ScaleProtect with Cisco UCS on the Cisco UCS C240 M5 Rack Server

This document provides an introduction to the process of deploying the Commvault Data Platform including Commvault HyperScale™ Software on the Cisco UCS® C240 M5 Rack Server using ScaleProtect™ with Cisco UCS® architecture.

JUNE 2018

Contents

Introduction 3
Purpose of this document 3
Test environment 3
Solution overview 4
Cisco Unified Computing System 5
Cisco UCS C240 M5 Rack Server 6
Commvault Data Platform 7
Solution design and reference architecture configurations 8
Reference architecture 9
Storage capacity explained 11
Configuration guidelines 12
Cisco UCS configuration 12
Standalone configuration with Cisco Integrated Management Controller 12
Disk configurations required for ScaleProtect with Cisco UCS installation 18
Cisco UCS managed configuration with Cisco UCS Manager 29
Setting up the Cisco UCS C240 M5 server 36
Creating the ScaleProtect with Cisco UCS server storage profile 36
Configuring the LAN 38
Configuring the SAN 54
Configuring a server pool 65
Configuring a service profile template 67
Commvault HyperScale Software installation and configuration 76
CommServe installation 76
ScaleProtect with Cisco UCS node installation and configuration 76
Using Cisco UCS Manager to launch the software installation process 76
Using Cisco IMC to launch the software installation process 79
Installing the software 80
Configuring the storage pool from AdminConsole 86
For more information 88

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 achieve 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. ScaleProtect™ with Cisco UCS® on the Cisco Unified Computing System™ (Cisco UCS) 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. ScaleProtect with Cisco UCS is a powerful and unique scale-out data protection solution that combines Commvault HyperScale™ Software with Cisco UCS. ScaleProtect with Cisco UCS offers enterprises a single, integrated solution that delivers infrastructure simplicity, elasticity, resiliency, flexibility, and scale for managing secondary data. It replaces traditional backup tools with a modern cloud-enabled data management solution.

Purpose of this document

This document describes the installation and configuration steps for deploying ScaleProtect with Cisco UCS on Cisco UCS C240 M5 Rack Servers to build an integrated data protection solution. It provides Cisco and Commvault configuration guidelines and best practices to help enterprises 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 on the Commvault console. This document does not cover the initial setup of the Cisco UCS platform 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 3.2(2b)
	Cisco UCS C240 M5 Rack Server	Release 3.2(2b)
Network	Cisco Nexus® 9372PX-E Switch pair	Release 7.0(3)I4(7)
Software	Cisco UCS Manager	Release 3.2(2b)
	Commvault Data Platform	Release V11 SP11
	Cisco Integrated Management Controller (IMC) Cisco UCS C240 M5 Rack Server Software (standalone)	Release 3.1(3a)

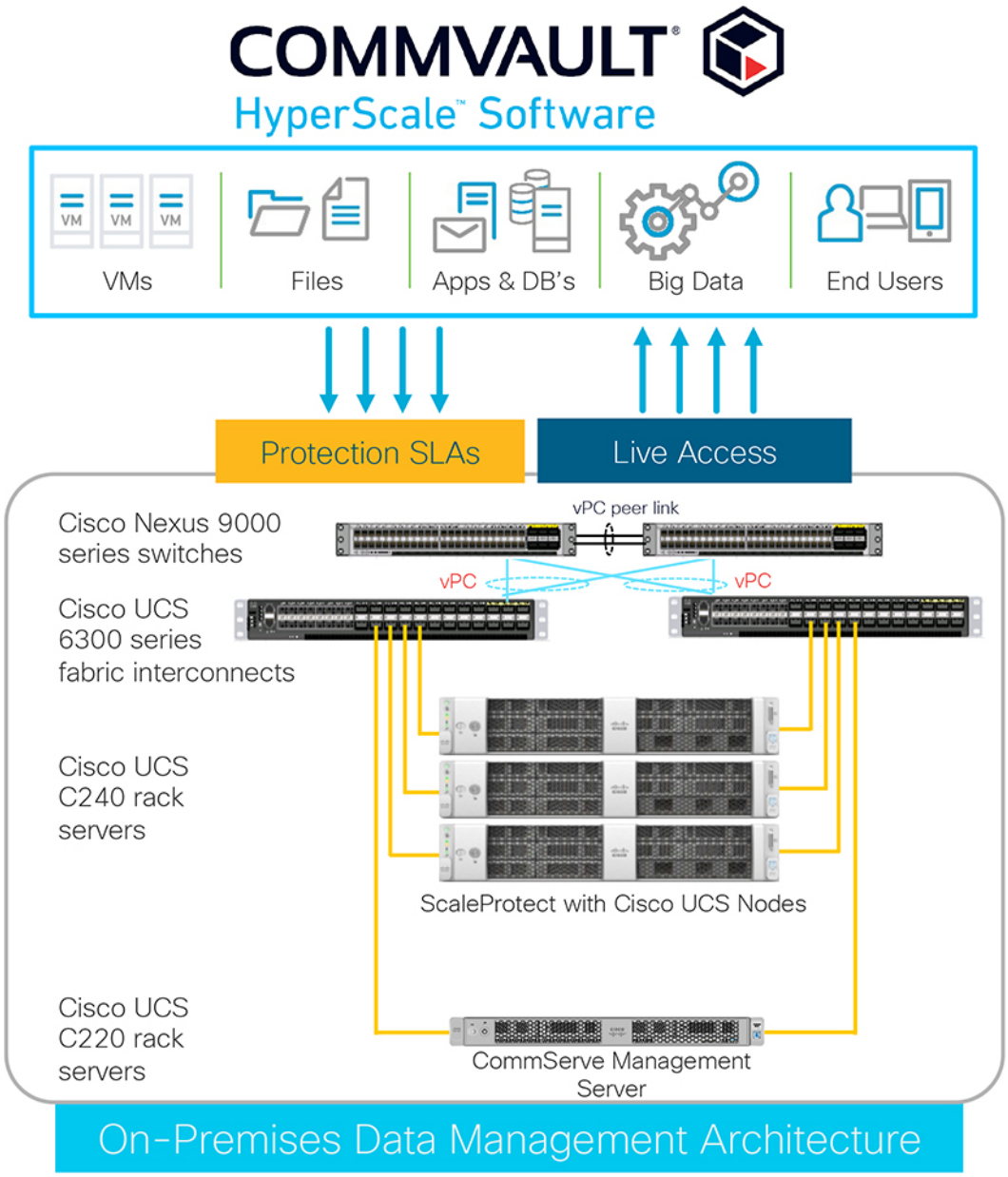
Solution overview

By combining Cisco UCS servers with industry-leading Commvault HyperScale Software, customers gain outstanding 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.

Commvault HyperScale Software provides a full suite of data services for protecting, indexing, securing, automating, reporting, and natively accessing data. In addition, Commvault HyperScale Software 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



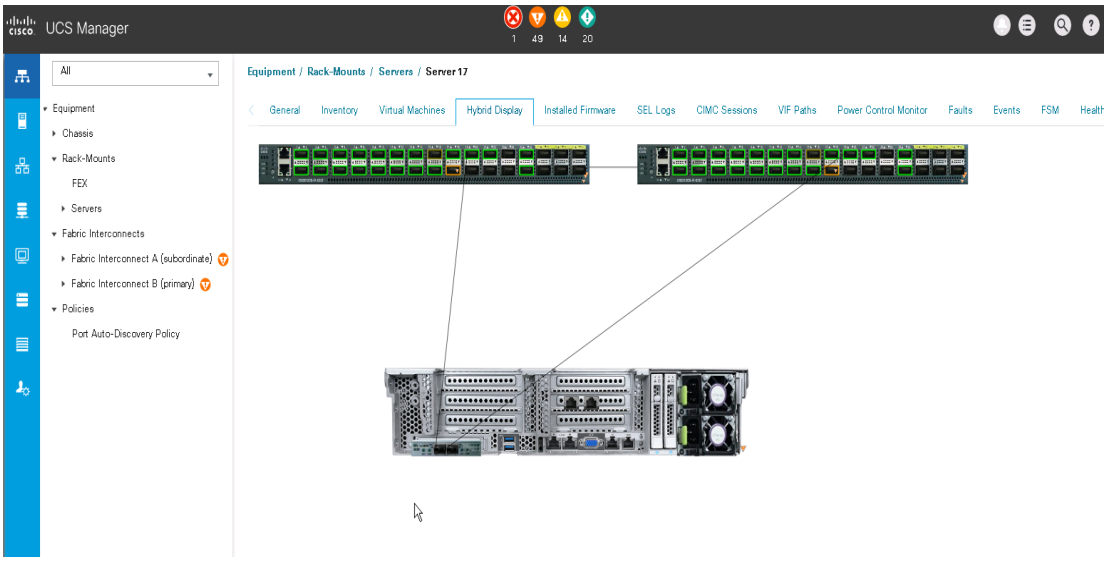
Cisco Unified Computing System

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.

The main components of Cisco UCS are described here:

- **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 the 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 choices 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 Cisco UCS software and hardware components (Figure 2).
- Cisco UCS 6000 Series Fabric Interconnects are line-rate, low-latency, lossless, 10-Gbps Ethernet and FCoE interconnect switches providing 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 six-rack unit (6RU) enclosure.
- Cisco UCS B-Series Blade Servers increase performance, efficiency, versatility, and productivity with Intel-based blade servers.
- 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 C240 M5 Rack Server

The Cisco UCS C240 M5 Rack Server (Figure 3) is a 2-socket, 2RU rack server offering industry-leading performance and expandability. It supports a wide range of storage and I/O-intensive infrastructure workloads, including big data and analytics, data protection, and collaboration workloads. Cisco UCS C-Series Rack 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 business agility.

Figure 3. Cisco UCS C240 M5 Rack Server

In response to ever-increasing computing and data-intensive real-time workloads, the enterprise-class Cisco UCS C240 M5 server extends the capabilities of the Cisco UCS portfolio in a 2RU form factor. It incorporates the Intel Xeon Scalable processors, supporting up to 20 percent more cores per socket, twice the memory capacity, and five times more Non-Volatile Memory Express (NVMe) PCI Express (PCIe) solid-state disks (SSDs) than the previous generation of servers. These improvements deliver significant performance and efficiency gains that will improve your application performance. The C240 M5 delivers outstanding levels of storage expandability with exceptional performance, with:

- The latest Intel Xeon Scalable CPUs, with up to 28 cores per socket
- Up to 24 DDR4 DIMMs for improved performance
- Intel 3D XPoint-ready support, with built-in support for next-generation nonvolatile memory technology
- Up to 26 hot-swappable small-form-factor (SFF) 2.5-inch drives, including 2 rear hot-swappable SFF drives (up to 10 support NVMe PCIe SSDs on the NVMe-optimized chassis version), or 12 large-form-factor (LFF) 3.5-inch drives plus 2 rear hot-swappable SFF drives

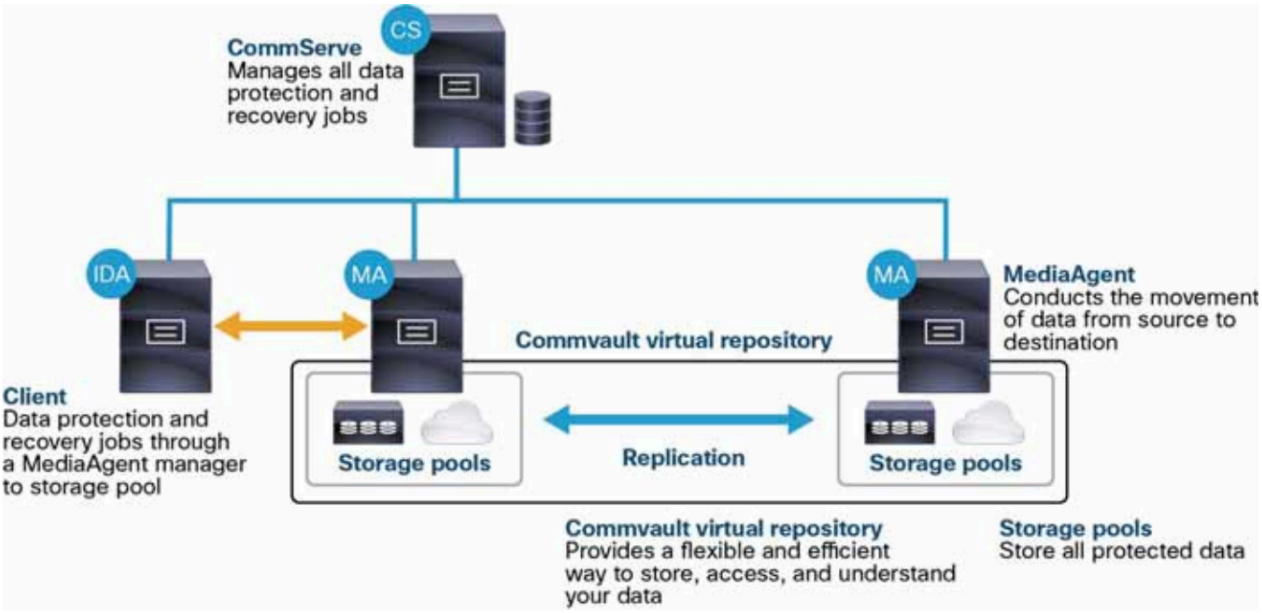
- Support for a 12-Gbps SAS modular RAID controller in a dedicated slot, leaving the remaining PCIe Generation 3.0 slots available for other expansion cards
- Modular LAN-on-motherboard (mLOM) slot that can be used to install a Cisco UCS virtual interface card (VIC) without consuming a PCIe slot, supporting dual 10- or 40-Gbps network connectivity
- Dual embedded Intel x550 10GBASE-T LAN-on-motherboard (LOM) ports
- Modular M.2 or Secure Digital (SD) cards that can be used for boot

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. The 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



- The CommServe (CS) server is the command and control center of the CommCell architecture. It coordinates and processes all CommCell operations, maintaining Microsoft SQL Server databases that contain all configuration, security, and operational history for the CommCell environment. A CommCell environment can have only one CommServe host. The CommServe software can be installed in physical, virtual, and clustered environments.
- The MediaAgent (MA) 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 IntelliSnap® snapshot integration with the underlying storage.

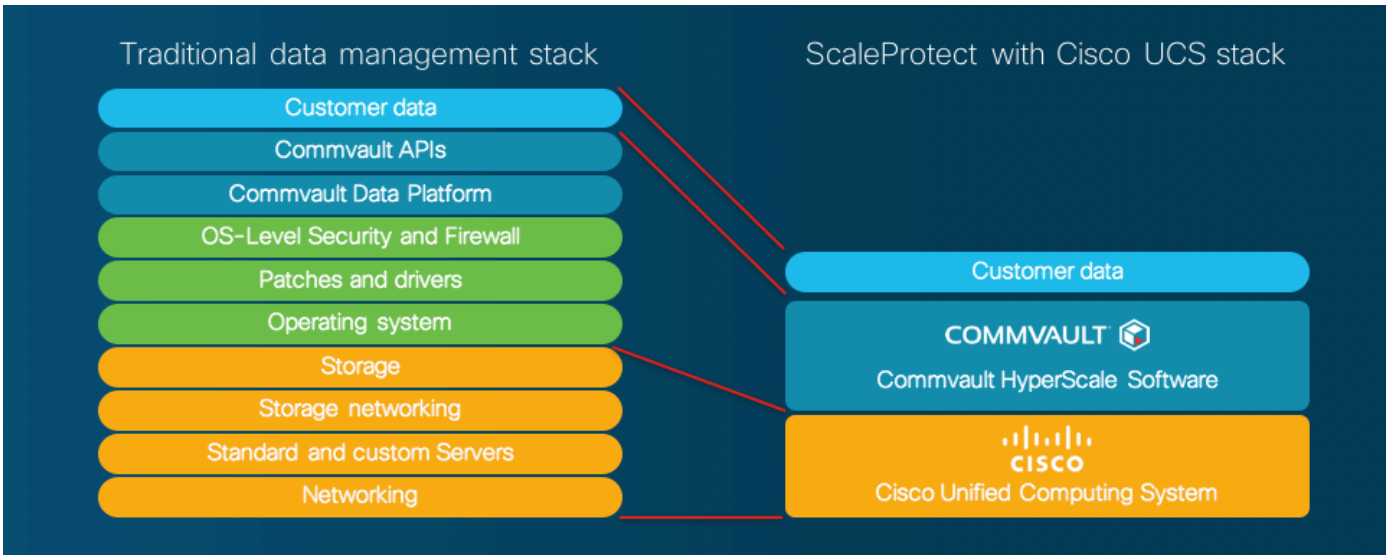
- The client is any system within a CommCell environment to be protected. iDataAgents (IDAs) are software modules that are installed on computers to access and protect data. The backup and recovery system uses agents to interface with file systems, applications, and databases to facilitate the protection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

These three Commvault components in combination result in the most comprehensive and flexible data protection solution on the market today.

Solution design and reference architecture configurations

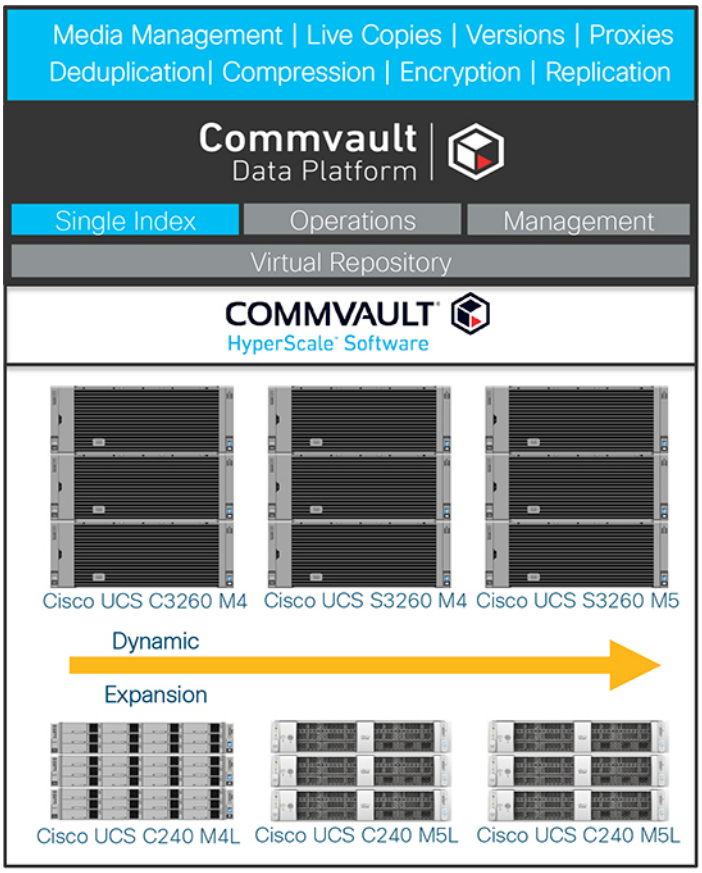
ScaleProtect with Cisco UCS addresses the data protection needs of modern data centers. The increasing percentage of virtualized workloads, the dramatic increase in the size and amount of data, and the changes in the ways that companies do business and work with data have had an immense impact on data 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 Software 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 ScaleProtect with Cisco UCS



The features and functions provided by Commvault Data Protection with Commvault HyperScale Software in combination 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: ScaleProtect with Cisco UCS. With the combination of Cisco and Commvault technologies, you can easily scale from tens of terabytes (TB) up to petabytes (PB) of protected data (Figure 6).

Figure 6. ScaleProtect with Cisco UCS scaling



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 backup systems. 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” location 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 with Cisco UCS nodes. This option also allows Cisco UCS Manager to manage all ScaleProtect with Cisco UCS servers in a central place.

Reference architecture

Using the rules for Commvault HyperScale Software technology as a basis, Commvault and Cisco have defined and tested various configurations (Tables 2, 3, and 4) and 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-node block model scales in increments of 3: to 3, 6, 9, 12, or more nodes. The 6-node block model scales in increments of 6: to 6, 12, 18, 24, or more nodes. When deploying nodes inside the same block (for example, in a 3-node initial configuration), choose nodes with the same hard-disk drive (HDD) count and size. All nodes in a block must have the same configuration. This requirement applies to resources such as CPU, memory, SSD, and HDD type, number, and capacity. This requirement helps ensure even performance and resource utilization across nodes within the

block. Separate node blocks in the same grid can use different HDDs (for example, a 3-node 6-TB block can be mixed with a second 3-node 10-TB block in the same grid). As a deployment option, you can run CommServe virtualized to manage the physical ScaleProtect with Cisco UCS server nodes.

Table 2. ScaleProtect with Cisco UCS server node configurations

	Cisco UCS C240 M5 node	Cisco UCS S3260 single-server node	Cisco UCS S3260 dual-server node
Boot disks	2 x 960-GB M.2 SSDs	2 x 480-GB SSDs	4 x 480-GB SSDs
Data disks	• 12 x 4-TB SAS • 12 x 6-TB SAS • 12 x 8-TB SAS • 12 x 10-TB SAS • 12 x 12-TB SAS	• 24 x 4-TB SAS • 24 x 6-TB SAS • 24 x 8-TB SAS • 24 x 10-TB SAS • 24 x 12-TB SAS	• 48 x 4-TB SAS • 48 x 6-TB SAS • 48 x 8-TB SAS • 48 x 10-TB SAS • 48 x 12-TB SAS
Flash storage	1 x 3.2-TB NVMe	4 x 1.6-TB SSD	8 x 1.6-TB SSD
Cisco UCS rack servers	C240 M5 LFF	S3260 M4	2 x S3260 M4
CPU	2 x Intel Xeon processor 4114 CPUs (with 10 cores, 2.2 GHz, and 85W)	2 x Intel Xeon processor E5-2650 v4 CPUs (with 12 cores, 2.2 GHz, and 105W)	2 x Intel Xeon processor E5-2650 v4 CPUs (with 12 cores, 2.2 GHz, and 105W)
Memory	256 GB	256 GB	2 x 256 GB
RAID cache	1 GB	4GB	2 x 4 GB
RAID	RAID 1 for OS and JBOD for SAS	RAID 1 for OS, RAID5 for SSD, and JBOD for HDD	RAID 1 for OS, RAID5 for SSD, and JBOD for HDD
Maximum number of 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	HDD count	HDD drive size[1]	3-node usable[2]	6-node usable[2]	9-Node usable[2]	12-Node usable[2]	15-Node usable[2]	18-Node usable[2]
Cisco UCS C240	12	4 TB	87 TB	174 TB	261 TB	349 TB	436 TB	523 TB
	12	6 TB	130 TB	261 TB	392 TB	523 TB	654 TB	785 TB
	12	8 TB	174 TB	349 TB	523 TB	698 TB	873 TB	1047 TB
	12	10 TB	218 TB	436 TB	654 TB	873 TB	1091 TB	1309 TB
	12	12 TB	261 TB	523 TB	785 TB	1047 TB	1309 TB	1571 TB
Cisco UCS S3260	24	4 TB	174 TB	349 TB	523 TB	698 TB	873 TB	1047 TB
	24	6 TB	261 TB	523 TB	785 TB	1047 TB	1309 TB	1571 TB
	24	8 TB	349 TB	698 TB	1047 TB	1396 TB	1746 TB	2095 TB
	24	10 TB	436 TB	873 TB	1309 TB	1746 TB	2182 TB	2619 TB
	24	12 TB	523 TB	1047 TB	1571 TB	2095 TB	2619 TB	3143 TB

1. HDD capacity values are calculated using base 10 (for example, 1 TB = 1,000,000,000,000 bytes).
2. Capacity values are calculated using base 2 (for example, 1 TB = 1,099,511,627,776 bytes).

Table 4. ScaleProtect with Cisco UCS node sizing

Cisco UCS model	Solution ID	Description	Node count	HDD size[1]	Rack size
Cisco UCS C240	ScaleProtect C240 M5 4 TB	C240 M5 with 12 x 4-TB drives	12	4 TB	2RU
	ScaleProtect C240 M5 6 TB	C240 M5 with 12 x 6-TB drives	12	6 TB	2RU
	ScaleProtect C240 M5 8 TB	C240 M5 with 12 x 8-TB drives	12	8 TB	2RU
	ScaleProtect C240 M5 10 TB	C240 M5 with 12 x 10-TB drives	12	10 TB	2RU
	ScaleProtect C240 M5 12 TB	C240 M5 with 12 x 12-TB drives	12	12 TB	2RU
Cisco UCS S3260	ScaleProtect S3260 M5 4 TB	S3260 M4 single-server node with 24 x 4-TB drives	24	4 TB	4RU
	ScaleProtect S3260 M5 4 TB 2N	S3260 M4 dual-server nodes with 48 x 4-TB drives	48	4 TB	4RU
	ScaleProtect S3260 M5 6 TB	S3260 M4 single-server node with 24 x 6-TB drives	24	6 TB	4RU
	ScaleProtect S3260 M5 6 TB 2N	S3260 M4 dual-server nodes with 48 x 6-TB drives	48	6 TB	4RU
	ScaleProtect S3260 M5 8 TB	S3260 M4 single-server node with 24 x 8-TB drives	24	8 TB	4RU
	ScaleProtect S3260 M5 8 TB 2N	S3260 M4 dual-server nodes with 48 x 8-TB drives	48	8 TB	4RU
	ScaleProtect S3260 M5 10 TB	S3260 M4 single-server node with 24 x 10-TB drives	24	10 TB	4RU
	ScaleProtect S3260 M5 10 TB 2N	S3260 M4 dual-server nodes with 48 x 10-TB drives	48	10 TB	4RU
	ScaleProtect S3260 M5 12 TB	S3260 M4 single-server node with 24 x 12-TB drives	24	12 TB	4RU
	ScaleProtect S3260 M5 12 TB 2N	S3260 M4 dual-server nodes with 48 x 12-TB drives	48	12 TB	4RU

1. HDD capacity values are calculated using base 10 (for example, 1 TB = 1,000,000,000,000 bytes).
2. Capacity values are calculated using base 2 (for example, 1 TB = 1,099,511,627,776 bytes).

Storage capacity explained

Sometimes customers ask why a freshly formatted hard disk or array is smaller than the advertised capacity. For example, when you format a 1-TB drive, the capacity shown as 931 GB after formatting.

This disparity occurs because hardware and storage manufacturers measure capacity differently than the file system does. The prefixes kilo-, mega-, giga-, and tera- are used to state powers of ten. However, in computer software, the data being handled typically is organized based on powers of 2, so it has become customary to call 2**10 a kilobyte, even though it actually is 1024 bytes—not exactly 1000 bytes.

Prefixes exist to differentiate between base 10 and base 2; however, they are seldom used. In base 2, the appropriate terms are kibibyte, mebibyte, gibibyte, and tebibyte. The “bi” refers to binary. The abbreviations for these terms are KiB, MiB, GiB, and TiB.

Here’s the math behind the two systems:

- Hard-disk manufacturers assumption: Kilo = 103 = 1000 (KB)
- File systems assumption: Kilo = 224 = 1024 (KiB)

To convert KB, MB, and GB to KiB, MiB, and GiB, use these guidelines:

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

Typically, software will list GB or TB as the storage unit, but the unit actually is GiB or TiB, so this disparity will remain unless the values are converted.

In the tables that follow, capacities are listed using the sizes stated by the hardware manufacturer (using base 10). Notes refer to the software-based sizes (using base 2).

Configuration guidelines

This section provides guidelines for configuring the solution.

Cisco UCS configuration

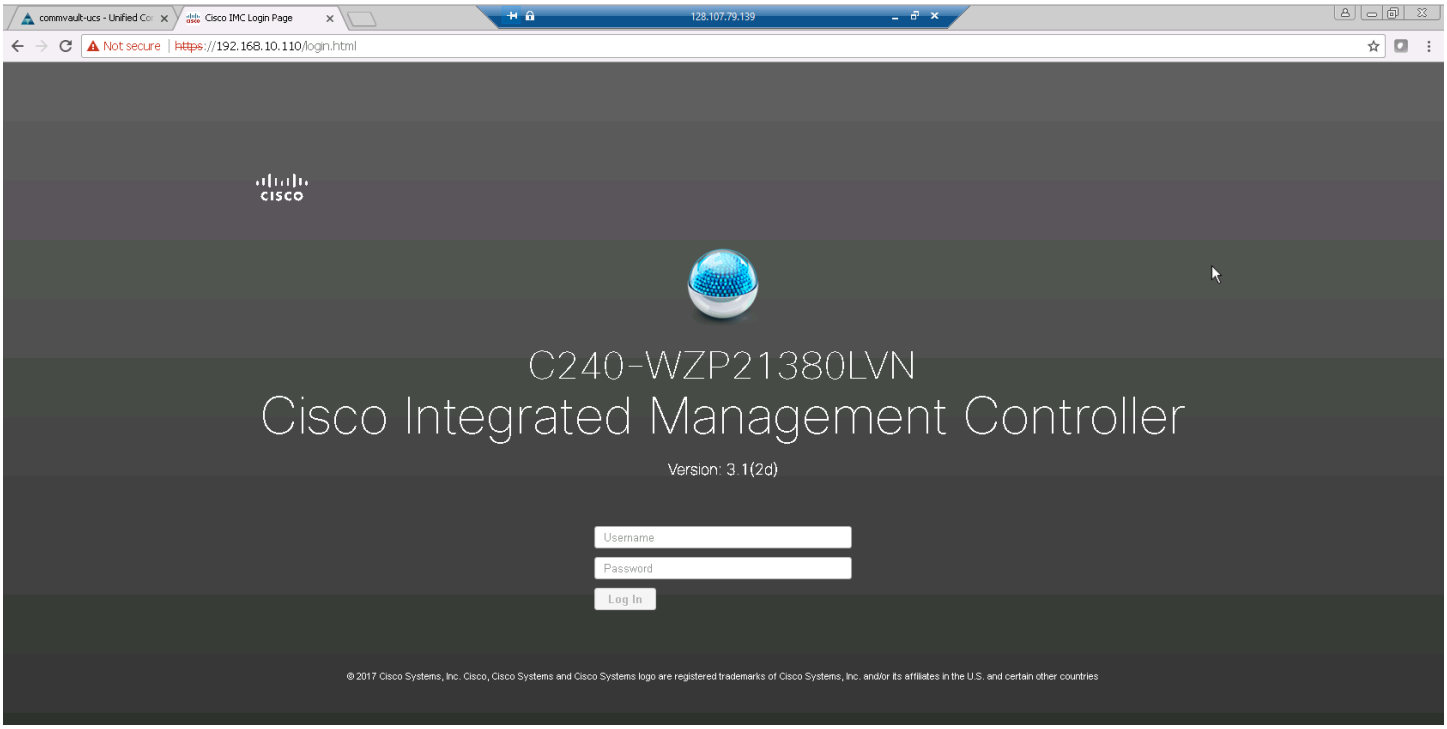
This document discusses the use of a standalone Cisco UCS C240 M5 server as well as the use of a Cisco UCS C240 M5 server managed by Cisco UCS to install ScaleProtect with Cisco UCS. The document thus discusses both placement within a Cisco UCS domain and connection to data center switches.

Please use the Cisco UCS C240 M5 installation guide to complete the initial configuration (IP addresses, passwords, software versions, etc.). This document assumes that the C240 is accessible through the Cisco Integrated Management Controller (IMC) or Cisco UCS Manager over the network.

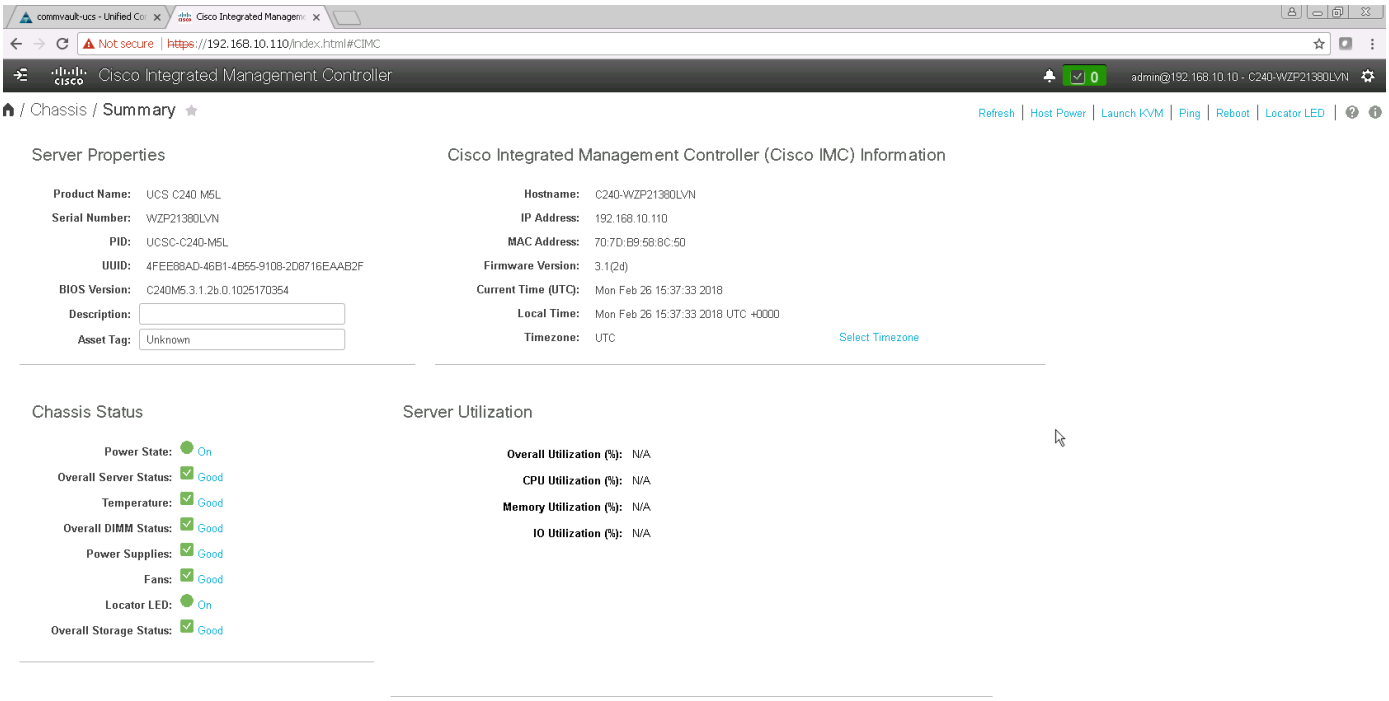
Standalone configuration with Cisco Integrated Management Controller

Follow the steps presented here to configure a standalone solution using the IMC.

1. Log in to the IMC as the admin user.

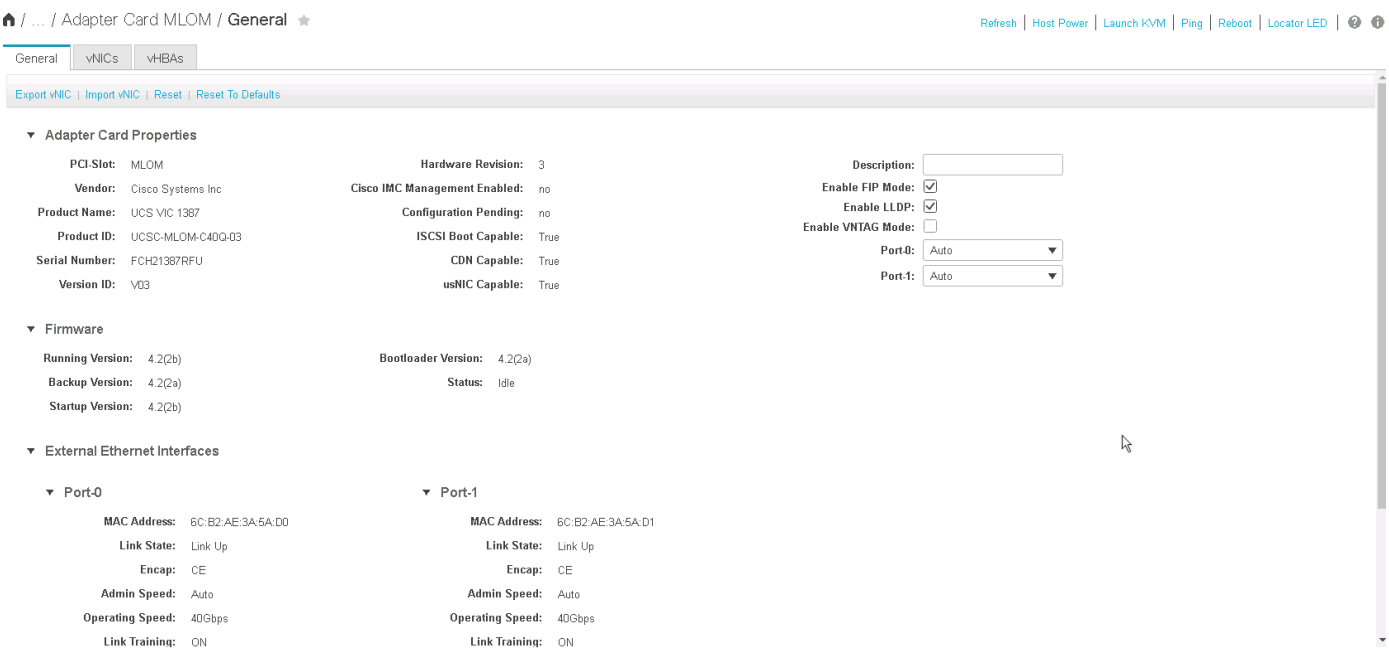


2. Check the condition of the system and the components required for the deployment by choosing Chassis > Summary.



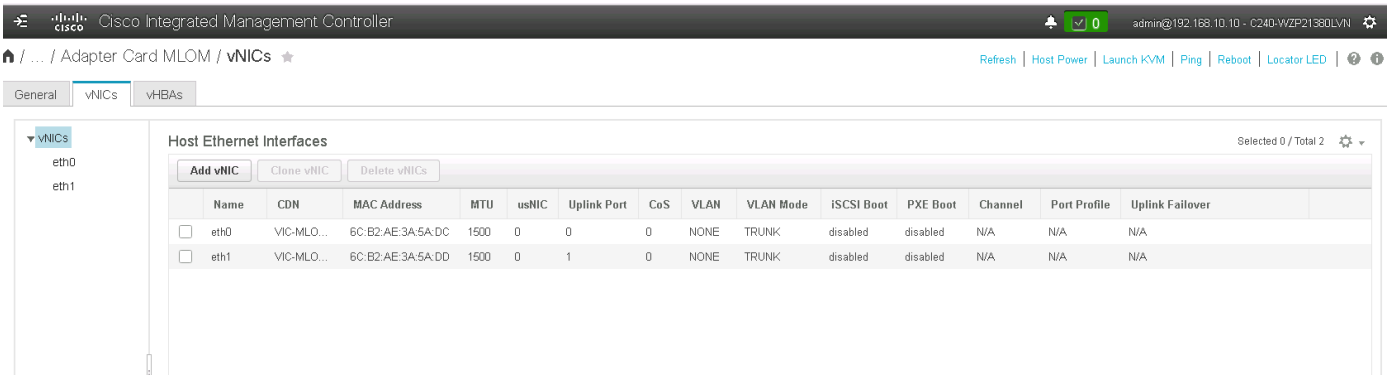
3. Choose Networking and Adapter Card to see the Cisco VIC configuration.

   The General tab provides an overview of the adapter card and Ethernet ports, including the uplink status and port speeds.

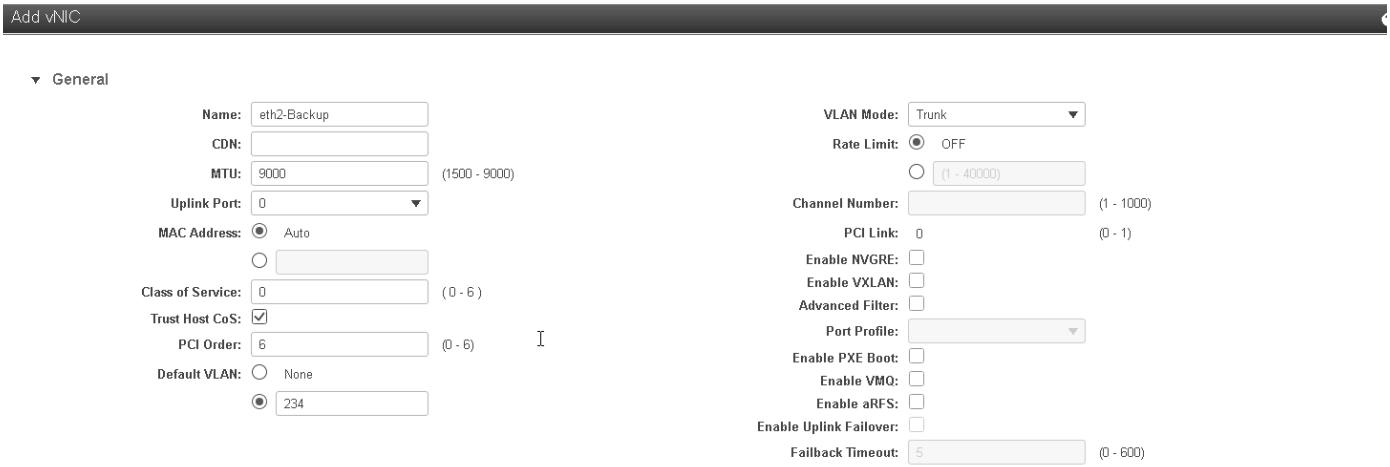


The virtual network interface card (vNIC) tab summarizes the existing host Ethernet interfaces, including the maximum transmission unit (MTU) size, the uplink port used, and VLAN information. As a best practice, you should create at least one vNIC per uplink port or one vNIC per VLAN ID.

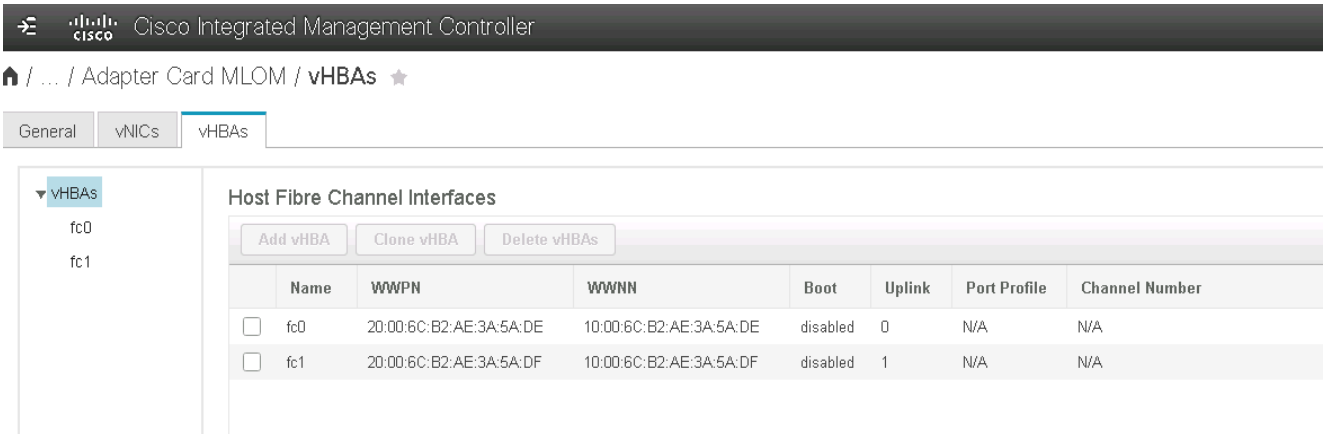
You should use MTU 9000 for the backup network if possible and on all participating devices in the network (clients, switches, and servers).



4. Click Add vNIC to create two additional vNICs. The solution requires four vNICs: two for the backup network and two for cluster communication between the ScaleProtect with Cisco UCS nodes. Select the vNIC parameters based on the network and the upstream switch to which the server is connected.



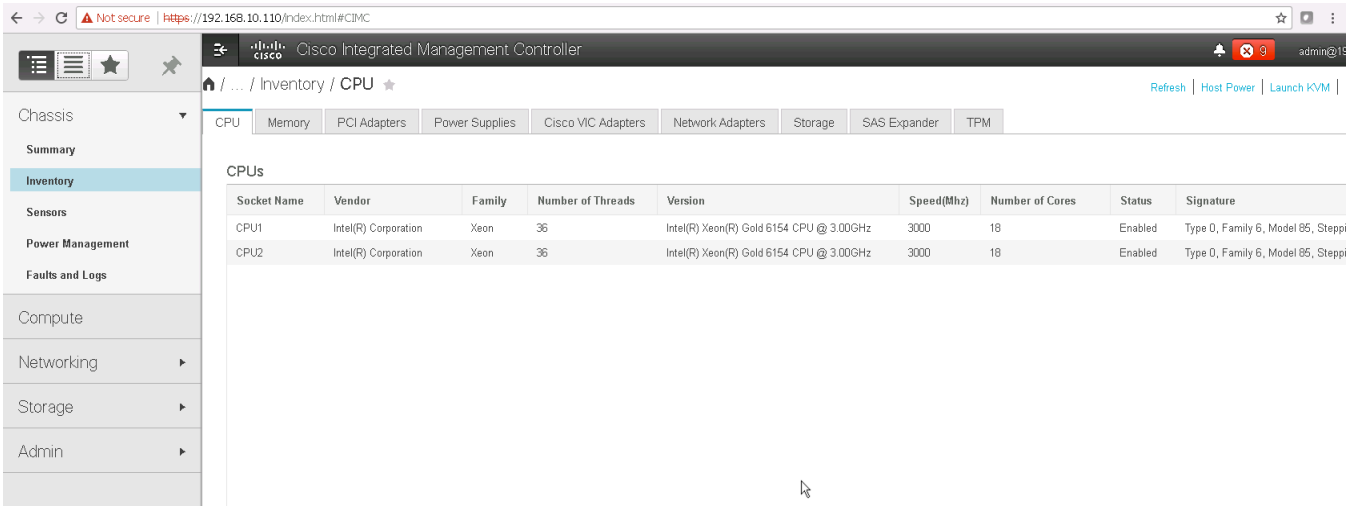
5. The virtual host bus adapter (vHBA) tab summarizes the existing host Fibre Channel interfaces, including the worldwide port name (WWPN) and worldwide node name (WWNN) and information about whether the vHBA is used to boot the system. As a best practice, you should create at least one vHBA per uplink 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.



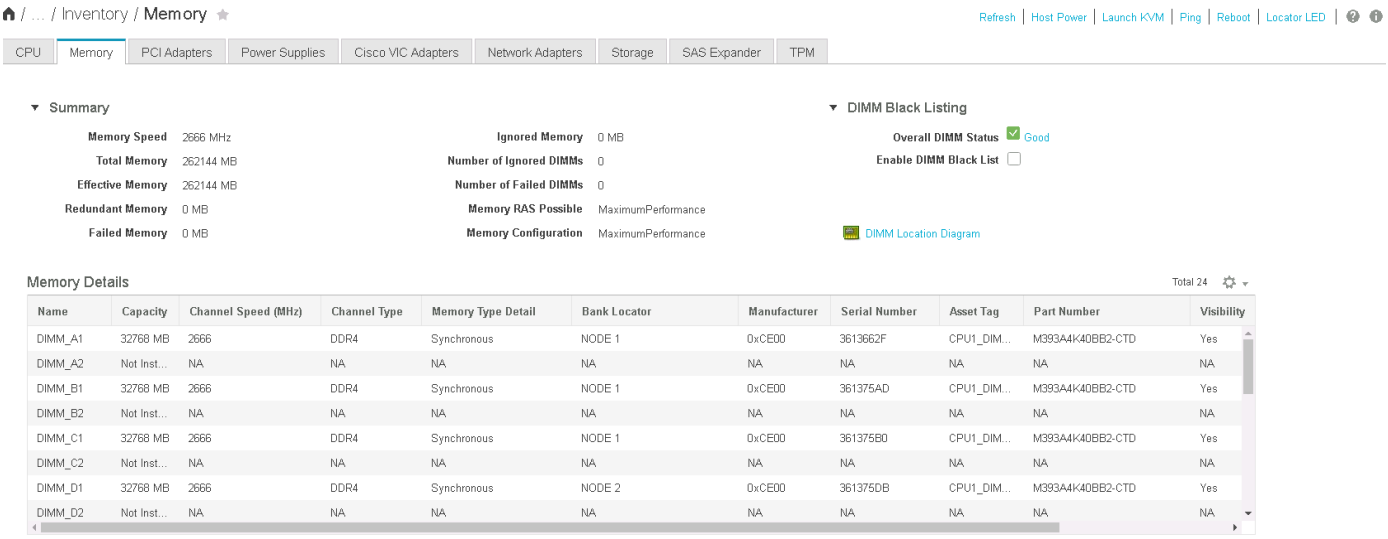
6. Choose Chassis.

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

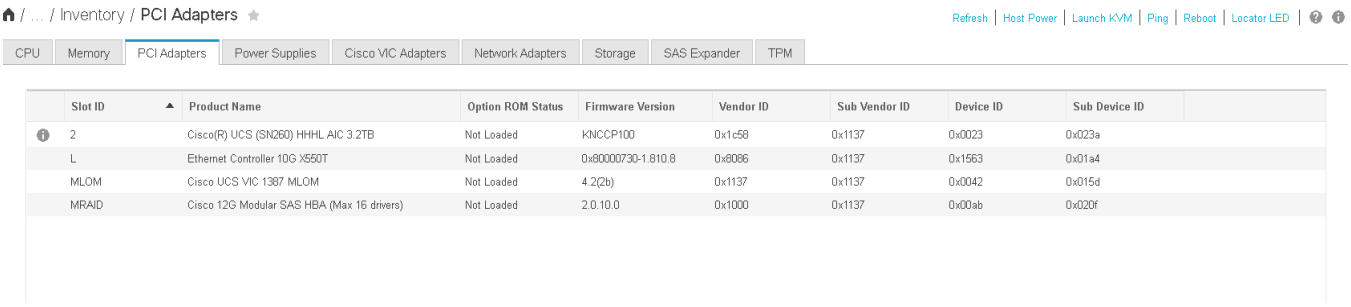
The CPU tab of the Chassis Inventory pane shows the CPUs.



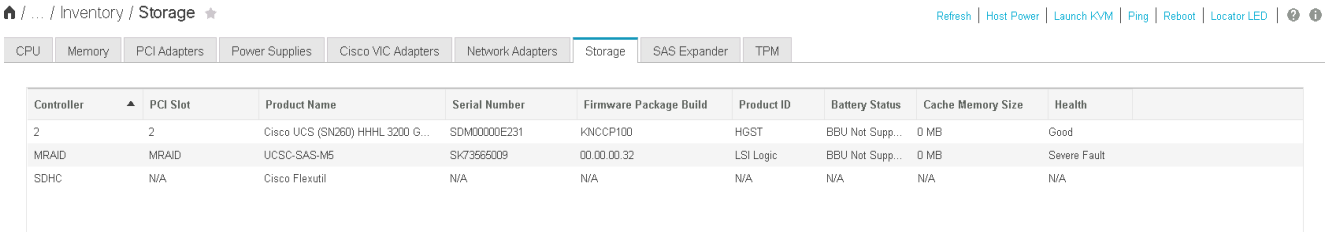
The Memory tab of the Chassis Inventory pane presents memory details.



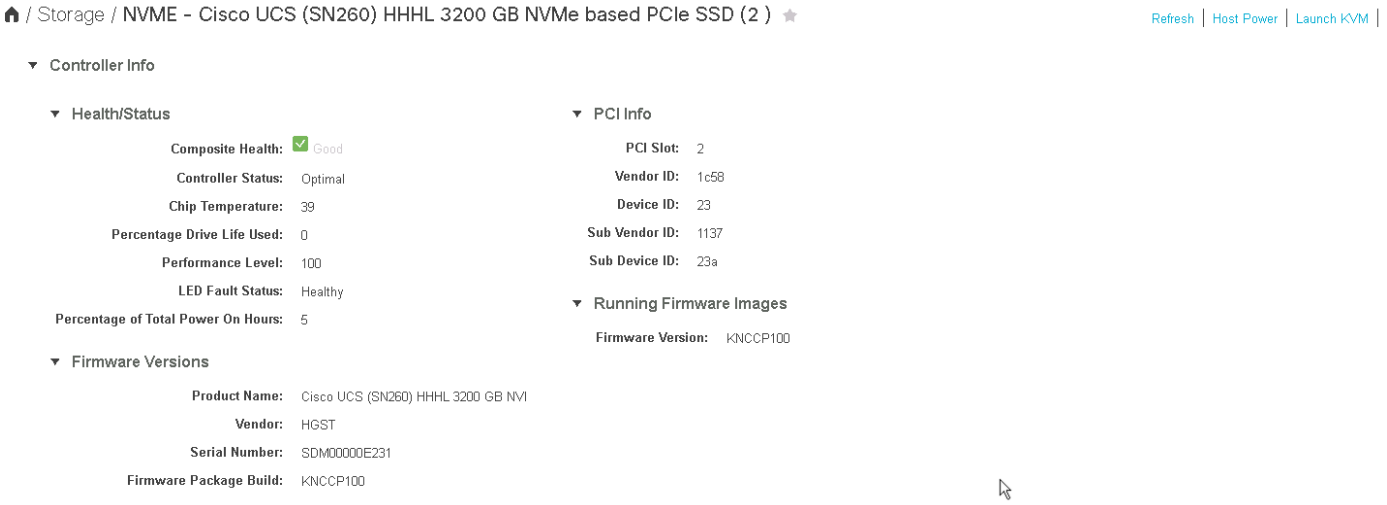
The PCI Adapters tab of the Chassis Inventory pane shows the PCIe adapter information such as the RAID controller and the Cisco VIC.



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



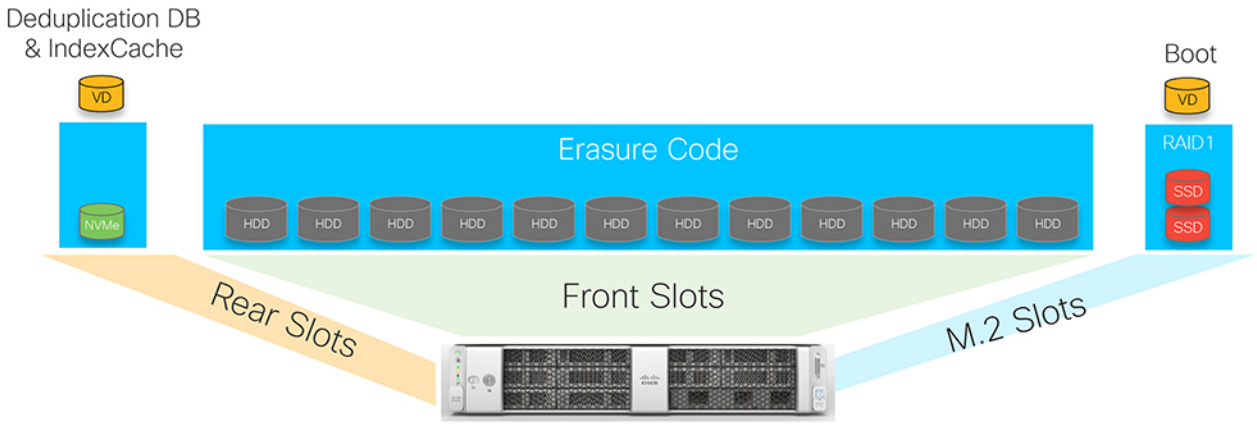
7. On the Storage tab of the Chassis Inventory pane, double-click the first row, which lists the NVMe in the Product Name column, to view the NVMe drive details.



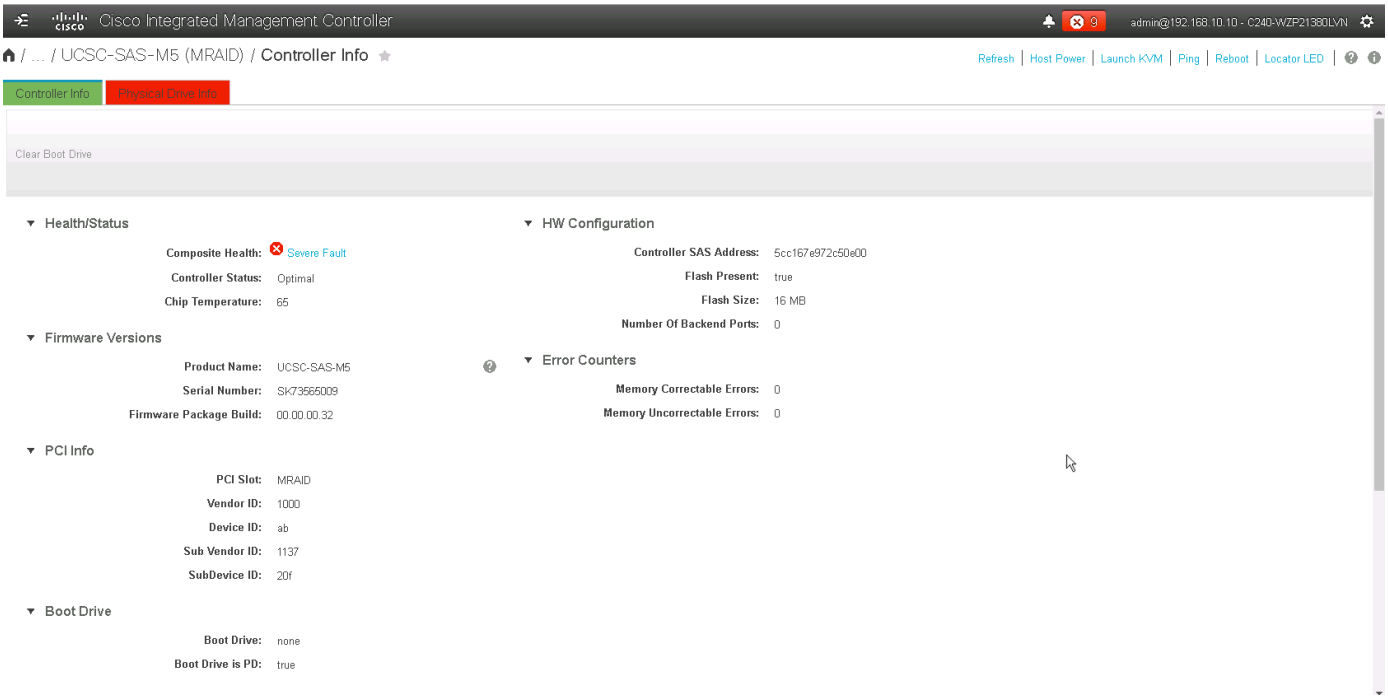
8. Return to the Storage tab of the Chassis Inventory pane and double-click the second row, which lists the Cisco 12-Gbps SAS HBA controller.

   The storage configuration is the most important part of the Cisco UCS C240 M5 configuration for the ScaleProtect with Cisco UCS server. Figure 7 shows the required storage configuration. It shows the HDD and SSD components and the layout.

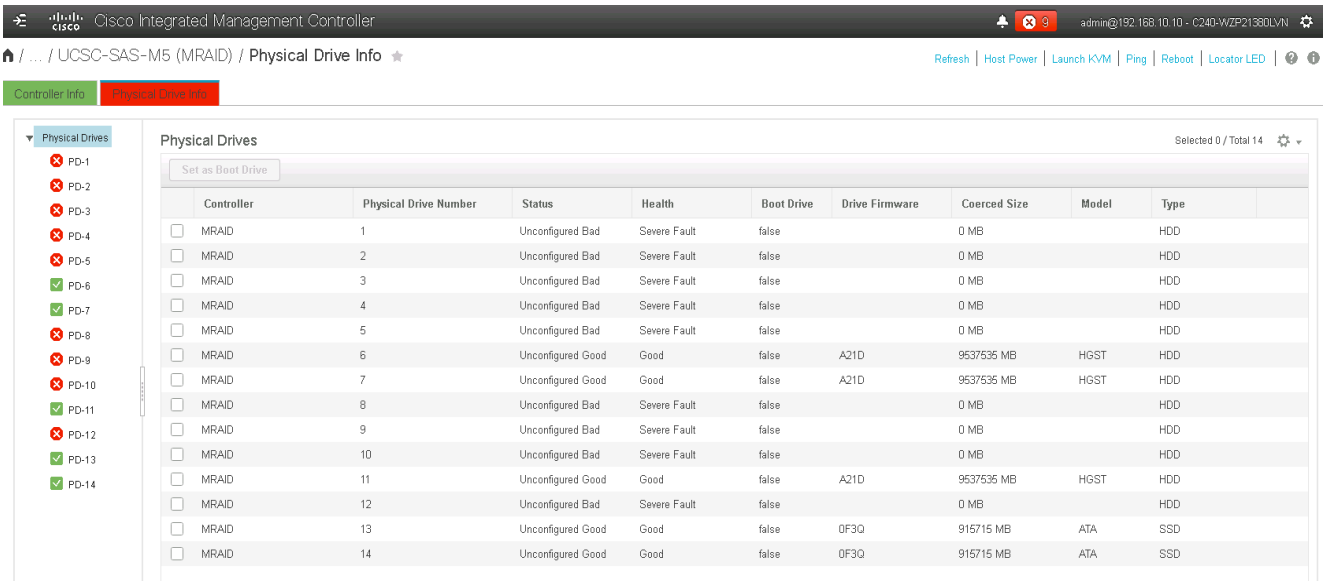
Figure 7. Cisco UCS C240 storage layout



The Controller Info pane shows the controller information.



The Physical Drive Info tab provides information about the physical drives.



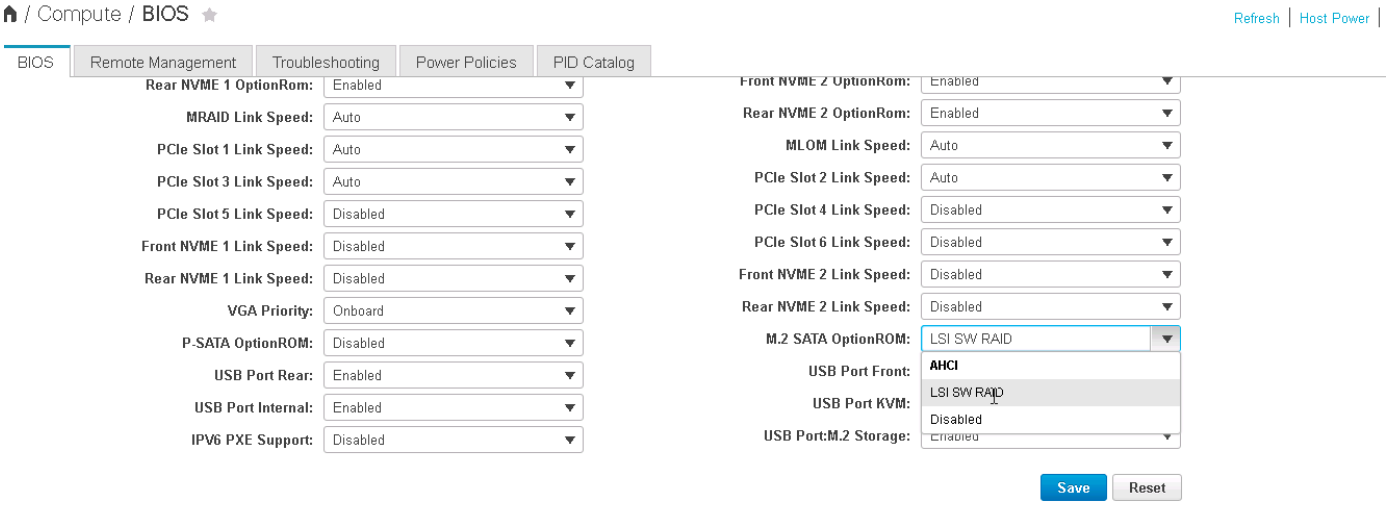
Note: In the Status column, the drives should be listed as Unconfigured Good. The drives can be presented to the hosts only as JBODs, and the controller cannot manage the drives in a RAID configuration.

Note: The current controller firmware has a bug that causes the drives to be listed as faulty and critical errors to be logged. This problem is a cosmetic bug and will be resolved in the next update.

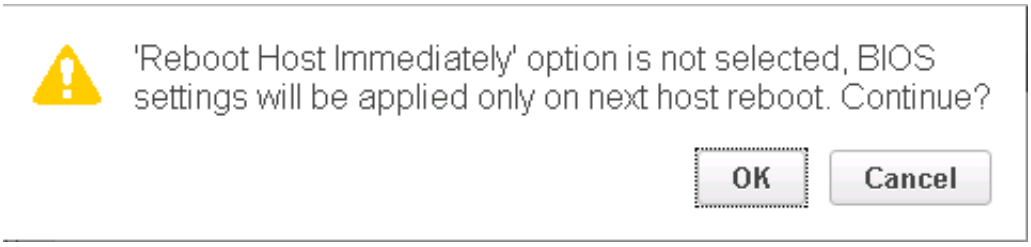
Disk configurations required for ScaleProtect with Cisco UCS installation

You need to create a software RAID 1 logical unit number for boot SSDs. The following procedure creates a software RAID 1 LUN using the internal (embedded) M.2 SSDs. You need to configure the BIOS.

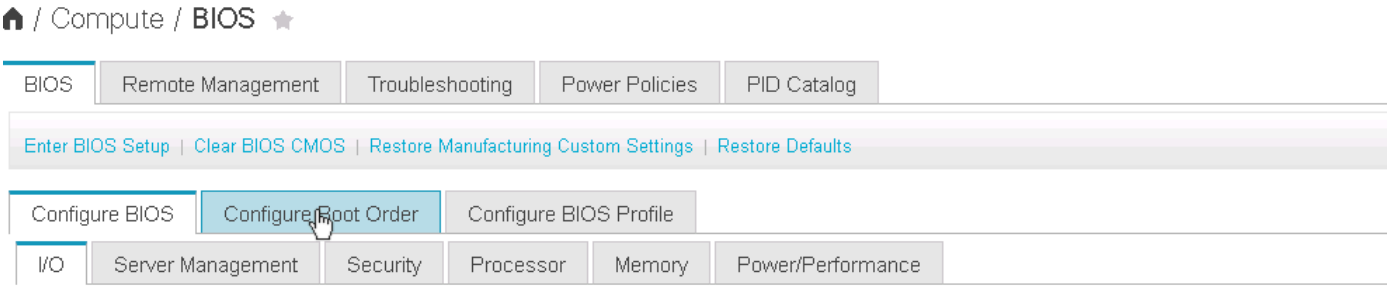
1. At the IMC console, choose Compute in the navigation panel on the left.
2. On the BIOS tab, under Configure BIOS > I/O, choose LSI SW RAID in the drop-down menu for M.2 SATA OptionROM.



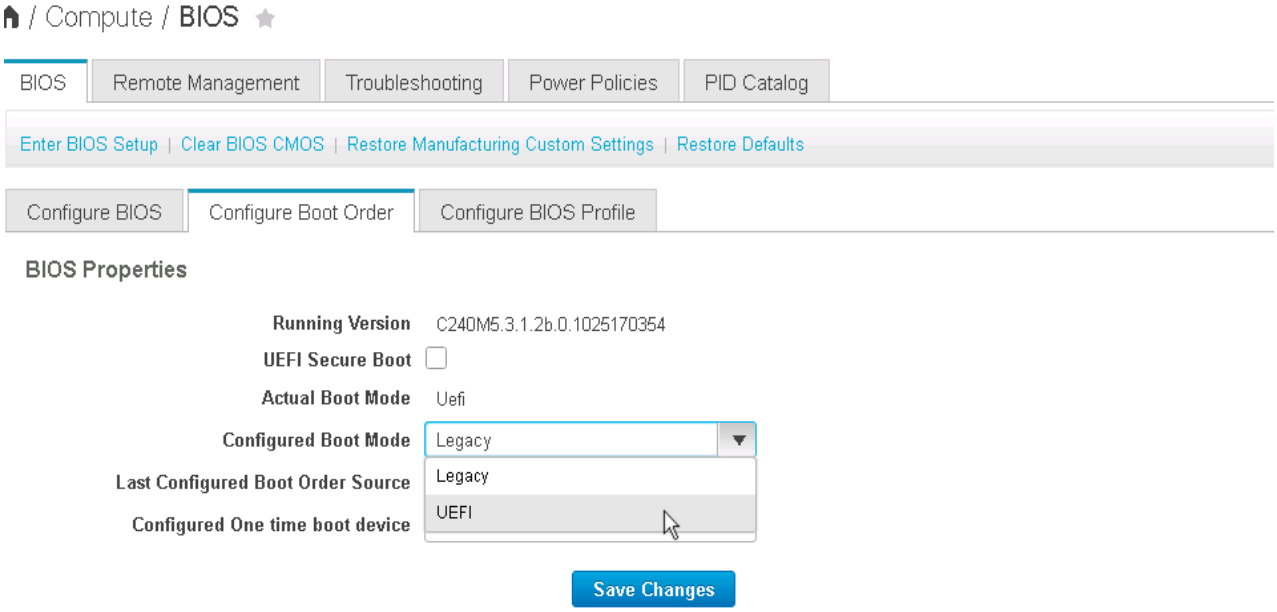
3. When the following message appears, click OK.



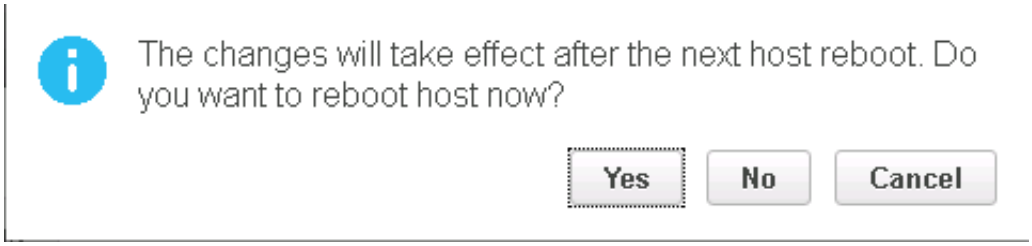
4. Click Configure Boot Order.



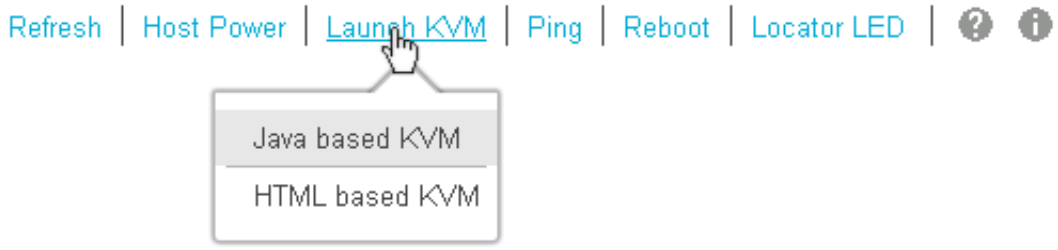
5. In the drop-down menu for Configured Boot Mode, choose UEFI. Then click Save Changes.



6. When the following message appears, click Yes to reboot the host.



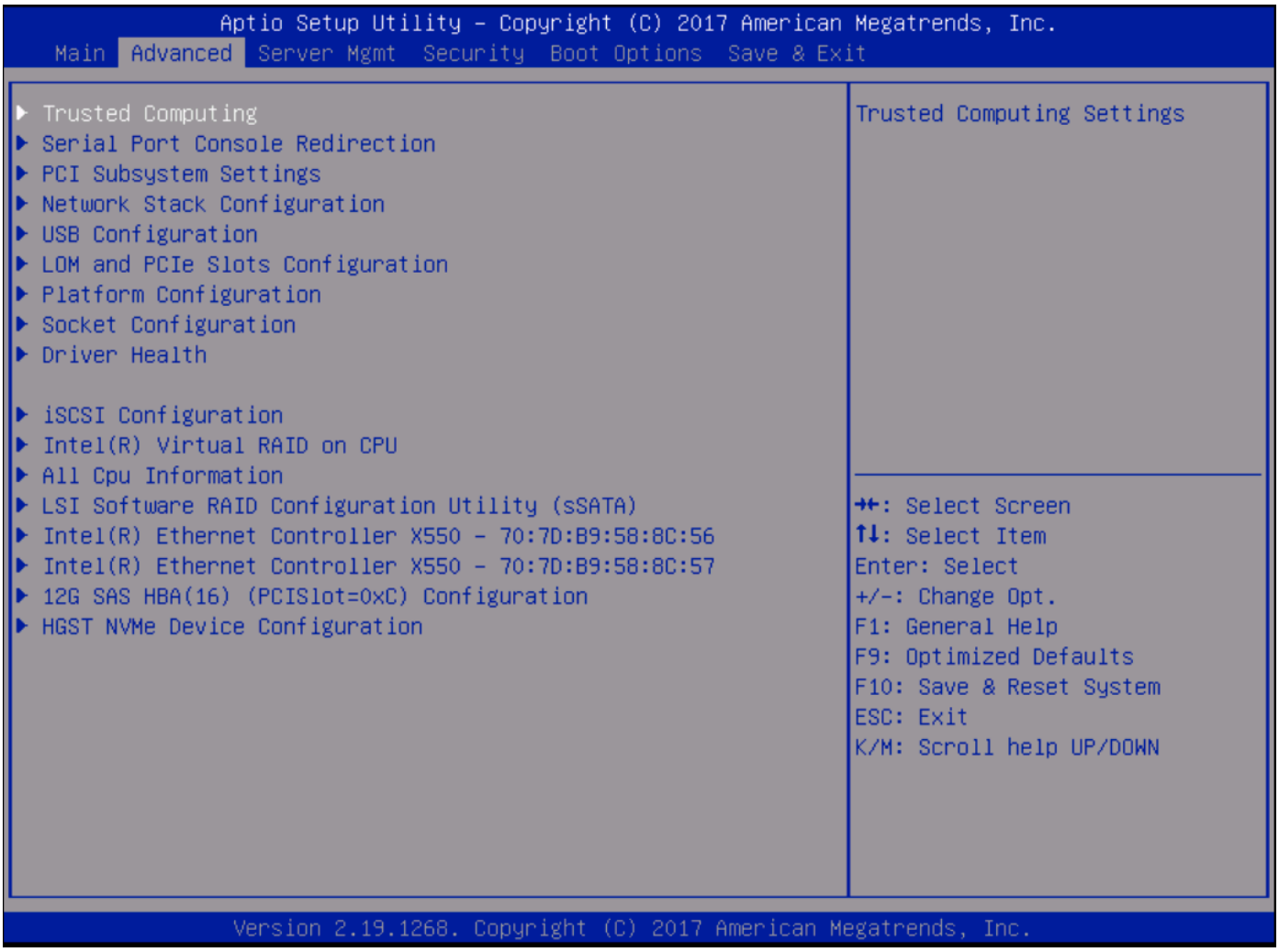
7. In the top-right corner of the IMC webpage, click Launch KVM.



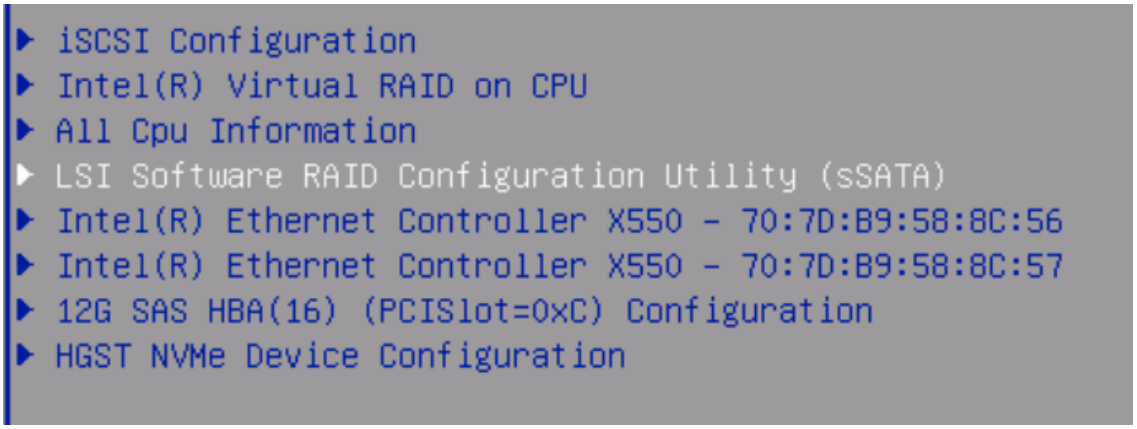
8. Choose “Java based KVM” and access the server console.

9. While accessing the console, press the F2 key to enter the BIOS setup utility.

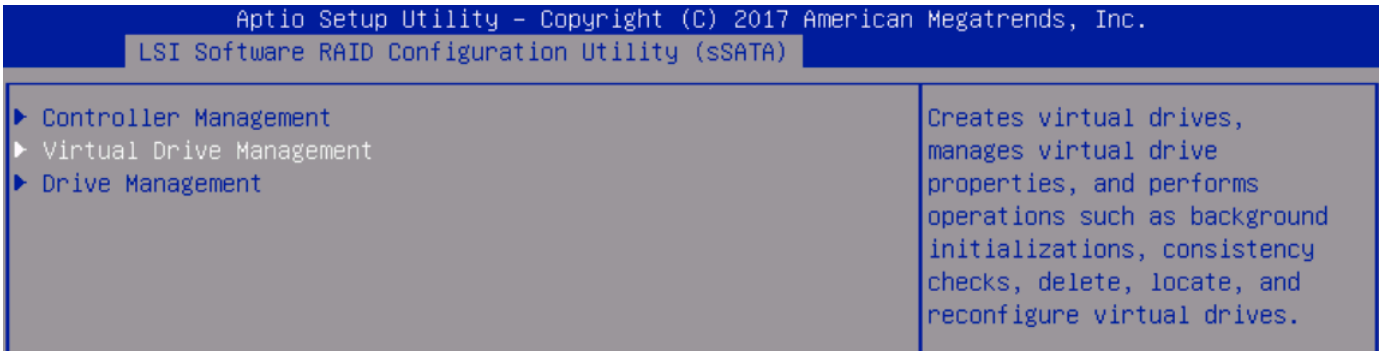
10. In the BIOS utility, use the right arrow on the keyboard to choose the Advanced tab.



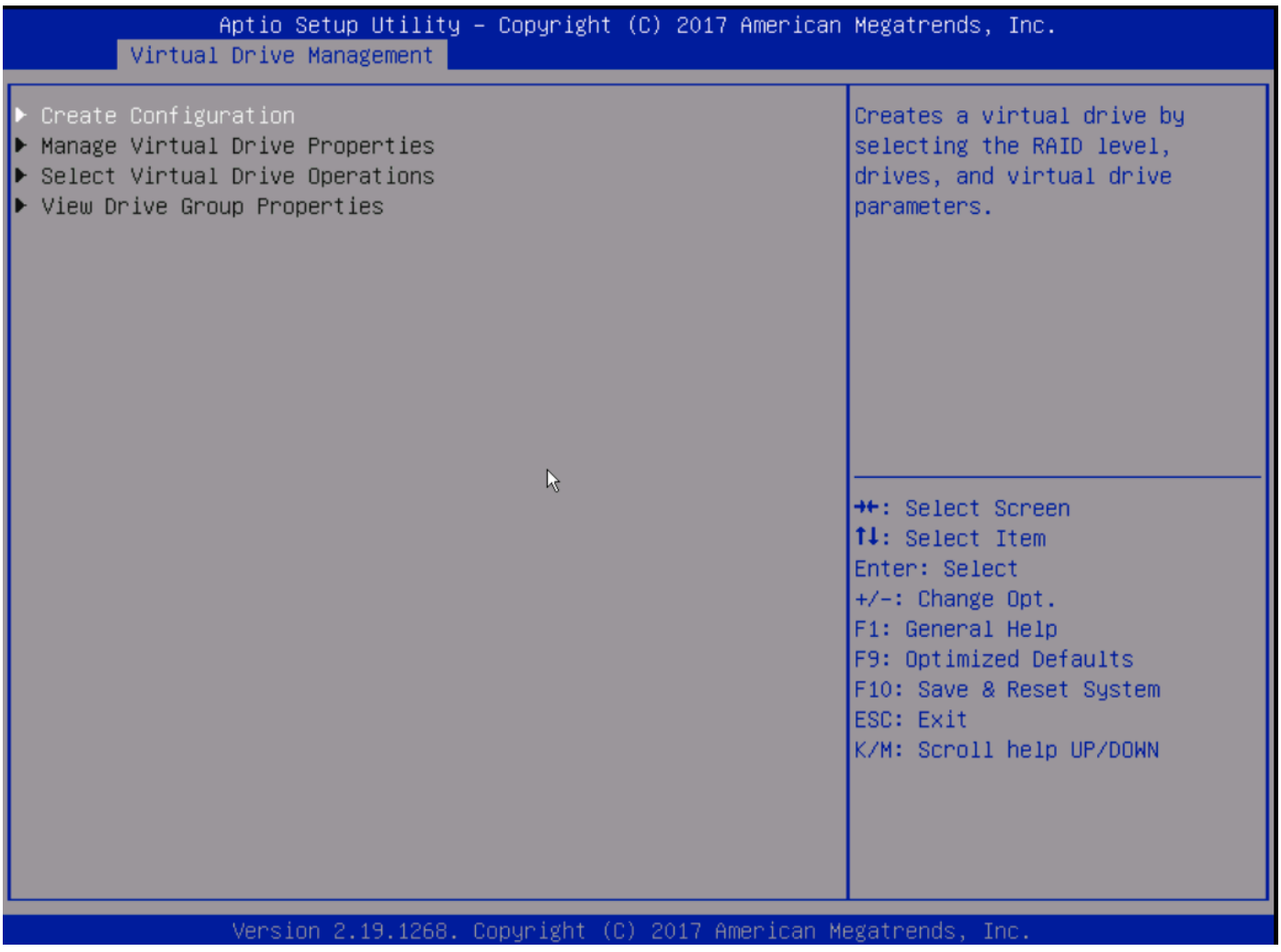
11. Select LSI Software RAID Configuration Utility (sSATA) and press Enter.



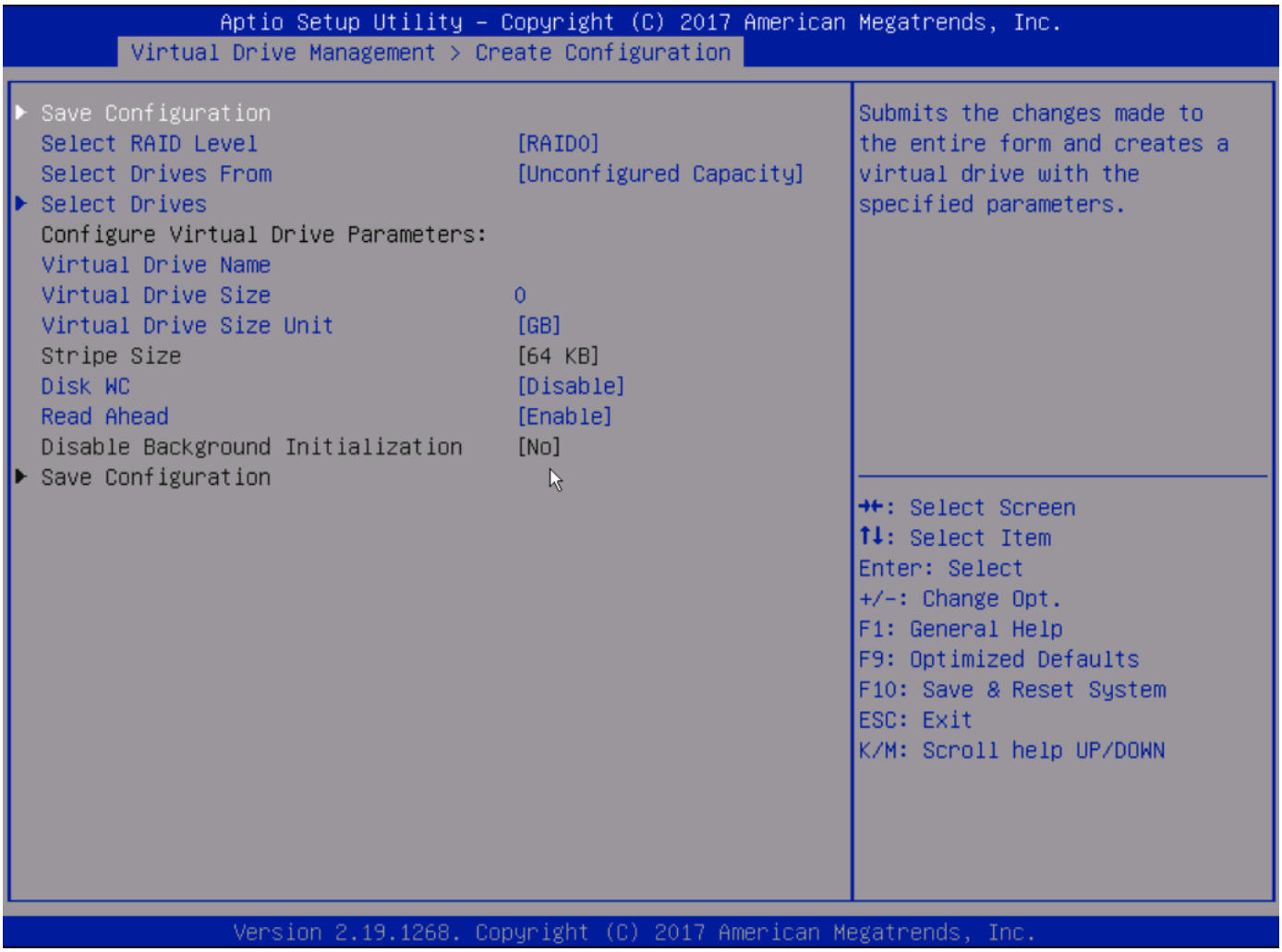
12. Select Virtual Drive Management.



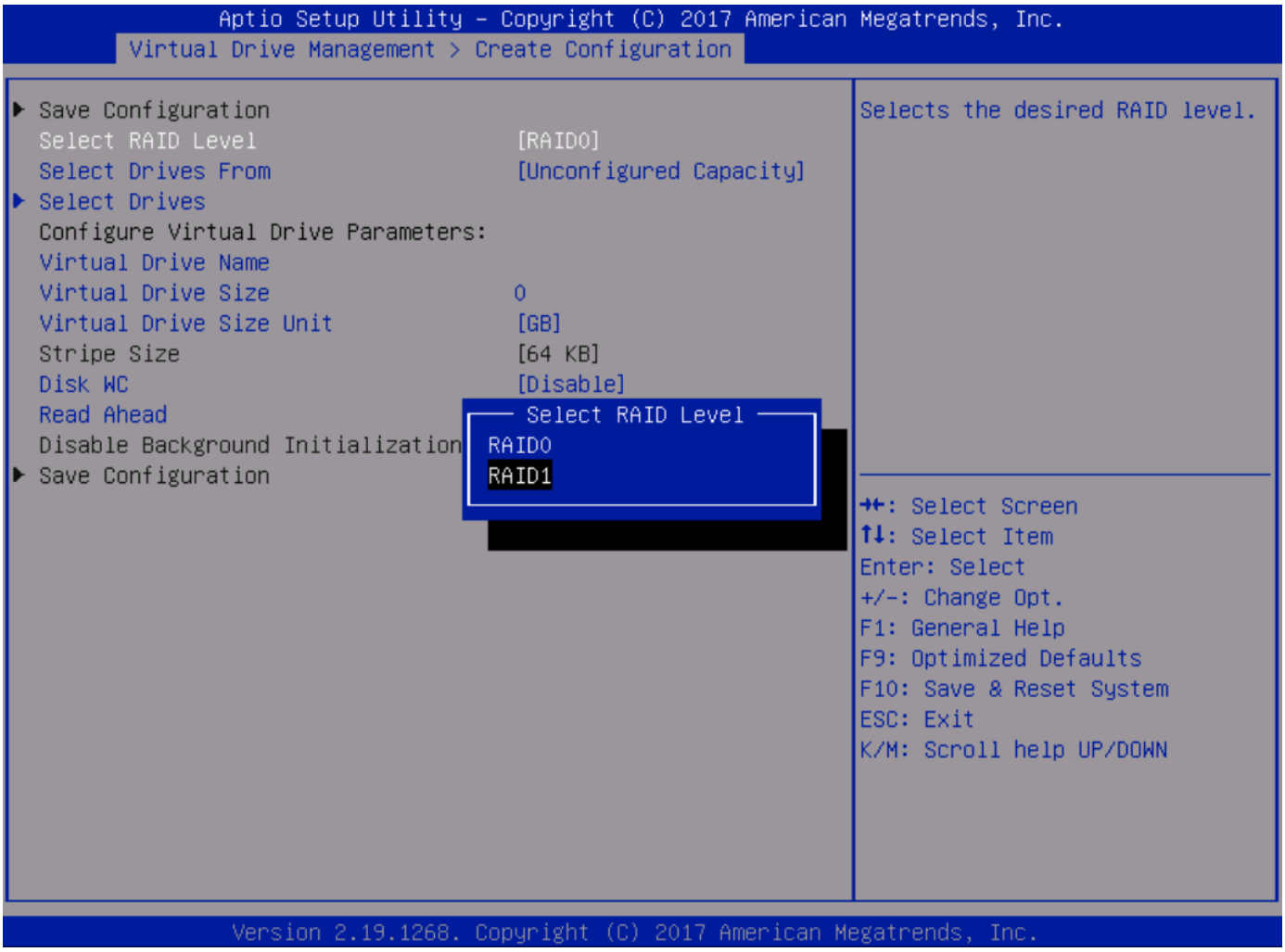
13. Select Create Configuration and press Enter.



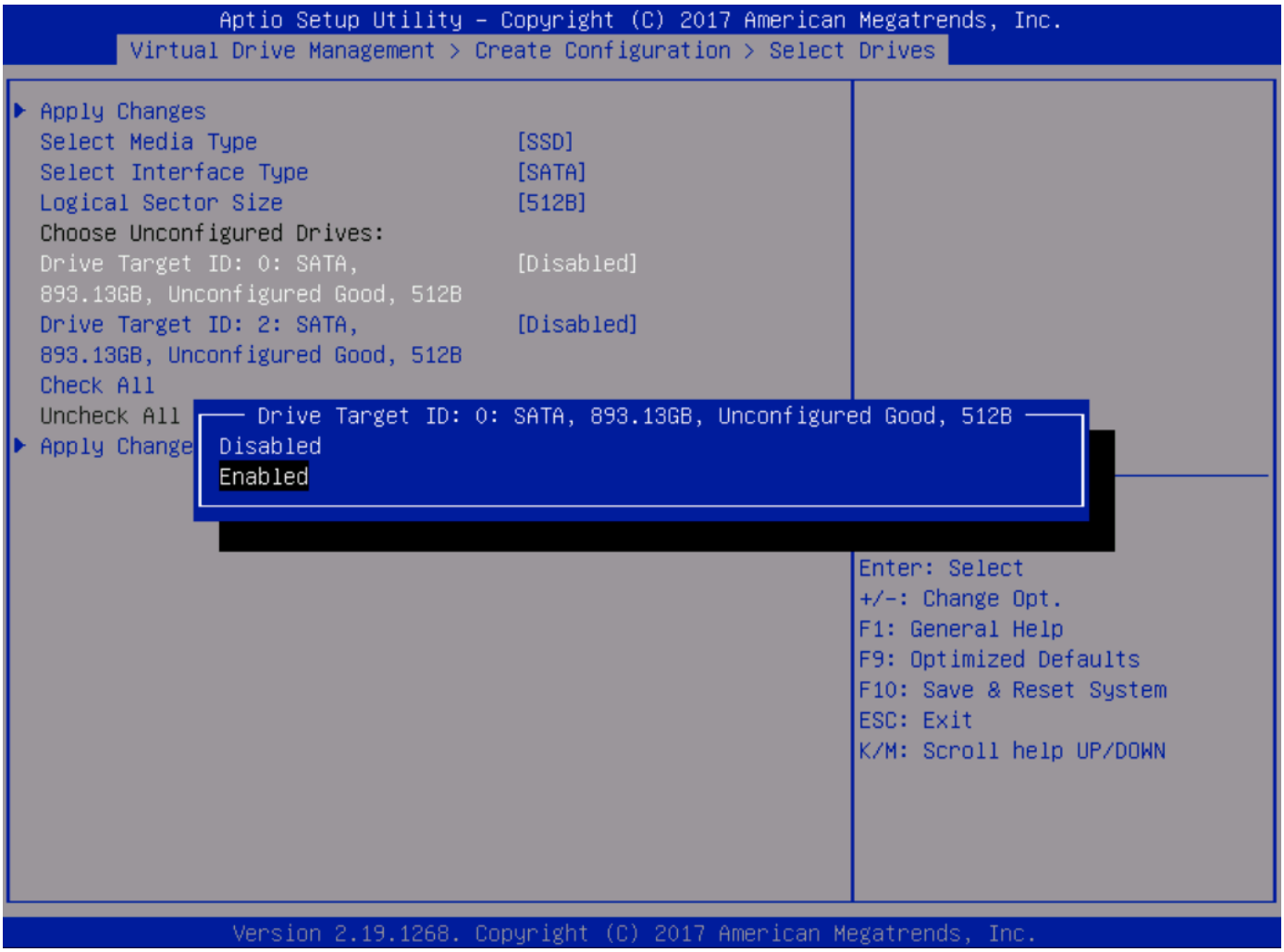
14. Select the Select RAID Level option and press Enter.



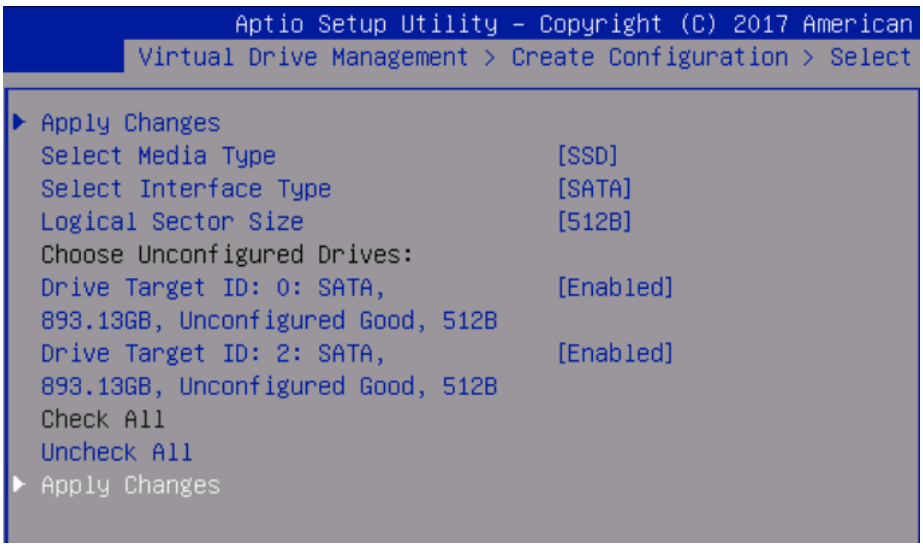
15. Select RAID1 as the RAID level.



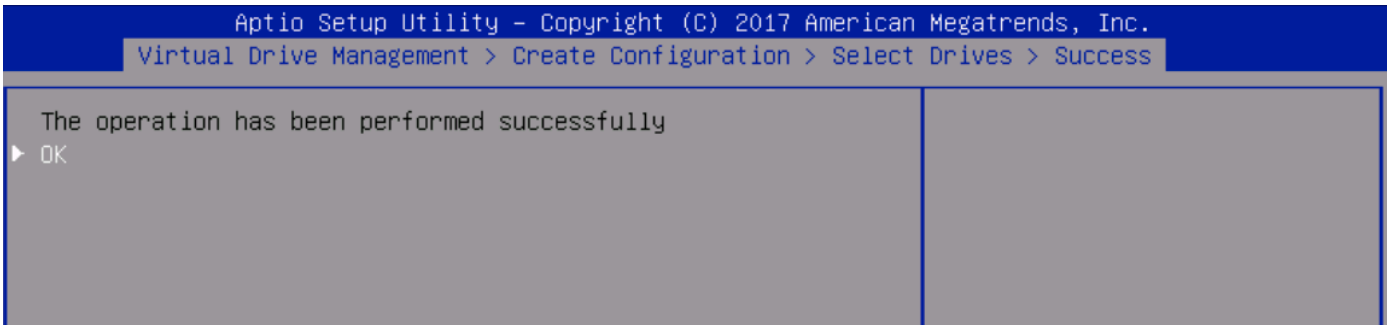
16. Select the Select Drives option and press Enter to expand drop-down menu. Enable the two embedded M.2 drives.



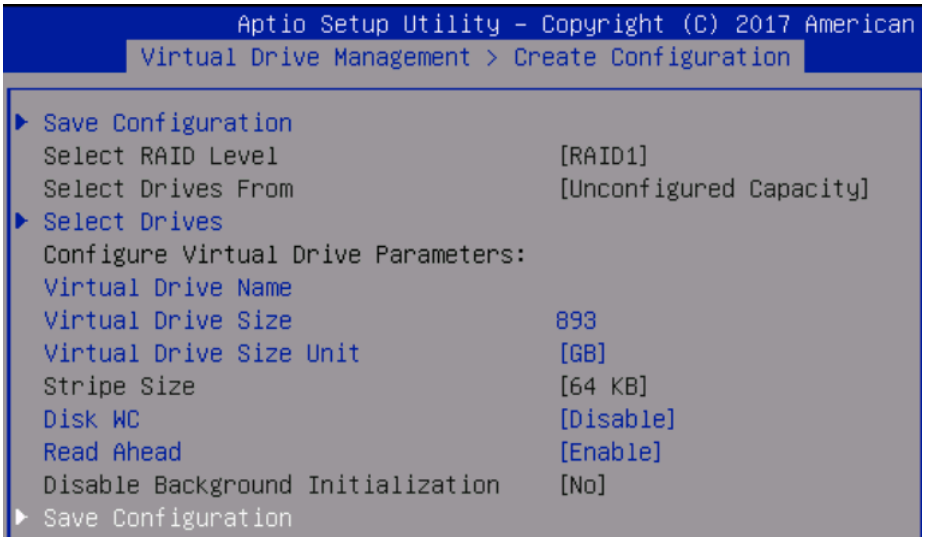
17. Select Apply Changes.



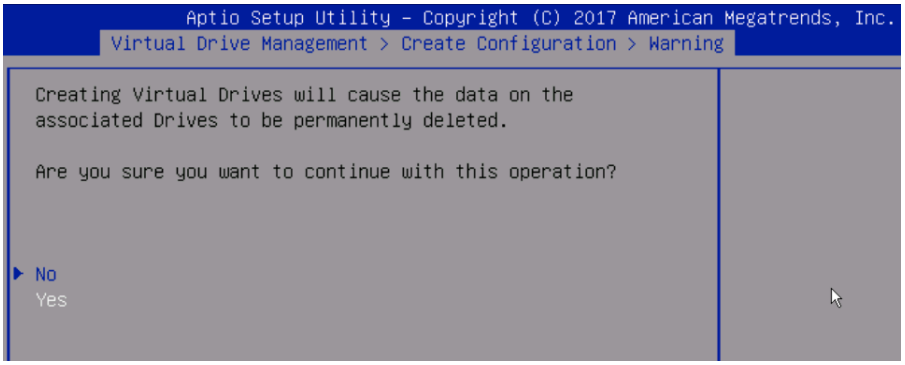
18. On the next screen, select OK.



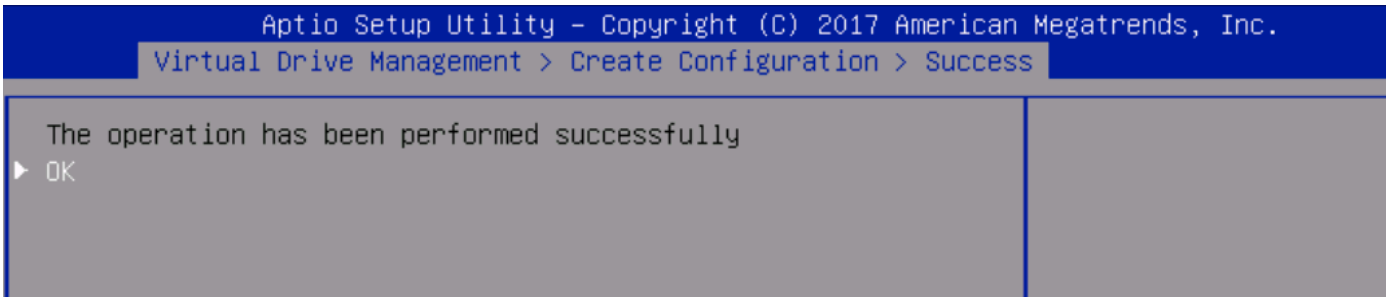
19. Select Save Configuration.



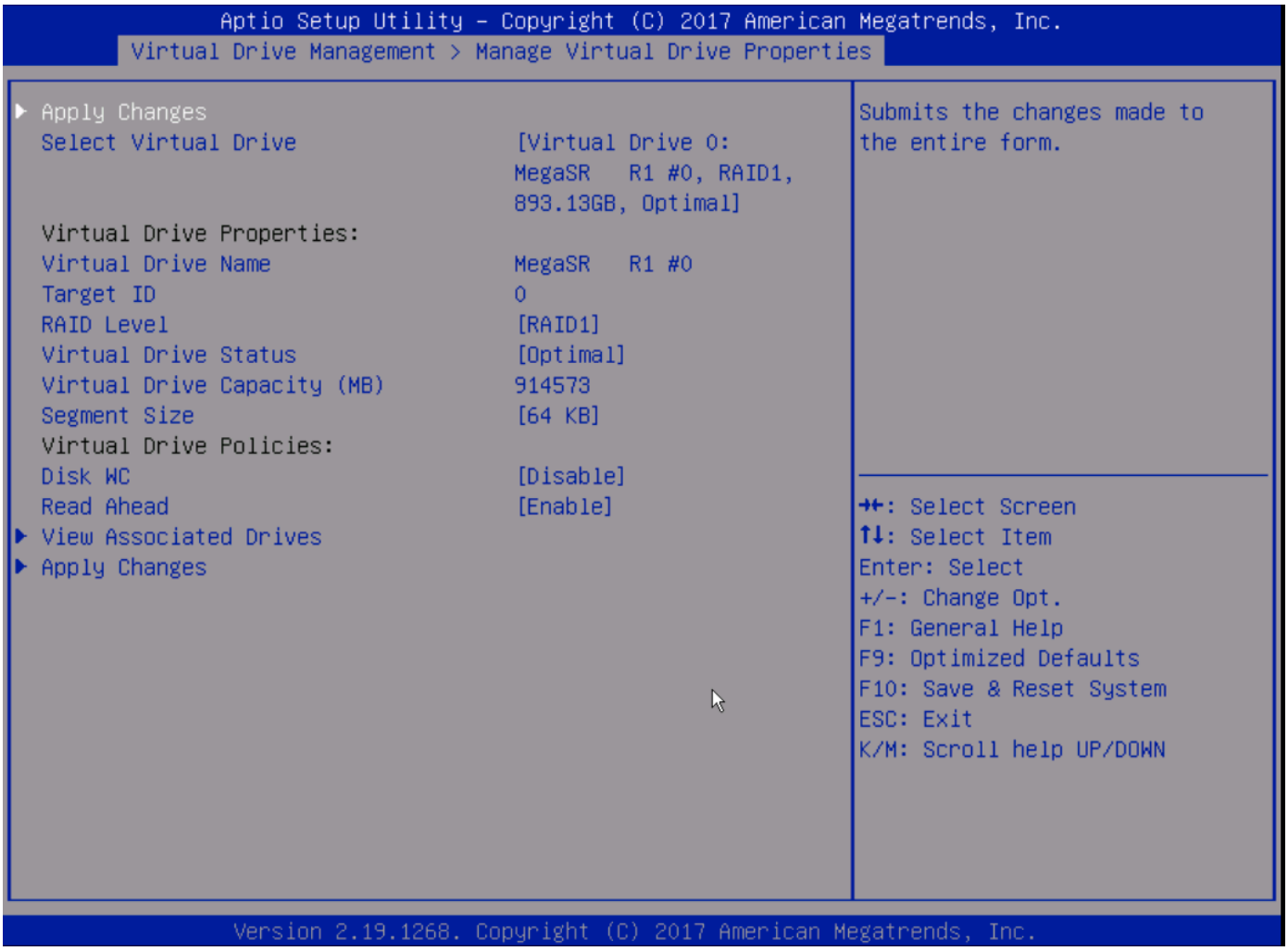
20. Select Yes to continue with virtual drive creation.



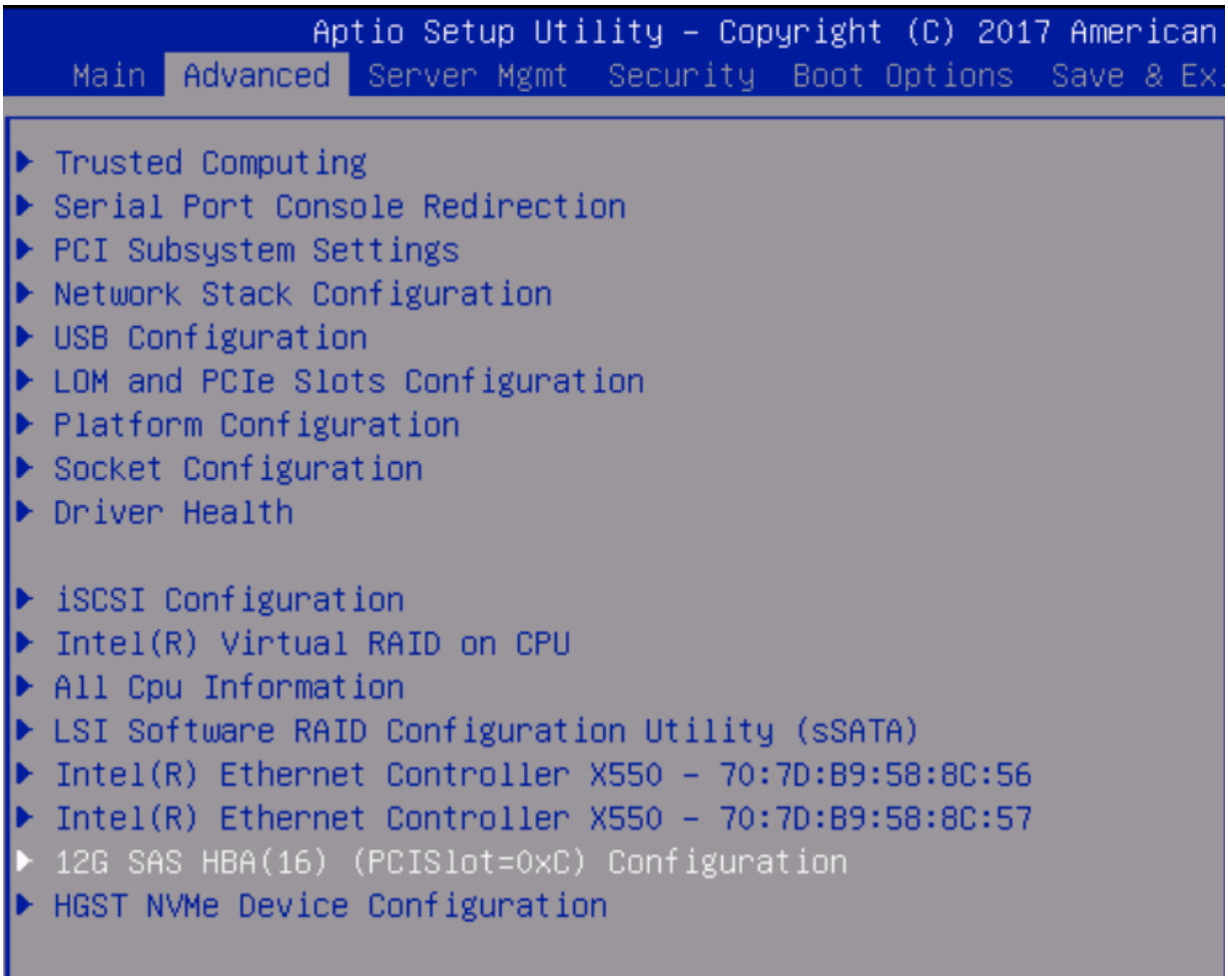
21. Select OK after the operation is completed.



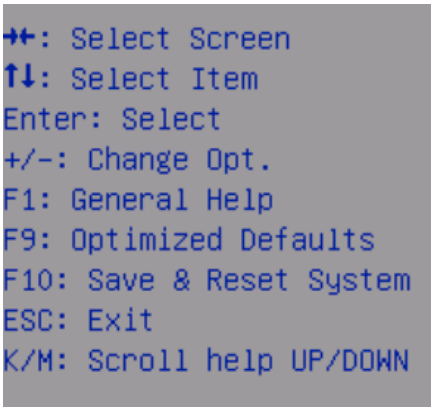
22. Verify the details of the virtual drives created in the previous steps.



23. Verify the status of the NVMe and the other disk drives by selecting the appropriate controller from the Advanced tab.



24. Press F10 to save your changes and reset the system to boot from the software RAID 1 device you have created.



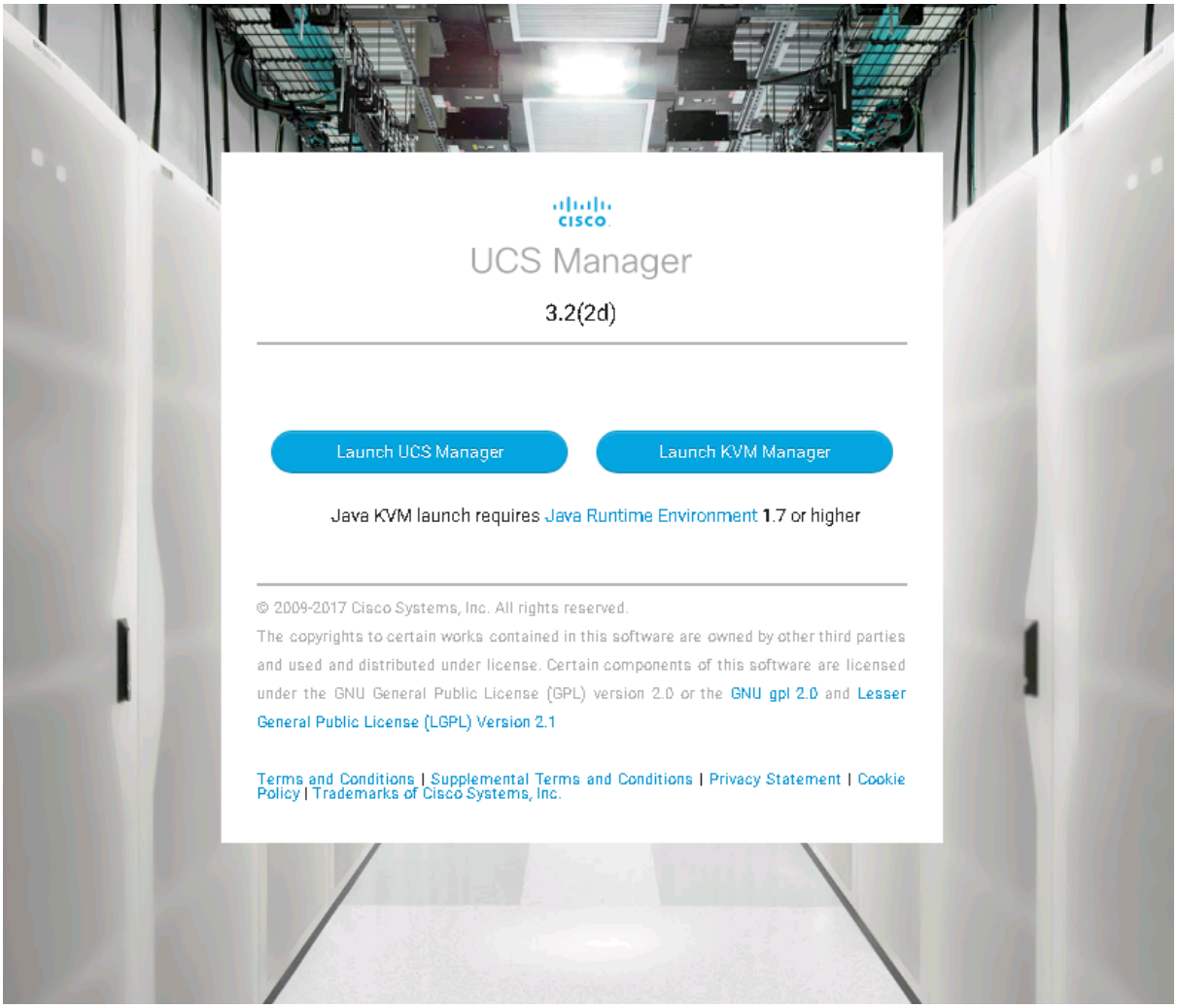
The server is now ready to load the OS.

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

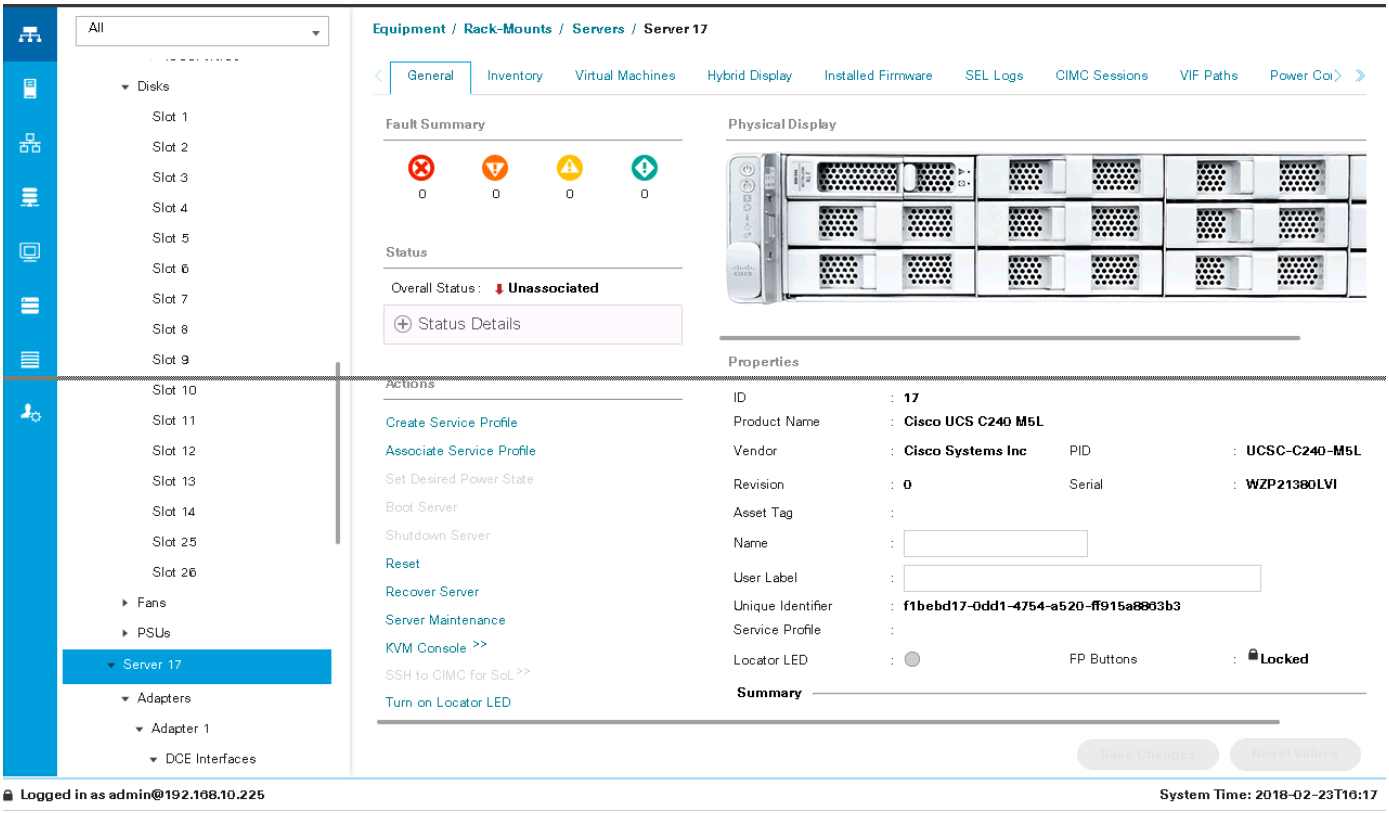
Cisco UCS managed configuration with Cisco UCS Manager

The following section describes the configuration of the Cisco UCS C240 M5 server managed through Cisco UCS.

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

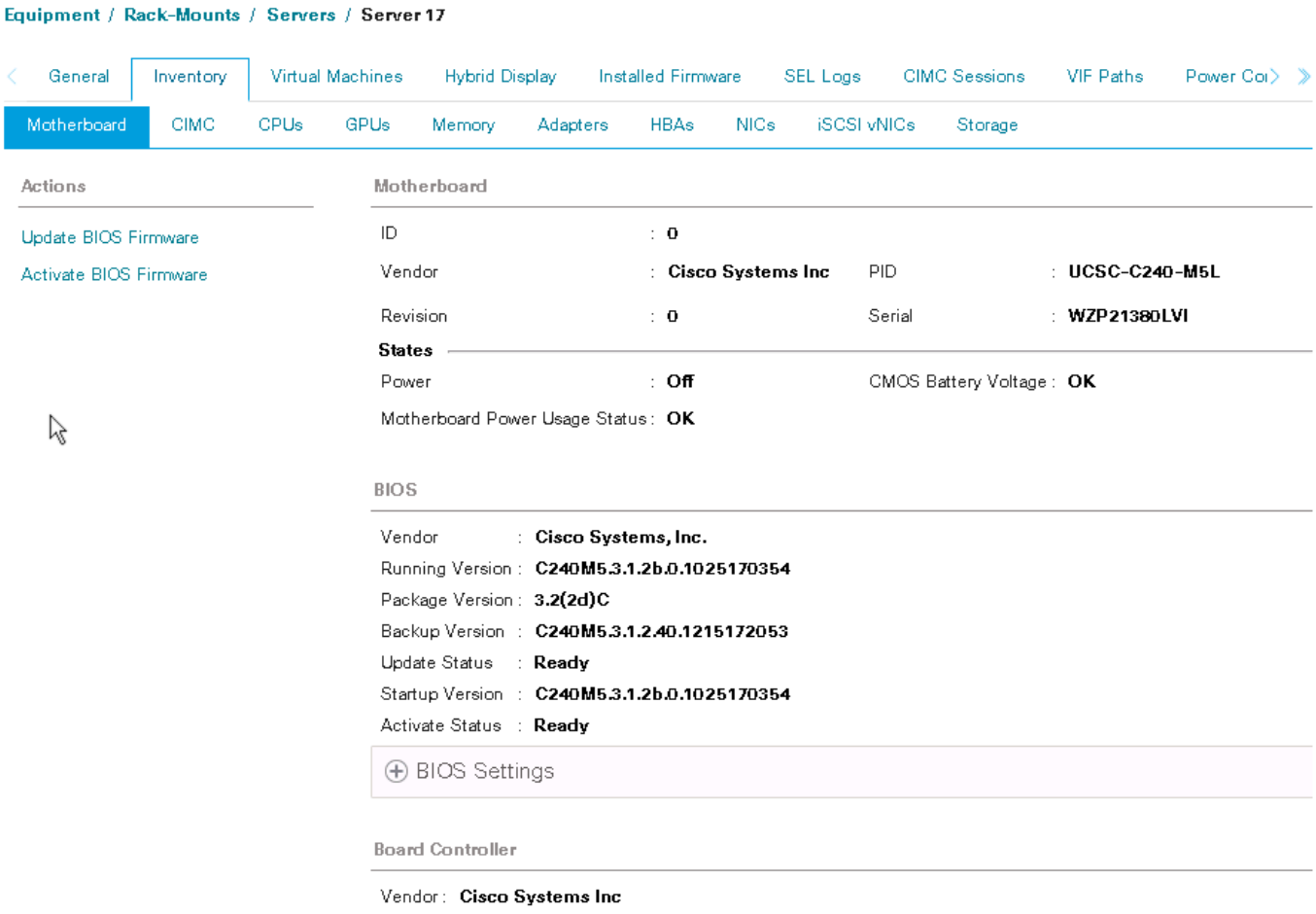


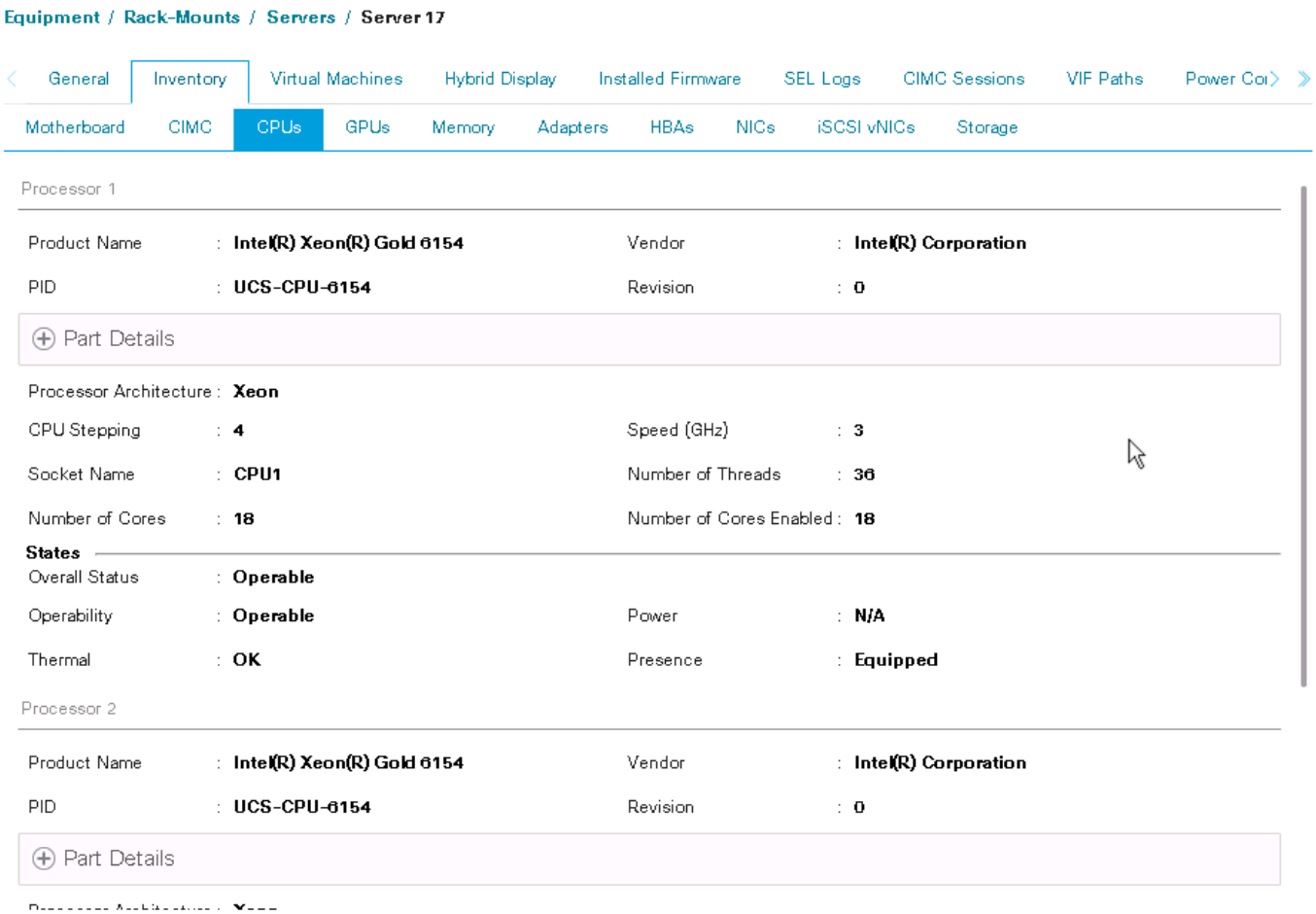
2. On the Equipment tab, identify the Cisco UCS C240 M5 server and check the condition of the system and the components required for the deployment.

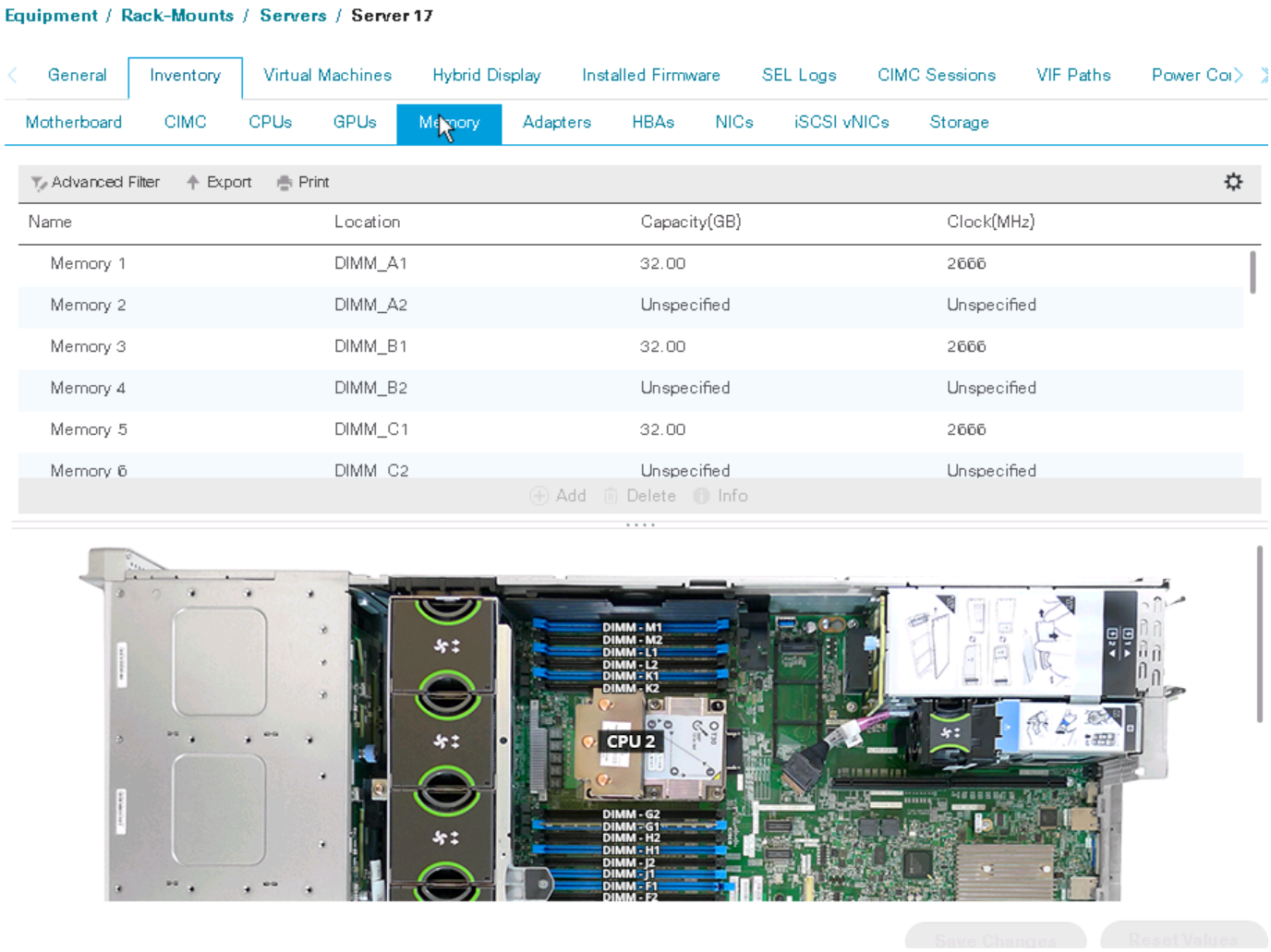


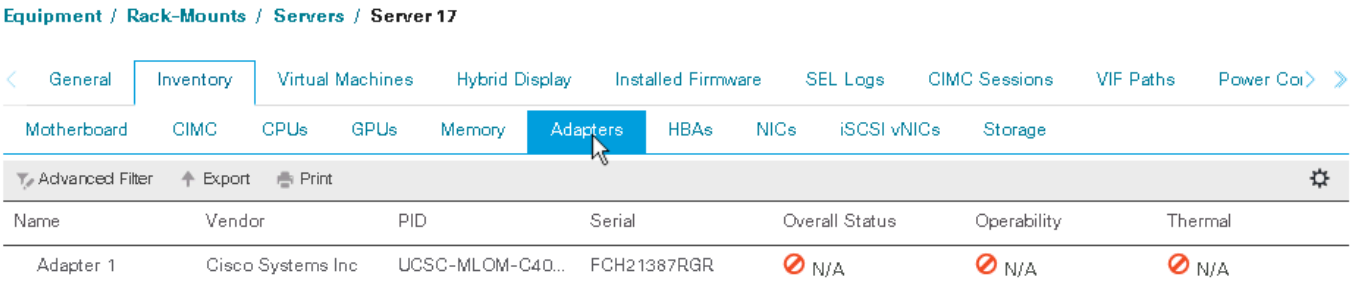
3. Check the server information.

   The Inventory tab shows the details of the server, including information about the CPU, memory, PCIe cards, and local storage.

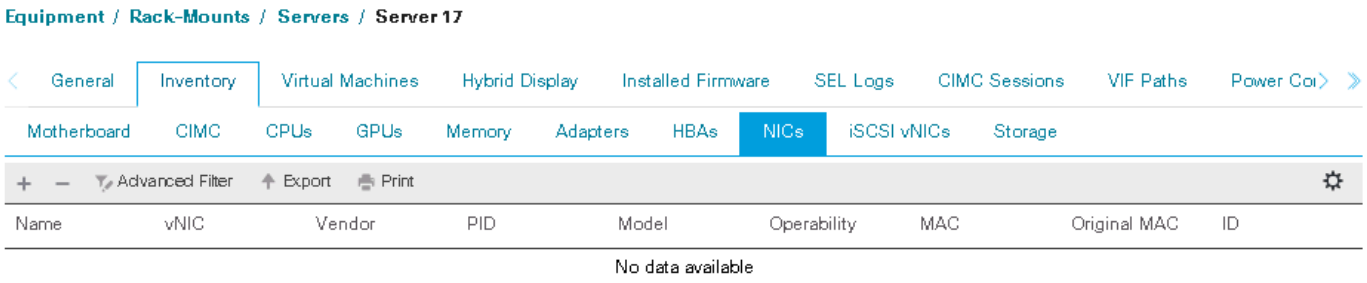


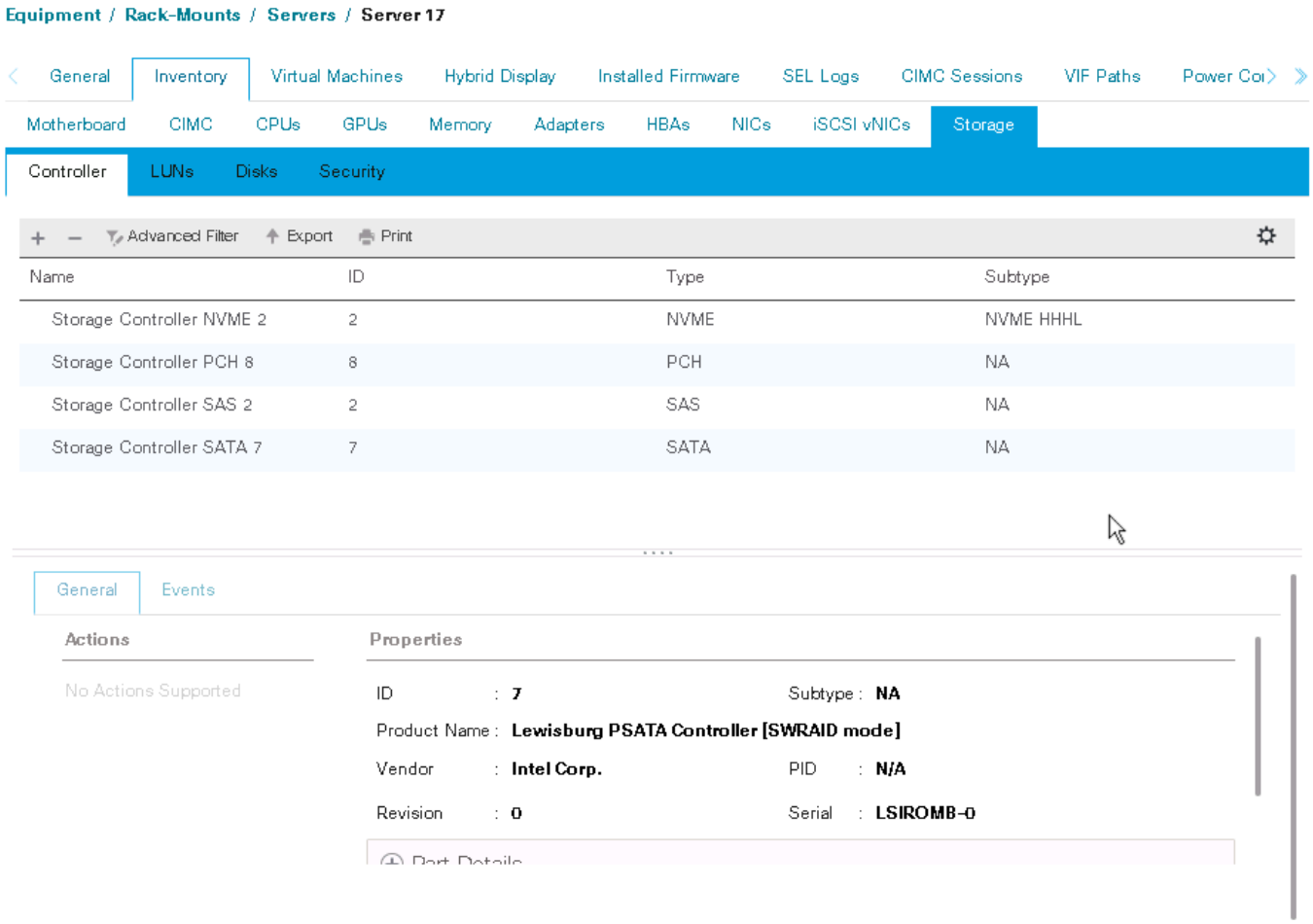






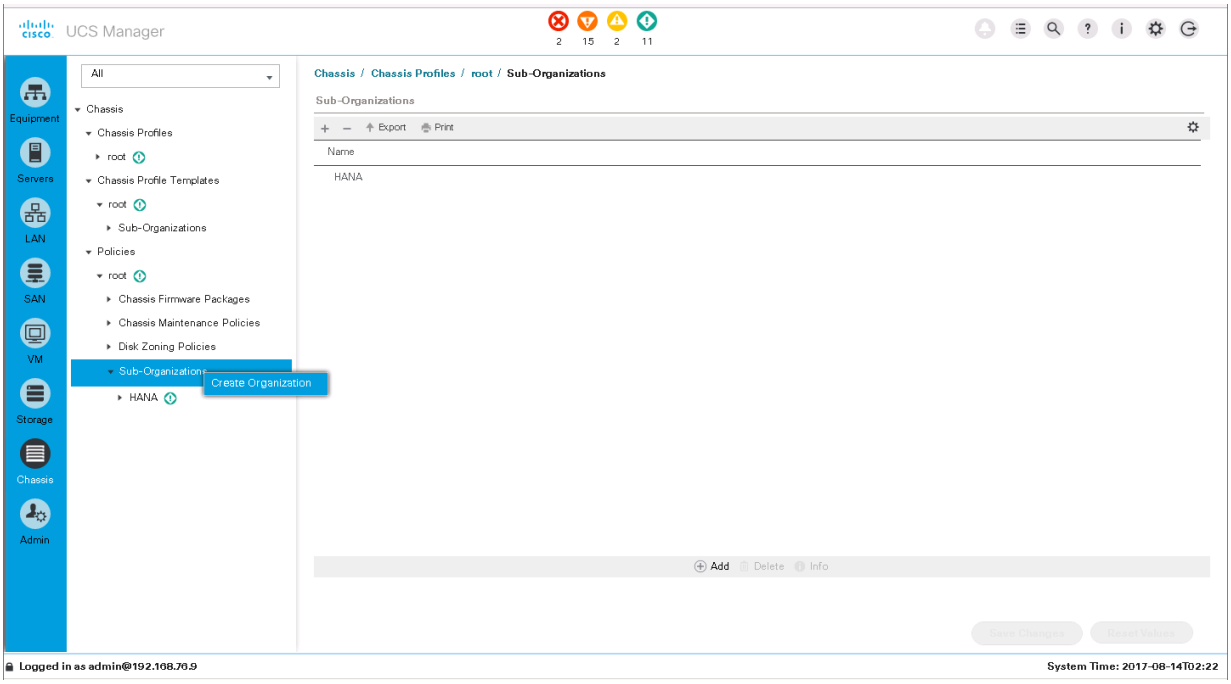
In a standalone configuration, the adapter includes predefined vNICs and vHBAs. In a configuration managed by Cisco UCS, however, nothing is defined. This definition is part of the service profile configuration. If PCIe cards for networking or Fibre Channel are installed, the information is listed on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



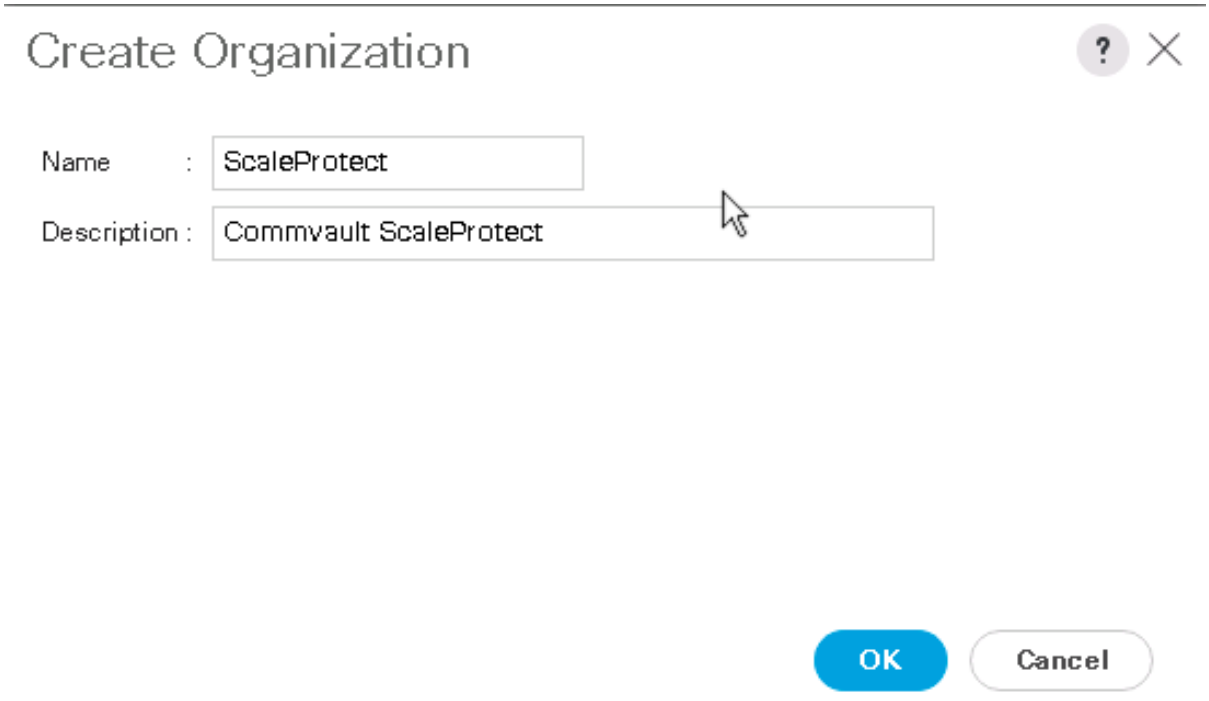


The Cisco UCS Manager configuration for the ScaleProtect with Cisco UCS server is specific to the use case, so you could optionally define a new suborganization for Commvault (ScaleProtect) to keep all configurations dedicated to this use case.

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



5. Enter an obvious name, such as **ScaleProtect**, enter a description, and click OK. You can use any name for the suborganization based on the naming conventions preferred at the deployment site.



Note: If you create a suborganization, all the tasks described here that are usually performed under the root organization must be performed under the suborganization you created.

Setting up the Cisco UCS C240 M5 server

The next steps are dependent on the available disk drives on the Cisco UCS C240 M5 used for ScaleProtect with Cisco UCS. To complete the storage configuration discussed earlier in this document, you need to identify the physical disks available for the operating system installation and disk library.

For a configuration with 12 disk drives for disk library, use the steps presented here.

The Cisco UCS C240 rack server will use a storage profile similar to that for the Cisco UCS S3260 Storage Server, but it will not need a controller definition, because the C240 in the environment has all disks in front-facing drive slots. Two disk policies need to be created for local LUNs to use for the boot device and disk library for the MediaAgent, and others can be created if additional local LUNs are needed.

The ScaleProtect with Cisco UCS architecture with the C240 M5 servers uses the internal M.2 SSD drives. These drives are managed by the software RAID controller in Cisco UCS, and server will boot to the internal M.2 SSDs in a software RAID 1 configuration.

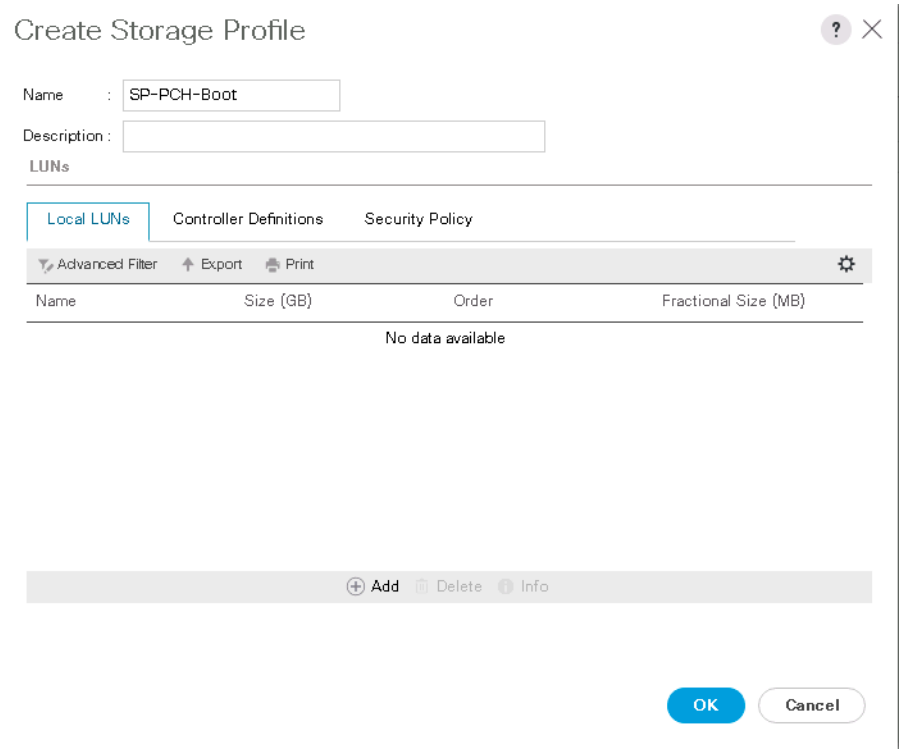
The storage profile consists of storage polices used for creating local LUNs from the allocated disks (disk group policies). Because the C240 M5 server for ScaleProtect with Cisco UCS uses internal M.2 SSDs for boot and the NVMe for the cache (deduplication database and the index cache) and the other HDDs as JBODs attached to the SAS HBA, you need to a create only a storage profile with the controller definition created to boot from software RAID.

All the other drives will be presented to the ScaleProtect with Cisco UCS nodes as JBODs.

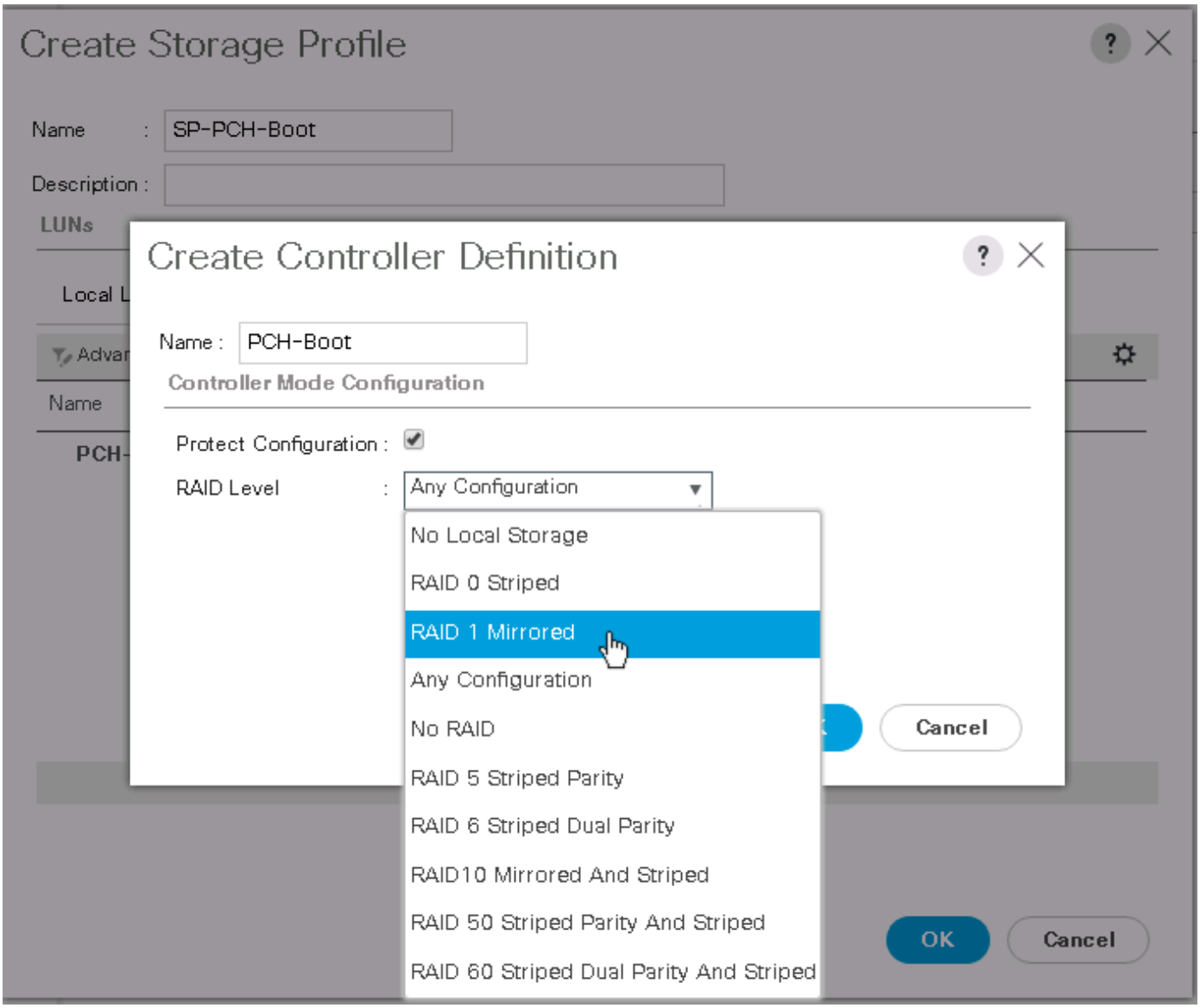
Creating the ScaleProtect with Cisco UCS server storage profile

To create the ScaleProtect with Cisco UCS server storage profile, perform the following actions:

1. In Cisco UCS Manager, in the navigation pane, click Storage and choose Storage Profiles from the Storage pull-down menu.
2. Right-click and choose Create Storage Profile.
3. Provide a name for the storage profile, such as **SP-PCH-Boot**.



4. Click the Controller Definitions tab.
5. Select Add to add a controller definition that will be create a software RAID 1 LUN for booting the operating system.
6. In the Create Local LUN dialog box, specify these options:
   a. For Name, enter **PCH-Boot**.
   b. Leave Protect Configuration checked.
   c. From the RAID Level Configuration pull-down menu, choose RAID 1 Mirrored.

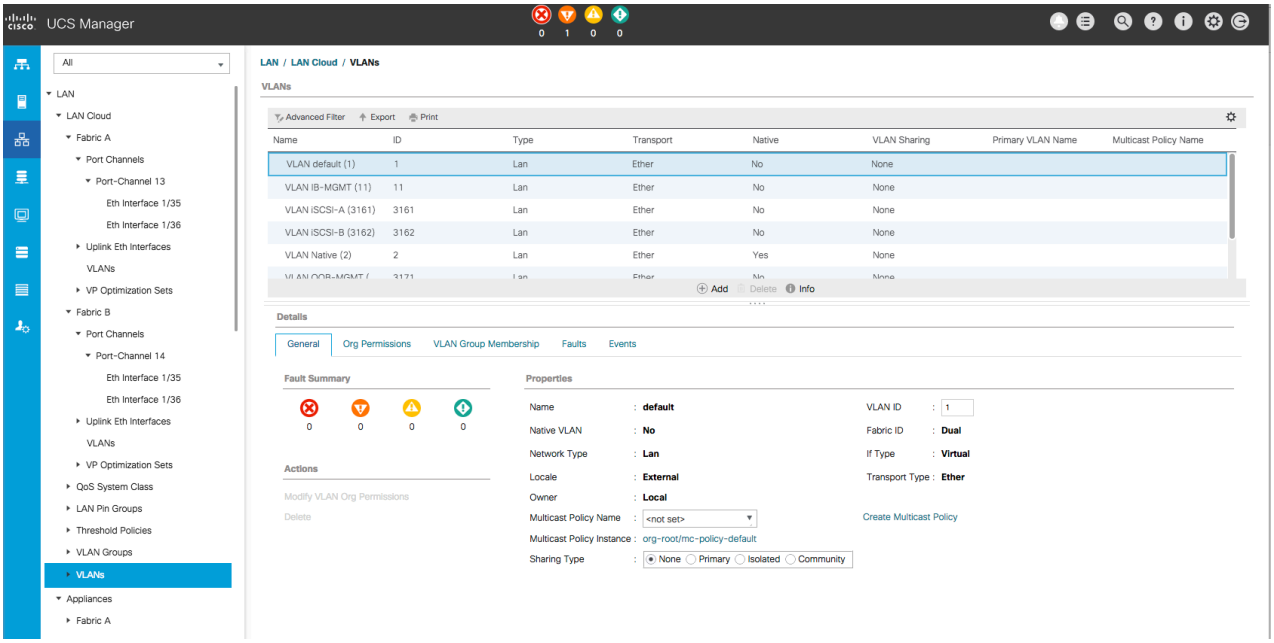


7. Click OK and then click OK again to add the controller definition and complete storage profile creation.

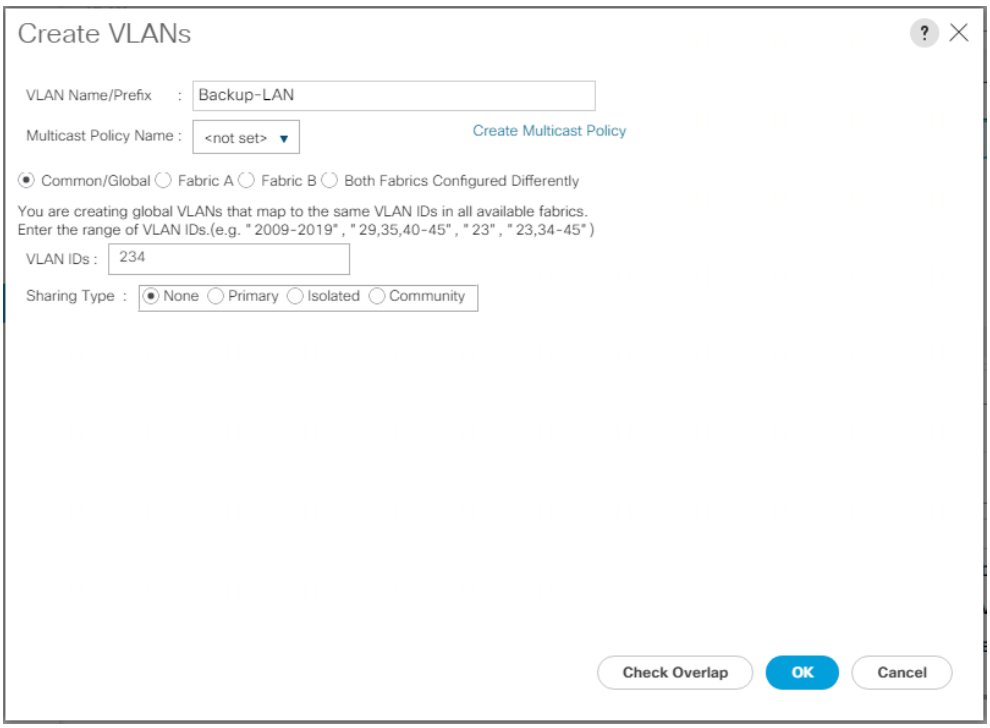
Configuring the LAN

The next task is to configure the networks required for ScaleProtect with 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 with Cisco UCS internal cluster network.

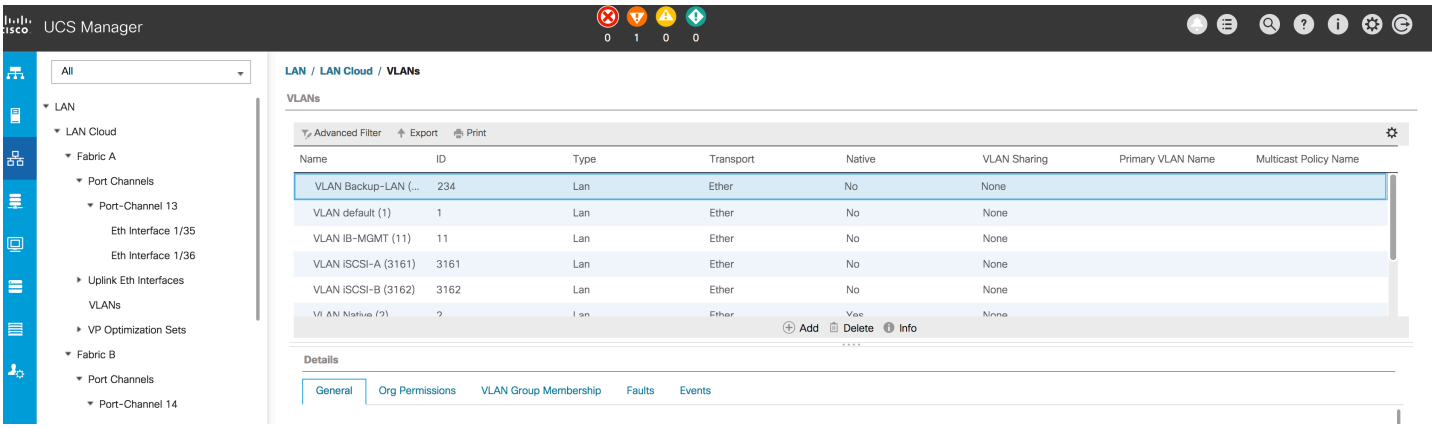
1. Choose LAN > LAN Cloud > VLANs and click Add.



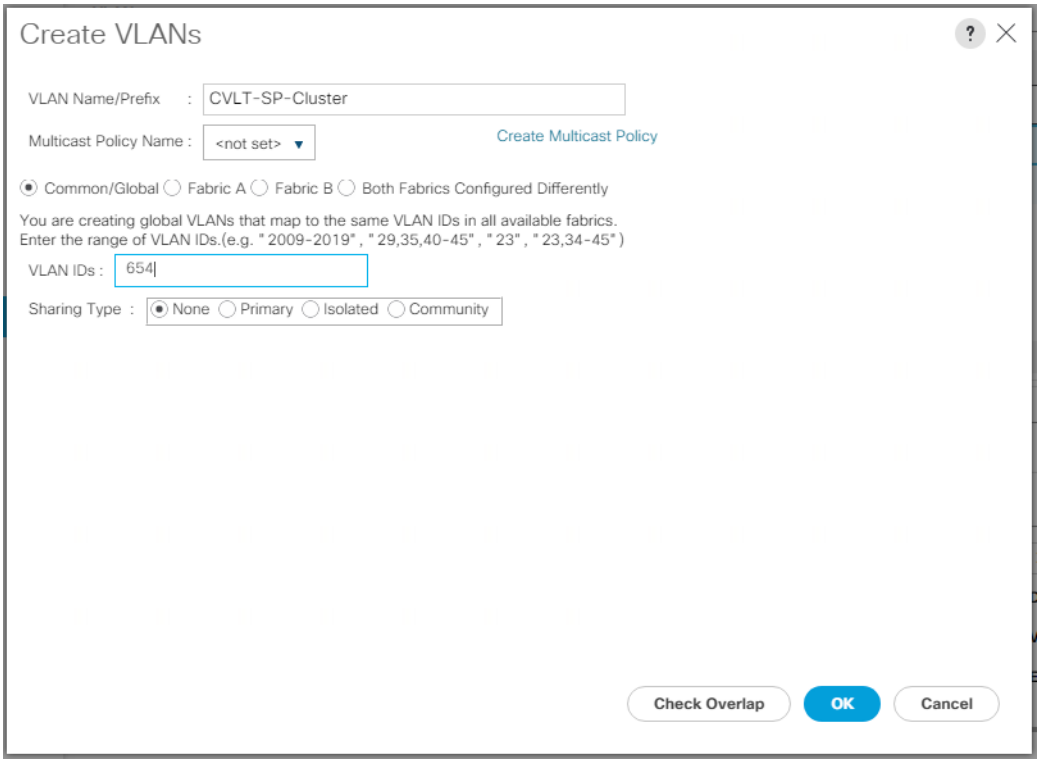
2. Enter an obvious name for the VLAN.
3. Enter the VLAN ID defined for the backup network in your landscape.
4. Click OK.

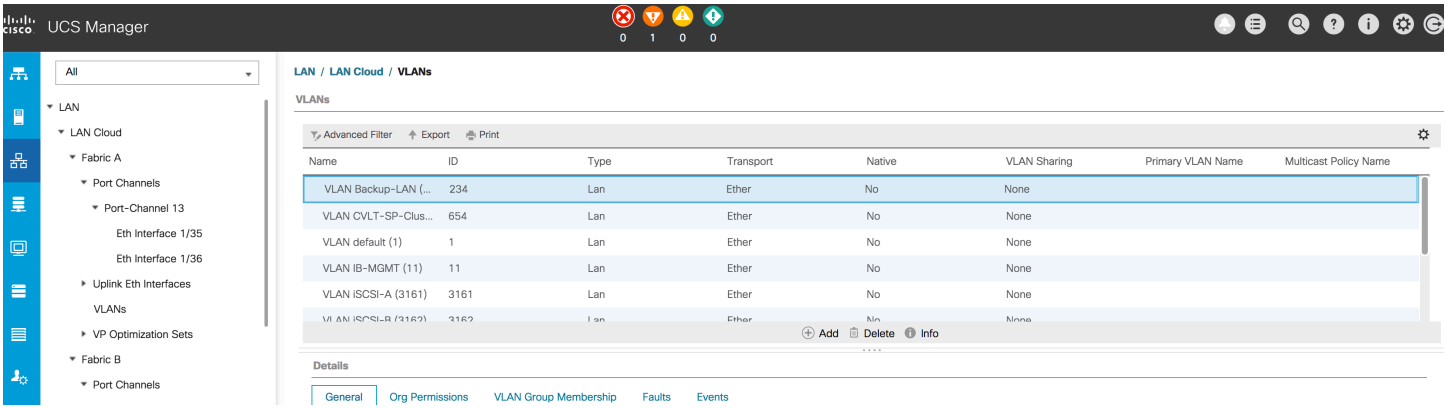


5. Click Add.

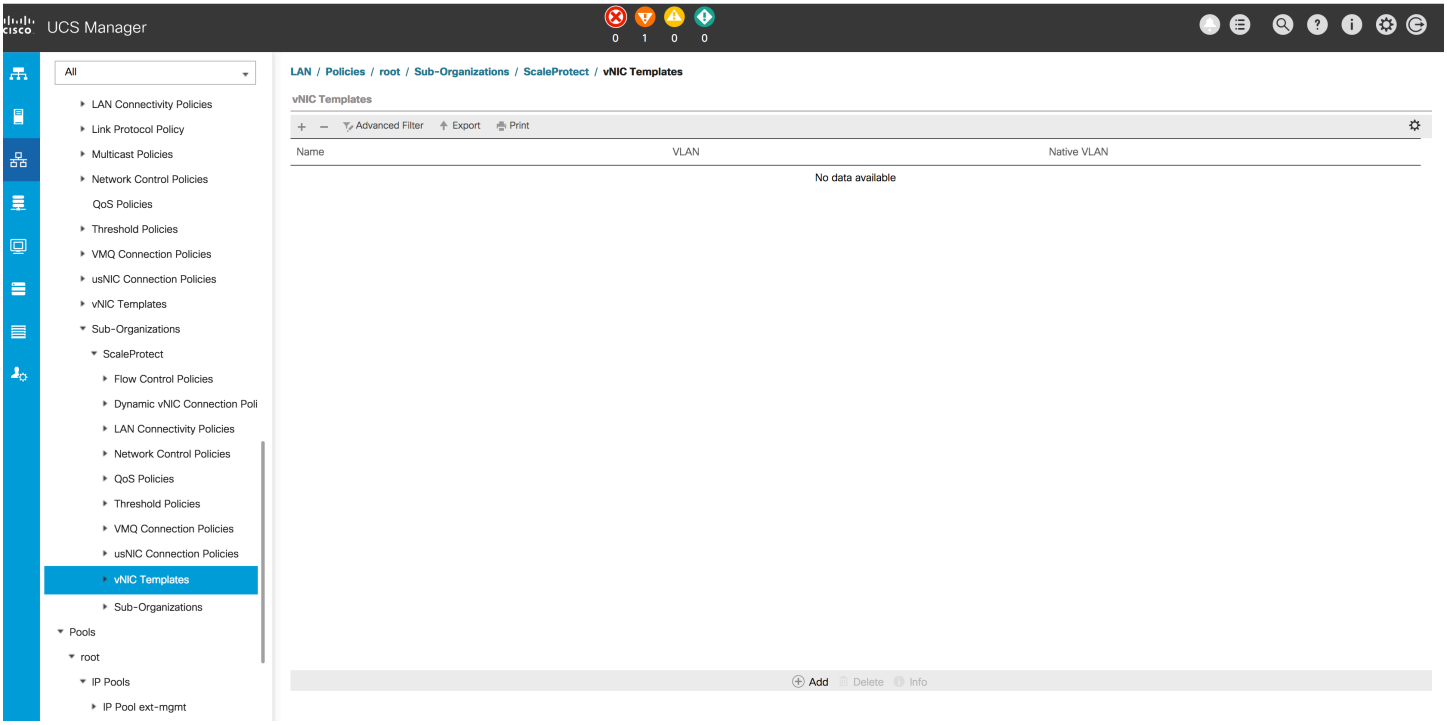


6. Enter an obvious name for the VLAN.
7. Enter the VLAN ID defined for the ScaleProtect with Cisco UCS cluster internal network.
8. Click OK.



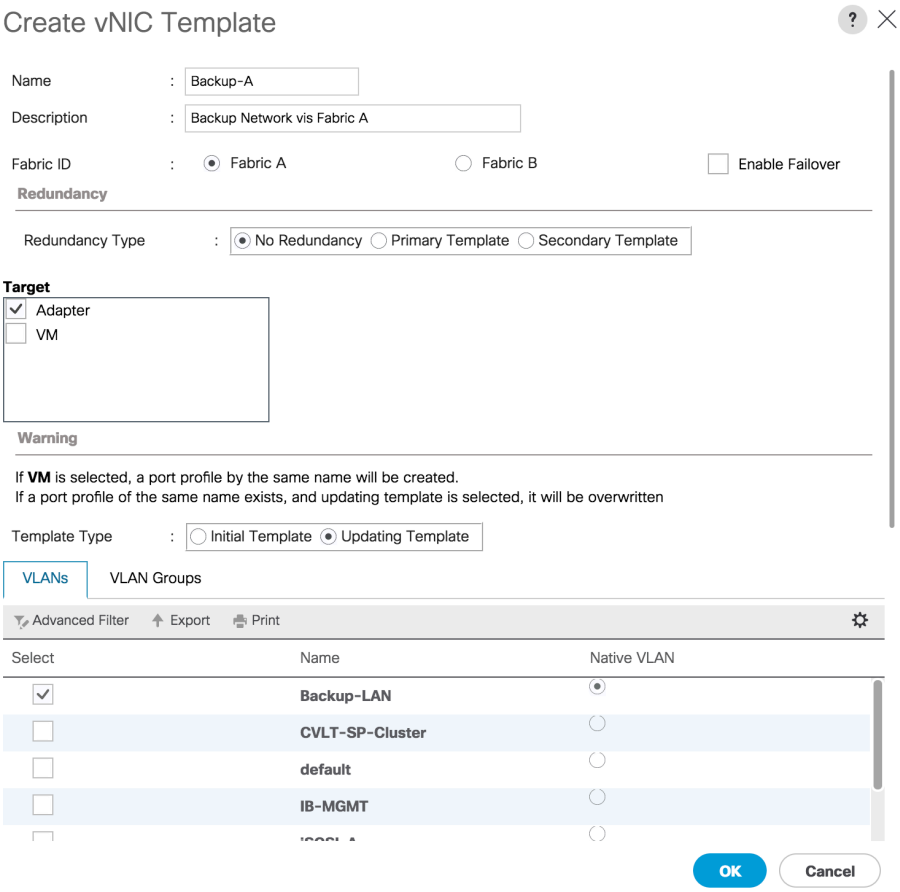


9. Choose LAN > Policies > root > Sub-Organizations > ScaleProtect > vNIC Templates and click Add.



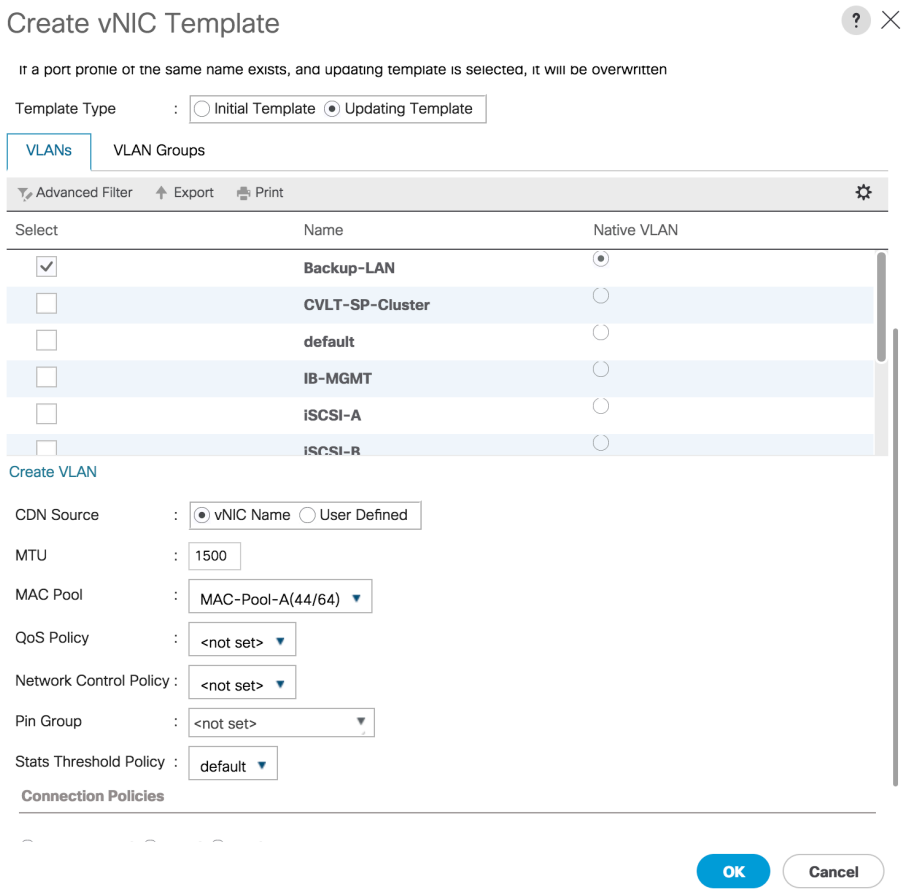
10. Enter an obvious name for the access network for the ScaleProtect with Cisco UCS solution, which is usually the backup network.
11. Select the radio button for Fabric A.
12. Select the Updating Template radio button.

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

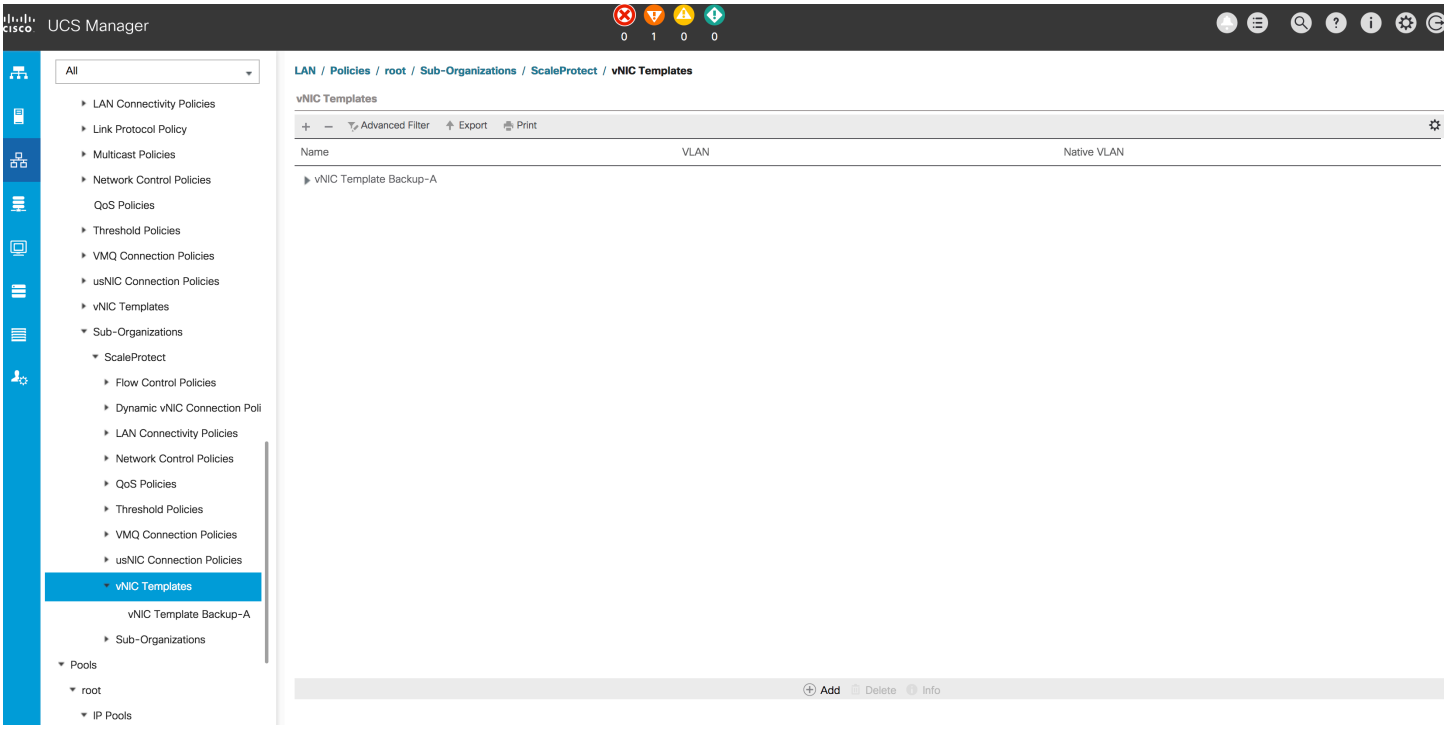


14. Enter **1500** or **9000** for the MTU value. MTU 9000 works only if all network components and the server are configured with MTU 9000. Check with your network administrator and server administrator to determine which value to use.
15. Select a MAC pool with free addresses.
16. Set the quality-of-service (QoS) policy and network control policy as defined by your local network administrator.

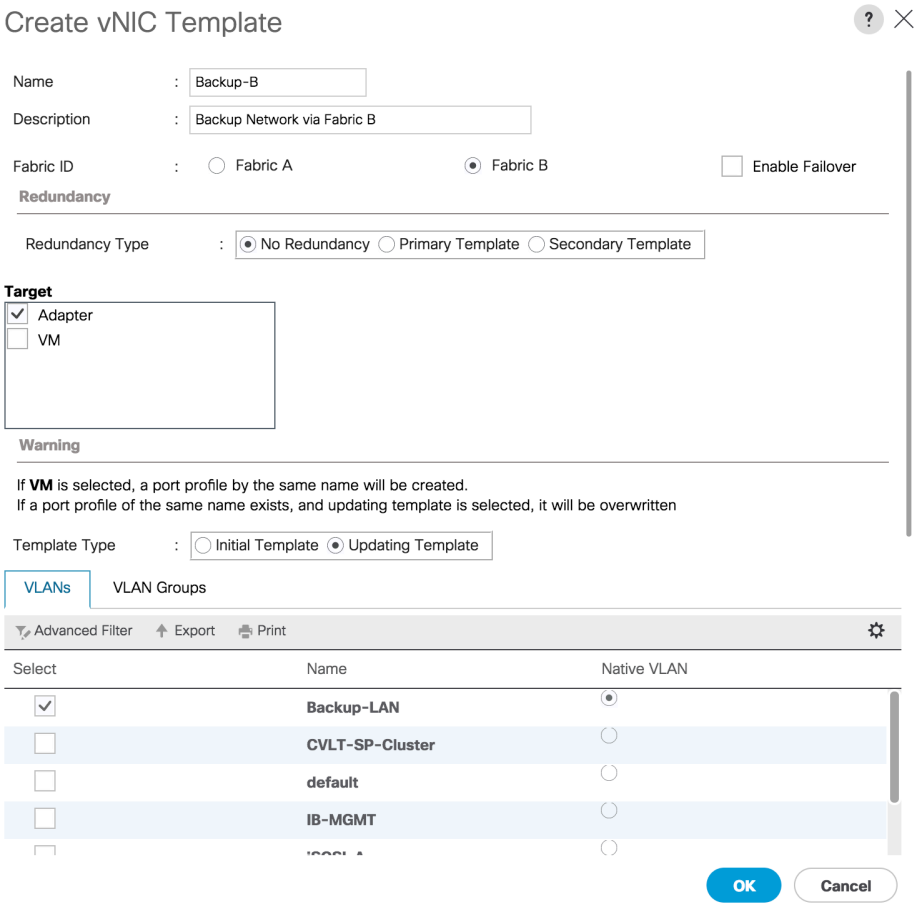
17. Click OK.



18. Click Add.

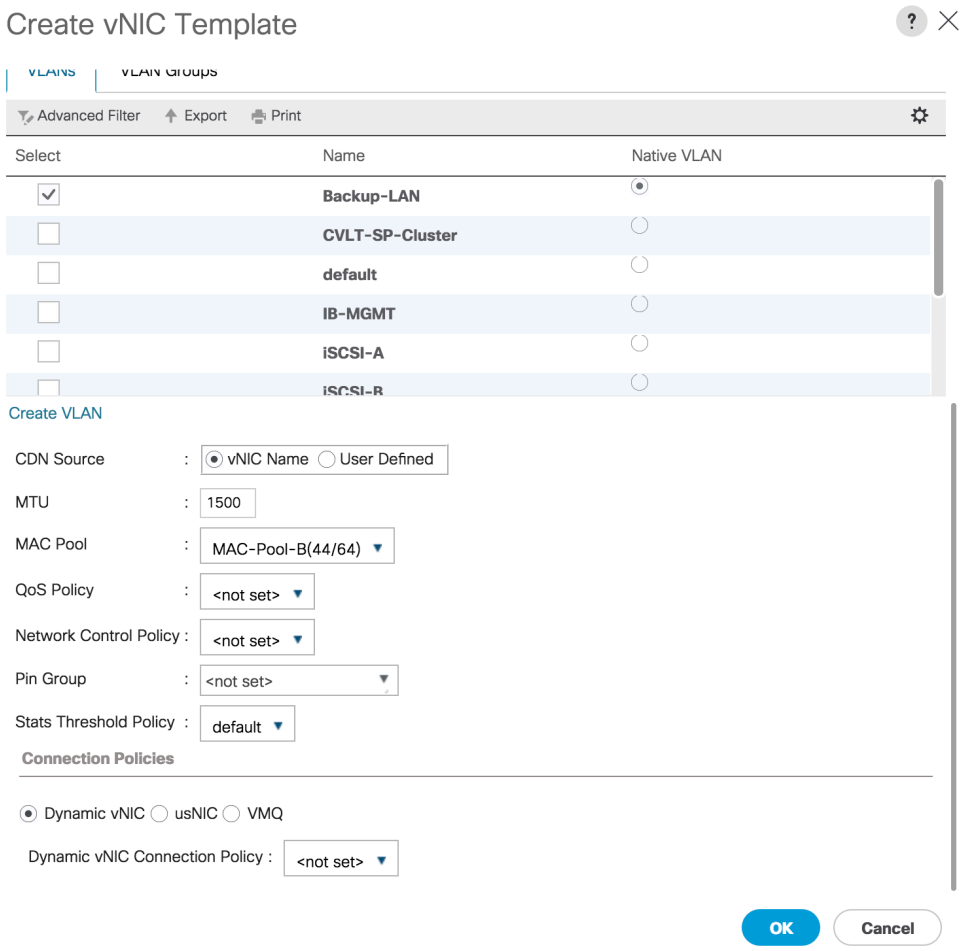


19. Enter an obvious name for the access network to the ScaleProtect with Cisco UCS solution, which is usually the backup network.
20. Select the radio button for Fabric B.
21. Select the Updating Template radio button.
22. Select the checkbox for Backup-LAN and select the Native VLAN radio button.

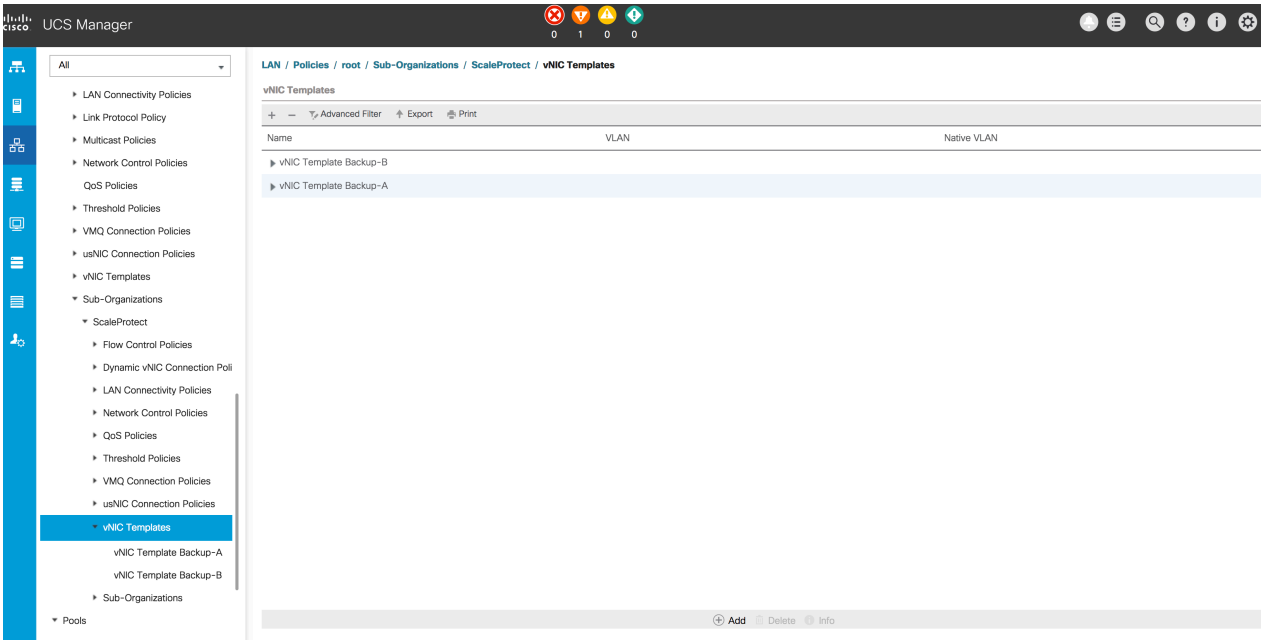


23. Enter **1500** or **9000** for the MTU value. MTU 9000 works only if all network components and the server are configured with MTU 9000. Check with your network administrator and server administrator to determine which value to use.
24. Select a MAC pool with free addresses.
25. Set the QoS policy and network control policy as defined by your local network administrator.

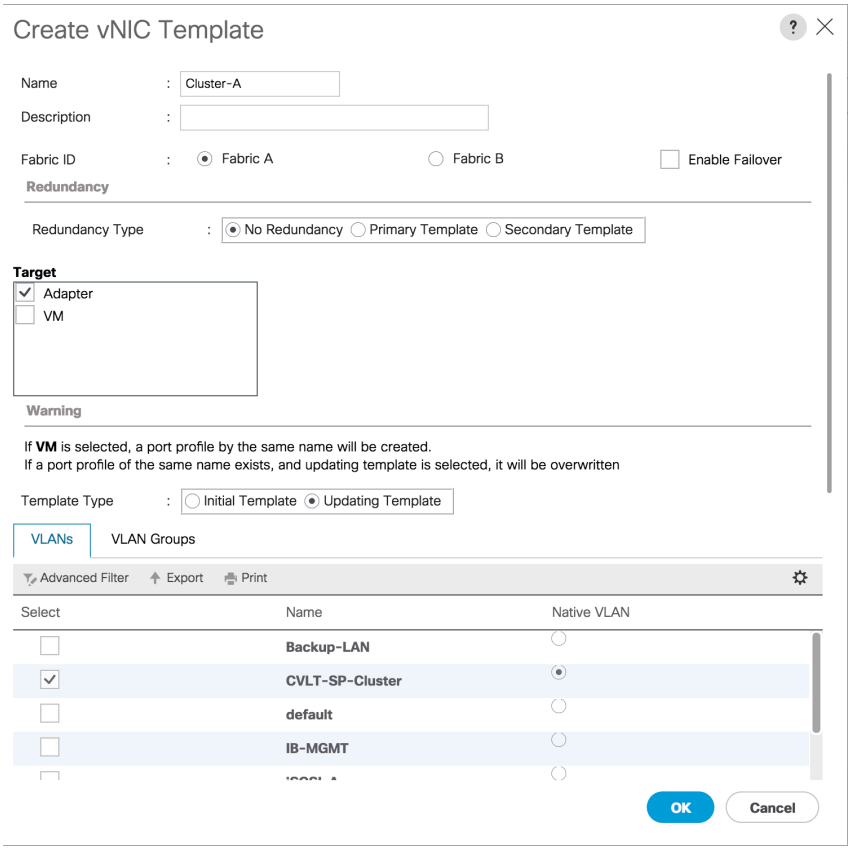
26. Click OK.



27. Click Add.

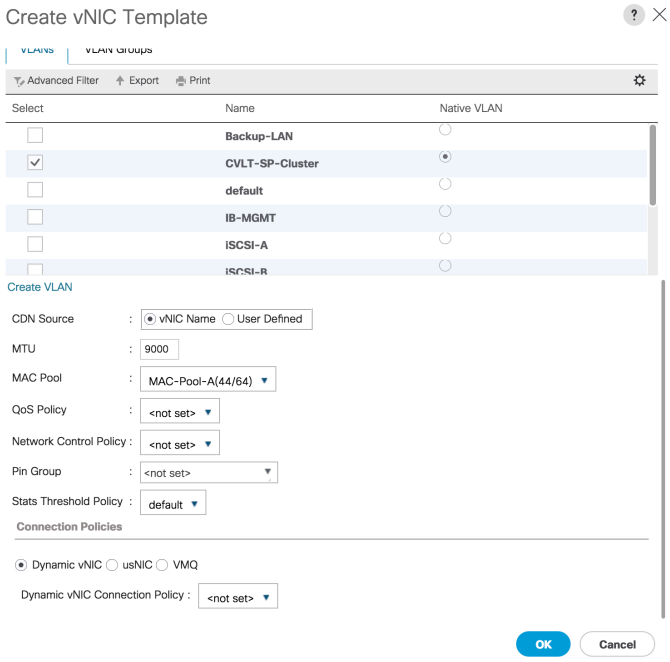


28. Enter an obvious name for the ScaleProtect with Cisco UCS internal cluster network.
29. Select the radio button for Fabric A.
30. Select the Updating Template radio button.
31. Select the checkbox for CVLT-SP-Cluster and select the Native VLAN radio button.

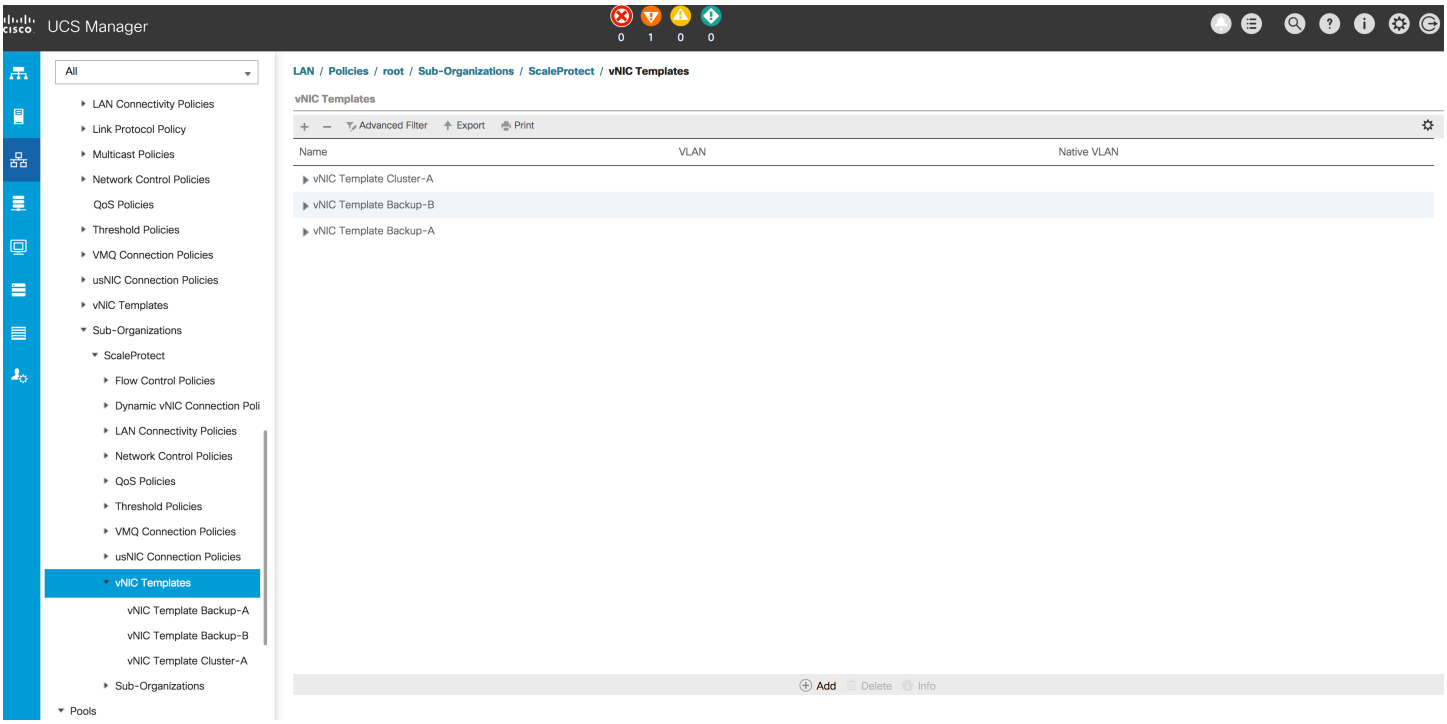


32. Enter **9000** for the MTU value. MTU 9000 works only if all network components and the server are configured with MTU 9000. Check with your network administrator and server administrator to determine the use.
33. Select a MAC pool with free addresses.
34. Set the QoS policy and network control policy as defined by your local network administrator.

35. Click OK.

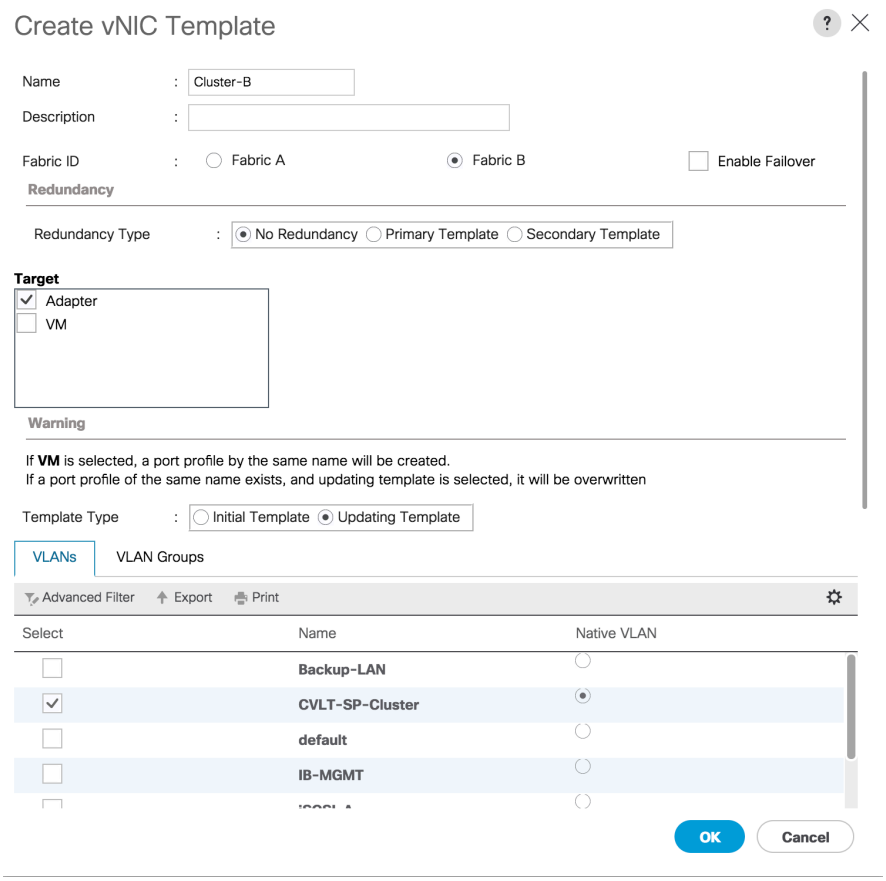


36. Click Add.



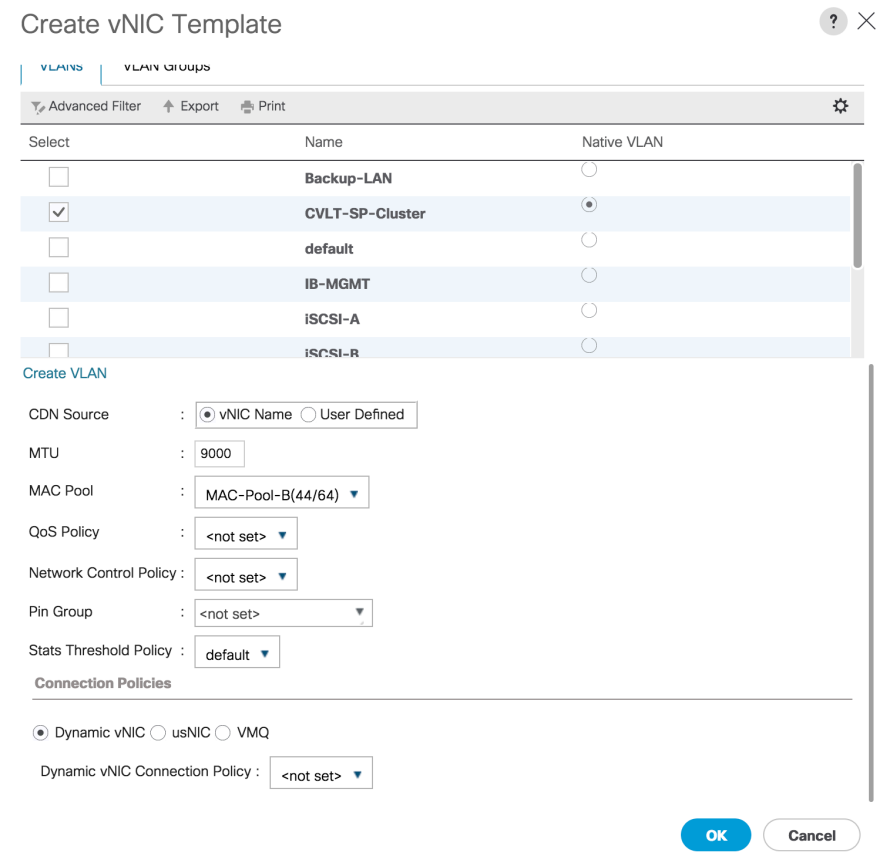
37. Enter an obvious name for the ScaleProtect with Cisco UCS internal cluster network.
38. Select the radio button for Fabric B.
39. Select the Updating Template radio button.

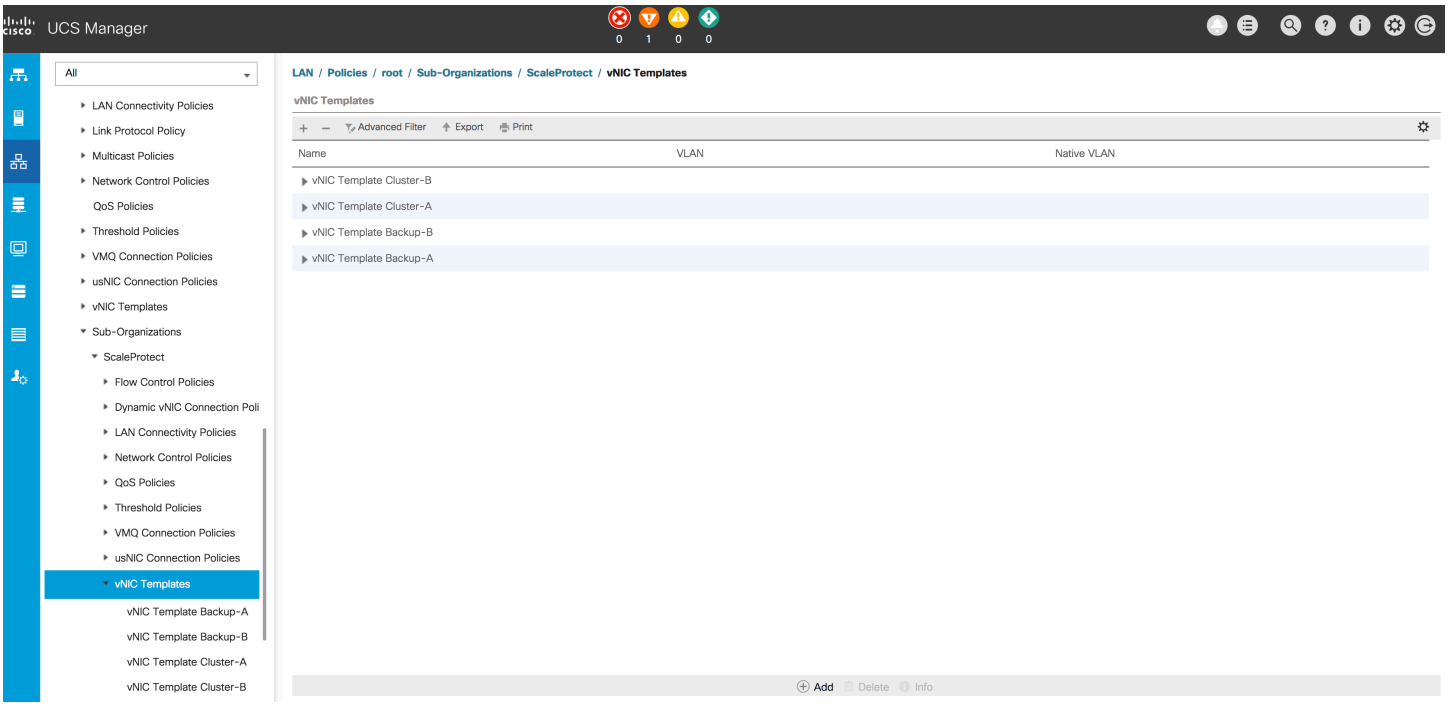
40. Select the checkbox for CVLT-SP-Cluster and select the Native VLAN radio button.



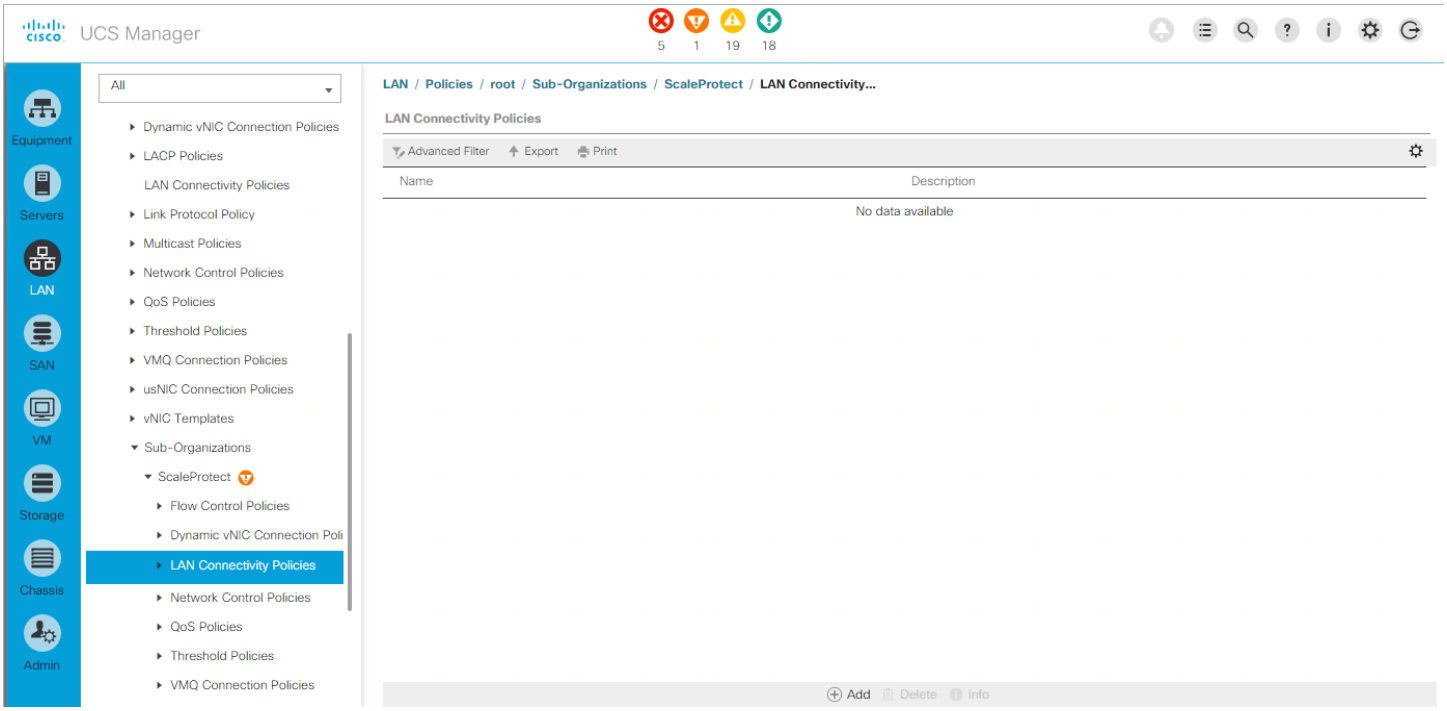
41. Enter **9000** for the MTU value. MTU 9000 works only if all network components and the server are configured with MTU 9000. Check with your network administrator and server administrator to determine the use.
42. Select a MAC pool with free addresses.
43. Set the QoS policy and network control policy as defined by your local network administrator.

44. Click OK.

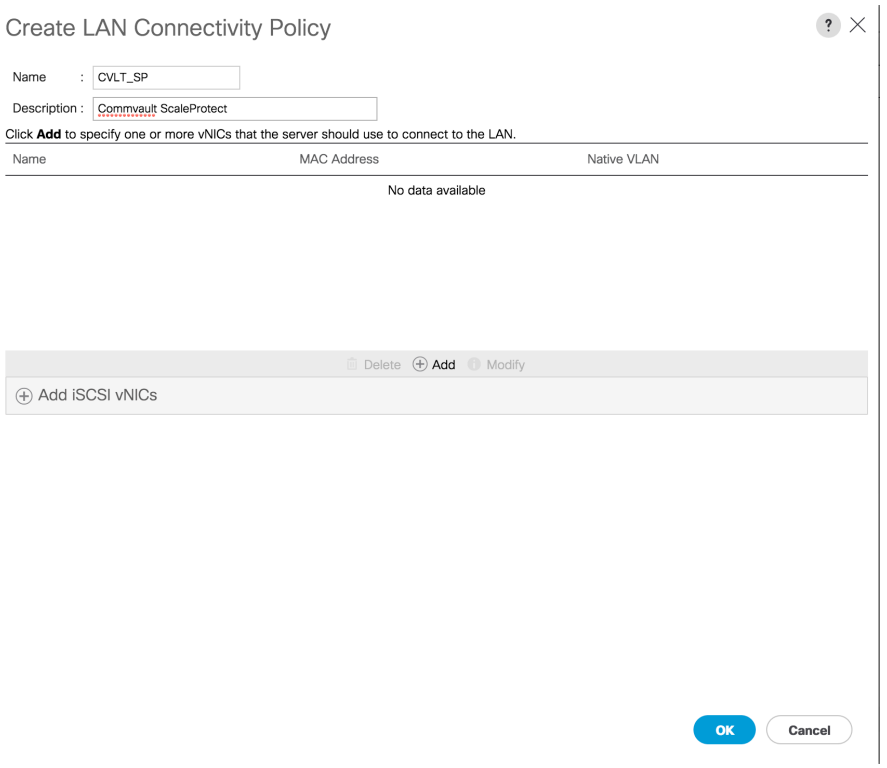




45. Choose LAN > Policies > root > Sub-Organizations > ScaleProtect > LAN Connectivity Policies and click Add.

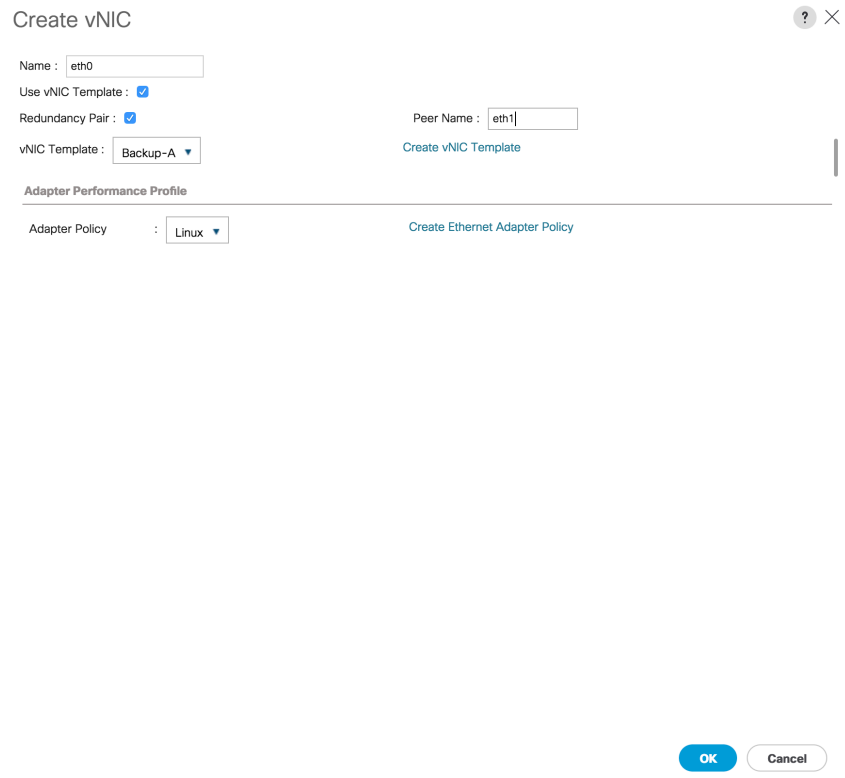


46. Enter an obvious name and description and click Add.

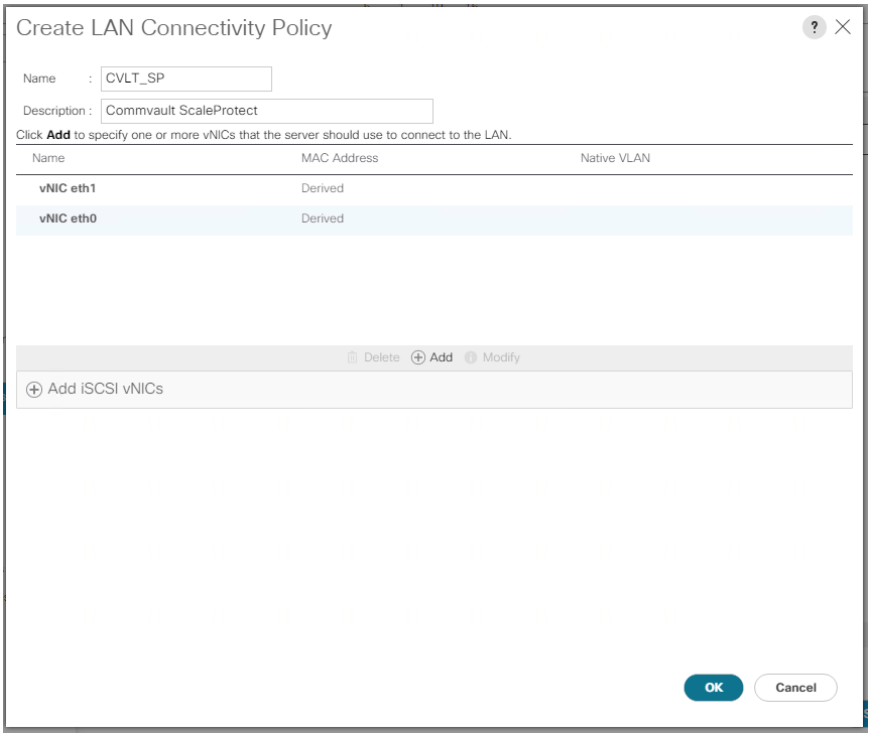


47. Enter **eth0** as the name of the vNIC.
48. Select Use vNIC Template.
49. Select Redundancy Pair end enter **eth1** as the peer name.

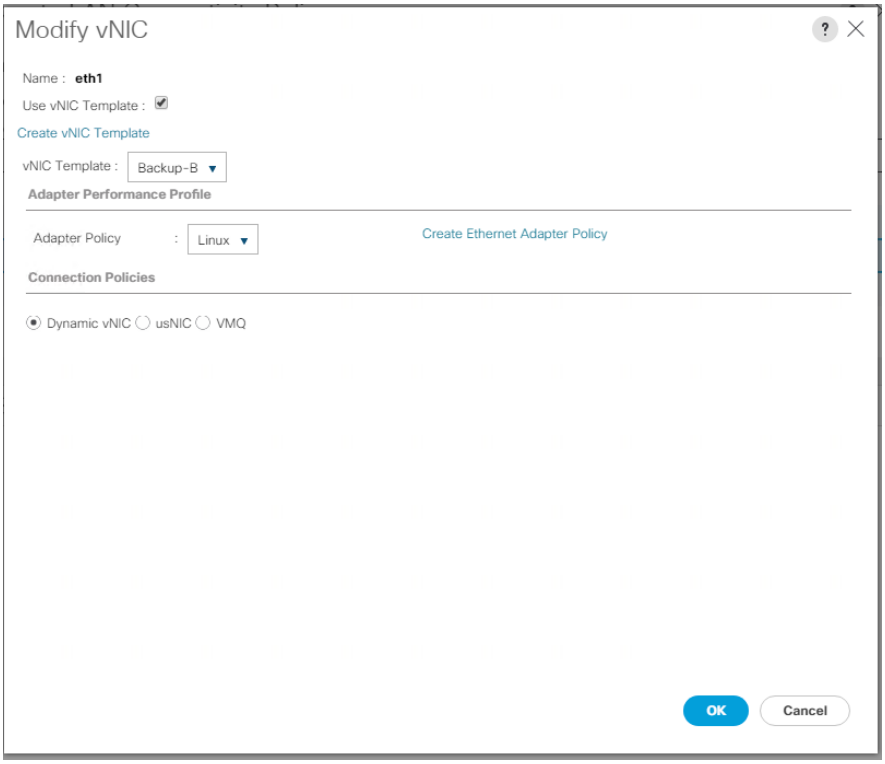
50. Select Backup-A as the vNIC template.
51. Select Linux as the adapter policy.
52. Click OK.



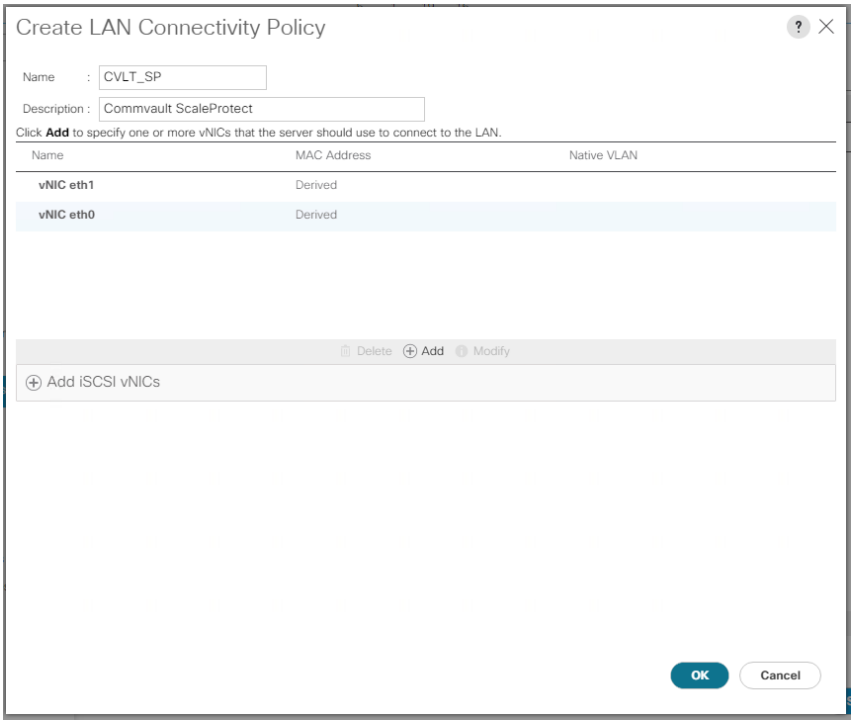
53. Select vNIC eth1 and click Modify.



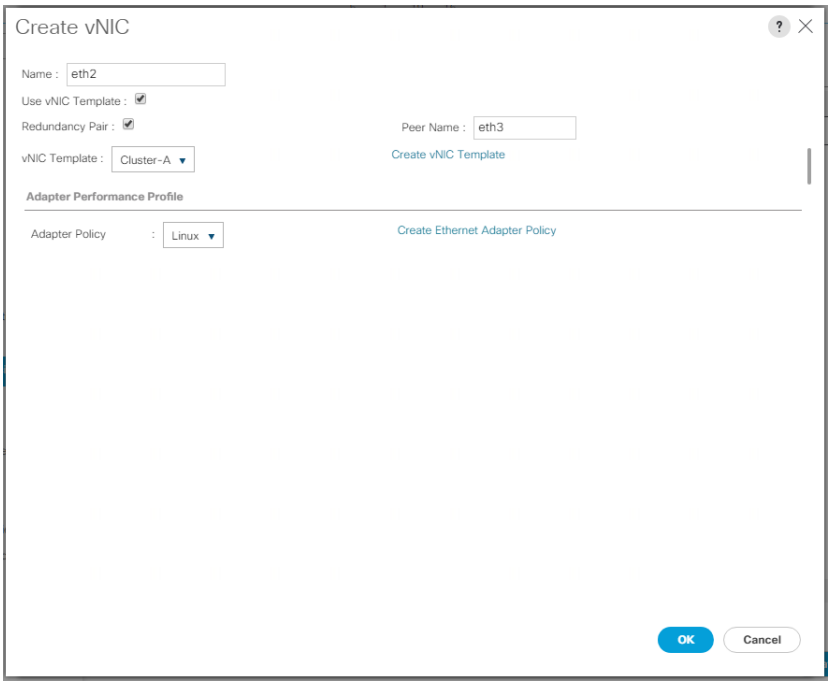
54. Select Use vNIC Template.
55. Select Backup-B as the template.
56. Select Linux as the adapter policy.
57. Click OK.



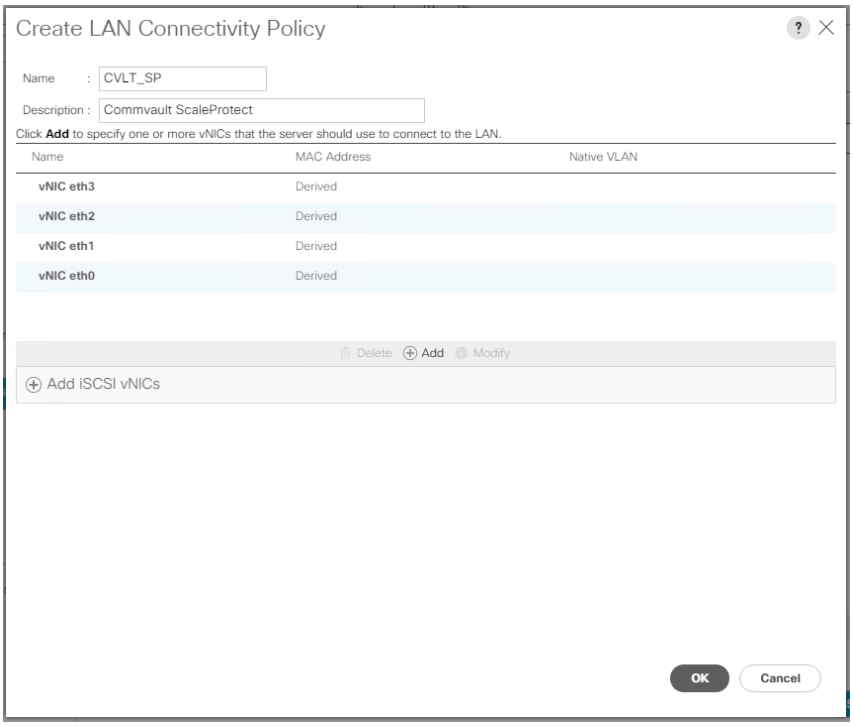
58. Click Add.



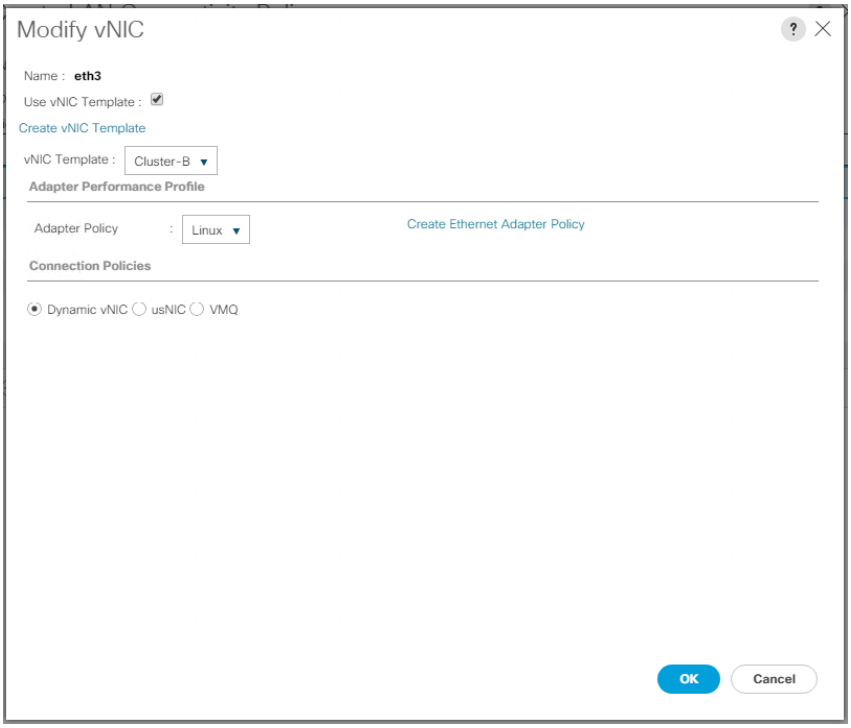
59. Enter **eth2** as the name of the vNIC.
60. Select Use vNIC Template.
61. Select Redundancy Pair end enter **eth3** as the peer name.
62. Select Cluster-A as the vNIC template.
63. Select Linux as the adapter policy.
64. Click OK.



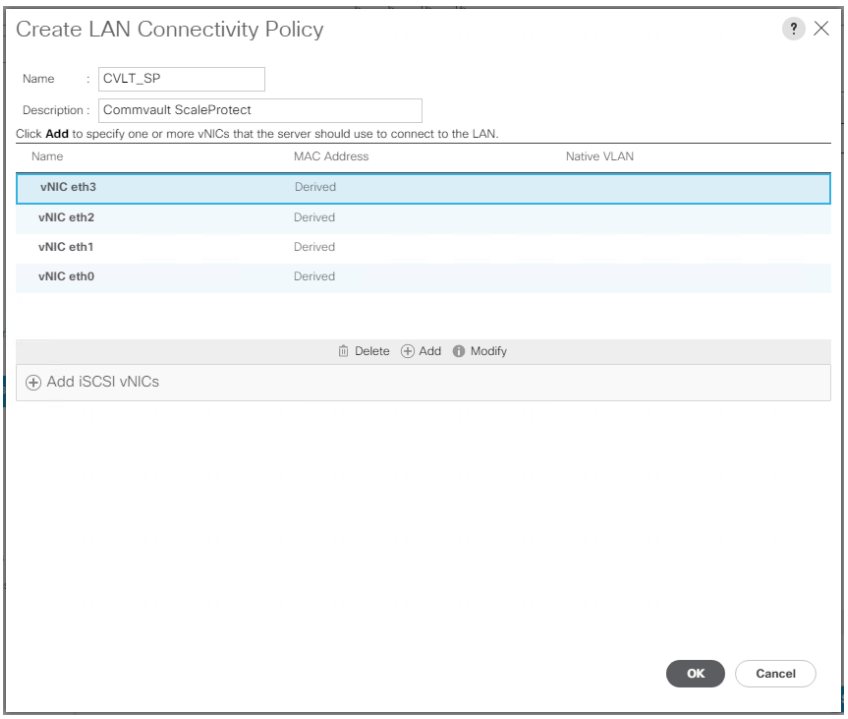
65. Select vNIC eth3 and click Modify.

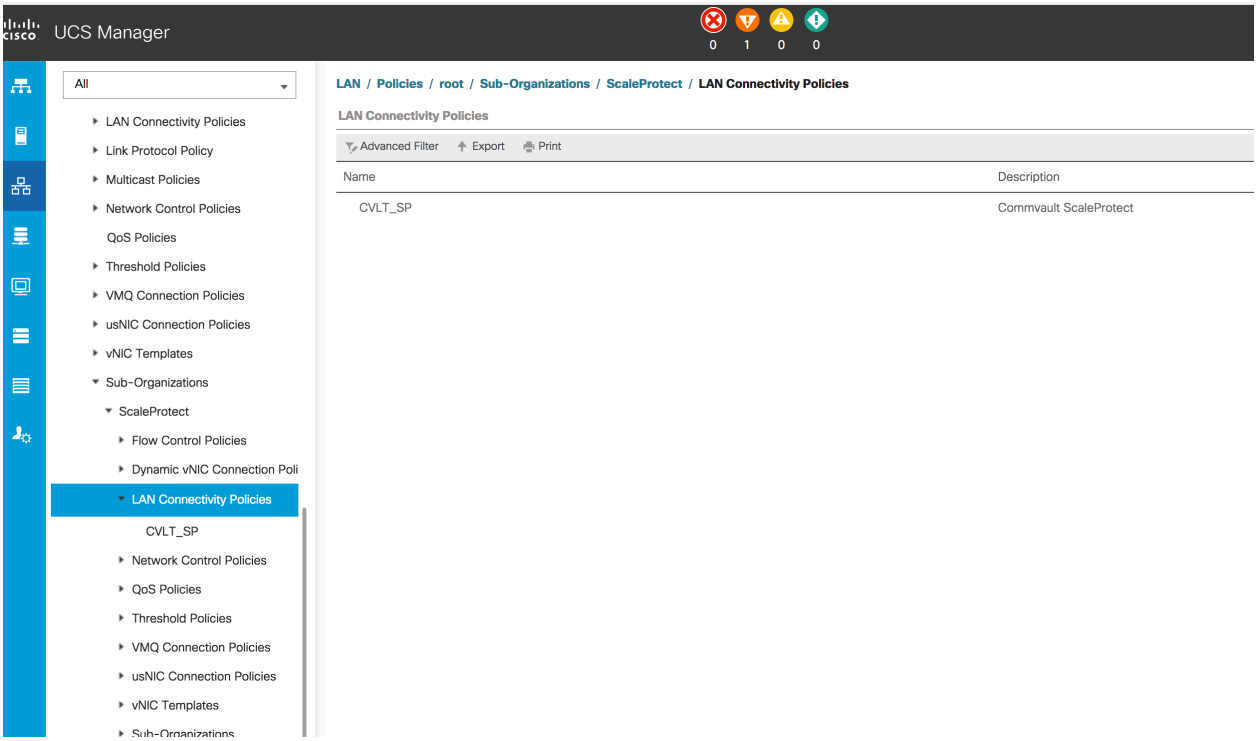


66. Select Use vNIC Template.
67. Select Cluster-B as the template.
68. Select Linux as the adapter policy.
69. Click OK.



70. Click OK.

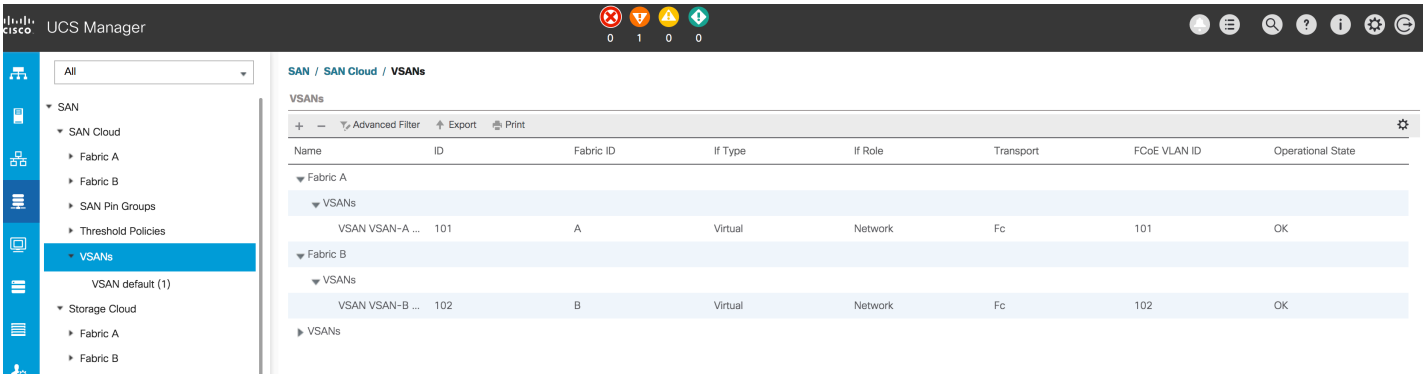




Configuring the SAN

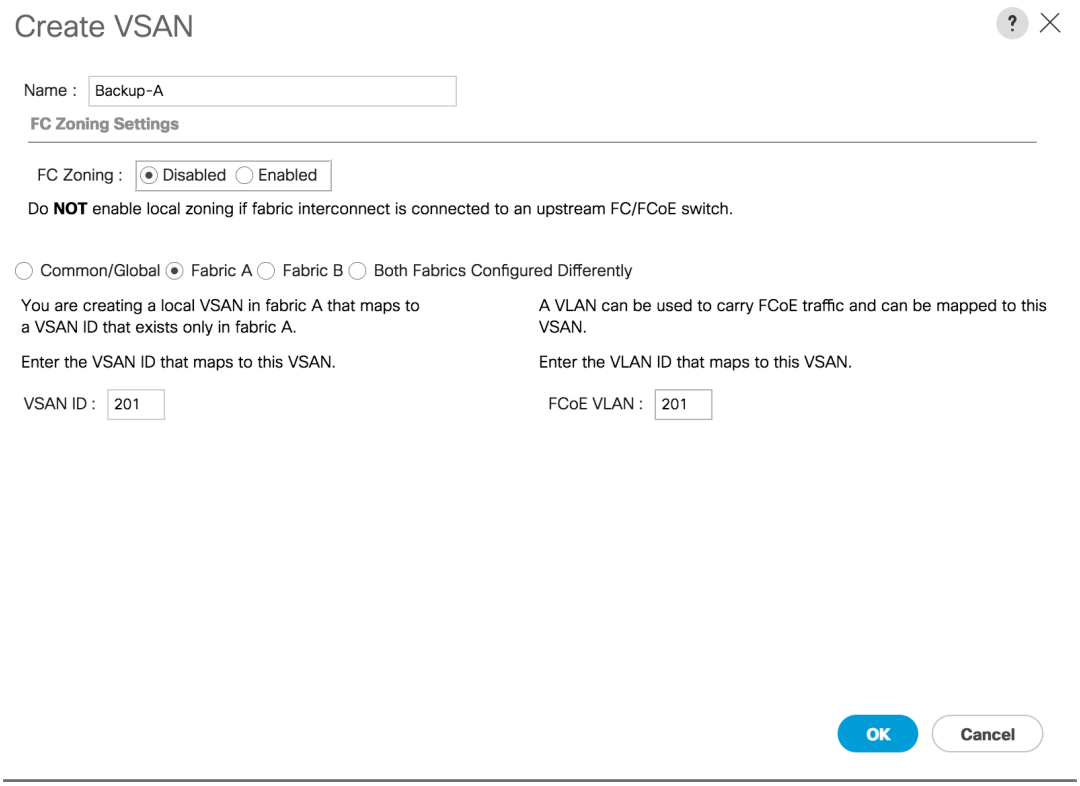
If you are planning to integrate IntelliSnap with existing SAN storage or backup to Fibre Channel–connected tape drives, configure the Cisco UCS SAN for access to the SAN environment through FCoE in the system.

1. Choose SAN > SAN Cloud > VSANs and check the configured VSANs.

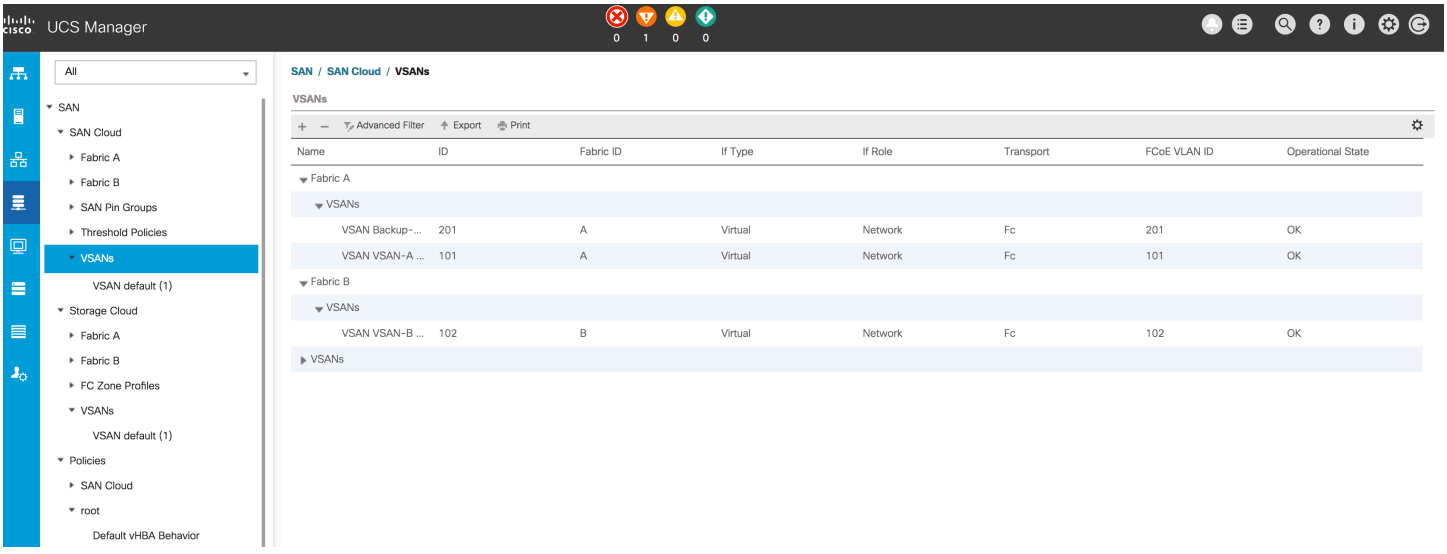


2. If a dedicated SAN configuration for backup is required, add the required VSAN configuration to the system.
3. Click Add.
4. Enter an obvious name.
5. Select Fabric A.
6. Enter the required VSAN ID and related FCoE VLAN ID.

7. Click OK.

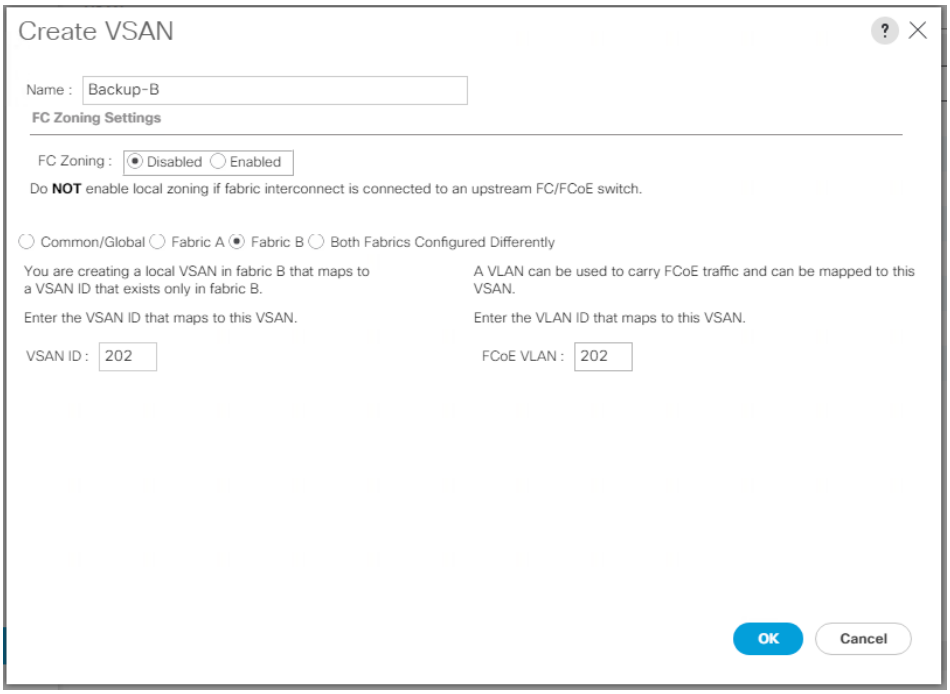


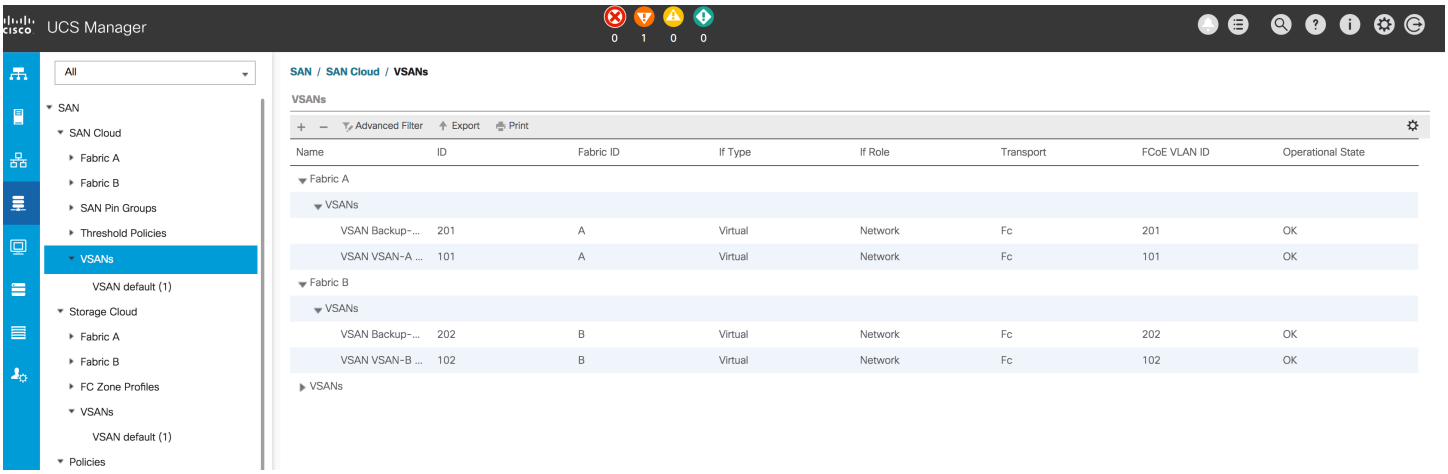
8. Click Add.



9. Enter an obvious name.
10. Select Fabric B.
11. Enter the required VSAN ID and related FCoE VLAN ID.

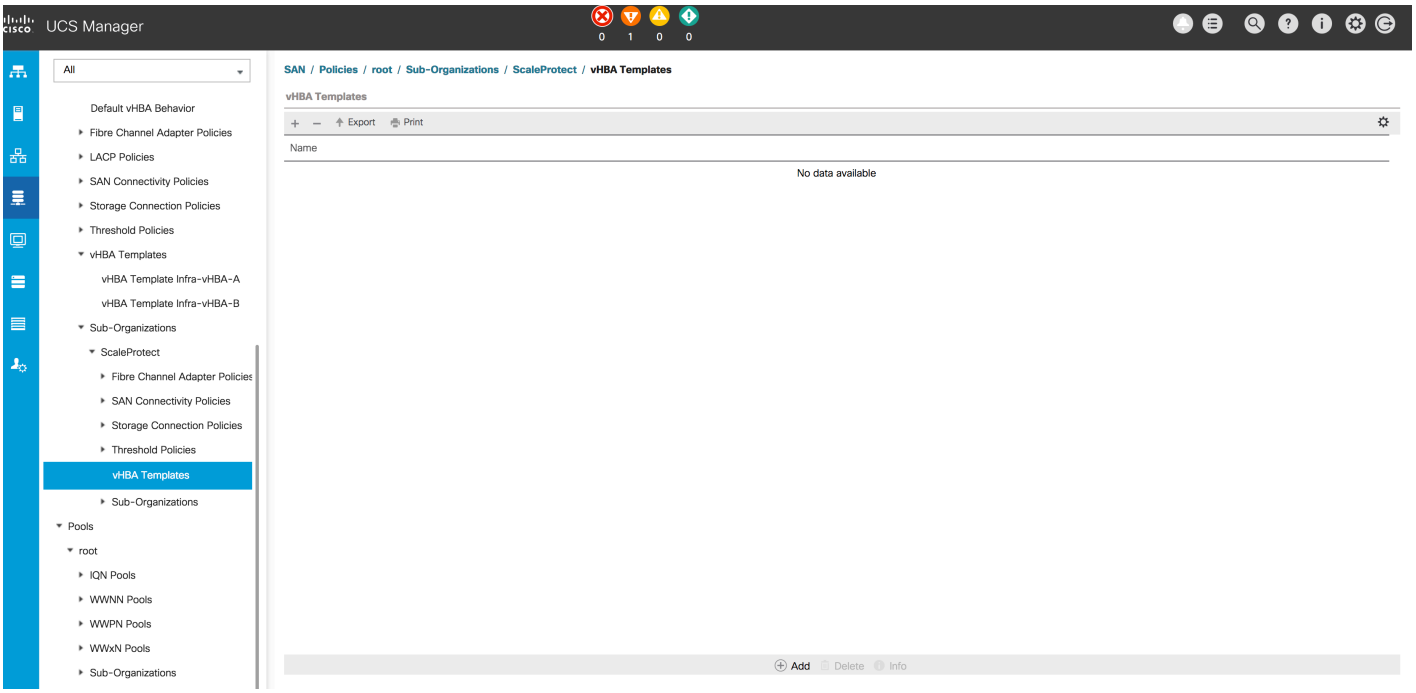
12. Click OK.



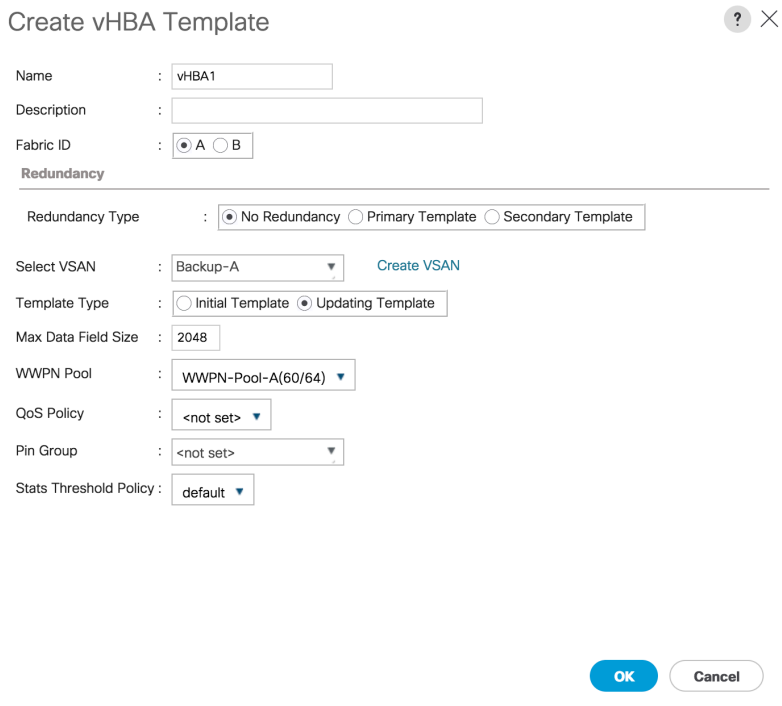


13. Choose SAN > Policies > root > Sub-Organization > ScaleProtect > vHBA Templates.
14. Create vHBA templates for Storage-A and Storage-B if they don't exist.

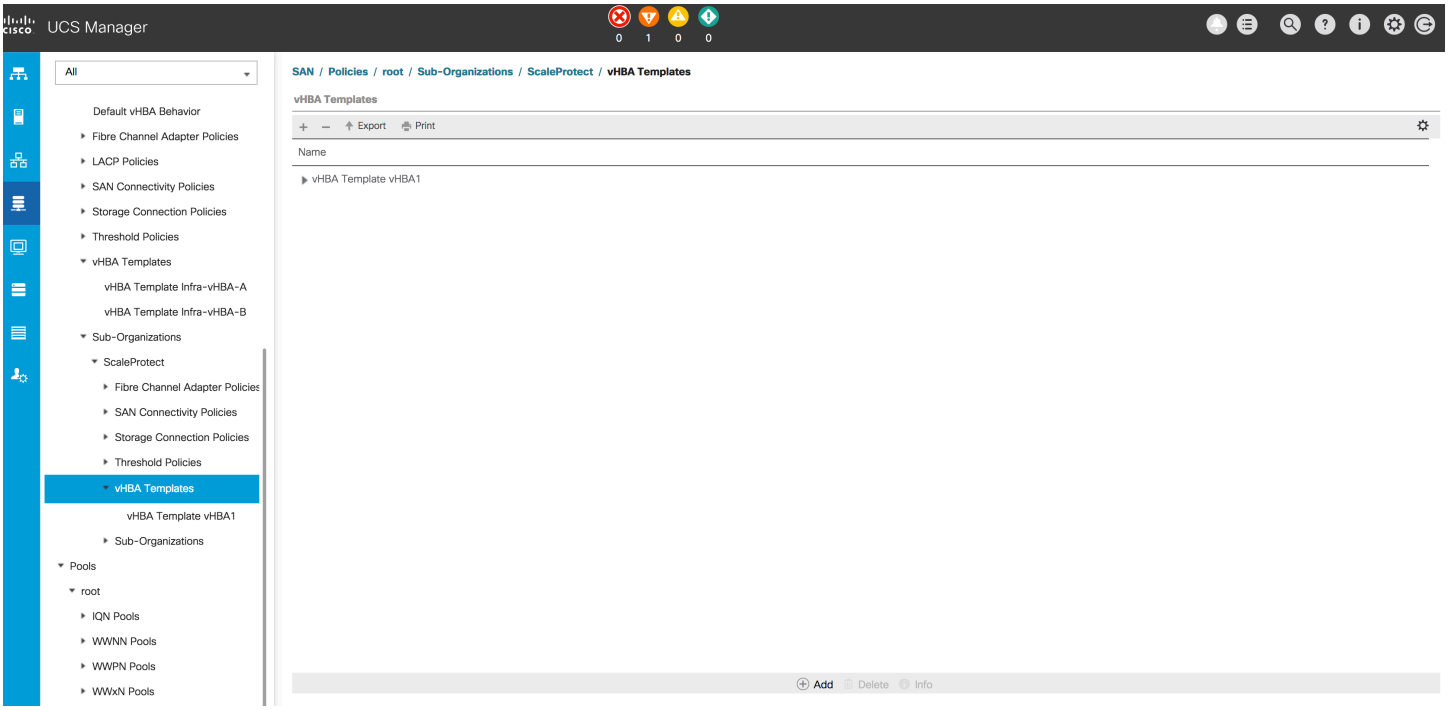
15. Click Add.



16. Enter an obvious name.
17. Select Fabric A.
18. Select Updating Template as the template type.
19. Select the backup VSAN on Fabric A as the VSAN.
20. Select a WWPN pool with available addresses.
21. Click OK.

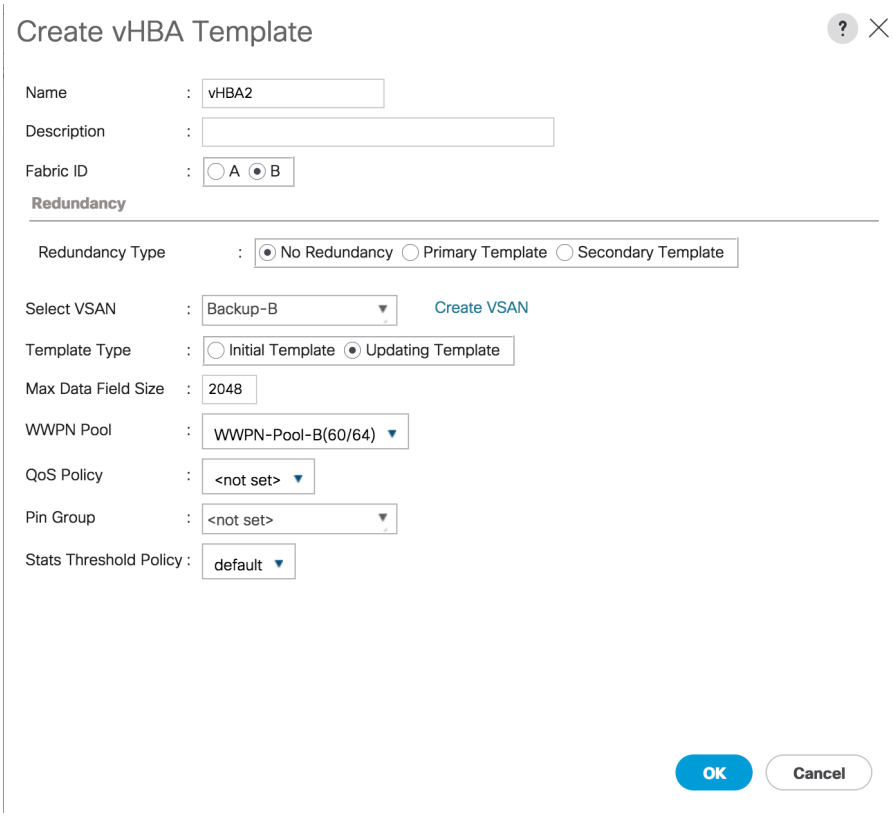


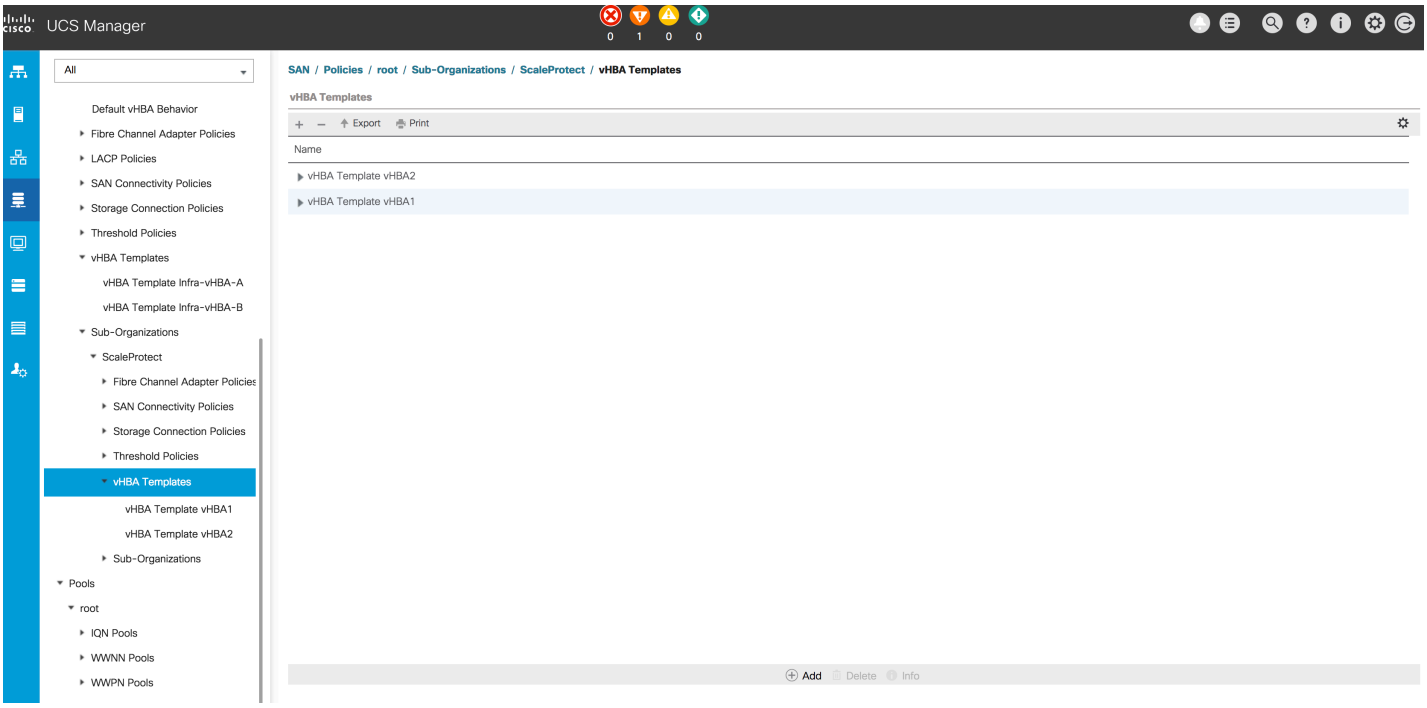
22. Click Add.



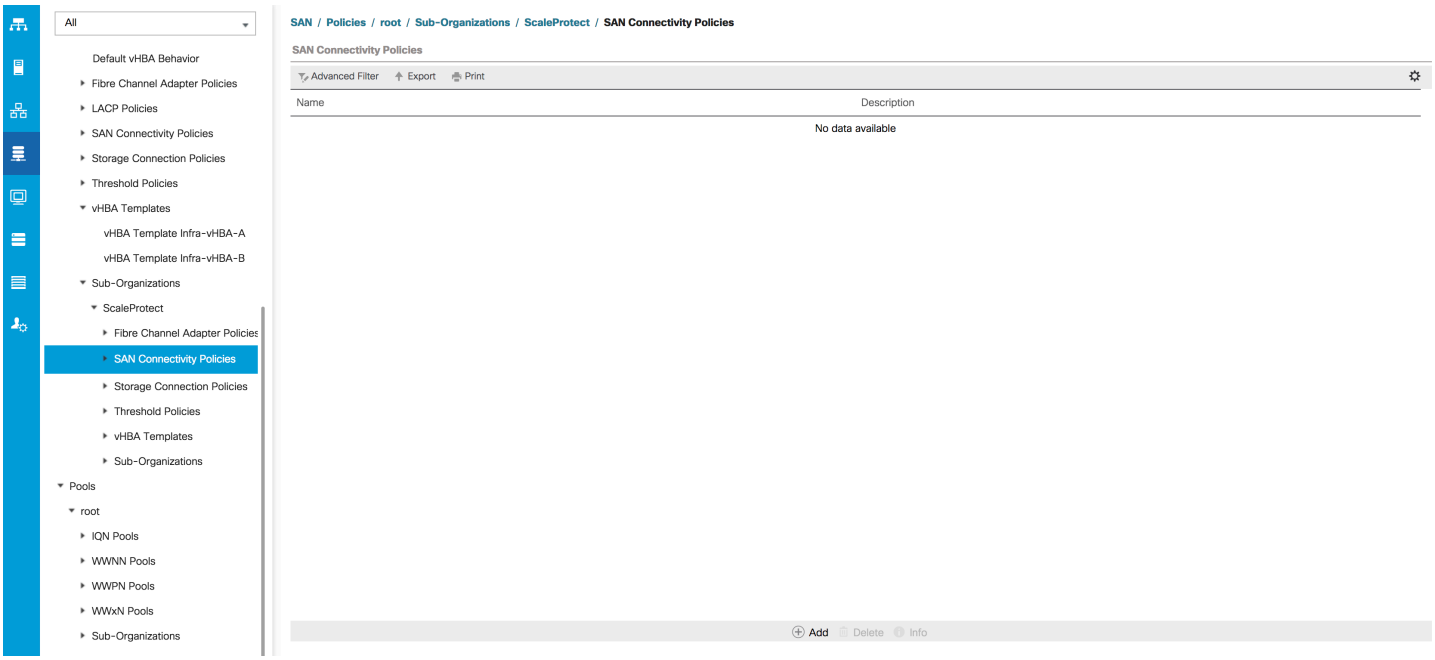
23. Enter an obvious name.
24. Select Fabric A.
25. Select Updating Template as the template type.
26. Select the backup VSAN on Fabric A as the VSAN.
27. Select a WWPN pool with available addresses.

28. Click OK.

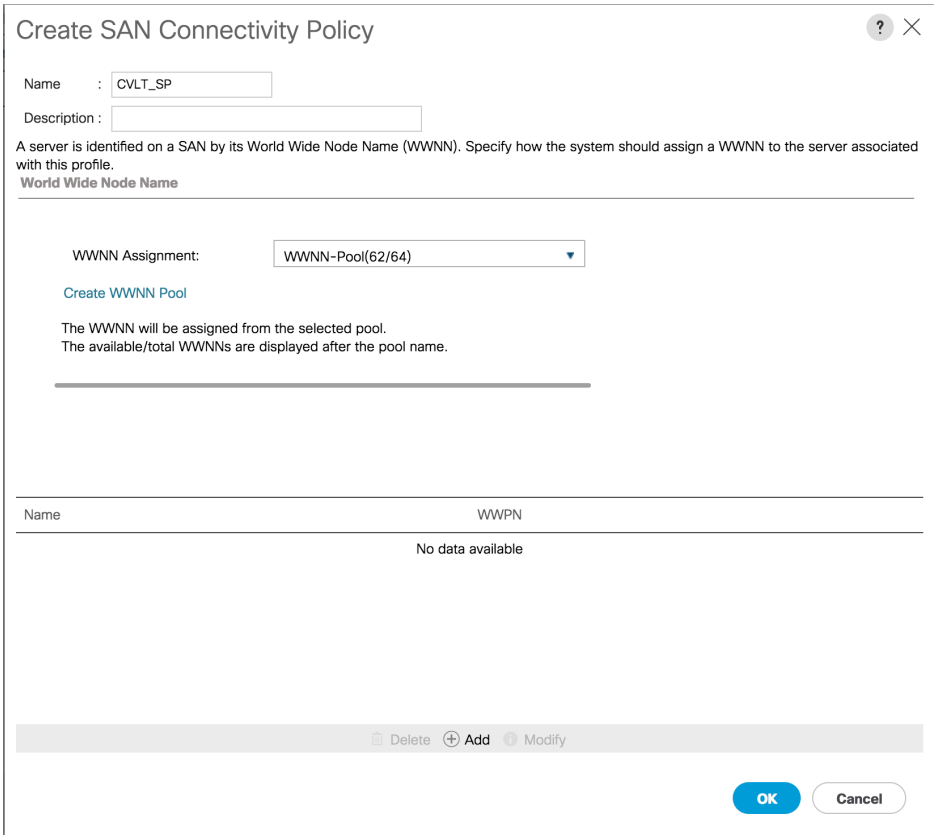




29. Choose SAN > Policies > root > Sub-Organization > ScaleProtect > SAN Connectivity Policies and click Add.

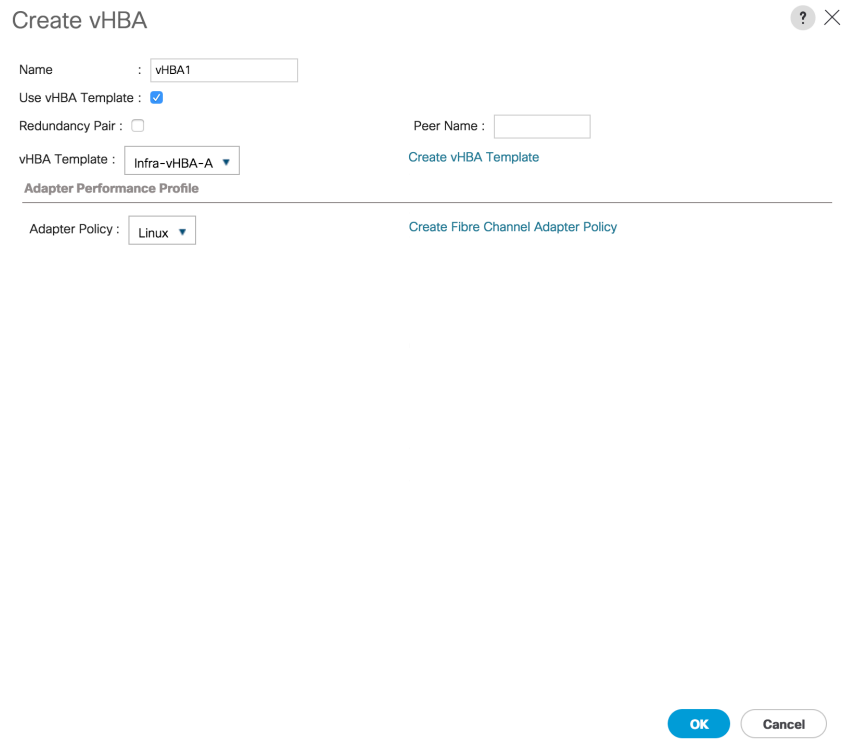


30. Enter an obvious name.
31. Select a WWNN pool with free addresses.
32. Click Add.

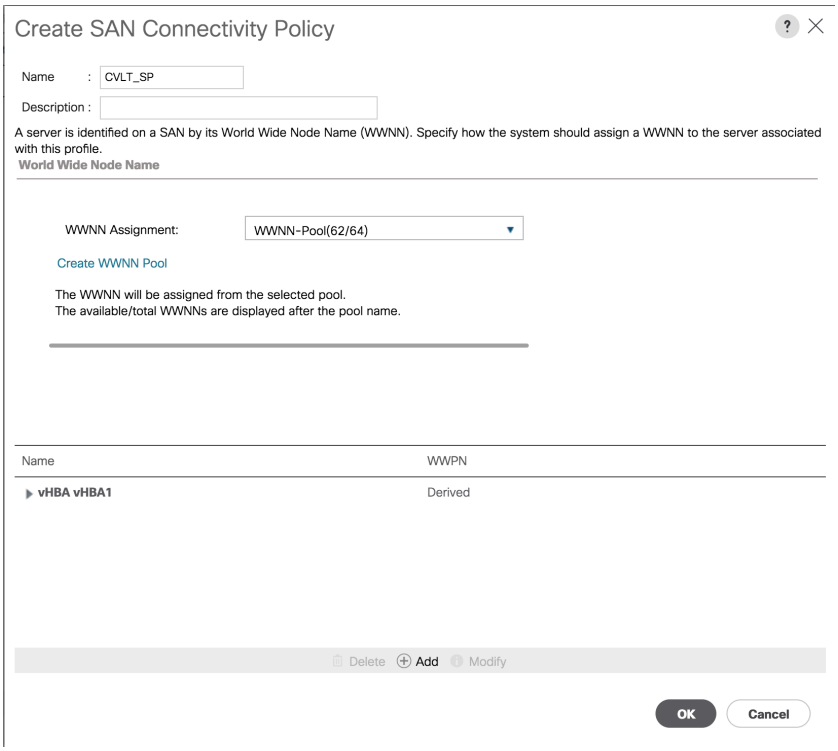


33. Enter an obvious name.

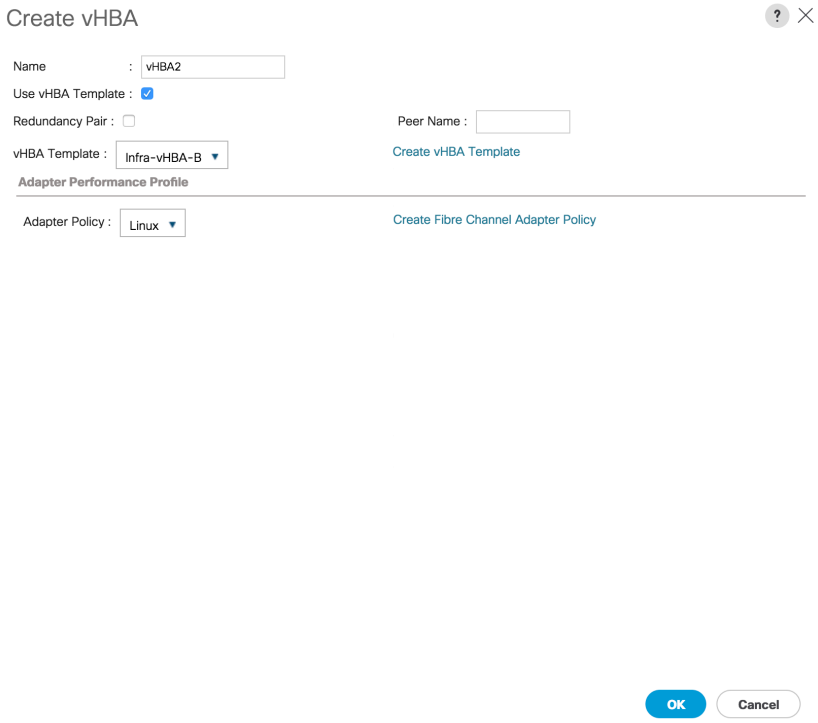
34. Select Use vHBA Template.
35. Select one of the vHBA templates.
36. Select Linux as the adapter policy.
37. Click OK.



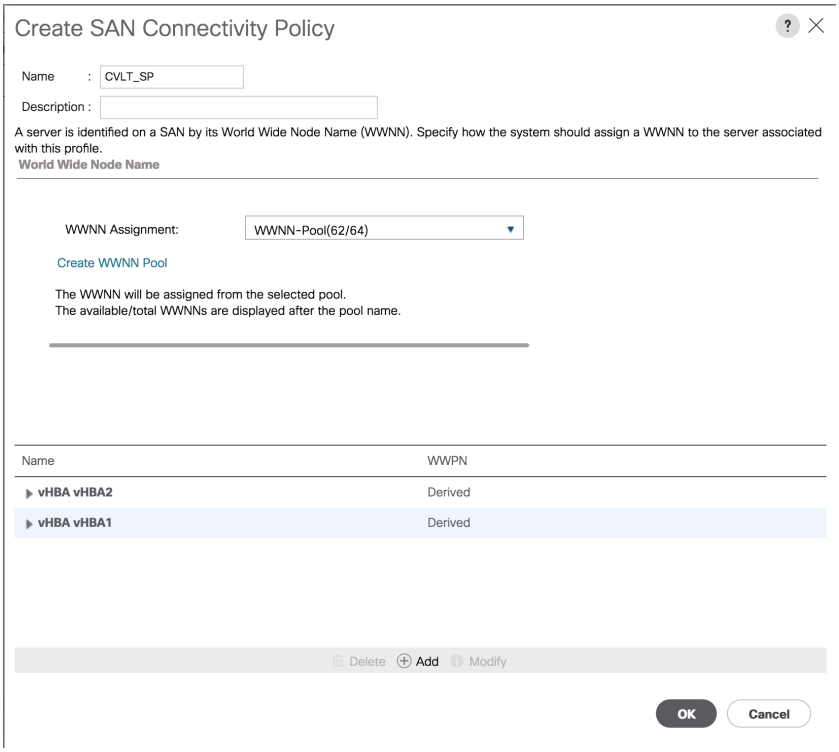
38. Click Add.



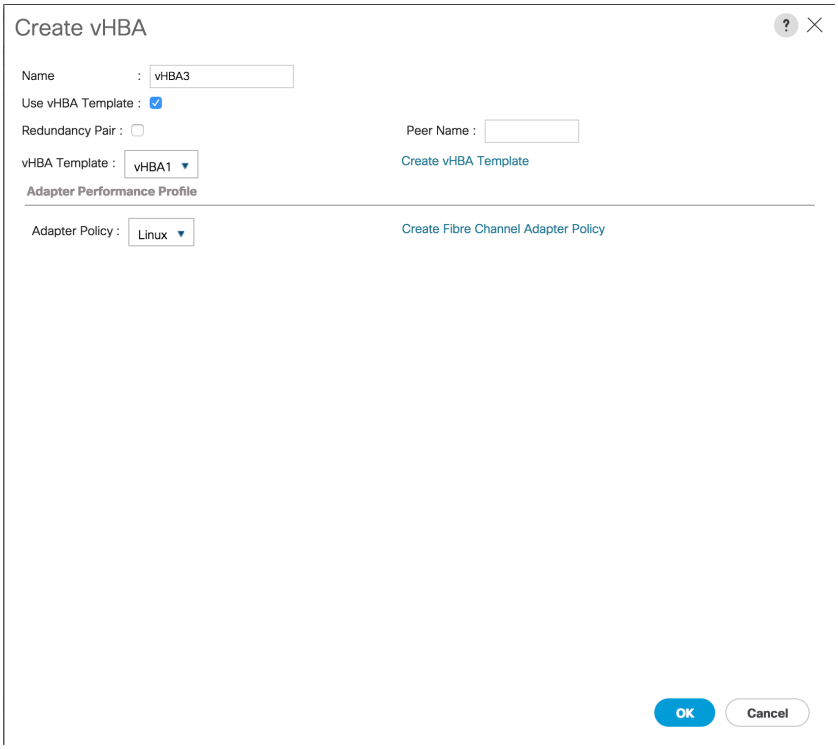
39. Enter an obvious name.
40. Select Use vHBA Template.
41. Select one of the vHBA templates.
42. Select Linux as the adapter policy.
43. Click OK.



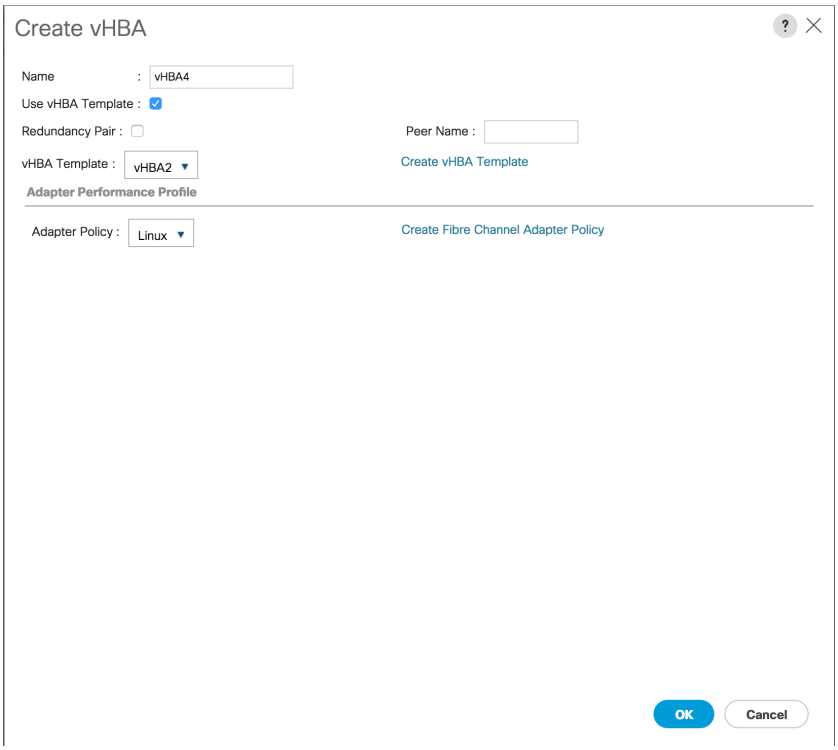
44. Click Add.



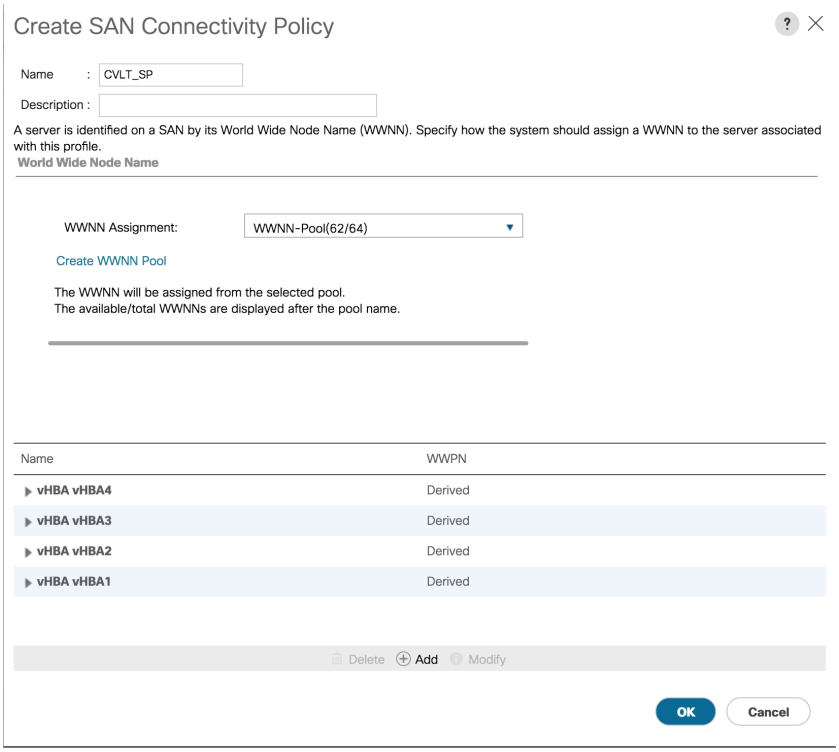
45. Enter an obvious name.
46. Select Use vHBA Template.
47. Select one of the vHBA templates.
48. Select Linux as the adapter policy.
49. Click OK.



50. Click Add.
51. Enter an obvious name.
52. Select Use vHBA Template.
53. Select one of the vHBA templates.
54. Select Linux as the adapter policy.
55. Click OK.



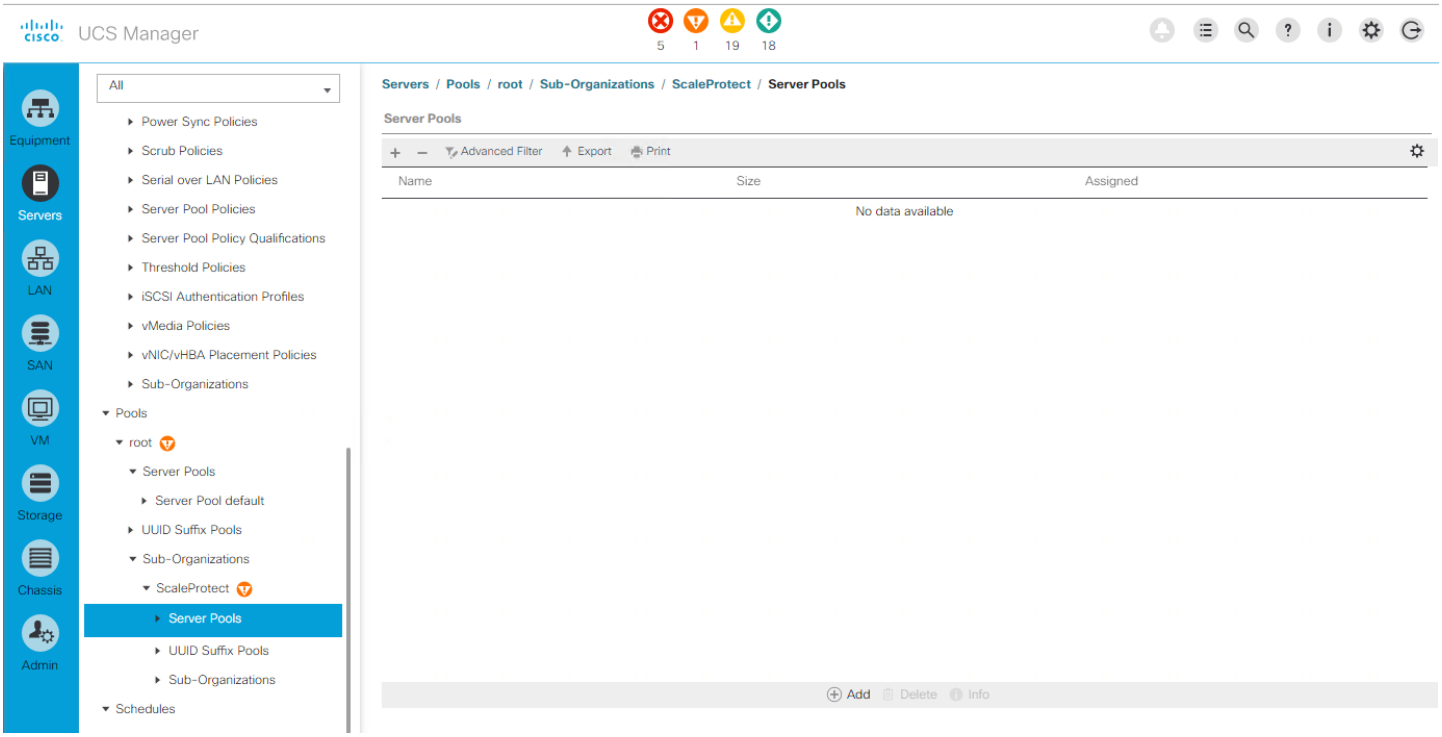
56. Click OK.



Configuring a server pool

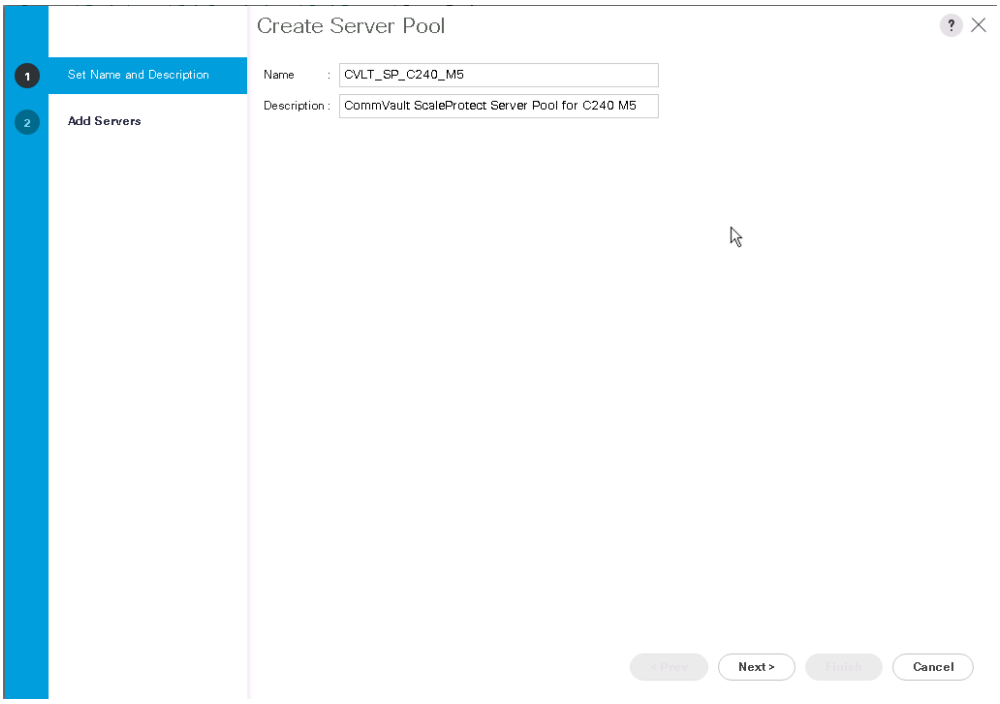
The next task is to define a server pool to collect all ScaleProtect with Cisco UCS servers in one place.

1. Choose Server > Pools > root > Sub-Organizations > ScaleProtect > Server Pool and click Add.

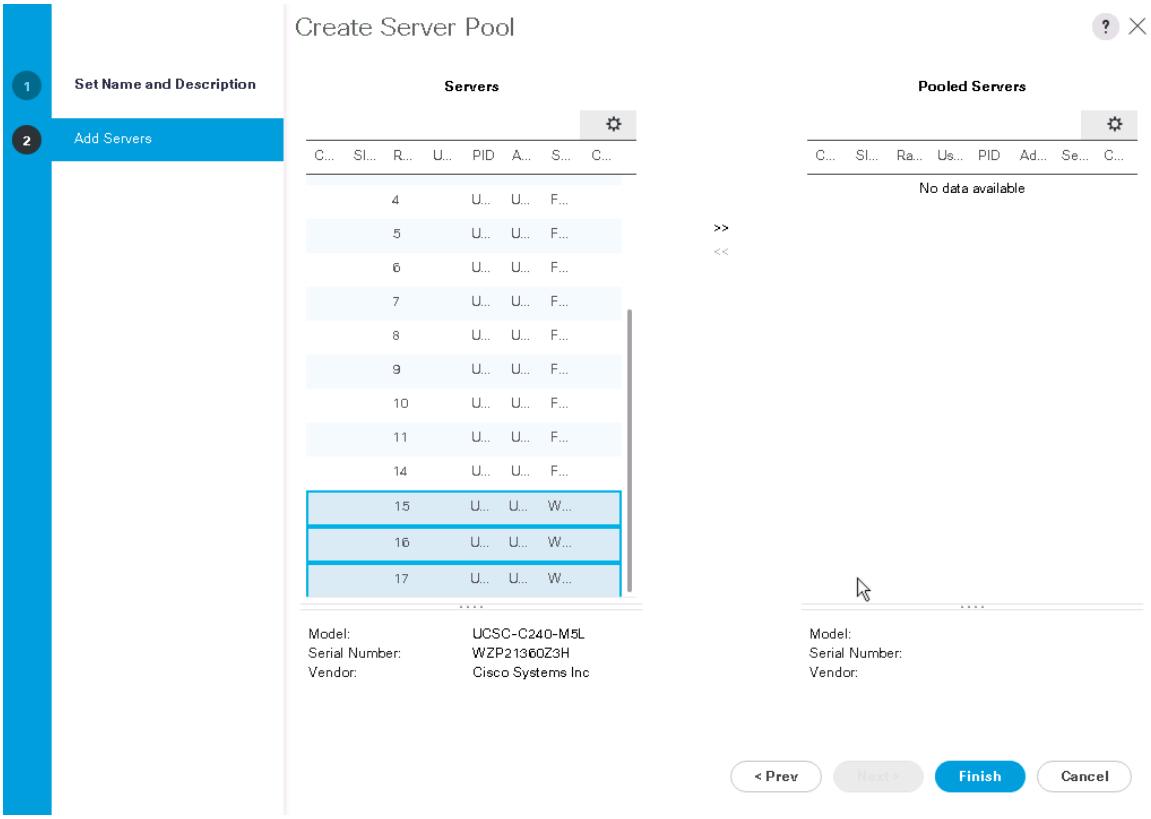


2. Enter an obvious name.

3. Click Next.



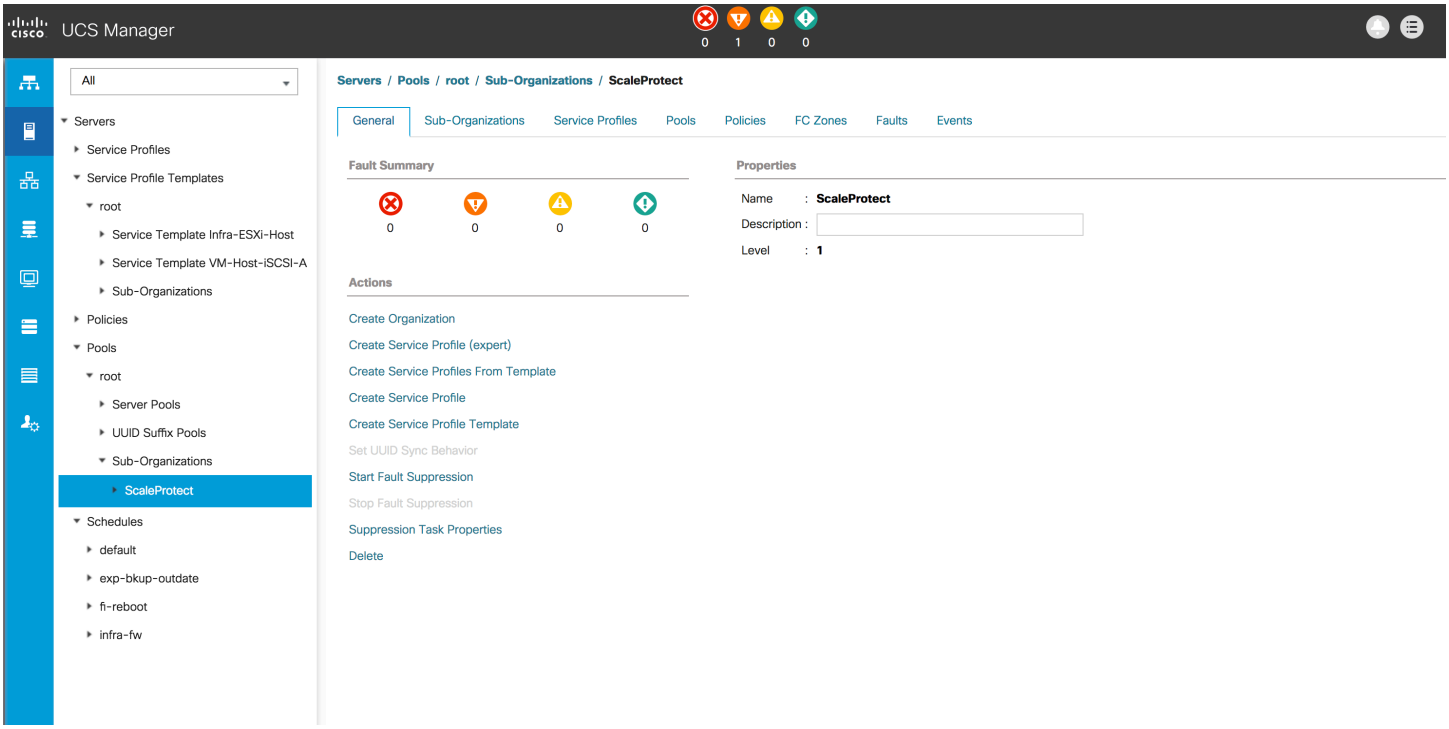
4. Click Finish.



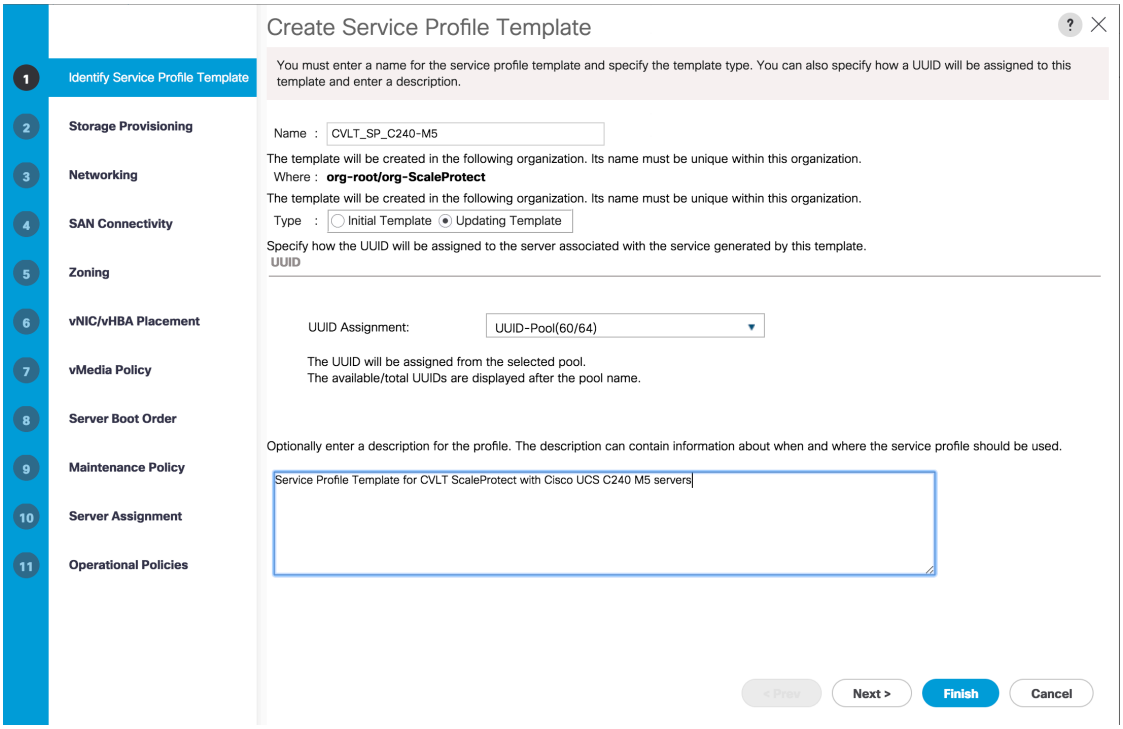
Configuring a service profile template

The final configuration task in Cisco UCS Manager is creating the service profiles. Because 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.

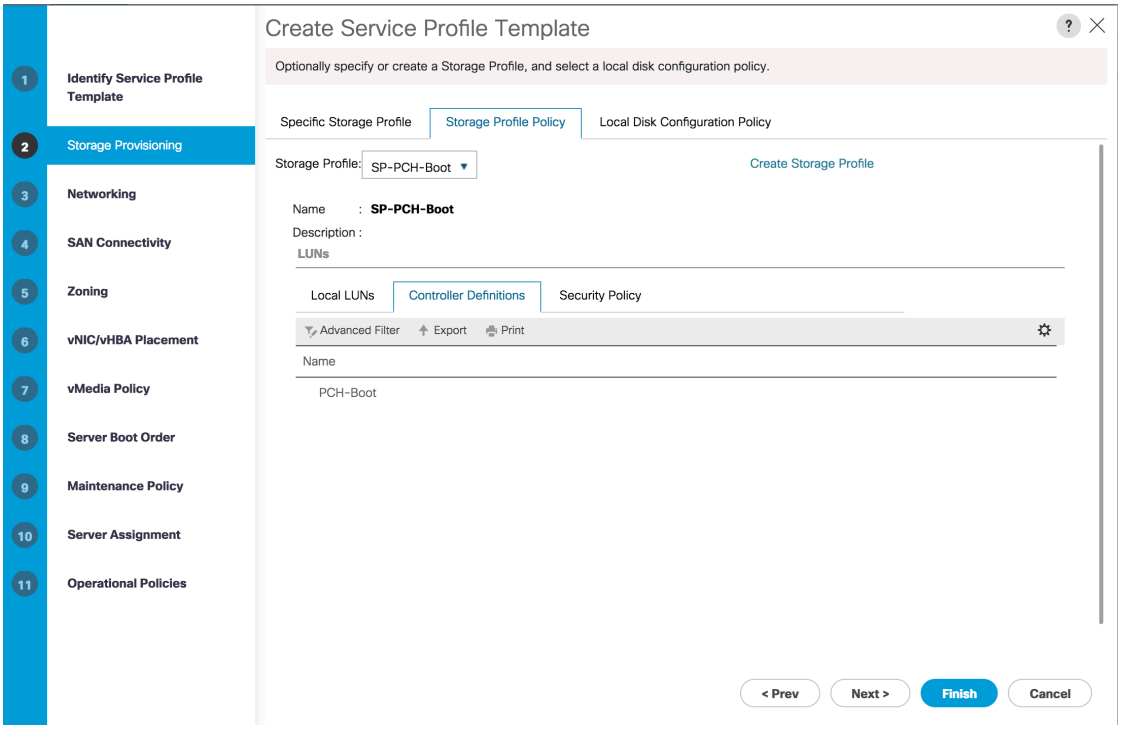
1. Choose Servers > root > Sub-Organizations > ScaleProtect and click Create Service Profile Template.



2. Enter an obvious name.
3. Select Updating Template.
4. Select a universally unique ID (UUID) pool with free IDs for UUID assignment.
5. Click Next.

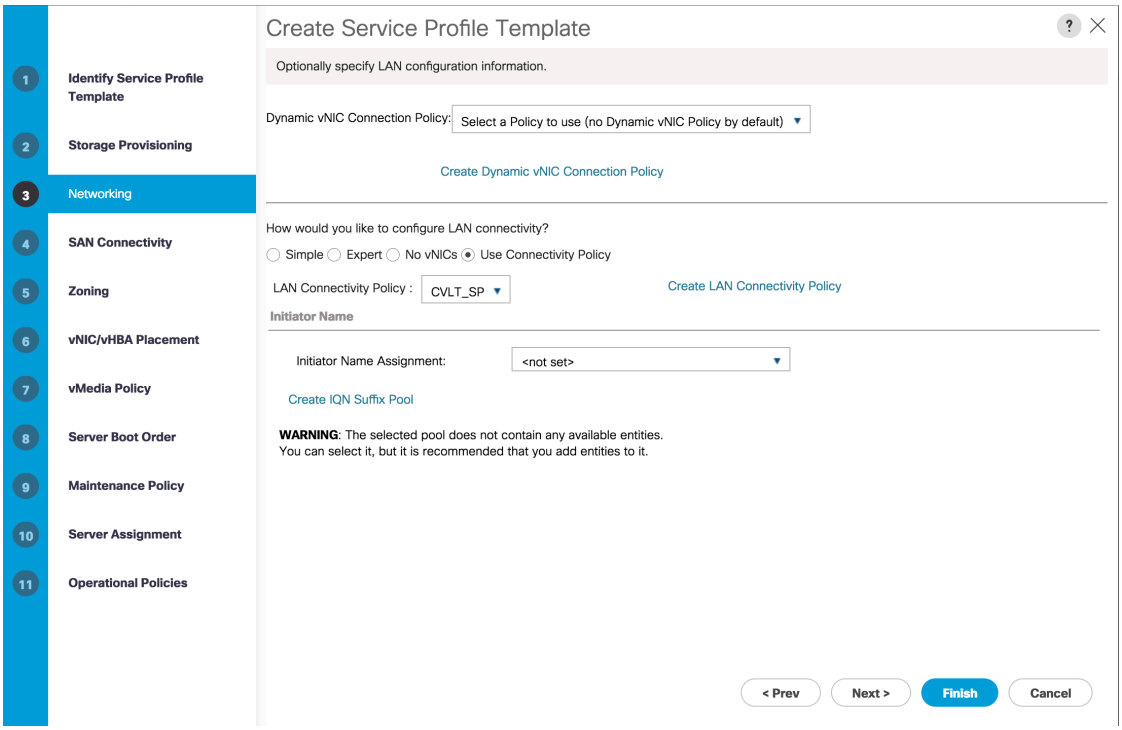


6. In the Storage Provisioning section, click the Storage Profile Policy tab.
7. Select the storage profile that you want (in the example here, SP-PCH-Boot is used).
8. Click Next.

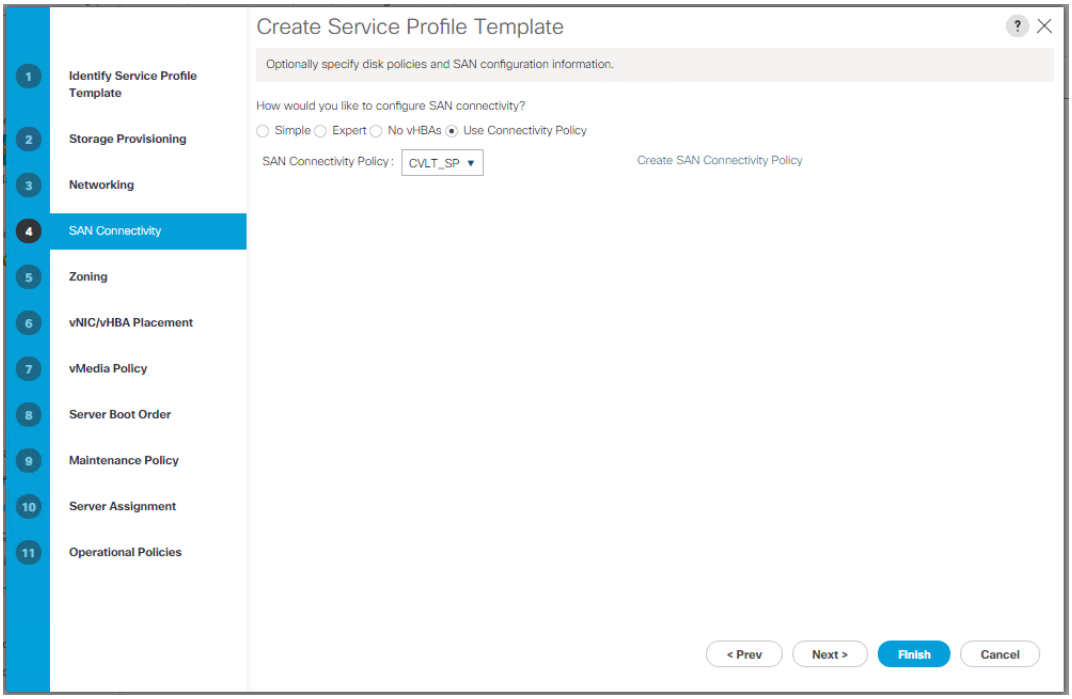


9. In the Networking section, select the Use Connectivity Policy button.
10. Select CVLT_SP as the LAN connectivity policy.

11. Click Next.

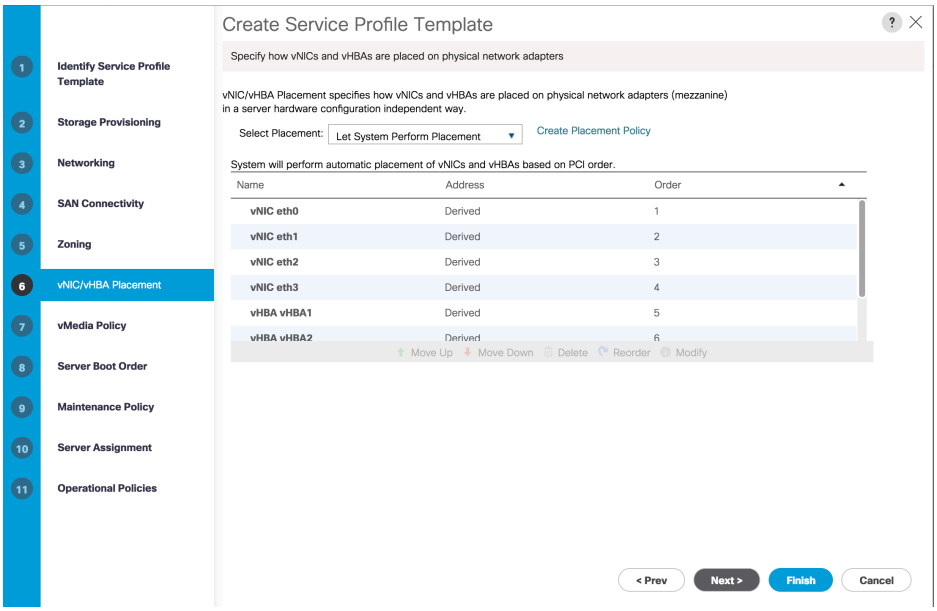


12. In the SAN connectivity section, select Use Connectivity Policy
13. Select CVLT_SP as the SAN connectivity policy.
14. Click Next.

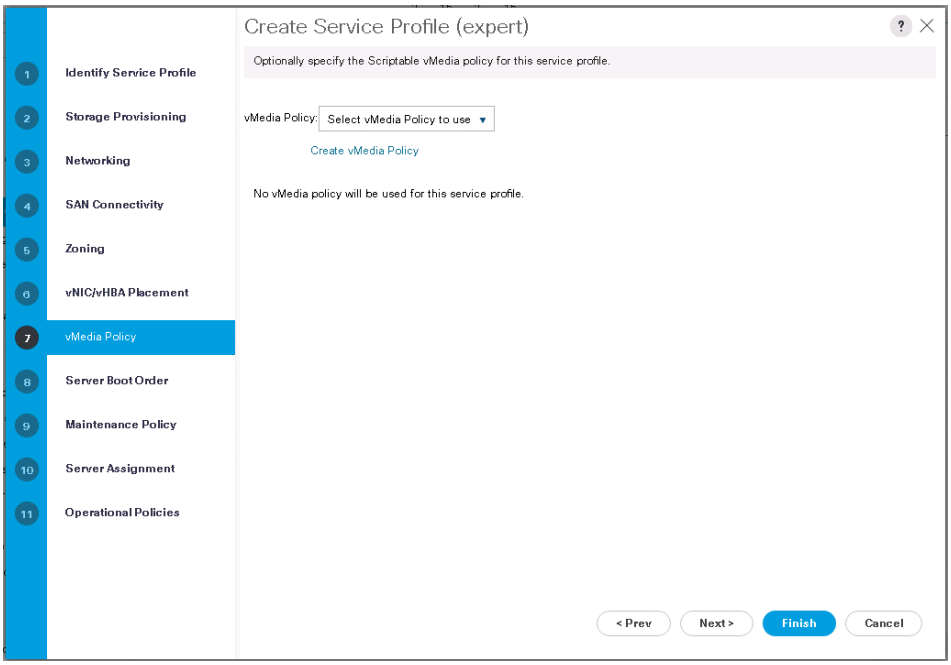


15. In the Zoning section, click Next.

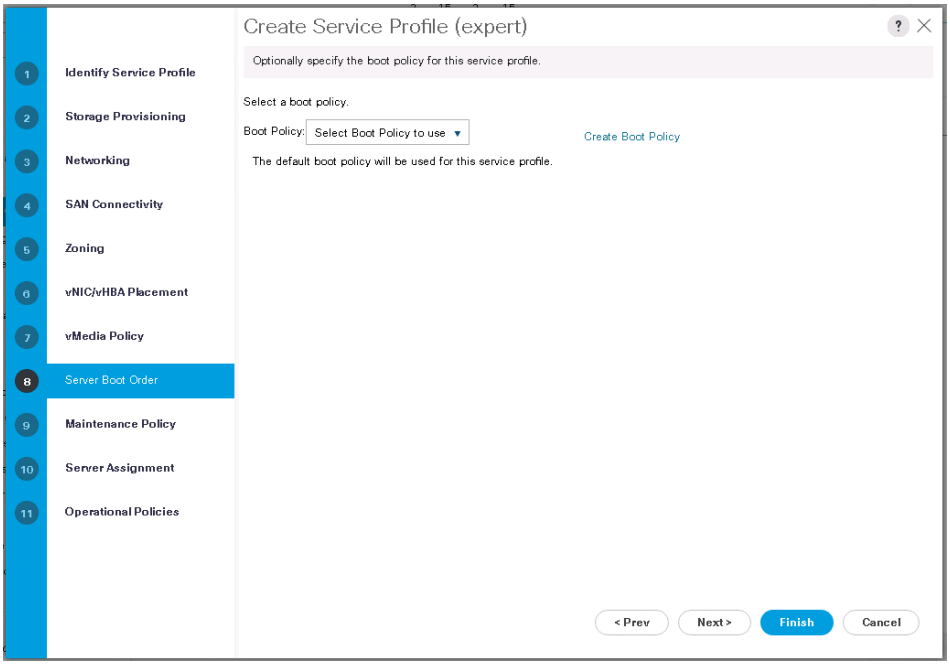
16. In the vNIC/vHBA Placement section, leave the setting Let System Perform Placement. With this setting, Cisco UCS will automatically distribute the vNIC and vHBA across both system I/O controllers (SIOCs) if they are available.
17. Click Next.



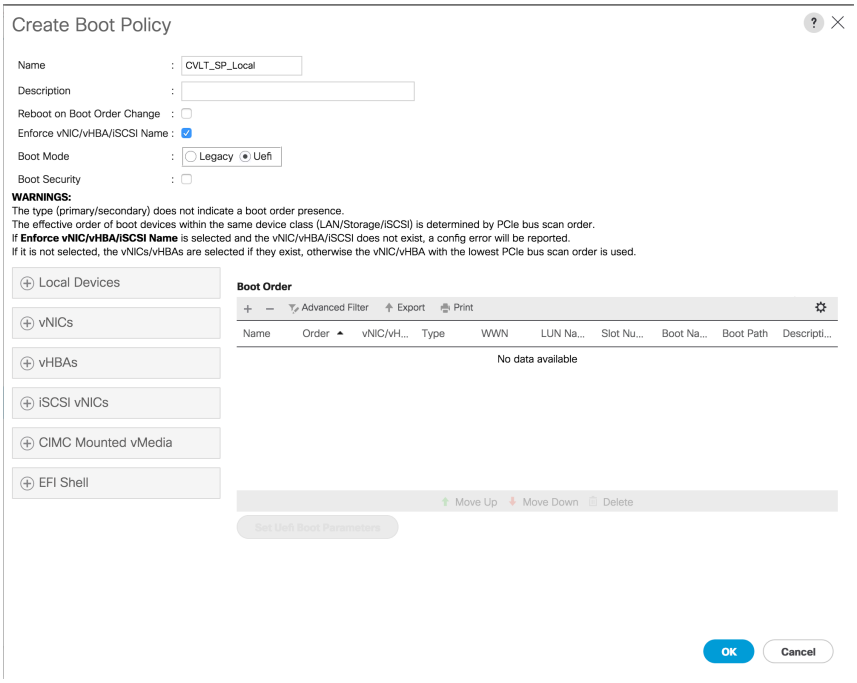
18. In the vMedia Policy section, click Next.



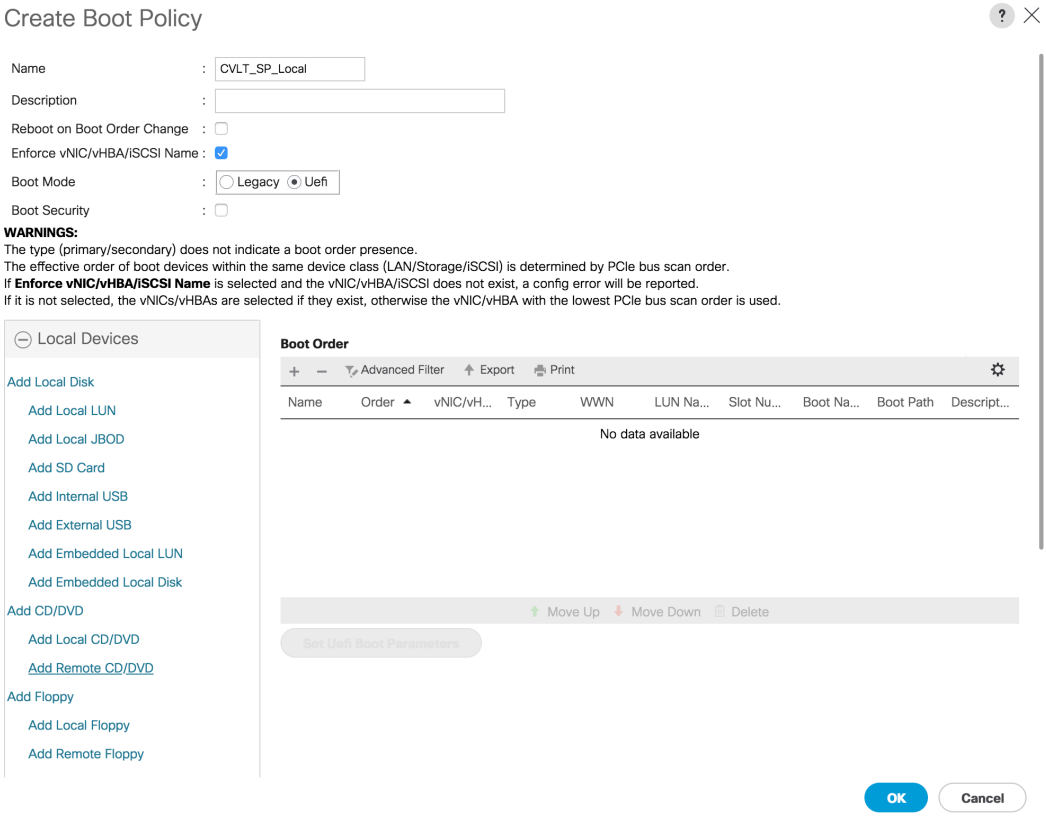
19. In the Server Boot Order section, click Create Boot Policy.



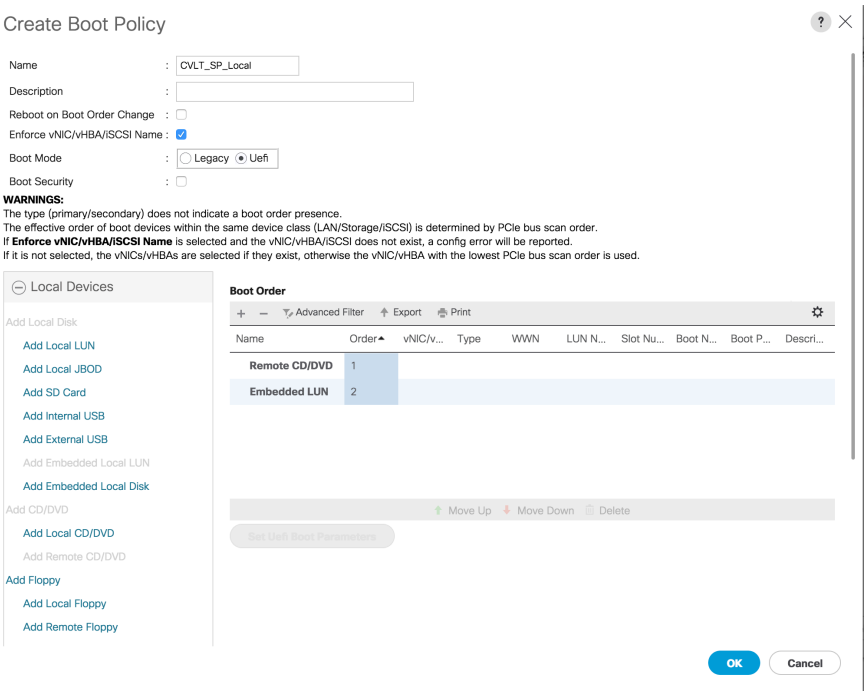
20. Enter an obvious name and a description.
21. Click the Uefi radio button to change the boot mode.



22. Click Local Devices.
23. Click Add Remote CD/DVD.

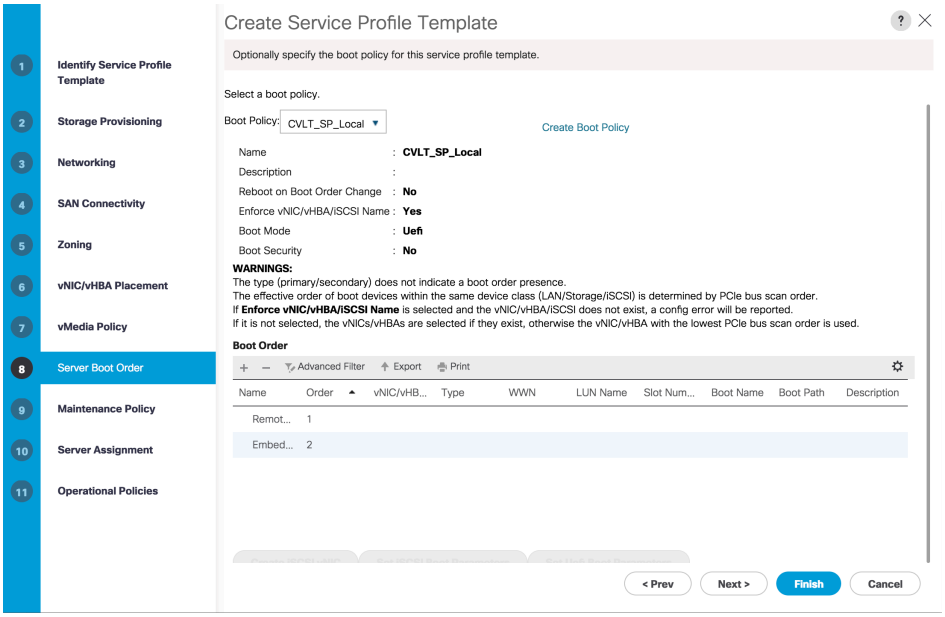


24. Click Add Embedded Local LUN

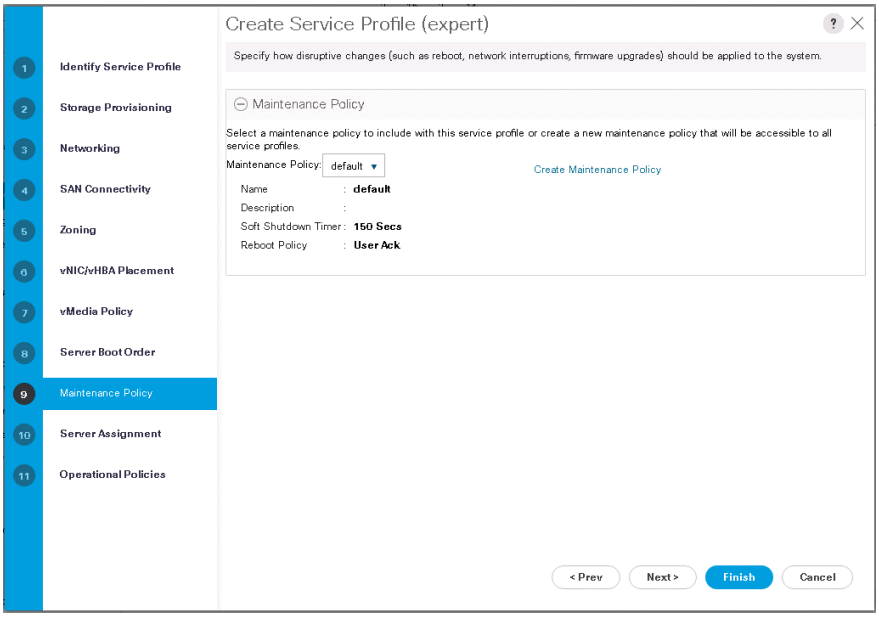


25. Click OK.

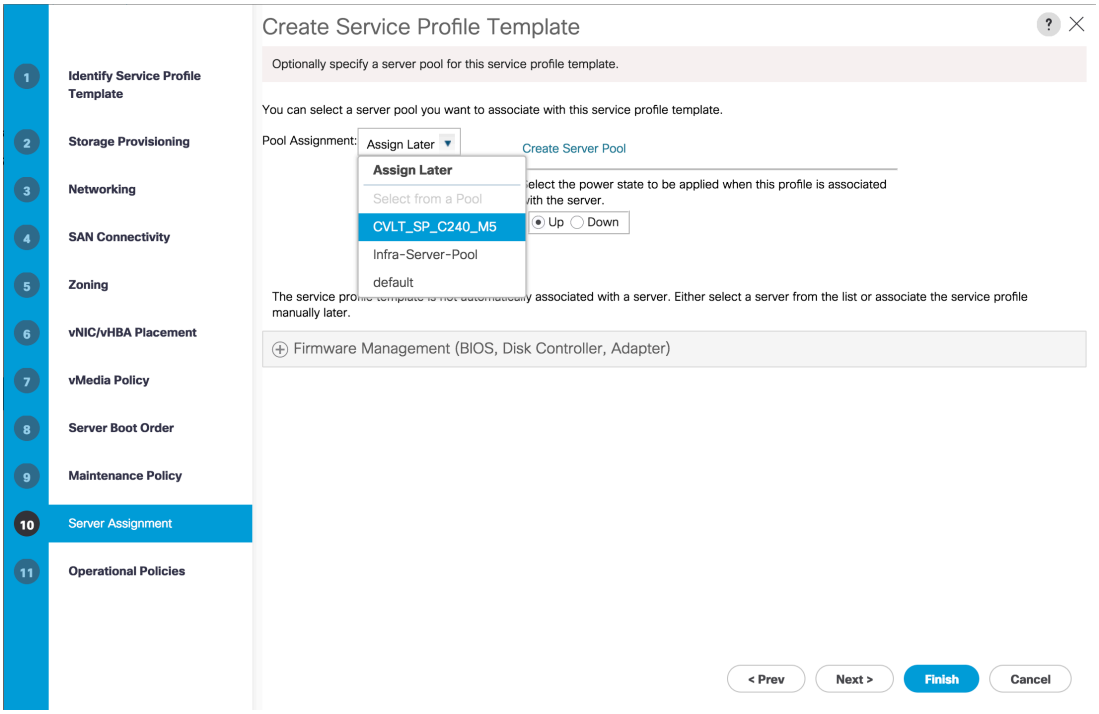
26. Click Next.



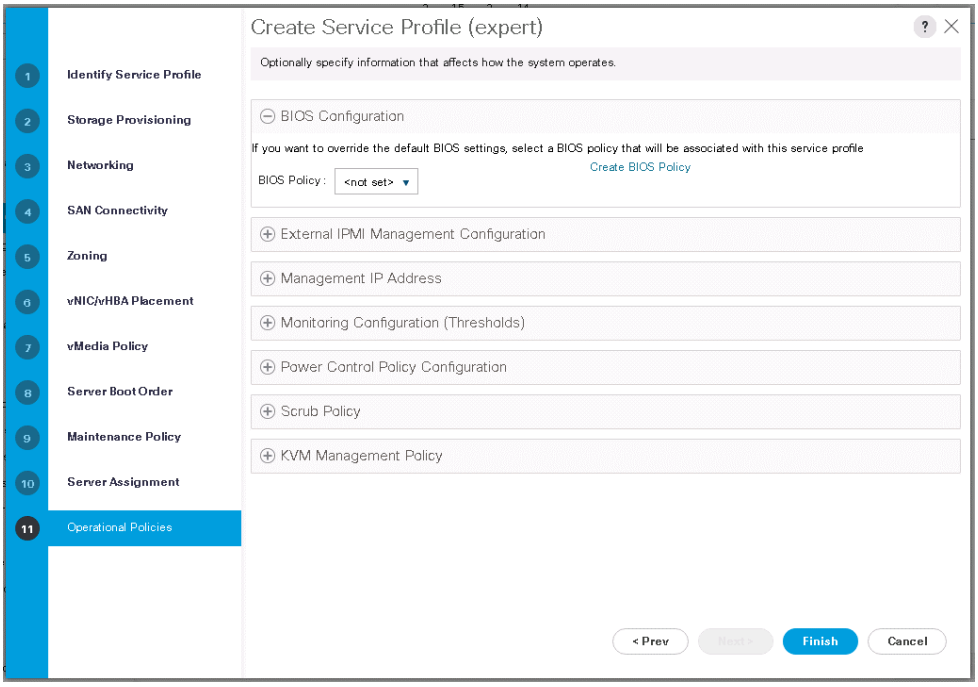
27. In the Maintenance section, select default for Maintenance Policy.
28. Click Next.



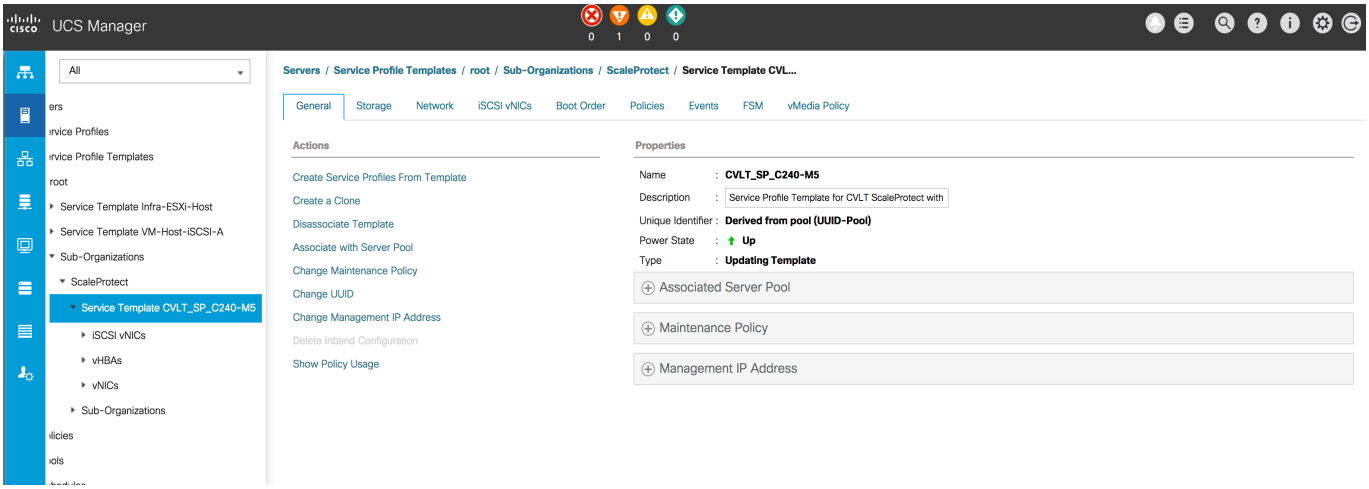
29. In the Server Assignment section, select the server pool and server pool qualification policy created for Server 1.
30. Click Next.



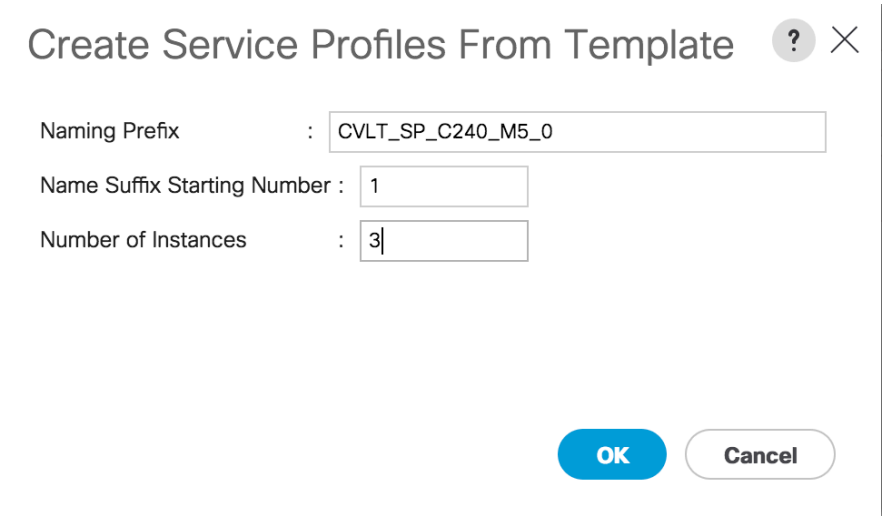
31. In the Operational Policies section, select the policies required for your installation.
    ScaleProtect with Cisco UCS does not require you to select any particular options.
32. Click Finish.



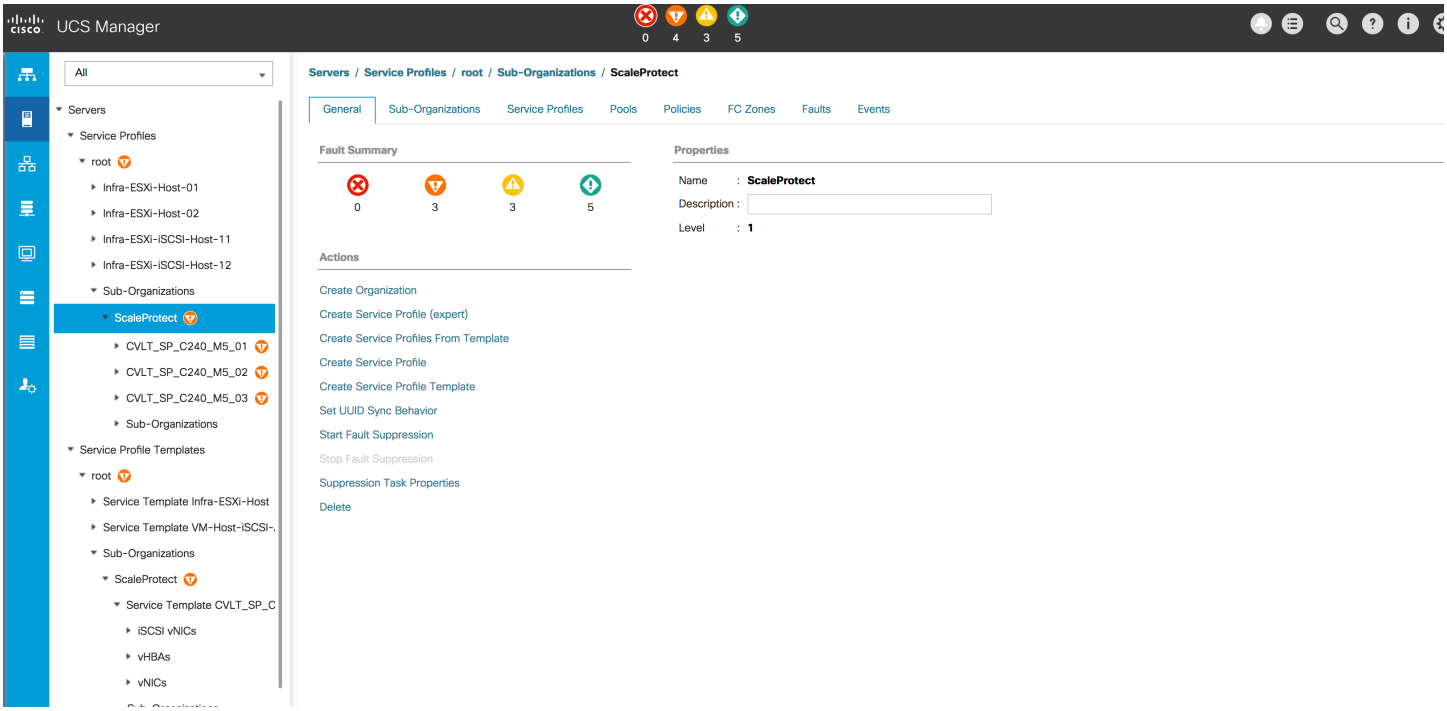
33. Click the service profile template that you created.
34. Click Create Service Profiles from Template.



35. Enter a naming prefix and the number of instances to create.
36. Click OK.



37. Click OK.
38. Check the result in the Service Profiles section.



The assignment of the service profile to the physical server will take some time. View 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 Software installation and configuration

CommServe installation

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

ScaleProtect with Cisco UCS node installation and configuration

Use the following procedures to install the ScaleProtect with Cisco UCS software on the Cisco UCS C240 rack server.

If you are using Cisco UCS manager, log into Cisco UCS and launch the KVM manager from there to connect to the nodes.

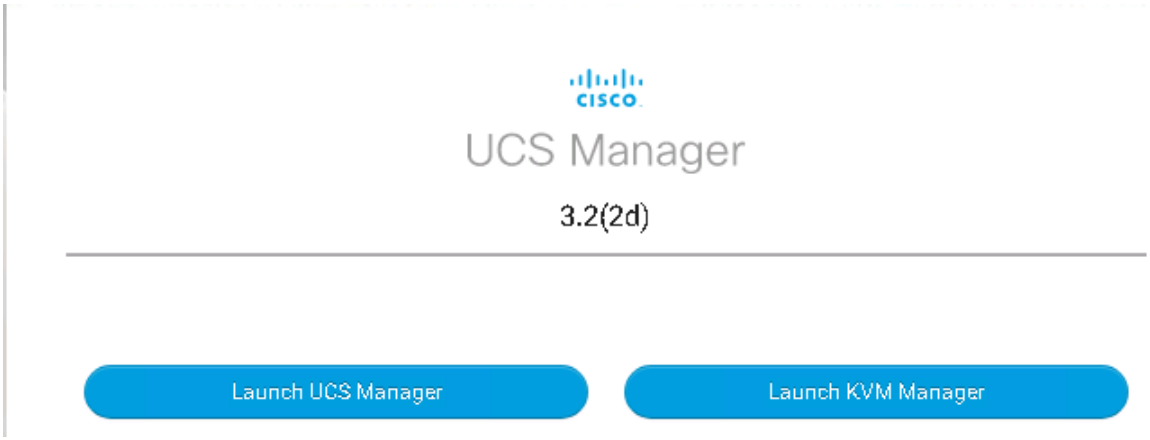
If you are not using Cisco UCS manager, log in to the IMC for the node and launch the KVM from there for each node.

Be sure that you have the latest copy of the Commvault HyperScale Software ISO downloaded from cloud.Commvault.com.

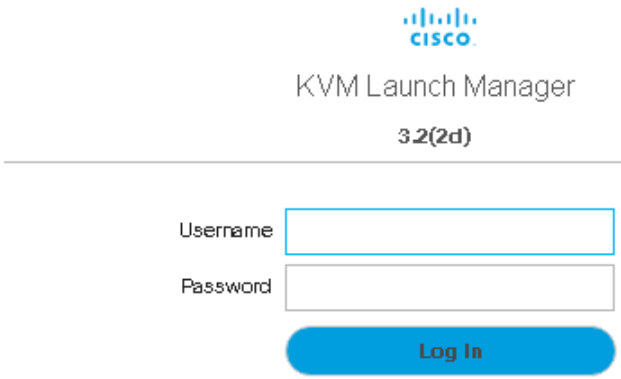
Using Cisco UCS Manager to launch the software installation process

Follow these steps to start the software installation process using Cisco UCS Manager.

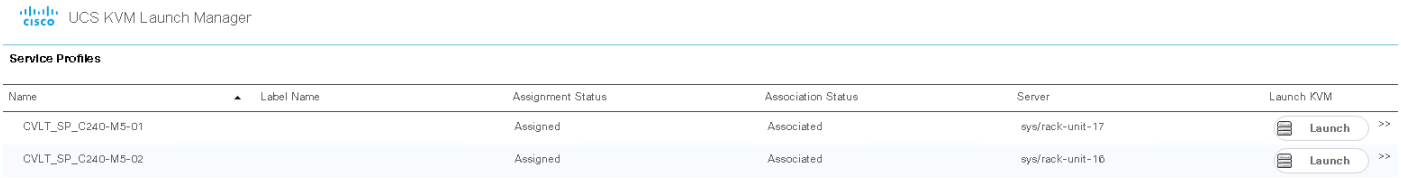
1. Log in to Cisco UCS Manager and click Launch KVM Manager.



2. Enter the proper credentials and click Log In.

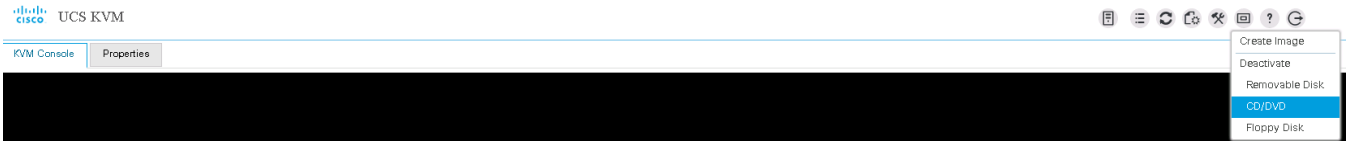


3. Click Launch for the server on which you want to install the software.

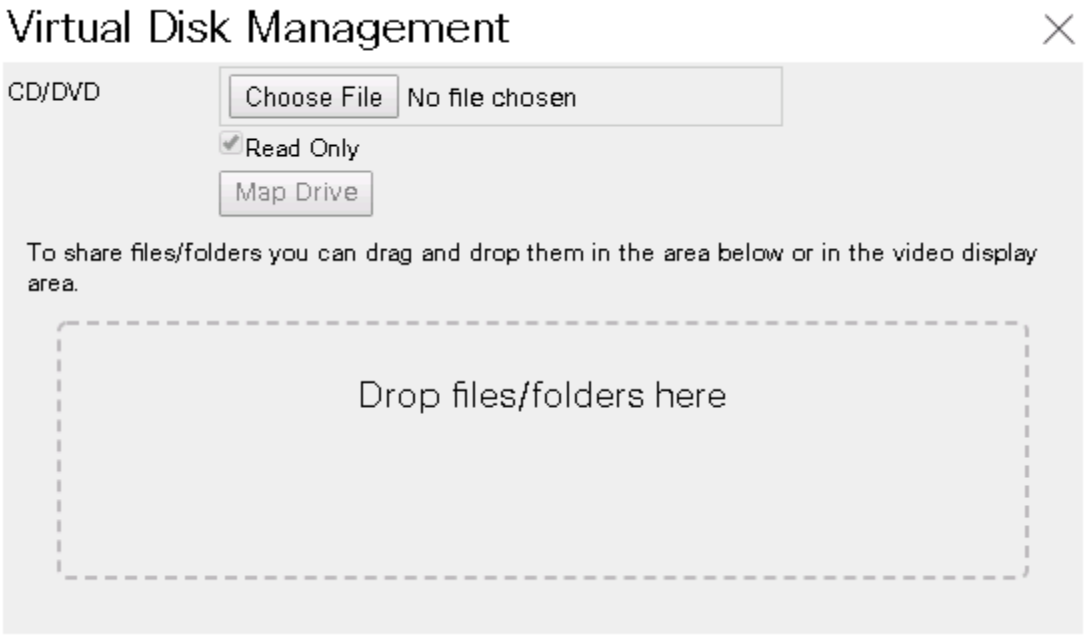


4. Click the virtual media icon and choose Activate Virtual Devices.

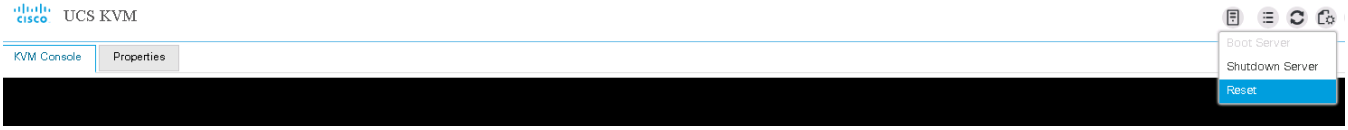
5. Click the virtual media icon again and choose CD/DVD.



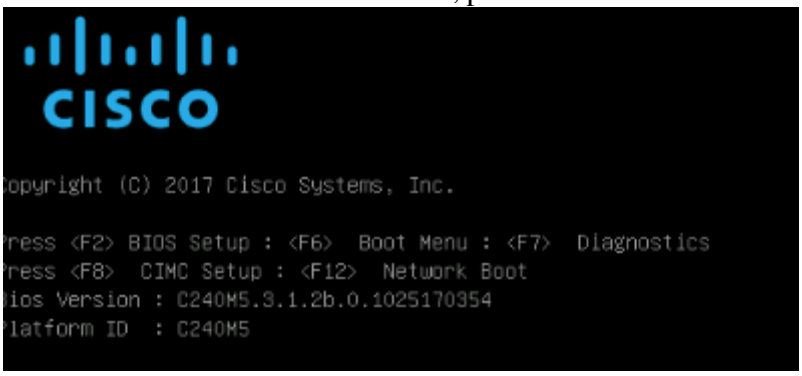
6. Click Choose File and select the Commvault HyperScale Software ISO. Then click Map Drive.



7. Click the Server Action icon and then boot the server if it is powered down or reset the server if it is already running. If you are resetting the server, click OK on the Reset Server pop-up screen.



1. After the server reboots, press F6 to enter the boot menu.



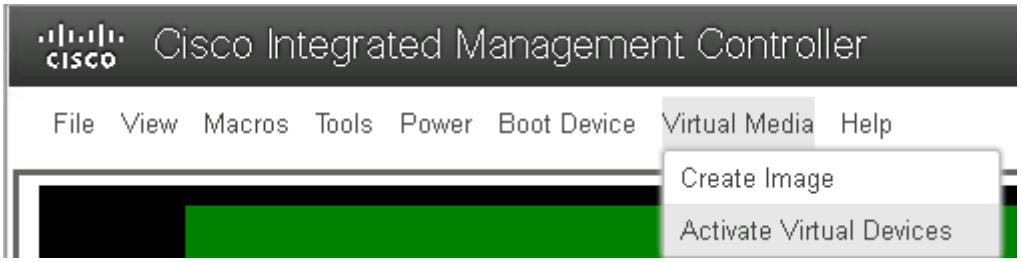
Using Cisco IMC to launch the software installation process

Follow these steps to start the software installation process using the IMC.

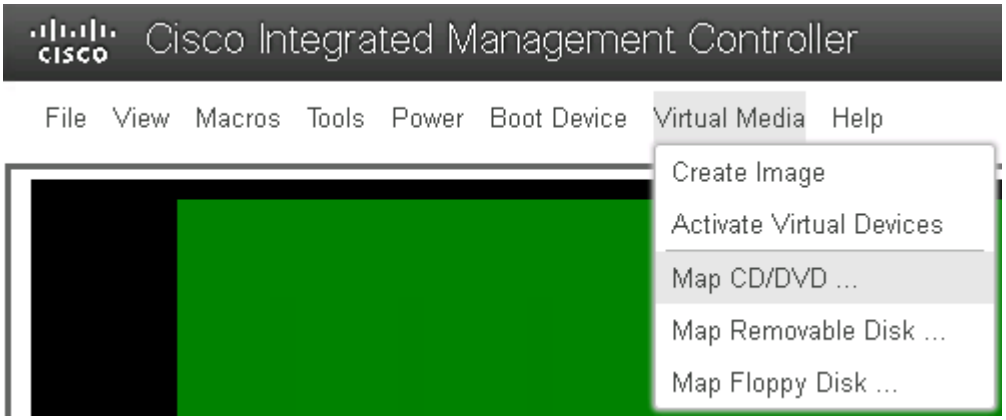
1. Log in to the IMC using the IP address of the chassis. Log in with the proper credentials.

2. In the upper-right corner, click Launch KVM. Then select either the Java- or HTML-based process.

3. Click the Virtual Media menu and choose Activate Virtual Devices.

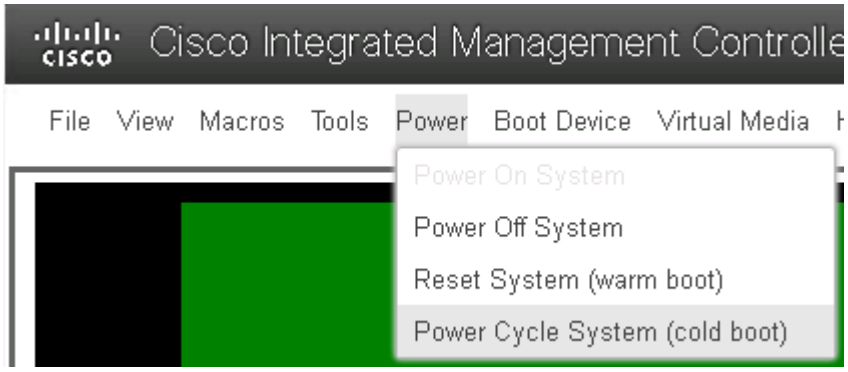


4. Click the Virtual Media menu again and choose Map CD/DVD.

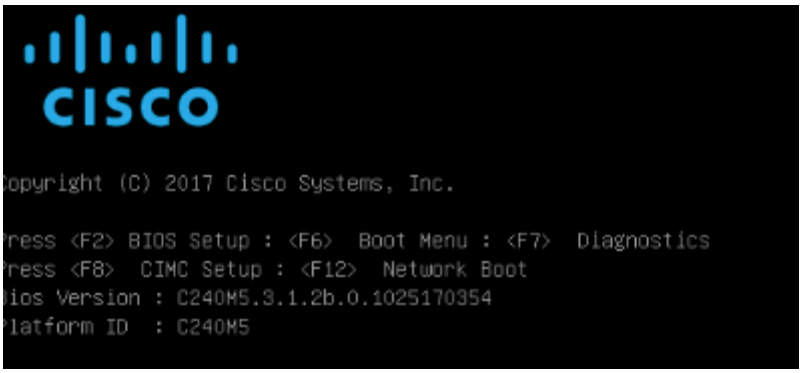


5. Click Browse and select the Commvault HyperScale Software ISO. Then click Map Drive.

6. Click the Power menu and choose Power Cycle System (cold boot). Then click OK in the Are You Sure pop-up screen.



7. After the server reboots, press F6 to enter the boot menu.



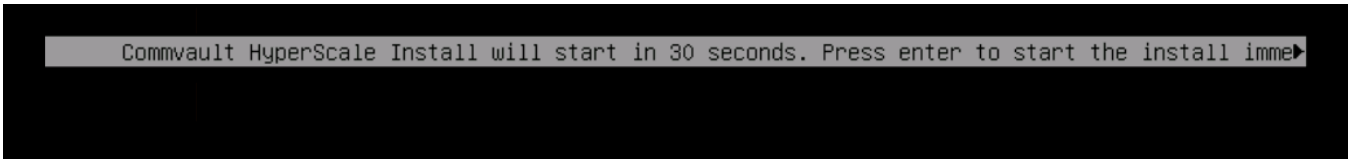
Installing the software

Now install the software.

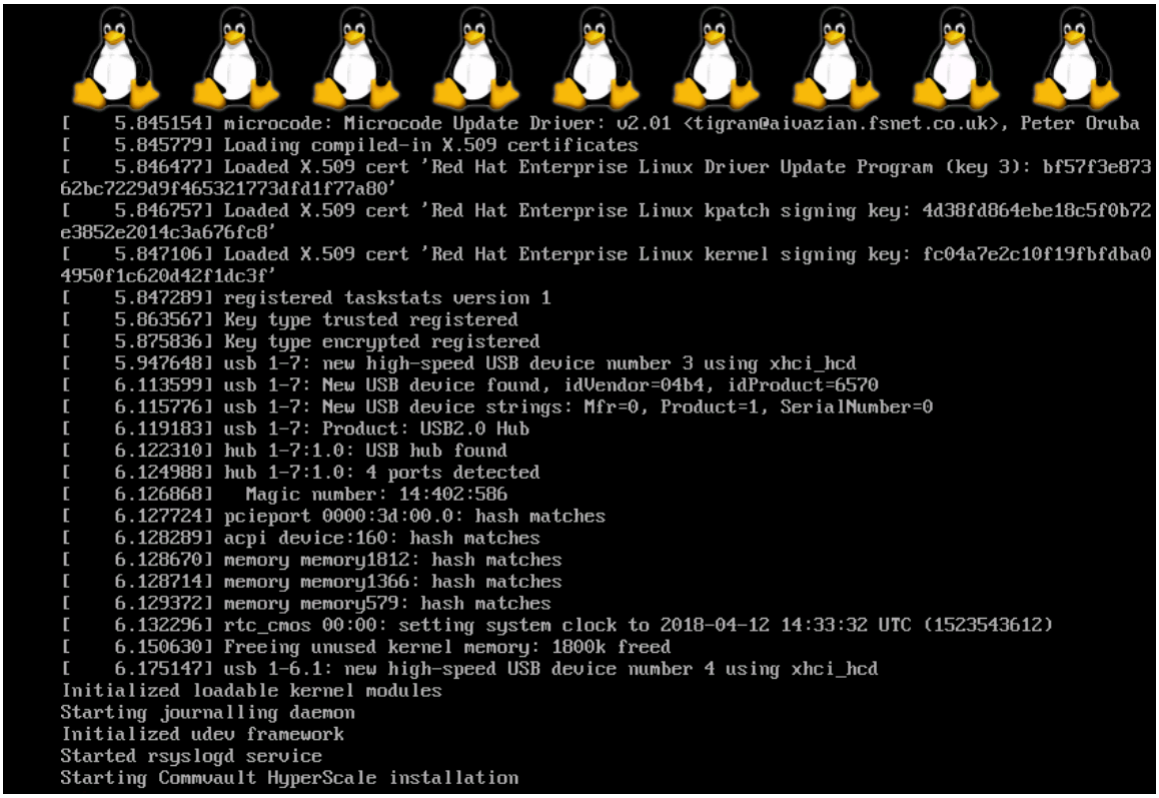
Before starting the installation, enter the nodes in the Domain Name System (DNS) serving your environment.

spc240m5node3	Host (A)	192.168.20.225	static
spc240m5node2	Host (A)	192.168.20.223	static
spc240m5node1	Host (A)	192.168.20.221	static

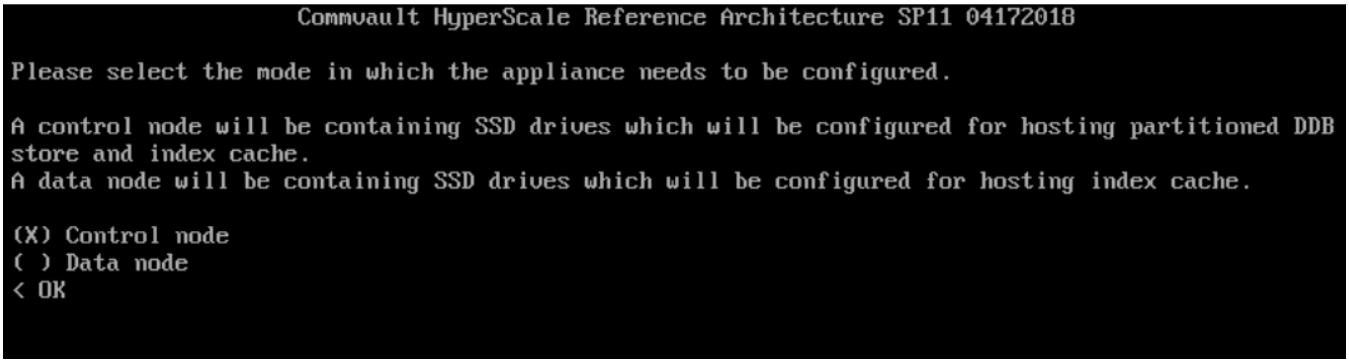
1. Press Enter to start.



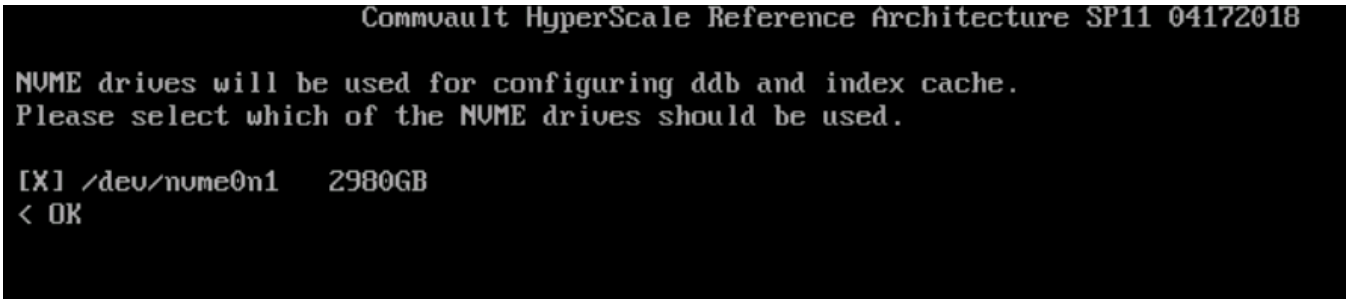
The process can take a while. In the demonstration for this document, 7 minutes elapsed between the key press and the appearance of the next screen, with just a black screen displayed during this interval.



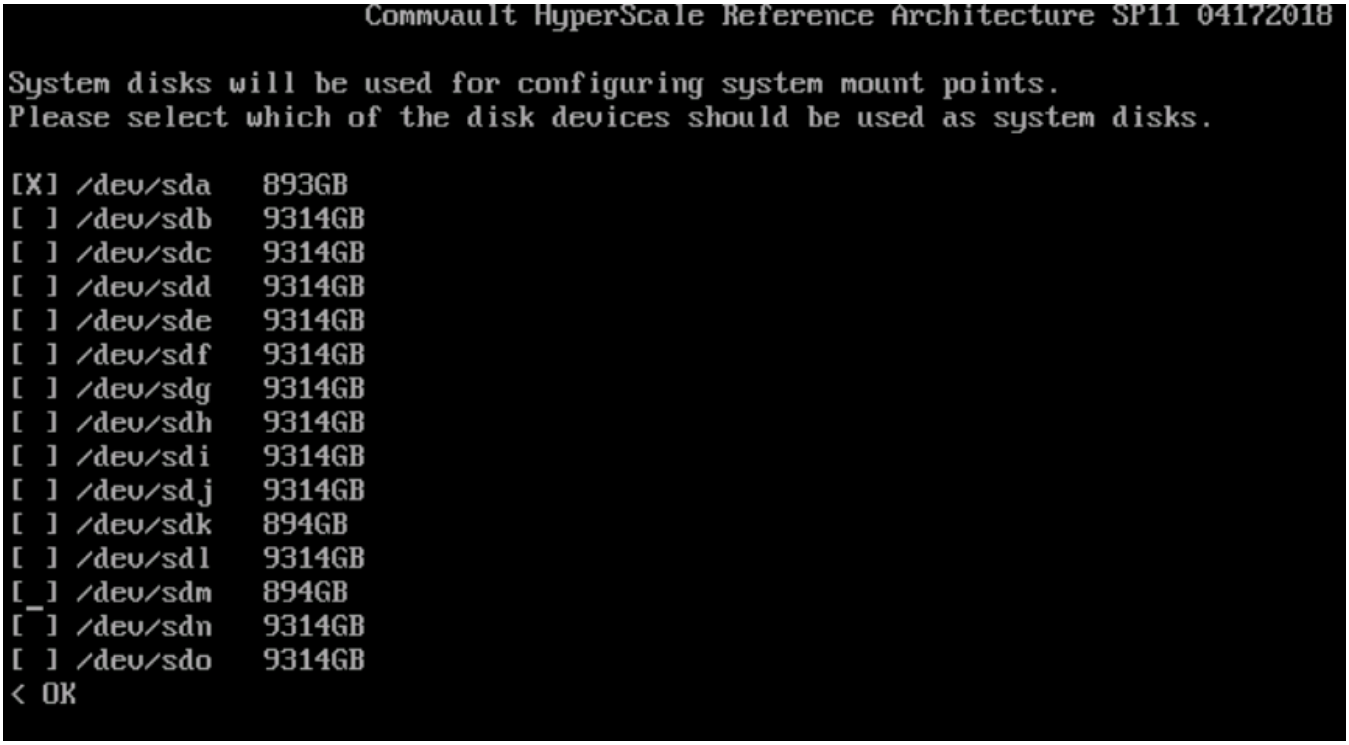
2. Select “Control node.”



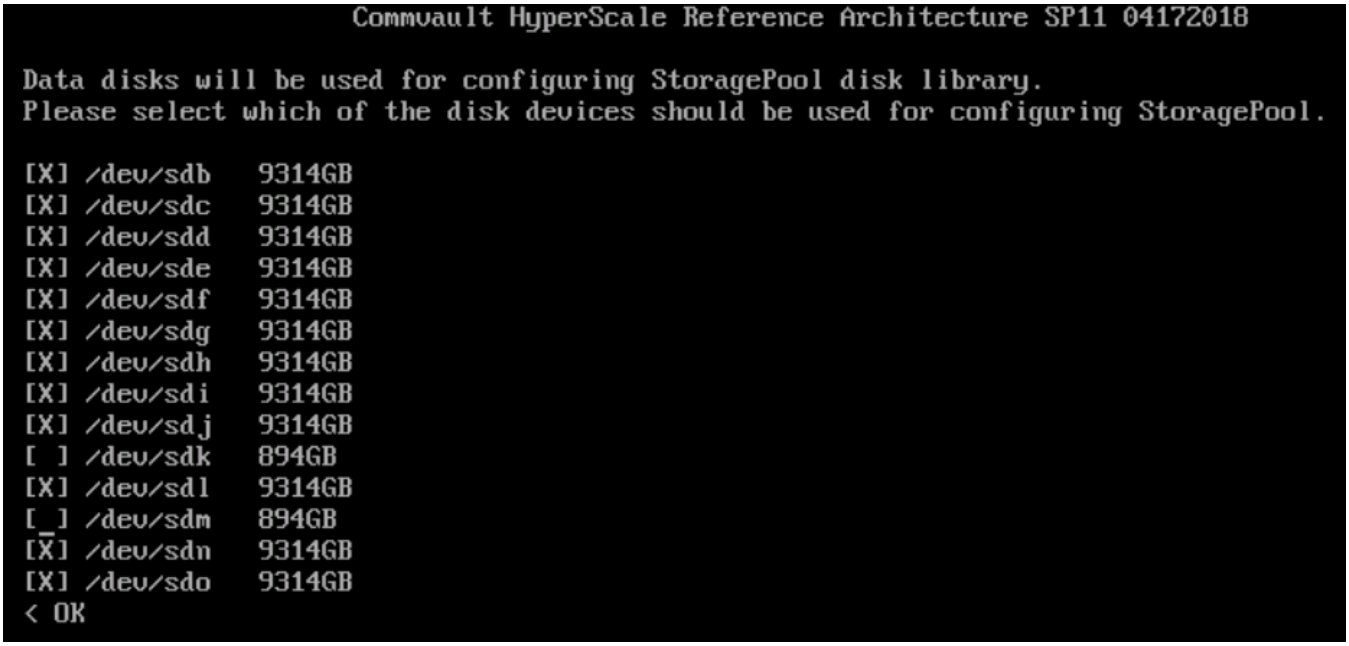
3. Select the NVMe card for the deduplication database (DDB) and index cache.



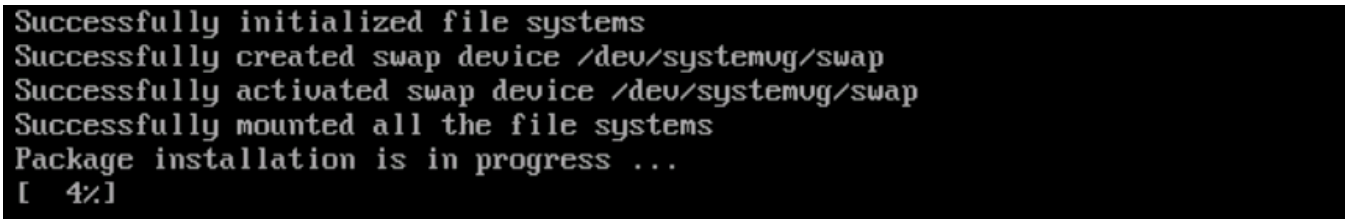
4. Select the RAID 1 (2 x 960-GB M.2) cards. Then select OK. The logical device /dev/sda is the Raid 1 virtual drive configured using the internal M.2 cards.



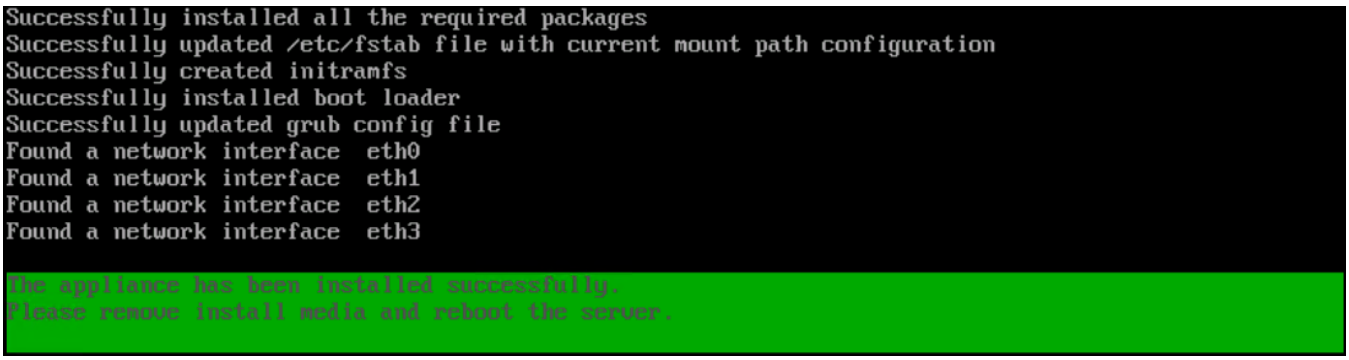
5. Select the 12 x 10-TB drives for the storage disks presented to the operating system. Then select OK.



6. Wait until the package installation is complete.



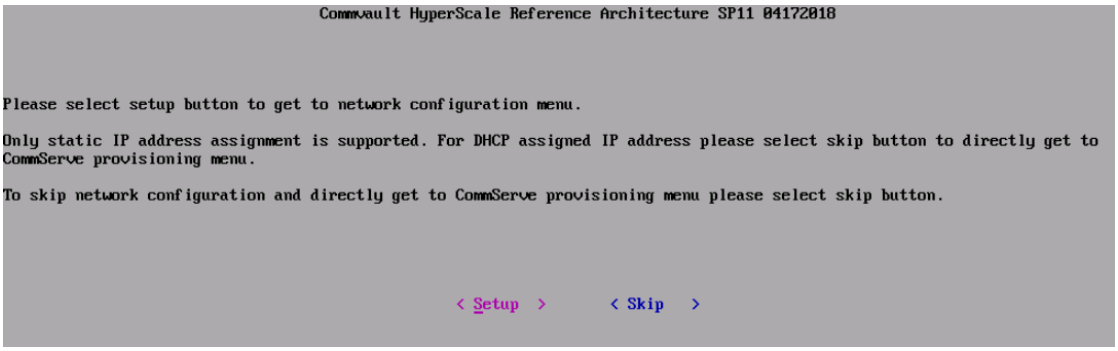
7. When the process is complete, reboot the server.



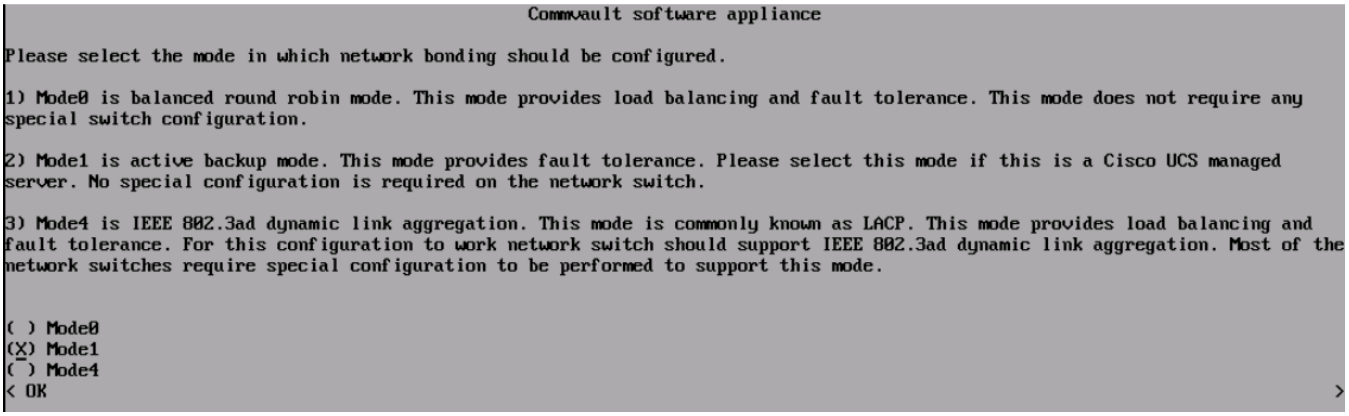
8. After the server reboots, log in as user **root** with password **cvadmin**. Then change to the /opt/Commvault/MediaAgent directory and run **setupsds**.

9. Enter the host name and password.

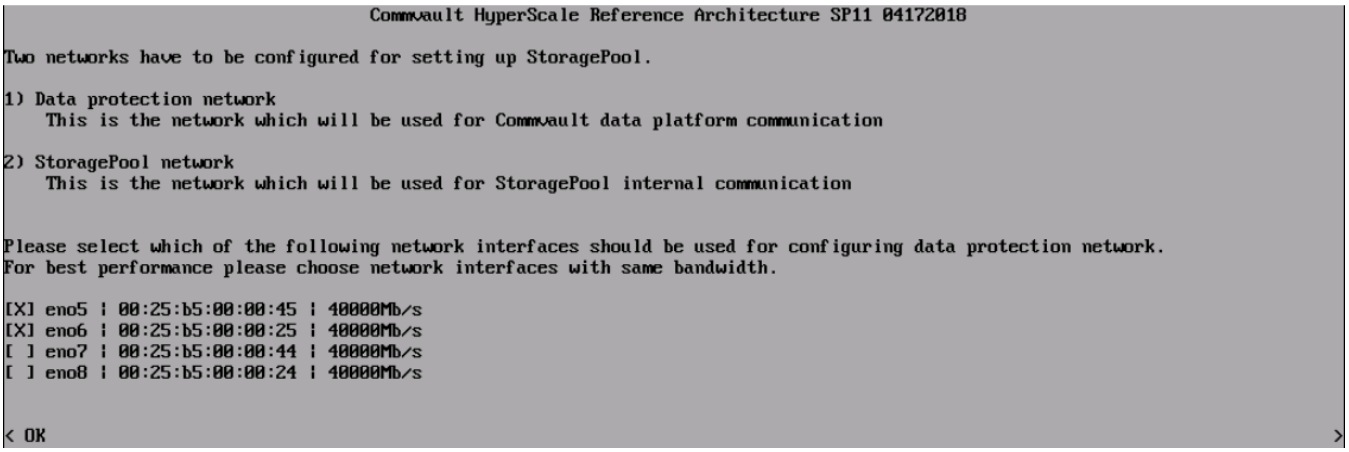
10. Select Setup to configure the static IP addresses.



11. Select Mode 1 for a Cisco UCS managed setup.

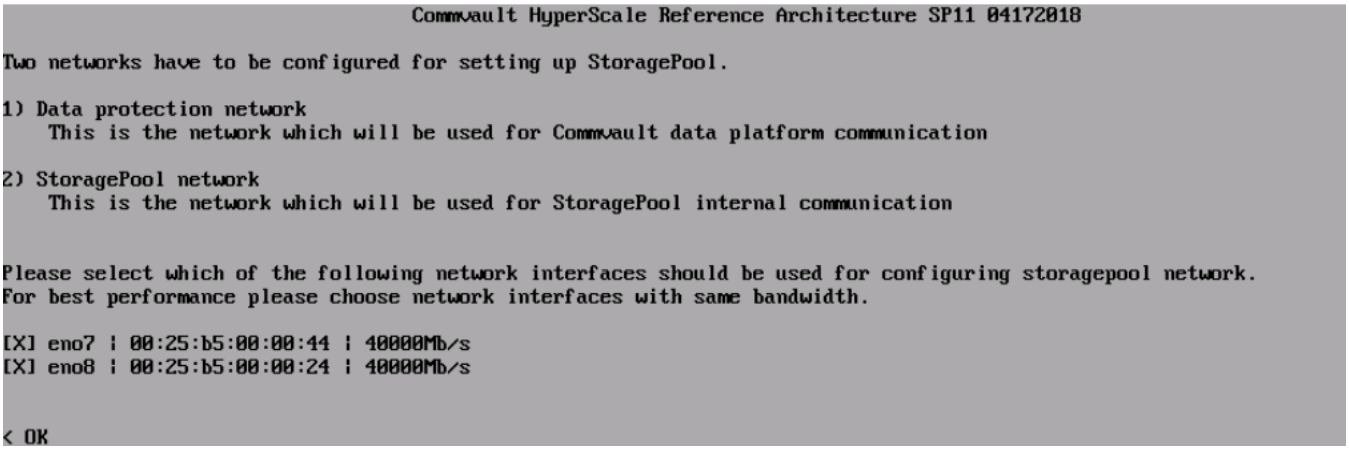


12. Select the NICs to be used for data protection operations.

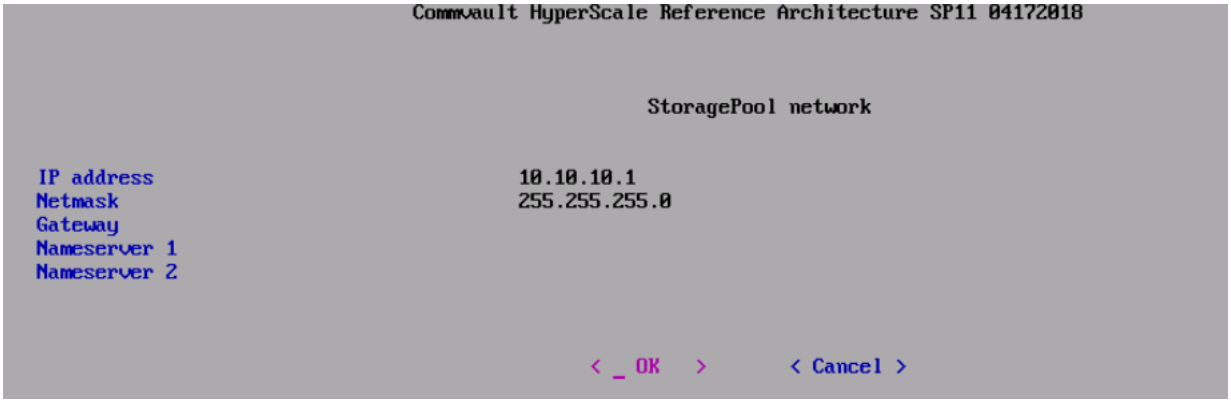


13. Set the IP address for the data protection network.

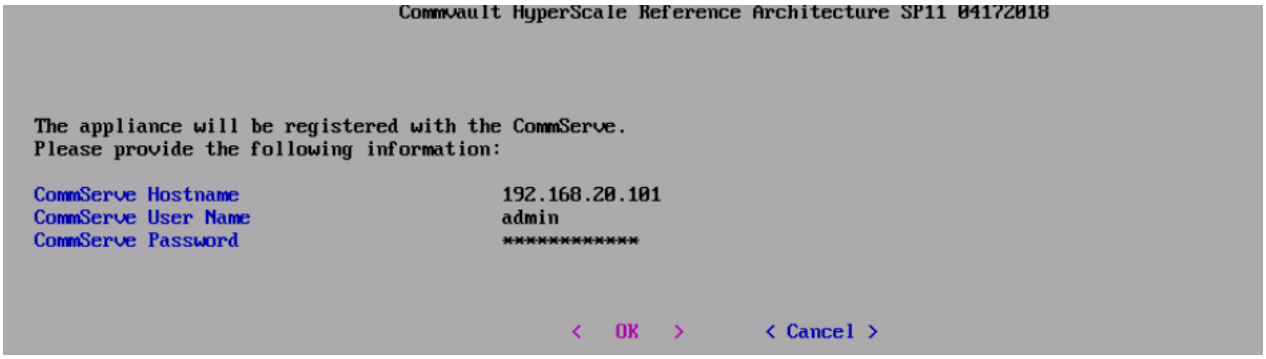
14. Select the NICs for the storage pool network.



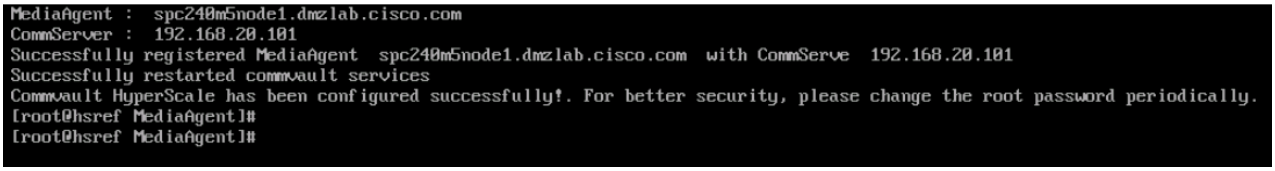
15. Enter the IP address information for the storage pool network.



16. Enter the CommServe information.



The installation on this node is complete.



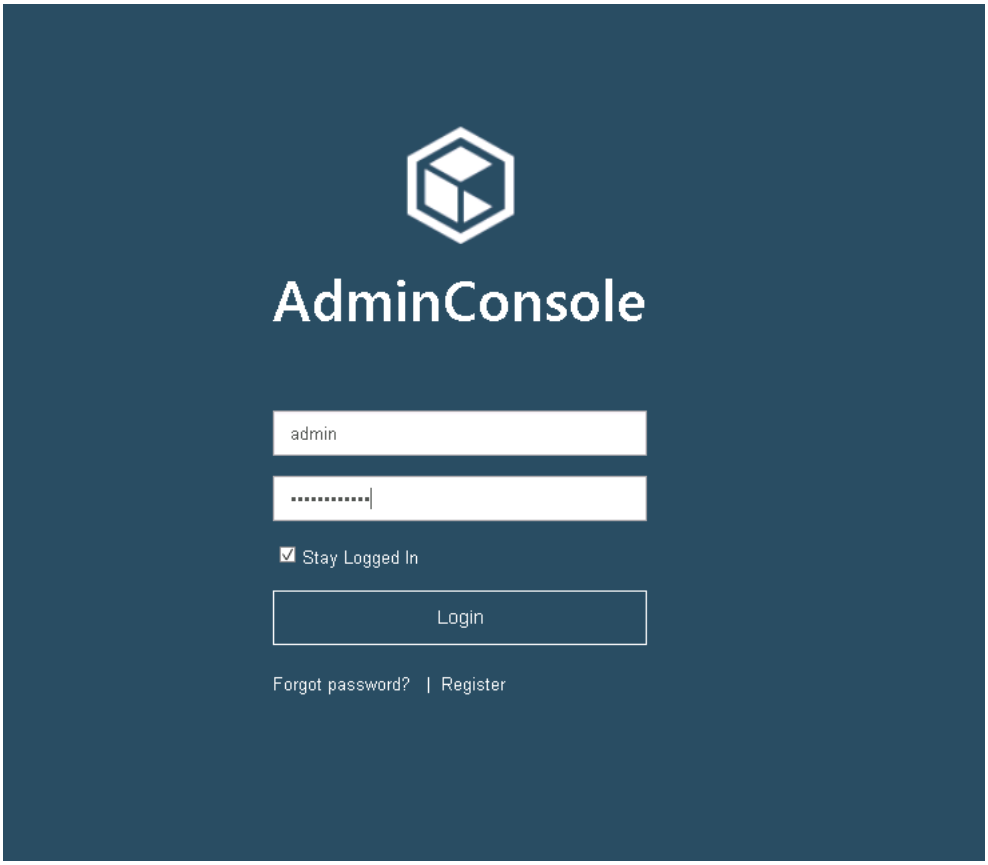
17. Repeat the process on the remaining two nodes.

18. For the storage pool network, the system will automatically add “sds” to the host name of each node. Enter the IP addresses for these host names in the /etc/hosts files on each node so the nodes can communicate properly.

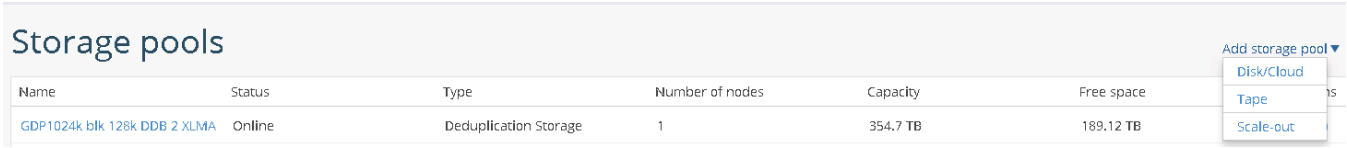
```
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
10.10.10.1  spc240m5node1sds    spc240m5node1sds.dmzlab.cisco.com
10.10.10.2  spc240m5node2sds    spc240m5node2sds.dmzlab.cisco.com
10.10.10.3  spc240m5node3sds    spc240m5node3sds.dmzlab.cisco.com
```

Configuring the storage pool from AdminConsole

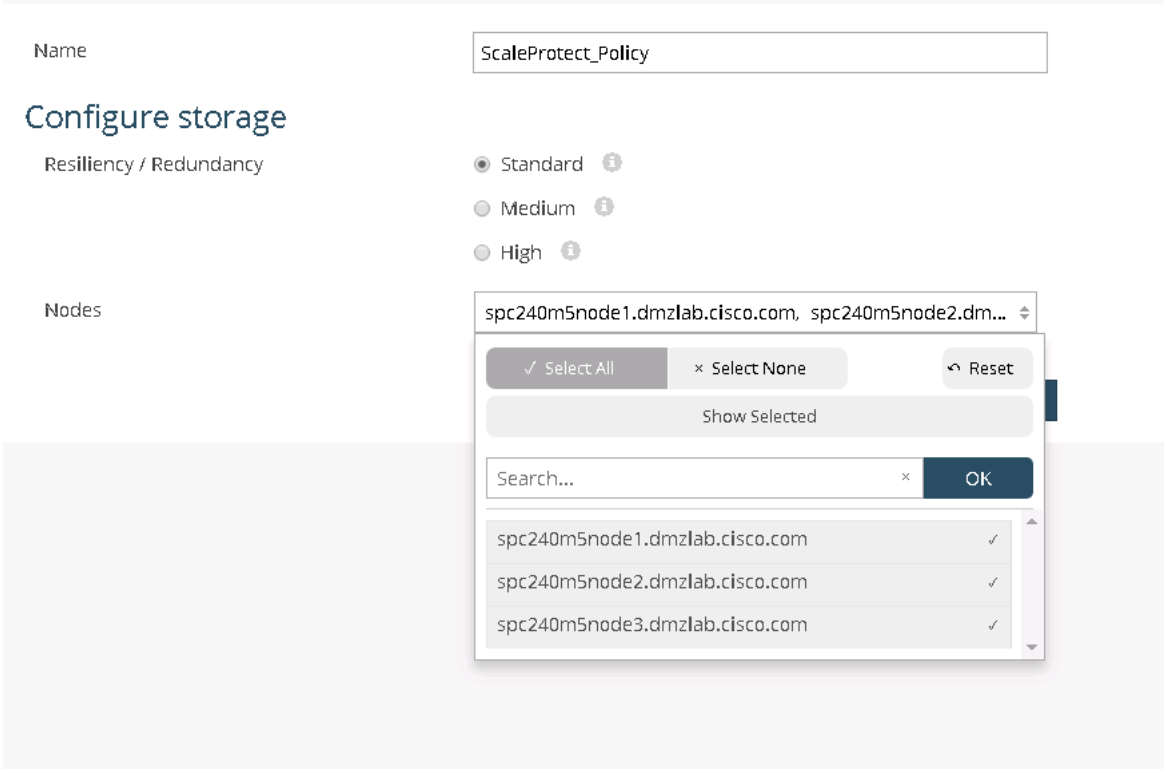
1. Log in to AdminConsole.



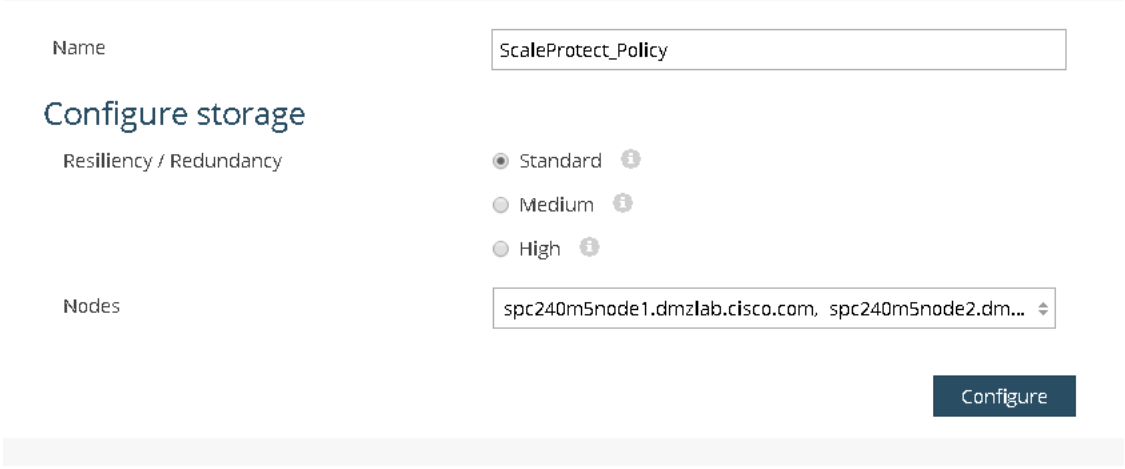
2. In the menu pane at the left, choose Storage and then “Storage pools.” Then click “Add storage pool” in the upper-right corner.



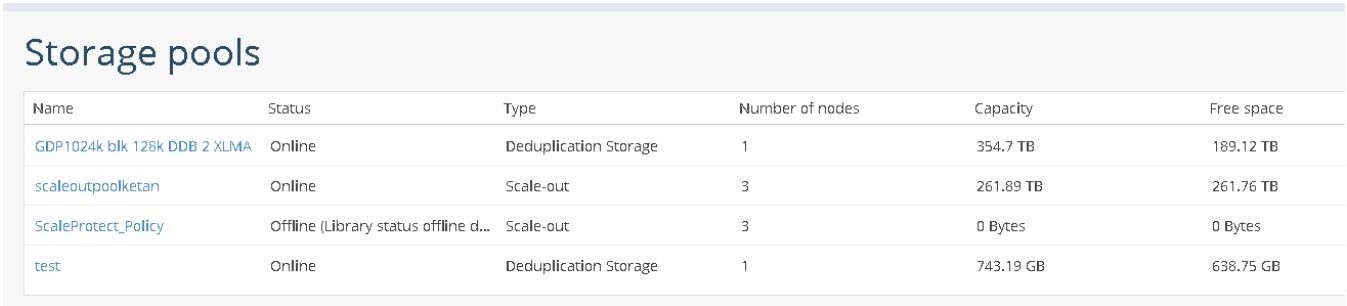
3. On the Create ScaleOut Storage Pool page, give the policy a name and select the Resiliency/Redundancy level (select Standard if you are installing only three nodes). Then select all the nodes and click OK.



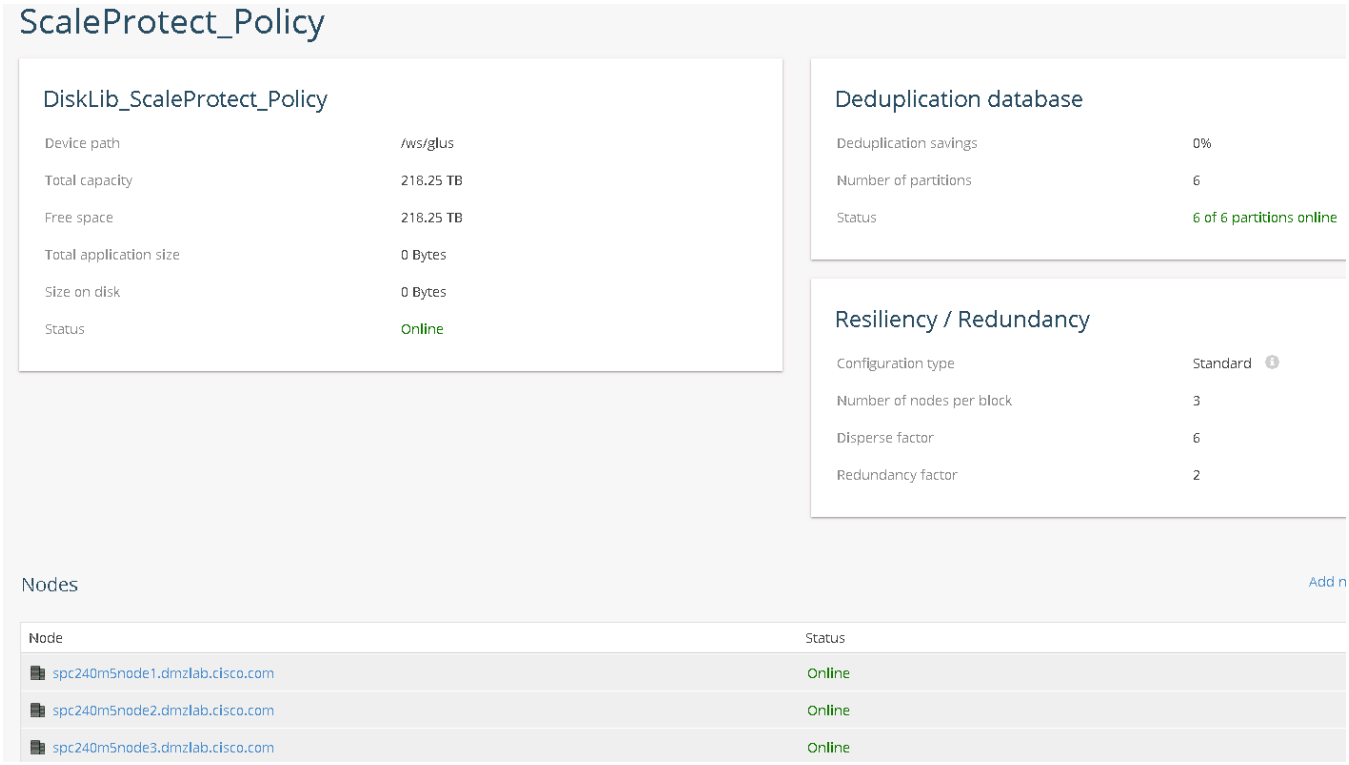
4. Click Configure.



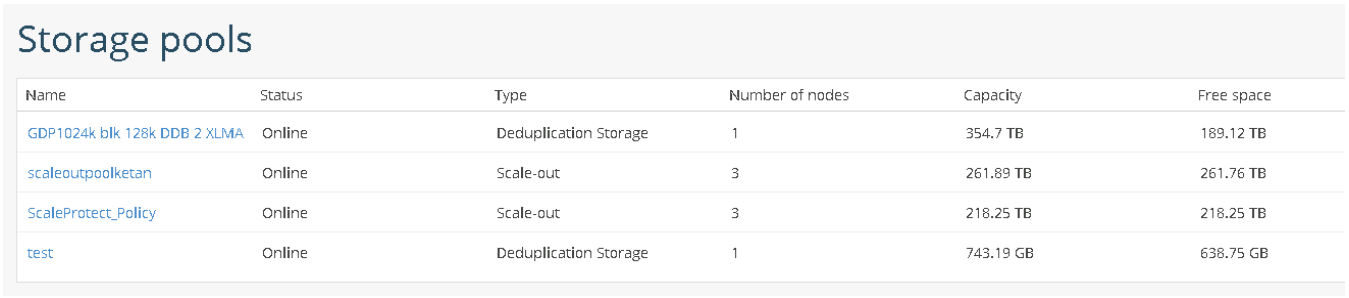
5. Immediately after the pool is created, it will be offline for a few minutes. Click the pool you just created.



The node status should be listed as Online and the screen should report “6 of 6 partitions online.”



The pool is now configured for use.



For more information

For additional information, see the following:

- Cisco UCS C240 rack server: https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c240-m5-rack-server/model.html
- Cisco UCS 6000 Series Fabric Interconnects: http://www.cisco.com/c/en/us/products/servers-unified-computing/fabric-interconnects.html
- Cisco UCS Manager: http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-manager/index.html
- Commvault: https://www.Commvault.com/solutions/by-function/data-protection-backup-and-recovery

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 C11-740797-00 06/18