

Cisco UCS for ScaleProtect with Cisco UCS S3260 Storage Servers

Deployment Guide for ScaleProtect with Cisco UCS Storage Servers, Cisco UCS S3260 M5 Server Nodes and Commvault HyperScale release 11 SP13

Last Updated: December 6, 2019



About the Cisco Validated Design Program

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

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

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

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

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unified Computing System (Cisco UCS), Cisco UCS B-Series Blade Servers, Cisco UCS C-Series Rack Servers, Cisco UCS S-Series Storage Servers, Cisco UCS Manager, Cisco UCS Management Software, Cisco Unified Fabric, Cisco Application Centric Infrastructure, Cisco Nexus 9000 Series, Cisco Nexus 7000 Series, Cisco Prime Data Center Network Manager, Cisco NX-OS Software, Cisco MDS Series, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

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

© 2019 Cisco Systems, Inc. All rights reserved.

Table of Contents

Executive Summary	6
Solution Overview	7
Introduction.....	7
Audience	7
Purpose of this Document	7
Solution Summary	7
Architectural Overview.....	8
Deployment Guidelines	11
Software Revisions	11
Configuration Guidelines.....	11
Physical Infrastructure	13
Cisco UCS Connectivity to Nexus Switches	13
Optional: Cisco UCS Connectivity to SAN Fabrics	14
Network Switch Configuration.....	16
ScaleProtect Implementation.....	16
Configure Cisco Nexus 9000 Switches.....	16
Cisco Nexus 9000 Initial Configuration Setup	17
Enable Appropriate Cisco Nexus 9000 Features and Settings.....	19
Cisco Nexus 9000 A and Cisco Nexus 9000 B.....	19
Create VLANs for ScaleProtect IP Traffic	20
Cisco Nexus 9000 A and Cisco Nexus 9000 B.....	20
Configure Virtual Port Channel Domain	20
Cisco Nexus 9000 A.....	20
Cisco Nexus 9000 B.....	21
Configure Network Interfaces for the vPC Peer Links	21
Cisco Nexus 9000 A.....	21
Cisco Nexus 9000 B.....	22
Configure Network Interfaces to Cisco UCS Fabric Interconnect.....	23
Cisco Nexus 9000 A.....	23
Cisco Nexus 9000 B.....	25
Uplink into Existing Network Infrastructure.....	26
Cisco Nexus 9000 A and B using Port Channel Example	26
Cisco UCS Server Configuration.....	28
Cisco UCS Base Configuration.....	28
Perform Initial Setup of Cisco UCS 6332-16UP Fabric Interconnects.....	28

Cisco UCS Setup	31
Log into Cisco UCS Manager.....	31
Upgrade Cisco UCS Manager Software to Version 4.0(1a).....	31
Anonymous Reporting	31
Configure Cisco UCS Call Home.....	32
Add Block IP Addresses for KVM Access	32
Synchronize Cisco UCS to NTP	33
Edit Chassis Discovery Policy	34
Enable Server Ports	35
Optional: Edit Policy to Automatically Discover Server Ports	36
Server Discovery	37
Optional: Enable Fibre Channel Ports	37
Optional: Create VSAN for the Fibre Channel Interfaces.....	39
Optional: Create Port Channels for the Fibre Channel Interfaces.....	43
Enable Ethernet Uplink Ports	45
Create Port Channels for Ethernet Uplinks.....	46
Cisco UCS S3260 Storage Server Configuration.....	49
Create Sub-Organization	50
Create MAC Address Pools	51
Create UUID Suffix Pool	55
Create Server Pool	56
Optional: Create a WWNN Address Pool for FC-based Storage Access	59
Optional: Create a WWPN Address Pools for FC Based Storage Access	60
Create VLANs	63
Create Host Firmware Package	65
Create Network Control Policy for Cisco Discovery Protocol.....	66
Create Power Control Policy	67
Create Server BIOS Policy	68
Create Maintenance Policy	70
Create Adapter Policy	71
Create vNIC Templates.....	72
Create LAN Connectivity Policy.....	78
Optional: Create vHBA Templates for FC Connectivity	82
Optional: Create FC SAN Connectivity Policies.....	86
Cisco UCS S3260 Chassis Setup	92
Chassis Profile Template.....	92
Create Chassis Firmware Packages.....	93

Create maintenance Policy	94
Create Disk Zoning Policy	94
Create Chassis Profile Template	99
Create Chassis Profile(s) from Template	101
Associate Chassis Profile to S3260 Chassis.....	102
Cisco UCS S3260 Server Node Setup	105
LUN Cleanup.....	105
Set Cisco UCS S3260 Disk to Unconfigured Good	105
Cisco UCS S3260 Storage Profile	106
Create Disk Group Policies.....	106
Create Storage Profile.....	115
Create Boot Policy	124
Cisco UCS S3260 Service Profile Template	126
Create Service Profile Template	126
Create Service Profiles	141
Commvault HyperScale Installation and Configuration	145
Validation	164
Post Install Checklist.....	164
Verify Redundancy	165
About the Authors.....	166
Acknowledgements	166



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 S3260 Storage 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 UCS Solution.

The design that will be implemented is discussed in detail in the ScaleProtect with Cisco UCS design guide found here:

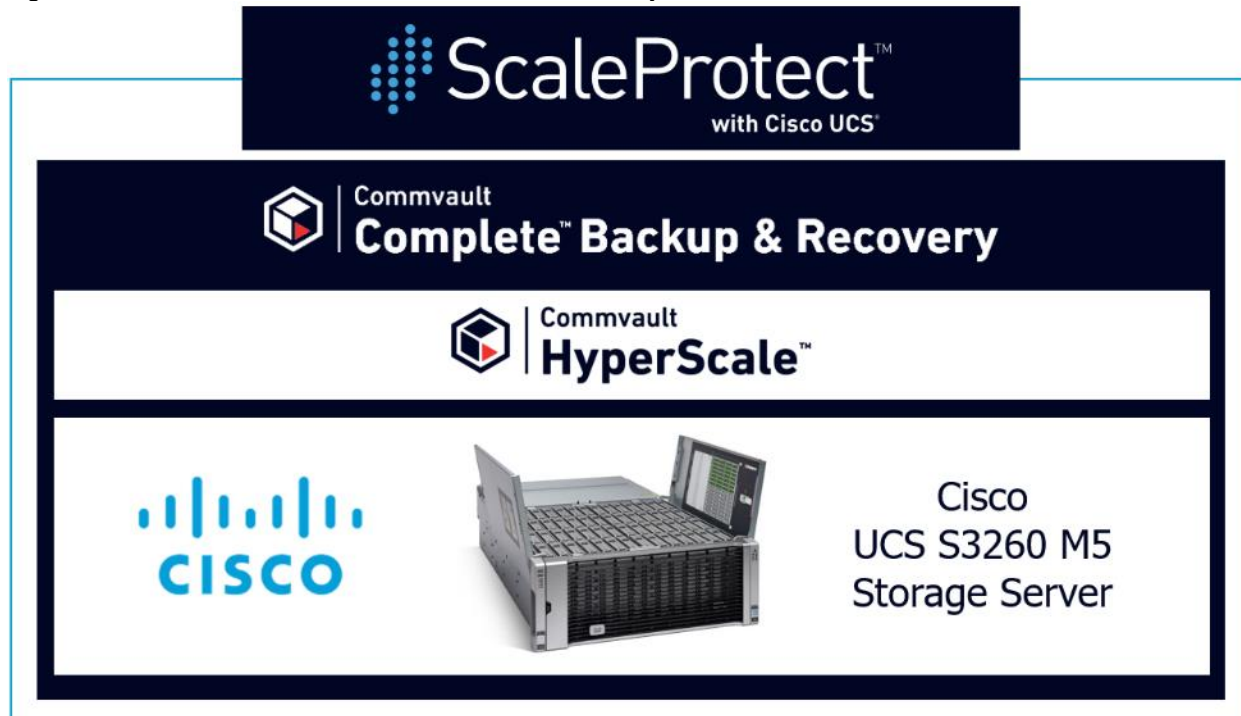
https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/ucs_s3260m5_commvault_scaleprotect_designguide.html

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.

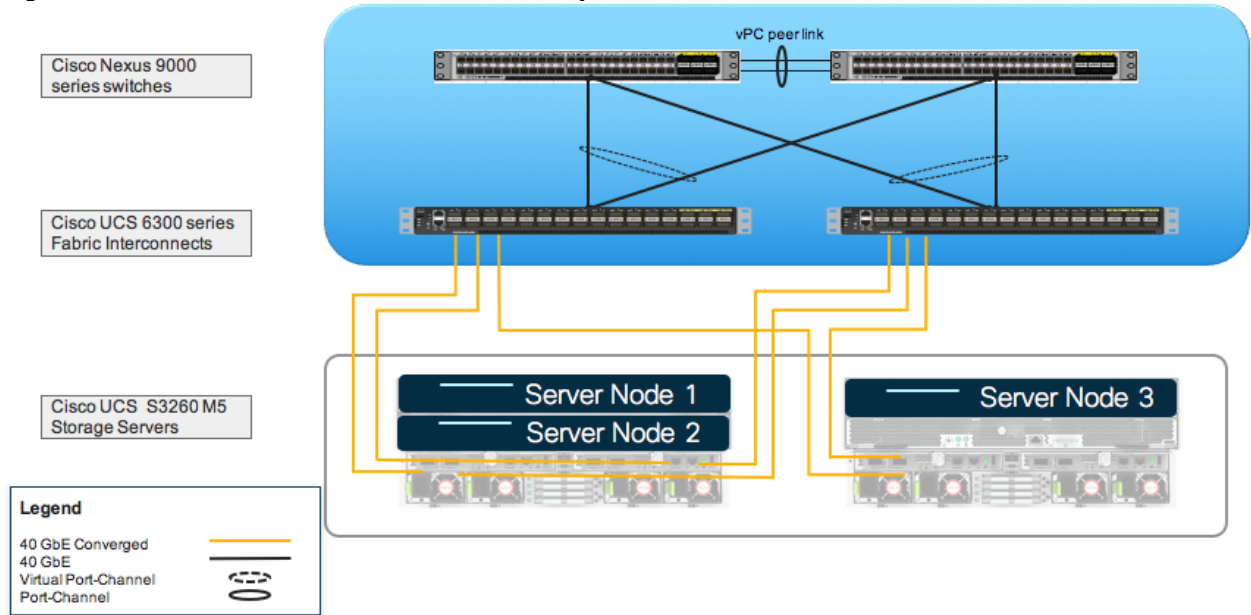
Figure 1 ScaleProtect with Cisco UCS Solution Summary



Architectural Overview

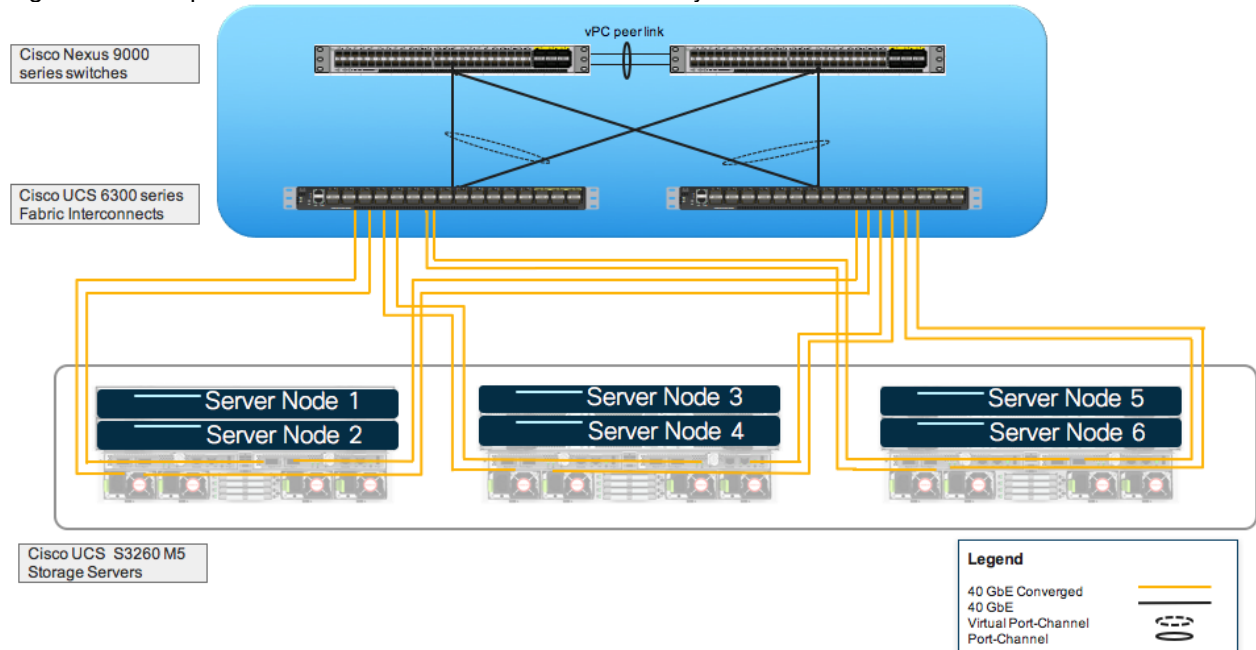
A typical ScaleProtect with Cisco UCS deployment starts with a 3-node block. The solution has been validated with three Cisco UCS S3260 M5 Server Nodes spread across two Cisco UCS S3260 Storage Server Chassis with built-in storage that consists of top-loaded Large Form Factor (LFF) HDDs for the software defined data storage tier, top-loaded Solid-State Drives (SSDs) for the accelerated cache tier, and rear mounted SSDs for the operating system and associated binaries. Connectivity for the solution is provided via a pair of Cisco UCS 6332-16UP Fabric Interconnects and to a pair of Cisco Nexus 9332PQ upstream network switches.

Figure 2 3-Node ScaleProtect with Cisco UCS Physical Architecture



ScaleProtect with Cisco UCS can start with more nodes than the standard 3 nodes; the additional nodes are simply added to the Cisco UCS 6300 Series Fabric Interconnects for linear scalability. The only difference between a 3 or 6-node configuration is the chassis configuration of the S3260 M5. In the 3-node starting block, there is a dual node S3260 and a single node S3260, while in the 6-node configuration there are 3 dual nodes. Figure 3 illustrates a 6-node starting architecture.

Figure 3 Example: 6-Node ScaleProtect with Cisco UCS Physical Architecture



This validated configuration uses the following components for deployment:

- Cisco Unified Computing System
 - Cisco UCS Manager

- Cisco UCS 6332 Series Fabric Interconnect
- Cisco UCS S3260 Storage Server
- Cisco UCS S3260 M5 Server Node
- Cisco UCS S3260 system IO controller with VIC 1380
- Cisco Nexus C9332PQ Series Switches
- Commvault Complete Backup and Recovery v11
- Commvault HyperScale Software

Deployment Guidelines

This document explains 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 the 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 6300 Series Fabric Interconnects	4.0(1a)
	Cisco UCS S3260 Storage Server	4.0(1a)
Network	Cisco Nexus 9332PQ NX-OS	9.2(1)
Software	Cisco UCS Manager	4.0(1a)
	Commvault Complete Backup and Recovery	v11 Service Pack 13
	Commvault HyperScale Software	v11 Service Pack 13

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-9332-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.

Enter the required IP addresses for the installation of a 3-node ScaleProtect cluster in the following tables:

Table 4 Out of Band Network Details

Network	Subnet Mask	Gateway

Table 5 Out of Band IP Address Details

Device	Hostname	Management IP Address
Nexus 9k Switch A		
Nexus 9k Switch B		
UCS Fabric Interconnect 6300 A		
UCS Fabric Interconnect 6300 B		
UCS Cluster VIP		

Table 6 HyperScale IP Address Details

Device	Hostname	Data Protection / Management IP Address	Cluster IP Address
HyperScale Node1			

Device	Hostname	Data Protection / Management IP Address	Cluster IP Address
HyperScale Node2			
HyperScale Node3			

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.



You can choose interfaces and ports of your liking but failure to follow the exact connectivity shown in the 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 4.

Figure 4 Cisco UCS Connectivity to the Nexus Switches

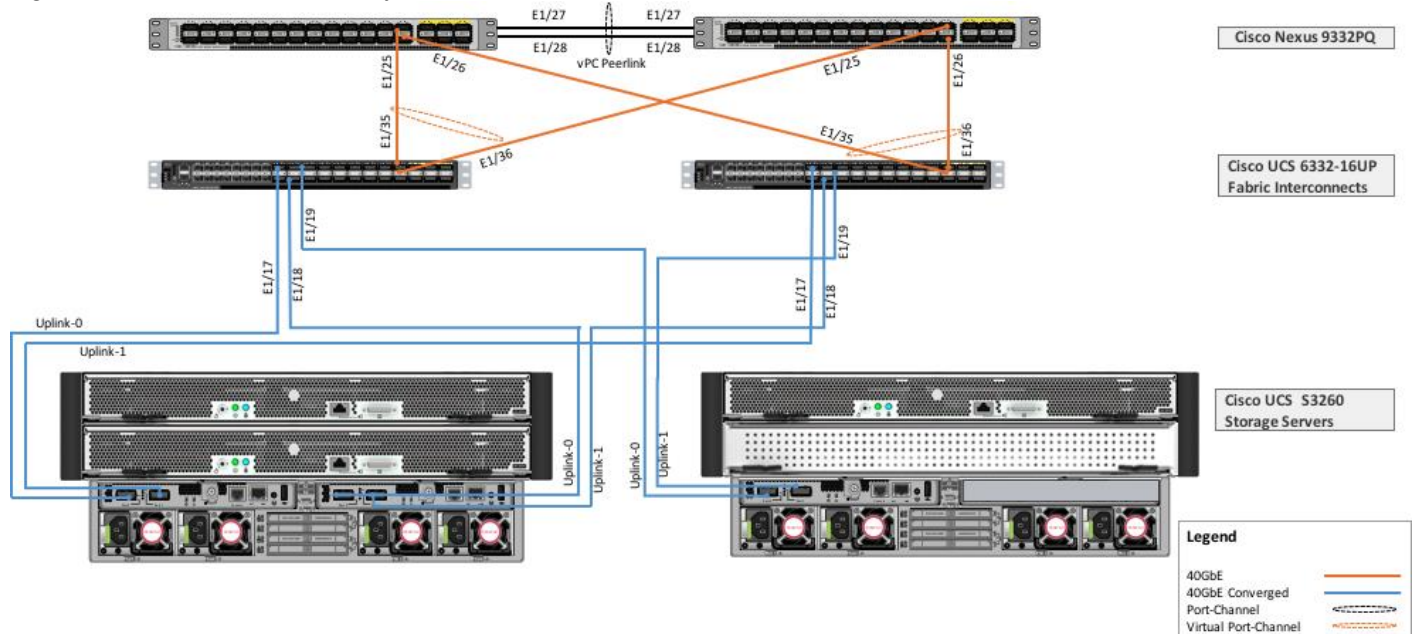


Table 7 Cisco UCS S3260 Chassis Connectivity to Cisco UCS Fabric Interconnects

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect A	Eth1/17	40GbE	Cisco UCS S3260 Chassis1 SIOC-1	VIC Port 0
Cisco UCS Fabric Interconnect A	Eth1/18	40GbE	Cisco UCS S3260 Chassis1 SIOC-2	VIC Port 0
Cisco UCS Fabric Interconnect A	Eth1/19	40GbE	Cisco UCS S3260 Chassis2 SIOC-1	VIC Port 0

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect B	Eth1/17	40GbE	Cisco UCS S3260 Chassis1 SIOC-1	VIC Port 1
Cisco UCS Fabric Interconnect B	Eth1/18	40GbE	Cisco UCS S3260 Chassis1 SIOC-2	VIC Port 1
Cisco UCS Fabric Interconnect B	Eth1/19	40GbE	Cisco UCS S3260 Chassis2 SIOC-1	VIC Port 1

Table 8 Cisco UCS FI Connectivity to Nexus Switches

Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect A	Eth1/35	40GbE	Cisco Nexus 9332PQ A	Eth1/25
Cisco UCS Fabric Interconnect A	Eth1/36	40GbE	Cisco Nexus 9332PQ B	Eth1/25
Cisco UCS Fabric Interconnect B	Eth1/35	40GbE	Cisco Nexus 9332PQ A	Eth1/26
Cisco UCS Fabric Interconnect B	Eth1/36	40GbE	Cisco Nexus 9332PQ B	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 9396S has been shown as an example), refer to Figure 5. 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 on UCS but doesn't cover the Cisco MDS switch configuration details and end device configurations such as Storage Arrays or Tape Library's.

Figure 5 Cisco UCS Connectivity to Cisco MDS Switches

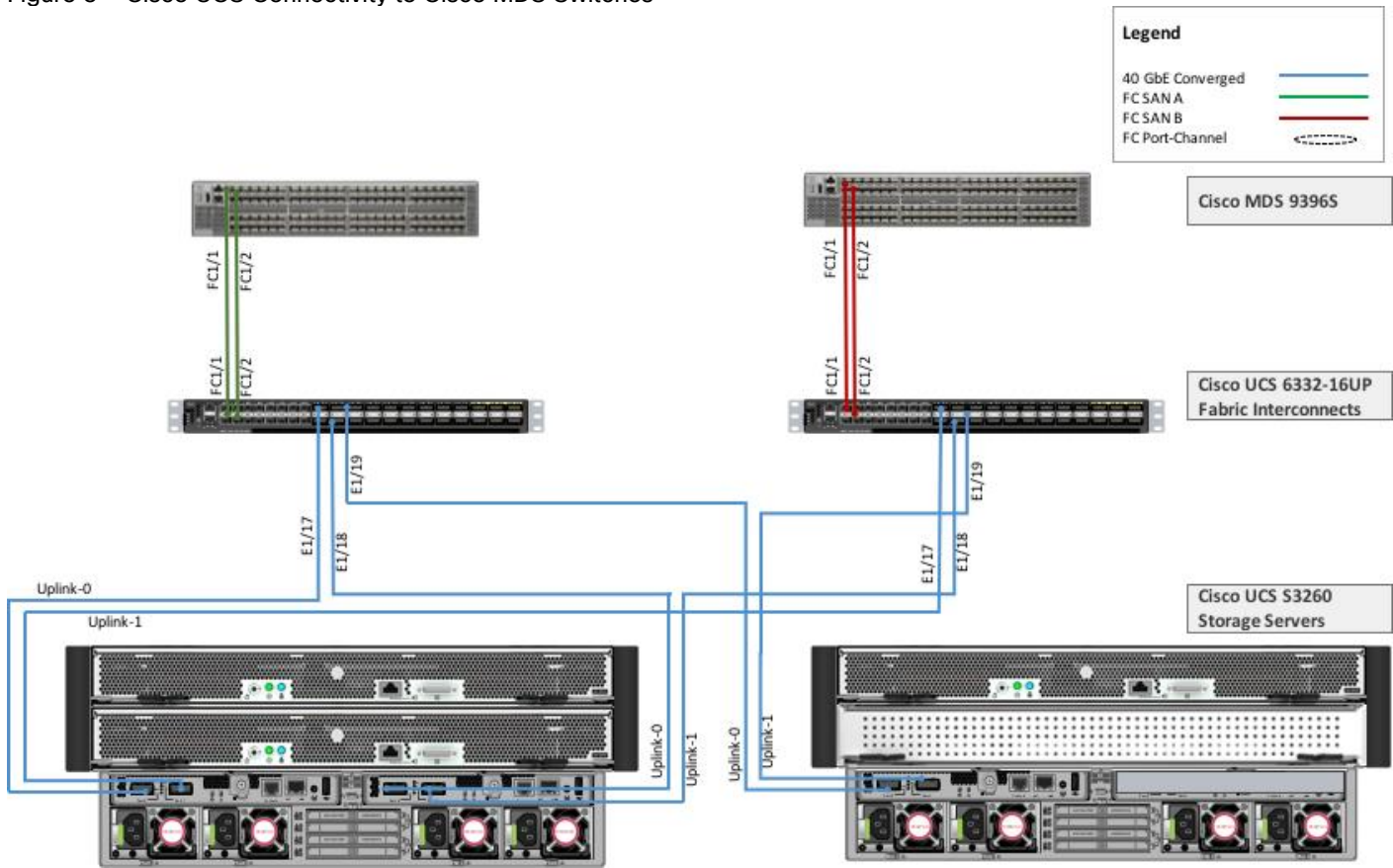


Table 9 Optional: Cisco UCS Connectivity to Cisco MDS Switches

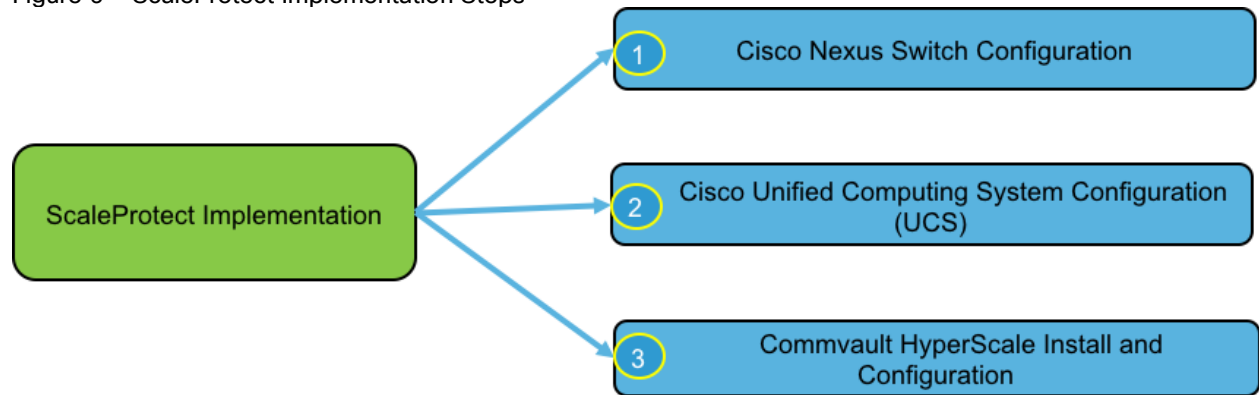
Local Device	Local Port	Connection	Remote Device	Remote Port
Cisco UCS Fabric Interconnect A	FC1/1	16Gbps	Cisco MDS 9396S A	FC1/1
Cisco UCS Fabric Interconnect A	FC1/2	16Gbps	Cisco MDS 9396S A	FC1/2
Cisco UCS Fabric Interconnect B	FC1/1	16Gbps	Cisco MDS 9396S B	FC1/1
Cisco UCS Fabric Interconnect B	FC1/2	16Gbps	Cisco MDS 9396S B	FC1/2

Network Switch Configuration

ScaleProtect Implementation

Figure 6 illustrates the ScaleProtect implementation workflow which is explained in the following sections.

Figure 6 ScaleProtect Implementation Steps

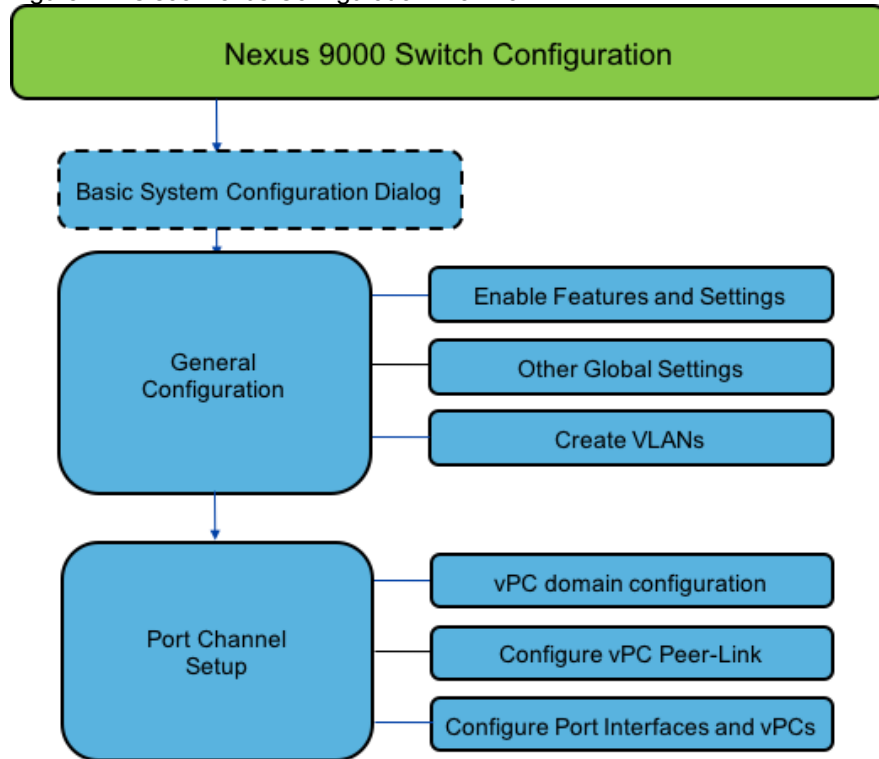


Configure Cisco Nexus 9000 Switches

This section explains how to configure the Cisco Nexus 9000 switches used in this ScaleProtect environment. Some changes may be appropriate for your environment, but care should be taken when deviating from these instructions as it may lead to an improper configuration.

For detailed information, refer to [Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide](#).

Figure 7 Cisco Nexus Configuration Workflow



Cisco Nexus 9000 Initial Configuration Setup

This section explains describes how to configure the Cisco Nexus switches to use in a ScaleProtect environment. This procedure assumes that you are using Cisco Nexus 9000 9.2(1).

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.

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

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

```
Enter the password for "admin": <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

Review the configuration summary before enabling the configuration.

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

```

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.

```

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

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

    Enter the password for "admin": <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

Review the configuration summary before enabling the configuration.

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

```

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 lldp
```

```
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
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 this step 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 Po11
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 11
```

```
no shutdown
```

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

```
interface Eth1/25
description <UCS Cluster Name>-A:35
```

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

```
channel-group 11 force mode active
no shutdown
```

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

```
interface Po12
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 12
no shutdown
```

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

```
interface Eth1/26
description <UCS Cluster Name>-B:1/35
```

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

```
channel-group 12 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 Po11
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 11
no shutdown
```

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

```
interface Eth1/25
description <UCS Cluster Name>-A:1/36
```

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

```
channel-group 11 force mode active
no shutdown
```

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

```
interface Po12
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:1/36
```

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

```
channel-group 12 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 9332PQ 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
```

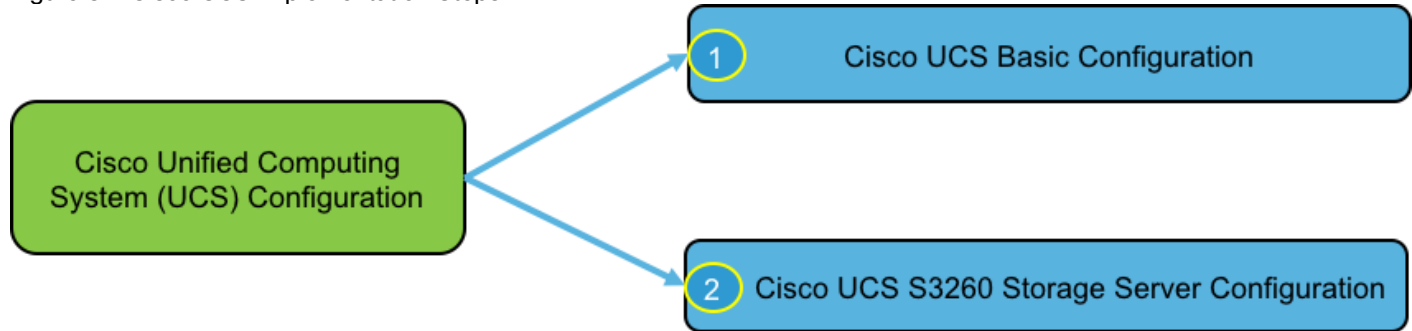
7. Save the running configuration to start-up in both Nexus 9000s and run commands to look at port and port channel information.

```
Copy run start
sh int eth1/33 br
sh port-channel summary
```

Cisco UCS Server Configuration

This section explains how to configure the Cisco Unified Computing System to use in a ScaleProtect environment. These steps are necessary to provision the Cisco UCS S3260 Storage Servers and should be followed precisely to avoid improper configuration.

Figure 8 Cisco UCS Implementation Steps



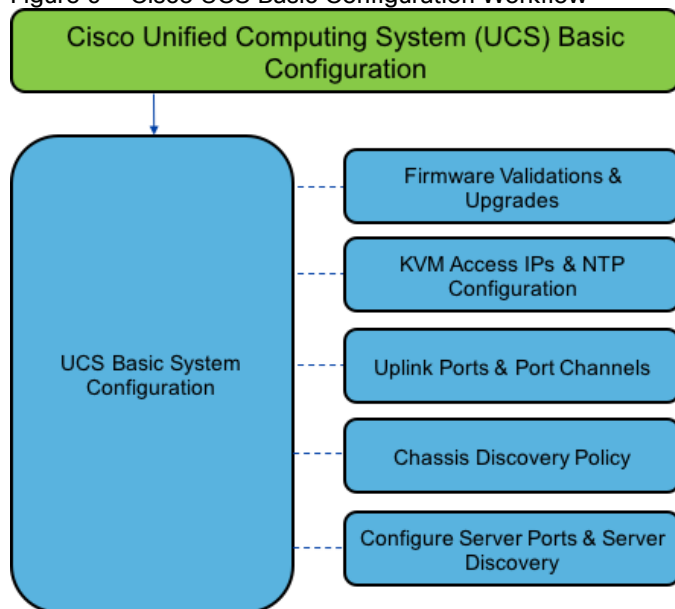
This document includes the configuration of the Cisco UCS infrastructure to enable SAN connectivity to existing storage environment. The ScaleProtect design for this solution doesn't need SAN connectivity and additional information is included only as a reference and should be skipped if SAN connectivity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

Cisco UCS Base Configuration

Perform Initial Setup of Cisco UCS 6332-16UP Fabric Interconnects

This section covers the configuration steps for the Cisco UCS 6332-16UP Fabric Interconnects (FI) in a ScaleProtect design that includes Cisco UCS S3260 Storage Servers.

Figure 9 Cisco UCS Basic Configuration Workflow



Cisco UCS 6332-16UP 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:

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

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

Type Ctrl-C at any time to abort configuration and reboot system.

To back track or make modifications to already entered values, complete input till end of section and answer no when prompted to apply configuration.

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

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

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

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

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

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

Enter the system name: <Name of the UCS System, ex:AA10-CVLT-6332>

Physical Switch Mgmt0 IP address : <Mgmt. IP address for Fabric A, ex:192.168.163.131>

Physical Switch Mgmt0 IPv4 netmask : <Mgmt. IP Subnet Mask, ex:255.255.252.0>

IPv4 address of the default gateway : <Default GW for the Mgmt. IP, ex:192.168.160.1>

Cluster IPv4 address : <Cluster Mgmt. IP address, ex:192.168.163.130>

Configure the DNS Server IP address? (yes/no) [n]: <DNS IP address, ex:192.168.160.50>

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

DNS IP address : <DNS IP Address, ex:192.168.160.50>

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

Default domain name : <<DNS Domain Name, ex:scaleprotect.cisco.com>

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

Following configurations will be applied:

```
Switch Fabric=A
System Name=AA10-CVLT-6332
Enforced Strong Password=yes
Physical Switch Mgmt0 IP Address=192.168.163.131
Physical Switch Mgmt0 IP Netmask=255.255.252.0
Default Gateway=192.168.160.1
Ipv6 value=0
DNS Server=192.168.160.50
Domain Name=scaleprotect.cisco.com
```

```
Cluster Enabled=yes
Cluster IP Address=192.168.163.130
```

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

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

Configuration file - Ok

Cisco UCS 6332 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:

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

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

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

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

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

```

Enter the admin password of the peer Fabric interconnect:
Connecting to peer Fabric interconnect... done
Retrieving config from peer Fabric interconnect... done
Peer Fabric interconnect Mgmt0 IPv4 Address: <Mgmt. IP address for Fabric A,
ex:192.168.163.131>
Peer Fabric interconnect Mgmt0 IPv4 Netmask: <Mgmt. IP Subnet Mask, ex:255.255.252.0>
Cluster IPv4 address      : <Cluster Mgmt. IP address, ex:192.168.163.130>

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, ex:192.168.163.132>

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

Configuration file - Ok

```

Cisco UCS Setup

Log into Cisco UCS Manager

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

1. Open a web browser and navigate to the Cisco UCS fabric interconnect cluster address.
2. Click the Launch UCS Manager link 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 into Cisco UCS Manager.

Upgrade Cisco UCS Manager Software to Version 4.0(1a)

This document assumes you are using Cisco UCS 4.0(1a). To upgrade the Cisco UCS Manager software and the Cisco UCS Fabric Interconnect software to version 4.0(1a), refer to [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:

Anonymous Reporting

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

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

[View Sample Data](#)

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

☒ Yes ☐ No

☐ Don't show this message again.

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.

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.

Create Block of IPv4 Addresses



From :	<input type="text" value="192.168.163.181"/>	Size :	<input type="text" value="20"/>
Subnet Mask :	<input type="text" value="255.255.252.0"/>	Default Gateway :	<input type="text" value="192.168.160.1"/>
Primary DNS :	<input type="text" value="0.0.0.0"/>	Secondary DNS :	<input type="text" value="0.0.0.0"/>

OK

Cancel

- Click OK to create.
- Click OK in the confirmation message.

Synchronize Cisco UCS to NTP

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

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

All / Time Zone Management / Timezone

General Events

Actions

Add NTP Server

Properties

Time Zone :

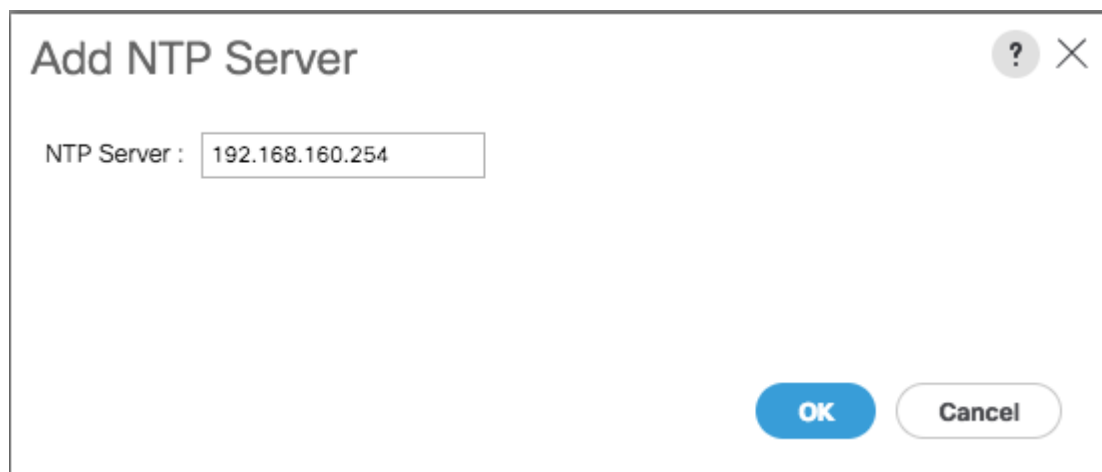
NTP Servers

Advanced Filter Export Print

Name

No data available

- In the Properties pane, select the appropriate time zone in the Timezone menu.
- Click Save Changes and then click OK.
- Click Add NTP Server.
- Enter <NTP Server IP Address> and click OK.

A dialog box titled "Add NTP Server" with a question mark icon and a close button (X) in the top right corner. Inside the dialog, there is a label "NTP Server :" followed by a text input field containing the IP address "192.168.160.254". At the bottom right of the dialog, there are two buttons: a blue "OK" button and a white "Cancel" button with a grey border.

Add NTP Server

NTP Server : 192.168.160.254

OK Cancel

Edit Chassis Discovery Policy

The chassis discovery policy determines how the system reacts when you add a new Cisco UCS S3260 chassis to a Cisco UCS system. Cisco UCS Manager uses the settings in the chassis discovery policy to determine whether to group links from the system I/O controllers (SIOCs) to the fabric interconnects in fabric port channels. To modify the chassis discovery policy, follow these steps:



To add a previously standalone Cisco UCS S3260 chassis to a Cisco UCS system, you must first configure it to the factory default. You can then connect both SIOCs on the chassis to both fabric interconnects. After you connect the SIOCs on the chassis to the fabric interconnects, and mark the ports as server ports, chassis discovery begins.

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. Set the Link Grouping Preference to None.

Equipment

Main Topology View	Fabric Interconnects	Servers	Thermal	Decommissioned	Firmware Management	Policies
--------------------	----------------------	---------	---------	----------------	---------------------	-----------------

Global Policies	Autoconfig Policies	Server Inheritance Policies	Server Discovery Policies	SEL Policy	Power Groups
------------------------	---------------------	-----------------------------	---------------------------	------------	--------------

Chassis/FEX Discovery Policy

Action : 1 Link ▼

Link Grouping Preference : ☒ None ☐ Port Channel

Backplane Speed Preference : ☒ 40G ☐ 4x10G

Rack Server Discovery Policy

Action : ☒ Immediate ☐ User Acknowledged

Scrub Policy : <not set> ▼

Rack Management Connection Policy

Action : ☒ Auto Acknowledged ☐ User Acknowledged

Power Policy

Redundancy : ☐ Non Redundant ☒ N+1 ☐ Grid

MAC Address Table Aging

Aging Time : ☐ Never ☒ Mode Default ☐ other

Global Power Allocation Policy

Allocation Method : ☐ Manual Blade Level Cap ☒ Policy Driven Chassis Group Cap

5. Click Save Changes.

6. 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.



UCS Port Auto-Discovery Policy can be optionally enabled to discover the servers without having to manually define the server ports. The procedure in the 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 S3260 M5 Server Nodes.
9. Wait for a brief period, until the rack-mount server appears in the Equipment tab underneath Equipment > Rack Mounts > Servers, or the chassis appears underneath Equipment > Chassis.

The screenshot shows the Cisco UCS Manager interface. On the left, the navigation pane is expanded to 'Equipment' > 'Fabric Interconnects' > 'Fabric Interconnect A (primary)' > 'Fixed Module' > 'Ethernet Ports'. The main pane shows a table of Ethernet ports. The first port (Slot 1, Aggr. Port ID 0, Port ID 17) is selected. The table has columns: Slot, Aggr. Port ID, Port ID, MAC, If Role, If Type, Overall Status, Admin State, and Peer.

Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status	Admin State	Peer
1	0	17	00:DE:FB:AE:FA:DC	Server	Physical	Up	Enabled	sys/chassis-1/slot-1/...
1	0	18	00:DE:FB:AE:FA:E0	Server	Physical	Up	Enabled	sys/chassis-1/slot-2/...
1	0	19	00:DE:FB:AE:FA:E4	Server	Physical	Up	Enabled	sys/chassis-2/slot-1/...

Optional: Edit Policy to Automatically Discover Server Ports

If the 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**.

The screenshot shows the 'Equipment' section of the Cisco UCS Manager. The 'Policies' tab is selected. Under 'Policies', the 'Port Auto-Discovery Policy' is selected. The 'Properties' section shows the 'Auto Configure Server Port' setting set to 'Enabled'.

Equipment

Main Topology View Fabric Interconnects Servers Thermal Decommissioned Firmware Management **Policies** Faults Diagnostics

Global Policies Autoconfig Policies Server Inheritance Policies Server Discovery Policies SEL Policy Power Groups **Port Auto-Discovery Policy** Security

Actions

Use Global

Properties

Owner : **Local**

Auto Configure Server Port : ☐ Disabled ☒ Enabled

5. Click Save Changes.

- 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 S3260 storage 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:

- In Cisco UCS Manager, click the Equipment tab in the navigation pane and click Equipment in the top of the navigation tree on the left. In the properties pane, click the Servers tab.
- Click the Chassis > Chassis1 Tab and view the Chassis status in the Overall Status column.
- When the chassis is discovered, the Cisco UCS S3260 storage server is displayed as shown below:

- Click the Equipment > Chassis Tab and view the servers' status in the Overall Status column. Below are the Cisco S3260 M5 Servers for ScaleProtect Cluster:

Name	Chassi...	PID	Model	User L...	Cores	Cores ...	Memory	Adapt...	NICs	HBAs	Overall Status	Operability	Power State
Ser...	1	UCS-S3260-M5S...	Cisco UCS S...		20	20	2621.44	1	0	0	Unassociated	Operable	On
Ser...	1	UCS-S3260-M5S...	Cisco UCS S...		20	20	2621.44	1	0	0	Unassociated	Operable	On
Ser...	2	UCS-S3260-M5S...	Cisco UCS S...		20	20	2621.44	1	0	0	Unassociated	Operable	On

Optional: Enable Fibre Channel Ports



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

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.

The screenshot shows the Cisco UCS Manager interface. On the left, a navigation sidebar has 'Equipment' selected. The main panel displays the configuration for 'Fabric Interconnect B (subordinate)'. The 'General' tab is active, showing a 'Fault Summary' with four status indicators (all at 0). Below this, the 'Status' section shows 'Overall Status : Operable', 'Thermal : OK', 'Ethernet Mode : End Host', 'FC Mode : End Host', 'Admin Evac Mode : Off', and 'Oper Evac Mode : Off'. The 'Actions' section lists various management tasks, with 'Configure Unified Ports' highlighted.

2. Slide the lever to change the ports 1–6 to Fiber Channel. Click Finish followed by Yes to the reboot message. Click OK.

Configure Unified Ports



Instructions

The position of the slider determines the type of the ports.

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

- 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



Creation of 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:

- In Cisco UCS Manager, click the SAN tab in the navigation pane.
- Expand the SAN > SAN Cloud and select Fabric A.
- Right-click VSANs and choose Create VSAN.
- Enter **Backup-A** as the name of the VSAN for fabric A.
- Keep the Disabled option selected for FC Zoning.
- Click the Fabric A radio button.
- Enter **201** as the VSAN ID for Fabric A.
- Enter **201** as the FCoE VLAN ID for fabric A. Click OK twice.

Create VSAN



Name :

FC Zoning Settings

FC Zoning : ☒ Disabled ☐ Enabled

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

☐ Common/Global ☒ Fabric A ☐ Fabric B ☐ Both Fabrics Configured Differently

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

Enter the VSAN ID that maps to this VSAN.

VSAN ID :

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

Enter the VLAN ID that maps to this VSAN.

FCoE VLAN :

OK

Cancel

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

Create VSAN



Name : Backup-B

FC Zoning Settings

FC Zoning : ☒ Disabled ☐ EnabledDo **NOT** enable local zoning if fabric interconnect is connected to an upstream FC/FCoE switch.
☐ Common/Global
 ☐ Fabric A
 ☒ Fabric B
 ☐ Both Fabrics Configured Differently

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

Enter the VSAN ID that maps to this VSAN.

VSAN ID : 202

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

Enter the VLAN ID that maps to this VSAN.

FCoE VLAN : 202

OK

Cancel

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

Create VSAN

Name : vSAN-A

FC Zoning Settings

FC Zoning : ☒ Disabled ☐ Enabled

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

☐ Common/Global
☒ Fabric A
☐ Fabric B
☐ Both Fabrics Configured Differently

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

Enter the VSAN ID that maps to this VSAN.

VSAN ID : 101

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

Enter the VLAN ID that maps to this VSAN.

FCoE VLAN : 101

OK

Cancel

23. In the SAN tab, expand SAN > SAN Cloud > Fabric-B.

24. Right-click VSANs and choose Create VSAN.

25. Enter **vSAN-B** as the name of the VSAN for fabric B.

26. Keep the Disabled option selected for FC Zoning.

27. Click the Fabric B radio button.

28. Enter 102 as the VSAN ID for Fabric B. Enter 102 as the FCoE VLAN ID for Fabric B. Click OK twice.

42

Create VSAN

?

×

Name :

FC Zoning Settings

FC Zoning : ☒ Disabled ☐ Enabled

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

☐ Common/Global ☐ Fabric A ☒ Fabric B ☐ Both Fabrics Configured Differently

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

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

Enter the VSAN ID that maps to this VSAN.

Enter the VLAN ID that maps to this VSAN.

VSAN ID :

FCoE VLAN :

OK

Cancel

Optional: Create Port Channels for the Fibre Channel Interfaces

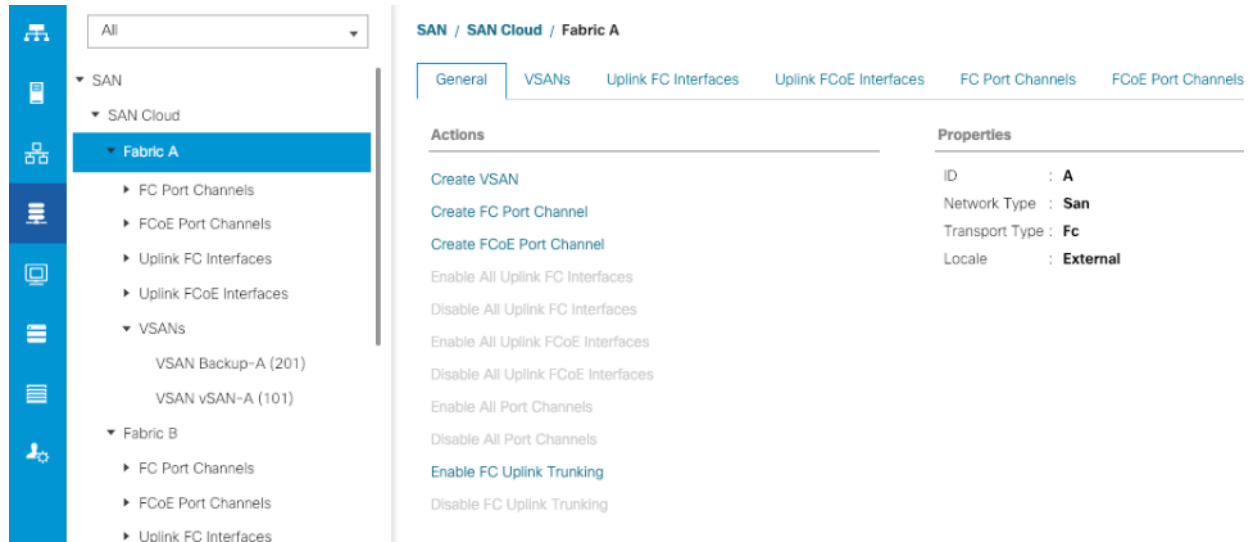


As mentioned above, Fibre channel connectivity is optional and the following procedure to create port-channels is included for reference and the procedure varies depending on the upstream SAN infrastructure.

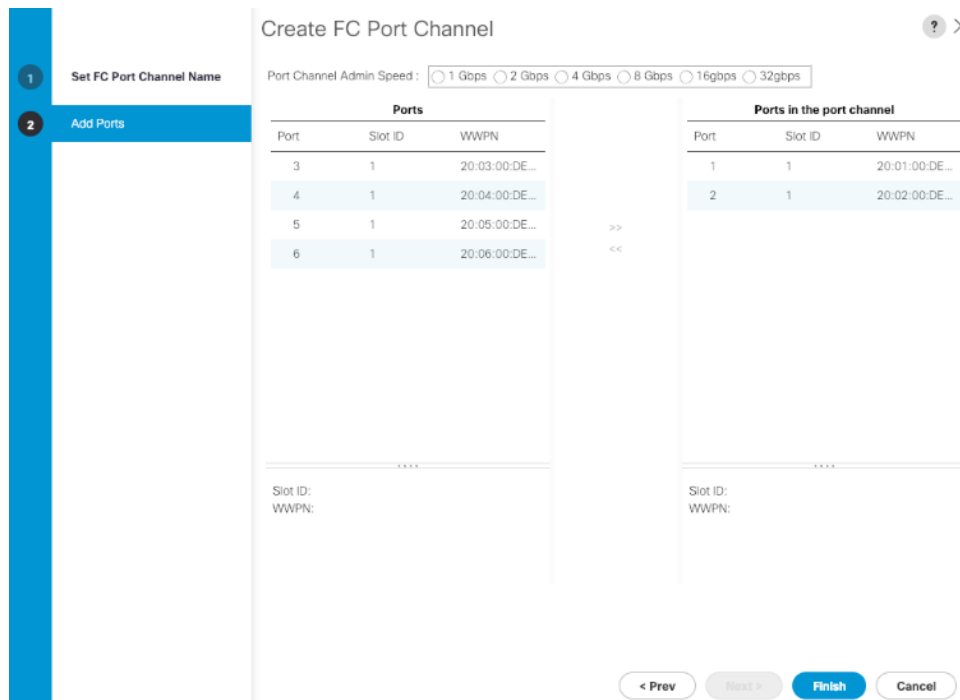
To configure the necessary port channels for the Cisco UCS environment, follow these steps:

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. Click Finish.



7. Click OK.
8. Select FC Port-Channel 6 from the menu in the left pane and from the VSAN drop-down list, keep VSAN 1 selected in the right pane.

SAN / SAN Cloud / Fabric A / FC Port Channels / FC Port-Channel 6 Po6

General Ports Faults Events Statistics

Status

Overall Status : ● **Down**

Additional Info : **No operational members**

Actions

Enable Port Channel

Disable Port Channel

Add Ports

Properties

ID : **6**

Fabric ID : **A**

Port Type : **Aggregation**

Transport Type : **Fc**

Name : Po6

Description :

VSAN : Fabric Dual/vsan defau ▼

Operational Speed(3bps) : Fabric A/vsan Backup-A (201)
Fabric A/vsan vSAN-A (101)
Fabric Dual/vsan default (1)

9. 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.



This 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.

Enable Ethernet Uplink Ports

The Ethernet ports of a Cisco UCS 6332-16UP 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, 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, 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.

Equipment / Fabric Interconnects **Fabric Interconnect A (subordinate)** /

Fabric Interconnects		IO Modules	Thermal	Power	Fans	Installed Firmware	Faults	Events	Performance
+ - Advanced Filter Export Print									
Name		Address	If Role	If Type	Overall Status	Admin State			
Port 19		8C:60:4F:BF:0D:7A	Server	Physical	Sfp Not Present	Enabled			
Port 20		8C:60:4F:BF:0D:7B	Server	Physical	Sfp Not Present	Enabled			
Port 21		8C:60:4F:BF:0D:7C	Server	Physical	Sfp Not Present	Enabled			
Port 22		8C:60:4F:BF:0D:7D	Server	Physical	Sfp Not Present	Enabled			
Port 23		8C:60:4F:BF:0D:7E	Server	Physical	Sfp Not Present	Enabled			
Port 24		8C:60:4F:BF:0D:7F	Server	Physical	Sfp Not Present	Enabled			
Port 25		8C:60:4F:BF:0D:80	Network	Physical	Up	Enabled			
Port 26		8C:60:4F:BF:0D:81	Network	Physical	Up	Enabled			
Port 27		8C:60:4F:BF:0D:82	Unconfigured	Physical	Sfp Not Present	Disabled			
Port 28		8C:60:4F:BF:0D:83	Unconfigured	Physical	Sfp Not Present	Disabled			
Port 29		8C:60:4F:BF:0D:84	Unconfigured	Physical	Sfp Not Present	Disabled			
Port 30		8C:60:4F:BF:0D:85	Unconfigured	Physical	Sfp Not Present	Disabled			
Port 31		8C:60:4F:BF:0D:86	Unconfigured	Physical	Sfp Not Present	Disabled			
Port 32		8C:60:4F:BF:0D:87	Unconfigured	Physical	Sfp Not Present	Disabled			
FC Ports									
Fabric Interconnect B (p...									

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, (11 in our example, to correspond with the upstream Nexus port channel).
5. With 11 selected, enter vPC-11-Nexus for the name of the port channel.

Create Port Channel

1 Set Port Channel Name

2 Add Ports

ID : 11

Name : vPC-11-Nexus

< Prev Next > Finish Cancel

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.

Create Port Channel

1 Set Port Channel Name

2 Add Ports

Ports			
Slot ID	Aggr. Po...	Port	MAC
1	0	35	00:DE:F...
1	0	36	00:DE:F...

>>
<<

Ports in the port channel			
Slot ID	Aggr. Po...	Port	MAC
No data available			

< Prev Next > Finish Cancel

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, (12 in our example, to correspond with the upstream Nexus port channel).
13. With 12 selected, enter vPC-12-Nexus for the name of the port channel.

The screenshot shows the 'Create Port Channel' configuration window. On the left, a blue sidebar contains two steps: '1 Set Port Channel Name' (which is selected and highlighted in blue) and '2 Add Ports'. The main content area has the title 'Create Port Channel' at the top right, followed by a help icon (?) and a close icon (X). Below the title, there are two input fields: 'ID : 12' and 'Name : vPC-12-Nexus'. At the bottom right, there are four buttons: '< Prev' (disabled), 'Next >' (active), 'Finish' (disabled), and 'Cancel' (disabled).

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.

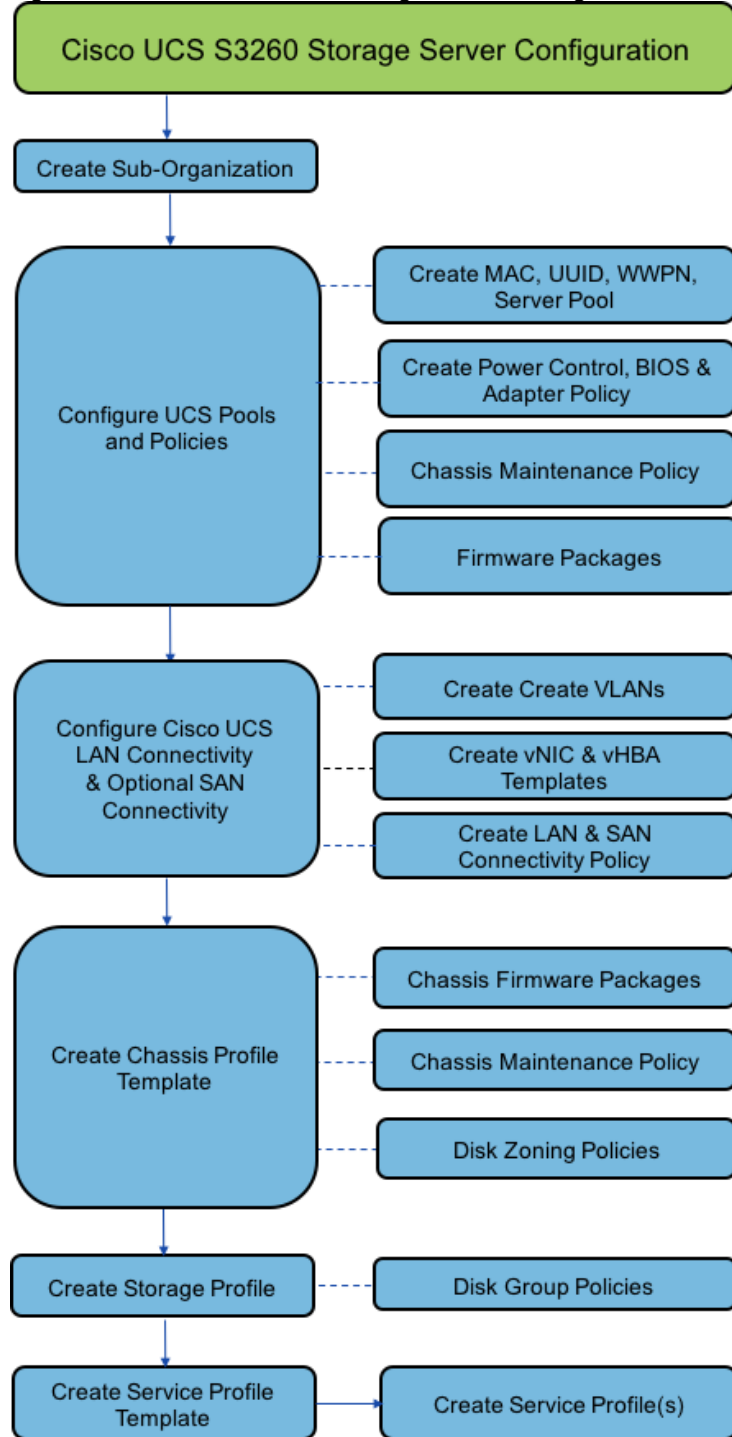
17. Click OK.

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 S3260 Storage Server Configuration

The section explains the Cisco UCS S3260 Storage Server setup. The procedure includes creating ScaleProtect environment specific UCS pools and policies, followed by creating and associating the Cisco UCS S3260 Chassis Profile, and finally the Cisco UCS S3260 Server Node setup that involves creating the Service Profile and association using the Storage Profile.

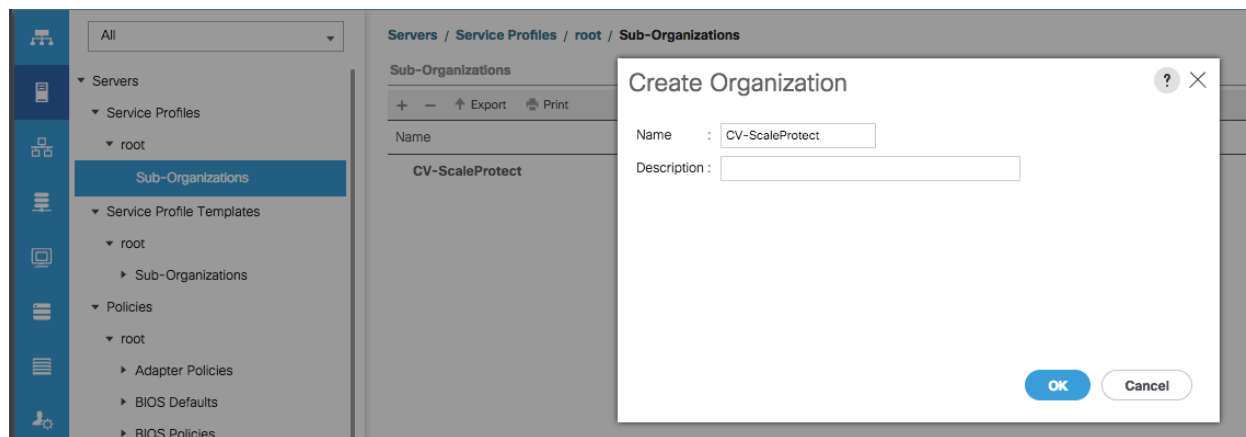
Figure 10 Cisco UCS S3260 Storage Server Configuration



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 facility security 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

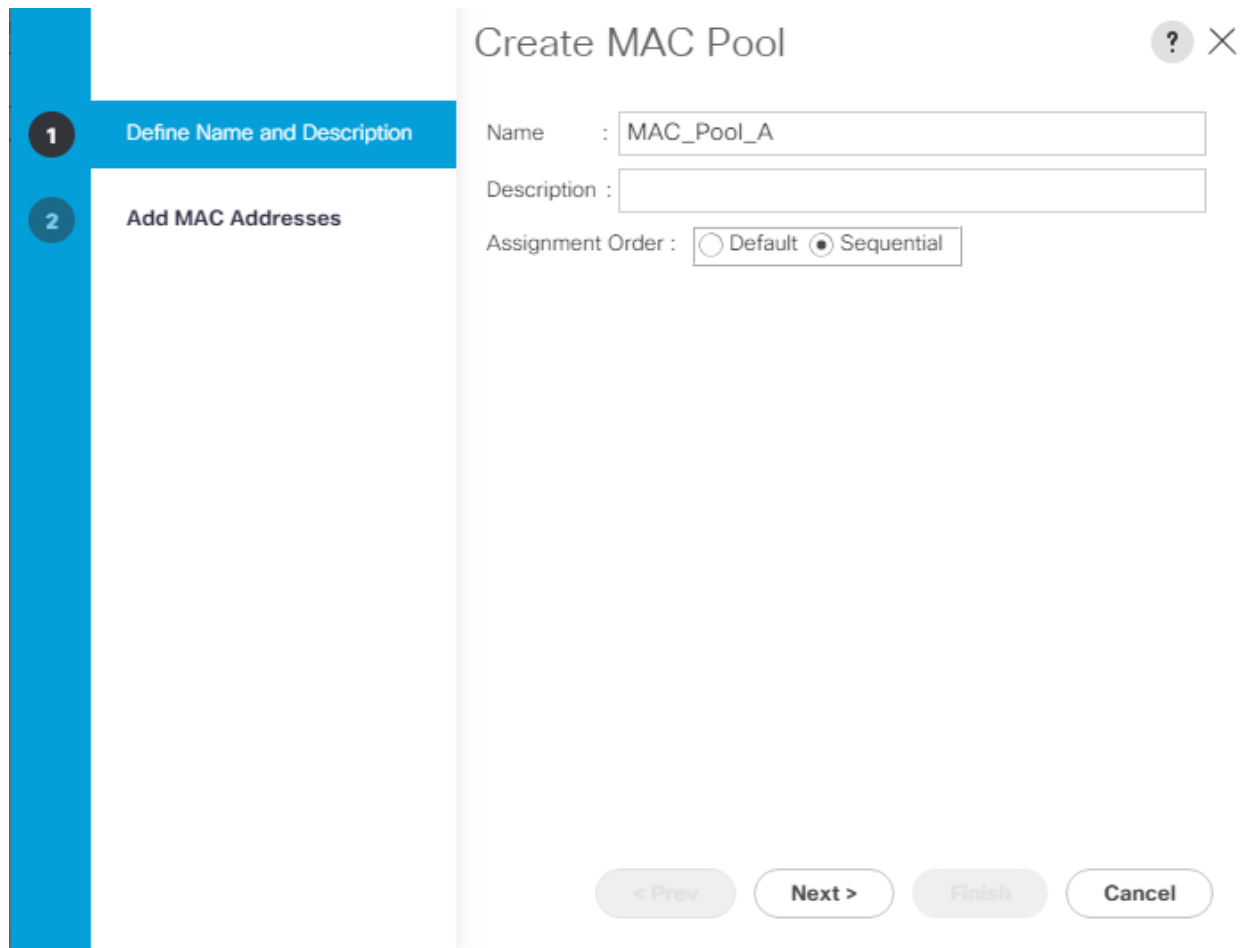
To configure the necessary MAC address pools for the Cisco UCS environment, follow these steps:

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.



1 Define Name and Description

2 Add MAC Addresses

Create MAC Pool

Name : MAC_Pool_A

Description :

Assignment Order : ☐ Default ☒ Sequential

< Prev Next > Finish Cancel

8. Click Next.

9. Click Add.

10. Specify a starting MAC address.



It is recommended to place 0A 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.

Create a Block of MAC Addresses



First MAC Address : Size :

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

00:25:B5:xx:xx:xx

OK

Cancel

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.

1

Define Name and Description

2

Add MAC Addresses

Create MAC Pool

?

×

Name

:

MAC_Pool_B

Description

:

Assignment Order

:

☐ Default

☒ Sequential

< Prev

Next >

Finish

Cancel

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.

?

×

Create a Block of MAC Addresses

First MAC Address :

00:25:B5:06:0B:00

Size :

64

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

00:25:B5:xx:xx:xx

OK

Cancel

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.

Create a Block of UUID Suffixes



From :

Size :

OK

Cancel

13. Click OK.

14. Click Finish.

15. Click OK.

Create Server Pool

The following procedure explains how to create two server pools, one for first server nodes in the chassis and the other of the second server nodes. To configure the necessary server pool for the Cisco UCS environment, follow these steps:



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

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Pools > root.
3. Right-click Server Pools.
4. Select Create Server Pool.
5. Enter `CVLT_SP_Pool_SN1` as the name of the server pool.
6. Optional: Enter a description for the server pool.

1

Set Name and Description

2

Add Servers

Create Server Pool

?

×

Name

:

CVLT_SP_Pool_SN1

Description

:

ScaleProtect Server Pool with Server Nodes #1

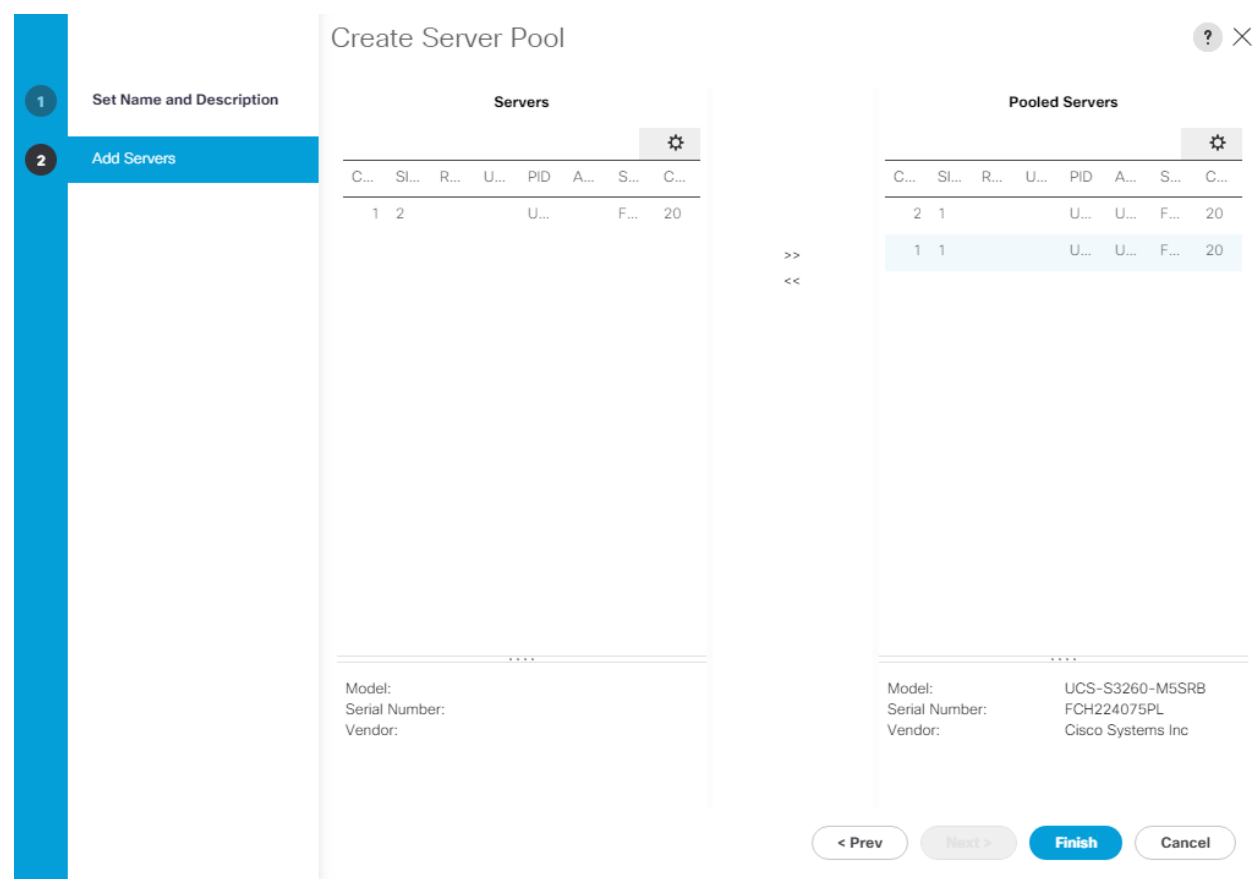
< Prev

Next >

Finish

Cancel

7. Click Next.
8. Select S3260 first server nodes from the two chassis and click >> to add them to the CVLT_SP_Pool1_SN1 server pool.



- 9. Click Finish.
- 10. Click OK.
- 11. Repeat steps 1-10 for second server nodes in the chassis and create a pool named CVLT_SP_Pool_SN2, in this case we have only one server node for a three node ScaleProtect cluster.

1

Set Name and Description

2

Add Servers

Create Server Pool

Servers

C...	SI...	R...	U...	PID	A...	S...	C...
1	1		U...	U...	F...	20	
2	1		U...	U...	F...	20	

Model:
Serial Number:
Vendor:

Pooled Servers

C...	SI...	R...	U...	PID	A...	S...	C...
1	2		U...		F...	20	

Model: UCS-S3260-M5SRB
Serial Number: FCH224075SF
Vendor: Cisco Systems Inc

>>

<<

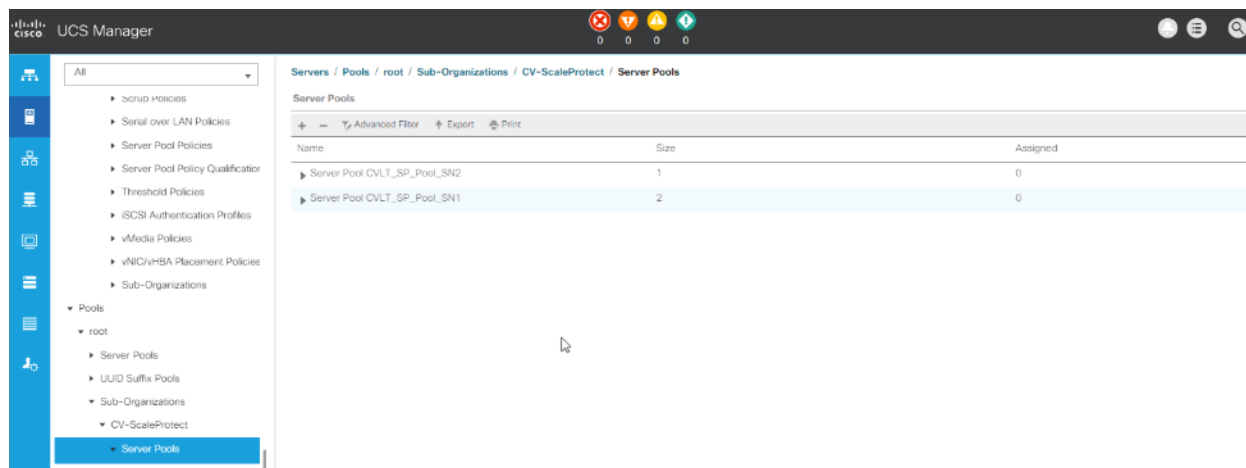
< Prev

Next >

Finish

Cancel

12. Verify that the server pools have been created.



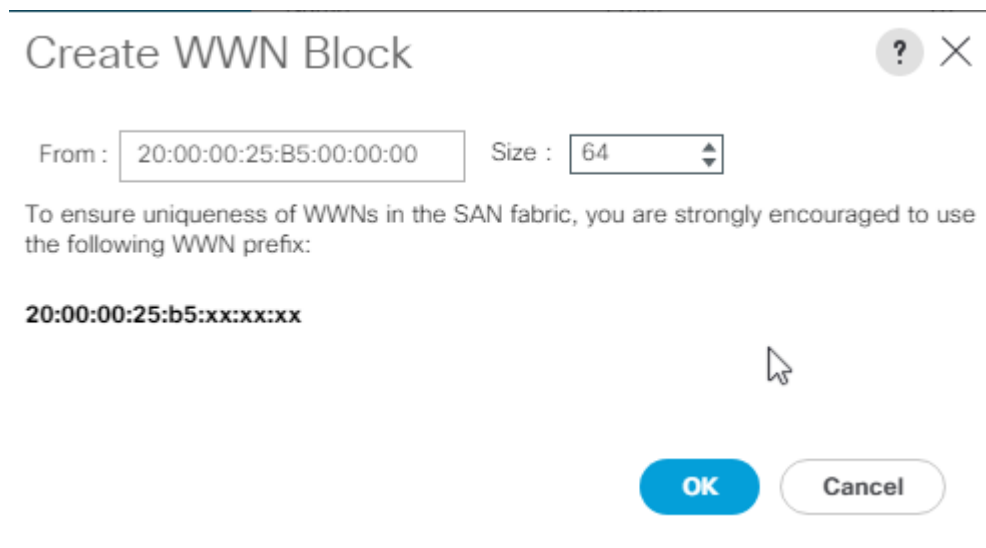
Optional: Create a WWNN Address Pool for FC-based Storage Access



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

To create a World Wide Node Name (WWNN) pool for FC connectivity to SAN fabrics, follow 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.



Create WWN Block

From : Size :

To ensure uniqueness of WWNs in the SAN fabric, you are strongly encouraged to use the following WWN prefix:

20:00:00:25:b5:xx:xx:xx

OK **Cancel**

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.

To create a World Wide Port Name (WWPN) pool for each SAN switching fabric for FC connectivity to SAN fabrics, follow 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.

Create WWPN Pool ? X

1 Define Name and Description

2 Add WWN Blocks

Name : WWPN-Pool-A

Description :

Assignment Order : ☐ Default ☒ Sequential

< Prev Next > Finish Cancel

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.

Create WWN Block



From : Size :

To ensure uniqueness of WWNs in the SAN fabric, you are strongly encouraged to use the following WWN prefix:

20:00:00:25:b5:xx:xx:xx

OK

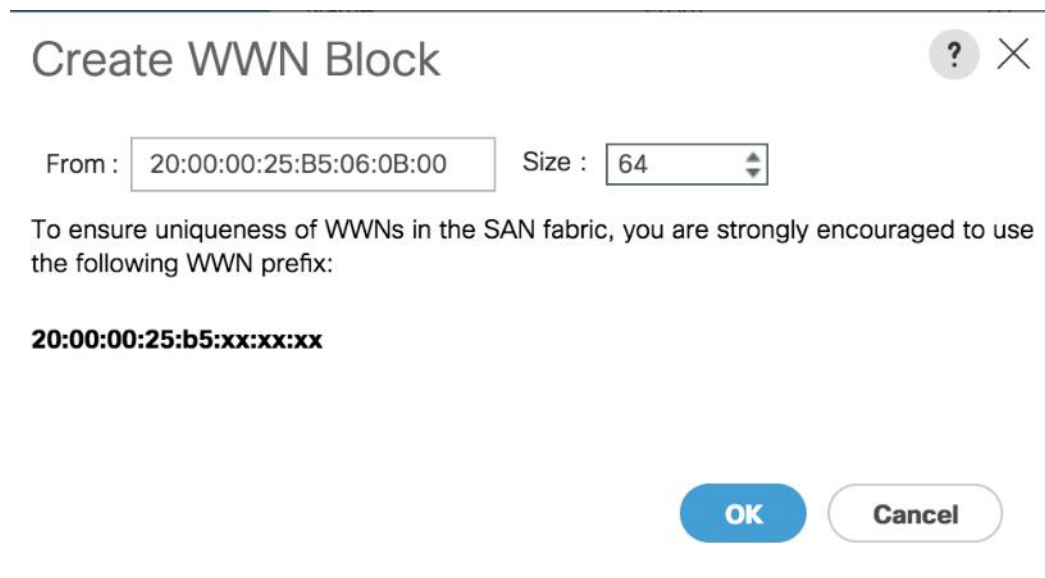
Cancel

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.



The dialog box is titled "Create WWN Block" and has a close button (X) and a help button (?) in the top right corner. It contains two input fields: "From :" with the value "20:00:00:25:B5:06:0B:00" and "Size :" with the value "64". Below these fields, there is a text instruction: "To ensure uniqueness of WWNs in the SAN fabric, you are strongly encouraged to use the following WWN prefix:". Underneath the instruction, the prefix "20:00:00:25:b5:xx:xx:xx" is displayed in bold. At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (white with a grey border).

Create WWN Block

From : 20:00:00:25:B5:06:0B:00 Size : 64

To ensure uniqueness of WWNs in the SAN fabric, you are strongly encouraged to use the following WWN prefix:

20:00:00:25:b5:xx:xx:xx

OK Cancel

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`.

Create VLANs



VLAN Name/Prefix : Data_VLAN

Multicast Policy Name : <not set>

[Create Multicast Policy](#)

☒ Common/Global ☐ Fabric A ☐ Fabric B ☐ Both Fabrics Configured Differently

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

VLAN IDs : 111

Sharing Type : ☒ None ☐ Primary ☐ Isolated ☐ Community

Check Overlap

OK

Cancel

- 8. Click OK and then click OK again.
- 9. Repeat Step 3-8 to add Cluster VLAN as shown in the figure below:

Create VLANs

? X

VLAN Name/Prefix :

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

☒ Common/Global
 ☐ Fabric A
 ☐ Fabric B
 ☐ Both Fabrics Configured Differently

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

VLAN IDs :

Sharing Type : ☒ None ☐ Primary ☐ Isolated ☐ Community

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 (1a) C** for Rack Packages.

Create Host Firmware Package



Name : CV_SP_Firmware

Description :

How would you like to configure the Host Firmware Package?

☒ Simple ☐ Advanced

Blade Package : <not set>

Rack Package : 4.0(1a)C

Service Pack : <not set>

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

Excluded Components:

<input type="checkbox"/>	Adapter
<input type="checkbox"/>	BIOS
<input type="checkbox"/>	Board Controller
<input type="checkbox"/>	CIMC
<input type="checkbox"/>	FC Adapters
<input type="checkbox"/>	Flex Flash Controller
<input type="checkbox"/>	GPUs
<input type="checkbox"/>	HBA Option ROM
<input type="checkbox"/>	Host NIC
<input type="checkbox"/>	Host NIC Option ROM
<input checked="" type="checkbox"/>	Local Disk
<input type="checkbox"/>	NVME Mswitch Firmware
<input type="checkbox"/>	PSU
<input type="checkbox"/>	SAS Expander

OK

Cancel

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.

- Click OK to create the network control policy.

Create Network Control Policy

?
×

Name : ScaleProtect_NCP

Description :

CDP : ☐ Disabled ☒ Enabled

MAC Register Mode : ☒ Only Native Vlan ☐ All Host Vlans

Action on Uplink Fail : ☒ Link Down ☐ Warning

MAC Security

Forge : ☒ Allow ☐ Deny

LLDP

OK

Cancel

- Click OK.

Create Power Control Policy

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

- In Cisco UCS Manager, click the Servers tab in the navigation pane. Select Policies > root >Sub-Organizations > CV-ScaleProtect.
- Right-click Power Control Policies.
- Select Create Power Control Policy.
- Enter **No-Power-Cap** as the power control policy name.
- Change the power capping setting to **No Cap**.
- Click OK to create the power control policy.

Create Power Control Policy



Name :

Description :

Fan Speed Policy :

Power Capping

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

☒ No Cap ☐ cap

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

OK

Cancel

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-S3260-BIOS** as the BIOS policy name.

Create BIOS Policy



Name : SP-S3260-BIOS

Description :

Reboot on BIOS Settings Change : ☐



Cancel

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**.

The screenshot shows the Cisco UCS Manager interface. On the left is a navigation pane with a tree view containing various policy categories like Server Pool Policies, Threshold Policies, and BIOS Policies. The 'BIOS Policies' section is expanded, and 'SP-S3260-BIOS' is selected. The main panel displays the configuration for this policy. It includes tabs for Main, Advanced, Boot Options, Server Management, and Events. The 'Main' tab is active, showing the 'Properties' section with fields for Name (SP-S3260-BIOS), Description, Owner (Local), and a checkbox for 'Reboot on BIOS Settings Change'. Below this is a table of BIOS settings.

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

10. Click Advanced tab and then select Processor.
11. On the Processor screen, make changes as captured in the following figure.

Servers / Policies / root / Sub-Organizations / CV-ScaleProtect / BIOS Policies / SP-S3260-BIOS

Main Advanced Boot Options Server Management Events

Processor Intel Directed IO RAS Memory Serial Port USB PCI QPI LOM and PCIe Slots Trusted Platform Graphics Configuration

Advanced Filter Export Print

BIOS Setting	Value
Local X2 Apic	Platform Default
Max Variable MTRR Setting	Platform Default
P STATE Coordination	Platform Default
Package C State Limit	C0 C1 State
Autonomous Core C-state	Disabled
Processor C State	Disabled
Processor C1E	Disabled
Processor C3 Report	Disabled
Processor C6 Report	Disabled
Processor C7 Report	Disabled
Processor CMCi	Platform Default
Power Technology	Custom
Energy Performance	Platform Default
ProcessorEppProfile	Platform Default
Adjacent Cache Line Prefetcher	Platform Default
DCU IP Prefetcher	Platform Default

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

SMT Mode	Platform Default
SVM Mode	Platform Default
Demand Scrub	Platform Default
Patrol Scrub	Platform Default
Workload Configuration	IO Sensitive

Add Delete Info

Save Changes Reset Values

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_Po1** 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 Maintenance Policy

Name

:

UserAck_Pol

Description

:

Soft Shutdown Timer

:

150 Secs

Storage Config. Deployment Policy

:

☐ Immediate
 ☒ User Ack

Reboot Policy

:

☐ Immediate
 ☒ User Ack
 ☐ Timer Automatic

☐ On Next Boot

(Apply pending changes at next reboot.)

OK

Cancel

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.

?

×

Create Ethernet Adapter Policy

Name : ScaleP_Adap_Pol

Description :

⊖ Resources

Pooled : ☒ Disabled ☐ Enabled

Transmit Queues : 8 [1-1000]

Ring Size : 4096 [64-4096]

Receive Queues : 8 [1-1000]

Ring Size : 4096 [64-4096]

Completion Queues : 16 [1-2000]

Interrupts : 32 [1-1024]

⊖ Options

Transmit Checksum Offload : ☐ Disabled ☒ Enabled

Receive Checksum Offload : ☐ Disabled ☒ Enabled

TCP Segmentation Offload : ☐ Disabled ☒ Enabled

TCP Large Receive Offload : ☐ Disabled ☒ Enabled

Receive Side Scaling (RSS) : ☐ Disabled ☒ Enabled

Accelerated Receive Flow Steering : ☒ Disabled ☐ Enabled

OK

Cancel



To enable maximum throughput, 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

A total of 2 vNIC Templates are 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.

To create multiple vNIC templates for the Cisco UCS environment, follow these steps:

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.

Create vNIC Template

?

×

Name

:

vNIC_SP_Data

Description

:

Fabric ID

:

☒ Fabric A

☐ Fabric B

☒ Enable Failover

Redundancy

Redundancy Type

:

☒ No Redundancy

☐ Primary Template

☐ Secondary Template

Target

☒ Adapter

☐ VM

Warning

If **VM** is selected, a port profile by the same name will be created.

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

Template Type

:

☐ Initial Template

☒ Updating Template

VLANs

VLAN Groups

Advanced Filter

Export

Print

⚙

Select	Name	Native VLAN
<input type="checkbox"/>	Cluster_VLAN	<input type="radio"/>
<input checked="" type="checkbox"/>	Data_VLAN	<input checked="" type="radio"/>
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	Native VLAN	<input type="radio"/>

OK

Cancel

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.

Create vNIC Template



Select	Name	Native VLAN
<input type="checkbox"/>	Cluster_VLAN	<input type="radio"/>
<input checked="" type="checkbox"/>	Data_VLAN	<input checked="" type="radio"/>
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>

Create VLAN

CDN Source : ☒ vNIC Name ☐ User Defined

MTU : 1500

MAC Pool : MAC_Pool_A(64/64) ▼

QoS Policy : <not set> ▼

Network Control Policy : ScaleProtect_NCP ▼

Pin Group : <not set> ▼

Stats Threshold Policy : default ▼

Connection Policies

☒ Dynamic vNIC ☐ usNIC ☐ VMQ

Dynamic vNIC Connection Policy : <not set> ▼

OK

Cancel

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.

To create the Cluster VLAN template, follow these steps:

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

4. Select Create vNIC Template
5. Enter `vNIC_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.

Create vNIC Template

?

×

Name

:

vNIC_SP_Cluster

Description

:

Fabric ID

:

Fabric A

Fabric B

Enable Failover

Redundancy

Redundancy Type

:

No Redundancy

Primary Template

Secondary Template

Target

Adapter

VM

Warning

If **VM** is selected, a port profile by the same name will be created.

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

Template Type

:

Initial Template

Updating Template

VLANs

VLAN Groups

Advanced Filter

Export

Print

⚙

Select	Name	Native VLAN
<input checked="" type="checkbox"/>	Cluster_VLAN	<input checked="" type="radio"/>
<input type="checkbox"/>	Data_VLAN	<input type="radio"/>
<input type="checkbox"/>	default	<input type="radio"/>
<input type="checkbox"/>	Native_VLAN	<input type="radio"/>

OK

Cancel

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.

77

Create vNIC Template



Advanced Filter Export Print			
Select	Name	Native VLAN	
<input checked="" type="checkbox"/>	Cluster_VLAN	<input checked="" type="radio"/>	
<input type="checkbox"/>	Data_VLAN	<input type="radio"/>	
<input type="checkbox"/>	default	<input type="radio"/>	
<input type="checkbox"/>	Native-VLAN	<input type="radio"/>	

Create VLAN

CDN Source : ☒ vNIC Name ☐ User Defined

MTU : 9000

MAC Pool : MAC_Pool_B(64/64) ▼

QoS Policy : <not set> ▼

Network Control Policy : ScaleProtect_NCP ▼

Pin Group : <not set> ▼

Stats Threshold Policy : default ▼

Connection Policies

☒ Dynamic vNIC ☐ usNIC ☐ VMQ

Dynamic vNIC Connection Policy : <not set> ▼

OK

Cancel

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.

Create LAN Connectivity Policy ? ×

Name : CVLT_SP_LAN

Description : Commvault ScaleProtect LAN Connectivity Policy

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

Name	MAC Address	Native VLAN
No data available		

Delete

Add


Modify

+ Add iSCSI vNICs

OK

Cancel

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_Po1.
11. Click OK to add this vNIC to the policy.

Create vNIC

Name :

Use vNIC Template : ☒

Redundancy Pair : ☐

Peer Name :

vNIC Template :

Adapter Policy :

OK Cancel

12. Click the upper Add button 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**.

Create vNIC

Name : vNIC_Clus_eth1

Use vNIC Template : ☒

Redundancy Pair : ☐

vNIC Template : vNIC_SP_Cluster

Peer Name :

Create vNIC Template

Adapter Performance Profile

Adapter Policy : ScaleP_Adap_Pol

Create Ethernet Adapter Policy

OK

Cancel

17. Click OK to add the vNIC to the policy.
18. Click OK, then click OK again to create the LAN Connectivity Policy.

Create LAN Connectivity Policy



Name : CVLT_SP_LAN

Description : Commvault ScaleProtect LAN Connectivity Policy

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

Name	MAC Address	Native VLAN
vNIC vNIC_Clus_eth1	Derived	
vNIC vNIC_Data_eth0	Derived	

Delete Add Modify

Add iSCSI vNICs

OK

Cancel

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**.

Create vHBA Template



Name	:	<input type="text" value="Infra-vHBA-A"/>
Description	:	<input type="text"/>
Fabric ID	:	<input checked="" type="radio"/> A <input type="radio"/> B
Redundancy		
Redundancy Type	:	<input checked="" type="radio"/> No Redundancy <input type="radio"/> Primary Template <input type="radio"/> Secondary Template
Select VSAN	:	<input type="text" value="vSAN-A"/> Create VSAN
Template Type	:	<input type="radio"/> Initial Template <input checked="" type="radio"/> Updating Template
Max Data Field Size	:	<input type="text" value="2048"/>
WWPN Pool	:	<input type="text" value="WWPN-Pool-A(64/64)"/> ▼
QoS Policy	:	<input type="text" value="<not set>"/> ▼
Pin Group	:	<input type="text" value="<not set>"/> ▼
Stats Threshold Policy	:	<input type="text" value="default"/> ▼



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**.

Create vHBA Template



Name : Infra-vHBA-B

Description :

Fabric ID : ☐ A ☒ B

Redundancy

Redundancy Type : ☒ No Redundancy ☐ Primary Template ☐ Secondary Template

Select VSAN : vSAN-B [Create VSAN](#)

Template Type : ☐ Initial Template ☒ Updating Template

Max Data Field Size : 2048

WWPN Pool : WWPN-Pool-B(64/64) ▼

QoS Policy : <not set> ▼

Pin Group : <not set> ▼

Stats Threshold Policy : default ▼

OK **Cancel**

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**.

Create vHBA Template



Name : Backup-vHBA-A

Description :

Fabric ID : ☒ A ☐ B

Redundancy

Redundancy Type : ☒ No Redundancy ☐ Primary Template ☐ Secondary Template

Select VSAN : Backup-A [Create VSAN](#)

Template Type : ☐ Initial Template ☒ Updating Template

Max Data Field Size : 2048

WWPN Pool : WWPN-Pool-A(64/64)

QoS Policy : <not set>

Pin Group : <not set>

Stats Threshold Policy : default

OK **Cancel**

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**.

Create vHBA Template



Name : Backup-vHBA-B

Description :

Fabric ID : ☐ A ☒ B

Redundancy

Redundancy Type : ☒ No Redundancy ☐ Primary Template ☐ Secondary Template

Select VSAN : Backup-B [Create VSAN](#)

Template Type : ☒ Initial Template ☐ Updating Template

Max Data Field Size : 2048

WWPN Pool : WWPN-Pool-B(58/64)

QoS Policy : <not set>

Pin Group : <not set>

Stats Threshold Policy : default

OK

Cancel

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 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.

Create SAN Connectivity Policy



Name : CVLT_SP_SAN

Description : Commvault ScaleProtect SAN Connectivity Policy

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

World Wide Node Name

WWNN Assignment:

WWNN-Pool(64/64) ▼

[Create WWNN Pool](#)

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

Name	WWPN
No data available	

Delete
 Add
 Modify

OK

Cancel

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**.

Create vHBA



Name :

Use vHBA Template : ☒

Redundancy Pair : ☐

Peer Name :

vHBA Template :

[Create vHBA Template](#)

Adapter Performance Profile

Adapter Policy :

[Create Fibre Channel Adapter Policy](#)

OK

Cancel

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**.

Create vHBA

?

×

Name

:

vHBA2

Use vHBA Template

:

☒

Redundancy Pair

:

☐

vHBA Template

:

Infra-vHBA-B

▼

Peer Name

:

Create vHBA Template

Adapter Performance Profile

Adapter Policy

:

Linux

▼

Create Fibre Channel Adapter Policy

OK

Cancel

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.

89

Create vHBA

?

×

Name : vHBA3

Use vHBA Template : ☒

Redundancy Pair : ☐

Peer Name :

vHBA Template : Backup-vHBA-A

Create vHBA Template

Adapter Performance Profile

Adapter Policy : Linux

Create Fibre Channel Adapter Policy

OK

Cancel

- 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.

Create SAN Connectivity Policy



Name : CVLT_SP_SAN

Description : Commvault ScaleProtect SAN Connectivity Policy

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

World Wide Node Name

WWNN Assignment:

WWNN-Pool(64/64)

[Create WWNN Pool](#)

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

Name	WWPN
▶ vHBA vHBA4	Derived
▶ vHBA vHBA3	Derived
▶ vHBA vHBA2	Derived
▶ vHBA vHBA1	Derived

🗑 Delete ➕ Add ⓘ Modify

OK

Cancel

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

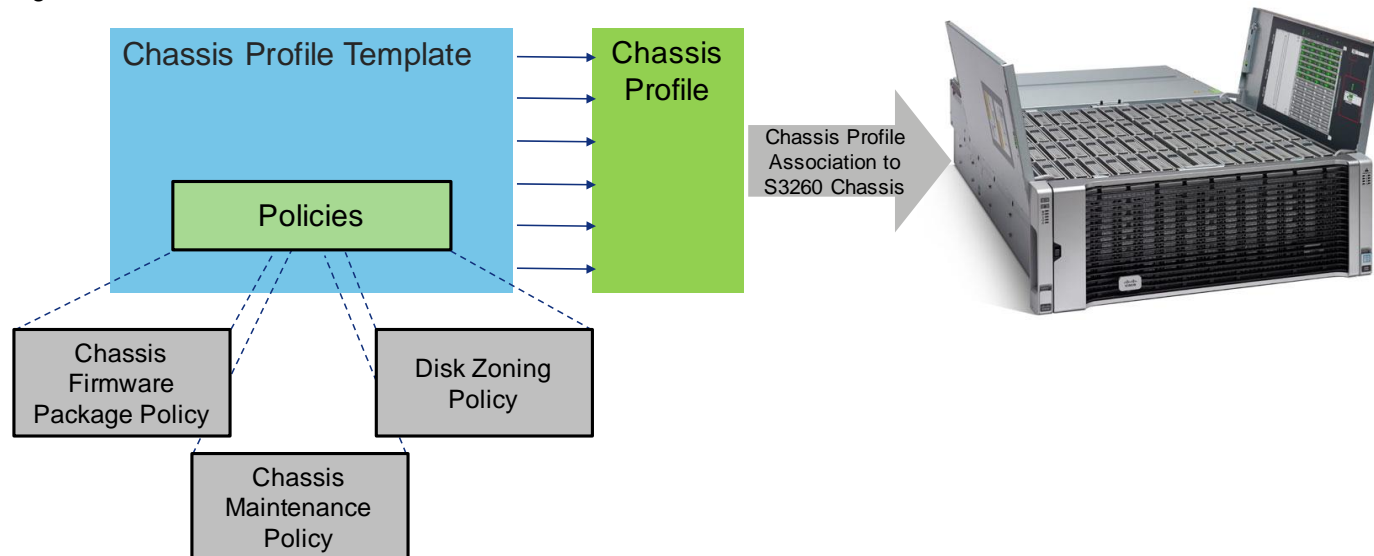
Cisco UCS S3260 Chassis Setup

This section explains the Cisco UCS S3260 Chassis setup for ScaleProtect infrastructure.

Chassis Profile Template

A chassis profile defines the storage, firmware, and maintenance characteristics of a chassis. You can create a chassis profile for the Cisco UCS S3260 chassis. When a chassis profile is associated to a chassis, Cisco UCS Manager automatically configures the chassis to match the configuration specified in the chassis profile.

Figure 11 Cisco UCS S3260 Chassis Profile Association



A chassis profile includes the following information:

- Chassis definition—Defines the specific chassis to which the profile is assigned.
- Maintenance policy—Includes the maintenance policy to be applied to the profile.
- Firmware specifications—Defines the chassis firmware package that can be applied to a chassis through this profile.
- Disk zoning policy—Includes the zoning policy to be applied to the storage disks.
- Compute Connection policy – Defines the data path between the primary, auxiliary SIOC, and server.

Create Chassis Firmware Packages

The Chassis Firmware Package applies the appropriate firmware package to the chassis. To create a Chassis Firmware Package, follow these steps:

1. In the Navigation pane, click the Chassis tab.
2. In the Chassis tab, expand Policies > root > sub-Organizations > CV-ScaleProtect.
3. Right-click Chassis Firmware Packages and select Create Chassis Firmware Packages.
4. Enter `s3260_FW_Package` as the Package name.
5. Select `4.0 (1a) C` from the Chassis Package drop-down list.
6. Click OK.

Create Chassis Firmware Package



Name : S3260_firmware

Description : Chassis Firmware Policy

Chassis Package : 4.0(1a)C

Service Pack : <not set>

The images from Service Pack will take precedence over the images from Chassis Package

Excluded Components:

- ☐ Chassis Adaptor
- ☐ Chassis Board Controller
- ☐ Chassis Management Controller
- ☒ Local Disk
- ☐ SAS Expander

OK

Cancel



The Local disk is excluded by default in Chassis 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 maintenance Policy

The available policy is the Default Chassis Maintenance Policy and it is set for User Ack for Reboot.

Create Disk Zoning Policy

The Disk Zoning Policy allocates disk slots between server nodes in the chassis. To create the S3260 Disk Zoning Policy, follow these steps:



The following steps use the Dual-chip RAID controller (**UCS-S3260-DRAID**) based on LSI 3316 ROC with 4-GB RAID cache per chip. Please allocate all drive slots designated for both servers to Controller 1 if the servers have older raid controllers with a single chip.

1. In the Navigation pane, click Chassis.
2. Expand Policies > root > Sub-Organizations > CV-ScaleProtect.

3. Right-click Disk Zoning Policies and choose Create Disk Zoning Policy.

Create Disk Zoning Policy ? ×

Name :

Description :

Preserve Config : ☐

Disk Zoning Information

+

−

Advanced Filter

↑ Export

Print

⚙

Name	Slot Number	Ownership	Assigned to S...	Assigned to C...	Controller Type	Drive Path
No data available						

+

 Add

🗑

 Delete

⚙

 Modify

OK

Cancel

4. Enter `s3260_DiskZone` as the Disk Zone Name.
5. In the Disk Zoning Information Area, click Add.
6. Select Ownership as Dedicated.
7. Select 1 for the Server (disks get assigned to node 1 of the S3260 Storage server).
8. Select 1 for the Controller.
9. Slot range as 49–52.

Add Slots to Policy



Ownership : ☐ Unassigned ☒ Dedicated ☐ Shared ☐ Chassis Global Hot Spare

Server :

Controller :

Controller Type : **SAS**

Drive Path : ☒ Path Both ☐ Path 0 ☐ Path 1

Slot Range :

OK**Cancel**

10. Click OK.
11. In the Disk Zoning Information Area, click Add.
12. Select Ownership as Dedicated.
13. Select 1 for the Server.
14. Select 2 for the Controller.
15. Slot range as 1–24.
16. Select 2 for the Server (disks get assigned to node 2 of the S3260 Storage server).
17. Select 1 for the Controller.
18. Slot range as 53–56.

Add Slots to Policy



Ownership : ☐ Unassigned ☒ Dedicated ☐ Shared ☐ Chassis Global Hot Spare

Server :

Controller :

Controller Type : **SAS**

Drive Path : ☒ Path Both ☐ Path 0 ☐ Path 1

Slot Range :

OK**Cancel**

-
19. Click OK.
 20. In the Disk Zoning Information Area, click Add.
 21. Select Ownership as Dedicated.
 22. Select Server as 2
 23. Select Controller as 2.
 24. Slot range as 25-48.

Add Slots to Policy?×

Ownership : ☐ Unassigned ☒ Dedicated ☐ Shared ☐ Chassis Global Hot Spare

Server :

2

Controller :

2

Controller Type : **SAS**

Drive Path : ☒ Path Both ☐ Path 0 ☐ Path 1

Slot Range :

25-48

OKCancel

25. Click OK.
26. Click OK again to complete the Disk Zoning Policy creation

Properties for: S3260_DiskZone×

GeneralEvents

Actions

Add Slots to PolicyDeleteShow Policy UsageUse Global

Properties

Name : S3260_DiskZone

Description : Disk Zoning Policy

Preserve Config : ☐

Disks Zoned

+ - Advanced Filter Export Print

Name	Slot Number	Ownership	Assigned to Se...	Assigned to Co...	Controller Type	Drive Path
▶ disk-slot-1	1	Dedicated				Path Both
▶ disk-slot-2	2	Dedicated				Path Both
▶ disk-slot-3	3	Dedicated				Path Both
▶ disk-slot-4	4	Dedicated				Path Both
▶ disk-slot-5	5	Dedicated				Path Both
▶ disk-slot-6	6	Dedicated				Path Both

+

 Add

⌫

 Delete

⚙

 Modify

OKApplyCancelHelp

98

Create Chassis Profile Template

With the Policies used by the Chassis Profile in place, to create Chassis Profile Template for Cisco UCS S3260 storage server, follow these steps:

1. In Cisco UCS Manager, click the Chassis tab in the navigation pane.
2. Select Chassis Profile Templates > root > Sub-Organizations > CV-ScaleProtect.
3. Right-click and select Create Chassis Profile Template.
4. Enter name as `CVLT_SP_Chassis`.
5. Select Type as `Updating Template`.

Create Chassis Profile Template

You must enter a name for the chassis profile template and specify the template type. You can also enter a description of the template.

Name :

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

Where : **org-root**

Type : ☐ Initial Template ☒ Updating Template

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

< Back Next > **Finish** Cancel

6. Select `default` as the Maintenance Policy and click Next.
7. Select Chassis Firmware Package as `s3260_firmware`.

1

Identify Chassis Profile Template

2

Chassis Maintenance Policy

3

Policies

4

Disk Zoning Policy

Create Chassis Profile Template

Optionally configure chassis firmware package for this chassis profile template.

⊖

Chassis Firmware Package

If you select a chassis firmware policy for this chassis profile template, the template will update the firmware on the chassis that it is associated with.
Otherwise the system uses the firmware already installed on the associated chassis.

Chassis Firmware Package :

S3260_firmware

Create Chassis Firmware Package

⊕

Compute Connection Policy

⊕

Sas Expander Configuration Policy

< Prev

Next >

Finish

Cancel

8. Select Disk Zoning Policy as S3260_DiskZone and click Finish.

1

Identify Chassis Profile Template

2

Chassis Maintenance Policy

3

Policies

4

Disk Zoning Policy

Create Chassis Profile Template

Optionally specify information that affects how the system operates.
Disk Zoning policies are applicable only to UCSC-C3X60-BASE chassis

Disk Zoning Policy:

S3260_DiskZone

Create Disk Zoning Policy

Name : S3260_DiskZone

Description : Disk Zoning Policy

Preserve Config : No

Disks Zoned

⊕

⊖

Advanced Filter

Export

Print

⚙

Name	Slot Number	Ownership	Assigned to S...	Assigned to ...	Controller Type	Drive Path
▶ disk-slot-1	1	Dedicated				Path Both
▶ disk-slot-10	10	Dedicated				Path Both
▶ disk-slot-11	11	Dedicated				Path Both
▶ disk-slot-12	12	Dedicated				Path Both
▶ disk-slot-13	13	Dedicated				Path Both
▶ disk-slot-14	14	Dedicated				Path Both

< Prev

Next >

Finish

Cancel

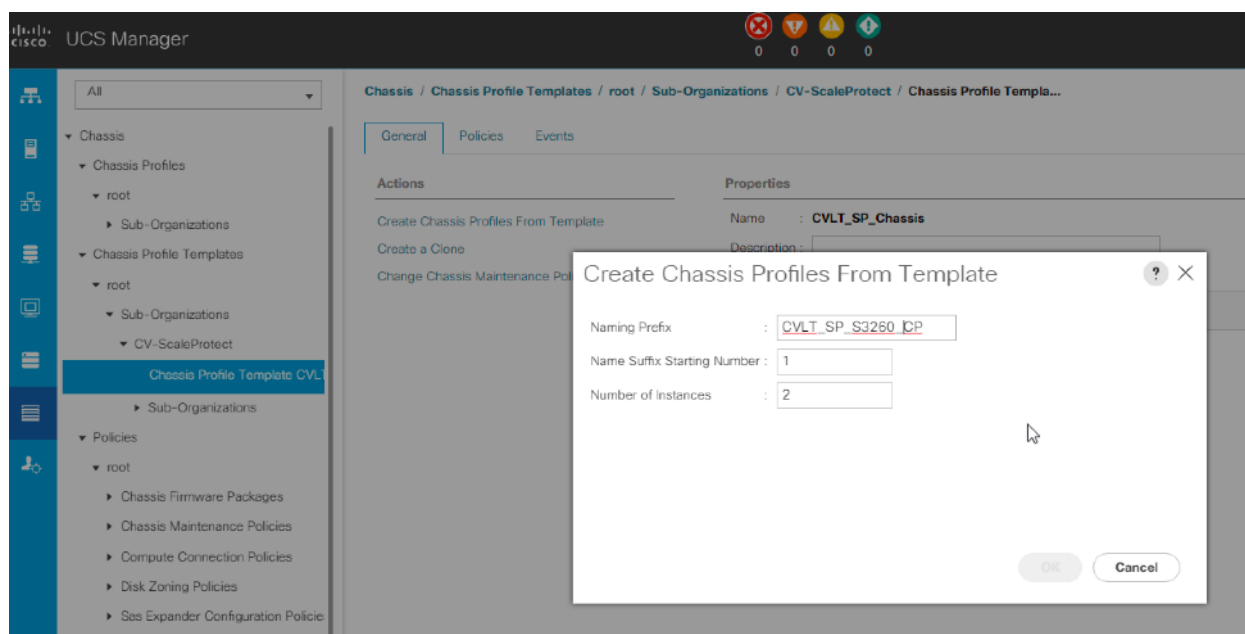
100

Create Chassis Profile(s) from Template

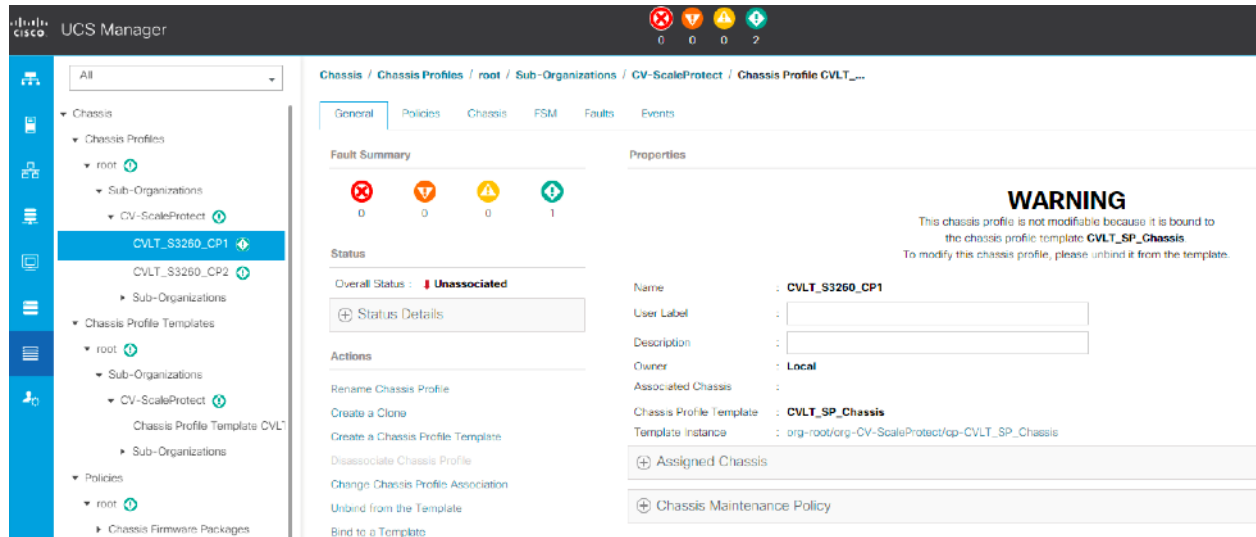
The Chassis Profile Template has been created with policies appropriate for both S3260 Storage Servers used in the environment, so as a result there will be two Chassis Profiles created in this section.

To create chassis profile from the chassis profile template, follow these steps:

1. Click the Chassis tab in the navigation pane.
2. Select Chassis Profile Templates > root > Sub-Organizations > CV-ScaleProtect.
3. Right-click CV-ScaleProtect and Select Create Chassis Profiles from Template.
4. Enter CVLT_SP_S3260_CP as the Chassis profile prefix.
5. Enter 1 as Name Suffix Starting Number and 2 as Number of Instances.



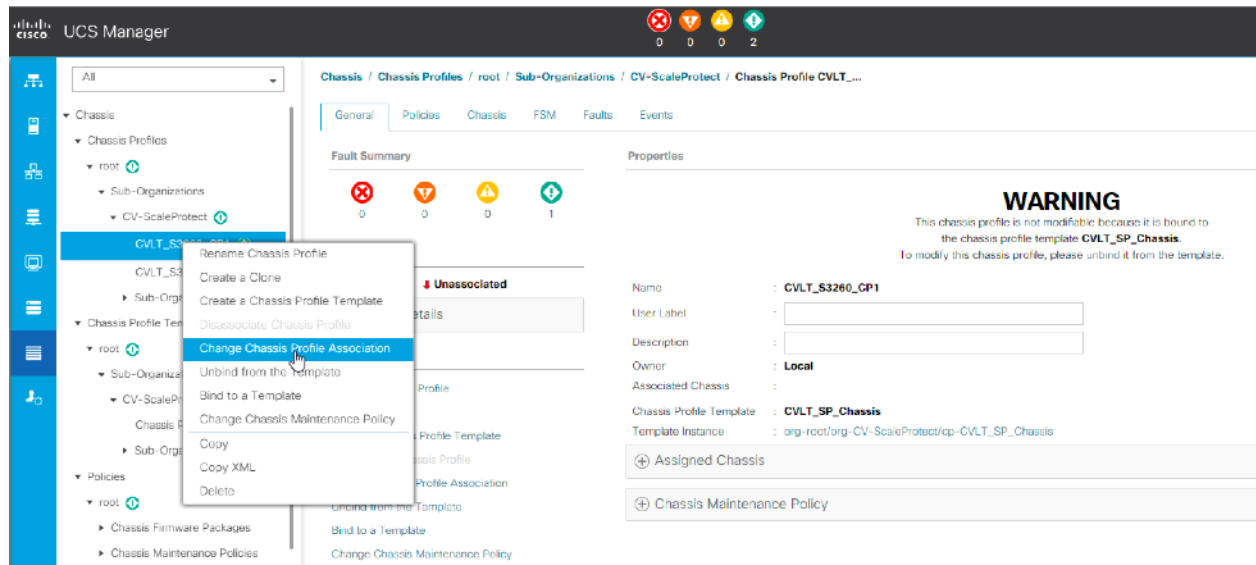
6. The screenshot below displays created chassis profiles under Chassis > root > Sub_organizations > CV-ScaleProtect.



Associate Chassis Profile to S3260 Chassis

To Associate Chassis Profile to S3260 Chassis, follow these steps:

1. Click the Chassis tab in the navigation pane.
2. Select Chassis Profiles > root > Sub-Organizations > CV-ScaleProtect.
3. Right-click CVLT_S3260_CP1 and select Change Chassis Profile Association.



4. In the Assignment tab, Select Existing Chassis.
5. Select the Available Chassis and select ID 1.

Associate Chassis Profile

?

×

Select a previously-discovered chassis by name, or manually specify a custom chassis by entering its chassis ID. If no chassis currently exists at that location, the system waits until one is discovered.

You can select an existing chassis you want to associate with this chassis profile.

Chassis Assignment:

Select existing Chassis

▼

☒ Available Chassis

☐ All Chassis

Select	ID
<input checked="" type="radio"/>	1
<input type="radio"/>	2

Restrict Migration

:

☐

OK

Cancel

6. Click OK.
7. Since we have selected User Ack for the Maintenance Policy, acknowledge Chassis Reboot for Chassis Profile Association.

Associate Chassis Profile

×

⚠

Your changes:

Create: **chassis** (*org-root/org-CV-ScaleProtect/cp-CVLT_S3260_CP1/chassis*)

Will require User Acknowledgement before the Reboot of:

Chassis Profile CVLT_S3260_CP1 (*org-root/org-CV-ScaleProtect/cp-CVLT_S3260_CP1*) [Chassis: **sys/chassis-1**]

Are you sure you want to apply the changes?

Press **Yes** to disregard the warning and submit changes, **No** to quit the wizard or **Cancel** to make changes to the current configuration.

Yes

No

Cancel

8. On FSM Tab you will see the Association Status.

103

GeneralPoliciesChassisFSMFaultsEvents

ChassisChassis Profile

FSM Status : In Progress

Description :

Current FSM Name : Associate

Completed at :

Progress Status :

86%

Remote Invocation Result :

Remote Invocation Error Code : None

Remote Invocation Description :

Step Sequence

Order	Name	Description	Status	Timestamp	Retried
1	Associate Download...	Download images(F...	Skipped	2017-01-10T19:33:22	0

9. Repeat steps 1-8 to associate second Chassis with the Chassis Profile cvLT_s3260_CP2.

Associate Chassis Profile

Select a previously-discovered chassis by name, or manually specify a custom chassis by entering its chassis ID. If no chassis currently exists at that location, the system waits until one is discovered.

You can select an existing chassis you want to associate with this chassis profile.

Chassis Assignment:

Select existing Chassis

☒ Available Chassis

☐ All Chassis

Select	ID
<input checked="" type="radio"/>	2

Restrict Migration : ☐

OK

Cancel

10. Once the Chassis profile association is complete, we will see the assigned status as **Assigned**.



Cisco UCS S3260 Server Node Setup

The server nodes will be configured using Service Profiles like other Cisco UCS Manager managed server resources but will require a Storage Profile to use disks made available to them by disk slots designated for the server in the Disk Zoning Policy of Chassis Profile associated to the Chassis.

LUN Cleanup

For any S3260 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:

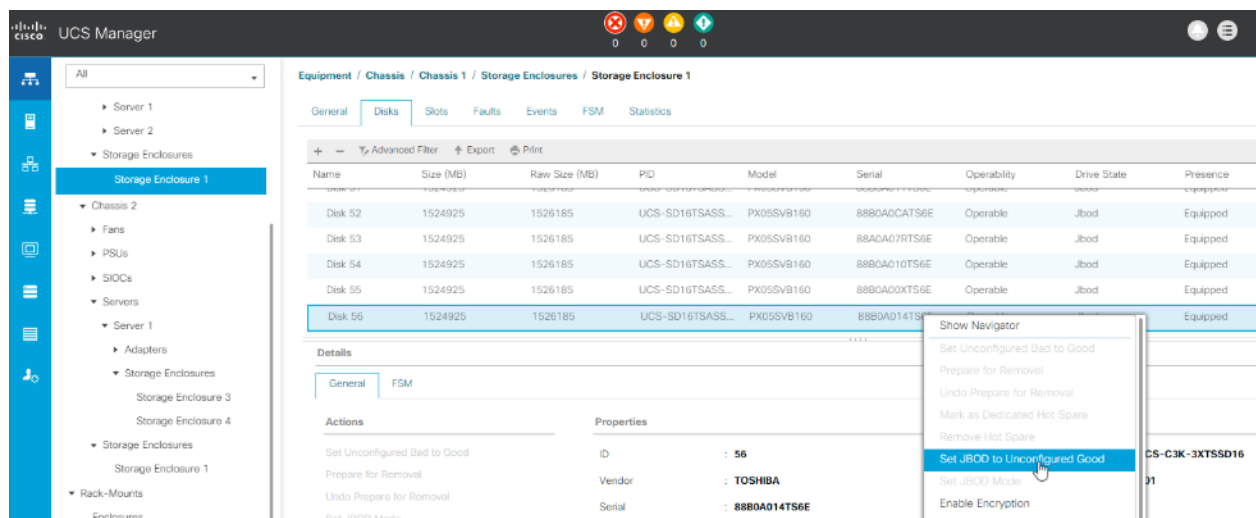
1. In Cisco UCS Manager, click Equipment within the Navigation Pane and select Chassis from within the Equipment drop-down options. Select the Chassis of the S3260 and click the server node within that chassis to clear LUNs from.
2. Within that server node, click the Inventory tab, then the Storage tab 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 OK to continue.

Set Cisco UCS S3260 Disk to Unconfigured Good

After the Cisco UCS S3260 server nodes have had disks allocated to them through the Chassis Profile Association, new Cisco UCS S3260s, as well as when newly inserted disks into an Cisco UCS S3260, there will be disks set as Jbod within the Disks view of the Storage tab.

To prepare all disks from the Cisco UCS S3260 Storage Servers for storage profiles, the SSD drives for accelerated cache tier have to be converted from JBOD to Unconfigured Good. To convert the disks, follow these steps:

1. Select the Equipment tab in the left pane of the Cisco UCS Manager GUI.
2. Go to Equipment > Chassis > Chassis 1 > Storage Enclosures > Enclosure1.
3. Select Disks and right-click. Select Set JBOD to Unconfigured Good.



For setting a large number of disks from JBOD to Unconfigured Good, it might take some time, and the best view of the status will be in the FSM tab of the server node.

Cisco UCS S3260 Storage Profile

The Storage Profile consists of Storage Policies used for creating Local LUNs out of allocated disks (Disk Group Policies).

A storage profile encapsulates the storage requirements for one or more service profiles. Volumes configured in a storage profile can be used as boot LUNs or data LUNs and can be dedicated to a specific server. You can also specify a local LUN as a boot device. Storage profiles allows you to do the following:

- Configure multiple virtual drives and select the physical drives that are used by a virtual drive. You can also configure the storage capacity of a virtual drive.
- Configure the number, type and role of disks in a disk group.
- Associate a storage profile with a service profile

Cisco UCS Manager's Storage Profile and Disk Group Policies are utilized to define storage disks; disk allocation and management in the Cisco UCS S3260 system.

Create Disk Group Policies

Three Disk Group Policies needs to be created for the solution as follows:

- CVLT_SP-Boot: Boot Volume for all Server Nodes – 2x 480GB SSDs
 - Configured in RAID 1
- CVLT_SP_Raid5-N1: Server Node 1 Accelerated Cache Volume – 4x 1.6TB SSDs
 - Configured in RAID 5
- CVLT_SP_Raid5-N2: Server Node 2 Accelerated Cache Volume – 4x 1.6TB SSDs
 - Configured in RAID 5

Software Defined Storage Tier utilizes the drives presented in JBOD mode to the Cisco UCS Server Nodes and a disk group policy is not required.

- Software Defined Storage Tier – 24x NL-SAS HDDs (Option of 4/6/8/12 TB sizes)
 - Configured in Pass-through (JBOD) mode

Figure 12 Single Node Disk Layout

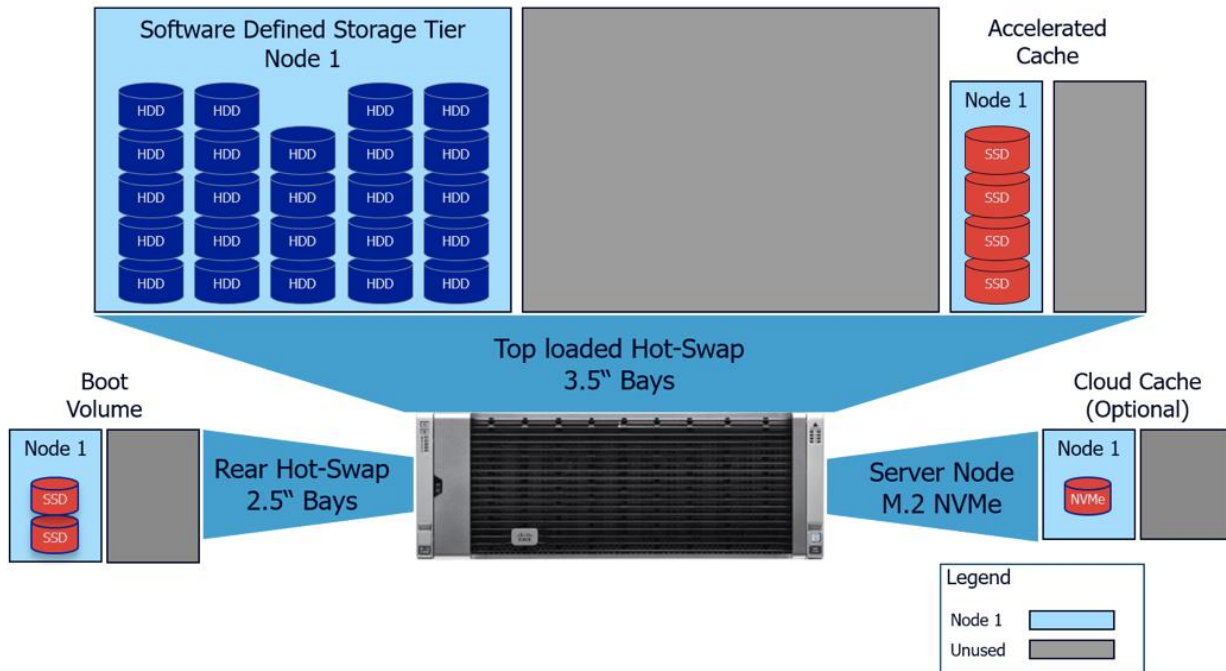
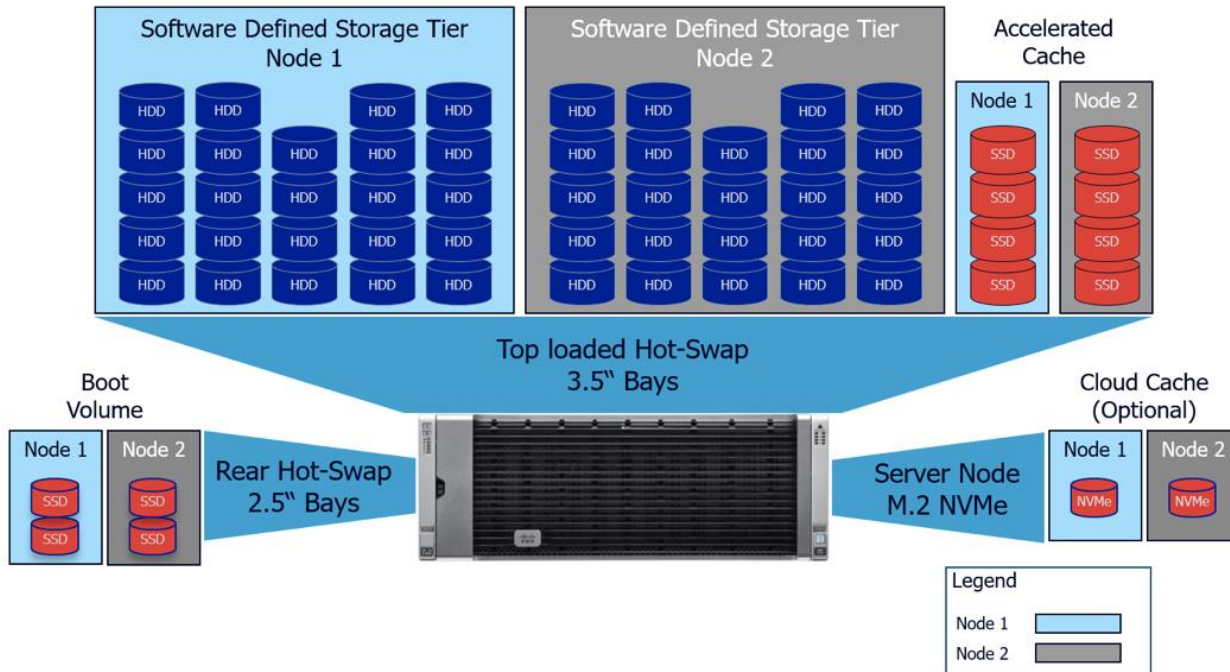


Figure 13 Dual Node Disk Layout



To create a Disk Group Policy, 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 > Disk Group Policies.
- 3. Right-click Disk Group Policy and Select Create Disk Group Policy.
- 4. Enter the name as CVLT_SP-Boot.
- 5. Select RAID Level as RAID 1 Mirrored.
- 6. Select Disk Group Configuration (Manual) and click Add.

Create Disk Group Policy

Name : CVLT_SP-Boot

Description : ScaleProtect Disk Boot Policy

RAID Level : RAID 1 Mirrored

☐ Disk Group Configuration (Automatic)

☒ Disk Group Configuration (Manual)

Disk Group Configuration (Manual)

Advanced FilterExportPrint

Slot Number	Role	Span ID
No data available		

AddDeleteInfo

Virtual Drive Configuration

Strip Size (KB) : Platform Default

Access Policy : ☒ Platform Default ☐ Read Write ☐ Read Only ☐ Blocked

OK

Cancel

- 7. Enter 201 as the slot number and click OK.

Create Disk Group Policy

Name : CVLT_SP-Boot

Description : ScaleProtect Disk Boot Policy

RAID Level : RAID 1 Mirrored

☐ Disk Group Configuration (Automatic)

Disk Group Configuration (Manual)

Advanced Filter Export Print

Slot Number
201

Virtual Drive Configuration

Strip Size (KB) : Platform Default

Create Local Disk Configuration Reference

Slot Number : 201 [1-205]

Role : ☒ Normal ☐ Dedicated Hot Spare ☐ Global Hot Spare

Span ID : unspecified [0-8]

OK Cancel

8. Click OK.

9. Click Add again.

10. Enter 202 as the slot number and click OK.

Create Disk Group Policy

Name : CVLT_SP-Boot

Description : ScaleProtect Disk Boot Policy

RAID Level : RAID 1 Mirrored

☐ Disk Group Configuration (Automatic)

Disk Group Configuration (Manual)

Advanced Filter Export Print

Slot Number
201
202

Virtual Drive Configuration

Create Local Disk Configuration Reference

Slot Number : 202 [1-205]

Role : ☒ Normal ☐ Dedicated Hot Spare ☐ Global Hot Spare

Span ID : unspecified [0-8]

OK Cancel

11. Click OK again.

12. Select **Read Ahead** for Read Policy.

13. Select **Write Back Good BBU** for Write Cache Policy.

14. Select **Cached** for IO Policy.

15. Select **Platform Default** for Drive Cache (any other option will cause a failure because the drive cache on SSDs cannot be changed).

Create Disk Group Policy ? ×

Advanced Filter Export Print ⚙

Slot Number	Role	Span ID
201	Normal	Unspecified
202	Normal	Unspecified

+ Add ✕ Delete i Info

Virtual Drive Configuration

Strip Size (KB) :

Access Policy : ☒ Platform Default ☐ Read Write ☐ Read Only ☐ Blocked

Read Policy : ☐ Platform Default ☒ Read Ahead ☐ Normal

Write Cache Policy : ☐ Platform Default ☐ Write Through ☒ Write Back Good Bbu ☐ Always Write Back

IO Policy : ☐ Platform Default ☐ Direct ☒ Cached

Drive Cache : ☒ Platform Default ☐ No Change ☐ Enable ☐ Disable

Security : ☐

OK **Cancel**

16. Click OK.

17. Create a second Disk Group Policy with RAID-5 for Cache Tier for first Server Nodes in both S3260 chassis.

18. Enter name as **CVLT_SP_Raid5-N1** and optional description.

19. For the RAID level, select **RAID 5 Striped Parity**.

20. Select Disk Group Configuration (Manual) and click Add.

Create Disk Group Policy ? ×

Name : CVLT_SP_Raid5-N1

Description : Commvault Raid5 cache volume

RAID Level : RAID 5 Striped Parity

☐ Disk Group Configuration (Automatic)

☒ Disk Group Configuration (Manual)

Disk Group Configuration (Manual)

Advanced Filter

Export

Print

⚙

Slot Number	Role	Span ID
No data available		

+

Add

⌵

Delete

ⓘ

Info

Virtual Drive Configuration

Strip Size (KB) : Platform Default

Access Policy : ☒ Platform Default ☐ Read Write ☐ Read Only ☐ Blocked

OK

Cancel

21. Enter 49 as the slot number and click OK.

Create Local Disk Configuration Reference ? ×

Slot Number : 49 [1-205]

Role : ☒ Normal ☐ Dedicated Hot Spare ☐ Global Hot Spare

Span ID : unspecified [0-8]

OK

Cancel

22. Repeat steps 1-21 for Slots 50 through 52.

Create Disk Group Policy



Name : CVLT_SP_Raid5-N1

Description : Commvault Raid 5 Cache Volume

RAID Level : RAID 5 Striped Parity

☐ Disk Group Configuration (Automatic)
 ☒ Disk Group Configuration (Manual)

Disk Group Configuration (Manual)

Advanced Filter Export Print		
Slot Number	Role	Span ID
49	Normal	Unspecified
50	Normal	Unspecified
51	Normal	Unspecified
52	Normal	Unspecified

Add
 Delete
 Info

Virtual Drive Configuration

Strip Size (KB) : Platform Default

Access Policy : ☒ Platform Default ☐ Read Write ☐ Read Only ☐ Blocked

OK

Cancel

23. Select **Stripe Size** as **64KB**.

24. Select **Read Ahead** for Read Policy.

25. Select **Write Back Good BBU** for Write Cache Policy.

26. Select **cached** for IO Policy.

27. Select **Platform Default** for Drive Cache (any other option will cause a failure because the drive cache on SSDs cannot be changed).

28. Click OK.

Create Disk Group Policy



Advanced Filter Export Print

Slot Number	Role	Span ID
49	Normal	Unspecified
50	Normal	Unspecified
51	Normal	Unspecified
52	Normal	Unspecified

+ Add - Delete Info

Virtual Drive Configuration

Strip Size (KB) : 64KB

Access Policy : ☒ Platform Default ☐ Read Write ☐ Read Only ☐ Blocked

Read Policy : ☐ Platform Default ☒ Read Ahead ☐ Normal

Write Cache Policy : ☐ Platform Default ☐ Write Through ☒ Write Back Good Bbu ☐ Always Write Back

IO Policy : ☐ Platform Default ☐ Direct ☒ Cached

Drive Cache : ☒ Platform Default ☐ No Change ☐ Enable ☐ Disable

Security : ☐

OK Cancel

29. Create a third Disk Group Policy with RAID-5 for Cache Tier to be used for second server nodes in both S3260 chassis.

30. Enter name as CVLT_SP_Raid5-N2 and optional description.

31. For the RAID level, select RAID 5 Striped Parity.

32. Select Disk Group Configuration (Manual) and click Add.

Create Disk Group Policy



Name : CVLT_SP_Raid5-N2

Description : Commvault Raid5 Cache Volume

RAID Level : RAID 5 Striped Parity

☐ Disk Group Configuration (Automatic) ☒ Disk Group Configuration (Manual)

Disk Group Configuration (Manual)

Advanced Filter Export Print

Slot Number	Role	Span ID
No data available		

+ Add - Delete Info

Virtual Drive Configuration

Strip Size (KB) : Platform Default

Access Policy : ☒ Platform Default ☐ Read Write ☐ Read Only ☐ Blocked

OK Cancel

33. Enter 53 as the slot number and click OK.

Create Local Disk Configuration Reference



Slot Number : [1-205]

Role : ☒ Normal ☐ Dedicated Hot Spare ☐ Global Hot Spare

Span ID : [0-8]



34. Repeat steps 1-33 for Slots 54 through 56.

Create Disk Group Policy



Name :

Description :

RAID Level :

☐ Disk Group Configuration (Automatic) ☒ Disk Group Configuration (Manual)

Disk Group Configuration (Manual)

<input type="button" value="Advanced Filter"/> <input type="button" value="Export"/> <input type="button" value="Print"/>		
Slot Number	Role	Span ID
53	Normal	Unspecified
54	Normal	Unspecified
55	Normal	Unspecified
56	Normal	Unspecified

Virtual Drive Configuration

Strip Size (KB) :

Access Policy : ☒ Platform Default ☐ Read Write ☐ Read Only ☐ Blocked



35. Select **Stripe Size** as **64KB**.

36. Select **Read Ahead** for Read Policy.

37. Select **Write Back Good BBU** for Write Cache Policy.

38. Select **cached** for IO Policy.

39. Select **Platform Default** for Drive Cache (any other option will cause a failure because the drive cache on SSDs cannot be changed).

40. Click OK.

Create Disk Group Policy

? X

Advanced Filter Export Print

Slot Number	Role	Span ID
53	Normal	Unspecified
54	Normal	Unspecified
55	Normal	Unspecified
56	Normal	Unspecified

Add Delete Info

Virtual Drive Configuration

Strip Size (KB) : 64KB

Access Policy : ☒ Platform Default ☐ Read Write ☐ Read Only ☐ Blocked

Read Policy : ☐ Platform Default ☒ Read Ahead ☐ Normal

Write Cache Policy : ☐ Platform Default ☐ Write Through ☒ Write Back Good Bbu ☐ Always Write Back

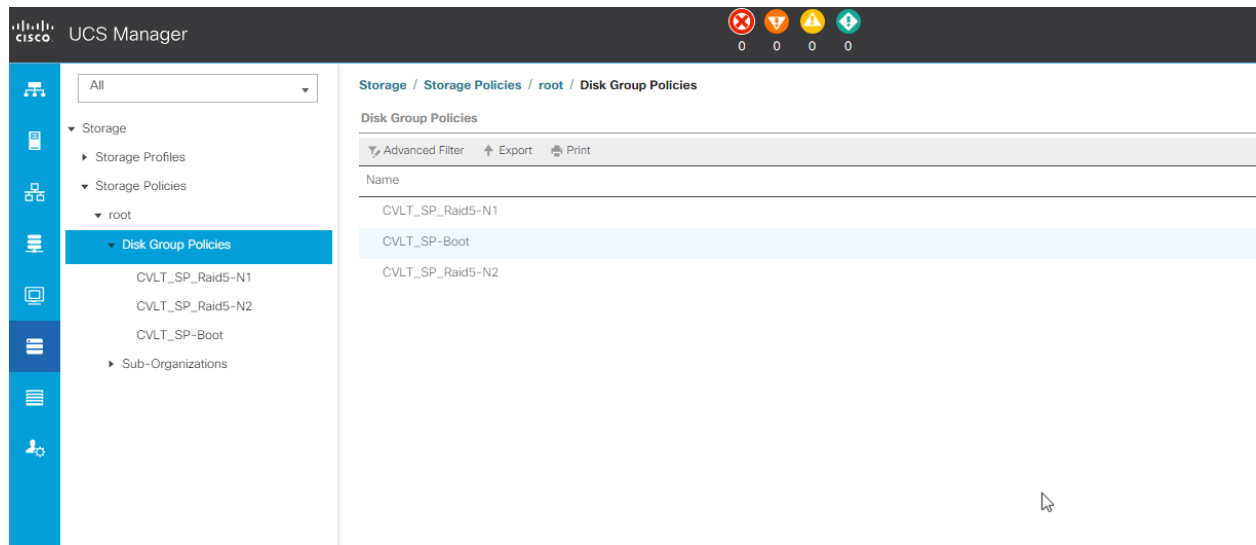
IO Policy : ☐ Platform Default ☐ Direct ☒ Cached

Drive Cache : ☒ Platform Default ☐ No Change ☐ Enable ☐ Disable

Security : ☐

OK Cancel

41. Verify the three disk group policies are created successfully.



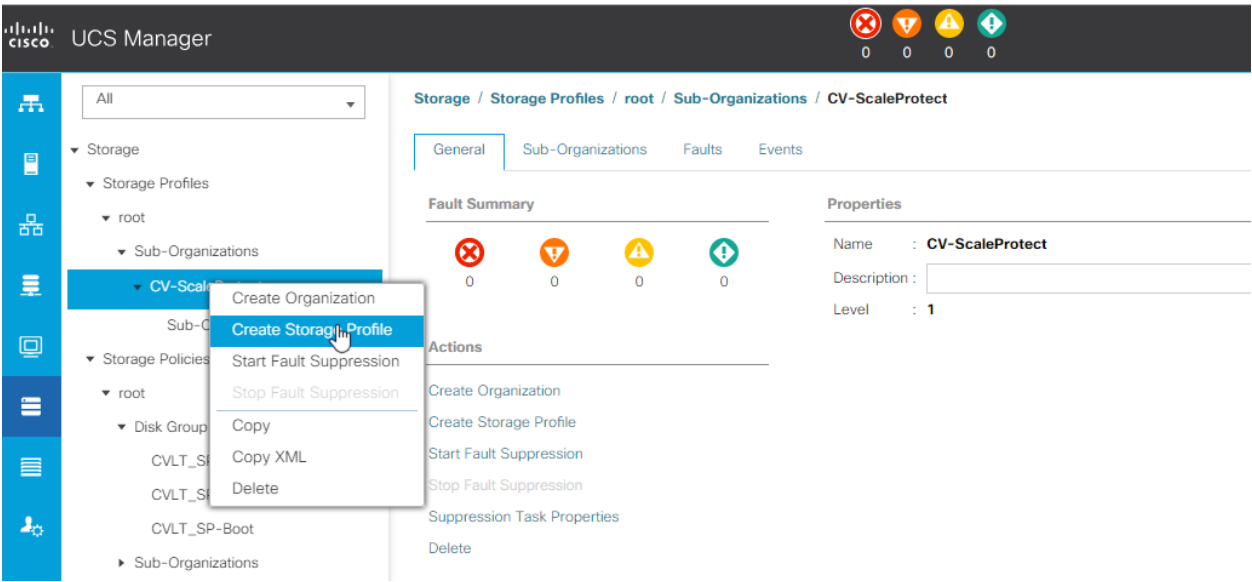
42. For the top-loaded HDDs, no RAID configuration is required because they are used in JBOD mode.

Create Storage Profile

To create Storage Profile for S3260, 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_S3260_S1.

5. Under Local LUNs Selection, click Add.

Create Storage Profile

?

×

Name : CVLT_SP_S3260_S1

Description : ScaleProtect Storage Profile for Node #1

LUNs

Local LUNs

Controller Definitions

Security Policy

⌵ Advanced Filter

⬆ Export

🖨 Print

⚙

Name	Size (GB)	Order	Fractional Size (MB)
No data available			

⊕ Add

🗑 Delete

ℹ Info

OK

Cancel

6. Enter Name as Boot.

7. Enter 1 as the size in GB.

8. Check **Expand to Available**, this creates a single LUN with maximum space available.

9. Select Disk Group Selection as CVLT_SP-Boot and click OK.

Create Local LUN ? ×

☒ Create Local LUN

☐ Prepare Claim Local LUN

Name

:

Boot

Size (GB)

:

1

[0-245760]

Fractional Size (MB)

:

0

Auto Deploy

:

☒ Auto Deploy

☐ No Auto Deploy

Expand To Available

:

☒

Select Disk Group Configuration :

<not set>

Create Disk Group Policy

<not set>

Domain Policies

CVLT_SP-Boot

CVLT_SP_Raid5-N1

CVLT_SP_Raid5-N2

OK

Cancel

10. Click Add under Local LUN to continue creating LUNs in the SSD Disk Group.

Create Storage Profile

?

×

Name : CVLT_SP_S3260_S1

Description : ScaleProtect Storage Profile for Node #1

LUNs

Local LUNs

Controller Definitions

Security Policy

⌵ Advanced Filter

⬆ Export

🖨 Print

⚙

Name	Size (GB)	Order	Fractional Size (MB)
Boot	1	Not Applicable	0

⊕ Add

🗑 Delete

ℹ Info

OK

Cancel

- 11. Enter Name as `Cache`; this is the LUN used by first Server Nodes for Cache.
- 12. Enter 1 as the size in GB.
- 13. Check `Expand to Available` and Select Disk Group Configuration as `CVLT_SP_Raid5-N1`.
- 14. Click OK.

Create Local LUN



☒ Create Local LUN ☐ Prepare Claim Local LUN

Name	:	Cache
------	---	-------

Size (GB) : 1 [0-245760]

Fractional Size (MB)	:	0
----------------------	---	---

Auto Deploy : ☒ Auto Deploy ☐ No Auto Deploy

Expand To Available : ☒

Select Disk Group Configuration : CVLT_SP_Raid5-N1  [Create Disk Group Policy](#)

<not set>

Domain Policies

CVLT_SP-Boot

CVLT_SP_Raid5-N1

CVLT_SP_Raid5-N2

OK

Cancel

15. Verify that all the LUNs are configured as documented and click OK.

Create Storage Profile



Name : CVLT_SP_S3260_S1

Description : ScaleProtect Storage Profile for Node #1

LUNs

Local LUNs Controller Definitions Security Policy			
Advanced Filter Export Print			
Name	Size (GB)	Order	Fractional Size (MB)
Cache	1	Not Applicable	0
Boot	1	Not Applicable	0

Add
 Delete
 Info

OK

Cancel

16. Create another Storage Profile with name as CVLT_SP_S3260_S2 for second server nodes in the S3260 Chassis.
17. Under Local LUN Selection, click Add.
18. Enter Name as Boot.
19. Enter 1 as the size in GB.
20. Check **Expand to Available**, this creates a single LUN with maximum space available.
21. Select Disk Group Selection as CVLT_SP-Boot and click OK.

Create Local LUN



☒ Create Local LUN ☐ Prepare Claim Local LUN

Name :

Size (GB) : [0-245760]

Fractional Size (MB) :

Auto Deploy : ☒ Auto Deploy ☐ No Auto Deploy

Expand To Available : ☒

Select Disk Group Configuration :

<not set>

Domain Policies

CVLT_SP-Boot

CVLT_SP_Raid5-N1

CVLT_SP_Raid5-N2

OK

Cancel

22. Click Add under Local LUN to continue creating LUNs in the SSD Disk Group
23. Enter Name as `cache`; this is the LUN used by first Server Nodes for Cache.
24. Enter 1 as the size in GB.
25. Check Expand to Available and Select Disk Group Configuration as `CVLT_SP_Raid5-N2`.
26. Click OK.

Create Local LUN

?

×

Create Local LUN

Prepare Claim Local LUN

Name

:

Cache

Size (GB)

:

1

[0-245760]

Fractional Size (MB)

:

0

Auto Deploy

:

Auto Deploy

No Auto Deploy

Expand To Available

:

Select Disk Group Configuration :

CVLT_SP_Raid5-N2

Create Disk Group Policy

OK

Cancel

27. Verify that all the LUNs are configured as documented and click OK.

Create Storage Profile



Name : CVLT_SP_S3260_S2

Description : ScaleProtect Storage Profile for Node #2

LUNs

Local LUNs			
Controller Definitions			
Security Policy			
Advanced Filter Export Print			
Name	Size (GB)	Order	Fractional Size (MB)
Cache	1	Not Applicable	0
Boot	1	Not Applicable	0

Add Delete Info

OK

Cancel

Create Boot Policy

A boot policy will be needed to boot from the `CV_SP_Boot` Local LUN created during the Disk Group Policy part of the Storage Profile.

To create boot policy, follow these steps:

1. In Cisco UCS Manager, click Server within the Navigation Pane, and select Policies from within the Server drop-down options.
2. Select root > Sub-Organizations > CV-ScaleProtect > Boot Policies.
3. Right-click Boot Policies and select Create Boot Policy.
4. Enter `CVLT_S3260_Boot` as the name of the boot policy.
5. Optional: Enter a description for the boot policy.
6. Keep the Reboot on the Boot Order Change check box unchecked.

Create Boot Policy

?

X

Name

:

CVLT_S3260_Boot

Description

:

Reboot on Boot Order Change

:

☐

Enforce vNIC/vHBA/iSCSI Name

:

☒

Boot Mode

:

☒ Legacy

☐ Uefi

WARNINGS:

The type (primary/secondary) does not indicate a boot order presence.

The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.

If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.

If it is not selected, the vNICs/vHBAs are selected if they exist, otherwise the vNIC/vHBA with the lowest PCIe bus scan order is used.

+ Local Devices

+ CIMC Mounted vMedia

+ vNICs

+ vHBAs

+ iSCSI vNICs

+ EFI Shell

Boot Order

+ - Advanced Filter Export Print

Name	Order	vNIC/vH...	Type	LUN Na...	WWN	Slot Nu...	Boot Na...	Boot Path	Descripti...
No data available									

Move Up

Move Down

Delete

Set Uefi Boot Parameters

OK

Cancel

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

Add SD Card

Add Internal USB

Add External USB

Add Embedded Local LUN

Add Embedded Local Disk

Add CD/DVD

Add Local CD/DVD

Add Remote CD/DVD

Add Floppy

Add Local Floppy

Add Remote Floppy

Add Remote Virtual Drive

Add NVMe

- CIMC Mounted vMedia

Move Up

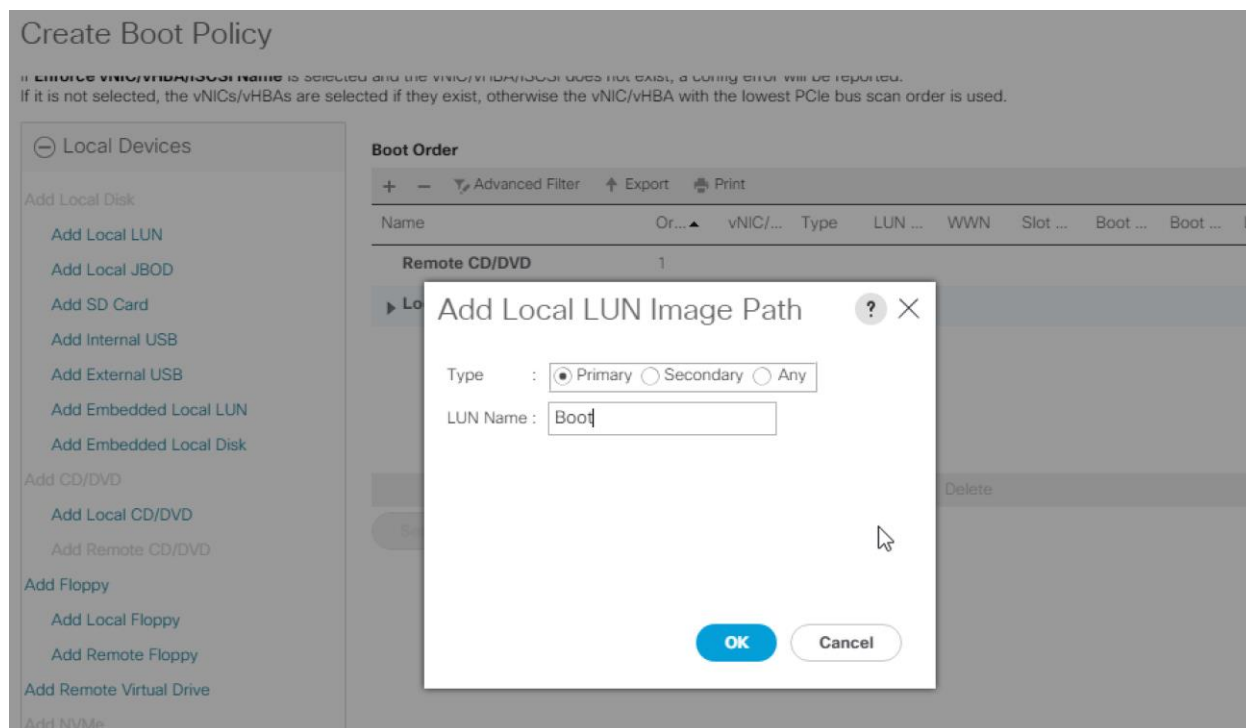
Move Down

Delete

Set Uefi Boot Parameters

8. Click Add Local LUN to reference the Boot LUN created by the CV_SP_Boot Disk Group Policy.

125



9. Click OK and click OK again to create the Boot Policy.

Cisco UCS S3260 Service Profile Template

Service profile template configuration for the Cisco UCS S3260 server nodes is covered 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.



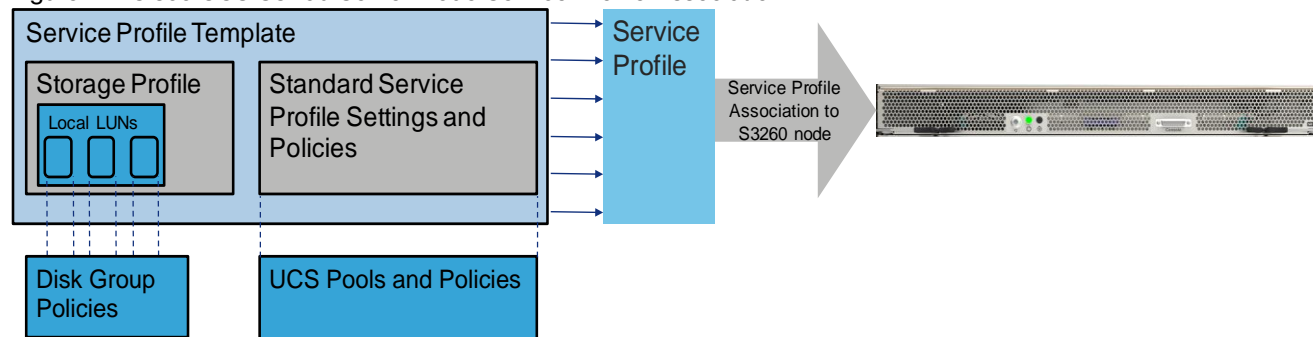
If you need only one service profile with similar values to an existing service profile, you can clone a service profile in the Cisco UCS Manager GUI.

For example, if you need several service profiles with similar values to configure servers to host database software, 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 14 Cisco UCS S3260 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_S3260_SN1` as the name of the service profile template.
6. Select the Updating Template option.
7. Under UUID, select `UUID_Pool1` as the UUID pool.

Create Service Profile Template

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

Name :

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

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

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

UUID Assignment:

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

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

< Prev Next > **Finish** Cancel

8. Click Next.

Configure Storage Provisioning

To configure storage provisioning, follow these steps:

1. Click Storage Profile Policy Tab and select `CVLT_SP_S3260_S1` (as created under Storage Profile section).

Create Service Profile Template

Optionally specify or create a Storage Profile, and select a local disk configuration policy.

Specific Storage Profile | **Storage Profile Policy** | Local Disk Configuration Policy

Storage Profile: `CVLT_SP_S3260_S1` [Create Storage Profile](#)

Name : **CVLT_SP_S3260_S1**
 Description : **ScaleProtect Storage Profile for Node #1**

LUNs

Local LUNs | Controller Definitions | Security Policy

Advanced Filter | Export | Print

Name	Size (GB)	Order	Fractional Size (MB)
Boot	1	Not Applicable	0
Cache	1	Not Applicable	0

< Prev Next > **Finish** Cancel

2. Click Next.

Configure Networking Options

To configure 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.

Create Service Profile Template

Optionally specify LAN configuration information.

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

[Create Dynamic vNIC Connection Policy](#)

How would you like to configure LAN connectivity?

☐ Simple ☐ Expert ☐ No vNICs ☒ Use Connectivity Policy

LAN Connectivity Policy : CVLT_SP_LAN ▼ [Create LAN Connectivity Policy](#)

Initiator Name

Initiator Name Assignment: <not set> ▼ [Create IQN Suffix Pool](#)

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

< Prev Next > Finish Cancel

4. Click Next.

Configure Storage Options



Skip the SAN Connectivity since you will use local storage for S3260 created through Storage Policy and Select No vHBAs.

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.

Create Service Profile Template

Optionally specify disk policies and SAN configuration information.

How would you like to configure SAN connectivity?

☐ Simple
 ☐ Expert
 ☐ No vHBAs
 ☒ Use Connectivity Policy

SAN Connectivity Policy : CVLT_SP_SAN ▼ [Create SAN Connectivity Policy](#)

< Prev Next > **Finish** Cancel

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 vNIC/HBA placement, follow these steps:

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

Figure 15 Default Installation without HBAs

1

Identify Service Profile Template

2

3

Storage Provisioning

4

5

Networking

6

7

8

9

10

11

12

13

14

15

16

Create Service Profile Template

?

×

Specify how vNICs and vHBAs are placed on physical network adapters

vNIC/vHBA Placement specifies how vNICs and vHBAs are placed on physical network adapters (mezzanine) in a server hardware configuration independent way.

Select Placement:

Let System Perform Placement

[Create Placement Policy](#)

System will perform automatic placement of vNICs and vHBAs based on PCI order.

Name	Address	Order
vNIC vNIC_Clus_eth1	Derived	1
vNIC vNIC_Data_eth0	Derived	2

↑ Move Up

↓ Move Down

🗑 Delete

↻ Reorder

⚙ Modify

< Prev

Next >

Finish

Cancel

Figure 16 Installation with HBAs for SAN Connectivity

1

Identify Service Profile Template

2

3

Storage Provisioning

4

5

Networking

6

7

8

9

10

11

12

13

14

15

16

Create Service Profile Template

?

×

Specify how vNICs and vHBAs are placed on physical network adapters

vNIC/vHBA Placement specifies how vNICs and vHBAs are placed on physical network adapters (mezzanine) in a server hardware configuration independent way.

Select Placement:

Let System Perform Placement

[Create Placement Policy](#)

System will perform automatic placement of vNICs and vHBAs based on PCI order.

Name	Address	Order
vHBA vHBA4	Derived	1
vHBA vHBA3	Derived	2
vHBA vHBA2	Derived	3
vHBA vHBA1	Derived	4
vNIC vNIC_Clus_eth1	Derived	5
vNIC vNIC_Data_eth0	Derived	6

↑ Move Up

↓ Move Down

🗑 Delete

↻ Reorder

⚙ Modify

< Prev

Next >

Finish

Cancel

2. Click Next.

Configure vMedia Policy

To configure the vMedia policy, follow these steps:

1. From the vMedia Policy, leave as `default`.

The screenshot displays the 'Create Service Profile Template' wizard in Cisco UCS Manager. The left-hand navigation pane lists 11 steps: 1. Identify Service Profile Template, 2. Storage Provisioning, 3. Networking, 4. SAN Connectivity, 5. Zoning, 6. vNIC/vHBA Placement, 7. vMedia Policy (highlighted in blue), 8. Server Boot Order, 9. Maintenance Policy, 10. Server Assignment, and 11. Operational Policies. The main content area for step 7 is titled 'Create Service Profile Template' and includes a sub-header 'Optionally specify the Scriptable vMedia policy for this service profile template.' Below this, there is a 'vMedia Policy:' label followed by a dropdown menu currently set to 'Select vMedia Policy to use'. A blue link 'Create vMedia Policy' is positioned below the dropdown. A note states, 'The default boot policy will be used for this service profile.' At the bottom right, there are four buttons: '< Prev', 'Next >', 'Finish' (highlighted in blue), and 'Cancel'.

2. Click Next.

Configure Server Boot Order

To configure the server boot order, follow this step:

1. Choose `CVLT_S3260_Boot` as the Boot Policy that was created earlier.

1

Identify Service Profile Template

2

Storage Provisioning

3

Networking

4

SAN Connectivity

5

Zoning

6

vNIC/vHBA Placement

7

vMedia Policy

8

Server Boot Order

9

Maintenance Policy

10

Server Assignment

11

Operational Policies

Create Service Profile Template

?

×

Optionally specify the boot policy for this service profile template.

Select a boot policy.

Boot Policy: CVLT_S3260_Boot

Create Boot Policy

Name

:

CVLT_S3260_Boot

Description

:

Reboot on Boot Order Change

:

No

Enforce vNIC/vHBA/iSCSI Name

:

Yes

Boot Mode

:

Legacy

WARNINGS:

The type (primary/secondary) does not indicate a boot order presence.

The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.

If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.

If it is not selected, the vNICs/vHBAs are selected if they exist, otherwise the vNIC/vHBA with the lowest PCIe bus scan order is used.

Boot Order

+ - Advanced Filter Export Print

Name	Order	vNIC/vHB...	Type	LUN Name	WWN	Slot Numb...	Boot Name	Boot Path	Description
Remot...	1								
Local L...	2								
Loc...			Primary	Boot					

Create iSCSI vNIC

Set iSCSI Boot Parameters

Set UEFI Boot Parameters

< Prev

Next >

Finish

Cancel

Configure Maintenance Policy

To configure the maintenance policy, follow these steps:

- 1. Change the Maintenance Policy to `UserAck_Pol`.

1

Identify Service Profile Template

2

3

Storage Provisioning

4

5

Networking

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

Create Service Profile Template

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

⊖ Maintenance Policy

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

Maintenance Policy:

UserAck_Pol

Create Maintenance Policy

Name

: UserAck_Pol

Description

:

Soft Shutdown Timer

: 150 Secs

Storage Config. Deployment Policy

: User Ack

Reboot Policy

: User Ack

< Prev

Next >

Finish

Cancel

2. Click Next.

Configure Server Assignment

To configure server assignment, follow these steps:

1. In the Pool Assignment list, select the server pool created for the first Server Nodes in the Chassis.

Create Service Profile Template

Optionally specify a server pool for this service profile template.

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

Pool Assignment: CVLT_SP_Pool_SN1 ▼ [Create Server Pool](#)

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

☒ Up ☐ Down

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

Server Pool Qualification : all-chassis ▼

Restrict Migration : ☐

+ Firmware Management (BIOS, Disk Controller, Adapter)

< Prev Next > **Finish** Cancel

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

− Firmware Management (BIOS, Disk Controller, Adapter)

If you select a host firmware policy for this service profile, the profile will update the firmware on the server that it is associated with. Otherwise the system uses the firmware already installed on the associated server.

Host Firmware Package: CV_SP_Firmware ▼

[Create Host Firmware Package](#)

- Click Next.

Create Service Profile Template [?] X

Optionally specify a server pool for this service profile template.

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

Pool Assignment: CVLT_SP_Pool_LSN1 [Create Server Pool](#)

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

☒ Up ☐ Down

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

Server Pool Qualification: all-chassis

Restrict Migration: ☐

Firmware Management (BIOS, Disk Controller, Adapter)

If you select a host firmware policy for this service profile, the profile will update the firmware on the server that it is associated with. Otherwise the system uses the firmware already installed on the associated server.

Host Firmware Package: CV_SP_Firmware [Create Host Firmware Package](#)

< Prev Next > **Finish** Cancel

4. Click Next.

Configure Operational Policies

To configure the operational policies, follow these steps:

1. In the BIOS Policy list, select **SP-S3260-BIOS**.
2. Expand **Power Control Policy Configuration** and select **No-Power-Cap** in the Power Control Policy list.

Create Service Profile Template

Optionally specify information that affects how the system operates.

BIOS Configuration

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

BIOS Policy : SP-S3260-BIOS ▼

External IPMI Management Configuration

Management IP Address

Monitoring Configuration (Thresholds)

Power Control Policy Configuration

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

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

Scrub Policy

KVM Management Policy

Graphics Card Policy

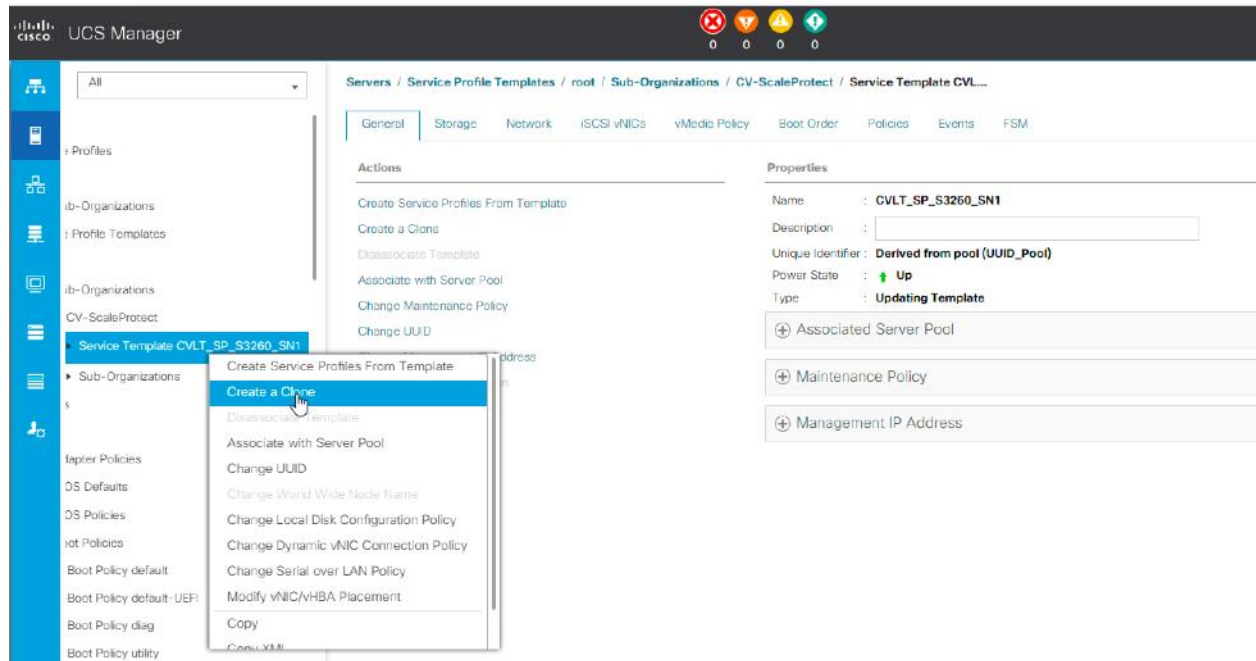
< Prev Next > **Finish** Cancel

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.

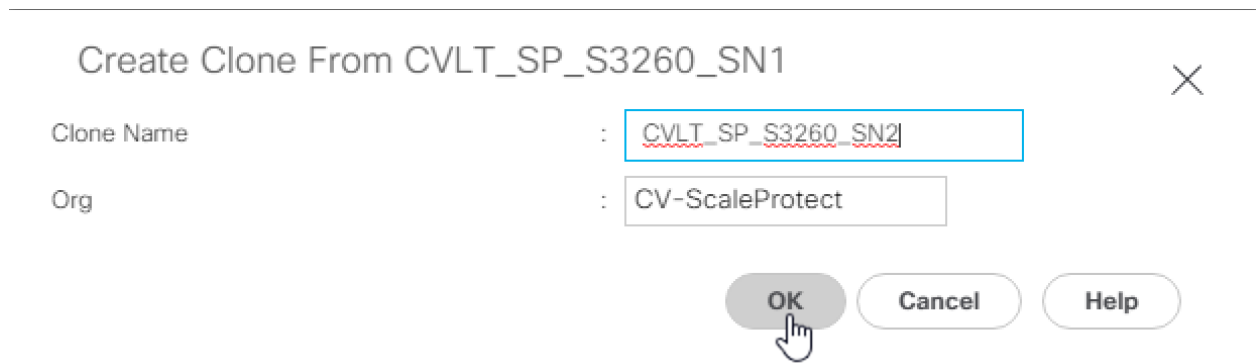


The following steps create the service profile template for the second server nodes in the chassis.

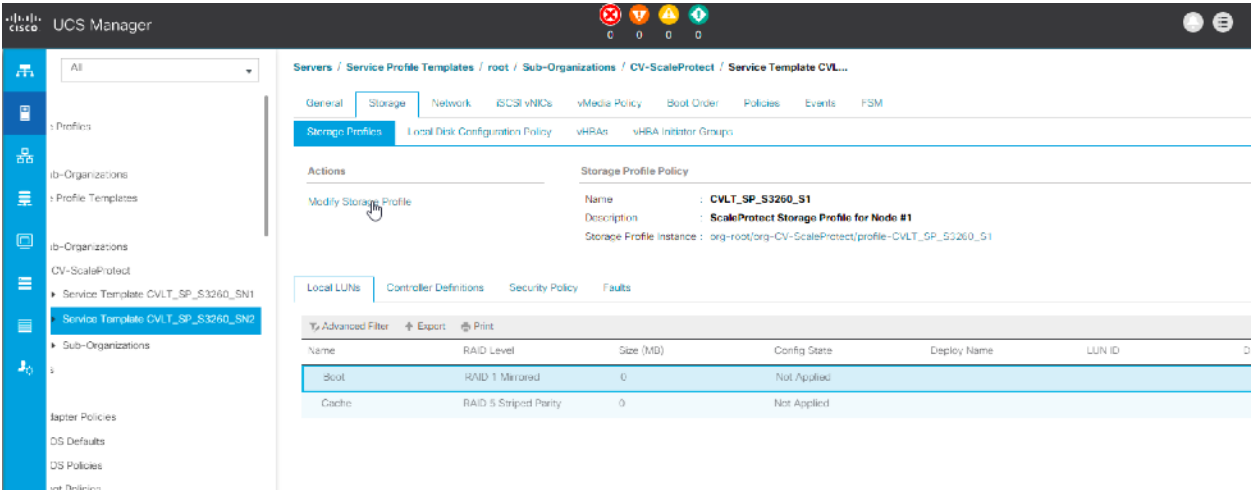
5. Right-click the newly created service profile template CVLT_SP_S3260_SN1.
6. Choose Create a Clone.



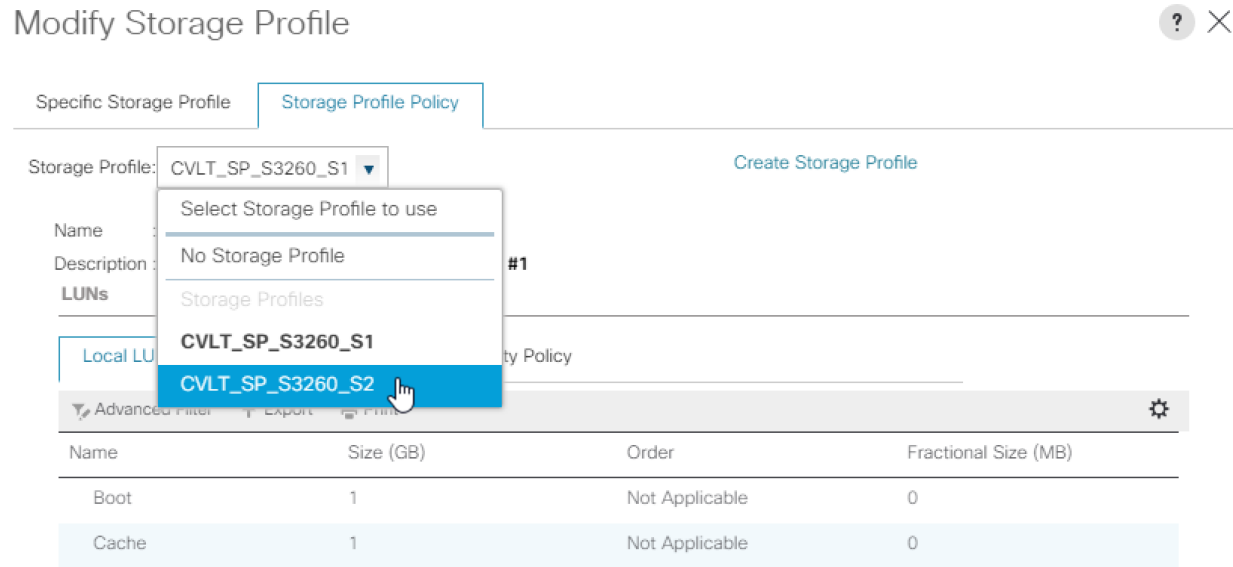
7. In the dialog box, enter CVLT_SP_S3260_SN2 as the name of the clone, choose the CV-ScaleProtect org, and click OK.



8. Select the template CVLT_SP_S3260_SN2
9. Under Storage > Storage Profiles in the right pane.
10. Click Modify Storage Profile to modify the storage profile.



11. Select `CVLT_SP_S3260_S2` storage profile to be used in the template.

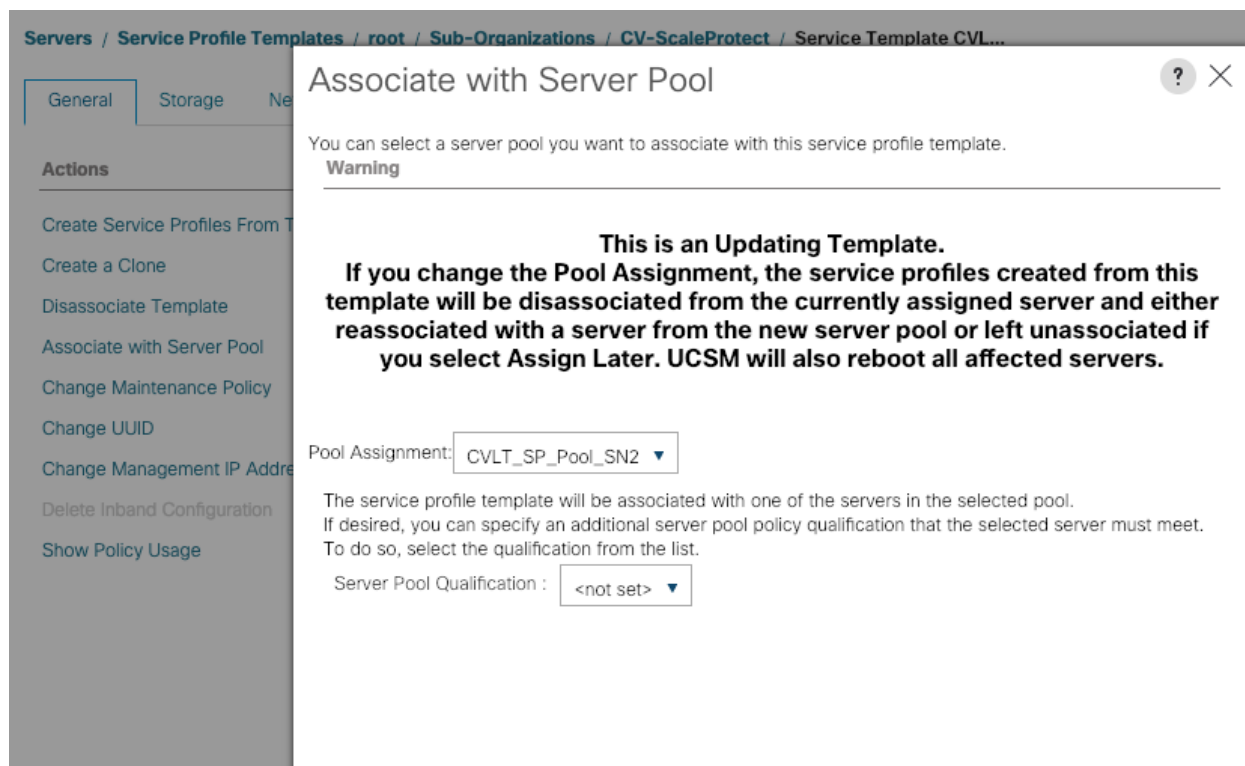


12. Click Associate with Server Pool under General tab.

13. Change the pool assignment to `CVLT_SP_Pool_SN2`.

14. Click OK.

15. Click OK again.



Create Service Profiles

This section describes how to associate the Compute Node on S3260 Storage server 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_S3260_SN1.
3. Right-click CVLT_SP_S3260_SN1 Template and select Create Service Profiles from Template.
4. Enter CVLT_SP_S3260_SN1- as the service profile prefix.
5. Enter 1 as "Name Suffix Starting Number."
6. Enter 2 as the "Number of Instances."
7. Click OK to create the service profiles.
8. Click OK in the confirmation message.

Create Service Profiles From Template

Naming Prefix

:

CVLT_SP_S3260_SN1-

Name Suffix Starting Number

:

1

Number of Instances

:

2

OK

Cancel

9. Right-click CVLT_SP_S3260_SN2 Template and select Create Service Profiles from Template.
10. Enter CVLT_SP_S3260_SN2- as the service profile prefix.
11. Enter 1 for "Name Suffix Starting Number."
12. Enter 1 for the "Number of Instances."
13. Click OK to create the service profiles.

Create Service Profiles From Template ? ×

Naming Prefix : CVLT_SP_S3260_SN2-

Name Suffix Starting Number : 1

Number of Instances : 1



Cancel

14. Click OK in the confirmation message.

15. 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.

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

All

Servers

Service Profiles

root

Sub-Organizations

CV-ScaleProtect

CVLT_SP_S3260_SN1-1

CVLT_SP_S3260_SN1-2

CVLT_SP_S3260_SN2-1

Sub-Organizations

Service Profile Templates

root

Servers

Service Profiles

AllFailedActivePassiveDisassociatedPendingHierarchicalPending Activities

Advanced FilterExportPrint

Name	User Label	Overall Status	Assoc State	Server
Service Profile CVLT_SP_S3260_SN1-1		OK	Associated	sys/chassis-2/blade-1
Service Profile CVLT_SP_S3260_SN1-2		OK	Associated	sys/chassis-1/blade-1
Service Profile CVLT_SP_S3260_SN2-1		OK	Associated	sys/chassis-1/blade-2

AddDeleteInfo

17. Verify the Boot LUN and Cache LUNs under Storage tab of Service Profile.

All

Servers

Service Profiles

root

Sub-Organizations

CV-ScaleProtect

CVLT_SP_S3260_SN1-1

ISCSI vNICs

vHBAs

vNICs

CVLT_SP_S3260_SN1-2

CVLT_SP_S3260_SN2-1

Sub-Organizations

Service Profile Templates

root

Sub-Organizations

CV-ScaleProtect

Service Template CVLT_SP_S

Service Template CVLT_SP_S

Servers / Service Profiles / root / Sub-Organizations / CV-ScaleProtect / Service Profile CVLT...

GeneralStorageNetworkISCSI vNICsvMedia PolicyBoot OrderVirtual MachinesFC ZonesPoliciesServer DetailsCIMC SessionsFSMVIF PathsFaultsEvents

Storage ProfilesLocal Disk Configuration PolicyvHBAsvHBA Initiator Groups

ActionsStorage Profile Policy

Modify Storage ProfileNameCVLT_SP_S3260_S1DescriptionScaleProtect Storage Profile for Node #1Storage Profile Instance : org-root/org-CV-ScaleProtect/profile-CVLT_SP_S3260_S1

Local LUNsController DefinitionsSecurity PolicyFaults

Advanced FilterExportPrint

Name	RAID Level	Size (MB)	Config State	Deploy Name	LUN ID	Drive State
Boot	RAID 1 Mirrored	456809	Applied	Boot-3	1001	optimal
Cache	RAID 5 Striped Parity	4574775	Applied	Cache-3	1000	optimal

AddDeleteInfo

18. Verify Service Profile has 2 vNICs.

Sub-Organizations

CV-ScaleProtect

CVLT_SP_S3260_SN1-1

ISCSI vNICs

vHBAs

vNICs

vNIC vNIC_Clus_eth1

vNIC vNIC_Data_eth0

CVLT_SP_S3260_SN1-2

CVLT_SP_S3260_SN2-1

Sub-Organizations

Service Profile Templates

root

Sub-Organizations

CV-ScaleProtect

Change Dynamic vNIC Connection PolicyNothing Selected

Modify vNIC/vHBA PlacementvNIC/vHBA Placement PolicyNothing Selected

LAN Connectivity PolicyLAN Connectivity Policy : CVLT_SP_LANLAN Connectivity Policy Instance : org-root/org-CV-ScaleProtect/lan-conn-pol-CVLT_SP_LANCreate LAN Connectivity Policy

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

Advanced FilterExportPrint

Name	MAC Address	Desired Order	Actual Order	Fabric ID	Desired Placement	Actual Placement	Admin Host Port	Actual Host Port
vNIC vNIC_Clus_e...	00:25:B5:55:B0:2F	2	2	B A	Any	1	ANY	NONE
vNIC vNIC_Data_e...	00:25:B5:55:A0:00	1	1	A B	Any	1	ANY	NONE

Commvault HyperScale Installation and Configuration

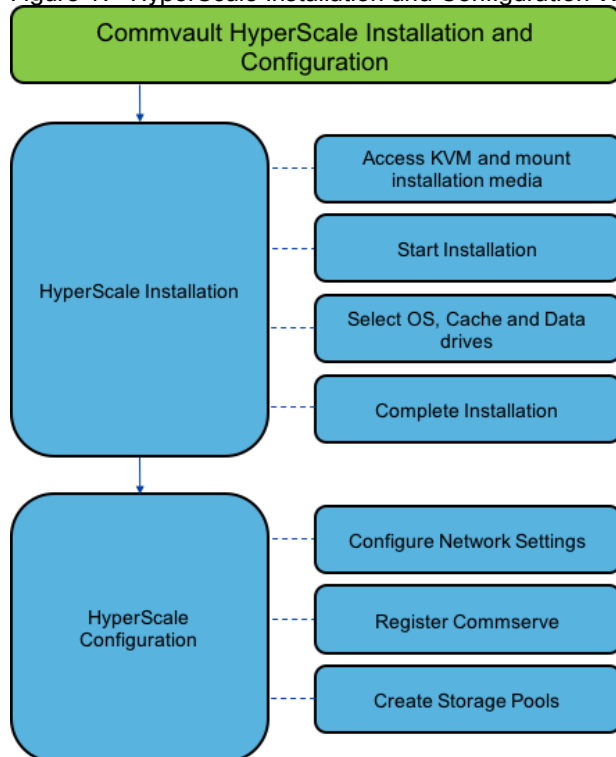
This section explains the Commvault HyperScale installation and configuration on Cisco UCS S3260 Storage Servers.

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



Make sure you have the latest copy of the Commvault HyperScale ISO downloaded from <https://cloud.commvault.com>.

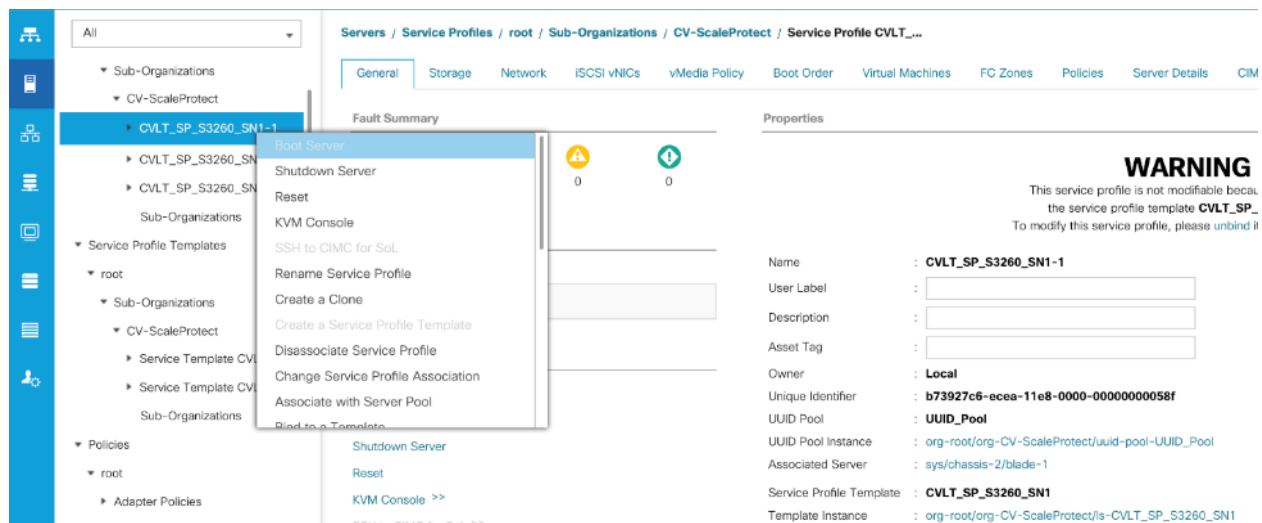
Figure 17 HyperScale Installation and Configuration Workflow



1. Open a web browser and navigate to the Cisco UCS 6332 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.



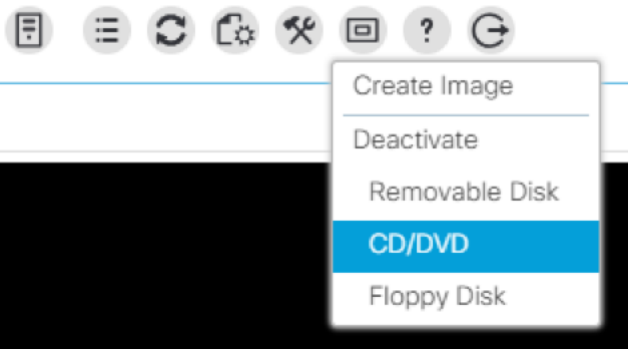
5. From the main menu, click the Servers tab.
6. Select Servers > Service Profiles > root > Sub-Organizations > CV-ScaleProtect > CVLT_SP_S3260_SN1-1.
7. Right-click CVLT_SP_S3260_SN1-1 and select KVM Console.
8. If prompted to accept an Unencrypted KVM session, accept as necessary.



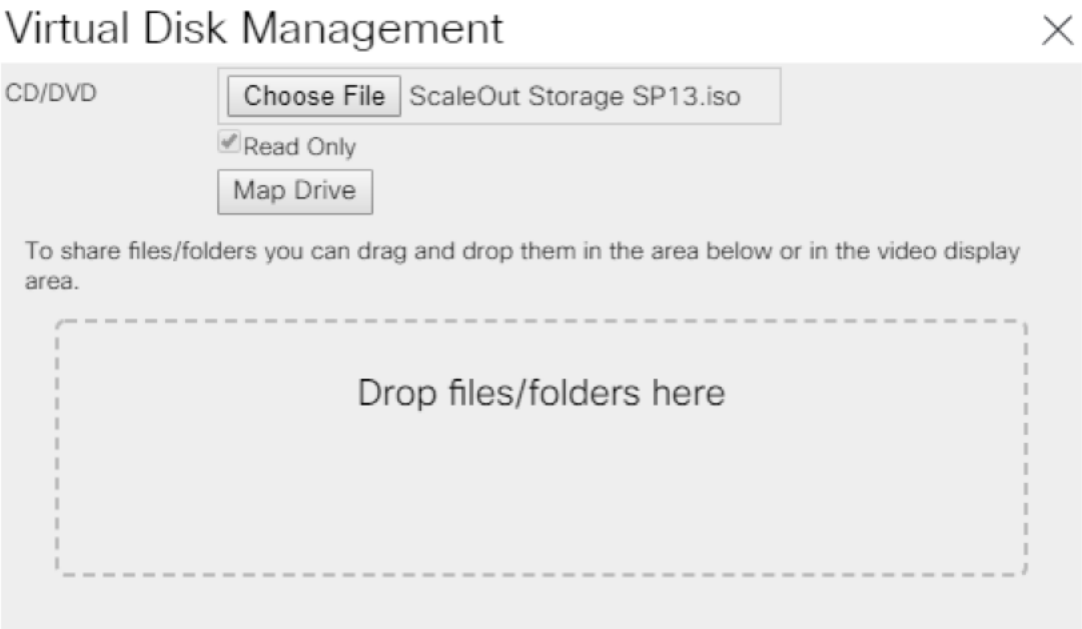
9. Attach the ISO to the server node using the KVM.
10. In the KVM windows, click the Virtual Media icon and select Activate Virtual Devices.



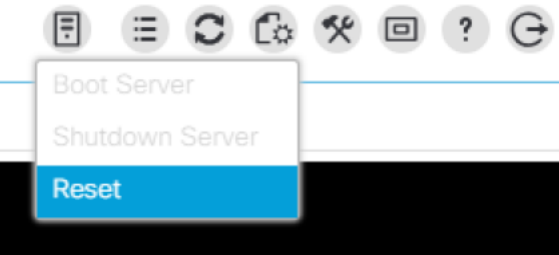
11. Click the Virtual Media icon and now select CD/DVD and browse to where the ISO is located, then click Map Device.



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



13. Click the Server icon the menu up top, then click Reset.



14. On the Reset Server pop up, click OK.

Reset Server



You have selected the **Reset** action for one or more servers.

If you are trying to boot a server from a power-down state, you should not use this method.

If you continue the power-up with this process, the desired power state of the servers will become out of sync with the actual power state and the servers may unexpectedly shut down at a later time.

To safely reboot the selected servers from a power-down state, click **Cancel** then select the **Boot Server** action.

If you are certain that you want to continue with the **Reset** operation, click **OK**.

OK

Cancel

15. Select Power Cycle, then click OK.

Do you want to reset the selected servers?



You are attempting to reset a server. The server can be reset by gracefully restarting the OS or via a brute force power cycle. How would you like to reset?

- ☒ Power Cycle
☐ Gracefully restart OS

If Graceful OS Restart is not supported by the OS or it does not happen within a reasonable amount of time, the system will perform a power cycle.

To reset the slot, please go to the recover server action.

The UCS system might be in the process of performing some tasks on this server. Would you like this operation to wait until the completion of outstanding activities?

☐ Wait for completion of outstanding UCS tasks on this server.

OK

Cancel

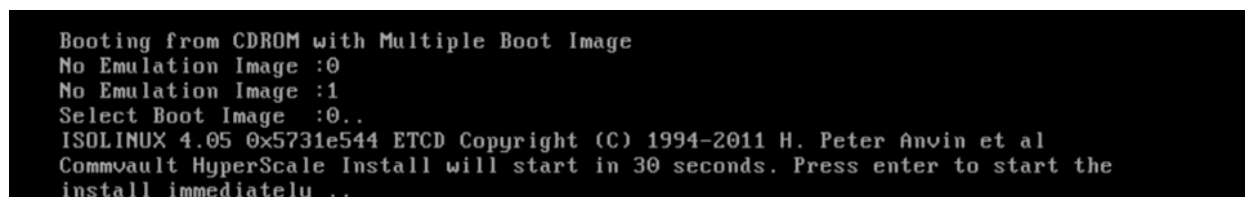
16. As the server is coming up, at the main screen, press F6 to enter the boot menu.



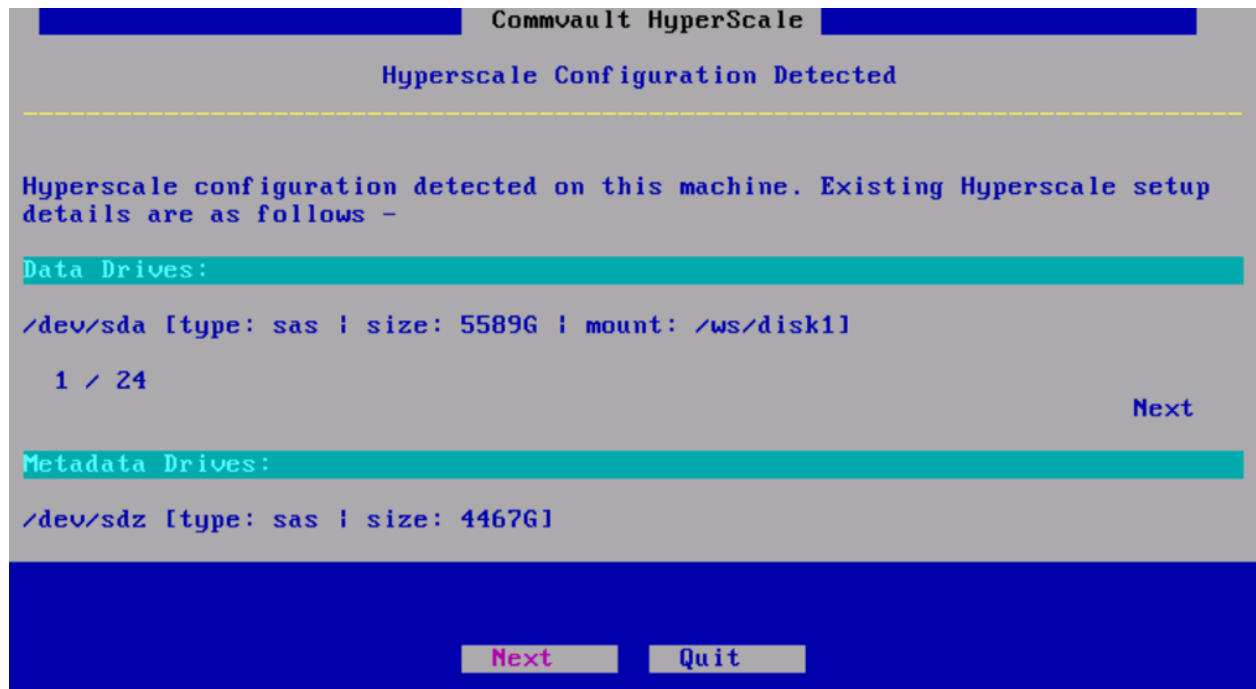
17. When the boot menu appears select Cisco vKVM-Mapped vDVD.



18. Once the ISO loads, it will ask which Image to boot from, select the default image 0.



19. The first screen shows the drives detected for the storage and the accelerated cache metadata, in the case of the S3260, it sees the Data drives (in this case the 6TB drives, and it shows it found 24 (1/24)) and also found the Raid 5 SSD cache of 4.4TB. Press Tab to click Next to continue.

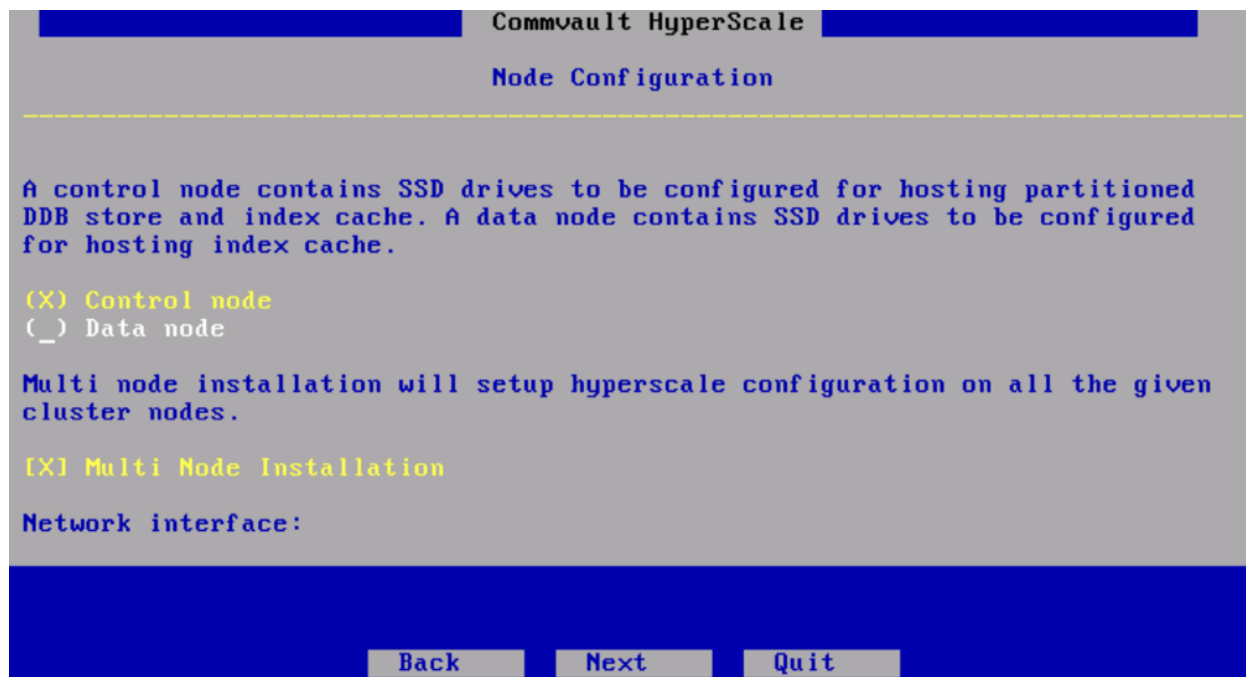


20. Select the option to Reinitialize Drives. Tab to select Next at the bottom, then press Enter.

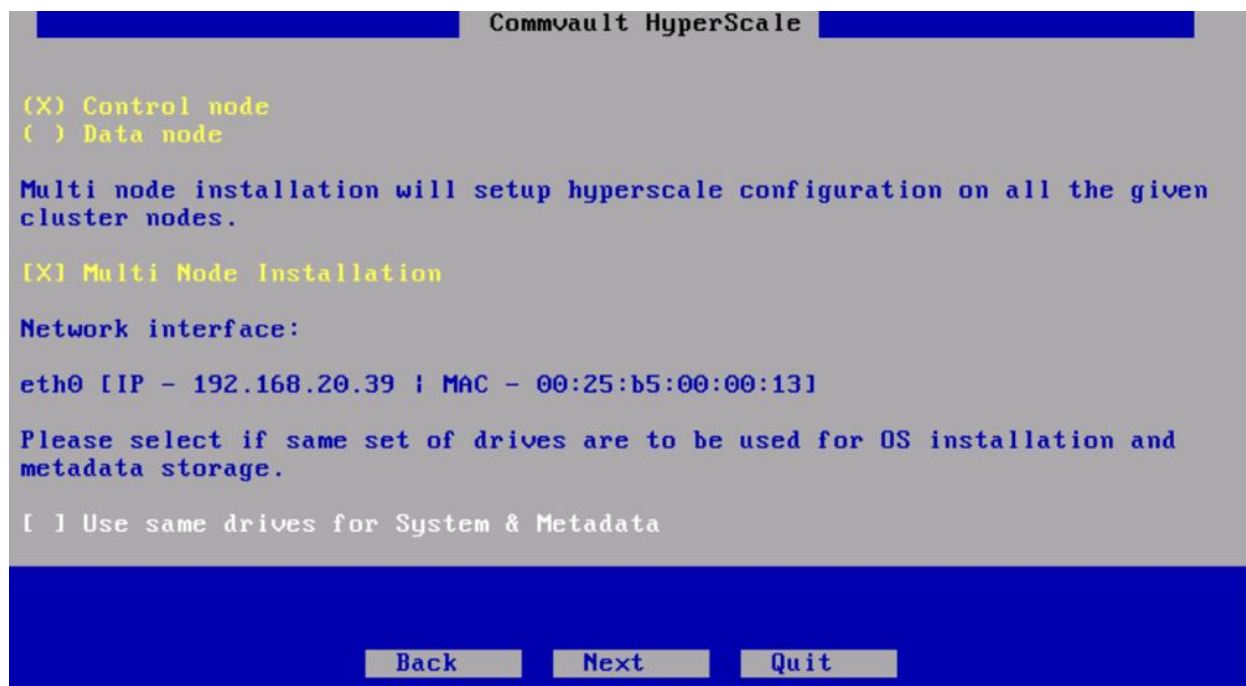


If DHCP is enabled in the environment, continue to step 21. If not, go to step 25.

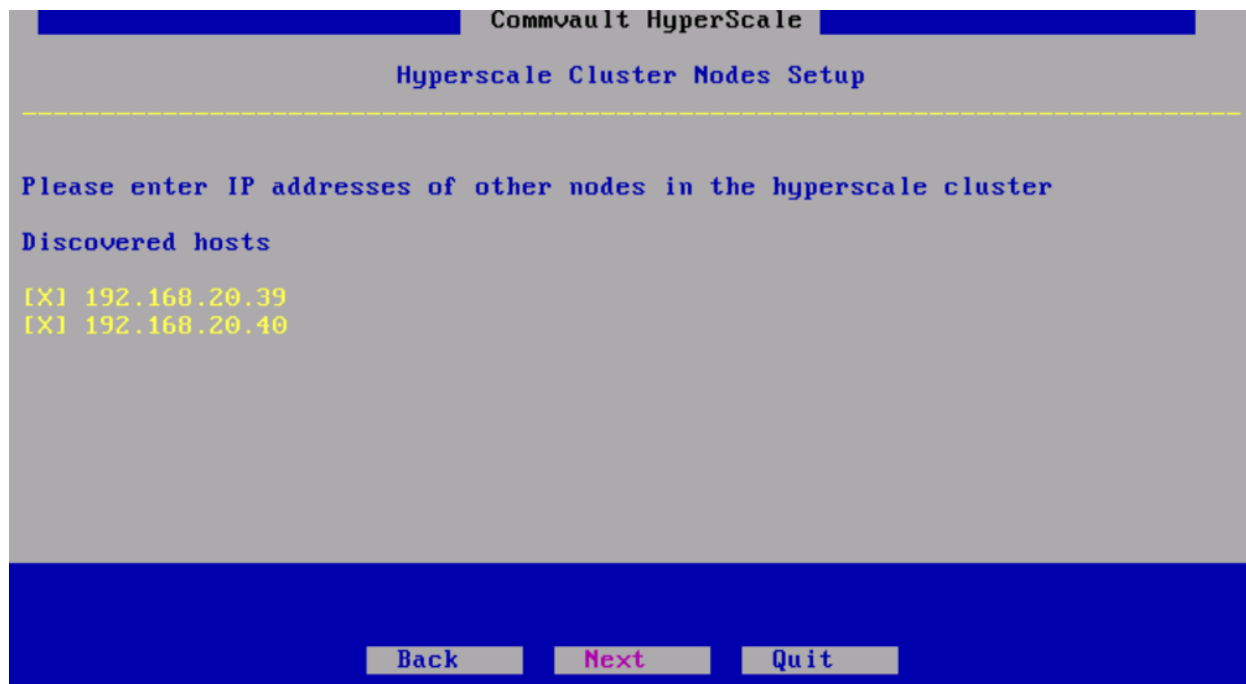
21. Select Control Node and select Multi Node Installation then press the Tab button to move down to Next. Before pressing Enter, see the next step.



22. When pressing Tab to move down, you will see the IP address which was assigned through DHCP and another option. DO NOT select Use Same drives for System & Metadata. DO NOT select Next or press Enter.



23. Start the installer repeating steps 3-22 on the remaining nodes until you get to the screen above. When they are all at the same screen, then you can continue on by selecting Next. It does not matter which host you select next on, it will detect the other hosts as shown below.



Commvault HyperScale

Hyperscale Cluster Nodes Setup

Please enter IP addresses of other nodes in the hyperscale cluster

Discovered hosts

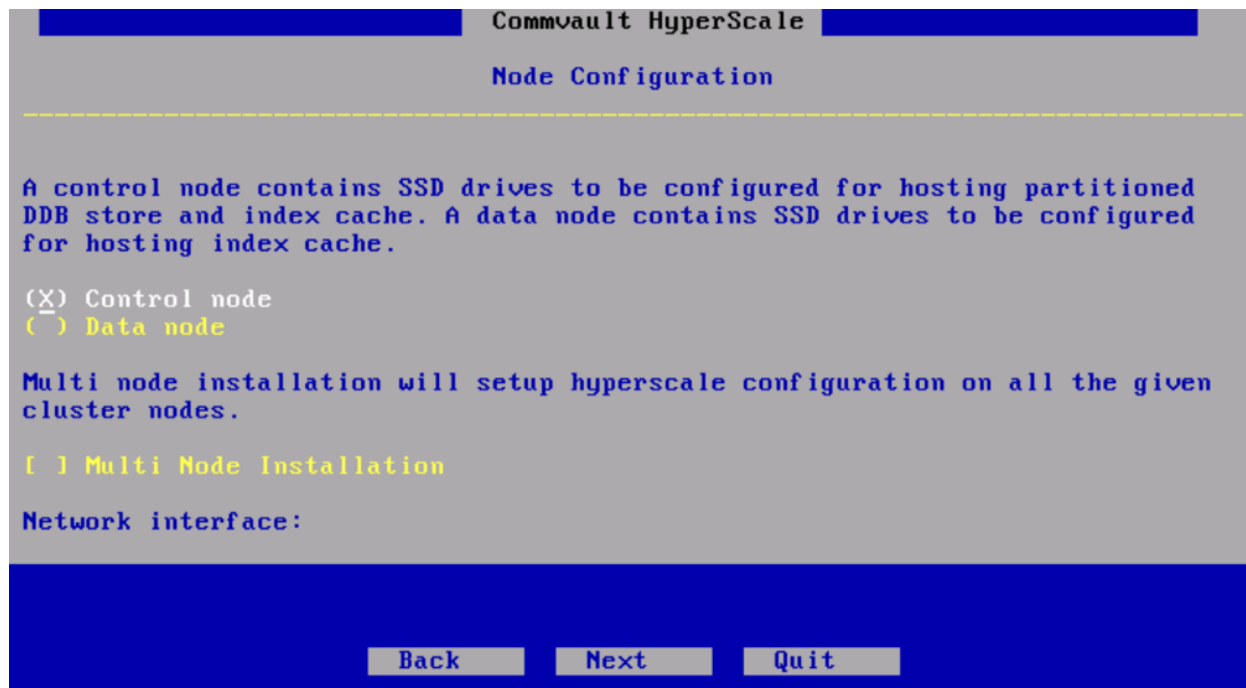
[X] 192.168.20.39
[X] 192.168.20.40

Back Next Quit



It does not matter which host you select Next on, it will detect the other hosts as shown below.

24. Stay on the same host from the previous step and sgokit to step 27.
25. Non Multi Node Install option continued (for example, no DHCP server is available), DO NOT select the Multi Node Installation option. Press the Tab button to move down to Next. Before pressing Enter, see the next step.



Commvault HyperScale

Node Configuration

A control node contains SSD drives to be configured for hosting partitioned DDB store and index cache. A data node contains SSD drives to be configured for hosting index cache.

(X) Control node
() Data node

Multi node installation will setup hyperscale configuration on all the given cluster nodes.

[] Multi Node Installation

Network interface:

Back Next Quit

26. When pressing Tab to move down you will see another option; DO NOT select Use Same drives for System & Metadata. Select Next and press Enter.

Commvault HyperScale

☒ Control node
☐ Data node

Multi node installation will setup hyperscale configuration on all the given cluster nodes.

☐ Multi Node Installation

Network interface:

Please select if same set of drives are to be used for OS installation and metadata storage.

☐ Use same drives for System & Metadata

Back **Next** **Quit**

27. On the System Drives screen, use the arrow keys to move down until Next appears in the bottom right corner, select Next.

Commvault HyperScale

System drives are used for Operating System installation.

Please select which of the following drives should be used as System drives.

☐ /dev/sda [type: sas | size: 5589G]
☐ /dev/sdb [type: sas | size: 5589G]
☐ /dev/sdc [type: sas | size: 5589G]
☐ /dev/sdd [type: sas | size: 5589G]
☐ /dev/sde [type: sas | size: 5589G]
☐ /dev/sdf [type: sas | size: 5589G]
☐ /dev/sdg [type: sas | size: 5589G]

1 / 4

Next

Back **Next** **Quit**

28. Repeat this process until you see the OS drive; in this case the 2 x 480GB Raid1 drives (446GB), and select it, then select Next and press enter.

Commvault HyperScale

System Drives

System drives are used for Operating System installation.

Please select which of the following drives should be used as System drives.

```

[ ] /dev/sdv [type: sas | size: 5589G]
[ ] /dev/sdw [type: sas | size: 5589G]
[ ] /dev/sdx [type: sas | size: 5589G]
[X] /dev/sdy [type: sas | size: 446G]
[ ] /dev/sdz [type: sas | size: 4467G]

```

4 / 4

Back
Next
Quit

29. On the Metadata Drives screen, use the arrow keys to move down until Next, select that Next.

Commvault HyperScale

Metadata drives are used for storing Deduplication Database and Index Cache.

Please select which of the following drives should be used as Metadata drives.

```

[ ] /dev/sda [type: sas | size: 5589G]
[ ] /dev/sdb [type: sas | size: 5589G]
[ ] /dev/sdc [type: sas | size: 5589G]
[ ] /dev/sdd [type: sas | size: 5589G]
[ ] /dev/sde [type: sas | size: 5589G]
[ ] /dev/sdf [type: sas | size: 5589G]
[ ] /dev/sdg [type: sas | size: 5589G]

```

1 / 4

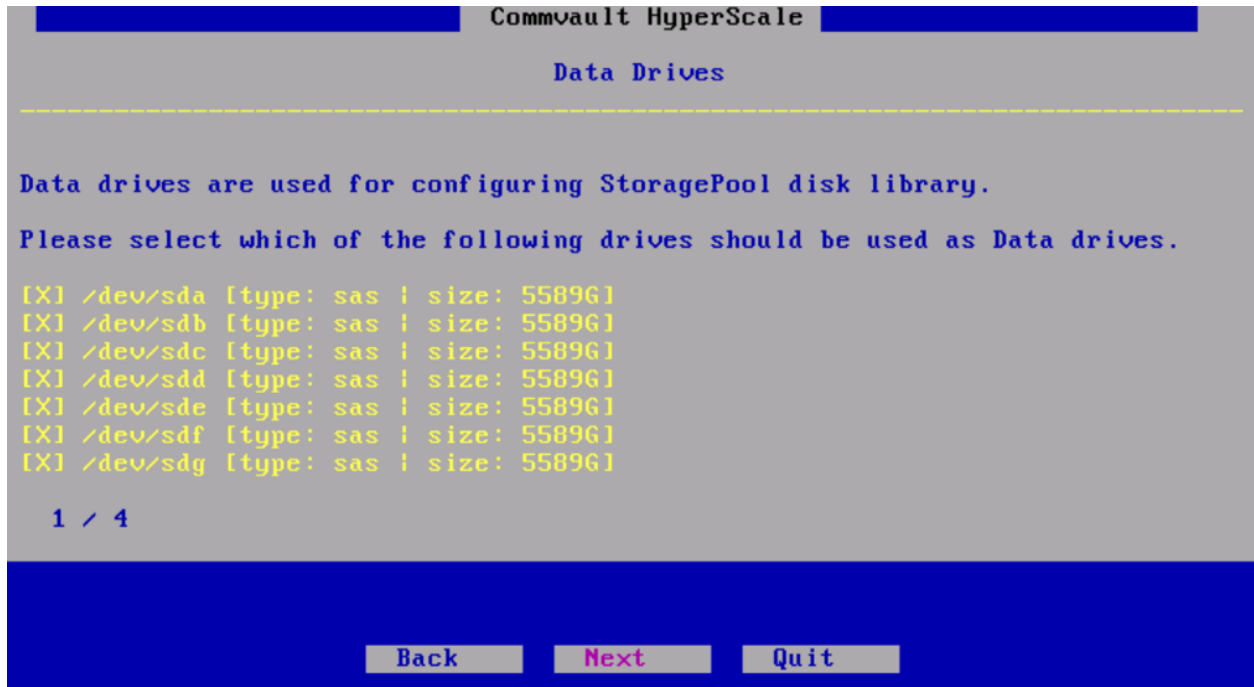
Next

Back
Next
Quit

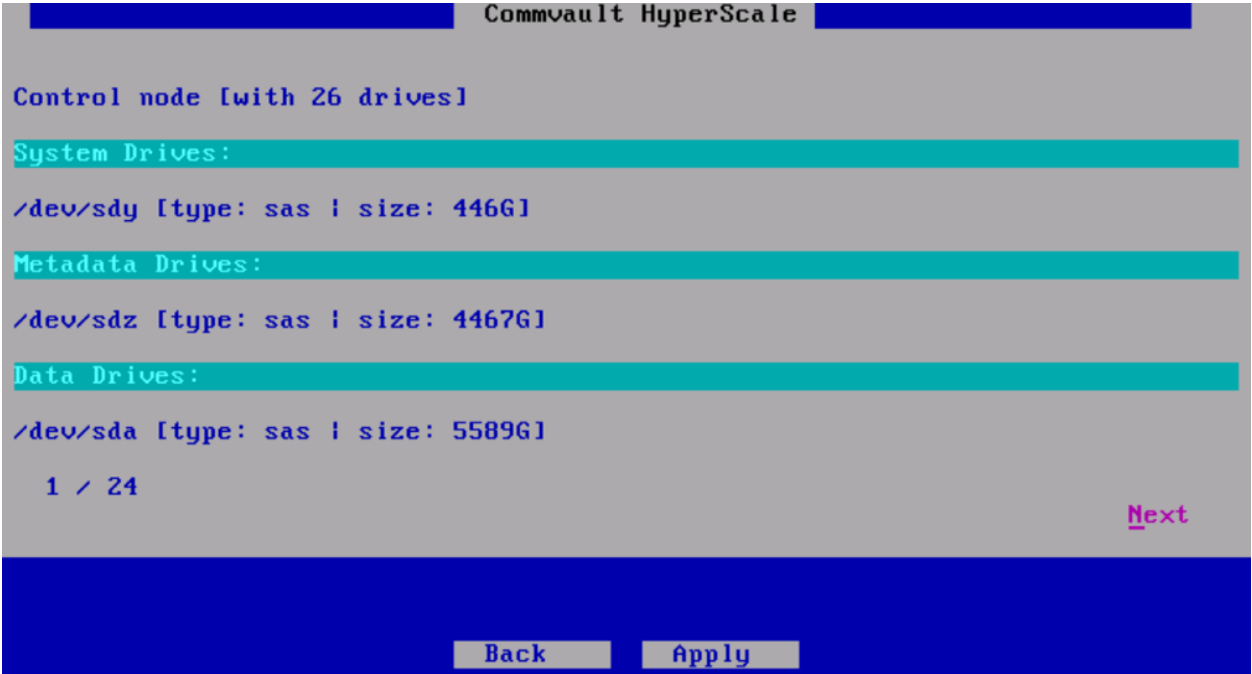
30. Repeat this process until you see the Metadata drive, in this case the 4 x 1.6TB Raid5 drives (4467GB), and select it, then select Next at the bottom and press Enter.



31. On the Data Drives screen, the remaining drives should be selected, press Tab to select Next, then press Enter.



32. On the last summary screen, the selected drives will be displayed. Press Tab and select Apply, then press Enter.



33. The Commvault HyperScale OS installation begins.

Figure 18 Install for the **Non Multi Node Installation** Option

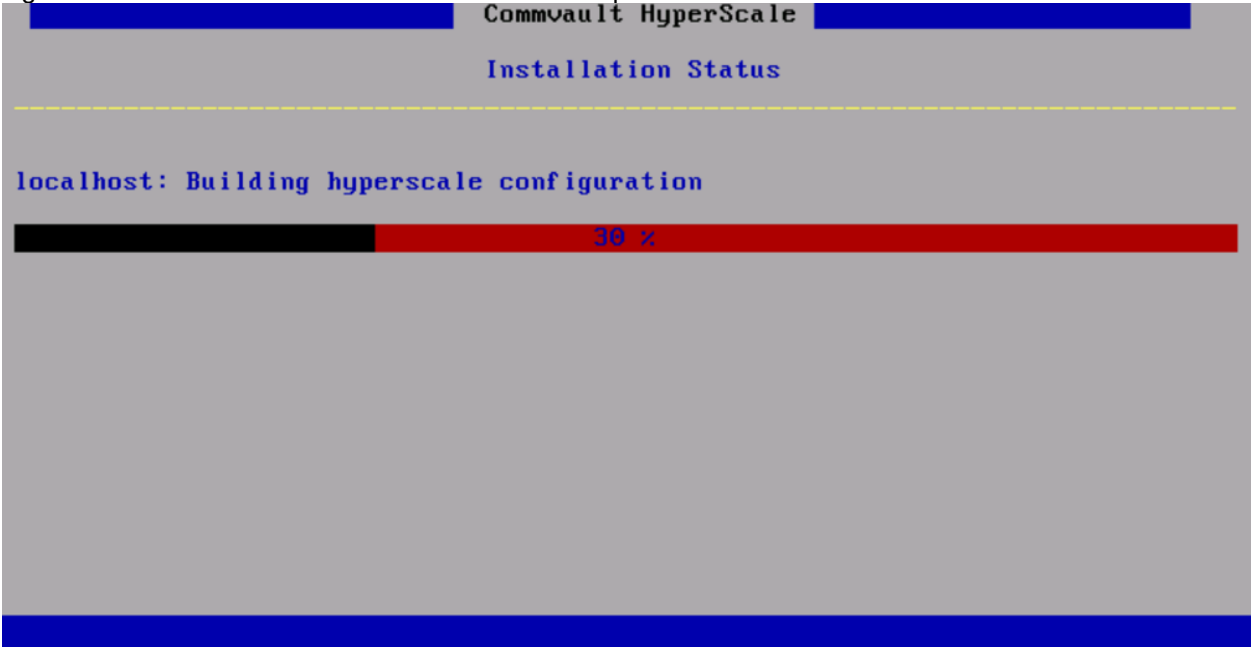
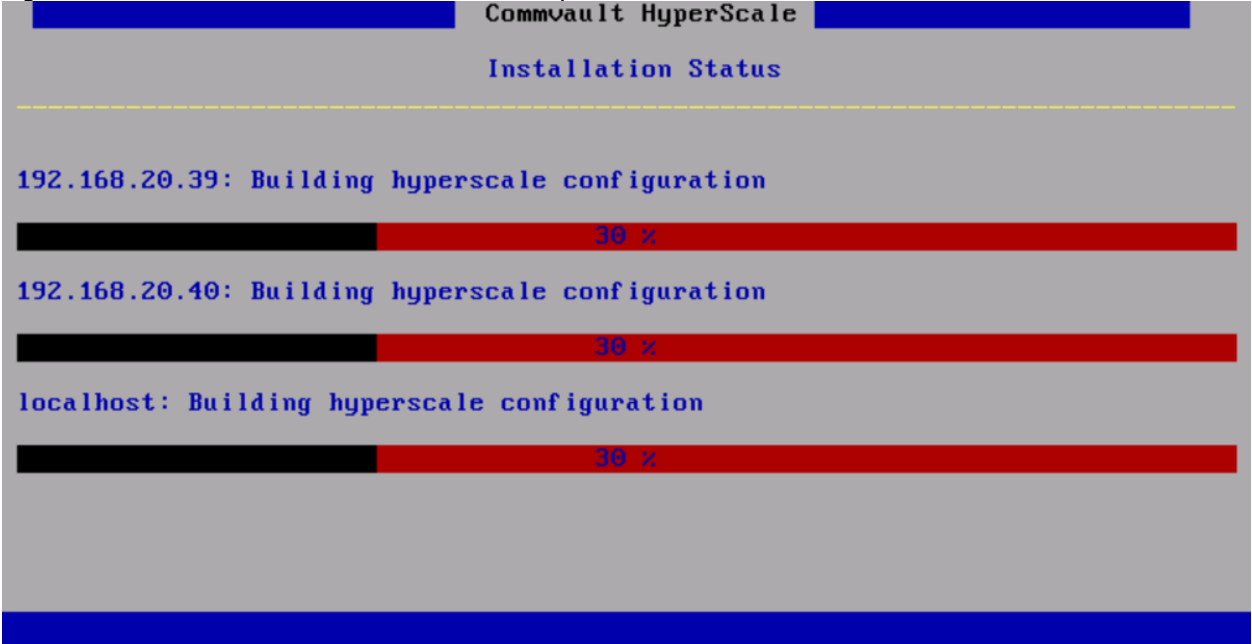


Figure 19 Install for the **Multi Node Installation** Option



34. The OS install is now complete, select Finish. Repeat the same steps on the remaining nodes before continuing to step 35.

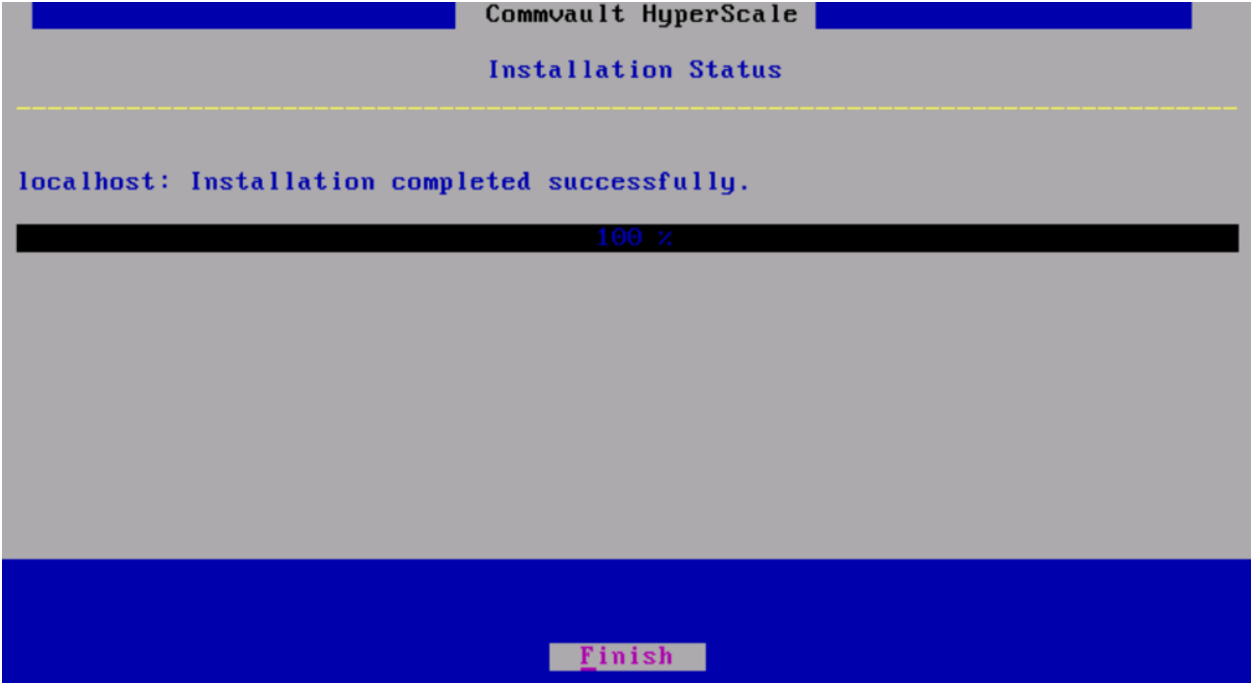
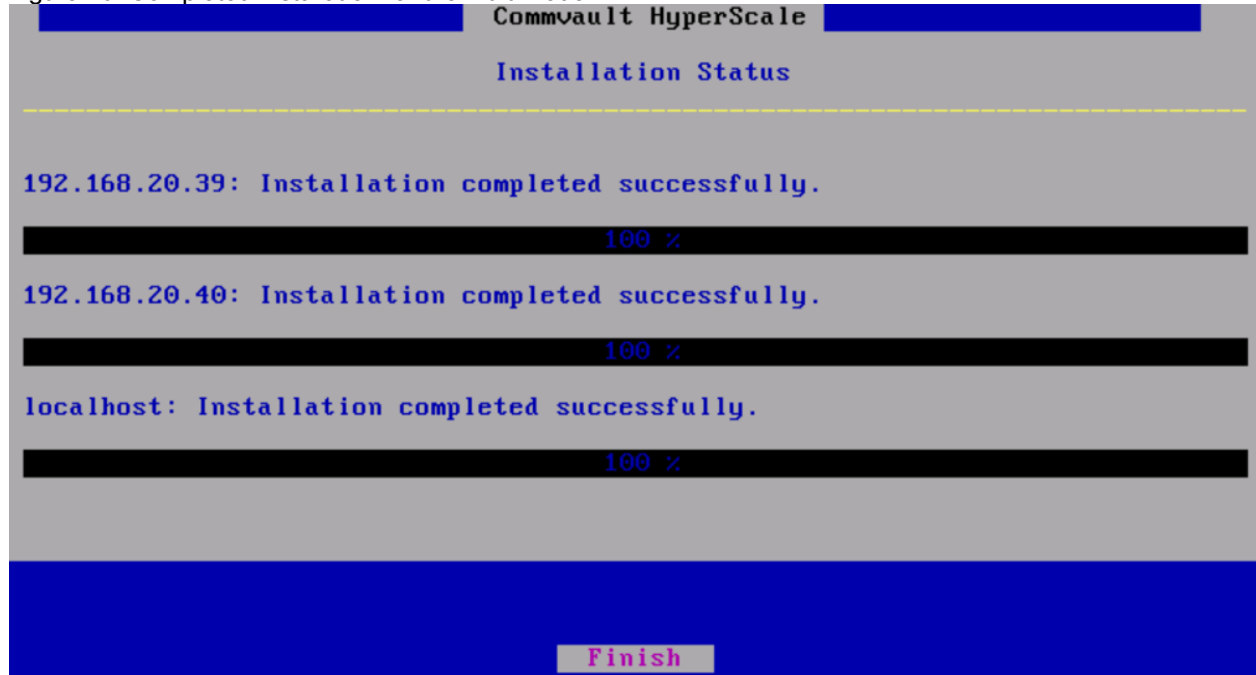


Figure 20 Completed Installation for the Multi Node



35. 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 Cisco UCS Manager, 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 you do not need to touch this one.

```

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

```

36. Type ifconfig, then press Enter to see the network interfaces. In this case they are enp63s0f0 and enp63s0f1 (lo is the loopback interface). Also note the MAC address for each interface beside the word ether (in our case 00:25:b5:00:00:14 and 00:25:b5:00:00:34).

```
[root@hsref network-scripts]# ifconfig
enp63s0f0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9000
    inet 192.168.20.42 netmask 255.255.255.0 broadcast 192.168.20.255
    inet6 fe80::225:b5ff:fe00:14 prefixlen 64 scopeid 0x20<link>
    ether 00:25:b5:00:00:14 txqueuelen 1000 (Ethernet)
    RX packets 216230 bytes 38597980 (36.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22713 bytes 7518241 (7.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp63s0f1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9000
    inet6 fe80::225:b5ff:fe00:34 prefixlen 64 scopeid 0x20<link>
    ether 00:25:b5:00:00:34 txqueuelen 1000 (Ethernet)
    RX packets 1321608 bytes 424751614 (405.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 605000 bytes 209327912 (199.6 MiB)
    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 1 (Local Loopback)
    RX packets 92 bytes 6784 (6.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 92 bytes 6784 (6.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@hsref network-scripts]#
```

37. 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 following example, it is `00:25:b5:00:00:14` which matches the interface `enp63s0f0` above, so this is the configuration file for that interface. This means that `ifcfg-hca2` is the configuration file for interface `enp63s0f1`, which can be verified by viewing that file with the `cat` command and looking at the MAC address in that file.

```
[root@hsref network-scripts]# cat ifcfg-hca1
TYPE=Ethernet
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
IPV6INIT=no
NM_CONTROLLED=no
HWADDR=00:25:b5:00:00:14
[root@hsref network-scripts]# _
```

38. Change the `ifcfg` files to match the interface names by using the `mv` command (for example, `mv ifcfg-hca1 ifcfg-enp63s0f0`). Use the `ls` command to verify.

```

[root@hsref network-scripts]# mv ifcfg-hca1 ifcfg-enp63s0f0
[root@hsref network-scripts]# mv ifcfg-hca2 ifcfg-enp63s0f1
[root@hsref network-scripts]# ls
ifcfg-enp63s0f0  ifdown-eth  ifdown-post  ifdown-TeamPort  ifup-eth  ifup-plip  ifup-sit  init.ipv6-global
ifcfg-enp63s0f1  ifdown-ib   ifdown-ppp   ifdown-tunnel    ifup-ib   ifup-plusb  ifup-Team  network-functions
ifcfg-lo        ifdown-ippp ifdown-routes ifup              ifup-ippp ifup-post   ifup-TeamPort network-functions-ipv6
ifdown         ifdown-ipv6 ifdown-sit   ifup-aliases     ifup-ipv6 ifup-ppp    ifup-tunnel
ifdown-bnep    ifdown-isdn ifdown-Team  ifup-bnep        ifup-isdn ifup-routes ifup-wireless
[root@hsref network-scripts]#

```

39. Modify the ifcfg-enp63s0f0 file as shown 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=enp63s0f0
TYPE=Ethernet
ONBOOT=yes
BOOTPROTO=static
USERCTL=no
IPV6INIT=no
NM_CONTROLLED=no
IPADDR=192.168.20.102
NETMASK=255.255.255.0
GATEWAY=192.168.20.1
DNS1=192.168.20.219
HWADDR=00:25:b5:00:00:14

```

40. Modify the ifcfg-enp63s0f1 file as shown 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=enp63s0f1
TYPE=Ethernet
ONBOOT=yes
BOOTPROTO=static
USERCTL=no
IPV6INIT=no
NM_CONTROLLED=no
IPADDR=10.10.10.1
NETMASK=255.255.255.0
HWADDR=00:25:b5:00:00:34

```

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

```

[root@hsref network-scripts]# ls
ifcfg-enp63s0f0  ifdown-eth  ifdown-post  ifdown-TeamPort  ifup-eth  ifup-plip  ifup-sit  init.ipv6-global
ifcfg-enp63s0f1  ifdown-ib   ifdown-ppp   ifdown-tunnel    ifup-ib   ifup-plusb  ifup-Team  network-functions
ifcfg-lo        ifdown-ippp ifdown-routes ifup              ifup-ippp ifup-post   ifup-TeamPort network-functions-ipv6
ifdown         ifdown-ipv6 ifdown-sit   ifup-aliases     ifup-ipv6 ifup-ppp    ifup-tunnel
ifdown-bnep    ifdown-isdn ifdown-Team  ifup-bnep        ifup-isdn ifup-routes ifup-wireless
[root@hsref network-scripts]# systemctl restart network
[root@hsref network-scripts]#

```

42. Type ifconfig to verify the IP addresses are assigned to the interfaces.

```
[root@hsref network-scripts]# ifconfig
enp63s0f0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9000
    inet 192.168.20.102 netmask 255.255.255.0 broadcast 192.168.20.255
    inet6 fe80::225:b5ff:fe00:14 prefixlen 64 scopeid 0x20<link>
    ether 00:25:b5:00:00:14 txqueuelen 1000 (Ethernet)
    RX packets 222982 bytes 39410144 (37.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22798 bytes 7527945 (7.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp63s0f1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9000
    inet 10.10.10.1 netmask 255.255.255.0 broadcast 10.10.10.255
    inet6 fe80::225:b5ff:fe00:34 prefixlen 64 scopeid 0x20<link>
    ether 00:25:b5:00:00:34 txqueuelen 1000 (Ethernet)
    RX packets 1326517 bytes 425119837 (405.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 605086 bytes 209338243 (199.6 MiB)
    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 1 (Local Loopback)
    RX packets 92 bytes 6784 (6.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 92 bytes 6784 (6.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@hsref network-scripts]#
```

43. Repeat steps 35-42 on the remaining nodes.

44. Login and change the directory to /opt/commvault/MediaAgent and type the following command ./setupsds.

```
[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.tml  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  cvhconfig.py          cvremotenwconfig.py  IndexCache             setupsds
compressor           cv_hs_auto_nwconf.py  cvrestartinstall.py  indexRestore           setupsds.tml
createcd.py          cvhyperscale          cvsetuphelper.py     init                  SynthFull
createcd.sh          cvhyperscale_install.py  cvsetuphname.py     init.py                test_cmd
createIndex          CJobReplicator        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      cvmgmtwizard.py       cvupdate_avahi.sh    libGifsPbba.so         uncompressor
cvavahi.py           cvmkavahi.py          diskui.py             lvm.conf               updateIndex
cvchroot.sh          cvmonitor.py          dmWriter              MediaLabelReader       utils.py
cvcInwmgmt.py        CMountd               dsBackup              modeui.py              utils.pyc
cvcInw.py            CUNasFileScan         dsRestore             NasBackup              wrappers.py
cvcloudinit.sh       CUNasSnapBackup       efiboot.img           NASCreateIndex         wrappers.pyc
cvcluster.py          CUNasSnapRestore     efiboot.sh            nasRestore
cvconfigcleanup.py   CUNdmpRemoteServer   filter_drives.py      nwconfig.py
cvconfignw.py         CUNdmpSynthRemoteServer  FsIndexedRestore     nwintfx.py

[root@hsref MediaAgent]# ./setupsds_
```


45. 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.

```

HyperScale Reference Architecture SP13 11/19/2018

Please set the hostname and root user password of the server.

Hostname of the server      s3260node1.dmzlab.cisco.com
Root password              *****
Retype root password       *****

< OK >      < Cancel >

```

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

```

HyperScale Reference Architecture SP13 11/19/2018

Please select setup button to get to network configuration menu.

Only static IP address assignment is supported. For DHCP assigned IP address please select skip button to directly get to
CommServe provisioning menu.

To skip network configuration and directly get to CommServe provisioning menu please select skip button.

< Setup >      < Skip >

```

47. Enter the CommServe information, then select OK.

```

HyperScale Reference Architecture SP13 11/19/2018

The appliance will be registered with the CommServe.
Please provide the following information:

CommServe Hostname      commserve.dmzlab.cisco.com
CommServe User Name     admin
CommServe Password      *****

< OK >      < Cancel >

```

48. The server is now registered with the CommServe.

```

MediaAgent : s3260node1.dmzlab.cisco.com
CommServer : commserve.dmzlab.cisco.com
Successfully registered MediaAgent s3260node1.dmzlab.cisco.com with CommServe commserve.dmzlab.cisco.com
Successfully restarted commvault services
Commvault HyperScale has been configured successfully!. For better security, please change the root password periodically.
[root@hsref MediaAgent]# _

```

49. Commvault appends a suffix of "sds" to the node names, for example our name of S3260NODE1.dmzlab.cisco.com will use S3260NODE1SDS.dmzlab.cisco.com for the intercluster communication. Put these intercluster names into the hosts file on each server.

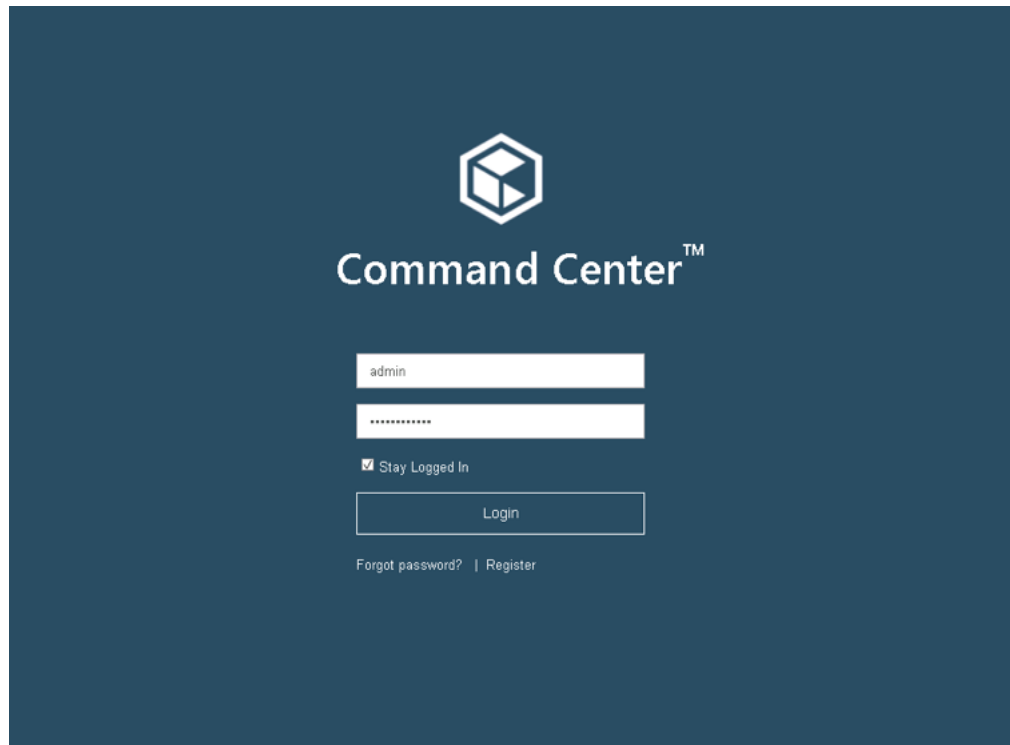
```

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
10.10.10.1 s3260node1sds.dmzlab.cisco.com s3260node1sds
10.10.10.2 s3260node2sds.dmzlab.cisco.com s3260node2sds
10.10.10.4 s3260node3sds.dmzlab.cisco.com s3260node3sds

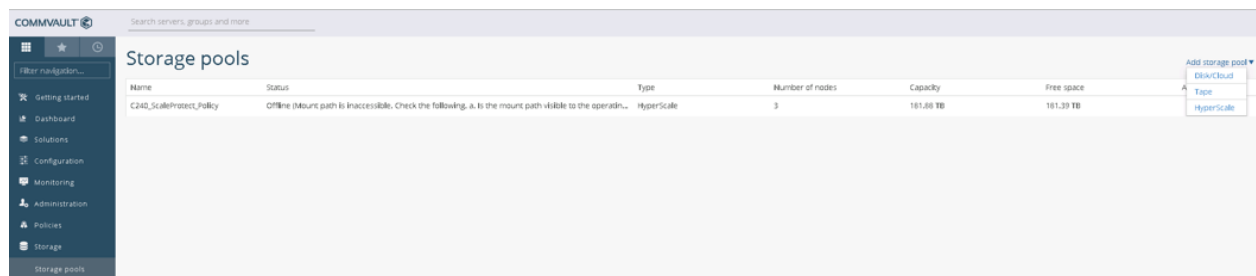
```

50. Repeat these steps on the remaining nodes.

51. Once the final node has completed successfully, log into the Command Center to complete the installation.




52. In the left pane, click Storage, then click Storage pools, click Add storage pool and select HyperScale.



53. On the Create HyperScale storage pool page, enter a name for the pool, select the Resiliency/Redundancy factor:

- 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.



If installing 3 nodes, always select Standard. If installing 6 nodes, choose Medium or High. Select the nodes to be part of a pool, then click Configure.

Create HyperScale storage pool

Name

SS260HyperScale-Pool

Configure storage

Resiliency / Redundancy

Standard

Medium

High

Nodes

None Selected

Select All

Select None

s3260node1.dmtab.cllice.com

s3260node2.dmtab.cllice.com

s3260node3.dmtab.cllice.com

54. The Storage Pool is created. It may display as Offline with 0 capacity for a few minutes since there is a background process that runs, creating the cluster 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.

Storage pools

Name	Status	Type	Number of nodes	Capacity	Free space
C240_ScaleProtect_Policy	Offline (Mount path is inaccessible. Check ...	Scale-out	3	161.68 TB	161.39 TB
SS260HyperScale-Pool	Scale-out storage pool creation is in progres...	Scale-out	3	0 Bytes	0 Bytes

Now the Commvault HyperScale setup is complete and ready for backup.

Validation




This section provides a list of items that should be reviewed after the ScaleProtect system has been deployed and configured. The objective of this section is to verify the configuration and functionality of the solution and ensure that the configuration supports core availability requirements.

Post Install Checklist

The following tests are critical to functionality of the solution, and should be verified before deploying for production:

- Verify the expected number of storage nodes are members of the HyperScale cluster.

Nodes

Node	Status
 s3260node1.dmzlab.cisco.com	Online
 s3260node2.dmzlab.cisco.com	Online
 s3260node3.dmzlab.cisco.com	Online

- Verify the expected storage pool capacity is seen in the Commvault CommServe GUI:

Storage pools

Name	Status	Type	Number of nodes	Capacity
S3260HyperScale-Pool	Online	HyperScale	3	261.89 TB

- Perform test backup and make sure the storage pool is accessible to read/write data.

Verify Redundancy

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.

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 Cisco 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.

Bryan Clarke, Technical Alliances Architect, Commvault Systems, Inc.

Bryan Clarke is a Product Technical Architect in the Commvault Product Management Group. Bryan has worked in IT since 1995 after completing a Computer Engineering degree. He has started in IT in the data center managing and supporting Windows systems. He has a deep background in data protection, information security, information life-cycle management, DR, business continuity, compliance and cloud strategies. Bryan has been working with Commvault software for the past 16 years and holds several Commvault certifications.

Acknowledgements

- Ulrich Kleidon, Cisco Systems, Inc.
- Jonathan Howard, Commvault Systems, Inc.
- Nivas Iyer, Cisco Systems, Inc.