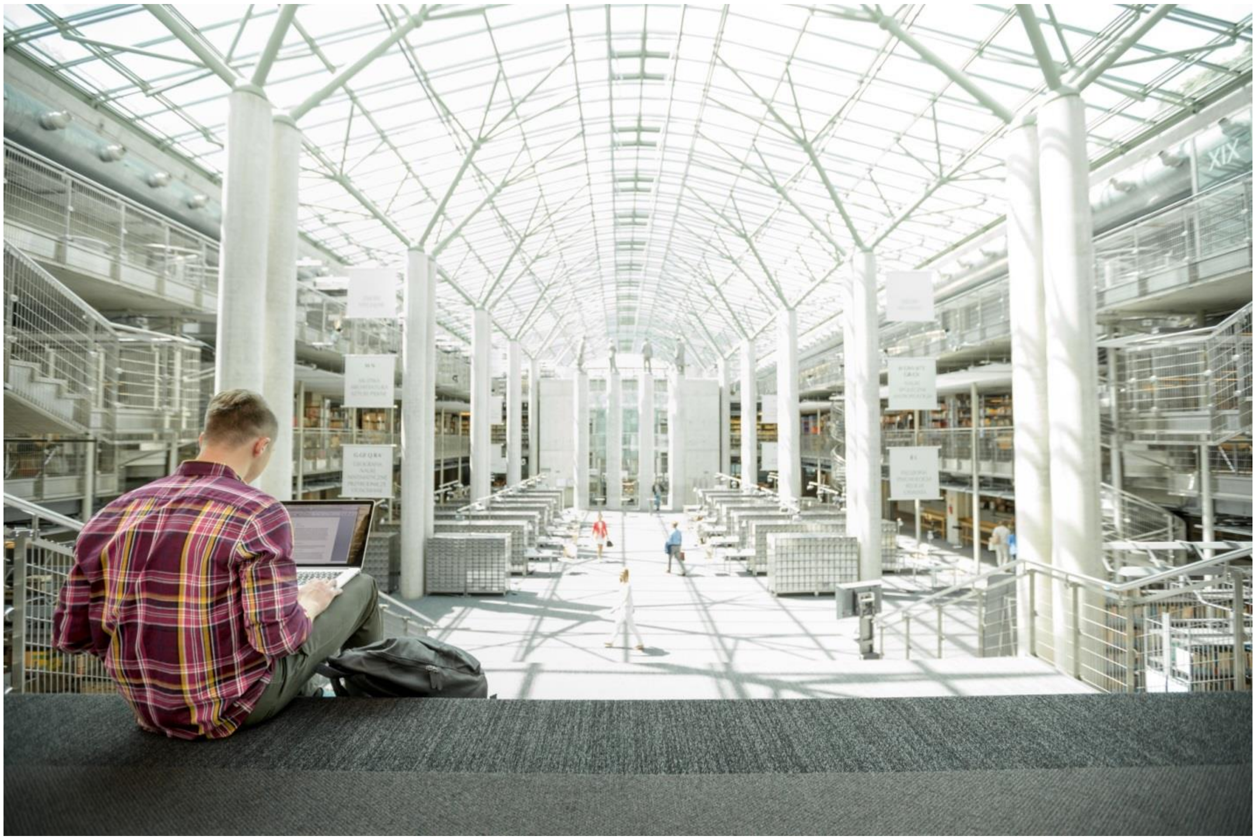


FlashStack Virtual Server Infrastructure with iSCSI Storage for VMware vSphere 6.7 U1

Deployment Guide for iSCSI and FlashStack with Cisco UCS 6400 Fabric Interconnect and Pure Storage FlashArray//X Series

Last Updated: August 13, 2019

About the Cisco Validated Design Program

The Cisco Validated Design (CVD) program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information, go to:

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

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

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

Table of Contents

Executive Summary

Cisco Validated Designs (CVDs) consist of systems and solutions that are designed, tested, and documented to facilitate and improve customer deployments. These designs incorporate a wide range of technologies and products into a portfolio of solutions that have been developed to address the business needs of our customers.

This document details the design described in the FlashStack Virtual Server Infrastructure for VMware vSphere 6.7 Update 1 Design Guide, which details a validated converged infrastructure jointly developed by Cisco and Pure Storage. In this solution, we explain the deployment of a predesigned, best-practice data center architecture with VMware vSphere built on Cisco Unified Computing System (Cisco UCS), the Cisco Nexus® 9000 family of switches, and Pure Storage FlashArray//X Series all flash storage configured for iSCSI based storage access.

When deployed, the architecture presents a robust infrastructure viable for a wide range of application workloads implemented as a virtual server infrastructure.

Solution Overview

Introduction

Currently in our industry, there is a trend for pre-engineered solutions which standardize the data center infrastructure, offering the business operational efficiencies, agility, and scale to address cloud, bi-modal IT and their business needs. The challenge is complexity, diverse application support, efficiency and risk; all these are met by FlashStack with:

- Reduced complexity and automatable infrastructure and easily deployed resources
- Robust components capable of supporting high performance and high bandwidth virtualized applications
- Efficiency through optimization of network bandwidth and in-line storage compression with de-duplication
- Risk reduction at each level of the design with resiliency built into each touch point throughout

Cisco and Pure Storage have partnered to deliver this Cisco Validated Design, combining storage, server and network components to serve as the foundation for virtualized workloads, enabling efficient architectural designs that can be quickly and confidently deployed.

In this document we will describe a reference architecture detailing a virtual server infrastructure composed of Cisco Nexus switches, Cisco UCS Compute, and a Pure Storage FlashArray//X R2 delivering a VMware vSphere 6.7 Update1 hypervisor environment.

Audience

The audience for this document includes, but is not limited to; sales engineers, field consultants, professional services, IT managers, partner engineers, and customers who want to modernize their infrastructure to meet their business needs

Purpose of this Document

This document details a step-by-step configuration and implementation guide for FlashStack, centered around the Cisco UCS 6454 Fabric Interconnect and the Pure Storage FlashArray//X70 R2. These components are supported by the 100G capable Cisco Nexus 9336C-FX2 switch to deliver a Virtual Server infrastructure on Cisco UCS B200 M5 Blade Servers and Cisco UCS C220 M5 Rack Servers running VMware vSphere 6.7 U1.

The design that will be implemented is discussed in the FlashStack Virtual Server Infrastructure for VMware vSphere 6.7 Update 1 Design Guide.

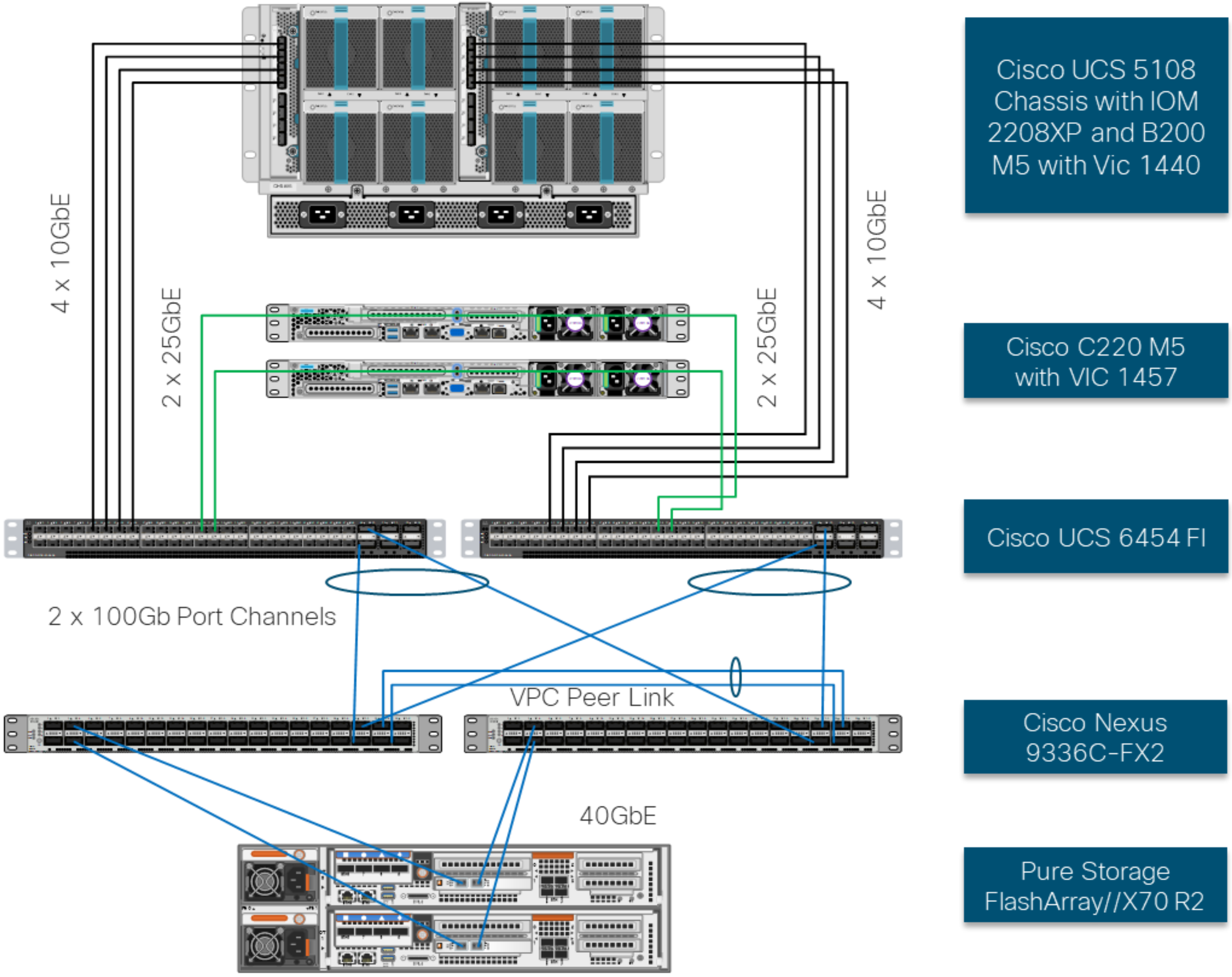
Solution Summary

The FlashStack Virtual Server Infrastructure is a validated reference architecture, collaborated on by Cisco and Pure Storage, built to serve enterprise data centers. The solution is built to deliver a VMware vSphere based environment, leveraging Cisco Unified Computing System (Cisco UCS), Cisco Nexus switches, and Pure Storage FlashArray.

The architecture brings together a simple, wire-once solution that is SAN booted from iSCSI and is highly resilient at each layer of the design. This creates an infrastructure that is ideal for a variety of virtual application deployments that can reliably scale when growth is needed.

Figure 1 illustrates the base physical architecture used in FlashStack Virtual Server Infrastructure.

Figure 1 FlashStack with Cisco UCS 6454 and Pure Storage FlashArray //70 R2


4 x 10GbE
2 x 25GbE
2 x 25GbE
4 x 10GbE
Cisco UCS 5108 Chassis with IOM 2208XP and B200 M5 with Vic 1440
Cisco C220 M5 with VIC 1457
Cisco UCS 6454 FI
2 x 100Gb Port Channels
VPC Peer Link
Cisco Nexus 9336C-FX2
40GbE
Pure Storage FlashArray//X70 R2

The reference hardware configuration includes:

- Two Cisco Nexus 9336C-FX2 Switches
- Two Cisco UCS 6454 Fabric Interconnects
- Cisco UCS 5108 Chassis with two Cisco UCS 2308 Fabric Extenders
- Two Cisco UCS B200 M5 Blade Servers
- Four Cisco UCS C220 M5 Rack Servers
- One Pure Storage FlashArray//X70 R2

The virtual environment this supports is within VMware vSphere 6.7 U1 and includes virtual management and automation components from Cisco and Pure Storage built into the solution, or as optional add-ons.

This document will provide a low-level example of steps to deploy this base architecture that may need some adjustments depending on the customer environment. These steps include physical cabling, network, storage, compute, and virtual device configurations.

Deployment Hardware and Software

Software Revisions

Table 1 lists the software versions for hardware and virtual components used in this solution. Each of these versions have been certified within interoperability matrixes supported by Cisco, Pure Storage, and VMware. For additional supported version information, consult the following sources:

- Cisco UCS Hardware and Software Interoperability Tool: http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html
- Pure Storage Interoperability(note, this interoperability list will require a support login from Pure): https://support.purestorage.com/FlashArray/Getting_Started/Compatibility_Matrix
- Pure Storage FlashStack Compatibility Matrix (note, this interoperability list will require a support login from Pure): https://support.purestorage.com/FlashStack/Product_Information/FlashStack_Compatibility_Matrix
- VMware Compatibility Guide: http://www.vmware.com/resources/compatibility/search.php
- Additionally, it is also strongly suggested to align FlashStack deployments with the recommended release for the Cisco Nexus 9000 switches used in the architecture:
  - Cisco Nexus: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/recommended_release/b_Minimum_and_Recommended_Cisco_NX-OS_Releases_for_Cisco_Nexus_9000_Series_Switches.html

If the selected versions differ from the validated versions listed in Table 1, it is highly recommended to read the release notes of the selected version to be aware of any changes to features or commands.

Table 1 Software Revisions

Layer	Device	Image	Comments
Compute	Cisco UCS Fabric Interconnects 6400 Series, UCS B-200 M5, UCS C-220 M5	4.0(2b)	Includes Cisco UCS IOM 2208 and Cisco VIC 1400 Series
Network	Cisco Nexus 9000 NX-OS	7.0(3)I7(5)	
Storage	Pure Storage FlashArray//X70 R2	5.1.9	
Software	Cisco UCS Manager	4.0(2b)	
	VMware vSphere ESXi Cisco Custom ISO	6.7 U1	
	VMware vSphere nenic Driver for ESXi	1.0.26.0	
	VMware vCenter	6.7 U1	
	Pure Storage vSphere Web Client Plugin	3.1.1	

Configuration Guidelines

This document details the step-by-step configuration of a fully redundant and highly available virtual server infrastructure built on Cisco and Pure Storage components. References are made to which component is configured with each step, either 01 or 02 or A and B. For example, controller-1 and controller-2 are used to identify the two controllers within the Pure Storage FlashArray//X that are provisioned in this document, and Cisco Nexus A or Cisco Nexus B identifies the pair of Cisco Nexus switches that are configured. The Cisco UCS fabric interconnects are similarly configured. Additionally, this document details the steps for provisioning multiple Cisco UCS hosts, and these examples are identified as: VM-Host-iSCSI-01, VM-Host-iSCSI-02 to represent iSCSI booted infrastructure and production hosts deployed to the fabric interconnects in this document. Finally, to indicate that you should include information pertinent to your environment in a given step, <<text>> appears as part of the command structure. See the following example during a configuration step for both Nexus switches:

```
AA12-9336C-A&B (config)# ntp server <<var_oob_ntp>> use-vrf management
```

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, and Table 3 lists the virtual machines (VMs) necessary for deployment as outlined in this guide.

Table 2 Required VLANs

VLAN Name	VLAN Purpose	ID Used in Validating this Document	Customer Deployed Value
Native	VLAN for untagged frames	2	
Out of Band Mgmt	VLAN for out-of-band management interfaces	15	
In-band Mgmt	VLAN for in-band management interfaces	215	
vMotion	VLAN for vMotion	1130	
VM-App-1301	VLAN for Production VM interfaces	1301	
VM-App-1302	VLAN for Production VM interfaces	1302	
VM-App-1303	VLAN for Production VM interfaces	1303	
iSCSI-A	VLAN for iSCSI A	1110	
iSCSI-B	VLAN for iSCSI b	1120	

Table 3 Infrastructure Servers

Server Description	Server Name Used in Validating This Document	Customer Deployed Value
vCenter Server	Pure-VC	
Active Directory	Pure-AD	

Table 4 Configuration Variables

Variable Name	Variable Description	Customer Deployed Value
<<var_nexus_A_hostname>>	Nexus switch A Host name (Example: AA12-9336C-A)	
<<var_nexus_A_mgmt_ip>>	Out-of-band management IP for Nexus switch A (Example: 192.168.164.90)	
<<var_oob_mgmt_mask>>	Out-of-band network mask (Example: 255.255.255.0)	
<<var_oob_gateway>>	Out-of-band network gateway (Example: 192.168.164.254)	
<<var_oob_ntp>>	Out-of-band management network NTP Server (Example: 172.26.163.254)	
<<var_nexus_B_hostname>>	Nexus switch B Host name (Example: AA12-9336C-B)	
<<var_nexus_B_mgmt_ip>>	Out-of-band management IP for Nexus switch B (Example: 162.168.164.91)	
<<var_flasharray_hostname>>	Array Hostname set during setup (Example: flashstack-1)	
<<var_flasharray_vip>>	Virtual IP that will answer for the active management controller (Example: 10.2.164.45)	
<<var_contoller-1_mgmt_ip>>	Out-of-band management IP for FlashArray controller-1 (Example:10.2.164.47)	
<<var_contoller-1_mgmt_mask>>	Out-of-band management network netmask (Example: 255.255.255.0)	
<<var_contoller-1_mgmt_gateway>>	Out-of-band management network default gateway (Example: 192.168.164.254)	
<<var_contoller-2_mgmt_ip>>	Out-of-band management IP for FlashArray controller-2 (Example:10.2.164.49)	
<<var_contoller-2_mgmt_mask>>	Out-of-band management network netmask (Example: 255.255.255.0)	
<<var_ contoller-2_mgmt_gateway>>	Out-of-band management network default gateway (Example: 192.168.164.254)	
<<var_password>>	Administrative password (Example: Fl@shSt4x)	
<<var_dns_domain_name>>	DNS domain name (Example: flashstack.cisco.com)	
<<var_nameserver_ip>>	DNS server IP(s) (Example: 10.1.164.9)	
<<var_smtp_ip>>	Email Relay Server IP Address or FQDN (Example: smtp.flashstack.cisco.com)	

Variable Name	Variable Description	Customer Deployed Value
<<var_smtp_domain_name>>	Email Domain Name (Example: flashstack.cisco.com)	
<<var_timezone>>	FlashStack time zone (Example: America/New_York)	
<<var_oob_mgmt_vlan_id>>	Out-of-band management network VLAN ID (Example: 15)	
<<var_ib_mgmt_vlan_id>>	In-band management network VLAN ID (Example: 215)	
<<var_ib_mgmt_vlan_netmask_length>>	Length of IB-MGMT-VLAN Netmask (Example: /24)	
<<var_ib_gateway_ip>>	In-band management network VLAN ID (Example: 10.2.164.254)	
<<var_iscsi-a_vlan_id>>	iSCSI-A VLAN ID (Example: 1110)	
<<var_iscsi-b_vlan_id>>	iSCSI-B VLAN ID (Example: 1120)	
<<var_vmotion_vlan_id>>	vMotion network VLAN ID (Example: 1130)	
<<var_vmotion_vlan_netmask_length>>	Length of vMotion VLAN Netmask (Example: /24)	
<<var_native_vlan_id>>	Native network VLAN ID (Example: 2)	
<<var_app_vlan_id>>	Example Application network VLAN ID (Example: 1301)	
<<var_snmp_contact>>	Administrator e-mail address (Example: admin@flashstack.cisco.com)	
<<var_snmp_location>>	Cluster location string (Example: RTP9-AA12)	
<<var_ucs_clustername>>	Cisco UCS Manager cluster host name (Example: AA-12-ucs-6454)	
<<var_ucs_a_mgmt_ip>>	Cisco UCS fabric interconnect (FI) A out-of-band management IP address (Example: 10.2.164.51)	
<<var_ucs_mgmt_vip>>	Cisco UCS fabric interconnect (FI) Cluster out-of-band management IP address (Example: 10.2.164.50)	
<<var_ucs b_mgmt_ip>>	Cisco UCS fabric interconnect (FI) Cluster out-of-band management IP address (Example: 10.2.164.52)	
<<var_vm_host_iscsi_01_ip>>	VMware ESXi host 01 in-band management IP (Example:10.2.164.71)	

Variable Name	Variable Description	Customer Deployed Value
<<var_vm_host_iscsi_vmotion_01_ip>>	VMware ESXi host 01 vMotion IP (Example: 192.168.130.71)	
<<var_vm_host_iscsi_02_ip>>	VMware ESXi host 02 in-band management IP (Example:10.2.164.72)	
<<var_vm_host_iscsi_vmotion_02_ip>>	VMware ESXi host 02 vMotion IP (Example: 192.168.130.72)	
<<var_vmotion_subnet_mask>>	vMotion subnet mask (Example: 255.255.255.0)	
<<var_vcenter_server_ip>>	IP address of the vCenter Server (Example: 10.1.164.20)	

Physical Topology

This section details a cabling example for a FlashStack environment. To make connectivity clear in this example, the tables include both the local and remote port locations.

This document assumes that out-of-band management ports are plugged into an existing management infrastructure at the deployment site. The upstream network from the Nexus 9336C-FX2 switches is out of scope of this document, with only the assumption that these switches will connect to the upstream switch or switches with a vPC.

Figure 2 shows the cabling configuration used in this FlashStack design.

Figure 2 FlashStack Cabling in the Validate Topology

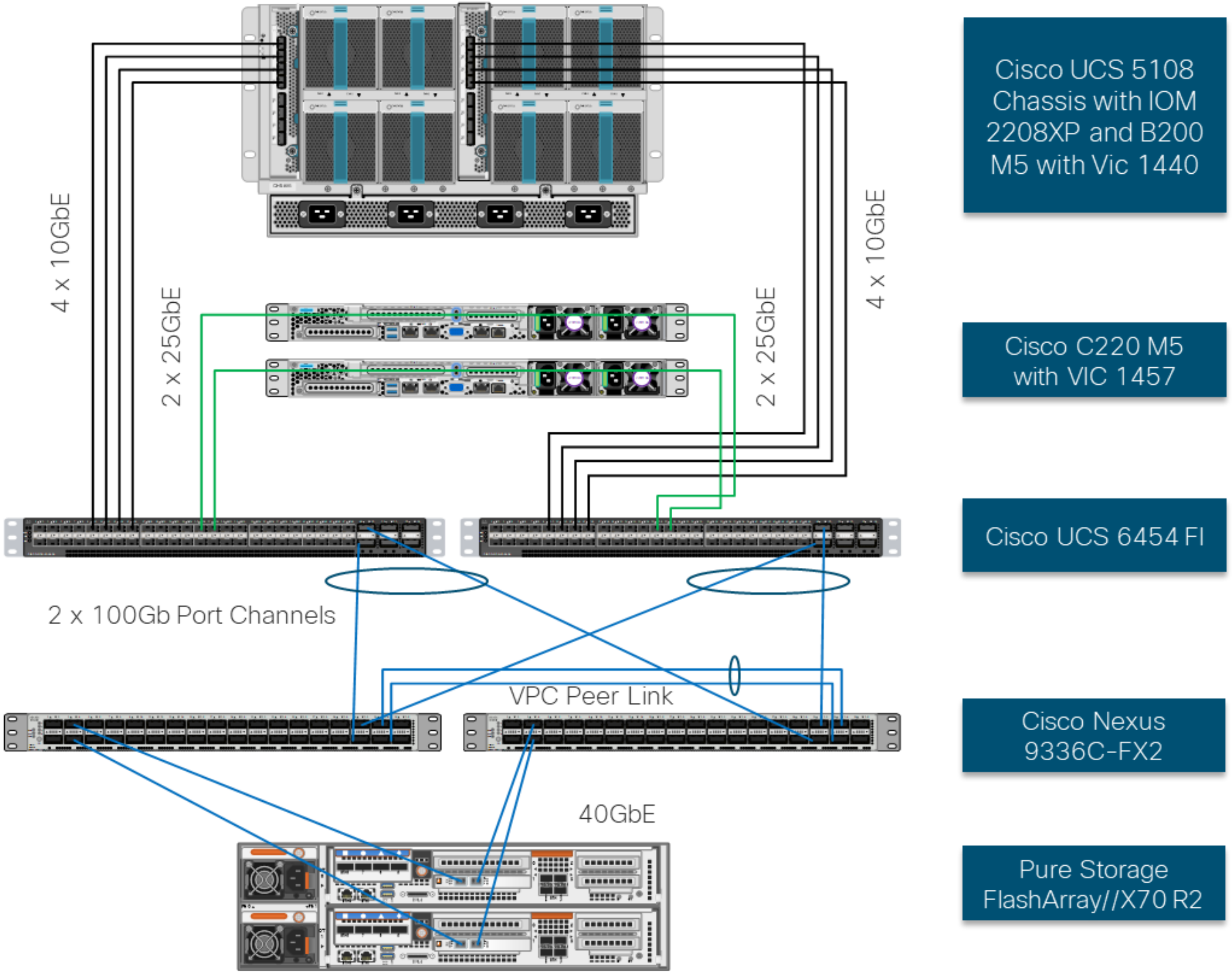

4 x 10GbE
2 x 25GbE
2 x 25GbE
4 x 10GbE
2 x 100Gb Port Channels
VPC Peer Link
40GbE
Cisco UCS 5108 Chassis with IOM 2208XP and B200 M5 with Vic 1440
Cisco C220 M5 with VIC 1457
Cisco UCS 6454 FI
Cisco Nexus 9336C-FX2
Pure Storage FlashArray//X70 R2

Table 5 Cisco Nexus 9336C-FX2-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote port
Cisco Nexus 9336C-FX2-A	Eth 1/1	40Gbe	FlashArray//X70 R2 Controller 1	CT0.ETH14
	Eth 1/2	40Gbe	FlashArray//X70 R2 Controller 2	CT1.ETH14
	Eth 1/31	100Gbe	Cisco UCS 6454-A	Eth 1/49
	Eth 1/32	100Gbe	Cisco UCS 6454-B	Eth 1/49
	Eth 1/33	100Gbe	Cisco Nexus 9336C-FX2-B	Eth 1/33
	Eth 1/34	100Gbe	Cisco Nexus 9336C-FX2-B	Eth 1/33

Local Device	Local Port	Connection	Remote Device	Remote port
	Eth 1/35	10Gbe or 40Gbe or 100Gbe	Upstream Network Switch	Any
	Eth 1/36	10Gbe or 40Gbe or 100Gbe	Upstream Network Switch	Any
	Mgmt0	Gbe	Gbe Management Switch	Any

Table 6 Cisco Nexus 9336C-FX2-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote port
Cisco Nexus 9336C-FX2-B	Eth 1/1	40Gbe	FlashArray//X70 R2 Controller 1	CT0.ETH15
	Eth 1/2	40Gbe	FlashArray//X70 R2 Controller 2	CT1.ETH15
	Eth 1/31	100Gbe	Cisco UCS 6454-A	Eth 1/50
	Eth 1/32	100Gbe	Cisco UCS 6454-B	Eth 1/50
	Eth 1/33	100Gbe	Cisco Nexus 9336C-FX2-A	Eth 1/33
	Eth 1/34	100Gbe	Cisco Nexus 9336C-FX2-A	Eth 1/33
	Eth 1/35	10Gbe or 40Gbe or 100Gbe	Upstream Network Switch	Any
	Eth 1/36	10Gbe or 40Gbe or 100Gbe	Upstream Network Switch	Any
	Mgmt0	Gbe	Gbe Management Switch	Any

Table 7 Cisco UCS-6545-A Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote port
Cisco UCS-6454-A	Eth 1/49	100Gbe	Cisco Nexus 9336C-FX2-A	Eth 1/31
	Eth 1/50	100Gbe	Cisco Nexus 9336C-FX2-B	Eth 1/31
	Eth 1/9	10Gbe	Cisco UCS Chassis 1 2208 FEX A	IOM 1/1
	Eth 1/10	10Gbe	Cisco UCS Chassis 1 2208 FEX A	IOM 1/2
	Eth 1/11	10Gbe	Cisco UCS Chassis 1	IOM 1/3

Local Device	Local Port	Connection	Remote Device	Remote port
			2208 FEX A	
	Eth 1/12	10Gbe	Cisco UCS Chassis 1 2208 FEX A	IOM 1/4
	Eth 1/17	25Gbe	Cisco UCS C220-01	Eth 1
	Eth 1/18	25Gbe	Cisco UCS C220-01	Eth 2
	Eth 1/19	25Gbe	Cisco UCS C220-02	Eth 1
	Eth 1/20	25Gbe	Cisco UCS C220-02	Eth 2
	Mgmto	Gbe	Gbe Management Switch	Any

Table 8 Cisco UCS-6545-B Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote port
Cisco UCS-6454-B	Eth 1/49	100Gbe	Cisco Nexus 9336C-FX2-A	Eth 1/32
	Eth 1/50	100Gbe	Cisco Nexus 9336C-FX2-B	Eth 1/32
	Eth 1/9	10Gbe	Cisco UCS Chassis 1 2208 FEX B	IOM 1/1
	Eth 1/10	10Gbe	Cisco UCS Chassis 1 2208 FEX B	IOM 1/2
	Eth 1/11	10Gbe	Cisco UCS Chassis 1 2208 FEX B	IOM 1/3
	Eth 1/12	10Gbe	Cisco UCS Chassis 1 2208 FEX B	IOM 1/4
	Eth 1/17	25Gbe	Cisco UCS C220-01	Eth 3
	Eth 1/18	25Gbe	Cisco UCS C220-01	Eth 4
	Eth 1/19	25Gbe	Cisco UCS C220-02	Eth 3
	Eth 1/20	25Gbe	Cisco UCS C220-02	Eth 4
	Mgmto	Gbe	Gbe Management Switch	Any

Table 9 Pure Storage FlashArray//X70 R2 Controller 1 Cabling Information

Local Device	Local Port	Connection	Remote Device	Remote port
FlashArray//X70 R2 Controller 1	Eth 14	40Gbe	Cisco Nexus 9336C-FX2-A	Eth 1/1
	Eth 15	40Gbe	Cisco Nexus 9336C-FX2-B	Eth 1/1
	Eth0	Gbe	Gbe Management Switch	Any

Table 10 Pure Storage FlashArray//X70 R2 Controller 2 Cabling Information

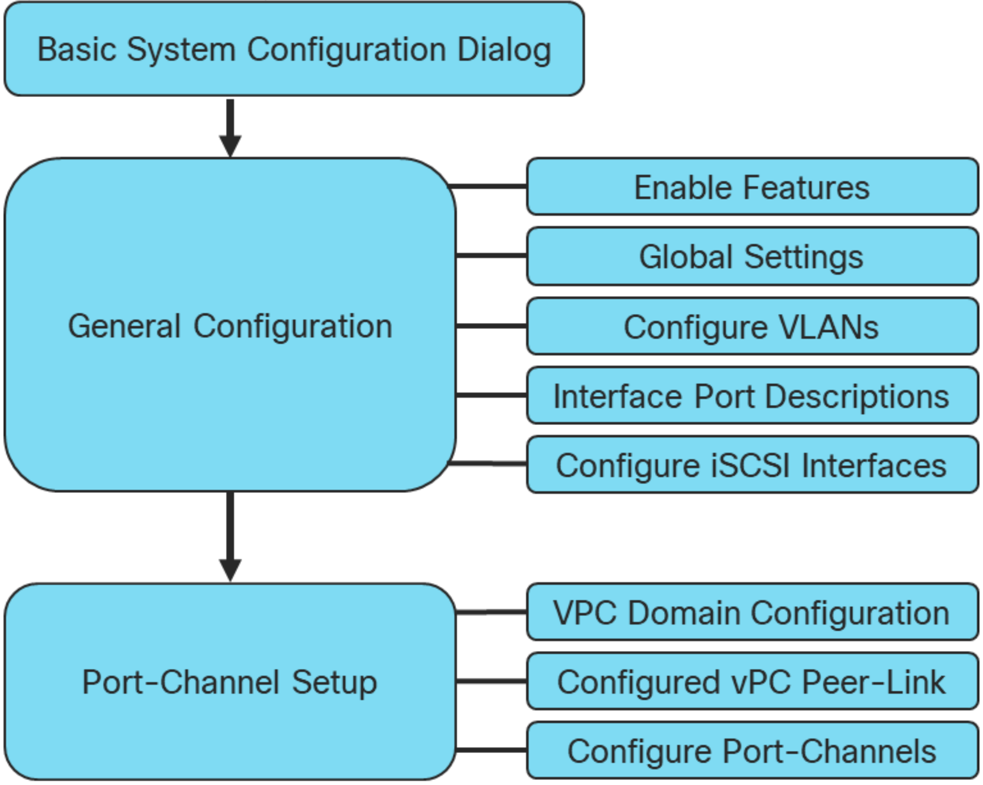
Local Device	Local Port	Connection	Remote Device	Remote port
FlashArray//X70 R2 Controller 2	Eth 14	40Gbe	Cisco Nexus 9336C-FX2-A	Eth 1/2
	Eth 15	40Gbe	Cisco Nexus 9336C-FX2-B	Eth 1/2
	Eth0	Gbe	Gbe Management Switch	Any

Network Switch Configuration

Network Configuration

The following procedures describe how to configure the Cisco Nexus switches for use in a base FlashStack environment. This procedure assumes the use of Nexus 9336C-FX2 switches running 7.0(3)I7(5). Configuration on a differing model of Nexus 9000 series switch should be comparable but may differ slightly with model and changes in NX-OS release. The Cisco Nexus 9336C-FX2 switch and NX-OS 7.0(3)I7(5) release were used in validation of this FlashStack solution, so steps will reflect this model and release.

Figure 3 Network Configuration Workflow



Physical Connectivity

Physical cabling should be completed by following the diagram and table references in the previous section referenced as FlashStack Cabling.

Cisco Nexus Basic System Configuration Dialog

This section provides detailed instructions for the configuration of the Cisco Nexus 9336C-FX2 switches used in this FlashStack solution. Some changes may be appropriate for a customer's environment, but care should be taken when stepping outside of these instructions as it may lead to an improper configuration.

Cisco Nexus Basic System Configuration Dialog

```
Abort Auto Provisioning and continue with normal setup ?(yes/no)[n]: y
---- System Admin Account Setup ----
```

```
Do you want to enforce secure password standard (yes/no) [y]: yes

  Enter the password for "admin":
  Confirm the password for "admin":

         ---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus9000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus9000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

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

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

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

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

  Enter the switch name : <<var_nexus_A_hostname>>

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

    Mgmt0 IPv4 address : <<var_nexus_A_mgmt_ip>>

    Mgmt0 IPv4 netmask : <<var_oob_mgmt_mask>>

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

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

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

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

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

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

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

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

    NTP server IPv4 address : <<var_oob_ntp>>

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

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

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

The following configuration will be applied:
  password strength-check
  switchname AA12-9336C-A
```

```
vrf context management
ip route 0.0.0.0/0 192.168.164.254
exit
  no feature telnet
  ssh key rsa 2048 force
  feature ssh
  ntp server 172.26.163.254
  system default switchport
  no system default switchport shutdown
  copp profile strict
interface mgmt0
ip address 192.168.164.90 255.255.252.0
no shutdown

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

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

Cisco Nexus Switch Configuration

Enable Features and Settings

To enable IP switching features, run the following commands on each Cisco Nexus:

```
AA12-9336C-A&B (config)# feature lacp
AA12-9336C-A&B (config)# feature vpc
AA12-9336C-A&B (config)# feature interface-vlan
```

The feature interface-vlan is an optional requirement if configuring an In-Band VLAN interface to redistribute NTP. Layer-3 routing is possible with Nexus switches after setting this feature but is not covered in this architecture.

Additionally, configure spanning tree and save the running configuration to start-up:

```
AA12-9336C-A&B (config)# spanning-tree port type network default
AA12-9336C-A&B (config)# spanning-tree port type edge bpduguard default
AA12-9336C-A&B (config)# spanning-tree port type edge bpdufilter default
```

Configure Global Settings

Run the following commands on both switches to set global configurations:

```
AA12-9336C-A&B (config)# port-channel load-balance src-dst l4port
AA12-9336C-A&B (config)# ip route 0.0.0.0/0 <<var ib-mgmt-vlan_gateway>>
AA12-9336C-A&B (config)# ntp server <<var_oob_ntp>> use-vrf management
AA12-9336C-A&B (config)# ntp master 3
```

Configure VLANs

Run the following commands on both switches to create VLANs:

```
AA12-9336C-A&B (config)# vlan <<var_ib-mgmt_vlan_id>>
AA12-9336C-A&B (config-vlan)# name IB-MGMT-VLAN
AA12-9336C-A&B (config-vlan)# vlan <<var_native_vlan_id>>
AA12-9336C-A&B (config-vlan)# name Native-VLAN
AA12-9336C-A&B (config-vlan)# vlan <<var_vmotion_vlan_id>>
AA12-9336C-A&B (config-vlan)# name vMotion-VLAN
AA12-9336C-A&B (config-vlan)#  vlan <<var_application_vlan_id>>
AA12-9336C-A&B (config-vlan)#  name VM-App1-VLAN
AA12-9336C-A&B (config-vlan)#  vlan <<var_iscsi-a_vlan_id>>
AA12-9336C-A&B (config-vlan)#  name iSCSI-A-VLAN
```

```
AA12-9336C-A&B (config-vlan)#  vlan <<var_iscsi-b_vlan_id>>
AA12-9336C-A&B (config-vlan)#  name iSCSI-B-VLAN
```

Continue adding VLANs as appropriate to your environment.

Add Interface Port Descriptions

To add individual port descriptions for troubleshooting activity and verification for switch A, run the following commands from the global configuration mode:

```
AA12-9336C-A(config-if)# interface Ethernet1/1
AA12-9336C-A(config-if)# description AA12-FlashArray-CT0.ETH14
AA12-9336C-A(config-if)# interface Ethernet1/2
AA12-9336C-A(config-if)# description AA12-FlashArray-CT1.ETH14
AA12-9336C-A(config-if)# interface Ethernet1/31
AA12-9336C-A(config-if)# description AA12-UCS-6454-A-Eth1/53
AA12-9336C-A(config-if)# interface Ethernet1/32
AA12-9336C-A(config-if)# description AA12-UCS-6454-B-Eth1/53
AA12-9336C-A(config-if)# interface Ethernet1/33
AA12-9336C-A(config-if)# description AA12-9336C-B-Eth1/33 Peer Link
AA12-9336C-A(config-if)# interface Ethernet1/34
AA12-9336C-A(config-if)# description AA12-9336C-B-Eth1/34 Peer Link
AA12-9336C-A(config-if)# interface Ethernet1/35
AA12-9336C-A(config-if)# description Network-Uplink-A
AA12-9336C-A(config-if)# interface Ethernet1/36
AA12-9336C-A(config-if)# description Network-Uplink-B
```

To add individual port descriptions for troubleshooting activity and verification for switch B, run the following commands from the global configuration mode:

```
AA12-9336C-B(config-if)# interface Ethernet1/1
AA12-9336C-B(config-if)# description AA12-FlashArray-CT0.ETH15
AA12-9336C-B(config-if)# interface Ethernet1/2
AA12-9336C-B(config-if)# description AA12-FlashArray-CT1.ETH15
AA12-9336C-B(config-if)# interface Ethernet1/31
AA12-9336C-B(config-if)# description AA12-UCS-6454-A-Eth1/54
AA12-9336C-B(config-if)# interface Ethernet1/32
AA12-9336C-B(config-if)# description AA12-UCS-6454-B-Eth1/54
AA12-9336C-B(config-if)# interface Ethernet1/33
AA12-9336C-B(config-if)# description AA12-9336C-A-Eth1/33 Peer Link
AA12-9336C-B(config-if)# interface Ethernet1/34
AA12-9336C-B(config-if)# description AA12-9336C-A-Eth1/34 Peer Link
AA12-9336C-B(config-if)# interface Ethernet1/35
AA12-9336C-B(config-if)# description Network-Uplink-A
AA12-9336C-B(config-if)# interface Ethernet1/36
AA12-9336C-B(config-if)# description Network-Uplink-B
```

Configure iSCSI Interfaces

Configure the iSCSI interfaces to connect to the FlashArray//X R2.

For 9336C-A

```
AA12-9336C-A(config-if)# interface Ethernet1/1
AA12-9336C-A(config-if)# switchport access vlan <<var_iscsi-a_vlan_id>>
AA12-9336C-A(config-if)# spanning-tree port type edge
AA12-9336C-A(config-if)# mtu 9216
AA12-9336C-A(config-if)# no negotiate auto
AA12-9336C-A(config-if)# no shutdown
AA12-9336C-A(config-if)# interface Ethernet1/2
AA12-9336C-A(config-if)# switchport access vlan <<var_iscsi-a_vlan_id>>
AA12-9336C-A(config-if)# spanning-tree port type edge
AA12-9336C-A(config-if)# mtu 9216
AA12-9336C-A(config-if)# no negotiate auto
AA12-9336C-A(config-if)# no shutdown
```

Configure iSCSI interfaces for connecting to the FlashArray//X R2.

For 9336C-B

```
AA12-9336C-B(config-if)# interface Ethernet1/1
AA12-9336C-B(config-if)# switchport access vlan <<var_iscsi-a_vlan_id>>
AA12-9336C-B(config-if)# spanning-tree port type edge
AA12-9336C-B(config-if)# mtu 9216
AA12-9336C-B(config-if)# no negotiate auto
AA12-9336C-B(config-if)# no shutdown

AA12-9336C-B(config-if)# interface Ethernet1/2
AA12-9336C-B(config-if)# switchport access vlan <<var_iscsi-a_vlan_id>>
AA12-9336C-B(config-if)# spanning-tree port type edge
AA12-9336C-B(config-if)# mtu 9216
AA12-9336C-B(config-if)# no negotiate auto
AA12-9336C-B(config-if)# no shutdown
```

Configure vPC Domain Settings

The vPC domain will be assigned a unique number from 1-1000 and will handle the vPC settings specified within the switches.

To set the vPC domain configuration on 9336C-A, run the following commands:

```
AA12-9336C-A(config)# vpc domain 10
AA12-9336C-A(config-vpc-domain)# peer-switch
AA12-9336C-A(config-vpc-domain)# role priority 10
AA12-9336C-A(config-vpc-domain)# peer-keepalive destina-
tion <<var_nexus_B_mgmt_ip>> source <<var_nexus_A_mgmt_ip>>
AA12-9336C-A(config-vpc-domain)# delay restore 150
AA12-9336C-A(config-vpc-domain)# peer-gateway
AA12-9336C-A(config-vpc-domain)# auto-recovery
AA12-9336C-A(config-vpc-domain)# ip arp synchronize
```

To set the vPC domain configuration on 9336C-B, run the following commands:

```
AA12-9336C-B(config)# vpc domain 10
AA12-9336C-B(config-vpc-domain)# peer-switch
AA12-9336C-B(config-vpc-domain)# role priority 20
AA12-9336C-B(config-vpc-domain)# peer-keepalive destina-
tion <<var_nexus_A_mgmt_ip>> source <<var_nexus_B_mgmt_ip>>
AA12-9336C-B(config-vpc-domain)# delay restore 150
AA12-9336C-B(config-vpc-domain)# peer-gateway
AA12-9336C-B(config-vpc-domain)# auto-recovery
AA12-9336C-B(config-vpc-domain)# ip arp synchronize
```

Configure vPC Peer-Link

On each switch, configure the Port Channel member interfaces that will be part of the vPC Peer Link and configure the vPC Peer Link:

```
AA12-9336C-A&B (config)# int eth 1/33-34
AA12-9336C-A&B (config-if-range)# switchport mode trunk
AA12-9336C-A&B (config-if-range)# switchport trunk native vlan 2
AA12-9336C-A&B (config-if-range)# switchport trunk allowed vlan 215,1110,1120,1130,1301-1303
AA12-9336C-A&B (config-if-range)# channel-group 133 mode active
AA12-9336C-A&B (config-if-range)# no shut
AA12-9336C-A&B (config-if-range)# int port-channel 133
AA12-9336C-A&B (config-if)# description AA12-9336C Peer Link
AA12-9336C-A&B (config-if)# vpc peer-link
```

Configure Port Channels

On each switch, configure the Port Channel member interfaces and the vPC Port Channels to the Cisco UCS Fabric Interconnect and the upstream network switches:

Nexus Connection vPC to UCS Fabric Interconnect A

```
AA12-9336C-A&B (config)# int eth 1/31
AA12-9336C-A&B (config-if)# switchport mode trunk
AA12-9336C-A&B (config-if)# switchport trunk native vlan 2
AA12-9336C-A&B (config-if)# switchport trunk allowed vlan 215,1110,1120,1130,1301-1303
AA12-9336C-A&B (config-if)# channel-group 131 mode active
AA12-9336C-A&B (config-if)# no shut
AA12-9336C-A&B (config-if)# int port-channel 131
AA12-9336C-A&B (config-if)# description AA12-UCS-6454-A
AA12-9336C-A&B (config-if)# vpc 131
```

Nexus Connection vPC to UCS Fabric Interconnect B

```
AA12-9336C-A&B (config)# int eth 1/32
AA12-9336C-A&B (config-if)# switchport mode trunk
AA12-9336C-A&B (config-if)# switchport trunk native vlan 2
AA12-9336C-A&B (config-if)# switchport trunk allowed vlan 215,1110,1120,1130,1301-1303
AA12-9336C-A&B (config-if)# channel-group 132 mode active
AA12-9336C-A&B (config-if)# no shut
AA12-9336C-A&B (config-if)# int port-channel 132
AA12-9336C-A&B (config-if)# description AA12-UCS-6454-B
AA12-9336C-A&B (config-if)# vpc 132
```

Nexus Connection vPC to Upstream Network

```
AA12-9336C-A&B (config)# int eth 1/35-36
AA12-9336C-A&B (config-if-range)# switchport mode trunk
AA12-9336C-A&B (config-if-range)# switchport trunk native vlan 2
AA12-9336C-A&B (config-if-range)# switchport trunk allowed vlan 215,1110,1120,1130,1301-1303
AA12-9336C-A&B (config-if-range)# channel-group 135 mode active
AA12-9336C-A&B (config-if-range)# no shut
AA12-9336C-A&B (config-if-range)# int port-channel 135
AA12-9336C-A&B (config-if)# description Uplink
AA12-9336C-A&B (config-if)# vpc 135
```

Storage Configuration

Pure Storage FlashArray//X70 R2 Configuration

FlashArray Initial Configuration

The information listed in Table 11 should be gathered to enable the installation and configuration of the FlashArray. An official representative of Pure Storage or a Certified Partner will help rack and configure the new installation of the FlashArray.

Table 11 FlashArray Setup Information

Global Array Settings Heading Title	
Array Name (Hostname for Pure Array):	<<var_flasharray_hostname>>
Virtual IP Address for Management:	<<var_flasharray_vip>>
Physical IP Address for Management on Controller 0 (CT0):	<<var_contoller-1_mgmt_ip>>
Physical IP Address for Management on Controller 1 (CT1):	<<var_contoller-2_mgmt_ip>>
Netmask:	<<var_contoller-1_mgmt_mask>>
Gateway IP Address:	<<var_contoller-1_mgmt_gateway>>
DNS Server IP Address(es):	<<var_nameserver_ip>>
DNS Domain Suffix: (Optional)	<<var_dns_domain_name>>
NTP Server IP Address or FQDN:	<<var_oob_ntp>>
Email Relay Server (SMTP Gateway IP address or FQDN): (Optional)	<<var_smtp_ip>>
Email Domain Name:	<<var_smtp_domain_name>>
Alert Email Recipients Address(es): (Optional)	
HTTP Proxy Server ad Port (For Pure1): (Optional)	
Time Zone:	<<var_timezone>>

When the FlashArray has completed initial configuration, it is important to configure the Cloud Assist phone-home connection to provide the best pro-active support experience possible. Furthermore, this will enable the analytics functionalities provided by Pure1.

Add an Alert Recipient

The Alerts sub-view is used to manage the list of addresses to which Purity delivers alert notifications, and the attributes of alert message delivery. You can designate up to 19 alert recipients. The Alert Recipients section displays a list of email addresses that are designated to receive Purity alert messages. Up to 20 alert recipients can be designated. The list includes the built-in flasharray-alerts@purestorage.com address, which cannot be deleted.

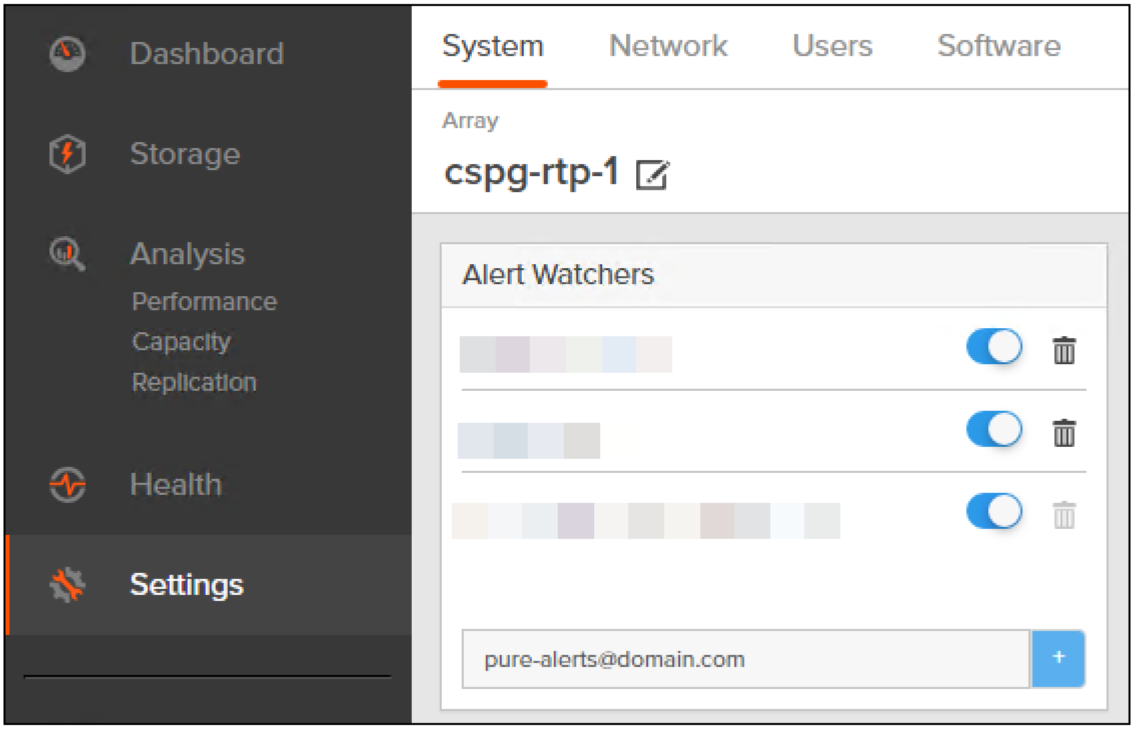
The email address that Purity uses to send alert messages includes the sender domain name and is comprised of the following components:

<Array_Name>-<Controller_Name>@<Sender_Domain_Name>.com

To add an alert recipient, follow these steps:

1. Select Settings

2. In the Alert Watchers section, enter the email address of the alert recipient and click the + icon.

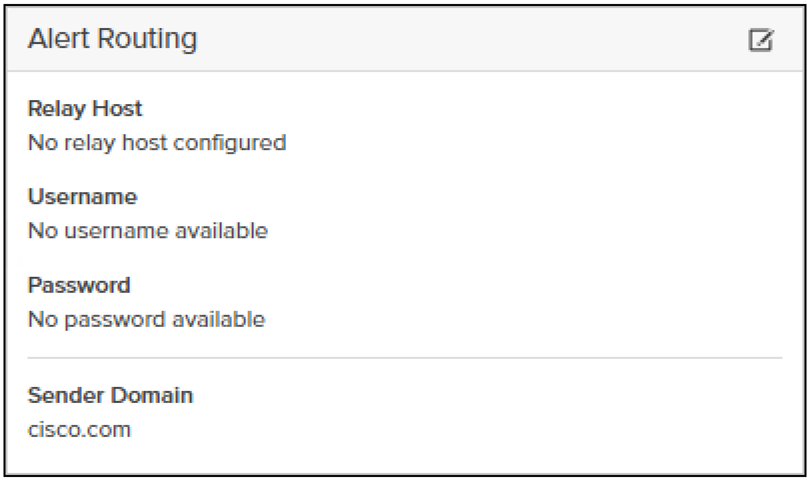


pure-alerts@domain.com

The **Relay Host** section displays the hostname or IP address of an SMTP relay host, if one is configured for the array. If you specify a relay host, Purity routes the email messages via the relay (mail forwarding) address rather than sending them directly to the alert recipient addresses.

In the **Sender Domain** section, the sender domain determines how Purity logs are parsed and treated by Pure Storage Support and Escalations. By default, the sender domain is set to the domain name please-configure.me.

It is crucial that you set the sender domain to the correct domain name. If the array is not a Pure Storage test array, set the sender domain to the actual customer domain name. For example, mycompany.com.



Alert Routing

Relay Host
No relay host configured

Username
No username available

Password
No password available

Sender Domain
cisco.com

Configure Pure1 Support

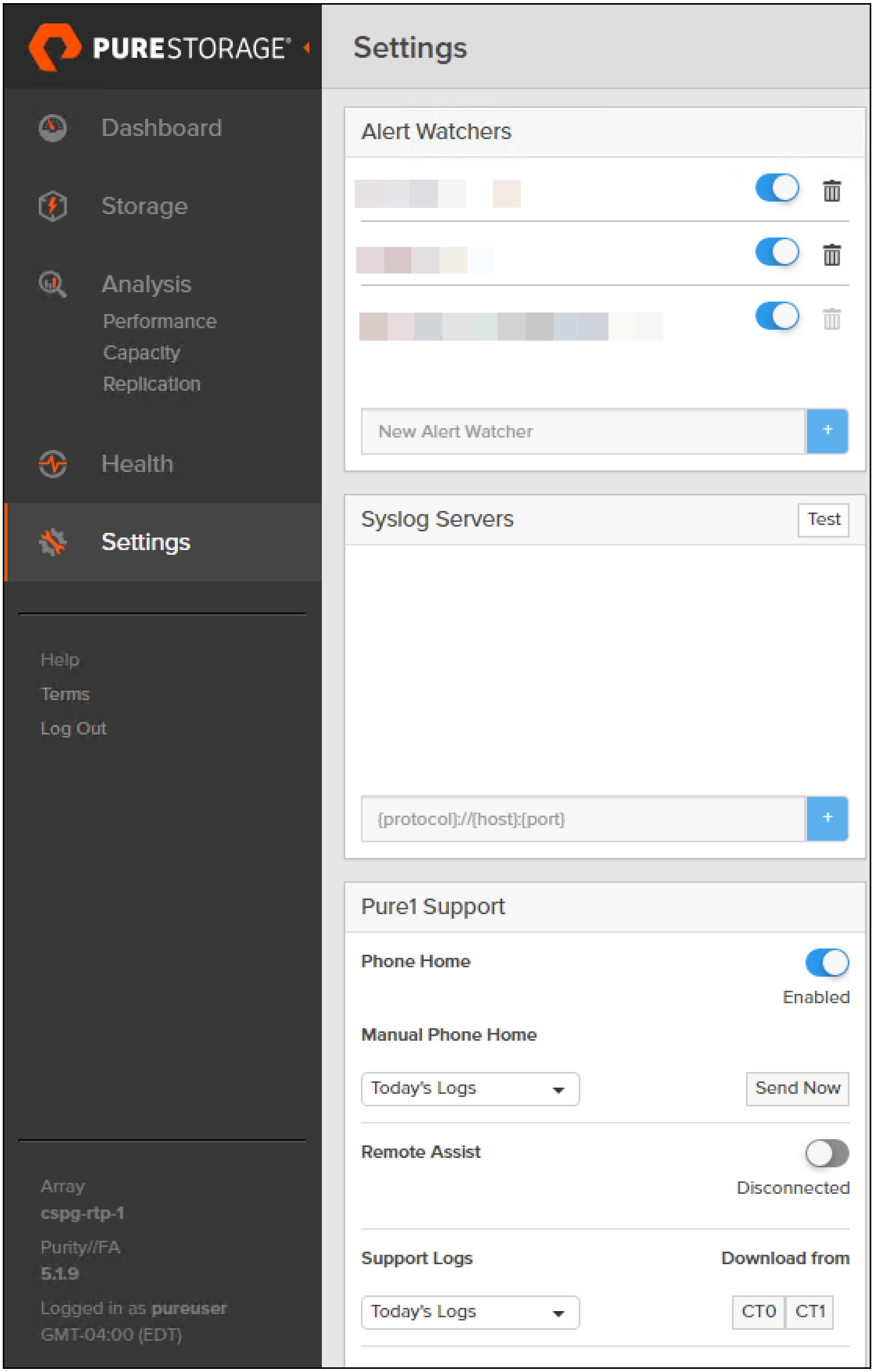
The **Pure1 Support** section manages the phone home facility. The phone home facility provides a secure direct link between the array and the Pure Storage Technical Support web site. The link is used to transmit log contents and alert messages to the Pure Storage Support team so that when diagnosis or remedial action is required, complete recent history about array performance and significant events is available.

The **Remote Assist** section displays the remote assist status as "Connected" or "Disconnected". By default, remote assist is disconnected. A connected remote assist status means that a remote assist session has been opened, allowing Pure Storage Support to connect to the array. Disconnect the remote assist session to close the session.

By default, the phone home facility is enabled. If the phone home facility is enabled to send information automatically, Purity transmits log and alert information directly to Pure Storage Support via a secure network connection. Log contents are transmitted hourly and stored at the support web site, enabling detection of array performance and error rate trends. Alerts are reported immediately when they occur so that timely action can be taken.

Phone home logs can also be sent to Pure Storage Technical support on demand, with options including Today's Logs, Yesterday's Logs, or All Log History.

The Support Logs section allows you to download the Purity log contents of the specified controller to the current administrative workstation. Purity continuously logs a variety of array activities, including performance summaries, hardware and operating status reports, and administrative actions.



Settings

Alert Watchers

[redacted]

[redacted]

[redacted]

New Alert Watcher

Syslog Servers

{protocol}://{host}:{port}

Pure1 Support

Phone Home: Enabled

Manual Phone Home: Today's Logs

Remote Assist: Disconnected

Support Logs: Today's Logs

Download from

Array
cspg-rtp-1

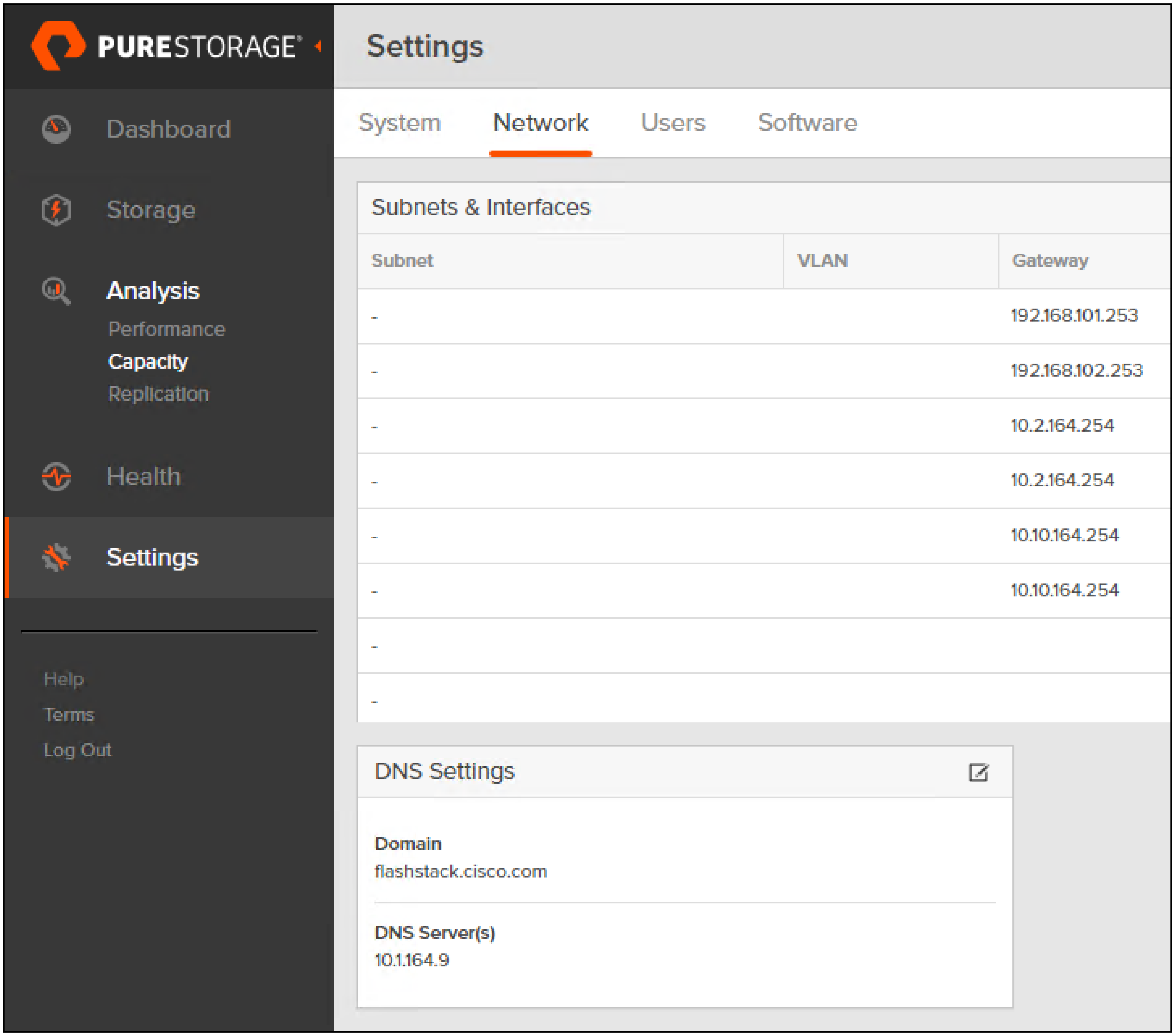
Purity//FA
5.1.9

Logged in as **pureuser**
GMT-04:00 (EDT)

Configure the Domain Name System (DNS) Server IP Addresses

To configure the DNS server IP addresses, follow these steps:

1. Select Settings > Network.
2. In the DNS section, hover over the domain name and click the pencil icon. The Edit DNS dialog box appears.



Subnets & Interfaces

Subnet	VLAN	Gateway
-		192.168.101.253
-		192.168.102.253
-		10.2.164.254
-		10.2.164.254
-		10.10.164.254
-		10.10.164.254
-		
-		

DNS Settings

Domain
flashstack.cisco.com

DNS Server(s)
10.1.164.9

3. Complete the following fields:
   a. Domain: Specify the domain suffix to be appended by the array when doing DNS lookups.
   b. NS#: Specify up to three DNS server IP addresses for Purity to use to resolve hostnames to IP addresses. Enter one IP address in each DNS# field. Purity queries the DNS servers in the order that the IP addresses are listed.
4. Click Save.

iSCSI Interface Configuration

The iSCSI traffic will be carried on two VLANs, A (901) and B (902) that are configured in our example with the following values:

Table 12 iSCSI A FlashArray//X70 R2 Interface Configuration Settings

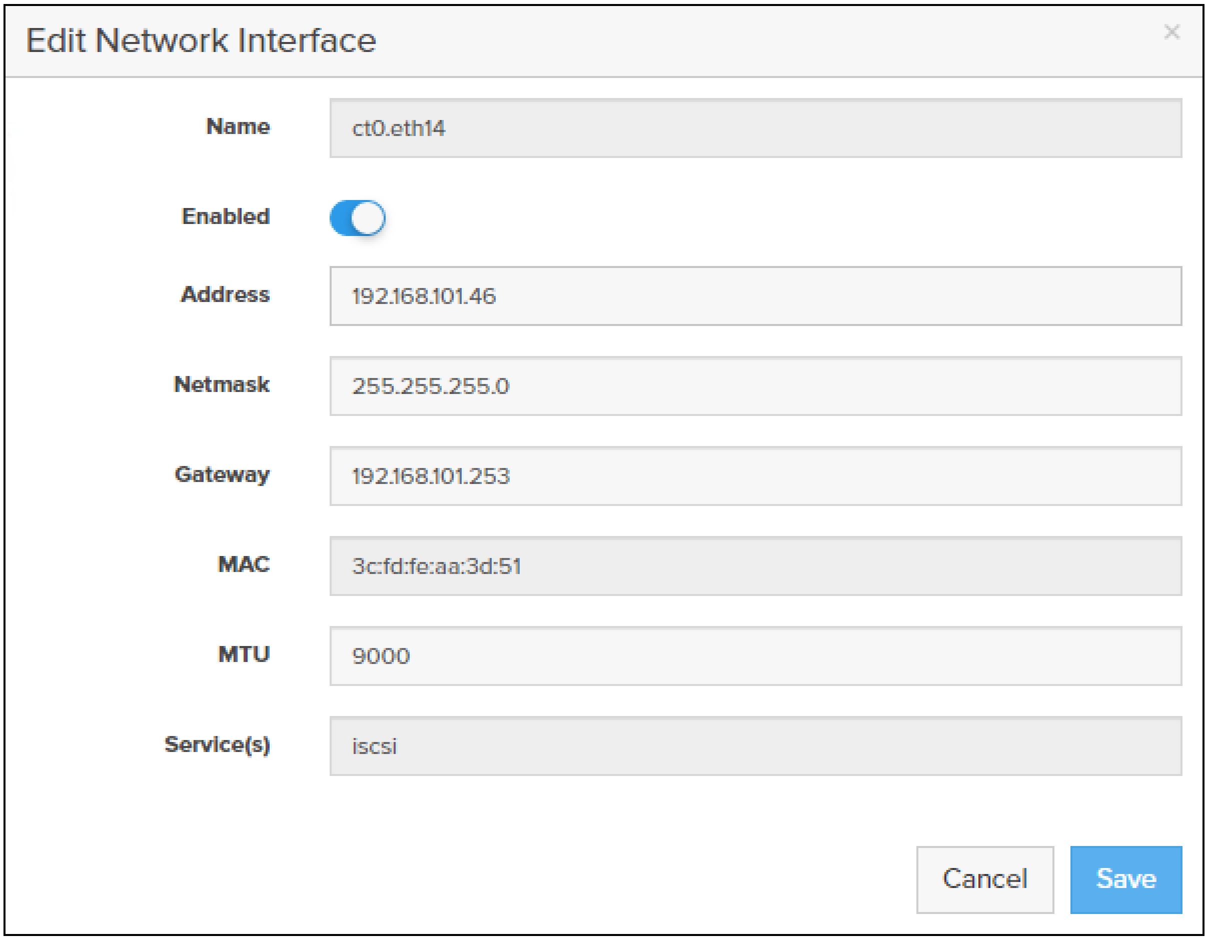
Device	Interface	IP	Netmask
FlashArray//X70 R2 Controller 0	CT0.ETH14	192.168.101.46	255.255.255.0
FlashArray//X70 R2 Controller 1	CT1.ETH14	192.168.101.47	255.255.255.0

Table 13 iSCSI B FlashArray//X70 R2 Interface Configuration Settings

Device	Interface	IP	Netmask
FlashArray//X70 R2 Controller 0	CT0.ETH15	192.168.102.46	255.255.255.0
FlashArray//X70 R2 Controller 1	CT1.ETH15	192.168.102.47	255.255.255.0

To configure iSCSI interfaces for environments deploying iSCSI boot LUNs and/or datastores, follow these steps:

1. Select Settings > Network.
2. Click the ✎.
3. Select the Enabled check mark box within the Edit Network Interface dialogue window, enter the Address and Netmask from Table 12, and set the MTU to 9000 to enable jumbo frames.



Edit Network Interface

Name: ct0.eth14

Enabled: ●

Address: 192.168.101.46

Netmask: 255.255.255.0

Gateway: 192.168.101.253

MAC: 3c:fd:fe:aa:3d:51

MTU: 9000

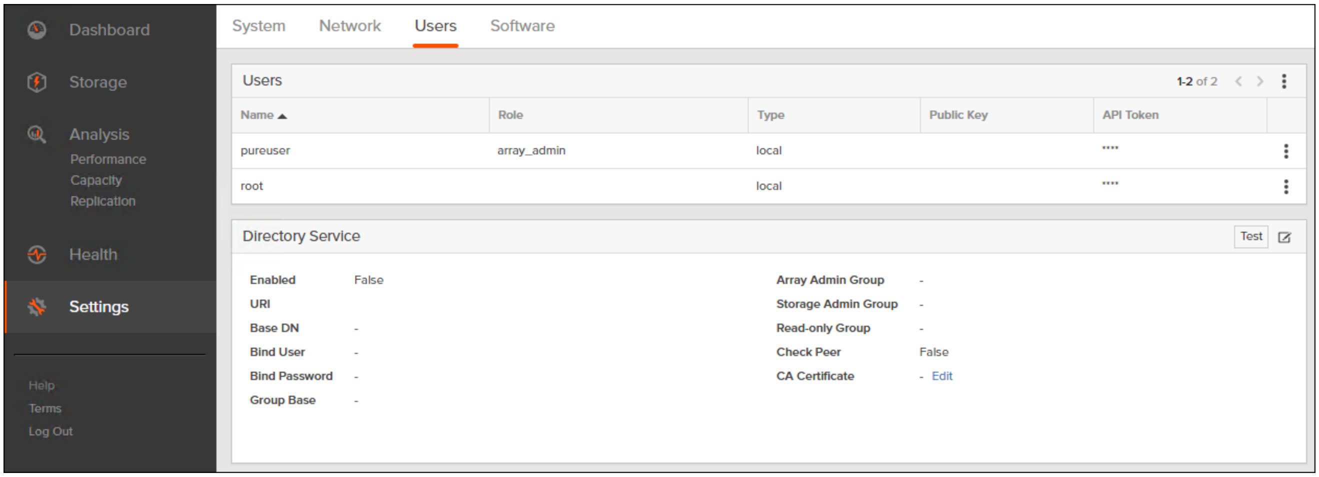
Service(s): iscsi

4. Click Save.

5. Repeat steps 1-4 for ct0.eth15, ct1.eth14, and ct1.eth15 using values from Table 12 and Table 13.

Directory Service Sub-view

The Directory Service sub-view manages the integration of FlashArray with an existing directory service. When the Directory Service sub-view is configured and enabled, the FlashArray leverages a directory service to perform user account and permission level searches. Configuring directory services is OPTIONAL.



Users

Name ▲	Role	Type	Public Key	API Token
pureuser	array_admin	local		****
root		local		****

Directory Service

Enabled	False	Array Admin Group	-
URI		Storage Admin Group	-
Base DN	-	Read-only Group	-
Bind User	-	Check Peer	False
Bind Password	-	CA Certificate	- Edit
Group Base	-		

The FlashArray is delivered with a single local user, named pureuser, with array-wide (Array Admin) permissions.

To support multiple FlashArray users, integrate the array with a directory service, such as Microsoft Active Directory or OpenLDAP.

Role-based access control is achieved by configuring groups in the directory that correspond to the following permission groups (roles) on the array:

- Read Only Group. Read Only users have read-only privilege to run commands that convey the state of the array. Read Only uses cannot alter the state of the array.
- Storage Admin Group. Storage Admin users have all the privileges of Read Only users, plus the ability to run commands related to storage operations, such as administering volumes, hosts, and host groups. Storage Admin users cannot perform operations that deal with global and system configurations.
- Array Admin Group. Array Admin users have all the privileges of Storage Admin users, plus the ability to perform array-wide changes. In other words, Array Admin users can perform all FlashArray operations.

To configure and enable the Directory Service sub-view, follow these steps:

1. Select Settings > Users.
2. Select the ✎ icon in the Directory Services panel:
   a. **Enabled**: Select the check box to leverage the directory service to perform user account and permission level searches.
   b. **URI**: Enter the comma-separated list of up to 30 URIs of the directory servers. The URI must include a URL scheme (ldap, or ldaps for LDAP over SSL), the hostname, and the domain. You can optionally specify a port. For example, ldap://ad.company.com configures the directory service with the hostname "ad" in the domain "company.com" while specifying the unencrypted LDAP protocol.
   c. **Base DN**: Enter the base distinguished name (DN) of the directory service. The Base DN is built from the domain and should consist only of domain components (DCs). For example, for ldap://ad.storage.company.com, the Base DN would be: “DC=storage,DC=company,DC=com”
   d. **Bind User**: Username used to bind to and query the directory. For Active Directory, enter the username - often referred to as sAMAccountName or User Logon Name - of the account that is used to perform directory lookups. The username cannot contain the characters " [ ] : ; | = + * ? < > / \ and cannot exceed 20 characters in length. For OpenLDAP, enter the full DN of the user. For example, "CN=John,OU=Users,DC=example,DC=com".

e. **Bind Password**: Enter the password for the bind user account.

f. **Group Base**: Enter the organizational unit (OU) to the configured groups in the directory tree. The Group Base consists of OUs that, when combined with the base DN attribute and the configured group CNs, complete the full Distinguished Name of each groups. The group base should specify "OU=" for each OU and multiple OUs should be separated by commas. The order of OUs should get larger in scope from left to right. In the following example, SANManagers contains the sub-organizational unit PureGroups: "OU=PureGroups,OU=SANManagers".

g. **Array Admin Group**: Common Name (CN) of the directory service group containing administrators with full privileges to manage the FlashArray. Array Admin Group administrators have the same privileges as pureuser. The name should be the Common Name of the group without the "CN=" specifier. If the configured groups are not in the same OU, also specify the OU. For example, "pureadmins,OU=PureStorage", where pureadmins is the common name of the directory service group.

h. **Storage Admin Group**: Common Name (CN) of the configured directory service group containing administrators with storage related privileges on the FlashArray. The name should be the Common Name of the group without the "CN=" specifier. If the configured groups are not in the same OU, also specify the OU. For example, "pureusers,OU=PureStorage", where pureusers is the common name of the directory service group.

i. **Read Only Group**: Common Name (CN) of the configured directory service group containing users with read-only privileges on the FlashArray. The name should be the Common Name of the group without the "CN=" specifier. If the configured groups are not in the same OU, also specify the OU. For example, "purereadonly,OU=PureStorage", where purereadonly is the common name of the directory service group.

j. **Check Peer**: Select the check box to validate the authenticity of the directory servers using the CA Certificate. If you enable Check Peer, you must provide a CA Certificate.

k. **CA Certificate**: Enter the certificate of the issuing certificate authority. Only one certificate can be configured at a time, so the same certificate authority should be the issuer of all directory server certificates. The certificate must be PEM formatted (Base64 encoded) and include the "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines. The certificate cannot exceed 3000 characters in total length.

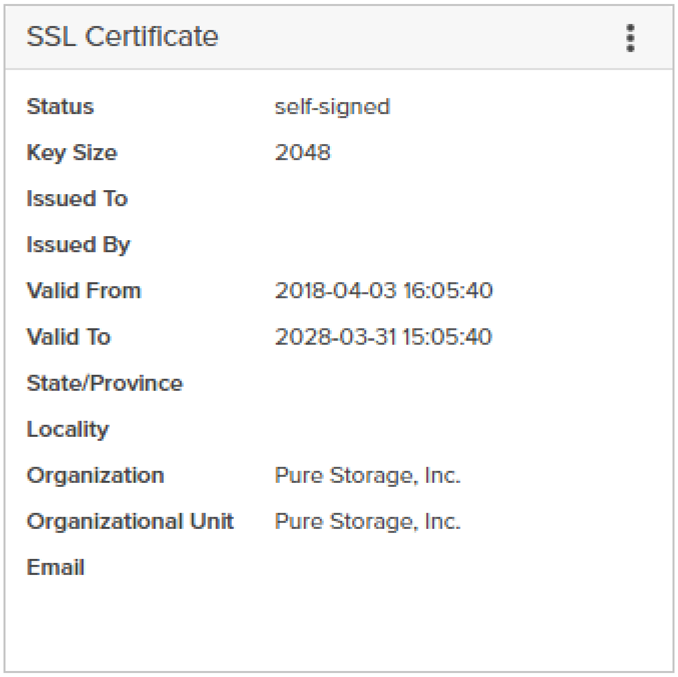
3. Click Save.

4. Click Test to test the configuration settings. The LDAP Test Results pop-up window appears. Green squares represent successful checks. Red squares represent failed checks.

SSL Certificate Sub-view

Purity creates a self-signed certificate and private key when you start the system for the first time. The SSL Certificate sub-view allows you to view and change certificate attributes, create a new self-signed certificate, construct certificate signing requests, import certificates and private keys, and export certificates.

Creating a self-signed certificate replaces the current certificate. When you create a self-signed certificate, include any attribute changes, specify the validity period of the new certificate, and optionally generate a new private key.



SSL Certificate

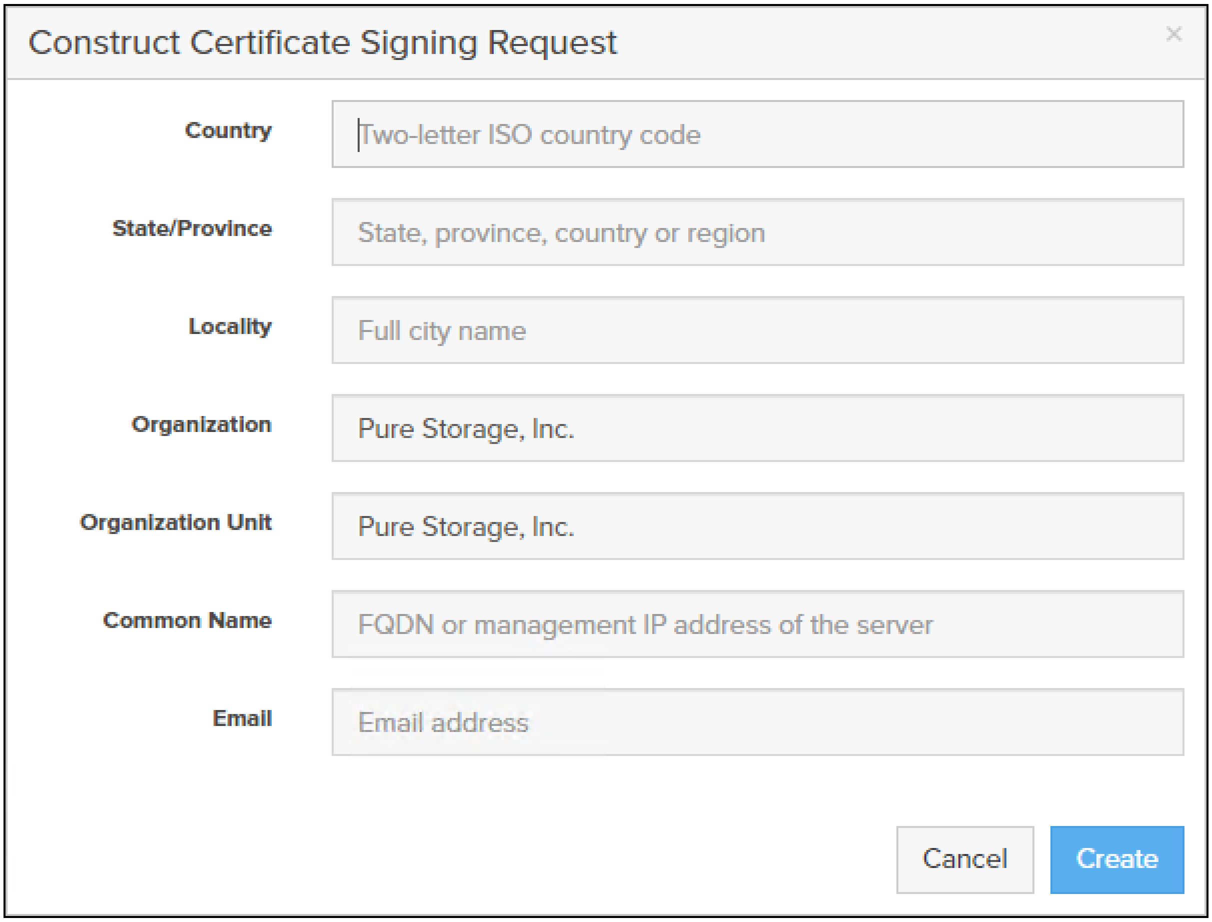
Status	self-signed
Key Size	2048
Issued To	
Issued By	
Valid From	2018-04-03 16:05:40
Valid To	2028-03-31 15:05:40
State/Province	
Locality	
Organization	Pure Storage, Inc.
Organizational Unit	Pure Storage, Inc.
Email	

When you create the self-signed certificate, you can generate a private key and specify a different key size. If you do not generate a private key, the new certificate uses the existing key.

You can change the validity period of the new self-signed certificate. By default, self-signed certificates are valid for 3650 days

CA-Sign Certificate

Certificate Authorities (CA) are third party entities outside the organization that issue certificates. To obtain a CA certificate, you must first construct a certificate signing request (CSR) on the array.

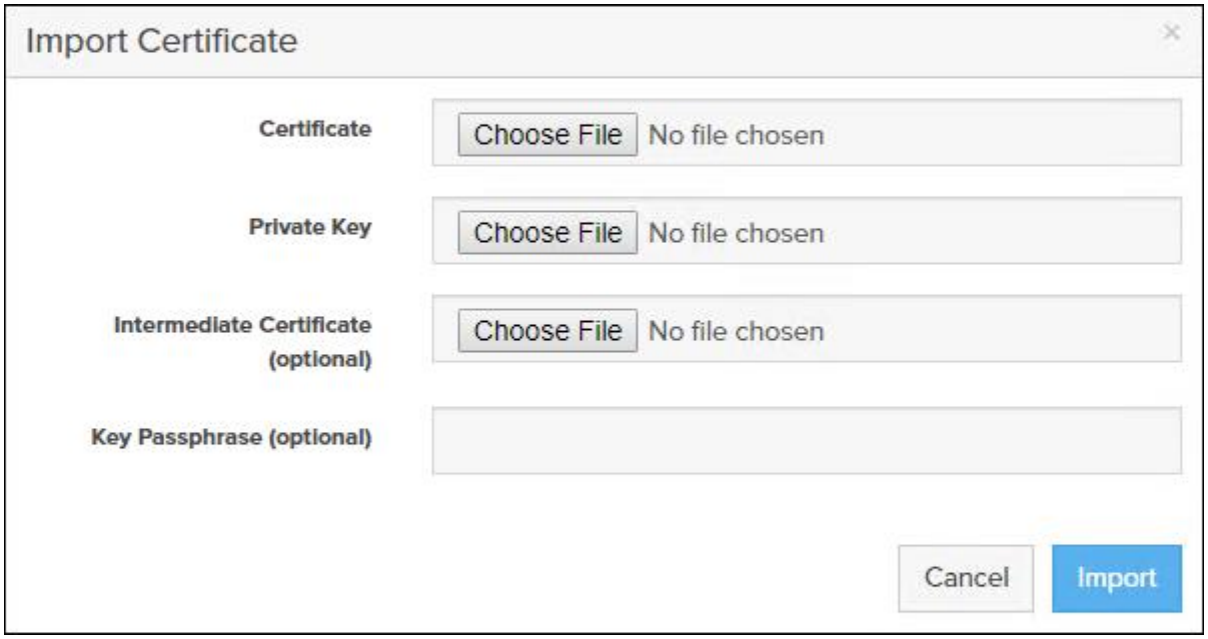


Construct Certificate Signing Request

Country	Two-letter ISO country code
State/Province	State, province, country or region
Locality	Full city name
Organization	Pure Storage, Inc.
Organization Unit	Pure Storage, Inc.
Common Name	FQDN or management IP address of the server
Email	Email address

The CSR represents a block of encrypted data specific to your organization. You can change the certificate attributes when you construct the CSR; otherwise, Purity will reuse the attributes of the current certificate (self-signed or imported) to construct the new one. Note that the certificate attribute changes will only be visible after you import the signed certificate from the CA.

Send the CSR to a certificate authority for signing. The certificate authority returns the SSL certificate for you to import. Verify that the signed certificate is PEM formatted (Base64 encoded), includes the "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines, and does not exceed 3000 characters in total length. When you import the certificate, also import the intermediate certificate if it is not bundled with the CA certificate.



Import Certificate

Certificate: No file chosen

Private Key: No file chosen

Intermediate Certificate (optional): No file chosen

Key Passphrase (optional):

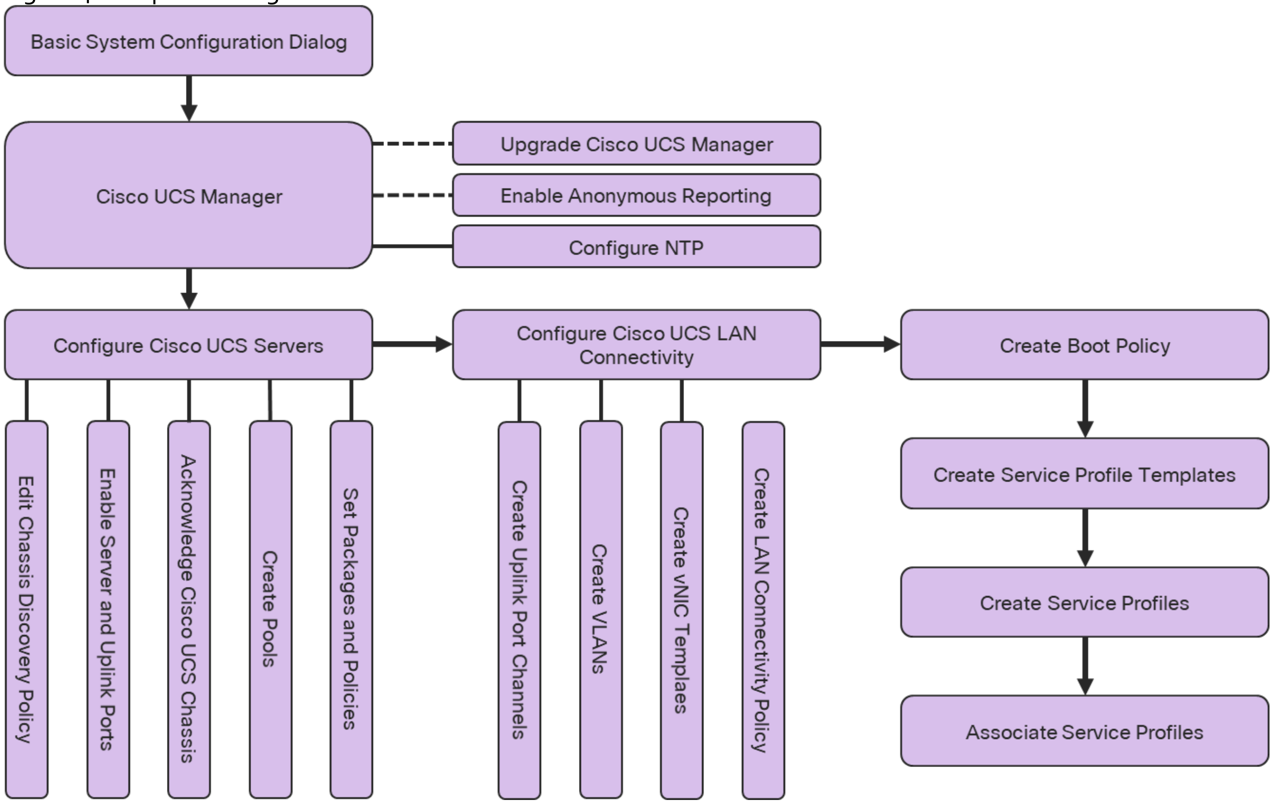
If the certificate is signed with the CSR that was constructed on the current array and you did not change the private key, you do not need to import the key. However, if the CSR was not constructed on the current array or if the private key has changed since you constructed the CSR, you must import the private key. If the private key is encrypted, also specify the passphrase.

Compute Configuration

Cisco UCS Compute Configuration

The following procedures describe how to configure the Cisco UCS domain for use in a base FlashStack environment. This procedure assumes the use of UCS Fabric Interconnects running 4.0(2b). Configuration on a different model of Cisco UCS Fabric Interconnects should be comparable but may differ slightly with model and changes in the UCSM release. The Cisco USC 6454 Fabric Interconnects and Cisco UCS Manger 4.0(2b) release were used in validation of this FlashStack solution, so the steps will reflect this model and release.

Figure 4 Compute Configuration Workflow



Basic System Configuration Dialog
Cisco UCS Manager
Upgrade Cisco UCS Manager
Enable Anonymous Reporting
Configure NTP
Configure Cisco UCS Servers
Configure Cisco UCS LAN Connectivity
Create Boot Policy
Edit Chassis Discovery Policy
Enable Server and Uplink Ports
Acknowledge Cisco UCS Chassis
Create Pools
Set Packages and Policies
Create Uplink Port Channels
Create VLANs
Create vNIC Templaes
Create LAN Connectivity Policy
Create Service Profile Templates
Create Service Profiles
Associate Service Profiles

Physical Connectivity

Physical cabling should be completed by following the diagram and table references in the previous section referenced as FlashStack Cabling.

Cisco UCS Basic System Configuration Dialog

This section provides detailed instructions for the configuration of the Cisco UCS 6454 Fabric Interconnects used in this FlashStack solution. Some changes may be appropriate for a customer's environment, but care should be taken when stepping outside of these instructions as it may lead to an improper configuration.

To start on the configuration of the Fabric Interconnect A, connect to the console of the fabric interconnect and step through the Basic System Configuration Dialogue:

```
UCSM image signature verification successful

           ---- Basic System Configuration Dialog ----

  This setup utility will guide you through the basic configuration of
  the system. Only minimal configuration including IP connectivity to
  the Fabric interconnect and its clustering mode is performed through these steps.

  Type Ctrl-C at any time to abort configuration and reboot system.
  To back track or make modifications to already entered values,
  complete input till end of section and answer no when prompted
  to apply configuration.

  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]: y
  Enter the password for "admin":
  Confirm the password for "admin":

  Is this Fabric interconnect part of a cluster(select 'no' for standalone)? (yes/no) [n]:
yes
  Enter the switch fabric (A/B) []: A
  Enter the system name:  <var_ucs_clustername>>
  Physical Switch Mgmt0 IP address : <<var_ucs_a_mgmt_ip>>
  Physical Switch Mgmt0 IPv4 netmask : <<var_oob_mgmt_mask>>
  IPv4 address of the default gateway : <<var_oob_gateway>>

  Cluster IPv4 address : <<var_ucs_mgmt_vip>
  Configure the DNS Server IP address? (yes/no) [n]: yes
    DNS IP address : <<var_nameserver_ip>>
  Configure the default domain name? (yes/no) [n]: yes
    Default domain name : <<var_dns_domain_name>>

  Join centralized management environment (UCS Central)? (yes/no) [n]: no
  Following configurations will be applied:
    Switch Fabric=A
    System Name=AA12-UCS-6454
    Enforced Strong Password=yes
    Physical Switch Mgmt0 IP Address=10.2.164.51
    Physical Switch Mgmt0 IP Netmask=255.255.255.0
    Default Gateway=10.2.164.254
    Ipv6 value=0
    DNS Server=10.1.164.9
    Domain Name=flashstack.cisco.com

    Cluster Enabled=yes
    Cluster IP Address=10.2.164.50
    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
```

Continue the configuration on the console of the Fabric Interconnect B:

```
---- Basic System Configuration Dialog ----

  This setup utility will guide you through the basic configuration of
  the system. Only minimal configuration including IP connectivity to
  the Fabric interconnect and its clustering mode is performed through these steps.

  Type Ctrl-C at any time to abort configuration and reboot system.
  To back track or make modifications to already entered values,
  complete input till end of section and answer no when prompted
  to apply configuration.
  Enter the configuration method. (console/gui) ? console

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

  Enter the admin password of the peer Fabric interconnect:
    Connecting to peer Fabric interconnect... done
    Retrieving config from peer Fabric interconnect... done
    Peer Fabric interconnect Mgmt0 IPv4 Address: 10.2.164.51
    Peer Fabric interconnect Mgmt0 IPv4 Netmask: 255.255.255.0
    Cluster IPv4 address          : 10.2.164.50

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

  Physical Switch Mgmt0 IP address : <<var_ucs_b_mgmt_ip>>

  Local fabric interconnect model(UCS-FI-6454)
  Peer fabric interconnect is compatible with the local fabric interconnect. Continuing with the install-
er...

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

Cisco UCS Manager Configuration

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

1. Open a web browser and navigate to the Cisco UCS fabric interconnect cluster address.
2. Click the Launch UCS Manager link within the opening page.
3. If prompted to accept security certificates, accept as necessary.
4. When the UCS Manager login is prompted, enter admin as the user name and enter the administrative password.
5. Click Login to log in to Cisco UCS Manager.

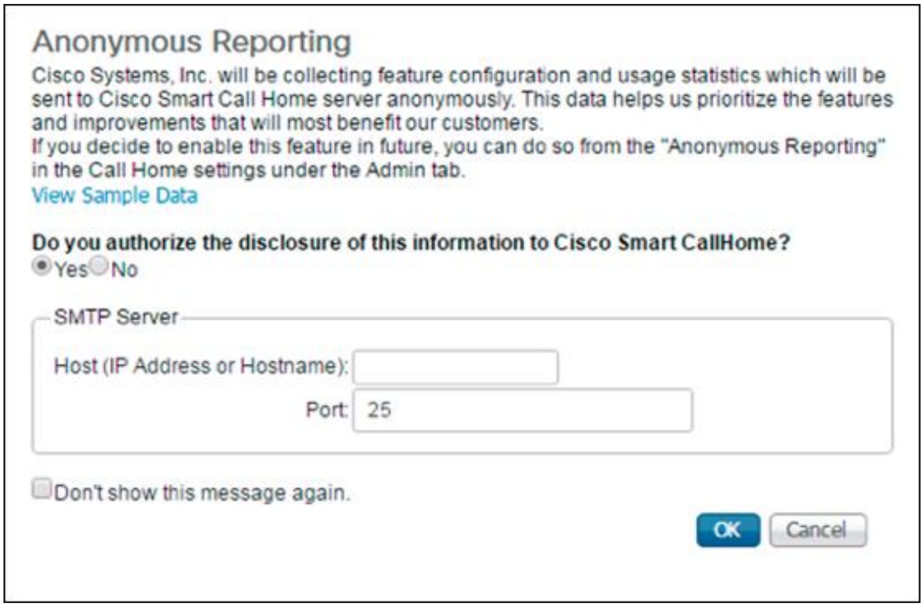
Upgrade Cisco UCS Manager to Version 4.0(2b)

This document assumes the use of Cisco UCS 4.0(2b). To upgrade the Cisco UCS Manager software and the Cisco UCS Fabric Interconnect software to version 4.0(2b), refer to Cisco UCS Manager Install and Upgrade Guides.

Enable Anonymous Reporting

During the first connection to the Cisco UCS Manager GUI, a pop-up window will appear to allow for the configuration of Anonymous Reporting to Cisco on use to help with future development. To create anonymous reporting, complete the following step:

1. In the Anonymous Reporting window, select whether to send anonymous data to Cisco for improving future products, and provide the appropriate SMTP server gateway information if configuring:



Anonymous Reporting

Cisco Systems, Inc. will be collecting feature configuration and usage statistics which will be sent to Cisco Smart Call Home server anonymously. This data helps us prioritize the features and improvements that will most benefit our customers.
If you decide to enable this feature in future, you can do so from the "Anonymous Reporting" in the Call Home settings under the Admin tab.

View Sample Data

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

● Yes ○ No

SMTP Server

Host (IP Address or Hostname):

Port: 25

□ Don't show this message again.

If you want to enable or disable Anonymous Reporting at a later date, it can be found within Cisco UCS Manager under: **Admin** -> **Communication Management** -> **Call Home**, which has a tab on the far right for **Anonymous Reporting**.

Configure Cisco UCS Call Home

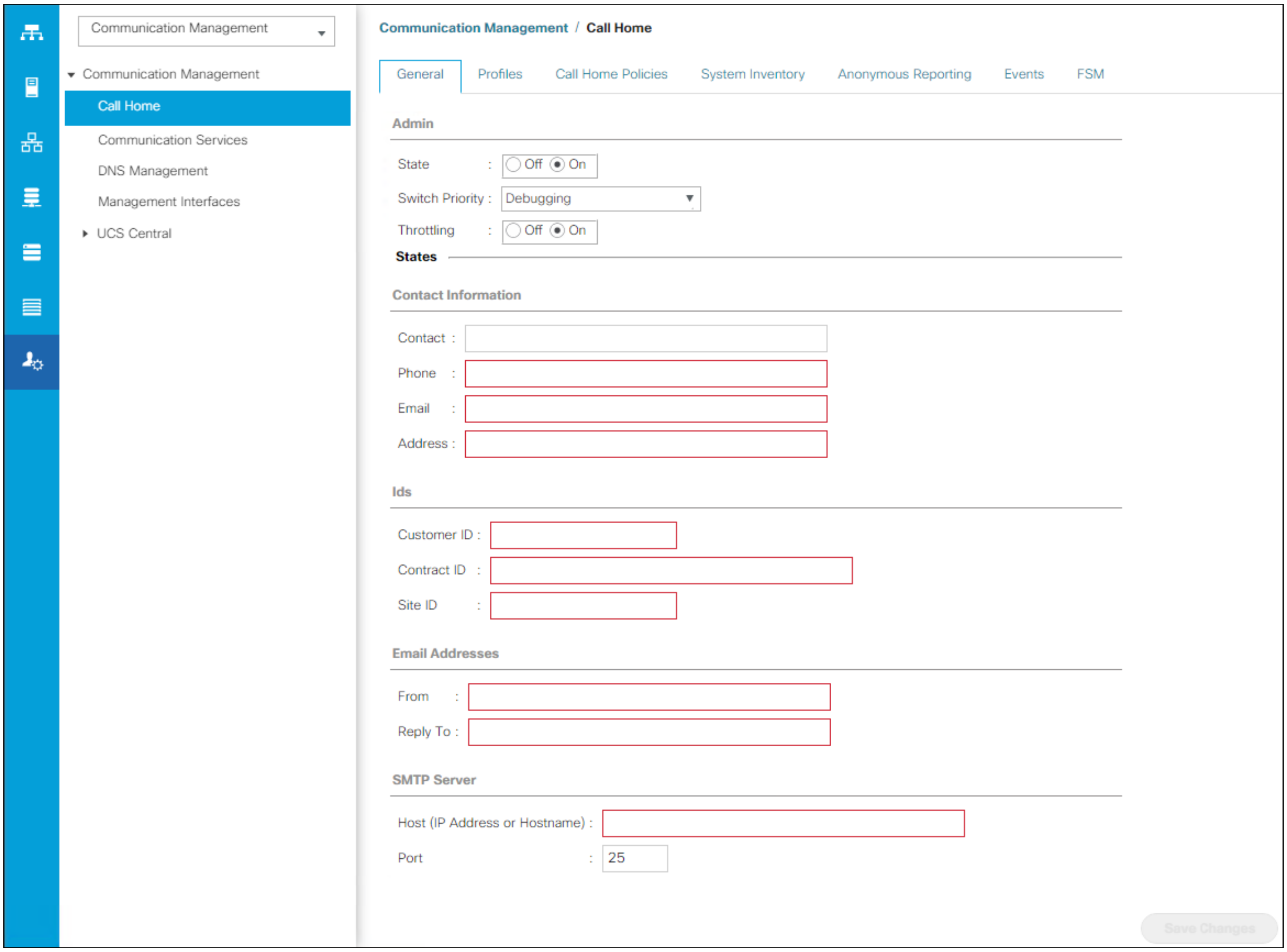
During the first connection to the Cisco UCS Manager GUI, a pop-up window will appear to allow for the configuration of Anonymous Reporting to Cisco on use to help with future development. To create anonymous reporting, follow these steps:

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

2. Expand Communication Management and click Call Home

3. Change State to On.

4. Fill in the fields according to your preferences and click Save Changes and OK



Communication Management / Call Home

Admin

State : ○ Off ● On

Switch Priority : Debugging

Throttling : ○ Off ● On

States

Contact Information

Contact :

Phone :

Email :

Address :

Ids

Customer ID :

Contract ID :

Site ID :

Email Addresses

From :

Reply To :

SMTP Server

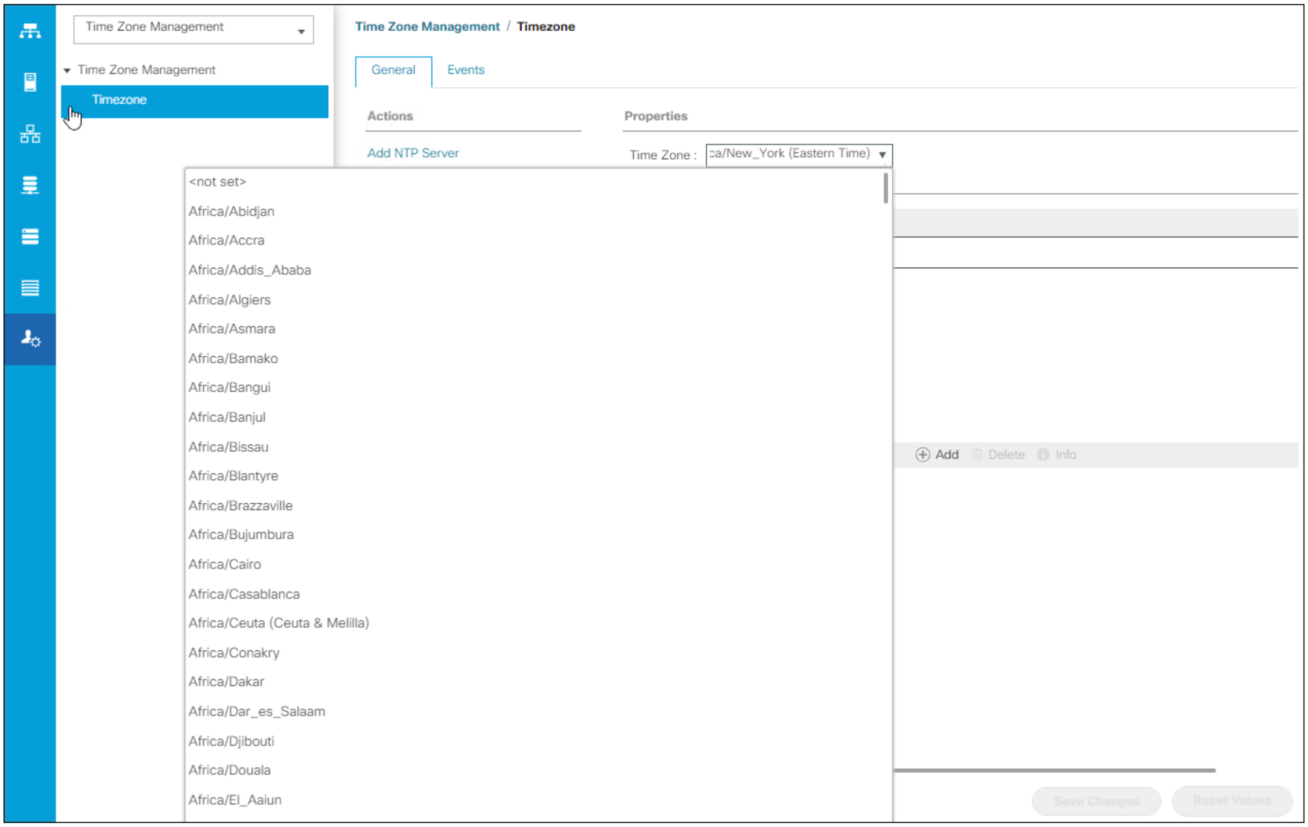
Host (IP Address or Hostname) :

Port : 25

Configure NTP

To synchronize the Cisco UCS environment to the NTP server, follow these steps:

1. In Cisco UCS Manager, click the Admin tab in the navigation pane.
2. Expand Timezone Management and click Timezone.



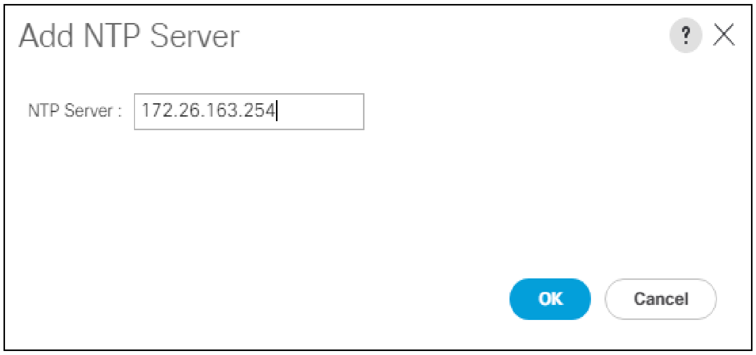
Time Zone : ca/New_York (Eastern Time)

3. In the Properties pane, select the appropriate time zone in the Timezone menu.

4. Click Save Changes and then click OK.

5. Click Add NTP Server.

6. Enter <<var_oob_ntp>> and click OK.



NTP Server : 172.26.163.254

7. Click OK.

Configure Cisco UCS Servers

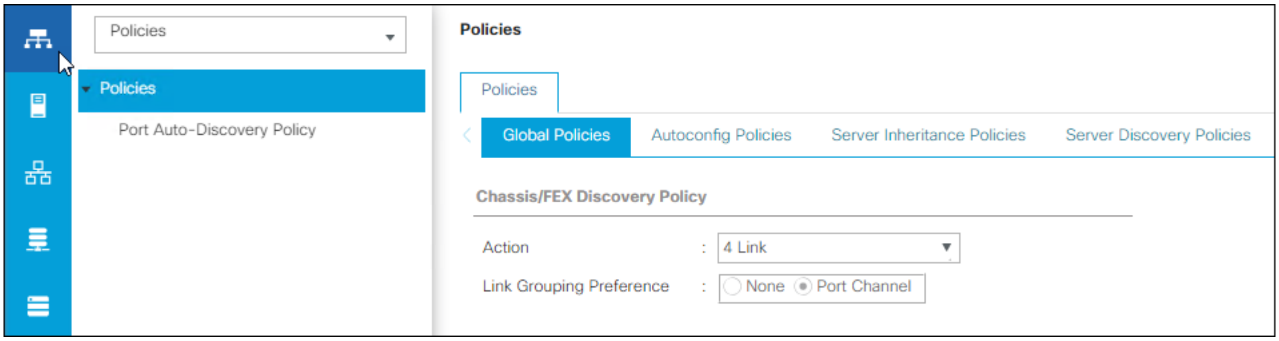
Edit Chassis Discovery Policy

Setting the discovery policy simplifies the addition of B-Series Cisco UCS chassis. To modify the chassis discovery policy, follow these steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane and select Policies in the list under the drop-down.

2. Under Global Policies, set the Chassis/FEX Discovery Policy to match the number of uplink ports that are cabled between the chassis or fabric extenders (FEXes) and the fabric interconnects.

3. Set the Link Grouping Preference to Port Channel.


Policies
Policies
Port Auto-Discovery Policy
Policies
Policies
Global Policies
Autoconfig Policies
Server Inheritance Policies
Server Discovery Policies

Chassis/FEX Discovery Policy

Action : 4 Link

Link Grouping Preference : ○ None ● Port Channel

4. Leave other settings alone or change if appropriate to your environment.

5. Click Save Changes.

6. Click OK.

Enable Server and Uplink Ports

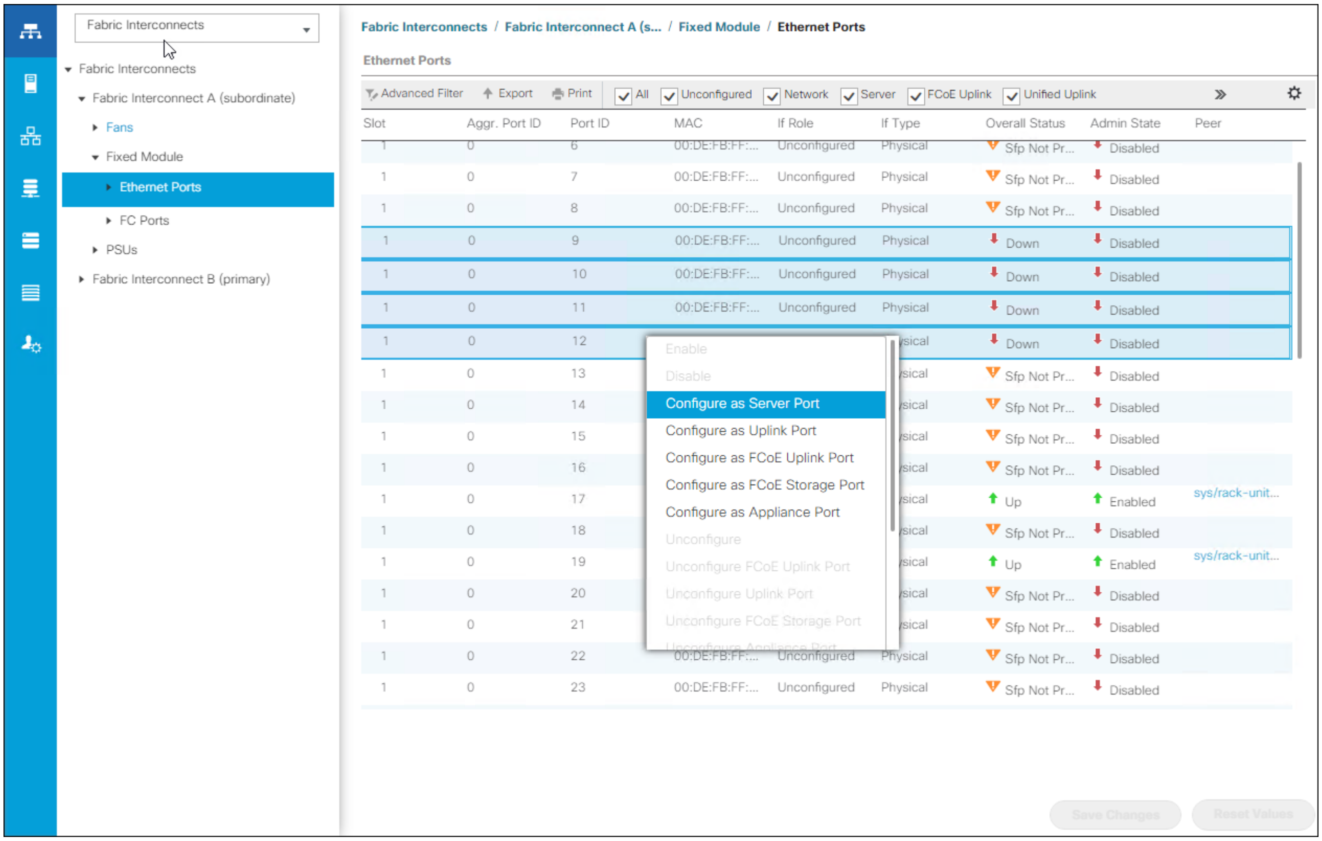
To enable server and uplink ports, follow these steps:

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

2. Select Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Fixed Module.

3. Expand Ethernet Ports.

4. Select the ports that are connected to the chassis, right-click them, and select "Configure as Server Port."

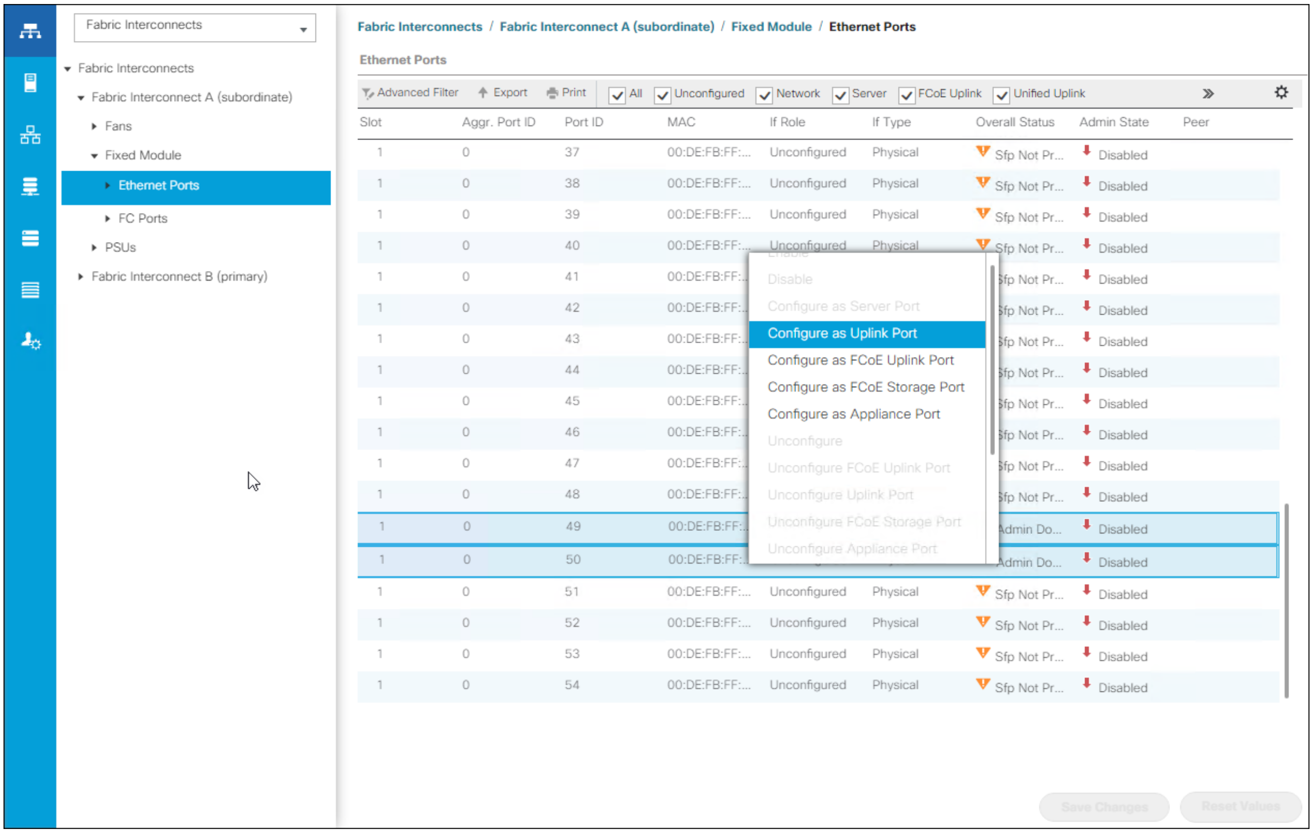

Fabric Interconnects
Fabric Interconnects
Fabric Interconnect A (subordinate)
Fans
Fixed Module
Ethernet Ports
FC Ports
PSUs
Fabric Interconnect B (primary)
Fabric Interconnects / Fabric Interconnect A (s... / Fixed Module / Ethernet Ports
Ethernet Ports
Advanced Filter
Export
Print
☑ All
☑ Unconfigured
☑ Network
☑ Server
☑ FCoE Uplink
☑ Unified Uplink
Enable
Disable
Configure as Server Port
Configure as Uplink Port
Configure as FCoE Uplink Port
Configure as FCoE Storage Port
Configure as Appliance Port
Unconfigure
Unconfigure FCoE Uplink Port
Unconfigure Uplink Port
Unconfigure FCoE Storage Port
Unconfigure Appliance Port
Save Changes
Reset Values

Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status	Admin State	Peer
1	0	6	00:DE:FB:FF:...	Unconfigured	Physical	Sfp Not Pr...	Disabled	
1	0	7	00:DE:FB:FF:...	Unconfigured	Physical	Sfp Not Pr...	Disabled	
1	0	8	00:DE:FB:FF:...	Unconfigured	Physical	Sfp Not Pr...	Disabled	
1	0	9	00:DE:FB:FF:...	Unconfigured	Physical	Down	Disabled	
1	0	10	00:DE:FB:FF:...	Unconfigured	Physical	Down	Disabled	
1	0	11	00:DE:FB:FF:...	Unconfigured	Physical	Down	Disabled	
1	0	12			ysical	Down	Disabled	
1	0	13			sical	Sfp Not Pr...	Disabled	
1	0	14			sical	Sfp Not Pr...	Disabled	
1	0	15			sical	Sfp Not Pr...	Disabled	
1	0	16			sical	Sfp Not Pr...	Disabled	
1	0	17			sical	Up	Enabled	sys/rack-unit...
1	0	18			sical	Sfp Not Pr...	Disabled	
1	0	19			sical	Up	Enabled	sys/rack-unit...
1	0	20			sical	Sfp Not Pr...	Disabled	
1	0	21			sical	Sfp Not Pr...	Disabled	
1	0	22	00:DE:FB:FF:...	Unconfigured	Physical	Sfp Not Pr...	Disabled	
1	0	23	00:DE:FB:FF:...	Unconfigured	Physical	Sfp Not Pr...	Disabled	

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

6. Verify that the ports connected to the chassis are now configured as server ports.

7. Select ports 39 and 40 that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.


Fabric Interconnects
Fabric Interconnects
Fabric Interconnect A (subordinate)
Fans
Fixed Module
Ethernet Ports
FC Ports
PSUs
Fabric Interconnect B (primary)
Fabric Interconnects / Fabric Interconnect A (subordinate) / Fixed Module / Ethernet Ports
Ethernet Ports
Advanced Filter
Export
Print
All
Unconfigured
Network
Server
FCoE Uplink
Unified Uplink
Enable
Disable
Configure as Server Port
Configure as Uplink Port
Configure as FCoE Uplink Port
Configure as FCoE Storage Port
Configure as Appliance Port
Unconfigure
Unconfigure FCoE Uplink Port
Unconfigure Uplink Port
Unconfigure FCoE Storage Port
Unconfigure Appliance Port
Save Changes
Reset Values

Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status	Admin State	Peer
1	0	37	00:DE:FB:FF:...	Unconfigured	Physical	Sfp Not Pr...	Disabled	
1	0	38	00:DE:FB:FF:...	Unconfigured	Physical	Sfp Not Pr...	Disabled	
1	0	39	00:DE:FB:FF:...	Unconfigured	Physical	Sfp Not Pr...	Disabled	
1	0	40	00:DE:FB:FF:...	Unconfigured	Physical	Sfp Not Pr...	Disabled	
1	0	41	00:DE:FB:FF:			fp Not Pr...	Disabled	
1	0	42	00:DE:FB:FF:			fp Not Pr...	Disabled	
1	0	43	00:DE:FB:FF:			fp Not Pr...	Disabled	
1	0	44	00:DE:FB:FF:			fp Not Pr...	Disabled	
1	0	45	00:DE:FB:FF:			fp Not Pr...	Disabled	
1	0	46	00:DE:FB:FF:			fp Not Pr...	Disabled	
1	0	47	00:DE:FB:FF:			fp Not Pr...	Disabled	
1	0	48	00:DE:FB:FF:			fp Not Pr...	Disabled	
1	0	49	00:DE:FB:FF:			Admin Do...	Disabled	
1	0	50	00:DE:FB:FF:			Admin Do...	Disabled	
1	0	51	00:DE:FB:FF:...	Unconfigured	Physical	Sfp Not Pr...	Disabled	
1	0	52	00:DE:FB:FF:...	Unconfigured	Physical	Sfp Not Pr...	Disabled	
1	0	53	00:DE:FB:FF:...	Unconfigured	Physical	Sfp Not Pr...	Disabled	
1	0	54	00:DE:FB:FF:...	Unconfigured	Physical	Sfp Not Pr...	Disabled	

8. Click Yes to confirm uplink ports and click OK.

9. Select Equipment > Fabric Interconnects > Fabric Interconnect B (subordinate) > Fixed Module.

10. Expand Ethernet Ports.

11. Select the ports that are connected to the chassis, right-click them and select Configure as Server Port.

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

13. Select ports 39 and 40 that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.

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

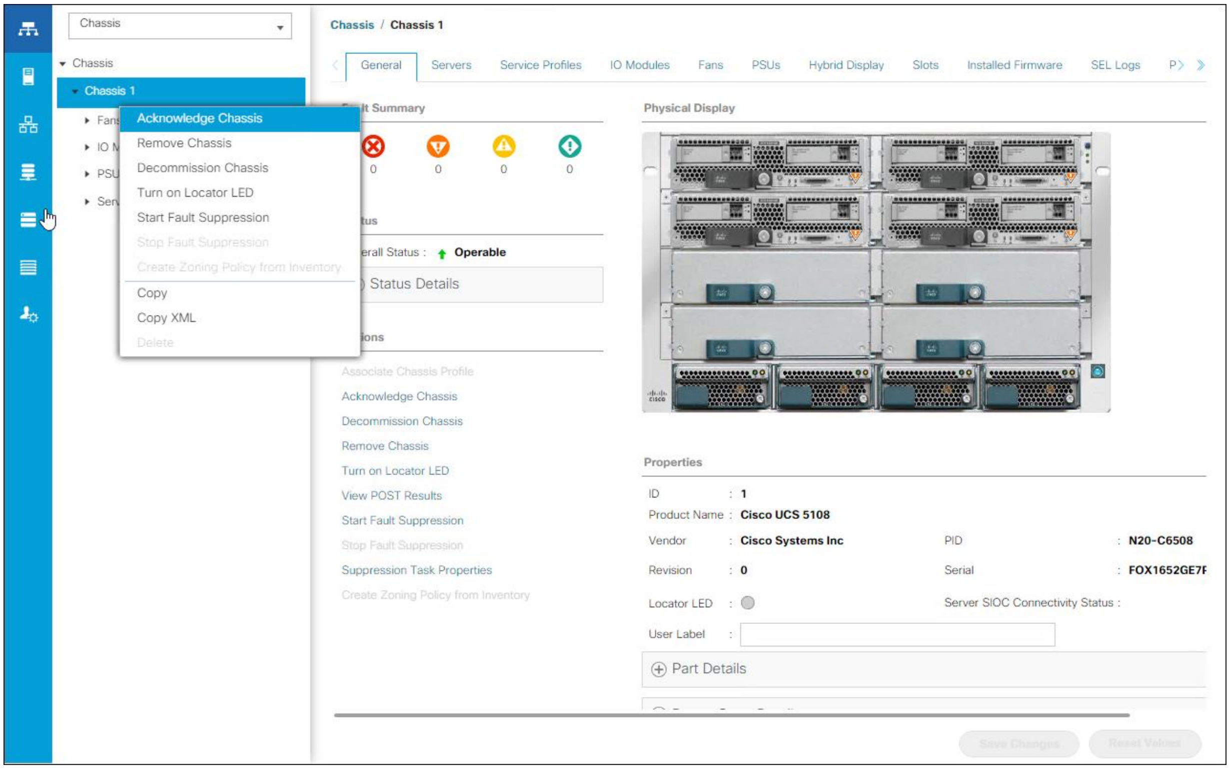
Acknowledge Cisco UCS Chassis

To acknowledge all Cisco UCS chassis, follow these steps:

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

2. Expand Chassis and select each chassis that is listed.

3. Right-click each chassis and select Acknowledge Chassis.



Overall Status : Operable

ID : 1
Product Name : Cisco UCS 5108
Vendor : Cisco Systems Inc
PID : N20-C6508
Revision : 0
Serial : FOX1652GE7F
Locator LED : ○
Server SIOC Connectivity Status :
User Label :

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

Create Pools

Create MAC Address Pools

To configure the necessary MAC address pools for the Cisco UCS environment, follow these steps:

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

2. Select Pools > root.

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

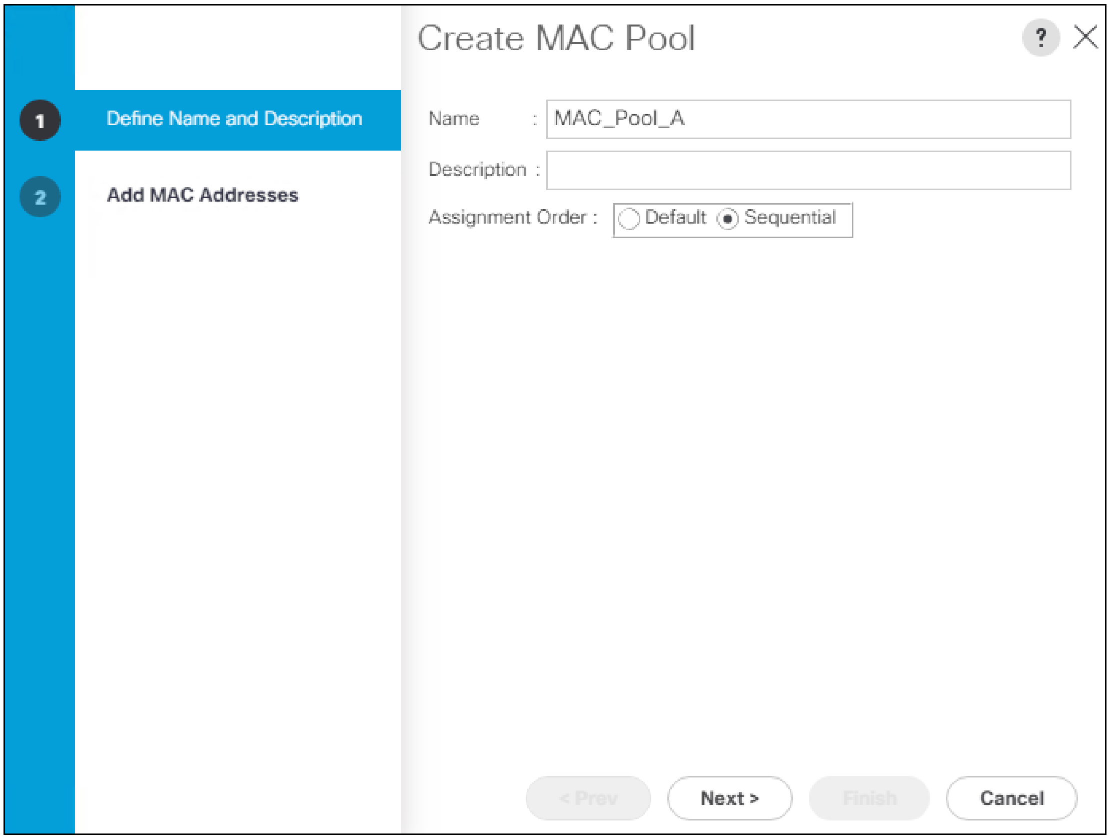
3. Right-click MAC Pools under the root organization.

4. Select Create MAC Pool to create the MAC address pool.

5. Enter MAC_Pool_A as the name of the MAC pool.

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

7. Select Sequential as the option for Assignment Order.



Name : MAC_Pool_A

Description :

Assignment Order : ○ Default ● Sequential

8. Click Next.

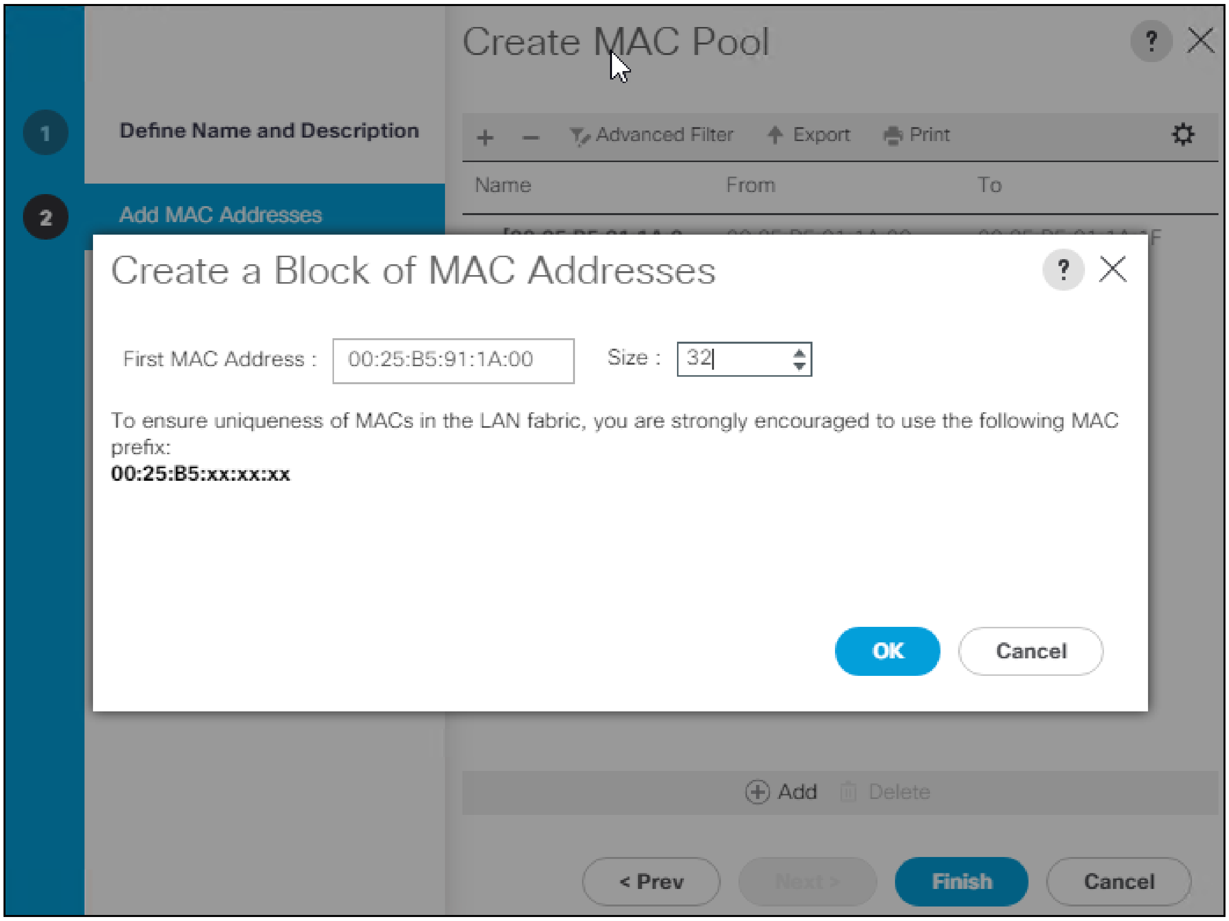
9. Click Add.

10. Specify a starting MAC address.

For Cisco UCS deployments, the recommendation is to place 0A in the next-to-last octet of the starting MAC address to identify all of the MAC addresses as fabric A addresses. In our example, we have carried forward the of also embedding the extra building, floor and Cisco UCS domain number information giving us `00:25:B5:91:1A:00` as our first MAC address.

---

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



Create a Block of MAC Addresses

First MAC Address : 00:25:B5:91:1A:00 Size : 32

To ensure uniqueness of MACs in the LAN fabric, you are strongly encouraged to use the following MAC prefix:
00:25:B5:xx:xx:xx

12. Click OK.

13. Click Finish.

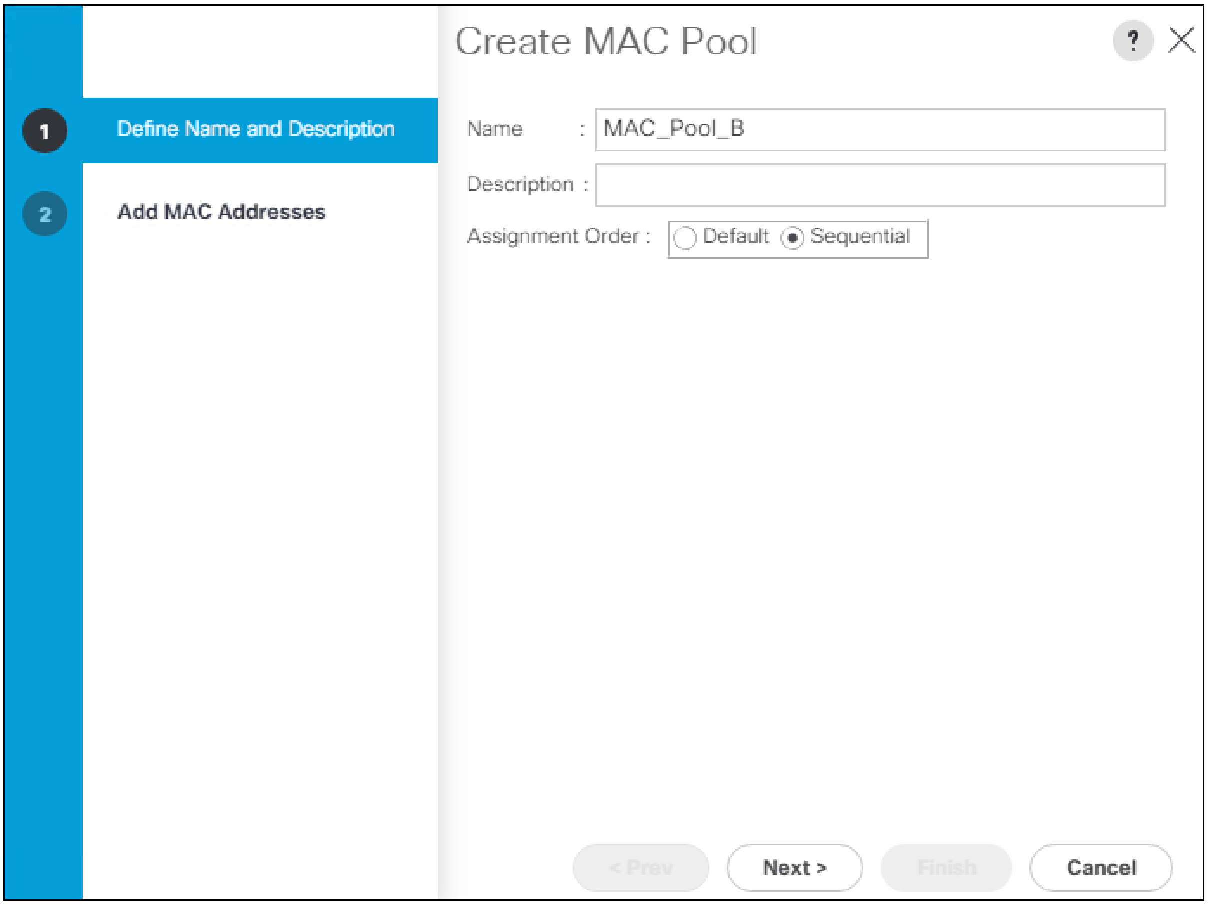
14. In the confirmation message, click OK.

15. Right-click MAC Pools under the root organization.

16. Select Create MAC Pool to create the MAC address pool.

17. Enter MAC_Pool_B as the name of the MAC pool.

18. Optional: Enter a description for the MAC pool.



Create MAC Pool

Name : MAC_Pool_B

Description :

Assignment Order : ○ Default ● Sequential

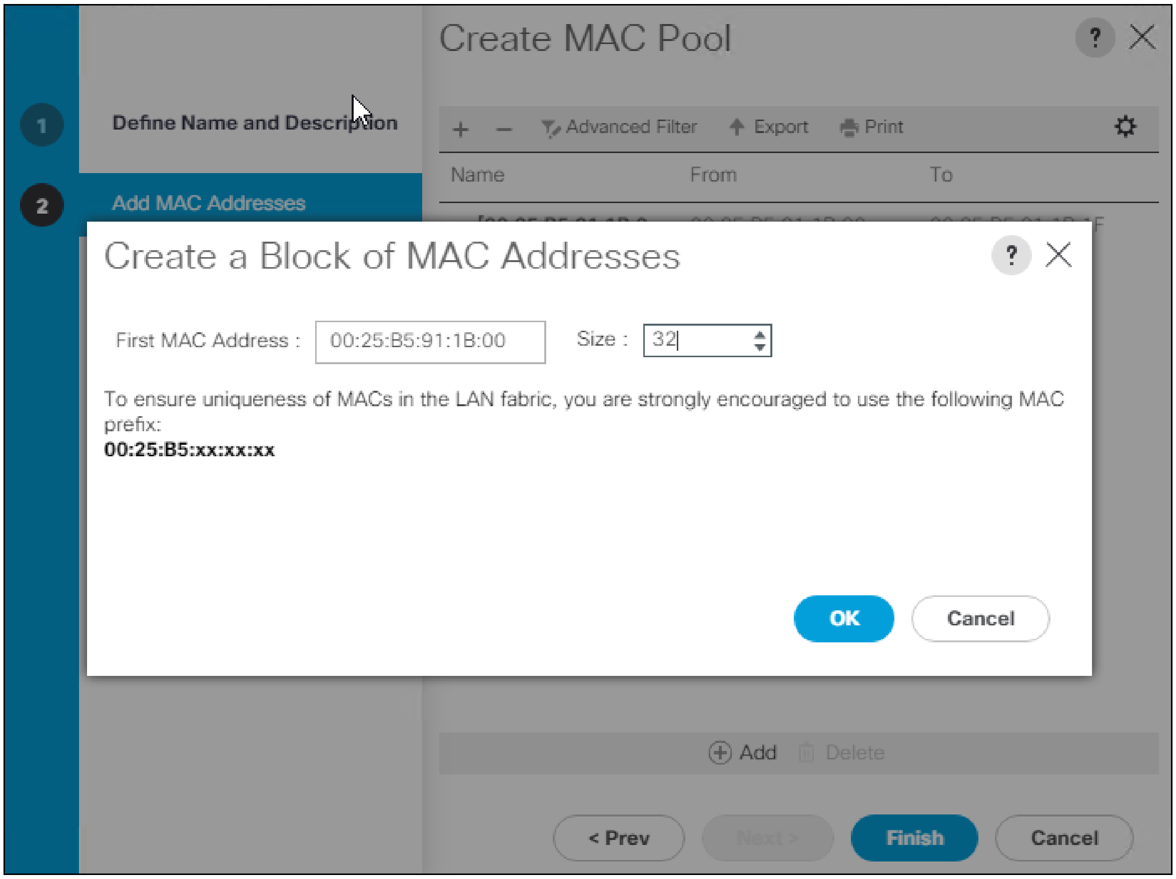
19. Click Next.

20. Click Add.

21. Specify a starting MAC address.

> For Cisco UCS deployments, the recommendation is to place 0B in the next-to-last octet of the starting MAC address to identify all of the MAC addresses as fabric B addresses. In our example, we have carried forward the of also embedding the extra building, floor and Cisco UCS domain number information giving us `00:25:B5:91:1B:00` as our first MAC address.

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


Create MAC Pool
1
Define Name and Description
2
Add MAC Addresses
+ − Advanced Filter Export Print
Name
From
To
Create a Block of MAC Addresses
OK
Cancel
Add Delete
< Prev
Next >
Finish
Cancel

First MAC Address : 00:25:B5:91:1B:00

Size : 32

To ensure uniqueness of MACs in the LAN fabric, you are strongly encouraged to use the following MAC prefix:
00:25:B5:xx:xx:xx

23. Click OK.

24. Click Finish.

25. In the confirmation message, click OK.

Create UUID Suffix Pool

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

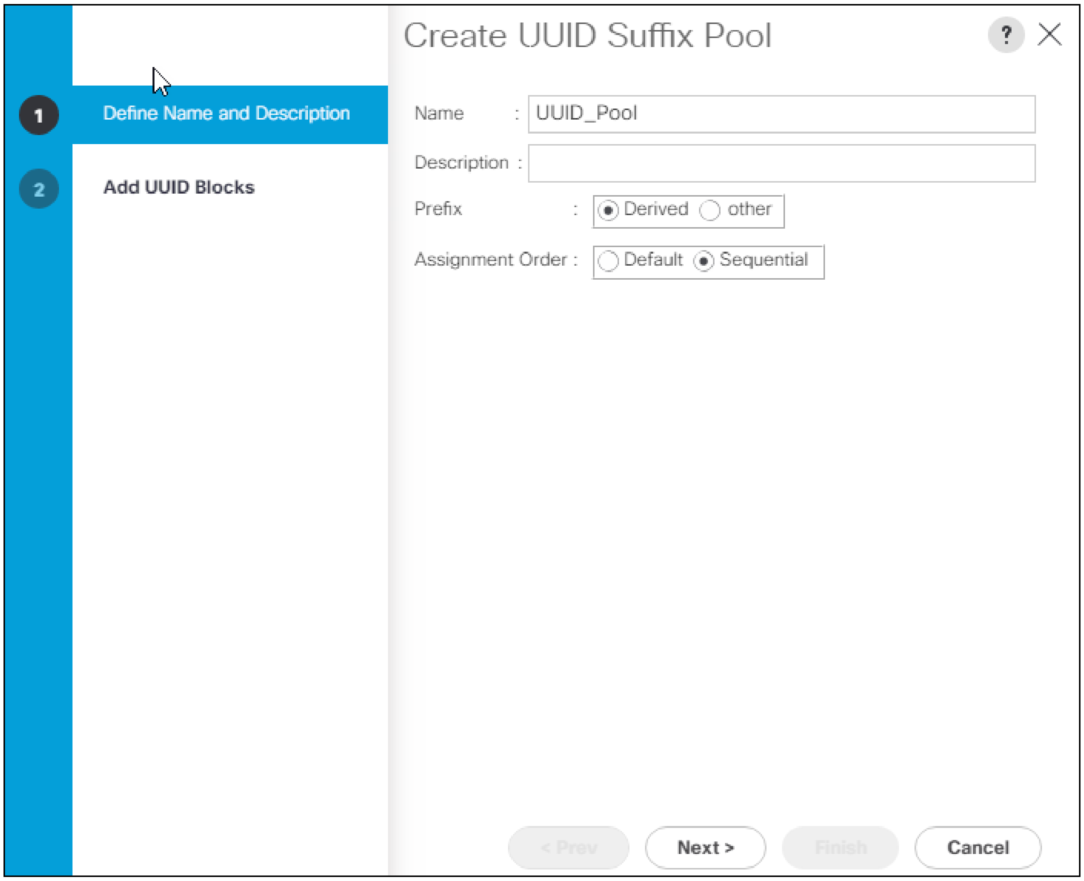
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.

2. Select Pools > root.

3. Right-click UUID Suffix Pools.

4. Select Create UUID Suffix Pool.

5. Enter UUID_Pool as the name of the UUID suffix pool.



Create UUID Suffix Pool

Name : UUID_Pool

Description :

Prefix : ● Derived ○ other

Assignment Order : ○ Default ● Sequential

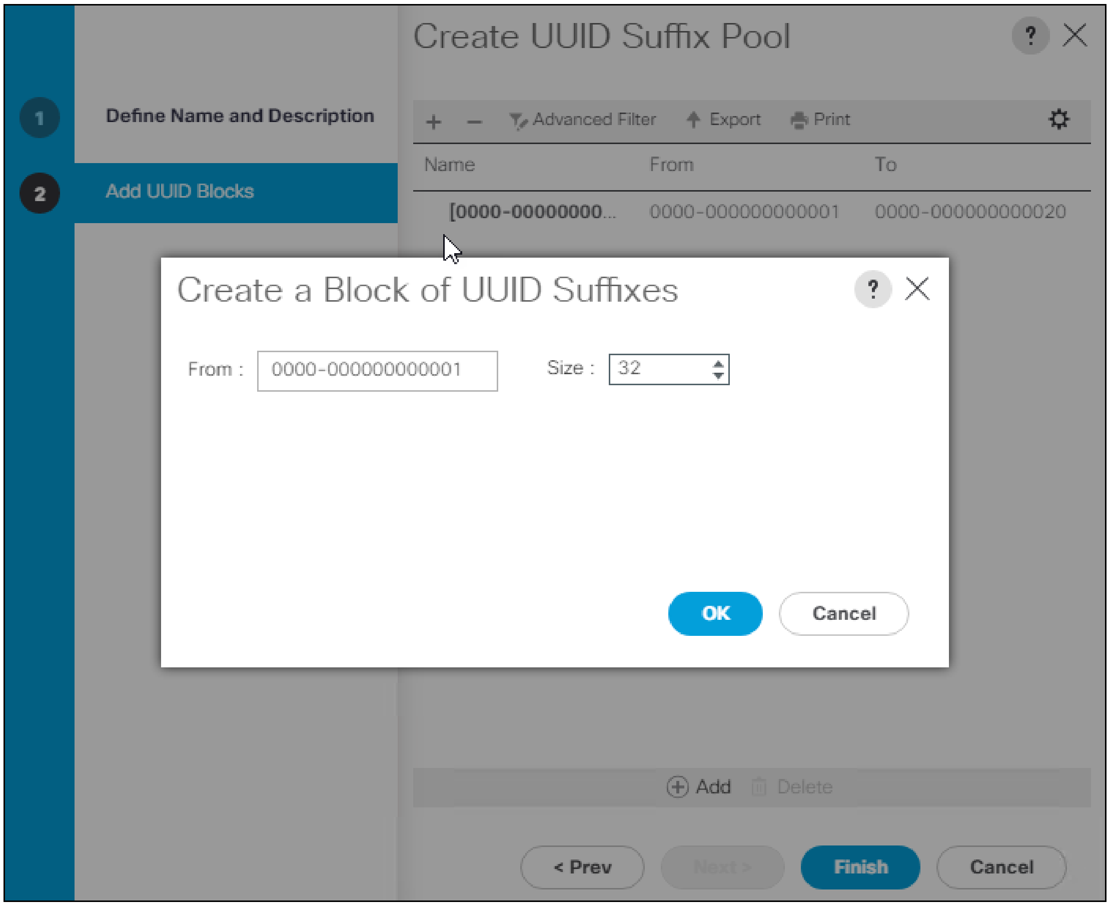
6. Optional: Enter a description for the UUID suffix pool.

7. Keep the prefix at the derived option.

8. Select Sequential for the Assignment Order.

9. Click Next.

10. Click Add to add a block of UUIDs.



Name	From	To
[0000-00000000...	0000-000000000001	0000-000000000020

Create a Block of UUID Suffixes

From : 0000-000000000001 Size : 32

11. Keep the From: field at the default setting.

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

13. Click OK.

14. Click Finish.

15. Click OK.

Create Server Pool

To configure the necessary server pool for the Cisco UCS environment, follow these steps:

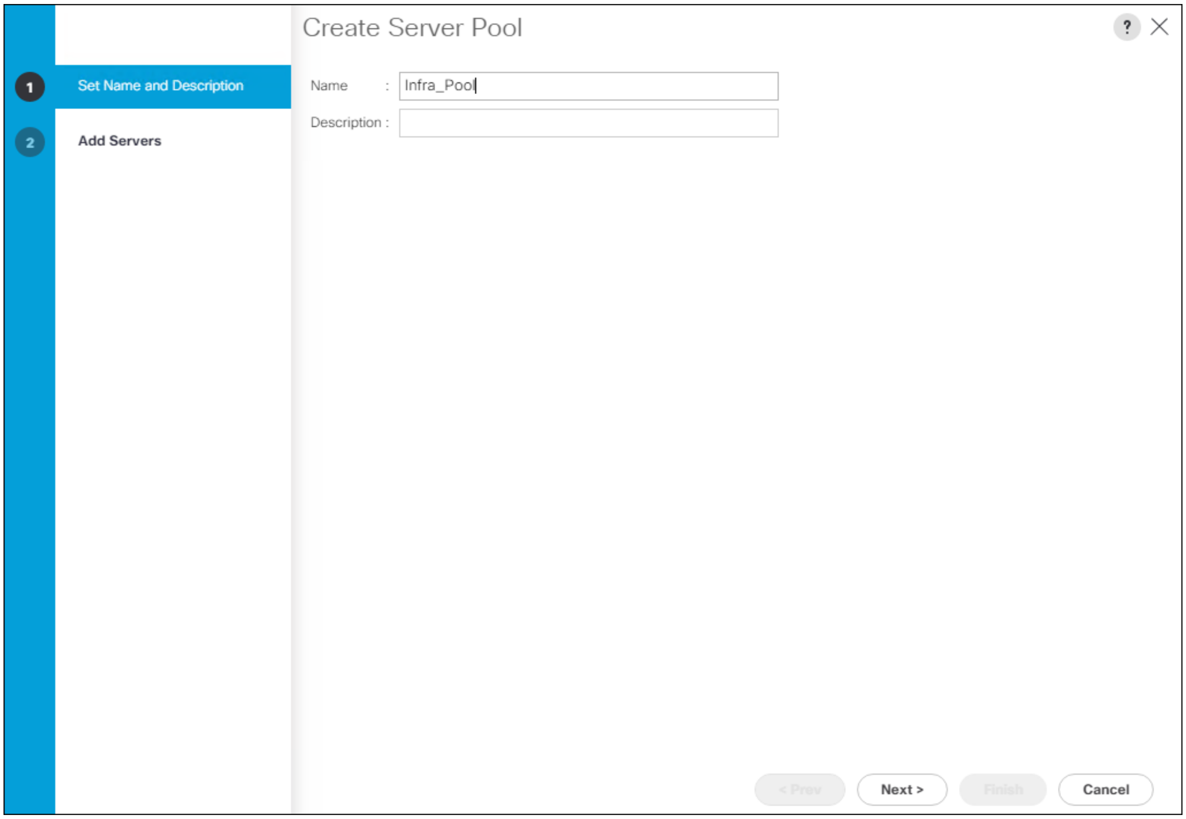
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.

2. Select Pools > root.

3. Right-click Server Pools.

4. Select Create Server Pool.

5. Enter Infra_Pool as the name of the server pool.



Create Server Pool

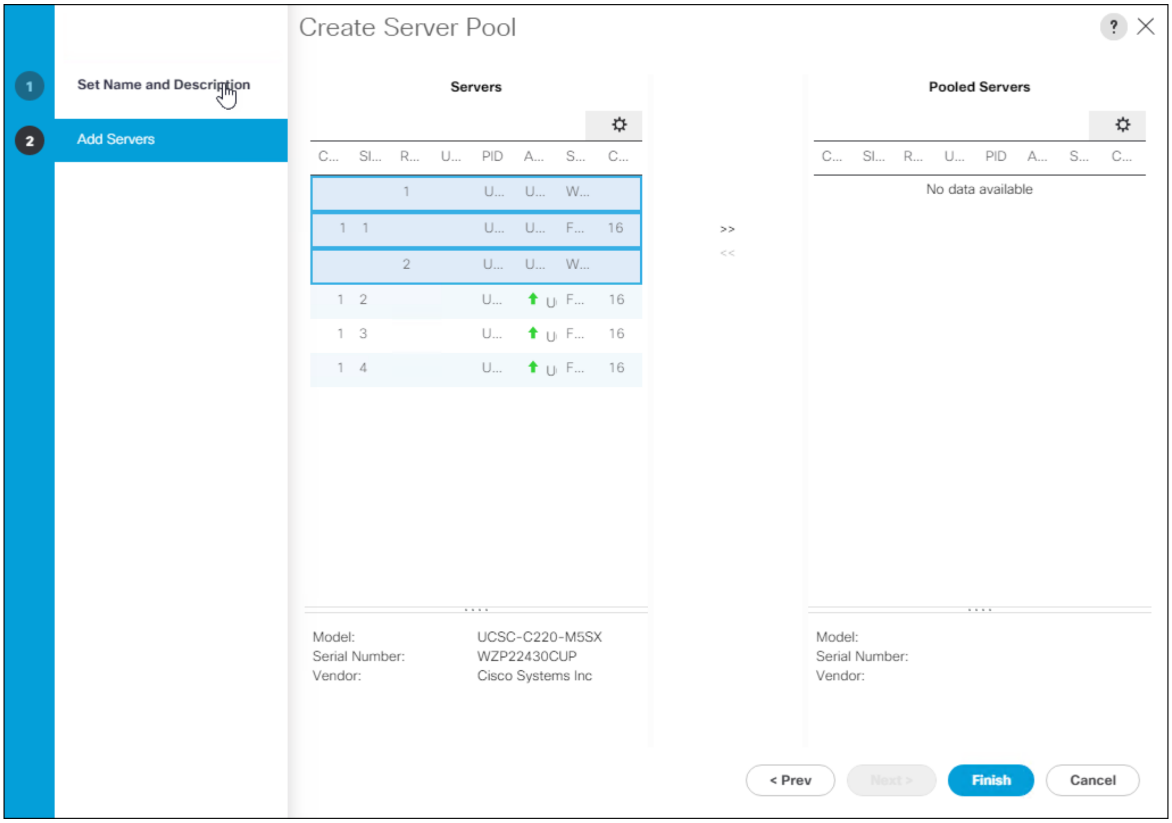
Name : Infra_Pool

Description :

6. Optional: Enter a description for the server pool.

7. Click Next.

8. Select two (or more) servers to be used for the VMware management cluster and click >> to add them to the Infra_Pool server pool.



C...	Sl...	R...	U...	PID	A...	S...	C...
		1		U...	U...	W...	
1	1			U...	U...	F...	16
		2		U...	U...	W...	
1	2			U...	↑ U	F...	16
1	3			U...	↑ U	F...	16
1	4			U...	↑ U	F...	16

Model: UCSC-C220-M5SX
Serial Number: WZP22430CUP
Vendor: Cisco Systems Inc

C...	Sl...	R...	U...	PID	A...	S...	C...

No data available

Model:
Serial Number:
Vendor:

9. Click Finish.

10. Click OK

Create IQN Pool for iSCSI Boot

To configure the necessary IQN pools for the Cisco UCS environment, follow these steps:

1. In Cisco UCS Manager, click SAN.

2. Select Pools > root.

3. Right-click IQN Pools.

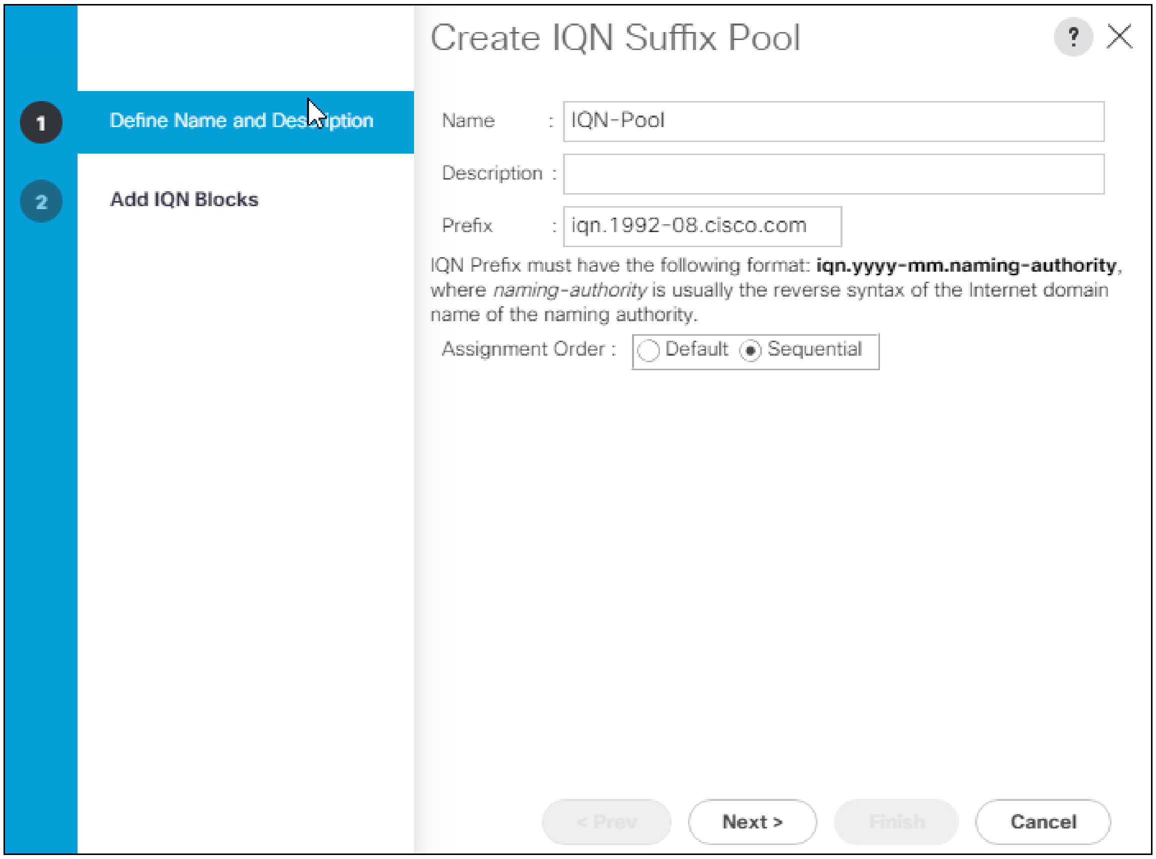
4. Select Create IQN Suffix Pool to create the IQN pool.

5. Enter IQN-Pool for the name of the IQN pool

6. Optional: Enter a description for the IQN pool

7. Enter iqn.1992-08.com.cisco as the prefix.

8. Select Sequential for Assignment Order



Create IQN Suffix Pool

Name : IQN-Pool

Description :

Prefix : iqn.1992-08.cisco.com

IQN Prefix must have the following format: **iqn.yyyy-mm.naming-authority**, where *naming-authority* is usually the reverse syntax of the Internet domain name of the naming authority.

Assignment Order : ○ Default ● Sequential

9. Click Next.

10. Click Add.

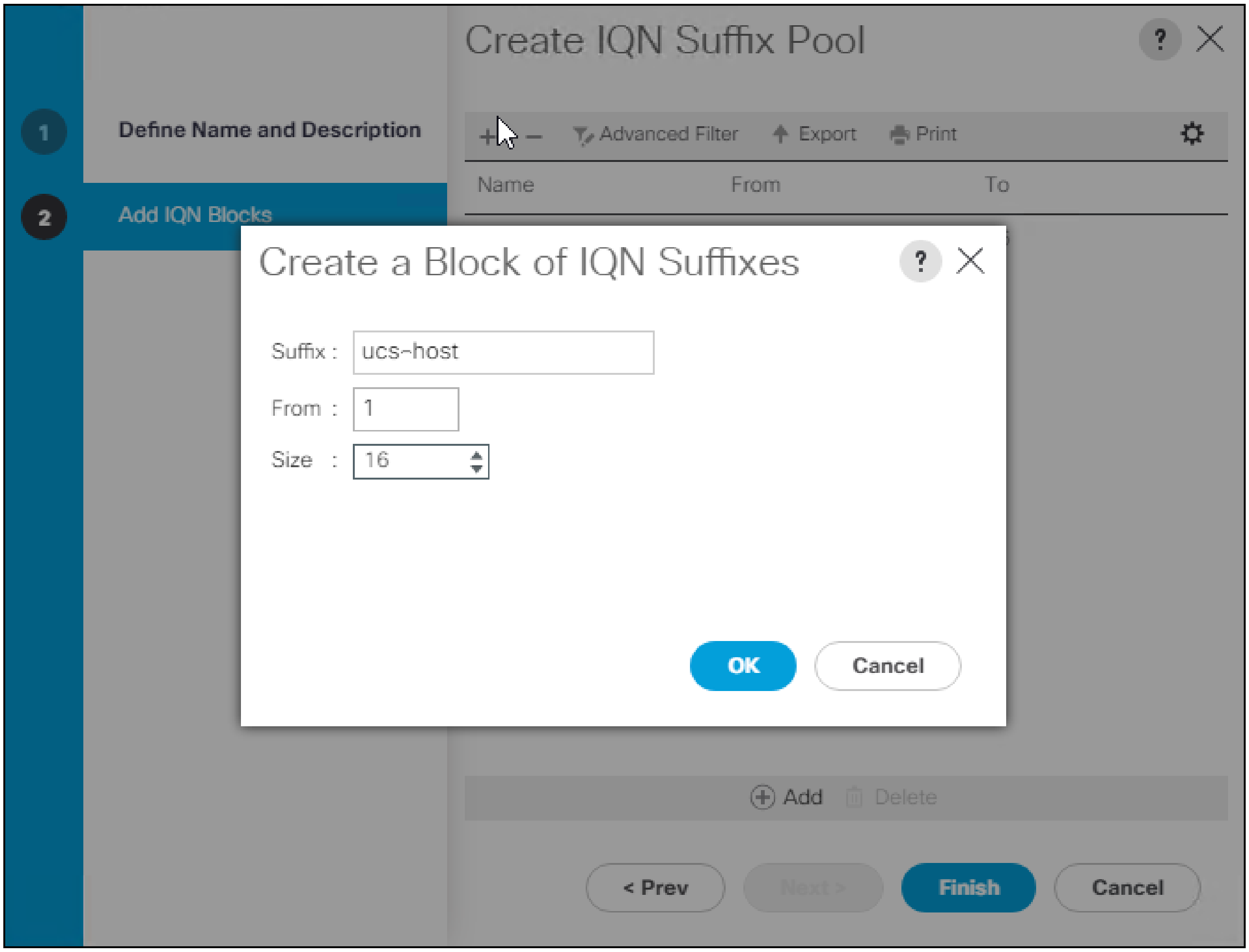
11. Enter ucs-host as the suffix.

If multiple Cisco UCS domains are being used, a more specific IQN suffix may need to be used.

12. Enter 1 in the From field.

13. Specify the size of the IQN block sufficient to support the available server resources.

14. Click OK.



Create IQN Suffix Pool

Create a Block of IQN Suffixes

Suffix : ucs-host

From : 1

Size : 16

15. Click Finish.

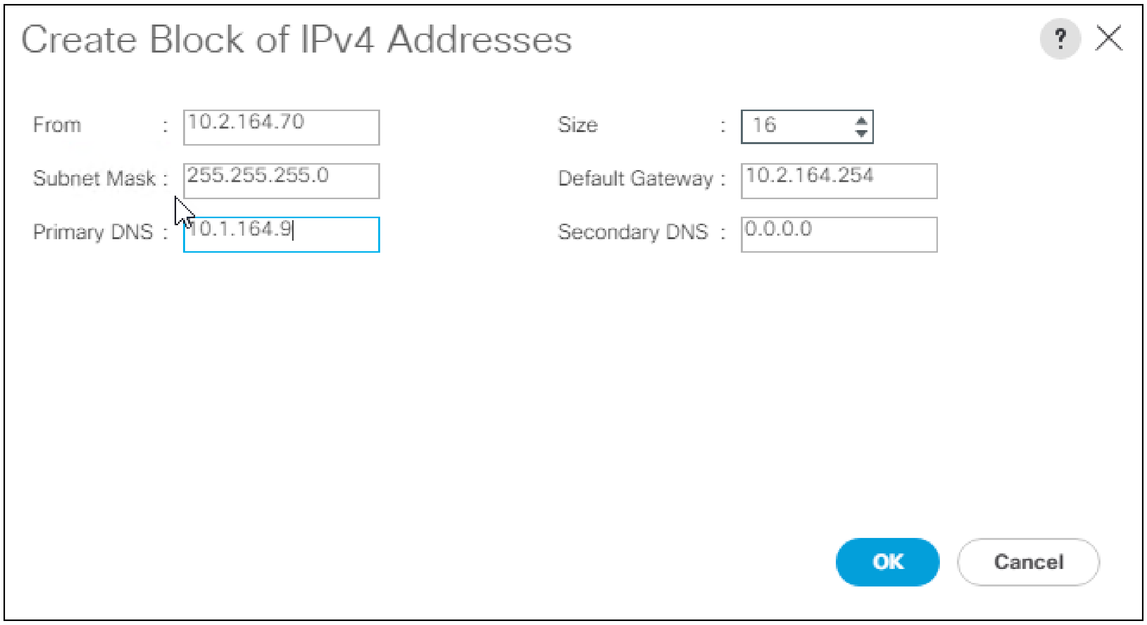
Create IP Pool for KVM Access

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

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

2. Select Pools > root > IP Pools.

3. Right-click IP Pool ext-mgmt and select Create Block of IPv4 Addresses.



Create Block of IPv4 Addresses

From : 10.2.164.70

Size : 16

Subnet Mask : 255.255.255.0

Default Gateway : 10.2.164.254

Primary DNS : 10.1.164.9

Secondary DNS : 0.0.0.0

4. Enter the starting IP address of the block and the number of IP addresses required, and the subnet and gateway information.

5. Click OK to create the block of IPs.

6. Click OK.

Create IP Pools for iSCSI Boot

To configure the necessary IP pools iSCSI boot for the Cisco UCS environment, follow these steps:

1. In Cisco UCS Manager, click LAN.

2. Select Pools > root.

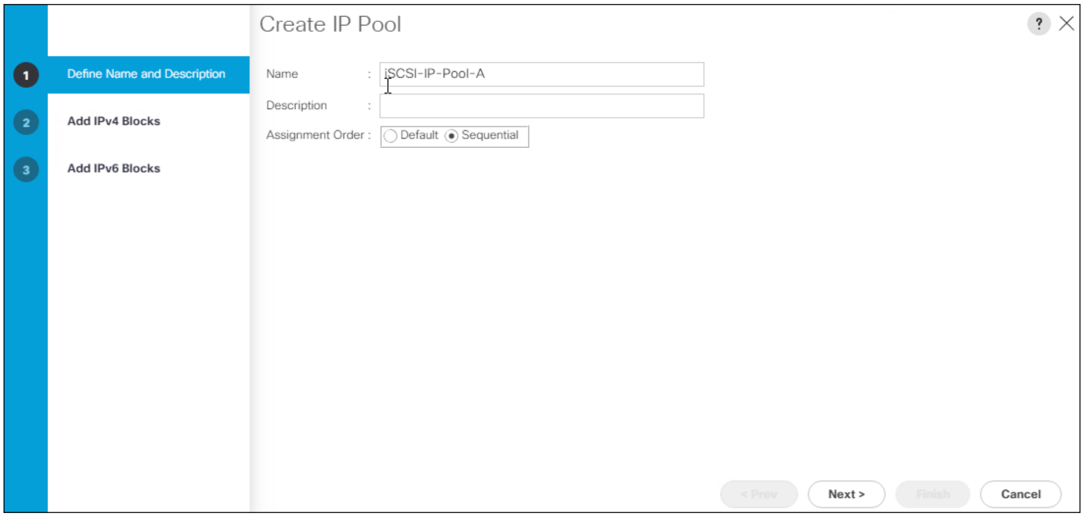
3. Right-click IP Pools.

4. Select Create IP Pool.

5. Enter iSCSI-IP-Pool-A as the name of IP pool.

6. Optional: Enter a description for the IP pool.

7. Select Sequential for the assignment order.



Create IP Pool

1 Define Name and Description

2 Add IPv4 Blocks

3 Add IPv6 Blocks

Name : iSCSI-IP-Pool-A

Description :

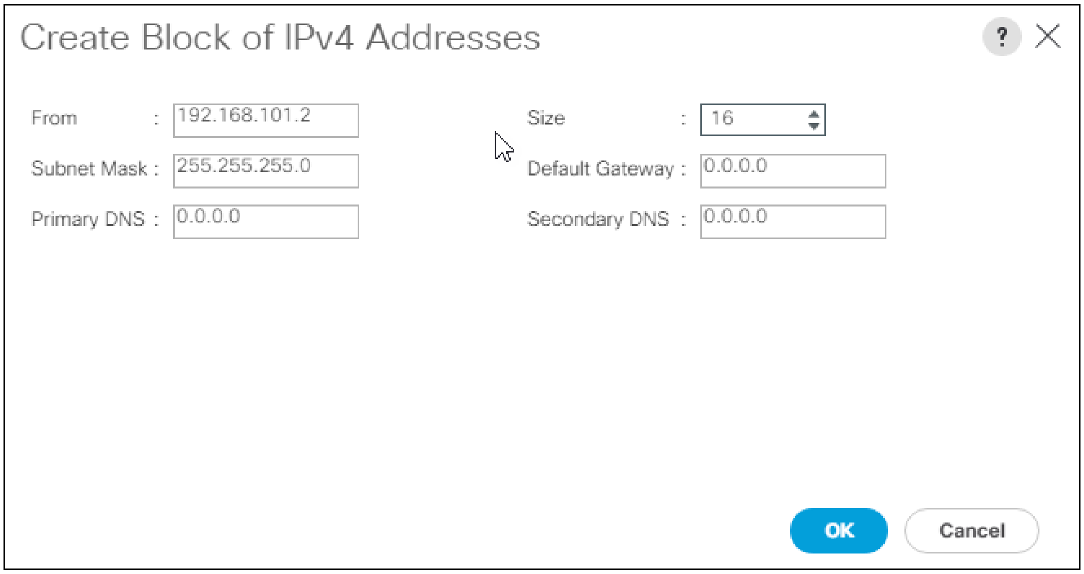
Assignment Order : ○ Default ● Sequential

8. Click Next.

9. Click Add to add a block of IP address.

10. In the **From** field, enter the beginning of the range to assign as iSCSI IP addresses

11. Set the size to enough addresses to accommodate the servers.



Create Block of IPv4 Addresses

From : 192.168.101.2

Size : 16

Subnet Mask : 255.255.255.0

Default Gateway : 0.0.0.0

Primary DNS : 0.0.0.0

Secondary DNS : 0.0.0.0

12. Click OK.

13. Click Next.

14. Click Finish.

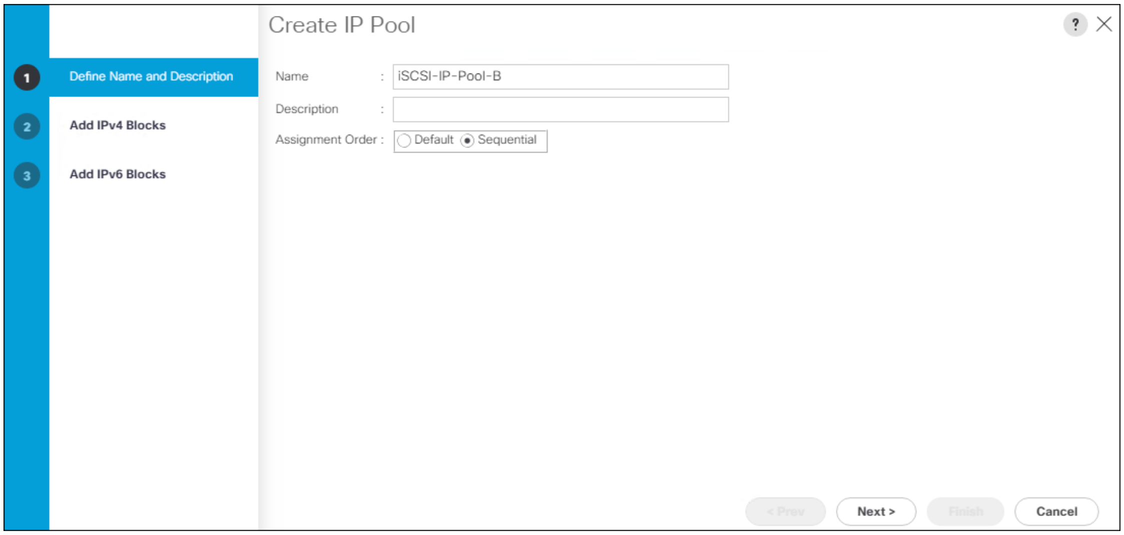
15. Right-click IP Pools.

16. Select Create IP Pool.

17. Enter iSCSI-IP-Pool-B as the name of IP pool.

18. Optional: Enter a description for the IP pool.

19. Select Sequential for the assignment order.



Name : iSCSI-IP-Pool-B

Description :

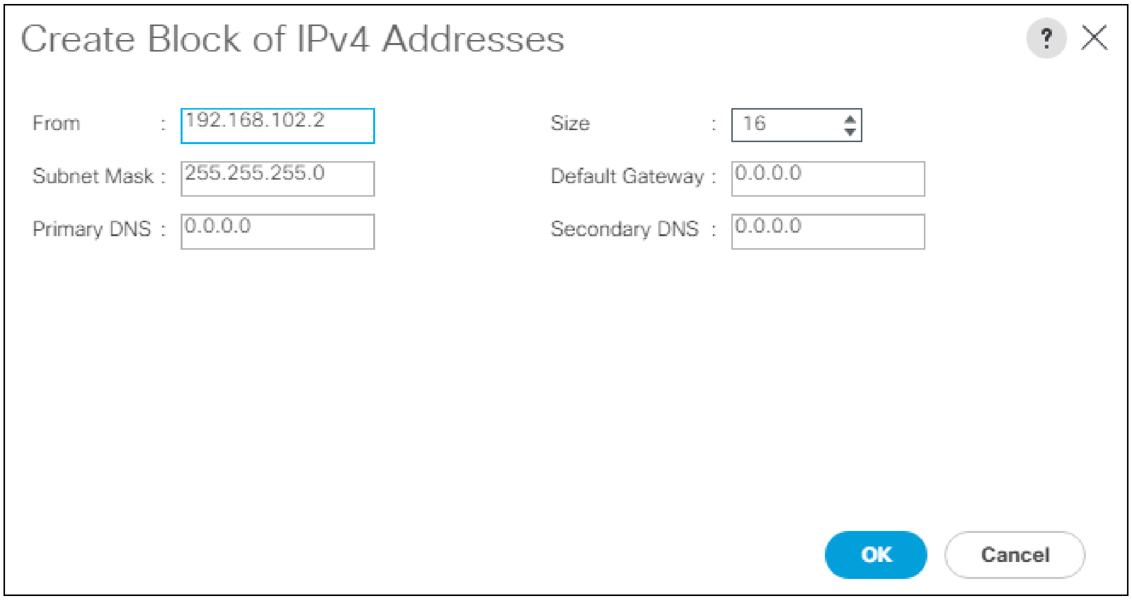
Assignment Order : ○ Default ● Sequential

20. Click Next.

21. Click Add to add a block of IP address.

22. In the From field, enter the beginning of the range to assign as iSCSI IP addresses

23. Set the size to enough addresses to accommodate the servers.



From : 192.168.102.2

Size : 16

Subnet Mask : 255.255.255.0

Default Gateway : 0.0.0.0

Primary DNS : 0.0.0.0

Secondary DNS : 0.0.0.0

24. Click OK.

25. Click Next.

26. Click Finish.

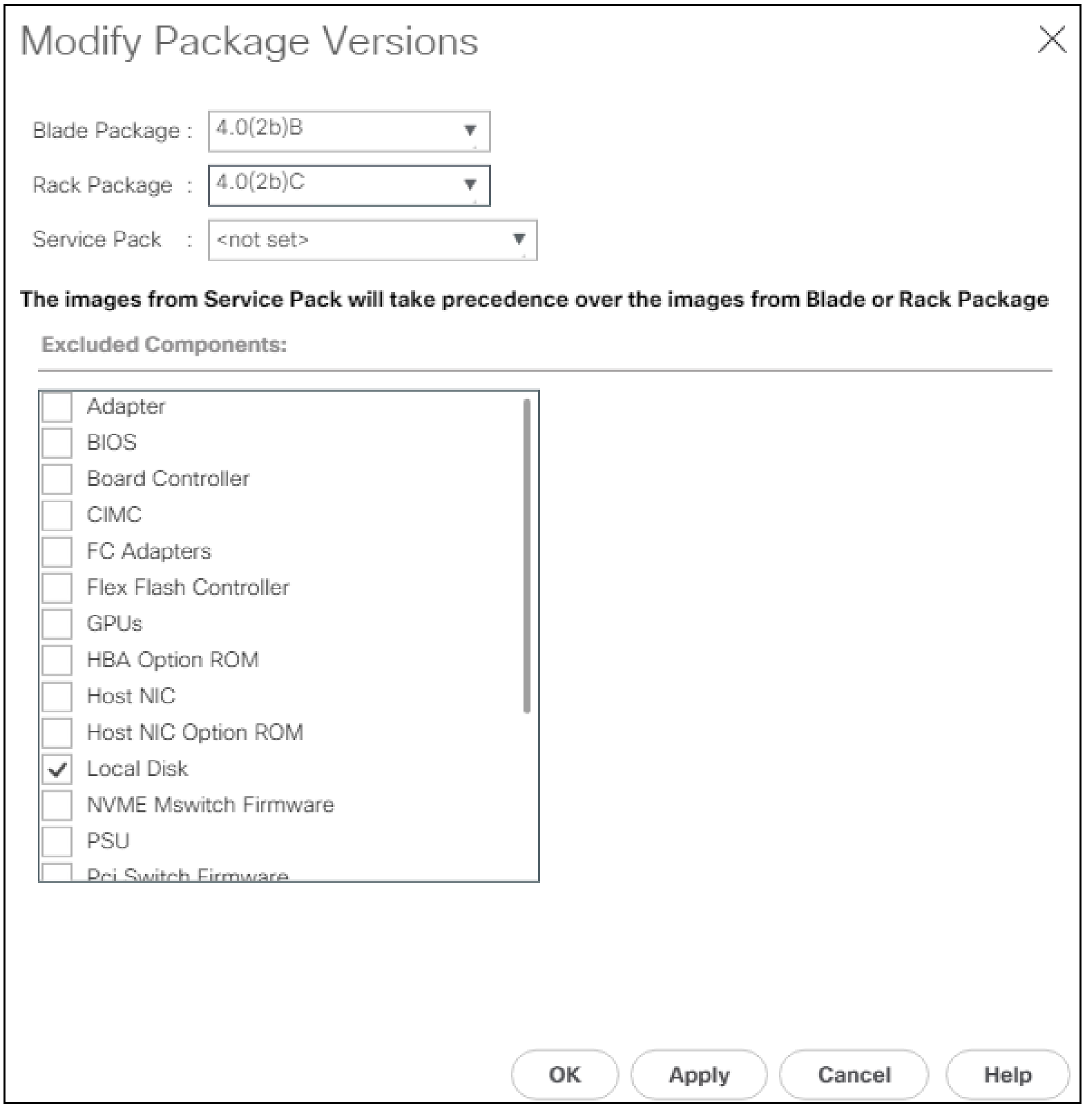
Set Packages and Policies

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, follow these steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Expand Host Firmware Packages.
4. Select default.
5. In the Actions pane, select Modify Package Versions.
6. Select the version 4.0(2b)B for the Blade Package, and optionally set version 4.0(2b)C for the Rack Package.
7. Leave Excluded Components with only Local Disk selected.



Modify Package Versions

Blade Package : 4.0(2b)B

Rack Package : 4.0(2b)C

Service Pack : <not set>

The images from Service Pack will take precedence over the images from Blade or Rack Package

Excluded Components:

□ Adapter
□ BIOS
□ Board Controller
□ CIMC
□ FC Adapters
□ Flex Flash Controller
□ GPUs
□ HBA Option ROM
□ Host NIC
□ Host NIC Option ROM
☑ Local Disk
□ NVME Mswitch Firmware
□ PSU
□ Pci Switch Firmware

8. Click OK to modify the host firmware package.

Create Server Pool Qualification Policy (Optional)

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

This example creates a policy for Cisco UCS B200 M5 servers for a server pool.

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

2. Select Policies > root.

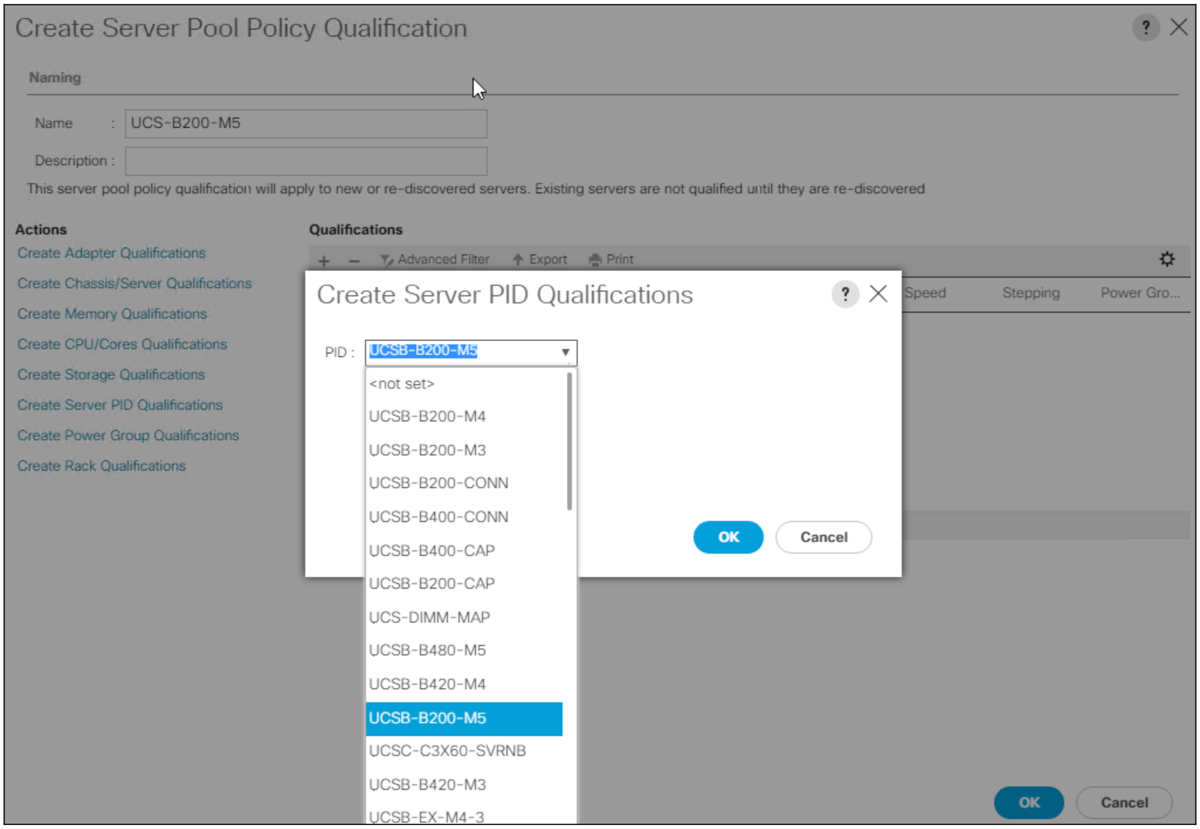
3. Right-click Server Pool Policy Qualifications.

4. Select Create Server Pool Policy Qualification.

5. Name the policy UCS-B200M5.

6. Select Create Server PID Qualifications.

7. Select UCS-B200-M5 from the PID drop-down.


Create Server Pool Policy Qualification
Naming
Actions
Create Adapter Qualifications
Create Chassis/Server Qualifications
Create Memory Qualifications
Create CPU/Cores Qualifications
Create Storage Qualifications
Create Server PID Qualifications
Create Power Group Qualifications
Create Rack Qualifications
Qualifications
Advanced Filter
Export
Print
Speed
Stepping
Power Gro...
Create Server PID Qualifications
<not set>
UCSB-B200-M4
UCSB-B200-M3
UCSB-B200-CONN
UCSB-B400-CONN
UCSB-B400-CAP
UCSB-B200-CAP
UCS-DIMM-MAP
UCSB-B480-M5
UCSB-B420-M4
UCSB-B200-M5
UCSC-C3X60-SVRNB
UCSB-B420-M3
UCSB-EX-M4-3
OK
Cancel
OK
Cancel

Name : UCS-B200-M5

Description :

This server pool policy qualification will apply to new or re-discovered servers. Existing servers are not qualified until they are re-discovered

PID : UCSB-B200-M5

8. Click OK.

9. Optionally select additional qualifications to refine server selection parameters for the server pool.

10. Click OK to create the policy then OK for the confirmation.

Create vMedia Policy for VMware ESXi 6.7 U1 Install Boot (Optional)

A separate HTTP web server is required to automate the availability of the ESXi image to each Service Profile on first power on. The creation of this web server is not covered in this document but can be any existing web server capable of serving files via HTTP that are accessible on the OOB network that the ESXi image can be placed upon.

Place the Cisco Custom Image VMware ESXi 6.7 U1 ISO on the HTTP server and follow these steps to create a vMedia Policy:

1. In Cisco UCS Manager, select Servers.

2. Select Policies > root.

3. Right-click vMedia Policies.

4. Select Create vMedia Policy.

5. Name the policy ESXi-6.7U1-HTTP.

6. Enter "Mounts ISO for ESXi 6.7 U1" in the Description field.

7. Click Add.

8. Name the mount ESXi-6.7U1-HTTP.

9. Select the CDD Device Type.

10. Select the HTTP Protocol.

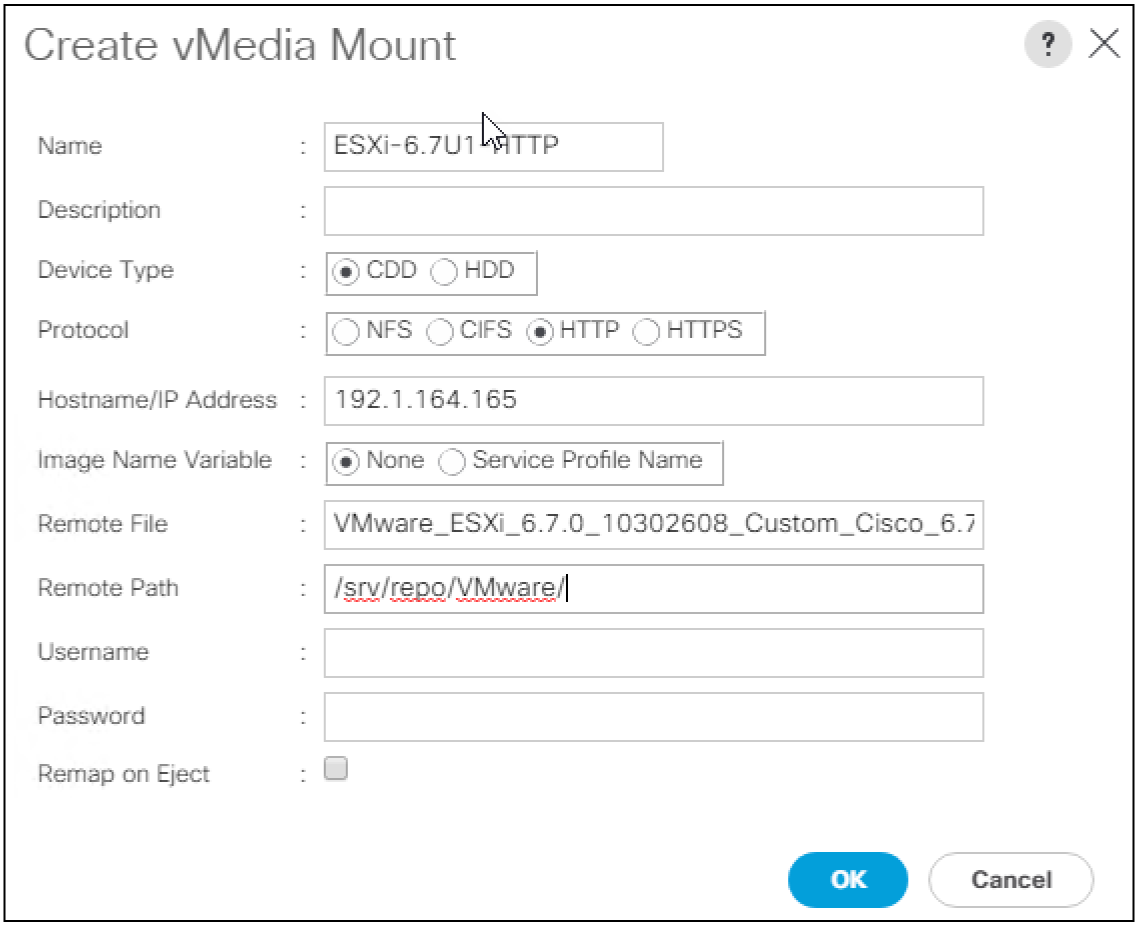
11. Enter the IP Address of the web server.

> Since DNS server IPs are not required in the KVM IP earlier, it is may be necessary to enter the IP of the web server instead of the hostname.

12. Leave "None" selected for Image Name Variable.

13. Enter VMware_ESXi_6.7.0_10302608_Custom_Cisco_6.7.1.1 as the Remote File name.

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



Create vMedia Mount

Name	:	ESXi-6.7U1-HTTP
Description	:	
Device Type	:	● CDD ○ HDD
Protocol	:	○ NFS ○ CIFS ● HTTP ○ HTTPS
Hostname/IP Address	:	192.1.164.165
Image Name Variable	:	● None ○ Service Profile Name
Remote File	:	VMware_ESXi_6.7.0_10302608_Custom_Cisco_6.7
Remote Path	:	/srv/repo/VMware/
Username	:	
Password	:	
Remap on Eject	:	□

15. Click OK to create the vMedia Mount.

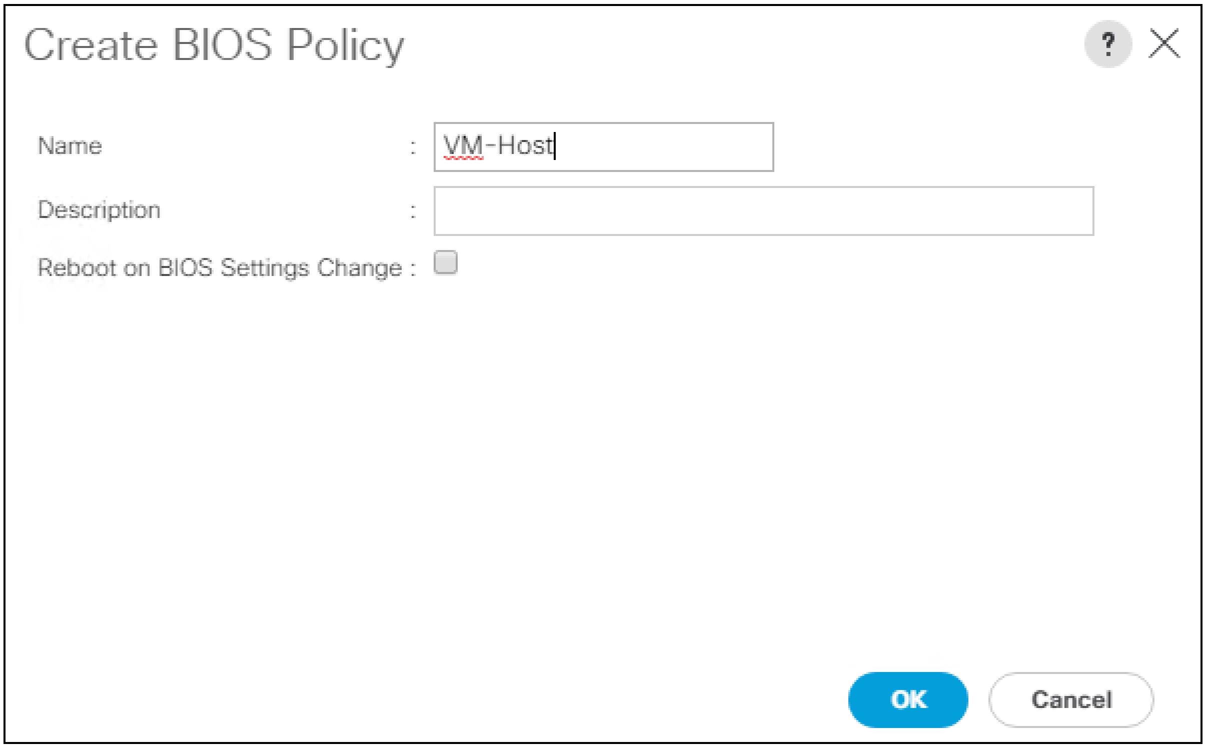
16. Click OK then OK again to complete creating the vMedia Policy.

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

Create Server BIOS Policy

To create a server BIOS policy for the Cisco UCS environment, follow these steps:

1. In Cisco UCS Manager, click Servers.
2. Select Policies > root.
3. Right-click BIOS Policies.
4. Select Create BIOS Policy.
5. Enter VM-Host as the BIOS policy name.



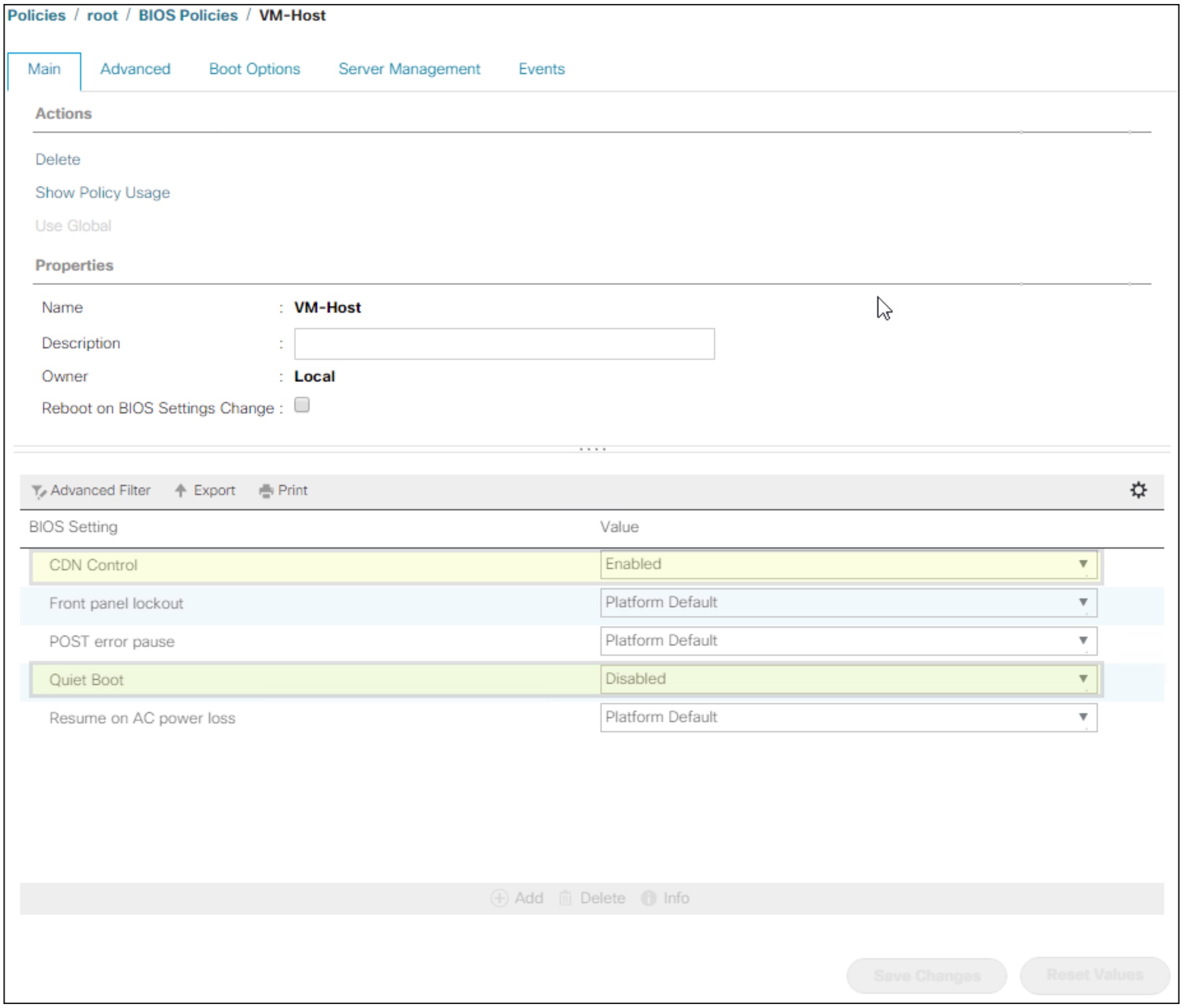
Create BIOS Policy

Name : VM-Host

Description :

Reboot on BIOS Settings Change : □

6. Select and right-click the newly created BIOS Policy.
7. Within the Main tab of the Policy:
8. Change CDN Control to enabled.
9. Change the Quiet Boot setting to disabled.



Name : **VM-Host**

Description :

Owner : **Local**

Reboot on BIOS Settings Change : □

BIOS Setting	Value
CDN Control	Enabled
Front panel lockout	Platform Default
POST error pause	Platform Default
Quiet Boot	Disabled
Resume on AC power loss	Platform Default

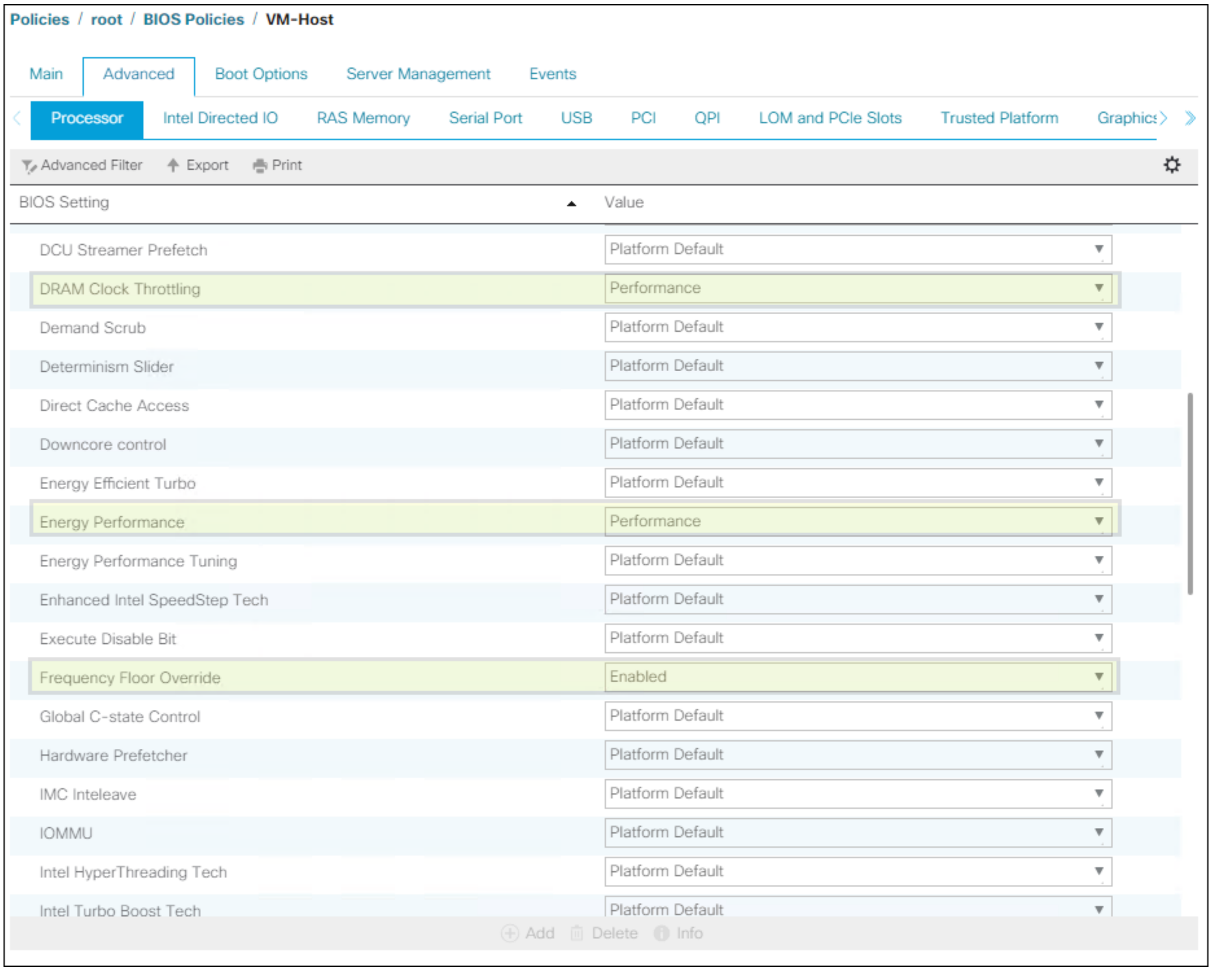
10. Click the Advanced tab, leaving the Processor tab selected within the Advanced tab.

11. Set the following within the Processor tab:

    a. DRAM Clock Throttling -> Performance

    b. Frequency Floor Override -> Enabled

    c. Energy Performance -> performance



BIOS Setting	Value
DCU Streamer Prefetch	Platform Default
DRAM Clock Throttling	Performance
Demand Scrub	Platform Default
Determinism Slider	Platform Default
Direct Cache Access	Platform Default
Downcore control	Platform Default
Energy Efficient Turbo	Platform Default
Energy Performance	Performance
Energy Performance Tuning	Platform Default
Enhanced Intel SpeedStep Tech	Platform Default
Execute Disable Bit	Platform Default
Frequency Floor Override	Enabled
Global C-state Control	Platform Default
Hardware Prefetcher	Platform Default
IMC Inteleave	Platform Default
IOMMU	Platform Default
Intel HyperThreading Tech	Platform Default
Intel Turbo Boost Tech	Platform Default

12. Scroll down to the remaining Processor options and select:

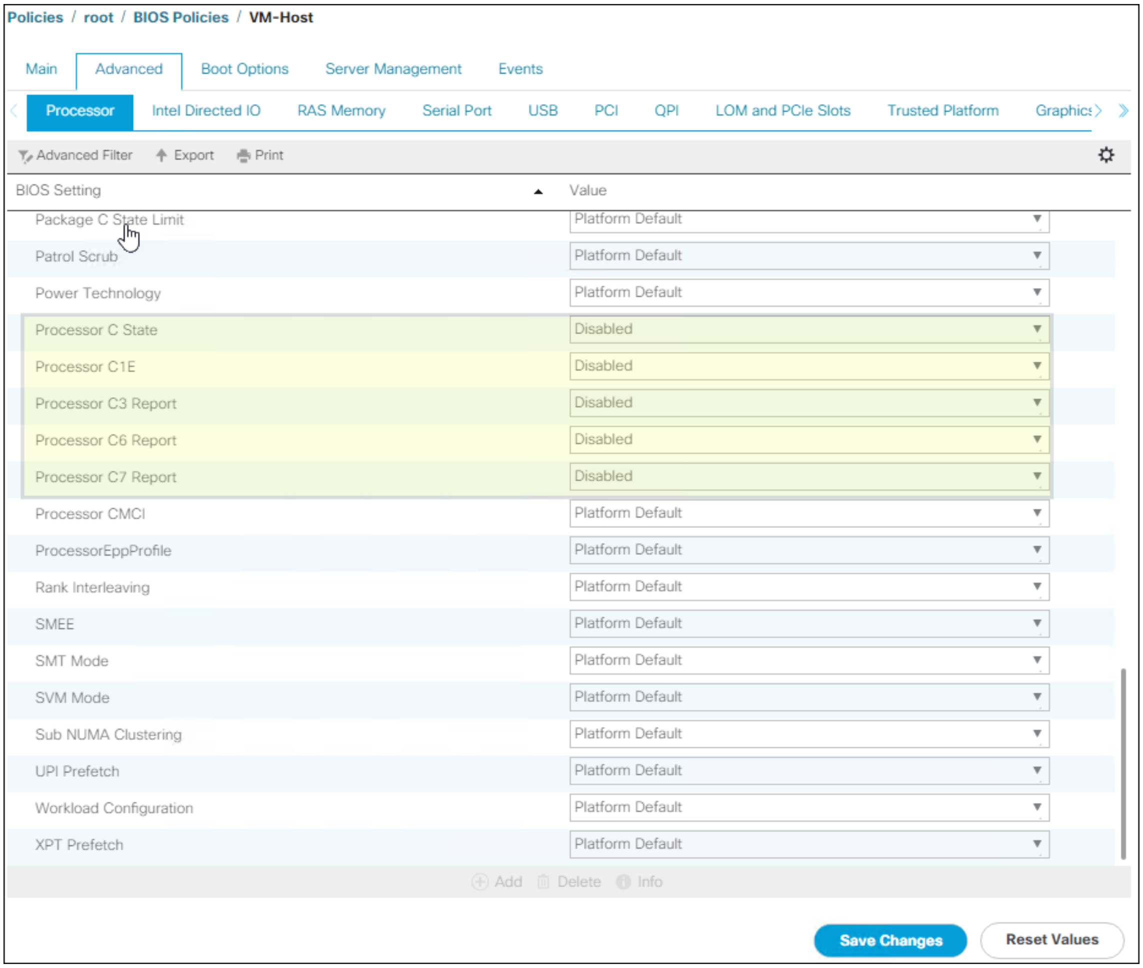
    a. Processor C State -> Disabled

    b. Processor C1E -> disabled

    c. Processor C3 Report -> disabled

    d. Processor C6 Report -> disabled

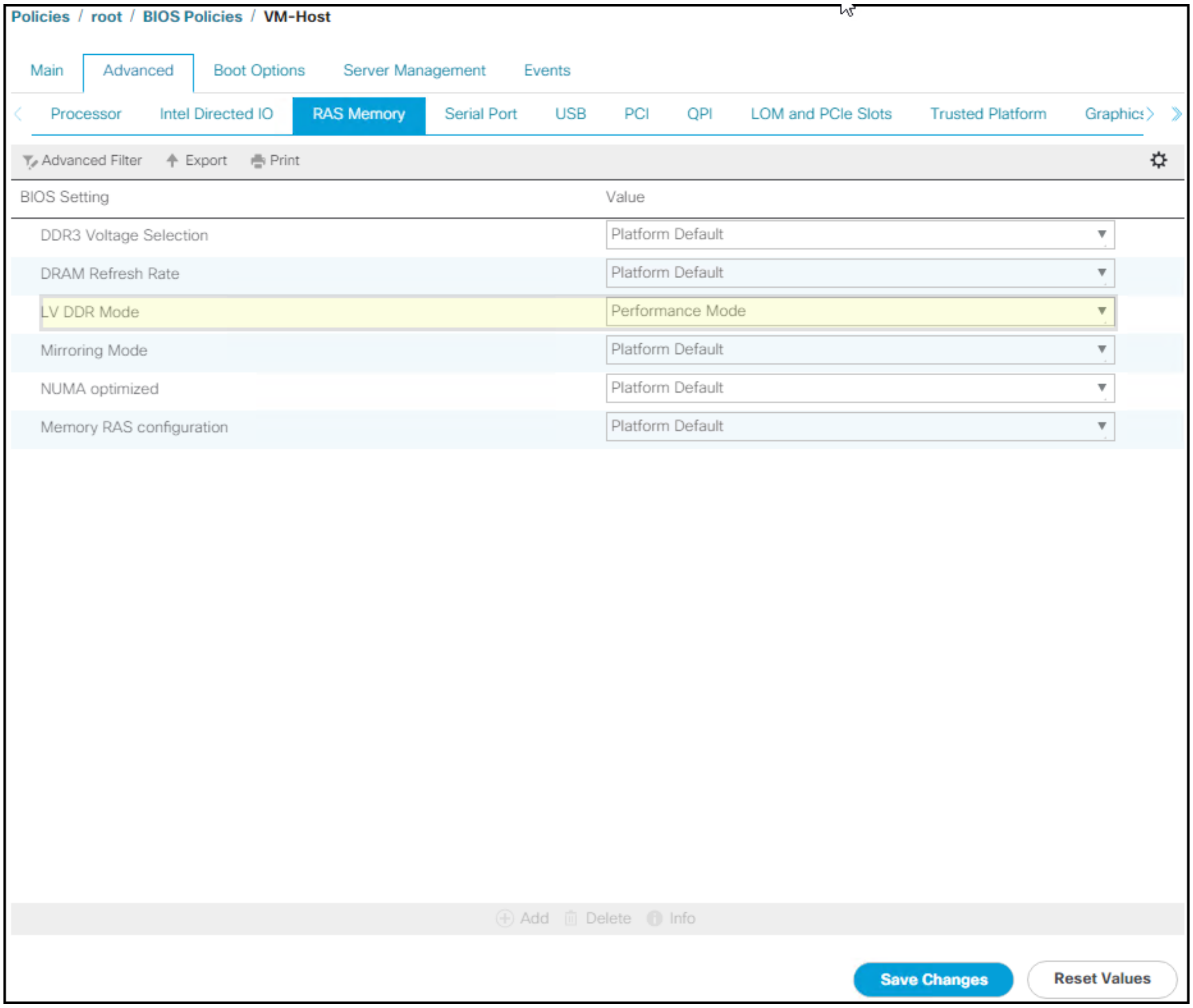
    e. Processor C7 Report -> disabled



BIOS Setting	Value
Package C State Limit	Platform Default
Patrol Scrub	Platform Default
Power Technology	Platform Default
Processor C State	Disabled
Processor C1E	Disabled
Processor C3 Report	Disabled
Processor C6 Report	Disabled
Processor C7 Report	Disabled
Processor CMCI	Platform Default
ProcessorEppProfile	Platform Default
Rank Interleaving	Platform Default
SMEE	Platform Default
SMT Mode	Platform Default
SVM Mode	Platform Default
Sub NUMA Clustering	Platform Default
UPI Prefetch	Platform Default
Workload Configuration	Platform Default
XPT Prefetch	Platform Default

13. Click the RAS Memory tab and select:

    a. LV DDR Mode -> performance-mode



BIOS Setting	Value
DDR3 Voltage Selection	Platform Default
DRAM Refresh Rate	Platform Default
LV DDR Mode	Performance Mode
Mirroring Mode	Platform Default
NUMA optimized	Platform Default
Memory RAS configuration	Platform Default

14. Click Save Changes.

15. Click OK.

Update Default Maintenance Policy

To update the default Maintenance Policy, follow these steps:

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

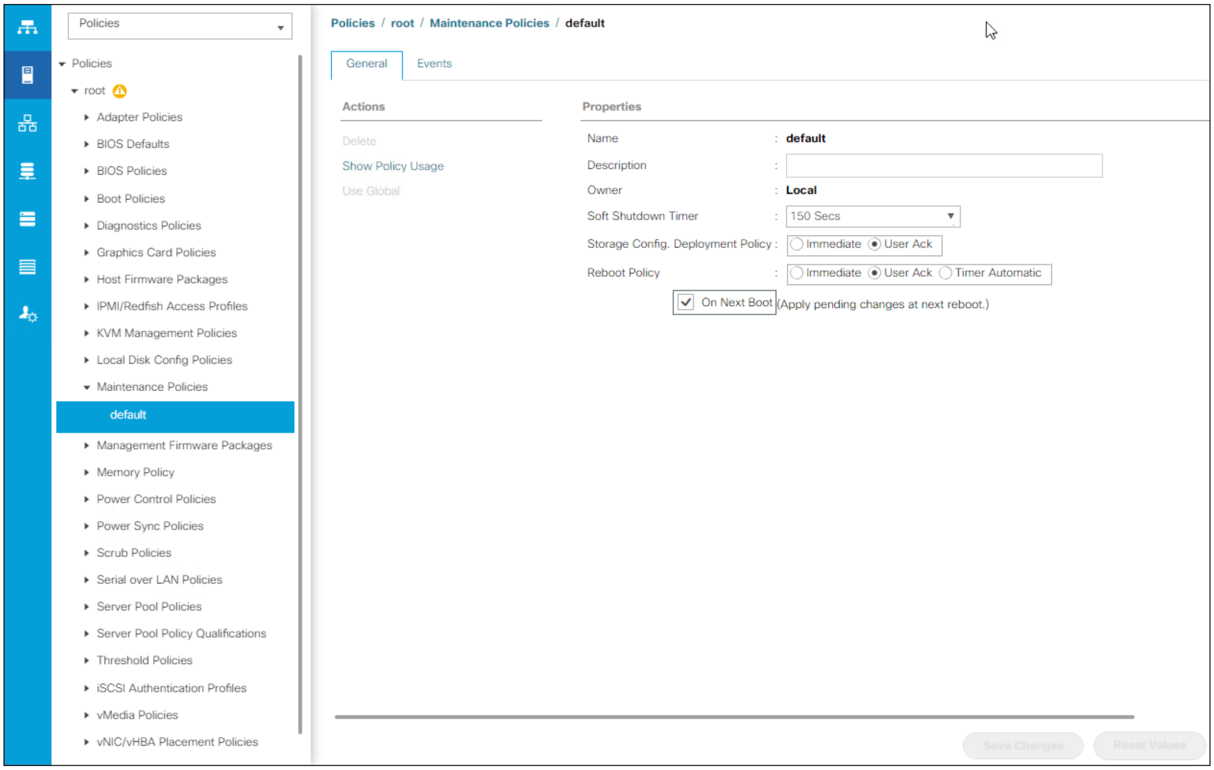
2. Select Policies > root.

3. Select Maintenance Policies > default.

4. Change the Reboot Policy to User Ack.

Setting the Reboot Policy to User Ack prevents the possibility of a policy driven server reboot.

5. (Optional: Click "On Next Boot" to delegate maintenance windows to server owners).



Name : default

Description :

Owner : Local

Soft Shutdown Timer : 150 Secs

Storage Config. Deployment Policy : ○ Immediate ● User Ack

Reboot Policy : ○ Immediate ● User Ack ○ Timer Automatic

☑ On Next Boot (Apply pending changes at next reboot.)

6. Click Save Changes.

7. Click OK to accept the change.

Create Local Disk Configuration Policy (Optional)

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

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

To create a local disk configuration policy, follow these steps:

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

2. Select Policies > root.

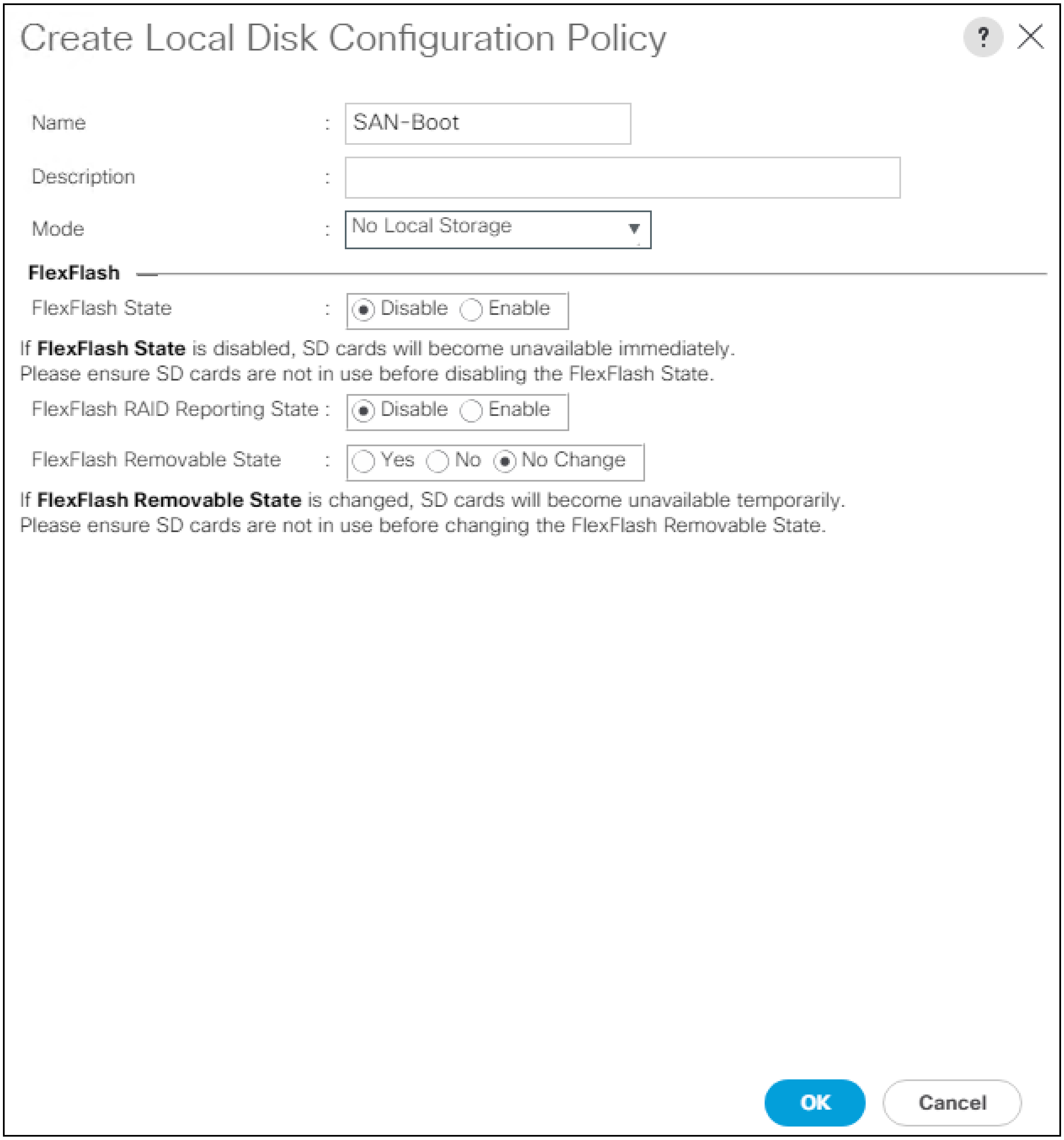
3. Right-click Local Disk Config Policies.

4. Select Create Local Disk Configuration Policy.

5. Enter SAN-Boot as the local disk configuration policy name.

6. Change the mode to No Local Storage.

7. Click OK to create the local disk configuration policy.



Create Local Disk Configuration Policy

Name : SAN-Boot

Description :

Mode : No Local Storage

FlexFlash

FlexFlash State : ● Disable ○ Enable

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

FlexFlash RAID Reporting State : ● Disable ○ Enable

FlexFlash Removable State : ○ Yes ○ No ● No Change

If **FlexFlash Removable State** is changed, SD cards will become unavailable temporarily.
Please ensure SD cards are not in use before changing the FlexFlash Removable State.

8. Click OK.

Create Power Control Policy

To create a power control policy for the Cisco UCS environment, follow these steps:

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

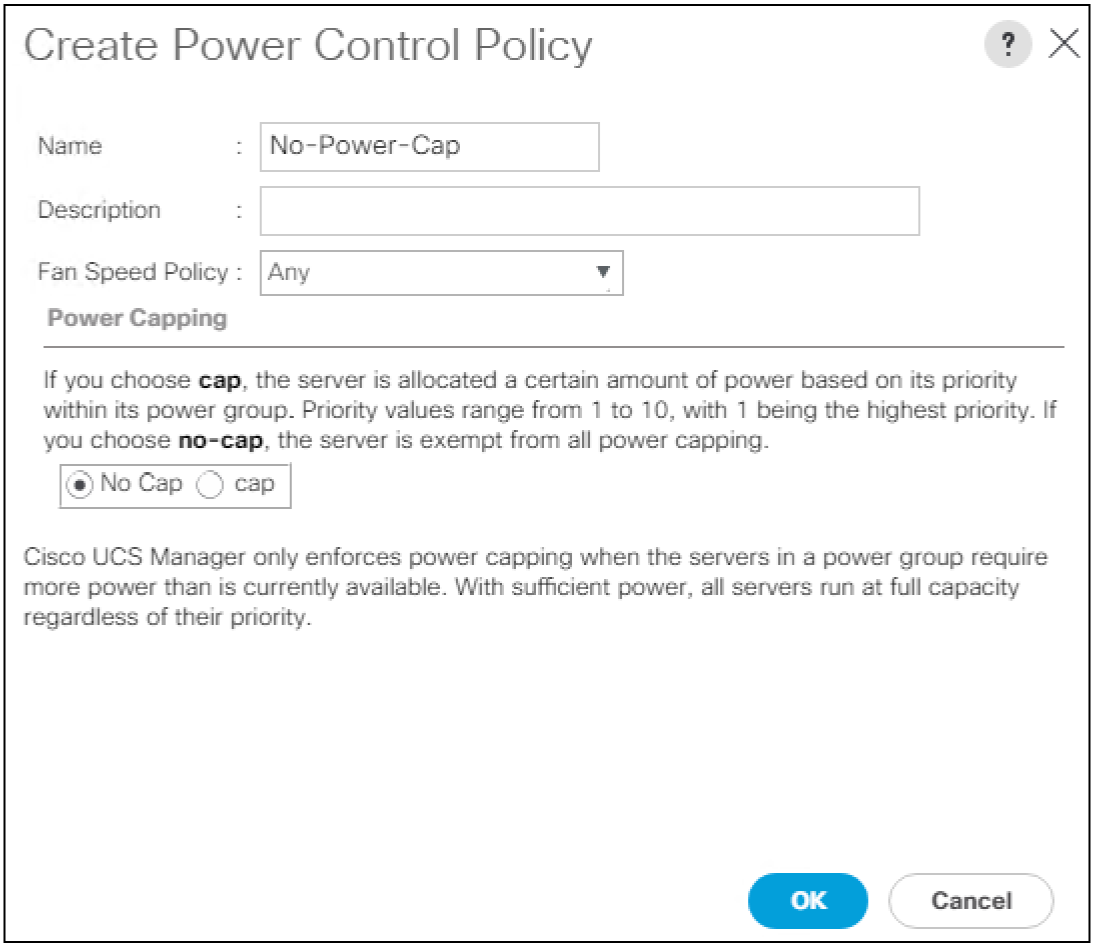
2. Select Policies > root.

3. Right-click Power Control Policies.

4. Select Create Power Control Policy.

5. Enter No-Power-Cap as the power control policy name.

6. Change the power capping setting to No Cap.



Create Power Control Policy

Name : No-Power-Cap

Description :

Fan Speed Policy : Any

Power Capping

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

● No Cap ○ cap

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

7. Click OK to create the power control policy.

8. Click OK.

Create Network Control Policy for Cisco Discovery Protocol

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

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

2. Select Policies > root.

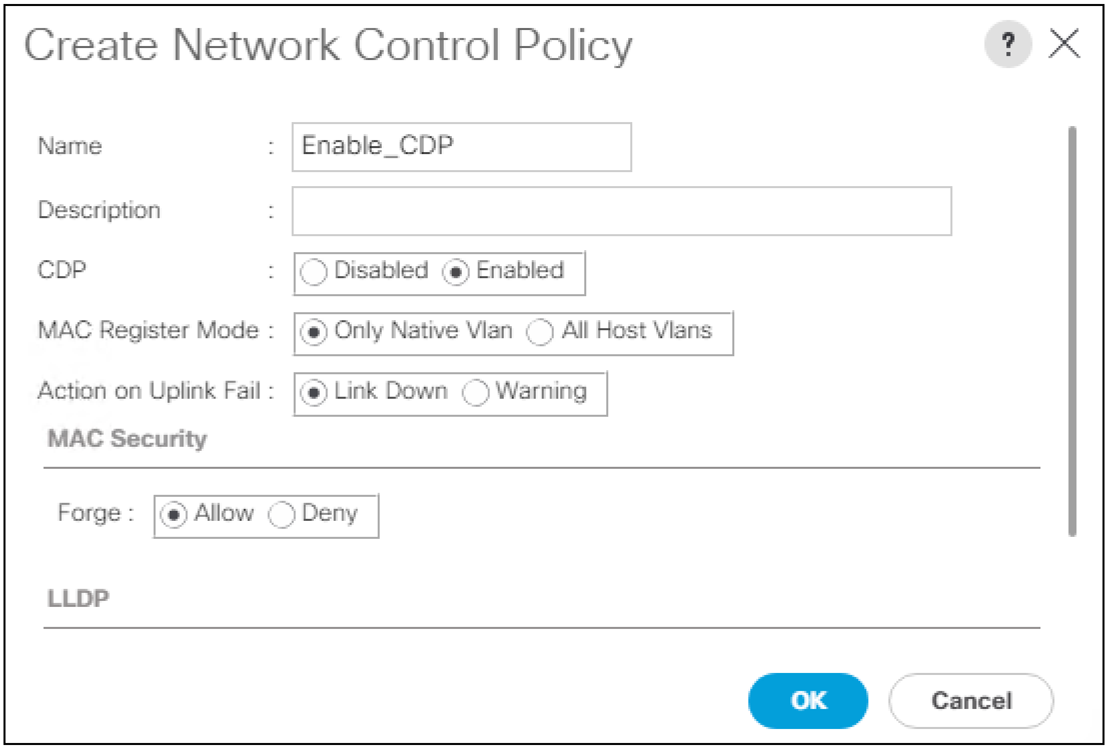
3. Right-click Network Control Policies.

4. Select Create Network Control Policy.

5. Enter Enable_CDP as the policy name.

6. For CDP, select the Enabled option.

7. Click OK to create the network control policy.



Create Network Control Policy

Name : Enable_CDP

Description :

CDP : ○ Disabled ● Enabled

MAC Register Mode : ● Only Native Vlan ○ All Host Vlans

Action on Uplink Fail : ● Link Down ○ Warning

MAC Security

Forge : ● Allow ○ Deny

LLDP

8. Click OK.

Configure Cisco UCS LAN Connectivity

Create Uplink Port Channels

To configure the necessary port channels out of the Cisco UCS environment, follow these steps:

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

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

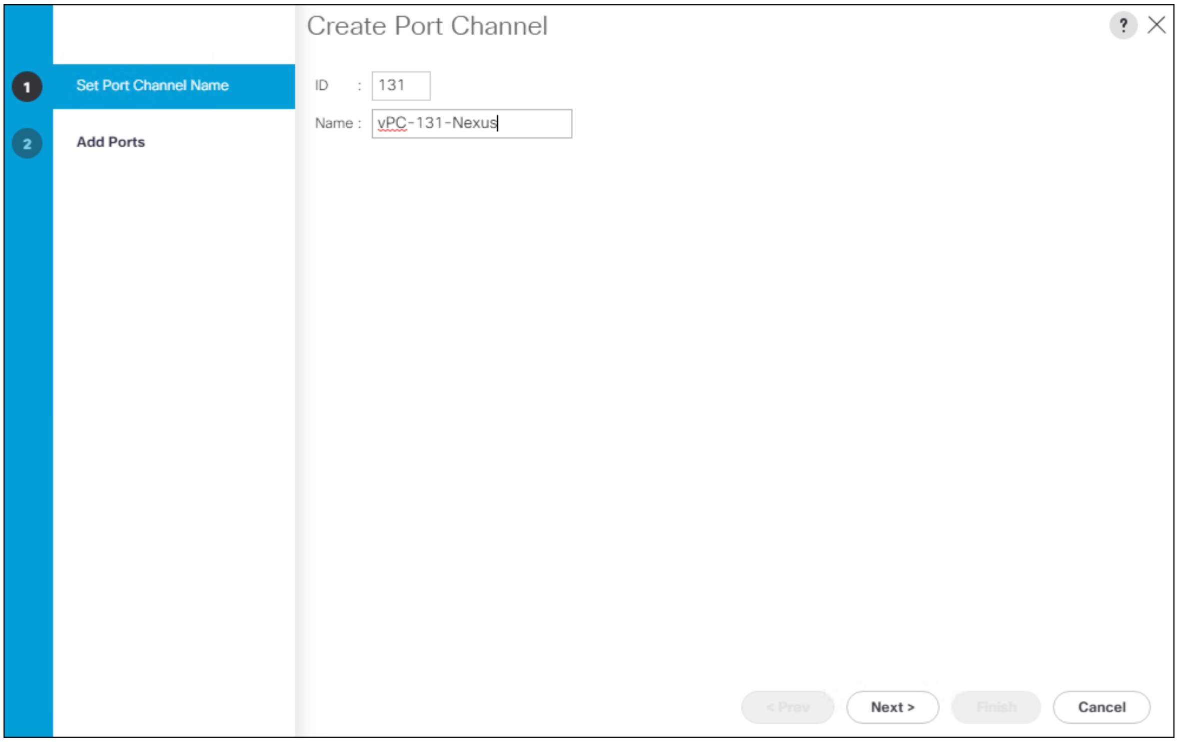
2. Under LAN > LAN Cloud, expand the Fabric A tree.

3. Right-click Port Channels.

4. Select Create Port Channel.

5. Enter a unique ID for the port channel, (131 in our example to correspond with the upstream Nexus port channel).

6. With 131 selected, enter vPC-131-Nexus as the name of the port channel.



Create Port Channel

ID : 131

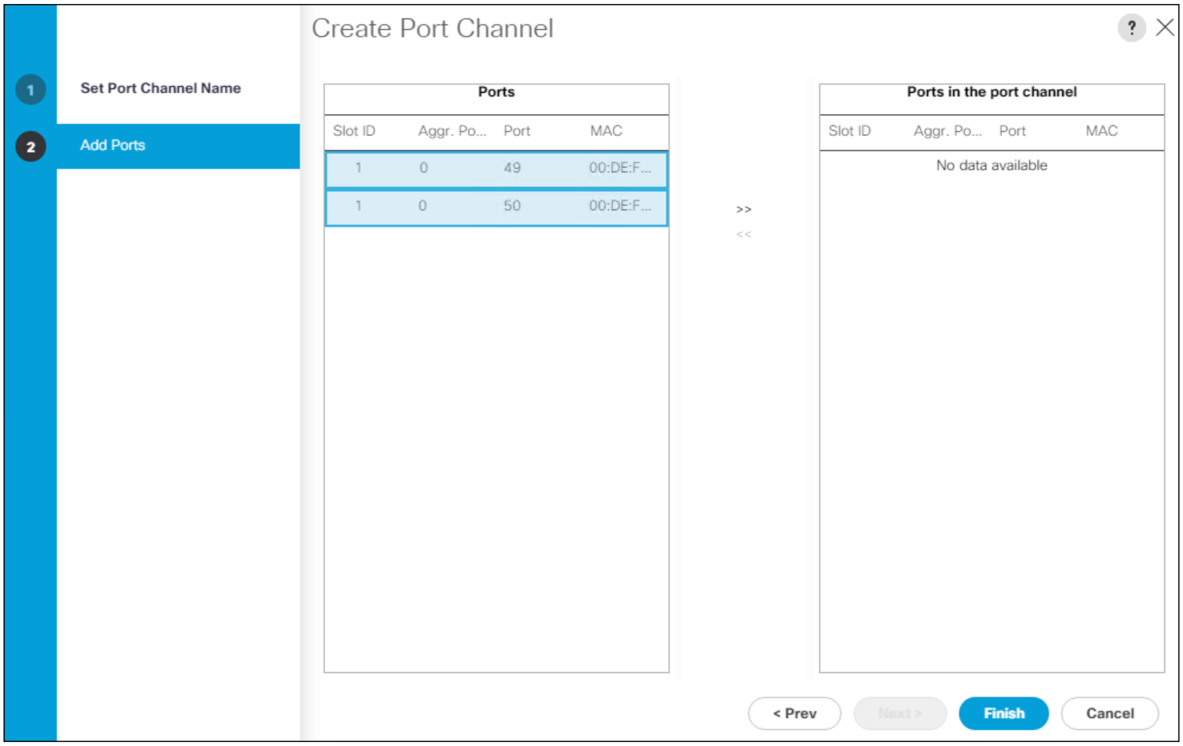
Name : vPC-131-Nexus

7. Click Next.

8. Select the following ports to be added to the port channel:

   a. Slot ID 1 and port 49

   b. Slot ID 1 and port 50



Create Port Channel

Ports

Slot ID	Aggr. Po...	Port	MAC
1	0	49	00:DE:F...
1	0	50	00:DE:F...

Ports in the port channel

Slot ID	Aggr. Po...	Port	MAC
No data available			

9. Click >> to add the ports to the port channel.

10. Click Finish to create the port channel.

11. Click OK.

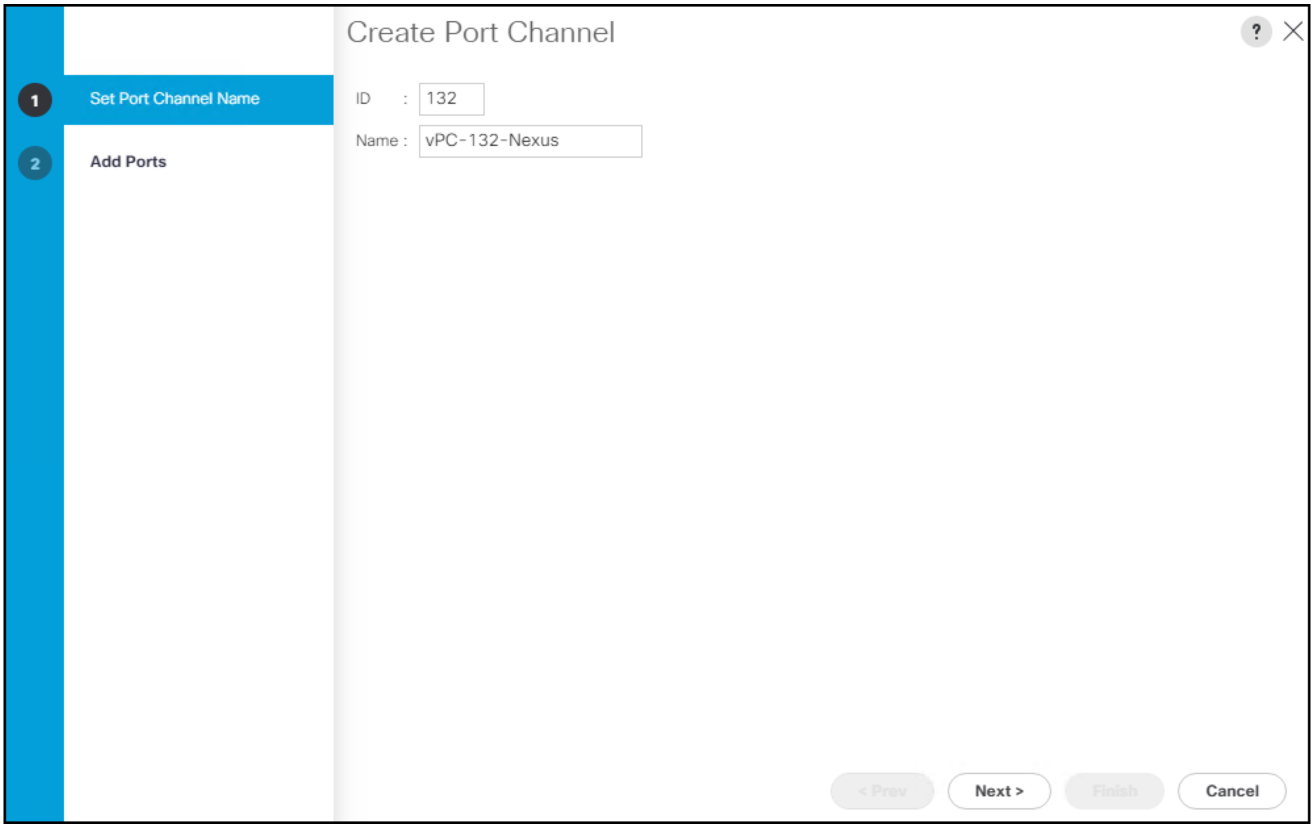
12. In the navigation pane, under LAN > LAN Cloud, expand the fabric B tree.

13. Right-click Port Channels.

14. Select Create Port Channel.

15. Enter a unique ID for the port channel, (132 in our example to correspond with the upstream Nexus port channel).

16. With 132 selected, enter vPC-132-Nexus as the name of the port channel.



Create Port Channel

1 Set Port Channel Name

2 Add Ports

ID : 132

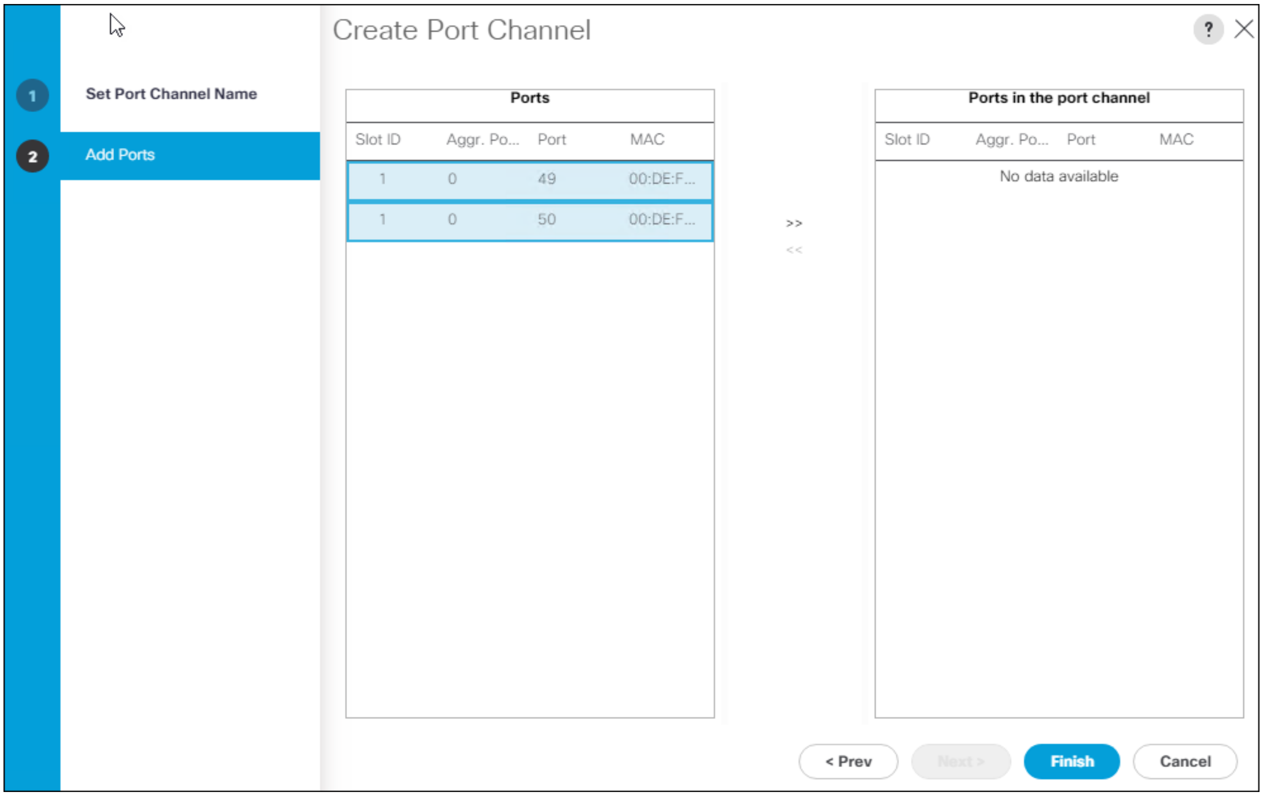
Name : vPC-132-Nexus

17. Click Next.

18. Select the following ports to be added to the port channel:

    a. Slot ID 1 and port 49

    b. Slot ID 1 and port 50



Ports

Slot ID	Aggr. Po...	Port	MAC
1	0	49	00:DE:F...
1	0	50	00:DE:F...

Ports in the port channel

Slot ID	Aggr. Po...	Port	MAC
No data available			

19. Click >> to add the ports to the port channel.

20. Click Finish to create the port channel.

21. Click OK.

Create VLANS

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

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

In this procedure, six unique VLANs are created. See Table 2 for a list of VLANs to be created.

2. Select LAN > LAN Cloud.

3. Right-click VLANs.

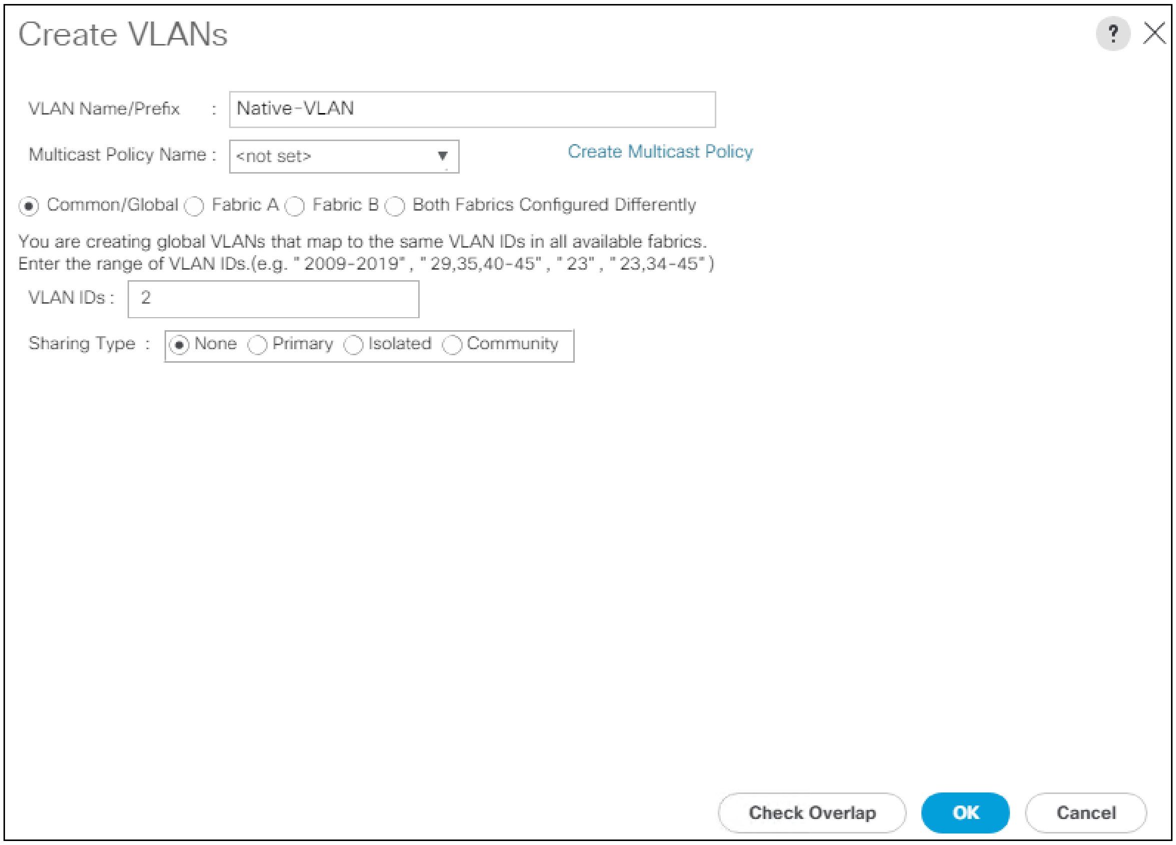
4. Select Create VLANs.

5. Enter Native-VLAN as the name of the VLAN to be used as the native VLAN.

6. Keep the Common/Global option selected for the scope of the VLAN.

7. Enter the native VLAN ID.

8. Keep the Sharing Type as None.



Create VLANs

VLAN Name/Prefix : Native-VLAN

Multicast Policy Name : <not set>

● Common/Global ○ Fabric A ○ Fabric B ○ Both Fabrics Configured Differently

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

VLAN IDs : 2

Sharing Type : ● None ○ Primary ○ Isolated ○ Community

9. Click OK and then click OK again.

10. Expand the list of VLANs in the navigation pane, right-click the newly created Native-VLAN and select Set as Native VLAN.

11. Click Yes, and then click OK.

12. Right-click VLANs.

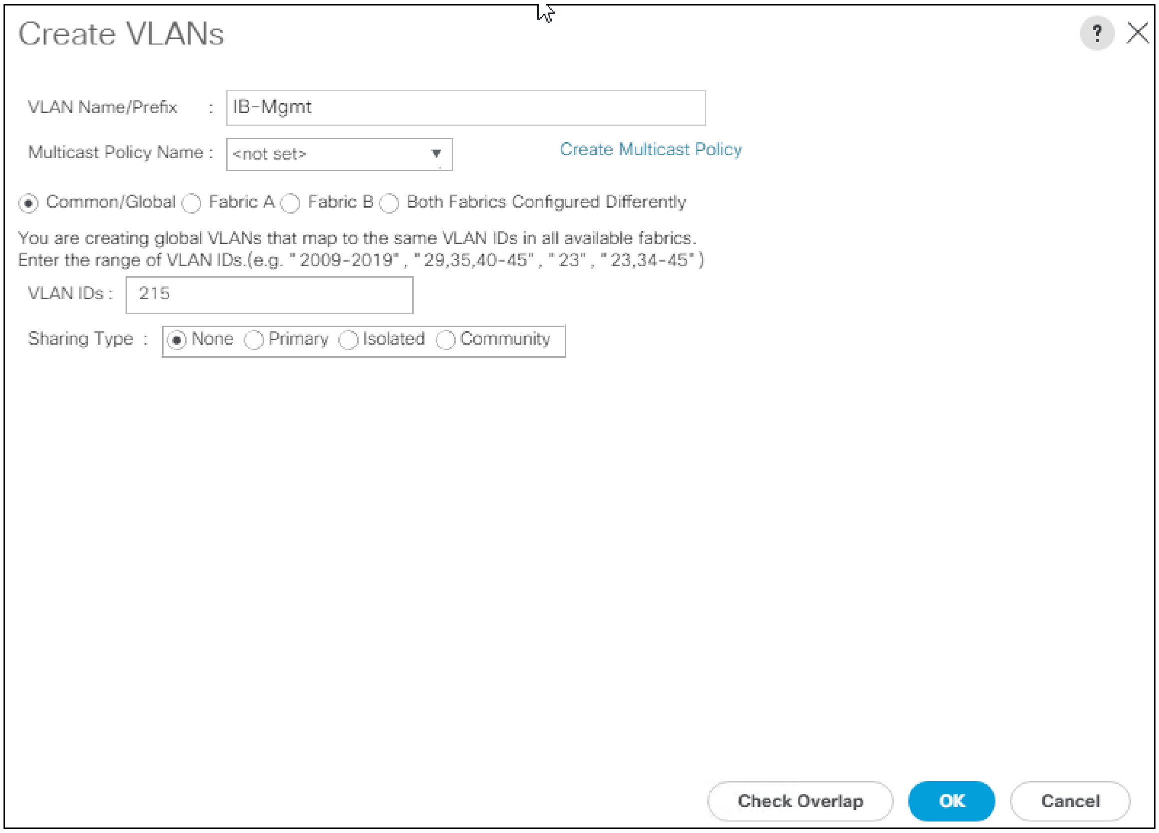
13. Select Create VLANs

14. Enter IB-Mgmt as the name of the VLAN to be used for management traffic.

15. Keep the Common/Global option selected for the scope of the VLAN.

16. Enter the In-Band management VLAN ID.

17. Keep the Sharing Type as None.



Create VLANs

VLAN Name/Prefix : IB-Mgmt

Multicast Policy Name : <not set>

● Common/Global ○ Fabric A ○ Fabric B ○ Both Fabrics Configured Differently

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

VLAN IDs : 215

Sharing Type : ● None ○ Primary ○ Isolated ○ Community

18. Click OK and then click OK again.

19. Right-click VLANs.

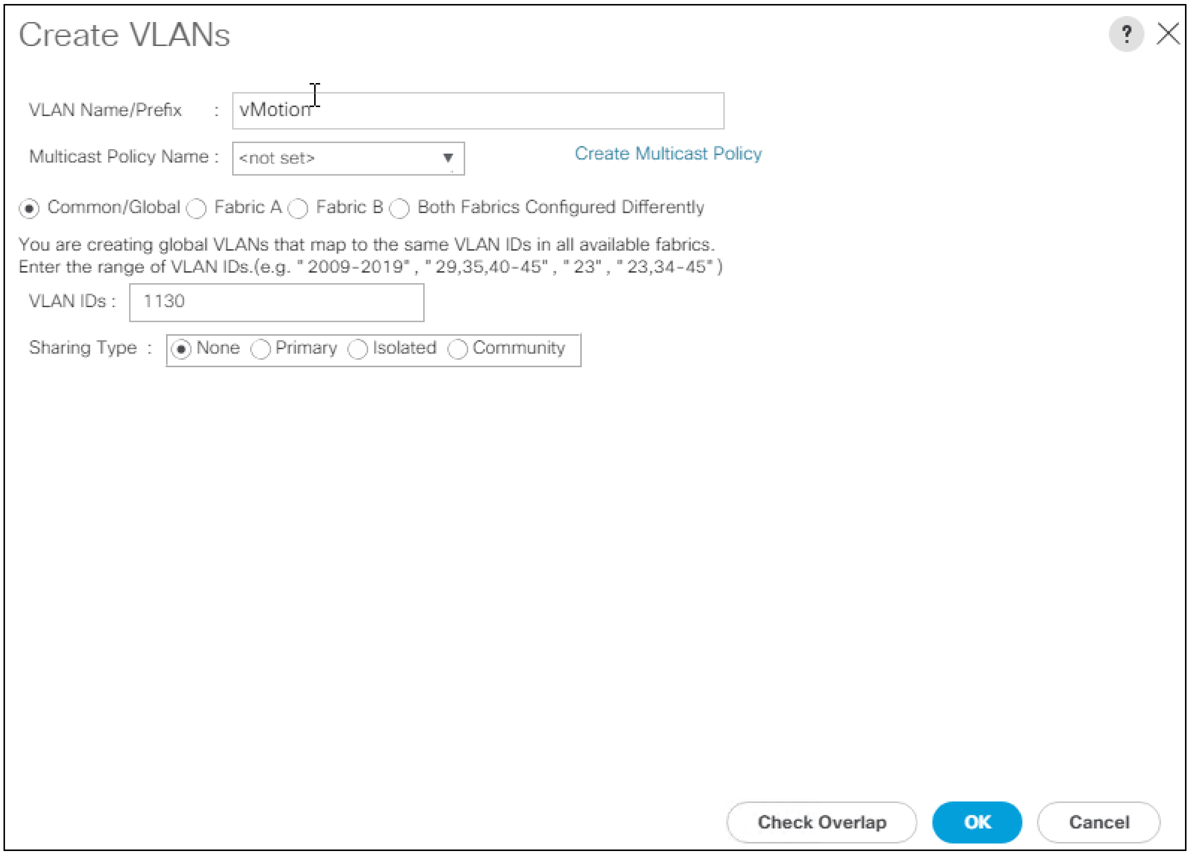
20. Select Create VLANs.

21. Enter vMotion as the name of the VLAN to be used for vMotion.

22. Keep the Common/Global option selected for the scope of the VLAN.

23. Enter the vMotion VLAN ID.

24. Keep the Sharing Type as None.



Create VLANs

VLAN Name/Prefix : vMotion

Multicast Policy Name : <not set>

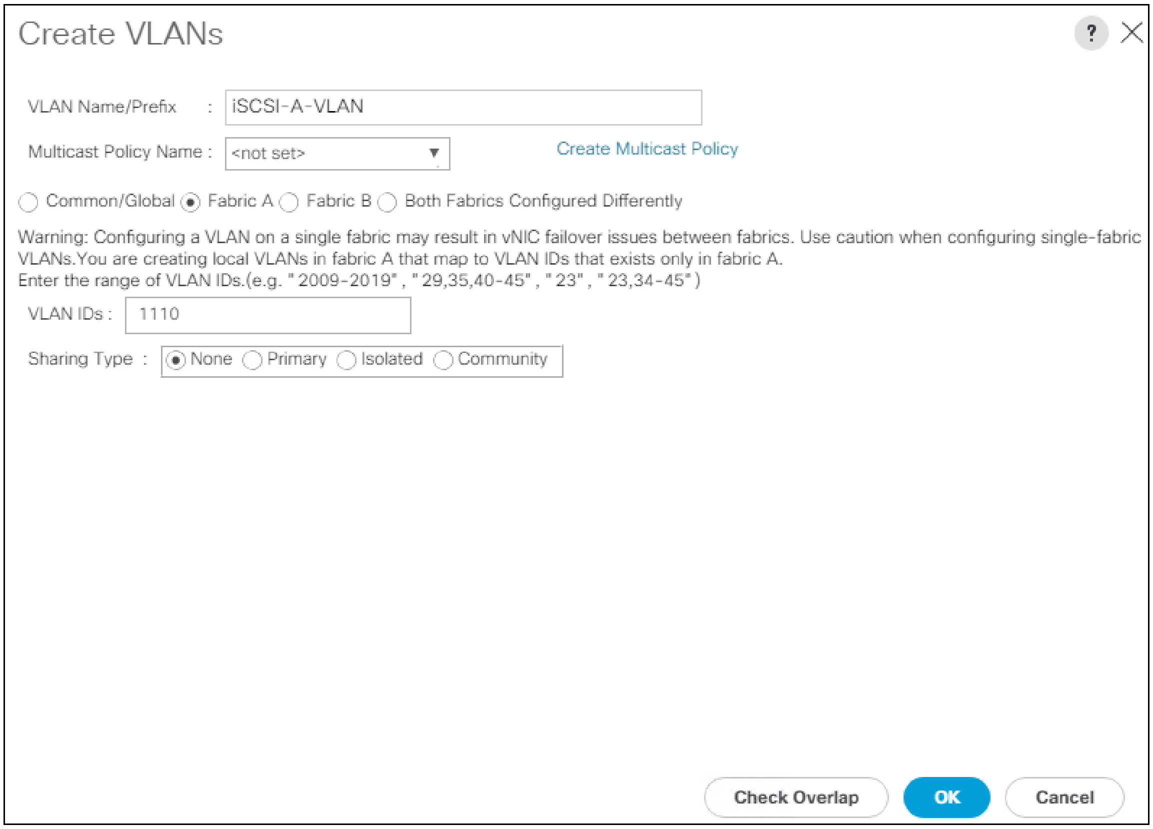
● Common/Global ○ Fabric A ○ Fabric B ○ Both Fabrics Configured Differently

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

VLAN IDs : 1130

Sharing Type : ● None ○ Primary ○ Isolated ○ Community

25. Click OK and then click OK again.
26. Right-click VLANs.
27. Select Create VLANs.
28. Enter iSCSI-A-VLAN as the name of the VLAN to be used for iSCSI-A.
29. Keep the Common/Global option selected for the scope of the VLAN.
30. Enter the iSCSI-A VLAN ID.
31. Keep the Sharing Type as None.



Create VLANs

VLAN Name/Prefix : iSCSI-A-VLAN

Multicast Policy Name : <not set>

○ Common/Global ● Fabric A ○ Fabric B ○ Both Fabrics Configured Differently

Warning: Configuring a VLAN on a single fabric may result in vNIC failover issues between fabrics. Use caution when configuring single-fabric VLANs.You are creating local VLANs in fabric A that map to VLAN IDs that exists only in fabric A.
Enter the range of VLAN IDs.(e.g. " 2009-2019" , " 29,35,40-45" , " 23" , " 23,34-45")

VLAN IDs : 1110

Sharing Type : ● None ○ Primary ○ Isolated ○ Community

32. Click OK and then click OK again.

33. Right-click VLANs.

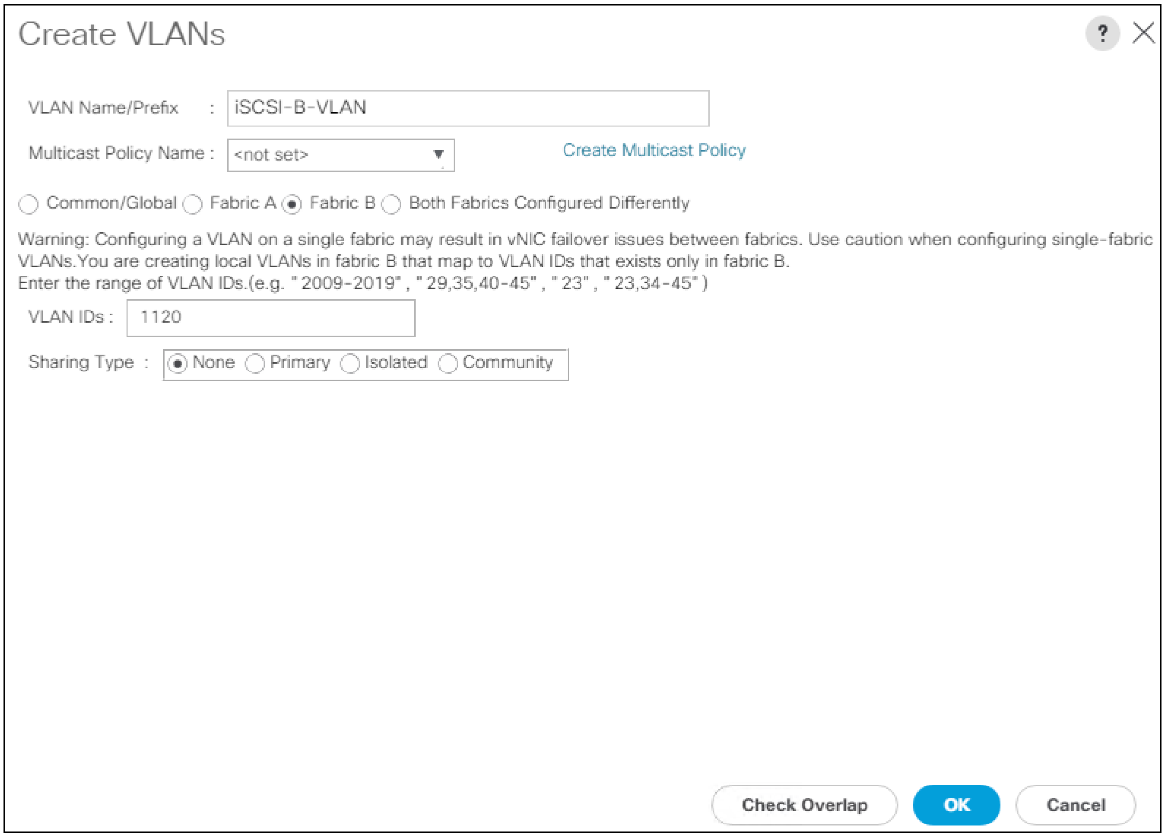
34. Select Create VLANs.

35. Enter iSCSI-B-VLAN as the name of the VLAN to be used for iSCSI-B.

36. Keep the Common/Global option selected for the scope of the VLAN.

37. Enter the iSCSI-B VLAN ID.

38. Keep the Sharing Type as None



Create VLANs

VLAN Name/Prefix : iSCSI-B-VLAN

Multicast Policy Name : <not set>

○ Common/Global ○ Fabric A ● Fabric B ○ Both Fabrics Configured Differently

Warning: Configuring a VLAN on a single fabric may result in vNIC failover issues between fabrics. Use caution when configuring single-fabric VLANs.You are creating local VLANs in fabric B that map to VLAN IDs that exists only in fabric B.
Enter the range of VLAN IDs.(e.g. " 2009-2019" , " 29,35,40-45" , " 23" , " 23,34-45")

VLAN IDs : 1120

Sharing Type : ● None ○ Primary ○ Isolated ○ Community

39. Click OK and then click OK again.

40. Right-click VLANs.

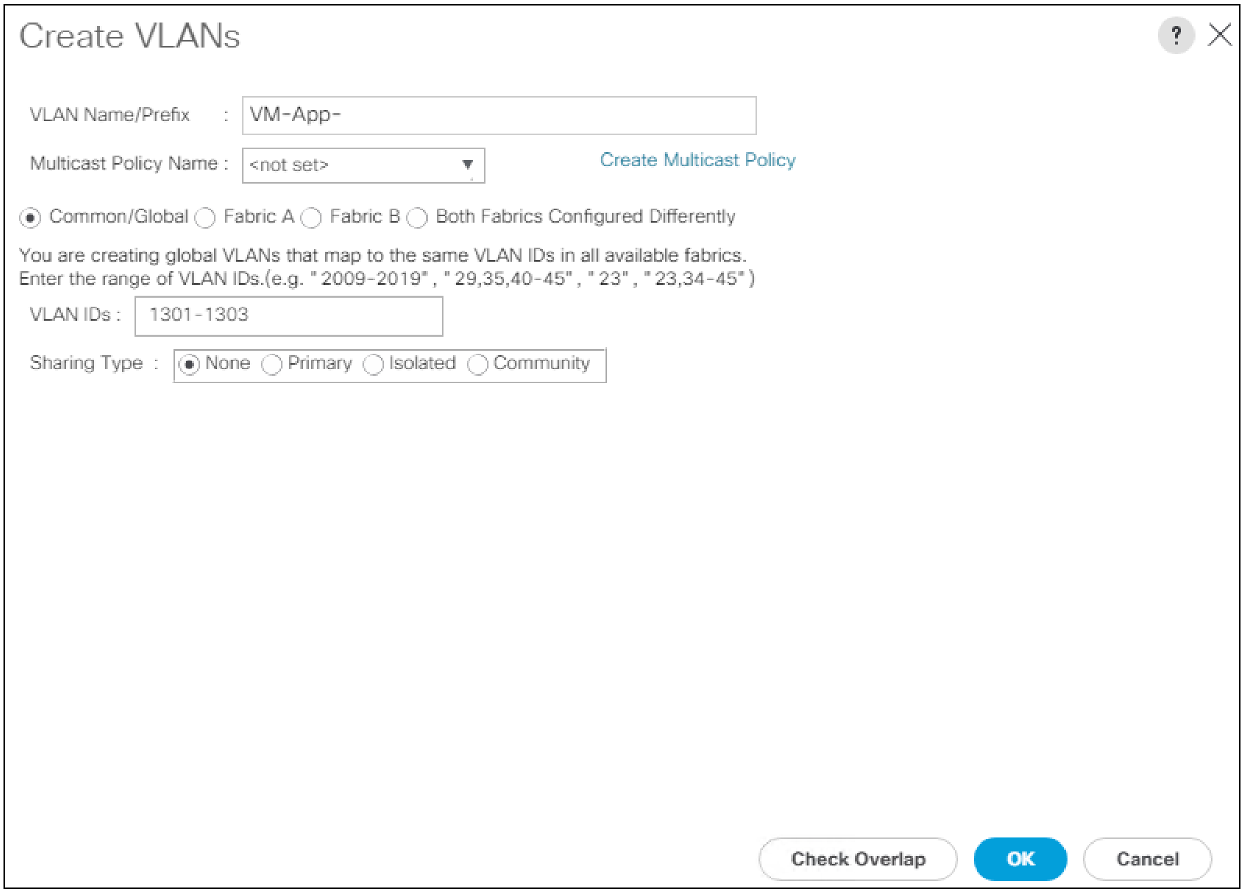
41. Select Create VLANs.

42. Enter VM-App- as the prefix of the VLANs to be used for VM Traffic.

43. Keep the Common/Global option selected for the scope of the VLAN.

44. Enter the VM-Traffic VLAN ID range.

45. Keep the Sharing Type as None.



VLAN Name/Prefix : VM-App-

Multicast Policy Name : <not set>

● Common/Global ○ Fabric A ○ Fabric B ○ Both Fabrics Configured Differently

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

VLAN IDs : 1301-1303

Sharing Type : ● None ○ Primary ○ Isolated ○ Community

46. Click OK and then click OK again.

47. Repeat as needed for any additional VLANs created on the upstream Nexus switches.

Create vNIC Templates

To create the multiple virtual network interface card (vNIC) templates for the Cisco UCS environment, follow the steps detailed below.

Create Management vNICs

For the vNIC_Mgmt_A Template, follow these steps:

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

2. Select Policies > root.

3. Right-click vNIC Templates.

4. Select Create vNIC Template.

5. Enter vNIC_Mgmt_A as the vNIC template name.

6. Keep Fabric A selected.

7. Select Primary Template for the Redundancy Type.

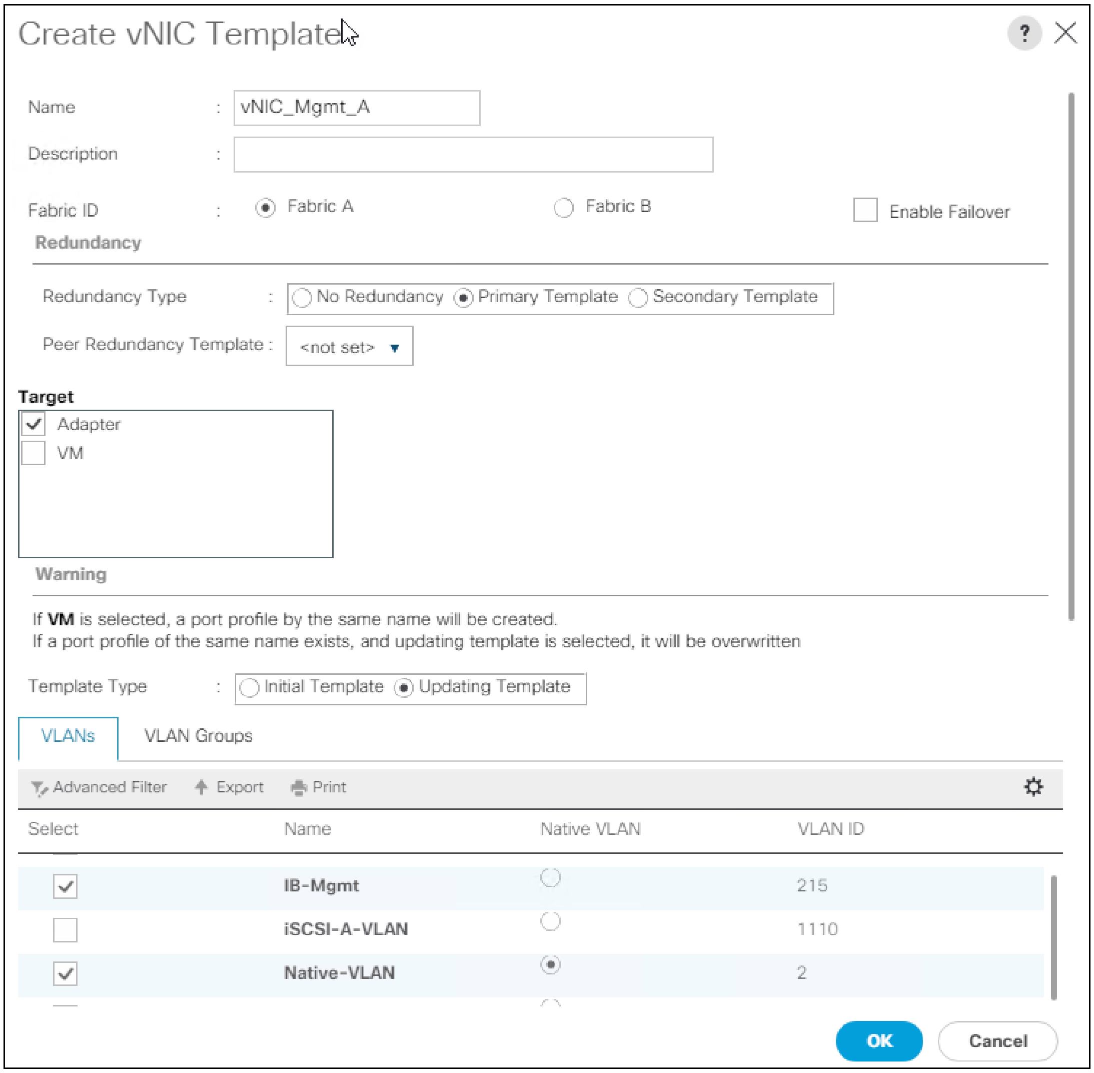
8. Leave Peer Redundancy Template as <not set>

Redundancy Type and specification of Redundancy Template are configuration options to later allow changes to the Primary Template to automatically adjust onto the Secondary Template.

9. Under Target, make sure that the VM checkbox is not selected.

10. Select Updating Template as the Template Type.

11. Under VLANs, select the checkboxes for IB-Mgmt and Native-VLAN VLANs.



Create vNIC Template

Name : vNIC_Mgmt_A

Description :

Fabric ID : ● Fabric A ○ Fabric B □ Enable Failover

Redundancy

Redundancy Type : ○ No Redundancy ● Primary Template ○ Secondary Template

Peer Redundancy Template : <not set>

Target

☑ Adapter
□ VM

Warning

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

Template Type : ○ Initial Template ● Updating Template

Select	Name	Native VLAN	VLAN ID
☑	IB-Mgmt	○	215
□	iSCSI-A-VLAN	○	1110
☑	Native-VLAN	●	2

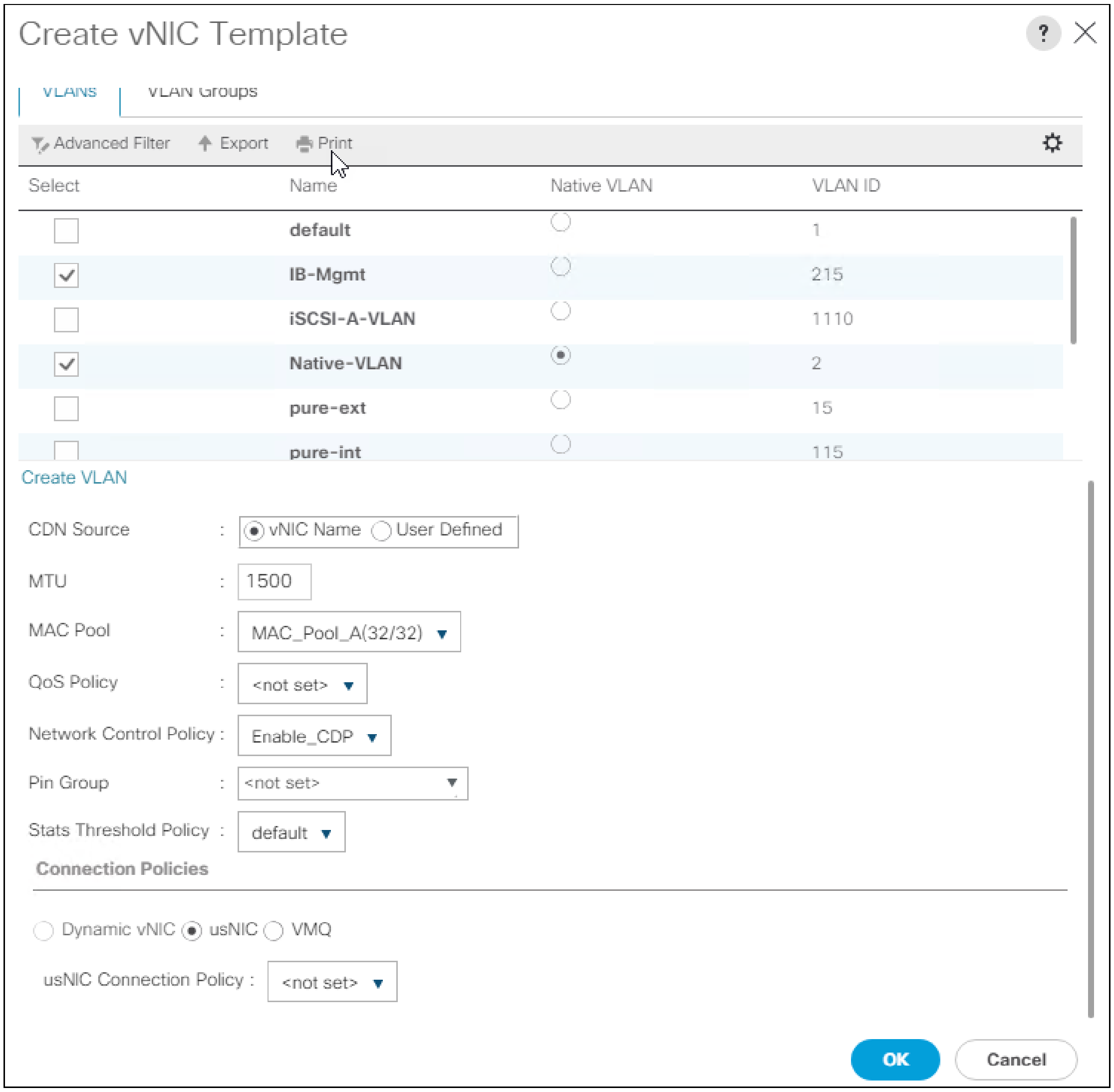
12. Set Native-VLAN as the native VLAN.

13. Leave vNIC Name selected for the CDN Source.

14. Leave 1500 for the MTU.

15. In the MAC Pool list, select MAC_Pool_A.

16. In the Network Control Policy list, select Enable_CDP.



Select	Name	Native VLAN	VLAN ID
□	default	○	1
☑	IB-Mgmt	○	215
□	iSCSI-A-VLAN	○	1110
☑	Native-VLAN	●	2
□	pure-ext	○	15
□	pure-int	○	115

CDN Source : ● vNIC Name ○ User Defined

MTU : 1500

MAC Pool : MAC_Pool_A(32/32)

QoS Policy : <not set>

Network Control Policy : Enable_CDP

Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

○ Dynamic vNIC ● usNIC ○ VMQ

usNIC Connection Policy : <not set>

17. Click OK to create the vNIC template.

18. Click OK.

For the vNIC_Mgmt_B Template, follow these steps:

1. In the navigation pane, select the LAN tab.

2. Select Policies > root.

3. Right-click vNIC Templates.

4. Select Create vNIC Template

5. Enter `vNIC_Mgmt_B` as the vNIC template name.

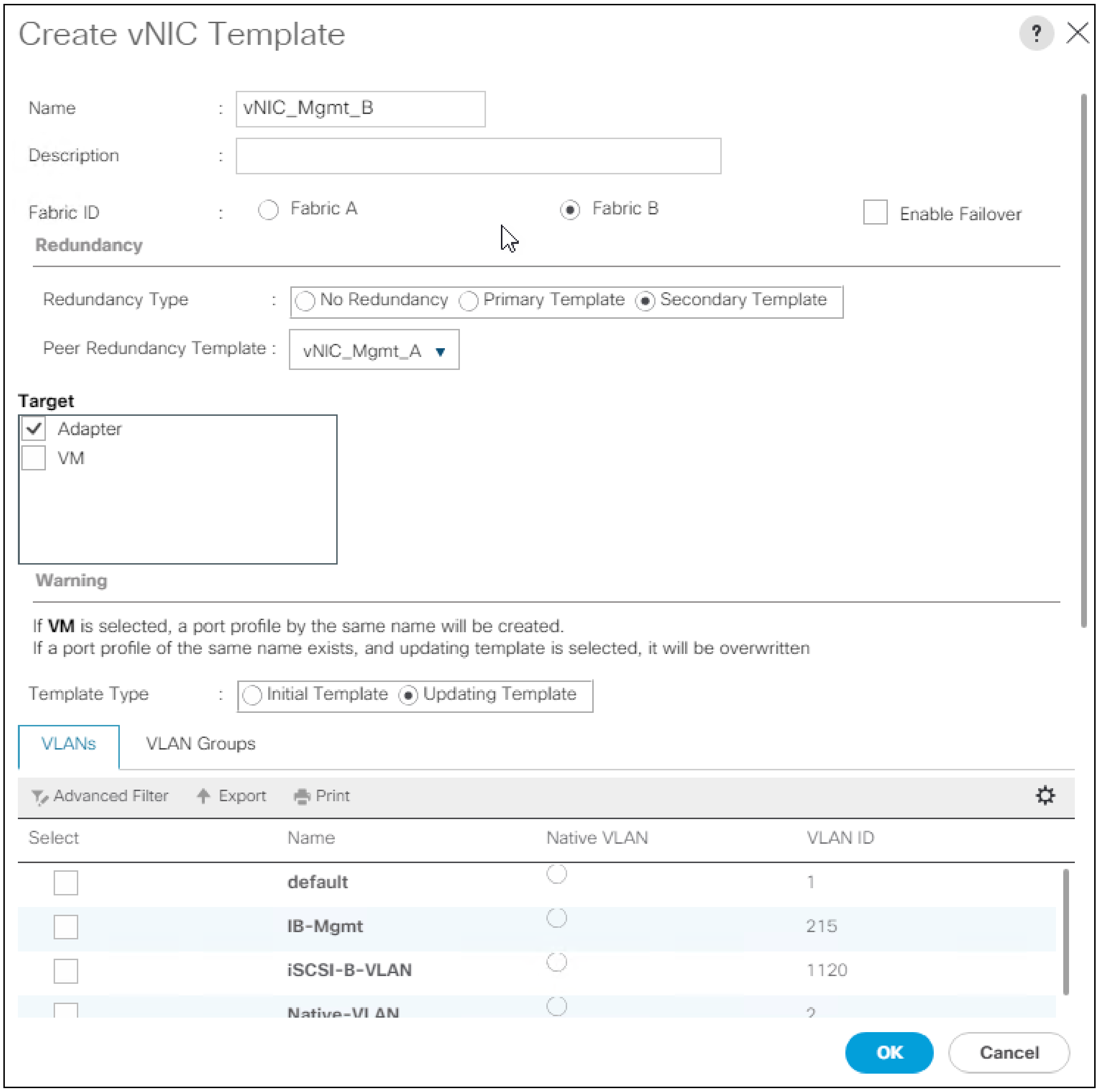
6. Select Fabric B.

7. Select Secondary Template for Redundancy Type.

8. For the Peer Redundancy Template drop-down, select vNIC_Mgmt_A.

With Peer Redundancy Template selected, Failover specification, Template Type, VLANs, CDN Source, MTU, and Network Control Policy are all pulled from the Primary Template.

9. Under Target, make sure the VM checkbox is not selected.



Create vNIC Template

Name : vNIC_Mgmt_B

Description :

Fabric ID : ○ Fabric A ● Fabric B □ Enable Failover

Redundancy

Redundancy Type : ○ No Redundancy ○ Primary Template ● Secondary Template

Peer Redundancy Template : vNIC_Mgmt_A

Target

☑ Adapter

□ VM

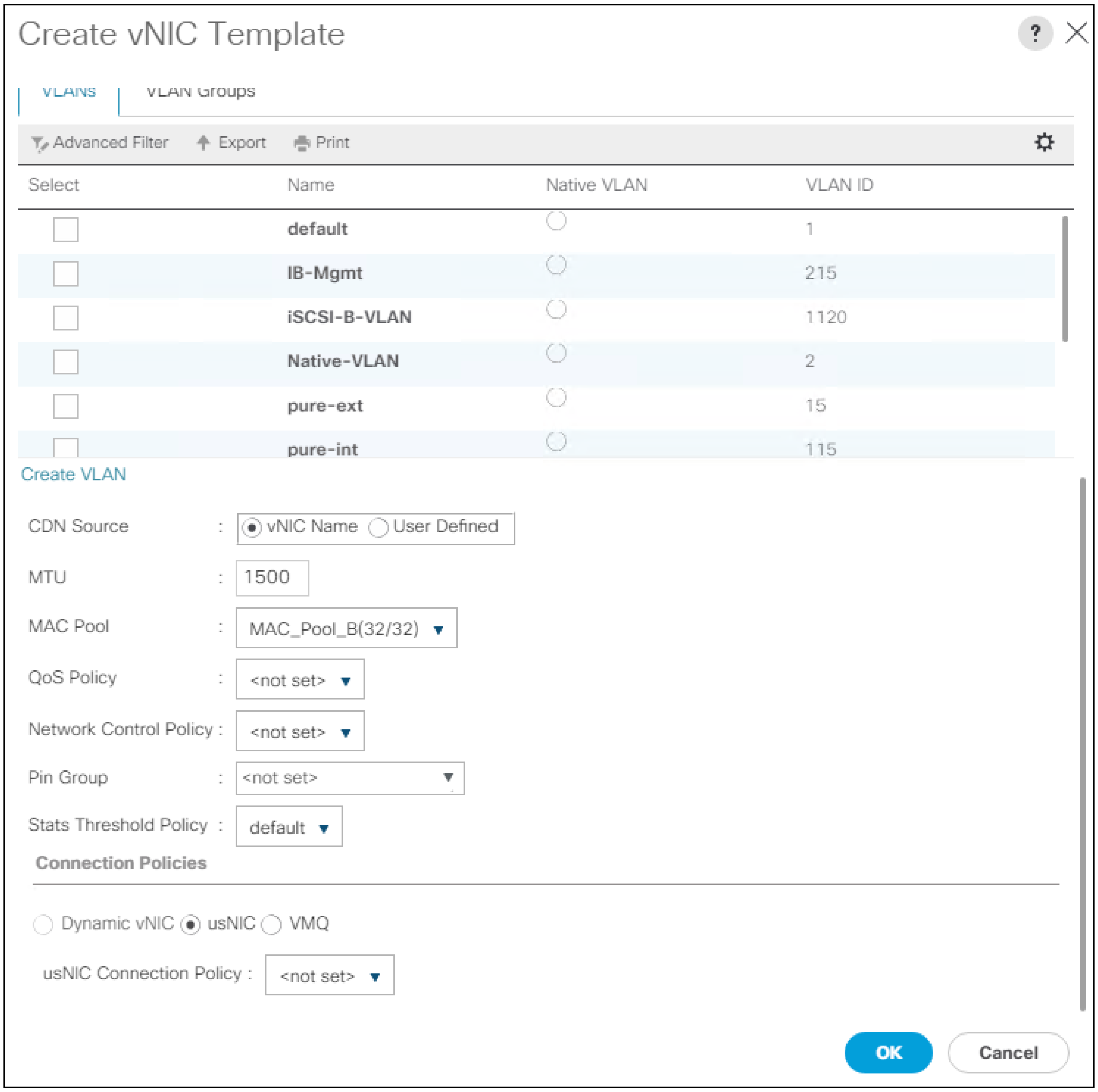
Warning

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

Template Type : ○ Initial Template ● Updating Template

Select	Name	Native VLAN	VLAN ID
□	default	○	1
□	IB-Mgmt	○	215
□	iSCSI-B-VLAN	○	1120
□	Native-VLAN	○	2

10. In the MAC Pool list, select MAC_Pool_B.



Create vNIC Template

Select	Name	Native VLAN	VLAN ID
□	default	○	1
□	IB-Mgmt	○	215
□	iSCSI-B-VLAN	○	1120
□	Native-VLAN	○	2
□	pure-ext	○	15
□	pure-int	○	115

CDN Source : ● vNIC Name ○ User Defined

MTU : 1500

MAC Pool : MAC_Pool_B(32/32)

QoS Policy : <not set>

Network Control Policy : <not set>

Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

○ Dynamic vNIC ● usNIC ○ VMQ

usNIC Connection Policy : <not set>

11. Click OK to create the vNIC template.

12. Click OK.

Create vMotion vNICs

For the vNIC_vMotion_A Template, follow these steps:

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

2. Select Policies > root.

3. Right-click vNIC Templates.

4. Select Create vNIC Template.

5. Enter `vNIC_vMotion_A` as the vNIC template name.

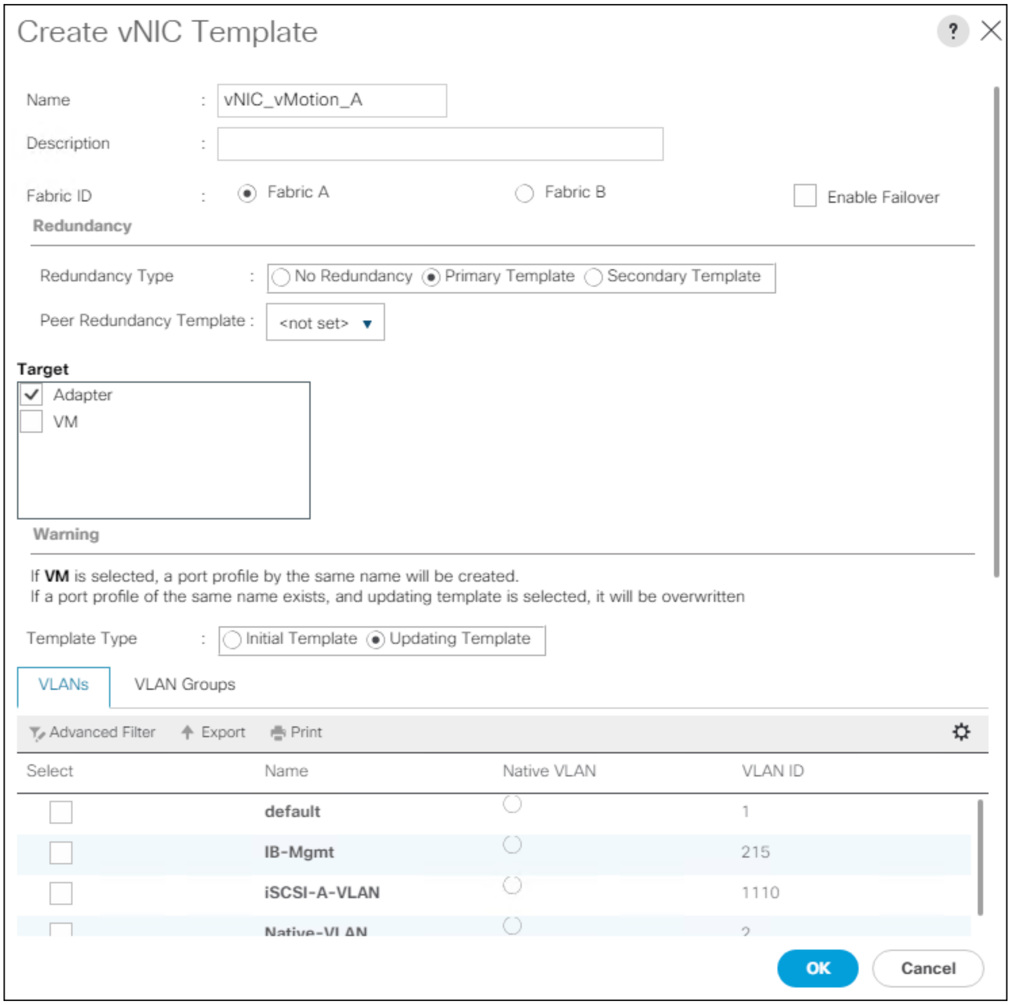
6. Keep Fabric A selected.

7. Select Primary Template for the Redundancy Type.

8. Leave Peer Redundancy Template as `<not set>`

9. Under Target, make sure that the VM checkbox is not selected.

10. Select Updating Template as the Template Type.



Create vNIC Template

Name : vNIC_vMotion_A

Description :

Fabric ID : ● Fabric A ○ Fabric B □ Enable Failover

Redundancy

Redundancy Type : ○ No Redundancy ● Primary Template ○ Secondary Template

Peer Redundancy Template : <not set>

Target

☑ Adapter
□ VM

Warning

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

Template Type : ○ Initial Template ● Updating Template

VLANs | VLAN Groups

Select	Name	Native VLAN	VLAN ID
□	**default**	○	1
□	**IB-Mgmt**	○	215
□	**iSCSI-A-VLAN**	○	1110
□	**Native-VLAN**	○	2

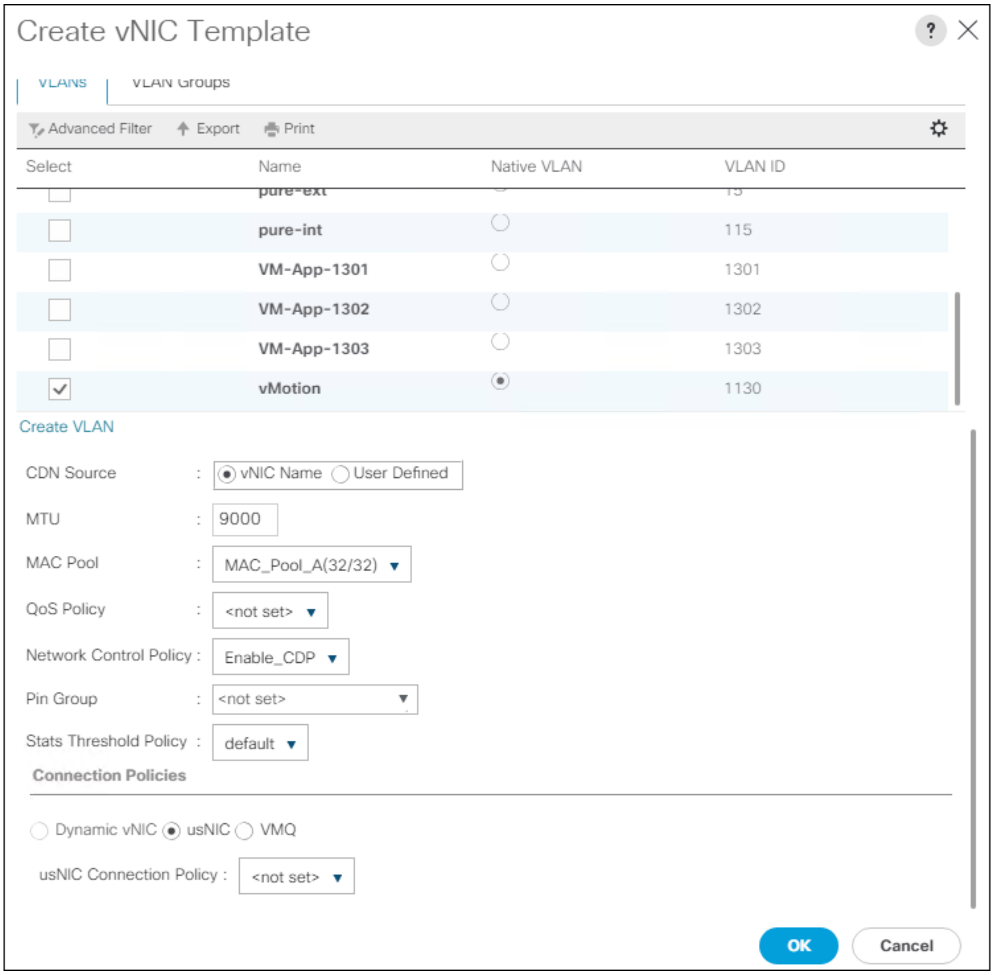
11. Under VLANs, select the checkboxes vMotion and Native-VLAN.

12. Set vMotion as the native VLAN.

13. For MTU, enter 9000.

14. In the MAC Pool list, select MAC_Pool_A.

15. In the Network Control Policy list, select Enable_CDP.



Create vNIC Template

Select	Name	Native VLAN	VLAN ID
□	pure-ext	○	15
□	pure-int	○	115
□	VM-App-1301	○	1301
□	VM-App-1302	○	1302
□	VM-App-1303	○	1303
☑	vMotion	●	1130

CDN Source : ● vNIC Name ○ User Defined

MTU : 9000

MAC Pool : MAC_Pool_A(32/32)

QoS Policy : <not set>

Network Control Policy : Enable_CDP

Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

○ Dynamic vNIC ● usNIC ○ VMQ

usNIC Connection Policy : <not set>

16. Click OK to create the vNIC template.

17. Click OK.

For the vNIC_vMotion_B Template, follow these steps:

1. In the navigation pane, select the LAN tab.

2. Select Policies > root.

3. Right-click vNIC Templates.

4. Select Create vNIC Template

5. Enter vNIC_vMotion_B as the vNIC template name.

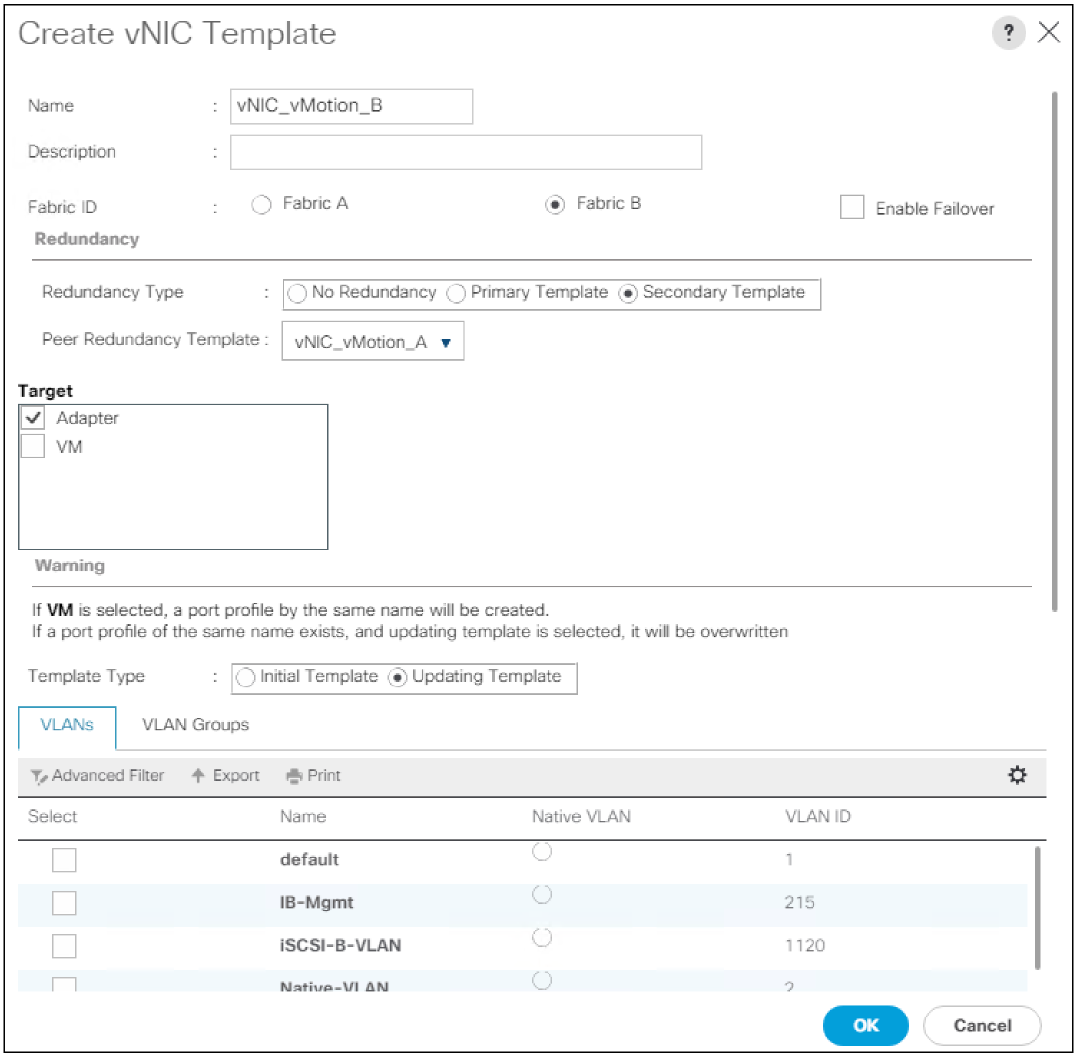
6. Select Fabric B.

7. Select Secondary Template for Redundancy Type.

8. For the Peer Redundancy Template drop-down, select vNIC_vMotion_A.

With Peer Redundancy Template selected, MAC Pool will be the main configuration option left for this vNIC template.

9. Under Target, make sure the VM checkbox is not selected.



Create vNIC Template

Name : vNIC_vMotion_B

Description :

Fabric ID : ○ Fabric A ● Fabric B □ Enable Failover

Redundancy

Redundancy Type : ○ No Redundancy ○ Primary Template ● Secondary Template

Peer Redundancy Template : vNIC_vMotion_A ▾

Target

☑ Adapter

□ VM

Warning

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

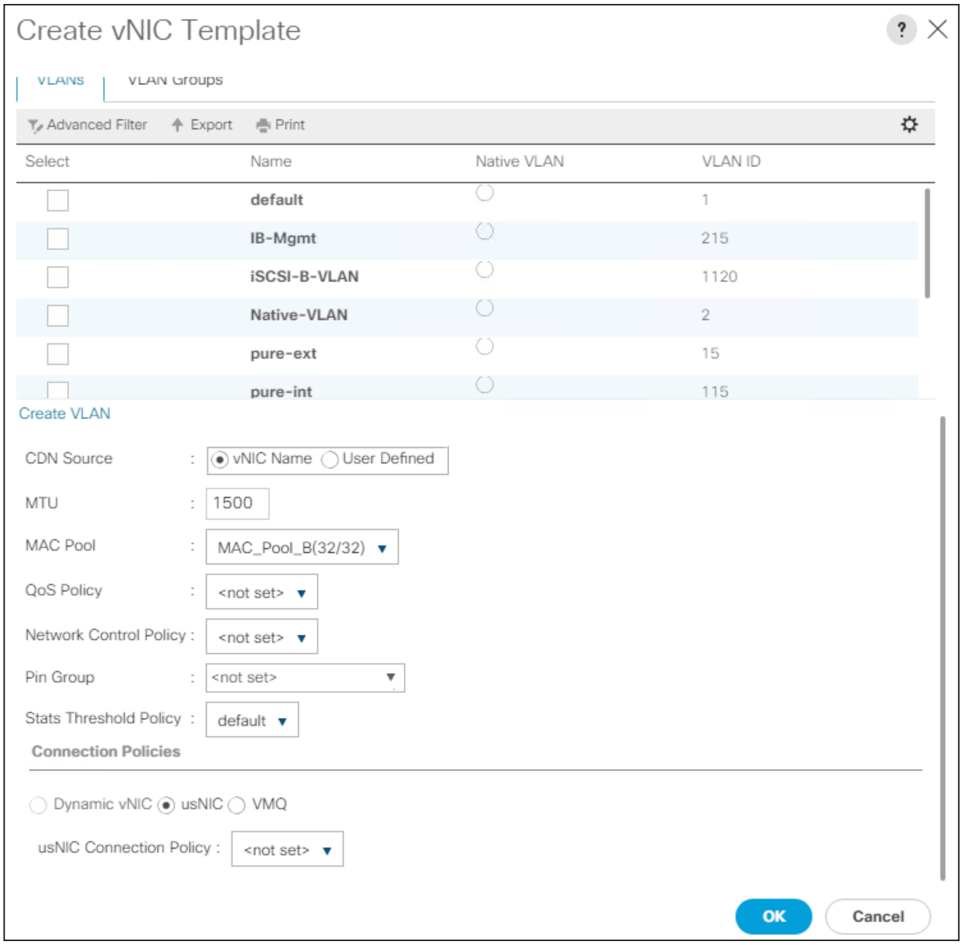
Template Type : ○ Initial Template ● Updating Template

VLANs | VLAN Groups

Advanced Filter | Export | Print

Select	Name	Native VLAN	VLAN ID
□	**default**	○	1
□	**IB-Mgmt**	○	215
□	**iSCSI-B-VLAN**	○	1120
□	**Native-VLAN**	○	2

10. In the MAC Pool list, select MAC_Pool_B.



Create vNIC Template

Select	Name	Native VLAN	VLAN ID
□	default	○	1
□	IB-Mgmt	○	215
□	iSCSI-B-VLAN	○	1120
□	Native-VLAN	○	2
□	pure-ext	○	15
□	pure-int	○	115

CDN Source : ● vNIC Name ○ User Defined

MTU : 1500

MAC Pool : MAC_Pool_B(32/32)

QoS Policy : <not set>

Network Control Policy : <not set>

Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

○ Dynamic vNIC ● usNIC ○ VMQ

usNIC Connection Policy : <not set>

11. Click OK to create the vNIC template.

12. Click OK.

Create Application vNICs

For the vNIC_App_A Template, follow these steps:

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

2. Select Policies > root.

3. Right-click vNIC Templates.

4. Select Create vNIC Template.

5. Enter vNIC_App_A as the vNIC template name.

6. Keep Fabric A selected.

7. Optional: select the Enable Failover checkbox.

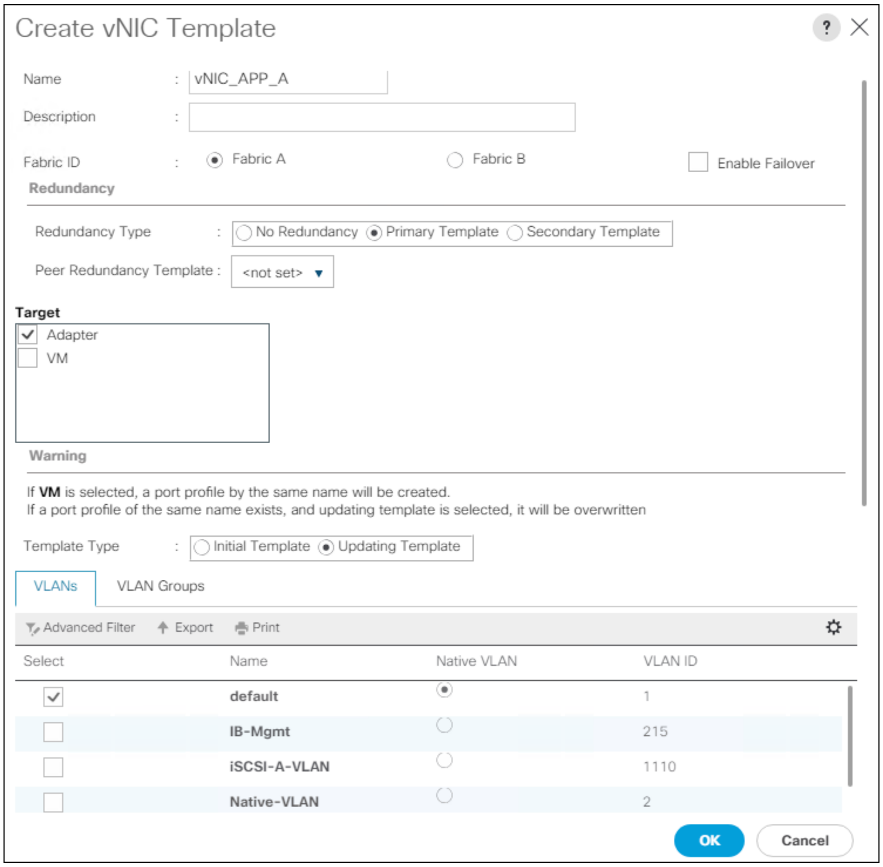
8. Select Primary Template for the Redundancy Type.

9. Leave Peer Redundancy Template as <not set>

10. Under Target, make sure that the VM checkbox is not selected.

11. Select Updating Template as the Template Type.

12. Set default as the native VLAN.



Create vNIC Template

Name : vNIC_APP_A

Description :

Fabric ID : ● Fabric A ○ Fabric B □ Enable Failover

Redundancy

Redundancy Type : ○ No Redundancy ● Primary Template ○ Secondary Template

Peer Redundancy Template : <not set>

Target

☑ Adapter
□ VM

Warning

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

Template Type : ○ Initial Template ● Updating Template

VLANs | VLAN Groups

Advanced Filter | Export | Print

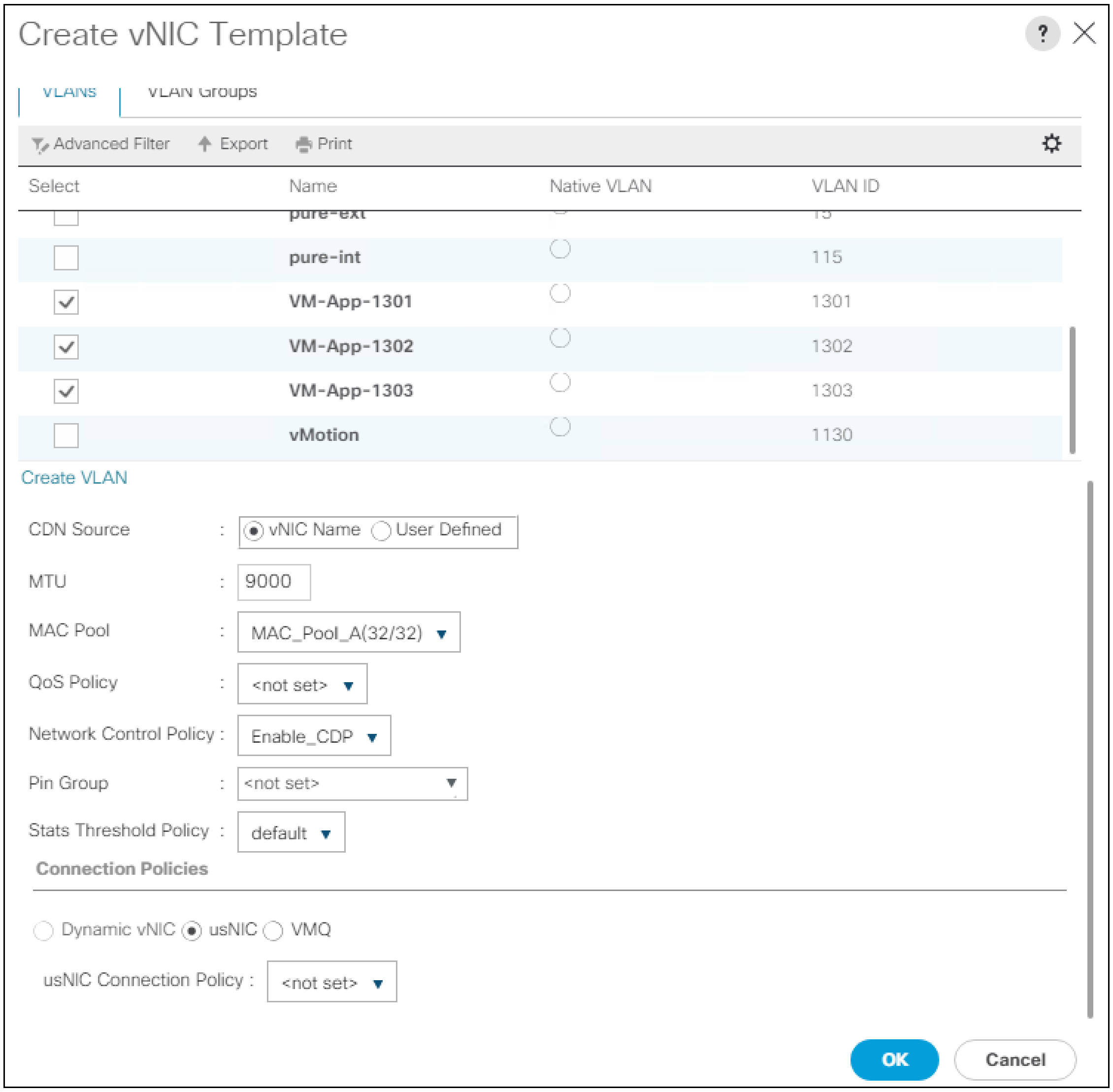
Select	Name	Native VLAN	VLAN ID
☑	**default**	●	1
□	**IB-Mgmt**	○	215
□	**iSCSI-A-VLAN**	○	1110
□	**Native-VLAN**	○	2

13. Under VLANs, select the checkboxes for any application or production VLANs that should be delivered to the ESXi hosts.

14. For MTU, enter 9000.

15. In the MAC Pool list, select MAC_Pool_A.

16. In the Network Control Policy list, select Enable_CDP.



Create vNIC Template

Select	Name	Native VLAN	VLAN ID
□	pure-ext	○	15
□	pure-int	○	115
☑	VM-App-1301	○	1301
☑	VM-App-1302	○	1302
☑	VM-App-1303	○	1303
□	vMotion	○	1130

CDN Source : ● vNIC Name ○ User Defined

MTU : 9000

MAC Pool : MAC_Pool_A(32/32)

QoS Policy : <not set>

Network Control Policy : Enable_CDP

Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

○ Dynamic vNIC ● usNIC ○ VMQ

usNIC Connection Policy : <not set>

17. Click OK to create the vNIC template.

18. Click OK.

For the vNIC_App_B Templates, follow these steps:

1. In the navigation pane, select the LAN tab.

2. Select Policies > root.

3. Right-click vNIC Templates.

4. Select Create vNIC Template

5. Enter vNIC_App_B as the vNIC template name.

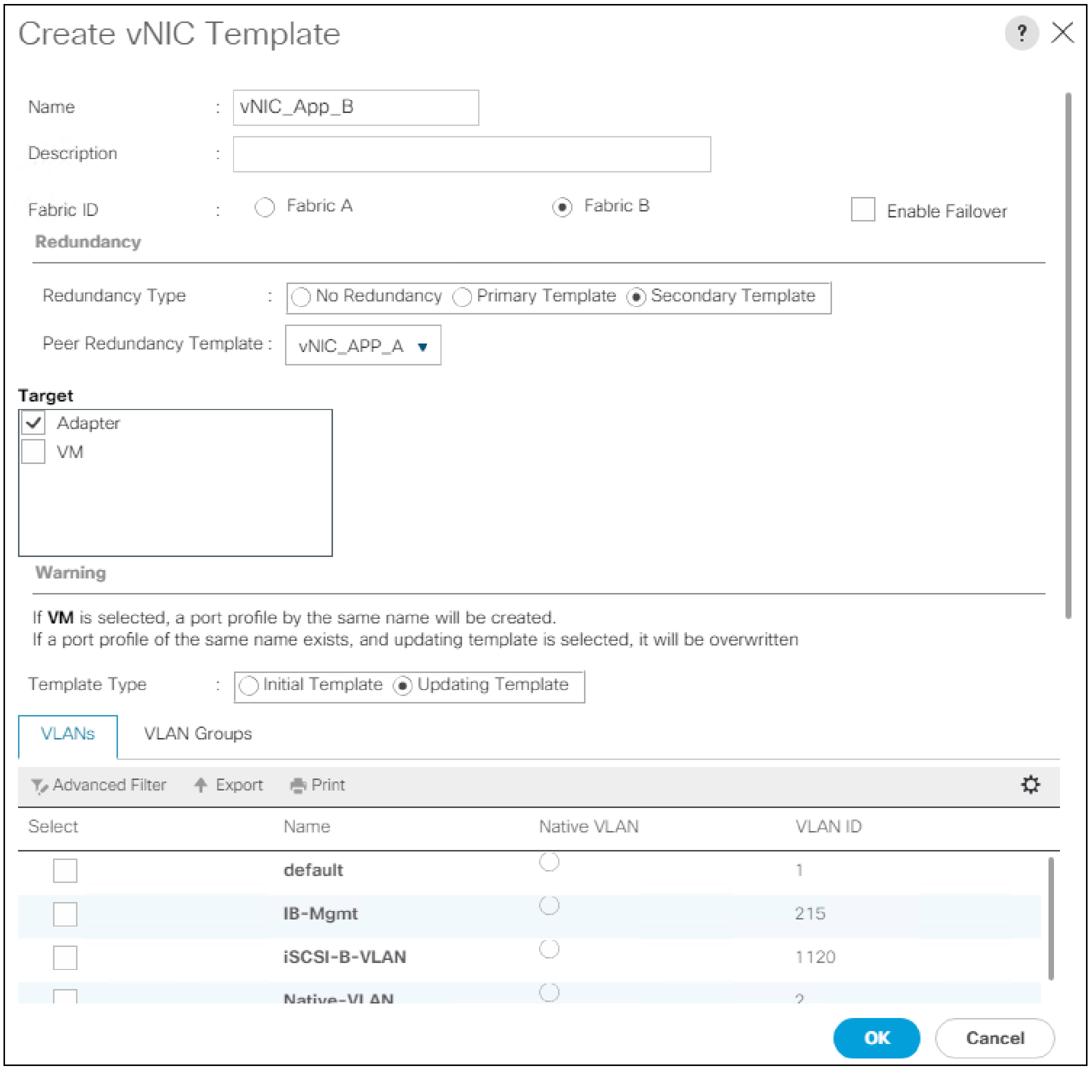
6. Select Fabric B.

7. Select Secondary Template for Redundancy Type.

8. For the Peer Redundancy Template drop-down, select vNIC_App_A.

With Peer Redundancy Template selected, MAC Pool will be the main configuration option left for this vNIC template.

9. Under Target, make sure the VM checkbox is not selected.



Create vNIC Template

Name : vNIC_App_B

Description :

Fabric ID : ○ Fabric A ● Fabric B □ Enable Failover

Redundancy

Redundancy Type : ○ No Redundancy ○ Primary Template ● Secondary Template

Peer Redundancy Template : vNIC_APP_A

Target

☑ Adapter

□ VM

Warning

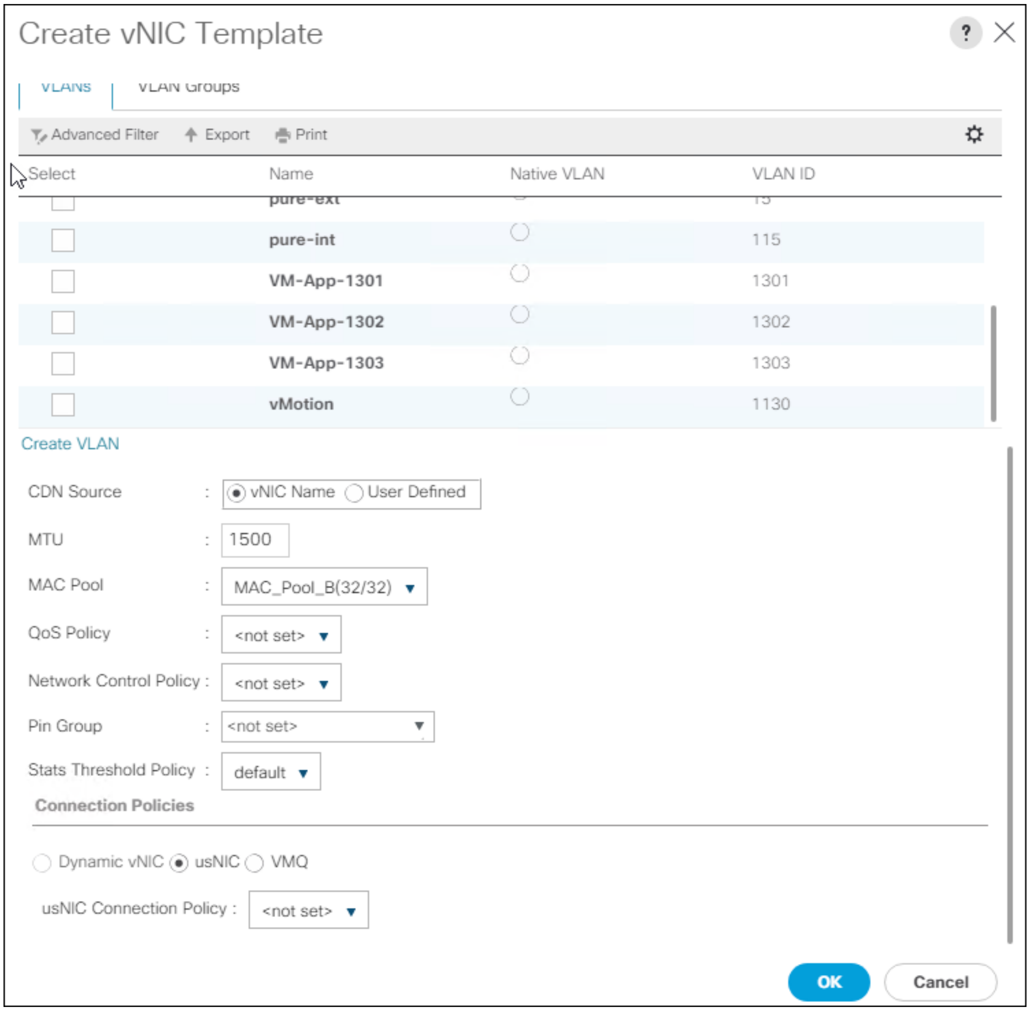
If **VM** is selected, a port profile by the same name will be created.
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type : ○ Initial Template ● Updating Template

VLANs | VLAN Groups

Select	Name	Native VLAN	VLAN ID
□	**default**	○	1
□	**IB-Mgmt**	○	215
□	**iSCSI-B-VLAN**	○	1120
□	**Native-VLAN**	○	2

10. In the MAC Pool list, select MAC_Pool_B.



Select	Name	Native VLAN	VLAN ID
□	pure-ext	○	15
□	pure-int	○	115
□	VM-App-1301	○	1301
□	VM-App-1302	○	1302
□	VM-App-1303	○	1303
□	vMotion	○	1130

CDN Source : ● vNIC Name ○ User Defined

MTU : 1500

MAC Pool : MAC_Pool_B(32/32)

QoS Policy : <not set>

Network Control Policy : <not set>

Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

○ Dynamic vNIC ● usNIC ○ VMQ

usNIC Connection Policy : <not set>

11. Click OK to create the vNIC template.

12. Click OK.

Create iSCSI vNICs

To create iSCSI vNICs, follow these steps:

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

2. Select Policies > root.

3. Right-click vNIC Templates.

4. Select Create vNIC Template.

5. Enter `vNIC_iSCSI_A` as the vNIC template name.

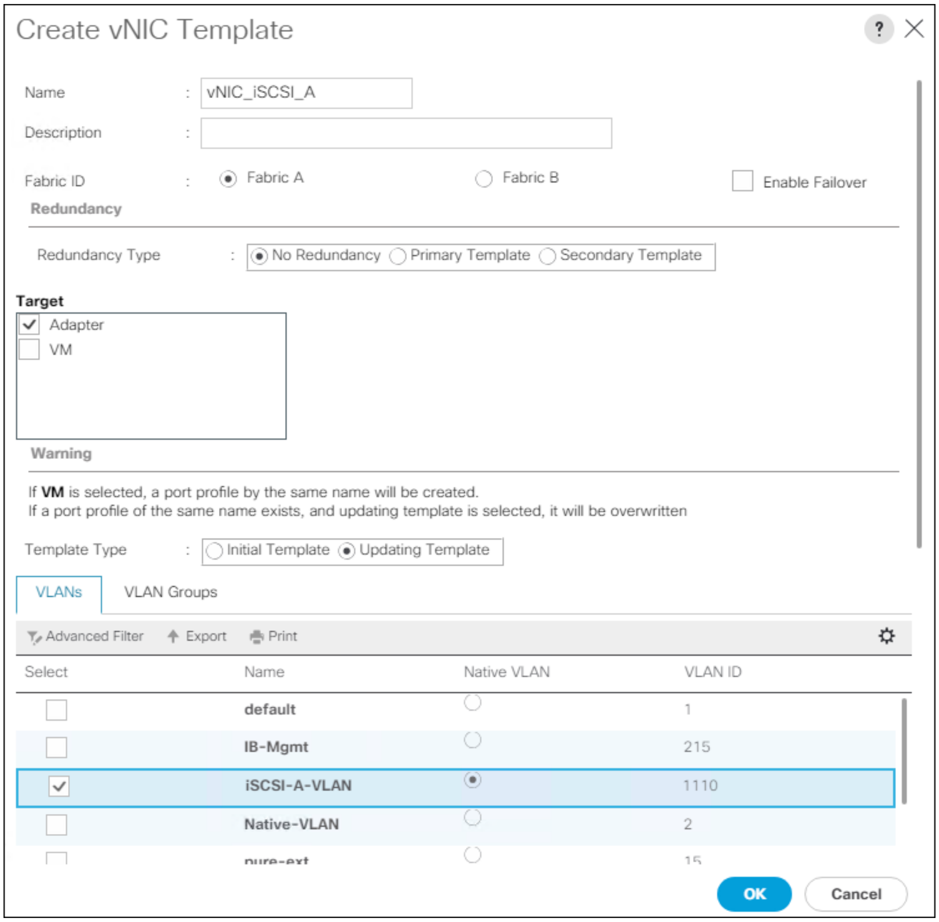
6. Keep Fabric A selected.

7. Keep the No Redundancy options selected for the Redundancy Type.

8. Under Target, make sure that the Adapter checkbox is selected.

9. Select Updating Template as the Template Type.

10. Under VLANs, select iSCSI-A-VLAN as the only VLAN and set it as the Native VLAN.



Create vNIC Template

Name : vNIC_iSCSI_A

Description :

Fabric ID : ● Fabric A ○ Fabric B □ Enable Failover

Redundancy

Redundancy Type : ● No Redundancy ○ Primary Template ○ Secondary Template

Target

☑ Adapter
□ VM

Warning

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

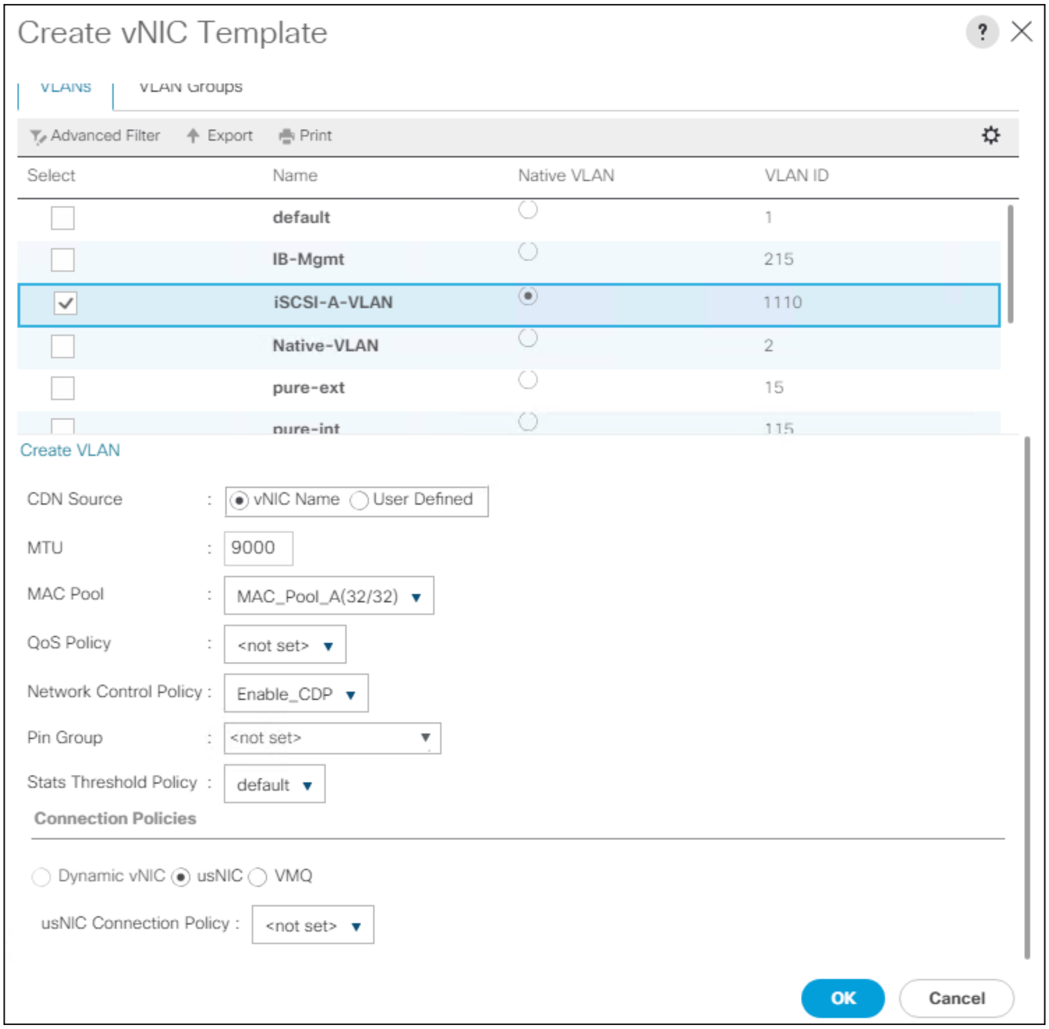
Template Type : ○ Initial Template ● Updating Template

Select	Name	Native VLAN	VLAN ID
□	default	○	1
□	IB-Mgmt	○	215
☑	iSCSI-A-VLAN	●	1110
□	Native-VLAN	○	2
□	pure-ext	○	15

11. For MTU, enter 9000.

12. In the MAC Pool list, select MAC_Pool_A.

13. In the Network Control Policy list, select Enable_CDP.



Select	Name	Native VLAN	VLAN ID
□	default	○	1
□	IB-Mgmt	○	215
☑	iSCSI-A-VLAN	●	1110
□	Native-VLAN	○	2
□	pure-ext	○	15
□	pure-int	○	115

CDN Source : ● vNIC Name ○ User Defined

MTU : 9000

MAC Pool : MAC_Pool_A(32/32)

QoS Policy : <not set>

Network Control Policy : Enable_CDP

Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

○ Dynamic vNIC ● usNIC ○ VMQ

usNIC Connection Policy : <not set>

14. Click OK to create the vNIC template.

15. Click OK.

For the vNIC_iSCSI_B Template, follow these steps:

1. In the navigation pane, select the LAN tab.

2. Select Policies > root.

3. Right-click vNIC Templates.

4. Select Create vNIC Template.

5. Enter `vNIC_iSCSI_B` as the vNIC template name.

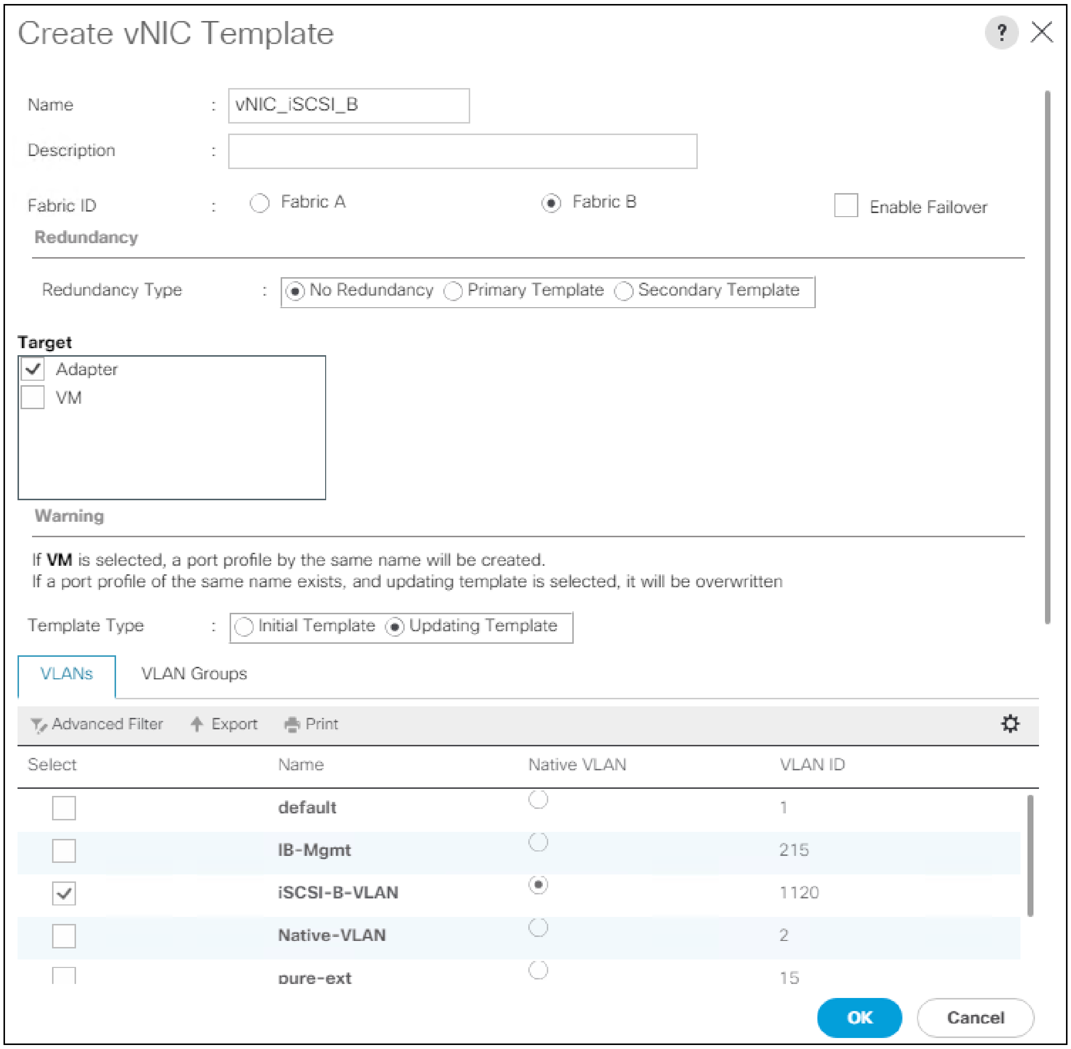
6. Keep Fabric B selected.

7. Keep the No Redundancy options selected for the Redundancy Type.

8. Under Target, make sure that the Adapter checkbox is selected.

9. Select Updating Template as the Template Type.

10. Under VLANs, select iSCSI-B-VLAN as the only VLAN and set it as the Native VLAN.



Create vNIC Template

Name : vNIC_iSCSI_B

Description :

Fabric ID : ○ Fabric A ● Fabric B □ Enable Failover

Redundancy

Redundancy Type : ● No Redundancy ○ Primary Template ○ Secondary Template

Target

☑ Adapter

□ VM

Warning

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

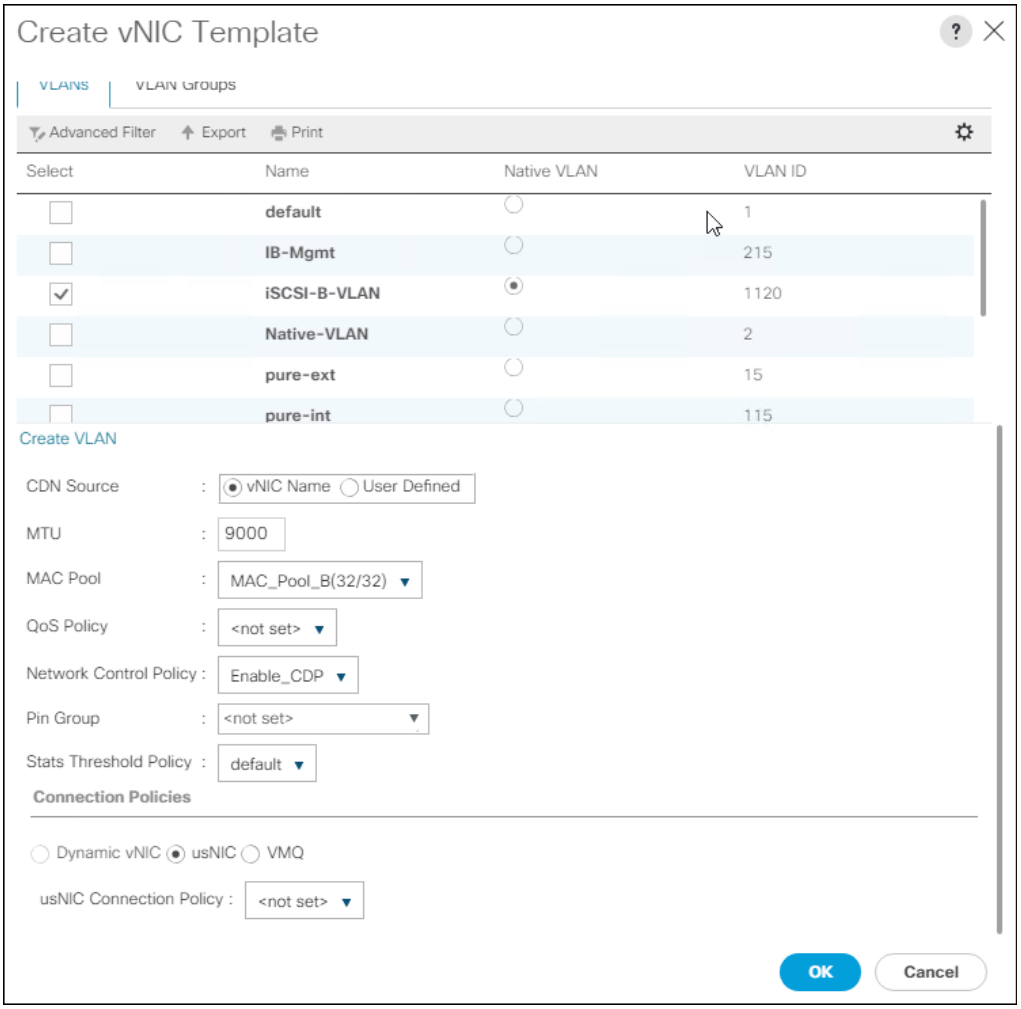
Template Type : ○ Initial Template ● Updating Template

Select	Name	Native VLAN	VLAN ID
□	default	○	1
□	IB-Mgmt	○	215
☑	iSCSI-B-VLAN	●	1120
□	Native-VLAN	○	2
□	pure-ext	○	15

11. For MTU, enter 9000.

12. In the MAC Pool list, select MAC_Pool_A.

13. In the Network Control Policy list, select Enable_CDP.



Create vNIC Template

Select	Name	Native VLAN	VLAN ID
□	default	○	1
□	IB-Mgmt	○	215
☑	iSCSI-B-VLAN	●	1120
□	Native-VLAN	○	2
□	pure-ext	○	15
□	pure-int	○	115

CDN Source : ● vNIC Name ○ User Defined

MTU : 9000

MAC Pool : MAC_Pool_B(32/32)

QoS Policy : <not set>

Network Control Policy : Enable_CDP

Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

○ Dynamic vNIC ● usNIC ○ VMQ

usNIC Connection Policy : <not set>

14. Click OK to create the vNIC template.

15. Click OK.

Create LAN Connectivity Policy

To configure the necessary iSCSI Infrastructure LAN Connectivity Policy, follow these steps:

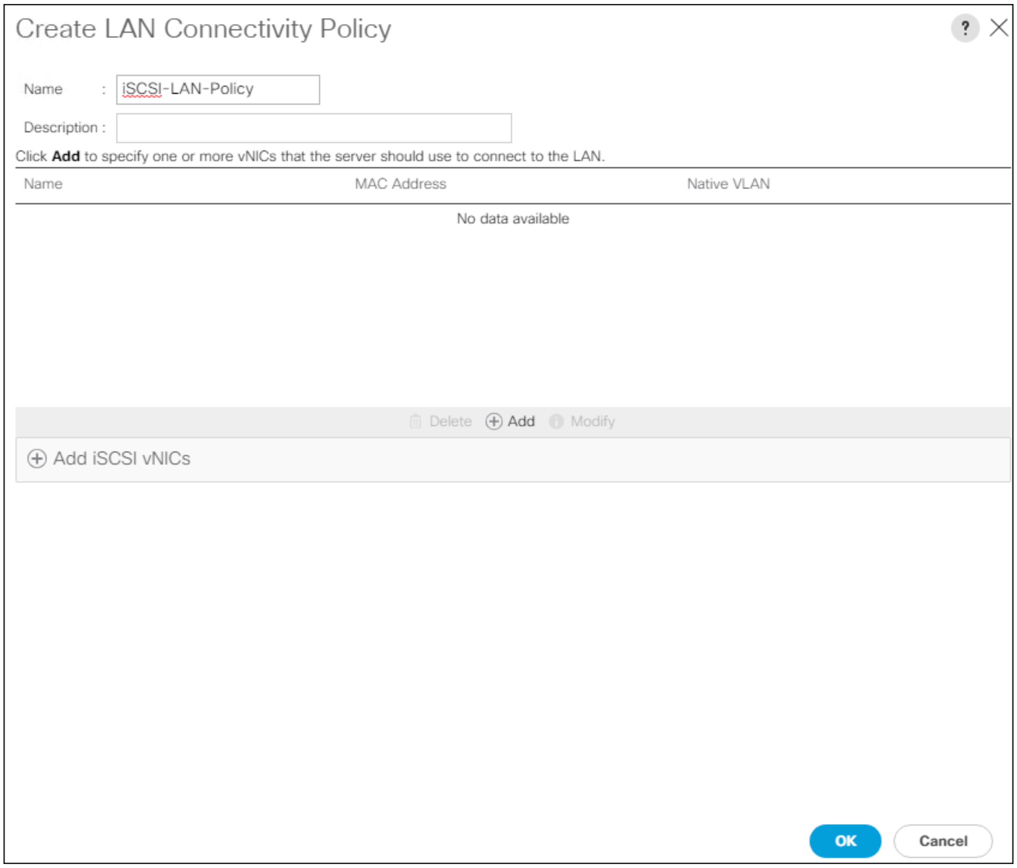
1. In Cisco UCS Manager, click LAN.

2. Select LAN > Policies > root.

3. Right-click LAN Connectivity Policies.

4. Select Create LAN Connectivity Policy.

5. Enter `iSCSI-LAN-Policy` as the name of the policy.



Create LAN Connectivity Policy

Name : iSCSI-LAN-Policy

Description :

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

Name	MAC Address	Native VLAN
No data available		

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

7. In the Create vNIC dialog box, enter `00-Mgmt-A` as the name of the vNIC.

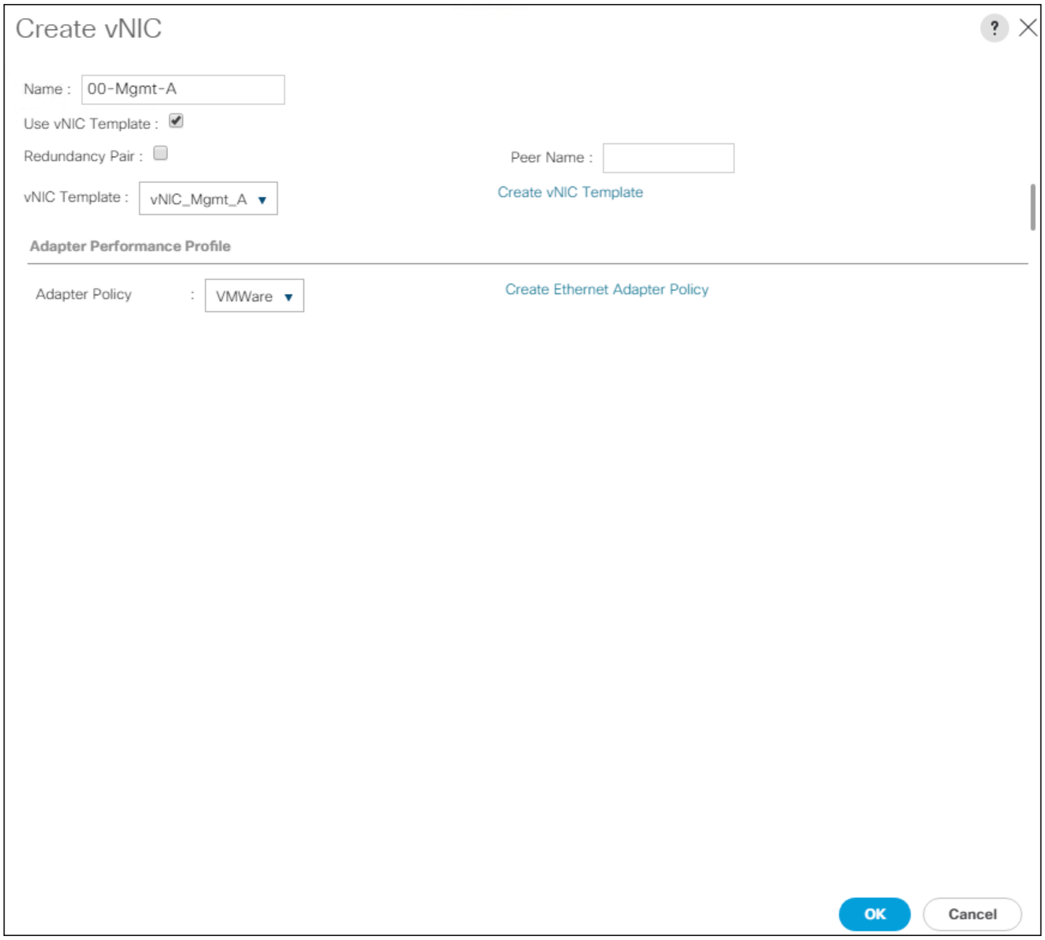
> The numeric prefix of "oo-" and subsequent increments on the later vNICs are used in the vNIC naming to force the device ordering through Consistent Device Naming (CDN). Without this, some operating systems might not respect the device ordering that is set within Cisco UCS.

8. Select the Use vNIC Template checkbox.

9. In the vNIC Template list, select oo-Mgmt-A.

10. In the Adapter Policy list, select VMWare.

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



Create vNIC

Name : 00-Mgmt-A

Use vNIC Template : ☑

Redundancy Pair : □

Peer Name :

vNIC Template : vNIC_Mgmt_A

Adapter Performance Profile

Adapter Policy : VMWare

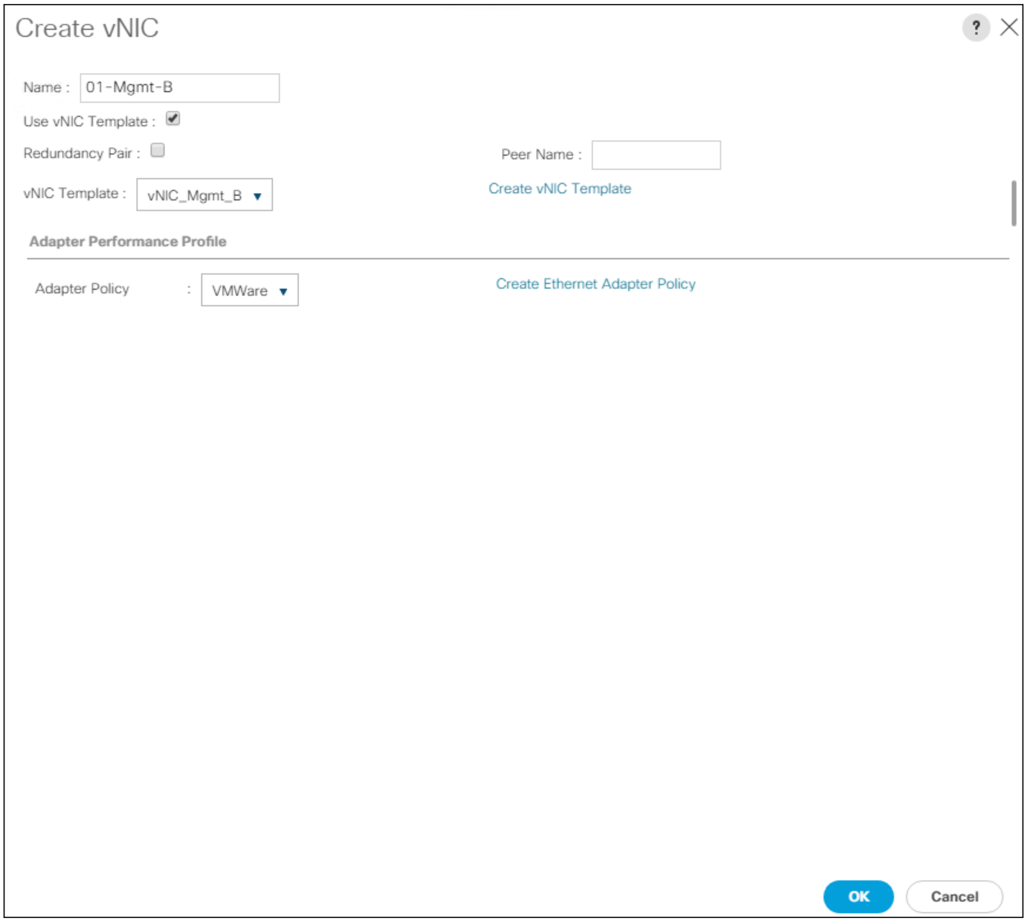
12. Click the upper Add button to add another vNIC to the policy.

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

14. Select the Use vNIC Template checkbox.

15. In the vNIC Template list, select 01-Mgmt-B.

16. In the Adapter Policy list, select VMWare.



Create vNIC

Name : 01-Mgmt-B

Use vNIC Template : ☑

Redundancy Pair : □

Peer Name :

vNIC Template : vNIC_Mgmt_B

Adapter Performance Profile

Adapter Policy : VMWare

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

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

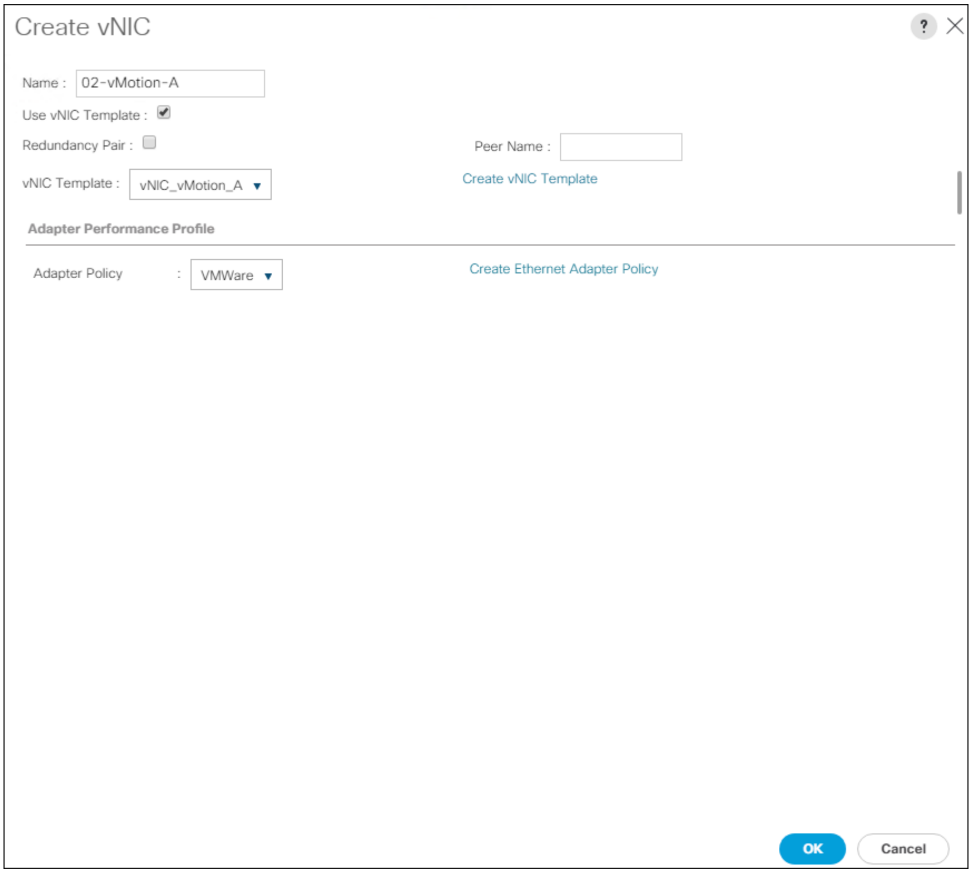
19. In the Create vNIC dialog box, enter 02-vMotion-A as the name of the vNIC.

20. Select the Use vNIC Template checkbox.

21. In the vNIC Template list, select vNIC_vMotion_A.

22. In the Adapter Policy list, select VMWare.

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



Create vNIC

Name : 02-vMotion-A

Use vNIC Template : ☑

Redundancy Pair : □

Peer Name :

vNIC Template : vNIC_vMotion_A

Adapter Performance Profile

Adapter Policy : VMWare

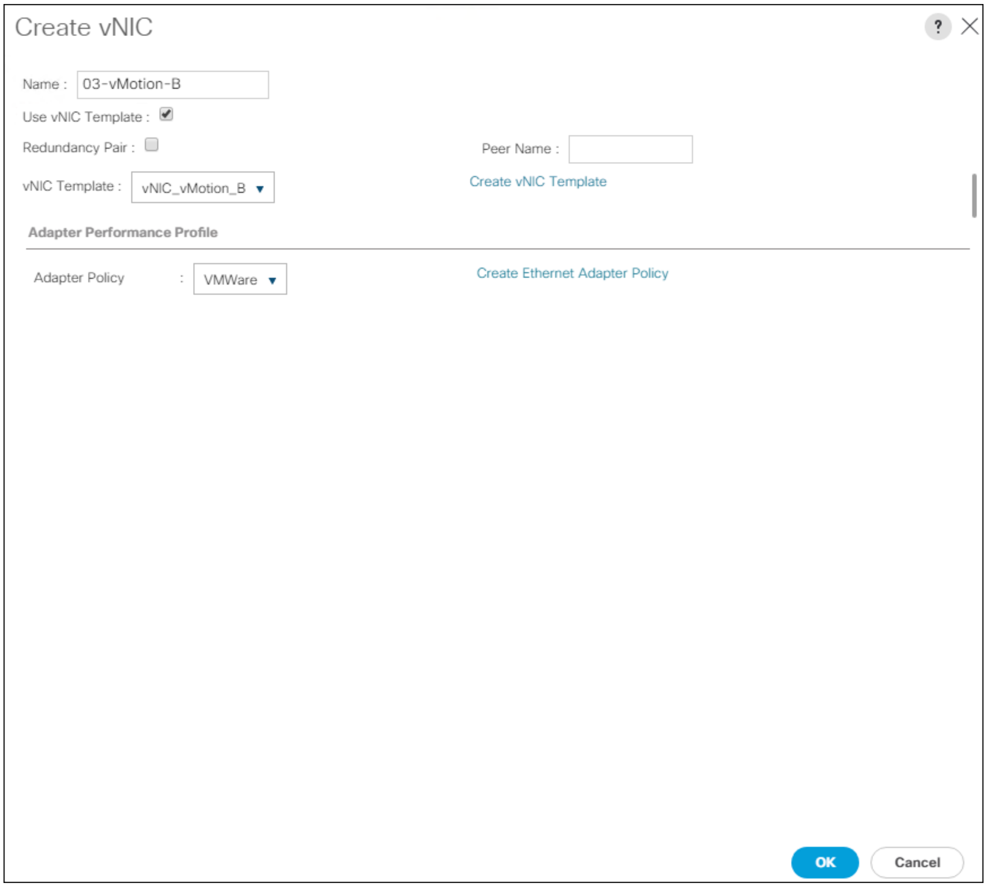
24. Click the upper Add button to add a vNIC to the policy.

25. In the Create vNIC dialog box, enter 03-vMotion-B as the name of the vNIC.

26. Select the Use vNIC Template checkbox.

27. In the vNIC Template list, select vNIC_vMotion_B.

28. In the Adapter Policy list, select VMWare.



Create vNIC

Name : 03-vMotion-B

Use vNIC Template : ☑

Redundancy Pair : □

Peer Name :

vNIC Template : vNIC_vMotion_B

Adapter Performance Profile

Adapter Policy : VMWare

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

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

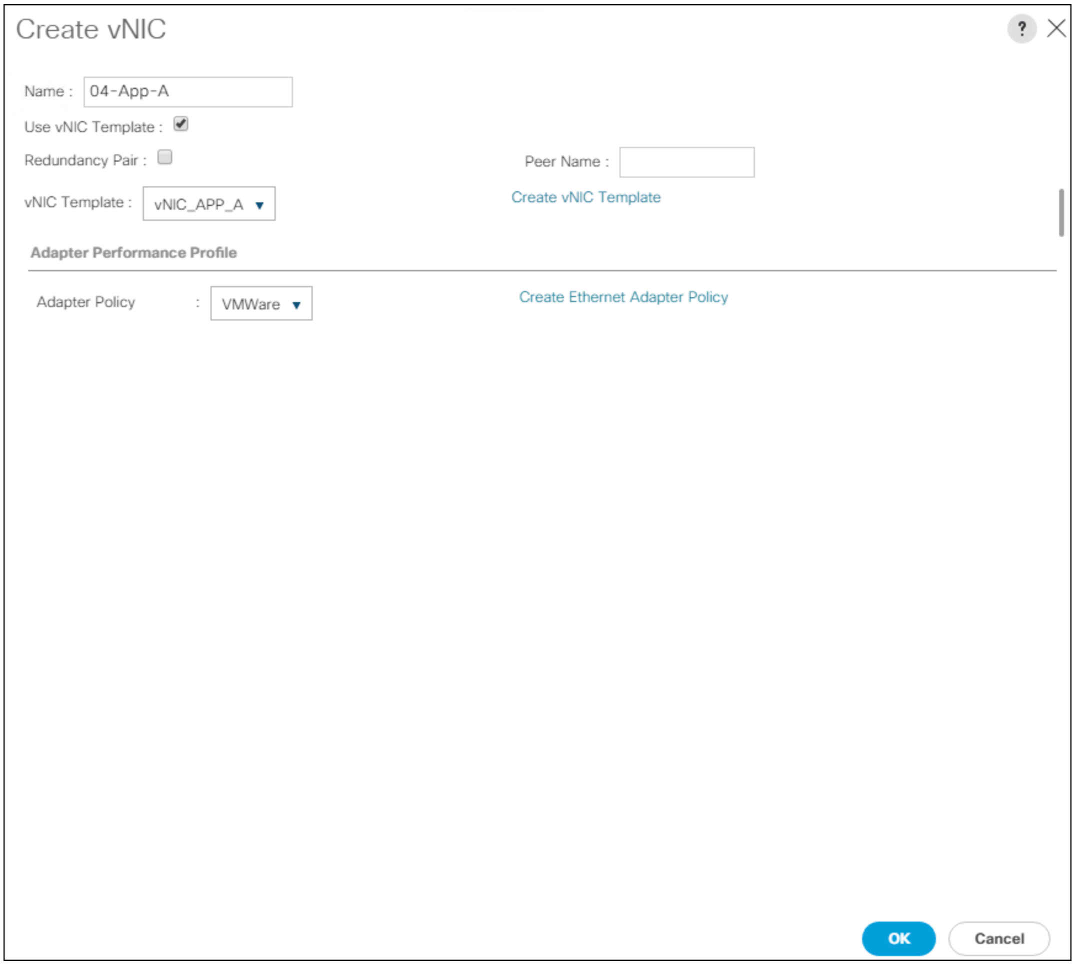
31. In the Create vNIC dialog box, enter 04-App-A as the name of the vNIC.

32. Select the Use vNIC Template checkbox.

33. In the vNIC Template list, select vNIC_App_A.

34. In the Adapter Policy list, select VMWare.

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



Create vNIC

Name : 04-App-A

Use vNIC Template : ☑

Redundancy Pair : □

Peer Name :

vNIC Template : vNIC_APP_A

Adapter Performance Profile

Adapter Policy : VMWare

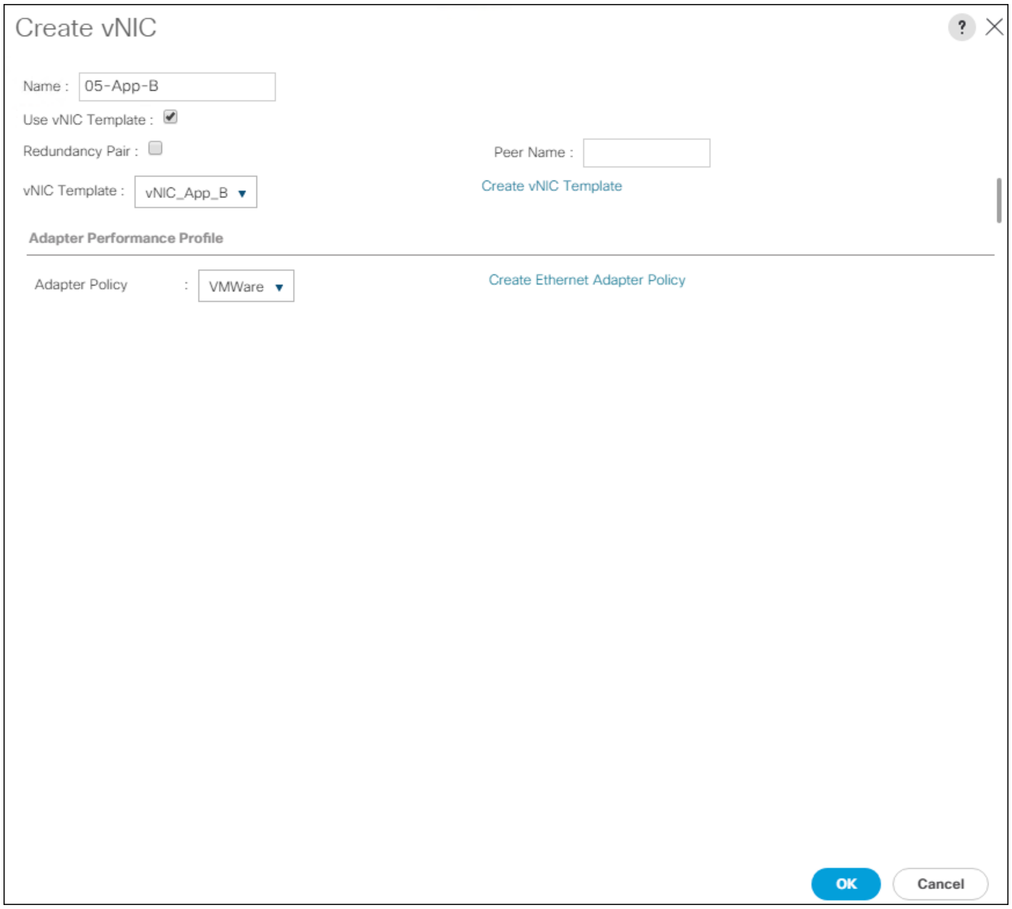
36. Click Add to add a vNIC to the policy.

37. In the Create vNIC dialog box, enter 05-App-B as the name of the vNIC.

38. Select the Use vNIC Template checkbox.

39. In the vNIC Template list, select vNIC_App_B.

40. In the Adapter Policy list, select VMWare.



Create vNIC

Name : 05-App-B

Use vNIC Template : ☑

Redundancy Pair : □

Peer Name :

vNIC Template : vNIC_App_B

Adapter Performance Profile

Adapter Policy : VMWare

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

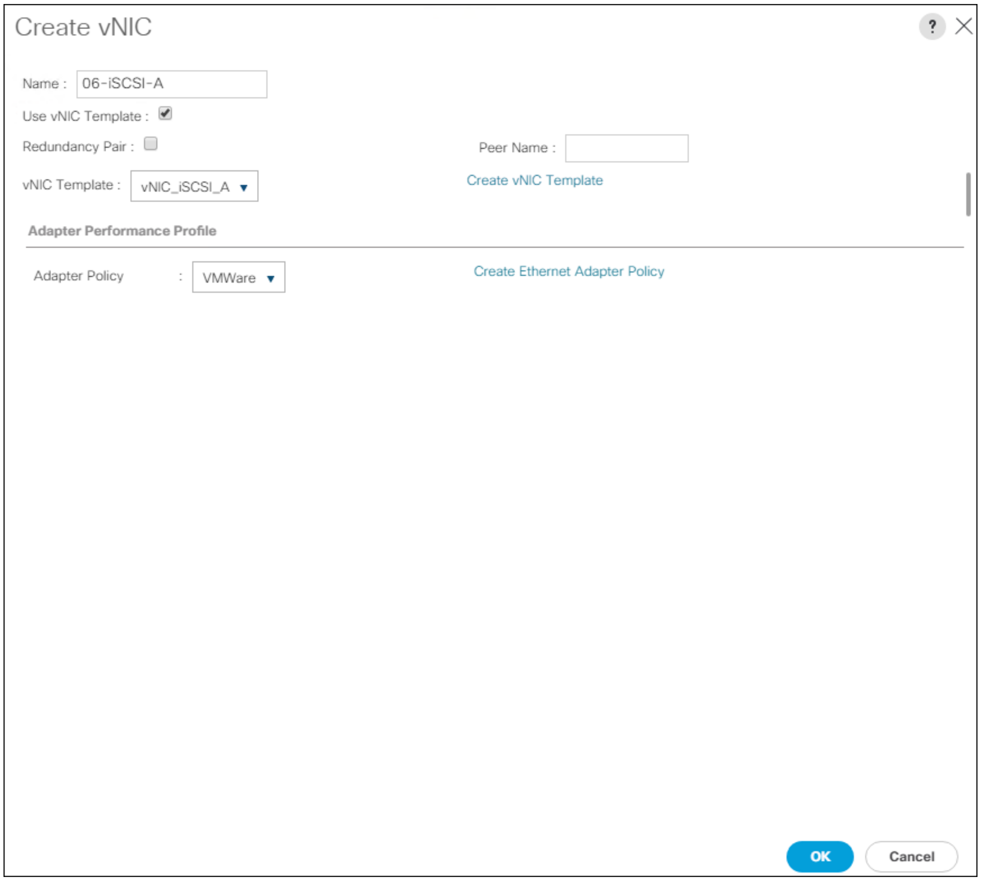
42. Click the upper Add button to add a vNIC.

43. In the Create vNIC dialog box, enter `06-iSCSI-A` as the name of the vNIC.

44. Select the Use vNIC Template checkbox.

45. In the vNIC Template list, select iSCSI-Template-A.

46. In the Adapter Policy list, select VMWare.



Create vNIC

Name : 06-iSCSI-A

Use vNIC Template : ☑

Redundancy Pair : □

Peer Name :

vNIC Template : vNIC_iSCSI_A

Adapter Policy : VMWare

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

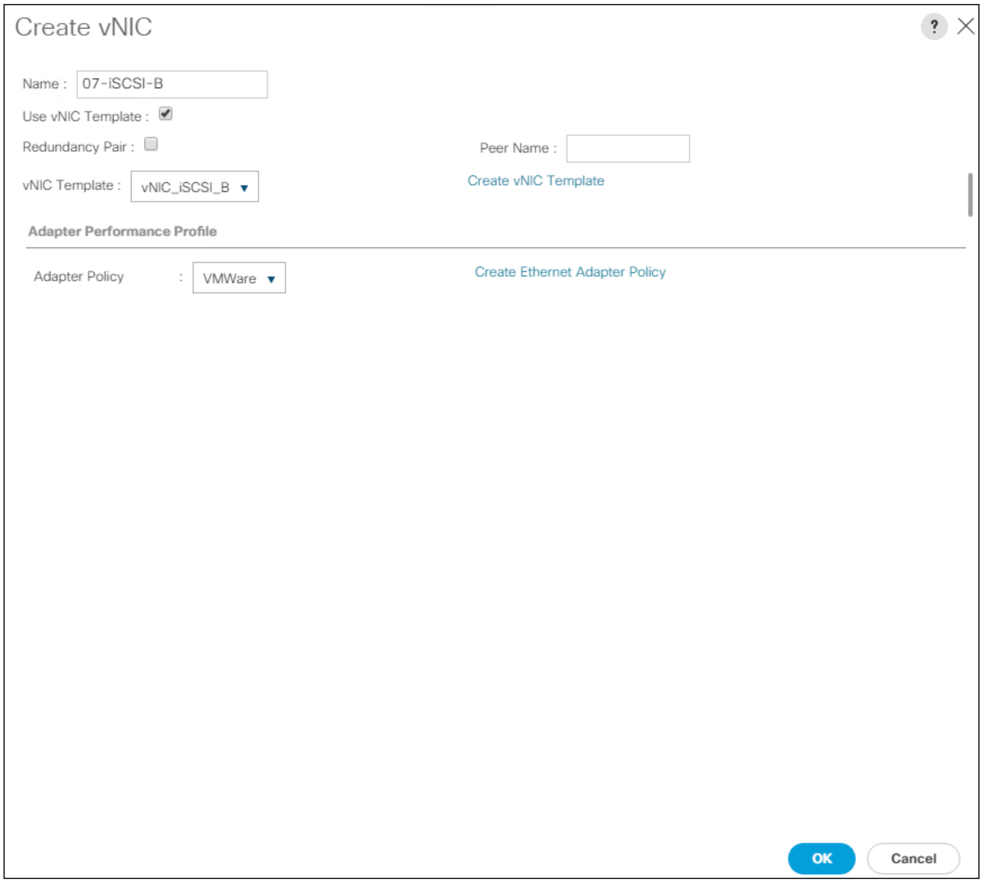
48. Click the upper Add button to add a vNIC to the policy.

49. In the Create vNIC dialog box, enter `07-iSCSI-B` as the name of the vNIC.

50. Select the Use vNIC Template checkbox.

51. In the vNIC Template list, select iSCSI-Template-B.

52. In the Adapter Policy list, select VMWare.



Create vNIC

Name : 07-iSCSI-B

Use vNIC Template : ☑

Redundancy Pair : □

Peer Name :

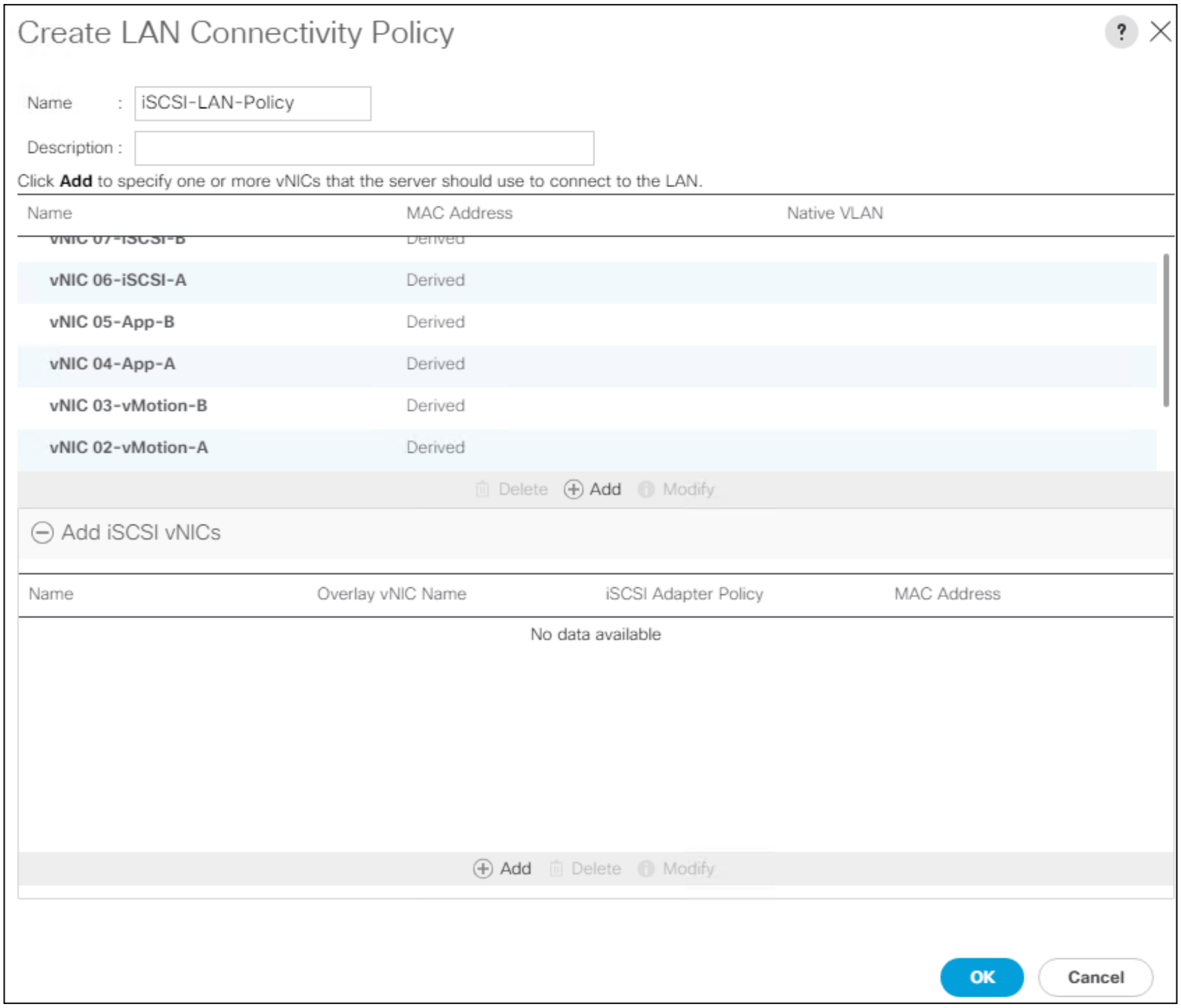
vNIC Template : vNIC_iSCSI_B

Adapter Performance Profile

Adapter Policy : VMWare

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

54. Expand the Add iSCSI vNICs.



Create LAN Connectivity Policy

Name : iSCSI-LAN-Policy

Description :

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

Name	MAC Address	Native VLAN
vNIC 07-iSCSI-B	Derived	
vNIC 06-iSCSI-A	Derived	
vNIC 05-App-B	Derived	
vNIC 04-App-A	Derived	
vNIC 03-vMotion-B	Derived	
vNIC 02-vMotion-A	Derived	

Add iSCSI vNICs

Name	Overlay vNIC Name	iSCSI Adapter Policy	MAC Address
No data available			

55. Select Add in the Add iSCSI vNICs section.

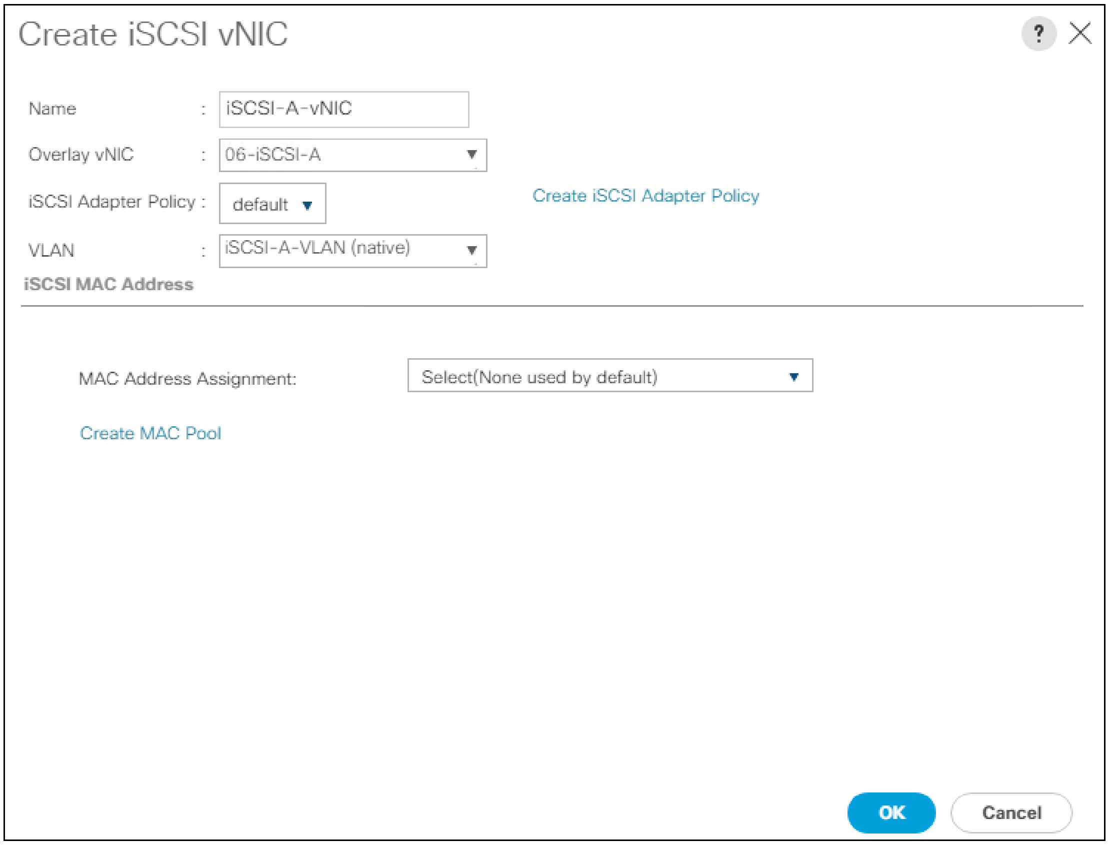
56. Set the name to iSCSI—A-vNIC.

57. Select the 06-iSCSI-A as Overlay vNIC.

58. Set the VLAN to iSCSI-A-VLAN (native).

59. Set the iSCSI Adapter Policy to default

60. Leave the MAC Address set to None.



Create iSCSI vNIC

Name : iSCSI-A-vNIC

Overlay vNIC : 06-iSCSI-A

iSCSI Adapter Policy : default

VLAN : iSCSI-A-VLAN (native)

iSCSI MAC Address

MAC Address Assignment: Select(None used by default)

61. Click OK.

62. Select Add in the Add iSCSI vNICs section.

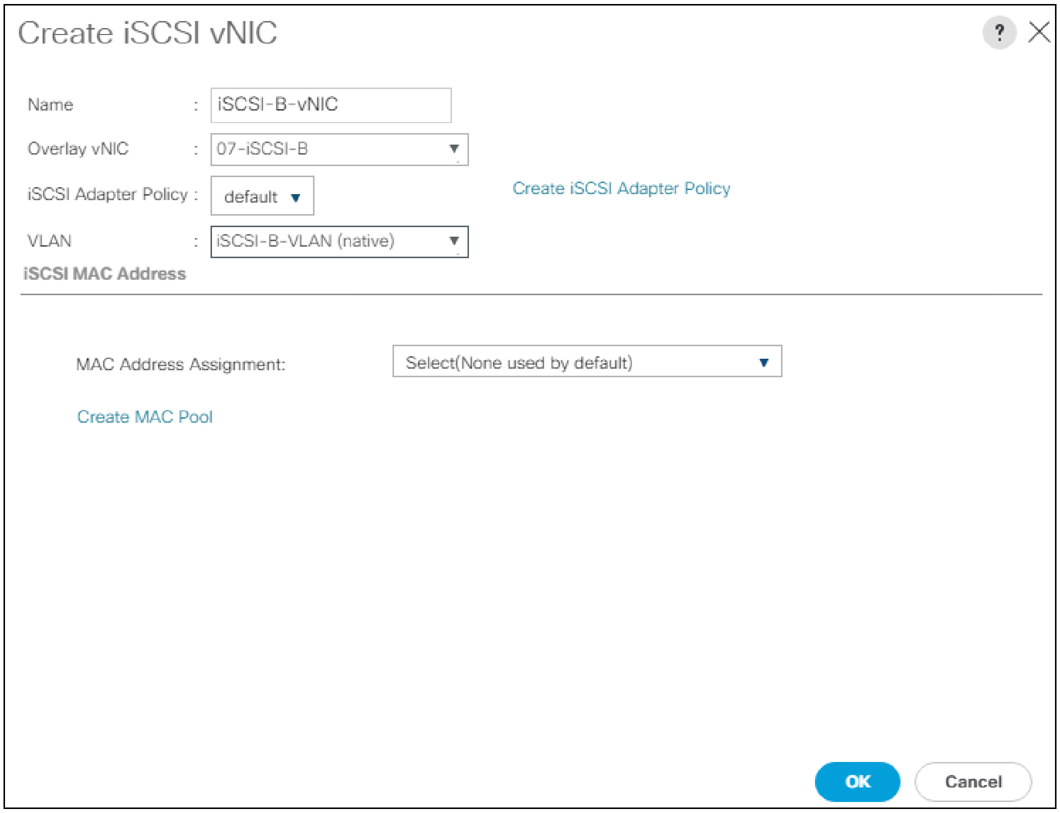
63. Set the name to iSCSI-B-vNIC.

64. Select the 07-iSCSI-A as Overlay vNIC.

65. Set the VLAN to iSCSI-B-VLAN.

66. Set the iSCSI Adapter Policy to default.

67. Leave the MAC Address set to None.



Create iSCSI vNIC

Name : iSCSI-B-vNIC

Overlay vNIC : 07-iSCSI-B

iSCSI Adapter Policy : default

VLAN : iSCSI-B-VLAN (native)

iSCSI MAC Address

MAC Address Assignment: Select(None used by default)

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

Create Boot Policy

This procedure creates a boot policy for iSCSI boot from the FlashArray//X70 R2 pointing to the two iSCSI interfaces on controller 1 (ct0.eth8 and ct0.eth9) and the two iSCSI interfaces on controller 2 (ct1.eth8 and ct1.eth9).

To create a boot policy for the Cisco UCS environment, follow these steps:

1. In Cisco UCS Manager, click Servers.

2. Select Policies > root.

3. Right-click Boot Policies.

4. Select Create Boot Policy.

5. Enter `Boot-iSCSI-X-A` as the name of the boot policy.

6. Optional: Enter a description for the boot policy.

Do not select the Reboot on Boot Order Change checkbox.

7. Keep the Reboot on Boot Order Change option cleared.

8. Expand the Local Devices drop-down menu and select `Add Remote CD/DVD`.

9. Expand the iSCSI vNICs drop-down menu and select Add iSCSI Boot.

10. In the Add iSCSI Boot dialog box, enter `iSCSI-A-vNIC`.

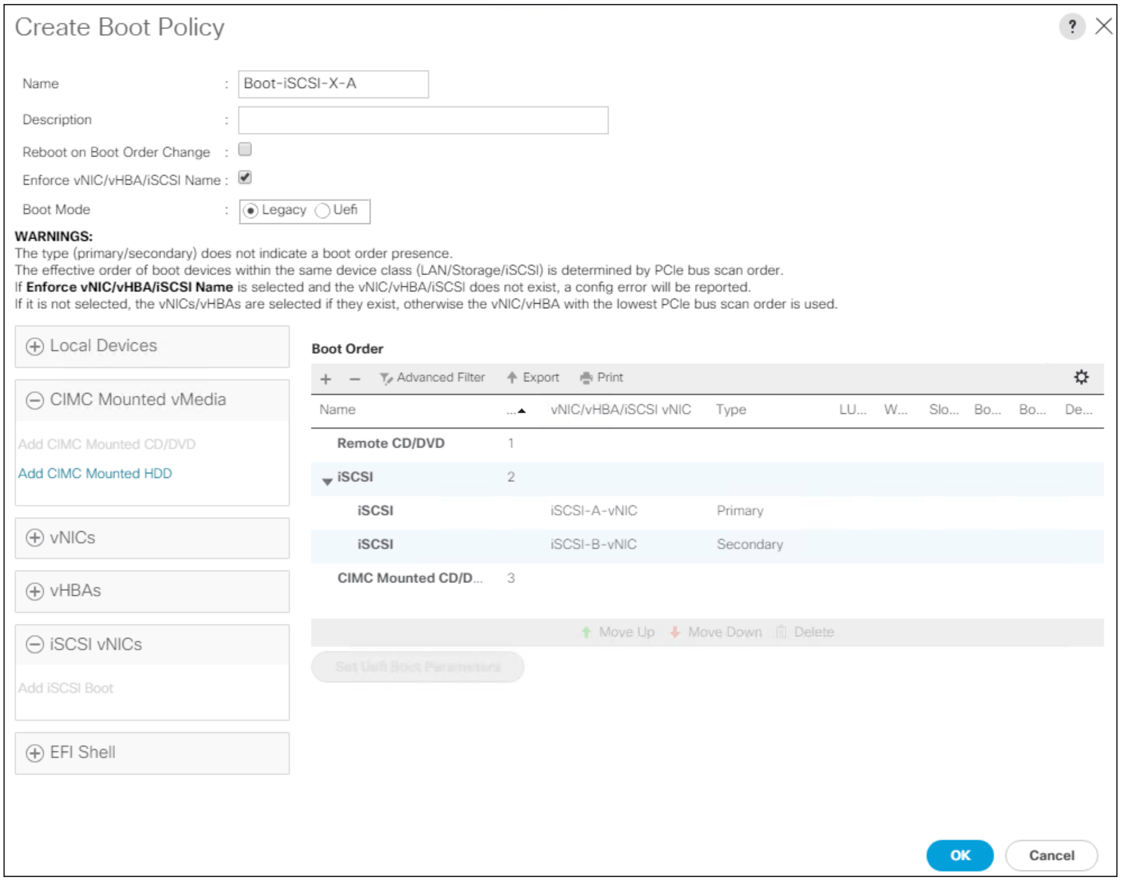
11. Click OK.

12. Select Add iSCSI Boot.

13. In the Add iSCSI Boot dialog box, enter `iSCSI-B-vNIC`.

14. Click OK.

15. Expand CIMC Mounted Media and select Add CIMC Mounted CD/DVD.



Create Boot Policy

Name : Boot-iSCSI-X-A

Description :

Reboot on Boot Order Change : □

Enforce vNIC/vHBA/iSCSI Name : ☑

Boot Mode : ● Legacy ○ Uefi

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

Boot Order

Name	...▲	vNIC/vHBA/iSCSI vNIC	Type	LU...	W...	Slo...	Bo...	Bo...	De...
Remote CD/DVD	1								
iSCSI	2								
iSCSI		iSCSI-A-vNIC	Primary						
iSCSI		iSCSI-B-vNIC	Secondary						
CIMC Mounted CD/D...	3								

16. Click OK to create the policy.

Create Service Profile Templates

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

To create the service profile template, follow these steps:

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

2. Select Service Profile Templates > root.

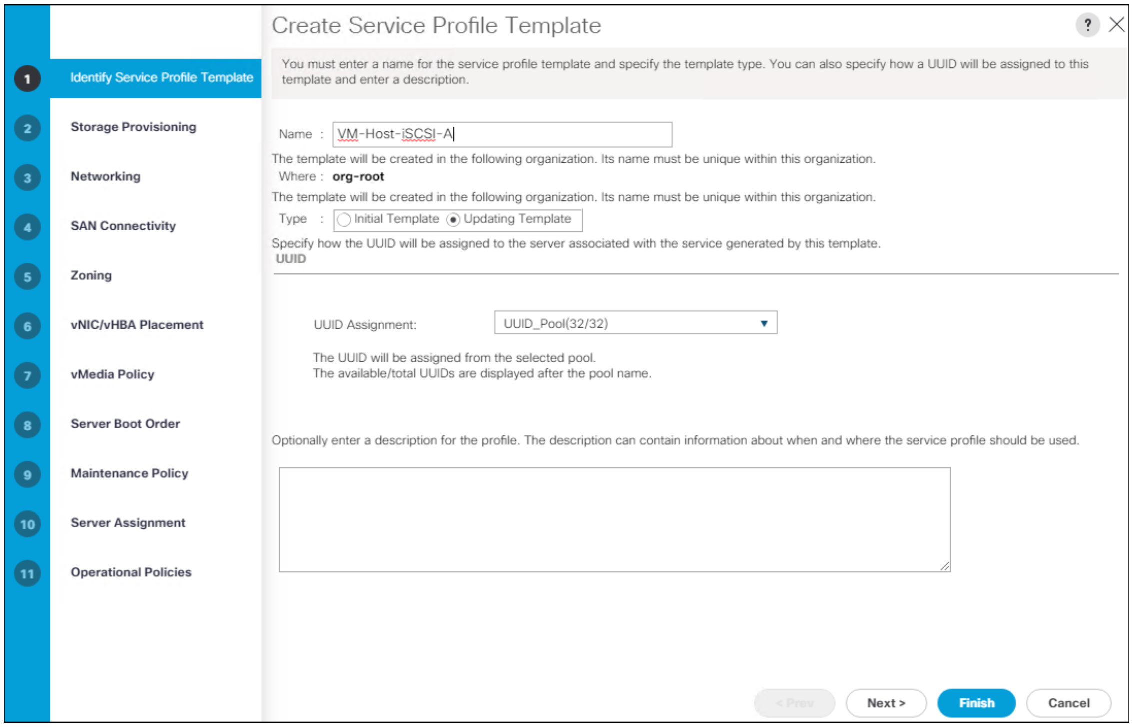
3. Right-click root.

4. Select Create Service Profile Template to open the Create Service Profile Template wizard.

5. Enter VM-Host-iSCSI-A as the name of the service profile template. This service profile template is configured to boot from FlashArray//X70 R2 controller 1 on fabric A.

6. Select the "Updating Template" option.

7. Under UUID, select UUID_Pool as the UUID pool.



Create Service Profile Template

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

Name : VM-Host-iSCSI-A

The template will be created in the following organization. Its name must be unique within this organization.

Where : **org-root**

The template will be created in the following organization. Its name must be unique within this organization.

Type : ○ Initial Template ● Updating Template

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

UUID

UUID Assignment: UUID_Pool(32/32)

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

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

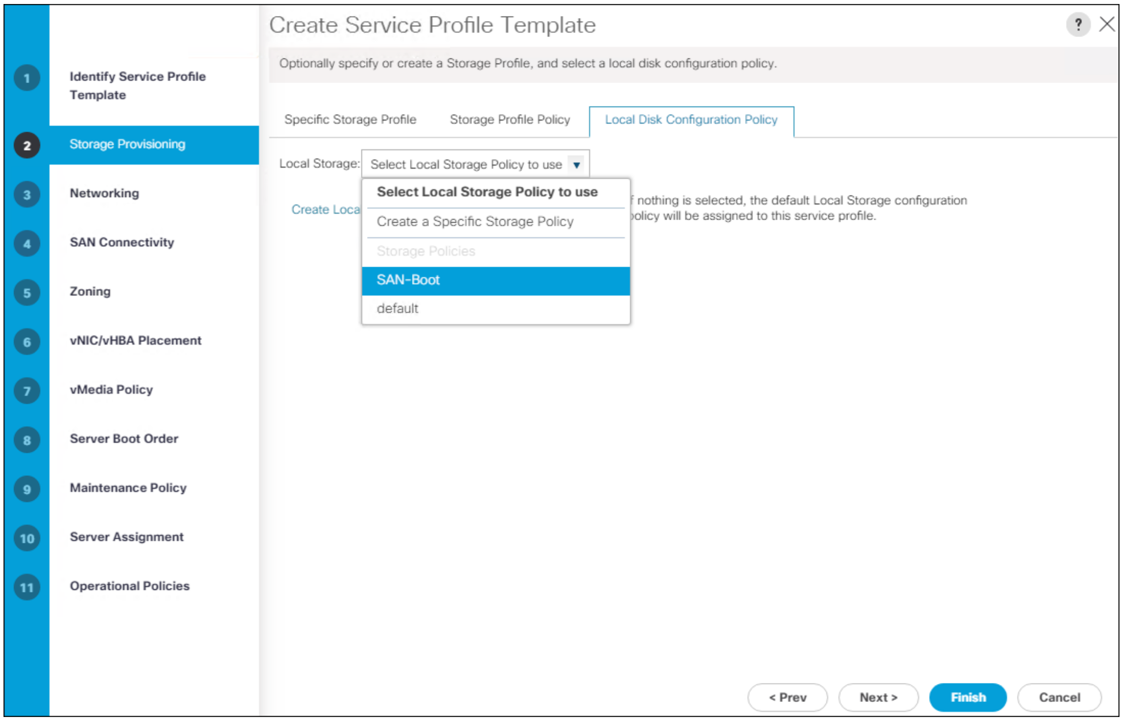
8. Click Next.

Configure Storage Provisioning

To configure the storage provisioning, follow these steps:

1. Select Local Disk Configuration Policy tab

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


Create Service Profile Template
Optionally specify or create a Storage Profile, and select a local disk configuration policy.
1 Identify Service Profile Template
2 Storage Provisioning
3 Networking
4 SAN Connectivity
5 Zoning
6 vNIC/vHBA Placement
7 vMedia Policy
8 Server Boot Order
9 Maintenance Policy
10 Server Assignment
11 Operational Policies
Specific Storage Profile
Storage Profile Policy
Local Disk Configuration Policy
Local Storage: Select Local Storage Policy to use
Create Loca
Select Local Storage Policy to use
Create a Specific Storage Policy
Storage Policies
SAN-Boot
default
f nothing is selected, the default Local Storage configuration policy will be assigned to this service profile.
< Prev
Next >
Finish
Cancel

3. Click Next.

Configure Networking Options

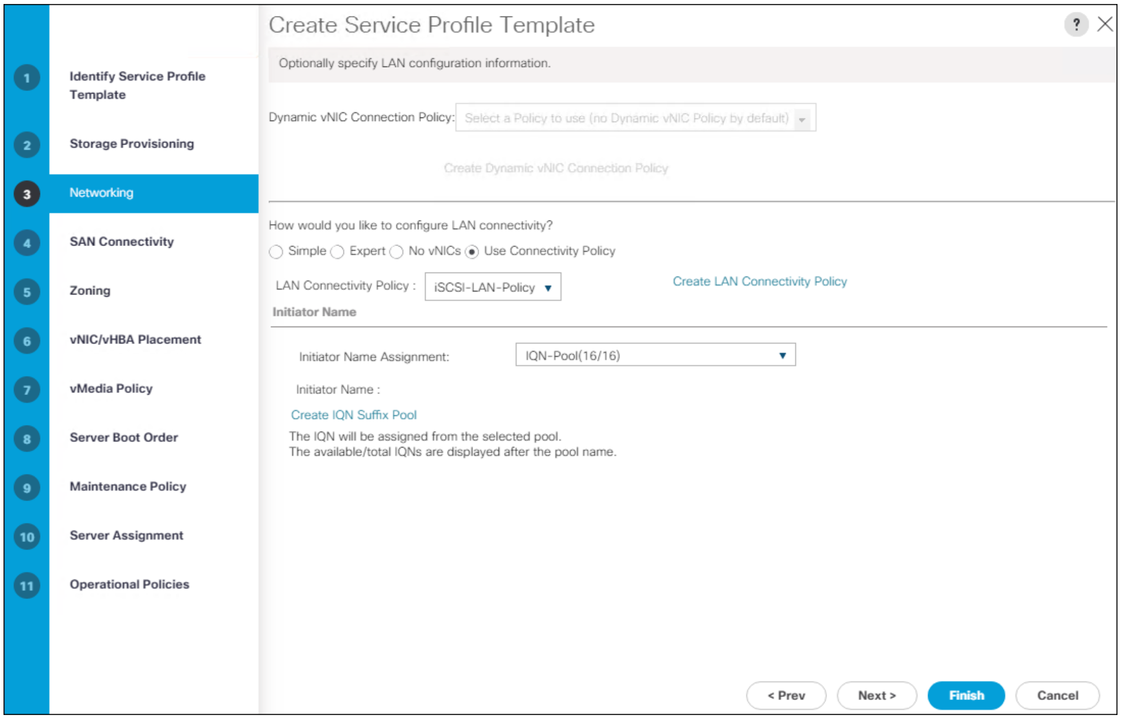
To configure the network options, follow these steps:

1. Keep the default setting for Dynamic vNIC Connection Policy.

2. Select the "Use Connectivity Policy" option to configure the LAN connectivity.

3. Select iSCSI-LAN-Policy from the LAN Connectivity Policy pull-down.

4. Select IQN_Pool in Initiator Name Assignment.



Create Service Profile Template

Optionally specify LAN configuration information.

Dynamic vNIC Connection Policy: Select a Policy to use (no Dynamic vNIC Policy by default)

Create Dynamic vNIC Connection Policy

How would you like to configure LAN connectivity?

○ Simple ○ Expert ○ No vNICs ● Use Connectivity Policy

LAN Connectivity Policy : iSCSI-LAN-Policy ▼

Create LAN Connectivity Policy

Initiator Name

Initiator Name Assignment: IQN-Pool(16/16) ▼

Initiator Name :

Create IQN Suffix Pool

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

5. Click Next.

Configure Storage Options

1. Select the **No vHBA** option for the “How would you like to configure SAN connectivity?” field.

2. Click Next.

Configure Zoning Options

1. Leave Zoning configuration unspecified and click Next.

Configure vNIC/HBA Placement

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

2. Click Next.

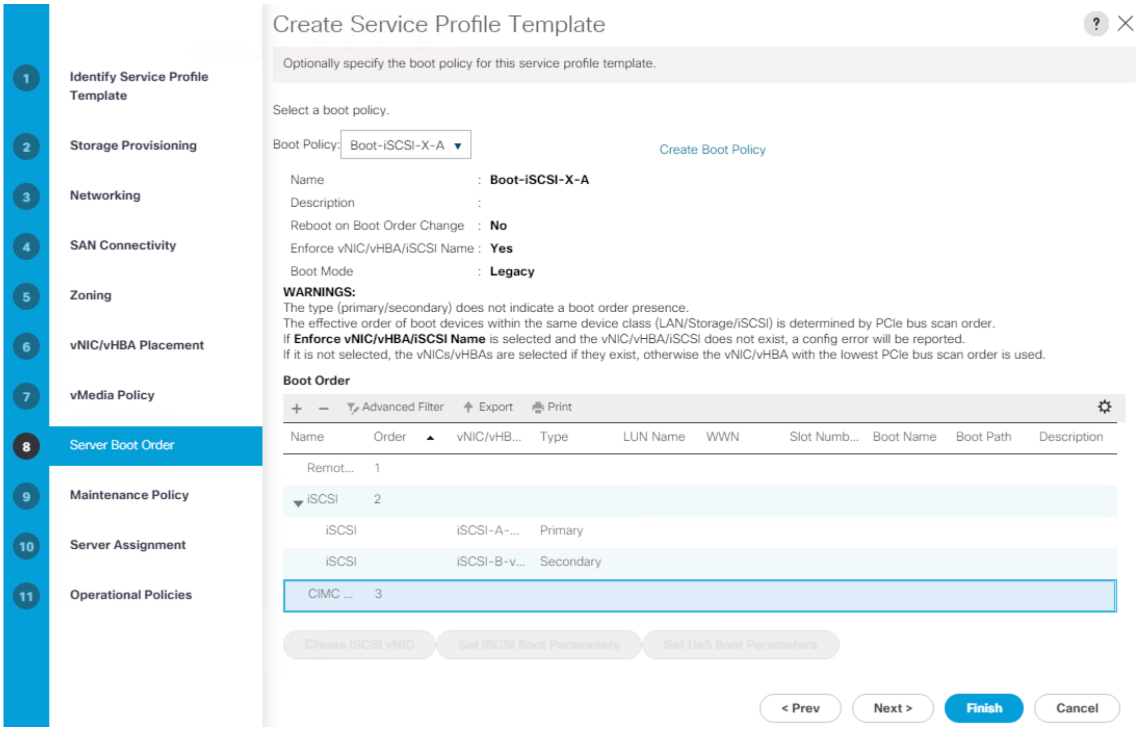
Configure vMedia Policy

1. Do not select a vMedia Policy.

2. Click Next.

Configure Server Boot Order

1. Select `Boot-iSCSI-X-A` for Boot Policy.



Create Service Profile Template

Optionally specify the boot policy for this service profile template.

Select a boot policy.

Boot Policy: Boot-iSCSI-X-A ▾ Create Boot Policy

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

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

Boot Order

Name	Order ▲	vNIC/vHB...	Type	LUN Name	WWN	Slot Numb...	Boot Name	Boot Path	Description
Remot...	1								
▾ iSCSI	2								
iSCSI		iSCSI-A-...	Primary						
iSCSI		iSCSI-B-v...	Secondary						
CIMC ...	3								

2. In the Boor order, select iSCSI-A-vNIC.

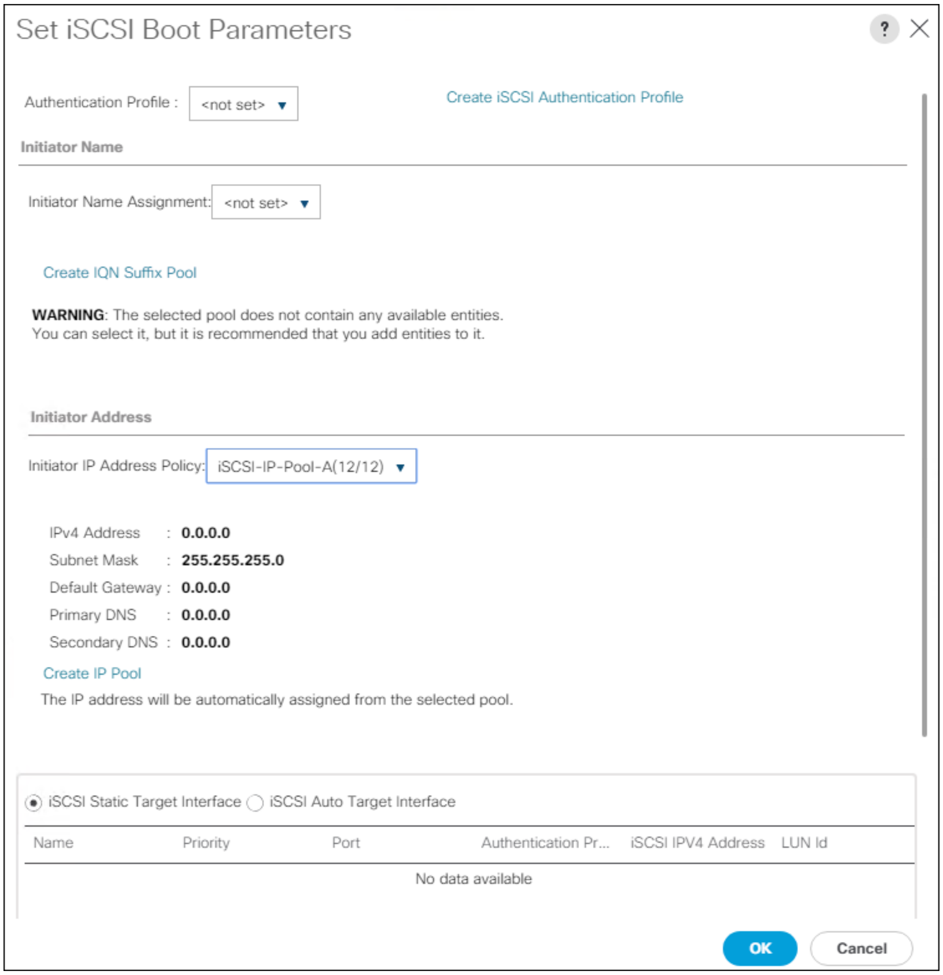
3. Click Set iSCSI Boot Parameters button.

4. In the Set iSCSI Boot Parameters pop-up, leave Authentication Profile to <not set> unless you have independently created one appropriate to your environment.

5. Leave the “Initiator Name Assignment” dialog box <not set> to use the single Service Profile Initiator Name defined in the previous steps.

6. Set “Initiator IP address Policy” to iSCSI_IP_Pool_A.

7. Select iSCSI Static Target Interface option.



Set iSCSI Boot Parameters

Authentication Profile : <not set> ▾

Create iSCSI Authentication Profile

Initiator Name

Initiator Name Assignment: <not set> ▾

Create IQN Suffix Pool

WARNING: The selected pool does not contain any available entities.
You can select it, but it is recommended that you add entities to it.

Initiator Address

Initiator IP Address Policy: iSCSI-IP-Pool-A(12/12) ▾

IPv4 Address	: **0.0.0.0**
Subnet Mask	: **255.255.255.0**
Default Gateway	: **0.0.0.0**
Primary DNS	: **0.0.0.0**
Secondary DNS	: **0.0.0.0**

Create IP Pool

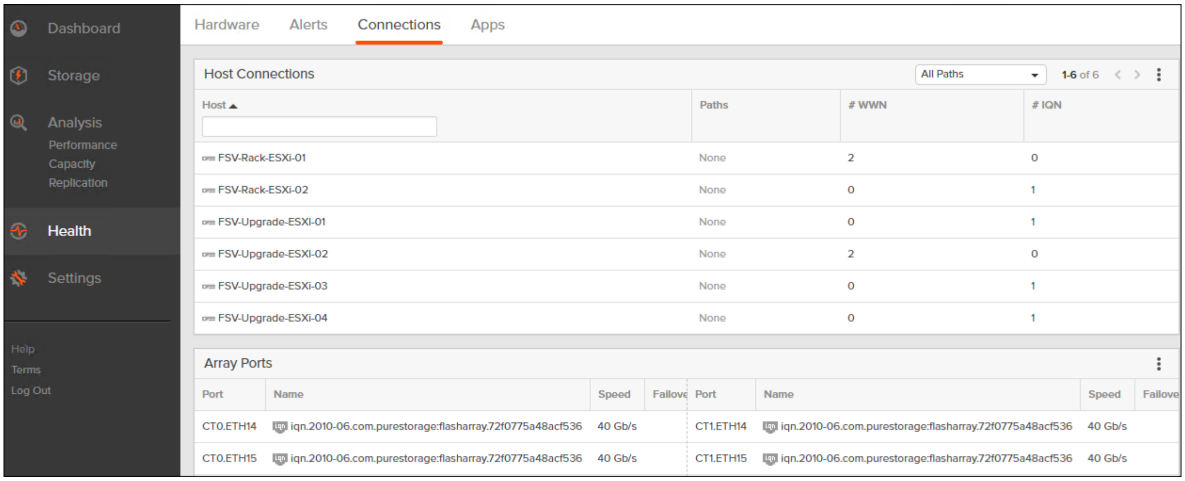
The IP address will be automatically assigned from the selected pool.

● iSCSI Static Target Interface ○ iSCSI Auto Target Interface

Name	Priority	Port	Authentication Pr...	iSCSI IPV4 Address	LUN Id
No data available					

8. Scroll down and click Add.

9. Enter the iSCSI Target Name for cto.eth14. To get the iSCSI target name of the FlashArray//X70 R2, login to the Pure Web console and navigate to Health -> Connections -> Array Ports.



Host Connections

All Paths ▾ 1-6 of 6

Host ▲	Paths	# WWN	# IQN
FSV-Rack-ESXi-01	None	2	0
FSV-Rack-ESXi-02	None	0	1
FSV-Upgrade-ESXI-01	None	0	1
FSV-Upgrade-ESXI-02	None	2	0
FSV-Upgrade-ESXi-03	None	0	1
FSV-Upgrade-ESXi-04	None	0	1

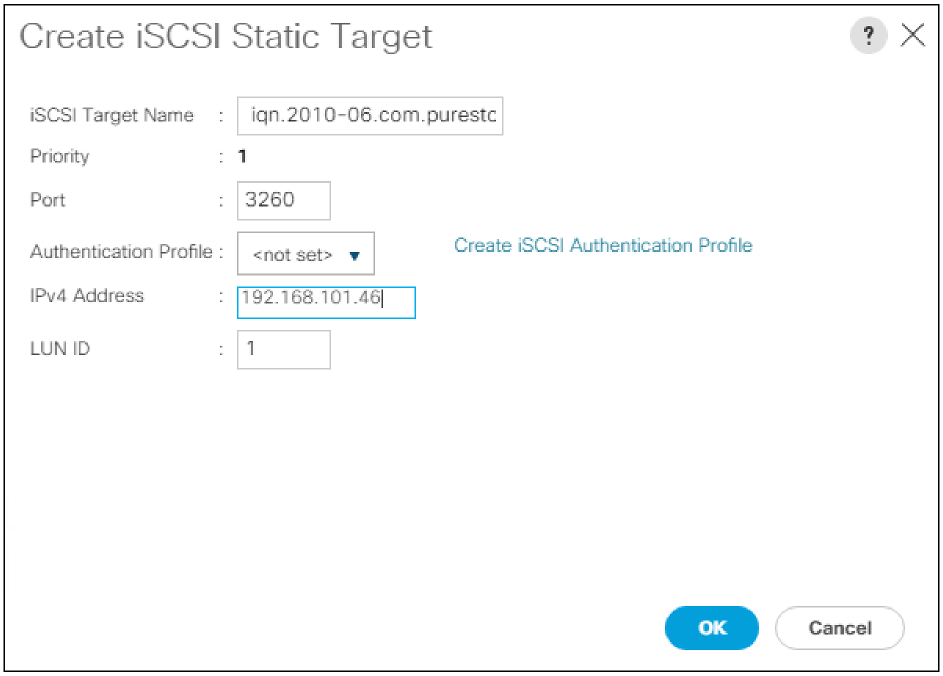
Array Ports

Port	Name	Speed	Failove	Port	Name	Speed	Failove
CT0.ETH14	iqn.2010-06.com.purestorage:flasharray.72f0775a48acf536	40 Gb/s		CT1.ETH14	iqn.2010-06.com.purestorage:flasharray.72f0775a48acf536	40 Gb/s	
CT0.ETH15	iqn.2010-06.com.purestorage:flasharray.72f0775a48acf536	40 Gb/s		CT1.ETH15	iqn.2010-06.com.purestorage:flasharray.72f0775a48acf536	40 Gb/s	

10. Or find the targets from connecting to the controller with ssh using the pureuser login and run the pureport list command.

```
pureuser@cspg-rtp-1> pureport list

Name        Portal                  IQN

CT0.ETH14   192.168.101.46:3260  iqn.2010-06.com.purestorage:flasharray.72f0775a48acf536


CT0.ETH15   192.168.102.46:3260  iqn.2010-06.com.purestorage:flasharray.72f0775a48acf536


CT1.ETH14   192.168.101.47:3260  iqn.2010-06.com.purestorage:flasharray.72f0775a48acf536


CT1.ETH15   192.168.102.47:3260  iqn.2010-06.com.purestorage:flasharray.72f0775a48acf536
```

11. Leave the Port set to 3260, Authentication Profile as <not set>, provide the appropriate IPv4 Address configured to ct0.eth14, and set the LUN ID to 1.



Create iSCSI Static Target

iSCSI Target Name : iqn.2010-06.com.purestc

Priority : 1

Port : 3260

Authentication Profile : <not set>

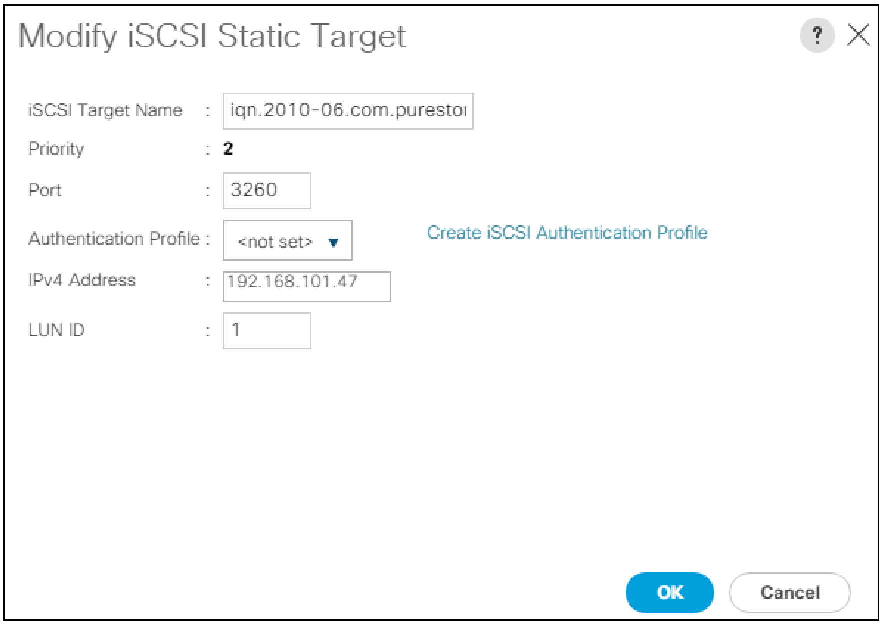
IPv4 Address : 192.168.101.46

LUN ID : 1

12. Click OK to add the iSCSI Static Target.

13. Click Add again to add another iSCSI Target for the iSCSI-A-vNIC that will associate with ct1.eth14.

14. Enter the same iSCSI Target Name, leave the Port set to 3260, the Authentication Profile as <not set>, provide the appropriate IPv4 Address configured to ct1.eth14, and set the LUN ID to 1.



Modify iSCSI Static Target

iSCSI Target Name : iqn.2010-06.com.puresto

Priority : **2**

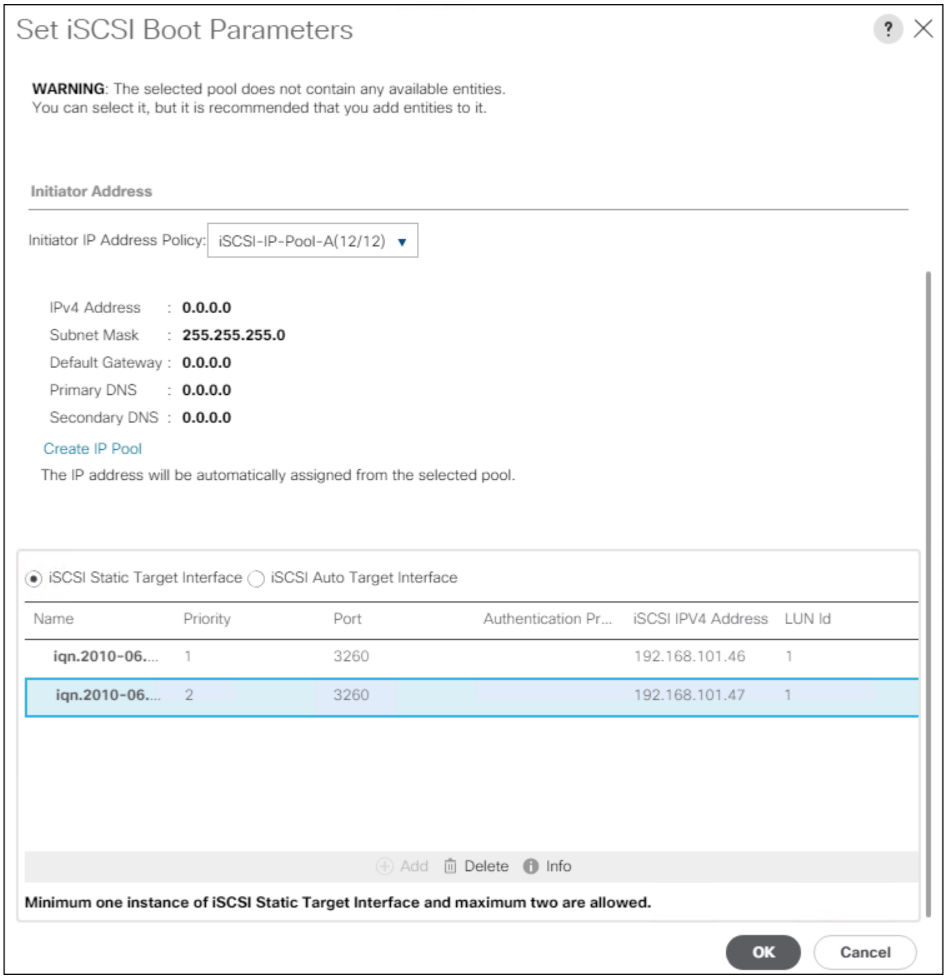
Port : 3260

Authentication Profile : <not set>

IPv4 Address : 192.168.101.47

LUN ID : 1

15. Click OK to add the iSCSI Static Target.



Set iSCSI Boot Parameters

WARNING: The selected pool does not contain any available entities.
You can select it, but it is recommended that you add entities to it.

Initiator Address

Initiator IP Address Policy: iSCSI-IP-Pool-A(12/12)

IPv4 Address : **0.0.0.0**
Subnet Mask : **255.255.255.0**
Default Gateway : **0.0.0.0**
Primary DNS : **0.0.0.0**
Secondary DNS : **0.0.0.0**

The IP address will be automatically assigned from the selected pool.

● iSCSI Static Target Interface ○ iSCSI Auto Target Interface

Name	Priority	Port	Authentication Pr...	iSCSI IPV4 Address	LUN Id
iqn.2010-06....	1	3260		192.168.101.46	1
iqn.2010-06....	2	3260		192.168.101.47	1

Minimum one instance of iSCSI Static Target Interface and maximum two are allowed.

16. Click OK to set the iSCSI-A-vNIC ISCSI Boot Parameters.

17. In the Boor order, select iSCSI-B-vNIC.

18. Click Set iSCSI Boot Parameters button.

19. In the Set iSCSI Boot Parameters pop-up, leave Authentication Profile to <not set> unless you have independently created one appropriate to your environment.

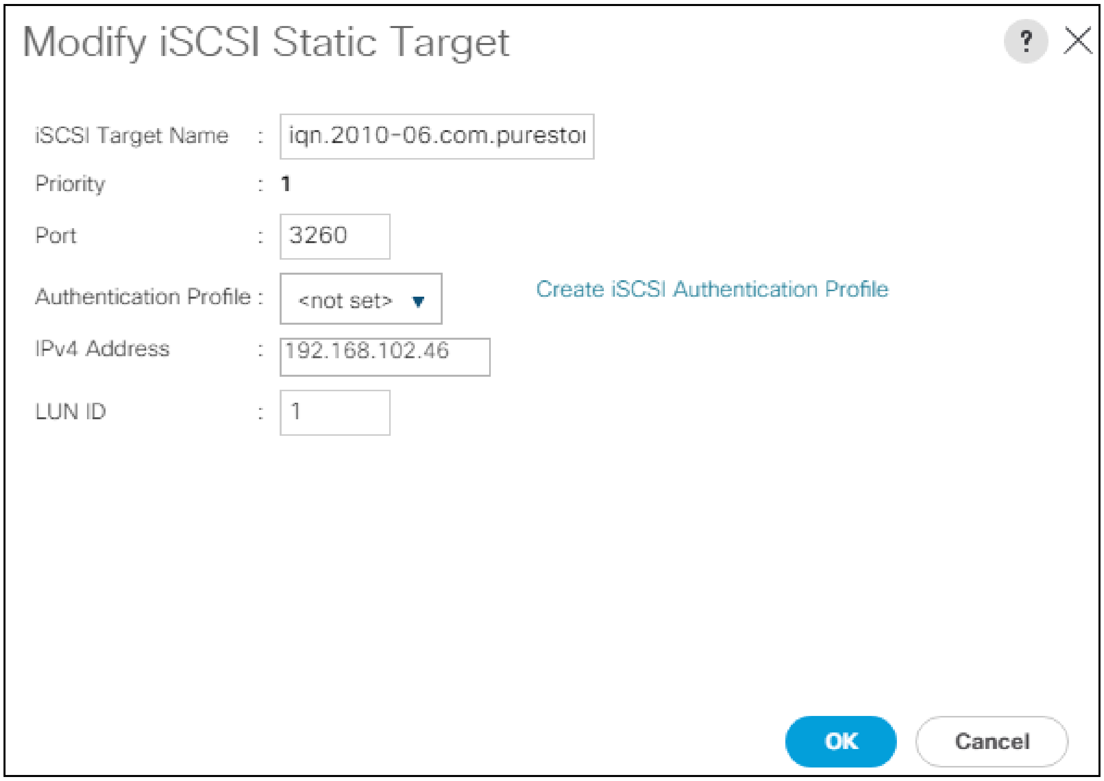
20. Leave the "Initiator Name Assignment" dialog box <not set> to use the single Service Profile Initiator Name defined in the previous steps.

21. Set iSCSI_IP_Pool_B as the "Initiator IP address Policy".

22. Select iSCSI Static Target Interface option.

23. Click Add.

24. Enter the same iSCSI Target Name, leave the Port set to 3260, the Authentication Profile as <not set>, provide the appropriate IPv4 Address configured to cto.eth15, and set the LUN ID to 1.



Modify iSCSI Static Target

iSCSI Target Name : iqn.2010-06.com.purestoı

Priority : 1

Port : 3260

Authentication Profile : <not set>

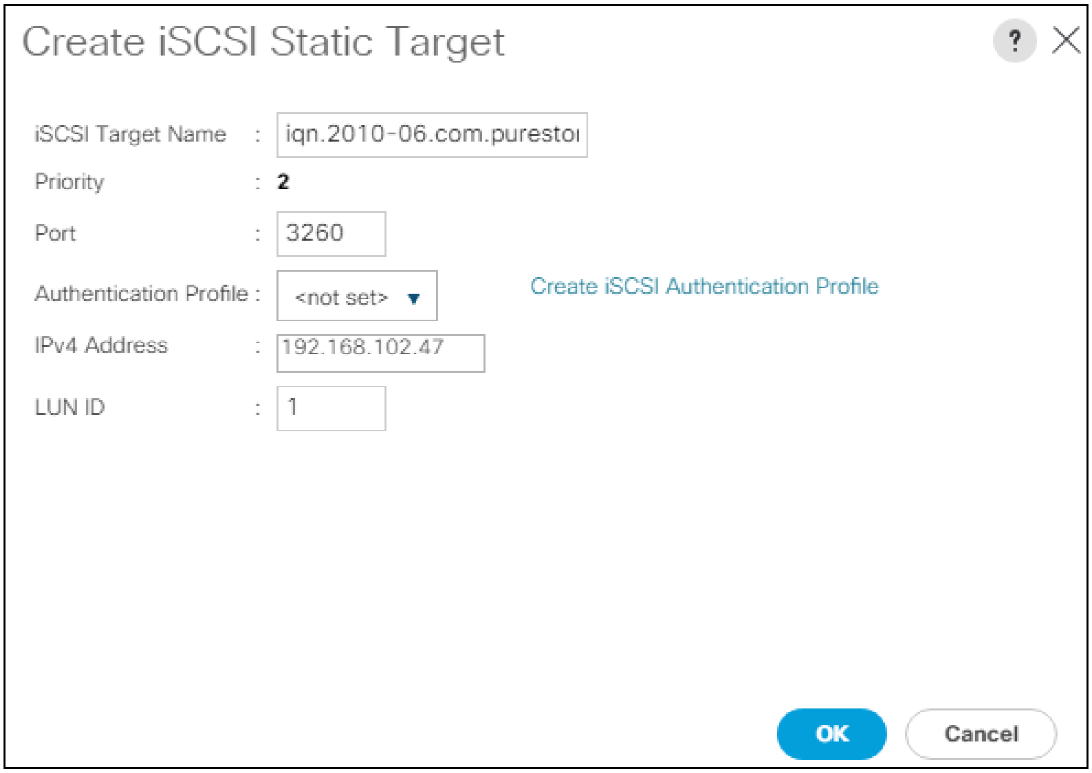
IPv4 Address : 192.168.102.46

LUN ID : 1

25. Click OK to add the iSCSI Static Target.

26. Click Add again to add another iSCSI Target for the iSCSI-B-vNIC that will associate with ct1.eth15.

27. Enter the same iSCSI Target Name, leave the Port set to 3260, the Authentication Profile as <not set>, provide the appropriate IPv4 Address configured to ct1.et15, and set the LUN ID to 1.



Create iSCSI Static Target

iSCSI Target Name : iqn.2010-06.com.purestoı

Priority : 2

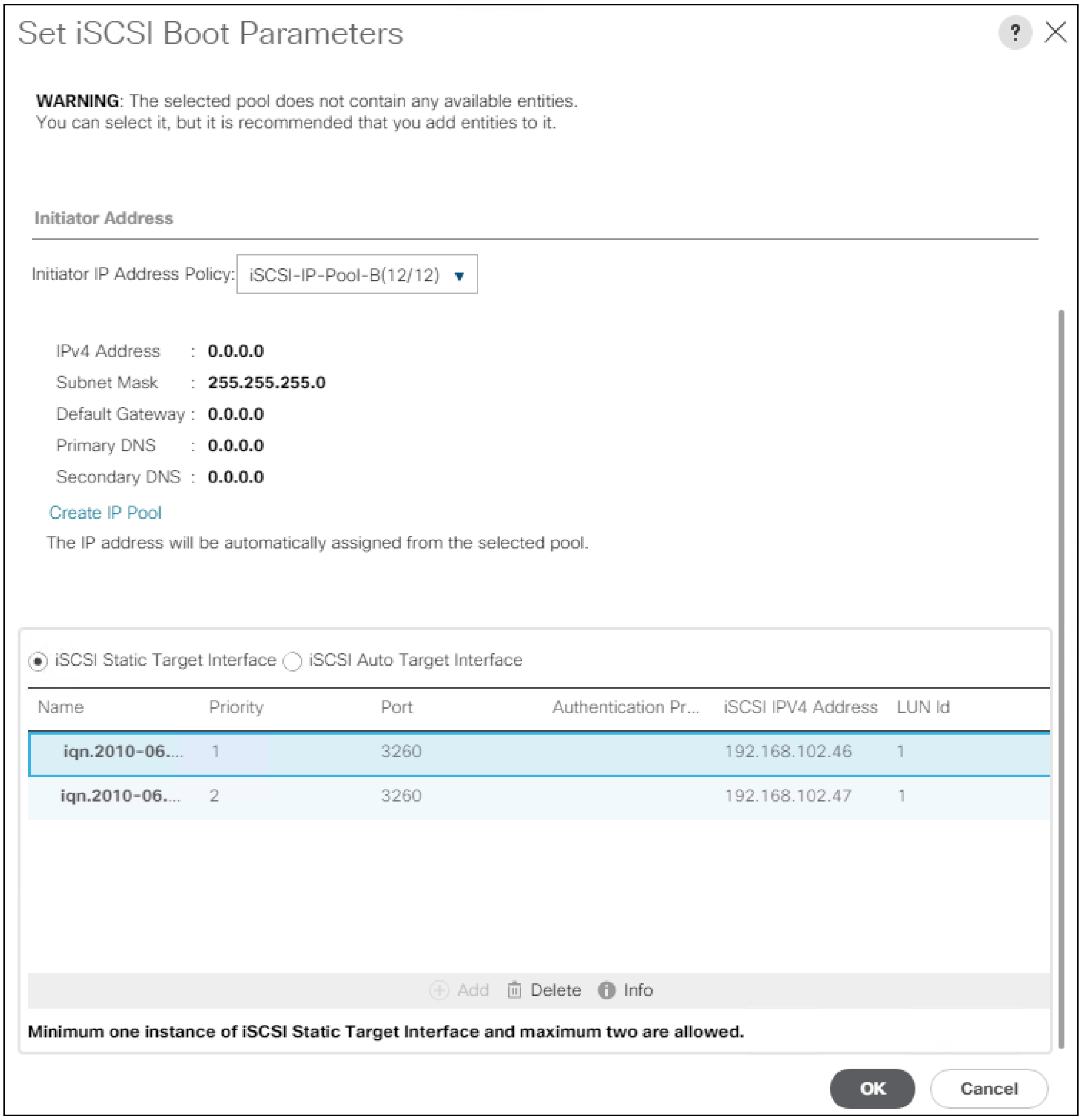
Port : 3260

Authentication Profile : <not set> ▼

IPv4 Address : 192.168.102.47

LUN ID : 1

28. Click OK to add the iSCSI Static Target.



Set iSCSI Boot Parameters

WARNING: The selected pool does not contain any available entities.
You can select it, but it is recommended that you add entities to it.

Initiator Address

Initiator IP Address Policy: iSCSI-IP-Pool-B(12/12)

IPv4 Address : **0.0.0.0**
Subnet Mask : **255.255.255.0**
Default Gateway : **0.0.0.0**
Primary DNS : **0.0.0.0**
Secondary DNS : **0.0.0.0**

Create IP Pool

The IP address will be automatically assigned from the selected pool.

● iSCSI Static Target Interface ○ iSCSI Auto Target Interface

Name	Priority	Port	Authentication Pr...	iSCSI IPV4 Address	LUN Id
iqn.2010-06....	1	3260		192.168.102.46	1
iqn.2010-06....	2	3260		192.168.102.47	1

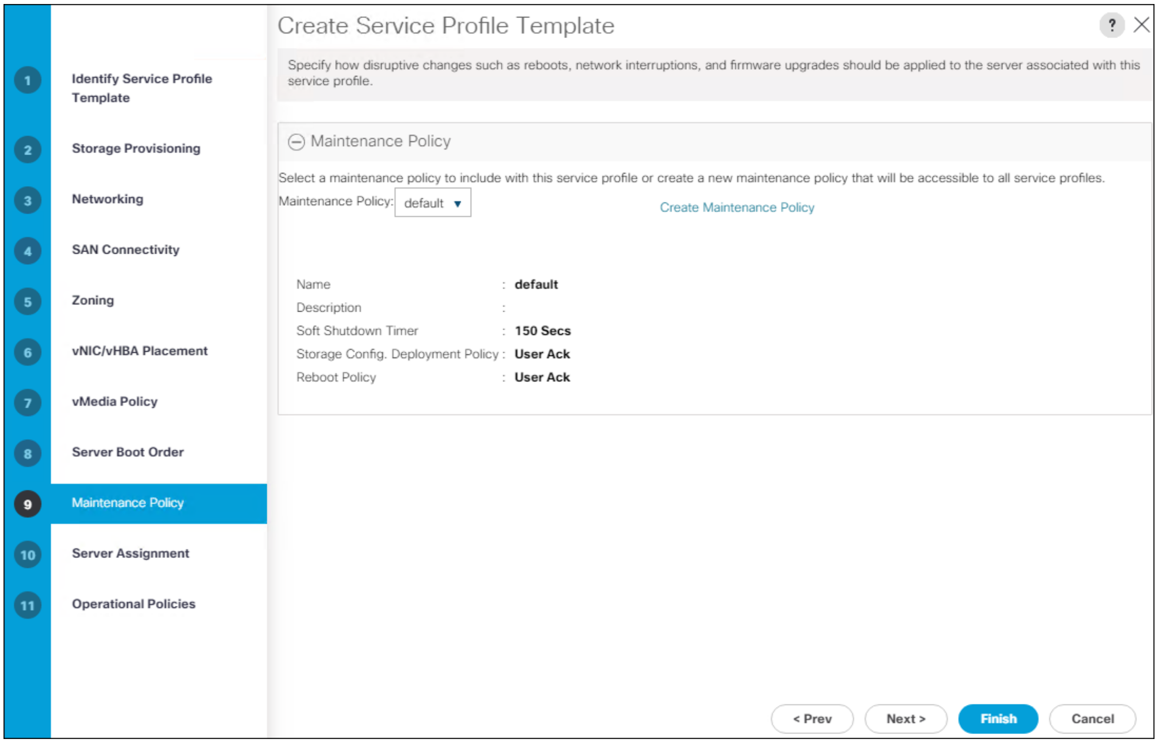
Minimum one instance of iSCSI Static Target Interface and maximum two are allowed.

29. Click OK to set the iSCSI-B-vNIC ISCSI Boot Parameters.

30. Click Next to continue to the next section.

Configure Maintenance Policy

1. Change the Maintenance Policy to default.



Create Service Profile Template

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

Maintenance Policy

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

Maintenance Policy: default

Create Maintenance Policy

Name : default

Description :

Soft Shutdown Timer : 150 Secs

Storage Config. Deployment Policy : User Ack

Reboot Policy : User Ack

2. Click Next.

Configure Server Assignment

To configure server assignment, follow these steps:

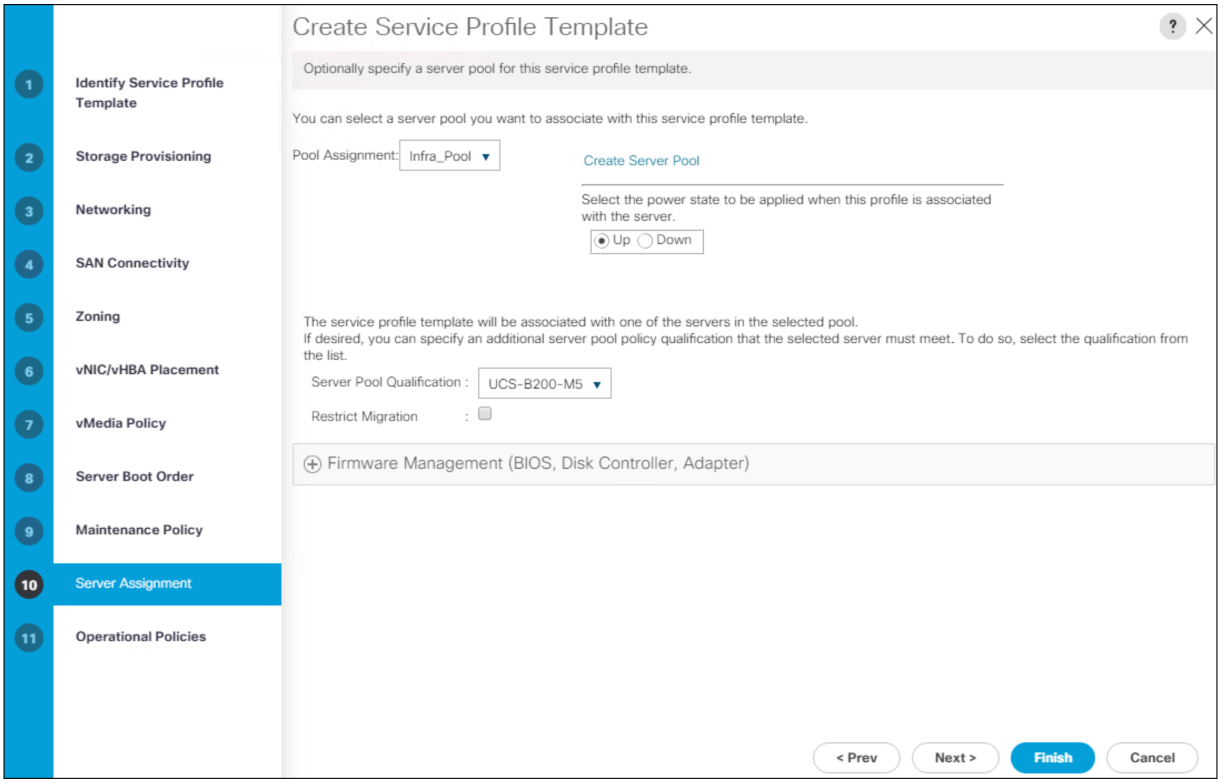
1. In the Pool Assignment list, select `Infra_Pool`.

2. Optional: Select a Server Pool Qualification policy.

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

4. Optional: Select “UCS-B200M5” for the Server Pool Qualification.

5. Firmware Management at the bottom of the page can be left alone as it will use default from the Host Firmware list.



Create Service Profile Template

Optionally specify a server pool for this service profile template.

You can select a server pool you want to associate with this service profile template.

Pool Assignment: Infra_Pool ▾

Create Server Pool

Select the power state to be applied when this profile is associated with the server.

● Up ○ Down

The service profile template will be associated with one of the servers in the selected pool.
If desired, you can specify an additional server pool policy qualification that the selected server must meet. To do so, select the qualification from the list.

Server Pool Qualification : UCS-B200-M5 ▾

Restrict Migration : □

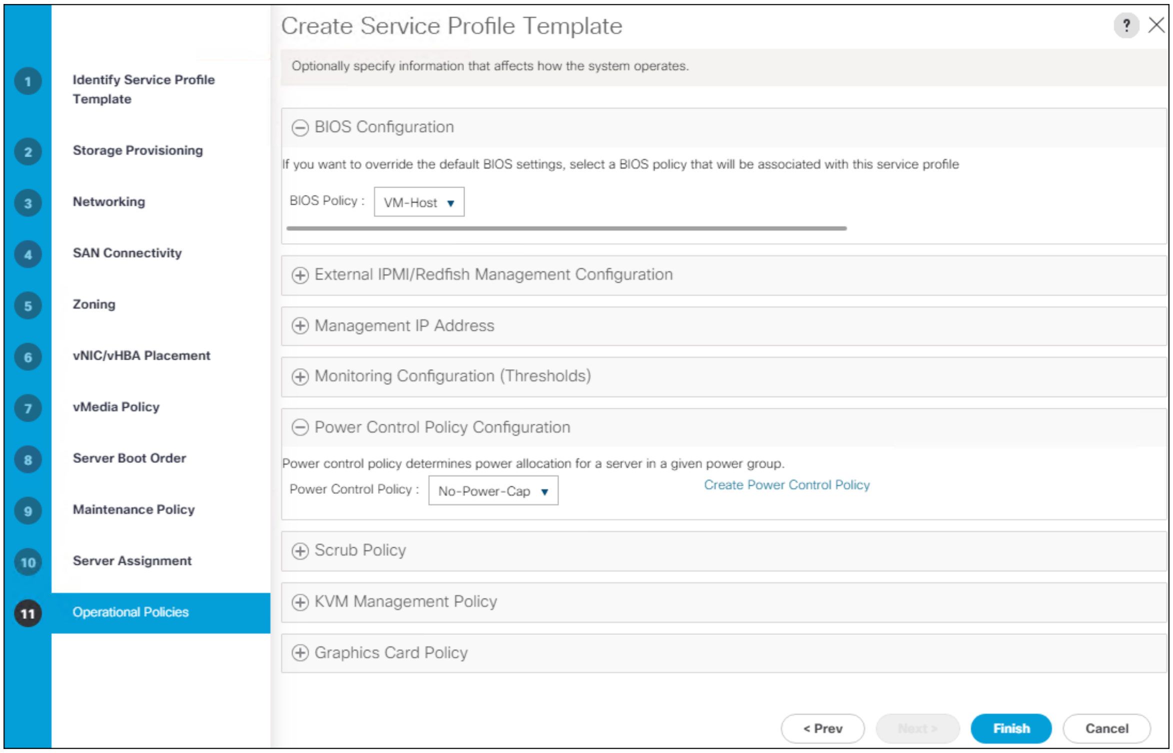
⊕ Firmware Management (BIOS, Disk Controller, Adapter)

6. Click Next.

Configure Operational Policies

To configure the operational policies, follow these steps:

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



Create Service Profile Template

Optionally specify information that affects how the system operates.

⊖ BIOS Configuration

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

BIOS Policy : VM-Host

⊕ External IPMI/Redfish Management Configuration

⊕ Management IP Address

⊕ Monitoring Configuration (Thresholds)

⊖ Power Control Policy Configuration

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

Power Control Policy : No-Power-Cap

⊕ Scrub Policy

⊕ KVM Management Policy

⊕ Graphics Card Policy

3. Click Finish to create the service profile template.

4. Click OK in the confirmation message.

Create vMedia Service Profile Template

If the optional ESXi 6.7 U1 vMedia Policy is being used, a clone of the created service profile template will be made to reference this vMedia Policy. The clone of the service profile template will have the vMedia Policy configured for it, and service profiles created from it, will be unbound and re-associated to the original service profile template after ESXi installation. To create a clone of the VM-Host-iSCSI-A service profile template, and associate the vMedia Policy to it, follow these steps:

1. Connect to UCS Manager, click Servers.

2. Select Service Profile Templates > root > Service Template VM-Host-iSCSI-A.

3. Right-click Service Template VM-Host-iSCSI-A and select Create a Clone.

4. Name the clone VM-Host-iSCSi-A-vM and click OK.

5. Select Service Template VM-Host-iSCSi-A-vM.

6. In the right pane, select the vMedia Policy tab.

7. Under Actions, select Modify vMedia Policy.

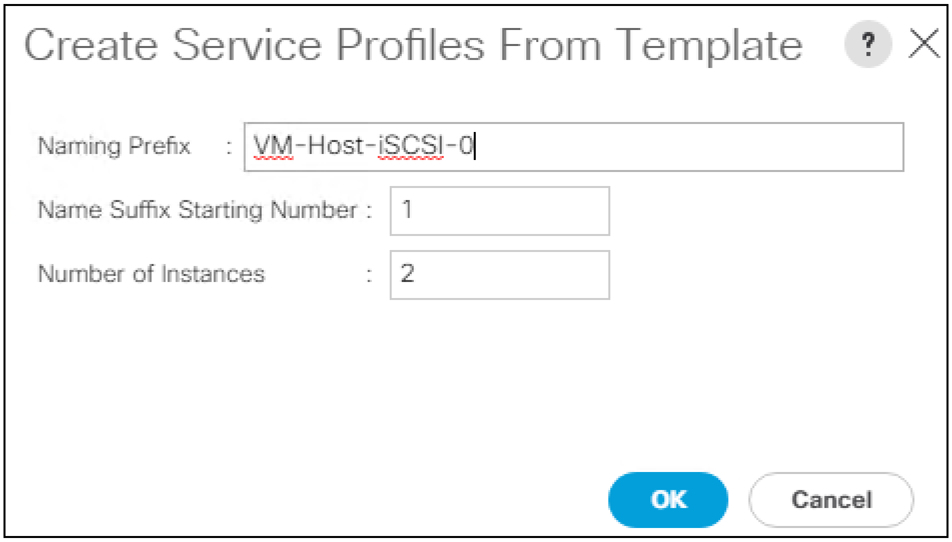
8. From the drop-down list, select the ESXi-6.7U1-HTTP vMedia Policy.

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

Create Service Profiles

To create service profiles from the service profile template, follow these steps:

1. Connect to the UCS 6454 Fabric Interconnect UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Service Template VM-Host-iSCSI-A.
3. Right-click `VM-Host-iSCSI-A` and select Create Service Profiles from Template.
4. Enter `VM-Host-iSCSI-0` as the service profile prefix.
5. Leave `1` as "Name Suffix Starting Number."
6. Leave `2` as the "Number of Instances."
7. Click OK to create the service profiles.



Create Service Profiles From Template

Naming Prefix : VM-Host-iSCSI-0

Name Suffix Starting Number : 1

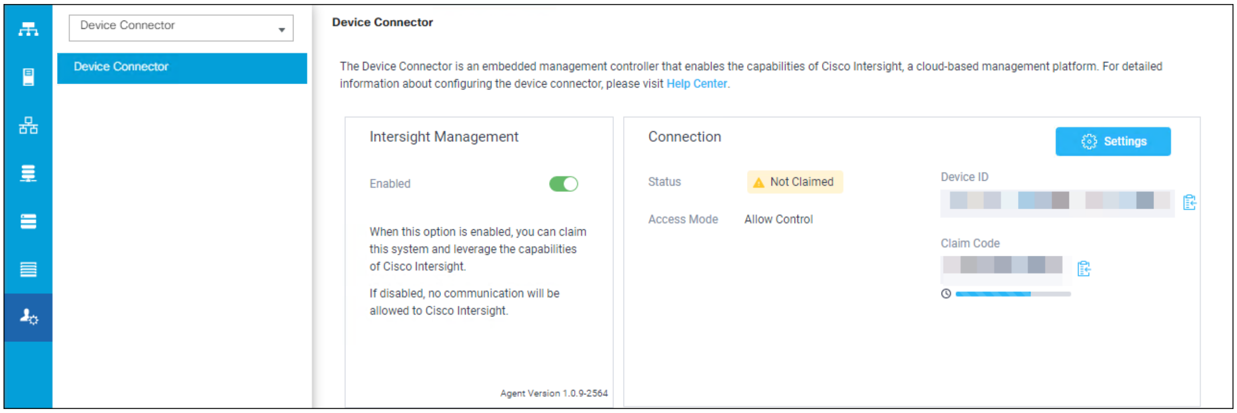
Number of Instances : 2

8. Click OK in the confirmation message to provision two FlashStack Service Profiles.
9. When VMware ESXi 6.5 U1 has been installed on the hosts, the host Service Profiles can be unbound from the VM-Host-iSCSI-A-vM and rebound to the VM-Host-iSCSI-A Service Profile Template to remove the vMedia mapping from the host, to prevent issues at boot time if the HTTP source for the ESXi ISO is somehow not available.

Claim in Intersight

To claim the UCS 6454 Domain in Intersight, follow these steps:

1. Connect to the UCS 6454 Fabric Interconnect UCS Manager, click the Admin tab in the navigation pane.
2. Select Device Connector.
3. Set Intersight Management to Enabled.
4. Copy the Device ID and Claim Code.



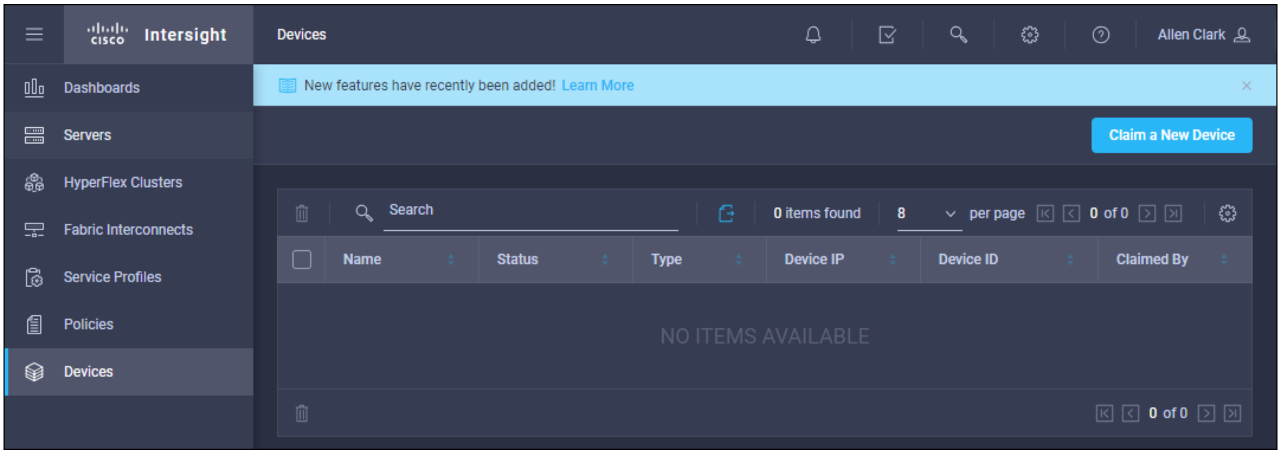
The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed information about configuring the device connector, please visit Help Center.

When this option is enabled, you can claim this system and leverage the capabilities of Cisco Intersight.

If disabled, no communication will be allowed to Cisco Intersight.

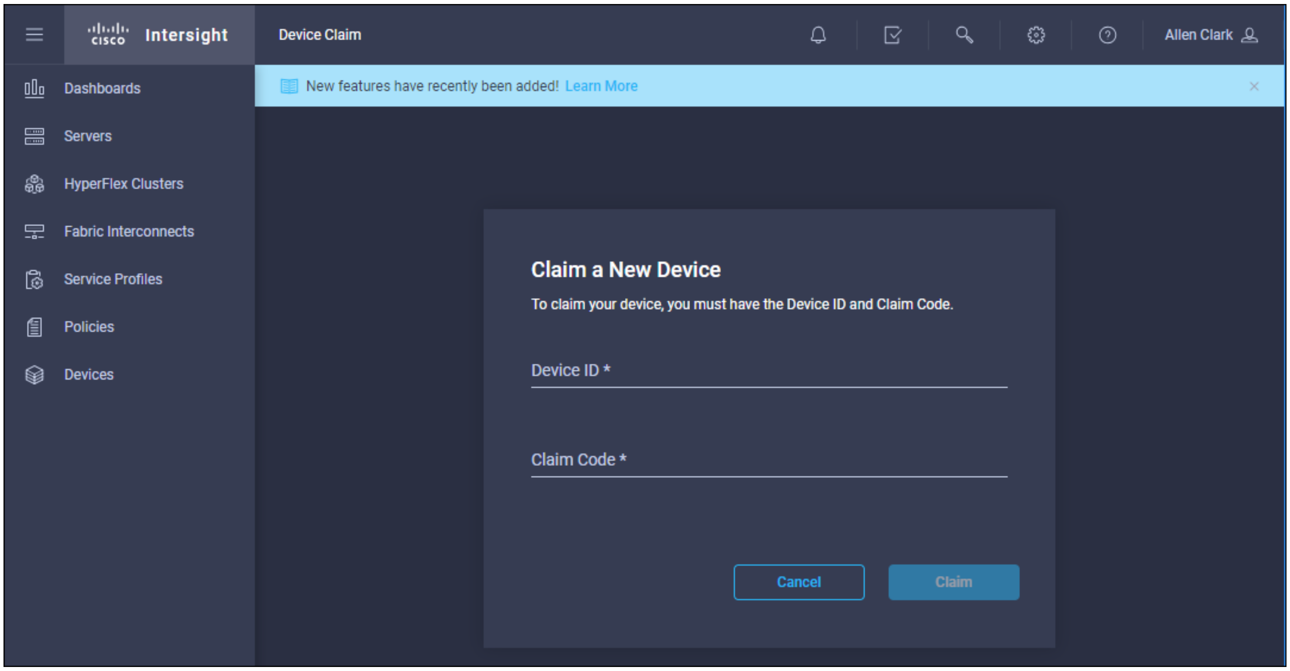
5. Open a browser to Cisco Intersight, https://intersight.com and log in to your Intersight account.

6. Select Devices.



New features have recently been added! Learn More

7. Click Claim a New Device and enter your Device ID and Claim Code.



New features have recently been added! Learn More

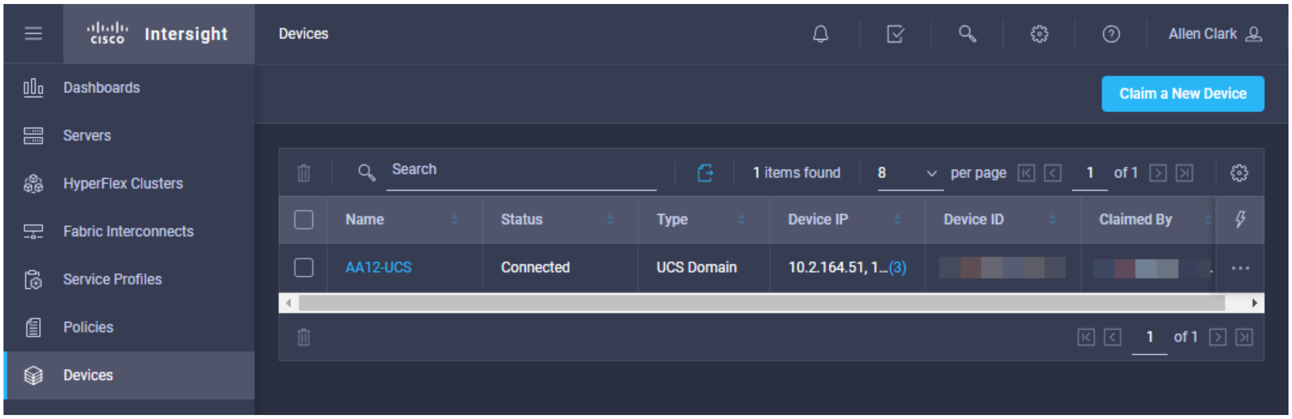
Claim a New Device

To claim your device, you must have the Device ID and Claim Code.

Device ID *

Claim Code *

8. Click Claim.



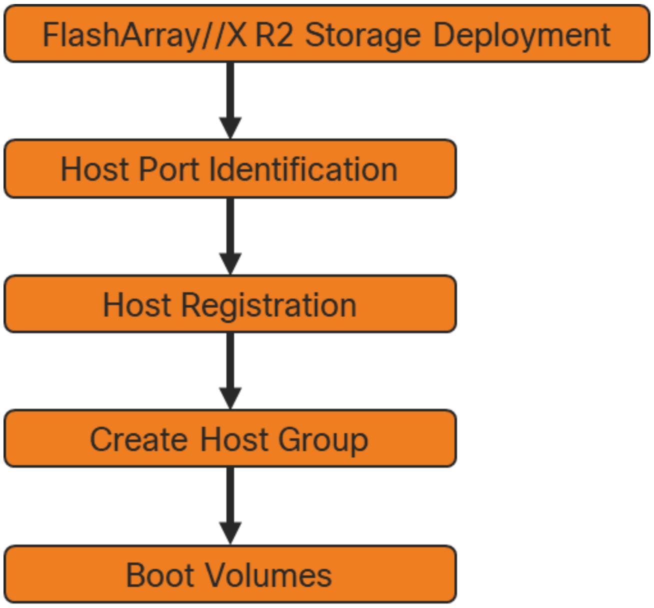
□	Name	Status	Type	Device IP	Device ID	Claimed By
□	AA12-UCS	Connected	UCS Domain	10.2.164.51, 1...(3)	[redacted]	[redacted]

FlashArray Storage Deployment

The Pure Storage FlashArray//X is accessible to the FlashStack, but no storage has been deployed at this point. The storage to be deployed will include:

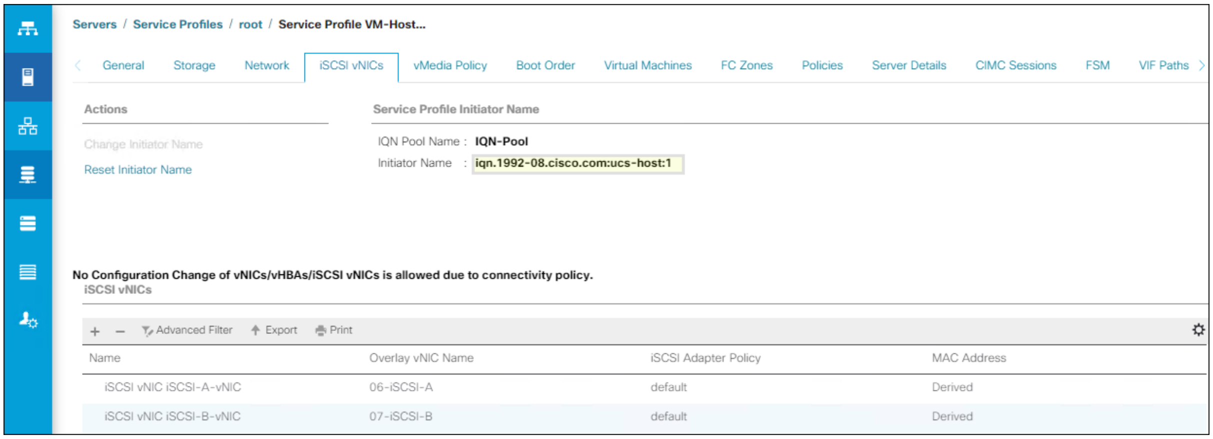
- ESXi iSCSI Boot LUNs
- VMFS Datastores
- VVol Datastores

The iSCSI Boot LUNs will need to be setup from the Pure Storage Web Portal, and the VMFS datastores will be directly provisioned from the vSphere Web Client after the Pure Storage vSphere Web Client Plugin has later been registered with the vCenter.



Host Port Identification

iSCSI Boot LUNs will be mapped by the FlashArray//X using the assigned Initiator Name to the provisioned service profiles. This information can be found within the service profile located within the iSCSI vNICs tab:



Service Profile Initiator Name

IQN Pool Name : **IQN-Pool**

Initiator Name : **iqn.1992-08.cisco.com:ucs-host:1**

No Configuration Change of vNICs/vHBAs/iSCSI vNICs is allowed due to connectivity policy.

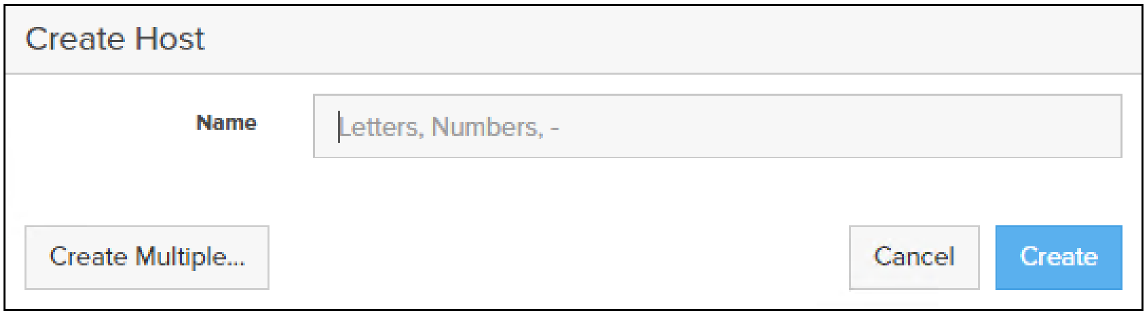
iSCSI vNICs

Name	Overlay vNIC Name	iSCSI Adapter Policy	MAC Address
iSCSI vNIC iSCSI-A-vNIC	06-iSCSI-A	default	Derived
iSCSI vNIC iSCSI-B-vNIC	07-iSCSI-B	default	Derived

Host Registration

For Host registration, from the Pure Storage Web Portal, follow these steps:

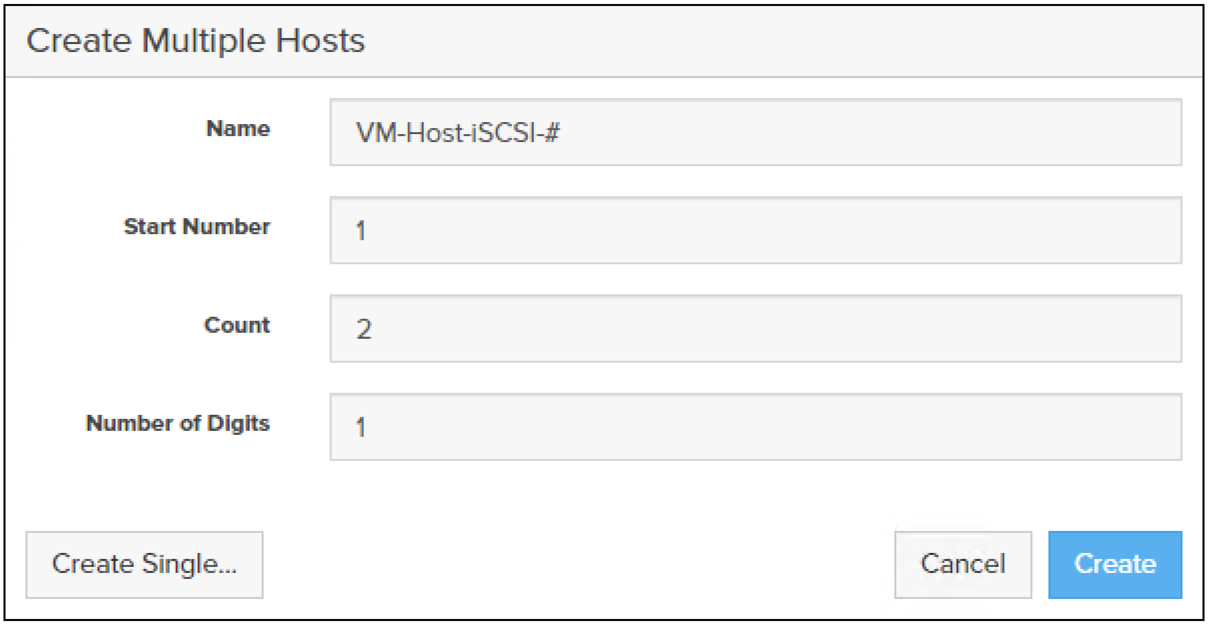
1. Select Storage > Hosts
2. Select the + icon in the Hosts Panel
3. After clicking the Create Host (+) option, a pop-up will appear to create an individual host entry on the FlashArray



Create Host

Name: Letters, Numbers, -

4. To create more than one host entry, click the Create Multiple… option, filling in the Name, Start Number, Count, and Number of Digits, with a "#" appearing in the name where an iterating number will appear:



Create Multiple Hosts

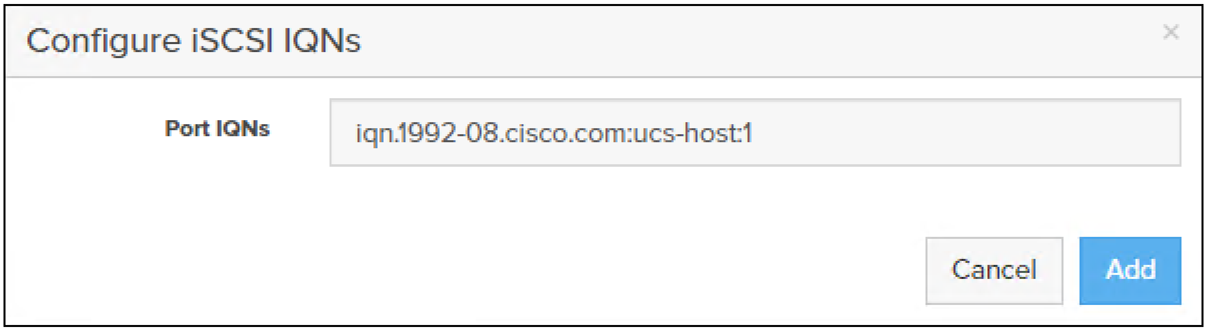
Name: VM-Host-iSCSI-#

Start Number: 1

Count: 2

Number of Digits: 1

5. Click Create to add the hosts.
6. For each host created, select the host.
7. In the Host view, select 'Configure IQNs…' from the Host Ports menu.
8. A pop-up will appear for Configure iSCSI IQNs for Host <host being configured>. Within this pop-up, enter the IQN Initiator Name found within the service profile for the host being configured:

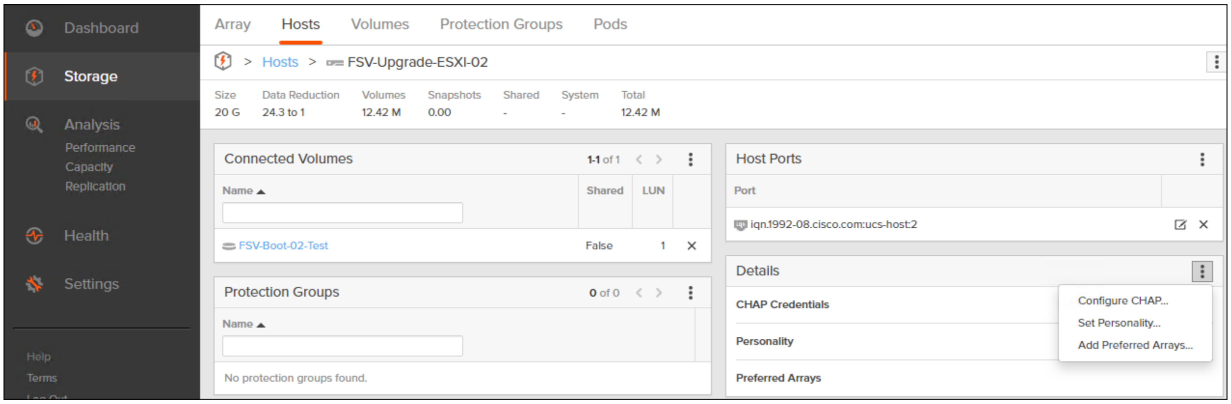


Configure iSCSI IQNs

Port IQNs: iqn.1992-08.cisco.com:ucs-host:1

9. After entering the IQN, click Add to add the Host Ports.

10. Select 'Set Personality…' in the Details Menu.



Size	Data Reduction	Volumes	Snapshots	Shared	System	Total
20 G	24.3 to 1	12.42 M	0.00	-	-	12.42 M

Connected Volumes (1-1 of 1)

Name ▲	Shared	LUN
FSV-Boot-02-Test	False	1

Protection Groups (0 of 0)

Name ▲

No protection groups found.

Host Ports

Port
iqn.1992-08.cisco.com:ucs-host:2

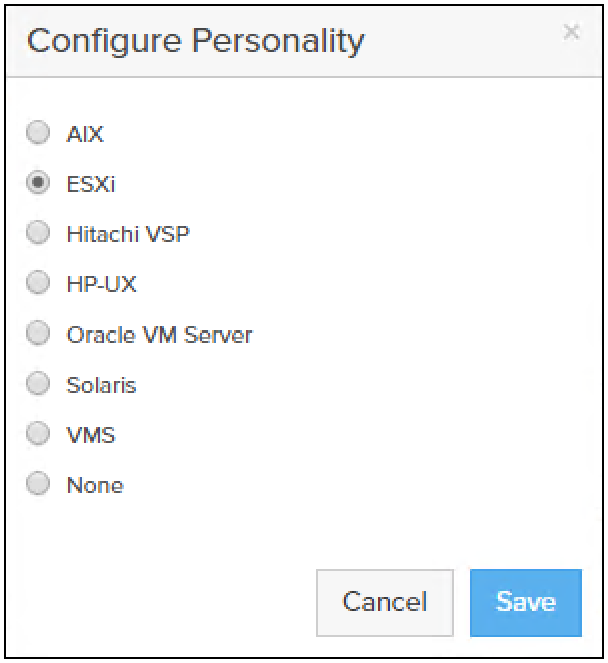
Details

CHAP Credentials

Personality

Preferred Arrays

11. Select ESXi and click Save.



Configure Personality

○ AIX
● ESXi
○ Hitachi VSP
○ HP-UX
○ Oracle VM Server
○ Solaris
○ VMS
○ None

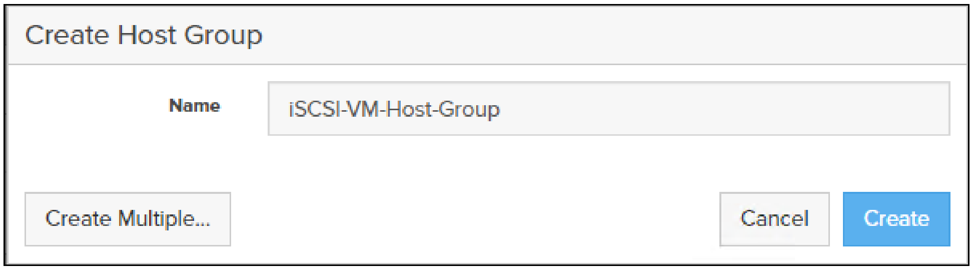
12. Repeat steps 1-11 for each host created.

To create a Host Group, follow these steps in the Pure Storage Web Portal:

1. Select Storage > Hosts.

2. Select the + icon in the Host Groups Panel.

3. A pop-up will appear to create a host group on the FlashArray.



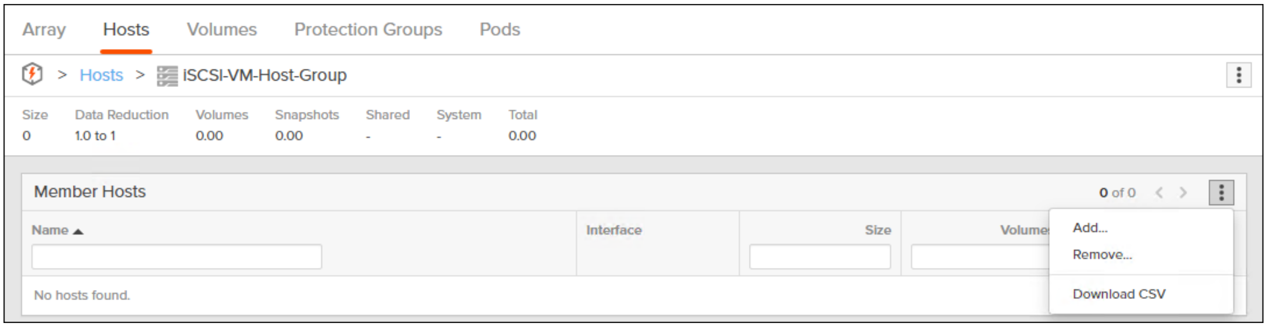
Create Host Group

Name: iSCSI-VM-Host-Group

4. Provide a name for the group and click Create.

5. Select the group in the Host Groups Panel.

6. In the Host Group view, select 'Add...' from the Member Hosts menu.

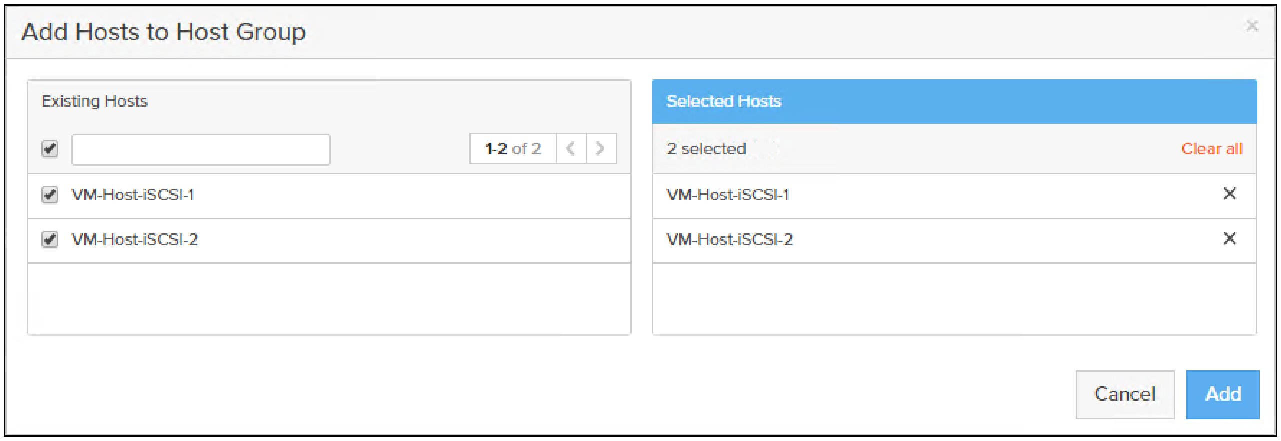


Size	Data Reduction	Volumes	Snapshots	Shared	System	Total
0	1.0 to 1	0.00	0.00	-	-	0.00

Member Hosts

No hosts found.

7. Select the host to be part of the host group.



Add Hosts to Host Group

Existing Hosts
☑ VM-Host-iSCSI-1
☑ VM-Host-iSCSI-2

Selected Hosts (2 selected)
VM-Host-iSCSI-1 ✕
VM-Host-iSCSI-2 ✕

8. Click Add.

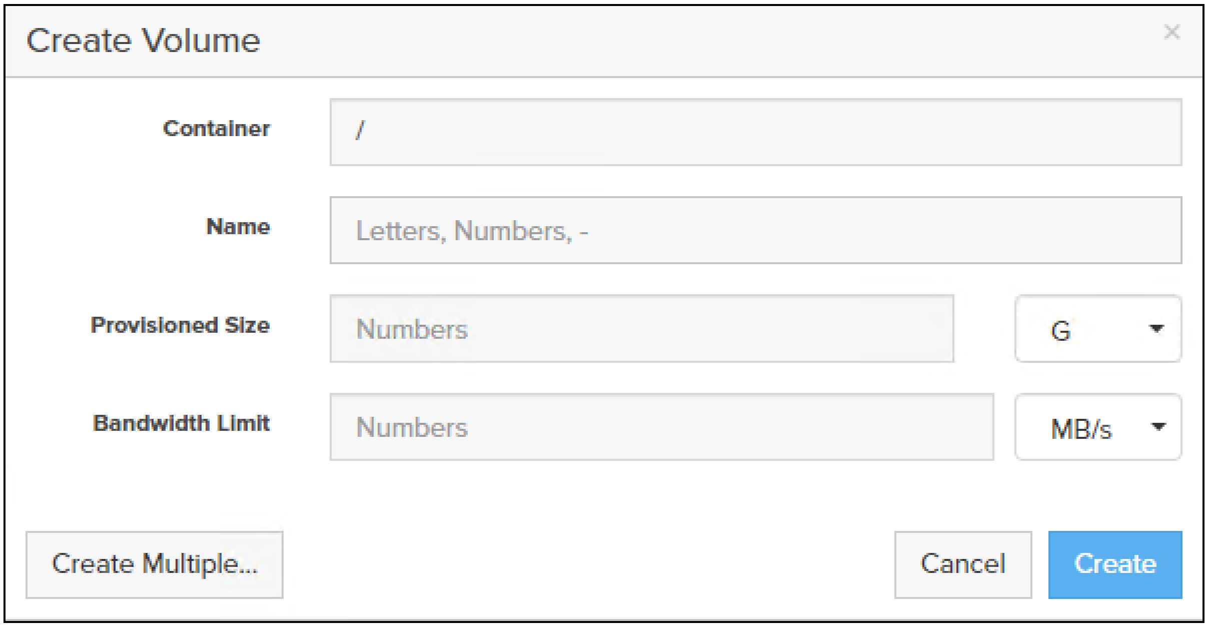
Private Boot Volumes for each ESXi Host

To create private boot volumes for each ESXi Host, from the Pure Storage Web Portal, follow these steps:

1. Select Storage > Volumes.

2. Select the + icon in the Volumes Panel.

3. A pop-up will appear to create a volume on the FlashArray.



Create Volume

Container /

Name Letters, Numbers, -

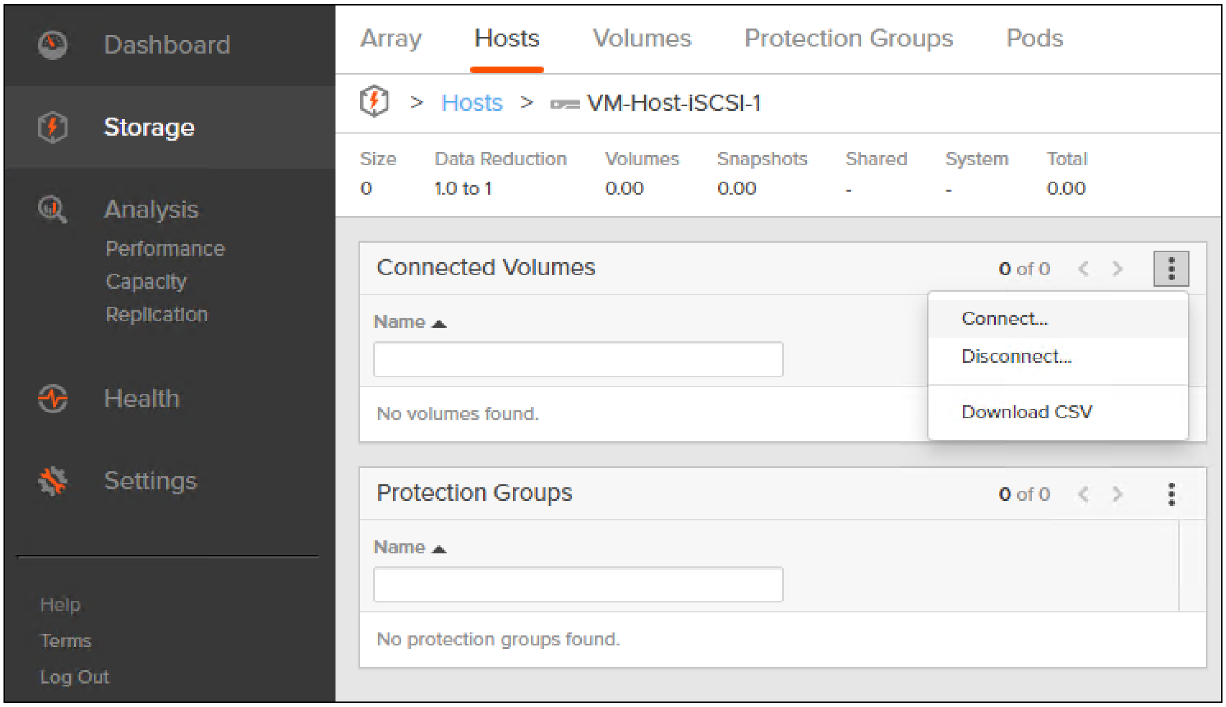
Provisioned Size Numbers G

Bandwidth Limit Numbers MB/s

4. To create more than one volume, click the Create Multiple… option, filling in the Name, Provisioned Size, Staring Number, Count, and Number of Digits, with a "#" appearing in the name where an iterating number will appear.

5. Click **Create** to provision the volumes to be used as iSCSI boot LUNs.

6. Go back to the Hosts section under the Storage tab. Click one of the hosts and select the gear icon pull-down within the Connected Volumes tab within that host.



> Hosts > VM-Host-iSCSI-1

Size	Data Reduction	Volumes	Snapshots	Shared	System	Total
0	1.0 to 1	0.00	0.00	-	-	0.00

Connected Volumes 0 of 0

Name ▲

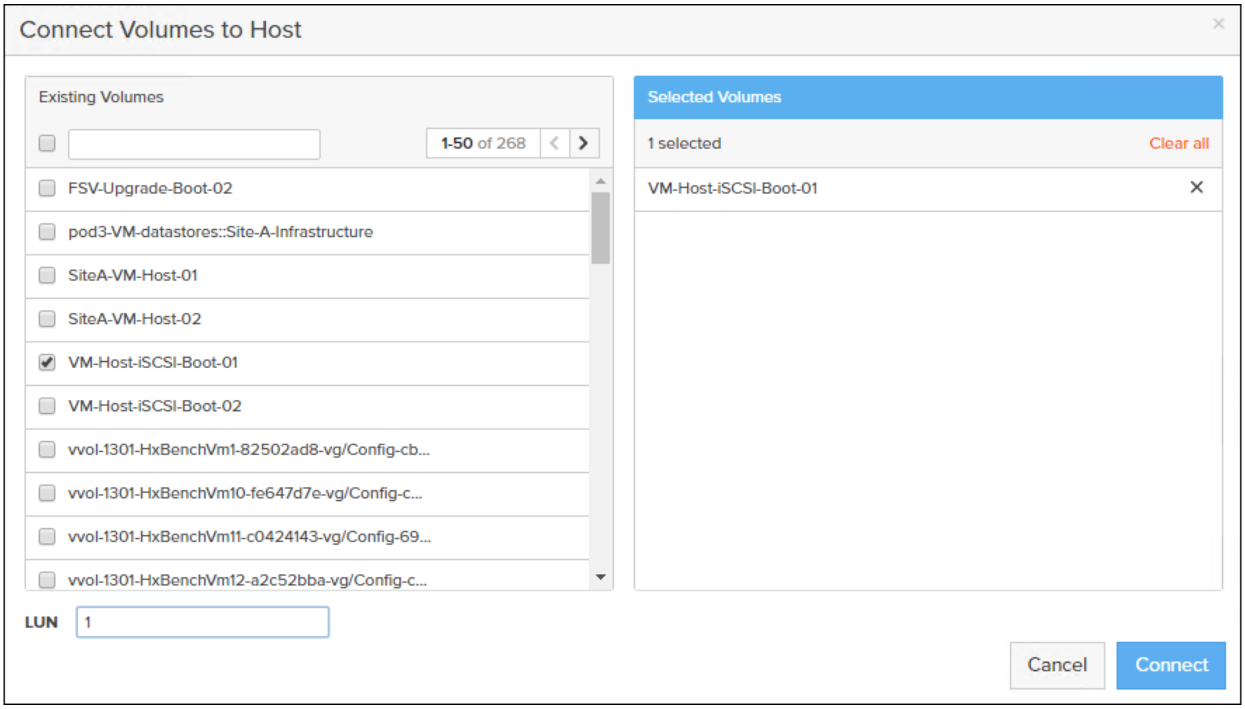
No volumes found.

Protection Groups 0 of 0

Name ▲

No protection groups found.

7. Within the drop-down list of the gear icon, select **Connect Volumes**, and a pop-up will appear.



Connect Volumes to Host

Existing Volumes 1-50 of 268

- □ FSV-Upgrade-Boot-02
- □ pod3-VM-datastores::Site-A-Infrastructure
- □ SiteA-VM-Host-01
- □ SiteA-VM-Host-02
- ☑ VM-Host-iSCSI-Boot-01
- □ VM-Host-iSCSI-Boot-02
- □ vvol-1301-HxBenchVm1-82502ad8-vg/Config-cb...
- □ vvol-1301-HxBenchVm10-fe647d7e-vg/Config-c...
- □ vvol-1301-HxBenchVm11-c0424143-vg/Config-69...
- □ vvol-1301-HxBenchVm12-a2c52bba-vg/Config-c...

Selected Volumes

1 selected

VM-Host-iSCSI-Boot-01 ✕

LUN 1

LUN ID 1 should be used for the boot.

8. Select the volume that has been provisioned for the host, set the LUN ID for the volume, click the + next to the volume, and select Confirm to proceed. Repeat the steps for connecting volumes for each of the host/volume pairs configured.

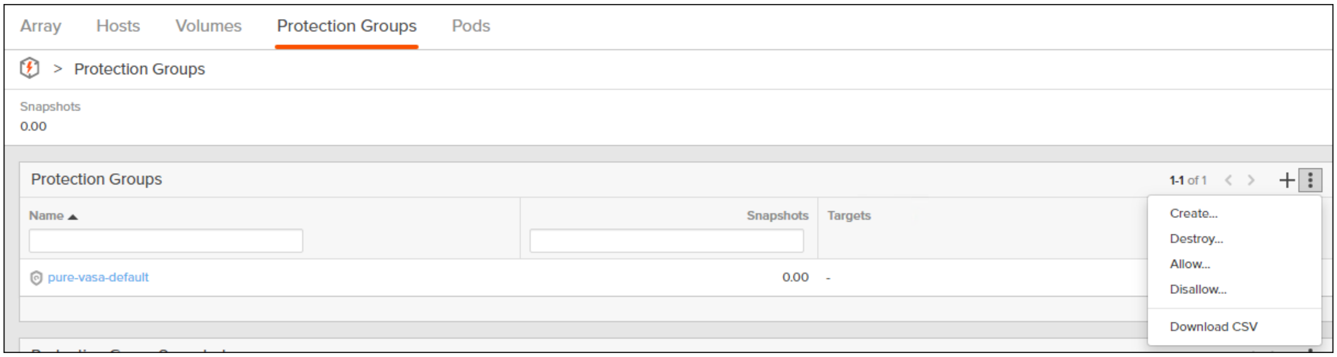
Configure Storage Policy Based Management

vSphere can communicate to the array through the VASA provider to find out what features it supports and allow the vSphere administrator to assign, change, or remove functionality on a VVol on demand and policies.
Below is an example of how to configure a Protection group that will provide hourly snapshots that will be retained for 1 day, with 4 snapshots per day retained for 7 days. These policies should be configured based on application snapshot need.

To configure Storage Policy Based Management, follow these steps:

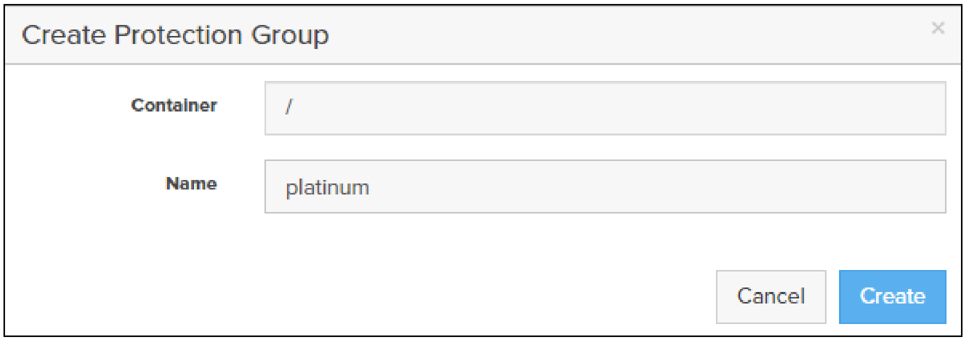
1. From the Pure Storage Web Porta, select Storage > Protection Groups.

2. Select 'Create…' from the Protection Groups menu.



Name ▲	Snapshots	Targets
pure-vasa-default	0.00	-

3. Enter a name.

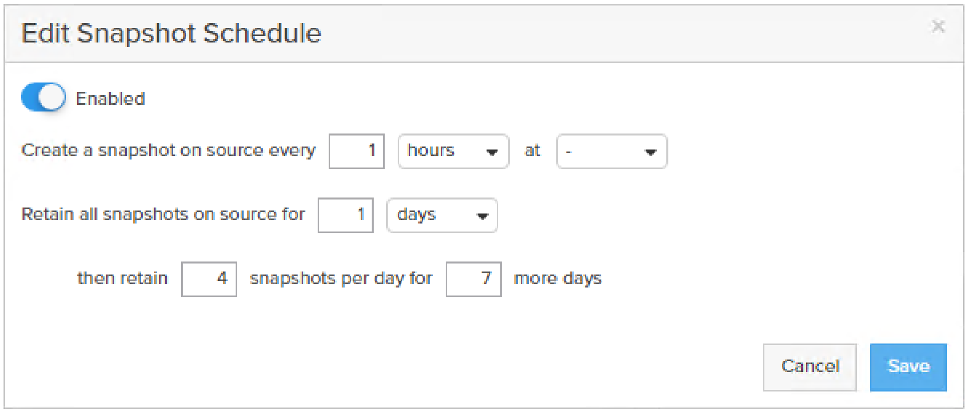


Container: /

Name: platinum

4. Select the protection group.

5. Edit the Snapshot Schedule based on your operational requirements.



Enabled

Create a snapshot on source every 1 hours at -

Retain all snapshots on source for 1 days

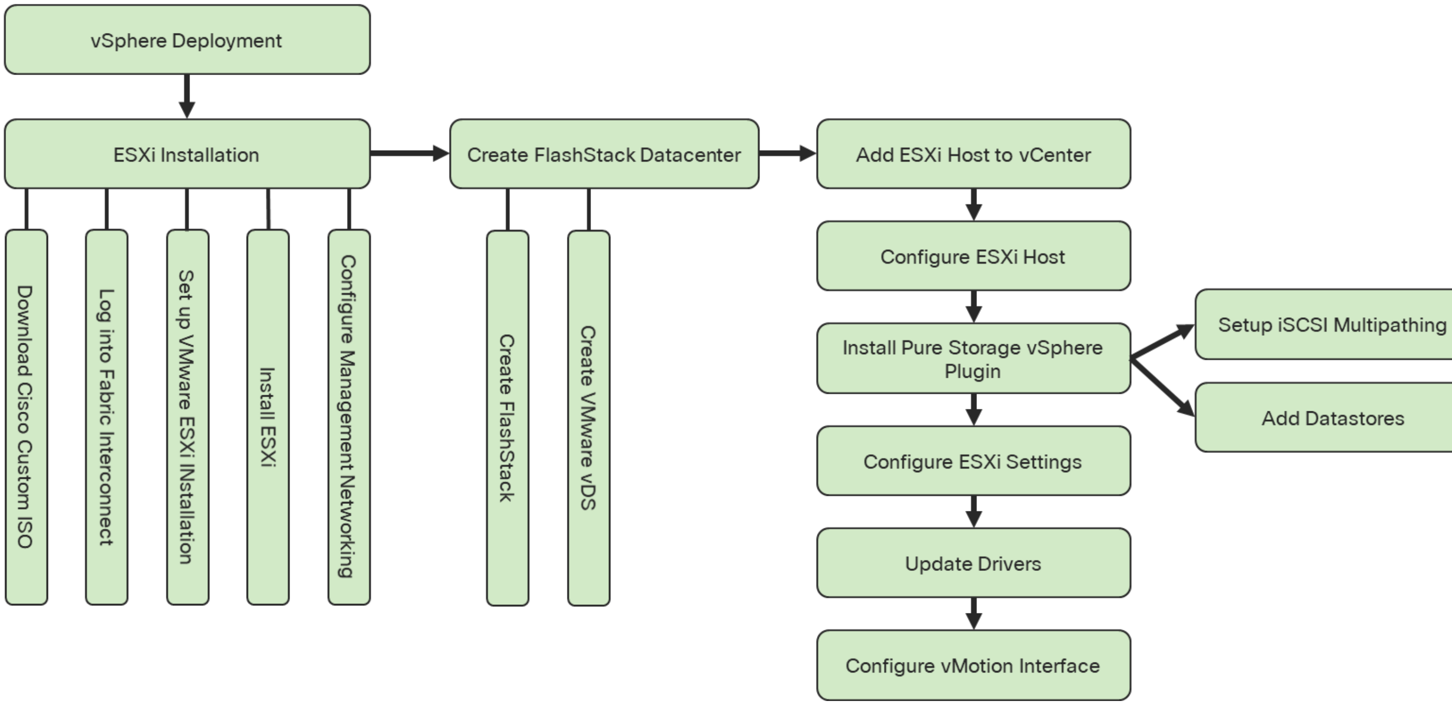
then retain 4 snapshots per day for 7 more days

6. Click Save.

vSphere Deployment

ESXi Installation

This section provides detailed instructions to install VMware ESXi 6.7 U1 in a FlashStack environment. After the procedures are completed, the iSCSI SAN booted ESXi hosts will be configured.


vSphere Deployment
ESXi Installation
Create FlashStack Datacenter
Add ESXi Host to vCenter
Download Cisco Custom ISO
Log into Fabric Interconnect
Set up VMware ESXi INstallation
Install ESXi
Configure Management Networking
Create FlashStack
Create VMware vDS
Configure ESXi Host
Install Pure Storage vSphere Plugin
Setup iSCSI Multipathing
Add Datastores
Configure ESXi Settings
Update Drivers
Configure vMotion Interface

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

Download Cisco Custom Image for ESXi 6.7 U1

The VMware Cisco Custom Image will be needed for use during installation by manual access to the Cisco UCS KVM vMedia, or through a vMedia Policy covered in a previous subsection. If the Cisco Custom Image was not downloaded during the vMedia Policy setup, download it now by following these steps:

1. Click the following link: https://my.vmware.com/web/vmware/details?downloadGroup=OEM-ESXI67U1-CISCO&productId=859
2. You will need a user id and password on vmware.com to download this software.
3. Download the .iso file.

Log into Cisco UCS 6454 Fabric Interconnect

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

To log into the Cisco UCS environment, follow these steps:

1. Open a web browser to https:// <<var_ucs_mgmt_vip>>
2. Select the Launch UCS Manager Section in the HTML section to pull up the UCSM HTML5 GUI.
3. Enter admin for the **Username**, and provide the password used during setup.
4. Within the UCSM select **Servers** -> **Service Profiles** and pick the first host provisioned as VM-Host-iSCSI-01.
5. Click the **KVM Console** option within **Actions** and accept the KVM server certificate in the new window or browser tab that is spawned for the KVM session.
6. Click the link within the new window or browser tab to load the KVM client application.

Setup VMware ESXi Installation

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

To prepare the server for the OS installation, follow these steps on each ESXi host:

1. In the KVM window, click Virtual Media icon in the upper right of the screen.
2. Click Activate Virtual Devices
3. Click Virtual Media again and select Map CD/DVD.
4. Browse to the ESXi installer ISO image file and click Open.
5. Click Map Device.
6. Click the KVM tab to monitor the server boot.
7. Boot the server by selecting Boot Server and clicking OK, then click OK again.

Install ESXi

To install VMware ESXi to the iSCSI bootable LUN of the hosts, follow these 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 LUN that was previously set up as the installation disk for ESXi and press Enter to continue with the installation.
5. Select the appropriate keyboard layout and press Enter.
6. Enter and confirm the root password and press Enter.

7. The installer issues a warning that the selected disk will be repartitioned. Press F11 to continue with the installation.
8. After the installation is complete, if using locally mapped Virtual Media, click the Virtual Media tab and clear the ✓ mark next to the ESXi installation media. Click Yes.
9. From the KVM window, press Enter to reboot the server.

Setup 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, follow these steps on each ESXi host.

To configure the ESXi host with access to the management network, follow these 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 **Network Adapters** option leave vmnic0 selected, arrow down to vmnic1 and press space to select vmnic1 as well and press Enter.
5. Select the **VLAN (Optional)** option and press Enter.
6. Enter the <<var_ib_mgmt_vlan_id>> and press Enter.
7. From the Configure Management Network menu, select **IPv4 Configuration** and press Enter.
8. Select the Set Static IP Address and Network Configuration option by using the space bar.
9. Enter <<var_vm_host_iscsi_01_ip>> for the **IPv4 Address** for managing the first ESXi host.
10. Enter <<var_ib_mgmt_vlan_netmask_length>> for the **Subnet Mask** for the first ESXi host.
11. Enter <<var_ib_mgmt_gateway>> for the **Default Gateway** for the first ESXi host.
12. Press Enter to accept the changes to the IPv4 configuration.
13. Select the **DNS Configuration** option and press Enter.

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

14. Enter the IP address of <<var_nameserver_ip>> for the **Primary DNS Server**.
15. Optional: Enter the IP address of the **Secondary DNS Server**.
16. Enter the fully qualified domain name (FQDN) for the first ESXi host.
17. Press Enter to accept the changes to the DNS configuration.
18. Select the **IPv6 Configuration** option and press Enter.

19. Using the spacebar, select Disable IPv6 (restart required) and press Enter.

20. Press Esc to exit the Configure Management Network submenu.

21. Press Y to confirm the changes and return to the main menu.

22. The ESXi host reboots. After reboot, press F2 and log back in as root.

23. Select Test Management Network to verify that the management network is set up correctly and press Enter.

24. Press Enter to run the test.

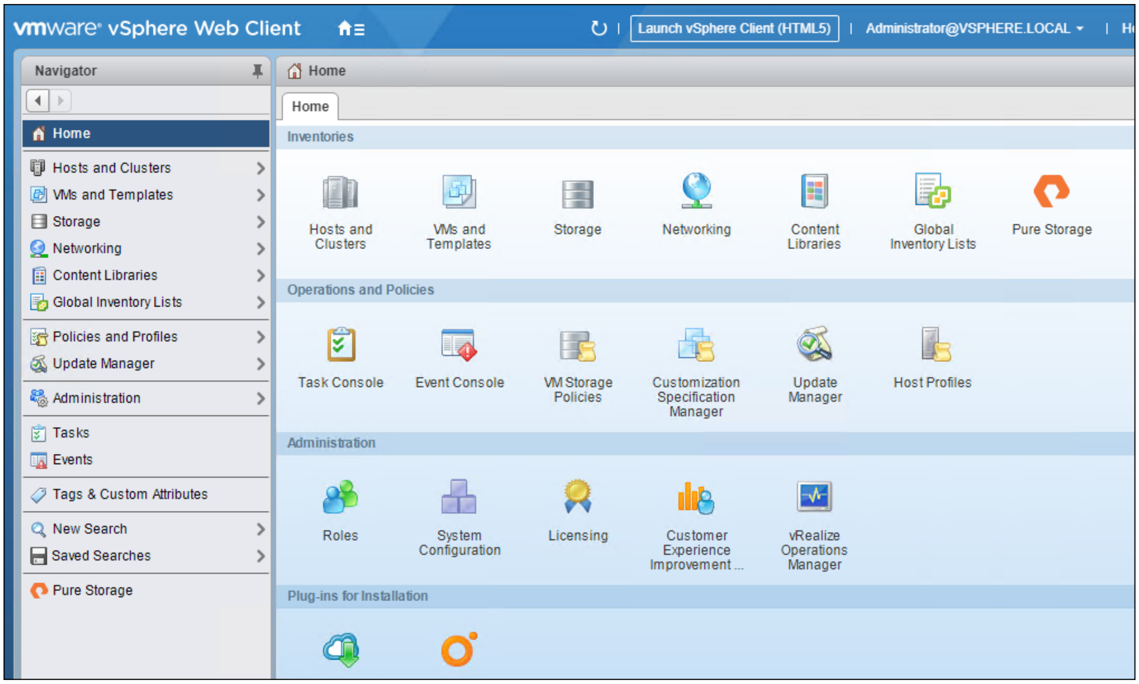
25. Press Enter to exit the window, and press Esc to log out of the VMware console.

26. Repeat steps in Set Up VMware ESXi Installation, Install ESXi, and Set UP Management Networking for ESXi Host for additional hosts provisioned, using appropriate values.

Create FlashStack Datacenter

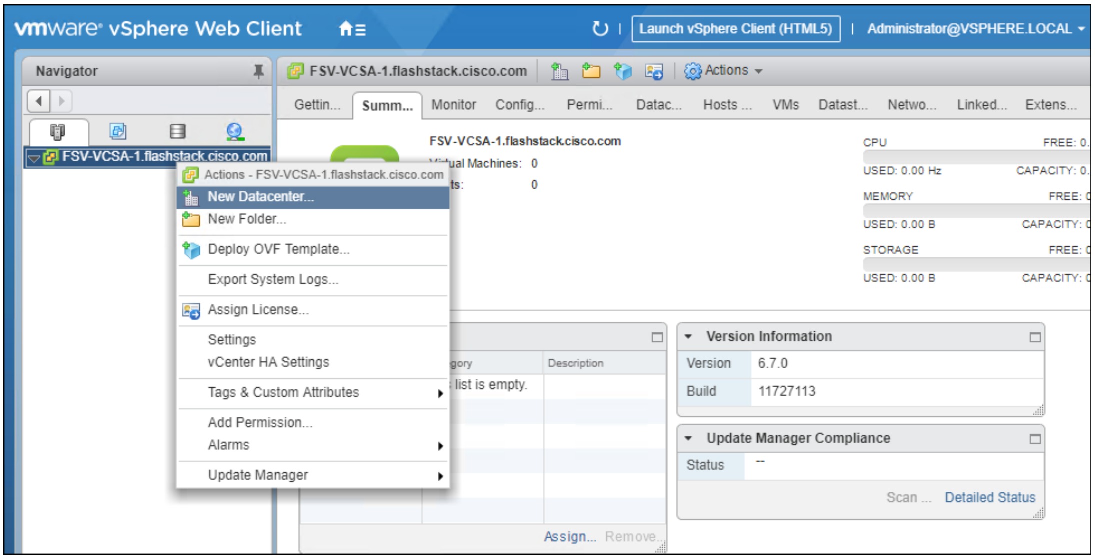
If a new Datacenter is needed for the FlashStack, follow these steps on the vCenter:

1. Connect to the vSphere Web Client and click **Hosts and Clusters** from the left side Navigator window or the **Hosts and Clusters** icon from the Home center window.

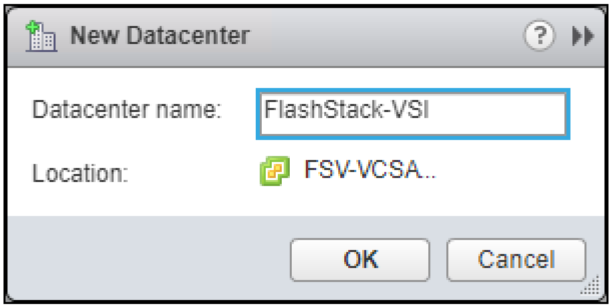


2. From Hosts and Clusters:

   a. Right-click the vCenter icon and select New Datacenter… from the drop-down list.



b. From the New Datacenter pop-up dialogue enter in a Datacenter name and click OK.


New Datacenter

Datacenter name: FlashStack-VSI

Location: FSV-VCSA...

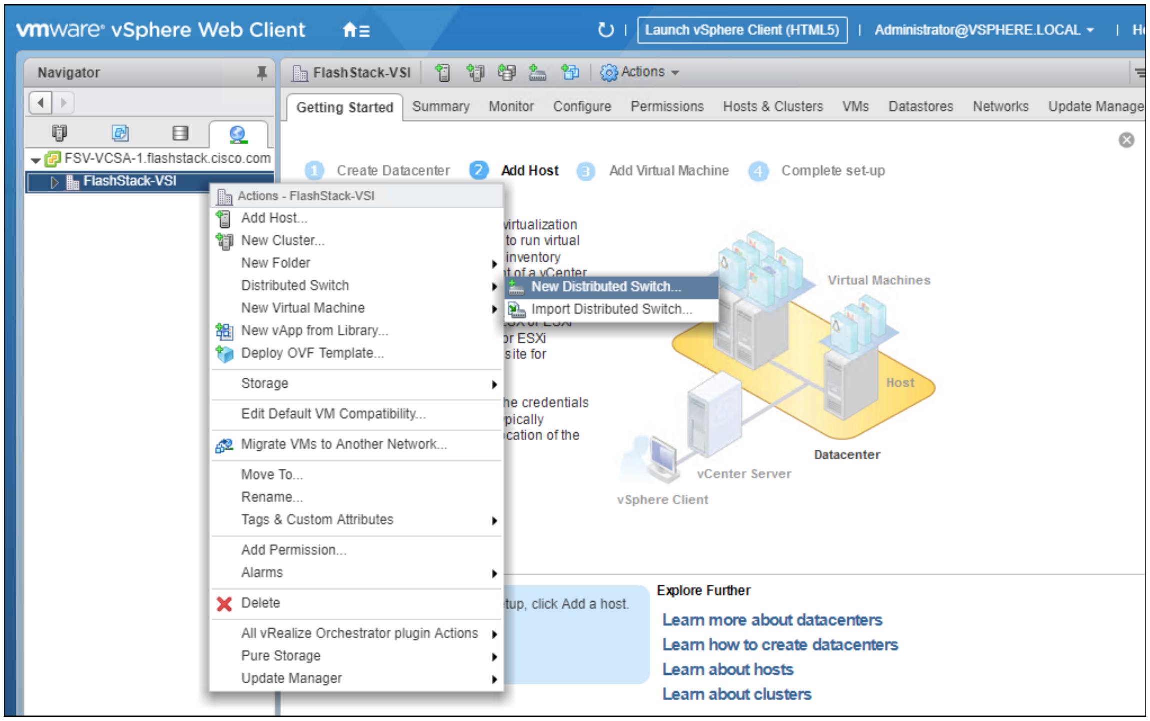
Create VMware vDS for Infrastructure and Application Traffic

The VMware vDS setup will consist of two vDS that are separated for Infrastructure use versus Application traffic.

FlashStack Infrastructure vDS

To configure the first VMware vDS, follow these steps:

1. Connect to the vSphere Web Client and click Networking from the left side Navigator window or the Networking icon from the Home center window.
2. Right-click the FlashStack-VSI datacenter and select Distributed Switch > New Distributed Switch…

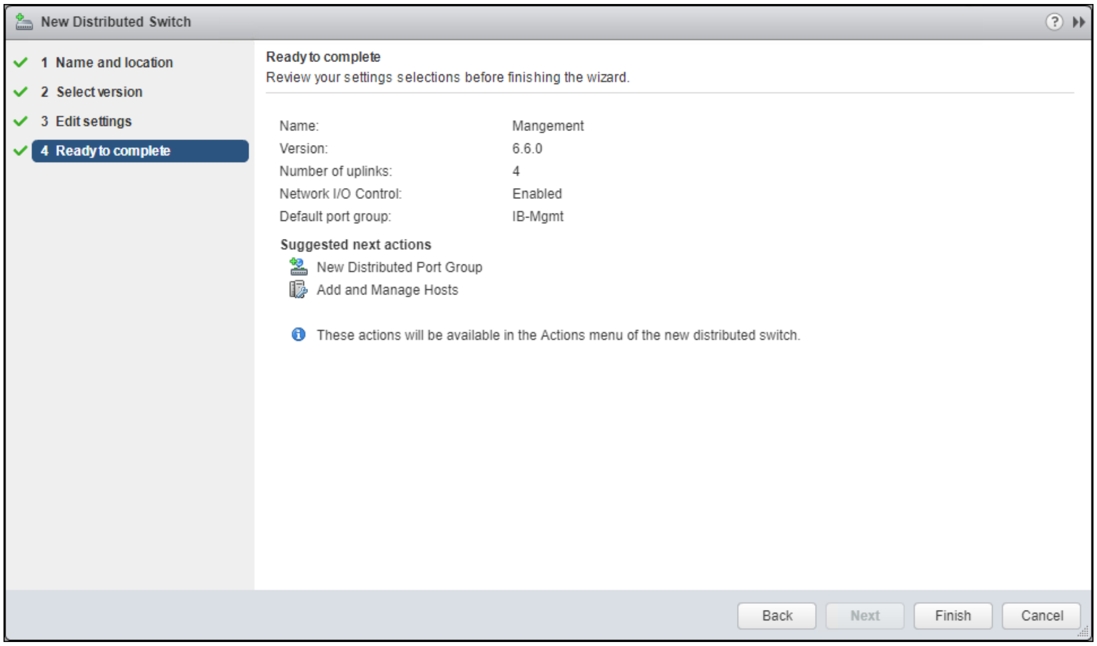


3. Give the Distributed Switch a descriptive name and click Next.

4. Make sure Distributed switch: 6.6.0 is selected and click Next.

5. Leave the Number of uplinks at 4. If VMware Network I/O Control is to be used for Quality of Service, leave Network I/O Control Enabled. Otherwise, Disable Network I/O Control. Enter IB-Mgmt for the name of the default Port group to be created. Click Next.

6. Review the information and click Finish to complete creating the vDS.



New Distributed Switch

1 Name and location
2 Select version
3 Edit settings
4 Ready to complete

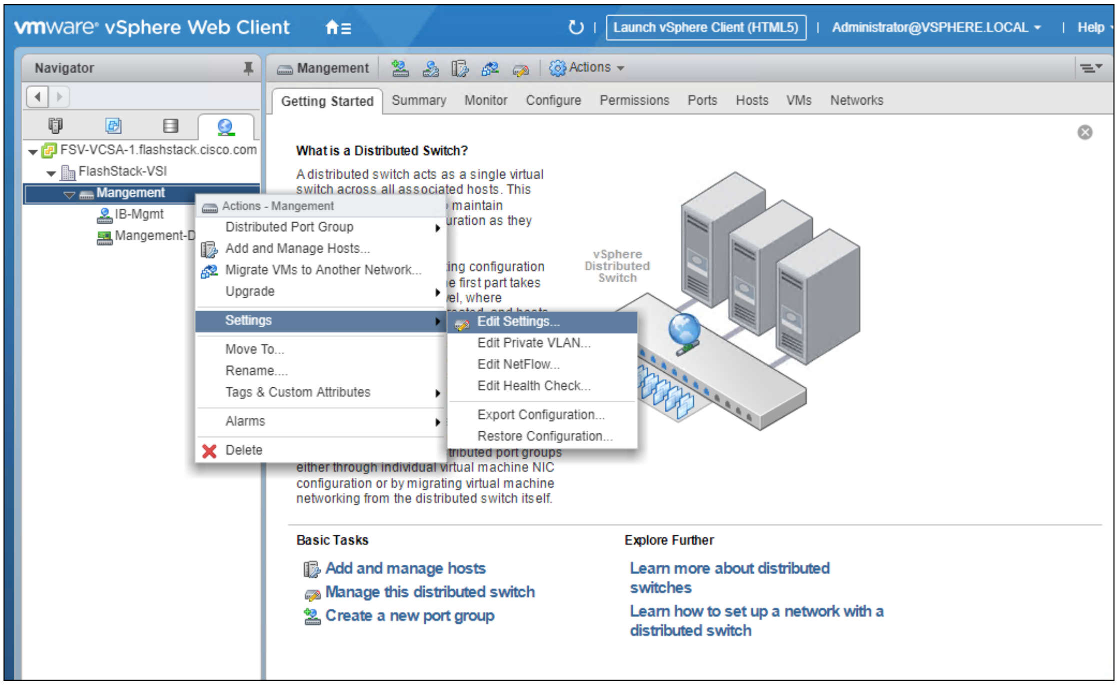
Ready to complete
Review your settings selections before finishing the wizard.

Name:	Mangement
Version:	6.6.0
Number of uplinks:	4
Network I/O Control:	Enabled
Default port group:	IB-Mgmt

Suggested next actions
New Distributed Port Group
Add and Manage Hosts

These actions will be available in the Actions menu of the new distributed switch.

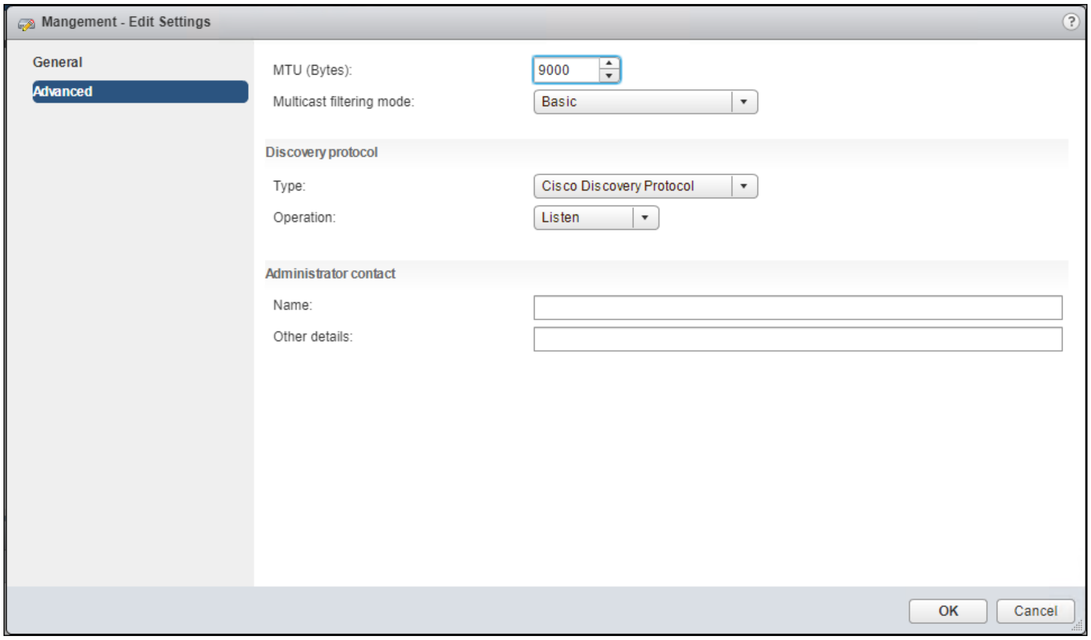
7. Right-click the newly created vDS, and select Settings -> Edit Settings…



What is a Distributed Switch?

A distributed switch acts as a single virtual switch across all associated hosts. This … maintain … uration as they … ing configuration … e first part takes … el, where … tributed port groups either through individual virtual machine NIC configuration or by migrating virtual machine networking from the distributed switch itself.

8. Click the Advanced option side of the Edit Settings window and adjust the MTU from 1500 to 9000.



MTU (Bytes): 9000

Multicast filtering mode: Basic

Discovery protocol

Type: Cisco Discovery Protocol

Operation: Listen

Administrator contact

Name:

Other details:

9. Click OK to save the changes.

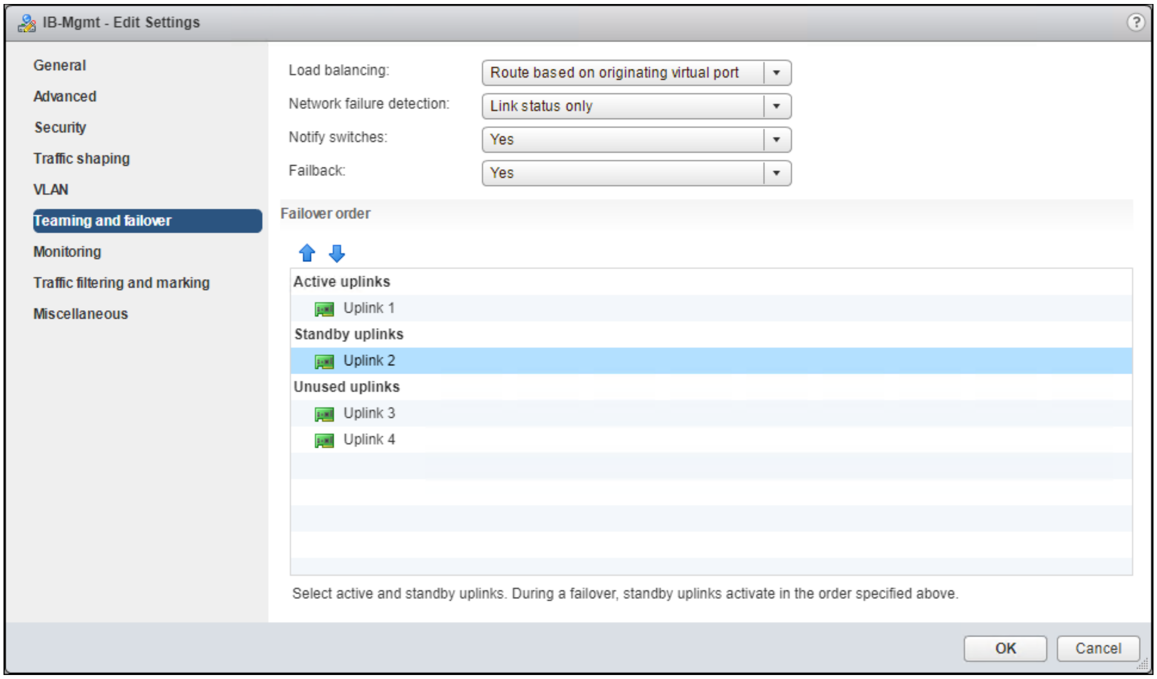
10. Expand the FlashStack VSI datacenter and the newly created vDS.

11. Right-click the IB-Mgmt Distributed Port Group, and select Edit Settings…

12. Click VLAN, changing VLAN type from None to VLAN, and enter in the appropriate VLAN number for the IB-Mgmt network.

13. Click the Teaming and Failover and move the Uplinks 3 and 4 to the Unused uplinks state and move the Uplink 2 to the Standby uplinks state.

> The movement of Uplink 2 to standby is guiding Management traffic to stay within the A side fabric contained within Uplink 1 to prevent unnecessary traffic hops up into the Nexus switch to traverse between fabrics. Uplinks 3 and 4 are set as unused as these are the vMotion vNICs and will be used by the other Distributed Port Group in this vDS.



Load balancing: Route based on originating virtual port

Network failure detection: Link status only

Notify switches: Yes

Failback: Yes

Failover order

Active uplinks
- Uplink 1

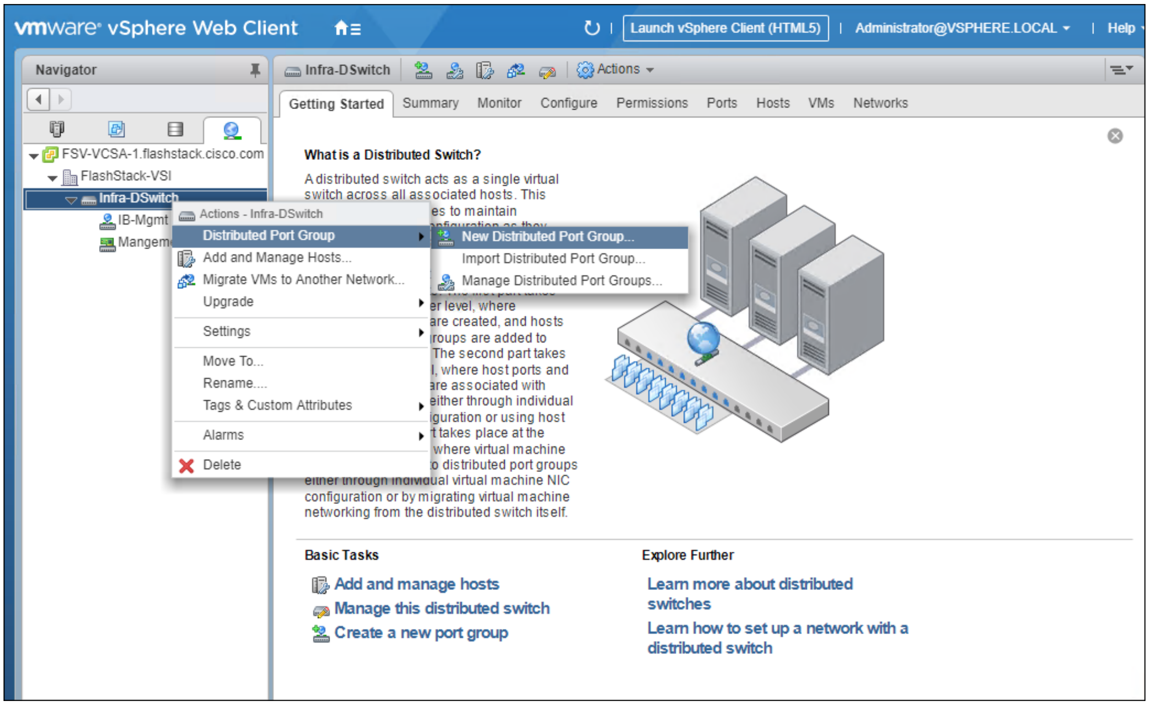
Standby uplinks
- Uplink 2

Unused uplinks
- Uplink 3
- Uplink 4

Select active and standby uplinks. During a failover, standby uplinks activate in the order specified above.

14. Click OK to save the changes.

15. Right-click the infrastructure vDS (Infra-DSwitch), and select Distributed Port Group -> New Distributed Port Group…



What is a Distributed Switch?

A distributed switch acts as a single virtual switch across all associated hosts. This ...es to maintain ...er level, where ...are created, and hosts ...roups are added to ... The second part takes ..., where host ports and ...are associated with ...either through individual ...guration or using host ...t takes place at the ... where virtual machine ...o distributed port groups either through individual virtual machine NIC configuration or by migrating virtual machine networking from the distributed switch itself.

Basic Tasks

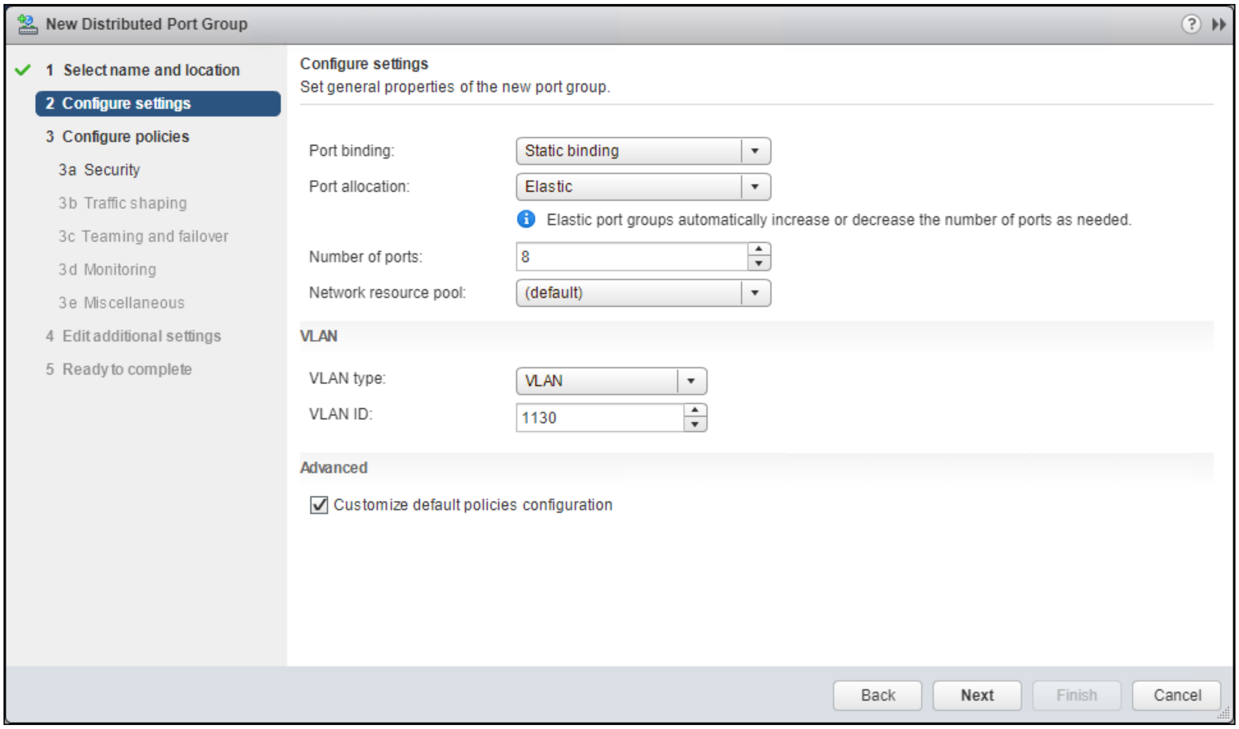
- Add and manage hosts
- Manage this distributed switch
- Create a new port group

Explore Further

- Learn more about distributed switches
- Learn how to set up a network with a distributed switch

16. Name the new Port Group vMotion and click Next.

17. Change the VLAN type from None to VLAN, select the VLAN ID appropriate for your vMotion traffic, and select the Customize default policies configuration check box under the Advanced section.



Configure settings

Set general properties of the new port group.

Port binding:	Static binding
Port allocation:	Elastic
	Elastic port groups automatically increase or decrease the number of ports as needed.
Number of ports:	8
Network resource pool:	(default)

VLAN

VLAN type:	VLAN
VLAN ID:	1130

Advanced

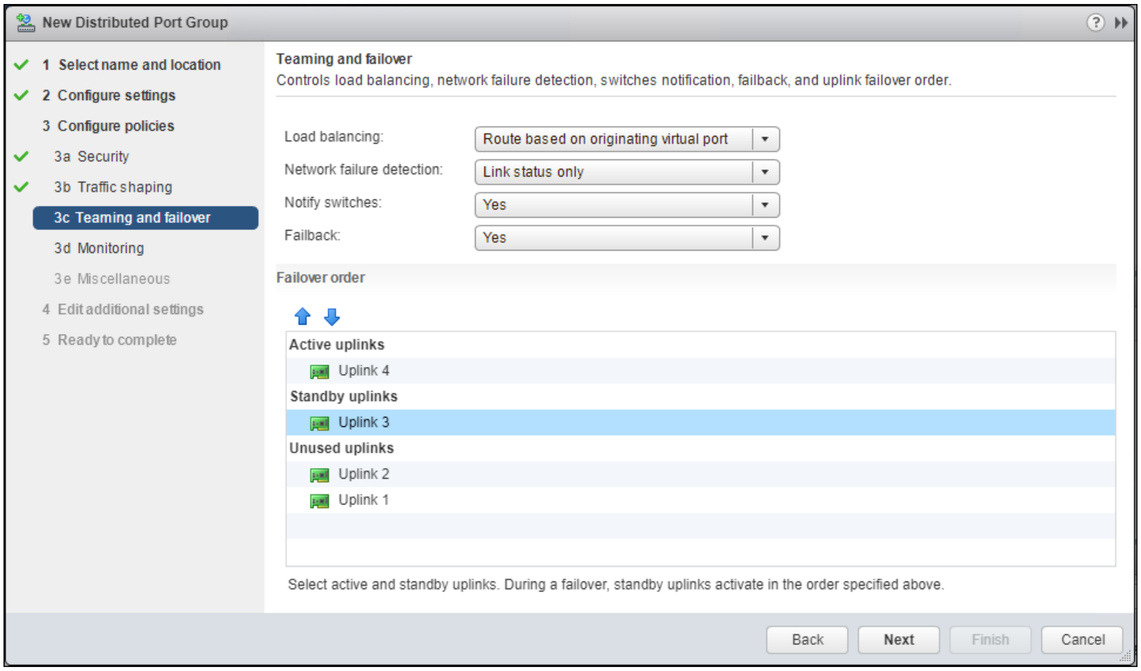
☑ Customize default policies configuration

18. Click Next.

19. Click Next through the Security and Traffic Shaping sections.

20. Within the Teaming and failover section, move Uplinks 1 & 2 to the Unused uplinks section, and move Uplink 3 to the Standby uplinks section.

Teaming for the vMotion Distributed Port Group will be a mirror of teaming on the Infrastructure Distributed Port group. Uplinks 1 and 2 are unused because they are used by the Infrastructure Distributed Port group, and Uplink 3 will be moved to standby to guide vMotion traffic to stay within the B side fabric contained within Uplink 4



New Distributed Port Group

- ✓ 1 Select name and location
- ✓ 2 Configure settings
- 3 Configure policies
- ✓ 3a Security
- ✓ 3b Traffic shaping
- 3c Teaming and failover
- 3d Monitoring
- 3e Miscellaneous
- 4 Edit additional settings
- 5 Ready to complete

Teaming and failover

Controls load balancing, network failure detection, switches notification, failback, and uplink failover order.

Load balancing: Route based on originating virtual port

Network failure detection: Link status only

Notify switches: Yes

Failback: Yes

Failover order

Active uplinks
- Uplink 4

Standby uplinks
- Uplink 3

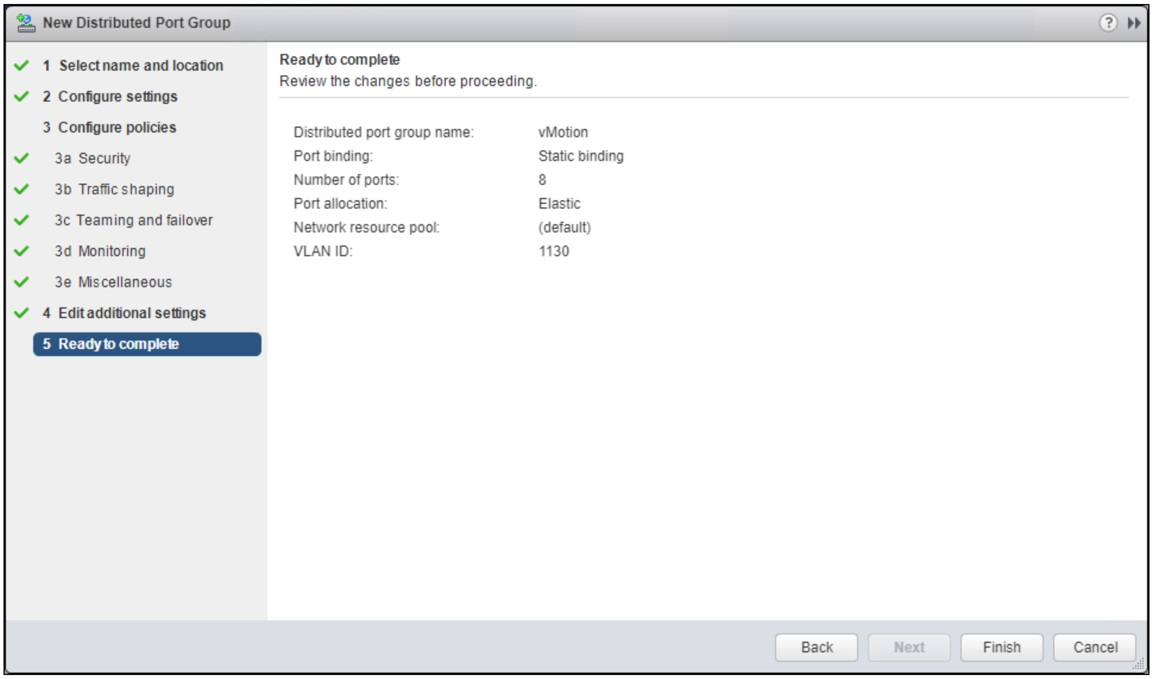
Unused uplinks
- Uplink 2
- Uplink 1

Select active and standby uplinks. During a failover, standby uplinks activate in the order specified above.

21. Click Next

22. Click Next Past Monitoring, Miscellaneous, and Edit additional settings sections.

23. Review the Ready to complete section.



Ready to complete

Review the changes before proceeding.

Distributed port group name:	vMotion
Port binding:	Static binding
Number of ports:	8
Port allocation:	Elastic
Network resource pool:	(default)
VLAN ID:	1130

24. Click Finish to create the Distributed Port Group.

FlashStack Application vDS

To configure the second VMware vDS, follow these steps:

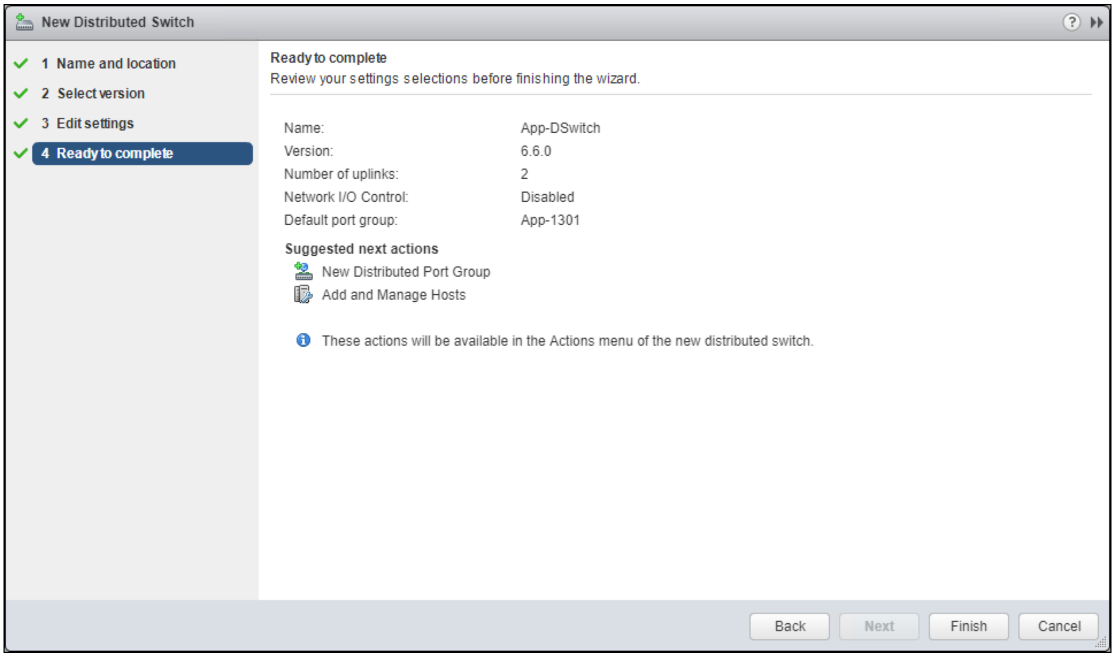
1. Right-click the FlashStack-VSI Datacenter and select Distributed Switch -> New Distributed Switch… to create the Application vDS.

Provide a name for the vDS (App-DSwitch) and click Next.

2. Make sure Distributed switch: 6.6.0 is selected and click Next.

3. Change the Number of uplinks to 2. If VMware Network I/O Control is to be used for Quality of Service, leave Network I/O Control Enabled. Otherwise, Disable Network I/O Control. Enter App-1301 for the name of the default Port group to be created. Click Next.

4. Review the information and click Finish to complete creating the vDS.



Ready to complete

Review your settings selections before finishing the wizard.

Name:	App-DSwitch
Version:	6.6.0
Number of uplinks:	2
Network I/O Control:	Disabled
Default port group:	App-1301

Suggested next actions

- New Distributed Port Group
- Add and Manage Hosts

These actions will be available in the Actions menu of the new distributed switch.

5. Right-click the newly created App-DSwitch vDS, and select Settings -> Edit Settings…

6. Click the Advanced option for the Edit Settings window and change the MTU from 1500 to 9000.

7. Click OK to save the changes.

8. Right-click the App-1301 Distributed Port Group, and select Edit Settings…

9. Click VLAN, changing VLAN type from None to VLAN, and enter in the appropriate VLAN number for the first application network.

> The application Distributed Port Groups will not need to adjust their NIC Teaming as they will be Active/Active within the two vNICs uplinks associated to the App-DSwitch, using the default VMware Route based on originating virtual port load balancing algorithm.

10. Click OK to save the changes.

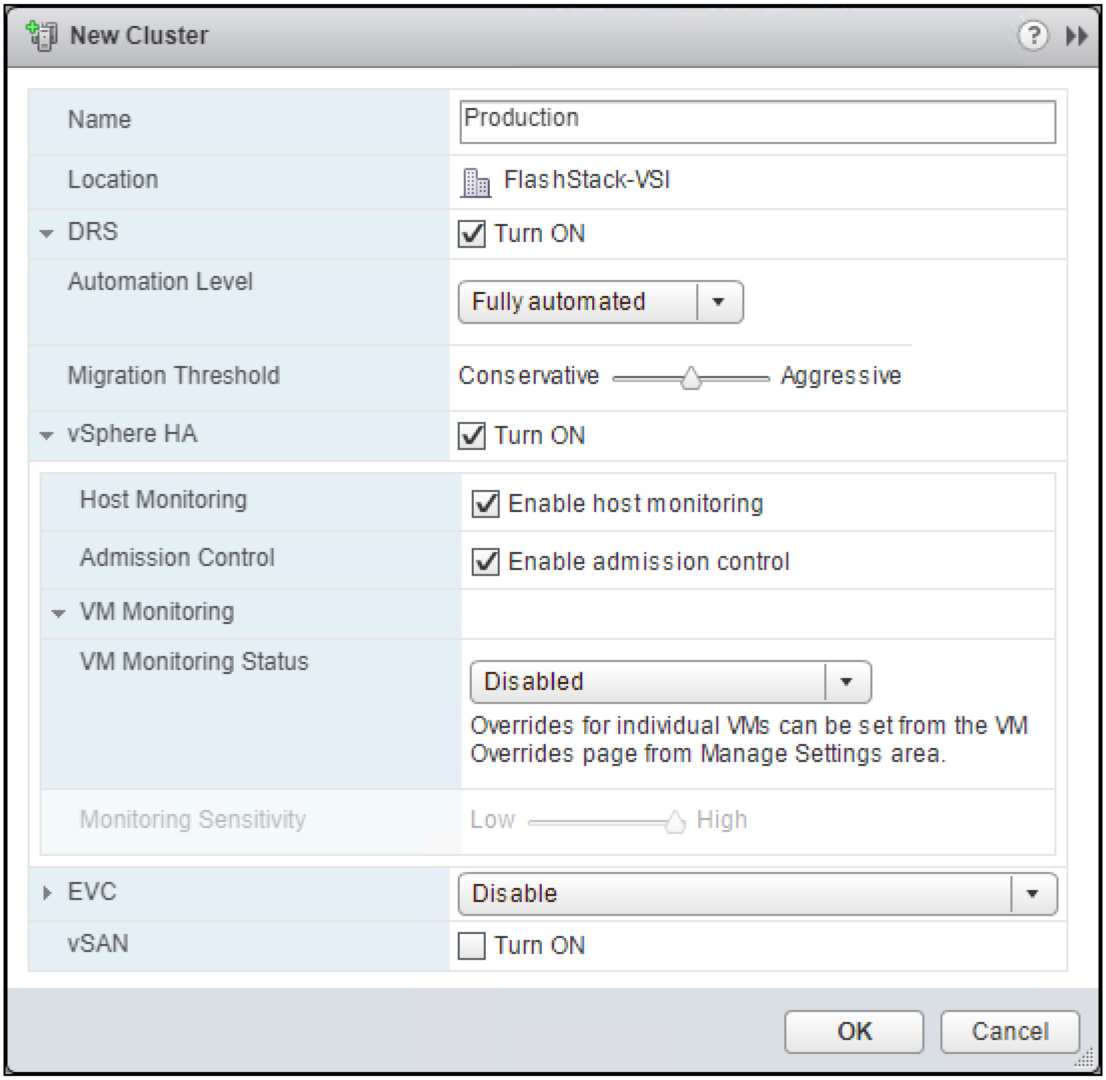
11. Right-Click the App-DSwitch, selecting Distributed Port Group -> New Distributed Port Group… for any additional application networks to be created, setting the appropriate VLAN for each new Distributed Port Group.

Add the VMware ESXi Hosts Using the VMware vSphere Web Client

To add the VMware ESXi Hosts using the VMware vSphere Web Client, follow these steps:

1. From the Hosts and Clusters tab, right-click the new or existing Datacenter within the Navigation window and select **New Cluster…** from the drop-down list.

2. Enter a name for the new cluster, select the DRS and HA checkmark boxes, leaving all other options with defaults.

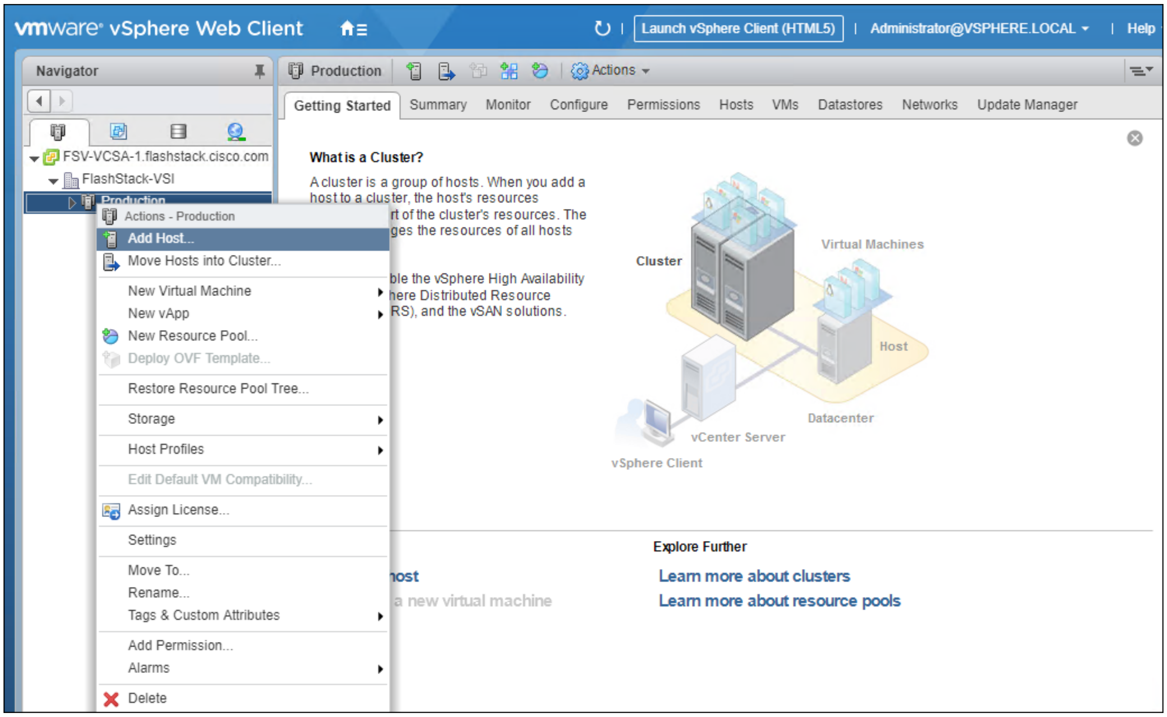


New Cluster

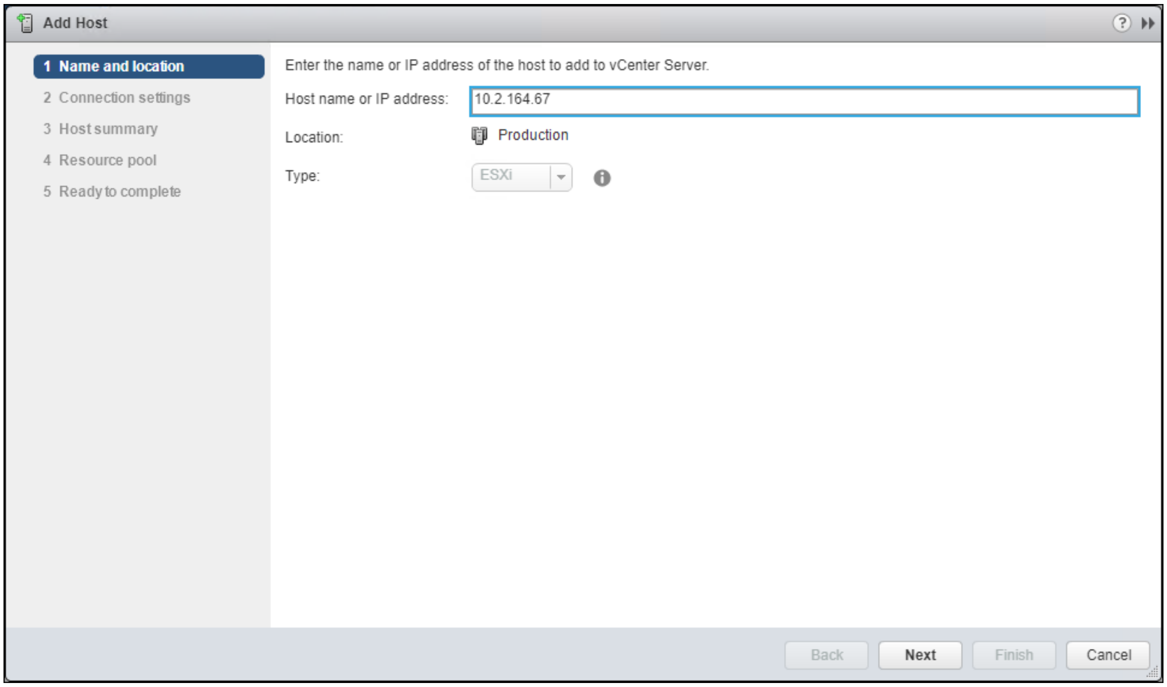
Name	Production
Location	FlashStack-VSI
DRS	☑ Turn ON
Automation Level	Fully automated
Migration Threshold	Conservative — Aggressive
vSphere HA	☑ Turn ON
Host Monitoring	☑ Enable host monitoring
Admission Control	☑ Enable admission control
VM Monitoring	
VM Monitoring Status	Disabled Overrides for individual VMs can be set from the VM Overrides page from Manage Settings area.
Monitoring Sensitivity	Low — High
EVC	Disable
vSAN	□ Turn ON

3. Click OK to create the cluster.

4. Right-click the newly created cluster and select the Add Host… drop-down list.


vmware vSphere Web Client
Launch vSphere Client (HTML5)
Administrator@VSPHERE.LOCAL
Help
Navigator
FSV-VCSA-1.flashstack.cisco.com
FlashStack-VSI
Production
Actions - Production
Add Host...
Move Hosts into Cluster...
New Virtual Machine
New vApp
New Resource Pool...
Deploy OVF Template...
Restore Resource Pool Tree...
Storage
Host Profiles
Edit Default VM Compatibility...
Assign License...
Settings
Move To...
Rename...
Tags & Custom Attributes
Add Permission...
Alarms
Delete
Production
Actions
Getting Started
Summary
Monitor
Configure
Permissions
Hosts
VMs
Datastores
Networks
Update Manager
What is a Cluster?
A cluster is a group of hosts. When you add a host to a cluster, the host's resources
rt of the cluster's resources. The
ges the resources of all hosts
ble the vSphere High Availability
here Distributed Resource
RS), and the vSAN solutions.
Cluster
Virtual Machines
Host
Datacenter
vCenter Server
vSphere Client
Explore Further
host
a new virtual machine
Learn more about clusters
Learn more about resource pools

5. Enter the IP or FQDN of the first ESXi host and click Next.



Enter the name or IP address of the host to add to vCenter Server.

Host name or IP address: 10.2.164.67

Location: Production

Type: ESXi

6. Enter root for the User Name, provide the password set during initial setup and click Next.

7. Click Yes in the Security Alert pop-up to confirm the host’s certificate.

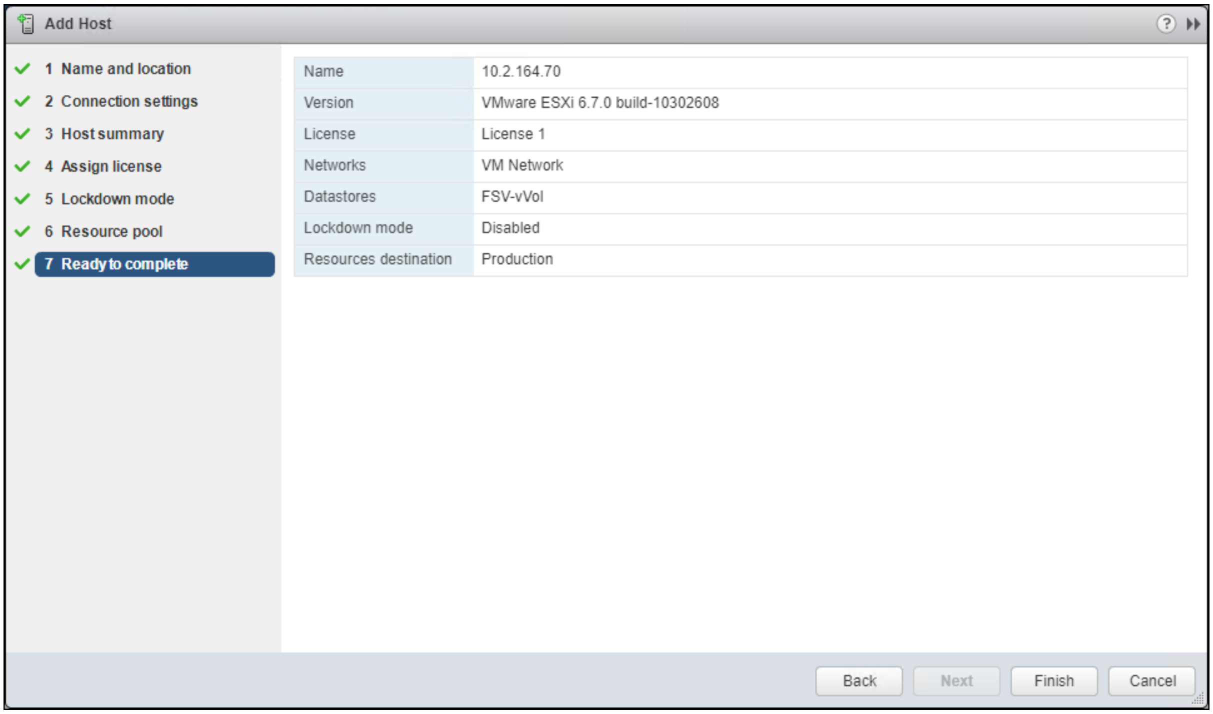
8. Click Next past the Host summary dialogue.

9. Provide a license by clicking the green + icon under the License title, select an existing license, or skip past the Assign license dialogue by clicking Next.

10. Leave lockdown mode Disabled within the Lockdown mode dialogue window and click Next.

11. Skip past the Resource pool dialogue by clicking Next.

12. Confirm the Summary dialogue and add the ESXi host to the cluster by clicking Next.



Add Host

- ✓ 1 Name and location
- ✓ 2 Connection settings
- ✓ 3 Host summary
- ✓ 4 Assign license
- ✓ 5 Lockdown mode
- ✓ 6 Resource pool
- ✓ 7 Ready to complete

Name	10.2.164.70
Version	VMware ESXi 6.7.0 build-10302608
License	License 1
Networks	VM Network
Datastores	FSV-vVol
Lockdown mode	Disabled
Resources destination	Production

13. Repeat steps 4-12 for each ESXi host to be added to the cluster.

Configure ESXi Hosts in the Cluster

With the hosts added and the base vCenter configuration complete, some additional configurations will be needed for each ESXi host provisioned for the FlashStack.

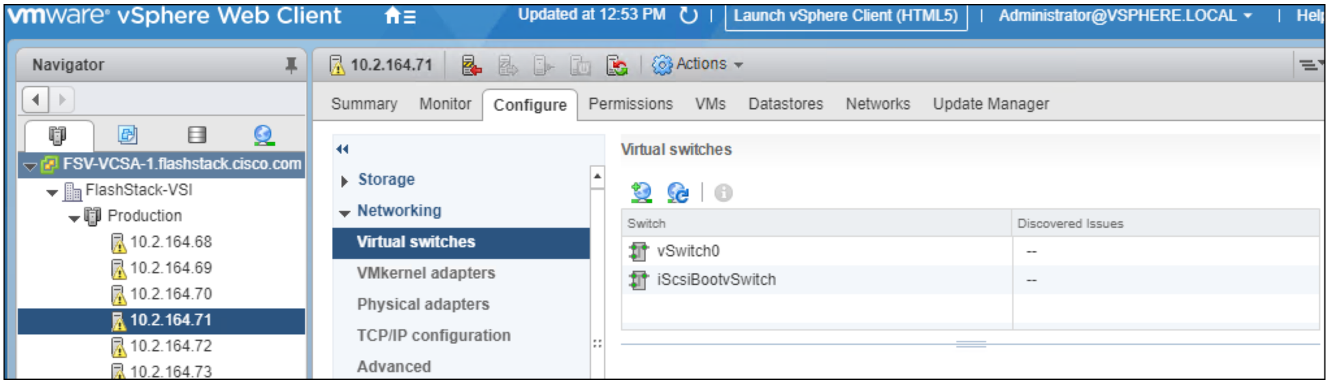
Configure iSCSI Adapters

The base installation will set up one vmkernel adapter for the iSCSI boot, with a generated vSwitch named iScsiBootvSwitch. vSwitch changes will be needed, as well as the creation of a second vmkernel adapter used for the B side iSCSI boot.

To make the vSwitch changes and create the vmkernel adapter, follow these steps for each host:

Adjust iSCSI A vSwitch MTU

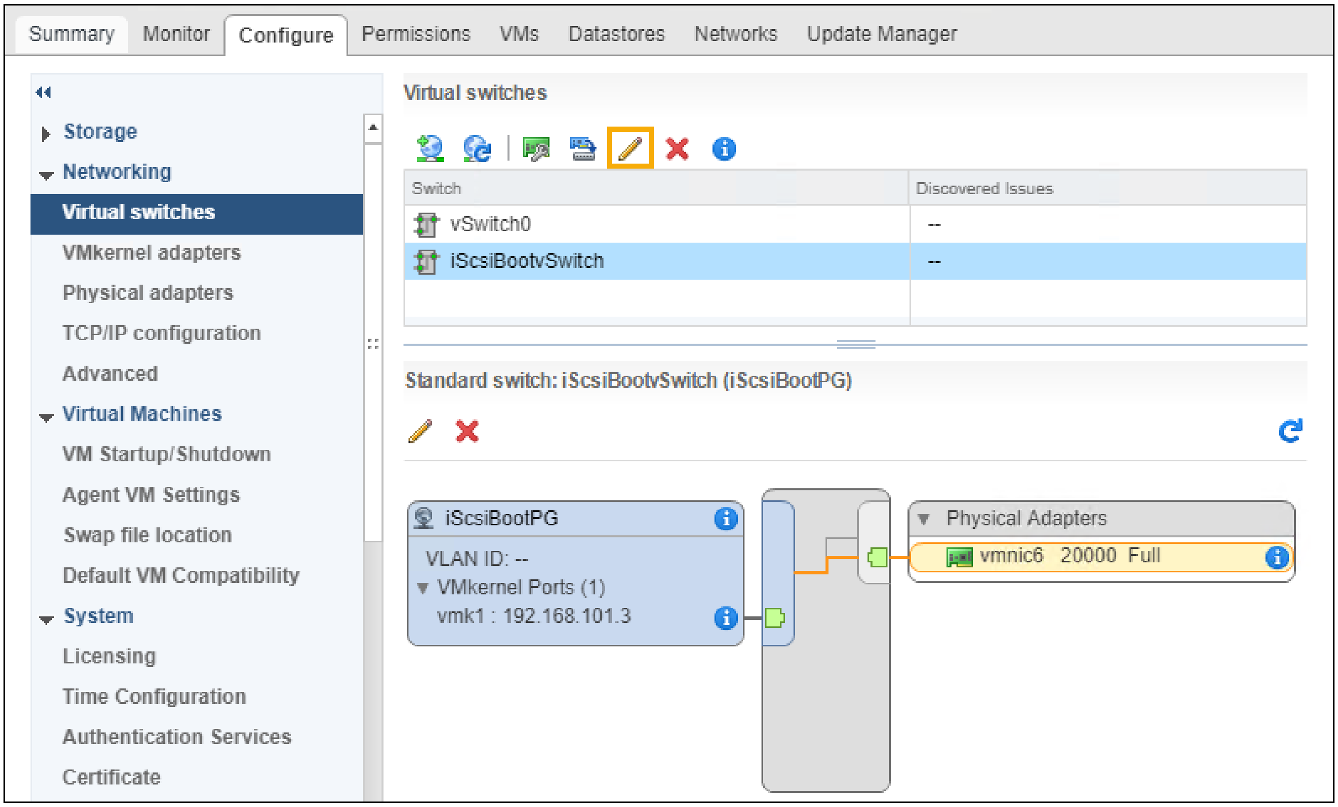
1. From the vSphere Web Client, select the installed iSCSI host, click the Configure tab, and select the Virtual switches section from the Networking section.



Virtual switches

Switch	Discovered Issues
vSwitch0	--
iScsiBootvSwitch	--

2. Select the iScsiBootvSwitch and click the pencil icon to open Edit settings for the vSwitch.



Virtual switches

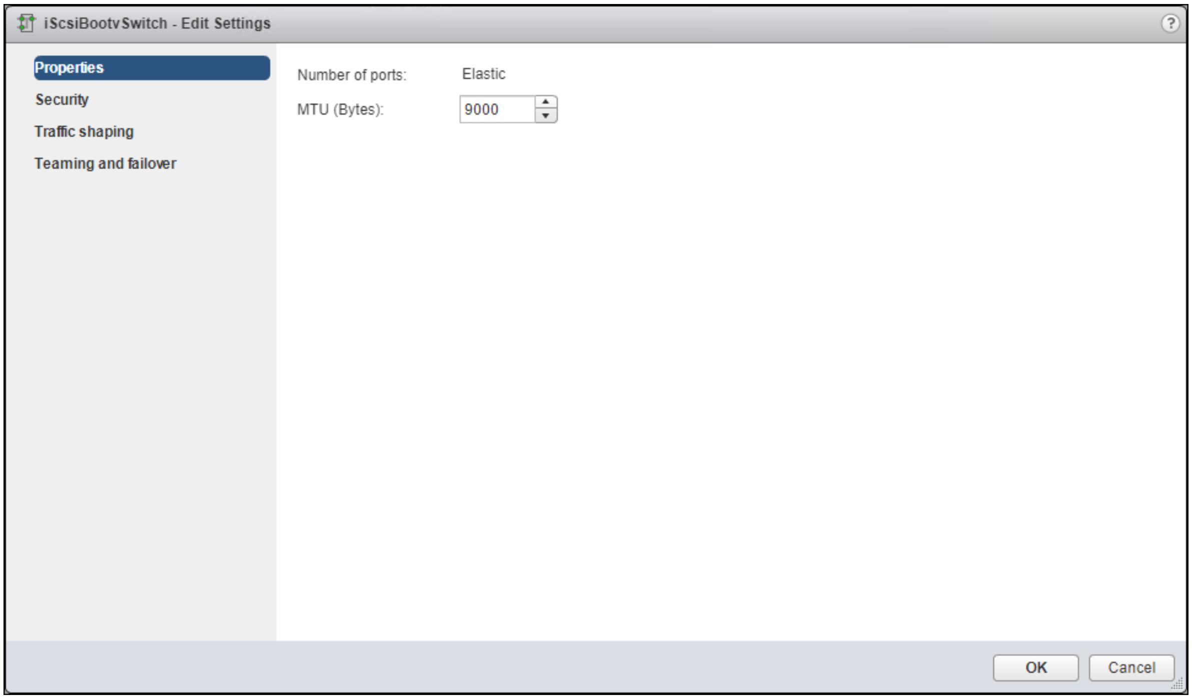
Switch	Discovered Issues
vSwitch0	--
iScsiBootvSwitch	--

Standard switch: iScsiBootvSwitch (iScsiBootPG)

iScsiBootPG
VLAN ID: --
VMkernel Ports (1)
vmk1 : 192.168.101.3

Physical Adapters
vmnic6 20000 Full

3. Within the Properties section, change the MTU from 1500 to 9000 and click OK to save the changes.

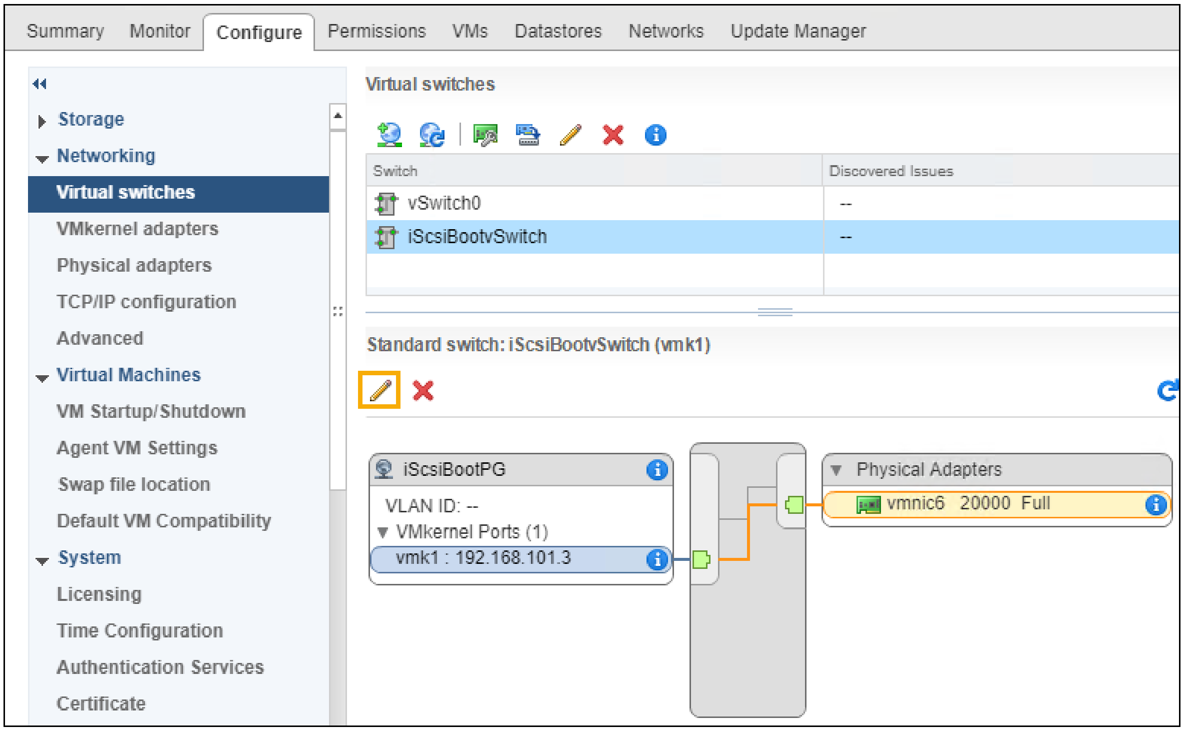


iScsiBootvSwitch - Edit Settings

Number of ports: Elastic

MTU (Bytes): 9000

4. Click the vmk1 entry within the iScsiBootPG and select the pencil icon to edit the settings of the vmkernel adapter.



Switch	Discovered Issues
vSwitch0	--
iScsiBootvSwitch	--

Standard switch: iScsiBootvSwitch (vmk1)

iScsiBootPG

VLAN ID: --

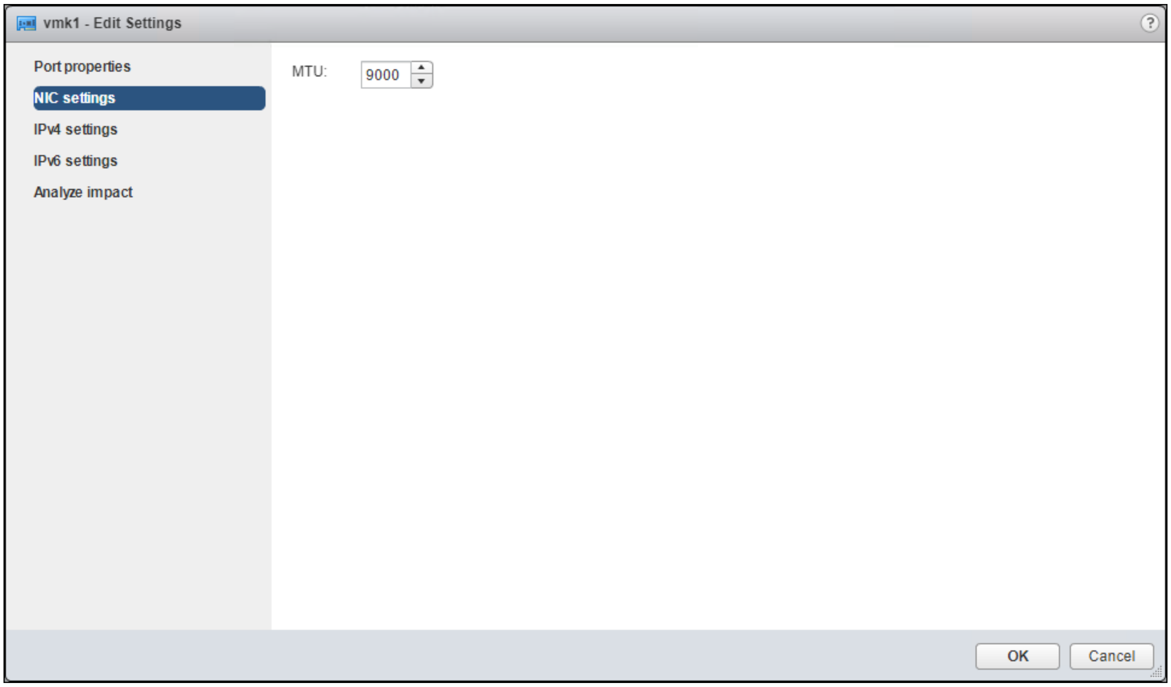
VMkernel Ports (1)

vmk1 : 192.168.101.3

Physical Adapters

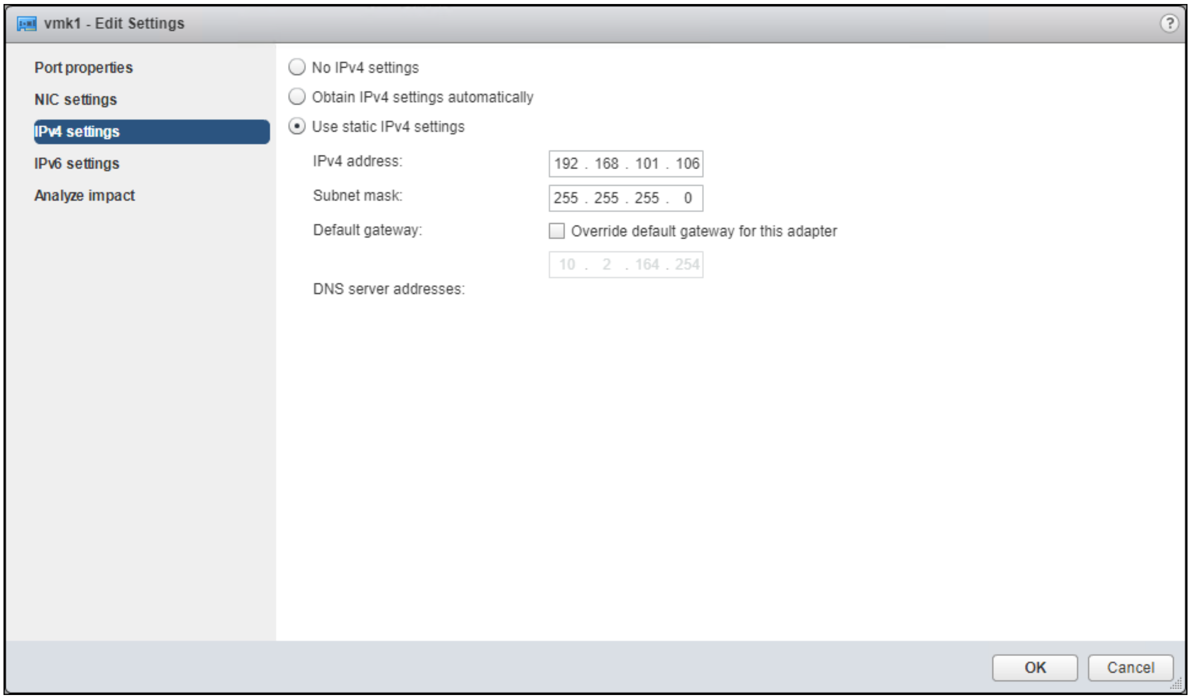
vmnic6 20000 Full

5. Select NIC settings side of the Edit Settings window and adjust the MTU from 1500 to 9000.



MTU: 9000

6. Click the IPv4 settings for vmk1 and change the IPv4 settings from the Cisco UCS Manager iSCSI-A-Pool assigned IP to one that is not in the IP block.



○ No IPv4 settings

○ Obtain IPv4 settings automatically

● Use static IPv4 settings

IPv4 address: 192 . 168 . 101 . 106

Subnet mask: 255 . 255 . 255 . 0

Default gateway: □ Override default gateway for this adapter

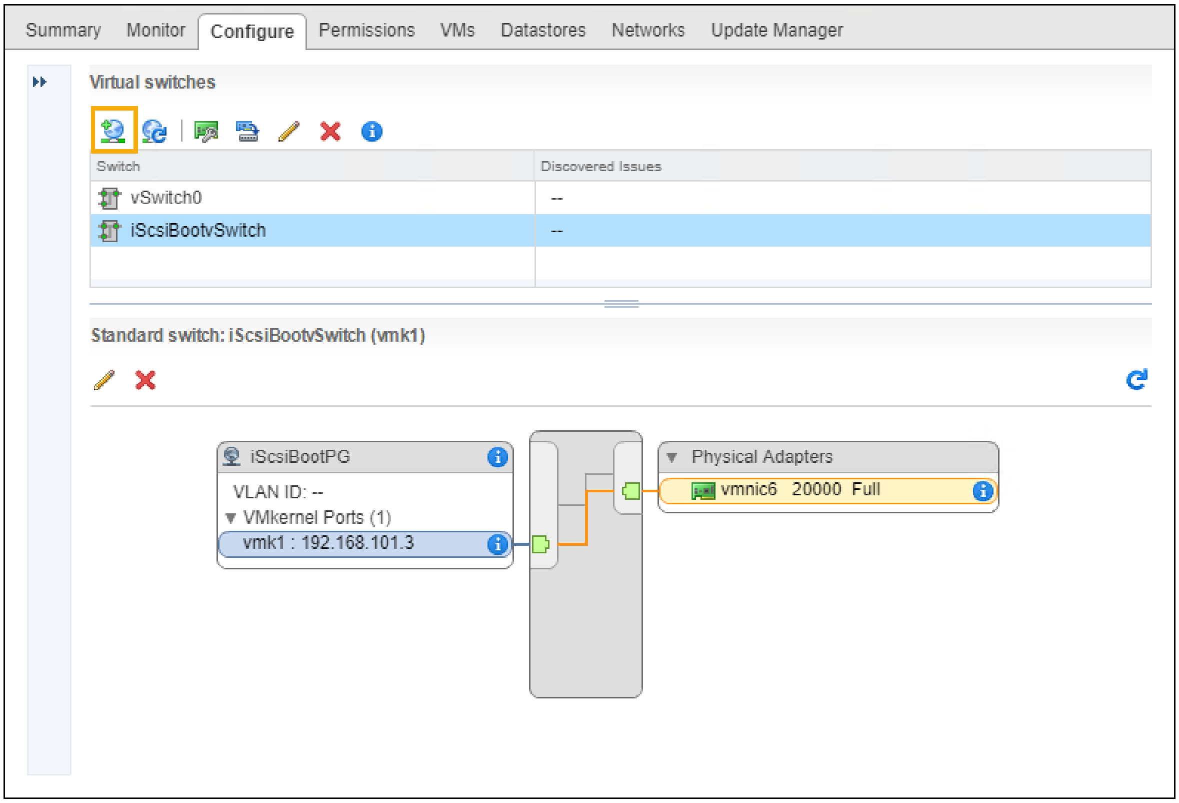
10 . 2 . 164 . 254

DNS server addresses:

7. Click OK to apply the changes to the vmkernel adapter.

Create iSCSI B vSwitch and vmkernel Adapter

1. Click the Add host networking icon under Virtual switches.



Virtual switches

Switch	Discovered Issues
vSwitch0	--
iScsiBootvSwitch	--

Standard switch: iScsiBootvSwitch (vmk1)

iScsiBootPG

VLAN ID: --

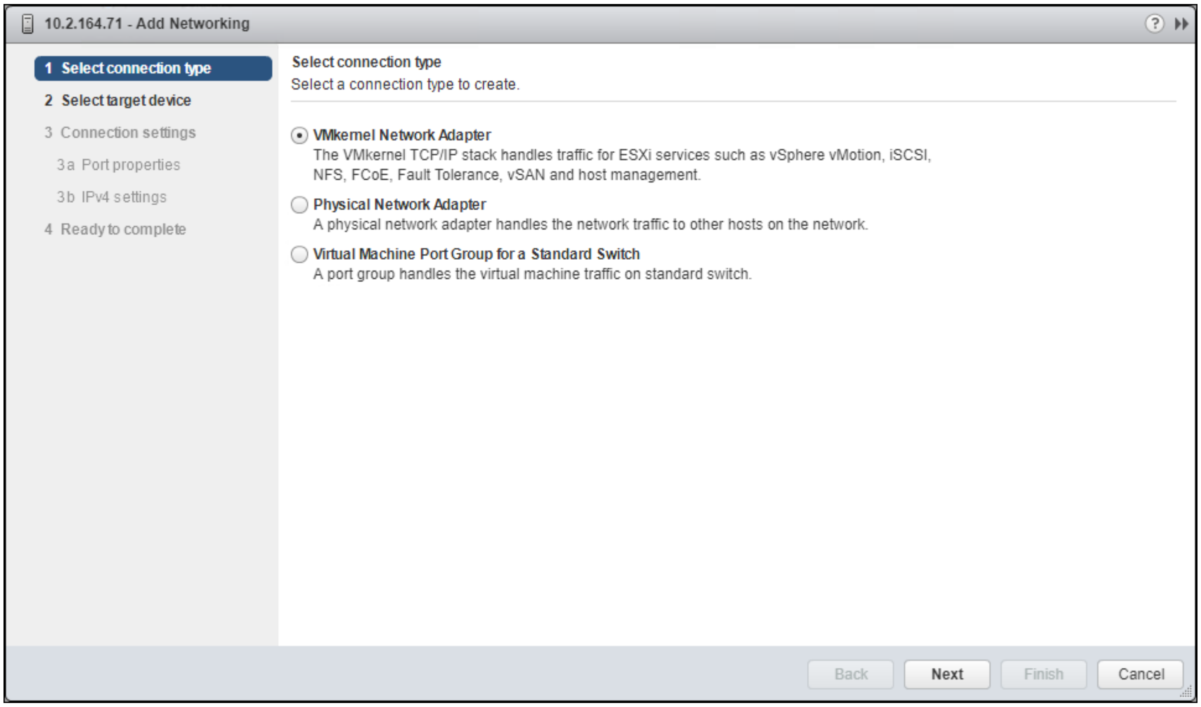
▼ VMkernel Ports (1)

vmk1 : 192.168.101.3

▼ Physical Adapters

vmnic6 20000 Full

2. Leave VMkernel Network Adapter selected and click Next.


10.2.164.71 - Add Networking

1 Select connection type
2 Select target device
3 Connection settings
3a Port properties
3b IPv4 settings
4 Ready to complete

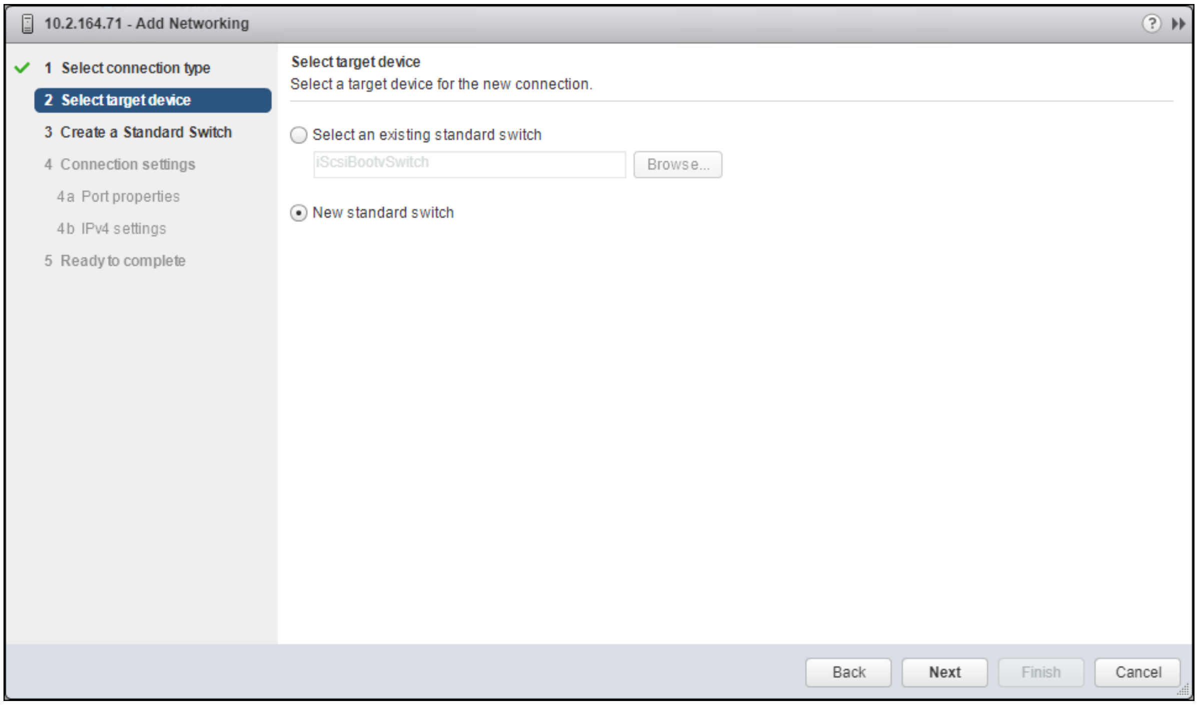
Select connection type
Select a connection type to create.

● VMkernel Network Adapter
The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN and host management.

○ Physical Network Adapter
A physical network adapter handles the network traffic to other hosts on the network.

○ Virtual Machine Port Group for a Standard Switch
A port group handles the virtual machine traffic on standard switch.

3. Change the Select target device option to New standard switch and click Next.



10.2.164.71 - Add Networking

Select target device

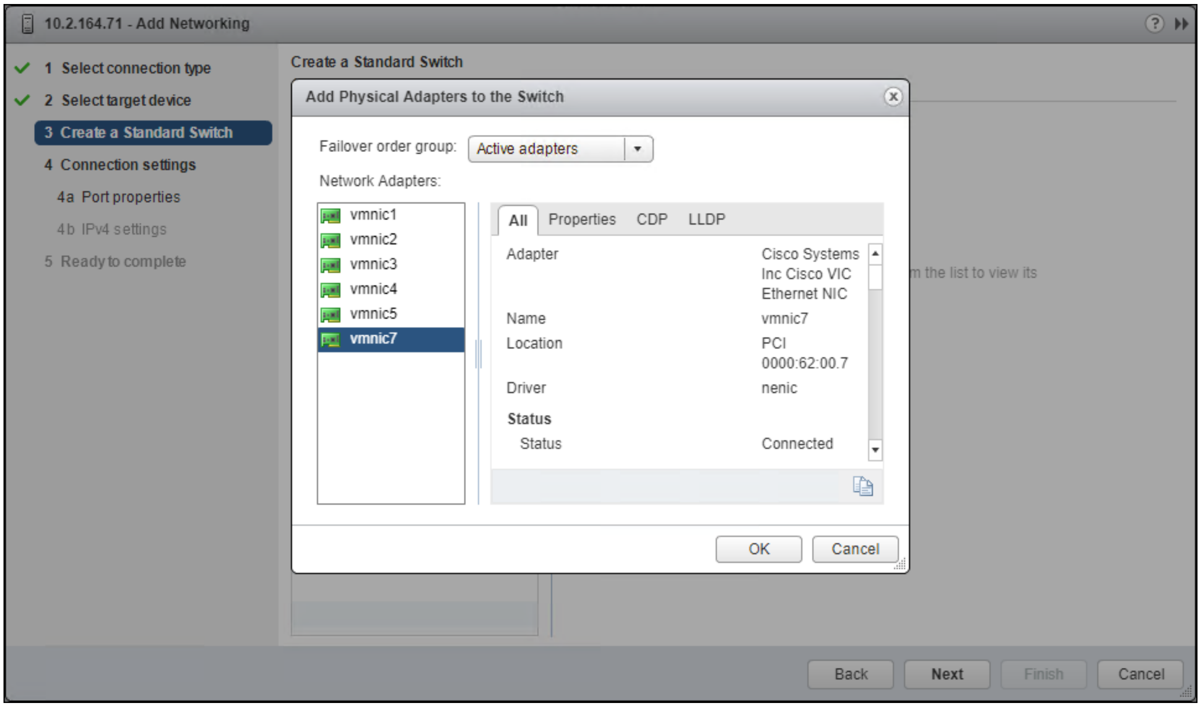
Select a target device for the new connection.

○ Select an existing standard switch

iScsiBootvSwitch

● New standard switch

4. Click the green plus icon under Assigned adapters and select vmnic7 from the listed adapters in the resulting window.



10.2.164.71 - Add Networking

Create a Standard Switch

Add Physical Adapters to the Switch

Failover order group: Active adapters

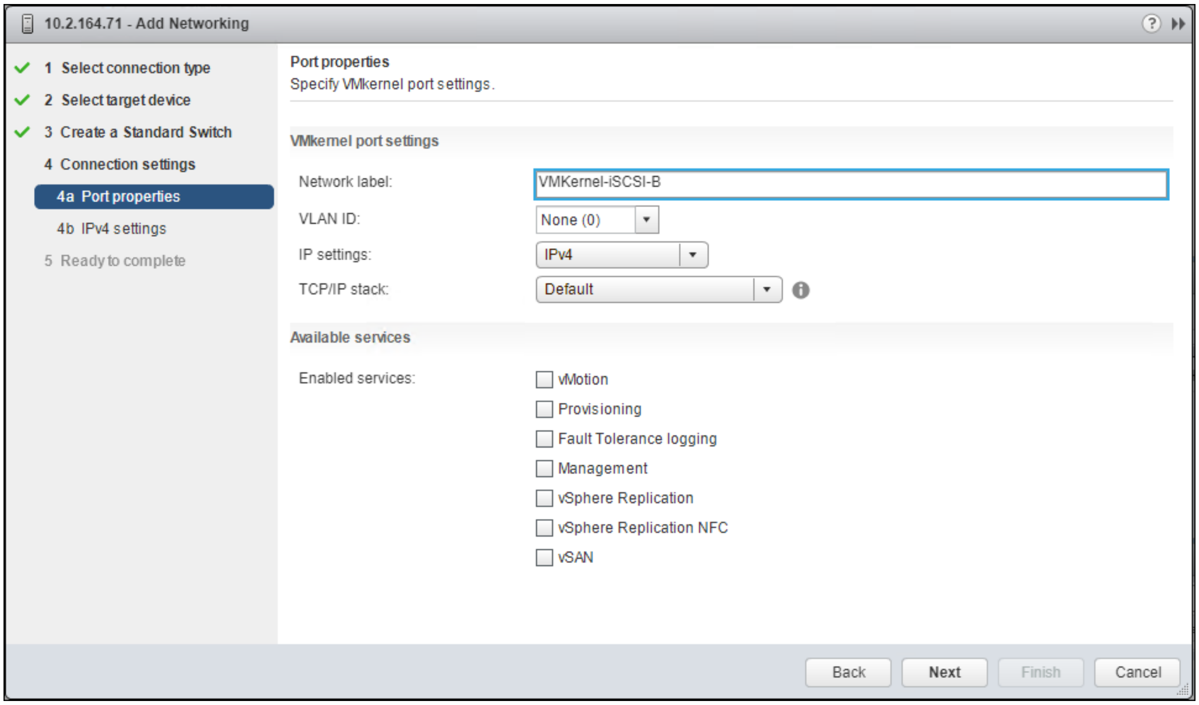
Network Adapters:

- vmnic1
- vmnic2
- vmnic3
- vmnic4
- vmnic5
- vmnic7

Adapter	Cisco Systems Inc Cisco VIC Ethernet NIC
Name	vmnic7
Location	PCI 0000:62:00.7
Driver	nenic
Status	
Status	Connected

5. Click OK to add the vmnic to the vSwitch and click Next.

6. (Optional) Enter a relevant name for the Network label.



Port properties
Specify VMkernel port settings.

VMkernel port settings

Network label: VMKernel-iSCSI-B

VLAN ID: None (0)

IP settings: IPv4

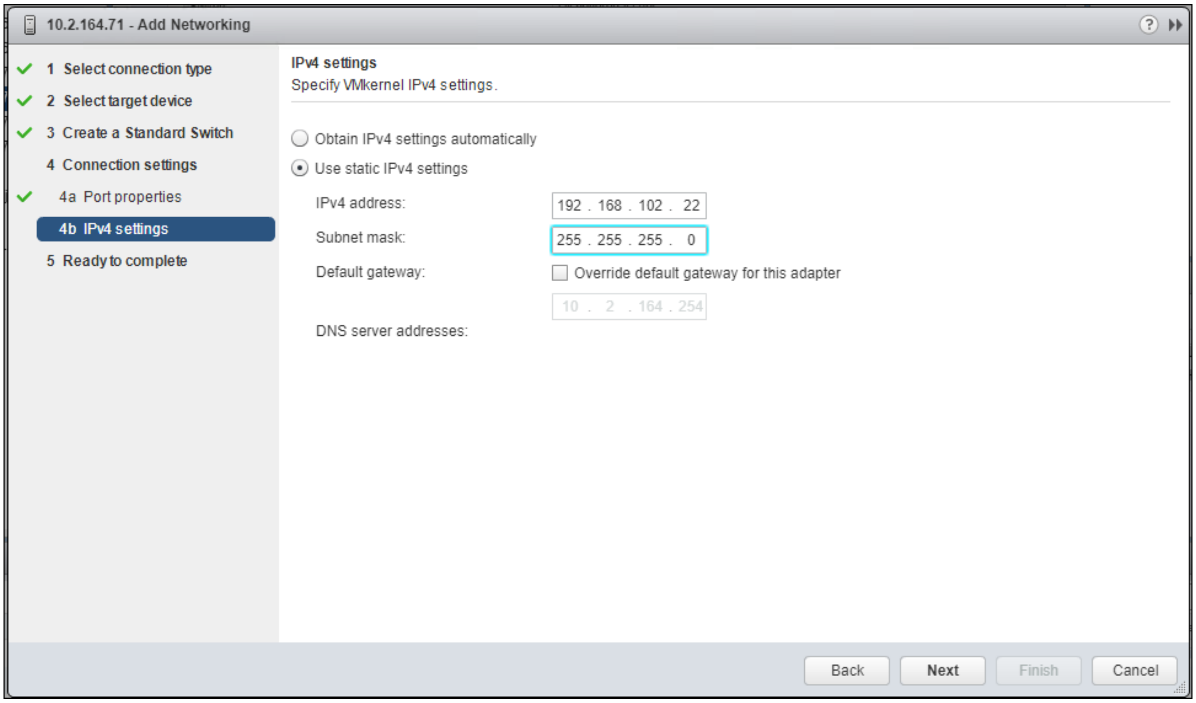
TCP/IP stack: Default

Available services

Enabled services:
□ vMotion
□ Provisioning
□ Fault Tolerance logging
□ Management
□ vSphere Replication
□ vSphere Replication NFC
□ vSAN

7. Click Next.

8. Change the option for IPv4 settings to Use static IPv4 settings and enter valid IP and subnet mask information that is outside of the UCS iSCSI Pool B.



IPv4 settings
Specify VMkernel IPv4 settings.

○ Obtain IPv4 settings automatically

● Use static IPv4 settings

IPv4 address: 192 . 168 . 102 . 22

Subnet mask: 255 . 255 . 255 . 0

Default gateway: □ Override default gateway for this adapter

10 . 2 . 164 . 254

DNS server addresses:

9. Click Next and click Finish in the resulting Summary window.

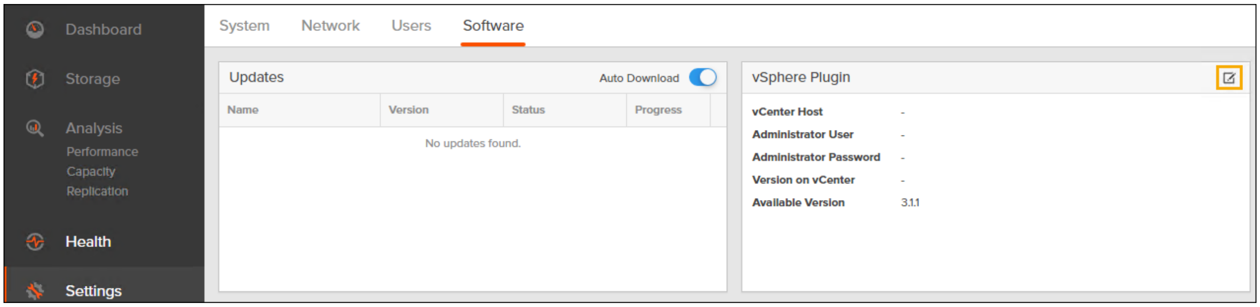
Pure Storage vSphere Web Client Plugin

The Pure Storage vSphere Web Client Plugin will be accessible through the vSphere Web Client after registration through the Pure Storage Web Portal.

To access the Pure Storage vSphere Web Client Plugin, follow these steps:

1. Go to Settings > Software.

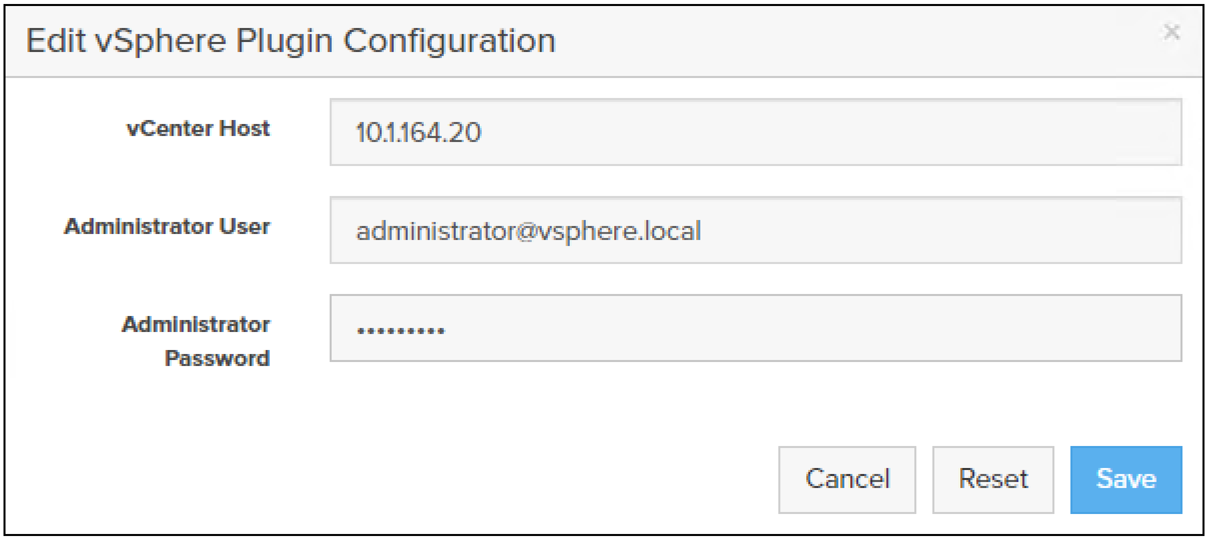
2. Select the edit icon in the vSphere Plugin panel.



Name	Version	Status	Progress
No updates found.			

vCenter Host	-
Administrator User	-
Administrator Password	-
Version on vCenter	-
Available Version	3.1.1

3. Enter the vCenter information in the pop-up window and click Save.

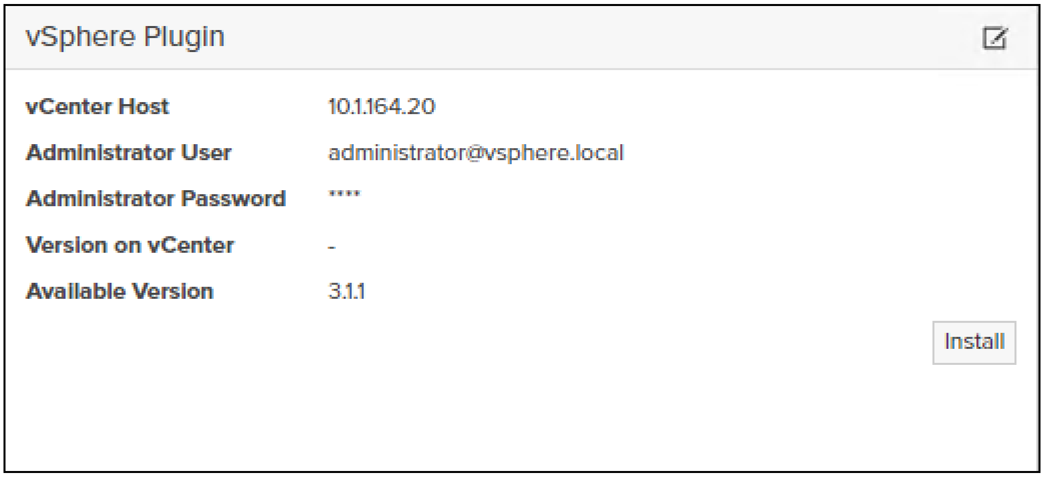


vCenter Host: 10.1.164.20

Administrator User: administrator@vsphere.local

Administrator Password: •••••••••

4. After the discovery completes. Click Install.

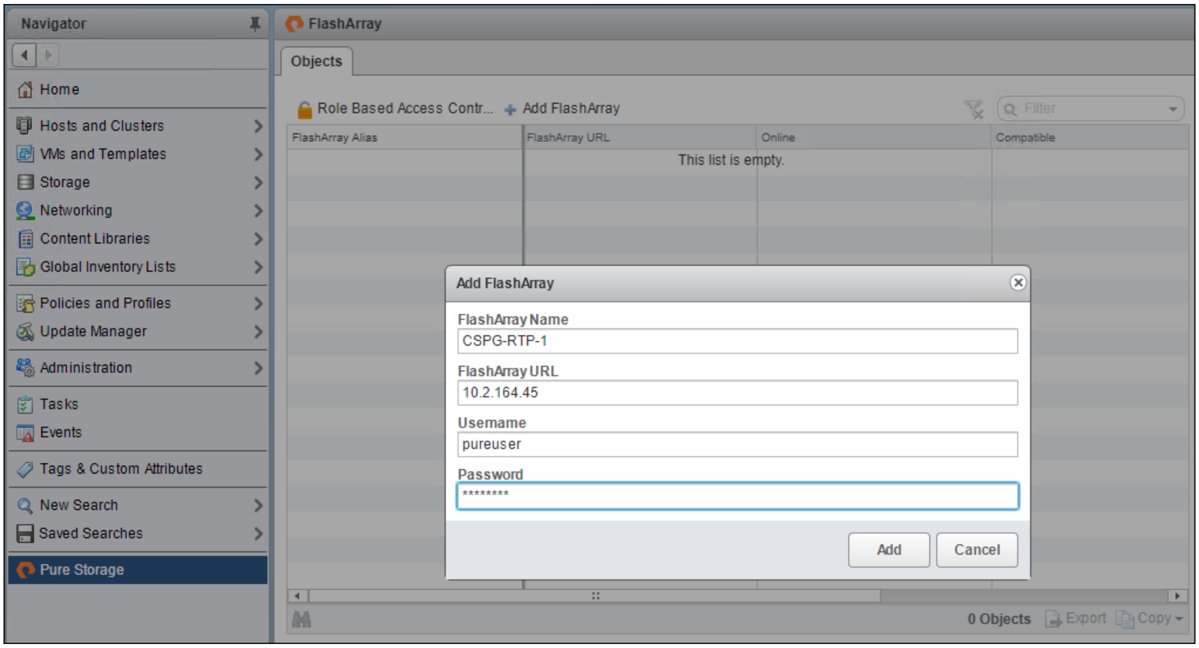


vSphere Plugin

vCenter Host	10.1.164.20
Administrator User	administrator@vsphere.local
Administrator Password	****
Version on vCenter	-
Available Version	3.1.1

Install

5. In vCenter, register the FlashArray to the plugin by navigating to Home and selecting the Pure Storage Plugin. Then select Add FlashArray.



Add FlashArray

FlashArray Name: CSPG-RTP-1

FlashArray URL: 10.2.164.45

Username: pureuser

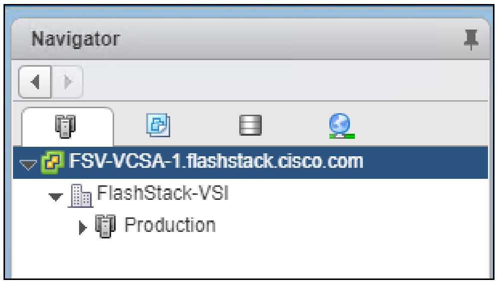
Password: ********

Add | Cancel

6. Add the FlashArray as a Storage Provider by clicking the ‘Register Storage Provider’ ( ) icon and providing the login information for the FlashArray.

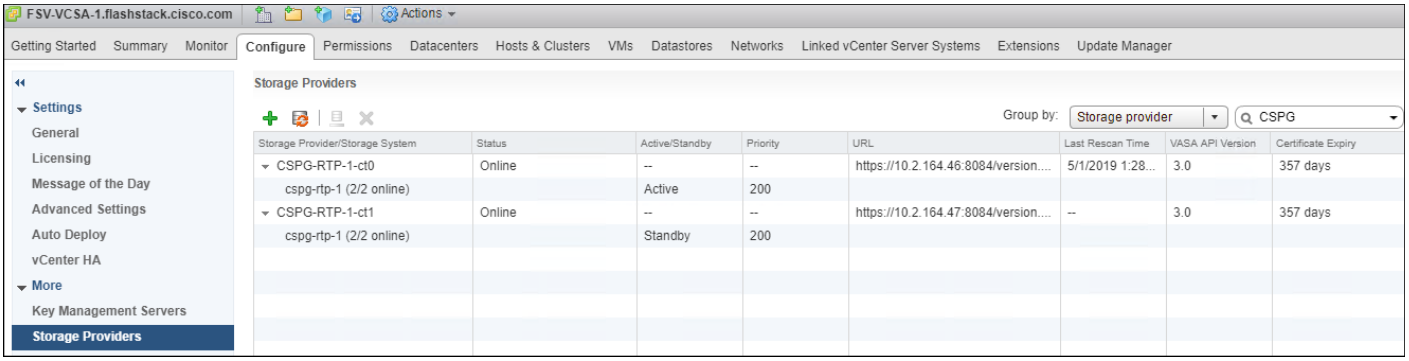
7. Verify that the FlashArray is registered correctly as a storage provider.

8. Select Host and Cluster, Select the vCenter Server.



9. Select Configure > Storage Providers.

10. Filter on the name.



Storage Providers

Group by: Storage provider ▾ CSPG

Storage Provider/Storage System	Status	Active/Standby	Priority	URL	Last Rescan Time	VASA API Version	Certificate Expiry
CSPG-RTP-1-ct0	Online	--	--	https://10.2.164.46:8084/version....	5/1/2019 1:28...	3.0	357 days
cspg-rtp-1 (2/2 online)		Active	200				
CSPG-RTP-1-ct1	Online	--	--	https://10.2.164.47:8084/version....	--	3.0	357 days
cspg-rtp-1 (2/2 online)		Standby	200				

11. Verify that one controller is Active and the other is Standby.

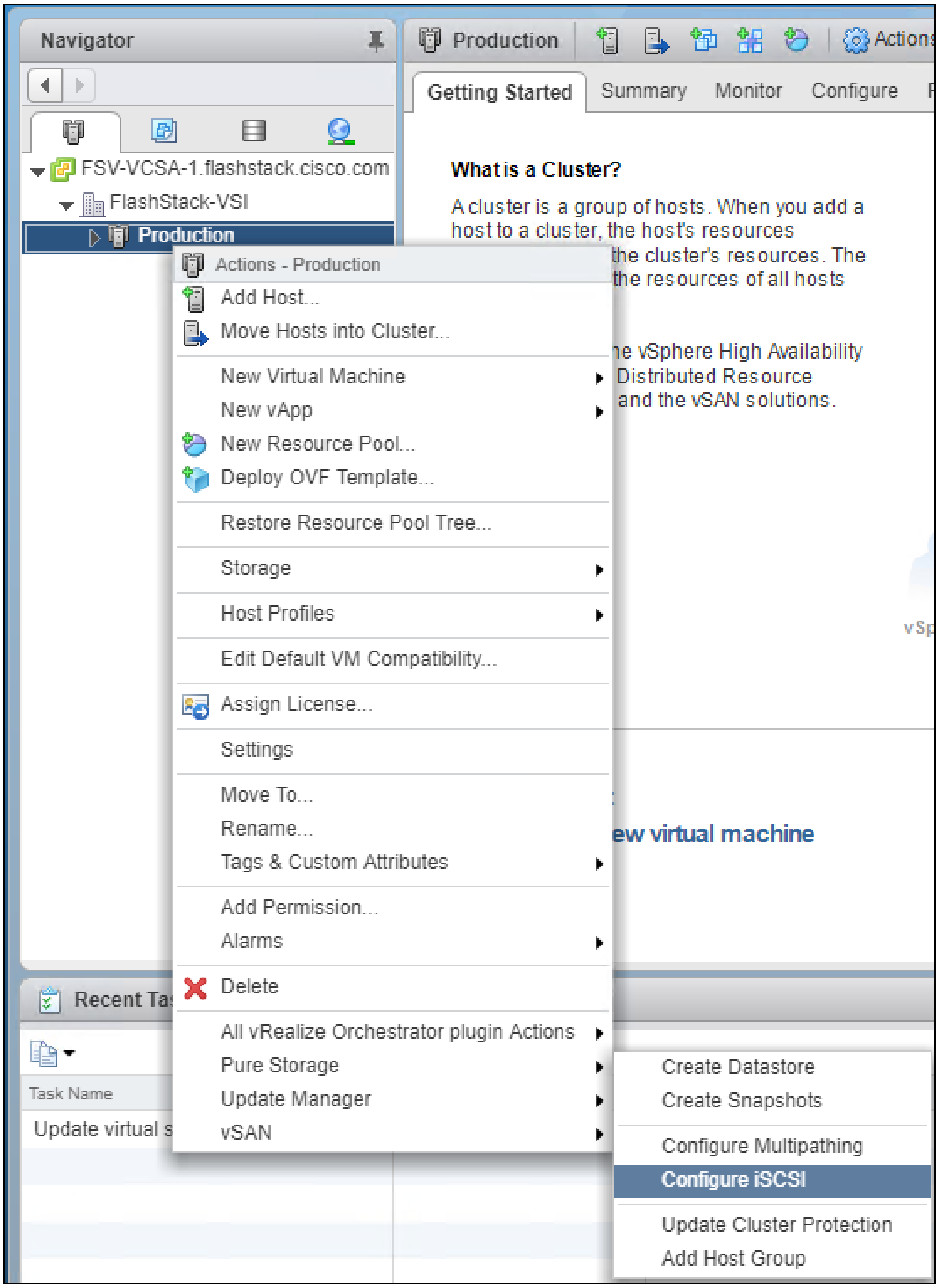
Setup iSCSI

The Pure Storage plugin provides for automating the iSCSI multipathing at a cluster level.

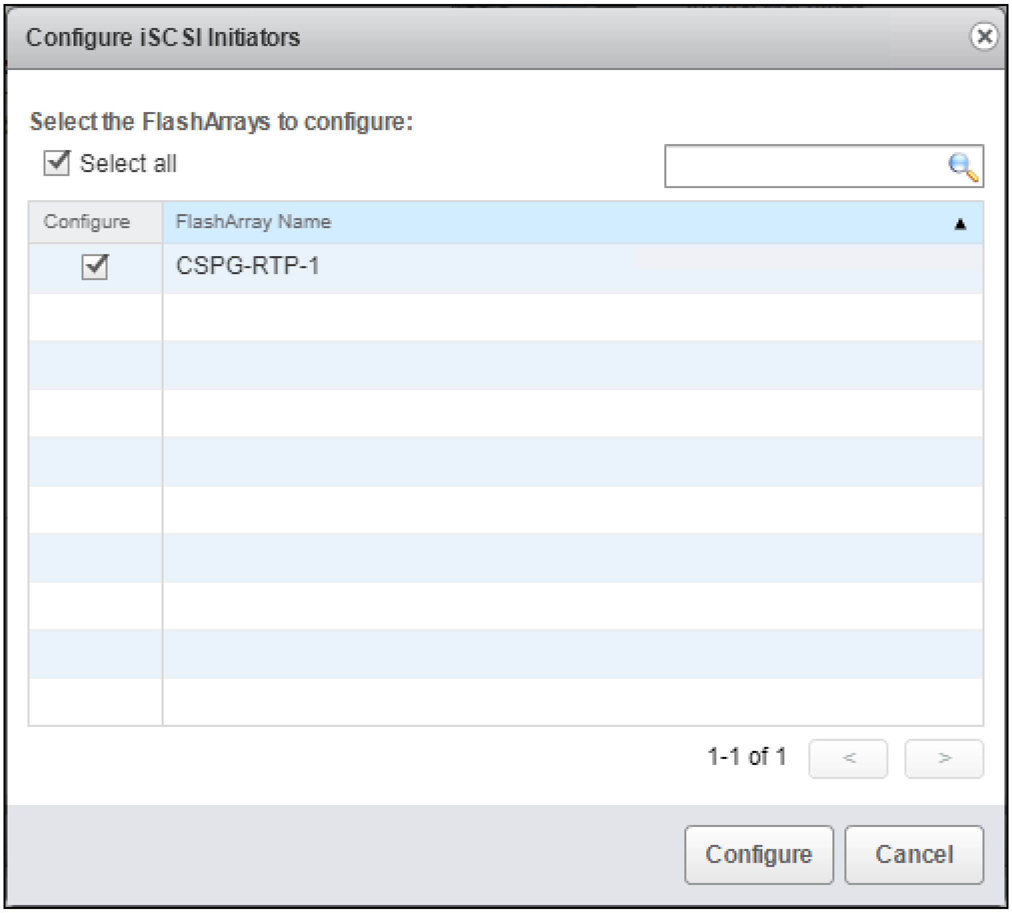
To configure Multipathing settings, follow these steps:

1. Navigate to the Hosts and Clusters view in the vCenter web client.

2. Right-click the FlashStack cluster and select Pure Storage > Configure iSCSI.



3. Select the FlashArray from the list and click Configure.


Configure iSCSI Initiators
Select the FlashArrays to configure:
☑ Select all
1-1 of 1
<
>
Configure
Cancel

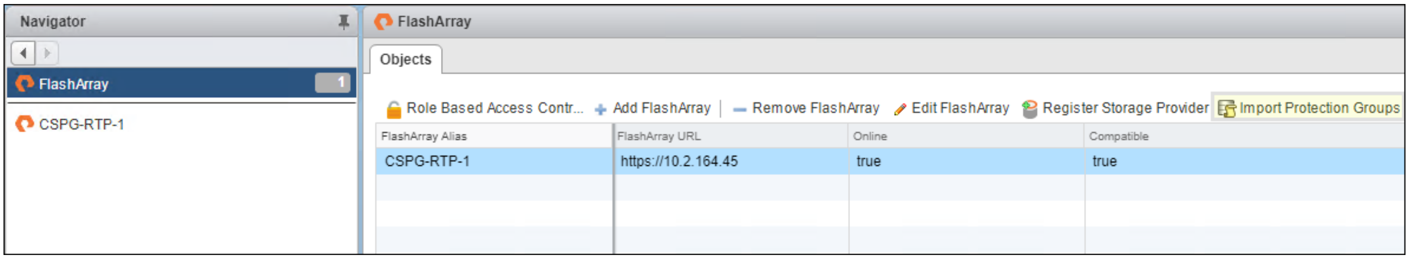
Configure	FlashArray Name
☑	CSPG-RTP-1

Import Protection Group as VM Storage Policy

To import the FlashArray Protection Group settings as VM Storage Policies, follow these steps:

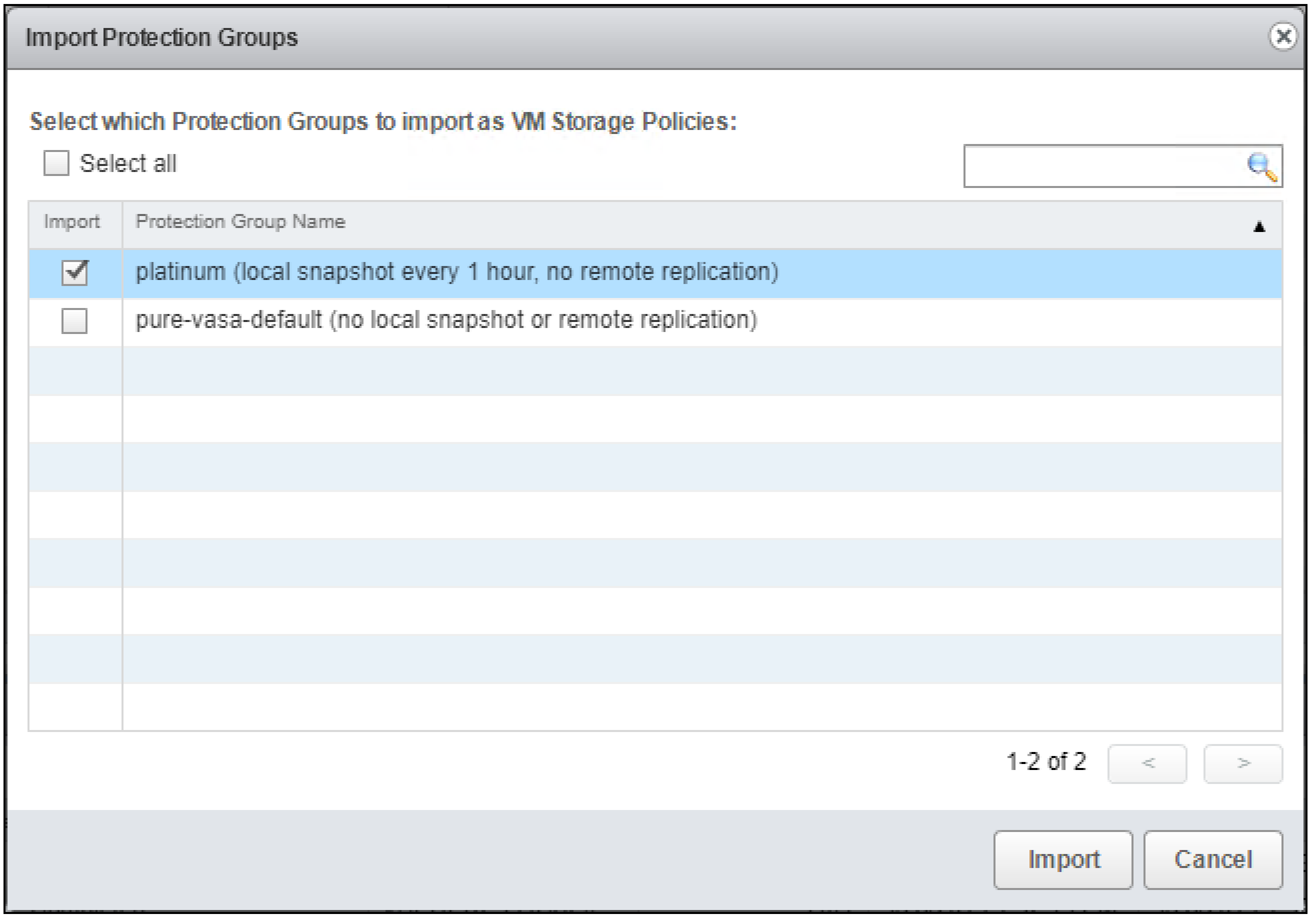
1. From the vSphere Web Client home screen Select the Pure Storage Plugin.

2. Select Import Protection Groups.



FlashArray Alias	FlashArray URL	Online	Compatible
CSPG-RTP-1	https://10.2.164.45	true	true

3. Select the local snapshot Protection Group that was created during the "Configure Storage Policy Based Management" step and click Import.



Select which Protection Groups to import as VM Storage Policies:

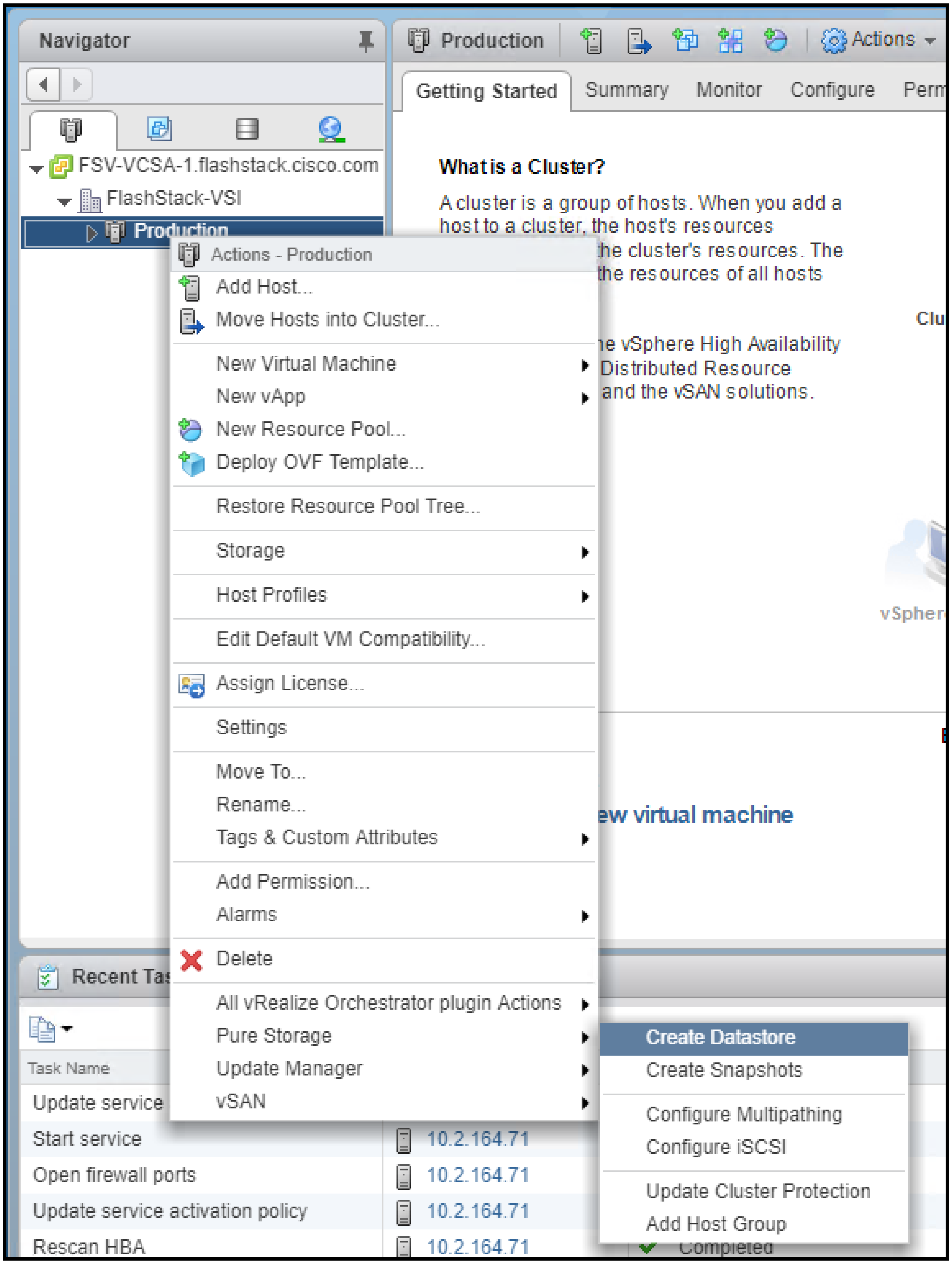
Import	Protection Group Name
☑	platinum (local snapshot every 1 hour, no remote replication)
□	pure-vasa-default (no local snapshot or remote replication)

Add Datastores

To add VMFS to place swap and driver files and a VVol datastore to place virtual machines on the FlashArray//X R2, follow these steps:

A dedicated swapfile location will not provide a performance increase over the existing all flash datastores created from the FlashArray//X but can be useful to have these files in a separate location to have them excluded from snapshots and backups.

1. Right-click the cluster and select **Pure Storage** -> **Create Datastore** from the drop-down list.



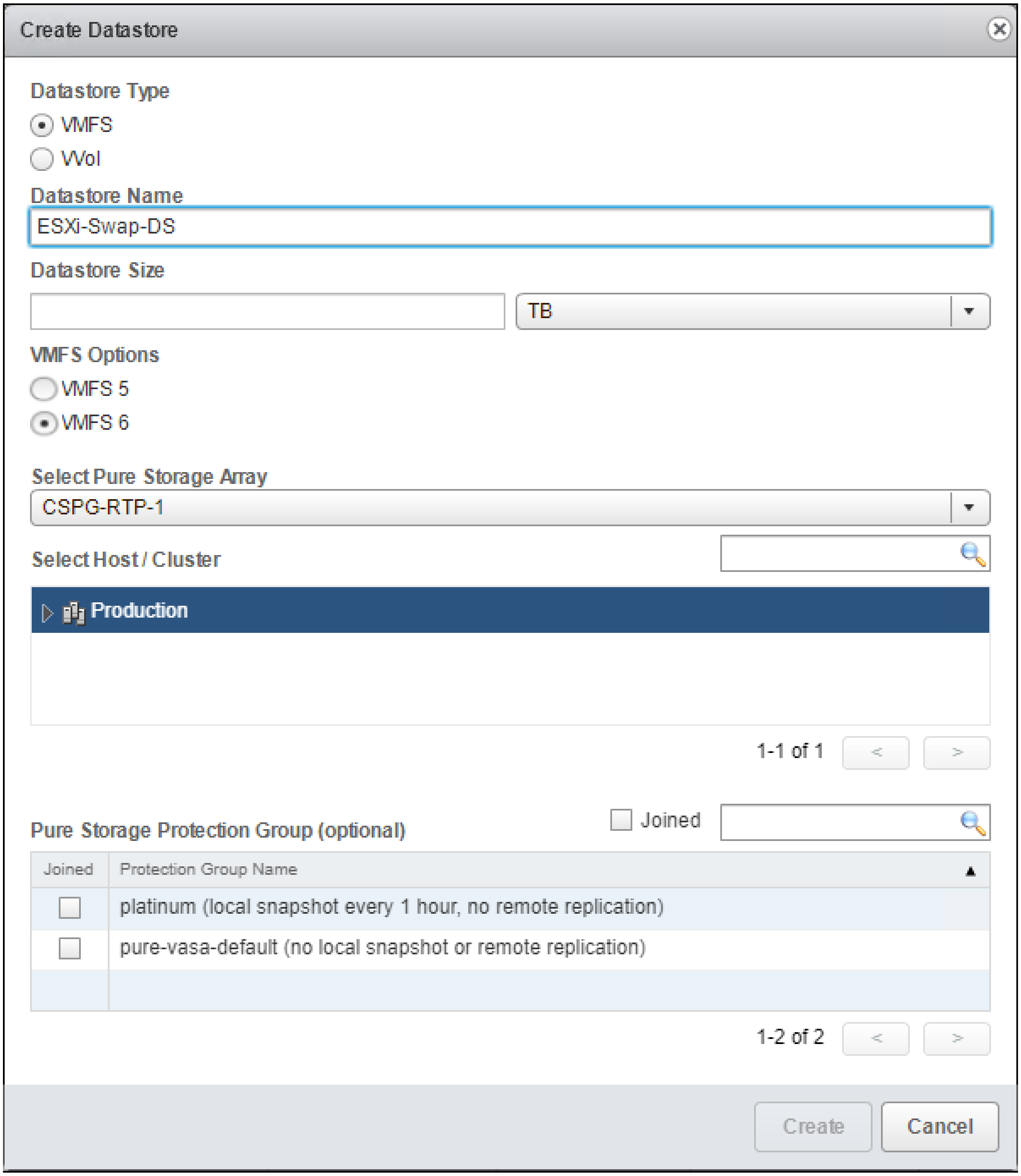
What is a Cluster?

A cluster is a group of hosts. When you add a host to a cluster, the host's resources
the cluster's resources. The
the resources of all hosts

e vSphere High Availability
Distributed Resource
and the vSAN solutions.

Task Name		
Update service		
Start service	10.2.164.71	
Open firewall ports	10.2.164.71	
Update service activation policy	10.2.164.71	
Rescan HBA	10.2.164.71	Completed

2. Select Datastore type VMFS, provide a Datastore Name, Datastore size, Cluster, Protection Group settings, and Select VMFS 6.



Create Datastore

Datastore Type

● VMFS

○ VVol

Datastore Name

ESXi-Swap-DS

Datastore Size

TB

VMFS Options

○ VMFS 5

● VMFS 6

Select Pure Storage Array

CSPG-RTP-1

Select Host / Cluster

Production

1-1 of 1

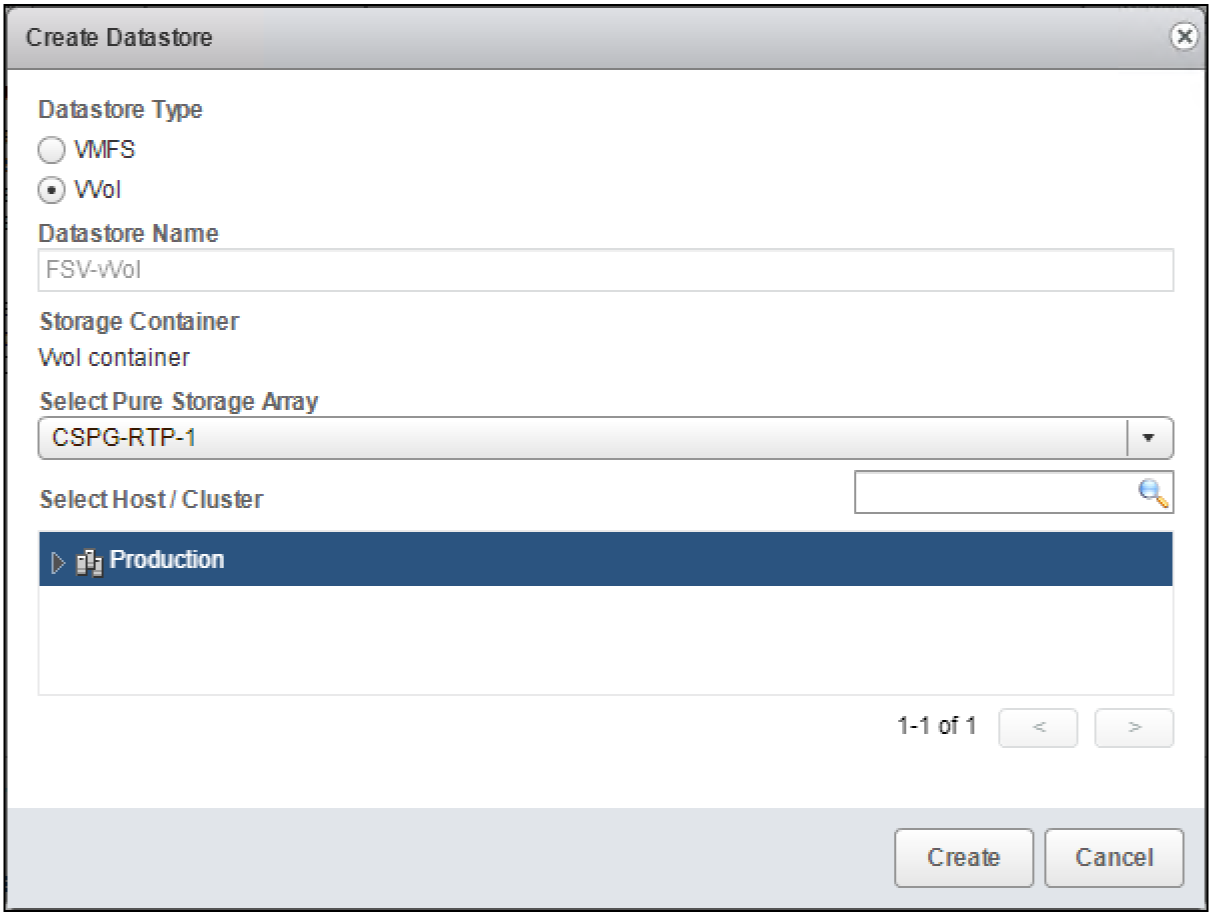
Pure Storage Protection Group (optional) □ Joined

Joined	Protection Group Name
□	platinum (local snapshot every 1 hour, no remote replication)
□	pure-vasa-default (no local snapshot or remote replication)

1-2 of 2

3. Right-click the cluster and select the **Pure Storage** -> **Create Datastore** option from the drop-down to create a second datastore.

4. Select Datastore Type VVol and click Create to finish.



Create Datastore

Datastore Type

○ VMFS

● VVol

Datastore Name

FSV-VVol

Storage Container

VVol container

Select Pure Storage Array

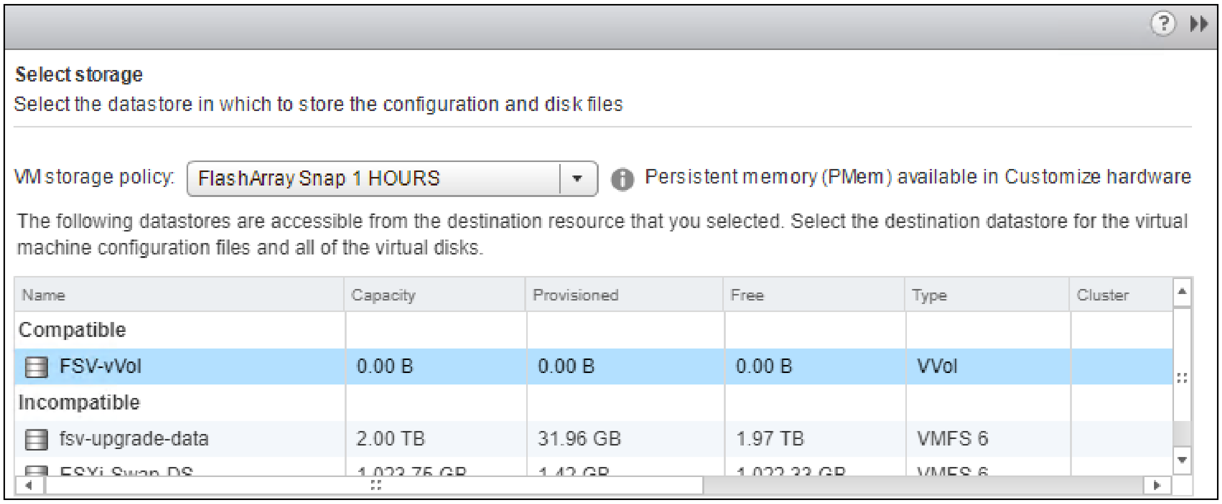
CSPG-RTP-1

Select Host / Cluster

Production

1-1 of 1

You're now able to select the VM storage policy when creating or migrating Virtual Machines.



Select storage

Select the datastore in which to store the configuration and disk files

VM storage policy: FlashArray Snap 1 HOURS

Persistent memory (PMem) available in Customize hardware

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Provisioned	Free	Type	Cluster
Compatible					
FSV-vVol	0.00 B	0.00 B	0.00 B	VVol	
Incompatible					
fsv-upgrade-data	2.00 TB	31.96 GB	1.97 TB	VMFS 6	
ESXi Swap DS	1,023.75 GB	1.42 GB	1,022.33 GB	VMFS 6	

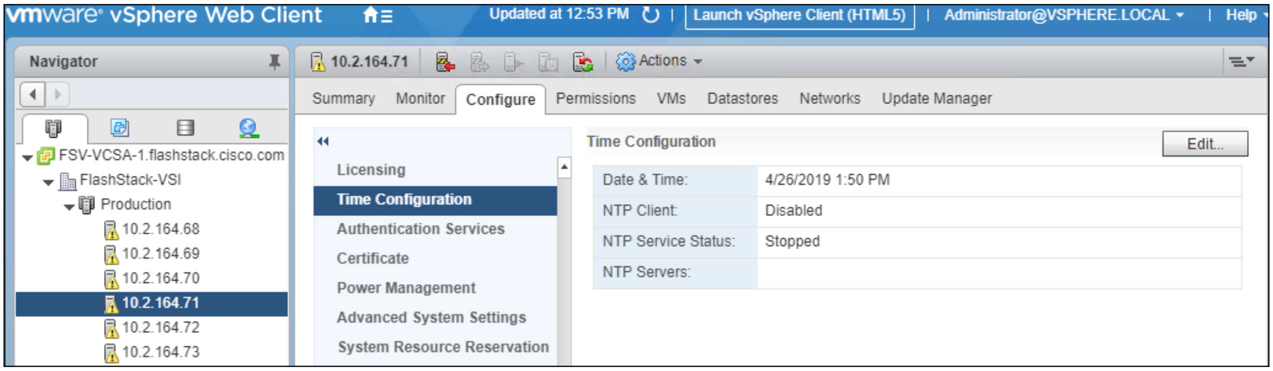
Configure ESXi Settings

A couple of base settings are needed for stability of the vSphere environment, as well as optional enablement of SSH connectivity to each host for the updating of drivers.

To configure ESXi settings, follow these steps:

1. Select the first ESXi host to configure with standard settings.

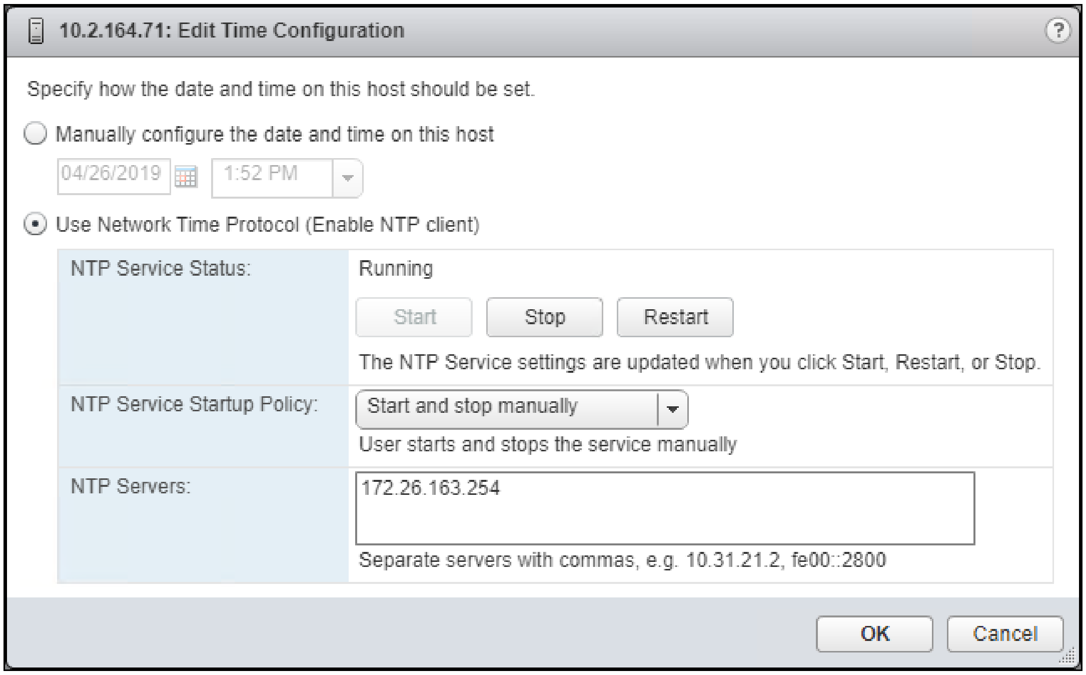
2. Select the Configure tab and select Time Configuration within the options under System and click Edit within Time Configuration.



Time Configuration

Date & Time:	4/26/2019 1:50 PM
NTP Client:	Disabled
NTP Service Status:	Stopped
NTP Servers:	

3. Select Use Network Time Protocol (Enable NTP client), enter <<var_oob_ntp>> for the NTP Servers, select Start and stop with port usage for NTP Service Startup Policy, and click Start within NTP Service Status. Click OK to submit the changes.



10.2.164.71: Edit Time Configuration

Specify how the date and time on this host should be set.

○ Manually configure the date and time on this host

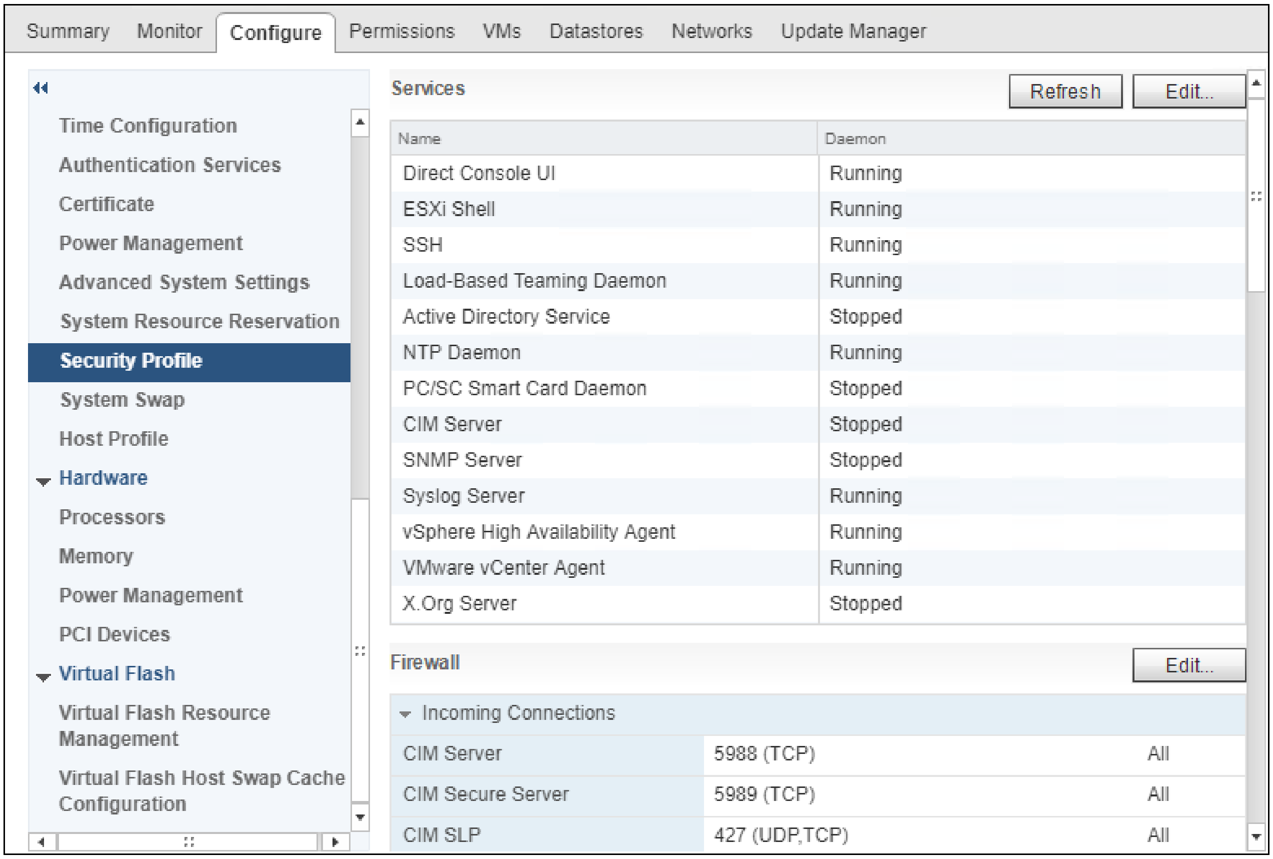
04/26/2019 1:52 PM

● Use Network Time Protocol (Enable NTP client)

NTP Service Status:	Running Start Stop Restart The NTP Service settings are updated when you click Start, Restart, or Stop.
NTP Service Startup Policy:	Start and stop manually User starts and stops the service manually
NTP Servers:	172.26.163.254 Separate servers with commas, e.g. 10.31.21.2, fe00::2800

4. (Optional) Click **Security Profile** within the **Configure** tab under the **System** section for the host.

The Security Profile settings for the ESXi Shell and SSH are enabled later for the potential update of the nenic driver. These steps are unnecessary if you're using VMware Update Manager and these drivers are being handled by being included into a configured baseline. If SSH is enabled for updates, it is recommended to later disable this service if it is considered a security risk in the environment.



Services

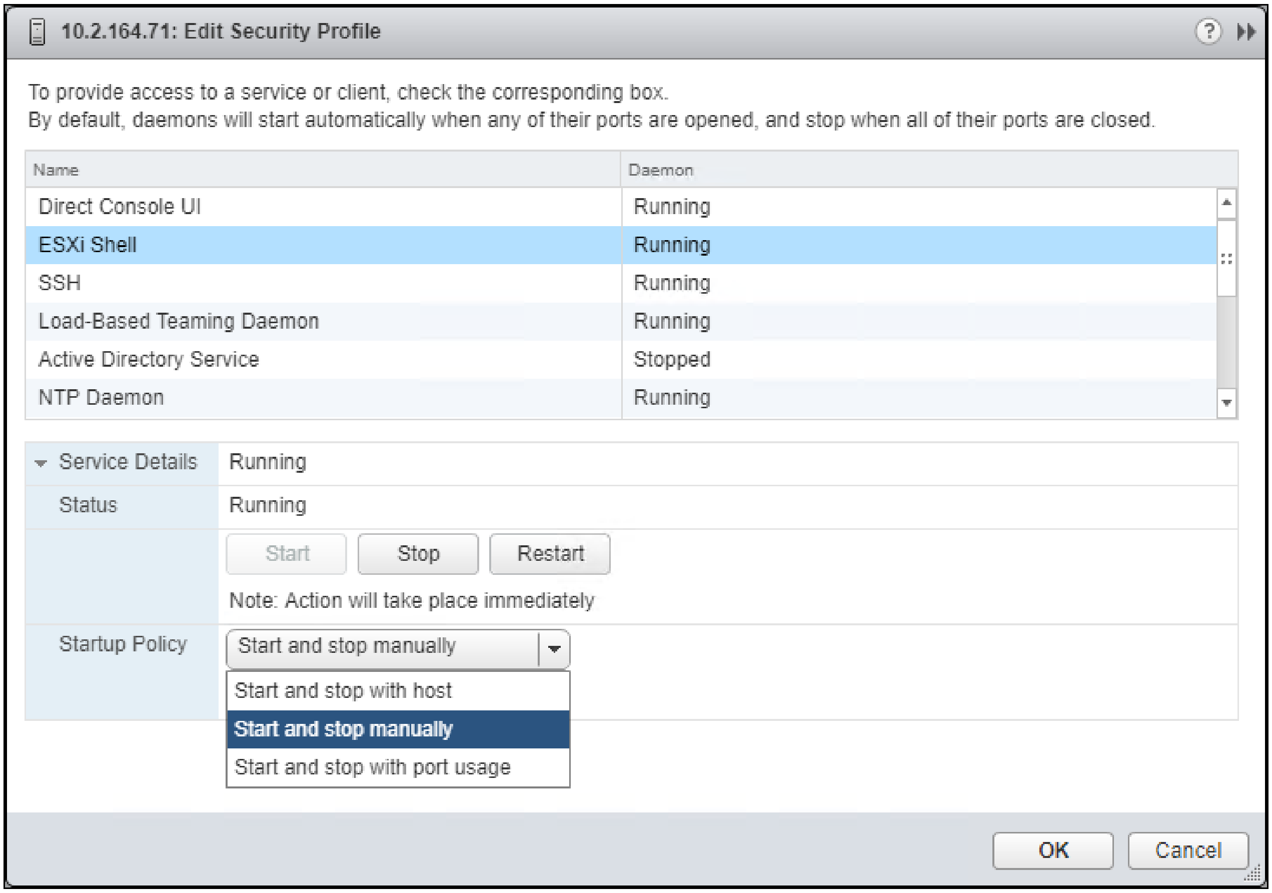
Name	Daemon
Direct Console UI	Running
ESXi Shell	Running
SSH	Running
Load-Based Teaming Daemon	Running
Active Directory Service	Stopped
NTP Daemon	Running
PC/SC Smart Card Daemon	Stopped
CIM Server	Stopped
SNMP Server	Stopped
Syslog Server	Running
vSphere High Availability Agent	Running
VMware vCenter Agent	Running
X.Org Server	Stopped

Firewall

Incoming Connections

CIM Server	5988 (TCP)	All
CIM Secure Server	5989 (TCP)	All
CIM SLP	427 (UDP,TCP)	All

5. Scroll down to the Services section within Security Profile and click the Edit.



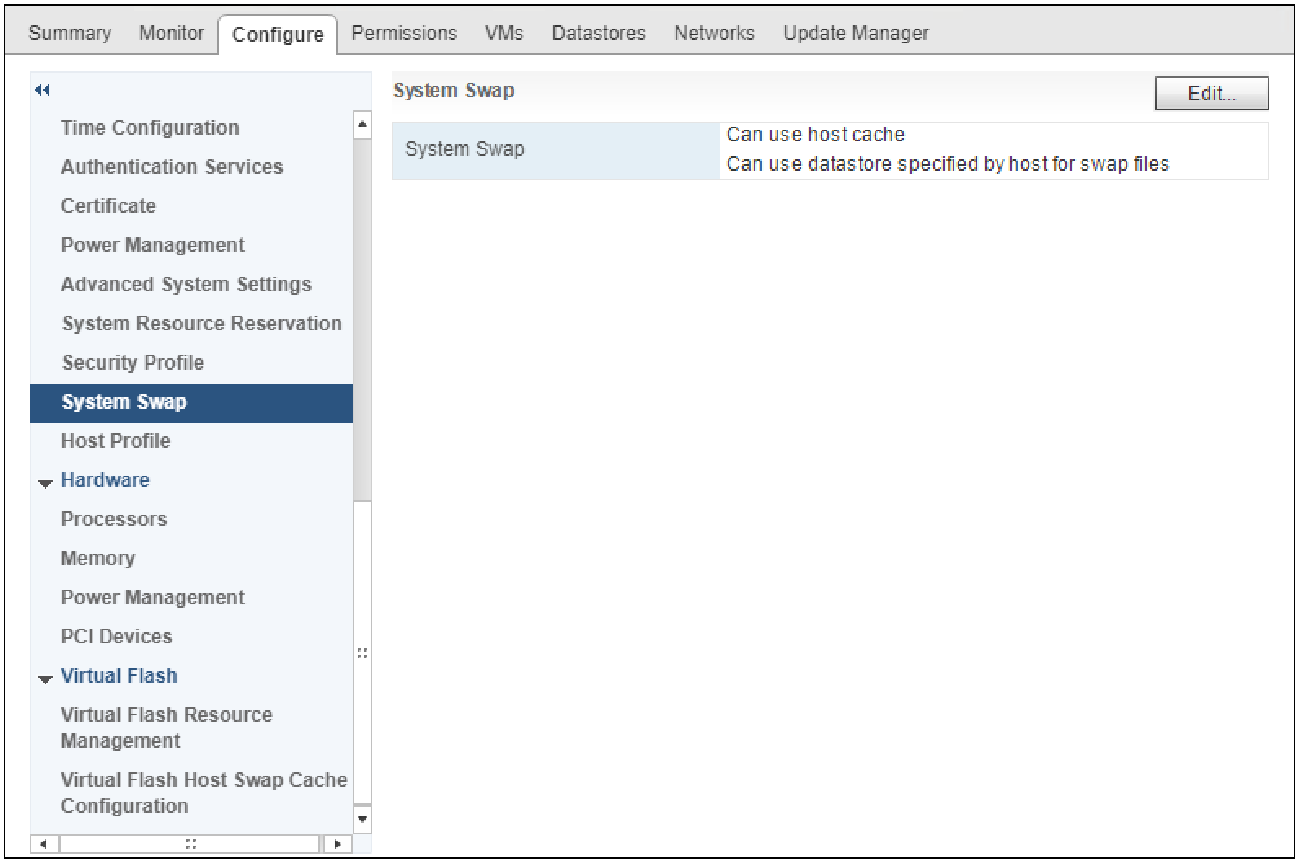
10.2.164.71: Edit Security Profile

To provide access to a service or client, check the corresponding box.
By default, daemons will start automatically when any of their ports are opened, and stop when all of their ports are closed.

Name	Daemon
Direct Console UI	Running
ESXi Shell	Running
SSH	Running
Load-Based Teaming Daemon	Running
Active Directory Service	Stopped
NTP Daemon	Running

Service Details	Running
Status	Running
	Start Stop Restart Note: Action will take place immediately
Startup Policy	Start and stop manually

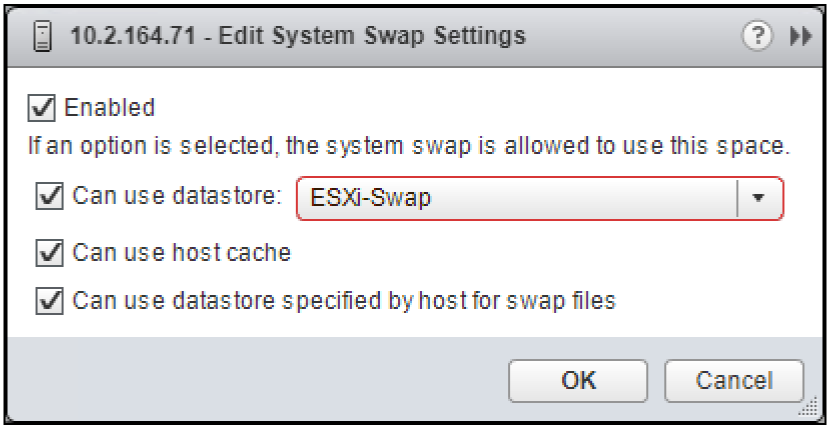
6. Select the ESXi Shell entry, change the Startup Policy to Start and stop with port usage, and click Start. Repeat these steps for the SSH entry. Click OK.



System Swap

System Swap	Can use host cache Can use datastore specified by host for swap files

7. If an optional ESXi swap datastore was configured earlier, click System Swap the System section within the Configure tab and click Edit.



10.2.164.71 - Edit System Swap Settings

☑ Enabled

If an option is selected, the system swap is allowed to use this space.

☑ Can use datastore: ESXi-Swap

☑ Can use host cache

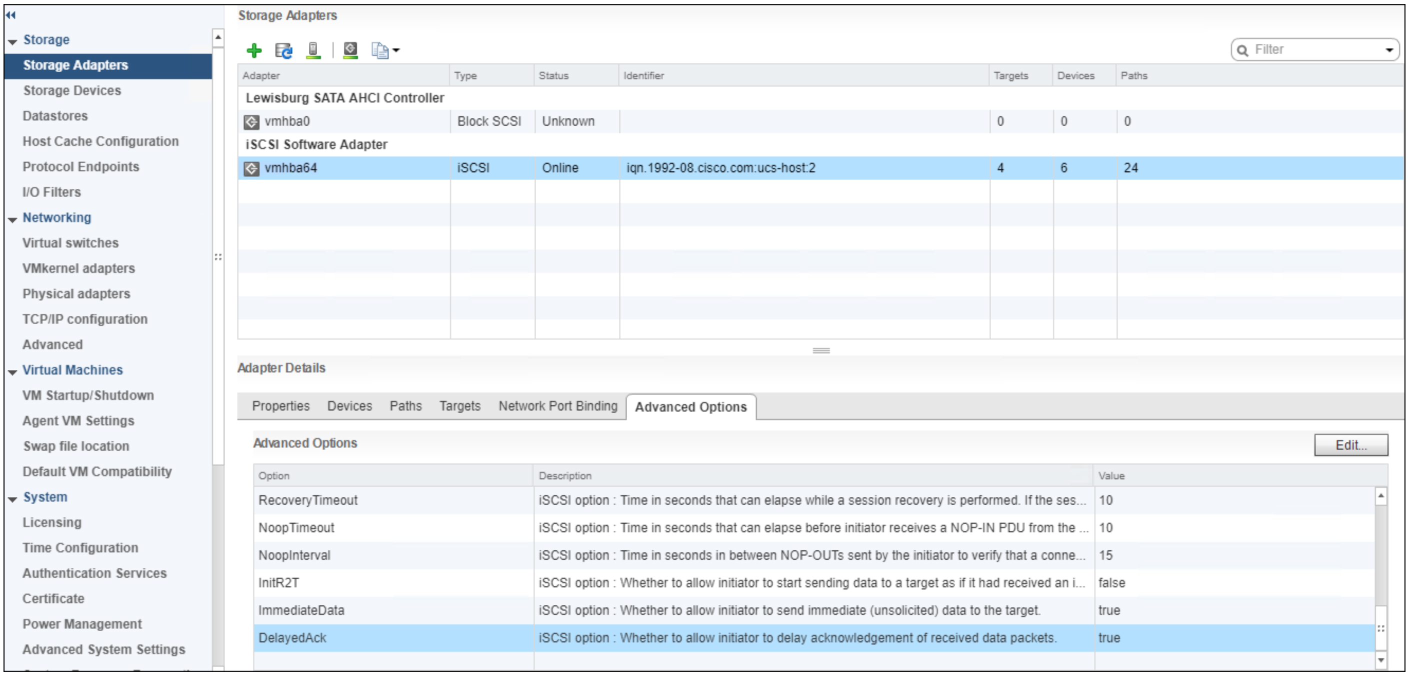
☑ Can use datastore specified by host for swap files

8. Select the Can use datastore box and from the drop-down list select the ESXi swap datastore that was configured. Click OK.

9. Select Storage Adapters.

10. Select the iSCSI Software Adapter.

11. Select Advanced Options in the Adapter Details section.



Storage Adapters

Adapter	Type	Status	Identifier	Targets	Devices	Paths
Lewisburg SATA AHCI Controller						
vmhba0	Block SCSI	Unknown		0	0	0
iSCSI Software Adapter						
vmhba64	iSCSI	Online	iqn.1992-08.cisco.com:ucs-host:2	4	6	24

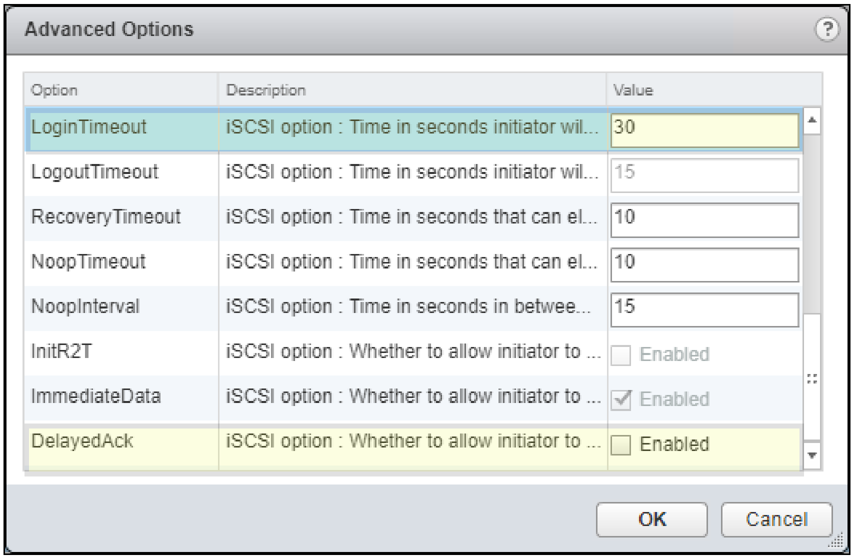
Adapter Details

Advanced Options

Option	Description	Value
RecoveryTimeout	iSCSI option : Time in seconds that can elapse while a session recovery is performed. If the ses...	10
NoopTimeout	iSCSI option : Time in seconds that can elapse before initiator receives a NOP-IN PDU from the ...	10
NoopInterval	iSCSI option : Time in seconds in between NOP-OUTs sent by the initiator to verify that a conne...	15
InitR2T	iSCSI option : Whether to allow initiator to start sending data to a target as if it had received an i...	false
ImmediateData	iSCSI option : Whether to allow initiator to send immediate (unsolicited) data to the target.	true
DelayedAck	iSCSI option : Whether to allow initiator to delay acknowledgement of received data packets.	true

12. Select Edit

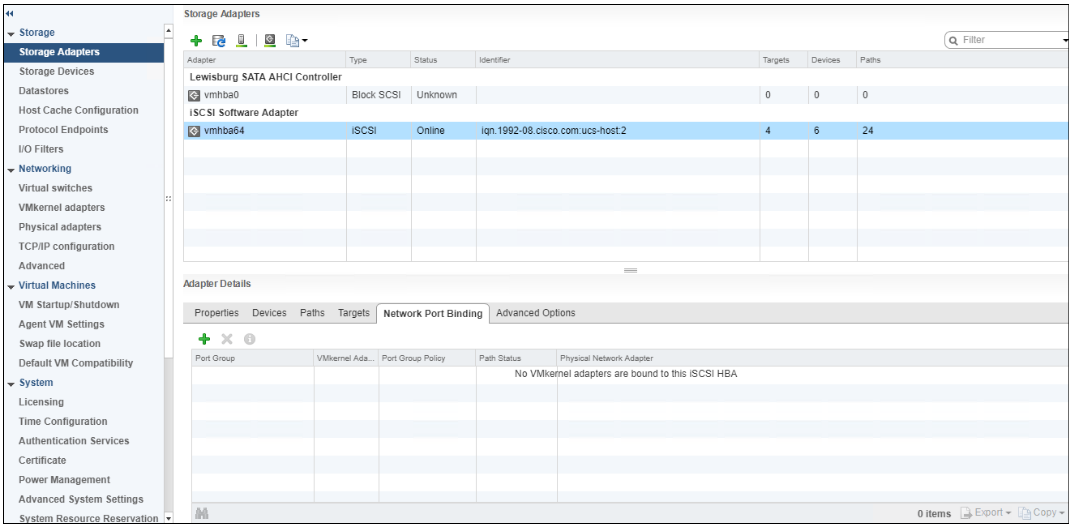
13. Change the LoginTimeout to 30 and Uncheck DelayedAck.



Advanced Options

Option	Description	Value
LoginTimeout	iSCSI option : Time in seconds initiator wil...	30
LogoutTimeout	iSCSI option : Time in seconds initiator wil...	15
RecoveryTimeout	iSCSI option : Time in seconds that can el...	10
NoopTimeout	iSCSI option : Time in seconds that can el...	10
NoopInterval	iSCSI option : Time in seconds in betwee...	15
InitR2T	iSCSI option : Whether to allow initiator to ...	□ Enabled
ImmediateData	iSCSI option : Whether to allow initiator to ...	☑ Enabled
DelayedAck	iSCSI option : Whether to allow initiator to ...	□ Enabled

14. Select Network Port Binding in the Adapter Details section.



Storage Adapters

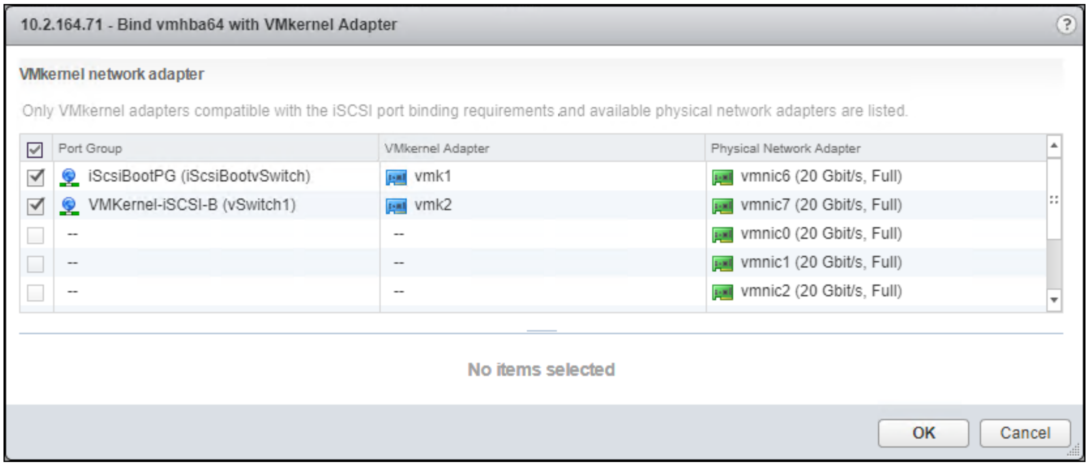
Adapter	Type	Status	Identifier	Targets	Devices	Paths
Lewisburg SATA AHCI Controller						
vmhba0	Block SCSI	Unknown		0	0	0
iSCSI Software Adapter						
vmhba64	iSCSI	Online	iqn.1992-08.cisco.com:ucs-host:2	4	6	24

Port Group	VMkernel Ada...	Port Group Policy	Path Status	Physical Network Adapter

No VMkernel adapters are bound to this iSCSI HBA

15. Click the green + icon.

16. Select both iSCSI VMkernel Adapters.



10.2.164.71 - Bind vmhba64 with VMkernel Adapter

VMkernel network adapter

Only VMkernel adapters compatible with the iSCSI port binding requirements and available physical network adapters are listed.

☑	Port Group	VMkernel Adapter	Physical Network Adapter
☑	iScsiBootPG (iScsiBootvSwitch)	vmk1	vmnic6 (20 Gbit/s, Full)
☑	VMKernel-iSCSI-B (vSwitch1)	vmk2	vmnic7 (20 Gbit/s, Full)
□	--	--	vmnic0 (20 Gbit/s, Full)
□	--	--	vmnic1 (20 Gbit/s, Full)
□	--	--	vmnic2 (20 Gbit/s, Full)

No items selected

17. Select OK

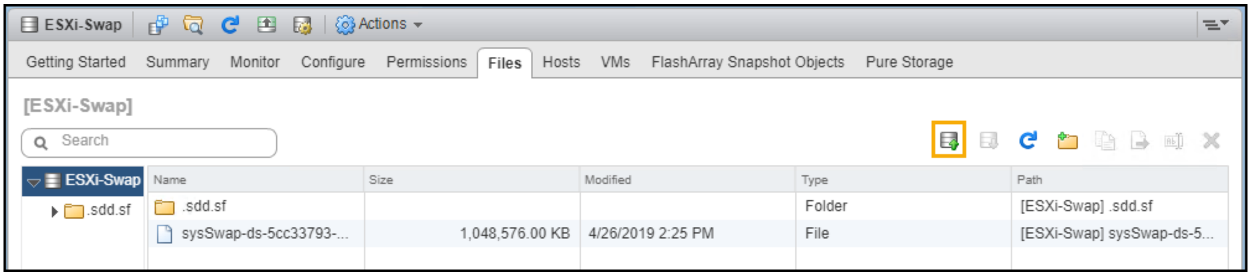
18. Repeat steps 1-17 on each ESXi host being added into the cluster.

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

The Cisco Custom Image for VMware vSphere 6.7 U1 comes with the nenic 1.0.25.0 for Ethernet traffic from the ESXi host and an upgrade is recommended. For the most recent versions, please refer to Cisco UCS HW and SW Availability Interoperability Matrix. To update the drivers for VMware vSphere 6.7 U1, follow these steps:

1. Download and extract either driver bundle (for example, nenic Driver version 1.0.26.0) to the system the vSphere Web Client is running.

2. Within the vSphere Web Client, select one of the datastores common to all the hosts.



Name	Size	Modified	Type	Path
.sdd.sf			Folder	[ESXi-Swap] .sdd.sf
sysSwap-ds-5cc33793-...	1,048,576.00 KB	4/26/2019 2:25 PM	File	[ESXi-Swap] sysSwap-ds-5...

3. Click Upload a file to the Datastore.

4. Select and upload the offline_bundle (VMW-ESX-6.7.0-nenic-1.0.26.0-offline_bundle-10825029.zip) from each of the extracted driver downloads.

5. Place all hosts in Maintenance mode requiring update.

6. Connect to each ESXi host through ssh from a shell connection or putty terminal.

7. Login as root with the root password.

8. Run the following command (substituting the appropriate datastore directory if needed) on each host:

```
esxcli software vib update -d /vmfs/volumes/ESXi-Swap/VMW-ESX-6.7.0-nenic-1.0.26.0-offline_bundle-10825029.zip
```

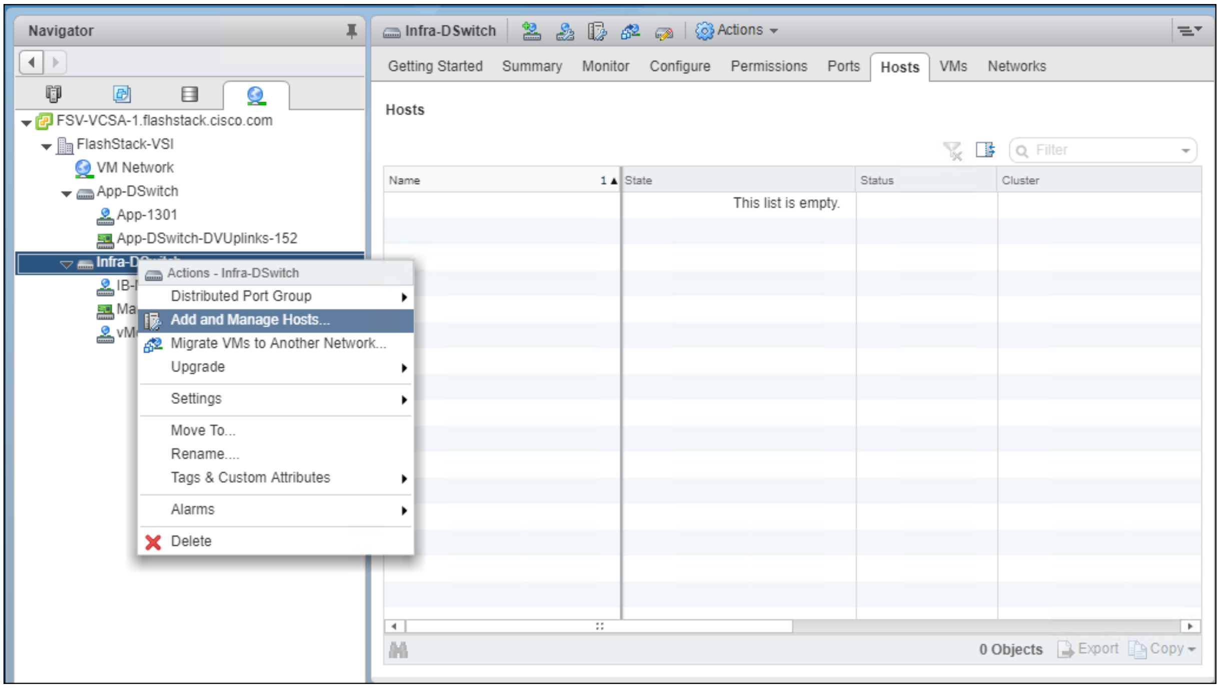
9. Reboot each host by typing `reboot` from the SSH connection after the command has run.

10. Log into the Host Client on each host once reboot is complete.

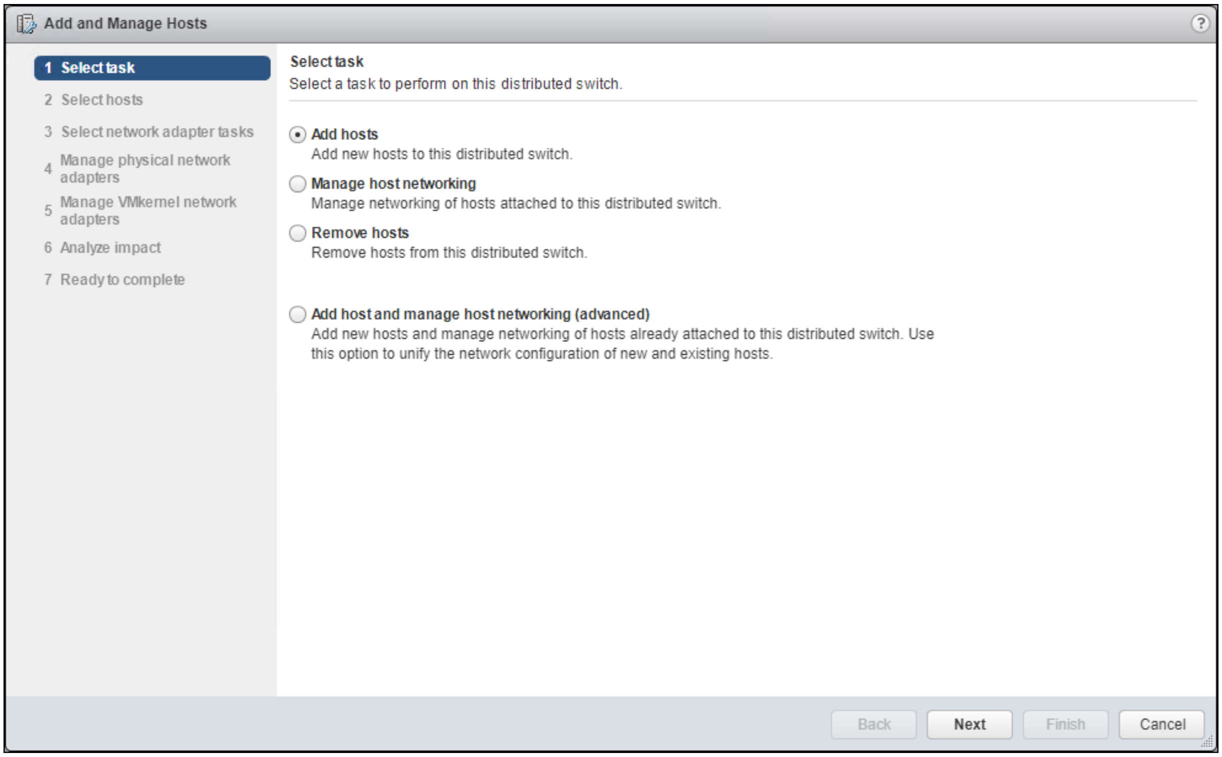
Add the ESXi hosts to the vDS

To Add the ESXi Hosts to each vDS, follow these steps:

1. Within the Networking tab of the Navigator window, right-click the Infra-DSwitch vDS and select Add and Manage Hosts.



2. Leave Add hosts selected and click Next.



Select task

Select a task to perform on this distributed switch.

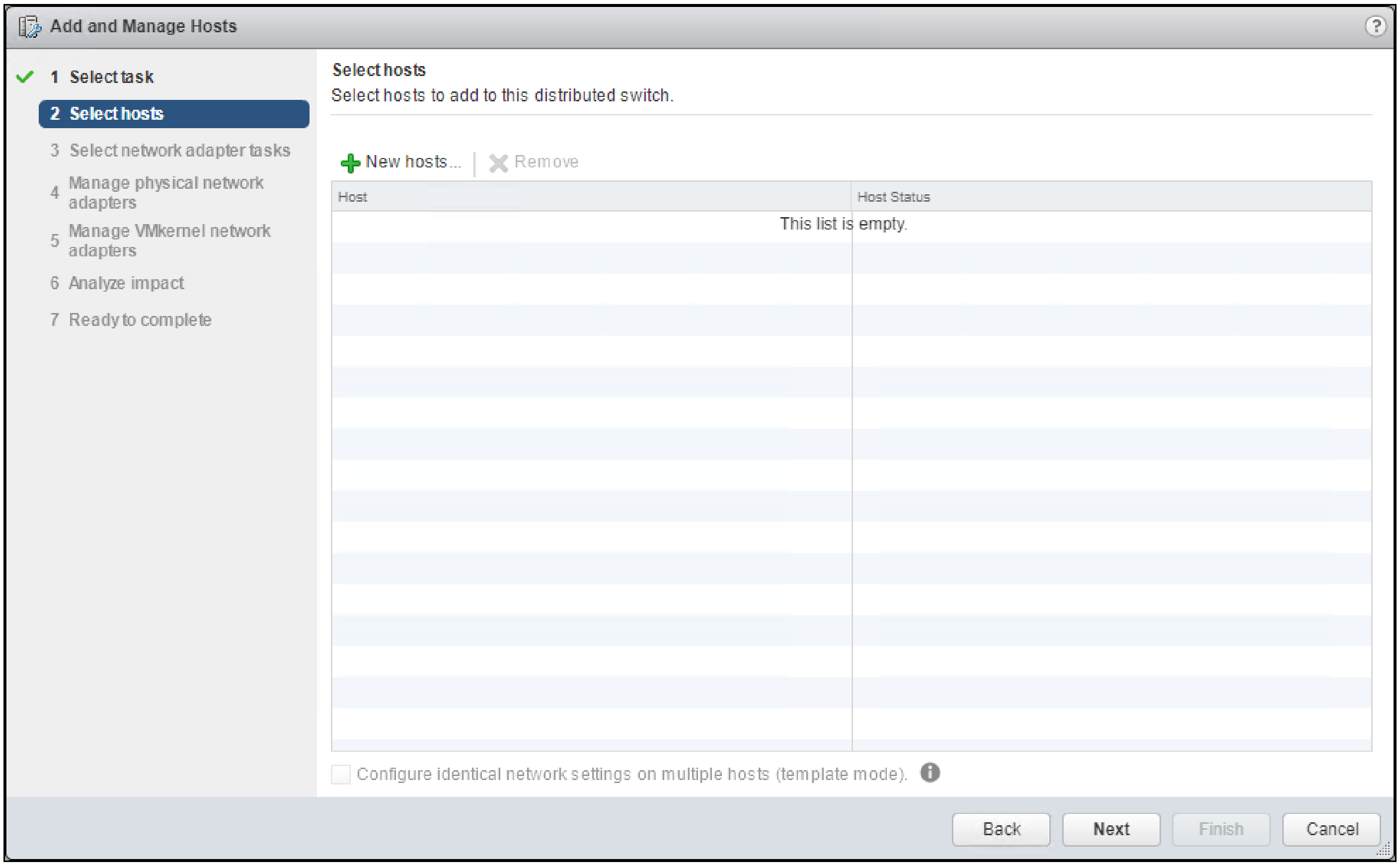
● Add hosts
Add new hosts to this distributed switch.

○ Manage host networking
Manage networking of hosts attached to this distributed switch.

○ Remove hosts
Remove hosts from this distributed switch.

○ Add host and manage host networking (advanced)
Add new hosts and manage networking of hosts already attached to this distributed switch. Use this option to unify the network configuration of new and existing hosts.

3. Click the green + icon next to New hosts.



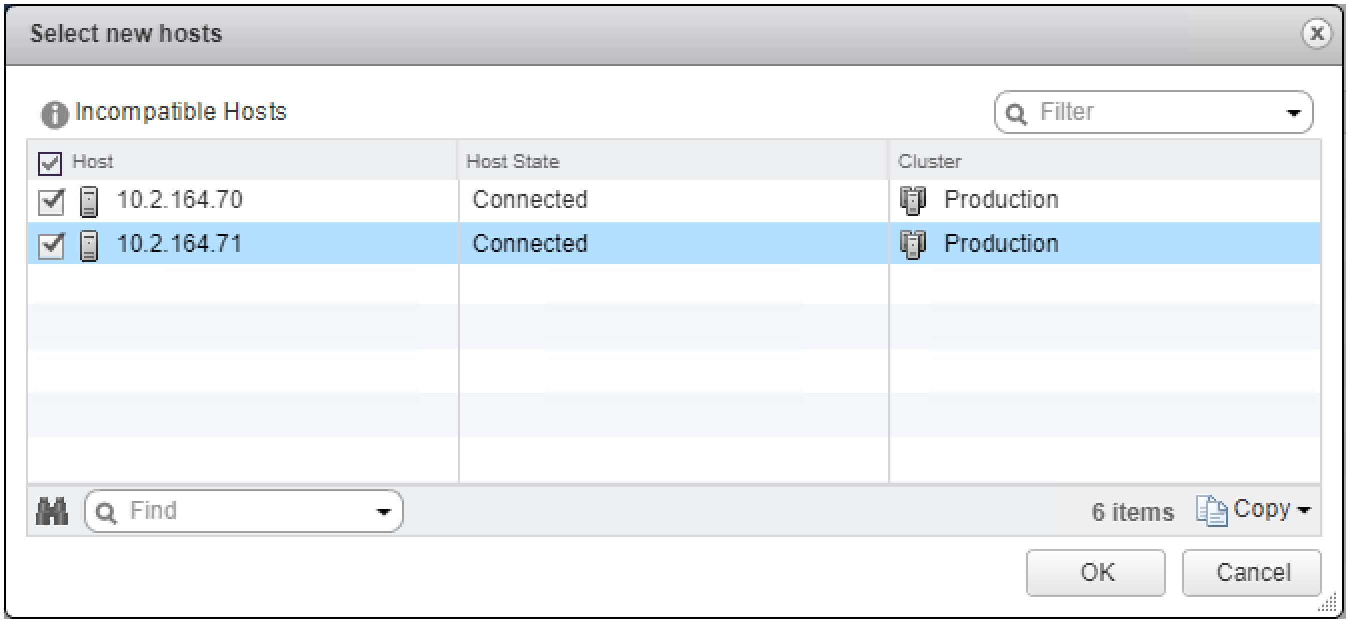
Select hosts

Select hosts to add to this distributed switch.

Host	Host Status
This list is empty.	

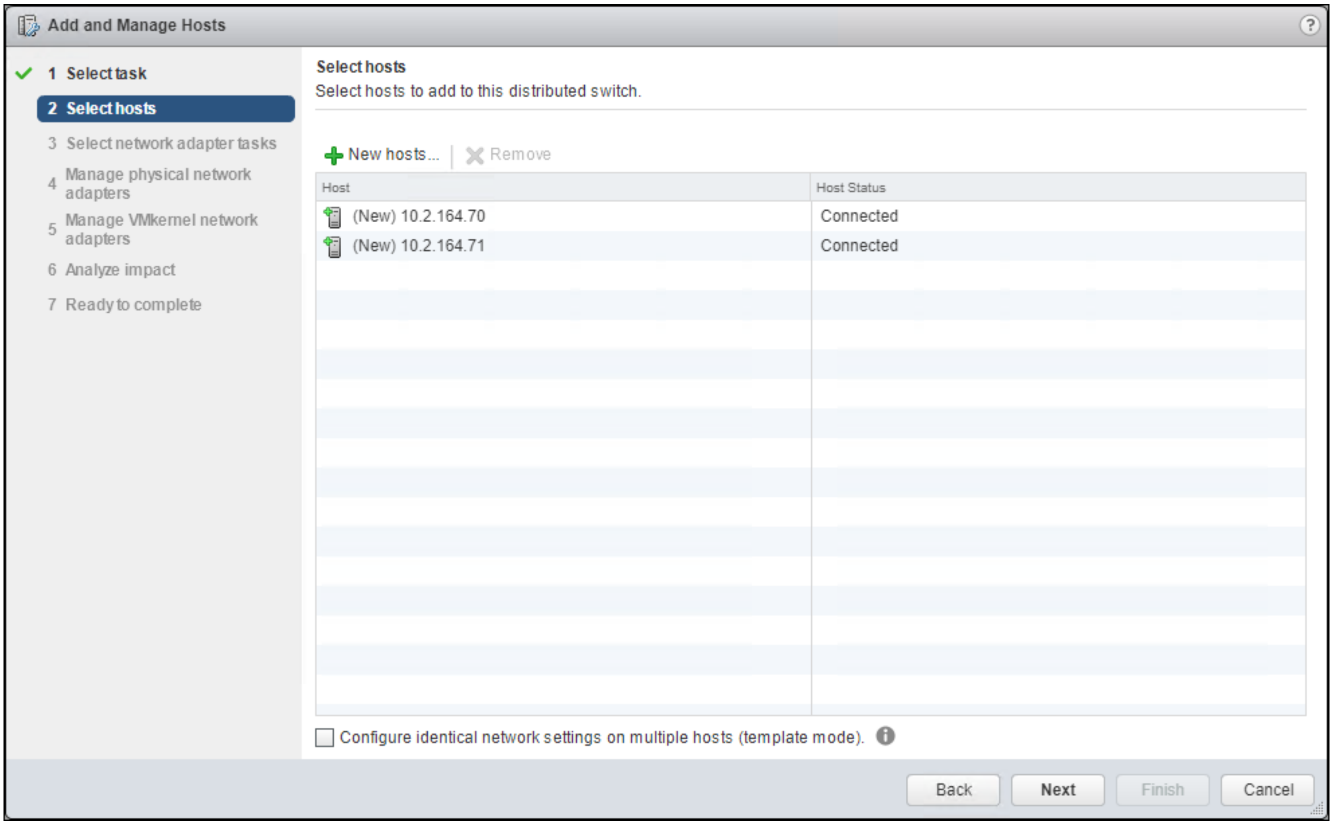
□ Configure identical network settings on multiple hosts (template mode).

4. In the **Select new hosts** pop-up that appears, select the hosts to be added, and click **OK** to begin joining them to the vDS.



☑ Host	Host State	Cluster
☑ 10.2.164.70	Connected	Production
☑ 10.2.164.71	Connected	Production

5. Click Next.



Add and Model Hosts

✓ 1 Select task
2 Select hosts
3 Select network adapter tasks
4 Manage physical network adapters
5 Manage VMkernel network adapters
6 Analyze impact
7 Ready to complete

Select hosts
Select hosts to add to this distributed switch.

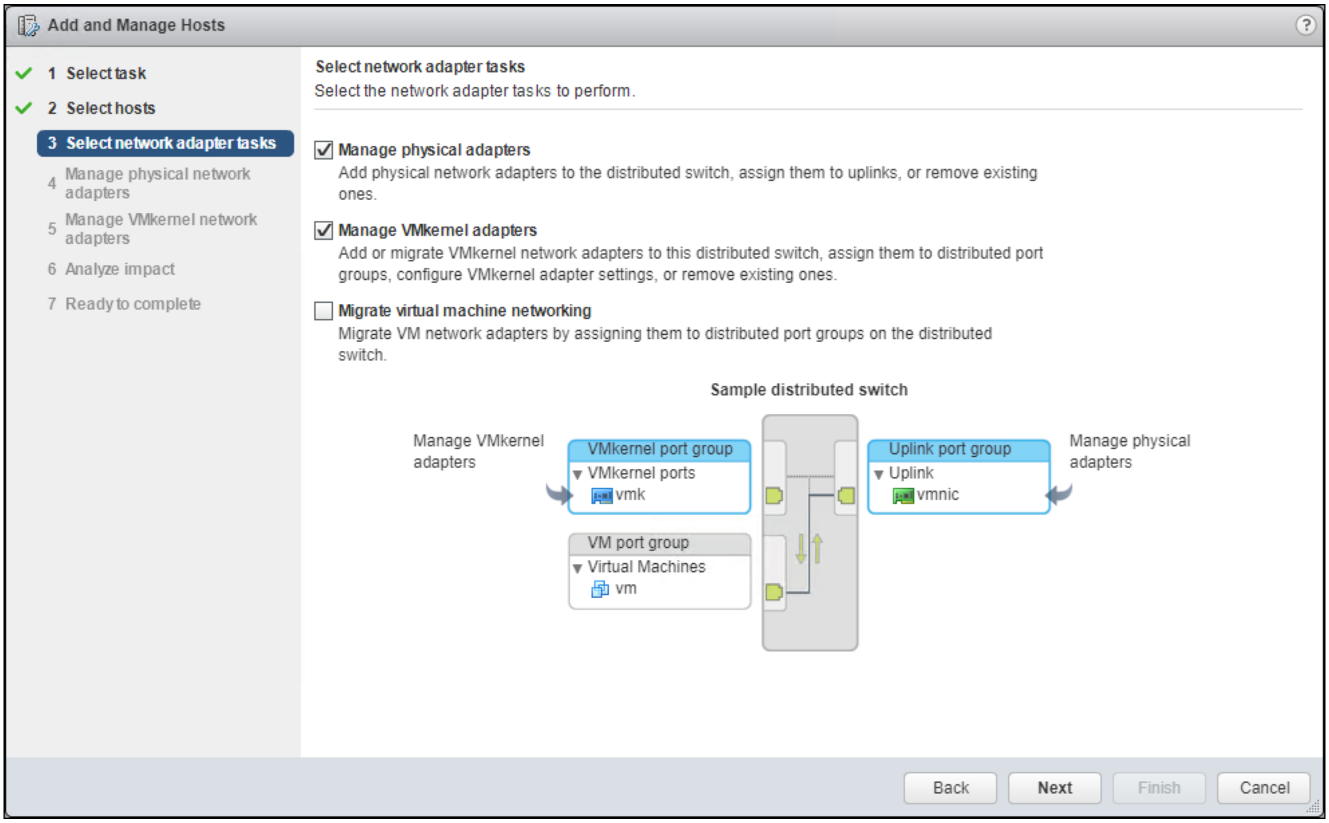
+ New hosts... | ✕ Remove

Host	Host Status
(New) 10.2.164.70	Connected
(New) 10.2.164.71	Connected

□ Configure identical network settings on multiple hosts (template mode).

Back | Next | Finish | Cancel

6. Leave Manage physical adapters and Manage VMkernel adapters both selected and click Next.



Add and Manage Hosts

✓ 1 Select task
✓ 2 Select hosts
3 Select network adapter tasks
4 Manage physical network adapters
5 Manage VMkernel network adapters
6 Analyze impact
7 Ready to complete

Select network adapter tasks
Select the network adapter tasks to perform.

☑ **Manage physical adapters**
Add physical network adapters to the distributed switch, assign them to uplinks, or remove existing ones.

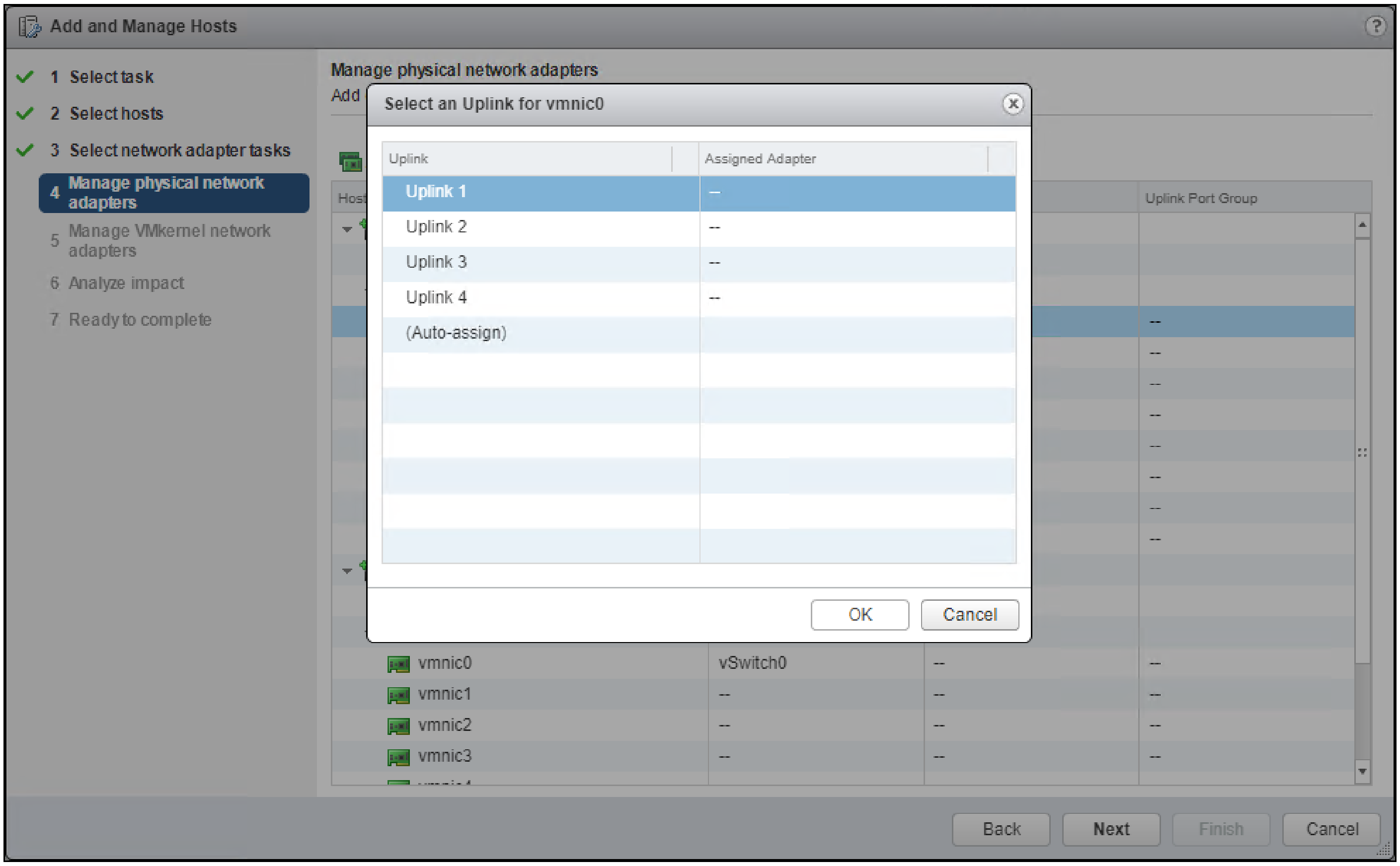
☑ **Manage VMkernel adapters**
Add or migrate VMkernel network adapters to this distributed switch, assign them to distributed port groups, configure VMkernel adapter settings, or remove existing ones.

□ **Migrate virtual machine networking**
Migrate VM network adapters by assigning them to distributed port groups on the distributed switch.

Sample distributed switch

Back | Next | Finish | Cancel

7. Select vmnic0 from the **Host/Physical Network Adapters** column and click the **Assign uplink** option.

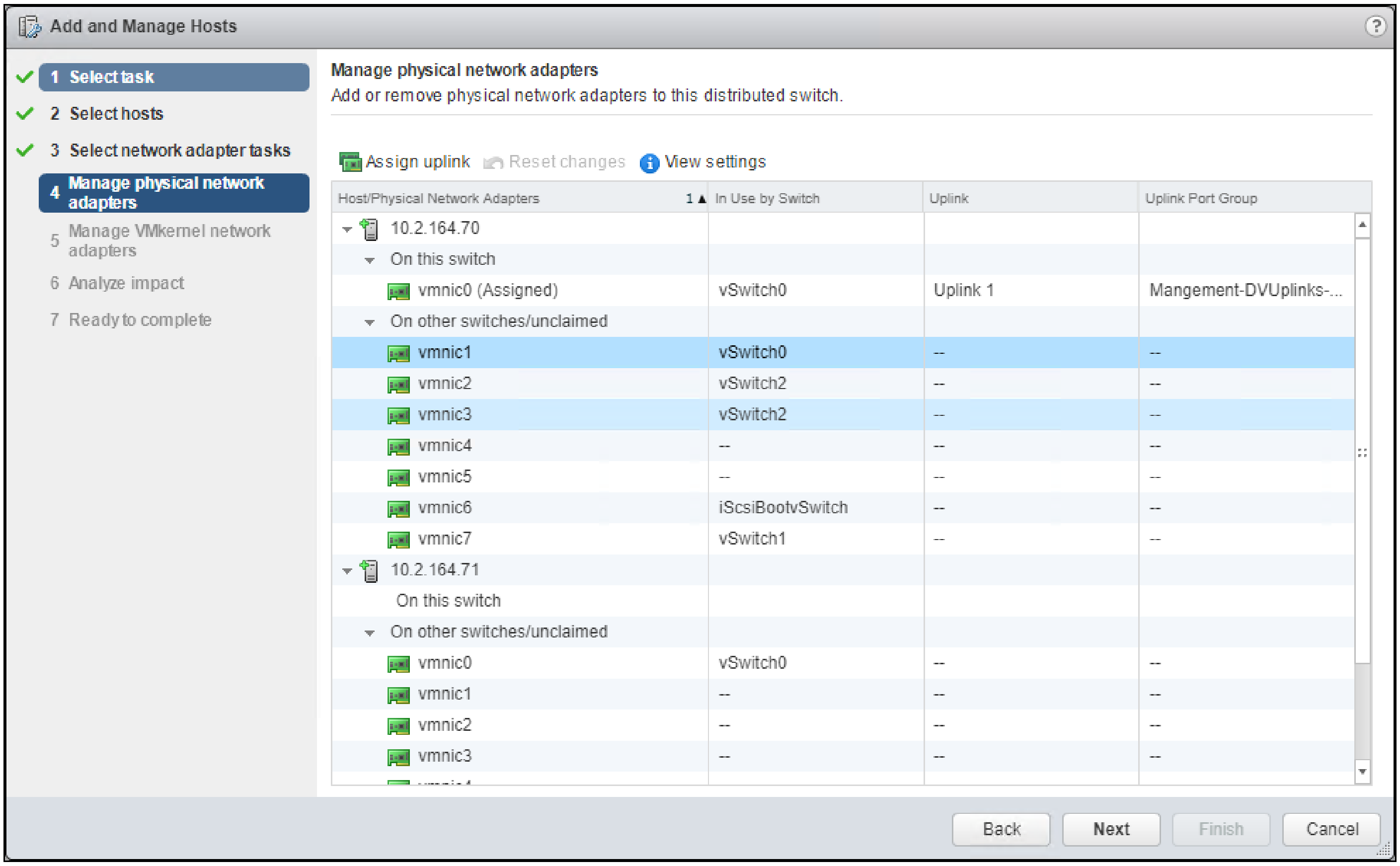

Add and Manage Hosts
1 Select task
2 Select hosts
3 Select network adapter tasks
4 Manage physical network adapters
5 Manage VMkernel network adapters
6 Analyze impact
7 Ready to complete
Manage physical network adapters
Add
Host
Uplink Port Group
Back
Next
Finish
Cancel

Select an Uplink for vmnic0

Uplink	Assigned Adapter
Uplink 1	--
Uplink 2	--
Uplink 3	--
Uplink 4	--
(Auto-assign)	

vmnic0	vSwitch0	--	--
vmnic1	--	--	--
vmnic2	--	--	--
vmnic3	--	--	--

8. Leave Uplink 1 selected and click OK.

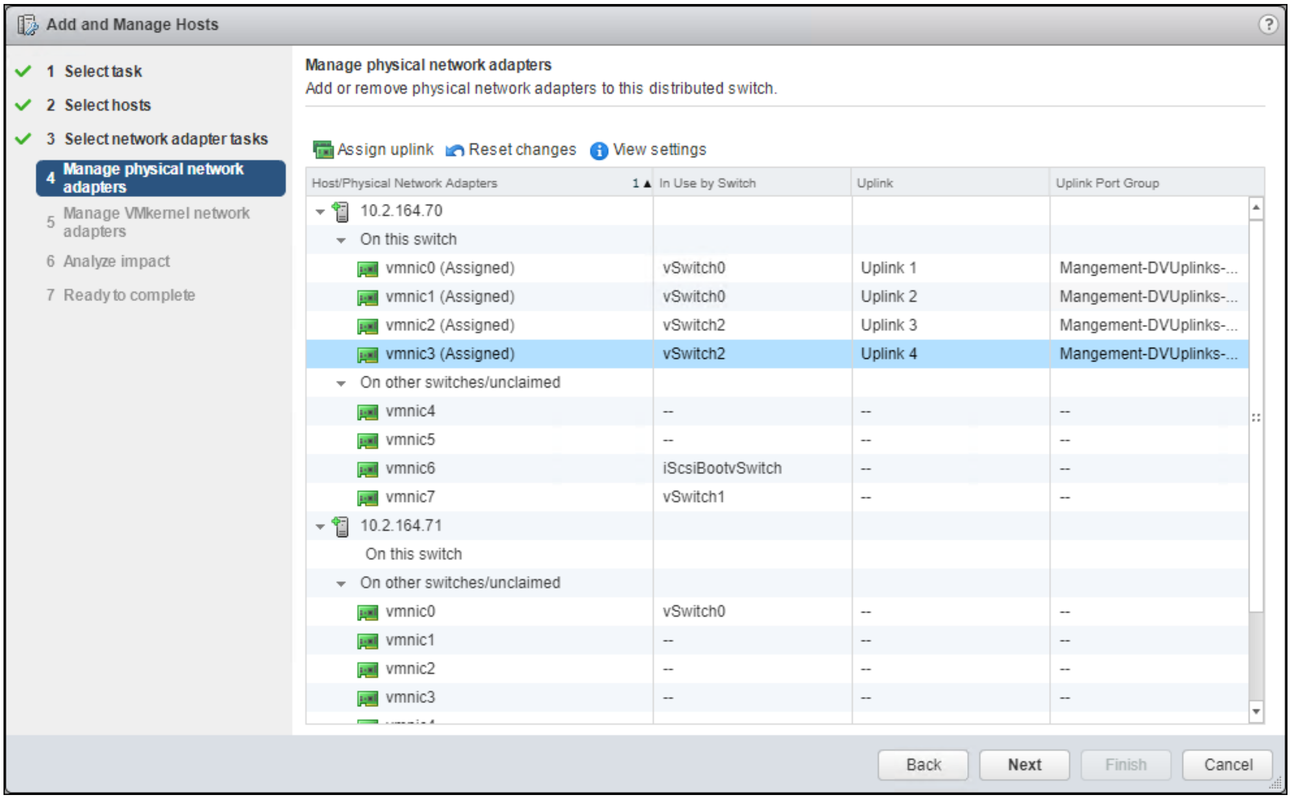


Manage physical network adapters

Add or remove physical network adapters to this distributed switch.

Host/Physical Network Adapters	In Use by Switch	Uplink	Uplink Port Group
10.2.164.70			
On this switch			
vmnic0 (Assigned)	vSwitch0	Uplink 1	Mangement-DVUplinks-...
On other switches/unclaimed			
vmnic1	vSwitch0	--	--
vmnic2	vSwitch2	--	--
vmnic3	vSwitch2	--	--
vmnic4	--	--	--
vmnic5	--	--	--
vmnic6	iScsiBootvSwitch	--	--
vmnic7	vSwitch1	--	--
10.2.164.71			
On this switch			
On other switches/unclaimed			
vmnic0	vSwitch0	--	--
vmnic1	--	--	--
vmnic2	--	--	--
vmnic3	--	--	--

9. Repeat this step for vmnic1-3, assigning them to uplinks 2-4 in corresponding sequence.



Add and Manage Hosts

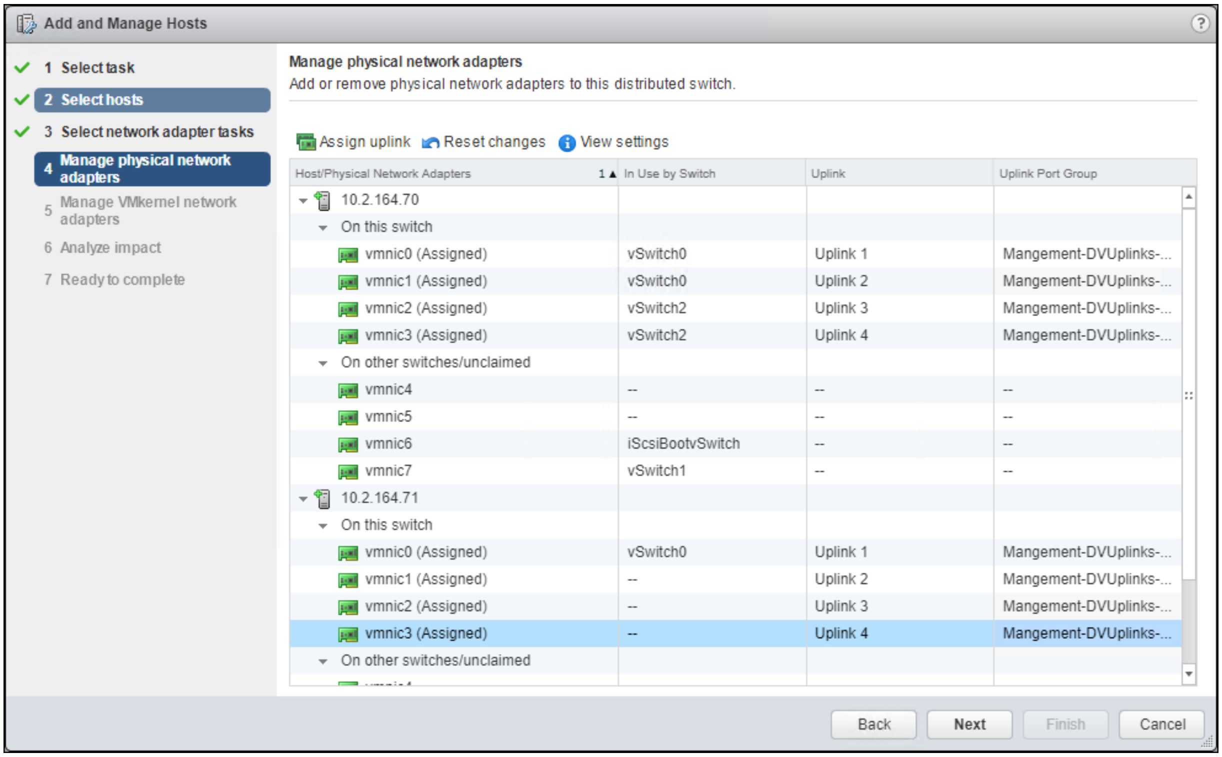
✓ 1 Select task
✓ 2 Select hosts
✓ 3 Select network adapter tasks
4 Manage physical network adapters
5 Manage VMkernel network adapters
6 Analyze impact
7 Ready to complete

Manage physical network adapters

Add or remove physical network adapters to this distributed switch.

Host/Physical Network Adapters	In Use by Switch	Uplink	Uplink Port Group
10.2.164.70			
On this switch			
vmnic0 (Assigned)	vSwitch0	Uplink 1	Mangement-DVUplinks-...
vmnic1 (Assigned)	vSwitch0	Uplink 2	Mangement-DVUplinks-...
vmnic2 (Assigned)	vSwitch2	Uplink 3	Mangement-DVUplinks-...
vmnic3 (Assigned)	vSwitch2	Uplink 4	Mangement-DVUplinks-...
On other switches/unclaimed			
vmnic4	--	--	--
vmnic5	--	--	--
vmnic6	iScsiBootvSwitch	--	--
vmnic7	vSwitch1	--	--
10.2.164.71			
On this switch			
On other switches/unclaimed			
vmnic0	vSwitch0	--	--
vmnic1	--	--	--
vmnic2	--	--	--
vmnic3	--	--	--

10. Repeat these assignments for all additional ESXi hosts being configured.



Add and Manage Hosts

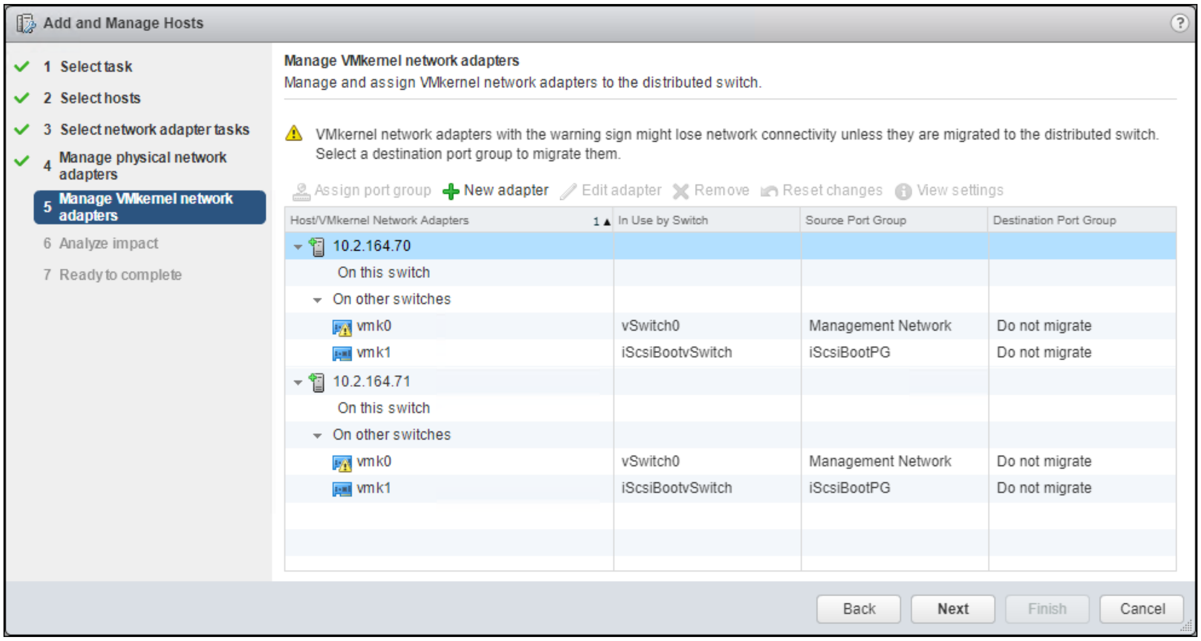
✓ 1 Select task
✓ 2 Select hosts
✓ 3 Select network adapter tasks
4 Manage physical network adapters
5 Manage VMkernel network adapters
6 Analyze impact
7 Ready to complete

Manage physical network adapters

Add or remove physical network adapters to this distributed switch.

Host/Physical Network Adapters	In Use by Switch	Uplink	Uplink Port Group
10.2.164.70			
On this switch			
vmnic0 (Assigned)	vSwitch0	Uplink 1	Mangement-DVUplinks-...
vmnic1 (Assigned)	vSwitch0	Uplink 2	Mangement-DVUplinks-...
vmnic2 (Assigned)	vSwitch2	Uplink 3	Mangement-DVUplinks-...
vmnic3 (Assigned)	vSwitch2	Uplink 4	Mangement-DVUplinks-...
On other switches/unclaimed			
vmnic4	--	--	--
vmnic5	--	--	--
vmnic6	iScsiBootvSwitch	--	--
vmnic7	vSwitch1	--	--
10.2.164.71			
On this switch			
vmnic0 (Assigned)	vSwitch0	Uplink 1	Mangement-DVUplinks-...
vmnic1 (Assigned)	--	Uplink 2	Mangement-DVUplinks-...
vmnic2 (Assigned)	--	Uplink 3	Mangement-DVUplinks-...
vmnic3 (Assigned)	--	Uplink 4	Mangement-DVUplinks-...
On other switches/unclaimed			

11. Click Next.

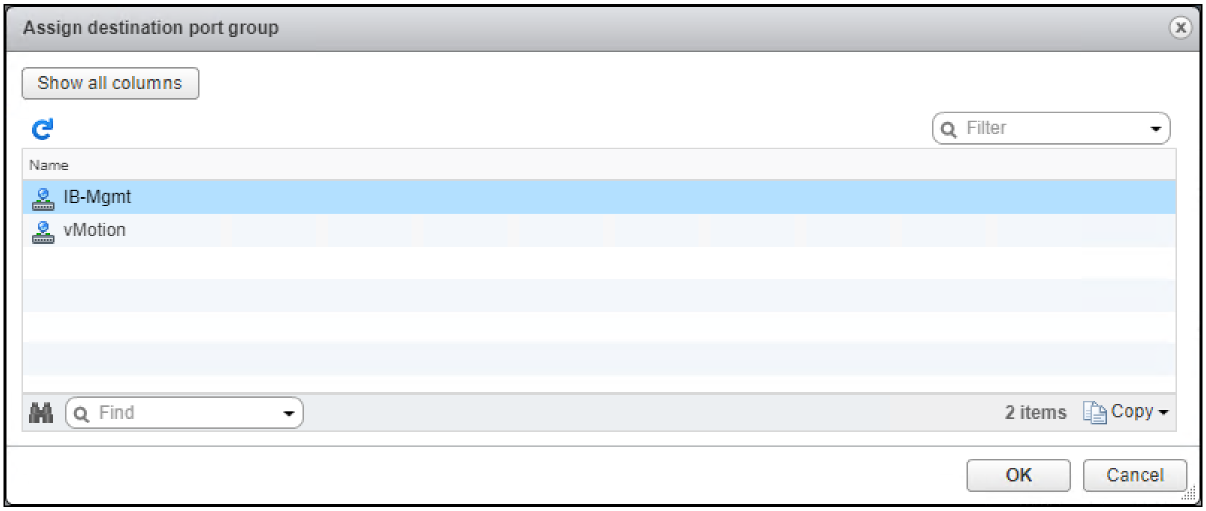


Manage VMkernel network adapters
Manage and assign VMkernel network adapters to the distributed switch.

VMkernel network adapters with the warning sign might lose network connectivity unless they are migrated to the distributed switch. Select a destination port group to migrate them.

Host/VMkernel Network Adapters	In Use by Switch	Source Port Group	Destination Port Group
10.2.164.70			
On this switch			
On other switches			
vmk0	vSwitch0	Management Network	Do not migrate
vmk1	iScsiBootvSwitch	iScsiBootPG	Do not migrate
10.2.164.71			
On this switch			
On other switches			
vmk0	vSwitch0	Management Network	Do not migrate
vmk1	iScsiBootvSwitch	iScsiBootPG	Do not migrate

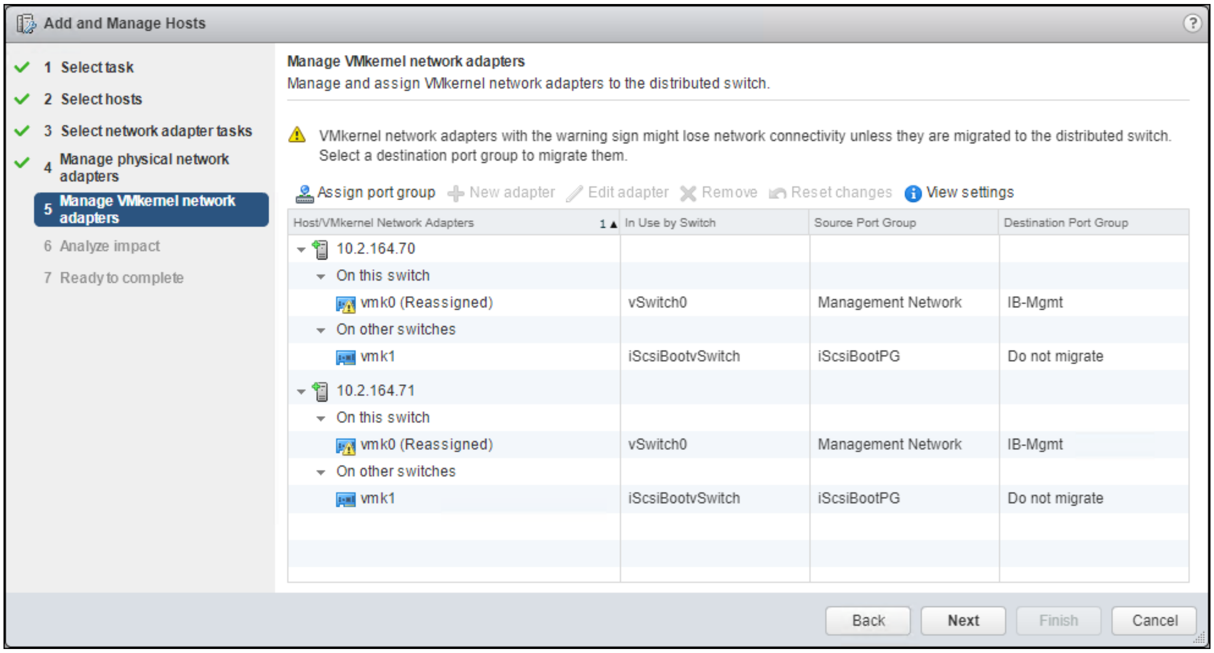
12. Select the vmko of the first host and click the Assign port group option.



Name
IB-Mgmt
vMotion

13. Select the IB-Mgmt destination port group and click OK.

14. Repeat this step for all additional hosts being configured.



Manage VMkernel network adapters

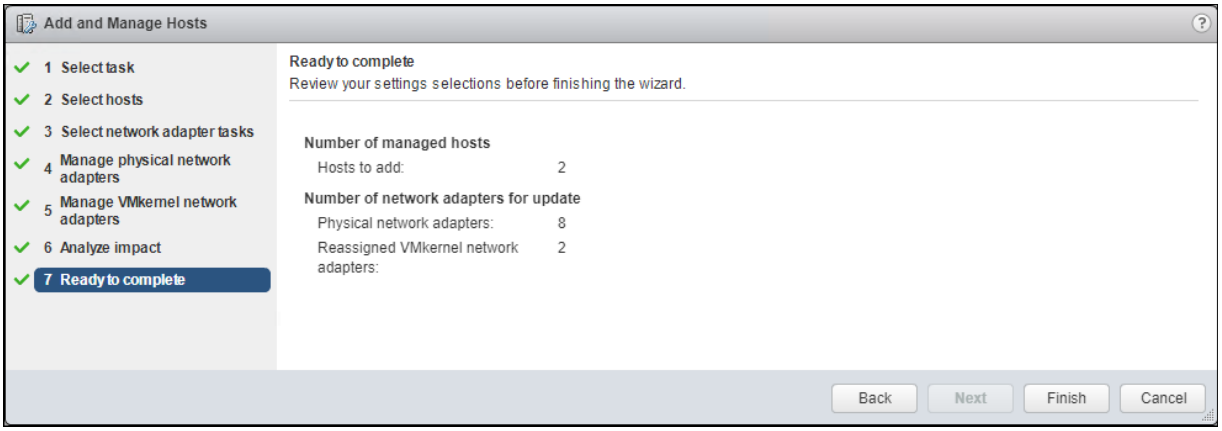
Manage and assign VMkernel network adapters to the distributed switch.

VMkernel network adapters with the warning sign might lose network connectivity unless they are migrated to the distributed switch. Select a destination port group to migrate them.

Host/VMkernel Network Adapters	In Use by Switch	Source Port Group	Destination Port Group
10.2.164.70			
On this switch			
vmk0 (Reassigned)	vSwitch0	Management Network	IB-Mgmt
On other switches			
vmk1	iScsiBootvSwitch	iScsiBootPG	Do not migrate
10.2.164.71			
On this switch			
vmk0 (Reassigned)	vSwitch0	Management Network	IB-Mgmt
On other switches			
vmk1	iScsiBootvSwitch	iScsiBootPG	Do not migrate

15. Click Next.

16. Click Next past Analyze impact.



Ready to complete

Review your settings selections before finishing the wizard.

Number of managed hosts

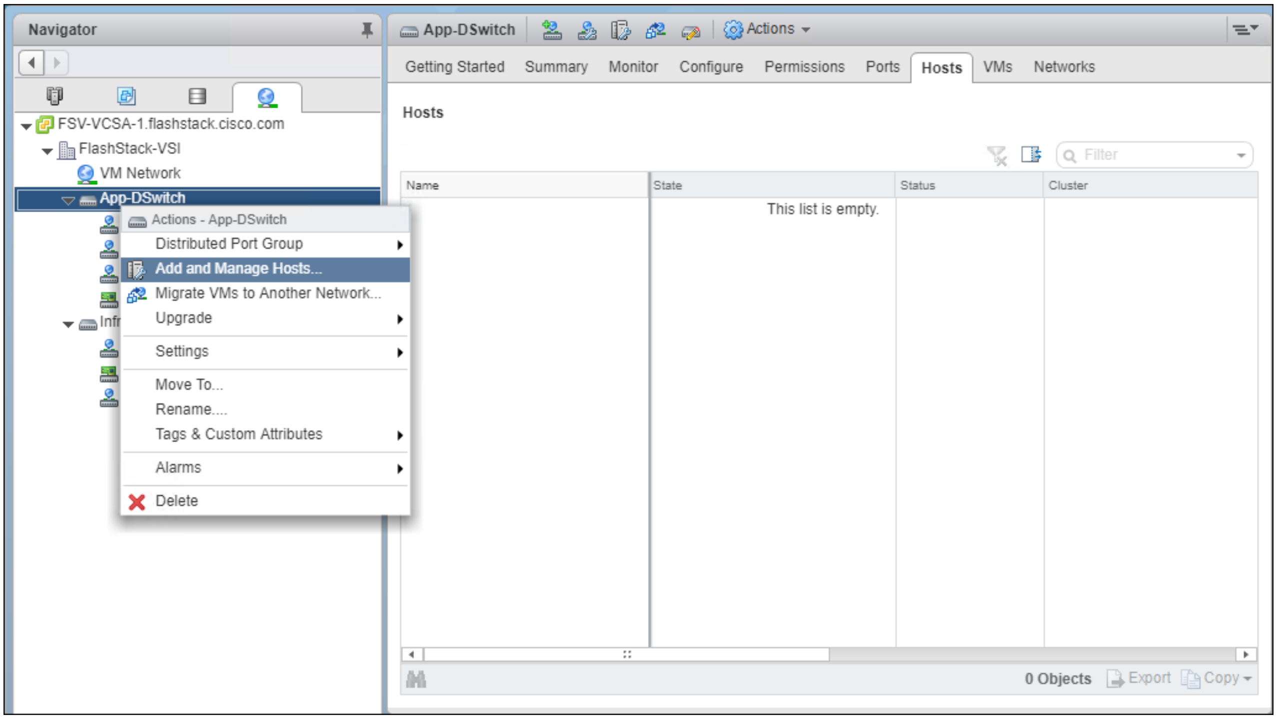
Hosts to add:	2

Number of network adapters for update

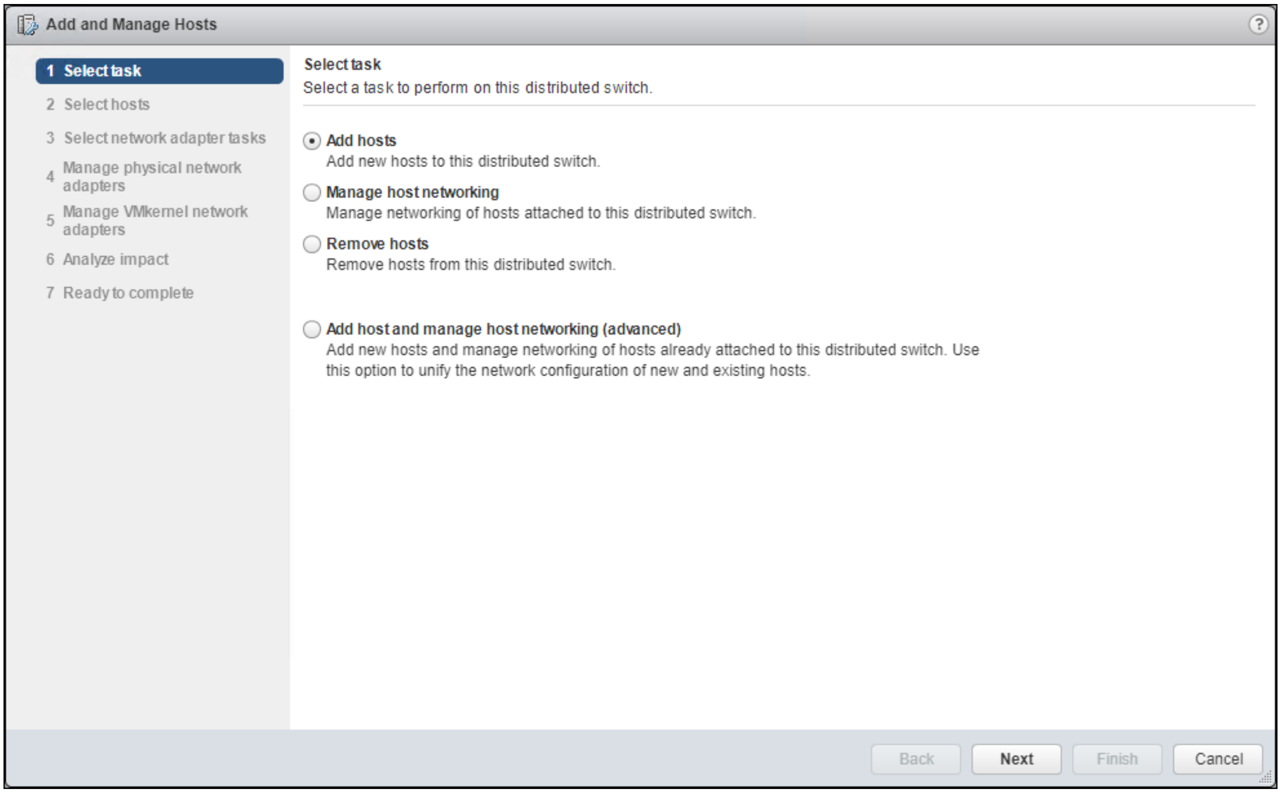
Physical network adapters:	8
Reassigned VMkernel network adapters:	2

17. Review the settings and click Finish to apply.

18. Within the Networking tab of the Navigator window, right-click the App-DSwitch vDS and select Add and Manage Hosts…



19. Leave Add hosts selected and click Next.


Add and Manage Hosts

1 Select task
2 Select hosts
3 Select network adapter tasks
4 Manage physical network adapters
5 Manage VMkernel network adapters
6 Analyze impact
7 Ready to complete

Select task
Select a task to perform on this distributed switch.

● **Add hosts**
Add new hosts to this distributed switch.

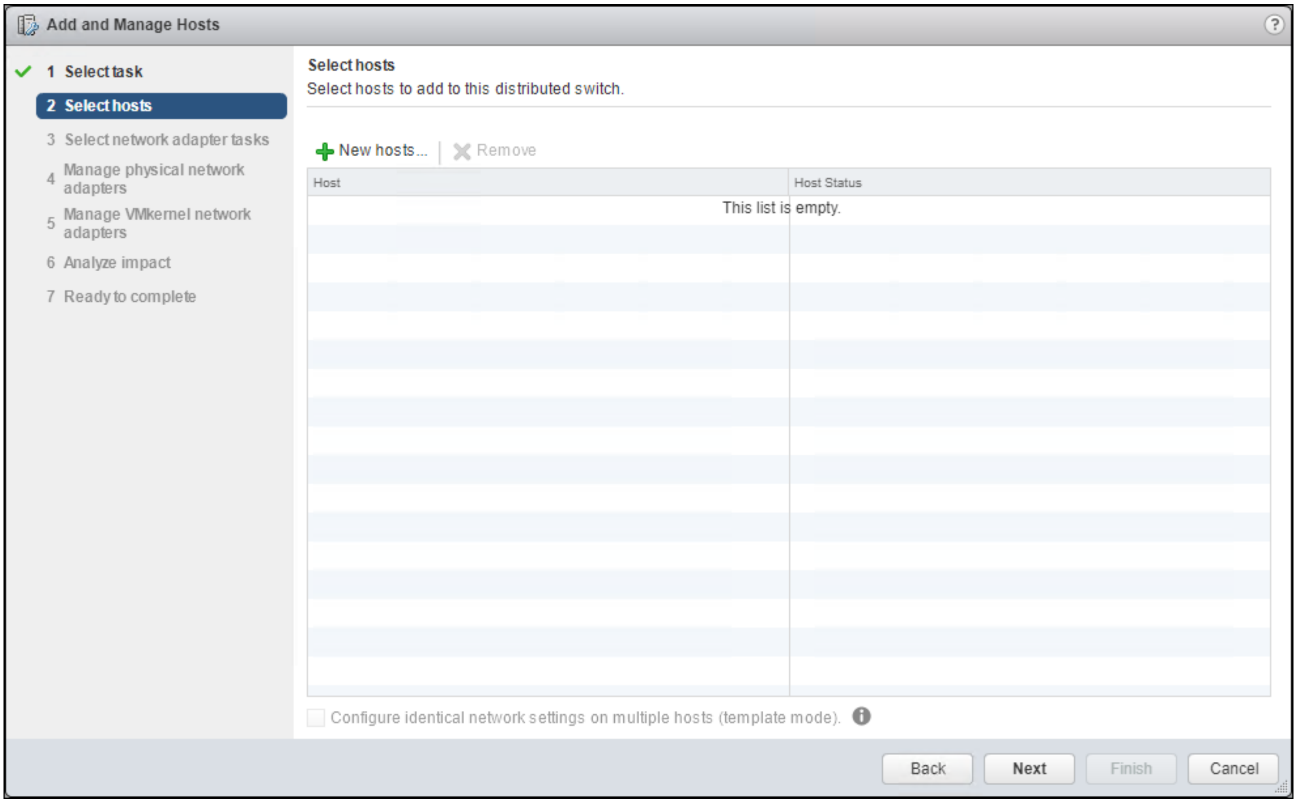
○ **Manage host networking**
Manage networking of hosts attached to this distributed switch.

○ **Remove hosts**
Remove hosts from this distributed switch.

○ **Add host and manage host networking (advanced)**
Add new hosts and manage networking of hosts already attached to this distributed switch. Use this option to unify the network configuration of new and existing hosts.

Back | Next | Finish | Cancel

20. Click the green + icon next to New hosts…



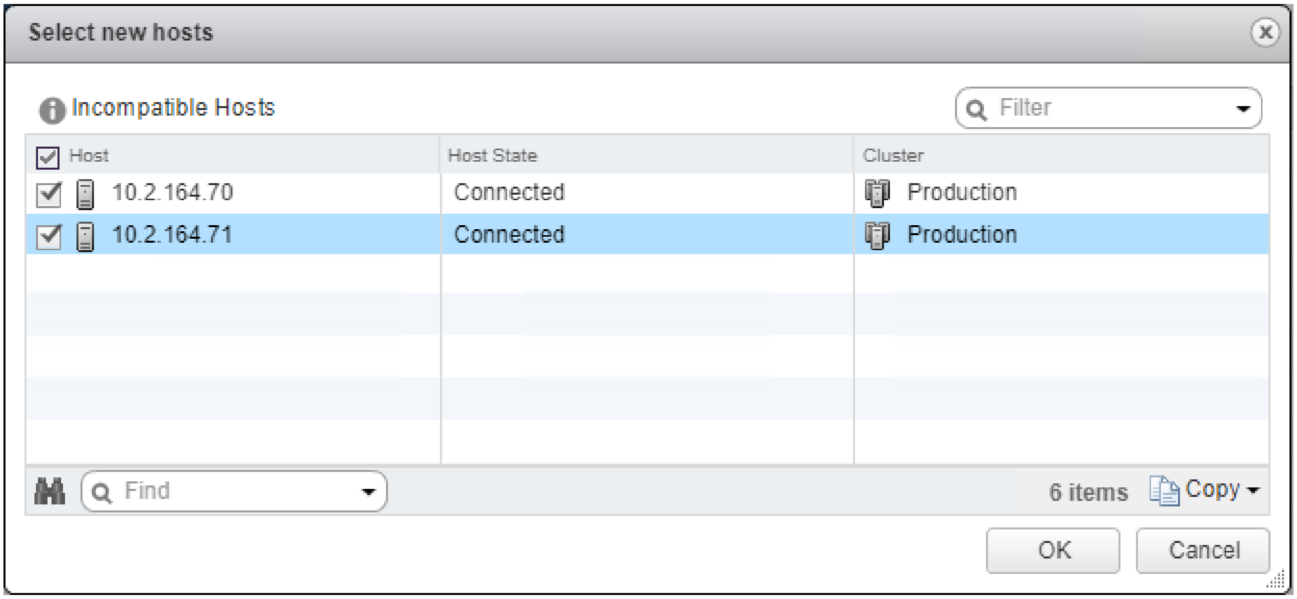
Select hosts

Select hosts to add to this distributed switch.

Host	Host Status
This list is empty.	

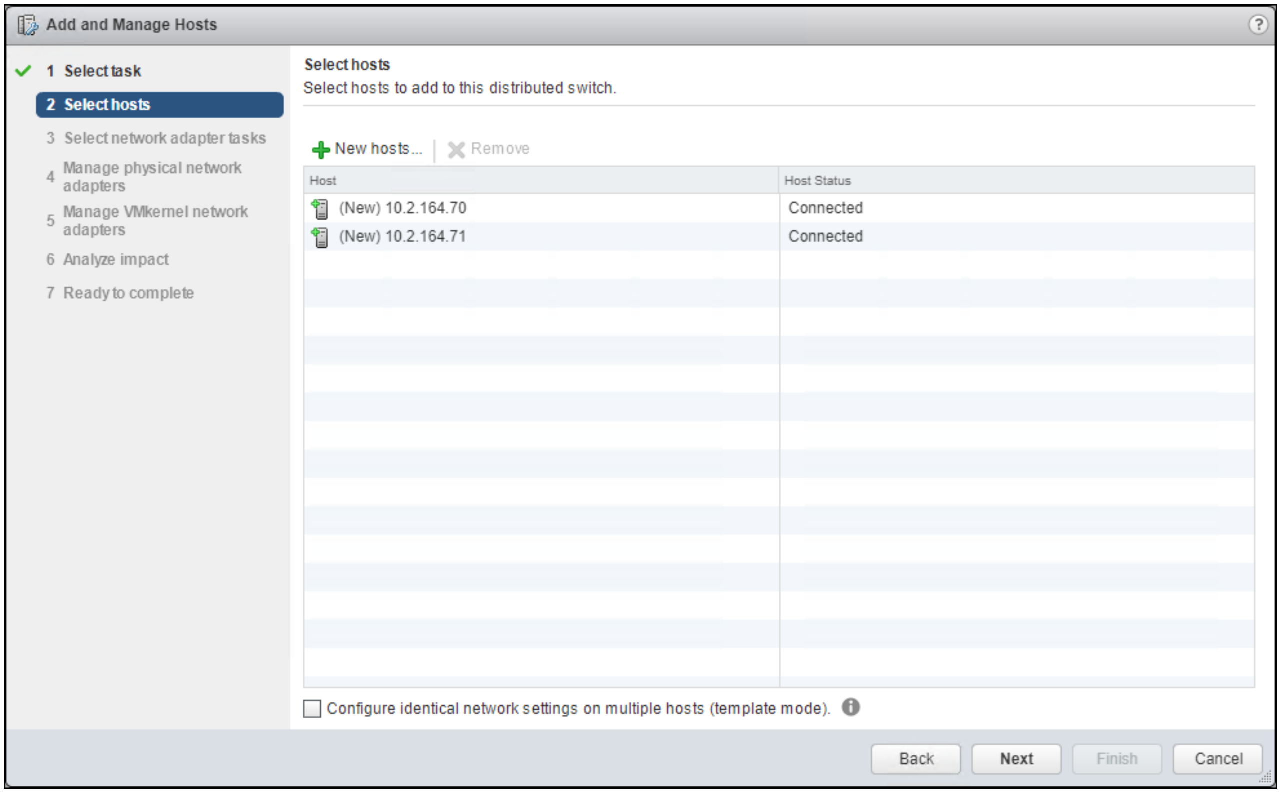
□ Configure identical network settings on multiple hosts (template mode).

21. In the Select new hosts pop-up that appears, select the hosts to be added, and click OK to begin joining them to the vDS.



☑ Host	Host State	Cluster
☑ 10.2.164.70	Connected	Production
☑ 10.2.164.71	Connected	Production

22. Click Next.



Add and Manage Hosts

- ✓ 1 Select task
- 2 Select hosts
- 3 Select network adapter tasks
- 4 Manage physical network adapters
- 5 Manage VMkernel network adapters
- 6 Analyze impact
- 7 Ready to complete

Select hosts

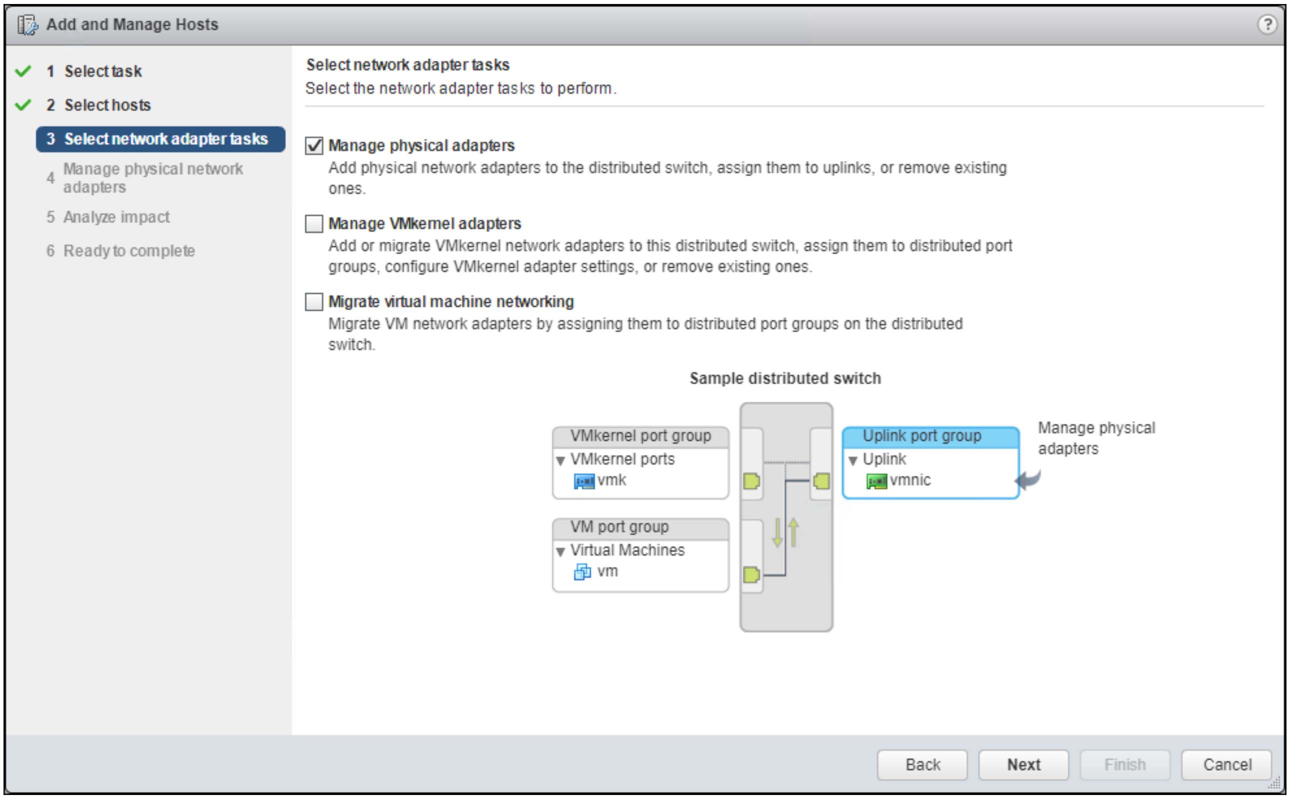
Select hosts to add to this distributed switch.

New hosts... | Remove

Host	Host Status
(New) 10.2.164.70	Connected
(New) 10.2.164.71	Connected

□ Configure identical network settings on multiple hosts (template mode).

23. Leave Manage physical adapters selected and unselect Manage VMkernel adapters.



Add and Manage Hosts

- ✓ 1 Select task
- ✓ 2 Select hosts
- 3 Select network adapter tasks
- 4 Manage physical network adapters
- 5 Analyze impact
- 6 Ready to complete

Select network adapter tasks

Select the network adapter tasks to perform.

☑ **Manage physical adapters**
Add physical network adapters to the distributed switch, assign them to uplinks, or remove existing ones.

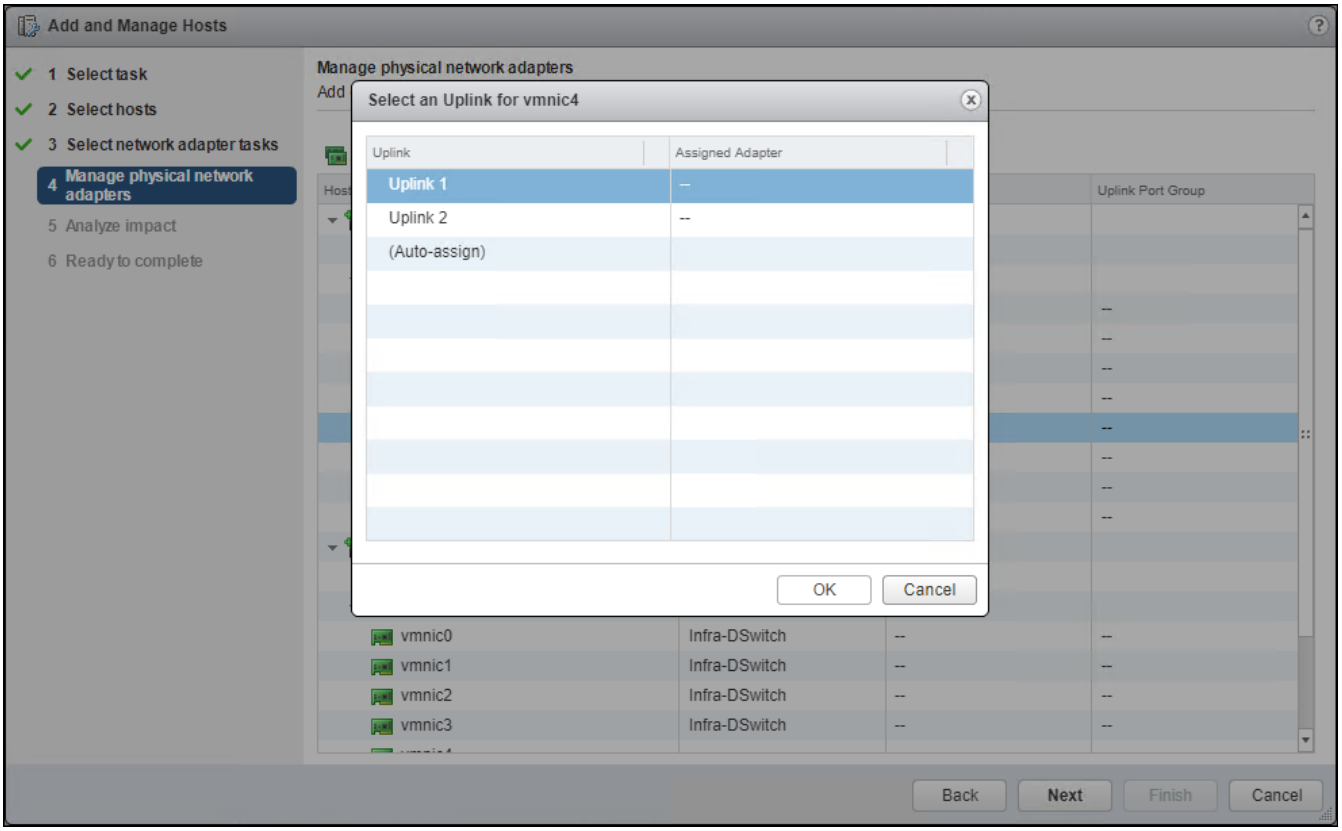
□ **Manage VMkernel adapters**
Add or migrate VMkernel network adapters to this distributed switch, assign them to distributed port groups, configure VMkernel adapter settings, or remove existing ones.

□ **Migrate virtual machine networking**
Migrate VM network adapters by assigning them to distributed port groups on the distributed switch.

Sample distributed switch

24. Click Next.

25. Select vmnic4 from the Host/Physical Network Adapters column and click the Assign uplink option.

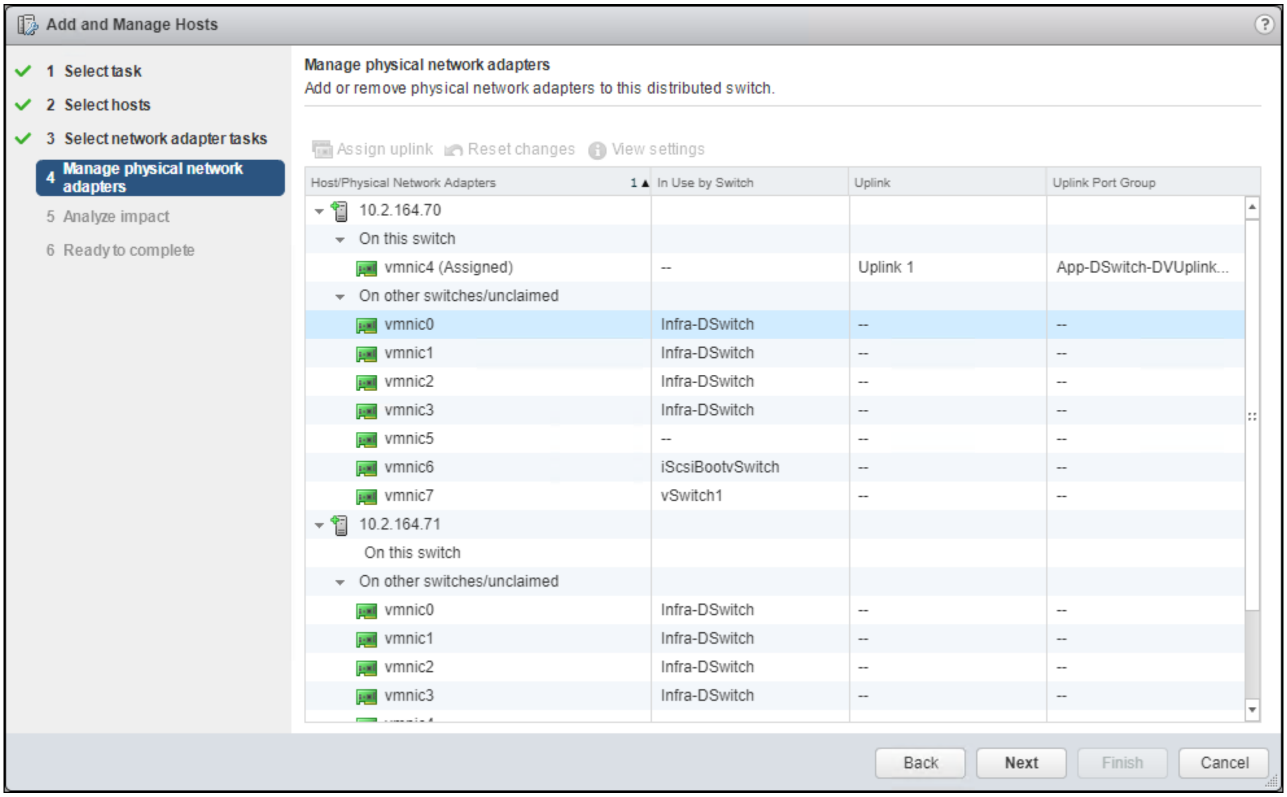


Select an Uplink for vmnic4

Uplink	Assigned Adapter
Uplink 1	--
Uplink 2	--
(Auto-assign)	

vmnic0	Infra-DSwitch	--	--
vmnic1	Infra-DSwitch	--	--
vmnic2	Infra-DSwitch	--	--
vmnic3	Infra-DSwitch	--	--

26. Leave Uplink 1 selected and click OK.



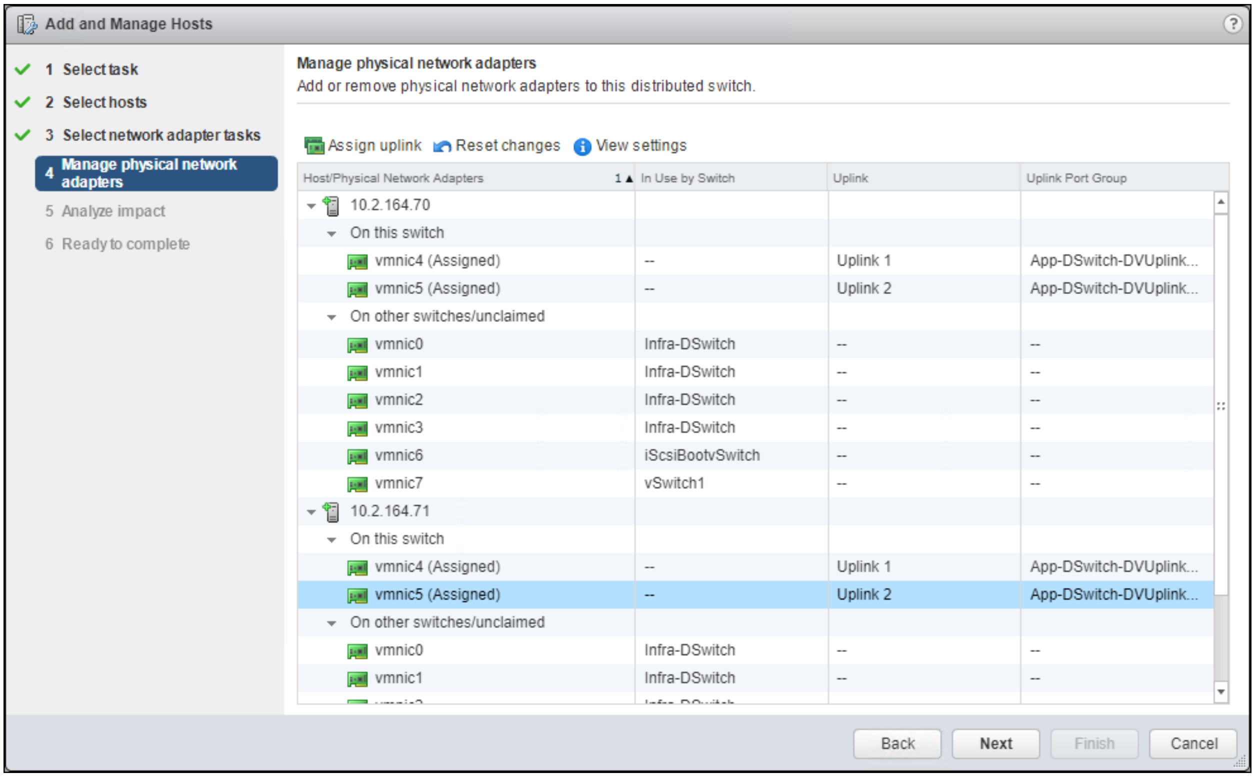
- ✓ 1 Select task
- ✓ 2 Select hosts
- ✓ 3 Select network adapter tasks
- 4 Manage physical network adapters
- 5 Analyze impact
- 6 Ready to complete

Manage physical network adapters

Add or remove physical network adapters to this distributed switch.

Host/Physical Network Adapters 1 ▲	In Use by Switch	Uplink	Uplink Port Group
10.2.164.70			
On this switch			
vmnic4 (Assigned)	--	Uplink 1	App-DSwitch-DVUplink...
On other switches/unclaimed			
vmnic0	Infra-DSwitch	--	--
vmnic1	Infra-DSwitch	--	--
vmnic2	Infra-DSwitch	--	--
vmnic3	Infra-DSwitch	--	--
vmnic5	--	--	--
vmnic6	iScsiBootvSwitch	--	--
vmnic7	vSwitch1	--	--
10.2.164.71			
On this switch			
On other switches/unclaimed			
vmnic0	Infra-DSwitch	--	--
vmnic1	Infra-DSwitch	--	--
vmnic2	Infra-DSwitch	--	--
vmnic3	Infra-DSwitch	--	--

27. Repeat this step for vmnic5, assigning it to uplink 2, then perform these same steps for vmnic4 and vmnic5 for all remaining ESXi hosts to be configured.



- ✓ 1 Select task
- ✓ 2 Select hosts
- ✓ 3 Select network adapter tasks
- 4 Manage physical network adapters
- 5 Analyze impact
- 6 Ready to complete

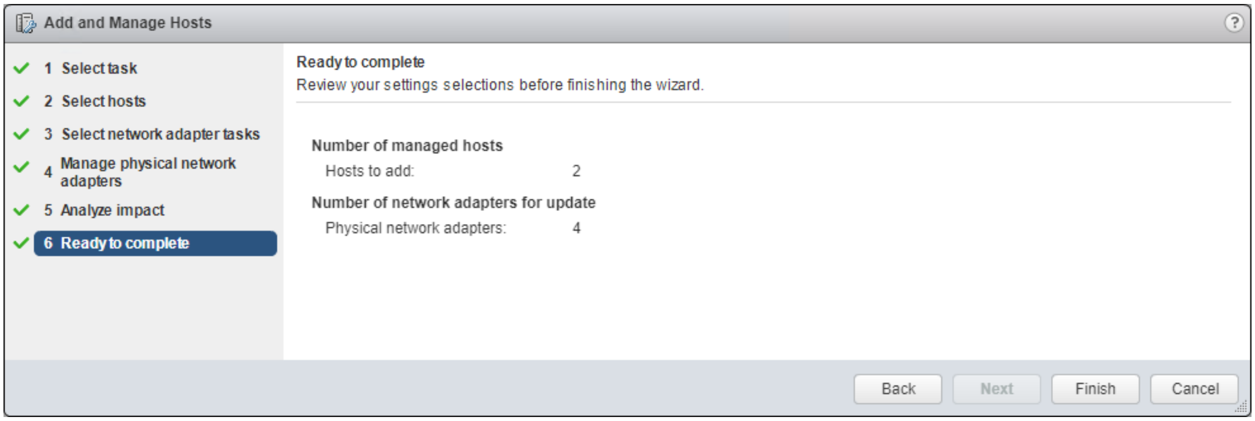
Manage physical network adapters

Add or remove physical network adapters to this distributed switch.

Host/Physical Network Adapters 1 ▲	In Use by Switch	Uplink	Uplink Port Group
10.2.164.70			
On this switch			
vmnic4 (Assigned)	--	Uplink 1	App-DSwitch-DVUplink...
vmnic5 (Assigned)	--	Uplink 2	App-DSwitch-DVUplink...
On other switches/unclaimed			
vmnic0	Infra-DSwitch	--	--
vmnic1	Infra-DSwitch	--	--
vmnic2	Infra-DSwitch	--	--
vmnic3	Infra-DSwitch	--	--
vmnic6	iScsiBootvSwitch	--	--
vmnic7	vSwitch1	--	--
10.2.164.71			
On this switch			
vmnic4 (Assigned)	--	Uplink 1	App-DSwitch-DVUplink...
vmnic5 (Assigned)	--	Uplink 2	App-DSwitch-DVUplink...
On other switches/unclaimed			
vmnic0	Infra-DSwitch	--	--
vmnic1	Infra-DSwitch	--	--

28. Click Next.

29. Click Next past Analyze impact.



Add and Manage Hosts

- ✓ 1 Select task
- ✓ 2 Select hosts
- ✓ 3 Select network adapter tasks
- ✓ 4 Manage physical network adapters
- ✓ 5 Analyze impact
- ✓ 6 Ready to complete

Ready to complete
Review your settings selections before finishing the wizard.

Number of managed hosts

Hosts to add:	2

Number of network adapters for update

Physical network adapters:	4

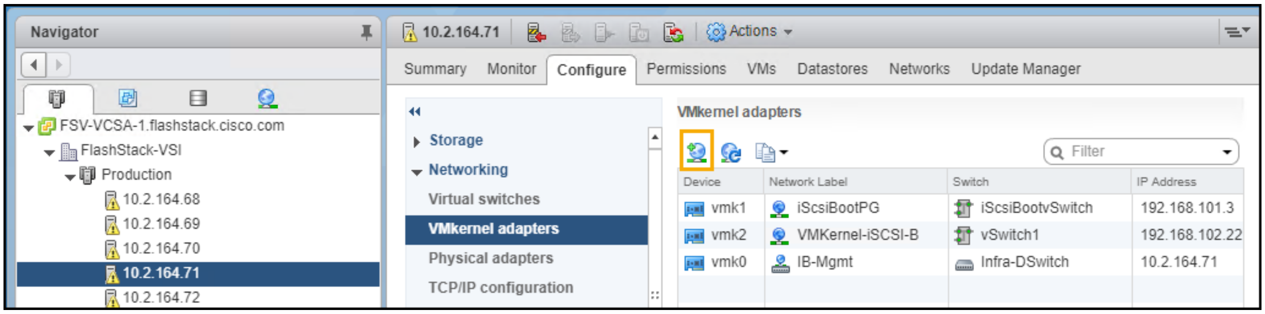
30. Review the settings and click Finish to apply.

Create vMotion VMkernel Adapters

A vMotion VMkernel adapter will be created for FlashStack infrastructure to keep vMotion traffic independent of management traffic. To create the vMotion VMkernel adapters, follow these steps:

1. From the Hosts and Clusters, drill down to the first host and select the Configure tab for that host.

2. Select the VMkernel adapters option within the Navigating section of Configure.



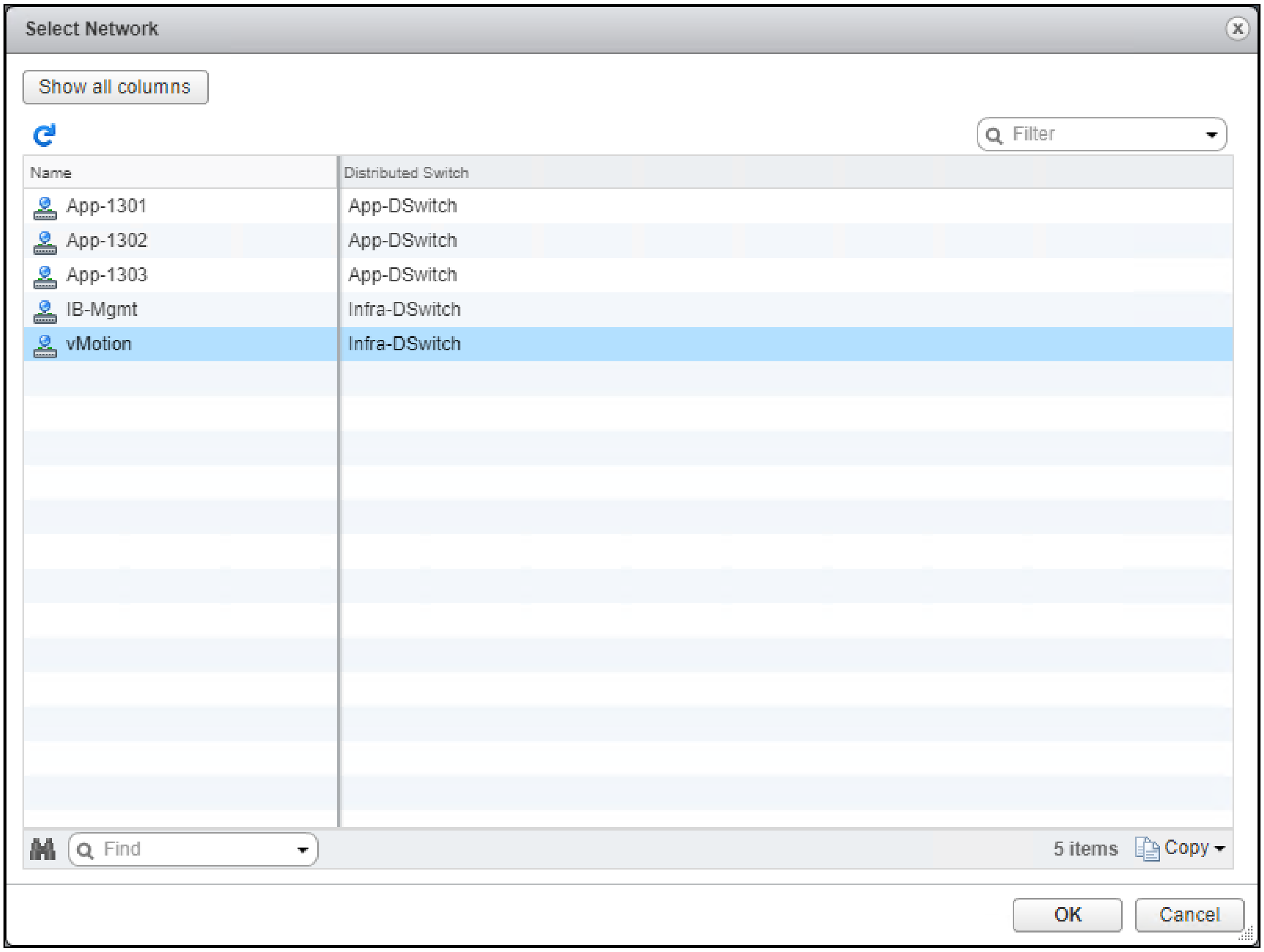
VMkernel adapters

Device	Network Label	Switch	IP Address
vmk1	iScsiBootPG	iScsiBootvSwitch	192.168.101.3
vmk2	VMKernel-iSCSI-B	vSwitch1	192.168.102.22
vmk0	IB-Mgmt	Infra-DSwitch	10.2.164.71

3. Click the first icon under VMkernel adapters to Add host networking.

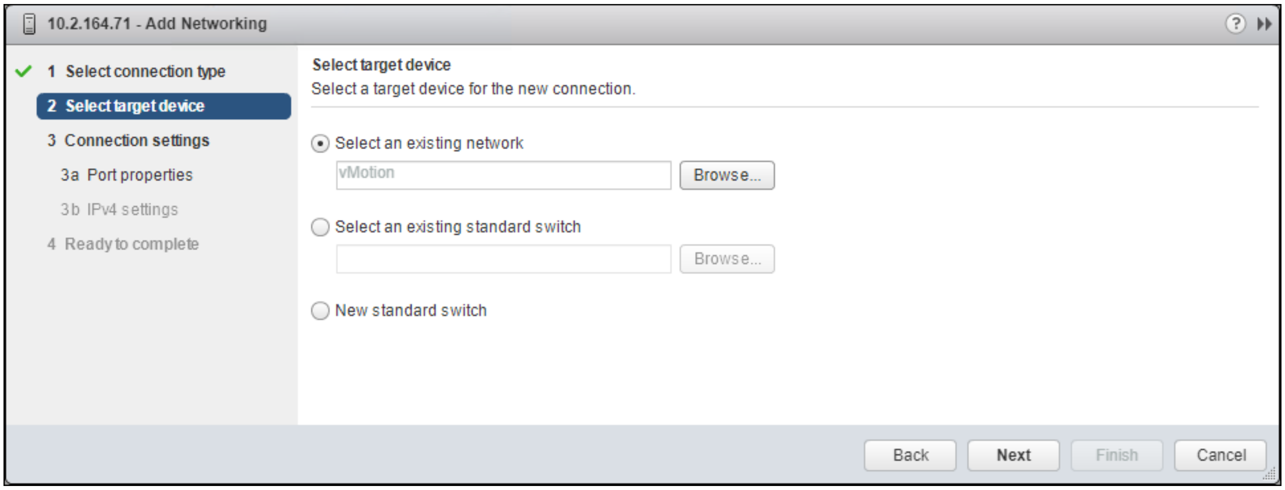
4. Leave the connection type selected as VMkernel Network Adapter and click Next.

5. Select Browse with Select an existing network selected.



Name	Distributed Switch
App-1301	App-DSwitch
App-1302	App-DSwitch
App-1303	App-DSwitch
IB-Mgmt	Infra-DSwitch
vMotion	Infra-DSwitch

6. Pick the vMotion network from the list shown and click OK.



Select target device

Select a target device for the new connection.

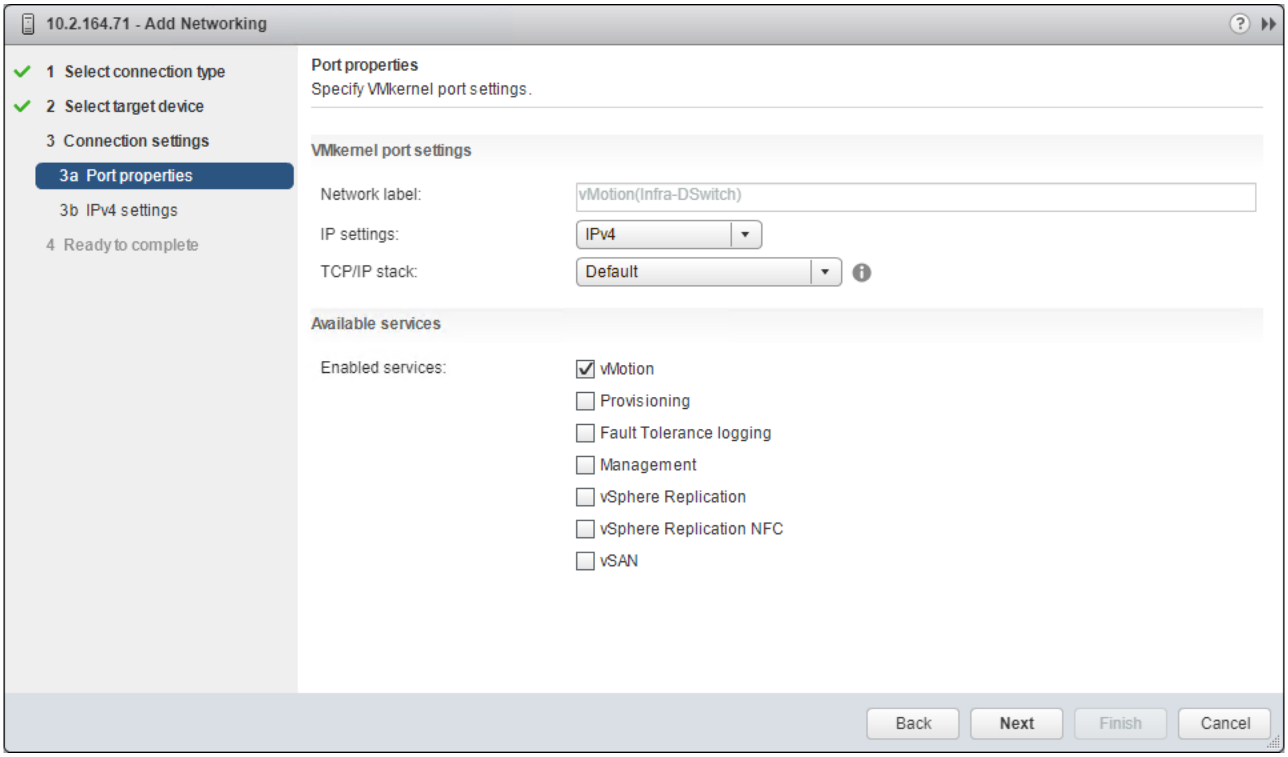
● Select an existing network

vMotion

○ Select an existing standard switch

○ New standard switch

7. Click Next.



Port properties

Specify VMkernel port settings.

VMkernel port settings

Network label: vMotion(Infra-DSwitch)

IP settings: IPv4

TCP/IP stack: Default

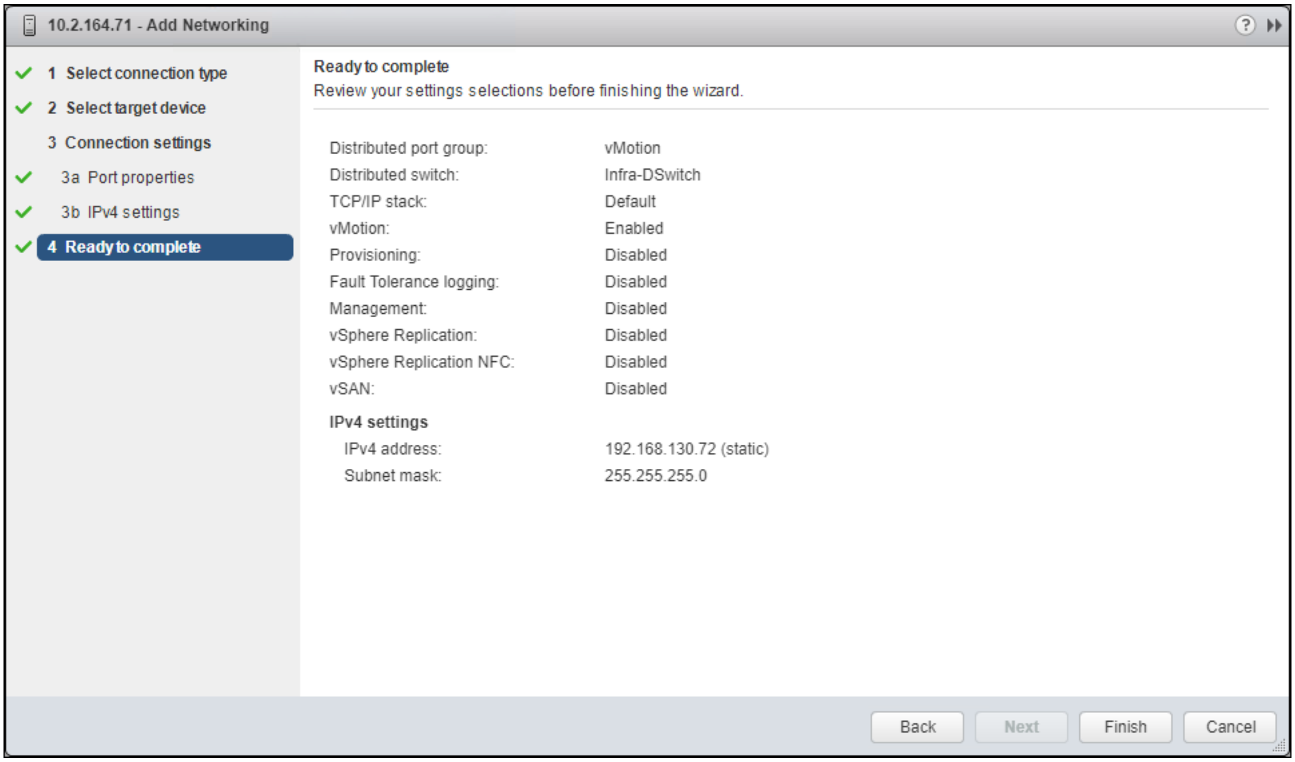
Available services

Enabled services:

- ☑ vMotion
- □ Provisioning
- □ Fault Tolerance logging
- □ Management
- □ vSphere Replication
- □ vSphere Replication NFC
- □ vSAN

8. Select the vMotion from the Available services and click Next.

9. Provide and IP address and subnet mask within the vMotion network. Click Next.



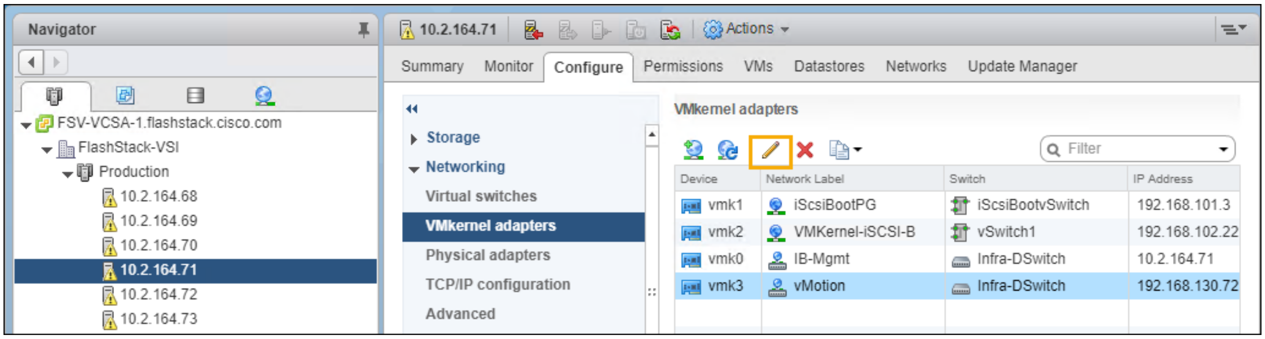
Ready to complete

Review your settings selections before finishing the wizard.

Distributed port group:	vMotion
Distributed switch:	Infra-DSwitch
TCP/IP stack:	Default
vMotion:	Enabled
Provisioning:	Disabled
Fault Tolerance logging:	Disabled
Management:	Disabled
vSphere Replication:	Disabled
vSphere Replication NFC:	Disabled
vSAN:	Disabled
IPv4 settings	
IPv4 address:	192.168.130.72 (static)
Subnet mask:	255.255.255.0

10. Review the settings and click Finish to create the VMkernel adapter.

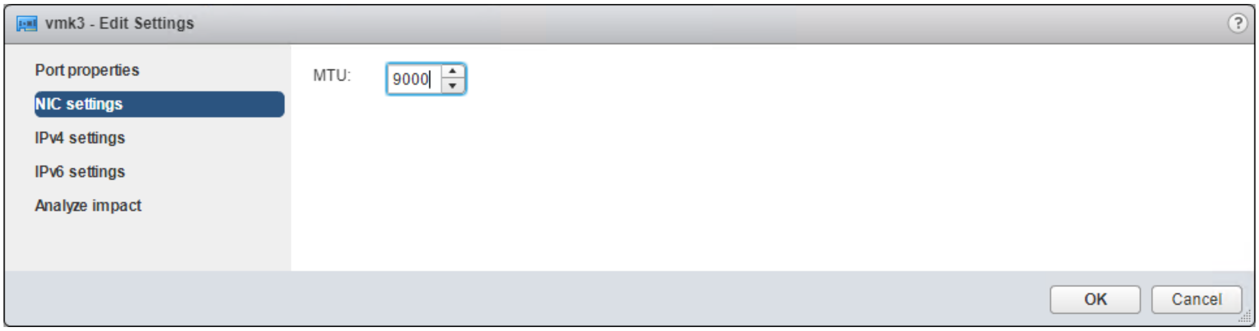
11. Select the newly created vMotion VMkernel adapter.



Device	Network Label	Switch	IP Address
vmk1	iScsiBootPG	iScsiBootvSwitch	192.168.101.3
vmk2	VMKernel-iSCSI-B	vSwitch1	192.168.102.22
vmk0	IB-Mgmt	Infra-DSwitch	10.2.164.71
vmk3	vMotion	Infra-DSwitch	192.168.130.72

12. Click the pencil icon to Edit settings for the VMkernel adapter.

13. Select the NIC Settings option and change the MTU from 1500 to 9000.



MTU: 9000

14. Click OK to save the changes.

15. Repeat these steps to create and adjust vMotion VMkernel adapters for each additional ESXi host.

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 not enabled by default on the vCenter Appliance. To setup the ESXi Dump Collector, follow these steps:

1. In the vSphere web client, select Home.

2. In the center pane, click System Configuration under the Administration section.

3. In the left pane, select Services.

4. Under services, click VMware vSphere ESXi Dump Collector.

5. In the center pane, click the green start icon to start the service.

6. In the Actions menu, click Edit Startup Type.

7. Select Automatic.

8. Click OK.

9. Connect to each ESXi host via ssh as root

10. Run the following commands:

```
esxcli system coredump network set –v vmk0 –j <vcenter-ip>
esxcli system coredump network set –e true
esxcli system coredump network check
```

Appendix

Sample Switch Configuration

```
switchname AA12-9336C-A
vdc AA12-9336C-A id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 511
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

cfs eth distribute
feature interface-vlan
feature lacp
feature vpc
feature lldp

ssh key rsa 2048
ip domain-lookup
system default switchport
copp profile strict
rmon event 1 description FATAL(1) owner PMON@FATAL
rmon event 2 description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 description ERROR(3) owner PMON@ERROR
rmon event 4 description WARNING(4) owner PMON@WARNING
rmon event 5 description INFORMATION(5) owner PMON@INFO
ntp server 172.26.163.254 use-vrf default
```

```
vlan 1,15,215,1110,1120,1130,1301-1303

vlan 15

  name pure-oob

vlan 215

  name Management

vlan 1110

  name iSCSI-A

vlan 1120

  name iSCSI-B

vlan 1130

  name vMotion

vlan 1301

  name VM-Apps-1

vlan 1302

  name VM-Apps-2

vlan 1303

  name VM-Apps-3


vrf context management

  ip route 0.0.0.0/0 10.2.164.254

vpc domain 10

  peer-keepalive destination 10.2.164.91




interface port-channel136

  switchport mode trunk

  switchport trunk allowed vlan 15,215,1301-1303

  mtu 9216

  vpc 136
```

```
interface port-channel133
  switchport mode trunk
  spanning-tree port type network
  vpc peer-link

interface port-channel129
  switchport mode trunk
  switchport trunk allowed vlan 215,1110,1130,1301-1303
  spanning-tree port type edge trunk
  mtu 9216
  vpc 129

interface port-channel130
  switchport mode trunk
  switchport trunk allowed vlan 215,1120,1130,1301-1303
  spanning-tree port type edge trunk
  mtu 9216
  vpc 130

interface Ethernet1/1

interface Ethernet1/2

interface Ethernet1/3

interface Ethernet1/4

interface Ethernet1/5

interface Ethernet1/6
interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16


interface Ethernet1/17
  switchport access vlan 1110
  spanning-tree port type edge
  mtu 9216

interface Ethernet1/18
  switchport access vlan 1110
  spanning-tree port type edge
  mtu 9216
```

```
interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28

interface Ethernet1/29
  description FSV-UCS-FI-A
  switchport mode trunk
  switchport trunk allowed vlan 215,1110,1130,1301-1303
  spanning-tree port type edge trunk
  mtu 9216
  channel-group 129 mode active

interface Ethernet1/30
  description FSV-UCS-FI-B
  switchport mode trunk
  switchport trunk allowed vlan 215,1120,1130,1301-1303
  mtu 9216
  channel-group 130 mode active

interface Ethernet1/31

interface Ethernet1/32

interface Ethernet1/33
  switchport mode trunk
  channel-group 133 mode active

interface Ethernet1/34
  switchport mode trunk
  channel-group 133 mode active

interface Ethernet1/35

interface Ethernet1/36
  switchport mode trunk
  switchport trunk allowed vlan 15,115,215,1301-1303
  mtu 9216
  channel-group 136 mode active

interface mgmt0
  vrf member management
  ip address 10.2.164.90/24
line console
line vty
boot nxos bootflash:/nxos.7.0.3.I7.3.bin
no system default switchport shutdown
```

About the Authors

Allen Clark, Technical Marketing Engineer, Cisco Systems, Inc.

Allen Clark has over 15 years of experience working with enterprise storage and data center technologies. As a member of various organizations within Cisco, Allen has worked with hundreds of customers on implementation and support of compute and storage products. Allen holds a bachelor's degree in Computer Science from North Carolina State University and is a dual Cisco Certified Internetwork Expert (CCIE 39519, Storage Networking and Data Center).

Acknowledgements

For their support and contribution to the design, validation, and creation of this Cisco Validated Design, the authors would like to thank:

- Ramesh Isaac, Technical Marketing Engineer, Cisco Systems, Inc.
- Haseeb Niazi, Technical Marketing Engineer, Cisco Systems, Inc.
- Craig Waters, Solutions Architecture / Product Management, Pure Storage Inc.
- Alex Carver, Solutions Architecture, Pure Storage Inc.