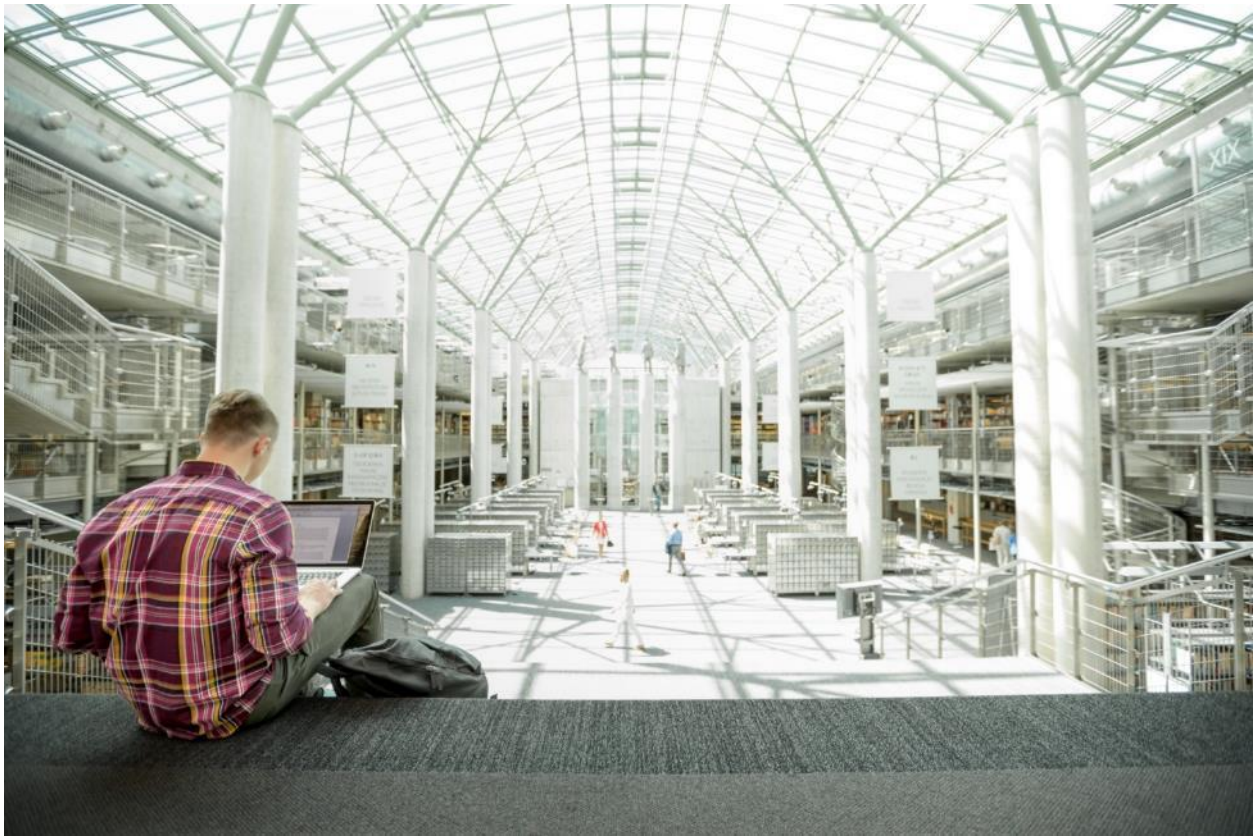


Cisco UCS® C220 M5 Rack Servers with ScaleProtect™

Deployment Guide for ScaleProtect with Cisco UCS C220 M5 Rack Servers and Commvault HyperScale Release 11 SP16

Last Updated: November 15, 2019

CISCO VALIDATED DESIGN

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.

Table of Contents

Executive Summary

Cisco Validated Designs (CVDs) deliver 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 the customers and to guide them from design to deployment. Cisco and Commvault have partnered to deliver a series of data protection solutions that provide customers with a new level of management simplicity and scale for managing secondary data on premises.

Secondary storage and their associated workloads account for the vast majority of storage today. Enterprises face increasing demands to store and protect data while addressing the need to find new value in these secondary storage locations as a means to drive key business and IT transformation initiatives. ScaleProtect™ with Cisco Unified Computing System (Cisco UCS) supports these initiatives by providing a unified modern data protection and management platform that delivers cloud-scalable services on-premises. The solution drives down costs across the enterprise by eliminating costly point solutions that do not scale and lack visibility into secondary data.

This CVD provides implementation details for the ScaleProtect with Cisco UCS solution, specifically focusing on the Cisco UCS C220 M5 Rack Server. ScaleProtect with Cisco UCS is deployed as a single cohesive system, which is made up of Commvault® Software and Cisco UCS infrastructure. Cisco UCS infrastructure provides the compute, storage, and networking, while Commvault Software provides the data protection and software designed scale-out platform.

Solution Overview

Introduction

ScaleProtect with Cisco UCS solution is a pre-designed, integrated, and validated architecture for modern data protection that combines Cisco UCS servers, Cisco Nexus switches, Commvault Complete™ Backup & Recovery, and Commvault HyperScale™ Software into a single software-defined scale-out flexible architecture. ScaleProtect with Cisco UCS is designed for high availability and resiliency, with no single point of failure, while maintaining cost-effectiveness and flexibility in design to support secondary storage workloads (for example; backup and recovery, disaster recovery, dev/test copies, and so on.).

ScaleProtect design discussed in this document has been validated for resiliency and fault tolerance during system upgrades, component failures, and partial as well as complete loss of power scenarios.

Audience

The audience for this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineers, IT architects, and customers who want to take advantage of an infrastructure that is built to deliver IT efficiency and enable IT innovation. The reader of this document is expected to have the necessary training and background to install and configure Cisco UCS, Cisco Nexus, and Cisco UCS Manager as well as a high-level understanding of Commvault Software and its components. External references are provided where applicable and it is recommended that the reader be familiar with these documents.

Purpose of this Document

This document provides step-by-step configuration and implementation guidelines for setting up ScaleProtect with Cisco UCS C220 M5 Solution.

The design that is implemented is discussed in detail in the ScaleProtect with Cisco UCS Design Guide found here:

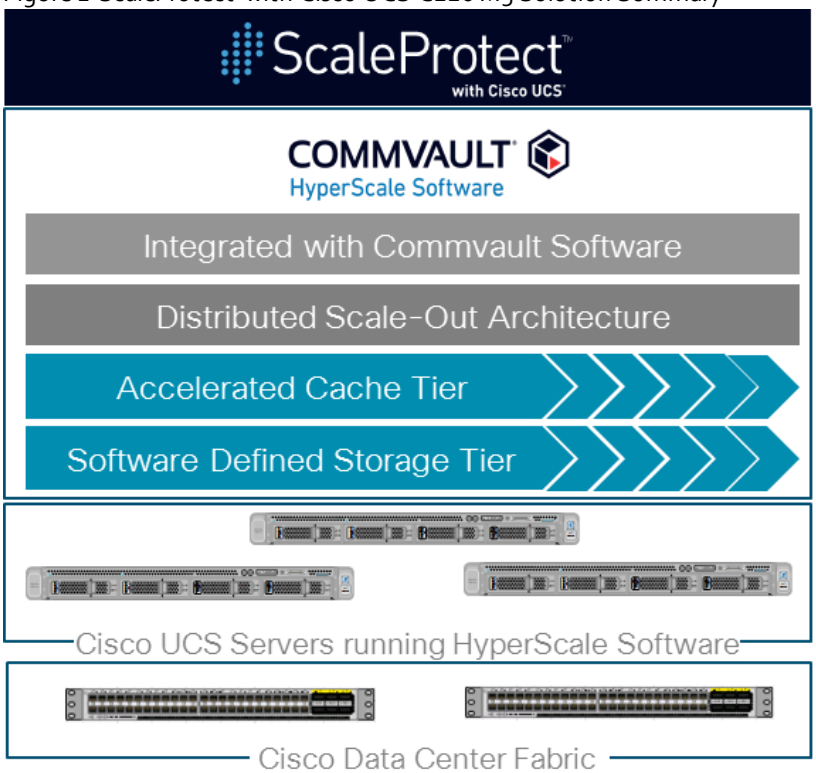
https://www.cisco.com/c/en/us/td/docs/unified_compting/ucs/UCS_CVDs/ucs_commvault_scaleprotect_designguide.html

Solution Summary

Cisco UCS revolutionized the server market through its programmable fabric and automated management that simplify application and service deployment. Commvault HyperScale™ Software provides the software-defined scale-out architecture that is fully integrated and includes true hybrid cloud capabilities. Commvault Complete Backup & Recovery provides a full suite of functionality for protecting, recovering, indexing, securing, automating, reporting, and natively accessing data. Cisco UCS, along with Commvault Software delivers an integrated software defined scale-out solution called ScaleProtect with Cisco UCS.

It is the only solution available with enterprise-class data management services that takes full advantage of industry-standard scale-out infrastructure together with Cisco UCS Servers.

Figure 1 ScaleProtect with Cisco UCS C220 M5 Solution Summary

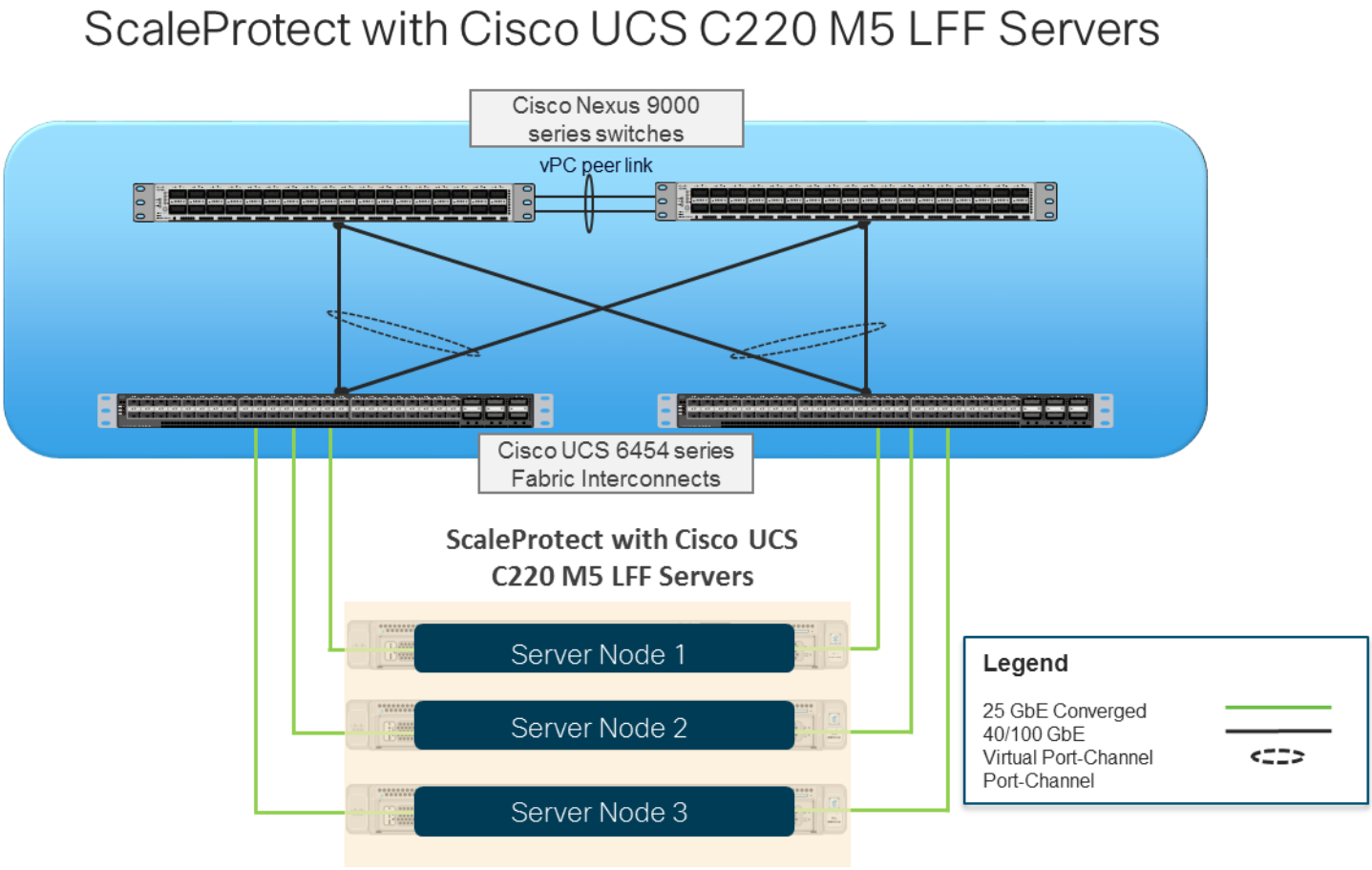


Architectural Overview

A typical ScaleProtect with Cisco UCS deployment starts with a 3-node block. The solution has been validated with three Cisco UCS C220 M5 Server Nodes with built-in storage that consists of 4 front-facing internal Large Form Factor (LFF) HDDs for the software defined data storage tier, rear-loaded NVMe PCIe SSD for the accelerated cache tier, and internal M.2 SATA SSD's for the operating system and associated binaries. Connectivity for the solution is provided via a pair of Cisco UCS 6454 Fabric Interconnects connected to a pair of Cisco Nexus 9336C-FX2 upstream network switches.

ScaleProtect with Cisco UCS can start with more than 3 nodes, the additional nodes are simply added to the Cisco UCS 6454 Series Fabric Interconnects for linear scalability.

Figure 2 3-Node ScaleProtect with Cisco UCS Physical Architecture



The validated configuration uses the following components for deployment:

- Cisco Unified Computing System (Cisco UCS)
  - Cisco UCS Manager
  - Cisco UCS 6454 Series Fabric Interconnects
  - Cisco UCS C220 M5 LFF Server
  - Cisco VIC 1457
  - Cisco Nexus 9336C-FX2 Series Switches
  - Commvault Complete™ Backup and Recovery v11
  - Commvault HyperScale Software release 11 SP16

Deployment Guidelines

This document guides customers through the low-level steps for deploying the ScaleProtect solution base architecture. These procedures describe everything from physical cabling to network, compute, and storage device configurations.

This document includes additional Cisco UCS configuration information that helps in enabling SAN connectivity to existing storage environment. The ScaleProtect design for this solution doesn't need SAN connectivity and additional information is included only as a reference and should be skipped if SAN connectivity is not required. All the sections that should be skipped for default design have been marked as optional.

Software Revisions

Table 1 lists the hardware and software versions used for the solution validation.

Table 1 Hardware and Software Revisions

Layer	Device	Image
Compute	Cisco UCS 6454 Series Fabric Interconnects	4.0(4b)
	Cisco UCS C220 M5 Rack Server	4.0(4b)
Network	Cisco Nexus 9336C-FX2 NX-OS	7.0(3)I7(6)
Software	Cisco UCS Manager	4.0(4b)
	Commvault Complete Backup and Recovery	v11 Service Pack 16
	Commvault HyperScale Software	v11 Service Pack 16

Configuration Guidelines

This document provides details for configuring a fully redundant, highly available ScaleProtect configuration. Therefore, appropriate references are provided to indicate the component being configured at each step, such as 01 and 02 or A and B. For example, the Cisco UCS fabric interconnects are identified as FI-A or FI-B. 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 Cisco Nexus switches:

Nexus-9000-A (config)# ntp server **<NTP Server IP Address>** use-vrf management

This document is intended to enable customers and partners to fully configure the customer environment and during this process, various steps may require the use of customer-specific naming conventions, IP addresses, and VLAN schemes, as well as appropriate MAC addresses etc.

This document details network (Cisco Nexus), compute (Cisco UCS), software (Commvault) and related storage configurations.

Table 2 and Table 3 lists various VLANs, VSANs and subnets used to setup ScaleProtect infrastructure to provide connectivity between core elements of the design.

Table 2 ScaleProtect VLAN Configuration

VLAN Name	VLAN	VLAN Purpose	Example Subnet
Out of Band Mgmt	11	VLAN for out-of-band management	192.168.160.0/22
SP-Data-VLAN	111	VLAN for data protection and management network	192.168.20.0/24
SP-Cluster-VLAN	3000	VLAN for ScaleProtect Cluster internal network	10.10.10.0/24
Native-VLAN	2	Native VLAN	

VSAN ids are optional and are only required if SAN connectivity is needed from the ScaleProtect Cluster to existing Tape Library or SAN fabrics.

Table 3 Optional: ScaleProtect VSAN Configuration

VSAN Name	VSAN	VSAN Purpose
Backup-VSAN-A	201	Fabric-A VSAN for connectivity to data protection devices.
Backup-VSAN-B	202	Fabric-B VSAN for connectivity to data protection devices.
Prod-VSAN-A	101	Fabric-A VSAN for connectivity to production SAN Fabrics.
Prod-VSAN-B	102	Fabric-B VSAN for connectivity to production SAN Fabrics.

Physical Infrastructure

The information in this section is provided as a reference for cabling the equipment in ScaleProtect environment.

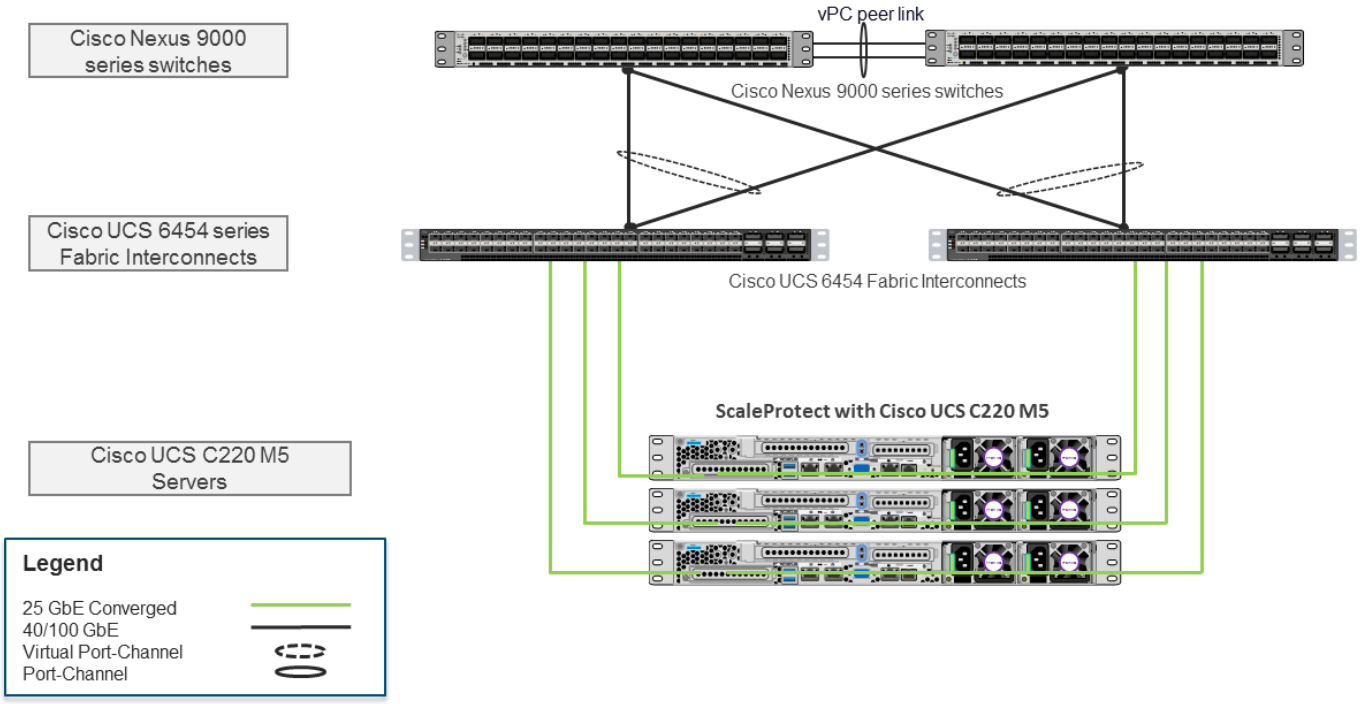
This document assumes that the out-of-band management ports are plugged into an existing management infrastructure at the deployment site. These interfaces will be used in various configuration steps.

Customers can choose interfaces and ports of their liking but failure to follow the exact connectivity shown in figures below will result in changes to the deployment procedures since specific port information is used in various configuration steps.

Cisco UCS Connectivity to Nexus Switches

For physical connectivity details of Cisco UCS to the Cisco Nexus switches, refer to Figure 3.

Figure 3 Cisco UCS Connectivity to the Nexus Switches



Each Cisco UCS C220 M5 rack server in the design is redundantly connected to the managing fabric interconnects with at least one port connected to each FI to support converged traffic. Internally the Cisco UCS C220 M5 servers are equipped with a Cisco VIC 1457 network interface card (NIC) with quad 10/25 Gigabit Ethernet (GbE) ports. The Cisco VIC is installed in a modular LAN on motherboard (MLOM) slot. The standard practice for redundant connectivity is to connect port 1 of each server's VIC card to a numbered port on FI A, and port 3 of each server's VIC card to the same numbered port on FI B. The use of ports 1 and 3 are because ports 1 and 2 form an internal port-channel, as does ports 3 and 4. This allows an optional 4 cable connection method providing an effective 50GbE bandwidth to each fabric interconnect.

Table 4 Cisco UCS C220 Server Connectivity to Cisco UCS Fabric Interconnects

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect A	Eth1/17	25GbE	Cisco UCS C220 M5 LFF Server1	VIC Port 1
Cisco UCS Fabric Interconnect A	Eth1/18	25GbE	Cisco UCS C220 M5 LFF Server2	VIC Port 1
Cisco UCS Fabric Interconnect A	Eth1/19	25GbE	Cisco UCS C220 M5 LFF Server3	VIC Port 1
Cisco UCS Fabric Interconnect B	Eth1/17	25GbE	Cisco UCS C220 M5 LFF Server1	VIC Port 3
Cisco UCS Fabric Interconnect B	Eth1/18	25GbE	Cisco UCS C220 M5 LFF Server2	VIC Port 3
Cisco UCS Fabric Interconnect B	Eth1/19	25GbE	Cisco UCS C220 M5 LFF Server3	VIC Port 3

Table 5 Cisco UCS FI Connectivity to Nexus Switches

Local Device	Local Port	Connection	Remote Device	Remote Port

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect A	Eth1/49	40/100GbE	Cisco Nexus 9336C-FX2	Eth1/25
Cisco UCS Fabric Interconnect A	Eth1/50	40/100GbE	Cisco Nexus 9336C-FX2	Eth1/25
Cisco UCS Fabric Interconnect B	Eth1/49	40/100GbE	Cisco Nexus 9336C-FX2	Eth1/26
Cisco UCS Fabric Interconnect B	Eth1/50	40/100GbE	Cisco Nexus 9336C-FX2	Eth1/26

Optional: Cisco UCS connectivity to SAN Fabrics

For physical connectivity details of Cisco UCS to a Cisco MDS based redundant SAN fabric (MDS 9132T has been shown as an example), refer to Figure 4. Cisco UCS to SAN connectivity is optional and is not required for default ScaleProtect implementation. SAN connectivity details are included in the document as a reference which can be leveraged to connect ScaleProtect infrastructure to existing SAN fabrics in customers environment.

This document includes SAN configuration details for Cisco UCS but doesn't explain the Cisco MDS switch configuration details and end device configurations such as Storage Arrays or Tape Library's.

Figure 4 Cisco UCS Connectivity to Cisco MDS Switches

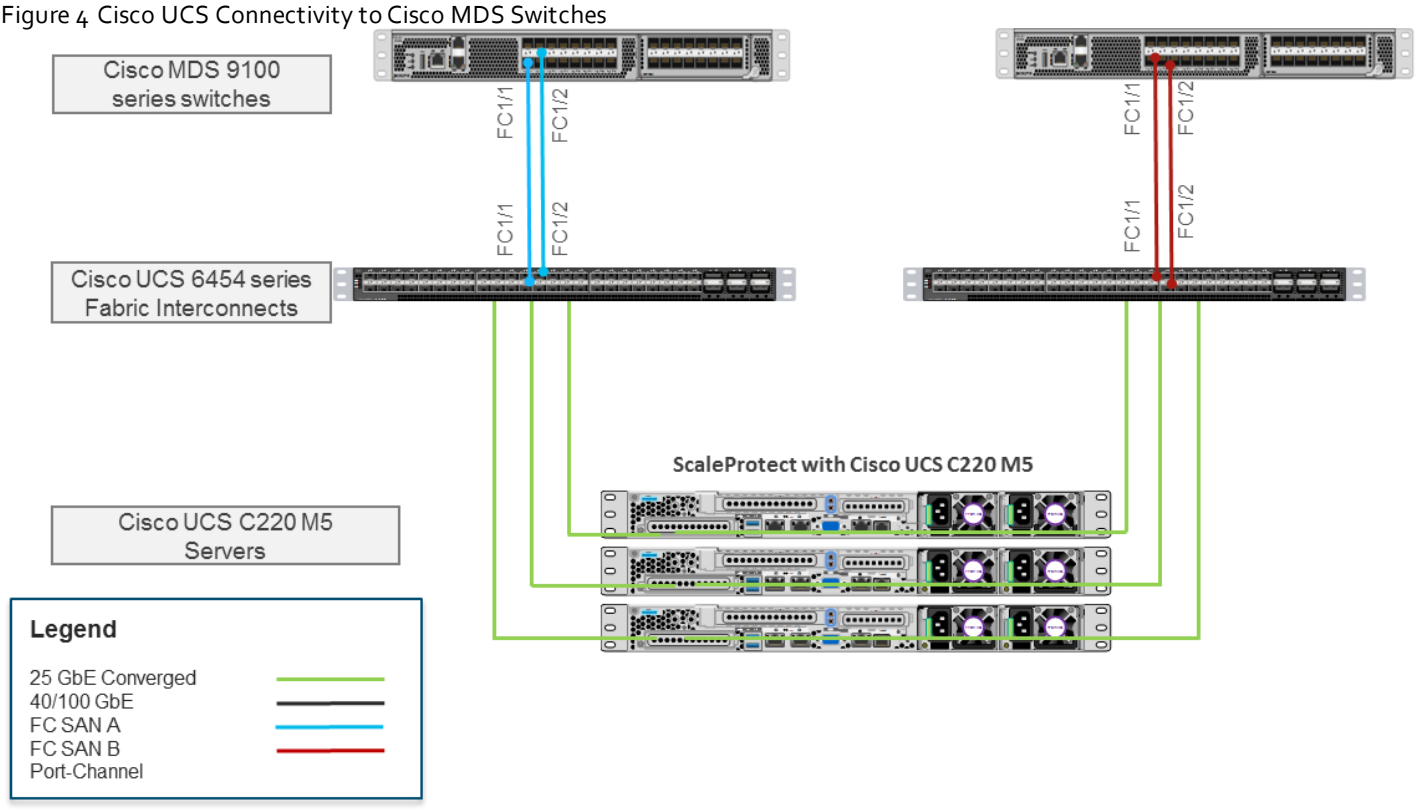


Table 6 Optional: Cisco UCS Connectivity to Cisco MDS Switches

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect A	FC1/1	32Gbps	Cisco MDS 9132T A	FC1/1

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect A	FC1/2	32Gbps	Cisco MDS 9132T A	FC1/2
Cisco UCS Fabric Interconnect B	FC1/1	32Gbps	Cisco MDS 9132T B	FC1/1
Cisco UCS Fabric Interconnect B	FC1/2	32Gbps	Cisco MDS 9132T B	FC1/2

Table 7 and Table 8 lists the hardware configuration and sizing options of Cisco UCS C220 M5 nodes for ScaleProtect Solution.

Table 7 Cisco UCS C220 M5 Server Node Configuration

Resources	Cisco UCS C220 M5 LFF
CPU	2x 2nd Gen Intel® Xeon® Scalable Silver 4214 52.8GHz (24 Cores)
Memory	96GB DDR4
Storage	**Boot Drives**
	(2) 960GB SSD – RAID1
	Accelerated Cache Tier
	(1) 1.6TB NVMe
	Software Defined Data Storage Tier
	(4) 4/6/8/10/12TB HDD
Storage Controller	SAS 12G RAID
Network	(2/4) 25Gbps

Table 8 ScaleProtect with Cisco UCS C220 M5 Solution Sizing

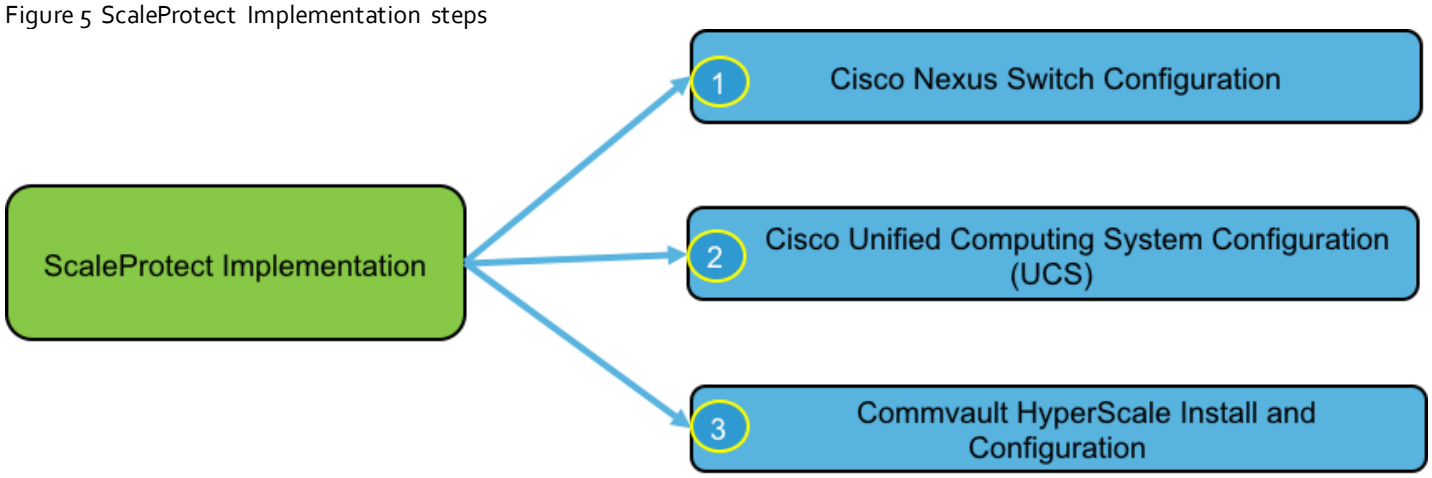
Cisco UCS Model	HDD Size[1]	3 Node Usable[2]	6 Node Usable[2]	9 Node Usable[2]	12 Node Usable[2]	15 Node Usable[2]
Cisco UCS C220 M5 (4 Drives per node)	4 TB	29 TiB	58 TiB	87 TiB	116 TiB	145 TiB
	6 TB	44 TiB	88 TiB	132 TiB	176 TiB	220 TiB
	8 TB	58 TiB	116 TiB	174 TiB	232 TiB	290 TiB
	10 TB	72 TiB	144 TiB	222 TiB	296 TiB	370 TiB
	12 TB	87 TiB	174 TiB	261 TiB	348 TiB	435 TiB

1. HDD capacity values are calculated using Base10 (e.g. 1TB = 1,000,000,000,000 bytes)
2. Usable capacity values are calculated using Base2 (e.g. 1TiB = 1,099,511,627,776 bytes), post erasure coding

ScaleProtect Implementation

Figure 5 illustrates the ScaleProtect implementation workflow which is explained in the following sections of this document.

Figure 5 ScaleProtect Implementation steps



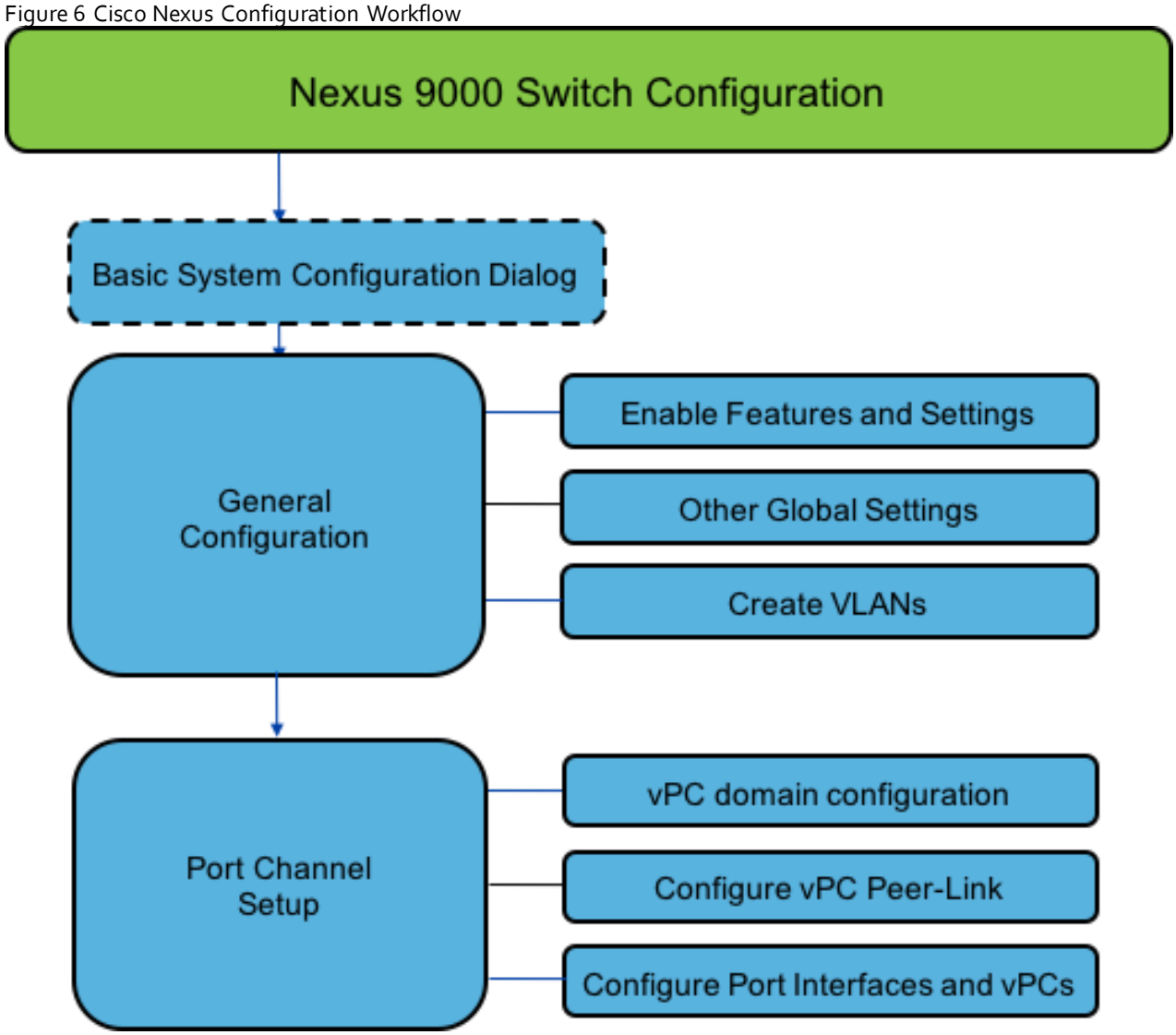
Network Switch Configuration

This section provides detailed steps to configure the Cisco Nexus 9000 switches used in this ScaleProtect environment. 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.

For detailed configuration details, refer to the Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide.

Any Cisco Nexus 9k switches can be used in the deployment based on the bandwidth requirements. However, be aware that there may be slight differences in setup and configuration based on the switch used. The switch model also dictates the connectivity options between the devices including the bandwidth supported, transceiver and cable types required.

Figure 6 Cisco Nexus Configuration Workflow



Cisco Nexus 9000 Initial Configuration Setup

This section describes how to configure the Cisco Nexus switches to use in a ScaleProtect environment. This procedure assumes that you are using Cisco Nexus 9000 switches running 7.0(3)I7(6) code.

Cisco Nexus 9000 A

To set up the initial configuration for the Cisco Nexus A switch, follow these steps:

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

1. Configure the switch.

```
Abort Power On Auto Provisioning [yes - continue with normal setup, skip - bypass password and basic
configuration, no - continue with Power On Auto Provisioning] (yes/skip/no)[no]: yes

Disabling POAP.......Disabling POAP

poap: Rolling back, please wait... (This may take 5-15 minutes)

         ---- System Admin Account Setup ----

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

Enter the password for "admin": <Switch Password>

Confirm the password for "admin": <Switch Password>

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

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

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

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

Enter the switch name: <Name of the Switch A>

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

Mgmt0 IPv4 address: <Mgmt. IP address for Switch A>

Mgmt0 IPv4 netmask: <Mgmt. IP Subnet Mask>

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

IPv4 address of the default gateway: <Default GW for the Mgmt. IP>

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

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

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

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

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

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

NTP server IPv4 address: <NTP Server IP Address>

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

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

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

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

2. Review the configuration summary before enabling the configuration.

Cisco Nexus 9000 B

To set up the initial configuration for the Cisco Nexus B switch, follow these steps:

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

1. Configure the switch.

```
Abort Power On Auto Provisioning [yes - continue with normal setup, skip - bypass password and basic
configuration, no - continue with Power On Auto Provisioning] (yes/skip/no)[no]: yes

Disabling POAP.......Disabling POAP

poap: Rolling back, please wait... (This may take 5-15 minutes)

         ---- System Admin Account Setup ----

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

Enter the password for "admin": <Switch Password>

Confirm the password for "admin": <Switch Password>

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

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

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

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

Enter the switch name: <Name of the Switch B>

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

Mgmt0 IPv4 address: <Mgmt. IP address for Switch B>

Mgmt0 IPv4 netmask: <Mgmt. IP Subnet Mask>

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

IPv4 address of the default gateway: <Default GW for the Mgmt. IP>

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

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

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

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

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

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

NTP server IPv4 address: <NTP Server IP Address>
```

```
Configure default interface layer (L3/L2) [L2]: Enter
Configure default switchport interface state (shut/noshut) [noshut]: shut
Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]: Enter
Would you like to edit the configuration? (yes/no) [n]: Enter
```

2. Review the configuration summary before enabling the configuration.

Enable Appropriate Cisco Nexus 9000 Features and Settings

Cisco Nexus 9000 A and Cisco Nexus 9000 B

To enable the IP switching feature and set default spanning tree behaviors, follow these steps:

1. On each Nexus 9000, enter the configuration mode:

```
config terminal
```

2. Use the following commands to enable the necessary features:

```
feature lacp
feature vpc
feature interface-vlan
feature udld
feature lacp
feature nxapi
```

3. Configure the spanning tree and save the running configuration to start-up:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
port-channel load-balance src-dst l4port

copy run start
```

Create VLANs for ScaleProtect IP Traffic

Cisco Nexus 9000 A and Cisco Nexus 9000 B

To create the necessary virtual local area networks (VLANs), follow these steps on both switches:

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

```
vlan <ScaleProtect-Data VLAN id>
name SP-Data-VLAN
```

```
exit
vlan <ScaleProtect-Cluster VLAN id>
name SP-Cluster-VLAN
exit
vlan <Native VLAN id>>
name Native-VLAN
exit
copy run start
```

Configure Virtual Port Channel Domain

Cisco Nexus 9000 A

To configure vPC domain for switch A, follow these steps:

1. From the global configuration mode, create a new vPC domain:

```
vpc domain 10
```

2. Make the Nexus 9000A the primary vPC peer by defining a low priority value:

```
 role priority 10
```

3. Use the management interfaces on the supervisors of the Nexus 9000s to establish a keepalive link:

```
peer-keepalive destination <Mgmt. IP address for Switch B> source <Mgmt. IP address for Switch A>
```

4. Enable the following features for this vPC domain:

```
peer-switch
delay restore 150
peer-gateway
ip arp synchronize
auto-recovery
copy run start
```

Cisco Nexus 9000 B

To configure the vPC domain for switch B, follow these steps:

1. From the global configuration mode, create a new vPC domain:

```
vpc domain 10
```

2. Make the Nexus 9000A the primary vPC peer by defining a low priority value:

```
role priority 20
```

3. Use the management interfaces on the supervisors of the Nexus 9000s to establish a keepalive link:

```
peer-keepalive destination <Mgmt. IP address for Switch A> source <Mgmt. IP address for Switch B>
```

4. Enable the following features for this vPC domain:

```
peer-switch
delay restore 150
peer-gateway
ip arp synchronize
auto-recovery
copy run start
```

Configure Network Interfaces for the vPC Peer Links

To configure the network interfaces for the vPC Peer links, follow these steps:

Cisco Nexus 9000 A

1. Define a port description for the interfaces connecting to vPC Peer <Nexus Switch B>>.

```
interface Eth1/27
description VPC Peer <Nexus-B Switch Name>:1/27
interface Eth1/28
description VPC Peer <Nexus-B Switch Name>:1/28
```

2. Apply a port channel to both vPC Peer links and bring up the interfaces.

```
interface Eth1/27,Eth1/28
channel-group 10 mode active
no shutdown
```

3. Define a description for the port-channel connecting to <Nexus Switch B>.

```
interface Po10
description vPC peer-link
```

4. Make the port-channel a switchport, and configure a trunk to allow Data, Cluster and the native VLAN.

```
switchport
switchport mode trunk
switchport trunk native vlan <Native VLAN id>
```

```
switchport trunk allowed vlan <ScaleProtect-Data VLAN id> <ScaleProtect-Cluster VLAN id>
spanning-tree port type network
```

5. Make this port-channel the VPC peer link and bring it up.

```
vpc peer-link
no shutdown
copy run start
```

Cisco Nexus 9000 B

1. Define a port description for the interfaces connecting to VPC Peer <Nexus Switch A>.

```
interface Eth1/27
description VPC Peer <Nexus-A Switch Name>:1/27
interface Eth1/28
description VPC Peer <Nexus-A Switch Name>:1/28
```

2. Apply a port channel to both VPC Peer links and bring up the interfaces.

```
interface Eth1/27,Eth1/28
channel-group 10 mode active
no shutdown
```

3. Define a description for the port-channel connecting to <Nexus Switch A>.

```
interface Po10
description vPC peer-link
```

4. Make the port-channel a switchport, and configure a trunk to allow Data, Cluster and the native VLAN.

```
switchport
switchport mode trunk
switchport trunk native vlan <Native VLAN id>
switchport trunk allowed vlan <ScaleProtect-Data VLAN id> <ScaleProtect-Cluster VLAN id>
spanning-tree port type network
```

5. Make this port-channel the VPC peer link and bring it up.

```
vpc peer-link no shutdown
copy run start
```

Configure Network Interfaces to Cisco UCS Fabric Interconnect

Cisco Nexus 9000 A

1. Define a description for the port-channel connecting to <<UCS Cluster Name>>-A.

```
interface Po40
description <UCS Cluster Name>-A
```

2. Make the port-channel a switchport and configure a trunk to allow ScaleProtect Data, ScaleProtect Cluster and the native VLANs.

```
switchport
switchport mode trunk
switchport trunk native vlan <Native VLAN id>
switchport trunk allowed vlan <ScaleProtect-Data VLAN id> <ScaleProtect-Cluster VLAN id>
```

3. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

4. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

5. Make this a VPC port-channel and bring it up.

```
vpc 40
no shutdown
```

6. Define a port description for the interface connecting to <UCS Cluster Name>-A.

```
interface Eth1/25
description <UCS Cluster Name>-A:49
```

7. Apply it to a port channel and bring up the interface.

```
channel-group 40 force mode active
no shutdown
```

8. Define a description for the port-channel connecting to <UCS Cluster Name>-B.

```
interface Po50
description <UCS Cluster Name>-B
```

9. Make the port-channel a switchport and configure a trunk to ScaleProtect Data, ScaleProtect Cluster and the native VLANs.

```
switchport
switchport mode trunk
switchport trunk native vlan <Native VLAN id>
switchport trunk allowed vlan <ScaleProtect-Data VLAN id> <ScaleProtect-Cluster VLAN id>
```

10. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

11. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

12. Make this a VPC port-channel and bring it up.

```
vpc 50
no shutdown
```

13. Define a port description for the interface connecting to <UCS Cluster Name>-B.

```
interface Eth1/26
description <UCS Cluster Name>-B:1/49
```

14. Apply it to a port channel and bring up the interface.

```
channel-group 50 force mode active
no shutdown
copy run start
```

Cisco Nexus 9000 B

1. Define a description for the port-channel connecting to <UCS Cluster Name>-B.

```
interface Po40
description <UCS Cluster Name>-A
```

2. Make the port-channel a switchport and configure a trunk to allow ScaleProtect Data, ScaleProtect Cluster and the native VLANs.

```
switchport
switchport mode trunk
switchport trunk native vlan <Native VLAN id>
```

```
switchport trunk allowed vlan <ScaleProtect-Data VLAN id> <ScaleProtect-Cluster VLAN id>
```

3. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

4. Set the MTU to 9216 to support jumbo frames.

```
mtu 9216
```

5. Make this a VPC port-channel and bring it up.

```
vpc 40
no shutdown
```

6. Define a port description for the interface connecting to <UCS Cluster Name>-B.

```
interface Eth1/25
description <UCS Cluster Name>-A:1/50
```

7. Apply it to a port channel and bring up the interface.

```
channel-group 40 force mode active
no shutdown
```

8. Define a description for the port-channel connecting to <UCS Cluster Name>-A.

```
interface Po50
description <UCS Cluster Name>-B
```

9. Make the port-channel a switchport and configure a trunk to allow ScaleProtect Data, ScaleProtect Cluster and the native VLANs.

```
switchport
switchport mode trunk
switchport trunk native vlan <Native VLAN id>
switchport trunk allowed vlan <ScaleProtect-Data VLAN id> <ScaleProtect-Cluster VLAN id>
```

10. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

11. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

12. Make this a VPC port-channel and bring it up.

```
vpc 12

no shutdown
```

13. Define a port description for the interface connecting to <UCS Cluster Name>-A.

```
interface Eth1/26

description <UCS Cluster Name>-B:1/50
```

14. Apply it to a port channel and bring up the interface.

```
channel-group 50 force mode active

no shutdown

copy run start
```

Uplink into Existing Network Infrastructure

Depending on the available network infrastructure, several methods and features can be used to uplink the ScaleProtect environment. If an existing Cisco Nexus environment is present, it is recommended to use vPCs to uplink the Cisco Nexus 9336C-FX2 switches included in the present environment into the infrastructure. The previously described procedures can be used to create an uplink vPC to the existing environment. Make sure to run `copy run start` to save the configuration on each switch after the configuration is completed.

Cisco Nexus 9000 A and B using Port Channel Example

To enable data protection and management network access across the IP switching environment leveraging port channel to a single switch run the following commands in config mode:

The connectivity to existing network is specific to each customer and the following is just an example for reference. Please consult the customer network team during implementation of the solution.

1. Define a description for the port-channel connecting to uplink switch.

```
interface po6

description <ScaleProtect Data VLAN>
```

2. Configure the port as an access VLAN carrying the management/data protection VLAN traffic.

```
switchport

switchport mode access

switchport access vlan <ScaleProtect Data VLAN id>
```

3. Make the port channel and associated interfaces normal spanning tree ports.

```
 spanning-tree port type normal
```

4. Make this a VPC port-channel and bring it up.

```
vpc 6

no shutdown
```

5. Define a port description for the interface connecting to the existing network infrastructure.

```
interface Eth1/33

description <ScaleProtect Data VLAN>_uplink
```

6. Apply it to a port channel and bring up the interface.

```
channel-group 6 force mode active

no shutdown
```

7. Save the running configuration to start-up in both Nexus 9000s and run commands to look at port and port channel information.

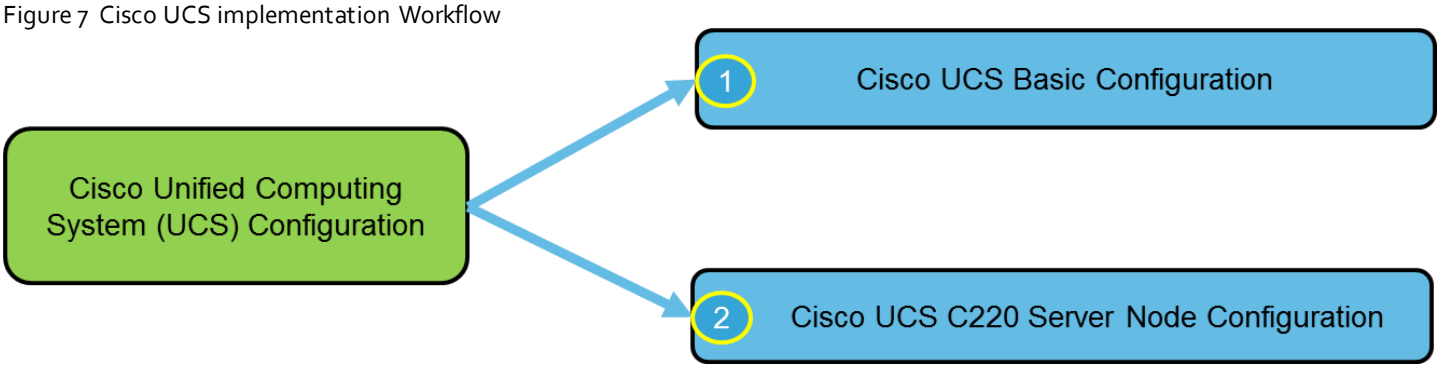
```
Copy run start

sh int eth1/33 br

sh port-channel summary
```

Cisco UCS Server Configuration

This section describes the steps to configure the Cisco Unified Computing System (Cisco UCS) to use in a ScaleProtect environment.

These steps are necessary to provision the Cisco UCS C220 M5 Servers and should be followed precisely to avoid improper configuration.

Figure 7 Cisco UCS implementation Workflow



This document includes the configuration of the Cisco UCS infrastructure to enable SAN connectivity to existing storage environment. The ScaleProtect design for this solution doesn't need SAN connectivity and additional information is included only as a reference and should be skipped if SAN connectivity is not required. All the sections that should be skipped for default design have been marked as optional.

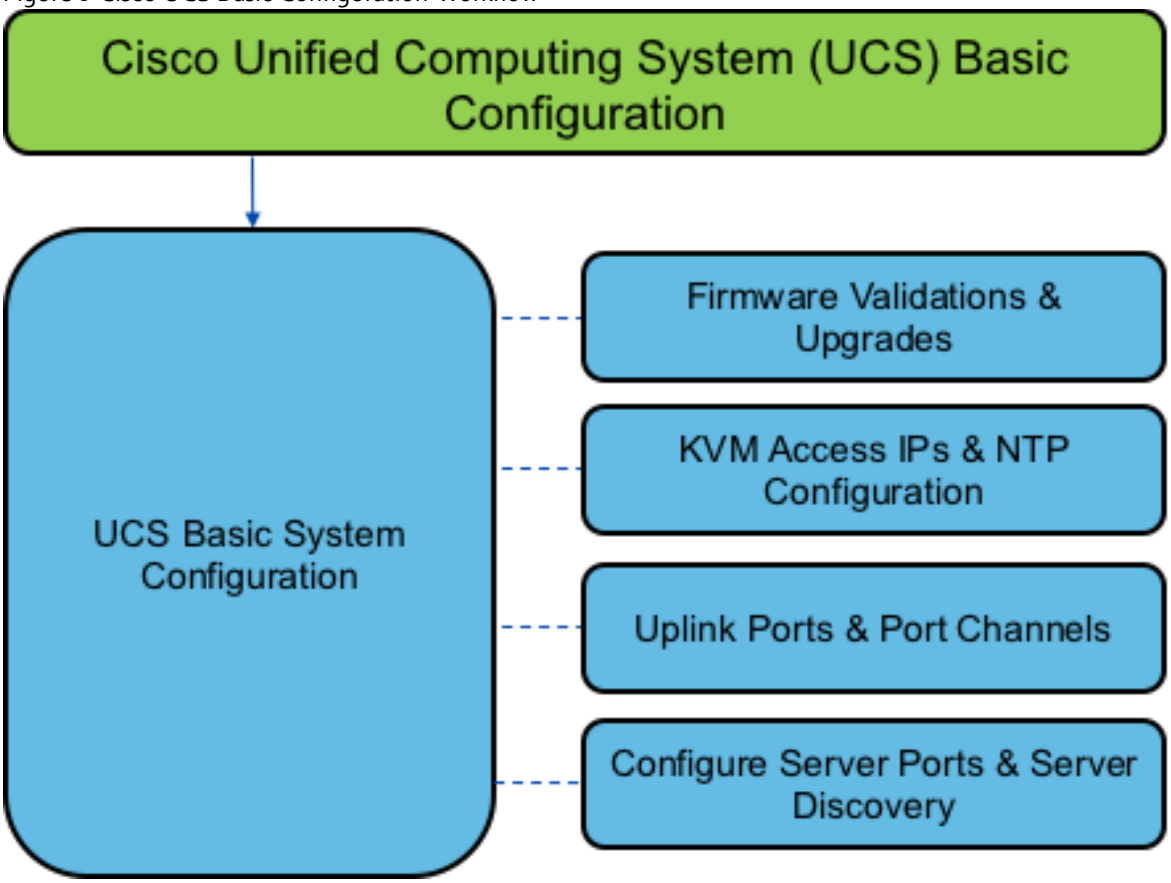
Cisco UCS Base Configuration

To complete Cisco UCS base configuration, follow the steps in this section.

Perform Initial Setup of Cisco UCS 6454 Fabric Interconnects

This section provides the configuration steps for the Cisco UCS 6454 Fabric Interconnects (FI) in a ScaleProtect design that includes Cisco UCS C220 M5 LFF Rack Servers.

Figure 8 Cisco UCS Basic Configuration Workflow



Cisco UCS 6454 Fabric Interconnect A

To configure Fabric Interconnect A, follow these steps:

1. Make sure the Fabric Interconnect cabling is properly connected, including the L1 and L2 cluster links, and power the Fabric Interconnects on by inserting the power cords.

2. Connect to the console port on the first Fabric Interconnect, which will be designated as the A fabric device. Use the supplied Cisco console cable (CAB-CONSOLE-RJ45=), and connect it to a built-in DB9 serial port, or use a USB to DB9 serial port adapter.

3. Start your terminal emulator software.

4. Create a connection to the COM port of the computer's DB9 port, or the USB to serial adapter. Set the terminal emulation to VT100, and the settings to 9600 baud, 8 data bits, no parity, 1 stop bit.

5. Open the connection just created. You may have to press **ENTER** to see the first prompt.

6. Configure the first Fabric Interconnect, using the following example as a guideline.

7. Connect to the console port on the first Cisco UCS 6454 fabric interconnect.

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

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

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

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

Enter the password for "admin": <UCS Password>

Confirm the password for "admin": <UCS Password>

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

Which switch fabric (A/B)[]: A

Enter the system name: <Name of the System>

Physical Switch Mgmt0 IP address: <Mgmt. IP address for Fabric A>

Physical Switch Mgmt0 IPv4 netmask: <Mgmt. IP Subnet Mask>

IPv4 address of the default gateway: <Default GW for the Mgmt. IP >

Cluster IPv4 address: <Cluster Mgmt. IP address>

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

DNS IP address: <DNS IP address>

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

Default domain name: <DNS Domain Name>

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

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

8. Wait for the login prompt to make sure that the configuration has been saved.

Cisco UCS 6454 Fabric Interconnect B

To configure Fabric Interconnect B, follow these steps:

1. Connect to the console port on the first Fabric Interconnect, which will be designated as the B fabric device. Use the supplied Cisco console cable (CAB-CONSOLE-RJ45=), and connect it to a built-in DB9 serial port, or use a USB to DB9 serial port adapter.

2. Start your terminal emulator software.

3. Create a connection to the COM port of the computer's DB9 port, or the USB to serial adapter. Set the terminal emulation to VT100, and the settings to 9600 baud, 8 data bits, no parity, 1 stop bit.

4. Open the connection just created. You may have to press **ENTER** to see the first prompt.

5. Configure the second Fabric Interconnect, using the following example as a guideline.

6. Connect to the console port on the second Cisco UCS 6454 fabric interconnect.

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

Installer has detected the presence of a peer Fabric interconnect. This

Fabric interconnect will be added to the cluster.  Continue (y|n)? y

Enter the admin password for the peer Fabric interconnect: <Admin Password>

 Connecting to peer Fabric interconnect... done
```

```
Retrieving config from peer Fabric interconnect... done

Peer Fabric interconnect Mgmt0 IPv4 Address: <Address provided in last step>

Peer Fabric interconnect Mgmt0 IPv4 Netmask: <Mask provided in last step>

Cluster IPv4 address          : <Cluster IP provided in last step>

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

Physical switch Mgmt0 IP address: < Mgmt. IP address for Fabric B>

Apply and save the configuration (select no if you want to re-enter)?

(yes/no): yes
```

7. Wait for the login prompt to make sure that the configuration has been saved.

Cisco UCS Setup

Log into Cisco UCS Manager

To log into the Cisco Unified Computing System (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 to download the Cisco UCS Manager software.
3. If prompted to accept security certificates, accept as necessary.
4. When prompted, enter `admin` as the user name and enter the administrative password.
5. Click **Login** to log in to Cisco UCS Manager.

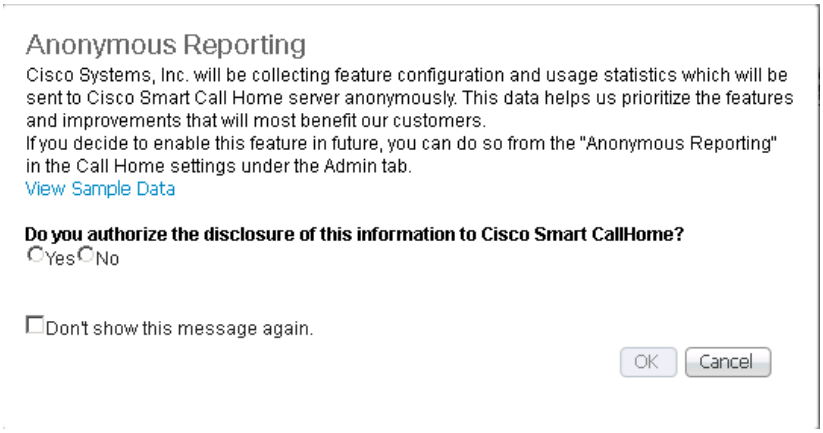
Upgrade Cisco UCS Manager Software to Version 4.0(4b)

This document assumes you are using Cisco UCS 4.0(4b). To upgrade the Cisco UCS Manager software and the Cisco UCS Fabric Interconnect software to version 4.0(4b), refer to the Cisco UCS Manager Install and Upgrade Guides.

Anonymous Reporting

To enable anonymous reporting, follow this step:

1. In the Anonymous Reporting window, select whether to send anonymous data to Cisco for improving future products:



Configure Cisco UCS Call Home

It is highly recommended by Cisco to configure Call Home in Cisco UCS Manager. Configuring Call Home will accelerate resolution of support cases.

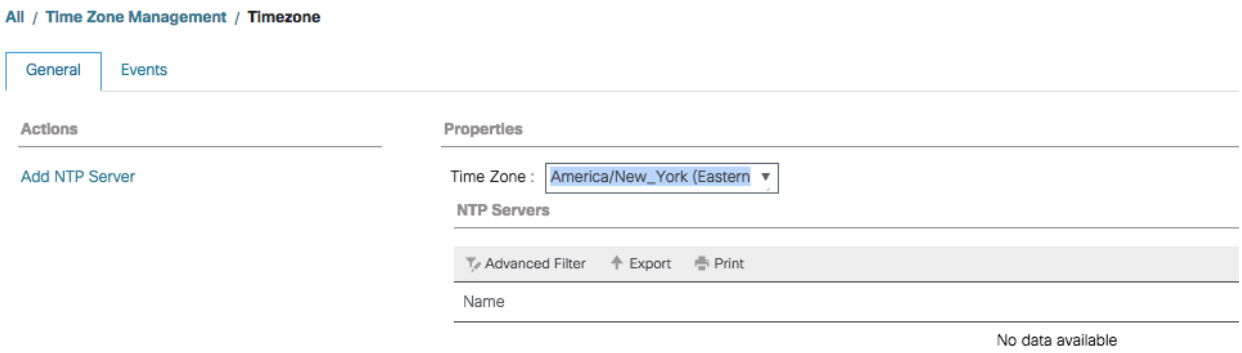
To configure Call Home, follow these steps:

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

Synchronize Cisco UCS to NTP

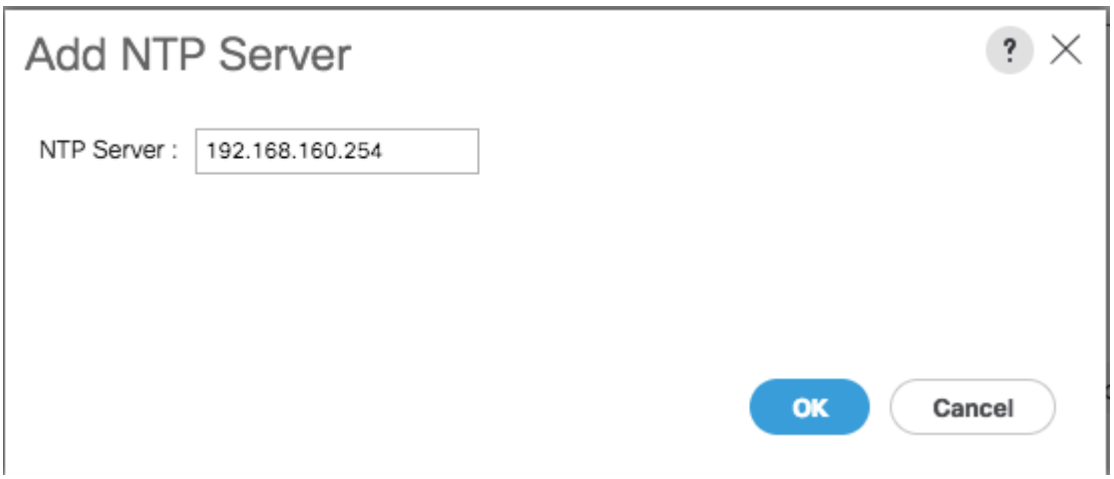
To synchronize the Cisco UCS environment to the NTP server, follow these steps:

1. In Cisco UCS Manager, click the **Admin** tab in the navigation pane.
2. Select All > Timezone Management > Timezone.



3. In the Properties pane, select the appropriate time zone in the Timezone menu.
4. Click Add NTP Server.

5. Enter <NTP Server IP Address> and click **OK**.

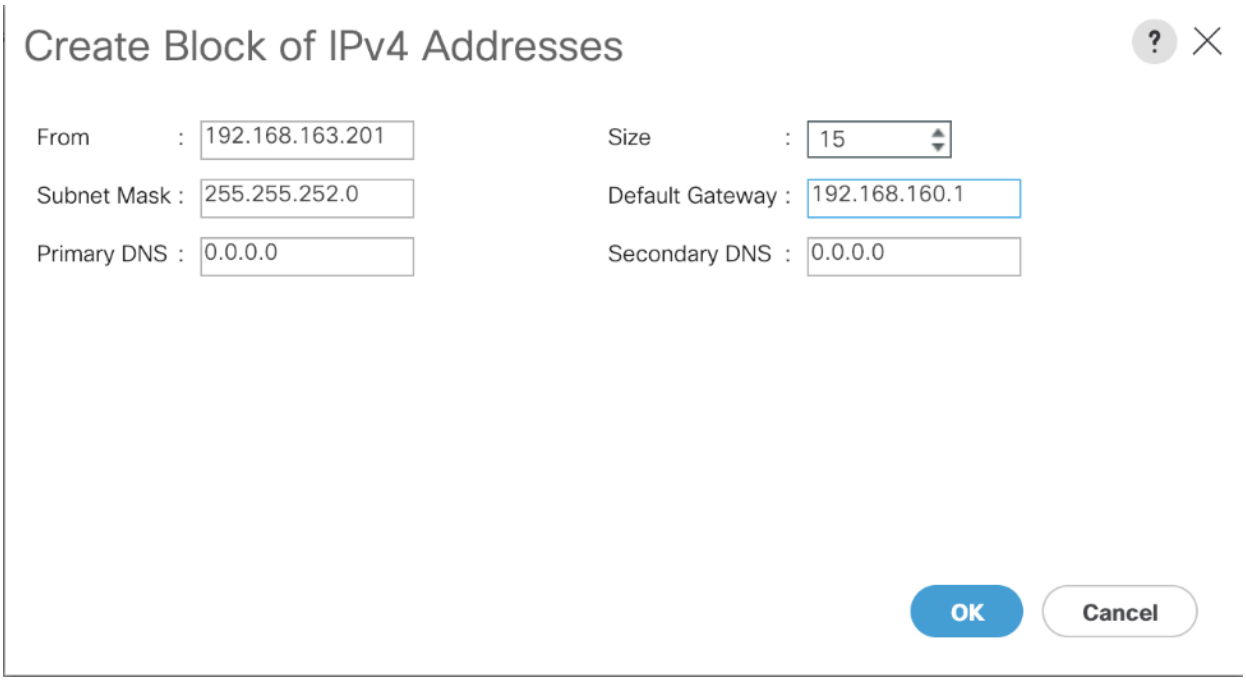


6. Click **Save Changes** and then click **OK**.

Add Block IP Addresses for KVM Access

To create a block of IP addresses for in band server Keyboard, Video, Mouse (KVM) access in the Cisco UCS environment, 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.
4. Enter the starting IP address of the block, the number of IP addresses required, and the subnet and gateway information.



5. Click **OK** to create.

6. Click **OK** in the confirmation message.

Server Discovery Policy

The Server discovery policy determines how the system reacts when you add a new Cisco UCS server to a Cisco UCS system. Cisco UCS Manager uses the settings in the chassis discovery policy to determine whether to group links from the VIC's to the fabric interconnects in fabric port channels.

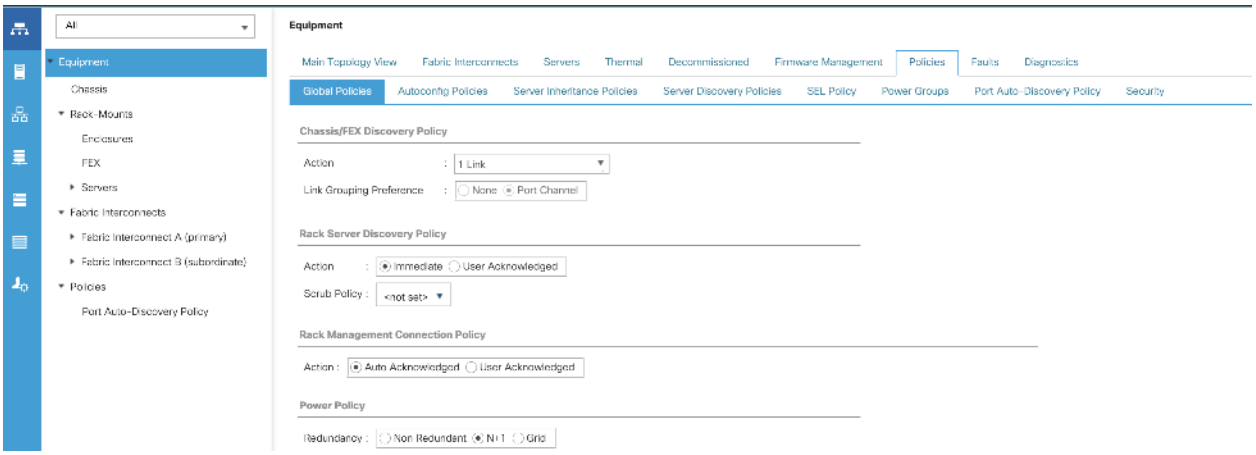
To add a previously standalone Cisco UCS C220 to a Cisco UCS system, you must first configure it to factory default. You can then connect both ports of the VIC on the server to both fabric interconnects. After you connect the VIC ports to the fabric interconnects, and mark the ports as server ports, server discovery begins.

To modify the chassis discovery policy, follow these steps:

1. In Cisco UCS Manager, click the **Equipment** tab in the navigation pane and select Equipment in the list on the left

2. In the right pane, click the **Policies** tab.

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



4. Click **Save Changes** if values changed from default values.

5. Click **OK**.

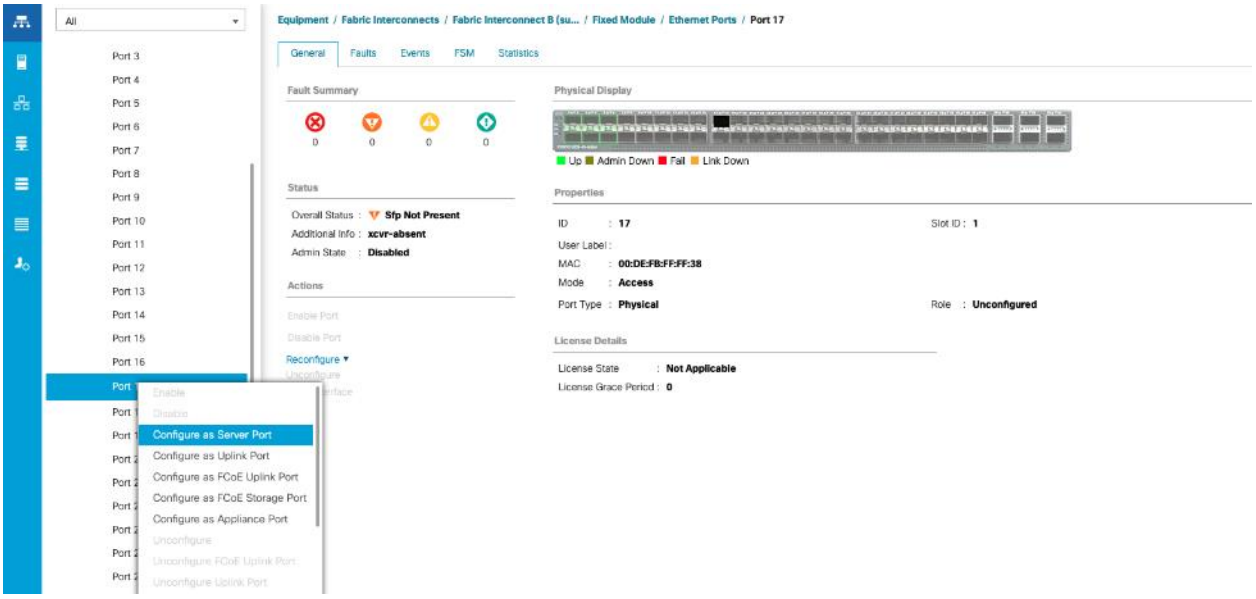
Enable Server Ports

The Ethernet ports of a Cisco UCS Fabric Interconnect connected to the rack-mount servers, or to the blade chassis or to Cisco UCS S3260 Storage Server must be defined as server ports. When a server port is activated, the connected server or chassis will begin the discovery process shortly afterwards. Rack-mount servers, blade chassis, and Cisco UCS S3260 chassis are automatically numbered in the order which they are first discovered. For this reason, it is important to configure the server ports sequentially in the order you wish the physical servers and/or chassis to appear within Cisco UCS Manager. For example, if you installed your servers in a cabinet or rack with server #1 on the bottom, counting up as you go higher in the cabinet or rack, then you need to enable the server ports to the bottom-most server first, and enable them one-by-one as you move upward. You must wait until the server appears in the Equipment tab of Cisco UCS Manager before configuring the ports for the next server. The same numbering procedure applies to blade server chassis.

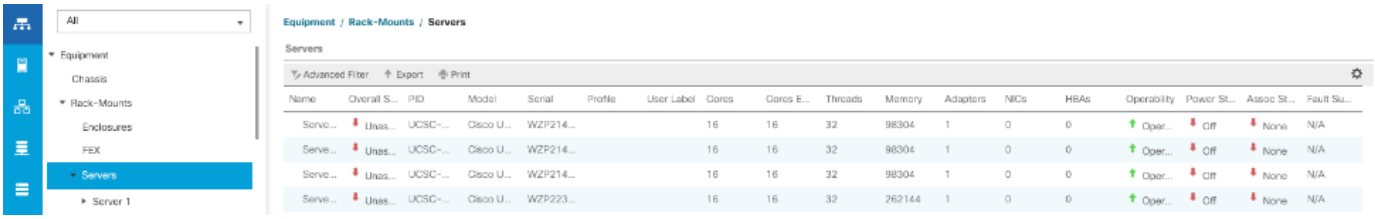
Cisco UCS Port Auto-Discovery Policy can be optionally enabled to discover the servers without having to manually define the server ports. The procedure in next section details the process of enabling Auto-Discovery Policy.

To define the specified ports to be used as server ports, follow these steps:

1. In Cisco UCS Manager, click the **Equipment** tab in the navigation pane
2. Select Fabric Interconnects > Fabric Interconnect A > Fixed Module > Ethernet Ports.
3. Select the first port that is to be a server port, right-click it, and click **Configure as Server Port**.
4. Click **Yes** to confirm the configuration and click **OK**.



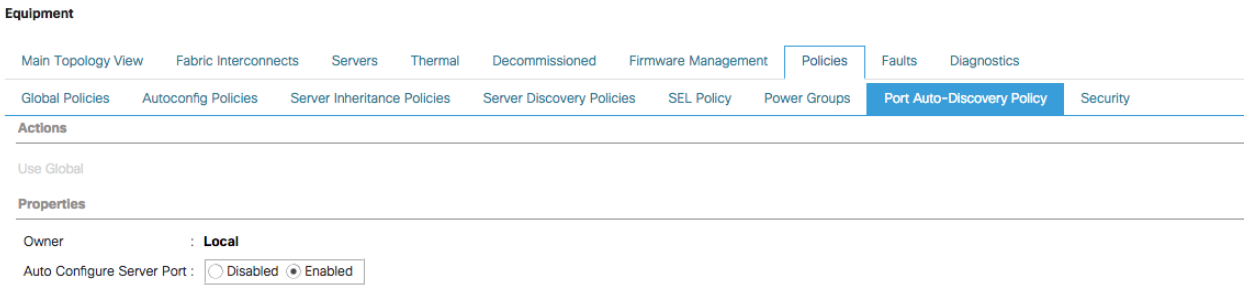
5. Select Fabric Interconnects > Fabric Interconnect B > Fixed Module > Ethernet Ports.
6. Select the matching port as chosen for Fabric Interconnect A which would be configured as Server Port.
7. Click **Yes** to confirm the configuration and click **OK**.
8. Repeat steps **1-7** for enabling other ports connected to the other C220 M5 Server Nodes.
9. Wait for a brief period, until the rack-mount server appears in the Equipment tab underneath **Equipment > Rack Mounts > Servers**.



Optional: Edit Policy to Automatically Discover Server Ports

If the Cisco UCS Port Auto-Discovery Policy is enabled, server ports will be discovered automatically. To enable the Port Auto-Discovery Policy, follow these steps:

1. In Cisco UCS Manager, click the **Equipment** icon on the left and select Equipment in the second list
2. In the right pane, click the **Policies** tab.
3. Under **Policies**, select the Port Auto-Discovery Policy tab.
4. Under **Properties**, set Auto Configure Server Port to `Enabled`.



5. Click Save Changes.
6. Click **OK**.

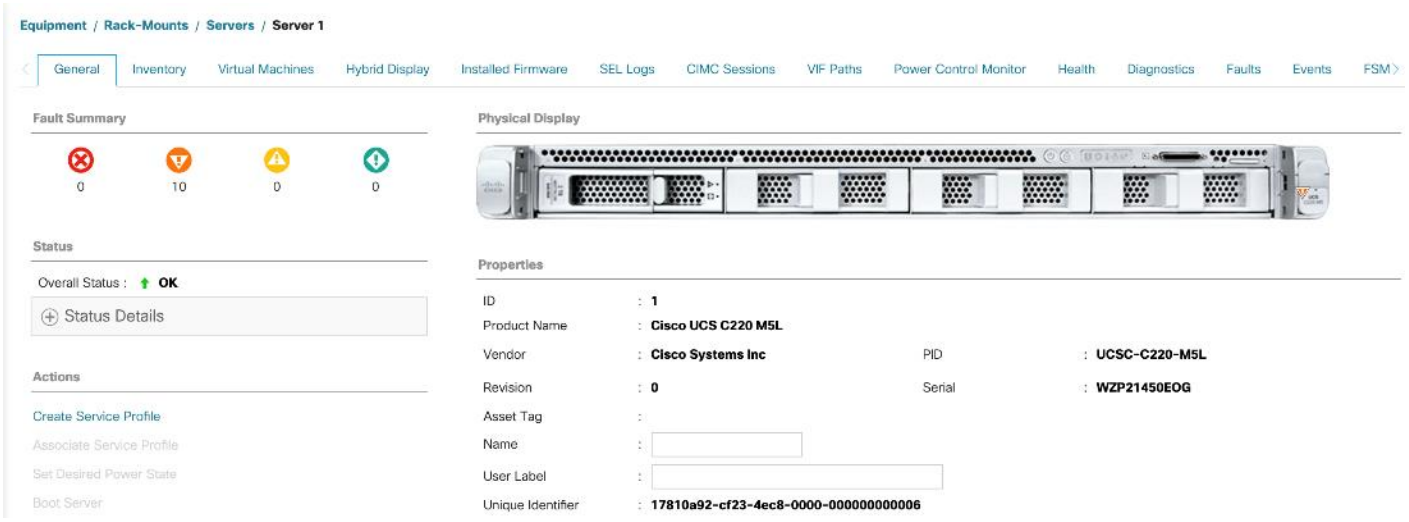
The first discovery process can take some time and is dependent on installed firmware on the chassis.

Server Discovery

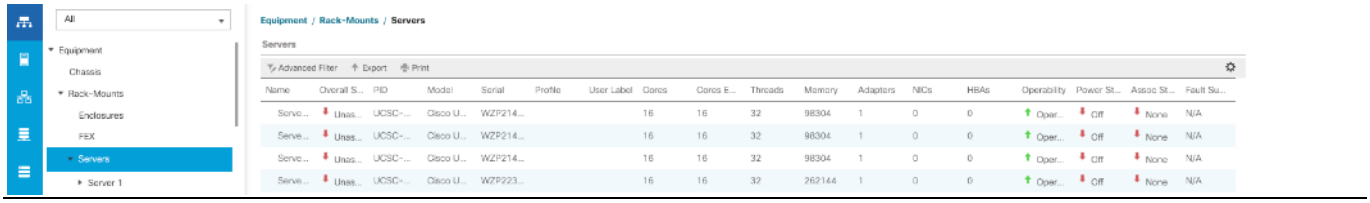
As previously described, when the server ports of the Fabric Interconnects are configured and active, the servers connected to those ports will begin a discovery process. During discovery the servers' internal hardware inventories are collected, along with their current firmware revisions. Before continuing with the Cisco UCS C220 rack server installation processes, wait for all of the servers to finish their discovery process and show as unassociated servers that are powered off, with no errors.

To view the servers' discovery status, follow these steps:

1. In Cisco UCS Manager, click the **Equipment** tab in the navigation pane.
2. Click **Rack-Mounts** and click the **Servers** tab.
3. Select the respective server and view the Server status in the Overall Status column.
4. When the server is discovered, the C220 M5 server is displayed as shown below:



5. Click the **Equipment > Rack–Mounts > Servers** Tab and view the servers' status in the Overall Status column. Below are the Cisco UCS C220 M5 Servers for ScaleProtect Cluster:



Optional: Enable Fibre Channel Ports

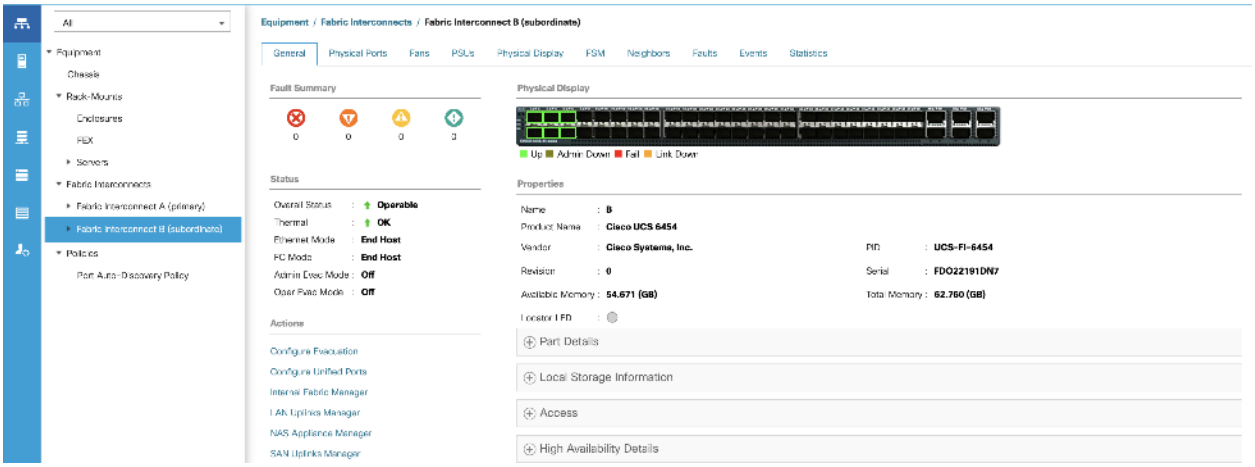
The FC port and uplink configurations can be skipped if the ScaleProtect Cisco UCS environment does not need access to storage environment using FC SAN.

Fibre Channel port configurations differ between the 6454, 6332-16UP and the 6248UP Fabric Interconnects. All Fabric Interconnects have a slider mechanism within the Cisco UCS Manager GUI interface, but the fibre channel port selection options for the 6454 are from the first 8 ports starting from the first port and configured in increments of 4 ports from the left. For the 6332-16UP the port selection options are from the first 16 ports starting from the first port, and configured in increments of the first 6, 12, or all 16 of the unified ports. With the 6248UP, the port selection options will start from the right of the 32 fixed ports, or the right of the 16 ports of the expansion module, going down in contiguous increments of 2. The remainder of this section shows configuration of the 6454. Modify as necessary for the 6332-16UP or 6248UP.

To enable FC uplink ports, follow these steps.

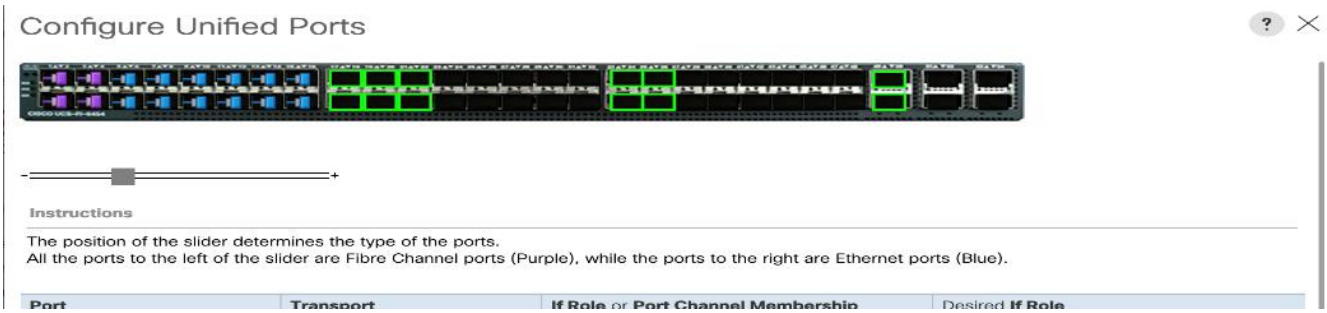
This step requires a reboot. To avoid an unnecessary switchover, configure the subordinate Fabric Interconnect first.

1. In the **Equipment** tab, select the **Fabric Interconnect B** (subordinate FI in this example), and in the **Actions** pane, select **Configure Unified Ports**, and click **Yes** on the splash screen.



2. Slide the lever to change the ports `1-4` to Fiber Channel. Click **Finish** followed by **Yes** to the reboot message. Click **OK**.

Select the number of ports to be enabled as FC uplinks based on the amount of bandwidth required in the customer specific setup.



3. When the subordinate has completed reboot, repeat the procedure to configure FC ports on primary Fabric Interconnect. As before, the Fabric Interconnect will reboot after the configuration is complete.

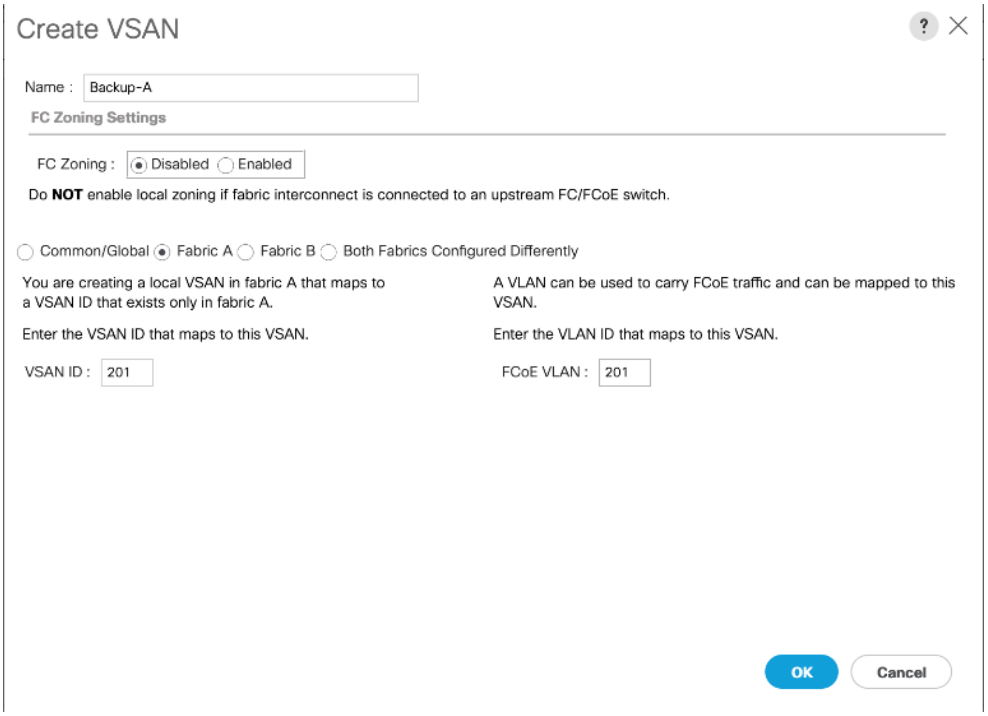
Optional: Create VSAN for the Fibre Channel Interfaces

Creating VSANs is optional and is only required if connectivity to existing production and backup SAN fabrics is required for the solution. Sample VSAN ids are used in the document for both production and backup fibre channel networks, match the VSAN ids based on customer specific environment.

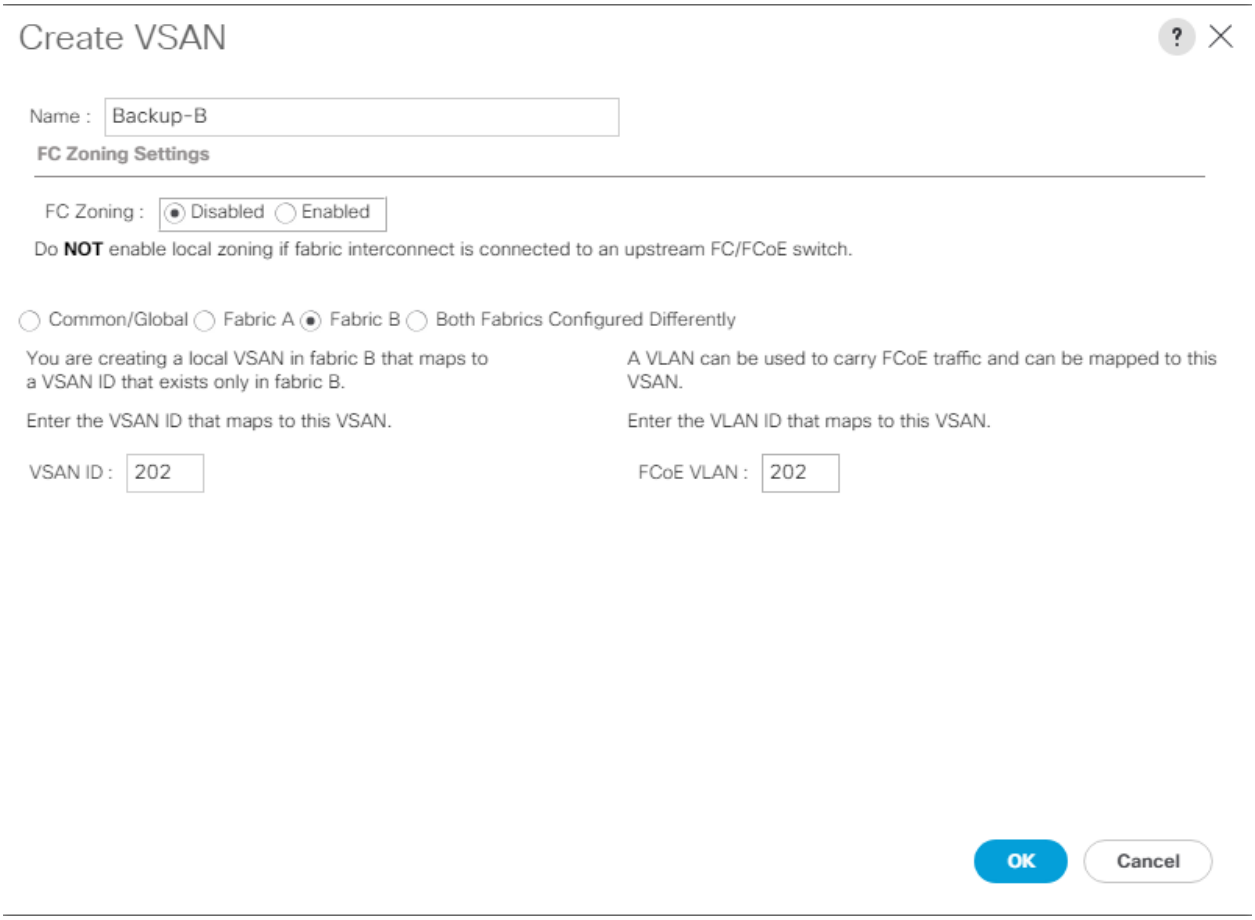
To configure the necessary virtual storage area networks (VSANs) for FC uplinks for the Cisco UCS environment, follow these steps:

1. In Cisco UCS Manager, click the **SAN** tab in the navigation pane.
2. Expand the **SAN** > **SAN Cloud** and select **Fabric A**.
3. Right-click **VSANs** and choose **Create VSAN**.
4. Enter `Backup-A` as the name of the VSAN for fabric A.

6. Keep the Disabled option selected for FC Zoning.
5. Click the **Fabric A** radio button.
6. Enter `201` as the VSAN ID for Fabric A.
7. Enter `201` as the FCoE VLAN ID for fabric A. Click **OK** twice.

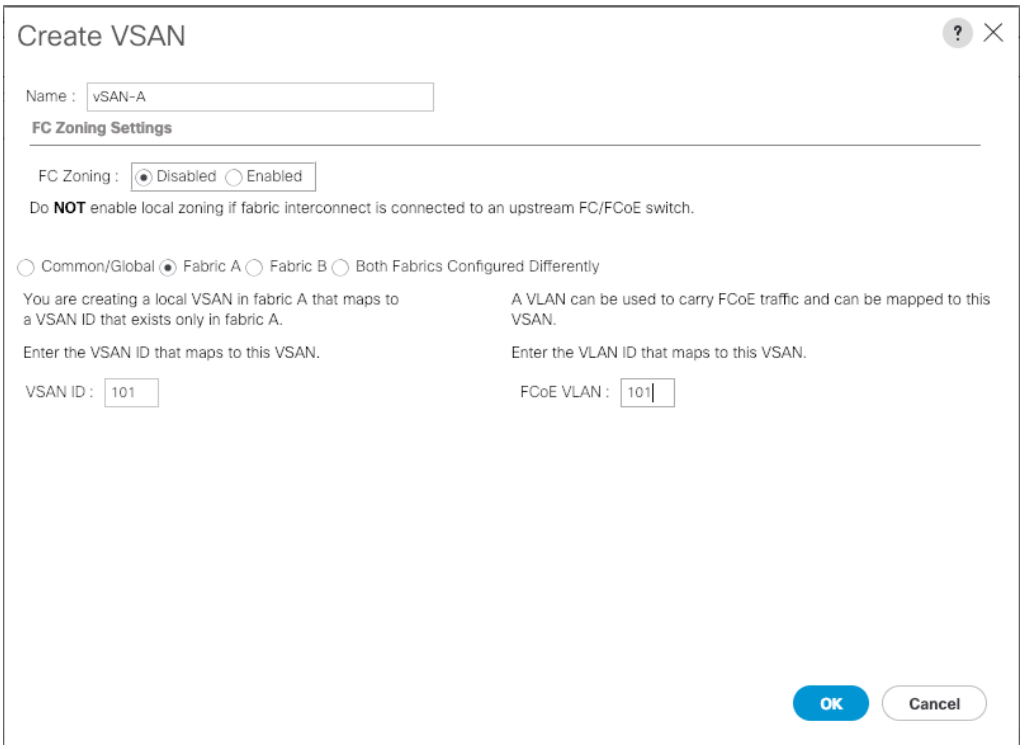


8. In the **SAN** tab, expand **SAN** > **SAN Cloud** > **Fabric-B**.
9. Right-click **VSANs** and choose **Create VSAN**.
10. Enter `Backup-B` as the name of the VSAN for fabric B.
11. Keep the Disabled option selected for FC Zoning.
12. Click the **Fabric B** radio button.
13. Enter `202` as the VSAN ID for Fabric B. Enter `202` as the FCoE VLAN ID for Fabric B. Click **OK** twice.

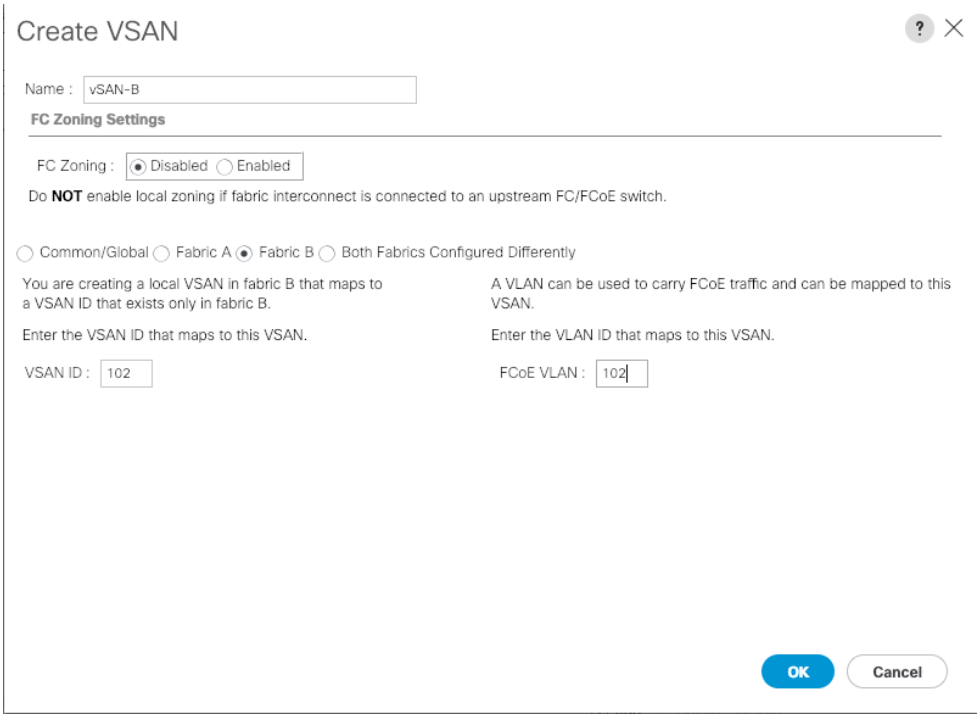


The VSANs created in the following steps are an example of production VSANs used in the document for access to production storage. Adjust the VSAN id's based on customer specific deployment.

14. In Cisco UCS Manager, click the **SAN** tab in the navigation pane.
15. Expand the **SAN** > **SAN Cloud** and select **Fabric A**.
16. Right-click **VSANs** and choose **Create VSAN**.
17. Enter `vsan-A` as the name of the VSAN for fabric A.
7. Keep the Disabled option selected for FC Zoning.
18. Click the **Fabric A** radio button.
19. Enter `101` as the VSAN ID for Fabric A.
20. Enter `101` as the FCoE VLAN ID for fabric A. Click **OK** twice.



21. In the **SAN** tab, expand **SAN** > **SAN Cloud** > **Fabric-B**.
22. Right-click VSANs and choose **Create VSAN**.
23. Enter `vsan-B` as the name of the VSAN for fabric B.
24. Keep the Disabled option selected for FC Zoning.
25. Click the **Fabric B** radio button.
26. Enter `102` as the VSAN ID for Fabric B. Enter `102` as the FCoE VLAN ID for Fabric B. Click **OK** twice.



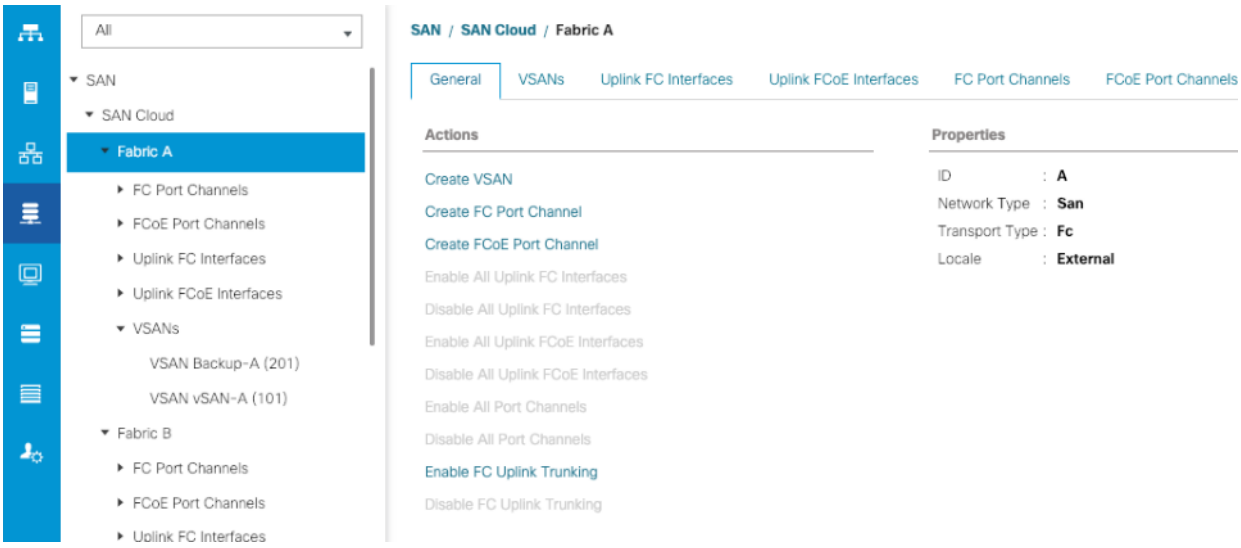
Optional: Create Port Channels for the Fibre Channel Interfaces

As previously mentioned, Fibre channel connectivity is optional and the following procedure to create port-channels is included for reference and the procedure varies depending on the upstream SAN infrastructure.

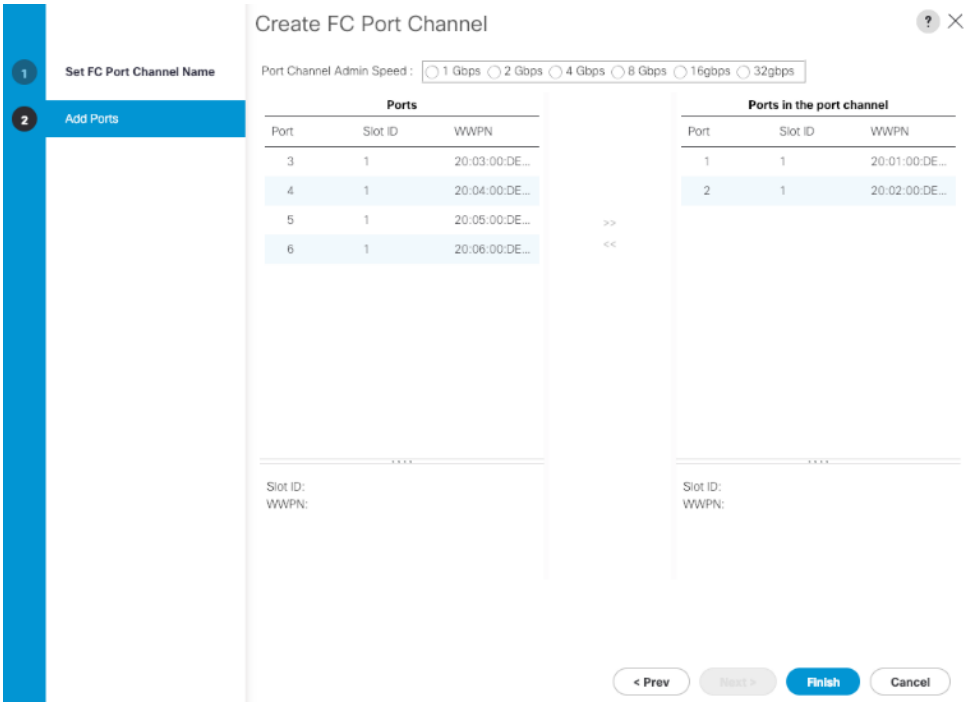
To configure the necessary FC port channels for the Cisco UCS environment, follow these steps:

Fabric-A

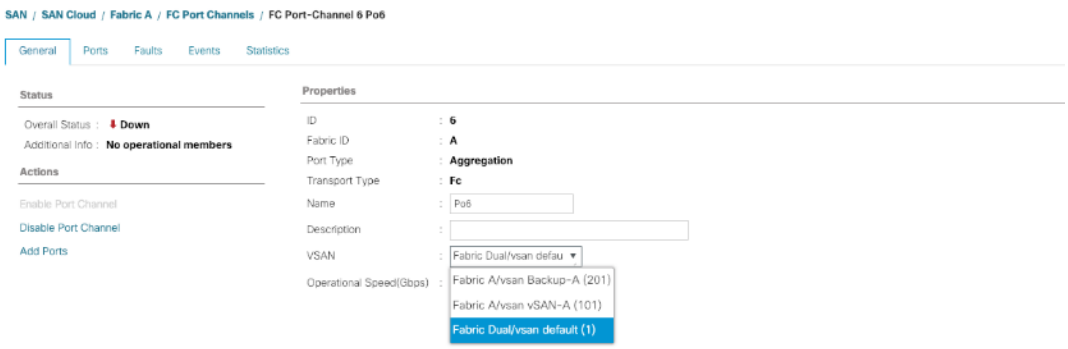
1. In the navigation pane, under **SAN** > **SAN Cloud**, expand the Fabric A tree.
2. Click Enable FC Uplink Trunking.



3. Click **Yes** on the warning message.
4. Click **Create FC Port Channel** on the same screen.
5. Enter `6` for the port channel ID and Po6 for the port channel name.
6. Click **Next** then choose ports `1 and 2` and click **>>** to add the ports to the port channel.
7. Select Port Channel Admin Speed as 32gbps.
8. Click **Finish**.



9. Click **OK**.
10. Select FC Port-Channel `6` from the menu in the left pane and from the VSAN drop-down field, keep `VSAN 1` selected in the right pane.



11. Click **Save Changes** and then click **OK**.

Fabric-B

1. Click the **SAN** tab. In the navigation pane, under **SAN** > **SAN Cloud**, expand the Fabric B.
2. Right-click `FC Port Channels` and choose **Create Port Channel**.
3. Enter `7` for the port channel ID and Po7 for the port channel name. Click **Next**.
4. Choose ports `1 and 2` and click **>>** to add the ports to the port channel.
5. Click **Finish**, and then click **OK**.
6. Select FC Port-Channel `7` from the menu in the left pane and from the VSAN drop-down list, keep `VSAN 1` selected in the right pane.
7. Click **Save Changes** and then click **OK**.

The procedure (above) creates port channels with trunking enabled to allow both production and backup VSANs, the necessary configuration needs to be completed on the upstream switches to establish connectivity successfully.

Disable Unused FC Uplink Ports (FCP)

When Unified Ports were configured earlier in this procedure, on the Cisco UCS 6454 FI and the Cisco UCS 6332 -16UP FI, FC ports are configured in groups. Because of this group configuration, some FC ports are unused and need to be disabled to prevent alerts.

To disable the unused FC ports 3 and 4 on the Cisco UCS 6454 FIs, follow these steps:

1. In Cisco UCS Manager, click **Equipment**.
2. In the Navigation Pane, expand Equipment > Fabric Interconnects > Fabric Interconnect A > Fixed Module > FC Ports.
3. Select FC Port `3` and FC Port `4`. Right-click and select `Disable`.

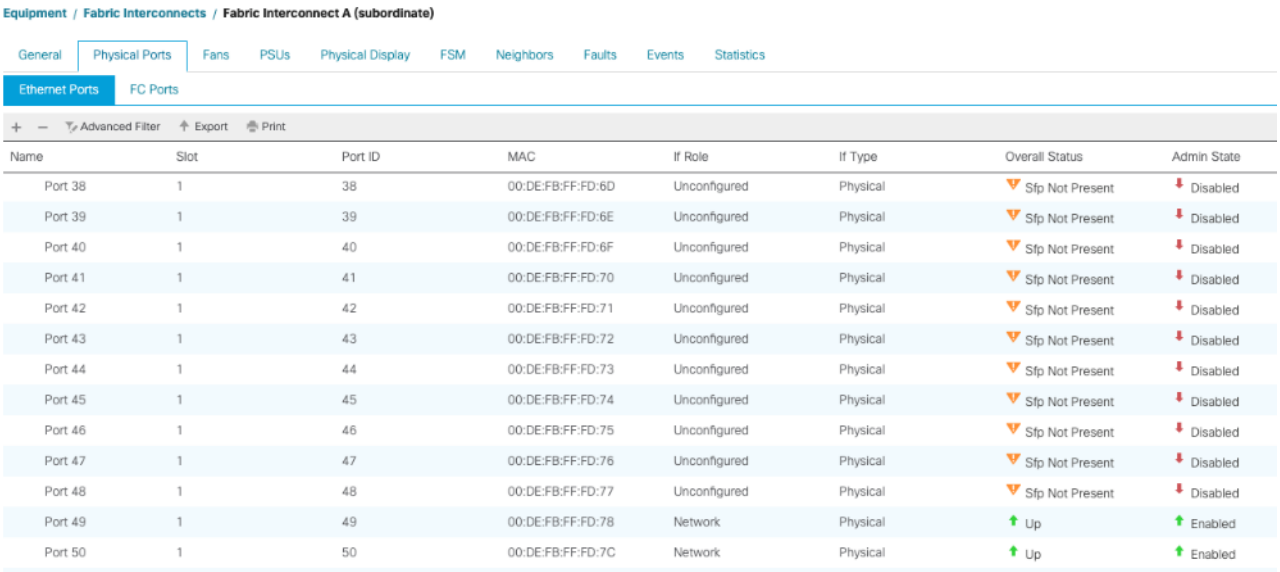
4. Click **Yes** and **OK** to complete disabling the unused FC ports.
5. In the Navigation Pane, expand Equipment > Fabric Interconnects > Fabric Interconnect B > Fixed Module > FC Ports.
6. Select FC Port `3` and FC Port `4`. Right-click and select `Disable`.
7. Click **Yes** and **OK** to complete disabling the unused FC ports.

Enable Ethernet Uplink Ports

The Ethernet ports of a Cisco UCS 6554 Fabric Interconnect are all capable of performing several functions, such as network uplinks or server ports, and more. By default, all ports are unconfigured, and their function must be defined by the administrator.

To define the specified ports to be used as network uplinks to the upstream network, follow these steps:

1. In Cisco UCS Manager, click the **Equipment** tab in the navigation pane.
2. Select Fabric Interconnects > Fabric Interconnect A > Fixed Module > Ethernet Ports.
3. Select the ports that are to be uplink ports (`49 & 50`), right click them, and click **Configure as Uplink Port**.
4. Click **Yes** to confirm the configuration and click **OK**.
5. Select Fabric Interconnects > Fabric Interconnect B > Fixed Module > Ethernet Ports.
6. Select the ports that are to be uplink ports (`49 & 50`), right-click them, and click **Configure as Uplink Port**.
7. Click **Yes** to confirm the configuration and click **OK**.
8. Verify all the necessary ports are now configured as uplink ports.

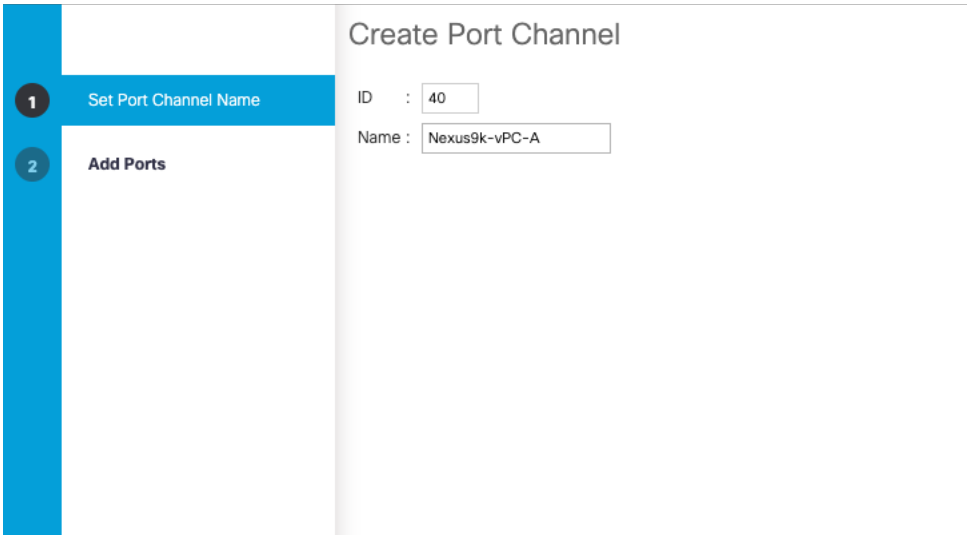


Create Port Channels for Ethernet Uplinks

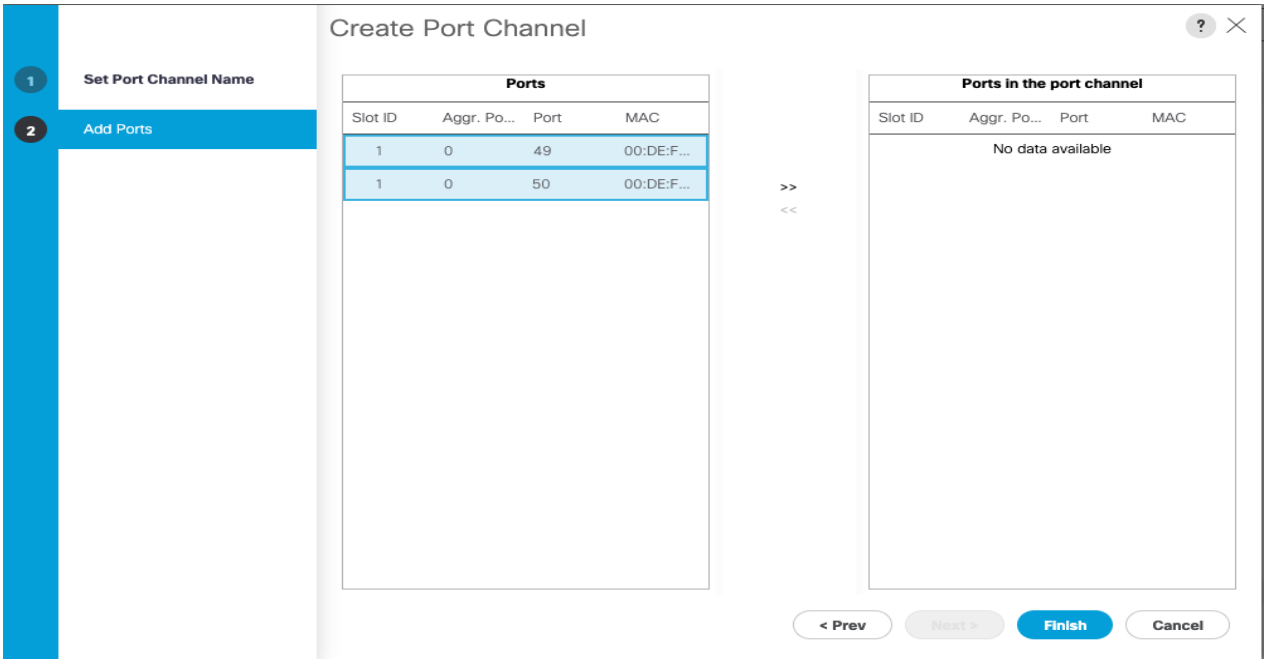
If the Cisco UCS uplinks from one Fabric Interconnect are to be combined into a port channel or vPC, you must separately configure the port channels using the previously configured uplink ports.

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

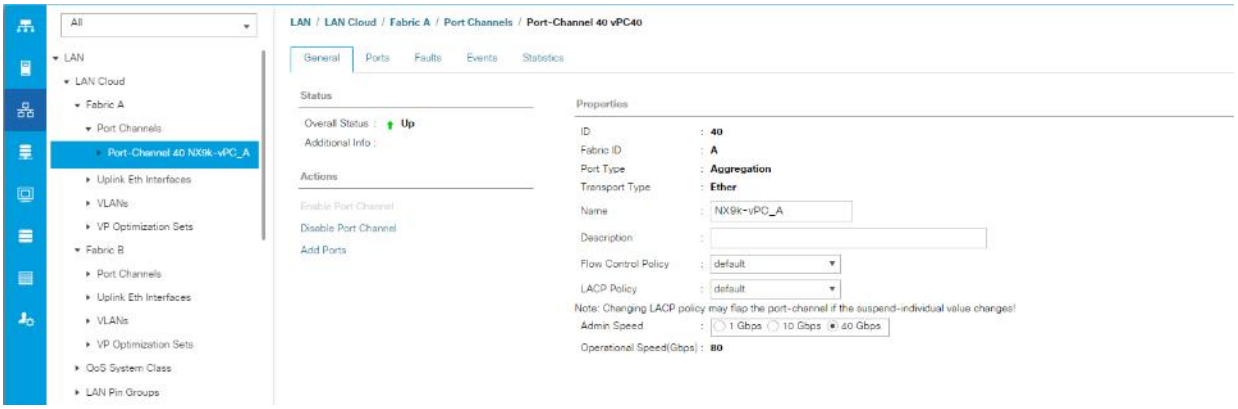
1. In Cisco UCS Manager, click the **LAN** tab in the navigation pane.
2. Under **LAN > LAN Cloud**, click to expand the **Fabric A** tree.
3. Right-click **Port Channels** underneath Fabric A and select Create Port Channel.
4. Enter the port channel ID number as the unique ID of the port channel.



5. Enter the name of the port channel.
6. Click **Next**.
7. Click each port from Fabric Interconnect A that will participate in the port channel and click the **>>** button to add them to the port channel.



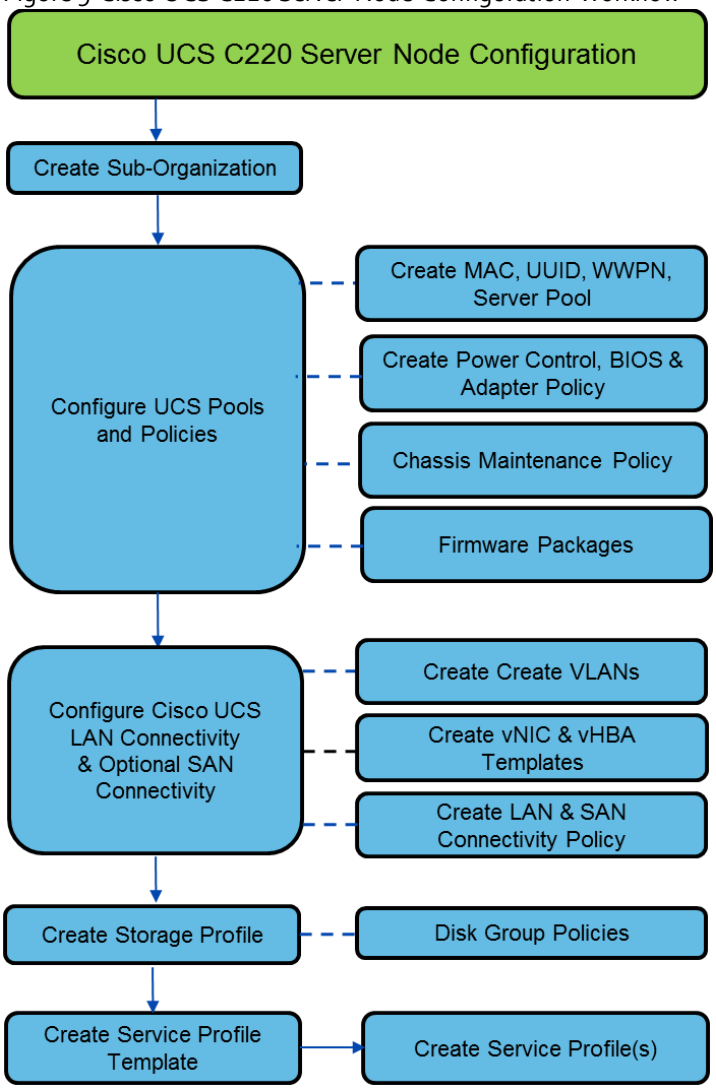
8. Click **Finish**.
9. Click **OK**.
10. Under **LAN > LAN Cloud,** click to expand the Fabric B tree.
11. Right-click **Port Channels** underneath Fabric B and select Create **Port Channel**.
12. Enter the port channel ID number as the unique ID of the port channel.
13. Enter the name of the port channel.
14. Click **Next**.
15. Click each port from Fabric Interconnect B that will participate in the port channel and click the **>>** button to add them to the port channel.
16. Click **Finish**.
17. Click **OK**.
18. Verify the necessary port channels have been created. It can take a few minutes for the newly formed port channels to converge and come online.



Cisco UCS C220 M5 Server Node Configuration

The steps provided in this section details for Cisco UCS C220 M5 Server setup. The procedure includes creation of ScaleProtect environment specific UCS pools and policies, followed by the Cisco UCS C220 M5 Server Node setup which will involve Service Profile creation and association using Storage Profile.

Figure 9 Cisco UCS C220 Server Node Configuration Workflow

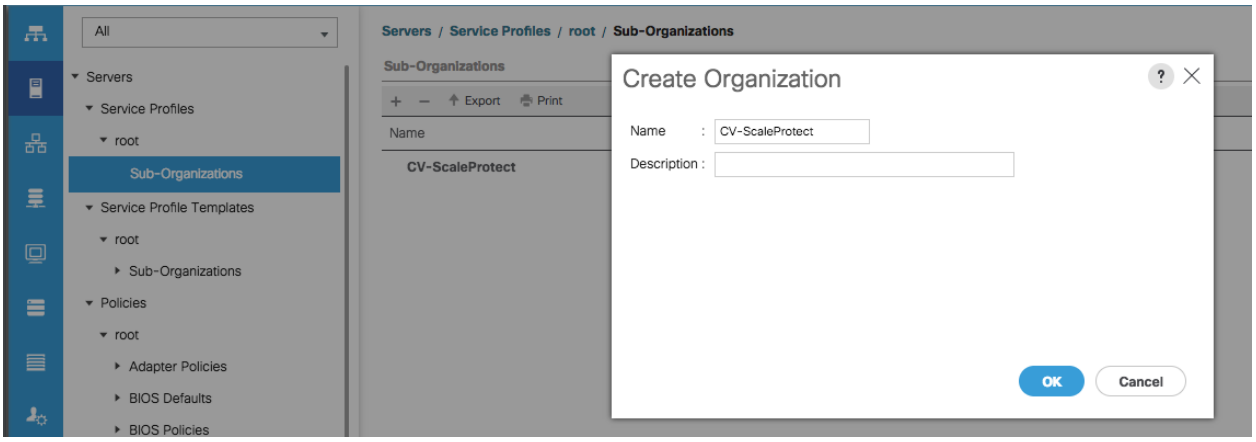


Create Sub-Organization

In this setup, one sub-organization under the root has been created. Sub-organizations help to restrict user access to logical pools and objects in order to facilitate secure provisioning and to provide easier user interaction. For ScaleProtect backup infrastructure, create a sub-organization as "`CV-ScaleProtect`".

To create a sub-organization, follow these steps:

1. In the Navigation pane, click the **Servers** tab.
2. In the Servers tab, expand **Service Profiles > root**. You can also access the Sub-Organizations node under the Policies or Pools nodes.
3. Right-click **Sub-Organizations** and choose Create Organization.
4. Enter `CV-ScaleProtect` as the name or any other obvious name, enter a description, and click **OK**.



Create MAC Address Pools

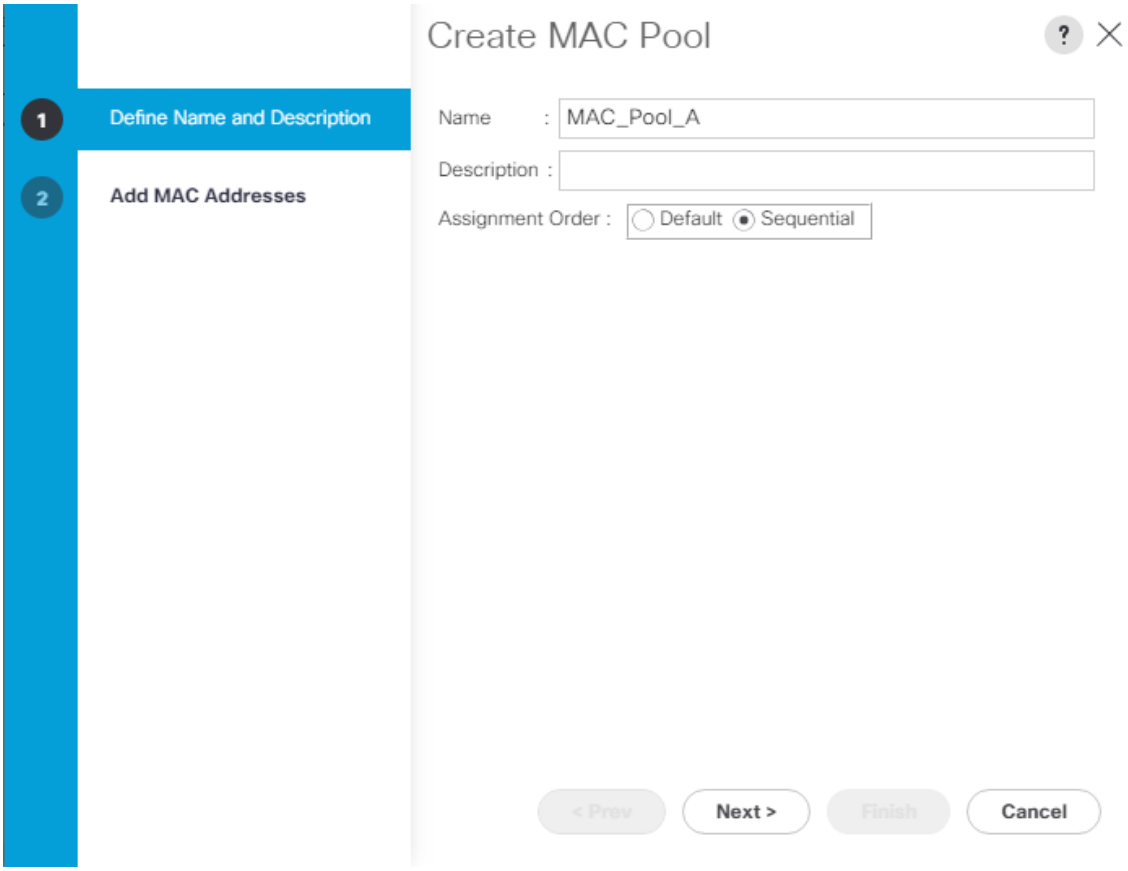
To configure the necessary MAC address pools for the Cisco UCS environment, follow these steps:

1. In Cisco UCS Manager, click the **LAN** tab in the navigation pane.
2. Select Pools > root > Sub-organizations > CV-ScaleProtect.

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

---

3. Right-click **MAC Pools** under the root organization.
4. Select Create MAC Pool to create the MAC address pool.
5. Enter `MAC_Pool_A` as the name of the MAC pool.
6. **Optional:** Enter a description for the MAC pool.
7. Select **Sequential** as the option for Assignment Order.



8. Click **Next**.

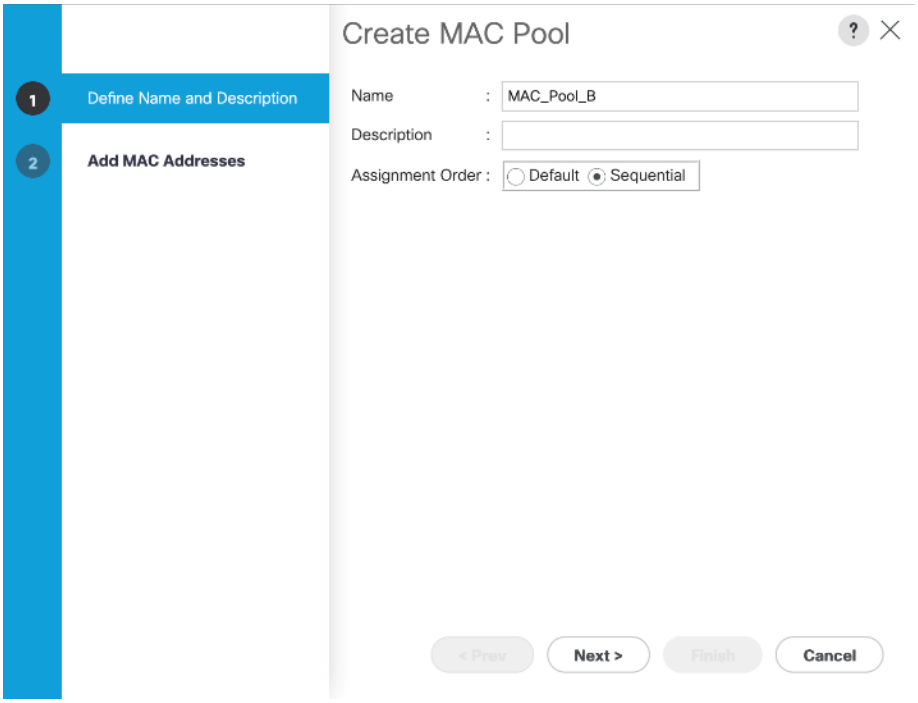
9. Click **Add**.

10. Specify a starting MAC address.

It is recommended to place oA in the second last octet of the starting MAC address to identify all of the MAC addresses as Fabric A addresses. It is also recommended to not change the first three octets of the MAC address.

11. Specify a size for the MAC address pool that is sufficient to support the future ScaleProtect cluster expansion and any available blade or server resources.

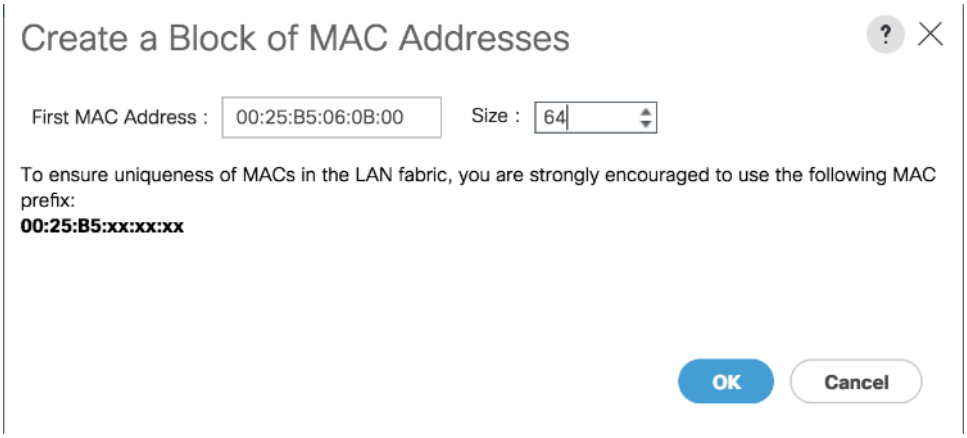
12. Click **OK**.
13. Click **Finish**.
14. In the confirmation message, click **OK**.
15. Right-click **MAC Pools** under the root organization.
16. Select Create MAC Pool to create the MAC address pool.
17. Enter `MAC_Pool_B` as the name of the MAC pool.
18. **Optional:** Enter a description for the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



20. Click **Next**.
21. Click **Add**.
22. Specify a starting MAC address.

It is recommended to place 0B in the second last octet of the starting MAC address to identify all of the MAC addresses as Fabric A addresses. It is also recommended to not change the first three octets of the MAC address.

23. Specify a size for the MAC address pool that is sufficient to support the future ScaleProtect cluster expansion and any available blade or server resources.

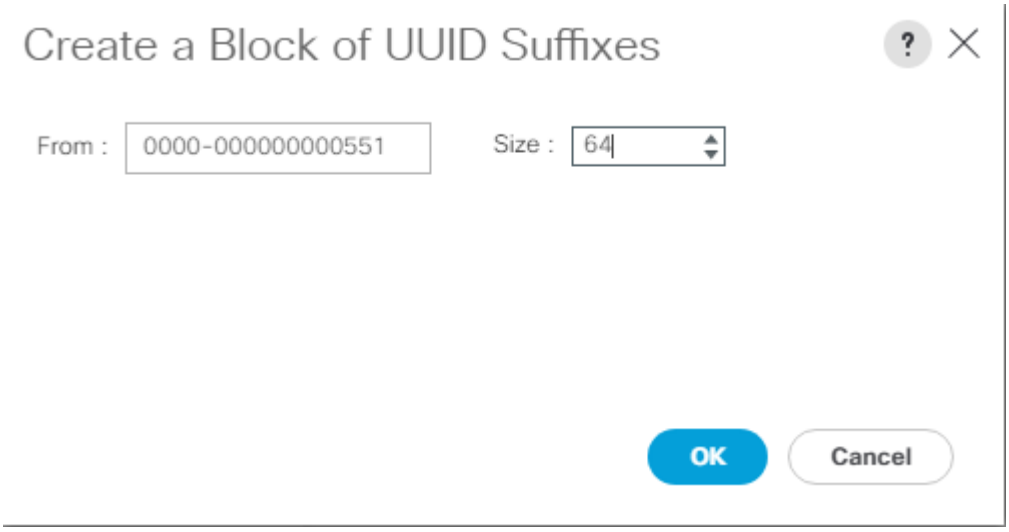


24. Click **OK**.
25. Click **Finish**.
26. In the confirmation message, click **OK**.

Create UUID Suffix Pool

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

1. In Cisco UCS Manager, click the **Servers** tab in the navigation pane.
2. Select Pools > root > Sub-Organizations > CV-ScaleProtect.
3. Right-click UUID Suffix Pools.
4. Select Create UUID Suffix Pool.
5. Enter `UUID_Pool` as the name of the UUID suffix pool.
6. **Optional:** Enter a description for the UUID suffix pool.
7. Keep the prefix at the derived option.
8. Select Sequential for the Assignment Order.
9. Click **Next**.
10. Click **Add** to add a block of UUIDs.
11. Keep the value in From field at the default setting.
12. Specify a size for the UUID block that is sufficient to support the available server resources.



13. Click **OK**.
14. Click **Finish**.
15. Click **OK**.

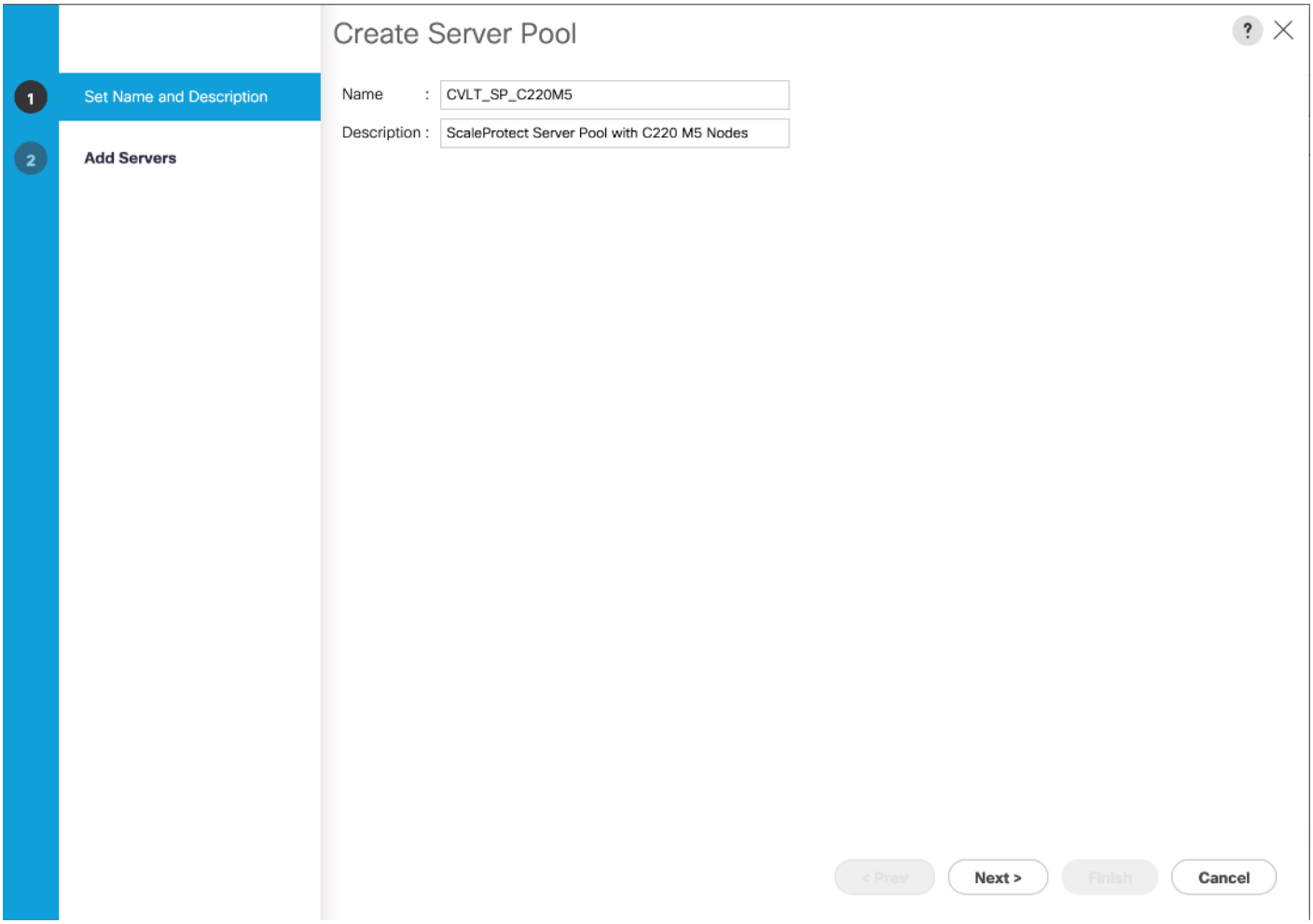
Create Server Pool

The following procedure guides you in creating two server pools, one for first server nodes in the chassis and the other of the second server nodes.

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

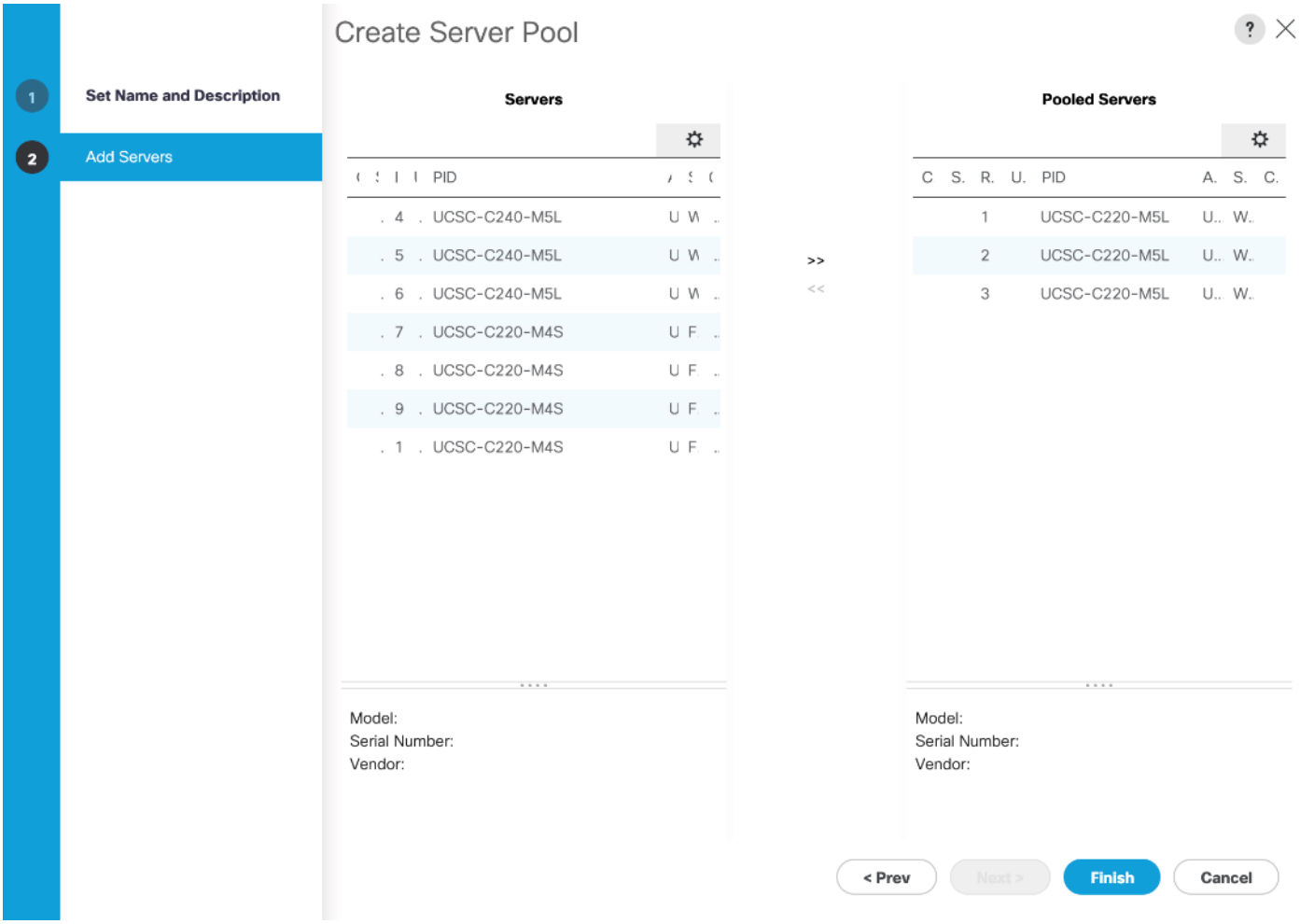
To configure the necessary server pool for the Cisco UCS environment, follow these steps:

1. In Cisco UCS Manager, click the **Servers** tab in the navigation pane.
2. Select **Pools > root** > Sub-Organizations > CV-ScaleProtect.
3. Right-click **Server Pools**.
4. Select Create Server Pool.
5. Enter `CVLT_SP_C220_M5` as the name of the server pool.
6. **Optional:** Enter a description for the server pool.

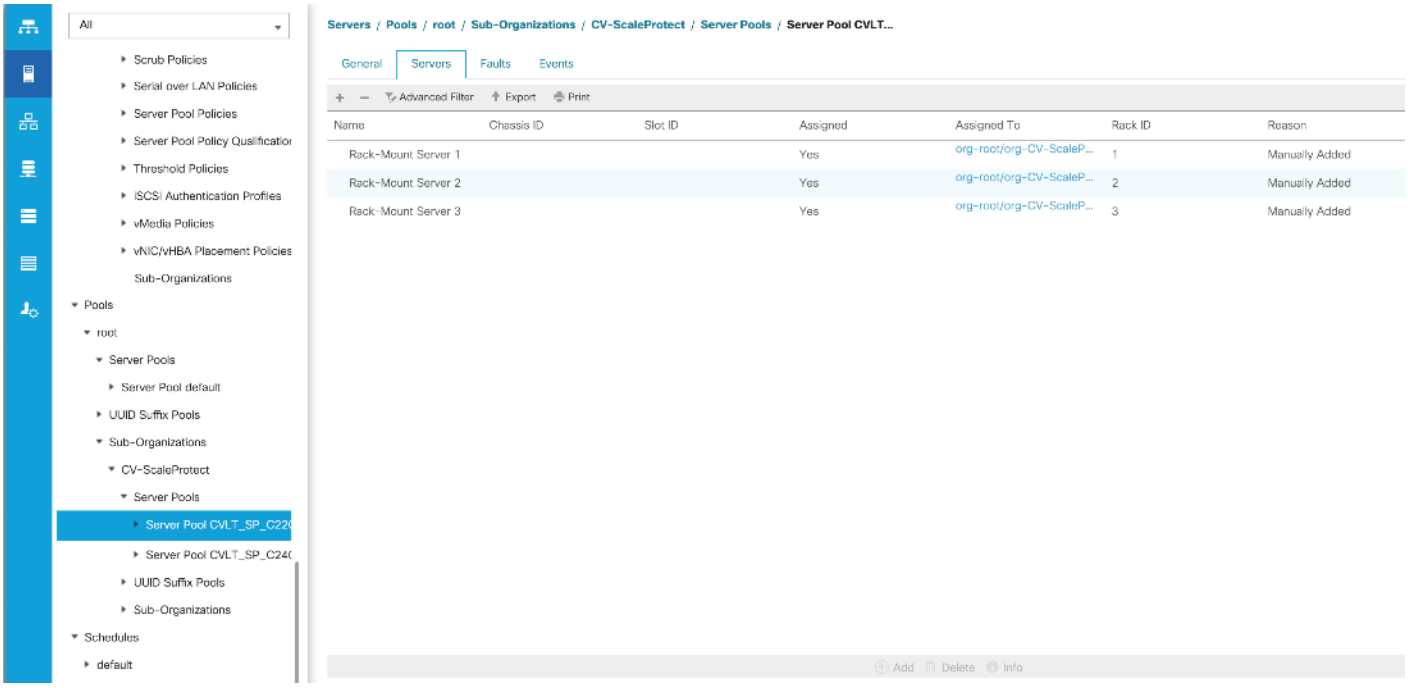


7. Click **Next**.

8. Select C220 M5 server nodes and click **>>** to add them to the `CVLT_SP_C220M5` server pool.



9. Click **Finish**.
10. Click **OK**.
11. Verify that the server pools have been created.

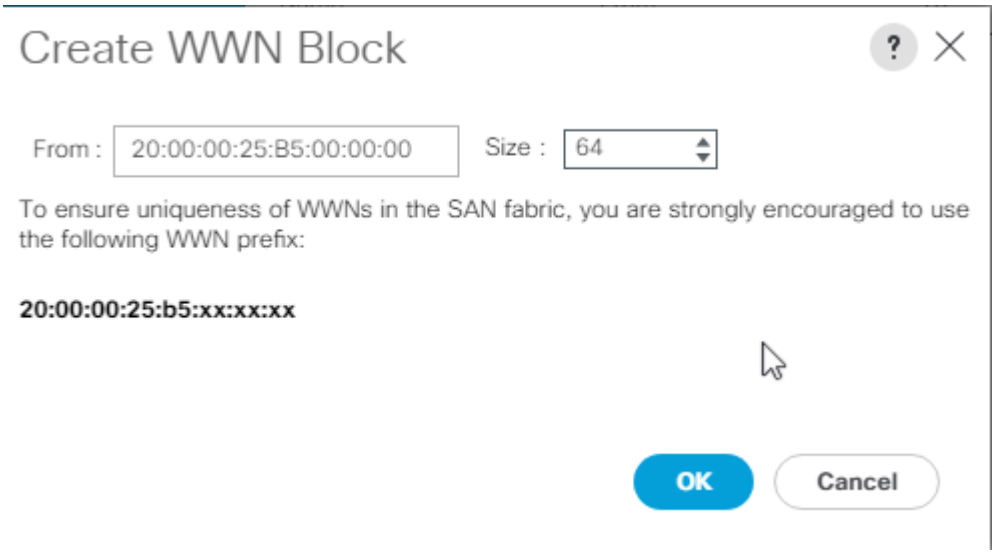


Optional: Create a WWNN Address Pool for FC-based Storage Access

This configuration step can be skipped if the UCS environment does not need to access storage environment using FC.

For FC connectivity to SAN fabrics, create a World Wide Node Name (WWNN) pool by following these steps:

1. In Cisco UCS Manager, click the **SAN** tab in the navigation pane.
2. Select **Pools** > **root**.
3. Right-click **WWNN Pools** under the root organization and choose **Create WWNN Pool** to create the WWNN address pool.
4. Enter `WWNN-Pool` as the name of the WWNN pool.
5. **Optional**: Enter a description for the WWNN pool.
6. Select the Sequential Assignment Order and click **Next**.
7. Click **Add**.
8. Specify a starting WWNN address.
9. Specify a size for the WWNN address pool that is sufficient to support the available blade or rack server resources. Each server will receive one WWNN.



10. Click **OK** and click **Finish**.

11. In the confirmation message, click **OK**.

Optional: Create a WWPN Address Pools for FC-based Storage Access

This configuration step can be skipped if the UCS environment does not need access to storage environment using FC.

For FC connectivity to SAN fabrics, create a World Wide Port Name (WWPN) pool for each SAN switching fabric by following these steps:

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

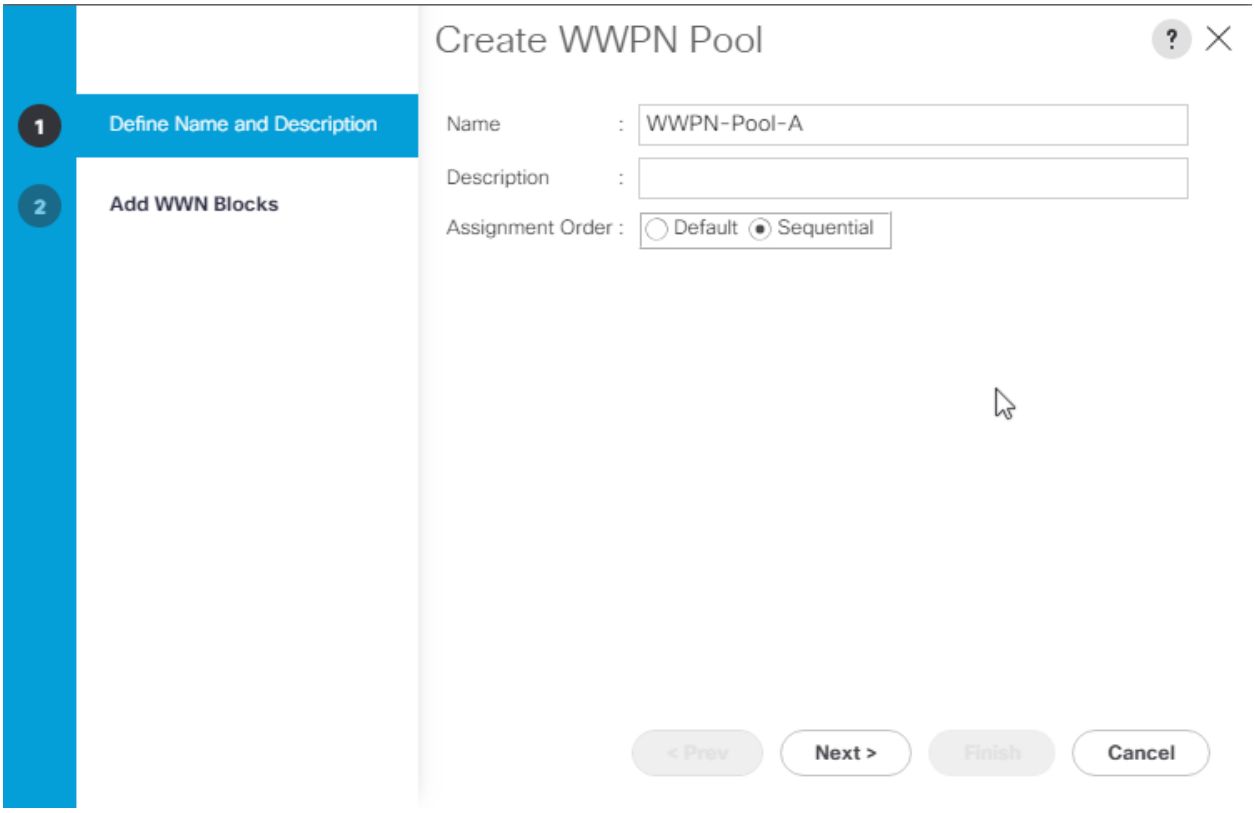
2. Select **Pools** > **root**.

3. Right-click **WWPN Pools** under the root organization and choose **Create WWPN Pool** to create the first WWPN address pool.

4. Enter WWPN-Pool-A as the name of the WWPN pool.

5. **Optional**: Enter a description for the WWPN pool.

6. Select the Sequential Assignment Order and click **Next**.

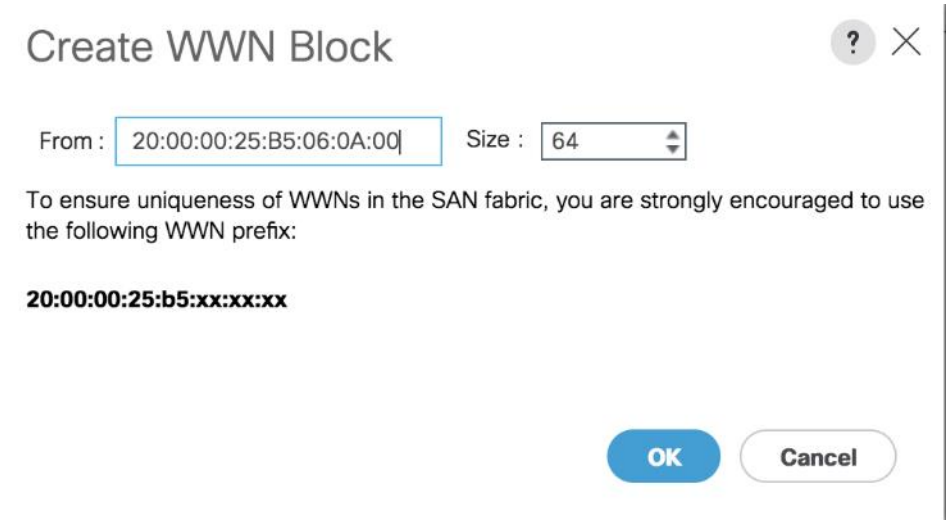


7. Click **Add**.

8. Specify a starting WWPN address.

It is recommended to place 0A in the second last octet of the starting WWPN address to identify all of the WWPN addresses as Fabric A addresses.

9. Specify a size for the WWPN address pool that is sufficient to support the available blade or rack server resources. Each server's Fabric A vHBA will receive one WWPN from this pool.



10. Click **OK** and click **Finish**.
11. In the confirmation message, click **OK**.
12. Right-click **WWPN Pools** under the root organization and choose **Create WWPN Pool** to create the second WWPN address pool.
13. Enter `WWPN-Pool-B` as the name of the WWPN pool.
14. **Optional**: Enter a description for the WWPN pool.
15. Select the Sequential Assignment Order and click **Next**.
16. Click **Add**.
17. Specify a starting WWPN address.

It is recommended to place 0B in the second last octet of the starting WWPN address to identify all of the WWPN addresses as Fabric B addresses.

18. Specify a size for the WWPN address pool that is sufficient to support the available blade or rack server resources. Each server's Fabric B vHBA will receive one WWPN from this pool.

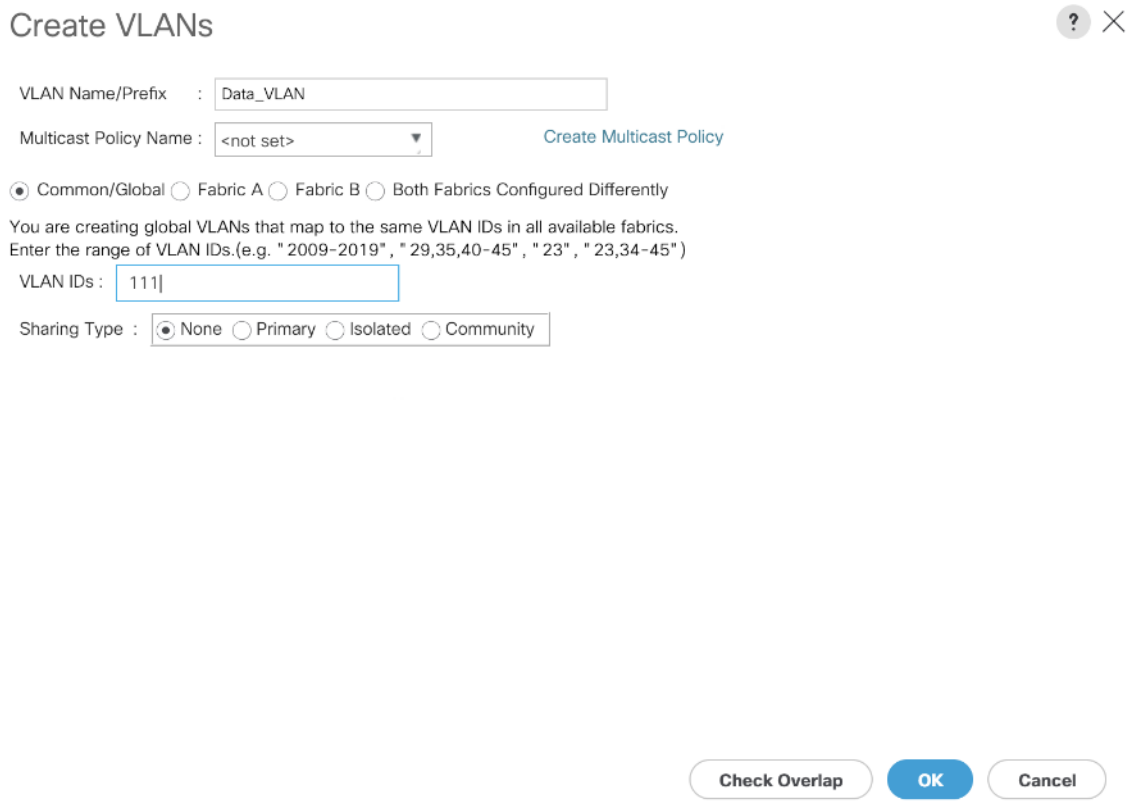
19. Click **OK** and click **Finish**.
20. In the confirmation message, click **OK**.

Create VLANs

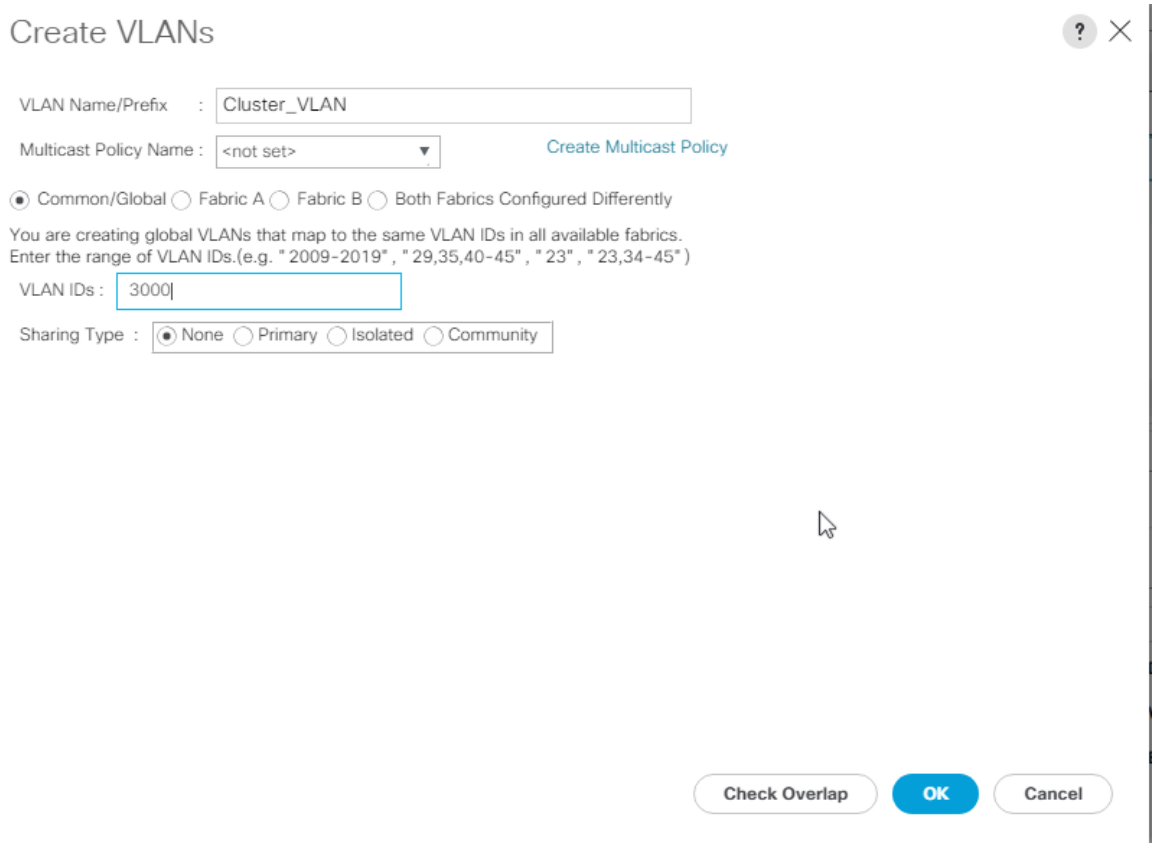
To configure the necessary virtual local area networks (VLANs) for the Cisco UCS ScaleProtect environment, follow these steps:

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

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



8. Click **OK** and then click **OK** again.
9. Repeat steps 3-8 to add Cluster VLAN as shown below:

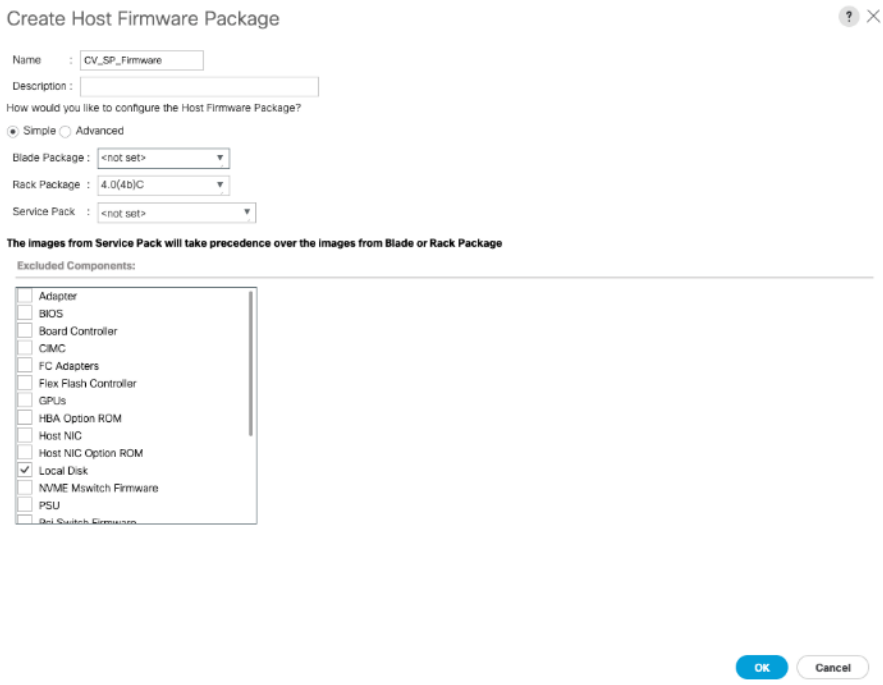


Create Host Firmware Package

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 > Sub-Organizations > CV-ScaleProtect.
3. Expand Host Firmware Packages.
4. Right-click and Select Create Host Firmware Package.
5. Enter name as `CV_SP_Firmware`
6. Select the version `4.0(4b)C` for Rack Packages.



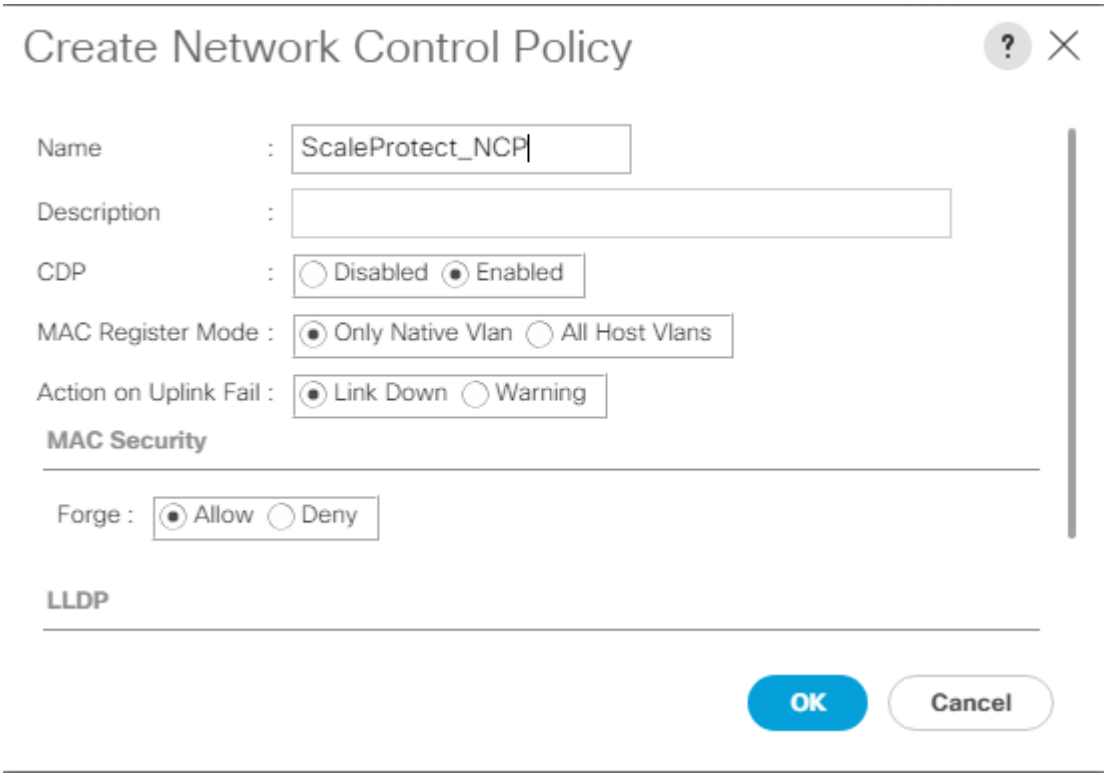
7. Click **OK** to add the host firmware package.

The Local disk is excluded by default in host firmware policy as a safety feature. Un-Exclude Local Disk within the firmware policy during initial deployment, only if drive firmware is required to be upgraded and is not at the minimum firmware level. Keep it excluded for any future updates and update the drives manually if required.

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 >Sub-Organization > CV-ScaleProtect.
3. Right-click Network Control Policies.
4. Select Create Network Control Policy.
5. Enter `ScaleProtect_NCP` as the policy name.
6. For CDP, select the `Enabled` option.
7. For LLDP, scroll down and select Enabled for both Transit and Receive.
8. Click **OK** to create the network control policy.

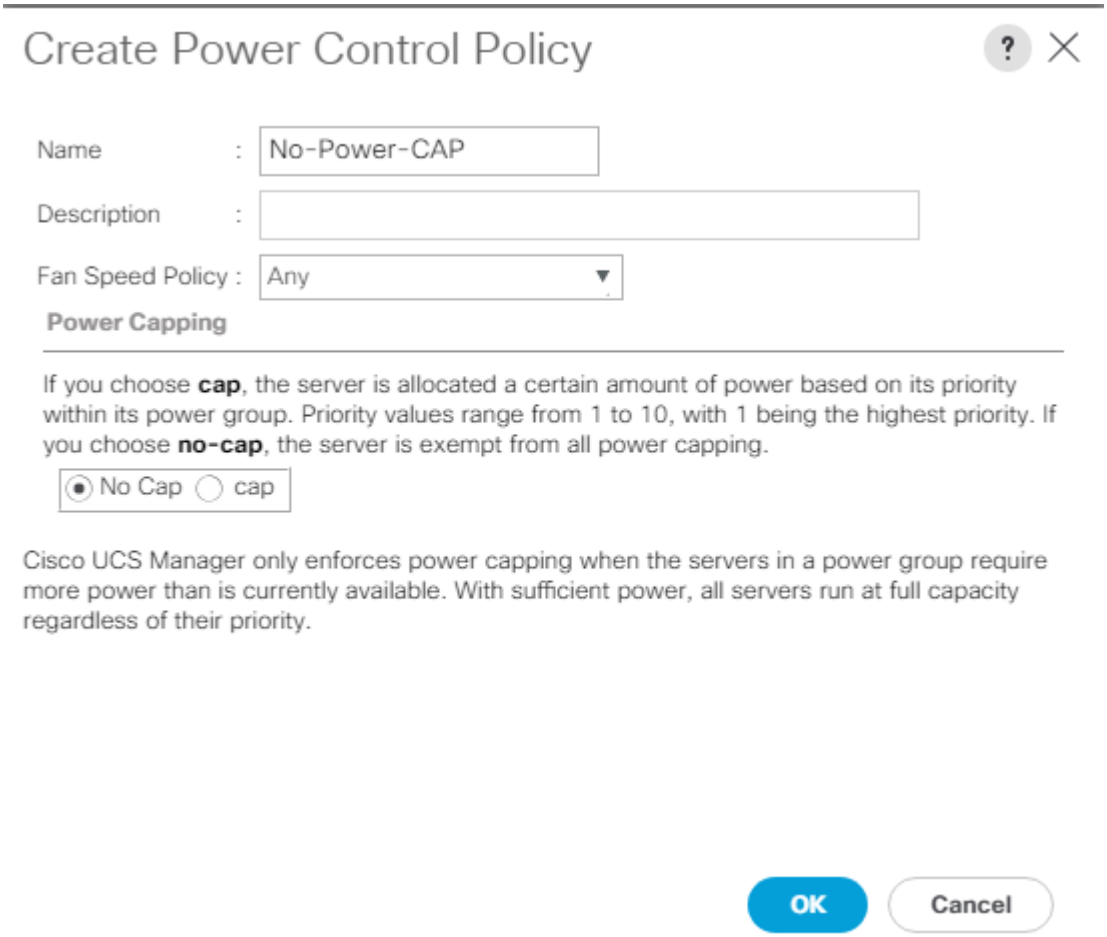


9. Click **OK**.

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. Select **Policies > root >Sub-Organizations > CV-ScaleProtect**.
2. Right-click Power Control Policies.
3. Select Create Power Control Policy.
4. Enter `No-Power-Cap` as the power control policy name.
5. Change the power capping setting to `No Cap`.
6. Click **OK** to create the power control policy.

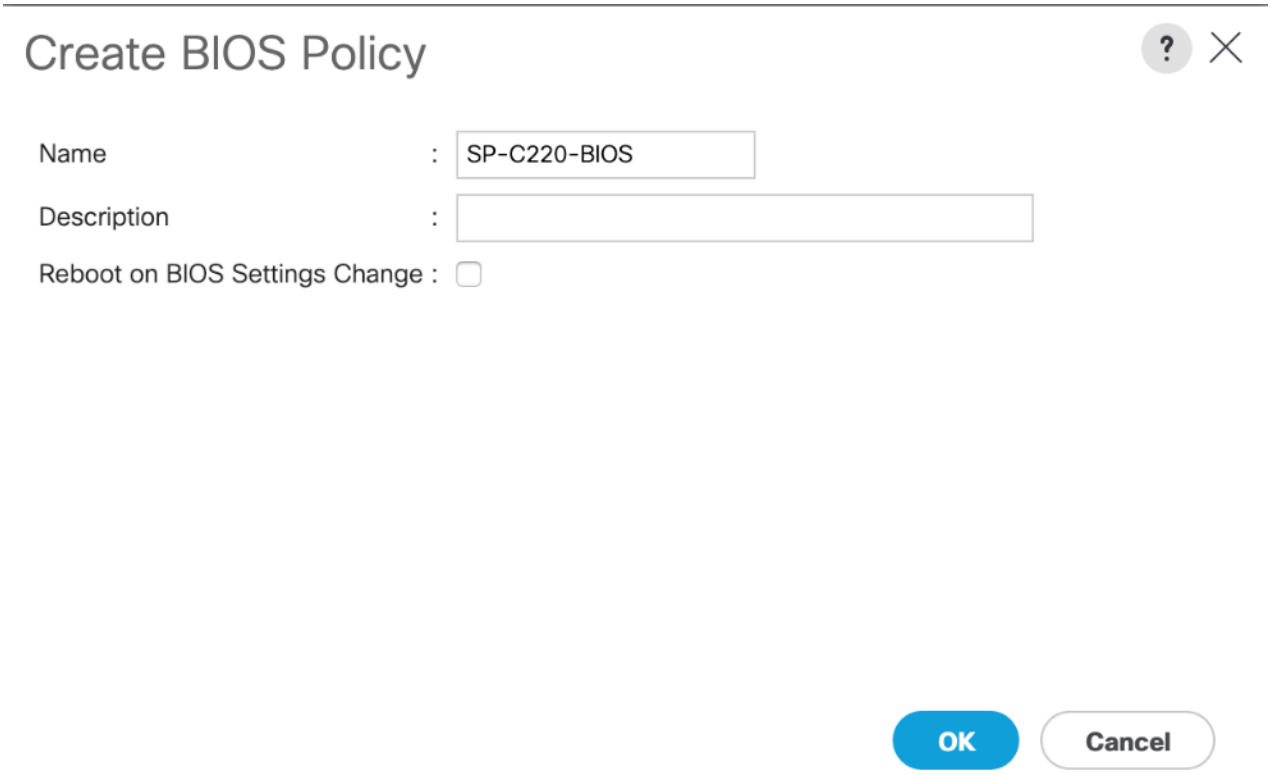


7. Click **OK**.

Create Server BIOS Policy

To create a server BIOS 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 > sub-Organizations > CV-ScaleProtect.
3. Right-click **BIOS Policies**.
4. Select Create BIOS Policy.
5. Enter `SP-C220-BIOS` as the BIOS policy name.

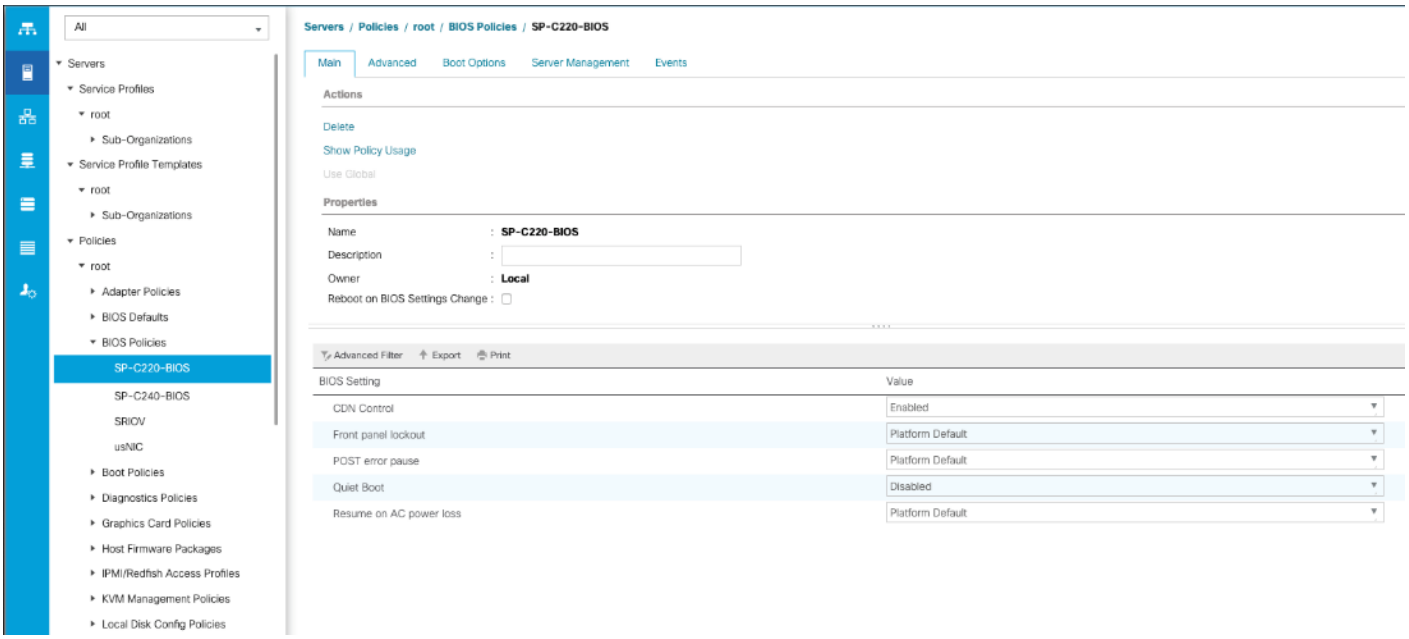


6. Click **OK**.

7. Select the newly created BIOS Policy.

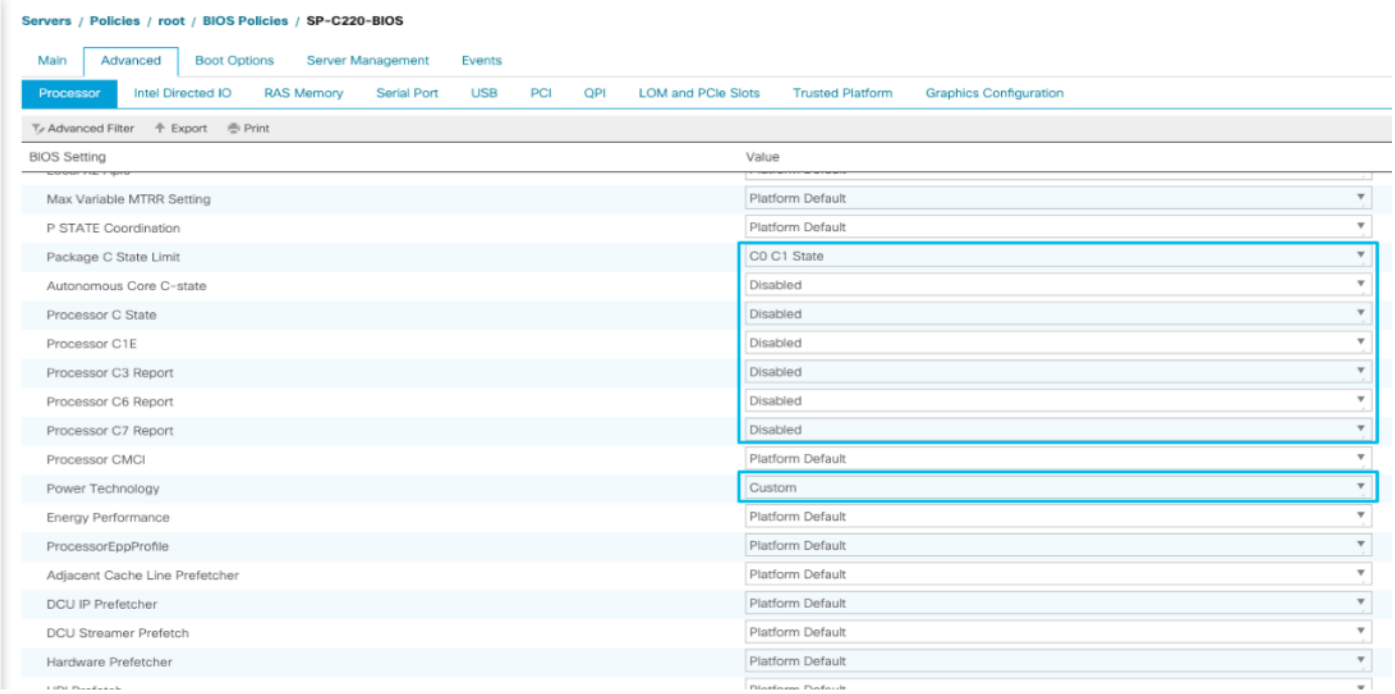
8. Change the Quiet Boot setting to `disabled`.

9. Change Consistent Device Naming to `enabled`.



10. Click **Advanced** tab and then select Processor.

11. From the **Processer** tab, make changes as shown below.



12. Change the Workload Configuration to `IO Sensitive` on the same page.

13. Click Save Changes.

Create 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 > sub-Organizations > CV-ScaleProtect.

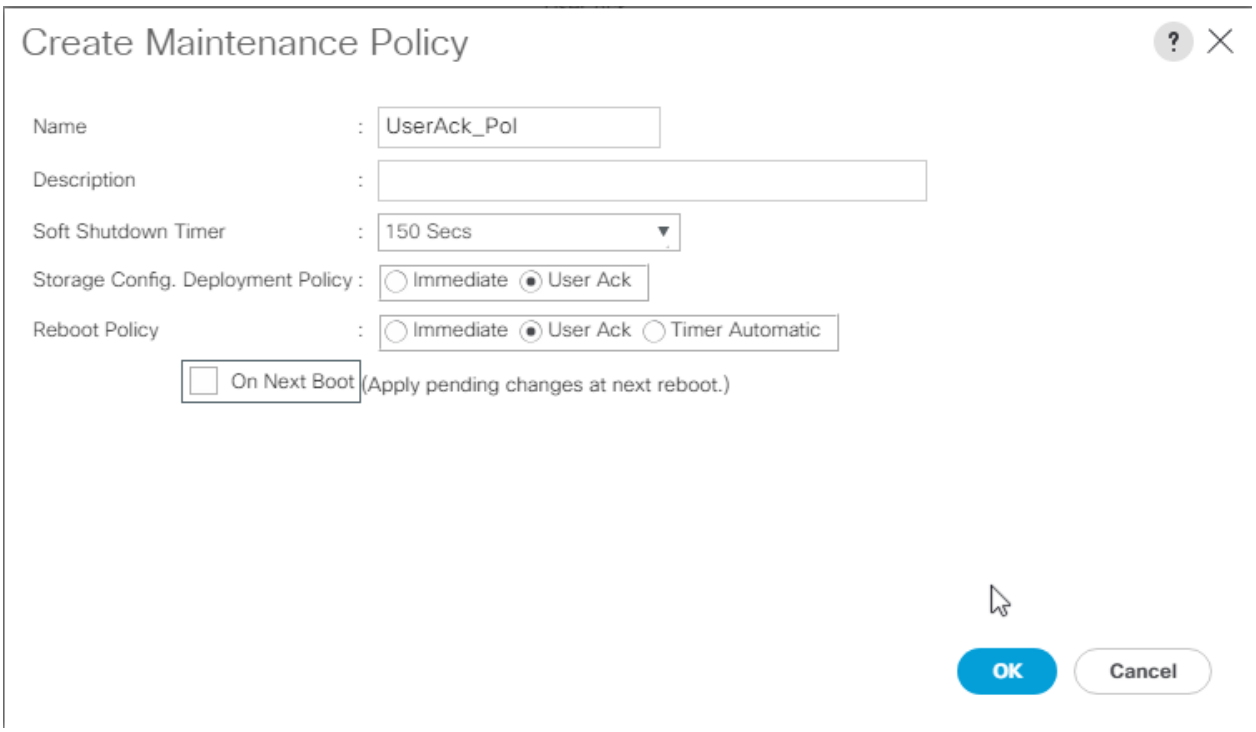
3. Right-click **Maintenance Policies** and Select Create Maintenance Policy.

4. Enter `UserAck_Pol` as the Maintenance Policy name

5. Change the Reboot Policy to `User Ack`.

6. Optional: Click "`On Next Boot`" to delegate maintenance windows to server owners.

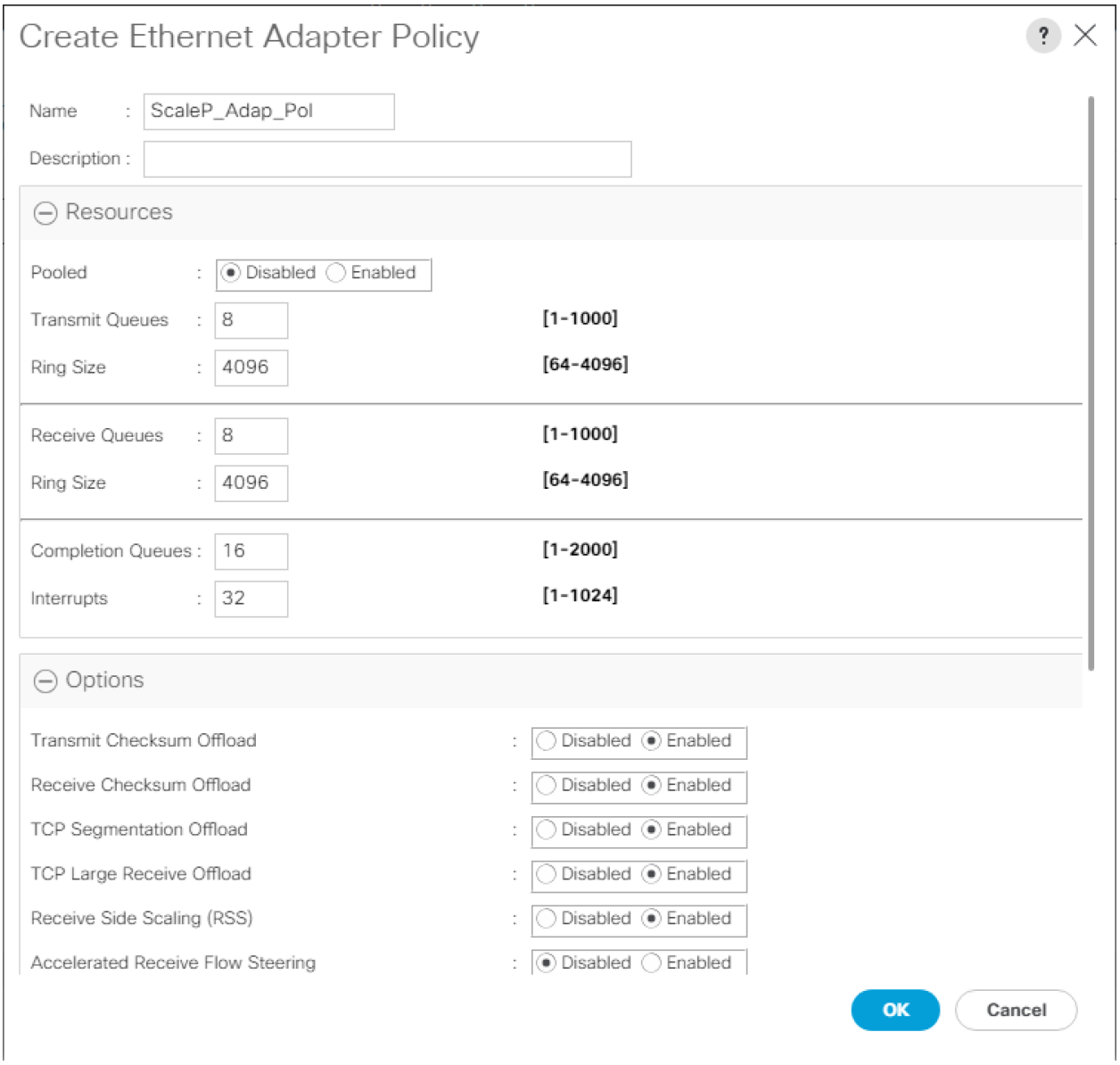
7. Click **OK**.



Create Adapter Policy

To create adaptor policy, follow these steps:

1. In Cisco UCS Manager, click the **Servers** tab in the navigation pane.
1. Select Policies > root > Sub-Organizations > CV-ScaleProtect.
2. Right-click **Adapter Policies** and Select Ethernet Adaptor Policy.
3. Enter name as `ScaleP_Adap_Pol`.
4. Enter Transmit Queues = `8`, Receive Queues = **8** , Ring Size = `4096`.
5. Enter Completion Queues = `16` and Interrupts = `32`.
6. Under **Options**, make sure Receive Side Scaling (RSS) is enabled.
7. Click **OK**.



To enable maximum throughout, it is recommended to change the default size of Rx and Tx Queues. RSS should be enabled, since it allows the distribution of network receive processing across multiple CPUs in a multiprocessor system.

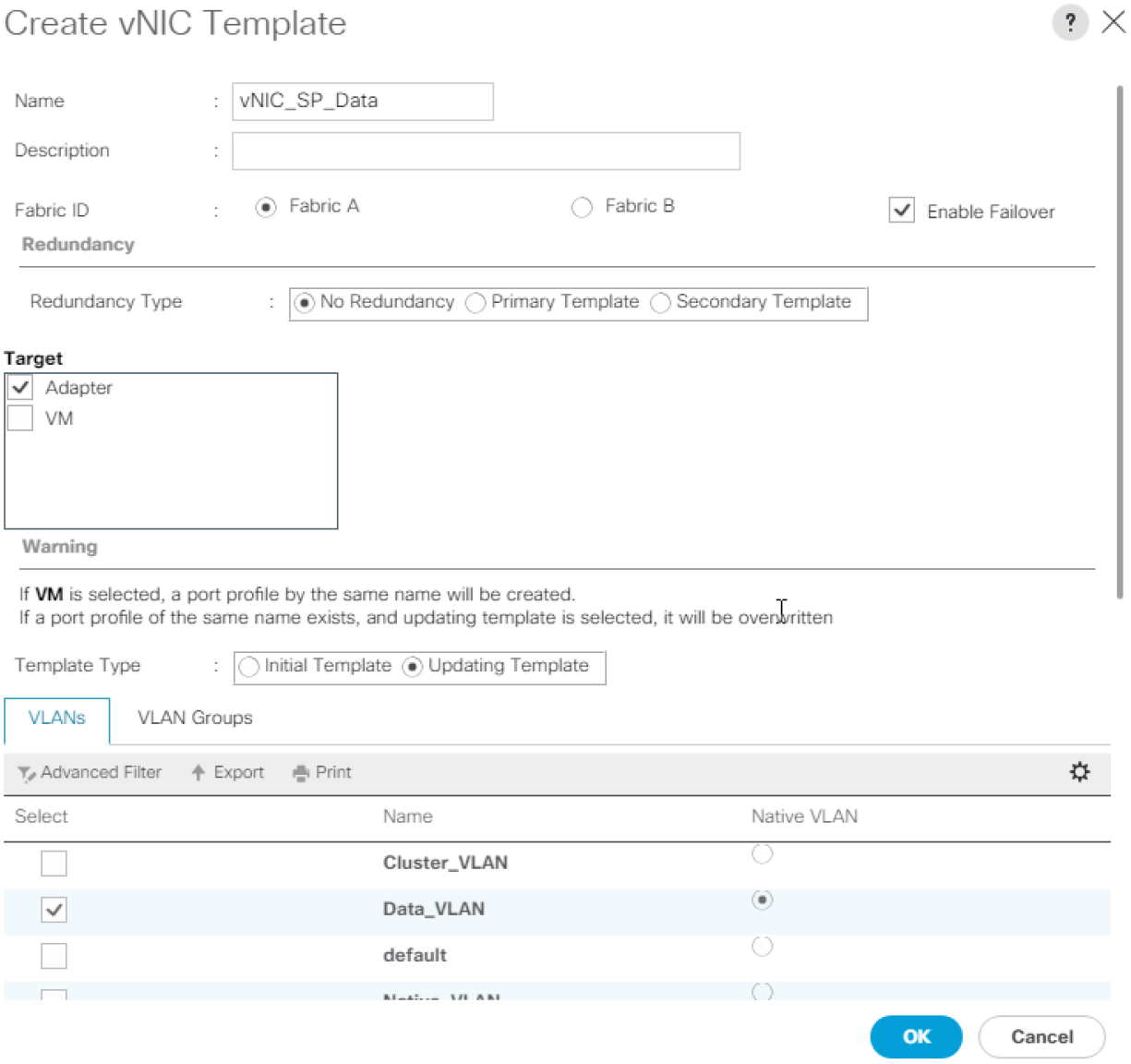
Create vNIC Templates

To create multiple virtual network interface card (vNIC) templates for the Cisco UCS environment, follow these steps. A total of 2 vNIC Templates will be created:

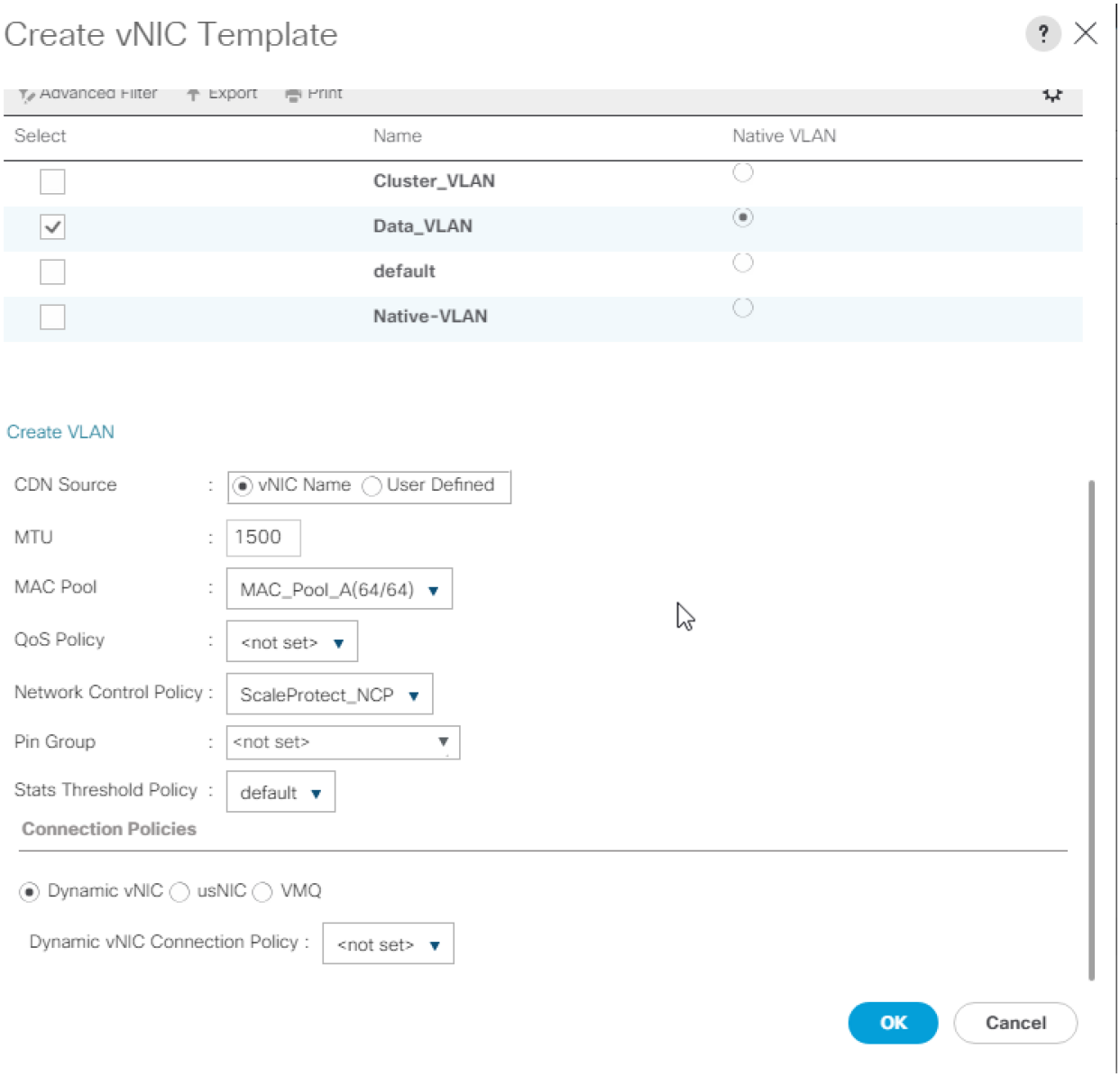
- **vNIC_data** – ScaleProtect Data Protection and Management vNIC. This vNIC provides management access and enables communication from backup clients to ScaleProtect Cluster.
- **vNIC_cluster** - ScaleProtect Cluster vNIC. This vNIC provides communication with in ScaleProtect Cluster for Cluster related traffic.

Create Data and Cluster vNICs

1. In Cisco UCS Manager, click the **LAN** tab in the navigation pane.
2. Select Policies > root > Sub-Organizations > CV-ScaleProtect.
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter `vNIC_SP_Data` as the vNIC template name.
6. Keep `Fabric A` selected.
7. Select the `Enable Failover` checkbox.
8. Select Updating Template as the Template Type.
9. Select Redundancy Type as `No Redundancy`
10. Under VLANs, select the checkbox for `Data_VLAN` VLAN.



11. Set Data_VLAN as the native VLAN.
12. For MTU, enter 1500.
13. In the MAC Pool list, select MAC_Pool_A.
14. In the Network Control Policy list, select ScaleProtect_NCP.



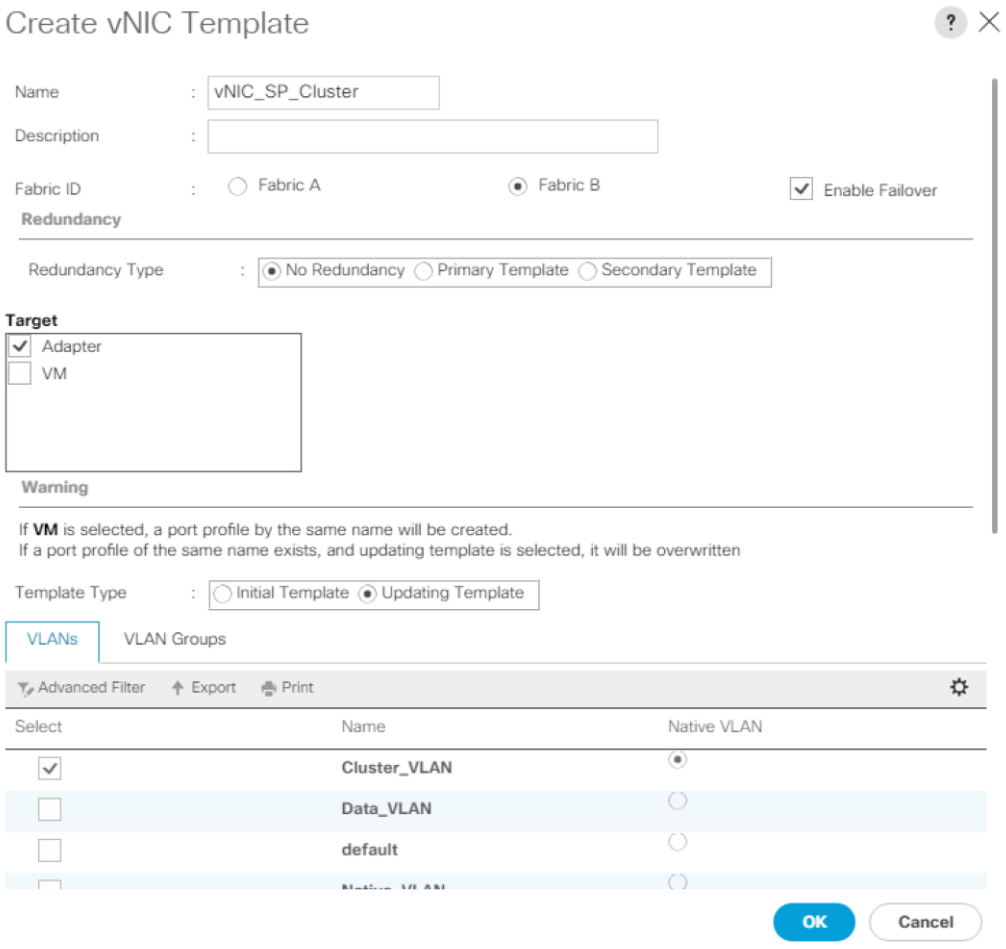
15. Click **OK** to create the vNIC template.
16. Click **OK**.

Use MTU 9000 for the backup network if possible and on all participating devices in the network (clients, switches, and servers). Use standard 1500 MTU if any connections or devices are not configured to support a larger MTU to prevent drops.

Follow these steps for Cluster VLAN template:

1. In the navigation pane, select the **LAN** tab.
2. Select Policies > root.
3. Right-click vNIC Templates.

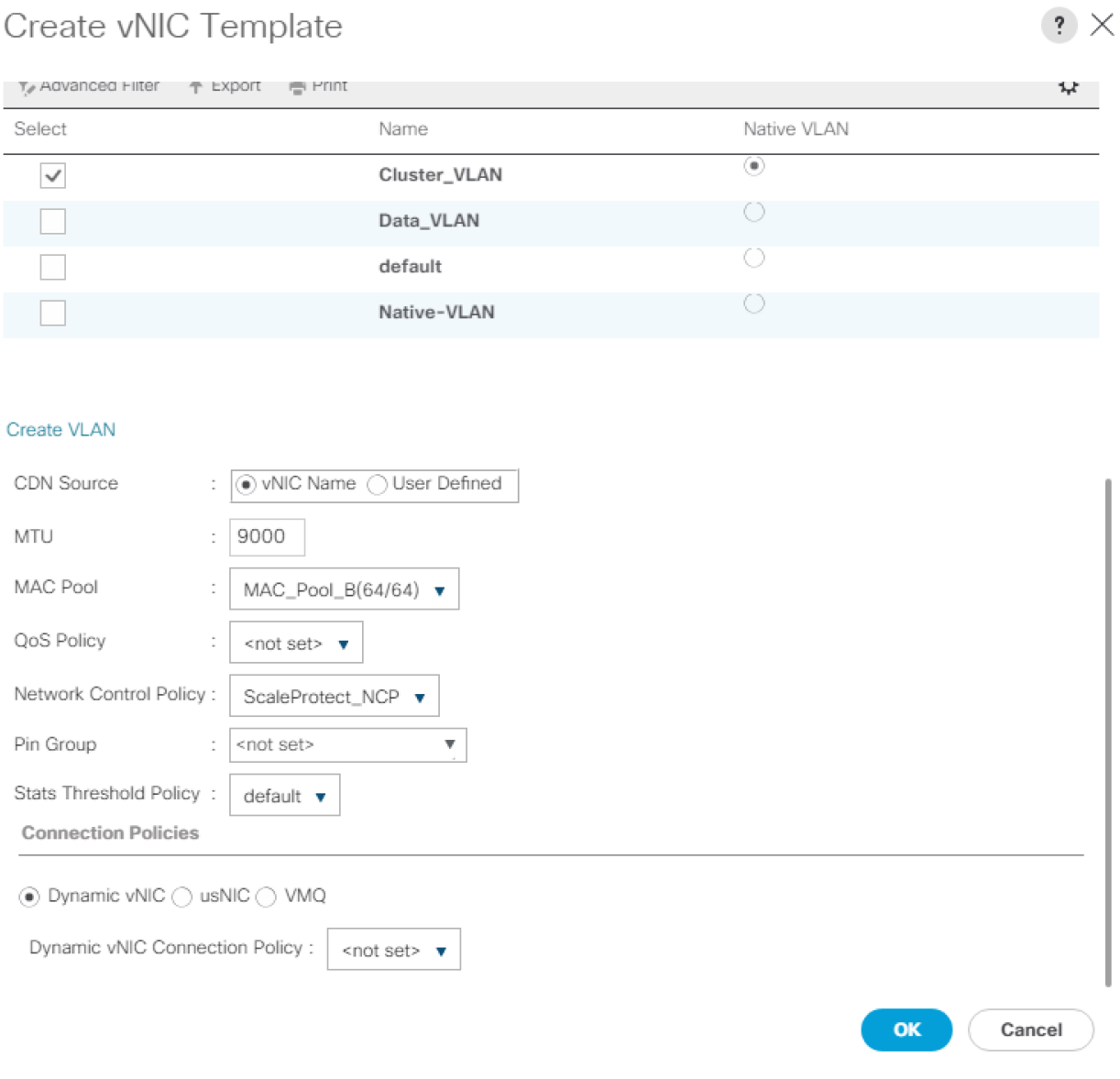
4. Select Create vNIC Template.
5. Enter `vNIC_SP_Cluster` as the vNIC template name.
6. Select `Fabric B`.
7. Select the Enable Failover checkbox.
8. Under Target, make sure the VM checkbox is not selected.
9. Select Redundancy Type as `No Redundancy`.
10. Select `Updating Template` as the template type.
11. Under VLANs, select the checkboxes for `Cluster_VLAN`.
12. Set Cluster_VLAN as the native VLAN.



13. Select `vNIC Name` for the CDN Source.
14. For MTU, enter `9000`.

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

16. In the Network Control Policy list, select `ScaleProtect_NCP`.



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

18. Click **OK**.

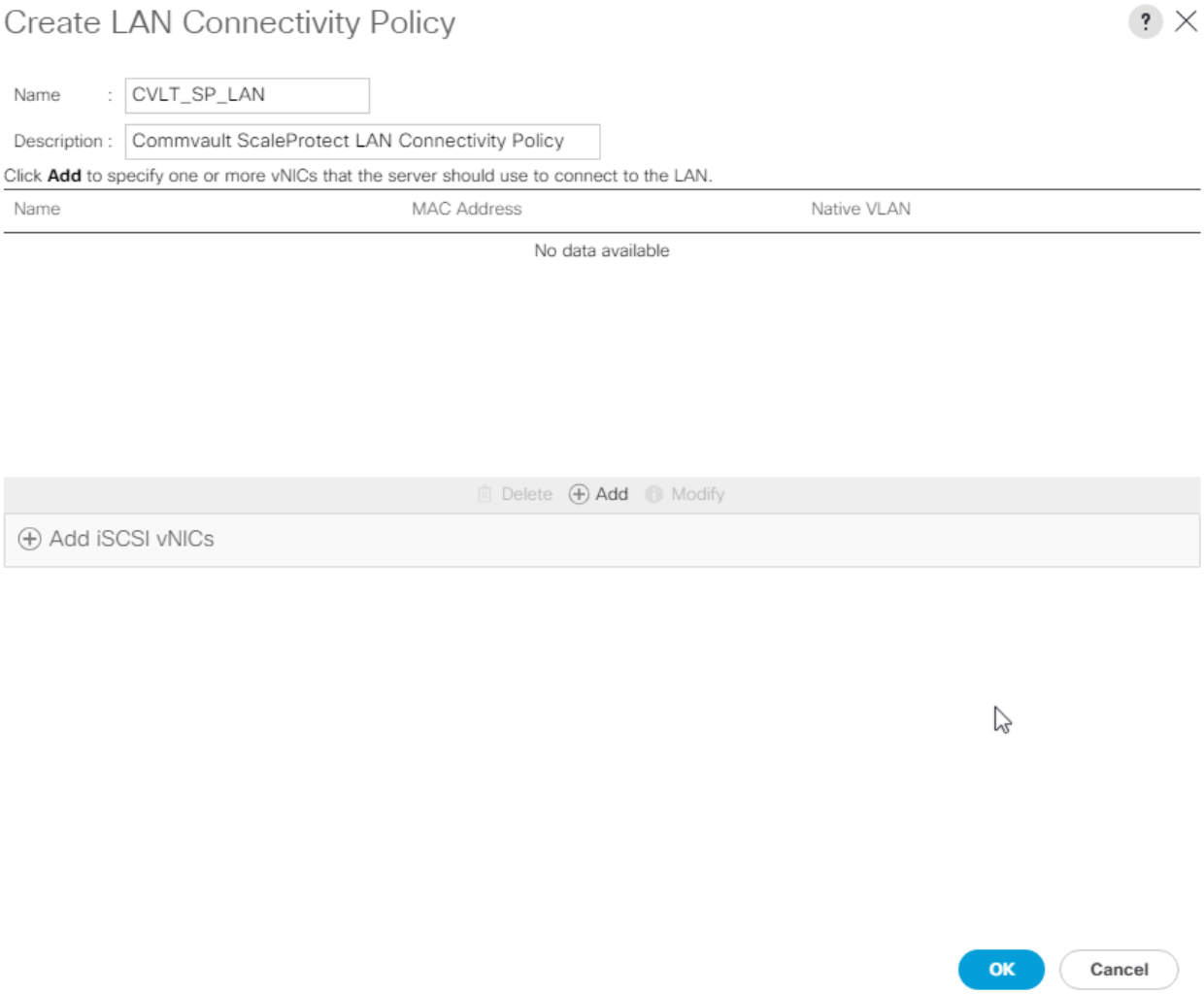
Create LAN Connectivity Policy

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

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

2. Select LAN > Policies > root > Sub-Organizations > CV-ScaleProtect.

3. Right-click LAN Connectivity Policies.
4. Select Create LAN Connectivity Policy.
5. Enter `CVLT_SP_LAN` as the name of the policy.

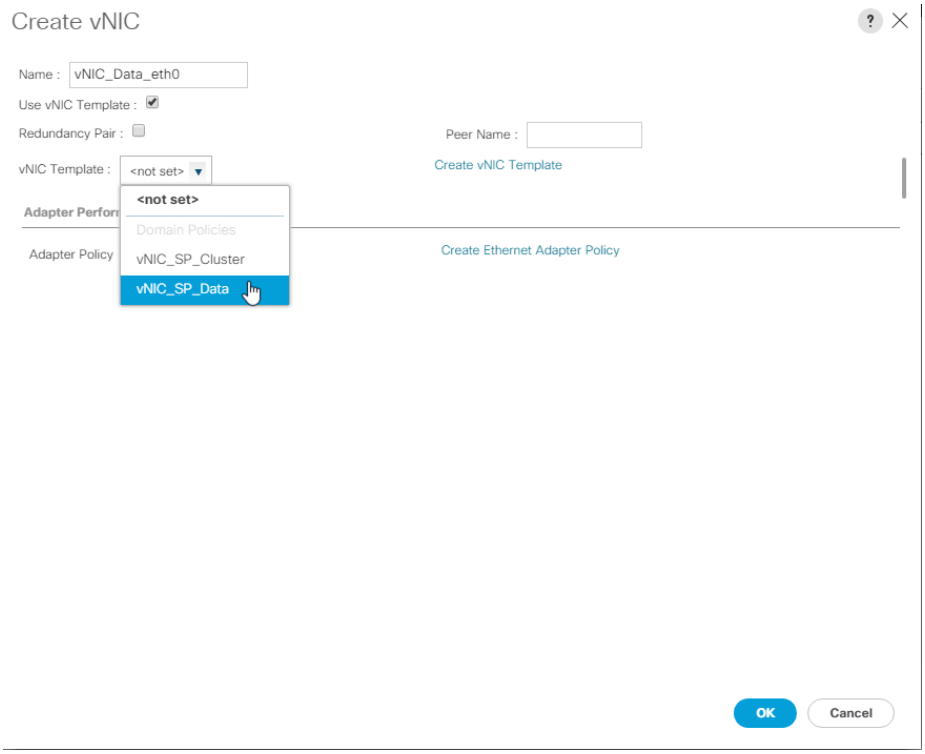


6. Click the upper **Add** button to add a vNIC.
7. In the **Create vNIC** dialog box, enter `vNIC_Data_eth0` as the name of the vNIC.

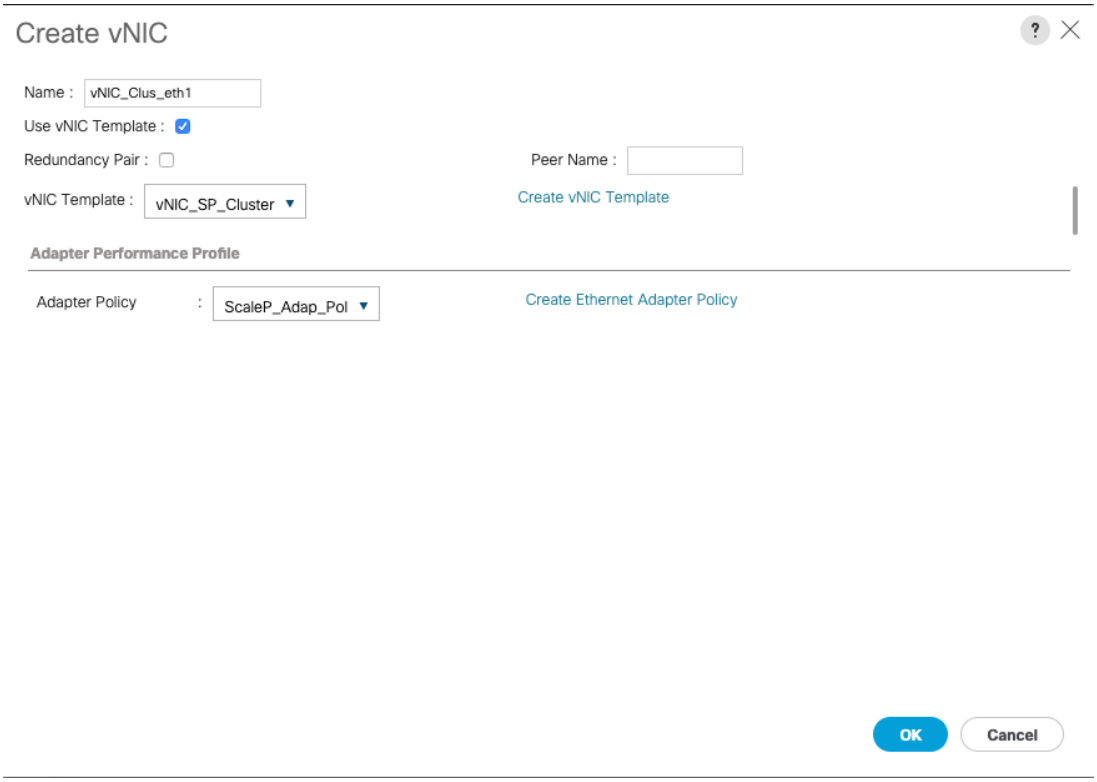
The numeric 0 and subsequent increment on the later vNIC are used in the vNIC naming to force the device ordering through Consistent Device Naming (CDN). Without this, some operating systems might not respect the device ordering that is set within Cisco UCS.

8. Select the Use vNIC Template checkbox.
9. In the vNIC Template list, select `vNIC_Data_eth0`.
10. In the Adapter Policy list, select `ScaleP_Adap_Pol`.

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

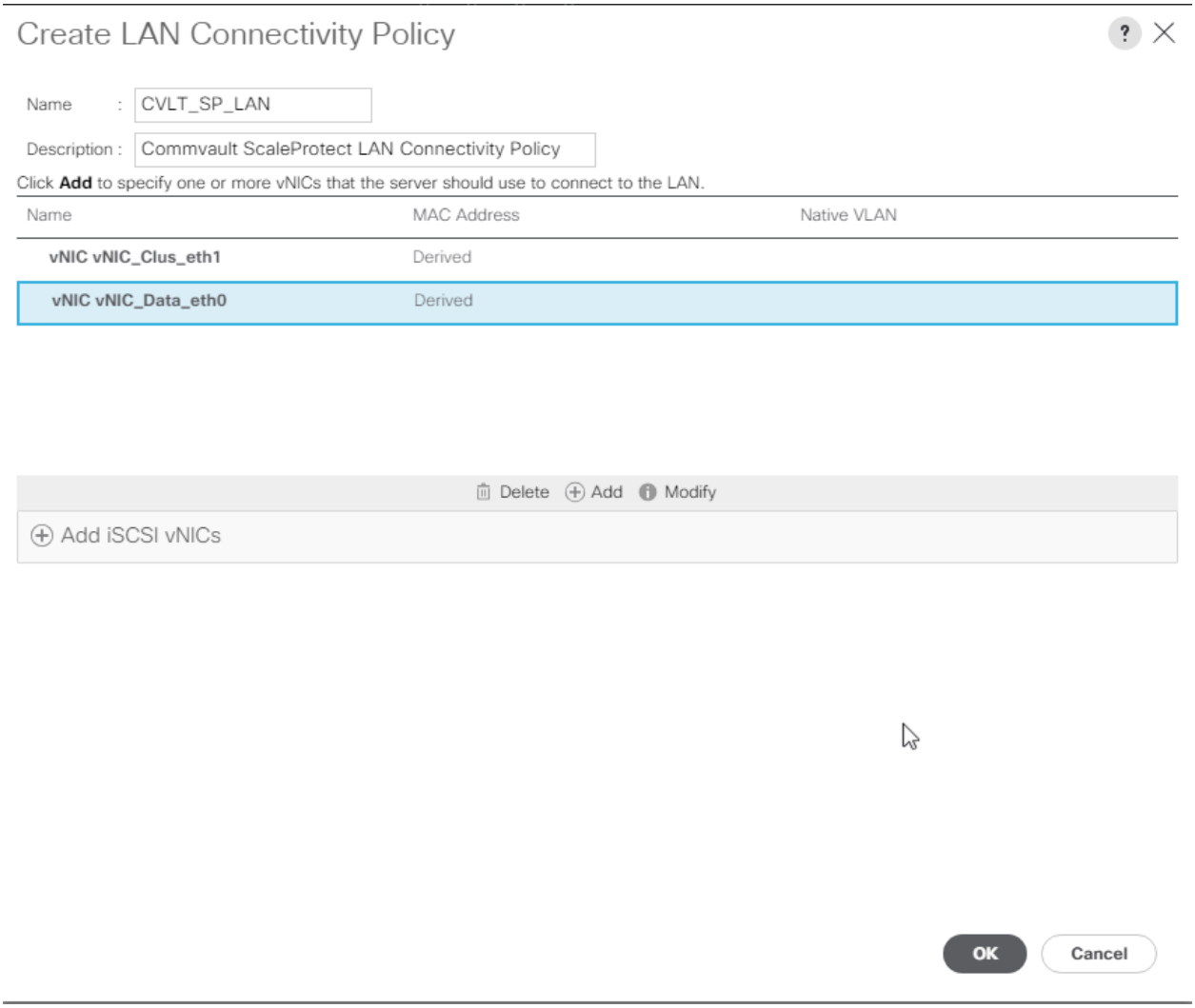


12. Click Add to add another vNIC to the policy.
13. In the Create vNIC box, `vNIC_Clus_eth1` as the name of the vNIC.
14. Select the Use vNIC Template checkbox.
15. In the vNIC Template list, select `vNIC_SP_Cluster`.
16. In the Adapter Policy list, select `ScaleP_Adap_Pol`.



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

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



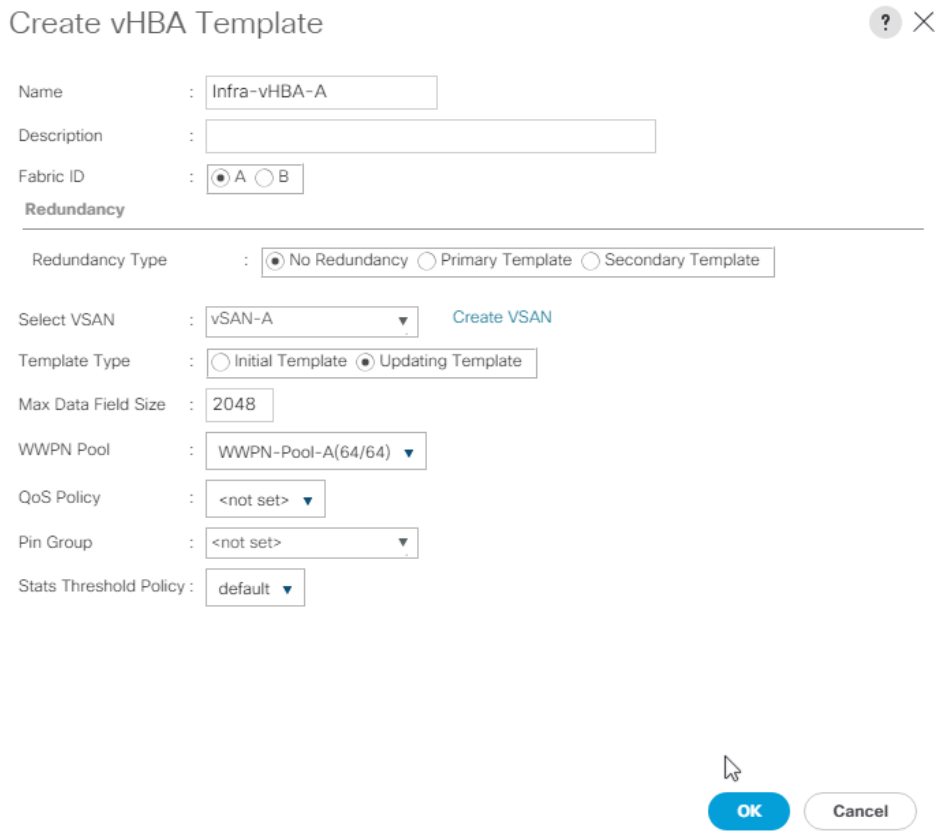
Optional: Create vHBA Templates for FC Connectivity

This configuration step can be skipped if the ScaleProtect UCS environment does not need to access storage infrastructure using FC SAN.

To create virtual host bus adapter (vHBA) templates for the Cisco UCS environment, follow these steps:

1. In Cisco UCS Manager, click the **SAN** tab in the navigation pane.
2. Select Policies > root.
3. Right-click **vHBA Templates** and choose Create vHBA Template.
4. Enter `Infra-vHBA-A` as the vHBA template name.
5. Click the radio button to select `Fabric A`.
6. In the Select VSAN list, Choose `vsan-A`.

7. In the WWPN Pool list, Choose `WWPN-Pool-A`.



8. Click **OK** to create the vHBA template.

9. Click **OK**.

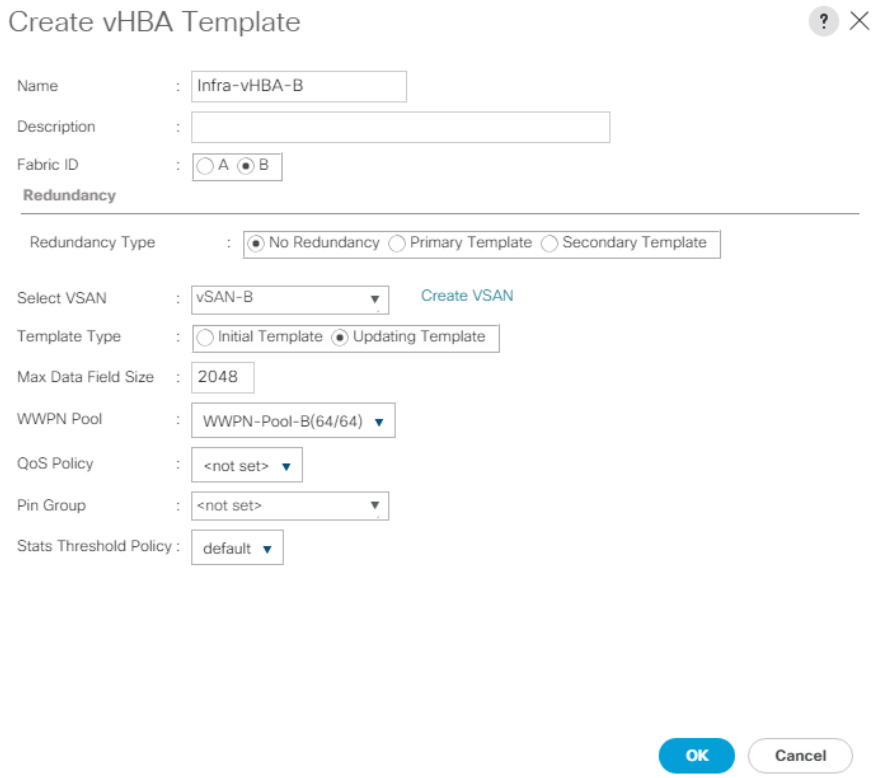
10. Right-click **vHBA Templates** again and choose Create vHBA Template.

11. Enter `Infra-vHBA-B` as the vHBA template name.

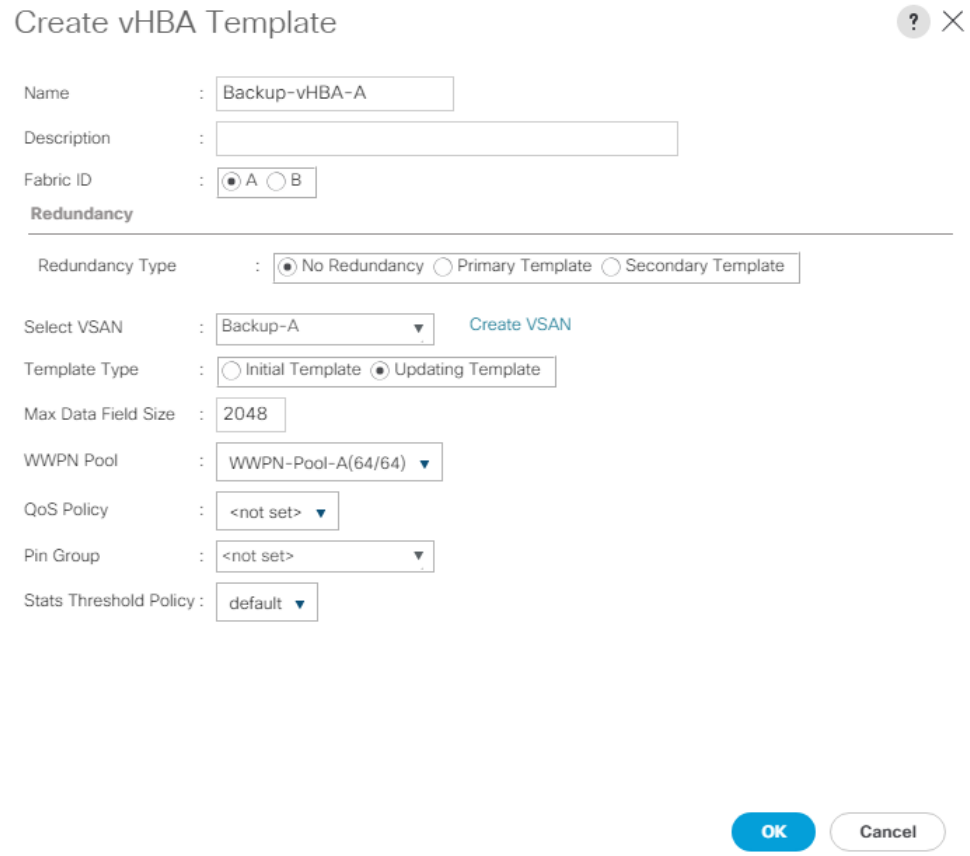
12. Click the radio button to select `Fabric B`.

13. In the Select VSAN list, Choose `VSAN-B`.

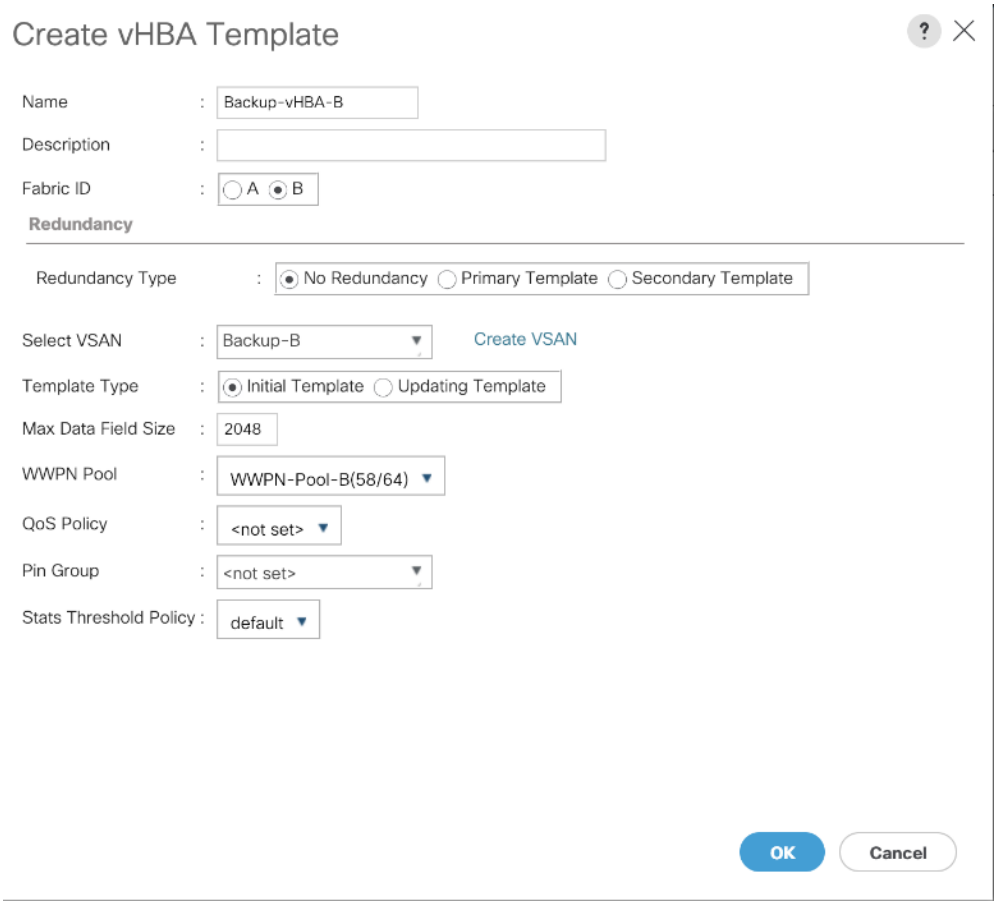
14. In the WWPN Pool, Choose `WWPN-Pool-B`.



15. Click **OK** to create the vHBA template.
16. Click **OK**.
17. In Cisco UCS Manager, click the **SAN** tab in the navigation pane.
18. Select Policies > root > Sub-Organizations > CV-ScaleProtect.
19. Right-click **vHBA Templates** and choose Create vHBA Template.
20. Enter `Backup-vHBA-A` as the vHBA template name.
21. Click the radio button to select `Fabric A`.
22. In the Select VSAN list, Choose `Backup-A`.
23. In the WWPN Pool list, Choose `WWPN-Pool-A`.



24. Click **OK** to create the vHBA template.
25. Click **OK**.
26. Right-click **vHBA Templates** again and choose Create vHBA Template.
27. Enter `Backup-vHBA-B` as the vHBA template name.
28. Click the radio button to select `Fabric B`.
29. In the Select VSAN list, Choose `Backup-B`.
30. In the WWPN Pool, Choose `WWPN-Pool-B`.



31. Click **OK** to create the vHBA template.

32. Click **OK**.

Optional: Create FC SAN Connectivity Policies

This configuration step can be skipped if the ScaleProtect Cisco UCS environment does not need to access storage environment using FC.

A SAN connectivity policy defines the vHBAs that will be created as part of a service profile deployment.

To configure the necessary FC SAN Connectivity Policies, follow these steps:

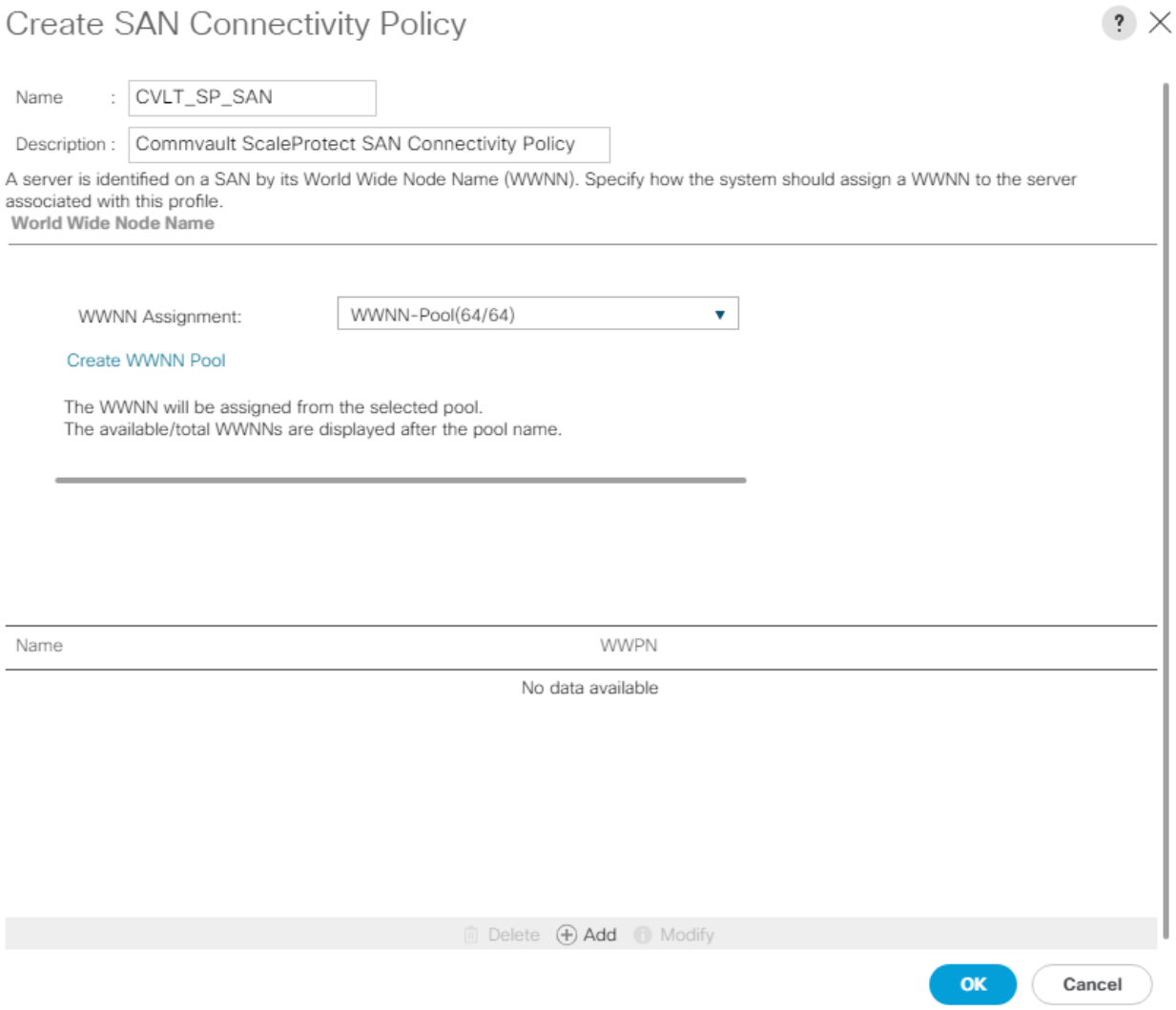
1. In Cisco UCS Manager, click the **SAN** tab in the navigation pane.

2. Select SAN > Policies > root >Sub-Organizations > CV-ScaleProtect.

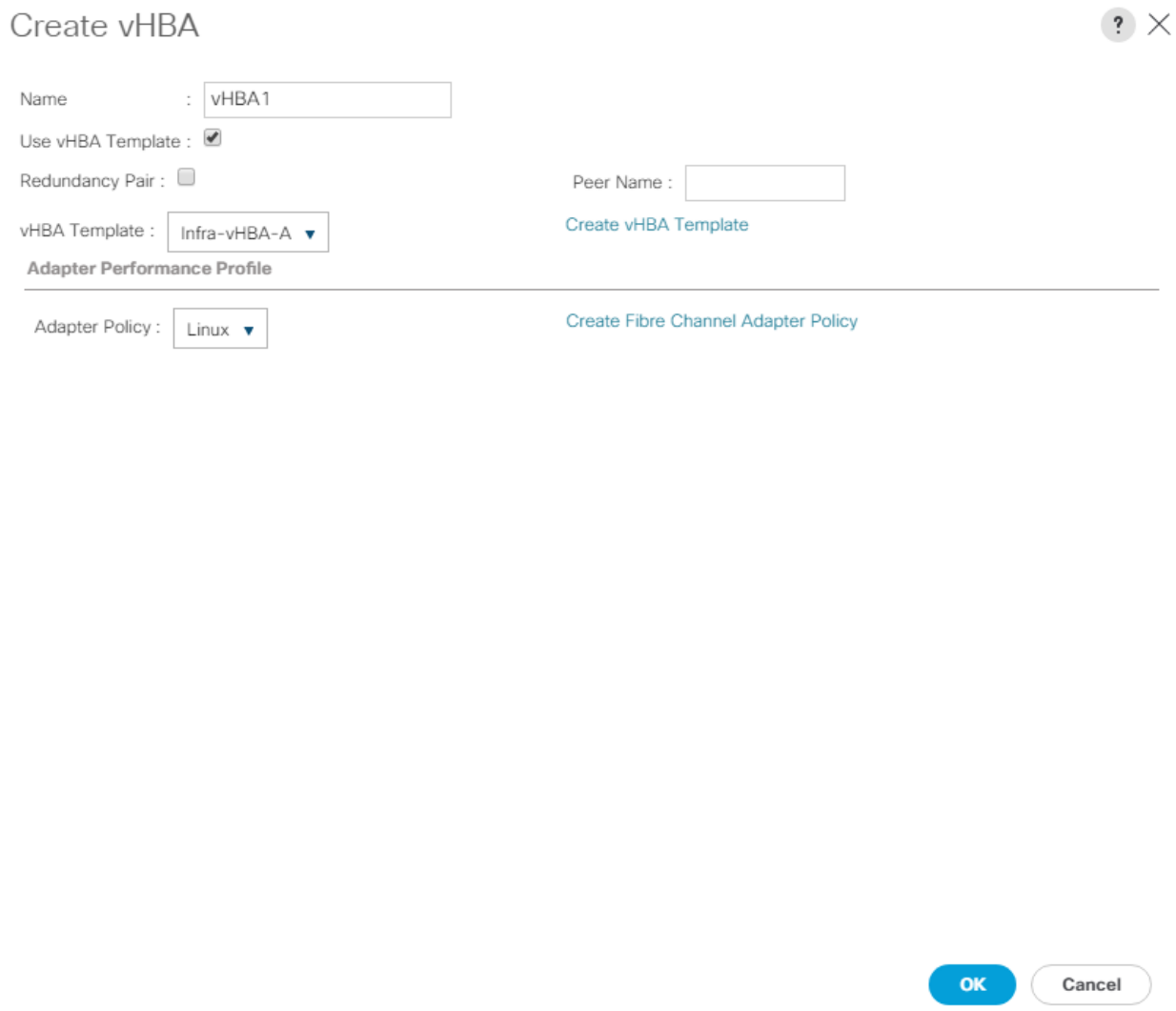
3. Right-click **SAN Connectivity Policies** and choose Create SAN Connectivity Policy.

4. Enter `CVLT_SP_SAN` as the name of the policy.

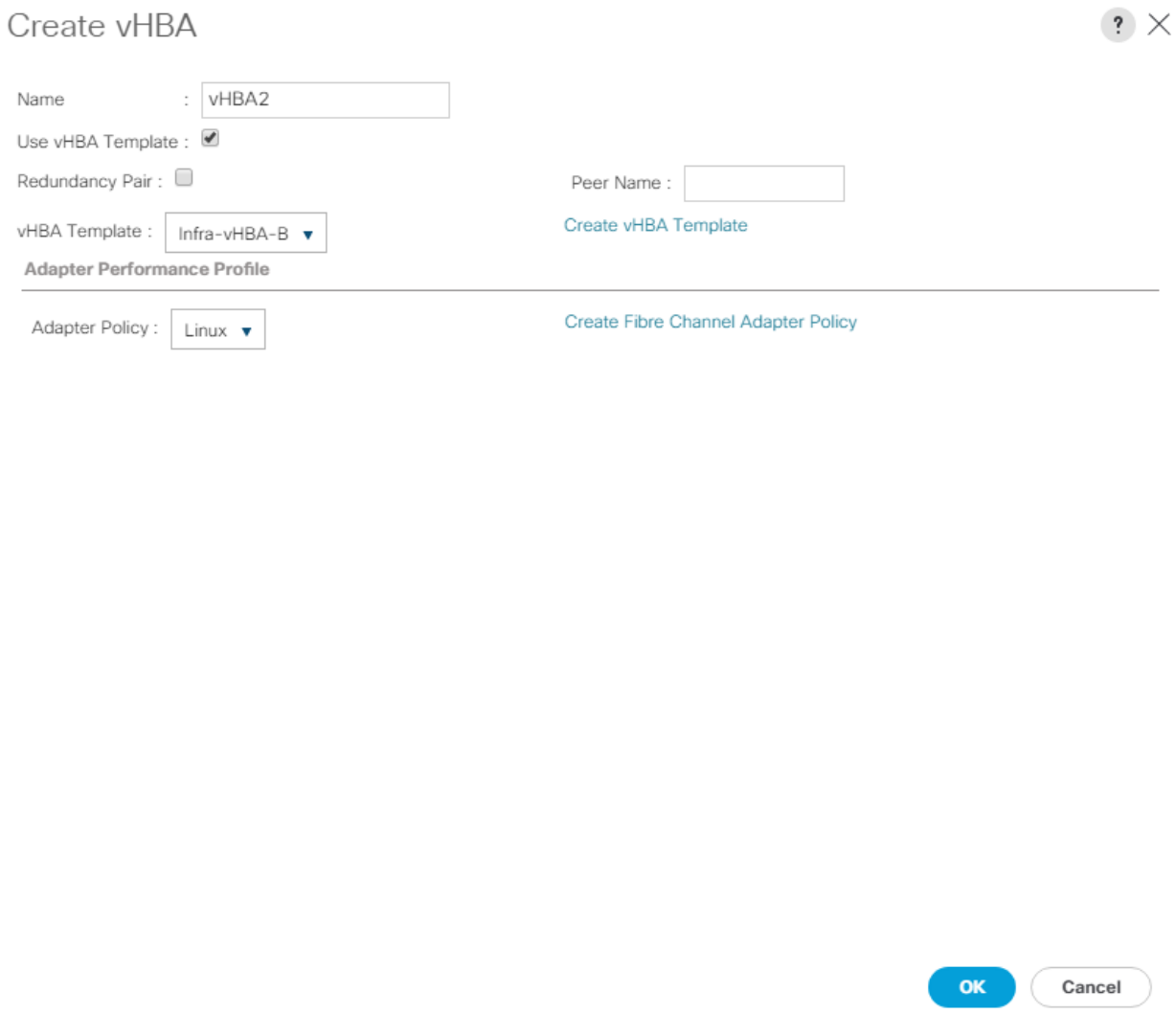
5. Select WWNN-Pool from the drop-down list under World Wide Node Name.



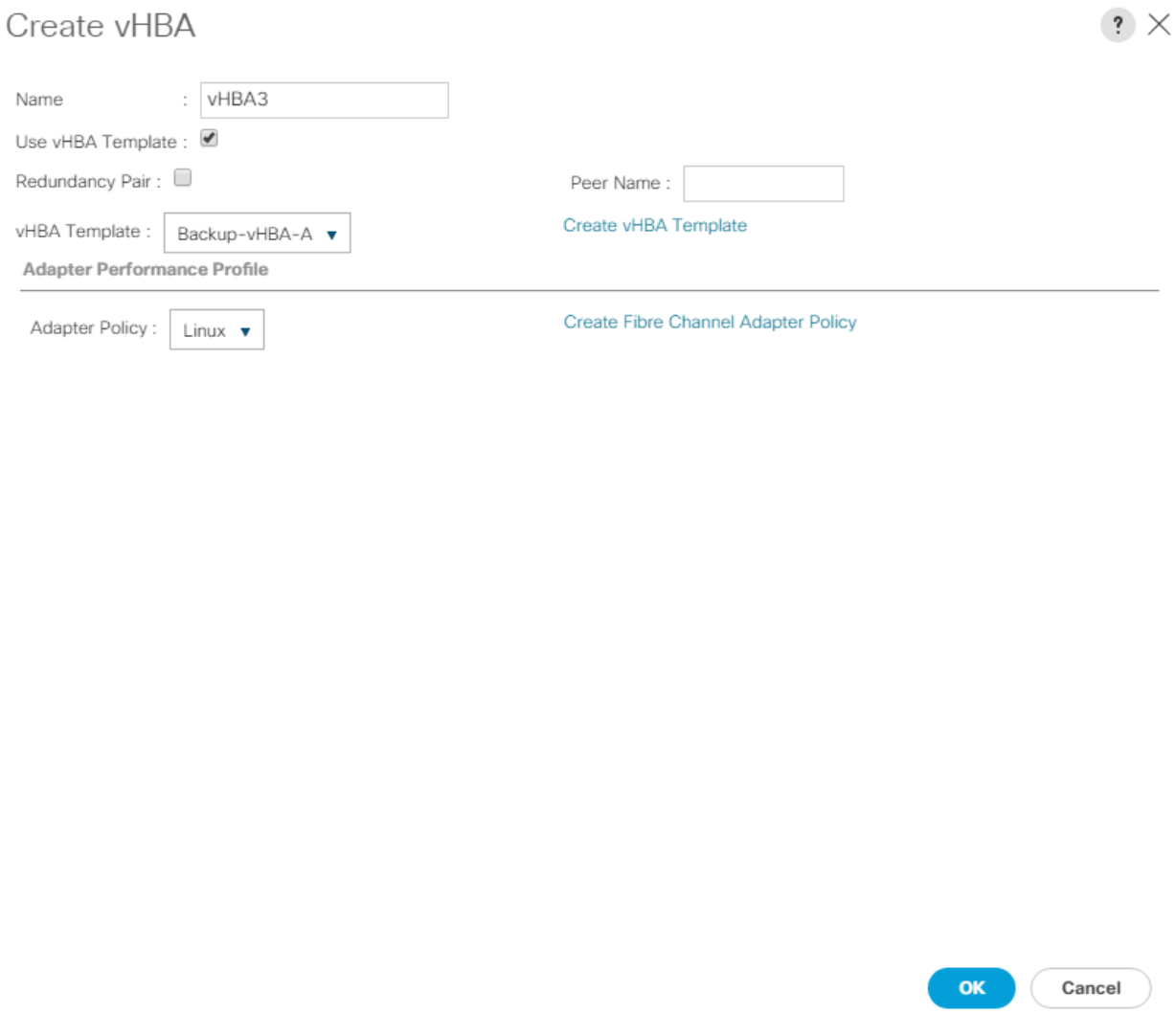
6. Click **Add**. You might have to scroll down the screen to see the Add link.
7. Under Create vHBA, enter `vHBA1` in the Name field.
8. Check the check box `Use vHBA Template`.
9. From the vHBA Template drop-down list, select `Infra-vHBA-A`.
10. From the Adapter Policy drop-down list, select `Linux`.



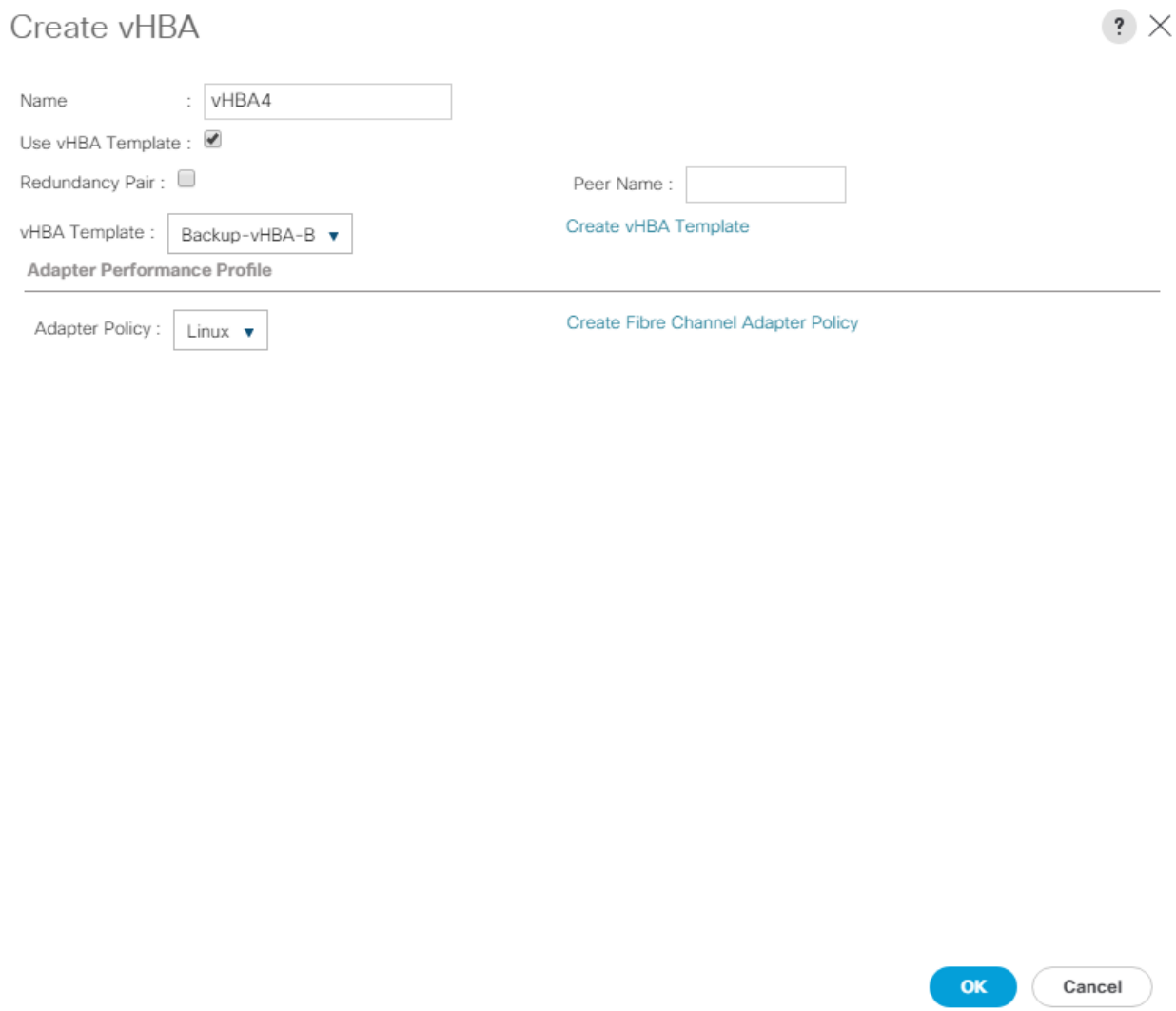
11. Click **OK**.
12. Click **Add**.
13. Under Create vHBA, enter `vHBA2` in the Name field.
14. Check the check box next to Use `vHBA Template`.
15. From the vHBA Template drop-down list, select `Infra-vHBA-B`.
16. From the Adapter Policy drop-down list, select `Linux`.



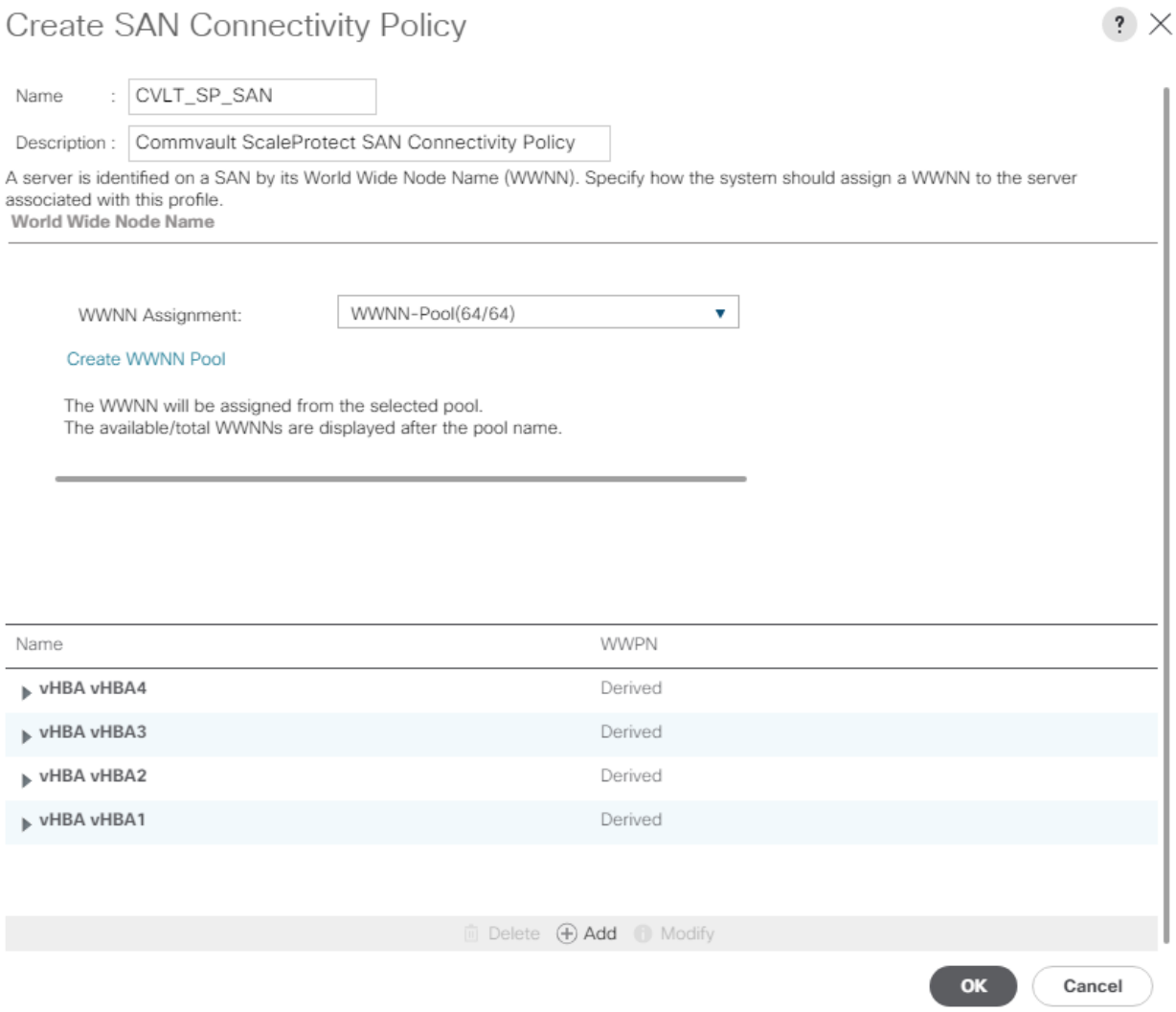
17. Click **OK**.
18. Click **Add**.
19. Under Create vHBA, enter `vHBA3` in the Name field.
20. Check the check box next to Use `vHBA Template`.
21. From the vHBA Template drop-down list, select `Backup-vHBA-A`.
22. From the Adapter Policy drop-down list, select `Linux`.



23. Click **OK**.
24. Click **Add**.
25. Under Create vHBA, enter `vHBA4` in the Name field.
26. Check the check box next to Use `vHBA Template`.
27. From the vHBA Template drop-down list, select `Backup-vHBA-B`.
28. From the Adapter Policy drop-down list, select `Linux`.


Create vHBA
Name : vHBA4
Use vHBA Template :
Redundancy Pair :
Peer Name :
vHBA Template : Backup-vHBA-B
Create vHBA Template
Adapter Performance Profile
Adapter Policy : Linux
Create Fibre Channel Adapter Policy
OK
Cancel

29. Click **OK**.



30. Click **OK** again to accept creating the SAN connectivity policy.

Cisco UCS C220 M5 Server Storage Setup

The following procedures describe how to configure the Cisco UCS C220 M5 Server's disk storage.

LUN Cleanup

For any Cisco UCS C220 server nodes that had LUNs created from previous Service Profile associations, there will be LUNs existing on those server nodes in an orphaned state preventing use of the disks from those LUNs to a new Service Profile association.

To clear up orphaned LUNs, follow these steps:

1. In Cisco UCS Manager, click **Equipment** within the Navigation Pane and click the server node from the displayed list to clear LUNs from.

2. Within that server node, click the **Inventory** tab, then the **Storage** tab within that, and finally the **LUNs** tab of the Storage tab of the server node.

3. Select each of the Orphaned LUNs, and right-click the Delete Orphaned LUN option.

4. Click **Yes** to confirm the action and click **OK** to continue.

ScaleProtect with Cisco UCS Server Storage Profile

The Storage Profile consists of Storage Polices used for creating Local LUNs out of allocated disks.

The next steps are dependent on the available disk drives on the Cisco UCS C220 M5 used for ScaleProtect with Cisco UCS. To complete the storage configuration, you need to identify the physical disks available for the operating system installation and disk library. For a configuration with 4 disk drives for disk library, use the steps presented here.

The Cisco UCS C220 rack server will use a storage profile similar to that for the Cisco UCS S3260 Storage Server, but it will not need a controller definition, because the C220 in the environment has all disks in front-facing drive slots. Two disk policies need to be created for local LUNs to use for the boot device and disk library for the MediaAgent, and others can be created if additional local LUNs are needed. The ScaleProtect with Cisco UCS architecture with the Cisco UCS C220 M5 servers uses the internal M.2 SSD drives. These drives are managed by the software RAID controller in Cisco UCS, and server will boot to the internal M.2 SSDs in a software RAID 1 configuration.

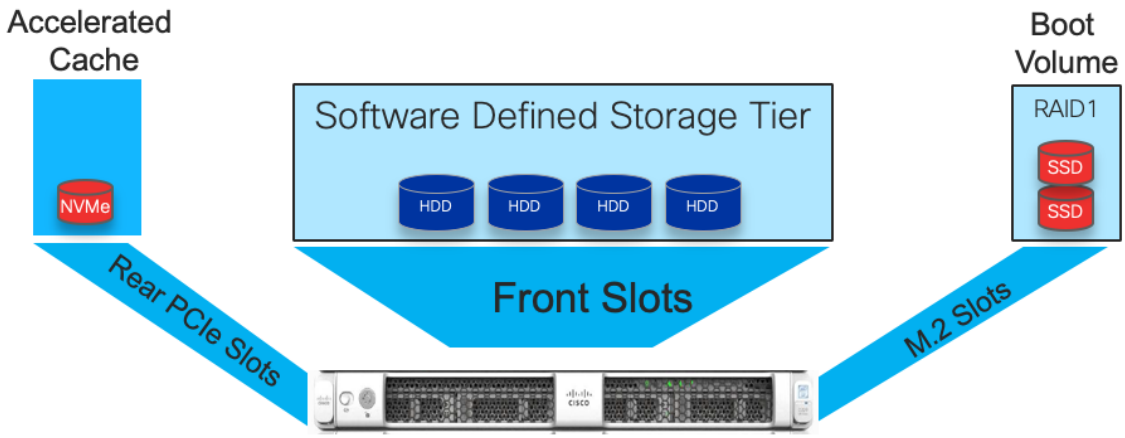
The storage profile consists of storage polices used for creating local LUNs from the allocated disks (disk group policies). Since the Cisco UCS C220 M5 server for ScaleProtect with Cisco UCS uses internal M.2 SSDs for boot and the NVMe for the cache (deduplication database and the index cache) and the other HDDs as JBODs attached to the SAS HBA, you need to create only a storage profile with the controller definition created to boot from software RAID. All the other drives will be presented to the ScaleProtect with Cisco UCS nodes as JBODs.

The disk layout of the Cisco UCS C220 M5 LFF nodes is as follows:

- Boot Volume – 2x 960GB M.2 SSDs
  - Configured in RAID 1 using Software Raid
- Accelerated Cache Volume – 1x 1.6TB NVMe SSD
  - Configured in Pass-through (JBOD) mode
- Software Defined Storage Tier – 4x NL-SAS HDDs (Option of 4/6/8/12 TB sizes)
  - Configured in Pass-through (JBOD) mode

Figure 10 illustrates the disk layout of Cisco UCS C220 M5 LLF server node:

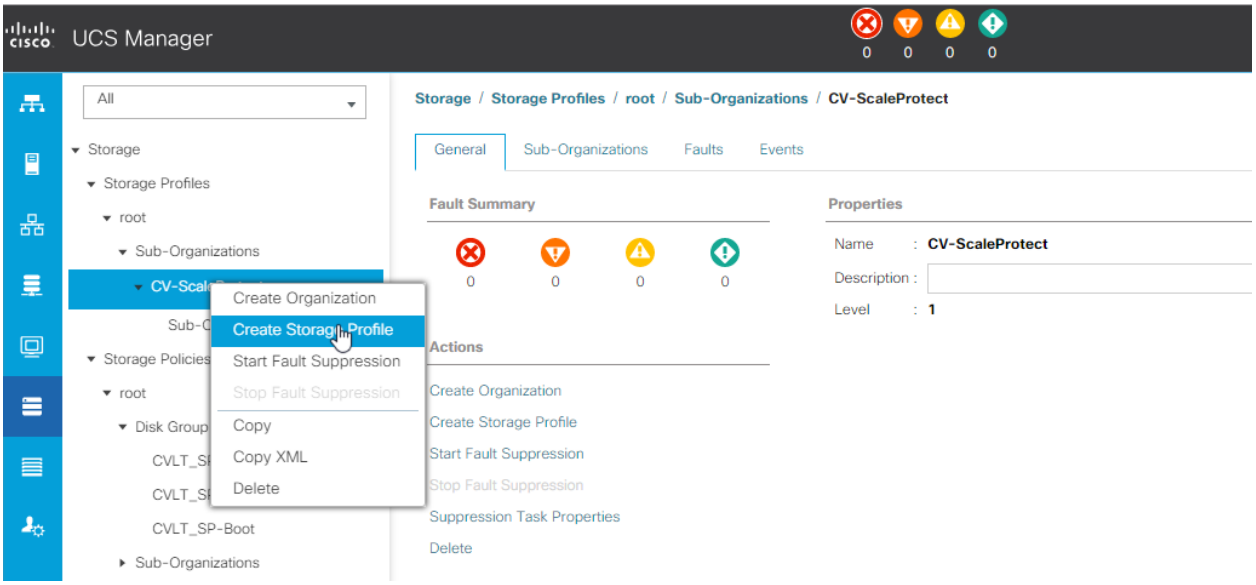
Figure 10 Cisco UCS C220M5 LFF Disk Layout



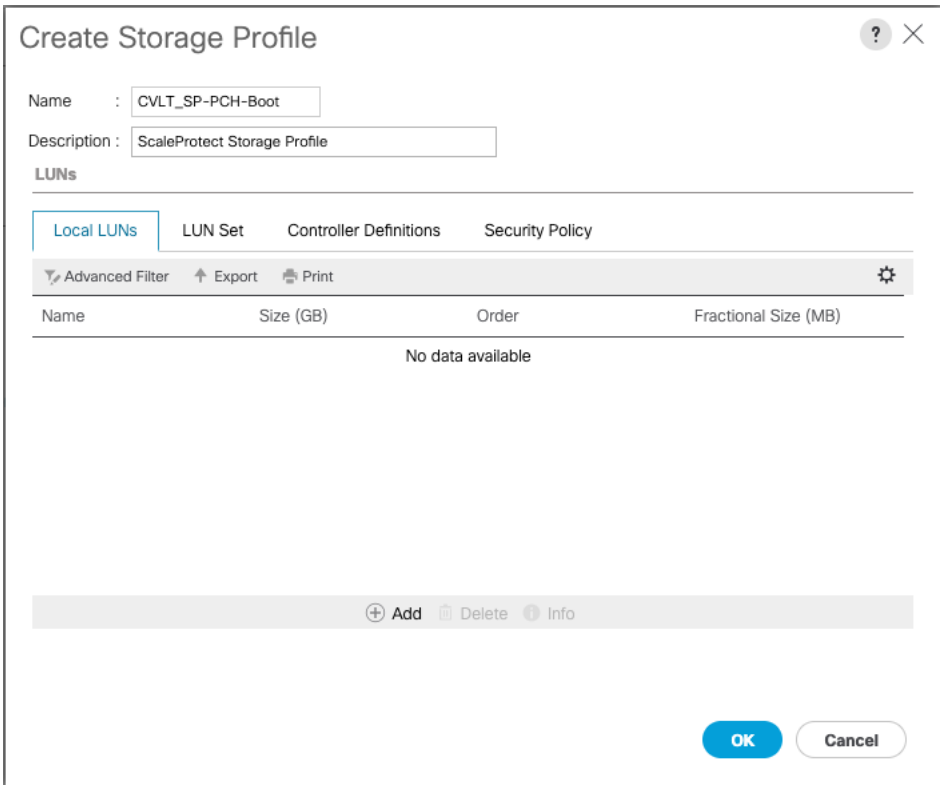
Create Storage Profile

To create ScaleProtect Storage Profile for Cisco UCS C220 M5, follow these steps:

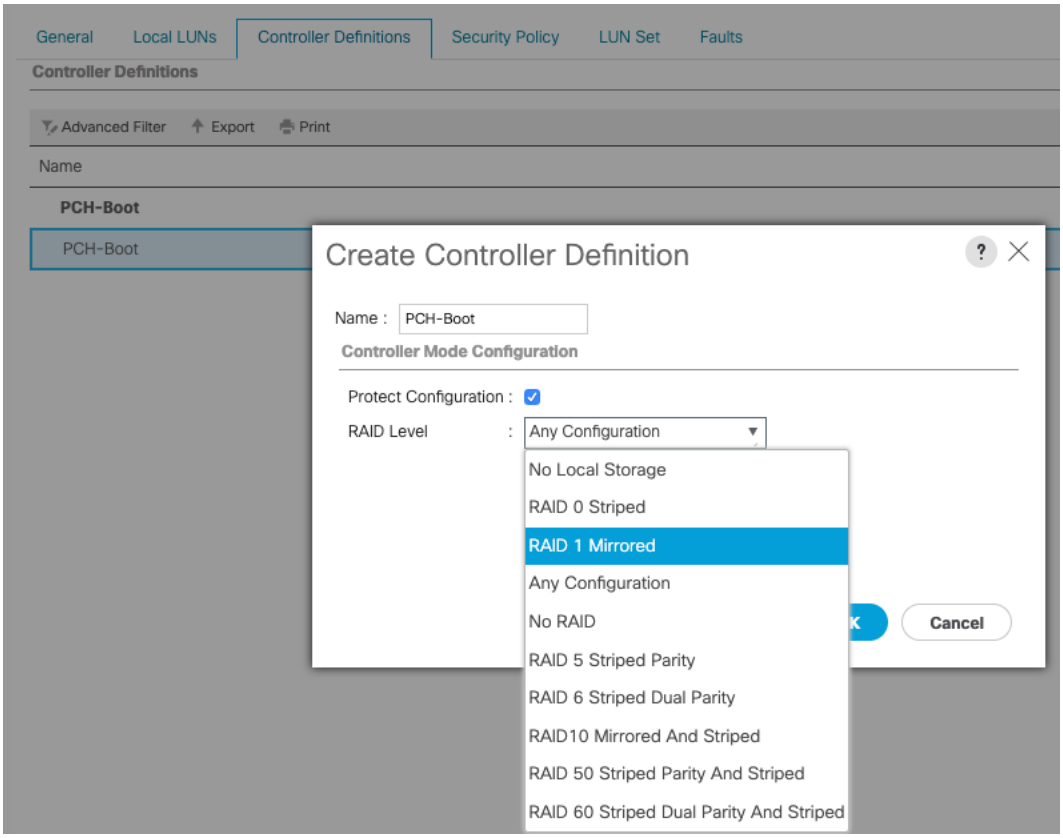
1. In Cisco UCS Manager, click the **Storage** tab in the navigation pane.
2. Select Storage Policies > root >Sub-Organizations > CV-ScaleProtect.
3. Right-click and Select **Create Storage Profile**.



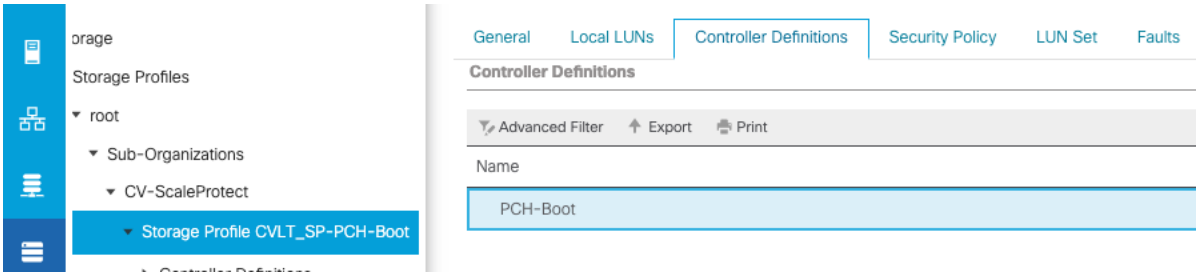
4. Enter name as `CVLT_SP-PCH-Boot`.



5. Click on Controller Definitions tab.
6. Select Add to add a controller definition that will be create a software Raid 1 LUN for operating system boot.
7. Provide the following in the Create Controller Definition dialogue:
    a. Name: enter PCH-Boot.
    b. Leave Protect Configuration checked.
    c. From the RAID Level Configuration pull-down menu, choose RAID 1 Mirrored.
8. Enter `1` as the size in GB.
9. Check `Expand to Available`, this creates a single lun with maximum space available.
10. Select Disk Group Selection as `CVLT_SP-Boot` and click **OK**.



11. Click **OK** and then click **OK** again to add the controller definition and complete storage profile creation.



Create Boot Policy

Cisco UCS Boot Policies define the boot devices used by blade and rack-mount servers, and the order that they are attempted to boot from. Cisco UCS C-Series M5 generation rack-mount servers which run the ScaleProtect Platform have their operating system installed to a pair of internal M.2 SSD boot drives, therefore they require a unique boot policy defining that the servers should boot from that location. In addition, a local CD/DVD boot option is included to allow the server to search for the installation ISO media during the Cohesity installation steps.

To configure the Boot Policy, follow these steps:

1. In Cisco UCS Manager, click **Server** within the Navigation Pane, and select Policies from within the Server pull-down options.

2. Select root > Sub-Organizations > CV-ScaleProtect > Boot Policies.

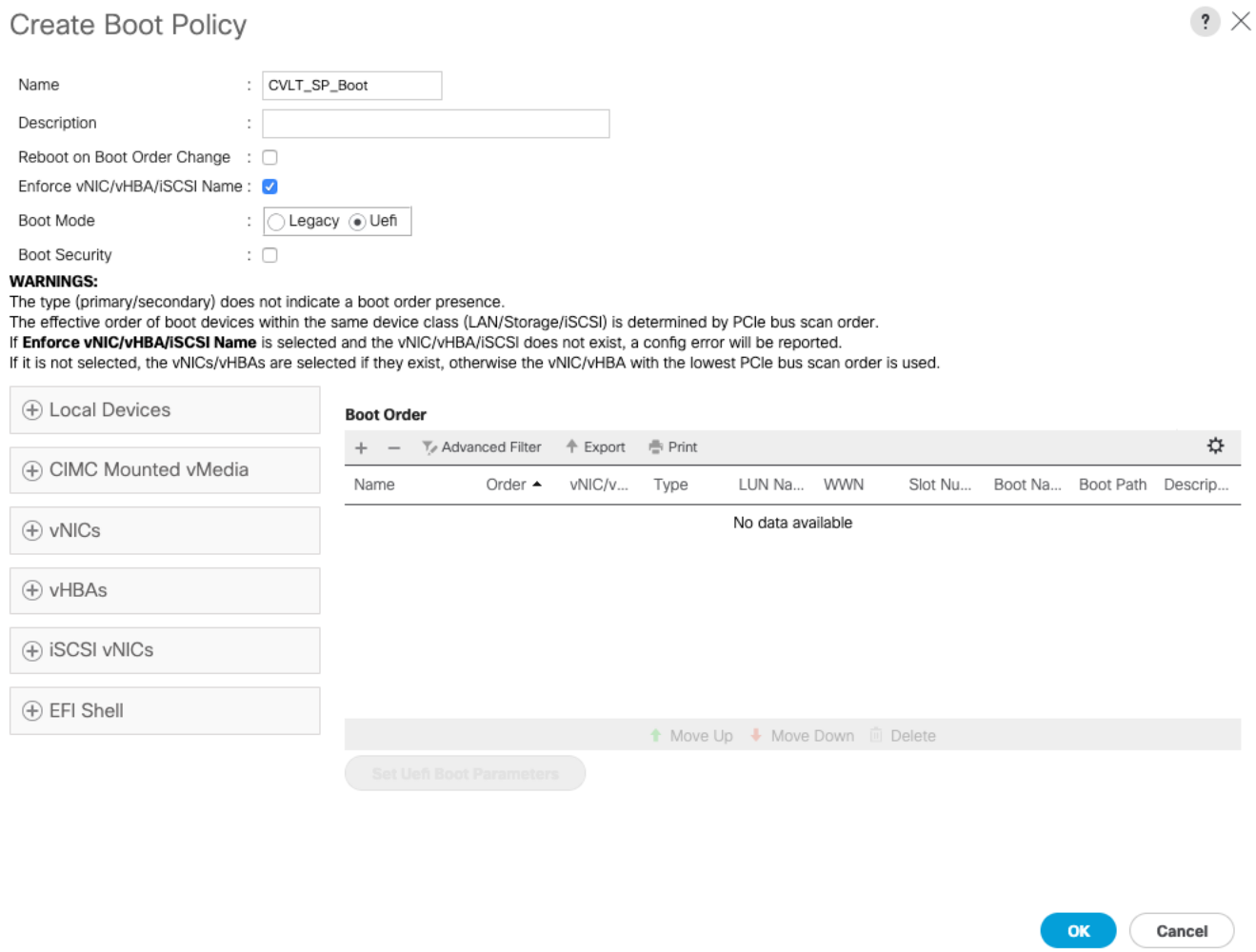
3. Right-click **Boot Policies** and select Create Boot Policy.

4. Enter `CVLT_SP_Boot` as the name of the boot policy.

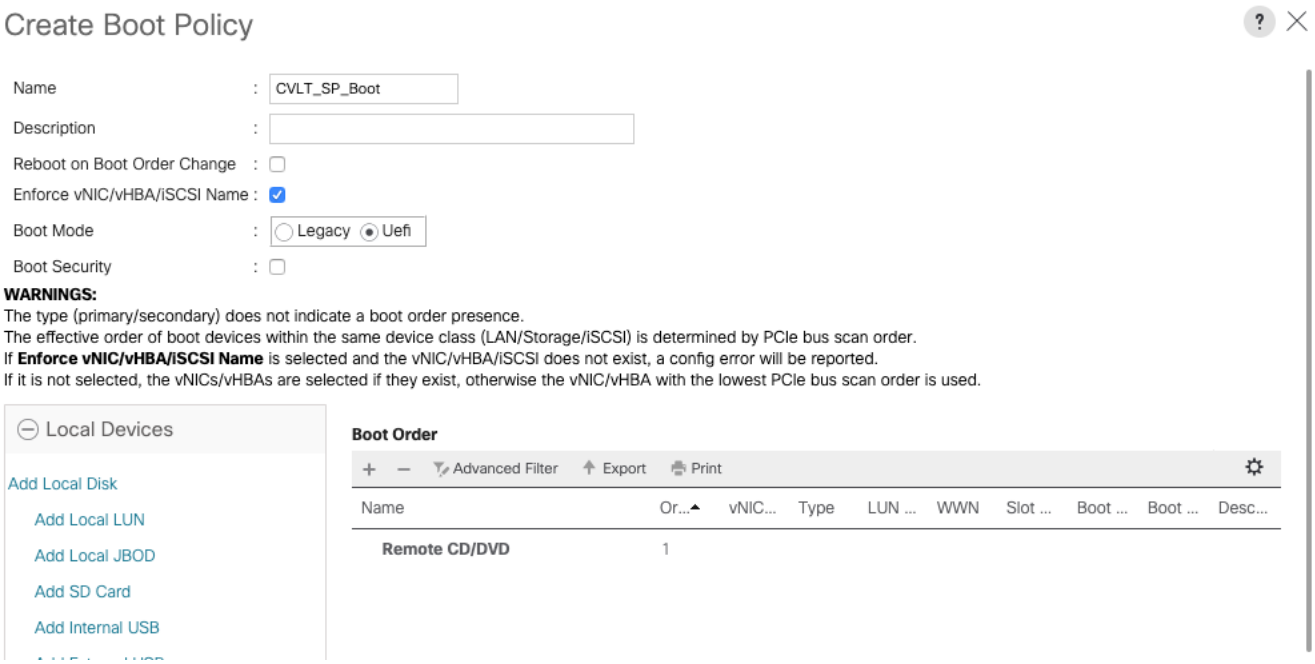
5. **Optional**: Enter a description for the boot policy.

6. Click the Uefi radio button to change the boot mode.

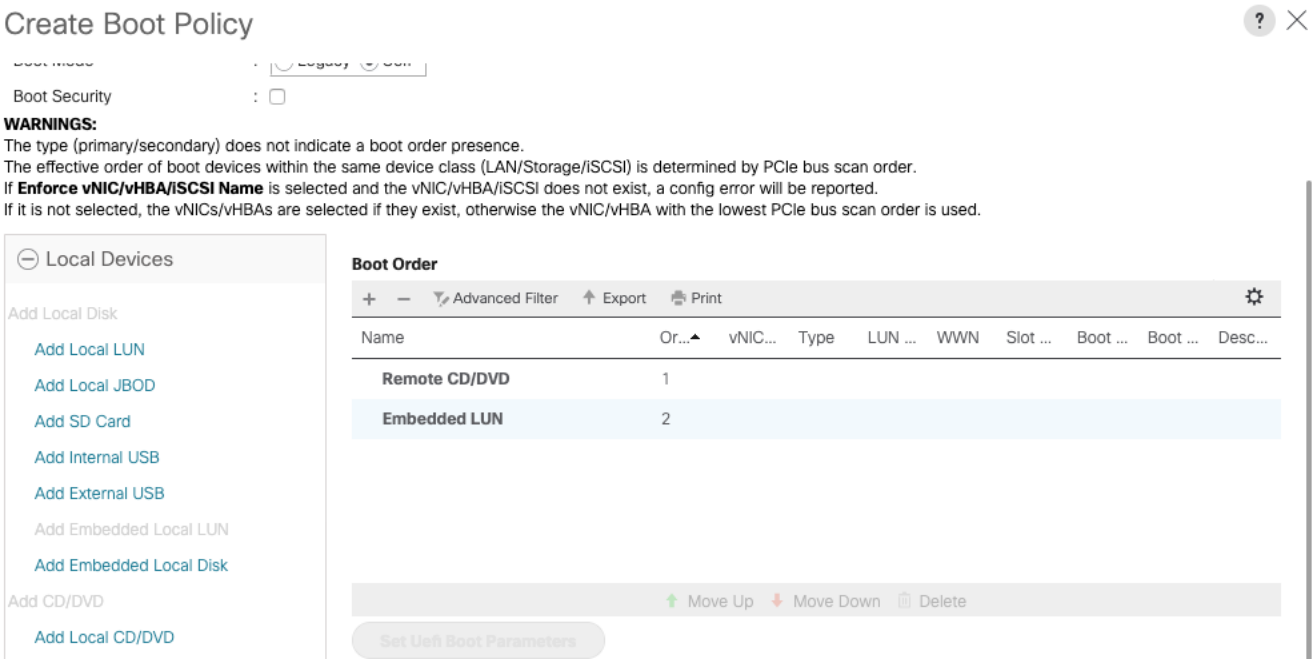
7. Keep the Reboot on the Boot Order Change check box unchecked.



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



9. Click Add Embedded Local LUN.



10. Click **OK** and click **OK** again to create the Boot Policy.

Cisco UCS C220 Service Profile Template

Service profile template configuration for the Cisco UCS C220 server nodes is explained in this section.

Create Service Profile Template

With a service profile template, you can quickly create several service profiles with the same basic parameters, such as the number of vNICs and vHBAs, and with identity information drawn from the same pools.

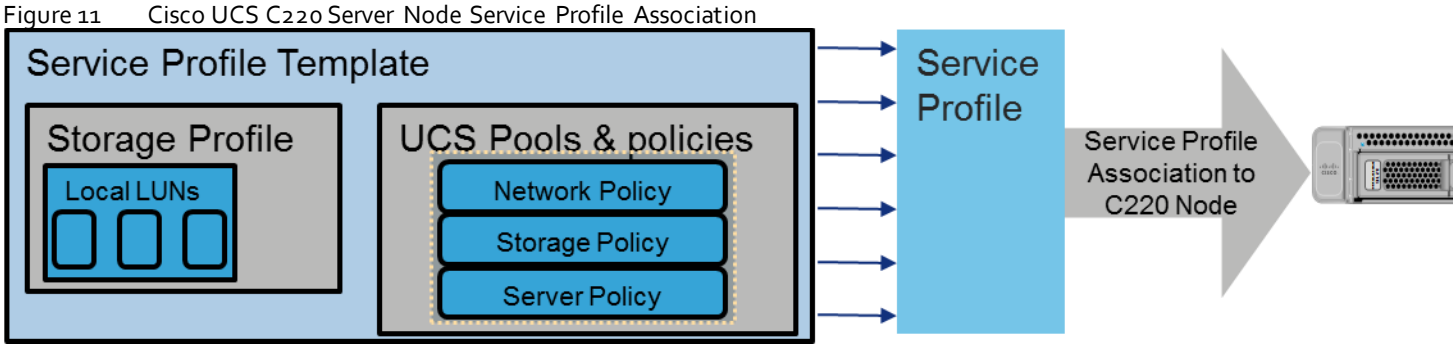
If you need only one service profile with similar values to an existing service profile, you can clone a service profile in the Cisco UCS Manager GUI.

For example, if you need several service profiles with similar values to configure servers to host Commvault software in a cluster, you can create a service profile template, either manually or from an existing service profile. You then use the template to create the service profiles.

Cisco UCS supports the following types of service profile templates:

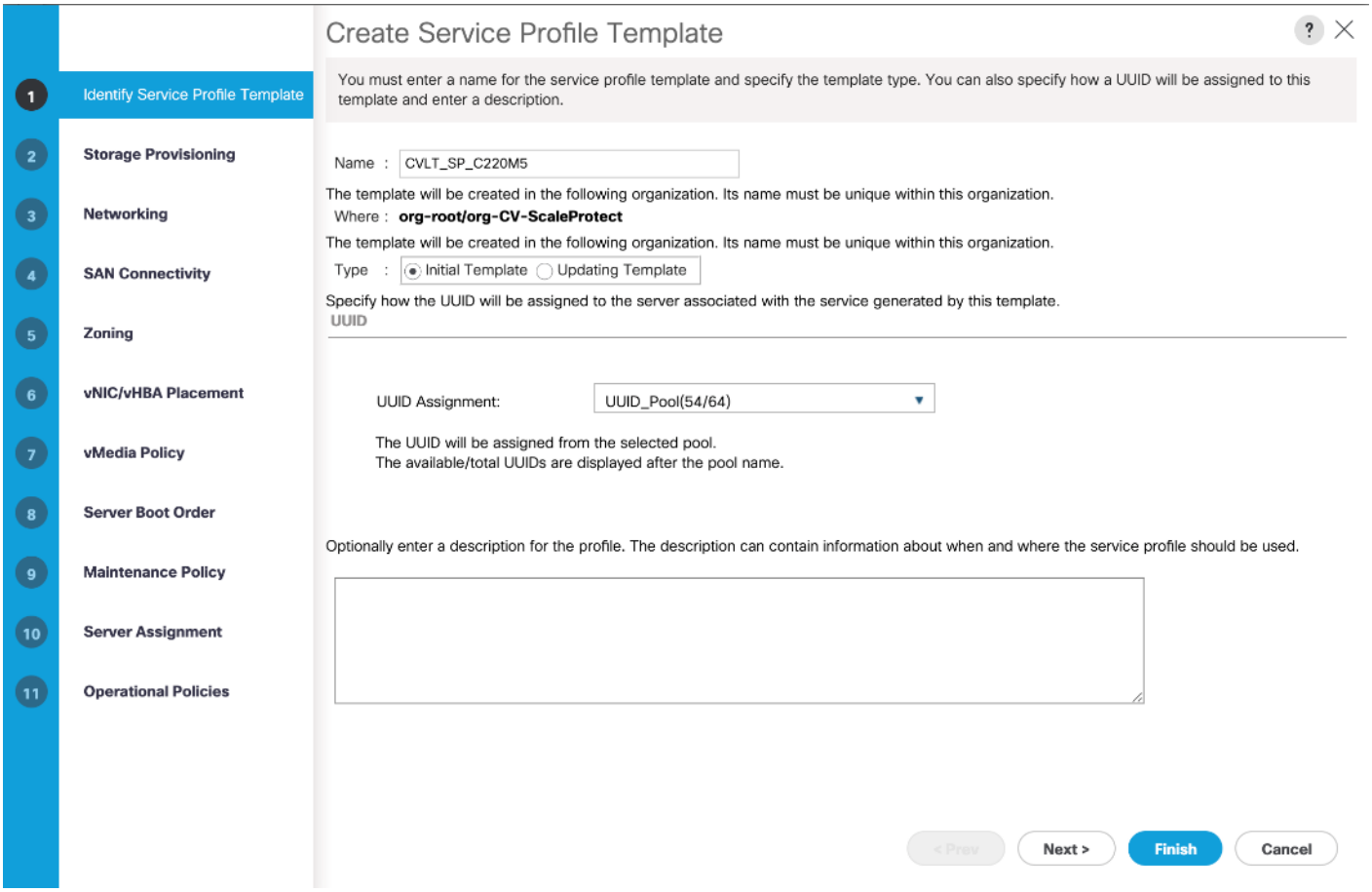
- **Initial template:** Service profiles created from an initial template inherit all the properties of the template. However, after you create the profile, it is no longer connected to the template. If you need to make changes to one or more profiles created from this template, you must change each profile individually.
- **Updating template:** Service profiles created from an updating template inherit all the properties of the template and remain connected to the template. Any changes to the template automatically update the service profiles created from the template.

Figure 11 Cisco UCS C220 Server Node Service Profile Association



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 > Sub-Organizations > CV-ScaleProtect.
3. Right-click `CV-ScaleProtect`.
4. Select Create Service Profile Template to open the Create Service Profile Template wizard.
5. Enter `CVLT_SP_C220M5` as the name of the service profile template.
6. Select the `Updating Template` option.
7. Under UUID, select `UUID_Pool` as the UUID pool.

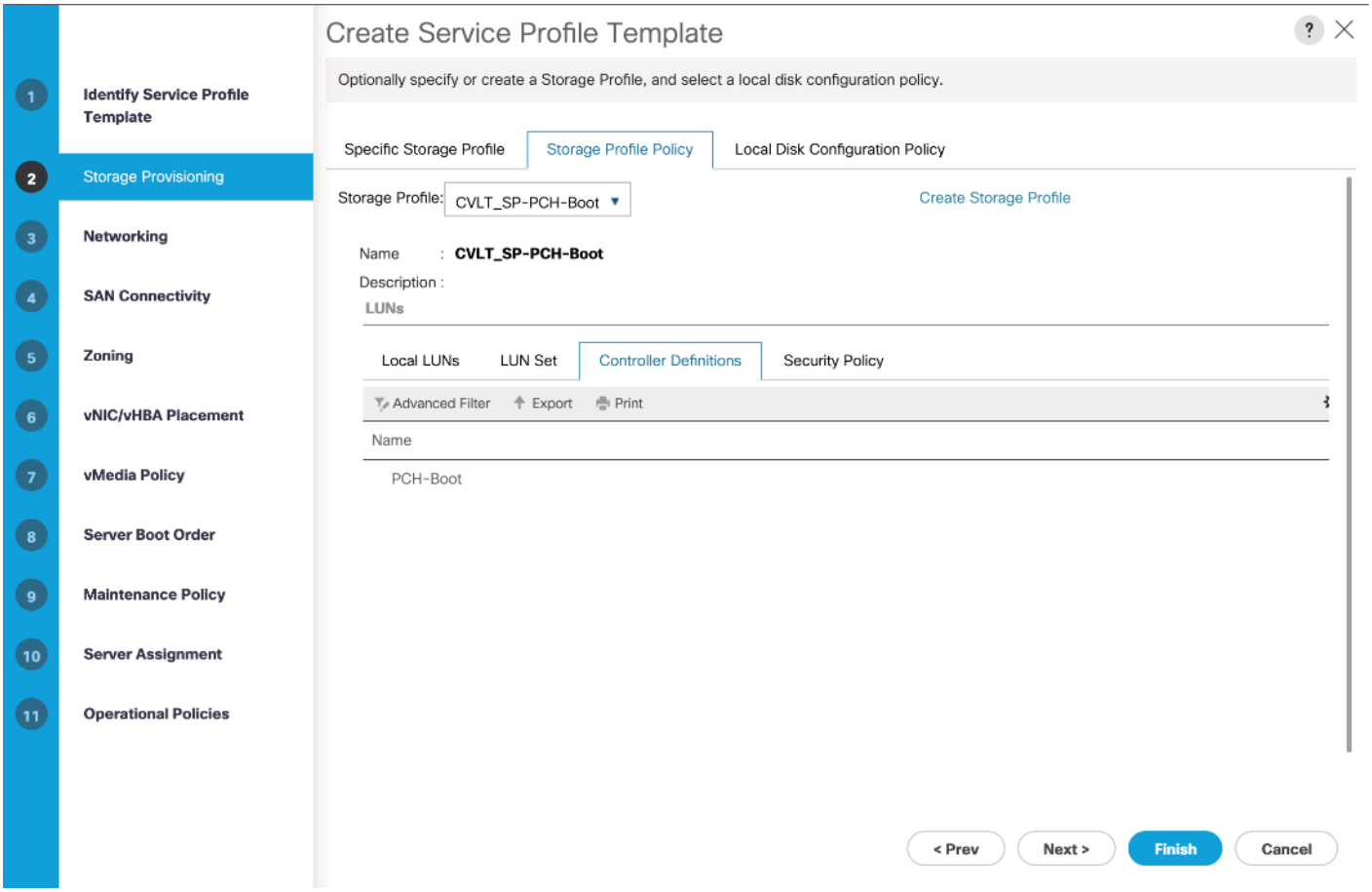


8. Click **Next**.

Configure Storage Provisioning

To configure the storage provisioning, follow these steps:

1. Click **Storage Profile Policy** Tab and select `CVLT_SP-PCH-Boot` (as created under Storage Profile section).

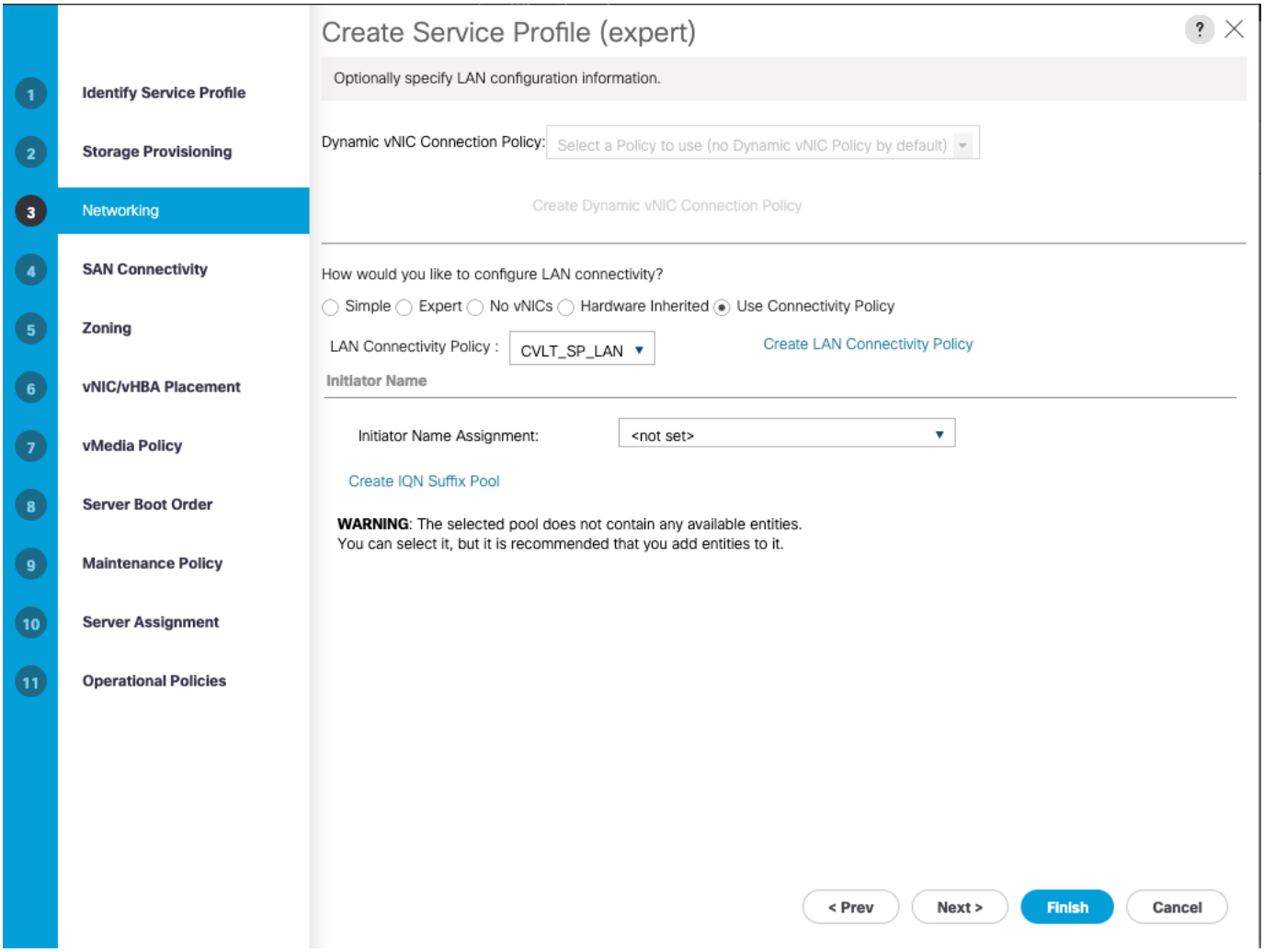


2. Click **Next**.

Configure Networking Options

To configure the networking 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 `CVLT_SP_LAN` as the LAN connectivity policy.



4. Click **Next**.

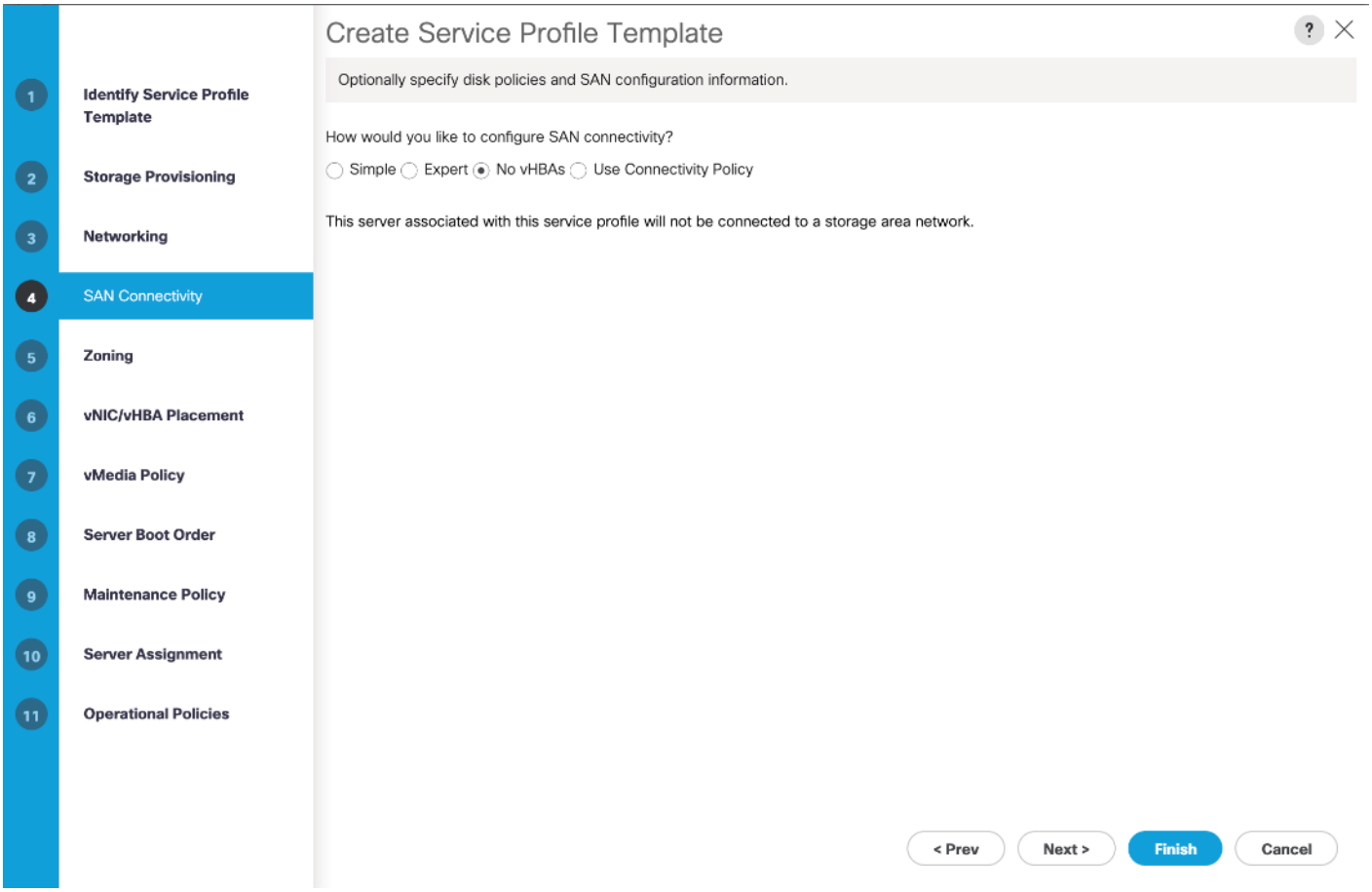
Configure Storage Options

Skip the SAN Connectivity since you will use local storage for Cisco UCS C220 created through Storage Policy and Select No vHBAs.

To configure the storage options, follow these steps:

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

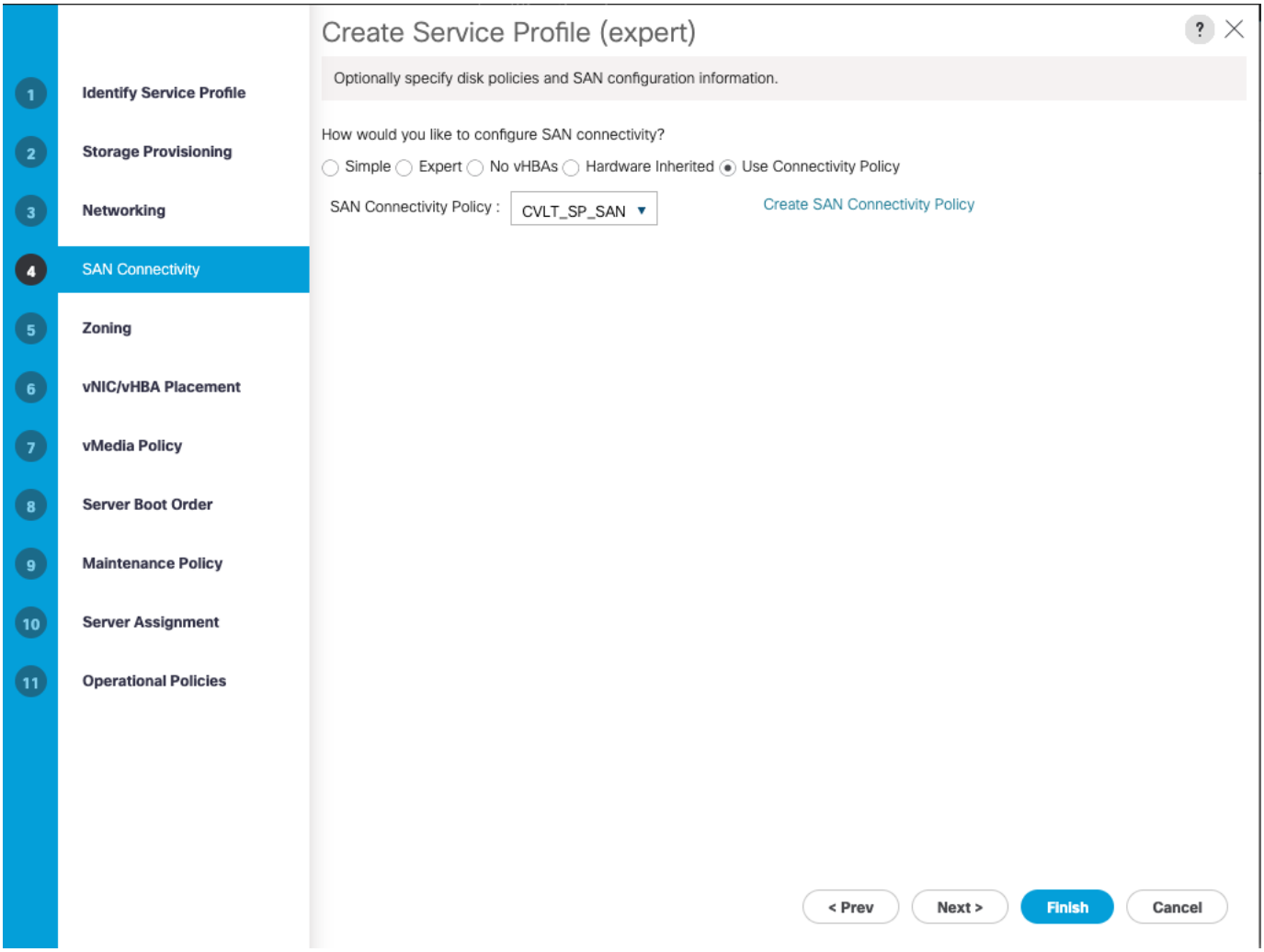
2. Click **Next**.



If SAN Connectivity is required from the ScaleProtect Cluster to existing SAN fabrics, select the SAN connectivity policy created earlier. For default implementation without SAN connectivity, skip the next two steps.

3. In the SAN connectivity section, select `Use Connectivity Policy` in "How would you like to configure SAN connectivity?" field.

4. Select `CVLT_SP_SAN` as the SAN connectivity policy. Click **Next**.



Configure Zoning Options

To configure the zoning options, follow these steps:

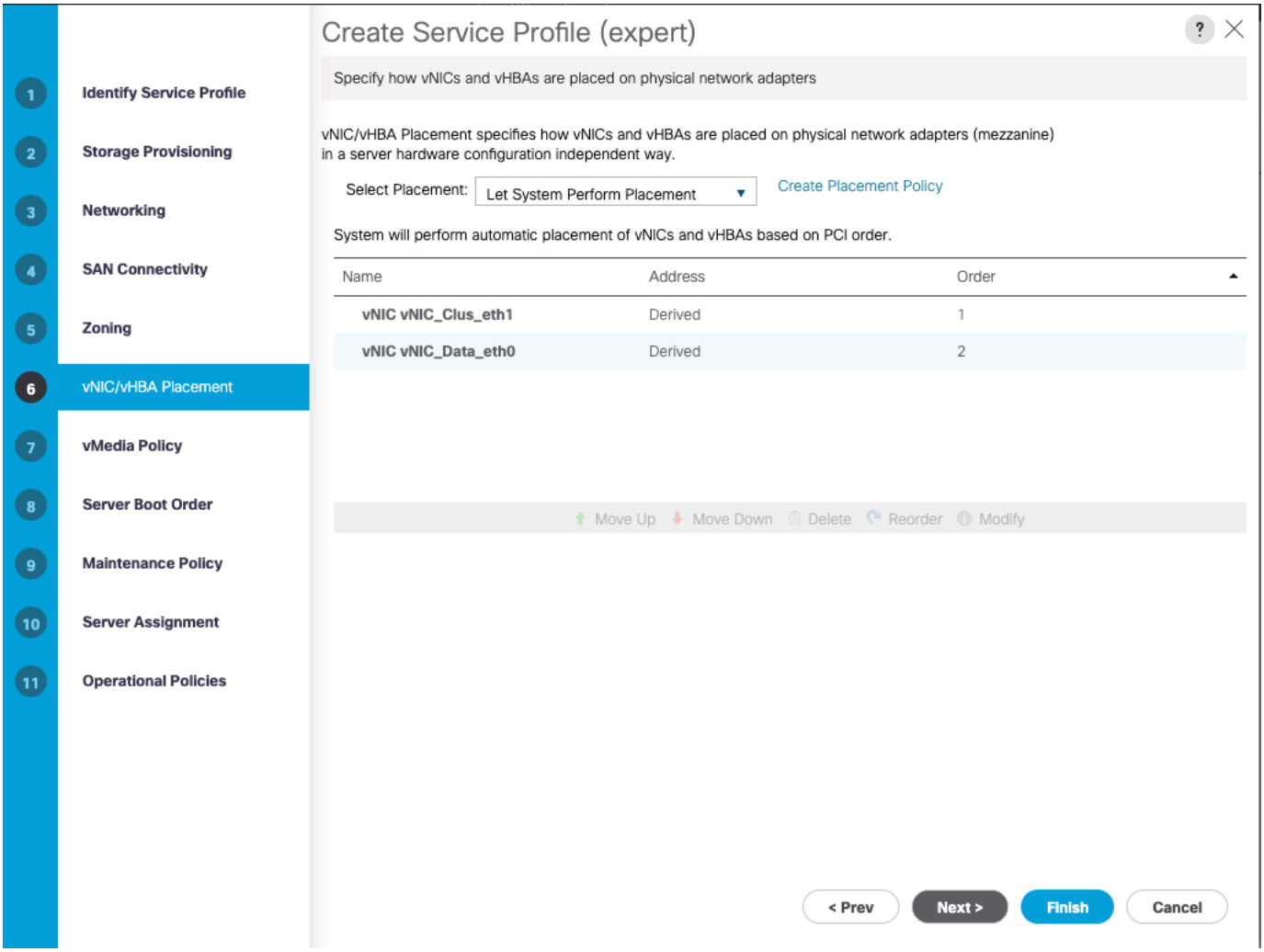
1. It is not necessary to configure any Zoning options.
2. Click **Next**.

Configure vNIC/HBA Placement

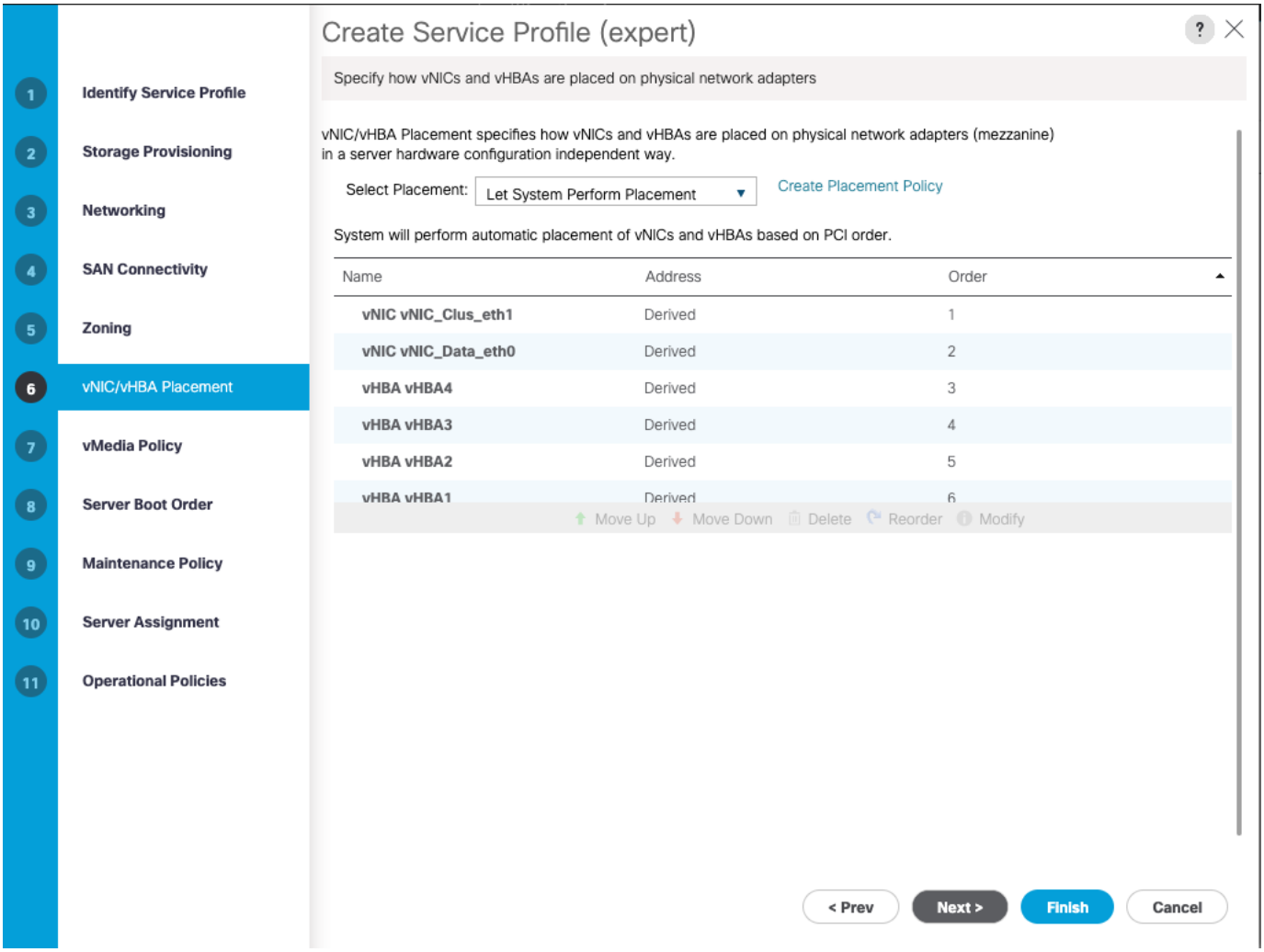
To configure the vNIC/HBA placement, follow these steps:

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

Default Installation without HBAs.



Installation with HBAs for SAN Connectivity.

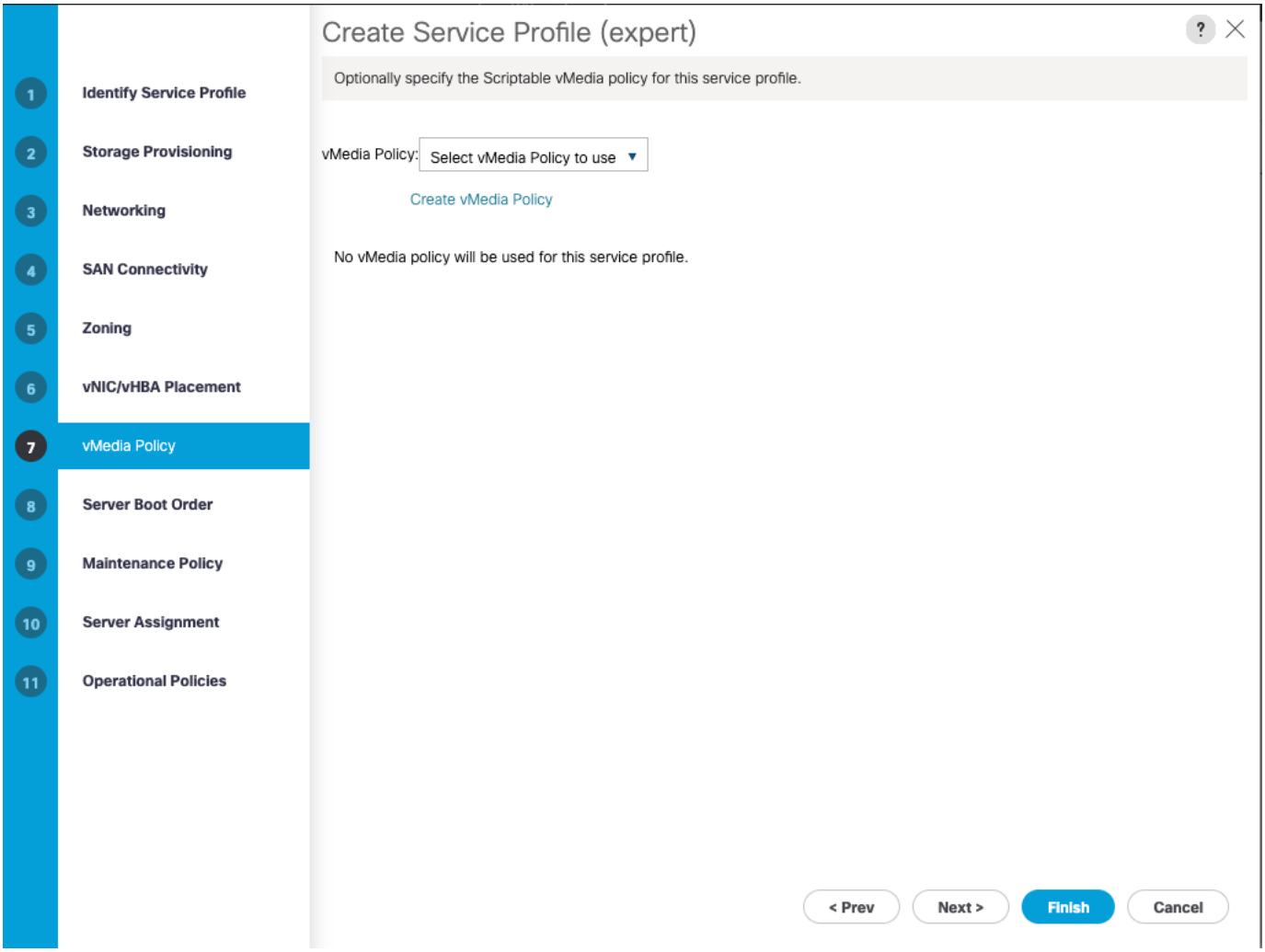


2. Click **Next**.

Configure vMedia Policy

To configure the vMedia policy, follow these steps:

1. From the vMedia Policy, leave as default.

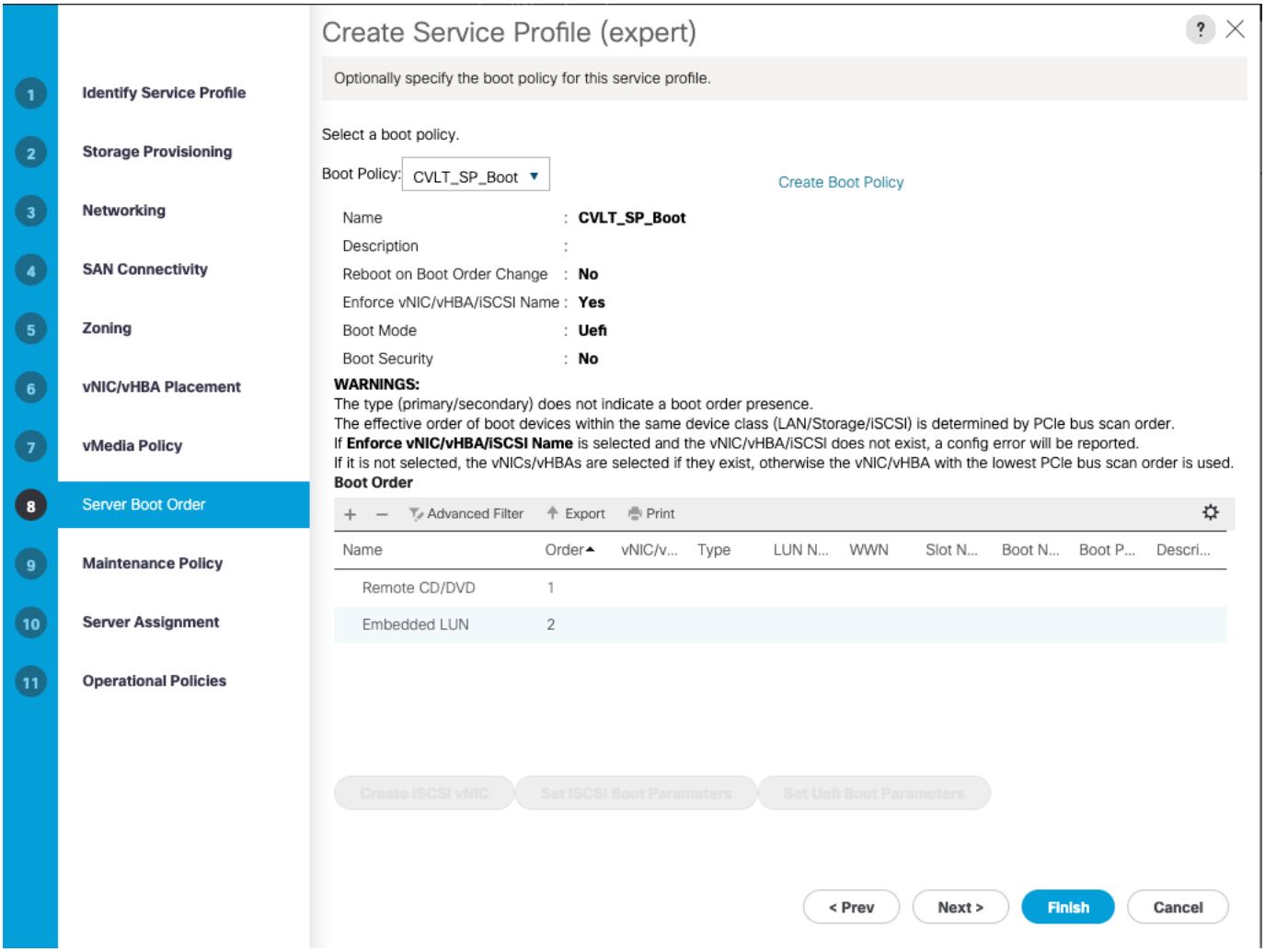


2. Click **Next**.

Configure Server Boot Order

To configure the server boot order, follow these steps:

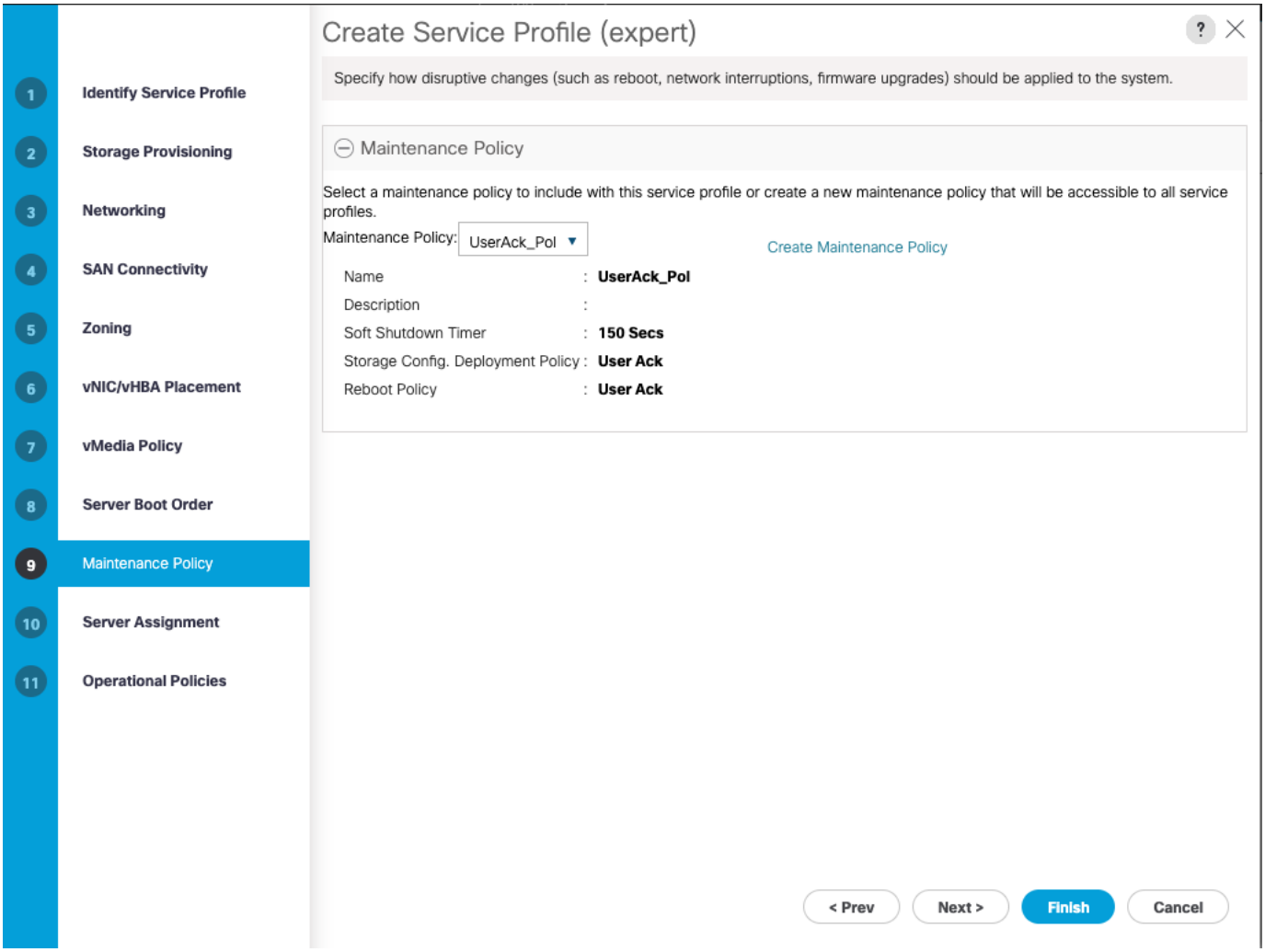
1. Choose `CVLT_SP_Boot` as the Boot Policy that was created earlier.



Configure Maintenance Policy

To configure the maintenance policy, follow these steps:

1. Change the Maintenance Policy to `UserAck_Pol`.

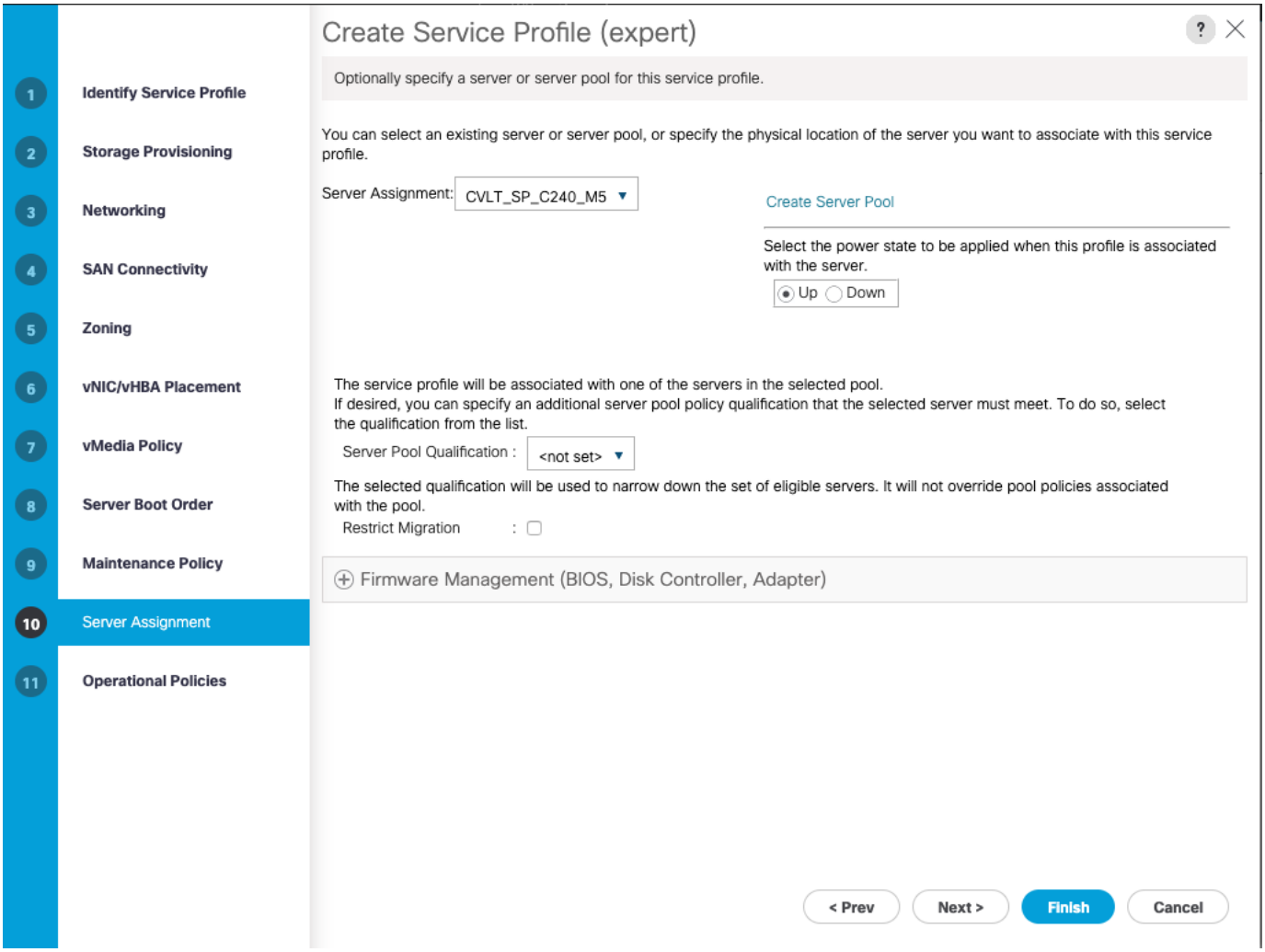


2. Click **Next**.

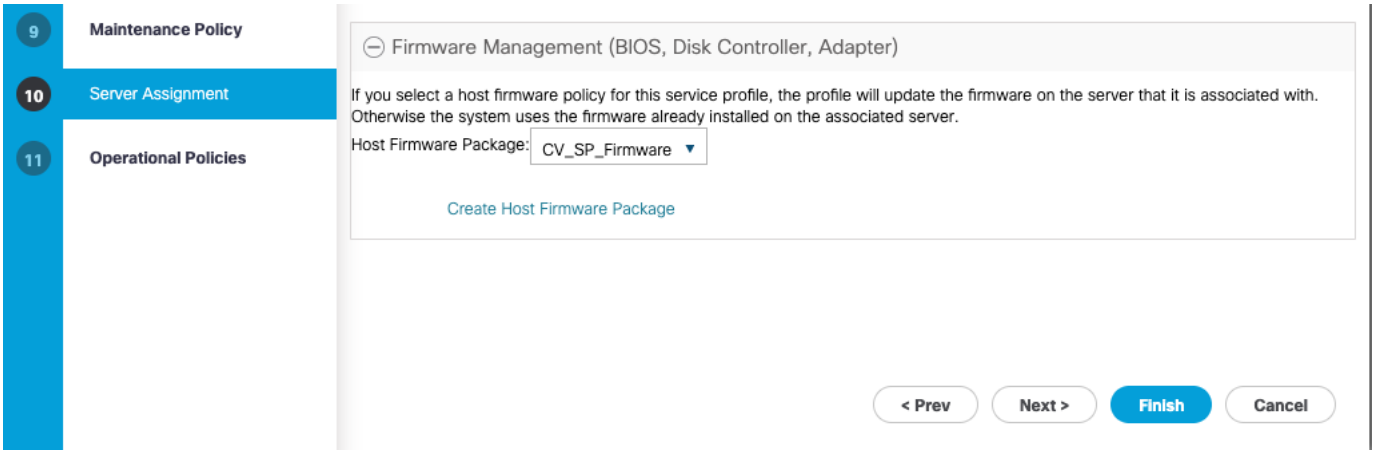
Configure Server Assignment

To configure server assignment, follow these steps:

1. In the Server Assignment section, select the server pool created earlier.



2. Expand Firmware Management at the bottom of the page and select `CV_SP_Firmware` as created in the previous section.

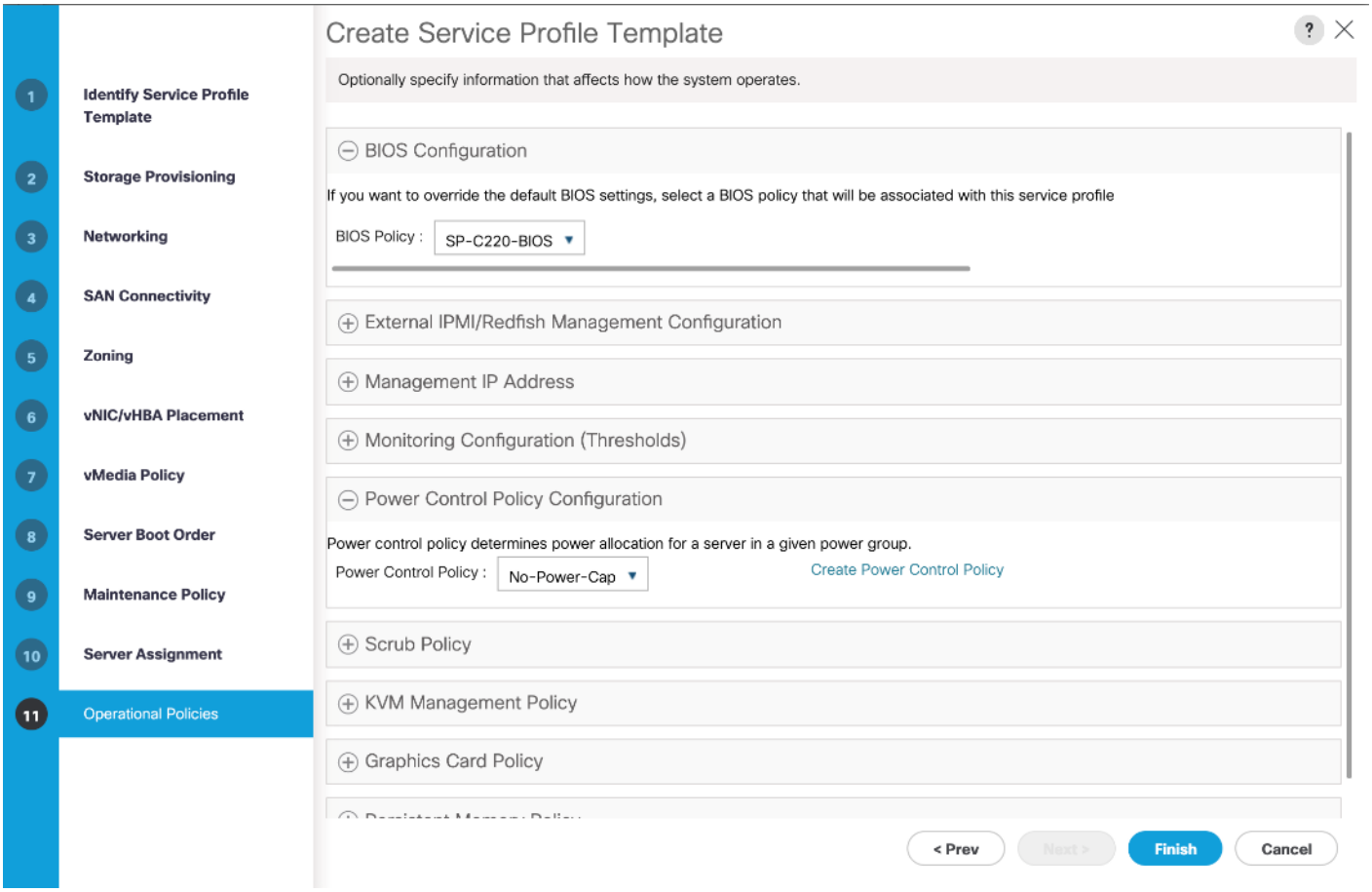


3. Click **Next**.

Configure Operational Policies

To configure the operational policies, follow these steps:

1. In the BIOS Policy list, select `SP-C220-BIOS`.
2. Expand Power Control Policy Configuration and select `No-Power-Cap` in the Power Control Policy list.



3. Click **Finish** to create the service profile template.
4. Click **OK** in the confirmation message to complete service profile template creation for first server nodes in the chassis.

Create Service Profiles

This section describes how to associate the Cisco UCS C220 Compute Node to a Service Profile.

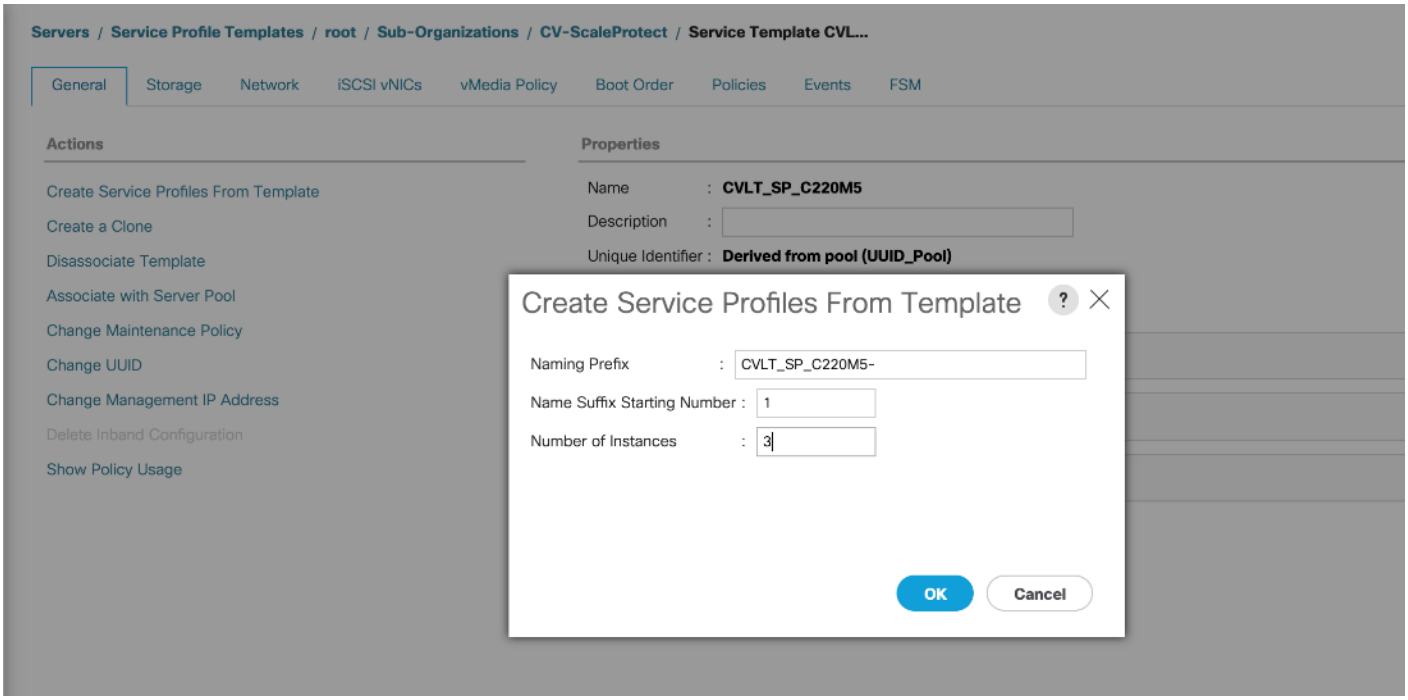
To create service profiles from the service profile template, follow these steps:

1. On **Servers** tab in the navigation pane.
2. Select Service Profile Templates > root > Sub-Organizations > CV-ScaleProtect > Service Template > `CVLT_SP_C220M5`.
3. Right-click `CVLT_SP_C220M5` Template and select Create Service Profiles from Template.
4. Enter `CVLT_SP_C220M5-` as the service profile prefix.

5. Enter 1 as "Name Suffix Starting Number."

6. Enter 3 as the "Number of Instances."

7. Click **OK** to create the service profiles.

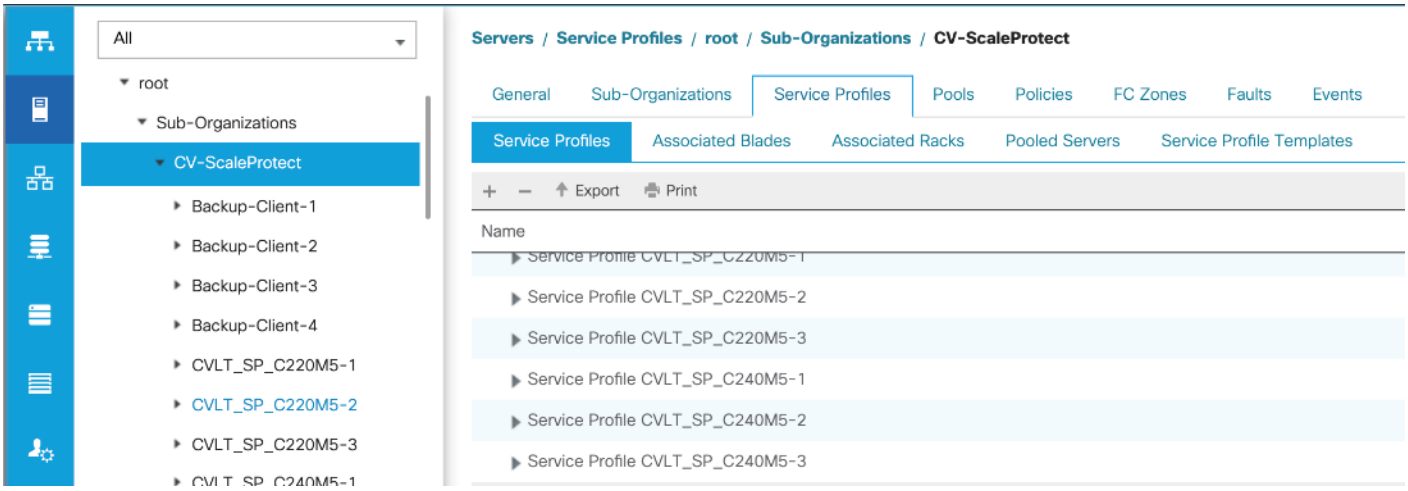


8. Click **OK** in the confirmation message.

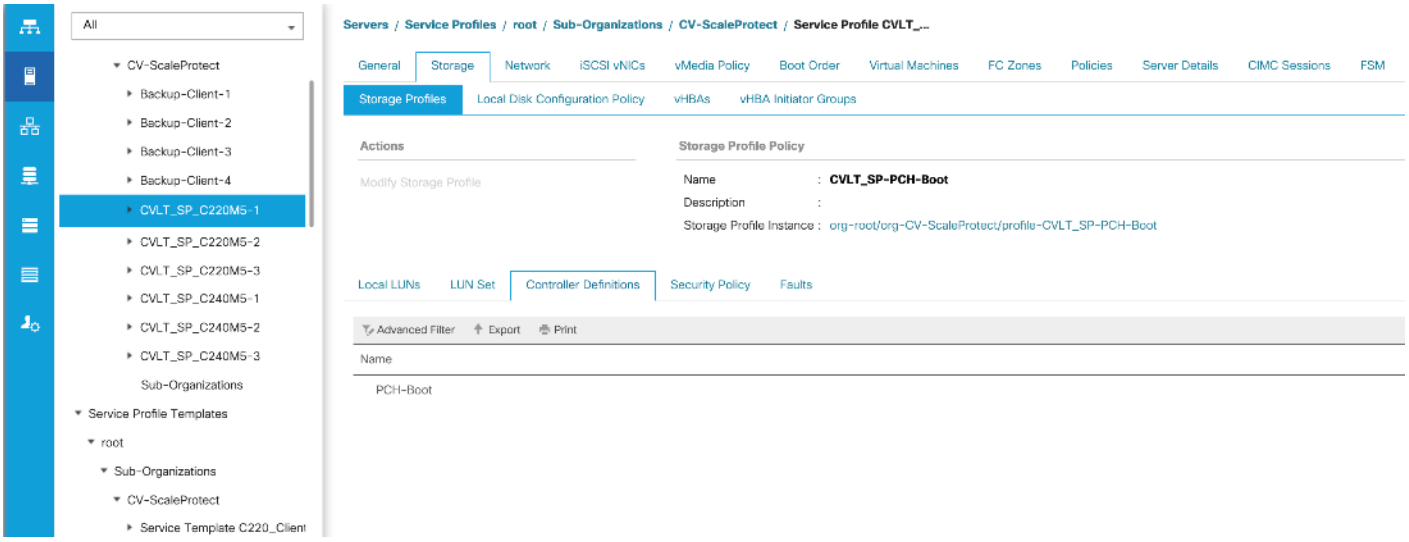
9. If a warning displays, click **Yes**.

The assignment of the service profile to the physical server will take some time. Check the FSM tab to monitor the status. If a firmware update is required, the overall process can take up to an hour to finish.

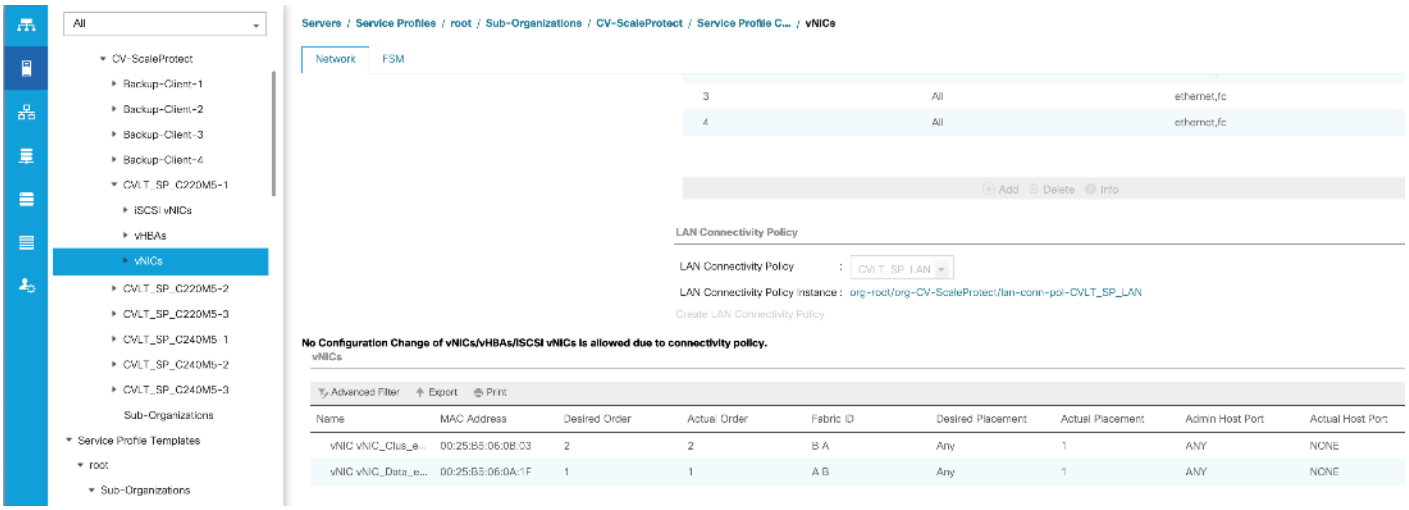
10. When Service Profile Association is complete, confirm that the overall status is OK.



11. Verify the Controller Definition is added under Storage tab of Service Profile.



12. Verify Service Profile has 2 vNICs.

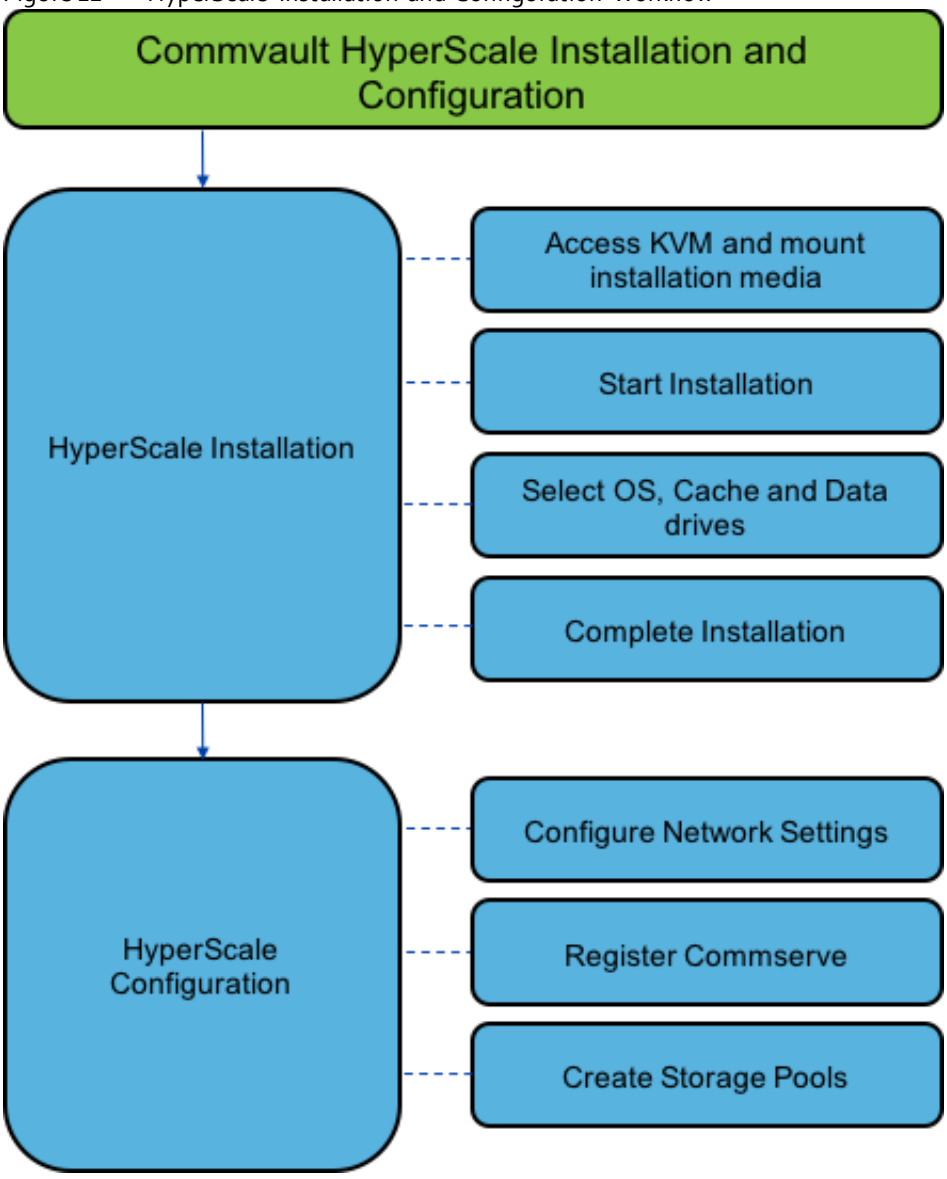


Commvault HyperScale Installation and Configuration

This section explains the Commvault HyperScale installation and configuration on Cisco UCS C220 M5 Servers.

Ensure you have the latest copy of the Commvault HyperScale ISO downloaded from https://cloud.commvault.com. Also, its critical to make sure that the HyperScale release is compatible with the Cisco UCS software versions.

Figure 12 HyperScale Installation and Configuration Workflow

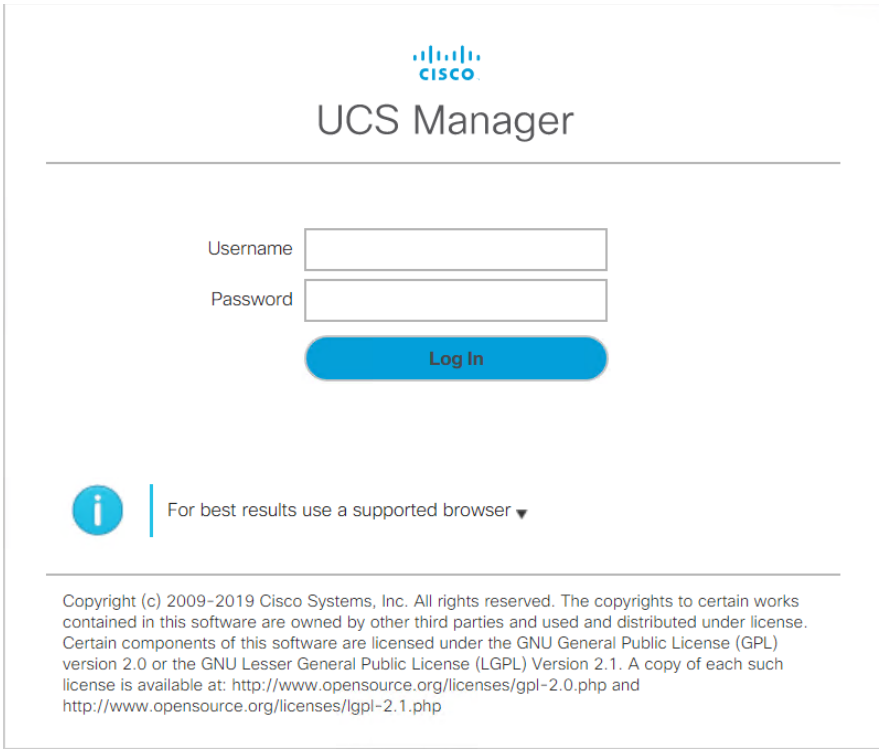


To install and configure the Commvault HyperScale software, follow these steps:

1. Open a web browser and navigate to the Cisco UCS 6454 fabric interconnect cluster address.
2. Under HTML, click the Launch UCS Manager link to launch the Cisco UCS Manager HTML5 User Interface.

3. When prompted, enter admin as the user name and enter the administrative password.

4. Click **Login** to log into Cisco UCS Manager.

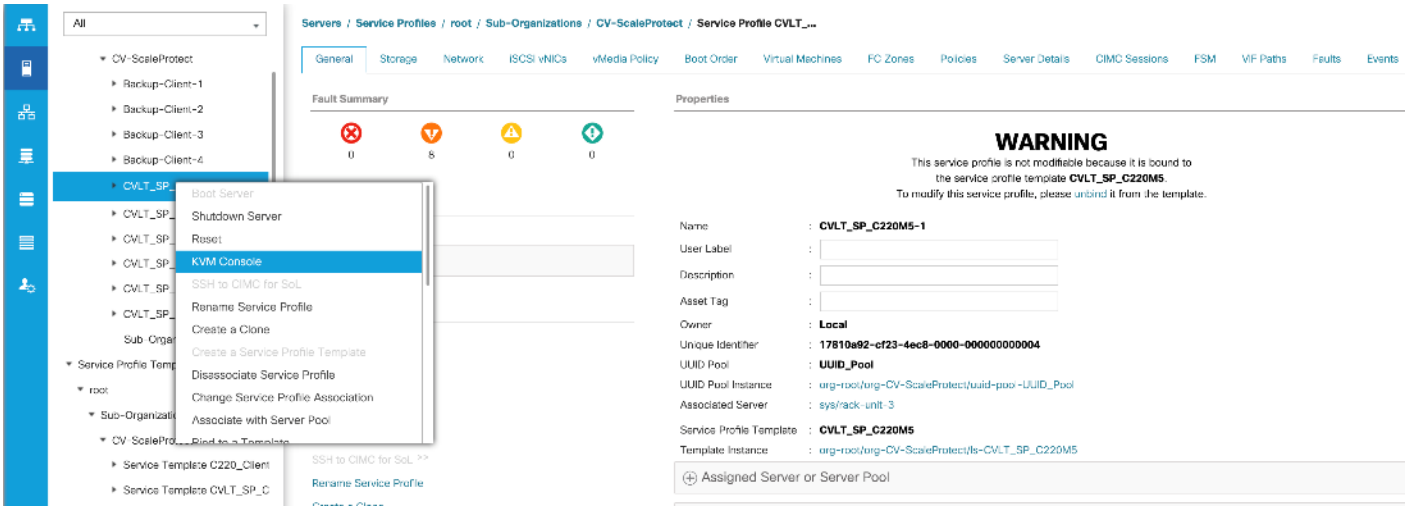


5. From the main menu, click the **Servers** tab.

6. Select Servers > Service Profiles > root > Sub-Organizations > CV-ScaleProtect > `CVLT_SP_C220M5-1`.

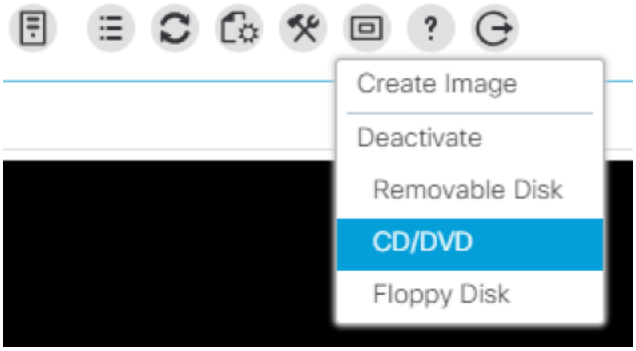
7. Right-click `CVLT_SP_C220M5-1` and select KVM Console.

8. If prompted to accept an Unencrypted KVM session, accept as necessary

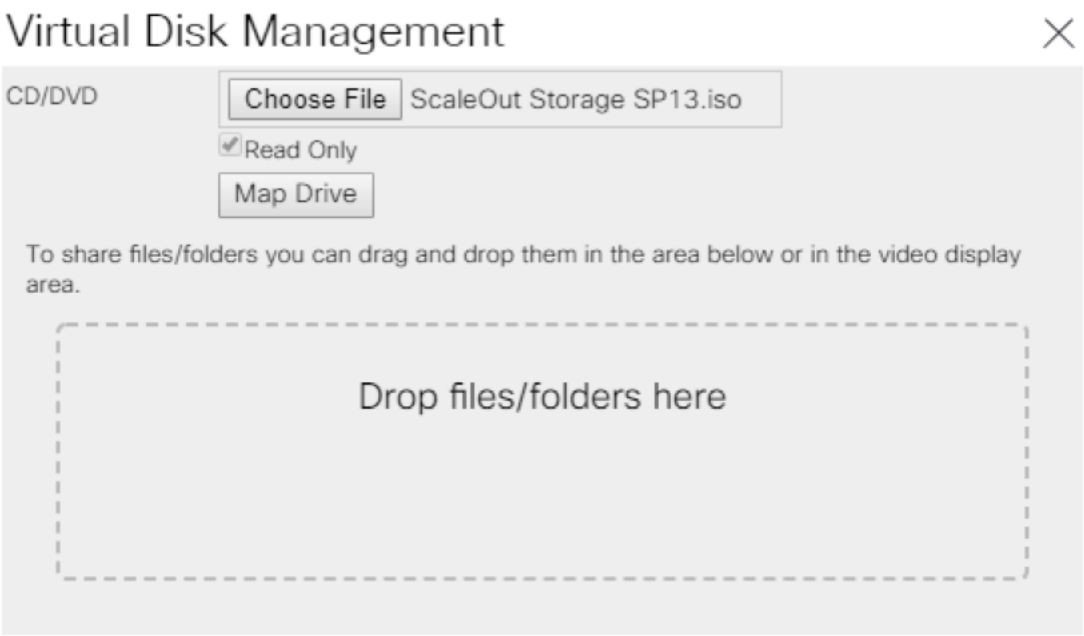


9. Attach the ISO to the server node using the KVM.

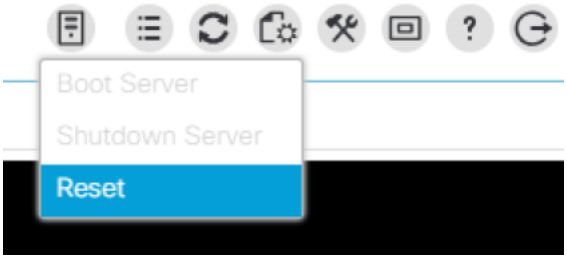
10. Click the **Virtual Media** icon and now select **CD/DVD** and browse to where the ISO is located, then click **Map Device.**



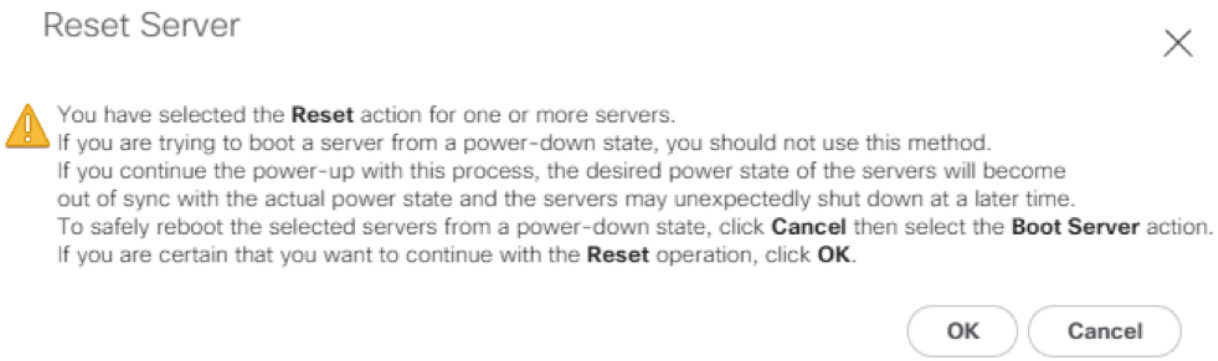
11. Click **Chose file** and browse to the Commvault HyperScale ISO, then click **Map Drive.**



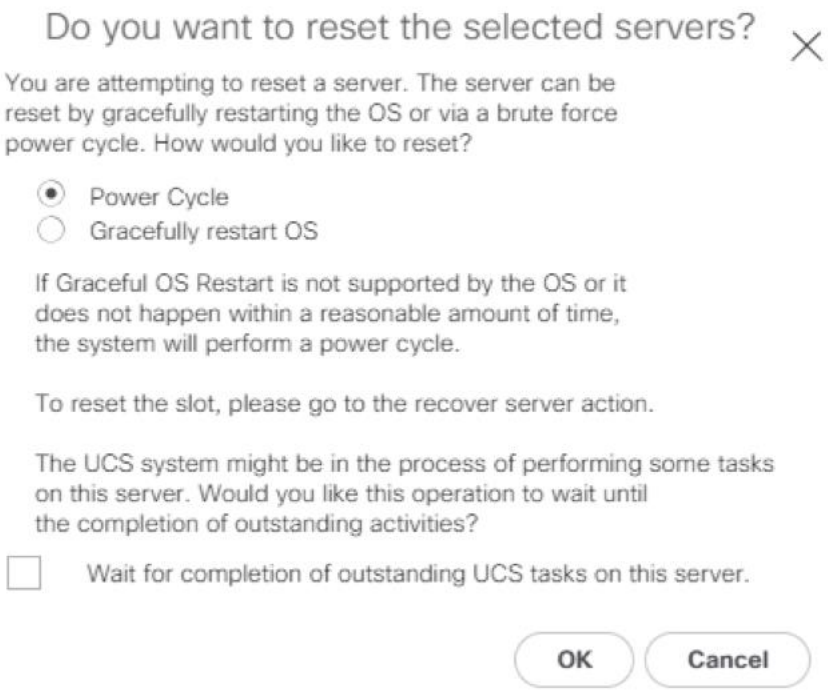
12. Click the **Server icon,** then click **Reset**.



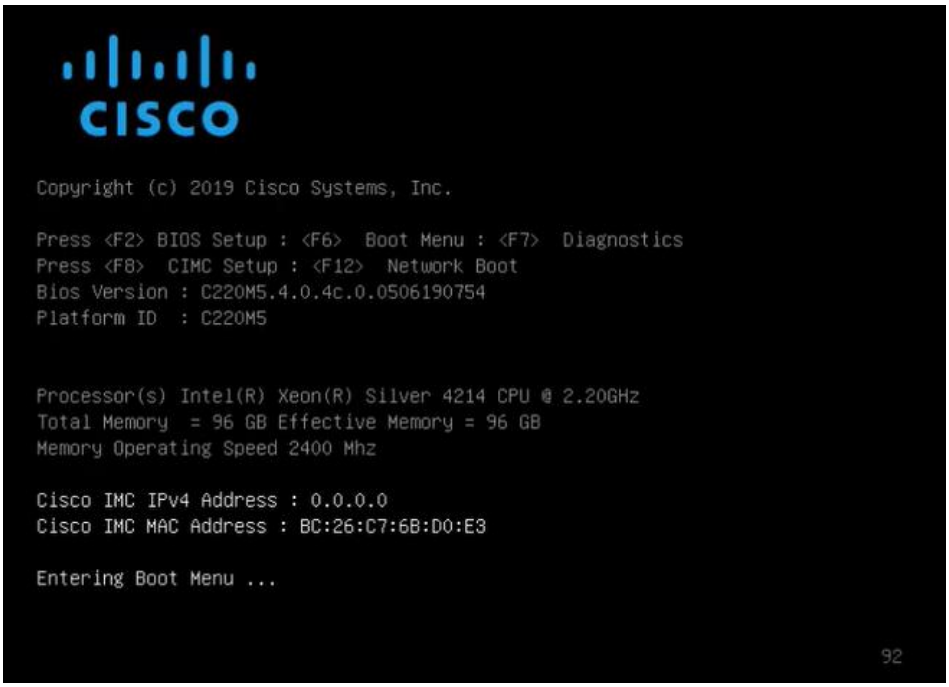
13. On the **Reset Server** pop up, click **OK.**



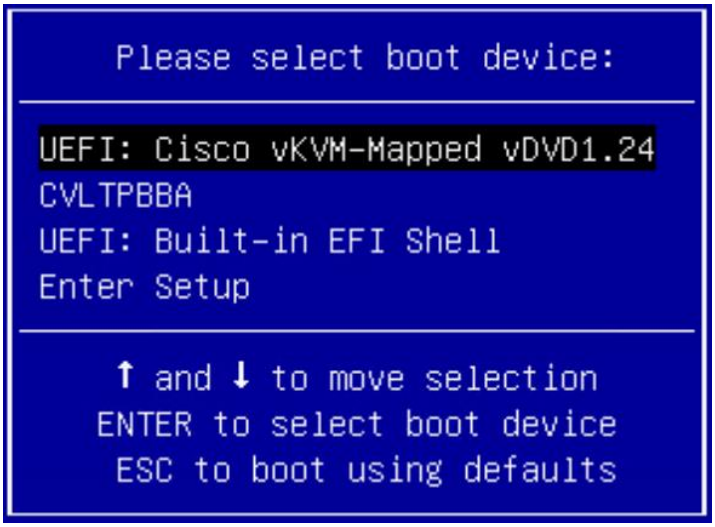
14. Select **Power Cycle,** then click **OK**.



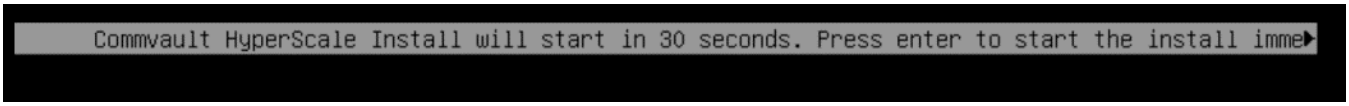
15. As the server is coming up, at the main screen, press **F6** to enter the boot menu.



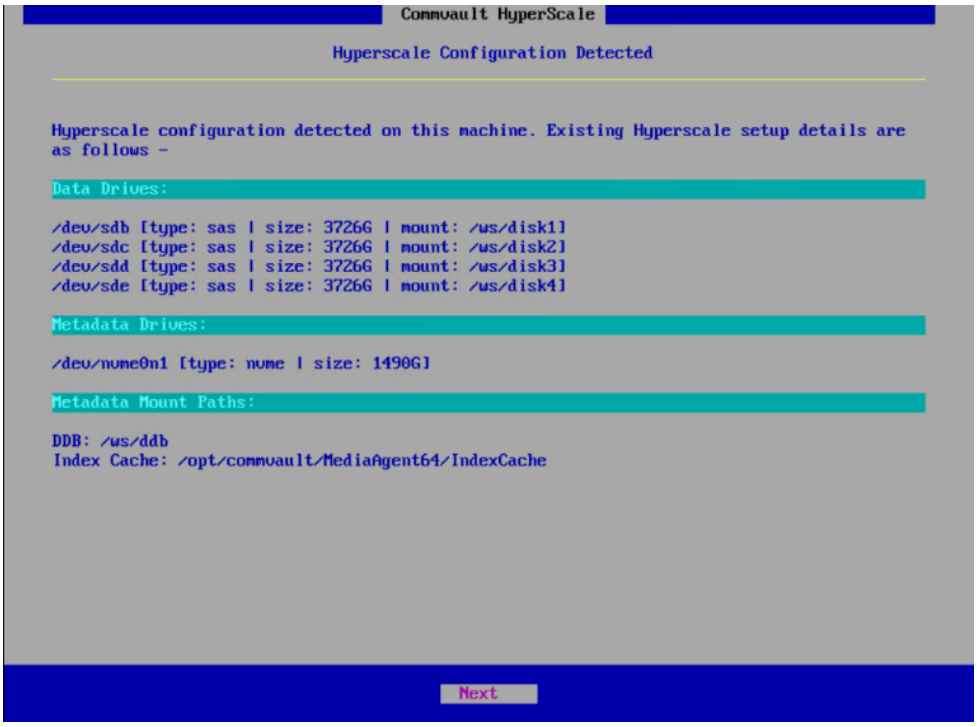
16. When the boot menu appears select `Cisco vKVM-Mapped vDVD`.



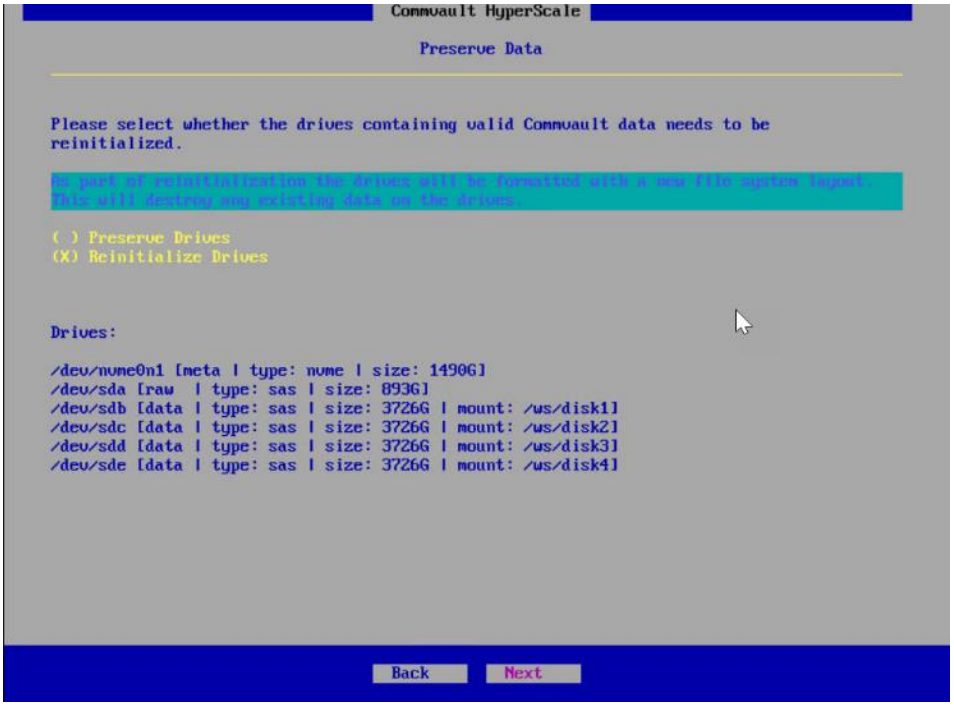
17. Once the ISO loads, it will start the install automatically in 30 seconds, or press **Enter** to start immediately.



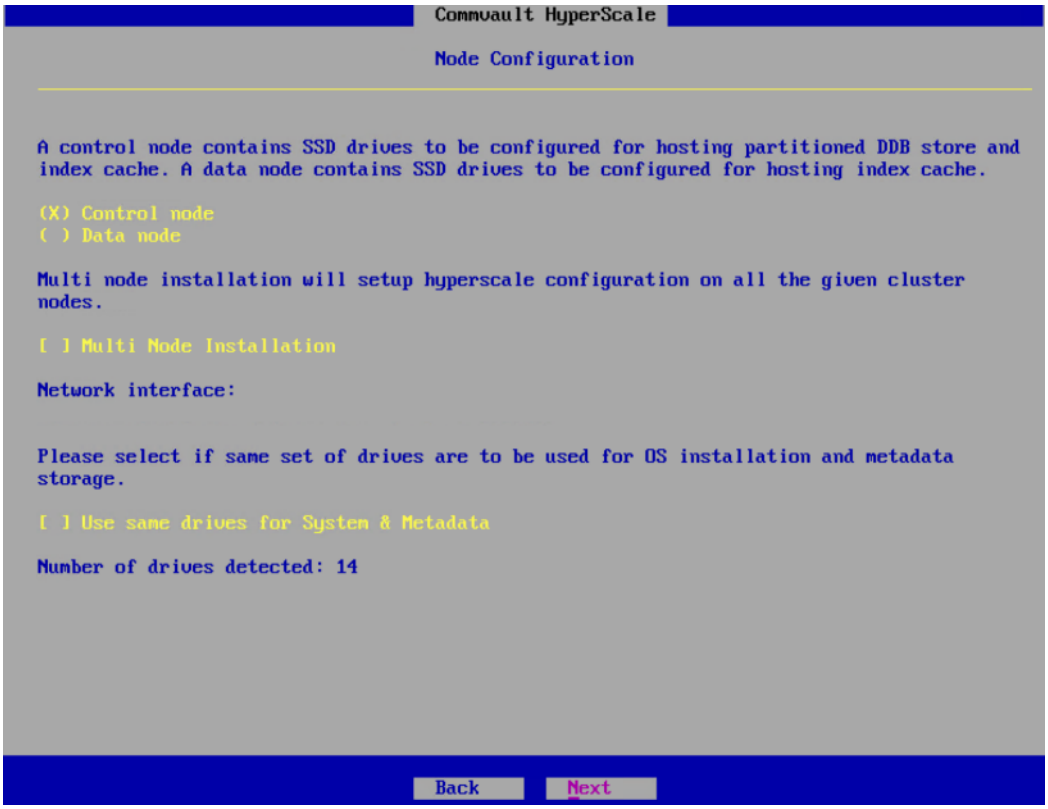
18. The first screen will come up and show the drives detected for the storage and the accelerated cache metadata, in the case of the UCS C220, it sees the Data drives (in this case the 10TB drives, and it shows it found 4 (1/4) and also found the NVMe cache of 1.6TB. Press **Tab** to select Next at the bottom to continue.



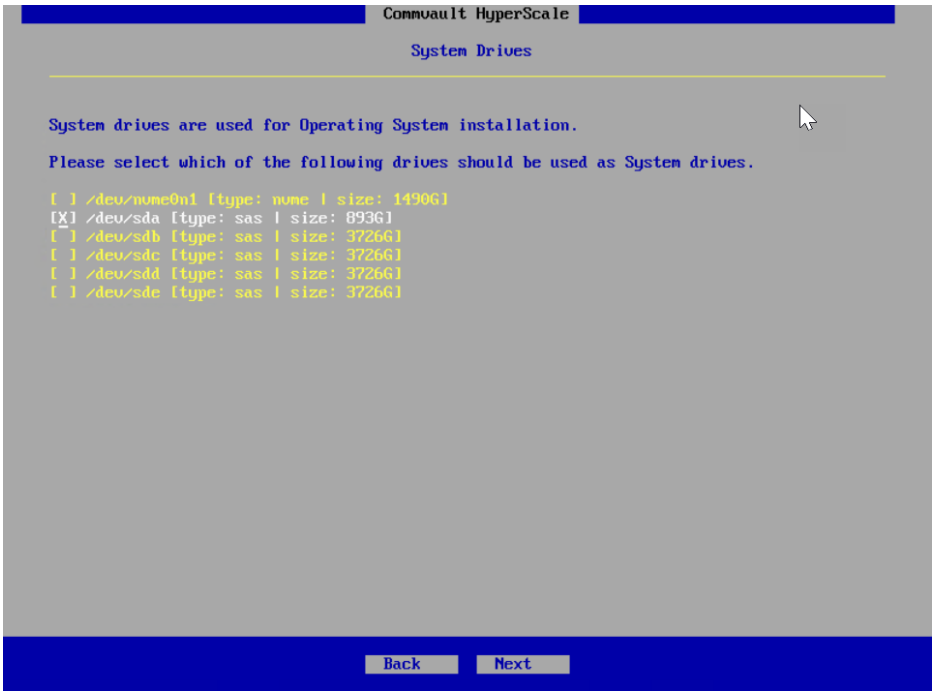
19. Select the option to **Reinitialize Drives**. Press tab to select **Next** at the bottom, then press **Enter**.



20. Select **Control Node** and select Multi Node Installation then press the Tab button to move down to **Next**. Before pressing **Enter**, see the next step.



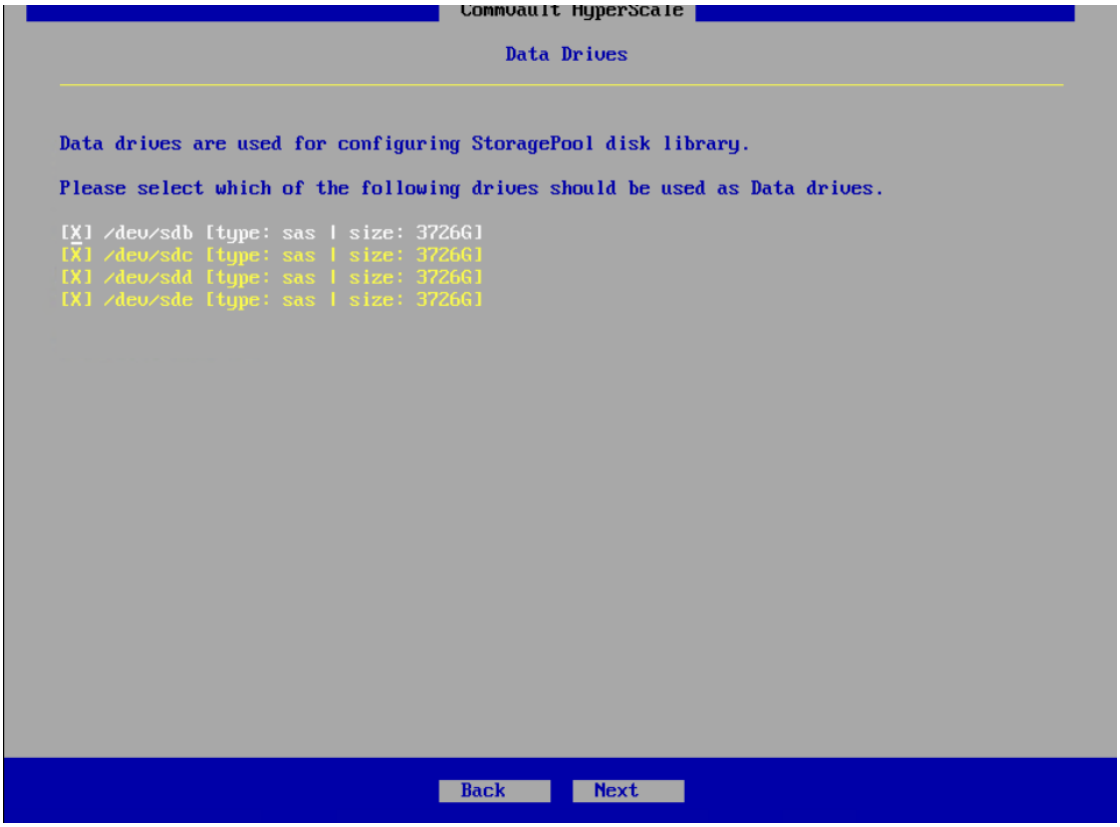
If the customer has **DHCP** available, you can select the **Multi Node Installation** option. If selected, you **MUST** run the installer on the remaining nodes and advance them to this screen before continuing. Whether using the **Multi Node** option or not, the next steps are the same.



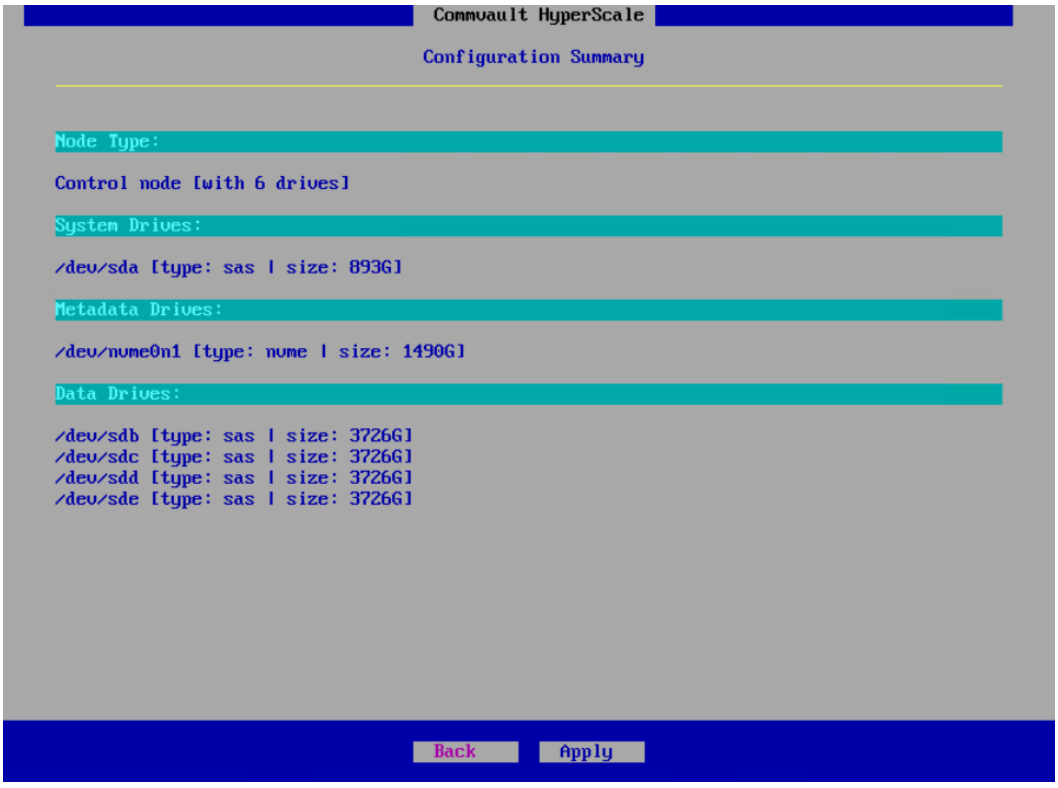
21. On the **System Drives** screen, select the **893GB** Drive (the 2 x M.2 960GB RAID1 drive), for the **OS**, then use Tab to select **Next** and press **Enter**.

22. On the **MetaData Drives** screen, select the 1490GB Drive (the 1.6TB NVMe) for the DDB and Index Cache, then press tab to select **Next**, then press **Enter**.

23. On the **Data Drives** screen, the remaining drives should be selected, press Tab to select **Next** at the bottom, then press **Enter**.

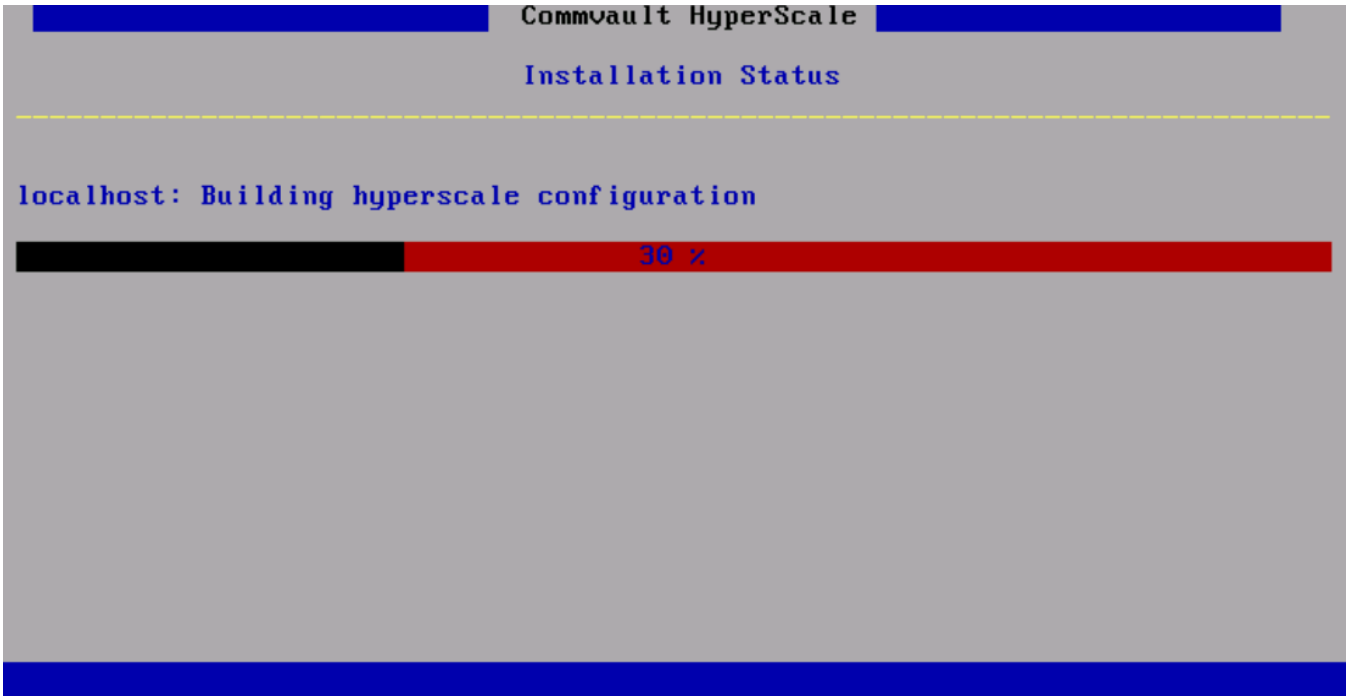


24. On the **Configuration Summary** screen, the selected drives will be displayed. Press Tab to select **Apply**, then press **Enter**.

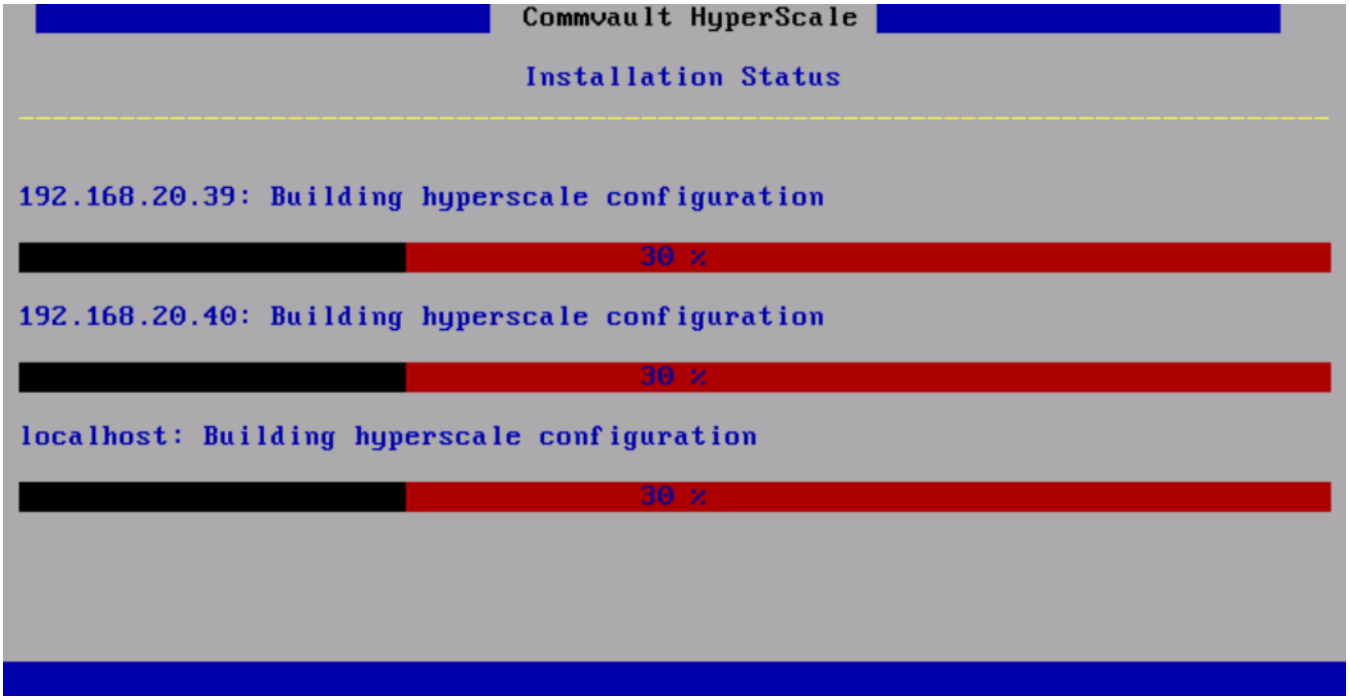


The Commvault HyperScale OS installation begins.

If using the **Non Multi Node Installation** option, the screen will look as follows:

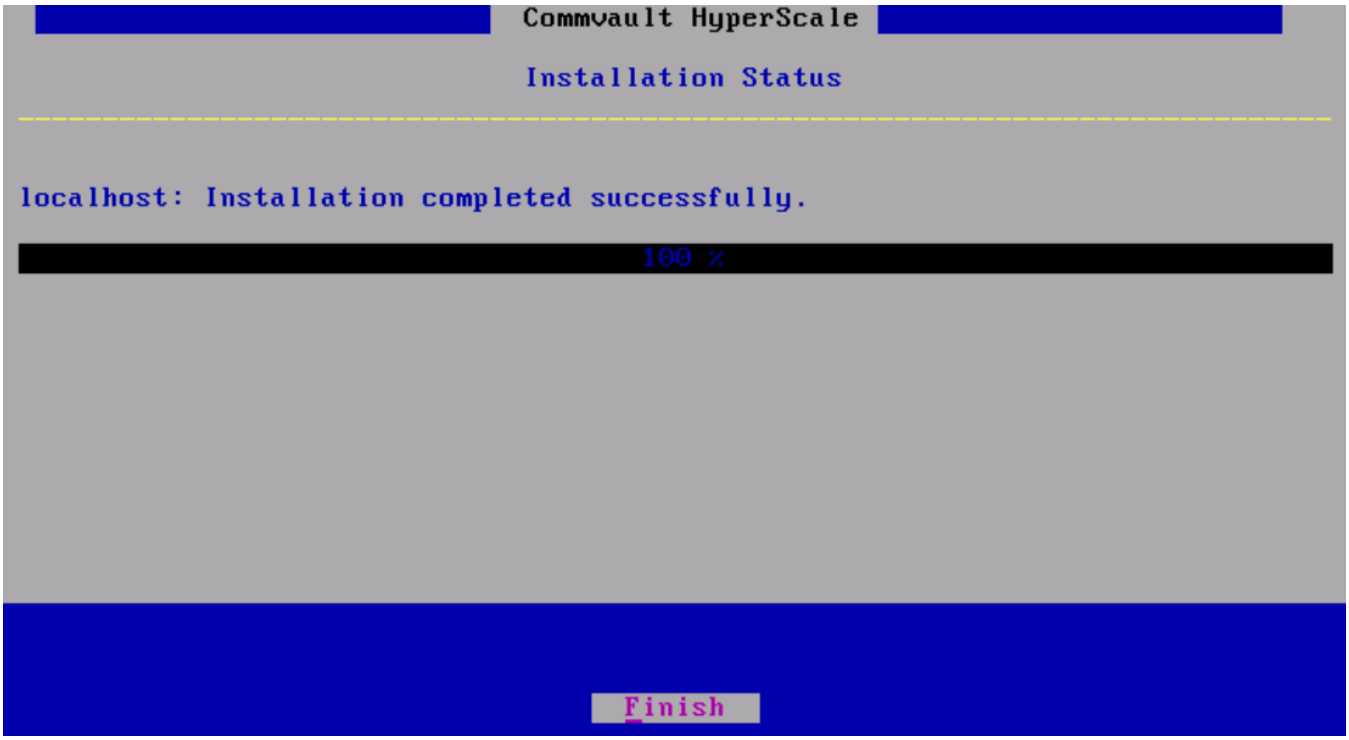


If using the **Multi Node Installation** option, the screen will look as follows:

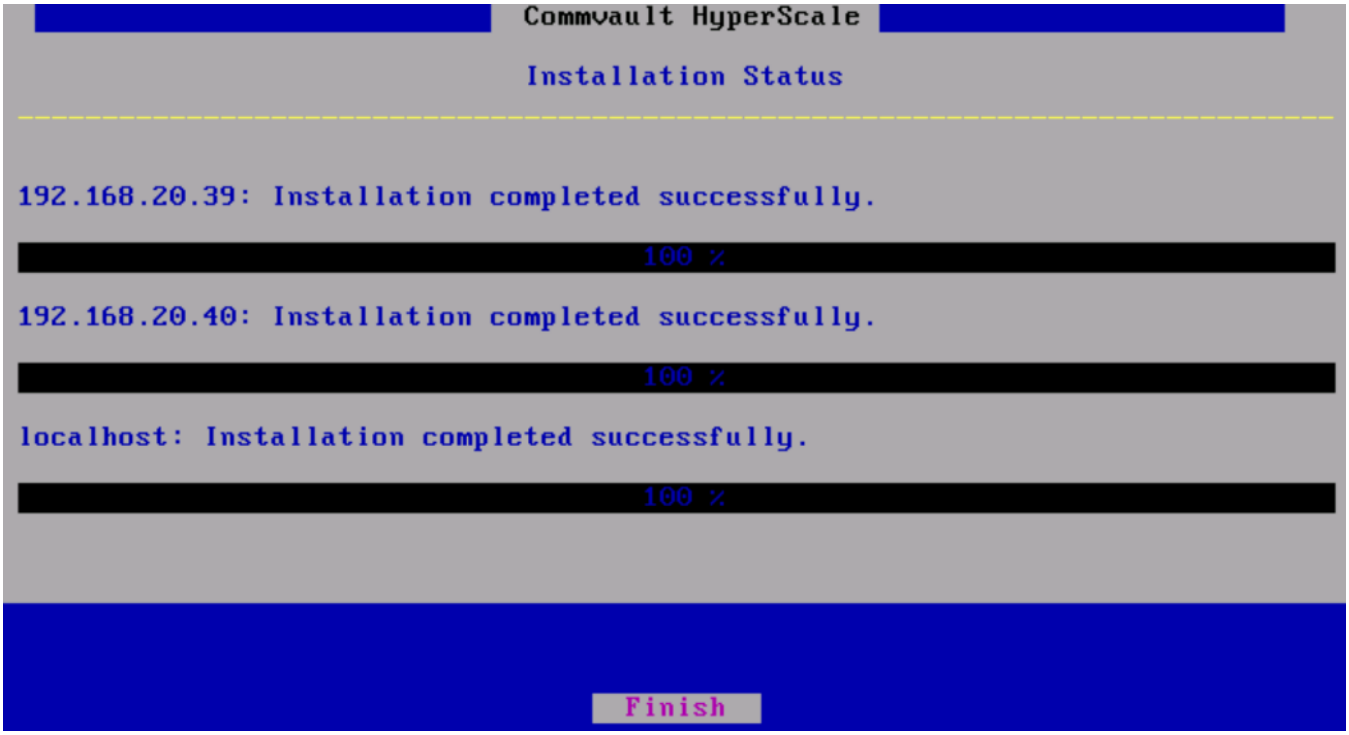


25. The OS install is now complete, select **Finish** and press **Enter.**

26. The completed installation screen for the Non-Multi Node Installation is shown below. Repeat steps 1-25 on the remaining nodes before continuing.



27. Completed install screen for the **Multi Node** Installation.



28. Allow the server to reboot and Linux to start up. At the login screen, the default login is **root** and the password is **cvadmin**. When using UCS Manager, the networking must be configured first. To do this from the prompt change to the **/etc/sysconfig/network-scripts** directory and type **ls** then enter. You will see a few files beginning with ifcfg-XXXXX. These are the network interface configuration files (in this case **ifcfg-hca1** and **ifcfg-hca2**). The **ifcfg-lo** is the loopback adapter and we do not need to touch this one.

```
[root@wzp21450eog ~]# cd /etc/sysconfig/network-scripts/
[root@wzp21450eog network-scripts]# ls
ifcfg-hca1   ifdown-eth   ifdown-ovs     ifdown-Team      ifup-bnep  ifup-isdn  ifup-ppp       ifup-tunnel
ifcfg-hca2   ifdown-ib    ifdown-post    ifdown-TeamPort  ifup-eth   ifup-ovs   ifup-routes    ifup-wireless
ifcfg-lo     ifdown-ippp  ifdown-ppp     ifdown-tunnel    ifup-ib    ifup-plip  ifup-sit       init.ipv6-global
ifdown       ifdown-ipv6  ifdown-routes  ifup             ifup-ippp  ifup-plusb ifup-Team      network-functions
ifdown-bnep  ifdown-isdn  ifdown-sit     ifup-aliases     ifup-ipv6  ifup-post  ifup-TeamPort  network-functions-ipv6
[root@wzp21450eog network-scripts]#
[root@wzp21450eog network-scripts]#
```

29. Type ifconfig, then enter, to see the network interfaces. In this case they are **enp28sofo** and **enp28sof1 (lo** is the loop-back interface). Also note the MAC address for each interface beside the word ether (in our case **00:25:b5:06:0a:3e** and **00:25:b5:06:0b:05**)

```
[root@wzp21450eog network-scripts]# ifconfig
enp28s0f0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::225:b5ff:fe06:a3e  prefixlen 64  scopeid 0x20<link>
        ether 00:25:b5:06:0a:3e  txqueuelen 1000  (Ethernet)
        RX packets 2599197  bytes 878066434 (837.3 MiB)
        RX errors 0  dropped 52  overruns 0  frame 0
        TX packets 48  bytes 3936 (3.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp28s0f1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9000
        inet6 fe80::225:b5ff:fe06:b05  prefixlen 64  scopeid 0x20<link>
        ether 00:25:b5:06:0b:05  txqueuelen 1000  (Ethernet)
        RX packets 2811223  bytes 957587134 (913.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 656 (656.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1978  bytes 124160 (121.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1978  bytes 124160 (121.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@wzp21450eog network-scripts]# _
```

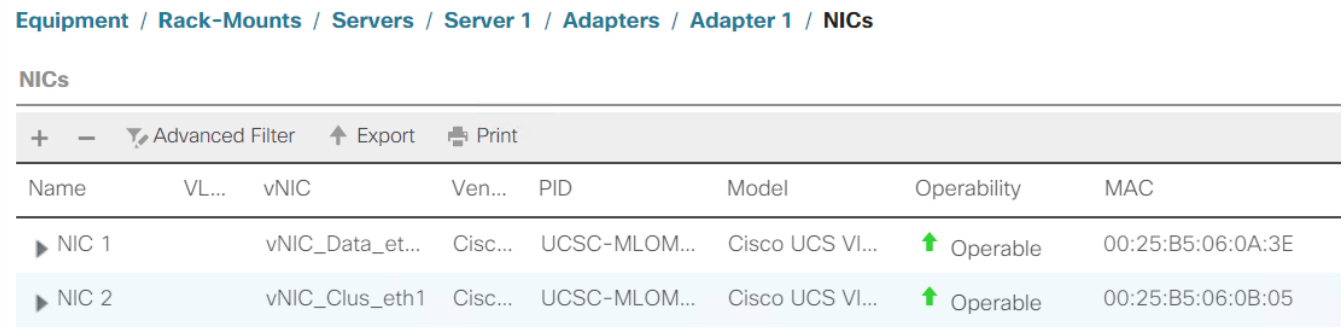
30. Type **cat ifcfg-hca1** to view the contents of the file. Look for the MAC address on the HWADDR line and match it to the interface from the previous step. In the below example it is **00:25:b5:06:0a:3e** which matches the interface **enp28sofo** above, so this is the configuration file for that interface. Which means that **ifcfg-hca2** is the configuration file for interface **enp28sof1,** which can be verified by viewing that file with the **cat** command and looking at the MAC address in that file.

```
[root@wzp21450eog network-scripts]# cat ifcfg-hca1
TYPE=Ethernet
ONBOOT=yes
BOOTPROTO=none
USERCTL=no
IPV6INIT=no
NM_CONTROLLED=no
HWADDR=00:25:b5:06:0a:3e
[root@wzp21450eog network-scripts]# _
```

31. Change the ifcfg files to match the interface names by using the **mv** command (for example, mv ifcfg-hca1 ifcfg-enp28sofo). Then use the **ls** command to verify.

```
[root@wzp21450eog network-scripts]# ls
ifcfg-enp28s0f0  ifdown-eth   ifdown-ovs     ifdown-Team      ifup-bnep  ifup-isdn  ifup-ppp       ifup-tunnel
ifcfg-enp28s0f1  ifdown-ib    ifdown-post    ifdown-TeamPort  ifup-eth   ifup-ovs   ifup-routes    ifup-wireless
ifcfg-lo         ifdown-ippp  ifdown-ppp     ifdown-tunnel    ifup-ib    ifup-plip  ifup-sit       init.ipv6-global
ifdown           ifdown-ipv6  ifdown-routes  ifup             ifup-ippp  ifup-plusb ifup-Team      network-functions
ifdown-bnep      ifdown-isdn  ifdown-sit     ifup-aliases     ifup-ipv6  ifup-post  ifup-TeamPort  network-functions-ipv6
[root@wzp21450eog network-scripts]#
```

32. Verify in Cisco UCS Manager which NIC is for Data and which one is for the Cluster. From below by the description in UCS Manager we can see that NIC 1 with MAC address **00:25:b5:06:0a:3e (enp28s0f0)** is the data NIC, and NIC 2 is the cluster NIC.



33. Modify the **ifcfg-enp28s0f0** file as per below, entering the device, IP address, default gateway, subnet mask, DNS server(s) and set the IP to static. This will be the Data network IP address.

```
DEVICE=enp28s0f0
TYPE=Ethernet
ONBOOT=yes
BOOTPROTO=static
USERCTL=no
IPV6INIT=no
NM_CONTROLLED=no
IPADDR=192.168.163.159
NETMASK=255.255.252.0
GATEWAY=192.168.160.1
DNS1=192.168.163.4
HWADDR=00:25:b5:06:0a:3e
```

34. Modify the **ifcfg-enp28s0f1** file as per below, entering the device, IP address, default gateway, subnet mask, DNS server(s) and set the IP to static. Depending on the network configuration, you may not need a DNS or gateway IP address. This will be the Cluster network IP address.

```
DEVICE=enp28s0f1
TYPE=Ethernet
ONBOOT=yes
BOOTPROTO=static
USERCTL=no
IPV6INIT=no
NM_CONTROLLED=no
IPADDR=10.168.163.159
NETMASK=255.255.255.0
HWADDR=00:25:b5:06:0b:05
```

35. Once modified, type in the **systemctl restart network** command to restart the networking on the server.

```
[root@wzp22380nn4 network-scripts]# ls
ifcfg-enp63s0f0  ifdown-eth   ifdown-ovs      ifdown-Team      ifup-bnep
ifcfg-enp63s0f1  ifdown-ib    ifdown-post     ifdown-TeamPort  ifup-eth
ifcfg-lo         ifdown-ippp  ifdown-ppp      ifdown-tunnel    ifup-ib
ifdown           ifdown-ipv6  ifdown-routes   ifup             ifup-ippp
ifdown-bnep      ifdown-isdn  ifdown-sit      ifup-aliases     ifup-ipv6
[root@wzp22380nn4 network-scripts]# systemctl restart network
```

36. Type **ifconfig** to verify the IP addresses are now assigned to the interfaces.

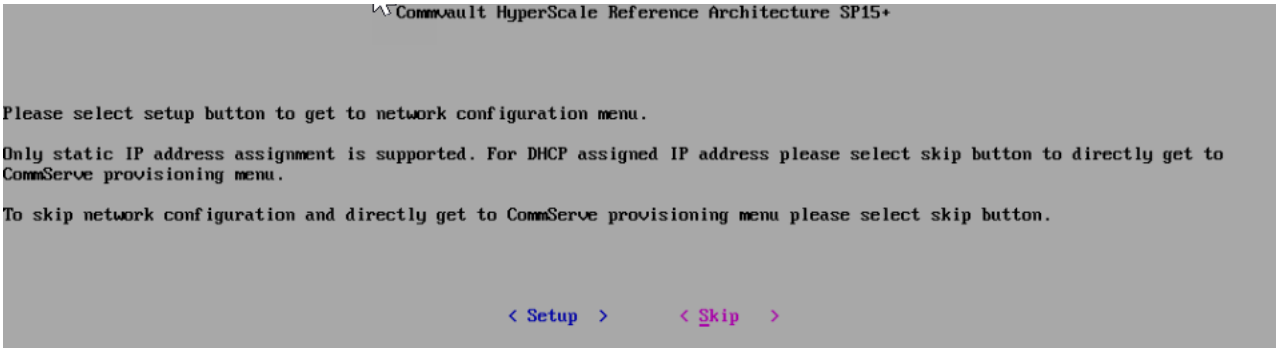
```
[root@c220node1 network-scripts]# ifconfig
enp28s0f0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.163.159  netmask 255.255.252.0  broadcast 192.168.163.255
        inet6 fe80::225:b5ff:fe06:a3e  prefixlen 64  scopeid 0x20<link>
        ether 00:25:b5:06:0a:3e  txqueuelen 1000  (Ethernet)
        RX packets 19435  bytes 1752751 (1.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2102  bytes 398437 (389.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp28s0f1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9000
        inet 10.168.163.159  netmask 255.255.255.0  broadcast 10.168.163.255
        inet6 fe80::225:b5ff:fe06:b05  prefixlen 64  scopeid 0x20<link>
        ether 00:25:b5:06:0b:05  txqueuelen 1000  (Ethernet)
        RX packets 99  bytes 18332 (17.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 43  bytes 3054 (2.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1897  bytes 240956 (235.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1897  bytes 240956 (235.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
[root@hsref MediaAgent]# cd /opt/commvault/MediaAgent
[root@hsref MediaAgent]# ls
answer_file.cfg       cvcreatefactory.py       cvnodetype.py          GlusterCommon.sh       nwwizard.py
archiveIndex          cvcsinit.py              cv_nw_sysconfig.py     GlusterInstaller       python_ui
auxCopy               cvcstype.py              cvnwtype.py            GlusterInstaller.tmpl  registertocs.py
binlist               cvdetectusb.py           cvovirtconfig.py       GlusterPreReqCheck.sh  registertocsui.py
bmr                   cvethwizard.py           cvovirtfence.py        gluster_rpms           Scripts
bmr.py                cvfirewalld.py           cvovirtsdk.py          gluster_rpms.tar       scsi_inq
CatalogMigration      cvfixperm.py             cvrbashcmdlist         grub.cfg               setkernelconsole
common.py             cvgatherlogs.py          cvrbashcommand.sh      IdxLabelUtil           setup.py
commvault_title.cfg   cvhcconfig.py            cvremotenwconfig.py    IndexCache             setupsds
compressor            cv_hs_auto_nwconf.py     cvrestartinstall.py    indexRestore           setupsds.tmpl
createcd.py           cvhyperscale             cvsetuphelper.py       init                   SynthFull
createcd.sh           cvhyperscale_install.py  cvsetuphname.py        init.py                test_cmd
createIndex           CVJobReplicator          cvsetupmgmthname.py    isolinux.bin           test_ready
createinitrd.sh       cvmagui                  cvsystem_config.py     isolinux.cfg           ui.py
cvaddovirthost.py     cvmetavgui.py            cvtestovirtsdk.py      libcvtinyxml2.so       ui.pyc
cvarchhelper.py       cvmgmtnwwizard.py        cvupdate_avahi.sh      libGlfsPbba.so         uncompressor
cvavahi.py            cvmkavahi.py             diskui.py              lvm.conf               updateIndex
cvchroot.sh           cvmonitor.py             dmWriter               MediaLabelReader       utils.py
cvclnwmgmt.py         CvMountd                 dsBackup               modeui.py              utils.pyc
cvclnw.py             CVNasFileScan            dsRestore              NasBackup              wrappers.py
cvcloudinit.sh        CVNasSnapBackup          efiboot.img            NASCreateIndex         wrappers.pyc
cvcluster.py          CVNasSnapRestore         efiboot.sh             nasRestore
cvconfigcleanup.py    CVNdmpRemoteServer       filter_drives.py       nwconfig.py
cvconfignw.py         CVNdmpSynthRemoteServer  FsIndexedRestore       nwintfx.py
[root@hsref MediaAgent]# ./setupsds_
```

37. Change the directory to **/opt/commvault/MediaAgent** and type the following command **./setupsds**

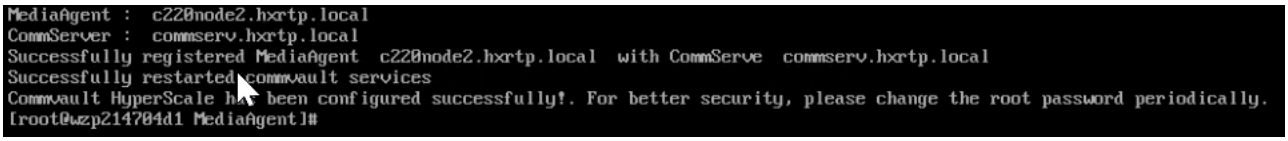
38. Enter the **hostname** of the server (use a FQDN if this will be part of a domain) and enter a **new password,** then use the arrow keys to select **OK.**

39. Select **Skip** to skip the network configuration since this was already completed in the previous steps.



40. Enter the **CommServe** information, then select **OK**.

The server is now registered with the Commserve.



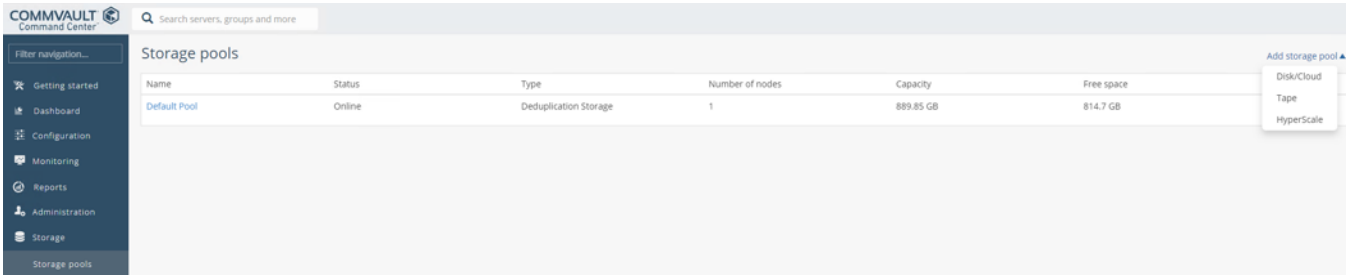
41. Commvault appends a suffix of "sds" to the node names, for example our name of **c220node1.hxrtp.local** will use **c220node1sds.hxrtp.local** for the inter-cluster communication. You may want to put these inter-cluster names into the hosts file on each server.

```
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
10.168.163.159  c220node1sds.hxrtp.local        c220node1sds
10.168.163.158  c220node2sds.hxrtp.local        c220node2sds
10.168.163.157  c220node3sds.hxrtp.local        c220node3sds
```

42. Repeat steps 1-41 on the remaining nodes.

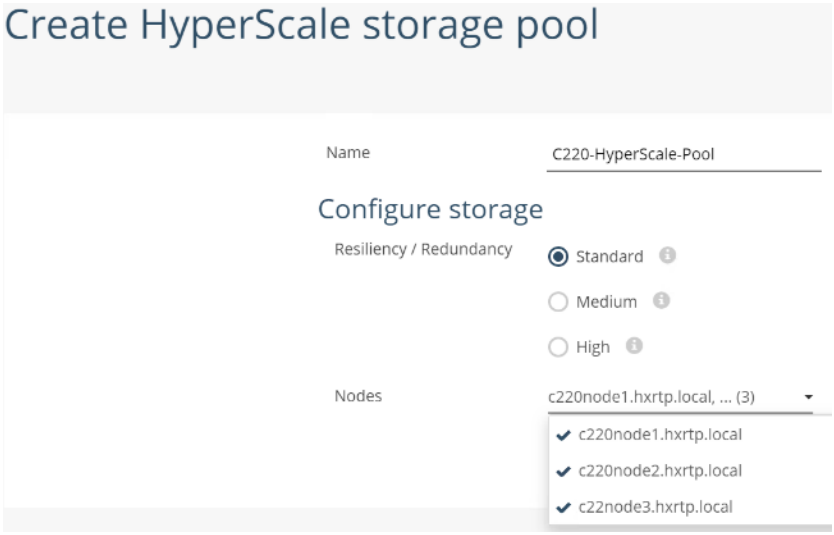
43. Once the final node has completed successfully, log on to the Command Center to complete the installation.

44. On the left pane, click **Storage**, then **Storage pools**, click **Add storage pool** and select **HyperScale**.

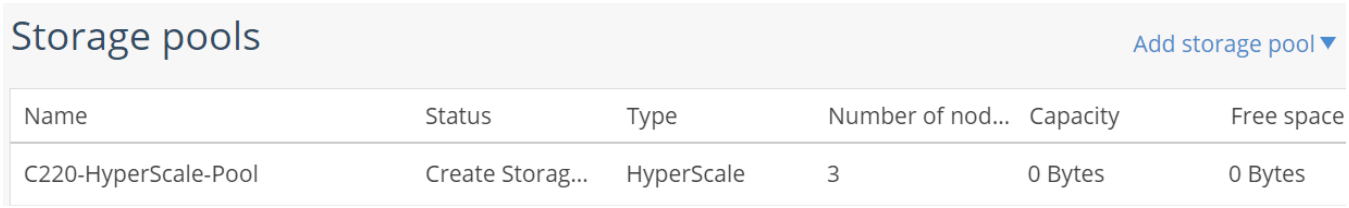


45. On the Create HyperScale storage pool page, enter a **name** for the pool, select the desired Resiliency/Redundancy factor and then click **Configure**.

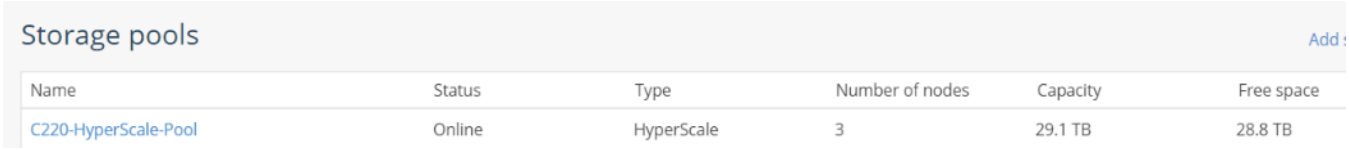
    - Standard – 3 Nodes, Disperse factor 6, Redundancy factor 2. Withstands loss of 2 drives or 1 node.
    - Medium – 6 Nodes, Disperse factor 6, Redundancy factor 2. Withstands loss of 2 drives or 2 nodes.
    - High – 6 Nodes, Disperse factor 12, Redundancy factor 4. Withstands loss of 4 drives or 2 nodes.

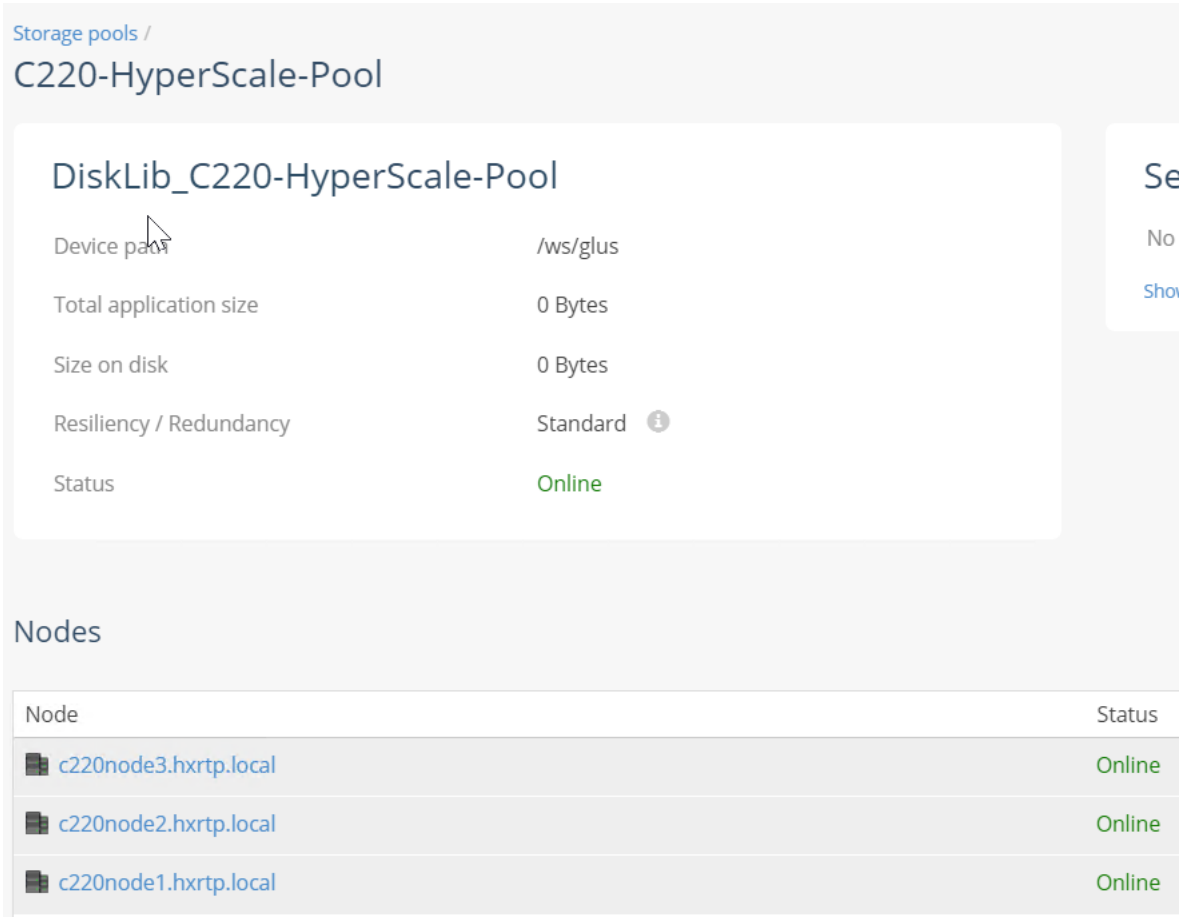


46. The Storage Pool will get created. It will show "Scale-out pool creation in progress" with 0 capacity for a few minutes as there is a background process that runs to create the gluster file system then bring it online. As part of the Storage Pool creation, the disk library will be created along with a Global dedup policy.



47. Click the newly created HyperScale Pool and verify that the pool and all nodes show as online. The HyperScale Pool is now ready for use.





Post Install Checklist

The following redundancy checks can be performed to verify the robustness of the system. Network traffic, such as a continuous ping from backup client or CommServe to ScaleProtect Cluster IP address, which should not show significant failures (one or two ping drops might be observed at times). Also, all of the Storage Pools must remain mounted and accessible from all the hosts at all times.

- Administratively disable one of the server ports on Fabric Interconnect A which is connected to one of the ScaleProtect hosts. The Data protection vNIC active on that Fabric Interconnect should failover to Fabric Interconnect B. Upon administratively re-enabling the port, the vNIC should return to normal state by failing back to the Fabric Interconnect A.
- Administratively disable one of the server ports on Fabric Interconnect B which is connected to one of the ScaleProtect hosts. The Cluster vNIC active on that Fabric Interconnect should failover to Fabric Interconnect B. Upon administratively re-enabling the port, the vNIC should return to normal state by failing back to the Fabric Interconnect B.
- Place a representative load of backup on the system. Log on to one of the nodes and shutdown the services (commvault stop). The backup operations and the access to storage pool should not be affected.
- Log into the node and start the services (commvault start). The ScaleProtect cluster will show as healthy after a brief time after starting the services on that node. HyperScale should rebalance the VM distribution across the cluster over time.

- Reboot one of the two Cisco UCS Fabric Interconnects while traffic is being sent and received on the ScaleProtect storage pool and the network. The reboot should not affect the proper operation of storage pool access and network traffic generated by the backup clients. Numerous faults and errors will be noted in Cisco UCS Manager, but all will be cleared after the FI comes back online.

References

Products and Solutions

Cisco Unified Computing System:

http://www.cisco.com/en/US/products/ps10265/index.html

Cisco UCS Fabric Interconnects:

https://www.cisco.com/c/en/us/products/servers-unified-computing/fabric-interconnects.html

Cisco UCS S-Series Storage Servers

https://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-s-series-storage-servers/index.html

Cisco UCS C-Series Rack Servers:

http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-c-series-rack-servers/index.html

Cisco UCS Adapters:

http://www.cisco.com/en/US/products/ps10277/prod_module_series_home.html

Cisco UCS Manager:

http://www.cisco.com/en/US/products/ps10281/index.html

Cisco Nexus 9000 Series Switches:

http://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/tsd-products-support-series-home.html

Commvault Complete Backup and Recovery:

https://www.commvault.com/solutions/by-function/data-protection-backup-and-recovery

Commvault HyperScale Software:

https://www.commvault.com/solutions/by-function/cloud-and-infrastructure-management/hyperscale

ScaleProtect with Cisco UCS:

https://www.commvault.com/solutions/by-technology/infrastructure/cisco-ucs/scaleprotect

About the Authors

Sreenivasa Edula, Technical Marketing Engineer, Cisco UCS Data Center Solutions Engineering, Cisco Systems, Inc.

Sreeni is a Technical Marketing Engineer in the UCS Data Center Solutions Engineering team focusing on converged and hyper-converged infrastructure solutions, prior to that he worked as a Solutions Architect at EMC Corporation. He has experience in Information Systems with expertise across Cisco Data Center technology portfolio, including DC architecture design, virtualization, compute, network, storage and cloud computing.

Acknowledgements

- Ulrich Kleidon, Cisco Systems, Inc.
- Samuel Nagalingam, Cisco Systems, Inc.
- Julio Calderon, Commvault Systems, Inc.
- Bryan Clarke, Commvault Systems, Inc.