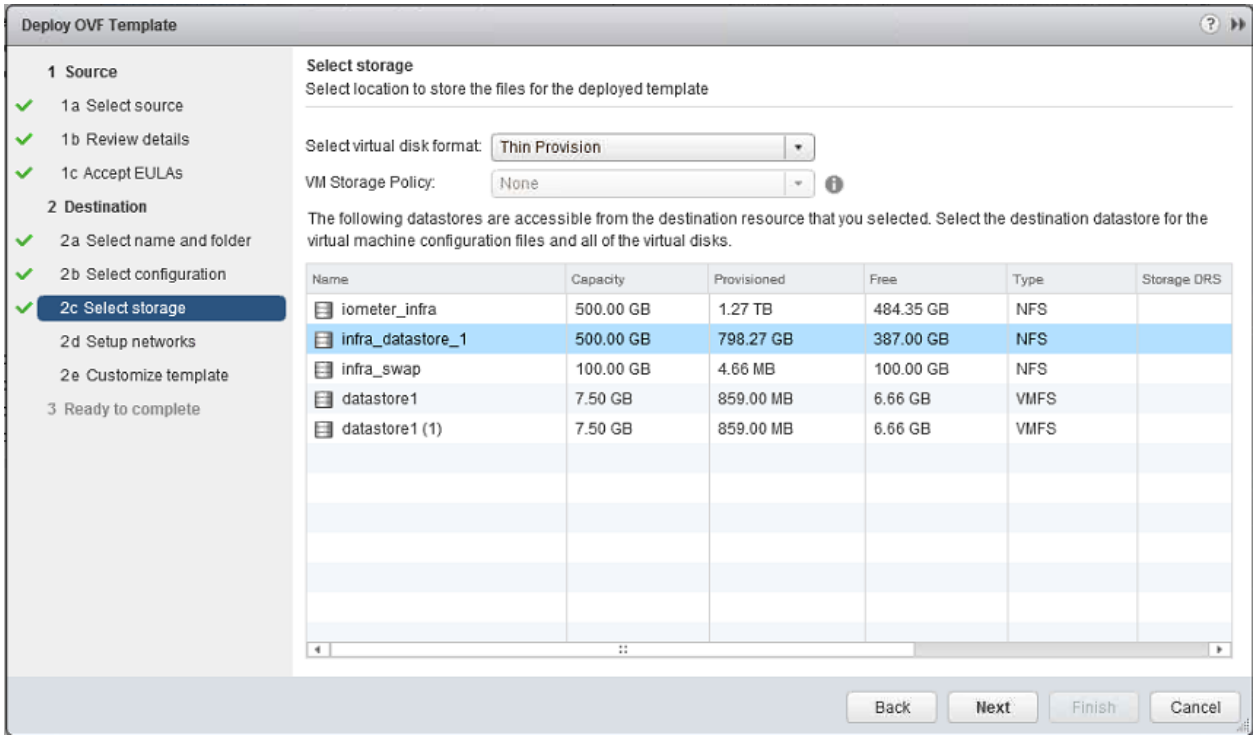
4. Click Next at the Review Details page.
5. Accept the EULA, and then click Next.
6. Enter a name for the primary Nexus 1000V Virtual Supervisor Module (VSM) virtual machine.
7. Select FlexPod_DC_1 and then click Next.



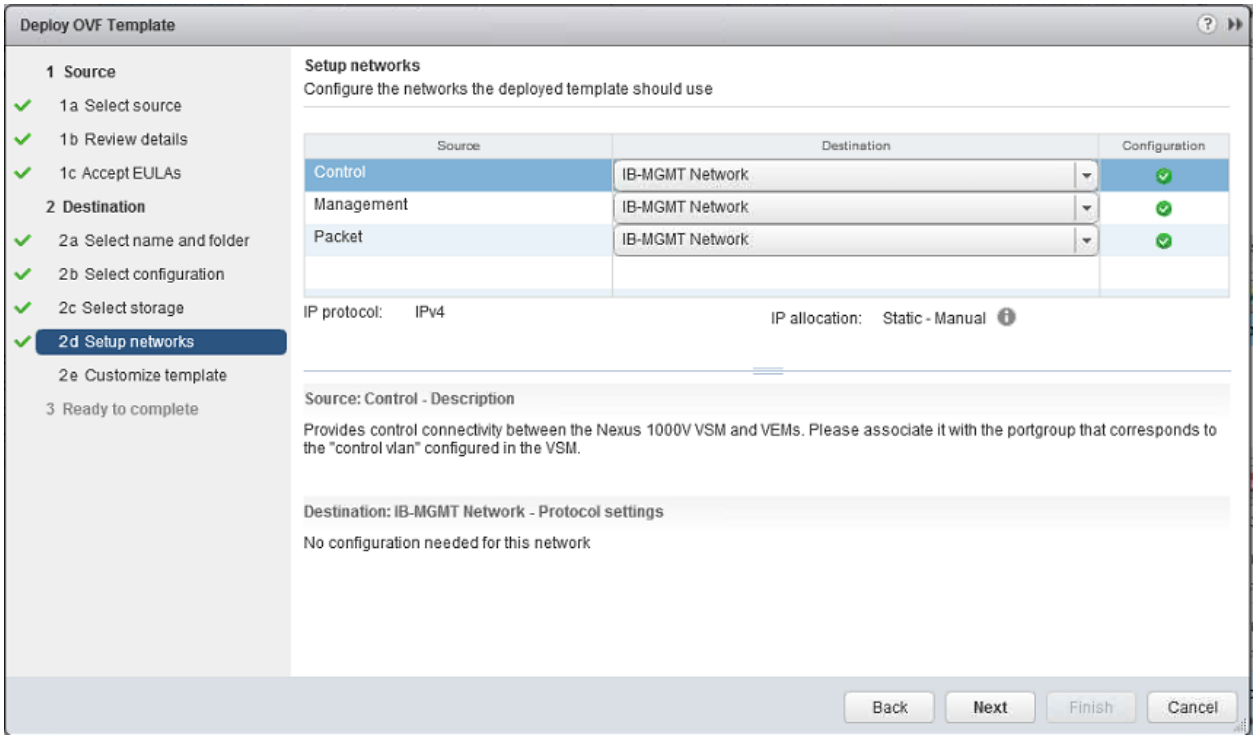
8. Ensure Manually Configure is selected and click Next.



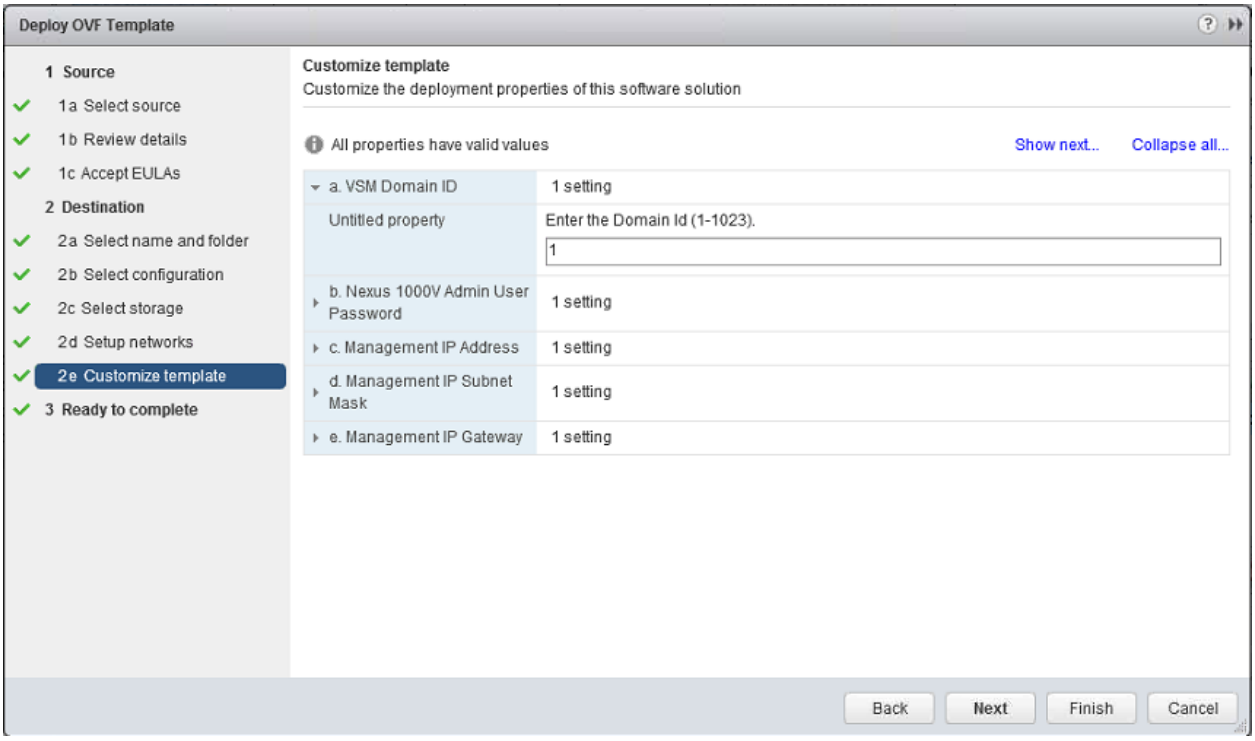
9. Make sure the Thin Provision virtual disk format is selected in the drop down menu. Select infra_datastore_1 then click Next.



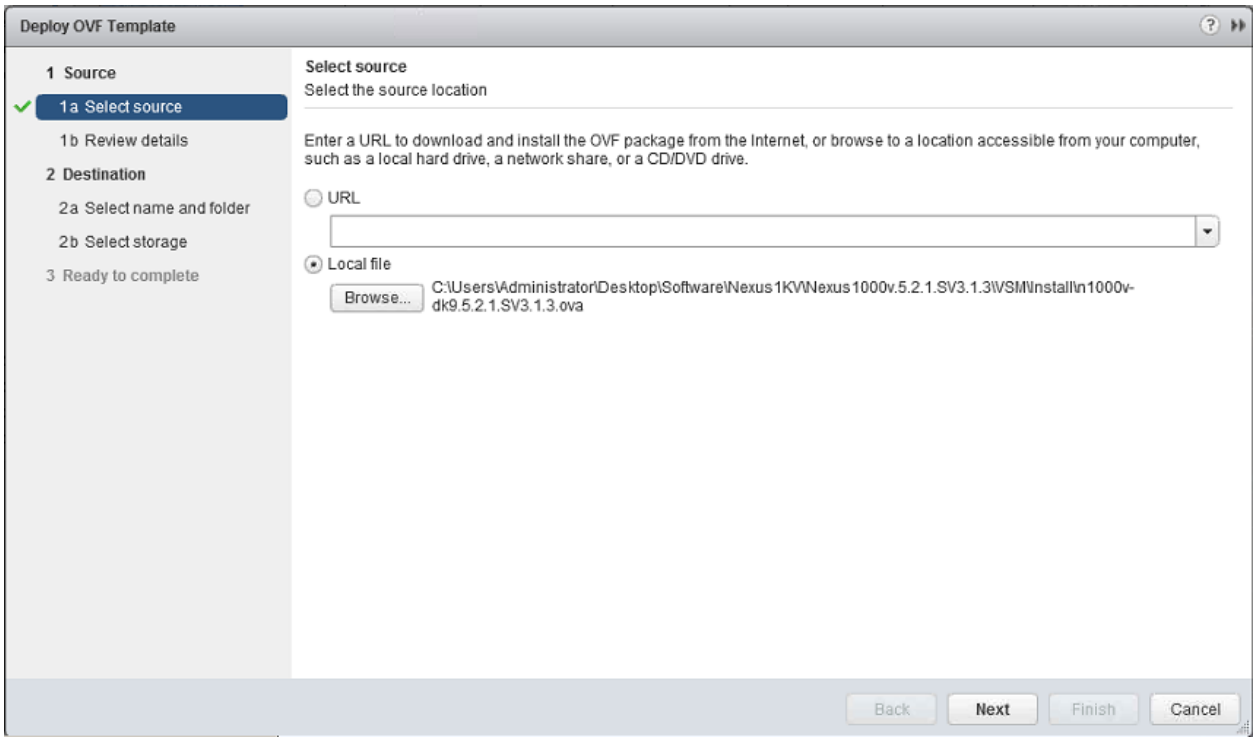
10. Make sure the IB-MGMT Network is selected as the management destination for all three sources. Click Next.



11. Click Finish. Wait for the appliance to deploy.



12. From the vSphere Web Client, right-click the FlexPod_Management cluster and select Deploy OVF Template. Browse to the unzipped VSM/Install/n1000v-dk9.5.2.1.SV3.1.3.ova file and click Open. Click Next.

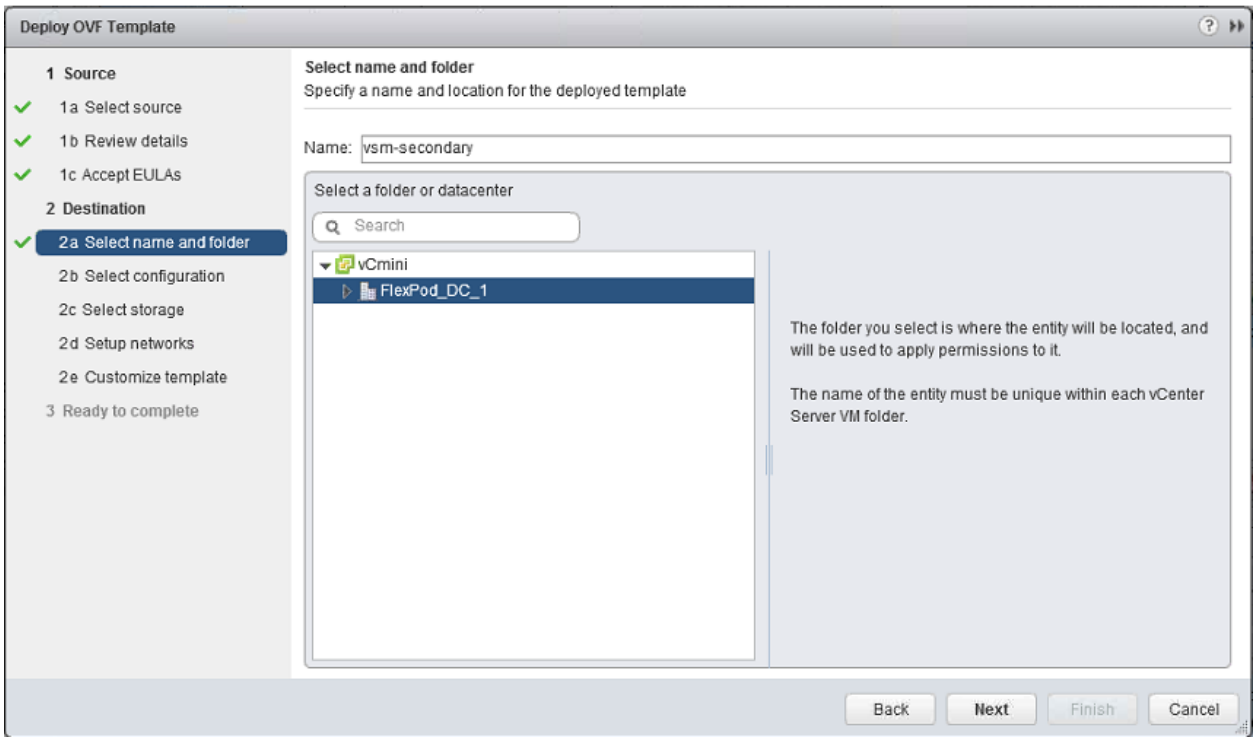


13. Click Next at the Review Details page.

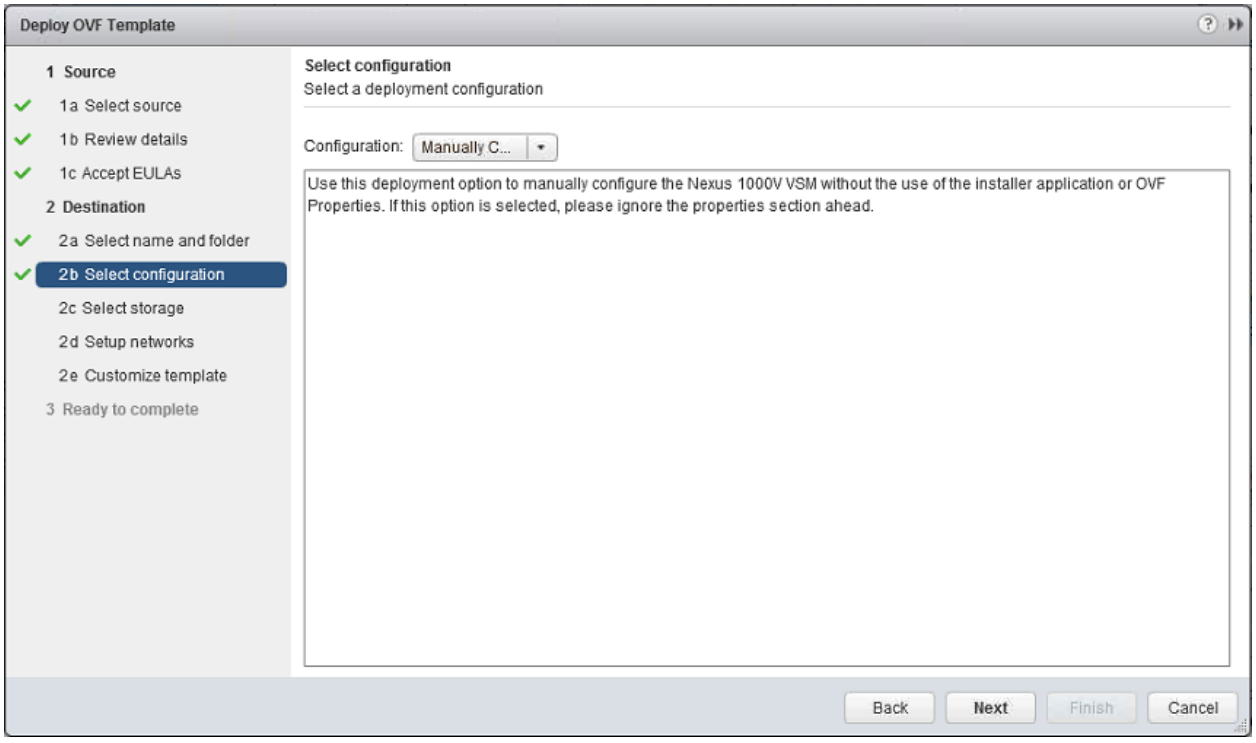
14. Accept the EULA, and then click Next.

15. Enter a name for the secondary Nexus 1000V Virtual Supervisor Module (VSM) virtual machine.

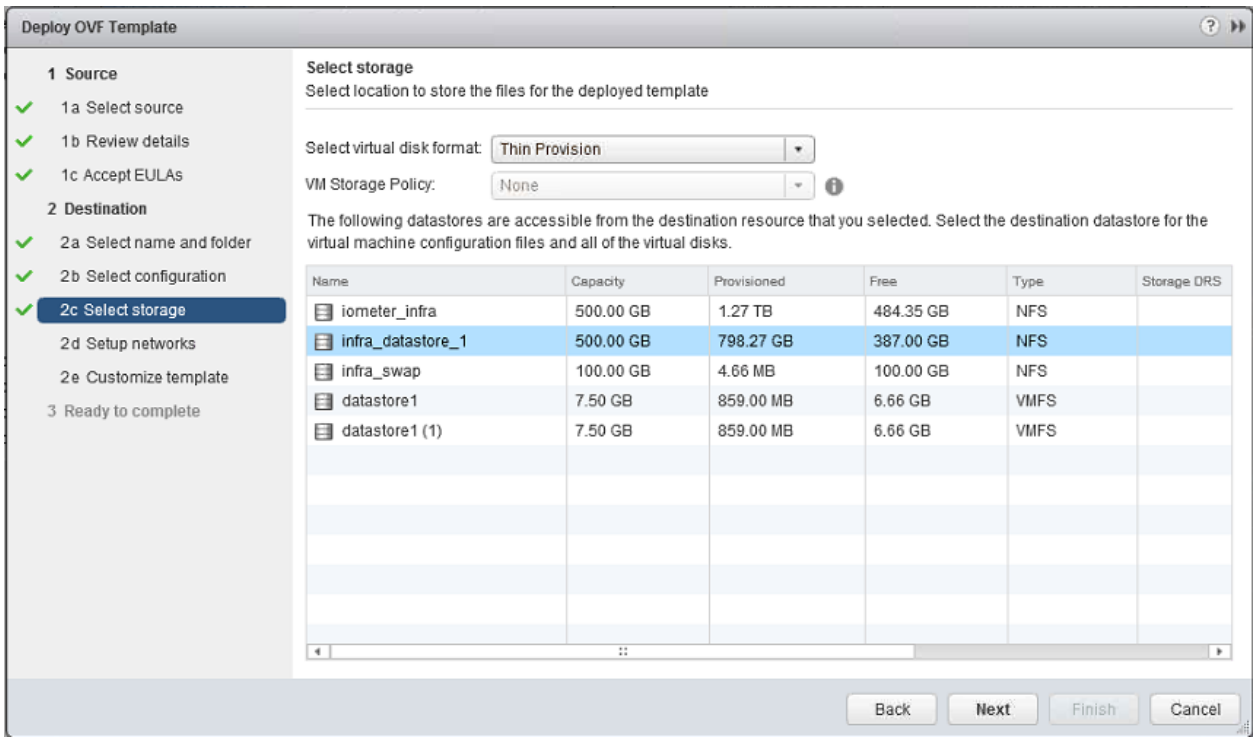
16. Select FlexPod_DC_1 and then click Next.



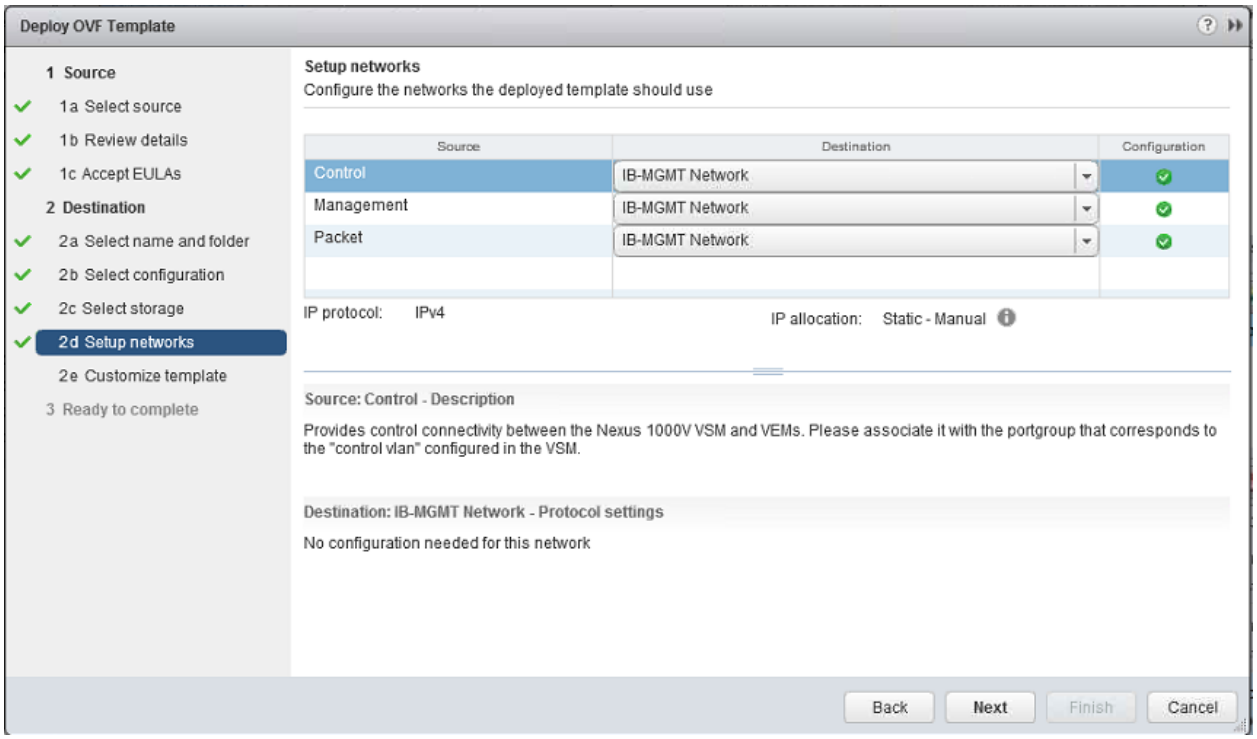
17. Ensure Manually Configure is selected and click Next.



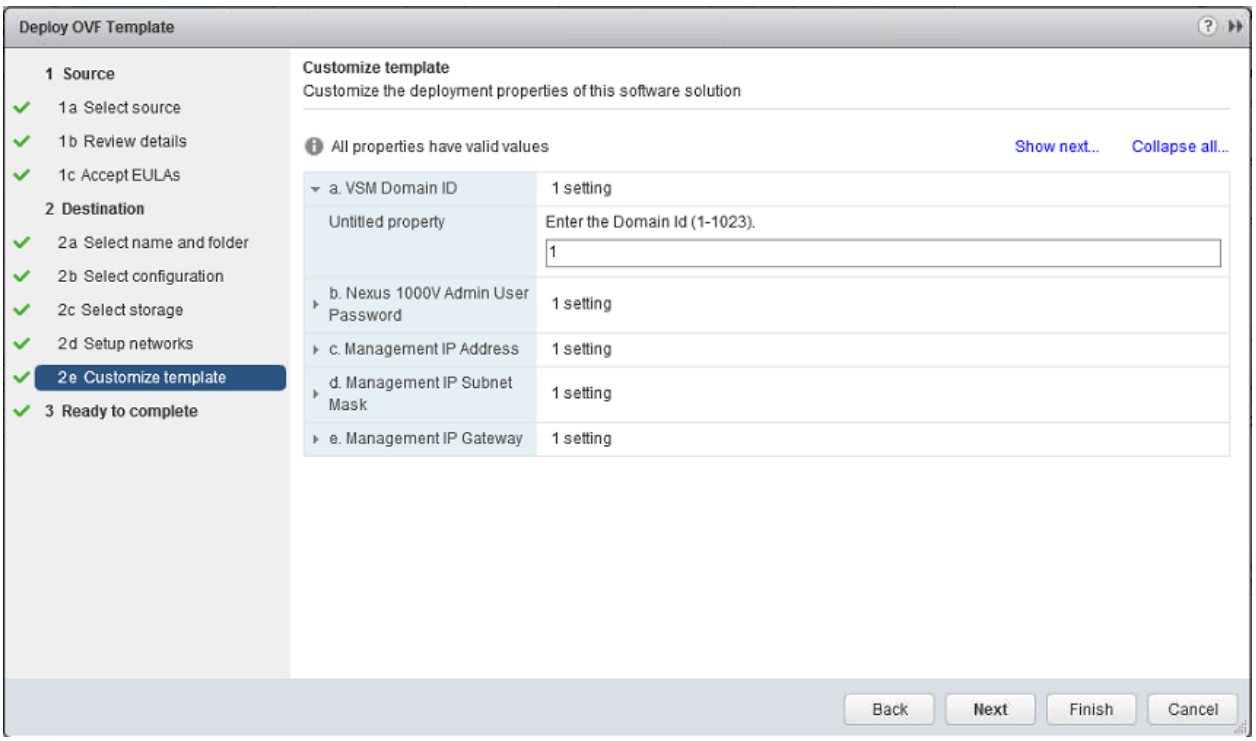
18. Ensure Thin Provision virtual disk format is selected in the drop down menu. Select infra_datastore_1 then click Next.



19. Ensure IB-MGMT Network is selected as the management destination for all three sources. Click Next.

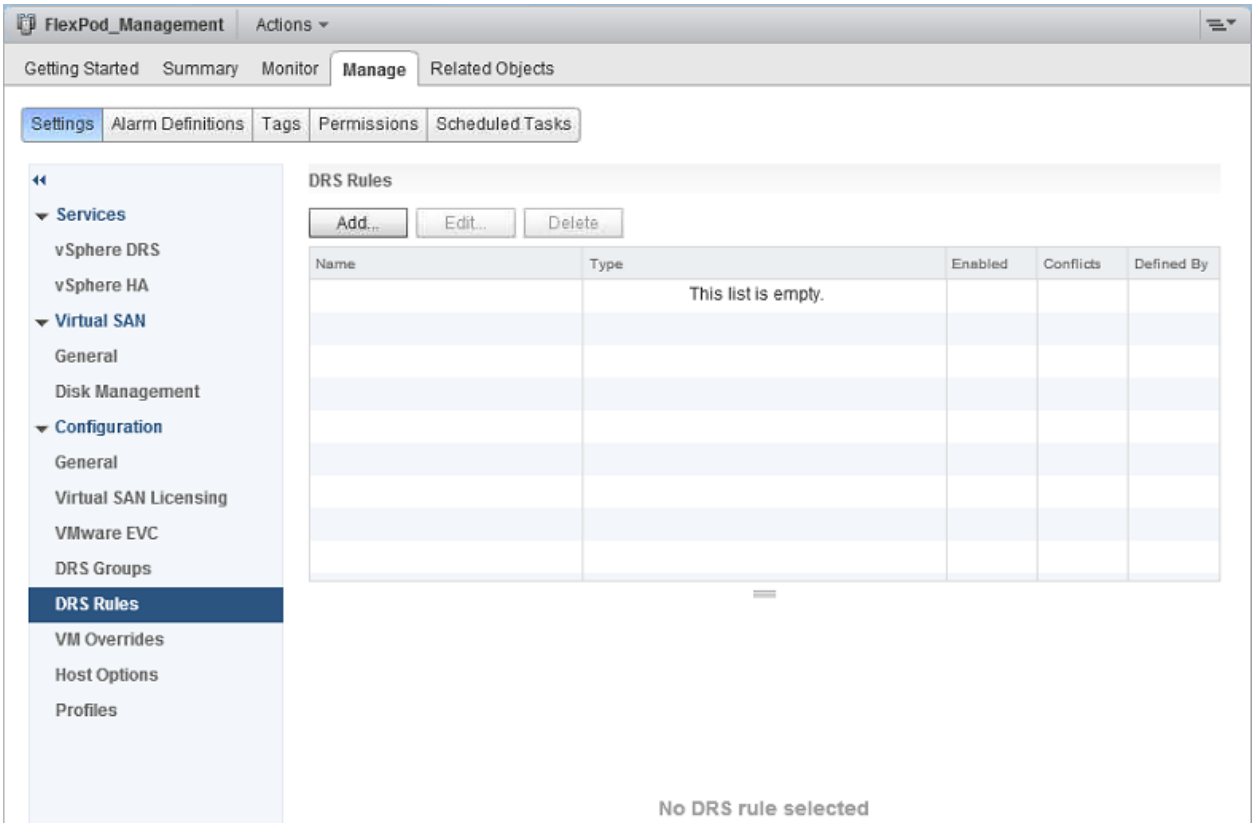


20. Click Finish. Wait for the appliance to deploy.

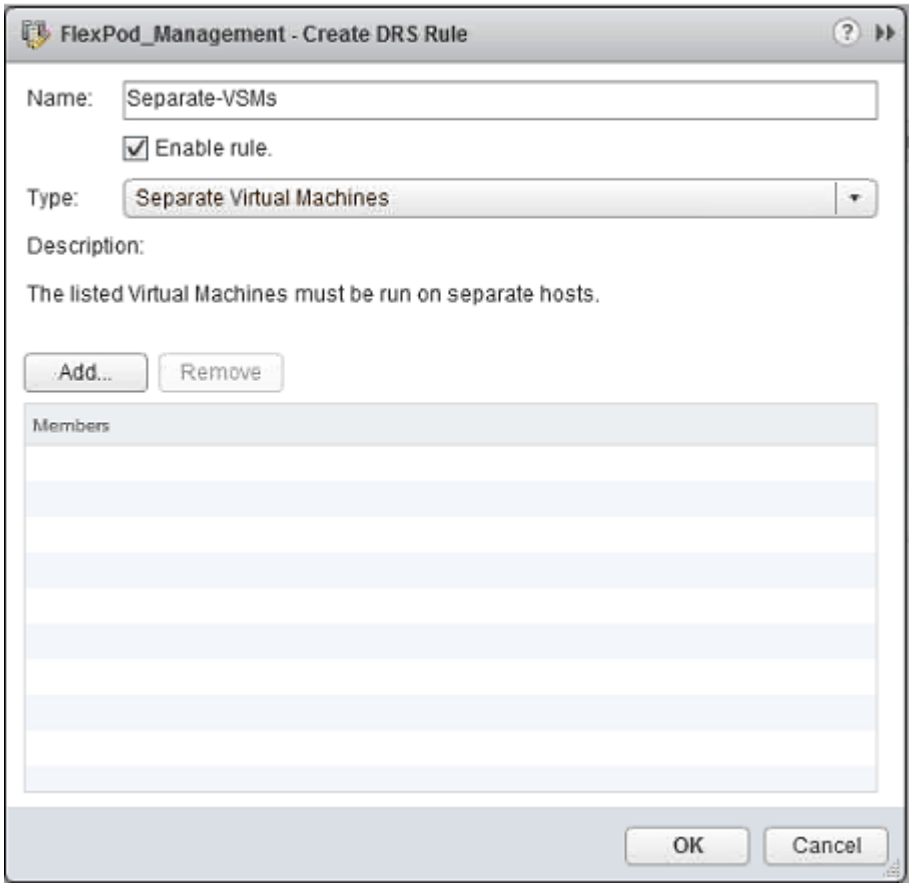


21. In the vSphere Web Client Hosts and Clusters list, right-click the FlexPod_Management cluster and select Settings.

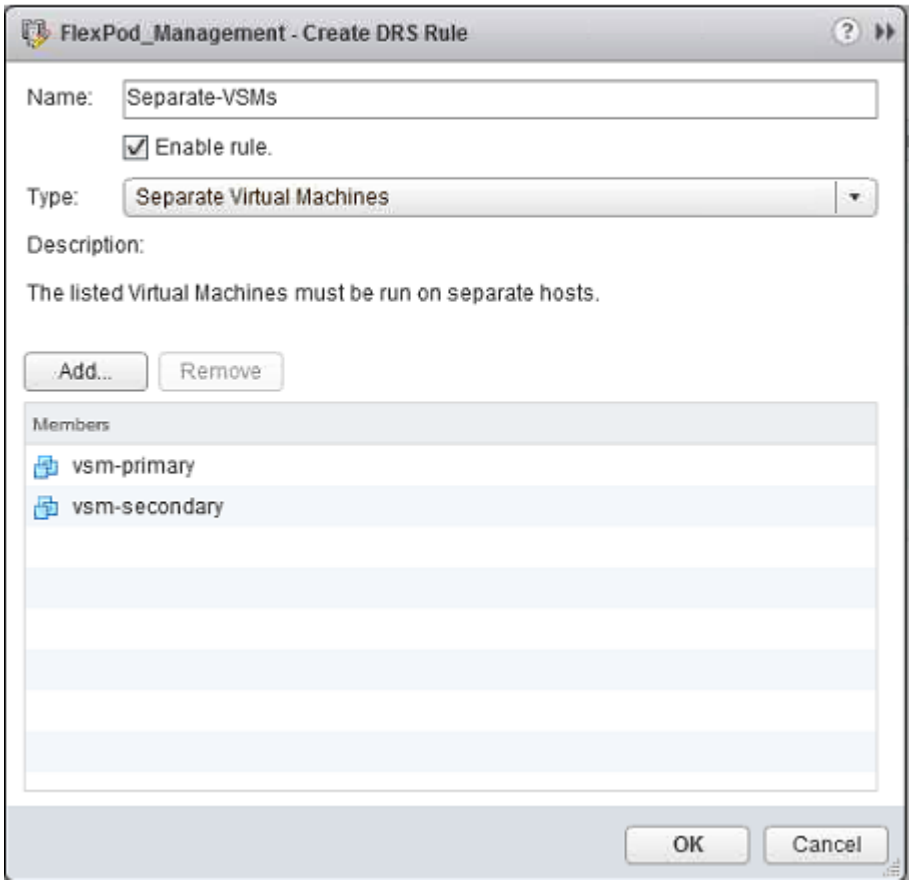
22. In the list on the left of the center pane, select DRS Rules. Click Add.



23. Name the rule Separate-VSMs and select Separate Virtual Machines for Type.



24. Click Add. Select the primary and secondary VSMs. Click OK. Click OK.



25. In the vSphere Web Client Hosts and Clusters list, right-click the primary VSM and select Power On.

26. Select the primary VSM and in the center pane select Open with VMRC.

27. In the primary VSM console, execute the VSM setup wizard.

```
Enter the password for "admin":  <<var_password>>
Confirm the password for "admin":  <<var_password>>
Enter HA role[standalone/primary/secondary]: primary
Enter the domain id<1-1023>: <<var_vsm_domain>>

Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [no]: Enter
Configure read-onlu SNMP community string (yes/no) [n]: Enter
Configure read-wirte SNMP community string (yes/no) [n]: Enter
Enter the switch name : <<var_vsm_name>>
Continue with Out-of-band (mgmt0) management configuration? (yes/no) {y}: Enter
Mgmt0 IP address type V4/V6? (V4): V4
Mgmt0 IPv4 address : <<var_vsm_mgmt_ip>>
Mgmt0 IPv4 netmask : <<var_vsm_mgmt_mask>>
Configure the default gatewary? (yes/no) [y]: Enter
IPv4 address of the default gateway : <<var_vsm_mgmt_gateway>>
Configure advanced IP options? (yes/no) [n]: Enter
Enable the telnet service? (yes/no) [n]: Enter
Enable the ssh service? (yes/no) [y]: Enter
Type of ssh key you would like to generate (dsa/rsa) [rsa]: Enter
Number of rsa key bits <768-2048> [1024]: Enter
Enable the http-server? (yes/no) [y]: Enter
Configure the ntp server? (yes/no) [n]: Enter
```

```
Vem feature level will be set to 5.2(1)SV3(1.3). Do you want to reconfigure? (yes/no) [n]: Enter
Configure svs domain parameters? (yes/no) [y]: Enter
Enter SVS Control mode (L2 / L3) [L3]: Enter
Would you like to edit the configuration? (yes/no) [n]: Enter
Use this configuration and save it? (yes/no) [y]: Enter
```

28. Log into the primary VSM with the admin user id and password.

29. In the vSphere Web Client Hosts and Clusters list, right-click the secondary VSM and select Power On.

30. Select the secondary VSM and in the center pane select Open with VMRC.

31. In the secondary VSM console, execute the VSM setup wizard. Use the same values for password and domain ID entered on the primary VSM.

```
Enter the password for "admin":  <<var_password>>
Confirm the password for "admin":  <<var_password>>
Enter HA role[standalone/primary/secondary]: secondary
Setting HA role to secondary will cause a system reboot. Are you sure (yes/no)?: yes
Enter the domain id<1-1023>: <<var_vsm_domain>>
```

32. Once the secondary VSM has rebooted, use an ssh client to log into the primary VSM with the admin user id and password.

33. Type "show module" repeatedly until the secondary VSM shows the status ha-standby.

Register Cisco Nexus 1000V as a vCenter Plug-in

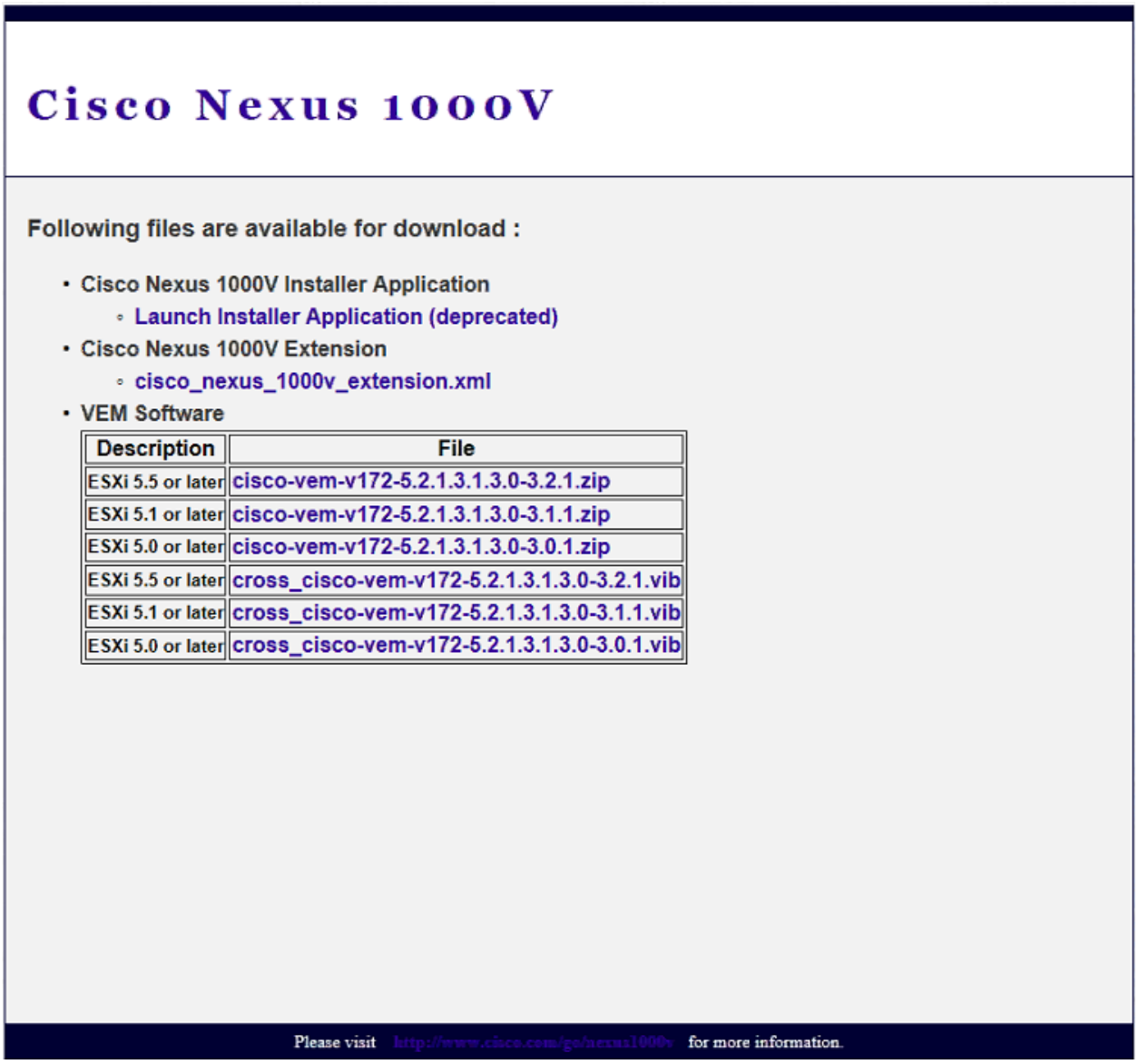
To register the Cisco Nexus 1000V as a vCenter plug-in, complete the following steps:

1. Using a web browser, navigate to the `<<var_vsm_mgmt_ip>>` enter `http://<<var_vsm_mgmt_ip>>`.
2. Right-click `cisco_nexus_1000v_extension.xml` and select Save target as.
3. Save the XML file to the local desktop.
4. Open the VMware vSphere Client and connect to the vCenter as an administrator. Select Plug-ins > Manage Plug-ins.
5. Right-click in the white space in the window and select New Plug-in.
6. Browse to the desktop and select the `cisco_nexus_1000v_extension.xml` document that was previously saved. Click Open.
7. Click Register Plug-in.
8. Click Ignore.
9. Click OK.
10. The `Cisco_Nexus_1000V` should now appear in the list of available plug-ins

Install Virtual Ethernet Module (VEM) on each VMware ESXi Host

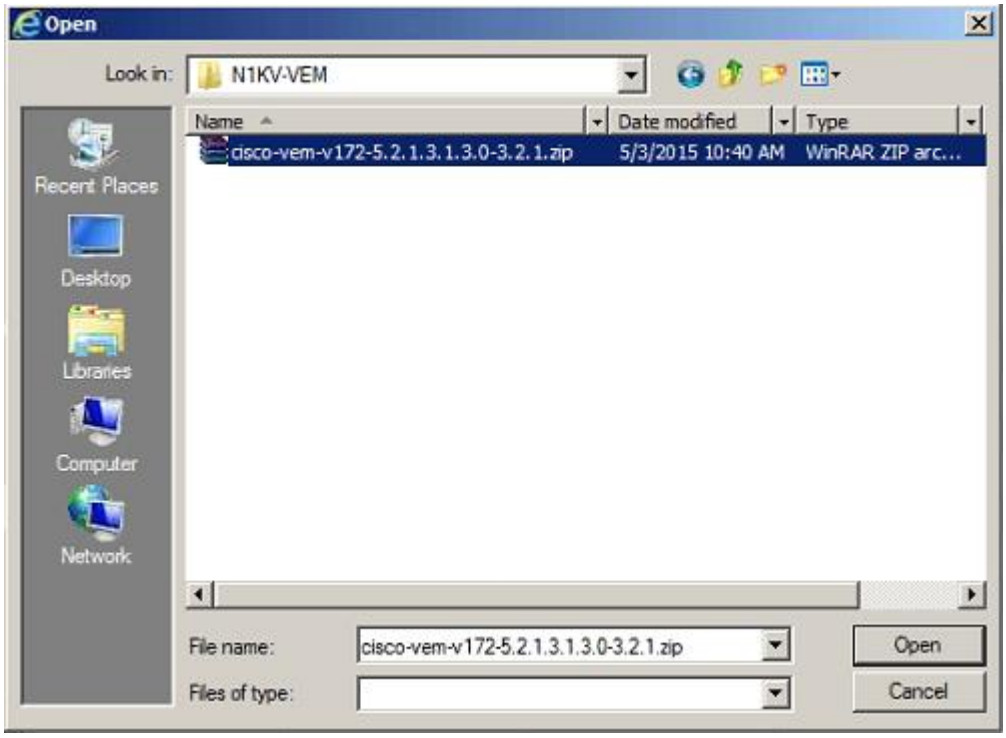
To install the Cisco Nexus 1000V VEM on each ESXi host, complete the following steps:

1. Using a web browser, navigate to the <<var_vsm_mgmt_ip>> enter http://<<var_vsm_mgmt_ip>>.



2. Right-click cisco-vem-v172-5.2.1.3.1.3.0-3.2.1.zip and select Save target as.
3. Save the ZIP file to the local desktop.
4. In the VMware vSphere Web Client from the Home page, select Storage.
5. In the list on the left, right-click infra_datastore_1 and select Browse Files.
6. On the right, click the icon to add a folder.
7. Name the folder VEM and click Create.
8. In the list of folders, select the VEM folder.
9. On the right, click the icon to upload a file to the Datastore.

10. Browse to the ZIP file downloaded above and click Open.



11. On the Management Workstation, open the VMware vSphere CLI command prompt.

12. Install the VEM on each ESXi Host by running the following commands:

```
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> software vib install -d
/vmfs/volumes/infra_datastore_1/VEM/cisco-vem-v172-5.2.1.3.1.3.0-3.2.1.zip
esxcli -s <<var_vm_host_infra_02_ip>> -u root -p <<var_password>> software vib install -d
/vmfs/volumes/infra_datastore_1/VEM/cisco-vem-v172-5.2.1.3.1.3.0-3.2.1.zip
```

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. If using a centralized Nexus 1000v, adjust names accordingly, but putting Site-XX in front of each name.

```
config t

svs connection vCenter
protocol vmware-vim
remote ip address <<var_vcenter_server_ip>> port 80
vmware dvs datacenter-name FlexPod_DC_1
connect
exit

ntp server <<var_global_ntp_server_ip>> use-vrf management

vlan <<var_ib-mgmt_vlan_id>>
name IB-MGMT-VLAN
```

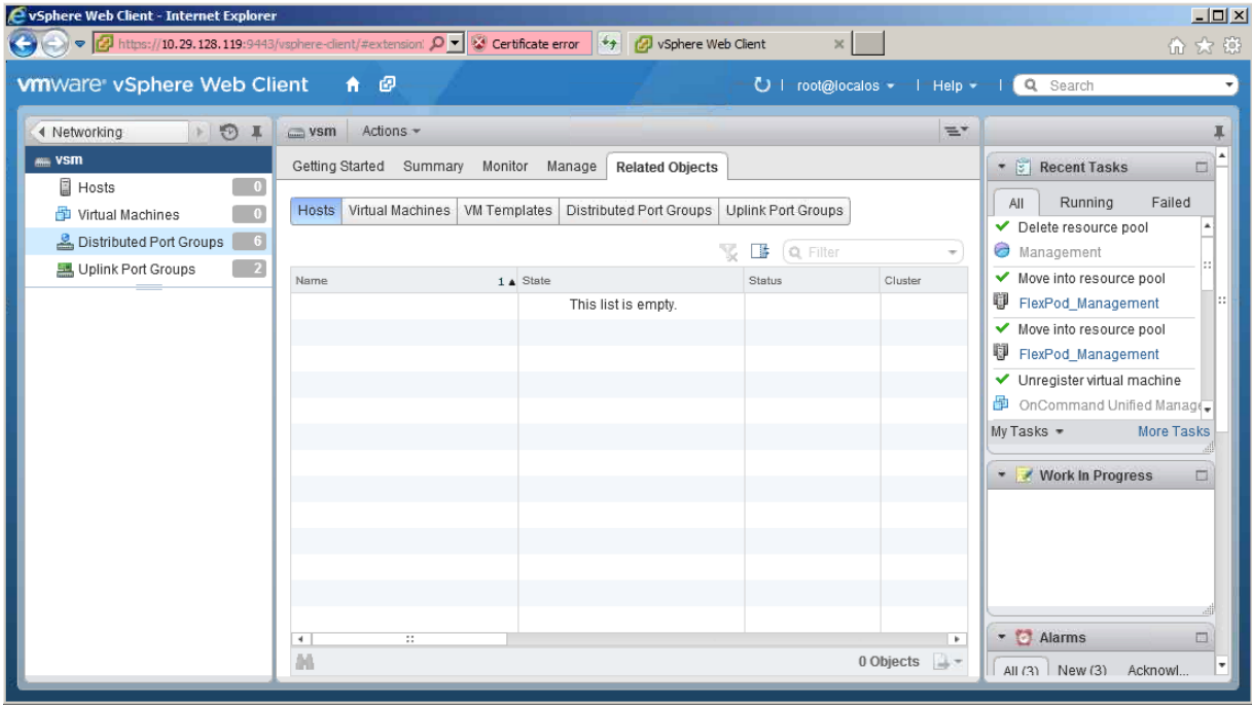
```
vlan <<var_nfs_vlan_id>>
name NFS-VLAN
vlan <<var_vmotion_vlan_id>>
name vMotion-VLAN
vlan <<var_vm-traffic_vlan_id>>
name VM-Traffic-VLAN
vlan <<var_native_vlan_id>>
name Native-VLAN
exit

system vlan <<var_ib-mgmt_vlan_id>>
state enabled
exit

copy run start
```

Note: The pinning id command is used here to pin all NFS traffic to Cisco UCS Fabric B and to pin all other traffic (management, vMotion, and VM Traffic) to Fabric A. This pinning along with the NFS LIF placement on Fabric B ensures that internal traffic in this solution is switched within the Cisco UCS Fabric interconnects and not by the standard Ethernet switches. Traffic only passes through the Ethernet switches in the event of a failover or when exiting the environment.

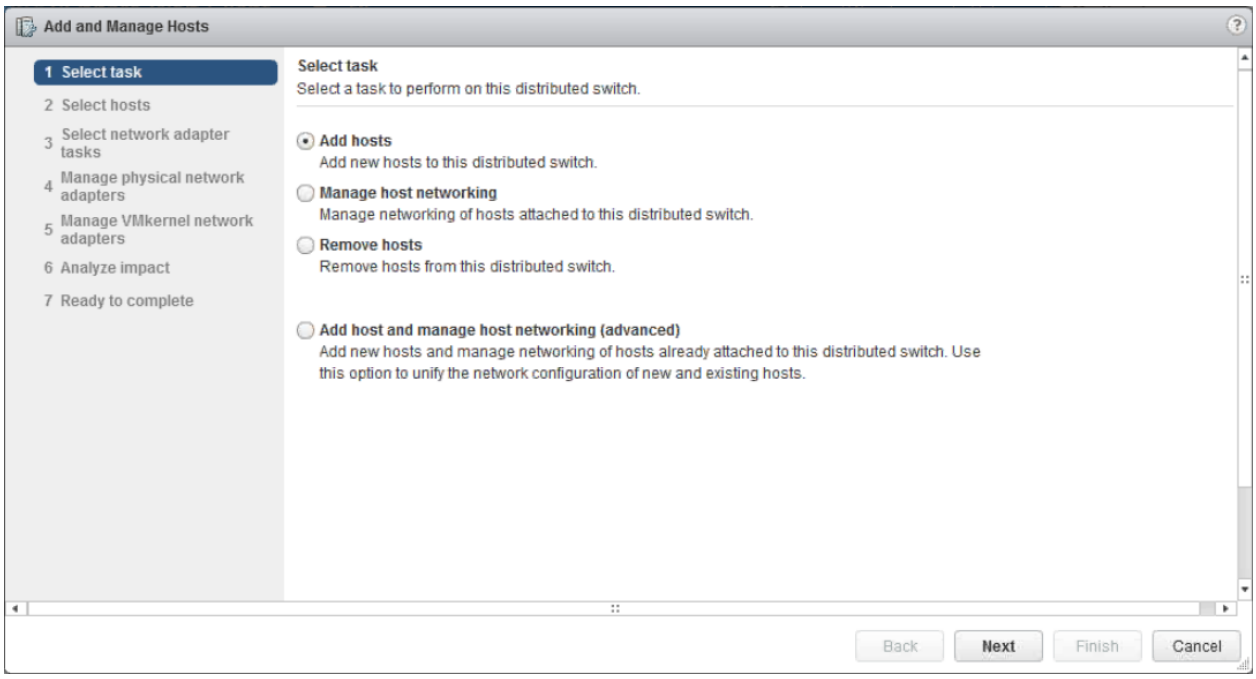
Migrate Networking Components for ESXi Hosts to Cisco Nexus 1000V

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

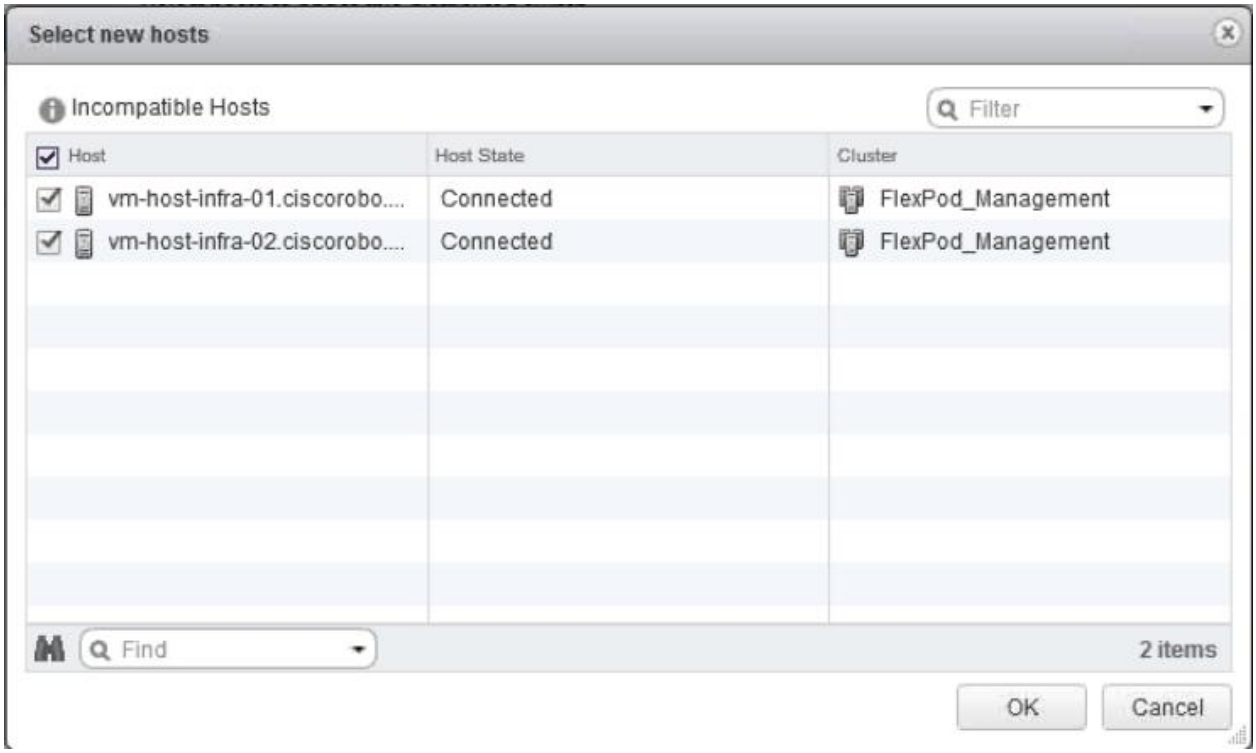
1. In VMware vSphere Web Client, click the Home button and then select Networking. Expand the list on the left and select the Nexus 1000V VSM.



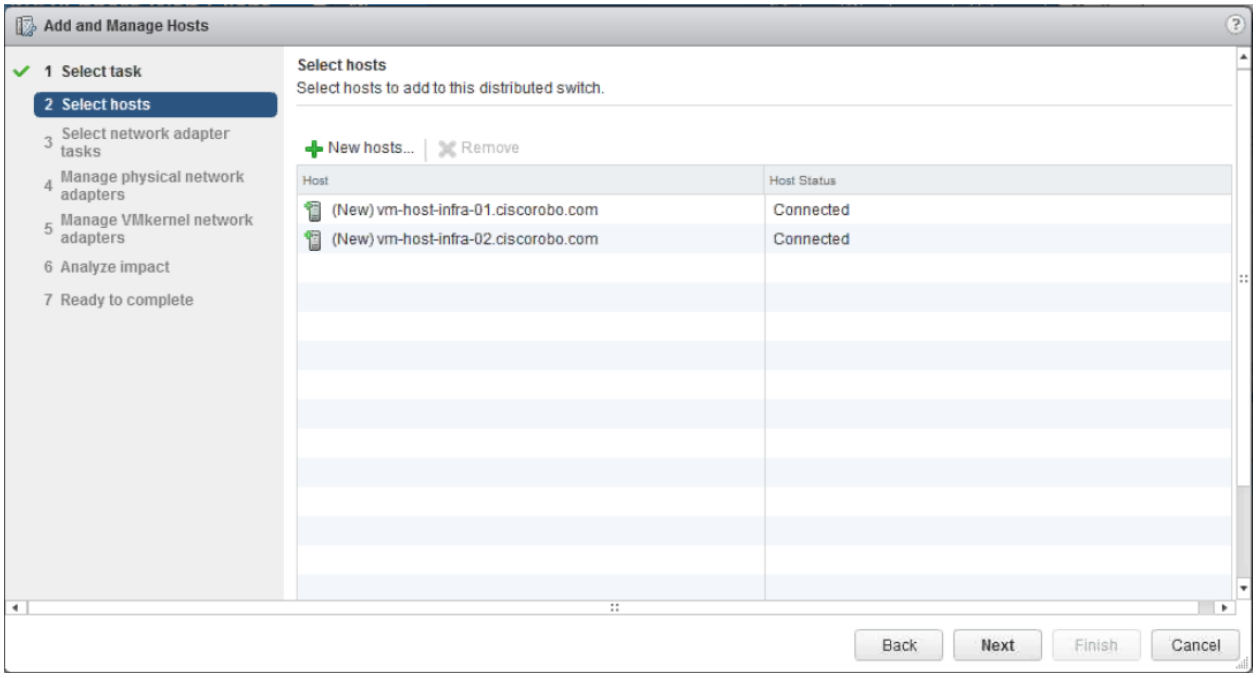
2. Right-click the Nexus 1000V VSM and select Add and Manage Hosts. Select Add hosts and click Next.



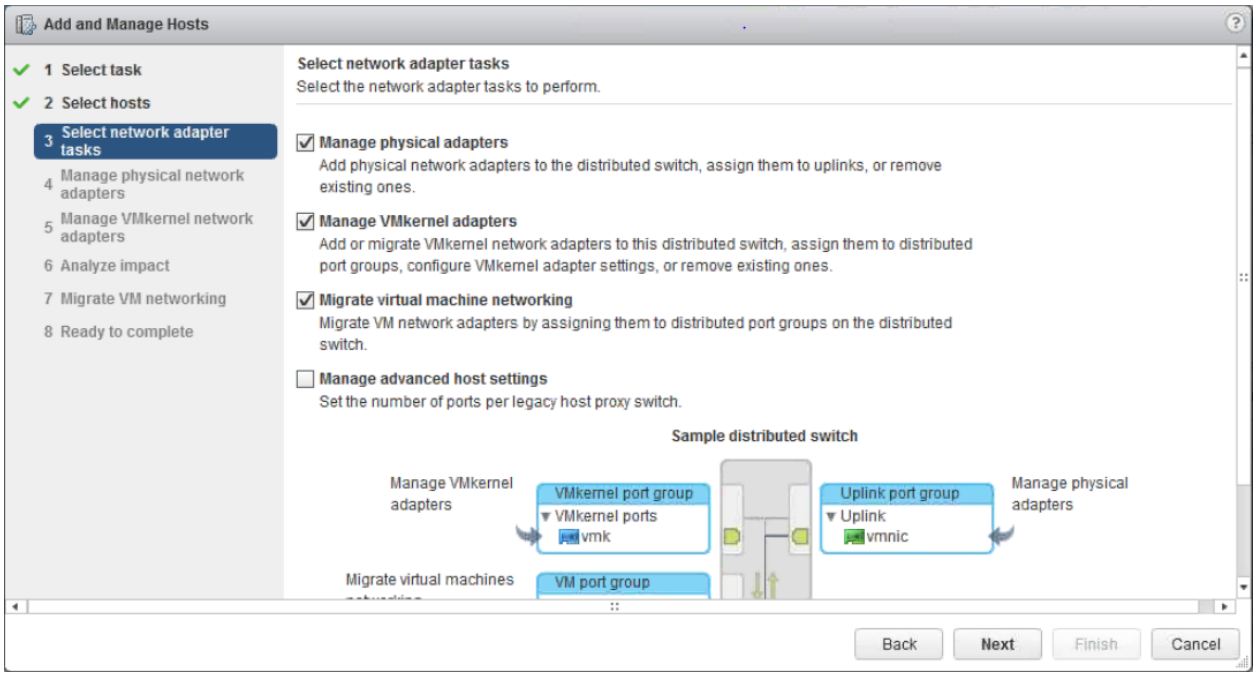
3. Click the green plus to add New hosts. Select the two FlexPod management hosts and click OK.



4. Click Next.



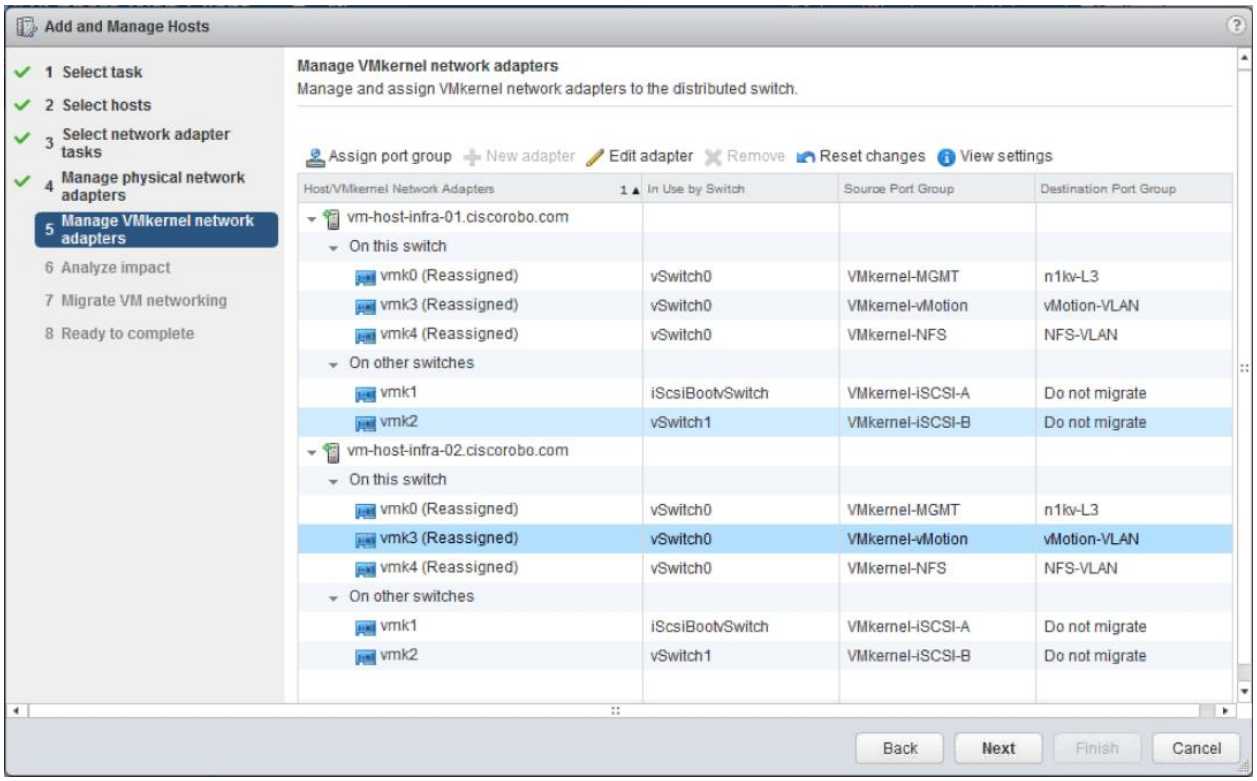
5. Select the checkboxes next to Manage physical adapters, Manage VMkernel adapters, and Migrate virtual machine networking. Click Next.



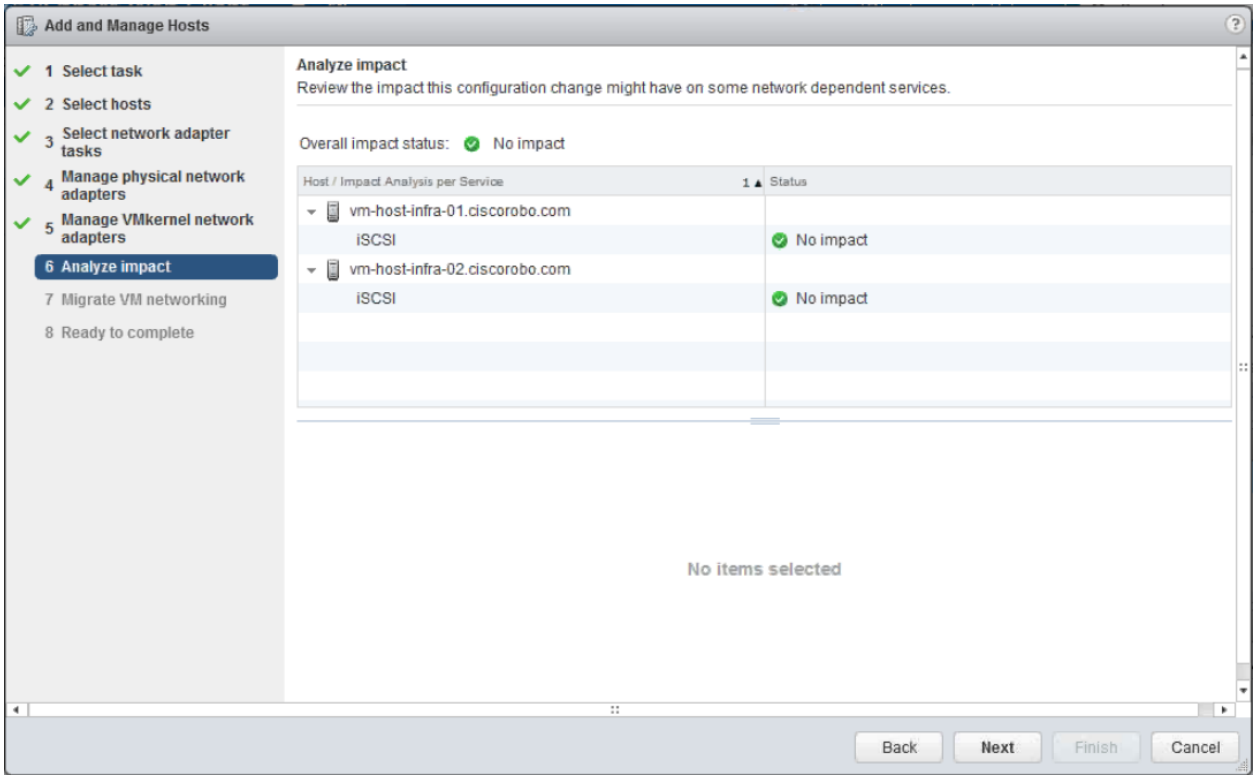
6. On each host, select vmnic1 and click Assign uplink. Select Uplink01 and the system-uplink Uplink port group. Click OK. Repeat this step for both hosts.

7. Click Next.

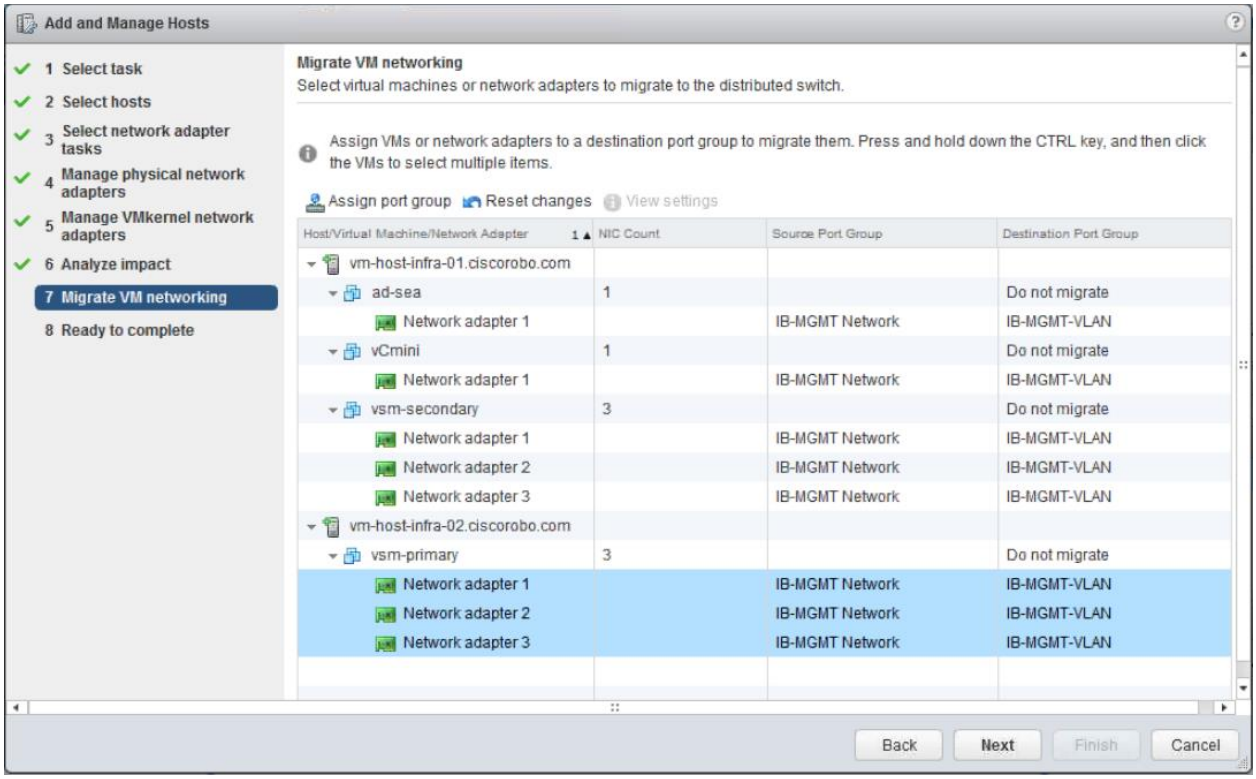
8. On each host, select VMkernel-MGMT and then select Assign port group. In the pop-up, select n1kv-L3 and click OK. Assign the remaining port groups as shown below. Do not migrate the iSCSI VMkernel port groups. Click Next.



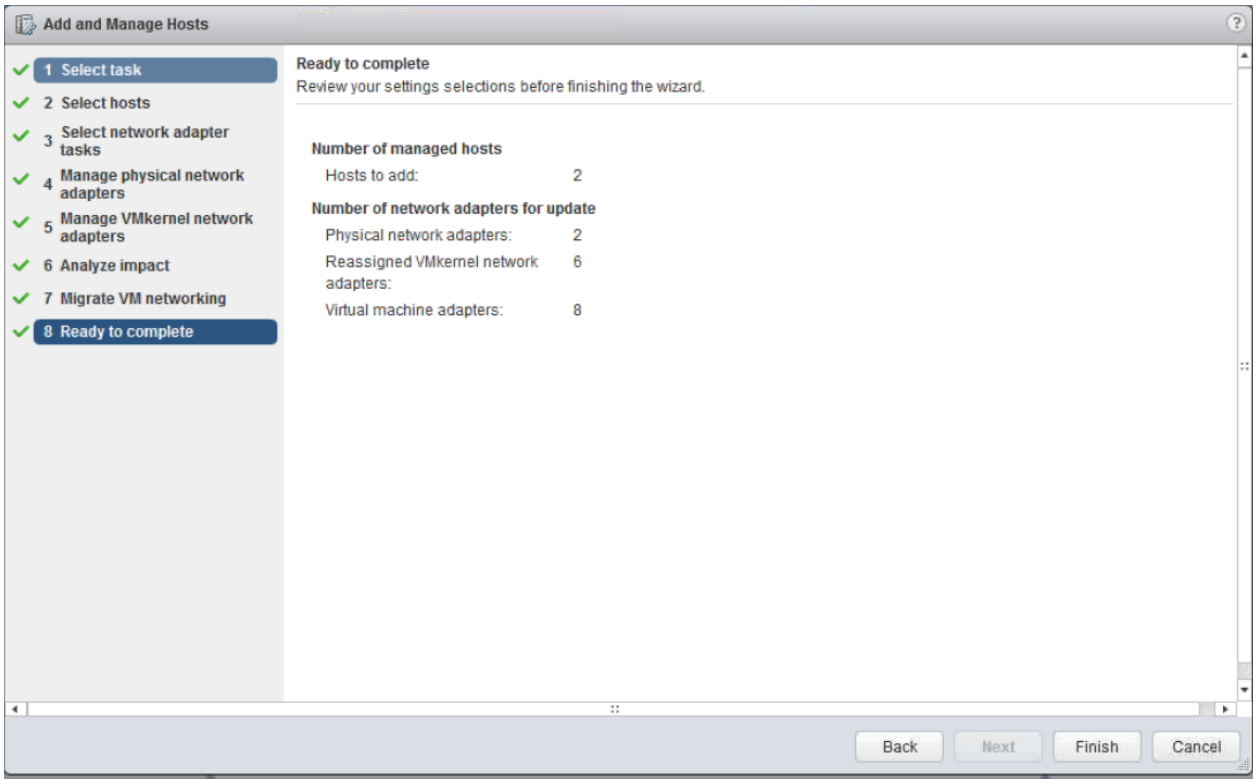
9. Click Next.



10. Expand each VM and select each network adapter. Click Assign port group, select the appropriate port group and click OK. Assign all VM network adapters as shown below. Click Next.



11. Click Finish. Wait for the hosts to be added to the Nexus 1000V.



Remove Standard Switch Networking Components for ESXi Hosts

To remove the unused standard switch components and assign the second vnic on all ESXi servers, complete the following steps:

ESXi Host VM-Host-Infra-01

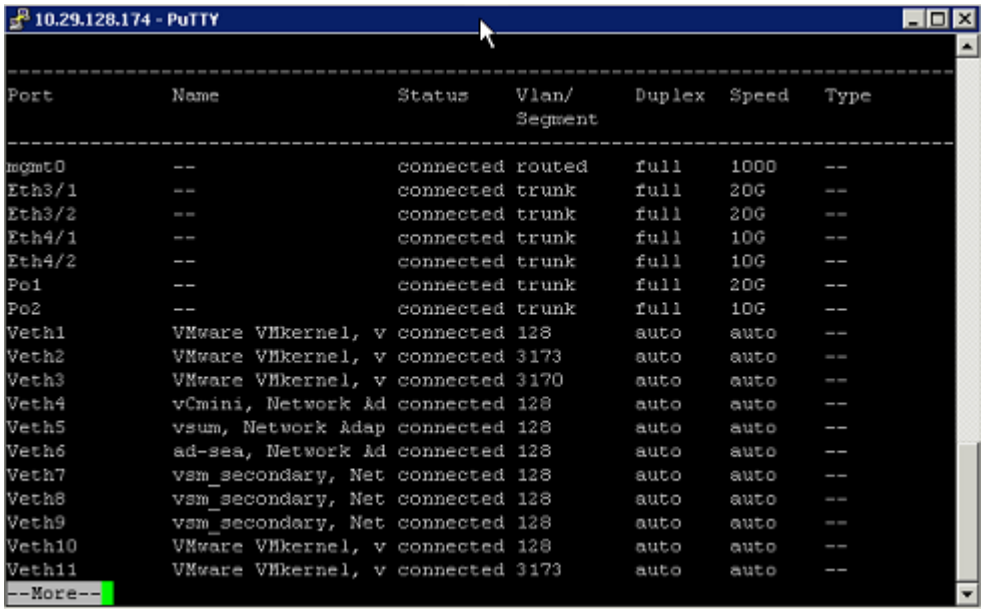
Repeat the steps in this section for all ESXi Hosts.

1. From vSphere web client click the Home button then select Hosts and Clusters.
2. Select vm-host-infra-01 in the list on the left.
3. In the Center pane click Manage and select the Networking tab.
4. In the list select vSwitch0, and click the upper red X to delete.
5. Click yes to remove vSwitch0.
6. Select the Nexus 1000V in the list and click the third icon to manage the physical network adapters connected to the switch.
7. In the pop up window, select UpLink00 and click the green + to add an adapter.
8. Select the system-uplink uplink port group and vmnic0 and click OK.
9. Click OK.
10. The distributed switch should now show 2 connected system uplinks.
11. Select vm-host-infra-02 in the list on the left.
12. In the Center pane click Manage and select the Networking tab.
13. In the list select vSwitch0, and click the upper red X to delete.
14. Click yes to remove vSwitch0.
15. Select the Nexus 1000V in the list and click the third icon to manage the physical network adapter connected to the switch.
16. In the pop up window, select uplink00 and click the green + to add an adapter.
17. Select the system-uplink uplink port group and vmnic0 and click OK.
18. Click OK.
19. The distributed switch should now show 2 connected system uplinks.

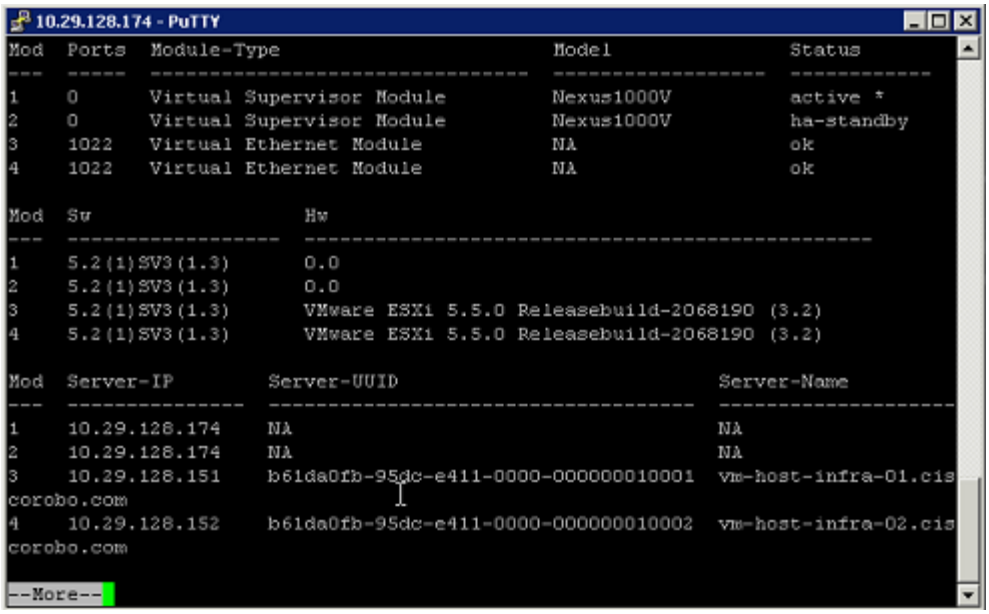
Cisco Nexus 1000V Configuration Verification

To verify the Nexus 1000v configuration, complete the following steps:

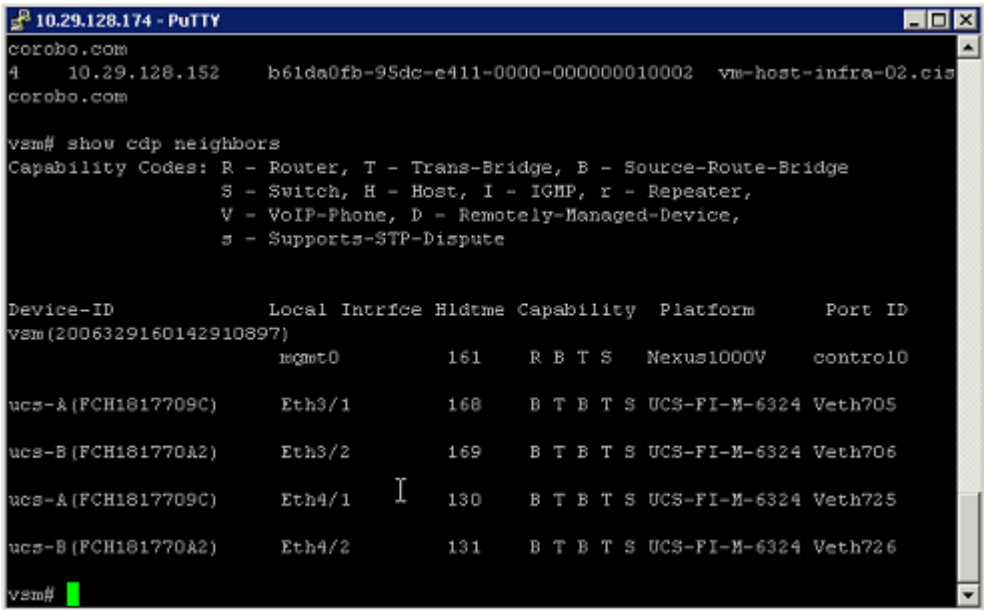
1. From the SSH client that is connected to the Cisco Nexus 1000V VSM, run `show interface status` to verify that all interfaces and port channels have been correctly configured.



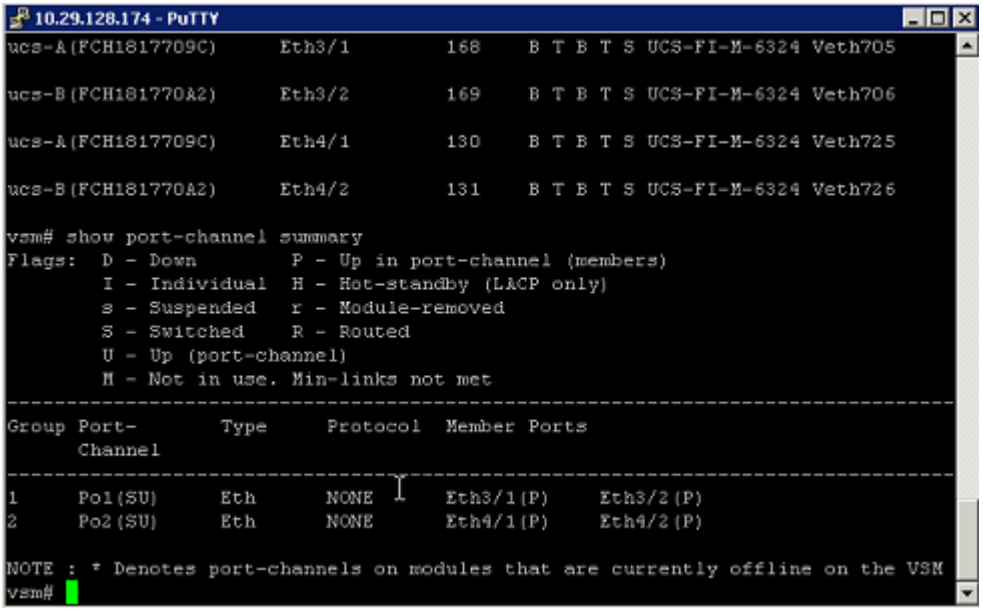
2. Run `show module` and verify that the two ESXi hosts are present as modules.



3. Run `show cdp neighbors` to verify the UCS connections



4. Run `show port-channel summary` to verify all uplinks are operating within port channels.



5. Run `copy run start`.

6. Type `exit` to log out of the Cisco Nexus 1000v.

FlexPod Management Tool Setup

NetApp Virtual Storage Console 6.0 Deployment Procedure

VSC 6.0 Prerequisites

The following licenses are required for Virtual Storage Console (VSC) on storage systems that run clustered Data ONTAP 8.3:

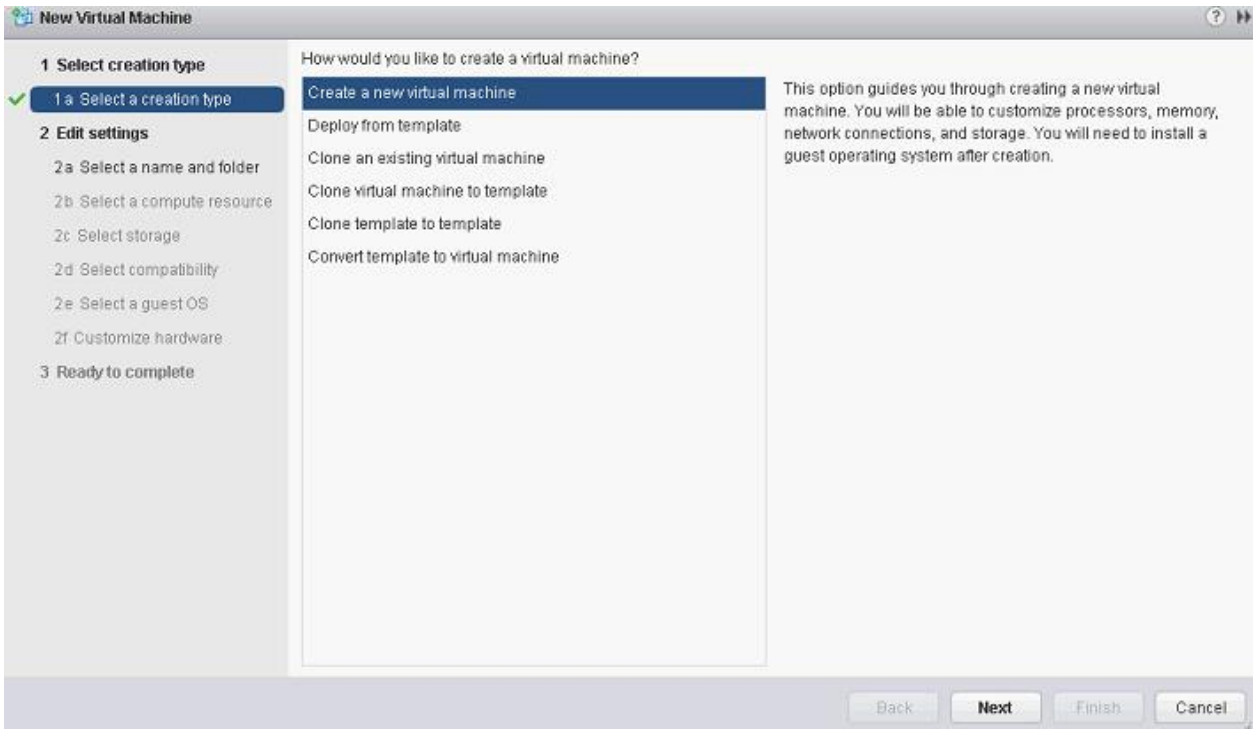
- iSCSI, or NFS license
- FlexClone (for provisioning and cloning only)
- SnapRestore (for backup and recovery)
- SnapManager Suite

Install VSC 6.0

Note: If a centralized vCenter is being used, VSC 6.0 should already be installed with that vCenter and it is not necessary to install VSC 6.0. Continue this procedure below at the heading Optimal Storage Settings for ESXi Hosts.

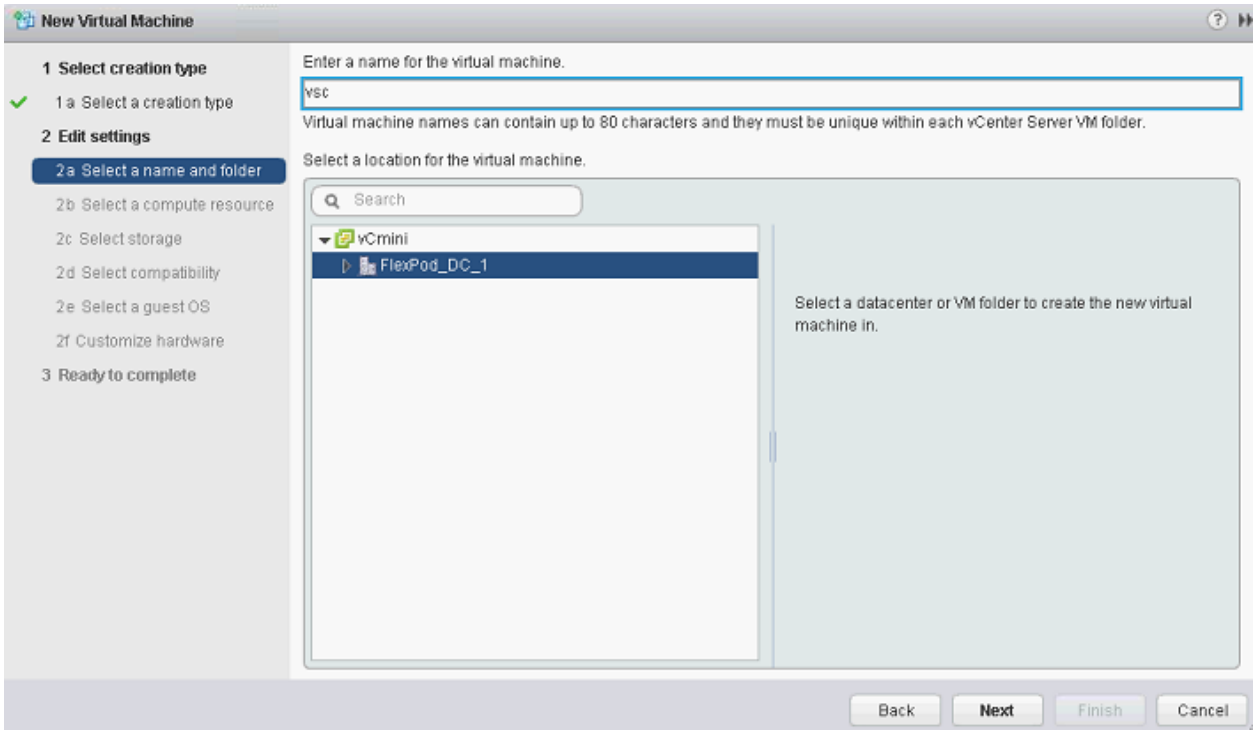
To install VSC 6.0, complete the following steps:

1. Build a VSC VM with 4GB RAM, two CPUs, and one virtual network interface in the `<<var_ib-mgmt_vlan_id>>` VLAN using the following steps. The virtual network interface should be a VMXNET 3 adapter.
2. In the vSphere web client click Home and then click Hosts and Clusters.
3. Right-click the FlexPod_Management cluster and select New Virtual Machine.
4. In the New Virtual Machine window, make sure Create a New Virtual Machine is selected.



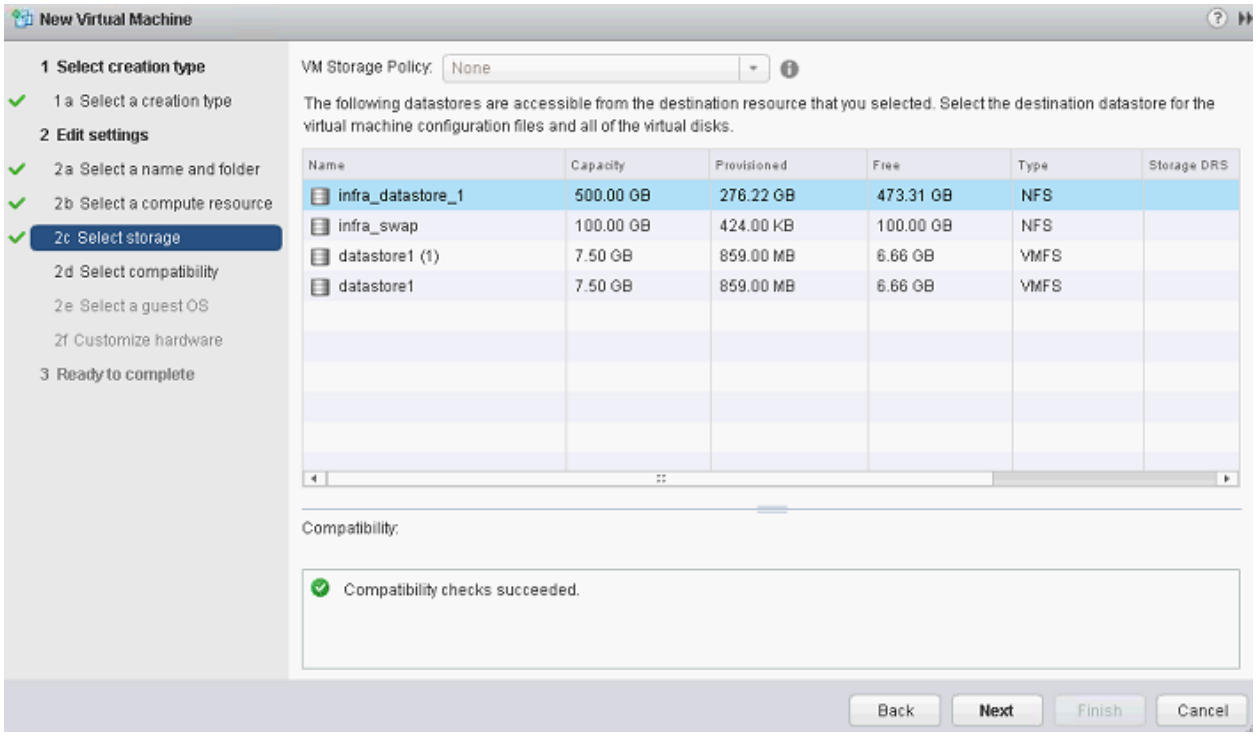
5. Click Next.

6. In the New Virtual Machine window for setting 2a, enter a name for the VM and make sure FlexPod_DC_1 is selected and click Next.

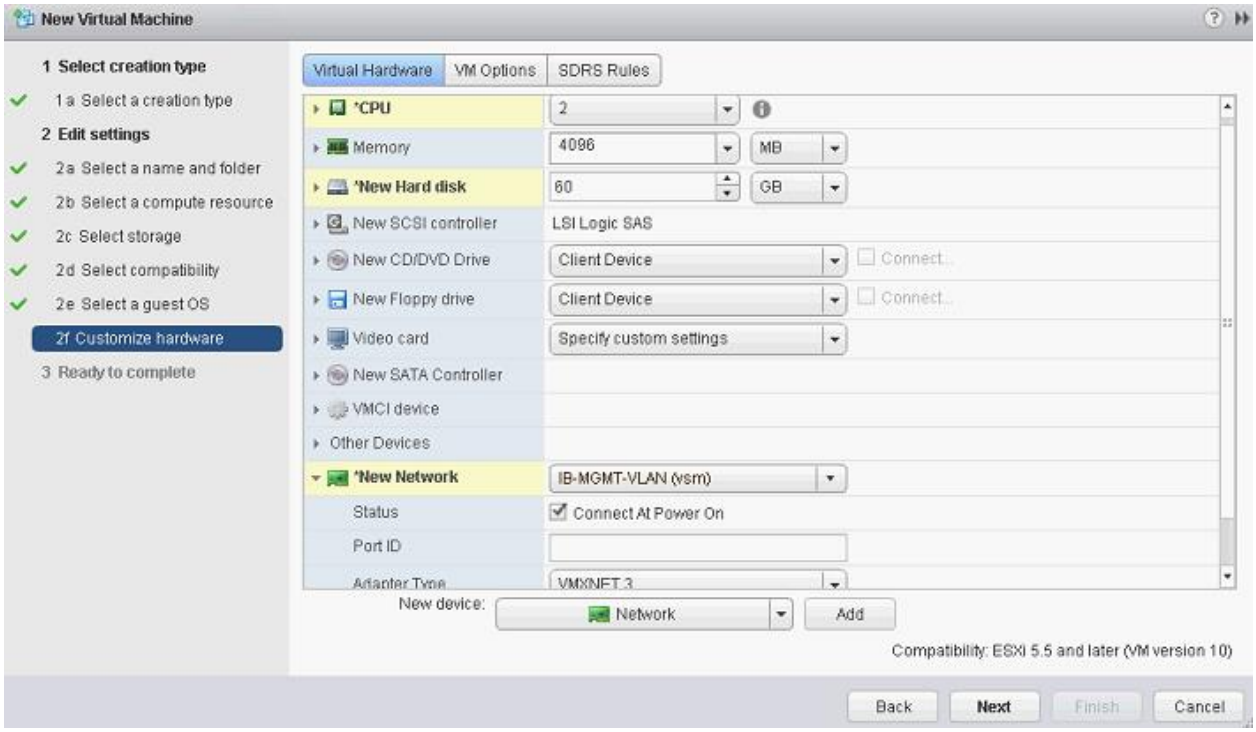


7. For setting 2b, make sure FlexPod Management is selected and click Next.

8. For setting 2c, select infra_datastore_1 and click Next.



9. For setting 2d, make sure ESXi 5.5 and later is selected and click Next.
10. For setting 2e, select the appropriate guest OS (Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2) and click Next.
11. For setting 2f, select the Virtual Hardware tab and do the following:
    a. Select 2 CPUs.
    b. Select 60GB as the size of the new hard disk.
12. For New Device, select Network and click Add.
13. In the New Network drop-down menu, select IB-MGMT-VLAN (vsm).
14. Expand New Network and select VMXNET 3 as the adapter type.



15. Click the VM Options tab.

16. Expand Boot Options and select The Next Time the Virtual Machine Boots, Force Entry into the BIOS Setup Screen checkbox.

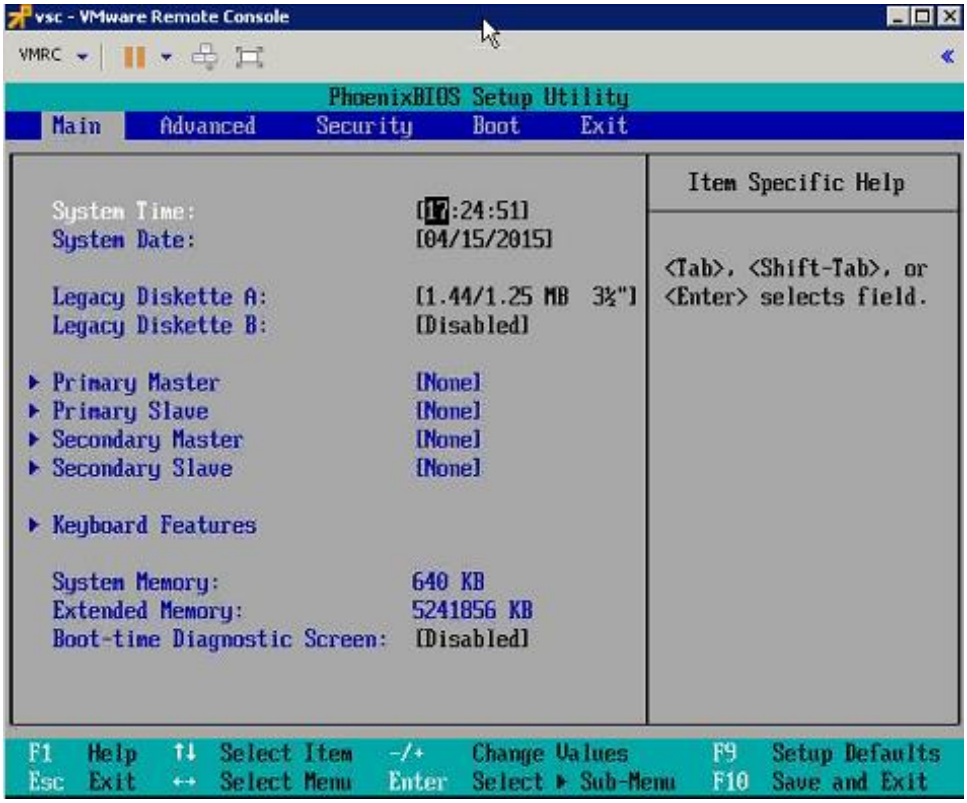
17. Click Next.

18. Verify that the configuration is correct and click Finish.

19. In the vSphere web client, right-click the newly created VM and select Power On.

20. In the center pane, select Open with VMRC.

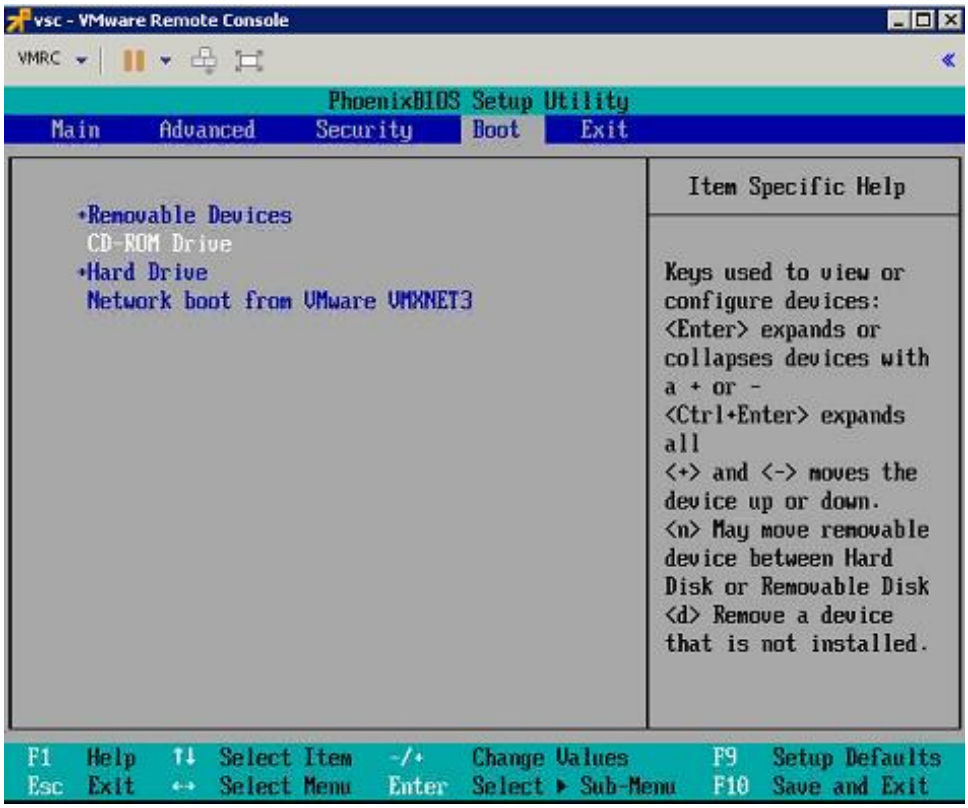
21. The VMware Remote Console opens.



22. From the VMRC drop-down menu, select Removable Devices > CD/DVD drive 1> Connect to Disk Image File (iso).

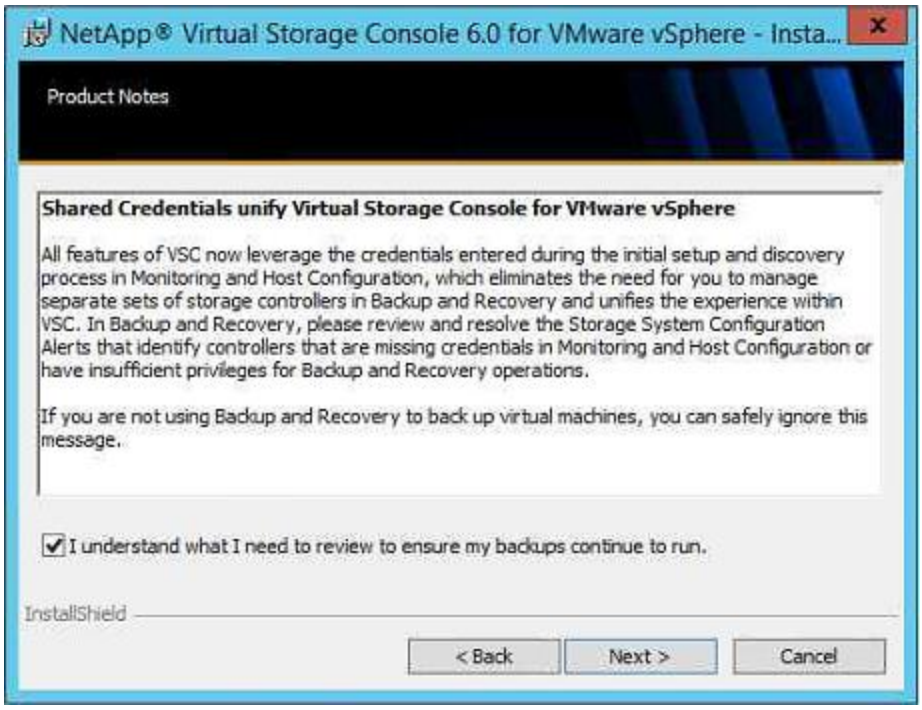
23. Browse to the Windows Server installation ISO image and click Open.

24. Click in the VMware Remote Console and use the right arrow key to open the BIOS boot menu. Using the arrow keys and the + key, move CD-ROM Drive above Hard Drive in the list.



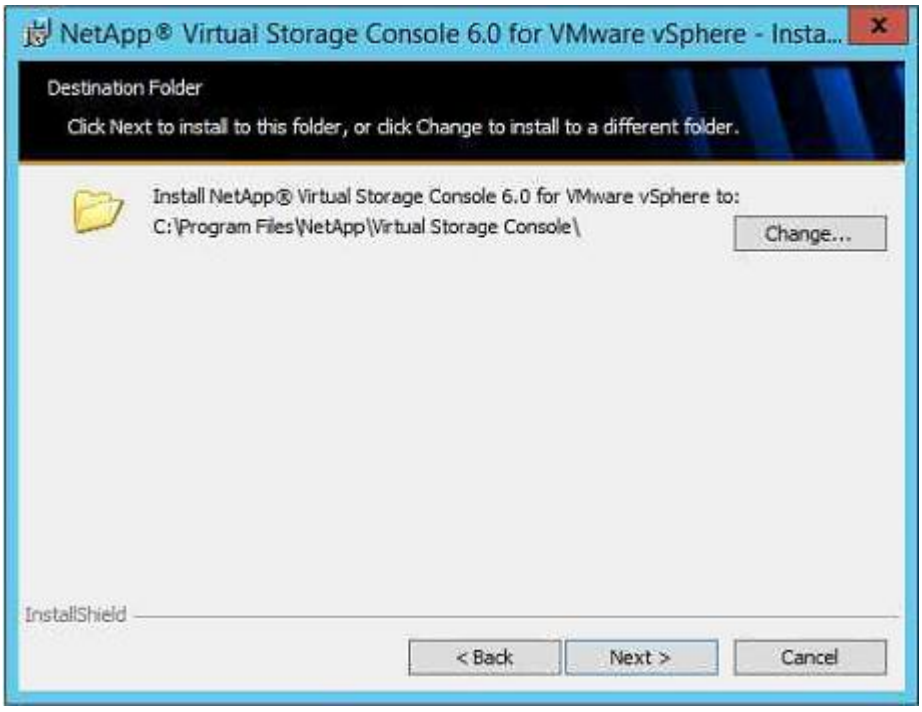
25. Using the arrow keys, navigate to the Exit menu and select Exit Saving Changes.
26. Press Enter to select Yes to confirm setup.
27. The VM boots into the Windows installer.
28. Install Microsoft Windows Server, VMware Tools, and all Windows updates. If available, join the machine to the Active Directory domain.
29. Log in to the VM.
30. Download Virtual Storage Console 6.0 for VMWare from the NetApp Support site and unzip the file.
31. Right-click the extracted `VSC-6.0-win64.exe` file and select Run as Administrator.
32. On the InstallShield Wizard welcome page, click Next.

33. Select the checkbox to accept the message and click Next.



34. Select the Backup and Recovery checkbox and click Next.

35. Click Next to accept the default installation location.



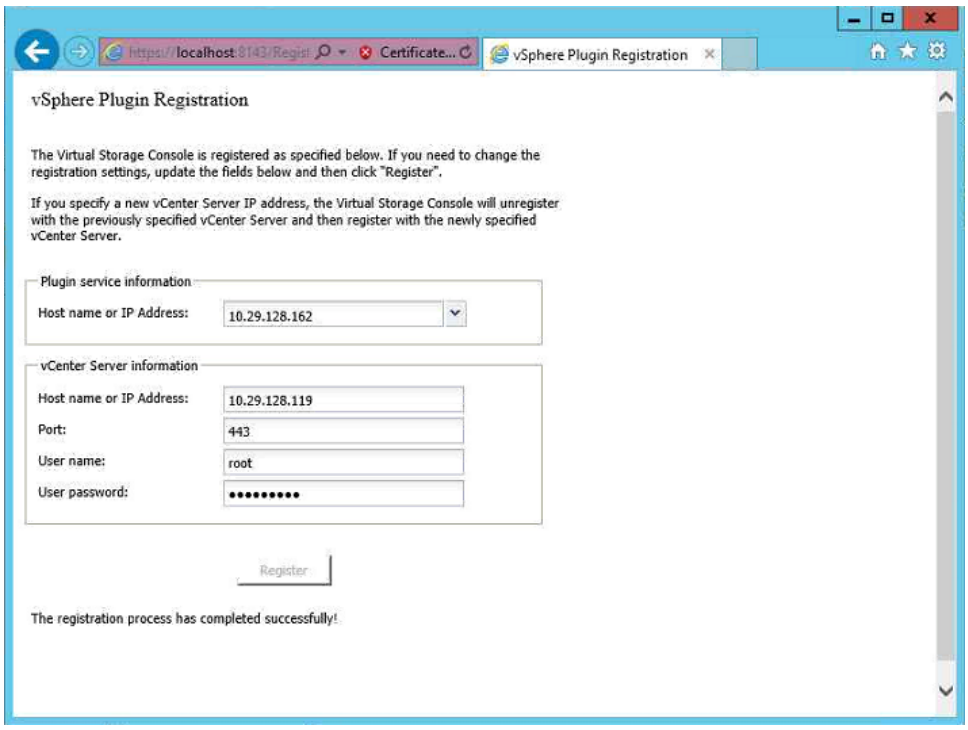
36. Click Install.

37. 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 completes.
2. In the security message, click Continue to This Website (Not Recommended).
3. In the drop-down list in the Plug-in Service Information section, select the local IP address of the VSC VMs that the vCenter Server uses to access the VSC.
4. In the vCenter Server Information section, enter the host name or IP address, user name (root), and the user password for the vCenter Server. Click Register to complete the registration.

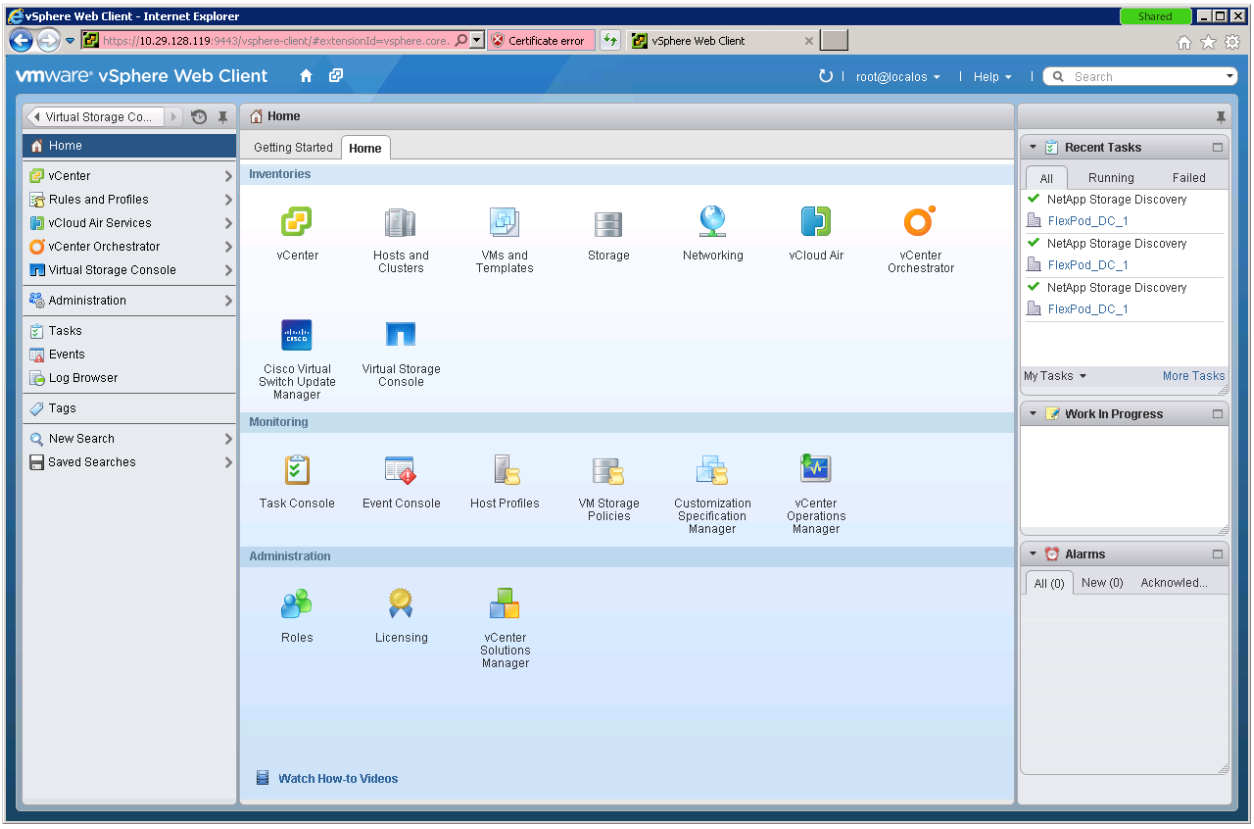


5. Close the web browser.
6. Log out of the VMware vSphere Web Client and log back in again.
7. Click Home and select Virtual Storage Console.

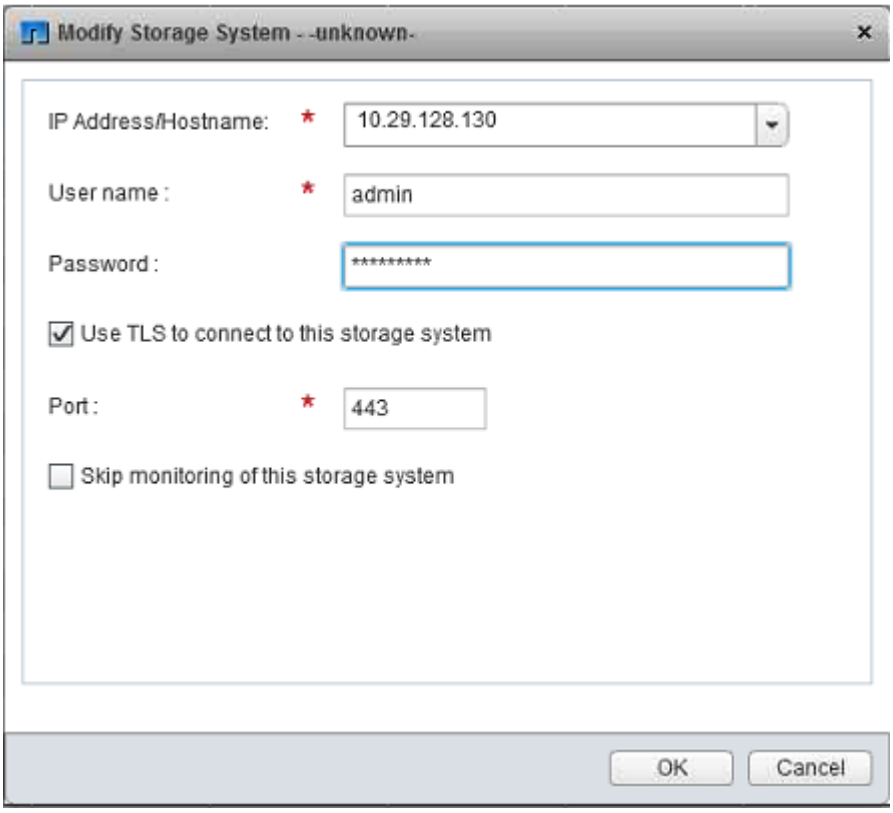
Discover and Add Storage Resources

To discover storage resources for monitoring, host configuration, and provisioning and cloning capabilities, complete the following steps:

1. Using the vSphere web client, click Home and then select the Virtual Storage Console icon.

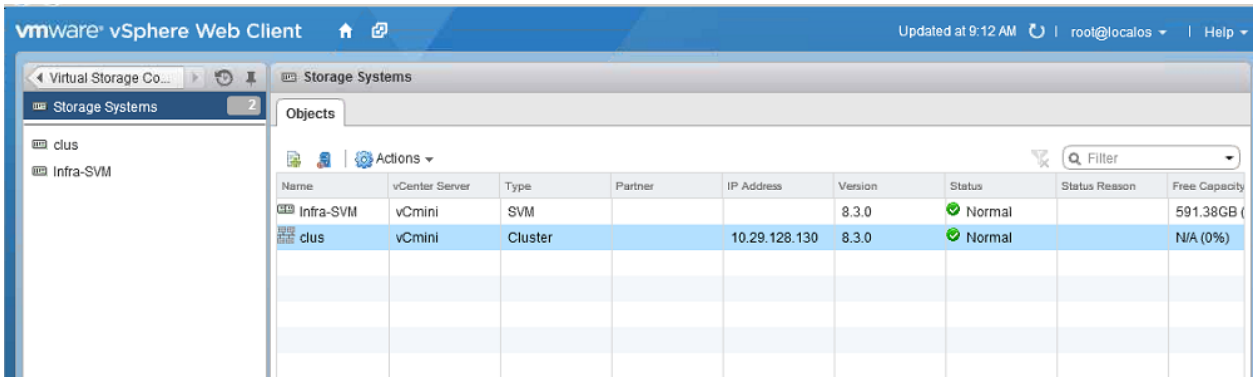


2. In the left pane, select Storage Systems.
3. In the center pane, right-click the storage system that does not have an IP address and select Modify.
4. Enter the storage cluster IP address, user name, and password for the admin user. Click OK.



5. In the Privileges window, click OK. Wait for the Storage Systems Objects tab to update. Click the Refresh icon at the top of the page to update the page, if necessary. It might also be necessary to click the Update All icon located under the Objects tab to make the storage cluster and Infra-SVM appear.

6. From VMware vSphere Web Client, verify that the storage systems are discovered.



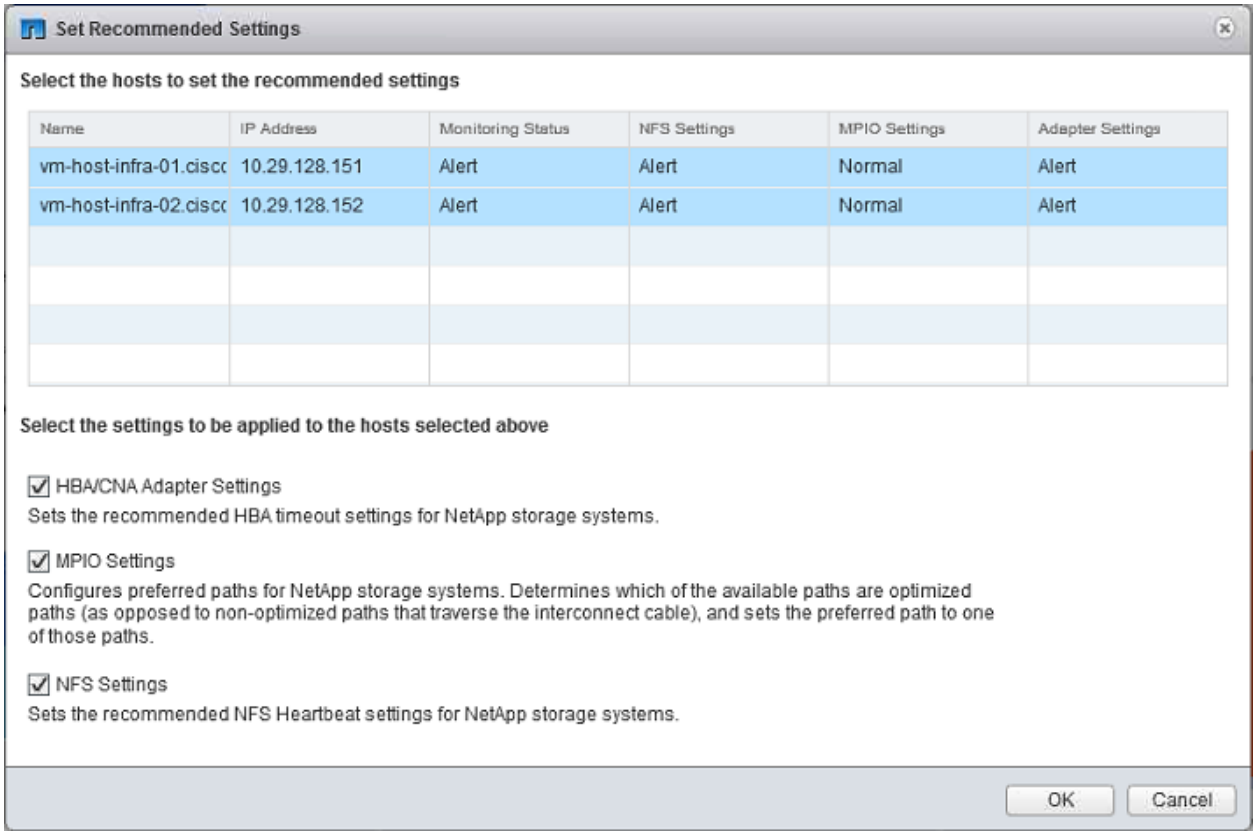
Optimal Storage Settings for ESXi Hosts

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:

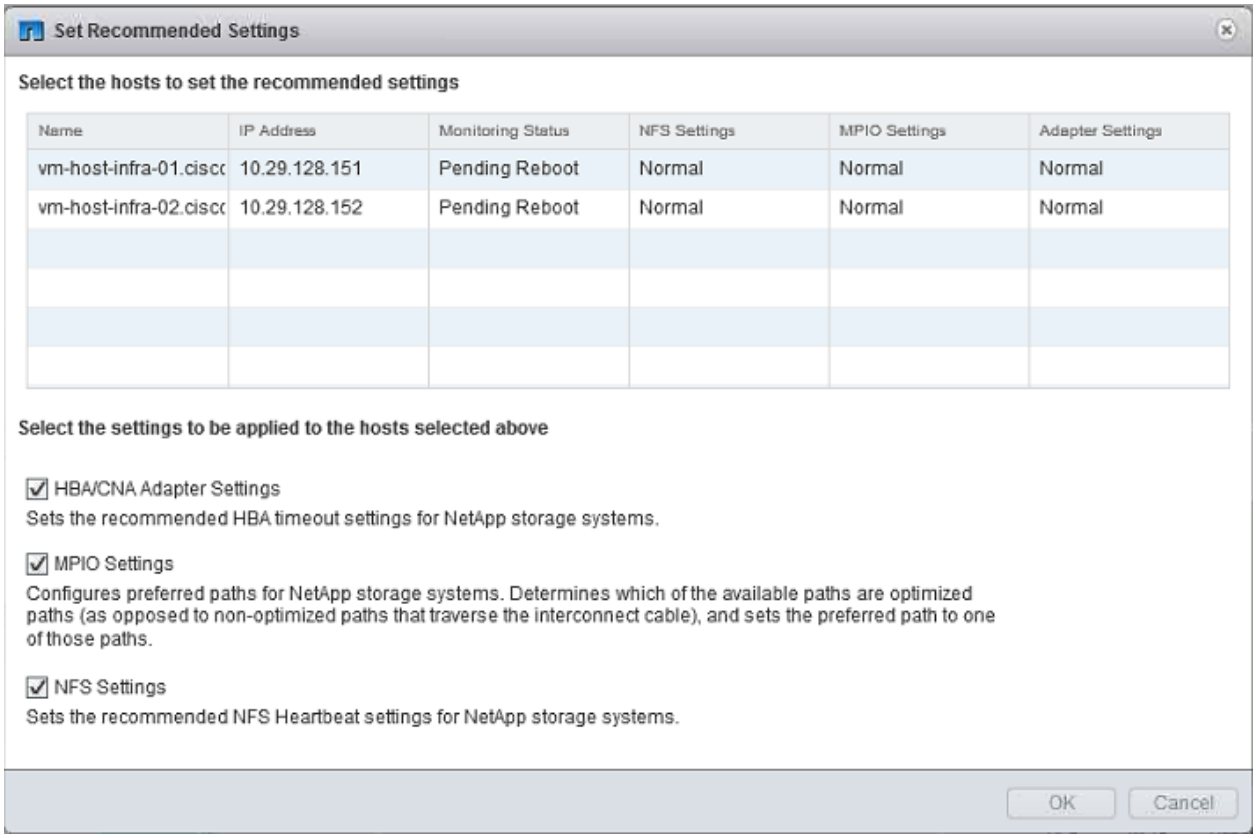
1. From the vSphere web client, click Home and then select the Virtual Storage Console icon.

2. In the center pane, click in the bar graph located under Host Settings Status.

3. Select both of the VMware ESXi hosts and click OK to apply the settings.



4. The monitoring status for both hosts should be Pending Reboot.



5. Click the X the right-hand corner of the page to close the Set Recommended Settings window.
6. One at a time, place each ESXi host in maintenance mode and reboot:
    a. Click Home and select Hosts and Clusters.
    b. Right-click the ESXi host and select Enter Maintenance Mode.
    c. Deselect the Move Powered-off and Suspended Virtual Machines to Other Hosts in the Cluster checkbox. Click OK and click OK again.
    d. It might be necessary to migrate all running machines to the other ESXi host. With the host selected in the left pane, click the Related Objects tab. Select all running VMs in the center pane, right-click, and select Migrate.
    e. Make sure Change Host is selected and click Next.
    f. Select the Allow Host Selection Within This Cluster checkbox and click Next.
    g. Select the host that is not being rebooted and click Next.
    h. Click Next.
    i. Click Finish.
    j. Wait for the maintenance mode task to complete.
    k. Right-click the host and select Reboot.
    l. Enter a reason for the reboot and click OK.
    m. Wait for the host to reboot and rejoin the cluster.

n. Right-click the host and select Exit Maintenance Mode. Wait for the task to complete.

VSC 6.0 Backup and Recovery

Backup and Recovery Capability Prerequisites

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

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

Configure Backup and Recovery

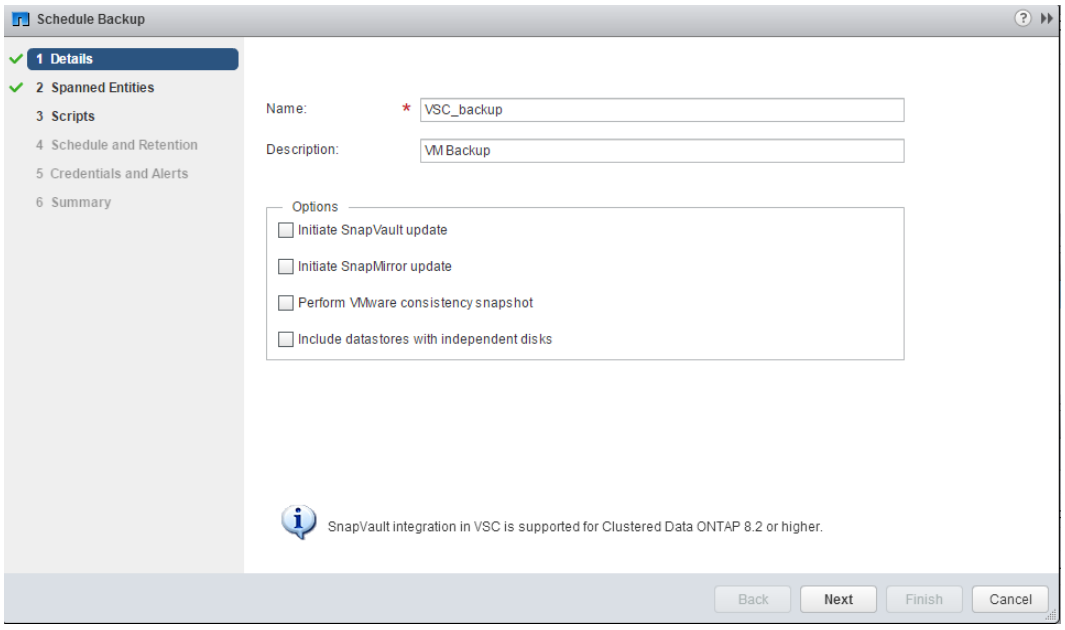
To configure a backup job for a datastore, complete the following steps:

1. From the Home page, click the Home tab and select Storage.
2. Right-click the infra_datastore_1 datastore and select NetApp VSC > Backup > Schedule Backup Job.

Note: To schedule a one-time backup, select Backup Now instead of Schedule Backup.

3. Enter a backup job name and description.

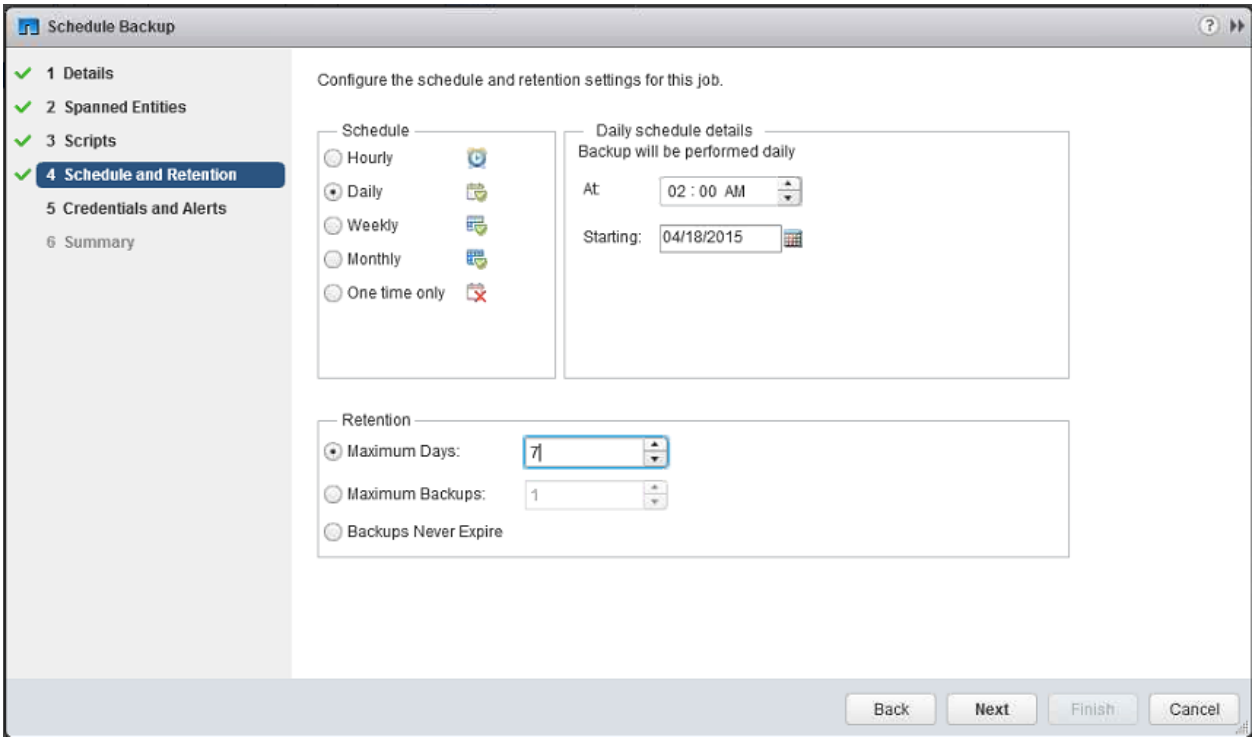
Note: To create a VMware consistency snapshot for each backup, select Perform VMware Consistency Snapshot in the Options pane.



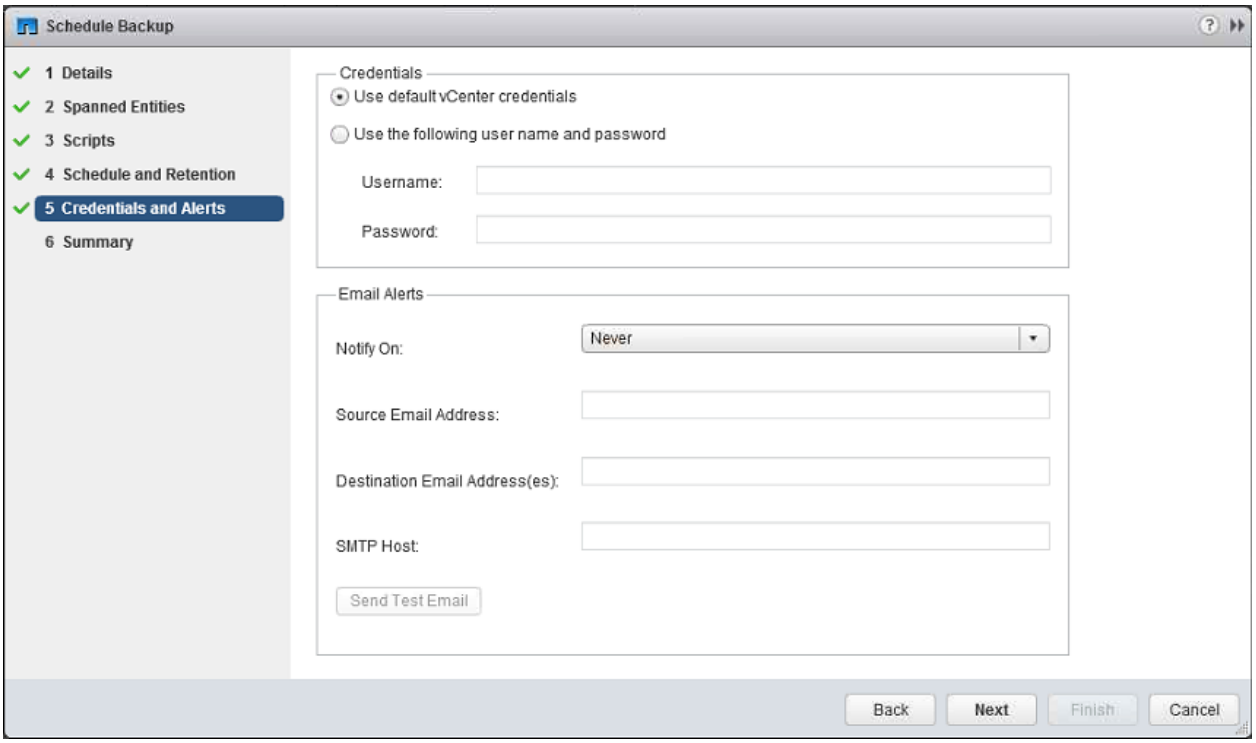
4. Click Next.
5. Click Next.

6. Click Next.

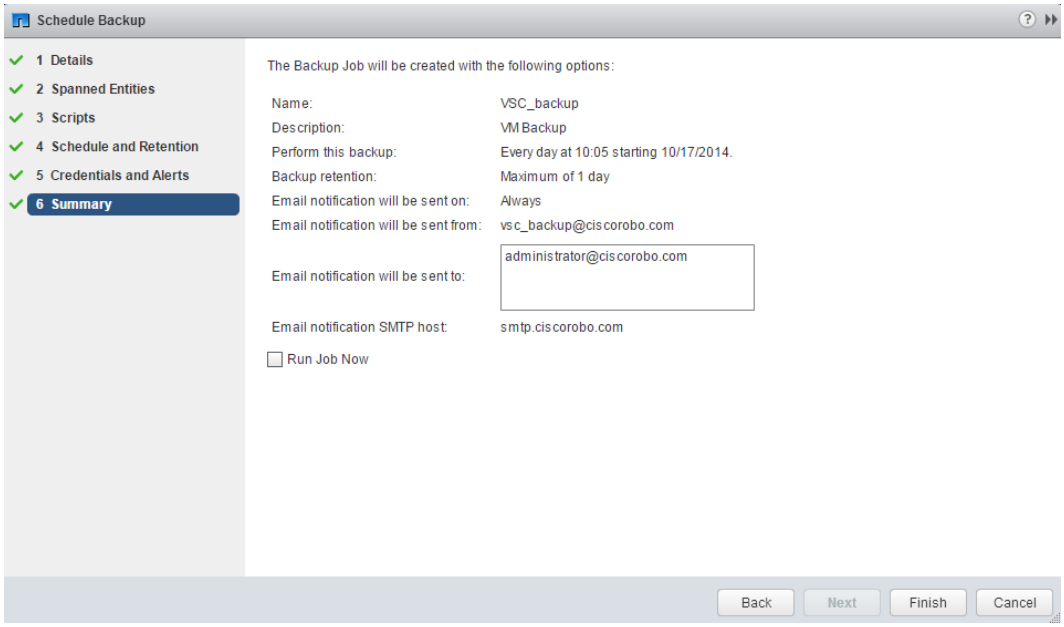
7. Select the hourly, daily, weekly, or monthly schedule for this backup job and click Next.



8. Use the default vCenter credentials or enter the user name and password for the vCenter Server. Complete the Email Alerts section to receive email alerts. If no alerts are required, set Notify On to Never and click Next.



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



10. Click OK.

11. Right-click infra_datastore_1 datastore and select NetApp VSC > Restore to verify that the job completed. The backup should appear in the list. Click Cancel.

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

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

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

13. 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 -vserver Infra-SVM -snapshot <snapshot name>
```

Install NetApp NFS Plug-in for VMware VAAI

The NetApp NFS Plug-in for VMware VAAI runs on the ESXi hosts and takes advantage of enhanced storage features offered by VMware vSphere. The plug-in includes copy offload and space reservation.

To install the NetApp NFS Plug-in for VMware VAAI version 1.0.21 on both ESXi hosts, complete the following steps:

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

1. From the storage cluster SSH interface, run the following command:

```
vserver nfs show –vserver Infra-SVM –fields vstorage
```

2. The `vstorage` field should show enabled. If this field is disabled, run the following command:

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

3. Run the following command to verify that the NFS export rules are properly set up to support the VAAI plugin:

```
vserver export-policy rule show -vserver Infra-SVM
```

4. All rules should have the NFS access protocol. If any rule does not have the NFS access protocol, run the following command:

```
vserver export-policy rule modify -policyname default -ruleindex <rule_number> -vserver Infra-SVM -protocol
nfs
```

5. From the VMware vSphere Web Client, click Home and select Hosts and Clusters.

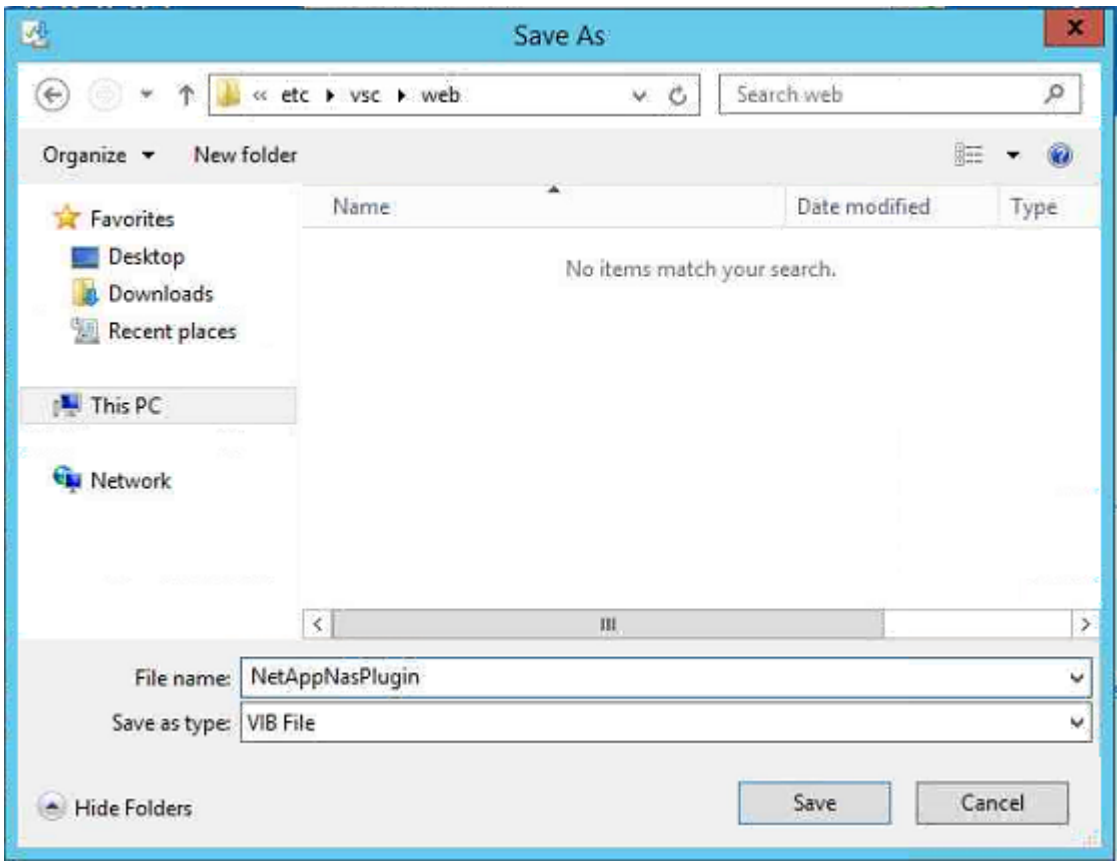
6. In the left pane, select the VSC VM. In the center pane, select Open with VMRC.

7. If necessary, log in to the VM and, using a web browser, navigate to http://mysupport.netapp.com/NOW/download/software/nfs_plugin_vaai/1.0.21.

8. Click Continue.

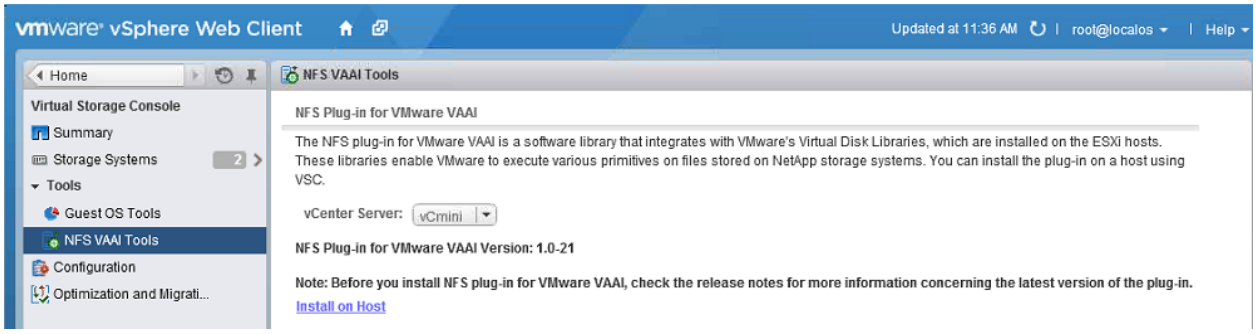
9. Click Accept to accept the EULA.

10. Download `NetAppNasPlugin.v21.vib` to `C:\Program Files\NetApp\Virtual Storage Console\etc\vsc\web` and save as `NetAppNASPlugin.vib`. Click Save.



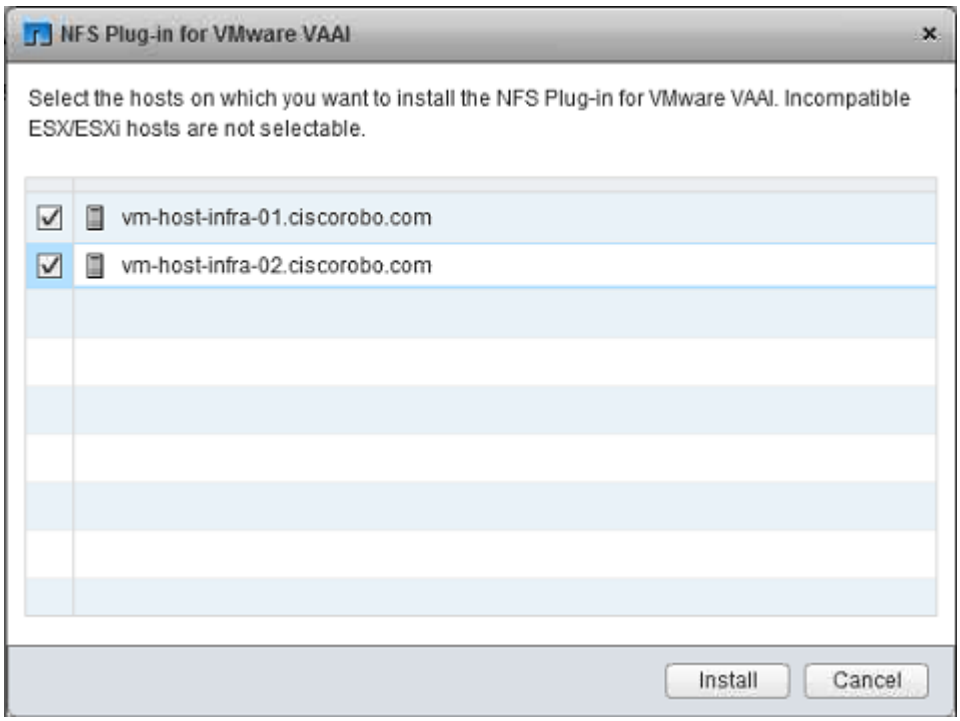
11. In the VMware vSphere Web Client, click Home and select Virtual Storage Console.

12. In the left pane, select NFS VAAI tools. Verify that the NFS Plug-in for VMware VAAI version is 1.0-21.



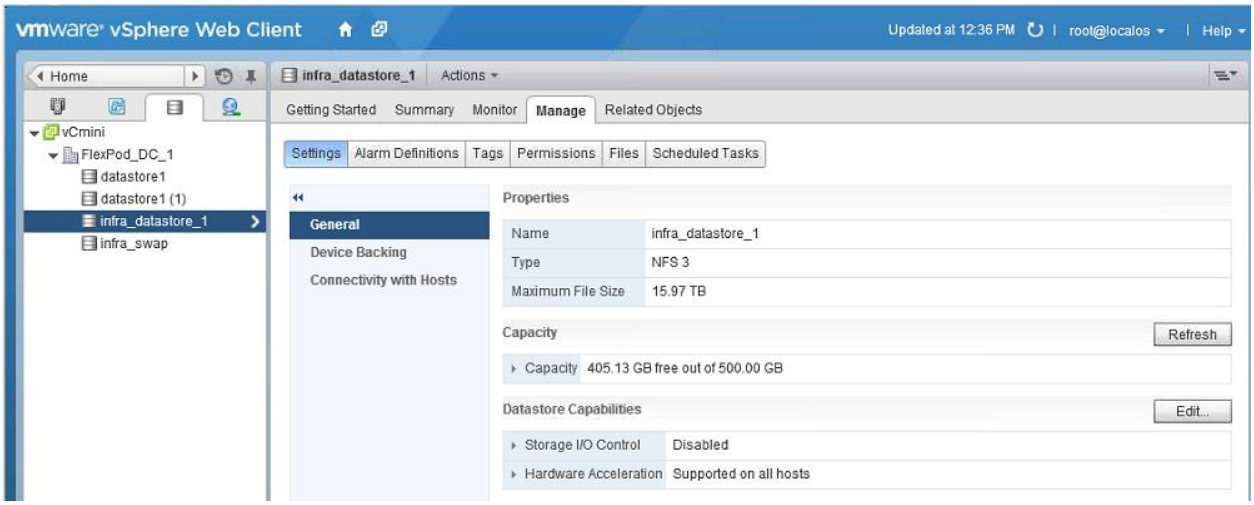
13. Click Install on Host.

14. Select both ESXi hosts and click Install. Click OK in the confirmation message. Wait for the plugin to install on both hosts.



15. One at a time, place each ESXi host in Maintenance Mode and reboot.
    a. Click Home and select Hosts and Clusters.
    b. Right-click the ESXi host and select Enter Maintenance Mode.
    c. Deselect the Move Powered-off and Suspended Virtual Machines to Other Hosts in the Cluster checkbox. Click OK and then click OK again.
    d. It might be necessary to migrate all running machines to the other ESXi host. With the host selected in the left pane, click the Related Objects tab. Select all running VMs in the center pane, right-click, and select Migrate.
    e. Make sure Change Host is selected and click Next.
    f. Select the Allow Host Selection Within this Cluster checkbox and click Next.
    g. Select the host that is not being rebooted and click Next.
    h. Click Next.
    i. Click Finish.
    j. Wait for the maintenance mode task to complete.
    k. Right-click the host and select Reboot.
    l. Enter a reason for the reboot and click OK.
    m. Wait for the host to reboot and rejoin the cluster.
    n. Right-click the host and select Exit Maintenance Mode. Wait for the task to complete.
16. To verify that the plug-in is properly installed, in the VMware vSphere Web Client, click Home then select Storage.

17. In the left pane, select infra_datastore_1. In the center pane, click the Manage tab and select Settings. Under Datastore Capabilities, verify that the Hardware Acceleration field shows Support on All Hosts.



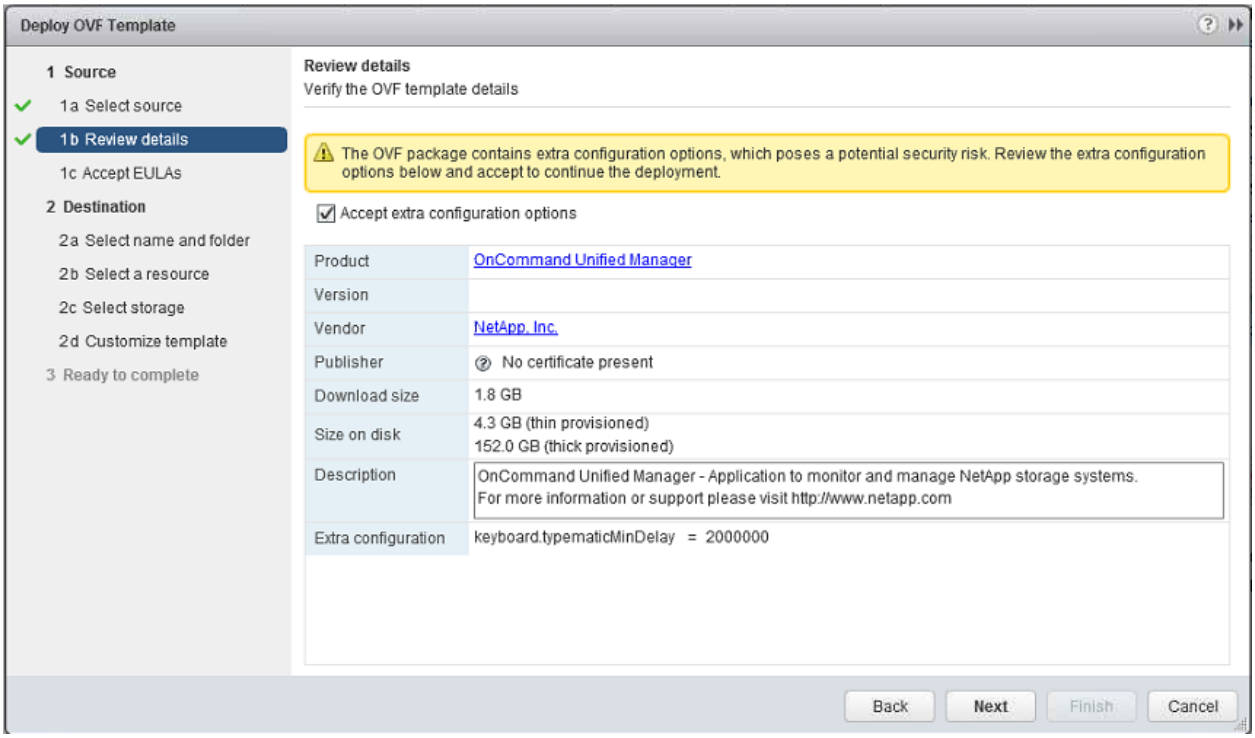
OnCommand Unified Manager 6.2

Install OnCommand Unified Manager

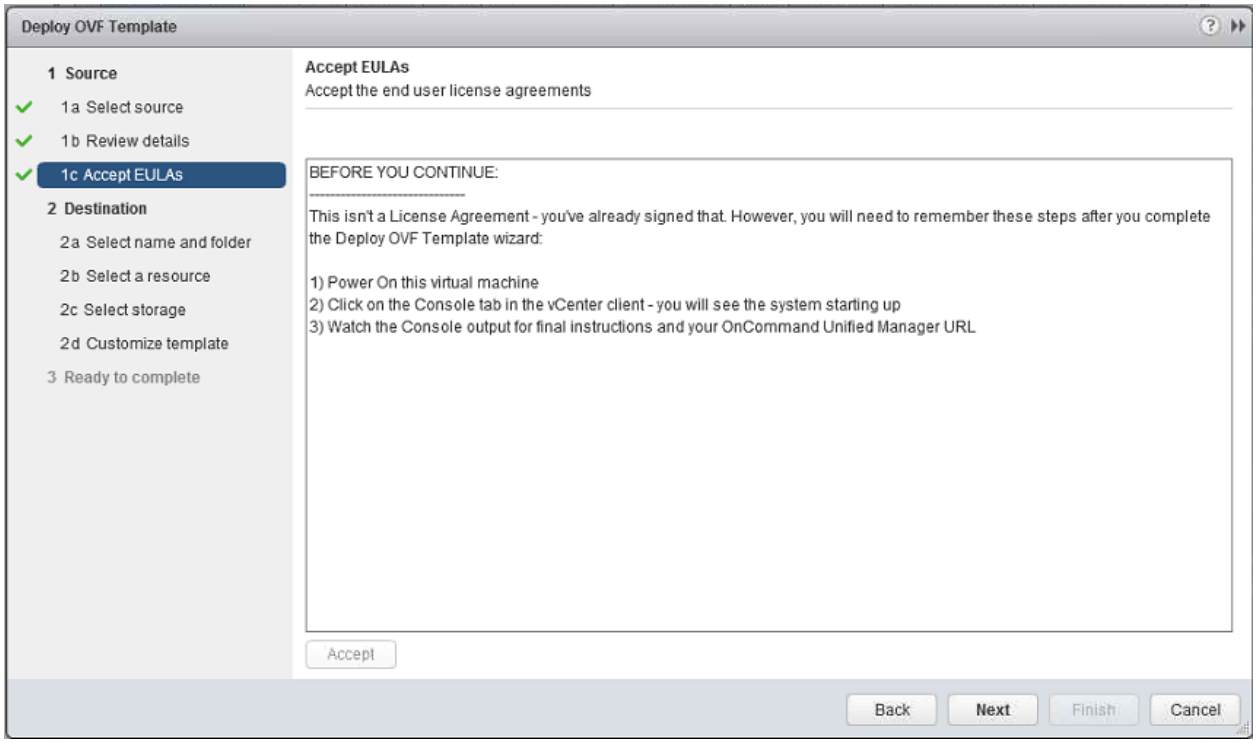
To install the NetApp OnCommand® Unified Manager, complete the following steps:

Note: If a centralized OnCommand Unified Manager is being used, it is not necessary to install On-Command Unified Manager. The storage cluster from the remote office site will need to be added to OnCommand.

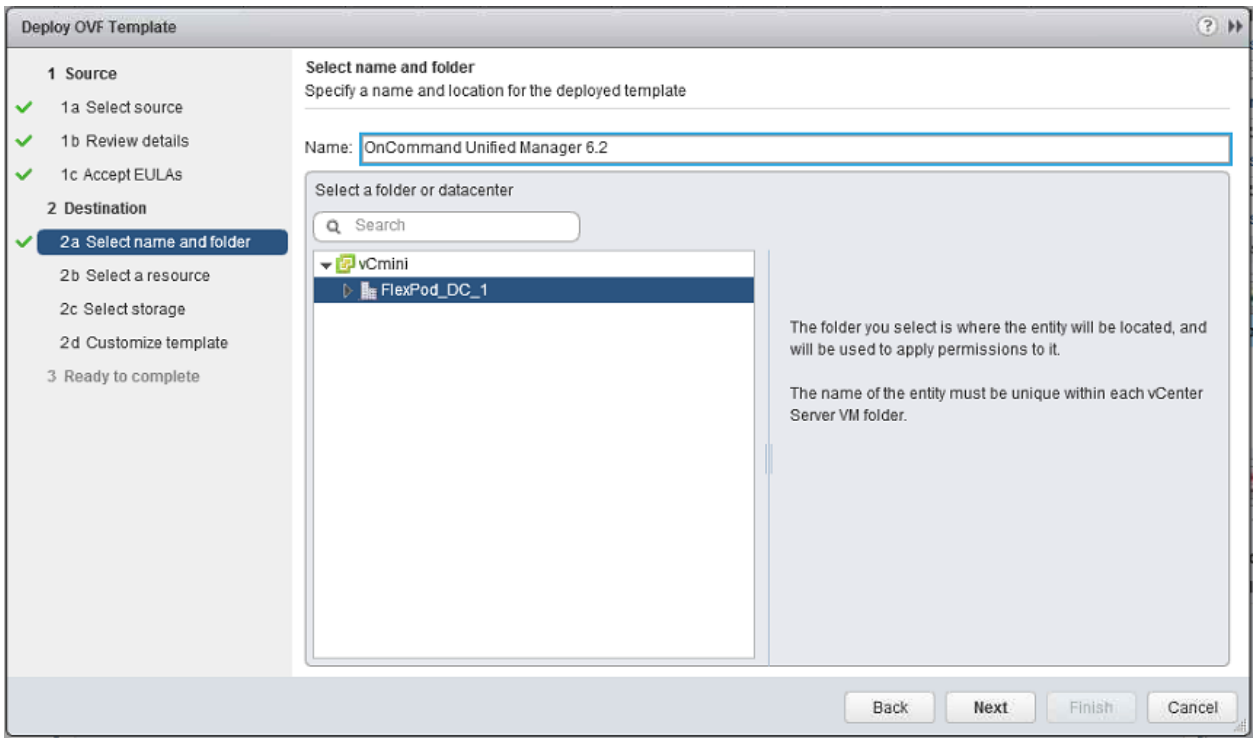
1. Download and review the OnCommand Unified Manager 6.2 Installation and Setup Guide.
2. Download OnCommand Unified Manager (`OnCommandUnifiedManager-6.2.ova`) from the NetApp Support site.
3. Log in to the VMware vSphere Web Client and click Home > VMs and Templates.
4. At the top of the center pane, click Actions > Deploy OVF Template.
5. Click Browse to navigate to the .ova file that was downloaded locally. Click Open to select the file. Click Next.
6. Select the Accept Extra Configuration Options checkbox and click Next.



7. Read the EULA and click Accept to accept the agreement. Click Next.

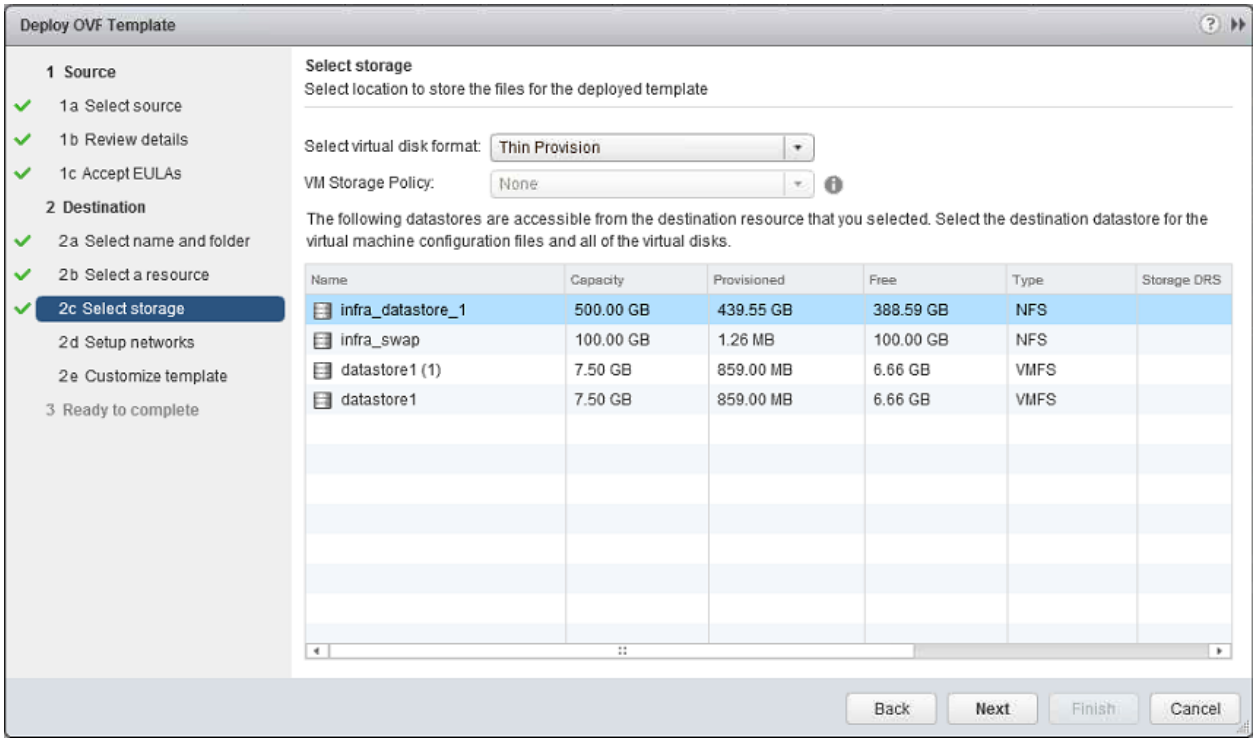


8. Enter the name of the VM and select the FlexPod_DC_1 folder as the location of the VM. Click Next.

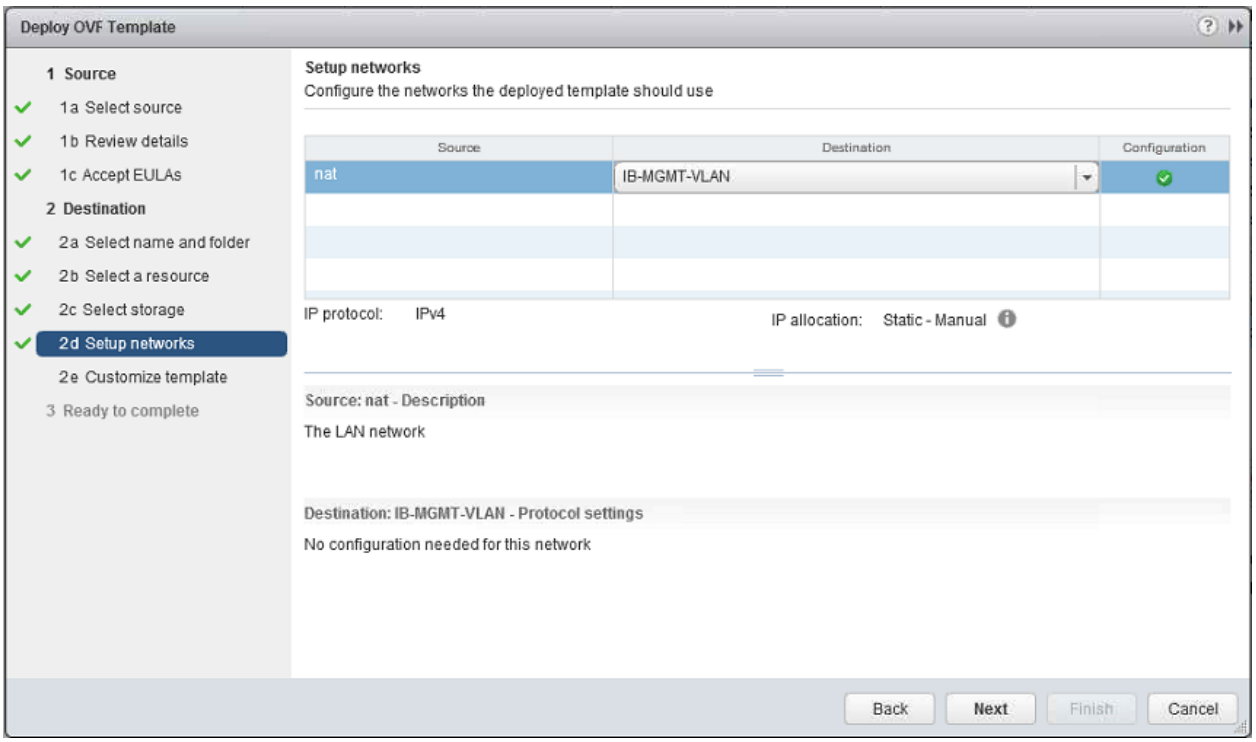


9. Within the FlexPod_DC_1 datacenter, select FlexPod_Management as the destination to host the VM compute resource pool. Click Next.

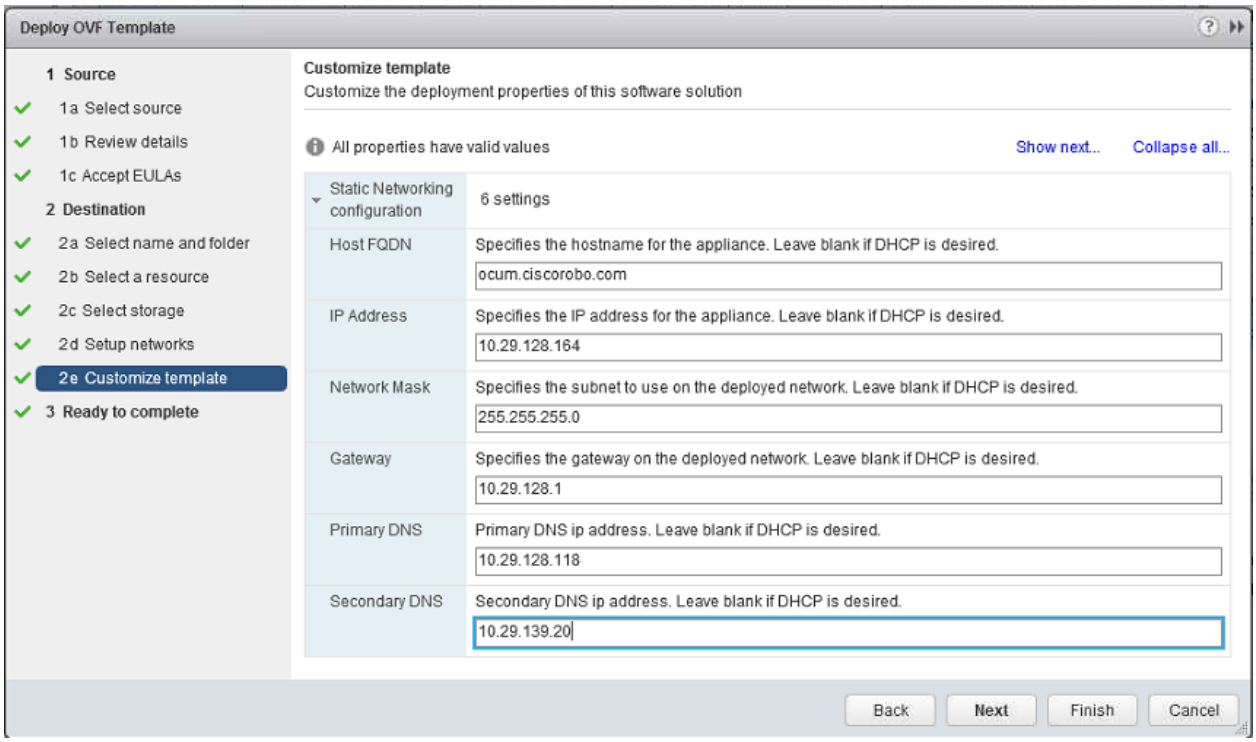
10. Select infra_datastore_1 as the storage target for the VM and select Thin Provision as the virtual disk format. Click Next.



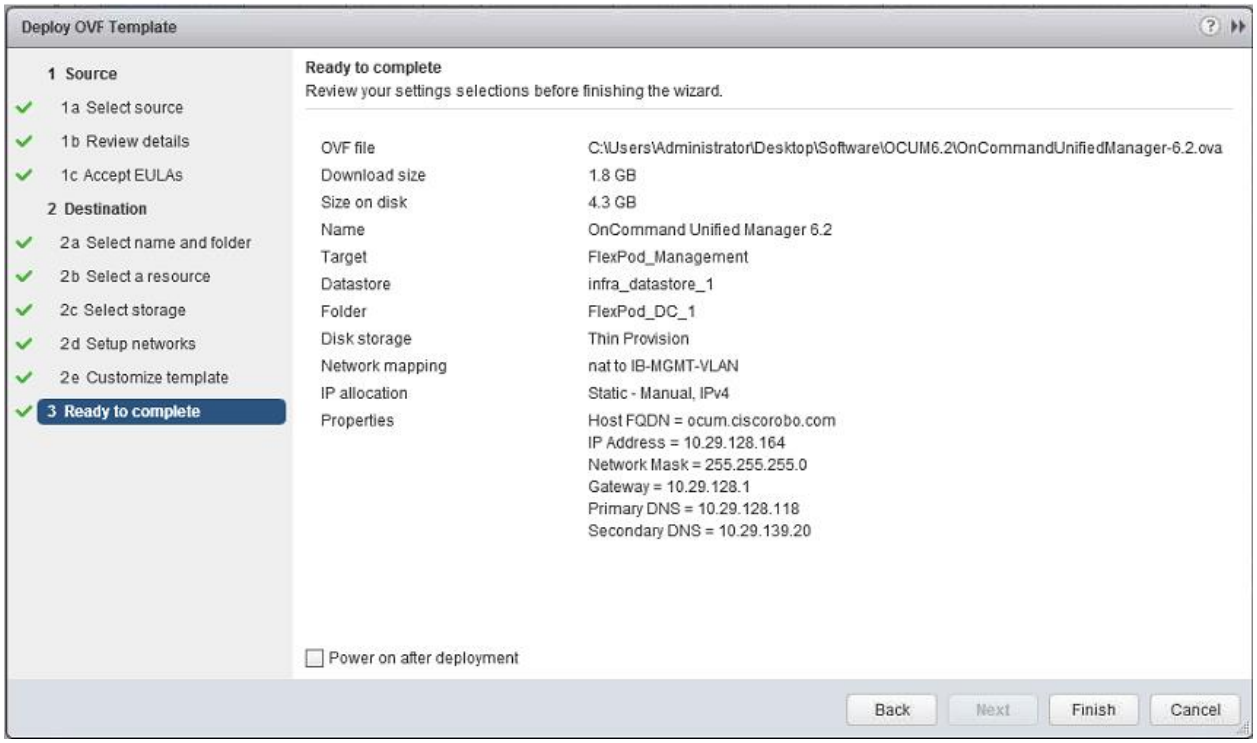
11. Select `IB-MGMT-VLAN` as the destination for the nat source network. Click Next.



12. Enter the hostname, IP address, network subnet mask, gateway, and DNS information. Click Next.



13. Verify the details for the host name, IP address, network mask, gateway, primary DNS, and secondary DNS. Click Finish.



14. In the left pane, expand the FlexPod_DC_1 datacenter, right-click the newly created VM, and select Edit Settings.

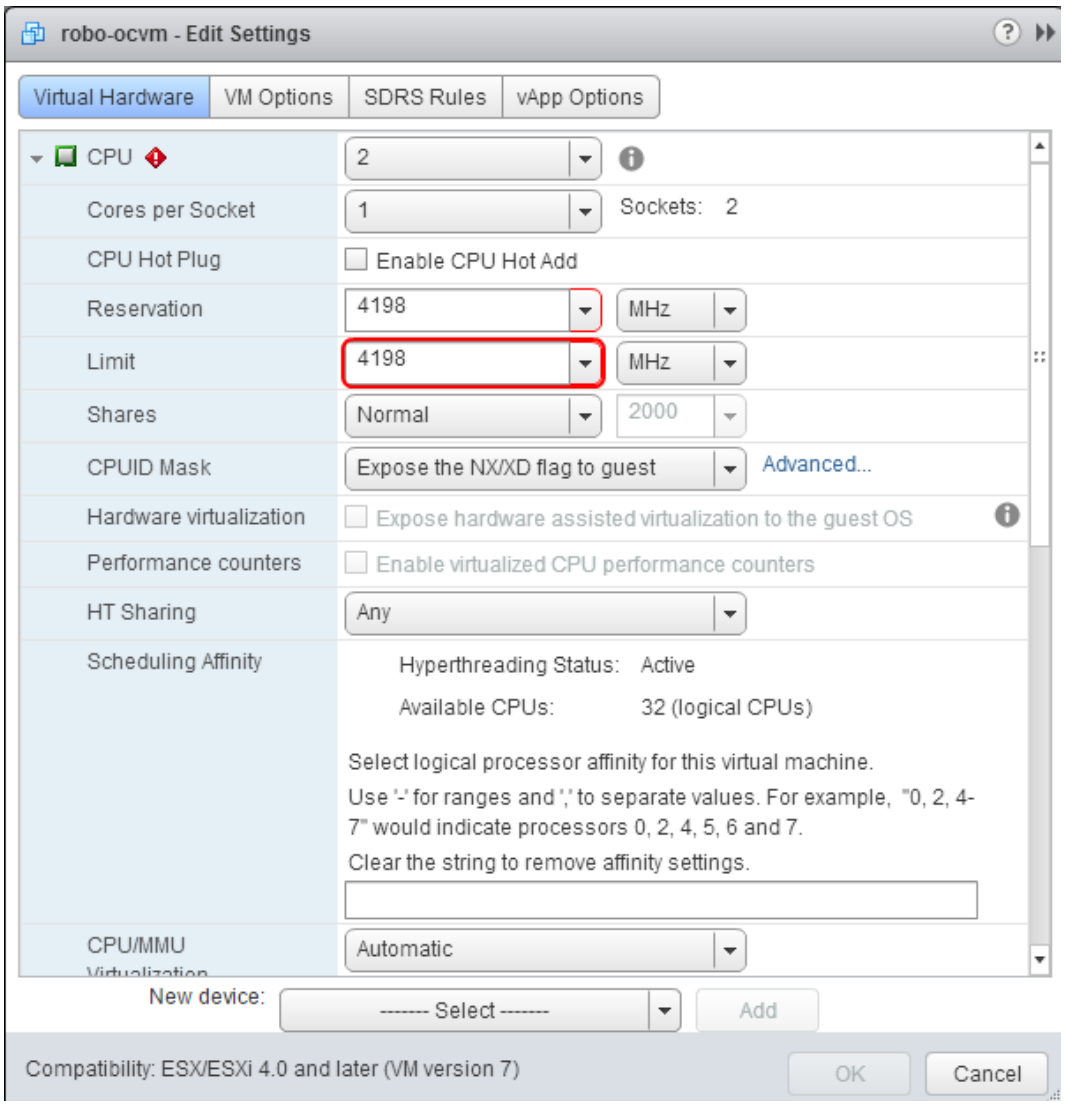
15. Expand the CPU options.

    a. Set the number of CPUs to match the number of CPUs present in the host (2).

    b. Set the reservation and limit in MHz by using the following calculation:

    ```
    (Number of CPUs) × (Processor speed of the CPUs in the host)
    ```

    For example, if a host has 2 CPUs operating at a speed of 2099MHz, the reservation and limit should be set to 4198MHz.



Note: To determine the proper resource size for your environment, refer to the OnCommand Unified Manager 6.2 Installation and Setup Guide.

16. Collapse the CPU section.

17. Set the memory to 8GB.

18. Click OK to accept the changes.

19. Right-click the VM in the left-hand pane and click Power On.

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

a. Decrease the VM resources, such as CPU and memory settings.

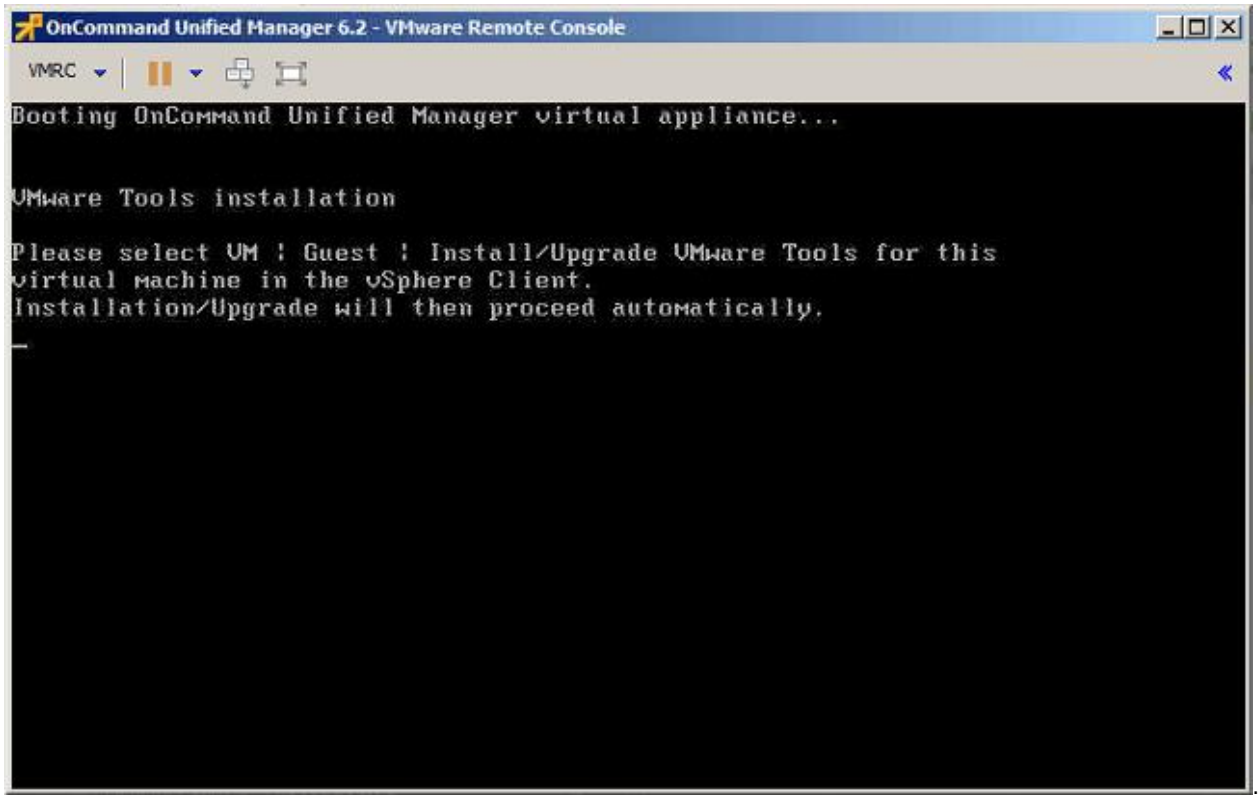
b. Decrease the vSphere HA admission control policy to use less than the default percentage of CPU and memory.

c. Modify the cluster features VM options by disabling the VM restart priority and leaving the host isolation response powered on.

Set Up OnCommand Unified Manager

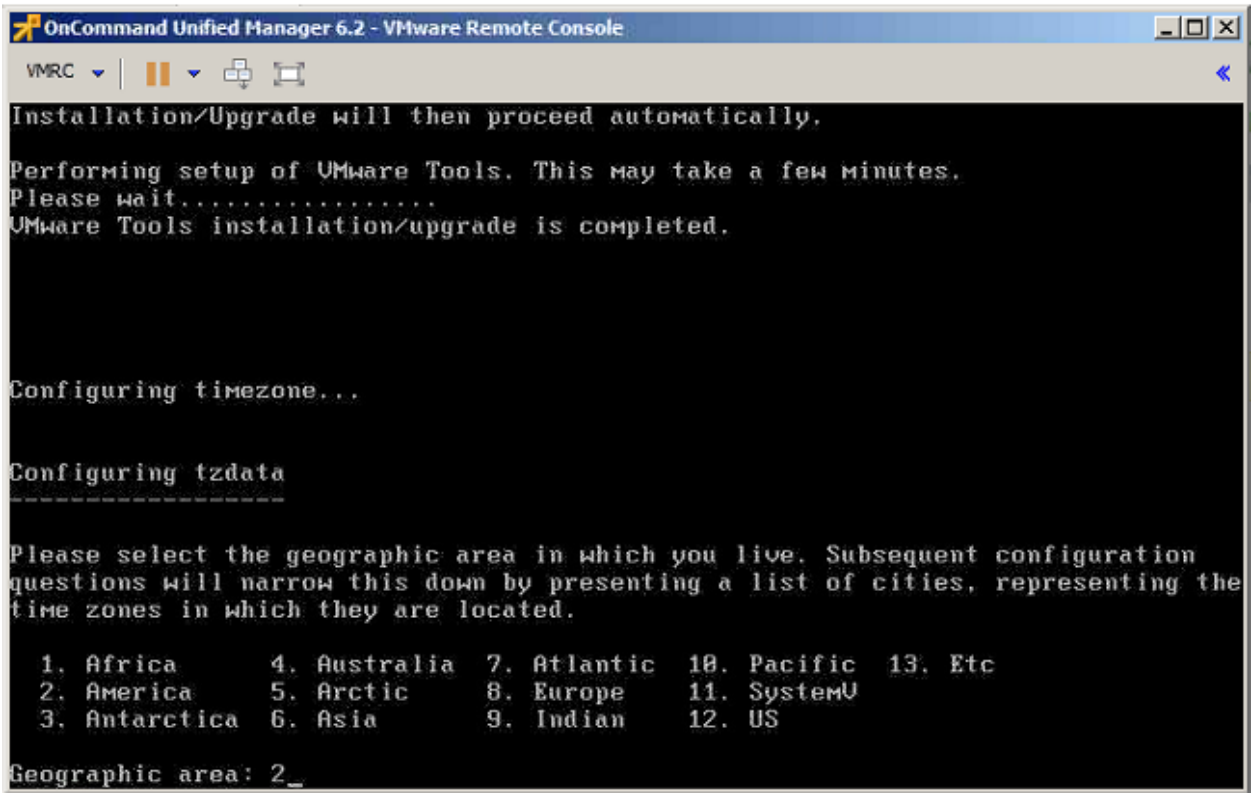
To perform the basic setup for OnCommand Unified Manager, complete the following steps:

1. Select the VM in the left-hand pane. In the center pane, from the Summary tab, select Open with VMRC.



2. From the VMRC drop-down menu in the console window, select Manage > Install VMware Tools to start the installation.

3. Enter the number for the appropriate geographic region and press Enter.



4. Press Enter three times to step though all the time zones. Enter the number that corresponds to your time zone and press Enter.
5. If the network configuration is not valid, complete the following:
    a. Enter 2 to set up a static network configuration.
    b. Enter the OnCommand Unified Manager FQDN.
    c. Enter the OnCommand host IP address.
    d. Enter the network mask.
    e. Enter the default gateway.
    f. Enter the primary DNS address.
    g. Enter the secondary DNS address.
    h. Enter any additional search domains.
    i. Review the information and enter y
6. Run the following commands to create a maintenance user account:

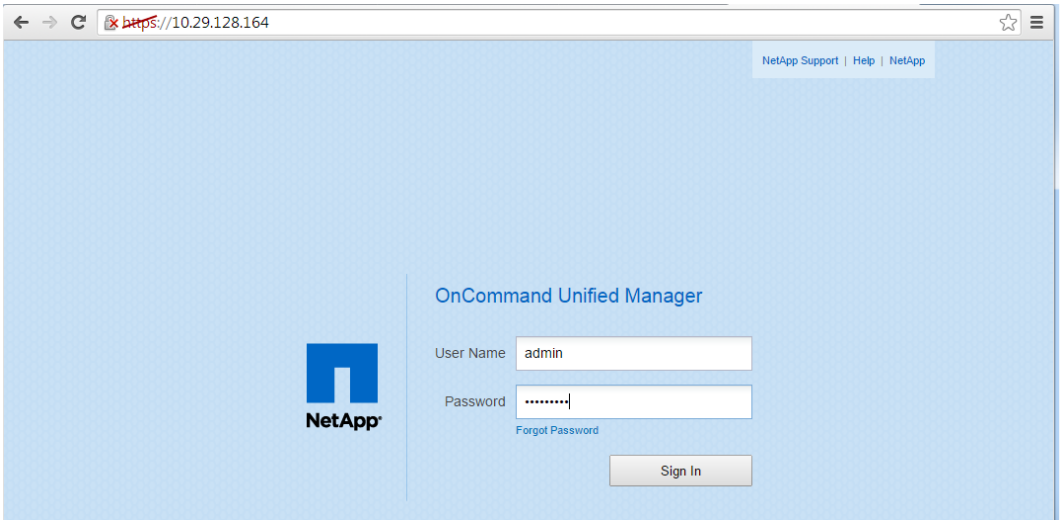
Note: The maintenance user manages and maintains the settings on the OnCommand Unified Manager virtual appliance.

```
Username : admin
Enter new UNIX password: <<var_password>>
Retype new UNIX password: <<var_password>>
```

Configure OnCommand Unified Manager

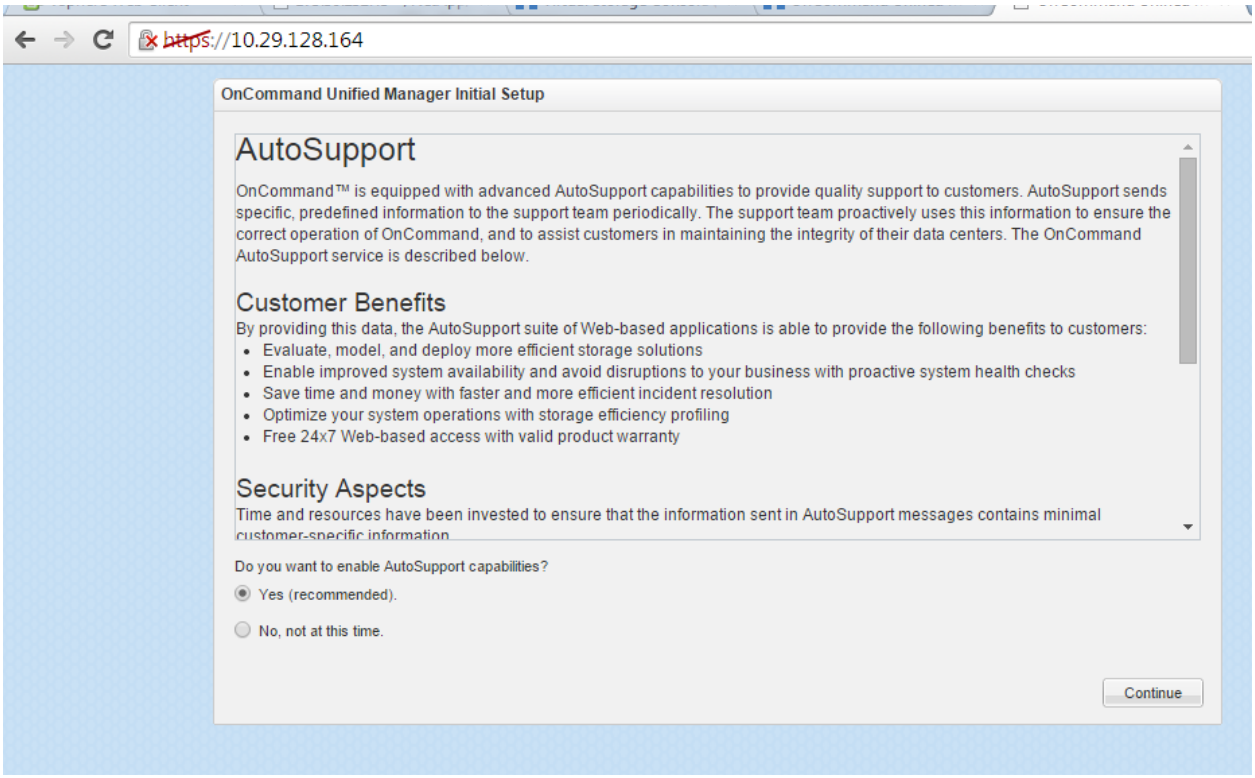
To configure OnCommand Unified Manager, complete the following steps:

1. Using a web browser, navigate to OnCommand Unified Manager by using the following URL: `https://<<var_oncommand_server_ip>>`.

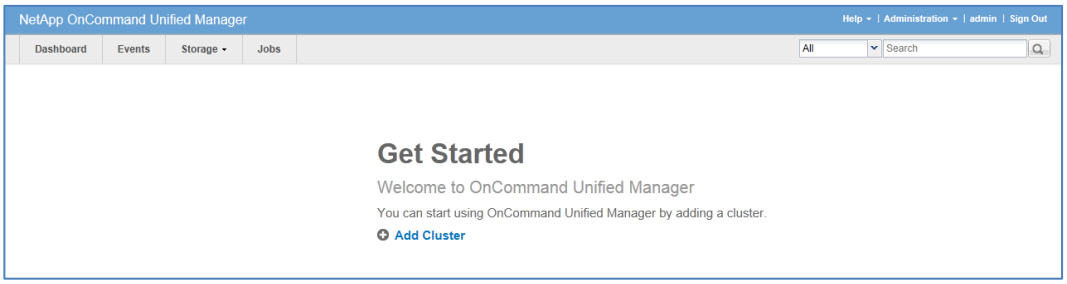


2. Log in by using the maintenance user account credentials.

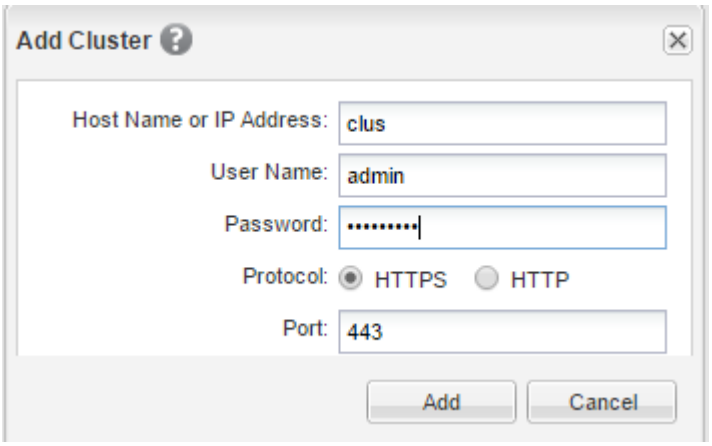
3. Select Yes to enable AutoSupport capabilities and click Continue.

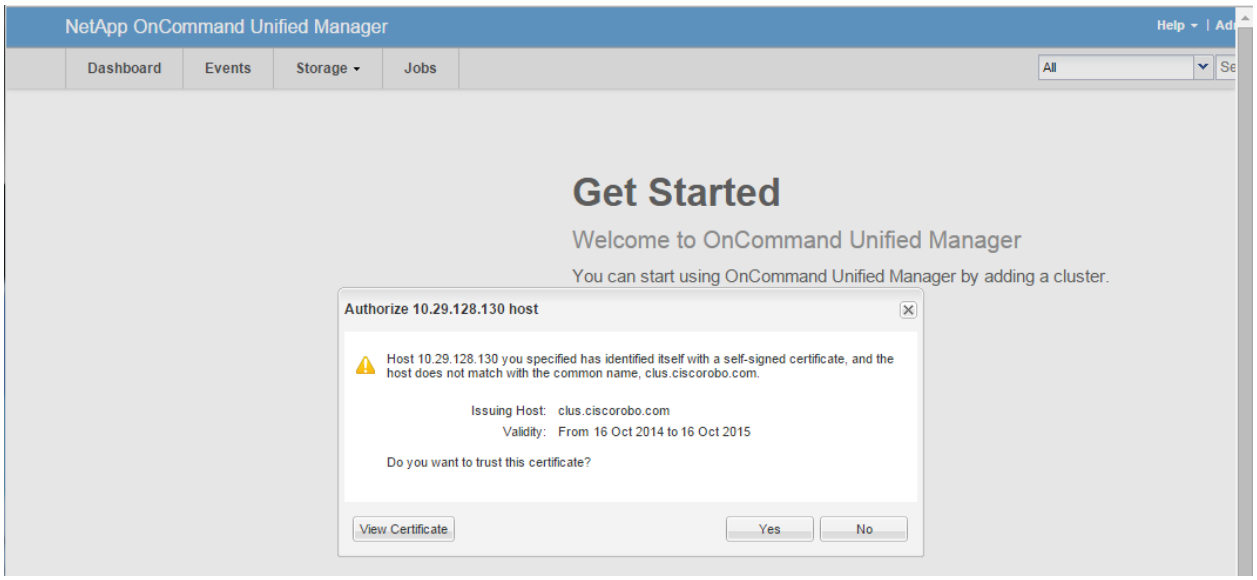


4. Enter the NTP server IP address <<var_global_ntp_server_ip>>.
5. Enter the maintenance user email <<var_storage_admin_email>>.
6. Enter the SMTP server hostname.
7. Click Save.
8. Click Add Cluster.



9. Enter the cluster management IP address, user name, password, protocol, and port and click Add.

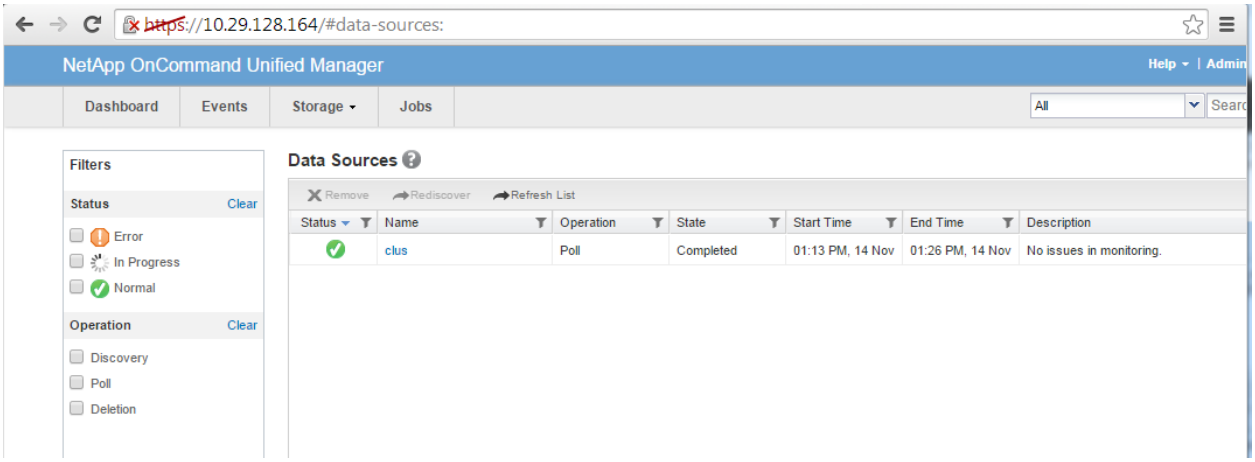




10. Click Yes.

Note: The cluster-add operation might take a couple of minutes.

11. After the cluster is added, click the Dashboard tab to review the storage statistics.

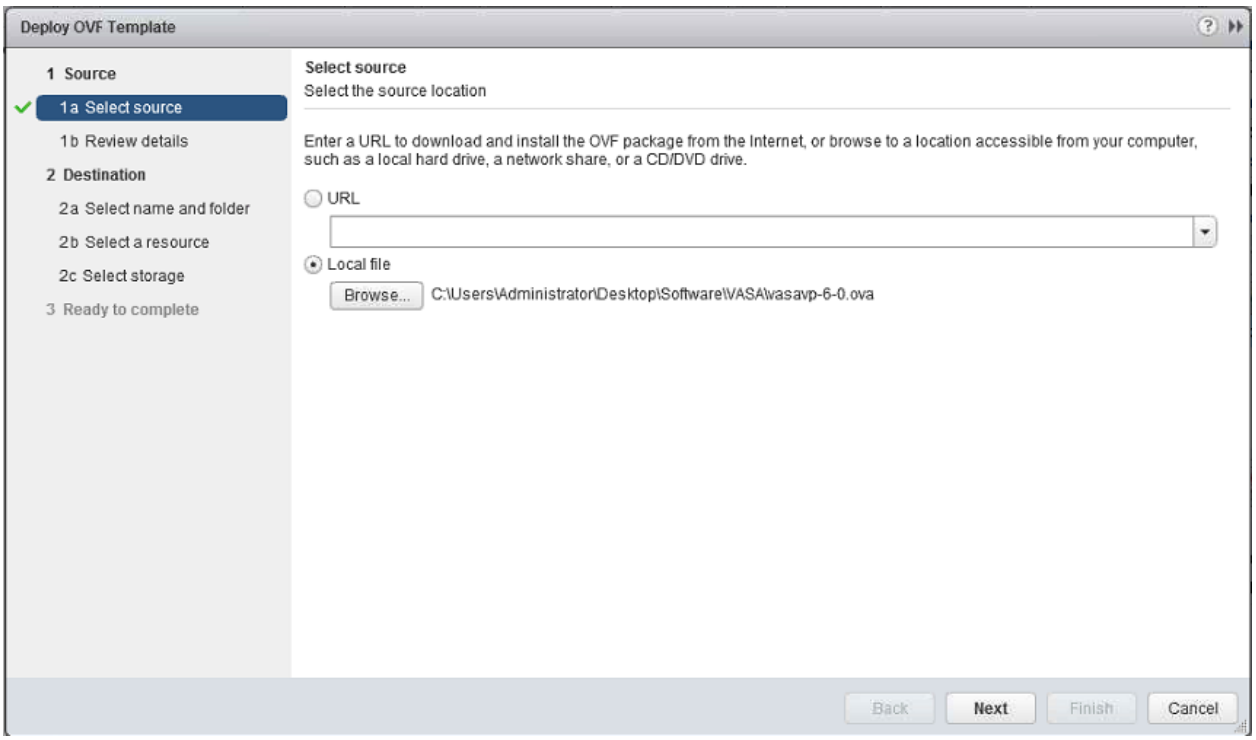


Install NetApp VASA Provider

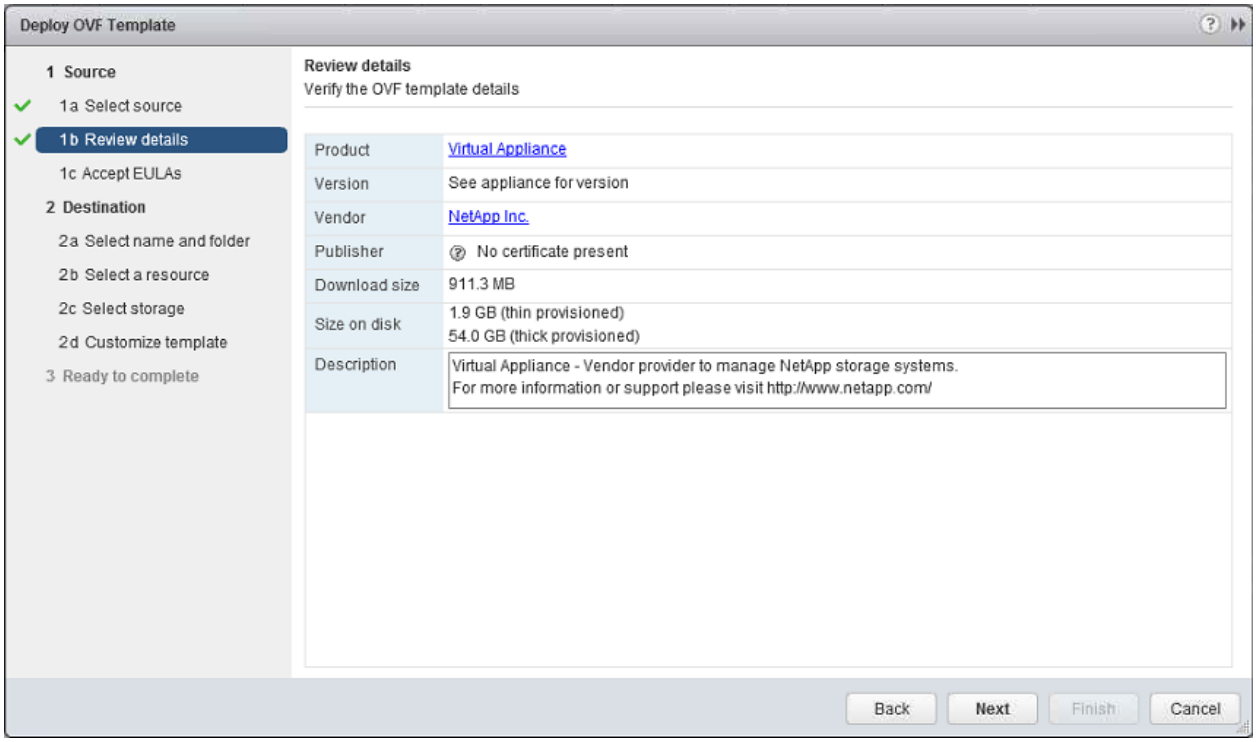
NetApp VASA Provider for clustered Data ONTAP uses VMware vSphere APIs for Storage Awareness (VASA) to provide better storage management. By providing information about storage used by VSC for VMware vSphere to the vCenter Server, VASA Provider enables you to make more intelligent VM provisioning decisions and allows the vCenter Server to warn you when certain storage conditions might affect your VMware environment. VSC 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 6.0 OVA file from the NetApp Support site.
2. Log in to the vSphere Web Client, click Home and select VMs and Templates.
3. At the top of the center pane, click Actions > Deploy OVF Template.
4. Browse to the `.ova` file that was downloaded locally and click Open to select the file.



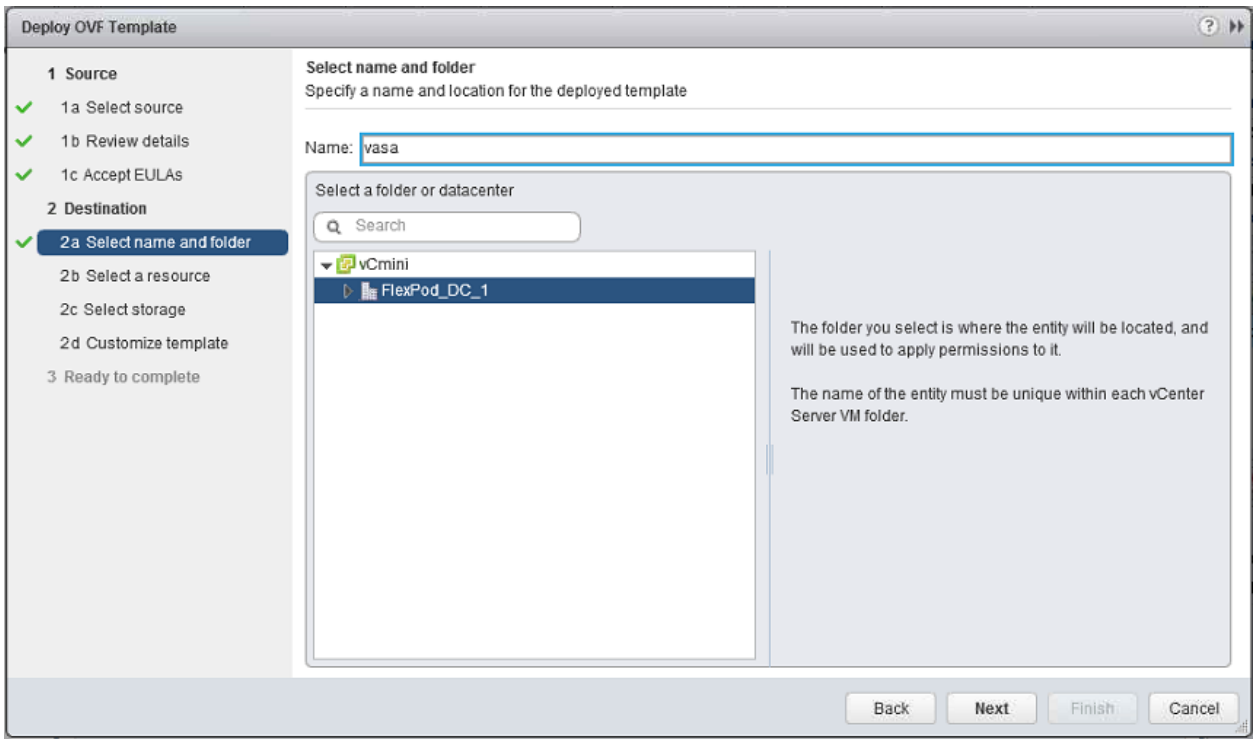
5. Review the OVF template of the selected source and click Next.



6. Click Next.

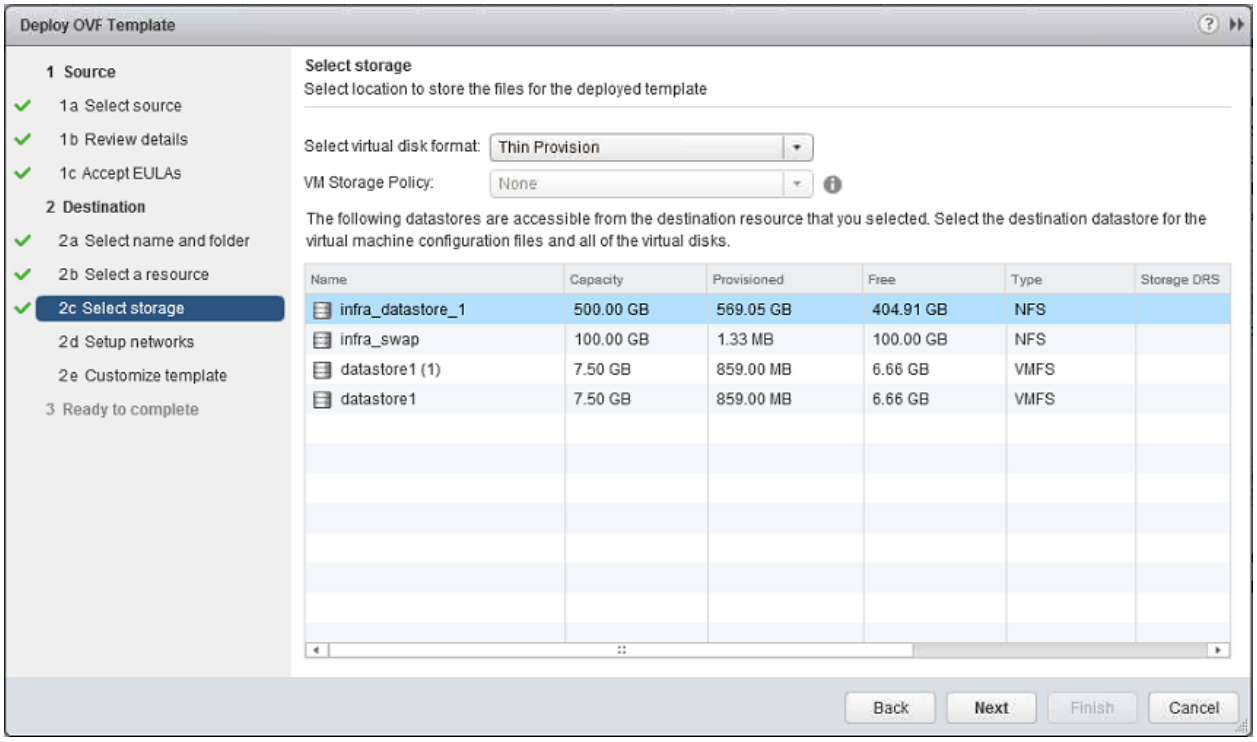
7. Read and accept the EULA, and then click Next.

8. Enter the name of the VM and select the FlexPod_DC_1 folder as the location of the VM. Click Next.

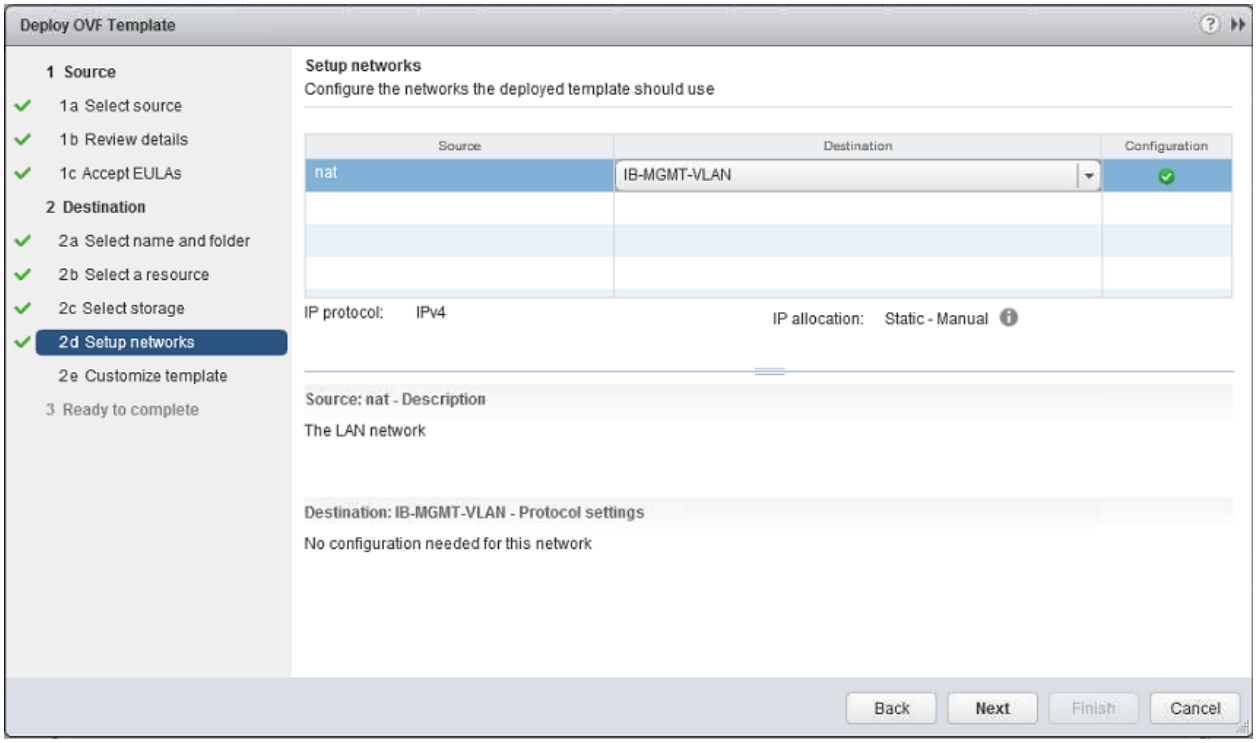


9. Within the FlexPod_DC_1 datacenter, select FlexPod_Management as the destination to host the VM compute resource pool. Click Next.

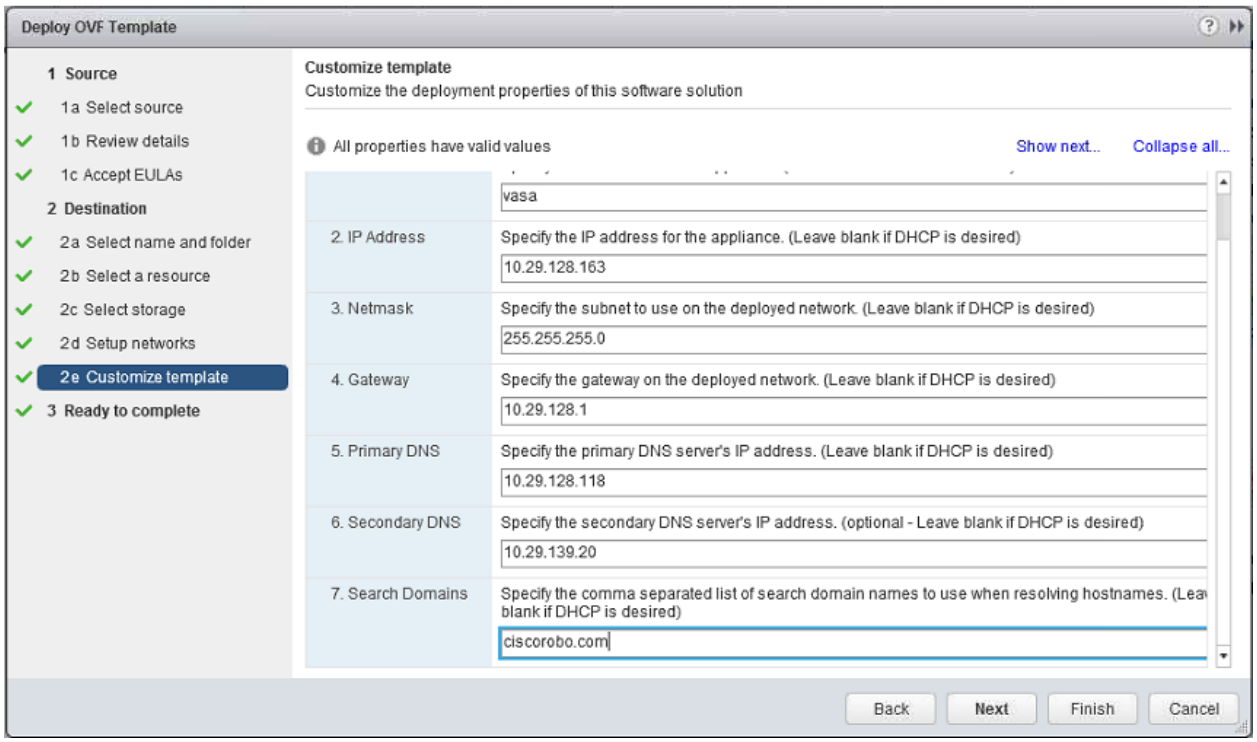
10. Select infra_datastore_1 as the storage target for the VM and select Thin Provision as the virtual disk format. Click Next.



11. Select IB-MGMT-VLAN as the destination to the nat source network. Click Next.

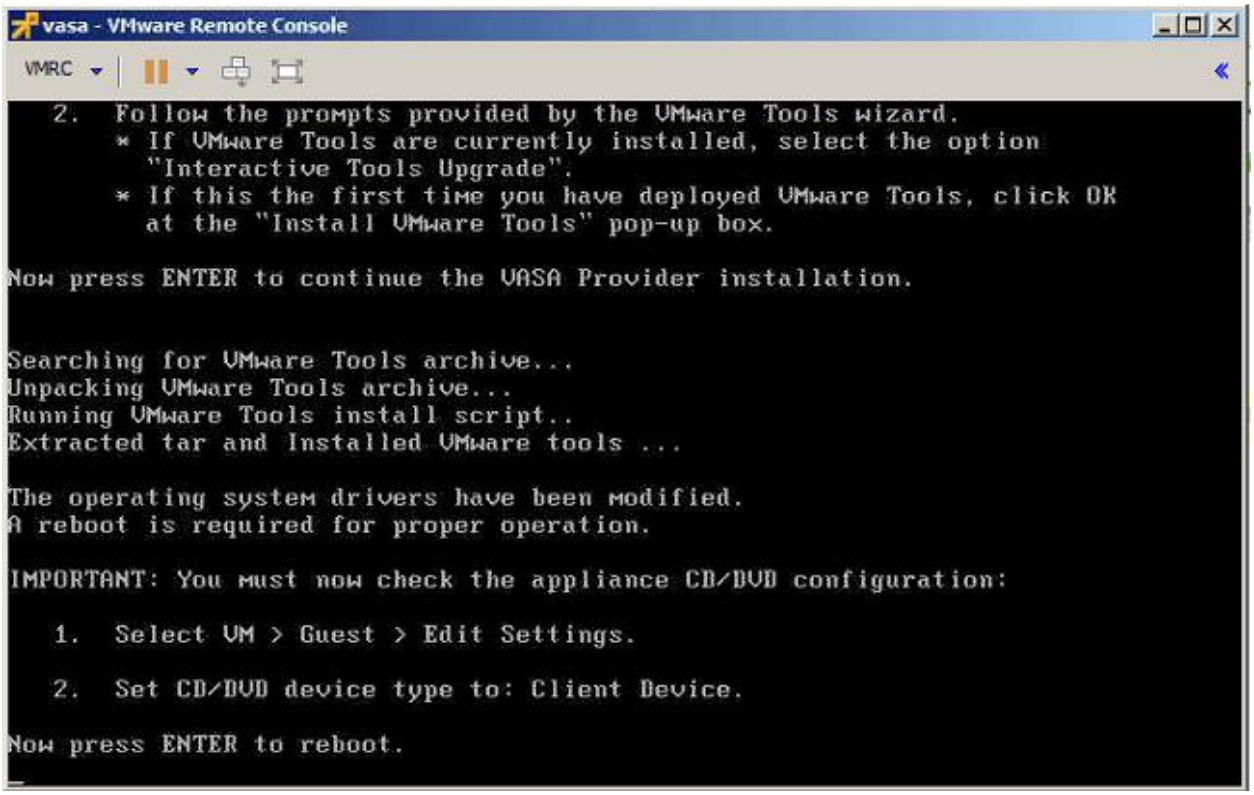


12. Enter the details for the host name, IP address, network mask, gateway, primary DNS, secondary DNS, and search domain. Make sure the hostname is properly registered in the DNS servers. Click Next.

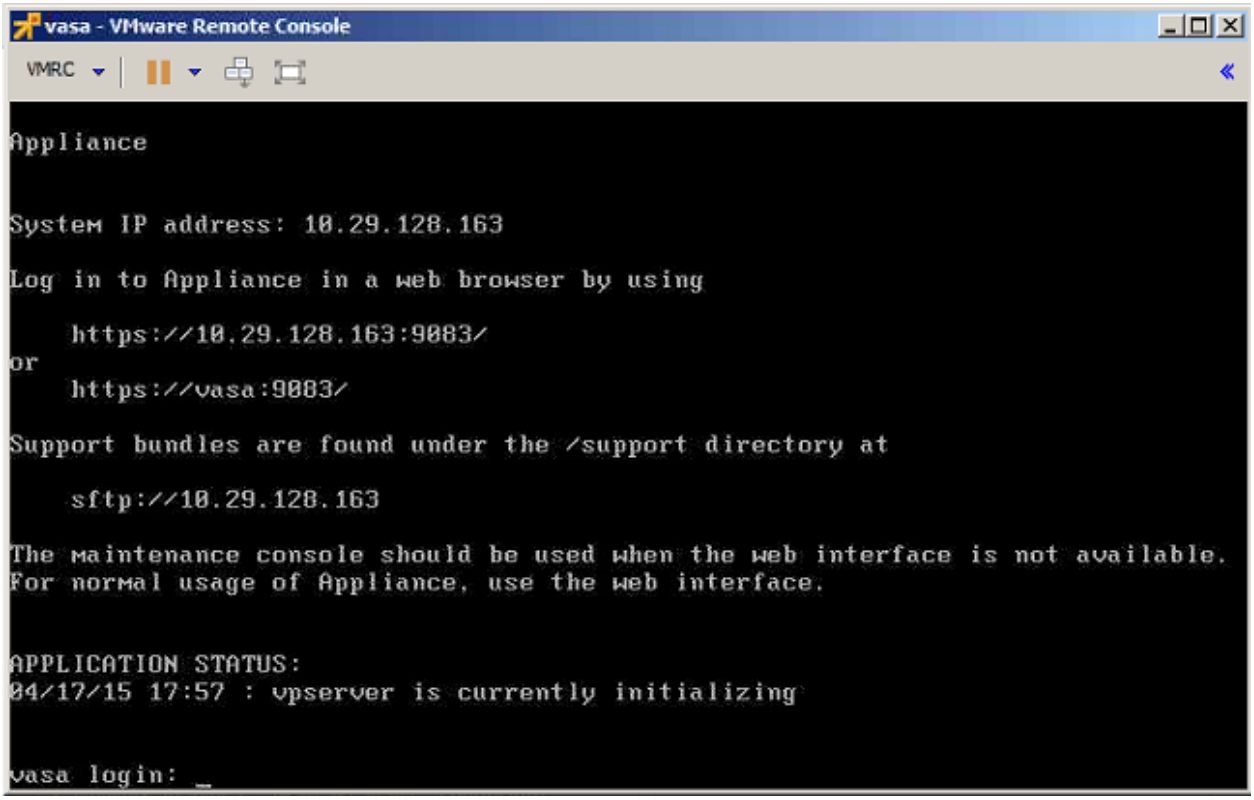


13. Leave Power on After Deployment deselected and click Finish.

14. Wait for the Deploy OVF template task to complete.
15. In the left pane, right-click the VASA VM and select Power On.
16. In the left pane, select the VASA VM. In the center pane, select Open with VMRC.
17. In the console, follow the VASA Provider installation prompts to install VMware Tools. From the VMRC drop-down menu, select Manage > Install VMware Tools. In the console, press Enter to complete the VMware Tools installation.



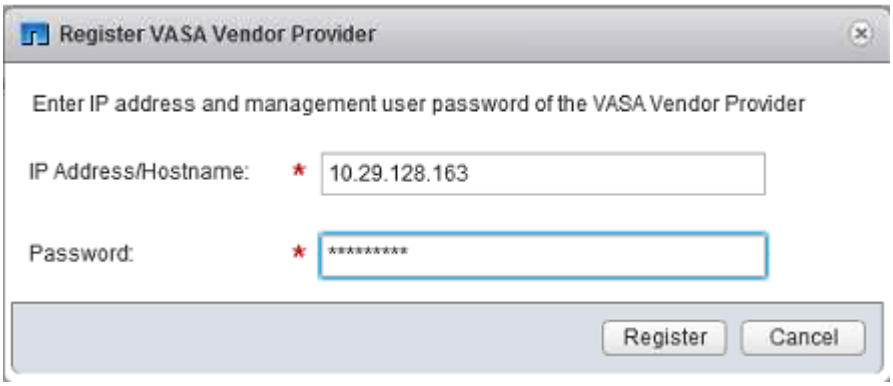
18. In the console, press Enter to reboot the VASA VM.
19. After reboot, in the console, enter and confirm a password for the maintenance user.
20. Enter and confirm a password for the vpserver user.



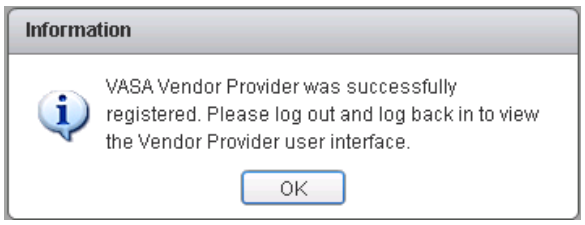
Register VASA Provider for Clustered Data ONTAP with VSC

To register the VASA provider for clustered Data ONTAP, complete the following steps:

1. Log in to the VMware vSphere Web Client and click Home > Virtual Storage Console.
2. In the left pane, click Configuration.
3. Click Register/Unregister VASA Vendor Provider.
4. In the thank you message, click OK.
5. Enter the IP address and vpserver password for the VASA VM and click Register.

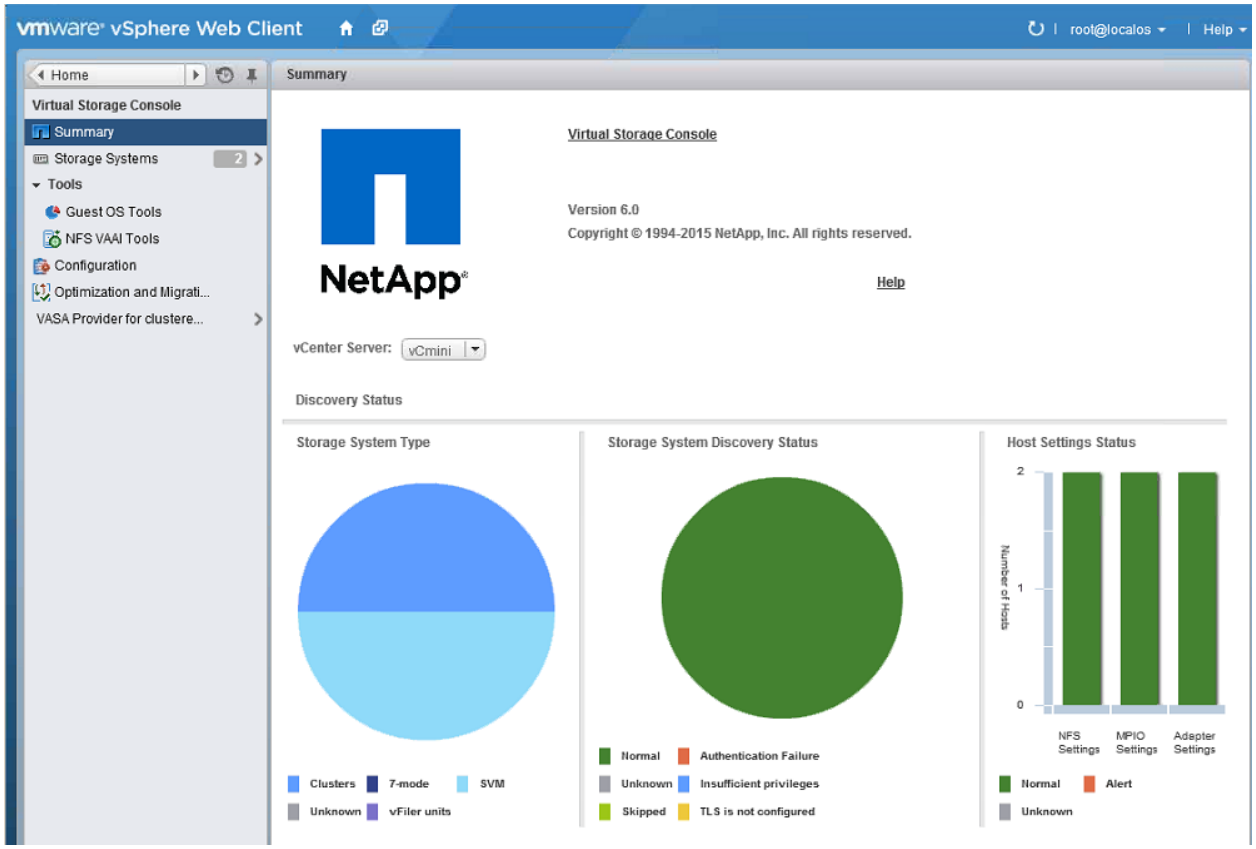


6. Click OK in the message box, log out of the web client, and log back in to view the vendor provider user interface.



7. Log out and log back in to VMware vSphere Web Client. From the Home page, select Virtual Storage Console.

8. Verify that VASA Provider for Clustered Data ONTAP appears in the left pane.



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, branches provide the same advantages of datacenter with no or minimal IT support at the branches or remote offices.

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 data center, Cisco UCS Central can be used to globally setup and manage the UCS Managers at multiple branch offices. The branch office setups of this solution will be detailed in the FlexPod Express with UCS Mini Deployment Guide.

This section provides a detailed overview of UCS Central setup in standalone mode.

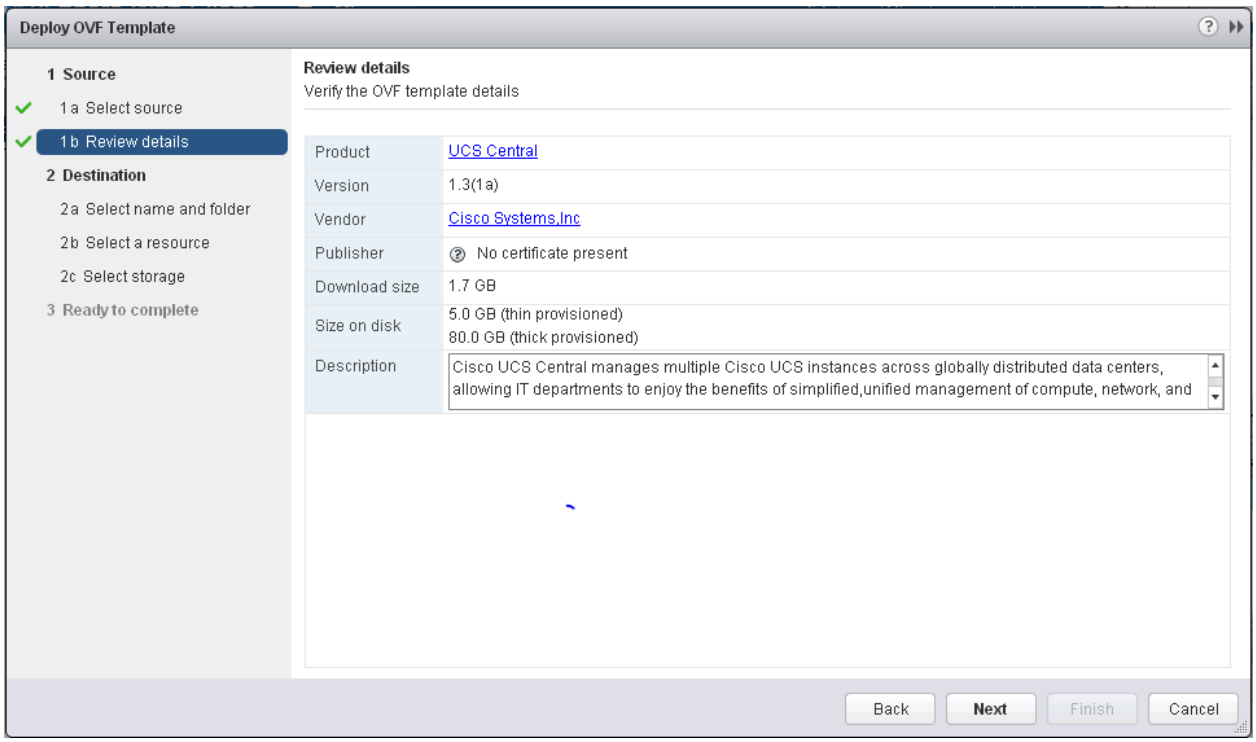
The installation and upgrade guide is available at:
http://www.cisco.com/en/US/docs/unified_computing/ucs/ucs-central/install-upgrade/1.1/b_UCSC_Installation_and_Upgrade_Guide_11.html

Obtain the Cisco UCS Central Software

1. Navigate to the Cisco UCS Central Download page.
2. Download the OVA file ucs-central.1.3.1a.ova.

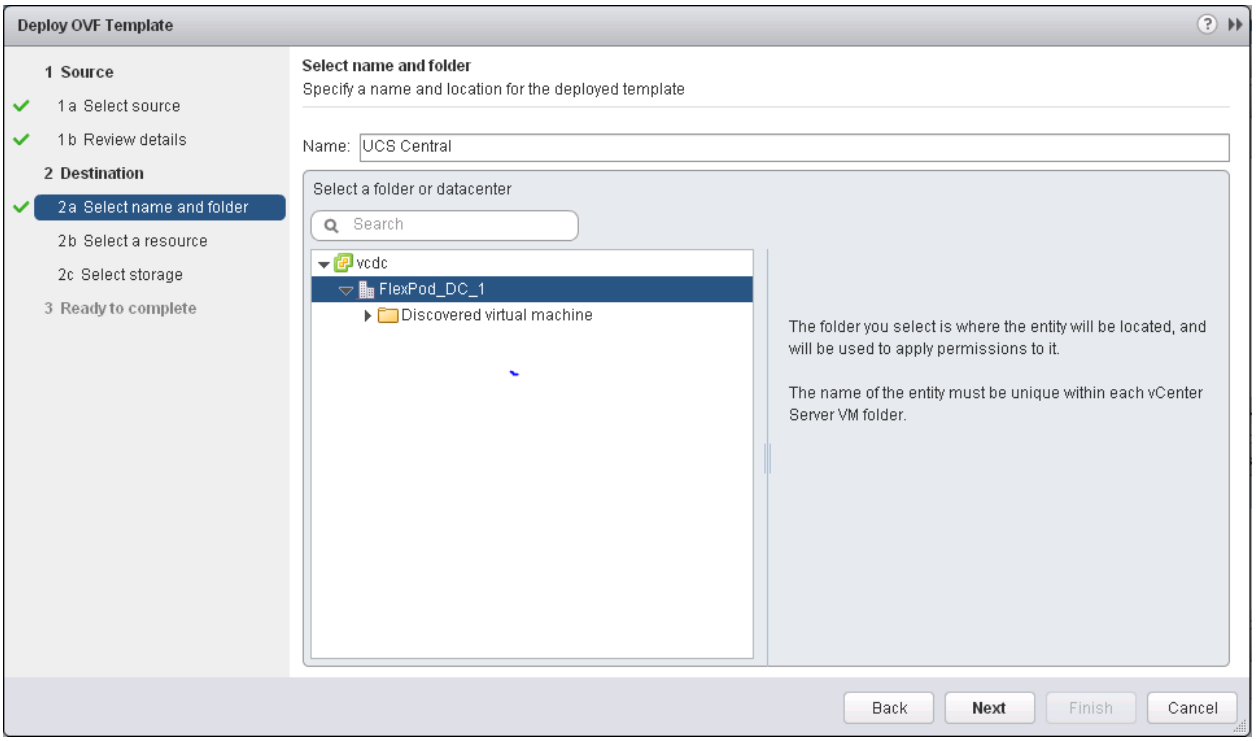
Install the Cisco UCS Central Software

1. Using the vSphere web client, log in to the vCenter Server as the 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.

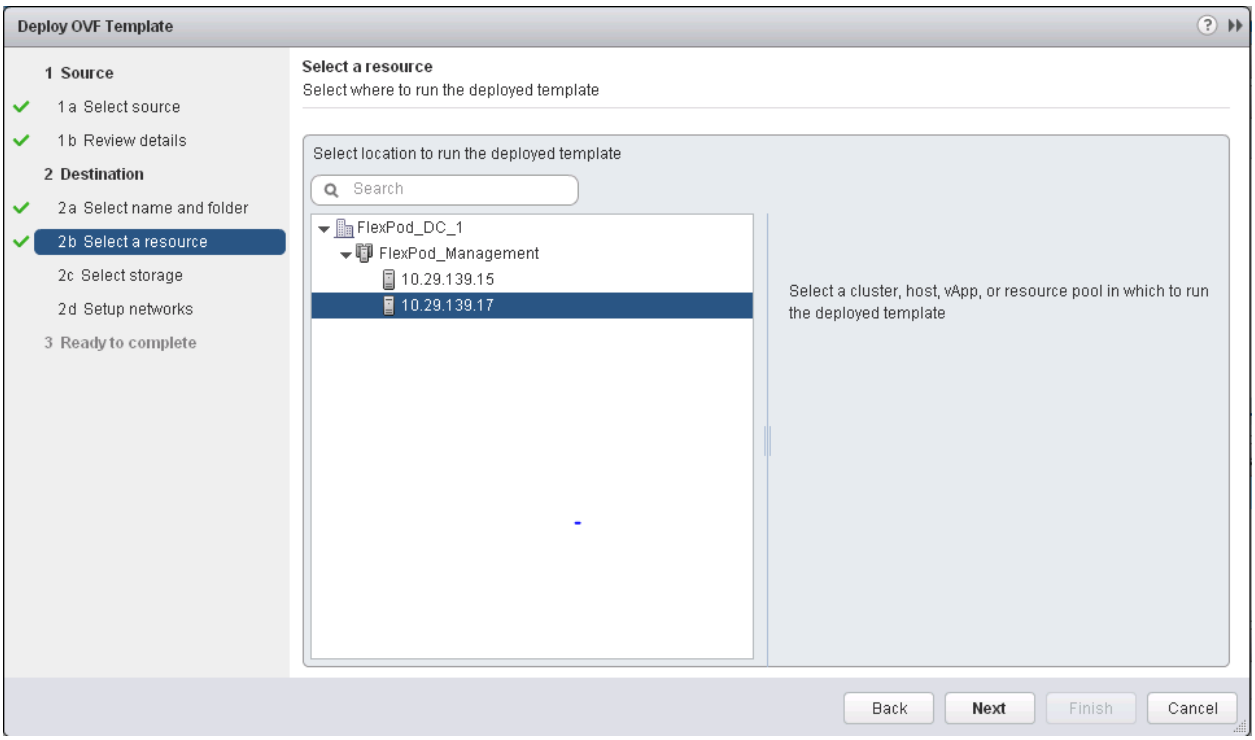


4. Click Next.

5. Modify the default name if desired and select the Inventory Location. Click Next.



6. Select a cluster/server on which you want to host the UCS Central virtual machine. Click Next.



7. Select the datastore in which the virtual machine files will be stored. Select the Thin Provision virtual disk format. Click Next.

8. Select the appropriate network. Click Next.

9. Select the checkbox to power on the VM after deployment.

10. Click Finish.

11. Open a VMRC console window to the UCS Central virtual machine. Answer yes to continue installation. Enter setup to setup a new configuration.

```
Shutting down pmon:                                        [  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  : _
```

12. Enter the IPv4 address, Network and gateway information in the console window.

```
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 / M=Microsoft Sql
Server] : 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.

13. 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 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.

Bill of Materials for Cisco UCS Mini Used in this Validation

0 and Table 24provides 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 23 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 M4 Blades	UCSB-B200-M4
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 24 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-M4	UCS B200 M4 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

Product Bundle	Sub Components	
	UCSB-HS-EP-M4	CPU Heat Sink for UCS B200 M4 and B420 M3
	UCSB-M4-V2-LBL	Cisco M4 – 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

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 3524 Example Configuration

Cisco Nexus 3524 A

```
!Command: show running-config
!Time: Fri Jun  5 22:21:19 2015

version 6.0(2)A6(2)
switchname n3k-a

no feature telnet
cfs eth distribute
feature interface-vlan
feature lacp
feature vpc
feature lldp

username admin password 5 $1$zcRyc4IV$WVUhWHPWgUhxVlCNgF2uO.  role network-admin
ip domain-lookup
system default switchport shutdown
ip access-list copp-system-acl-bfd
  10 permit udp any any eq 3784
  20 permit udp any any eq 3785
ip access-list copp-system-acl-eigrp
  10 permit eigrp any 224.0.0.10/32
ip access-list copp-system-acl-ftp
  10 permit tcp any any eq ftp-data
  20 permit tcp any any eq ftp
  30 permit tcp any eq ftp-data any
  40 permit tcp any eq ftp any
ip access-list copp-system-acl-http
  10 permit tcp any any eq www
  20 permit tcp any any eq 443
ip access-list copp-system-acl-icmp
  10 permit icmp any any
ip access-list copp-system-acl-ntp
  10 permit udp any any eq ntp
  20 permit udp any eq ntp any
ip access-list copp-system-acl-ping
```

```
  10 permit icmp any any echo
  20 permit icmp any any echo-reply
ip access-list copp-system-acl-routingproto1
  10 permit tcp any any eq bgp
  20 permit tcp any eq bgp any
  30 permit udp any 224.0.0.0/24 eq rip
  40 permit tcp any any eq 639
  50 permit tcp any eq 639 any
  70 permit ospf any any
  80 permit ospf any 224.0.0.5/32
  90 permit ospf any 224.0.0.6/32
ip access-list copp-system-acl-routingproto2
  10 permit udp any 224.0.0.0/24 eq 1985
  20 permit 112 any 224.0.0.0/24
ip access-list copp-system-acl-snmp
  10 permit udp any any eq snmp
  20 permit udp any any eq snmptrap
ip access-list copp-system-acl-ssh
  10 permit tcp any any eq 22
  20 permit tcp any eq 22 any
ip access-list copp-system-acl-stftp
  10 permit udp any any eq tftp
  20 permit udp any any eq 1758
  30 permit udp any eq tftp any
  40 permit udp any eq 1758 any
  50 permit tcp any any eq 115
  60 permit tcp any eq 115 any
ip access-list copp-system-acl-tacacsradius
  10 permit tcp any any eq tacacs
  20 permit tcp any eq tacacs any
  30 permit udp any any eq 1812
  40 permit udp any any eq 1813
  50 permit udp any any eq 1645
  60 permit udp any any eq 1646
  70 permit udp any eq 1812 any
  80 permit udp any eq 1813 any
  90 permit udp any eq 1645 any
  100 permit udp any eq 1646 any
ip access-list copp-system-acl-telnet
  10 permit tcp any any eq telnet
  20 permit tcp any any eq 107
  30 permit tcp any eq telnet any
  40 permit tcp any eq 107 any
ip access-list copp-system-dhcp-relay
  10 permit udp any eq bootps any eq bootps
policy-map type network-qos jumbo
  class type network-qos class-default
    mtu 9216
system qos
  service-policy type network-qos jumbo
class-map type control-plane match-any copp-ftp
  match access-group name copp-system-acl-ftp
class-map type control-plane match-any copp-http
  match access-group name copp-system-acl-http
class-map type control-plane match-any copp-icmp
  match access-group name copp-system-acl-icmp
class-map type control-plane match-any copp-ntp
  match access-group name copp-system-acl-ntp
class-map type control-plane match-any copp-s-arp
class-map type control-plane match-any copp-s-bpdu
class-map type control-plane match-any copp-s-cdp
class-map type control-plane match-any copp-s-default
class-map type control-plane match-any copp-s-dhcpreq
class-map type control-plane match-any copp-s-dhcpresp
  match access-group name copp-system-dhcp-relay
class-map type control-plane match-any copp-s-dpss
class-map type control-plane match-any copp-s-eigrp
  match access-group name copp-system-acl-eigrp
class-map type control-plane match-any copp-s-glean
class-map type control-plane match-any copp-s-igmp
class-map type control-plane match-any copp-s-ip-nat
class-map type control-plane match-any copp-s-ip-options
class-map type control-plane match-any copp-s-ipmc-g-hit
class-map type control-plane match-any copp-s-ipmc-rpf-fail-g
```

```
class-map type control-plane match-any copp-s-ipmc-rpf-fail-sg
class-map type control-plane match-any copp-s-ipmcmiss
class-map type control-plane match-any copp-s-l3destmiss
class-map type control-plane match-any copp-s-l3mtufail
class-map type control-plane match-any copp-s-lacp
class-map type control-plane match-any copp-s-lldp
class-map type control-plane match-any copp-s-pimautorp
class-map type control-plane match-any copp-s-pimreg
class-map type control-plane match-any copp-s-ping
  match access-group name copp-system-acl-ping
class-map type control-plane match-any copp-s-ptp
class-map type control-plane match-any copp-s-routingProto1
  match access-group name copp-system-acl-routingproto1
class-map type control-plane match-any copp-s-routingProto2
  match access-group name copp-system-acl-routingproto2
class-map type control-plane match-any copp-s-ttl1
class-map type control-plane match-any copp-snmp
  match access-group name copp-system-acl-snmp
class-map type control-plane match-any copp-ssh
  match access-group name copp-system-acl-ssh
class-map type control-plane match-any copp-stftp
  match access-group name copp-system-acl-stftp
class-map type control-plane match-any copp-tacacsradius
  match access-group name copp-system-acl-tacacsradius
class-map type control-plane match-any copp-telnet
  match access-group name copp-system-acl-telnet
policy-map type control-plane copp-system-policy
  class copp-s-default
    police pps 400
  class copp-s-ping
    police pps 100
  class copp-s-l3destmiss
    police pps 100
  class copp-s-glean
    police pps 500
  class copp-s-l3mtufail
    police pps 100
  class copp-s-ttl1
    police pps 100
  class copp-s-ip-options
    police pps 100
  class copp-s-ip-nat
    police pps 100
  class copp-s-ipmcmiss
    police pps 400
  class copp-s-ipmc-g-hit
    police pps 400
  class copp-s-ipmc-rpf-fail-g
    police pps 400
  class copp-s-ipmc-rpf-fail-sg
    police pps 400
  class copp-s-dhcpreq
    police pps 300
  class copp-s-dhcpresp
    police pps 300
  class copp-s-igmp
    police pps 400
  class copp-s-eigrp
    police pps 200
  class copp-s-pimreg
    police pps 200
  class copp-s-pimautorp
    police pps 200
  class copp-s-routingProto2
    police pps 1300
  class copp-s-routingProto1
    police pps 1000
  class copp-s-arp
    police pps 200
  class copp-s-ptp
    police pps 1000
  class copp-s-bpdu
    police pps 12000
  class copp-s-dpss
```

```
    police pps 6400
  class copp-s-cdp
    police pps 400
  class copp-s-lacp
    police pps 400
  class copp-s-lldp
    police pps 500
  class copp-icmp
    police pps 200
  class copp-telnet
    police pps 500
  class copp-ssh
    police pps 500
  class copp-snmp
    police pps 500
  class copp-ntp
    police pps 100
  class copp-tacacsradius
    police pps 400
  class copp-stftp
    police pps 400
  class copp-ftp
    police pps 100
  class copp-http
    police pps 100
control-plane
  service-policy input copp-system-policy
snmp-server user admin network-admin auth md5 0x891e7c54b39e744c26b79658584b2fe4 priv
0x891e7c54b39e744c26b79658584b2fe4 localizedkey
ntp server 171.68.38.66 use-vrf default

vlan 1
vlan 2
  name Native-VLAN
vlan 128
  name IB-MGMT-VLAN
vlan 3170
  name NFS-VLAN
vlan 3171
  name iSCSI-A-VLAN
vlan 3172
  name iSCSI-B-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
port-channel load-balance ethernet source-dest-port
vpc domain 24
  peer-switch
  role priority 10
  peer-keepalive destination 172.20.254.2 source 172.20.254.1
  peer-gateway
  auto-recovery


interface Vlan1

interface Vlan128
  no shutdown
  ip address 10.29.128.201/24

interface port-channel10
  description vPC peer-link
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128,3170-3174
  spanning-tree port type network
  vpc peer-link

interface port-channel13
  description ucs-A
```

```
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128,3170-3174
  spanning-tree port type edge trunk
  vpc 13

interface port-channel14
  description ucs-B
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128,3170-3174
  spanning-tree port type edge trunk
  vpc 14

interface port-channel119
  speed 1000
  description TOR-SW-SJC2-1-151-AAC-27 Uplink
  switchport access vlan 128
  spanning-tree port type normal
  vpc 119

interface Ethernet1/1
  speed 1000
  description clus-01:e0M
  switchport access vlan 128
  spanning-tree port type edge
  no shutdown

interface Ethernet1/2
  speed 1000
  description clus-02:e0a
  switchport access vlan 128
  spanning-tree port type edge
  no shutdown

interface Ethernet1/3
  description ucs-A:1/3
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128,3170-3174
  channel-group 13 mode active
  no shutdown

interface Ethernet1/4
  description ucs-B:1/3
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128,3170-3174
  channel-group 14 mode active
  no shutdown

interface Ethernet1/5
  shutdown

interface Ethernet1/6
  shutdown

interface Ethernet1/7
  shutdown

interface Ethernet1/8
  shutdown

interface Ethernet1/9
  shutdown

interface Ethernet1/10
  shutdown

interface Ethernet1/11
  shutdown

interface Ethernet1/12
  shutdown
```

```
interface Ethernet1/13
  description n3k-b:1/13
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128,3170-3174
  channel-group 10 mode active
  no shutdown

interface Ethernet1/14
  description n3k-b:1/14
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128,3170-3174
  channel-group 10 mode active
  no shutdown

interface Ethernet1/15
  shutdown

interface Ethernet1/16
  shutdown

interface Ethernet1/17
  shutdown

interface Ethernet1/18
  shutdown

interface Ethernet1/19
  speed 1000
  description TOR-SW:1/0/10
  switchport access vlan 128
  channel-group 119 mode active
  no shutdown

interface Ethernet1/20
  shutdown

interface Ethernet1/21
  speed 1000
  description ucs-A:mgmt0
  switchport access vlan 128
  spanning-tree port type edge
  no shutdown

interface Ethernet1/22
  shutdown

interface Ethernet1/23
  shutdown

interface Ethernet1/24
  shutdown

interface Ethernet1/25
  shutdown

interface Ethernet1/26
  shutdown

interface Ethernet1/27
  shutdown

interface Ethernet1/28
  shutdown

interface Ethernet1/29
  shutdown

interface Ethernet1/30
  shutdown

interface Ethernet1/31
```

```
  shutdown

interface Ethernet1/32
  shutdown

interface Ethernet1/33
  shutdown

interface Ethernet1/34
  shutdown

interface Ethernet1/35
  shutdown

interface Ethernet1/36
  shutdown

interface Ethernet1/37
  shutdown

interface Ethernet1/38
  shutdown

interface Ethernet1/39
  shutdown

interface Ethernet1/40
  shutdown

interface Ethernet1/41
  shutdown

interface Ethernet1/42
  shutdown

interface Ethernet1/43
  shutdown

interface Ethernet1/44
  shutdown

interface Ethernet1/45
  shutdown

interface Ethernet1/46
  shutdown

interface Ethernet1/47
  shutdown

interface Ethernet1/48
  shutdown

interface mgmt0
  vrf member management
  ip address 172.20.254.1/24
ip route 0.0.0.0/0 10.29.128.1
line console
line vty
boot kickstart bootflash:/n3500-uk9-kickstart.6.0.2.A6.2.bin
boot system bootflash:/n3500-uk9.6.0.2.A6.2.bin
```

Cisco Nexus 3524 B

```
!Command: show running-config
!Time: Fri Jun  5 22:22:50 2015

version 6.0(2)A6(2)
switchname n3k-b

no feature telnet
cfs eth distribute
```

```
feature interface-vlan
feature lacp
feature vpc
feature lldp

username admin password 5 $1$DiscyDhG$PvGADTkyoVwgDoi.hniFJ.  role network-admin
ip domain-lookup
system default switchport shutdown
ip access-list copp-system-acl-bfd
  10 permit udp any any eq 3784
  20 permit udp any any eq 3785
ip access-list copp-system-acl-eigrp
  10 permit eigrp any 224.0.0.10/32
ip access-list copp-system-acl-ftp
  10 permit tcp any any eq ftp-data
  20 permit tcp any any eq ftp
  30 permit tcp any eq ftp-data any
  40 permit tcp any eq ftp any
ip access-list copp-system-acl-http
  10 permit tcp any any eq www
  20 permit tcp any any eq 443
ip access-list copp-system-acl-icmp
  10 permit icmp any any
ip access-list copp-system-acl-ntp
  10 permit udp any any eq ntp
  20 permit udp any eq ntp any
ip access-list copp-system-acl-ping
  10 permit icmp any any echo
  20 permit icmp any any echo-reply
ip access-list copp-system-acl-routingproto1
  10 permit tcp any any eq bgp
  20 permit tcp any eq bgp any
  30 permit udp any 224.0.0.0/24 eq rip
  40 permit tcp any any eq 639
  50 permit tcp any eq 639 any
  70 permit ospf any any
  80 permit ospf any 224.0.0.5/32
  90 permit ospf any 224.0.0.6/32
ip access-list copp-system-acl-routingproto2
  10 permit udp any 224.0.0.0/24 eq 1985
  20 permit 112 any 224.0.0.0/24
ip access-list copp-system-acl-snmp
  10 permit udp any any eq snmp
  20 permit udp any any eq snmptrap
ip access-list copp-system-acl-ssh
  10 permit tcp any any eq 22
  20 permit tcp any eq 22 any
ip access-list copp-system-acl-stftp
  10 permit udp any any eq tftp
  20 permit udp any any eq 1758
  30 permit udp any eq tftp any
  40 permit udp any eq 1758 any
  50 permit tcp any any eq 115
  60 permit tcp any eq 115 any
ip access-list copp-system-acl-tacacsradius
  10 permit tcp any any eq tacacs
  20 permit tcp any eq tacacs any
  30 permit udp any any eq 1812
  40 permit udp any any eq 1813
  50 permit udp any any eq 1645
  60 permit udp any any eq 1646
  70 permit udp any eq 1812 any
  80 permit udp any eq 1813 any
  90 permit udp any eq 1645 any
  100 permit udp any eq 1646 any
ip access-list copp-system-acl-telnet
  10 permit tcp any any eq telnet
  20 permit tcp any any eq 107
  30 permit tcp any eq telnet any
  40 permit tcp any eq 107 any
ip access-list copp-system-dhcp-relay
  10 permit udp any eq bootps any eq bootps
policy-map type network-qos jumbo
  class type network-qos class-default
```

```
    mtu 9216
system qos
  service-policy type network-qos jumbo
class-map type control-plane match-any copp-ftp
  match access-group name copp-system-acl-ftp
class-map type control-plane match-any copp-http
  match access-group name copp-system-acl-http
class-map type control-plane match-any copp-icmp
  match access-group name copp-system-acl-icmp
class-map type control-plane match-any copp-ntp
  match access-group name copp-system-acl-ntp
class-map type control-plane match-any copp-s-arp
class-map type control-plane match-any copp-s-bpdu
class-map type control-plane match-any copp-s-cdp
class-map type control-plane match-any copp-s-default
class-map type control-plane match-any copp-s-dhcpreq
class-map type control-plane match-any copp-s-dhcpresp
  match access-group name copp-system-dhcp-relay
class-map type control-plane match-any copp-s-dpss
class-map type control-plane match-any copp-s-eigrp
  match access-group name copp-system-acl-eigrp
class-map type control-plane match-any copp-s-glean
class-map type control-plane match-any copp-s-igmp
class-map type control-plane match-any copp-s-ip-nat
class-map type control-plane match-any copp-s-ip-options
class-map type control-plane match-any copp-s-ipmc-g-hit
class-map type control-plane match-any copp-s-ipmc-rpf-fail-g
class-map type control-plane match-any copp-s-ipmc-rpf-fail-sg
class-map type control-plane match-any copp-s-ipmcmiss
class-map type control-plane match-any copp-s-l3destmiss
class-map type control-plane match-any copp-s-l3mtufail
class-map type control-plane match-any copp-s-lacp
class-map type control-plane match-any copp-s-lldp
class-map type control-plane match-any copp-s-pimautorp
class-map type control-plane match-any copp-s-pimreg
class-map type control-plane match-any copp-s-ping
  match access-group name copp-system-acl-ping
class-map type control-plane match-any copp-s-ptp
class-map type control-plane match-any copp-s-routingProto1
  match access-group name copp-system-acl-routingproto1
class-map type control-plane match-any copp-s-routingProto2
  match access-group name copp-system-acl-routingproto2
class-map type control-plane match-any copp-s-ttl1
class-map type control-plane match-any copp-snmp
  match access-group name copp-system-acl-snmp
class-map type control-plane match-any copp-ssh
  match access-group name copp-system-acl-ssh
class-map type control-plane match-any copp-stftp
  match access-group name copp-system-acl-stftp
class-map type control-plane match-any copp-tacacsradius
  match access-group name copp-system-acl-tacacsradius
class-map type control-plane match-any copp-telnet
  match access-group name copp-system-acl-telnet
policy-map type control-plane copp-system-policy
  class copp-s-default
    police pps 400
  class copp-s-ping
    police pps 100
  class copp-s-l3destmiss
    police pps 100
  class copp-s-glean
    police pps 500
  class copp-s-l3mtufail
    police pps 100
  class copp-s-ttl1
    police pps 100
  class copp-s-ip-options
    police pps 100
  class copp-s-ip-nat
    police pps 100
  class copp-s-ipmcmiss
    police pps 400
  class copp-s-ipmc-g-hit
    police pps 400
```

```
  class copp-s-ipmc-rpf-fail-g
    police pps 400
  class copp-s-ipmc-rpf-fail-sg
    police pps 400
  class copp-s-dhcpreq
    police pps 300
  class copp-s-dhcpresp
    police pps 300
  class copp-s-igmp
    police pps 400
  class copp-s-eigrp
    police pps 200
  class copp-s-pimreg
    police pps 200
  class copp-s-pimautorp
    police pps 200
  class copp-s-routingProto2
    police pps 1300
  class copp-s-routingProto1
    police pps 1000
  class copp-s-arp
    police pps 200
  class copp-s-ptp
    police pps 1000
  class copp-s-bpdu
    police pps 12000
  class copp-s-dpss
    police pps 6400
  class copp-s-cdp
    police pps 400
  class copp-s-lacp
    police pps 400
  class copp-s-lldp
    police pps 500
  class copp-icmp
    police pps 200
  class copp-telnet
    police pps 500
  class copp-ssh
    police pps 500
  class copp-snmp
    police pps 500
  class copp-ntp
    police pps 100
  class copp-tacacsradius
    police pps 400
  class copp-stftp
    police pps 400
  class copp-ftp
    police pps 100
  class copp-http
    police pps 100
control-plane
  service-policy input copp-system-policy
snmp-server user admin network-admin auth md5 0xf58e36d254601781e5bc76b3dd0b7b5a priv
0xf58e36d254601781e5bc76b3dd0b7b5a localizedkey
ntp server 171.68.38.66 use-vrf default

vlan 1
vlan 2
  name Native-VLAN
vlan 128
  name IB-MGMT-VLAN
vlan 3170
  name NFS-VLAN
vlan 3171
  name iSCSI-A-VLAN
vlan 3172
  name iSCSI-B-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
port-channel load-balance ethernet source-dest-port
vpc domain 24
  peer-switch
  role priority 20
  peer-keepalive destination 172.20.254.1 source 172.20.254.2
  peer-gateway
  auto-recovery


interface Vlan1

interface Vlan128
  no shutdown
  ip address 10.29.128.202/24

interface port-channel10
  description vPC peer-link
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128,3170-3174
  spanning-tree port type network
  vpc peer-link

interface port-channel13
  description ucs-A
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128,3170-3174
  spanning-tree port type edge trunk
  vpc 13

interface port-channel14
  description ucs-B
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128,3170-3174
  spanning-tree port type edge trunk
  vpc 14

interface port-channel119
  speed 1000
  description TOR-SW Uplink
  switchport access vlan 128
  spanning-tree port type normal
  vpc 119

interface Ethernet1/1
  speed 1000
  description clus-02:e0M
  switchport access vlan 128
  spanning-tree port type edge
  vpc orphan-port suspend
  no shutdown

interface Ethernet1/2
  speed 1000
  description clus-01:e0a
  switchport access vlan 128
  spanning-tree port type edge
  vpc orphan-port suspend
  no shutdown

interface Ethernet1/3
  description ucs-A:1/4
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128,3170-3174
  channel-group 13 mode active
  no shutdown

interface Ethernet1/4
  description ucs-B:1/4
```

```
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128,3170-3174
  channel-group 14 mode active
  no shutdown

interface Ethernet1/5
  shutdown

interface Ethernet1/6
  shutdown

interface Ethernet1/7
  shutdown

interface Ethernet1/8
  shutdown

interface Ethernet1/9
  shutdown

interface Ethernet1/10
  shutdown

interface Ethernet1/11
  shutdown

interface Ethernet1/12
  shutdown

interface Ethernet1/13
  description n3k-a:1/13
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128,3170-3174
  channel-group 10 mode active
  no shutdown

interface Ethernet1/14
  description n3k-a:1/14
  switchport mode trunk
  switchport trunk native vlan 2
  switchport trunk allowed vlan 128,3170-3174
  channel-group 10 mode active
  no shutdown

interface Ethernet1/15
  shutdown

interface Ethernet1/16
  shutdown

interface Ethernet1/17
  shutdown

interface Ethernet1/18
  shutdown

interface Ethernet1/19
  speed 1000
  description TOR-SW-SJC2-1-151-AAC-27:1/0/24
  switchport access vlan 128
  channel-group 119 mode active
  no shutdown

interface Ethernet1/20
  shutdown

interface Ethernet1/21
  speed 1000
  description ucs-B:mgmt0
  switchport access vlan 128
  spanning-tree port type edge
  vpc orphan-port suspend
```

```
  no shutdown

interface Ethernet1/22
  shutdown

interface Ethernet1/23
  shutdown

interface Ethernet1/24
  shutdown

interface Ethernet1/25
  shutdown

interface Ethernet1/26
  shutdown

interface Ethernet1/27
  shutdown

interface Ethernet1/28
  shutdown

interface Ethernet1/29
  shutdown

interface Ethernet1/30
  shutdown

interface Ethernet1/31
  shutdown

interface Ethernet1/32
  shutdown

interface Ethernet1/33
  shutdown

interface Ethernet1/34
  shutdown

interface Ethernet1/35
  shutdown

interface Ethernet1/36
  shutdown

interface Ethernet1/37
  shutdown

interface Ethernet1/38
  shutdown

interface Ethernet1/39
  shutdown

interface Ethernet1/40
  shutdown

interface Ethernet1/41
  shutdown

interface Ethernet1/42
  shutdown

interface Ethernet1/43
  shutdown

interface Ethernet1/44
  shutdown

interface Ethernet1/45
  shutdown
```

```
interface Ethernet1/46
  shutdown

interface Ethernet1/47
  shutdown

interface Ethernet1/48
  shutdown

interface mgmt0
  vrf member management
  ip address 172.20.254.2/24
ip route 0.0.0.0/0 10.29.128.1
line console
line vty
boot kickstart bootflash:/n3500-uk9-kickstart.6.0.2.A6.2.bin
boot system bootflash:/n3500-uk9.6.0.2.A6.2.bin
```

About Authors

Gangoor Sridhara, Systems Engineer, Cisco Systems, Inc.

Gangoor Sridhara is a Systems Engineer with Cisco UCS Solutions and Performance group has experience in UCS, storage and server virtualization design. Gangoor has worked on Enterprise Storage solutions, server virtualization, performance and analysis. He has worked on database performance benchmark tests. He holds certification from VMware and NetApp. Gangoor worked as 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.

Lindsey Street, Solutions Architect, Infrastructure and Cloud Engineering, NetApp

Lindsey Street is a Solutions Architect in the NetApp Infrastructure and Cloud Engineering team. She focuses on the architecture, implementation, compatibility, and security of innovative vendor technologies to develop competitive and high-performance end-to-end cloud solutions for customers. Lindsey started her career in 2006 at Nortel as an interoperability test engineer, testing customer equipment interoperability for certification. Lindsey has her Bachelors of Science degree in Computer Networking and her Masters of Science in Information Security from East Carolina University.

Acknowledgements

- John Kennedy, Lead Technical Marketing Engineer, Cisco Systems, Inc.
- Chris O’Brien, Manager, Technical Marketing Team, Cisco Systems, Inc.