

Design and Deployment Guide Cisco Public

# Cisco Compute Hyperconverged with Nutanix using Cohesity on Cisco UCS for Data Protection

**Design and Deployment Guide** 

Published: December 2024



In partnership with:



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

# Executive Summary

Designing and deploying a secure data protection solution is a complex challenge for organizations. It requires selecting and managing the most effective, secure, and reliable data protection and infrastructure services. In particular, backing up high-transactional and critical databases such as Microsoft SQL Server can be particularly challenging as frequent backups can impact application performance, create data inconsistencies during high transaction volumes, and require significant resources to meet low recovery time objectives (RTOs) for large datasets.

Enterprise Hyperconverged Infrastructure (HCI) solutions, such as Cisco Compute Hyperconverged with Nutanix (CCHC + N), offer simplified management, rapid deployment, cost efficiency, and scalability. Many organizations are consolidating enterprise workloads, including Microsoft SQL Server, on HCI platforms. To defend against ransomware and enable rapid recovery, customers are seeking distributed data protection solutions that combine simplified management, scalability, performance, and security, aligning with the benefits of deploying primary workloads on CCHC with Nutanix.

The Cohesity Data Cloud on Cisco UCS brings hyperconvergence to secondary data-backups, archives, file shares, object stores, test and development systems, and analytics datasets. The Data Cloud provides simplified management, scalability, secure and fast backups, instant recovery, cloud integration, and ransomware protection. Cohesity's integrated approach complements HCl in primary environments by providing robust, efficient, and flexible data protection including for SQL Server environments, ensuring that critical databases like SQL Server are well-protected and quickly recoverable.

Joint Cisco and Cohesity solutions deliver enterprise-grade security:

- Zero Trust: These principles are enforced through immutable snapshots, granular role-based access control, multifactor authentication, separation of duties via Cohesity's Quorum capabilities, and encryption.
- DataLock: Time-bound, write-once, ready-many (WORM) locks on a backup snapshot ensure data can't be modified in our file system (and extends to cloud storage by incorporating S3 object lock).
- Ransomware protection: ML-based anomaly detection safeguards against threats.
- Cisco UCS security: Hardware platform is secured from the firmware up, and a secure boot process helps ensure that the software customers intend to run is what runs.
- Automated ransomware response: Integration with Cisco XDR automates the backing up of critical data to accelerate recovery.

This Cisco Validated Design and Deployment Guide provides prescriptive guidance for the design, setup, configuration, and ongoing use of Cohesity DataProtect, part of the Cohesity Data Cloud, on the Cisco UCS C-Series Rack Servers. This unique integrated solution provides industry-leading data protection and predictable recovery with modern cloud-managed infrastructure that frees you from yesterday's constraints and future-proofs your data.

For more information on joint Cisco and Cohesity solutions, see https://www.cohesity.com/cisco.

# Solution Overview

This chapter contains the following:

- <u>Audience</u>
- Purpose of this Document
- Solution Summary

# 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 protecting enterprise workloads deployed on CCHC + N.

# **Purpose of this Document**

This document describes the design, configuration, deployment steps and validation of SQL Server protection with the Cohesity Data Cloud on Cisco UCS managed through Cisco Intersight.

# **Solution Summary**

This solution provides a reference architecture, deployment procedure and validation for protecting SQL Server on CCHC + N with the Cohesity Data Cloud on Cisco UCS managed through Cisco Intersight. At a high level, the solution delivers a simple, flexible, and scalable infrastructure approach, enabling fast backup and recoveries of enterprise applications and workloads provisioned on a hyperconverged platform. The solution also allows for consistent operations and management across Cisco infrastructure and Cohesity software environment.

The key elements of this solution are as follows:

• Cisco Intersight—is a cloud operations platform that delivers intelligent visualization, optimization, and orchestration for applications and infrastructure across public cloud and on-premises environments. Cisco Intersight provides an essential control point for you to get more value from hybrid IT investments by simplifying operations across on-prem and your public clouds, continuously optimizing their multi cloud environments and accelerating service delivery to address business needs.

• Cisco UCS C-Series platform— The Cisco UCS C240 M6 Rack Server is a 2-socket, 2-Rack-Unit (2RU) rack server offering industry-leading performance and expandability. It supports a wide range of storage and I/O-intensive infrastructure workloads, from big data and analytics to collaboration. Cisco UCS C-Series M6 Rack Servers can be deployed as standalone servers or as part of a Cisco Unified Computing System (Cisco UCS) managed environment, and now with Cisco Intersight is able to take advantage of Cisco's standards-based unified computing innovations that help reduce customers' Total Cost of Ownership (TCO) and increase their business agility.

Cohesity Data Cloud—is a unified platform for securing, managing, and extracting value from enterprise 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 and 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. The Data Cloud includes Cohesity DataProtect, Cohesity DataHawk, and more. Cohesity DataProtect—is a high-performance, secure backup and recovery solution. It converges multiple-point products into a single software that can be deployed on-premises or consumed as a service. Designed to safeguard your data against sophisticated cyber threats, it offers the most comprehensive policy-based protection for your cloud-native, SaaS, and traditional workloads.

• The Cisco Compute Hyperconverged with Nutanix family of appliances delivers pre-configured Cisco UCS servers that are ready to be deployed as nodes to form Nutanix clusters in a variety of configurations. Each server appliance contains three software layers: UCS server firmware, hypervisor (Nutanix AHV), and hyperconverged storage software (Nutanix AOS). Physically, nodes are deployed into clusters, with a cluster consisting of Cisco Compute Hyperconverged All-Flash Servers. Clusters support a variety of workloads like virtual desktops, general-purpose server virtual machines in edge, data center and mission-critical high-performance environments. Nutanix clusters can be scaled out to the max cluster server limit documented by Nutanix.

• SQL Server 2022 on Microsoft windows 2022 is the latest relational database from Microsoft and builds on previous releases to grow SQL Server as a platform that gives you choices of development languages, data types, on-premises or cloud environments, and operating systems.

Figure 1 illustrates the solution overview detailed in this design

#### Figure 1. Solution Overview



# **Technology Overview**

This chapter contains the following:

- <u>Cisco Intersight Platform</u>
- Cisco UCS C240 M6 Large Form Factor (LFF) Rack Server.
- <u>Cisco Compute Hyperconverged HCIAF240C M7 All-NVMe/All-Flash Servers</u>
- <u>Cisco XDR and Cohesity Data Cloud Integration</u>
- <u>Cohesity Data Cloud</u>

The components deployed in this solution are configured using best practices to deliver an enterprise-class data protection solution deployed on Cisco UCS C-Series Rack Servers. This join solution is validated to protect enterprise workloads such as Microsoft SQL Server deployed on Cisco Compute Hyperconverged with Nutanix (CCHC + N). The upcoming sections provide a summary of the key features and capabilities available across the deployment architecture.

# **Cisco Intersight Platform**

As applications and data become more distributed from core data center and edge locations to public clouds, a centralized management platform is essential. IT agility will be a struggle without a consolidated view of the infrastructure resources and centralized operations. Cisco Intersight provides a cloud-hosted, management and analytics platform for all Cisco Compute for Hyperconverged, Cisco UCS, and other supported third-party infrastructure deployed across the globe. It provides an efficient way of deploying, managing, and upgrading infrastructure in the data center, ROBO, edge, and co-location environments.



Cisco Intersight provides:

- No Impact Transition: Embedded connector (Cisco HyperFlex, Cisco UCS) will allow you to start consuming benefits without forklift upgrade.
- SaaS/Subscription Model: SaaS model provides for centralized, cloud-scale management and operations across hundreds of sites around the globe without the administrative overhead of managing the platform.
- Enhanced Support Experience: A hosted platform allows Cisco to address issues platform-wide with the experience extending into TAC supported platforms.

• Unified Management: Single pane of glass, consistent operations model, and experience for managing all systems and solutions.

• Programmability: End to end programmability with native API, SDK's and popular DevOps toolsets will enable you to deploy and manage the infrastructure quickly and easily.

• Single point of automation: Automation using Ansible, Terraform, and other tools can be done through Intersight for all systems it manages.

• Recommendation Engine: Our approach of visibility, insight and action powered by machine intelligence and analytics provide real-time recommendations with agility and scale. Embedded recommendation platform with insights sourced from across Cisco install base and tailored to each customer.

For more information, go to the Cisco Intersight product page on <u>cisco.com</u>.

# **Cisco Intersight Virtual Appliance and Private Virtual Appliance**

In addition to the SaaS deployment model running on Intersight.com, you can purchase on-premises options separately. The Cisco Intersight virtual appliance and Cisco Intersight private virtual appliance are available for organizations that have additional data locality or security requirements for managing systems. The Cisco Intersight virtual appliance delivers the management features of the Cisco Intersight platform in an easy-to-deploy VMware Open Virtualization Appliance (OVA) or Microsoft Hyper-V Server virtual machine that allows you to control the system details that leave your premises. The Cisco Intersight private virtual appliance is provided in a form factor designed specifically for users who operate in disconnected (air gap) environments. The private virtual appliance requires no connection to public networks or to Cisco network.

# **Licensing Requirements**

The Cisco Intersight platform uses a subscription-based license with multiple tiers. You can purchase a subscription duration of 1, 3, or 5 years and choose the required Cisco UCS server volume tier for the selected subscription duration. Each Cisco endpoint automatically includes a Cisco Intersight Base license at no additional cost when you access the Cisco Intersight portal and claim a device. You can purchase any of the following higher-tier Cisco Intersight licenses using the Cisco ordering tool:

- Cisco Intersight Essentials: Essentials includes all the functions of the Base license plus additional features, including Cisco UCS Central software and Cisco Integrated Management Controller (IMC) supervisor entitlement, policy-based configuration with server profiles, firmware management, and evaluation of compatibility with the Cisco Hardware Compatibility List (HCL).
- Cisco Intersight Advantage: Advantage offers all the features and functions of the Base and Essentials tiers. It also includes storage widgets and cross-domain inventory correlation across compute, storage, and virtual environments (VMware ESXi). OS installation for supported Cisco UCS platforms is also included.

Servers in the Cisco Intersight managed mode require at least the Essentials license. For more information about the features provided in the various licensing tiers, go to:

https://www.intersight.com/help/saas/getting\_started/licensing\_requirements

# Cisco UCS C240 M6 Large Form Factor (LFF) Rack Server

The Cisco UCS C240 M6 Rack Server is a 2-socket, 2-Rack-Unit (2RU) rack server offering industry-leading performance and expandability. It supports a wide range of storage and I/O-intensive infrastructure workloads, from big data and analytics to collaboration. Cisco UCS C-Series M6 Rack Servers can be deployed as standalone servers or as part of a Cisco Unified Computing System (Cisco UCS) managed environment, and now with Cisco Intersight is able to take advantage of Cisco's standards-based unified computing innovations that help reduce customers' Total Cost of Ownership (TCO) and increase their business agility.

In response to ever-increasing computing and data-intensive real-time workloads, the enterprise-class Cisco UCS C240 M6 server extends the capabilities of the Cisco UCS portfolio in a 2RU form factor. It incorporates 3rd Generation Intel Xeon Scalable processors, supporting up to 40 cores per socket and 33 percent more memory versus the previous generation.

The Cisco UCS C240 M6 rack server brings many new innovations to the Cisco UCS rack server portfolio. With the introduction of PCIe Gen 4.0 expansion slots for high-speed I/O, DDR4 memory bus, and expanded storage capabilities, the server delivers significant performance and efficiency gains that will improve your application performance. Its features including the following:

- Supports the third-generation Intel Xeon Scalable CPU, with up to 40 cores per socket
- Up to 32 DDR4 DIMMs for improved performance, including higher density DDR4 DIMMs (16 DIMMs per socket)
- 16x DDR4 DIMMs + 16x Intel Optane persistent memory modules for up to 12 TB of memory
- Up to 8 PCIe Gen 4.0 expansion slots plus a modular LAN-on-motherboard (mLOM) slot
- · Support for Cisco UCS VIC 1400 Series adapters as well as third-party options
- 16 LFF drives with options 4 rear SFF (SAS/SATA/NVMe) disk drives

• Support for a 12-Gbps SAS modular RAID controller in a dedicated slot, leaving the remaining PCIe Gen 4.0 expansion slots available for other expansion cards

- M.2 boot options
  - Up to 960 GB with optional hardware RAID
- Up to five GPUs supported

• Modular LAN-on-motherboard (mLOM) slot that can be used to install a Cisco UCS Virtual Interface Card (VIC) without consuming a PCIe slot, supporting quad port 10/40 Gbps or dual port 40/100 Gbps network connectivity

- Dual embedded Intel x550 10GBASE-T LAN-on-motherboard (LOM) ports
- Modular M.2 SATA SSDs for boot

#### Figure 2. Front View: Cisco UCS C240 M6 Large Form Factor (LFF) server

	A D		
10-00	Market and a second sec		
tibidir. Eiseo			US CONTRACTOR



#### Figure 3. Rear View: Cisco UCS C240 M6 Large Form Factor (LFF) server

# **Cisco UCS VICs**

Cisco UCS C240 M6 Rack Server support the following Cisco MLOM VICs and PCIe VICs:

- Cisco UCS VIC 1467 quad port 10/25G SFP28 mLOM
- Cisco UCS VIC 1477 dual port 40/100G QSFP28 mLOM
- Cisco UCS VIC 15428 quad port 10/25/50G MLOM
- Cisco UCS VIC 15238 dual port 40/100/200G MLOM
- Cisco UCS VIC 15427 Quad Port CNA MLOM with Secure Boot
- Cisco UCS VIC 15237, MLOM, 2x40/100/200G for Rack
- Cisco UCS VIC 1495 Dual Port 40/100G QSFP28 CNA PCIe
- Cisco UCS VIC 1455 quad port 10/25G SFP28 PCIe
- Cisco UCS VIC 15425 Quad Port 10/25/50G CNA PCIE
- Cisco UCS VIC 15235 Dual Port 40/100/200G CNA PCIE

In the present configuration with the Cohesity Data Cloud, Cisco UCS VIC 1467 quad port 10/25G SFP28 mLOM with deployed on Cisco UCS C240 M6 LFF server.

#### Cisco VIC 1467

The Cisco UCS VIC 1467 is a quad-port Small Form-Factor Pluggable (SFP28) mLOM card designed for Cisco UCS C-Series M6 Rack Servers. The card supports 10/25-Gbps Ethernet or FCoE. The card can present PCle standards-compliant interfaces to the host, and these can be dynamically configured as either NICs or HBA. For more details visit, <u>https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/unified-computing-system-adapters/datasheet-c78-741130.html</u>

#### Figure 4. Cisco UCS VIC 1467



Figure 5. Cisco UCS VIC 1467 Infrastructure



# **Cisco UCS 6400 Fabric Interconnects**

The Cisco UCS fabric interconnects provide a single point for connectivity and management for the entire Cisco UCS system. Typically deployed as an active-active pair, the fabric interconnects of the system integrate all

components into a single, highly available management domain that Cisco UCS Manager or the Cisco Intersight platform manages. Cisco UCS Fabric Interconnects provide a single unified fabric for the system, with low-latency, lossless, cut-through switching that supports LAN, storage-area network (SAN), and management traffic using a single set of cables (Figure 6).

Figure 6. Cisco UCS 6454 Fabric Interconnect

The Cisco UCS 6454 used in the current design is a 54-port fabric interconnect. This 1RU device includes twenty-eight 10-/25-GE ports, four 1-/10-/25-GE ports, six 40-/100-GE uplink ports, and sixteen unified ports that can support 10-/25-GE or 8-/16-/32-Gbps Fibre Channel, depending on the Small Form-Factor Pluggable (SFP) adapter.

# Cisco Compute Hyperconverged HCIAF240C M7 All-NVMe/All-Flash Servers

The Cisco Compute Hyperconverged HCIAF240C M7 All-NVMe/All-Flash Servers extends the capabilities of Cisco's Compute Hyperconverged portfolio in a 2U form factor with the addition of the 4th Gen Intel<sup>®</sup> Xeon<sup>®</sup> Scalable Processors (codenamed Sapphire Rapids), 16 DIMM slots per CPU for DDR5-4800 DIMMs with DIMM capacity points up to 256GB.

The All-NVMe/all-Flash Server supports 2x 4th Gen Intel<sup>®</sup> Xeon<sup>®</sup> Scalable Processors (codenamed Sapphire Rapids) with up to 60 cores per processor. With memory up to 8TB with 32 x 256GB DDR5-4800 DIMMs, in a 2-socket configuration. There are two servers to choose from:

- HCIAF240C-M7SN with up to 24 front facing SFF NVMe SSDs (drives are direct-attach to PCIe Gen4 x2)
- HCIAF240C-M7SX with up to 24 front facing SFF SAS/SATA SSDs

For more details, go to: HCIAF240C M7 All-NVMe/All-Flash Server specification sheet

#### Figure 7. Front View: HCIAF240C M7 All-NVMe/All-Flash Servers

CISCO	102.68	101.50	000.00	820 CB		320 60	820 Q.B	010 GB	100 GB	ALCO GR	801 (JB	820 GB	HOD GR	820 GB	201.68	102.05	EDE GR	BOLGS	100.58	800 GB	100.68	800.08	UCS C240 M/

# **Cisco XDR and Cohesity Data Cloud Integration\***

The powerful combination of Cisco XDR with Cohesity minimizes data loss during a ransomware attack through early and rapid response. The first integration of this kind in the industry, this solution reduces the time between threat detection and backing up critical data to near zero. When indications of a ransomware attack are detected, Cisco XDR triggers a snapshot request of the targeted assets, ensuring your organization has a clean and current backup. Backup snapshots can be quickly recovered to a clean room environment to expedite digital forensics and recovery activities, thus reducing recovery time objectives (RTOs). Workloads backed up by Cohesity and monitored by Cisco XDR for threats can be scanned using Cohesity DataHawk's highly accurate, ML-based engine for sensitive data, including personally identifiable information (PII), PCI, and HIPAA.

Note: \* supports VMware environments only.

Figure 8. Cisco XDR and the Cohesity Data Cloud Integration Workflow



# **Cohesity Data Cloud**

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 Data Cloud platform takes this same three-tier hyperscaler architectural approach and adapts it to the specific needs of enterprise data management.

Helios is the user interface or control plane in which all customers interact with their data and Cohesity products. It 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.

# SpanFS: A Unique File System that Powers the Cohesity Data Cloud Platform

The foundation of the Cohesity Data Cloud 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, the Data Cloud 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 as shown in Figure 9.



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.

# Architecture and Design Considerations

This chapter contains the following:

- Deployment Architecture for Cisco UCS C-Series with Cohesity
- Network Bond Modes with Cohesity and Cisco UCS Fabric Interconnect Managed Systems
- Licensing
- Software Components

# **Deployment Architecture for Cisco UCS C-Series with Cohesity**

The Cohesity Data Cloud on Cisco UCS C-Series nodes requires a minimum four (4) nodes. Each Cisco UCS node is equipped with both the compute and storage required to operate the Data Cloud and Cohesity storage domains to protect application workloads such as SQL Server on Cisco Compute Hyperconverged with Nutanix (CCHC + N)

Figure 10 illustrates the deployment architecture overview of Cohesity on Cisco UCS C-Series nodes, protecting SQL Server on CCHC with Nutanix.

#### Figure 10. Deployment Architecture Overview



Figure 11 illustrates the cabling diagram for protection of SQL Server on CCHC with Nutanix through Cohesity on Cisco UCS C-Series servers.



**Note:** Figure 11 does not showcase the CCHC with Nutanix cluster. Review the CVD for <u>CCHC with</u> <u>Nutanix for SQL Server</u> for the deployment configuration.

**Note:** The Cisco UCS C-Series Servers are connected directly to the Cisco UCS Fabric Interconnects in Direct Connect mode. Internally the Cisco UCS C-Series servers are configured with the PCIe-based system I/O controller for Quad Port 10/25G Cisco VIC 1467. 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.

**Note:** Do not connect port 1 of the VIC 1467 (quad port 10/25G) to Fabric Interconnect A, and then connect port 2 of the VIC 1467 to Fabric Interconnect B. Using ports 1 and 2, each connected to FI A and FI B will lead to discovery and configuration failures.

The Cohesity Data Cloud on Cisco UCS C-Series requires a minimum four (4) nodes. Each Cisco UCS C240 M6 LFF node is equipped with both the compute and storage required to operate the Cohesity cluster. The entire deployment is managed through Cisco Intersight.

Each Cisco UCS C240 M6 LFF node was deployed in Intersight Managed Mode (IMM) and is equipped with:

- 2x Intel 6326 (2.9GHz/185W 16C/24MB DDR4 3200MHz)
- 128 GB DDR4 memory
- 2x 240GB M.2 card managed through M.2 RAID controller for the Cohesity Data Cloud operating system
- 2x 6.4 TB NVMe
- 16x 12TB,12G SAS 7.2K RPM LFF HDD (4K) managed through 1x Cisco M6 12G SAS HBA

In addition to Cisco UCS C-Series nodes for Cohesity Data Cloud, the entire deployment includes:

• Two Cisco Nexus 93360YC-FX Switches in Cisco NX-OS mode provide the switching fabric.

• Two Cisco UCS 6454 Fabric Interconnects (FI). One 100 Gigabit Ethernet port from each FI, configured as a Port-Channel, is connected to each Cisco Nexus 93360YC-FX. Cisco UCS Fabric Interconnect was deployed in IMM mode and is managed through Cisco Intersight.

• Cisco Intersight as the SaaS management platform for both Cisco UCS C-Series nodes for Cohesity and . Cisco Compute Hyperconverged with Nutanix.

Cisco UCS nodes for SQL Server on Nutanix and the Cohesity Data Cloud were connected to separate switches providing separation of Primary and Secondary workloads. In general, it is recommended to replicate the Backups to a secondary site with addition to archives of primary workload backups on Cohesity Cluster. Deployment and cabling diagram can be referenced from Cisco Validated design, <u>SQL Server on Cisco Compute Hyperconverged with Nutanix</u>

# Network Bond Modes with Cohesity and Cisco UCS Fabric Interconnect Managed Systems

All teaming/bonding methods that are switch independent are supported in the Cisco UCS Fabric Interconnect environment. These bonding modes do not require any special configuration on the switch/UCS side.

The restriction is that any load balancing method used in a switch independent configuration must send traffic for a given source MAC address via a single Cisco UCS Fabric Interconnect other than in a failover event (where the traffic should be sent to the alternate fabric interconnect) and not periodically to redistribute load.

Using other load balancing methods that operate on mechanisms beyond the source MAC address (such as IP address hashing, TCP port hashing, and so on) can cause instability since a MAC address is flapped between Cisco UCS Fabric Interconnects. This type of configuration is unsupported.

Switch dependent bonding modes require a port-channel to be configured on the switch side. The fabric interconnect, which is the switch in this case, cannot form a port-channel with the VIC card present in the servers. Furthermore, such bonding modes will also cause MAC flapping on Cisco UCS and upstream switches and is unsupported.

Cisco UCS Servers with Linux Operating System and managed through fabric interconnects, support activebackup (mode 1), balance-tlb (mode 5) and balance-alb (mode 6). The networking mode in the Cohesity operating system (Linux based) deployed on Cisco UCS C-Series or Cisco UCS X-Series managed through a Cisco UCS Fabric Interconnect is validated with bond mode 1 (active-backup). For reference, go to: <u>https://www.cisco.com/c/en/us/support/docs/servers-unified-computing/ucs-b-series-blade-</u> <u>servers/200519-UCS-B-series-Teaming-Bonding-Options-wi.html</u>

# Licensing

# **Cisco Intersight Licensing**

Cisco Intersight uses a subscription-based license with multiple tiers. Each Cisco automatically includes a Cisco Intersight Essential trial license when you access the Cisco Intersight portal and claim a device. The Essential Tier allows configuration of Server Profiles for Cohesity on Cisco UCS C-Series Rack Servers.

More information about Cisco Intersight Licensing and the features supported in each license can be found here: <u>https://www.cisco.com/site/us/en/products/computing/hybrid-cloud-operations/intersight-infrastructure-service/licensing.html</u>

In this solution, using Cisco Intersight Advantage License Tier enables the following:

- Cohesity Data Cloud operating system installation through Cisco Intersight OS install feature. Customers have to download certified Cohesity Data Cloud software and provide a local NFS, CIFS or HTTPS repository.
- Tunneled vKVM access, allowing remote KVM access to Cohesity nodes.

# **Software Components**

<u>Table 1</u> lists the software components and the versions required for the Cohesity Data Cloud and Cisco UCS C-Series Rack Servers, as tested, and validated in this document.

Component	Version
Cohesity Data Cloud	cohesity-6.8.2_u1_release-20240509_a5da4644-redhat
Cisco Fabric Interconnect 6454	4.3(4.240066)
Cisco C240 M6 LFF servers	4.3(4.240152)
AOS and AHV bundled	nutanix_installer_package-release-fraser-6.5.5.6
Prism Central	pc.2024.1.0.2
AHV	5.10.194-5.20230302.0.991650.el8.x86_64
Cisco C240 M7 All NVMe server	4.3(3.240043)
VirtlO Driver	1.2.3-x64

#### Table 1. Software Components

# Solution Deployment

This chapter contains the following:

- Prerequisites
- <u>Create Cisco Intersight Account</u>
- Intersight Managed Mode Setup (IMM)
- Set up Domain Profile
- Manual Setup Server Template
- Install Cohesity on Cisco UCS C-Series Nodes
- Configure Cohesity Data Cloud

This chapter describes the solution deployment for the Cohesity Data Cloud on Cisco UCS C-Series Rack Servers in Intersight Managed Mode (IMM), with step-by-step procedures for implementing and managing the solution.

# **Prerequisites**

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

# **IP Addressing**

IP addresses for the Cohesity Data Cloud on Cisco UCS C-Series, need to be allocated from the appropriate subnets and VLANs to be used. IP addresses that are used by the system are comprised of the following groups:

• **Cisco UCS Management:** These addresses are used and assigned as management IPs for Cisco UCS Fabric interconnects. Two out of band, IP addresses are used; one address is assigned to each Cisco UCS Fabric Interconnect, this address should be routable to https://intersight.com or you can have proxy configuration.

**Note:** For more details on claiming Fabric Interconnects on Intersight, please refer <u>Device connector</u> <u>configuration</u> page

• **Cisco C240 M6 LFF node management**: Each Cisco C240 M6 LFF server/node, is managed through an IMC Access policy mapped to IP pools through the Server Profile. Both In-Band and Out of Band configuration is supported for IMC Access Policy. One IP is allocated to each of the node configured through In-Band or Out of Band access policy. In the present configuration each Cohesity node is allocated both In-Band and Out of Band Access Policy. This allocates (two)2 IP addresses for each node using the IMC Access Policy

• **Cohesity Operating System IP:** 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 as the Cisco UCS Management addresses, or they may be separate.

• Once Cohesity cluster is configured, Customers have the option to configure sub-interfaces through Cohesity Dashboard. This allows accessibility to **multiple networks** through different VLANs.

**Note: OS Installation through Intersight** for FI-attached servers in IMM requires an In-Band Management IP address.(ref: <u>https://intersight.com/help/saas/resources/adding\_OSimage</u>). Deployments not using In-Band Management address can install OS by mounting the ISO through KVM.

**Note:** Cohesity on Cisco UCS C-Series Servers **do not support IPMI configuration**. In this configuration, Cisco UCS C-Series nodes are attached to Cisco Fabric Interconnect and do not utilize IPMI configuration. Therefore, in the following table, the IPMI IPs are defined as 0.0.0.0

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.

Address Group:	UCS Management		Cohesity Cluster Nodes			
VLAN ID:			< <this be="" n<br="" should="">tagged on the uplin</this>	ative VLAN or k switch>>		
Subnet Mask:						
Gateway:						
DNS						
NTP						
Device	KVM Management Addresses (Out of Band)	KVM Management Addresses (In-Band)	Node IP	Node IPMI IP		
Fabric Interconnect A						
Fabric Interconnect B						
Cohesity Node #1						
Cohesity Node #2						
Cohesity Node #3						
Cohesity Node #4						

Table 2.	Cohesity	Cluster	IP	Addressing

Note: <u>Table 3</u> is a true representation of configuration deployed during Solution Validation.

Address Group:	UCS Mana	gement	Cohesity Cluster Nodes			
VLAN ID:	KVM Management Addresses (Out of Band)	KVM Management Addresses (In-Band)	Node IP	Node IPMI IP		
Subnet Mask:	255.255.255.0	255.255.255.0	255.255.255.0	< <black>&gt;</black>		
Gateway:	10.108.0.254	10.108.0.254	10.108.1.254	< blank>>		
DNS	10.108.1.6		10.108.1.6			
NTP	172.20.10.18		172.20.10.18			
Device	KVM Management Addresses (Out of Band)	KVM Management Addresses (In-Band)	Node IP	Node IPMI IP		
Fabric Interconnect A	10.108.0.161					
Fabric Interconnect B	10.108.0.162					
Cohesity Node #1	10.108.0.163	10.108.0.167	10.108.1.163	0.0.0.0		
Cohesity Node #2	10.108.0.164	10.108.0.168	10.108.1.164	0.0.0.0		
Cohesity Node #3	10.108.0.165	10.108.0.169	10.108.1.165	0.0.0.0		
Cohesity Node #4	10.108.0.166	10.108.0.170	10.108.1.166	0.0.0		

#### Table 3. Example Cohesity Cluster IP Addressing

#### 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 /		Server	Information
lable 4.	DING	Server	mormation

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

Item	Value	A Records
UCS Domain Name		
Cohesity Cluster Name		

#### Table 5. DNS Server Example Information

ltem	Value	A Records
DNS Server #1	10.108.0.6	
DNS Server #2		
DNS Domain		
UCS Domain Name		

# 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 6. NTP Server Information

Item	Value
NTP Server #1	
NTP Server #2	
Timezone	

Table 7. NTP Server Example Information

Item	Value
NTP Server #1	10.108.0.6
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. Only the VLAN for the Cohesity Application group needs to be trunked to the two Cisco UCS Fabric Interconnects that manage the Cohesity cluster. The VLAN IDs must be supplied during the Cisco UCS configuration steps, and the VLAN names should be customized to make them easily identifiable.

**Note:** Ensure all VLANs are part of LAN Connectivity Policy defined in Cisco Server Profile for each Cisco UCS C-Series node.

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

Name	ID
< <in-band vlan="">&gt;</in-band>	
< <cohesity_vlan>&gt;</cohesity_vlan>	

#### Table 9. VLAN Example Information

Name	ID
< <in-band vlan="">&gt;</in-band>	1080
< <cohesity_vlan>&gt;</cohesity_vlan>	1081

# **Network Uplinks**

The Cisco UCS uplink connectivity design needs to be finalized prior to beginning the installation.

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

#### Table 10. Network Uplink Configuration

Fabric Interconnect Port	Port Channel	Port Channel Type	Port Channel ID	Port Channel Name
	🗆 Yes 🗆 No	□ LACP		
	🗆 Yes 🗆 No	□ vPC		
A	🗆 Yes 🗆 No			
	🗆 Yes 🗆 No			
	□ Yes □ No			
	🗆 Yes 🗆 No	□ vPC		
В	🗆 Yes 🗆 No			
	□ Yes □ No	-		

Fabric Interconnec	t Port	Port Channel	Port Channel Type	Port Channel ID	Port Channel Name
	1/53	🖾 Yes 🗆 No	LACP		
	1/54	🖾 Yes 🗆 No	⊠ vPC		
A		🗆 Yes 🗆 No		61	Vpc61
		🗆 Yes 🗆 No			
	1/53	🛛 Yes 🗆 No	LACP		
	1/54	🛛 Yes 🗆 No	⊠ vPC		
В	8	□ Yes □ No		62	Vpc62
		🗆 Yes 🗆 No			

#### **Table 11.** Network Uplink Example Configuration

#### **Usernames and Passwords**

Several usernames and passwords need to be defined or known as part of the Cohesity installation and configuration process.

Use the following table to list the required username and password information and review an example configuration.

#### Table 12. Usernames and Passwords

Account	Username	Password
Cohesity Administrator	admin	< <cohesity_admin_pw>&gt;</cohesity_admin_pw>

#### **Create Cisco Intersight Account**

**Procedure 1.** Create an account on Cisco Intersight

**Note:** Skip this step if you already have a Cisco Intersight account.

The procedure to create an account in Cisco Intersight is explained below. For more details, go to: <a href="https://intersight.com/help/saas/getting\_started/create\_cisco\_intersight\_account">https://intersight.com/help/saas/getting\_started/create\_cisco\_intersight\_account</a>

**Step 1.** Go to https://intersight.com/ to create your Intersight account. You must have a valid Cisco ID to create a Cisco Intersight account.

Step 2. Click Create an account.

	cisco Intersight © Englis	sh
	Welcome to Intersight Don't have an Intersight Account? Create an account	
	Sign In with Cisco ID	
	Don't have a Cisco ID? Sign Up	
	Or	
	Email	
	Sign In with SSO	
	Help Center Terms Privacy Cookles © 2022 Cisco Systems, Inc.	
Step 3. Sign-In with your Cisco I	D.	
Step 4. Select Region		
$\leftarrow$ $\rightarrow$ C O A https://intersight.com/onboar	rding/acct/	
ೆಟ್ಟ್ Intersight		

and Intersight	
	Select Region
	Region * ① US East ~
	Cancel Next

Step 5. Read the End User License Agreement and select I accept and click Next.

ende Intersight	
	General Terms Please read the general terms carefully.
	OVERVIEW <ul> <li>By clicking accept or using the Cisco Technology, you agree that such use is governed by the Cisco Ceneral Terms and the applicable Product Specific Terms(collectively, the "Agreement"). You also acknowledge and agree that you have read the Cisco Privacy Statement and the Privacy Data Sheet for Cisco Cloud Services delivered by the Intersight Platform.   how read the Cisco Privacy Statement and the Privacy Data Sheet for Cisco Cloud Services delivered by the Intersight Platform.             If you do not have authority to bind your company and its affiliates, or if you do not              Z</li></ul>
	Cancel Next



www.Intersight	
	Account Creation
	Cancel Create

Step 7. Register for Smart Licensing or Start Trial.

tintersight	
	Licensing
	If you have purchased license tiers for Cisco Intersight Services you can register smart licensing to start using the services.
	Register Smart Licensing
	Or
	If you would like to evaluate Intersight Services you can register for a trial.
	Start Trial

Step 8. Select Infrastructure Service & Cloud Orchestrator and click Start Trial.

Start Trial
Select the Intersight Service to request trial.  Infrastructure Service & Cloud Orchestrator 90 days trial
Workload Optimizer Registration Required 45 days trial

Step 9. One logged in, browse through different services on the top left selection option

ē	••• Overview   Intersight	× +	
← -	> C	0 A https://us-east-1.intersight.com/an/infrastructure-service/an/infrast	tructure/over
≡	disco Intersight	°se Infrastructure Service ∨	
;@:	Overview	. Expand All	
(0)	Operate /	Cloud Orchestrator	
	Integrated Systems	My Dachboard	Se
©,	Analyze		36
	Explorer New	. System	
.0	Configure	Explore More Services 🖸	
	Profiles	HyperFlex Cluster Health Summary	
	Templates	6	
	Policies	No Hyperflex Clusters	
	Pools	Capacity Utilization	

**Note:** Go to: <u>https://intersight.com/help/saas</u> to configure Cisco Intersight Platform.

# Intersight Managed Mode Setup (IMM)

#### Procedure 1. Set up Cisco Intersight Managed Mode on Cisco UCS Fabric Interconnects

The Cisco UCS Fabric Interconnects need to be set up to support Cisco Intersight managed mode. When converting an existing pair of Cisco UCS fabric interconnects from Cisco UCS Manager mode to Intersight Manage Mode (IMM), first erase the configuration and reboot your system.

**Note:** Converting fabric interconnects to Cisco Intersight Managed Mode is a disruptive process, and configuration information will be lost. You are encouraged to make a backup of their existing configuration. If a software version that supports Intersight Managed Mode (4.1(3) or later) is already installed on Cisco UCS Fabric Interconnects, do not upgrade the software to a recommended recent release using Cisco UCS Manager. The software upgrade will be performed using Cisco Intersight to make sure Cisco UCS C-Series firmware is part of the software upgrade.

**Step 1.** Configure Fabric Interconnect A (FI-A). On the Basic System Configuration Dialog screen, set the management mode to Intersight. All the remaining settings are similar to those for the Cisco UCS Manager Managed Mode (UCSM-Managed).

Cisco UCS Fabric Interconnect A
To configure the Cisco UCS for use in a FlexPod environment in ucsm managed mode, follow these steps: Connect to the console port on the first Cisco UCS fabric interconnect
Enter the configuration method. (console/gui) ? console
Enter the management mode. (ucsm/intersight)? <b>intersight</b>
The Fabric interconnect will be configured in the intersight managed mode. Choose (y/n) to proceed: y
Enforce strong password? (y/n) [y]: Enter
Enter the password for "admin": <password> Confirm the password for "admin": <password></password></password>
Enter the switch fabric (A/B) []: A
Enter the system name: <ucs-cluster-name></ucs-cluster-name>
Physical Switch Mgmt0 IP address : <ucsa-mgmt-ip></ucsa-mgmt-ip>
Physical Switch Mgmt0 IPv4 netmask : <ucs-mgmt-mask></ucs-mgmt-mask>
IPv4 address of the default gateway : <ucs-mgmt-gateway></ucs-mgmt-gateway>
DNS IP address : <dns-server-1-ip></dns-server-1-ip>
Configure the default domain name? (yes/no) [n]: y
Default domain name : <ad-dns-domain-name></ad-dns-domain-name>
Following configurations will be applied:
Management Mode=intersight Switch Fabric=A
System Name= <ucs-cluster-name></ucs-cluster-name>
Enforced Strong Password=yes Physical Switch MomtO IP Address= <ucsa-momt-in></ucsa-momt-in>
Physical Switch Mgmt0 IP Netmask= <ucs-mgmt-mask></ucs-mgmt-mask>
Default Gateway= <ucs-mgmt-gateway></ucs-mgmt-gateway>
DNS Server= <dns-server-l-ip> Domain Name=<ad-dns-domain-name></ad-dns-domain-name></dns-server-l-ip>
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes

**Step 2.** After applying the settings, make sure you can ping the fabric interconnect management IP address. When Fabric Interconnect A is correctly set up and is available, Fabric Interconnect B will automatically discover Fabric Interconnect A during its setup process as shown in the next step.

**Step 3.** Configure Fabric Interconnect B (FI-B). For the configuration method, select console. Fabric Interconnect B will detect the presence of Fabric Interconnect A and will prompt you to enter the admin password for Fabric Interconnect A. Provide the management IP address for Fabric Interconnect B and apply the configuration.

```
Cisco UCS Fabric Interconnect B
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: <password>
Connecting to peer Fabric interconnect... done
Retrieving config from peer Fabric interconnect... done
Peer Fabric interconnect Mgmt0 IPv4 Address: <ucsa-mgmt-ip>
Peer Fabric interconnect Mgmt0 IPv4 Netmask: <ucs-mgmt-mask>
Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv4 Address
Physical Switch Mgmt0 IP address : <ucsb-mgmt-ip>
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

#### Procedure 2. Set Up Cisco Intersight Organization and Roles

An organization is a logical entity which enables multi-tenancy through separation of resources in an account. The organization allows you to use the Resource Groups and enables you to apply the configuration settings on a subset of targets.

#### **Role-Based Access Control in Intersight**

Intersight provides Role-Based Access Control (RBAC) to authorize or restrict system access to a user, based on user roles and privileges. A user role in Intersight represents a collection of the privileges a user has to perform a set of operations and provides granular access to resources. Intersight provides role-based access to individual users or a set of users under Groups.

**Note:** To learn and configure more about Organizations and Roles in Intersight , please refer https://intersight.com/help/saas/resources/RBAC#role-based access control in intersight

**Note:** In the present solution, "default" organization is used for all configurations. "Default" organization is automatically created once an Intersight account is created.

#### Procedure 3. Claim Cisco UCS Fabric Interconnects in Cisco Intersight

**Note:** Make sure the initial configuration for the fabric interconnects has been completed. Log into the Fabric Interconnect A Device Console using a web browser to capture the Cisco Intersight connectivity information.

**Step 1.** Use the management IP address of Fabric Interconnect A to access the device from a web browser and the previously configured admin password to log into the device.

**Step 2.** Under DEVICE CONNECTOR, the current device status will show "Not claimed." Note or copy, the Device ID, and Claim Code information for claiming the device in Cisco Intersight.

← → C O Not secure https://10.108.0.161/an/device-connector/	
India Device Console AA09-FI-DP-6454	
System Information Device Connector Inventory Diagnostic Data	
The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platfo connector, please visit Help Center	rm. For detailed information about configuring the device
Device Connector	③ Settings   〇 Refresh
ACCESS MODE ALLOW CONTROL	Device ID Claim Code
Not Claimed  The connection to the Cisco Intersight Portal is successful, but device is still not claimed. To claim the device open Cisco Intersight, create a new account and follow the guidance or go to the Targets page and click Claim a New Device for existing account.	

- Step 3. Log into Cisco Intersight.
- **Step 4.** Select System. Click Administration > Targets.
- Step 5. Click Claim a New Target.
- **Step 6.** Select Cisco UCS Domain (Intersight Managed) and click Start.

#### ← Targets **Claim a New Target** Select Target Type Filters Q Search Compute / Fabric Available for Claiming 습 습 습 altalta cisco 0 alialia cisco diada cisco Categories Cisco UCS Server Cisco UCS Domain Cisco UCS Domain (Standalone) (Intersight Managed) (UCSM Managed) All O Cloud 습 습 -ili-ili-cisco O Compute / Fabric Cisco UCS C890 Hyperconverged Redfish Server Network Platform Services Orchestrator 습 습 습 Platform Services altalta cisco diala cisco alialia cisco Intersight Workload Cisco Intersight Cisco Intersight Assist Appliance Engine Cloud 7 Terraform Cloud Orchestrator 습 습 습 diada cisco Cisco UCS Director PowerShell Endpoint HTTP Endpoint 습 습 Ansible Endpoint SSH Endpoint Hyperconverged 습 altalta cisco Cisco HyperFlex Cluster Cancel Start

- Step 7. Copy and paste the Device ID and Claim from the Cisco UCS FI to Intersight.
- **Step 8.** Select the previously created Resource Group and click Claim.

- Targets (	Claim a New Target   Int 🗴 🟦 CIMC	🛪 🛛 🎎 Cisco IMC Login Page 🛛 🗙 🗍 🕮 Cisco IMC Login	Page × +				-	0
< → C	us-east-1.intersight.com/an/system/a	an/asset/targets/create/cisco-ucs-fiism/?\$currentPage=18c5pageSize=10					☆	+
	Intersight 📲 System 🗸		Q Search		C ©	41 Q 💿	• • • • •	2   2
© C	Targets Claim a New Target Claim Cisco UCS Domain (Inte To claim your target, provide the Device General Device ID* ① Resource Groups	rsight Managed) Target ID, Claim Code and select the appropriate Resource Groups.						
	Select resource groups, if ret     Name	quired. This is not mandatory, since by default, the clair ded target will be a Usage NO ITEMS AVAILABLE	added to "All" type resource groups. Description	©				

Step 9. With a successful device claim, Cisco UCS FI should appear as a target in Cisco Intersight:

isco In	itersight 🛛 📲 System 🗸				Q Search	C O 4 000	• •
Tai	rgets				0	Your target has been successfully claim	ied.
*	k All Targets 🛞 +						
	0 🔋 🗌 📿 Search		Filters 1 results				📥 Exp
	Health	Connection	Top Targets by Types	Vendor			
	1 Healthy 1	O Connected 1	1 Intersight Managed 1	Cisco Systems, Inc. 1			
	Name	: Health	: Status	: Туре	: Claimed Time	Claimed By	
(	AA09-FI-DP-6454	O Healthy	Connected	Intersight Managed Domain	a few seconds ago	andhiman@cisco.com	
						Rows per page 10 ~	

**Step 10.** In the Cisco Intersight window, click Settings and select Licensing. If this is a new account, all servers connected to the Cisco UCS domain will appear under the Base license tier. If you have purchased Cisco Intersight licenses and have them in your Cisco Smart Account, click Register and follow the prompts to register this Cisco Intersight account to your Cisco Smart Account. Cisco Intersight also offers a one-time 90-day trial of Advantage licensing for new accounts. Click Start Trial and then Start to begin this evaluation. The remainder of this section will assume Advantage licensing. A minimum of Cisco Intersight Essentials licensing is required to configure Cisco UCS C-Series in Intersight Managed Mode (IMM)

#### Procedure 4. Verify Addition of Cisco UCS Fabric Interconnects to Cisco Intersight

Step 1. Log into the web GUI of the Cisco UCS fabric interconnect and click the browser refresh button.

 Device Console
 AA09-FI-DP-6454

 System Information
 Device Connector
 Inventory
 Diagnostic Data

 The Device Connector is an embedded management controler that enables the capabilities of Cisco intersight, a coust-based management platform. For detailed information about configuring the device connector passes visit Heip Center

 Device Connector
 Intersignt

 Device Connector
 Intersignt

The fabric interconnect status should now be set to Claimed.

Step 2. Select Infrastructure Service.

≡	Cisco Intersight	📲 System 🗸
0	Settings	Manage compute and converged infrastructure operations.
•	Admin /	Cloud Orchestrator
	Software Repository Tech Support Bundles	Workload Optimizer
	Audit Logs	My Dashboard
	Sessions	System
		Explore More Services

**Step 3.** Go to the Fabric Interconnects tab and verify the pair of fabric interconnects are visible on the Intersight dashboard.

" Intersignt Intrastruct	ure Service 🗸			Q Search	C⊘	\$1 Q (	0 (1) (2)
Fabric Interconnect	s						
* All Fabric Interconne							
··· 🧷 Q Search	₹ Fi	Iters 2 results					( 🛧 E)
Health	Connection	Bundle Version NX-OS	Version Mod	dels			
2 Healthy 2	Connected 2	2 • 4.2(3h) 2 2	■ 9.3(5)142(3f) 2	2 6454 2			
Name	: Health	: Model	: Bundle Version	uCS Domain Profile	Total	Ports Used	Available
AA09-FI-DP-6454 FI-A	O Healthy	UCS-FI-6454	4.2(3h)		54	0	54
	(B) Manufalan	LICS-EL-RAEA	4 2(3b)		54	0	54

**Step 4.** You can verify whether a Cisco UCS fabric interconnect is in Cisco UCS Manager Managed Mode or Cisco Intersight managed mode by clicking the fabric interconnect name and looking at the detailed information screen for the fabric interconnect, as shown below:

, Intersignt Infrastructure	Service ~	Q Search		• •
Fabric Interconnects     AA09-FI-DP-6454 FI-A     General Inventory Connect	C Heatthy	s		Ac
Details	Properties		Events	
Health	Cisco UCS-FI-6454		Front Rear - Alarms	No
Name AA09-FI-DP-6454 FI-A Peer Switch		sindraindrainainal estrainainainainainaina	Active Acknowledged     Active Acknowledged     Active Acknowledged     Active Acknowledged     Active Acknowledged	
AA09-FI-DP-6454 FI-B			+ Requests	No R
User Label	Mode	Access	+ Advisories	No Ad
	Ethernet Switching Mode	IP-Address		
Model	end-host	10.108.0.161		
UCS-FI-6454	FC Switching Mode	Subnet Mask		
Serial	end-host	255.255.255.0		
FD0260419XX	Admin Evacuation Mode	Default Gateway		
Management IP	Disabled	10.108.0.254		
10.108.0.161	Operational Evacuation Mode	MAC		
Mode 🕞	Disabled	00:08:31:0B:5D:A0		
Intersight	VLAN Details	FC Zone Count		
UCS Domain Profile	VLAN Port Limit	FC Zone Limit		
UCS Domain Profile Status	Access VLAN Port Count	FC User Zone Limit		
	· ·	1.4		

#### Procedure 5. Upgrade Fabric Interconnect Firmware using Cisco Intersight

**Note:** If your Cisco UCS 6454 Fabric Interconnects are not already running firmware release 4.3(4.240066) or higher , upgrade them to 4.3(4.240066) or to the recommended release.

**Step 1.** Log into the Cisco Intersight portal.

**Step 2.** From the drop-down list, select Infrastructure Service and then select Fabric Interconnects under Operate.

Step 3. Click the ellipses "..." for either of the Fabric Interconnects and select Upgrade Firmware.

C Patrice Interconnects          C Constrained       Arsiane         C Constrained       C Patrice         C Version       The selected fitmware version to upgrade the Fabric Interconnect to I.         C Version       The selected fitmware version to upgrade the Fabric Interconnect traffic evacuation.         C Marine Version       The selected fitmware version to upgrade the Fabric Interconnect traffic evacuation.         C Marine Version       The selected fitmware bundle will be downbaded from intersight com. By default, the upgrade enables Fabric Interconnect traffic evacuation.         C Marine Version       The selected fitmware bundle will be downbaded from intersight Infrastructure Bundle         C Marine Version       The selected fitmware bundle will be downbaded from intersight Infrastructure Bundle         C Marine Version       The selected fitmware bundle will be downbaded from intersight Infrastructure Bundle         C Marine Version       The selected fitmware bundle will be downbaded from intersight Infrastructure Bundle         C Marine Version       The selected fitmware bundle will be downbaded from intersight Infrastructure Bundle         C Marine Version       The selected fitmware bundle will be downbaded form intersight Infrastructure Bundle         C Marine Version       The selected fitmware bundle will be downbaded form intersight Infrastructure Bundle         C Marine Version       The selected fitmware bundle will be downbaded form intersight Infrastructure Bundle	Intersight 🐉 Infrastruc	ure Service 🗸	Q Search C O G	\$1 Q @ @1 @
Version   ③ Version   ③ Summary     Version     ● Version     ● The selected firmware bundle will be downloaded from intersight con. By default, the upgrade enables Fabric Interconnect traffic evacuation.     ● The selected firmware bundle will be downloaded from intersight con. By default, the upgrade enables Fabric Interconnect traffic evacuation.   ● Filters 35 results   ● Filters 35 results   ● 4.316.2400021   ● 4.316.2400021   1.72 0B   For Beinse Date   ● 4.312.2400021   1.72 0B   For Beinse Date   ● 4	← Fabric Interconnects Upgrade Firmware			
Version         Size         Release Date         Description         C           • # Jild 240074)         1.85 GB         Sep 2, 2024 10:50         Cisco Intersight Infrastructure Bundle         C           • 4.314.240074)         1.85 GB         Sep 2, 2024 10:50         Cisco Intersight Infrastructure Bundle         C           • 4.314.2400701         1.72 GB         Feb 5, 2024 10:21         Cisco Intersight Infrastructure Bundle         C           • 4.312.2400071         1.72 GB         Feb 5, 2024 10:21         Cisco Intersight Infrastructure Bundle         C           • 4.312.2400071         1.72 GB         Nov 15, 2023 11:52         Cisco Intersight Infrastructure Bundle         C           • 4.312.2400071         1.72 GB         Nov 15, 2023 11:52         Cisco Intersight Infrastructure Bundle         C           • 4.312.2400071         1.70 GB         Nov 15, 2023 11:52         Cisco Intersight Infrastructure Bundle         C           • 4.312.2400071         1.70 GB         Nov 15, 2023 11:52         Cisco Intersight Infrastructure Bundle         C           • 4.312.2400071         1.70 GB         Aug 15, 2024 423         Cisco Intersight Infrastructure Bundle         C           • 4.312.2400071         1.70 GB         Feb 22, 2024 1011         Cisco Intersight Infrastructure Bundle         C </th <th>General     Version     Summary</th> <th>Version Select a firmware version to upgrade the Fabric Inter The selected firmware bundle will be downlo Use Advanced Mode to exclude Fabric Inter</th> <th>onnects to. aded from intersight.com. By default, the upgrade enables Fabric Interconnect traffic evacuation. onnect traffic evacuation.</th> <th></th>	General     Version     Summary	Version Select a firmware version to upgrade the Fabric Inter The selected firmware bundle will be downlo Use Advanced Mode to exclude Fabric Inter	onnects to. aded from intersight.com. By default, the upgrade enables Fabric Interconnect traffic evacuation. onnect traffic evacuation.	
4.3(4240074)       1.85 0/B       Sep 2, 2024 10:50       Cisco intersight infrastructure Bundle       Gisco intersight infrastructure Bundle <ul> <li>4.3(4240076)</li> <li>1.12 0/B</li> <li>Feb 15, 2024 10:21</li> <li>Cisco intersight infrastructure Bundle</li> <li>4.3(3240007)</li> <li>1.72 0/B</li> <li>Feb 15, 2024 10:21</li> <li>Cisco intersight infrastructure Bundle</li> <li>4.3(2240002)</li> <li>1.72 0/B</li> <li>Feb 15, 2024 10:21</li> <li>Cisco intersight infrastructure Bundle</li> <li>4.3(2240002)</li> <li>1.72 0/B</li> <li>Nov 15, 2023 11:52</li> <li>Cisco intersight infrastructure Bundle</li> <li>4.3(2230177)</li> <li>1.70 0/B</li> <li>Aug 15, 2023 11:55</li> <li>Cisco intersight infrastructure Bundle</li> <li>4.2(33)</li> <li>1.72 0/B</li> <li>Jun 17, 2024 4:23</li> <li>Cisco intersight Infrastructure Bundle</li> <li>4.2(33)</li> <li>1.72 0/B</li> <li>Feb 22, 2024 10:11</li> <li>Cisco intersight Infrastructure Bundle</li> <li>4.2(34)</li> <li>1.72 0/B</li> <li>Feb 22, 2024 10:11</li> <li>Cisco intersight Infrastructure Bundle</li> <li>4.2(33)</li> <li>1.72 0/B</li> <li>Feb 22, 2024 10:11</li> <li>Cisco intersight Infrastructure Bundle</li> <li>4.2(34)</li> <li>1.70 0/B</li> <li>Sep 30, 2023 10:51</li> <li>Cisco intersight Infrastructure Bundle</li> <li>4.2(39)</li> <li>1.70 0/B</li> <li>Jul 31, 2023 11:01</li> <li>Cisco intersight Infras</li></ul>		Advanced Mode      Filters 35 results      Monitor 5 Size - Beleau		
<ul> <li>A.3/4 240066)</li> <li>I.84 GB</li> <li>Jun 4, 2024 11:03</li> <li>Cisco intersight infrastructure Bundle</li> <li>A.3/3 2400077</li> <li>I.72 GB</li> <li>Feb 15, 2024 10:21</li> <li>Cisco intersight infrastructure Bundle</li> <li>A.3/2 240002</li> <li>I.72 GB</li> <li>Jan 25, 2024 7:31</li> <li>Cisco intersight infrastructure Bundle</li> <li>A.3/2 240002</li> <li>I.72 GB</li> <li>Jan 25, 2024 7:31</li> <li>Cisco intersight infrastructure Bundle</li> <li>A.3/2 230129</li> <li>I.70 GB</li> <li>Nov 15, 2023 11:52</li> <li>Cisco intersight infrastructure Bundle</li> <li>A.3/2 230177</li> <li>I.70 GB</li> <li>Aug 15, 2023 11:55</li> <li>Cisco intersight infrastructure Bundle</li> <li>A.3/2 230177</li> <li>I.70 GB</li> <li>Aug 15, 2023 11:55</li> <li>Cisco intersight infrastructure Bundle</li> <li>A.3/2 3017</li> <li>I.70 GB</li> <li>Aug 15, 2023 11:55</li> <li>Cisco intersight infrastructure Bundle</li> <li>A.2/3(3)</li> <li>I.72 GB</li> <li>Feb 22, 2024 10:11</li> <li>Cisco intersight infrastructure Bundle</li> <li>A.2/3(3)</li> <li>I.70 GB</li> <li>Seg 30, 2023 10:51</li> <li>Cisco intersight infrastructure Bundle</li> <li>A.2/3(3)</li> <li>I.70 GB</li> <li>Jul 3, 2023 11:51</li> <li>Cisco intersight infrastructure Bundle</li> <li>A.2/3(3)</li> <li>I.70 GB</li> <li>Jul 3, 2023 11:51</li> <li>Cisco intersight infrastructure Bundle</li> <li>A.2/3(3)</li></ul>			e Date Description	: 0
4.313.2400077       1.72 GIB       Feb 15, 2024 10:21       Cisco intersight infrastructure Bundle         4.312.2400021       1.72 GIB       Jan 25, 2024 7:31       Cisco intersight infrastructure Bundle         4.312.2301291       1.70 GIB       Nov 15, 2023 11:52       Cisco intersight infrastructure Bundle         4.312.2301791       1.70 GIB       Nov 15, 2023 11:55       Cisco intersight infrastructure Bundle         4.312.3301791       1.70 GIB       Aug 15, 2023 11:55       Cisco intersight infrastructure Bundle         4.213(a)       1.72 GIB       Jun 17, 2024 4:23       Cisco intersight infrastructure Bundle         4.213(a)       1.72 GIB       Feb 22, 2024 10:11       Cisco intersight infrastructure Bundle         4.213(a)       1.72 GIB       Feb 22, 2024 10:11       Cisco intersight infrastructure Bundle         4.213(a)       1.70 GIB       Sep 30, 2023 10:51       Cisco intersight infrastructure Bundle         4.213(a)       1.70 GIB       Sep 30, 2023 10:51       Cisco intersight infrastructure Bundle         4.213(a)       1.70 GIB       Jul 31, 2023 11:01       Cisco intersight infrastructure Bundle		() 4.3(4.240074) 1.85 GiB Sep 2,	e Date : Description 2024 10:50 Cisco Intersight Infrastructure Bundle	: @
4.312.2400021       1.72 GIB       Jan 25, 2024 7:31       Cisco intersight infrastructure Bundle         4.312.230129       1.70 GIB       Nov 15, 2023 11:52       Cisco intersight infrastructure Bundle         4.312.2301171       1.70 GIB       Aug 15, 2023 11:55       Cisco intersight infrastructure Bundle         4.312.2301171       1.70 GIB       Aug 15, 2023 11:55       Cisco intersight infrastructure Bundle         4.2(3k)       1.72 GIB       Jun 17, 2024 4:23       Cisco intersight infrastructure Bundle         4.2(3k)       1.72 GIB       Feb 22, 2024 10:11       Cisco intersight infrastructure Bundle         4.2(3k)       1.72 GIB       Feb 22, 2024 10:11       Cisco intersight infrastructure Bundle         4.2(3k)       1.70 GIB       Sep 30, 2023 11:51       Cisco intersight infrastructure Bundle         4.2(3k)       1.70 GIB       Sep 30, 2023 11:51       Cisco intersight infrastructure Bundle         4.2(3k)       1.70 GIB       Jul 31, 2023 11:01       Cisco intersight infrastructure Bundle		•         •	Date : Description     2024 10:50 Cisco Intersight Infrastructure Bundle     2024 11:03 Cisco Intersight Infrastructure Bundle	: @ @
4.312.230129)         1.70 GIB         Nov 15, 2023 11:52         Cisco intersight infrastructure Bundle         Image: Cisco Intersight Infrastructure Bundle           4.312.230117)         1.70 GIB         Aug 15, 2023 11:55         Cisco Intersight Infrastructure Bundle         Image: Cisco Intersight Infrastructure Bundle <td< td=""><td></td><td>↓ 4.3(4.240074)         1.85 GiB Sep 2,           ● 4.3(4.240066)         ↓ 1.84 GiB Jun 4,           ↓ 4.3(3.240007)         1.72 GiB Feb 15</td><td>e Date         :         Description           2024 10:50         Cisco Intersight Infrastructure Bundle           2024 10:31         Cisco Intersight Infrastructure Bundle           2024 10:21         Cisco Intersight Infrastructure Bundle           2024 10:21         Cisco Intersight Infrastructure Bundle</td><td>2 @ 00 00</td></td<>		↓ 4.3(4.240074)         1.85 GiB Sep 2,           ● 4.3(4.240066)         ↓ 1.84 GiB Jun 4,           ↓ 4.3(3.240007)         1.72 GiB Feb 15	e Date         :         Description           2024 10:50         Cisco Intersight Infrastructure Bundle           2024 10:31         Cisco Intersight Infrastructure Bundle           2024 10:21         Cisco Intersight Infrastructure Bundle           2024 10:21         Cisco Intersight Infrastructure Bundle	2 @ 00 00
4.312.230117)         1.70 GIB         Aug 15, 2023 11:55         Citsco Intersight Infrastructure Bundle         Image: Cites Contensight Infrastructure Bundle           4.2(3k)         1.72 GIB         Jun 17, 2024 4:23         Cites Contensight Infrastructure Bundle         Image: Cites Contensight Infrastructure B		4.314.2400741         1.85 GB         Sep 2.           (a)         4.314.2400661         1.184 GB         Jun 4.           4.313.2400071         1.72 GB         Feb 15           4.312.2400021         1.72 GB         Jan 2.2	e Date         :         Description           2024 10:50         Cisco Intersight Infrastructure Bundle           2024 10:21         Cisco Intersight Infrastructure Bundle           2024 10:21         Cisco Intersight Infrastructure Bundle           2024 10:21         Cisco Intersight Infrastructure Bundle           2024 7:31         Cisco Intersight Infrastructure Bundle	: @ @ @ @
4.2(3k)         1.72 GIB         Jun 17, 2024 4:23         Cisco Intersight Infrastructure Bundle         Image: Cisco Intersight Infrastructure Bundle           4.2(3j)         1.72 GIB         Feb 22, 2024 10:11         Cisco Intersight Infrastructure Bundle         Image: Cis		4.3(4,240074)         1.85 GB         Sep 2.           (a)         4.3(4,240076)         1.85 GB         Sep 2.           (a)         4.3(4,240076)         1.12 GB         Feb 13           (a)         4.3(2,240007)         1.72 GB         Feb 13           (a)         4.3(2,240002)         1.72 GB         Jan 22           (a)         4.3(2,24002)         1.70 GB         Nov 11	Date         :         Description           2024 10:50         Cisco Intersight Infrastructure Bundle           2024 10:21         Cisco Intersight Infrastructure Bundle           2024 7:31         Cisco Intersight Infrastructure Bundle           2023 11:52         Cisco Intersight Infrastructure Bundle	: @ 
4.2(3)         1.72 GIB         Feb 22, 2024 10:11         Cisco intersight infrastructure Bundle         Image: Cisco Intersight Infrastructure Bundle		4.3(4.240074)         1.85 GB Sep 2.           (a) 4.3(4.240074)         1.84 GB Jun 4.           (a) 4.3(4.240074)         1.72 GB Feb 15           (a) 4.3(4.240074)         1.72 GB Jan 22           (a) 4.3(4.240074)         1.72 GB Nov 11           (a) 4.3(4.240074)         1.70 GB Nov 11           (a) 4.3(4.230177)         1.70 GB Aug 11	Date         :         Description           2024 10:03         Cisco Intersight Infrastructure Bundle	2 00 00 00 00 00 00 00 00 00 00 00 00 00
4.2(3h)         1.70 G/B         Sep 30, 2023 10-51         Citico intersight infrastructure Bundle           4.2(3g)         1.70 G/B         Jul 31, 2023 11:01         Citico intersight infrastructure Bundle         Image: Citico intersight infrastructure Bundle		4.3(4.240074)         1.85 GB Sep 2.           (e)         4.3(4.240074)         1.72 GB Feb 15           (e)         4.3(4.240074)         1.72 GB Nov 11           (e)         4.3(4.240074)         1.70 GB Nov 11           (e)         4.3(4.230179)         1.70 GB Aug 11           (e)         4.3(4.230177)         1.70 GB Aug 11           (e)         4.2(3k)         1.72 GB Jun 17	Date         Description           2024 10:30         Cisco Intersight Infrastructure Bundle           2024 10:31         Cisco Intersight Infrastructure Bundle           2024 20:31         Cisco Intersight Infrastructure Bundle           2024 7:331         Cisco Intersight Infrastructure Bundle           2023 11:52         Cisco Intersight Infrastructure Bundle           2023 11:52         Cisco Intersight Infrastructure Bundle           2023 11:52         Cisco Intersight Infrastructure Bundle           2024 4:23         Cisco Intersight Infrastructure Bundle	
4.2(3g) 1.70 G/B Jul 31, 2023 11:01 Cisco Intersight Infrastructure Bundle		4.3(4.240074)         1.85 GiB Sep 2.           (a) 4.3(4.240076)         1.85 GiB Sep 2.           (a) 4.3(2.40066)         1.84 GiB Jun 4.           4.3(3.240067)         1.72 GiB Feb 15           4.3(2.240062)         1.72 GiB Ana 21           4.3(2.240062)         1.72 GiB Nov 11           4.3(2.23017)         1.70 GiB Nov 11           4.3(2.23017)         1.70 GiB Nov 11           4.3(2.23017)         1.70 GiB Jun 17           4.3(2.33017)         1.70 GiB Jun 17           4.3(2.33017)         1.72 GiB Jun 17           4.2(3k)         1.72 GiB Feb 22	Date         Description           2024 10:50         Cisco Intersight Infrastructure Bundle           2024 11:03         Cisco Intersight Infrastructure Bundle           2024 10:14         Cisco Intersight Infrastructure Bundle           2024 7:31         Cisco Intersight Infrastructure Bundle           2023 11:52         Cisco Intersight Infrastructure Bundle           2024 7:31         Cisco Intersight Infrastructure Bundle           2023 11:52         Cisco Intersight Infrastructure Bundle           2024 4:23         Cisco Intersight Infrastructure Bundle           2024 4:24         Cisco Intersight Infrastructure Bundle           2024 10:11         Cisco Intersight Infrastructure Bundle	
		4.3(4.240074)         1.85 GiB Sep 2.           (a) 4.3(4.240074)         1.85 GiB Sep 2.           (a) 4.3(4.240076)         1.84 GiB Jun 4.           4.3(3.240066)         1.12 GiB Feb 15           4.3(2.240062)         1.72 GiB Jun 4.           4.3(2.240062)         1.72 GiB Ana 21           4.3(2.240071)         1.70 GiB Nov 11           4.3(2.230129)         1.70 GiB Nov 11           4.3(2.23017)         1.70 GiB Jun 17           4.3(2.33017)         1.70 GiB Nov 11           4.3(2.33017)         1.70 GiB Sep 3.           4.3(2.33017)         1.70 GiB Sep 3.           4.3(2.33017)         1.70 GiB Sep 3.           4.2(3k)         1.72 GiB Feb 22           4.2(3k)         1.70 GiB Sep 3.	Date         Description           2024 10:50         Cisco Intersight Infrastructure Bundle           2024 11:03         Cisco Intersight Infrastructure Bundle           2024 11:03         Cisco Intersight Infrastructure Bundle           2024 11:03         Cisco Intersight Infrastructure Bundle           2024 7:31         Cisco Intersight Infrastructure Bundle           2023 11:52         Cisco Intersight Infrastructure Bundle           2024 4:23         Cisco Intersight Infrastructure Bundle           2024 4:24         Cisco Intersight Infrastructure Bundle           2024 10:11         Cisco Intersight Infrastructure Bundle           2024 10:21         Cisco Intersight Infrastructure Bundle           2024 10:21         Cisco Intersight Infrastructure Bundle           2023 10:51         Cisco Intersight Infrastructure Bundle	

Step 4. Click Start.

Step 5. Verify the Fabric Interconnect information and click Next.

**Step 6.** Select 4.3(4.240066)) release (or the latest release which has the 'Recommended' icon) from the list and click Next.

l" Intersight 🛛 🖧 Infrastru	ture Service ∨ Q. Search C ⊘ ⊄ Q	• • • •
+ Fabric Interconnects Upgrade Firmware		
General	Version Select a firmware version to upgrade the Fabric interconnects to.	
3 Summary	The selected firmware bundle will be downloaded from intersight.com. By default, the upgrade enables Fabric Interconnect traffic evacuation. Use Advanced Mode to exclude Fabric Interconnect traffic evacuation.	
	Advanced Mode	
	Filters 35 results	
	Version : Size : Release Date : Description	:
	Version         :         Size         Release Date         :         Description           0         4.3(4,240074)         1.85 0i8         Sep 2, 2024 10:50         Cisco Intersight Infrastructure Bundle	1
	Version         :         Size         Release Date         :         Description           0         4.3(4,240074)         1.85 0/8         Sep 2, 2024 10:50         Cisco Intersight Infrastructure Bundle           (i)         4.3(4,240066)         0         1.84 0/18         Jun 4, 2024 11:03         Cisco Intersight Infrastructure Bundle	:
	Version         :         Size         Release Date         :         Description <ul></ul>	-
	Version         :         Size         Release Date         :         Description <ul></ul>	:
	Version         :         Size         Release Date         :         Description <ul></ul>	:
	Version         :         Size         Release Date         :         Description <ul></ul>	2
	Version         :         Size         Release Date         :         Description <ul></ul>	2
	Version         :         Size         Release Date         :         Description           4.3/4.240074         1.85 GB         Sep 2, 2024 10:50         Cisco Intersight Infrastructure Bundle           •         4.3/4.240076         •         1.86 GB         Jun 4, 2024 1103         Cisco Intersight Infrastructure Bundle           •         4.3/4.240070         1.72 GB         Feb 15, 2024 1021         Cisco Intersight Infrastructure Bundle           •         4.3/2.240002         1.72 GB         Feb 15, 2024 7:31         Cisco Intersight Infrastructure Bundle           •         4.3/2.240021         1.72 GB         No 15, 2023 11:52         Cisco Intersight Infrastructure Bundle           •         4.3/2.2301291         1.70 GB         No 15, 2023 11:52         Cisco Intersight Infrastructure Bundle           •         4.3/2.230171         1.72 GB         Jun 17, 2024 423         Cisco Intersight Infrastructure Bundle           •         4.2(3)         1.72 GB         Jun 17, 2024 423         Cisco Intersight Infrastructure Bundle           •         4.2(3)         1.72 GB         Jun 17, 2024 423         Cisco Intersight Infrastructure Bundle	2
	Version         :         Size         Release Date         :         Description                4.314.240074)          1.85 GiB         Sep 2, 2024 10:50         Cisco Intersight Infrastructure Bundle                6             4.314.240078)                6             4.314.240078)                4             313.240077               172 GiB               4.312.240028)                4.312.240029               172 GiB               4.312.240029               4.312.240029               172 GiB               4.312.240029               4.312.240029               172 GiB               4.312.240029               172 GiB               4.312.240029               170 GiB             800 t5, 2023 11:52               Cisco Intersight Infrastructure Bundle               4.312.230179               170 GiB             400 t5, 2023 11:52               Cisco Intersight Infrastructure Bundle               4.2(3)               4.2(3)               4.2(3)               172 GiB               172 GiB               172 GiB	2
	Version         :         Size         Release Date         :         Description                4.314.240074)          1.85 GiB         Sep 2, 2024 10:50         Cisco Intersight Infrastructure Bundle                6. 4.314.240078)          1.85 GiB         Sep 2, 2024 10:50         Cisco Intersight Infrastructure Bundle                6. 4.314.240078)          1.84 GiB         Jun 4, 2024 11:03         Cisco Intersight Infrastructure Bundle                4.312.240002          1.72 GiB         Feb 15, 2024 10:21         Cisco Intersight Infrastructure Bundle                4.312.240002          1.72 GiB          Jan 25, 2024 7:31         Cisco Intersight Infrastructure Bundle                4.312.240002          1.70 GiB         Avis 15, 2023 11:52         Cisco Intersight Infrastructure Bundle                4.312.24007          1.70 GiB         Avis 15, 2023 11:52         Cisco Intersight Infrastructure Bundle                4.312.24007          1.70 GiB         Jun 7, 2024 423         Cisco Intersight Infrastructure Bundle                4.312.24007          1.70 GiB         Jun 7, 2024 423         Cisco Intersight Infrastructure Bundle                4.2131          Jun 77, 2024 22, 2024 1011         Cisco Intersight Infrast	

Step 7. Verify the information and click Upgrade to start the upgrade process.

**Step 8.** Watch the Request panel of the main Intersight screen as the system will ask for user permission before upgrading each FI. Click the Circle with Arrow and follow the prompts on screen to grant permission.

**Step 9.** Wait for both the FIs to successfully upgrade.

ast-1.intersight.com/an/infrastructur	re-service/an/network/element-s	ummaries/?\$currentPage=1&\$p	ageSize=22&Sorderby=Name%20asc&Scu	urrentCustomView=1			\$	
ht 🛛 🖧 Infrastructure Servic	e ~			Q Search	C ⊘ ⊄	۵ ۵ 🛛	•	3
Interconnects								
bric Interconne 🛞 +								
Q Search	Filters 2 resu	lts					≙	Exp
Connec	ction Contract Stat	us Bundle Version	NX-OS Version	Models				
Healthy 2	inected 2 00 Not Covered	2	4.3(4.240066) 2	9.3(5)143(4a) 2 2 64	54 2			
						Ports		
	A. R							
ame 1	Health	: Model	Bundle Version	OCS Domain Profile	Total	Used	Available	_
	east-Lintersight.com/an/infrastructure Interconnects bric Interconne@ + (Q. Search (Q. Search (Orme (Orme) (Orme) (Orme) (Orme)	east-Lintersight.com/an/infrastructure-service/an/network/dement-service > Interconnects  bric Interconne@_+  Q_Search	east-Lintersight com/an/infrastructure-service/an/inetwork/element-summaries/?ScurrentPage=1845p ght the interconnects interconnects interconnected * Filters :2 results Connection Contract Status : Priters :2 results Connected 2 Priters :2 results Priters :2	east-Lintersight.com/an/infrastructure-service/an/network/element-summaries/7ScurrentPage=185pageSize=2285orderby=Name%i2Dasc85o pht  the infrastructure Service  inferconnects  inferconnects  inferconnection  Connection  Connection  Rife Covered 2  Automatic Status  NX-OS Version  Connected 2  Automatic Status  Auto	east-Lintersight com/an/infrastructure-service/an/network/element-summaries/?ScurrentPage=185pageSize=228.5orderby=Name/Si20asc85currentCustomView=1  (	east-Lintersight Com/an/infrastructure-service/an/inetwork/element-summaries/75currentPage=1845pageSize=2285orderby=NameHi2Dasc85currentCustomView=1  Q Search Q Search P Filters 2 results D Connection P Filters 2 results D Connected 2 P Models P	east-Lintersight Com/an/infrastructure-service/an/inetwork/element-summaries/75currentPage=1845pageSize=22845orderby=Name%20ascd5currentCutomView=1	east-Lintersight Com/an/Infrastructure-service/an/Intersort/element-summaries/75currentPage=1845pageSize=2285orderby=Name%i20ascdScurrentCustomViewe=1 *

Note: For more details on Firmware upgrade of Cisco Fabric Interconnect in IMM mode, go to https://www.cisco.com/c/en/us/support/docs/servers-unified-computing/unified-computingsystem/217433-upgrade-infrastructure-and-server-firmwa.html

# Set up Domain Profile

A Cisco UCS domain profile configures a fabric interconnect pair through reusable policies, allows configuration of the ports and port channels, and configures the VLANs and VSANs in the network. It defines the characteristics of and configured ports on fabric interconnects. The domain-related policies can be attached to the profile either at the time of creation or later. One Cisco UCS domain profile can be assigned to one fabric interconnect domain.

Some of the characteristics of the Cisco UCS domain profile in the for Cohesity Helios environment include:

- A single domain profile is created for the pair of Cisco UCS fabric interconnects.
- Unique port policies are defined for the two fabric interconnects.
- The VLAN configuration policy is common to the fabric interconnect pair because both fabric interconnects are configured for the same set of VLANs.
- The Network Time Protocol (NTP), network connectivity, and system Quality-of-Service (QoS) policies are common to the fabric interconnect pair.

Next, you need to create a Cisco UCS domain profile to configure the fabric interconnect ports and discover connected chassis. A domain profile is composed of several policies. Table 13 lists the policies required for the solution described in this document.

able 13. Policies required for a Cisco UCS Do	main Profile
Policy	Description
/LAN and VSAN Policy	Network connectivity
Port configuration policy for fabric A	Definition of Server Ports, FC ports and uplink ports channels
Port configuration policy for fabric B	Definition of Server Ports, FC ports and uplink ports channels

T

Network Time Protocol (NTP) policy
Policy	Description
Syslog policy	
System QoS	

**Procedure 1.** Create VLAN configuration Policy

Step 1. Select Infrastructure Services.



Step 2. Under Policies, select Create Policy, then select VLAN and click Start.



Step 3. Provide a name for the VLAN (for example, Coh-VLANPolicy) and click Next.

dinde Intersight 3t Infrastructur	re Service 🗸	Q Search	C	⊘ \$1	000	0	٩
Policies > VLAN Create							
General     Z     Policy Details	Openceal         Add a name, description and tag for the policy.         Organization*         default          Coh-VLANPolicy         Set Tags         Exter a tag in the key value format.         Description         Description         0/1024						

Step 4. Click Add VLANs to add your required VLANs.

**Step 5.** Click Multicast Policy to add or create a multicast policy with default settings for your VLAN policy as show below:

≡ disco Intersight 🍂 Infrastruction	ure Service 🗸		Q Search	C 0 4	ር 😰 🚳 💿 ጸ
© Overview Policies	> Multicast Policy				
Operate     Servers     Chassis     Fabric Interconnects     Hyperfiles     Configure     Configure     Configure     Temptass     Pools	eneral olicy Detaits	Oeneral Ada anawa sebraption, and tag for the po Organization*  default  tages Con-multicast Set Tage Ever a tag in the keywakes format.  Description Description	ery.		
New Command Palette	*	Cancel			Next
$\equiv \frac{10000}{cisco}$ Intersight	••• Infrastructure ••• Service	<sup>e</sup> ∨ Q Search	Ø © 2	\$1 💶 🗘 🚺	47 🛆 10
: Overview	Policies     Crea		Policy		
<ul> <li>Operate</li> <li>Servers</li> <li>Chassis</li> <li>Fabric Interconnects</li> <li>HyperFlex Clusters</li> <li>Virtualization</li> <li>Kubernetes</li> </ul>		General Policy Details	Policy Details Add policy details Multicast Po Snoopin Querier	o <b>licy</b> ng State ⊙ State ⊙	ĺ
Integrated Systems	^		< Cancel	IP Proxy State o Back	- Create

≡ :	alla Intersight 💦 👫 Infrastructure Service 🗸		Q Search	C	⊘ ⊄	1 0 💿 🚳	0	<u> </u>
.0	Policies > VLAN							
0	Add VLANs Add VLANs to the policy							
©.	VLANs should have one Multicast policy association Configuration	sted to it						
	Prefix * ① VLANIOSI  Auto Allow On Uplinks ①  Enable VLAN Sharing ①  Multicast Policy * Selected Policy C ④ ② Edit Selection ②	VLANIDs* ① 1001						
					La.			
	Cancel						A	dd

Step 6. Add VLAN as required in the network setup with default options and multicast policy, click Create.

Step 7. Add additional VLANs as required in the network setup and click Create.

elisels Intersight 💦 👫 Infrastru	sture Service 🗸	Q Search	C ⊚	\$1 Q	• •	0
Policies > VLAN Create						
General     Policy Details	Policy Details Add policy details This policy is applicable only for UCS Domains VLANs Add VLANs Show VLAN ID Ranges Show VLAN ID Ranges Show VLAN ID Ranges Show VLAN ID Ranges Show VLAN ID Ranges Share to share the	· Primary VI AN ID · · Multicas	t Policy	Auto Alleo	v On Unit.	
	1 default None     1080 VLAN1080,1080 None	Coh-mul	ticast	Yes		
	1081 VLAN1081,1081 None     1082 VLAN082,1082 None	Coh-mul Coh-mul	ticast	Yes Yes		
	Set Native VLAN ID		Rows pe	er page 10		) >
						N

**Note:** If you will be using the same VLANs on fabric interconnect A and fabric interconnect B, you can use the same policy for both.

**Note:** In the event any of the VLANs are marked native on the uplink Cisco Nexus switch, ensure to mark that VLAN native during VLAN Policy creation. This will avoid any syslog errors.

#### **Procedure 2.** Create Port Configuration Policy

Note: This policy has to be created for each of the fabric interconnects.

Step 1. Under Policies, for the platform type, select UCS Domain, then select Port and click Start.



**Step 2.** Provide a name for the port policy, select the Switch Model (present configuration is deployed with FI 6454) and click Next.

	Intersight structure Service		Q Search	C	⊘ ⊄	Q 🗿 🖾	0	۹
\$	Policies > Port Create							
0 <b>0</b> 0 •	Ceneral Curified Port Breakout Options  Port Roles	Oranization*         @default         Sob-PortPolicy()         Switch Model*         UCS-Fi-6454         Set Tags         Enter a tag in the key/value fi]mat.         Description         Description         0/1024						
	¢	Cancel					Ne	ext

**Step 3.** Click Next. Define the port roles; server ports for chassis and server connections, Fibre Channel ports for SAN connections, or network uplink ports.

**Step 4.** If you need Fibre Channel, use the slider to define Fibre Channel ports.

**Step 5.** Select ports 1 through 16 and click Next, this creates ports 1-16 as type FC with Role as unconfigured. When you need Fibre Channel connectivity, these ports can be configured with FC Uplink/Storage ports.

**Note:** Selection of FC ports should be confirmed with your administrators. In event customers are not looking to have FC connectivity, they can you Server Ports starting from Port 1

≡ diala intersight	3 infrastructure Service $$		Q Search		0 62	¢] 📧 (	047 610	0	
©. Overview	Policies > Port								
<ul> <li>Operate</li> <li>Servers</li> <li>Chassis</li> <li>Fabric Interconnects</li> <li>HyperFlex Clusters</li> <li>Virtualization</li> <li>Kubernetes</li> <li>Integrated Systems</li> <li>Configure</li> <li>Profiles</li> </ul>	Ceneral Cutified Port Cutified Port Cutified Port Cutified Port Roles Cutified Port Roles	Unified Port Configure the port	modes to carry FC or Ethernet traffic. ave slider to configure unified ports and select po Channel Ports 16 Fibre Channel Port 16 Fib	rt to set breakout. Is (Port 1-16)		ore don of the second s	De la constanti		
Templates Policies Pools		rc	Ports 1-15	Ethernet	Ports 17	-54			
		< Cancel					Bac	k No	

Step 6. Click Next.

**Step 7.** If required, configure the FC or Ethernet breakout ports, and click Next. In this configuration, no breakout ports were configured. Click Next.

**Step 8.** To configure server ports, select the ports that have chassis or rack-mounted servers plugged into them and click Configure.

P	ort Roles	Port Channe	els Pin Groups	
	Configure	Selected Ports	Port 17, Port 18, Port 19, Port 20, Port 21, Port 22, Port 23, Port 24, Port 25, Port 26, Port 27, Port 28, Port 29, Port 30, Port 31, Port 32	Clea Sele
				0

Step 9. From the drop-down list, select Server and click Save.

#### Configure (16 Ports)

Configuration         Selected Ports       Port 17, Port 18, Port 20, Port 21, Port 22, Port 23, Port 24, Port 25, Port 26, Port 27, Port 28, Port 29, Port 30, Port 31, Port 32         Role       Server         Server       ~         Image: N9K-C93180YC-FX3 requires CI74 FEC for 25G speed ports. Learn more at Help Center.         FEC       ©         Image: Auto       CI74	Configuration         Selected Ports       Port 17, Port 18, Port 20, Port 21, Port 22, Port 23, Port 24, Port 25, Port 26, Port 27, Port 28, Port 29, Port 30, Port 31, Port 32         Role       Server         Server       ✓         Image: N9K-C93180YC-FX3 requires CI74 FEC for 25G speed ports. Learn more at Help Center.         FEC       ©         Auto       CI74         Image: Manual Chassis/Server Numbering ©
Selected       Port 17, Port 18, Port 19, Port 20, Port 21, Port 22, Port 23, Port 24, Port 25, Port 26, Port 27, Port 28, Port 29, Port 30, Port 31, Port 32         Role	Selected       Port 17, Port 18, Port 19, Port 20, Port 21, Port 22, Port 23, Port 24, Port 25, Port 26, Port 27, Port 28, Port 29, Port 30, Port 31, Port 32         Role
Role         Server <ul> <li>N9K-C93180YC-FX3 requires CI74 FEC for 25G speed ports. Learn more at Help Center.</li> </ul> FEC © <ul> <li>Auto CI74</li> </ul>	Role         Server <ul> <li>N9K-C93180YC-FX3 requires CI74 FEC for 25G speed ports. Learn more at Help Center.</li> </ul> FEC <ul> <li>Auto</li> <li>CI74</li> </ul> Manual Chassis/Server Numbering <ul> <li>Manual Chassis/Server Numbering</li> <li> </li></ul>
N9K-C93180YC-FX3 requires CI74 FEC for 25G speed ports. Learn more at Help Center.  FEC      Auto CI74	<ul> <li>N9K-C93180YC-FX3 requires CI74 FEC for 25G speed ports. Learn more at Help Center.</li> </ul> FEC © <ul> <li>Auto Cl74</li> </ul> Manual Chassis/Server Numbering ©
FEC © Auto CI74	FEC © Auto CI74 Manual Chassis/Server Numbering ©
	Manual Chassis/Server Numbering $\odot$

Save

**Step 10.** Configure the uplink ports as per your deployment configuration. In this setup, port 53/54 are configured as uplink ports. Select the Port Channel tab and configure the port channel as per the network configuration. In this setup, port 53/54 are port channeled and provide uplink connectivity to the Cisco Nexus switch.

Policies > Port					
Create					
	The combined maximum is 12 and the maximum	m num I numbi	ber of Ethernet Uplink, F er of FC port channels p	CoE Uplink, and A armitted is 4.	Appliance port channels permitted
Rol	e ernet Uplink Port Channel	~			
Por 65	t Channel ID *	0	Admin Speed Auto	× ©	
Eth	ernet Network Group ⊙ ect Policy 🗐				
Flo	w Control ect Policy				
Lin Sei	k Aggregation ect Policy 🗐				
Lin Sel	k Control <b>ect Policy</b> 個				

Indersight Second Infrastructure Sec	vice 🗸		Q Search	C © 4	Q (11) (12)
Policies > Port					
Ceneral Unified Port Breakout Options. Port Roles	Port Roles Configure port roles to define the traffic ty Port Roles Port Channel Create Port Channel	pe carried through a unified port connects Plin Groups		FT4 PT4 PT4 PT4	
		ID : Role	: Port	€ Et	ernet Uplink Port Channel
	 _/ =	65 Ethernet Uplin	k Port Channel Port	53, Port 54 Rows per page 10	• • • • • •
	Cancel				Back

**Step 11.** Repeat this procedure to create a port policy for Fabric Interconnect B. Configure the port channel ID for Fabric B as per the network configuration. In this setup, the port channel ID 66 is created for Fabric Interconnect B, as shown below:

≡ "	isco Intersight 💦 🎥 Infrastructure Ser	vice 🗸		Q Search	C O A	ር 💿 💶 🔍
	Policies > Port Create					
0 0	<ul> <li>General</li> <li>Unified Port</li> <li>Breakout Options</li> <li>Port Roles</li> </ul>	Port Roles Configure port roles to define the traff Port Roles Port Channel Create Port Channel	fic type carried through a unified port connection.			thernet Uplink Port Channel
			ID : Role 66 Ethernet Uplink Po	: Ports rt Channel Port 53, Port	🖑	© . 
		Cancel				Back

# Procedure 3. Create NTP Policy

Step 1. Under Policies, select Create Policy, then select UCS Domain and then select NTP. Click Start.

≡	cisco Intersight	3 Infrastructure Service $$		Q Searc	ch	0 @2	FJ 💶	Q 047 A 10	0	R
×\$1.	Overview	← Policies Create								
ø ,•	Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Urtrustization Kubernetes Configure Configure Profiles Templates Pools	<ul> <li>Filters</li> <li>Platform Type</li> <li>All</li> <li>UCS Sanwar</li> <li>UCS Chaels</li> <li>Hyperflex Cluster</li> <li>Kudernetes Cluster</li> </ul>	Q. Search     Pithamet Network Control     Pithamet Network Croup     Flow Control     Unk Aggregation	Link Control     Multicast Policy     Network Conactivity     NTP	Port SHAP Switch Dontrol Syslog		System QaS VLAN VSAN			
			Cancel						Sta	n

- **Step 2.** Provide a name for the NTP policy.
- Step 3. Click Next.

**Step 4.** Define the name or IP address for the NTP servers. Define the correct time zone.

Policles > NTP Create			
General     Policy Details	Policy Details Add policy details		√ All Platforms   UCS Server (Standalone)   UCS Domain
	NTP Servers * 172.20.10.18	Ē	
	NTP Servers * 172.20.10.15 ©	Ŵ	+
	Timezone America/Los_Angeles		~ 0
<	Cancel		Back Create

Step 5. Click Create.

# Procedure 4. Create syslog Policy

Note: You do not need to enable the syslog server.

Step 1. Under Policies, select Create Policy, then select UCS Domain, and then select syslog. Click Start.

≡	tisco Intersight	🍂 Infrastructure Service 🗸		Q Searc	h	⊘ 💿 🤉	FJ 💶	Q @47 @10	0	<u>م</u>
.¢.	Overview	← Policies Create								
۵	Oparata Servers Chassis Fabric Interconnects HyperFlex Cluatars Virtualization Kubernates Integrated Systems Configure Profiles Templates Policies Pools	<ul> <li>Filters</li> <li>Platform Type</li> <li>All</li> <li>UCS Server</li> <li>UCS Chassis</li> <li>HyperFlex Cluster</li> <li>Kubernetes Cluster</li> </ul>	Search     Ethemet Network Control     Ethemet Network Group     Flow Control     Unk Aggregation	Link Control Multicest Policy Network Connectivity NTP	Port SHAP Switch Control Systog	es () v () v ()	ristem QoS JAN SAN			
			Cancel						Sta	art

- Step 2. Provide a name for the syslog policy.
- Step 3. Click Next.
- Step 4. Define the syslog severity level that triggers a report.
- Step 5. Define the name or IP address for the syslog servers.
- Step 6. Click Create.

### **Procedure 5.** Create QoS Policy

**Note:** QoS Policy should be created as per the defined QoS setting on uplink switch. In this Cohesity deployment, no Platinum/Gold/Silver, or Bronze Class of Service (CoS) were defined and thus all the traffic would go through best efforts.

≡	altale Intersight 🦂 🕷 🕷	nfrastructure Service 🗸		Q Search		0 💿 🕫 🖪	Q 💶 💶	©   ۶
XB).	Overview	← Policies Create						
(i) , e	Oparata     A       Servers     -       Chassis     -       Fabric Interconnects     -       HyperFlex Clusters     -       Virtualization     -       Kubernetes     -       Integrated Systems     -       Configure     A       Policies     -       Policies     -       Peols     -	Filters Platform Type All UCS Starver UCS Chassis UCS Chassis HyperFlar Cluster Kubernates Dustar	Ethernet Network Control     Uthernet Network Scoup     How Control     How Control     How Aggregation	Link Control     Multicast Policy     Network Dannestivey     NTP	Pari SNAP Switch Dantral Rykog	Syster     VLAN     VSAN	II OuS	
			Cancel					Start

Step 1. Under Policies, select Create Policy, select UCS Domain, then select System QoS. Click Start.

Step 2. Provide a name for the System QoS policy.

#### Step 3. Click Next.

**Step 4.** In this Cohesity configuration, no Platinum/Gold/Silver, or Bronze Class of Service (CoS) were defined and thus all the traffic would go through best efforts. Change the MTU of best effort to 9216. Click Create.

Policies > System QoS							
Create Ceneral Policy Details	Policy Details Add policy details This policy is a Configure Prior Platinum Gold	policable only for UCS Domain rities	15				
	Silver						
	Best Effort	CoS CoS 3 O	Weight 5 Weight 5	0 a 0 - 10	Allow Packet Drops O	MTU 9216 MTU 2240	() 0 1600 - 0216
<	Cancel				( ) more casket propa		1500 - 9216 Back Create

**Note:** All the Domain Policies created in this procedure will be attached to a Domain Profile. You can clone the Cisco UCS domain profile to install additional Cisco UCS Systems. When cloning the Cisco UCS domain profile, the new Cisco UCS domains use the existing policies for consistent deployment of additional Cisco Systems at scale.

In the previous section, the following polices were created to successfully configure a Domain Profile:

- 1. VLAN Policy and multicast policy
- 2. Port Policy for Fabric Interconnect A and B
- 3. NTP Policy
- 4. Syslog Policy
- 5. System QoS

The screenshot below displays the Policies created to configure a Domain Profile:

sco Intersight 🔒 🖧 Infrastructu	re Service 🗸		Q Search	C 0 4 0 0	💵 💿 👂
Policies					Create Poll
* All Policies  +  All Policies  +  Q. Search  Platform Type UCS Server 2  UCS Domain 7	▼ Filters 7 results • Not Used 6 ● Indirect 1				Export
Name	: Platform Type	Туре	: Usage	Last Update	: \$
Coh-systemQoS	UCS Domain	System QoS	⊘ Not Used	a few seconds ago	
Coh-syslog	UCS Server, UCS Domain	Syslog	Not Used	a few seconds ago	
Coh-NTP	UCS Server, UCS Domain	NTP	Not Used	a minute ago	
Coh-PortPolicy-FIA	UCS DQnain	Port	Not Used	3 minutes ago	30
Coh-PortPolicy-FIB	UCS Domain	Port	🖉 Not Used	4 minutes ago	
Coh-VLANPolicy	UCS Domain	VLAN	⊘ Not Used	13 minutes ago	
Coh-multicast	UCS Domain	Multicast Policy	O Used - Indirect	15 minutes ago	
200				Rows per page 10 ~	< 1 >

### **Procedure 6.** Create Domain Profile

**Note:** All the Domain Policies created in this procedure will be attached to a Domain Profile. You can clone the Cisco UCS domain profile to install additional Cisco UCS Systems. When cloning the Cisco UCS domain profile, the new Cisco UCS domains use the existing policies for consistent deployment of additional Cisco Systems at scale.

- Step 1. Prior to creating Domain Profile, please ensure the below Domain Policies are created.
- Step 2. Select the Infrastructure Service option and click Profiles.
- Step 3. Select UCS Domain Profiles.
- Step 4. Click Create UCS Domain Profile.

=	alada Intersight	🎉 Infrastructure Service 🗸			Q Search	0	2 📢 14	Q (047) (A10)	ଡ
ф.	Overview	Profiles							
0	Operate Servers	A HyperFlex Cluster Profi	es UCS Chassis Profile	UCS Domain Profiles	UCS Server Profiles Kuberne	etes Cluster Profiles		Consta 11/28 Day	uto Destita
	Chassis Fabric Interconnects	* All UCS Domain Pr.	. e + Q Add Filter			G Export 4 iter	ns found 10 ~	per page 🗟 🕤 1	of 1 2 3
	HyperFlex Clusters	Name	5	Status	Fabric Interconnec.	Domain Fabric Interconnec	Last Update		: Ø
	Virtualization	AA08-DomainP	ofile-1	🔁 Nat Assigned			11 hours ago		
	Kubernetes	C25-FI6454-Do	mainProfile	() OK	C25-FLFLA	C25-FI FI-B	Mar 14, 2023 3:5	1 PM	
	Integrated Systems	📋 ucs-domain-pre	file-H13-1_CLONE-1	81 Not Assigned			Jul 26, 2022 5:3	7 PM	111
		ucs-domain-pro	file-H13-T	81 Not Assigned			Jul 26, 2022 3:2	9 PM	
Ĩ	Profiles	- <i>× ∞</i> ±						1	of 1 🔲 🗐
-	Templates								
	Policies								

Step 5. Provide a name for the profile (for example, Coh-DomainProfile) and click Next.

≣ "#	isco Intersight 🛼 👫 Infrastructure Serv	rice ~	Q Search		٩
8	← UCS Domain Profiles Create UCS Domain Prof	ile			
	<ul> <li>Ceneral</li> <li>UCS Domain Assignment</li> <li>VLAN &amp; VSAN Configuration</li> <li>Ports Configuration</li> <li>UCS Domain Configuration</li> <li>Summary</li> </ul>	Seneral         Add a name, description and tag for the UCS domain profile         Interview         Interview         Coh-DomainProfile         Description         Description         O/ 1024			
	<	Close		Back	ext

**Step 6.** Select the fabric interconnect domain pair created when you claimed your Fabric Interconnects.

Create UCS Domain Profiles	ofile		e	Successfully created UCS Domain Profile "Coh- > DomainProfile".
General     UCS Domain Assignment     ULS Domain Assignment     VLAN & VSAN Configuration     Ports Configuration     UCS Domain Configuration	UCS Domain Assignment Choose to assign a fabric interconnect pair to Assign Now Assign Later Choose to assign a Fabric Interconn you choose Assign Later, click Next Show Assigned	o the profile now or later. ect pair now or later. If you choose Assign Now, sele to proceed to policy selection.	ect a pair that you want to assig	in and click Next . If
6 Summary	Filters 1 results			
	Domain N         - Model <ul></ul>	Fabric Interconnect A Serial Bundle Version FD0260419XX 4.3(4.240066) elect All	Model UCS-FI-6454	Fabric Interconnect B Serial         Bundle Version         Image: Constraint of the series of the se

**Step 7.** Under VLAN & VSAN Configuration, click Select Policy to select the policies created earlier. (Be sure that you select the appropriate policy for each side of the fabric.) In this configuration the VLAN policy is same for both the fabric interconnects.

c:	sco Intersight Se Infrastructure Ser	vice 🗸	Q Search	C © 4 C @ @ 0
	← UCS Domain Profiles Create UCS Domain Pro	file		
	General     UCS Domain Assignment	VLAN & VSAN Configuration Create or select a policy for the Fabric Interconnect pair. A Fabric Interconnect A 0 of 2 Policies Configured		
	VLAN & VSAN Configuration     Ports Configuration     UCS Domain Configuration	VLAN Configuration VSAN Configuration		O      O      Coh-VLANPalicy     Select Policy
	6 Summary	Fabric Interconnect B 0 of 2 Policies Configured  VLAN Configuration		B 2 @ Con-VLANPelicy
		VSAN Configuration		Select Policy
				G
		Close		Back

**Step 8.** Under Ports Configuration, select the port configuration policies created earlier. Each fabric has different port configuration policy. In this setup, only the port channel ID is different across both the Port Configuration Policy.

= :	lisco Intersight 💦 😽 Infrastructure Servic	• ~	Q Search	CO	\$	Q 💿 🚳	0	۹
*	← UCS Domain Profiles Create UCS Domain Profile	e						
	General     UCS Domain Assignment	Ports Configuration Create or select a port policy for the Fabric Interconnect Configure ports by creating or selecting a policy	par.					ĺ
,o	VLAN & VSAN Configuration Ports Configuration	Fabric Interconnect A Configured				_		
	CCS Demain Configuration     Summary			cy Coh-Po	Ports	Port Channel		
		×	Ethernet	Uplink Port Chan	nel 🌘 Ser	ver 🕘 Unconfig	ured +	
		Port Type FC 8 Ethernet 46 Port Role	Port Channel Type Ethernet Uplink 1 Port Channel Role					
	c	Close				Ba	=k	lext

**Step 9.** Under UCS Domain Configuration, select syslog, System QoS, and the NTP policies you created earlier. Click Next.

151	infrastructure Ser	vice 🗸	Q Search	
	← UCS Domain Profiles Create UCS Domain Prof	file		
	General     UCS Domain Assignment     VLAN & VSAN Configuration	UCS Domain Configuration Select the compute and management policies to be associated Show Attached Policies (2) Anagement 2 of 4 Policies Configured	I with the Fabric Interconnect.	
	Ports Configuration     UCS Domain Configuration     Summary	NTP Syslog Network Connectivity		∅         ∅         ●         Coh-NTP           ∅         ∅         ●         Coh-systog           Select Policy
		SNMP		Select Policy
		Network 0 of 2 Policies Configured		
		System QoS *		🖹 🖉 💷 🔍 Coh-systemQoS
		Switch Control		Select Policy

**Step 10.** Review the Summary and click Deploy. Accept the warning for the Fabric Interconnect reboot and click Deploy.

≡ :	isco Intersight 🌲 Infrastructure Ser	vice ~		Q Search		C ⊚ ⊄	Q 💿 🚳 💿 🛛	۹
18	← UCS Domain Profiles Create UCS Domain Pro	file						
0 0	<ul> <li>Ceneral</li> <li>UCS Domain Assignment</li> <li>VLAN &amp; VSAN Configuration</li> <li>Ports Configuration</li> <li>UCS Domain Configuration</li> <li>Summary</li> </ul>	Summary Review Constant of the second of t	Domain Profile "Coh-DomainProfile" will be deplor 454". upures the FIs in some of the domains to a 50 this complete, and the FI reconnects to boot is complete, and the FI reconnects to Domain Profile -A Coh-DomainProfile -B Coh-DomainProfile	yed to the assigned Fabric Interconnec operebooted, resulting in a traffic disruption taggred. One of the Fis will be rebooted firs intersight, the other Fi in the domain will be <b>Reboot</b> Yes Yes Rows per page 10 - < 1 Cancel Design	× in r (0)	Requires Reboot Yes Yes Rows per page 1	Coh-PortPolicy-FIA	
		Close					Back Deploy	

**Step 11.** Monitor the Domain Profile deployment status and ensure the successful deployment of Domain Profile.

Profiles	← Requests Deploy Domain Profile	+ Requests Deploy Domain Profile							
HyperFlex Cluster Profiles	Details	Execution Flow							
* All UCS Domain Prof @	Status	Progress	54%						
- 100	A. Name	Wait for Peer Fabric Interconnect to come up after reboot O Deploy Fiber Channel and Ethernet Breakout Ports	Sep 27, 2024 11:54 AM						
Name     Coh-DomainProfile	Deploy Domain Profile ID 66/6/f53696/6e32013da1cc	O Deploy System QoS Policy	Sep 27, 2024 11:54 AM						
		Deploy Enernet Network Policy     O Deploy SNMP Policy	Sep 27, 2024 11:54 AM						
	Target Type Fabric Interconnect	O Deploy Syslog Policy	Sep 27, 2024 11:54 AM						
	Target Name	Depidy NTP Policy     Update Domain Profile State	Sep 27, 2024 11:54 AM Sep 27, 2024 11:54 AM						
	AA09-FI-DP-6454 FI-A	⊘ Validate Syslog Policy	Sep 27, 2024 11:54 AM						
	Source Type Domain Profile	Validate SNMP Policy     Validate NTP Policy     Validate NTP Policy	Sep 27, 2024 11:54 AM Sep 27, 2024 11:54 AM						
	Source Name	Validate Ethernet Network Policy	Sep 27, 2024 11-54 AM						
	Coh-DomainProfile-A	<ul> <li>Validate Port Policy</li> </ul>	Sep 27, 2024 11:54 AM						
	Initiator andhiman@cisco.com	Validate System QoS Policy     Validate Liser Access to Estric Policies	Sep 27, 2024 11:54 AM						
		Validate Gaer Access to Facility Folicies							

**Step 12.** In the event Cisco UCS Servers are already connected to server ports on Fabric Interconnect, they would be discovered in this process.

	isco Intersight 🎝 🖧 Infrastruc	cture Service 🗸				Q s	arch	C	$\odot$	<b>4</b> 1 Q	0 (11)	0	R
*	Profiles	Requests											×
	HyperFlex Cluster Profiles	* All Requests 🐵 +											
0	(	Q Search		Status = In Progr	rss × ₹ Filters	4 results Reset All					0	Export	٦
0													J
.0	* All UCS Domain Prof	Status Exe	ecution Type									XX	
	··· / / 🖄 🔍	C In Progress 4	lecute 4										
	Name												
	Con-DomainProfile	Name S	Status :	Initiator 0	Target Type	Target Name	Start Time :	Duration	ID		Execution Typ	e 4	8
	··· 1 0 0	Rack Server Dis	In Progress 15%	system@intersi	Rack Server	AA09-FI-DP-64	a few seconds a	23 s	661703c4	696f6	Execute		
		Rack Server Dis	<ul> <li>In Progress 15%</li> </ul>	system@intersi	Rack Server	AA09-FI-DP-64	a few seconds a	26 s	661703c16	696f6	Execute	•••	£.
		Rack Server Dis	<ul> <li>In Progress 15%</li> </ul>	system@intersi	Rack Server	AA09-FI-DP-64	a few seconds a	37 s	66f703b7	696f6	Execute		•
		Rack Server Dis	In Progress 15%	system@intersi	Rack Server	AA09-FI-DP-64	a minute ago	57 s	661703a2	696f6	Execute		e. 
			N						Rows per p	page 23	~). <	1 >	
≡ "¦!::	ll' Intersight <b>3</b> Infrastructure	Service 🗸				Q Search	c	0	A 000	• ?	L A		
	Fabric Interconnects												
-49.													
a.	* All Fabric Interconne @ +												
0	···· Ø Q. Search	♥ Filters 2 res	ults							🖞 Ex	port		
	Health C	Connection Contract Sta	atus Bundi	e Version	NX-OS Ver	slon	Models				ж		
	2 Warning 1 Healthy 1	Connected 2 0 Not Cover	ed 2	4.3(4.24006	6) 2	■ 9.3(5)643(4a) 2	2 •64	54 2					
	Name	: Health	: Model	-	Bundle Version	: UCS	Domain Profile	Total	Ports Used	Available	\$		
	AA09-FI-DP-6454 FI-A	A Warning	UCS-FI-64	54	4.3(4.240066)	Coh	-DomainProfile	54	18	36			
	AA09-FI-DP-6454 FI-B	<ul> <li>Healthy</li> </ul>	UCS-FI-64	54	4.3(4.240066)	Coh	-DomainProfile	54	18	36	📮		
	Ø							Rows per ;	bage 22 ~	< 1	) >		

**Step 13.** Verify the uplink and Server ports are online across both Fabric Interconnects. In the event, the uplink ports are not green, please verify the configuration on the uplink Nexus switches.



In the Port Policy, port 17-32 were defined as Server Ports. The 4x C240 M6 LFF certified for Cohesity DataProtect deployment were already attached to these ports. The Servers are automatically discovered when the Domain Profile is configured on the Fabric Interconnects.

Step 14. To view the servers, go to the Connections tab and select Servers from the right navigation bar.

≡	-ihali- Intersight 💦 🍂	Infrastructure Service 🗸		Q Search	
:¢:	Overview	← Fabric Interconnects	5454 FI-B O Healthy		Actions
0	Operate ^ Servers	General Inventory Co	nnections UCS Domain Profile		
	Chassis	COMPUTE			
	Fabric Interconnects	Servers	Servers		
	HyperFlex Clusters	Chassis			
	Integrated Systems	NETWORK	🖉 🔍 Add Filter	C Export 4 items found 10 v per page	K < 1 of 1 > X 🚯
9,	Configure ^	Fabric Extenders	Name : Health : User L	Label C Slot Id C Model C	Serial 🗧 🖗
	Profiles	DECOMMISSIONED	AA09-FI-DP-6454-1 Healthy	N/A UCSC-C240-M6L	L WZP26510561
	Templates	Servers	G AA09-FI-DP-6454-2 O Healthy	N/A UCSC-C240-M6L	U WZP2651059D +++
	Templates Policies	Servers		N/A UCSC-C240-M6I N/A UCSC-C240-M6I N/A UCSC-C240-M6I N/A UCSC-C240-M6I	L WZP2651059D ···· L WZP2651056H ····
	Templates Policies Pools	Servers Chassis Fabric Extenders	AA09-FI-DP-6454-2     O Healthy     AA09-FI-DP-6454-3     O Healthy     AA09-FI-DP-6454-4     O Healthy	N/A         UCSC-C240-M6I           N/A         UCSC-C240-M6I           N/A         UCSC-C240-M6I	L WZP2651059D L WZP2651056H L WZP2651055Z
	Templates Policies Poots	Servers Chassis Fabric Extenders	C         AA09-H-OP-6454-2         © Healthy           O         AA09-FI-DP-6454-3         © Healthy           O         AA09-FI-DP-6454-4         © Healthy            Ø	N/A         UCSC-C240-M6I           N/A         UCSC-C240-M6I           N/A         UCSC-C240-M6I	L         WZP2651056H         ····           L         WZP2651056H         ····           L         WZP2651055Z         ····           E         I         of 1         Image: Contract of 1
Ner	Templates Policies Pools	Servers Chassis Fabric Extenders	<td>N/A         UCSC-C240-M6I           N/A         UCSC-C240-M6I           N/A         UCSC-C240-M6I</td> <td>L         WZP2651056H         ····           L         WZP2651056H         ····           L         WZP2651055Z         ····           E         E         1         of 1         E         M</td>	N/A         UCSC-C240-M6I           N/A         UCSC-C240-M6I           N/A         UCSC-C240-M6I	L         WZP2651056H         ····           L         WZP2651056H         ····           L         WZP2651055Z         ····           E         E         1         of 1         E         M
Ner Navi to Hi	Templates Policies Pools Command Palette Sate Interciptin with Ctrl+K or go also Command Paletts	Servers Chassis Fabric Extenders	C         AA09-FI-DP-6454-2         © Healthy           O         AA09-FI-DP-6454-3         © Healthy           O         AA09-FI-DP-6454-4         © Healthy            Ø	N/A         UCSC-C240-M6I           N/A         UCSC-C240-M6I           N/A         UCSC-C240-M6I	L         WZP2651056H         ····           L         WZP2651056H         ····           L         WZP2651055Z         ····           E         I         of 1         Image: Second se
Ner Navi to He	Templates Policies Pools Command Palette Sate Intersight with Ctri+K or go tap > Command Palette	Servers Chassis Fabric Extenders	C     AA09-FI-DP-6454-2     © Healthy       O     AA09-FI-DP-6454-3     © Healthy       O     AA09-FI-DP-6454-4     © Healthy        Ø	N/A         UCSC-C240-M6I           N/A         UCSC-C240-M6I           N/A         UCSC-C240-M6I	L         WZP2651056H         ····           L         WZP2651056H         ····           L         WZP2651055Z         ····           M         C         1         of 1         2         M

# **Manual Setup Server Template**

A server profile template enables resource management by simplifying policy alignment and server configuration. You can create a server profile template by using the server profile template wizard, which groups the server policies into the following categories to provide a quick summary view of the policies that are attached to a profile:

- Pools: KVM Management IP Pool, MAC Pool and UUID Pool
- · Compute policies: Basic input/output system (BIOS), boot order, and virtual media policies
- · Network policies: Adapter configuration and LAN policies
  - The LAN connectivity policy requires you to create an Ethernet network group policy, Ethernet network control policy, Ethernet QoS policy and Ethernet adapter policy
- Storage policies: Not used in Cohesity Deployment
- Management policies: IMC Access Policy for Cohesity certified Cisco C240 M6 LFF node, Intelligent Platform Management Interface (IPMI) over LAN, Serial over LAN (SOL) and local user policy.

### **Procedure 1.** Create Out of Band IP Pool

The IP Pool is a group of IP for KVM access, Server management of Cohesity certified nodes. The management IP addresses used to access the CIMC on a server can be out-of-band (OOB) addresses, through which traffic traverses the fabric interconnect via the management port.

Step 1. Click Infrastructure Service, select Pool, and click Create Pool.

≡	cisco Intersight	<b>3</b> 6 II	nfrastructure Service 🗸				Q Search	Ø	\$1 Q	ଡ
:¢:	Overview		Pools							
0	Operate	^	Pools Reserved Identi	iers VRFs						
	Servers									
	Chassis									Freate Pool
	Fabric Interconnects									
	HyperFlex Clusters							ana ioano io perpej	90 01 0	
	Integrated Systems		IP x	MAC	UUID ×	WWNN ×	WWPN #	IQN #	Reso	ource 👯
,9	Configure	^	NO IP POOLS	NO MAC POOLS	NO UUID POOLS	NO WWNN POOLS	NO WWPN POOLS	NO IQN POOLS	NO R	ESOU
	Profiles									
	Templates		Name	: Туре	Size 🔅	Used	Available Reserved	Description :	Last Up	date :
6	Policies					NO ITEMS AVAILABLE				
l	Pools					NO TEMO AVAILABLE	-			
									<b>⊠</b> < 0	of 0 🗵 🗵
Ne	Command Palette									
Navi to H	gate Intersight with Ctrl+K or go elp > Command Palette	0								

Step 2. Select IP and click Start.

Step 3. Select Organization as default, Enter a Name for IP Pool and click Next.

≡ "!	sco Intersight 🍂 Infrastructure S	Service 🗸	Q Search	C ⊘	4	00	0	8
.(e).	Pools > IP Pool Create							
9 0 ,	<ul> <li>Ceneral</li> <li>Piv4 Pool Details</li> <li>Piv6 Pool Details</li> </ul>	General         Pool represents a collection of IPv4 and/or IPv6 addresses that can be entities like server profiles.         Organization*         ofault         Name*         Coh-008-IP         Set Tags         Enter a tag in the keyvalue format.         Description         Options         0/1024	allocated to other configuration					
		< Cancel					Ne	xt

Step 4. Enter the required IP details and click Next.

≡ dualte Intersigh	t 💦 🖓 Infrastructure Service 🗸	Q Search	ତ <b>ସ</b> ନ ଡ   ୧
ŵ Overview	Pools > IP Pool Create		
<ul> <li>Operate</li> <li>Servers</li> <li>Chassis</li> <li>Fabric Interconnects</li> <li>HyperFlex Clusters</li> <li>Integrated Systems</li> <li>Configure</li> <li>Profiles</li> <li>Templates</li> <li>Pools</li> </ul>	<ul> <li>General</li> <li>IPv4 Pool Details</li> <li>IPv6 Pool Details</li> </ul>	IPv4 Pool Details Network Interface configuration data for IPv4 Interfaces. Configure IPv4 Pool Configuration Netmask * Cateway 255255.255.0 0 10.108.0.254 Primary DNS 172.20.4.33 0 172.20.4.54 IP Blocks From Size	0
New Command Palette Navigata Intersight with Ctrl+K to Heip > Command Palette	× arga	10.108.0.163 • 4	

Step 5. Deselect the IPV6 configuration and click Create.

#### **Procedure 2.** Create In-Band IP Pool

The IP Pool is a group of IP for KVM access, Server management and IPMI access of Cohesity Certified nodes. The management IP addresses used to access the CIMC on a server can be inband addresses, through which traffic traverses the fabric interconnect via the fabric uplink port.

**Note:** Since vMedia is not supported for out-of-band IP configurations, the OS Installation through Intersight for FI-attached servers in IMM requires an In-Band Management IP address. For more information, go to: <u>https://intersight.com/help/saas/resources/adding\_OSimage</u>.

≡	the Intersight	🔩 Infrastructure Service 🗸				Q Search	0	4 Q @ A
:Ø:	Overview	Pools						
0	Operate /	Pools Reserved Iden	ntifiers VRFs					
	Servers Chassis	* All Pools ⊗ +						Create Pool
	Fabric Interconnects	200 Q	Add Filter			🕒 Export 0 i	tems found 10 - per pa	ige K < 0 of 0 ≥ ≥
	Integrated Systems	IP x	MAC #		WWNN =	WWPN #		Resource 38
.e	Configure /	NO IP POOLS	NO MAC POOLS	NO UUID POOLS	NO WWNN POOLS	NO WWPN POOLS	NO IQN POOLS	NO RESOU
	Templates	Name	: Туре	Size :	Used	Available Reserved	Description	Last Update :
(	Policies Pools				NO ITEMS AVAILABLE			
								K < 0 of 0 ≥ ≥
Navi	Command Palette     Section 2 Command Palette							

Step 1. Click Infrastructure Service, select Pool, and click Create Pool.

**Step 2.** Select IP and click Start.

≡	tited: Intersight % In	nfrastructure Service 🗸	Q Search Ø 4 @ Q
:@:	Overview	Pools > IP Pool Create	
0	Operate ^	1 General	General
	Chassis	2 IPv4 Pool Details	Pool represents a collection of IPv4 and/or IPv6 addresses that can be allocated to other configuration entities like server profiles.
	Fabric Interconnects HyperFlex Clusters	3 IPv6 Pool Details	Organization * Ru-Org
0	Integrated Systems		Name * Ruhingand-Pool
Q	Analyze A Explorer New		
,0	Configure ^		Set lags
	Profiles		Description d <- 1024
	Policies		
	Pools		
Ne	Command Palette		
Navi to H	jate Intersight with Ctrl+K or go Ip > Command Palette	<	Cancel Next

Step 3. Select Organization, Enter a Name for IP Pool and click Next.

Step 4. Enter the required IP details and click Next.

<ul> <li>General</li> <li>IPv4 Pool Details</li> </ul>	IPv4 Pool Details Network interface configuration data for IPv4 interfaces.	
3 IPv6 Pool Details	Previously saved parameters cannot be changed. You can find Cisco recommendations at Help Center.	
	Configuration	
	Netmask *         Gateway           255.255.255.0         0         10.108.0.254         0	٥
	Primary DNS O Secondary DNS O	0
	IP Blocks	
	From Size 10.108.0.167 © 4 © 0 1 - 1024	+
<	Close	Back Nex



### Procedure 3. Create MAC Pool

**Note:** 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.

**Note:** Create two MAC Pools for the vNIC pinned to each of the Fabric Interconnect (A/B). This allows easier debugging during MAC tracing either on Fabric Interconnect or on the uplink Cisco Nexus switch.

**Step 6.** Click Infrastructure Service, select Pool, and click Create Pool.

≣ :!	isco Intersight 38 Infrastruct	ture Service 🗸			Q	Search		A   © 🕰
	Pools							
	Pools Reserved Identifiers	VRFs						
0								Create Pool
0	* All Pools 💿 +							
	0 0 🖹 🔍 Q. Search	h .	Filters 1 results					📥 Export
	IP	MAC	UUID	WWNN	WWPN	IQN	Resource	ж
	4 • Available 4	NO MAC POOLS	NO UUID POOLS	NO WWNN POOLS	NO WWPN POOLS	NO IQN POOLS	NO RESOURCE POOLS	
	Name	Type	Size	Used	Available	Reserved Description	an : Last Upd	late : 🎸 🚊

Step 7. Select MAC and click Start.

Step 8. Enter a Name for Mac Pool (A) and click Start.

Step 9. Enter the last three octet of MAC address and the size of the Pool and click Create.

≡	the Intersight	🎝 Infrastructure Service 🗸		Q Search	Ø 💿	¢] 🕫	Q 053 A14	0	8
:¢:	Overview	Pools > MAC Pool							
© ,e	Operate     A       Servers     A       Chassis     A       Fabric Interconnects     A       HyperFlex Clusters     A       Virtualization     A       Kubernetes     A       Integrated Systems     A       Porfiles     A       Policies     A       Policies     A	Concernation of the second sec	Pool Details Collection of MAC Blocks. MAC Blocks From 00:23:85:45:45:44	0 24			<u>₽</u> • 1-1024	+	
		<	Cancel				Back	Creat	•

Step 10. Repeat this procedure for the MAC Pool for the vNIC pinned to Fabric Interconnect B, shown below:

≡	cisco Intersight	est infrastructure Service ∨		Q Search	⊘ <u>@</u> 2 ⊄1 15	Д <b>(13) (14) (14)</b> (14) (14) (14) (14) (14) (14) (14) (14)
:¢:	Overview	Pools > MAC Pool Create				
0	Operate Servers Chassis Fabric Interconnects HyperFlex Clusters Virtualization Kubernetes Integrated Systems Configure	<ul> <li>∧ General</li> <li>② Pool Details</li> </ul>	Pool Details Cellection of MAC Blocks. MAC Blocks From 0225/83/45/4588	© <sup>Size</sup> 24	_	<u>Ω</u> ● 1 - 1024 +
	Profiles Templates Policies Pools	•	Cancel			Back Create

### Procedure 4. Create UUID Pool

Step 1. Click Infrastructure Service, select Pool, and click Create Pool.

- Step 2. Select UUID and click Start.
- Step 3. Enter a Name for UUID Pool and click Next.
- Step 4. Enter a UUID Prefix (the UUID prefix must be in hexadecimal format xxxxxxx-xxxx).
- Step 5. Enter UUID Suffix (starting UUID suffix of the block must be in hexadecimal format xxxx-xxxxxxxxx).

Step 6. Enter the size of the UUID Pool and click Create. The details are shown below:

≡	eisce Intersight 🐉	🖇 Infrastructure Service 🗸		Q Search	Ø © 2 ⊄1 15	ር 🚥 🚥 🕐 🔍
:@:	Overview	Pools > UUID Pool Create				
0 ,e	Operate        Servers        Chassis        Fabric Interconnects        HyperFlex Clusters        Virtualization        Kubernetes        Integrated Systems        Configure        Profiles        Policies	Oraneral         Image: Pool Details	Pool Details Collection of UUID suffix Blocks. Configuration Prefix * BBBBBBB-6444-6444 UUID Blocks From 2000-22222222222	• • • • •		<u>2 0</u> 1-1024 +
		<	Cancel			Back Create

### **Create Server Policies**

### Procedure 1. Create BIOS Policy

Table 14 lists the required polices for the BIOS policy.

Tahla	1/	RIOS	sottings	for	Cohesity	nodes
lable	14.	DIUS	seungs	101	Conesity	noues

Option	Settings
Memory -> Memory Refresh Rate	1x Refresh
Power and Performance -> Enhanced CPU Performance	Auto
Processor -> Boot Performance Mode	Max Performance
Processor -> Energy-Performance	Performance
Processor -> Processor EPP Enable	enabled
Processor -> EPP Profile	Performance
Processor -> Package C State Limit	C0 C1 state
Serial Port -> Serial A Enable	enabled

**Step 1.** Click Infrastructure Service, select Policies, and click Create Policy.

Step 2. Select UCS Server, BIOS and click Start.

=	diade Intersight	🍂 Infrastructure Service 🗸		Q Searc	h	⊘ <u>◎</u> 2 ¢1 15 Q (	<b>0</b> 53 <b>A</b> 14 ⑦	A
¢.	Overview	← Policies						
¢	Operate Servers Chassis Fabric Interconnects HyperFlex Clusters VirtusEzetion Kubernetes Integrated Systems Configure Profiles Templates Podicies Pools	Fitters Fatform Type AI UCS Storen UCS Storen UCS Storen Kubernetes Cluster	C. Snarch Adapter Configuration Boat Order Dettificate Management Device Connector Drive Sociarly Libernet Adapter Ethernet Network Different Network Group	Ethernet QoS FC Zone Fibre Channel Adopter Fibre Channel Adopter Fibre Channel OoS Fibre Channel OoS Fibre Channel OoS Fibre Channel OoS IND Access IPAti Over LAN ISCSI Adopter ISCSI Boot	BOSI Static Target     LAN Connectivity     LDAP     Local User     Network Connectivity     NTP     Perdistent Memory     Power     SAN Connectivity	SD Cand Serial Over LÁN SMTP SHAP SH Sterage Syslog Virtual KvM Virtual Media		
			Cancel				S	tart

**Step 3.** Enter a Name for BIOS Policy.

**Step 4.** Select UCS Server (FI-Attached), In the policy detail page, select processor option (+) and change the below options and click Create:

- Boot Performance Mode to Max Performance
- Energy Performance to Performance
- Processor EPP Enable to Enable
- EPP Profile to Performance
- Package C State Limit to C0 C1 State

	Boot Performance Mode	1.774.000	APBDIS	
General	Max Performance	× 0	platform-default	
Policy Details	Downcore Control		Streaming Stores Control	
	platform-default	~ Ø	platform-default	V
	Fixed SOC P-State		DF C-States	
	platform-default	v ©	platform-default	Ŷ
	CCD Control		CPU Downcore control	
	platform-default.	~ ©	platform-default	
	CPU SMT Mode		ACPI SRAT L3 Cache As NUMA Domain	
	platform-default	× 0	platform-default	×
	Channel Interleaving		Cisco xGMI Max Speed	
	platform-default	v 0	platform-default	
	Closed Loop Thermal Throttling		Processor CMCI	
	platform-default	~ @	platform-default	104

Policies > BIOS

	С	re	a	te	
--	---	----	---	----	--

GeneralPolicy Details

Core Multi Processing			Energy Performance		
platform-default	$\sim$	0	performance	$\sim$	0
Frequency Floor Override			CPU Performance		
platform-default	$\sim$	0	platform-default	$\sim$	0
Power Technology			Demand Scrub		
nlatform-default	~	0	nlatform-default	~	0
plation of ant			processing of the second		
Direct Cache Access Support			DRAM Clock Throttling		
platform-default		~	platform-default		0
platformulatable		0	plationin-deladat		0
Frances Filleland Tarles			Francis Barfamana Turkan		
Energy Efficient Turbo		_	Energy Performance Tuning		_
platform-default	~	Θ	platform-default	~	O
Enhanced Intel Speedstep(R) Technology			Processor EPP Enable		
platform-default	×	$\odot$	enabled	~	0
EPP Profile			Execute Disable Bit		
Performance	v	0	platform-default	$\sim$	0

Intel(R) VT	IIO Error Enable	
platform-default		× 0
DCU IP Prefetcher	KTI Prefetch	
platform-default	<ul> <li>o platform-default</li> </ul>	∨ ©
LLC Prefetch	Intel Memory Interleaving	
platform-default		✓ ②
Package C State Limit	Patrol Scrub	
CO CT State	v o platform-default	× 0
Patrol Scrub Interval *	Processor C1E	
plationn-defaux	plationPortant	* 0
	P	
platform-default	v o platform-default	× 0
procession account	- protection document	
CPU C State	P-STATE Coordination	
platform-default	<ul> <li>platform-default</li> </ul>	~ ©
	Intel(R) VT platform-default DCU IP Prefetcher platform-default LLC Prefetch platform-default LLC Prefetch platform-default Package C State Limit C0 C1 State Patrol Scrub Interval * platform-default Processor C3 Report platform-default CPU C State platform-default CPU C State	Intel(R) VT       IIO Error Enable         platform-default       v         DCU IP Prefetcher       v         platform-default       v         LLC Prefetch       platform-default         LLC Prefetch       intel Memory interleaving         platform-default       v         Package C State Limit       v         C C C I State       v         Patrol Scrub       platform-default         Processor CIS Report       platform-default         Pictor State       v         o       Processor CIE Report         platform-default       v         CPU C State       v         platform-default       v         v       v         Potrol Scrub       platform-default

Step 5. Click Create.

## Procedure 2. Create Boot Order Policy

The boot order policy is configured with the Unified Extensible Firmware Interface (UEFI) boot mode, mapping of two M.2 boot drives and the virtual Media (KVM mapper DVD). Cohesity creates a software RAID across 2x M.2 drives provisioned in JBOD mode.

- **Step 1.** Click Infrastructure Service, select Policies, and click Create Policy.
- Step 2. Select UCS Server, Boot Order, and click Start.
- Step 3. Enter a Name for Boot Order Policy.
- Step 4. Under Policy Detail, select UCS Server (FI Attached), and ensure UEFI is checked.
- **Step 5.** Select Add Boot Device and click Local Disk, name the device name as m2-2 and slot as MSTOR-RAID.
- **Step 6.** Select Add Boot Device and click Local Disk, name the device name as m2-1 and slot as MSTOR-RAID.
- **Step 7.** Select Add Boot Device and click vMedia and name the 'vmedia-1' device name.
- **Step 8.** Ensure vMedia is at the lowest boot priority as shown below:

$\equiv \frac{1}{2} $	📽 Infrastructure Service 🗸		Q Search	D ©	1 ር 💶 💶 🌒 🛛 ደ
© Overview	Policies > Boot Order > Coh-BootOrder Edit	)			
Operate      Servers	<ul> <li>General</li> <li>Policy Details</li> </ul>	Policy Details Add policy details.		V All Platforms UICS Server	(Standalone) LICS Server (FI-Attached)
Chassis Fabric Interconnects		Configured Boot Mode © Unified Extensible Firmware Interface (UEFI) Enable Secure Boot ①	O Legacy		
HyperFlex Clusters		Add Boot Device ~			_
🛇 Analyze 🔿		+ Local Disk (m2-1) @ + Local Disk (m2-2) @			Enabled in A V
Explorer New Configure ^		+ Virtual Media (vmedia-1) ③			Enabled 🗎 🛧 🗸
Profiles Templates					
Policies					
New Command Palette					
	i (	Cancel		(	Back Save Save & Deploy

# **Procedure 3.** Create Virtual Media Policy

**Step 1.** Click Infrastructure Service, select Policies, and click Create Policy.

- Step 2. Select UCS Server, then select Virtual Media and click Start.
- Step 3. Name the Virtual Media policy and click Next.
- Step 4. Select UCS Server (FI Attached), keep the defaults. Click Create.

Ξ	intersight 🦂 😪 Ir	nfrastructure Service 🗸		Q Search	Q 41 19 Q 000 Q 0 Q
(e):	Overview	Policies > Virtual Media			
0	Operate ^ Servers Chassis Fabric Interconnects	General     Policy Details	Policy Details Add policy details	√ All Platform	UCS Server (Standalone) UCS Server (FI-Attached)
.0	HyperFlex Clusters Virtualization Kubernetes Integrated Systems Configure ^ Profiles		Configuration  Enable Virtual Media   Enable Virtual Media Encryption  Enable Low Power USB		
	Templates Policies Pools		Add Virtual Media           Image: Name         Type	0 items found Protocol	11 - per page ★ € 0 of 0 > > € €) File Location
				NO ITEMS AVAILABLE	e C 0 to 0 2 B
		K	Cancel		Back Create

#### **Procedure 4.** Create virtual KVM Policy

Step 1. Click Infrastructure Service, select Policies, and click Create Policy.

**Step 2.** Select UCS Server, then select Virtual KVM and click Start.

**Step 3.** Name the virtual KVM policy and click Next.

Step 4. Select UCS Server (FI Attached), keep the defaults and enable Allow tunneled KVM. Click Create.

≡	tisco Intersight 🔒	Infrastructure Service 🗸		Q Search	Ø@2 ¢1 115 Q @53	an 0   २
:@:	Overview					
© ,¢	Operate        Servers        Chassis        Fabric Interconnects        HyperFlax Clusters        Virtualization        Kubernetes        Integrated Systems        Configure        Potflies        Potflies	General     Policy Details	Policy Details Add policy details Cable Virtual KVM O Max Sessions * 4 (2) Cable Video Encryption O Allow Tunneled vKVM O	<b>0</b> -4	All Pistorms   UCS Server (Standatione)	UCS Server (FI-Attached)
		<	Cancel			Back Create

#### **Procedure 5.** Create IMC Access Policy

The IMC Access policy allows you to configure your network and associate an IP address from an IP Pool with a server. In-Band IP address, Out-Of-Band IP address, or both In-Band and Out-Of-Band IP addresses can be configured using IMC Access Policy and is supported on Drive Security, SNMP, Syslog, and vMedia policies.

In the present configuration, customers can create both IN-Band Out of Band IMC Access Policy.

**Note:** In-Band IMC Access Policy is required to utilize operating system installation feature of Cisco Intersight.

- **Step 1.** Click Infrastructure Service, select Policies, and click Create Policy.
- Step 2. Select UCS Server, then select IMC Access and click Start.
- Step 3. Select Organization, Name the IMC Access policy, then click Next.
- **Step 4.** Select UCS Server (FI-Attached).
- **Step 5.** Select the In-Band Configuration option.
- Step 6. Enter VLAN for IN-Band Access and select the IN-Band IP Pool created during IP Pool configuration.
- Step 7. Enable Out-of-Band (OOB) configuration, Select IP Pool (as created under 'Create Pools') section.
- Step 8. Click Create.

General	Policy Details Add policy details.	
2 Policy Details	In-Band Configuration VLAN ID* 1080 0 - 4093 IPv6 address configuration IPv6 Address configur	VCS Chassis
	Selected IP Pool Coh-INBand (D) (D) Edit Selection (E) (D) (D) (D) (D) (D) (D) (D) (D) (D) (D	

### Procedure 6. Create IPMI over LAN Policy

**Note:** The highest privilege level that can be assigned to an IPMI session on a server. All standalone rack servers support this configuration. FI-attached rack servers with firmware at minimum of 4.2.3a support this configuration.

**Note:** The encryption key to use for IPMI communication. It should have an even number of hexadecimal characters and not exceed 40 characters.

- Step 1. Click Infrastructure Service, select Policies, and click Create Policy.
- Step 2. Select UCS Server, IPMI over LAN and click Start.
- Step 3. Select Organization, Name the IPMI Over LAN policy, then click Next.
- Step 4. Select UCS Server (FI-Attached).
- Step 5. For the Privilege Level, select admin and enter an encryption key.

≡	eisee Intersight 🐉	g Infrastructure Service 🤟		Q Search	Ø	41 Q	0	R
:\$:	Overview							
© ,¢	Oparata        Servers        Chassis        Fabric Interconnects        HyperFlex Clusters        Integrated Systems        Configure        Profiles        Pools	General     Policy Details	Policy Details Ad policy datalis C C C C C C C C C C C C C C C C C C C	∑ ATPattores   UCS Server (5)	entstores)	UCS Ser	w (f)-Attac	41m2)
		<	Cancel			Bac	Crea	ite

#### Step 6. Click Save.

#### Procedure 7. Create Serial over LAN Policy

**Step 1.** Click Infrastructure Service, select Policies, and click Create Policy.

**Step 2.** Select UCS Server, then select Serial Over LAN and click Start.

Step 3. Name the Serial Over LAN policy and click Next.

Step 4. Select UCS Server (FI- Attached) and the select the Baud Rate of 11520. Click Create.

	tiste Intersight	nfrastructure Service 🗸		Q Search	Ø 💷 🕫 📧	Q 053 A14 (?)	<u>ר</u> א
XÂX	Overview	Policies > Serial Over LAN > AA08-XSeries-	sol				
	Operate        Servers        Chassis        Fabric Interconnects        HyperFlex Clusters        Virtualization        Kubernets        Integrated Systems        Configure        Profiles        Profiles        Pools	Ceneral     Policy Details	Policy Details Add policy details Enable Senal Over LAN () Baud Rate 115200 $\checkmark$ ()		All Platforms   UCB Server 198	udalone) UCS Server 01-A	tached)

#### **Procedure 8.** Create Local User Policy

Step 1. Click Infrastructure Service, select Policies, and click Create Policy.

Step 2. Select UCS Server, then select Local User and click Start.

Step 3. Name the Local User policy and click Next.

**Step 4.** Add a local user with the name admin and role as admin and enter a password. This is used to access the server KVM through KVM IP. Click Create.

there intersight	t 🎝 🖓 Infrastructure Servic		Q Search	
Policies > Lo Create	ocal User			
General     Policy Details	ai Details	Policy Details Add policy details Password Properties Enforce Strong Password () Password History () 5 Local Users () This policy will remove existing user accounts other than the ones config deleted from the endpoint device. You can only enable/disable or chang user name and role as "admin", if there are no users in the policy, only the deleted from the endpoint device. You can only enable/disable or chang user name and role as "admin", if there are no users in the policy, only the default, IPM support is enabled for all users	All Pair  assword Expiry      and User Password      C      gured with this policy. However, the default admin      e account password for the admin account by cre     admin user account will be available on the end	tforms UCS Server (Standaione) UCS Server (FI-Attached)
		Add New User  - admin (admin)  Username *  admin Password *	Role ① admin Password Confirmation * ① Show	Enable 🗎
	<	Cancel	show	Show Back Cree

### Procedure 9. Create LAN Connectivity Policy

**Note:** For Cohesity network access, the LAN connectivity policy is used to create two virtual network interfaces (vNICs); vNIC0 and vNIC1. Each vNIC0 and vNIC1 are pinned on Switch ID A and Switch ID B respectively with the same Ethernet network group policy, Ethernet network control policy, Ethernet QoS policy and Ethernet adapter policy. The two vNICs managed by Cohesity for all UCS Managed mode or Intersight Managed mode (connected to Cisco UCS Fabric Interconnect) should be in Active-Backup mode (bond mode 1).

**Note:** The primary network VLAN for Cohesity should be marked as native or the primary network VLAN should be tagged at the uplink switch.

**Note:** For UCS Managed or IMM deployments, it is recommended to have only two (2) x vNIC (active-backup) for all Cohesity deployments. To allow multiple network access through VLAN, Cohesity supports configuration of a sub-interface, which allows you to can add multiple VLANs to the vNIC.

**Note:** This configuration does allow more than two (2) vNICs (required for Layer2 disjoint network); the PCI Order should allow the correct vNIC enumeration by the Operation System.

Step 1. Click Infrastructure Service, select Policies, and click Create Policy.

Step 2. Select UCS Server, then select Lan Connectivity Policy and click Start.

≡	the intersight	📲 Infrastructure Service 🗸		Q Sear	ch	⊘ <u>⊜</u> ≱ g	a 🚥 🕻 C	) <b>(0</b> 53) ( <b>A</b> 14)	0	۶
:0:	Overview	+ Policies Create								
0	Operate ^ Servers Chassis	Filters	Adapter Configuration	Ethernet GoS	ISCSI Static Target	() sp	Card			
ç	Fabric Interconnects HyperFlex Clusters Virtuelization Kubernetes Integrated Systems Configure	All  UCS Sorver  UCS Domain  UCS Denseis  HyperFlex Cluster  Kubernetes Cluster	BIOS Boot Order Certificate Management Device Derinector Drive Security Ethernet Adapter	FC Zone     Fibre Channel Adapter     Fibre Channel Network     Fibre Channel QoB     Firmware     IMC Access	LAN Connectivity     LDAP     Local User     Network Connectivity     NTP     Persistent Memory	580 554 554 554 555 555 556 556 556 556	tal Over LAN ITP MIP H Frage slog			
(	Templates Policies Pools		Ethernet Network Control     Ethernet Network Croup	IPMI Over LAN	SAN Connectivity	O VI	tual KVM tual Media			
			Cancel						Sta	ert

Step 3. Name the LAN Connectivity Policy and select UCS Server (FI Attached).

## Step 4. Click Add vNIC.

≡	esso Intersight	"%: Infrastructure Service $$	Q Search 🧿 💿 🕫 🗘 🕫 🥵 🥵 🖉
:0:	Overview	Policies > LAN Connectivity	
0	Operate		
	Servers	General	None Pool Static
	Chassis	2 Policy Details	
	Fabric Interconnects		Inside of the second s second second sec
	HyperFlex Clusters		vNIC Configuration
	Virtualization		
	Kubernetes		Manual vNICs Placement Auto vNICs Placement
	Integrated Systems		
,0	Configure	×	For manual placement option you need to specify placement for each vNIC. Learn more at Help Center
	Profiles		Add while
	Templates		
	Policies		□ / Add Filter 0 items found 9 ∨ per page K < 0 of 0 ∑ ∞ . ③
	Pools		Name  Slot ID  Switch ID  PCI Order  Failover  NAC Pool
			NO ITEMS AVAILABLE
			के १ न जिस्सार जिस्सार
		<	Cancel Back Create

- Step 5. Name the vNIC "vNIC0."
- **Step 6.** For the for vNIC Placement, select Advanced.
- Step 7. Select MAC Pool A previously created, Switch ID A, PCI Order 0.

eilede Intersight Structure Service V	Q Search
Policies > LAN Connectivity Create	
Add vNIC	
VNICO Pin Group Name ~	
Pool     Static       Mac Pool * ①        Selected Pool Coh-MAC-A     Ø       Edit Selection     🖻	
Placement Simple Advanced	
When Simple Placement is selected, the Slot ID and PCI Link are automatically determined by the system. vNICs are deployed on the first VIC. The Slot ID determines the first VIC. Slot ID numbering begins with MLOM, and thereafter it keeps incrementing by 1, starting from 1.	
Switch ID* ① A	
PCI Order () 0	
Consistent Device Naming (CDN)	

**Step 8.** Create the Ethernet Network Group Policy; add the allowed VLANs and add the native VLAN. The primary network VLAN for Cohesity should be marked as native or the primary network VLAN should be tagged at the uplink switch.

≡ '' <sup>1</sup> !:	ili: Intersight 🍂 Infrastructure Servic	• ~	Q Search	C	0	Å	۵ 💿 🕰	0	A
۰	Policies > LAN Connectivity > Create Create Ethernet Network	Group							
0 0 0	General     Policy Details	Policy Details         Manage policy settings and allowed VLANs.         Enable QinQ (802:10-in-802:10) Tunneling on the vNIC         Add VLANs ~         Ito set a native VLAN, in the row actions, select Set Native VLAN. To rest and the vNLAN.	emove a native VLAN, select <b>Unset Native VLAN</b> . If a nat	ive VLA	N is		Show VL	AN ID F	langes
		atready assigned, any change may lead to brief network interruptions	at the time of profile deployment.				(	₫Exp	xort \$
		□ 1062 □			Rows p	er page	<u>10 ~</u> <	1	>
			Þ						
	K	Cancel					Back	6	eate

**Step 9.** Create the Ethernet Network Control policy; name the policy, enable CDP, set MAC Register Mode as All Host VLANs, and keep the other settings as default.

	disto Intersight	👌 Infrastructure Service 🗸		Q Search	Ø @2 A ™	Q 053 (A14)	0
÷	Overview	Policies > LAN Connectivity > Create	twork Control				
0	Operate Servers Chassis Fabric Interconnects HyparFlex Clusters Virtualization Kubernetes Integrated Systems Configure Profiles Templates	<ul> <li>General</li> <li>Policy Datalls</li> </ul>	Policy Details Ad policy details This policy is applicable onthe Denable CDP MAC Register Mode © Action on Uplink Fall © Ministry With ©	y for UC3 Servers (FI-Attached)	ver if uplink connectivity is lost, .		
	Policies	c	Cancel			Back	Create

**Step 10.** Create the Ethernet QoS Policy; edit the MTU to 9000 and keep the Priority as best-effort.

≡	attation Intersight 🥼	infrastructure Service 🖂		Q Search	Ø 💿 2	¶] 📧	Q 053 A14	0	2
:@:	Overview	Policies > LAN Connectivity > Create	S						
0	Operate ^ Servers Chassis Fabric Interconnects	General     Policy Details	Policy Details Add policy details QoS Settings		₹ AIPIstices   UCS	Server (Stan	delone)   <u>UCS Server ()</u>	I Attached	<u>1</u>
	HyperFlex Clusters Virtualization Kubernetes Integrated Systems		MTU, Bytes 9000 Burst 10240	1500 - 9000	ate Limit, Mbps riority est-effort			ූ ෙ - 100000 - 4	0
ĺ	Configure A Profiles Templates Policies Pools		Enable Trust Host CaS ©	1 - 100000					
		K	Cancel				Back	Create	

**Step 11.** Create the Ethernet Adaptor Policy; select UCS Server (FI-Attached), Interrupts=10, Receive Queue Count = 8 Receive Ring Size =4096, Transmit Queue Count = 4, Transmit Ring Size = 4096, Completion Queue = 12, keep the others as default, ensure Receive Side Scaling is enabled.

≡	diale Intersight	📽 Infrastructure Service 🗸	Q Search	⊘ © 2
X\$K	Overview	Policies > LAN Connectivity > Create	ter	
0	Operate ^ Servers Chassis Fabric Interconnects HyperFlex Clusters	General       Policy Details	Interrupt Settings	Interrupt Timer, us v © 125 © 0 - 65535
,e	Virtualization Kubernetes Integrated Systems Configure ^		Receive Queue Count         Q         Receive Ring Size         Q           8         1 - 1000         04 - 1	) <b>o</b> 8384
	Profiles Templates Policies		Transmit Gueue Count         Transmit Ring Size         Case         Case	) <b>e</b> 6384
	Pools	<	Completion Queue Count         Completion Ring Size           12         0         1         0           1 - 2000         1         0         1           5         0         0         1	• -255 Back Create

Step 12. Ensure the four policies are attached and Enable Failover is disabled (default). Click Add.

≡	cisco Intersight % Infrastructure Service ~
:@:	Policies > LAN Connectivity Create
0	Consistent Device Naming (CDN)
©,	vNIC Name ~
0	Failover Enabled ()
	Ethernet Network Group * ①         Selected Policy Coh-ethNetworkGrp       Image: Complexity of the selection
	Ethernet Network Control * () Selected Policy Coh-ethControl () Control () Edit Selection ()
	Ethernet QoS * ① Selected Policy Coh-ServerQoS ③ ② 2 Edit Selection ③
	Ethernet Adapter * ① Selected Policy Coh-ethAdapter
	iSCSI Boot ① Select Policy
	Connection
	Disabled usNIC VMQ SR-IOV

diale Intersight 38 Infrastructu	re Service 🗸	Q Search	C 🛛 🕫 🗘 🖓 🖓
Policies > LAN Connectivity Create			
O General     Policy Details	Policy Details Add policy details Enable Azure Stack Host QoS ③ ION		
	None         Pool         Static           This option ensures the IQN name is not associated with the policy		
	VNIC Configuration  Manual vNICs Placement  Auto vNICs Placement  Add  ~	)	Graphic vNICs Edite
	C. Search      Filters 1 results      Name : Stot ID : Switch ID : PCI Order :      vNICO Auto A 0	Fallover : Pin Group : MAC Pool Disabled - Coh-MAC-A	: vNIC Template Template Sync 🛞
			Rows per page 10 ~ (1)
	< Cancel		Back

**Step 13.** Add vNIC as vNIC1. Select the same setting as vNIC0, the only changes shown below.

Step 14. For Switch ID, select B, and the PCI Order should be 1.

Step 15. Optional. The MAC Pool can be selected as the MAC Pool for Fabric B.

**Step 16.** Select the Ethernet Network Group Policy, Ethernet Network Control Policy, Ethernet QoS, and Ethernet Adapter policy as created for vNICO and click Add.

Police 2 LAN Connectivity Create Add vNIC Vitic I Pool Static Pool Static Pool Static Placement Simple Advanced Placement	ritrativ Intersight 🚽 🖧 Infrastructure Service 🗸	Q Sear		
Add vNIC     Name * ①   Image:	Policies > LAN Connectivity Create			
Pool       Static         Mac Pool* ①       ③         Selected Pool Coh-MAC-B       ②         Edit Selection       ③         Placement       □         Simple       Advanced         It       When Simple Placement is selected, the Slot ID and PCI Link are automatically determined by the system. vNICs are deposited on the first VIC. The Slot ID determines the first VIC. Slot ID numbering begins with MLOM, and thereafter it keeps incrementing by 1, starting from 1.         Switch ID* ①       □         PCI Order ②       □         1       □         >=0       >=0	Add vNIC	Pin Group Name ①		
When Simple Placement is selected, the Slot ID and PCI Link are automatically determined by the system. vNICs are deployed on the first VIC. The Slot ID determines the first VIC. Slot ID numbering begins with MLOM, and thereafter it keeps incrementing by 1, starting from 1.   We have the starting from the first VIC. The Slot ID determines the first VIC. Slot ID numbering begins with MLOM, and thereafter it keeps incrementing by 1, starting from 1.   PCI Order () 1 () >= 0	Pool     Static       Mac Pool* ①			
Switch ID* ①       B       PCI Order ①       1       >= 0	When Simple Placement is selected, the Slot ID and PCI deployed on the first VIC. The Slot ID determines the first keeps incrementing by 1, starting from 1.	Link are automatically determined by the system. vNICs are st VIC. Slot ID numbering begins with MLOM, and thereafter it		
	Switch ID * ① B v			
Consistent Device Naming (CDN)	Consistent Device Naming (CDN)			
	' Intersight 🛛 🖧 Infrastructure Service 🗸			
-------------	--	-------------------------------	--------	--
.@.	Policies > LAN Connectivity Create			
© ⊙ €	Consistent Device Naming (CDN) Source ① VNIC Name Failover Enabled ①	~		
	Ethernet Network Group * ①         Selected Policy Coh-ethNetworkGrp       Image: Coh-eth Policy Coh-ethControl * ①         Selected Policy Coh-ethControl       Image: Coh-eth Policy Coh-ethControl * ②         Ethernet QoS * ①         Selected Policy Coh-ServerQoS       Image: Coh-eth Policy Coh-ServerQoS * ③	t Selection 🛛 🕮 ection 📄 🕮		
	Ethernet Adapter * ① Selected Policy Coh-ethAdapter @ Ø Edit Sel iSCSI Boot ① Select Policy Connection	lection 🛛 🖻		
	Disabled usNIC	VMQ	SR-IOV	

**Step 17.** Ensure the LAN connectivity Policy is created as shown below with 2x vNIC and click Create.

≡ :‼	ntersight 3.8 Infrastructur	re Service 🗸	Q Search	0 0 4	Q ( ( ) Q ( ) Q
:0:	Policies > LAN Connectivity				
© 0.	<ul> <li>General</li> <li>Policy Details</li> </ul>	Policy Details Add policy details Enable Azure Stack Host QoS (*) IGN None Pool Static This option ensures the IQN name is not associated with the policy vNIC Configuration			
		Manual vNICs Placement     Auto vNICs Placement       Add        Ø     Q. Search	sults		Graphic vNICs Editor
		Name         :         Slot ID         :         Switch ID         :         PCI Order         :           vNiCO         Auto         A         0	Failover         :         Pin Group         :         MAC Pool           Disabled         -         Coh-MAC-E         Disabled         -         Coh-MAC-E	; vNIC Template	e Template Syn 🛞
		< Cancel			Back Criste

## **Create Server Profile Template**

### Procedure 1. Create Server Profile Template

A server profile template enables resource management by simplifying policy alignment and server configuration. All the policies created in previous section would be attached to Server Profile Template. You can derive Server Profiles from templates and attach to Cisco UCS C-Series nodes for Cohesity. For more information, go to: <u>https://www.intersight.com/help/saas/features/servers/configure#server\_profiles</u>

The pools and policies attached to Server Profile Template are listed in Table 15.

Pools	Compute Policies	Network Policies	Management Policies
KVM Management IP Pool for In-Band and Out-of-Band (OOB) Access	BIOS Policy	LAN Connectivity Policy	IMC Access Policy
MAC Pool for Fabric A/B	Boot Order Policy	Ethernet Network Group Policy	IPMI Over LAN Policy
UUID Pool	Virtual Media	Ethernet Network Control Policy	Local User Policy
		Ethernet QoS Policy	Serial Over LAN Policy
		Ethernet Adapter Policy	Virtual KVM Policy

Table 15. Policies required for Server profile template

Step 1. Click Infrastructure Service, select Templates, and click Create UCS Server Profile Template.

::!: Intersight	re Service 🗸		Q Search	0 0 4 00	4 © 4
 Templates					
UCS Chassis Profile Templates	UCS Domain Profile Templates	UCS Server Profile Templates	vNIC Templates vHBA Templates		
				Create UCS	ver Profile Template
 * All UCS Server Profil  +					
Name	Pilters On	Q Search       C       O       C       Q<	Export :		
		NO ITEM	S AVAILABLE		

Step 2. Name the Server Profile Template, select UCS Sever (FI-Attached) and click Next.

Step 3. Select UUID Pool and all Compute Policies created in the previous section. Click Next.

	" Intersight 💦 🖧 Infrastructure Servic	•	Q Search	C 0 4 0 00 0 X
*	← UCS Server Profile Templates Create UCS Server Profile	Template		
	General     Compute Configuration     Management Configuration     Storage Configuration     Storage Configuration     Setwork Configuration     Ge Summary	Compute Configuration Create or select existing Compute policies that you want to associate with this template. UUID Assignment UUID Pool O Selected Pool Coh-UUID © C Edit Selection © BIOS Boot Order Firmware Power Thermal Virtual Media		Coh-BiOS     Ch-BiOS     Ch-BiOS
	K	Close		Back Next

**Step 4.** Select all Management Configuration Policies and attach to the Server Profile Template.

≣ '¦	🕬 Intersight 💦 🍰 Infrastructure Servi	ce ~	Q Search	C	Ø	₽	Q 🔘 🚳	0	<u>୍</u>
:0:	← Templates Create UCS Server Profile	e Template							
0. • •	<ul> <li>Ceneral</li> <li>Compute Configuration</li> <li>Management Configuration</li> <li>Storage Configuration</li> <li>Network Configuration</li> <li>Summary</li> </ul>	Management Configuration Create or select existing Management policies that you want to associate with this template. Certificate Management IMC Access. IPMI Over LAN Local User Berial Over LAN SNMP Syslog Virtual KVM					© Coh-IMC © C © Coh-Ic © Coh-Ic	Access oh-IPMI caluser -syslog • vKVM	
	<	Close					Ba	ck N	lext

Step 5. Skip Storage Polices and click Next.

**Step 6.** Under Network Configuration, select the LAN connectivity Policy created in the previous section and click Next.

<b>≡</b> -the	;' Intersight 🌐 🎝 🕯 Infrastructure Serv	ice 🗸	Q Search	C © 4 0 00 0 X
÷	← Templates Create UCS Server Profil	le Template		
© © •	<ul> <li>General</li> <li>Compute Configuration</li> <li>Management Configuration</li> <li>Storage Configuration</li> <li>Network Configuration</li> <li>Summary</li> </ul>	Network Configuration Create or select existing Network Configuration policies that you wan LAN Connectivity SAN Connectivity	nt to associate with this template.	Coh-LANConnectivity
	K	Close		Back

**Step 7.** Verify the summary and click Close. This completes the creation of Server Profiles. The details of the policies attached to the Server Profile Template are detailed below.

	" Intersight % Infrastructure Service		Q Search	0 0 0 0	A
:@.	← Templates Create UCS Server Profile	Template			
	<ul> <li>General</li> <li>Compute Configuration</li> <li>Management Configuration</li> <li>Storage Configuration</li> <li>Network Configuration</li> <li>Summary</li> </ul>	Summary         Verify details of the template and the policies, resolve errors and deploy. <ul> <li>General</li> <li>Name</li> <li>Organizatio</li> <li>default</li> <li>Target Platform</li> <li>UCS Server (FI-Attached)</li> </ul> Management Configuration     Istorage Configuration         BIOS       Boot Order       UUID       UUID         Virtual Media       Virtual Media       Istorage	n Network Configuration	Coh-BiOS () Coh-BiOS () Coh-BiOtOrder () Coh-UUID X virtualMedia1 ()	
	¢	Close		Back Derive Pro	ofiles
- CIS	Intercient an Intracture Convice		O Count		0
¢.	Templates     Create UCS Server Profile	~ Template	Q Search	0 14 0 19 0	A
@ 0 0	Tremplates     Create UCS Server Profile     General     Compute Configuration	Template Summary Verify details of the template and the policies, resolve errors and deploy. General	Q Search		<u>م</u>
* 0 0		Template Summary Verify details of the template and the policies, resolve errors and deploy. General Name Organizatik Coh-ServerTemplate default Target Platform UCS Server (FH-Attached)	Q Search		Α

≡ #	sco Intersight 💏 Infrastructure Ser	rvice v	Q Search	C 0 4 0 0 8
181	← Templates Create UCS Server Prof	ile Template		
10 0	<ul> <li>General</li> <li>Compute Configuration</li> <li>Management Configuration</li> <li>Storage Configuration</li> <li>Network Configuration</li> <li>Summary</li> </ul>	Summary Verify details of the template and the policies, resolve errors General Name Coh-Server(Template Target Platform UCS Server (FI-Attached) Compute Configuration Management Configura LAN Connectivity	and deptoy. Organization default tion Storage Configuration Network Configur	ation Errora/Warnings (0) Coh-LANConnectivity
		Close		Back Derive Profiles

## Install Cohesity on Cisco UCS C-Series Nodes

The Cohesity Data Cloud can be installed on Cohesity certified Cisco UCS nodes with one of two options:

• Install OS through Intersight OS installation.

This allows installing the Cohesity Data Cloud operating System through Cisco Intersight. You are required to have an Intersight Advantage license for this feature. The operating system resides on a local software repository as an OS Image Link configured in Cisco Intersight. The repository can be a HTTTPS, NFS or CIFS repository accessible through the KVM management network. This feature benefits in the following ways:

- It allows the operating system installation simultaneously across several Cisco UCS nodes provisioned for the Cohesity Data Cloud.
- It reduces Day0 installation time by avoiding mounting the ISO as Virtual Media on the KVM console for each node deployed for the Cohesity Data Cloud on each Cisco UCS C-Series node.
- Install the OS by mounting ISO as virtual Media for each node.

### **Derive and Deploy Server Profiles**

### **Procedure 1.** Derive and Deploy Server Profiles

In this procedure, Server Profiles are derived from Server Profile Template and deployed on Cisco UCS C-Series nodes certified for the Cohesity Data Cloud.

**Note:** The Server Profile Template specific to the Cohesity Data Cloud were configured in the previous section. The Server Profile Template can be created through the Cohesity Ansible Automation playbook or through the Manual creation of Server Policies and Server Template.

**Step 1.** Select Infrastructure Service, then select Templates and identify the Server Template created in the previous section.

UCS Chassis Profile Templates UCS Domain Profile Templates UCS Server Profile Templates vNIC Templates vHBA Templates * AI UCS Server Profile @ +	Templates				
KAI UCS Server Profil.      +      Create UCS Server Profil.      *      Al UCS Server Profil.      *      *      Create UCS Server Profil.      *      Create UCS Server Profil.      Con-ServerTemplate     0 UCS Server (I'-Attached)     a few seconds ago	UCS Chassis Profile Templates	UCS Domain Profile Templates UCS Server Profile Templates	vNIC Templates vHBA Templates		
* All UCS Server Profil         +           Image:         Target Platform         :         Description         Last Update         :           Image:         Target Platform         :         Description         Last Update         :         :           Image:         Coh-ServerTemplate         :         UCS Server (FI-Attached)         :         :         :         :				Create UCS Serve	er Profile Temp
Image: Search         Tristers         Tresuits           Image: Target Platform         : Description         Last Update         : Image: Target Platform           Image: Coh-ServerTemplate         0         UCS Server (FI-Attached)         a few seconds ago					
Name         :         Usage :         Target Platform         :         Description         Last Update         :           Coh-ServerTemplate         0         UCS Server (FI-Attached)         a few seconds ago         .	* All UCS Server Profil				
Coh-Server/Emplate 0 UCS Server (Fi-Attached) a few seconds ago	* All UCS Server Profil  + Q Q P Q Q Search	▼ Filters 1 results			් Exp
	* All UCS Server Profil  +   All UCS Server Profil +   C Search  Name	Filters 1 results     Usage : Target Platform	: Description	Last Update	É Exp

Step 2. Click the ... icon and select Derive Profiles.

-	tise Intersight	~~ Infrastructure Service $~~$	Q Search	C ⊘	\$1 D @	<b>2 (11)</b> ⑦   久
:@:	Overview	Templates				
		UCS Chassis Profile Templates UCS Domain Profile Templates	UCS Server Profile Templates vNIC Templates vHB	A Templates		
0	Operate ^				Create UCS S	erver Profile Template
	Servers	* All UCS Server Profil				
	Chassis	Ø  ☐ Q Search  ▼ Filters 1 res	ults			🛆 Export
	Fabric Interconnects	Name : Usage :	Target Platform Description		Last Update	: 4
	HyperFlex Clusters	Coh-ServerTemplate 4	UCS Server (FI-Attached)		Oct 29, 2024 5:28	AM
	Integrated Systems	/ / 8		R	ows per page 10	Derive Profiles
~						Delete
O.	Analyze ^					Edit

Step 3. Identify and select the Cisco UCS C-Series nodes for Server Profile deployment and click Next.

UCS Server Profile Templates >					Ű
Derive	Coh-ServerTemplate				
5 Ceneral 9 2 Details 6 3 Summary	General Select the server(s) that need to be assigned to pro derive and assign the servers later. Source UCS Server Profile Template Name Coh-ServerTemplate Target Platform	offie(s) or specify the number of profiles that you want to Organization default			
	UCS Server (H-Artached)    Server Assignment  Assign Now From a Resource Pool C	Chassis Slot Location Serial Number Assign Later			
	Q Search Filters View Control V	: 4 results : Health : Model	UCS Domain	Serial Number :	xpo
	Q Search V Filters Vame : User Label AA09-FI-DP-6454-1	i 4 results i Health i Model O Healthy UCSC-C240-M6L	UCS Domain AA09-FI-DP-6454	Serial Number : WZP2651059D	xpor
	Q. Search         V Filters           V         Name         : User Label           AA09-F1-DP-6454-1         AA09-F1-DP-6454-2	i 4 results i Health i Model O Healthy UCSC-C240-MBL O Healthy UCSC-C240-MBL	UCS Domain AA09-FI-DP-6454 AA09-FI-DP-6454	Serial Number : WZP26510590 WZP2651055Z	xpor

Step 4. Select organization (default in this deployment), edit the name of Profiles if required and click Next.

UCS Server Profile Templates > 0 Derive	Coh-ServerTemplate			
-	UCS Server (FI-Attached)			
General	Description			
2 Details	Description			
3 Summary	1	0 / 1024		
0	Set Tags			
	Enter a tag in the key:value format.			
	^ Derive			
	Profile Name Prefix	Digits Count	Start Index for Suffix	
	Coh-ServerTemplate_DERIVED-	1	1	
			>=1 >=	0
	1 Name *	Organization *	Assigned Server	
	Coh-ServerTemplate_DERIVED-1	default	~ AA09-FI-DP-645	4-1
	2 Name*	Organization *	Assigned Server	
	Coh-ServerTemplate_DERIVED-2	default	AA09-FI-DP-645	4-2
	3 Name*	Organization *	Assigned Server	
	Coh-ServerTemplate_DERIVED-3	default	AA09-FI-DP-645	4-3
	4 Name*	Organization *	Assigned Server	
	Coh-ServerTemplate_DERIVED-4	default	AA09-FI-DP-645	4-4

**Step 5.** All Server policies attached to the template will be attached to the derived Server Profiles. Click Derive.

**Step 6.** The Server Profiles will be validated and ready to be deployed to the Cisco UCS C-Series nodes. A "Not Deployed" icon will be displayed on the derived Server Profiles.

	l" Intersight 🏻 🖧 In	frastructure Service 🗸				Q Search	C © & ¢ @ (	<u>।</u> 🤨 🖉
.@	Profiles HyperFlex Cluster Profi	iles UCS Chassis Profil	es UCS Domain	Profiles UCS Server Profile	s			
0	* All UCS Server Profil	@ + Q. Search	▼ Filters	4 results			Create U	CS Server Profile
	Status	Inconsistency Reason	Target Platform					ж
	Name	: Status	:	Target Platform	UCS Server Template	Server	Last Update	: \$
	Coh-ServerTem	plate_DERIVED-4 A Not De	ployed	UCS Server (FI-Attached)	Coh-ServerTemplate	AA09-FI-DP-6454-4	a minute ago	
	Coh-ServerTem	plate_DERIVED-1	ployed	UCS Server (FI-Attached)	Coh-ServerTemplate	AA09-FI-DP-6454-3	a minute ago	
	Coh-ServerTem	plate_DERIVED-2	bloyed	UCS Server (FI-Attached)	Coh-ServerTemplate	AA09-FI-DP-6454-2	a minute ago	
							Rows per page 25 ~	< 1 >

**Step 7.** Select the Not Deployed Server Profiles, click the ... icon and click Deploy.

= :	isco Intersight 💡 🖧 Infrastructure Servi	ce v		Q	Search	C 0 4 000	0 A
ŵ.	Profiles HyperFlex Cluster Profiles UCS Chi	assis Profiles UCS Domai	n Profiles UCS Server Profile	s			
0 • •	* All UCS Server Profil  +	⊽ Filters	4 résults	-		Create U	CS Server Profile
	Activate Unassign Server No data av	YReason Target Platform Pi-Attached 4	Target Platform	UCS Server Template	Server	Last Undate	ж
	Coh-ServerTemplate_DERIVED-4	A Not Deployed	UCS Server (FI-Attached)	Coh-ServerTemplate	AA09-FI-DP-6454-4	a minute ago	
	Coh-ServerTemplate_DERIVED-1	📥 Not Deployed	UCS Server (FI-Attached)	Coh-ServerTemplate	AA09-FI-DP-6454-1	a minute ago	
	Coh-ServerTemplate_DERIVED-3	A Not Deployed	UCS Server (FI-Attached)	Coh-ServerTemplate	AA09-FI-DP-6454-3	a minute ago	
	Coh-ServerTemplate_DERIVED-2	A Not Deployed	UCS Server (FI-Attached)	Coh-ServerTemplate	AA09-FI-DP-6454-2	a minute ago	
	🖉 🧷 📋 Selected 4 of 4 🛛 S	how Selected Unselect All				Rows per page 25 ~	< 1 >

Step 8. Enable Reboot Immediately to Activate and click Deploy.

Deploy (4 UCS Serve	Deploy (4 UCS Server Profiles)									
Selected UCS server profiles w	ill be deployed to their assigned	servers.								
If policy configuration required deployment will not be initiated by the second	If policy configuration requires an immediate reboot and the option below is disabled, then profile deployment will not be initiated.									
∧ More Details										
Q Search		( Export								
Server Name	Profile Name	Reboot								
AA09-FI-DP-6454-4	Coh-ServerTemplate_DERIVED-4	YES								
AA09-FI-DP-6454-1	Coh-ServerTemplate_DERIVED-1	YES								
AA09-FI-DP-6454-3	Coh-ServerTemplate_DERIVED-3	YES								
AA09-FI-DP-6454-2	Coh-ServerTemplate_DERIVED-2	YES								
	Rows pe	r page $25 \vee (1) >$								
Reboot Immediately to Activate		$\searrow$								
		Cancel								



Profiles	← Requests Deploy Server Profile		
HyperFlex Cluster Profiles	Details	Execution Flow	
* All UCS Server Profil @	Status	Progress	8%
		Power on server	
	Name Deploy Server Profile	<ul> <li>Validate user access to the network policies</li> </ul>	Sep 27, 2024 1:31 PM
Status	Inc	<ul> <li>Validate user access to the compute and management policies</li> </ul>	Sep 27, 2024 1:31 PM
Not Deployed 2	ID NC 66f7162e696f6e32013f4896	<ul> <li>Validate user access to the profile</li> </ul>	Sep 27, 2024 1:31 PM
Name	Target Type Rack Server		
Coh-ServerTemplate	AA09-FI-DP-6454-1		
Coh-ServerTemplate	Source Type		
Coh-ServerTemplate	Server Profile		
	Source Name Coh-ServerTemplate_DERI		
	Initiator andhiman@cisco.com		

**Step 10.** When the Server Profile deployment completes successfully, you can proceed to the Cohesity Data Cloud deployment on the Cisco UCS nodes.

≡	elision Intersight 😪 😪 Infrastructure Service 🗸			Q Search	C 0 4	1 Q 💿 🚳	ଡ
	Servers						
•	* All Servers  +  Q Search	<b>Filters</b> 4 results				l	∆ Export
,e	Health Power (1) On 4 W Healthy 4	HCL Status Bundle Versi	on         Firmware Version           • 4.2(3h) 4         • 4.2(3)	h) 4 <b>Models</b>	Contract Status O Not Covered 4 4	Profile Status	ж → ←
	Name : Health	: Model :	CPU Capacity 💿 : Memory Capa	city : UCS Domain	Server Profile	Bundle Version	: \$
	C O AA09-FI-DP-645 O Healthy	UCSC-C240-M6L	128.0	128.0 AA09-FI-DP-6454	Coh-ServerTempla ⊘	4.2(3h)	***
	C AA09-FI-DP-645 O Healthy	UCSC-C240-M6L	128.0	128.0 AA09-FI-DP-6454	Coh-ServerTempla 🕗	4.2(3h)	
	C O AA09-FI-DP-645 O Healthy	UCSC-C240-M6L	128.0	128.0 AA09-FI-DP-6454	Coh-ServerTempla 📀	4.2(3h)	
	C AA09-FI-DP-645 O Healthy	UCSC-C240-M6L	128.0	128.0 AA09-FI-DP-6454	Coh-ServerTempla 🥝	4.2(3h)	***
					Rows per pa	ige 10 ~	1 >

**Step 11.** Access KVM with KVM username > admin and password > <<as configured in local user policy>>, and make sure the node is accessible.

**Step 12.** Virtual KVM can be accessed by directly launching from Cisco Intersight (Launch vKVM) or access the node management IP.

**Note:** Installing OS through Launch vKVM may lead to timeout during Cohesity OS installation. It is recommended to directly access the KVM through node management IP during OS installation. Install OS through Cisco Intersight

### Day 0 Firmware Upgrade

### Procedure 2. Day 0 Firmware Upgrade

Prior to installing Cohesity OS, it is highly recommended to upgrade the Cisco UCS C-Series Firmware to the recommended Cisco UCS C-Series Firmware release. This procedure expands on the process to upgrade the Cisco UCS C-Series node firmware and should be executed only during the following scenarios:

- 1. During creating of a **new cohesity cluster** with Cisco UCS C-Series nodes.
- Adding new nodes to cluster. The firmware should be upgraded to new nodes before installing Cohesity OS.
- 3. Firmware upgrade of Cisco UCS C-Series nodes during **maintenance window**. This requires shutting down the entire Cohesity cluster.

**Step 1.** Select Infrastructure Service, then select Servers and identify the new Cisco UCS C-Series nodes available for Cohesity cluster creation or nodes available to add to existing cluster. Ensure Server Profile is successfully deployed to the Cohesity nodes

≡ "å	sco Intersight 🦂 📲 Infrastructure Service 🗸			Q Search	C ⊚ ⊄	۵ 💿 🕰	0	R
	Servers							
	* All Servers 🐵 +							
	··· Ø Q Search	Filters 4 results					🛆 Exp	ort
	Health Power	HCL Status Bundle Version	Firmware Version	Models	Contract Status	Profile Status		X
	4 #Healthy 4	() Incomplete 4	• 4.2(3h) 4 4.2(3h) 4	4 C240 M6L 4	Not Covered 4	4	OK 4	→ ←
	Name ÷	Health : Model :	CPU Cap © : Memory Cap :	UCS Domain : Server Pr	ofile	1	Bundle Ve	\$
	C 0 AA09-FI-DP16454-1	CSC-C240-M6L	128.0 128.0	0 AA09-FI-DP-6454 Coh-Ser	verTemplate_DERIVED-1	0	4.2(3h)	***
	C 4A09-FI-DP-6454-2	Healthy UCSC-C240-M6L	128.0 128.0	AA09-FI-DP-6454 Coh-Ser	verTemplate_DERIVED-2	Ø	4.2(3h)	***
	O AA09-FI-DP-6454-3	C Healthy UCSC-C240-M6L	128.0 128.0	AA09-FI-DP-6454 Coh-Ser	verTemplate_DERIVED-3	Ø	4.2(3h)	•••
	C AA09-FI-DP-6454-4	Healthy     UCSC-C240-M6L	128.0 128.0	AA09-FI-DP-6454 Coh-Sen	verTemplate_DERIVED-4	0	4.2(3h)	••••
	Ø				Rows per page	10 ~	< 1	

Step 2. Select the servers, Click the ellipses "..." and select 'Upgrade Firmware' option

≡ :	ill' Intersight 🕴 🔐 Infrastr	ructure Service 🗸			يد فرار عا		Q Search	C © d	A 000	0	l A
۹	Servers										
	* All Servers  + Q Search		Filters 4 resul	s						🛆 Exp	port
9 9	Power > System > Profile >	Power (1) On 4	HCL Status	Bundle Version 4 4.2(3h) 4	Firmware Versio	n 4.2(3h) 4	Models	Contract Status Not Covered 4 240 M6L 4	Profile Status	• OK 4	$\rightarrow$
	VMware >	: He	alth : M	odel : CPU Cap	<ul> <li>: Memory C</li> </ul>	ap :	UCS Domain :	Server Profile		Bundle V	÷
	Start Alarm Suppression	i4-1	O Healthy U	CSC-C240-M6L	128.0	128.0	AA09-FI-DP-6454	Coh-ServerTemplate_DERIVED-1	0	4.2(3h)	
	Stop Alarm Suppression	64-2 64-3	C Healthy U	CSC-C240-M6L CSC-C240-M6L	128.0	128.0	AA09-FI-DP-6454 AA09-FI-DP-6454	Coh-ServerTemplate_DERIVED-2 Coh-ServerTemplate_DERIVED-3	Ø	4.2(3h) 4.2(3h)	
		i4-4	O Healthy U	CSC-C240-M6L	128.0	128.0	AA09-FI-DP-6454	Coh-ServerTemplate_DERIVED-4	0	4.2(3h)	••••
	···· 🧷 Selected 4 of 4	Show Selected	Inselect All					Rows per p	age 🚺 🖂	< 1	>

**Step 3.** Select Start Firmware upgrade and ensure the Cisco UCS C-Series nodes are selected. Click Next.

← Servers	mware								
1 General 2 Version		General	nents for firmware upgrade.						
3 Summary	(	Q Search	Filters 4 results	: Model		Firmware Version		UCS Domain	6
	-	AA09-FI-DP-6454-4		UCSC-C240	M6L	4.2(3h)		AA09-FI-DP-6454	0
		AA09-FI-DP-6454-1		UCSC-C240	M6L	4.2(3h)		AA09-FI-DP-6454	
		AA09-FI-DP-6454-3		UCSC-C240	M6L	4.2(3h)		AA09-FI-DP-6454	
		AA09-FI-DP-6454-2		UCSC-C240	M6L	4.2(3h)		AA09-FI-DP-6454	
		Selected 4 of 4 Show Selected	Unselect All				Rows	per page 10 ~	) (1)

**Step 4.** Identify the recommended Firmware version. In general, the recommended sign is displayed on the firmware. Click Next.

**Note:** By default the drive and storage controller firmware is also upgraded. To avoid drive failure and improve the resiliency of drives, it is recommended to upgrade drive firmware. Drives can be excluded from firmware upgrades, through 'Advanced Mode'.

	ilialle Intersight 👘 🖧 Infrastructure Servi	ce 🗸			Q Search	C	$\odot$	₽	۵ 💿 🖾	0	2
.0	← Servers Upgrade Firmware										
0	General	Version Select a firmware version to u	pgrade the serv	ers to.							Ì
©. ,©	3 Summary	The selected firmwar storage controllers. U	e bundle will be Jse Advanced M	downloaded from inter ode to exclude upgrade	sight.com. All the server components will be upgraded along with o a of drives and storage controllers.	Irives ar	nd				
		Advanced Mode									
		Filters 27 results	Size :	Release Date :	Description					0	
		0 4.3(4.242038)	889.16 MiB	Sep 26, 2024 7:57	Cisco Intersight Server Bundle					٢	
		0 4.3(4.241063)	917.00 MiB	Aug 21, 2024 8:25	Cisco Intersight Server Bundle					Ð	
		4.3(4.240152) 6	916.98 MiB	Jun 4, 2024 10:13	Cisco Intersight Server Bundle						
		0 4.3(3.240043)	€51.35 MiB	Apr 24, 2024 7:06	Cisco Intersight Server Bundle					æ	
		0 4.3(3.240022)	851.58 MiB	Feb 15, 2024 9:32	Cisco Intersight Server Bundle					Ð	
		0 4.3(2.240009)	805.19 MiB	Mar 7, 2024 9:47 AM	Cisco Intersight Server Bundle					æ	
		0 4.3(2.240002)	804.51 MIB	Jan 24, 2024 10:38	Cisco Intersight Server Bundle					ø	
		4.3(2.230270)	804.67 MiB	Nov 15, 2023 11:12	Cisco Intersight Server Bundle					Ð	
		0 4.3(2.230207)	797.52 MiB	Aug 15, 2023 11:11	Cisco Intersight Server Bundle					¢	
		O 4.2(3I)	870.77 MiB	Jun 17, 2024 11:12	Cisco Intersight Server Bundle					æ	
		Selected 1 of 27 Show Se	elected Uns	elect All	Rows or	r nane	10			>	_
	<	Cancel							Bac	k I	lext

Step 5. Confirm the firmware version for upgrades on Cohesity nodes. Click Upgrade.

Upgrade Firmware						
General     Version     Summary	Summary Confirm configuration and initiate the upgrad Firmware Version 4.3(4.240152) @ Size 916.98 MiB Servers to be Upgraded Q. Search	de. ilters 4 results	Exclud No Exclud No	e Drives e Storage Controllers		습 Export
	Name : User Label	: Model :	Firmware Versi	Requires Reboot 🛇	UCS Domain	UCS Domain
	AA09-FI-DP-6454-4	UCSC-C240-M6L	4.2(3h)	) Yes	AA09-FI-DP-6454	AA09-FI-DP-6454
	AA09-FI-DP-6454-1	UCSC-C240-M6L	4.2(3h)	) Yes	AA09-FI-DP-6454	AA09-FI-DP-6454
	AA09-FI-DP-6454-3	UCSC-C240-M6L	4.2(3h)	) Yes	AA09-FI-DP-6454	AA09-FI-DP-6454
	AA09-FI-DP-6454-2	UCSC-C240-M6L	4.2(3h)	) Yes	AA09-FI-DP-6454	AA09-FI-DP-6454
					Rows per pag	ge 25 ~ (1)

**Step 6.** On the Upgrade Firmware confirmation screen, enable Reboot Immediately to Begin Upgrade.

= :	rule: Intersight   🎉 Infrastructure Service 🗸	Q Search	C ⊘ ⊄	1 <b>0 10 1</b> 0   A
xix	Templates			
	UCS Chassis Profile Templates UCS Domain Profile Templates UCS Server Profile Templates	vNIC Templates vHBA Templates		
0			Cre	ate UCS Server Profile Template
©.	* All UCS Server Profil () +			
	Ø Ø			🛆 Export
	Name : Usage : Target Platform	: Description	Last Update	: 4 1
	Coh-ServerTemplate 0 UCS Server (FI-Attached)	J	a few second	is ago …
			Rows per pa	ge 10 ~ ( 1 )

**Step 7.** Select Infrastructure Service, then select Servers and identify the new Cisco UCS C-Series nodes available for Cohesity cluster creation or nodes available to add to existing cluster.



**Step 8.** Monitor the firmware upgrade process. The firmware is automatically downloaded to the sever end point.

discle Intersight 🔒 🗯 Int	rastructure Service 🗸	Q Search C O	\$ A Q	0 (41)	0	\$
Servers	← Requests Upgrade Firmware					×
* All Servers @ +	Details	Execution Flow				
Health	Status	Progress			13%	
4 • Head	thy 4 Name Upgrade Firmware	Initiate image download to endpoint. Download request for intersight-ucs-server-c240-m6.4.3.4.240152.bin submitted successfully.		Sep 27, 2024	1 2:03 PN	l.
Name	ID: 66f71d95696f6e32013fbf5c	Validate the requirements for the endpoint.		Sep 27, 2024	1 2:03 PN	1
	-6454 Target Type Rack Server					
C AROS I CO	Target Name AA09-FI-DP-6454-2	4				
	Source Type Firmware Upgrade					
	Source Name AA09-FI-DP-6454-2					
	Initiator andhiman@cisco.com					
	Start Time					

Step 9. Confirm on completion of C-Series node firmware to the installed version.

≡	rilision Intersight	Infrastructure Service 🗸		Q Search	C © 40	Ο Ο Ο Ο Ο Ο	୭
:0:	Overview	Servers					
0	Operate ^	* All Servers  +  Q. Search	▼ Filters 4 results			۵	Export
	Chassis Fabric Interconnects	Health Critical 1 Critical 1 Contaction 1 Contaction 1	HCL Status (a) Incomplete 4 Bundle Version 4.3(4.240152) 4	Utility Storage	ersion 4.3(4.240152) 4	Models 4 • C240	₩ → ←
	HyperFlex Clusters	Name :	Health : Model : Server Profile	: UCS Domain :	Bundle Ver :	Serial	: \$
	Integrated Systems	O AA09-FI-DP-6454-1	Healthy UCSC-C240-M Coh-ServerTempla	te_DERIVED-1	4.3(4.240152)	WZP2651059D	
O,	Analyze ^	© AA09-FI-DP-6454-2	Healthy UCSC-C240-M Coh-ServerTempla     UCSC-C240-M Coh-ServerTempla	te_DERIVED-2 ② AA09-FI-DP-64. te_DERIVED-3 ③ AA09-FI-DP-64.	4.3(4.240152) 4.3(4.240152)	WZP2651055Z WZP2651056H	•••
	Explorer New	O AA09-FI-DP-6454-4	Critical UCSC-C240-M Coh-ServerTempla	te_DERIVED-4	4.3(4.240152)	WZP26510561	
,0	Configure ^				Rows per j	page 10 ~ < (	1 >

## **Cohesity OS installation through Cisco Intersight**

#### Procedure 1. Install Cohesity Data Cloud through Cisco Intersight OS Installation feature

This procedure expands on the process to install the Cohesity Data Cloud operating system through the Cisco Intersight OS installation feature.

**Note:** Before proceeding to installing Cohesity OS through Intersight Install feature, please ensure virtual media (vmedia) has the lowest priority in the Cohesity Boot Order policy. This is displayed in screenshot below:

≡	cisco Intersight	🚴 Infrastructure Service 🗸	Q Search	C O 🔹 41 D 02 🗤 O D
	Overview	Policies > Boot Order > Coh-BootOrder     Edit		
0	Operate ^ Servers Chassis Fabric Interconnects	<ul> <li>General</li> <li>Policy Details</li> </ul>	Policy Details Add policy details. Configured Boot Mode © () Unified Extensible Firmware Interface (UEFI) () Legacy () Enable Secure Boot ()	With Platforms         UCS Server (Standalone)         UCS Server (FI-Attached)
	HyperFlex Clusters		Add Boot Device  + Local Disk (m2-1)	Enabled 👜 🛆 🗸
O,	Analyze ^		+ Local Disk (m2-2) 🛇	Enabled in A V
	Explorer New		+ Virtual Media (vmedia-1) 📀	Enabled in A V
1	Configure ^ Profiles Templates Policies Pools			
Nev	Command Palette ×		Cancel	Back Save Save & Deploy

**Note:** This feature is only supported with the Intersight Advantage Tier License.

**Note:** Make sure the certified Cohesity Data Cloud ISO is available from a local repository, for example an HTTPS/NFS/CIFS server. This is a one-time process for each version of the Cohesity Data Cloud ISO.

**Note: OS Installation through Intersight** for FI-attached servers in IMM requires an In-Band Management IP address.(ref: <u>https://intersight.com/help/saas/resources/adding\_OSimage</u>). Deployments not using In-Band Management address can install OS by mounting the ISO through KVM.

- Step 1. Login to Cisco Intersight and click System.
- Step 2. Click Software Repository and click the OS Image Links tab.
- Step 3. Click Add OS Image Link.

=	cisco Intersight	∎∰ System ∨	Q Search	0	<b>和 15 0 000 000 ス</b>
o	Settings	Software Repository			
0	Admin o	Firmware Links OS Image Links SCU Links OS Configuration Files			
ſ	Targets Software Repository				Add 05 Imane Link
	Tech Support Bundles				
	Audit Logs	* All OS Image Links 🐵 🕂			
	Sessions	1 / C Q Add Filter	🕒 Export	10 items found	10 - per page 10 1 of 1 2 2
	Licensing	Name : Vendor : Version : File Locat	ion		: Description : L &

Step 4. Add the location of the Cohesity Data Cloud ISO (NFS/CIFS or HTTPS server) and click Next.

$\equiv$ the line of the second se	ystem ∨	Q Sear	ch C	0	\$	Q @2 A1	0	R
Control of the second sec	ystem V OS Image Links General 2 Details	Ceneral Specify the Operating System source to be used during the installation proc Organization* default File Location* Thips://10.008.18/cohe Mount Options	ch C :ess. ::sity-6.8.2_u1_release-20240509()	⊘	¢1 🖲	Q 02 A3	•	8
	×	Cancel					Ne	ext

**Step 5.** Enter a name for the Repository, for the Vendor enter RedHat, and for the Version enter RHEL7.9. Click Add.

≡ "Indus" Intersight   ∎8 System ∨		Q	Search	C © \$1	Q 💷 🛋 💿   ႙
Settings OS Image Links					
Admin ^ ② General Targets ③ Details Software Repository	Details Review Operating System Name * Cohesi	image details, modify as required, and save t tyLTS	he Operating System image	2.	
Tech Support Bundles	Vendor* Red Ha	it	Version *	rprise Linux 7.9	
Audit Logs Sessions	Set Tags Enter a	tag in the key:value format.	Description Description		
Licensing					
New Command Palette X Navigate Intersignt with CRL+K or go to Help > Command Palette					
	< Cancel				Back

Step 6. Make sure the OS Repository is successfully created in Cisco Intersight.

≡	diale Intersight	System V	Q Search	C	⊙ <b>⊄</b> ] ①	Q 02 (A1)	ଡ   ନ
0	Settings	Software Repository					
U	Admin ^	Firmware Links OS Image Links SCU Links OS Configuration Files					
	Targets					Add OS In	nage Link
1	Software Repository						
	Tech Support Bundles	* All OS Image Links  +				-	
	Audit Logs	Q Search Filters 1 results				e	Export
	Sessions	Name         Vendor         Version         File           CohesityLTS-6.8         Red Hat         Red Hat Enterprise Linux 7.9         htt	e Location : Description ps://10.108.1.8/cohesity-6.8	n	: Last	Update : 17, 2024 3:40 PM	\$ 
	Licensing	n 2 3			Rows per pa	ge 10 ~ <	1 >

**Step 7.** From Cisco Intersight, click Infrastructure Service, then click Servers, and select the Cisco UCS C-Series nodes ready for the Cohesity Data Cloud installation.

Step 8.	Click the .	and select	Install	Operating	System.
---------	-------------	------------	---------	-----------	---------

Healthy	, i	🖧 Infrastructure Service 🗸			Q Search	00400	• •	R
<b>(0</b> )	No Alarma	Servers						
.¢.	Overview							
0	Operate ^	* All Servers . +	च Filters 4 result	s			👌 Exp	oort
1	Servers	Power	HCL Status	Bundle Version	Eirmware Version	Models	Contract S	
	Chassis	System >	(1) On 4 (5) Incomplete 4			-	Not Cov	»× →
	Fabric Interconnects	VMware >		4 • 4.3(4.240152) 4	4.3(4.240152) 4	4 • C240 M6L 4		÷-
	HyperFlex Clusters	Install Operating System	: Health : M	del : CPU.C. © :	Memory C	Server Profile	Bundle	6
	Integrated Systems	- Upgrade Firmware	O Healthy UC	CSC-C240-M 92.8	128.0 AA09-FI-DP-64	Coh-ServerTemplate_DERIVED-1	⊘ 4.3(4.2	2
0	Analyze A	Start Alarm Suppression 54-2 Stop Alarm Suppression	G Healthy UC	SC-C240-M 92.8	128.0 AA09-FI-DP-64	Coh-ServerTemplate_DERIVED-2	⊘ 4.3(4.2	
~	Evelager New	Set License Tier	G Healthy UC	CSC-C240-M 92.8	128.0 AA09-FI-DP-64	Coh-ServerTemplate_DERIVED-3	⊘ 4.3(4.2	2
	Explorer New	C nnos tr pr 0454-4	O Healthy UC	CSC-C240-M 92.8	128.0 AA09-FI-DP-64	Coh-ServerTemplate_DERIVED-4	Ø 4.3(4.2	*
.0	Configure ^	···· Ø Selected 3 of 4 Show	Selected Unselect All			Rows per page 10. ~		

Step 9. Make sure the servers are already selected and click Next.

ealthy	💏 Infrastructure Service 🗸		Q Search	C ⊘	\$1 Q 💿	an 🧿 🛛
<ol> <li>Ho Akrms</li> <li>Overview</li> </ol>	Install Operating System					
Operate     Servers     Chassis	<ol> <li>General</li> <li>Operating System</li> <li>Configuration</li> </ol>	General Select the servers for the Operating System installation Select Servers				
Fabric Interconnects	Server Configuration Utility     Sinstallation Target	Q Search Filters 4 results Name : User Label :	Health : Model		Serial Number	Export
Integrated Systems	6 Summary		Healthy     UCSC     Healthy     UCSC     Healthy     UCSC     Healthy     UCSC	-C240-M6L -C240-M6L -C240-M6L	WZP2651059D WZP2651055Z WZP2651056H	
Analyze     Analyze     Analyze     New		AA09-FI-DP-6454-4 Selected 3 of 4 Show Selected Unselect All	Healthy     UCSC	-C240-M6L Rows per pa	WZP26510561 ge 10 ~	< 1 >
Configure ^		þ				
Templates Policies						
Pools New Command Palette						

**Step 10.** Select the Operating System repository which was previously created with the Cohesity Data Cloud ISO and click Next.

Healthy	🔩 Infrastructure Service 🗸	Q Search	C 0 4 0 00 0 2
No Alarms     Overview	Install Operating System		
Operate Operat	Ceneral Coperating System Configuration Configuration Configuration Utility Configuration Target	Operating System Select an Operating System from the list or add a new image to the repository. Select Operating System Image Add OS Image Link	
HyperFlex Clusters Integrated Systems O Analyze ~ Explorer New	© Summary	Selected servers belong to : 'default'. You can choose to install Operating System from one of th Center:  Search Filters 1 results Name Filte Location Vendor Ven	ne common organizations. Learn more at Help
Configure ^ Profiles Templates Policies Pools		CohesityLTS-6.8 https://10.1081.8/cohesity- Red Hat Red Hat Selected 1 of 1 Show Selected Unselect All	Rows per page 10 ~ < 1 >
New Command Palette		Cancel	Back Next

**Step 11.** From Configuration, click Embedded and click Next (the OS configuration file is already part of Cohesity ISO).

≡	ीकीः Intersight 🏻 🎉 ।	Infrastructure Service 🗸	Q Search 🕑 © 2. 91 15	Q 049 A14	:ତ   ନ
:@:	Overview	OPERATE > Servers	item		
٩	Operate        Servers        Chassis        Fabric Interconnects        HyperFlex Clusters        Virtualization        Kubernetes        Integrated Systems        Configure     ^       Profiles	Ceneral     Operating System     Configuration     Server Configuration Utility     Installation Target     Summary	Configuration         Select configuration source         Cisco       Custom         Embedded         Operating System image must include a configuration file. For an example of the configuration file, see Help Center.		
	Templates Policies Pools	¢	Cancel	Back	( Next

## Step 12. Click Next.

≡	cisco Intersight	📲 Infrastructure Service 🗸	Q Search 🥥 (0.2) 42 (15) Q (0.49) (0.14) (7) Q
:@:	Overview	OPERATE > Servers	tem
0	Operate A Servers Chassis Fabric Interconnects HyperFlex Clusters	Ceneral Operating System Configuration	Server Configuration Utility Select a Software Configuration Utility from the list or add a new image to the repository Select Server Configuration Utility Optional Add SCU Link
,c	Virtualization Kubernetes Integrated Systems Configure	Server Connguration Utility     S Installation Target     B Summary	Server Configuration Utility images are fittered based on the Operating System image selection. Learn more at Help Center.
	Templates Policies Pools		Installing an Operating System is supported only if the Server Configuration Utility image is at version 6.1.3(x) and later.  Add Filter I litems found 10  per page I I of 1 I I I I I I I I I I I I I I I I I I
		<	Cancel Back Hext

**Step 13.** Click Next from the Installation target. Cohesity ISO automatically identifies the Installation target as the 2x M.2 internal drives configured in the Boot Order Server Policy.

Step 14. Verify the summary and click Install.

Healthy	📲 Infrastructure Service 🗸		Q Search	С	Ø	Ø	0	0	R
<ul> <li>No Alattes</li> <li>Overview</li> </ul>	Install Operating System								
Operate     Servers     Chassis	General     Operating System     Configuration	Summary Verify details of your selections, make change Operating System Image	s where required and proceed to install the Operating System						
Fabric Interconnects HyperFlex Clusters Integrated Systems	<ul> <li>Server Configuration Utility</li> <li>Installation Target</li> <li>Summary</li> </ul>	CohesityLTS-8.8 Vendor Red Hat Configuration	version Red Hat Enterprise Linu	x 7.9					
<ul> <li>Analyze</li> <li>Explorer</li> <li>New</li> </ul>		Embedded Selected Servers							
ی Configure ∧ Profiles		AA09-FI-DP-6454-1 Serial: WZP2651059 AA09-FI-DP-6454-2 Serial: WZP2651055	D Z				View	Details	
Templates Policies Pools		AA09-FI-DP-6454-3 Serial: WZP2651056	н				View	Details	ן
New Command Palette		Cancel					Back	Inst	

Step 15. Accept the warning for overwriting the existing OS image on the node and click Install.

DPERATE > Servers	stem
General Operating System	Summary Verify details of your selections, make changes where required and p
Configuration	
Server Configuration Utility	Warning!
Installation Target	Existing Operating System, if any, will be overwritten and system files will be deleted. Configuration changes required to facilitate OS installation will be made and restored at completion.
6 Summary	
	Cancel Install
	Empeaaea

**Step 16.** Monitor the OS installation progress and wait for completion. Depending on the network bandwidth between the node management network and the repository network, it can take up to 45 minutes for the OS installation to complete.

← Requests Operating System Insta	Ш	×
Details	Execution Flow	
Status	Progress D Install Operating System on Cisco UCS server View Execution Flow	33%
Name Operating System Install ID 644aa929696f6e3101ec4824 Target Type Blade Server	⊘ Confirm Server Configuration for Installation	Apr 27, 2023 9:56 AM
Target Name AA08-XSeries-2-1 Source Type Blade Server		

**Step 17.** Since this is an embedded installation without the Cisco Server Configuration utility, Cisco Intersight displays the OS installation completion in about five minutes. Open a virtual KVM session and monitor the Cohesity OS install progress. Since this is an automated install, you are not required to provide any inputs on the virtual KVM screen. The OS installation progress is shown below:



Step 18. Ensure Cohesity OS is successfully installed on Cisco UCS C-Series nodes.

=	-ili-ili- cisco	Intersight	AA09-F1-DP-6454-1 (Coh-ServerTemplate_DERIVED-1)   KVM Console UCSC-C24D-M6L WZP2651059D
E	Console		Cohesity Version: 6.8.2_u1_release-20240509_a5da4644
	File		Product Name: UCS-C240M6H12 Hostname: chassis-wzp2651059d-node-1
	View		node IPV6; Node IPV6; Link Local IPv4: 169 254 11 119
8	Macros		Link Local IPv6: fe80::ccf7:a1ff:fec9:2941
×	Tools		FOR LOCAL ACCESS, PLEASE CONNECT TO THE SAME SWITCH AS THE NODE AND USE THE LINK LOCAL IP ADDRESS. ENTER THE IP IN YOUR BROWSER TO ACCESS THE COHESITY UI.
Ċ	Power		Hint: Num Lock on
	Boot Devi	ce >	chassis-wzp2651859d-node-1 login:
۵	Virtual Me	edia >	
	Chat		

## Install OS through Virtual Media

### **Procedure 1.** Install the Cohesity Data Cloud through virtual media

This procedure expands on the process to install the Cohesity Data Cloud operating system through virtual media. You need to open a virtual KVM session for each node. Virtual KVM session can be accessed through Cisco Intersight or logging into node management IP assigned during Server Profile deployment.

**Note:** During the OS installation, it is recommended to open vKVM through node management IP. Access the vKVM through the user created in useraccess policy (admin/<<password>>)

**Step 1.** Login to Intersight, Navigate to Infrastructure Service > Servers and identify the node management IP > Identify the node Management IP

iligitic Intersight	📌 Infrastructure Service 🗸		Q Search
) Overview		Critical	
	General Inventory UCS Ser	ver Profile HCL Topology Metrics Conne	ctivity
Operate ^	Details	Properties	
Chassis	Health	Cisco UCSC-C240-M6L	Front Rear Top
Fabric Interconnects	Name		
HyperFlex Clusters	AA09-FI-DP-6454-4		
Integrated Systems	User Label		
Analyze ^	Management IP 10.108.0.164, 10.108.0.167	Power (2) On Locator LED (0) C	Health Overla
Explorer New	Serial WZP26510561	CPUs 2	CPU Capacity (GHz) 92.8
Configure ^	Mac Address	Threads 64	1D 4
Profiles	PID	CPU Cores 32	Adapters 1
Templates	Vendor	CPU Cores Enabled	
Policies	Cisco Systems Inc	32 Memory Capacity (GiB)	300001-000-110-0101-010101011114
Pools	-	128.0	
	Asset Tag		
w Command Palette ×	License Tier		
	Advantage		

**Note:** The existing deployment displays two management IPs. These are IN-Band and Out of Bank management IPs as defined in the Cisco IMC Access Policy. If customers want to install the Cohesity OS only through KVM access then only Out of Band Management IP is required.

Step 2. Login to vKVM with the username/password as defined in the user access policy.



**Step 3.** Select the Cohesity Data Cloud ISO from your local file system and click Map Drive.

=	oliolio cisco vKVM	KVM Console UCSC	C-C240-M6L WZP26510561	
E				
1				
0				
8				
$\times$				
Ċ				
$\uparrow$				
	Virtual Media			
9			Map Virtual Media - CD/DVD	
			Browse Selected File cohesity-6.8.2 u1 releas ×	
			Read Only	
			Cancel	

**Step 4.** Modify the Boot Device to Any Virtual Media , this will implement a one time boot through virtual media and override the default Boot Order Policy.

≡	cisco vKVM	KVM Console	UCSC-C240-M6L	WZP26510561
5	Console >		Product Hostname	Name: UCS-C240M6H12 : chx-c240-1-wzp26510561-
1	File >		Node IPv Node IPv Link Loc	4: 10.108.1.165 6: al IP:4: 169 254 11 133
0	View >		Link Loc	al IPv6: fe80::9071:fdff:
6 <u>6</u>	Macros >		FOR LOCA LINK LOC	L ACCESS, PLEASE CONNECT ' AL IP ADDRESS, ENTER THE
≫	Tools >		Hint: Nu	m Lock on
Ċ	Power >		chx-c240	-1-wzp26510561-node-1 log
$(\uparrow$	Boot Device >	None	5726 5958	.383221] IPMI Watchdog: r .967724] power meter ACPI
٢	Virtual Media >	Any Virtual Me	dia 1602 1602	.449080] XFS (loop1): Sup .636397] XFS (loop1): Sup
Q	Chat	Local HDD	1602 1603 13170605 13170605	.8063621 XFS (loop1): Sup .0923441 XFS (loop1): Sup .5139841 XFS (loop2): Sup .6844451 XFS (loop2): Sup

**Step 5.** Click Power and then click Reset System to reset the power cycle on the node. The Cohesity ISO automatically loads (with virtual Media having highest priority in Boot Order Server Policy).



**Step 6.** The ISO automatically identifies the drives to install the Cohesity ISO; the OS installation completes in about 45-60 minutes.

÷	→ C (▲ Not s	secure	https://10.108.0.21/kvm/
=	cisco VKVM		KVM Console UCSX-210C-M6 FCH243974YZ
b	Console		Starting installer, one moment anaconda 21.48.22.159-1 for CentDS 7 started.
6	File		<ul> <li>solution for the set of the set</li></ul>
0	View		17:25:22 Running pre-installation scripts 17:27:47 Not asking for UNC because of an automated install
6	Macros		17:27:47 Not asking for UMC because text mode was explicitly asked for in kickstart Starting automated install
×	Tools		Generating updated storage configuration Checking storage configuration
O	Power		You have not specified a swap partition. Although not strictly required in all cases, it will s for most installations.
$\uparrow$	Boot Device		
۵	Virtual Media		Installation
Q	Chat		1) [x] Language settings (English (United States))       2) [x] Time settings (America/Los Angeles timezone)         3) [x] Installation source (Local media)       4) [x] Software selection (Custom software selected)         5) [x] Installation Destination (Warning checking storage configuration)       6) [x] Kdump (Kdump is enabled)         7) [ ] Network configuration (Not connected)       8) [ ] User creation (No user will be created)
			Progress Setting up the installation environment Creating ext4 on /dev/nvme1n1pZ Creating mdmember on /dev/nvme1n1p1 Creating ext4 on /dev/nvme0n1pZ

**Step 7.** Repeat this procedure for all the other Cohesity C-Series nodes to be configured for the Cohesity cluster.

## **Configure Cohesity Data Cloud**

This section elaborates on the configuration of the Cohesity Data Cloud on Cisco UCS C-Series Rack servers. The existing deployment is deployed with four (4) Cisco UCS C240 M6 nodes with each node configured with both compute and storage.

**Note:** Make sure the Cohesity OS ISO is installed on each node.

**Note:** The network bonding mode on the Cohesity operating systems (RHEL 7.9)\_ with Cisco UCS C-Series or Cisco UCS Fabric Interconnect Managed C-Series servers does not support bond mode 4. For reference, go to: <u>https://www.cisco.com/c/en/us/support/docs/servers-unified-computing/ucs-b-series-blade-servers/200519-UCS-B-series-Teaming-Bonding-Options-wi.html</u>)

The Data Cloud Cluster configuration is a two-step process:

- · Initial network configuration on 1x Cisco UCS C-Series node
- Cluster configuration across all Cisco UCS C-Series nodes

### **Configure First Node**

#### Procedure 1. Initial Network Configuration on 1x Cisco UCS C-Series Node

In this procedure, any one of the Cisco UCS nodes are accessed through the virtual KVM and the initial operating system network is configured.

**Step 1.** Login to Cisco Intersight, click Infrastructure Service and click Servers. Identify the Cisco UCS C-Series nodes installed with the Cohesity ISO.

	disco Intersight	Infrastructure Service $$	Q Search	C O	ମ ଢ୍ 🚥 💷 💿 🛛 ୧
18	Overview	Servers			
0	Operate ^		ults		👌 Export
	Servers				
	Chassis	Health Power HCL Status	Bundle Version Utility Storag	e Firmware Version	Models yr →
	Fabric Interconnects	4 Healthy 3	4 4.3(4.240152) 4	4.3(4.240152) 4	4 ■ C240 M ←
	HyperFlex Clusters				
	Integrated Systems	AA09-FI-DP-6454-1 Healthy	UCSC-C240-M Coh-ServerTemplate_DERIVED-1	AA09-FI-DP-64 4.3(4.240152)	WZP2651059D
~		C AA09-FI-DP-6454-2 O Healthy	UCSC-C240-M Coh-ServerTemplate_DERIVED-2	AA09-FI-DP-64 4.3(4.240152)	WZP2651055Z ····
(O)	Analyze ^	O AA09-FI-DP-6454-3 O Healthy	UCSC-C240-M Coh-ServerTemplate_DERIVED-3	AA09-FI-DP-64 4.3(4.240152)	WZP2651056H ····
	Explorer New	Critical	UCSC-C240-M Coh-ServerTemplate_DERIVED-4	AA09-FI-DP-64 4.3(4.240152)	WZP26510561
,9	Configure ^			Rows pe	r page 10 ~ < 1 >

Step 2. Select the first node and launch the virtual KVM.

≡	allada Intersight 🍂	Infrastructure Service 🗸		Q Search	C © 4	Q @2 @1 @	8
:0:	Overview	Servers				Power	2
		* All Servers  +				System	5
0	Operate ^	··· Ø Q Search	▼ Filters 4 results			Profile	2
1	Servers					VMware	>
	Chassis	Health Power	HCL Status Bundle Version	Utility Storage Firmware Ver	slon	Install Operating System	
	Fabric Interconnects	4 Critical 1 Healthy 3	4 • 4.3(4.240152) 4	4	<b>4</b> .3(4.240152) <b>4</b>	Launc	
	HyperFlex Clusters					Launch Tunneled vKVM	
	Interested Evisions	Name H	ealth : Model : Server Profile	: UCS Domain :	Bundle Ver	Start Alarm Suppression	
	integrated systems	O AA09-FI-DP-6454-1	Healthy UCSC-C240-M Coh-ServerTemplate	AA09-FI-DP-64	4,3(4.240152)	W Open TAC Case	
0	Applyze	() AA09-FI-DP-6454-2	Healthy UCSC-C240-M Coh-ServerTemplate	DERIVED-2 @ AA09-FI-DP-64	4.3(4.240152)	W Set License Tier	
~	Principation	C 4A09-FI-DP-6454-3	G Healthy UCSC-C240-M Coh-ServerTemplate	DERIVED-3 @ AA09-FI-DP-64	4,3(4.240152)	W Collect Tech Support Bundle	le l
	Explorer New	O AA09-FI-DP-6454-4	Critical UCSC-C240-M Coh-ServerTemplate	DERIVED-4 @ AA09-FI-DP-64	4,3(4.240152)	WZP26510561	D
,6	Configure ^				Rows per pa	ge 10 ~ < 1 >	
	Profiles						

Step 3. Confirm Cohesity OS is installed on the node.



- Step 4. Login to the node with the username <cohesity> and password <received from Cohesity>.
- **Step 5.** Edit the network configuration through the network configuration script:

sudo ~/bin/network/configure\_network.sh.

- **Step 6.** Select option 2 Configure IP Address on interface.
- **Step 7.** Select default interface bond0.
- **Step 8.** Enter the IP Address, Interface Prefix, and Gateway.
- Step 9. Select the default MTU to 1500.
- **Step 10.** Select Y/Yes to make the interface active.
- Step 11. Quit the configure\_network script by entering option 12.

**Step 12.** 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 13.** When network is configured, make sure the OS IP is reachable.



### **Setup Cohesity Cluster**

### **Procedure 1.** Cohesity Cluster Configuration Across all Cisco UCS C-Series Nodes

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, make sure that all Cohesity nodes which are to be included in the cluster have completed their initial software installation, and are fully booted. Additionally, make sure that all necessary IP addresses for all interfaces are known and assigned, and the DNS round-robin entries have been created.

**Step 1.** In a web browser, navigate to the IP address of the first Cohesity node, which was configured in the previous steps. For example: http://10.108.1.163

**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 following credentials:

- Username: admin
- Password: <password>

C	phosity Dask	aboard
Username	Dhesity Dasi	IDUAIU
Password		

**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.

		COHESITY
Start	t Initial Cluster Setup	
The fol	bllowing hardware was detected.	
4	4	
Chassis	Nodes	N
The entir	tire Cluster setup process should take less than an hour. You will need the following information to set i	up your Cluster:
<ul> <li>IP add</li> <li>Cluster</li> <li>Cluster</li> <li>IPMI S</li> <li>IPMI u</li> <li>Search</li> <li>DNS se</li> <li>NTP se</li> </ul>	ldress and IPMI IP address for each of your Nodes er name and cluster domain name er subnet gateway and subnet mask Subnet Gateway and Subnet Mask username and password ch domains servers	
Get St	Started	

**Step 5.** Select the nodes to add to this initial cluster, then click Select Nodes.

	1	2	3
	Select Nodes	Network Settings	Cluster Settings
he following Nodes were	e detected.		Select All
u need a minimum of 3 Nodes	to create a Cluster		
nassis WZP2651055Z		Chassis WZP26510561	
	Veder 1 - 161963887787 Preduct Model: UCS-C240M6H12		Hode 1 - 16190382729 Product Model: UCS C280M6H2
assis WZP2651056H		Chassis WZP2651059D	
	Node 1 - 161963887788 Product Model: UCS-C240M6412		Node 1 - 161963887786 Connected Product Model: UCS-C240M6H12

Step 6. Enter the OS IP determined for each node, The IPMI IP should be 0.0.0.0 for all nodes in the cluster

**Note:** With Cohesity release 6.6 or later, all Cisco UCS servers do not require any IPMI configuration. Keep the IPMI IP as 0.0.0.0 and delete any pre-existing IPMI IP during cluster creation.

		COHESITY	
Cluster Setup			
Chassis WZP26510561		_	
Node	IP		IPMI IP
Node 1 - 161963887789 Host Name: chassis-wzp26510561-node-1	10.108.1.164		0.0.0.0
Chassis WZP2651056H			
Node	IP		IPMI IP
Node 1 - 161963887788 Host Name: chassis-wzp2651056h-node-1	10.108.1.165		0.0.0.0
Chassis WZP2651059D			
Node	IP	*	IPMI IP
Node 1 - 161963887786 Host Name: chassis-wzp2651059d-node-1	10.108.1.163		0.0.0.0

**Step 7.** Enter the Cluster Subnet, Gateway, DNS, NTP, Virtual IP and FQDN details and click Create Cluster.

Cluster Setup			
			2
	Select Nodes	Netv	vork Settings
Cluster Name *		Cluster Domain Name	
chx-c240-1		aa08.rtp4.local	
Cluster Subnet Gateway		Cluster Subnet Mask *	
10.108.1.254		255.255.255.0	
PMI Subnet Gateway		IPMI Subnet Mask	
PMI Username		IPMI Password	
			Show Password
Search Domains			
our Cluster domain is always included in	n the search domains list. Separate multiple values i	vith commas.	
DNS Servers *			
10.108.1.6 ×			
separate multiple IPs with commas, E.g.,	. 192.0.2.0, 198.51.100.0, 203.0.113.0		
Use Authentication Key			
72.20.10.18 × 172.20.1	0.15 ×		
arate multiple ntp servers with commas.	E.g., pool.ntp.org. 198. 1.100.0, 203.0.113.0		
DN* x-c240-1 aa08 rtp4 local			
<sub>DN*</sub> x-c240-1.aa08.rtp4.local	)		
ov. x-c240-1.aa08.rtp4.local			
P Address or Range	Count (Optional)	2	
PS PAddress or Range 92.0.2.1	Count (Optional) 24	Add	
PS P2.0.2.1	Count (Optional)	Add	Delete
DN* x-c240-1.aa08.rtp4.local PS P Address or Range 92.0.2.1 0 108.1.167	Count (Optional) 24	<b>↓</b> Add	Delete
DN* x-c240-1.aa08.rtp4.local PS P Address or Range 92.0.2.1 108.1.167 108.1.168	Count (Optional) 24	Add	Delete T T
DN* x-c240-1.aa08.rtp4.local PS P Address or Range 92.0.2.1 108.1.167 108.1.168 108.1.169	Count (Optional) 24	Add	Delete T T T T T T T
DN* x-c240-1.aa08.rtp4.local PS P Address or Range 92.0.2.1 108.1.167 108.1.167 108.1.169 108.1.170	Count (Optional)	Add	Delete T T T T T T T T T T T T T
DN* x-c240-1.aa08.rtp4.local PS PAddress or Range 92.0.2.1 108.1.167 108.1.168 108.1.169 108.1.170 Storage Domain Encryptin 149.2 validated cryptography ciphers ar	Count (Optional) 24	Add	Delete Delete Delete Delete Delete Delete Delete Delete

Step 8. When the cluster is created, login with FQDN and register the cluster to Cohesity Helios.Step 9. Confirm the 4x Cisco UCS C240 nodes are configured for the new Cohesity cluster.

		Q Search							chx-c240-1	(€ © H	ф г
Dashboards		Cluster									
O Data Protection	>	Summary	Storage Domains	Nodes Key Mana	igement System Syst	og					
A Infrastructure	>	Com	k a Nada Status	- 0							
SmartFiles	>	Chussi	Noue status							Disk	
Security Tools	>	Slot	ID	Host Name	Node Serial	Node Status	Capacity	Ib	Version	Status Data Disk	ł
🖏 Test & Dev		1	Chassis: WZP265105 161963887787 UCS-C240M6H12	5Z chx-c240-1-wzp26 5z-node-1	5105 WZP2651055Z	Active	174.4 TiB	10.108.1.166	6.8.2_u1_release-2024 0509_a5da4644	16 HDDs	:
Marketplace	>										
System	>		Chassis: WZP265105	.61						1.24	
Reporting		1	UCS-C240M6H12	61-node-1	WZP26510561	C Active	174.4 TiB	10.108.1.165	6.8.2_01_release-2024 0509_a5da4644	16 HDDs	:
🛱 Settings	~	-	Chassis: WZP265105	6H							
Summary		1	161963887788 UCS-C240M6H12	chx-c240-1-wzp26 6h-node-1	5105 WZP2651056H	C Active	174.4 TiB	10.108.1.164	6.8.2_u1_release-2024 0509_a5da4644	16 HDDs	:
Access Manageme	nt	-	Chassis: WZP265105	9D							
Networking		1	161963887786 UCS-C240M6H12	chx-c240-1-wzp26 9d-node-1	5105 WZP2651059D	Active	174.4 TiB	10.108.1.163	6.8.2_u1_release-2024 0509 a5da4644	16 HDDs	1

# **Cluster Expansion and Firmware Upgrades**

This chapter contains the following:

- <u>Cohesity Cluster Expansion</u>
- <u>Upgrade Firmware and Software</u>

# **Cohesity Cluster Expansion**

This section details the process to expand the existing cluster deployed on Cisco UCS C-Series nodes. You can add a new Cisco UCS C-Series node in the existing Cisco Fabric Interconnect, derive a Server Profile from existing Template, install the Cohesity OS from Cisco Intersight, and expand the cluster in Cohesity Helios.

The new Cisco UCS C-Series node has to be cabled to the existing Cisco Fabric Interconnect requiring minimal effort to expand both compute and storage.

**Note:** Before adding a node to existing Cohesity cluster , please check with Cohesity support for compatibility of new node with the nodes configured in existing cluster.

## **Procedure 1.** Derive and Deploy Server Profile to New Node

Note: Skip this step if you already have a Cisco Intersight account.

**Step 1.** Go to <u>https://intersight.com/</u>, click Infrastructure Service and click Server. Identify the new Cisco UCS C-Series node provisioned for the existing Cohesity cluster expansion.

**Note:** The node would be auto discovered, if the C-Series node is connected to the configured server port of Fabric Interconnect.

**Note:** The following screenshot demonstrates a Cohesity certified C-Series node which is discovered on Intersight and not assigned to any Server Profile.



Step 2. Click "... ", select Profile and Derive Profile from the template.

≡	cisco Intersight	🎗 Infrastructure Service 🗸	Q Search C O A	0 Q 💷 💷 🕘 🛛 A
:@:	Overview	Servers		
0	Operate ^ Servers	* All Servers ⊕ +     ⊘ Q. Search     ▼ Filters 4 results	(Hulle-Facers) Flowing Viola	C Export
	Chassis Fabric Interconnects	Critical 1     Or 01     On 3	4241063) 4 No 4 4.3(4.241063) 4	
	HyperFlex Clusters	Name : Health : Model : Server	Profile : UCS Domain : Bundle Ver : AA09-FI-DP-64 4.3(4.241063)	Serial : ∳ WZP2651059D
Ø	Analyze ^ Explorer New	O         AA09-FI-DP-6454-2         O         Healthy         UCSC-C240-M         Coh-Si           O         AA09-FI-DP-6454-3         O         Healthy         UCSC-C240-M         Coh-Si           O         AA09-FI-DP-6454-3         O         Healthy         UCSC-C240-M         Coh-Si           O         AA09-FI-DP-6454-4         O         O         Coh-Si	rverTemplate_DERIVED-2         AA09-FI-DP-64         4.3(4.241063)           rverTemplate_DERIVED-3         AA09-FI-DP-64         4.3(4.241063)           rverTemplate_DERIVED-4         AA09-FI-DP-64         Derive from Temp	W Power >
,c	Configure ^	0	Rows per j	page VMware > Install Operating System
	Templates Policies Pools			Upgrade Firmware Launch vKVM Launch Tunneled vKVM Start Alarm Suppression Open TAC Case Set License Tier
Nev	Command Palette			Collect Tech Support Bundle

**Step 3.** Select the Server Profile template created to deploy the Cisco UCS C-Series node for the Cohesity cluster and click Next.

Servers   Operate   Servers   Chaskis   Chaskis   Chaskis   Servers   Operate   Details   Operate   Details   Operate   Details   Operate   Operate   Operate   Details   Operate   Operate   Operate   Details   Operate	≡	diale Intersight	🍰 Infrastructure Service 🗸				Q Search	C	⊗ ≰11		ଡ
<ul> <li>Consult</li> <li>Consult</li> <li>Consult</li> <li>Consult</li> <li>Consult</li> <li>Consult</li> <li>Consult</li> <li>Consult</li> <li>Summary</li> </ul> Template <ul> <li>Configure</li> <li>Nor</li> <li>Configure</li> <li>Potices</li> <li>Pot</li></ul>	:@:	Overview	Servers								
Chasas     A subject interconnects     HyperFlex Clusters   Integrated Systems     Configure   Porfiles   Profiles   Policies   Policies   Policies        Policies        New Command Palette *        ConserverTemplate     ConserverTemplate     New Command Palette *        ConserverTemplate     New Command Palette *	0	Operate ^ Servers	General     Template     G     Details	Template Select the Templ	late that need to be UCS Server Profi	assigned to profile.					
Fabric Interconnects   HyperFlex Clusters   Integrated Systems   Analyze   Analyze   Explorer   Now   Configure   Profiles   Policies   Policies   Policies   Policies   Policies		Chassis	(4) Summary		Q Search		Filters 1 results				
Hyperflex Clusters   Integrated Systems   Analyze   Analyze   Explorer   New   Configure   Profiles   Policies   Policies   Policies   Policies   Policies   Policies   Policies		Fabric Interconnects		(	Name	:	Description	Last U	pdate	i	
Integrated Systems   Analyze   Analyze   Explorer   New   Profiles   Policies   Policies   Policies   Policies   Policies   New   Command Palette *		HyperFlex Clusters		l	O Coh-Serve	erTemplate		2 minu	tes ago		
Analyze   Explorer   New   Pofiles   Policies   Policies   Policies		Integrated Systems			Selected 1 of 1	Show Selected	Unselect All	Rows per page	10 ×	< 1 >	
Explorer New Configure  Profiles Policies Pools  New Command Palette * Close Close	Q	Analyze ^									
Configure   Profiles   Templates   Policies   Policies   Policies		Explorer New									
Profiles  Policies Pools  New Command Palette *  Close	,0	Configure ^									
Tempiates       Policies       Poois		Profiles									
Policies Pools New Command Palette * Close Close Reach IN	1	Templates									
Pools New Command Palette * Close Back		Policies									
New Command Palette * Close Back		Pools									
	Nev	w Command Palette ×		< Close						Ва	ck Next

Step 4. Rename the Derive profile and click Next.

eisco Intersight 🐉 Infrastructure Service 🗸	Q Search C (	୬ ⊄11 0,002 41 0
© Overview		
<ul> <li>Operate</li> <li>Servers</li> <li>Chassis</li> <li>Chassis</li> <li>Template</li> <li>Details</li> <li>Details</li> <li>Summary</li> <li>Fabric Interconnects</li> <li>HyperFlex Clusters</li> <li>Integrated Systems</li> <li>Analyze</li> <li>Explorer New</li> </ul>	Details Edit the description, tags, and auto-generated names of the profiles. Ceneral Organization* default Target Platform ① UCS Server (Pl-Attached) Description Description 0 / 1024 Set Tags Enter a tag in the key/value format.	
Configure  Profiles Templates Policies Poois	1 Name*     Organization*       Coh-ServerTemplate_DERIVED-5     Image: Cohe ServerTemplate_DERiveD-5	Assigned Server AA09-FI-DP-8454-1

**Step 5.** Verify the policies and click Derive. As we are using the original Server Template to derive Server Profile, the policies would be exactly the same. To ensure consistency and avoid misconfigurations, it is recommended to use the same Server Template as that of original cluster.

$\equiv \frac{-1 1+1 1+}{c_{15}c_{0}}$ Intersight	$^{\circ}$ Infrastructure Service $$			Q Search	C ⊘ ⊄0	Q 🐽 🚺 💿 🛛
Overview	Servers					
Operate            Servers            Chassis            Fabric Interconnects            HyperFlex Clusters            Integrated Systems	General     Template     Details     Summary	Summary Summary of the profiles that n General Name Coh-ServerTemplate Target Platform UCS Server (FI-Attached) UCS Server Profiles Name	need to be derived from the profile ter	mptate. Organization defauit rver	Organization	© 1
		Coh-ServerTemplate_DER	NVED-5 AA09-FI-DP-	-6454-1	default	
🛇 Analyze 🗠		Compute Configuration	Management Configuration	Storage Configuration	Network Configuration	Errors/Warnings (0)
Explorer New		BIOS				Coh-BIOS 🗐
🖋 Configure 🔿		Boot Order				Coh-BootOrder
Profiles						Coh-UUID 🗶
Templates		Virtual Media				virtualMedia1
Policies Pools	1					
New Command Palette ×	*	< Close				Back Derive
New Command Palette ×	↓ ↓ Infrastructure Service ∨	< Close	C	) Search	ି ୯ ୦ ସ 🛙	Back         Derive           Q         Q2         (A1)         (P)         (A)
New Command Palette * entering intersight @ Overview	Infrastructure Service V Servers	< Close	C	) Search	ି ୦ ବା	Back Derive
New Command Palette *	Infrastructure Service      Servers     General	< Close Close Summary Summary of the orofiles that or	C sed to be derived from the profile tem	) Search	C © 41	Back         Darive           Q         Q         A1         O         Q
New Command Palette *	Servers Ceneral Template	< Close  Summary Summary of the profiles that ne  General	ced to be derived from the profile tem	), Search splate.	0 9 9	Back         Derive           Q         02         0         Q
New Command Palette *	<ul> <li>Infrastructure Service </li> <li>Servers</li> <li>General</li> <li>Template</li> <li>Details</li> </ul>	< Close Summary Summary of the profiles that ne A General Name	C eed to be derived from the profile tem	), Search plate. Organization		Back Derive
New Command Palette × curco Intersight Coverview Overview Operate Servers Chassis	<ul> <li>Marfrastructure Service ~</li> <li>Servers</li> <li>General</li> <li>Template</li> <li>Details</li> <li>Summary</li> </ul>	< Close Summary Summary of the profiles that nd A General Name Coh-ServerCemplate Targat Platform	C eed to be derived from the profile term	2 Search Iplate. Organization default		Back Derive
New Command Palette *	<ul> <li>Mrfrastructure Service </li> <li>Servers</li> <li>General</li> <li>Template</li> <li>Details</li> <li>Summary</li> </ul>	< Close Summary Summary of the profiles that ne General Name Con-ServerTemplate Target Platform UCS Server (Pl-Attached)	eed to be derived from the profile tem	) Gearch splate. Organization default		Back Derive
New Command Palette	<ul> <li>Infrastructure Service </li> <li>Servers</li> <li>General</li> <li>Template</li> <li>Details</li> <li>Summary</li> </ul>	< Close  Summary Summary of the profiles that ne  General Name Coh-ServerTemplate Target Platform UCS Server (FF-Attached) UCS Server Profiles	eed to be derived from the profile tem	) Search splate. Organization default	0 4 3	Back Derive
New Command Palette	<ul> <li>Infrastructure Service </li> <li>Servers</li> <li>General</li> <li>Template</li> <li>Details</li> <li>Summary</li> </ul>	< Close Summary Summary of the profiles that ne General Name Coh-ServerTemplate Target Platform UCS Server (Pf-Attached) UCS Server Profiles Name Coh-SenartTemplate DEEE	eed to be derived from the profile term	) Search splate. Organization default:	C O 4 3	Back Derive
New Command Palette *  Chassis Fabric Interconnects HyperFlex Clusters Integrated Systems  (), Analyze ^	<ul> <li>Infrastructure Service </li> <li>Servers</li> <li>General</li> <li>Template</li> <li>Details</li> <li>Summary</li> </ul>	< Close Summary Summary of the profiles that nd Coh-ServerTemplate Target Platform UCS Server (FF-Attached) UCS Server Profiles Name Coh-ServerTemplate.DERI Compute Configuration	eed to be derived from the profile term  Assigned Serr  VED-5 AAD9-FI-DP-6  Management Configuration	2 Search Iplate. Organization default Ver Ver Storage Configuration	C O C I C	Back Derive
New Command Palette *	<ul> <li>Infrastructure Service </li> <li>Servers</li> <li>General</li> <li>Template</li> <li>Details</li> <li>Summary</li> </ul>	< Close Summary Summary of the profiles that nd General Name Coh-ServerTemplate UCS Server (Fir-Attached) UCS Server (Fir-Attached) UCS Server Profiles Name Coh-ServerTemplate_DERR Compute Configuration UCC Access	eed to be derived from the profile term Assigned Ser VED-5 AA09-FI-DP-0 Management Configuration	2 Search Iplate. Organization default Ver Ver Storage Configuration	C O C I C C C C C C C C C C C C C C C C	Back Derive
New Command Palette	<ul> <li>Infrastructure Service </li> <li>Servers</li> <li>General</li> <li>Template</li> <li>Details</li> <li>Summary</li> </ul>	< Close  Summary Summary of the profiles that nd General Name UCS Server(Fri-Attached) UCS Serve	eed to be derived from the profile term Assigned Ser VED-5 AA09-FI-DP-6 Management Configuration	Storage Configuration	C O C I C	Back Derive
New Command Palette	<ul> <li>Infrastructure Service </li> <li>Servers</li> <li>General</li> <li>Template</li> <li>Details</li> <li>Summary</li> </ul>	<ul> <li>Close</li> <li>Summary</li> <li>Summary of the profiles that network</li> <li>General</li> <li>Name</li> <li>Coh-ServerTemplate</li> <li>Target Platform</li> <li>UCS Server Profiles</li> <li>Name</li> <li>Coh-ServerTemplate_DERI</li> <li>Compute Configuration</li> <li>IMC Access</li> <li>IPMI Over LAN</li> <li>Local User</li> </ul>	eed to be derived from the profile term Assigned Serr VED-5 AA09-FI-DP-0 Management Configuration	Search  plate.  Organization default  ver  id54-1  Storage Configuration	C O 4 D	Back     Derive       Q     Q     A     Q     Q       Image: Second state of the
New Command Palette	<ul> <li>Infrastructure Service </li> <li>Servers</li> <li>General</li> <li>Template</li> <li>Details</li> <li>Summary</li> </ul>	<ul> <li>Close</li> <li>Summary</li> <li>Summary of the profiles that net conserverTemplate</li> <li>Con-ServerTemplate</li> <li>Target Platform</li> <li>UCS Server Profiles</li> <li>Name</li> <li>Coh-ServerTemplate.DEBI</li> <li>Compute Configuration</li> <li>IMC Access</li> <li>IPMI Over LAN</li> <li>Local User</li> <li>Serial Over LAN</li> </ul>	eed to be derived from the profile term Assigned Ser VED-5 AA9-FI-DP-0 Management Configuration	Search      splate.      Organization     default  ver  ids4-1  Storage Configuration	C O <table-cell> T</table-cell>	Back Derive
New Command Palette	<ul> <li>Infrastructure Service </li> <li>Servers</li> <li>General</li> <li>Template</li> <li>Details</li> <li>Summary</li> </ul>	< Close  Summary Summary Summary of the profiles that ne  Goh-ServerTemplate Target Platform UCS Server(Fri-Attached) UCS Server(Fri-Attached) UCS Server(Fri-Attached) UCS ServerTemplateDERI Compute Configuration IMC Access IPMI Over LAN Local User Serial Over LAN Syslog	eed to be derived from the profile term Assigned Ser VED-5 AA9-FI-DP-0 Management Configuration	Search      splate.      Organization     default:      ver      ids4-1      Storage Configuration	C O <table-cell> T</table-cell>	Eack Derive
New Command Palette	<ul> <li>Infrastructure Service </li> <li>Servers</li> <li>General</li> <li>Template</li> <li>Details</li> <li>Summary</li> </ul>	< Close  Summary Summary Summary of the profiles that ne  Goh-ServerTemplate Target Platform UCS Server (Fri-Attached) UCS	eed to be derived from the profile term Assigned Ser VED-5 AA9-FI-DP-0 Management Configuration	Search      splate.      Organization     default:      ver      storage Configuration	C O <table-cell> T</table-cell>	Eack Derive
=	uluulu Intersight	Infrastructure Service 🗸		Q Search	C 0 4	
-------------	--	---	--	---	-----------------------	---
.0	Overview	Servers				
0	Operate ^ Servers Chassis Fabric Interconnects HyporFlex Clusters Integrated Systems	<ul> <li>General</li> <li>Template</li> <li>Detalis</li> <li>Summary</li> </ul>	Summary Summary of the profiles that need to be derived from the p      General      Name     Coh-ServerTemplate     Target Platform     UCS Server (FF.Attached)     UCS Server Profiles      Mane     Assa      Coh-ServerTemplate DERIVED_5	rofile template. Organization default gned Server	Organization	@ *
© ,• 	Analyze Analyz		Compute Configuration Management Configu	ation Storage Configuration	Network Configuration	Errors/Warnings (0)
A New	Command Palette	<	Close			Back Derive
_						
=	iliniti Intersight 💦 🕯 🕯	nfrastructure Service 🗸		Q Search	0 0 ⊄1	ር 💶 💶 🌀 🛛 ደ
*	overview	nfrastructure Service V		Q Search	C © 41	ር 🐽 🖬 🎯 🛛 ጽ
*	Overview Operate Chassis Fabric Interconnects HyperFlex Clusters	nfrastructure Service V Servers Ceneral Template Details Summary	Summary Summary of the profiles that need to be derived from the pr General Name Coh-ServerTemplate Target Platform UCS Server (FI-Attached) UCS Server Profiles	Q Search ofile template: Organization default	୯୦ ୟା	Q 2 A3 0 A
	Coverview Operate Servers Chassis Fabric Interconnects HyperFiex Clusters Integrated Systems	nfrastructure Service V Servers General Template Details Summary	Summary Summary of the profiles that need to be derived from the pr General Name Coh-ServerTemplate Target Platform UCS Server (FI-Attached) UCS Server Profiles Name Assig	Q Search offle template. Organization default	C O C 0	Q 2 1 0 X
* © 	Overview     Image: Constraint of the second s	nfrastructure Service V Servers © General © Template © Details 3 Summary	Summary Summary of the profiles that need to be derived from the pr General Name Coh-ServerTemplate Target Platform UCS Server (FI-Attached) UCS Server Profiles Mame Assig Coh-ServerTemplate_DERIVED-5 AA09 Compute Configuration Management Configurat LAN Connectivity	Q Search ofile template. Organization default ned Server -FP-DP-6454-1 tion Storage Configuration (	C O C I	Q     Q     A     Q     Q       Errors/Warnings (0)

**Step 6.** When the Sever Profile is derived, go to the Servers tab, identify the Profile displayed as "Not Deployed," click the "..." and select Deploy.

≡ diada Intersight 3	8 Infrastructure Service ∨			Q Search	C O	\$1 D (	12 🕰 🌒 🖇
) Overview	Profiles     HyperFlex Cluster Profiles UCS Chase	sis Profiles UCS Domair	Profiles UCS Server Pro	ofiles			
0 Operate ^ Servers	* All UCS Server Profil 🛞 +					Cre	ate UCS Server Profile
Chassis Fabric Interconnects HyperFlex Clusters	Image: Status     Image: Colored status       Image: Colored status     Image: Colored status       Image: Colored status     Image: Colored status       Image: Colored status     Image: Colored status	Target Platform FF-Attached 4	4 results				🛆 Export
Analyze     Analyze     Analyze     Analyze	Not Deployed 1  Name  Coh-ServerTemplate_DERIVED-5	Status :	Target Platform : UCS Server (FI-Attached)	UCS Server Template	Server AA09-FI-DP-6454-1	Last Updat	e : 🤣 nds ago 🗰
Configure	Coh-ServerTemplate_DERIVED-4 Coh-ServerTemplate_DERIVED-2 Coh-ServerTemplate_DERIVED-2	© ок © ок	UCS Server (FI-Attached) UCS Server (FI-Attached)	Coh-ServerTemplate Coh-ServerTemplate	AA09-FI-DP-6454-4 AA09-FI-DP-6454-2	2 hours age 2 hours age	Deploy Activate
Templates			oca server an PAttacheu)	our-server template	Row	s per page 25	Clone Edit
Pools							Delete Set User Label Detach from Template Server Actions

**Step 7.** On the Deploy Profile confirmation screen, enable Reboot Immediately to Activate and click Deploy.

Deploy UCS Server Profile							
UCS Server profile "Coh-ServerTemplate_DERIVED-5" will be deployed to server "AA09-FI-DP- 6454-1".							
If policy configuration requires an immediate reboot and the option below is disabled, then profile deployment will not be initiated.							
<ul> <li>More Details</li> <li>Reboot Immediately to Activate</li> </ul>							
Cancel Deploy							

**Step 8.** Once the server profile is deployed, ensure the firmware is same or higher than the firmware deployed on existing nodes. Please update the firmware to recommended firmware release.

≡ "listo" Intersight 🦂 אייניים	nfrastructure Service 🗸		Q Search	C 0 40 0	02 🖾 🕐 🔎
Overview	← Servers AA09-FI-DP-6454-1 ② Healt	hy			Actions ~
Operate ^	General Inventory UCS Server Profi	ile HCL Topology Metrics Connecti	vity		
Servers	Details	Properties		Events	
Chassis		Cisco UCSC-C240-M6L	Front Re	ar Top – Alarms	No Alarms
Fabric Interconnects	Asset Tag			Active Acknowle	dged Suppressed
HyperFlex Clusters	License Tier			i I.	() Alarms
Integrated Systems	Management Mode			+ Requests	QA
	Intersight Server Perconality	Power () On Locator LED () Off	Hea	alth Overlay + Advisories	No Advisories
Z Analyze	-	CPUs	CPU Capacity (GHz)		
	Chassis	2 Threads	92.8 ID		
Configure ^		64	1		
Profiles	Profile	CPU Cores	Adapters		
Templates	Profile Status	CPU Cores Enabled	UUD		
Policies	O OK	32	01010101-0100-1110-0101-01010101	1111	
Pools	Bundle Version 4.3(4.241063)	Memory Capacity (GiB) 128.0			
New Command Palette	Firmware Version 4.3(4.241063)				
	Firmware Status				

**Step 9.** Install the OS using Cisco Intersight or through vMedia, provided in section <u>Install Cohesity on Cisco</u> <u>UCS C-Series Nodes</u> The screenshot below displays on the OS deployed on the new Cisco UCS C-Series node.

AA08-XSeries-2-4 (AA08-XSeries-Manual_DERIVED-4)   KVM Console
Cohesity Version: 6.6.0d_u6_release-20221204_c03629f0 Product Name: UCS-X210CM6SN15 Hostname: chassis-fch243974v3-node-1 Node IPv4: Node IPv6: Link Local IPv4: 169.254.7.207 Link Local IPv6: fe00::00c7:3dff:fe2c:774c
FUR LUCAL ACCESS, PLEASE CONNECT TO THE SAME SWITCH AS THE NUDE AND USE THE LINK LOCAL IP ADDRESS. ENTER THE IP IN YOUR BROWSER TO ACCESS THE COHESITY UI.
chassis-fch243974v3-node-1 login: [   702.262046] kvm [53233]: vcpu0 disabled perfctr wrmsr: 0xc2 data 0xffff
Cohesity Version: 6.6.0d_u6_release-20221204_c03629f0 Product Name: UCS-X210CM6SN15 Hostname: chassis-fch243974v3-node-1 Node IPv4: Node IPv6: Link Local IPv4: 169.254.7.207 Link Local IPv6: fe80::80c7:3dff:fe2c:774c
FOR LOCAL ACCESS, PLEASE CONNECT TO THE SAME SWITCH AS THE NODE AND USE THE LINK LOCAL IP ADDRESS. ENTER THE IP IN YOUR BROWSER TO ACCESS THE COHESITY UI.
Hint: Num Lock on
chassis-fch243974v3-node-1 login: _

#### **Procedure 2.** Expand existing Cluster through Cohesity Helios

When the new Cisco UCS C-Series node is configured with the Cohesity OS, the Cohesity Cluster is expanded to add the Cisco UCS C-Series node. This process expands both compute and storage on the Cohesity Cluster.

**Step 1.** Access the Cohesity Cluster dashboard. Go to Summary > Nodes and click the + sign and select Add Node.

< 1/3 > 🛕 En	able Multi-Factor Authentication to improve system s	ecurity Manage Setting	a				
	Q Search					chx-c240-1 🐧	୭ H <sup>®</sup> ໍ ≏ ≗
Dashboards	Cluster						
Data Protection >	Summary Storage Domains Hardware	Key Management System	Syslog				
A Infrastructure >	Chassis • Node Status • Q						Configure Rack
SmartFiles	Chasas Hode Status						Add Node
🖏 Test & Dev	Slot Node ID	Node Status	Node Serial	IP Address	Disks	Disk Status	Activate Disks
Marketplace	<ul> <li>Chassis: WZP2651055Z</li> <li>161963887787</li> <li>UCS-C240M6H12 + chx+c240-1-wzp26510552-m ode-1</li> </ul>	Active	WZP2651055Z	10.108.1.166	2 SSDs 16 HDDs	<b>P</b>	
H Reports	Chassis: WZP26510561						
🕸 Settings 🗸 🗸	161963887789 UCS-C240M6H12 + chx-c240-1-wzp26510561-n ode-1	Active	WZP26510561	10.108.1.165	2 SSDs 16 HDDs	6	
Summary Access Management	Chassis: WZP2651056H						
Account Security	1 161963887788 UCS-C240M6H12 + chx-c240-1-wzp2651056h-r ode-1	Active	WZP2651056H	10.108.1.164	2 SSDs 16 HDDs	2	

**Step 2.** The Cohesity cluster automatically identifies the new node. Confirm the serial number of the node, which was configured for the cluster expansion, select the node, and click Next.

≕ COHESITY		Q Search		chx-c240-1 🔇 🕐 🕂 🎗 올
Dashboards		Add Node		
Ø Data Protection	>	0	2	3
A Infrastructure	>	Select Node(s)	Network Settings	Assign VIPs
SmartFiles	>	The following Nodes were detected.		Select All
🍳 Test & Dev		Chassis WZP2651059D		
Marketplace	>	_		
System	>	Node 1 - 101903887786 Hots: Name: chasis: wwzp2651059d-node-1 Product Model: UCS-C240M6H12		
Reports				
83 Settings	>	2U4N Node slots are displayed according to a rear view of the Chassis.		

- Step 3. Add the available Node IP and click Next.
- **Step 4.** Add the Virtual IP as configured on DNS and click Finish.

≍ COHESITY		Q Search		chx-c240-1 🐧
Dashboards		Add Node		
Data Protection	>	0	2	3
A Infrastructure	>	Select Node(s)	Network Settings	Assign VIPs
SmartFiles	>	Assian VIPs		
💐 Test & Dev		VIPs		
Marketplace	>	VIP Address or Range 192.0.2.1	Count (Optional) 24	
System	>			
H Reports		Add		
🐯 Settings	>	VIP	Delete	
		10.108.1.171		
		Finish Back Cancel		

**Step 5.** The Cohesity Cluster is expanded from three to four nodes of Cisco UCS C-Series servers. It takes some time to assimilate the drives of the new Cisco UCS C-Series node to the existing Cohesity Cluster.

COHES	ITY	C	<b>Q</b> Search							chx-xseries1	S	ØН	ò	8
Dashboar	rds	C	luster											
😡 Data Prot	tection >	s	Summary	Storage Domains	Nodes Key Manag	gement System	Syslog							-
🚠 Infrastru	cture >			L L										Ð
🕒 File Servi	ces >		Charole	Node Status	0									
🛞 Security 1	Tools >		Cristana	(Node Status +)	~									
🔍 Test & De	ev.										<b>D</b> 1-1-			
🖬 Marketpl	ace >		Slot	ID	Host Name	Node Serial	Node Status	Capacity	IP	Version	Statu	Data Dis	cs	
[]] System	>			Chassis: FCH243974YZ										
II. Reporting	9		1	161955005867	chx-xseries1-		🗳 Active	83.5 TIB	10.108.1.33	6.6.0d_u6_release-	2	6 SSDs		
😂 Settings	~			UCS-X210CM6SN15	tch243974yz-node-1					20221204_c03629f0				
Summary	у			Chassis: FCH243974Z3										
Access M Networki	lanagement ing		1	775946439168 UCS-X210CM6SN15	chx-xseries1- fch243974z3-node-1		🗳 Active	83.5 TIB	10.108.1.34	6.6.0d_u6_release- 20221204_c03629f0	ſ	6 SSDs		
SNMP			-	Chassis: FCH250671P5										
Upgrade License			1	161955005866 UCS-X210CM6SN15	chx-xseries1- fch250671p5-node-1	FCH250671P5	🗳 Active	83.5 TIB	10.108.1.32	6.6.0d_u6_release- 20221204_c03629f0	P	6 SSDs		
			-	Chassis: FCH243974V3										
			1	161955005868 UCS-X210CM6SN15	chx-xseries1- fch243974v3-node-1		🖆 Active	0 Bytes	10.108.1.35	6.6.0d_u6_release- 20221204_c03629f0	K <sup>o</sup>	0 HDDs		
														-

## **Upgrade Firmware and Software**

**Note:** With the Intersight SaaS Management platform, the server firmware upgrade does not require you to download any firmware bundles to a local repository. When the suggested firmware upgrade request is issued, it automatically downloads the selected firmware and starts the upgrade process.

For detailed instructions to perform firmware upgrades, see Firmware Management in Intersight

Firmware for Cisco UCS C-Series with the Cohesity can be upgraded for the following main use cases:

• Upgrade Cisco UCS C-Series node firmware in combination with software upgrades for the Cohesity Data Cloud. Cohesity non-distributive upgrades manage the sequential server reboot, allowing upgrades of Cisco UCS C-Series node firmware during a Cohesity software upgrade. Because each node is upgrading sequentially, the Cohesity Cluster upgrade time increases by about 25 to 30 minutes per Cohesity node.

• Upgrade Cisco UCS C-Series node independent of the Cohesity Data Cloud software upgrades. In this process, you need to manually reboot the Cisco UCS C-Series node and verify that the Cohesity node is back online after the server firmware upgrade. Verify that each node is rebooted serially, and that the first node comes back online and joins the Cohesity cluster before initiating a reboot on the second node. This process can also be done in parallel across all Cisco UCS C-Series nodes but requires maintenance window for Cohesity Cluster downtime.

**Note:** Prior to upgrading Cisco UCS C-Series node firmware, you are required to upgrade the Cisco Fabric Interconnect.

To successfully upgrade the Cisco UCS Fabric Interconnect and IO module firmware, see: <a href="https://intersight.com/help/saas/resources/Upgrading Fabric Interconnect Firmware imm#procedure">https://intersight.com/help/saas/resources/Upgrading Fabric Interconnect Firmware imm#procedure</a>

**Note:** During the upgrade of the Intersight Managed Fabric Interconnect, the fabric interconnect traffic evacuation is enabled by default. The fabric interconnect traffic evacuation evacuates all traffic that flows through the fabric interconnect from all servers attached to it, and the traffic will fail over to the peer fabric interconnect for fail over vNICs with no disruptions in the network.

#### **Upgrade Fabric Interconnect**

#### Procedure 1. Upgrade Cisco UCS Fabric Interconnect and Cisco UCSX 9108 IFM Firmware

This procedure expands on the high-level procedure to upgrade firmware of the Cisco UCS Fabric Interconnect in Intersight Managed Mode (IMM). For more details, go to:

https://intersight.com/help/saas/resources/Upgrading Fabric Interconnect Firmware imm#before you begin

**Step 1.** Login to <u>https://Intersight.com</u>, click Infrastructure Service, then click Fabric Interconnects, and select the Fabric Interconnect Pair (IMM). Click "..." and select Upgrade Firmware.

	Intersight	📲 Infrastructure Service 🗸			Q Sea	rch C	ତ <b>ୟ</b> ା ପ୍	2 💶 💿 🛛 A
)) Overv	iew	Fabric Interconnect	s					
Opera	te ^	* All Fabric Interconne  +		Filters 2 results				Export
Chass	is	Health	Connection	Contract Status Not Covered 2	Bundle Version	NX-OS Version	Models	ж
Hyper	Flex Clusters	Name	: Health	: Model	: Bundle Version	: UCS Domain Profil	e Total Used	ts Availa
🕘 Analy	ze ^	AA09-FI-DP-6454 FI-A     AA09-FI-DP-6454 FI-B     Selected 2 of 2	Healthy     Healthy     Healthy	UCS-FI-6454 UCS-FI-6454	4 4.3(4.240066) 4 4.3(4.240066)	Coh-DomainProfile	e 54 18 Turn On Locator Upgrade Firmware	36
Exploi	gure ^						Reboot Derive Profile from Create Traffic Mirro	Mode Template
Temp	ates 25						Open TAC Case Set User Label	ang (3PAN) Session
Pools		1					Collect Tech Suppo	rt bundle

Step 2. Click Start and from Upgrade firmware make sure the UCS Domain Profile is selected and click Next.

= "listo" Intersight 🎝	🖁 Infrastructure Service 🗸	Q. Search	C 🛛 🕫 C 🖉 C 🖉
. Overview	<ul> <li>← Fabric Interconnects</li> <li>Upgrade Firmware</li> </ul>		
Operate     Servers     Chassis     Fabric Interconnects	General     Version     Summary	General         Ensure selected Fabric Interconnects meet requirements for firmware upgrade.         Single Fabric Interconnect Upgrade •         Q Search         V Filters 1 results         Domain N Fabric Interconnect A	Fabric Interconnect B
HyperFlex Clusters Integrated Systems O Analyze ^		AA09-FI-DP-6 UCS-FI-6454 FD0260419XX 4.3(4.240066) UCS-FI Selected 1 of 1 Show Selected Unselect All	Settial     Building version       1-6454     FD0260419ZA     4.3(4.240066)       Rows per page     10 ~
Explorer New Configure ^ Profiles Templates			
Policies Pools			
New Command Palette	• <	Cancel	Back

**Step 3.** Select the recommended Firmware release. By default, the upgrade enables the Fabric Interconnect traffic evacuation. Use Advanced Mode to exclude the Fabric Interconnect traffic evacuation.

**Note:** In the existing document, we are upgrading to a Firmware version which is not a recommended version. This is just to demonstrate the process of Firmware upgrades. You should make sure to be on the recommended version of Cisco UCS Firmware.

≡ duala Intersig	ht 💦 🖧 Infrastructure Service 🗸	Q Search C O 41 0 Q 02 A1 0
. Overview	<ul> <li>← Fabric Interconnects</li> <li>Upgrade Firmware</li> </ul>	
Operate	General General Version	Version Select a firmware version to upgrade the Fabric Interconnects to.
Chassis	3 Summary	In the selected firmware bundle will be downloaded from intersight.com. By default, the upgrade enables Fabric Interconnect traffic evacuation. Use Advanced Mode to exclude Fabric Interconnect traffic evacuation.
Fabric Interconn	ects	Advanced Mode
HyperFlex Cluste	ers	Q. Search Filters 36 results
Integrated Syste	ms	Version : Size : Release Date : Description : ③
🕘 Analyze	A.	
Explorer	New	O 4.3(4.240066) 👌 1.84 GiB Jun 4, 2024 11:03 Cisco Intersight Infrastructure Bundle 👳
🖉 Configure	^	4.3(3.240007)         1.72 GiB         Feb 15, 2024 10:21         Cisco Intersight Infrastructure Bundle         Image: Cisco Intersight Infrastructure Bundl
Profiles		O 4.3(2.230129) 1.70 GIB Nov 15, 2023 11:52 Cisco Intersight Infrastructure Bundle @
Templates		4.3(2.230117)         1.70 G/B         Aug 15, 2023 11:55         Cisco Intersight Infrastructure Bundle         Image: Cisco Intersight Infrastructure Bundle           4.7(3)         1.73 G/B         Oct 1. 2024 10:52         Cisco Intersight Infrastructure Bundle         Image:
Policies		0         4.2(3k)         1.72 GIB         Jun 17, 2024 4:23         Cisco Intersight Infrastructure Bundle         Image: Cisco Intersight Infrast
Pools		O 4.2(3)) 1.72 GIB Feb 22, 2024 10:11 Cisco Intersight Infrastructure Bundle @
		Selected 1 of 38 Show Selected Unselect All Rows ner name 10 V (1) 2 4 >
New Command Palett	te × , •	Cancel Back Next

Step 4. On the Summary page, confirm the firmware to be upgraded and click Upgrade.

= "livelin Intersight 4	) Infrastructure Service V	Q. Search C 🔗 📢 1 🗘 🐠 🗛 🚺	@ A
Overview	Fabric Interconnects     Upgrade Firmware		
0 Operate ^ Servers Chassis	<ul> <li>General</li> <li>Version</li> <li>Summary</li> </ul>	Summary Confirm configuration and initiate the upgrade.  Selected firmware bundle will be downloaded to the Fabric Interconnects and upgraded. Click on Requests to monitor the progress of the firmware upgrade.	
Fabric Interconnects HyperFlex Clusters Integrated Systems		Firmware       Version     Size       4.3(4.240074) @     1.85 GiB       Fabric Interconnects to be Upgraded     1.85 GiB	
<ul> <li>Analyze ^</li> <li>Explorer New</li> </ul>		Q. Search     ▼ Filters     1 results       Domain N :     Fabric Interconnect A     Fabric Interconnect B       Bundle Version     Model     Serial       Bundle Version     Model     Serial       Bundle Version     Model     Serial       Bundle Version     Model     Serial	(port
Configure ^ Profiles		Rows per page 25 ~ < 1	) >
Policies Pools			
New Command Palette ×		Cancel Back	Upgrade

Step 5. Monitor the upgrade process and wait for it to complete.

**Step 6.** When the Firmware downloads, acknowledge the Fabric Interconnect B upgrade, and click Continue.

petails	Execution Flow	
Status	Progress ③ Wait for a user acknowledgement on Fabric Interconnect - B.	19%
ame pgrade Firmware	Ensure Fabric Interconnects meet requirements to continue upgrade. Please acknowledge to contil     B upgrade. Learn more at Help Center.	nue with Fabric Interconnect -
) 732771e696f6e3201a36844	Proceed	
arget Type	⊘ Evacuate data traffic on Fabric Interconnect - B.	Nov 11, 2024 1:37 PM
bric Interconnect	Wait for image download to complete in endpoint. Image ucs-intersight-infra-4gfi.4.3.4.240074.bin successfully cached in Fabric Interconnect(s).	Nov 11, 2024 1:37 PM
arget Name A09-FI-DP-6454 FI-A A09-FI-DP-6454 FI-B	Initiate image download to the endpoint. Download request for ucs-intersight-infra-4gfi.4.3.4.240074.bin submitted successfully.	Nov 11, 2024 1:29 PM
ource Type pgrade Firmware	<ul> <li>Validate the requirements for the endpoint.</li> <li>Validation of pre-upgrade space availability completed successfully.</li> </ul>	Nov 11, 2024 1:29 PM
ource Name A09-FI-DP-6454 FI-A,AA		
itiator ndhiman@cisco.com		
tart Time		

**Step 7.** When Fabric Interconnect -B is upgraded, acknowledge the alarms and Fabric Interconnect - A upgrade.

etails	Execution Flow	
atus	Progress	52
Action Required	Wait for a user acknowledgement on Fabric Interconnect - A.	
ame ograde Firmware	Before continuing the upgrade, ensure that it meets requirements. Review all new alarms to understand any potential issues. To continue with the Fabric Interconnect - A upgrade, select "Proceed". Learn more	d implications and address re at Help Center.
/32771e696f6e3201a36844	View Alarms Proceed	
rget Type bric Interconnect	<ul> <li>Wait for IO Path Connectivity on Fabric Interconnect - B</li> <li>IO paths are up.</li> </ul>	Nov 11, 2024 1:57 P
rget Name	Wait for image download to complete. Image ucs-intersight-infra-4gfi.4.3.4.240074.bin successfully cached in Fabric Interconnect(s).	Nov 11, 2024 1:53 P
109-FI-DP-6454 FI-A 109-FI-DP-6454 FI-B	Initiate image download to endpoint. Image ucs-intersight-infra-4gfi.4.3.4.240074.bin is already available in the cache. Skipping the download. The is selected endpoints.	Nov 11, 2024 1:53 P mage will be synced to the
urce Type grade Firmware	Check if the image has been cached. Verified that the image is available in the cache.	Nov 11, 2024 1:53 P
urce Name 09-FI-DP-6454 FI-A,AA	Wait for firmware upgrade in Fabric Interconnect - B. Fabric Interconnect upgraded from 4.3(4.240066) to 4.3(4.240074) successfully.	Nov 11, 2024 1:53 P
iator	Initiate firmware upgrade in Fabric Interconnect - B. Firmware upgrade request submitted successfully.	Nov 11, 2024 1:38 P
animan@cisco.com	⊘ Wait for a user acknowledgement on Fabric Interconnect - B.	Nov 11, 2024 1:38 P
art Time	⊘ Evacuate data traffic on Fabric Interconnect - B.	Nov 11, 2024 1:37 P
v 11, 2024 1:29 PM	<ul> <li>Wait for image download to complete in endpoint.</li> </ul>	Nov 11, 2024 1:37 F

Step 8. Make sure the Firmware upgrade completed successfully.

#### ← Requests × **Upgrade Firmware** Details **Execution Flow** Status ⊘ Wait for IO Path Connectivity on Fabric Interconnect - A Nov 11, 2024 2:17 PM ⊘ Success IO paths are up. Nov 11, 2024 2:14 PM ⊘ Wait for firmware upgrade in Fabric Interconnect - A. Name Fabric Interconnect upgraded from 4.3(4.240066) to 4.3(4.240074) successfully. Upgrade Firmware Nov 11, 2024 2:00 PM ⊘ Initiate firmware upgrade in Fabric Interconnect - A. ID Firmware upgrade request submitted successfully. 6732771e696f6e3201a36844 ⊘ Evacuate data traffic on Fabric Interconnect - A. Nov 11, 2024 2:00 PM ⊘ Wait for a user acknowledgement on Fabric Interconnect - A. Nov 11, 2024 2:00 PM Target Type Fabric Interconnect ⊘ Wait for IO Path Connectivity on Fabric Interconnect - B Nov 11, 2024 1:57 PM IO paths are up. Target Name AA09-FI-DP-6454 FI-A Wait for image download to complete. Nov 11, 2024 1:53 PM Image ucs-intersight-infra-4gfi.4.3.4.240074.bin successfully cached in Fabric Interconnect(s). AA09-FI-DP-6454 FI-B



≡	cisco Intersight	🔩 Infrastructure Service 🗸			Q s	earch	C	Ø 🗗 🖲	Q 💷	A2 (?	)   A
(¢.	Overview	Fabric Interconnect	S								
(0)	Operate ^	* All Fabric Interconne  +  Q Search		Filters 2 results							xport
	Servers	Health	Connection	Contract Status	Rundle Version	NX-OS Version		Models			24
	Chassis		O Connected 2	Not Covered 2							34
1	Fabric Interconnects	2 Healthy 2			2 • 4.3(4.240074) 2	2 9.3(5))4	43(4b) 2	2	6454 2		
	HyperFlex Clusters										
	Integrated Systems	Name	: Health	: Model	: Bundle Versie	on : UCS Doma	ain Profile	Total	Ports Used	Availa	\$
	integrated systems	AA09-FI-DP-6454 FI-A	O Healthy	UCS-FI-64	54 4.3(4.240074	Coh-Doma	ainProfile	54	18	36	
G	Analyze	AA09-FI-DP-6454 FI-B	O Healthy	UCS-FI-64	54 4.3(4.240074	Coh-Dom:	ainProfile	54	18	36	
	Explorer New							Rows per pag	ge 22 ~	) < 💽	>

## Rolling Upgrades (Node Firmware and Cohesity software)

#### Procedure 1. Upgrade Cisco UCS C-Series Node Firmware with Cohesity Data Cloud Software Upgrade

This procedure expands on the procedure to upgrade the firmware of Cisco UCS C-Series Cohesity certified nodes with Cohesity Cluster software upgrade.

**Note:** Before starting the upgrade procedure, make sure the recommended Cisco UCS C-Series firmware is compatible with the Cohesity software version.

**Step 1.** Login to <u>https://Intersight.com</u>, click Infrastructure Service, then click Servers. Select the Cisco UCS C-Series nodes that are part of the Cohesity cluster. Click the ... icon and select Upgrade Firmware.

	-ilialia Intersight	Infrastructure Service 🗸		Q Search	C ⊗ ⊄11	ር 💷 💶 💿 🛛 ደ
:0:	Overview	Servers				
(Ø)	Operate ^	* All Servers	▼ Filters 4 results			👌 Export
	Chassis	System > (1) On 4	HCL Status Bundle Version	Utility Storage Firmware V	/erslon	Models
	Fabric Interconnects	Profile > VMware >	4 • 4.3(4.240152) 4	4	<b>4</b> .3(4.240152) <b>4</b>	4 • C240 M
	HyperFlex Clusters	Install Operating System : H	ealth : Model : Server Profile	: UCS Domain :	Bundle Ver :	Serial : 🖇
	Integrated Systems	Upgrade Firmware Start Alarm Suppression	Healthy UCSC-C240-M Coh-ServerTemple     Healthy UCSC-C240-M Coh-ServerTemple	ate_DERIVED-1	4.3(4.240152)	WZP2651059D
O,	Analyze	Stop Alarm Suppression 54-3	Healthy UCSC-C240-M Coh-ServerTemple	ate_DERIVED-3 ② AA09-FI-DP-64	4.3(4.240152)	WZP26510552 ····
	Explorer New	Construction un54-4	Critical UCSC-C240-M Coh-ServerTemple	ate_DERIVED-4	4.3(4.240152)	WZP26510561
.0	Configure ^	··· 🖉 Selected 4 of 4 Show Selected	Unselect All		Rows per pa	age 10 ~ < 1 >

**Step 2.** Make sure all Cisco UCS C-Series nodes which are part of single Cohesity cluster are selected for upgrade. Click Next.

≡ "listo" Intersight	s infrastructure Service 🗸		Q Search	C © 4	) ር 🚥 💶 💿 🏻
. Overview	Contraction of the servers Upgrade Firmware				
Operate ^	(1) General	General Ensure selected servers meet requirements for firmware upgrad	0.		
Servers	2 Version				
Chassis	3 Summary	Q Search Filters 4 results			
Fabric Interconnects		Name User Label :	Model : Firmw	are Version : I	UCS Domain 🛞
		AA09-FI-DP-6454-4	UCSC-C240-M6L 4.3(4.)	240152)	AA09-FI-DP-6454
HyperFlex Clusters		AA09-FI-DP-6454-1	UCSC-C240-M6L 4.3(4.3	240152)	AA09-FI-DP-6454
Integrated Systems		AA09-FI-DP-6454-3	UCSC-C240-M6L 4.3(4.3	240152)	AA09-FI-DP-6454
		AA09-FI-DP-6454-2	UCSC-C240-M6L 4.3(4.3	240152)	AA09-FI-DP-6454
Analyze     Analyze     New		Selected 4 of 4 Show Selected Unselect All		Rows per pag	je 10 ~ < 1 >

**Step 3.** Select the recommended Server Firmware version and click Next. At the time of publishing this guide, the suggested firmware was 4.3(4.240152). If the firmware upgrade does not require drive firmware updates, select Advanced Mode, and check the Exclude Drive option.

**Note:** In the existing document, we are upgrading to a Firmware version which is not a recommended version. This is just to demonstrate the process of Firmware upgrades. You should make sure to be on the recommended version of Cisco UCS Firmware.

≡	disco Intersight	🚴 Infrastructure Service 🗸		Q Search	C ⊘	¢] 🕦	Q 02 A1	0	۶
	Overview	<ul> <li>← Servers</li> <li>Upgrade Firmware</li> </ul>							
0	Operate ^	General	Version Select a firmware version to upgrade the servers to.						
	Servers Chassis	3 Summary	The selected firmware bundle will be downloaded from storage controllers. Use Advanced Mode to exclude up	n intersight.com. All the server compone ograde of drives and storage controllers	nts will be upg	araded along	with drives and		
	Fabric Interconnects		Advanced Mode						
	HyperFlex Clusters		Q Search         ₹ Filters 29 results           Version         :         Size : Release Date	: Description			:	0	
Q	Analyze ^		4.3(5.240021)         897.29 MiB         Oct 22, 2024 11           4.3(4.242038)         889.16 MiB         Sep 26, 2024 7:	Cisco Intersight Server Bundle     Cisco Intersight Server Bundle     Cisco Intersight Server Bundle	_			0	
	Explorer New		4.3(4,241063)     917.00 MiB Aug 21, 2024 8:     4.3(4,240152)     4.3(4,240152)     4.3(4,240152)     4.3(4,240152)	25 Cisco Intersight Server Bundle				9	
,0	Configure ^		0         4.3(3.240043)         851.35 MiB         Apr 24, 2024 7:0	06 Cisco Intersight Server Bundle				0	
	Profiles		O 4.3(3.240022) 851.58 MiB Feb 15, 2024 9:	32 Cisco Intersight Server Bundle					
	Templates		O 4.3(2.240009) 805.19 MiB Mar 7, 2024 9:4	7 AM Cisco Intersight Server Bundle				¢	
	Policies		O 4.3(2.240002) 804.51 MiB Jan 24, 2024 10	38 Cisco Intersight Server Bundle				Ð	
	Pools		() 4.3(2.230270) 804.67 MiB Nov 15, 2023 11	12 Cisco Intersight Server Bundle				æ	
			() 4,3(2.230207) 797.52 MiB Aug 15, 2023 11	11 Cisco Intersight Server Bundle				Ð	
New	Command Palette		Selected 1 of 29 Show Selected Unselect All Cancel	R	ws ner nane (	10 ~	< 1 2 3 Bac	> *	lext

Step 4. Click Upgrade.

≡ diado Intersight 🎝 🖧 Inf	astructure Service 🗸		Q Sear	ch	C ⊗	¢1 1 Q 02 A1	0
© Overview	Servers Jpgrade Firmware						
Operate     Operate     Chassis	General     Version     Summary	Summary Confirm configuration and initiate the upgrade. Firmware Version		Exclude Drives			
Fabric Interconnects HyperFlex Clusters Integrated Systems		4.3(4.241063) Size 917.00 MiB Servers to be Upgraded		Yes Exclude Storage Contro Yes	ollers		
Analyze     Analyze     Analyze		Q Search Vame : User Label : AA09-FI-DP-6454-4	4 results Model : UCSC-C240-M6L	Firmware Versi : 4.3(4.240152)	Requires Reboot	UCS Domain	xport ©
Configure		AA09-FI-DP-6454-1 AA09-FI-DP-6454-3 AA09-FI-DP-6454-2	UCSC-C240-M6L UCSC-C240-M6L UCSC-C240-M6L	4.3(4.240152)     (2)       4.3(4.240152)     (2)       4.3(4.240152)     (2)	Yes Yes Yes	AA09-FI-DP-6454 AA09-FI-DP-6454 AA09-FI-DP-6454	
Templates Policies					Rows per	page 25 × (1	
Pools		Cancel				Back	Upgrade

**Step 5.** Retain the Reboot Immediately to Begin Upgrade option as unselected. When the firmware is mounted and the reboot server message appears, start upgrading the Cohesity Cluster software which will ensure the serial reboots of each node (rolling reboots) and avoid any disruption of operations on Cohesity Data protection services.



≡ diado Intersight	en Prastructure Service ∨		Q Search	C © A1 0 0 A
() Overview	<ul> <li>← Servers</li> <li>Upgrade Firmware</li> </ul>			
Operate     Servers     Chassis     Fabric Interconnects     HyperFlex Clusters     Integrated Systems	<ul> <li>General</li> <li>Version</li> <li>Summary</li> </ul>	Summary Confirm configuration and initiate the upgrade. Firmware Version 4.3(4.241063) @ Size 9 Size 9 Size 9 Firmware will be installed on next boot. To reboot	Exclude Drives Yes Exclude Storage Control Yes	ilers
<ul> <li>Analyze ^</li> <li>Explorer New</li> </ul>		mmediately, please enable the option below.     Reboot Immediately to Begin Upgrade     Cancel Up	Firmware Versi         :         I           4.3(4.240152)         (i)         :         :           grade         4.3(4.240152)         (i)         :	Export           Requires Reboot         UCS Domain           Yes         AA09-FI-DP-6454           Yes         AA09-FI-DP-6454
Configure ^ Profiles		AA09-FI-DP-6454-3 UCSC-C240 AA09-FI-DP-6454-2 UCSC-C240	0-M6L 4.3(4.240152) ⑦	Yes AA09-FI-DP-6454 Yes AA09-FI-DP-6454
Templates Policies Pools				Rowsperpage 25 🕜 🤇 1 🚿
New Command Palette ×	•	Cancel		Back Upgrade

**Step 7.** The Firmware image is downloaded to the end point and staged to the respective node:

etails	Execution Flow	
tatus	Progress	56%
^ In Progress	Wait for firmware staging to complete. Upgrade is in progress.20% completed.	
lame Ipgrade Firmware	Initiate firmware upgrade. Initiated upgrade from 4.3(4.240152) to 4.3(4.241063) successfully.	Nov 11, 2024 2:36 PM
)	⊘ Cancel the previous firmware upgrade task if it is in pending state.	Nov 11, 2024 2:36 PM
732851f696f6e3201a4043c	⊘ Wait for the server to be powered on	Nov 11, 2024 2:36 PM
arget Type	⊘ Update server power status.	Nov 11, 2024 2:36 PM
ack Server	⊘ Wait for BIOS POST completion.	Nov 11, 2024 2:36 PM
arget Name	⊘ Power On server.	Nov 11, 2024 2:36 PM
AU9-FI-DF-6454-3	⊘ Find image source to download.	Nov 11, 2024 2:36 PM
ource Type Ipgrade Firmware	Wait for image download to complete in endpoint. Image intersight-ucs-server-c240-m6.4.3.4.241063.bin successfully cached in Fabric Interconnect(s).	Nov 11, 2024 2:36 PM
ource Name A09-FI-DP-6454-3	Initiate image download to endpoint. Download request for intersight-ucs-server-c240-m6.4.3.4.241063.bin submitted successfully.	Nov 11, 2024 2:28 PM
	<ul> <li>Validate the requirements for the endpoint.</li> </ul>	Nov 11, 2024 2:28 PM
nitiator ndhiman@cisco.com		
tart Timo		

**Step 8.** Once the firmware staging completes, the Server Power cycle option is displayed, close the message, and do not click Proceed. Before proceeding to the next step, make sure all nodes are at this stage.

← Requests Upgrade Firmware		$\times$
Details	Execution Flow	^
Status	Progress 61%	1
Action Required	Wait for server reboot.	
iame Jpgrade Firmware	Ensure server meet requirements to continue upgrade. Please acknowledge to continue with server power cycle. Learn more at Help Center.	
D 64502027696f6e310112c55b	Proceed Do not click on proceed	
arget Type Ilade Server	Wait for firmware staging to complete.     May 1, 2023 1:26 PM     Staging completed successfully.	
← Requests Upgrade Firmware		×
Details	Execution Flow	
Status	Progress	61%
Action Required	<ul> <li>Wait for server reboot.</li> </ul>	
Name Upgrade Firmware	Ensure server meet requirements to continue upgrade. Please acknowledge to continue with server power cycle. Learn more at Help Center.	
ID 6732851f696f6e3201a4043c	Proceed	

**Step 9.** Login to the Cohesity cluster dashboard and click Settings. Click Upgrade.

**Step 10.** Run a Pre-Check to ensure cohesity cluster is in a healthy state and compatible for upgrades.

E COHESITY		Q Search	chx-c240-1 (、 ⑦ H <sup>P</sup> 수 올
Dashboards		Update	
O Data Protection	>		
A Infrastructure	>	Product Patches Security Patches Upgrade	
SmartFiles	>	During the upgrade, the listed Nodes will be updated with the Cohesity Software Version selected previously. Current Version: 6.8.2,u1_release-20240599_aSda4644	
Security Tools	>	Available Upgrade Packages	Get New Package
🕰 Test & Dev		These packages were automatically found and available for upgrading. You can also get a different package and upgrade to it by clicking	"Get New Package".
Marketplace	>	Version Package Name Release Date	Status
System	>	There are currently no Packages on the Cluster. Use the Upload Software Packag	je form to add a Package.
II. Reporting			
😥 Settings	>	Upgrade Pre-check To ensure a smoother cluster upgrade, it is recommended to run a pre-check before upgrading.	
		Passed Nov 11, 2024 2:44pm Status Last Run Time	
		Bug Bro shack	

**Step 11.** Click on get New package, upload the latest version of Cohesity. At the time of writing this document cohesity was tested for upgrade to cohesity-7.1.2\_u2\_release-20240925\_66722648. Click on upload and upgrade option.

Upgrade Options	×
O Provide download URL	
cohesity-7.1.2_u2_release-20240925_66722648.tar.gz × Select File During a rolling Cluster upgrade, all Nodes are updated and the Cluster continues to be available.	
Upload and Upgrade Cancel	

**Step 12.** This step of the upgrade process will take some time, about 20-30 minutes per node when the Cisco UCS C-Series nodes are rebooted and upgraded serially. It will take an additional 2-hours for the four node Cohesity Cluster rolling upgrade of the server firmware.

	0	Enable Multi-Factor Authentication for Linux support user to improve system security.	Go to Setup MFA	× × 1/2 >
≡ COHESITY	Q Search	Upgrade Options	×	сhx-c240-1 🕻 🔘 📙 Ф 😤
Dashboards	Update	Provide download URL     Upload a package file     cohesity-7.1.2 u2 release-20240925 66722648 tar.oz		
O Data Protection	> Product Patc	70% Complete Upload in Progress	-	
A Infrastructure	> During the up	During a rolling Cluster upgrade, all Nodes are updated and the Cluster continues to be availa	ble.	
SmartFiles	> Current Ve	Upload and Upgrade Cancel		
Security Tools	> Available L	lpgrade Packages		Get New Package
🔍 Test & Dev	These packag	es were automatically found and available for upgrading. You can also get a different package and	upgrade to it by clicking "Get New Pa	ickage".
G Marketplace	> Version	Package Name Rele	ase Date Stat	us
D System	> 7.1.2	7.1.2_u2_release-20240925_66722648	Uplo	Seding 56% Com
Reporting	Upgrade P To ensure a s	re-check nother cluster upgrade, it is recommended to run a pre-check before upgrading.		
😵 Settings	> Ø Passed Status	Nov 11, 2024 2:44pm Last Run Time		
	Run Pre-cl	eck View Details		

**Step 13.** During the Rebooting of Cohesity node executed through the Cohesity upgrade process, upgrade of Cisco UCS C-Series nodes is invoked through the staged UCS firmware from Intersight.

≡ C	OHESITY		Q Search			chx-c240-1 🐧 🤅	) <b>H</b> <sup>®</sup> ¢ &
	Dashboards		Cluster				
0	Data Protection	>	Cluster Upgrading Target Version 7.1.2_u2_release-202	40925_66722648	11% completed 56m 37s remaining		
<u>له</u> ۱	nfrastructure	>	Node 10.108.1.166				
	imartFiles	>	Current Version 6.8.2_u1_release-2 Upgrade in progress.	0240509_a5da4644			
@ s	ecurity Tools	>	45% completed Hide Subtasks				
2	est & Dev						-
	Marketplace	>	Start Time	Task		)	
<b>()</b> s	lystem	>	Nov 11, 2024 2:58pm	[7/13]Stop Services -> 30 services stopped			
			Nov 11, 2024 2:58pm	[7/13]Stop Services -> 39 services stopped			
th F	leporting		Nov 11, 2024 2:58pm	[8/13]Install Package -> Starting			
<b>\$</b>	iettings	~	Nov 11, 2024 2:58pm	[7/13]Stop Services -> 10 services stopped			
	Summary		Nov 11, 2024 2:58pm	[7/13]Stop Services -> 20 services stopped			
	Arcess Manageme	at.	Nov 11, 2024 2:58pm	[7/13]Stop Services -> Stopping cluster services			
	Networking	~	Nov 11, 2024 2:58om	17/131Stop Services -> 39 services stopped			*
$\leftarrow \rightarrow$	C S	us-east-	.intersight.com/cisco-vkvm/direct?se	lectedServerMoid=66f7045a6176753701c03057	7&selectedServerName=AA09-FI-DP-6454-2&serverProf	ileName=Coh-ServerTemplate_D	ERIVED-2
≡	officiality inters	ight	AA09-FI-DP-6454-2 (Coh-ServerTempla	e_DERIVED-2)   KVM Console UCSC-C240-M6L	WZP2651055Z		
⊡ c	onsole		Resoluin	g modules dependancy ng modules			
🗐 Fi	le		/deu/sr1 Checking	/deu/sr1			
©ν	iew		Booted i Mounted	the boot device			
ቆ M	lacros		Containe Copying	er file type: squashfs container This may take a fe	w minutes.		
¥ -	nolo		15,	761,408 13% 833.33kB/s 0:0	01:58		
Ú P	ower						
↑в	oot Device						
Öv	irtual Madia						

**Step 14.** You can also monitor the firmware upgrade status of the node with Cisco Intersight in Progress Request.

← Requests Upgrade Firmware			×
Details	Execution Flow		-
Status in Progress	Progress Wait for firmware upgrade to complete. Upgrade is in progress.60% completed.	61%	Î
Upgrade Firmware	⊘ Wait for server reboot.		
ID 672285156965652201540407	Wait for firmware staging to complete. Staging 4.3(4.241063) completed successfully.	Nov 11, 2024 2:43 PM	
Target Type	<ul> <li>Initiate firmware upgrade.</li> <li>Initiated upgrade from 4.3(4,240152) to 4.3(4,241063) successfully.</li> </ul>	Nov 11, 2024 2:37 PM	
Rack Server	${\scriptsize \bigcirc}$ Cancel the previous firmware upgrade task if it is in pending state.	Nov 11, 2024 2:37 PM	
Target Name	$\oslash$ Wait for the server to be powered on	Nov 11, 2024 2:37 PM	
AA09-FI-DP-6454-2	⊘ Update server power status.	Nov 11, 2024 2:37 PM	
Source Type	Wait for BIOS POST completion.	Nov 11, 2024 2:37 PM	

**Step 15.** The details of the firmware and software upgrade completing the first Cisco UCS C-Series node and the beginning of the upgrade procedure for the second Cisco UCS C-Series node initiated through the Cohesity Data Cloud is shown below:

=	diale Intersight	Infrastructure Service 🗸	Q s	earch	C 0 03 41	Q 💶 💶 💿 🛛 ႙
ġ.	Overview	Servers				
0	Operate ^	* All Servers  +  Q Search	▼ Filters 4 results			🖒 Export
I	Chassis	Health Critical 1 Power () On 4	HCL Status (1) Incomplete 4 (2) Incomplete 4 (3) Incomplete 4 (4) Incomplete (4) Incomplete	Utility Storage	Firmware Version	Models
	Fabric Interconnects HyperFlex Clusters	Name : He	ealth : Model : Server Profile	:	UCS Domain : Bundle Ver :	Serial : \$
~	Integrated Systems	○         AA09-FI-DP-6454-1 ⊙           ○         O           ○         AA09-FI-DP-6454-2	Healthy UCSC-C240-M, Coh-ServerTemplat     UCSC-C240-M, Coh-ServerTemplat     UCSC-C240-M, Coh-ServerTemplat	e_DERIVED-1	AA09-FI-DP-64 4.3(4.240152) AA09-FI-DP-64 4.3(4.241063)	WZP2651059D WZP2651055Z
Q	Analyze ^ Explorer New	○         AA09-FI-DP-6454-3 ④           ○         AA09-FI-DP-6454-4 ④	Healthy UCSC-C240-M Coh-ServerTemplat     UCSC-C240-M Coh-ServerTemplat	e_DERIVED-3	AA09-FI-DP-64 4.3(4.240152) AA09-FI-DP-64 4.3(4.240152)	WZP2651056H WZP26510561
,0	Configure ^				Rows per p	age 10 ~ < 1 >



**Step 16.** All the nodes are upgraded serially in the cluster, confirm the upgraded versions for the Cohesity Cluster and Cisco UCS C-Series node firmware.

	Enable Multi-Factor Authentication for Linux support user to improve system security.	Go to Setup MFA	× < 1/2
	Q Search		chx-c240-1 ( @ H <sup>2</sup> ) s
			5 0 H ÷ L
5 Infrastructure >	Cluster		
SmartFiles	Summary Storage Domains Nodes Key Management System Syslog		
Security Tools	Chuster Summer		
Test & Dev	Cluster Summary		Upgrade
Marketplace >	721.2 TiB	Cluster Name	chx-c240-1 449643612523690
	Total Size	Creation Date	Oct 4, 2024 4:59pm
] System >	(	Software	7.1.2_u2_release-20240925_66722648
Reporting	Free 720.6 TIB     Used 682.9 GB	Software Encryption	Disabled
🕻 Settings 🗸 🗸		Hardware Encryption	Disabled
		Storage Domains	3
Summary		Nodes Support Channel	4 Temporarily On
Access Management		and the second	Expires on Nov 27, 2024 5:54pm
Networking		Support Channel token	JDIkUU5DU1RocE4vU0dDeU1aeTZaQys 🛱
SNMP		Storage Capacity for Metadata	43.1 TiB
		Storage Used for Metadata Failure Domain	0% Node
Software Update			
Infrastructure > SmartFiles >	Cluster Summary Storage Domains Nodes Key Management System Syslog		
Security Tools >			
Test & Dev	Chassis 🔹 Node Status 🔹 Q		
ica d Der	Slot ID Host Name Node Serial Node Status	Capacity IP	Version Disk Status Data Disks
Marketplace >	Chassis: WZP2651055Z		
System >	161963887787 chx-c240-1-wztp265105	174.47.0	7.1.2 u2 release-2024
Reporting	UCS-C240M6H12 5z-node-1 WZP2651055Z C Active	174.4 118 10.108.1.166	0925_66722648 16 HDDs
Settings	Chassis: WZP26510561		
Summary	161963887789 chv-c240.1-wzp265105 WZP26510561 € Active	174.4 TiB 10.108.1.165	7.1.2_U2_release-2024 0925_66722648 IG HDDs
	Chassis: W7P2651056H		
Access Management	161963887788 chy.c240.1.urm265105		7 1 2 u2 release 2024
Networking	1 UCS-C240M6H12 6h-node-1 WZP2651056H C Active	174.4 TiB 10.108.1.164	0925_66722648
SNMP	Chassis: WZP2651059D		
Software Update	1 161963887786 chx-c240-1-wzp265105 WZP2651059D C Active	174.4 TIB 10.108.1.163	7.1.2_u2_release-2024 0925_66722648 16 HDDs
License	Infrastructure Service V	O Search	
	Servers	Q search	
Overview			
	* All Servers 🛞 +		
Operate ^	··· Ø Q Search Filters 4 results		🛆 Export
Servers	Health Power HCL Status Bundle Version	Utility Storage Firmware Vers	Ion Models
hassis	Critical 1 () On 4 () Incomplete 4	No 4	· · · · ·
abric Interconnects	4 • Healthy 3 • 4.3(4.24106)	53) 4	• 4.3(4.241063) 4 4 • C240 M (
HyperFlex Clusters			
tegrated Systems	Name : Health : Model : Server Profile	: UCS Domain :	Bundle Ver : Serial : 5
	UCSC-C240-M Coh-ServerTer	AA09-FI-DP-64	4.3(4.241003) WZP2651059D ····
	Cob-ServerTer	mplate_DERIVED-2  AA09-FI-DD-64	4.3(4.241063) WZP26510557
nalyze ^	O         AA09-FI-DP-6454-2         O         Healthy         UCSC-C240-M         Coh-ServerTer           O         AA09-FI-DP-6454-3         O         Healthy         UCSC-C240-M         Coh-ServerTer	mplate_DERIVED-2 @ AA09-FI-DP-64 mplate_DERIVED-3 @ AA09-FI-DP-64	4.3(4.241063) WZP2651055Z ···· 4.3(4.241063) WZP2651056H ····
lyze ^	©         AA09-FI-DP-6454-2         © Healthy         UCSC-C240-M         Coh-ServerTer           ©         AA09-FI-DP-6454-3         © Healthy         UCSC-C240-M         Coh-ServerTer           ©         AA09-FI-DP-6454-3         © Healthy         UCSC-C240-M         Coh-ServerTer           ©         AA09-FI-DP-6454-4         © Critical         UCSC-C240-M         Coh-ServerTer	Implate_DERIVED-2     O     AA09-FI-DP-64       Implate_DERIVED-3     O     AA09-FI-DP-64       Implate_DERIVED-4     O     AA09-FI-DP-64	4.3(4.241063)         WZP2651055Z         ···           4.3(4.241063)         WZP2651056H         ···           4.3(4.241063)         WZP2651056H         ···
nalyze ^ kplorer New onfigure ^	O         AA09-FI-DP-6454-2         O Healthy         UCSC-C240-M         Coh-ServerTe           O         AA09-FI-DP-6454-3         O Healthy         UCSC-C240-M         Coh-ServerTe           O         AA09-FI-DP-6454-4         O critical         UCSC-C240-M         Coh-ServerTer            Ø           Ø	Implate_DERIVED-2     AA09-FI-DP-64       Implate_DERIVED-3     AA09-FI-DP-64       Implate_DERIVED-4     AA09-FI-DP-64	4.3(4.241063) WZP26510552 ···· 4.3(4.241063) WZP2651056H ···· 4.3(4.241063) WZP2651056H ···· Rows per page 10 · · · · · · · · · · · · · · · · · ·

Upgrade Node Firmware (Cohesity Cluster in maintenance window)

**Procedure 1.** Upgrade Cisco UCS C-Series Firmware independent of Cohesity Data Cloud Upgrades

**Note:** This procedure expands on the procedure to upgrade the firmware of only Cisco UCS C-Series Cohesity certified nodes. The Cohesity software upgrade is not part of this procedure.

**Note:** Before starting the upgrade procedure, make sure the recommended Cisco UCS C-Series firmware is compatible with the Cohesity software version.

**Note:** Since the Cisco UCS C-Series node firmware upgrade requires a reboot, please initiate support of Cohesity to shut down the Cohesity cluster during the maintenance window.

This procedure is utilized in three key circumstances.

- Only the Cisco UCS C-Series node firmware requires an upgrade.
- You are comfortable with having a maintenance window for the Cohesity cluster downtime.

• Since the Rolling upgrade adds up to 20-30 minutes per node and is executed serially, it could be time consuming for Cohesity cluster with several nodes. In this case, you can initiate a node reboot from Cisco Intersight and upgrade the Cisco UCS C-Series node firmware in parallel to all nodes. This requires downtime for Cohesity cluster and can only be initiated in a maintenance window.

**Step 1.** Login to <u>https://intersight.com</u> and select the account registered to Cohesity C-Series nodes managed through Intersight.

**Step 2.** Select Infrastructure Service, then select Servers and identify the new Cisco UCS C-Series nodes available for Cohesity cluster creation or nodes available to add to existing cluster. Ensure Server Profile is successfully deployed to the Cohesity nodes.

=	cisco Intersight Service V			Q Search C	ତ ମ ଦ୍ 🍽 🗠	۶ 🕲 🚺	٩
.@:	Servers						
0	* All Servers 🗇 +	▼ Filters 4 results				🛆 Export	
,e	Health Power (C) On 4	HCL Status     Bundle Version       ⑦ Incomplete 4     4       ④ # 4.2(3h) 4	Firmware Version • 4.2(3h) 4	Models Contract Not Contract	t Status Profile Status	т Ж ■ ок 4 ←	
	Name 3 He	ealth : Model : CPU Cap	💿 🗧 Memory Cap 🗧	UCS Domain : Server Profile		Bundle Ve 💠	
	C & AA09-FI-DP16454-1	Healthy UCSC-C240-M6L	128.0 128.0	AA09-FI-DP-6454 Coh-ServerTemplate_	DERIVED-1 ©	4.2(3h)	
	() AA09-FI-DP-6454-2	Healthy     UCSC-C240-M6L	128.0 128.0	AA09-FI-DP-6454 Coh-ServerTemplate_	DERIVED-2	4.2(3h)	
	() AA09-FI-DP-6454-3	Healthy UCSC-C240-M6L	128.0 128.0	AA09-FI-DP-6454 Coh-ServerTemplate_	DERIVED-3 O	4.2(3h)	
	() AA09-FI-DP-6454-4	G Healthy UCSC-C240-M6L	128.0 128.0	AA09-FI-DP-6454 Coh-ServerTemplate_	DERIVED-4 O	4.2(3h)	
					Rows per page 10 ~	< 1 >	

**Step 3.** Select the servers, click the ellipses "..." and select 'Upgrade Firmware' option.

Servers									
* All Server	s @ +								
····)?	Q Search	▼ Filters 4 res	ults						🛆 Exp
Power System Profile VMware	> Power	HCL Status	Bundle Version	Firmware Ver	• 4.2(3h) 4	Models	Contract Status	Profile Status	• OK 4
Install Ope	ating System	Health	Model : CPU Cap	© : Memo	ry Cap :	UCS Domain :	Server Profile	:	Bundle V
Upgrade F	54-1	O Healthy	UCSC-C240-M6L	128.0	128.0	AA09-FI-DP-6454	Coh-ServerTemplate_DERIVED-1	0	4.2(3h)
Start Alarm	Suppression 54-2 Suppression	O Healthy	UCSC-C240-M6L	128.0	128.0	AA09-FI-DP-6454	Coh-ServerTemplate_DERIVED-2	0	4.2(3h)
Set License	54-3 Tier	C Healthy	UCSC-C240-M6L	128.0	128.0	AA09-FI-DP-6454	Coh-ServerTemplate_DERIVED-3	0	4.2(3h)
M	nuo 11 ur un54-4	Healthy	UCSC-C240-M6L	128.0	128.0	AA09-FI-DP-6454	Coh-ServerTemplate_DERIVED-4	Ø	4.2(3h)

Step 4. Select Start Firmware upgrade and ensure the Cisco UCS C-Series nodes are selected. Click Next.

≡	olin Intersight Serv	vice V		Q	Search	0 0 4 0 0 00	<u>ଡ</u> ୍ଚ
:@.	<ul> <li>← Servers</li> <li>Upgrade Firmware</li> </ul>						
•	<ol> <li>General</li> <li>Version</li> </ol>	General Ensure selected servers meet requirem	ents for firmware upgrade.				
,e	3 Summary	Q. Search	➡ Filters 4 results User Label	: Model	Firmware Version	: UCS Domain	0
		AA09-FI-DP-6454-4		UCSC-C240-M6L	4.2(3h)	AA09-FI-DP-6454	
		AA09-FI-DP-6454-1		UCSC-C240-M6L	4.2(3h)	AA09-FI-DP-6454	
		AA09-FI-DP-6454-3		UCSC-C240-M6L	4.2(3h)	AA09-FI-DP-6454	
		AA09-FI-DP-6454-2		UCSC-C240-M6L	4.2(3h)	AA09-FI-DP-6454	
		Selected 4 of 4 Show Selected	Unselect All			Rows per page 10 ~ (	1 >
	<	Cancel				Ba	ck

**Step 5.** Identify the recommended Firmware version. In general, the recommended sign is displayed on the firmware. Click Next.

By default the drive and storage controller firmware is also upgraded. To avoid drive failure and improve the resiliency of drives, it is recommended to upgrade drive firmware. Drives can be excluded from firmware upgrades, through 'Advanced Mode'.

ntersight 🍡 🎝 Infrastru	cture Service 🗸	Q Search	C ⊚ ≮	1 🗘 🔍 🚳	0
← Servers Upgrade Firmware					
General	Version Select a firmware version to upgrade the servers to.				
3 Summary	The selected firmware bundle will be downloaded from intersight.com. storage controllers. Use Advanced Mode to exclude upgrade of drives a	All the server components will be upgraded along with driv and storage controllers.	ves and		
	Advanced Mode				
	Titers 27 results				
	Version Size Release Date Descript	ion		1	0
	O 4.3(4.242038) 889.16 MiB Sep 26, 2024 7:57 Cisco Int	ersight Server Bundle			٢
	O 4.3(4.241063) 917.00 MiB Aug 21, 2024 8:25 Cisco Int	ersight Server Bundle			Ø
	④ 4.3(4.240152) ⑤ 916.98 MiB Jun 4, 2024 10:13 Cisco Int	ersight Server Bundle			٩
	O 4.3(3.240043) Im51.35 MiB Apr 24, 2024 7:06 Cisco Int	ersight Server Bundle			۲
	O 4.3(3.240022) 851.58 MiB Feb 15, 2024 9:32 Cisco Int	ersight Server Bundle			ø
	O 4.3(2.240009) 805.19 MiB Mar 7, 2024 9:47 AM Cisco Int	ersight Server Bundle			Ð
	O 4.3(2.240002) 804.51 MiB Jan 24, 2024 10:38 Cisco Int	ersight Server Bundle			Ø
	O 4.3(2.230270) 804.67 MiB Nov 15, 2023 11:12 Cisco Int	ersight Server Bundle			æ
	O 4.3(2.230207) 797.52 MiB Aug 15, 2023 11:11 Cisco Int	ersight Server Bundle			æ
	O 4.2(3I) 870.77 MiB Jun 17, 2024 11:12 Cisco Int	ersight Server Bundle			æ
	Selected 1 of 27 Show Selected Unselect All	Rows ner n	iane 10 ~	(1) 2 3	>

Step 6. Confirm the firmware version for upgrades on Cohesity nodes. Click Upgrade.

	← Servers						
l	General     Version	Summary Confirm configuration and initiate the upgrade	ь.				
	3 Summary	Firmware Version 4.3(4.240152) @ Size 916.98 MiB Servers to be Upgraded		Exclude No No	e Drives e Storage Controllers		
		Q Search Filte	ers 4 results	Firmware Versi	Requires Reboot O	UCS Domain	UCS Domain
		AA09-FI-DP-6454-4	UCSC-C240-M6L	4.2(3h)	) Yes	AA09-FI-DP-6454	AA09-FI-DP-6454
		AA09-FI-DP-6454-1	UCSC-C240-M6L	4.2(3h)	) Yes	AA09-FI-DP-6454	AA09-FI-DP-6454
		AA09-FI-DP-6454-1 AA09-FI-DP-6454-3	UCSC-C240-M6L UCSC-C240-M6L	4.2(3h) (0) 4.2(3h) (0)	) Yes	AA09-FI-DP-6454 AA09-FI-DP-6454	AA09-FI-DP-6454 AA09-FI-DP-6454
		AA09-FI-DP-6454-1 AA09-FI-DP-6454-3 AA09-FI-DP-6454-2	UCSC-C240-MBL UCSC-C240-MBL UCSC-C240-MBL	4.2(3h) ③ 4.2(3h) ④ 4.2(3h) ④	) Yes ) Yes ) Yes	AA09-FI-DP-6454 AA09-FI-DP-6454 AA09-FI-DP-6454 Rows per pag	AA09-FI-DP-6454 AA09-FI-DP-6454 AA09-FI-DP-6454 20 25 ~ < 1

**Step 7.** On the Upgrade Firmware confirmation screen, enable Reboot Immediately to Begin Upgrade.

Templates				
UCS Chassis Profile Templates UCS Domain Profile	Templates UCS Server Profile Templates vNIC Templates	nplates vHBA Templates		
	ALC: A CONTRACT OF		_	
* All UCS Server Profil			Create UCS Serve	er Profile Tempi
* All UCS Server Profit	Filters 1 results		Create UCS Serve	er Profile Templ
* All UCS Server Profil_ () +	Filters 1 results Usage : Target Platform :	Description	Create UCS Serve	er Profile Templ
* All UCS Server Profil_  +  All UCS Server Profil_  +  C Gasearch  Name  Coh-ServerTemplate	Filters 1 results Usage : Target Platform : 0 UCS Server (FI-Attached)	Description	Create UCS Serve	er Profile Templ

**Step 8.** Select Infrastructure Service, then select Servers and identify the new Cisco UCS C-Series nodes available for Cohesity cluster creation or nodes available to add to existing cluster.

	di Intersight 🍀 Infrastructure	) Service 🗸			Q	Search	C 0	\$1 Q @ @	0	13
c.	<ul> <li>Servers</li> <li>Upgrade Firmware</li> </ul>									
	General	Summary Confirm configuration and initiate th	e upgrade.							
6 Summary		Version 4.3(4.240152) @ Size 916.98 MIB Servers to be Upgraded Up	Firmware Version 4.3(4.240152) @ 5/2/2 915.98 MiB Servers to be Upgraded Firmware will be installed on next boot. To reboot			irives torage Controllers		_		
		Q Search imme	Adiately, please enable the option b	elow.		Requires Reboot O	UCS Domain	UCS Domain	Export	
		AA09-FI-DP-6454-4		Cancel U	pgrade	Yes	AA09-FI-DP-6454 AA09-FI-DP-6454	AA09-FI-DP-6454 AA09-FI-DP-6454		
		AA09-FI-DP-6454-3	UCSC-C240-M6L	4.2(3h)	٢	Yes	AA09-FI-DP-6454	AA09-FI-DP-6454		
		AA09-FI-DP-6454-2	UCSC-C240-M6L	4.2(3h)		Yes	AA09-FI-DP-6454	AA09-FI-DP-6454		
							Rows per pa	ge 25 👻 🤇 (	1 >	
		< Cancel						Bac		arad

**Step 9.** Monitor the firmware upgrade process. The firmware is automatically downloaded to the sever end point.

" Intersight " Infr	astructure Service 🗸	Q Search C O	■ 4	Q 💿 🚳	0
Servers	← Requests Upgrade Firmware				
* All Servers @ +	Details	Execution Flow			
Health	Status In Progress	Progress			13%
(A) + Health	y 4 Name Upgrade Firmware	Initiate image download to endpoint. Download request for intersight-ucs-server-c240-m6.4.3.4.240152 bin submitted successfully.		Sep 27, 202	4 2:03 PM
Name	ID 66f71d95696f6e32013fbf5c	Validate the requirements for the endpoint.	J	Sep 27, 202	4 2:03 PN
AA09-FI-DP-     O AA09-FI-DP-     O AA09-FI-DP-     O AA09-FI-DP-	6454 G454 Rack Server				
© AA09-FI-DP-	Target Name AA09-FI-DP-6454-2	lş.			
	Source Type Firmware Upgrade				
	Source Name AA09-FI-DP-6454-2				
	Initiator andhiman@cisco.com				
	and the second se				

Step 10. Confirm on completion of C-Series node firmware to the installed version.

≡	cisco Intersight	😂 Infrastructure Service 🗸	Q search C O A 1 Q @2 @1 0 A
(¢:	Overview	Servers	
0	Operate ^		▲ Export
	Chassis	Health Power HCL Status Bundle Version	Utility Storage Firmware Version Models
	Fabric Interconnects	4 •	4 • 4.3(4.240152) 4 4 • C240 M ←
	Integrated Systems	Name : Health : Model : Server Profile	: UCS Domain : Bundle Ver : Serial : 5
		C AA09-FI-DP-6454-1 O Healthy UCSC-C240-M Coh-ServerTem	mplate_DERIVED-1 @ AA09-FI-DP-64 4.3(4.240152) WZP2651059D
O.	Analyze ^	AA09-FI-DP-6454-2 @ Healthy UCSC-C240-M Coh-ServerTem	mplate_DERIVED-2 ② AA09-FI-DP-64 4.3(4.240152) WZP2651055Z ····
	Frontanan	Coh-ServerTem     O AA09-FI-DP-6454-3     O Healthy     UCSC-C240-M     Coh-ServerTem	mplate_DERIVED-3
	Explorer New	O AA09-FI-DP-6454-4     O Critical UCSC-C240-M Coh-ServerTem	mplate_DERIVED-4
,e	Configure ^		Rows per page 10 $$ ( 1 )

Step 11. When the firmware across all Cisco UCS C-Series nodes are upgraded, restart the Cohesity Cluster.

## Solution Validation

This chapter contains the following:

- Backup the SQL Server with Cohesity File Based Protection Group
- <u>Restore SQL Server with Cohesity File Based Protection Group</u>

This chapter provides a high level solution validation summary for protection of standalone Microsoft SQL Server database hosted on Cisco Compute Hyperconverged with Nutanix cloud platform. The validation environment for this CVD are detailed below:

• Cohesity Data Cloud was deployed on a four (4) node Cisco UCS C-Series cluster configured with Cisco UCS C240 M6 LFF rack servers

• SQL Server 2022 was deployed on Windows VM configured on AHV based Nutanix cluster on Cisco Compute Hyperconverged HCIAF240C M7 All-NVMe servers

• SQL Server Operational database workload (OLTP) was generated with HammerDB tool (v4.10) with a size of 500GB loaded using 5000 warehouse IDs and stored on multiple vDisks

**Note:** The HammerDB tool is used to simulate and run TPROC-C-like workloads on the SQL Server virtual machines. It is a leading benchmarking and load testing software for the world's most popular databases like Microsoft SQL Server. It implements a fair usage of <u>TPC</u> specifications for benchmarking the database workloads such as Online Transactional (OLTP) and Decision Support System(DSS). TPC is an industry body most widely recognized for defining benchmarks.

Cohesity supports the following MS SQL Server backups:

- Volume-based Backup
- File-based Backup
- VDI-based Backup

In the existing validation, File-based Backup was used to test protection of SQL Server on Nutanix AHV with the Cohesity Data Cloud. File-based backup protects only the MS SQL databases you choose. It captures only the database files for those selected databases. This approach contrasts with a volume-based backup, which captures any and all the files contained on the volume.

**Note:** To enable file-based backup, you must install the File System CBT component during Cohesity agent installation.

**Note:** The steps to enable protection of SQL Server with Cohesity is outside the scope of this document. To learn more, please refer to the <u>Cohesity documentation on protection of Microsoft SQL Server</u>

## Backup the SQL Server with Cohesity File-based Protection Group

The objective of this test is to demonstrate protection of a large SQL server database deployed on a single AHV based VM on Cisco Compute Hyperconverged with Nutanix. Cohesity File-based Protection Groups protect only the specific MS SQL databases that you select.

<u>Table 16</u> lists the test configuration details.

#### **Table 16.** File Based Backup configuration details

Component	Details
vCPUS	1
No of Cores	8
Memory	32GB
Storage Layout	<ul> <li>1x 120G disk for Widows OS + SQL Binaries + System Databases</li> <li>Following disks are used for storing 500G user/test database</li> <li>4x 200G disks for user Database data files</li> <li>2x 300G disks for TempDB data files</li> <li>1x 600G disk for user database and TempDB T-Log files</li> <li>1x 800G disks for backup</li> </ul>
Database Site and file Layout	500G Created with 4x data files each is 100G and 1x T-Log file of size 300G
SQL Server Settings	Max Memory = 122 Soft-NUMA disabled Enabled Lock Pages in memory and Instant file Initialization
Workload details	SQL Server Operational database workload (OLTP) generated with HammerDB tool (v4.10) Database Size= 500GB Warehouse IDs= 5000
Cohesity Agent	File Based Agent
Backup Type	Full backup

The screenshot below captured through the Cohesity dashboard details the successful backup of 500GB OLTP database on SQL Server in approximately 5 minutes.

≕ COHESITY	Q Search					chx-c240-1	< ⊘ H° ⊅ ≗
Dashboards	← Runs for tpc500G-protect						
🥥 Data Protection 🗸 🗸							
Protection	Run Details: tpc500G	-protect					1
Recoveries	Backup						
Sources	Succeeded	⊘ 1 Succeeded	0 Failed	Canceled	© 0 Skipped	5m 16s	Delete Snapshots
Policies	Status SUA Status	Objects	Objects	Objects	Objects	Duration	
CloudRetrieve	Status • Q						
Runbooks	Microsoft SQL Object Name	Start Time	End Time Duration	Data Read	Logical Size	Message	
A Infrastructure	□ Ø 10.108.2.151 Size: 650.1 GiB	Nov 1, 2024 9:12am	Nov 1, 2024 9:17am 5m 11s	650.1 GiB	650.1 GiB		
SmartFiles	Size: 650.1 GiB	Nov 1, 2024 9:12am	Nov 1, 2024 9:17am 4m 59s	650.1 GiB	650.1 GiB		
	1						

Dashboards	Protection	
😡 Data Protection 🗸 🗸	Group Details: tpc500G-protect	
Protection	Policy: SQLPolicy Runs Audit Trail Settings Consumption Trend	
Recoveries		
Sources	Source	
Policies	MS SQL Servers	
CloudRetrieve	Objects	
Runbooks	1 1	
A Infrastructure	Microsoft SQL Objects Manually Protected	
SmartFiles		
🖏 Test & Dev	Policy	
G Marketplace >	SQLPOIICY	
System >	Backup Every day   Retain 2 weeks	
H Reports	Ketty Options met 5 minutes apart	
Last login: Nov 12, 2024 2:01pm	Every 1 hour   fletinin 2 weeks	
≍ COHESITY	Q, Search chx-c240-1 (€ ⑦ H <sup>2</sup> A 2	8
COHESITY     Dashboards	Q search chx-c240-1 ( ③ H ♀ 2 ← Protection	<u>ڪ</u>
COHESITY  Dashboards  Data Protection	Q. Search       chx<2240-1	8
COHESITY  Dashboards  Data Protection  Protection	Q. Search       chx<240-1	2
COHESITY  Construction  Construction  Protection  Recoveries	Q Search       chx<240-1	2
COHESITY  Constants  DataProtection  Protection  Recoveries  Sources	Q. Search       chx<240-1	
COHESITY  Cashboards  Data Protection  Protection  Recoveries  Sources  Policies	Q. Search       chx <c2401< td="">       Q. O       H. A. 2         Image: Constraint of the second se</c2401<>	
COHESITY  Cate Protection  Protection  Recoveries  Sources  Policies  CloudRetrieve	Q. Search       chx<240·1	
COHESITY  Cashboards  Data Protection  Protection  Recoveries  Sources  Policies  CloudRetrieve  Runbooks	Q. Search       Chr. 22401       C. O. H. A. 2         C Protection       Settings         Storage Domain       SQLDomain         Start Time       9:12am   America/Los_Angeles         SLA       Full: 1 day         Incremental: 1 day       Incremental Backups complete within 1 day and Incremental Backups complete within 1 day         Microsoft SQL Settings       Site hand	
COHESITY  Cashboards  Cata Protection  Protection  Recoveries  Sources  Policies  CloudRetrieve  Runbooks  infrastructure	Q. Search       Chr. 22401       Q. O H. A. 2         ✓ Protection       Settings         Storage Domain       SQLDomain         Start Time       9:12am   America/Los_Angeles         SLA       Full: 1 day         Incremental: 1 day       Incremental Backups complete within 1 day and Incremental Backups complete within 1 day         Microsoft SQL Settings       File-based         Mate Full Backups Consecutiv       Off	2
COHESITY  Cashboards  Cata Protection  Protection  Recoveries  Sources  Policies  CloudRetrieve  Runbooks  Infrastructure  SmartFiles  SmartFiles	Q Search Chr 22401 C O H A 2     C Protection     Settings   Storage Domain   Start Time   Start Time   StA   Full: 1 day   Incremental: 1 day   Incremental: 1 day   O   SLA will be met if Full Backups complete within 1 day and Incremental Backups complete within 1 day     Microsoft SQL Settings   Backup Type   File-based   Make Full Backups Copy-only   Off   Databases to Backup   All user and system databases. Use server preferences for AAG databases.	2
COHESITY  Cashboards  Data Protection  Protection  Recoveries  Sources  Policies  CloudRetrieve Runbooks  Infrastructure  SmartFiles  Tast & Dev  Test & Dev  Test & Dev	Search Chr. C2401 C O H A Z   Fortexction   Settings   Storage Domain   Start Time   9:12am   America/Los_Angeles   SLA   Full: 1 day   Incremental: 1 day     Microsoft SQL Settings   Backup Type   File-based   Make Full Backups Copy-only   Off   Databases to Backup   Additional Settings	2
COHESITY  Cate Protection  Control  Recoveries  Sources  Policies  CloudRetrieve  Runbooks  CloudRetrieve  Runbooks  SmartFiles  SmartFiles  Marketplace  Marketplace	A Search     C Settings     Softings     Storage Domain     SQLDomain     Start Time     S12am [ America/Los_Angeles     SLA     Full: 1 day   Incremental: 1 day   Incremental: 1 day     Microsoft SQL Settings   Backup Type   File-based   Make Full Backups Complete   Make Full Backups Componly   Off   Databases to Backup   Additional Settings   Pause Fulture Buns   No	
COHESITY  Dashboards  Data Protection  Protection  Recoveries  Sources  Policies  CloudRetrieve Runbooks  Infrastructure  Infrastructure Inf	A starth     C Settings     Sorage Domain     Surtime     Startime     Startime   Startime   Startine   Startine <td></td>	
COHESITY  Cashboards  Cata Protection  Protection  Recoveries  Sources  Sources  Policies  CloudRetrieve  Runbooks  CloudRetrieve  Runbooks  SmartFiles  SmartFiles  Marketplace  System  Kashboards  Reports  Re	C Sarch     C Protection     Settings   Storage Domain   Start Time	

Cohesity protection group setting for the backup job is shown below:

## **Restore SQL Server with Cohesity File Based Protection Group**

The objective of this test is to demonstrate restoration of the protected SQL server database deployed on a single AHV based VM on Cisco Compute Hyperconverged with Nutanix. As mentioned in the previous section Cohesity File-based Protection Groups was utilized to protect the existing 500G TPC database. SQL Database was restored to same VM but as a different database

The screenshot below showcases the successful restore of SLQ database in approximately 9 minutes:

≡ COHESITY	(	Q Search				chx-c240-1	6 @ H	¢ <b>9</b> &
Dashboards		← Recoveries						
O Data Protection	>							
A Infrastructure	>	Recover_Microsoft_SQL	_Nov_14_2024_11_	36_AM				
SmartFiles	>	Details Options						
🌯 Test & Dev								
G Marketplace	>	Succeeded 9m 19S Status Duration						
System	>	Object	Recovered From	Recovery Point	Status	Start Time 🗸	Duration	
II. Reports		MSSQLSERVER/tpcc500g	C Local	Nov 14, 2024 11:12am	Succeeded	Nov 14, 2024 11:39am	9m 19s	
🔯 Settings	>	<u></u>				Items per page 50 👻	1 - 1 of 1 <	>

## The screenshot below elaborates on the restored SQL Server database:

	WIN. 1N2CC1 595C5 +	the sustainer of X			
enter H H H T Coulo	Column Name	Data Type	Allow Nulls		
WIN-1N2GCI 595G5 (SOI: Service 16.0.1000.6 - cm)		int			
Databases	c d id	tinvint			
🕀 🛑 System Databases		tanjan.			
🕀 🛑 Database Snapshots	c_w_id	int			
🗉 🗑 test-db	c_discount	smallmoney			
🛞 📄 tpcc500g	c_credit_lim	money			
E tpcc500grestore	c_last	char(16)			
Database Diagrams	c_first	char(16)			
E Tables	c credit	char(2)			
<ul> <li>System lables</li> <li>EileTables</li> </ul>	c halanca	money			
External Tables	Condition	money			
🗑 🗰 Graph Tables	c_ytd_payment	money			
🖂 🎹 dbo.customer	c_payment_cnt	smallint			
🕀 🗰 Columns	c_delivery_cnt	smallint			
🗉 📁 Keys	c_street_1	char(20)			
Constraints	c_street_2	char(20)			
Triggers	c city	char(20)			
Indexes	c_city	char(20)			
E Statistics	c_state	char(2)			
E E Columos	c_zip	char(9)			
E Kevs	c_phone	char(16)			
Constraints	c_since	datetime			
Triggers	c_middle	char(2)			
🗉 🗰 Indexes	c data	char(500)			
E iii Statistics					
dbo.history					
🕀 🏢 dbo.item					
m dbo.order_ine					
m dbo.stock					
dbo.warehouse					
🗄 🗰 Dropped Ledger Tables	Column Properties				
🗉 💼 Views	21 21				
External Resources	Y (General)				
🗉 🗰 Synonyms	(Name)			cid	
Programmability	Allow Nulls			No	
Guery Store     General Realize	Data Type			int	
Company Storage	Default Value or Bin	ding			
	V Table Decigner				

## Cohesity Certified Cisco UCS Nodes

This solution utilizes 4x Cisco UCS C240 M6 LFF nodes connected to Cisco UCS Fabric Interconnect in Intersight Managed Mode (IMM). Along with this configuration, Cisco and Cohesity have certified solutions with different capacity points available on All NVME Cisco X-Series modular system, all NVME Cisco UCS C-Series Rack Servers. This allows you to select your configuration based on key characteristics such as:

- Total Capacity
- Workload configurations such as Data Protection and File Services
- Performance requirements based on Cisco X-Series Modular System with All NVMe Cisco UCS X210c nodes, Cisco UCS C220 M6 All Flash or Cisco UCS C240 M6 LFF HDD configurations.
- Single node deployments for Remote offices and Branch offices (ROBO)
- Cohesity SmartFiles solution with Cisco UCS C-Series nodes

Table 17 lists the Cohesity-certified nodes on Cisco UCS Platform.

#### Table 17. Cohesity Certified Cisco UCS Nodes

Solution Name	Cisco UCS Platform	Capacity per Node	Caching SSDs/NVMe per Node
Cohesity X-Series All NVMe nodes	Cisco UCS X9508 platform	91.8 TB	
Cohesity-C240 M6 LFF-	Cisco UCS C240 M6 LFF Rack Server	12 TB	3.2 TB
Nodes		24 TB	3.2 TB
		36 TB	3.2 TB
		48 TB	3.2 TB
		64 TB	3.2 TB
		96 TB	6.4 TB
		128 TB	6.4 TB
		144 TB	6.4 TB
		192 TB	6.4 TB
		216 TB	12.8 TB
		288 TB	12.8 TB
Cohesity-M6-ROBO-Nodes	Cisco UCS C220 M6 LFF	8 TB	1920 GB
	Rack Server	16 TB	1920 GB
		24 TB	1920 GB
		36 TB	1920 GB
Cohesity-C220-All-NVMe-	Cisco UCS C220 M6 All	76 TB	

Solution Name	Cisco UCS Platform	Capacity per Node	Caching SSDs/NVMe per Node
Nodes	NVMe Rack Server	153 TB	

## About the Authors

# Anil Dhiman, Technical Leader, Technical Marketing Engineering, UCS Solutions, Compute & Networking 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, data protection and Gen Al solutions on Cisco UCS.

#### Damien Philip, Principal Solutions Architect, Cohesity

## Acknowledgements

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

- Rohit Mittal, Product Manager, Cisco Systems, Inc.
- Gopu Narasimha Reddy, Technical Marketing Engineer, Cisco Systems, Inc.
- John McAbel, Senior Product Manager, Cisco Systems, Inc.
- Francesca Harbert, Director, Cisco Global Alliance, Cohesity
- Eleonor Lee, Senior Product Marketing Manager Alliances Solutions

## Appendix

This appendix is organized into the following sections:

- Appendix A Bill of Materials
- <u>Appendix B References Used in Guide</u>
- Appendix C Known Issues and Workarounds
- <u>Appendix D Recommended for You</u>

## **Appendix A - Bill of Materials**

<u>Table 18</u> provides an example the Bill of Materials used for four (4) node Cohesity cluster for protection of SSLQ Server on Cisco Compute Hyperconverged with Nutanix, along with a pair of Cisco Fabric Interconnects, used in the testing and reference design described in this document.

1.0	UCS-M6-MLB	UCS M6 RACK, BLADE MLB	1
1.1	DC-MGT-SAAS	Cisco Intersight SaaS	1
1.1.1	DC-MGT-IS-SAAS-AD	Infrastructure Services SaaS/CVA - Advantage	4
1.1.2	SVS-DCM-SUPT-BAS	Basic Support for DCM	1
1.1.3	DC-MGT-UCSC-1S	UCS Central Per Server - 1 Server License	4
1.1.4	DC-MGT-ADOPT-BAS	Intersight - 3 virtual adopt session http://cs.co/requestCSS	1
1.2	UCSC-C240-M6L	UCS C240 M6 Rack w/o CPU, mem, drives, 2U w LFF	4
1.2.0.1	CON-L1NCO-UCSCC2L4	CX LEVEL 1 8X7XNCDOSUCS C240 M6 Rack wo CPU mem drives 2	4
1.2.1	UCS-HD12T7KL4KM	12TB 12G SAS 7.2K RPM LFF HDD (4K)	16
1.2.2	UCSC-M-V25-04	Cisco UCS VIC 1467 quad port 10/25G SFP28 mLOM	4
1.2.3	CIMC-LATEST	IMC SW (Recommended) latest release for C-Series Servers.	4
1.2.4	UCS-M2-I240GB	240GB M.2 Boot SATA Intel SSD	8
1.2.5	UCS-M2-HWRAID	Cisco Boot optimized M.2 Raid controller	4
1.2.6	UCSX-TPM-002C	TPM 2.0, TCG, FIPS140-2, CC EAL4+ Certified, for M6 servers	4

 Table 18.
 Cohesity C-Series (4 nodes) on Cisco UCS Bill of Materials

1.2.7	UCSC-RAIL-M6	Ball Bearing Rail Kit for C220 & C240 M6 rack servers	4
1.2.8	UCSC-BBLKD-S2	UCS C-Series M5 SFF drive blanking panel	8
1.2.9	UCS-DIMM-BLK	UCS DIMM Blanks	96
1.2.10	UCSC-RIS1B-240M6	C240 M6 Riser1B; 2xHDD/SSD; StBkt; (CPU1)	4
1.2.11	UCSC-RIS2A-240M6	C240 / C245 M6 Riser2A; (x8;x16;x8);StBkt; (CPU2)	4
1.2.12	UCSC-RIS3B-240M6	C240 M6 Riser 3B; 2xHDD; StBkt; (CPU2)	4
1.2.13	UCSC-HSLP-M6	Heatsink for 1U/2U LFF/SFF GPU SKU	8
1.2.14	UCSC-M2EXT-240M6	C240M6 / C245M6 2U M.2 Extender board	4
1.2.15	UCSC-MPSTOM6L-KIT	C240M6L MID PLANE KIT 4x3.5" HDD	4
1.2.16	UCS-CPU-I6326	Intel 6326 2.9GHz/185W 16C/24MB DDR4 3200MHz	8
1.2.17	UCS-MR-X16G1RW	16GB RDIMM SRx4 3200 (8Gb)	32
1.2.18	UCSC-SAS-M6HD	Cisco M6 12G SAS HBA (32 Drives)	4
1.2.19	UCS-HD12T7KL4KN	12TB 12G SAS 7.2K RPM LFF HDD (4K)	48
1.2.20	UCS-NVME4-6400	6.4TB 2.5in U.2 15mm P5620 Hg Perf Hg End NVMe (3X)	8
1.2.21	UCSC-PSU1-1200W	1200w AC Titanium Power Supply for C-series Rack Servers	8
1.2.22	CAB-C13-C14-2M	Power Cord Jumper, C13-C14 Connectors, 2 Meter Length	8
1.2.23	UCS-SID-INFR-DTP	Data Protection Platform	4
1.2.24	UCS-SID-WKL-OW	Other Workload	4
1.3	UCS-FI-6454-U	UCS Fabric Interconnect 6454	2
1.3.0.1	CON-L1NCO-SFI6454U	CX LEVEL 1 8X7XNCDOSUCS Fabric Interconnect 6454	2
1.3.1	N10-MGT018	UCS Manager v4.2 and Intersight Managed Mode v4.2	2

1.3.2	UCS-PSU-6332-AC	UCS 6332/ 6454 Power Supply/100-240VAC	4
1.3.3	CAB-C13-C14-2M	Power Cord Jumper, C13-C14 Connectors, 2 Meter Length	4
1.3.4	UCS-ACC-6332	UCS 6332/ 6454 Chassis Accessory Kit	2
1.3.5	UCS-FAN-6332	UCS 6332/ 6454 Fan Module	8

## Appendix B - References Used in Guide

Cisco Intersight: https://www.cisco.com/c/en/us/products/servers-unified-computing/intersight/index.html

Cisco Unified Computing System: http://www.cisco.com/en/US/products/ps10265/index.html

Cisco Compute Hyperconverged with Nutanix for Microsoft SQL Server 2022 Databases: <u>https://www.cisco.com/c/en/us/td/docs/unified\_computing/ucs/UCS\_CVDs/cisco\_nutanix\_sql.html</u>

Cisco Compute Hyperconverged with Nutanix in Intersight Standalone Mode: <u>https://www.cisco.com/c/en/us/td/docs/unified\_computing/ucs/UCS\_CVDs/CCHC\_Nutanix\_ISM.html</u>

#### Cisco UCS C-Series

Product Installation Guide:

https://www.cisco.com/c/en/us/td/docs/unified\_computing/ucs/c/hw/c240m6/install/b-c240-m6-installguide.html

Cohesity on Cisco: <u>https://www.cisco.com/c/en/us/solutions/global-partners/cohesity.html</u> and <u>https://www.cohesity.com/solutions/technology-partners/cisco/</u>

Cohesity Guide for Backup of Microsoft SQL Server:

https://docs.cohesity.com/6\_8\_1/Web/UserGuide/Content/MSSQL/SQLProtection.htm?tocpath=Databases%7 CMicrosoft%20SQL%20Server%7CBackup%20Microsoft%20SQL%20Server%7C\_\_\_\_0 and https://docs.cohesity.com/HomePage/PDFs/Cohesity-Solution-Guide-Protect-SQL-Server-Databases.pdf

## Appendix C - Known Issues and Workarounds

## **IPMI Warning on Cohesity System Health Status**

When the Cohesity cluster is configured, you may see "IPMI config Absent" alerts on Cohesity Health Tab. Cisco UCS C-Series with Cohesity does not require any IPMI configuration on the cluster. Please ignore this warning or contact Cohesity support for more details.

The warning is detailed below:

#### Details for IpmiConfigAbsent

25 Occurrences | First Occurrence Jun 5, 2023 7:58am | Last Occurrence Jun 5, 2023 10:04am

(May 30, 2023 - Jun 05 Chart	5, 2023								ବ୍ ୦ ୦
Chart with 25 data poin The chart has 1 X axis o The chart has 1 Y axis o	nts. displaying Time. R displaying values.	ange: 2023-06-05 00:0 Range: -1 to 3.	0:00 to 2023-06-05 23:59:	59.					
5. Jun 02:00 am	04:00 am	05:00 am 08	:00 am 10:00 am	12:00 pm	14:00 pm	16:00 pm	18:00 pm	20:00 pm	22:00 pm
Alert Code CE03701074	Severity Info	<b>Type</b> Maintenance	Category Configuration	Status Active					
Description IPMI config is absent o	n cluster id 21382	224323806634.							
Cause IPMI Config is highly re	ecommended on p	physical cluster but no	t configured.						
Resolution									
Create new resolut	tion () Associa	te with existing resolu	tion						

## Appendix D - Recommended for You

#### **Cisco Intersight**

Cisco Intersight Help Center: https://intersight.com/help/saas/home

#### **Cisco UCS C-Series**

#### **Product Installation Guide:**

https://www.cisco.com/c/en/us/td/docs/unified\_computing/ucs/c/hw/c240m6/install/b-c240-m6-installguide.html

#### **Cohesity on Cisco**

https://www.cisco.com/c/en/us/solutions/global-partners/cohesity.html

https://www.cohesity.com/solutions/technology-partners/cisco/

#### Microsoft SQL Server protection with Cohesity

https://docs.cohesity.com/HomePage/PDFs/Cohesity-Solution-Guide-Protect-SQL-Server-Databases.pdf

https://docs.cohesity.com/HomePage/PDFs/Cohesity-Solution-Guide-Protect-SQL-Server.pdf

#### **Cohesity on Cisco X-Series**

Validated Design:

https://www.cisco.com/c/en/us/td/docs/unified\_computing/ucs/UCS\_CVDs/ucs\_xseries\_cohesity.html

#### Ansible Automation

Ansible automation for Cohesity server profile for Cisco UCS X-Series: https://developer.cisco.com/codeexchange/github/repo/ucs-computesolutions/intersight\_cohesity\_xseries\_ansible/

## Feedback

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

## **CVD Program**

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 IMPLE-MENTING 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 UCS X-Series, 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 trade-marks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. (LDW P2)

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)

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)