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: February 14, 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:


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

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

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, CCD, 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, Networker, 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 .................................................................................................................................................. 10  
  Software Revisions .................................................................................................................................................... 10  
  Configuration Guidelines ............................................................................................................................................ 10  
  Physical Infrastructure .................................................................................................................................................. 12  
  Cisco UCS Connectivity to Nexus Switches ...................................................................................................................... 12  
    Optional: Cisco UCS Connectivity to SAN Fabrics ........................................................................................................... 13  
Network Switch Configuration ....................................................................................................................................... 15  
  ScaleProtect Implementation ...................................................................................................................................... 15  
  Configure Cisco Nexus 9000 Switches ............................................................................................................................... 15  
    Cisco Nexus 9000 Initial Configuration Setup .............................................................................................................. 16  
  Enable Appropriate Cisco Nexus 9000 Features and Settings ....................................................................................... 18  
    Cisco Nexus 9000 A and Cisco Nexus 9000 B .................................................................................................................. 18  
  Create VLANs for ScaleProtect IP Traffic ........................................................................................................................ 18  
    Cisco Nexus 9000 A and Cisco Nexus 9000 B .................................................................................................................. 18  
  Configure Virtual Port Channel Domain .......................................................................................................................... 19  
    Cisco Nexus 9000 A ...................................................................................................................................................... 19  
    Cisco Nexus 9000 B ...................................................................................................................................................... 19  
  Configure Network Interfaces for the vPC Peer Links ..................................................................................................... 20  
    Cisco Nexus 9000 A ...................................................................................................................................................... 20  
    Cisco Nexus 9000 B ...................................................................................................................................................... 21  
  Configure Network Interfaces to Cisco UCS Fabric Interconnect .................................................................................. 21  
    Cisco Nexus 9000 A ...................................................................................................................................................... 21  
    Cisco Nexus 9000 B ...................................................................................................................................................... 23  
  Uplink into Existing Network Infrastructure ................................................................................................................ 25  
    Cisco Nexus 9000 A and B using Port Channel Example ............................................................................................... 25  
Cisco UCS Server Configuration .................................................................................................................................. 27  
  Cisco UCS Base Configuration .................................................................................................................................. 27  
    Perform Initial Setup of Cisco UCS 6332-16UP Fabric Interconnects ........................................................................... 27  
Cisco UCS Setup .......................................................................................................................................................... 30
Log into Cisco UCS Manager .......................................................................................................................... 30
Upgrade Cisco UCS Manager Software to Version 4.0(1a) .................................................................................. 30
Anonymous Reporting ......................................................................................................................................... 30
Configure Cisco UCS Call Home .......................................................................................................................... 31
Add Block IP Addresses for KVM Access ............................................................................................................. 31
Synchronize Cisco UCS to NTP .............................................................................................................................. 32
Edit Chassis Discovery Policy ................................................................................................................................ 33
Enable Server Ports ............................................................................................................................................... 34
Optional: Edit Policy to Automatically Discover Server Ports ........................................................................... 35
Server Discovery ................................................................................................................................................... 36
Optional: Enable Fibre Channel Ports .................................................................................................................... 36
Optional: Create VSAN for the Fibre Channel Interfaces ....................................................................................... 38
Optional: Create Port Channels for the Fibre Channel Interfaces ........................................................................ 42
Enable Ethernet Uplink Ports ................................................................................................................................ 44
Create Port Channels for Ethernet Uplinks ........................................................................................................... 45
Cisco UCS S3260 Storage Server Configuration ................................................................................................. 48
Create Sub-Organization ...................................................................................................................................... 49
Create MAC Address Pools ................................................................................................................................... 49
Create UUID Suffix Pool ....................................................................................................................................... 53
Create Server Pool ............................................................................................................................................... 54
Optional: Create a WWNN Address Pool for FC-based Storage Access ............................................................. 57
Optional: Create a WWPN Address Pools for FC Based Storage Access ............................................................ 58
Create VLANs ...................................................................................................................................................... 61
Create Host Firmware Package ............................................................................................................................. 63
Create Network Control Policy for Cisco Discovery Protocol ............................................................................. 64
Create Power Control Policy ................................................................................................................................ 65
Create Server BIOS Policy .................................................................................................................................. 66
Create Maintenance Policy .................................................................................................................................. 68
Create Adapter Policy .......................................................................................................................................... 69
Create vNIC Templates .......................................................................................................................................... 70
Create LAN Connectivity Policy ........................................................................................................................... 76
Optional: Create vHBA Templates for FC Connectivity ....................................................................................... 80
Optional: Create FC SAN Connectivity Policies ................................................................................................ 84
Cisco UCS S3260 Chassis Setup ............................................................................................................................ 90
Chassis Profile Template ...................................................................................................................................... 90
Create Chassis Firmware Packages ..................................................................................................................... 91
Create maintenance Policy ................................................................................................................................... 92
Create Disk Zoning Policy ........................................................................................................................................... 92
Create Chassis Profile Template ..................................................................................................................................... 97
Create Chassis Profile(s) from Template .......................................................................................................................... 99
Associate Chassis Profile to S3260 Chassis ....................................................................................................................... 100
Cisco UCS S3260 Server Node Setup ............................................................................................................................ 103
  LUN Cleanup.................................................................................................................................................................. 103
  Setting S3260 Disk to Unconfigured Good...................................................................................................................... 103
Cisco UCS S3260 Storage Profile ..................................................................................................................................... 104
Create Disk Group Policies ............................................................................................................................................... 104
Create Storage Profile ......................................................................................................................................................... 113
Create Boot Policy .............................................................................................................................................................. 122
Cisco UCS S3260 Service Profile Template ........................................................................................................................ 124
Create Service Profile Template ....................................................................................................................................... 124
Create Service Profiles ....................................................................................................................................................... 139
Commvault HyperScale Installation and Configuration ....................................................................................................... 143
  Validation.......................................................................................................................................................................... 162
  Post Install Checklist ......................................................................................................................................................... 162
  Verify Redundancy............................................................................................................................................................ 163
About the Authors................................................................................................................................................................. 164
Acknowledgements............................................................................................................................................................ 164
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:


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.
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.
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>
<thead>
<tr>
<th>Layer</th>
<th>Device</th>
<th>Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute</td>
<td>Cisco UCS 6300 Series Fabric Interconnects</td>
<td>4.0(1a)</td>
</tr>
<tr>
<td></td>
<td>Cisco UCS S3260 Storage Server</td>
<td>4.0(1a)</td>
</tr>
<tr>
<td>Network</td>
<td>Cisco Nexus 9332PQ NX-OS</td>
<td>9.2(1)</td>
</tr>
<tr>
<td>Software</td>
<td>Cisco UCS Manager</td>
<td>4.0(1a)</td>
</tr>
<tr>
<td></td>
<td>Commvault Complete Backup and Recovery</td>
<td>v11 Service Pack 13</td>
</tr>
<tr>
<td></td>
<td>Commvault HyperScale Software</td>
<td>v11 Service Pack 13</td>
</tr>
</tbody>
</table>

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

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

> 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

<table>
<thead>
<tr>
<th>VSAN Name</th>
<th>VSAN</th>
<th>VSAN Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup-VSAN-A</td>
<td>201</td>
<td>Fabric-A VSAN for connectivity to data protection devices.</td>
</tr>
<tr>
<td>Backup-VSAN-B</td>
<td>202</td>
<td>Fabric-B VSAN for connectivity to data protection devices.</td>
</tr>
<tr>
<td>Prod-VSAN-A</td>
<td>102</td>
<td>Fabric-A VSAN for connectivity to production SAN Fabrics.</td>
</tr>
<tr>
<td>Prod-VSAN-B</td>
<td>101</td>
<td>Fabric-B VSAN for connectivity to production SAN Fabrics.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Network</th>
<th>Subnet Mask</th>
<th>Gateway</th>
</tr>
</thead>
</table>

### Table 5  Out of Band IP Address Details

<table>
<thead>
<tr>
<th>Device</th>
<th>Hostname</th>
<th>Management IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nexus 9k Switch A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nexus 9k Switch B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCS Fabric Interconnect 6300 A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCS Fabric Interconnect 6300 B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCS Cluster VIP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 6  HyperScale IP Address Details

<table>
<thead>
<tr>
<th>Device</th>
<th>Hostname</th>
<th>Data Protection / Management IP Address</th>
<th>Cluster IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>HyperScale Node1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HyperScale Node2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS Fabric Interconnect A</td>
<td>Eth1/17</td>
<td>40GbE</td>
<td>Cisco UCS S3260 Chassis1 SIOC-1</td>
<td>VIC Port 0</td>
</tr>
<tr>
<td>Cisco UCS Fabric Interconnect A</td>
<td>Eth1/18</td>
<td>40GbE</td>
<td>Cisco UCS S3260 Chassis1 SIOC-2</td>
<td>VIC Port 0</td>
</tr>
<tr>
<td>Cisco UCS Fabric Interconnect A</td>
<td>Eth1/19</td>
<td>40GbE</td>
<td>Cisco UCS S3260 Chassis2 SIOC-1</td>
<td>VIC Port 0</td>
</tr>
<tr>
<td>Cisco UCS Fabric Interconnect B</td>
<td>Eth1/17</td>
<td>40GbE</td>
<td>Cisco UCS S3260 Chassis1 SIOC-1</td>
<td>VIC Port 1</td>
</tr>
</tbody>
</table>
### 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

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS Fabric Interconnect A</td>
<td>FC1/1</td>
<td>16Gbps</td>
<td>Cisco MDS 9396S A</td>
<td>FC1/1</td>
</tr>
<tr>
<td>Cisco UCS Fabric Interconnect A</td>
<td>FC1/2</td>
<td>16Gbps</td>
<td>Cisco MDS 9396S A</td>
<td>FC1/2</td>
</tr>
<tr>
<td>Cisco UCS Fabric Interconnect B</td>
<td>FC1/1</td>
<td>16Gbps</td>
<td>Cisco MDS 9396S B</td>
<td>FC1/1</td>
</tr>
<tr>
<td>Cisco UCS Fabric Interconnect B</td>
<td>FC1/2</td>
<td>16Gbps</td>
<td>Cisco MDS 9396S B</td>
<td>FC1/2</td>
</tr>
</tbody>
</table>
ScaleProtect Implementation

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

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.
Cisco Nexus 9000 Initial Configuration Setup

This section explains 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:

1. Abort Power on Auto Provisioning and continue with normal setup? (yes/no) [n]: yes
2. 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>
3. 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
   ```
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:

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
   ```

⚠️ 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.
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

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=255.255.255.0
- 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:
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.
3. Right-click IP Pool ext-mgmt and select Create Block of IPv4 Addresses.
4. Enter the starting IP address of the block, the number of IP addresses required, and the subnet and gateway information.
5. Click OK to create.
6. Click OK in the confirmation message.

**Synchronize Cisco UCS to NTP**

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

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

3. In the Properties pane, select the appropriate time zone in the Timezone menu.
4. Click Save Changes and then click OK.
5. Click Add NTP Server.
6. Enter <NTP Server IP Address> and click OK.
Cisco UCS Server Configuration

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:

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.

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.
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:

5. Click Save Changes.

6. Click OK.
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.

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.
5. Click Save Changes.
6. Click OK.
The first discovery process can take some time and is dependent on installed firmware on the chassis.

Server Discovery

As previously described, when the server ports of the Fabric Interconnects are configured and active, the servers connected to those ports will begin a discovery process. During discovery the servers’ internal hardware inventories are collected, along with their current firmware revisions. Before continuing with the Cisco UCS 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:

1. 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.

2. Click the Chassis > Chassis1 Tab and view the Chassis status in the Overall Status column.

3. When the chassis is discovered, the Cisco UCS S3260 storage server is displayed as shown below:

4. 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:

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.

2. Slide the lever to change the ports 1–6 to Fiber Channel. Click Finish followed by Yes to the reboot message. Click OK.
3. When the subordinate has completed reboot, repeat the procedure to configure FC ports on primary Fabric Interconnect. As before, the Fabric Interconnect will reboot after the configuration is complete.

Optional: Create VSAN for the Fibre Channel Interfaces

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:

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

7. Click each port from Fabric Interconnect A that will participate in the port channel and click the >> button to add them to the port channel.
8. Click Finish.

9. Click OK.

10. Under LAN > LAN Cloud, click to expand the Fabric B tree.

11. Right-click Port Channels underneath Fabric B and select Create Port Channel.

12. Enter the port channel ID number as the unique ID of the port channel, (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.

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 facilitate 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.

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.

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

13. Click Finish.

14. In the confirmation message, click OK.

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

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

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

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

19. Select Sequential as the option for Assignment Order.
20. Click Next.

21. Click Add.

22. Specify a starting MAC address.

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

23. Specify a size for the MAC address pool that is sufficient to support the future ScaleProtect cluster expansion and any available blade or server resources.
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-O rganizations > CV-ScaleProtect.
3. Right-click UUID Suffix Pools.
4. Select Create UUID Suffix Pool.
5. Enter UUID_Pool as the name of the UUID suffix pool.
6. Optional: Enter a description for the UUID suffix pool.
7. Keep the prefix at the derived option.
8. Select Sequential for the Assignment Order.
9. Click Next.
10. Click Add to add a block of UUIDs.
11. Keep the value in From field at the default setting.
12. Specify a size for the UUID block that is sufficient to support the available server resources.
13. Click OK.

14. Click Finish.

15. Click OK.

Create Server Pool

The following procedure 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.
7. Click Next.

8. Select S3260 first server nodes from the two chassis and click >> to add them to the CVLT_SP_Pool_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.
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.

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.

7. Click Add.

8. Specify a starting WWPN address.

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

9. Specify a size for the WWPN address pool that is sufficient to support the available blade or rack server resources. Each server’s Fabric A vHBA will receive one WWPN from this pool.
10. Click OK and click Finish.

11. In the confirmation message, click OK.

12. Right-click WWPN Pools under the root organization and choose Create WWPN Pool to create the second WWPN address pool.

13. Enter WWPN-Pool-B as the name of the WWPN pool.

14. Optional: Enter a description for the WWPN pool.

15. Select the Sequential Assignment Order and click Next.

16. Click Add.

17. Specify a starting WWPN address.

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

18. Specify a size for the WWPN address pool that is sufficient to support the available blade or rack server resources. Each server’s Fabric B vHBA will receive one WWPN from this pool.
19. Click OK and click Finish.

20. In the confirmation message, click OK.

Create VLANs

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

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select LAN > LAN Cloud.
3. Right-click VLANs.
4. Select Create VLANs.
5. Enter Data_VLAN as the name of the VLAN to be used for the native VLAN.
6. Keep the Common/Global option selected for the scope of the VLAN.
7. Keep the Sharing Type as None.
8. Click OK and then click OK again.

9. Repeat Step 3-8 to add Cluster VLAN as shown in the figure below:
Create Host Firmware Package

Firmware management policies allow the administrator to select the corresponding packages for a given server configuration. These policies often include packages for adapter, BIOS, board controller, FC adapters, host bus adapter (HBA) option ROM, and storage controller properties.

To create a firmware management policy for a given server configuration in the Cisco UCS environment, follow these steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root > Sub-Organizations > CV-ScaleProtect.
3. Expand Host Firmware Packages.
4. Right-click and Select Create Host Firmware Package.
5. Enter name as CV_SP_Firmware
6. Select the version 4.0(1a)C for Rack Packages.
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.
4. Select Create Network Control Policy.
5. Enter ScaleProtect_NCP as the policy name.
6. For CDP, select the Enabled option.
7. Click OK to create the network control policy.
Create Power Control Policy

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

1. In Cisco UCS Manager, click the Servers tab in the navigation pane. Select Policies > root >Sub-Orga-
nizations > CV-ScaleProtect.
3. Select Create Power Control Policy.
4. Enter No-Power-Cap as the power control policy name.
5. Change the power capping setting to No Cap.
6. Click OK to create the power control policy.
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.
4. Select Create BIOS Policy.
5. Enter SP-S3260-BIOS as the BIOS policy name.

7. Click OK.
Cisco UCS Server Configuration

Create BIOS Policy

Name : SP-S3260-BIOS

Description : 

Reboot on BIOS Settings Change : 

6. Click OK.

7. Select the newly created BIOS Policy.

8. Change the Quiet Boot setting to disabled.

9. Change Consistent Device Naming to enabled.

10. Click Advanced tab and then select Processor.

11. On the Processor screen, make changes as captured in the following figure.
12. Change the Workload Configuration to IO Sensitive on the same page.

13. Click Save Changes.

Create Maintenance Policy

To update the default Maintenance Policy, follow these steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root > sub-Organizations > CV-ScaleProtect.
3. Right-click Maintenance Policies and Select Create Maintenance Policy.
4. Enter UserAck_Pol as the Maintenance Policy name.
5. Change the Reboot Policy to User Ack.
6. Optional: Click “On Next Boot” to delegate maintenance windows to server owners.
7. Click OK.
Create Adapter Policy

To create adaptor policy, follow these steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root > Sub-O rganizations > CV-ScaleProtect.
3. Right-click Adapter Policies and Select Ethernet Adaptor Policy.
4. Enter name as ScaleP_Adap_Pol.
5. Enter Transmit Queues = 8, Receive Queues = 8, Ring Size = 4096.
6. Enter Completion Queues = 16 and Interrupts = 32.
7. Under Options, make sure Receive Side Scaling (RSS) is enabled.
8. Click OK.
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.
7. Select the Enable Failover checkbox.
8. Select Updating Template as the Template Type.
9. Select Redundancy Type as No Redundancy
10. Under VLANs, select the checkbox for Data_VLAN VLAN.
11. Set Data_VLAN as the native VLAN.

12. For MTU, enter 1500.

13. In the MAC Pool list, select MAC_Pool_A.

14. In the Network Control Policy list, select ScaleProtect_NCP.
15. Click OK to create the vNIC template.

16. Click OK.

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

Follow these steps for the Cluster VLAN template:

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

2. Select Policies > root.

3. Right-click vNIC Templates.
4. Select Create vNIC Template

5. Enter vNIC_SP_Cluster as the vNIC template name.

6. Select Fabric B.

7. Select the Enable Failover checkbox.

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

9. Select Redundancy Type as No Redundancy.

10. Select Updating Template as the template type.

11. Under VLANs, select the checkboxes for Cluster_VLAN.

12. Set Cluster_VLAN as the native VLAN.
13. Select vNIC Name for the CDN Source.

14. For MTU, enter 9000.

15. In the MAC Pool list, select MAC_Pool_B.

16. In the Network Control Policy list, select ScaleProtect_NCP.
17. Click OK to create the vNIC template.

18. Click OK.

Create LAN Connectivity Policy

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

1. In Cisco UCS Manager, click LAN on the left.
2. Select LAN > Policies > root > Sub-O rganizations > CV-ScaleProtect.
3. Right-click LAN Connectivity Policies.
4. Select Create LAN Connectivity Policy.
5. Enter CVLT_SP_LAN as the name of the policy.

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

7. In the Create vNIC dialog box, enter vNIC_Data_eth0 as the name of the vNIC.

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

8. Select the Use vNIC Template checkbox.

9. In the vNIC Template list, select vNIC_Data_eth0.

10. In the Adapter Policy list, select Linux.

11. Click OK to add this vNIC to the policy.
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 `Linux`. 
17. Click OK to add the vNIC to the policy.

18. Click OK, then click OK again to create the LAN Connectivity Policy.
Optional: Create vhBA Templates for FC Connectivity

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

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

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

8. Click OK to create the vHBA template.

9. Click OK.

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

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

12. Click the radio button to select Fabric B.

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

14. In the WWPN Pool, Choose WWPN-Pool-B.
15. Click OK to create the vHBA template.

16. Click OK.

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

18. Select Policies > root > Sub-Organizations > CV-ScaleProtect.

19. Right-click vHBA Templates and choose Create vHBA Template.

20. Enter Backup-vHBA-A as the vHBA template name.

21. Click the radio button to select Fabric A.

22. In the Select VSAN list, Choose Backup-A.

23. In the WWPN Pool list, Choose WWPN-Pool-A.
24. Click OK to create the vHBA template.

25. Click OK.

26. Right-click vHBA Templates again and choose Create vHBA Template.

27. Enter Backup-vHBA-B as the vHBA template name.

28. Click the radio button to select Fabric B.

29. In the Select VSAN list, Choose Backup-B.

30. In the WWPN Pool, Choose WWPN-Pool-B.
31. Click OK to create the vHBA template.

32. Click OK.

Optional: Create FC SAN Connectivity Policies

This configuration step can be skipped if the ScaleProtect 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-O rganizations > CV-ScaleProtect.

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

4. Enter CVLT_SP_SAN as the name of the policy.

5. Select WWNN-Pool from the drop-down list under World Wide Node Name.
6. Click Add. You might have to scroll down the screen to see the Add link.

7. Under Create vHBA, enter vHBA1 in the Name field.

8. Check the check box Use vHBA Template.

9. From the vHBA Template drop-down list, select Infra-vHBA-A.

10. From the Adapter Policy drop-down list, select Linux.
11. Click OK.

12. Click Add.

13. Under Create vHBA, enter vHBA2 in the Name field.

14. Check the check box next to Use vHBA Template.

15. From the vHBA Template drop-down list, select Infra-vHBA-B.

16. From the Adapter Policy drop-down list, select Linux.
17. Click OK.

18. Click Add.

19. Under Create vHBA, enter vHBA3 in the Name field.

20. Check the check box next to Use vHBA Template.

21. From the vHBA Template drop-down list, select Backup-vHBA-A.

22. From the Adapter Policy drop-down list, select Linux.
23. Click OK.

24. Click Add.

25. Under Create vHBA, enter vHBA4 in the Name field.

26. Check the check box next to Use vHBA Template.

27. From the vHBA Template drop-down list, select Backup-vHBA-B.

28. From the Adapter Policy drop-down list, select Linux.
Create vHBA

Name: vHBA4
Use vHBA Template: 
Redundancy Pair: 

vHBA Template: Backup-vHBA-B

Adapter Performance Profile

Adapter Policy: Linux

Create vHBA Template

Create Fibre Channel Adapter Policy

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>WWPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>vHBA vHBA4</td>
<td>Derived</td>
</tr>
<tr>
<td>vHBA vHBA3</td>
<td>Derived</td>
</tr>
<tr>
<td>vHBA vHBA2</td>
<td>Derived</td>
</tr>
<tr>
<td>vHBA vHBA1</td>
<td>Derived</td>
</tr>
</tbody>
</table>

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.
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)` 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(1e)
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

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-O rganizations > CV-ScaleProtect.
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.
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.
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.

25. Click OK.

26. Click OK again to complete the Disk Zoning Policy creation.
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-O rganizations > CV-ScaleProtect.
3. Right-click and select Create Chassis Profile Template.
4. Enter name as CVLT_SP_Chassis.
5. Select Type as Updating Template.
6. Select default as the Maintenance Policy and click Next.
7. Select Chassis Firmware Package as S3260_firmware.
8. Select Disk Zoning Policy as `S3260_DiskZone` and click Finish.
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-O rganizations > 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-O rganizations > 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.
6. Click OK.

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

8. On FSM Tab you will see the Association Status.
9. Repeat steps 1-8 to associate second Chassis with the Chassis Profile CVLT_S3260_CP2.

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.

Setting S3260 Disk to Unconfigured Good

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

To prepare all disks from the 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.


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.

    | Name | Description | RAID Level |
    |------|-------------|------------|
    | CVLT_SP-Boot | ScaleProtect Disk Boot Policy | RAID 1 Mirrored |

    | Disk Group Configuration (Manual) |
    | Slot Number | Role | Span ID |
    |--------|--------|--------|
    | No data available |

    Virtual Drive Configuration
    | Strip Size (KB) | Access Policy |
    |----------------|---------------|
    | Platform Default | Platform Default, Read Write, Read Only, Blocked |

7. Enter 201 as the slot number and click OK.
8. Click OK.

9. Click Add again.

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

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).

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

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

33. Enter 53 as the slot number and click OK.
34. Repeat steps 1–33 for Slots 54 through 56.

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

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Role</th>
<th>Span ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>53</td>
<td>Normal</td>
<td>Unspecified</td>
</tr>
<tr>
<td>54</td>
<td>Normal</td>
<td>Unspecified</td>
</tr>
<tr>
<td>55</td>
<td>Normal</td>
<td>Unspecified</td>
</tr>
<tr>
<td>56</td>
<td>Normal</td>
<td>Unspecified</td>
</tr>
</tbody>
</table>

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.
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.
10. Click Add under Local LUN to continue creating LUNs in the SSD Disk Group.
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.
15. Verify that all the LUNs are configured as documented and click OK.
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.
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.
27. Verify that all the LUNs are configured as documented and click OK.
Cisco UCS Server Configuration

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_SP_S3260_S2 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.
7. Expand the Local Devices drop-down list and Choose Add Remote CD/DVD.

8. Click Add Local LUN to reference the Boot LUN created by the CV_SP_Boot Disk Group Policy.
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.
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-O rganizations > 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_Pool as the UUID pool.
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).

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.
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.
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

Figure 16 Installation with HBAs for SAN Connectivity
2. Click Next.

**Configure vMedia Policy**

To configure the vMedia policy, follow these steps:

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

2. Click Next.

**Configure Server Boot Order**

To configure the server boot order, follow this step:

1. Choose **CVLT_S3260_Boot** as the Boot Policy that was created earlier.
Configure Maintenance Policy

To configure the maintenance policy, follow these steps:

1. Change the Maintenance Policy to UserAck_Pol.
2. Click Next.

Configure Server Assignment

To configure server assignment, follow these steps:

1. In the Pool Assignment list, select the server pool created for the first Server Nodes in the Chassis.
2. Expand Firmware Management at the bottom of the page and select CV_SP_Firmware as created in the previous section.

3. Click Next.
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.
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


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.
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.
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.

17. Verify the Boot LUN and Cache LUNs under Storage tab of Service Profile.
18. Verify Service Profile has 2 vNICs.
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-O rganizations > 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.
15. Select Power Cycle, then click OK.

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.

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.

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

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

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

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

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).
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.

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.
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=192.168.20.182
NETMASK=255.255.255.0
GATEWAY=192.168.20.1
DNS1=192.168.20.19
HWADDR=00:25:b1:08:00:14
```

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:b1:08:00:34
```

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

```
[root@server network-scripts]# systemctl restart network
```

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

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

47. Enter the CommServe information, then select OK.

48. The server is now registered with the CommServe.

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.
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.
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**

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Type</th>
<th>Number of nodes</th>
<th>Capacity</th>
<th>Free space</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSV1 ScaleProtect.Policy</td>
<td>Offline</td>
<td>Online failures</td>
<td>2</td>
<td>2TB</td>
<td>0 bytes</td>
</tr>
<tr>
<td>ScaleProtect.pool1</td>
<td>Scale-out</td>
<td>Scale-out</td>
<td>3</td>
<td>161.00 TB</td>
<td>0 bytes</td>
</tr>
<tr>
<td>ScaleProtect.pool2</td>
<td>Scale-out</td>
<td>Scale-out</td>
<td>3</td>
<td>0 bytes</td>
<td>0 bytes</td>
</tr>
</tbody>
</table>

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.

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