



Cisco UCS S3260 Storage Servers with Cohesity SmartFiles

Deployment and Configuration Guide for Cohesity Helios Platform and Cohesity SmartFiles on Cisco S3260 M5 Storage Servers

Published: January 2022



In partnership with:

COHESITY

About the Cisco Validated Design Program

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

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

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

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

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unified Computing System (Cisco UCS), Cisco UCS B-Series Blade Servers, Cisco UCS C-Series Rack Servers, Cisco UCS S-Series Storage Servers, Cisco UCS Manager, Cisco UCS Management Software, Cisco Unified Fabric, Cisco Application Centric Infrastructure, Cisco Nexus 9000 Series, Cisco Nexus 7000 Series, Cisco Prime Data Center Network Manager, Cisco NX-OS Software, Cisco MDS Series, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. (LDW_P1)

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

© 2022 Cisco Systems, Inc. All rights reserved.

Contents

Executive Summary.....	5
Solution Overview	6
Technology Overview.....	9
Solution Design	21
Configuration and Installation.....	33
Cohesity SmartFiles	129
SmartFiles Use Cases and Validation.....	135
Bill of Materials	141
Cohesity Certified Cisco UCS Nodes.....	144
About the Authors	146
Feedback	147

Executive Summary

According to [Gartner](#), data will grow by 800% over the next five years, of which 80% will be unstructured in the form of file shares, backups, archives, logs, media files, dev/test and analytics. Traditional network attached storage (NAS) was designed over a decade ago for traditional use cases, and without serious architectural consideration for cloud and hybrid IT environments. The reality today is that there are multiple data silos resulting in mass data fragmentation across the data center and cloud. Challenges are not limited to the cost and management of multiple silos or delivering hybrid cloud seamlessly. Storage costs often destroy storage budgets. Addressing compliance, regulatory, and governance requirements adds to complexity and cost.

Cohesity SmartFiles is the industry's first software-defined, data-centric, multiprotocol file and object solution for the enterprise. SmartFiles is a discrete offering that is provided on top of the Cohesity Helios platform and goes beyond traditional scale-out NAS in terms of global data manageability, multicloud scale, storage efficiency, policy-based automation, integrated applications, AI-powered cybersecurity, and multi-tiered data management. Unlike traditional NAS, the Cohesity Helios data platform with SmartFiles is data-centric, not storage or infrastructure centric. This means there is no need to move data to apps because the apps and data are integrated in the same platform. This removes the complexity and cost of running disparate file ecosystem apps and associated infrastructure for file environments. Cohesity Marketplace apps and machine-learning assisted management provide intelligence and ease-of management that separates SmartFiles from traditional scale-out NAS appliances. It's smart and provides virtually effortless management, regardless of scale.

The Cisco UCS S3260 Storage Server is a modular storage server with dual M5 server nodes and is optimized for large datasets used in environments such as big data, cloud, object storage, video surveillance, and content delivery. The present deployment is optimized for best-in-class performance to capacity ratio, providing dual compute nodes and dense storage across a 4RU chassis. With UCS Management and stateless Service Profile capabilities, customers can easily expand to additional Cohesity nodes with minimal hardware and software configurations. Moreover, with UCS Managed S3260 storage chassis and Cohesity Helios platform, customers can achieve rolling upgrades of both software and hardware firmware with no cluster downtime.

This Cisco Validated Design and Deployment Guide provides prescriptive guidance for the design, setup, configuration, and ongoing use of the Cohesity Helios Platform with Cohesity SmartFiles, providing multi-protocol (NFS/CIFS/S3) file services and object storage capabilities on Cisco UCS S3260 dense storage server. This unique integrated solution is designed to solve siloed infrastructure, operational, and data management challenges faced by enterprises and service providers worldwide. The best-of-breed solution combines the web-scale simplicity and efficiency of Cohesity software with the power and flexibility of Cisco UCS servers. As a result, customers can more efficiently and effectively manage backup and unstructured data growth, acquire new insights, and reduce costs and complexity with a single, integrated solution. For more information on joint Cisco-Cohesity solutions, please see cohesity.com/cisco.

Solution Overview

Introduction

The Cisco UCS® S3260 Storage Server is a modular dual node x86 server designed for investment protection. Its architectural flexibility provides high performance or high capacity for your data intensive workloads. Combined with UCS Manager, customers users can easily deploy storage capacity from Terabytes to Petabytes within minutes.

The Cohesity Helios platform redefines data management with a web-scale solution that radically simplifies the way companies protect, control and extract value from their data. This software-defined platform spans across core, cloud, and edge, can be managed from a single GUI, and enables independent apps to run in the same environment. It is the only solution built on a hyperconverged, scale-out design that converges backup, files & objects, dev/test and analytics, and uniquely allows applications to run on the same platform to extract insights from data. Designed with Google-like principles, it delivers true global deduplication and impressive storage efficiency that spans edge to core to the public cloud.

Cohesity SmartFiles runs on top of the Helios platform. SmartFiles is an enterprise-class, software-defined, data-centric, multiprotocol file and object solution for the enterprise that transcends traditional offerings in terms of manageability, scale, security, efficiency, and multi-tiered data management. SmartFiles modernizes and simplifies data and application management by providing one platform for multiple workloads. It is a modern converged target for consolidating data silos and securely managing unstructured content and application data, including digital libraries, archives, rich media, video surveillance, big data, and backup data sets.

Cohesity SmartFiles on Cisco UCS S3260 storage server provides a dense storage, enterprise-class, software-defined, data-centric, multiprotocol file and object solution for the enterprise that go beyond the traditional offerings in terms of global manageability, multicloud scale, AI-powered security, efficiency, and multi-tiered data management. With Cohesity Helios management platform, customers can easily manage clusters deployed across data centers. The present architecture enables a high-density File Services solution providing modernized converged target for consolidating data silos and securely managing unstructured content and application data, including digital libraries, archives, rich media, video surveillance, big data, and backup data sets.

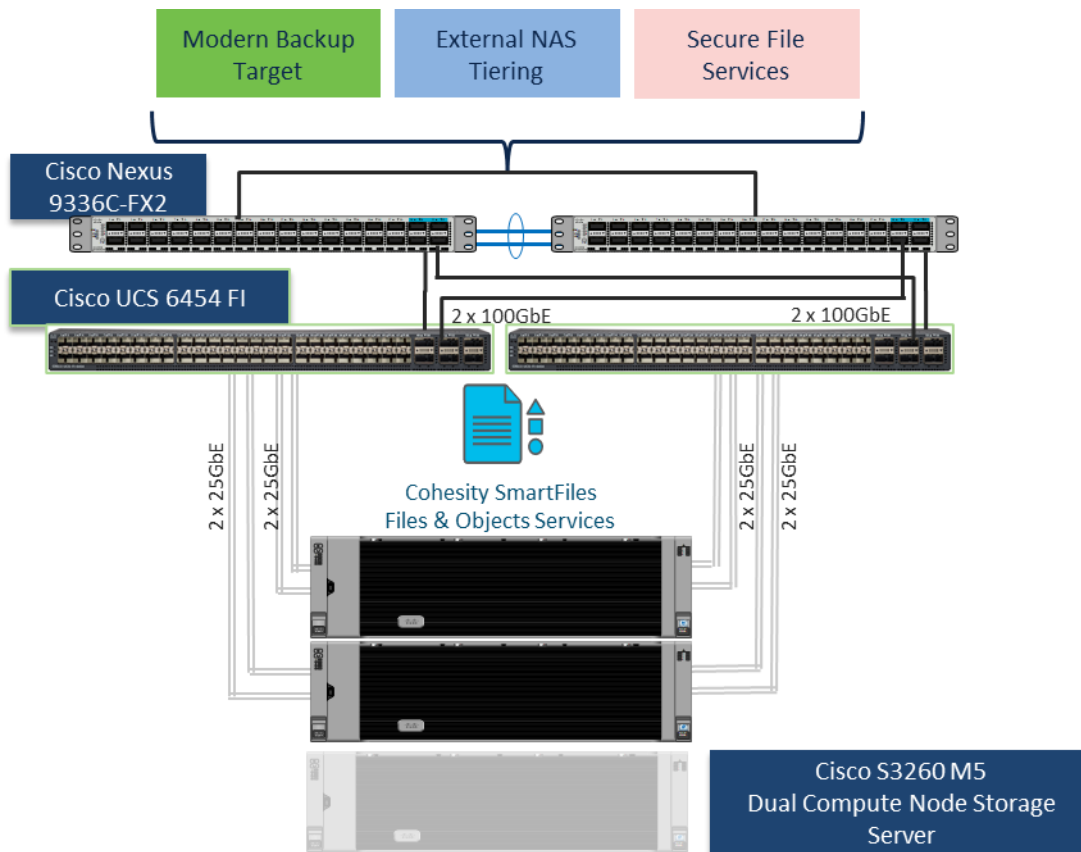
The 4RU Cisco UCS S3260 storage server is equipped with dual node compute server with each compute node managing 4 x 3.2 TB as the Flash Tier and 24 x 16 TB HDD for the capacity Tier. Cohesity SmartFiles on Cisco UCS solution - at minimum - is comprised of a four-node Cohesity Helios SmartFiles Cluster across two Cisco UCS S3260 storage chassis. With Cohesity web scale technology, the cluster can scale without limits, providing optimized efficiency and broad multiprotocol interoperability supporting NFS, SMB, S3, OpenStack Swift, and multiple leading public clouds. The solution ensures resiliency, consistency and linear performance and scale to seamlessly grow at your own pace by incrementally adding additional nodes, all while eliminating disruptive upgrades.

The solution extends across the following:

- Cohesity Helios Platform deployed as a four-node cluster across 2 x Cisco UCS S3260 Storage servers, each equipped with dual compute nodes, managed through a pair of Cisco Fabric Interconnect 6454.
- Cohesity SmartFiles cluster as a Backup target for external Backup software.
- Cohesity SmartFiles as a host for Secure File Services, thus eliminating inefficient and costly silos and allowing for provisioning of faster SSD storage or slower, less expensive HDD storage, depending on the use case.
- Cohesity SmartFiles for External NAS Tiering to allow tiering of unused or infrequently used data from NAS primary storage to the Cohesity cluster.

[Figure 1](#) provides a high-level view of various use cases configured and validated in this solution.

Figure 1. Cohesity SmartFiles on Cisco UCS S3260 Storage Server



Audience

The intended audience for this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, IT engineers, partners, and customers who are interested in learning about and deploying the Cohesity SmartFiles solution for non-latency-sensitive use cases,

such as target storage for backups, replication, archiving, file services with NFS, SMB/CIFS and S3 backed object storage.

Purpose of this document

This document describes the installation, configuration, and validated use cases for the Cohesity Helios Platform with Cohesity SmartFiles on dual node Cisco UCS S3260 Storage chassis. A reference architecture is provided to configure the Cohesity Helios Platform on Cisco UCS S-Series Storage servers. This document does not specifically explain the configuration of the Cohesity SmartFiles features; this is described here: [Cohesity SmartFiles](#)

Technology Overview

Cisco Unified Computing System

Cisco Unified Computing System (Cisco UCS) is a next-generation data center platform that integrates computing, networking, storage access, and virtualization resources into a cohesive system designed to reduce total cost of ownership and increase business agility. The system integrates a low-latency, lossless 10-100 Gigabit Ethernet unified network fabric with enterprise-class, x86-architecture servers. The system is an integrated, scalable, multi-chassis platform with a unified management domain for managing all resources.

Cisco Unified Computing System consists of the following subsystems:

Compute - The compute piece of the system incorporates servers based on the Second-Generation Intel® Xeon® Scalable processors. Servers are available in blade and rack form factor, managed by Cisco UCS Manager.

Network - The integrated network fabric in the system provides a low-latency, lossless, 10/25/40/100 Gbps Ethernet fabric. Networks for LAN, SAN and management access are consolidated within the fabric. The unified fabric uses the innovative Single Connect technology to lower costs by reducing the number of network adapters, switches, and cables. This in turn lowers the power and cooling needs of the system.

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 virtual environments to support evolving business needs.

Storage access - Cisco UCS system provides consolidated access to both SAN storage and Network Attached Storage over the unified fabric. This provides customers with storage choices and investment protection. Also, the server administrators can pre-assign storage-access policies to storage resources, for simplified storage connectivity and management leading to increased productivity.

Management: The system uniquely integrates compute, network, and storage access subsystems, enabling it to be managed as a single entity through Cisco UCS Manager software. Cisco UCS Manager increases IT staff productivity by enabling storage, network, and server administrators to collaborate on Service Profiles that define the desired physical configurations and infrastructure policies for applications. Service Profiles increase business agility by enabling IT to automate and provision resources in minutes instead of days.

Cisco UCS Differentiators

Cisco Unified Computing System is revolutionizing the way servers are managed in the datacenter. The following are the unique differentiators of Cisco Unified Computing System and Cisco UCS Manager:

Embedded Management – In Cisco UCS, the servers are managed by the embedded firmware in the Fabric Interconnects, eliminating the need for any external physical or virtual devices to manage the servers.

Unified Fabric – In Cisco UCS, from blade server chassis or rack servers to FI, there is a single Ethernet cable used for LAN, SAN, and management traffic. This converged I/O results in reduced cables, SFPs and adapters – reducing capital and operational expenses of the overall solution.

Auto Discovery – By simply inserting the blade server in the chassis or connecting the rack server to the fabric interconnect, discovery and inventory of compute resources occurs automatically without any management intervention. The combination of unified fabric and auto-discovery enables the wire-once architecture of Cisco UCS, where compute capability of Cisco UCS can be extended easily while keeping the existing external connectivity to LAN, SAN, and management networks.

Policy Based Resource Classification – Once a compute resource is discovered by Cisco UCS Manager, it can be automatically classified to a given resource pool based on policies defined. This capability is useful in multi-tenant cloud computing. This CVD showcases the policy-based resource classification of Cisco UCS Manager.

Combined Rack and Blade Server Management – Cisco UCS Manager can manage Cisco UCS B-series blade servers and Cisco UCS C-series rack servers under the same Cisco UCS domain. This feature, along with stateless computing makes compute resources truly hardware form factor agnostic.

Model based Management Architecture – The Cisco UCS Manager architecture and management database is model based, and data driven. An open XML API is provided to operate on the management model. This enables easy and scalable integration of Cisco UCS Manager with other management systems.

Policies, Pools, Templates – The management approach in Cisco UCS Manager is based on defining policies, pools, and templates, instead of cluttered configuration, which enables a simple, loosely coupled, data driven approach in managing compute, network, and storage resources.

Loose Referential Integrity – In Cisco UCS Manager, a service profile, port profile or policies can refer to other policies or logical resources with loose referential integrity. A referred policy cannot exist at the time of authoring the referring policy or a referred policy can be deleted even though other policies are referring to it. This provides different subject matter experts to work independently from each other. This provides great flexibility where different experts from different domains, such as network, storage, security, server, and virtualization work together to accomplish a complex task.

Policy Resolution – In Cisco UCS Manager, a tree structure of organizational unit hierarchy can be created that mimics the real-life tenants and/or organization relationships. Various policies, pools and templates can be defined at different levels of organization hierarchy. A policy referring to another policy by name is resolved in the organizational hierarchy with closest policy match. If no policy with specific name is found in the hierarchy of the root organization, then the special policy named “de-

fault” is searched. This policy resolution practice enables automation friendly management APIs and provides great flexibility to owners of different organizations.

Service Profiles and Stateless Computing – A service profile is a logical representation of a server, carrying its various identities and policies. This logical server can be assigned to any physical compute resource as far as it meets the resource requirements. Stateless computing enables procurement of a server within minutes, which used to take days in legacy server management systems.

Built-in Multi-Tenancy Support – The combination of policies, pools and templates, loose referential integrity, policy resolution in the organizational hierarchy and a service profiles-based approach to compute resources makes Cisco UCS Manager inherently friendly to multi-tenant environments typically observed in private and public clouds.

Extended Memory – The enterprise-class Cisco UCS Blade server extends the capabilities of the Cisco Unified Computing System portfolio in a half-width blade form factor. It harnesses the power of the latest Intel® Xeon® Scalable Series processor family CPUs and Intel® Optane DC Persistent Memory (DCPMM) with up to 18TB of RAM (using 256GB DDR4 DIMMs and 512GB DCPMM).

Simplified QoS – Even though Fibre Channel and Ethernet are converged in the Cisco UCS fabric, built-in support for QoS and lossless Ethernet makes it seamless. Network Quality of Service (QoS) is simplified in Cisco UCS Manager by representing all system classes in one GUI panel.

Cisco UCS Manager

Cisco UCS Manager (UCSM) provides unified, integrated management for all software and hardware components in Cisco UCS. Using [Cisco Single Connect](#) technology, it manages, controls, and administers multiple chassis for thousands of virtual machines. Administrators use the software to manage the entire Cisco Unified Computing System as a single logical entity through an intuitive graphical user interface (GUI), a command-line interface (CLI), or a through a robust application programming interface (API).

Cisco UCS Manager is embedded into the Cisco UCS Fabric Interconnect and provides a unified management interface that integrates server, network, and storage. Cisco UCS Manager performs auto-discovery to detect inventory, manage, and provision system components that are added or changed. It offers a comprehensive set of XML API for third party integration, exposes thousands of integration points, and facilitates custom development for automation, orchestration, and to achieve new levels of system visibility and control.

Cisco UCS™ Manager 4.0 provides unified, embedded management of all software and hardware components of the Cisco Unified Computing System™ (Cisco UCS) across multiple chassis and Cisco UCS servers. Cisco UCS Manager 4.0 is a unified software release for all supported Cisco UCS hardware platforms. Release 4.0 enables support for UCS 6454 Fabric Interconnects, VIC 1400 series adapter cards on Cisco UCS M5 servers and Second-Generation Intel® Xeon® Scalable processor refresh and Intel® Optane™ Data Center persistent memory modules on UCS Intel-based M5 servers.

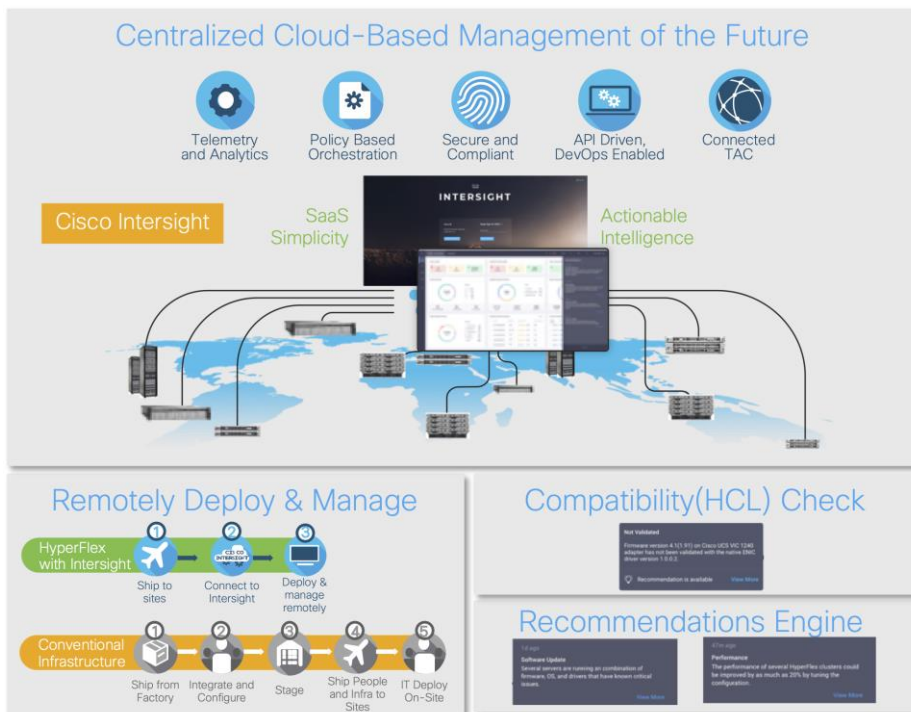
For more information on Cisco UCS Manager Release 4.0 refer to the [Release Notes page](#).

Cisco Intersight

Cisco Intersight™ is a lifecycle management platform for your infrastructure, regardless of where it resides. In your enterprise data center, at the edge, in remote and branch offices, at retail and industrial sites—all these locations present unique management challenges and have typically required separate tools. Cisco Intersight Software as a Service (SaaS) unifies and simplifies your experience of the Cisco Unified Computing System™ (Cisco UCS®) and Cisco HyperFlex™ systems.

Intersight software delivers a new level of cloud-powered intelligence that supports lifecycle management with continuous improvement. It is tightly integrated with the Cisco® Technical Assistance Center (TAC). Expertise and information flow seamlessly between Cisco Intersight and IT teams, providing global management of Cisco infrastructure, anywhere. Remediation and problem resolution are supported with automated upload of error logs for rapid root-cause analysis.

Figure 2. Cisco Intersight



Automate your infrastructure

Cisco has a strong track record for management solutions that deliver policy-based automation to daily operations. Intersight SaaS is a natural evolution of our strategies. Cisco designed Cisco UCS and HyperFlex to be 100 percent programmable. Cisco Intersight simply moves the control plane from the network into the cloud. Now you can manage your Cisco UCS and HyperFlex infrastructure wherever it resides through a single interface.

Deploy your way

If you need to control how your management data is handled, comply with data locality regulations, or consolidate the number of outbound connections from servers, you can use the Cisco Intersight Virtual Appliance for an on-premises experience. Cisco Intersight Virtual Appliance is continuously updated just like the SaaS version, so regardless of which approach you implement, you never have to worry about whether your management software is up to date.

DevOps ready

If you are implementing DevOps practices, you can use the Cisco Intersight API with either the cloud-based or virtual appliance offering. Through the API you can configure and manage infrastructure as code—you are not merely configuring an abstraction layer; you are managing the real thing. Through the API and support of cloud-based RESTful API, Terraform providers, Microsoft PowerShell scripts, or Python software, you can automate the deployment of settings and software for both physical and virtual layers. Using the API, you can simplify infrastructure lifecycle operations and increase the speed of continuous application delivery.

Pervasive simplicity

Simplify the user experience by managing your infrastructure regardless of where it is installed.

Automate updates to Cisco HyperFlex™ Data Platform software, reducing complexity and manual efforts.

Actionable intelligence

Use best practices to enable faster, proactive IT operations.

Gain actionable insight for ongoing improvement and problem avoidance.

Manage anywhere

Deploy in the data center and at the edge with massive scale.

Get visibility into the health and inventory detail for your Intersight Managed environment on-the-go with the Cisco Intersight Mobile App.

For more information about Cisco Intersight and the different deployment options, go to: [Cisco Intersight - Manage your systems anywhere.](#)

Cisco UCS Fabric Interconnect

The Cisco UCS Fabric Interconnect (FI) is a core part of the Cisco Unified Computing System, providing both network connectivity and management capabilities for the system. Depending on the model chosen, the Cisco UCS Fabric Interconnect offers line-rate, low-latency, lossless 10 Gigabit, 25 Gigabit, 40 Gigabit, or 100 Gigabit Ethernet, Fibre Channel over Ethernet (FCoE) and Fibre Channel connectivity. Cisco UCS Fabric Interconnects provide the management and communication backbone for the Cisco UCS C-Series, S-Series and HX-Series Rack-Mount Servers, Cisco UCS B-Series Blade

Servers, and Cisco UCS 5100 Series Blade Server Chassis. All servers and chassis, and therefore all blades, attached to the Cisco UCS Fabric Interconnects become part of a single, highly available management domain. In addition, by supporting unified fabrics, the Cisco UCS Fabric Interconnects provide both the LAN and SAN connectivity for all servers within its domain.

For networking performance, the Cisco UCS 6454 Series uses a cut-through architecture, supporting deterministic, low latency, line rate 10/25/40/100 Gigabit Ethernet ports, 3.82 Tbps of switching capacity, and 320 Gbps bandwidth per Cisco 5108 blade chassis when connected through the IOM 2208 model. The product family supports Cisco low-latency, lossless 10/25/40/100 Gigabit Ethernet unified network fabric capabilities, which increase the reliability, efficiency, and scalability of Ethernet networks. The Fabric Interconnect supports multiple traffic classes over the Ethernet fabric from the servers to the uplinks. Significant TCO savings come from an FCoE-optimized server design in which network interface cards (NICs), host bus adapters (HBAs), cables, and switches can be consolidated.

Cisco UCS 6454 Fabric Interconnect

The Cisco UCS 6454 Fabric Interconnect is a one-rack-unit (1RU) 10/25/40/100 Gigabit Ethernet, FCoE and Fiber Channel switch offering up to 3.82 Tbps throughput and up to 54 ports. The switch has eight (8) 10/25-Gbps fixed Ethernet ports, which can optionally be configured as 8/16/32-Gbps FC ports (ports 1 to 8), thirty-six (36) 10/25-Gbps fixed Ethernet ports (ports 9 to 44), four (4) 1/10/25-Gbps Ethernet ports (ports 45 to 48), and finally six (6) 40/100-Gbps Ethernet uplink ports (ports 49 to 54). For more information, refer to the Cisco UCS 6454 Fabric Interconnect spec sheet: (<https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/6400-specsheet.pdf>)

Figure 3. Cisco UCS 6454 Fabric Interconnect



Cisco UCS S-Series Cohesity-Certified Nodes

The Cisco UCS S3260 Storage Server is a modular, high-density, high-availability dual-node rack server well suited for service providers, enterprises, and industry-specific environments. It addresses the need for dense, cost-effective storage for the ever-growing amounts of data. Designed for a new class of cloud-scale applications and data-intensive workloads, it is simple to deploy and excellent for big data, software-defined storage, and data-protection environments.

Figure 4. Cisco UCS S3260 Storage Server



Cisco UCS S3260 is a four-rack-unit (4RU) Storage Server, providing a dense storage platform for Cohesity clusters. Each node in the S3260 chassis can be configured with a PCIe-based system I/O controller for Quad Port 10/25G Cisco VIC 1455 or Dual Port 100G Cisco VIC 1495. The Cisco S3260 storage server for Cohesity SmartFiles is a dual compute nodes system equipped with eight 3.2 TB high-performance SSD drives for data caching and 48 NL-SAS drives, each with 16 TB capacity. For more information, please refer to the [Cisco S3260 storage server spec sheet](#).

Cisco UCS C-Series Cohesity-Certified Nodes

A Cohesity cluster requires a minimum of three Cisco UCS C-Series nodes (with disk storage). Data is replicated across at least two of these nodes, and a third node is required for continuous operation in the event of a single-node failure. Each node is equipped with two high-performance SSD drives for data caching and rapid acknowledgment of write requests. Each node also is equipped with additional hard disks for long term storage and overall capacity.

Cisco UCS C240 M5 LFF Server

This two-rack-unit (2RU) Cisco C240 M5 Large Form Factor (LFF) model server contains a pair of 240 GB M.2 form factor solid-state disk (SSD) that acts as the boot drives, a pair of 1.6 TB or 3.2 TB NVMe SSD drives installed in the rear drive slots, and twelve 4 TB or 10 TB SATA HDD drives for storage capacity.

Figure 5. Cisco C240 M5 LFF Server



Cisco UCS VIC 1457 MLOM Interface Card

The Cisco UCS VIC 1457 Card is a quad-port Enhanced Small Form-Factor Pluggable (SFP+) 10/25-Gbps Ethernet, and Fibre Channel over Ethernet (FCoE)-capable PCI Express (PCIe) modular LAN-on-motherboard (mLOM) adapter installed in the Cisco UCS C-Series Rack Servers. The VIC 1457 is used in conjunction with the Cisco UCS 6454 model Fabric Interconnects. The mLOM slot can be used to install a Cisco VIC without consuming a PCIe slot, which provides greater I/O expandability. It incorporates next-generation converged network adapter (CNA) technology from Cisco, providing investment protection for future feature releases. The card enables a policy-based, stateless, agile server infrastructure that can present up to 256 PCIe standards-compliant interfaces to the host, each dynamically configured as either a network interface card (NICs) or host bus adapter (HBA). The personality of the interfaces is set programmatically using the service profile associated with the server. The number, type (NIC or HBA), identity (MAC address and Worldwide Name [WWN]), failover policy, adapter settings, bandwidth, and quality-of-service (QoS) policies of the PCIe interfaces are all specified using the service profile.

Figure 6. Cisco UCS VIC 1457 mLOM Card



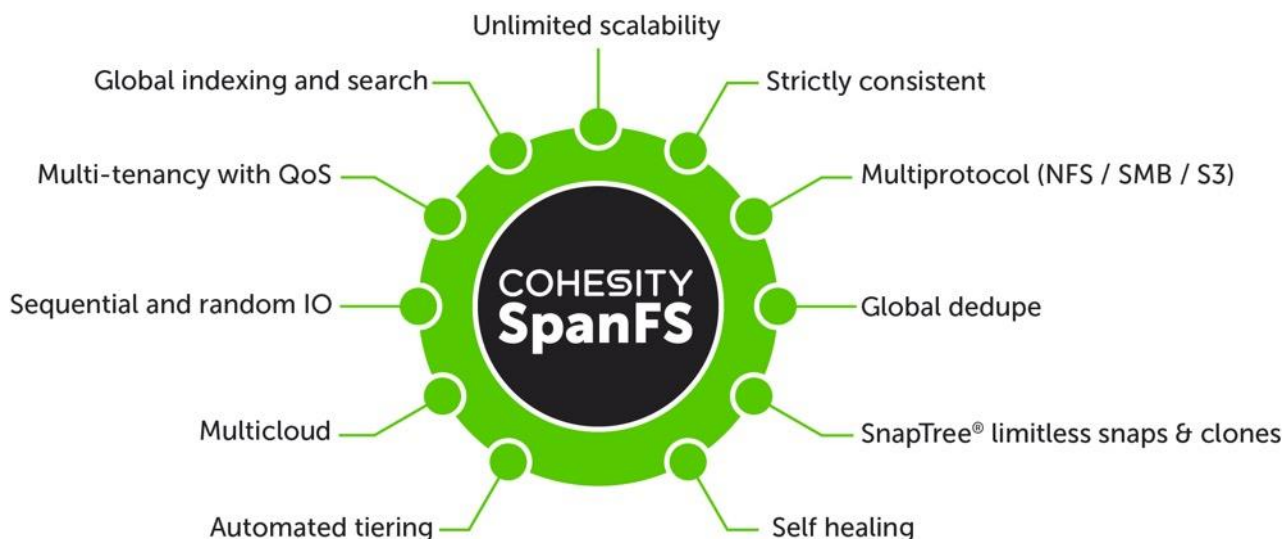
Cohesity Helios

Cohesity has built a unique solution based on the same architectural principles employed by cloud hyperscalers managing consumer data but optimized for the enterprise world. The secret to the hyperscalers' success lies in their architectural approach, which has three major components: a distributed file system—a single platform—to store data across locations, a single logical control plane through which to manage it, and the ability to run and expose services atop this platform to provide new functionality through a collection of applications. The Cohesity platform takes this same three-tier hyperscaler architectural approach and adapts it to the specific needs of enterprise data management.

SpanFS: A Unique File System that Powers the Cohesity Helios Platform

The foundation of the Cohesity Helios Platform is Cohesity SpanFS®, a 3rd generation web-scale distributed file system. SpanFS enables the consolidation of all data management services, data, and apps onto a single software-defined platform, eliminating the need for the complex jumble of siloed infrastructure required by the traditional approach.

Predicated on SpanFS, Cohesity Helios Platform's patented design allows all data management infrastructure functions— including backup and recovery, disaster recovery, long-term archival, file services and object storage, test data management, and analytics—to be run and managed in the same software environment at scale, whether in the public cloud, on-premises, or at the edge. Data is shared rather than siloed, stored efficiently rather than wastefully, and visible rather than kept in the dark— simultaneously addressing the problem of mass data fragmentation while allowing both IT and business teams to holistically leverage its value for the first time. In order to meet modern data management requirements, Cohesity SpanFS provides the following:



Key SpanFS attributes and implications include the following:

Unlimited Scalability: Start with as little as three nodes and grow limitlessly on-premises or in the cloud with a pay-as-you-grow model.

Strictly Consistent: Ensure data resiliency with strict consistency across nodes within a cluster.

Multi-Protocol: Support traditional NFS and SMB based applications as well as modern S3-based applications. Read and write to the same data volume with simultaneous multiprotocol access.

Global Dedupe: Significantly reduce data footprint by deduplicating across data sources and workloads with global variable-length deduplication.

Unlimited Snapshots and Clones: Create and store an unlimited number of snapshots and clones with significant space savings and no performance impact.

Self-Healing: Auto-balance and auto-distribute workloads across a distributed architecture.

Automated Tiering: Automatic data tiering across SSD, HDD, and cloud storage for achieving the right balance between cost optimization and performance.

Multi Cloud: Native integrations with leading public cloud providers for archival, tiering, replication, and protect cloud-native applications.

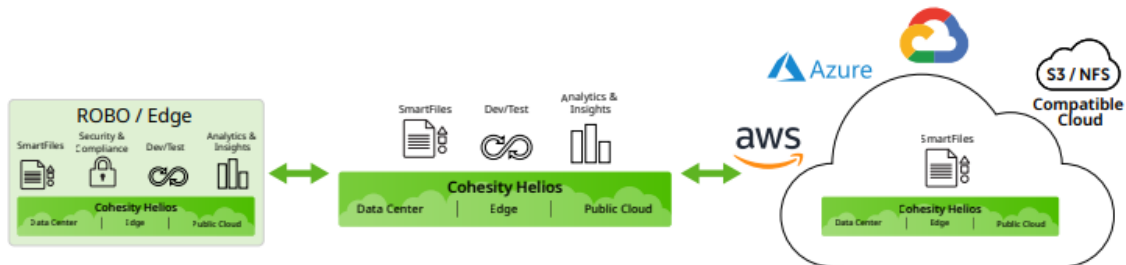
Sequential and Random IO: High I/O performance by auto-detecting the IO profile and placing data on the most appropriate media Multitenancy with QoS Native ability to support multiple tenants with QoS support, data isolation, separate encryption keys, and role-based access control.

Global Indexing and Search: Rapid global search due to indexing of file and object metadata.

Cohesity SmartFiles

Cohesity SmartFiles is an enterprise-class, software-defined, datacentric, multiprotocol file and object solution for the enterprise that transcends traditional offerings in terms of manageability, scale, security, efficiency and multi-tiered data management. It is based on the Cohesity Helios multicloud data platform, which delivers a patented distributed architecture for scale-out storage in a pay-as-you-grow model that never requires disruptive upgrades.

SmartFiles modernizes and simplifies data and application management by providing one platform for multiple workloads. It is a modern converged target for consolidating data silos and securely managing unstructured content and application data, including digital libraries, archives, rich media, video surveillance, big data and backup data sets.



Simplified Multicloud Data Management

SmartFiles software works efficiently on-premises as well as in the public cloud to make data visible and manageable. Its multicloud capabilities ensure seamless and rapid data mobility and application portability. Wherever data resides, it is always protected and preserved with integrated layers of security features and file integrity functions. Intelligent policy-based management and automation affirm efficient placement, governance and protection of volumes of data.

Do More With Data

SmartFiles enables you to extract value from data through an integrated Cohesity and third-party application ecosystem that runs directly on data in-place to mitigate risk from cyber threats and ransomware, accelerate content and metadata search, streamline compliance and eDiscovery, and detect anomalies and develop actionable insights with powerful analytics. SmartFiles also increases operational efficiency with multiple protocols, including native S3 compatibility, to integrate with leading business applications and clouds.

Flexible, Efficient And Cost Optimized

Available as a software defined solution, SmartFiles delivers drastically lower cost of ownership by providing the flexibility to match workload, capacity and cost requirements with a range of hardware choices, including flash-optimized options. Innovative data deduplication, compression and small file optimization extend storage capacity and enhance performance. Simplified tiering of cold content off valuable Tier 1 storage also assures investment protection while reducing the frequency of capacity upgrades on existing 3rd-party systems.

SmartFiles key capabilities include:

Multicloud Simplicity

- **Enterprise Class:** Designed to radically simplify enterprise data management and unlock unlimited value from enterprise data.
- **Deploy Anywhere:** As a software defined SmartFiles offers broad flexibility. Deploy on your choice of hardware, on virtual machines, or in one or more public clouds. It's easy to migrate workloads across these deployments to optimize capacity, performance and costs.
- **Unlimited Scale:** Grow compute and storage independently. Support for heterogeneous disk and all-flash platforms allow for seamless deployment of new platforms with older platforms. You can also retire end-of-life platforms without expensive data migrations or forklift upgrades.
- **Global Space Efficiency:** SmartFiles is highly efficient and can deliver as much as 2x or 3x capacity savings compared to traditional alternatives. This translates to less physical storage costs, a smaller footprint, lower energy consumption and easier management.
- **Multiprotocol Flexibility:** An API-first design for maximum flexibility and ease of automation. SmartFiles provides native multiprotocol file and object services with unified permissions via NFS, SMB, S3 and OpenStack Swift.

Global Data Management

- **One Global Control Plane:** The singular Helios UI allows data management functions—including backup and recovery, disaster recovery, long-term archival, file and object services, test data management, security and compliance, and analytics – to be run and managed at scale, whether in the public cloud, on-premises, or at the edge. It offers real-time multi-cluster monitoring, pre-built and custom global reporting, global policy configuration and management, orchestrated multi-cluster upgrades, and global search.
- **Automated Data Movement:** Scale anywhere - on-premises or in the cloud - wherever it makes the most sense for your business. Policy-based automated tiering, archiving and replication to the cloud are also all supported.
- **Burst for Compute:** Replicate and instantly access data for processing in the cloud(s).

-
- **Data Lifecycle Management:** SmartFiles provides the ability to simply, reliably and cost effectively administer data creation, utilization, sharing, storage, and deletion.
 - **Deep Data Insights:** Cohesity Helios leverages machine-learning-based algorithms to provide data driven insights to proactively assess your environment and automate infrastructure resources across multiple locations. From the Cohesity App Marketplace, Cohesity-developed apps and third-party apps are also available that can run directly on the platform and operate on data in-place for search, audit, antivirus.
 - **Simple Data Migration:** Use built-in external NAS tiering capability to transparently move cold data off of your NAS device to SmartFiles.

AI-Powered Cyber Security

- **Anti-Ransomware:** Helios looks at a large cross-section an organization's data footprint to enable accurate and proactive actions. Anti-ransomware alerts can scan backups across the footprint to detect encryption-based ransomware attacks.
- **WORM/Legal Hold:** SmartFiles prevents data tampering and helps meet compliance requirements with an immutable file system, software encryption, over the wire encryption, multi-factor authentication, DataLock (WORM), legal hold settings, and adherence to FIPS 140-1 and 140-2 standards.
- **Classification:** Define classification policies and make discovering data across multiple clusters and data sources simple and automatic. SmartFiles incorporates the ability to choose a pre-built compliance template or search and define custom classification policies directly from the user interface.
- **User Behavior:** Avoid paying for expensive third-party tools to help answer questions about who moved data, who deleted data and what happened to the data. We've built those capabilities directly into the free Spotlight app on the Marketplace.
- **Risk Exposure:** SmartFiles includes a number of features for preventing unwanted data exposure, including secure views, in-flight and at-rest encryption, role-based access control and support for secure SSH.

Solution Design

Requirements

The following sections detail the physical hardware, software revisions, and firmware versions required to install Cohesity SmartFiles Clusters running on Unified Computing System. A Cohesity SmartFiles cluster requires a minimum of two Cisco UCS S3260 Storage chassis, with each chassis equipped with dual UCS-S3260 M5 server nodes.

Physical components

Table 1. Cohesity Helios System Components

Component	Hardware Required
Fabric Interconnects	Two (2) Cisco UCS 6454 Fabric Interconnects
Servers	Minimum of (2) two Cisco UCS S3260 storage server chassis each with dual server node

[Table 2](#) lists the required hardware components and disk options for the Cisco UCS S3260 Storage Server Base Chassis, which are required for installing Cohesity SmartFiles.

Table 2. Cisco UCS S3260 M5 Chassis Options

Cisco UCS S3260 M5 options	Hardware Required	
Chassis	Cisco UCS S3260 Storage Server Base Chassis	
Server Node	2x Cisco UCS S3260 M5 Server Node for Intel Scalable CPUs	
Processors	Each server node equipped with two Intel 4214R 2.4GHz/100W 12C/16.50MB CPUs	
Memory	Each server node equipped with 256 GB of total memory using eight (8) RDIMM/2Rx4 (8Gb) 1.2v modules	
Disk Controller	Cisco UCS S3260 Dual Pass Through based on Broadcom IT Firmware	
System I/O Controller (SIOC)	PCIe slot based with Cisco UCS VIC 1455 Quad Port 10/25G adapter	
Storage	SSDs	8 x Cisco UCS C3000 Top Load 3X 3.2TB SSD
	HDDs	48 x 16TB 4Kn NL-SAS 7200 RPM 12Gb HDD

Cisco UCS S3260 M5 options	Hardware Required
Network	Cisco UCS VIC 1455 Quad Port 10/25G SFP28 CNA PCIE
Rear Drive / Boot Device	4 x UCS S3260 240G Boot SSD

Software components

[Table 3](#) lists the software components and the versions required for a single cluster of the Cohesity Helios Platform running in Cisco UCS, as tested, and validated in this document.

Table 3. Software Components

Component	Software Required
Cohesity Helios, Cohesity SmartFiles	6.6.0d_release-20211028_8aa8fd67 or later
Cisco UCS Firmware	Cisco UCS Infrastructure software, B-Series and C-Series bundles, revision 4.1(3b) or later

Licensing

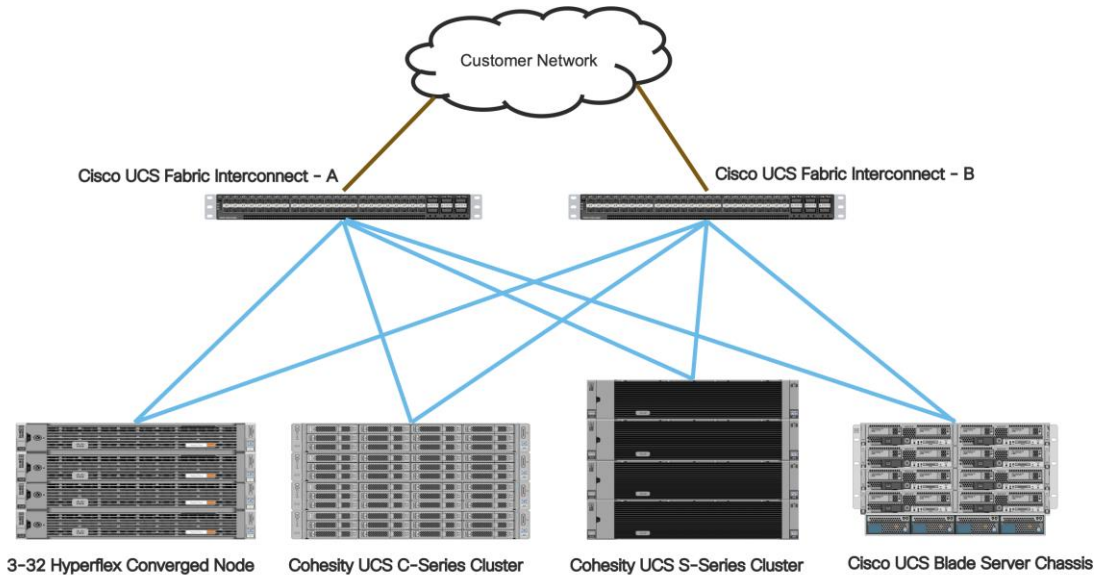
Cisco UCS systems and the Cohesity software must be properly licensed for all software features in use, and for all ports in use on the Cisco UCS Fabric Interconnects. Please contact your sales partner or your direct Cisco and Cohesity sales teams to ensure you order all the necessary and appropriate licenses for your solution.

Physical topology

Topology overview

Cisco Unified Computing System is composed of a pair of Cisco UCS Fabric Interconnects along with up to 160 Cisco UCS B-Series blade servers, Cisco UCS C-Series rack-mount servers, HX-Series hyper-converged servers, or S-Series storage servers per UCS domain. Inside of a Cisco UCS domain, multiple environments can be deployed for differing workloads. For example, a Cisco HyperFlex cluster can be built using Cisco HX-Series rack-mount servers, a Cohesity cluster can be built using high density Cisco S-Series Storage server chassis or Cisco UCS C-Series Rack-mount servers and Cisco UCS B-Series blade servers inside of Cisco 5108 blade chassis can be deployed for various bare-metal or virtualized environments. The two Fabric Interconnects both connect to every Cisco UCS C-Series, HX-Series, or Cisco UCS S-Series storage server, and also connect to every Cisco UCS 5108 blade chassis. Upstream network connections, also referred to as “northbound” network connections are made from the Fabric Interconnects to the customer datacenter network at the time of installation.

Figure 7. Cisco UCS Example Physical Topology



Cisco UCS Fabric Interconnects

Cisco UCS Fabric Interconnects (FI) are deployed in pairs, wherein the two units operate as a management cluster, while forming two separate network fabrics, referred to as the A side and B side fabrics. Therefore, many design elements will refer to FI A or FI B, alternatively called fabric A or fabric B. Both Fabric Interconnects are active at all times, passing data on both network fabrics for a redundant and highly available configuration. Management services, including Cisco UCS Manager, are also provided by the two FIs but in a clustered manner, where one FI is the primary, and one is secondary, with a roaming clustered IP address. This primary/secondary relationship is only for the management cluster and has no effect on data transmission.

Fabric Interconnects have the following ports, which must be connected for proper management of the Cisco UCS domain:

- **Mgmt:** A 10/100/1000 Mbps port for managing the Fabric Interconnect and the Cisco UCS domain through GUI and CLI tools. This port is also used by remote KVM, IPMI and SoL sessions to the managed servers within the domain. This is typically connected to the customer management network.
- **L1:** A cross connect port for forming the Cisco UCS management cluster. This port is connected directly to the L1 port of the paired Fabric Interconnect using a standard CAT5 or CAT6 Ethernet cable with RJ45 plugs. It is not necessary to connect this to a switch or hub.
- **L2:** A cross connect port for forming the Cisco UCS management cluster. This port is connected directly to the L2 port of the paired Fabric Interconnect using a standard CAT5 or CAT6 Ethernet cable with RJ45 plugs. It is not necessary to connect this to a switch or hub.

- Console: An RJ45 serial port for direct console access to the Fabric Interconnect. This port is typically used during the initial FI setup process with the included serial to RJ45 adapter cable. This can also be plugged into a terminal aggregator or remote console server device.

Cisco UCS S-Series Storage Server Chassis

Cohesity UCS clusters for SmartFiles require a minimum of three (3) compute nodes. Each Cisco UCS S Series Storage Server for Cohesity SmartFiles, is equipped with a dual Server node. The Cisco UCS S-Series Storage Servers are connected directly to the Cisco UCS Fabric Interconnects in Direct Connect mode. Internally the Cisco UCS S-Series servers are configured with the PCIe-based system I/O controller for Quad Port 10/25G Cisco VIC 1455. The standard and redundant connection practice is to connect port 1 and port 2 of each server's VIC card to a numbered port on FI A, and port 3 and port 4 of each server's VIC card to the same numbered port on FI B. The design also supports connecting just port 1 to FI A and port 3 to FI B. The use of ports 1 and 3 are because ports 1 and 2 form an internal port-channel, as does ports 3 and 4. *This allows an optional 2 cable connection method, which is not used in this design.*

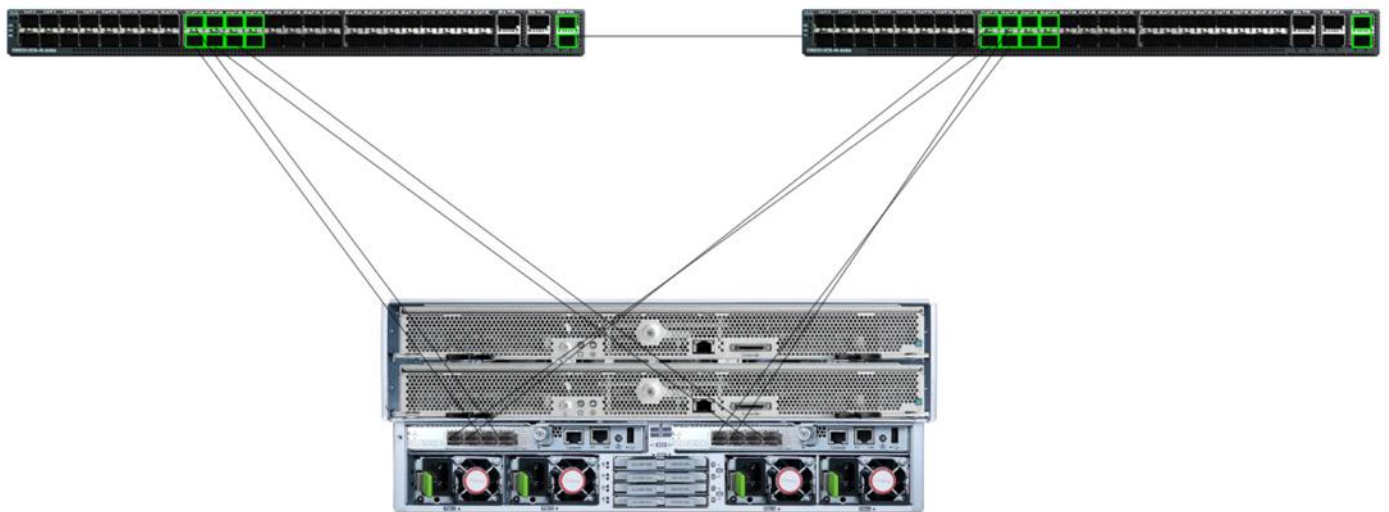
WARNING!

Failure to follow this cabling practice can lead to errors, discovery failures, and loss of redundant connectivity.

WARNING!

Do not connect port 1 of the VIC 1455 to Fabric Interconnect A, and then connect port 2 of the VIC 1455 to Fabric Interconnect B. Using ports 1 and 2, each connected to FI A and FI B will lead to discovery and configuration failures.

Figure 8. Cisco UCS S-Series Storage Server Connectivity



Logical topology

Logical network design

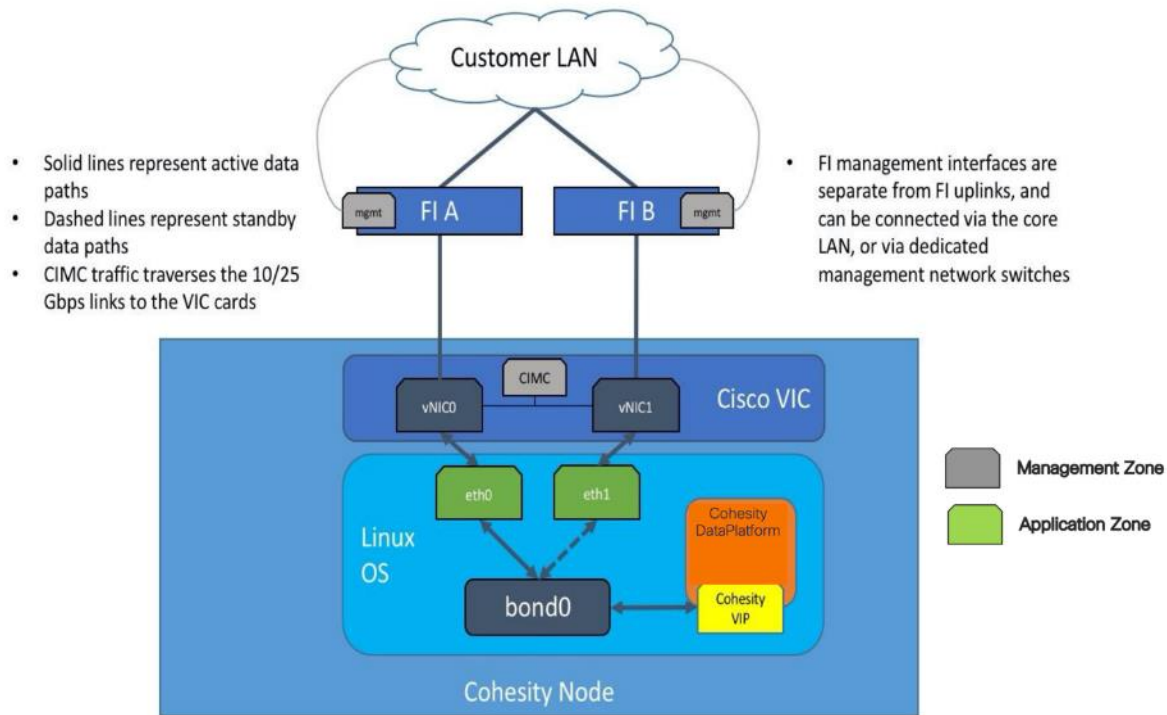
The Cohesity Helios Platform for Cohesity SmartFiles running on Cisco UCS has communication pathways that fall into two defined zones:

- **Management Zone:** This zone comprises the connections needed to manage the physical hardware, and the configuration of the Cisco UCS domain. These interfaces and IP addresses need to be available to all staff who will administer the UCS system, throughout the LAN/WAN. All IP addresses in this zone must be allocated from the same layer 2 (L2) subnet. This zone must provide access to Domain Name System (DNS), Network Time Protocol (NTP) services, and allow communication through HTTP/S and Secure Shell (SSH). In this zone are multiple physical and virtual components:
 - Fabric Interconnect management ports.
 - Cisco Intelligent Management Controller (CIMC) management interfaces used by each the rack-mount servers and blades, which answer through the FI management ports.
 - IPMI access over LAN, allowing Cohesity Operation System to obtain information about system hardware health to proactively raise alerts and warnings
- **Application Zone:** This zone comprises the connections used by the Cohesity Helios software and the underlying operating system on the nodes. These interfaces and IP addresses need to be able to always communicate with each other for proper operation, and they must be allocated from the same L2 subnet. The VLAN used for Cohesity application traffic must be accessible to/from all environments utilizing Cohesity File Services, such as the external NAS or external backup software utilizing Cohesity Views as Backup Target. This zone must provide access to

Domain Name System (DNS), Network Time Protocol (NTP) services, and allow communication through HTTP/S and Secure Shell (SSH). Finally, the VLAN must be able to traverse the network uplinks from the Cisco UCS domain, reaching FI A from FI B directly through the northbound switches, and vice-versa. In this zone are multiple components:

- A static IP address configured for the underlying Linux operating system of each Cohesity node. Two UCS vNICs are configured per node, one on the A side fabric, and one on the B side fabric. The two interfaces are configured as slave interfaces in a bond within the Linux operating system, using bond mode 1 (active/passive).
- A floating virtual IP address (VIP), one per node, that is used by Cohesity for all management, backup, and file services access. The assignment of the addresses is handled by the Cohesity software and will be re-assigned to an available node if any node should fall offline. These floating addresses are all assigned in DNS to a single A record, and the DNS server must respond to queries for that A record using DNS round-robin.

Figure 9. Logical Network Design



Network design

Cisco UCS uplink connectivity

Cisco UCS network uplinks connect “northbound” from the pair of Cisco UCS Fabric Interconnects to the LAN in the customer datacenter. All Cisco UCS uplinks operate as trunks, carrying multiple 802.1Q

VLAN IDs across the uplinks. The default Cisco UCS behavior is to assume that all VLAN IDs defined in the Cisco UCS configuration are eligible to be trunked across all available uplinks.

Cisco UCS Fabric Interconnects appear on the network as a collection of endpoints versus another network switch. Internally, the Fabric Interconnects do not participate in spanning-tree protocol (STP) domains, and the Fabric Interconnects cannot form a network loop, as they are not connected to each other with a layer 2 Ethernet link. All link up/down decisions through STP will be made by the upstream root bridges.

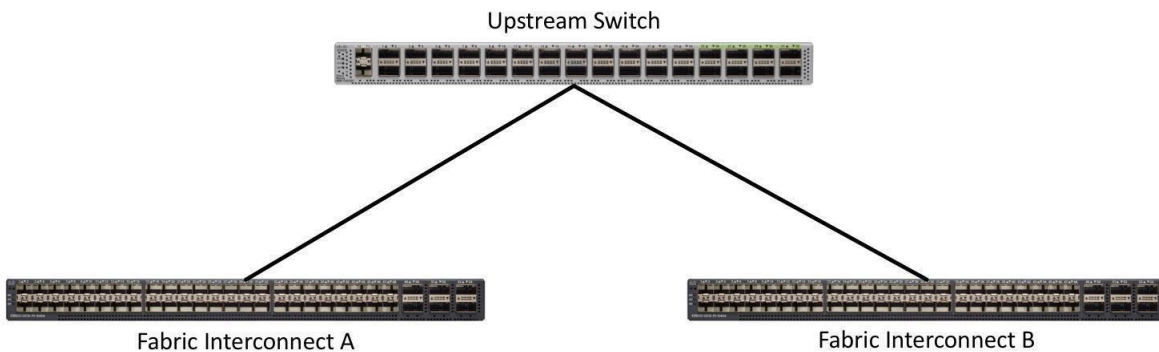
Uplinks need to be connected and active from both Fabric Interconnects. For redundancy, multiple uplinks can be used on each FI, either as 802.3ad Link Aggregation Control Protocol (LACP) port-channels or using individual links. For the best level of performance and redundancy, uplinks can be made as LACP port-channels to multiple upstream Cisco switches using the virtual port channel (vPC) feature. Using vPC uplinks allows all uplinks to be active passing data, plus protects against any individual link failure, and the failure of an upstream switch. Other uplink configurations can be redundant, however spanning-tree protocol loop avoidance may disable links if vPC is not available.

All uplink connectivity methods must allow for traffic to pass from one Fabric Interconnect to the other, or from fabric A to fabric B. There are scenarios where cable, port or link failures would require traffic that normally does not leave the Cisco UCS domain, to now be forced over the Cisco UCS uplinks. Additionally, this traffic flow pattern can be seen briefly during maintenance procedures, such as updating firmware on the Fabric Interconnects, which requires them to be rebooted. The following sections and figures detail several uplink connectivity options.

Single uplinks to single switch

This connection design is susceptible to failures at several points; single uplink failures on either Fabric Interconnect can lead to connectivity losses or functional failures, and the failure of the single uplink switch will cause a complete connectivity outage.

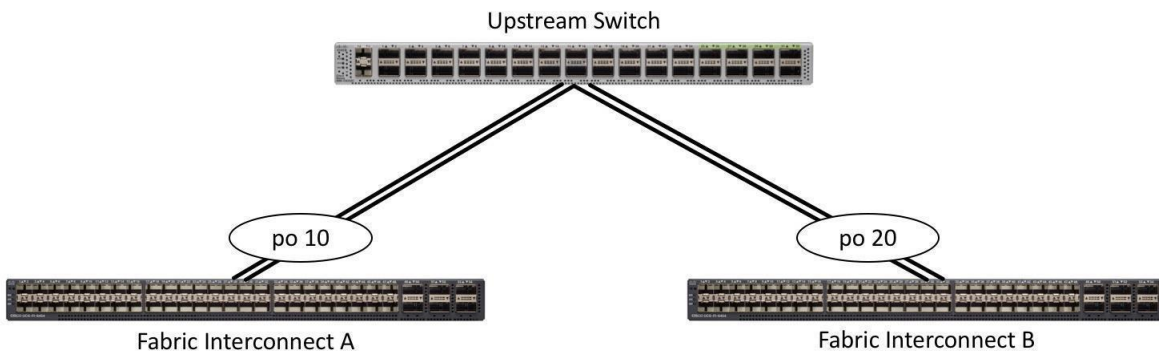
Figure 10. Connectivity with Single Uplink to Single Switch



Port channels to single switch

This connection design is now redundant against the loss of a single link but remains susceptible to the failure of the single switch.

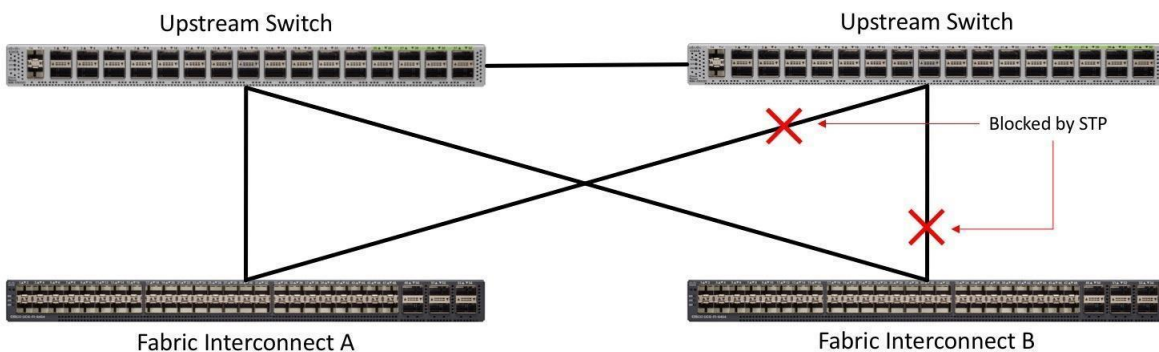
Figure 11. Connectivity with Port-Channels to Single Switch



Single uplinks or port channels to multiple switches

This connection design is redundant against the failure of an upstream switch, and redundant against a single link failure. In normal operation, STP is likely to block half of the links to avoid a loop across the two upstream switches. The side effect of this is to reduce bandwidth between the Cisco UCS domain and the LAN. If any of the active links were to fail, STP would bring the previously blocked link online to provide access to that Fabric Interconnect through the other switch. It is not recommended to connect both links from a single FI to a single switch, as that configuration is susceptible to a single switch failure breaking connectivity from fabric A to fabric B. For enhanced redundancy, the single links in the figure below could also be port-channels.

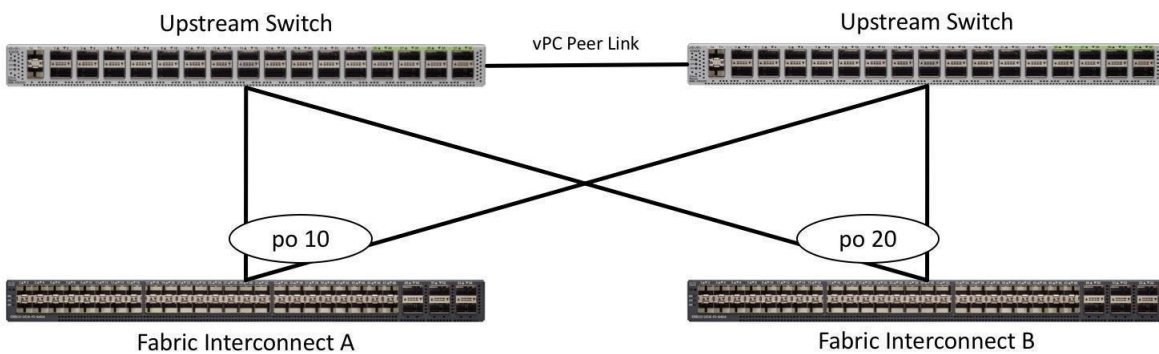
Figure 12. Connectivity with Multiple Uplink Switches



vPC to multiple switches

This recommended connection design relies on using Cisco switches that have the virtual port channel feature, such as Catalyst 6000 series switches running VSS, Cisco Nexus 5000 series, and Cisco Nexus 9000 series switches. Logically the two vPC enabled switches appear as one, and therefore spanning-tree protocol will not block any links. This configuration allows for all links to be active, achieving maximum bandwidth potential, and multiple redundancy at each level.

Figure 13. Connectivity with vPC



VLANs and subnets

For the Cohesity system configuration, one only one VLAN is needed to be carried to the Cisco UCS domain from the upstream LAN, and this VLAN is also defined in the Cisco UCS configuration. [Table 4](#) lists the VLANs required by Cohesity in Cisco UCS, and their functions:

Table 4. VLANs

VLAN Name	VLAN ID	Purpose
<<cohesity_vlan>>	Customer supplied	Cohesity node Linux OS interfaces Cohesity node software virtual IP addresses

Jumbo frames

All Cohesity traffic traversing the <<cohesity_vlan>> VLAN and subnet is configured by default to use standard ethernet frames.

Considerations

Prior to the installation of the cluster, proper consideration must be given to the number of nodes required for the Cohesity cluster, and the usable capacity that will result.

Scale

Cohesity clusters require a minimum of three (3) compute nodes, each Cisco UCS S3260 storage chassis can be equipped with two compute nodes. From that point, the cluster can grow to any size of cluster that is required by the end user which meets their overall storage space requirements. This limitless scaling is a key feature present in Cohesity which allows future growth without the fears of reaching an overall capacity restriction. Cohesity Data Platform allows addition of multiple nodes simultaneously.

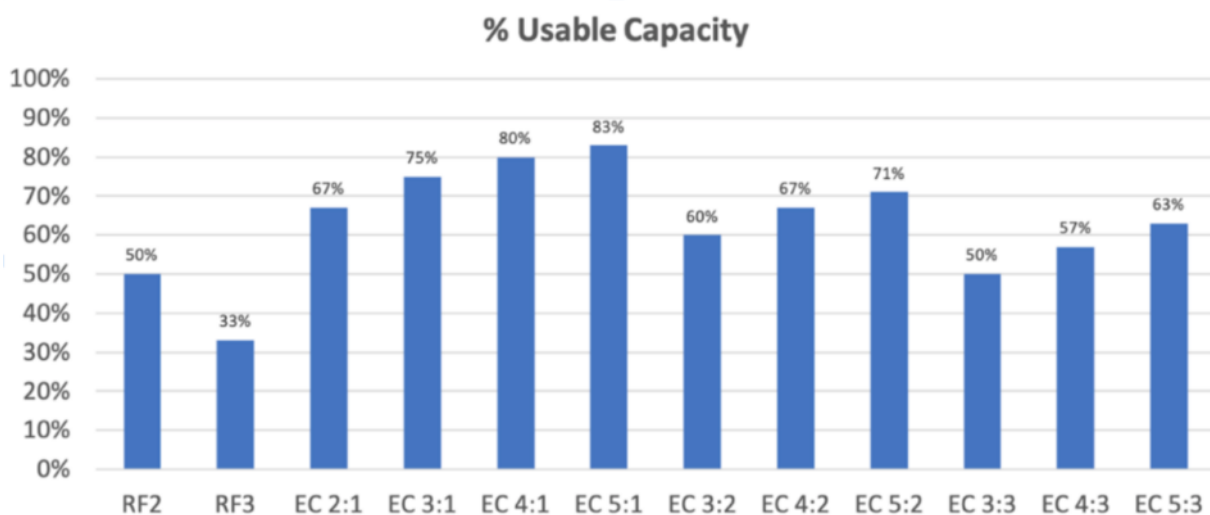
Capacity

Cohesity provides a configurable resiliency on HDDs or node failures. Both Replication Factor RF2 and RF3 along with the Erasure Coding (EC) scheme is supported with the Cohesity SpanFS filesystem. RF refers to the number of replicas of a unit of data. The unit of replication is a chunk file, and a chunk file is mirrored into either one or two other nodes depending on the RF number chosen. An RF2 mechanism provides resilience against a single data unit failure, and a RF3 provides resilience against two data unit failures.

EC refers to a scheme where a number of usable data stripe units can be protected from failures using code stripe units, which are in turn derived from the usable data stripe units. A single code stripe unit can protect against one data (or code) stripe failure, and two code stripe units can protect against two data (or code) stripe unit failures.

Based on the resiliency and fault tolerance chosen, the raw to usable capacity varies. The figure below provides a high-level understanding of the usable capacity when different types of RF or EC schemes are chosen.

Figure 14. Usable Capacity



For more information, please see the Cohesity resilience white paper: <https://info.cohesity.com/Cohesity-Fault-Tolerance-White-Paper.html>

Disk drive manufacturers have adopted a size reporting methodology using calculation by powers of 10, also known as decimal prefix. As an example, a 120 GB disk is listed with a minimum of 120 x 10⁹ bytes of usable addressable capacity, or 120 billion bytes. However, many operating systems and file systems report their space based on standard computer binary exponentiation, or calculation by powers of 2, also called binary prefix. In this example, 2¹⁰ or 1024 bytes make up a kilobyte, 2¹⁰ kilobytes make up a megabyte, 2¹⁰ megabytes make up a gigabyte, and 2¹⁰ gigabytes make up a terabyte. As the values increase, the disparity between the two systems of measurement and notation get worse, at the terabyte level, the deviation between a decimal prefix value and a binary prefix value is nearly 10 percent.

The International System of Units (SI) defines values and decimal prefix by powers of 10 as listed in [Table 5](#).

Table 5. SI Unit Values (Decimal Prefix)

Value	Symbol	Name
1000 bytes	kB	Kilobyte
1000 kB	MB	Megabyte
1000 MB	GB	Gigabyte
1000 GB	TB	Terabyte

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) defines values and binary prefix by powers of 2 in ISO/IEC 80000-13:2008 Clause 4 as listed in [Table 6](#).

Table 6. IEC Unit Values (binary prefix)

Value	Symbol	Name
1024 bytes	KiB	Kibibyte
1024 KiB	MiB	Mebibyte
1024 MiB	GiB	Gibibyte
1024 GiB	TiB	Tebibyte

For the purpose of this document, the decimal prefix numbers are used only for raw disk capacity as listed by the respective manufacturers. For all calculations where raw or usable capacities are shown from the perspective of the Cohesity software, filesystems or operating systems, the binary prefix numbers are used. This is done primarily to show a consistent set of values as seen by the end user

from within the Cohesity HTML management dashboard when viewing cluster capacity, allocation, and consumption, and also within most operating systems.

[Table 7](#) lists a set of Cohesity Helios cluster usable capacity values, using binary prefixes, for an array of cluster configurations. These values provide an example of the capacity calculations, for determining the appropriate size of Cohesity cluster to initially purchase. Additional savings from deduplication and compression will raise the effective logical capacity far beyond the physical capacity of the nodes. Additionally, the choice of replication factor 2, or erasure coding, will determine the overall efficiency of the real data being stored on the nodes.

Table 7. Cohesity Cluster Usable Physical Capacities

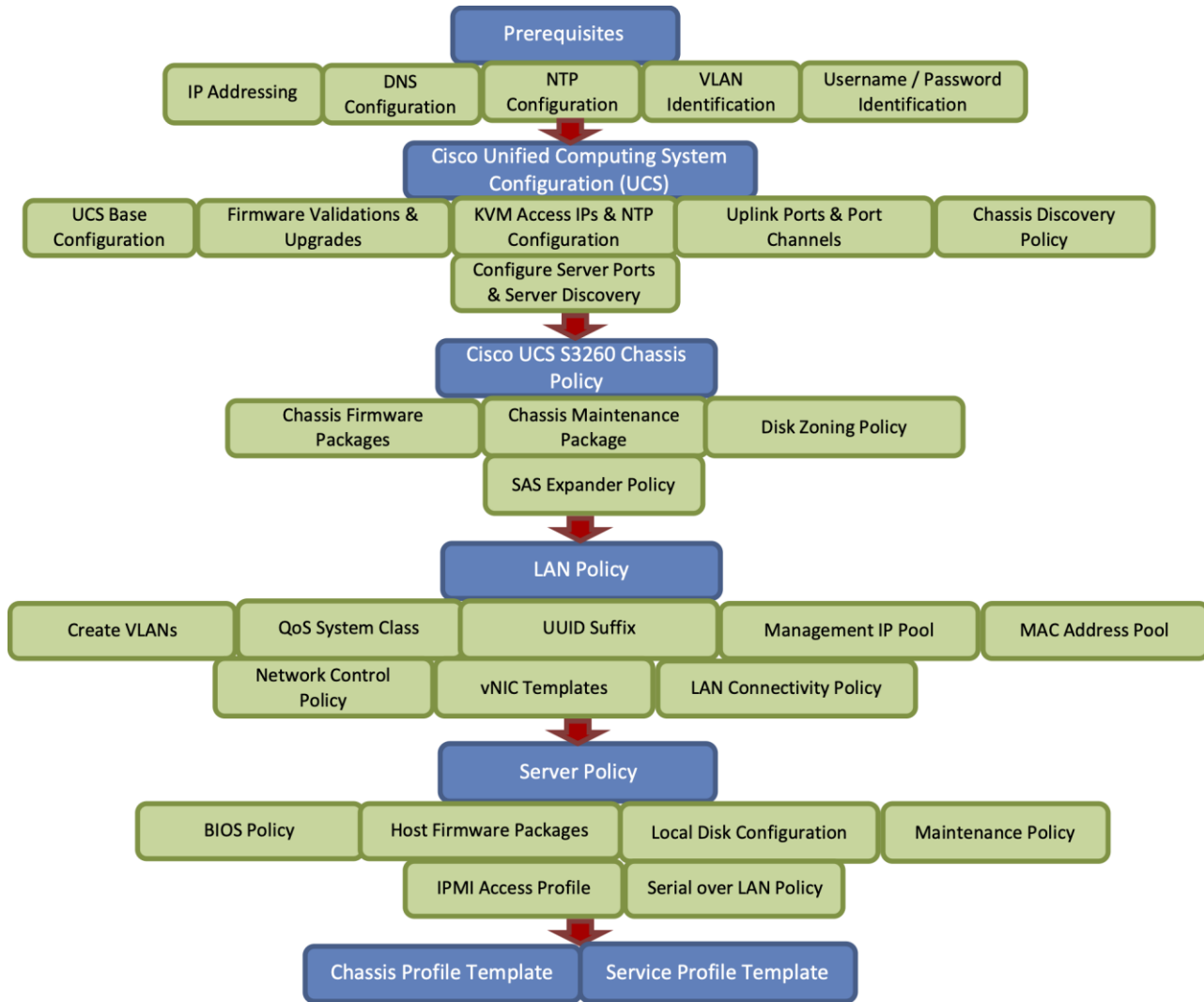
Cisco UCS C-Series Server Model	Capacity Disk Size (each)	Capacity Disk Quantity (per node)	Usable Capacity (per node)	Capacity per node @ RF2	Capacity per node with EC 2:1
C240-M5L	4 TB	12	43.7 TiB	21.8 TiB	29.1 TiB
	10 TB	12	109.2 TiB	54.6 TiB	72.8 TiB
S3260 M5	10 TB	42	382.2 TiB	191.1 TiB	254.8 TiB
	10 TB	21	191.1 TiB	95.6 TiB	127.4 TiB

Configuration and Installation

Installing the Cohesity Helios system is done through mounting a virtual DVD image to each Cisco UCS S-Series Storage Server node, which is available for download from Cohesity as an ISO file. The installation DVD validates the hardware configuration, installs the Linux operating system, copies the Cohesity software packages, and completes with the nodes ready for their final configuration to form a cluster. Prior to using the installation DVD, the configuration of the Cisco UCS domain, its policies, templates, and service profiles to be associated to the servers must be completed. The following sections will guide you through the prerequisites and manual steps needed to configure Cisco UCS Manager prior to booting the Cohesity installation DVD, the steps to install Cohesity to each node, and how to perform the remaining post-installation tasks to configure the Cohesity cluster. Finally, a basic configuration example is given for configuring Cohesity Storage Domains, Sources, Policies, Protection Jobs, file services Views, and Test/Dev virtual machine services.

The workflow to configure Cisco UCS for Cohesity cluster with the Cisco UCS S3260 Storage server is detailed in the workflow below. This is a one-time process to configure the Cisco UCS Chassis and Server Profiles Templates for Cohesity Cluster, Chassis Profiles and Service Profiles can be instantiated from templates and attached to multiple Cisco UCS S3260 Chassis and server nodes within the same UCS Domain. A Cisco UCS domain allows you to quickly align computing resources in the data center with rapidly changing business requirements. This built-in flexibility is determined by whether you choose to fully implement the stateless computing feature.

Figure 15. Cisco UCS Configuration Workflow



Note: The workflow (Figure 15) to configure the Cisco UCS chassis and server profiles templates for Cohesity Cluster is a one-time process. The chassis profiles and service profiles can be instantiated from templates and attached to multiple Cisco UCS S3260 chassis and server nodes within the same Cisco UCS domain.

Prerequisites

Prior to beginning the installation activities, complete the following necessary tasks and gather the required information.

IP addressing

IP addresses for the Cohesity system on Cisco UCS need to be allocated from the appropriate subnets and VLANs to be used. IP addresses that are used by the system fall into the following groups:

- Cisco UCS Management: These addresses are used and assigned by Cisco UCS Manager. Three IP addresses are used by Cisco UCS Manager; one address is assigned to each Cisco UCS Fabric Interconnect, and the third IP address is a roaming address for management of the Cisco UCS cluster. In addition, at least one IP address per Cisco UCS S-series compute node is required for the Cohesity external management IP address pool, which is assigned to the CIMC interface of the physical servers. Since these management addresses are assigned from a pool, they need to be provided in a contiguous block of addresses. These addresses must all be in the same subnet.
- Cohesity Application: These addresses are used by the Linux OS on each Cohesity node, and the Cohesity software. Two IP addresses per node in the Cohesity cluster are required from the same subnet. These addresses can be assigned from the same subnet at the Cisco UCS Management addresses, or they may be separate.

Use the following tables to list the required IP addresses for the installation of a 4-node standard Cohesity cluster and review an example IP configuration.

Note: Table cells shaded in black do not require an IP address

Table 8. Cohesity Cluster IP Addressing

Address Group:	UCS Management	Cohesity Application	
VLAN ID:			
Subnet:			
Subnet Mask:			
Gateway:			
Device	UCS Management Addresses	Node IP	Cohesity VIP
Fabric Interconnect A			
Fabric Interconnect B			
UCS Manager			
Cohesity Node #1			
Cohesity Node #2			
Cohesity Node #3			
Cohesity Node #4			

Table 9. Example Cohesity Cluster IP Addressing

Address Group:	UCS Management	Cohesity Application
----------------	----------------	----------------------

Address Group:	UCS Management	Cohesity Application	
VLAN ID:	3171	3171	
Subnet:	192.168.110.0	192.168.110.0	
Subnet Mask:	255.255.255.0	255.255.255.0	
Gateway:	192.168.110.1	192.168.110.1	
Device	UCS Management Addresses	Node IP	Cohesity VIP
Fabric Interconnect A	192.168.110.33		
Fabric Interconnect B	192.168.110.34		
UCS Manager	192.168.110.32		
Cohesity Node #1	192.168.110.146	192.168.110.151	192.168.110.155
Cohesity Node #2	192.168.110.147	192.168.110.152	192.168.110.156
Cohesity Node #3	192.168.110.148	192.168.110.153	192.168.110.157
Cohesity Node #4	192.168.110.149	192.168.110.154	192.168.110.158

DNS

DNS servers are required to be configured for querying Fully Qualified Domain Names (FQDN) in the Cohesity application group. DNS records need to be created prior to beginning the installation. At a minimum, it is required to create a single A record for the name of the Cohesity cluster, which answers with each of the virtual IP addresses used by the Cohesity nodes in round-robin fashion. Some DNS servers are not configured by default to return multiple addresses in round-robin fashion in response to a request for a single A record, please ensure your DNS server is properly configured for round-robin before continuing. The configuration can be tested by querying the DNS name of the Cohesity cluster from multiple clients and verifying that all of the different IP addresses are given as answers in turn.

Use the following tables to list the required DNS information for the installation and review an example configuration.

Table 10. DNS Server Information

Item	Value	A Records
DNS Server #1		
DNS Server #2		
DNS Domain		

Item	Value	A Records
UCS Domain Name		
Cohesity Cluster Name		

Table 11. DNS Server Example Information

Item	Value	A Records
DNS Server #1	192.168.110.16	
DNS Server #2		
DNS Domain		
UCS Domain Name	B22-FI	
Cohesity Cluster Name	192.168.110.155	192.168.110.155
		192.168.110.156
		192.168.110.157
		192.168.110.158

NTP

Consistent time clock synchronization is required across the components of the Cohesity cluster, provided by reliable NTP servers, accessible for querying in the Cisco UCS Management network group, and the Cohesity Application group.

Use the following tables to list the required NTP information for the installation and review an example configuration.

Table 12. NTP Server Information

Item	Value
------	-------

Item	Value
NTP Server #1	
NTP Server #2	
Timezone	

Table 13. NTP Server Example Information

Item	Value
NTP Server #1	192.168.110.16
NTP Server #2	
Timezone	(UTC-8:00) Pacific Time

VLANS

Prior to the installation, the required VLAN IDs need to be documented, and created in the upstream network if necessary. There is one VLAN that needs to be trunked to the two Cisco UCS Fabric Interconnects which manage the Cohesity cluster; the VLAN for the Cohesity Application group. The VLAN IDs must be supplied during the Cisco UCS configuration steps, and the VLAN names should be customized to make them easily identifiable.

Use the following tables to list the required VLAN information for the installation and review an example configuration:

Table 14. VLAN Information

Name	ID
<<cohesity_vlan>>	

Table 15. VLAN Example Information

Name	ID
VLAN3171	3171

Network uplinks

The Cisco UCS uplink connectivity design needs to be finalized prior to beginning the installation. Refer to the network uplink design possibilities in the [Network Design](#) section.

Use the following tables to list the required network uplink information for the installation and review an example configuration.

Table 16. Network Uplink Configuration

Fabric Interconnect Port		Port Channel	Port Channel Type	Port Channel ID	Port Channel Name
A		<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> LACP		
		<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> vPC		
		<input type="checkbox"/> Yes <input type="checkbox"/> No			
		<input type="checkbox"/> Yes <input type="checkbox"/> No			
B		<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> LACP		
		<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> vPC		
		<input type="checkbox"/> Yes <input type="checkbox"/> No			
		<input type="checkbox"/> Yes <input type="checkbox"/> No			

Table 17. Network Uplink Example Configuration

Fabric Interconnect Port		Port Channel	Port Channel Type	Port Channel ID	Port Channel Name
A	1/53	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> LACP	31	vpc31
	1/54	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input checked="" type="checkbox"/> vPC		
		<input type="checkbox"/> Yes <input type="checkbox"/> No			
		<input type="checkbox"/> Yes <input type="checkbox"/> No			
B	1/53	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> LACP	32	vpc32

Fabric Interconnect Port		Port Channel	Port Channel Type	Port Channel ID	Port Channel Name
	1/54	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	<input checked="" type="checkbox"/> vPC		
		<input type="checkbox"/> Yes <input type="checkbox"/> No			
		<input type="checkbox"/> Yes <input type="checkbox"/> No			

Username and passwords

Several usernames and passwords need to be defined or known as part of the Cohesity installation and configuration process. Use the following tables to list the required username and password information and review an example configuration.

Table 18. Usernames and Passwords

Account	Username	Password
UCS Administrator	admin	<<ucs_admin_pw>>
Cohesity Administrator	admin	<<cohesity_admin_pw>>

Table 19. Example Usernames and Passwords

Account	Username	Password
UCS Administrator	admin	xxxx
Cohesity Administrator	admin	xxxx

Physical installation

Install the Fabric Interconnects and the Cisco UCS C-Series rack-mount servers according to their corresponding hardware installation guides listed below:

Cisco UCS 6454 Fabric Interconnect:

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/hw/6454-install-guide/6454.pdf

Cisco UCS S Series Storage Server:

https://www.cisco.com/c/dam/en/us/td/docs/unified_computing/ucs/s/hw/S3260/installb/S3260.pdf

Cabling

The physical layout of the Cohesity system was previously described in section [Physical Topology](#). The Fabric Interconnects and S-series chassis need to be cabled properly before beginning the installation activities.

[Table 20](#) lists an example cabling map for installation of a Cohesity system, using four compute nodes, each Cisco UCS S3260 Chassis is equipped with two compute nodes.

Table 20. Example Cabling Map

Device	Port	Connected To	Port	Type	Length	Note
UCS6454-A	L1	UCS6454-B	L1	CAT5	1FT	
UCS6454-A	L2	UCS6454-B	L2	CAT5	1FT	
UCS6454-A	mgmt0	Customer LAN		CAT5		Management interface
UCS6454-A	1/17	Cohesity Chassis #1 server node#1	mLOM port 1	Twinax	3M	Chassis1/Server1
UCS6454-A	1/18	Cohesity Chassis #1 server node#1	mLOM port 2	Twinax	3M	Chassis1/Server1
UCS6454-A	1/19	Cohesity Chassis #1 server node#2	mLOM port 1	Twinax	3M	Chassis1/Server2
UCS6454-A	1/20	Cohesity Chassis #1 server node#2	mLOM port 2	Twinax	3M	Chassis1/Server2
UCS6454-A	1/21	Cohesity Chassis #2 server node#1	mLOM port 1	Twinax	3M	Chassis2/Server1
UCS6454-A	1/22	Cohesity Chassis #2 server node#1	mLOM port 2	Twinax	3M	Chassis2/Server1
UCS6454-A	1/23	Cohesity Chassis #2 server node#2	mLOM port 1	Twinax	3M	Chassis2/Server2
UCS6454-A	1/24	Cohesity Chassis #2 server node#2	mLOM port 2	Twinax	3M	Chassis2/Server2
UCS6454-A	1/53	Customer LAN				uplink
UCS6454-A	1/54	Customer LAN				uplink
UCS6454-B	L1	UCS6454-A	L1	CAT5	1FT	
UCS6454-B	L2	UCS6454-A	L2	CAT5	1FT	
UCS6454-B	mgmt0	Customer LAN		CAT5		Management interface
UCS6454-A	1/17	Cohesity Chassis #1	mLOM port 3	Twinax	3M	Chassis1/Server1

Device	Port	Connected To	Port	Type	Length	Note
		server node#1				
UCS6454-A	1/18	Cohesity Chassis #1 server node#1	mLOM port 4	Twinax	3M	Chassis1/Server1
UCS6454-A	1/19	Cohesity Chassis #1 server node#2	mLOM port 3	Twinax	3M	Chassis1/Server2
UCS6454-A	1/20	Cohesity Chassis #1 server node#2	mLOM port 4	Twinax	3M	Chassis1/Server2
UCS6454-A	1/21	Cohesity Chassis #2 server node#1	mLOM port 3	Twinax	3M	Chassis2/Server1
UCS6454-A	1/22	Cohesity Chassis #2 server node#1	mLOM port 4	Twinax	3M	Chassis2/Server1
UCS6454-A	1/23	Cohesity Chassis #2 server node#2	mLOM port 3	Twinax	3M	Chassis2/Server2
UCS6454-A	1/24	Cohesity Chassis #2 server node#2	mLOM port 4	Twinax	3M	Chassis2/Server2
UCS6454-B	1/53	Customer LAN				uplink
UCS6454-B	1/54	Customer LAN				uplink

Cisco UCS installation

This section describes the steps to initialize and configure the Cisco UCS Fabric Interconnects, to prepare them for the Cohesity installation. For installations of Cohesity being integrated into an existing Cisco UCS domain, the following steps outlining the initial setup of the Fabric Interconnects, and their uplink port configuration can be skipped. In this situation, the steps beginning with the configuration of the server ports and server discovery onwards, including sub-organizations, policies, pools, templates, and service profiles, must still be performed.

Procedure 1. Configure Cisco UCS Fabric Interconnect A

- Step 1.** Make sure the Fabric Interconnect cabling is properly connected, including the L1 and L2 cluster links, and the management ports, then power the Fabric Interconnects on by inserting the power cords.
- Step 2.** Connect to the console port on the first Fabric Interconnect, which will be designated as the A fabric device. Use the supplied Cisco console cable (CAB-CONSOLE-RJ45=), and connect it to a built-in DB9 serial port, or use a USB to DB9 serial port adapter.
- Step 3.** Start your terminal emulator software.
- Step 4.** Create a connection to the COM port of the computer's DB9 port, or the USB to serial adapter. Set the terminal emulation to VT100, and the settings to 9600 baud, 8 data bits, no parity, and 1 stop bit.

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

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

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

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

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

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

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

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

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

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

Enter the password for "admin":

Confirm the password for "admin":

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

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

Enter the system name: B22-FI

Physical Switch Mgmt0 IP address : 192.168.110.33

Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0

IPv4 address of the default gateway : 192.168.110.1

Cluster IPv4 address : 192.168.110.32

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

DNS IP address : 192.168.110.16

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

Default domain name :

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

Following configurations will be applied:

Switch Fabric=A

System Name=B22-FI

Enforced Strong Password=yes

Physical Switch Mgmt0 IP Address=192.168.110.33

Physical Switch Mgmt0 IP Netmask=255.255.255.0

Default Gateway=192.168.110.1

Ipv6 value=0

DNS Server=192.168.110.16

Domain Name=

Cluster Enabled=yes

Cluster IP Address=192.168.110.32

NOTE: Cluster IP will be configured only after both Fabric Interconnects are initialized

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

Applying configuration. Please wait.

Configuration file - Ok

Procedure 2. Configure Cisco UCS Fabric Interconnect B

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

Step 2. Start your terminal emulator software.

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

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

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

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

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

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

```
Enter the configuration method. (console/gui) ? console
Installer has detected the presence of a peer Fabric interconnect. This Fabric
interconnect will be added to the cluster. Continue (y/n) ? y
Enter the admin password of the peer Fabric interconnect:
Connecting to peer Fabric interconnect... done
Retrieving config from peer Fabric interconnect... done
Peer Fabric interconnect Mgmt0 IPv4 Address: 192.168.110.33
Peer Fabric interconnect Mgmt0 IPv4 Netmask: 255.255.255.0
Cluster IPv4 address          : 192.168.110.32
Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric Interconnect Mgmt0
IPv4 Address
Physical Switch Mgmt0 IP address : 192.168.110.34
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no):
yes
Applying configuration. Please wait.
Configuration file - Ok
```

Procedure 3. Log into Cisco UCS Manager

Step 1. Open a web browser and navigate to the Cisco UCS Manager Cluster IP address, for example <https://192.168.110.32/>

Figure 16. Cisco UCS Manager Web Interface



- Step 2.** Click the “Launch UCS Manager” HTML link to open the Cisco UCS Manager web client.
- Step 3.** At the login prompt, enter “admin” as the username, and enter the administrative password that was set during the initial console configuration.
- Step 4.** Click No when prompted to enable Cisco Smart Call Home, this feature can be enabled at a later time.
- Step 5.** Verify the Main Topology View as shown below:

Figure 17. Cisco UCS Main Topology View



Cisco UCS Configuration

Configure the following ports, settings, and policies in the Cisco UCS Manager interface prior to beginning the Cohesity Helios installation.

Cisco UCS Firmware

Your Cisco UCS firmware version should be current as shipped from the factory, as documented in the [Software Components](#) section. This document is based on Cisco UCS infrastructure, Cisco UCS B-series bundle, and Cisco UCS C-Series bundle software versions 4.1(3b). If the firmware version of the Fabric Interconnects is older than this version, the firmware must be upgraded to match the requirements prior to completing any further steps. To upgrade the Cisco UCS Manager version, the Fabric Interconnect firmware, and the server bundles, refer to these instructions:

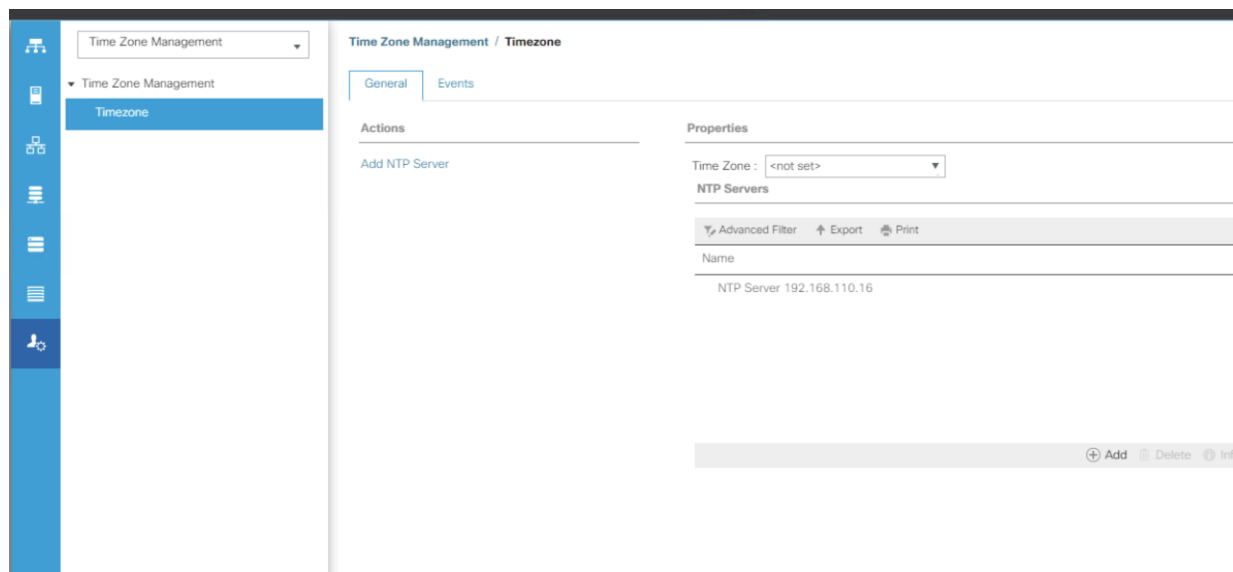
https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Getting-Started/4-0/b_UCSM_Getting_Started_Guide_4_0/b_UCSM_Getting_Started_Guide_4_0_chapter_01.html

Procedure 1. Synchronize the Cisco UCS environment time to the NTP server

- Step 1.** In Cisco UCS Manager, click Admin.
- Step 2.** In the navigation pane, select All > Time Zone Management, and click the carat next to Time Zone Management to expand it.
- Step 3.** Click Timezone.
- Step 4.** In the Properties pane, select the appropriate time zone in the Time Zone menu.
- Step 5.** Click Add NTP Server.
- Step 6.** Enter the NTP server IP address and click OK.
- Step 7.** Click OK.

Step 8. Click Save Changes and then click OK.

Figure 18. NTP Configuration



Uplink ports

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

Procedure 2. Define ports to use as network uplinks to the upstream network

- Step 1.** In Cisco UCS Manager, click Equipment.
- Step 2.** Select Fabric Interconnects > Fabric Interconnect A > Fixed Module or Expansion Module as appropriate > Ethernet Ports.
- Step 3.** Select the ports that are to be uplink ports, right-click them, and click Configure as Uplink Port.

Figure 19. Uplink Ports – Fabric Interconnect A

The screenshot shows the 'Ethernet Ports' configuration page for Fabric Interconnect A (primary). The left sidebar shows the navigation tree with 'Ethernet Ports' selected under 'Fixed Module'. The main area displays a table of ports with a context menu open over the table. The context menu options are:

- Enable
- Disable
- Configure as Server Port
- Configure as Uplink Port**
- Configure as FCoE Uplink Port
- Configure as FCoE Storage Port
- Configure as Appliance Port
- Unconfigure
- Unconfigure FCoE Uplink Port
- Unconfigure Uplink Port
- Unconfigure FCoE Storage Port
- Unconfigure Appliance Port

Slot	Aggr. Port ID	Port ID	MAC
1	0	34	00:3A:9C:95:E2:09
1	0	35	00:3A:9C:95:E2:0A
1	0	36	00:3A:9C:95:E2:0B
1	0	37	00:3A:9C:95:E2:0C
1	0	38	00:3A:9C:95:E2:0D
1	0	39	00:3A:9C:95:E2:0E
1	0	40	00:3A:9C:95:E2:0F
1	0	41	00:3A:9C:95:E2:10
1	0	42	00:3A:9C:95:E2:11
1	0	43	00:3A:9C:95:E2:12
1	0	44	00:3A:9C:95:E2:13
1	0	45	00:3A:9C:95:E2:14
1	0	46	00:3A:9C:95:E2:15
1	0	47	00:3A:9C:95:E2:16
1	0	48	00:3A:9C:95:E2:17
1	0	49	00:3A:9C:95:E2:18
1	0	50	00:3A:9C:95:E2:19
1	0	51	00:3A:9C:95:E2:1A
1	0	52	00:3A:9C:95:E2:1B
1	0	53	00:3A:9C:95:E2:1C
1	0	54	00:3A:9C:95:E2:1D
1	0	55	00:3A:9C:95:E2:1E
1	0	56	00:3A:9C:95:E2:1F
1	0	57	00:3A:9C:95:E2:20
1	0	58	00:3A:9C:95:E2:21
1	0	59	00:3A:9C:95:E2:22
1	0	60	00:3A:9C:95:E2:23
1	0	61	00:3A:9C:95:E2:24
1	0	62	00:3A:9C:95:E2:25
1	0	63	00:3A:9C:95:E2:26
1	0	64	00:3A:9C:95:E2:27
1	0	65	00:3A:9C:95:E2:28
1	0	66	00:3A:9C:95:E2:29
1	0	67	00:3A:9C:95:E2:2A
1	0	68	00:3A:9C:95:E2:2B
1	0	69	00:3A:9C:95:E2:2C

Step 4. Click Yes to confirm the configuration and click OK.

Step 5. Select Fabric Interconnects > Fabric Interconnect B > Fixed Module or Expansion Module as appropriate > Ethernet Ports.

Step 6. Select the ports that are to be uplink ports, right-click them, and click Configure as Uplink Port.

Step 7. Click Yes to confirm the configuration and click OK.

Step 8. Verify all the necessary ports are now configured as uplink ports, where their role is listed as “Network.”

Figure 20. Uplink Ports Configuration

The screenshot shows the 'Ethernet Ports' configuration page for Fabric Interconnect A (primary). The left sidebar shows the navigation tree with 'Ethernet Ports' selected under 'Fixed Module'. The main area displays a table of ports with their configuration details. The table has the following columns: Slot, Aggr. Port ID, Port ID, MAC, If Role, If Type, Overall Status, and Admin State.

Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status	Admin State
1	0	53	00:DE:FB:FD:1A:...	Network	Physical	Up	Enabled
1	0	54	00:DE:FB:FD:1A:...	Network	Physical	Up	Enabled

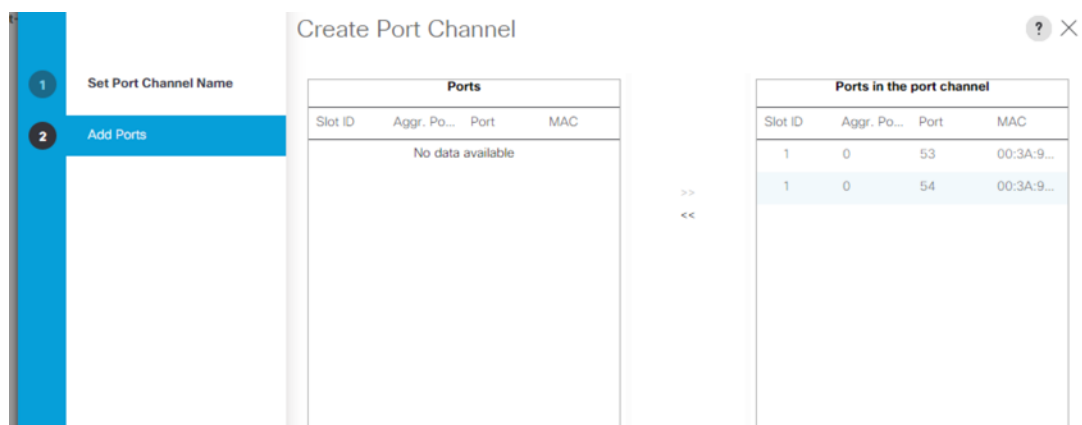
Uplink port channels

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

Procedure 3. Configure port channels in the Cisco UCS environment

- Step 1.** In Cisco UCS Manager, click LAN.
- Step 2.** Under LAN > LAN Cloud, click the carat to expand the Fabric A tree.
- Step 3.** Right-click Port Channels underneath Fabric A, then click Create Port Channel.
- Step 4.** Enter the port channel ID number as the unique ID of the port channel (this does not have to match the port-channel ID on the upstream switch).
- Step 5.** Enter the name of the port channel.
- Step 6.** Click Next.
- Step 7.** Click each port from Fabric Interconnect A that will participate in the port channel and click the >> button to add them to the port channel.

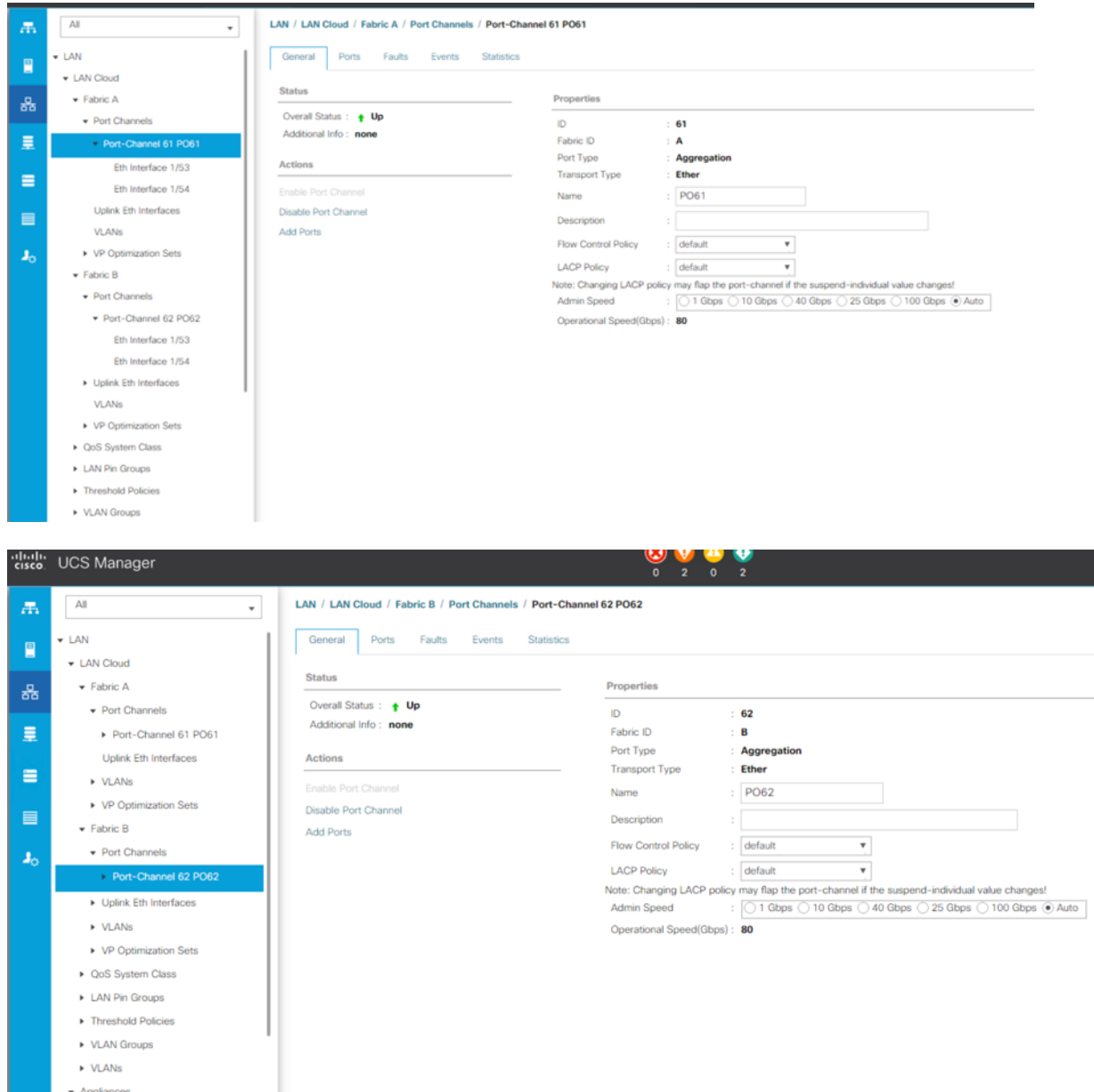
Figure 21. Port Channel Configuration - Fabric Interconnect A



- Step 8.** Click Finish.
- Step 9.** Click OK.
- Step 10.** Under LAN > LAN Cloud, click the carat to expand the Fabric B tree.
- Step 11.** Right-click Port Channels underneath Fabric B, then click Create Port Channel.
- Step 12.** Enter the port channel ID number as the unique ID of the port channel (this does not have to match the port-channel ID on the upstream switch).
- Step 13.** Enter the name of the port channel.
- Step 14.** Click Next.
- Step 15.** Click each port from Fabric Interconnect B that will participate in the port channel and click the >> button to add them to the port channel.
- Step 16.** Click Finish.
- Step 17.** Click OK.

Step 18. Verify the necessary port channels have been created. It can take a few minutes for the newly formed port channels to converge and come online.

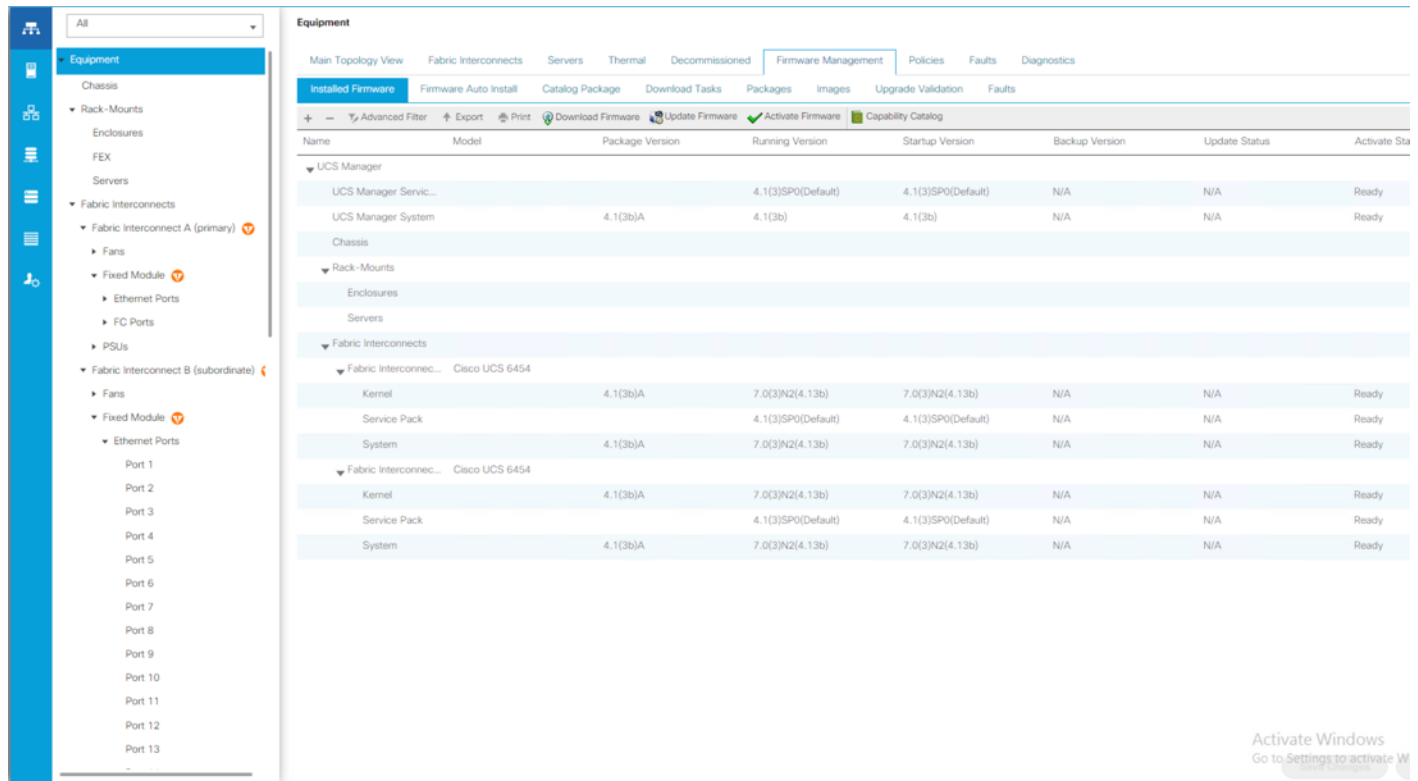
Figure 22. Port Channel - Fabric Interconnect A/B



Cisco UCS Manager Software Version 4.1(3b)

This document assumes you are using Cisco UCS Manager Software version 4.1(3b). To upgrade the Cisco UCS Manager software and the Cisco UCS 6454 Fabric Interconnect software to a higher version of the firmware,) refer to [Cisco UCS Manager Install and Upgrade Guides](#). The firmware on the present setup is detailed in the screenshot below:

Figure 23. Cisco UCS Manager Software Version 4.1(3b)



Server ports

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

Auto configuration

A new feature in Cisco UCS Manager 3.1(3a) and later is Server Port Auto-Discovery, which automates the configuration of ports on the Fabric Interconnects as server ports when a Cisco UCS rack-mount server or blade chassis is connected to them. The firmware on the rack-mount servers or blade chassis Fabric Extenders must already be at version 3.1(3a) or later in order for this feature to function properly. Enabling this policy eliminates the manual steps of configuring each server port, however it does configure the servers in a somewhat random order. For example, the rack-mount server at the

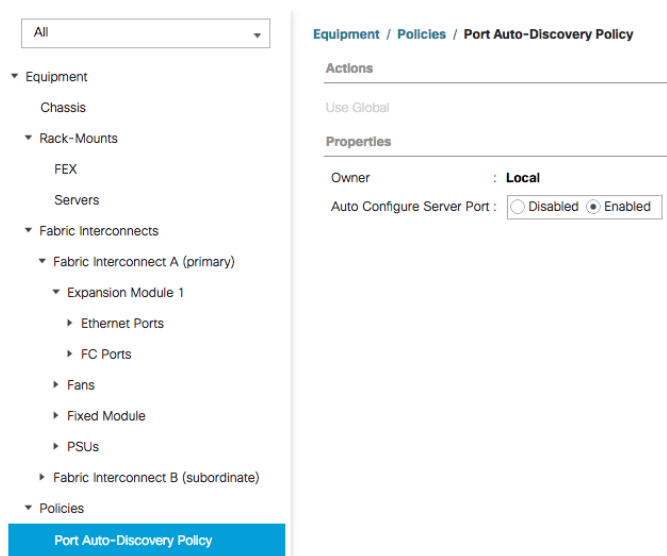
bottom of the stack, which you may refer to as server 1, and you may have plugged into port 1 of both Fabric Interconnects, could be discovered as server 2, or server 5, and so on.

Note: In order to have fine control of the rack-mount server or chassis numbering and order, the manual configuration steps listed in the next section must be followed.

Procedure 1. Configure the automatic server port definition and discovery

- Step 1.** In Cisco UCS Manager, click Equipment.
- Step 2.** In the navigation tree, under Policies, click Port Auto-Discovery Policy
- Step 3.** In the properties pane, set Auto Configure Server Port option to Enabled.
- Step 4.** Click Save Changes.
- Step 5.** Click OK.
- Step 6.** Wait for a brief period, until the rack-mount servers appear in the Equipment tab underneath Equipment > Rack Mounts > Servers, or the chassis appears underneath Equipment > Chassis.

Figure 24. Server Port Auto Discovery Policy



Manual configuration

Procedure 2. Manually define the specified ports

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

- Step 5.** Select Fabric Interconnects > Fabric Interconnect B > Fixed Module or Expansion Module as appropriate > Ethernet Ports.
- Step 6.** Select the matching port as chosen for Fabric Interconnect A that is to be a server port, right-click it, and click Configure as Server Port.
- Step 7.** Click Yes to confirm the configuration and click OK.
- Step 8.** Wait for a brief period, until the Chassis appears in the Equipment tab underneath Equipment > Chassis
- Step 9.** Repeat steps 1-8 for each pair of server ports, until all rack-mount servers and chassis appear in the order desired in the Equipment tab.

Figure 25. Server Port Manual Configuration

The screenshot shows the Cisco UCS Manager interface for configuring server ports on Fabric Interconnect A. The left navigation pane shows the hierarchy: Equipment > Fabric Interconnects > Fabric Interconnect A (primary) > Ethernet Ports. The main table displays the following data:

Name	Slot	Port ID	MAC	If Role	If Type	Overall Status	Admin State
Port 7	1	7	00:3A:9C:95:E3:0E	Unconfigured	Physical	Stp Not Present	Disabled
Port 8	1	8	00:3A:9C:95:E3:0F	Unconfigured	Physical	Stp Not Present	Disabled
Port 9	1	9	00:3A:9C:95:E3:10	Unconfigured	Physical	Stp Not Present	Disabled
Port 10	1	10	00:3A:9C:95:E3:11	Unconfigured	Physical	Stp Not Present	Disabled
Port 11	1	11	00:3A:9C:95:E3:12	Unconfigured	Physical	Stp Not Present	Disabled
Port 12	1	12	00:3A:9C:95:E3:13	Unconfigured	Physical	Stp Not Present	Disabled
Port 13	1	13	00:3A:9C:95:E3:14	Unconfigured	Physical	Stp Not Present	Disabled
Port 14	1	14	00:3A:9C:95:E3:15	Unconfigured	Physical	Stp Not Present	Disabled
Port 15	1	15	00:3A:9C:95:E3:16	Unconfigured	Physical	Stp Not Present	Disabled
Port 16	1	16	00:3A:9C:95:E3:17	Unconfigured	Physical	Stp Not Present	Disabled
Port 17	1	17	00:3A:9C:95:E3:18	Server	Physical	Up	Enabled
Port 18	1	18	00:3A:9C:95:E3:19	Server	Physical	Up	Enabled
Port 19	1	19	00:3A:9C:95:E3:1A	Server	Physical	Up	Enabled
Port 20	1	20	00:3A:9C:95:E3:1B	Server	Physical	Up	Enabled
Port 21	1	21	00:3A:9C:95:E3:1C	Server	Physical	Up	Enabled
Port 22	1	22	00:3A:9C:95:E3:1D	Server	Physical	Up	Enabled
Port 23	1	23	00:3A:9C:95:E3:1E	Server	Physical	Up	Enabled
Port 24	1	24	00:3A:9C:95:E3:1F	Server	Physical	Up	Enabled
Port 25	1	25	00:3A:9C:95:E3:20	Unconfigured	Physical	Stp Not Present	Disabled

Chassis and Server Discovery

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

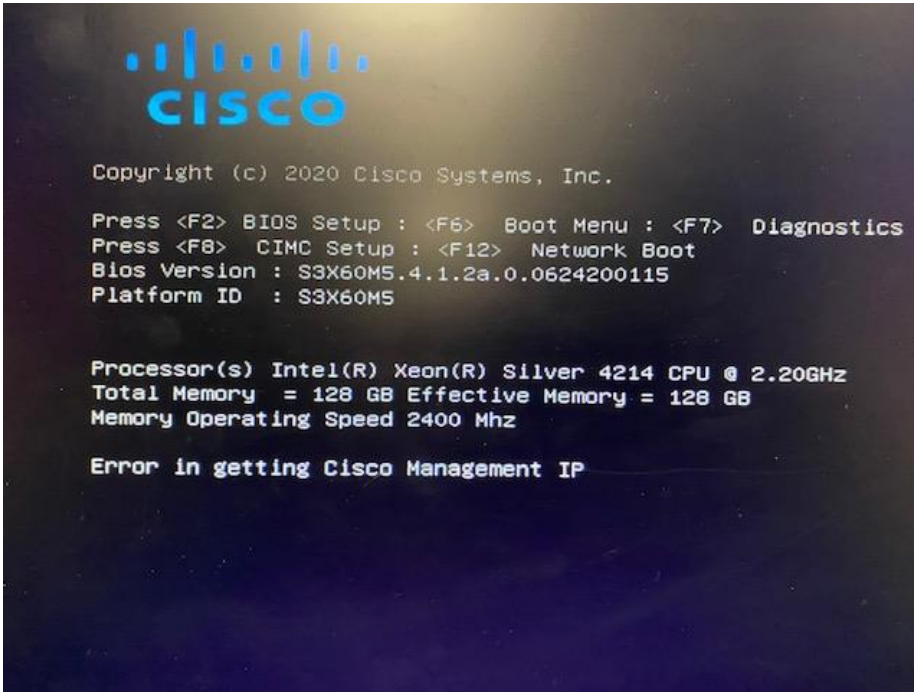
Note: The present setup has two server nodes in each Cisco UCS S3260 Storage Server Chassis. This configuration is specific to Cohesity File Services nodes.

Procedure 1. Discover the chassis using Cisco UCS Manager

Step 1. Connect a KVM cable (Cisco PID N20-BKVM) to the KVM connector on either server node at the rear of the system. For more details, please refer to [Cisco UCS S3260 Storage Server Chassis Installation and Service Guide](#).

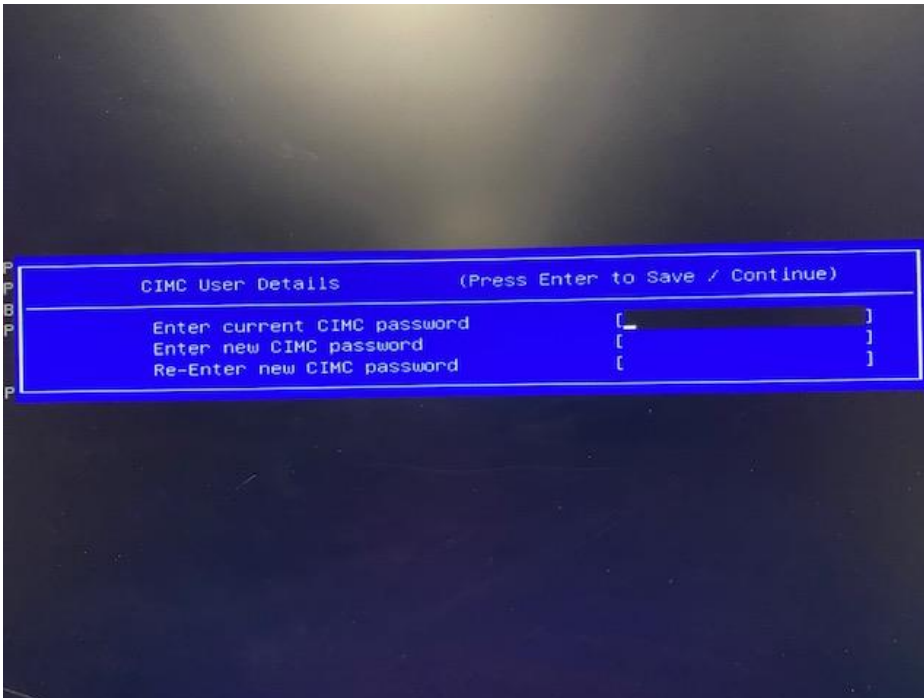
Step 2. During bootup, press F8 when prompted to open the Cisco IMC Configuration Utility.

Figure 26. CIMC Configuration - Server Boot



Step 3. Change the Password from default password='password'.

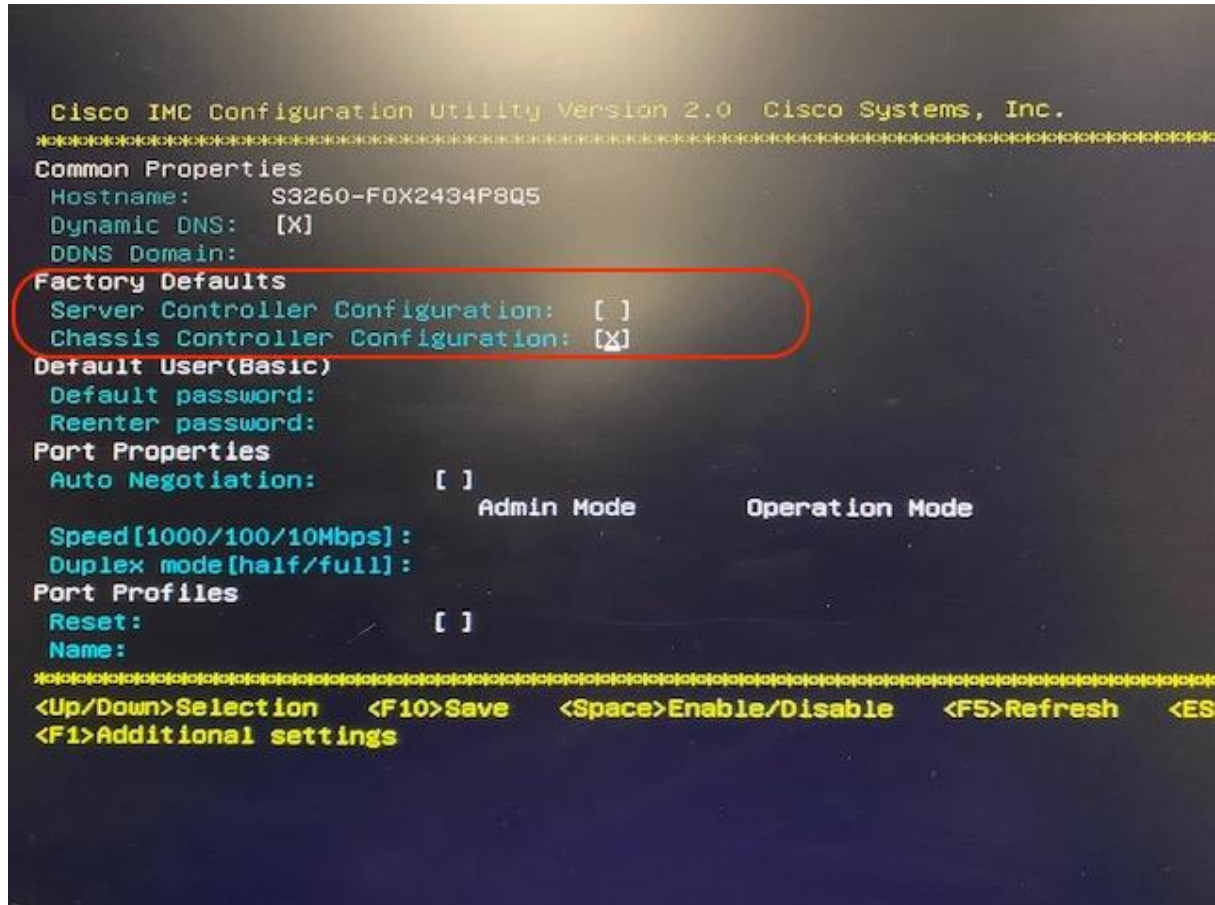
Figure 27. CIMC Configuration - Set Password



Step 4. Press F1 for Additional Settings.

Step 5. Select the Factory Default option for Chassis Controller Configuration.

Figure 28. CIMC Configuration - Reset Chassis Controller Configuration



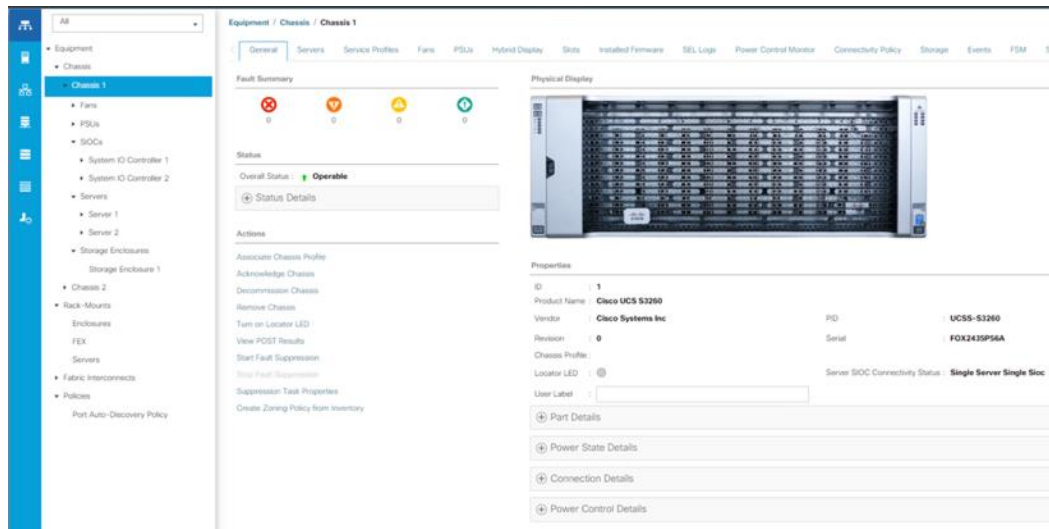
Step 6. The Chassis Management Controller resets, this initiates the discovery of the chassis through Cisco UCS Manager.

Procedure 2. View the chassis discovery status

Step 1. In Cisco UCS Manager, click the Equipment button, then click Equipment in the top of the navigation tree.

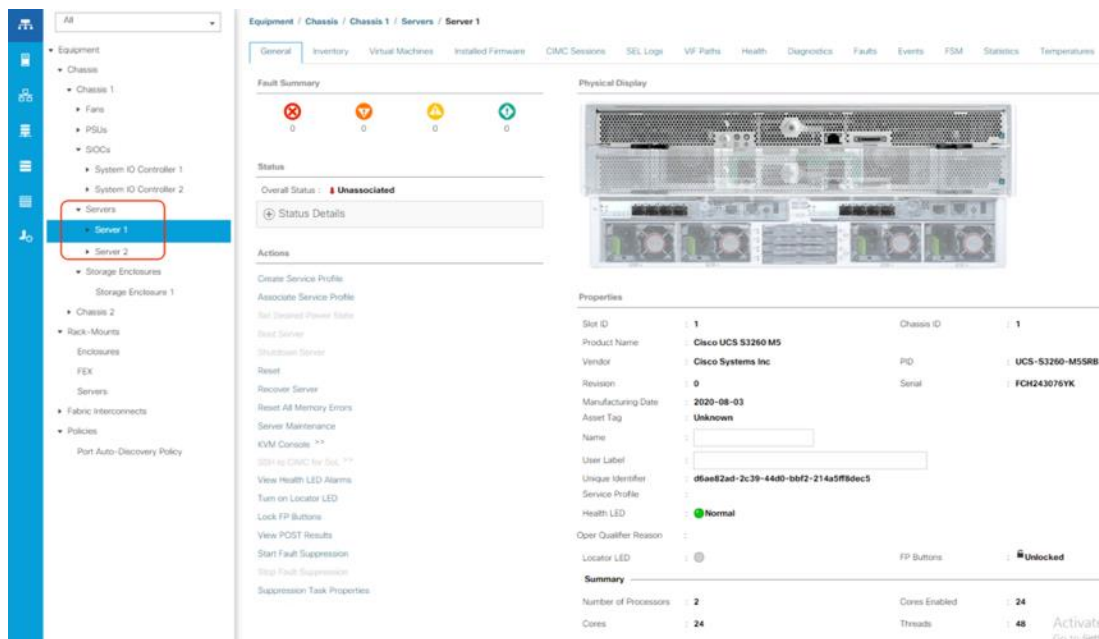
Step 2. Click Chassis > Chassis 1 and ensure that Chassis is discovered.

Figure 29. Chassis Discovery



Step 3. Under Chassis> Chassis <n> > Servers. Ensure two Server nodes on S3260 Chassis is discovered as Server1 and Server 2. In the current Cohesity deployment on S3260, the server node resides on Server slot 1 and slot 2 of the Chassis. Ensure both server nodes on each Chassis are discovered and is in unassociated state.

Figure 30. Chassis Discovery - Two Server Nodes



Step 4. In the tree hierarchy, underneath Equipment tab, select Chassis > Chassis {n} > Storage Enclosures > Storage Enclosure 1, ensure Disk 1-24 and Disk 29-52 are of type 'HDD' and Disk 25-28 and Disk 53-56 are of type SSD.

Step 5. Repeat steps 1 - 4 for other chassis which would be configured with Cohesity Cluster.

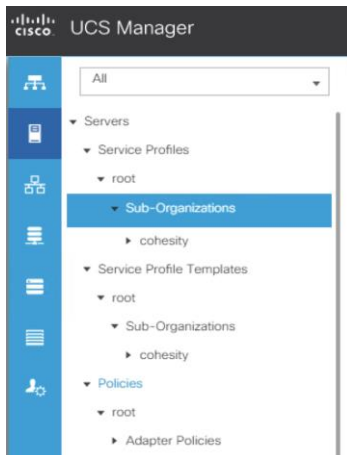
Cisco UCS Organization

Cisco UCS Manager sub-organizations are created underneath the root level of the Cisco UCS hierarchy, which are used to contain all policies, pools, templates, and service profiles used by the connected servers. Creating a sub-organization specifically for the Cohesity cluster prevents problems from overlapping settings across policies and pools. This arrangement also allows for organizational control using Role-Based Access Control (RBAC) and administrative locales within Cisco UCS Manager, if desired. In this way, control can be granted to administrators of only the Cohesity specific elements of the Cisco UCS domain, separate from control of root level elements or elements in other sub-organizations.

Procedure 1. Create a sub-organization for the Cohesity cluster

- Step 1.** In Cisco UCS Manager, click Servers.
- Step 2.** In the tree hierarchy, underneath Servers > Service Profiles, right-click root, then click Create Organization.
- Step 3.** Enter a name for the organization, for example “Cohesity” and optionally enter a description.
- Step 4.** Click OK.

Figure 31. Cisco UCS - Sub-Organization



Cisco UCS S3260 Chassis Policies

Procedure 1. Create Cisco UCS S3260 Chassis Firmware Packages

- Step 1.** In the Navigation pane, click the Chassis tab.
- Step 2.** In the Chassis tab, expand Policies > root > sub-Organizations > cohesity.
- Step 3.** Right-click Chassis Firmware Packages and select Create Chassis Firmware Packages.
- Step 4.** Enter cohesity_chs_fw as the Package name.
- Step 5.** From the Chassis Package drop-down list select 4.1(3b)C.
- Step 6.** Deselect the ‘Local Disk’ option.
- Step 7.** Click OK.

Figure 32. Chassis Firmware Package

Create Chassis Firmware Package

Name : cohesity_chs_fw

Description :

Chassis Package : 4.1(3b)C

Service Pack : <not set>

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

Excluded Components:

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

OK Cancel

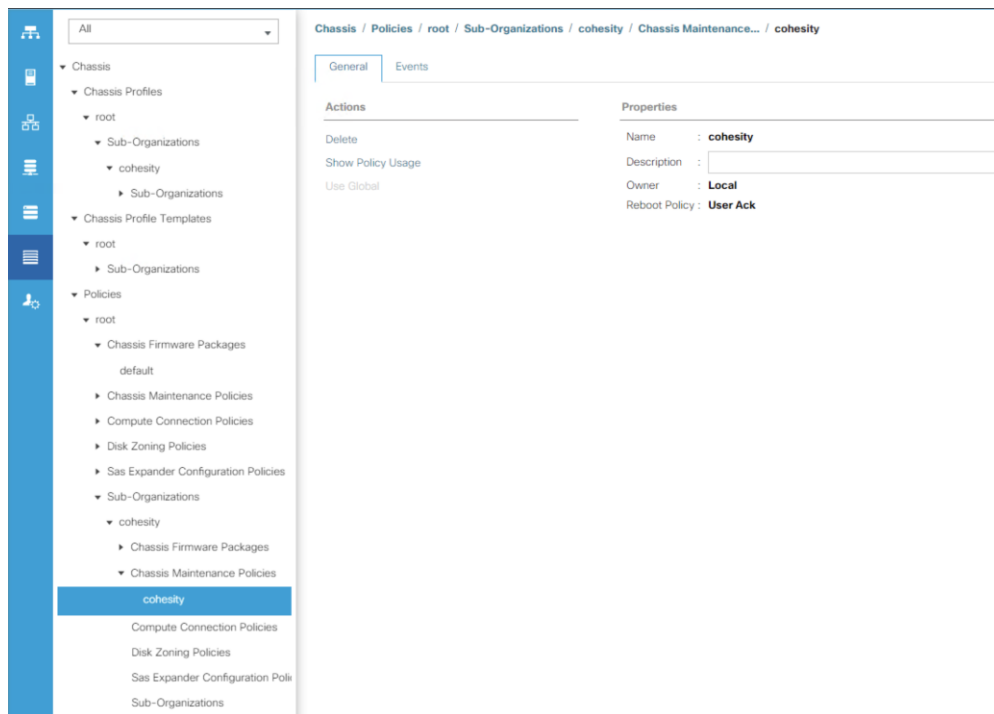
Chassis Maintenance Policies

Cisco UCS Maintenance Policies define the behavior of the attached blades, S3260 storage server and rack-mount servers when changes are made to the associated service profiles. The default Cisco UCS Maintenance Policy setting is “Immediate” meaning that any change to a service profile that requires a reboot of the chassis will result in an immediate reboot. The Cisco best practice is to use a Maintenance Policy set to “user-ack”, for example, the user must power cycle the chassis manually after the chassis profile association is complete or changes are made.

Procedure 2. Configure the Maintenance Policy

- Step 1.** In Cisco UCS Manager, click Chassis.
- Step 2.** In the tree hierarchy, underneath Policies > root > Sub-Organizations, click the carat next to the name of the sub-organization created for Cohesity to expand it.
- Step 3.** Right-click Maintenance Policies, then click Create Maintenance Policy.
- Step 4.** Enter a name for the policy, and optionally enter a description.
- Step 5.** Click the radio button for Reboot Policy: User Ack.
- Step 6.** Click OK.

Figure 33. Chassis Maintenance Policy



Disk Zoning Policy

You can assign disk drives to the server nodes using disk zoning. Disk zoning can be performed on the controllers in the same server or on the controllers on different servers.

Procedure 1. Create Disk Zoning Policy

Step 1. In the Navigation pane, click Chassis.

Step 2. Expand Policies > root > Sub-Organizations > Cohesity.

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

Step 4. For the Disk Zone Name, enter cohesity.

Step 5. In the Disk Zoning Information Area, click Add:

- For Ownership select Dedicated
- For Server select 1 (Disk 1-28 are assigned to node 1 of S3260 Storage server)
- For Controller select 1
- For Drive path select 1
- For Slot range select 1-28

Step 6. Click OK.

Create Disk Zoning Policy

Name : cohesity

Description :

Preserve Config :

Disk Zoning Information

+ - Y

Name

tempora

Add Slots to Policy

Ownership : Unassigned Dedicated Shared Chassis Global Hot Spare

Server : 1

Controller : 1

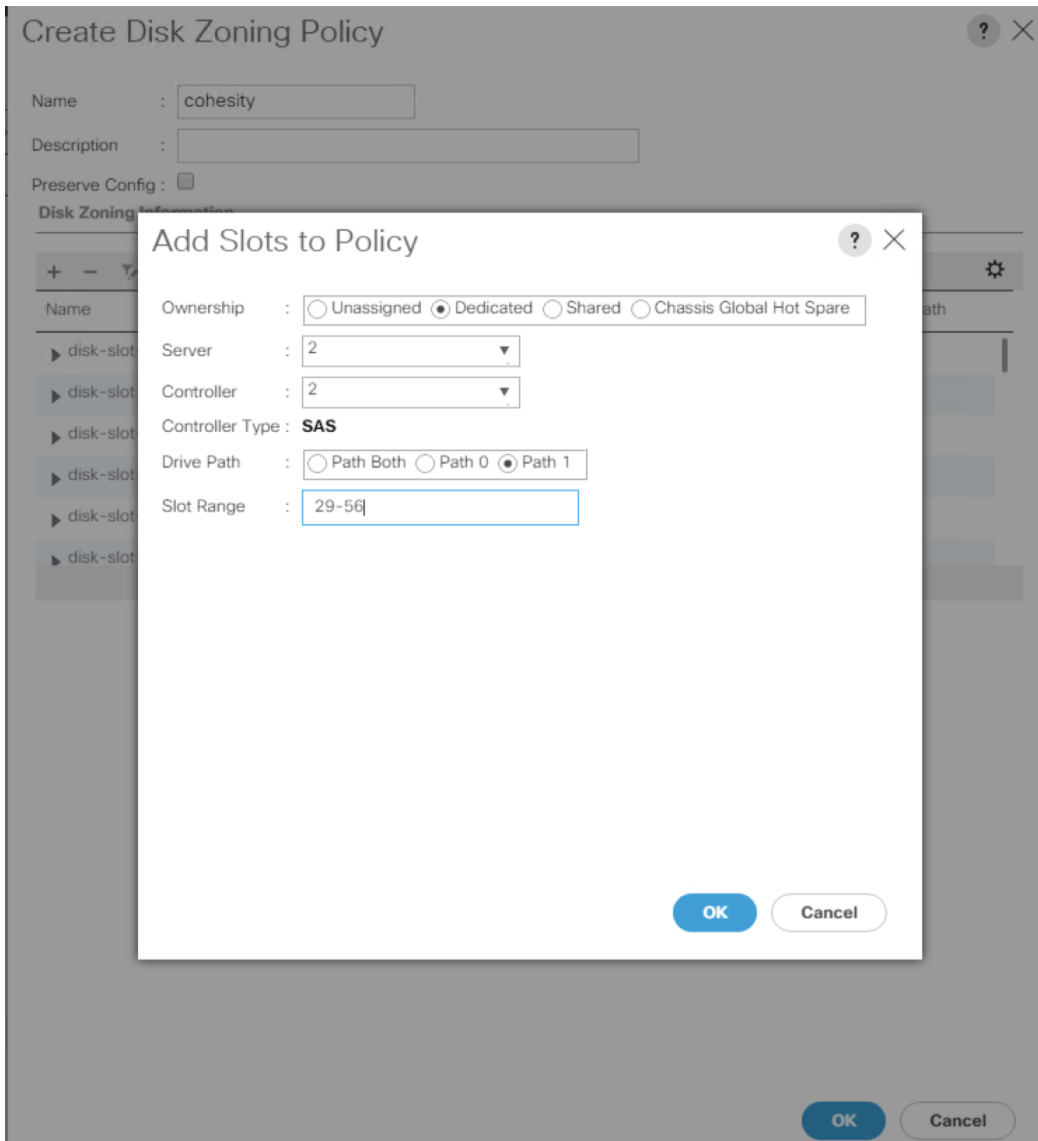
Controller Type : SAS

Drive Path : Path Both Path 0 Path 1

Slot Range : 1-28

OK Cancel

Step 7. Repeat step 5 and 6 and add Disk 29-56 and for Server select 2, Controller select 1, and Path 1 and Slot Range 29-56.



Step 8. Click OK to complete the Disk Zoning Configuration Policy. Disk Zoning policy is displayed below.

Figure 34. Disk Zoning Policy

The screenshot shows the configuration page for a Disk Zoning Policy named 'cohesity'. The breadcrumb path is 'Chassis / Policies / root / Sub-Organizations / cohesity / Disk Zoning Policies / cohesity'. The 'General' tab is active. On the left, there are 'Actions' such as 'Add Slots to Policy', 'Delete', 'Show Policy Usage', and 'Use Global'. The 'Properties' section shows the name 'cohesity' and a description field. Below this is a table titled 'Disks Zoned' with columns: Name, Slot Number, Ownership, Assigned to Server, Assigned to Controller, Controller Type, and Drive Path. The table contains four rows, with the second and third rows highlighted by a red box. The second row is 'server-1-controller-SAS...' and the third row is 'server-2-controller-SAS...'. At the bottom of the table are 'Add', 'Delete', and 'Modify' buttons.

Name	Slot Number	Ownership	Assigned to Server	Assigned to Controller	Controller Type	Drive Path
disk-slot-27	27	Dedicated				Path 1
disk-slot-28	28	Dedicated				Path 1
server-1-controller-SAS...			1	1	SAS	Path 1
disk-slot-29	29	Dedicated				Path 1
server-2-controller-SAS...			2	1	SAS	Path 1
disk-slot-30	30	Dedicated				Path 1

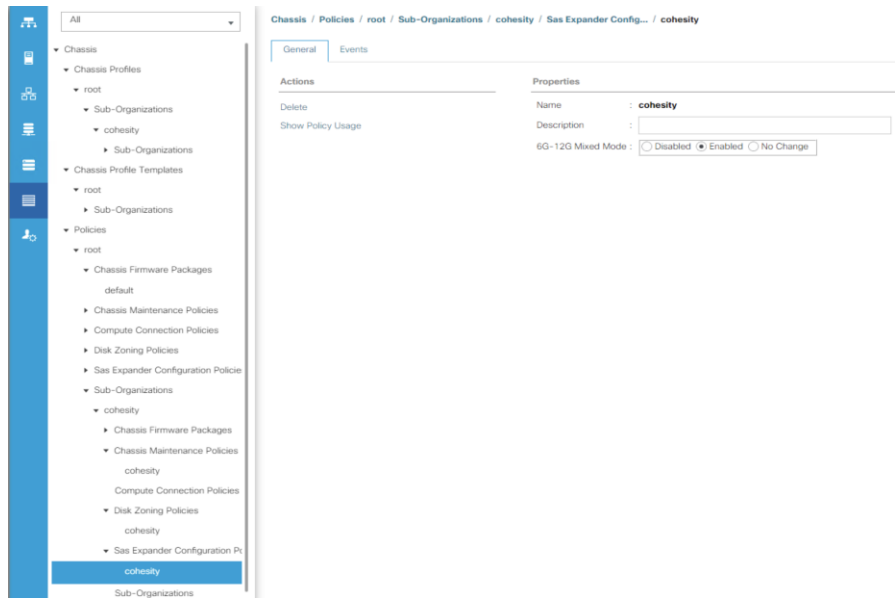
Note: The Disk Zoning policy defined in this guide is specific to Cohesity File Services nodes. This configuration has two server nodes in each Cisco UCS S3260 Storage Server Chassis. To configure disk zoning policy for Cohesity on Cisco UCS S3260 with single compute node Cohesity, please refer to [Cisco UCS S3260 Storage Servers with Cohesity DataPlatform](#)

Chassis Sas Expander Configuration Policy

Procedure 1. Create Sas Expander Configuration Policy

- Step 1.** In the Navigation pane, click Chassis.
- Step 2.** Expand Policies > root > Sub-Organizations > Cohesity.
- Step 3.** Right-click Sas Expander Configuration Policy and click Create.
- Step 4.** For the name, enter cohesity.
- Step 5.** For 6G-12G Mixed Mode select Enabled.
- Step 6.** Click OK.

Figure 35. Sas Expander Configuration



Cisco UCS LAN Policies

VLANS

Names and IDs for the required VLANs must be defined in the Cisco UCS configuration page prior to the Cohesity installation. The VLANs listed in Cisco UCS must already be present on the upstream network, and the Cisco UCS FIs do not participate in VLAN Trunk Protocol (VTP).

Procedure 1. Configure the VLAN(s) required for the installation

- Step 1.** In Cisco UCS Manager, click LAN.
- Step 2.** In the tree hierarchy, underneath LAN > LAN Cloud, right-click VLANs, then click Create VLANs.
- Step 3.** Enter a VLAN name which describes the VLAN purpose.
- Step 4.** Leave the Multicast Policy Name as <not set>.
- Step 5.** Choose the radio button for Common/Global.
- Step 6.** Enter the VLAN ID for this VLAN as defined in the upstream switches.
- Step 7.** Choose the radio button for Sharing Type: None.
- Step 8.** Click OK.

Table 21. VLANs Configurations

VLAN Name	VLAN ID	VLAN Purpose

VLAN Name	VLAN ID	VLAN Purpose
Default	1	Native VLAN
Cohesity-vlan	3171	Out-of-Band management interfaces, management interfaces and cohesity network
Public-vlan	149	Internet Access
Storage-vlan	3172	Access for NAS setup for NAS Tiering with cohesity
OOB-Mgmt	3171	Out-of-Band management interfaces

Figure 36. VLAN Configuration

The screenshot shows the network management interface. On the left is a navigation sidebar with a tree view including LAN, LAN Cloud, Fabric A, Fabric B, QoS System Class, LAN Pin Groups, Threshold Policies, VLAN Groups, and VLANs (selected). The main content area is titled 'LAN / LAN Cloud / VLANs' and contains a table of VLANs. Below the table are tabs for 'General', 'Org Permissions', 'VLAN Group Membership', 'Faults', and 'Events'. The 'General' tab is active, showing a 'Fault Summary' with four status icons (0 for each), 'Actions' for 'Modify VLAN Org Permissions' and 'Delete', and a 'Properties' section with the following details:

- Name: cohesity-vlan
- Native VLAN: No
- Network Type: Lan
- Locale: External
- Owner: Local
- Multicast Policy Name: <not set>
- Multicast Policy Instance: org-root/mc-policy-default
- Sharing Type: None Primary Isolated Community
- VLAN ID: 3171
- Fabric ID: Dual
- If Type: Virtual
- Transport Type: Ether

Note: This configuration utilizes three different VLANs, choice of VLANs is dependent on the customer network, some customers may choose a single VLAN for all traffic to cohesity cluster.

QoS System Classes

By default, Cohesity clusters do not utilize Quality of Service (QoS) policies in their service profiles, and instead place all network traffic into the default “Best-Effort” class. Notably, certain workloads may be deployed using QoS and a specific configuration for the Cisco UCS QoS System Classes is set during installation. Changes to the Cisco UCS QoS System Classes require a reboot of both Fabric Interconnects. For this reason, if a single UCS domain is intended to contain configuration with QoS System Class and Cohesity deployment, it is highly recommended to first deploy the configuration

with QoS System Class. This allows the correct QoS system classes to be set without interrupting service to an existing workload, afterwards Cohesity and other systems can be deployed without any additional impacts.

Create UUID Suffix Pool

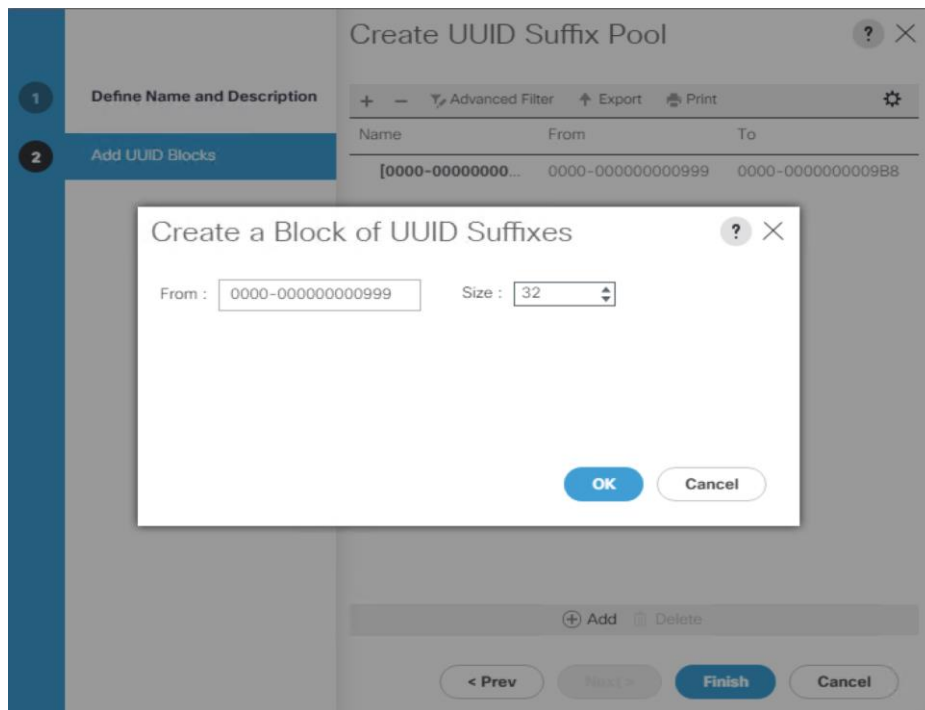
A UUID suffix pool is a collection of SMBIOS UUIDs that are available to be assigned to servers. The first number of digits that constitute the prefix of the UUID are fixed. The remaining digits, the UUID suffix, are variable. A UUID suffix pool ensures that these variable values are unique for each server associated with a service profile which uses that particular pool to avoid conflicts.

If you use UUID suffix pools in service profiles, you do not have to manually configure the UUID of the server associated with the service profile.

Procedure 2. Configure the necessary universally unique identifier (UUID) suffix pool for the Cisco UCS environment

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

Figure 37. UUID Suffix Pool



Step 13. Click OK.

Step 14. Click Finish.

Step 15. Click OK.

Management IP Address Pool

A Cisco UCS Management IP Address Pool must be populated with a block of IP addresses. These IP addresses are assigned to the Cisco Integrated Management Controller (CIMC) interface of the rack mount and blade servers that are managed in the Cisco UCS domain. The IP addresses are the communication endpoints for various functions, such as remote KVM, virtual media, Serial over LAN (SoL), and Intelligent Platform Management Interface (IPMI) for each rack mount or blade server. Therefore, a minimum of one IP address per physical server in the domain must be provided. The IP addresses are considered to be an “out-of-band” address, meaning that the communication pathway uses the Fabric Interconnects’ mgmt0 ports, which answer ARP requests for the management addresses. Because of this arrangement, the IP addresses in this pool must be in the same IP subnet as the IP addresses assigned to the Fabric Interconnects’ mgmt0 ports.

Procedure 3. Create the management IP address pool

Step 1. In Cisco UCS Manager, click LAN.

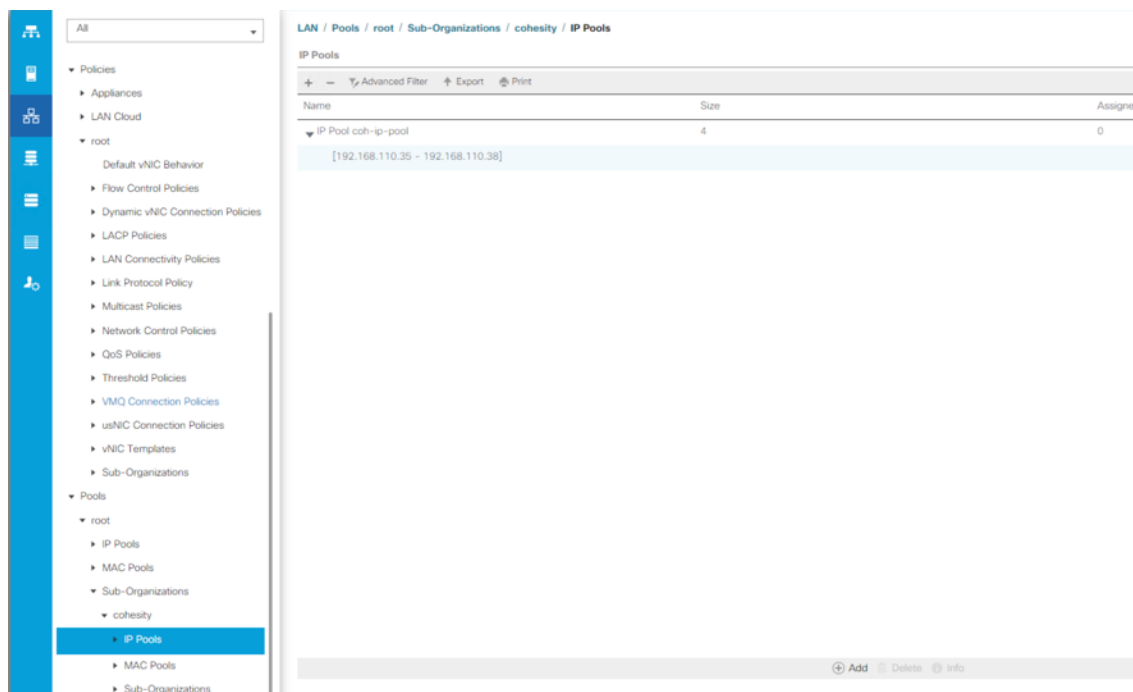
Step 2. In the tree hierarchy, underneath Pools > root > Sub-Organizations, click the carat next to the name of the sub-organization created for Cohesity to expand it.

Step 3. Right-click IP Pools, then click Create IP Pool.

Step 4. Enter a name for the IP address pool, such as “Cohesity”, and optionally enter a description.

- Step 5.** Click the radio button for Assignment Order: Sequential in order to apply the addresses to the servers in sequence. Choosing Default will result in a random assignment order.
- Step 6.** Click Next.
- Step 7.** Click Add near the bottom to add a block of IPv4 addresses.
- Step 8.** Enter the first IP address of the pool in the From: field.
- Step 9.** Enter the size of the address pool in the Size: field.
- Step 10.** Enter the correct values for the Subnet Mask, Default Gateway, and Primary and Secondary DNS servers.
- Step 11.** Click OK.
- Step 12.** Click Next.
- Step 13.** In most cases, a pool of IPv6 addresses is not necessary, click Finish.

Figure 38. Management IP Pool
Step 14.



MAC Address Pools

One of the core benefits of the Cisco UCS and Virtual Interface Card (VIC) technology is the assignment of the personality of the card through Cisco UCS Service Profiles. The number of virtual NIC (vNIC) interfaces, their VLAN associations, MAC addresses, QoS policies and more are all applied dynamically as part of the service profile association process. Media Access Control (MAC) addresses use 6 bytes of data as a unique address to identify the interface on the layer 2 network. All devices are assigned a unique MAC address, which is ultimately used for all data transmission and reception. The Cisco UCS and VIC technology picks a MAC address from a pool of addresses and assigns it to each vNIC defined in the service profile when that service profile is created.

Best practices mandate that MAC addresses used for Cisco UCS domains use 00:25:B5 as the first three bytes, which is one of the Organizationally Unique Identifiers (OUI) registered to Cisco Systems, Inc. The remaining 3 bytes can be manually set. The fourth byte (for example, 00:25:B5:xx) is often used to identify a specific UCS domain, meanwhile the fifth byte is often set to correlate to the Cisco UCS fabric and the vNIC placement order. Finally, the last byte is incremented upward from the starting value defined, according to the number of MAC addresses created in the pool. To avoid overlaps, when you define these values you must ensure that the MAC address pools are unique for each UCS domain installed in the same layer 2 network.

Cohesity servers running inside the Cisco UCS domain require two vNICs, one in the A side fabric, and one in the B side fabric. To make identification and troubleshooting easier, it is recommended to create two MAC address pools; one for the A side fabric vNICs, and a second for the B side fabric vNICs, each with a unique identifier in the fifth byte.

Procedure 4. Create the MAC address pools

- Step 1.** In Cisco UCS Manager, click LAN.
- Step 2.** In the tree hierarchy, underneath Pools > root > Sub-Organizations, click the carat next to the name of the sub-organization created for Cohesity to expand it.
- Step 3.** Right-click MAC Pools, then click Create MAC Pool.
- Step 4.** Enter a name for the MAC address pool, such as “cohesity-mac-a”, and optionally enter a description.
- Step 5.** Click the radio button for Assignment Order: Sequential in order to apply the addresses to the servers in sequence. Choosing Default will result in a random assignment order.
- Step 6.** Click Next.
- Step 7.** Click Add to add a block of MAC addresses.
- Step 8.** Modify the values in the 4th byte and 5th byte as necessary in the First MAC Address field. For example, change the field to read “00:25:B5:DA:00:00”
- Step 9.** Enter the size of the address pool in the Size: field.
- Step 10.** Click OK.
- Step 11.** Click Finish.
- Step 12.** Repeat steps 1-11 to create any additional MAC address pools required, for example a second pool for the B side vNICs.

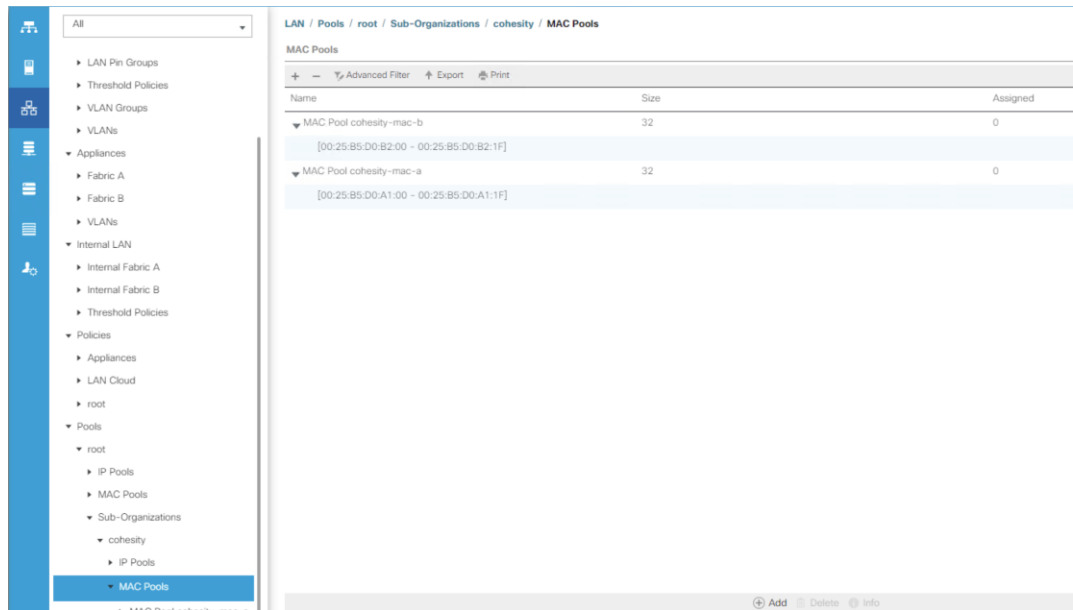
[Table 22](#) lists an example of MAC Address Pools configured for Cohesity and their association to the vNIC templates created afterward:

Table 22. MAC Pool

Name	Block Start	Size	Assignment Order	Used by vNIC Template
cohesity-mac-a	00:25:B5:DA:00:00	32	Sequential	cohesity-vnic-a

Name	Block Start	Size	Assignment Order	Used by vNIC Template
cohesity-mac-b	00:25:B5:DB:00:00	32	Sequential	cohesity-vnic-b

Figure 39. MAC Address Pools



Network Control Policies

Cisco UCS Network Control Policies control various aspects of the behavior of vNICs defined in the Cisco UCS Service Profiles. Settings controlled include enablement of Cisco Discovery Protocol (CDP), MAC address registration, MAC address forging, and the action taken on the vNIC status if the Cisco UCS network uplinks are failed. Of these settings, the most important for the Cohesity Helios is the setting to mark the vNICs as Link Down if there is a failure of all the uplinks from that Fabric Interconnect. This helps ensure that the OS level bonding in the Cohesity nodes will correctly fail over to the other fabric if all uplinks from one FI are lost.

Procedure 5. Configure the Network Control Policy

- Step 1.** In Cisco UCS Manager, click LAN.
- Step 2.** In the tree hierarchy, underneath Policies > root > Sub-Organizations, click the carat next to the name of the sub-organization created for Cohesity to expand it.
- Step 3.** Right-click Network Control Policies, then click Create Network Control Policy.
- Step 4.** Enter a name for the policy, and optionally enter a description.
- Step 5.** Click the radio button to set CDP: Enabled.
- Step 6.** Ensure the setting for Action on Uplink Fail is set to Link Down.

Step 7. All other settings can be left at their defaults.

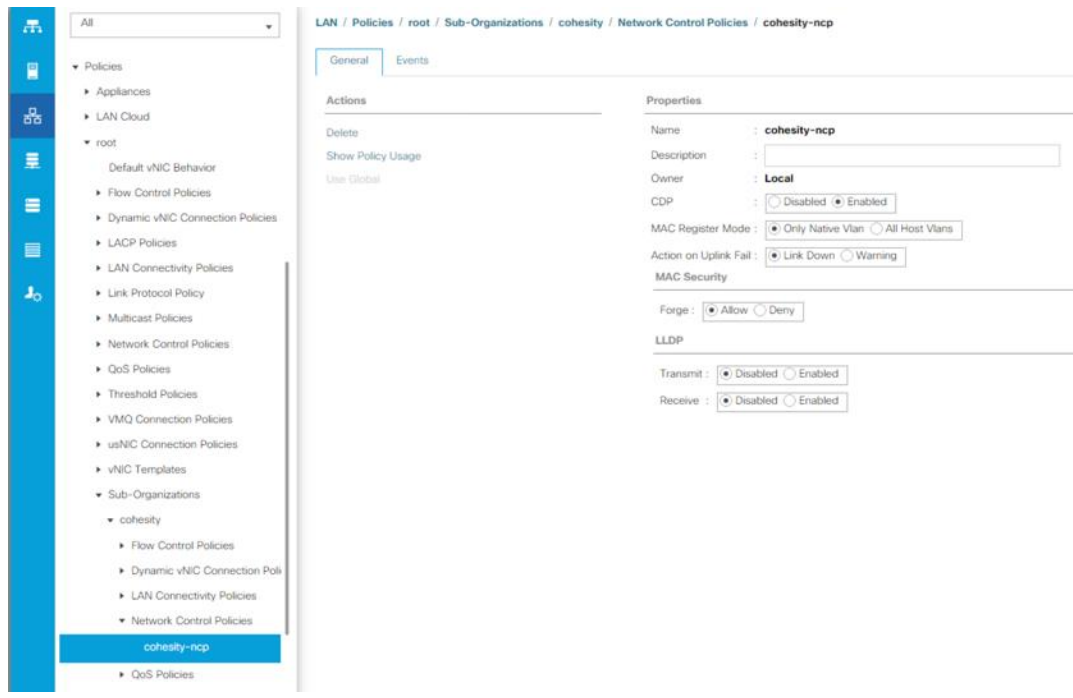
Step 8. Click OK.

[Table 23](#) lists the Network Control Policy configured for Cohesity, and the assignment to the vNIC templates created:

Table 23. Network Control Policy

Name	CDP	MAC Register Mode	Action on Uplink Fail	MAC Security	Used by vNIC Template
cohesity	Enabled	Only Native VLAN	Link-down	Forged: Allow	cohesity-vnic-a cohesity-vnic-b

Figure 40. Network Control Policy



vNIC Templates

Cisco UCS Manager has a feature to configure vNIC templates, which can be used to simplify and speed up configuration efforts. vNIC templates are referenced in service profiles and LAN connectivity policies, versus configuring the same vNICs individually in each service profile, or service profile template. vNIC templates contain all the configuration elements that make up a vNIC, including VLAN assignment, MAC address pool selection, fabric A or B assignment, fabric failover, MTU, QoS policy, Network Control Policy, and more. Templates are created as either initial templates or updating templates. Updating templates retain a link between the parent template and the child object, therefore when changes are made to the template, the changes are propagated to all remaining linked child objects. An additional feature named “vNIC Redundancy” allows vNICs to be configured in pairs, so that

the settings of one vNIC template, designated as a primary template, will automatically be applied to a configured secondary template. For all Cohesity vNIC templates, the “A” side vNIC template is configured as a primary template, and the related “B” side vNIC template is a secondary. In each case, the only configuration difference between the two templates is which fabric they are configured to connect through.

Procedure 6. Create vNIC templates

- Step 1.** In Cisco UCS Manager, click LAN.
- Step 2.** In the tree hierarchy, underneath Policies > root > Sub-Organizations, click the carat next to the name of the sub-organization created for Cohesity to expand it.
- Step 3.** Right-click vNIC Templates, then click Create vNIC Template.
- Step 4.** Enter a name for the template, and optionally enter a description.
- Step 5.** Click the radio button for Fabric ID: Fabric A and ensure the checkbox for Enable Failover is left unchecked.
- Step 6.** Click the radio button for Redundancy Type: Primary Template. Leave the Peer Redundancy Template as <not set>.
- Step 7.** Leave the Target checkbox for Adapter as checked, and for VM as unchecked.
- Step 8.** Click the radio button for Template Type: Updating Template.
- Step 9.** In the list of VLANs, click the checkbox next to the VLAN which was created for Cohesity cluster traffic in order to select it, and click the radio button on the right for Native VLAN in order to pass the traffic without VLAN ID tags.
- Step 10.** Scroll down in the window, ensure that the CDN source is left as vNIC Name, and the MTU is set to 1500.
- Step 11.** Choose the MAC Address Pool created earlier for the A side fabric for this vNIC.
- Step 12.** Choose the Network Control Policy created earlier for this Cohesity sub-organization.
- Step 13.** Click OK.

Figure 41. vNIC Template A

Create vNIC Template ? X

Name :

Description :

Fabric ID : Fabric A Fabric B Enable Failover

Redundancy

Redundancy Type : No Redundancy Primary Template Secondary Template

Peer Redundancy Template :

Target

Adapter

VM

Warning

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

Template Type : Initial Template Updating Template

VLANs | VLAN Groups

Advanced Filter | Export | Print ⚙

Select	Name	Native VLAN	VLAN ID
<input checked="" type="checkbox"/>	149	<input type="radio"/>	149
<input checked="" type="checkbox"/>	cohesity-vlan	<input checked="" type="radio"/>	3171
<input type="checkbox"/>	default	<input type="radio"/>	1
<input checked="" type="checkbox"/>	stroage-vlan	<input type="radio"/>	3172

Create VLAN

CDN Source : vNIC Name User Defined

MTU :

MAC Pool :

QoS Policy :

Network Control Policy :

Pin Group :

Stats Threshold Policy :

Connection Policies

Dynamic vNIC usNIC VMQ

usNIC Connection Policy :

OK
Cancel

Step 14. Repeat steps 1-13, but doing so for the B side vNIC template, which requires the following changes:

- Step 15.** Give the template a unique name for the B side template.
- Step 16.** Choose Fabric B for the Fabric ID.
- Step 17.** Choose Secondary Template for the Redundancy Type.
- Step 18.** Choose the vNIC template just created earlier as the Peer Redundancy Template.
- Step 19.** Choose the MAC Address Pool created earlier for the B side fabric.

Figure 42. vNIC Template B

Create vNIC Template
?
×

Name :

Description :

Fabric ID : Fabric A Fabric B Enable Failover

Redundancy

Redundancy Type : No Redundancy Primary Template Secondary Template

Peer Redundancy Template :

Target

Adapter

VM

Warning

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

Template Type : Initial Template Updating Template

VLANs | VLAN Groups

Advanced Filter | Export | Print

Select	Name	Native VLAN	VLAN ID
<input checked="" type="checkbox"/>	149	<input type="radio"/>	149
<input checked="" type="checkbox"/>	cohesity-vlan	<input checked="" type="radio"/>	3171
<input type="checkbox"/>	default	<input type="radio"/>	1
<input checked="" type="checkbox"/>	stroage-vlan	<input type="radio"/>	3172

Create VLAN

CDN Source : vNIC Name User Defined

MTU : 1500

MAC Pool : cohesity-mac-b(32/32) ▼

QoS Policy : <not set> ▼

Network Control Policy : cohesity-ncp ▼

Pin Group : <not set> ▼

Stats Threshold Policy : default ▼

Connection Policies

Dynamic vNIC usNIC VMQ

usNIC Connection Policy : <not set> ▼

OK Cancel

The following tables detail the initial settings in each of the vNIC templates created for the Cohesity Helios platform:

Table 24. vNIC Template cohesity-vnic-a

vNIC Template Name	vnic-cohesity-a	
Setting	Value	
Fabric ID	A	
Fabric Failover	Disabled	
Target	Adapter	
Type	Updating Template	
MTU	1500	
MAC Pool	cohesity-mac-a	
QoS Policy	<none>	
Network Control Policy	Cohesity	
VLANs	<<cohesity-vlan>>	Native: Yes

Table 25. vNIC Template cohesity-vnic-b

vNIC Template Name	vnic-cohesity-b	
--------------------	-----------------	--

vNIC Template Name	vnic-cohesity-b	
Setting	Value	
Fabric ID	B	
Fabric Failover	Disabled	
Target	Adapter	
Type	Updating Template	
MTU	1500	
MAC Pool	cohesity-mac-b	
QoS Policy	<none>	
Network Control Policy	Cohesity	
VLANs	<<cohesity-vlan>>	Native: Yes

LAN Connectivity Policies

Cisco UCS Manager has a feature for LAN Connectivity Policies, which aggregates all of the vNICs or vNIC templates desired for a service profile configuration into a single policy definition. This simplifies configuration efforts by defining a collection of vNICs or vNIC templates once and using that policy in the service profiles or service profile templates.

Procedure 7. Create the LAN Connectivity Policy

- Step 1.** In Cisco UCS Manager, click LAN.
- Step 2.** In the tree hierarchy, underneath Policies > root > Sub-Organizations, click the carat next to the name of the sub-organization created for Cohesity to expand it.
- Step 3.** Right-click LAN Connectivity Policies, then click Create LAN Connectivity Policy.
- Step 4.** Enter a name for the policy, and optionally enter a description.
- Step 5.** Click Add near the bottom to add a vNIC.
- Step 6.** Enter a name for the vNIC being added, for example vNIC0.
- Step 7.** Click the Use vNIC Template checkbox.
- Step 8.** In the vNIC Template drop-down box, choose the A side vNIC template created earlier.
- Step 9.** Click the Redundancy Pair checkbox.
- Step 10.** In the Peer Name field, enter a name for the redundant vNIC, for example vNIC1.

- Step 11.** In the Adapter Policy drop-down box, choose the Linux policy.
- Step 12.** Click OK.
- Step 13.** Click OK.

The LAN Connectivity Policy is shown below:

Figure 43. Lan Connectivity

Create LAN Connectivity Policy ? X

Name :

Description :

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

Name	MAC Address	Native VLAN
vNIC vNIC1	Derived	
vNIC vNIC0	Derived	

Delete + Add Modify

+ Add iSCSI vNICs

Create vNIC ? X

Name :

Use vNIC Template :

Redundancy Pair : Peer Name :

vNIC Template : Create vNIC Template

Adapter Performance Profile

Adapter Policy : Create Ethernet Adapter Policy

[Table 26](#) lists the LAN Connectivity Policy configured for Cohesity.

Table 26. LAN Connectivity Policy

Policy Name	Use vNIC Template	vNIC Name	vNIC Template Used	Adapter Policy
Cohesity	Yes	vNIC0	cohesity-vnic-a	Linux

Cisco UCS Server Policies

BIOS Policies

Cisco M5 generation servers no longer use pre-defined BIOS setting defaults derived from Cisco UCS Manager, instead the servers have default BIOS tokens set from the factory. The current default token settings can be viewed at [Cisco UCS Server BIOS Tokens, Release 4.0](#)

A BIOS policy must be created to modify the setting of M5 generation servers to enable optimal server performance and Serial over LAN communication, be used during troubleshooting efforts.

For more information on M5 server BIOS settings, go to: [Performance Tuning Guide for Cisco UCS M5 Servers White Paper](#)

Procedure 8. Configure the BIOS policy

Step 1. In Cisco UCS Manager, click Servers.

Step 2. In the tree hierarchy, underneath Policies > root > Sub-Organizations, click the carat next to the name of the sub-organization created for Cohesity to expand it.

Step 3. Right-click BIOS Policies, then click Create BIOS Policy.

Step 4. Enter a name for the policy, and optionally enter a description.

Step 5. Click OK.

Step 6. Click the name of the BIOS Policy which was just created.

Step 7. In the right-hand pane of the Cisco UCS Manager screen, click the Advanced tab.

Step 8. Click the Processor tab:

- Change CPU Performance to Enterprise
- Energy Efficient Turbo as Disabled
- Package C State Limit as C0 and C1 state
- Processor C State as Disabled
- Processor EPP Profile as Performance
- Workload Configuration as IO Sensitive

Step 9. Click LOM and PCIe Slots tab:

- SBMezz1 OptionROM as Disabled
- SBMezz2 OptionROM as Disabled

Step 10. Click the Serial Port tab:

- Change the Serial Port A enable Value to Enabled in the drop-down list.

- Step 11.** Click the Server Management tab at the top of the pane.
- Step 12.** Change the Console Redirection BIOS setting Value to Serial Port A in the drop-down list.
- Step 13.** Click Save Changes.

[Table 27](#) lists the BIOS Policy configured for Cohesity.

Table 27. BIOS Policy

Policy Name	BIOS Tab	BIOS Sub-Tab	BIOS Setting	Value
Cohesity-BIOS	Advanced	Processor	CPU Performance	Enterprise
			Energy Efficient Turbo	Disabled
			Package C State Limit	C0 C1 State
			Processor C State	Disabled
			Processor EPP Profile	Performance
			Workload Configuration	IO Sensitive
	Advanced	Serial Port	Serial Port A enable	Enabled
	Advanced	LOM and PCIe Slots	SBMezz1 OptionROM	Disabled
			SBMezz2 OptionROM	Disabled
	Server Management			Console Redirection

Boot Policies

Cisco UCS Boot Policies define the boot devices used by blade and rack-mount servers, and the order that they are attempted to boot from. Cisco UCS S3260 storage server which runs the Cohesity Helios have their Linux operating system installed to a pair of Rear Boot SSDs, therefore they require a unique boot policy defining that the servers should boot from that location. In addition, a local CD/DVD boot option is included to allow the server to search for the installation ISO media during the Cohesity installation steps.

Procedure 9. Configure the Boot Policy

Step 1. In Cisco UCS Manager, click Servers.

Step 2. In the tree hierarchy, underneath Policies > root > Sub-Organizations, click the carat next to the name of the sub-organization created for Cohesity to expand it.

Step 3. Right-click Boot Policies, then click Create Boot Policy.

Step 4. Enter a name for the template, and optionally enter a description.

Step 5. Leave all settings at their defaults, ensuring the Boot Mode option is set to 'Legacy'.

Step 6. In the Boot Order area, click the + symbol next to Local Devices to expand the list.

Step 7. Click the blue link for "Add CD/DVD", you will see this selection added to the boot order.

Step 8. Click the blue link for "Add Local Disk."

Step 9. In the pop-up window, click the radio button for Any, then click OK.

Step 10. Click OK.

The Cohesity Boot Policy is shown below:

Figure 44. Cohesity boot policy

Servers / Policies / root / Sub-Organizations / cohesity / Boot Policies / Boot Policy cohesity-bo...

General Events

Actions

Delete

Show Policy Usage

Use Global

Properties

Name : cohesity-boot

Description :

Owner : Local

Reboot on Boot Order Change :

Enforce vNIC/vHBA/iSCSI Name :

Boot Mode : Legacy Uefi

Warning

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

Local Devices

CIMC Mounted vMedia

vNICs

vHBAs

iSCSI vNICs

EFI Shell

Boot Order

Name	Order	vNIC/vHBA/iS...	Type	LUN Name	WWN
CD/DVD	1				
Local Disk	2				

Move Up Move Down Del

See Link Boot Parameters

Host Firmware Packages

Cisco UCS Host Firmware Packages represent one of the most powerful features of the Cisco UCS platform; the ability to control the firmware revision of all the managed blades and rack-mount servers through a policy specifications in the service profile. Host Firmware Packages are defined and referenced in the service profiles. Once a service profile is associated to a server, the firmware of all the components defined in the Host Firmware Package are automatically upgraded or downgraded to match the

package. A Host Firmware Package is created for the Cohesity nodes, which uses the simple package definition method, applying firmware revisions to all components that matches a specific Cisco UCS firmware bundle, versus defining the firmware revisions part by part.

Procedure 10. Configure the Host Firmware Package

- Step 1.** In Cisco UCS Manager, click Servers.
- Step 2.** In the tree hierarchy, underneath Policies > root > Sub-Organizations, click the carat next to the name of the sub-organization created for Cohesity to expand it.
- Step 3.** Right-click Host Firmware Packages, then click Create Host Firmware Package.
- Step 4.** Enter a name for the package, and optionally enter a description.
- Step 5.** Click the radio button for Simple package selection.
- Step 6.** In the Blade Package and Rack Package drop-down lists, choose the package version that matches the desired firmware version. In most cases, the version chosen would match the currently running Cisco UCS Manager and Fabric Interconnect versions, for example, 4.1(3b)B, and 4.1(3b)C.
- Step 7.** Choose a Service Pack revision if applicable.
- Step 8.** Click OK.

The Host Firmware Package used for Cohesity is shown below:

Figure 45. Cohesity server firmware policy

Create Host Firmware Package

Name : cohesity-huu

Description :

How would you like to configure the Host Firmware Package?

Simple Advanced

Blade Package : 4.1(3b)B

Rack Package : 4.1(3b)C

Service Pack : <not set>

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

Excluded Components:

- Adapter
- BIOS
- Board Controller
- CIMC
- FC Adapters
- Flex Flash Controller
- GPUs
- HBA Option ROM
- Host NIC
- Host NIC Option ROM
- Local Disk
- NVME Mswitch Firmware
- PSU
- Red Switch Firmware

OK Cancel

Local Disk Configuration Policies

Cisco UCS Local Disk Configuration Policies are used to define the configuration of disks installed locally within each blade or rack-mount server, most often to configure Redundant Array of Independent/Inexpensive Disks (RAID levels) when multiple disks are present for data protection. Since Cohesity converged nodes providing storage resources utilize software defined storage, the nodes do not require a local disk configuration to be set. Therefore, a simple policy which allows any local disk configuration is all that is required.

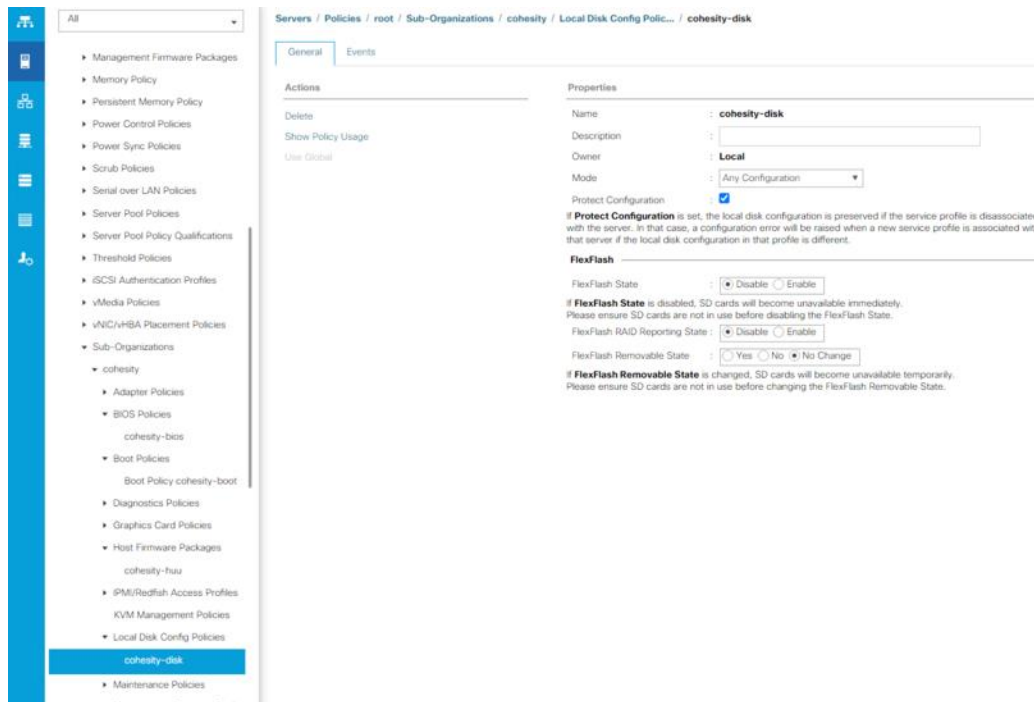
Procedure 11. Configure the Local Disk Configuration Policy

- Step 1.** In Cisco UCS Manager, click Servers.
- Step 2.** In the tree hierarchy, underneath Policies > root > Sub-Organizations, click the carat next to the name of the sub-organization created for Cohesity to expand it.
- Step 3.** Right-click Local Disk Config Policies, then click Create Local Disk Configuration Policy.
- Step 4.** Enter a name for the policy, and optionally enter a description.
- Step 5.** Leave all options at their default settings, ensuring the Mode drop-down list is set to “Any Configuration”.

Step 6. Click OK.

The Local Disk Configuration Policies configured for cohesity is shown below:

Figure 46. Cohesity local disk configuration policy



Maintenance Policies

Cisco UCS Maintenance Policies define the behavior of the attached blades and rack-mount servers when changes are made to the associated service profiles. The default Cisco UCS Maintenance Policy setting is “Immediate” meaning that any change to a service profile that requires a reboot of the physical server will result in an immediate reboot of that server. The Cisco best practice is to use a Maintenance Policy set to “user-ack”, which requires a secondary acknowledgement by a user with the appropriate rights within Cisco UCS Manager, before the server is rebooted to apply the changes. In addition, the On Next Boot setting is enabled, which will automatically apply changes the next time the server is rebooted, without any secondary acknowledgement.

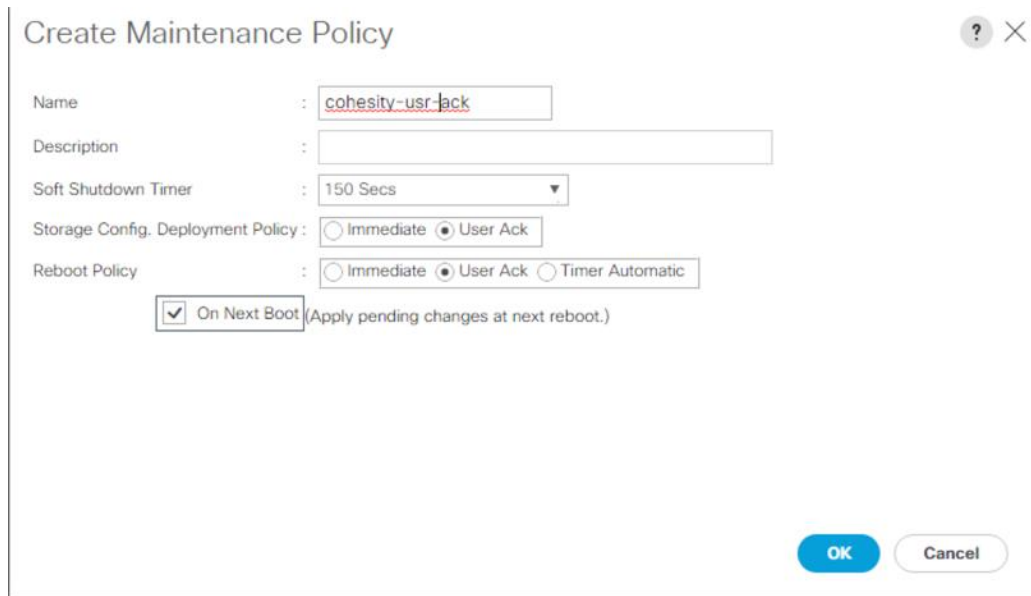
Procedure 12. Configure the Maintenance Policy

- Step 1.** In Cisco UCS Manager, click Servers.
- Step 2.** In the tree hierarchy, underneath Policies > root > Sub-Organizations, click the carat next to the name of the sub-organization created for Cohesity to expand it.
- Step 3.** Right-click Maintenance Policies, then click Create Maintenance Policy.
- Step 4.** Enter a name for the policy, and optionally enter a description.
- Step 5.** Click the radio button for Reboot Policy: User Ack.
- Step 6.** Check the checkbox for On Next Boot.

Step 7. Click OK.

The Maintenance Policy configured for Cohesity is shown below:

Figure 47. Cohesity server maintenance policy



Create Maintenance Policy

Name : cohesity-usr-jack

Description :

Soft Shutdown Timer : 150 Secs

Storage Config. Deployment Policy : Immediate User Ack

Reboot Policy : Immediate User Ack Timer Automatic

On Next Boot (Apply pending changes at next reboot.)

OK Cancel

Serial over LAN Policies

Cisco UCS Serial over LAN (SoL) Policies enable console output which is sent to the serial port of the server, to be accessible through the LAN. For many Linux based operating systems, the local serial port can be configured as a local console, where users can watch the system boot, and communicate with the system command prompt interactively. Since many servers do not have physical serial ports, and often administrators are working remotely, the ability to send and receive that traffic through the LAN is very helpful. Interaction with SoL can be initiated by connecting to the CIMC IP address configured by UCS Manager using SSH and entering valid Cisco UCS manager credentials.

Procedure 13. Configure the Serial Over LAN Policy

Step 1. In Cisco UCS Manager, click Servers.

Step 2. In the tree hierarchy, underneath Policies > root > Sub-Organizations, click the carat next to the name of the sub-organization created for Cohesity to expand it.

Step 3. Right-click Serial Over LAN Policies, then click Create Serial Over LAN Policy.

Step 4. Enter a name for the policy, and optionally enter a description.

Step 5. Select the radio button for Serial Over Lan State: Enable

Step 6. Select 115200 from the Speed drop-down list.

Step 7. Click OK.

The SoL Policy configured for Cohesity is shown below:

Figure 48. Cohesity serial over lan policy

Create Serial over LAN Policy

Name : cohesity-sol

Description :

Serial over LAN State : Disable Enable

Speed : 115200

OK Cancel

IPMI Access Profile

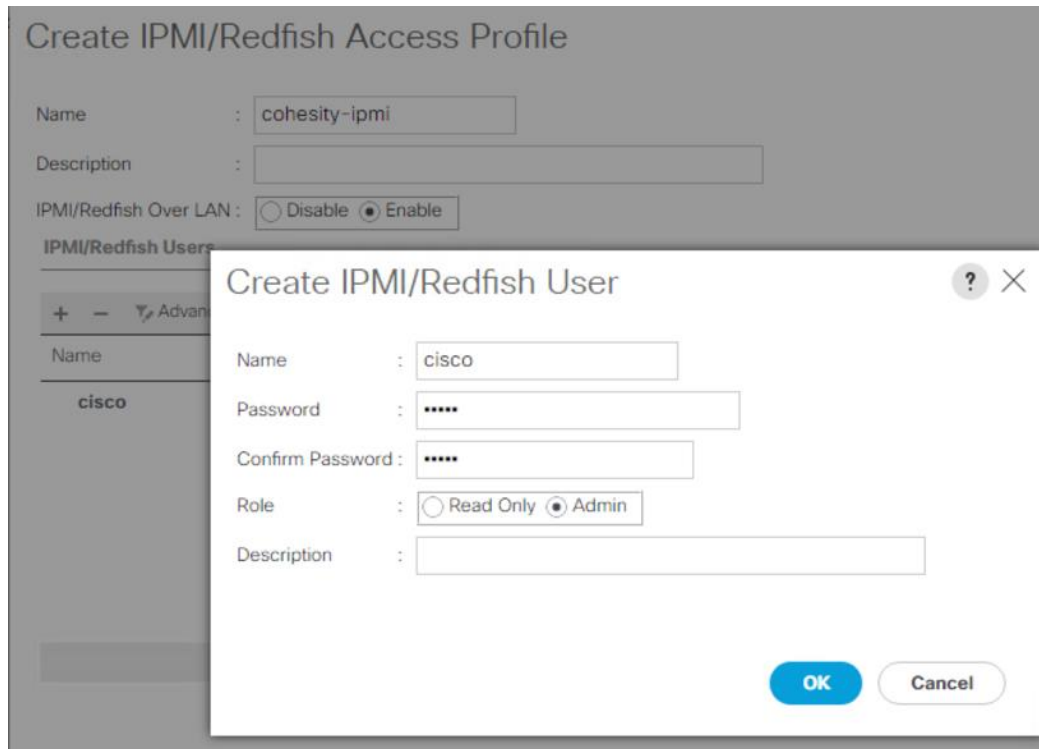
Cisco UCS Intelligent Platform Management Interface (IPMI) Policies allow for remote interactions with physical hardware resources through the LAN, such as querying power states or forcing servers to power on or off. The Cohesity Helios Platform requires IPMI access to each node and asks for the IPMI addresses and credentials during the installation. Consequently, an IPMI policy is required to enable the functionality through the CIMC interfaces, and to define the username and password which has access to the IPMI commands.

Procedure 14. Configure the IPMI Policy

- Step 1.** In Cisco UCS Manager, click Servers.
- Step 2.** In the tree hierarchy, underneath Policies > root > Sub-Organizations, click the carat next to the name of the sub-organization created for Cohesity to expand it.
- Step 3.** Right-click IPMI Access Profiles, then click Create IPMI Access Profile.
- Step 4.** Enter a name for the policy, and optionally enter a description.
- Step 5.** Click the radio button for IPMI Over LAN: Enable.
- Step 6.** Click Add to create a user.
- Step 7.** Enter the username.
- Step 8.** Enter and confirm the desired password.
- Step 9.** Click the radio button for Role: Admin.
- Step 10.** Click OK.
- Step 11.** Click OK.

The IPMI configured for Cohesity Helios Platform is shown below:

Figure 49. Cohesity ipmi policy



Cisco UCS Chassis Profile Templates

With a chassis profile template, you can quickly create several chassis profiles with the same basic parameters, such as the maintenance policy and the disk zoning policy.

For example, if you need several chassis profiles with similar values, you can create a chassis profile template, either manually or from an existing chassis profile. You can then use the template to create the chassis profiles.

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

Cisco UCS supports the following types of chassis profile templates:

- Initial template

Chassis profiles created from an initial template inherit all the properties of the template. Chassis profiles created from an initial chassis profile template are bound to the template. However, changes to the initial template do not automatically propagate to the bound chassis profiles. If you want to propagate changes to bound chassis profiles, unbind and rebind the chassis profile to the initial template.

- Updating template

Chassis profiles created from an updating template inherit all the properties of the template and remain connected to the template. Any changes to the template automatically update the chassis profiles created from the template.

Procedure 15. Create Chassis Profile Template for Cisco UCS S3260 Storage Server

Step 1. In Cisco UCS Manager, click the Chassis tab in the navigation pane.

Step 2. Select Chassis Profile Templates > root > Sub-Organizations > cohesity.

Step 3. Right-click and select Create Chassis Profile Template.

Step 4. Enter name as cohesity-chs-t

Step 5. Select Type as Updating Template.

Step 6. Select cohesity as the Maintenance Policy and click Next. This maintenance was created under S3260 Chassis Policies

Step 7. Select Chassis Firmware Package as cohesity_chs_fw and SAS Expander Policy as cohesity.

1 Identify Chassis Profile Template

2 Chassis Maintenance Policy

3 Policies

4 Disk Zoning Policy

Create Chassis Profile Template

Optionally configure chassis firmware package for this chassis profile template.

⊖ Chassis Firmware Package

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

Chassis Firmware Package : [Create Chassis Firmware Package](#)

⊕ Compute Connection Policy

⊖ Sas Expander Configuration Policy

The chassis profile will immediately reboot the servers when changes are applied.

Sas Expander Configuration Policy : [Create Sas Expander Configuration Policy](#)

Step 8. Select Disk Zoning Policy as cohesity and click Finish.

1 Identify Chassis Profile Template

2 Chassis Maintenance Policy

3 Policies

4 Disk Zoning Policy

Create Chassis Profile Template

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

Disk Zoning Policy: [Create Disk Zoning Policy](#)

Name : **cohesity**

Description :

Preserve Config : **No**

Disks Zoned

Name	Slot Number	Ownership	Assigned to S...	Assigned to ...	Controller Type	Drive Path
▶ disk-slot-...	27	Dedicated				Path 1
▼ disk-slot-...	28	Dedicated				Path 1
server...			1	1	SAS	
▼ disk-slot-29	29	Dedicated				Path 1
server...			2	1	SAS	

< Prev Next > **Finish** Cancel

The following table details the chassis profile template configured for the Cohesity Helios Platform:

Table 28. Cisco UCS Chassis Profile Template Settings and Values

Chassis Profile Template Name:	Cohesity-chs-t
Setting	Value
Chassis Firmware Package	Cohesity-chs-fw
Disk Zoning Policy	cohesity
Compute Connection Policy	<not set>
Sas Expander Configuration Policy	cohesity

Cisco UCS Service Profile Templates

Cisco UCS Manager has a feature to configure service profile templates, which can be used to simplify and speed up configuration efforts when the same configuration needs to be applied to multiple servers. Service profile templates are used to spawn multiple service profile copies to associate with a group of servers, versus configuring the same service profile manually each time it is needed. Service profile templates contain all the configuration elements that make up a service profile, including vNICs, vHBAs, local disk configurations, boot policies, host firmware packages, BIOS policies and more. Templates are created as either initial templates or updating templates. Updating templates retain a link between the parent template and the child object, therefore when changes are made to the template, the changes are propagated to all remaining linked child objects.

Procedure 1. Configure the Service Profile Template

- Step 1.** In Cisco UCS Manager, click Servers.
- Step 2.** In the tree hierarchy, underneath Service Profile Templates > root > Sub-Organizations, click the carat next to the name of the sub-organization created for Cohesity to expand it.
- Step 3.** Right-click the sub-org name, then click Create Service Profile Template.
- Step 4.** Enter a name for the template.
- Step 5.** Click the radio button for Type: Updating Template.
- Step 6.** In the UUID Assignment drop-down list, select coh-uuid, created in the previous section.

Create Service Profile Template

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

Name :

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

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

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

UUID Assignment:

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

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

< Prev Next > **Finish** Cancel

Step 7. Click Next.

Step 8. In the Storage Provisioning section, click the Local Disk Configuration Policy tab, then in the drop-down list below, select the Local Disk Configuration Policy as 'cohesity-disk', this was created for this template earlier.

Step 9. Click Next.

Create Service Profile Template

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

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

Local Storage:

Create Local Disk Configuration Policy

Mode : **Any Configuration**
Protect Configuration : **Yes**

If **Protect Configuration** is set, the local disk configuration is preserved if the service profile is disassociated with the server. In that case, a configuration error will be raised when a new service profile is associated with that server if the local disk configuration in that profile is different.

FlexFlash

FlexFlash State : **Disable**

If **FlexFlash State** is disabled, SD cards will become unavailable immediately.
Please ensure SD cards are not in use before disabling the FlexFlash State.

FlexFlash RAID Reporting State : **Disable**
FlexFlash Removable State : **No Change**

If **FlexFlash Removable State** is changed, SD cards will become unavailable temporarily.
Please ensure SD cards are not in use before changing the FlexFlash Removable State.

< Prev Next > **Finish** Cancel

Step 10. In the Networking section, click the radio button for Use Connectivity Policy, then in the drop-down list below, select the LAN Connectivity Policy as 'cohesity-lan-con', which was created for this template earlier.

Step 11. Click Next.

The screenshot shows the 'Create Service Profile Template' wizard in the Networking section. The left sidebar lists steps 1 through 11, with 'Networking' selected. The main content area is titled 'Create Service Profile Template' and includes a sub-header 'Optionally specify LAN configuration information.' Below this, there is a 'Dynamic vNIC Connection Policy' dropdown menu set to 'Select a Policy to use (no Dynamic vNIC Policy by default)' and a 'Create Dynamic vNIC Connection Policy' button. A horizontal separator is followed by the question 'How would you like to configure LAN connectivity?' with radio buttons for 'Simple', 'Expert', 'No vNICs', and 'Use Connectivity Policy' (which is selected). Below this is the 'LAN Connectivity Policy' dropdown menu set to 'cohesity-lan-con' and a 'Create LAN Connectivity Policy' button. Another separator is followed by the 'Initiator Name' section, which has an 'Initiator Name Assignment' dropdown menu set to '<not set>' and a 'Create IQN Suffix Pool' button. A warning message states: 'WARNING: The selected pool does not contain any available entities. You can select it, but it is recommended that you add entities to it.' At the bottom right, there are four buttons: '< Prev', 'Next >', 'Finish' (highlighted in blue), and 'Cancel'.

Step 12. In the SAN Connectivity section, click the radio button for No vHBAs, then click Next.

The screenshot shows the 'Create Service Profile Template' wizard in the SAN Connectivity section. The left sidebar lists steps 1 through 6, with 'SAN Connectivity' selected. The main content area is titled 'Create Service Profile Template' and includes a sub-header 'Optionally specify disk policies and SAN configuration information.' Below this, there is a question 'How would you like to configure SAN connectivity?' with radio buttons for 'Simple', 'Expert', 'No vHBAs' (which is selected), and 'Use Connectivity Policy'. Below this is a text message: 'This server associated with this service profile will not be connected to a storage area network.' At the bottom right, there are four buttons: '< Prev', 'Next >', 'Finish' (highlighted in blue), and 'Cancel'.

Step 13. In the Zoning section, no changes are required, click Next.

Step 14. In the vNIC/vHBA Placement section, no changes are required, click Next.

Step 15. In the vMedia Policy section, no changes are required, click Next.

Step 16. In the Server Boot Order section, in the Boot Policy drop-down list, select the Boot Policy as 'cohesity-boot', which was created for this template earlier.

Create Service Profile Template ? X

Optionally specify the boot policy for this service profile template.

Select a boot policy.

Boot Policy: [Create Boot Policy](#)

Name : **cohesity-boot**
Description :
Reboot on Boot Order Change : **No**
Enforce vNIC/vHBA/iSCSI Name : **Yes**
Boot Mode : **Legacy**

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

Boot Order

+ - Advanced Filter Export Print

Name	Order	vNIC/vHB...	Type	LUN Name	WWN	Slot Num...	Boot Name	Boot Path	Description
CD/DVD	1								
Local ...	2								

Create iSCSI vNIC Set iSCSI Boot Parameters Set iSCSI Boot Parameters

< Prev Next > **Finish** Cancel

Step 17. Click Next.

Step 18. In the Maintenance Policy section, select Maintenance Policy drop-down list, select the Maintenance Policy as 'cohesity-usr-ack', which was created for this template earlier.

Create Service Profile Template ? X

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

⊖ Maintenance Policy

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

Maintenance Policy: cohesity-usr-ack ▼ Create Maintenance Policy

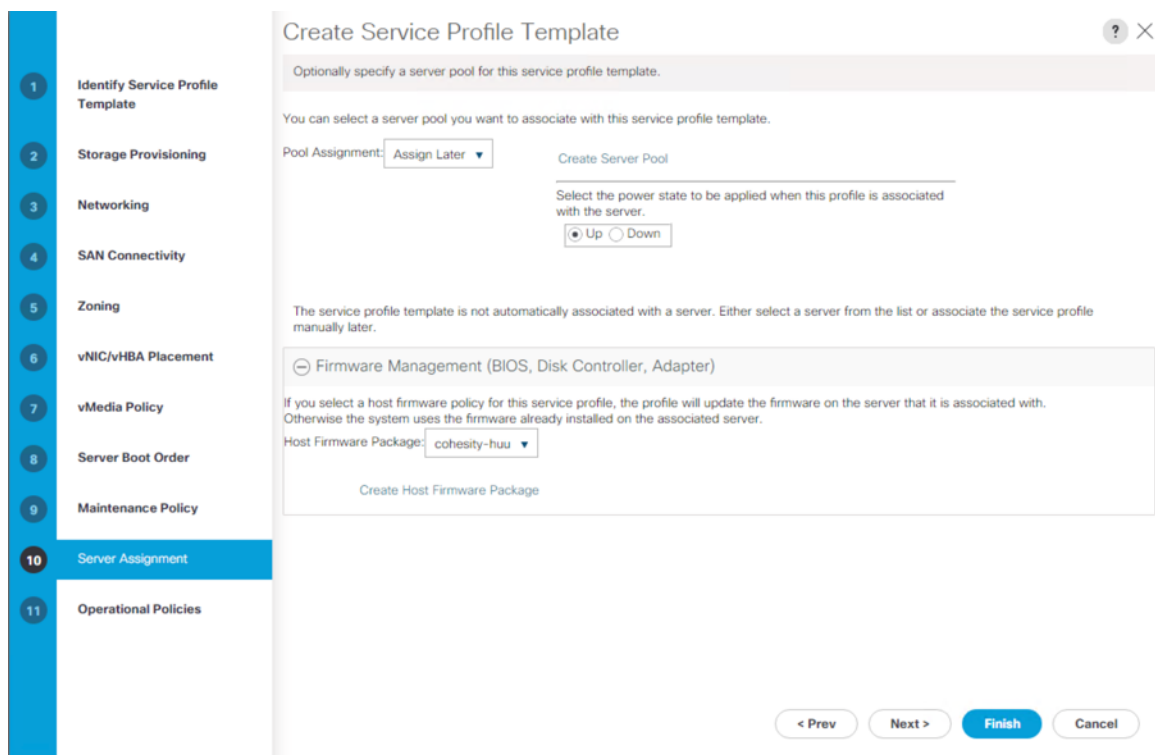
Name	:	cohesity-usr-ack
Description	:	
Soft Shutdown Timer	:	150 Secs
Storage Config. Deployment Policy	:	User Ack
Reboot Policy	:	User Ack

< Prev
Next >
Finish
Cancel

Step 19. Click Next.

Step 20. In the Server Assignment section, leave the Pool Assignment set to Assign Later, and select the radio button for the desired power state to Up.

Step 21. Click the + button next to Firmware Management to expand the section. In the Host Firmware Package drop-down list, select the Host Firmware Package as 'cohesity-huu', which was created for this template earlier.



Step 22. Click Next.

Step 23. In the Operation Policies section, click the + button next to BIOS Configuration to expand the section. In the BIOS Policy drop-down list, select the BIOS Policy as 'cohesity-bios', which was created for this template earlier.

Step 24. Click the + button next to External IPMI Management Configuration to expand the section. In the IPMI Access Profile drop-down list, select the IPMI Access Profile 'cohesity-ipmi', which was created for this template earlier.

Step 25. In the SoL Configuration Profile drop-down list, select the Serial Over LAN Policy 'cohesity-sol', which was created for this template earlier.

Step 26. Click the + button next to Management IP Address to expand the section. Click the Out-band IPv4 tab, then from the Management IP Address Policy drop-down list, select the Management IP Address Pool 'coh-ip-pool', which was created for this template earlier.

Step 27. Click Finish.

[Table 29](#) details the service profile template configured for the Cohesity Helios nodes:

Table 29. Cisco UCS Service Profile Template Settings and Values

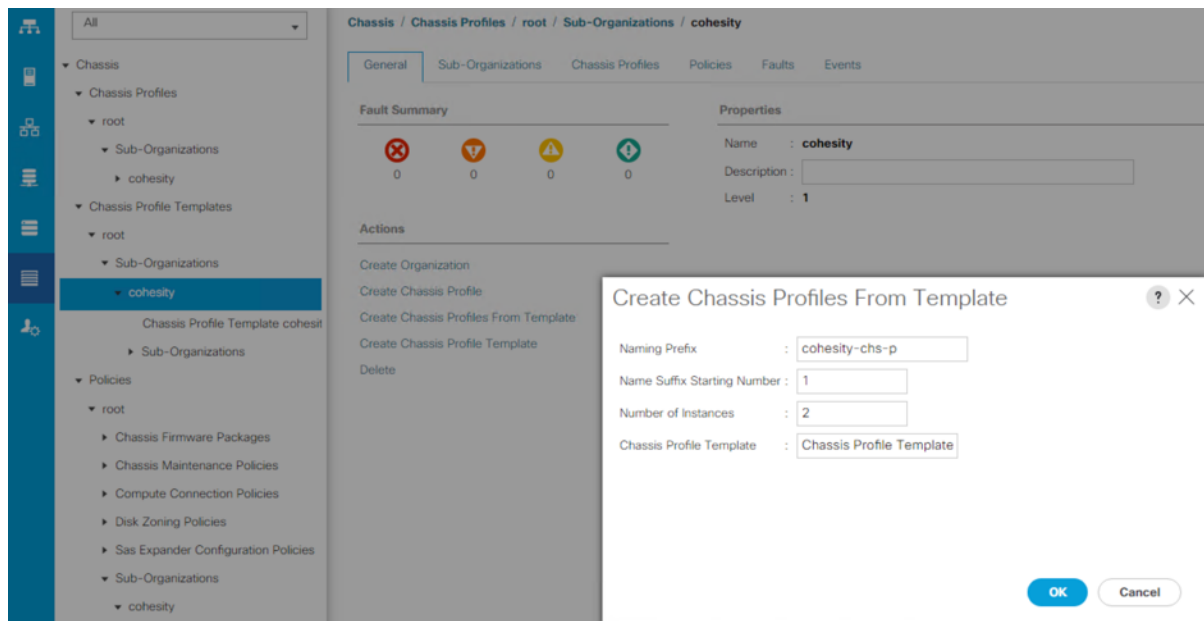
Service Profile Template Name:	cohesity-sp-t
Setting	Value
UUID Pool	cohesity-uuid
Local Disk Configuration Policy	cohesity-disk
Associated Server Pool	None
Maintenance Policy	cohesity-usr-ack
Management IP Address Policy	coh-ip-pool
Local Disk Configuration Policy	cohesity-disk
LAN Connectivity Policy	cohesity-lan-con
Boot Policy	cohesity-boot

Service Profile Template Name:	cohesity-sp-t
BIOS Policy	cohesity-bios
Firmware Policy	cohesity-huu
Serial over LAN Policy	cohesity-sol
IPMI Policy	cohesity-ipmi

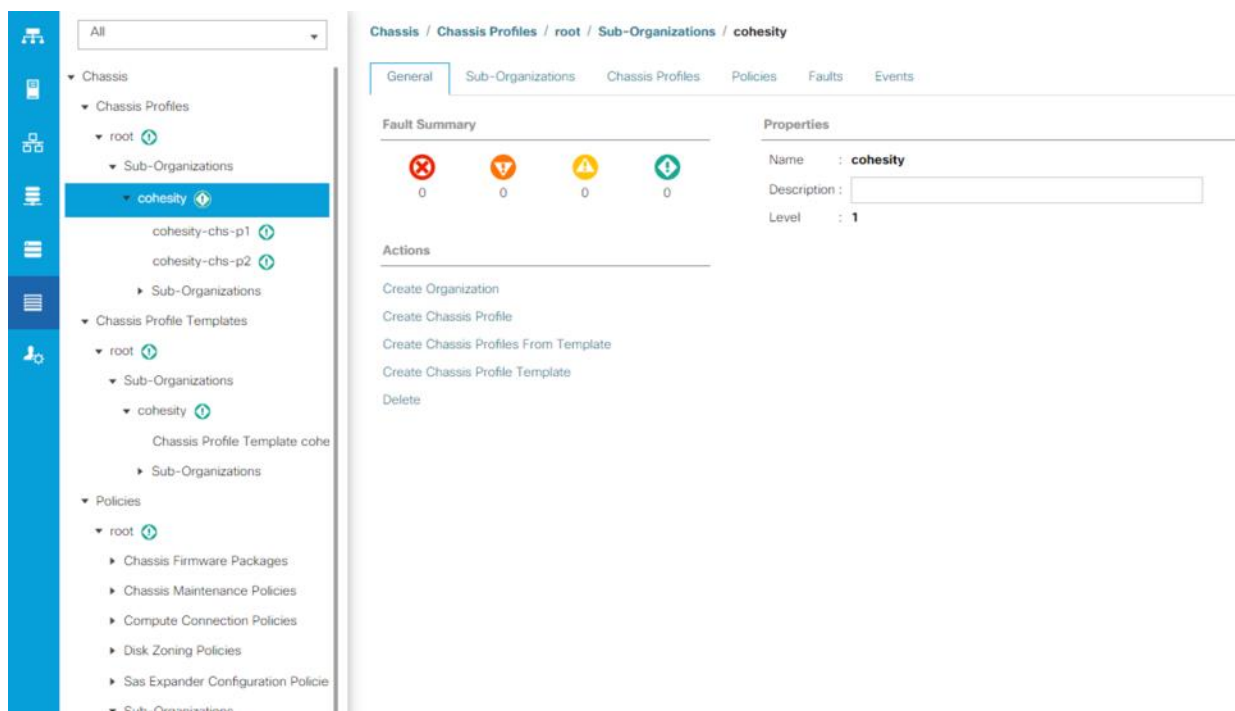
Create Chassis Profile

Procedure 2. Create the chassis profile from the chassis profile template

- Step 1.** Click the Chassis tab in the navigation pane.
- Step 2.** Select Chassis Profile Templates > root > Sub-Organizations > cohesity > Chassis Profile Template Chassis_Template.
- Step 3.** Right-click Chassis Profile Template cohesity-chs-t and Select Create Chassis Profiles from Template
- Step 4.** Enter cohesity-chs-p as the Chassis profile prefix.
- Step 5.** Enter 1 as “Name Suffix Starting Number and 2 as Number of Instances.
- Step 6.** Select Chassis Profile Template as ‘cohesity-chs-t’, created in previous section



- Step 7.** The screenshot below displays two Chassis Profiles, cohesity-chs-p1 and cohesity-chs-p2 under Chassis > root > Sub_organizations > cohesity > Chassis Profile.

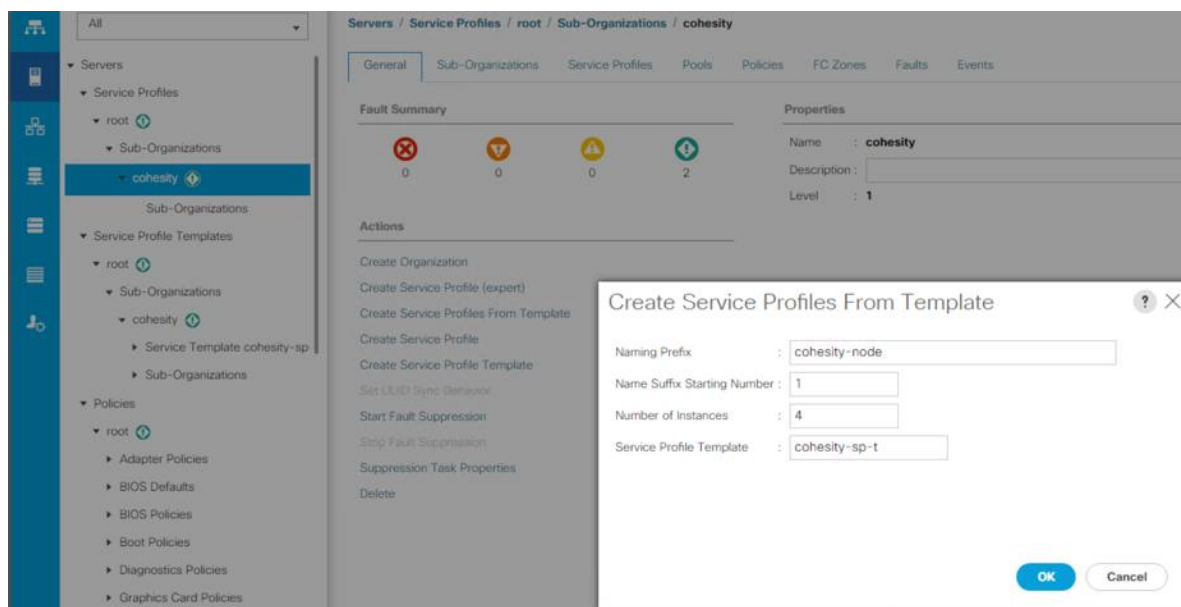


Create Service Profiles

When a Cisco UCS Service Profile Template has been created, individual Service Profiles for each Cohesity node can be created from the template. The unique identifying characteristics of the service profile, such as MAC addresses or IP addresses, are drawn from the pools and the configurations are set according to the policies, when the service profile is created. By basing the service profiles on a template, all of the service profiles will have identical configurations. Because the service profiles are based on an updating template, if any errors are found, or changes need to be made to all of the servers, the changes can be made in the parent template, and all child profiles will inherit the change.

Procedure 3. Configure the Service Profiles from the template

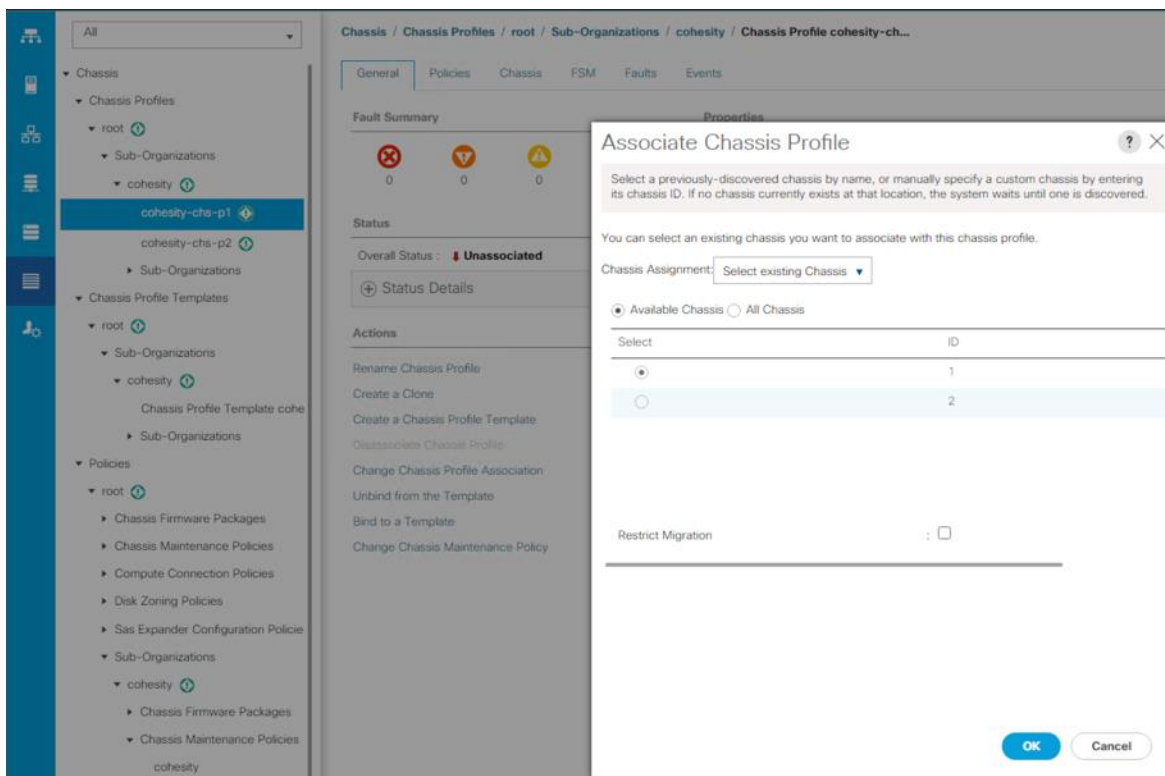
- Step 1.** In Cisco UCS Manager, click Servers.
- Step 2.** In the tree hierarchy, underneath Service Profile Templates > root > Sub-Organizations, click the carat next to the name of the sub-organization created for Cohesity to expand it.
- Step 3.** Right-click the Service Profile Template, then click Create Service Profiles From Template.
- Step 4.** Enter a naming prefix, which will be applied to all of the spawned service profiles, for example “Cohesity-node-“
- Step 5.** Enter the starting number for the number to be appended to the name prefix just entered.
- Step 6.** Enter the number of service profiles to create from this template.
- Step 7.** Select the service profile template as ‘cohesity-sp-t’, created in the previous section.
- Step 8.** Click OK.



Associate Chassis Profile to Cisco UCS S3260 Chassis

Procedure 4. Associate the Chassis Profile to the Cisco UCS S3260 Chassis

- Step 1.** Click the Chassis tab in the navigation pane.
- Step 2.** Select Chassis Profiles > root > Sub-Organizations > cohesity.
- Step 3.** Right-click 'cohesity-chs-p1 and select Change Chassis Profile Association.
- Step 4.** In the Assignment tab, select Existing Chassis.
- Step 5.** Select the existing chassis.



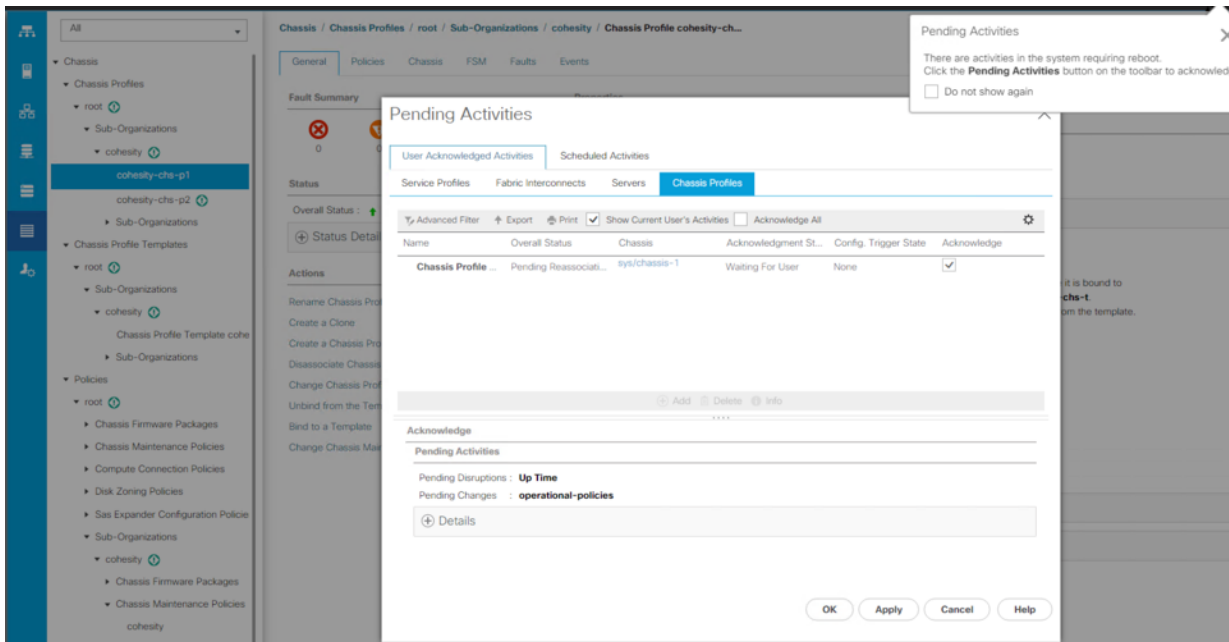
Step 6. Click OK.

Step 7. Since you have selected User Ack for the Maintenance Policy, you need to acknowledge Chassis Reboot for Chassis Profile Association.

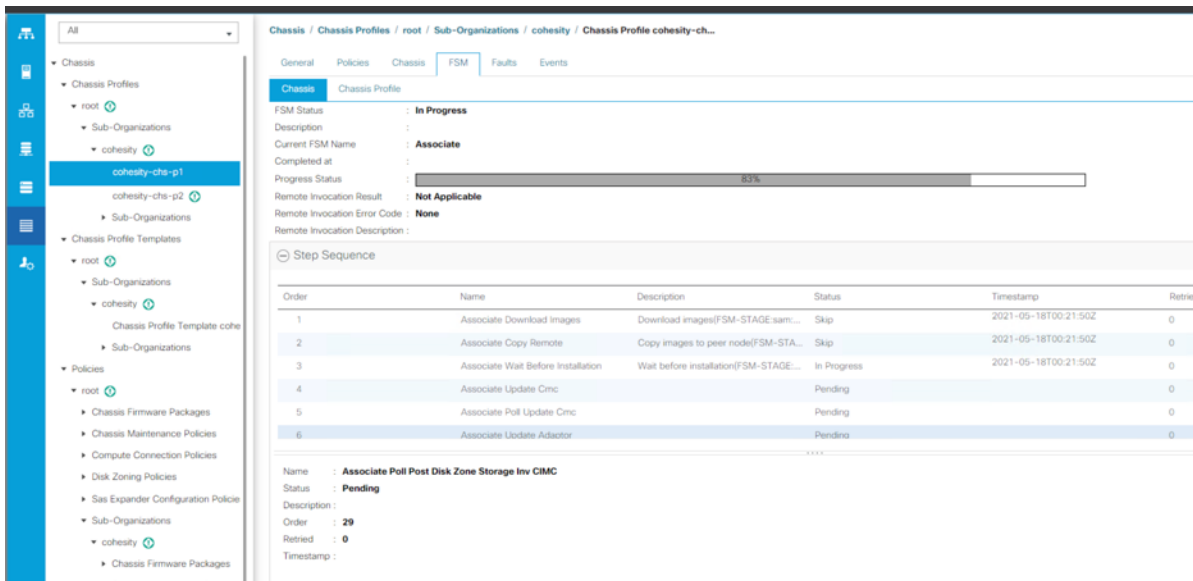
Step 8. Click on Pending Activities in the right top corner.

Step 9. Under User Acknowledged Activities tab, Select 'Chassis Profiles' tab.

Step 10. Select the 'Acknowledge' checkbox.

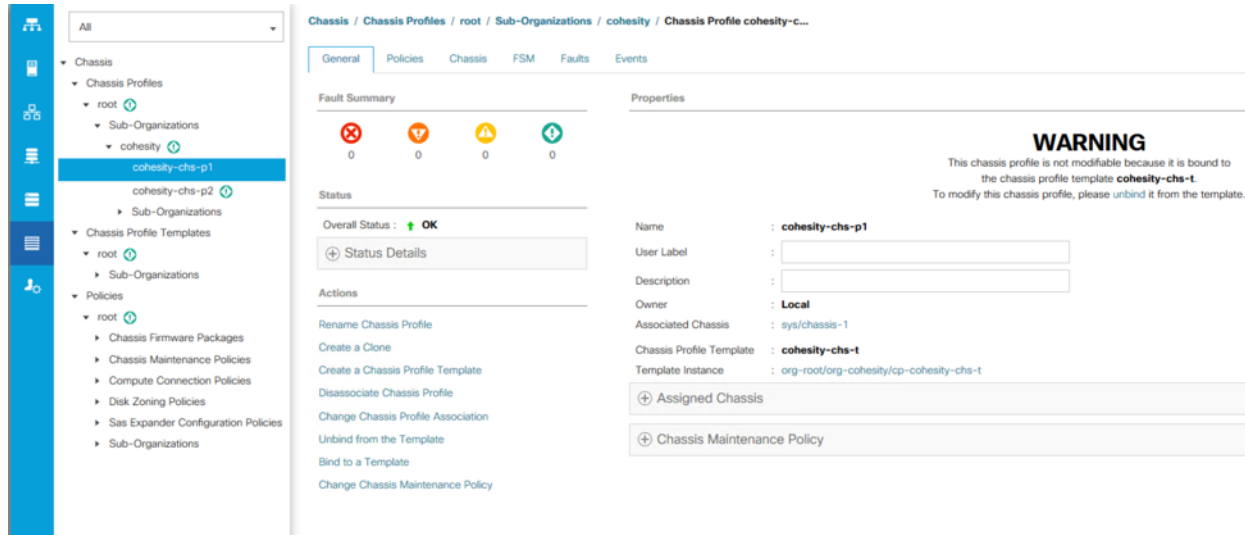


Step 11. On FSM Tab you will see the Association Status.



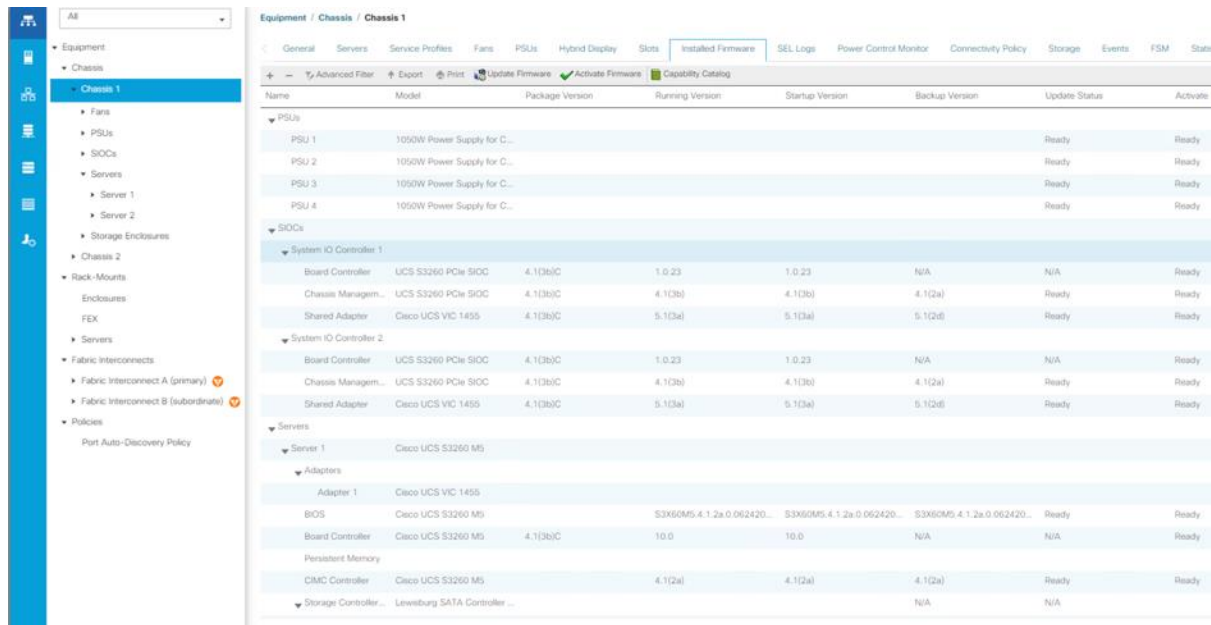
Step 12. When the Chassis is Associated you will see the assigned status as Assigned. Chassis Association may take some time, if the firmware of the associated Chassis is not same as the Chassis Firmware Profile attached to the Chassis Profile.

Figure 50. Associated Chassis Profile

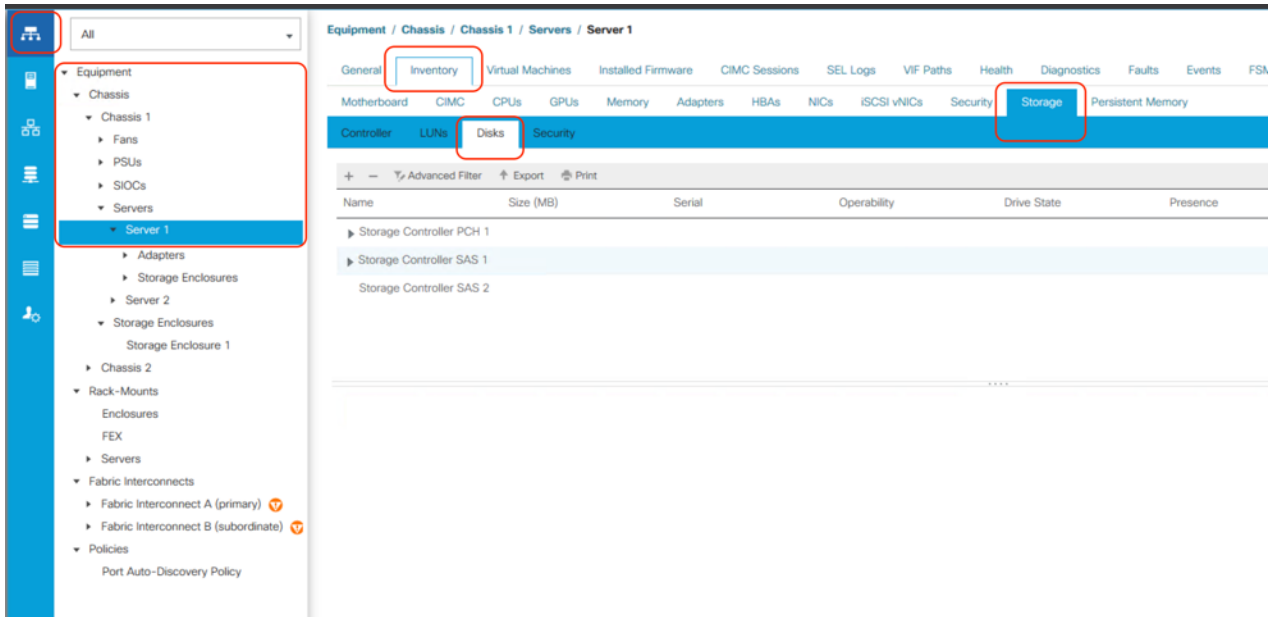


Step 13. Click the Equipment tab in the navigation pane and select Chassis tab.

Step 14. Select Equipment > Chassis > Chassis<n> select the 'Installed Firmware' tab, and verify the Firmware is upgraded to 4.1(3b).

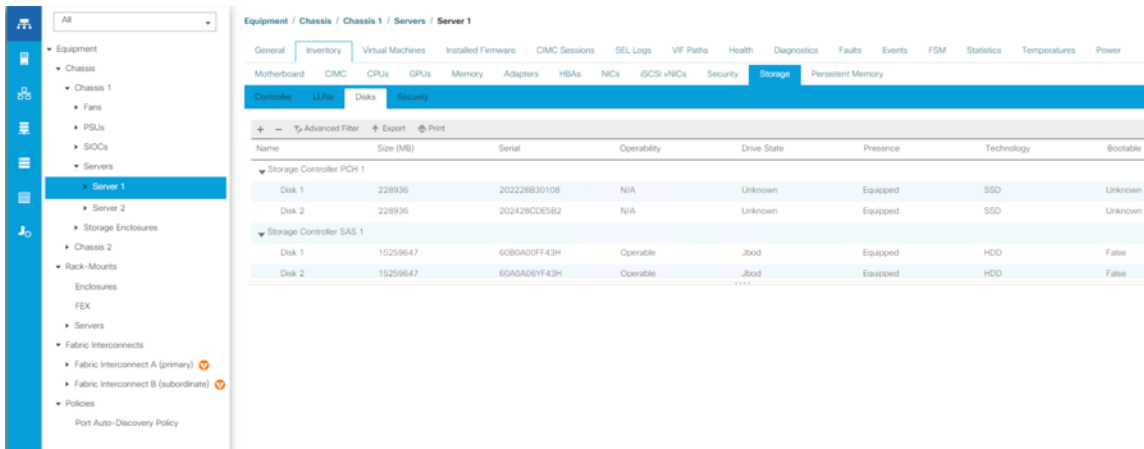


Step 15. Select Equipment > Chassis > Chassis<n> > Server1 > Inventory > Storage > Disks.

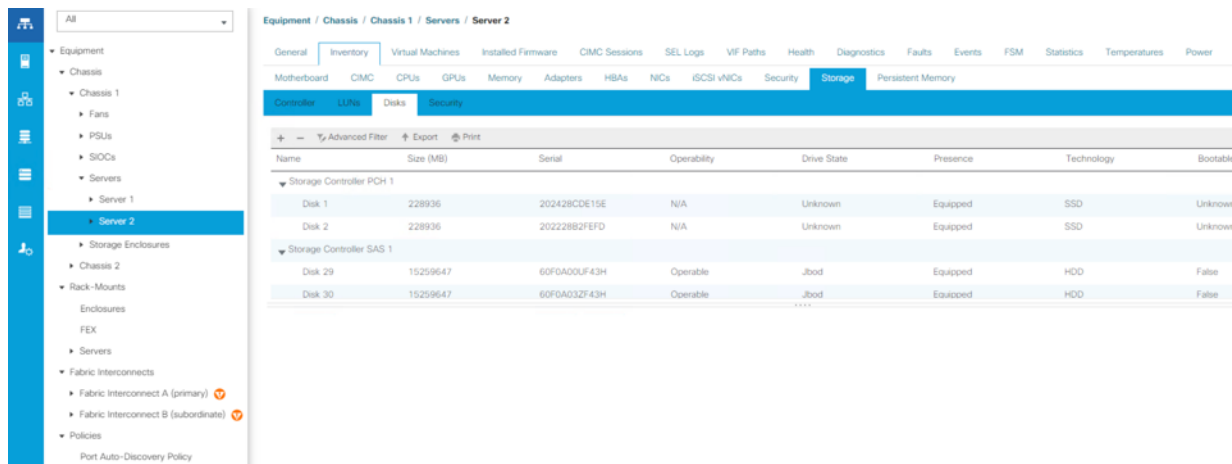


Step 16. Expand disk by clicking the carat next to the 'Storage Controller PCH 1' and 'Storage Controller SAS 1'.

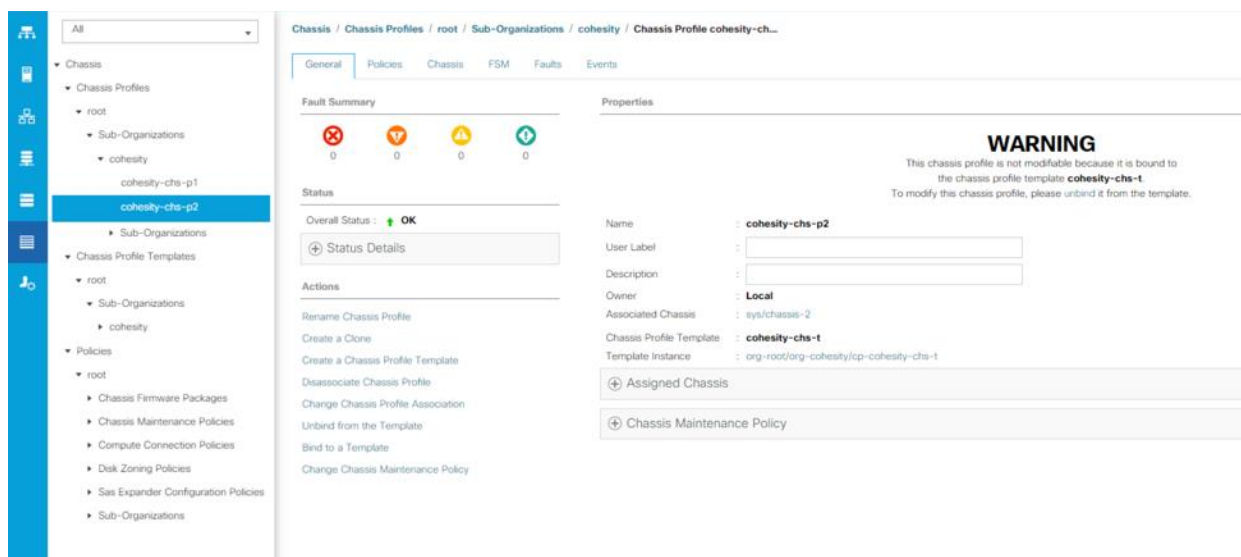
Step 17. Verify Disk allocation to Server 1.



Step 18. Similarly verify Disk allocation to Server 2.



Step 19. Repeat steps 1-18, associate Chassis Profile to the second Chassis available for cohesity cluster deployment.

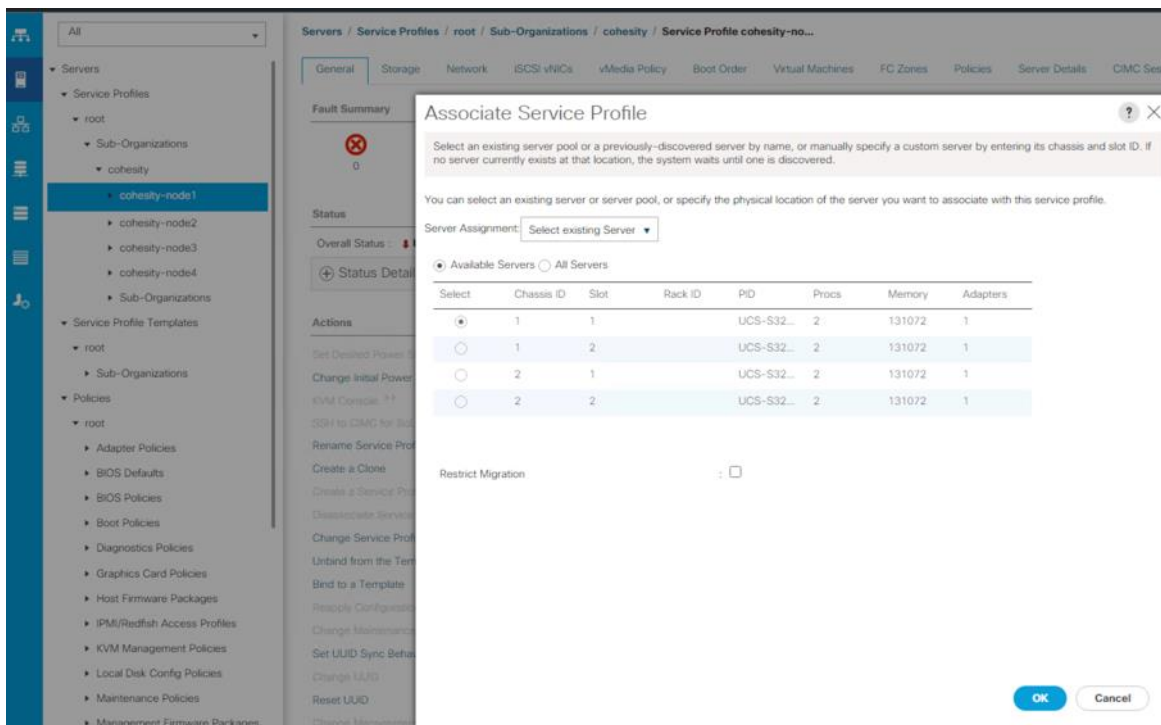


Service Profile Association

When a Cisco UCS Service Profile has been created, it must be associated with a physical hardware asset in order to take effect. Service profile association requires the server node in the Cisco UCS S3260 storage chassis to be present, fully discovered, and not currently associated with any other service profiles. Automatic assignment of service profiles can be done through the use of server pools and auto-discovery, but that configuration is not the recommended method for this paper, and therefore not covered in this document. Once the service profile association is initiated, all of the configuration elements and identities are applied to the server hardware, including storage, networking, policies, and firmware upgrades. At the conclusion of the association process, the server will be ready for use, but with no operating system installed.

Procedure 5. Associate the Service Profiles to the Cohesity node servers

- Step 1.** In Cisco UCS Manager, click Servers.
- Step 2.** In the tree hierarchy, underneath Service Profiles > root > Sub-Organizations, click the carat next to the name of the sub-organization created for Cohesity to expand it.
- Step 3.** Click the first Service Profile you wish to associate, then in the right-hand pane, click the blue link for “Change Service Profile Association.”
- Step 4.** In the Server Assignment drop-down list, choose “Select existing Server.”
- Step 5.** Ensure the radio button for Available Servers is selected, in the list below you should see the connected and discovered S3260 server nodes which have not yet been associated with a service profile.
- Step 6.** Select the radio button next to the first server to associate, then click OK.
- Step 7.** Repeat steps 1-6 for each remaining service profile, choosing a subsequent Cisco UCS S3260 nodes to associate with.



As previously described, when the service profile association is started, there are many activities that must take place to finalize the configuration of the server. The process can take some time to complete, especially if there are significant firmware updates to perform and comply with the policy. Before continuing with the Cohesity installation processes, wait for all the servers to finish their association process and to show an overall status of OK, with no errors.

Procedure 6. View the servers' discovery status

- Step 1.** In Cisco UCS Manager, click Equipment on the left-hand side, and click Equipment in the top of the navigation tree on the left.
- Step 2.** In the properties pane, click the Chassis tab.

Step 3. View the servers' status in the Overall Status column and confirm the status as OK.

The screenshot shows the 'Equipment / Chassis' page with a table of server status. The table has columns for Name, Chassis ID, PID, Model, User Label, Cores, Cores Em..., Memory, Adapters, HCs, HBAs, Overall Sta..., Operability, Power State, Assoc State, Profile, and Fault Sup. The 'Overall Sta...' column shows 'OK' for all servers.

Name	Chassis ID	PID	Model	User Label	Cores	Cores Em...	Memory	Adapters	HCs	HBAs	Overall Sta...	Operability	Power State	Assoc State	Profile	Fault Sup
Server 1	1	UCS-S32...	Cisco UCS...		24	24	131072	1	2	0	OK	Opera...	On	Assoc...	OPS-PROFIS...	N/A
Server 2	1	UCS-S32...	Cisco UCS...		24	24	131072	1	0	0	Unasso...	Opera...	Off	None		N/A
Server 1	2	UCS-S32...	Cisco UCS...		24	24	131072	1	0	0	Unasso...	Opera...	Off	None		N/A
Server 2	2	UCS-S32...	Cisco UCS...		24	24	131072	1	0	0	Unasso...	Opera...	Off	None		N/A

Step 4. Confirm the Installed Firmware Version for each Chassis and Server node has a package version of 4.1(3b).

The screenshot shows the 'Equipment / Chassis / Chassis 1' page with the 'Installed Firmware' section. The table has columns for Name, Model, Package Version, Running Version, Startup Version, Backup Version, Update Status, and Activate Stat. The 'Package Version' column shows '4.1(3b)' for all components.

Name	Model	Package Version	Running Version	Startup Version	Backup Version	Update Status	Activate Stat
SAS Expander 1	Cisco UCS S3260	4.1(3b)C	04.08.01.8063	04.08.01.8063	04.08.01.8062	Ready	Ready
SAS Expander 2	Cisco UCS S3260	4.1(3b)C	04.08.01.8063	04.08.01.8063	04.08.01.8063	Ready	Ready
System IO Controller 1							
Board Controller	UCS S3260 PCIe SIOC	4.1(3b)C	1.0.23	1.0.23	N/A	N/A	Ready
Chassis Managem...	UCS S3260 PCIe SIOC	4.1(3b)C	4.1(3b)	4.1(3b)	4.1(2a)	Ready	Ready
Shared Adapter	Cisco UCS VIC 1455	4.1(3b)C	5.1(3a)	5.1(3a)	5.1(2b)	Ready	Ready
System IO Controller 2							
Board Controller	UCS S3260 PCIe SIOC	4.1(3b)C	1.0.23	1.0.23	N/A	N/A	Ready
Chassis Managem...	UCS S3260 PCIe SIOC	4.1(3b)C	4.1(3b)	4.1(3b)	4.1(2a)	Ready	Ready
Shared Adapter	Cisco UCS VIC 1455	4.1(3b)C	5.1(3a)	5.1(3a)	5.1(2b)	Ready	Ready
Servers							
Server 1							
Cisco UCS S3260 M5							
Adapters							
Adapter 1	Cisco UCS VIC 1455						
BIOS	Cisco UCS S3260 M5	4.1(3b)C	S3X60M5.4.1.3a.0.121020...	S3X60M5.4.1.3a.0.121020...	S3X60M5.4.1.2a.0.062420...	Ready	Ready
Board Controller	Cisco UCS S3260 M5	4.1(3b)C	10.0	10.0	N/A	N/A	Ready
CMC Controller	Cisco UCS S3260 M5	4.1(3b)C	4.1(3b)	4.1(3b)	4.1(2a)	Ready	Ready
Persistent Memory							
Storage Controller... Lewisburg SATA Controller ...							
Disks							

Step 5. Verify all the S3260 chassis server nodes are associated with Overall Status as OK.

Name	Chassis ID	RD	Model	User Label	Cores	Cores Ena...	Memory	Adapters	NICs	HBAs	Overall Sta...	Operability	Power State	Assoc. State	Profile	Fault
Server 1	1	UCS-S32...	Cisco UCS...		24	24	131072	1	2	0	OK	Opera...	On	Assoc...	org-ucsd...	N/A
Server 2	1	UCS-S32...	Cisco UCS...		24	24	131072	1	2	0	OK	Opera...	On	Assoc...	org-ucsd...	N/A
Server 1	2	UCS-S32...	Cisco UCS...		24	24	131072	1	2	0	OK	Opera...	On	Assoc...	org-ucsd...	N/A
Server 2	2	UCS-S32...	Cisco UCS...		24	24	131072	1	2	0	OK	Opera...	On	Assoc...	org-ucsd...	N/A

Cohesity Installation

Cohesity Helios Platform is installed in three phases; first is the initial software installation to all the Cohesity nodes, followed by the initial network setup of a single node, allowing access the Cohesity configuration webpage, and finally the initial Cohesity cluster configuration, which is done from the aforementioned webpage.

Cohesity Software Installation

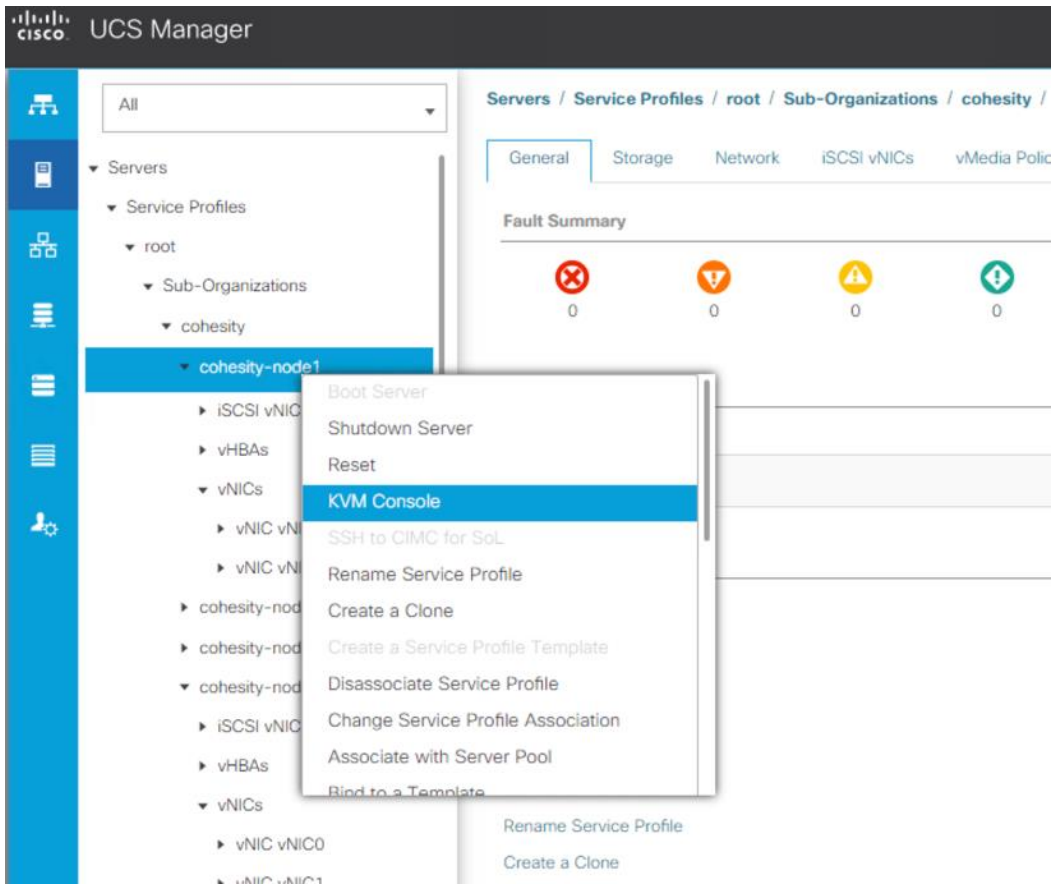
The installation of Cohesity Helios software is done through a bootable DVD ISO image file. Each node is booted from this image file, which will automate the process of installing the underlying Linux operating system, copy the Cohesity software packages, and prepare the nodes for the initial setup of the Cohesity cluster.

Procedure 7. Install the Cohesity software on each Cisco UCS S3260 node

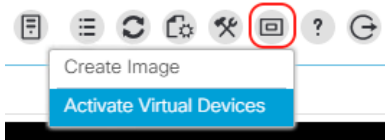
Step 1. In Cisco UCS Manager, click Servers.

Step 2. In the tree hierarchy, underneath Service Profiles > root > Sub-Organizations, click the carat next to the name of the sub-organization created for Cohesity to expand it.

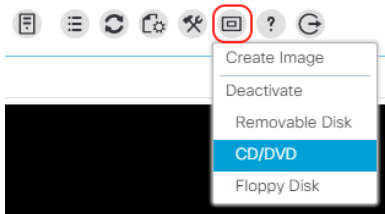
Step 3. Each Cohesity node will have its own service profile, for example: Cohesity-node1. Right-click the first service profile and click KVM Console. The remote KVM console will open in a new browser tab. Accept any SSL errors or alerts, then click the link to launch the KVM console.



Step 4. In the remote KVM tab, click the Virtual Media button in the top right-hand corner of the screen, then click Activate Virtual Devices.

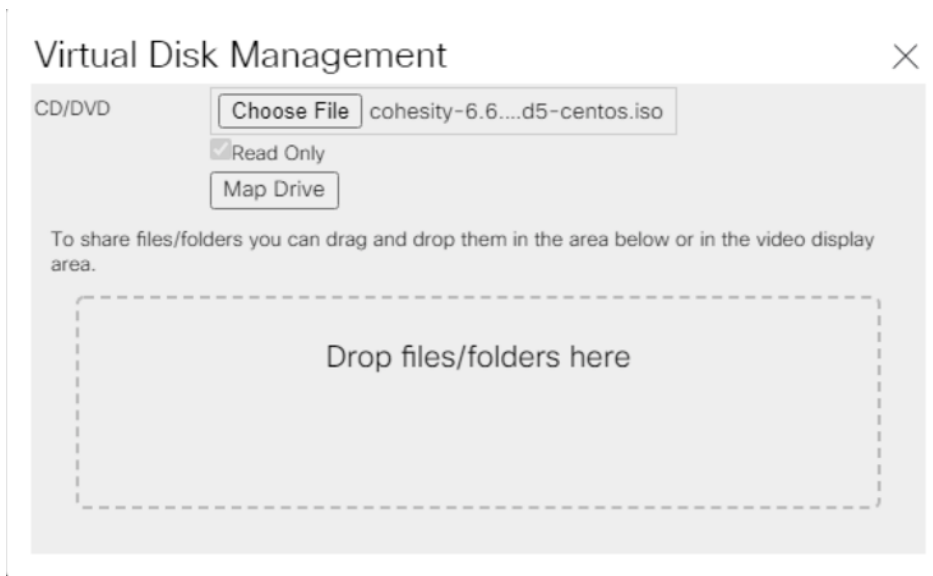


Step 5. In the remote KVM tab, click the Virtual Media button in the top right-hand corner of the screen, then click the CD/DVD option.

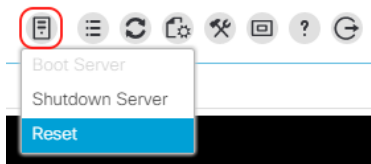


Step 6. Click Choose File, browse for the Cohesity ISO installer file, and click Open.

Step 7. Click CD/DVD.



Step 8. In the remote KVM tab, click the Server Actions button in the top right-hand corner of the screen, then click Reset.



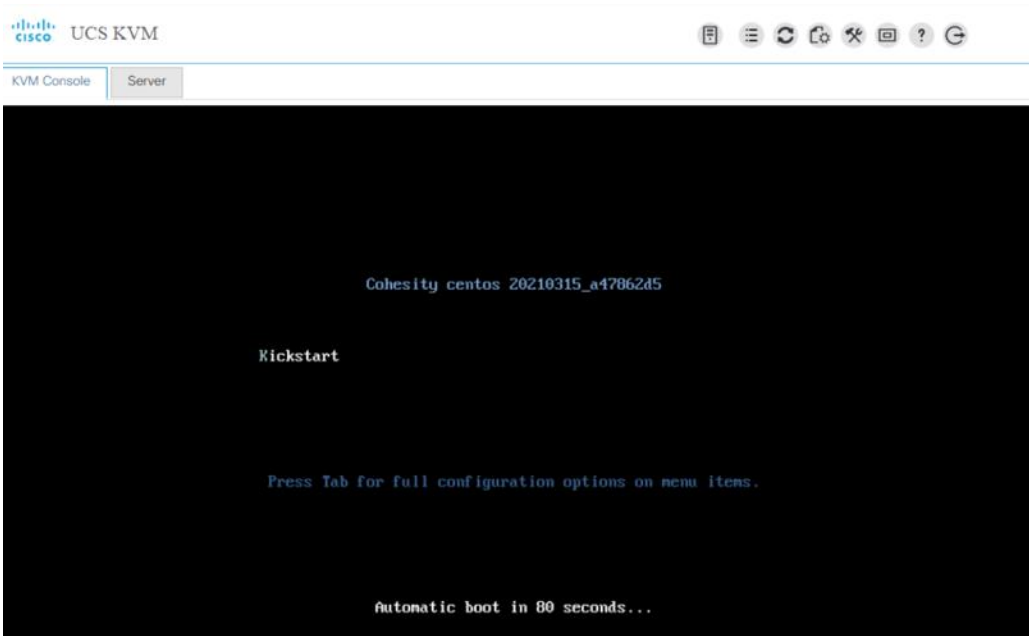
Step 9. Click OK.

Step 10. Choose the Power Cycle option, then click OK.

Step 11. Click OK.

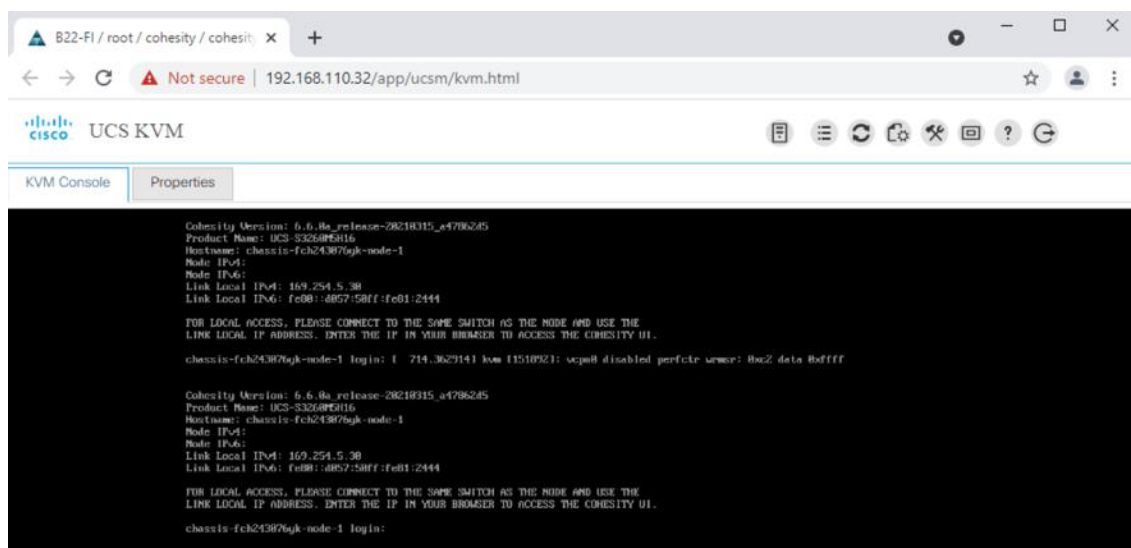
Step 12. Observe the server going through the POST process until the Cohesity installer screen is displayed. We configured the Boot Policy with CD/DVD in first boot order, hence the Cohesity installer will load automatically

The server will boot from the remote KVM mapped Cohesity ISO installer and display the following screen:



Step 13. Allow the automatic timer to count down from 120 seconds, or press Enter.

The Cohesity installer will now automatically perform the installation to the boot media. Installation time takes approximately 30-35 minutes. Once the new server has completed the installation, the server will reboot, and it will be waiting at the console login prompt screen seen below. Please note, the initial hostname is the serial number of the server node in the Cisco UCS S3260 chassis.



Step 14. In the remote KVM tab, click the Exit button, then click Yes.

Step 15. Repeat steps 3-14 for each additional Cohesity node being installed.

Cohesity First Node Configuration

In order to perform the initial cluster setup, the first node of the Cohesity cluster must be accessible through the network, so that the administrator performing the configuration can access the Cohesity configuration webpage running on that node. Cohesity nodes will automatically configure themselves with IPv6 link-local addresses and use these addresses to discover each other on the same subnet. These IPv6 addresses can also be used to perform the initial configuration through the webpage. However, many environments are not configured to use IPv6, therefore it is more common to use IPv4 addresses to perform the initial configuration. To use IPv4 addresses, the first node must be manually configured with an IPv4 address, so that the webpage is accessible to the administrator's client computer.

Procedure 8. Manually configure the first Cohesity node's IPv4 address

Step 1. In Cisco UCS Manager, click Servers.

Step 2. In the tree hierarchy, underneath Service Profiles > root > Sub-Organizations, click the carat next to the name of the sub-organization created for Cohesity to expand it.

Step 3. Each Cohesity node will have its own service profile, for example: Cohesity-sp-1. Right-click the first service profile and click KVM Console. The remote KVM console will open in a new browser tab. Accept any SSL errors or alerts, then click the link to launch the KVM console.

Step 4. When the node's local login prompt appears, login with the following credentials:

- Username: cohesity
- Password: <password>

Step 5. Go to the shell by entering 'sh' and password as <password>.

Step 6. Edit the network configuration through the network configuration script file.

```
sudo ~/bin/network/configure_network.sh
```

Note: Using sudo is required for root privileges.

Step 7. Select option 2 'Configure IP Address on interface'.

Step 8. Select default interface 'bond0'.

Step 9. Enter IP Address, Interface Prefix and Gateway.

Step 10. Choose default MTU as 1500.

Step 11. Select 'Y/Yes' to make the interface active.

Step 12. Quit the configure_network script by entering option '12'.

Step 13. Test the network is working properly by pinging the default gateway. You can also verify the IP address configuration by issuing the following command:

```
ip addr
```

Step 14. Log out of the node:

```
exit
```

Step 15. In the remote KVM tab, click Exit, then click Yes.

Cohesity Cluster Setup

The initial setup of the Cohesity cluster is done through the configuration webpage, which is now accessible on the first node, at the IP address which was configured in the previous steps. Prior to beginning the initial cluster configuration, ensure that all of the Cohesity nodes which are to be included in the cluster have completed their initial software installation, and are fully booted. Additionally, ensure that all of the necessary IP addresses for all of the interfaces are known and assigned, and the DNS round-robin entries have been created.

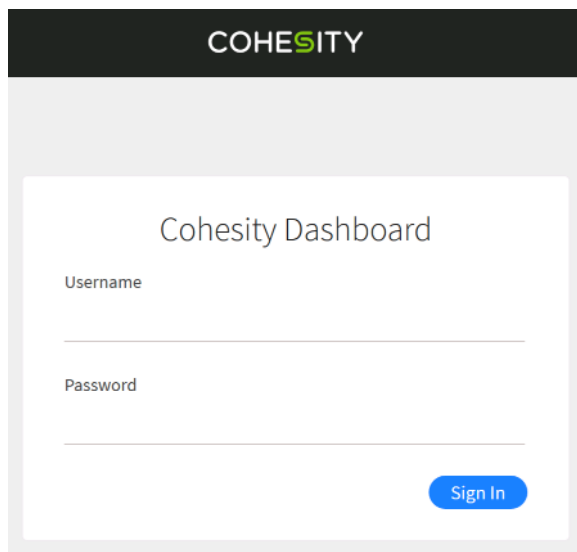
Procedure 9. Configure the Cohesity initial cluster

Step 1. In a web browser, navigate to the IP address of the first Cohesity node, which was just configured in the previous steps. For example: <http://192.168.110.85>

Step 2. Accept any SSL warnings or errors due to the default self-signed certificate on the server and proceed to the Cohesity Dashboard login screen.

Step 3. Log into the Cohesity Dashboard webpage using the credentials below:

- Username: admin
- Password: <password>



COHESITY

Cohesity Dashboard

Username

Password

Sign In

Step 4. When the Start Initial Cluster Setup screen appears, make sure that the number of nodes detected matches the number of servers you intend to install for this cluster. Click Get Started.

Start Initial Cluster Setup

The following hardware was detected.

5

Chassis

5

Nodes

The entire Cluster setup process should take less than an hour. You will need the following information to set up your Cluster:

- IP address and IPMI IP address for each of your Nodes
- Cluster name and cluster domain name
- Cluster subnet gateway and subnet mask
- IPMI Subnet Gateway and Subnet Mask
- IPMI username and password
- Search domains
- DNS servers
- NTP servers

[Get Started](#)

Note: Cohesity File Services setup in this guide is configured with 2 x Cisco UCS S3260 each with two compute node.

Note: The screenshot above displays 5 nodes; using 4 nodes for the present cluster configuration. Each Cisco UCS S3260 Chassis is configured with two nodes.

Step 5. Select the nodes to add to this initial cluster or click the link to Select All Available in the upper right-hand corner, then click Select Nodes.

Cluster Setup

1 Select Nodes 2 Network Settings 3 Cluster Settings

The following Nodes were detected. [Select All](#)

You need a minimum of 3 Nodes to create a Cluster

Chassis FCH224770KC

Node 1 - 161964138753
Product Model: UCS-S3260M5H16

Chassis FCH2430755B

Node 1 - 161964752898
Product Model: UCS-S3260M5H16

Chassis FCH243076YK

Node 1 - 161964752896 Connected
Product Model: UCS-S3260M5H16

Chassis FCH24327AAM5

Node 1 - 161964752897
Product Model: UCS-S3260M5H16

Chassis FCH24327AQK

Node 1 - 161964752899
Product Model: UCS-S3260M5H16

2U4N Node slots are displayed according to a rear view of the Chassis.

[Select Nodes](#) [Cancel](#)

Activate Windows
Go to Settings to activate Windows.

The screenshot displays the Cisco UCS Manager interface for a server node. The left sidebar shows a navigation tree with 'Chassis 2' and 'Server 1' highlighted. The main content area is titled 'Equipment / Chassis / Chassis 2 / Servers / Server 1'. It includes a 'Fault Summary' section with four status indicators (red, orange, yellow, green), a 'Status' section showing 'Overall Status: OK', and a 'Physical Display' image of the server rack. The 'Properties' section lists various attributes, with 'Serial' highlighted in a red box, showing the value 'FCH2430755B'. Other properties include Slot ID (1), Chassis ID (2), Product Name (Cisco UCS S3260 M5), Vendor (Cisco Systems Inc), Revision (0), Manufacturing Date (2020-08-10), and Health LED (Normal).

Note: Chassis ID for each node is mapped to the serial number of the compute node of each Cisco UCS S3260 chassis

Step 6. The Cohesity setup screen lists the serial numbers of the server node, which can be cross-referenced with the Equipment > Chassis > Chassis <1-2> > Server<1-2> view in Cisco UCS Manager. You need to traverse to all of the Chassis nodes to identify Serial numbers of nodes in each chassis.

Cluster Setup

IP Assignment for Selected Nodes

Enter the IP and IPMI address for each of your selected Nodes. You need a minimum of 3 Nodes to create a Cluster.

IPv4 IPv6

Chassis FCH243075SB

Node	IP	IPMI IP
Node 1 - 161964752898	192.0.2.1	127.5.2.1

Chassis FCH243076YK

Node	IP	IPMI IP
Node 1 - 161964752896	192.168.110.85	127.5.1.1

Chassis FCH24327AMS

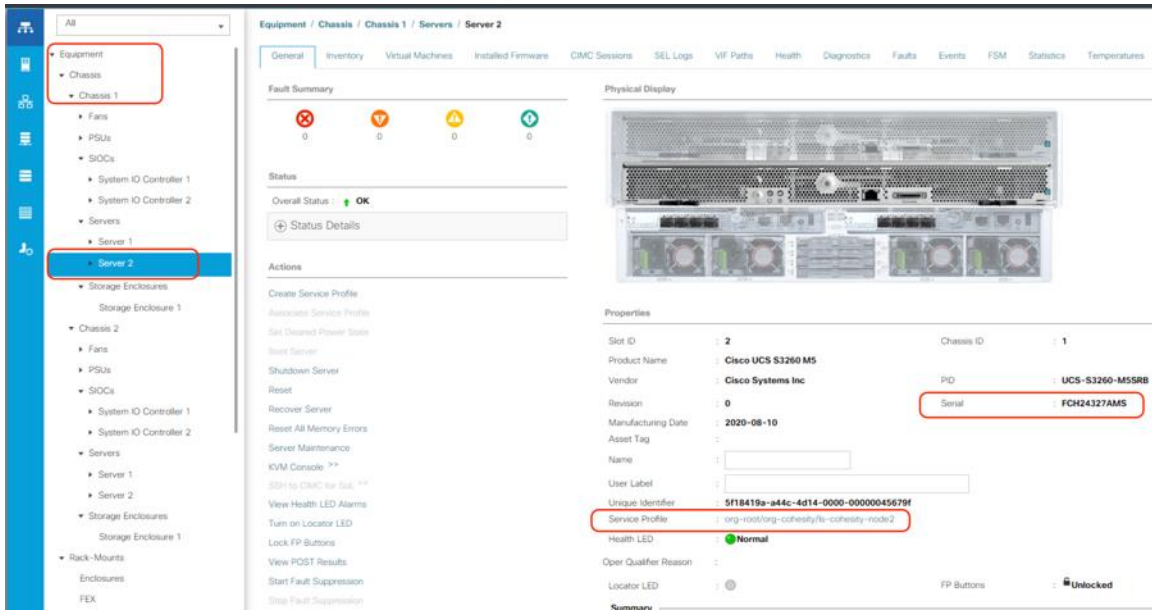
Node	IP	IPMI IP
Node 1 - 161964752897	192.0.2.1	127.5.1.2

Chassis FCH24327AQX

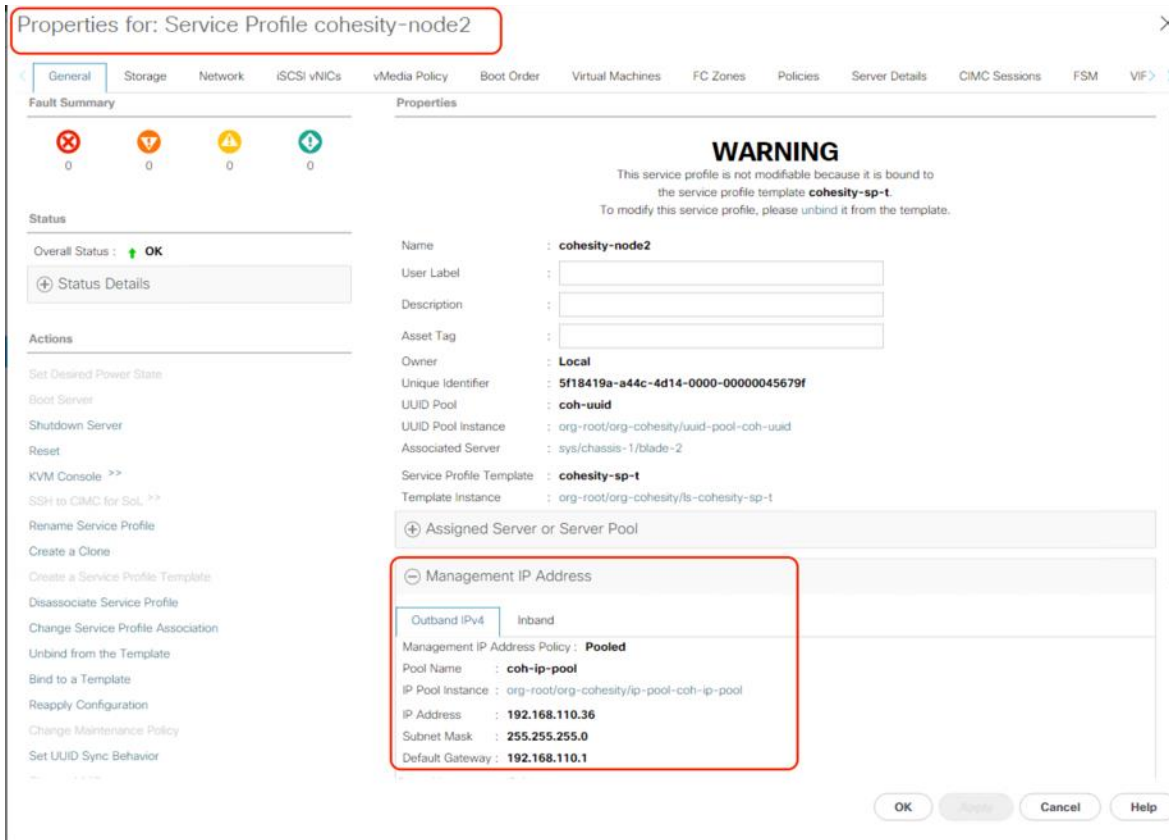
Node	IP	IPMI IP
Node 1 - 161964752899	192.0.2.1	127.5.2.2

Note: The servers may not be listed in order, please refer to Cisco UCS Manager to ensure that you are entering the IP addresses in an order that corresponds to the server node serial number and service profiles. The Cohesity installation screen lists the serial numbers of the servers, which can be cross-referenced with the Management IP of the Service Profile in Cisco UCS Manager.

Step 7. Click the Service Profile name, as marked in screenshot below and view Service Profile Properties



Step 8. Identify the IPMI address (CIMC Management IP Address) in the IPMI IP field and enter the address in the IPMI field, in the 'setup node' screen for the cohesity cluster creation and click Cancel.



Step 9. Enter the OS IP to the identified server node serial number.

Cluster Setup

Enter the IP and IPMI address for each of your selected Nodes. You need a minimum of 3 Nodes to create a Cluster.

IPv4 IPv6

Chassis FCH243075SB

Node	IP	IPMI IP
Node 1 - 161964752898	192.168.110.87	192.168.110.37

Chassis FCH243076YK

Node	IP	IPMI IP
Node 1 - 161964752896	192.168.110.85	192.168.110.35

Chassis FCH24327AMS

Node	IP	IPMI IP
Node 1 - 161964752897	192.168.110.86	192.168.110.36

Chassis FCH24327AQX

Node	IP	IPMI IP
Node 1 - 161964752899	192.168.110.88	192.168.110.38

[Continue to Cluster Settings](#)

[Back](#)

[Cancel](#)

- Step 10.** Repeat steps 7-9 and populate all the IPMI addresses corresponding to chassis server node serial numbers.
- Step 11.** Click Continue to Cluster Settings.
- Step 12.** Enter the desired name of the cluster and the DNS domain suffix.
- Step 13.** Enter the gateway IP address and subnet mask for the IP addresses being assigned to the OS and VIPs of the nodes.
- Step 14.** Enter the subnet mask and gateway address of the subnet where the nodes' IPMI interfaces are configured.
- Note:** This is the subnet mask and gateway for the IP subnet used by the CIMC interfaces, also called the external management IP addresses.
- Step 15.** Enter the username and password for IPMI access, to match the username and password configured in the Cisco UCS Manager IPMI Access Profile, which was configured earlier.
- Step 16.** Enter the required NTP server addresses, separated by commas.

-
- Step 17.** Enter the hostname for the Cohesity cluster partition. This hostname typically matches the name of the cluster.
- Step 18.** Enter the starting IP address for the VIP addresses that are being assigned to the Cohesity nodes. These IP addresses are the addresses which are resolved by DNS round-robin for the cluster, not the individual node IP addresses. For example: 192.168.110.155
- Step 19.** Enter the last octet value for the end of the VIP range, for example: 234
- Step 20.** Click Add VIP or VIP Range.
- Step 21.** Optionally, choose to enable system wide encryption by toggling the switch. Encryption can be enabled at a later time for each separately configured storage domain. Because the latter option provides more flexibility, it is not recommended to enable system wide encryption at this time, as this choice cannot be reversed.

Cohesity Dashboard

192.168.110.85/admin/cluster/setup/details

COHESITY

Cluster Setup

1 Select Nodes 2 Network Settings 3 Cluster Settings

Cluster Name *
chx-cluster03

Cluster Domain Name
lab3171.local

Cluster Subnet Gateway
192.168.110.1

Cluster Subnet Mask *
255.255.255.0

IPMI Subnet Gateway
192.168.110.1

IPMI Subnet Mask
255.255.255.0

IPMI Username
cisco

IPMI Password
***** Show Password

Search Domains

Your Cluster domain is always included in the search domains list. Separate multiple values with commas.

DNS Servers *
192.168.110.16 171.70.168.183

Separate multiple IPs with commas. E.g., 192.0.2.0, 198.51.100.0, 203.0.113.0

DNS Servers *

192.168.110.16 × 171.70.168.183 ×

Separate multiple IPs with commas. E.g., 192.0.2.0, 198.51.100.0, 203.0.113.0

NTP Servers *

Use Authentication Key

192.168.110.16 × 10.81.254.131 × 72.163.32.44 ×

Separate multiple ntp servers with commas. E.g., pool.ntp.org, 198.51.100.0, 203.0.113.0

FQDN*

chx-cluster03.lab3171.local

VIPs

VIP Address or Range	Count (Optional)
192.168.110.81	4

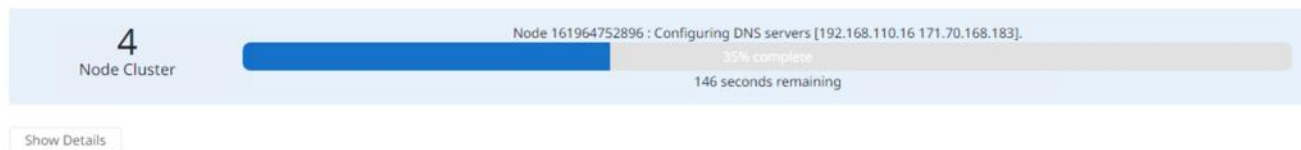
Encryption ⓘ
FIPS 140-2 validated cryptography ciphers are used.

Step 22. Click Create Cluster.

Step 23. Observe the cluster creation status. Additional details can be viewed by clicking Show Details.

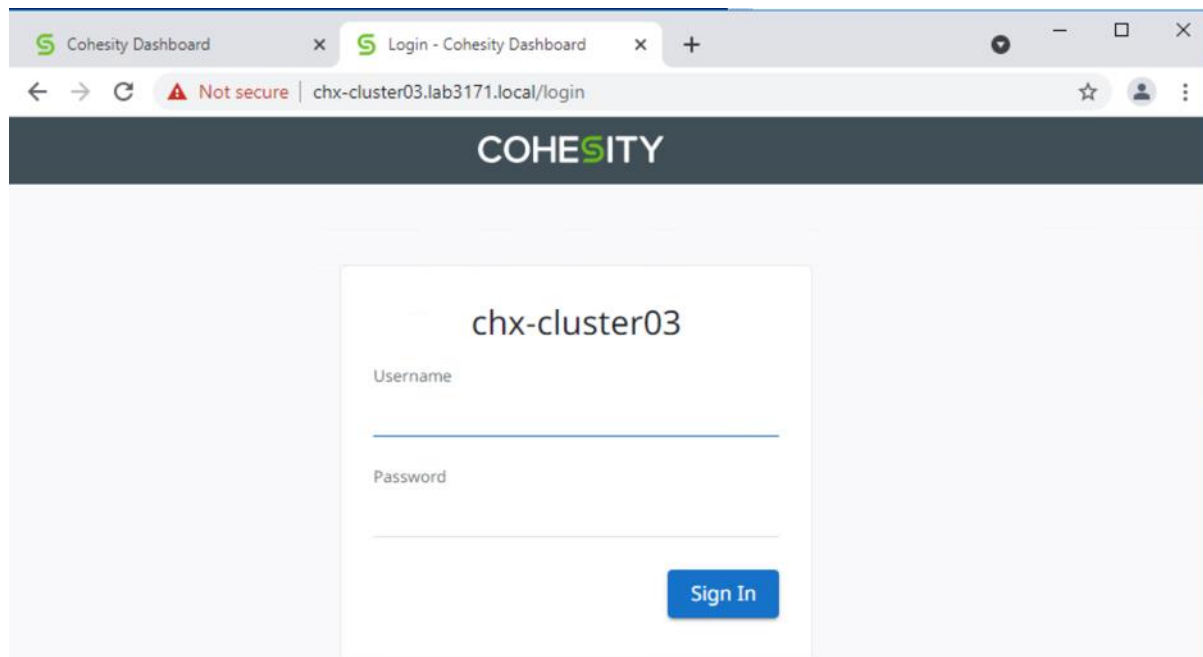
Cluster Setup Status

Your Cluster is unavailable while it is being created. When Cluster creation completes, the Cluster's URL will be displayed below.



The status will appear to pause at 98-99% for a significant period of time while formatting the disks. The time to format nodes with 16 TB capacity disks will be longer than the time for nodes with 410 TB capacity disks. The time to create the cluster for a 4-node cluster with 16 TB disks is approximately 50 minutes.

After the setup completes, the web services will restart. After a few minutes, the Cohesity Dashboard webpage for the cluster will be available at the DNS round-robin address configured for the cluster. For example: <https://chx-cluster03.lab3171.local>

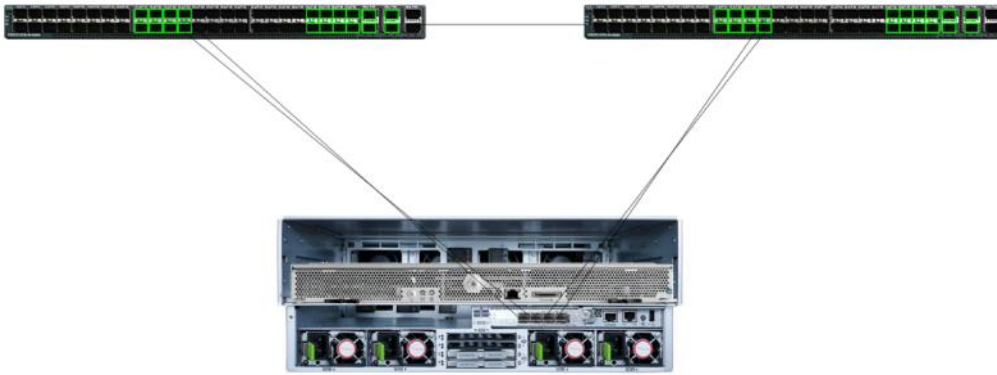


Cohesity Cluster Expansion

This section describes the Cohesity cluster expansion procedure. With Cisco UCS stateless Service Profile, the hardware configuration of new Cisco UCS S3260 storage server can be achieved in few minutes. You can just instantiate another Service Profile from the Service Profile template and associate it with the new server node configured for Cohesity cluster expansion.

Procedure 1. Configure a new Chassis for cluster expansion and view the chassis discovery status

- Step 1.** In Cisco UCS Manager, click the Equipment button and click Equipment in the top of the navigation tree.
- Step 2.** As the Server Port Auto-Discovery was set to auto, the chassis would be automatically discovered once the chassis MLOM ports are connected to the Fabric Interconnects. Ensure port 1 and port 2 of VIC 1455 are connected to Fabric Interconnect A, port 3 and port 4 are connected to Fabric Interconnect B



Step 3. Click Chassis > Chassis <n> and ensure that Chassis is discovered.

Equipment / Chassis / Chassis 4

General Servers Service Profiles Fans PSUs Hybrid Display Slots Installed Firmware SEL Logs Power Control Monitor Connectivity Policy Storage Events FSM Statistics

Fault Summary

0 0 0 0

Status

Overall Status : **Operable**

+ Status Details

Actions

- Associate Chassis Profile
- Acknowledge Chassis
- Decommission Chassis
- Remove Chassis
- Turn on Locator LED
- View POST Results
- Start Fault Suppression
- Stop Fault Suppression
- Suppression Task Properties
- Create Zoning Policy from Inventory

Physical Display

Properties

ID : 4

Product Name : **Cisco UCS S3260**

Vendor : **Cisco Systems Inc** PID : **UCSS-S3260**

Revision : 0 Serial : **FOX2241P17B**

Chassis Profile :

Locator LED :

Server SIOC Connectivity Status : **Single Server Single SIOC**

User Label :

+ Part Details

+ Power State Details

+ Connection Details

+ Power Control Details

Step 4. Under Chassis > Chassis <n> > Servers. Ensure the server node on the Cisco UCS S3260 Chassis is discovered as Server2 and is in unassociated state. In the Cohesity deployment on Cisco UCS S3260, the server node resides on Server slot 2 of the chassis. Ensure Server 2 on each chassis is discovered and is in unassociated state.

Equipment / Chassis / Chassis 4 / Servers / Server 2

General | Inventory | Virtual Machines | Installed Firmware | CIMC Sessions | SEL Logs | VIF Paths | Health | Diagnostics | Faults | Events | FSM | Statistics | Temperatures

Fault Summary

0 0 0 0

Status

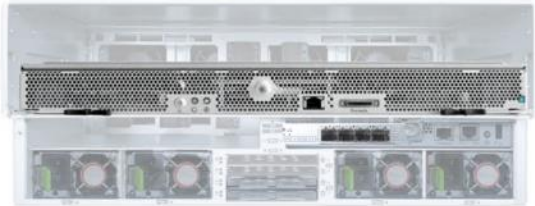
Overall Status : **Unassociated**

⊕ Status Details

Actions

- Create Service Profile
- Associate Service Profile
- Set Desired Power State
- Boot Server
- Shutdown Server
- Reset
- Recover Server
- Reset All Memory Errors
- Server Maintenance
- KVM Console >>
- SSH to CIMC for Sol. >>
- View Health LED Alarms
- Turn on Locator LED
- Unlock FP Buttons
- View POST Results
- Start Fault Suppression
- Stop Fault Suppression
- Suppression Task Properties

Physical Display



Properties

Slot ID	: 2	Chassis ID	: 4
Product Name	: Cisco UCS S3260M5		
Vendor	: Cisco Systems Inc	PID	: UCS-S3260-M5SRB
Revision	: 0	Serial	: FCH224770LR
Manufacturing Date	: 2018-11-26		
Asset Tag	:		
Name	:		
User Label	:		
Unique Identifier	: a9832994-ef3c-4acd-aa51-82bf7f49d41a		
Service Profile	:		
Health LED	: ● Normal		
Oper Qualifier Reason	:		
Locator LED	: <input type="radio"/>	FP Buttons	: <input checked="" type="checkbox"/> Locked

Summary

Number of Processors	: 2	Cores Enabled	: 36
Cores	: 36	Threads	: 72

Activate
Go to [Settings](#)

Note: The design also supports connecting just port 1 to FI A and port 3 to FI B.

Step 5. Click the Chassis tab, in the tree hierarchy, underneath Chassis Profile Template > root > Sub-Organizations, click the carat next to the name of the sib-organization and Cohesity Chassis Profile Template.

Step 6. Click Create Chassis Profile from Template.

Step 7. Enter <cohesity_chs-p> as the Chassis profile prefix.

Step 8. Enter 5 as Name Suffix Starting Number and 1 as Number of Instances.

Create Chassis Profiles From Template ? X

Naming Prefix :

Name Suffix Starting Number :

Number of Instances :

Step 9. In the tree hierarchy, underneath Chassis Profiles > root > Sub-Organizations, click the carat next to the name of the sub-organization created for Cohesity to expand it.

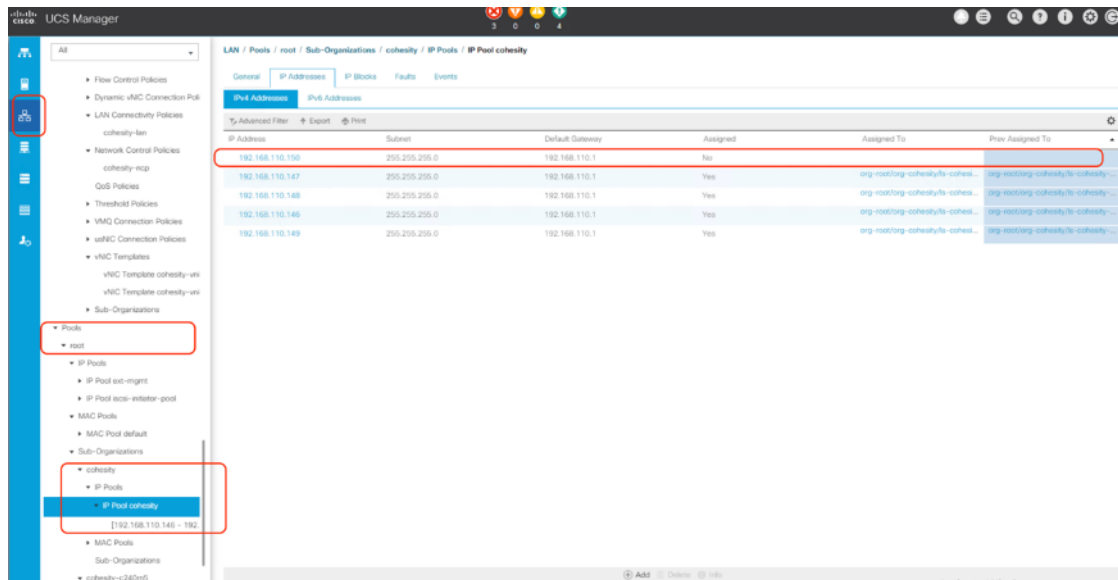
Step 10. Click the first Chassis Profile you wish to associate, then in the right-hand pane, click the blue link for “Change Chassis Profile Association”.

Step 11. Select the discovered Chassis and click OK.

Step 12. Monitor the Association of Chassis Profile in the FSM tab and ensure it succeeds.

Step 13. When Chassis is Associated to Chassis Profile, we can associate a Service Profile to server node 2 of the chassis. As we instantiated Chassis Profile from a Chassis Profile Template, we can create a Service Profile from the Service Profile Template created for Cohesity deployment.

Step 14. Ensure there is IP available in the IP Pool created for KVM management of cohesity server nodes. The figure below elaborates on the availability of in IP server Pool.



Step 15. Click the Server tab in the right pane of Cisco UCS Manager, go to Service Profile Template created for cohesity <cohesity_sp_t>.

Step 16. Right-click Template and create a Service Profile.

Create Service Profiles From Template ? ×

Naming Prefix :

Name Suffix Starting Number :

Number of Instances :

- Step 17.** When Service Profile is instantiated, we can associate it to the Service node 2 of new chassis for Cohesity cluster expansion
- Step 18.** Click the Server tab, go to Servers > Service Profiles > root > <sub-organization> and click the service profile created in the previous step.
- Step 19.** Click Change Service Profile Association, blue link and select existing server and check the server node under the S3260 Chassis.

Associate Service Profile ? ×

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

You can select an existing server or server pool, or specify the physical location of the server you want to associate with this service profile.

Server Assignment:

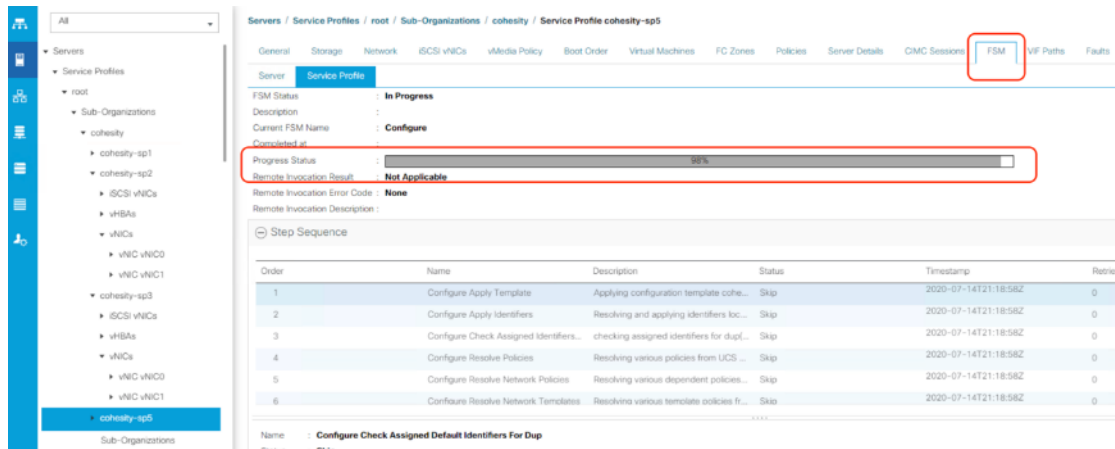
Available Servers All Servers

Select	Chassis ID	Slot	Rack ID	PID	Procs	Memory	Adapters
<input type="radio"/>			9	HX240C-M5L	2	393216	1
<input type="radio"/>			10	HX240C-M5L	2	393216	1
<input type="radio"/>			11	HX240C-M5L	2	393216	1
<input type="radio"/>			12	HX240C-M5L	2	393216	1
<input checked="" type="radio"/>	4	2		UCS-S3260-M5SRB	2	262144	1

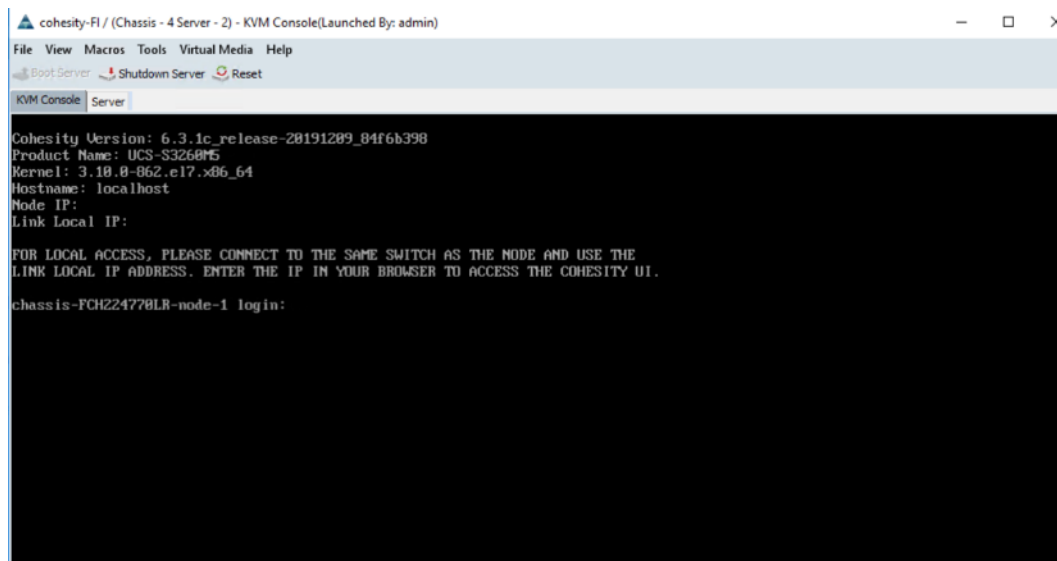
Restrict Migration :

- Step 20.** Click OK.

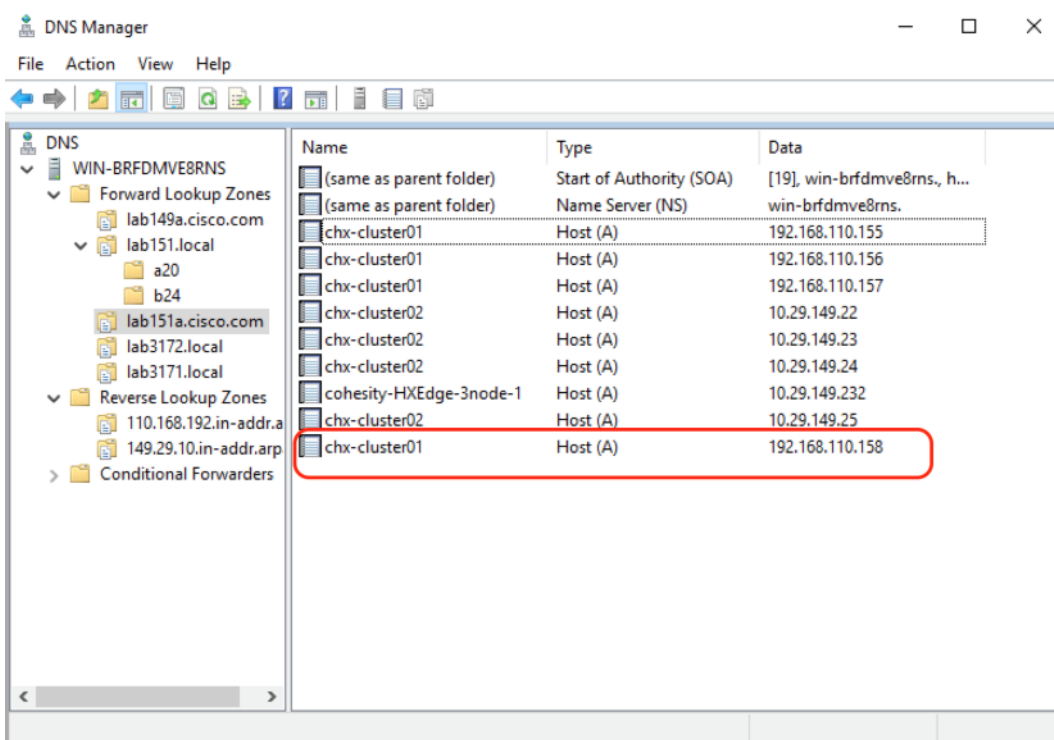
Step 21. Monitor the server association status in the Server FSM tab.



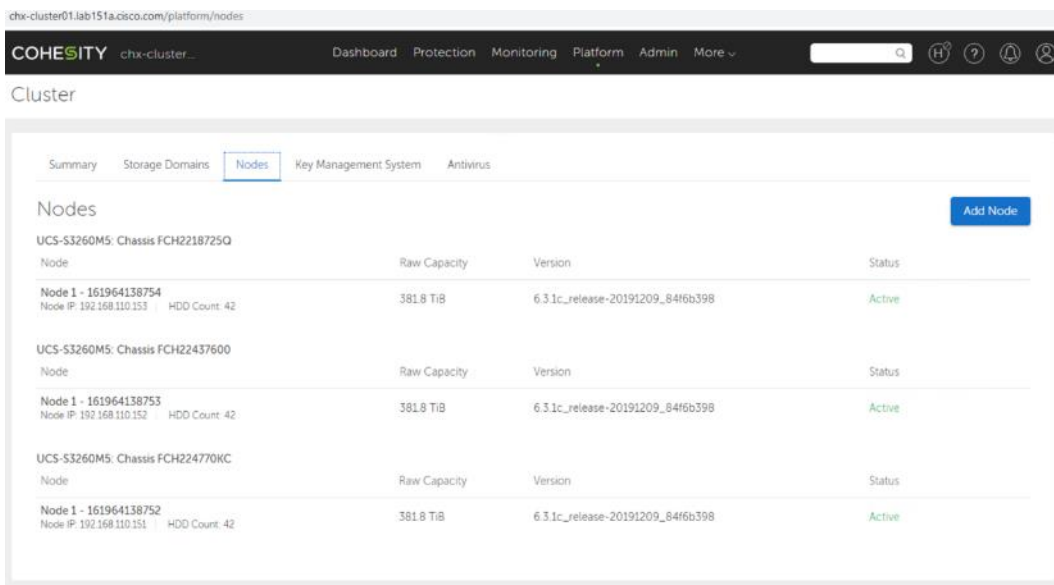
Step 22. When the server Overall status is OK we can continue to installation of Cohesity software ISO through the UCS KVM console.



Step 23. Add Virtual IP (VIP) in the DNS server for the new server node.



Step 24. Go to Cohesity Dashboard > Select Platform > Cluster and select Nodes tab.



Step 25. Click Add nodes. Cohesity Dashboard displays the new S3260 chassis node installed in the previous step.

Add Node

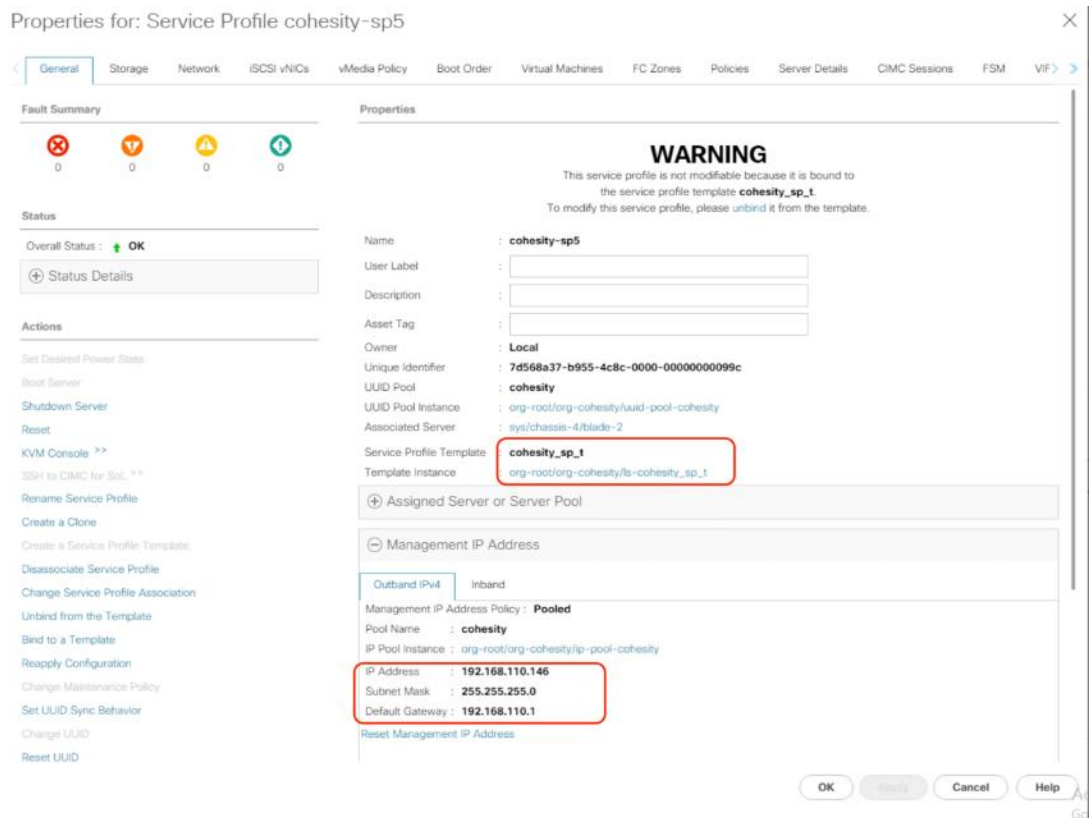
Step 26. Select the node and click Next.

Step 27. If there is a multiple node addition, the Cohesity installation screen lists the serial numbers of the server node, which can be cross-referenced with the Equipment > Chassis > Chassis <n> > Server2 view in Cisco UCS Manager. For more than one node addition, you need to traverse to all of the Chassis to identify Serial numbers of nodes in each chassis.

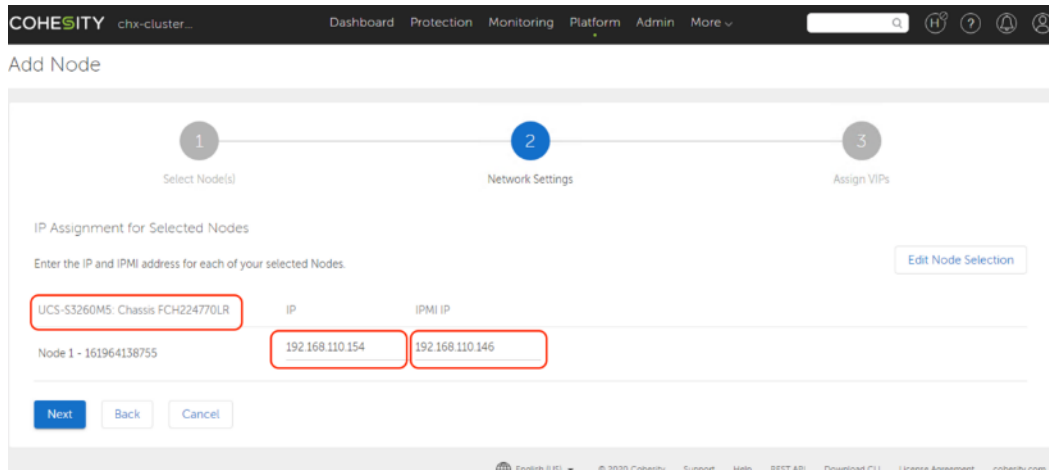
Note: For more than one node addition, the servers may not be listed in order, please refer to Cisco UCS Manager to ensure that you are entering the IP addresses in an order that corresponds to the server node serial number and service profiles. The Cohesity installation screen lists the serial numbers of the servers, which can be cross-referenced with the Management IP of the Service Profile in Cisco UCS Manager.

Step 28. Click the Service Profile name (as marked in screen above) and view Service Profile Properties.

Step 29. Identify the IPMI address (CIMC Management IP Address) in the IPMI IP field and enter the address in the IPMI field in 'setup node' screen for Cohesity cluster creation and click Cancel.

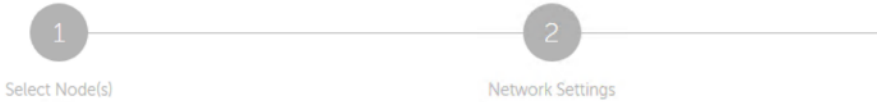


Step 30. Enter the IPMI address and OS IP Address to the identified server node serial number, click Next.



Step 31. Add the Virtual IP for the new node. This is already configured in the DNS server to map with the cluster hostname.

Add Node



Assign VIPs

VIPs

VIP Address or Range Upper Limit (Optional) Add

VIP	Delete
192.168.110.158	

Finish Back Cancel

Step 32. Click Finish. When the node addition workflow configured OS IP on the new node, go to Platform > Cluster > Nodes tab on Cohesity Dashboard and view the recently added node.

Cluster

Summary Storage Domains **Nodes** Key Management System Syslog

Nodes Configure Rack Add Node

UCS-S3260MSH16: Chassis FCH2430755B	Node	Node Serial	Raw Capacity	Version	Status
Node ID - 161964752898 Node IP: 10.20.143.59 HDD Count: 24 Node Location: Slot 1	FCH2430755B	349.1 TiB	6.6.0b_release-20210415_6b49fd10	Active	
UCS-S3260MSH16: Chassis FCH243076YK	Node	Node Serial	Raw Capacity	Version	Status
Node ID - 161964752896 Node IP: 10.20.143.57 HDD Count: 24 Node Location: Slot 1	FCH243076YK	349.1 TiB	6.6.0b_release-20210415_6b49fd10	Active	
UCS-S3260MSH16: Chassis FCH24327AM5	Node	Node Serial	Raw Capacity	Version	Status
Node ID - 161964752897 Node IP: 10.20.143.58 HDD Count: 24 Node Location: Slot 1	FCH24327AM5	349.1 TiB	6.6.0b_release-20210415_6b49fd10	Active	
UCS-S3260MSH16: Chassis FCH24327AQX	Node	Node Serial	Raw Capacity	Version	Status
Node ID - 161964752899 Node IP: 10.20.143.60 HDD Count: 24 Node Location: Slot 1	FCH24327AQX	349.1 TiB	6.6.0b_release-20210415_6b49fd10	Active	

Cohesity SmartFiles

Cohesity SmartFiles or Cohesity File and Object Services is an enterprise-class, software-defined, data-centric, multiprotocol file and object solution for the enterprise that transcends traditional offerings in terms of manageability, scale, security, efficiency and multi-tiered data management.

The present solution is targeted towards Cohesity File and Object Services on dual node Cisco UCS S3260 Storage servers. This configuration provides a dense storage platform with each compute node managing up to 384TB of storage. Customers require at a minimum of three compute node configuration. It is suggested to have a minimum of four node configuration across two Cisco UCS S3260 storage servers.

The section below elaborates on key Cohesity software components required to successfully configure Cohesity SmartFiles on Cisco UCS S3260 storage servers. For more information, go to: [File and Object Services \(SmartFiles\)](#)

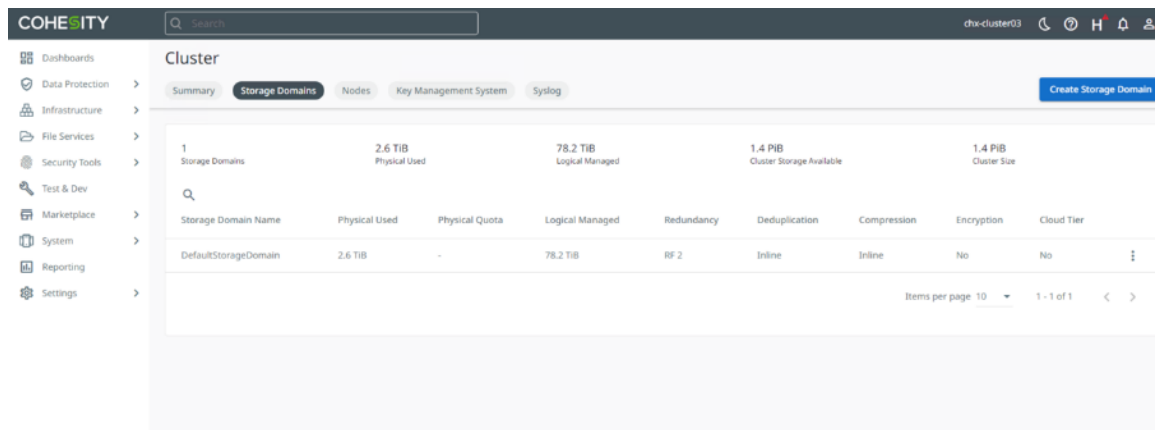
Key Components

SmartFiles utilizes the following Cohesity Cluster components.

Storage Domains

Storage Domains represent a subdivision of the default partition, and many settings can be modified at the Storage Domain level. In particular, settings for deduplication, compression, encryption, and data replication can all be controlled individually for each Storage Domain that is created. Protection Jobs and Views all target a specific Storage Domain in their configurations. When a cluster is created it provides with a default Storage Domain. New Storage Domains can be created and customized as per the intended use cases.

The figure shown below details the default storage domain created across a four node Cohesity FileServices cluster, deployed across two Cisco UCS S3260 storage chassis. Each chassis is installed with two compute nodes.

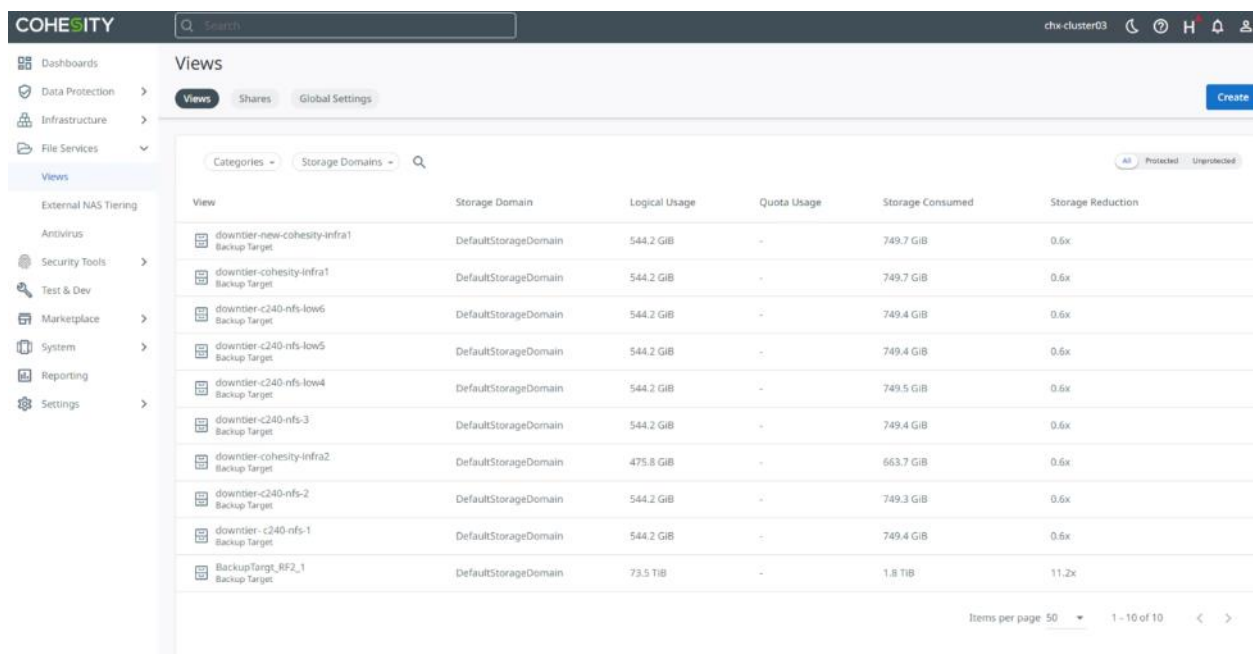


Views

A Cohesity View provides network accessible storage distributed across the Cohesity cluster, as either NFS volumes, SMB/CIFS mount paths, or S3 compliant object-based storage. A view targets a specific Cohesity storage domain, taking advantage of the settings in that domain regarding compression, deduplication, encryption, and the efficiency derived from the choice between data replication or erasure coding. In order to mount a view, the client computer must reside in a whitelisted subnet. The views created support the following protocols:

- NFS 3.0
- SMB 3.0 and SMB 2.x
- Amazon S3

The figure shown below details different views created on Cohesity FileServices cluster on the default storage domain.



View	Storage Domain	Logical Usage	Quota Usage	Storage Consumed	Storage Reduction
downTier-new-cohesity-infra1 Backup Target	DefaultStorageDomain	544.2 GiB	-	749.7 GiB	0.6x
downTier-cohesity-infra1 Backup Target	DefaultStorageDomain	544.2 GiB	-	749.7 GiB	0.6x
downTier-c240-nfs-low6 Backup Target	DefaultStorageDomain	544.2 GiB	-	749.4 GiB	0.6x
downTier-c240-nfs-low5 Backup Target	DefaultStorageDomain	544.2 GiB	-	749.4 GiB	0.6x
downTier-c240-nfs-low4 Backup Target	DefaultStorageDomain	544.2 GiB	-	749.5 GiB	0.6x
downTier-c240-nfs-3 Backup Target	DefaultStorageDomain	544.2 GiB	-	749.4 GiB	0.6x
downTier-cohesity-infra2 Backup Target	DefaultStorageDomain	475.8 GiB	-	663.7 GiB	0.6x
downTier-c240-nfs-2 Backup Target	DefaultStorageDomain	544.2 GiB	-	749.3 GiB	0.6x
downTier-c240-nfs-1 Backup Target	DefaultStorageDomain	544.2 GiB	-	749.4 GiB	0.6x
BackupTarget_RF2_1 Backup Target	DefaultStorageDomain	73.5 TiB	-	1.8 TiB	11.2x

AllowLists

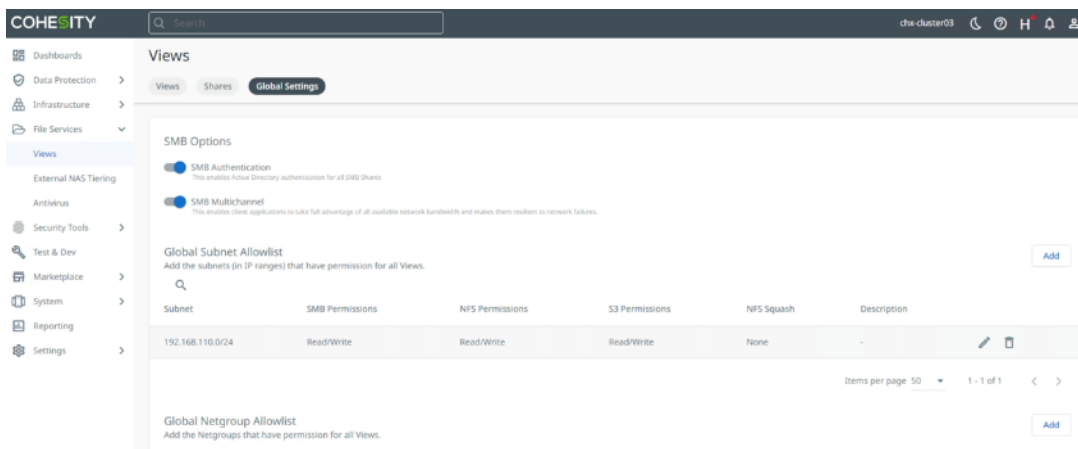
AllowList define the list of subnets. Systems with IP addresses in those subnets can mount and access views. The Cohesity cluster supports global, view-level and share-level AllowLists.

Procedure 1. Add or modify Global Subnet Allowlist

Step 1. Log into the Cohesity Dashboard web page.

Step 2. On the left management pane, click on FileServices > Views and Select Global Settings.

Step 3. You can add or edit Global Subnet Allowlist as detailed below.



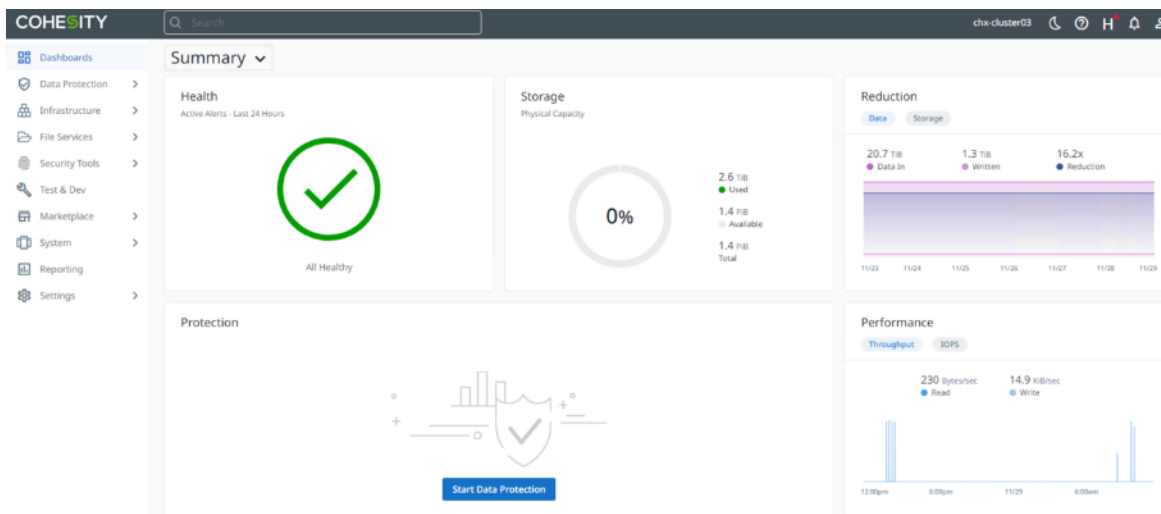
Monitoring

The Cohesity software offers numerous options for passive and proactive monitoring of the cluster, including job status, performance, hardware status, storage capacity and more.

Dashboard

The Dashboard screen in the Cohesity HTML management webpage provides a useful overview of the status of the overall system health, backup job runs, storage efficiency and performance over the past 24 hours. The dashboard allows the Cohesity administrator to see at a quick glance if any items need attention.

Figure 51. Cohesity Dashboard

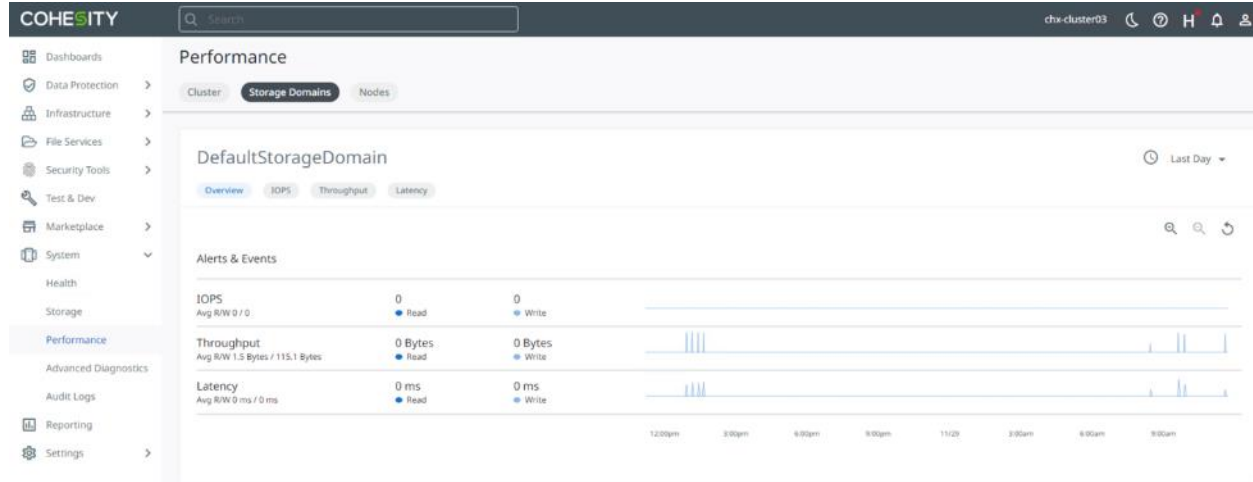


Performance

Under the SYSTEM > Monitoring menu, the Performance screen can be used to view the storage I/O per second (IOPS), latency and throughput, plus the CPU and memory usage of the nodes in the Cohesity cluster. Views can be modified to see figures for the entire cluster, individual nodes, or individ-

ual Storage Domains. The view timeframe can be modified, and the view can be zoomed in for greater detail.

Figure 52. Cohesity Performance



Alerts

Alerts in the Cohesity cluster can be viewed under the Monitoring menu by clicking Alerts. Alerts can be configured to automatically send a notice to an email recipient as well.

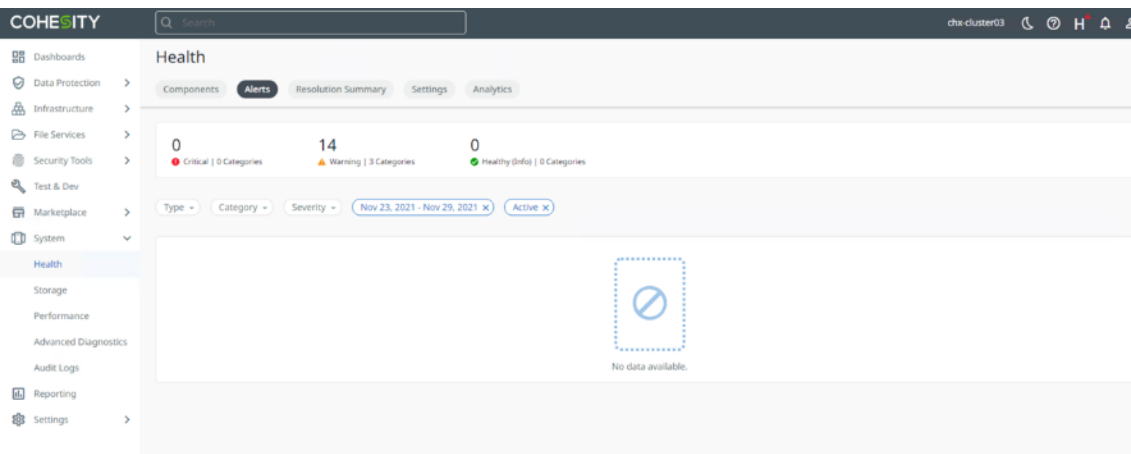
Procedure 2. View alerts

Step 4. Log into the Cohesity Dashboard web page.

Step 5. From the System menu, on the left navigation pane, select Health.

Step 6. Select Alerts on the display screen.

Figure 53. Cohesity Alerts

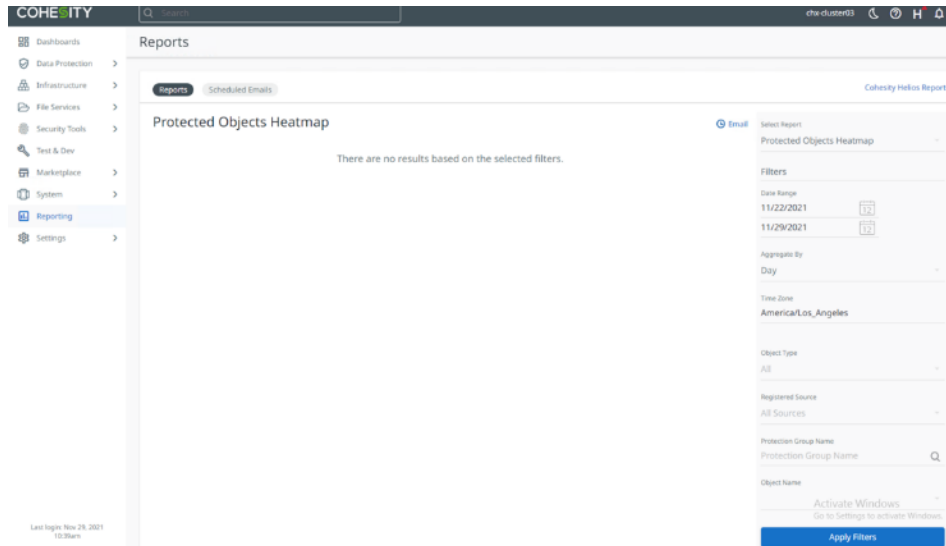


Reports

Procedure 3. Create or view reports

- Step 1.** On the right navigation pane on the Cohesity Dashboard, select Reporting.
- Step 2.** New Cohesity Helios Reports can be created from this screen.

Figure 54. Cohesity Reports



Reports can be tailored to show specific date ranges, sources, and statuses, and then configured to be regularly sent via email by clicking the email clock link. Note that not all reports can be configured to send automatically via email.

Remote Support

Cohesity offers a remote support service named Support Channel, which can be enabled for specific duration. Support Channel initiates outgoing sessions to register the Cohesity system with Cohesity's Support Channel server and technical support team. Cohesity support staff can securely connect and log into the cluster remotely for on-demand technical support and troubleshooting using SSH and secure keys. In some cases, Support Channel connections may require the use of a proxy server to function properly.

Helios

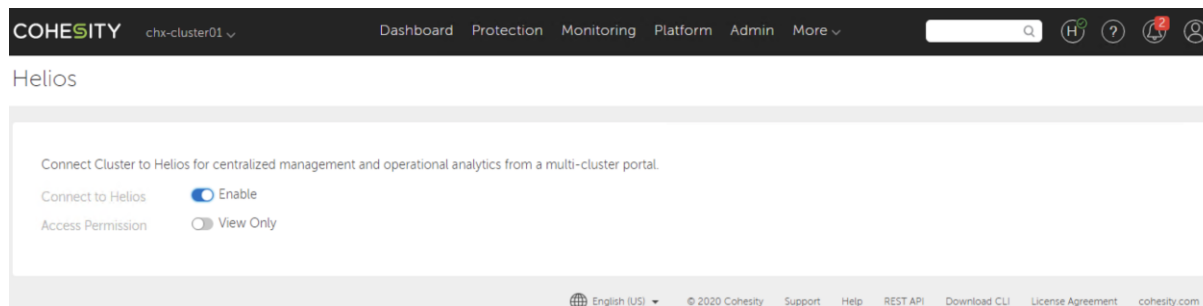
Helios is Cohesity's SaaS-based management platform that provides a single view and global management of all your Cohesity clusters, whether on-premises, cloud, or Virtual Edition, regardless of cluster size. You can quickly connect clusters to Helios and then access them from anywhere using an internet connection and your Cohesity Support Portal credentials.

For more details on Helios , see: [About Helios](#)

Procedure 4. Connect to Helios

- Step 1.** Sign into the cluster that you want to connect to Helios.
- Step 2.** In the Cohesity Dashboard, as a user with Admin privileges, click the Helios icon in the top right corner of the Dashboard and then click Enable Helios.

- Step 3.** Access Permission: If you want read-only access to the cluster in Helios, toggle on View Only. Otherwise you will have Admin privileges when accessing the cluster in Helios.
- Step 4.** Connect to Helios: Toggle on Enable. The Helios portal page is displayed.
- Step 5.** Enter your Cohesity Support Portal credentials.
- Step 6.** If the connection fails, make sure you have an internet connection and try to connect again.
- Step 7.** When the cluster is connected to Helios, a green check mark is displayed in Helios icon in the top right corner of the Cohesity Dashboard.



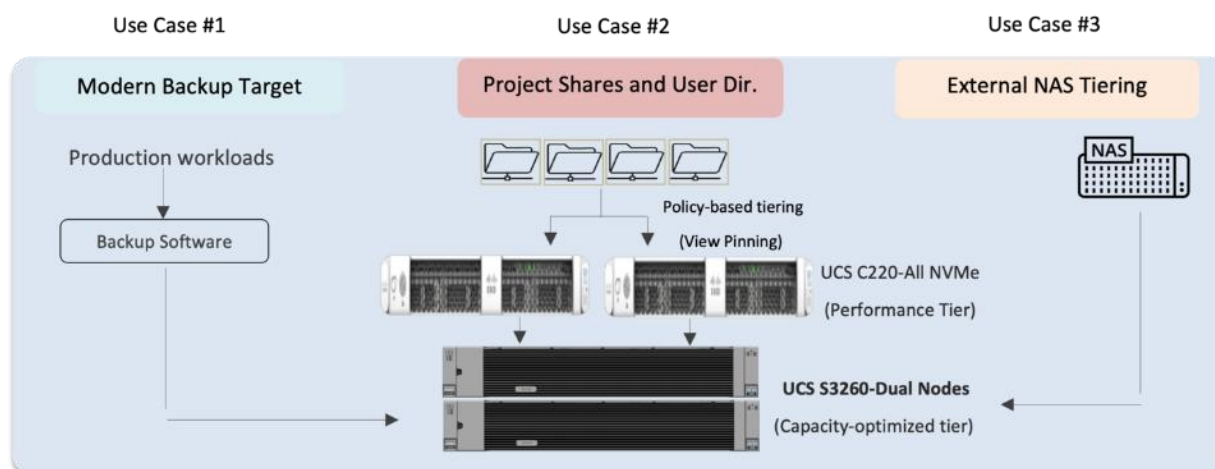
SmartFiles Use Cases and Validation

Cohesity FileServices/File and Objects Services, deployed on a dual node Cisco UCS S3260 storage server is targeted towards the following three key uses cases:

- Modern Backup Target
- Secure File Services, such as Project Shares and User Directories
- External NAS Tiering

[Figure 55](#) illustrates the key use cases for Cohesity FileServices

Figure 55. Cohesity FileServices Use Cases



The following section describes the deployment scenario and test results for each of these use cases.

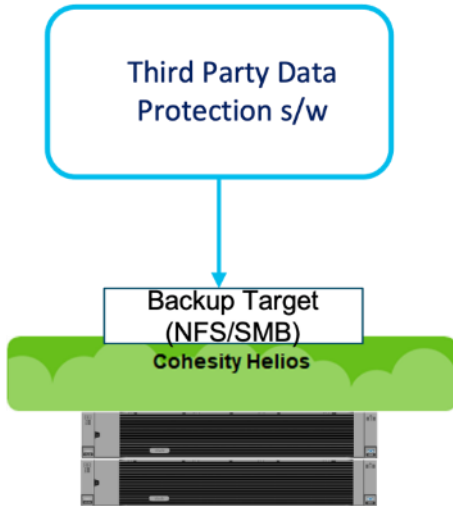
Backup Target

Cohesity NFS and SMB views can be utilized as a Backup target for data protection software. The key benefits from the various features of Cohesity Helios Platform are:

- Web-scale. Capacity grows with your business.
- Performance. Improved backup and restore times.
- Storage efficiency. Extremely high storage efficiency with global, variable-length deduplication and compression.
- Security. Your data is always secure, encrypted both at rest and in flight.
- Resilience. Highly resilient, fault-tolerant architecture.

[Figure 56](#) illustrates the Cohesity View deployed on Cisco UCS S3260 dual node configuration and leveraged for third party data protection software.

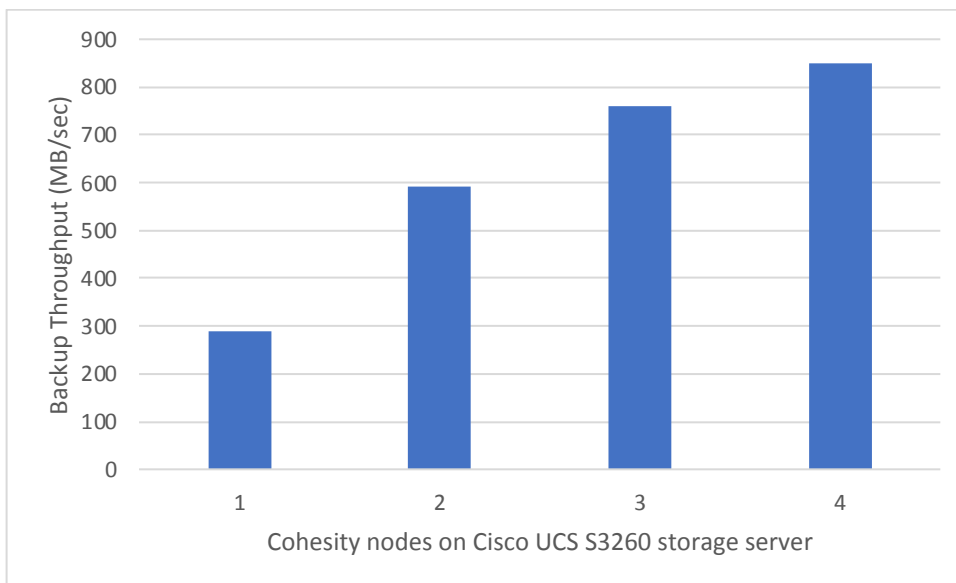
Figure 56. Backup Target



In the present test, Cohesity four node cluster was deployed across 2 x Cisco UCS S3260 chassis. Each Chassis was equipped with two compute nodes. Each compute nodes managed 24 x 16TB HDD and 4 x 3.2 TB SSDs.

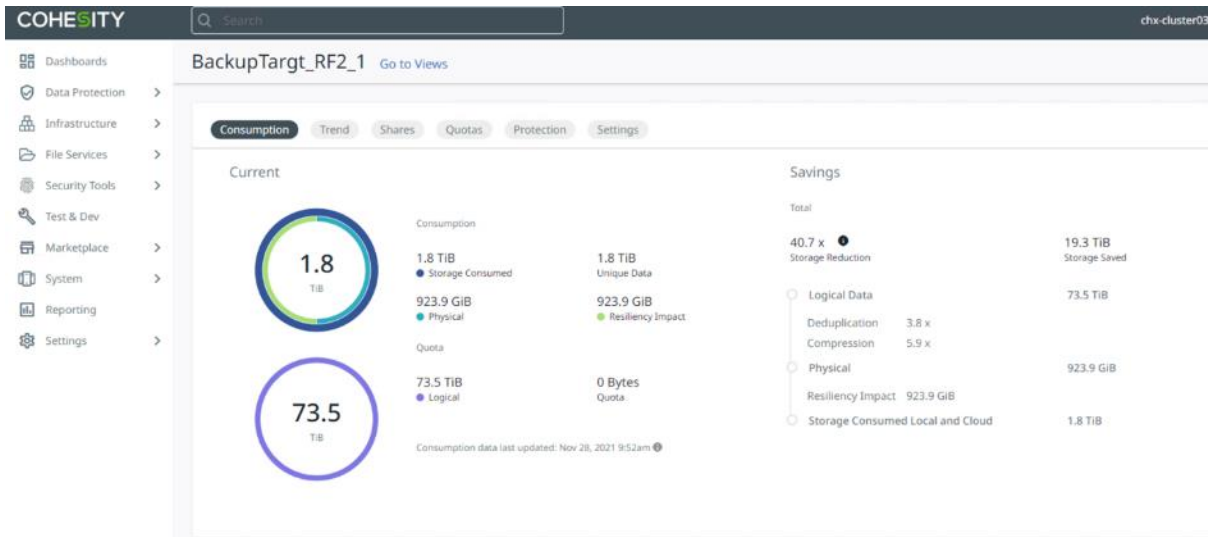
[Figure 57](#) illustrates the backup performance for a Cohesity Backup Target View when scaled from a single to a four node deployment across Cisco UCS S3260 Storage Server.

Figure 57. Cohesity performance as Backup Target



[Figure 58](#) extracted from the Cohesity Dashboard, illustrates the exceptional data efficiency achieved on Cohesity view deployed as backup target for third party backup software.

Figure 58. Data Efficiency snapshot



Secure File Services

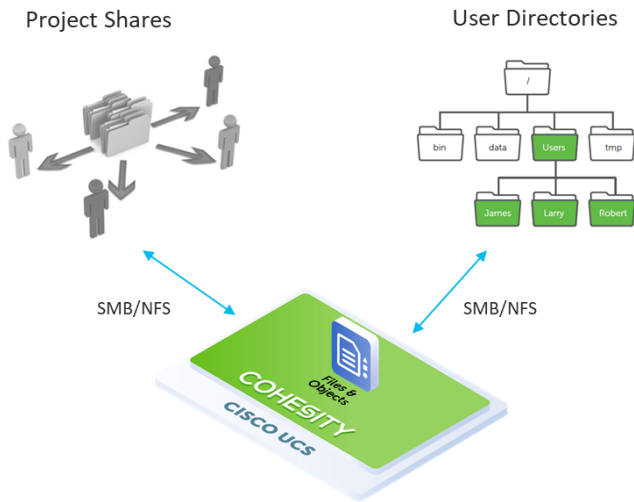
Secure file services, including Project Shares and User Directories, allow the data to be stored in a Cohesity View and can be written to faster SSD storage or slower, less expensive HDD storage, depending on the business requirement. Cohesity allows you to pin views to the SSD tier. This feature enables you to pin views to the SSD tier so that critical data and data that has to be retrieved quickly are not downtiered to HDD or cloud.

The key benefits are as follows:

- Reduced costs. considering migrating workloads to cloud services
- Prioritize NAS solutions for high performance workloads
- Move away from legacy NAS architectures
- Eliminate inefficient and costly silos and redundant file copies
- Simplify security, cyberthreat detection, encryption and data protection for files and objects

An overview of Cohesity Project Shares and User Directories deployed on dual nodes Cisco UCS S3260 storage server is illustrated [Figure 59](#).

Figure 59. Project Shares and User Directories



External NAS Tiering

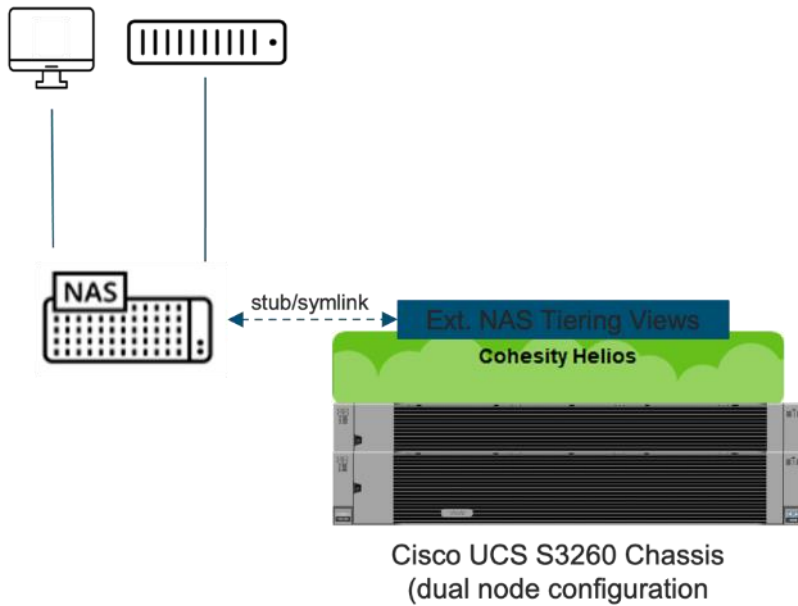
Cohesity supports the tiering of unused or infrequently used data from NAS primary storage to Cohesity cluster. The process of moving the unused data from the primary NAS storage to Cohesity cluster is called **downtiering**. Based on a tiering policy that the administrator sets while creating a data tiering job, the data from the NAS primary storage that is unused or infrequently used is periodically moved to the Cohesity cluster. When creating a data tiering job, the administrator determines how frequently the data tiering job runs, and sets a tiering policy based on various parameters, such as:

- The last time the file was accessed
- The last time the file was modified
- The size of the file
- The file type to be allowed or denied for downtiering

Once the data is tiered to Cohesity cluster, the subsequent read and write operations of the tiered data will be performed on the Cohesity server hosting the data. If the data tiered to the Cohesity cluster is frequently accessed again, then you can move the data back to the NAS primary storage by creating an uptiering job. The process of moving the frequently accessed data back from the Cohesity cluster is called **uptiering**.

[Figure 60](#) provides an overview of Cohesity NAS Tiering configuration deployed on Cisco UCS S3260 storage chassis.

Figure 60. External NAS tiering



A downtier plan for an External NAS, configured with Cohesity deployed on Cisco UCS S3260 storage Server, is shown below:

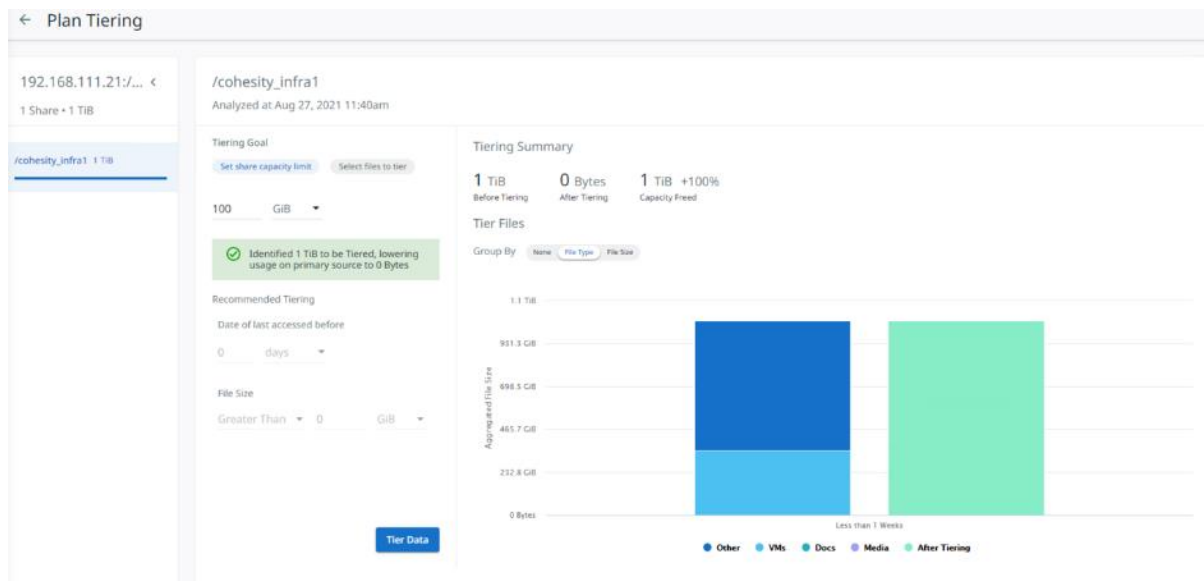
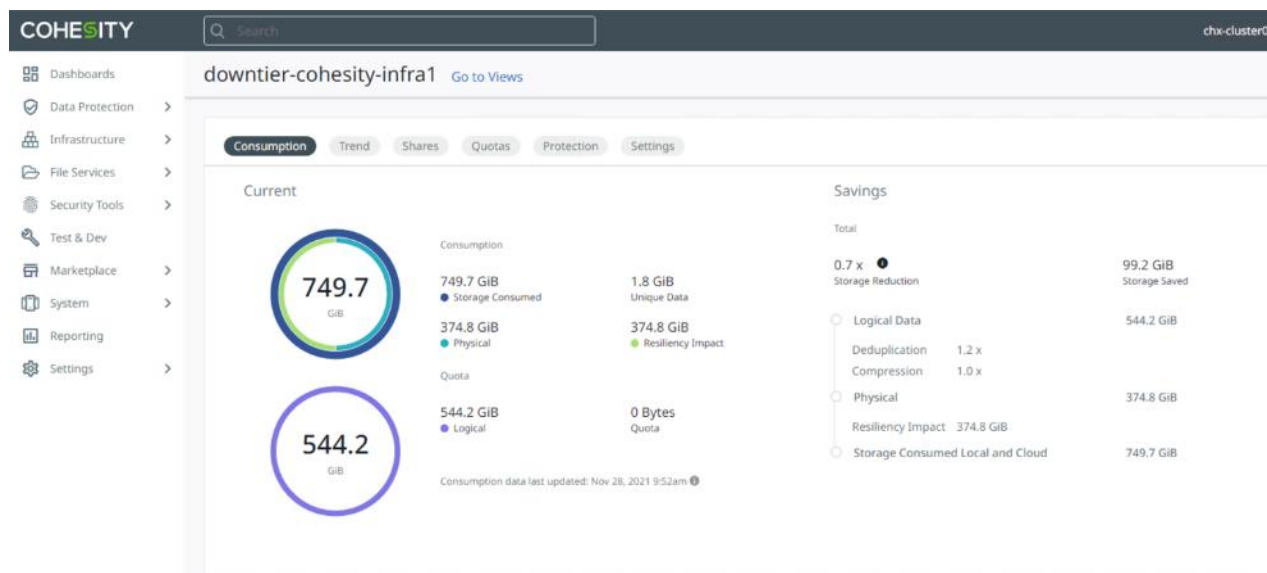


Figure 61 illustrates the storage efficiency achieved during a downtier job from an external NAS to Cohesity Helios deployed on Cisco UCS S3260 storage server.

Figure 61. Data efficiency for external NAS tiering



Failover and Redundancy Testing

The failover and redundancy testing consists of the following:

- All failover and redundancy tests were conducted while at least one active Cohesity Job was running.
- Fail the active network path for one Cohesity node.
- Fail all the network uplinks from a single Fabric Interconnect.
- Fail the active side Fabric Interconnect.

Bill of Materials

[Table 30](#) provides an example Bill of Materials used for four (4) node Cohesity SmartFiles cluster deployed on two (2) of the Cisco UCS S3260 Storage servers each equipped with two (2) compute nodes, which are compliant with the requirements to run the Cohesity Helios and Cohesity SmartFiles software, along with the pair of Cisco Fabric Interconnects, and the 25 GbE cables to connect them, as used in the testing and reference design outlined in this document.

Table 30. Cohesity FileServices (4 nodes) on Cisco UCS Bill of Materials

Cohesity FileServices on Cisco UCS Bill of Materials			
1.0.1	CON-OSP-UCSS3260	SNTC 24X7X40S, Cisco UCS S3260 Storage Server Base Chassis	2
1.1	UCS-S3260-HD16T	UCS S3260 16TB NL-SAS 7200 RPM 12Gb HDD wCarrier- Top Load	12
1.2	UCS-S3260-3KSD32	Cisco UCS S3260 Top Load 3X 3.2TB SSD	16
1.3	UCSC-PSU1-1050W	Cisco UCS 1050W AC Power Supply for Rack Server	8
1.4	CAB-N5K6A-NA	Power Cord, 200/240V 6A North America	8
1.5	CIMC-LATEST	IMC SW (Recommended) latest release for C-Series Servers.	2
1.6	N20-BKVM	KVM local IO cable for UCS servers console port	4
1.7	UCSC-C3X60-RAIL	UCS C3X60 Rack Rails Kit	2
1.8	UCSS-S3260-BBEZEL	Cisco UCS S3260 Bezel	2
1.9	UCS-S3260-M5SRB	UCS S3260 M5 Server Node for Intel Scalable CPUs	2
1.10	UCS-CPU-I4214R	Intel 4214R 2.4GHz/100W 12C/16.50MB DDR4 2400MHz	4
1.11	UCS-MR-X32G2RT-H	32GB DDR4-2933-MHz RDIMM/2Rx4/1.2v	16
1.12	UCS-S3260-DHBA	UCS S3260 Dual Pass Through based on LSI 3316	2

1.1 3	UCS-S3260-M5HS	UCS S3260 M5 Server Node HeatSink	4
1.1 4	UCS-S3260-M5SRB	UCS S3260 M5 Server Node for Intel Scalable CPUs	2
1.1 5	UCS-CPU-I4214R	Intel 4214R 2.4GHz/100W 12C/16.50MB DDR4 2400MHz	4
1.1 6	UCS-MR-X32G2RT-H	32GB DDR4-2933-MHz RDIMM/2Rx4/1.2v	16
1.1 7	UCS-S3260-DHBA	UCS S3260 Dual Pass Through based on LSI 3316	2
1.1 8	UCS-S3260-M5HS	UCS S3260 M5 Server Node HeatSink	4
1.1 9	UCS-S3260-PCISIOC	UCS S3260 PCIe SIOC	2
1.2 0	UCSC-PCIE-C25Q-04	Cisco UCS VIC 1455 Quad Port 10/25G SFP28 CNA PCIE	2
1.2 1	UCSC-LP-C25-1485	Low profile bracket for VIC	2
1.2 2	UCS-S3260-PCISIOC	UCS S3260 PCIe SIOC	2
1.2 3	UCSC-PCIE-C25Q-04	Cisco UCS VIC 1455 Quad Port 10/25G SFP28 CNA PCIE	2
1.2 4	UCSC-LP-C25-1485	Low profile bracket for VIC	2
1.2 5	UCS-S3260-42HD16	UCS S3260 3row of drives 42x 16TB SAS3 Total: 672TB	2
1.2 6	UCS-S3260-HD16T	UCS S3260 16TB NL-SAS 7200 RPM 12Gb HDD wCarrier- Top Load	84
1.2 7	UCS-S3260-G3SD24	UCS S3260 240G Boot SSD (Micron 6G SATA)	8
2.0	UCS-FI-6454-U	UCS Fabric Interconnect 6454	2

2.1	N10-MGT016	UCS Manager v4.0	2
2.2	UCS-FAN-6332	UCS 6332/ 6454 Fan Module	8
2.3	UCS-ACC-6332	UCS 6332/ 6454 Chassis Accessory Kit	2
2.4	UCS-PSU-6332-AC	UCS 6332 Power Supply/100-240VAC	4
2.5	CAB-C13-CBN	Cabinet Jumper Power Cord, 250 VAC 10A, C14-C13 Connectors	4
3.0	SFP-25G-AOC3M=	25GBASE Active Optical SFP28 Cable, 3M	16

Cohesity Certified Cisco UCS Nodes

The present solution explains the configuration of Cisco UCS S3260 storage server with Cohesity Helios Platform. Besides the present Cisco UCS S3260 Storage Server configuration, Cisco and Cohesity have certified solutions with different capacity points available on Cisco UCS C Series Rack Servers and Cisco UCS S3260 Storage servers. This allows customers to select their configuration based on key characteristics such as:

- Total Capacity
- Workload configurations such as Data Protection and File Services
- Performance requirements based on Cisco UCS C220 M5 All Flash or HDD configurations.
- Single node deployments for Remote offices and Branch offices (ROBO)
- Heterogenous configuration with mix of Cisco UCS S3260 storage sever, Cisco UCS C240 M5 LFF Rack servers, Cisco UCS C220 M5 LFF Rack Servers.
- Cohesity SmartFiles solution with Cisco UCS S3260 dual node configuration

[Table 31](#) lists the Cohesity certified nodes on Cisco UCS Platform.

Table 31. Cohesity Certified Cisco UCS Nodes

Solution Name	Cisco UCS Platform	Capacity per Node	Caching SSDs/NVMe per Node
Cohesity-C220-12TB-24TB-36TB-Nodes	Cisco UCS C220 M5 LFF Rack Server	12 TB	1.6 TB
		24 TB	1.6 TB
		36 TB	1.6 TB
Cohesity-C240-48TB-96TB-120TB-144TB-168TB-192TB-Nodes	Cisco UCS C240 M5 LFF Rack Server	48 TB	3.2 TB
		96 TB	6.4 TB
		120 TB	6.4 TB
		144 TB	6.4 TB
		168 TB	6.4 TB

Solution Name	Cisco UCS Platform	Capacity per Node	Caching SSDs/NVMe per Node
		192 TB	6.4 TB
Cohesity-C220-ROBO-8TB-and-16TB-Nodes	Cisco UCS C220 M5 LFF Rack Server	8 TB	1920 GB
		16 TB	1920 GB
Cohesity-C220-All-NVMe-Nodes	Cisco UCS C220 M5 All NVMe Rack Server	76 TB	
		80 TB	
Cohesity-S3260-210TB-294TB-420TB-588TB-704TB-768TB-Node	Cisco UCS S3260 M5 Storage Server	210 TB	12.8 TB
		294 TB	12.8 TB
		420 TB	12.8 TB
		588 TB	12.8 TB
		704 TB	12.8 TB
	Cisco UCS S3260 M5 dual node Storage Server (SmartFiles)	768 TB	25.6 TB
		384 TB 	12.8 TB

Note: **384 TB half populated S3260 chassis can only be purchased in conjunction with a dual node 768TB configuration.

About the Authors

Anil Dhiman, Technical Leader, Technical Marketing Engineering (UCS Solutions, Computing Systems Product Group, Cisco Systems, Inc.)

Anil Dhiman has nearly 20 years of experience specializing in Data Center solutions on Cisco UCS servers, and Performance Engineering of large-scale enterprise applications. Over the past 11 years, Anil has authored several Cisco Validated Designs for Enterprise Solutions on Cisco Data Center Technologies. Currently, Anil's focus is on Cisco's portfolio of Hyperconverged Infrastructure and Data Protection Solutions.

Acknowledgements

For their support and contribution to the design, validation, and creation of this Cisco Validated Design, the authors would like to thank:

- Jawwad Memon, Product Manager, Cisco Systems, Inc.
- Damien Philip, Principal Solutions Architect, Cohesity
- Tim Desai, Director, Product Marketing - SmartFiles, Cohesity

Feedback

For comments and suggestions about this guide and related guides, join the discussion on [Cisco Community](#) at <https://cs.co/en-cvds>.

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 <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)