Commvault® ScaleProtect™ with Cisco UCS S3260 Storage Server

This document introduces the Commvault® Data Platform deployment on the Cisco UCS® S3260 Storage Server.

Contents

Introduction

Enterprise IT is being transformed with the maturing of public cloud providers that offer computing, storage, and application services with exceptional elasticity, scale, resiliency, and availability with a consumption-based economic model. However, the choice between public cloud and on-premises infrastructure is not a binary one.

As some workloads shift to the cloud, enterprises are also seeking to transform their internal data centers and services into offerings that provide cloud-like scale, flexibility, resiliency, and operational methods, with similar positive economic outcomes. To this end, architects are augmenting or replacing traditional, proprietary, and single-purpose IT infrastructure and applications with software-defined services, distributed processing, big data applications, and hyperconverged architectures.

Transforming mission-critical applications and workloads can be difficult and disruptive, but transforming secondary infrastructure is less risky. By some estimates 50 to 70 percent of infrastructure capacity is used for secondary workloads and storage. Businesses can accelerate their transformation initiatives with less disruption by targeting this secondary infrastructure. Commvault ScaleProtect on the Cisco UCS® S3260 Storage Server enables this shift for secondary storage and workloads, supporting cloud-like economics and critical services using secondary data, and extending these services into the public cloud.

Purpose of this document

This document describes the installation and configuration steps for deploying Commvault ScaleProtect with Cisco UCS S3260 Storage Server to build an integrated data protection solution. It provides Cisco and Commvault configuration guidelines and best practices to deploy a modern data protection solution.

This document provides a detailed step-by-step guide for tasks required to configure the solution in Cisco UCS Manager and the Commvault console. This document does not cover the initial setup of the Cisco Unified Computing System™ (Cisco UCS) or the connectivity to the upstream LAN and SAN. It assumes that the reader has a basic knowledge of Cisco UCS and Commvault Data Platform installation and configuration.

Test environment

This section introduces the technologies used in the solution described in this document.

Table 1 lists the hardware and software versions used in the test environment described in this document.

Table 1. Test environment details

Layer	Device	Image
Computing	Cisco UCS 6332-16UP Fabric Interconnect pair	Release 3.1(2b)
	Cisco UCS S3260 Storage Server	Release 3.1(2b)
Network	Cisco Nexus® 9372PX-E Switch pair	Release 7.0(3)I2(4)
Software	Cisco UCS Manager	Release 3.1(2b)
	Commvault Data Platform	Release V11 SP9

Solution overview

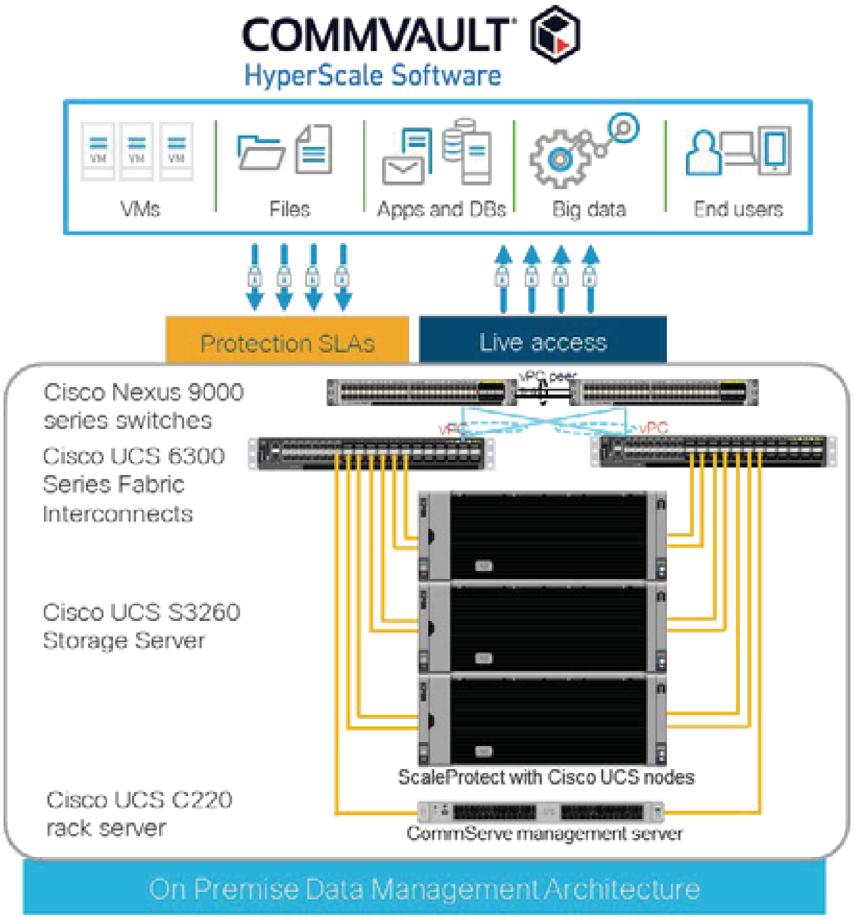
Commvault ScaleProtect with Cisco UCS delivers web-scale data services for data protection using industry-standard x86 servers while providing best-in-class data management.

By combining Cisco UCS servers with industry-leading Commvault HyperScale Software, customers gain exceptional scale-out flexibility and agility with uncompromised data management, all with cloud-like economics and true hybrid cloud capabilities. Cisco UCS revolutionized the server market through its programmable fabric and automated management that simplify application and service deployment.

ScaleProtect with Cisco UCS provides a full suite of data services for protecting, indexing, securing, automating, reporting, and natively accessing data. In addition, ScaleProtect provides insight into the data, thereby creating the value the business demands.

Figure 1 provides an overview of the solution.

Figure 1. High-level solution overview


COMMVAULT
HyperScale Software
VM
VMs
Files
Apps and DBs
Big data
End users
Protection SLAs
Live access
Cisco Nexus 9000 series switches
vPC peer
vPC
vPC
Cisco UCS 6300 Series Fabric Interconnects
Cisco UCS S3260 Storage Server
ScaleProtect with Cisco UCS nodes
Cisco UCS C220 rack server
CommServe management server
On Premise Data Management Architecture

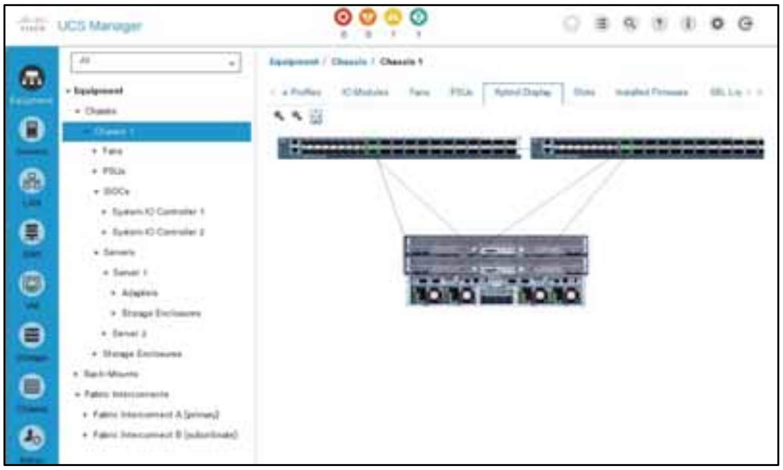
Cisco Unified Computing System

Cisco UCS is a state-of-the-art data center platform that unites computing, network, storage access, and virtualization resources into a single cohesive system.

Cisco UCS consists of these main resources:

- Computing: The system is based on an entirely new class of computing system that incorporates rack-mount and blade servers using Intel® Xeon® processor CPUs. The Cisco UCS servers offer patented Cisco® Extended Memory Technology to support applications with large data sets and allow more virtual machines per server.
- Network: The system is integrated onto a low-latency, lossless, 10- or 40-Gbps unified network fabric. This network foundation consolidates LANs, SANs, and high-performance computing (HPC) networks, which are separate networks today. The unified fabric lowers costs by reducing the number of network adapters, switches, and cables, and by decreasing the power and cooling requirements.
- Virtualization: The system unleashes the full potential of virtualization by enhancing the scalability, performance, and operational control of virtual environments. Cisco security, policy enforcement, and diagnostic features are now extended into virtualized environments to better support changing business and IT requirements.
- Storage access: The system provides consolidated access to both SAN storage and network-attached storage (NAS) over the unified fabric. By unifying the storage access layer, Cisco UCS can access storage over Ethernet (with Network File System [NFS] or Small Computer System Interface over IP [iSCSI]), Fibre Channel, and Fibre Channel over Ethernet (FCoE). This approach provides customers with choice for storage access and investment protection. In addition, server administrators can pre-assign storage-access policies for system connectivity to storage resources, simplifying storage connectivity and management for increased productivity.

Figure 2. Cisco UCS Manager



Cisco UCS consists of the following components:

- Cisco UCS Manager provides unified, embedded management of all software and hardware components in the Cisco Unified Computing System (Figure 2).
- Cisco UCS 6000 Series Fabric Interconnects are line-rate, low-latency, lossless, 10-Gbps Ethernet and FCoE interconnect switches that provide the management and communication backbone for Cisco UCS.
- Cisco UCS 5100 Series Blade Server Chassis supports up to eight blade servers and up to two fabric extenders in a 6-rack-unit (6RU) enclosure.
- Cisco UCS B-Series Blade Servers are Intel-based blade servers that increase performance, efficiency, versatility, and productivity.
- Cisco UCS C-Series Rack Servers deliver unified computing in an industry-standard form factor to reduce total cost of ownership (TCO) and increase agility.
- Cisco UCS S-Series Storage Servers deliver unified computing in an industry-standard form factor to address data-intensive workloads with reduced TCO and increased agility.
- Cisco UCS adapters with wire-once architecture offer a range of options to converge the fabric, optimize virtualization, and simplify management.

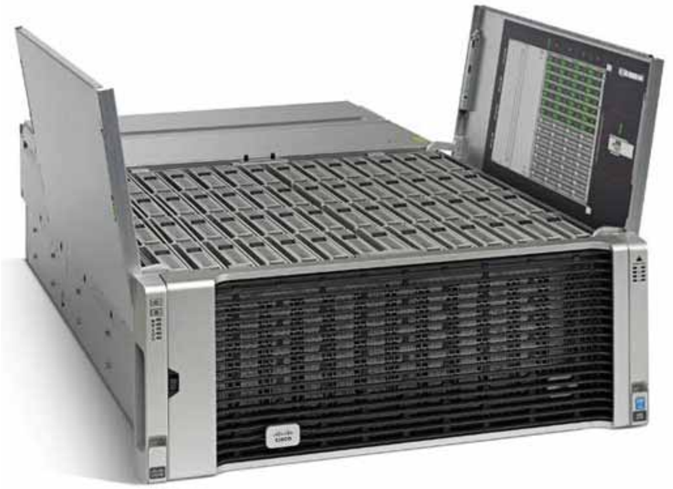
Cisco UCS is designed to deliver:

- Reduced TCO and increased business agility
- Increased IT staff productivity through just-in-time provisioning and mobility support
- A cohesive, integrated system that unifies the technology in the data center
- Industry standards supported by a partner ecosystem of industry leaders
- Unified, embedded management for easy-to-scale infrastructure

Cisco UCS S3260 Storage Server

The Cisco UCS S3260 Storage Server (Figure 3) is a modular, high-density, high-availability dual-node rack server well suited for service providers, enterprises, and industry-specific environments. It addresses the need for dense, cost-effective storage for the ever-growing amounts of data. Designed for a new class of cloud-scale applications, it is simple to deploy and excellent for data protection applications such as Commvault Data Platform, software-defined storage environments such as GlusterFS, and other unstructured data repositories, big data applications, media streaming, and content distribution.

Figure 3. Cisco UCS S3260 Storage Server



Extending the capabilities of the Cisco UCS C3000 platform, the Cisco UCS S3260 helps you achieve the highest levels of data availability. With dual-node capability that is based on the Intel Xeon processor E5-2600 v4 series, it offers up to 600 terabytes (TB) of local storage in a compact 4RU form factor. All hard-disk drives (HDDs) can be asymmetrically split between the dual nodes and are individually hot-swappable. The drives can be built in an enterprise-class Redundant Array of Independent Disks (RAID) redundant design or used in pass-through mode.

This high-density rack server easily fits in a standard 32-inch-depth rack, such as the Cisco R42610 Rack.

Cisco UCS S-Series Storage Servers can be deployed as standalone servers or as part of a Cisco UCS managed environment to take advantage of Cisco's standards-based unified computing innovations that help reduce customers' TCO and increase their business agility.

The Cisco UCS S3260 uses a modular server architecture that, using Cisco's blade technology expertise, allows you to upgrade the computing or network nodes in the system without the need to migrate data from one system to another. It delivers:

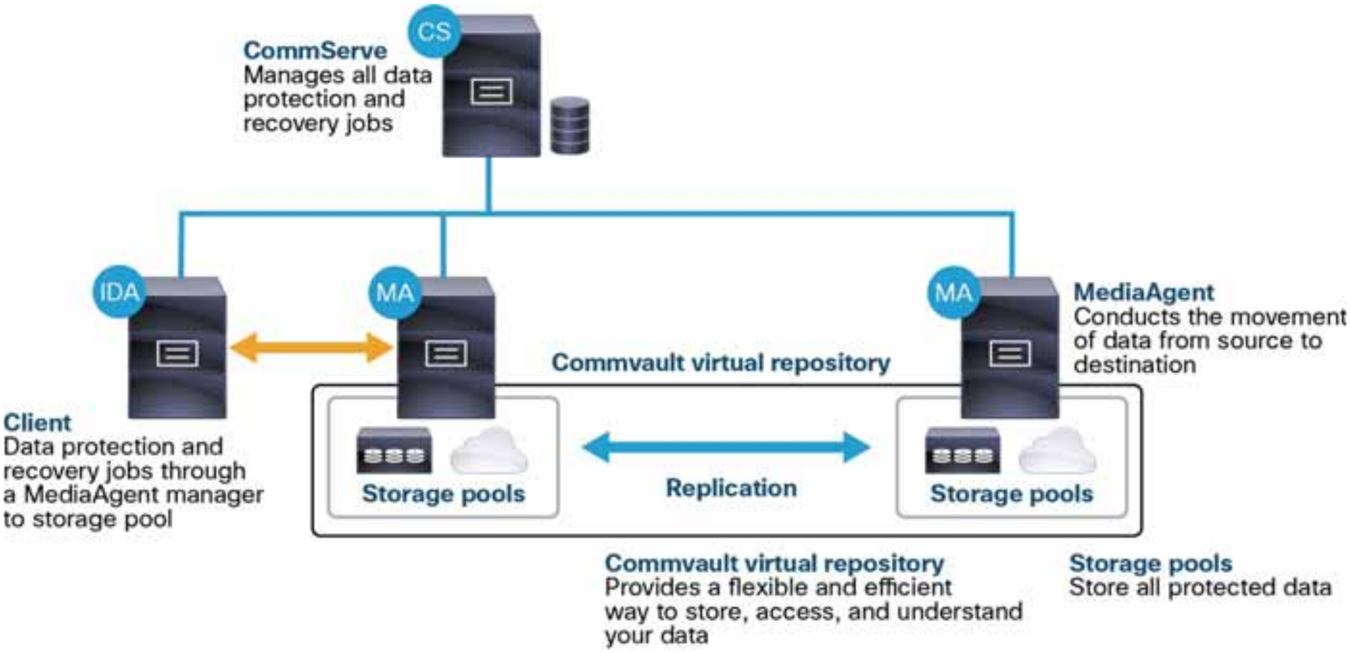
- Dual server nodes
- Up to 36 computing cores per server node
- Up to 60 drives, mixing a large form factor (LFF) with up to 28 solid-state disk (SSD) drives plus 2 SSD SATA boot drives per server node
- Up to 512 GB of memory per server node (1 TB total)
- Support for 12-Gbps serial-attached SCSI (SAS) drives
- A system I/O controller (SIOC) with a Cisco UCS Virtual Interface Card (VIC) 1300 platform embedded chip supporting dual-port 40-Gbps connectivity
- High reliability, availability, and serviceability (RAS) features with tool-free server nodes, SIOC, easy-to-use latching lid, and hot-swappable and hot-pluggable components

Commvault Data Platform

The Commvault Data Platform is a single platform for automated global protection, retention, and recovery. Commvault enterprise data protection and recovery software automates global data protection, accelerates recovery, reduces costs, and simplifies operations. Commvault integrates application awareness with hardware snapshots, indexing, global deduplication, replication, search, and reporting. The Commvault Data Platform converges all the needs of a modern data management solution in one place to seamlessly integrate protection, management, and access in one solution.

A comprehensive data protection and management strategy offers seamless and efficient backup, archiving, storage, and recovery of data in your enterprise from any operating system, database, and application. To protect and manage data in your environment, the Commvault software must be distributed to systems that you want to protect. CommServe, MediaAgent, and protected systems constitute a CommCell environment, and each protected system is referred to as a client (Figure 4).

Figure 4. Commvault Data Platform overview


CS
CommServe
Manages all data protection and recovery jobs
IDA
MA
MA
MediaAgent
Conducts the movement of data from source to destination
Commvault virtual repository
Client
Data protection and recovery jobs through a MediaAgent manager to storage pool
Storage pools
Replication
Storage pools
Commvault virtual repository
Provides a flexible and efficient way to store, access, and understand your data
Storage pools
Store all protected data

The CommServe server is the command and control center of the CommCell architecture. It coordinates and executes all CommCell operations, maintaining Microsoft SQL Server databases that contain all configuration, security, and operational history for the CommCell environment. A CommCell environment can contain only one CommServe host. The CommServe software can be installed in physical, virtual, and clustered environments.

MediaAgent is the data transmission manager. It provides high-performance data movement and manages the data storage pools. When installed on a client system, it also manages Commvault IntelliSnap snapshot integration with the underlying storage.

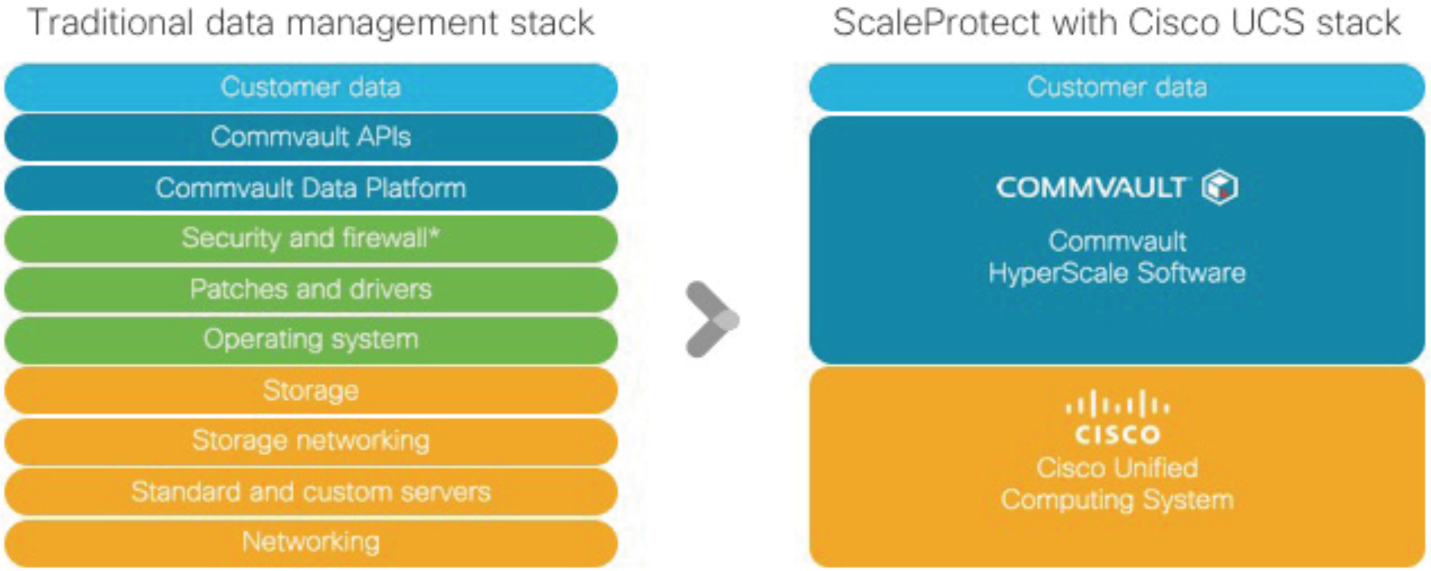
A client is any system within a CommCell environment to be protected. iDataAgents are software modules that are installed on computers to access and protect data. The backup and recovery system uses agents to interface with file systems, applications, and databases to facilitate the protection of data on production systems. By default, a file system iDataAgent module is installed when the Commvault software is added to a system. If the client hosts specific applications or databases, additional iDataAgents are required.

These three Commvault components combined offer the most comprehensive and flexible data protection solution on the market today.

Solution design and reference architecture configurations

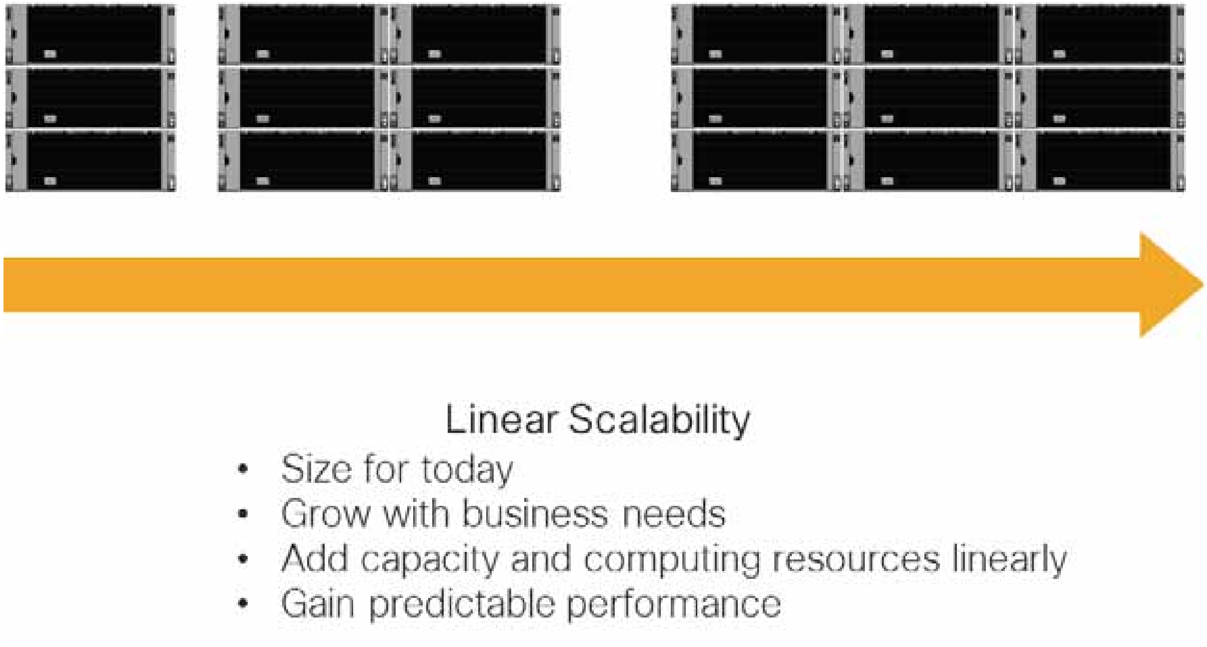
Commvault ScaleProtect with Cisco UCS addresses the data protection needs of modern data centers. The increasing percentage of virtualized workloads, the dramatic increase in the size and amount of data, and the changes in the ways that companies do business and work with data have had an immense impact on data protection solutions. With the time requirement for backup operations reduced to minutes, and with recovery point objective (RPO) and recovery time objective (RTO) requirements in the range of minutes to one hour, technologies such as compression, deduplication, replication, and backup to disk are essential in every design. The second-tier storage must be able to scale as quickly as the protected data grows, but the traditional silo-based approach has too many limitations to be effective. The Commvault HyperScale architecture introduces a modern way to perform second-tier data management by breaking down the silos and reducing the management overhead in second-tier environments (Figure 5).

Figure 5. Traditional data management stack compared to Commvault ScaleProtect with Cisco UCS



The features and functions provided by ScaleProtect, combined with the features and functions provided by Cisco UCS, create a powerful solution for fast backup and fast restore operations that is simple to implement and easy to scale and upgrade. With the combination of Cisco and Commvault technologies, you can easily scale from tens of terabytes up to hundreds of petabytes (PB) of protected data (Figure 6).

Figure 6. Commvault ScaleProtect with Cisco UCS S3260 scaling


Linear Scalability
• Size for today
• Grow with business needs
• Add capacity and computing resources linearly
• Gain predictable performance

Disks are now common backup media, and data backup on disk generally provides fast restore operations. Disk-based storage can be used for all types and sizes of backups. Backup to tape is still a good option to use to create an offline copy of data for media mobility, ransomware protection, and long-term archival.

There is no “best” position in the infrastructure to install a ScaleProtect with Cisco UCS solution. Many different options are available regardless of how big a data center is. One option is to position the solution in a central place in the physical network so that it can be accessed from everywhere with the required bandwidth. Another option is to place the solution as close as possible to the data source.

With most data transferred from the backup client to the server and not directly from storage, and with the unique design of Cisco UCS, the use of a Cisco UCS domain will limit the network bandwidth required for data replication between the ScaleProtect nodes. This option also allows Cisco UCS Manager to manage all ScaleProtect servers in a central place.

Reference architecture

Using the rules for the Commvault ScaleProtect™ server as a basis, Commvault and Cisco have defined and tested configurations (Tables 2 and 3) and various scale options. The underlying scale-out storage and the erasure coding option used dictate a building-block model of 3 or 6 nodes to start and for scaling. The 3 nodes model scales in increments of 3 -3, 6, 9, 12 or to more nodes. The 6 node model scales in increments of 6 - 6, 12, 18, 24, or to more nodes. The server configuration within a block of 3 or 6 nodes must be the same. However, you can use different server or storage options within a ScaleProtect cluster. As a deployment option, the Commvault CommServe can run virtualized to manage the physical ScaleProtect server.

Table 2. Cisco UCS configurations for Commvault ScaleProtect server

	Block of 3 Cisco UCS C240 M5 nodes	Block of 3 Cisco UCS S3260 nodes	Block of 3 Cisco UCS S3260 chassis
Boot disks	3 x 2 x 480-GB SSDs	3 x 2 x 480-GB SSDs	4 x 480-GB SSDs
Data disks	• 3 x 12 x 4-TB SAS • 3 x 12 x 6-TB SAS • 3 x 12 x 8-TB SAS • 3 x 12 x 10-TB SAS	• 3 x 24 x 4-TB SAS • 3 x 24 x 6-TB SAS • 3 x 24 x 8-TB SAS • 3 x 24 x 10-TB SAS	• 3 x 48 x 4-TB SAS • 3 x 48 x 6-TB SAS • 3 x 48 x 8-TB SAS • 3 x 48 x 10-TB SAS
Flash storage	3 x 1 x 1.6-TB NVMe	3 x 4 x 1.6-TB SSD	3 x 8 x 1.6-TB SSD
Cisco UCS rack servers	C240 M5 LFF	S3260 M4	2 x S3260 M4
CPU	Intel Xeon processor 5118 (12 cores, 2.3 GHz, and 105W)	Intel Xeon processor E5-2650 v4 (12 cores, 2.2 GHz, and 105W)	Intel Xeon processor E5-2695 v4 (18 cores, 2.1 GHz, and 120W)
Memory	3 x 64 GB	3 x 256 GB	3 x 2 x 256 GB
RAID cache	3 x 1 GB	3 x 4GB	3 x 2 x 4 GB
RAID	RAID1 for OS and JBOD for SAS	RAID1 for OS, RAID5 for SSD, and JBOD for HDD	RAID1 for OS, RAID5 for SSD, and JBOD for HDD
Maximum Fibre Channel ports	4 x 16 Gbps	None; FCoE through fabric interconnect	None; FCoE through fabric interconnect
Network ports	2 x 10 Gbps or 2 x 40 Gbps	2 x 40 Gbps	4 x 40 Gbps

Table 3. Solution sizing with building blocks

Cisco UCS model	Solution	Node drive count	Node count	Drive size[1]	Software drive size[2]	Usable[2] capacity
Cisco UCS C240	Commvault ScaleProtect and C240 87TB	12	3	4 TB	3.64 TB	87 TB
	Commvault ScaleProtect and C240 130TB	12	3	6 TB	5.46 TB	108 TB
	Commvault ScaleProtect and C240 174TB	12	3	8 TB	7.28 TB	174 TB
	Commvault ScaleProtect and C240 218TB	12	3	10 TB	9.10 TB	218 TB
Cisco UCS S3260	Commvault ScaleProtect and S3260 174TB	24	3	4 TB	3.64 TB	174 TB
	Commvault ScaleProtect and S3260 261TB	24	3	6 TB	5.46 TB	261 TB
	Commvault ScaleProtect and S3260 349TB	24	3	8 TB	7.28 TB	349 TB
	Commvault ScaleProtect and S3260 436TB	24	3	10 TB	9.10 TB	436 TB
	Commvault ScaleProtect and S3260 349TB	24	6	4 TB	3.64 TB	349 TB
	Commvault ScaleProtect and S3260 523TB	24	6	6 TB	5.46 TB	523 TB
	Commvault ScaleProtect and S3260 698TB	24	6	8 TB	7.28 TB	698 TB
	Commvault ScaleProtect and S3260 873TB	24	6	10 TB	9.10 TB	873 TB

Storage capacity explained

Customers sometimes ask why a freshly formatted hard disk or array is smaller than the advertised capacity. For example, a 1-TB drive has 931 GB after formatting.

The reason for this is that hardware and storage manufacturers count the capacity in different ways than the files system does. The prefixes kilo-, mega-, giga-, and tera- are used to state powers of ten. However, in computer software, the data being handled is typically organized based on powers of 2, so it became customary to call 2^{10} a kilobyte, which is actually 1024 bytes, not exactly 1000 bytes.

There are prefixes to differentiate between base 10 and base 2; however, these are seldom used. In base 2 the proper terms are kibibyte, mebibyte, gibibyte, and tebibyte. The “bi” refers to binary, and the shortened terms are KiB, MiB, GiB, and TiB.

Here’s the underlying math:

- Hard disk manufacturers assume kilo = 103 = 1000 (KB).
- File systems assume kilo = 224 = 1024 (KiB).

To convert KB, MB, and GB to KiB, MiB, and GiB, see the following list:

- KB to KiB: 1000/1024 = 0.9766
- MB to MiB: (1000 x 1000) / (1024 x 1024) = 0.9537
- GB to GiB: (1000 x 1000 x 1000) / (1024 x 1024 x 1024) = 0.9313
- TB to TiB: (1000 x 1000 x 1000 x 1000) / (1024 x 1024 x 1024 x 1024) = 0.9095

Typically, software will display GB or TB as the storage unit, but the amount actually is Gib or TiB, so this confusion will remain unless this approach is changed.

Configuration guidelines

This section provides guidelines for configuring the solution.

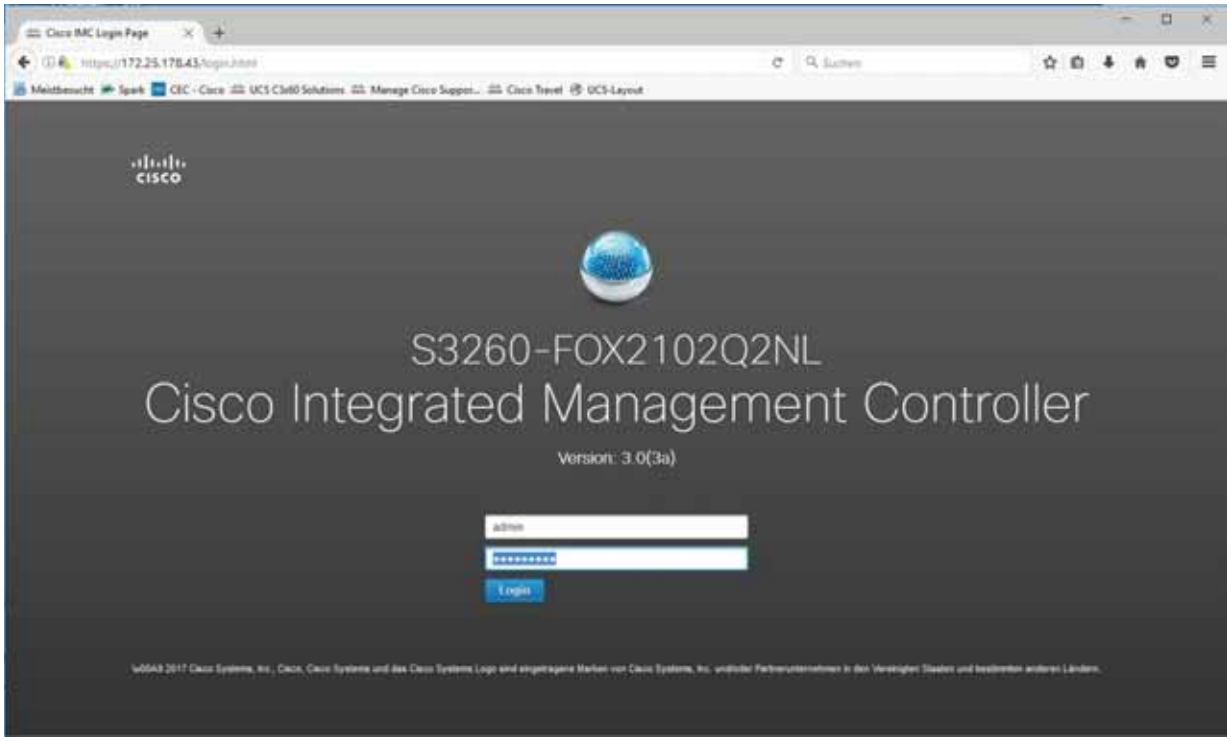
Cisco UCS configuration

This document discusses the use of a standalone Cisco UCS S32600 Storage Server as well as the use of a Cisco UCS 3260 Storage Server managed by Cisco UCS to install Commvault ScaleProtect to cover placement within a Cisco UCS domain or connected to data center switches.

Please use the Cisco UCS S3260 installation guide to complete the initial configuration (IP addresses, passwords, software versions, etc.). This document assumes that the S3260 is accessible through the Cisco Integrated Management Controller (IMC) or Cisco UCS Manager over the network.

Standalone configuration with Cisco Integrated Management Controller

Log on to the IMC as the admin user.



S3260-FOX2102Q2NL

Cisco Integrated Management Controller

Version: 3.0(3a)

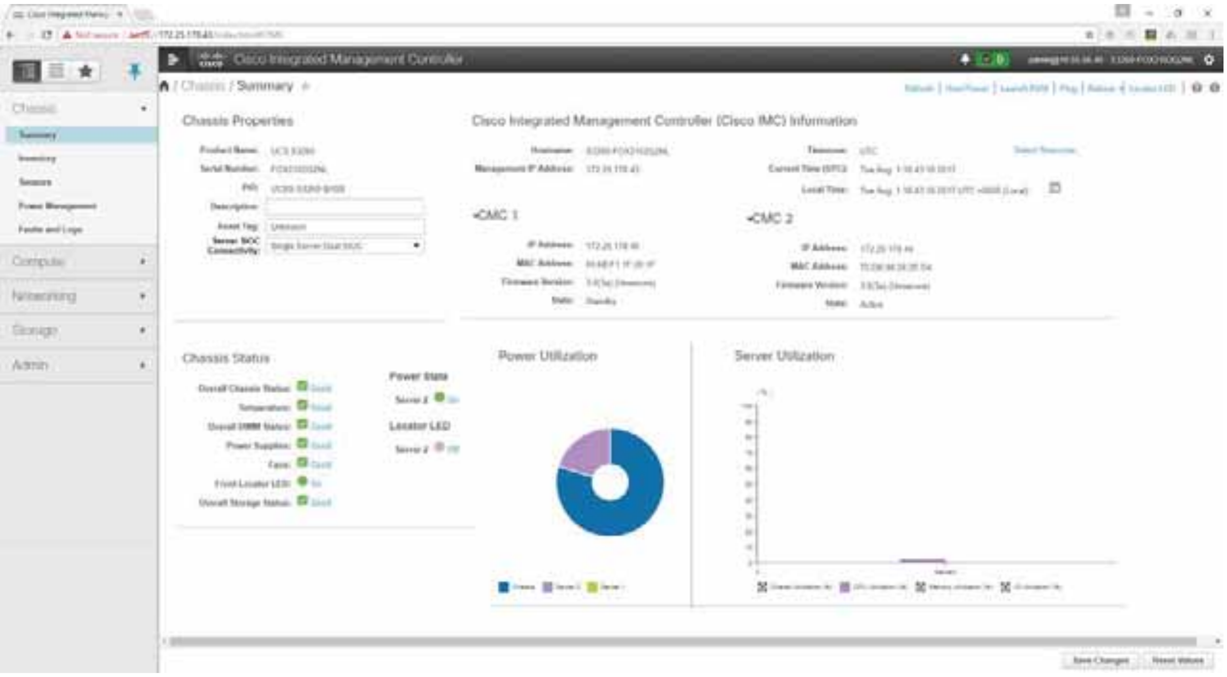
admin

••••••••••

Login

\u00A9 2017 Cisco Systems, Inc., Cisco, Cisco Systems und das Cisco Systems Logo sind eingetragene Marken von Cisco Systems, Inc. und/oder Partnerunternehmen in den Vereinigten Staaten und bestimmten anderen Ländern.

Check the condition of the system and the components required for the deployment on the Chassis > Summary page.



/ Chassis / Summary

Chassis Properties

Product Name: UCS S3260

Serial Number: FOX2102Q2NL

Description:

Asset Tag: Unknown

Server SIOC Connectivity: Single Server Dual SIOC

Cisco Integrated Management Controller (Cisco IMC) Information

Hostname: S3260-FOX2102Q2NL

Management IP Address: 172.25.178.43

Timezone: UTC

CMC 1

State: Standby

CMC 2

State: Active

Chassis Status

Overall Chassis Status: ☑ Good

Temperature: ☑ Normal

Overall DIMM Status: ☑ Good

Power Supplies: ☑ Good

Fans: ☑ Good

Front Locator LED: ● Off

Overall Storage Status: ☑ Good

Power State

Server 2 ● On

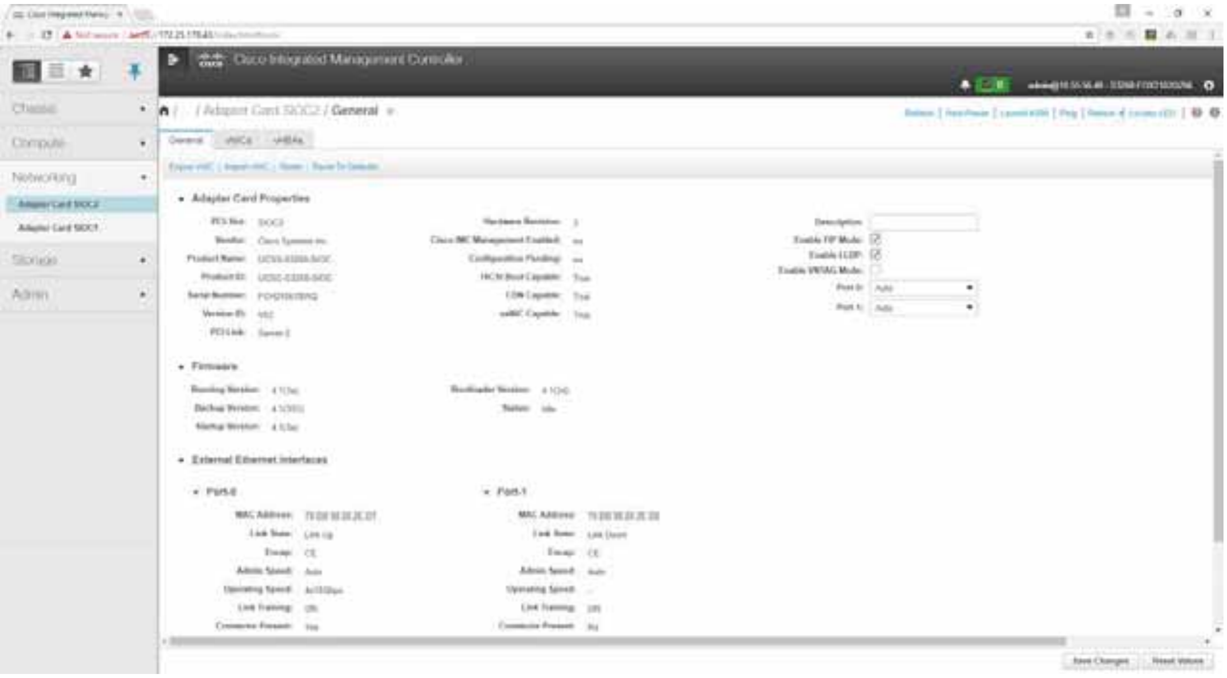
Locator LED

Server 2 ● Off

Choose Networking to see the SIOC configuration.

Only one SIOC is required. The second SIOC is optional and is used to achieve better high availability or greater throughput.

The General tab provides an overview of the SIOC and Ethernet ports, including the uplink status and port speeds. The operating speed can be 10 Gbps, 4 x 10 Gbps, or 40 Gbps. You should use 40 Gbps whenever possible.



Adapter Card Properties

PCI Slot: SIOC2
Vendor: Cisco Systems Inc
Product Name: UCSS-S3260-SIOC
Product ID: UCSC-S3260-SIOC
Serial Number: [illegible]
Version ID: V02
PCI Link: [illegible]
Hardware Revision: 3
Cisco IMC Management Enabled: no
Configuration Pending: no
ISCSI Boot Capable: True
CDN Capable: True
usNIC Capable: True
Description:
Enable FIP Mode: ☑
Enable LLDP: ☑
Enable VNTAG Mode: ☐
Port 0: Auto
Port 1: Auto

Firmware

Running Version: 4.1(3a)
Backup Version: [illegible]
Startup Version: 4.1(3a)
Bootloader Version: [illegible]
Status: Idle

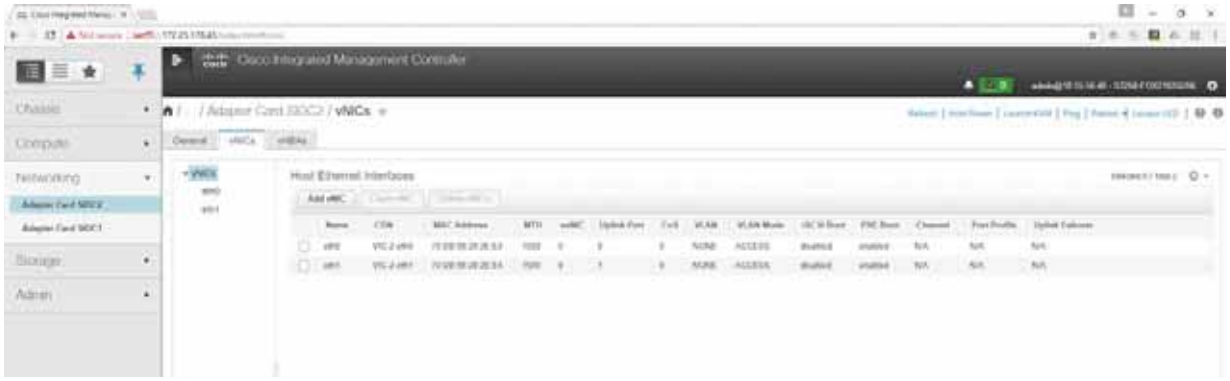
External Ethernet Interfaces

Port-0
MAC Address: [illegible]
Link State: Link Up
Encap: CE
Admin Speed: Auto
Operating Speed: 4x10Gbps
Link Training: ON
Connector Present: Yes

Port-1
MAC Address: [illegible]
Link State: Link Down
Encap: CE
Admin Speed: Auto
Operating Speed: -
Link Training: ON
Connector Present: No

The virtual network interface card (vNIC) tab summarizes the existing host Ethernet interfaces, including the maximum transmission unit (MTU) size, the uplink port used, and VLAN information. As a best practice, you should create at least one vNIC per uplink port or one vNIC per VLAN ID.

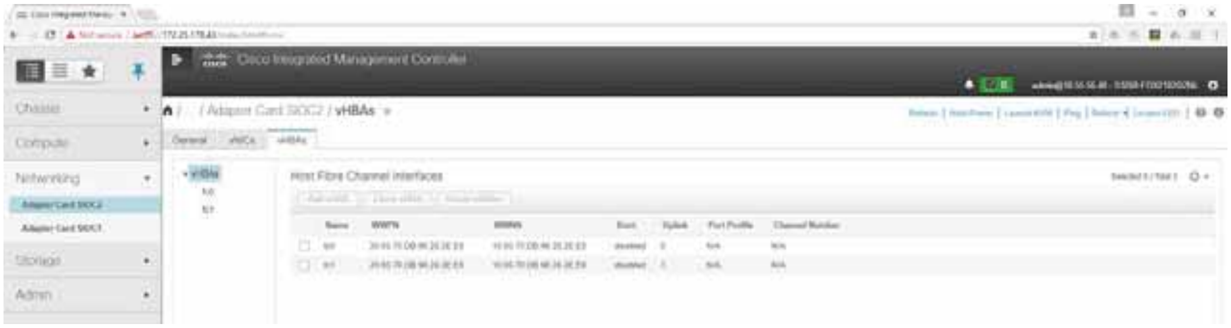
You should use MTU 9000 for the backup network if possible and on all participating devices in the network (clients, switches, and servers).



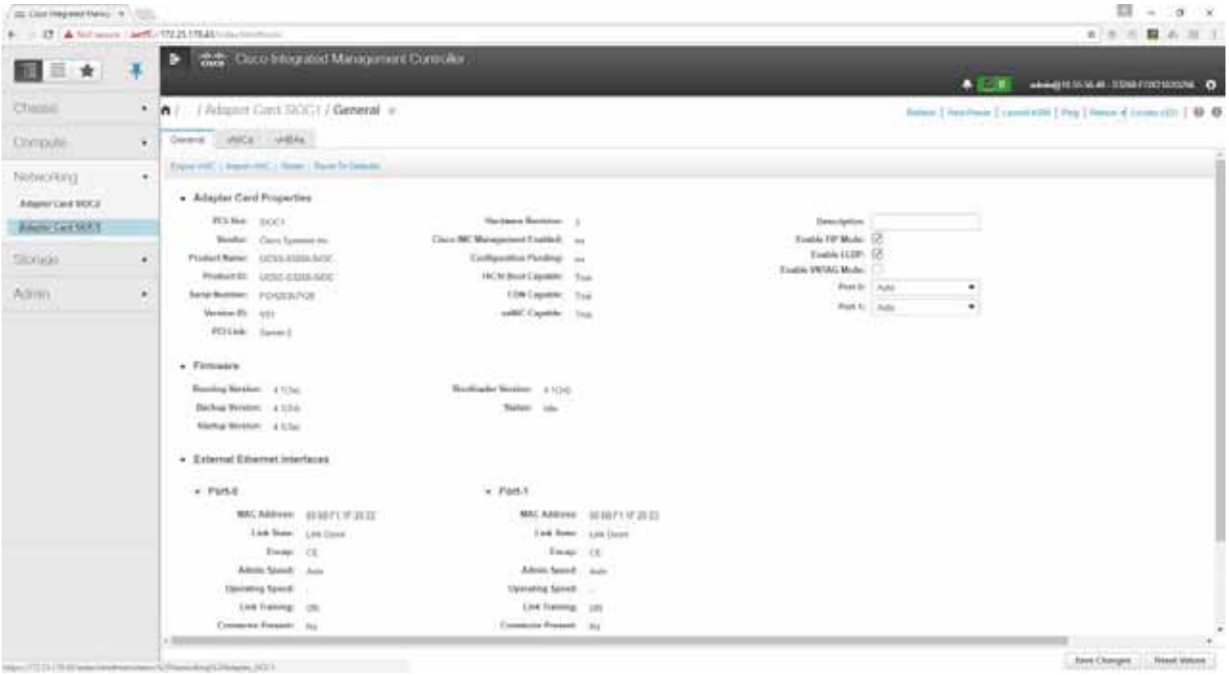
Host Ethernet Interfaces

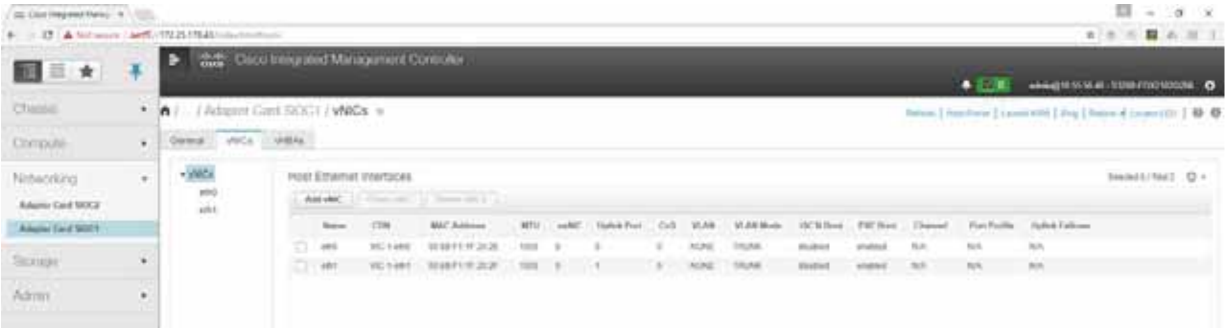
	Name	CDN	MAC Address	MTU	usNIC	Uplink Port	CoS	VLAN	VLAN Mode	iSCSI Boot	PXE Boot	Channel	Port Profile	Uplink Failover
☐	eth0	VIC-2-eth0	[illegible]	1500	0	0	0	NONE	ACCESS	disabled	enabled	N/A	N/A	N/A
☐	eth1	VIC-2-eth1	[illegible]	[illegible]	0	1	0	NONE	ACCESS	disabled	enabled	N/A	N/A	N/A

The virtual host bus adapter (vHBA) tab summarizes the existing host Fibre Channel Interfaces, including the worldwide port name (WWPN) and worldwide node name (WWNN) and information about whether the vHBA is used to boot the system. As a best practice, you should create at least one vHBA per uplink port or one vHBA per VSAN ID. Fibre Channel connectivity is used mainly for backup to Fibre Channel tape or for LAN-free backup directly from SAN storage.

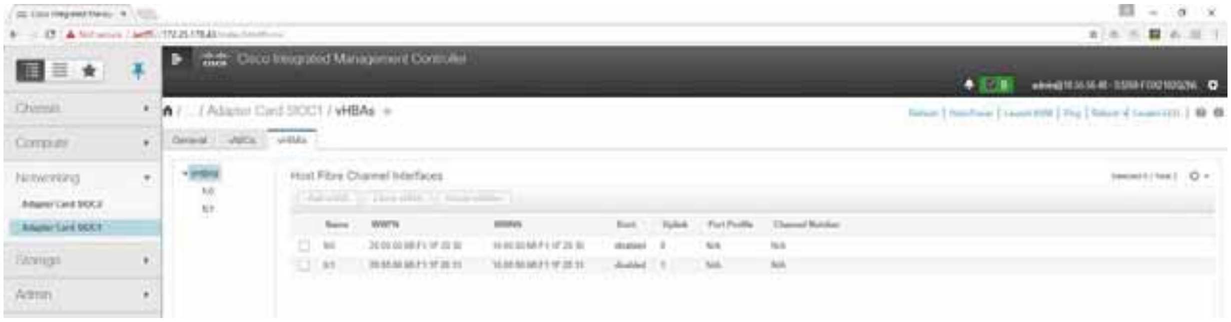


The second SIOC is required only if two nodes are installed.





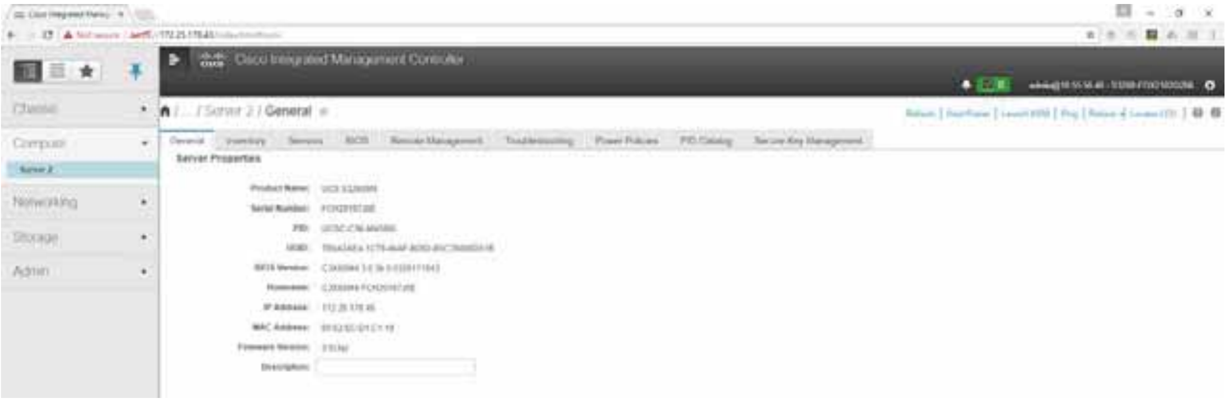
	Name	CDN	MAC Address	MTU	usNIC	Uplink Port	CoS	VLAN	VLAN Mode	iSCSI Boot	PXE Boot	Channel	Port Profile	Uplink Failover
□	eth0	VIC-1-eth0	[illegible]	1500	0	0	0	NONE	TRUNK	disabled	enabled	N/A	N/A	N/A
□	eth1	VIC-1-eth1	[illegible]	1500	0	1	0	NONE	TRUNK	disabled	enabled	N/A	N/A	N/A



	Name	WWPN	WWNN	Boot	Uplink	Port Profile	Channel Number
□	fc0	[illegible]	[illegible]	disabled	0	N/A	N/A
□	fc1	[illegible]	[illegible]	disabled	1	N/A	N/A

Choose Compute.

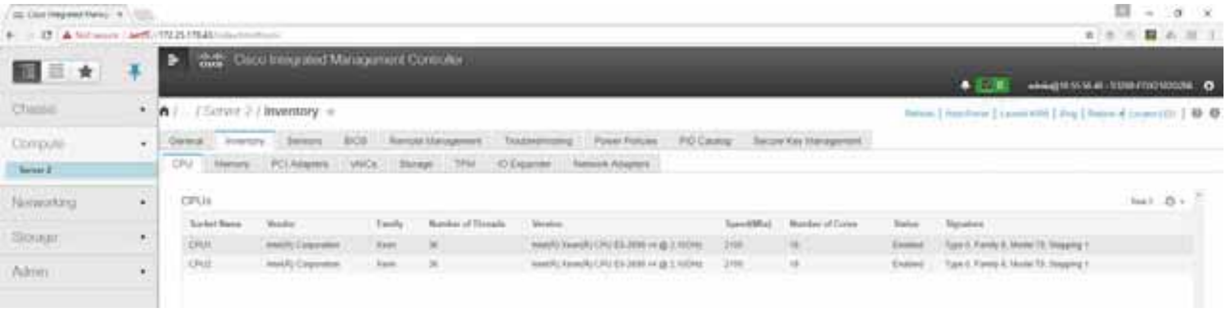
The Compute area summarizes the details of the server node, including information about the CPU, memory, PCIe cards, and local storage.



Server Properties

Product Name: [illegible]
Serial Number: [illegible]
PID: [illegible]
UUID: [illegible]
BIOS Version: [illegible]
Hostname: [illegible]
IP Address: [illegible]
MAC Address: [illegible]
Firmware Version: [illegible]
Description:

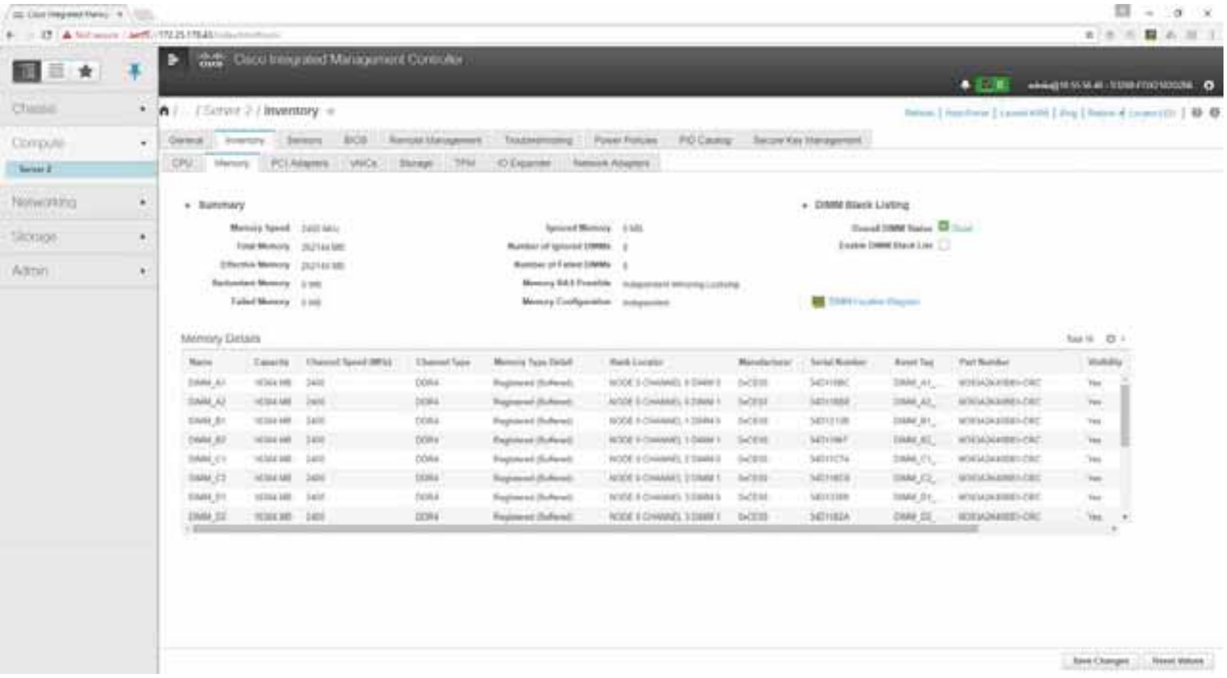
The CPU tab of the Inventory pane shows the CPUs.



CPUs

Socket Name	Vendor	Family	Number of Threads	Version	Speed(Mhz)	Number of Cores	Status	Signature
CPU1	Intel(R) Corporation	Xeon	36	Intel(R) Xeon(R) CPU E5-2695 v4 @ 2.10GHz	2100	18	Enabled	Type 0, Family 6, Model 79, Stepping 1
CPU2	Intel(R) Corporation	Xeon	36	Intel(R) Xeon(R) CPU E5-2695 v4 @ 2.10GHz	2100	18	Enabled	Type 0, Family 6, Model 79, Stepping 1

The Memory tab of the Inventory pane presents memory details.



Summary

Memory Speed: 2400 MHz
Total Memory: 262144 MB
Effective Memory: 262144 MB
Redundant Memory: 0 MB
Failed Memory: 0 MB
Ignored Memory: 0 MB
Number of Ignored DIMMs: 0
Number of Failed DIMMs: 0
Memory RAS Possible: Independent Mirroring Lockstep
Memory Configuration: Independent

DIMM Black Listing

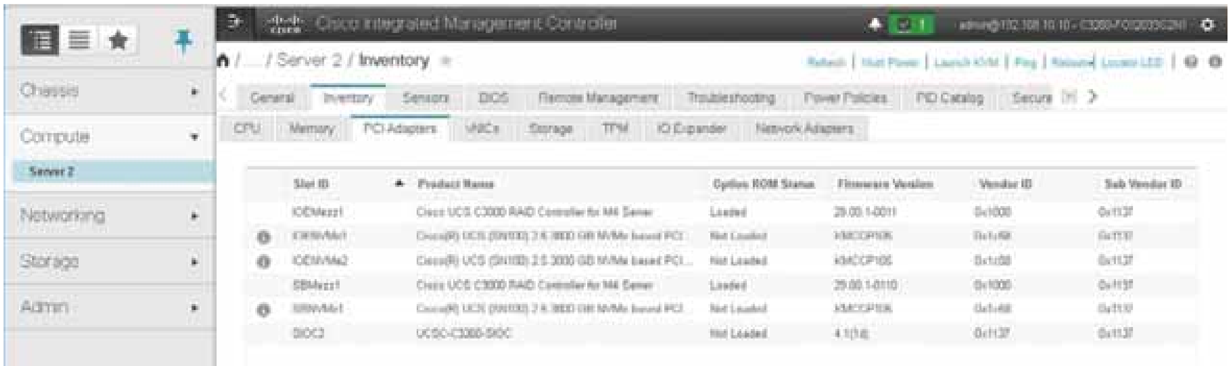
Overall DIMM Status: ☑ Good
Enable DIMM Black List: □

DIMM Location Diagram

Memory Details

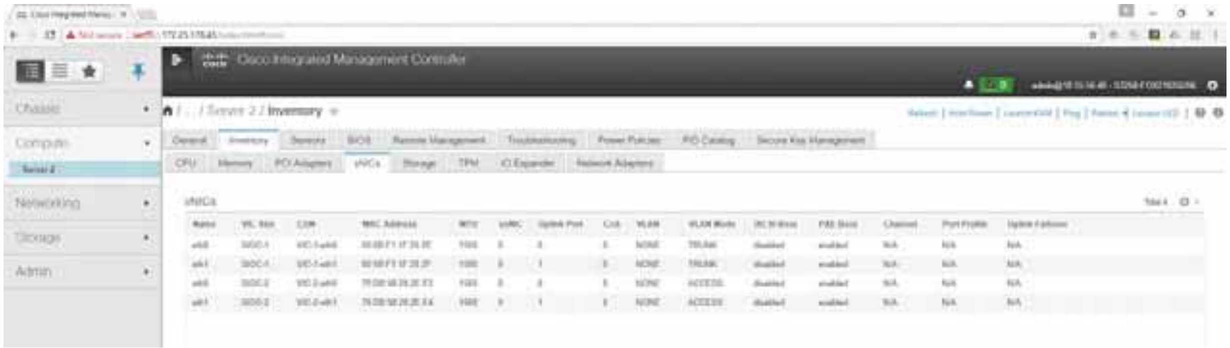
Name	Capacity	Channel Speed (MHz)	Channel Type	Memory Type Detail	Rank Locator	Manufacturer	Serial Number	Asset Tag	Part Number	Visibility
DIMM_A1	16384 MB	2400	DDR4	Registered (Buffered)	NODE 0 CHANNEL 0 DIMM 0	0xCE00	[illegible]	DIMM_A1_	[illegible]	Yes
DIMM_A2	16384 MB	2400	DDR4	Registered (Buffered)	NODE 0 CHANNEL 0 DIMM 1	0xCE00	[illegible]	DIMM_A2_	[illegible]	Yes
DIMM_B1	16384 MB	2400	DDR4	Registered (Buffered)	NODE 0 CHANNEL 1 DIMM 0	0xCE00	[illegible]	DIMM_B1_	[illegible]	Yes
DIMM_B2	16384 MB	2400	DDR4	Registered (Buffered)	NODE 0 CHANNEL 1 DIMM 1	0xCE00	[illegible]	DIMM_B2_	[illegible]	Yes
DIMM_C1	16384 MB	2400	DDR4	Registered (Buffered)	NODE 0 CHANNEL 2 DIMM 0	0xCE00	[illegible]	DIMM_C1_	[illegible]	Yes
DIMM_C2	16384 MB	2400	DDR4	Registered (Buffered)	NODE 0 CHANNEL 2 DIMM 1	0xCE00	[illegible]	DIMM_C2_	[illegible]	Yes
DIMM_D1	16384 MB	2400	DDR4	Registered (Buffered)	NODE 0 CHANNEL 3 DIMM 0	0xCE00	[illegible]	DIMM_D1_	[illegible]	Yes
DIMM_D2	16384 MB	2400	DDR4	Registered (Buffered)	NODE 0 CHANNEL 3 DIMM 1	0xCE00	[illegible]	DIMM_D2_	[illegible]	Yes

The S3260 SIOC is connected through PCIe and shown on the PCI Adapters tab.



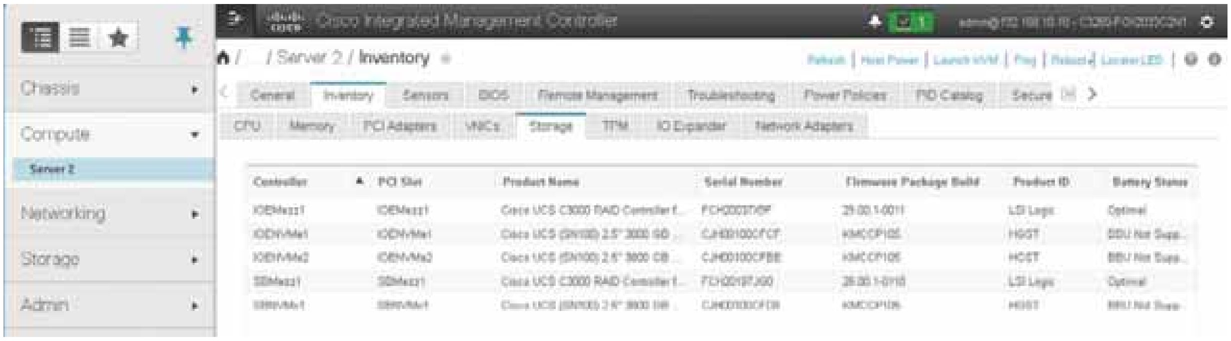
Slot ID	Product Name	Option ROM Status	Firmware Version	Vendor ID	Sub Vendor ID
IOEMezz1	Cisco UCS C3000 RAID Controller for M4 Server	Loaded	29.00.1-0011	0x1000	0x1137
IOENVMe1	Cisco(R) UCS (SN100) 2.5 3800 GB NVMe based PCI	Not Loaded	KMCCP106	0x1c58	0x1137
IOENVMe2	Cisco(R) UCS (SN100) 2.5 3000 GB NVMe based PCI...	Not Loaded	KMCCP105	0x1c58	0x1137
SBMezz1	Cisco UCS C3000 RAID Controller for M4 Server	Loaded	29.00.1-0110	0x1000	0x1137
SBNVMe1	Cisco(R) UCS (SN100) 2.5 3800 GB NVMe based PCI	Not Loaded	KMCCP106	0x1c58	0x1137
SIOC2	UCSC-C3260-SIOC	Not Loaded	4.1(1d)	0x1137	0x1137

The vNICs tab of the Inventory pane shows the vNICs.



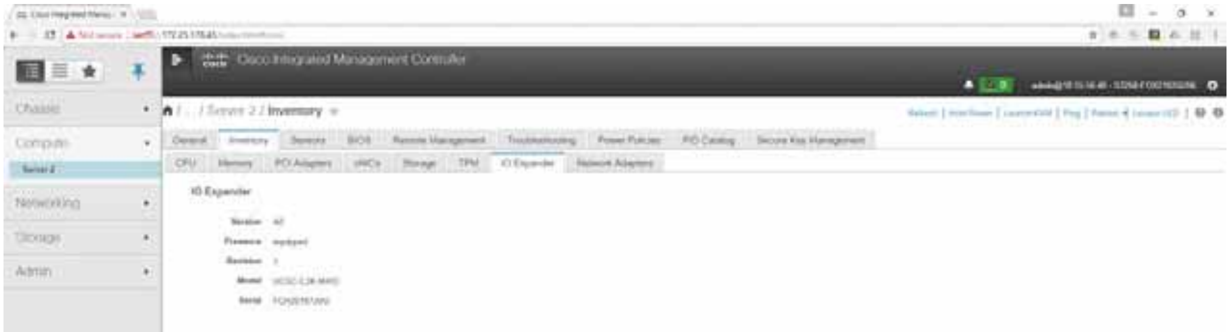
Name	VIC Slot	CDN	MAC Address	MTU	usNIC	Uplink Port	CoS	VLAN	VLAN Mode	iSCSI Boot	PXE Boot	Channel	Port Profile	Uplink Failover
eth0	SIOC-1	VIC-1-eth0	[illegible]	1500	0	0	0	NONE	TRUNK	disabled	enabled	N/A	N/A	N/A
eth1	SIOC-1	VIC-1-eth1	[illegible]	1500	0	1	0	NONE	TRUNK	disabled	enabled	N/A	N/A	N/A
eth0	SIOC-2	VIC-2-eth0	[illegible]	1500	0	0	0	NONE	ACCESS	disabled	enabled	N/A	N/A	N/A
eth1	SIOC-2	VIC-2-eth1	[illegible]	1500	0	1	0	NONE	ACCESS	disabled	enabled	N/A	N/A	N/A

The Storage tab of the Inventory pane shows the storage controller information.



Controller	PCI Slot	Product Name	Serial Number	Firmware Package Build	Product ID	Battery Status
IOEMezz1	IOEMezz1	Cisco UCS C3000 RAID Controller f...	FCH20037V5F	29.00.1-0011	LSI Logic	Optimal
IOENVMe1	IOENVMe1	Cisco UCS (SN100) 2.5" 3000 GB ...	CJH00100CFCF	KMCCP105	HGST	BBU Not Supp...
IOENVMe2	IOENVMe2	Cisco UCS (SN100) 2.5" 3800 GB ...	CJH00100CFBE	KMCCP105	HGST	BBU Not Supp...
SBMezz1	SBMezz1	Cisco UCS C3000 RAID Controller f...	FCH20197J00	28.00.1-0110	LSI Logic	Optimal
SBNVMe1	SBNVMe1	Cisco UCS (SN100) 2.5" 3800 GB ...	CJH00100CFD8	KMCCP105	HGST	BBU Not Supp...

If the S3260 is equipped with an I/O expander board for installing PCIe cards or additional Non-Volatile Memory Express (NVMe) devices, the details are shown on the IO Expander tab.



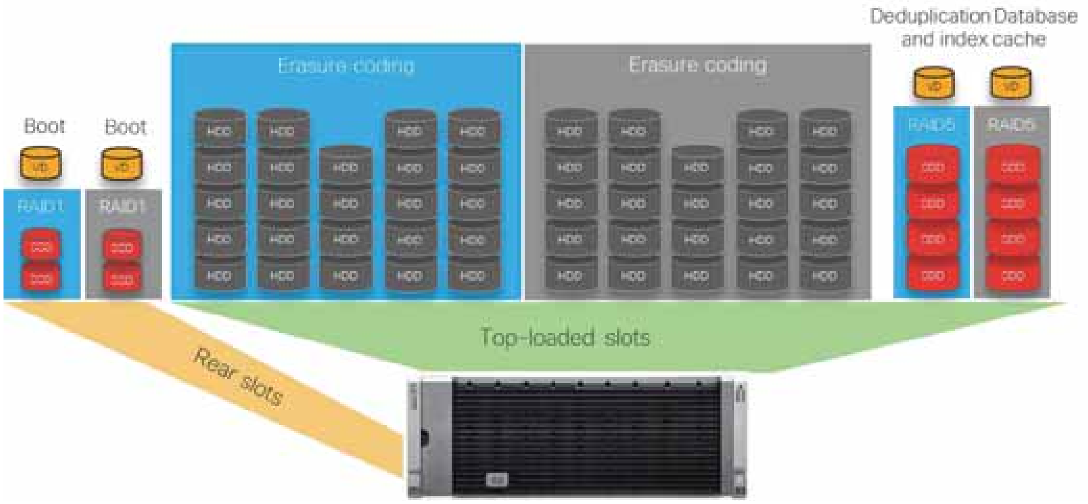
IO Expander

Version: A0
Presence: equipped
Revision: 0
Model: UCSC-C3K-M4IO
Serial: FCH2016T[illegible]

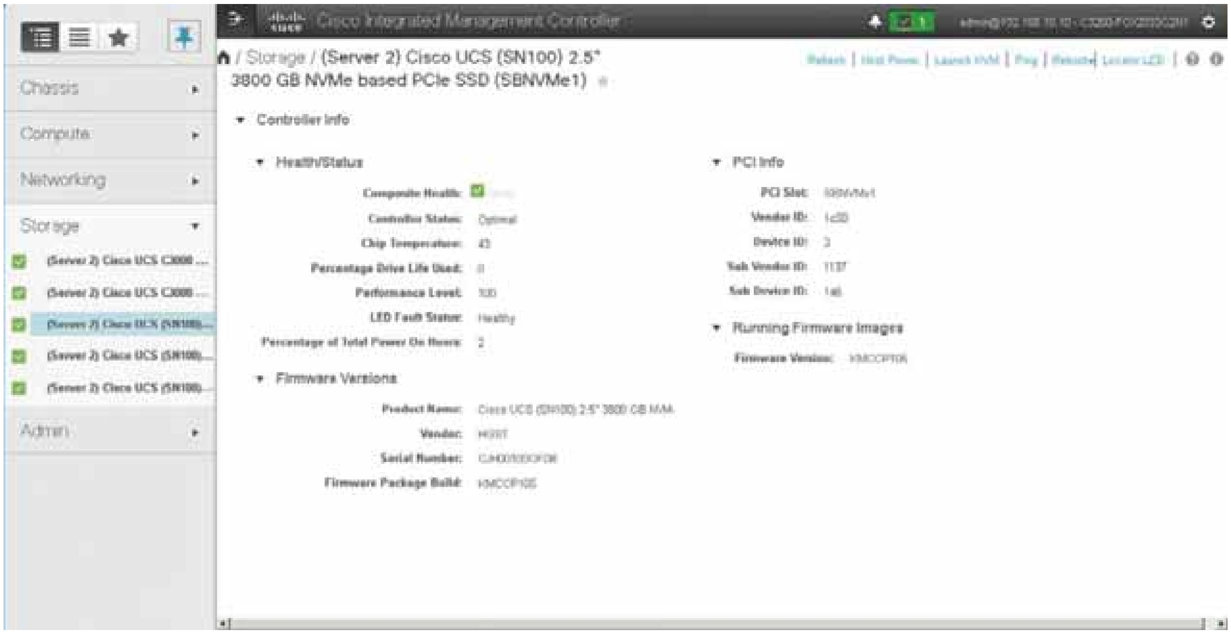
Choose Storage.

The storage configuration is an important part of the Cisco UCS S3260 configuration for Commvault ScaleProtect. To demonstrate the required storage configuration, Figure 7 shows the HDD and SSD components and the layout.

Figure 7. Cisco UCS S3260 storage layout



The Storage pane shows the NVMe details, RAID controller information, physical drive and virtual drive information, and RAID settings.


Cisco Integrated Management Controller
Chassis
Compute
Networking
Storage
(Server 2) Cisco UCS C3000 ...
(Server 2) Cisco UCS C3000 ...
(Server 2) Cisco UCS (SN100)...
(Server 2) Cisco UCS (SN100)...
(Server 2) Cisco UCS (SN100)...
Admin
Refresh | Host Power | Launch KVM | Ping | Reboot | Locator LED

/ Storage / (Server 2) Cisco UCS (SN100) 2.5" 3800 GB NVMe based PCIe SSD (SBNVMe1)

▾ Controller Info

▾ Health/Status

Composite Health: ☑ Good
Controller Status: Optimal
Chip Temperature: 43
Percentage Drive Life Used: 0
Performance Level: 100
LED Fault Status: Healthy
Percentage of Total Power On Hours: 2

▾ Firmware Versions

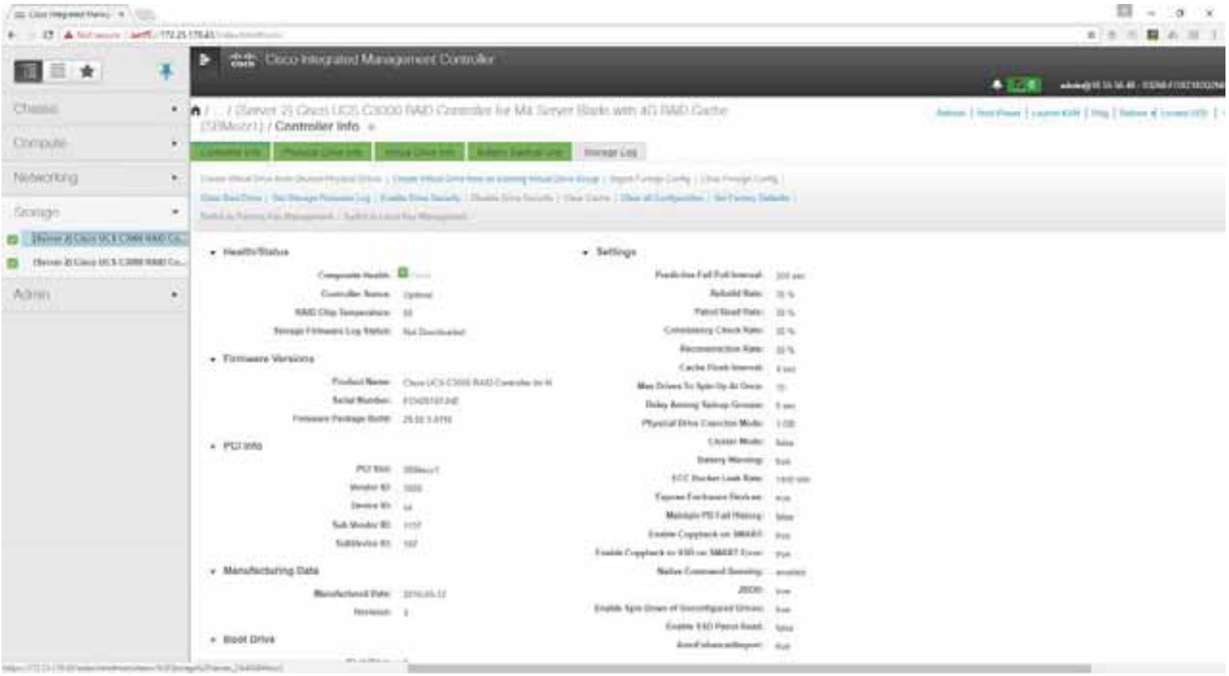
Product Name: Cisco UCS (SN100) 2.5" 3800 GB NVMe
Vendor: HGST
Serial Number: CJH0010D0F08
Firmware Package Build: KMCCP105

▾ PCI Info

PCI Slot: SBNVMe1
Vendor ID: 1c58
Device ID: 3
Sub Vendor ID: 1137
Sub Device ID: 1a6

▾ Running Firmware Images

Firmware Version: KMCCP105



/ ... / (Server 2) Cisco UCS C3000 RAID Controller for M4 Server Blade with 4G RAID Cache (SBMezz1) / Controller Info

Create Virtual Drive from Unused Physical Drives | Create Virtual Drive from an Existing Virtual Drive Group | Import Foreign Config | Clear Foreign Config | Clear Boot Drive | Get Storage Firmware Log | Enable Drive Security | Disable Drive Security | Clear Cache | Clear all Configuration | Set Factory Defaults | Switch to Remote Key Management | Switch to Local Key Management

Health/Status

Composite Health: Good
Controller Status: Optimal
RAID Chip Temperature: 55
Storage Firmware Log Status: Not Downloaded

Firmware Versions

Product Name: Cisco UCS C3000 RAID Controller for M
Serial Number: FCH2S1S7JHE
Firmware Package Build: 29.13.1-0116

PCI Info

PCI Slot: SBMezz1
Vendor ID: 1000
Device ID: 14
SubVendor ID: 1137
SubDevice ID: 187

Manufacturing Data

Manufactured Date: 2016-05-12
Revision: 1

Boot Drive

Settings

Predictive Fail Poll Interval: 300 sec
Rebuild Rate: 30 %
Patrol Read Rate: 30 %
Consistency Check Rate: 30 %
Reconstruction Rate: 30 %
Cache Flush Interval: 4 sec
Max Drives To Spin Up At Once: 10
Delay Among Spinup Groups: 5 sec
Physical Drive Coercion Mode: 1 GB
Cluster Mode: false
Battery Warning: true
ECC Bucket Leak Rate: 1440 min
Expose Enclosure Devices: true
Maintain PD Fail History: false
Enable Copyback on SMART: true
Enable Copyback to SSD on SMART Error: true
Native Command Queuing: enabled
JBOD: true
Enable Spin Down of Unconfigured Drives: true
Enable SSD Patrol Read: false
AutoEnhancedImport: true

Choose Chassis.

The RAID controller will see only the physical drives that are zoned for it in the Chassis area.

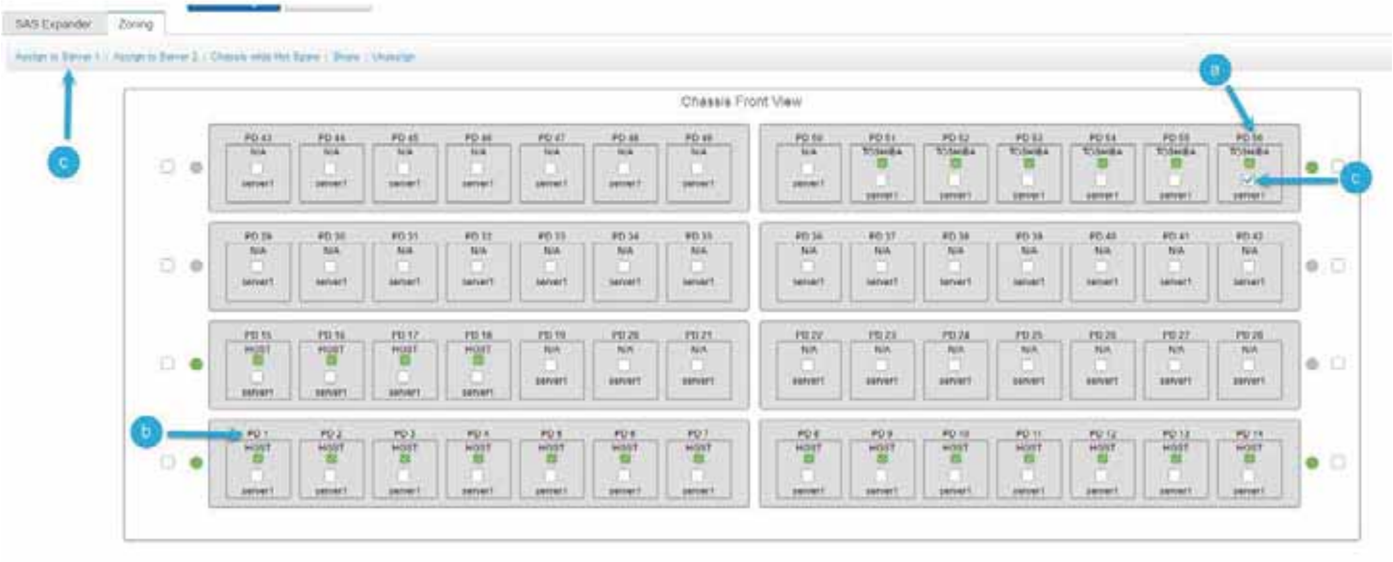
In the Chassis area, choose Inventory > Dynamic Storage. On this screen, click the Zoning tab.

On the zoning page there are a few things to check:

- The SSD drives should start in PD 56, going down.
- The HDD drives should start in PD 1 going up.

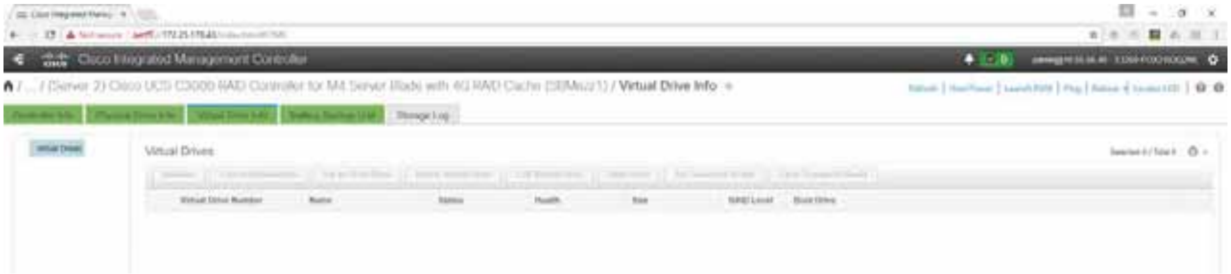
Select the drives PD1 to PD24 and PD49 to 52 and click Assign to Server 1. Then click Save Changes.

Select the drives PD25 to PD48 and PD53 to 56 and click Assign to Server 2. Then click Save Changes.

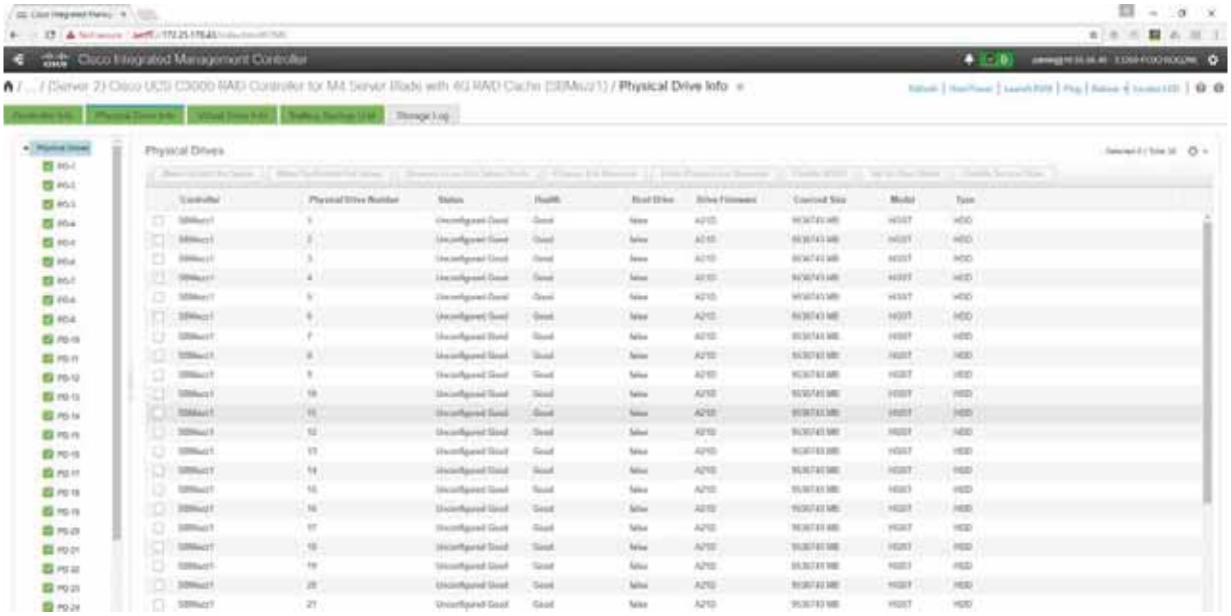


Give the system some time to complete the zoning process. Power on the server node so that the physical disk devices are discovered by the RAID controller before you start creating virtual drive groups and virtual drives in the Storage area.

In the Virtual Drive Info pane, no virtual drives should be listed. Remove any virtual drives that appear in this initial configuration.

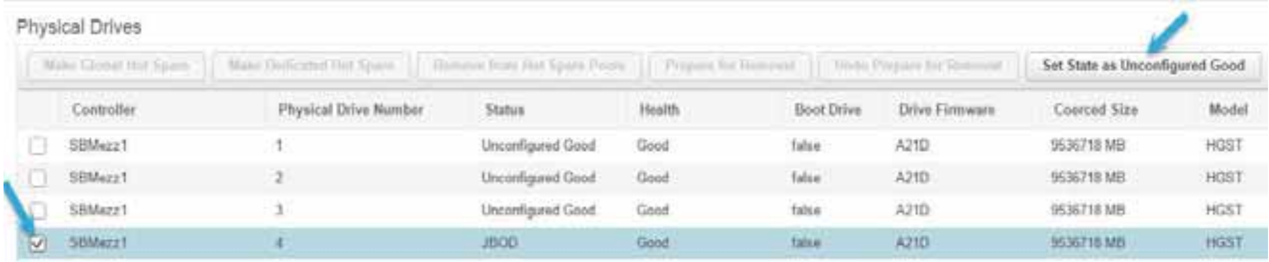

Cisco Integrated Management Controller
/ ... / (Server 2) Cisco UCS C3000 RAID Controller for M4 Server Blade with 4G RAID Cache (SBMezz1) / Virtual Drive Info
Controller Info
Physical Drive Info
Virtual Drive Info
Battery Backup Unit
Storage Log
Virtual Drives
Virtual Drive Number
Name
Status
Health
Size
RAID Level
Boot Drive

In the Physical Drive Info pane, the drives should be listed as Unconfigured Good for all SSDs or as JBOD for all HDDs.


Cisco Integrated Management Controller
/ ... / (Server 2) Cisco UCS C3000 RAID Controller for M4 Server Blade with 4G RAID Cache (SBMezz1) / Physical Drive Info
Controller Info
Physical Drive Info
Virtual Drive Info
Battery Backup Unit
Storage Log
Physical Drives

	Controller	Physical Drive Number	Status	Health	Boot Drive	Drive Firmware	Coerced Size	Model	Type
□	SBMezz1	1	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	2	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	3	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	4	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	5	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	6	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	7	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	8	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	9	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	10	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	11	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	12	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	13	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	14	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	15	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	16	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	17	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	18	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	19	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	20	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD
□	SBMezz1	21	Unconfigured Good	Good	false	A21D	9536743 MB	HGST	HDD

If not, select the drive and then click Set State as Unconfigured Good or Enable JBOD at the upper right.



	Controller	Physical Drive Number	Status	Health	Boot Drive	Drive Firmware	Coerced Size	Model
□	SBMezz1	1	Unconfigured Good	Good	false	A21D	9536718 MB	HGST
□	SBMezz1	2	Unconfigured Good	Good	false	A21D	9536718 MB	HGST
□	SBMezz1	3	Unconfigured Good	Good	false	A21D	9536718 MB	HGST
☑	SBMezz1	4	JBOD	Good	false	A21D	9536718 MB	HGST

To follow the guidelines for the Commvault ScaleProtect installation, the disk configurations listed in Tables 4 and 5 are required.

The IMC does not show the virtual disk group number. The numbers are used in this document only to show which LUNs exist in the same virtual device group.

Table 4. Virtual drive group 0 with disk 201 and 202 (SSDs in the back of the chassis)

Virtual drive group	LUN ID	Size	Used as
0	0	Fill to maximum	Boot and OS

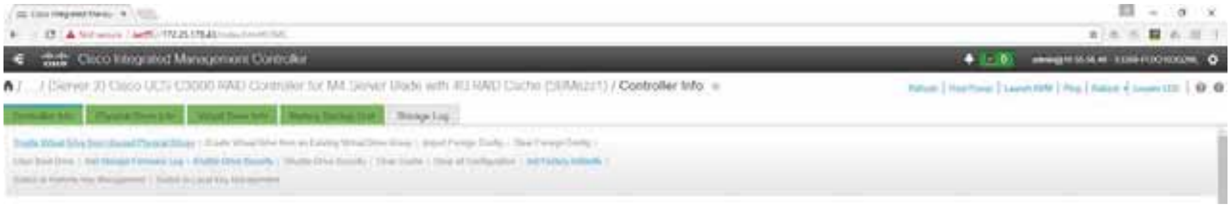
Table 5. Virtual drive group 1 with SSDs in the top of the chassis

Virtual drive group	LUN ID	Size	Used as
1	1	Fill to maximum	Index and deduplication database (DDB)

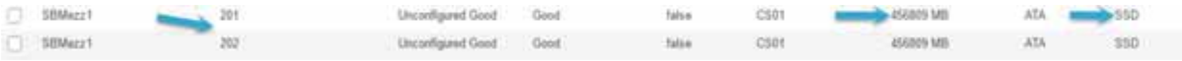
All top-loaded HDDs are used in JBOD mode; no RAID configuration is required.

Create virtual disk group 0.

On the Controller Info page, click Create Virtual Drive from Unused Physical Drives.


Cisco Integrated Management Controller
/ (Server 3) Cisco UCS C3000 RAID Controller for M4 Server Blade with 4G RAID Cache (SBMezz1) / Controller Info
Controller Info
Physical Drive Info
Virtual Drive Info
Battery Backup Unit
Storage Log
Create Virtual Drive from Unused Physical Drives

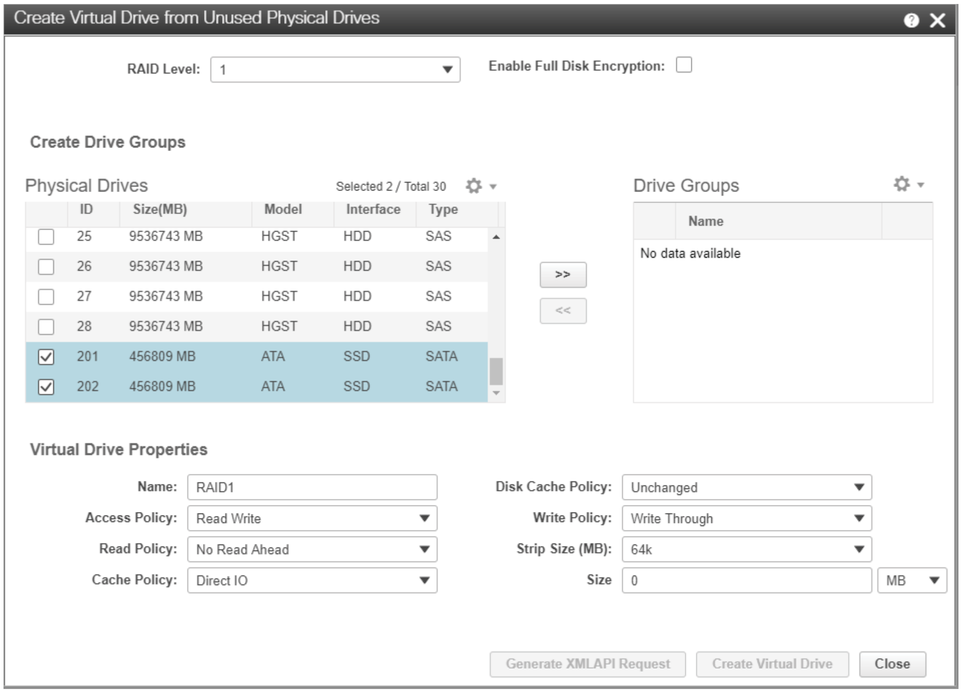
For the operating system and the active log, you must create a RAID 1 configuration on the two SSDs on the back of the chassis.



☐	SBMezz1	201	Unconfigured Good	Good	false	CS01	456809 MB	ATA	SSD
☐	SBMezz1	202	Unconfigured Good	Good	false	CS01	456809 MB	ATA	SSD

Select 1 as the RAID level.

Select physical drives 201 and 202 and add them to the drive group (click >>).



Create Virtual Drive from Unused Physical Drives

RAID Level: 1

Enable Full Disk Encryption: ☐

Create Drive Groups

Physical Drives — Selected 2 / Total 30

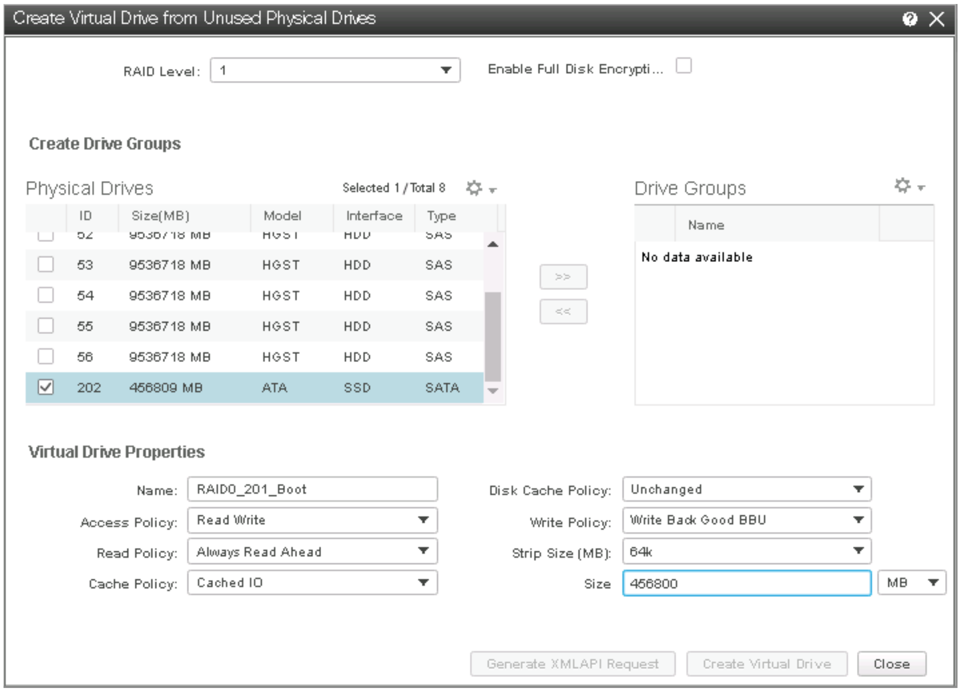
	ID	Size(MB)	Model	Interface	Type
☐	25	9536743 MB	HGST	HDD	SAS
☐	26	9536743 MB	HGST	HDD	SAS
☐	27	9536743 MB	HGST	HDD	SAS
☐	28	9536743 MB	HGST	HDD	SAS
☑	201	456809 MB	ATA	SSD	SATA
☑	202	456809 MB	ATA	SSD	SATA

Drive Groups

Name
No data available

Virtual Drive Properties

Name:	RAID1	Disk Cache Policy:	Unchanged
Access Policy:	Read Write	Write Policy:	Write Through
Read Policy:	No Read Ahead	Strip Size (MB):	64k
Cache Policy:	Direct IO	Size	0 MB



Create Virtual Drive from Unused Physical Drives

RAID Level: 1 　 Enable Full Disk Encrypti... □

Create Drive Groups

Physical Drives — Selected 1 / Total 8

	ID	Size(MB)	Model	Interface	Type
□	52	9536718 MB	HGST	HDD	SAS
□	53	9536718 MB	HGST	HDD	SAS
□	54	9536718 MB	HGST	HDD	SAS
□	55	9536718 MB	HGST	HDD	SAS
□	56	9536718 MB	HGST	HDD	SAS
☑	202	456809 MB	ATA	SSD	SATA

Drive Groups

Name
No data available

Virtual Drive Properties

Name: RAID0_201_Boot

Access Policy: Read Write

Read Policy: Always Read Ahead

Cache Policy: Cached IO

Disk Cache Policy: Unchanged

Write Policy: Write Back Good BBU

Strip Size (MB): 64k

Size 456800 MB

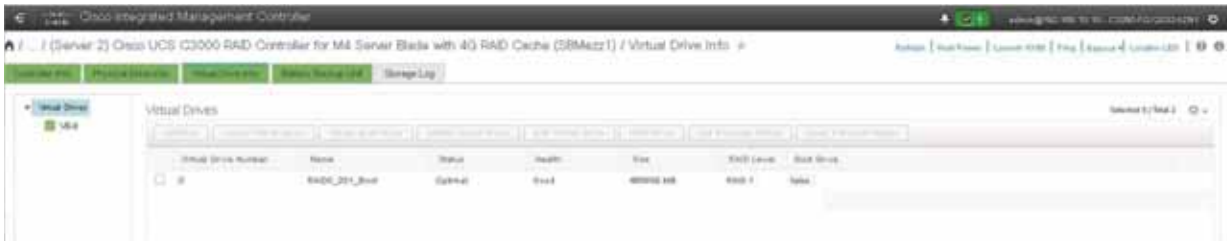
For the name, enter an obvious name.

Change Cache Policy from Direct IO to Cached IO

Change Write Policy from WriteThrough to Write Back Good BBU.

Enter **456800** as the size and select MB as the unit.

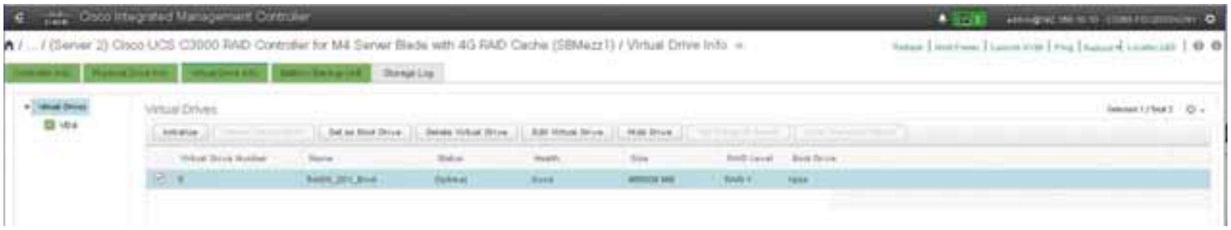
Go to the Virtual Drive Info tab and select the Boot virtual drive.



Cisco Integrated Management Controller

/ ... / (Server 2) Cisco UCS C3000 RAID Controller for M4 Server Blade with 4G RAID Cache (SBMezz1) / Virtual Drive Info

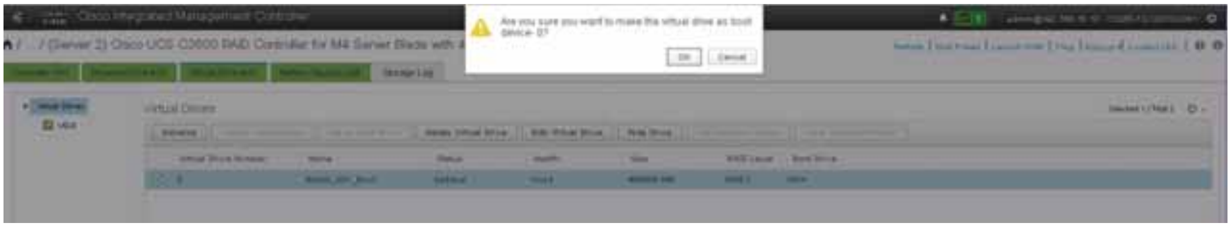
Click Set as Boot Drive.



Cisco Integrated Management Controller

/ ... / (Server 2) Cisco UCS C3000 RAID Controller for M4 Server Blade with 4G RAID Cache (SBMezz1) / Virtual Drive Info

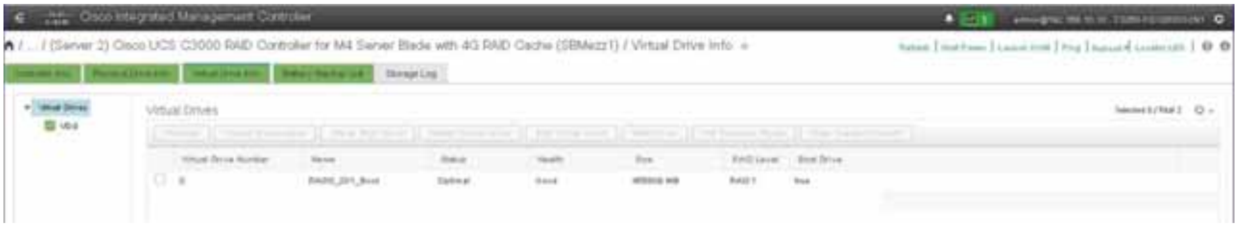
Confirm that you want to make the Boot virtual drive the boot drive.



Cisco Integrated Management Controller

Are you sure you want to make the virtual drive as boot device- 0?

OK | Cancel



Cisco Integrated Management Controller

/ ... / (Server 2) Cisco UCS C3000 RAID Controller for M4 Server Blade with 4G RAID Cache (SBMezz1) / Virtual Drive Info

Virtual Drives

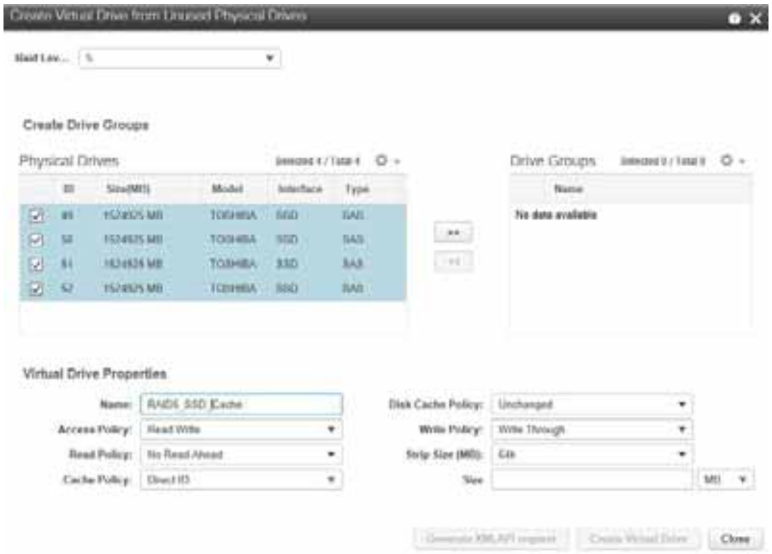
	Virtual Drive Number	Name	Status	Health	Size	RAID Level	Boot Drive
□	0	RAID1_201_Boot	Optimal	Good	[illegible] MB	RAID 1	true

Return to the Controller Info tab to create the additional virtual drive groups and virtual drives.

Click Create Virtual Drive from Unused Physical Drives.

Select 5 as the RAID level.

Select physical drives 49 through 52 and add them to the drive group (click >>).



Create Virtual Drive from Unused Physical Drives

Raid Lev...: 5

Create Drive Groups

Physical Drives — Selected 4 / Total 4

	ID	Size(MB)	Model	Interface	Type
☑	49	1524825 MB	TOSHIBA	SSD	SAS
☑	50	1524825 MB	TOSHIBA	SSD	SAS
☑	51	1524825 MB	TOSHIBA	SSD	SAS
☑	52	1524825 MB	TOSHIBA	SSD	SAS

Drive Groups — Selected 0 / Total 0

Name
No data available

Virtual Drive Properties

Name: RAID5_SSD_Cache

Access Policy: Read Write

Read Policy: No Read Ahead

Cache Policy: Direct IO

Disk Cache Policy: Unchanged

Write Policy: Write Through

Strip Size (MB): 64k

Size: MB

Generate XML API request | Create Virtual Drive | Close

For the name, enter an obvious name.

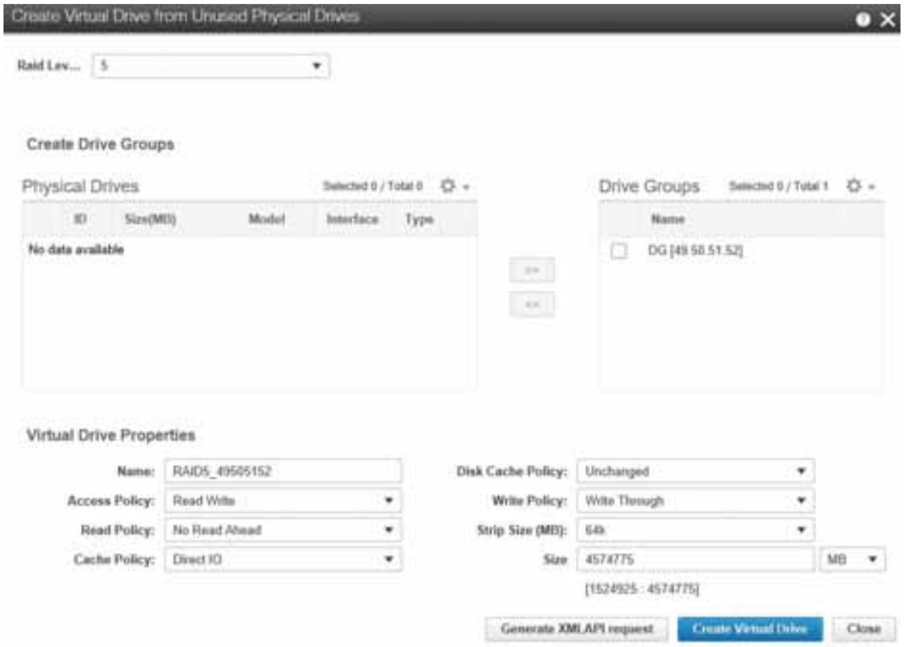
Change Read Policy to Always Read Ahead.

Change Cache Policy to Cached IO.

Change Write Policy to Write Back Good BBU.

Enter a maximum size and change the unit to GB.

Click Create Virtual Drive.



Create Virtual Drive from Unused Physical Drives

Raid Lev...: 5

Create Drive Groups

Physical Drives — Selected 0 / Total 0

ID	Size(MB)	Model	Interface	Type
No data available				

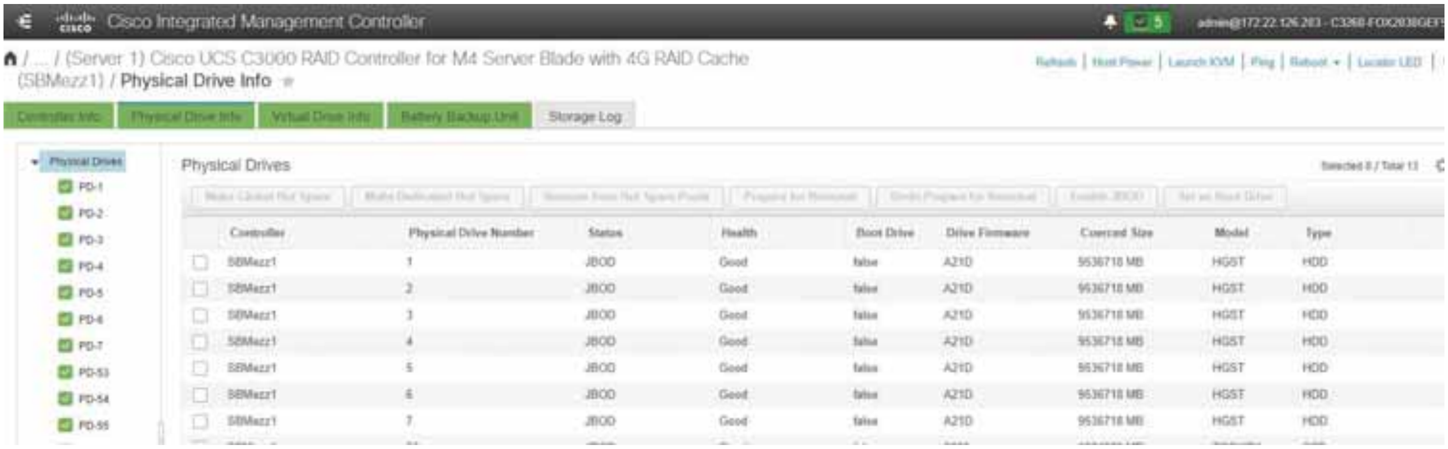
Drive Groups — Selected 0 / Total 1

	Name
□	DG [49.50.51.52]

Virtual Drive Properties

Name:	RAID5_49505152	Disk Cache Policy:	Unchanged
Access Policy:	Read Write	Write Policy:	Write Through
Read Policy:	No Read Ahead	Strip Size (MB):	64k
Cache Policy:	Direct IO	Size	4574775 MB
			[1524925 : 4574775]

For the SAS HDDs use JBOD mode, no additional configuration is required.



Cisco Integrated Management Controller — admin@172.22.126.203 - C3260-FOX2038GEF

/ ... / (Server 1) Cisco UCS C3000 RAID Controller for M4 Server Blade with 4G RAID Cache (SBMezz1) / Physical Drive Info

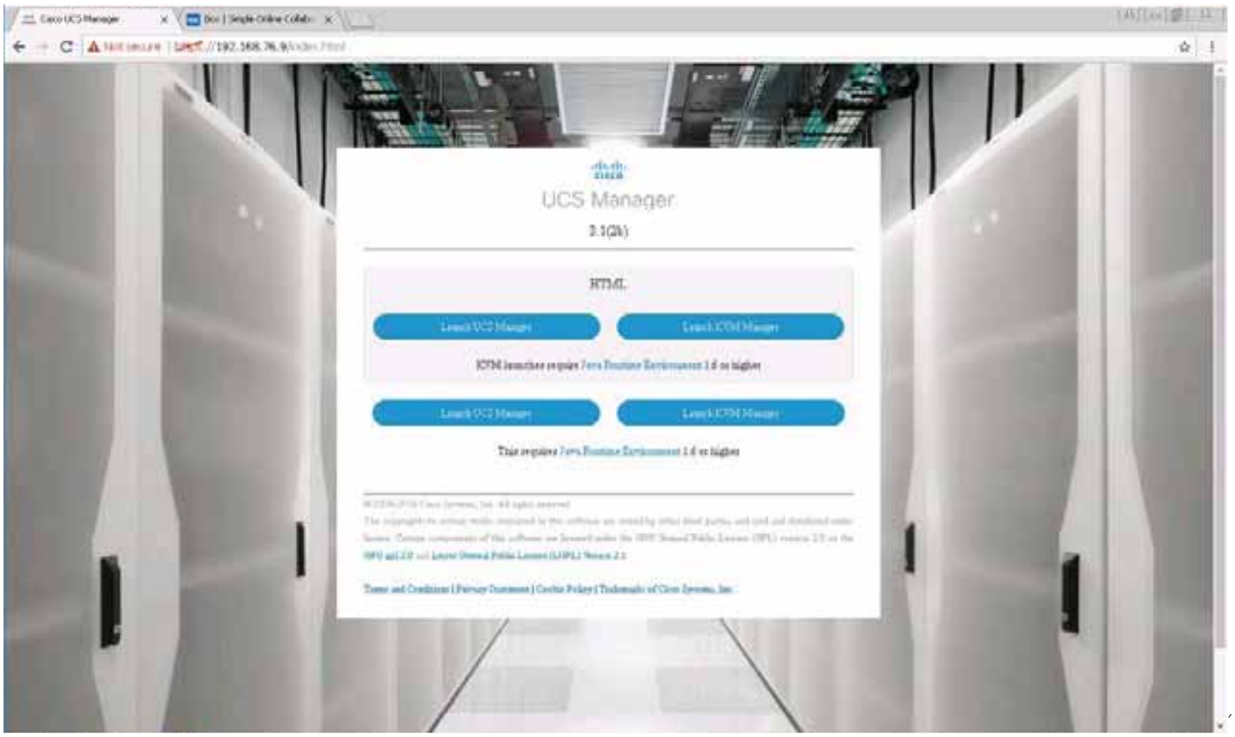
Physical Drives — Selected 0 / Total 13

	Controller	Physical Drive Number	Status	Health	Boot Drive	Drive Firmware	Coerced Size	Model	Type
□	SBMezz1	1	JBOD	Good	false	A21D	9536718 MB	HGST	HDD
□	SBMezz1	2	JBOD	Good	false	A21D	9536718 MB	HGST	HDD
□	SBMezz1	3	JBOD	Good	false	A21D	9536718 MB	HGST	HDD
□	SBMezz1	4	JBOD	Good	false	A21D	9536718 MB	HGST	HDD
□	SBMezz1	5	JBOD	Good	false	A21D	9536718 MB	HGST	HDD
□	SBMezz1	6	JBOD	Good	false	A21D	9536718 MB	HGST	HDD
□	SBMezz1	7	JBOD	Good	false	A21D	9536718 MB	HGST	HDD

The Cisco UCS configuration is now finished, and the Commvault ScaleProtect installation can start.

Cisco UCS managed configuration with Cisco UCS Manager

Log on to Cisco UCS Manager as the admin user or as another user with administrative rights.


Cisco UCS Manager
Not secure
https://192.168.76.9/index.html
UCS Manager
Launch UCS Manager
Launch KVM Manager
Launch UCS Manager
Launch KVM Manager
Terms and Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

UCS Manager

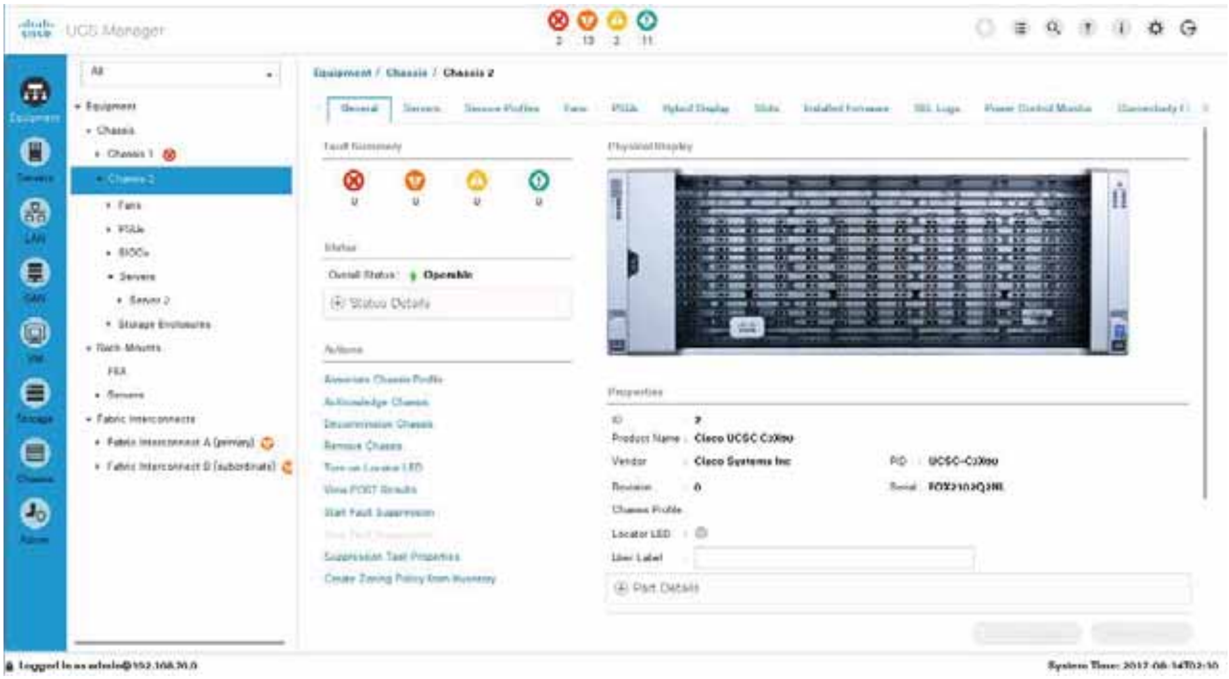
3.1(2b)

HTML

KVM launches require Java Runtime Environment 1.6 or higher

This requires Java Runtime Environment 1.6 or higher

On the Equipment tab, identify the Cisco UCS S3260 chassis and check the condition of the system and the components required for the deployment.



Overall Status : Operable

ID : 2

Product Name : Cisco UCSC C3X60

Vendor : Cisco Systems Inc   PID : UCSC-C3X60

Revision : 0   Serial : FOX2103Q2HL

Chassis Profile :

Locator LED :

User Label :

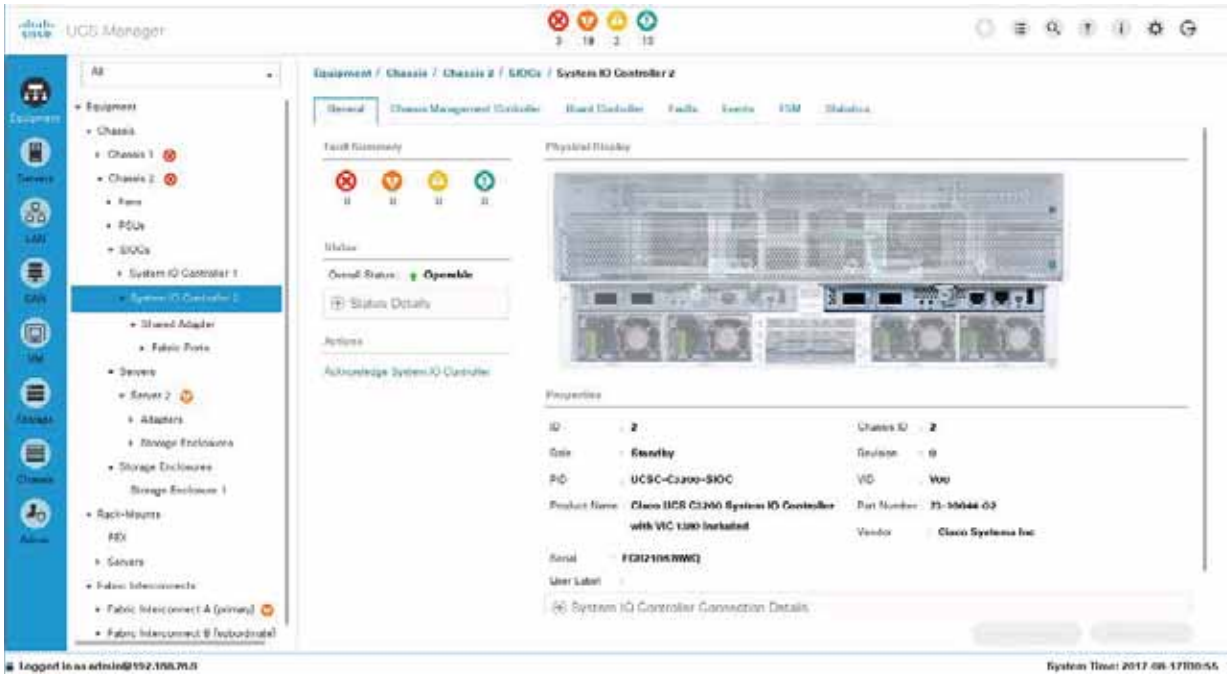
Logged in as admin@192.168.30.0

System Time: 2017-08-14T02:10

Check the SIOC Information.

One SIOC is required per server.

The General tab provides an overview of the SIOC and Ethernet ports, including the uplink status and port speeds. The operating speed can be 10 Gbps, 4 x 10 Gbps, or 40 Gbps. You should use 40 Gbps whenever possible.

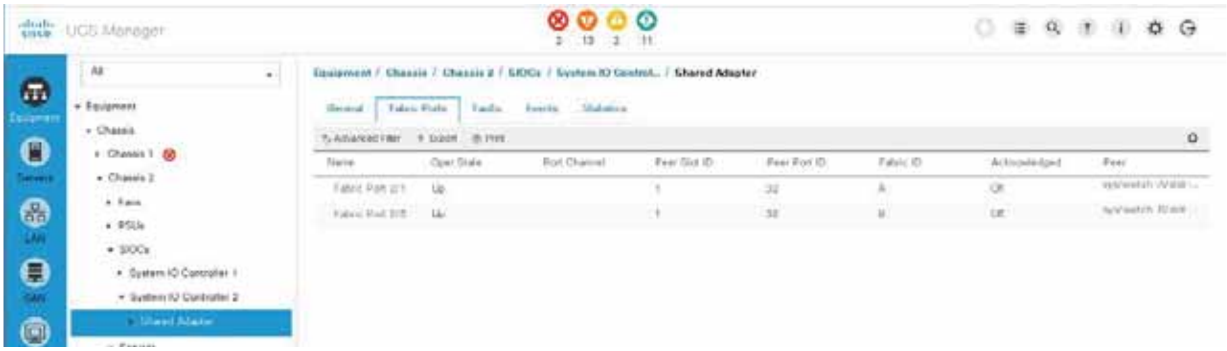


Overall Status : Operable

ID	: 2	Chassis ID	: 2
Role	: Standby	Revision	: 0
PID	: UCSC-C3260-SIOC	VID	: V00
Product Name	: Cisco UCS C3260 System IO Controller with VIC 1300 Included	Part Number	: 73-10044-02
		Vendor	: Cisco Systems Inc
Serial	: FCH2106706WQ		
User Label	:		

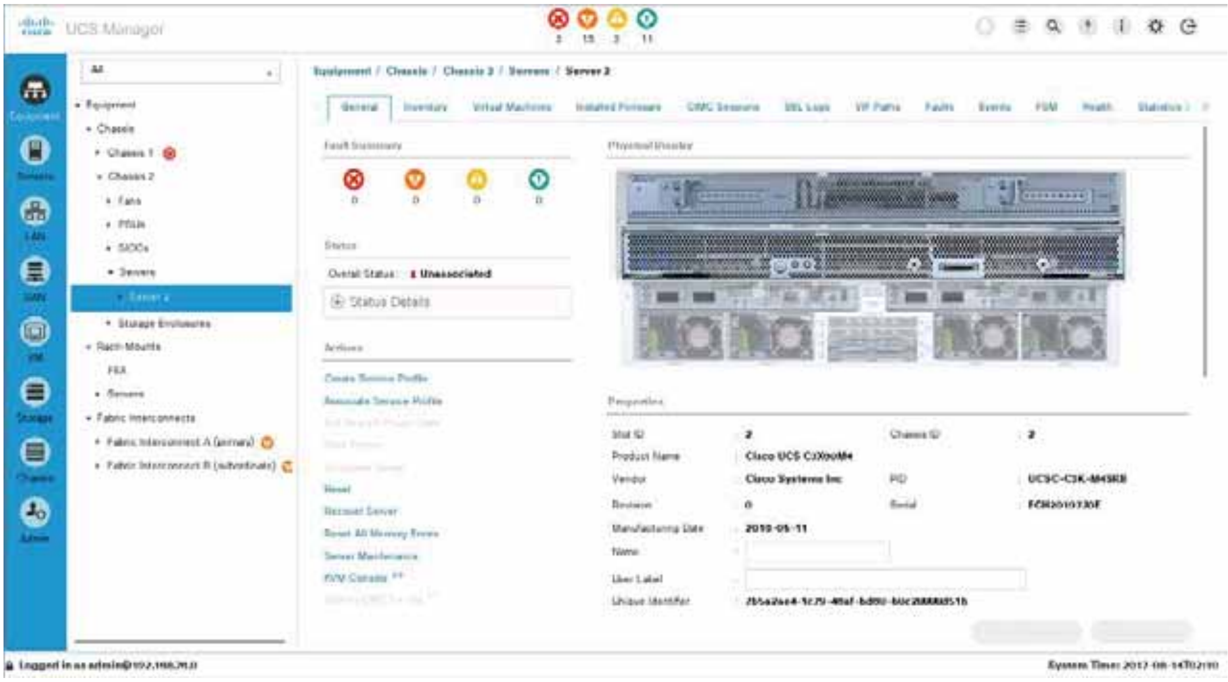
Logged in as admin@192.168.70.8

System Time: 2017-08-17T00:55



Name	Oper State	Port Channel	Peer Slot ID	Peer Port ID	Fabric ID	Acknowledged	Peer
Fabric Port 2/1	Up		1	32	A	OK	sys/switch-A/slot-...
Fabric Port 2/5	Up		1	32	B	OK	sys/switch-B/slot-...

The Servers area shows the details of the server node, including information about the CPU, memory, PCIe cards, and local storage.



Equipment / Chassis / Chassis 2 / Servers / Server 2

Overall Status: Unassociated

Properties

Slot ID: 2 Chassis ID: 2

Product Name: Cisco UCS C3X60M4

Vendor: Cisco Systems Inc PID: UCSC-C3K-M4SRB

Revision: 0 Serial: FCH2010730F

Manufacturing Date: 2016-05-11

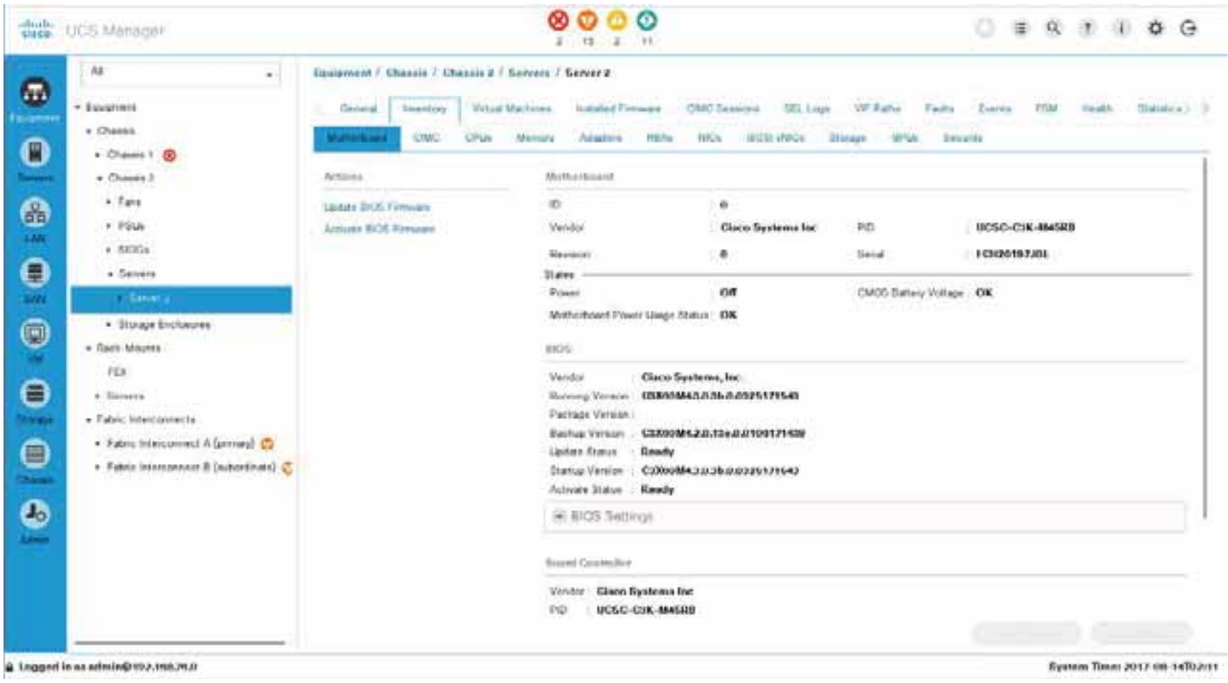
Name:

User Label:

Unique Identifier: 2b5a2ee4-1c79-4faf-bd80-b0c2888851b

Logged in as admin@192.168.20.0

System Time: 2017-08-14T02:10



Equipment / Chassis / Chassis 2 / Servers / Server 2

Motherboard

ID: 0

Vendor: Cisco Systems Inc PID: UCSC-C3K-M4SRB

Revision: 0 Serial: FCH2019[illegible]

States

Power: Off CMOS Battery Voltage: OK

Motherboard Power Usage Status: OK

BIOS

Vendor: Cisco Systems, Inc.

Running Version: C3X60M4.3.0.3b.0.0925171540

Package Version:

Backup Version: C3X60M4.2.0.13e.0.0100171439

Update Status: Ready

Startup Version: C3X60M4.3.0.3b.0.0925171540

Activate Status: Ready

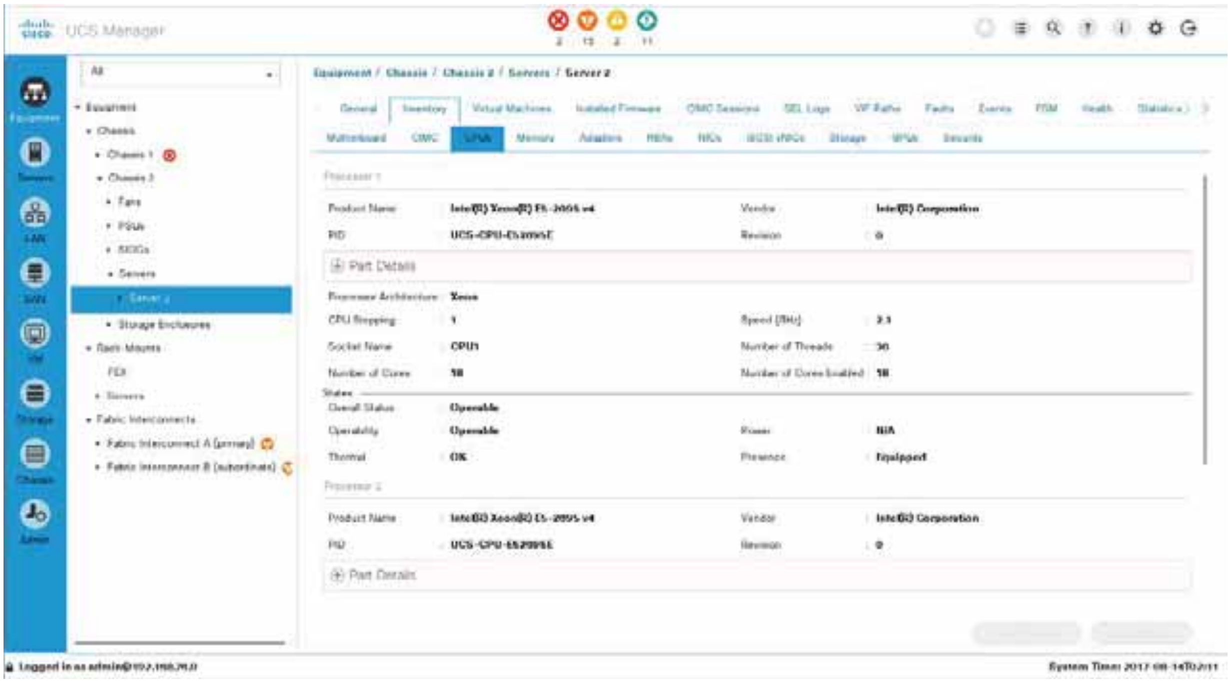
Board Controller

Vendor: Cisco Systems Inc

PID: UCSC-C3K-M4SRB

Logged in as admin@192.168.20.0

System Time: 2017-08-14T02:11



Equipment / Chassis / Chassis 2 / Servers / Server 2

Processor 1

Product Name : Intel(R) Xeon(R) E5-2695 v4
Vendor : Intel(R) Corporation
PID : UCS-CPU-E52695E
Revision : 0

⊕ Part Details

Processor Architecture : Xeon
CPU Stepping : 1
Speed (GHz) : 2.1
Socket Name : CPU1
Number of Threads : 36
Number of Cores : 18
Number of Cores Enabled : 18

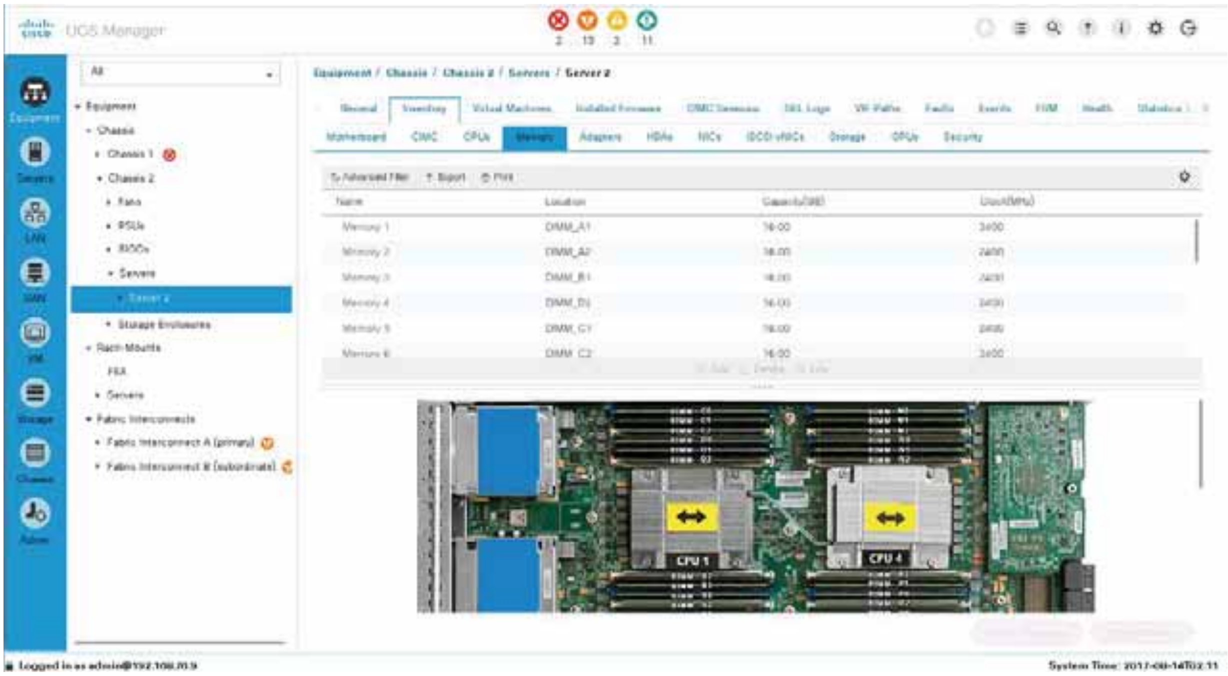
Status
Overall Status : Operable
Operability : Operable
Power : N/A
Thermal : OK
Presence : Equipped

Processor 2

Product Name : Intel(R) Xeon(R) E5-2695 v4
Vendor : Intel(R) Corporation
PID : UCS-CPU-E52695E
Revision : 0

⊕ Part Details

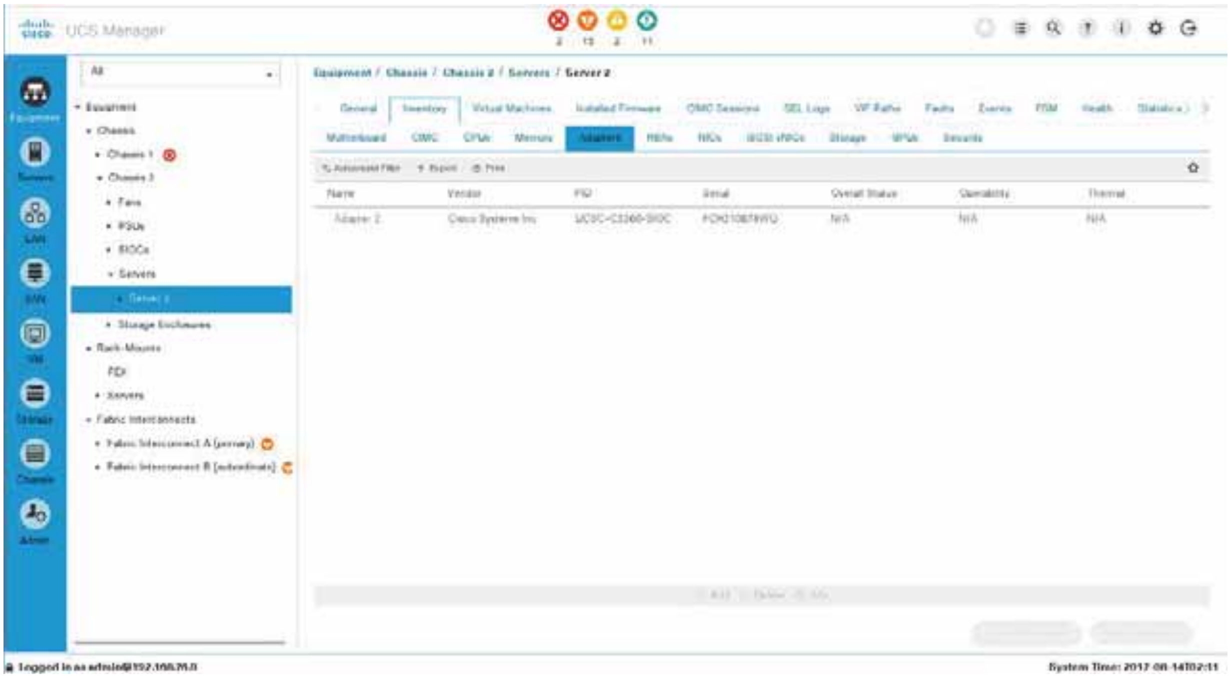
Logged in as admin@192.168.20.9
System Time: 2017-08-14T02:11



Equipment / Chassis / Chassis 2 / Servers / Server 2

Name	Location	Capacity(GB)	Clock(MHz)
Memory 1	DIMM_A1	16.00	2400
Memory 2	DIMM_A2	16.00	2400
Memory 3	DIMM_B1	16.00	2400
Memory 4	DIMM_B2	16.00	2400
Memory 5	DIMM_C1	16.00	2400
Memory 6	DIMM_C2	16.00	2400

Logged in as admin@192.168.20.9
System Time: 2017-08-14T02:11



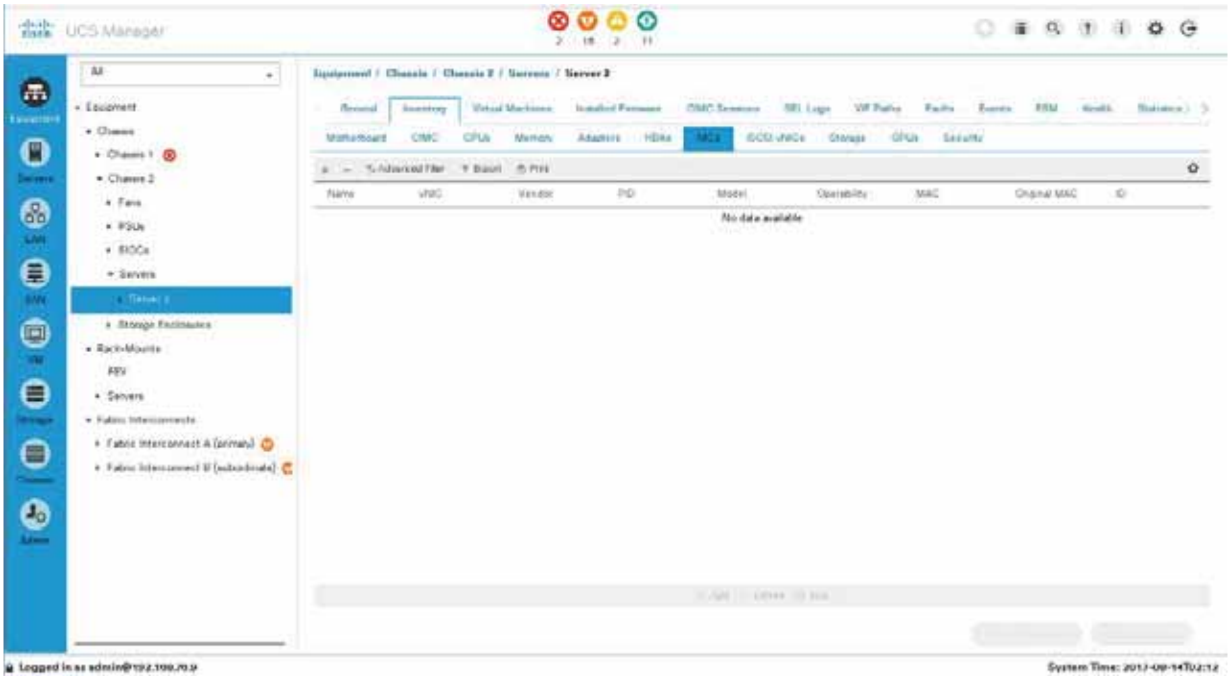
Equipment / Chassis / Chassis 2 / Servers / Server 2

Name	Vendor	PID	Serial	Overall Status	Operability	Thermal
Adapter 2	Cisco Systems Inc	UCSC-C3260-SIOC	FCH2108THWQ	N/A	N/A	N/A

Logged in as admin@192.168.76.8

System Time: 2017-08-14T02:11

In a standalone configuration, the SIOS includes predefined vNICs and vHBAs. In a configuration managed by Cisco UCS, however, nothing is defined. This definition is part of the service profile configuration. If PCIe cards for networking or Fibre Channel are installed, the information is listed on the NICs and HBAs tabs.



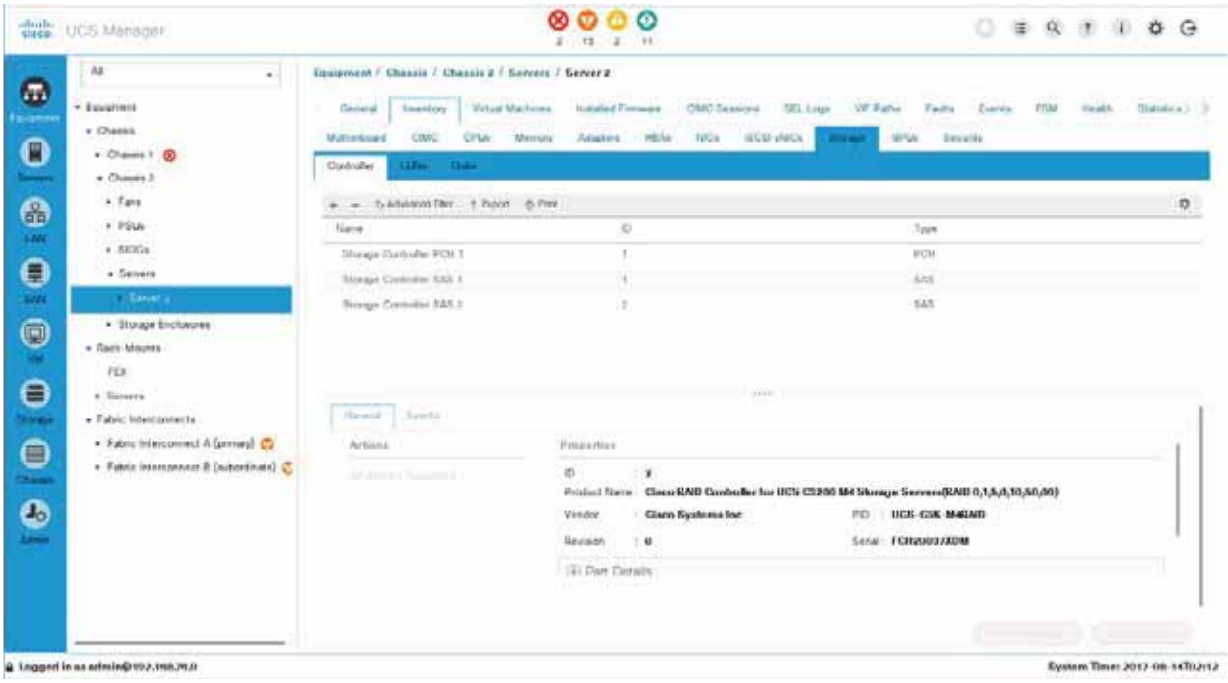
Equipment / Chassis / Chassis 2 / Servers / Server 2

Name	vNIC	Vendor	PID	Model	Operability	MAC	Original MAC	ID

No data available

Logged in as admin@192.168.76.9

System Time: 2017-08-14T02:12



Equipment / Chassis / Chassis 2 / Servers / Server 2

Name	ID	Type
Storage Controller PCH 1	1	PCH
Storage Controller SAS 1	1	SAS
Storage Controller SAS 2	2	SAS

Properties

ID : 2

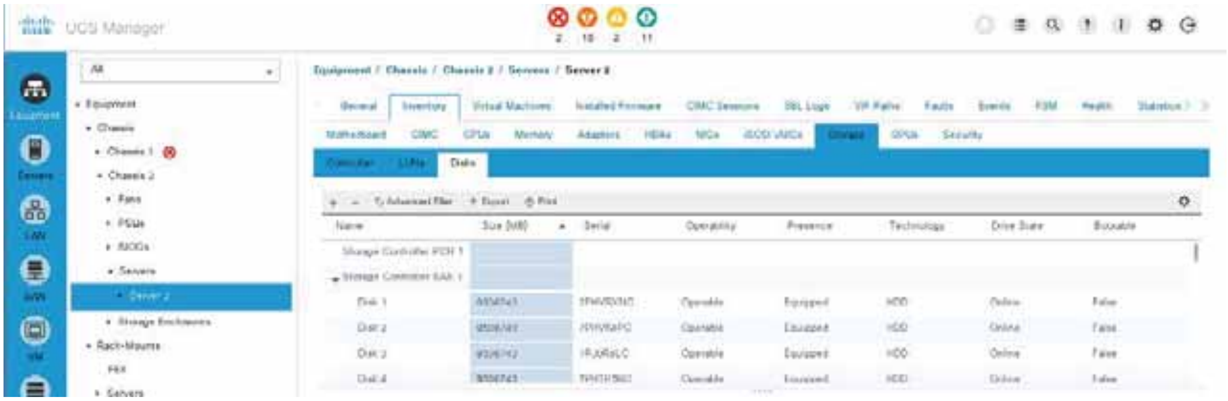
Product Name : Cisco RAID Controller for UCS C3260 M4 Storage Servers(RAID 0,1,5,6,10,50,60)

Vendor : Cisco Systems Inc PID : UCS-C3K-M4RAID

Revision : 0 Serial : FCH2003[illegible]

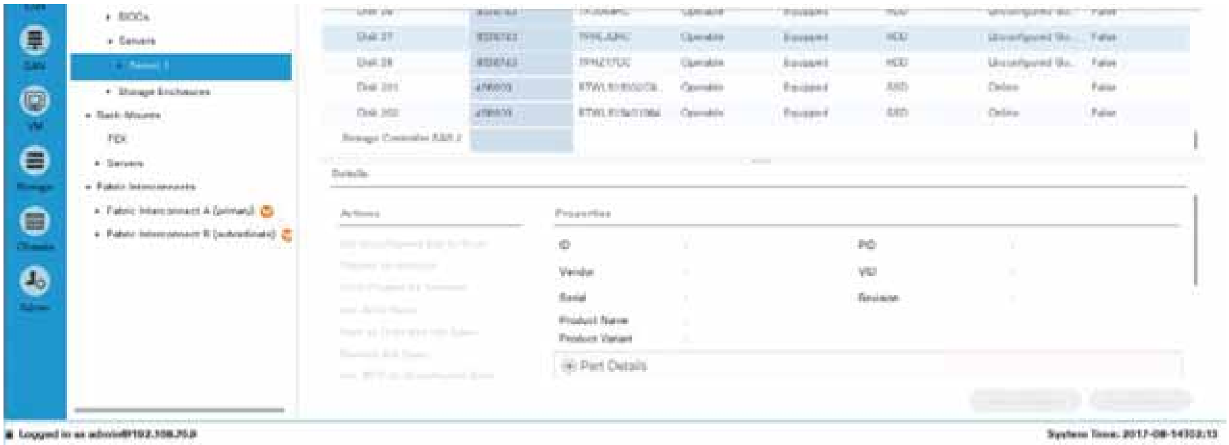
Logged in as admin@[illegible] System Time: 2017-08-14T02:12

To complete the storage configuration discussed later in this document, you need to identify the physical disks available for the operating system installation. The Cisco UCS S3260 chassis comes with four disk slots on the rear side, with disk numbers 201 through 205. Identify and note the disks that are available. In the example here, the available disks are 201 and 202.



Equipment / Chassis / Chassis 2 / Servers / Server 2

Name	Size (MB)	Serial	Operability	Presence	Technology	Drive State	Bootable
Storage Controller PCH 1							
Storage Controller SAS 1							
Disk 1	[illegible]	[illegible]	Operable	Equipped	HDD	Online	False
Disk 2	[illegible]	[illegible]	Operable	Equipped	HDD	Online	False
Disk 3	[illegible]	[illegible]	Operable	Equipped	HDD	Online	False
Disk 4	[illegible]	[illegible]	Operable	Equipped	HDD	Online	False



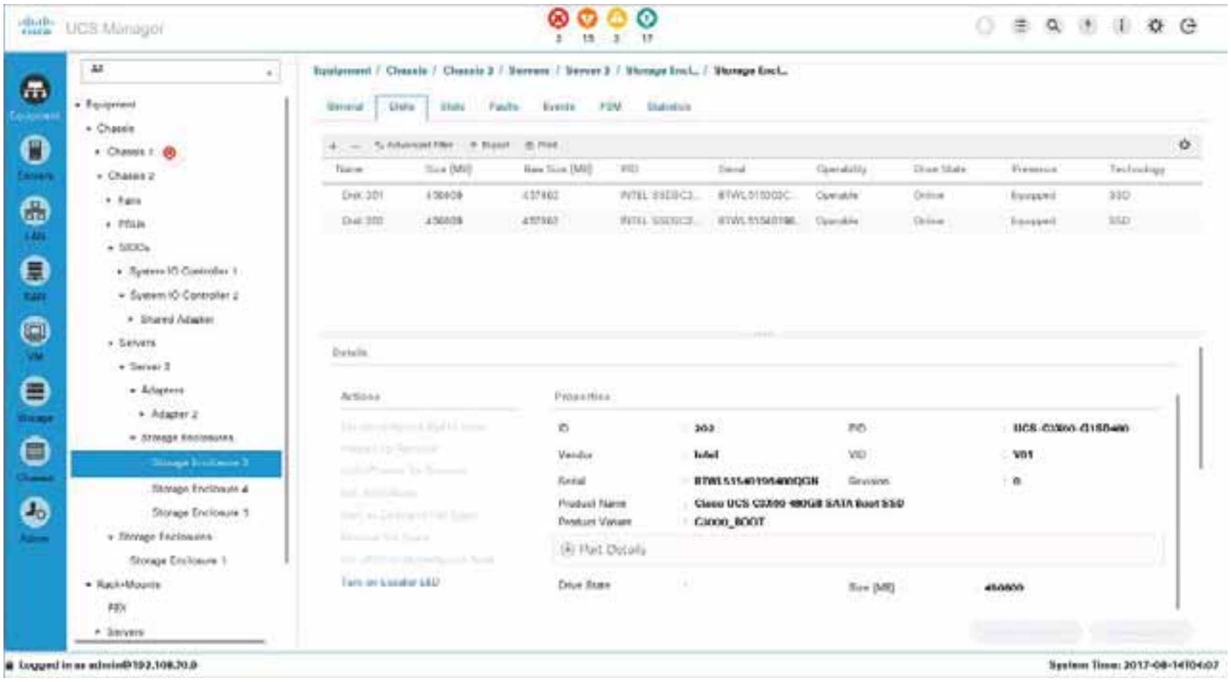
Disk 27	[illegible]	[illegible]	Operable	Equipped	HDD	Unconfigured Go...	False
Disk 28	[illegible]	[illegible]	Operable	Equipped	HDD	Unconfigured Go...	False
Disk 201	456809	BTWL5195020...	Operable	Equipped	SSD	Online	False
Disk 202	456809	BTWL5154019...	Operable	Equipped	SSD	Online	False
Storage Controller SAS 2							

ID :
PID :
Vendor :
VID :
Serial :
Revision :
Product Name :
Product Variant :

Logged in as admin@192.168.20.8

System Time: 2017-08-14T02:13

On the server node, Storage Enclosure 3 represents the disk slots on the back of the chassis, used for the operating system disks. Storage Enclosure 4 represents the NVMe slot on the server node, and Storage Enclosure 5 represents the two NVMe slots on the I/O expander board (if one is connected). Those storage enclosures are dedicated to the specific server.



Equipment / Chassis / Chassis 2 / Servers / Server 3 / Storage Encl... / Storage Encl...

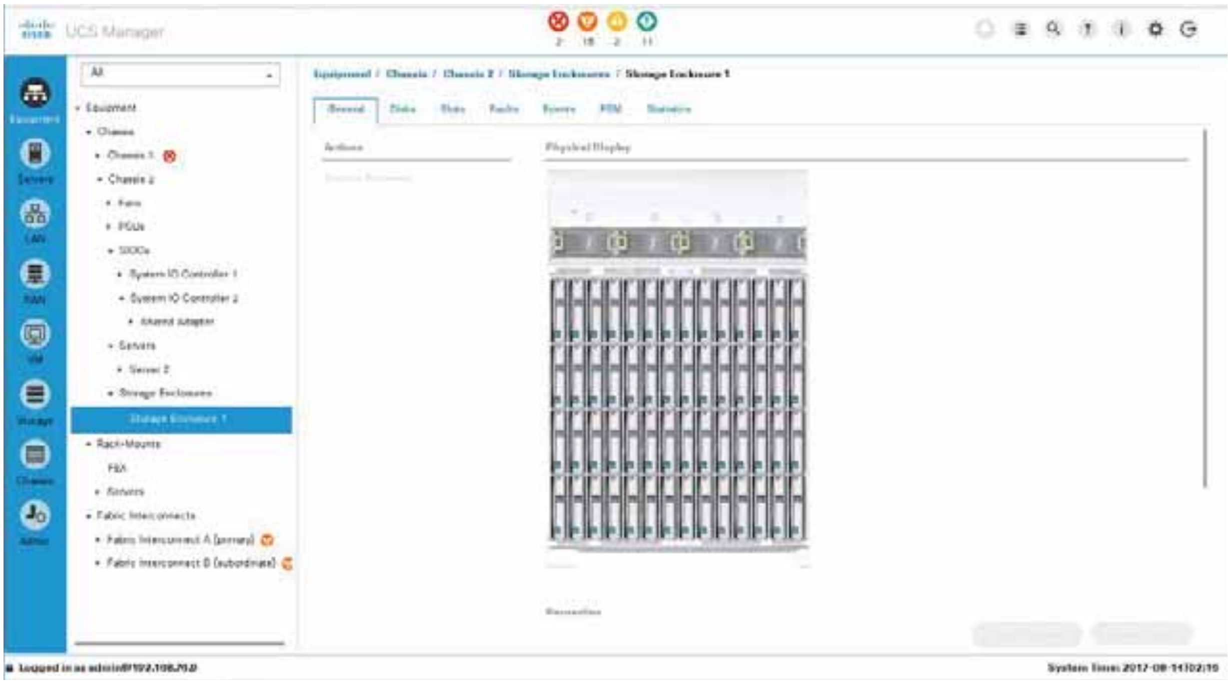
Name	Size (MB)	Raw Size (MB)	PID	Serial	Operability	Drive State	Presence	Technology
Disk 201	456808	457862	INTEL SSDSC2...	BTWL5150030C...	Operable	Online	Equipped	SSD
Disk 202	456808	457862	INTEL SSDSC2...	BTWL51540198...	Operable	Online	Equipped	SSD

ID : 202
PID : UCS-C3X60-G1SD480
Vendor : Intel
VID : V01
Serial : BTWL5154019S480QGN
Revision : 0
Product Name : Cisco UCS C3X60 480GB SATA Boot SSD
Product Variant : C3000_BOOT
Drive State :
Size (MB) : 456808

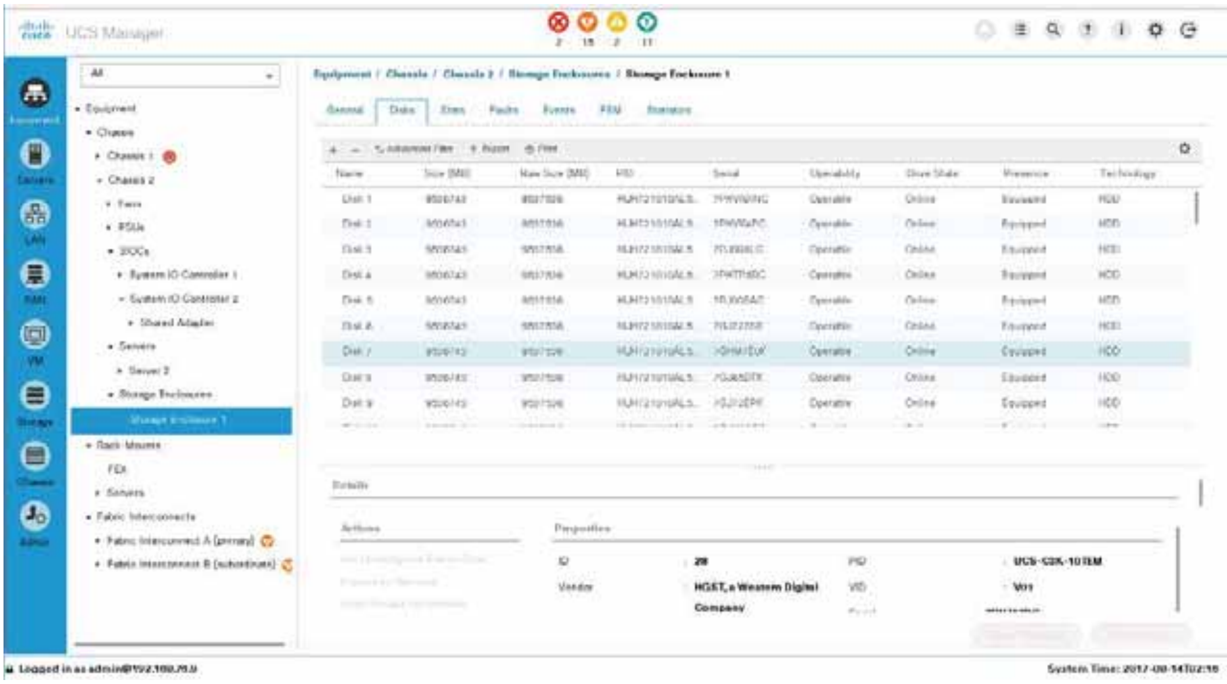
Logged in as admin@192.168.20.8

System Time: 2017-08-14T04:07

The Storage Enclosures area under Chassis, not under Servers, represents the top-loaded disk slots of the Cisco UCS S3260 chassis.



The Disks tab of Storage Enclosure 1 shows all the details about the top-loaded drives.



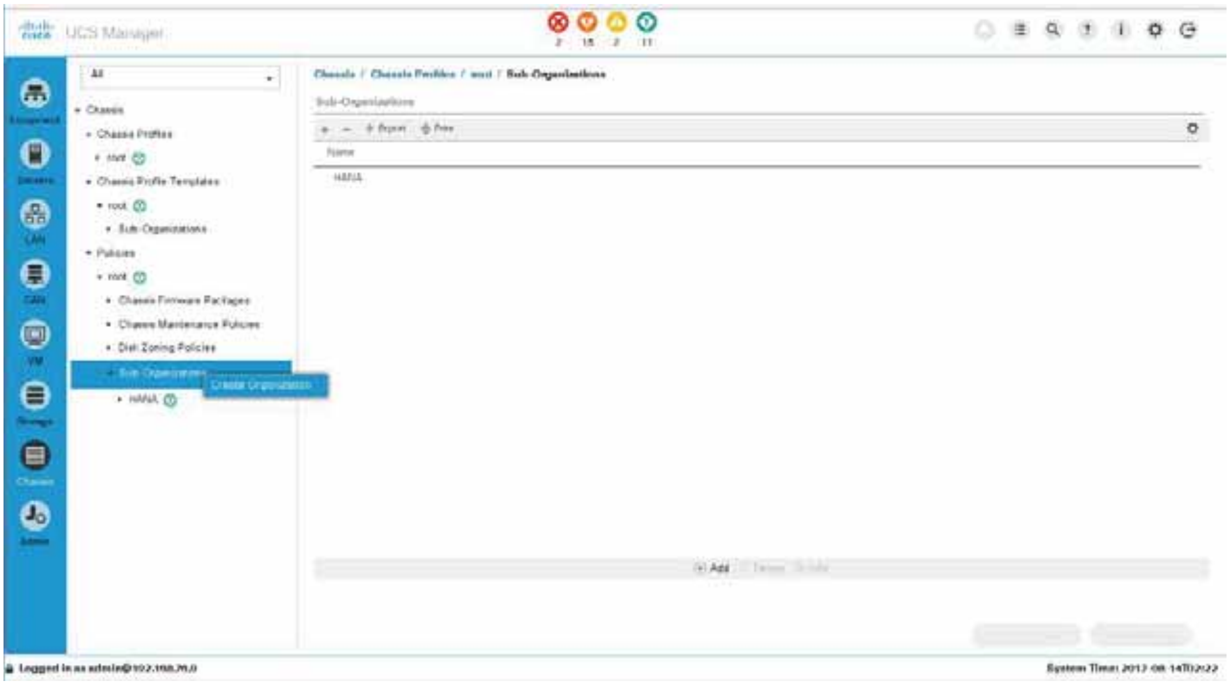
Name	Size (MB)	Raw Size (MB)	PID	Serial	Operability	Drive State	Presence	Technology
Disk 1	9536743	9537536	HUH721010AL5...	[illegible]	Operable	Online	Equipped	HDD
Disk 2	9536743	9537536	HUH721010AL5...	[illegible]	Operable	Online	Equipped	HDD
Disk 3	9536743	9537536	HUH721010AL5...	[illegible]	Operable	Online	Equipped	HDD
Disk 4	9536743	9537536	HUH721010AL5...	[illegible]	Operable	Online	Equipped	HDD
Disk 5	9536743	9537536	HUH721010AL5...	[illegible]	Operable	Online	Equipped	HDD
Disk 6	9536743	9537536	HUH721010AL5...	[illegible]	Operable	Online	Equipped	HDD
Disk 7	9536743	9537536	HUH721010AL5...	[illegible]	Operable	Online	Equipped	HDD
Disk 8	9536743	9537536	HUH721010AL5...	[illegible]	Operable	Online	Equipped	HDD
Disk 9	9536743	9537536	HUH721010AL5...	[illegible]	Operable	Online	Equipped	HDD

ID : 28
PID : UCS-C3K-10TEM
Vendor : HGST, a Western Digital Company
VID : V01

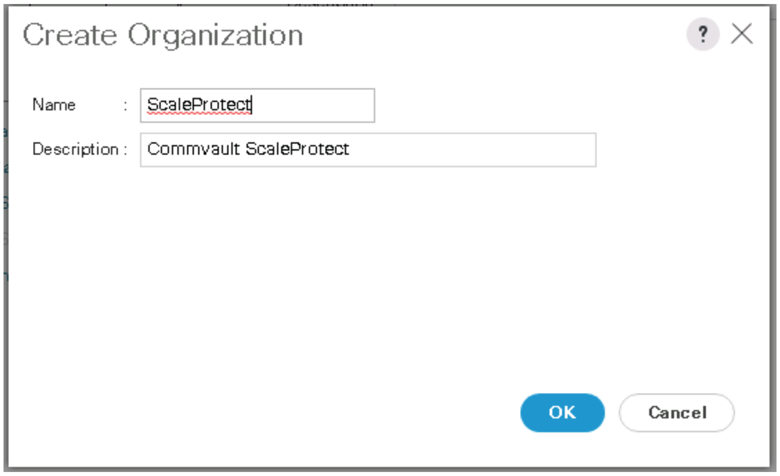
The next step is to specify a chassis profile for the Cisco UCS S3260 to define the disk zoning for the top-loaded drives (Storage Enclosure 1) within the chassis. Without a chassis profile, servers have no access to the top-loaded drives.

The Cisco UCS Manager configuration for Commvault ScaleProtect is specific to the use case, so you should define a new suborganization for ScaleProtect to keep all configurations dedicated to this use case.

In the Chassis area, choose one of the root options and then choose Sub-Organizations. Right-click and choose Create Organization.



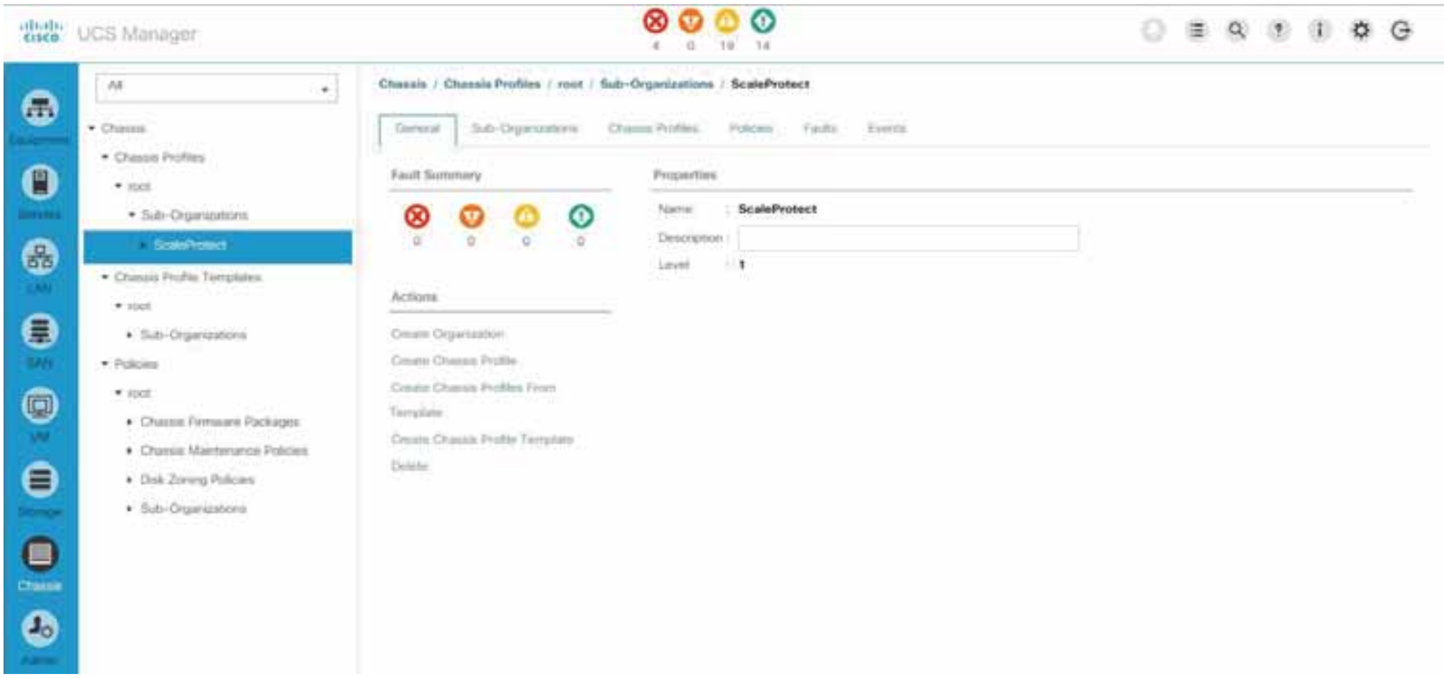
Enter an obvious name, such as **ScaleProtect**, enter a description, and click OK.



Name : ScaleProtect

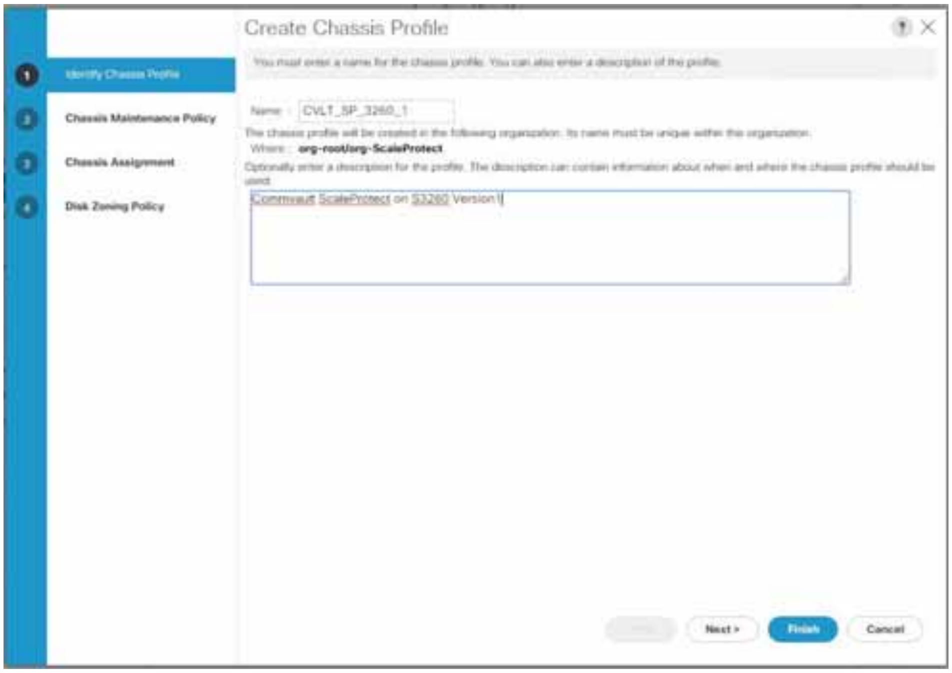
Description : Commvault ScaleProtect

Select the suborganization you created and click Create Chassis Profile.



Name : ScaleProtect
Description :
Level : 1

Enter an obvious name, such as **CVLT_SP_3260_1**, and click Next.



You must enter a name for the chassis profile. You can also enter a description of the profile.

Name : CVLT_SP_3260_1

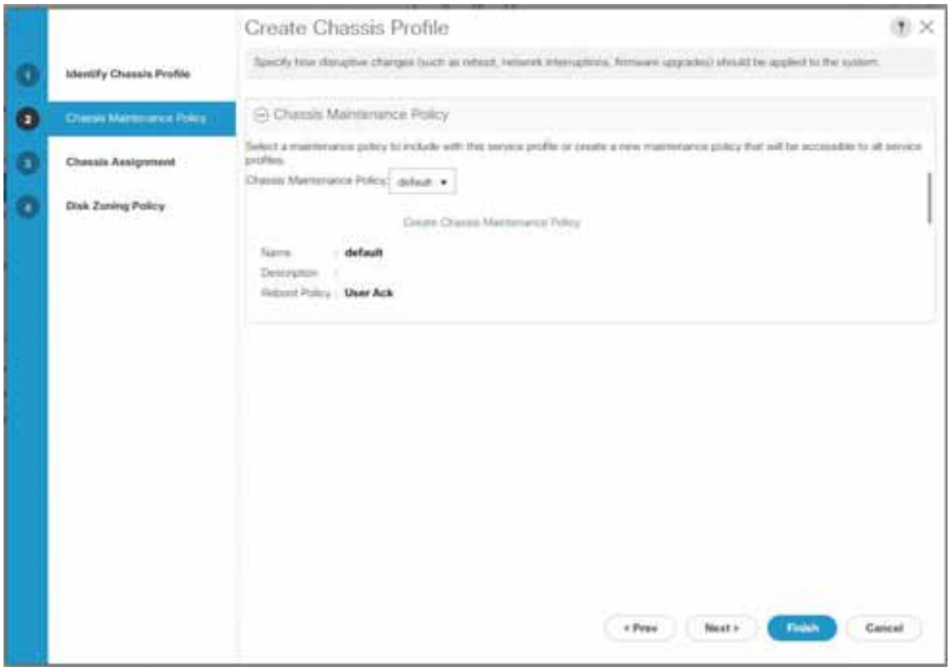
The chassis profile will be created in the following organization. Its name must be unique within this organization.

Where : **org-root/org-ScaleProtect**

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

Commvault ScaleProtect on S3260 Version1

Select a chassis maintenance policy, such as the default policy used in the example here, and click Next.


Create Chassis Profile
1 Identify Chassis Profile
2 Chassis Maintenance Policy
3 Chassis Assignment
4 Disk Zoning Policy
Chassis Maintenance Policy
Create Chassis Maintenance Policy
< Prev
Next >
Finish
Cancel

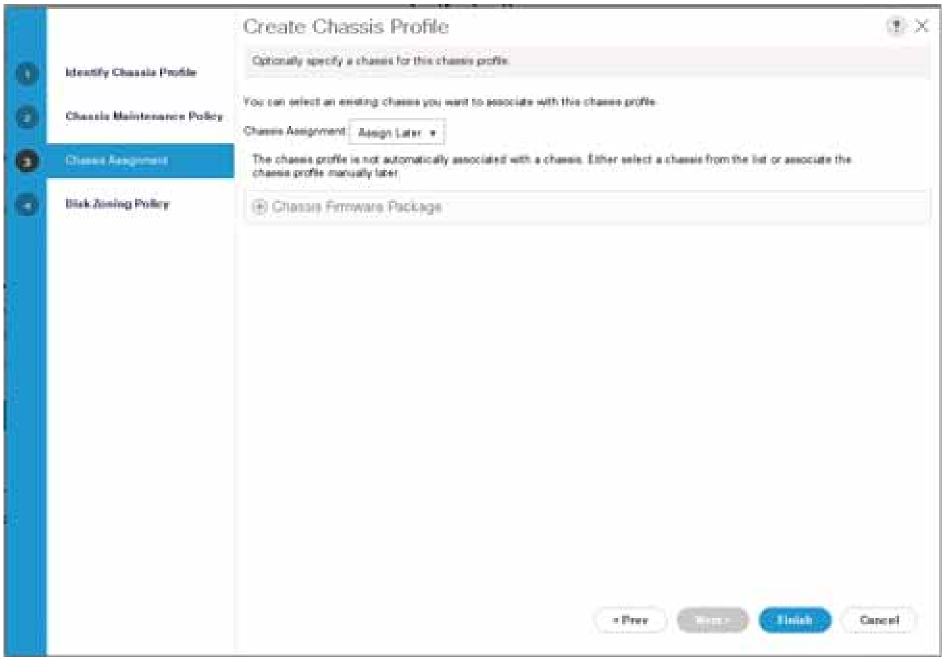
Specify how disruptive changes (such as reboot, network interruptions, firmware upgrades) should be applied to the system.

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

Chassis Maintenance Policy: default

Name : default
Description :
Reboot Policy : User Ack

Keep Assign Later selected and click Next.



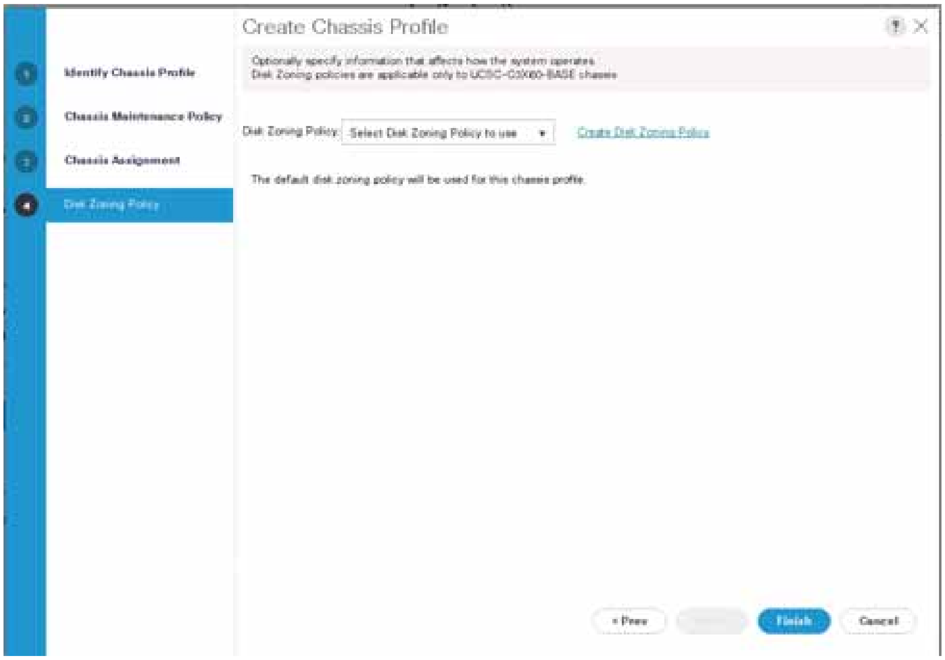
Optionally specify a chassis for this chassis profile.

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

Chassis Assignment: Assign Later

The chassis profile is not automatically associated with a chassis. Either select a chassis from the list or associate the chassis profile manually later.

Click Create Disk Zoning Policy.



Create Chassis Profile

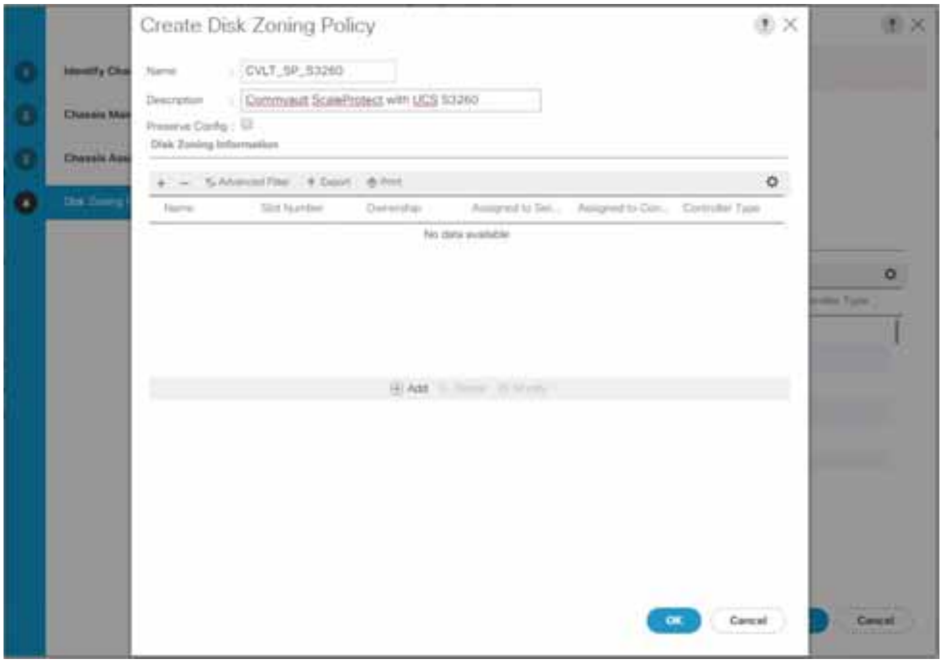
Optionally specify information that affects how the system operates.
Disk Zoning policies are applicable only to UCSC-C3X60-BASE chassis

Disk Zoning Policy: Select Disk Zoning Policy to use

The default disk zoning policy will be used for this chassis profile.

1 Identify Chassis Profile
2 Chassis Maintenance Policy
3 Chassis Assignment
4 Disk Zoning Policy
Create Disk Zoning Policy
< Prev
Finish
Cancel

Enter an obvious name, such as **CVLT_SP_S3260**, for the disk zoning policy and click Add.



Create Disk Zoning Policy

Name : CVLT_SP_S3260

Description : Commvault ScaleProtect with UCS S3260

Preserve Config : □

Disk Zoning Information

Name	Slot Number	Ownership	Assigned to Ser...	Assigned to Con...	Controller Type

No data available

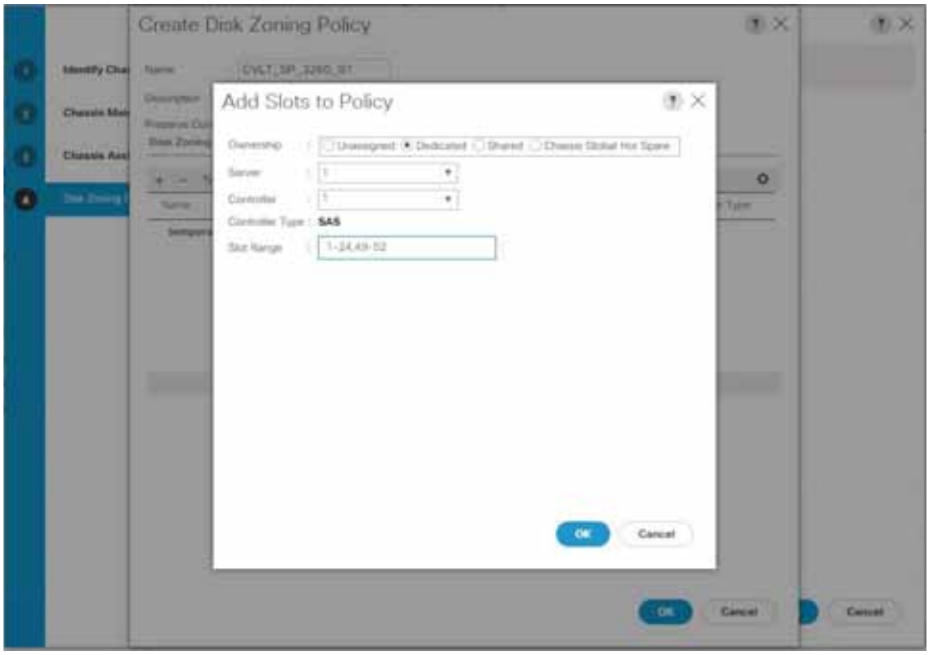
Select Dedicated as the ownership.

Select Server 1.

Select storage controller 1 for the RAID controller on the server.

Enter **1-24,49-52** as the slot range.

Click OK.



Create Disk Zoning Policy

Name : CVLT_SP_3260_S1

Add Slots to Policy

Ownership : ○ Unassigned ● Dedicated ○ Shared ○ Chassis Global Hot Spare

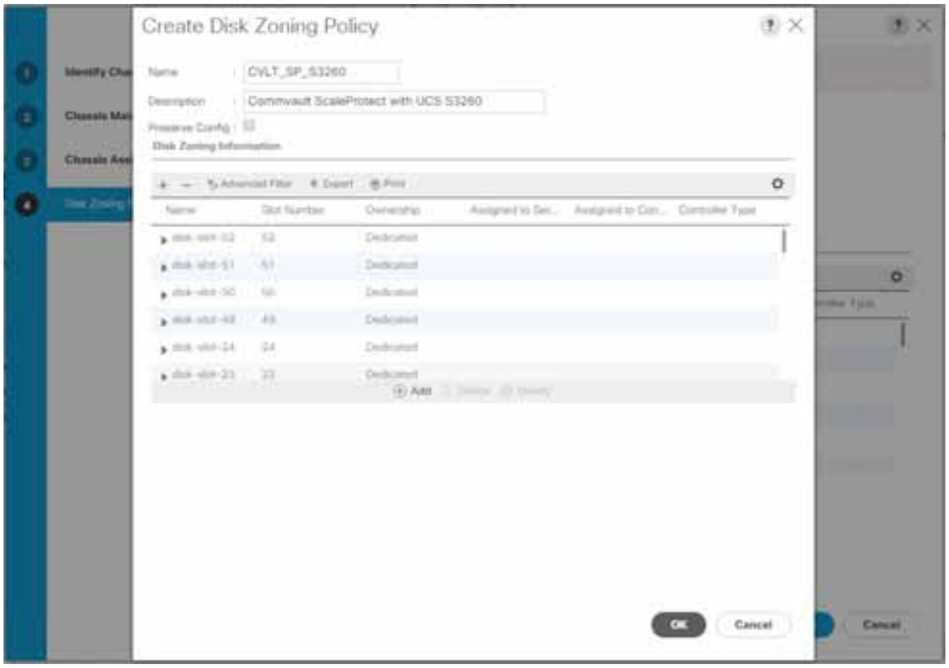
Server : 1

Controller : 1

Controller Type : SAS

Slot Range : 1-24,49-52

Verify that all information is correct and click OK.



Create Disk Zoning Policy

Name : CVLT_SP_S3260

Description : Commvault ScaleProtect with UCS S3260

Preserve Config : □

Disk Zoning Information

Name	Slot Number	Ownership	Assigned to Ser...	Assigned to Con...	Controller Type
disk-slot-52	52	Dedicated			
disk-slot-51	51	Dedicated			
disk-slot-50	50	Dedicated			
disk-slot-49	49	Dedicated			
disk-slot-24	24	Dedicated			
disk-slot-23	23	Dedicated			

Click Add.

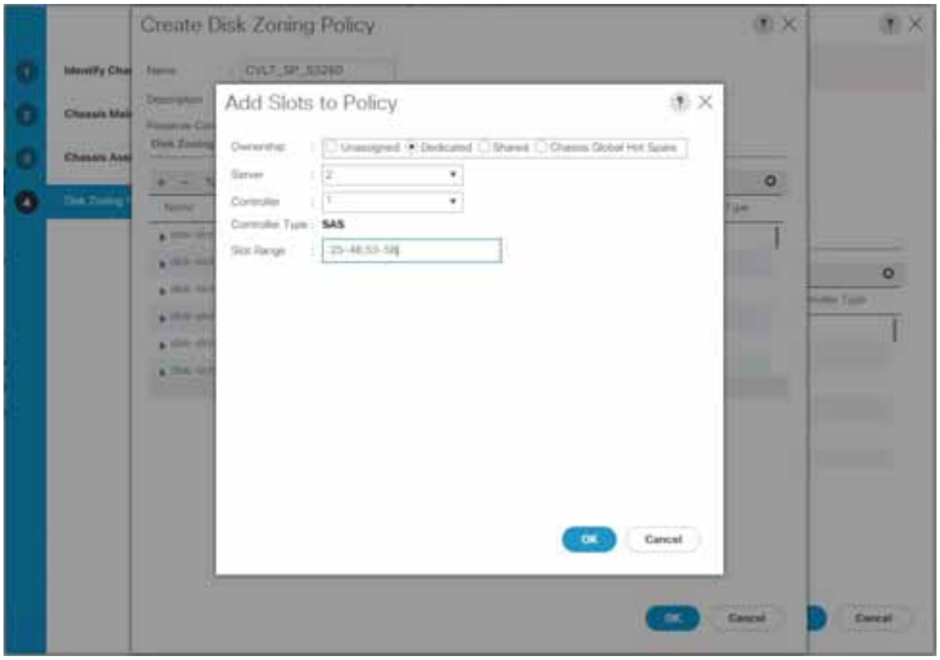
Select Dedicated as the ownership.

Select Server 1.

Select storage controller 1 for the RAID controller on the server.

Enter **1-24,49-52** as the slot range.

Click OK.



Create Disk Zoning Policy

Name: CVLT_SP_S3260

Add Slots to Policy

Ownership: ○ Unassigned ● Dedicated ○ Shared ○ Chassis Global Hot Spare

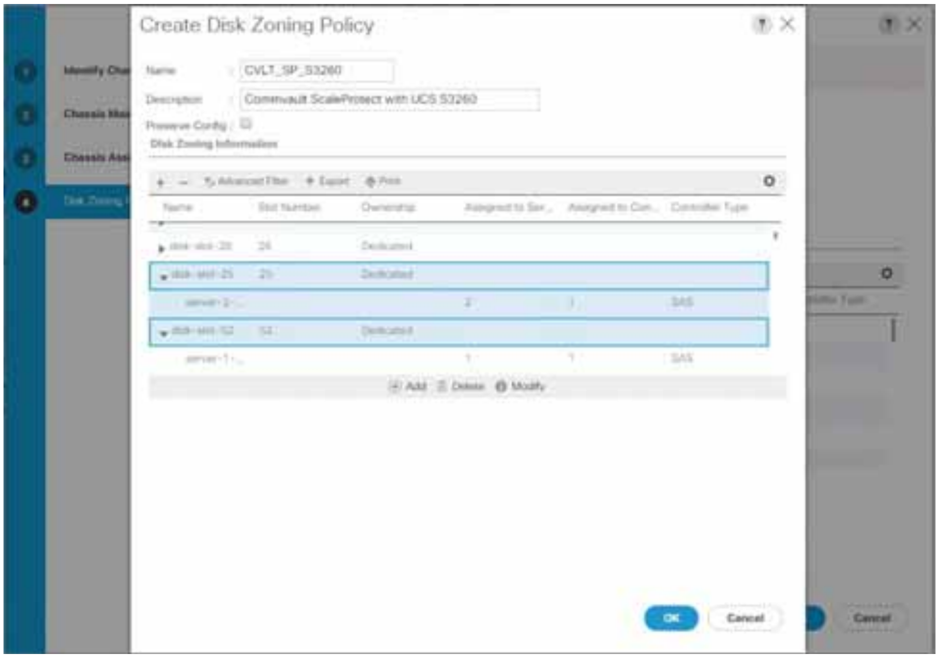
Server: 2

Controller: 1

Controller Type: SAS

Slot Range: 25-48,53-58

Verify that all information is correct and click OK.



Create Disk Zoning Policy

Name: CVLT_SP_S3260

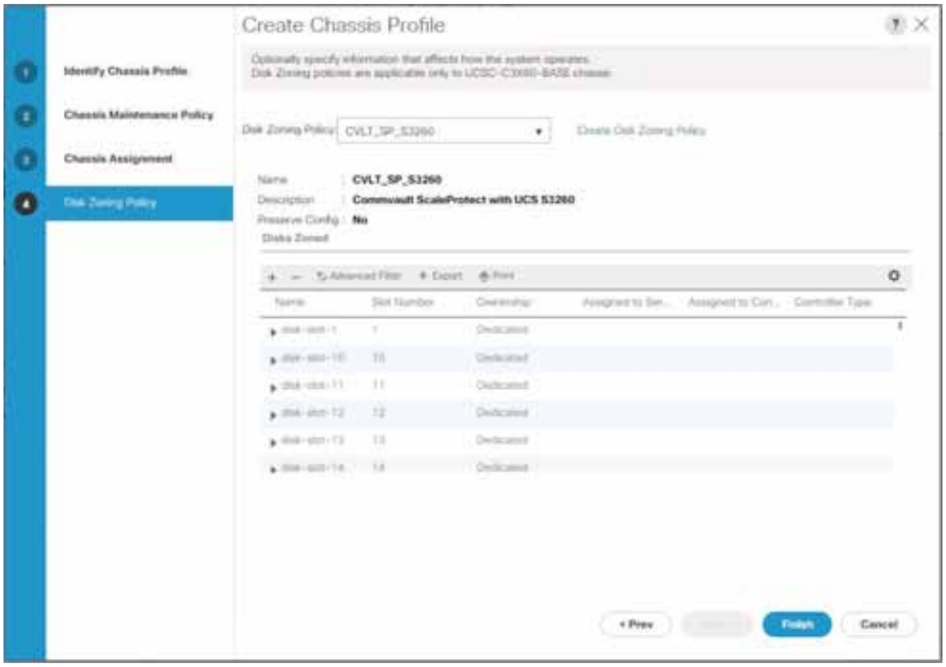
Description: Commvault ScaleProtect with UCS S3260

Preserve Config: □

Disk Zoning Information

Name	Slot Number	Ownership	Assigned to Ser...	Assigned to Con...	Controller Type
disk-slot-26	26	Dedicated			
disk-slot-25	25	Dedicated			
server-2-...			2	1	SAS
disk-slot-52	52	Dedicated			
server-1-...			1	1	SAS

Verify that all information is correct and click Finish.


1 Identify Chassis Profile
2 Chassis Maintenance Policy
3 Chassis Assignment
4 Disk Zoning Policy
Create Disk Zoning Policy
+ − Advanced Filter Export Print
< Prev
Next >
Finish
Cancel

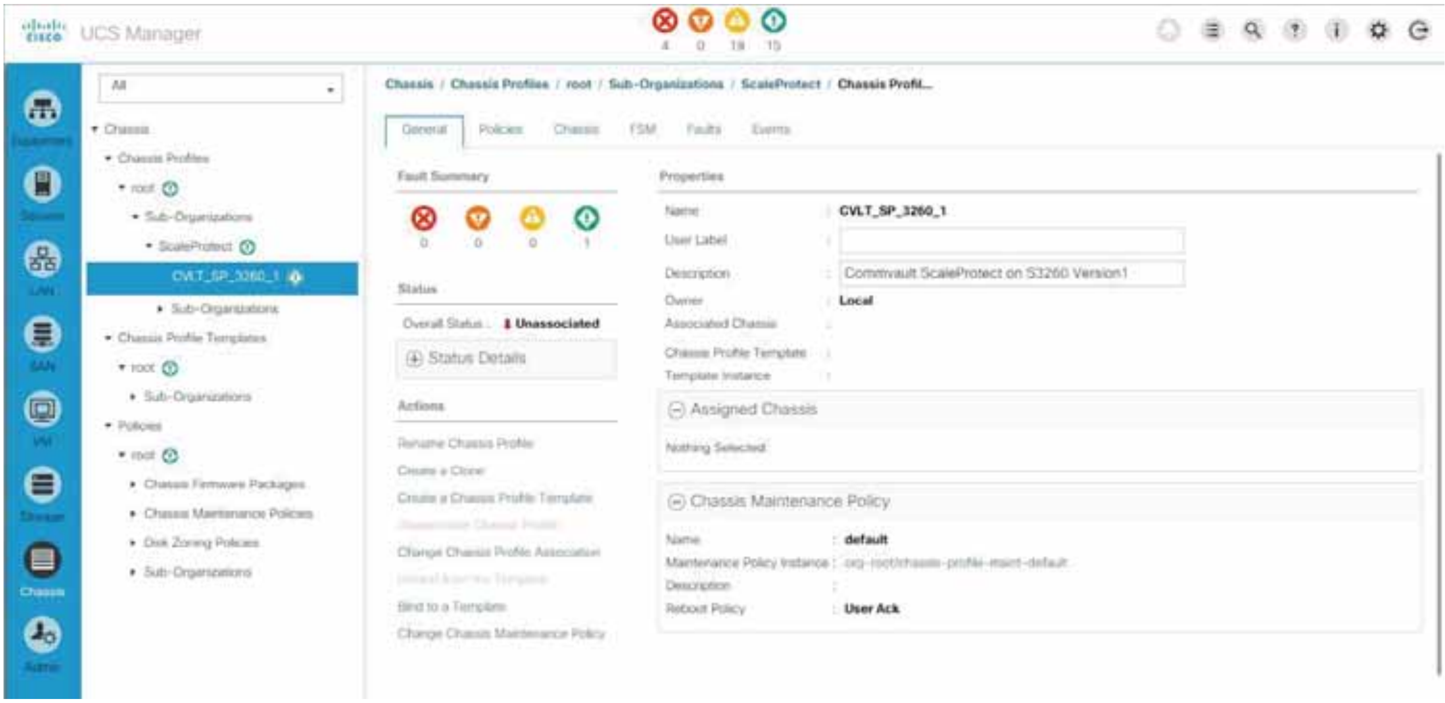
Create Chassis Profile

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

Disk Zoning Policy: CVLT_SP_S3260

Name : CVLT_SP_S3260
Description : Commvault ScaleProtect with UCS S3260
Preserve Config : No
Disks Zoned

Name	Slot Number	Ownership	Assigned to Ser...	Assigned to Con...	Controller Type
disk-slot-1	1	Dedicated			
disk-slot-10	10	Dedicated			
disk-slot-11	11	Dedicated			
disk-slot-12	12	Dedicated			
disk-slot-13	13	Dedicated			
disk-slot-14	14	Dedicated			



Chassis / Chassis Profiles / root / Sub-Organizations / ScaleProtect / Chassis Profil...

Status

Overall Status : Unassociated

Properties

Name : CVLT_SP_3260_1
User Label :
Description : Commvault ScaleProtect on S3260 Version1
Owner : Local
Associated Chassis :
Chassis Profile Template :
Template Instance :

Assigned Chassis

Nothing Selected

Chassis Maintenance Policy

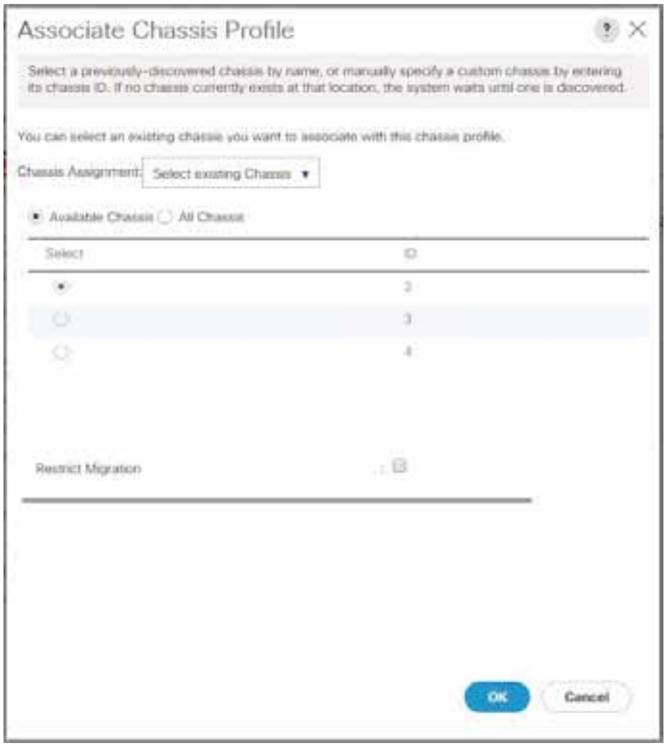
Name : default
Maintenance Policy Instance : org-root/chassis-profile-maint-default
Description :
Reboot Policy : User Ack

Click Change Chassis Profile Association.

In the Chassis Assignment drop-down menu, choose “Select existing Chassis.”

Select one of the chassis to be used for the ScaleProtect solution.

Click OK.



Associate Chassis Profile

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

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

Chassis Assignment: Select existing Chassis ▾

● Available Chassis ○ All Chassis

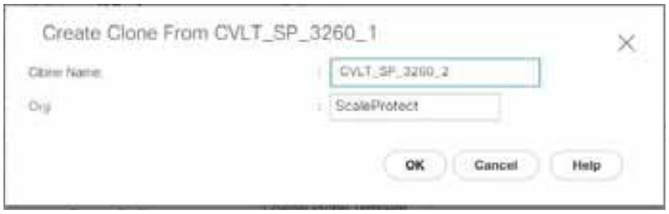
Select	ID
●	2
○	3
○	4

Restrict Migration : □

Each chassis requires its own chassis profile.

Click Create a Clone.

Enter an obvious name, such as **CVLT_SP_S3260_2**, and click OK.



Create Clone From CVLT_SP_3260_1

Clone Name: CVLT_SP_3260_2

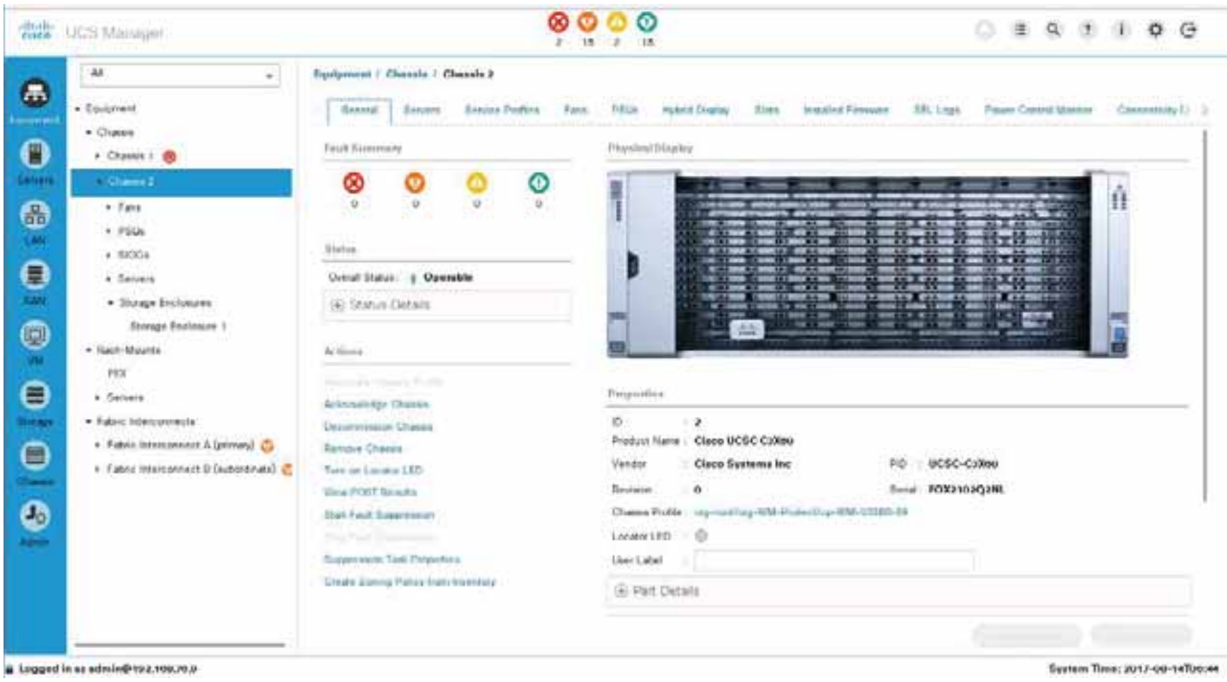
Org : ScaleProtect

Assign the new chassis profile to a chassis as shown in the preceding steps.

Repeat the “Create a Clone” and “Chassis Profile Association” processes for all chassis used for the ScaleProtect solution

Under Equipment > Chassis > Chassis X on the General tab (where X is the chassis number), the chassis profile is now listed.

For a short time, the overall status is shown for the configuration.



Equipment / Chassis / Chassis 2

Overall Status: Operable

Actions: Acknowledge Chassis, Decommission Chassis, Remove Chassis, Turn on Locator LED, View POST Results, Start Fault Suppression, Suppression Task Properties, Create Zoning Policy from Inventory

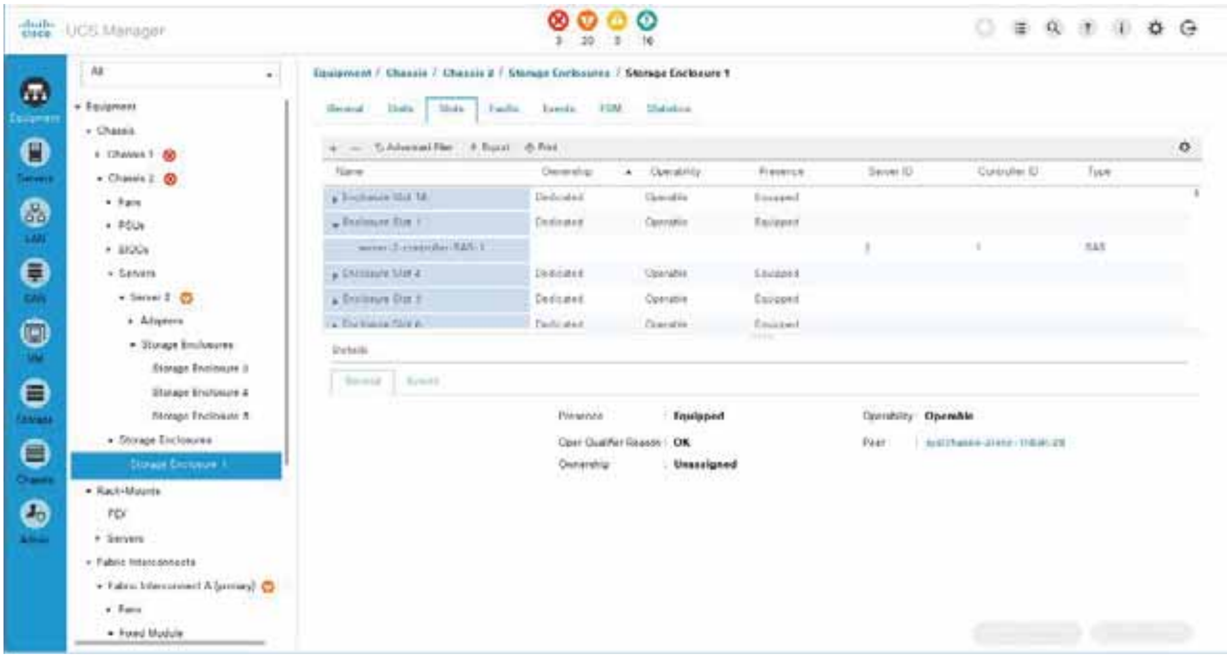
Properties

ID: 2
Product Name: Cisco UCSC C3X60
Vendor: Cisco Systems Inc
PID: UCSC-C3X60
Revision: 0
Serial: FOX2103Q2NL
Locator LED:
User Label:

Logged in as admin@192.168.70.9

System Time: 2017-09-14T06:44

Under Storage Enclosure 1, on the Slots tab, the status is now shown as dedicated to server X.



Equipment / Chassis / Chassis 2 / Storage Enclosures / Storage Enclosure 1

Name	Ownership	Operability	Presence	Server ID	Controller ID	Type
Enclosure Slot 14	Dedicated	Operable	Equipped			
Enclosure Slot 1	Dedicated	Operable	Equipped			
server-2-controller-SAS-1				2	1	SAS
Enclosure Slot 4	Dedicated	Operable	Equipped			
Enclosure Slot 2	Dedicated	Operable	Equipped			
Enclosure Slot 6	Dedicated	Operable	Equipped			

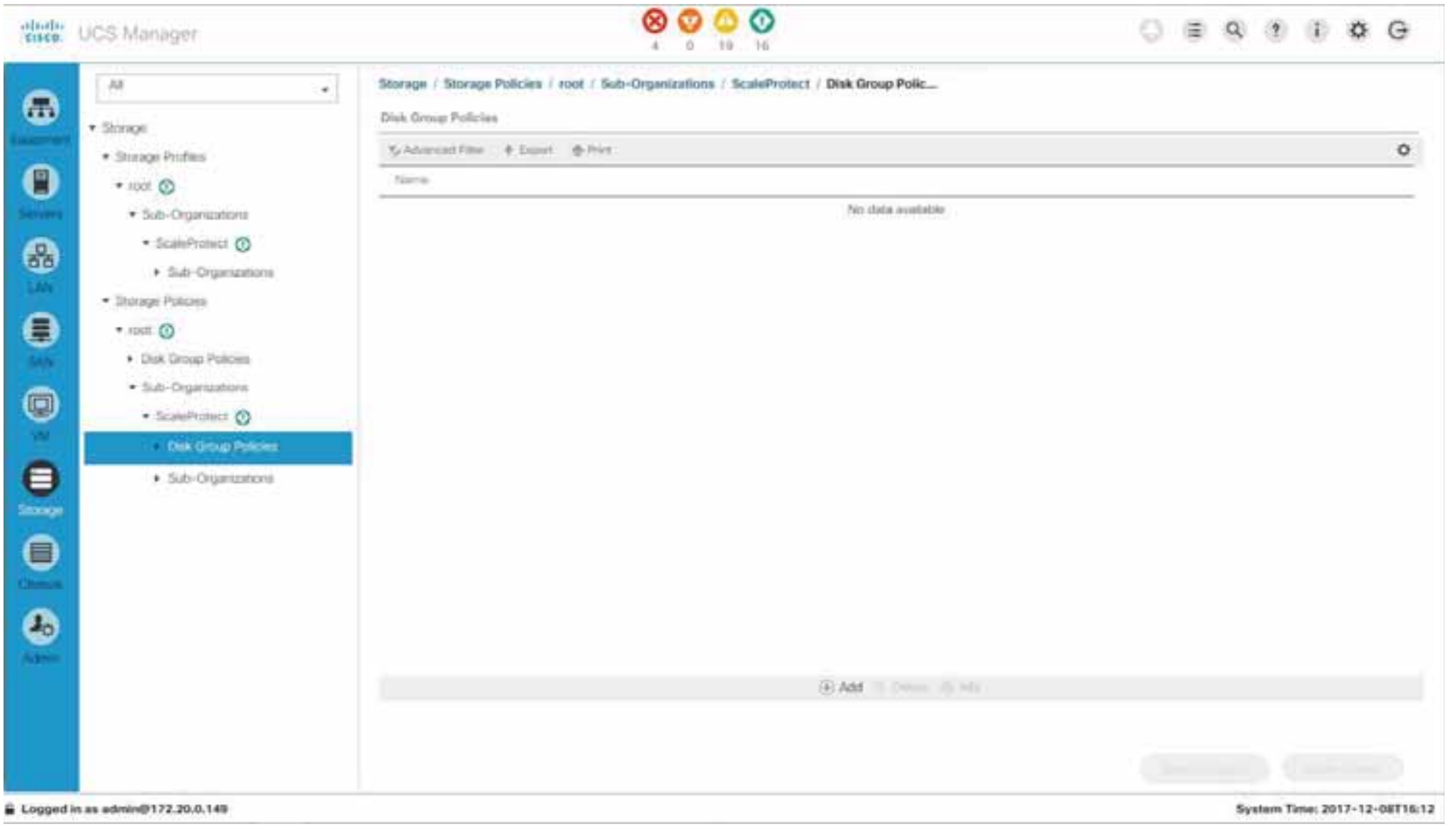
Details

Presence: Equipped
Oper Qualifier Reason: OK
Ownership: Unassigned
Operability: Operable
Peer: [illegible]

The next step is to define the disk groups and LUNs in the storage area of Cisco UCS Manager.

This is the most important part of the Cisco UCS S3260 configuration for Commvault ScaleProtect installation.

Choose Storage > Storage Policies > root > Sub-Organizations > ScaleProtect > Disk Group Policies and click Add.



Storage / Storage Policies / root / Sub-Organizations / ScaleProtect / Disk Group Polic...

- Storage
  - Storage Profiles
    - root
      - Sub-Organizations
        - ScaleProtect
          - Sub-Organizations
  - Storage Policies
    - root
      - Disk Group Policies
      - Sub-Organizations
        - ScaleProtect
          - Disk Group Policies
          - Sub-Organizations

Disk Group Policies

Name
No data available

Logged in as admin@172.20.0.149

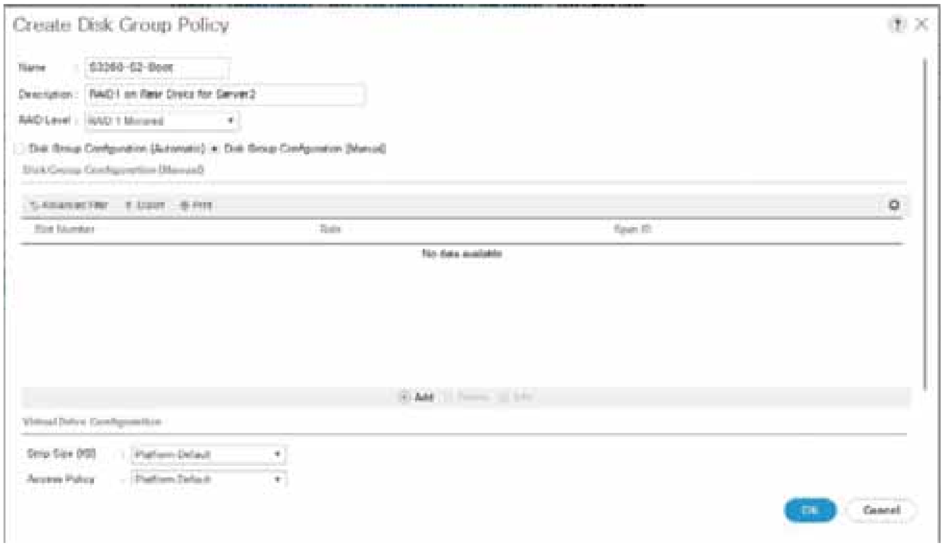
System Time: 2017-12-08T16:12

The first disk group policy is for the two disks in the back of the chassis for Server 2.

Enter an obvious name and a description.

For the RAID level, select RAID 1 Mirrored.

Select Disk Group Configuration (Manual) and click Add.



Create Disk Group Policy

Name : S3260-S2-Boot

Description : RAID1 on Rear Disks for Server2

RAID Level : RAID 1 Mirrored

○ Disk Group Configuration (Automatic) ● Disk Group Configuration (Manual)

Disk Group Configuration (Manual)

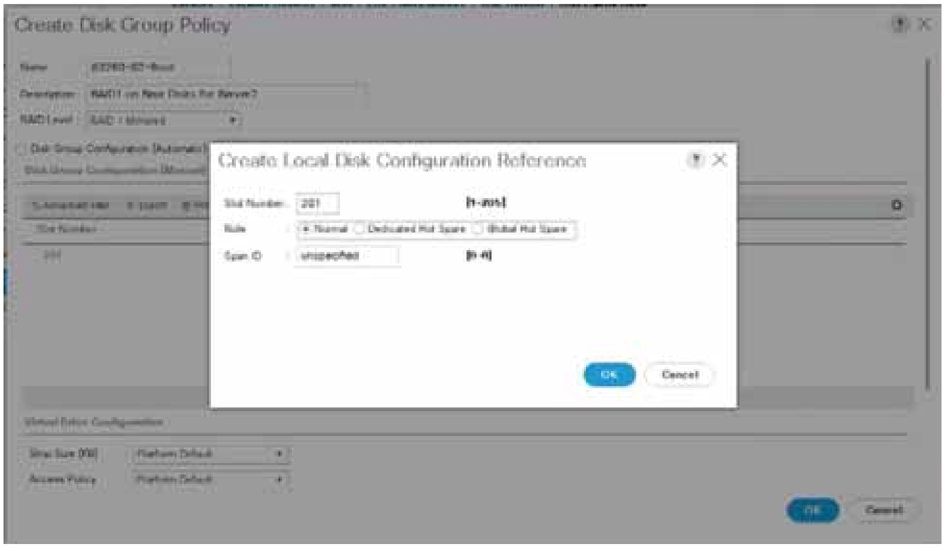
Slot Number	Role	Span ID
No data available		

Virtual Drive Configuration

Strip Size (KB) : Platform Default

Access Policy : Platform Default

Enter **201** as the slot number and click OK.



Create Disk Group Policy

Name: S3260-S2-Boot

Description: RAID1 on New Disks for Server2

RAID Level: RAID 1 Mirrored

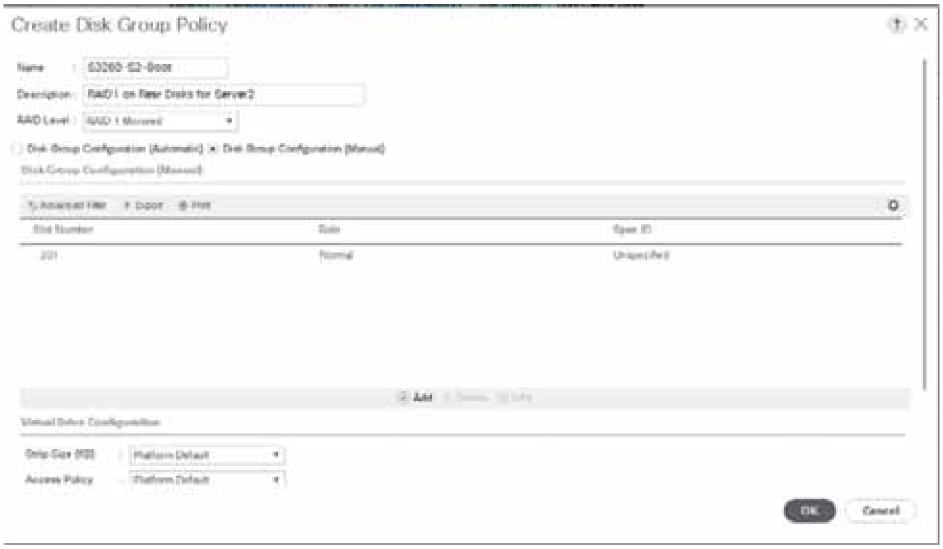
Create Local Disk Configuration Reference

Slot Number: 201 [1-205]

Role: ● Normal ○ Dedicated Hot Spare ○ Global Hot Spare

Span ID: unspecified [0-4]

Click Add.



Create Disk Group Policy

Name: S3260-S2-Boot

Description: RAID1 on New Disks for Server2

RAID Level: RAID 1 Mirrored

○ Disk Group Configuration (Automatic) ● Disk Group Configuration (Manual)

Disk Group Configuration (Manual)

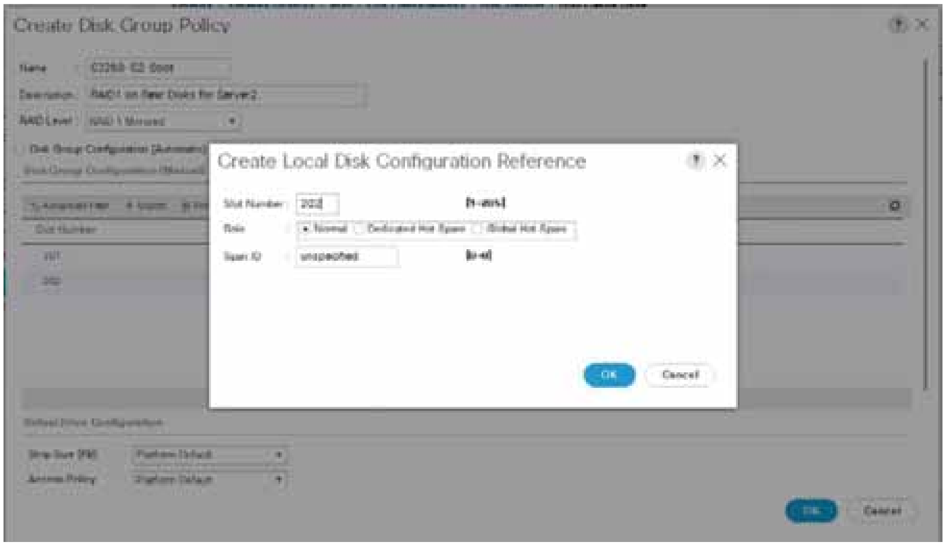
Slot Number	Role	Span ID
201	Normal	Unspecified

Virtual Drive Configuration

Strip Size (KB): Platform Default

Access Policy: Platform Default

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



Create Disk Group Policy

Name: S3260-S2-Boot

Description: RAID1 on Rear Disks for Server2

RAID Level: RAID 1 Mirrored

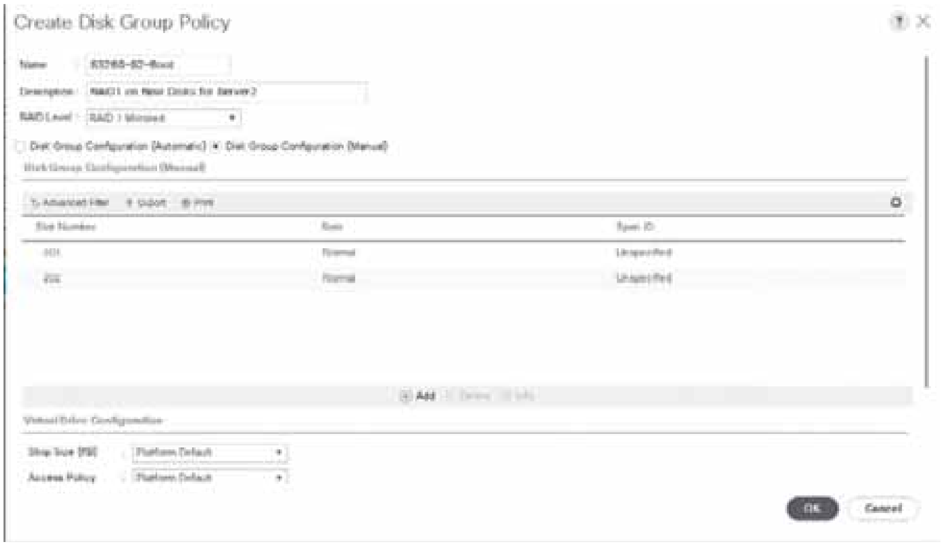
Create Local Disk Configuration Reference

Slot Number: 202 [1-254]

Role: ● Normal ○ Dedicated Hot Spare ○ Global Hot Spare

Span ID: unspecified [0-8]

Click OK again.



Create Disk Group Policy

Name: S3260-S2-Boot

Description: RAID1 on Rear Disks for Server2

RAID Level: RAID 1 Mirrored

○ Disk Group Configuration (Automatic) ● Disk Group Configuration (Manual)

Disk Group Configuration (Manual)

Slot Number	Role	Span ID
201	Normal	Unspecified
202	Normal	Unspecified

Virtual Drive Configuration

Strip Size (KB): Platform Default

Access Policy: Platform Default

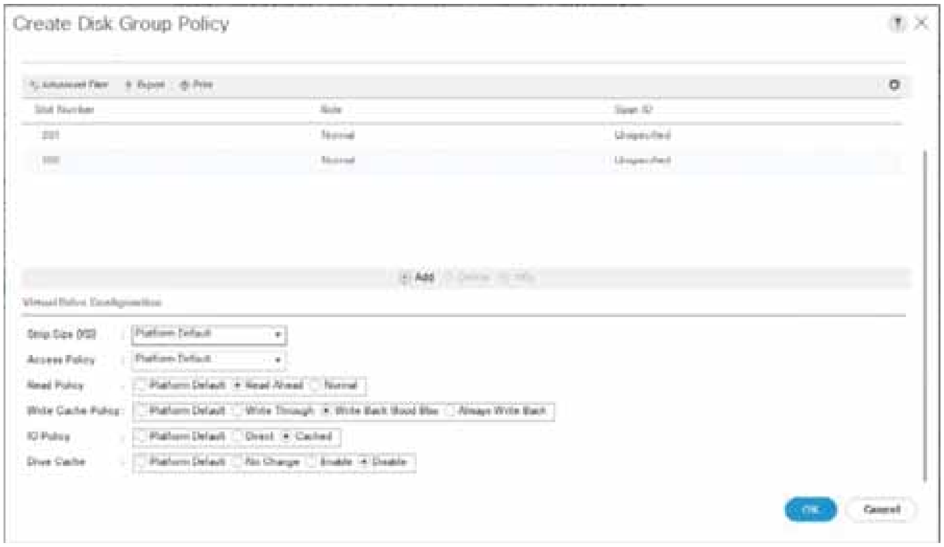
Select Read Ahead for Read Policy.

Select Write Back Good BBU for Write Cache Policy.

Select Cached for IO Policy.

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

Click OK.



Create Disk Group Policy

Slot Number	Role	Span ID
201	Normal	Unspecified
[illegible]	Normal	Unspecified

Virtual Drive Configuration

Strip Size (KB) : Platform Default

Access Policy : Platform Default

Read Policy : ○ Platform Default ● Read Ahead ○ Normal

Write Cache Policy : ○ Platform Default ○ Write Through ● Write Back Good Bbu ○ Always Write Back

IO Policy : ○ Platform Default ○ Direct ● Cached

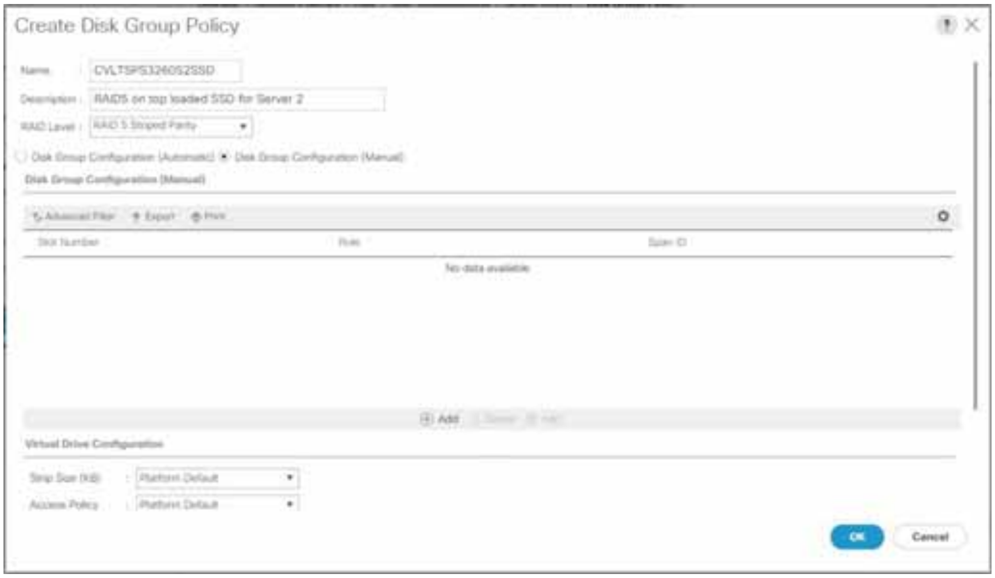
Drive Cache : ○ Platform Default ○ No Change ○ Enable ● Disable

Click Add for the set of SSD drives on Server 2.

Enter an obvious name and a description.

For the RAID level, select RAID 5 Striped Parity.

Select Disk Group Configuration (Manual) and click Add.



Create Disk Group Policy

Name : CVLTSPS3260S2SSD

Description : RAID5 on top loaded SSD for Server 2

RAID Level : RAID 5 Striped Parity

○ Disk Group Configuration (Automatic) ● Disk Group Configuration (Manual)

Disk Group Configuration (Manual)

Slot Number	Role	Span ID

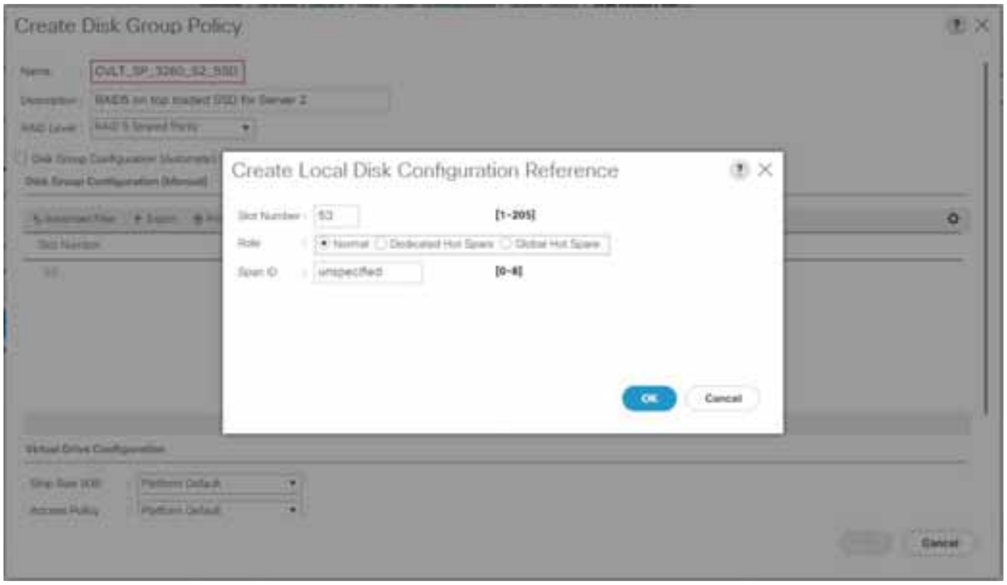
No data available

Virtual Drive Configuration

Strip Size (KB) : Platform Default

Access Policy : Platform Default

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



Create Disk Group Policy

Name: CVLT_SP_3260_S2_SSD

Description: RAID5 on top loaded SSD for Server 2

RAID Level: RAID 5 Striped Parity

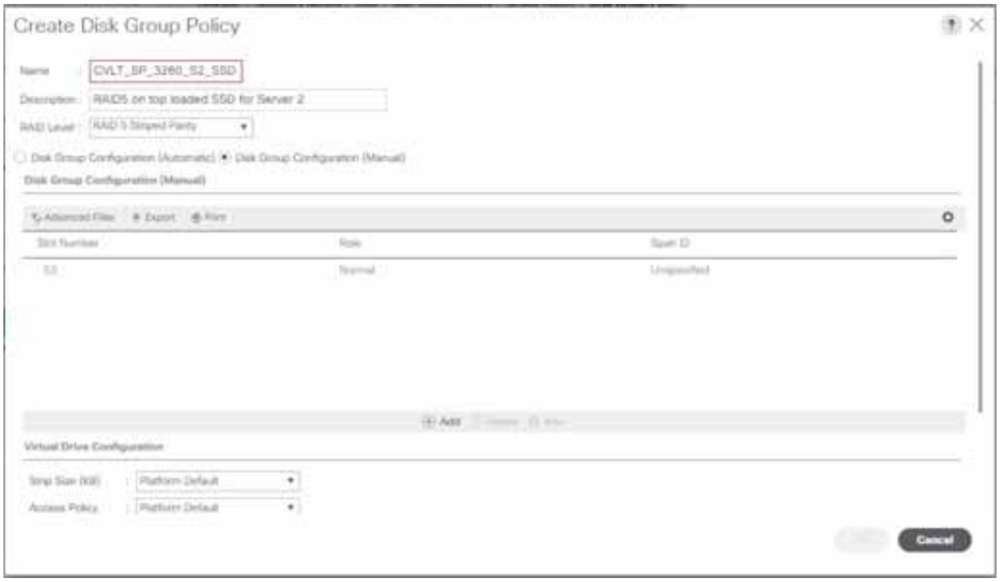
Create Local Disk Configuration Reference

Slot Number: 53 [1-205]

Role: ● Normal ○ Dedicated Hot Spare ○ Global Hot Spare

Span ID: unspecified [0-8]

Click Add.



Create Disk Group Policy

Name: CVLT_SP_3260_S2_SSD

Description: RAID5 on top loaded SSD for Server 2

RAID Level: RAID 5 Striped Parity ▾

○ Disk Group Configuration (Automatic) ● Disk Group Configuration (Manual)

Disk Group Configuration (Manual)

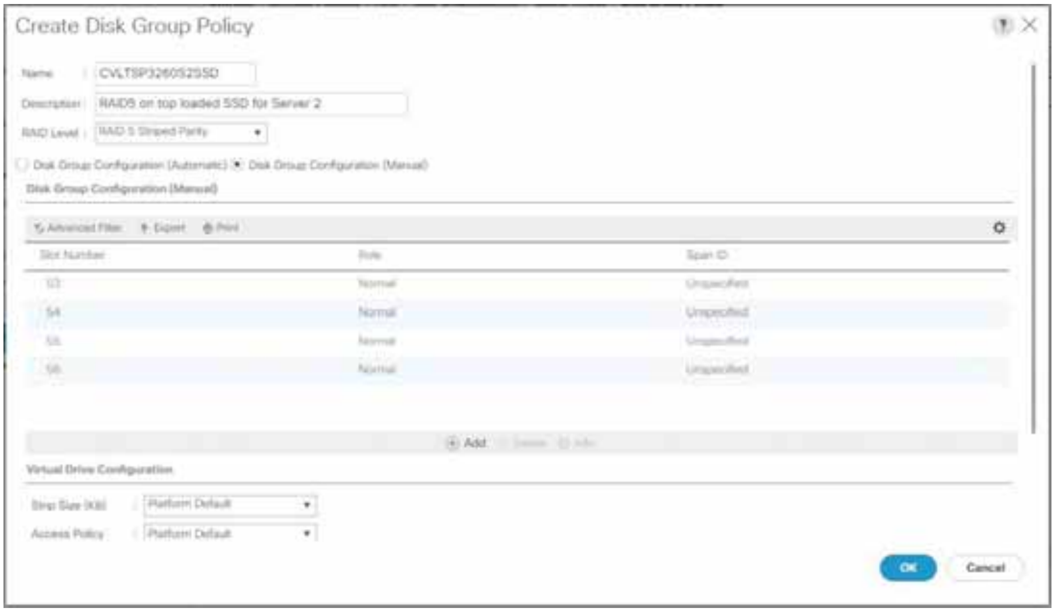
Slot Number	Role	Span ID
53	Normal	Unspecified

Virtual Drive Configuration

Strip Size (KB): Platform Default ▾

Access Policy: Platform Default ▾

Repeat these steps for Slots 54 through 56.



Create Disk Group Policy

Name: CVLTSP3260S2SSD

Description: RAID5 on top loaded SSD for Server 2

RAID Level: RAID 5 Striped Parity

○ Disk Group Configuration (Automatic) ● Disk Group Configuration (Manual)

Disk Group Configuration (Manual)

Slot Number	Role	Span ID
S3	Normal	Unspecified
S4	Normal	Unspecified
S5	Normal	Unspecified
S6	Normal	Unspecified

Virtual Drive Configuration

Strip Size (KB): Platform Default

Access Policy: Platform Default

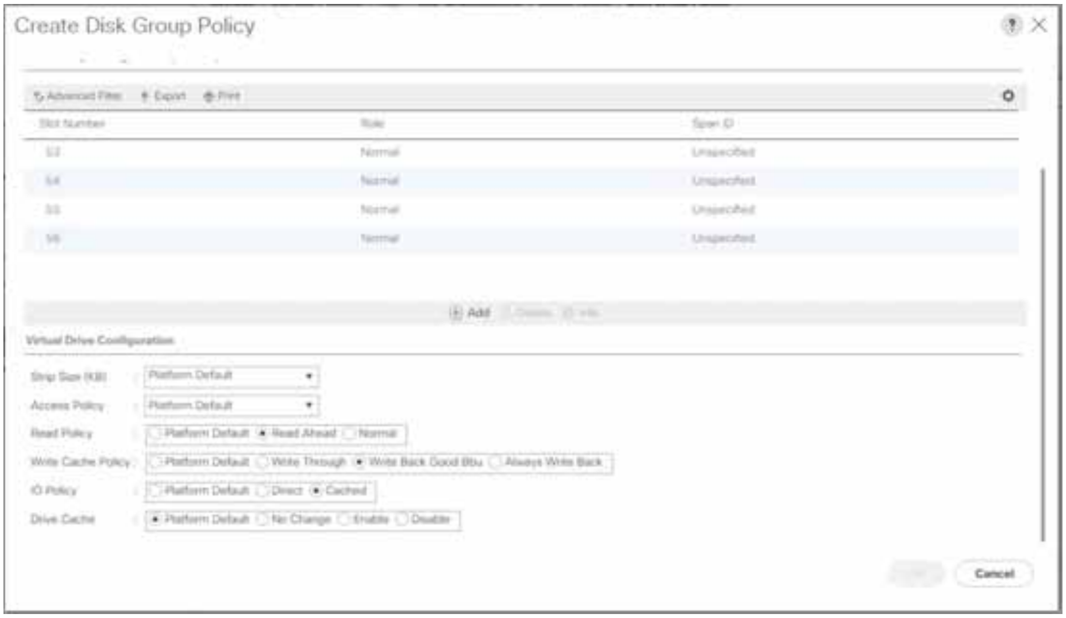
Select Read Ahead for Read Policy.

Select Write Back Good BBU for Write Cache Policy.

Select Cached for IO Policy.

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

Click OK.



Create Disk Group Policy

Slot Number	Role	Span ID
S3	Normal	Unspecified
S4	Normal	Unspecified
S5	Normal	Unspecified
S6	Normal	Unspecified

Virtual Drive Configuration

Strip Size (KB): Platform Default

Access Policy: Platform Default

Read Policy: ○ Platform Default ● Read Ahead ○ Normal

Write Cache Policy: ○ Platform Default ○ Write Through ● Write Back Good Bbu ○ Always Write Back

IO Policy: ○ Platform Default ○ Direct ● Cached

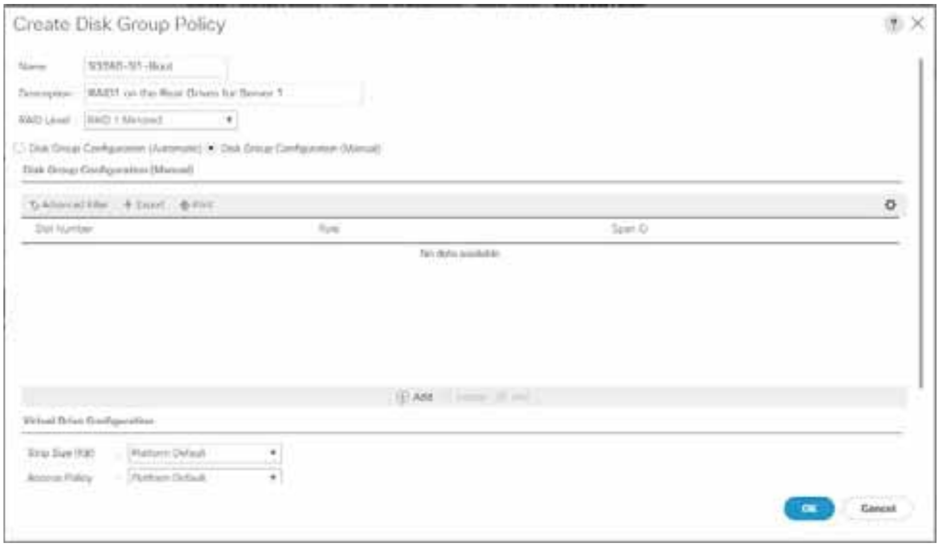
Drive Cache: ● Platform Default ○ No Change ○ Enable ○ Disable

The next disk group policy is for the two disks in the back of the chassis for Server 1.

Enter an obvious name and a description.

For the RAID level, select RAID 1 Mirrored.

Select Disk Group Configuration (Manual) and click Add.



Create Disk Group Policy

Name: S3260-S1-Boot

Description: RAID1 on the Rear Drives for Server 1

RAID Level: RAID 1 Mirrored

○ Disk Group Configuration (Automatic) ● Disk Group Configuration (Manual)

Disk Group Configuration (Manual)

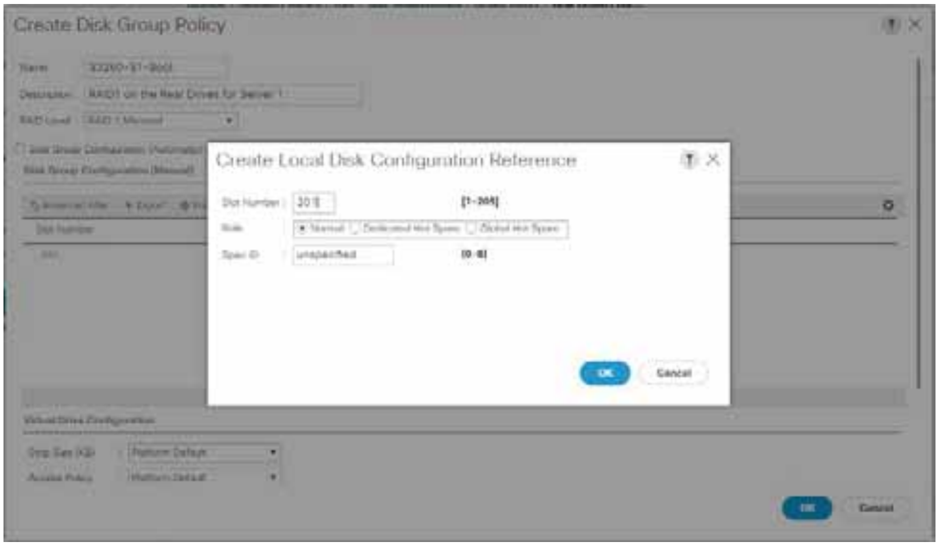
Slot Number	Role	Span ID
No data available		

Virtual Drive Configuration

Strip Size (KB): Platform Default

Access Policy: Platform Default

Enter **201** as the slot number and click OK.



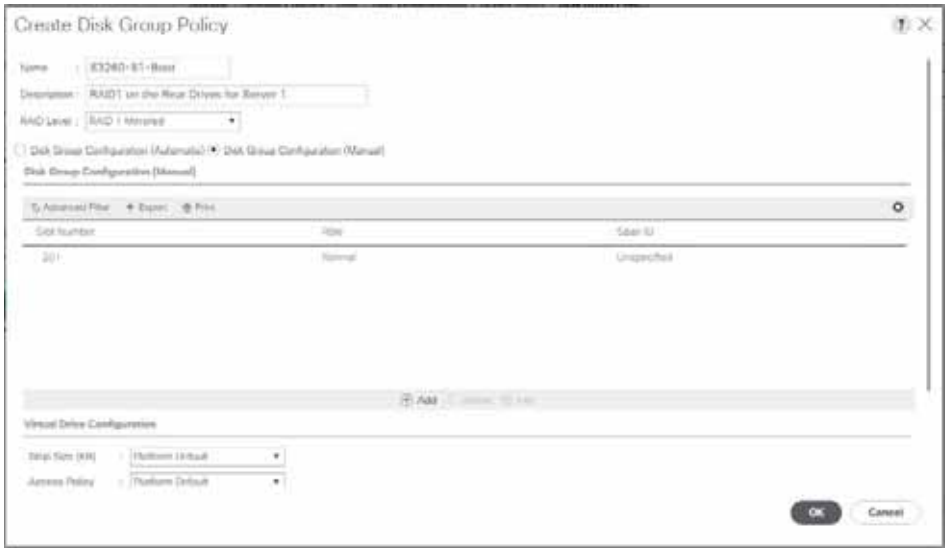
Create Local Disk Configuration Reference

Slot Number: 201 [1-208]

Role: ● Normal ○ Dedicated Hot Spare ○ Global Hot Spare

Span ID: unspecified [0-8]

Click Add.



Create Disk Group Policy

Name : S3260-S1-Boot

Description : RAID1 on the Rear Drives for Server 1

RAID Level : RAID 1 Mirrored

○ Disk Group Configuration (Automatic) ● Disk Group Configuration (Manual)

Disk Group Configuration (Manual)

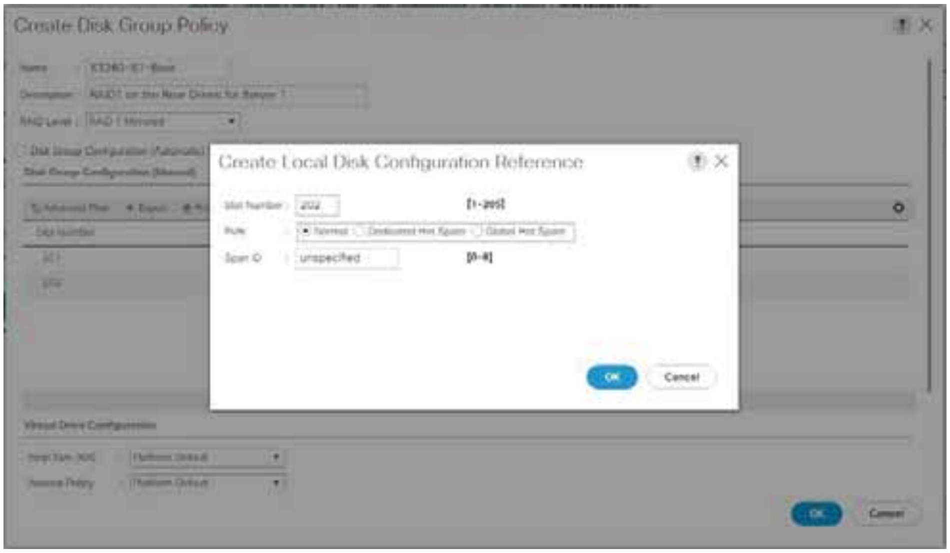
Slot Number	Role	Span ID
201	Normal	Unspecified

Virtual Drive Configuration

Strip Size (KB) : Platform Default

Access Policy : Platform Default

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



Create Local Disk Configuration Reference

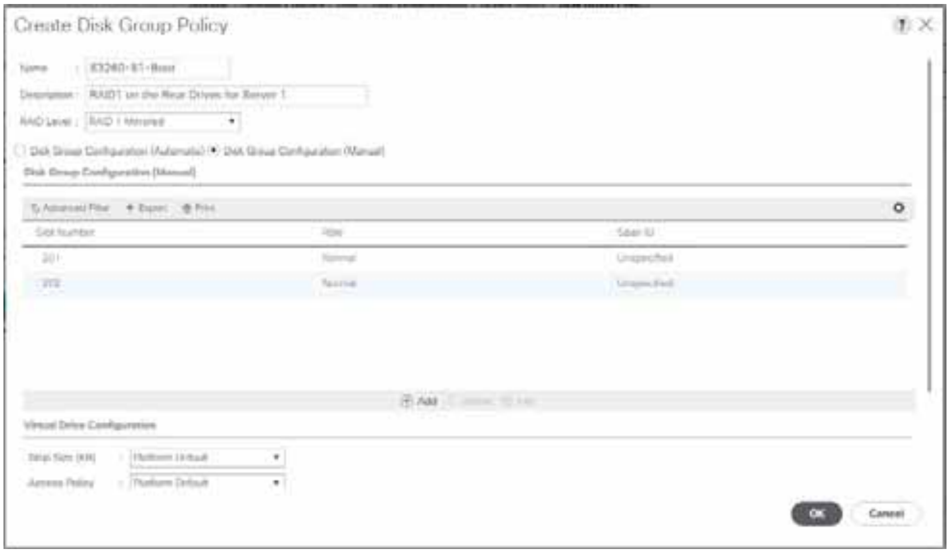
Slot Number : 202 [1-205]

Role : ● Normal ○ Dedicated Hot Spare ○ Global Hot Spare

Span ID : unspecified [0-8]

Slot Number
201
202

Click OK again.



Create Disk Group Policy

Name : S3260-S1-Boot

Description : RAID1 on the Rear Drives for Server 1

RAID Level : RAID 1 Mirrored

○ Disk Group Configuration (Automatic) ● Disk Group Configuration (Manual)

Disk Group Configuration (Manual)

Slot Number	Role	Span ID
201	Normal	Unspecified
202	Normal	Unspecified

Virtual Drive Configuration

Strip Size (KB) : Platform Default

Access Policy : Platform Default

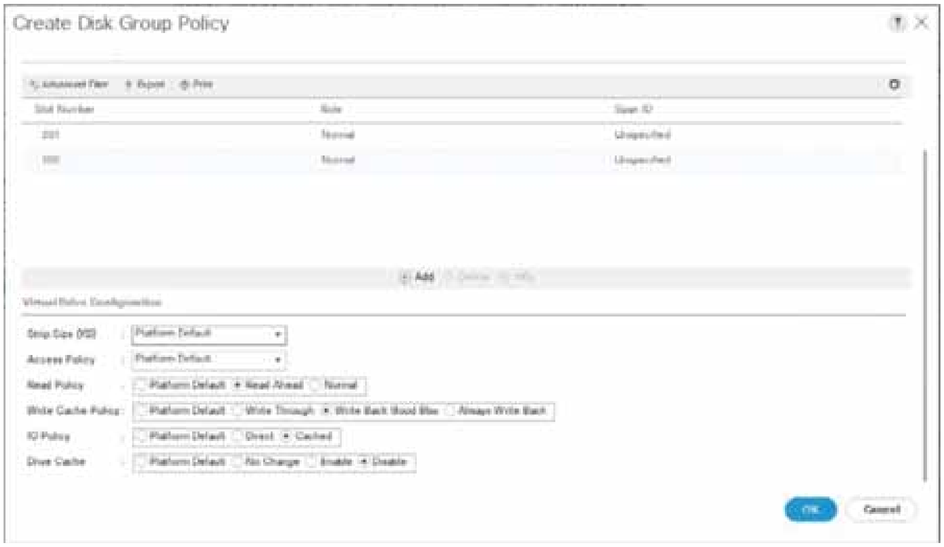
Select Read Ahead for Read Policy.

Select Write Back Good BBU for Write Cache Policy.

Select Cached for IO Policy.

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

Click OK.



Create Disk Group Policy

Slot Number	Role	Span ID
201	Normal	Unspecified
202	Normal	Unspecified

Virtual Drive Configuration

Strip Size (KB) : Platform Default

Access Policy : Platform Default

Read Policy : ○ Platform Default ● Read Ahead ○ Normal

Write Cache Policy : ○ Platform Default ○ Write Through ● Write Back Good Bbu ○ Always Write Back

IO Policy : ○ Platform Default ○ Direct ● Cached

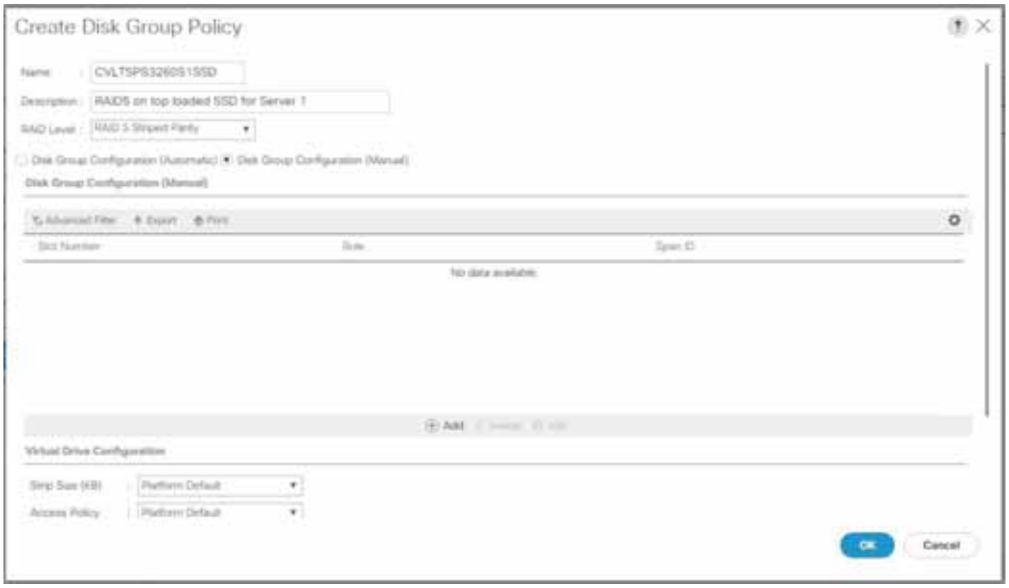
Drive Cache : ○ Platform Default ○ No Change ○ Enable ● Disable

Click Add for the set of SSD drives on Server 1.

Enter an obvious name and a description.

For the RAID level, select RAID 5 Striped Parity.

Select Disk Group Configuration (Manual) and click Add.



Create Disk Group Policy

Name : CVLTSPS3260S1SSD

Description : RAID5 on top loaded SSD for Server 1

RAID Level : RAID 5 Striped Parity

○ Disk Group Configuration (Automatic) ● Disk Group Configuration (Manual)

Disk Group Configuration (Manual)

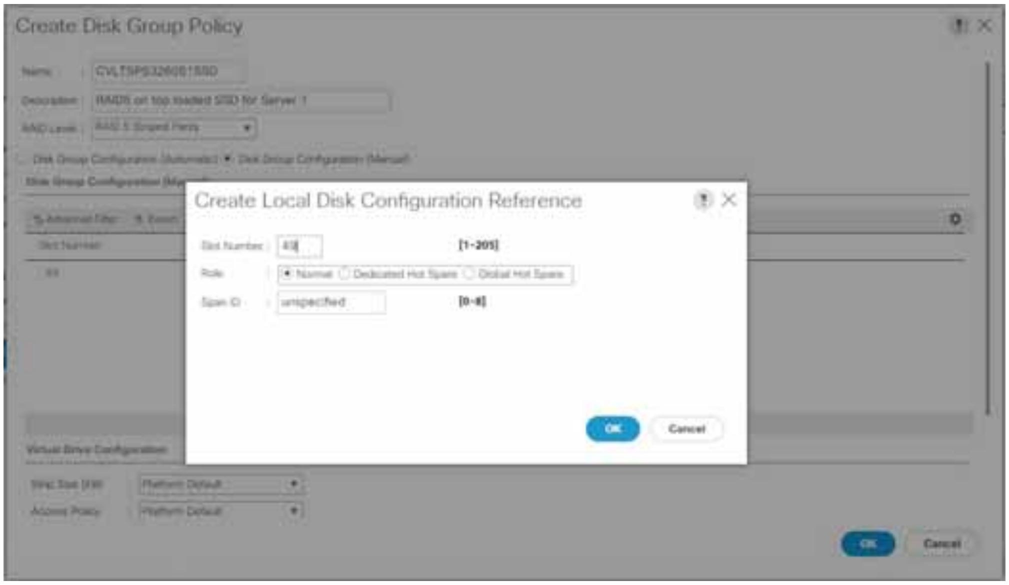
Slot Number	Role	Span ID
No data available		

Virtual Drive Configuration

Strip Size (KB) : Platform Default

Access Policy : Platform Default

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



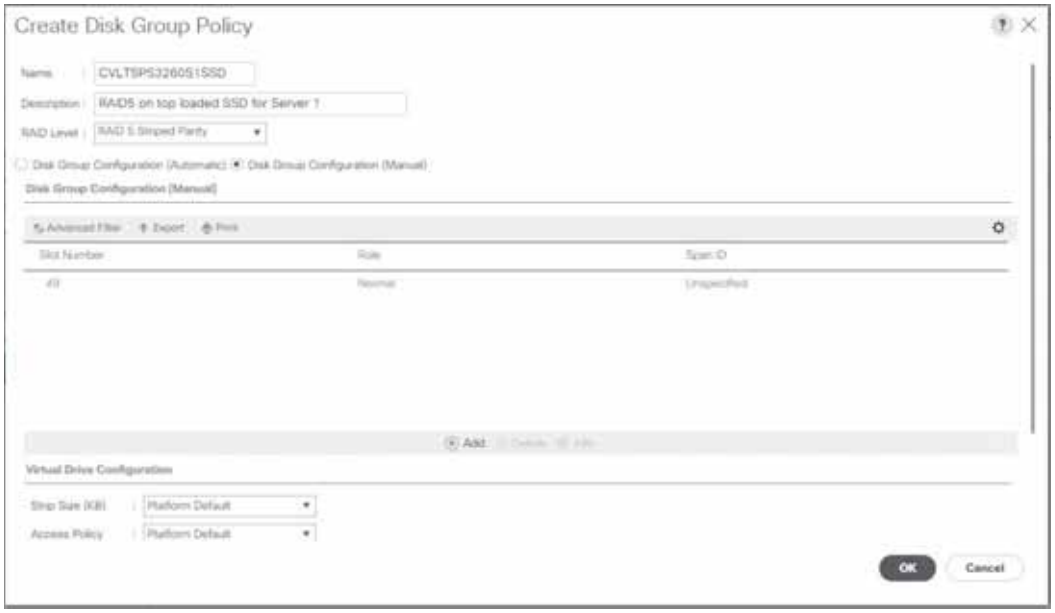
Create Local Disk Configuration Reference

Slot Number : 49 [1-205]

Role : ● Normal ○ Dedicated Hot Spare ○ Global Hot Spare

Span ID : unspecified [0-8]

Click Add.



Create Disk Group Policy

Name : CVLTSPS3260S1SSD

Description : RAID5 on top loaded SSD for Server 1

RAID Level : RAID 5 Striped Parity

○ Disk Group Configuration (Automatic) ● Disk Group Configuration (Manual)

Disk Group Configuration (Manual)

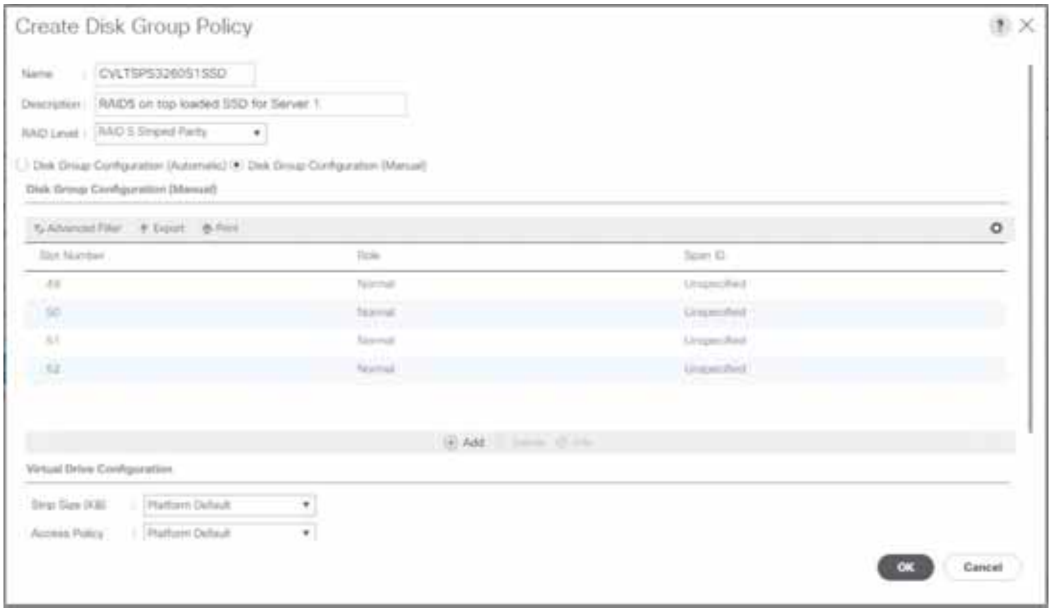
Slot Number	Role	Span ID
49	Normal	Unspecified

Virtual Drive Configuration

Strip Size (KB) : Platform Default

Access Policy : Platform Default

Repeat these steps for Slots 50 through 52.



Create Disk Group Policy

Name : CVLTSPS3260S1SSD

Description : RAID5 on top loaded SSD for Server 1

RAID Level : RAID 5 Striped Parity

○ Disk Group Configuration (Automatic) ● Disk Group Configuration (Manual)

Disk Group Configuration (Manual)

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

Virtual Drive Configuration

Strip Size (KB) : Platform Default

Access Policy : Platform Default

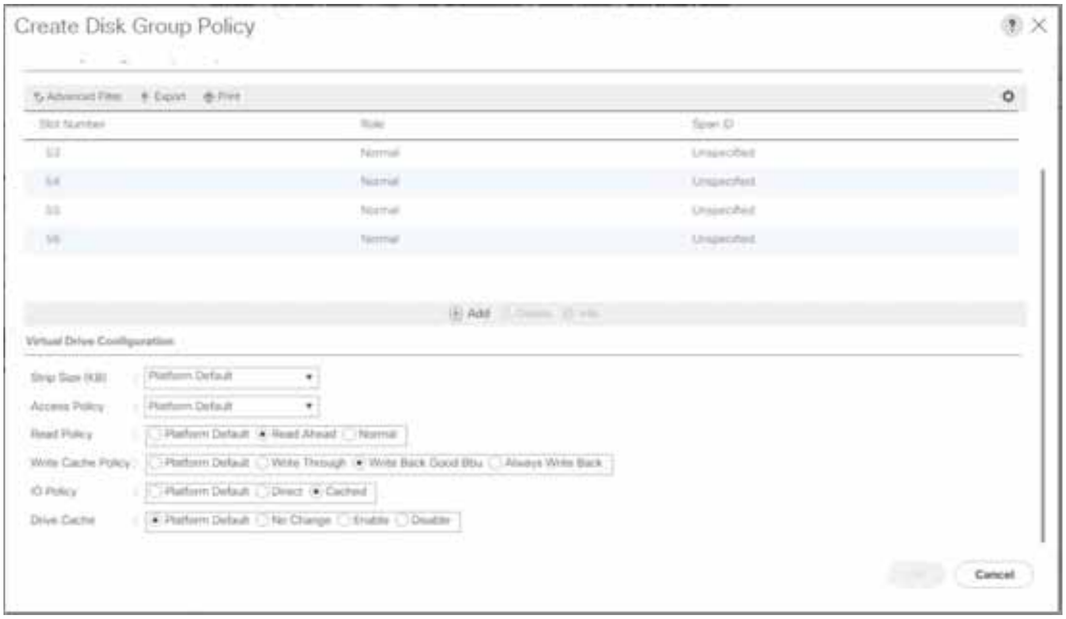
Select Read Ahead for Read Policy.

Select Write Back Good BBU for Write Cache Policy.

Select Cached for IO Policy.

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

Click OK.



Create Disk Group Policy

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

Virtual Drive Configuration

Strip Size (KB) : Platform Default

Access Policy : Platform Default

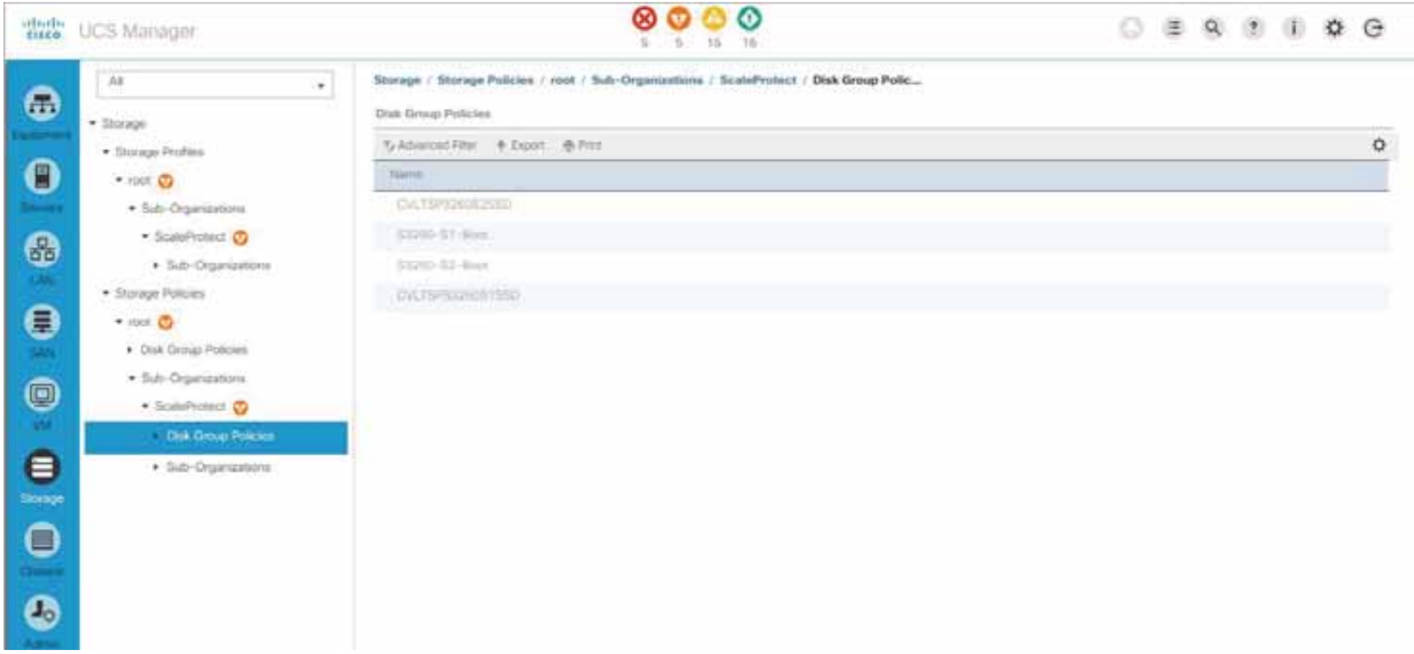
Read Policy : ○ Platform Default ● Read Ahead ○ Normal

Write Cache Policy : ○ Platform Default ○ Write Through ● Write Back Good Bbu ○ Always Write Back

IO Policy : ○ Platform Default ○ Direct ● Cached

Drive Cache : ● Platform Default ○ No Change ○ Enable ○ Disable

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



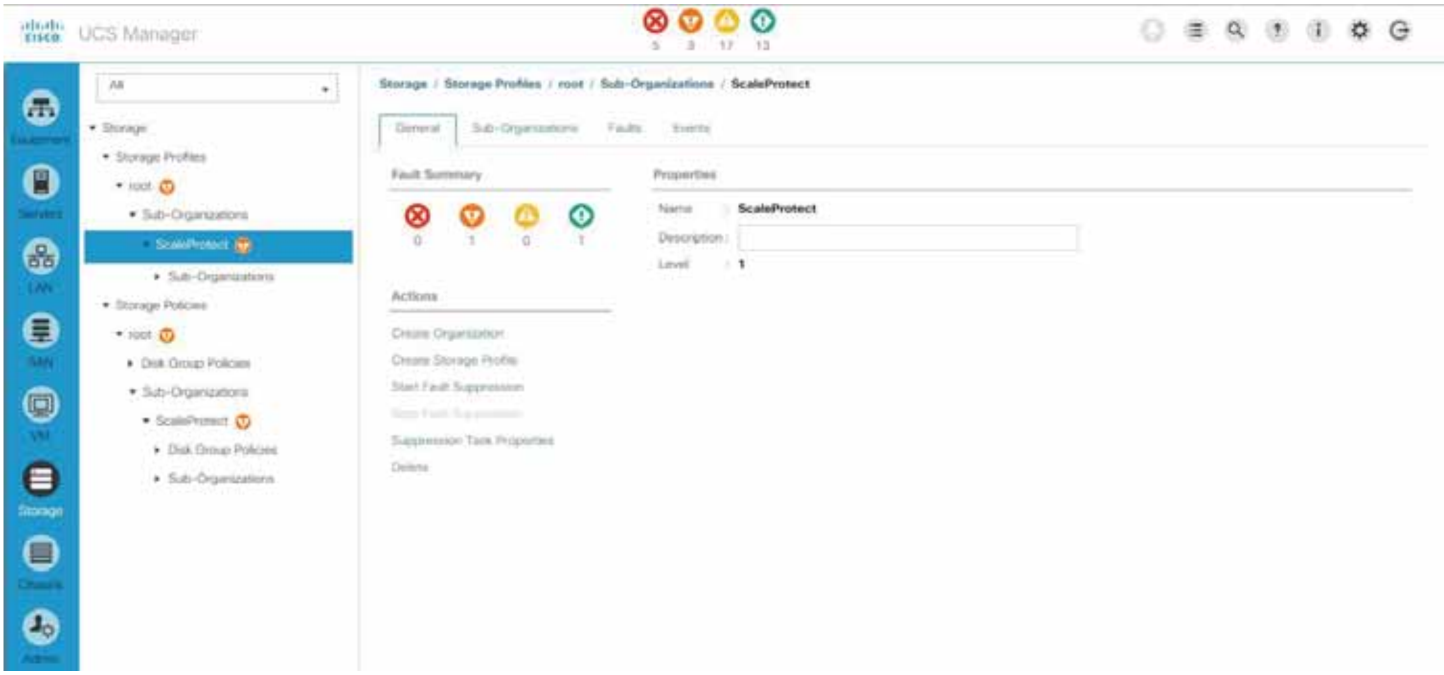
- Storage
  - Storage Profiles
    - root
      - Sub-Organizations
        - ScaleProtect
          - Sub-Organizations
  - Storage Policies
    - root
      - Disk Group Policies
      - Sub-Organizations
        - ScaleProtect
          - Disk Group Policies
          - Sub-Organizations

Storage / Storage Policies / root / Sub-Organizations / ScaleProtect / Disk Group Polic...

Disk Group Policies

Name
CVLTSP3260E2SSD
S3260-S1-Boot
S3260-S2-Boot
CVLTSP3260R1SSD

Go to Storage > Storage Profiles > root > Sub-Organizations > ScaleProtect and click Create Storage Profile.

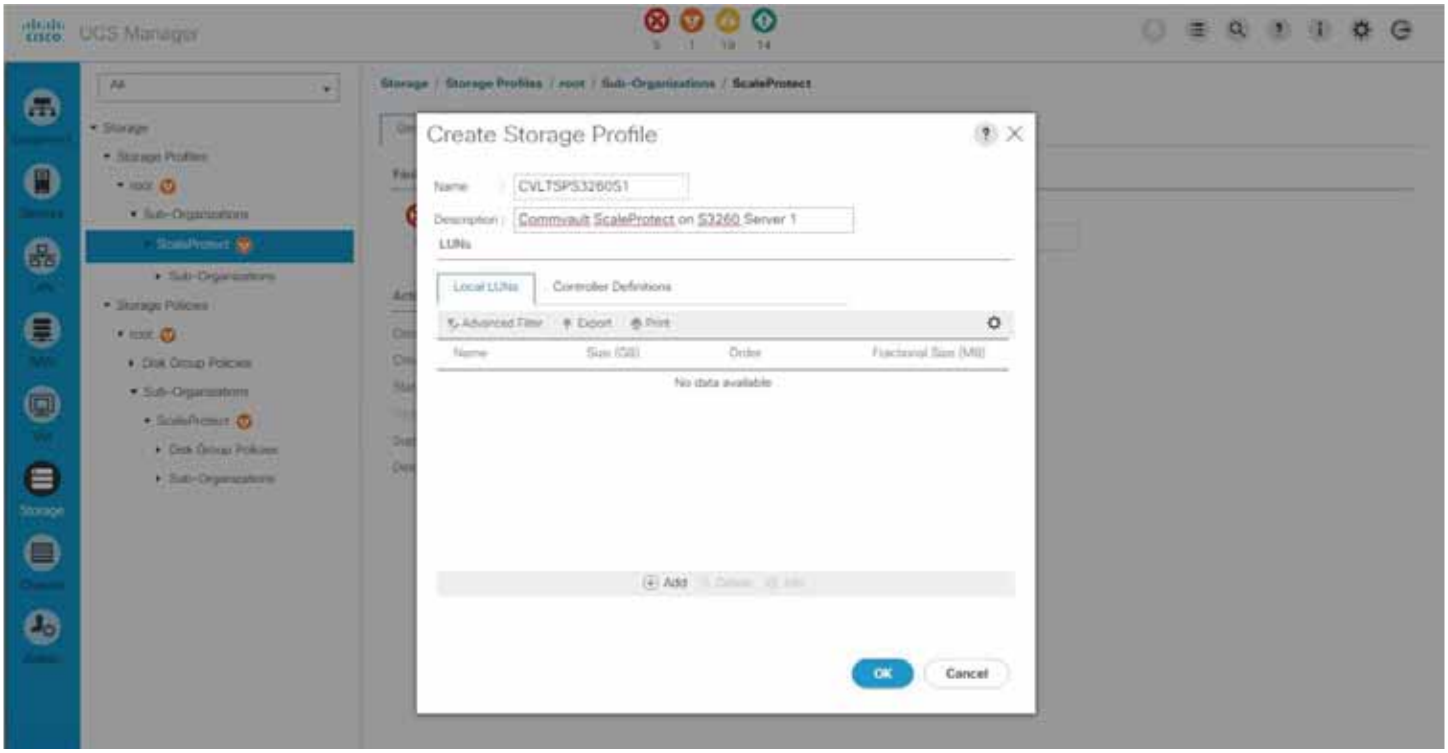


Name : ScaleProtect

Description :

Level : 1

Enter an obvious name and a description and click Add.



Name : CVLTSPS3260S1

Description : Commvault ScaleProtect on S3260 Server 1

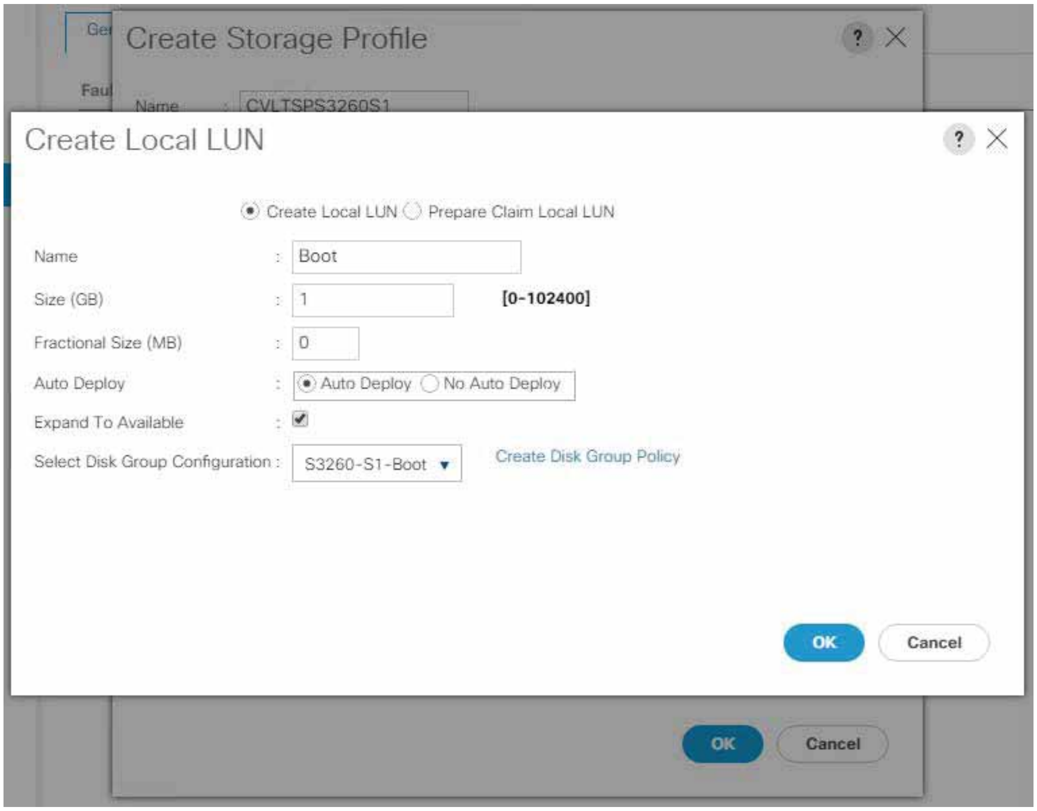
Enter **Boot** as the name.

Enter **1** as the size in GB.

Select the Expand to Available checkbox.

Select S3260-S1-Boot as the disk group configuration.

Click OK.



Create Storage Profile

Name : CVLTSPS3260S1

Create Local LUN

● Create Local LUN ○ Prepare Claim Local LUN

Name : Boot

Size (GB) : 1 [0-102400]

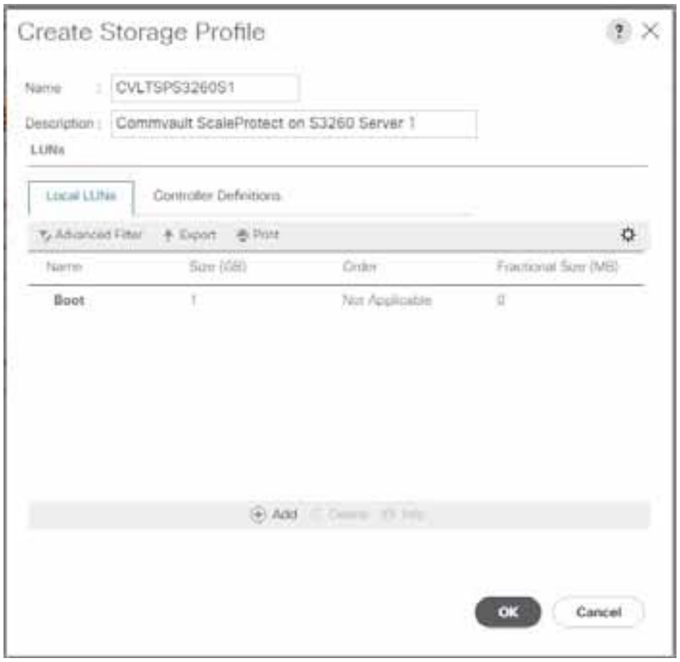
Fractional Size (MB) : 0

Auto Deploy : ● Auto Deploy ○ No Auto Deploy

Expand To Available : ☑

Select Disk Group Configuration : S3260-S1-Boot ▾

Click Add to continue creating LUNs in the SSD Disk Group.



Create Storage Profile

Name : CVLTSPS3260S1

Description : Commvault ScaleProtect on S3260 Server 1

LUNs

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

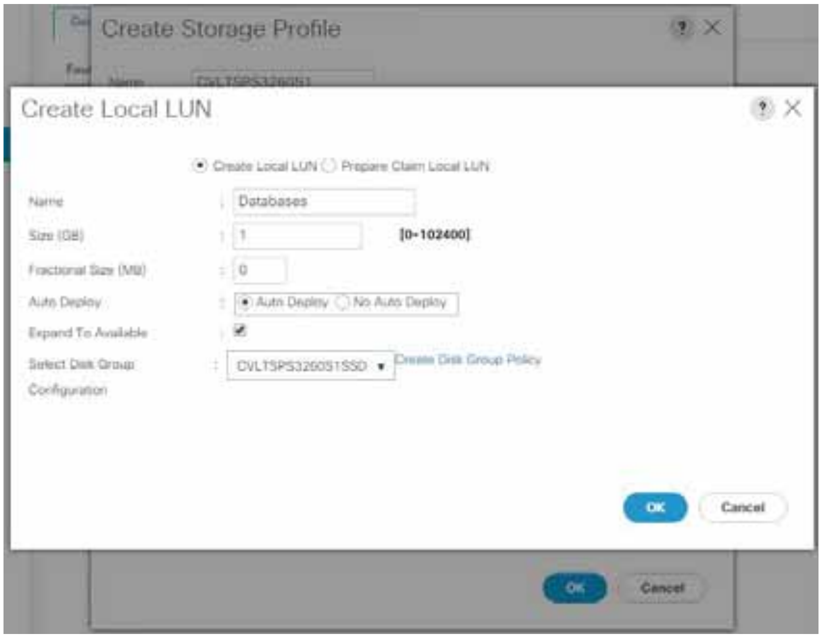
Enter **Databases** as the name.

Enter **1** as the size in GB.

Select the Expand to Available checkbox.

Select CVLTSPS3260S1SSD as the disk group.

Click OK.



Create Local LUN

● Create Local LUN ○ Prepare Claim Local LUN

Name : Databases

Size (GB) : 1 [0-102400]

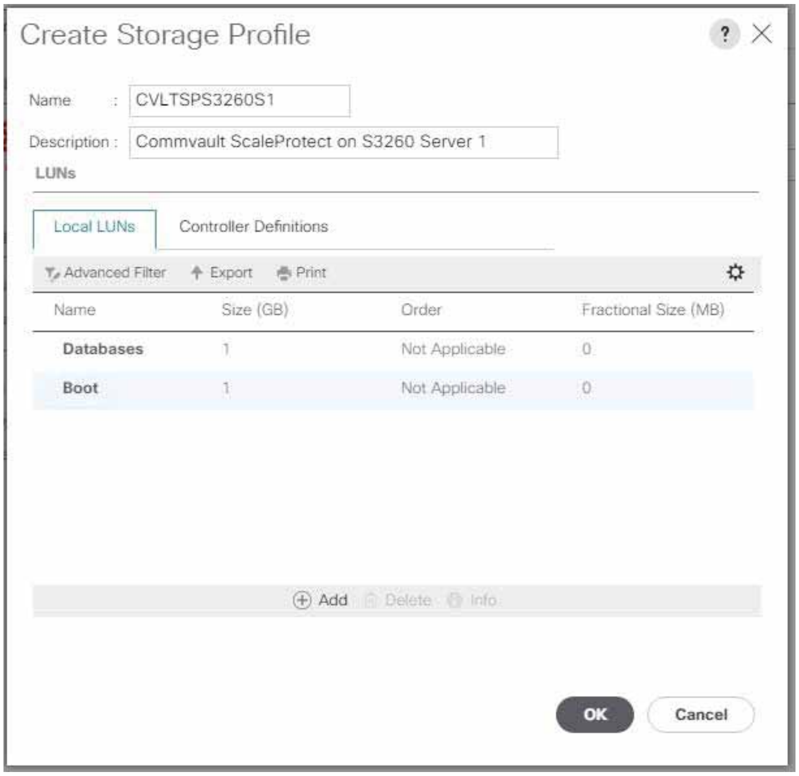
Fractional Size (MB) : 0

Auto Deploy : ● Auto Deploy ○ No Auto Deploy

Expand To Available : ☑

Select Disk Group Configuration : CVLTSPS3260S1SSD

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



Create Storage Profile

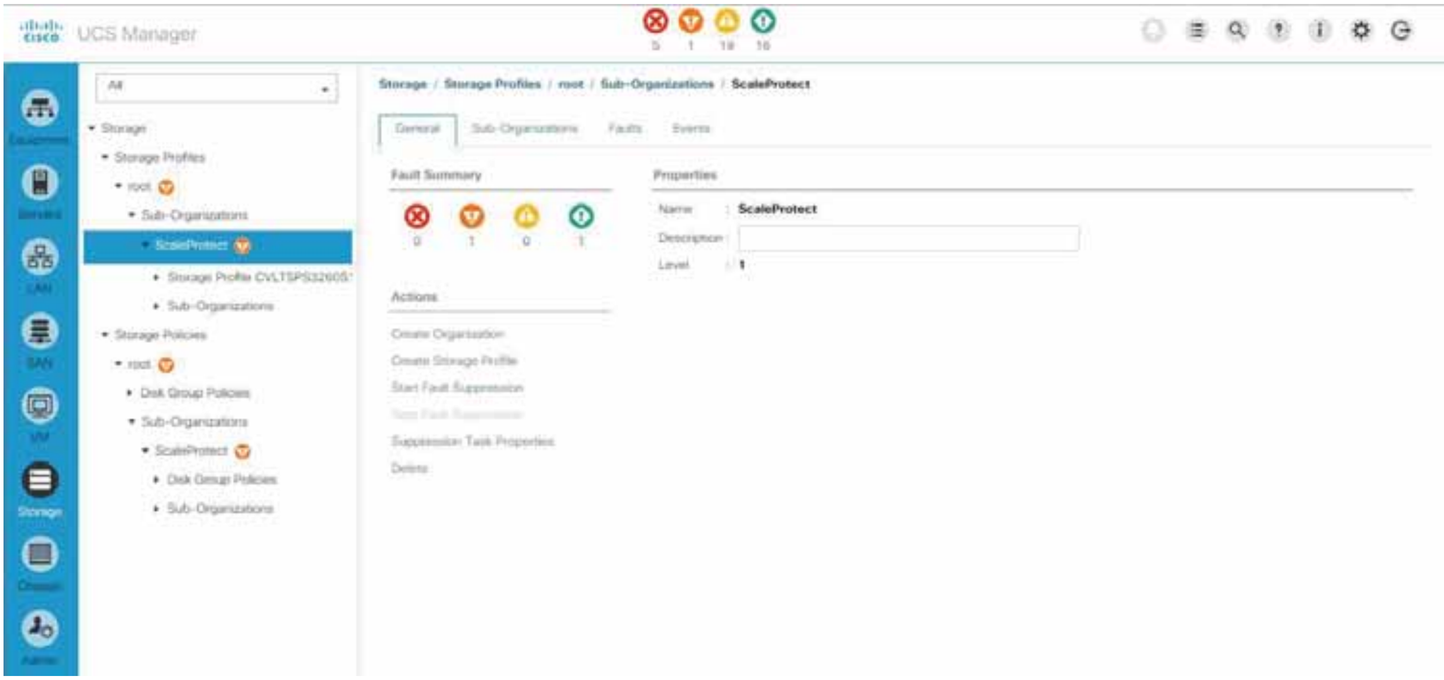
Name : CVLTSPS3260S1

Description : Commvault ScaleProtect on S3260 Server 1

LUNs

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

Click Create Storage Profile.



UCS Manager

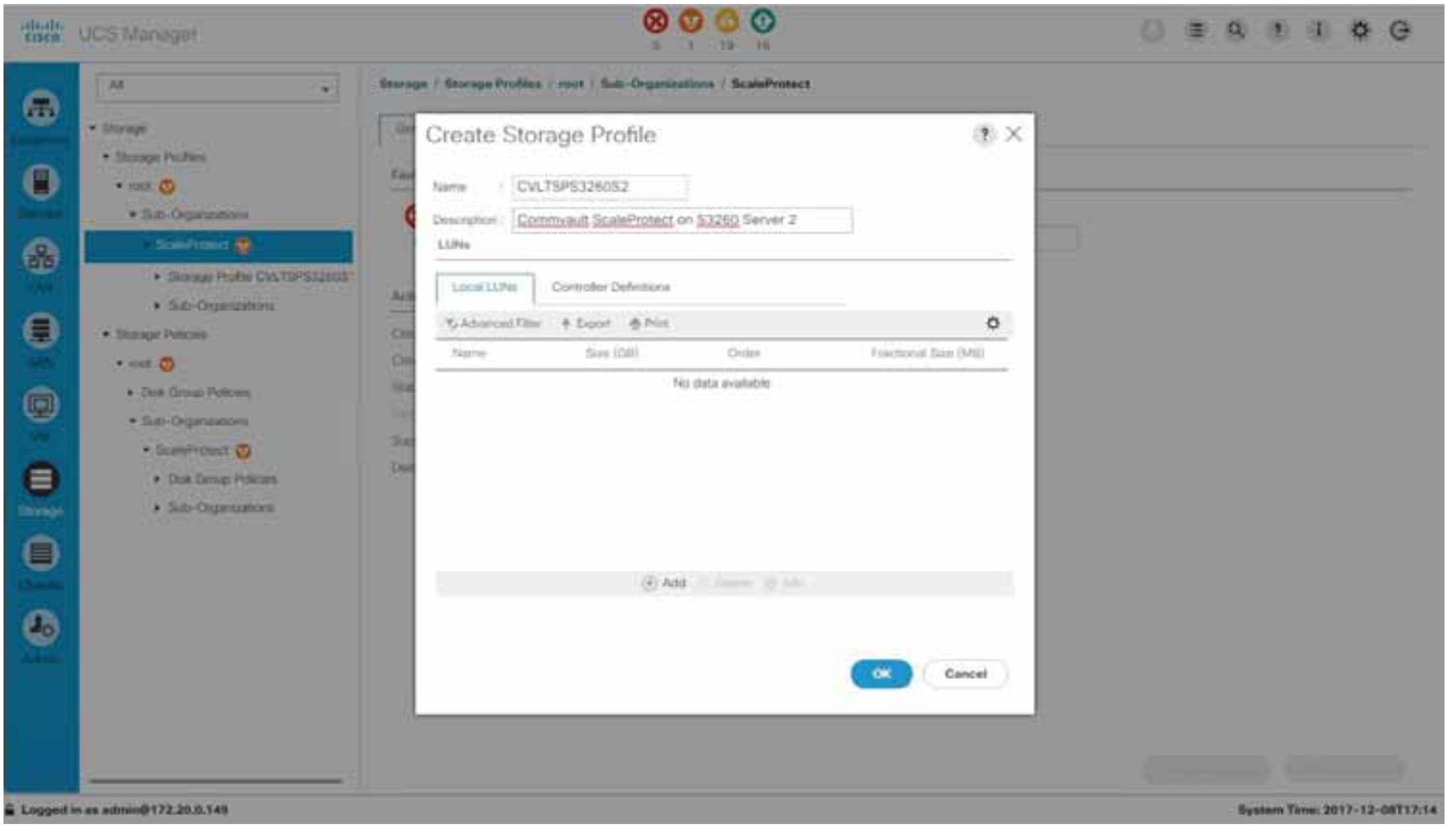
Storage / Storage Profiles / root / Sub-Organizations / ScaleProtect

Name : ScaleProtect

Description :

Level : 1

Enter an obvious name and a description and click Add.



Create Storage Profile

Name : CVLTSPS3260S2

Description : Commvault ScaleProtect on S3260 Server 2

LUNs

Local LUNs | Controller Definitions

Name	Size (GB)	Order	Fractional Size (MB)

No data available

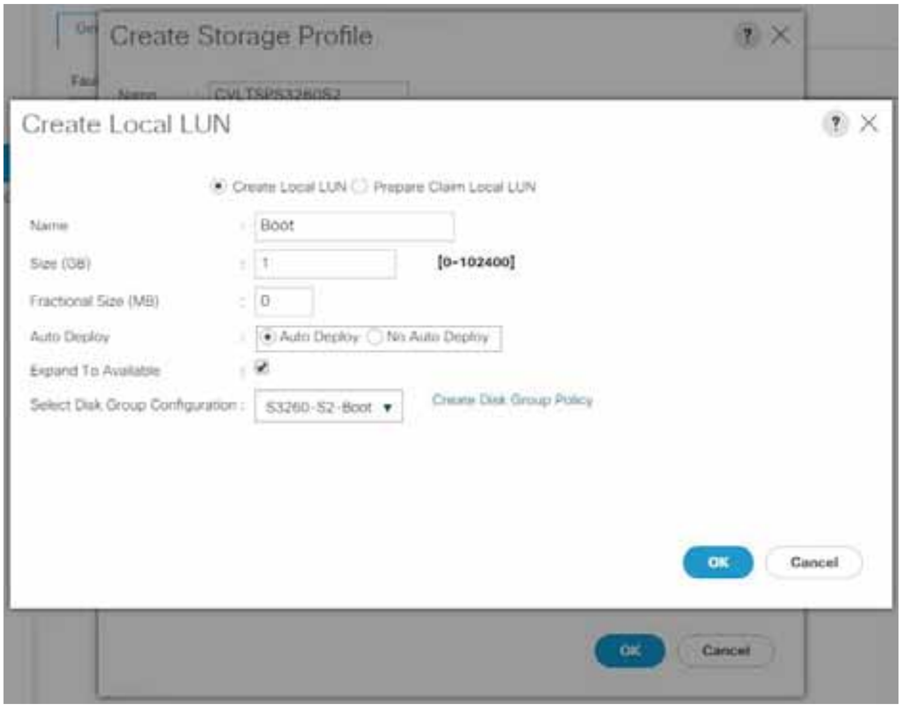
Enter **Boot** as the name.

Enter **1** as the size in GB.

Select the Expand to Available checkbox.

Select S3260-S2-Boot as the disk group configuration.

Click OK.



Create Local LUN

● Create Local LUN ○ Prepare Claim Local LUN

Name : Boot

Size (GB) : 1 [0-102400]

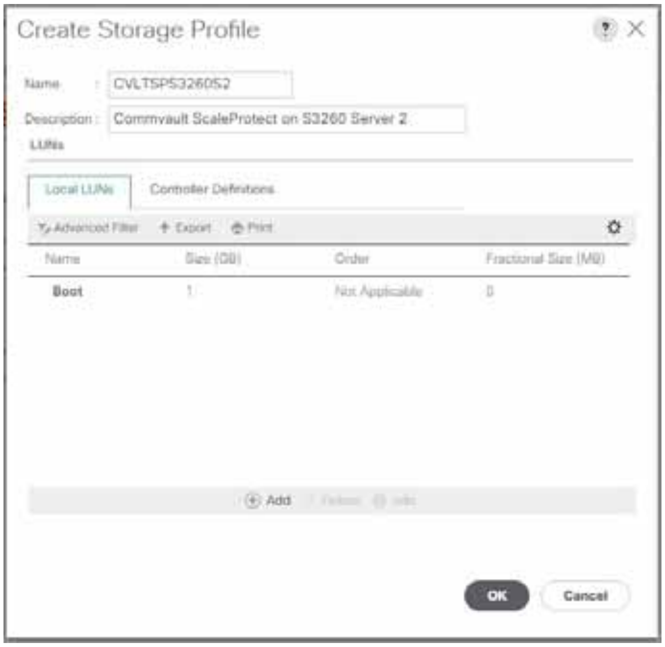
Fractional Size (MB) : 0

Auto Deploy : ● Auto Deploy ○ No Auto Deploy

Expand To Available : ☑

Select Disk Group Configuration : S3260-S2-Boot

Click Add to continue creating LUNs in the SSD disk group.



Create Storage Profile

Name : CVLTSPS326052

Description : Commvault ScaleProtect on S3260 Server 2

LUNs

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

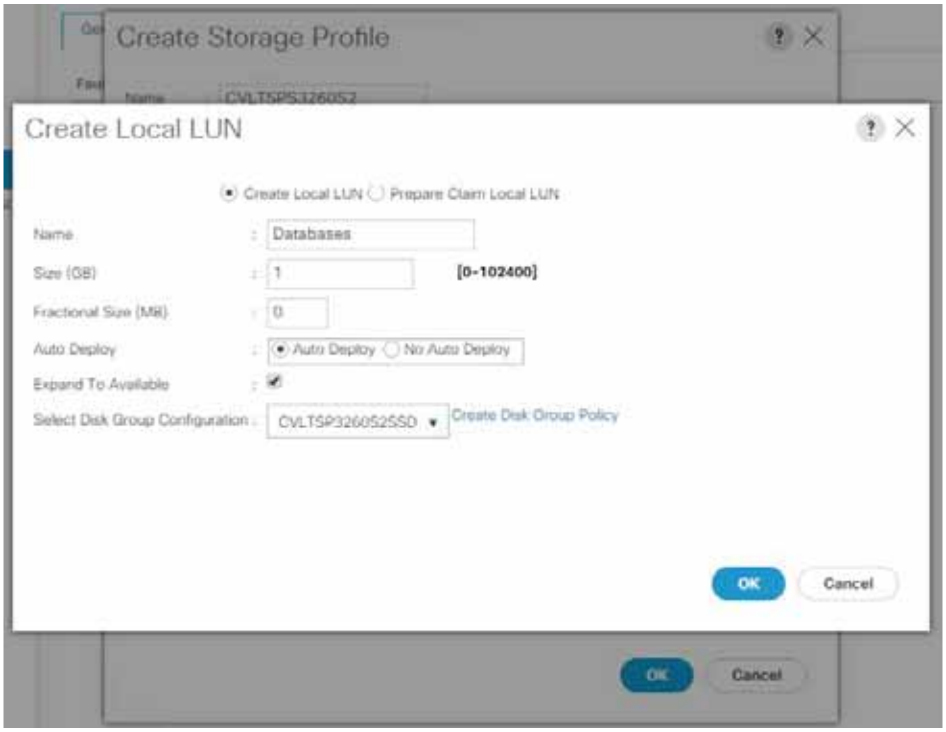
Enter **Databases** as the name.

Enter **1** as the size in GB.

Select the Expand to Available checkbox.

Select CVLTSPS3260S2SSD as the disk group.

Click OK.



Create Storage Profile

Name : CVLTSPS3260S2

Create Local LUN

● Create Local LUN ○ Prepare Claim Local LUN

Name : Databases

Size (GB) : 1 [0-102400]

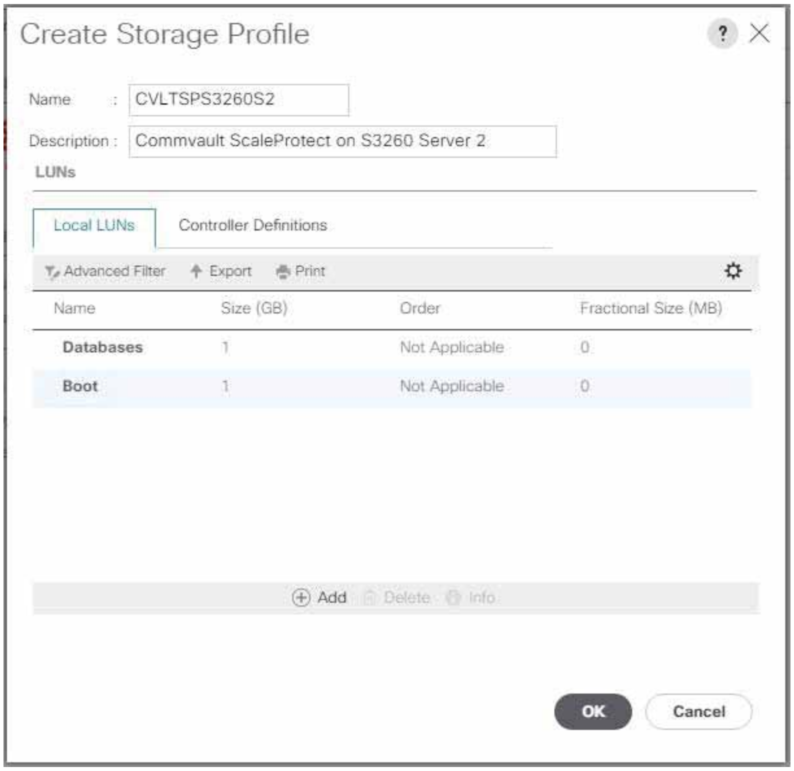
Fractional Size (MB) : 0

Auto Deploy : ● Auto Deploy ○ No Auto Deploy

Expand To Available : ☑

Select Disk Group Configuration : CVLTSP3260S2SSD ▾ Create Disk Group Policy

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



Create Storage Profile

Name : CVLTSPS3260S2

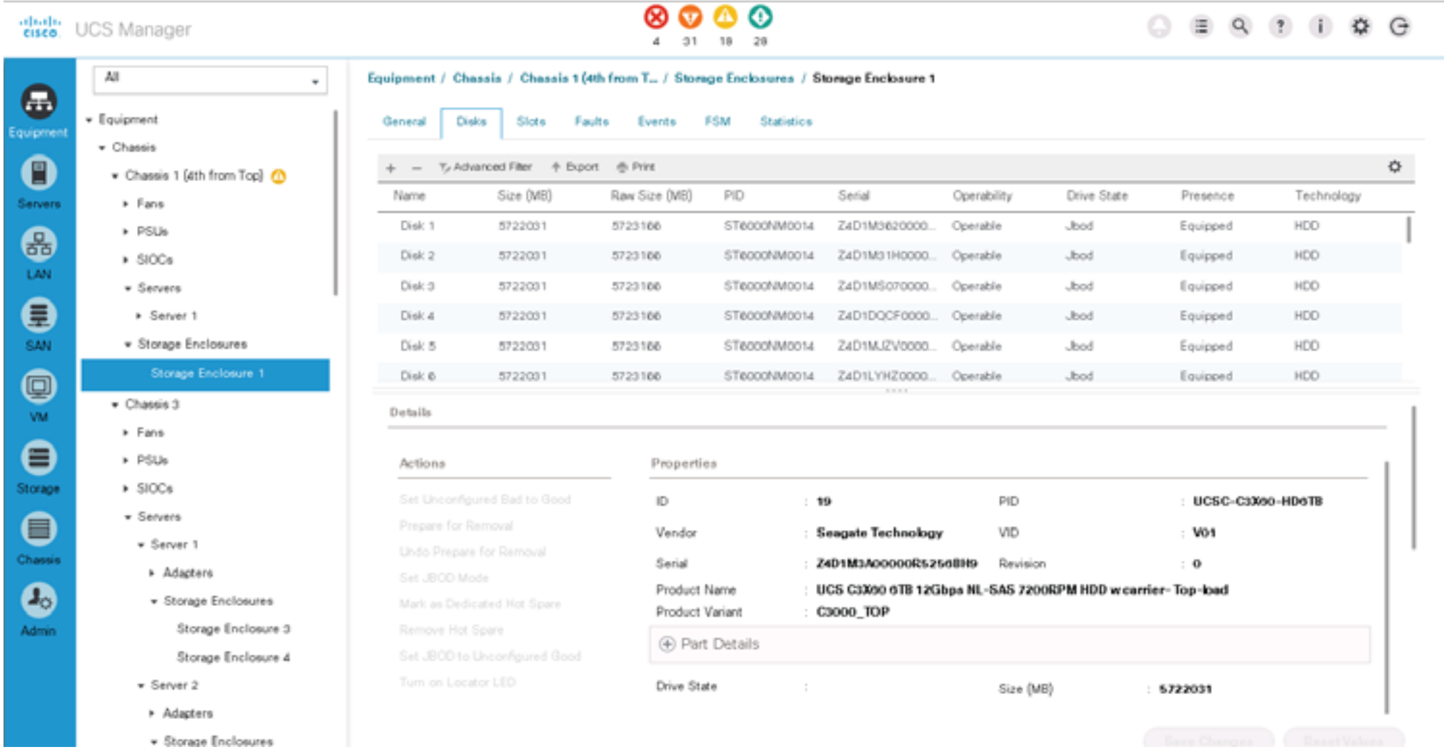
Description : Commvault ScaleProtect on S3260 Server 2

LUNs

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

All the HDDs are used in JBOD mode, so no LUNs need to be created.

To check or set the JBOD mode, go to Equipment > Chassis > Chassis X > Storage Enclosure 1 and select the Disks pane.



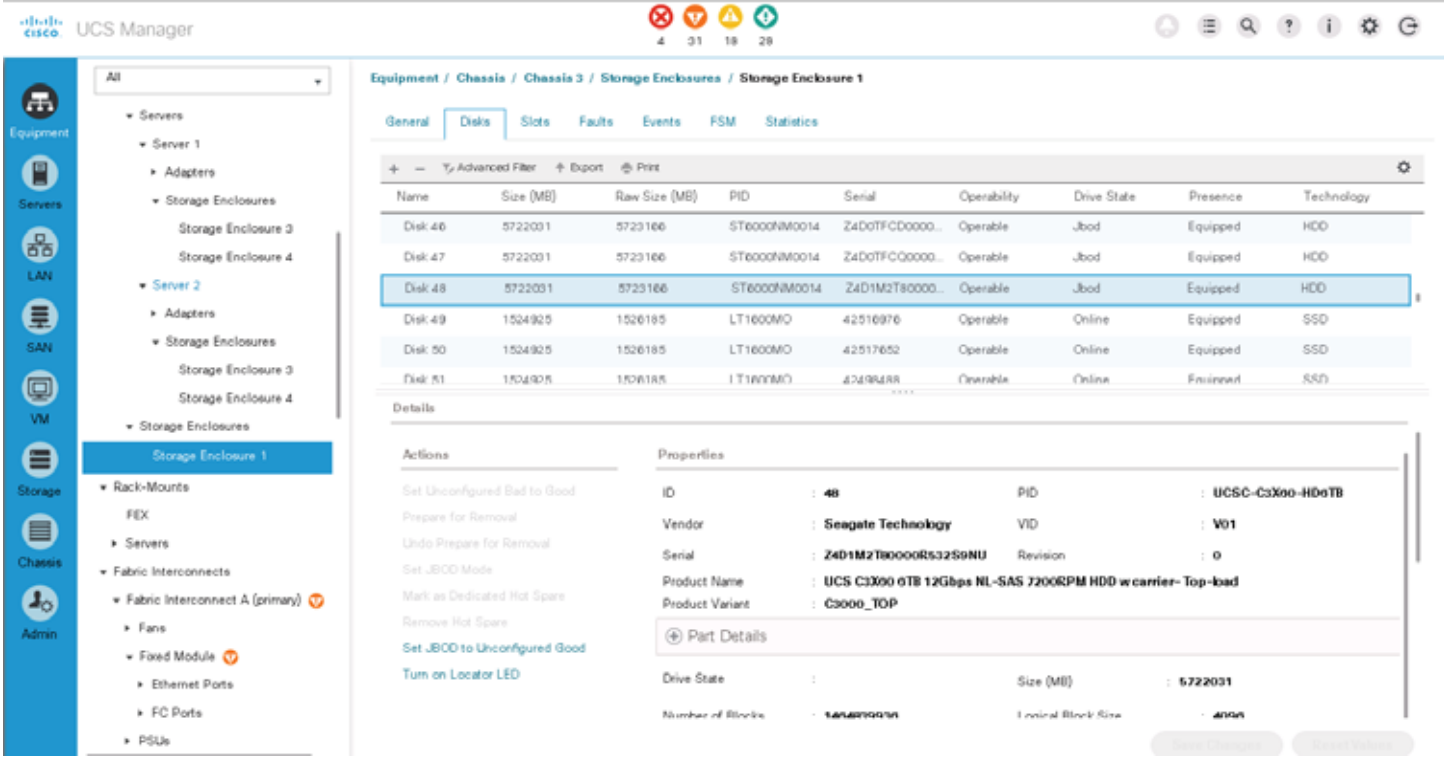
Name	Size (MB)	Raw Size (MB)	PID	Serial	Operability	Drive State	Presence	Technology
Disk 1	5722031	5723166	ST6000NM0014	Z4D1M3620000...	Operable	Jbod	Equipped	HDD
Disk 2	5722031	5723166	ST6000NM0014	Z4D1M31H0000...	Operable	Jbod	Equipped	HDD
Disk 3	5722031	5723166	ST6000NM0014	Z4D1MS070000...	Operable	Jbod	Equipped	HDD
Disk 4	5722031	5723166	ST6000NM0014	Z4D1DQCF0000...	Operable	Jbod	Equipped	HDD
Disk 5	5722031	5723166	ST6000NM0014	Z4D1MJZV0000...	Operable	Jbod	Equipped	HDD
Disk 6	5722031	5723166	ST6000NM0014	Z4D1LYHZ0000...	Operable	Jbod	Equipped	HDD

ID : 19
PID : UCSC-C3X60-HD6TB
Vendor : Seagate Technology
VID : V01
Serial : Z4D1M3A00000R52568H9
Revision : 0
Product Name : UCS C3X60 6TB 12Gbps NL-SAS 7200RPM HDD w carrier- Top-load
Product Variant : C3000_TOP
Drive State :
Size (MB) : 5722031

Select a disk to show the details.

If any of the HDDs shown as Online in the RAID group configuration on this disk need be deleted to convert the status to Unconfigured Good, use the Cisco UCS documentation to do so.

If any of the HHDs are shown as Unconfigured Good, select the drive and click Set JBOD mode.



Equipment / Chassis / Chassis 3 / Storage Enclosures / Storage Enclosure 1

Name	Size (MB)	Raw Size (MB)	PID	Serial	Operability	Drive State	Presence	Technology
Disk 46	5722031	5723166	ST6000NM0014	Z4D0TFCD0000...	Operable	Jbod	Equipped	HDD
Disk 47	5722031	5723166	ST6000NM0014	Z4D0TFCQ0000...	Operable	Jbod	Equipped	HDD
Disk 48	5722031	5723166	ST6000NM0014	Z4D1M2T80000...	Operable	Jbod	Equipped	HDD
Disk 49	1524925	1526185	LT1600MO	42516976	Operable	Online	Equipped	SSD
Disk 50	1524925	1526185	LT1600MO	42517652	Operable	Online	Equipped	SSD
Disk 51	1524925	1526185	LT1600MO	42498488	Operable	Online	Equipped	SSD

Details

Actions

- Set Unconfigured Bad to Good
- Prepare for Removal
- Undo Prepare for Removal
- Set JBOD Mode
- Mark as Dedicated Hot Spare
- Remove Hot Spare
- Set JBOD to Unconfigured Good
- Turn on Locator LED

Properties

ID	: 48	PID	: UCSC-C3X60-HD6TB
Vendor	: Seagate Technology	VID	: V01
Serial	: Z4D1M2T80000R532S9NU	Revision	: 0
Product Name	: UCS C3X60 6TB 12Gbps NL-SAS 7200RPM HDD w carrier- Top-load		
Product Variant	: C3000_TOP		

⊕ Part Details

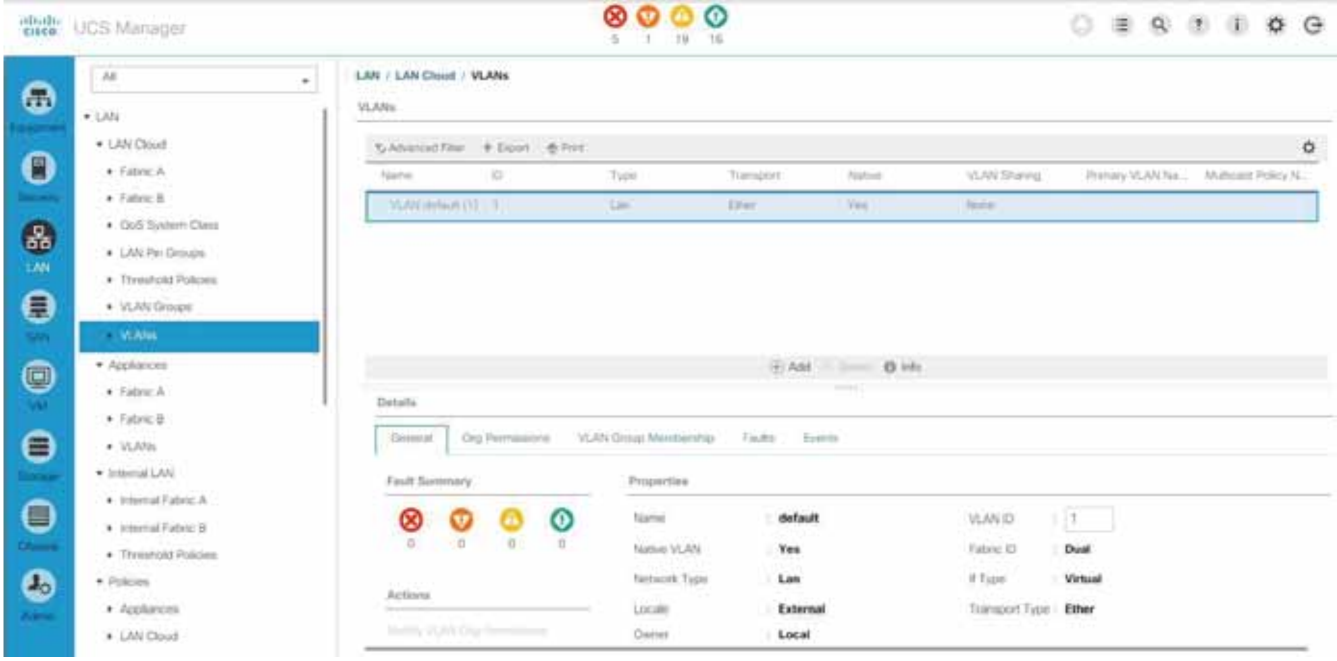
Drive State	:	Size (MB)	: 5722031
Number of Blocks	: 1464839936	Logical Block Size	: 4096

Repeat this step for all chassis used in the ScaleProtect solution.

LAN configuration

The next task is to configure the networks required for Commvault ScaleProtect. In general, two networks are required. The first network is the access network; in most cases, this is the data center backup network. The second network is the ScaleProtect internal cluster network.

Go to LAN > LAN Cloud > VLANs and click Add.



LAN / LAN Cloud / VLANs

VLANs

Name	ID	Type	Transport	Native	VLAN Sharing	Primary VLAN Na...	Multicast Policy N...
VLAN default (1)	1	Lan	Ether	Yes	None		

Details

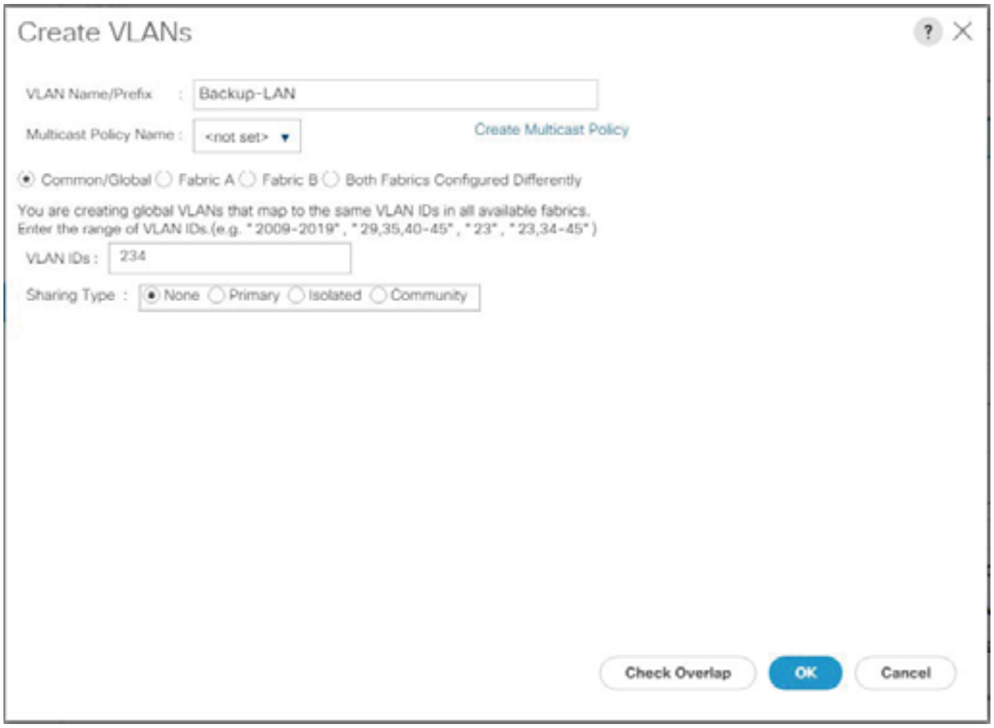
Properties

Name	: default	VLAN ID	: 1
Native VLAN	: Yes	Fabric ID	: Dual
Network Type	: Lan	If Type	: Virtual
Locale	: External	Transport Type	: Ether
Owner	: Local		

Enter an obvious name for the VLAN.

Enter the VLAN ID defined for the backup network in your landscape.

Click OK.



Create VLANs

VLAN Name/Prefix : Backup-LAN

Multicast Policy Name : <not set> ▾

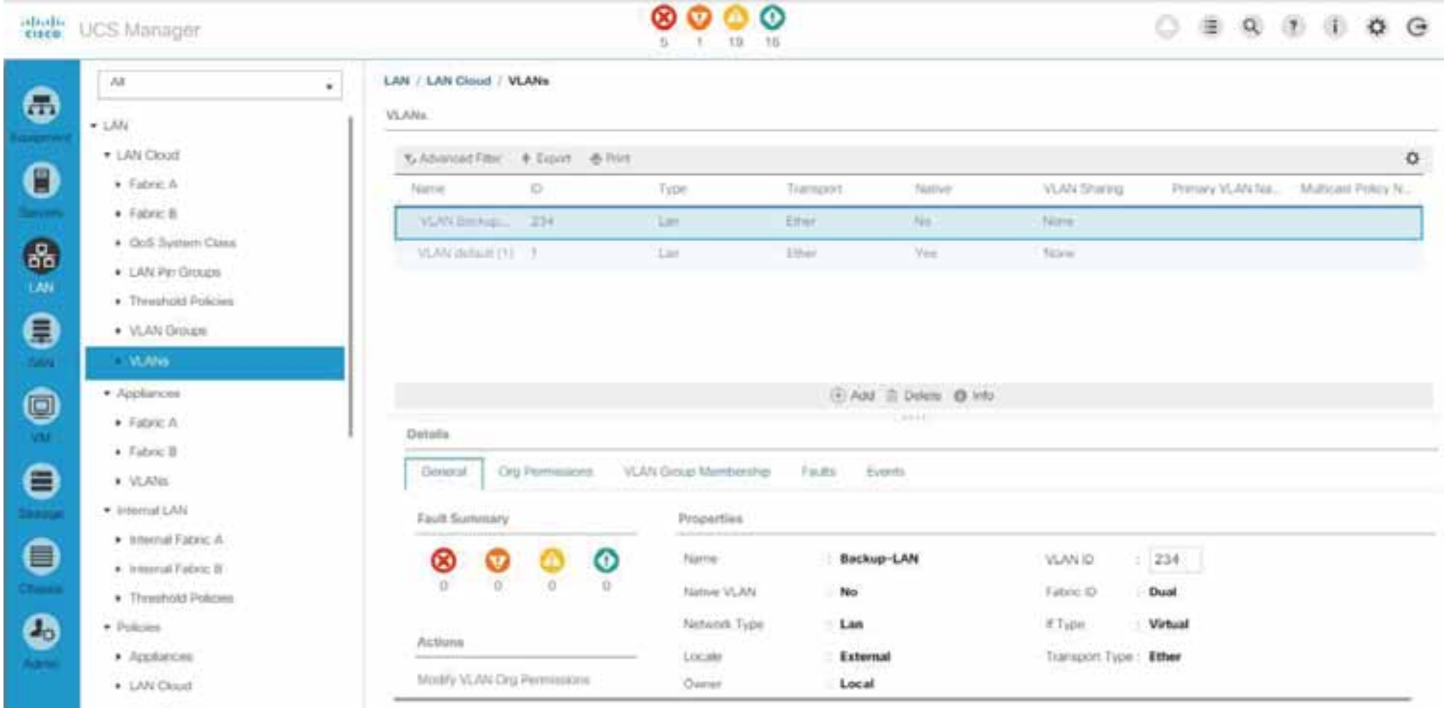
● Common/Global ○ Fabric A ○ Fabric B ○ Both Fabrics Configured Differently

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

VLAN IDs : 234

Sharing Type : ● None ○ Primary ○ Isolated ○ Community

Click Add.



LAN / LAN Cloud / VLANs

VLANs

Name	ID	Type	Transport	Native	VLAN Sharing	Primary VLAN Na...	Multicast Policy N...
VLAN Backup...	234	Lan	Ether	No	None		
VLAN default (1)	1	Lan	Ether	Yes	None		

Details

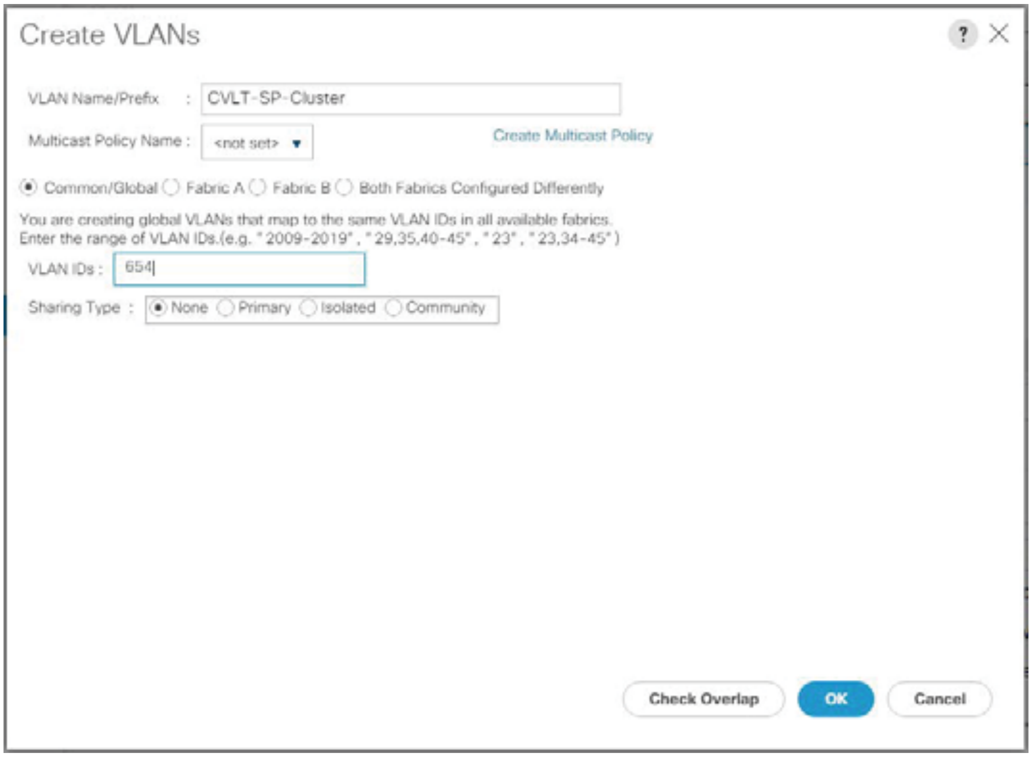
Properties

Name	: Backup-LAN	VLAN ID	: 234
Native VLAN	: No	Fabric ID	: Dual
Network Type	: Lan	If Type	: Virtual
Locale	: External	Transport Type	: Ether
Owner	: Local		

Enter an obvious name for the VLAN.

Enter the VLAN ID defined for the ScaleProtect cluster internal network.

Click OK.



Create VLANs

VLAN Name/Prefix : CVLT-SP-Cluster

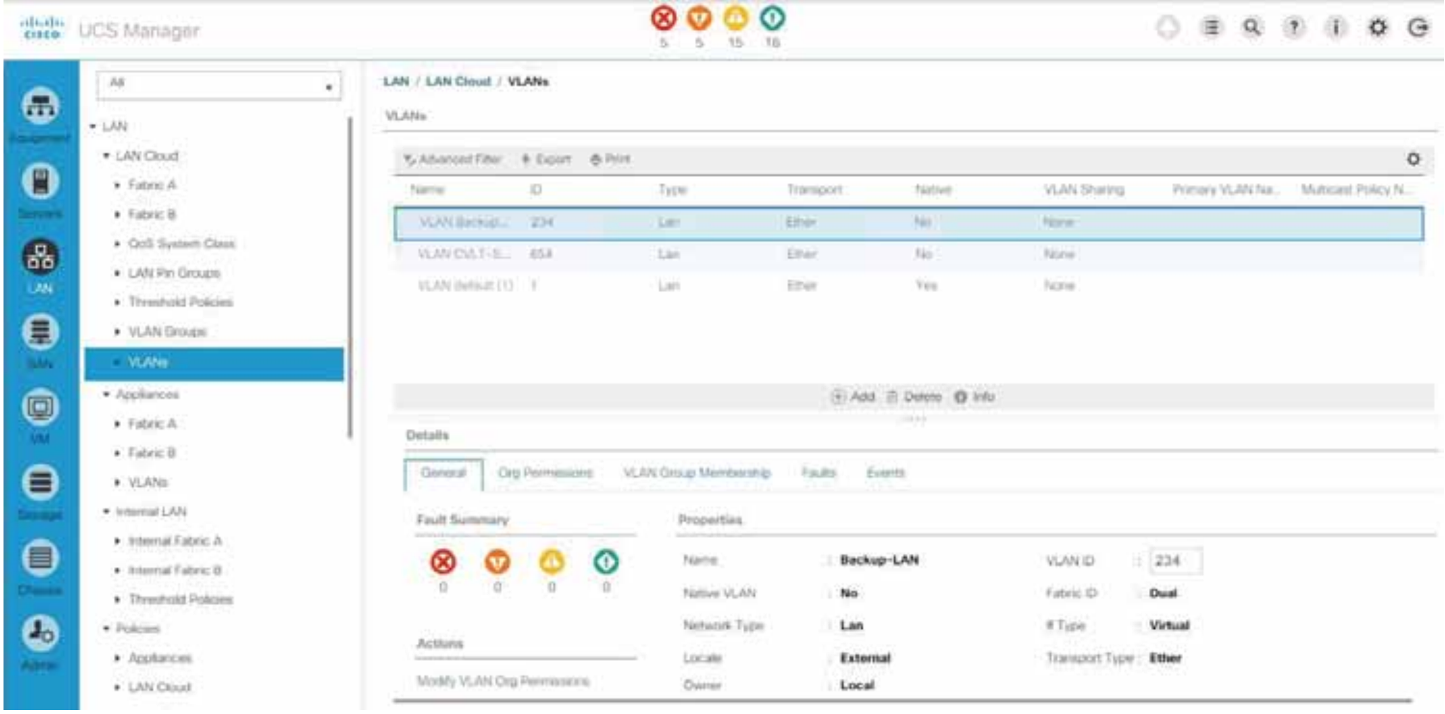
Multicast Policy Name : <not set>

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

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

VLAN IDs : 654

Sharing Type : ● None ○ Primary ○ Isolated ○ Community



LAN / LAN Cloud / VLANs

VLANs

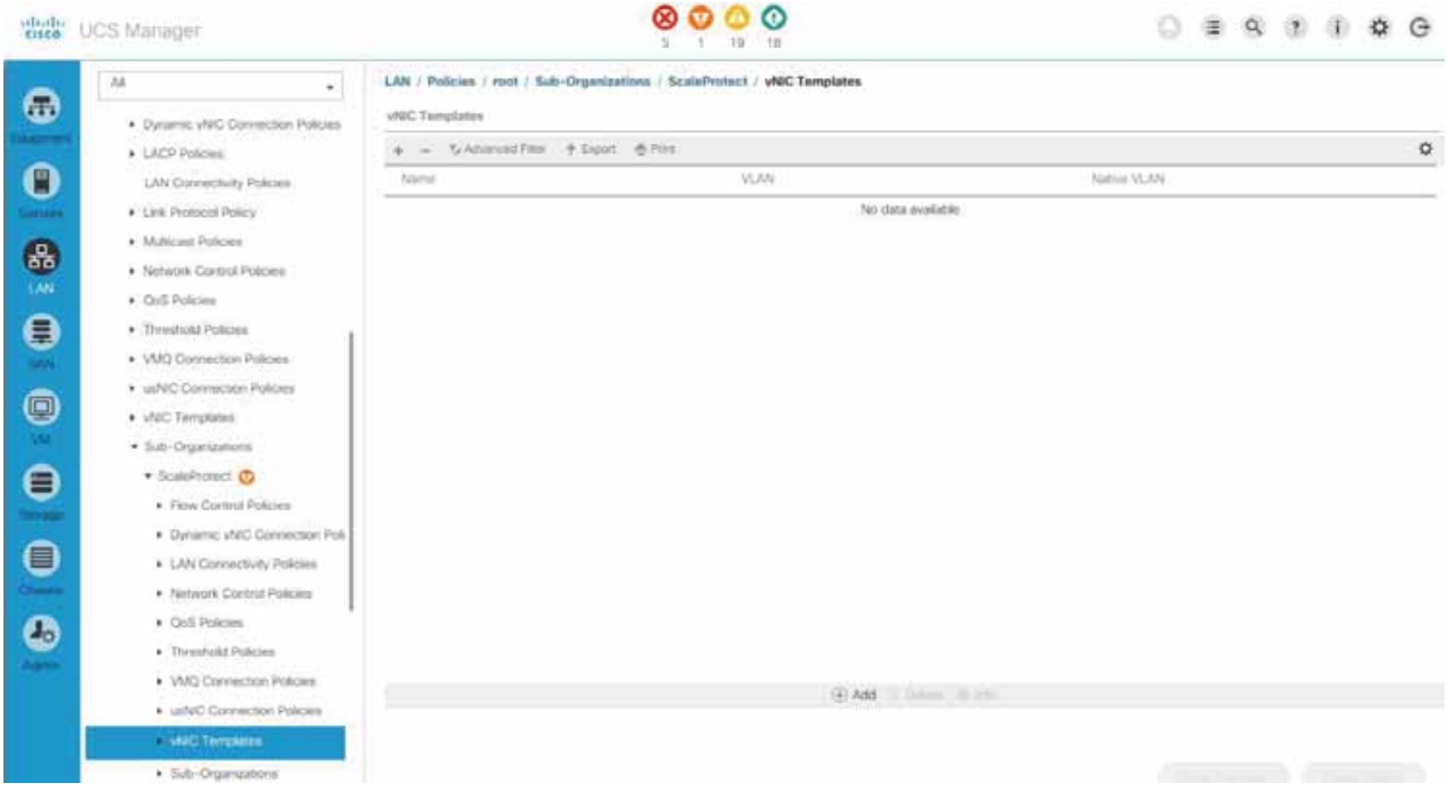
Name	ID	Type	Transport	Native	VLAN Sharing	Primary VLAN Na...	Multicast Policy N...
VLAN Backup-...	234	Lan	Ether	No	None		
VLAN CVLT-S...	654	Lan	Ether	No	None		
VLAN default (1)	1	Lan	Ether	Yes	None		

Details

Properties

Name	: Backup-LAN	VLAN ID	: 234
Native VLAN	: No	Fabric ID	: Dual
Network Type	: Lan	If Type	: Virtual
Locale	: External	Transport Type	: Ether
Owner	: Local		

Go to LAN > Policies > root > Sub-Organizations > ScaleProtect > vNIC Templates and click Add.



LAN / Policies / root / Sub-Organizations / ScaleProtect / vNIC Templates

vNIC Templates

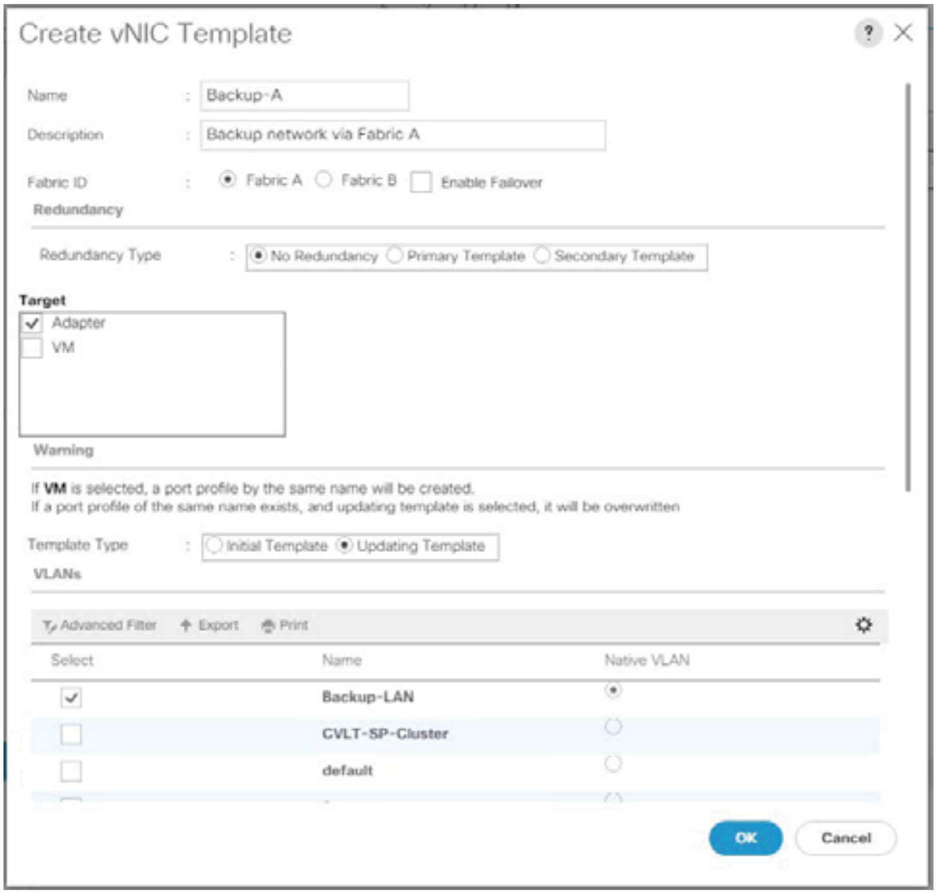
Name	VLAN	Native VLAN
No data available		

Enter an obvious name for the access network for the ScaleProtect solution, which is usually the backup network.

Select the radio button for Fabric A.

Select the radio button for Updating Template.

Select the checkbox for Backup-LAN and select the Native VLAN radio button.



Create vNIC Template

Name : Backup-A

Description : Backup network via Fabric A

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

Redundancy

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

Target

☑ Adapter

□ VM

Warning

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

Template Type : ○ Initial Template ● Updating Template

VLANs

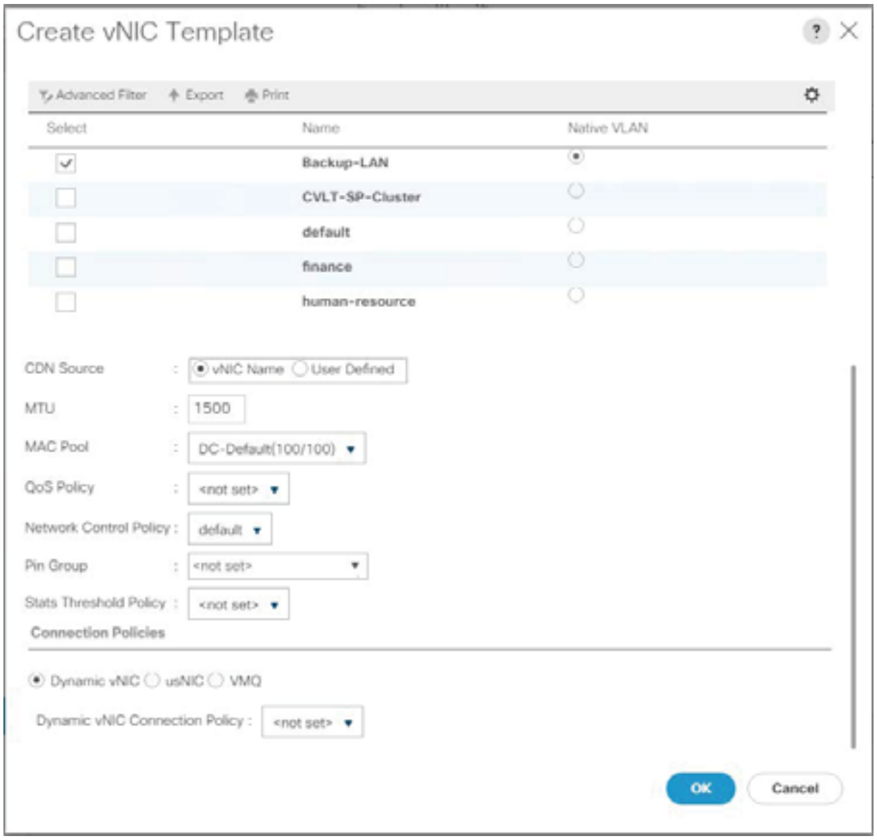
Select	Name	Native VLAN
☑	**Backup-LAN**	●
□	**CVLT-SP-Cluster**	○
□	**default**	○

Enter **1500** or **9000** for the MTU value. MTU 9000 works only if all network components and the server are configured with MTU 9000. Check with your network administrator and server administrator to determine which value to use.

Select a MAC pool with free addresses.

Set QoS policy and network control policy as defined by your local network administrator.

Click OK.



Create vNIC Template

Select	Name	Native VLAN
☑	Backup-LAN	●
□	CVLT-SP-Cluster	○
□	default	○
□	finance	○
□	human-resource	○

CDN Source : ● vNIC Name ○ User Defined

MTU : 1500

MAC Pool : DC-Default(100/100)

QoS Policy : <not set>

Network Control Policy : default

Pin Group : <not set>

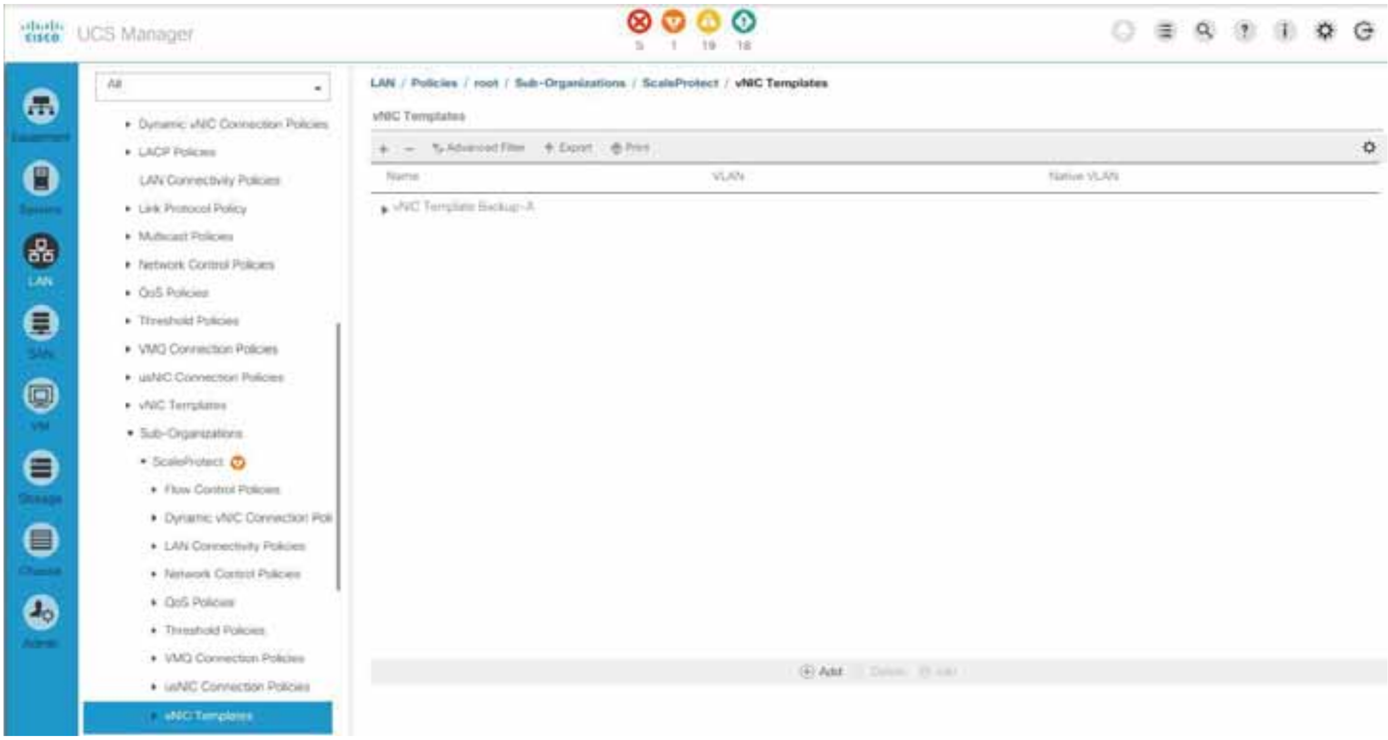
Stats Threshold Policy : <not set>

Connection Policies

● Dynamic vNIC ○ usNIC ○ VMQ

Dynamic vNIC Connection Policy : <not set>

Click Add.



LAN / Policies / root / Sub-Organizations / ScaleProtect / vNIC Templates

vNIC Templates

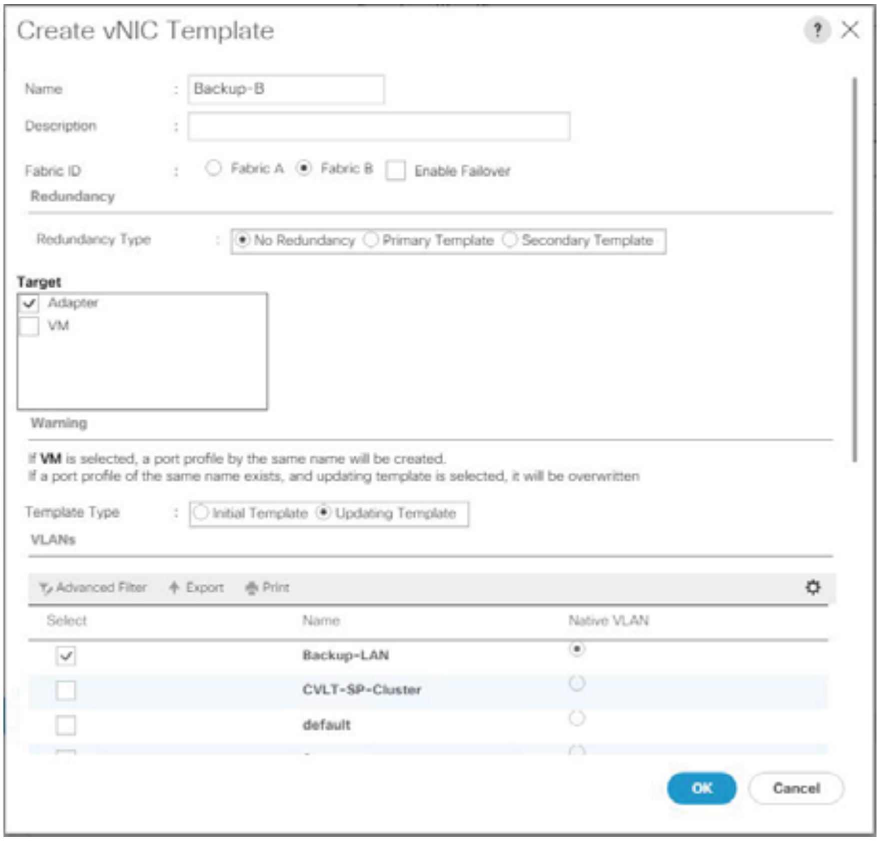
Name	VLAN	Native VLAN
vNIC Template Backup-A		

Enter an obvious name for the access network to the ScaleProtect solution, which is usually the backup network.

Select the radio button for Fabric B.

Select the radio button for Updating Template.

Select the checkbox for Backup-LAN and select the Native VLAN radio button.



Create vNIC Template

Name : Backup-B

Description :

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

Redundancy

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

Target

☑ Adapter

□ VM

Warning

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

Template Type : ○ Initial Template ● Updating Template

VLANs

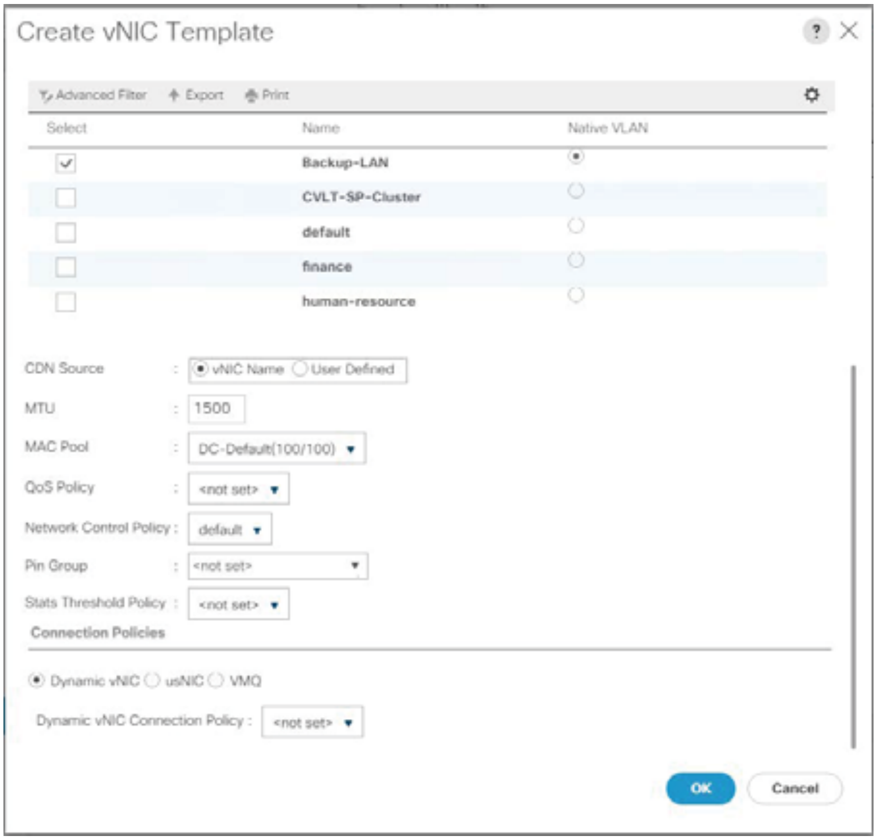
Select	Name	Native VLAN
☑	**Backup-LAN**	●
□	**CVLT-SP-Cluster**	○
□	**default**	○

Enter **1500** or **9000** for the MTU value. MTU 9000 works only if all network components and the server are configured with MTU 9000. Check with your network administrator and server administrator to determine which value to use.

Select a MAC pool with free addresses.

Set QoS policy and network control policy as defined by your local network administrator.

Click OK.



Create vNIC Template

Select	Name	Native VLAN
☑	Backup-LAN	●
□	CVLT-SP-Cluster	○
□	default	○
□	finance	○
□	human-resource	○

CDN Source : ● vNIC Name ○ User Defined

MTU : 1500

MAC Pool : DC-Default(100/100)

QoS Policy : <not set>

Network Control Policy : default

Pin Group : <not set>

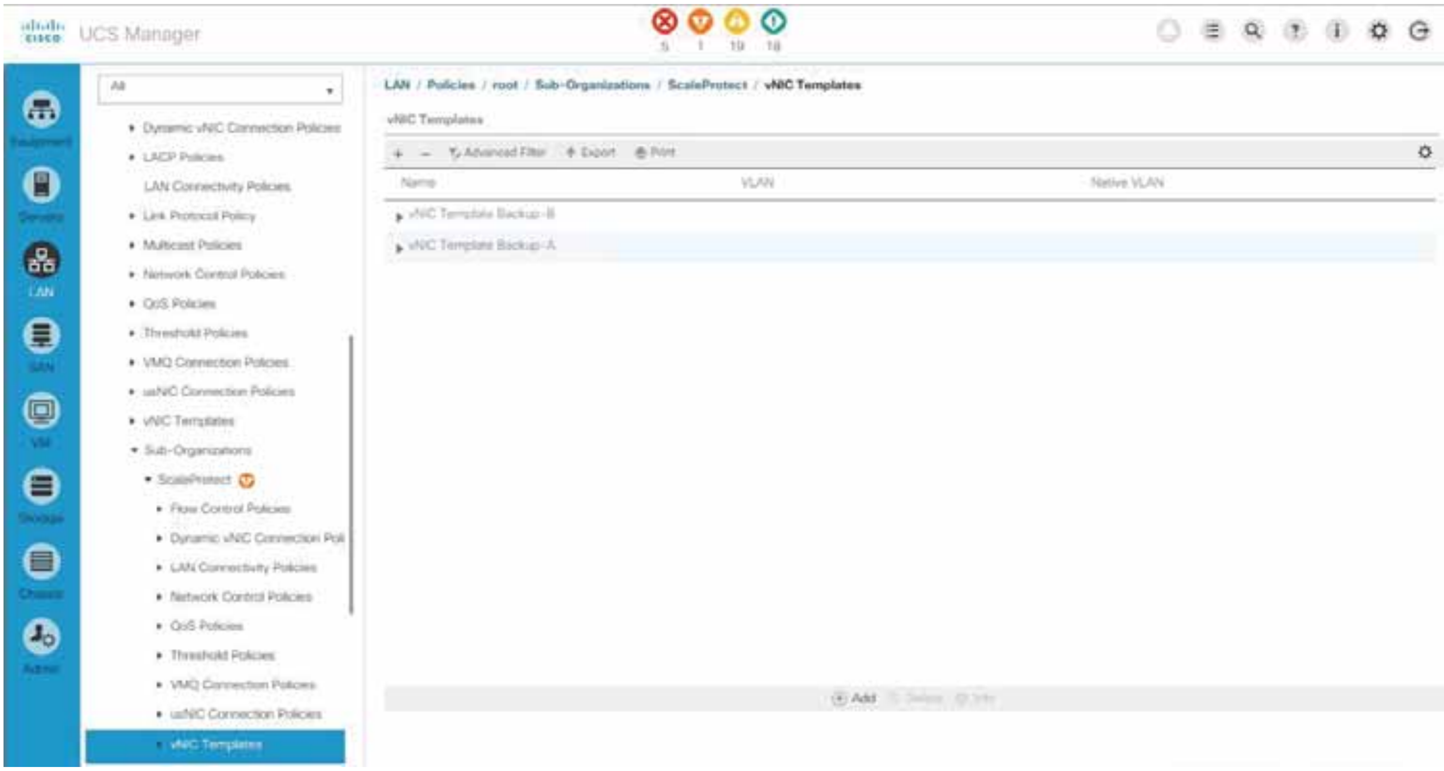
Stats Threshold Policy : <not set>

Connection Policies

● Dynamic vNIC ○ usNIC ○ VMQ

Dynamic vNIC Connection Policy : <not set>

Click Add.



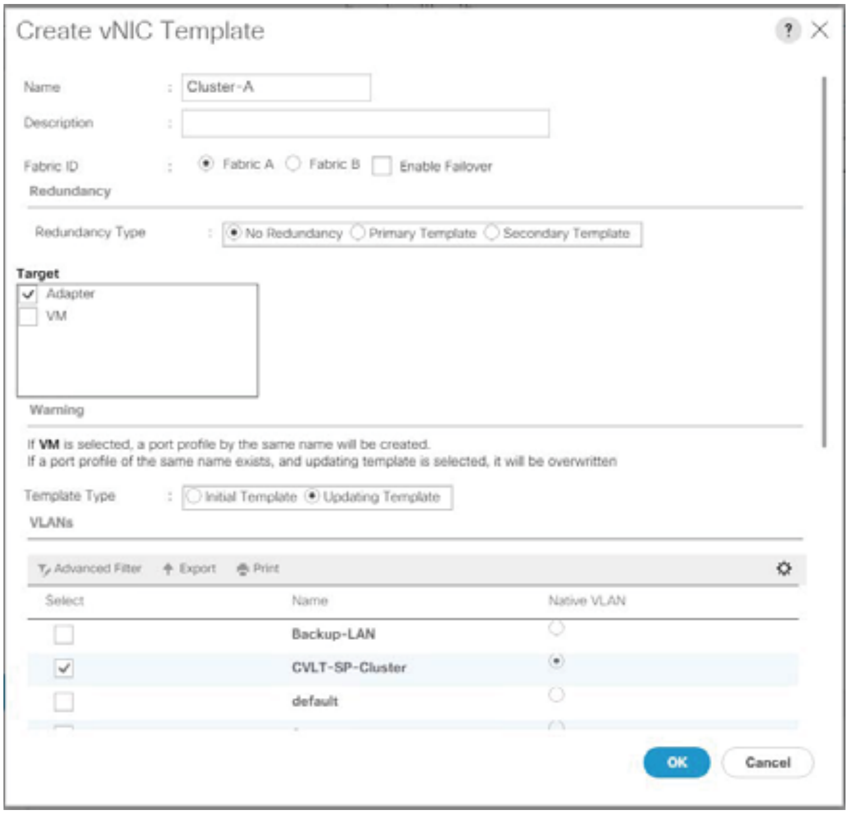
Name	VLAN	Native VLAN
vNIC Template Backup-B		
vNIC Template Backup-A		

Enter an obvious name for the ScaleProtect internal cluster network.

Select the radio button for Fabric A.

Select the radio button for Updating Template.

Select the checkbox for CVLT-SP-Cluster and select the Native VLAN radio button.



Create vNIC Template

Name : Cluster-A

Description :

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

Redundancy

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

Target

☑ Adapter

□ VM

Warning

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

Template Type : ○ Initial Template ● Updating Template

VLANs

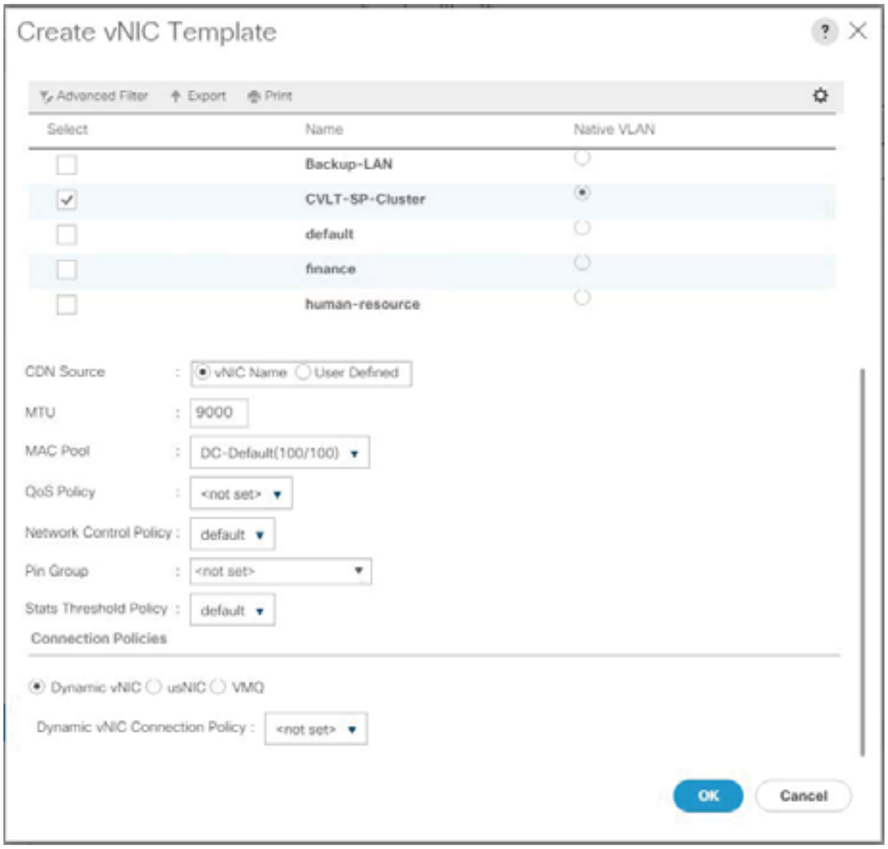
Select	Name	Native VLAN
□	Backup-LAN	○
☑	CVLT-SP-Cluster	●
□	default	○

Enter **9000** for the MTU value. MTU 9000 works only if all network components and the server are configured with MTU 9000. Check with your network administrator and server administrator to determine the use.

Select a MAC pool with free addresses.

Set QoS policy and network control policy as defined by your local network administrator.

Click OK.



Create vNIC Template

Select	Name	Native VLAN
□	Backup-LAN	○
☑	CVLT-SP-Cluster	●
□	default	○
□	finance	○
□	human-resource	○

CDN Source : ● vNIC Name ○ User Defined

MTU : 9000

MAC Pool : DC-Default(100/100)

QoS Policy : <not set>

Network Control Policy : default

Pin Group : <not set>

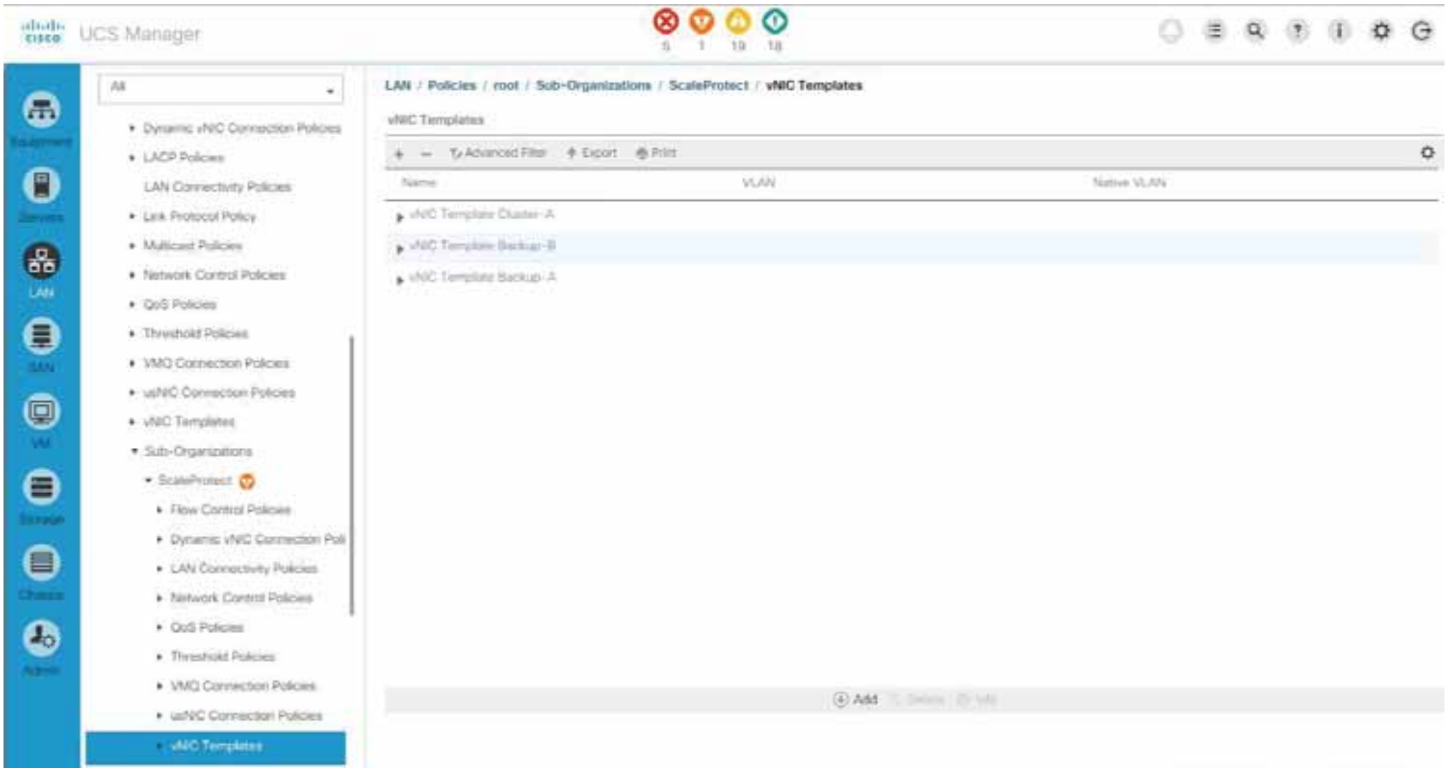
Stats Threshold Policy : default

Connection Policies

● Dynamic vNIC ○ usNIC ○ VMQ

Dynamic vNIC Connection Policy : <not set>

Click Add.



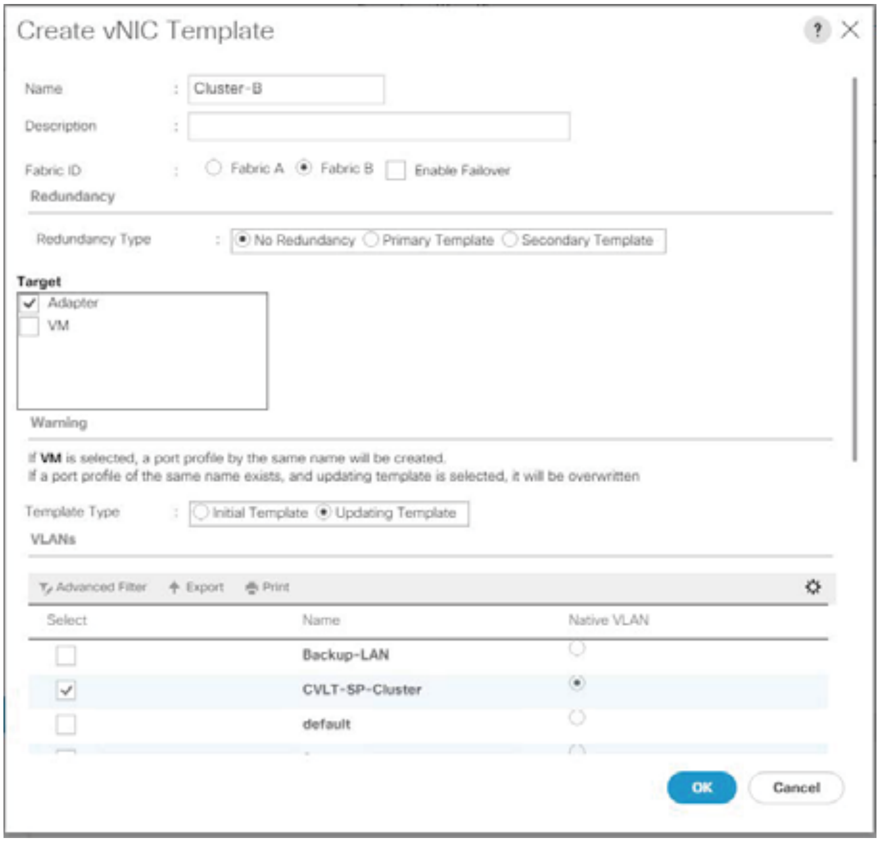
Name	VLAN	Native VLAN
vNIC Template Cluster-A		
vNIC Template Backup-B		
vNIC Template Backup-A		

Enter an obvious name for the ScaleProtect internal cluster network.

Select the radio button for Fabric B.

Select the radio button for Updating Template.

Select the checkbox for CVLT-SP-Cluster and select the Native VLAN radio button.



Create vNIC Template

Name : Cluster-B

Description :

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

Redundancy

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

Target

☑ Adapter
□ VM

Warning

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

Template Type : ○ Initial Template ● Updating Template

VLANs

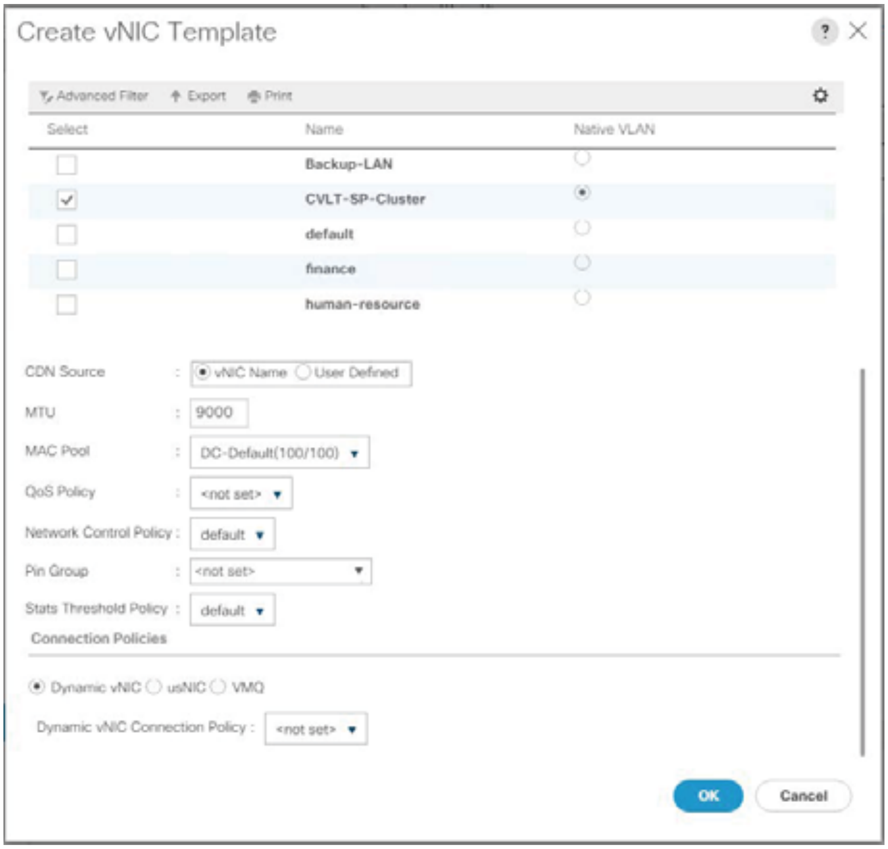
Select	Name	Native VLAN
□	Backup-LAN	○
☑	CVLT-SP-Cluster	●
□	default	○

Enter **9000** for the MTU value. MTU 9000 works only if all network components and the server are configured with MTU 9000. Check with your network administrator and server administrator to determine the use.

Select a MAC pool with free addresses.

Set QoS policy and network control policy as defined by your local network administrator.

Click OK.



Create vNIC Template

Select	Name	Native VLAN
□	Backup-LAN	○
☑	CVLT-SP-Cluster	●
□	default	○
□	finance	○
□	human-resource	○

CDN Source : ● vNIC Name ○ User Defined

MTU : 9000

MAC Pool : DC-Default(100/100)

QoS Policy : <not set>

Network Control Policy : default

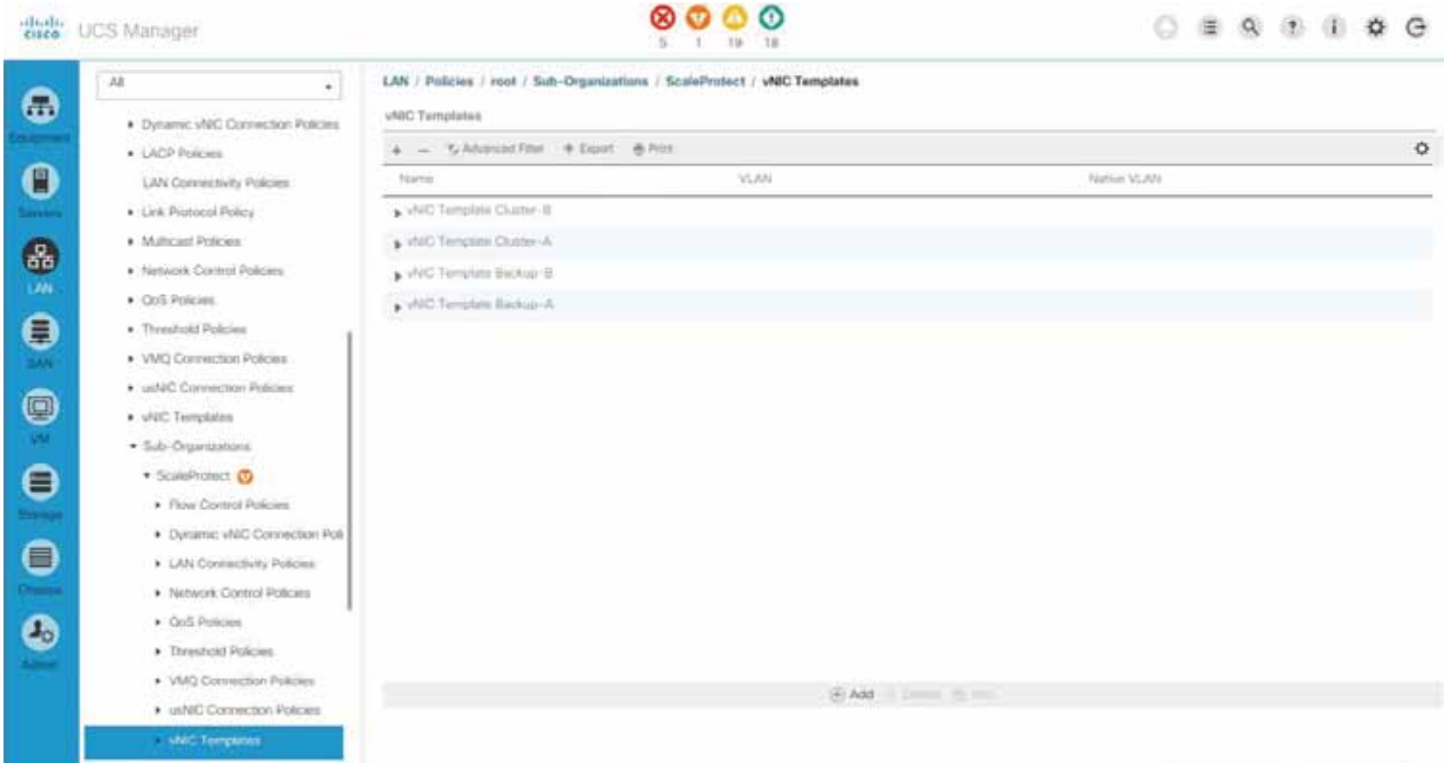
Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

● Dynamic vNIC ○ usNIC ○ VMQ

Dynamic vNIC Connection Policy : <not set>

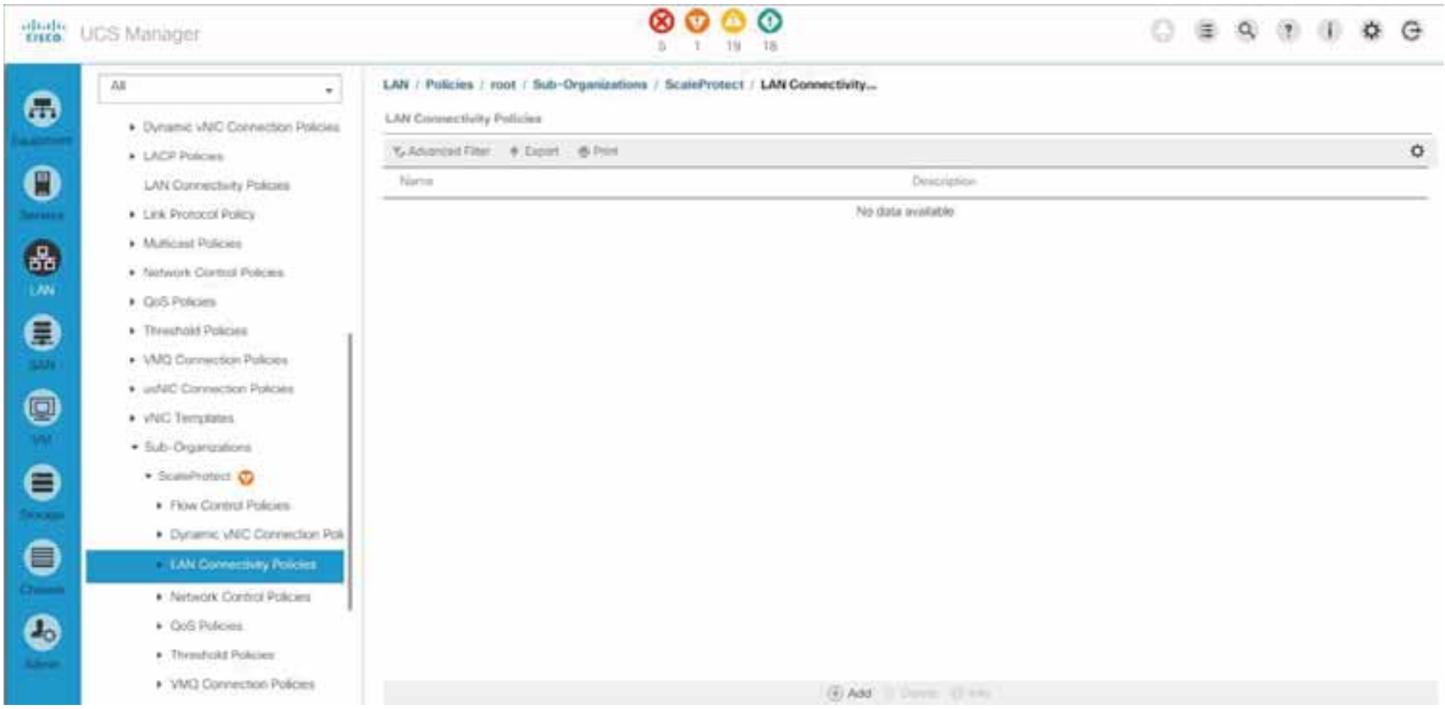


LAN / Policies / root / Sub-Organizations / ScaleProtect / vNIC Templates

vNIC Templates

Name	VLAN	Native VLAN
vNIC Template Cluster-B		
vNIC Template Cluster-A		
vNIC Template Backup-B		
vNIC Template Backup-A		

Go to LAN > Policies > root > Sub-Organizations > ScaleProtect > LAN Connectivity Policies and click Add.



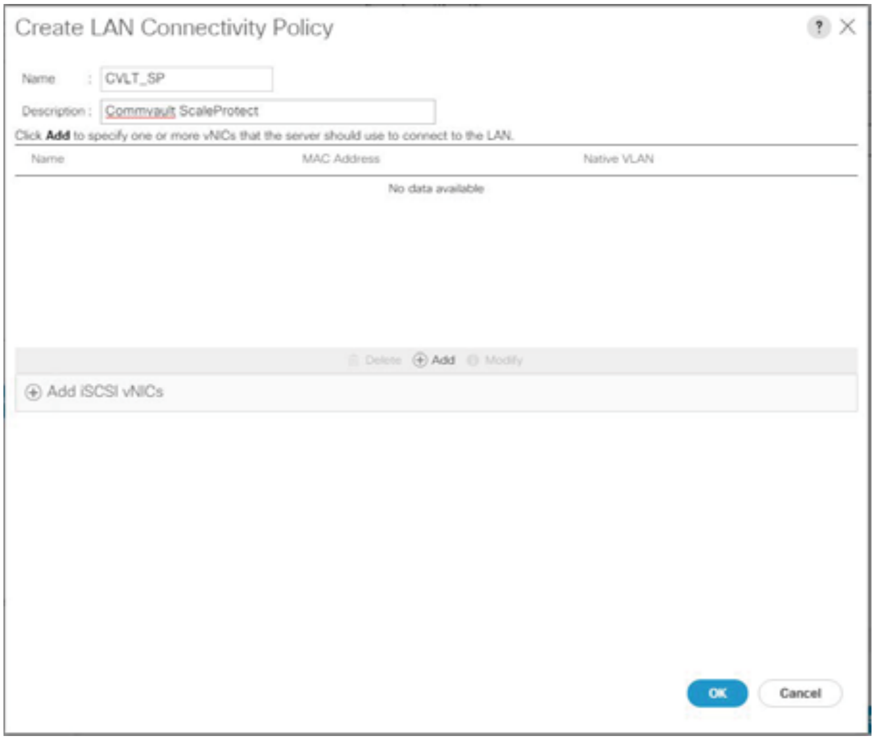
LAN / Policies / root / Sub-Organizations / ScaleProtect / LAN Connectivity...

LAN Connectivity Policies

Name	Description

No data available

Enter an obvious name and description and click Add.



Create LAN Connectivity Policy

Name : CVLT_SP

Description : Commvault ScaleProtect

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

Name	MAC Address	Native VLAN
No data available		

Enter **eth0** as the name of the vNIC.

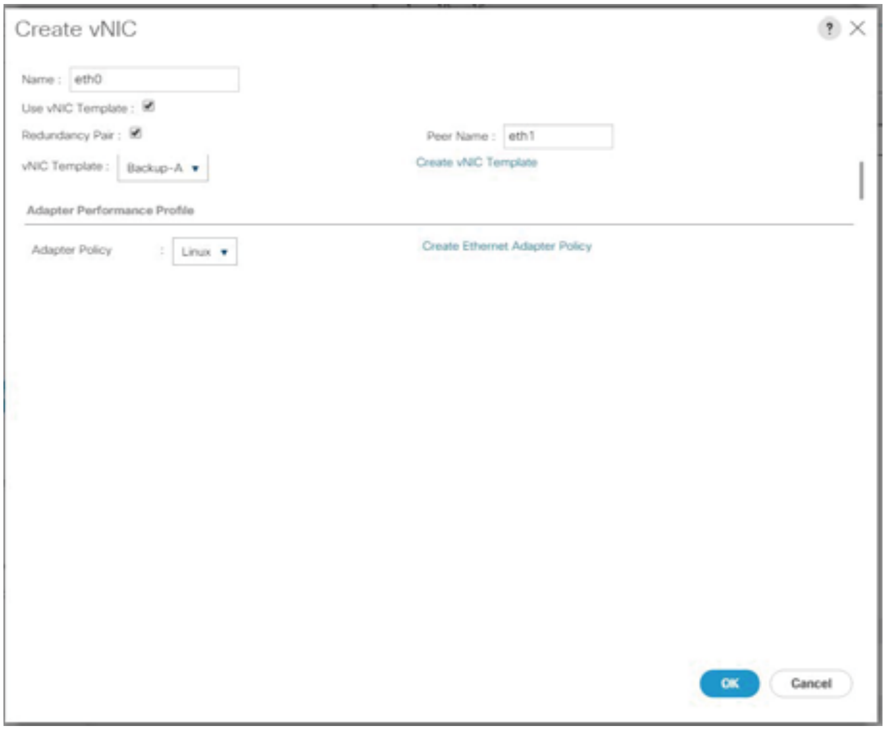
Select Use vNIC Template.

Select Redundancy Pair end enter **eth1** as the peer name.

Select Backup-A as the vNIC template.

Select Linux as the adapter policy.

Click OK.



Create vNIC

Name : eth0

Use vNIC Template : ☑

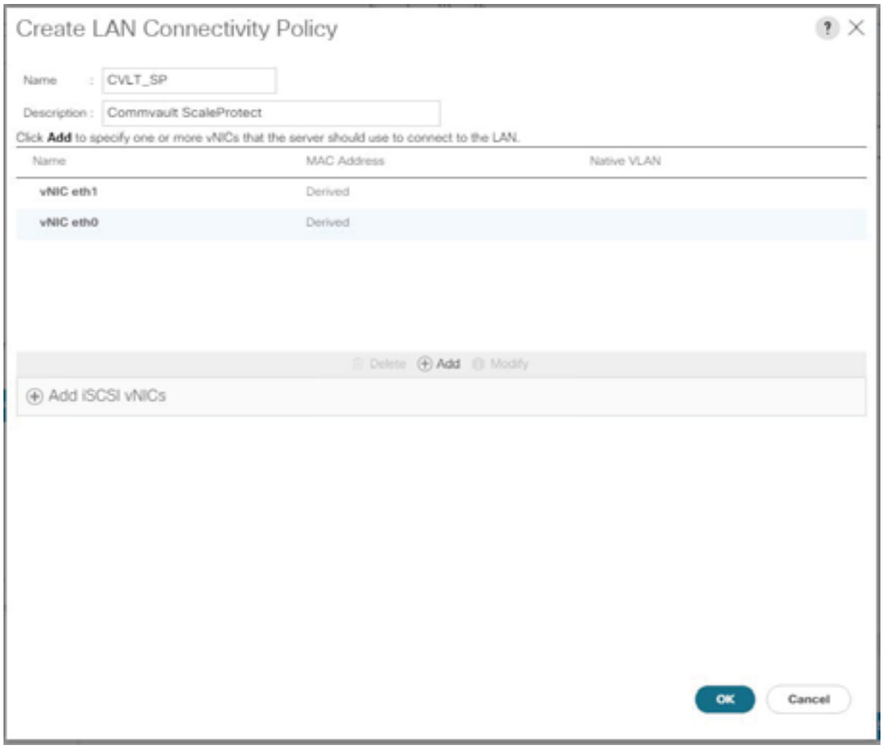
Redundancy Pair : ☑ Peer Name : eth1

vNIC Template : Backup-A ▾

Adapter Performance Profile

Adapter Policy : Linux ▾

Select vNIC eth1 and click Modify.



Create LAN Connectivity Policy

Name : CVLT_SP

Description : Commvault ScaleProtect

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

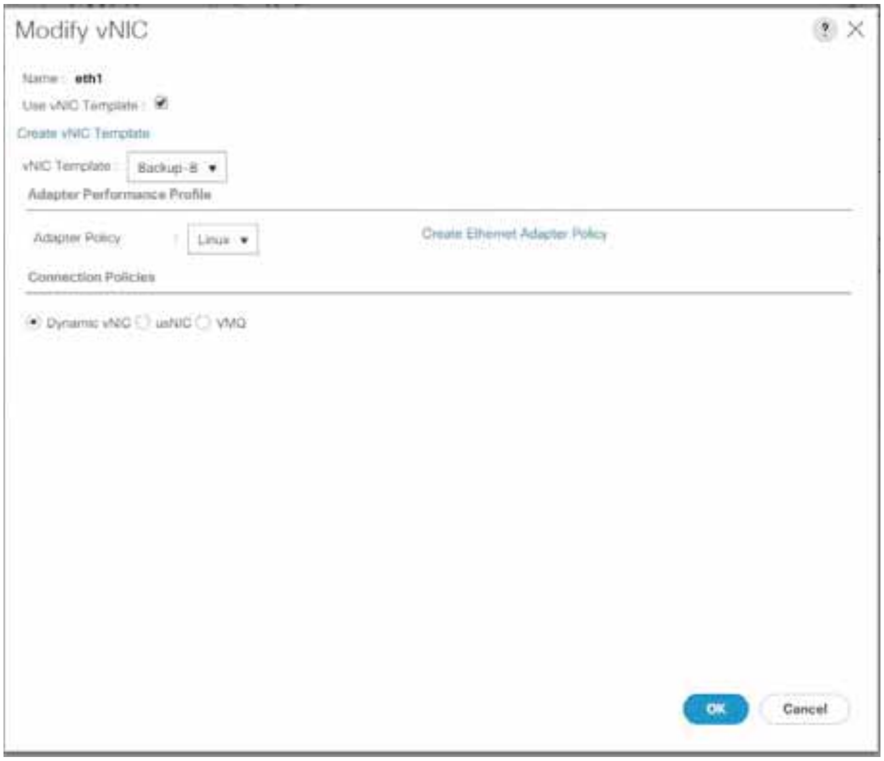
Name	MAC Address	Native VLAN
vNIC eth1	Derived	
vNIC eth0	Derived	

Select Use vNIC Template.

Select Backup-B as the template.

Select Linux as the adapter policy.

Click OK.



Modify vNIC

Name : eth1

Use vNIC Template : ☑

vNIC Template : Backup-B

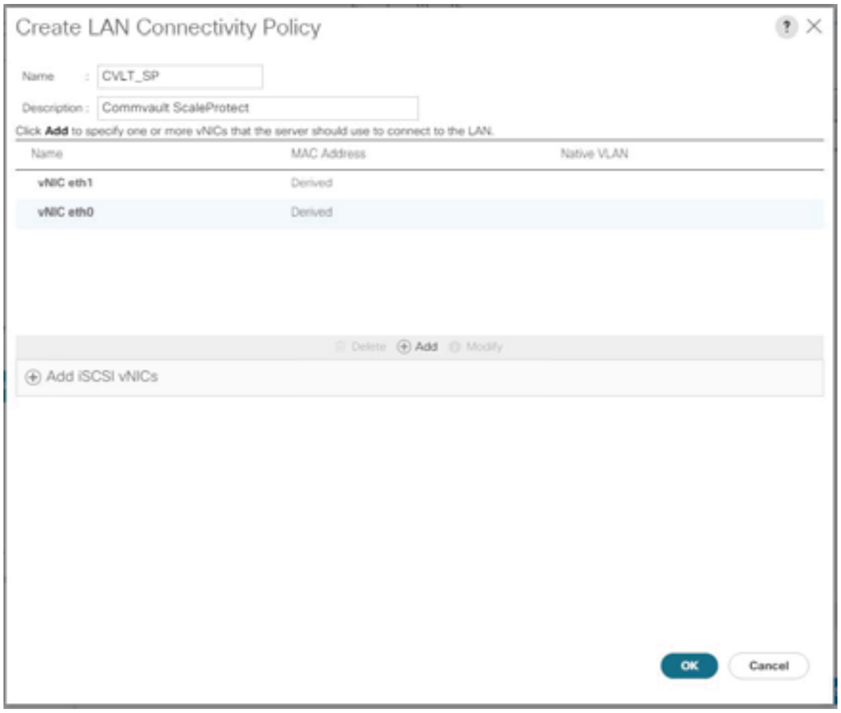
Adapter Performance Profile

Adapter Policy : Linux

Connection Policies

● Dynamic vNIC ○ usNIC ○ VMQ

Click Add.



Create LAN Connectivity Policy

Name : CVLT_SP

Description : Commvault ScaleProtect

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

Name	MAC Address	Native VLAN
vNIC eth1	Derived	
vNIC eth0	Derived	

Enter **eth2** as the name of the vNIC.

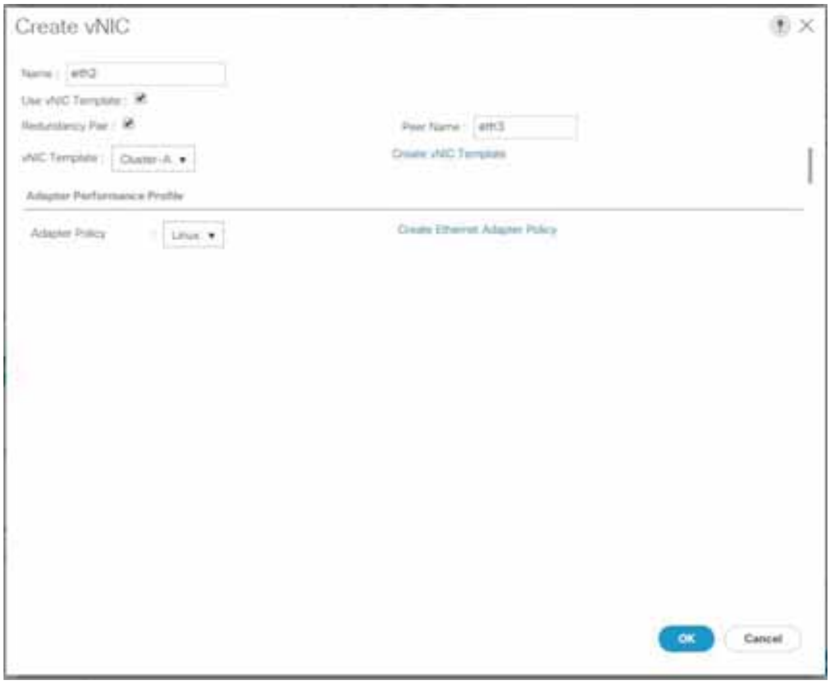
Select Use vNIC Template.

Select Redundancy Pair end enter **eth3** as the peer name.

Select Cluster-A as the vNIC template.

Select Linux as the adapter policy.

Click OK.



Create vNIC

Name : eth2

Use vNIC Template : ☑

Redundancy Pair : ☑

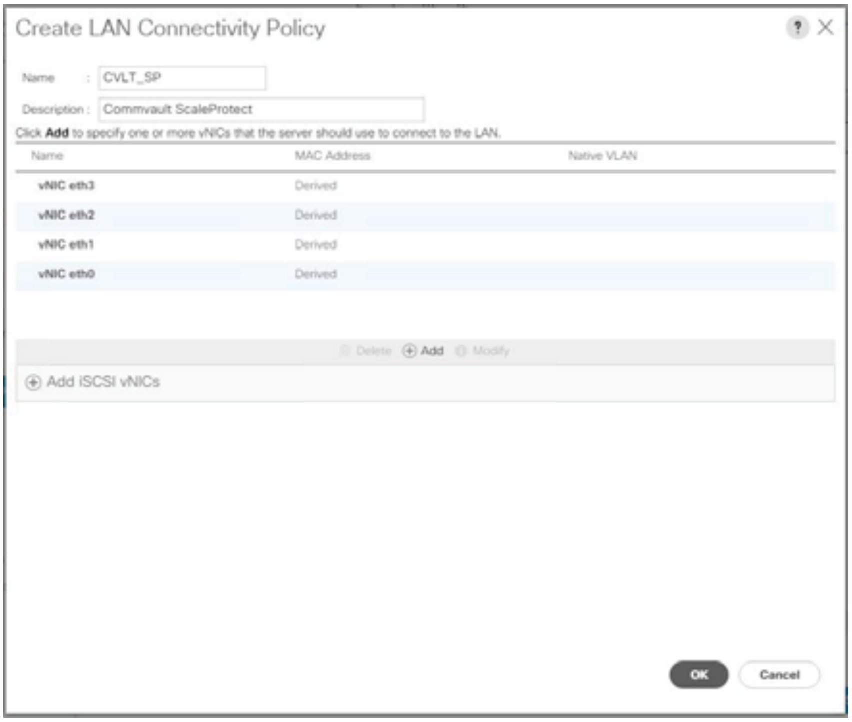
Peer Name : eth3

vNIC Template : Cluster-A

Adapter Performance Profile

Adapter Policy : Linux

Select vNIC eth3 and click Modify.



Create LAN Connectivity Policy

Name : CVLT_SP

Description : Commvault ScaleProtect

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

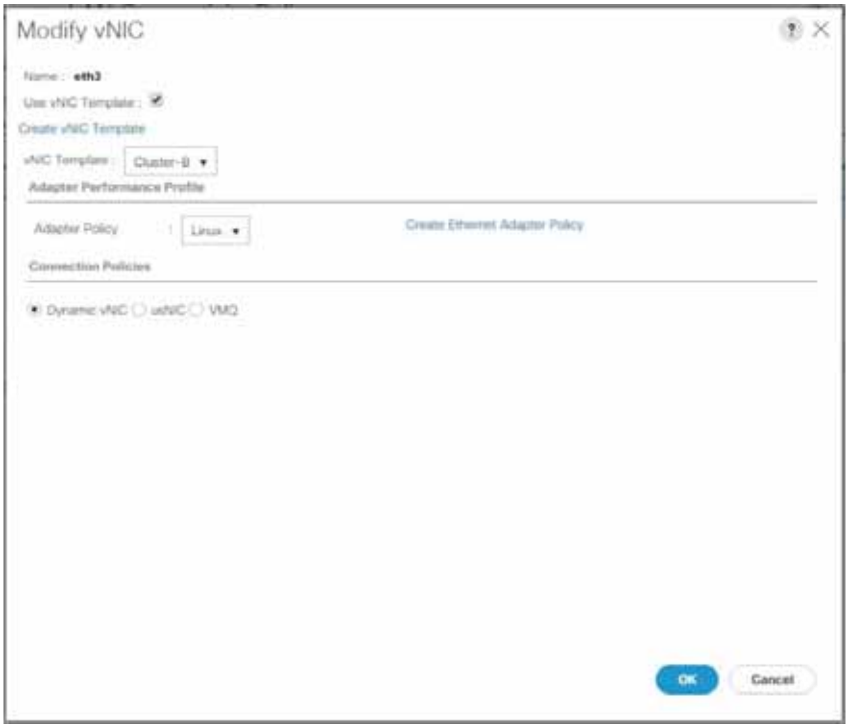
Name	MAC Address	Native VLAN
vNIC eth3	Derived	
vNIC eth2	Derived	
vNIC eth1	Derived	
vNIC eth0	Derived	

Select Use vNIC Template.

Select Cluster-B as the template.

Select Linux as the adapter policy.

Click OK.



Modify vNIC

Name : **eth3**

Use vNIC Template : ☑

Create vNIC Template

vNIC Template : Cluster-B ▾

Adapter Performance Profile

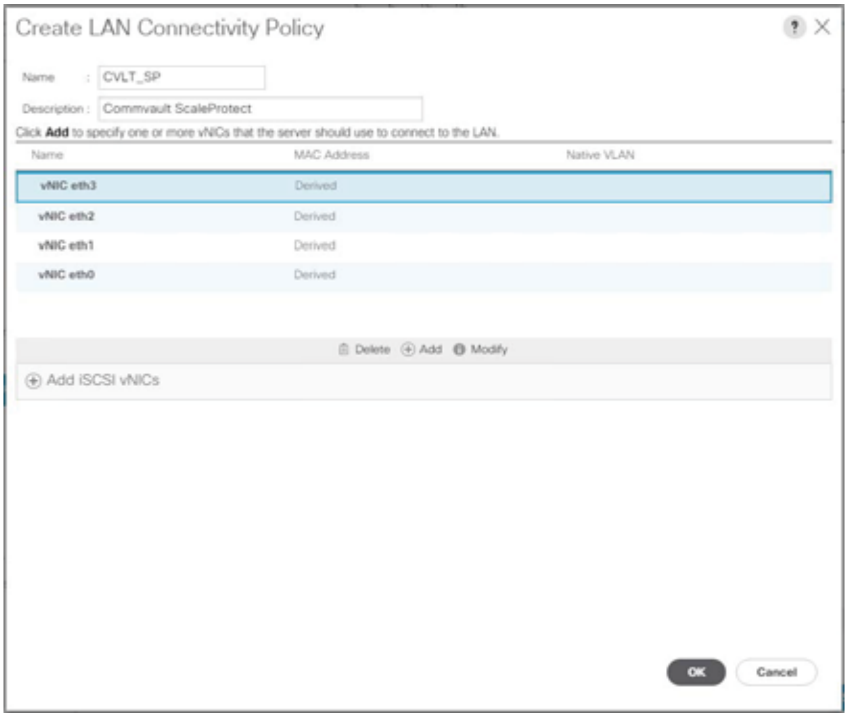
Adapter Policy : Linux ▾

Create Ethernet Adapter Policy

Connection Policies

● Dynamic vNIC ○ usNIC ○ VMQ

Click OK.



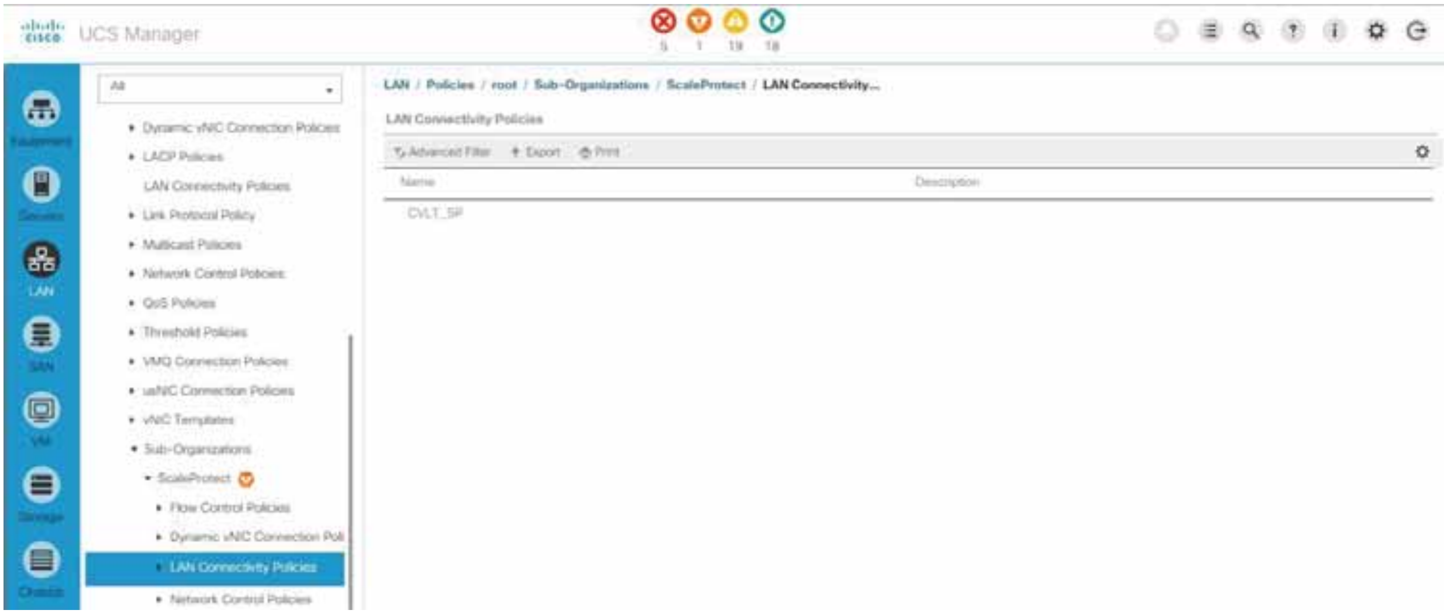
Create LAN Connectivity Policy

Name : CVLT_SP

Description : Commvault ScaleProtect

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

Name	MAC Address	Native VLAN
vNIC eth3	Derived	
vNIC eth2	Derived	
vNIC eth1	Derived	
vNIC eth0	Derived	

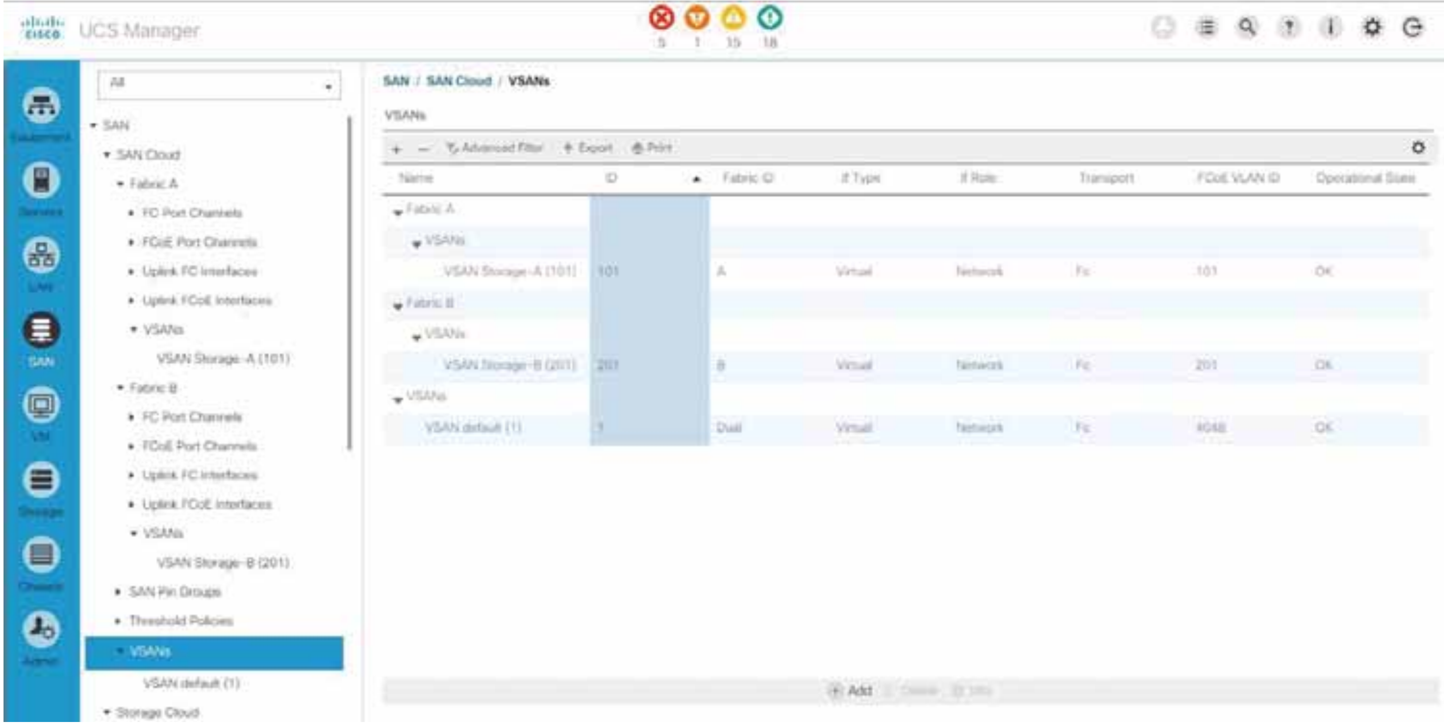


Name	Description
CVLT_SP	

SAN configuration

If IntelliSnap integration with existing SAN storages or backup to Fibre Channel connected tape drives is used or planned for use, configure the Cisco UCS SAN for access to the SAN environment through FCoE within the system.

Go to SAN > SAN Cloud > VSANs and check the configured VSANs.



Name	ID	Fabric ID	If Type	If Role	Transport	FCoE VLAN ID	Operational State
Fabric A							
VSANs							
VSAN Storage-A (101)	101	A	Virtual	Network	Fc	101	OK
Fabric B							
VSANs							
VSAN Storage-B (201)	201	B	Virtual	Network	Fc	201	OK
VSANs							
VSAN default (1)	1	Dual	Virtual	Network	Fc	4048	OK

If a dedicated SAN configuration for backup is required, add the required VSAN configuration to the system.

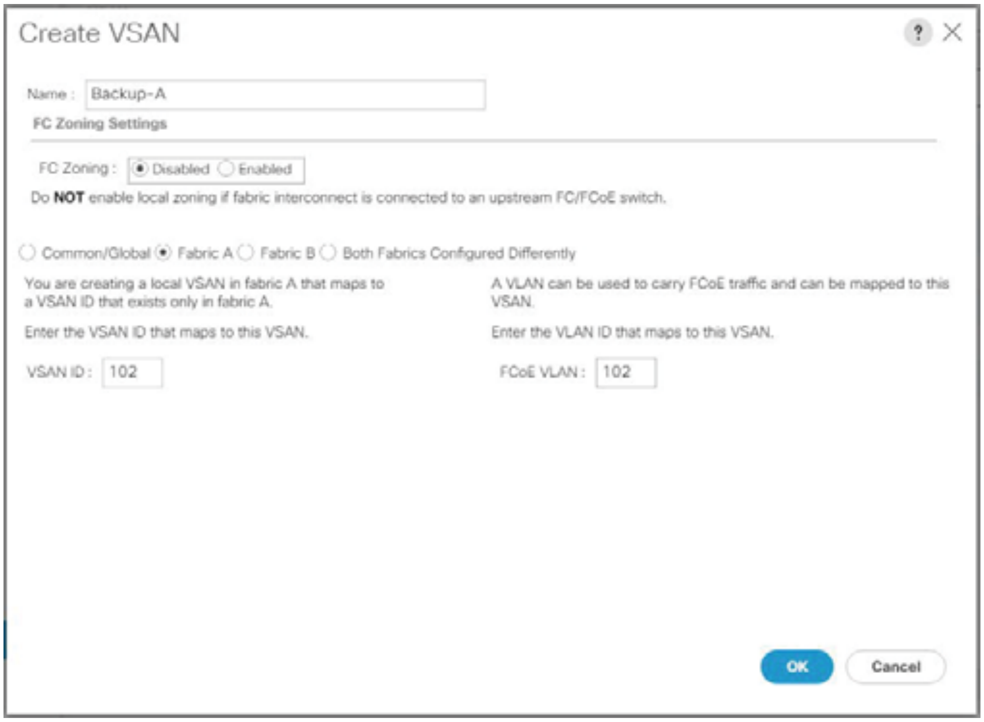
Click Add.

Enter an obvious name.

Select Fabric A.

Enter the required VSAN ID and related FCoE VLAN ID.

Click OK.



Create VSAN

Name : Backup-A

FC Zoning Settings

FC Zoning : ● Disabled ○ Enabled

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

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

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

Enter the VSAN ID that maps to this VSAN.

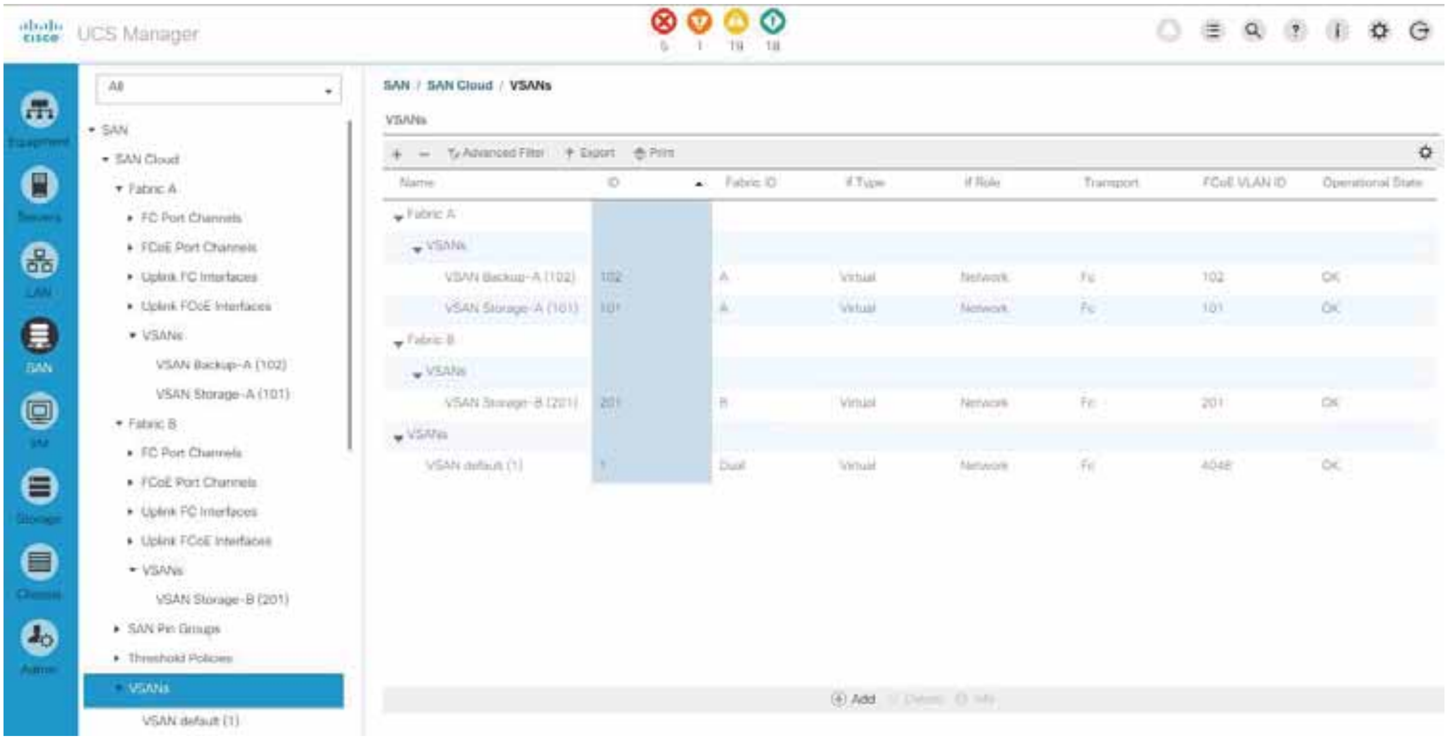
VSAN ID : 102

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

Enter the VLAN ID that maps to this VSAN.

FCoE VLAN : 102

Click Add.



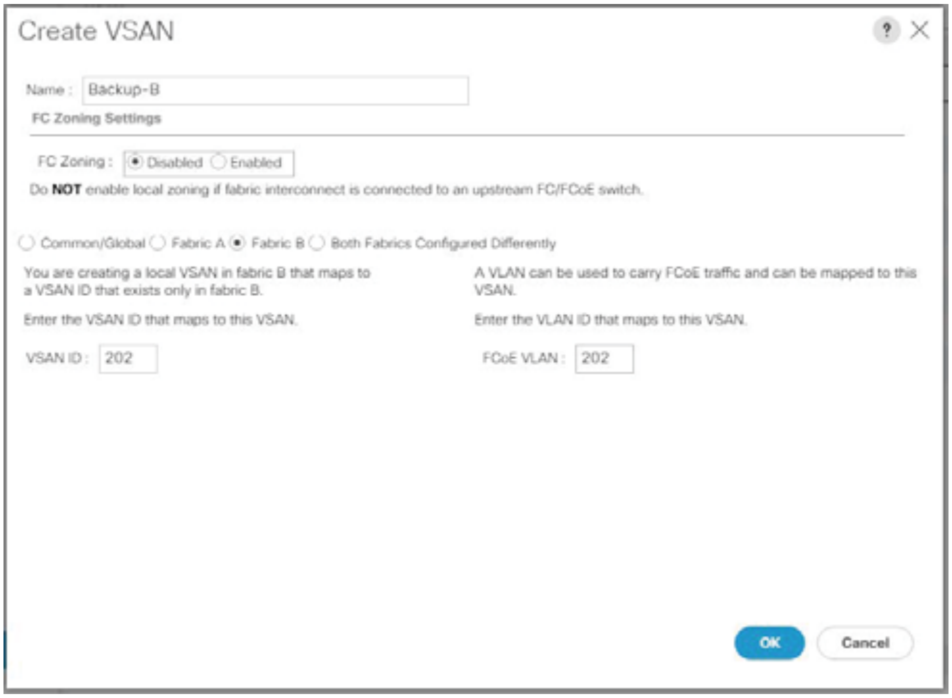
Name	ID	Fabric ID	If Type	If Role	Transport	FCoE VLAN ID	Operational State
Fabric A							
VSANs							
VSAN Backup-A (102)	102	A	Virtual	Network	Fc	102	OK
VSAN Storage-A (101)	101	A	Virtual	Network	Fc	101	OK
Fabric B							
VSANs							
VSAN Storage-B (201)	201	B	Virtual	Network	Fc	201	OK
VSANs							
VSAN default (1)	1	Dual	Virtual	Network	Fc	4048	OK

Enter an obvious name.

Select Fabric B.

Enter the required VSAN ID and related FCoE VLAN ID.

Click OK.



Create VSAN

Name : Backup-B

FC Zoning Settings

FC Zoning : ● Disabled ○ Enabled

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

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

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

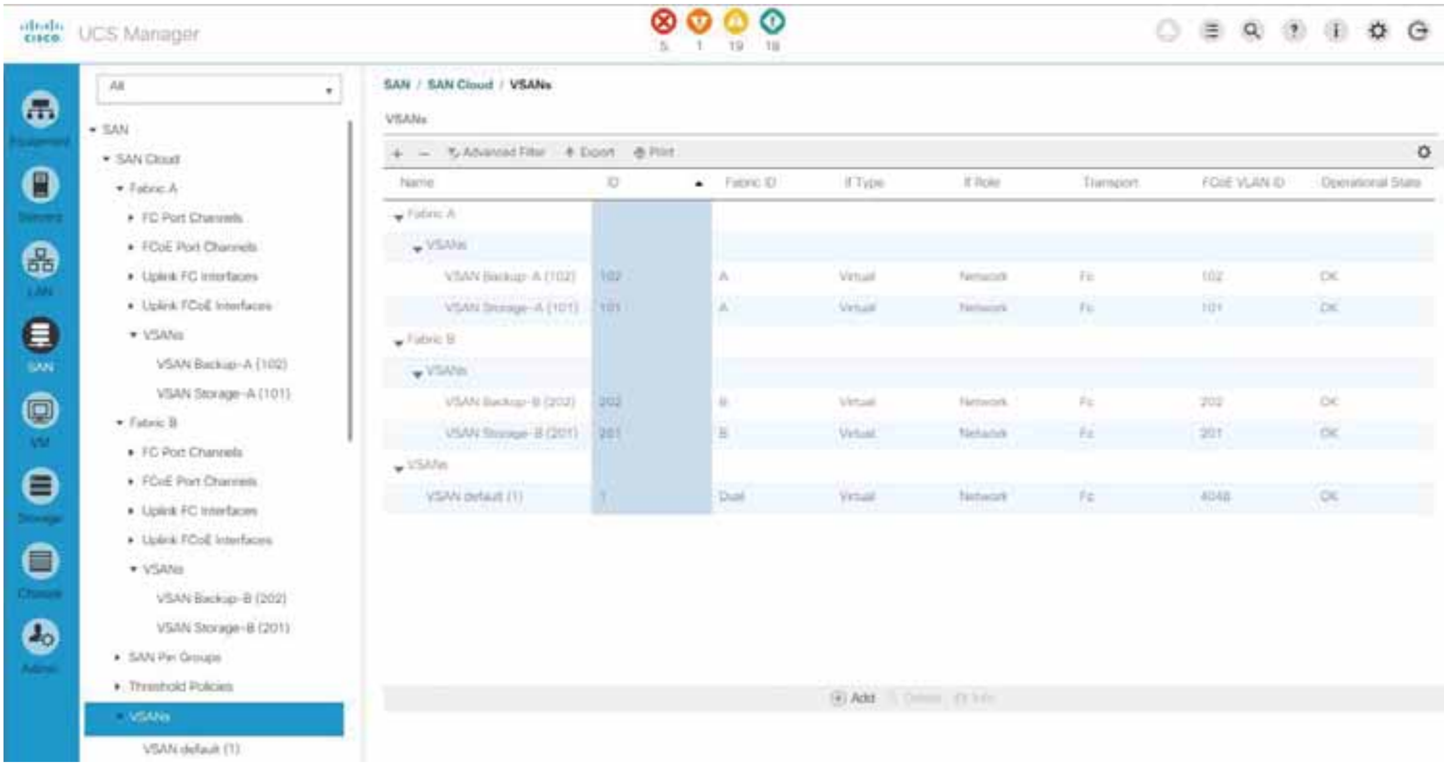
Enter the VSAN ID that maps to this VSAN.

VSAN ID : 202

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

Enter the VLAN ID that maps to this VSAN.

FCoE VLAN : 202



SAN / SAN Cloud / VSANs

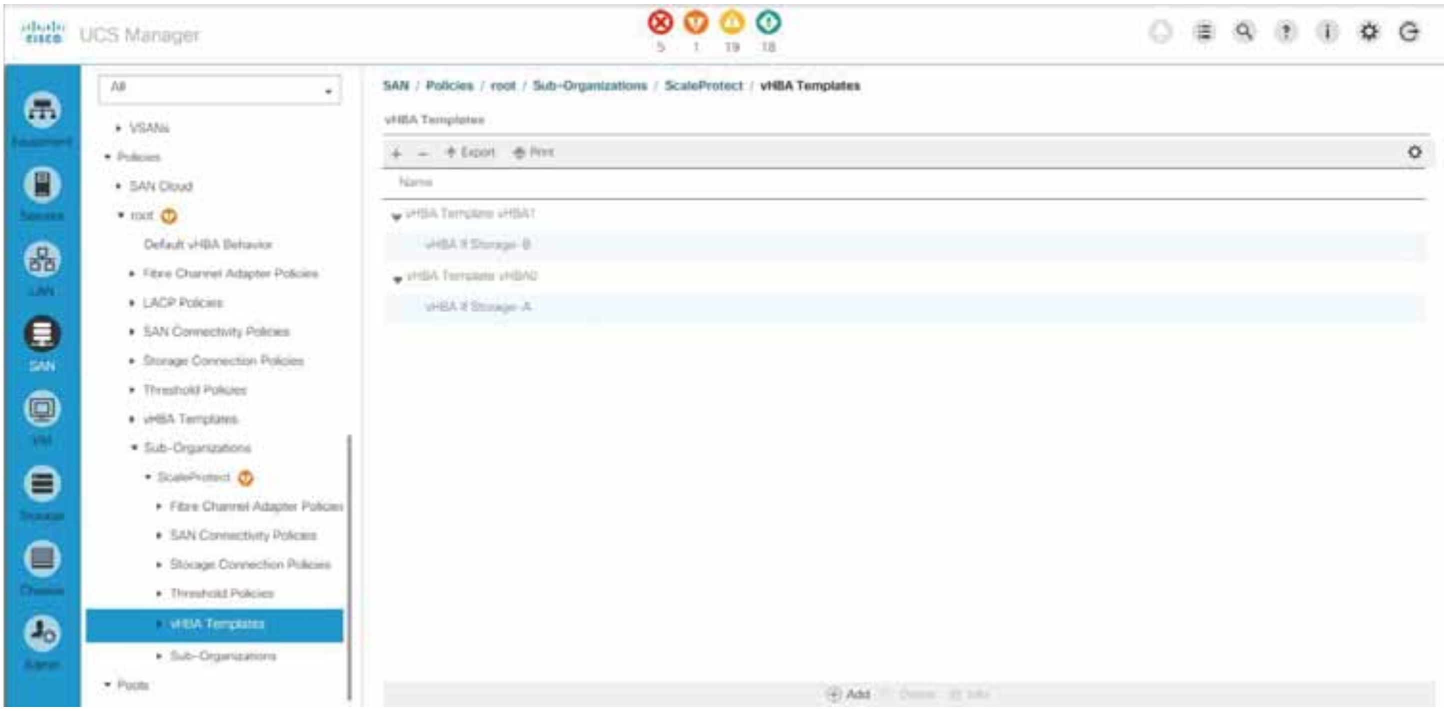
VSANs

Name	ID	Fabric ID	If Type	If Role	Transport	FCoE VLAN ID	Operational State
Fabric A							
VSANs							
VSAN Backup-A (102)	102	A	Virtual	Network	Fc	102	OK
VSAN Storage-A (101)	101	A	Virtual	Network	Fc	101	OK
Fabric B							
VSANs							
VSAN Backup-B (202)	202	B	Virtual	Network	Fc	202	OK
VSAN Storage-B (201)	201	B	Virtual	Network	Fc	201	OK
VSANs							
VSAN default (1)	1	Dual	Virtual	Network	Fc	4048	OK

Go to SAN > Policies > root > Sub-Organization > ScaleProtect > vHBA Templates.

The vHBA templates for Storage-A and Storage-B are already available in this system. If they don’t exist, you need to create them.

Click Add.



Enter an obvious name.

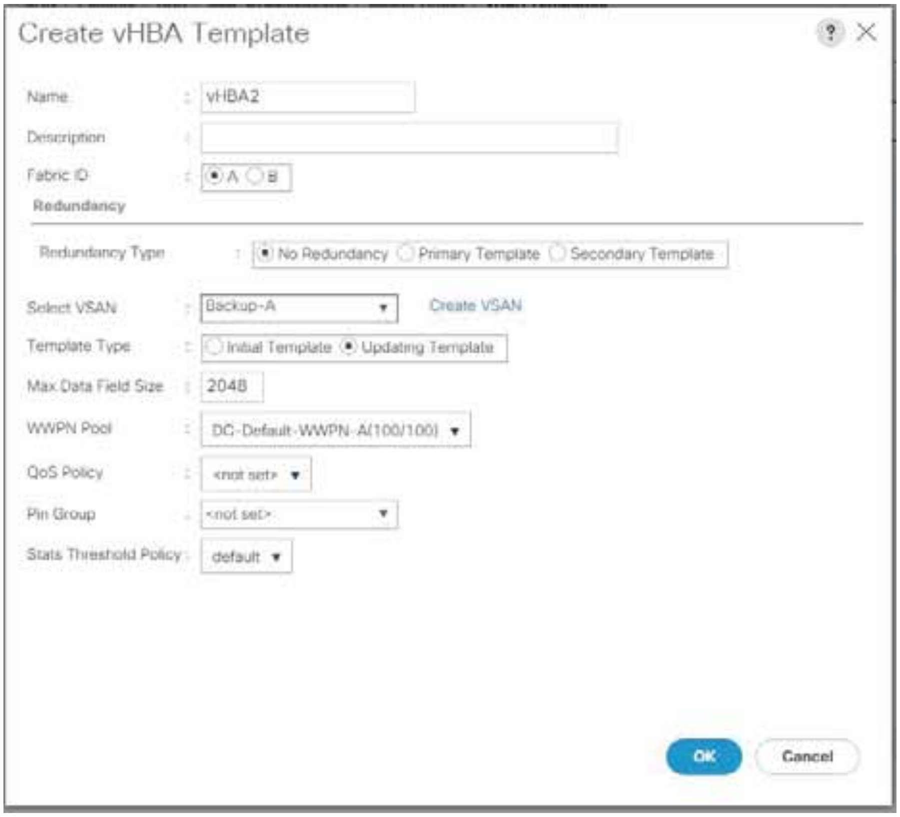
Select Fabric A.

Select Updating Template as the template type.

Select the backup VSAN on Fabric A as the VSAN.

Select a WWPN pool with available addresses.

Click OK.



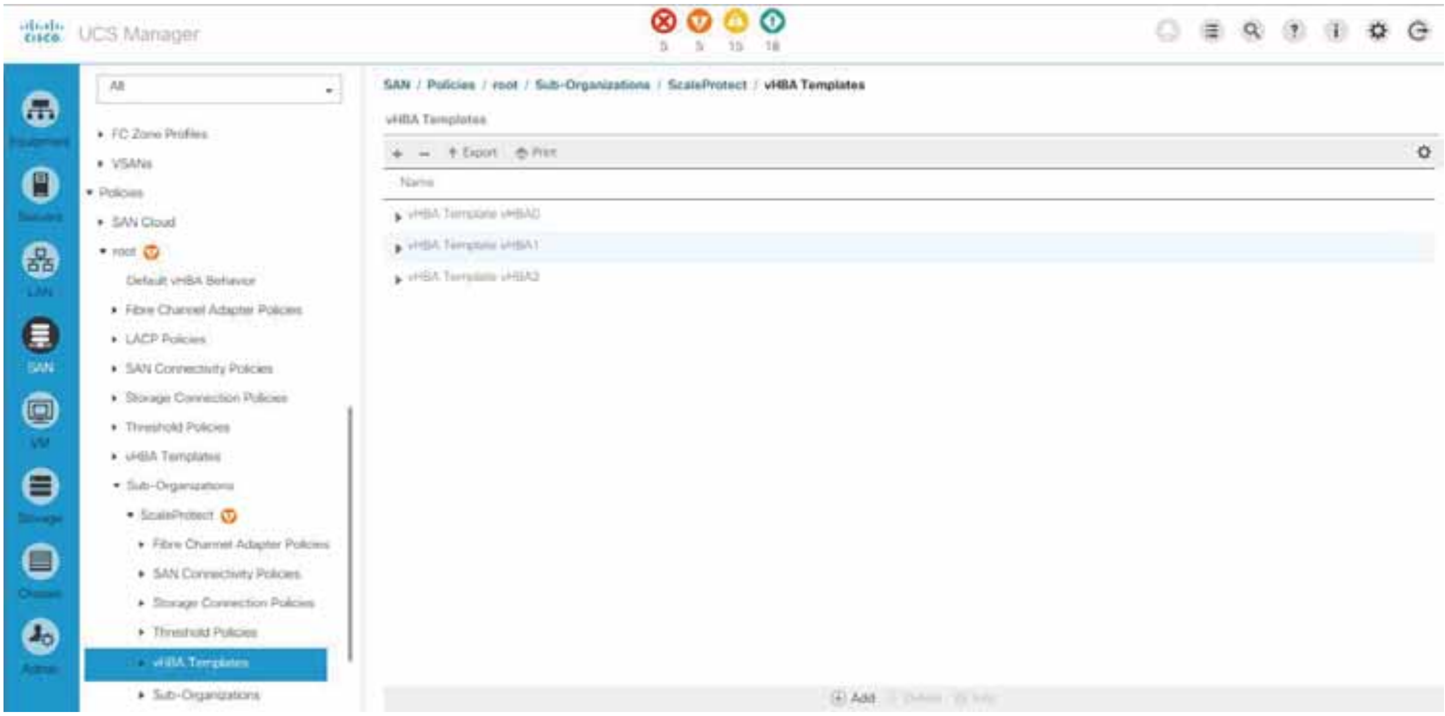
Create vHBA Template

Name	vHBA2
Description	
Fabric ID	● A ○ B

Redundancy

Redundancy Type	● No Redundancy ○ Primary Template ○ Secondary Template
Select VSAN	Backup-A
Template Type	○ Initial Template ● Updating Template
Max Data Field Size	2048
WWPN Pool	DC-Default-WWPN-A(100/100)
QoS Policy	<not set>
Pin Group	<not set>
Stats Threshold Policy	default

Click Add.



SAN / Policies / root / Sub-Organizations / ScaleProtect / vHBA Templates

vHBA Templates

Name
vHBA Template vHBA0
vHBA Template vHBA1
vHBA Template vHBA2

Enter an obvious name.

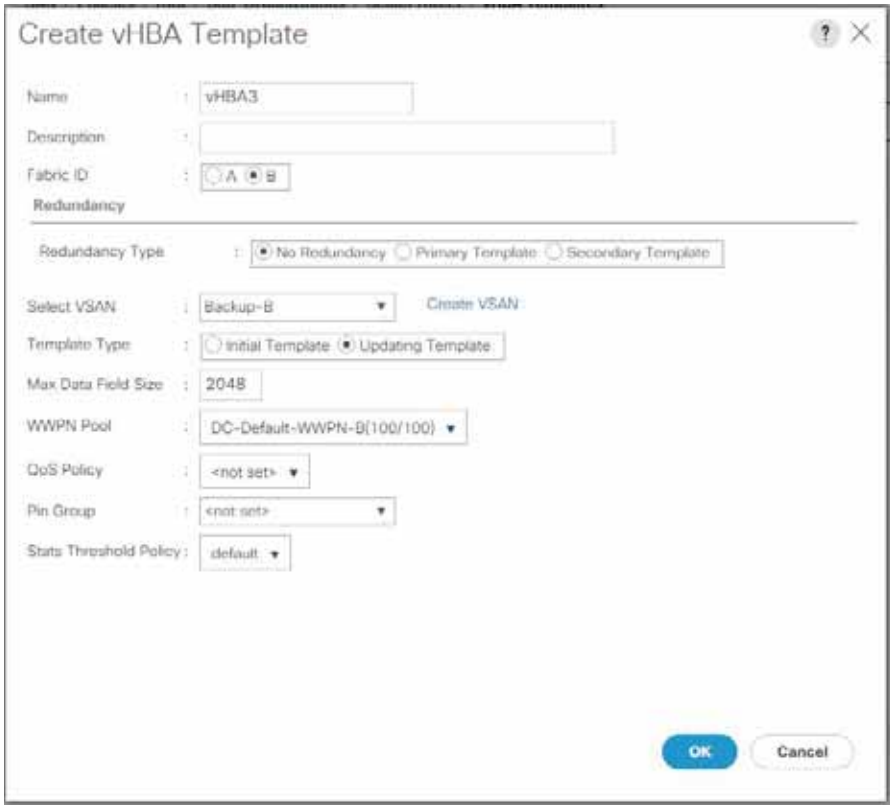
Select Fabric A.

Select Updating Template as the template type.

Select the backup VSAN on Fabric A as the VSAN.

Select a WWPN pool with available addresses.

Click OK.



Create vHBA Template

Name : vHBA3

Description :

Fabric ID : ○ A ● B

Redundancy

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

Select VSAN : Backup-B ▾ Create VSAN

Template Type : ○ Initial Template ● Updating Template

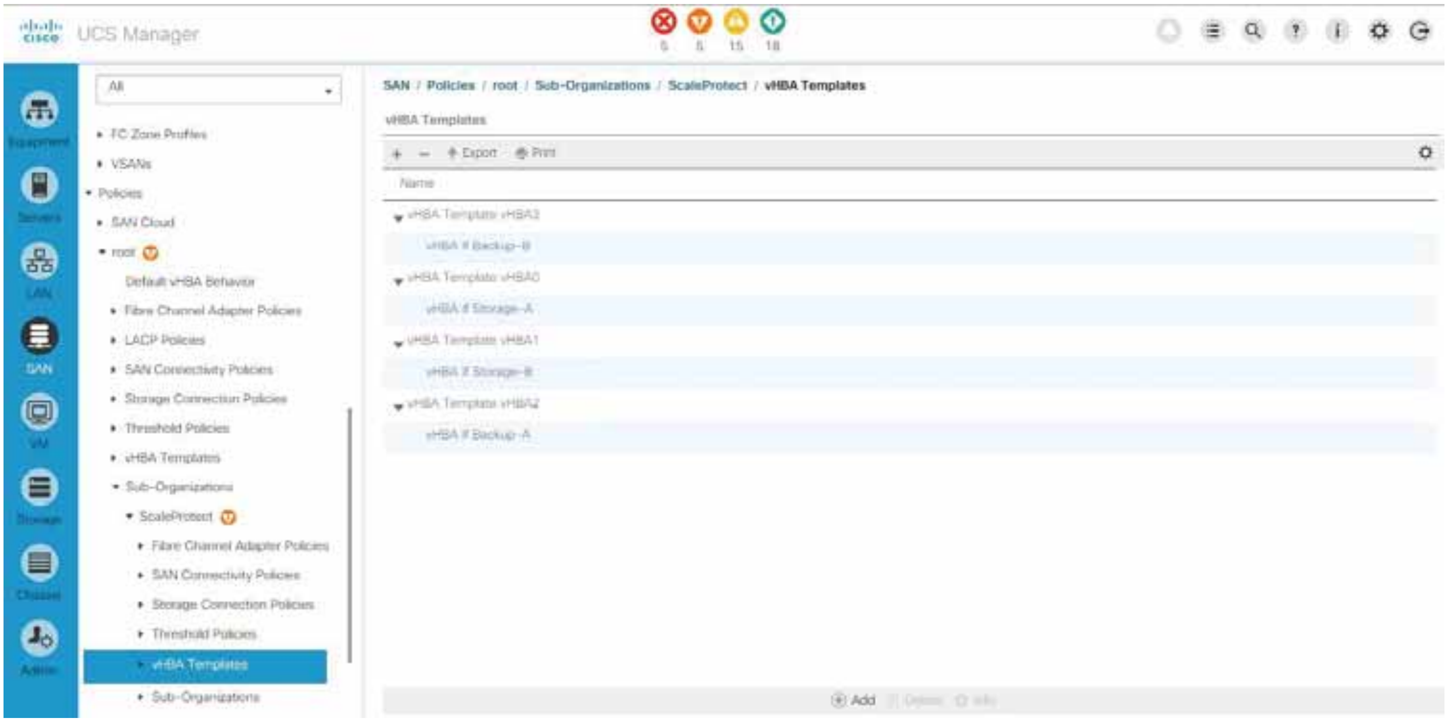
Max Data Field Size : 2048

WWPN Pool : DC-Default-WWPN-B(100/100) ▾

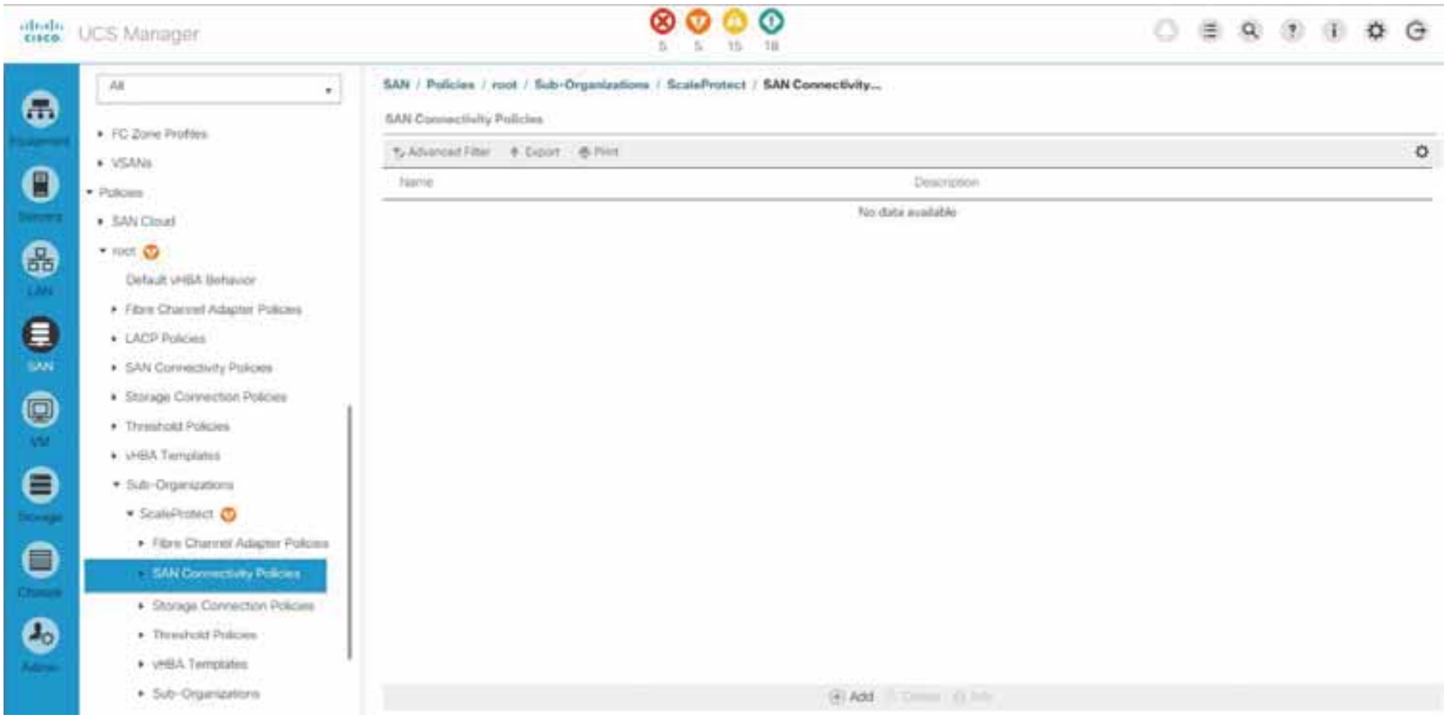
QoS Policy : <not set> ▾

Pin Group : <not set> ▾

Stats Threshold Policy : default ▾



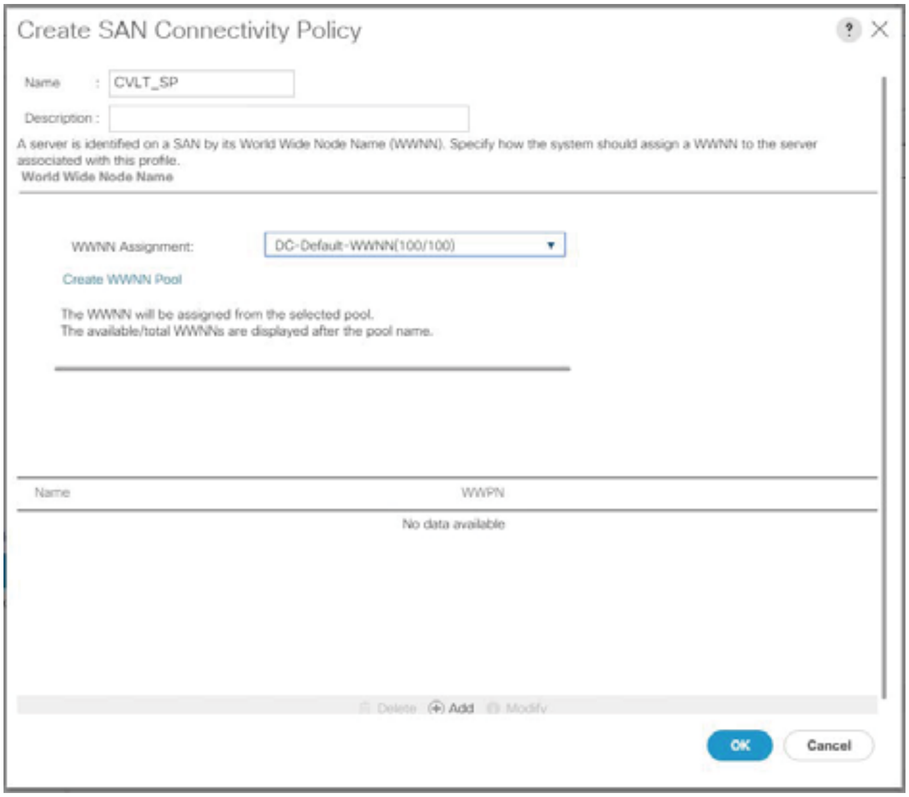
Go to SAN > Policies > root > Sub-Organization > ScaleProtect > SAN Connectivity Policies and click Add.



Enter an obvious name.

Select a WWNN pool with free addresses.

Click Add.



Create SAN Connectivity Policy

Name : CVLT_SP

Description :

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: DC-Default-WWNN(100/100)

Create WWNN Pool

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

Name	WWPN
No data available	

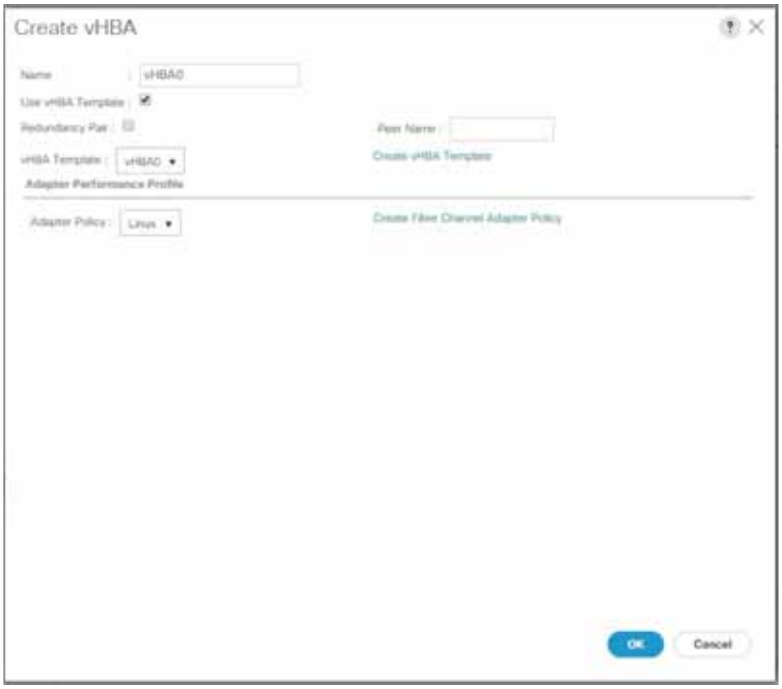
Enter an obvious name.

Select Use vHBA Template.

Select one of the vHBA templates.

Select Linux as the adapter policy.

Click OK.



Create vHBA

Name : vHBA0

Use vHBA Template : ☑

Redundancy Pair : □

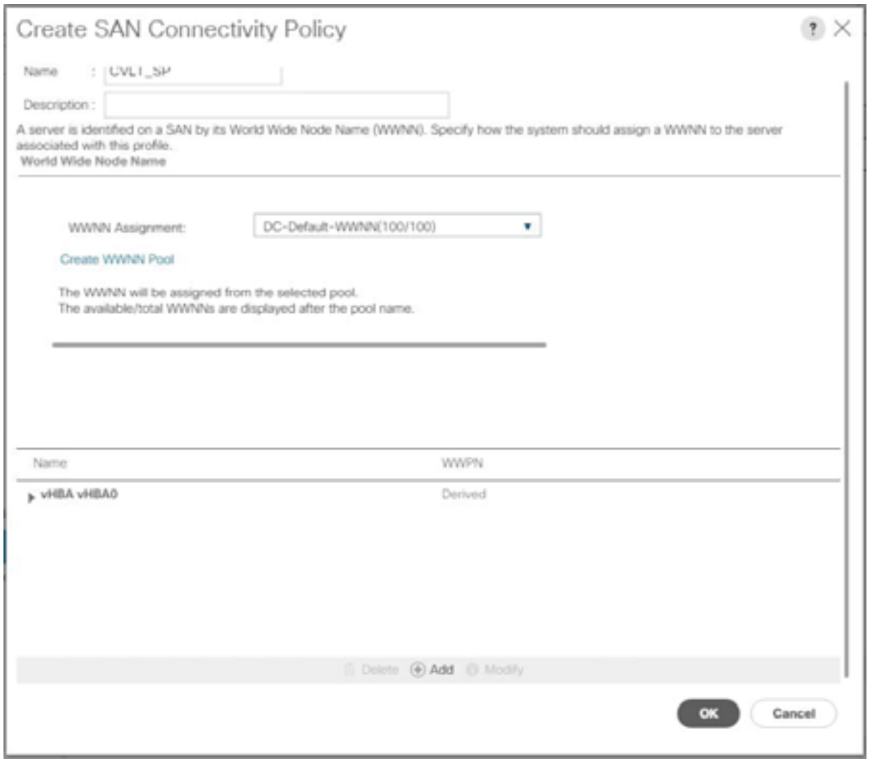
Peer Name :

vHBA Template : vHBA0

Adapter Performance Profile

Adapter Policy : Linux

Click Add.



Create SAN Connectivity Policy

Name : CVLT_SP

Description :

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: DC-Default-WWNN(100/100)

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

Name	WWPN
vHBA vHBA0	Derived

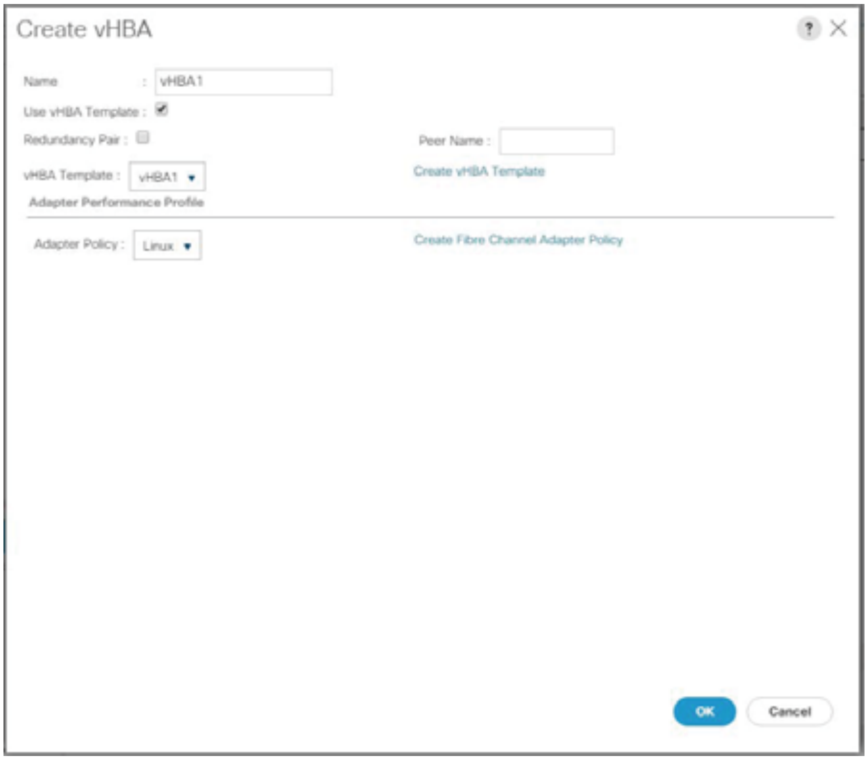
Enter an obvious name.

Select Use vHBA Template.

Select one of the vHBA templates.

Select Linux as the adapter policy.

Click OK.



Create vHBA

Name : vHBA1

Use vHBA Template : ☑

Redundancy Pair : □

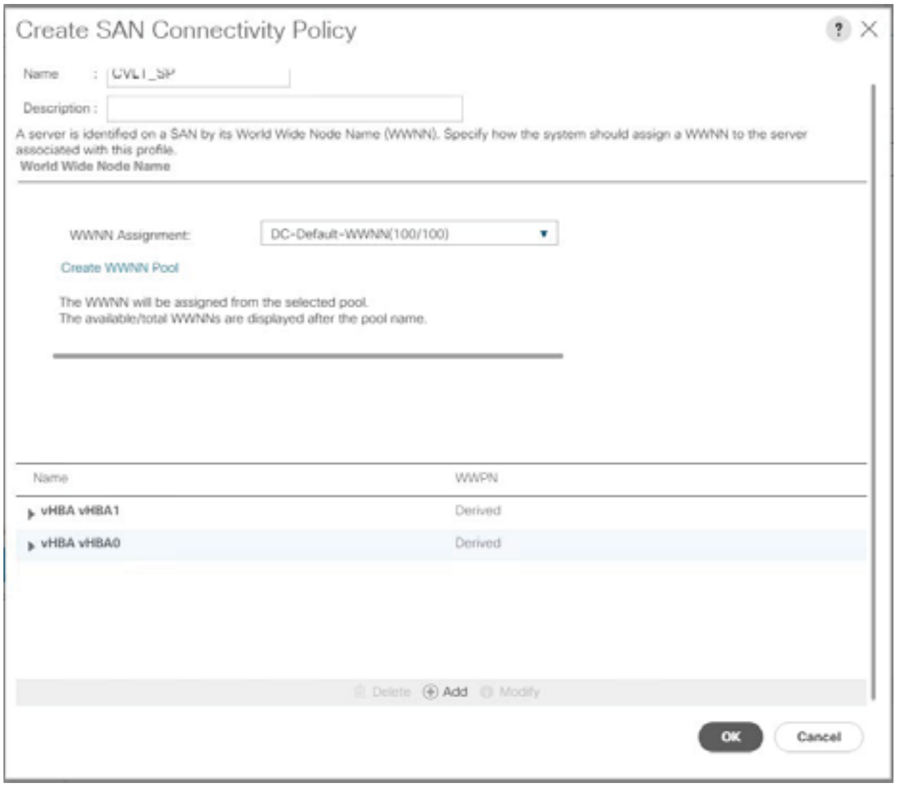
Peer Name :

vHBA Template : vHBA1

Adapter Performance Profile

Adapter Policy : Linux

Click Add.



Create SAN Connectivity Policy

Name : CVLT_SP

Description :

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: DC-Default-WWNN(100/100)

Create WWNN Pool

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

Name	WWPN
vHBA vHBA1	Derived
vHBA vHBA0	Derived

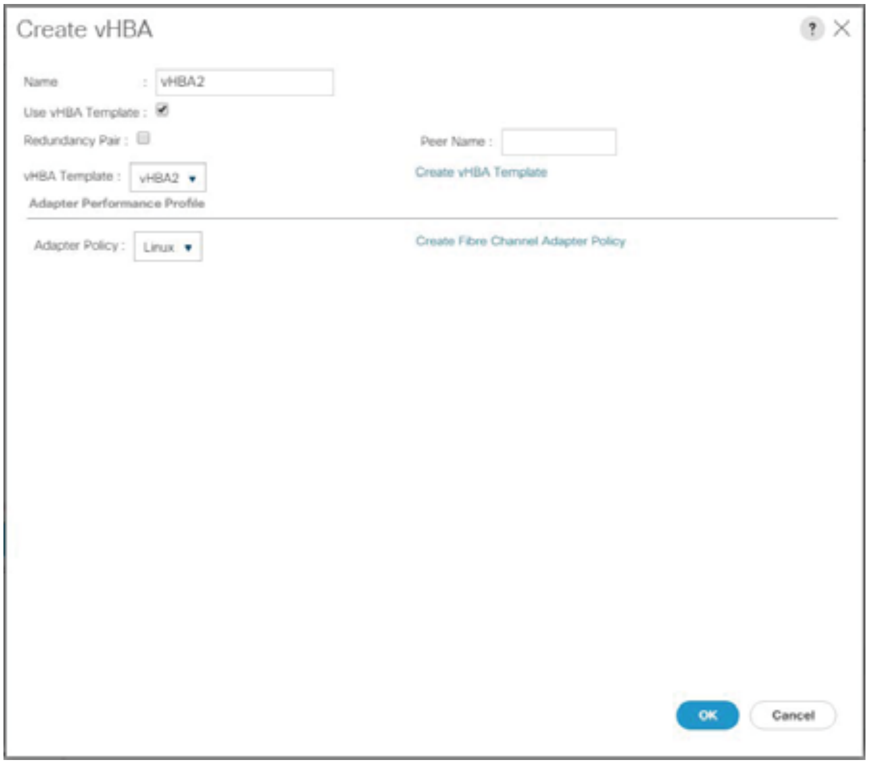
Enter an obvious name.

Select Use vHBA Template.

Select one of the vHBA templates.

Select Linux as the adapter policy.

Click OK.



Create vHBA

Name : vHBA2

Use vHBA Template : ☑

Redundancy Pair : □

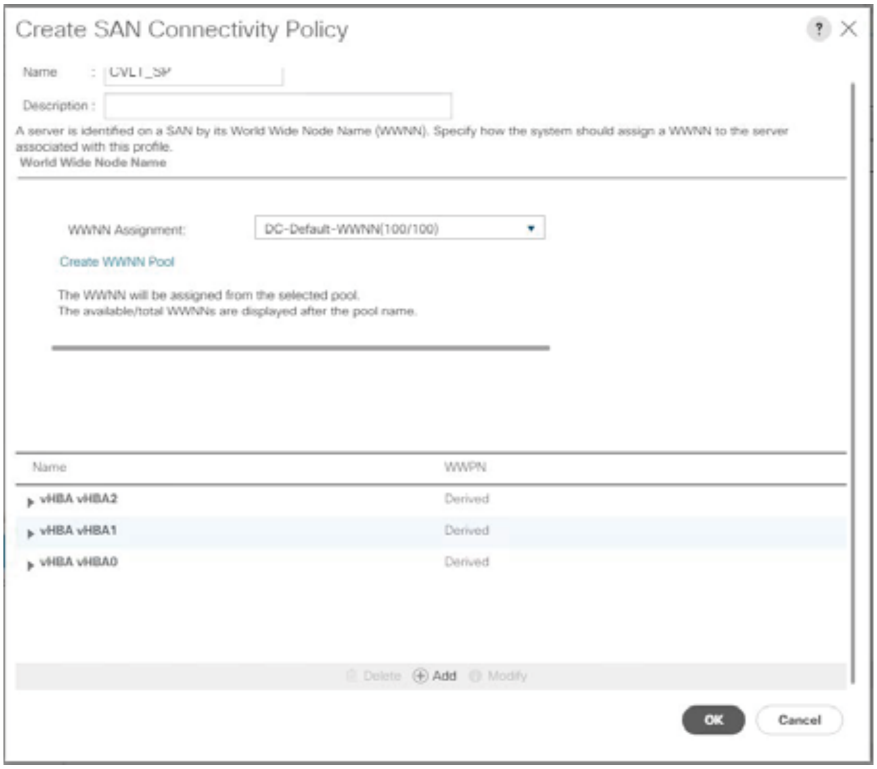
Peer Name :

vHBA Template : vHBA2 ▾

Adapter Performance Profile

Adapter Policy : Linux ▾

Click Add.



Create SAN Connectivity Policy

Name : CVLT_SP

Description :

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: DC-Default-WWNN(100/100) ▾

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

Name	WWPN
▸ vHBA vHBA2	Derived
▸ vHBA vHBA1	Derived
▸ vHBA vHBA0	Derived

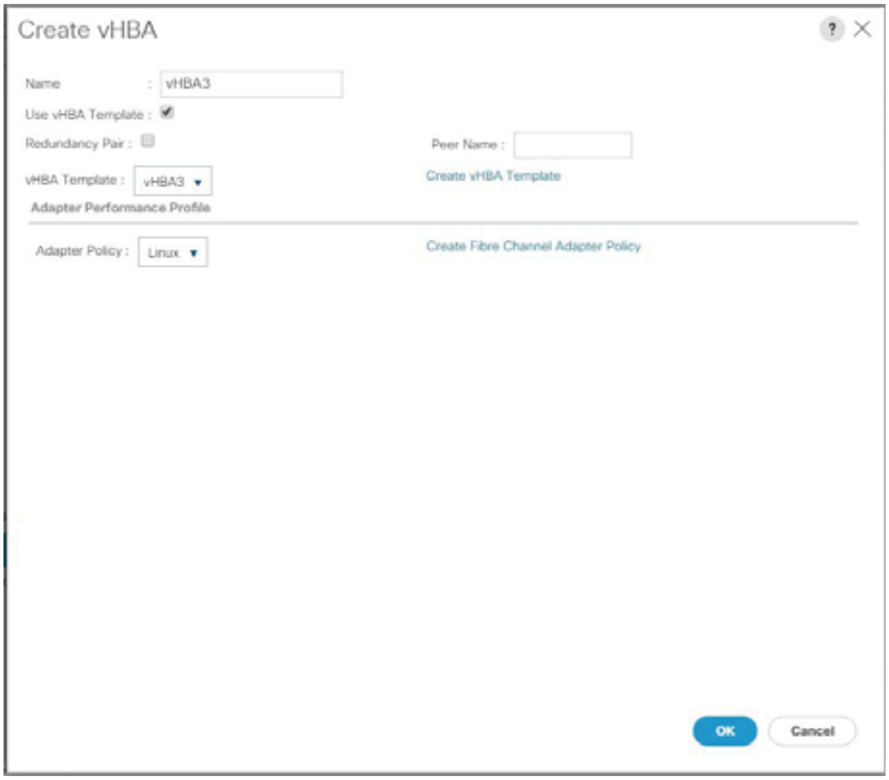
Enter an obvious name.

Select Use vHBA Template.

Select one of the vHBA templates.

Select Linux as the adapter policy.

Click OK.



Create vHBA

Name : vHBA3

Use vHBA Template : ☑

Redundancy Pair : □

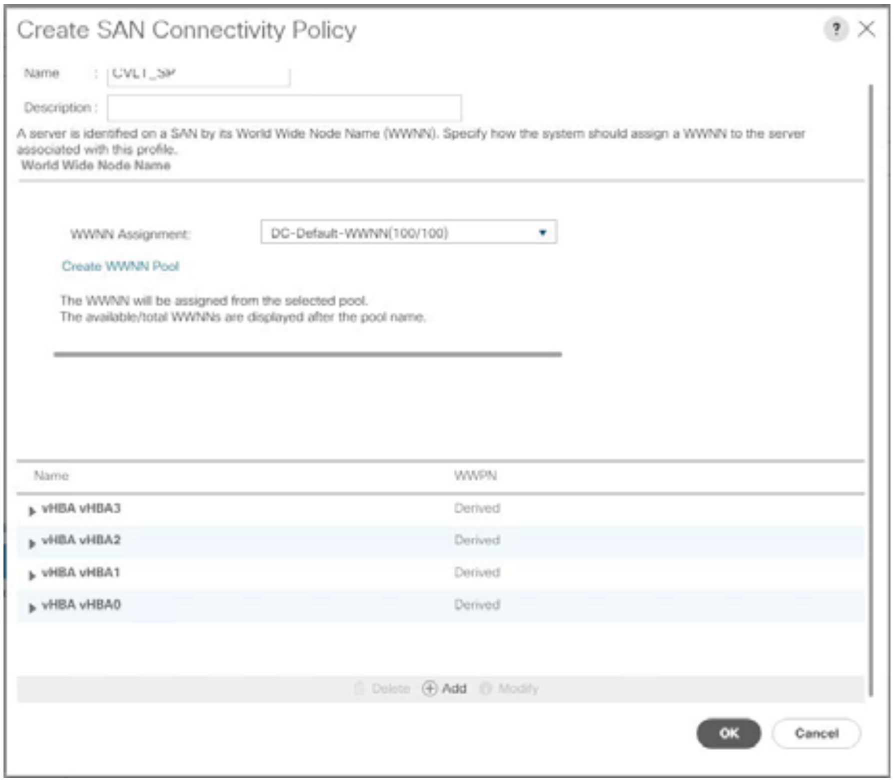
Peer Name :

vHBA Template : vHBA3

Adapter Performance Profile

Adapter Policy : Linux

Click OK.



Create SAN Connectivity Policy

Name : CVLT_SP

Description :

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.

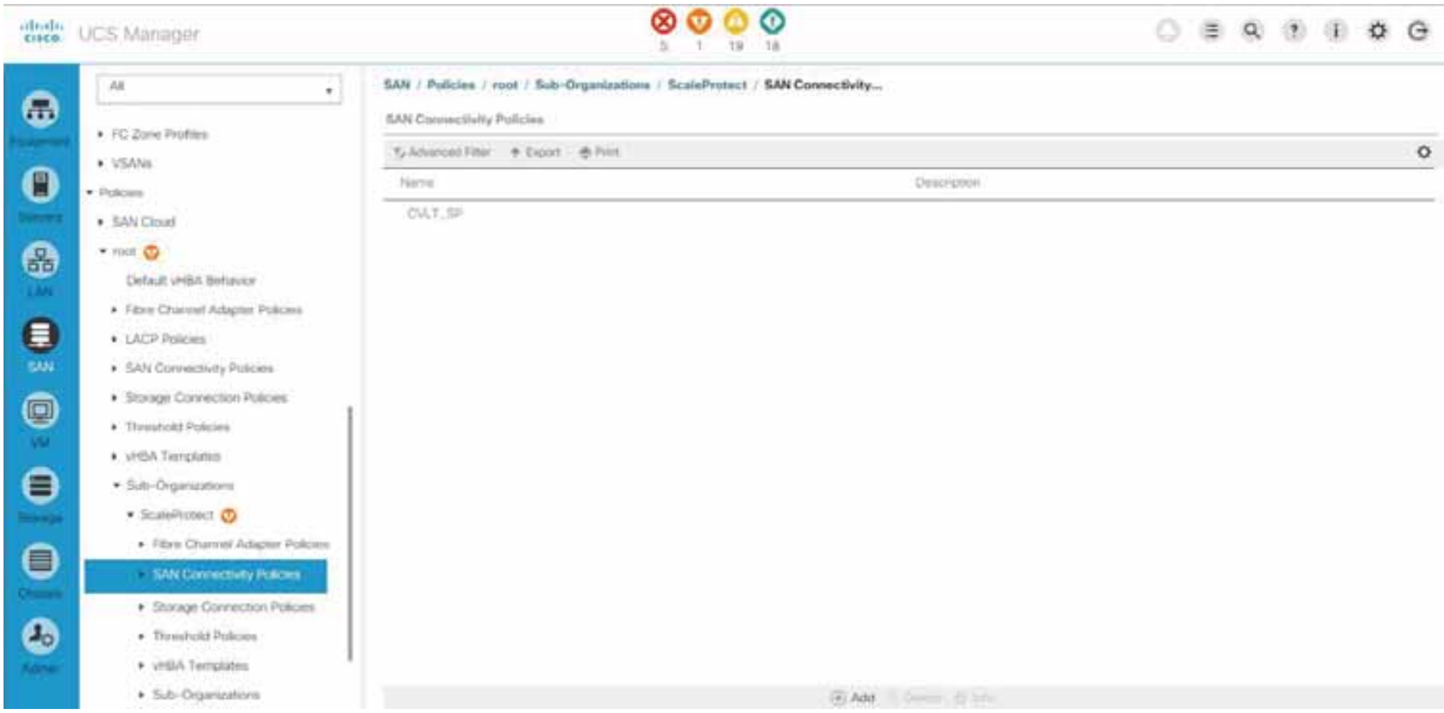
World Wide Node Name

WWNN Assignment: DC-Default-WWNN(100/100)

Create WWNN Pool

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

Name	WWPN
vHBA vHBA3	Derived
vHBA vHBA2	Derived
vHBA vHBA1	Derived
vHBA vHBA0	Derived



SAN / Policies / root / Sub-Organizations / ScaleProtect / SAN Connectivity...

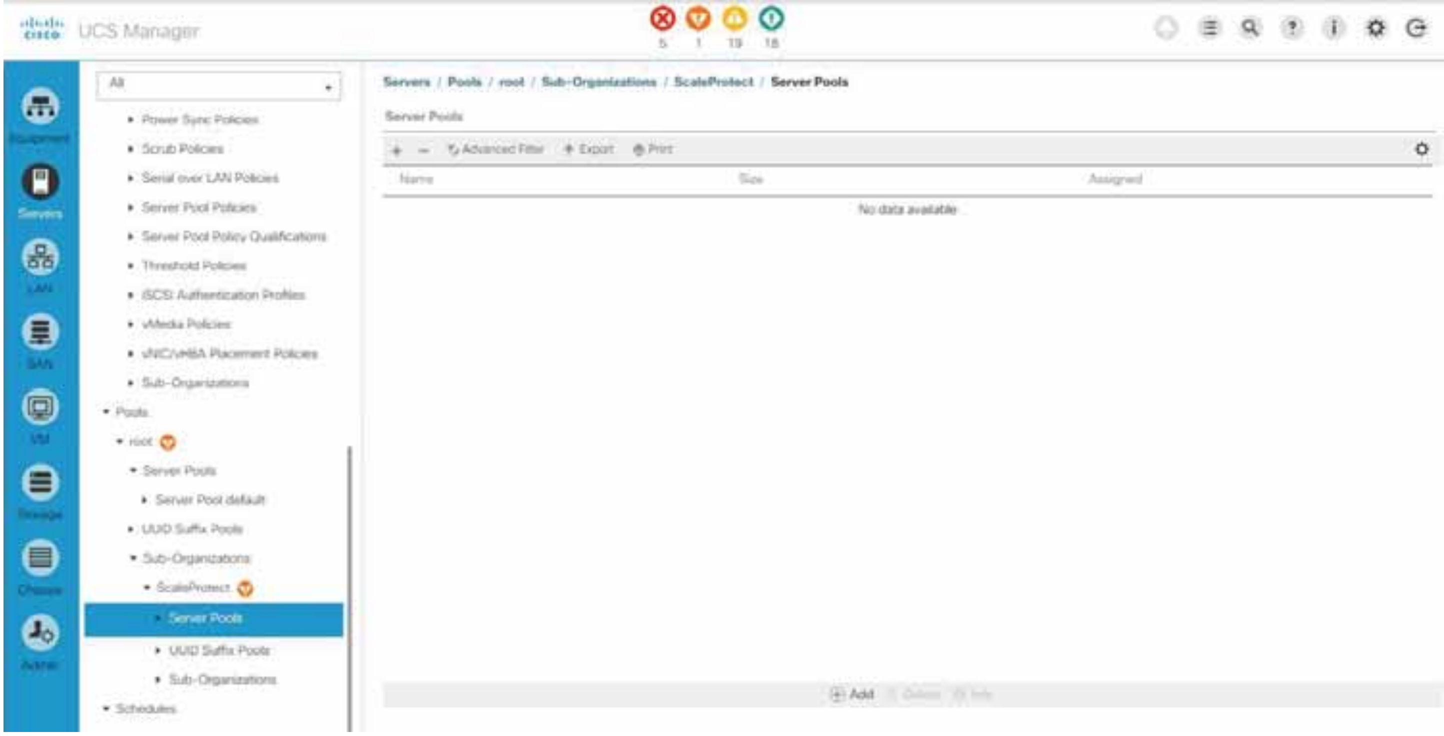
SAN Connectivity Policies

Name	Description
CVLT_SP	

Server pool configuration

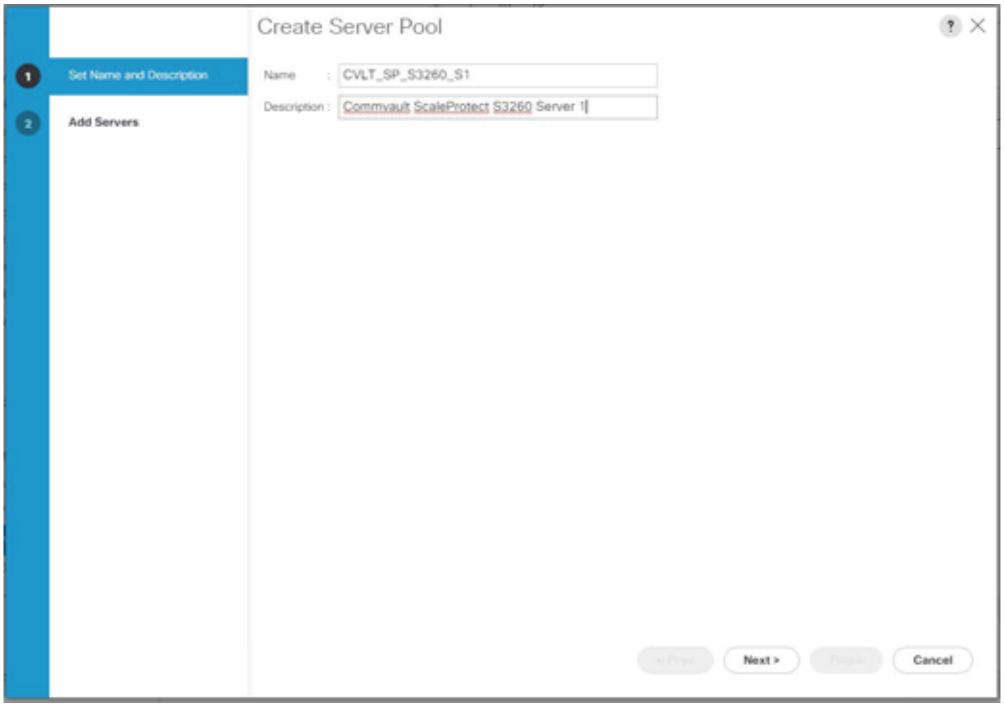
The next task is to define a server pool to collect all ScaleProtect servers in one place.

Go to Server > Pools > root > Sub-Organizations > ScaleProtect > Server Pool and click Add.



Enter an obvious name.

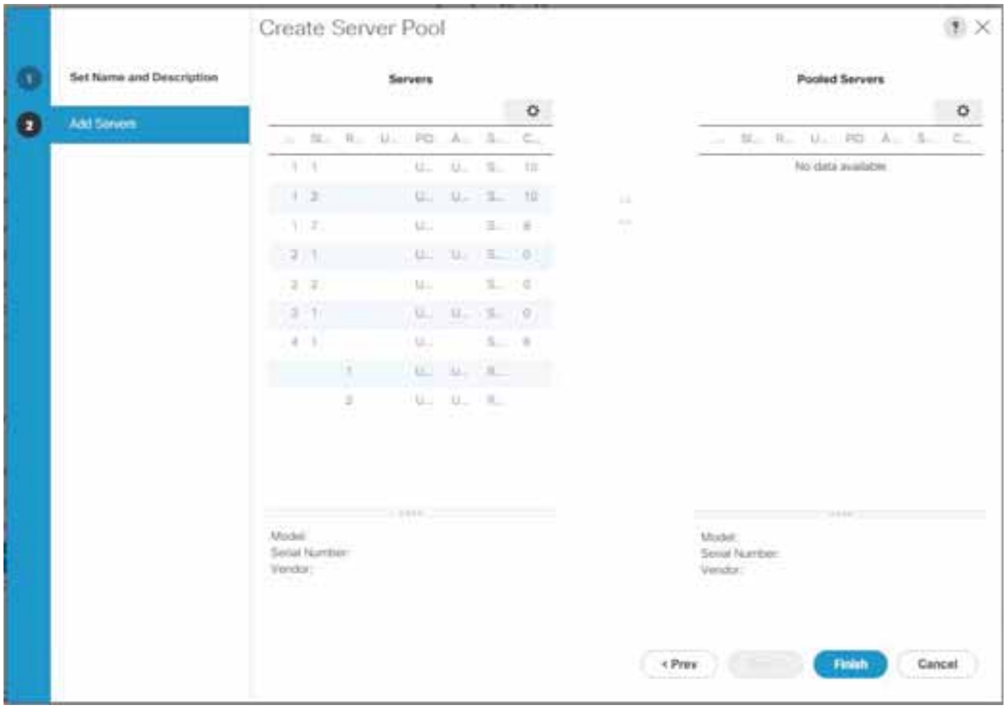
Click Next.



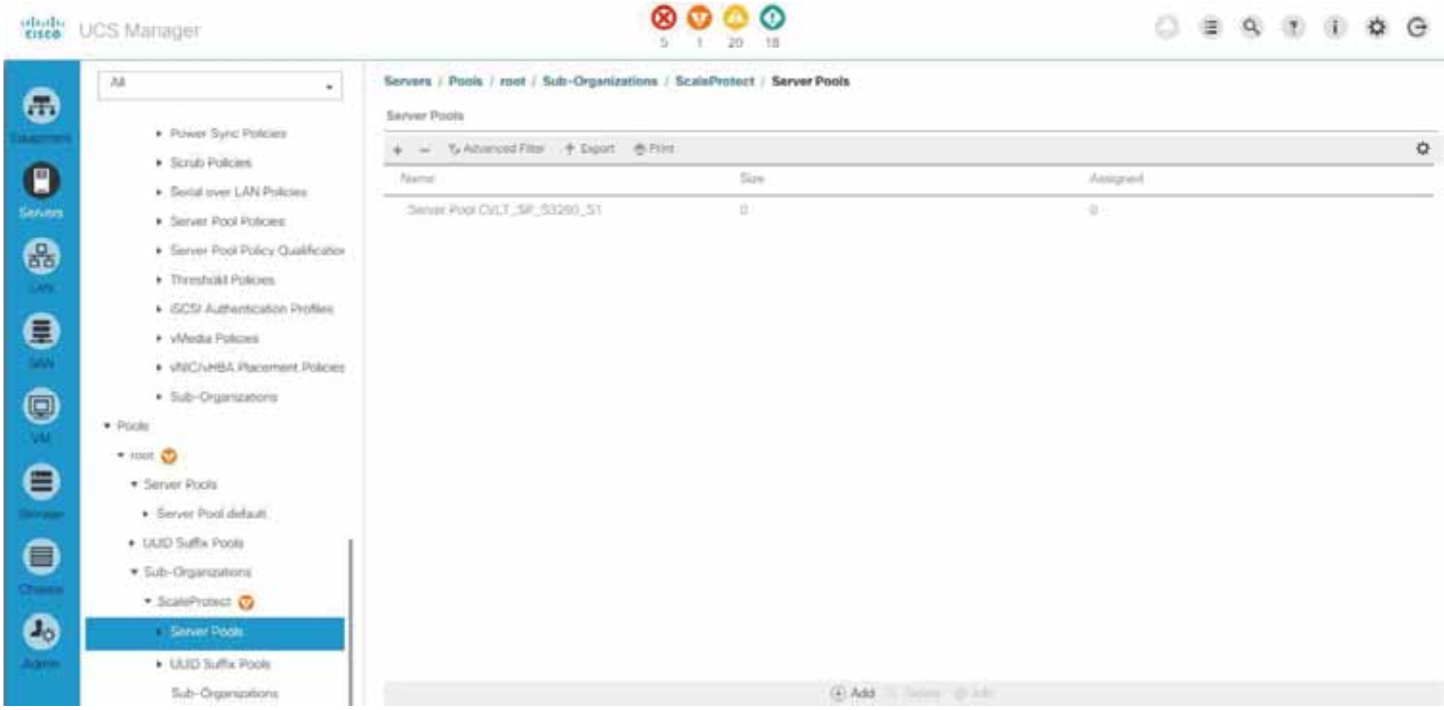
Name : CVLT_SP_S3260_S1

Description : Commvault ScaleProtect S3260 Server 1

Click Finish.



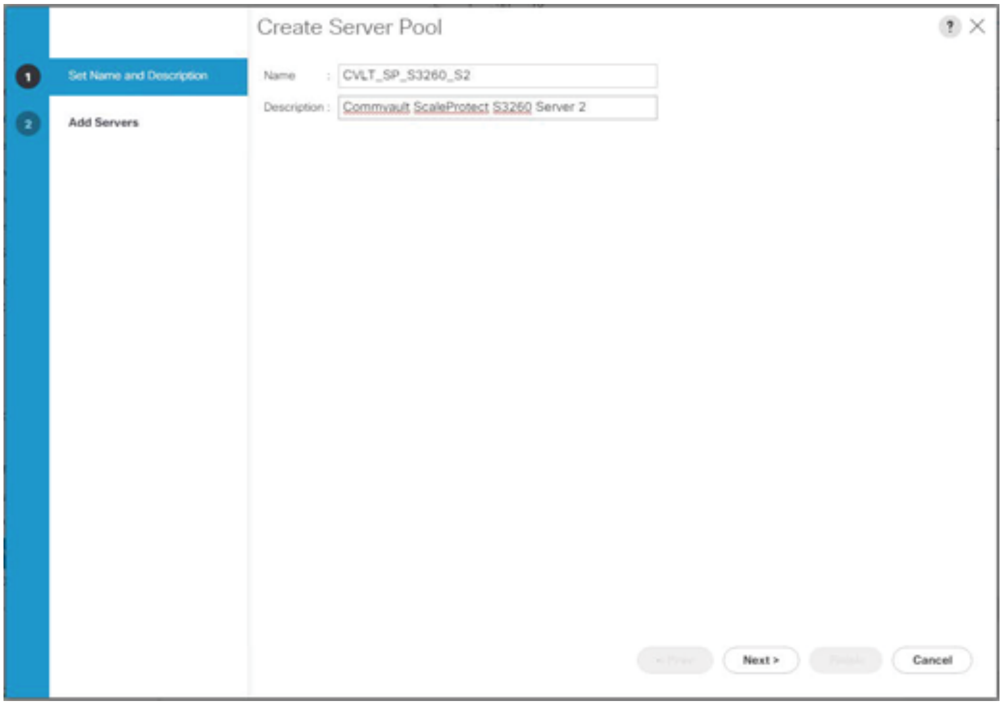
Click Add.



Name	Size	Assigned
Server Pool CVLT_SP_S3260_S1	0	0

Enter an obvious name.

Click Next.



Create Server Pool

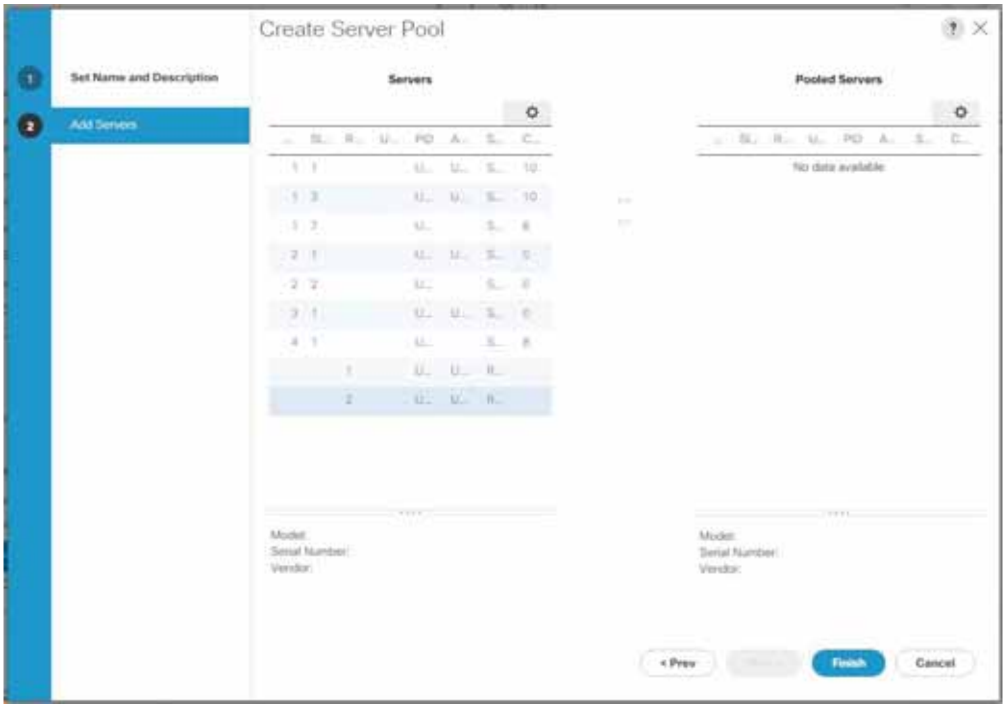
1 Set Name and Description

2 Add Servers

Name : CVLT_SP_S3260_S2

Description : Commvault ScaleProtect S3260 Server 2

Click Finish.



Create Server Pool

1 Set Name and Description

2 Add Servers

Servers

…	Sl…	R…	U…	PID	A…	S…	C…
1	1			U…	U…	S…	10
1	3			U…	U…	S…	10
1	2			U…		S…	6
2	1			U…	U…	S…	5
2	2			U…		S…	6
3	1			U…	U…	S…	6
4	1			U…		S…	8
		1		U…	U…	R…	
		2		U…	U…	R…	

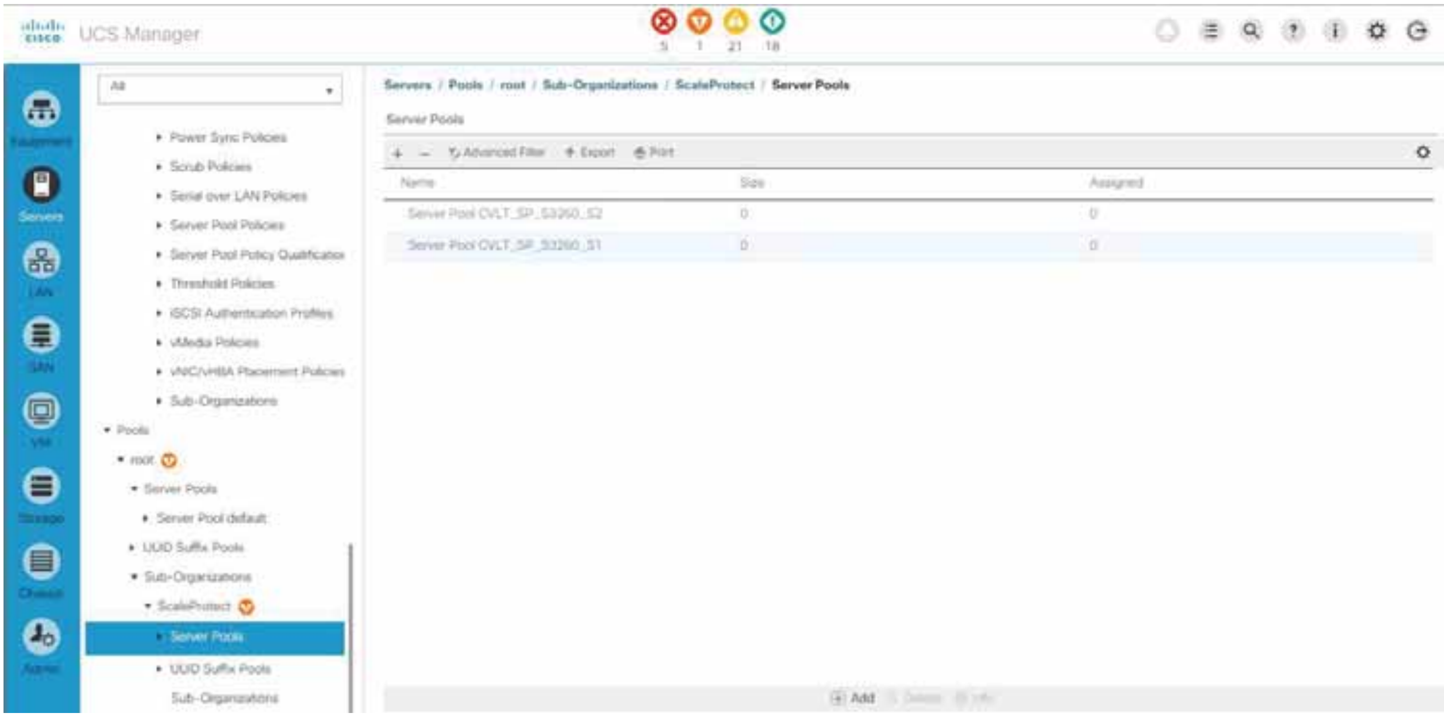
Model:
Serial Number:
Vendor:

Pooled Servers

…	Sl…	R…	U…	PID	A…	S…	C…

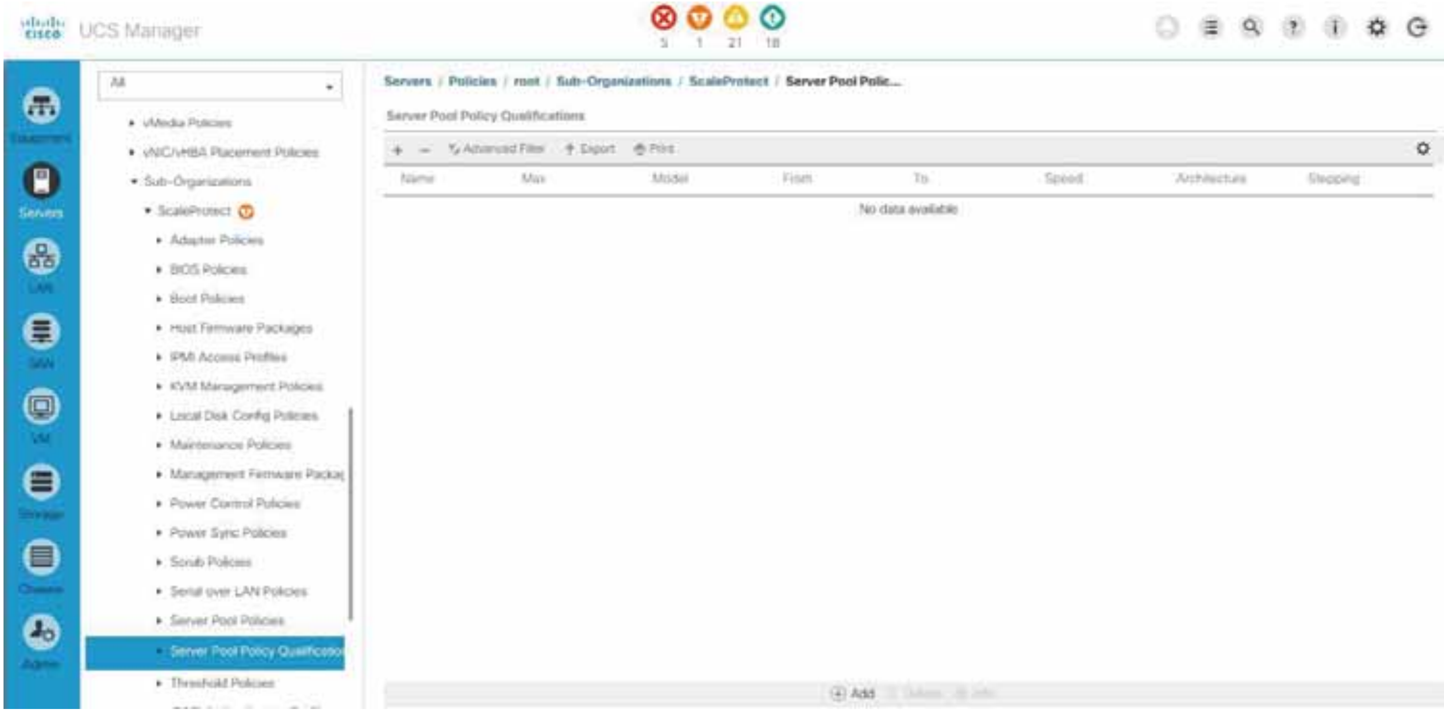
No data available

Model:
Serial Number:
Vendor:



Name	Size	Assigned
Server Pool CVLT_SP_S3260_S2	0	0
Server Pool CVLT_SP_S3260_S1	0	0

Go to Server > Policies > root > Sub-Organizations > ScaleProtect > Server Pool Policy Qualification and click Add.

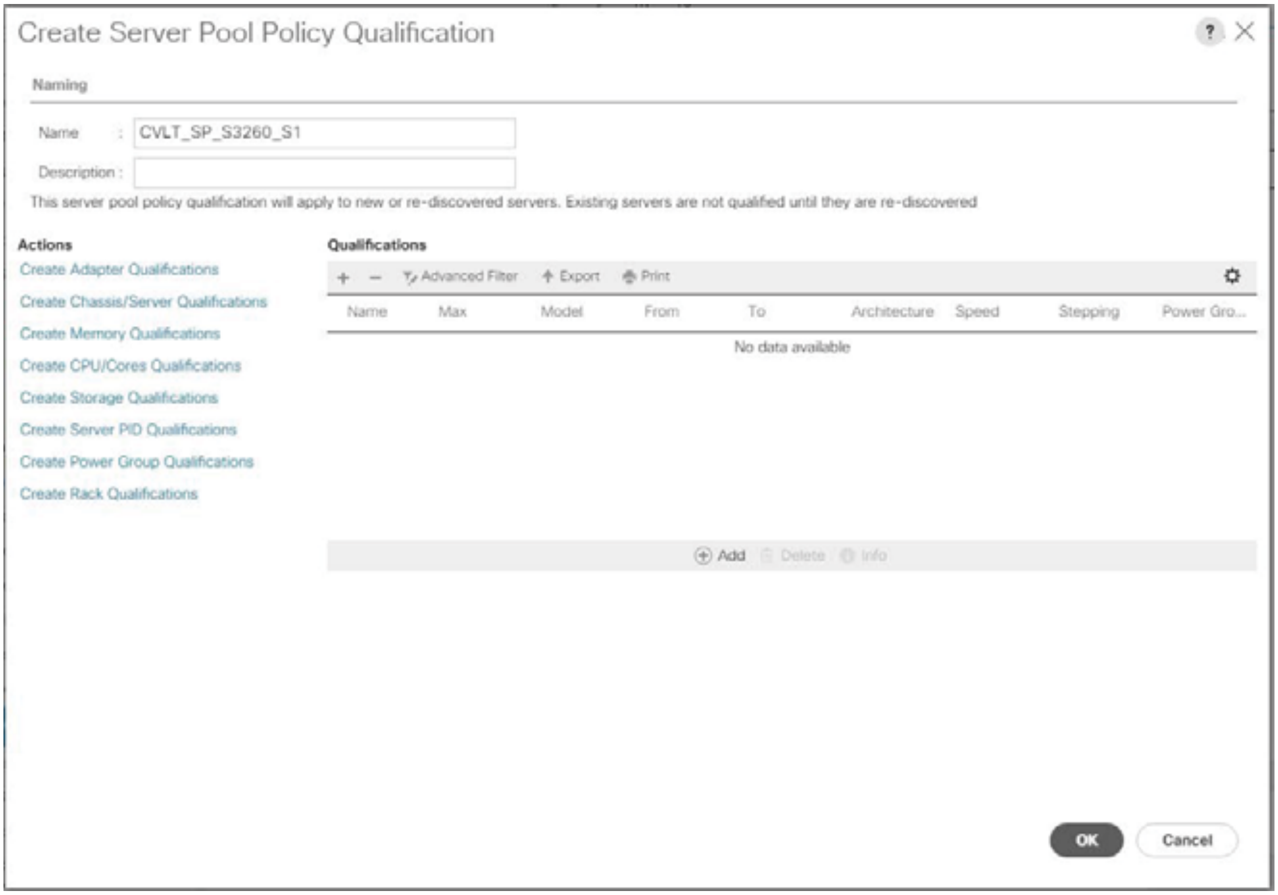


Name	Max	Model	From	To	Speed	Architecture	Stepping

No data available

Enter an obvious name.

Click Create Server PID Qualifications.



Create Server Pool Policy Qualification

Naming

Name : CVLT_SP_S3260_S1

Description :

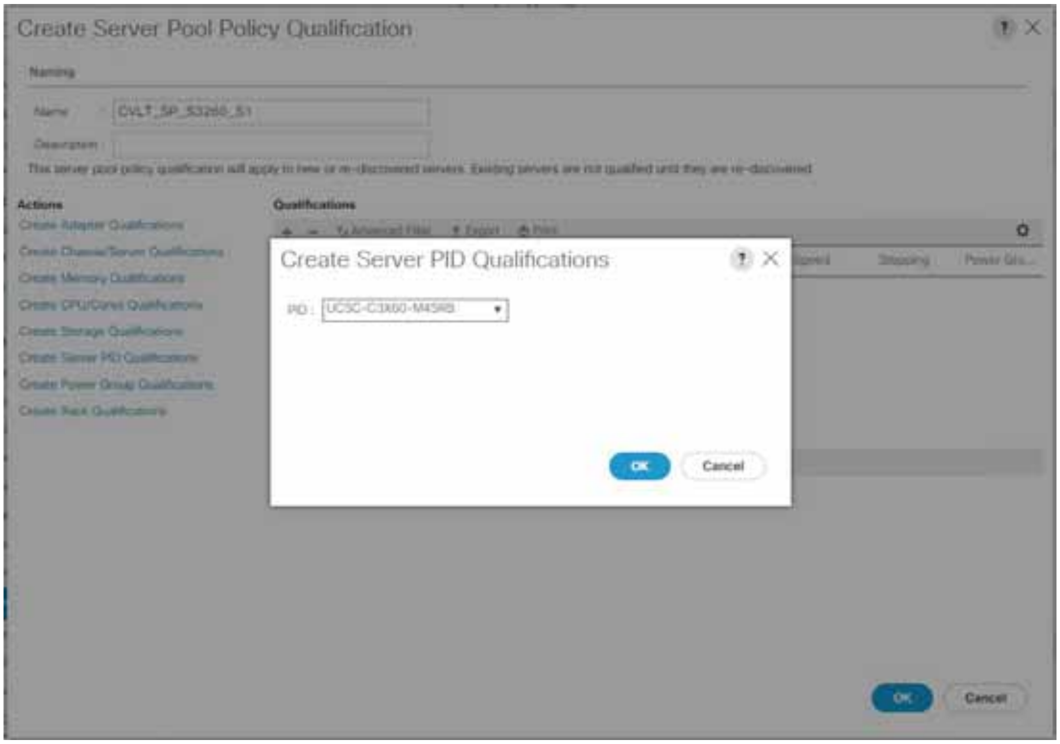
This server pool policy qualification will apply to new or re-discovered servers. Existing servers are not qualified until they are re-discovered

Actions
Create Adapter Qualifications
Create Chassis/Server Qualifications
Create Memory Qualifications
Create CPU/Cores Qualifications
Create Storage Qualifications
Create Server PID Qualifications
Create Power Group Qualifications
Create Rack Qualifications
Qualifications
Advanced Filter
Export
Print
Add
Delete
Info
OK
Cancel

Name	Max	Model	From	To	Architecture	Speed	Stepping	Power Gro...

No data available

Select UCSC-C3X60-M4SRB or UCSC-C3K-M4SRB, depending on what is shown under Equipment.



Create Server Pool Policy Qualification

Naming

Name : CVLT_SP_S3260_S1

Description :

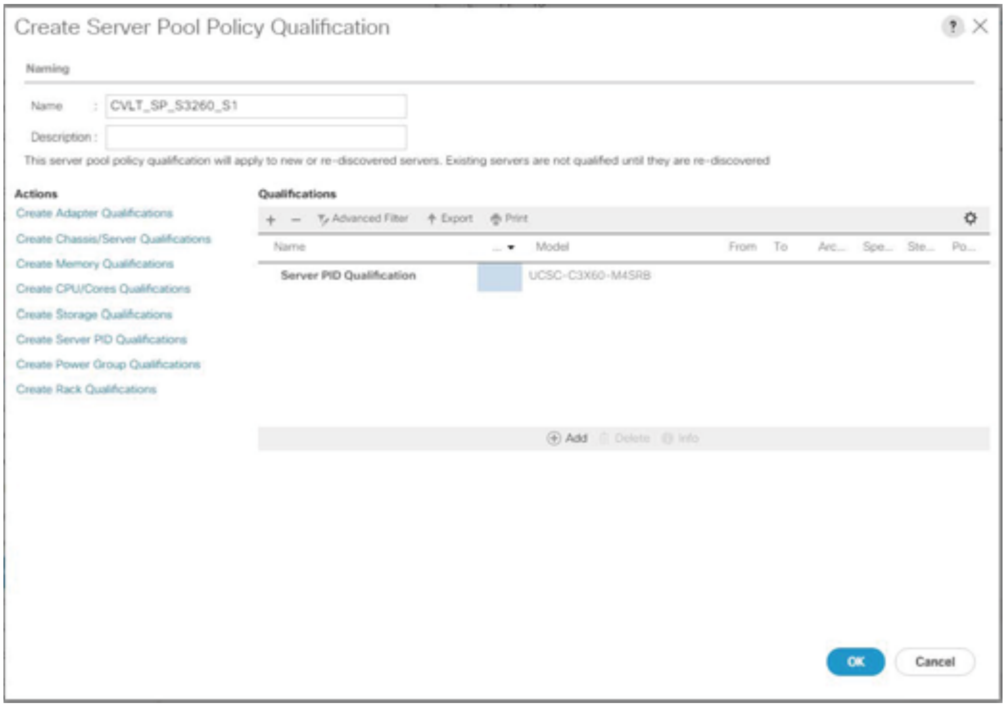
This server pool policy qualification will apply to new or re-discovered servers. Existing servers are not qualified until they are re-discovered

Create Server PID Qualifications

PID : UCSC-C3X60-M4SRB

Actions
Create Adapter Qualifications
Create Chassis/Server Qualifications
Create Memory Qualifications
Create CPU/Cores Qualifications
Create Storage Qualifications
Create Server PID Qualifications
Create Power Group Qualifications
Create Rack Qualifications
Qualifications
Advanced Filter
Export
Print
Stepping
Power Gro...
OK
Cancel
OK
Cancel

Click Create Chassis/Server Qualifications.



Create Server Pool Policy Qualification

Naming

Name : CVLT_SP_S3260_S1

Description :

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

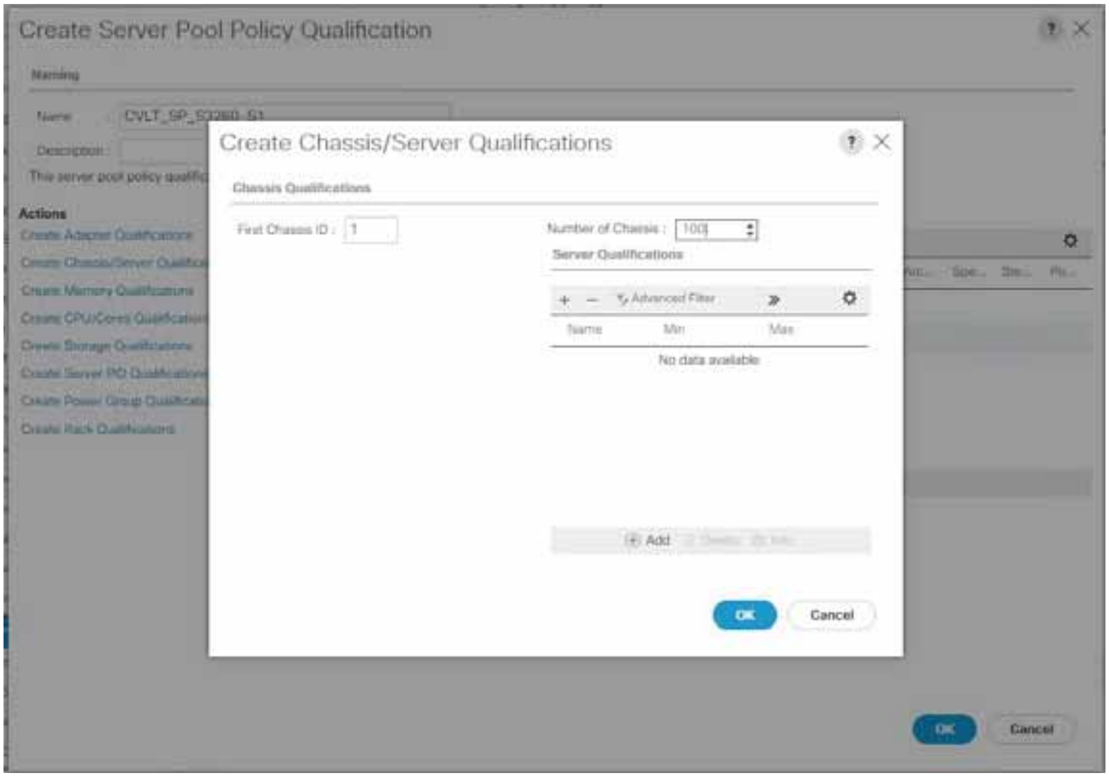
Qualifications

Name	Model	From	To	Arc...	Spe...	Ste...	Po...
Server PID Qualification	UCSC-C3X60-M4SRB						

Actions
Create Adapter Qualifications
Create Chassis/Server Qualifications
Create Memory Qualifications
Create CPU/Cores Qualifications
Create Storage Qualifications
Create Server PID Qualifications
Create Power Group Qualifications
Create Rack Qualifications
Advanced Filter
Export
Print
Add
Delete
Info
OK
Cancel

Enter **1** as the first chassis ID and enter **100** as the number of chassis.

Click Add.



Create Server Pool Policy Qualification

Naming

Name : CVLT_SP_S3260_S1

Description :

This server pool policy qualific

Create Chassis/Server Qualifications

Chassis Qualifications

First Chassis ID : 1

Number of Chassis : 100

Server Qualifications

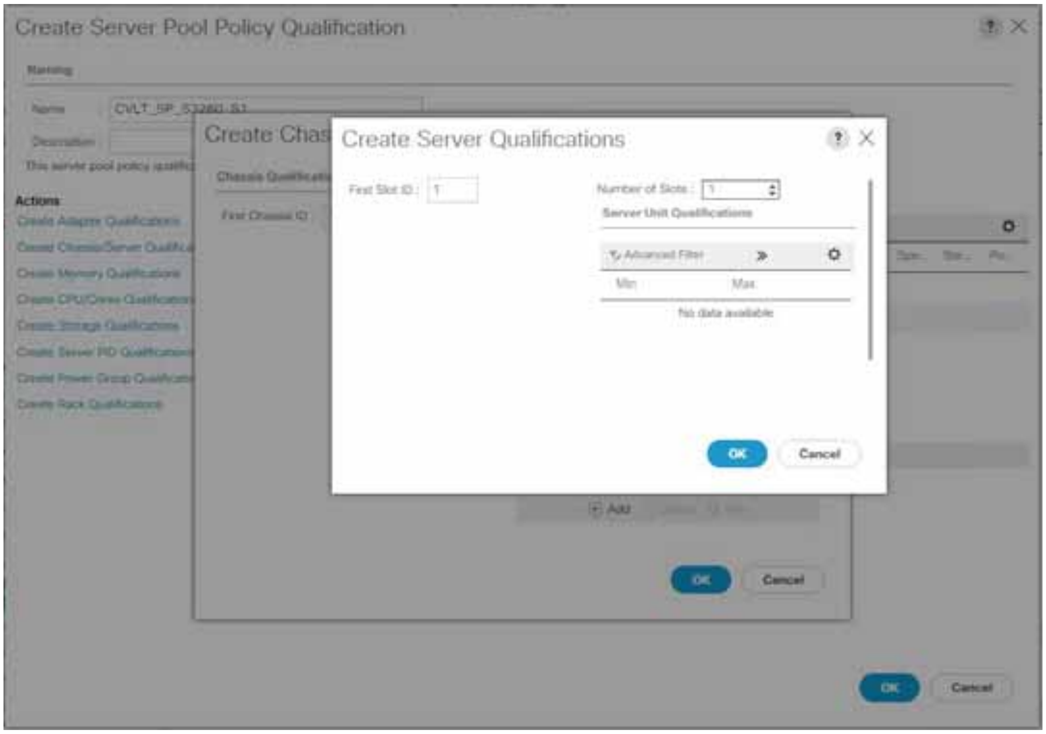
Name	Min	Max

No data available

?
Actions
Create Adapter Qualifications
Create Chassis/Server Qualific
Create Memory Qualifications
Create CPU/Cores Qualification
Create Storage Qualifications
Create Server PCI Qualification
Create Power Group Qualificati
Create Rack Qualifications
Arc... Spe... Ste... Po...
+ −
Advanced Filter
Add
Delete
Info
OK
Cancel
OK
Cancel

Enter **1** as first slot ID and **1** as the number of slots.

Click OK.



Create Server Pool Policy Qualification

Naming

Name : CVLT_SP_S3260_S1

Description :

This server pool policy qualific

Create Chas

Chassis Qualificati

First Chassis ID

Create Server Qualifications

First Slot ID : 1

Number of Slots : 1

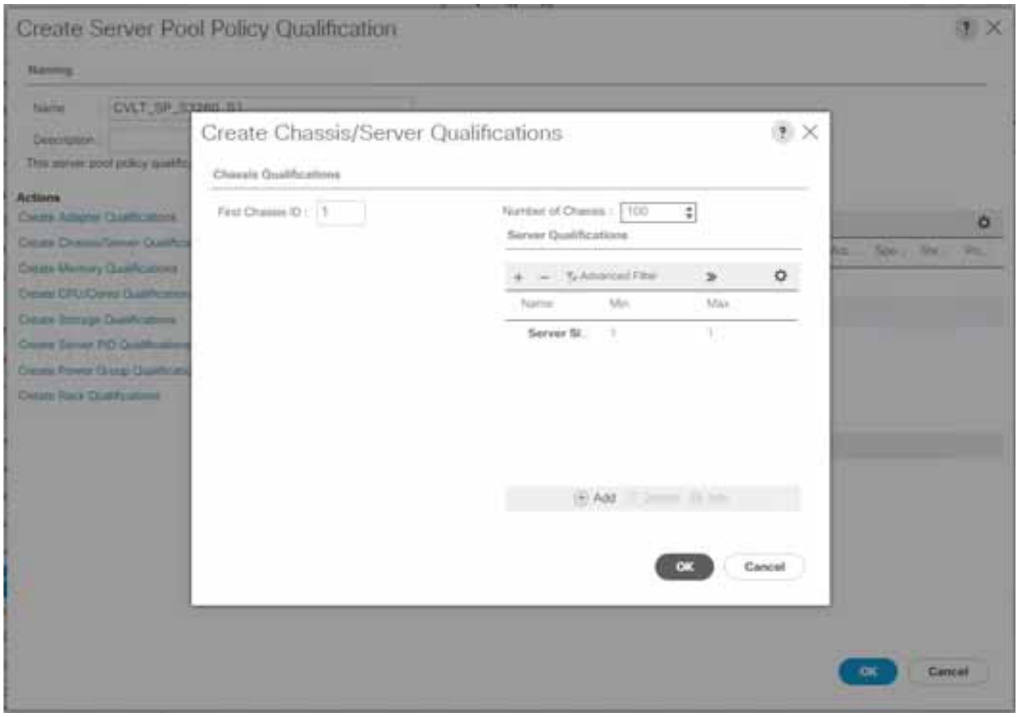
Server Unit Qualifications

Min	Max

No data available

?
Actions
Create Adapter Qualifications
Create Chassis/Server Qualifica
Create Memory Qualifications
Create CPU/Cores Qualification
Create Storage Qualifications
Create Server PCI Qualification
Create Power Group Qualificatio
Create Rack Qualifications
Spe... Ste... Po...
Advanced Filter
OK
Cancel
Add
Delete
Info
OK
Cancel
OK
Cancel

Click OK.


Create Server Pool Policy Qualification
Naming
Name
Description
Actions
Create Adapter Qualifications
Create Chassis/Server Qualific
Create Memory Qualifications
Create CPU/Cores Qualification
Create Storage Qualifications
Create Server PID Qualification
Create Power Group Qualificati
Create Rack Qualifications
OK
Cancel
Create Chassis/Server Qualifications
Chassis Qualifications
Server Qualifications
Advanced Filter
Add
Delete
Info
OK
Cancel

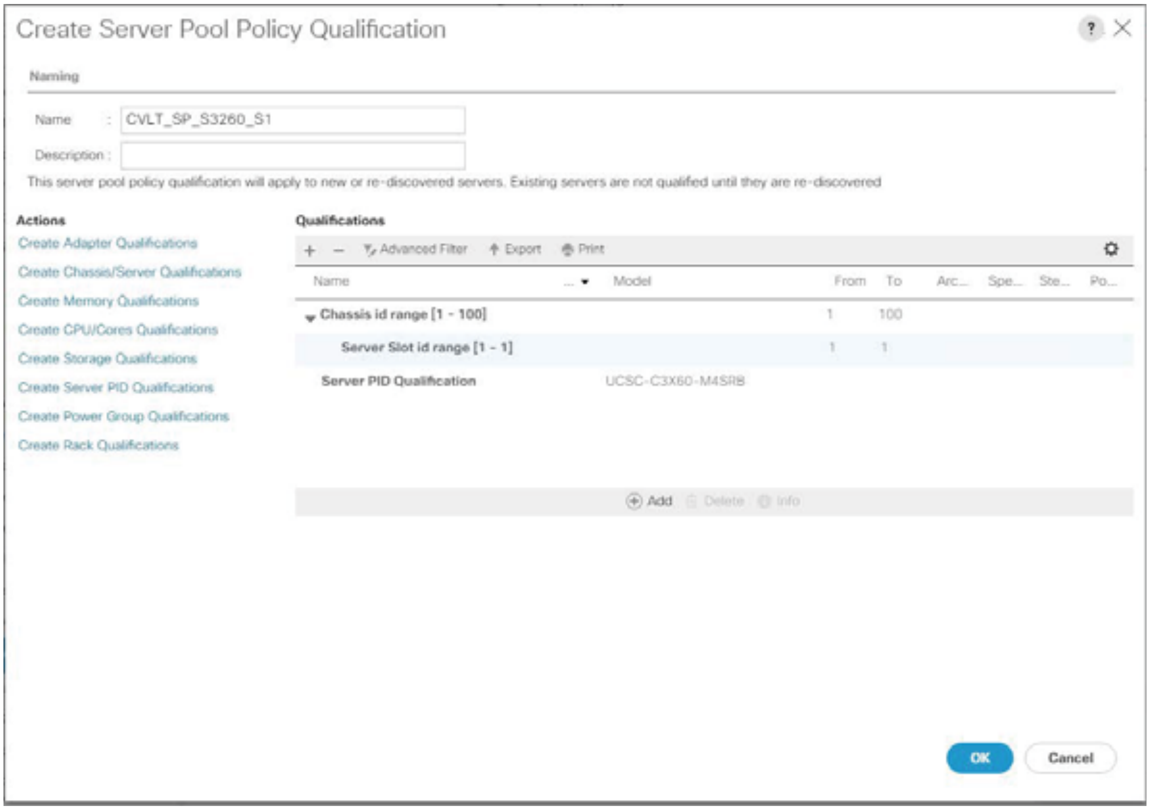
Name: CVLT_SP_S3260_S1

First Chassis ID : 1

Number of Chassis : 100

Name	Min	Max
Server Sl..	1	1

Click OK.


Create Server Pool Policy Qualification
Naming
Actions
Create Adapter Qualifications
Create Chassis/Server Qualifications
Create Memory Qualifications
Create CPU/Cores Qualifications
Create Storage Qualifications
Create Server PID Qualifications
Create Power Group Qualifications
Create Rack Qualifications
Qualifications
Advanced Filter
Export
Print
Add
Delete
Info
OK
Cancel

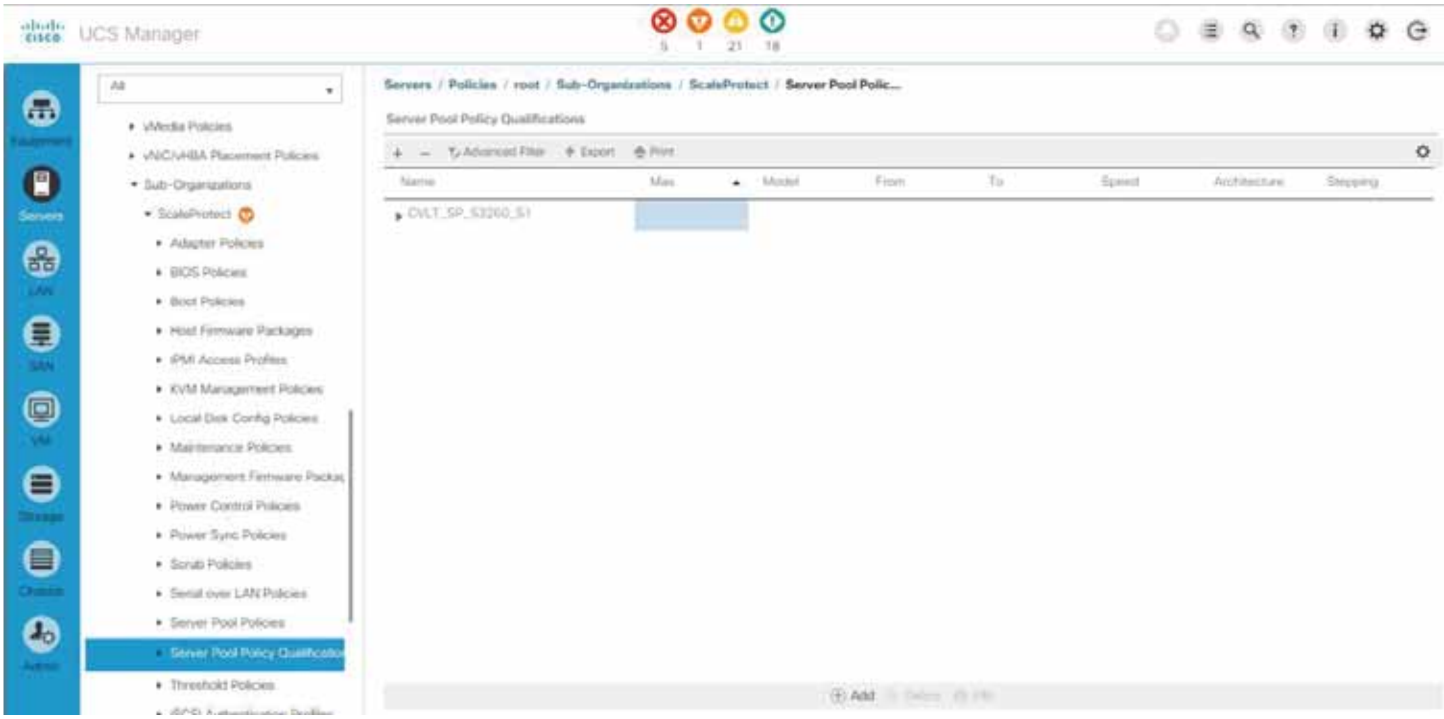
Name : CVLT_SP_S3260_S1

Description :

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

Name	Model	From	To	Arc...	Spe...	Ste...	Po...
Chassis id range [1 - 100]		1	100				
Server Slot id range [1 - 1]		1	1				
Server PID Qualification	UCSC-C3X60-M4SRB						

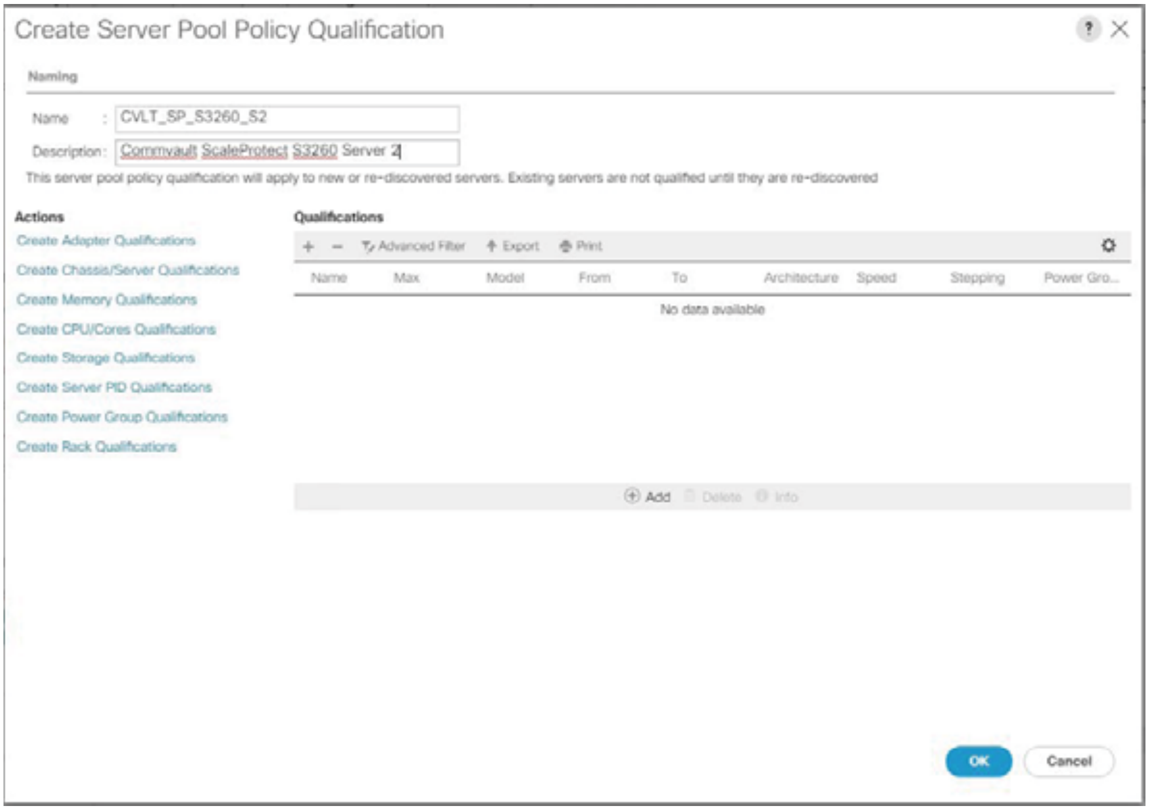
Click Add.



Name	Max	Model	From	To	Speed	Architecture	Stepping
CVLT_SP_S3260_S1							

Enter an obvious name.

Click Create Server PID Qualifications.



Create Server Pool Policy Qualification

Naming

Name : CVLT_SP_S3260_S2

Description : Commvault ScaleProtect S3260 Server 2

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

Actions

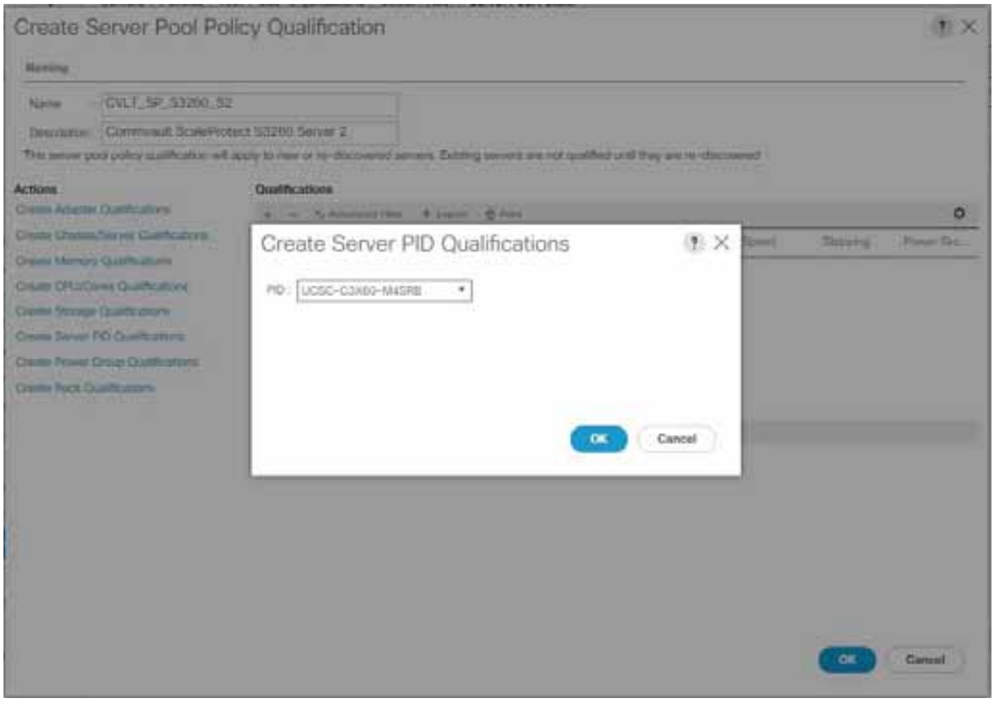
- Create Adapter Qualifications
- Create Chassis/Server Qualifications
- Create Memory Qualifications
- Create CPU/Cores Qualifications
- Create Storage Qualifications
- Create Server PID Qualifications
- Create Power Group Qualifications
- Create Rack Qualifications

Qualifications

Name	Max	Model	From	To	Architecture	Speed	Stepping	Power Gro...

No data available

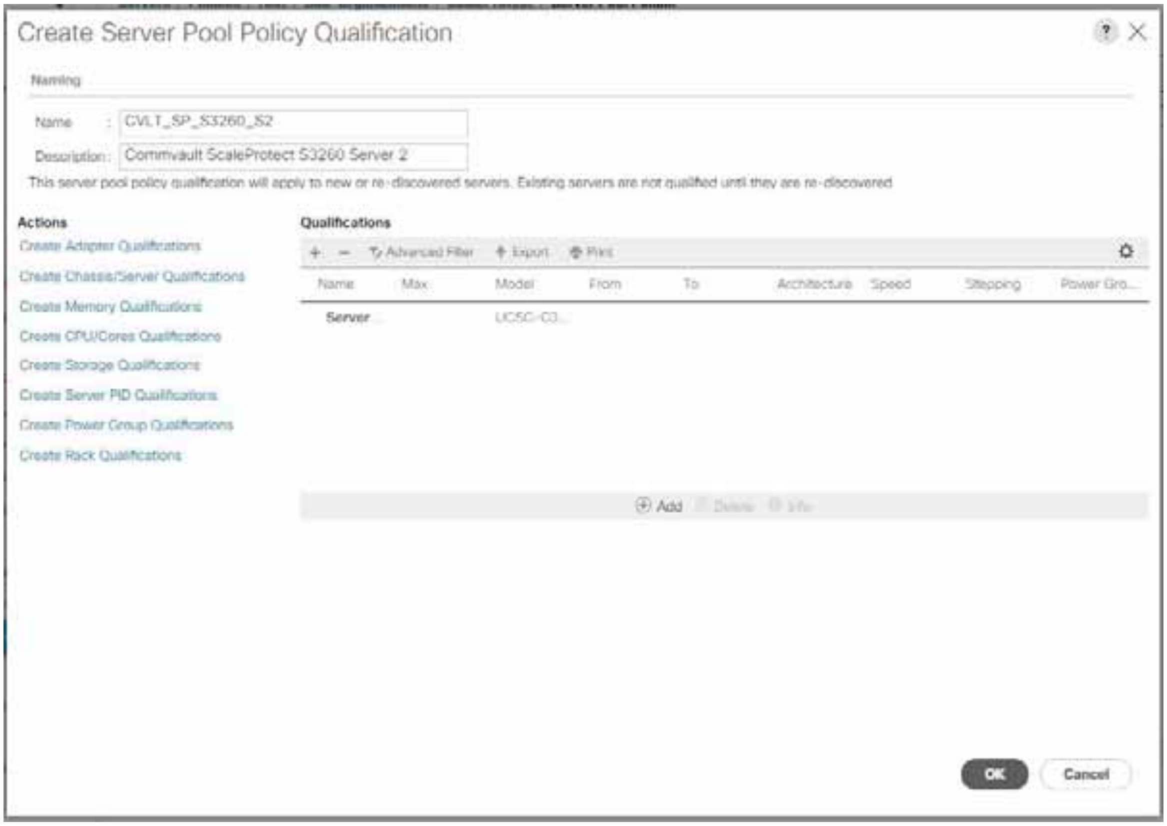
Select UCSC-C3X60-M4SRB or UCSC-C3K-M4SRB, depending on what is shown under Equipment.



Create Server PID Qualifications

PID : UCSC-C3X60-M4SRB

Click Create Chassis/Server Qualifications.



Create Server Pool Policy Qualification

Naming

Name : CVLT_SP_S3260_S2

Description : Commvault ScaleProtect S3260 Server 2

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

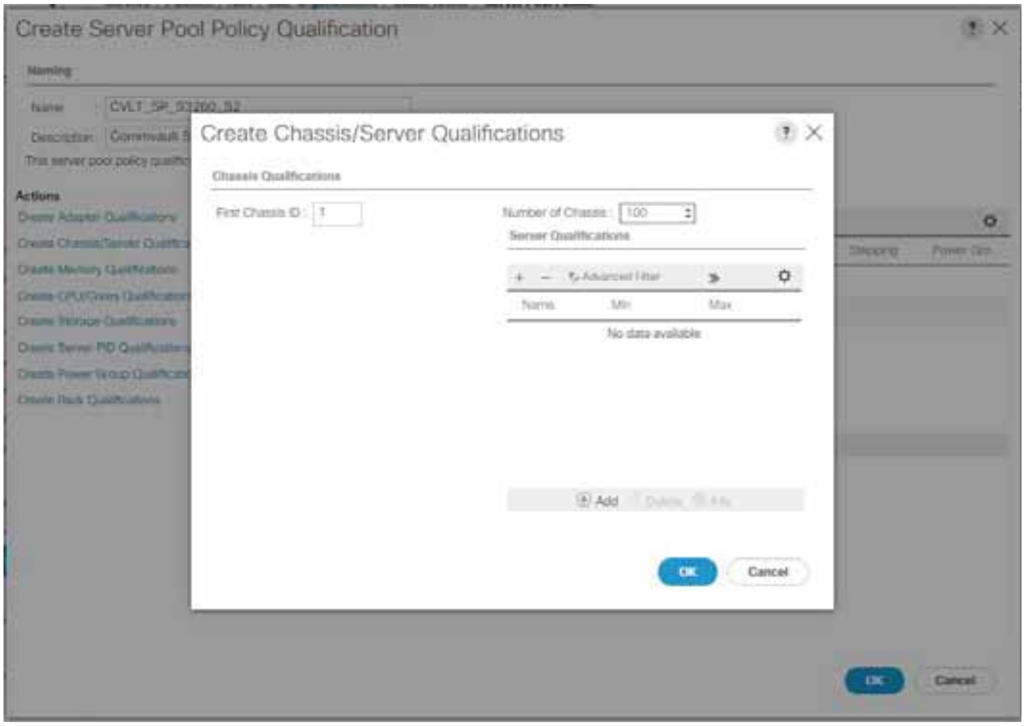
Qualifications

Name	Max	Model	From	To	Architecture	Speed	Stepping	Power Gro...
Server		UCSC-C3...						

Actions
Create Adapter Qualifications
Create Chassis/Server Qualifications
Create Memory Qualifications
Create CPU/Cores Qualifications
Create Storage Qualifications
Create Server PID Qualifications
Create Power Group Qualifications
Create Rack Qualifications
+ − Advanced Filter Export Print
Add Delete Info
OK
Cancel

Enter **1** as the first chassis ID and enter **100** as the number of chassis.

Click Add.


Create Server Pool Policy Qualification
Naming
Actions
Create Adapter Qualifications
Create Chassis/Server Qualifications
Create Memory Qualifications
Create CPU/Cores Qualifications
Create Storage Qualifications
Create Server PID Qualifications
Create Power Group Qualifications
Create Rack Qualifications
Create Chassis/Server Qualifications
Chassis Qualifications
Server Qualifications
Advanced Filter
Name
Min
Max
No data available
Add
Delete
Info
OK
Cancel
Shipping
Power Gro...

Name: CVLT_SP_S3260_S2

Description: Commvault S

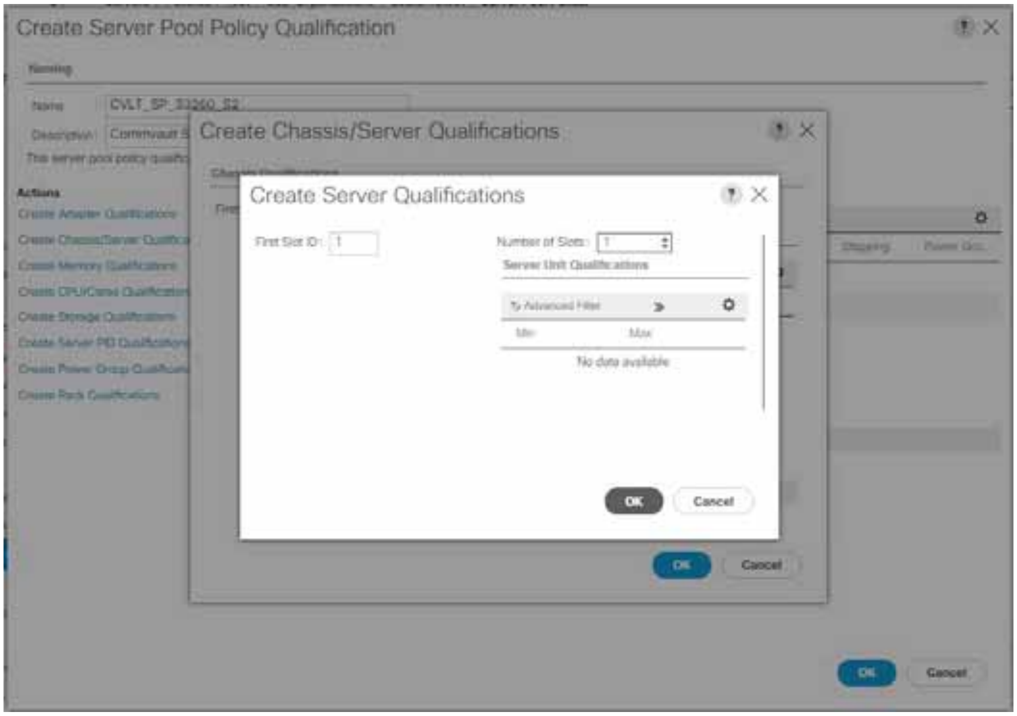
This server pool policy qualific

First Chassis ID: 1

Number of Chassis: 100

Enter 1 as first slot ID and **1** as the number of slots.

Click OK.


Create Server Pool Policy Qualification
Naming
Actions
Create Adapter Qualifications
Create Chassis/Server Qualifications
Create Memory Qualifications
Create CPU/Cores Qualifications
Create Storage Qualifications
Create Server PID Qualifications
Create Power Group Qualifications
Create Rack Qualifications
Create Chassis/Server Qualifications
Chassis Qualifications
Create Server Qualifications
Server Unit Qualifications
Advanced Filter
Min
Max
No data available
OK
Cancel
Shipping
Power Gro...

Name: CVLT_SP_S3260_S2

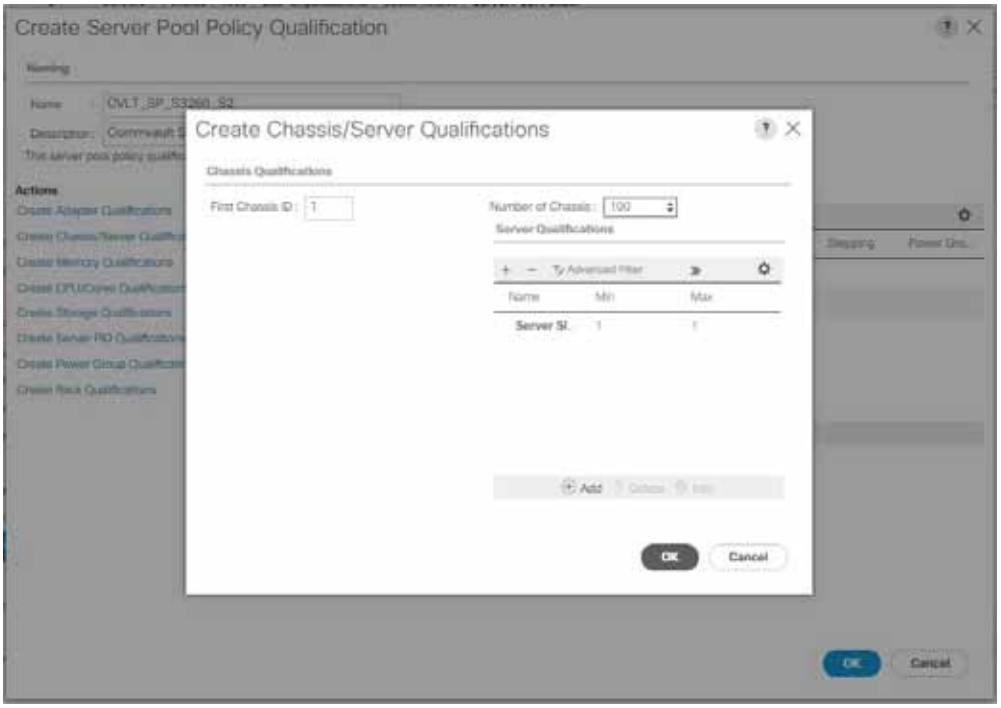
Description: Commvault S

This server pool policy qualific

First Slot ID: 1

Number of Slots: 1

Click OK.



Create Chassis/Server Qualifications

Chassis Qualifications

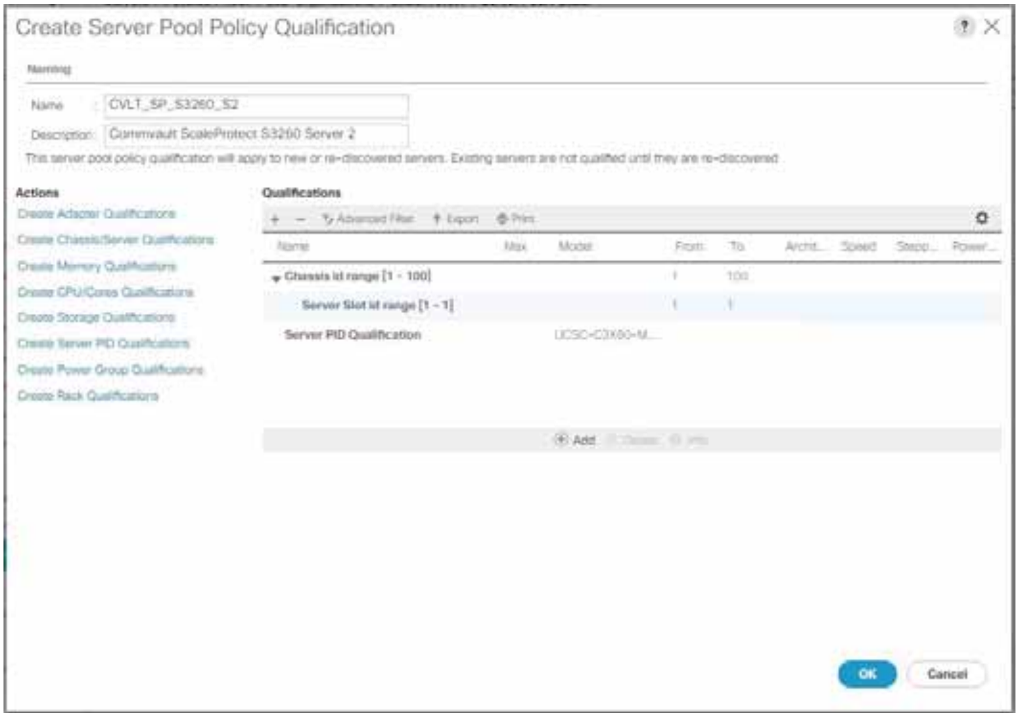
First Chassis ID : 1

Number of Chassis : 100

Server Qualifications

Name	Min	Max
Server Sl.	1	1

Click OK.



Create Server Pool Policy Qualification

Naming

Name : CVLT_SP_S3260_S2

Description : Commvault ScaleProtect S3260 Server 2

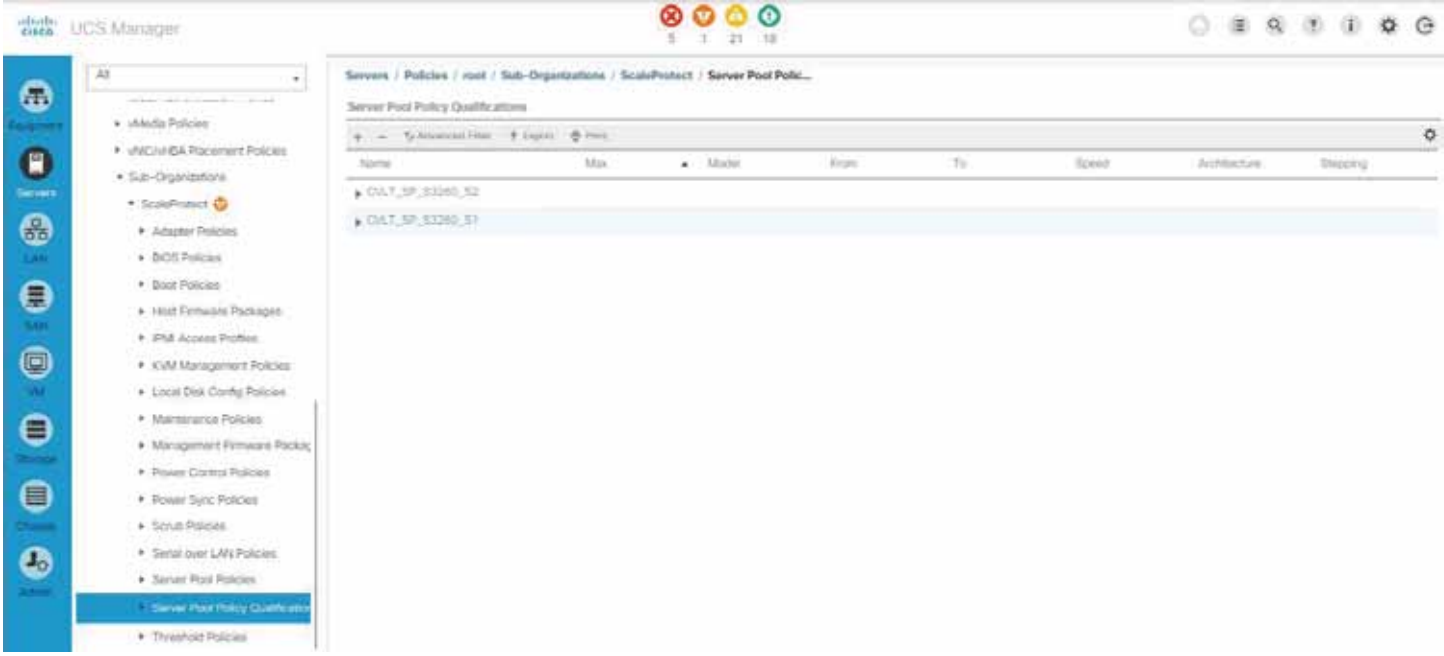
This server pool policy qualification will apply to new or re-discovered servers. Existing servers are not qualified until they are re-discovered

Actions

- Create Adapter Qualifications
- Create Chassis/Server Qualifications
- Create Memory Qualifications
- Create CPU/Cores Qualifications
- Create Storage Qualifications
- Create Server PID Qualifications
- Create Power Group Qualifications
- Create Rack Qualifications

Qualifications

Name	Max	Model	From	To	Archit...	Speed	Stepp...	Power...
Chassis Id range [1 - 100]			1	100				
Server Slot Id range [1 - 1]			1	1				
Server PID Qualification		UCSC-C3X60-M...						

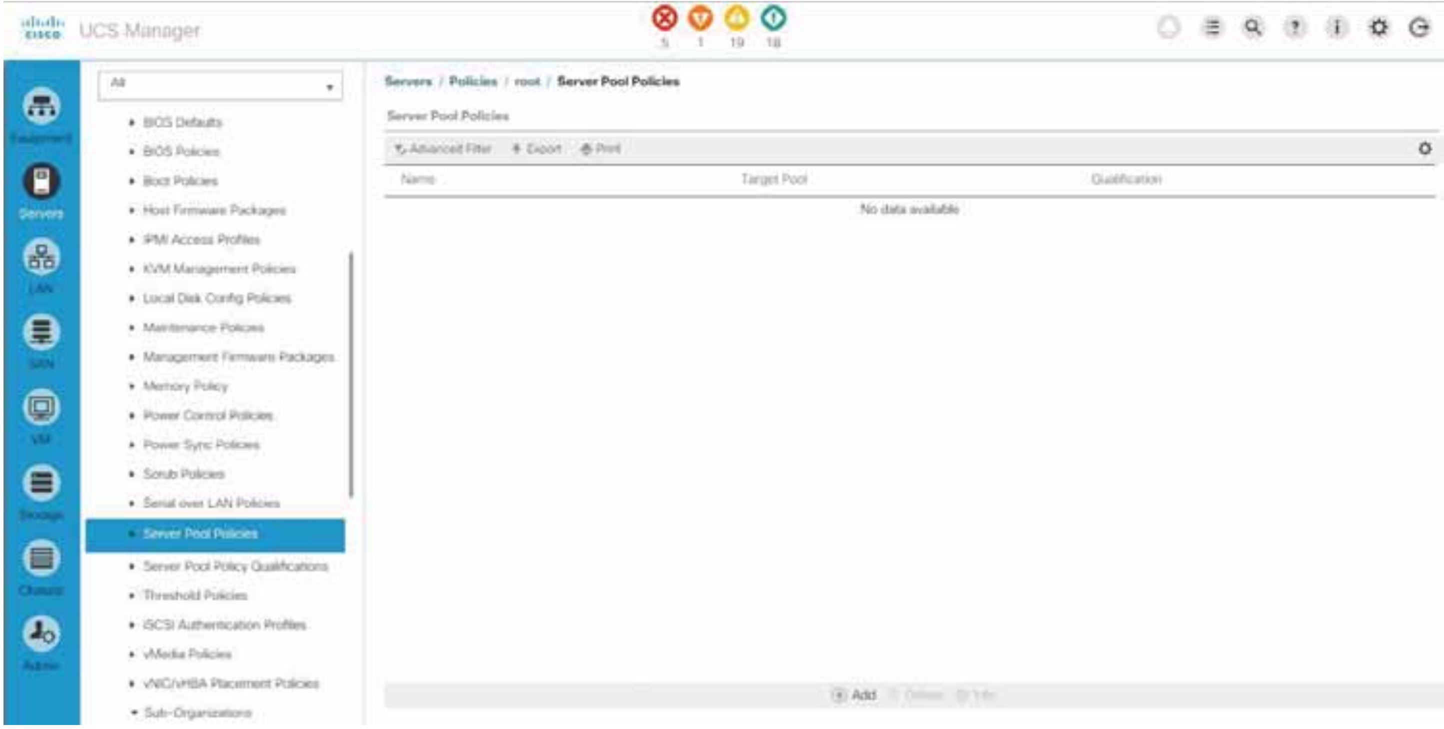


Servers / Policies / root / Sub-Organizations / ScaleProtect / Server Pool Polic...

Server Pool Policy Qualifications

Name	Max	Model	From	To	Speed	Architecture	Stepping
CVLT_SP_S3260_S2							
CVLT_SP_S3260_S1							

Go to Server > Policies > root > Sub-Organizations > ScaleProtect > Server Pool Policies and click Add.



Servers / Policies / root / Server Pool Policies

Server Pool Policies

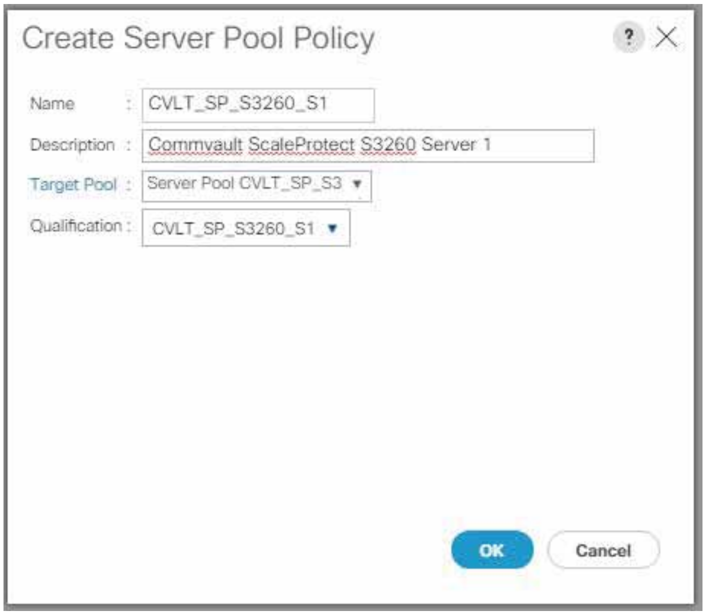
Name	Target Pool	Qualification
No data available		

Enter an obvious name.

Select the target pool for Server 1.

Select the qualification for Server 1.

Click OK.



Create Server Pool Policy

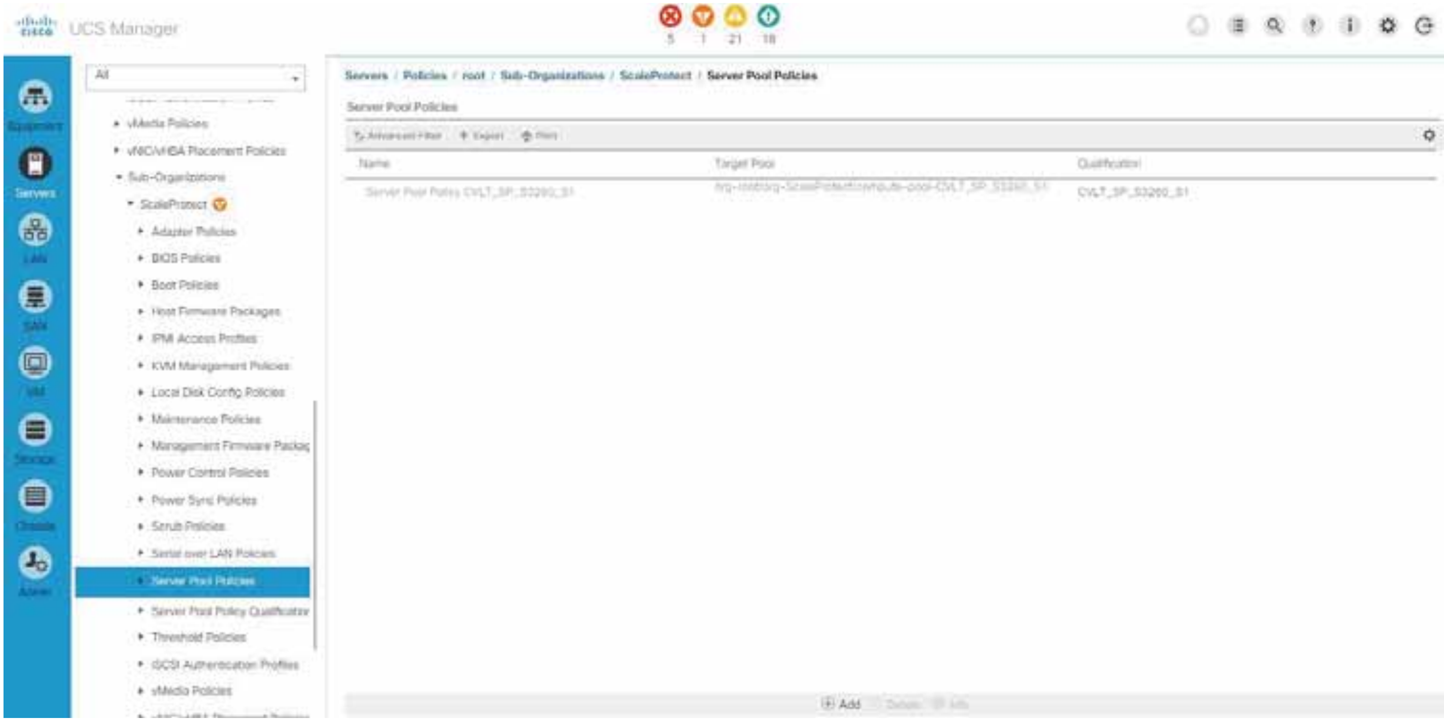
Name : CVLT_SP_S3260_S1

Description : Commvault ScaleProtect S3260 Server 1

Target Pool : Server Pool CVLT_SP_S3

Qualification : CVLT_SP_S3260_S1

Click Add.



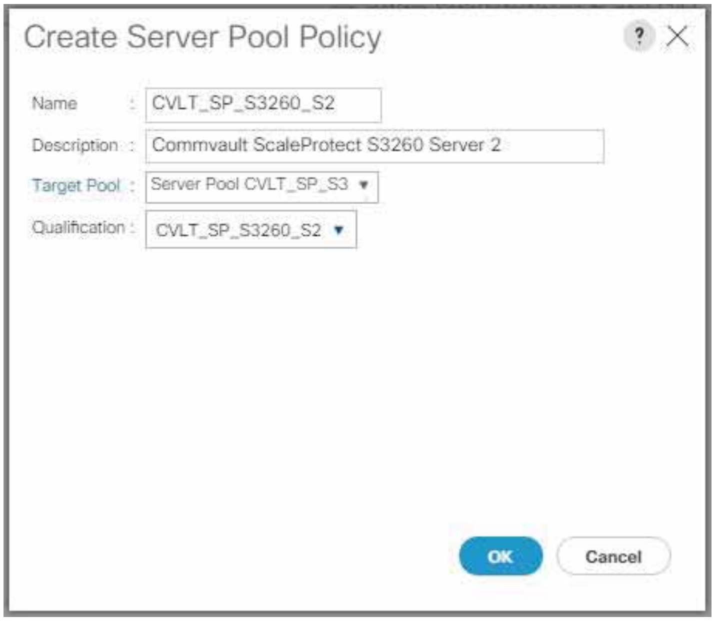
Name	Target Pool	Qualification
Server Pool Policy CVLT_SP_S3260_S1	org-root/org-ScaleProtect/compute-pool-CVLT_SP_S3260_S1	CVLT_SP_S3260_S1

Enter an obvious name.

Select the target pool for Server 2.

Select the qualification for Server 2.

Click OK.



Create Server Pool Policy

Name : CVLT_SP_S3260_S2

Description : Commvault ScaleProtect S3260 Server 2

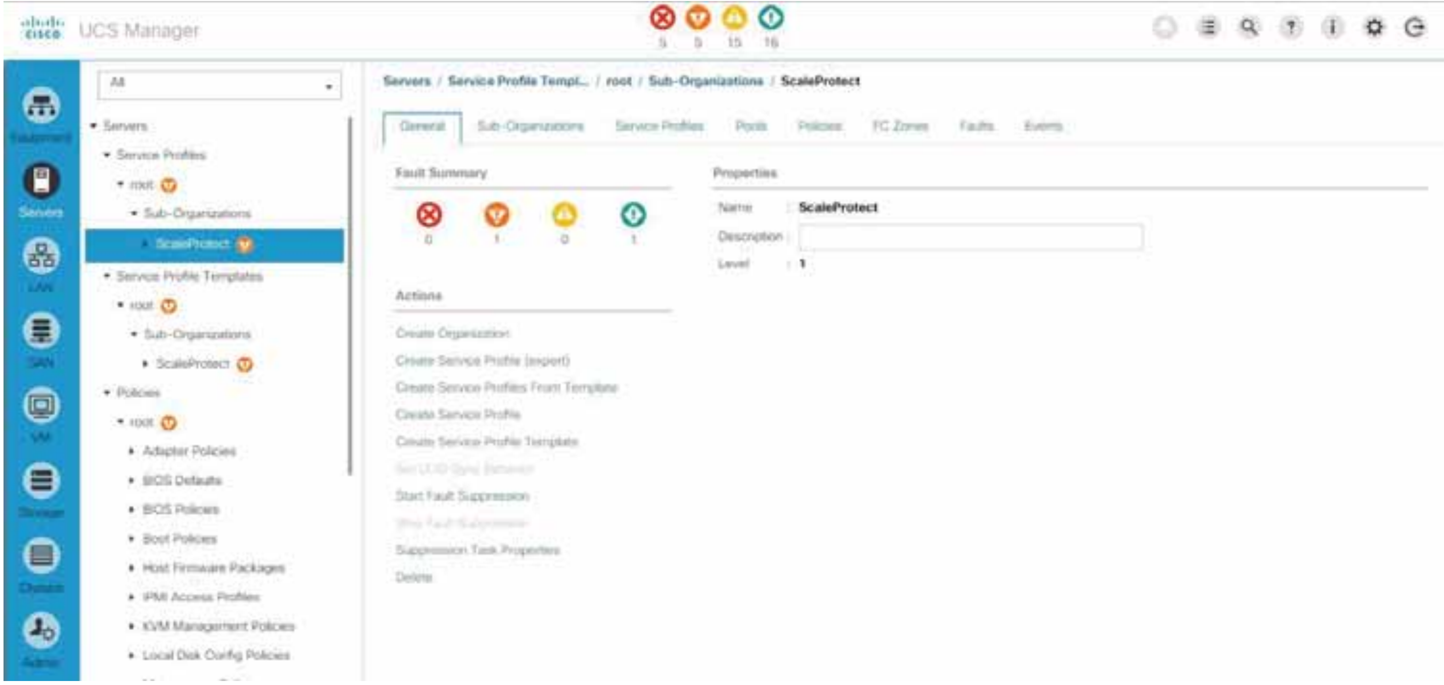
Target Pool : Server Pool CVLT_SP_S3

Qualification : CVLT_SP_S3260_S2

Service profile template configuration

The final configuration task in Cisco UCS Manager is creating the service profiles. Because Commvault ScaleProtect with Cisco UCS is a scale-out architecture using multiple servers, the creation of a service profile template is the best way to start.

Go to Servers > root > Sub-Organizations > ScaleProtect and click Create Service Profile Template.



Servers / Service Profile Templ... / root / Sub-Organizations / ScaleProtect

Name : ScaleProtect

Description :

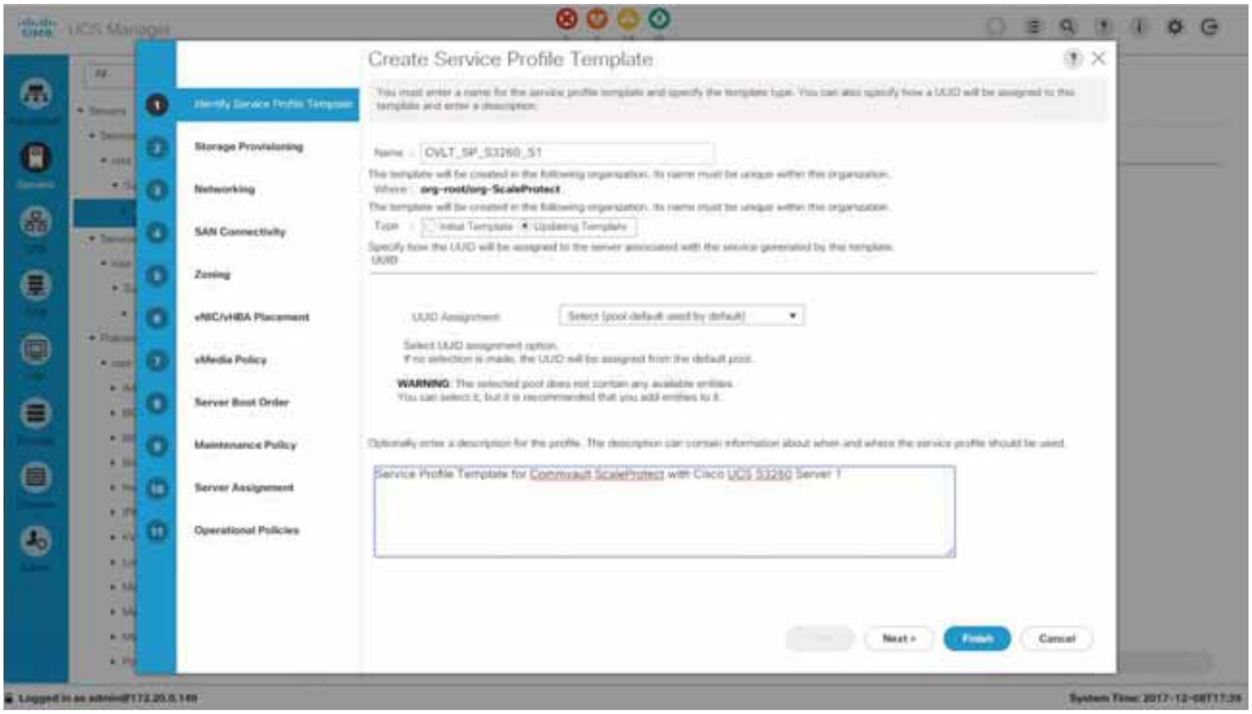
Level : 1

Enter an obvious name.

Select Updating Template.

Select a universally unique ID (UUID) pool with free IDs for UUID assignment.

Click Next.



Create Service Profile Template

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

1 Identify Service Profile Template
2 Storage Provisioning
3 Networking
4 SAN Connectivity
5 Zoning
6 vNIC/vHBA Placement
7 vMedia Policy
8 Server Boot Order
9 Maintenance Policy
10 Server Assignment
11 Operational Policies

Name : CVLT_SP_S3260_S1

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

Where : org-root/org-ScaleProtect

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

Type : ○ Initial Template ● Updating Template

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

UUID

UUID Assignment: Select (pool default used by default)

Select UUID assignment option.
If no selection is made, the UUID will be assigned from the default pool.

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

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

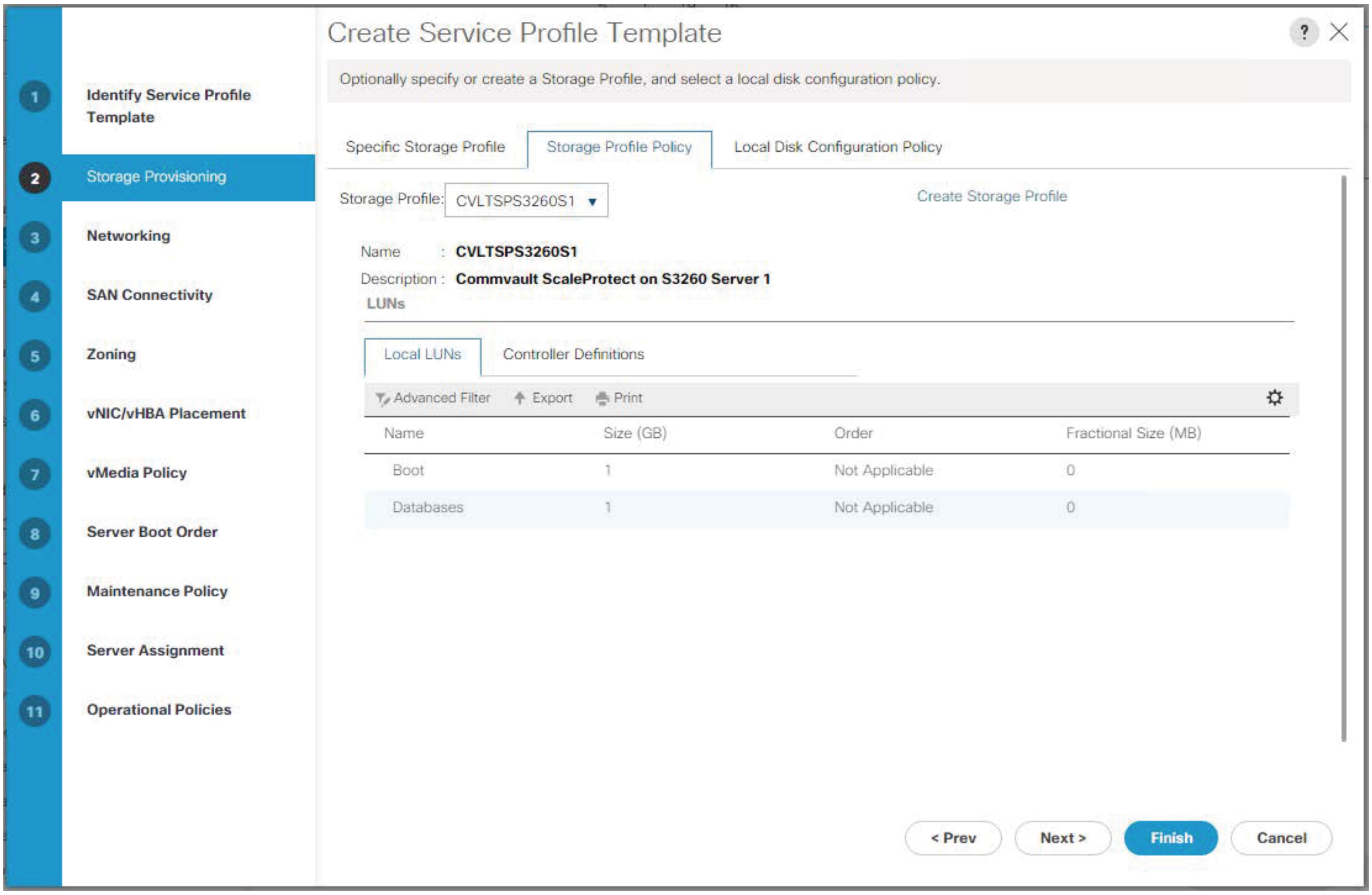
Service Profile Template for Commvault ScaleProtect with Cisco UCS S3260 Server 1

UCS Manager
Next >
Finish
Cancel
Logged in as admin@172.20.5.149
System Time: 2017-12-08T17:28

In the Storage Provisioning section, click the Storage Profile Policy tab.

Select the storage profile that you want (in the example here, CVLTSP3260S1 is used).

Click Next.



Create Service Profile Template

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

Storage Profile: CVLTSPS3260S1

Name : CVLTSPS3260S1

Description : Commvault ScaleProtect on S3260 Server 1

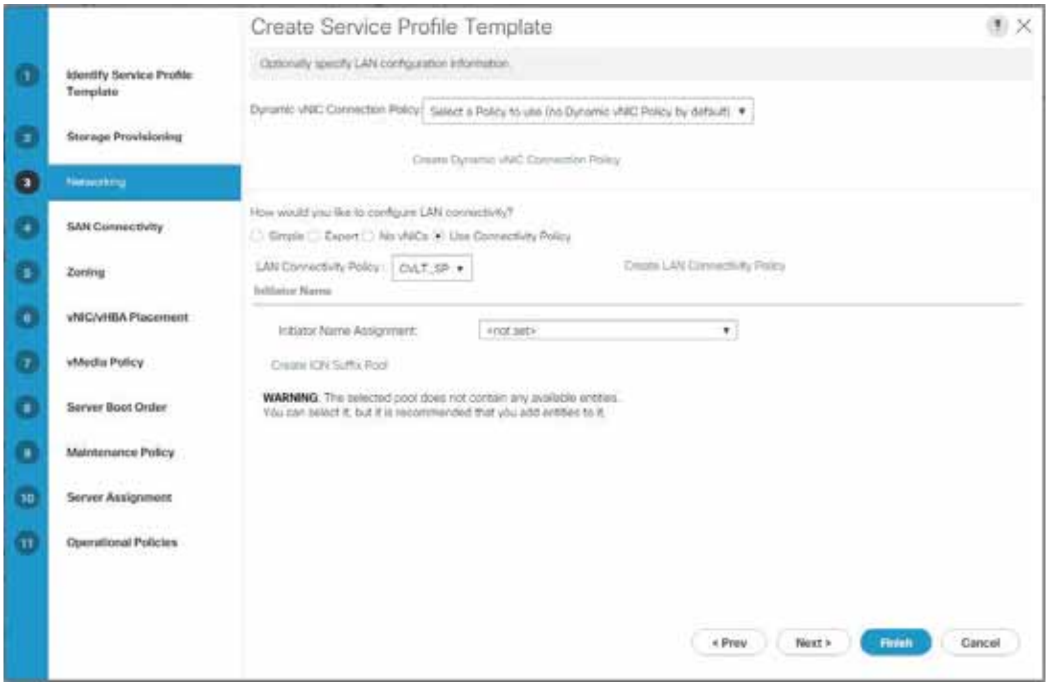
LUNs

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

In the Networking section, select the Use Connectivity Policy button.

Select CVLT_SP as the LAN connectivity policy.

Click Next.



Create Service Profile Template

Optionally specify LAN configuration information.

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

Create Dynamic vNIC Connection Policy

How would you like to configure LAN connectivity?

○ Simple ○ Expert ○ No vNICs ● Use Connectivity Policy

LAN Connectivity Policy : CVLT_SP

Create LAN Connectivity Policy

Initiator Name

Initiator Name Assignment: <not set>

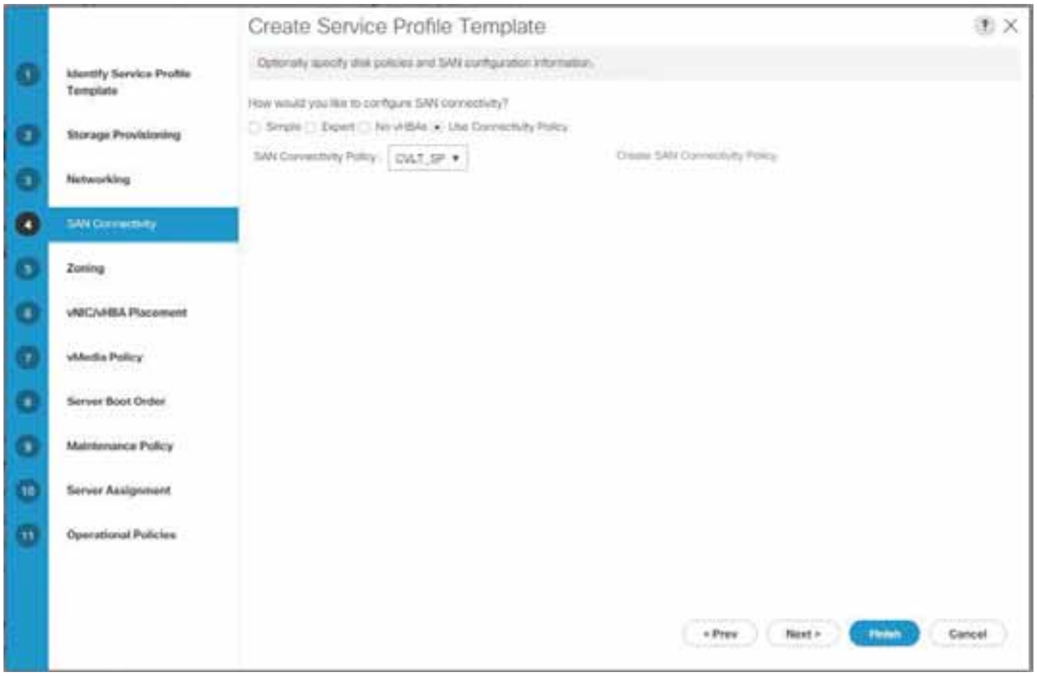
Create IQN Suffix Pool

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

In the SAN connectivity section, select Use Connectivity Policy

Select CVLT_SP as the SAN connectivity policy.

Click Next.



Create Service Profile Template

Optionally specify disk policies and SAN configuration information.

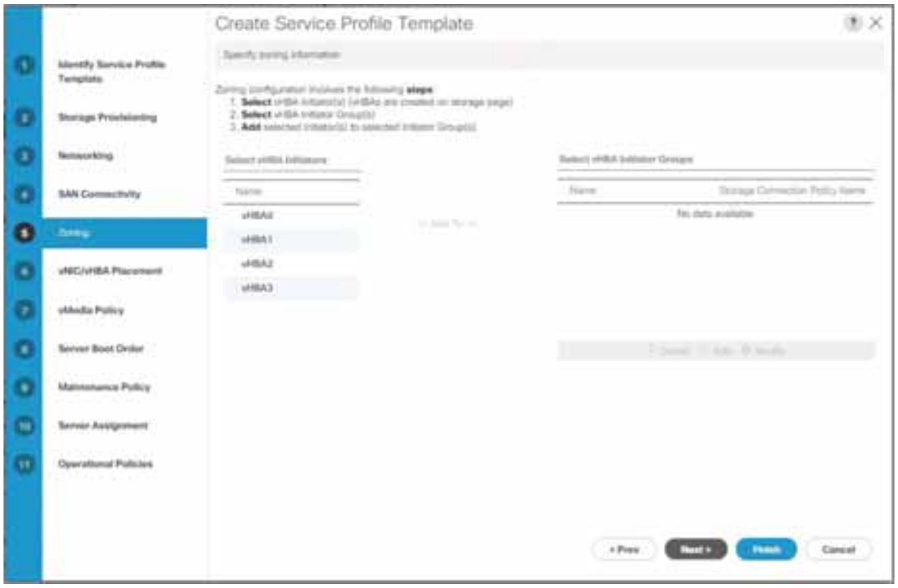
How would you like to configure SAN connectivity?

○ Simple ○ Expert ○ No vHBAs ● Use Connectivity Policy

SAN Connectivity Policy : CVLT_SP

Create SAN Connectivity Policy

In the Zoning section, click Next.



Create Service Profile Template

Specify zoning information

Zoning configuration involves the following **steps**:

1. **Select** vHBA Initiator(s) (vHBAs are created on storage page)
2. **Select** vHBA Initiator Group(s)
3. **Add** selected Initiator(s) to selected Initiator Group(s)

Select vHBA Initiators

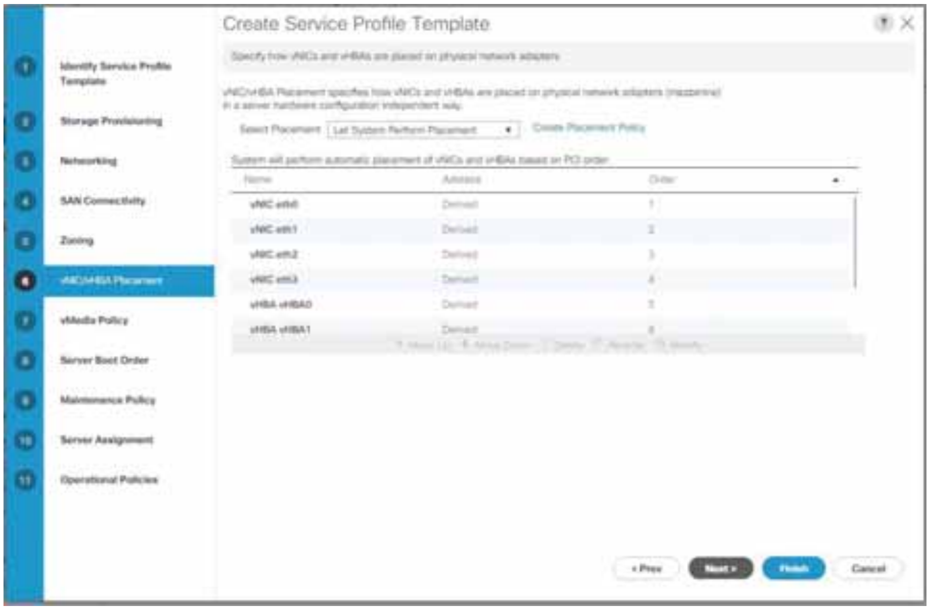
Name
vHBA0
vHBA1
vHBA2
vHBA3

Select vHBA Initiator Groups

Name	Storage Connection Policy Name
No data available	

In the vNIC/vHBA Placement section, leave the setting Let System Perform Placement. With this setting, Cisco UCS will automatically distribute the vNIC and vHBA across both SIOCs if they are available.

Click Next.



Create Service Profile Template

Specify how vNICs and vHBAs are placed on physical network adapters

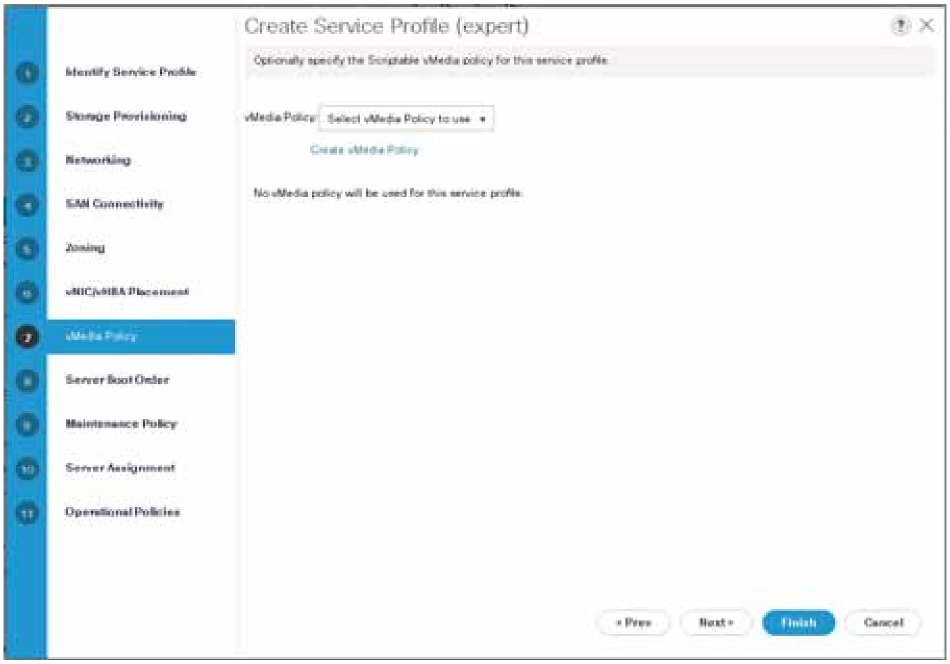
vNIC/vHBA Placement specifies how vNICs and vHBAs are placed on physical network adapters (mezzanine) in a server hardware configuration independent way.

Select Placement: Let System Perform Placement

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

Name	Address	Order
vNIC eth0	Derived	1
vNIC eth1	Derived	2
vNIC eth2	Derived	3
vNIC eth3	Derived	4
vHBA vHBA0	Derived	5
vHBA vHBA1	Derived	6

In the vMedia Policy section, click Next.



Create Service Profile (expert)

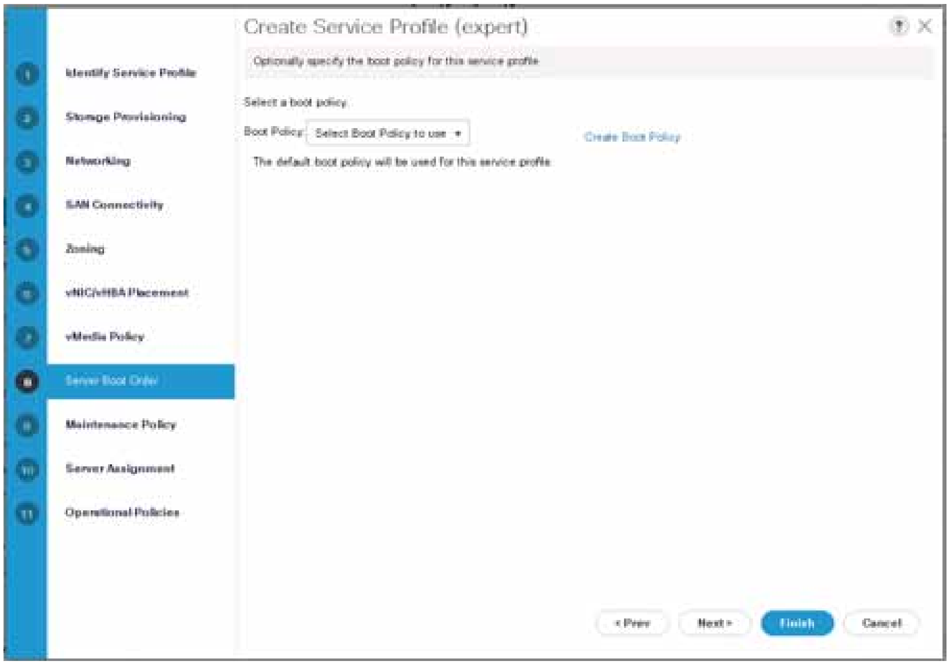
Optionally specify the Scriptable vMedia policy for this service profile.

vMedia Policy: Select vMedia Policy to use ▾

Create vMedia Policy

No vMedia policy will be used for this service profile.

In the Server Boot Order section, click Create Boot Policy.



Create Service Profile (expert)

Optionally specify the boot policy for this service profile

Select a boot policy.

Boot Policy: Select Boot Policy to use ▾

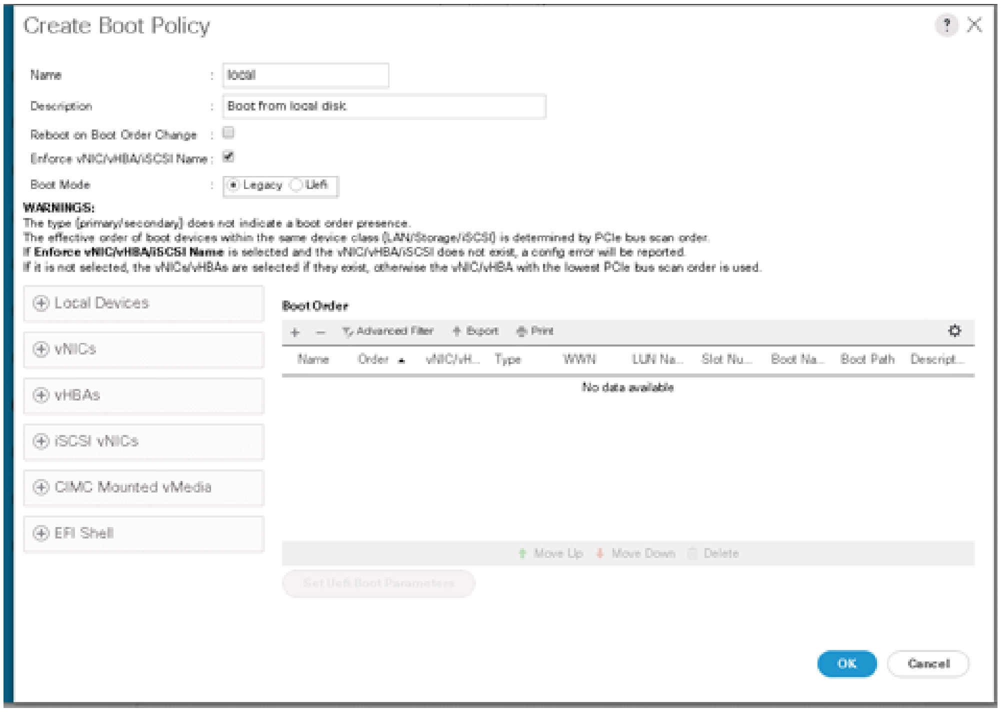
Create Boot Policy

The default boot policy will be used for this service profile.

Enter an obvious name and a description.

Click Local Devices.

Click Add Local LUN.



Create Boot Policy

Name : local

Description : Boot from local disk

Reboot on Boot Order Change : □

Enforce vNIC/vHBA/iSCSI Name : ☑

Boot Mode : ● Legacy ○ Uefi

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

Boot Order

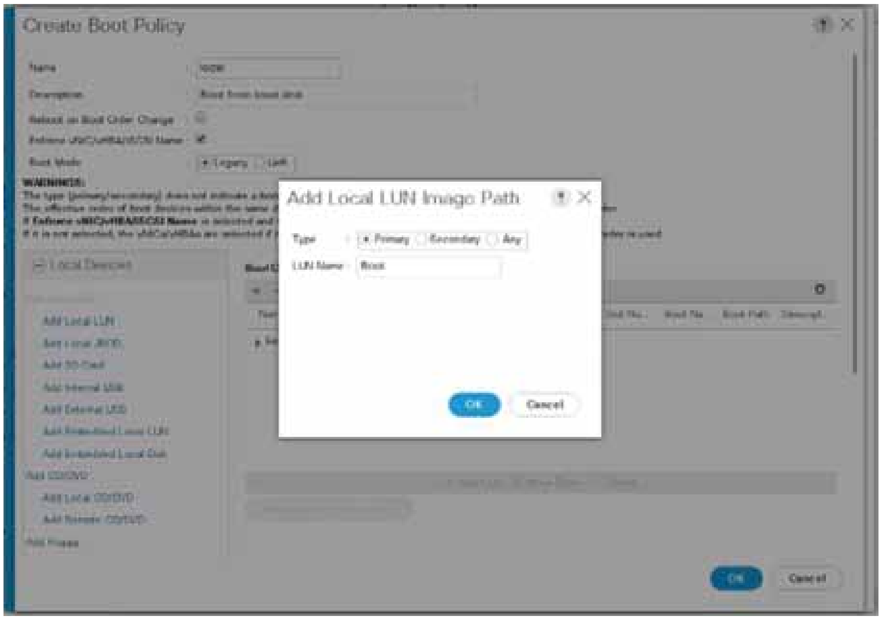
Name	Order ▲	vNIC/vH...	Type	WWN	LUN Na...	Slot Nu...	Boot Na...	Boot Path	Descript...

No data available

Select Primary as the type.

Enter **Boot** as the LUN name. Be aware that you must use the same name as the name for the boot LUN created in the Storage Profile section.

Click OK.



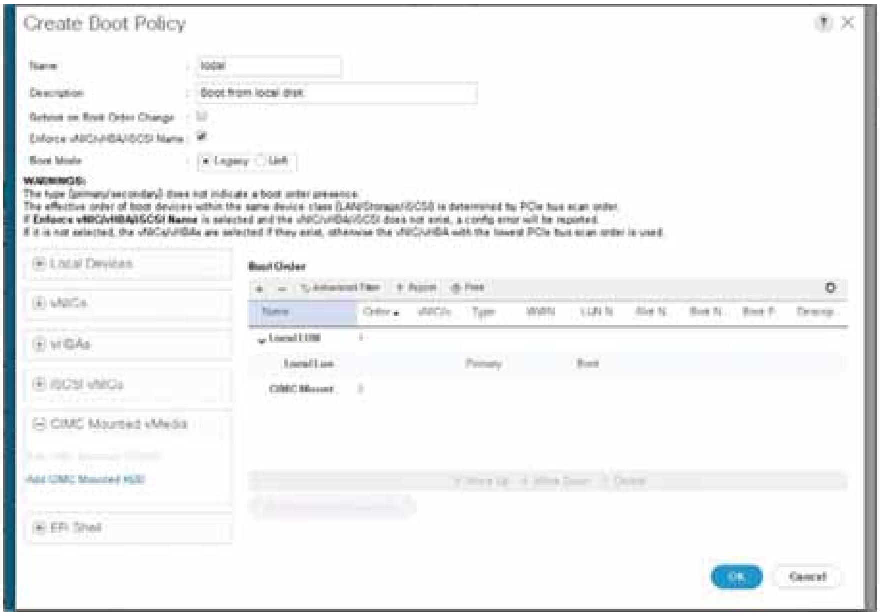
Add Local LUN Image Path

Type : ● Primary ○ Secondary ○ Any

LUN Name : Boot

Click CIMC Mounted Media.

Click Add CIMC Mounted CD/DVD.



Create Boot Policy

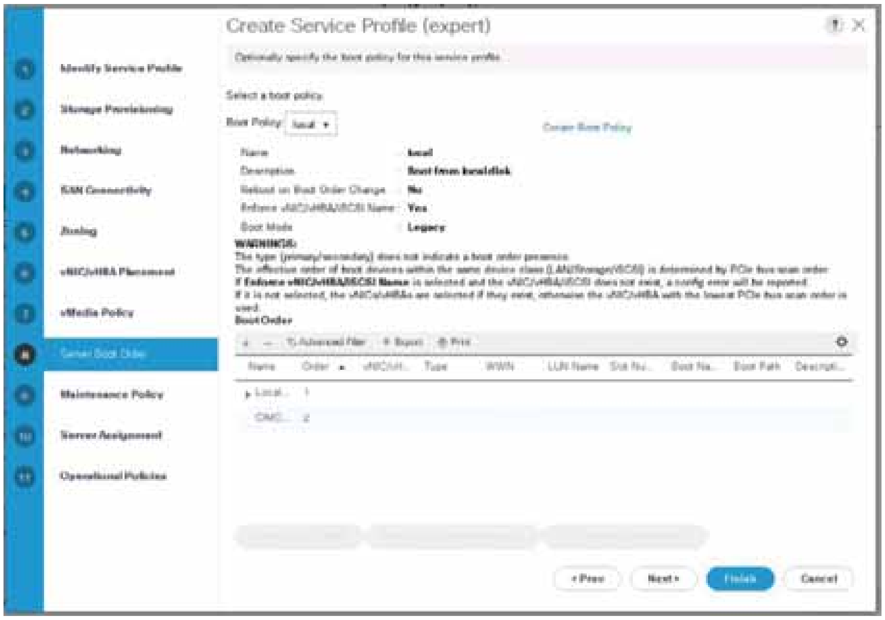
Name: local
Description: Boot from local disk
Reboot on Boot Order Change: ☐
Enforce vNIC/vHBA/iSCSI Name: ☑
Boot Mode: ● Legacy ○ Uefi

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

Boot Order

Name	Order	vNIC/v...	Type	WWN	LUN N...	Slot N...	Boot N...	Boot P...	Descrip...
Local LUN	1								
Local Lun			Primary		Boot				
CIMC Mount	2								

Click Next.



Create Service Profile (expert)

Optionally specify the boot policy for this service profile.

Select a boot policy.

Boot Policy: local

Name: local
Description: Boot from local disk
Reboot on Boot Order Change: No
Enforce vNIC/vHBA/iSCSI Name: Yes
Boot Mode: Legacy

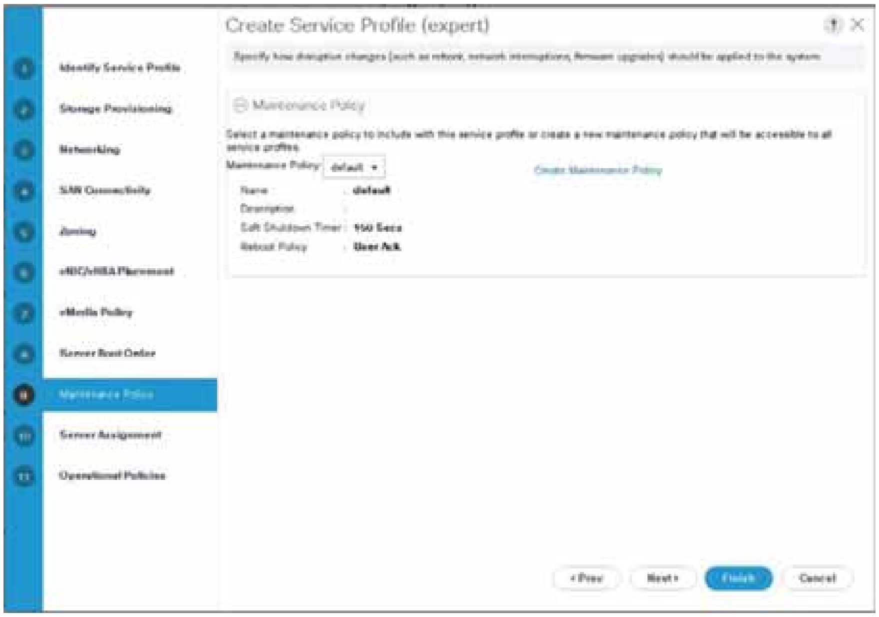
WARNINGS:
The type (primary/secondary) does not indicate a boot order presence.
The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.
If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error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

Boot Order

Name	Order	vNIC/vH...	Type	WWN	LUN Name	Slot Nu...	Boot Na...	Boot Path	Descripti...
Local...	1								
CIMC...	2								

In the Maintenance section, select default for Maintenance Policy.

Click Next.



Create Service Profile (expert)

Specify how disruptive changes (such as reboots, network interruptions, firmware upgrades) should be applied to the system.

⊖ Maintenance Policy

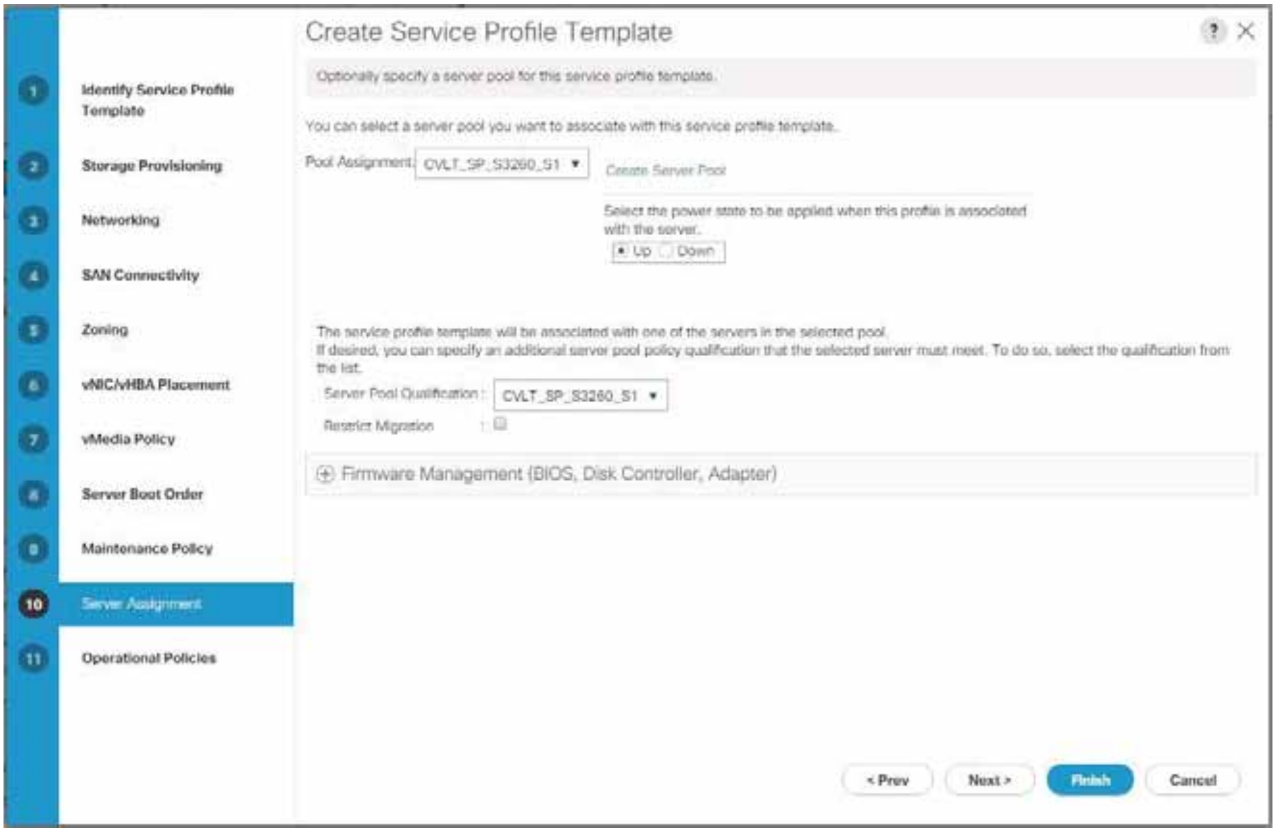
Select a maintenance policy to include with this service profile or create a new maintenance policy that will be accessible to all service profiles.

Maintenance Policy: default ▾

Name	: default
Description	:
Soft Shutdown Timer	: 150 Secs
Reboot Policy	: User Ack

In the Server Assignment section, select the server pool and server pool qualification policy created for Server 1.

Click Next.



Create Service Profile Template

Optionally specify a server pool for this service profile template.

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

Pool Assignment: CVLT_SP_S3260_S1 ▾

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

● Up ○ Down

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

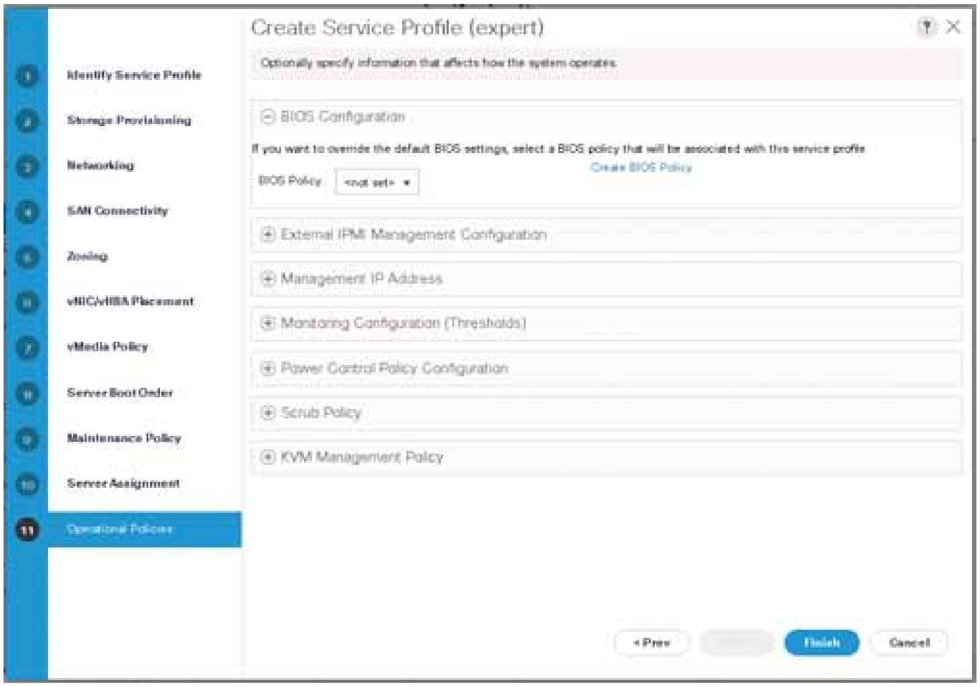
Server Pool Qualification : CVLT_SP_S3260_S1 ▾

Restrict Migration : □

In the Operational Policies section, select the policies required for your installation.

ScaleProtect does not require you to select any particular options.

Click Finish.



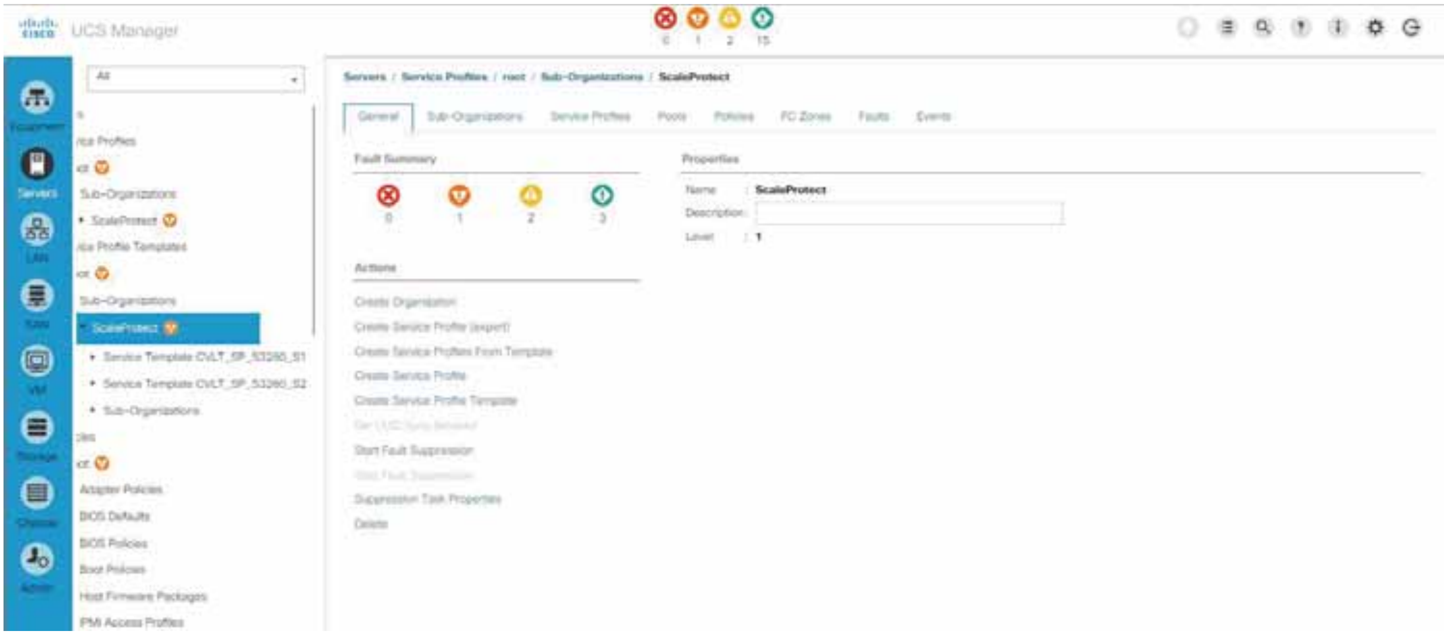
Create Service Profile (expert)

Optionally specify information that affects how the system operates.

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

BIOS Policy: <not set>

Repeat the service profile template creation for Server 2 in the Cisco UCS S3260.



Servers / Service Profiles / root / Sub-Organizations / ScaleProtect

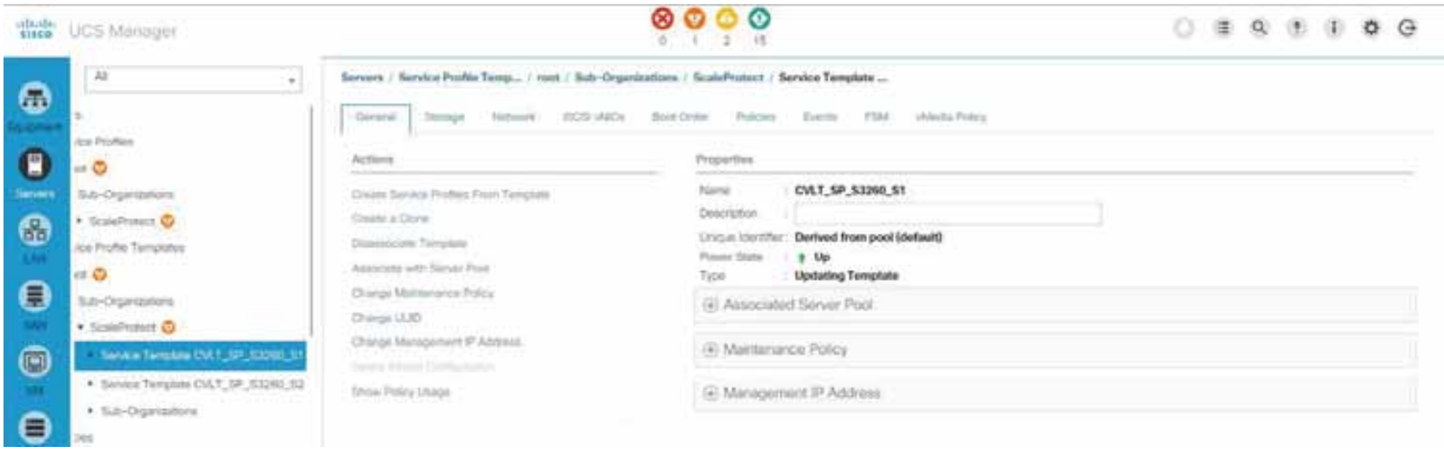
Name : ScaleProtect

Description :

Level : 1

Click one of the service profile templates.

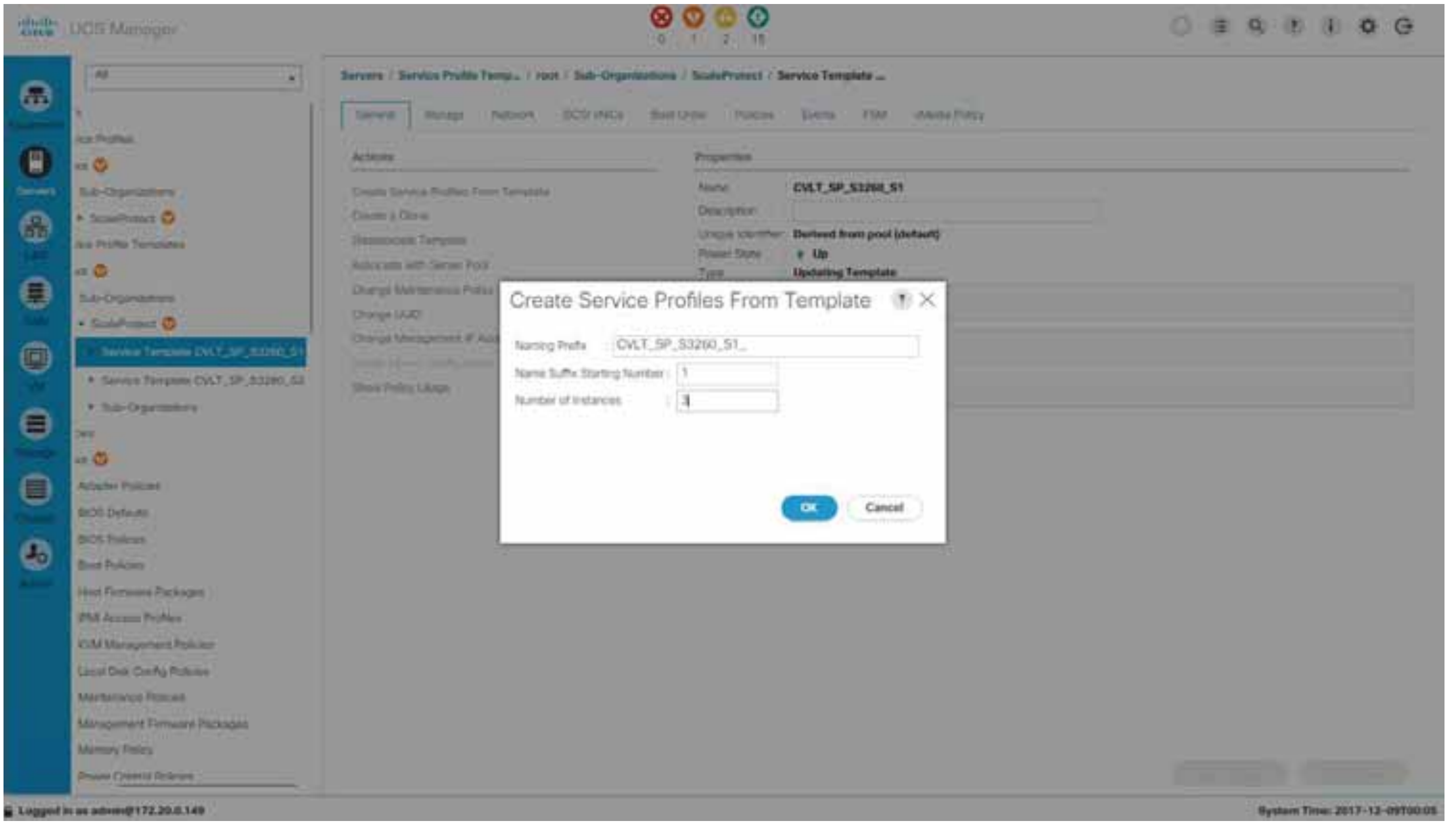
Click Create Service Profiles from Template.


UCS Manager
Servers / Service Profile Temp... / root / Sub-Organizations / ScaleProtect / Service Template ...
General
Storage
Network
iSCSI vNICs
Boot Order
Policies
Events
FSM
vMedia Policy
Actions
Create Service Profiles From Template
Create a Clone
Disassociate Template
Associate with Server Pool
Change Maintenance Policy
Change UUID
Change Management IP Address
Show Policy Usage
Properties
Associated Server Pool
Maintenance Policy
Management IP Address
Service Template CVLT_SP_S3260_S1
Service Template CVLT_SP_S3260_S2
Sub-Organizations
ScaleProtect

Name : CVLT_SP_S3260_S1
Description :
Unique Identifier: Derived from pool (default)
Power State : Up
Type : Updating Template

Enter a naming prefix and the number of instances to create.

Click OK.



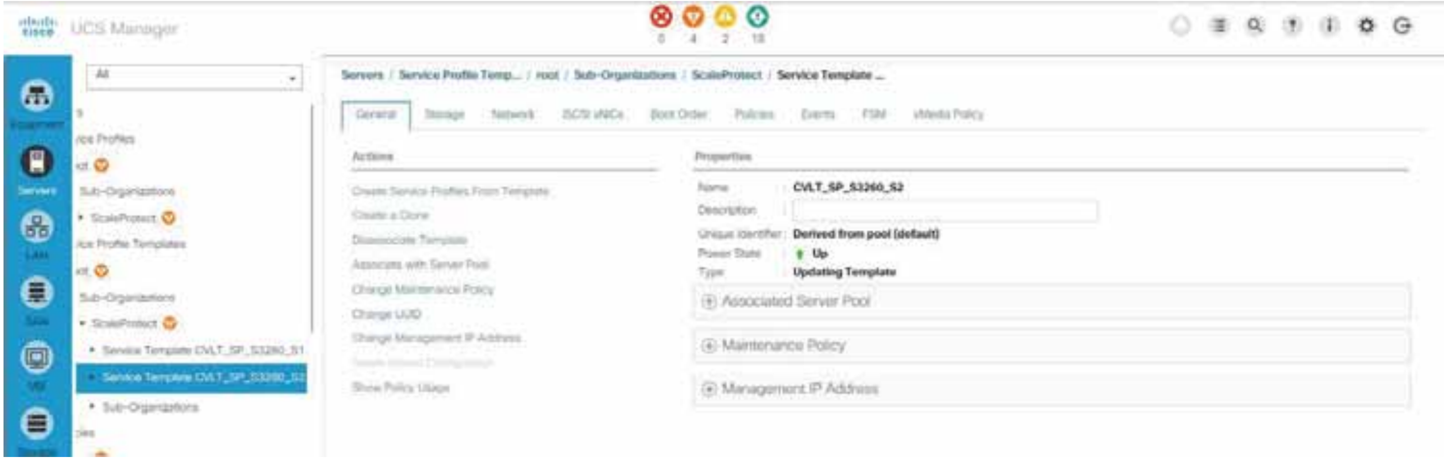
Naming Prefix : CVLT_SP_S3260_S1_
Name Suffix Starting Number : 1
Number of Instances : 3

Logged in as admin@172.20.0.149

System Time: 2017-12-09T00:05

Select the other service profile template.

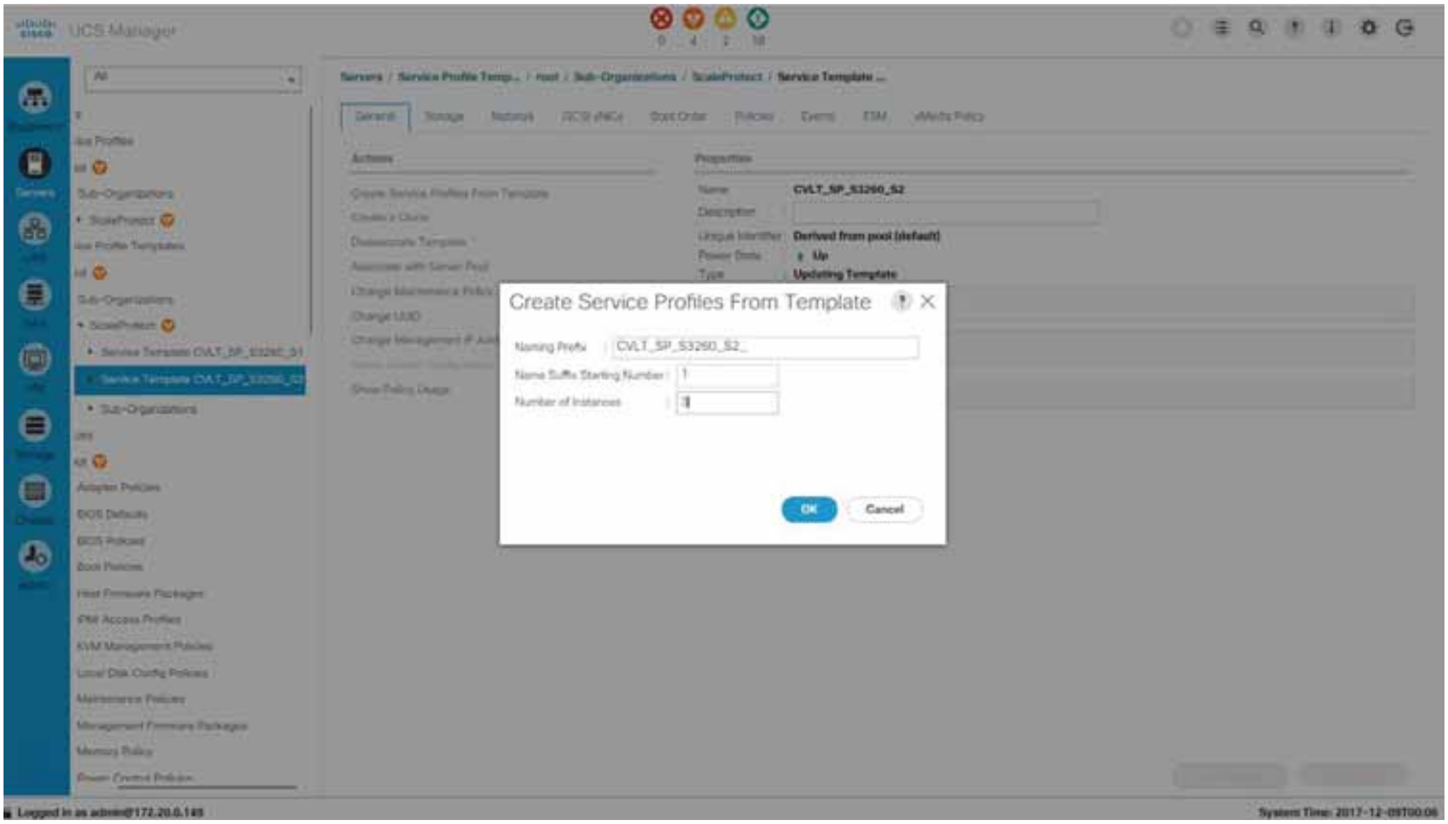
Click Create Service Profiles from Template.


UCS Manager
Servers / Service Profile Temp... / root / Sub-Organizations / ScaleProtect / Service Template ...
General
Storage
Network
iSCSI vNICs
Boot Order
Policies
Events
FSM
vMedia Policy
Actions
Create Service Profiles From Template
Create a Clone
Disassociate Template
Associate with Server Pool
Change Maintenance Policy
Change UUID
Change Management IP Address
Show Policy Usage
Properties
Associated Server Pool
Maintenance Policy
Management IP Address
Service Template CVLT_SP_S3260_S1
Service Template CVLT_SP_S3260_S2
Sub-Organizations

Name : CVLT_SP_S3260_S2
Description :
Unique Identifier : Derived from pool (default)
Power State : Up
Type : Updating Template

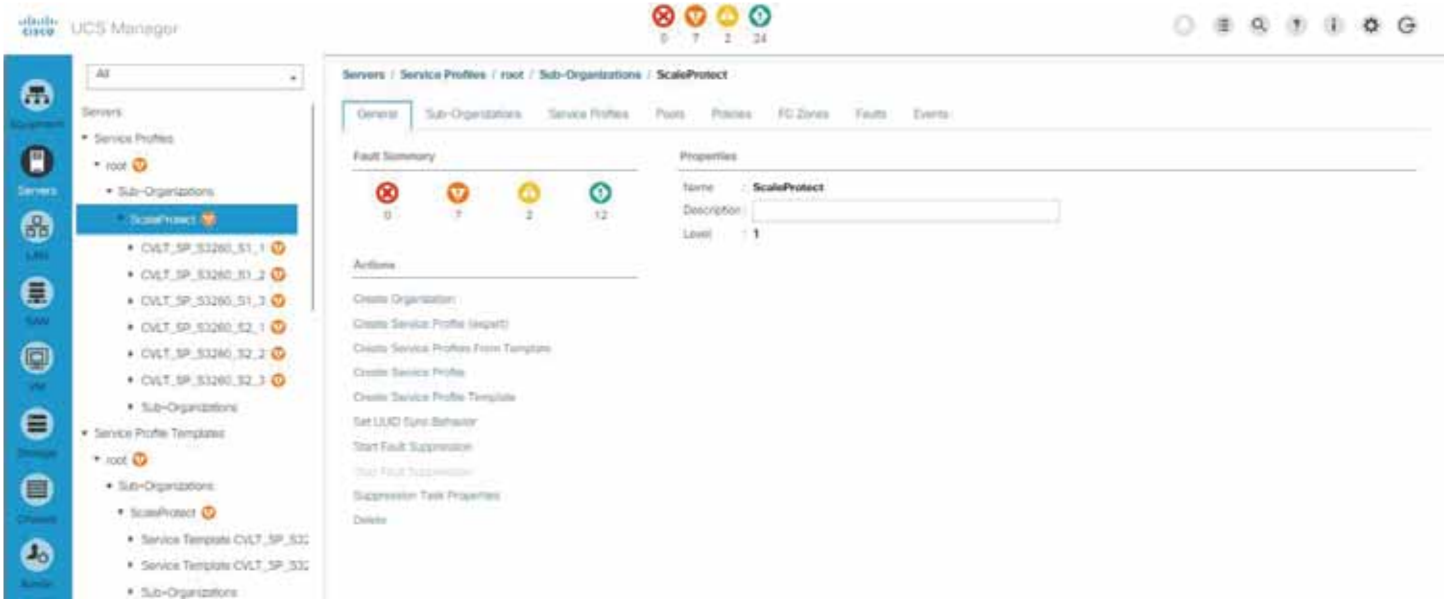
Enter a naming prefix and the number of instances to create.

Click OK.


UCS Manager
Create Service Profiles From Template
OK
Cancel
Logged in as admin@172.20.0.149
System Time: 2017-12-09T00:06

Naming Prefix : CVLT_SP_S3260_S2_
Name Suffix Starting Number : 1
Number of Instances : 3

Check the result in the Service Profiles section.



Name : ScaleProtect
Description :
Level : 1

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.

Commvault HyperScale installation

Now install HyperScale.

CommServe

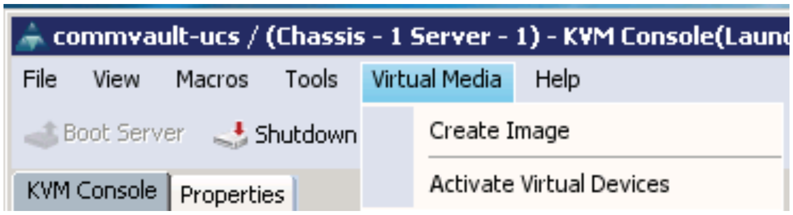
This procedure assumes the physical server or virtual machine hosting the CommServe server already has the CommServe software installed.

ScaleProtect

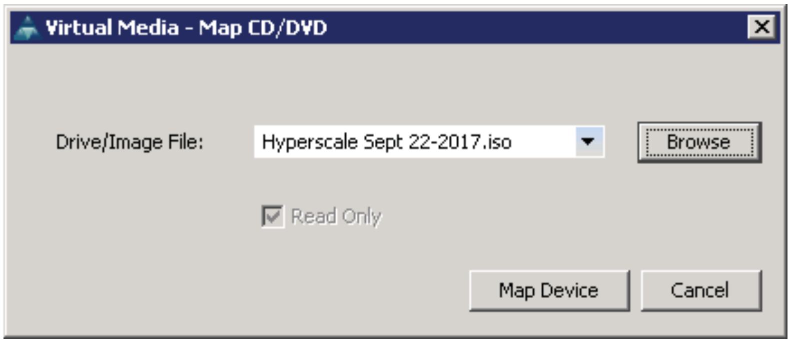
This following procedures are for installation for the Commvault ScaleProtect Software on the Cisco UCS S3260 Storage Server.

If you are using Cisco UCS Manager, log in to Cisco UCS and launch the Kernel-based Virtual Machine (KVM) manager from there to connect to the nodes. If you are not using Cisco UCS Manager, log in to the IMC for the node and launch the KVM from there for each node. Verify that you have the latest copy of the Commvault HyperScale ISO image downloaded from cloud.commvault.com.

Attach the ISO image to the server node using the KVM. Open the Virtual Media menu and choose Activate Virtual Devices.



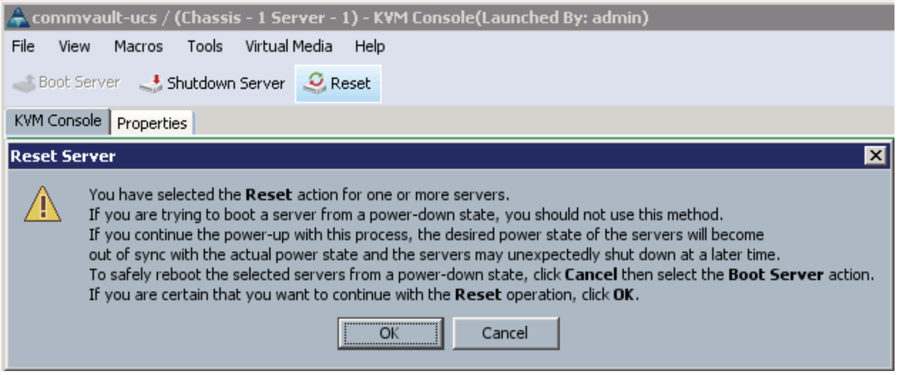
Again open the Virtual Media menu. Now choose Map CD/DVD and browse to the location of the ISO image. Then click Map Device.



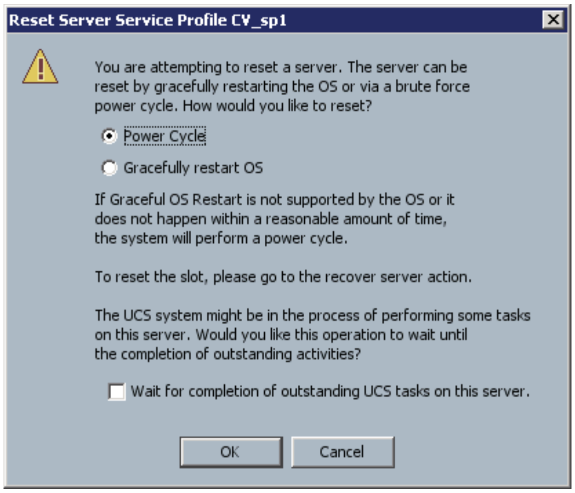
Drive/Image File: Hyperscale Sept 22-2017.iso

☑ Read Only

Click Reset on the menu at the top of the window and then click OK. On the next screen, select Power Cycle to reboot and reset the server.



You have selected the **Reset** action for one or more servers.
If you are trying to boot a server from a power-down state, you should not use this method.
If you continue the power-up with this process, the desired power state of the servers will become
out of sync with the actual power state and the servers may unexpectedly shut down at a later time.
To safely reboot the selected servers from a power-down state, click **Cancel** then select the **Boot Server** action.
If you are certain that you want to continue with the **Reset** operation, click **OK**.



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

● Power Cycle

○ Gracefully restart OS

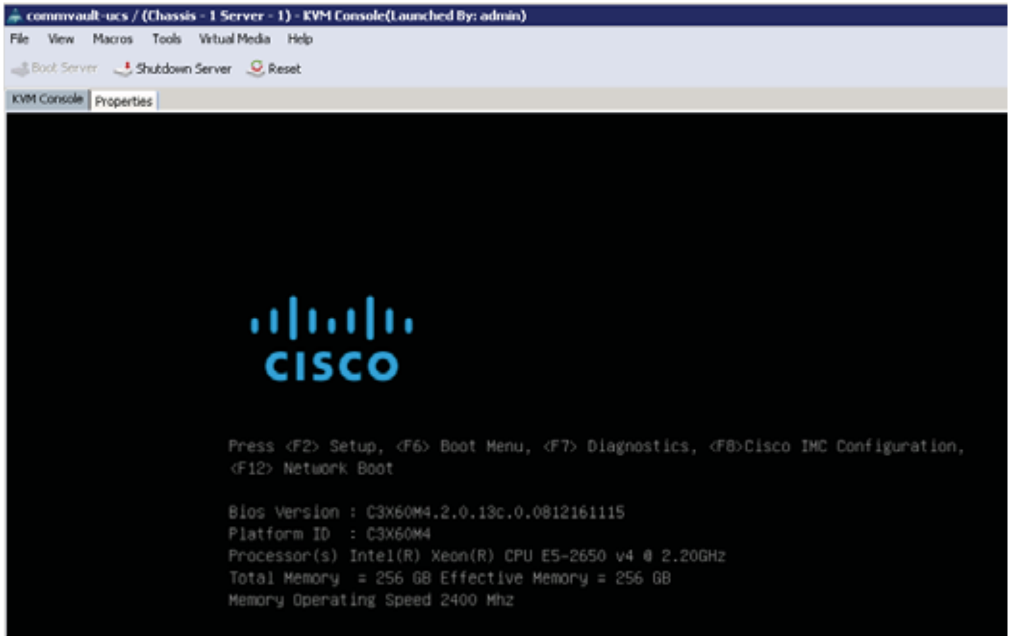
If Graceful OS Restart is not supported by the OS or it does not happen within a reasonable amount of time, the system will perform a power cycle.

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

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

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

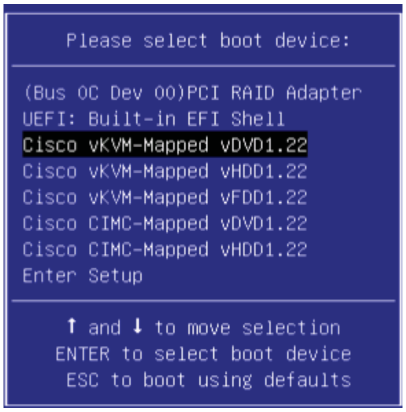
As the server is coming up, at the main screen press F6 to enter the boot menu.



commvault-ucs / (Chassis - 1 Server - 1) - KVM Console(Launched By: admin)
File View Macros Tools Virtual Media Help
Boot Server Shutdown Server Reset
KVM Console Properties

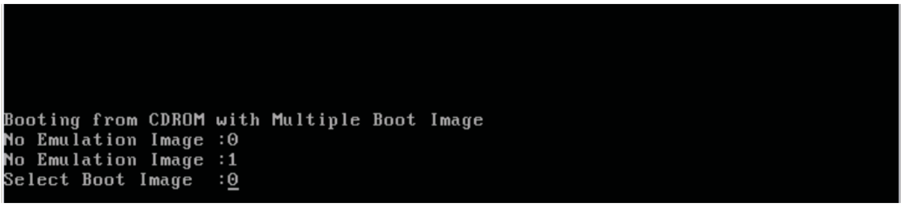
```
Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8>Cisco IMC Configuration,
<F12> Network Boot

Bios Version : C3X60M4.2.0.13c.0.0812161115
Platform ID  : C3X60M4
Processor(s) Intel(R) Xeon(R) CPU E5-2650 v4 @ 2.20GHz
Total Memory  = 256 GB Effective Memory = 256 GB
Memory Operating Speed 2400 Mhz
```

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



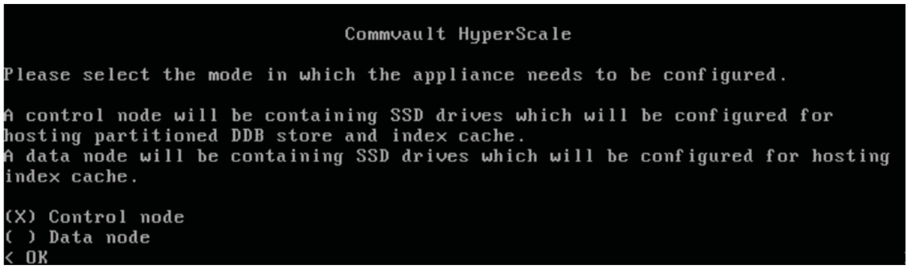
```
  Please select boot device:

(Bus 0C Dev 00)PCI RAID Adapter
UEFI: Built-in EFI Shell
Cisco vKVM-Mapped vDVD1.22
Cisco vKVM-Mapped vHDD1.22
Cisco vKVM-Mapped vFDD1.22
Cisco CIMC-Mapped vDVD1.22
Cisco CIMC-Mapped vHDD1.22
Enter Setup

  ↑ and ↓ to move selection
 ENTER to select boot device
  ESC to boot using defaults
```

After the ISO image loads, you will be asked which image to boot from. Select the default image: 0.



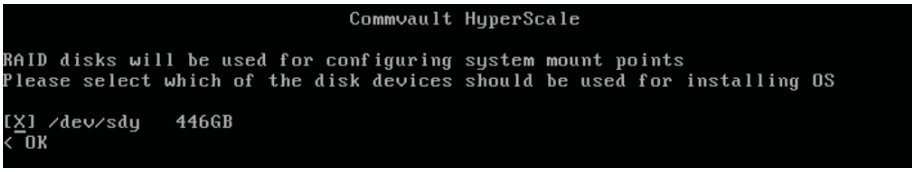
```
Booting from CDROM with Multiple Boot Image
No Emulation Image :0
No Emulation Image :1
Select Boot Image  :0
```

When you install HyperScale you have two options: Control node and Data node. The Control node has a database for deduplication and a disk for data, and the Data node just has the disk used for backup. In a three-node or six-node block, during the initial setup all three or six nodes should be control nodes. Click OK to continue with the default Control node for installation.



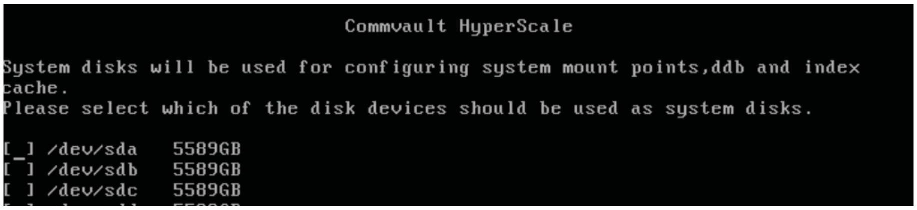
```
                              Commvault HyperScale

Please select the mode in which the appliance needs to be configured.

A control node will be containing SSD drives which will be configured for
hosting partitioned DDB store and index cache.
A data node will be containing SSD drives which will be configured for hosting
index cache.

(X) Control node
( ) Data node
< OK
```

Select the RAID1 disk created for the boot drive.

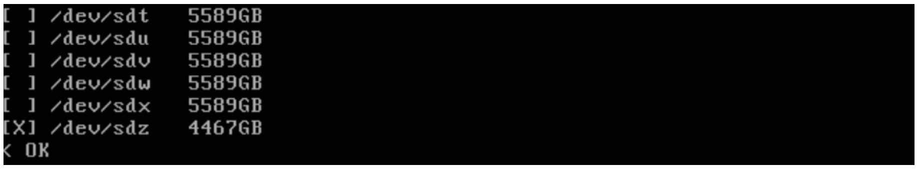


```
                              Commvault HyperScale

RAID disks will be used for configuring system mount points
Please select which of the disk devices should be used for installing OS

[X] /dev/sdy   446GB
< OK
```

Select the RAID 5 disk that will be used for the DDB and the index cache. You may need to scroll down the list to find it if the server contains a lot of disks.

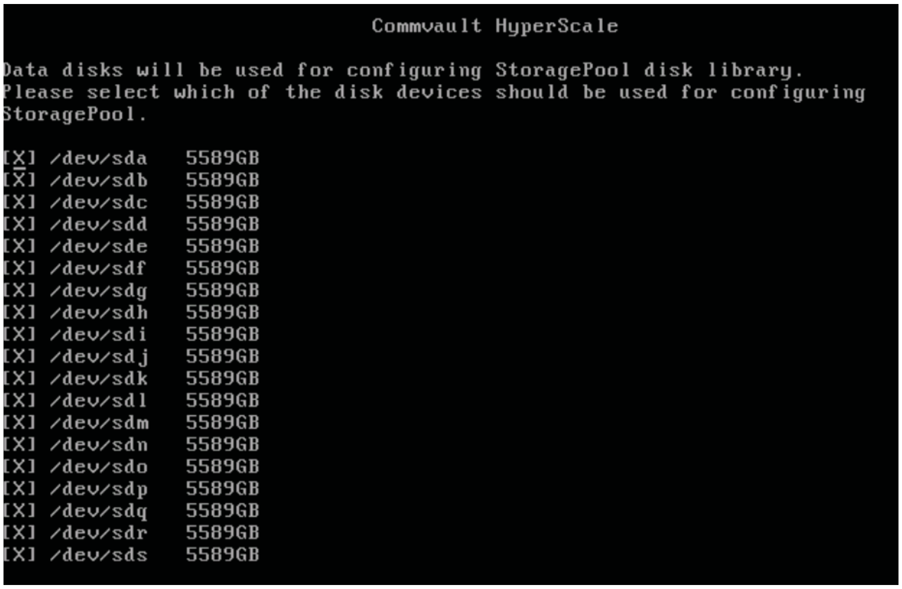


```
                              Commvault HyperScale

System disks will be used for configuring system mount points,ddb and index
cache.
Please select which of the disk devices should be used as system disks.

[_] /dev/sda   5589GB
[ ] /dev/sdb   5589GB
[ ] /dev/sdc   5589GB
```

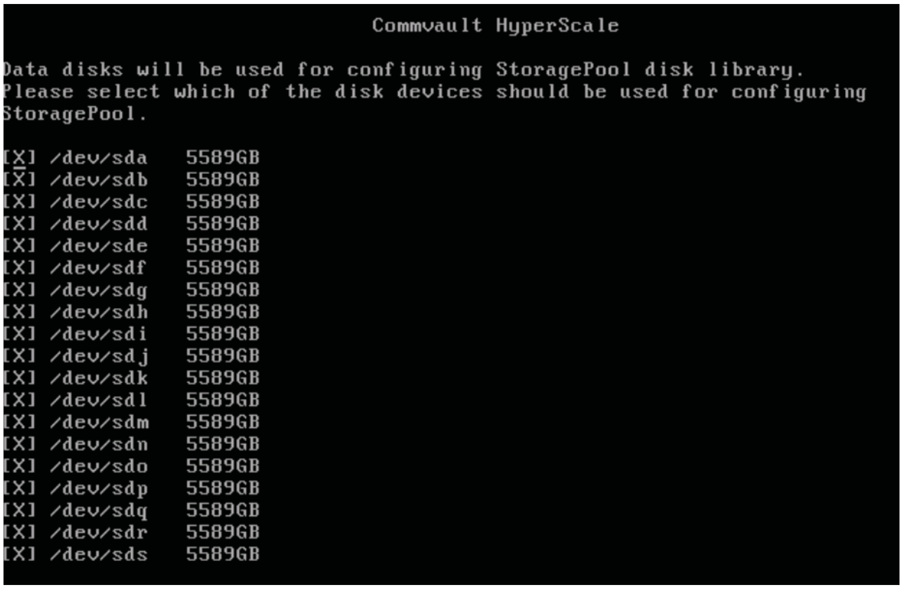


```
[ ] /dev/sdt   5589GB
[ ] /dev/sdu   5589GB
[ ] /dev/sdv   5589GB
[ ] /dev/sdw   5589GB
[ ] /dev/sdx   5589GB
[X] /dev/sdz   4467GB
< OK
```

Lastly, the remaining data disks should be selected to be used for the storage, select OK to continue.

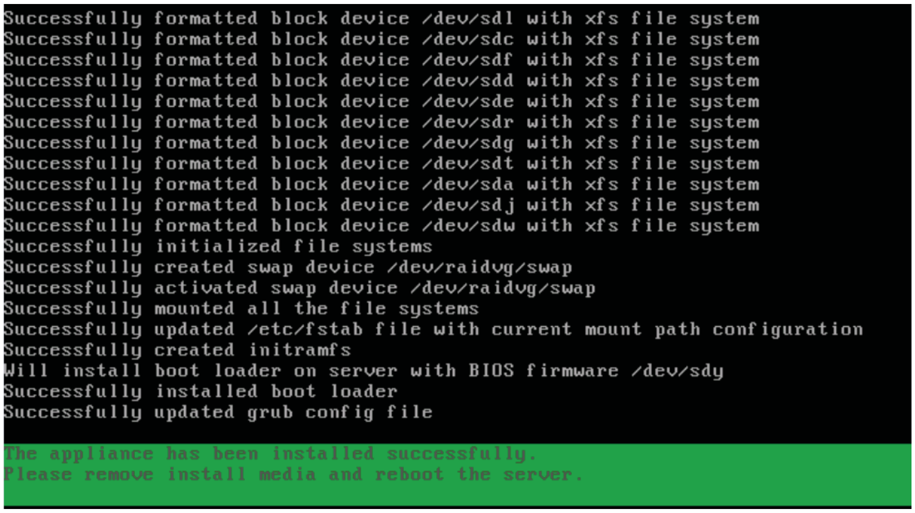


```
                         Commvault HyperScale

Data disks will be used for configuring StoragePool disk library.
Please select which of the disk devices should be used for configuring
StoragePool.

[X] /dev/sda   5589GB
[X] /dev/sdb   5589GB
[X] /dev/sdc   5589GB
[X] /dev/sdd   5589GB
[X] /dev/sde   5589GB
[X] /dev/sdf   5589GB
[X] /dev/sdg   5589GB
[X] /dev/sdh   5589GB
[X] /dev/sdi   5589GB
[X] /dev/sdj   5589GB
[X] /dev/sdk   5589GB
[X] /dev/sdl   5589GB
[X] /dev/sdm   5589GB
[X] /dev/sdn   5589GB
[X] /dev/sdo   5589GB
[X] /dev/sdp   5589GB
[X] /dev/sdq   5589GB
[X] /dev/sdr   5589GB
[X] /dev/sds   5589GB
```



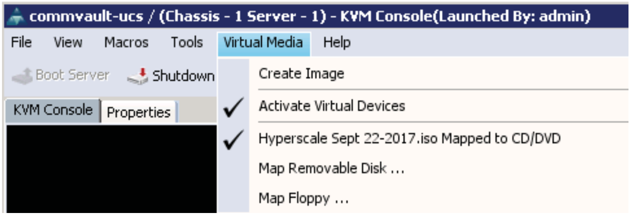
```
                         Commvault HyperScale

Data disks will be used for configuring StoragePool disk library.
Please select which of the disk devices should be used for configuring
StoragePool.

[X] /dev/sda   5589GB
[X] /dev/sdb   5589GB
[X] /dev/sdc   5589GB
[X] /dev/sdd   5589GB
[X] /dev/sde   5589GB
[X] /dev/sdf   5589GB
[X] /dev/sdg   5589GB
[X] /dev/sdh   5589GB
[X] /dev/sdi   5589GB
[X] /dev/sdj   5589GB
[X] /dev/sdk   5589GB
[X] /dev/sdl   5589GB
[X] /dev/sdm   5589GB
[X] /dev/sdn   5589GB
[X] /dev/sdo   5589GB
[X] /dev/sdp   5589GB
[X] /dev/sdq   5589GB
[X] /dev/sdr   5589GB
[X] /dev/sds   5589GB
```

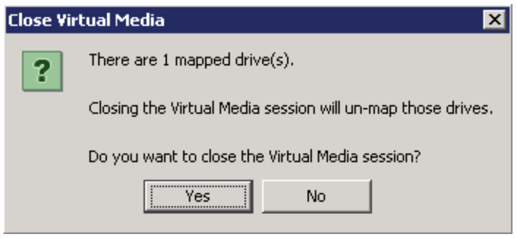
The system will now format and set up the volumes and mount them. This process will take several minutes to complete. When the process is complete, remove the installation DVD and reboot the server.



```
Successfully formatted block device /dev/sdl with xfs file system
Successfully formatted block device /dev/sdc with xfs file system
Successfully formatted block device /dev/sdf with xfs file system
Successfully formatted block device /dev/sdd with xfs file system
Successfully formatted block device /dev/sde with xfs file system
Successfully formatted block device /dev/sdr with xfs file system
Successfully formatted block device /dev/sdg with xfs file system
Successfully formatted block device /dev/sdt with xfs file system
Successfully formatted block device /dev/sda with xfs file system
Successfully formatted block device /dev/sdj with xfs file system
Successfully formatted block device /dev/sdw with xfs file system
Successfully initialized file systems
Successfully created swap device /dev/raidvg/swap
Successfully activated swap device /dev/raidvg/swap
Successfully mounted all the file systems
Successfully updated /etc/fstab file with current mount path configuration
Successfully created initramfs
Will install boot loader on server with BIOS firmware /dev/sdy
Successfully installed boot loader
Successfully updated grub config file

The appliance has been installed successfully.
Please remove install media and reboot the server.
```

To remove the installation media, click the Virtual Media menu at the top of the screen and unselect Activate Virtual Devices. Then click OK to unmap the ISO image. Click the Reset button again at the top of the screen to reboot and reset the server and then click OK. Select Power Cycle and click OK.


commvault-ucs / (Chassis - 1 Server - 1) - KVM Console(Launched By: admin)
File
View
Macros
Tools
Virtual Media
Help
Boot Server
Shutdown
KVM Console
Properties
Create Image
✓ Activate Virtual Devices
✓ Hyperscale Sept 22-2017.iso Mapped to CD/DVD
Map Removable Disk ...
Map Floppy ...



Close Virtual Media

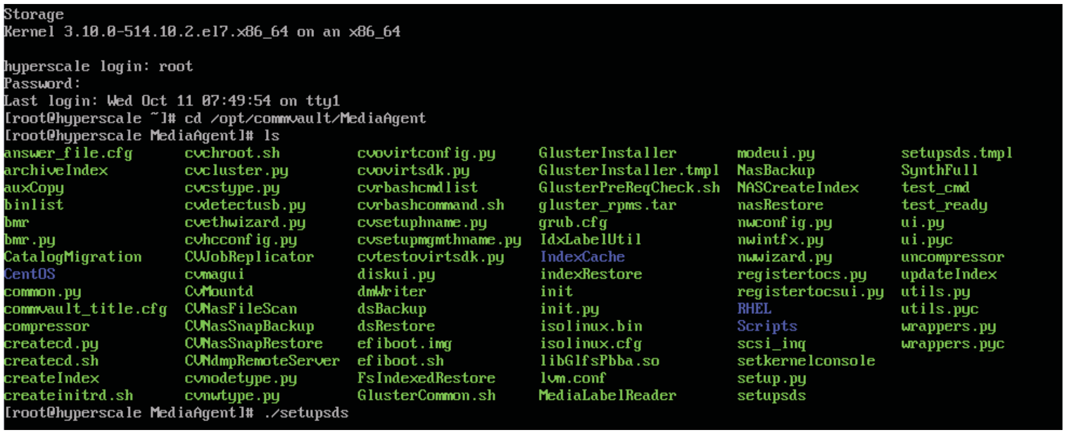
There are 1 mapped drive(s).

Closing the Virtual Media session will un-map those drives.

Do you want to close the Virtual Media session?

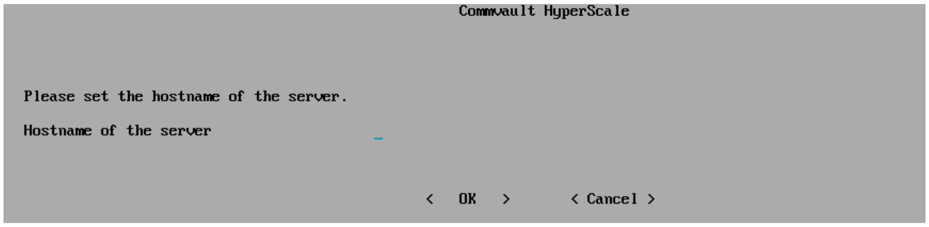
Allow the server to reboot and Linux to start. At the login screen, the default login is root/cvadmin. Log in and change the directory to /opt/commvault/MediaAgent and type the following command:

./setupsds



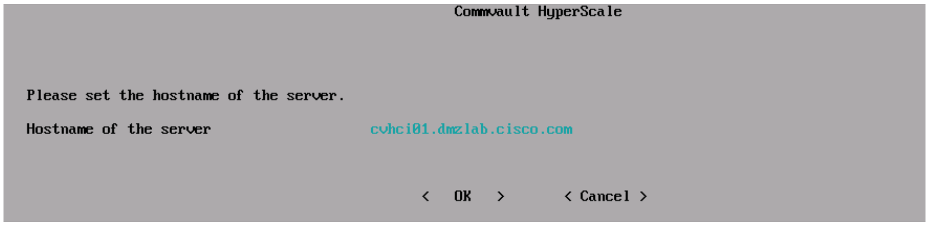
```
Storage
Kernel 3.10.0-514.10.2.el7.x86_64 on an x86_64

hyperscale login: root
Password:
Last login: Wed Oct 11 07:49:54 on tty1
[root@hyperscale ~]# cd /opt/commvault/MediaAgent
[root@hyperscale MediaAgent]# ls
answer_file.cfg      cvchroot.sh         cvovirtconfig.py     GlusterInstaller       modeui.py          setupsds.tmpl
archiveIndex         cvcluster.py        cvovirtsdk.py        GlusterInstaller.tmpl  NasBackup          SynthFull
auxCopy              cvcstype.py         cvrbashcmdlist       GlusterPreReqCheck.sh  NASCreateIndex     test_cmd
binlist              cvdetectusb.py      cvrbashcommand.sh    gluster_rpms.tar       nasRestore         test_ready
bmr                  cvethwizard.py      cvsetuphname.py      grub.cfg               nwconfig.py        ui.py
bmr.py               cvhcconfig.py       cvsetupmgmthname.py  IdxLabelUtil           nwintfx.py         ui.pyc
CatalogMigration     CVJobReplicator     cvtestovirtsdk.py    IndexCache             nwwizard.py        uncompressor
CentOS               cvmagui             diskui.py            indexRestore           registertocs.py    updateIndex
common.py            CvMountd            dmWriter             init                   registertocsui.py  utils.py
commvault_title.cfg  CVNasFileScan       dsBackup             init.py                RHEL               utils.pyc
compressor           CVNasSnapBackup     dsRestore            isolinux.bin           Scripts            wrappers.py
createcd.py          CVNasSnapRestore    efiboot.img          isolinux.cfg           scsi_inq           wrappers.pyc
createcd.sh          CVNdmpRemoteServer  efiboot.sh           libGlfsPbba.so         setkernelconsole
createIndex          cvnodetype.py       FsIndexedRestore     lvm.conf               setup.py
createinitrd.sh      cvnwtype.py         GlusterCommon.sh     MediaLabelReader       setupsds
[root@hyperscale MediaAgent]# ./setupsds
```

Enter the host name of the server, enter a fully qualified domain name (FQDN) if this server will be part of a domain, and use the arrow keys to select OK.



Please set the hostname of the server.

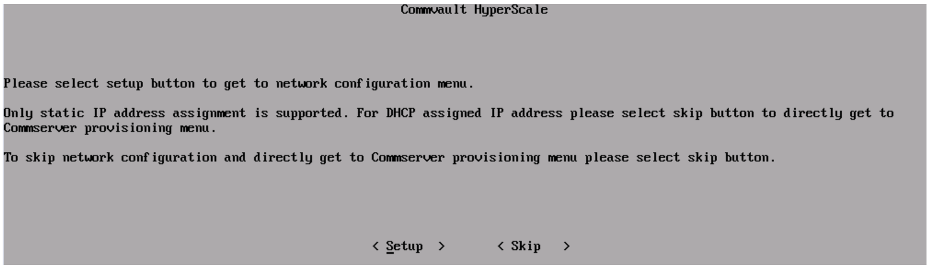
Hostname of the server _



Please set the hostname of the server.

Hostname of the server cvhci01.dmzlab.cisco.com

Select Setup to continue with IP address setup.

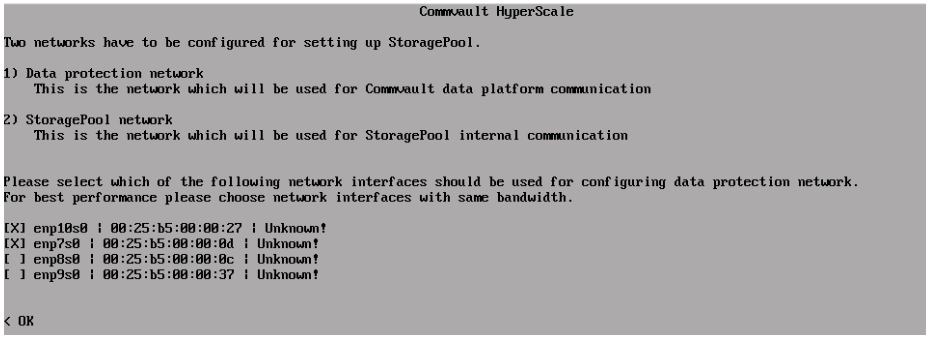


Please select setup button to get to network configuration menu.

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

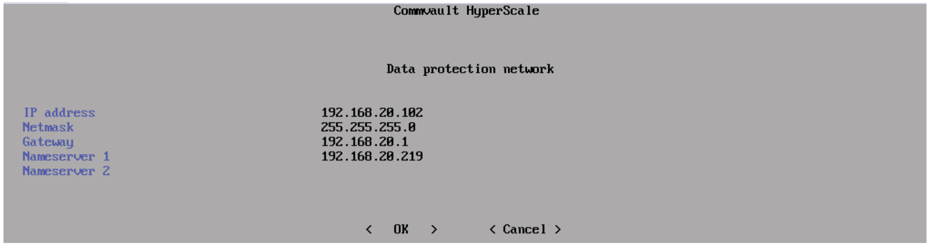
To skip network configuration and directly get to Commserver provisioning menu please select skip button.

You need to configure two networks: one for data protection (that is, an external network for data transfer), and one for internal communications between the nodes within the storage pool. Depending on the network configuration, you many see two or more NICs. Assuming an even number of NICs, verify that they are all connected, and select half for the data protection operations. On a later screen, you will select the other NICs for internal communications.



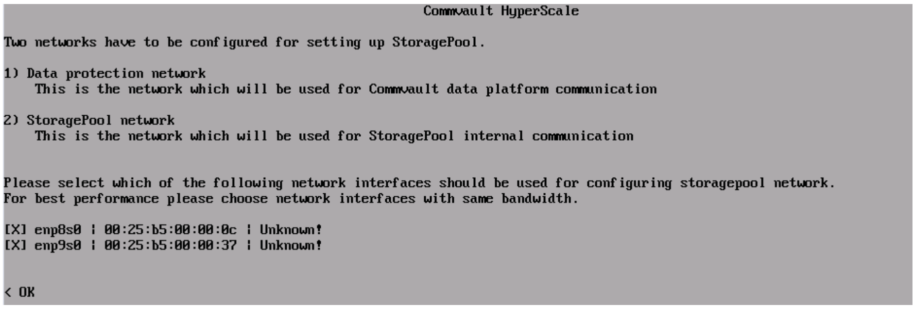
```
                                                      Commvault HyperScale

Two networks have to be configured for setting up StoragePool.

1) Data protection network
    This is the network which will be used for Commvault data platform communication

2) StoragePool network
    This is the network which will be used for StoragePool internal communication


Please select which of the following network interfaces should be used for configuring data protection network.
For best performance please choose network interfaces with same bandwidth.

[X] enp10s0 | 00:25:b5:00:00:27 | Unknown!
[X] enp7s0 | 00:25:b5:00:00:0d | Unknown!
[ ] enp8s0 | 00:25:b5:00:00:0c | Unknown!
[ ] enp9s0 | 00:25:b5:00:00:37 | Unknown!


< OK
```

Enter the IP address, mask, gateway, and Domain Name System (DNS) servers for the NICs selected previously. The NICs will be bonded, so only one IP address is required.



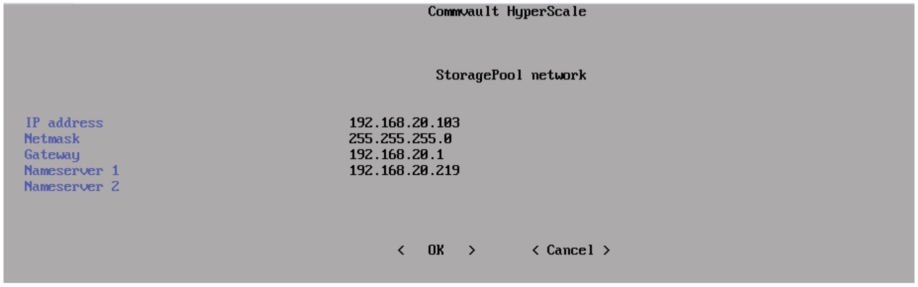
```
                                                Commvault HyperScale



                                               Data protection network


  IP address                             192.168.20.102
  Netmask                                255.255.255.0
  Gateway                                192.168.20.1
  Nameserver 1                           192.168.20.219
  Nameserver 2



                                     <   OK   >       < Cancel >
```

Now select the NICs to be used for the internal communications between the server nodes.



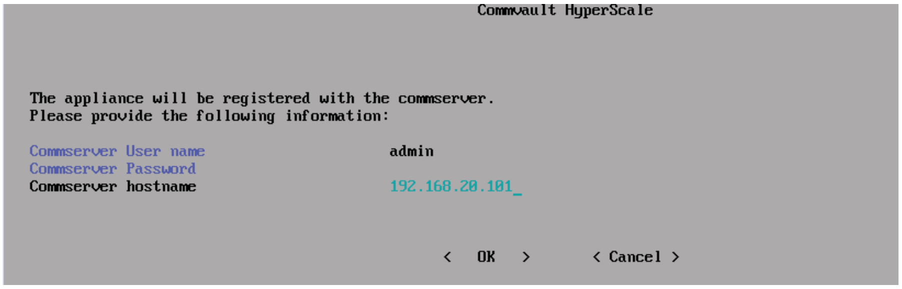
```
                                                      Commvault HyperScale
Two networks have to be configured for setting up StoragePool.

1) Data protection network
    This is the network which will be used for Commvault data platform communication

2) StoragePool network
    This is the network which will be used for StoragePool internal communication


Please select which of the following network interfaces should be used for configuring storagepool network.
For best performance please choose network interfaces with same bandwidth.

[X] enp8s0 | 00:25:b5:00:00:0c | Unknown!
[X] enp9s0 | 00:25:b5:00:00:37 | Unknown!


< OK
```

Enter the IP address, mask, gateway, and DNS servers for the internal network.



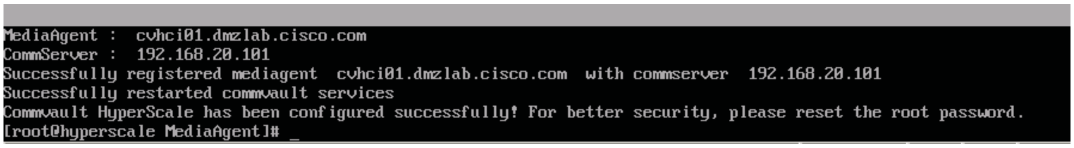
```
                                                      Commvault HyperScale



                                                        StoragePool network


  IP address                                   192.168.20.103
  Netmask                                      255.255.255.0
  Gateway                                      192.168.20.1
  Nameserver 1                                 192.168.20.219
  Nameserver 2



                                              <   OK   >       < Cancel >
```

Enter the username and password for the CommServe server and the CommServe name or IP address. If you are using a name, verify that it is resolvable from all nodes; otherwise, use the IP address.



```
                              Commvault HyperScale


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

 Commserver User name                    admin
 Commserver Password
 Commserver hostname                     192.168.20.101_


                            <  OK  >       < Cancel >
```

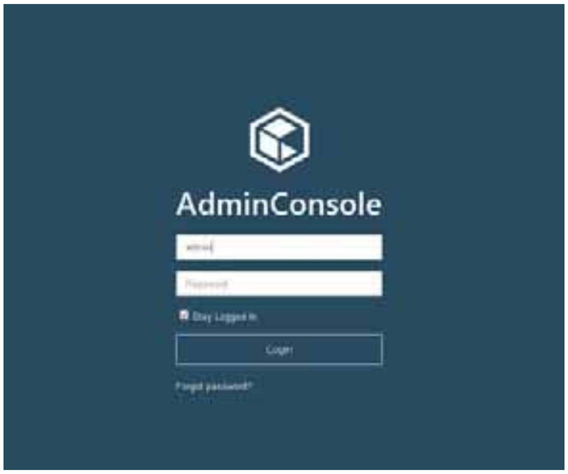
The node should register with CommServe. Setup for this node is complete.



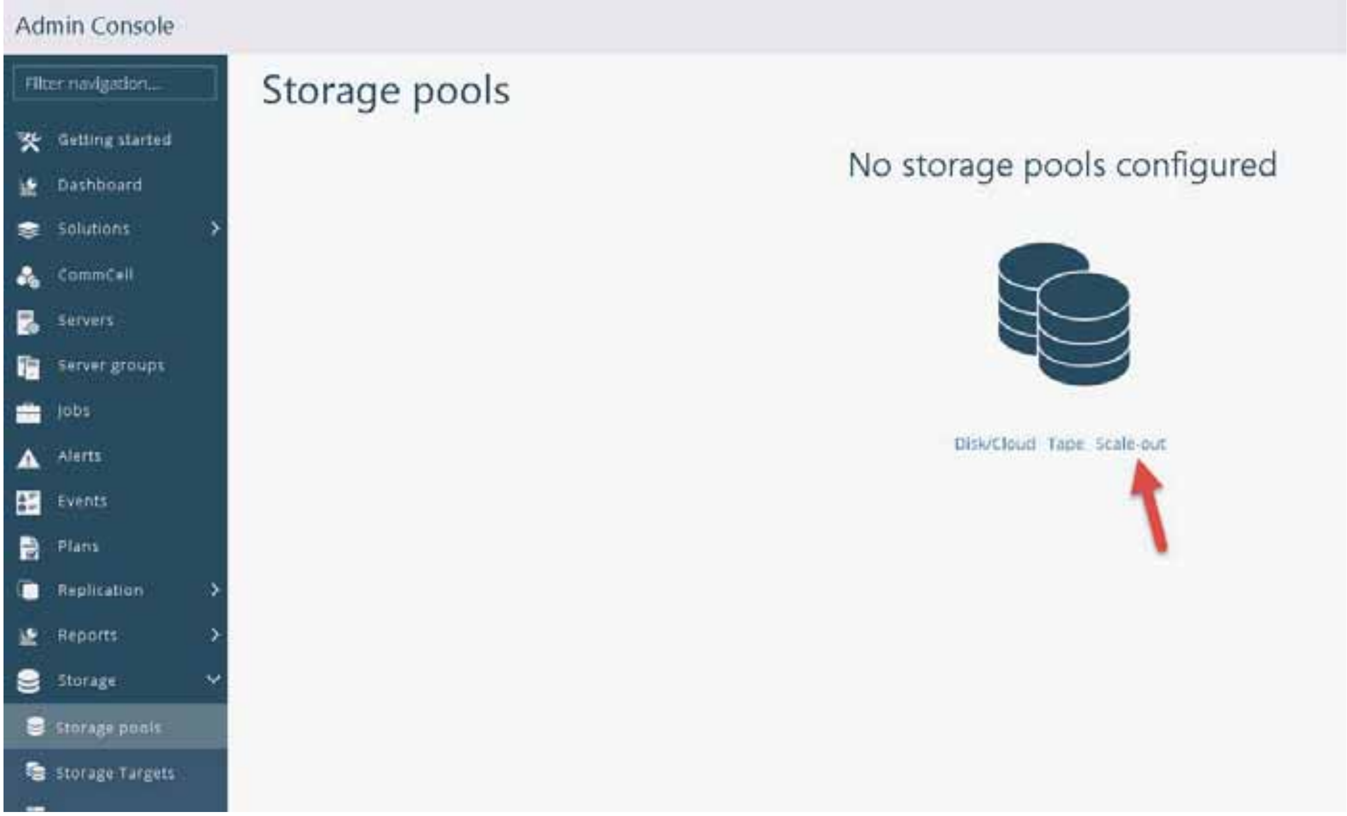
```
MediaAgent :  cvhci01.dmzlab.cisco.com
CommServer :  192.168.20.101
Successfully registered mediagent  cvhci01.dmzlab.cisco.com  with commserver  192.168.20.101
Successfully restarted commvault services
Commvault HyperScale has been configured successfully! For better security, please reset the root password.
[root@hyperscale MediaAgent]# _
```

Repeat the process for the other nodes. (**Note:** The nodes can be installed in parallel. They do not need to be installed one at a time.)

After the final node has completed setup successfully, log on to AdminConsole to complete the installation by creating a storage pool.



In the left pane, click Storage. Then click “Storage pools” and “Scale-out.”

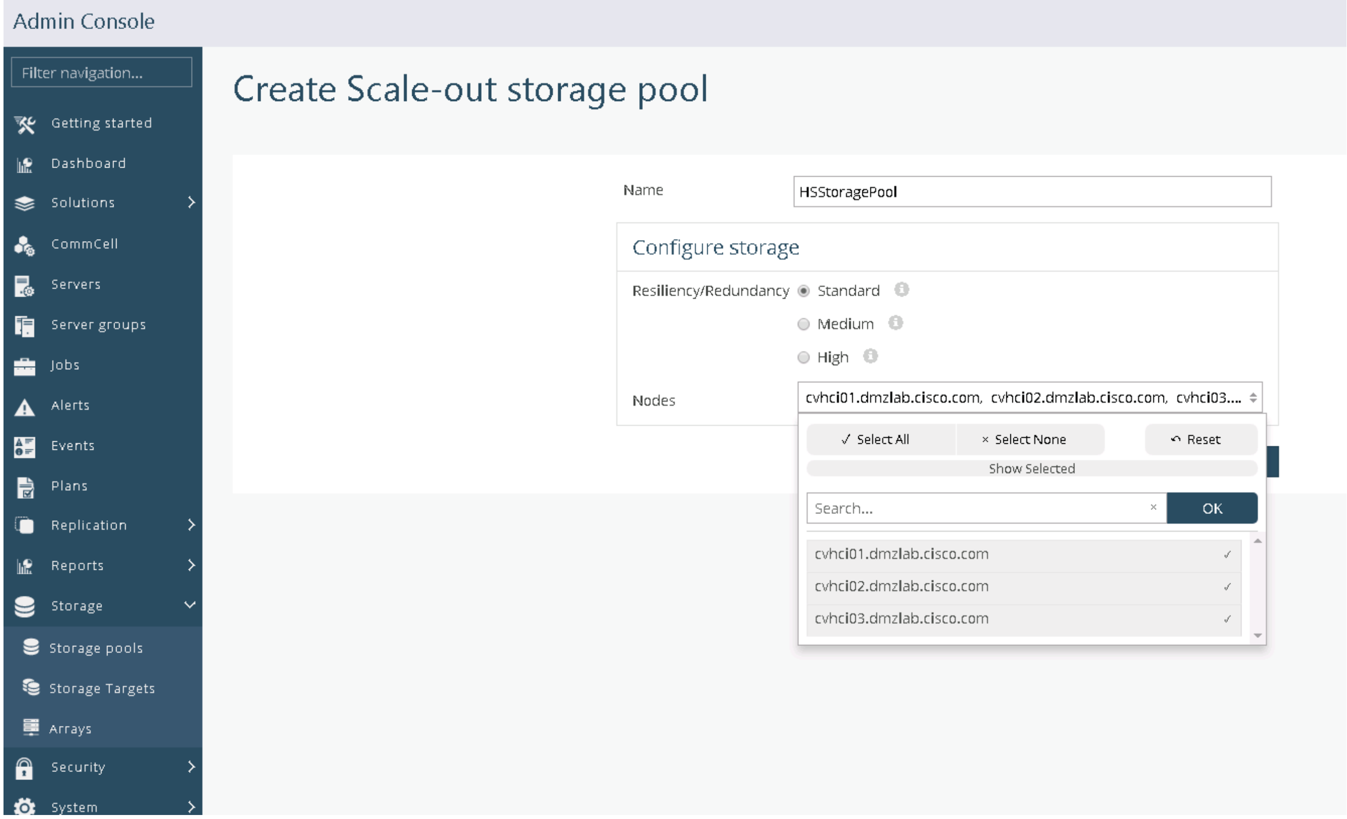


On the “Create Scale-out storage pool” page, enter a name for the pool and select the resiliency and redundancy factor:

- Standard: Three nodes, disperse factor 6, and redundancy factor 2; withstands loss of two drives or one node.
- Medium: Six nodes, disperse factor 6, and redundancy factor 2; withstands loss of two drives or two nodes.
- High: Six nodes, disperse factor 12, and redundancy factor 4; withstands loss of four drives or two nodes.

If you are installing three nodes, always select Standard. If you are installing six nodes, choose between Medium and High.

Next select the nodes to be part of the pool, click OK, and click Configure.



Create Scale-out storage pool

Name: HSStoragePool

Configure storage

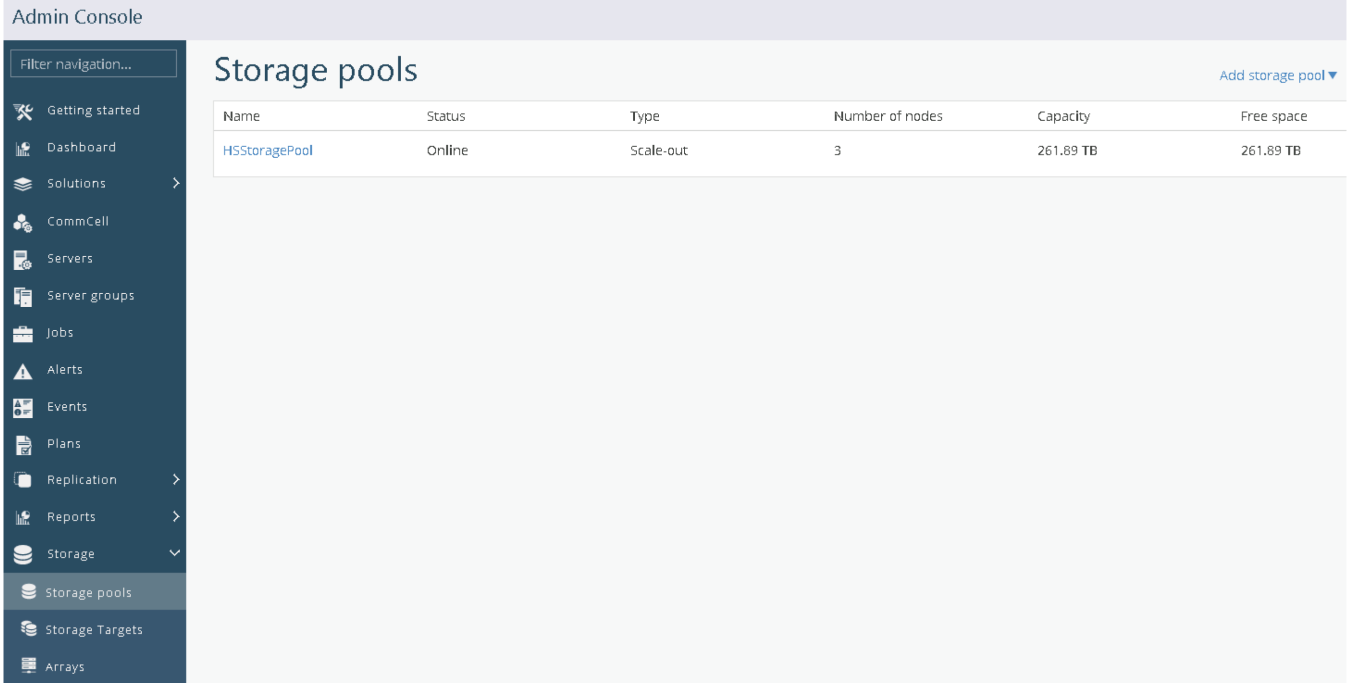
Resiliency/Redundancy: ● Standard ○ Medium ○ High

Nodes: cvhci01.dmzlab.cisco.com, cvhci02.dmzlab.cisco.com, cvhci03....

- cvhci01.dmzlab.cisco.com ✓
- cvhci02.dmzlab.cisco.com ✓
- cvhci03.dmzlab.cisco.com ✓

The storage pool will be created. It may be shown as offline with 0 capacity for a few minutes as a background process runs to create the gluster file system and then bring it online. As part of the storage pool creation process, the disk library will be created.

At this point, the HyperScale setup is complete and ready to perform backup operations.



Storage pools

Name	Status	Type	Number of nodes	Capacity	Free space
HSStoragePool	Online	Scale-out	3	261.89 TB	261.89 TB

Conclusion

Data Protection using Commvault ScaleProtect with Cisco UCS S3260 Storage Switches can meet every requirement and is simple and easy to use. Backup and restore operations can be initiated from a single GUI, and the complexity of the underlying system can be hidden from daily operators. The seamless integration of Commvault HyperScale technology and the Cisco UCS S3260 storage server make this a best-in-class solution for secondary-site backup operations, virtual machine archiving, and multiple options for restoration–all within a single management interface.

For more information

For additional information, see the following:

- Cisco UCS S3260 Storage Server
- Cisco UCS 6000 Series Fabric Interconnects
- Cisco UCS Manager
- Cisco white paper: Achieve Optimal Network Throughput on the Cisco UCS S3260 Storage Server
- Commvault Software Offline Installation

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-740112-00 01/18